Об Ideco NGFW Novum

> Ideco NGFW Novum - многофункциональный межсетевой экран с фильтрацией до уровня L7, поддержкой VPN, ZTNA и кластеризации. Обеспечивает защиту и контроль трафика в компаниях уровня enterprise.

Возможности Ideco NGFW Novum

- ☑ Межсетевой экран
- ☑ Система предотвращения вторжений
- ☑ Контент-фильтр
- ☑ Контроль приложений
- ☑ Антивирусная и антиспам-проверка трафика
- ☑ Защита от ботнетов, фишинга и шпионского ПО
- ☑ Поддержка работы до 100 тысяч правил Файрвола
- ☑ Производительность ядра сети: до 200 Гбит/с, поддержка до 25 миллионов сессий и 1 миллиона новых TCP-сессий в секунду.
- ☑ Настройка физических портов и перенос настроек на другой порт без изменения политик безопасности
- ☑ Внедрение без перестройки сети и быстрый запуск пилотных проектов благодаря L2-мосту
- ☑ VPN site-to-site (GRE, IPSec, ГОСТ VPN) и client-to-site (IKEv2/IPSec, L2TP/IPSec, SSTP, Wireguard, TLS в Ideco Client) с 2FA
- ☑ Логирование действий администратора
- ☑ Создание высокопроизводительного виртуального контекста с функциями NGFW Novum
- ☑ Управление через Ideco Center
- ☑ Отчетность по трафику пользователей и событиям безопасности
- ☑ Интеграция с Microsoft Active Directory, ALD Pro, Samba DC, SIEM, Zabbix и DLP-системами

И это далеко не полный список возможностей и сервисов Ideco NGFW Novum, которые позволяют создать надежный барьер для защиты локальной сети от современных угроз безопасности.

Техническое описание Ideco NGFW Novum доступно по ссылке.

Скачать Ideco NGFW Novum можно в личном кабинете.

Видеодокументация доступна на YouTube и Rutube.

О документации

Документация содержит подробные инструкции, описания функций и рекомендации по устранению проблем. Как эффективно использовать документацию:

Навигация по разделам

Слева на странице расположены блоки с разделами:

- **Общая информация** - блок содержит информацию о доступных в Ideco NGFW Novum лицензиях, системных требованиях, режимах работы технической поддержки и информацию о продуктах, которые могут интегрироваться в инфраструктуре с продуктами Ideco.
- **Быстрый старт** - блок статей поможет произвести первоначальные настройки Ideco NGFW Novum, включая создание загрузочного USB-накопителя, установку и подключение к веб-интерфейсу, импорт корневого сертификата, настройку Ethernet-подключения и активацию лицензии.
- **Настройка Ideco NGFW Novum** - включает разделы с подробными статьями по настройке Ideco NGFW Novum. Разделы повторяют структуру веб-интерфейса Ideco NGFW Novum, обеспечивая удобство и простоту использования.
- **Популярные инструкции и диагностика проблем** - содержит по тематике диагностики проблем и ответы на часто задаваемые вопросы.
- **API** - документация по API перенесена и доступна по ссылке. Блок описывает API-запросы, которые управляют функциями и настройками Ideco NGFW Novum. Среди них - авторизация, работа с объектами, настройка правил и многое другое.

Поиск информации

Введите запрос в строку поиска в правом верхнем углу страницы. Поиск выполняется по документации, относящейся к текущему продукту.

Документация высокопроизводительного контекста

В документации Ideco NGFW Novum добавлена новая функция - возможность переключаться между виртуальными контекстами. Подробнее о VCE в статье:

- **Классический контекст** - документация для **Системного контекста** и всех его дочерних контекстов, созданных с использованием классического типа.
- **Высокопроизводительный контекст** - документация, специально разработанная для высокопроизводительного контекста, учитывающая его уникальные особенности и отличия.

Переключение между контекстами осуществляется с помощью кнопок в верхней части статьи. Типы кнопок и их назначение:

- **Оранжевая кнопка** - подсвечивает, документация какого контекста сейчас активна.
- **Белая кнопка** - переключает на документацию другого контекста. Например, если активна кнопка **Классический контекст**, то белая кнопка **Высокопроизводительный контекст** откроет соответствующую статью в документации по высокопроизводительному контексту.

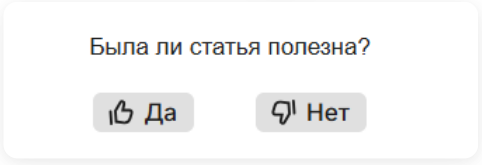
Поиск по документации осуществляется только в пределах выбранного контекста.

Обратная связь

Мы постоянно совершенствуем нашу документацию и всегда рады вашим отзывам.

Как оставить отзыв:

- Поставить реакцию в правом верхнем углу или в конце любой статьи:

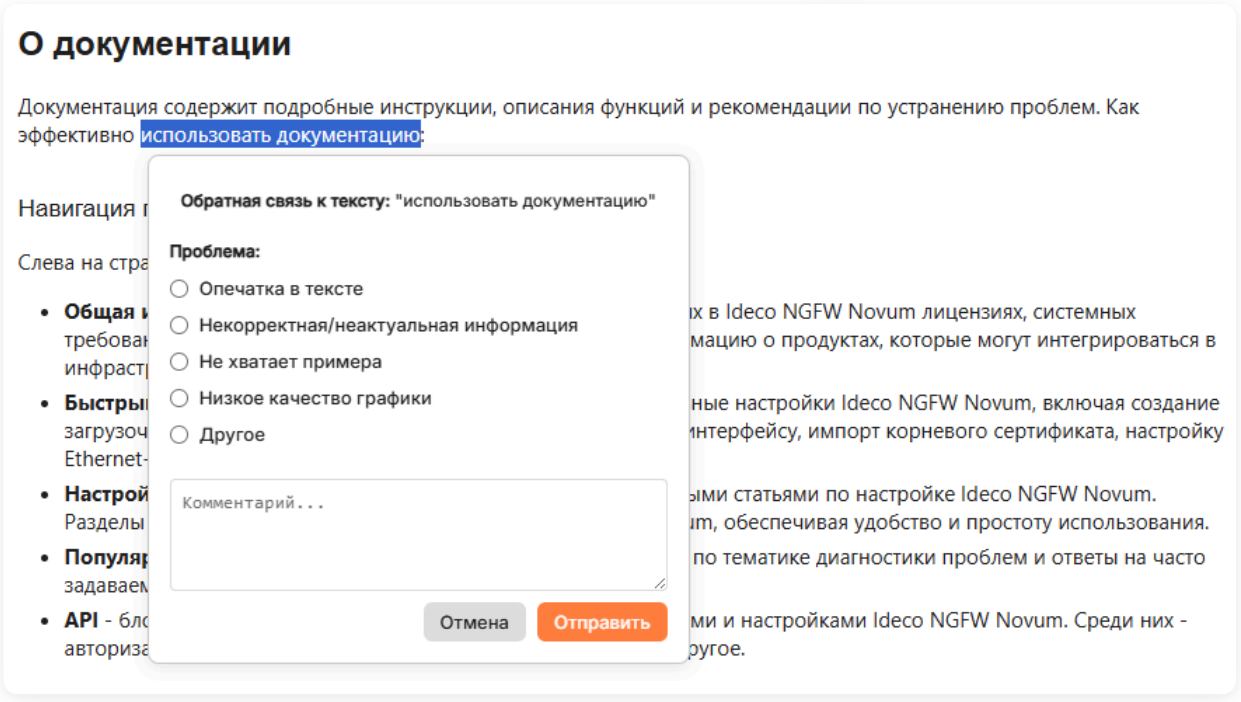


- Написать комментарий к фрагменту текста внутри статьи.

Если рекомендации из статьи не помогли, нажмите , заполните форму обратной связи, нажмите **Отправить**, а затем - **Обратиться в техподдержку**.

Чтобы написать комментарий:

1. Выделите фрагмент, который хотите прокомментировать, и нажмите на иконку . Иконка появляется при выделении фрагмента от 5 символов:



2. Выберите проблему и при необходимости опишите ее в поле **Комментарий** (не менее 5 символов).

3. Нажмите **Отправить**.

Лицензирование

> В статье представлено описание доступных в Ideco NGFW Novum лицензий.

Лицензирование позволяет передать программное обеспечение в пользование на условиях лицензии: пользователь получает возможность использовать продукт, а владелец продукта сохраняет за собой право собственности.

У лицензии Ideco NGFW Novum есть три основные характеристики:

- **Количество пользователей Ideco NGFW Novum** - авторизованные пользователи локальной сети или подключенные по VPN пользователи, трафик которых проверяется и контролируется шлюзом.
- **Редакция Ideco NGFW Novum (вид лицензии)** - набор доступных к использованию модулей в системе и особенности работы модулей.
- **Срок действия лицензии** - часть функций остается доступной после завершения срока.

Особенности лицензирования:

- Количество приобретенных по лицензии учетных записей ограничивает число авторизованных пользователей.
- Под одной учетной записью пользователя на Ideco NGFW Novum можно авторизовать до пяти устройств с помощью различных методов авторизации. При авторизации шестого устройства будет разорвана самая старая сессия.
- При изменении вида лицензирования некоторые модули могут работать некорректно в течение суток до автоматического обновления информации о лицензии. Для обновления информации о лицензии перейдите в **Управление сервером** → **Лицензия** веб-интерфейса NGFW и нажмите **Обновить информацию о лицензии**.

Подробнее об управлении лицензиями - в статье.

Виды лицензий

В Ideco NGFW Novum доступны лицензии:

Enterprise

Enterprise - коммерческая лицензия.

- [x] Бессрочное право на использование Ideco NGFW Novum
- [x] Включает в себя годовую подписку **Security Update**
- [x] Лицензирование по числу активных пользователей или по количеству ядер виртуальной машины
- [x] Для программно-аппаратных комплексов Ideco доступно лицензирование без ограничения по количеству пользователей

В период действия подписки **Security Update** доступны следующие преимущества:

- Обновления на новые версии Ideco NGFW Novum.
- Расширенная база категорий **Контент-фильтра**.
- Модуль **Предотвращение вторжений**.
- Модуль **Контроль приложений**.
- Автоматическое обновление баз модулей.
- Техническая поддержка.

По истечении срока подписки **Security Update** для сервера Ideco NGFW Novum:

- **Контроль приложений** - модуль отключается.
- **Контент-фильтр** - становятся доступны только пользовательские категории.
- **Предотвращение вторжений** - остается доступна старая отчетность, но анализ трафика отключается.
- **Техническая поддержка** - недоступна.
- Обновление баз модулей - недоступно.
- Обновление на версии, вышедшие после даты окончания подписки - недоступно.



Для использования кластера и/или модуля **DNS security** Ideco NGFW Novum потребуются дополнительные лицензии.

Enterprise-demo

Enterprise-demo - бесплатная лицензия сроком на 44 дня.

- ☑ Авторизация до 10 000 пользователей
- ☑ Включены все модули, кроме технологий Касперского для фильтрации почтового трафика
- ☑ Техническая поддержка

Лицензию нельзя переназначить на другой сервер или переместить в свободные лицензии. Выдается автоматически один раз при регистрации сервера в разделе **Управление сервером** → **Лицензия** веб-интерфейса NGFW.

По истечении срока действия лицензии для сервера Ideco NGFW Novum:

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокирован FORWARD- и INPUT-трафик. Кроме доступа к MY.IDECO.
- Доступен перехват DNS-запросов и подключение по SSH при включении удаленного помощника.

Free

Free - свободная лицензия с ограниченным набором функций, сроком на 5 лет.

- ☑ Авторизация до 22 пользователей
- ☑ Интеграция с **Active Directory** на 2 года
- ☑ **Контроль приложений**, **Предотвращение вторжений** и расширенный **Контент-фильтр** доступны на 2 года с даты создания лицензии

Техническая поддержка не предоставляется. Недоступно: **Кластеризация**, **Расширенная база правил** (от Лаборатории Касперского) для модуля **Предотвращение вторжений**, **Антивирус Касперского** и **Антиспам Касперского**.

Чтобы добавить лицензию **Free** в личный кабинет, нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Непривязанные лицензии**.

При отсутствии/окончании срока действия лицензии для сервера Ideco NGFW Novum:

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокирован FORWARD- и INPUT-трафик. Кроме доступа к MY.IDECO.
- Доступен перехват DNS-запросов и подключение по SSH при включении удаленного помощника.

Более подробная информация о видах лицензий в Ideco доступна на сайте.

Лицензия с режимом кластеризации и технологии Лаборатории Касперского приобретаются отдельно в отделе продаж.

> NGFW Novum без лицензии по умолчанию не пропускает трафик пользователей в интернет. Для получения лицензии используйте альтернативный (дополнительный) шлюз. Если это невозможно, временно включите опцию **Полный доступ** - для этого перейдите в раздел **Техническая поддержка**, нажав  в правом верхнем углу экрана. Подробнее - в статье.

Лицензирование с режимом кластеризации

- Если право использования ПО было приобретено до 01.08.2024, все Enterprise-лицензии с действующей подпиской (Security Update) включают в себя право использования ПО для всех нод кластера со сроком использования до 01.07.2029.
- Право использования ПО для ноды кластера нужно приобретать дополнительно.
- Если приобретается право использования ПО для нод кластера, то при продлении подписки Security Update возможно только совокупное продление подписки Security Update для всех нод кластера. Продление подписки Security Update для основной лицензии и для ноды кластера по отдельности не осуществляется.
- Функциональная возможность использования ПО в кластере после приобретения права на использование для ноды кластера является бессрочной, однако подписка Security Update остается срочной.
- После окончания срока действия подписки Security Update работа кластера не нарушается.

Просмотр информации о лицензиях

Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др. Посмотреть информацию о лицензии и доступных модулях можно:

- На MY.IDECO.RU. Здесь также можно получить лицензию, посмотреть информацию о зарегистрированных серверах и настроить связь лицензий с серверами.
- В разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum.

Подробная информация об управлении лицензиями и привязке лицензии к серверу представлена в статье.

Особенности работы онлайн-лицензии:

- При наличии доступа в интернет обновление данных о лицензии происходит один раз в сутки.
- Если связь с серверами лицензирования отсутствует, Ideco NGFW Novum предпринимает попытки соединения каждые 60 секунд до восстановления доступа.
- Если у Ideco NGFW Novum отсутствует связь с серверами лицензирования более 30 дней, то Ideco NGFW Novum перейдет в нелицензионный режим.
- Для использования Ideco NGFW Novum в закрытом контуре (без доступа к интернету) необходимо использовать офлайн-лицензию.

Классический контекст | Высокопроизводительный контекст

Системные требования

Перед регистрацией и загрузкой образа Ideco NGFW Novum с MY.IDECO ознакомьтесь с системными требованиями к платформе, на которую будет установлен Ideco NGFW Novum:

- Выбор аппаратной платформы
- Виртуальная платформа

Для ФСТЭК версий Ideco UTM используются платформы:

- Программно-аппаратный комплекс (ПАК) - для межсетевых экранов типа А четвертого класса защиты.
- Виртуальная платформа - для межсетевых экранов типа Б четвертого класса защиты.

Для ФСТЭК версии Ideco NGFW Novum четвертого класса защиты используется только ПАК.

Производительность платформы

Рекомендуем использовать физический сервер, так как производительность на сервере выше по сравнению с работой в гипервизоре при сопоставимых параметрах.

Частота процессора, а также объем и частота ОЗУ сервера сильно зависят от нагрузки на Ideco NGFW Novum. При подсчете нагрузки нужно учитывать два фактора:

- Задействованные компоненты NGFW Novum (**Контроль приложений**, **Прокси** с подключенными сервисами, проверка трафика на спам/вирусы, обширность настройки модуля **Контентной фильтрации** или **Межсетевого экрана**).
- **Система предотвращения вторжений** - при скорости подключения к провайдеру от 100 Мбит/с эта служба может потребовать значительных ресурсов процессора и памяти. Рекомендуется использовать многоядерные процессоры (4 и более ядер с частотой более 3 ГГц) и от 16 ГБ оперативной памяти.

При туннелировании по типу site-to-site с небольшим количеством соединений (от 3 до 5) допустимо использовать процессор с меньшим количеством ядер, но с большей частотой. Если Ideco NGFW Novum планируется использовать как VPN-сервер для S2S и C2S с большим количеством соединений, то лучше выбрать процессор и с большим количеством ядер, и с большей частотой. Это обусловлено тем, что соединения могут распределяться по ядрам.

Выбор аппаратной платформы

> В статье представлен набор требований для корректной работы Ideco NGFW Novum на аппаратной платформе.

Программно-аппаратный комплекс

Работа Ideco NGFW Novum с конечными устройствами гарантирована только на программно-аппаратных комплексах (ПАК). Для выбора ПАК обратитесь в отдел продаж.

Сертифицированные ПАК не имеют автономного управления платформой (IPMI).

ПАК имеют регистрацию в реестре Минпромторга на базе сетевых устройств Рубеж от компании АО "КРАФТВЭЙ КОРПОРЭЙШН ПЛС":

- Для Ideco NGFW Novum MX2/LX/LX+ - номер записи 10465633, ссылка.
- Для Ideco NGFW Novum EX - номер записи 10549715, ссылка.

Собственный сервер

Минимальные системные требования

Корректная работа на стороннем оборудовании не гарантируется.

Минимальные системные требования удовлетворяют низкой загруженности служб NGFW, обслуживающих небольшое количество авторизованных пользователей (до 50 человек).

Платформы Ideco SX+ и Ideco SMX в текущих версиях не поддерживают запуск VCE. Поддержка планируется в следующих версиях.

Требования	Характеристики
Процессор	• Intel i3/i5/i7/i9/Xeon минимум 4 поколения Haswell (2013г.) • AMD FX/Ryzen/EPYC. • Поддержка SSE 4.2. • От 4 ядер.
Объем оперативной памяти	• От 16 ГБ (16-64 ГБ в зависимости от количества пользователей, от 32 ГБ с созданием VCE).
Накопитель	• Объем 150 ГБ или более. • Запись 4K блоками в один поток, с синхронизацией каждой записи не менее 1000 IOPS. • SSD с интерфейсом SATA, mSATA, SAS, NVMe. • Дополнительный SSD при использовании почтового сервера. • Не гарантируется работа с аппаратными RAID-контроллерами (программные контроллеры, интегрированные в чипсет, не поддерживаются).
Сеть	• Две сетевые карты (или два сетевых порта) 100/1000 Mbps на чипах Intel.
BIOS	• Поддержка UEFI. • Отключенная опция Secure Boot в UEFI. • Отключенный режим Legacy, может называться CSM (Compatibility Support Module).
Дополнительно	• Монитор и клавиатура (не требуется, если используется IPMI).

Высокопроизводительный контекст поддерживает работу до 100 000 правил **Межсетевого экрана**.

Минимальные требования (для 10K-100K правил):

- Процессор: от 8 ядер.
- Оперативная память: от 64 ГБ.

Полная загрузка правил в интерфейсе может занять несколько минут.

На каждый VCE требуется:

- Классический контекст: не менее 2 ядер CPU и 8 ГБ оперативной памяти.
- Высокопроизводительный контекст: не менее 4 ядер CPU и 8 ГБ оперативной памяти.
- Дисковое пространство: дополнительное место на SSD в зависимости от нагрузки.

Рекомендации

Ознакомьтесь с требованиями к производительности платформы по ссылке.

Чипсеты и производители

- Рекомендуем чипсеты, контроллеры и сетевые карты компании Intel.
- Не гарантируем стабильную работу и заявленную производительность, а также поддержку работоспособности сети при использовании встроенных сетевых карт, особенно интерфейсов на бюджетных/редких/устаревших/noname чипсетах.
- Не рекомендуем использовать RAID-контроллеры, так как они официально не поддерживаются нашим продуктом.
- Материнские платы могут использоваться как серверные, так и десктопные. Рекомендуем использовать процессоры Intel и AMD.

Дисковая подсистема

- Рекомендуем использовать серверные SSD с технологией защиты от сбоев питания (Power Loss Protection (PLP)).
- В большинстве конфигураций достаточно одного SSD объемом от 200 ГБ.
- Если на NGFW развернут почтовый сервер, для хранения электронной почты необходимо подключить отдельный накопитель.
- Рекомендуемые производители: Micron, Transcend, Kingston, Samsung.

Виртуальная платформа

В статье представлен набор требований для корректной работы Ideco NGFW Novum на виртуальной платформе.

Минимальные системные требования

Минимальные системные требования удовлетворяют низкой загруженности служб NGFW, обслуживающих небольшое количество авторизованных пользователей (до 50 человек).

Требования	Характеристики
Платформы виртуализации	• VMware (Workstation и ESXi) версии не ниже 6.5.0. • Microsoft Hyper-V (виртуальные машины 2-го поколения). • VirtualBox версии не ниже 7.0.0. • KVM версии не ниже 1.2.0. • Citrix XenServer. • Proxmox VE.
Тип ОС для создания виртуальной машины	• Linux Fedora 64 bit.
Процессор	• Поддержка SSE 4.2. • От 4 ядер.
Объем оперативной памяти	• 16 ГБ (16-64 ГБ в зависимости от количества пользователей).
Накопитель	• Объем 150 ГБ или более. • Запись 4К блоками в один поток, с синхронизацией каждой записи не менее 1000 IOPS. • Дополнительный диск при использовании почтового сервера. • KVM: virtio для дисков.
Сеть	• WMWare: vmxnet3. • VirtualBox: сетевая карта с типом подключения NAT. • KVM: virtio. • Microsoft Hyper-V: виртуальный сетевой адаптер (Network Adapter).
BIOS	• Поддержка UEFI. • Отключенная опция Secure Boot в UEFI. • Отключенный режим Legacy, может называться CSM (Compatibility Support Module).
Дополнительно	• Внутренние часы виртуальной машины должны быть настроены на хранение времени во временной зоне UTC.

Высокопроизводительный контекст поддерживает работу до 100 000 правил **Межсетевого экрана**.

Минимальные требования (для 10К-100К правил):

- Процессор: от 8 ядер.
- Оперативная память: от 64 ГБ.

Полная загрузка правил в интерфейсе может занять несколько минут.

На каждый VCE требуется:

- Классический контекст: не менее 2 ядер CPU и 8 ГБ оперативной памяти.
- Высокопроизводительный контекст: не менее 4 ядер CPU и 8 ГБ оперативной памяти.

- Дисковое пространство: дополнительное место на SSD в зависимости от нагрузки.

Для максимальной производительности рекомендуем:

- Режим работы кэша виртуального диска: writeback. Хранилище должно гарантировать сохранность данных после завершения команды фиксации кэша.
- Настроить паравиртуализованный источник энтропии (Random Number Generator (RNG)).
- Настроить паравиртуализованные часы и таймер.
- Убедиться, что виртуальные процессоры, использующиеся для виртуальной машины, располагаются на одной физической NUMA-ноде.
- Гипервизор с аппаратной виртуализацией (вложенная виртуализация не требуется).

Ознакомьтесь с требованиями к производительности платформы по ссылке.

Информация по настройке гипервизора доступна по ссылке.

Техническая поддержка

Одним из главных приоритетов компании Ideco является высокий уровень удовлетворенности наших клиентов.

Техническая поддержка предоставляется в период действия подписки на сервис. Подписка включена в стоимость лицензии и действует в течение года с момента приобретения продукта. После окончания срока действия подписка может быть продлена на срок от 1 года и более.

Подробнее о подписке на техническую поддержку и обновления можно посмотреть на сайте компании Ideco.

График работы

Дни недели	Время работы (московское)
понедельник-пятница	04:00 - 21:00
суббота	09:00 - 16:00
воскресенье и праздничные дни	выходной/особое расписание

В рамках расширенной технической поддержки на договорных условиях техподдержка оказывается круглосуточно 24x7x365.

Способы обращения

Способ	Обращаться через
Портал поддержки. Для получения доступа к порталу отправьте запрос на электронную почту support@ideco.ru	support.ideco.ru
Телефон	+7 (495) 662-87-34
Telegram	ideco_support_bot
MAX	id6670208848_bot
Интерактивный онлайн-чат со специалистом технической поддержки	https://my.ideco.ru/, https://ideco.ru/, веб-интерфейс Ideco NGFW Novum

Правила обращения

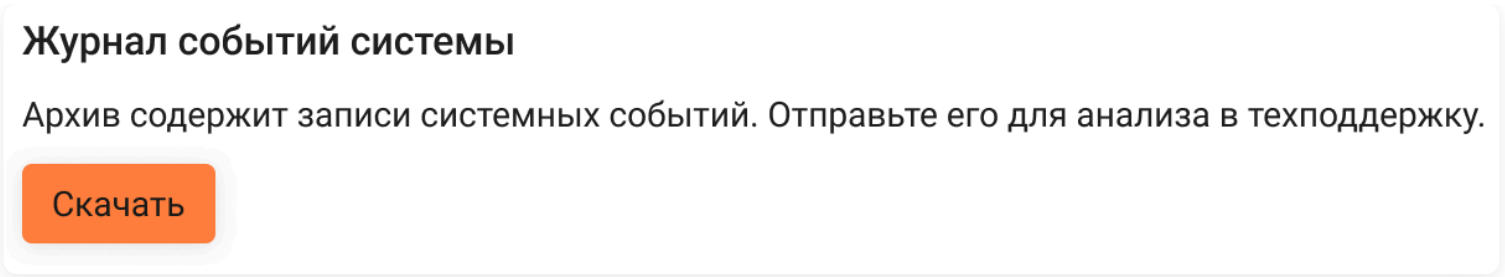
Техническая поддержка пользователей осуществляется в соответствии с регламентом.

- Техническая поддержка оказывается по вопросам настройки продуктов компании "Айдеко";
- Специалисты службы техподдержки не занимаются обучением пользователей продукту в рамках оказания услуг по поддержке.

При обращении необходимо предоставить следующую информацию: название организации, ваши контактные данные, номер лицензии.

Скачивание журнала системных событий

В веб-интерфейсе Ideco NGFW Novum доступно скачивание журнала системных событий для передачи в техническую поддержку.
Для скачивания нажмите в правом верхнем углу экрана, а затем **Скачать** в блоке **Журнал событий системы**:



Начнется загрузка архива в формате **zst** с файлом логов:

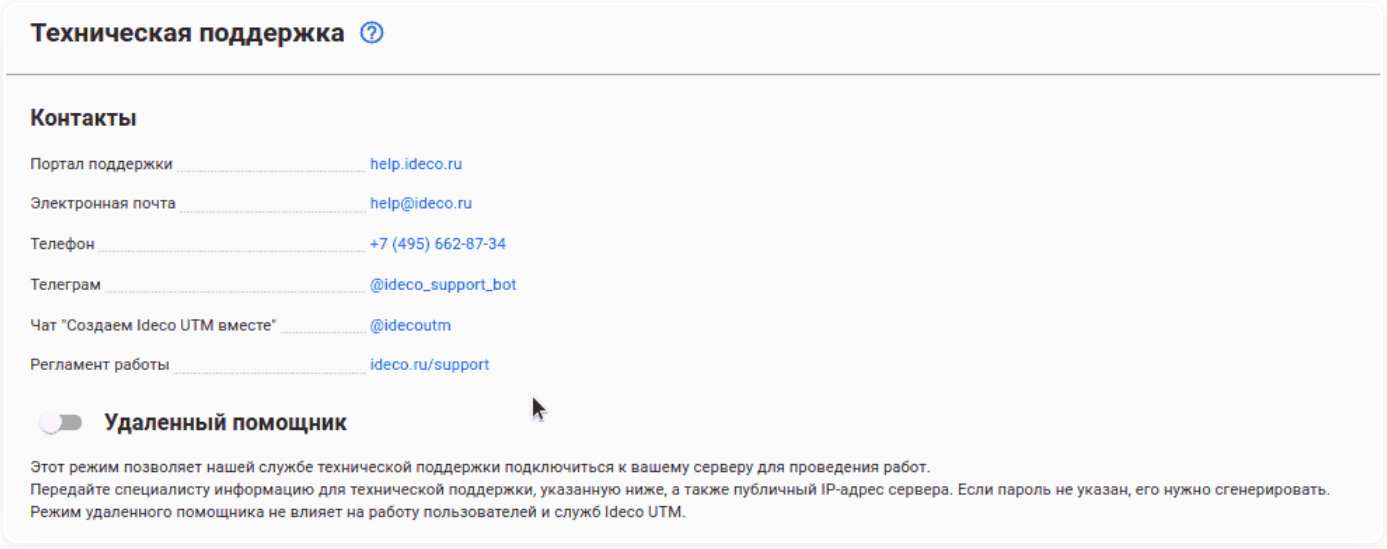
- Если установка первичная или не было возврата к предыдущей версии, файл будет содержать события текущей версии.
- Если был возврат к предыдущей версии, файл будет содержать события версии, с которой произошел возврат, и события текущей версии, записанные до возврата.

Режим удаленного помощника

Чтобы служба технической поддержки могла подключиться к серверу удаленно, необходимо включить режим удаленного помощника. Работа сервера в этом режиме не влияет на работу пользователей.

Для включения режима удаленного помощника нажмите на значок в правом верхнем углу экрана и переведите ползунок около пункта **Удаленный помощник** в статус **Включен**.

Включение режима удаленного помощника изменяет таблицу правил **Межсетевого экрана**. При этом становится доступно подключение по SSH: из WAN-зоны - только для ограниченного списка адресов Технической поддержки, из локальных сетей - для любого источника.



Включение режима удаленного помощника из веб-интерфейса

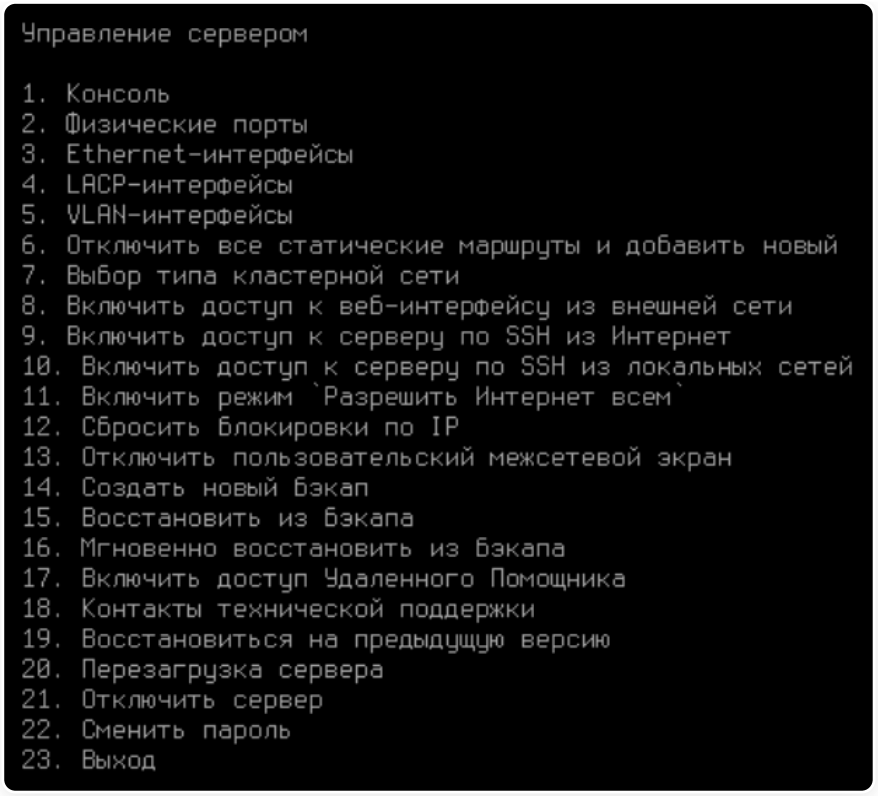
Для подключения специалиста технической поддержки сообщите ему **Информацию для технической поддержки**, нажав кнопку **Скопировать**. Также нужно отдельно передать публичный IP-адрес сервера. Если сервер подключен не напрямую к Ideco NGFW Novum, выполните проброс с внешнего маршрутизатора до 22-го порта на NGFW.

Режим удаленного помощника остается включенным даже при перезагрузке сервера. Отключайте режим удаленного помощника, когда использовать режим нет необходимости. **Крайне не рекомендуется постоянная эксплуатация сервера Ideco NGFW Novum в этом режиме.**

Включение режима удаленного помощника из локального меню сервера

Чтобы включить режим удаленного помощника, в локальном меню Ideco NGFW Novum введите номер пункта **Включить доступ Удаленного помощника**, затем нажмите **Enter**.

Сгенерируется пароль, который необходимо сообщить технической поддержке для подключения по SSH:



Работа с сервером по протоколу SSH в режиме удаленного помощника

Чтобы организовать работу с локальной консолью сервера удаленно по протоколу SSH от пользователя **root** в режиме удаленного помощника, необходимо выполнить следующие действия:

1. Подключитесь к серверу с помощью SSH-клиента **PuTTY**. Программа бесплатна, скачать можно на сайте разработчиков (https://www.putty.org/).

2. При подключении из локальной сети используйте адрес, который настроен на локальной сетевой карте Ideco. Введите необходимые параметры для подключения:

- **порт** - 22;
- **логин** - remsup;
- **пароль, указанный при включении удаленного помощника.**

Символ "#" свидетельствует, что работа ведется от имени суперпользователя.

Полный доступ

Классический контекст | Высокопроизводительный контекст

Используйте режим только для диагностики.

Режим **Полный доступ** не отключается автоматически и продолжает работать, пока режим не отключить вручную.

При включении:

- Сбор веб-статистики будет отключен.
- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включен автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Межсетевого экрана**.

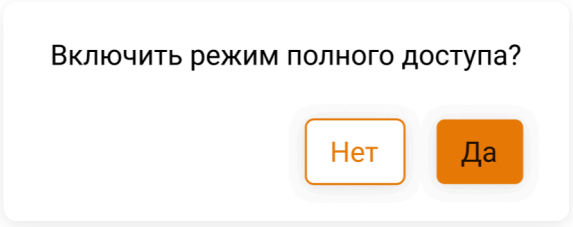
Цикл обработки трафика в Ideco NGFW Novum описан в статье.

Включить режим можно через:

Веб-интерфейс

Нажмите на иконку технической поддержки в верхней правой части окна, а затем в блоке **Полный доступ** нажмите **Включить**:

Подтвердите выбор, нажав **Да**:



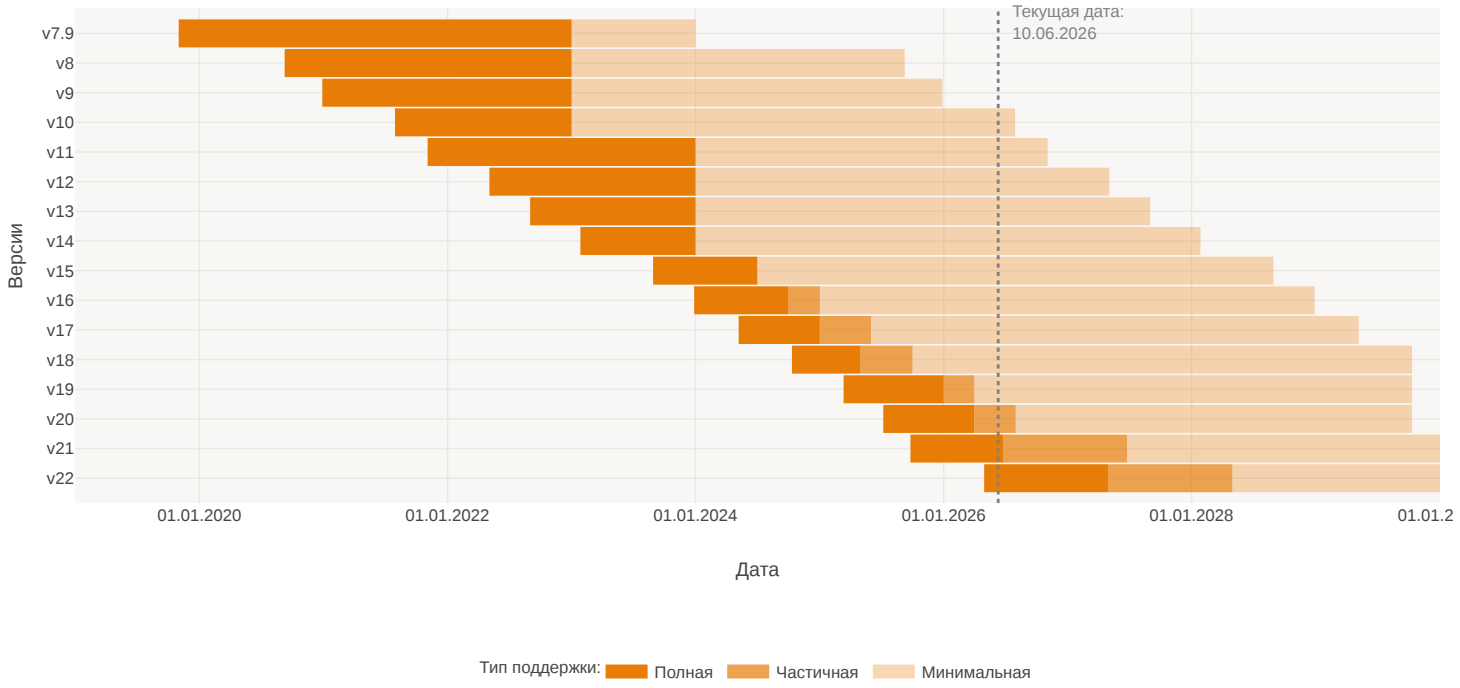
Локальное меню

Выберите **Включить режим Разрешить интернет всем** и нажмите **Enter** для применения настройки:

Информация о поддержке версий Ideco NGFW Novum

В статье описываются типы поддержки Ideco NGFW Novum и сроки поддержки по каждой версии.

Сроки поддержки



Что входит в типы поддержки

✅ Поддержка гарантируется.

❓ Поддержка не гарантируется. Стараемся поддерживать максимально долго, но гарантий нет.

Тип	Полная	Частичная	Минимальная
Автообновление системы	✅	✅	✅
Обновление баз: • Предотвращение вторжений • Контент-фильтр • IpList • GeoIP	✅	❓	❓
Антивирус Касперского	✅	❓	❓
Антивирус и антиспам Касперского для почты	✅	❓	❓
Сигнатуры IPS от Лаборатории Касперского	✅	❓	❓
Исправление некритичных багов (например, ошибка в тексте)	✅	❓	❓
Баги безопасности (CVE)	✅	✅	❓
Исправление критических багов (влияют на работу продукта в целом или отдельного модуля)	✅	✅	❓

Техническая поддержка (простое обращение)	✅	✅	❓
Техническая поддержка (сложное обращение)	✅	❓	❓
Документация	✅	✅	❓

Настройка двухфакторной аутентификации с использованием TOTP-токенов

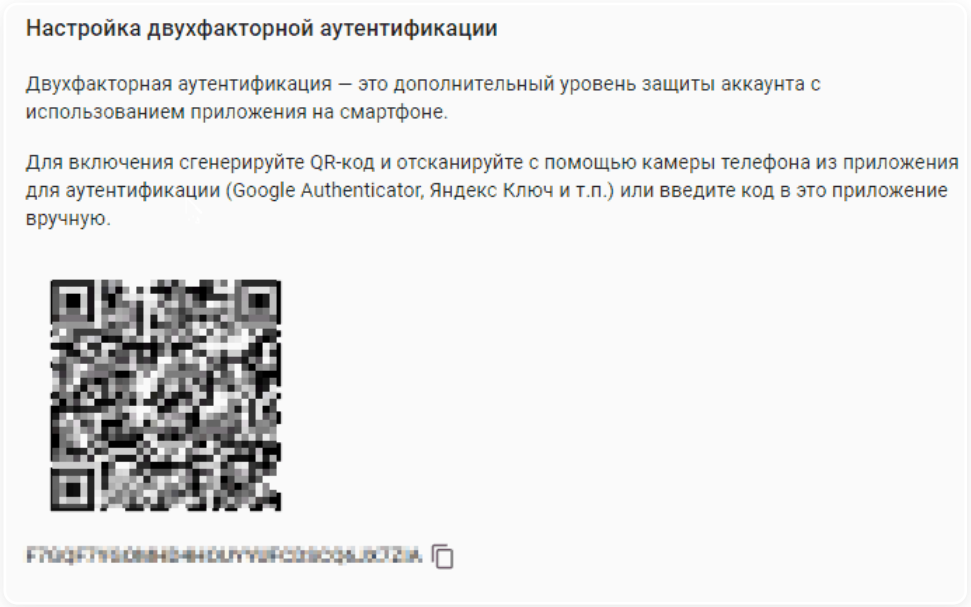
TOTP (Time-based One-Time Password) - это временные одноразовые пароли, которые меняются каждые 30 секунд. Метод аутентификации с использованием TOTP-токенов обеспечивает дополнительный уровень безопасности для ваших аккаунтов.

Для настройки выполните действия:

1. Установите приложение:

- Для смартфонов (Android/iOS):
  - Google Authenticator: Play Market (Android), App Store (iOS).
  - Яндекс ID: Play Market (Android), App Store (iOS).
  - Другое аналогичное приложение.
- Браузерное расширение для компьютеров, например:
  - Аутентификатор для Chrome.
  - Authenticator для Firefox.

2. Активируйте 2FA на NGFW Novum. Подробнее - в статье. Система отобразит QR-код и секретный ключ (строка букв и цифр):

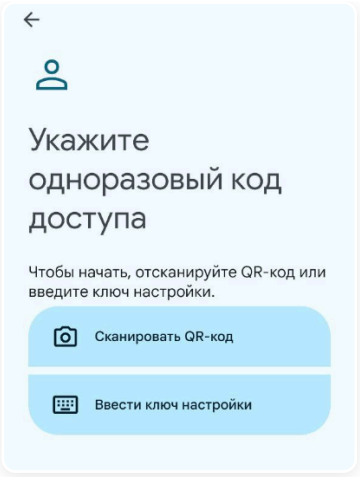


3. Добавьте аккаунт в приложение.

Google Authenticator

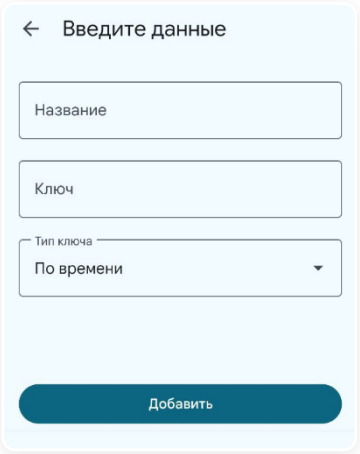
1. Запустите приложение и нажмите **Начать**.

2. Нажмите **Добавить код**:



3. Выберите опцию:

- **Сканировать QR-код** - наведите камеру и сканируйте код на сайте.
- **Ввести ключ настройки**:



- **Название** - укажите название аккаунта.
- **Ключ** - вставьте секретный ключ с сайта.
- **Тип ключа** - оставьте **По времени**.

4. Нажмите **Добавить**.

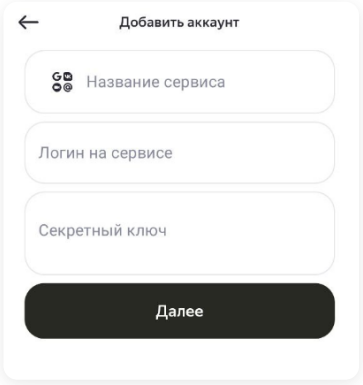
В приложении отобразится шестизначный код и таймер обратного отсчета (30 секунд). Код автоматически обновляется.

Яндекс ID

1. Запустите приложение и нажмите **Добавить аккаунт**.

2. Выберите опцию:

- **Сканировать QR** - наведите камеру и сканируйте код на сайте.
- **Добавить вручную**:



- **Название сервиса** - укажите название сервиса.
- **Логин на сервисе** - укажите логин на сервисе.
- **Секретный ключ** - укажите секретный ключ с сайта.

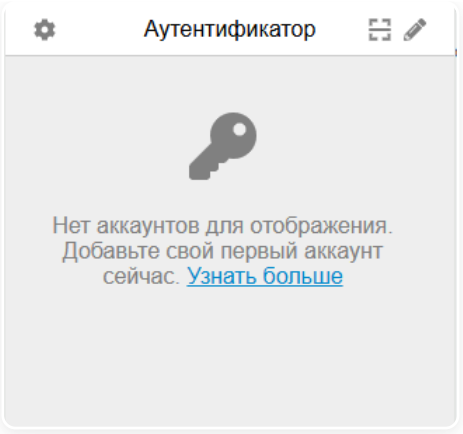
3. Нажмите **Далее**.

В приложении отобразится шестизначный код и таймер обратного отсчета (30 секунд). Код автоматически обновляется.

Расширение Аутентификатор

Для Chrome

1. Для сканирования QR-кода нажмите на иконку расширения в правом верхнем углу браузера, выберите установленное расширение, нажмите и выделите область с QR-кодом на сайте.



2. Для ручного ввода ключа нажмите , а затем - , из меню выберите **Ручной ввод** и укажите:

- Название сервиса.
- Секретный ключ с сайта.

Для Firefox

Процесс настройки аналогичен Chrome-расширению.

Технологические партнеры

> В статье представлена информация о продуктах других вендоров, совместимость с которыми была протестирована.

В таблице указаны продукты, которые могут интегрироваться в инфраструктуре с продуктами Ideco.

Продукт	Компания	Класс продукта
Alertix	ООО «ЭнДжиАр софтлаб»	SIEM-система
ALD Pro	ООО "РусБИТех-Астра"	Служба каталога для Linux
Astra Linux	ООО "РусБИТех-Астра"	Операционная система
DS Proxima	АО "НПП "Цифровые решения"	Аппаратный балансировщик нагрузки. Интеграция NGFW Novum и DS Integrity NG
Efros DefOps	ООО "Газинформсервис"	Многофункциональный комплекс по защите ИТ-инфраструктуры (сетевых и оконечных устройств, компонентов сред виртуализации), а также прикладного ПО: SCADA, RPA, СУБД, NAC, NA, VC, FA, CM
IVA MCU	ПАО "ИВА"	Платформа видеоконференцсвязи
IVA ONE	ПАО "ИВА"	Платформа бизнес-коммуникаций
JaCarta Management System 4LX (включает JaCarta Authentication Server и Aladdin 2FA)	АО "Аладдин Р.Д."	Корпоративная система централизованного управления для Linux
Kaspersky Anti-Spam	ЗАО "Лаборатория Касперского"	Антиспам
Kaspersky Anti Targeted Attack Platform (KATA Sandbox)	ЗАО "Лаборатория Касперского"	Сетевая песочница
Kaspersky Threat Intelligence	ЗАО "Лаборатория Касперского"	Сигнатуры
Microsoft Active Directory	Microsoft	Служба каталога для Windows
MIST Insight	ООО "МИСТ"	NSPM (Network Security Policy Management)
Multifactor	ООО "Мультифактор"	Система двухфакторной аутентификации и контроля доступа
Netopia	ООО "Нетопия"	Мониторинг и контроль сетевой безопасности
Securitm	ООО "СЕКЪЮРИТМ"	Система управления информационной безопасностью
SKY DNS	"СкайДНС"	Решение DNS Security и фильтрация контента. Интеграция NGFW Novum и SkyDNS
SMS Aero	ООО "СМС Аэро"	SMS-рассылка
UDV DATAPK Industrial Kit	ООО "СайберЛимфа"	Система обнаружения вторжений в промышленных сетях
UDV ITM	ООО "СайберЛимфа"	Единое решение для мониторинга на базе Zabbix. Подходит для мониторинга АСУ ТП, серверов, каналов связи и ИТ-услуг
VK Cloud	ООО "Цифровое Облако"	Платформа сетевого доступа к вычислительным ресурсам и различным облачным сервисам
Альт Домен	ООО "Базальт СПО"	Служба каталогов
Альт Рабочая станция	ООО "Базальт СПО"	Операционная система
Альт Сервер	ООО "Базальт СПО"	Серверный дистрибутив с широкой функциональностью
АльтерОС	ООО "Алми Партнер"	Сертифицированная российская операционная система на Linux последнего поколения
Антивирус Касперского	ЗАО "Лаборатория Касперского"	Антивирус
БИТ.Аутентификатор	ООО "Первый Бит"	Система двухфакторной аутентификации
MFASOFT	ООО «СИС разработка»	Система двухфакторной аутентификации
Indeed Access Manager	ООО «Индид»	Система двухфакторной аутентификации
Контур Staffcop Enterprise	ООО "АТОМ Безопасность"	Система расследования инцидентов внутренней информационной безопасности

КриптоПро NGate	ООО "КРИПТО-ПРО"	Универсальное высокопроизводительное средство криптографической защиты сетевого трафика (TLS- и VPN-сервер)
ОСОН "ОСнова"	АО "НППКТ"	Операционная система для рабочих станций и серверов
Ред АДМ	ООО "РЕД СОФТ"	Система централизованного управления ИТ-инфраструктурой
Ред Виртуализация	ООО "РЕД СОФТ"	Система управления виртуализацией серверов и рабочих станций
Ред ОС	ООО "РЕД СОФТ"	Операционная система
Рутокен ЭЦП 3.0	АО "Актив-софт"	Электронный идентификатор
СёрчИнформ КИБ	ООО "СёрчИнформ"	DLP-система

Источники данных

Классический контекст | Высокопроизводительный контекст

Ideco NGFW Novum может обращаться к адресам для получения данных:

Тип запроса	Адрес	Используемые порты
Отправка уведомлений в личный кабинет/телеграм-бот	api.ideco.ru	443 TCP-порт
Обновление баз Контент-фильтра	content-filter.v22.ideco.dev	443 TCP-порт
Отправка анонимной статистики	gatherstat.v22.ideco.dev	443 TCP-порт
Обновления баз GeoIP	ip-list.v22.ideco.dev	443 TCP-порт
Обмен информацией о лицензии	api.ideco.ru	443 TCP-порт
Отправка отчетов по почте	api.ideco.ru	443 TCP-порт
Обновления сигнатур IDS/IPS	suricata.v22.ideco.dev	443 TCP-порт
Обновления системы	api.ideco.ru	443 TCP-порт
Синхронизация времени	ntp.ideco.ru	123 UDP-порт
Получение сертификатов Let's Encrypt	acme-v02.api.letsencrypt.org	443 и 80 TCP-порты
Антивирус Касперского (обновление баз)	Серверы с официального сайта Лаборатории Касперского	443 и 80 TCP-порты
DNS security	193.58.251.10	853 TCP-порт

Часть запросов к указанным выше серверам может быть перенаправлена на `mcs-vm.ideco.ru`, `update.ideco.ru`, `storage.yandexcloud.net` (443 порт).

Для корректной работы всех модулей фильтрации Ideco NGFW Novum необходимо, чтобы доступ к вышеуказанным ресурсам был разрешен настройками фильтрации.

Учитывайте при обновлении, что `v22` в домене соответствует версии Ideco NGFW Novum. Эту часть можно заменить символом `*` при настройке фильтрации. Например: `license.*.ideco.dev`.

Таблица портов Ideco NGFW Novum, доступных из локальной и внешних сетей

- Протокол ICMP разрешен на внешних и локальных интерфейсах.
- TCP-порт 8443, предназначенный для веб-интерфейса, находится в состоянии **Listen** постоянно. Порт открыт в локальную сеть сразу после установки Ideco NGFW Novum и настройки интерфейсов.
- TCP-порты 80 и 443, открытые во внешнюю и локальную сеть сразу после установки Ideco NGFW Novum и настройки интерфейсов, находятся в состоянии **Listen** постоянно.

Доступные из внешней сети

Включенная служба	Порты
Доступ к веб-интерфейсу из внешних сетей	8443 TCP
Доступ по SSH из внешних сетей	22 TCP
VPN IPSec	500, 4500 UDP
VPN L2TP	500, 4500 UDP
VPN PPTP	1723 TCP
VPN SSTP	1443 TCP (порт настраивается пользователем)
Ideco Client	443 TCP (по умолчанию), 14765 TCP (резервный), 3051 UDP (для Wireguard)
SMTP(S)	25, 587 TCP
Веб-почта	443 TCP
Обратный прокси	443, 80 TCP
POP3(S)	110, 995 TCP
IMAP(S)	143, 993 TCP
BGP	179 TCP

Доступные из локальной сети

Включенная служба	Порты
Доступ к веб-интерфейсу из локальной сети	8443 TCP
Прокси	8080 TCP (порт настраивается пользователем)
DNS	53 TCP, UDP
DHCP-сервер	67, 68 UDP
NTP-сервер	123 UDP
Тест скорости	18080 TCP
OSPF	-
Zabbix-сервер	10050, 10051 TCP
Let's Encrypt	80 TCP
Веб-аутентификация	443 TCP
Двухфакторная аутентификация	443 TCP
Ideco Client	443 TCP (по умолчанию), 14765 TCP (резервный)
Обратный прокси (Веб-почта, Веб-интерфейс, Личный кабинет/Портал SSL VPN)	443 TCP

Как проверить, открыт ли порт

Чтобы проверить, открыт ли порт, воспользуйтесь инструментом nmap, выполнив команду:

```
nmap -v 192.168.0.150
```

- 192.168.0.150 - адрес локального или внешнего интерфейса Ideco NGFW Novum.

Рекомендации при первоначальной настройке

Рекомендуемая последовательность шагов для минимальной настройки Ideco NGFW Novum:

1. Зарегистрируйтесь в MY.IDECO. Подробнее в статье О личном кабинете MY.IDECO.

2. Скачайте загрузочный образ продукта. Дистрибутивы также доступны в личном кабинете MY.IDECO.

3. Определитесь с устройством, на которое собираетесь устанавливать Ideco NGFW Novum, и выполните предварительные действия. Ideco NGFW Novum можно устанавливать как на виртуальную машину, так и на физический сервер.

4. Установите Ideco NGFW Novum на устройство, создайте учетную запись администратора. Для этого воспользуйтесь статьей Установка.

5. Выполните первоначальную настройку Ideco NGFW Novum. Воспользуйтесь статьей Первоначальная настройка.

6. Зарегистрируйте сервер в MY.IDECO и получите лицензию.

7. Создайте учетные записи пользователей и настройте авторизацию, чтобы получить доступ в интернет через Ideco NGFW Novum. Более подробная информация представлена в статье Получение доступа в интернет.

Подготовка платформы к установке

Установка в гипервизоре

Перейти >

Создание загрузочного USB-накопителя

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка гипервизора

Если при установке Ideco NGFW Novum появилось окно с текстом **Installation in BIOS mode is not supported**, необходимо проверить включение режима UEFI в настройках.

Методы обеспечения отказоустойчивости:

- Встроенные технологии гипервизора:
  - High Availability (HA) - автоматический перезапуск виртуальных машин на другом узле при сбое.
  - Fault Tolerance (FT) - синхронное дублирование виртуальной машины для нулевого простоя.
- Кластеризация.

Не рекомендуется применять два метода одновременно.

VMware ESXi 6.7

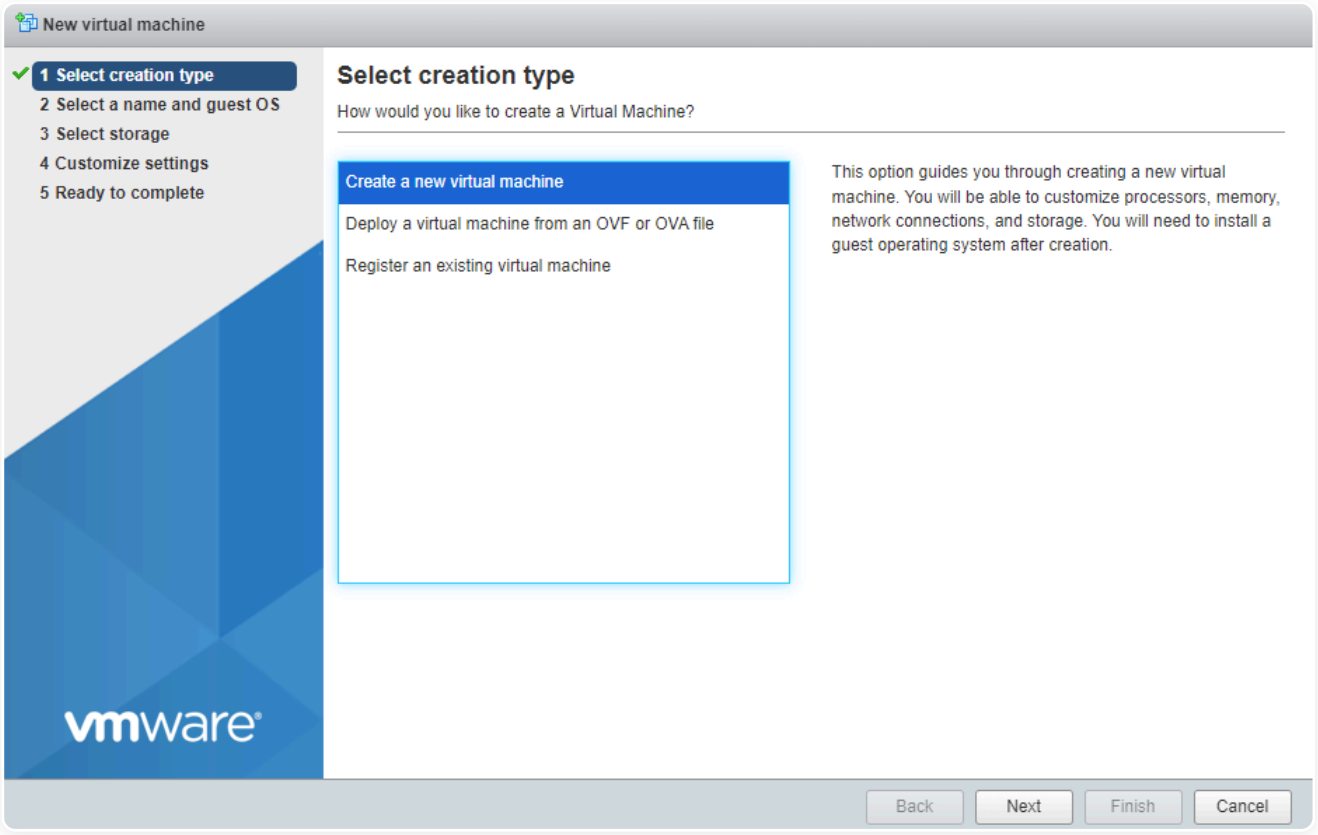
При установке Ideco NGFW Novum на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

Настройка

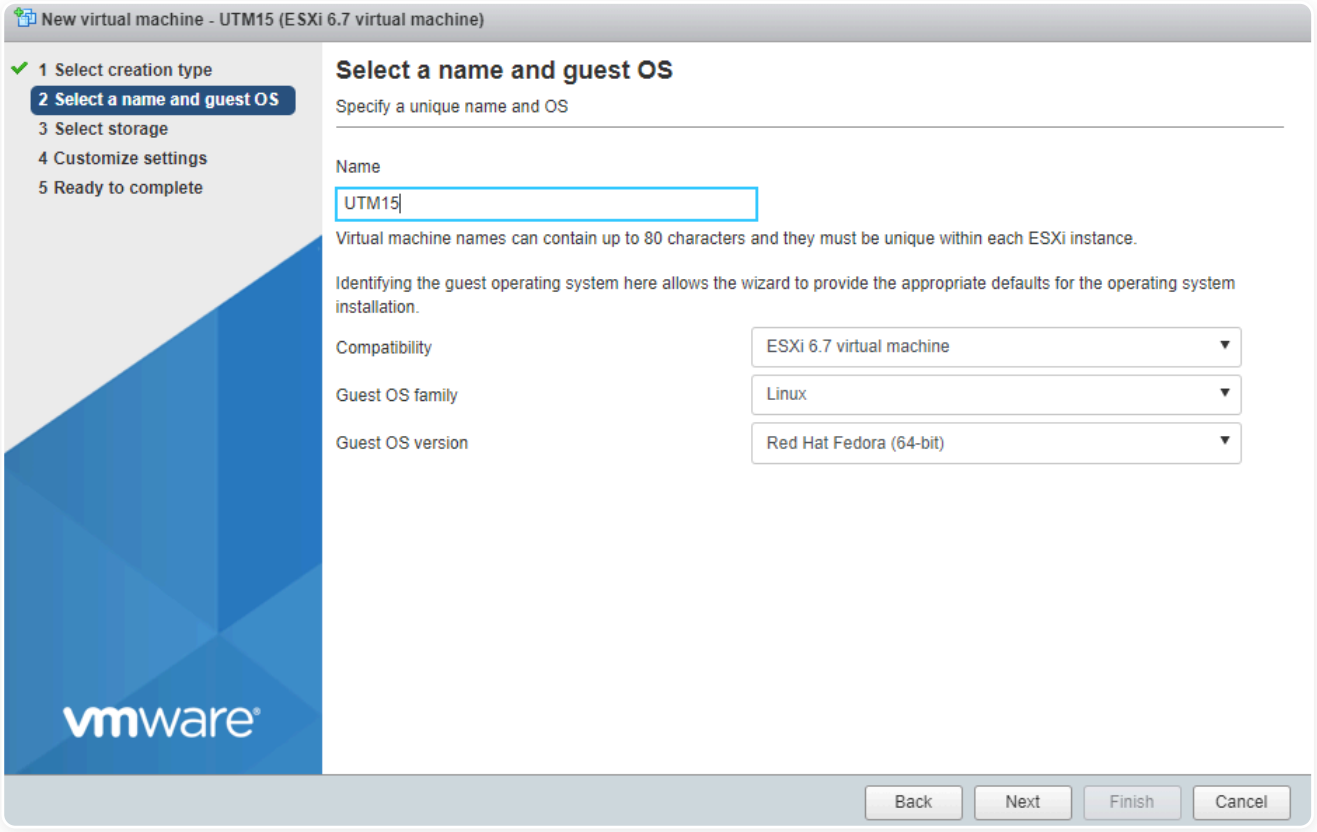
Перед установкой Ideco NGFW Novum:

- Загрузите образ, скачанный в MY.IDECO, на VMware ESXi. При настройке виртуальной машины потребуется указать путь к образу.
- Увеличьте размер видеопамяти для виртуальной машины до 16 МБ.
- Используйте виртуальные сетевые адаптеры **vmxnet3**, **e1000e**.

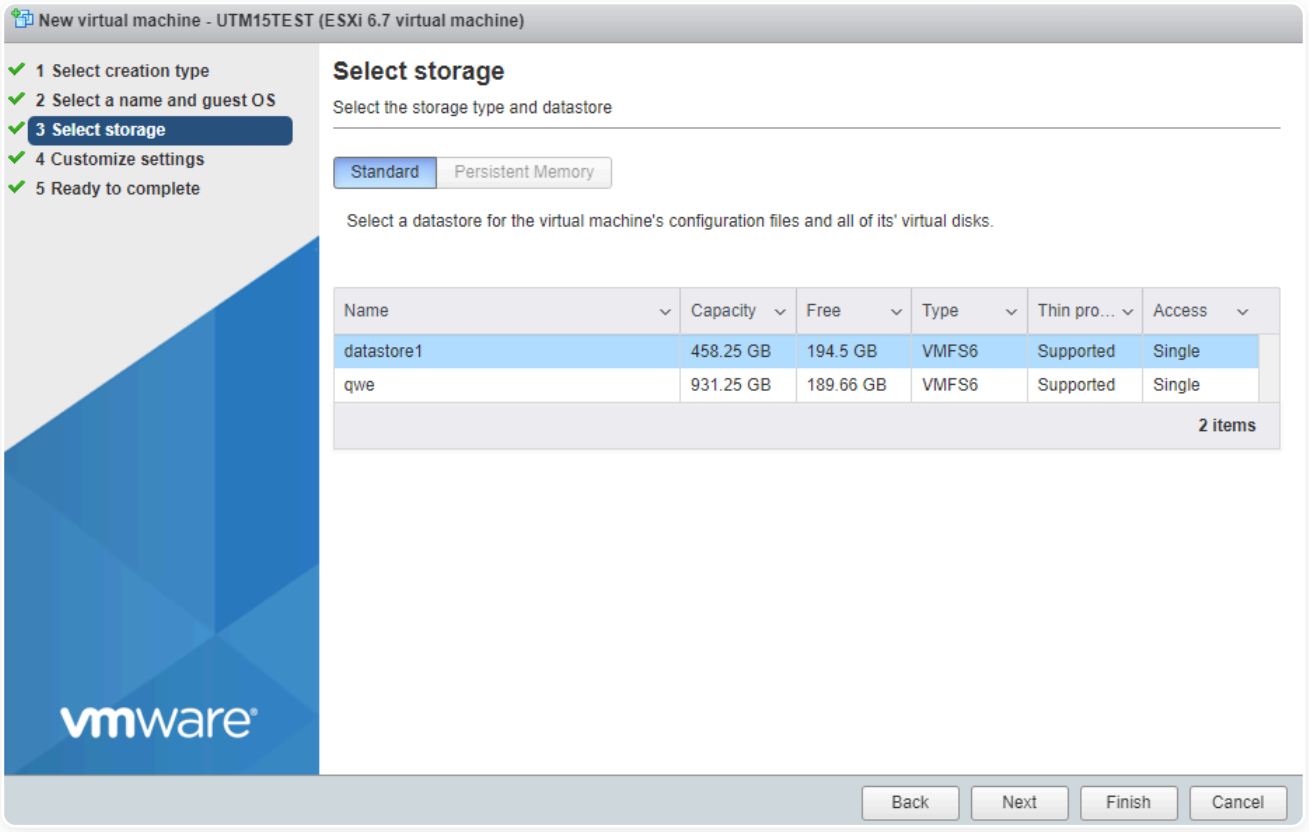
1. Создайте виртуальную машину:



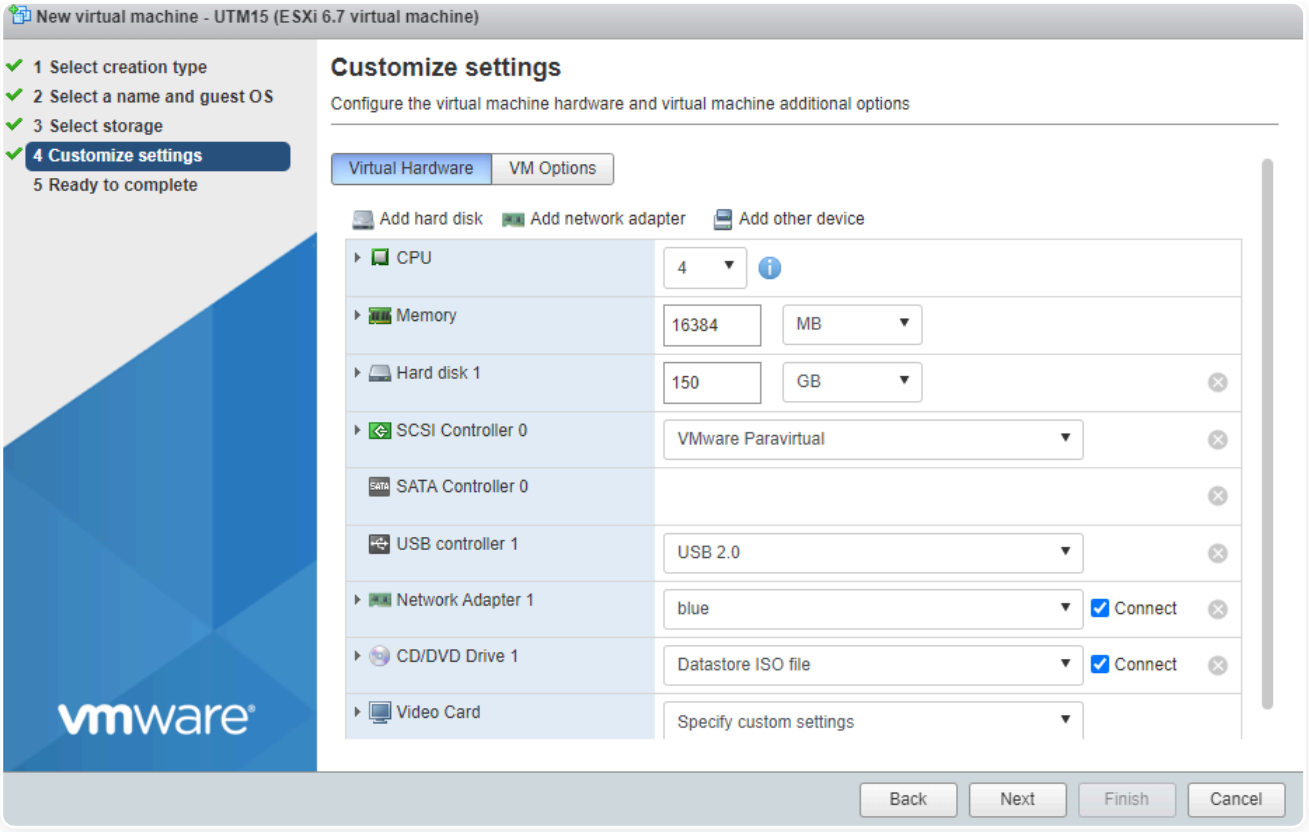
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



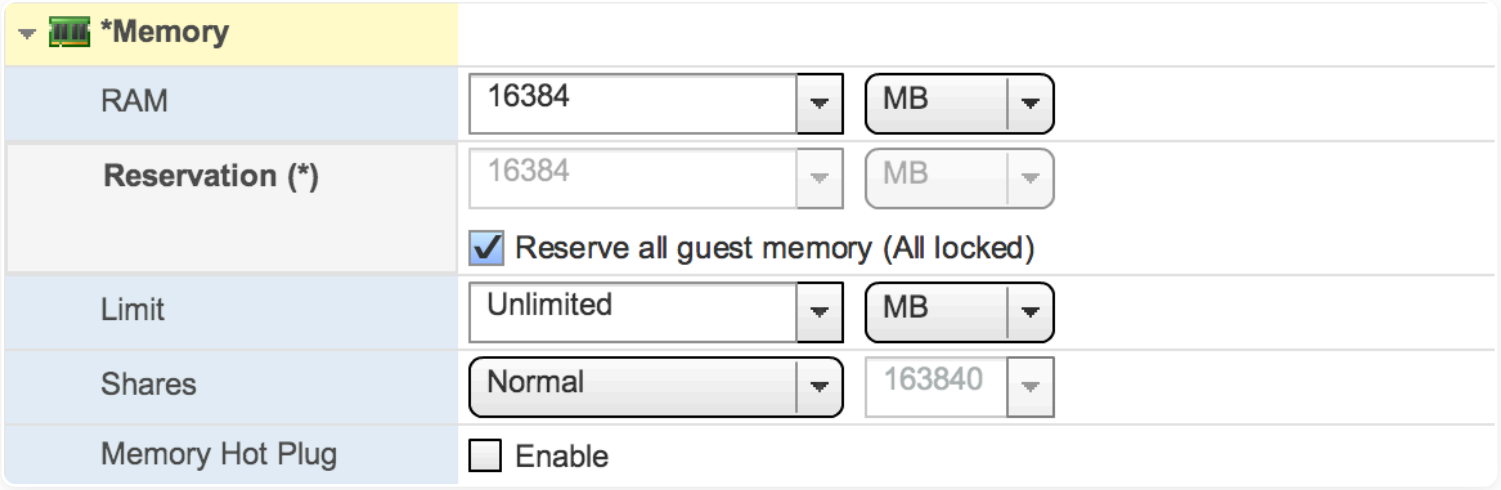
3. Выберите хранилище для виртуальной машины:



4. Установите размер оперативной памяти **16 ГБ**, количество ядер процессора **4** и размер диска **150 ГБ**. После выберите в поле **CD/DVD Drive** Datastore ISO file и укажите путь к загрузочному образу:

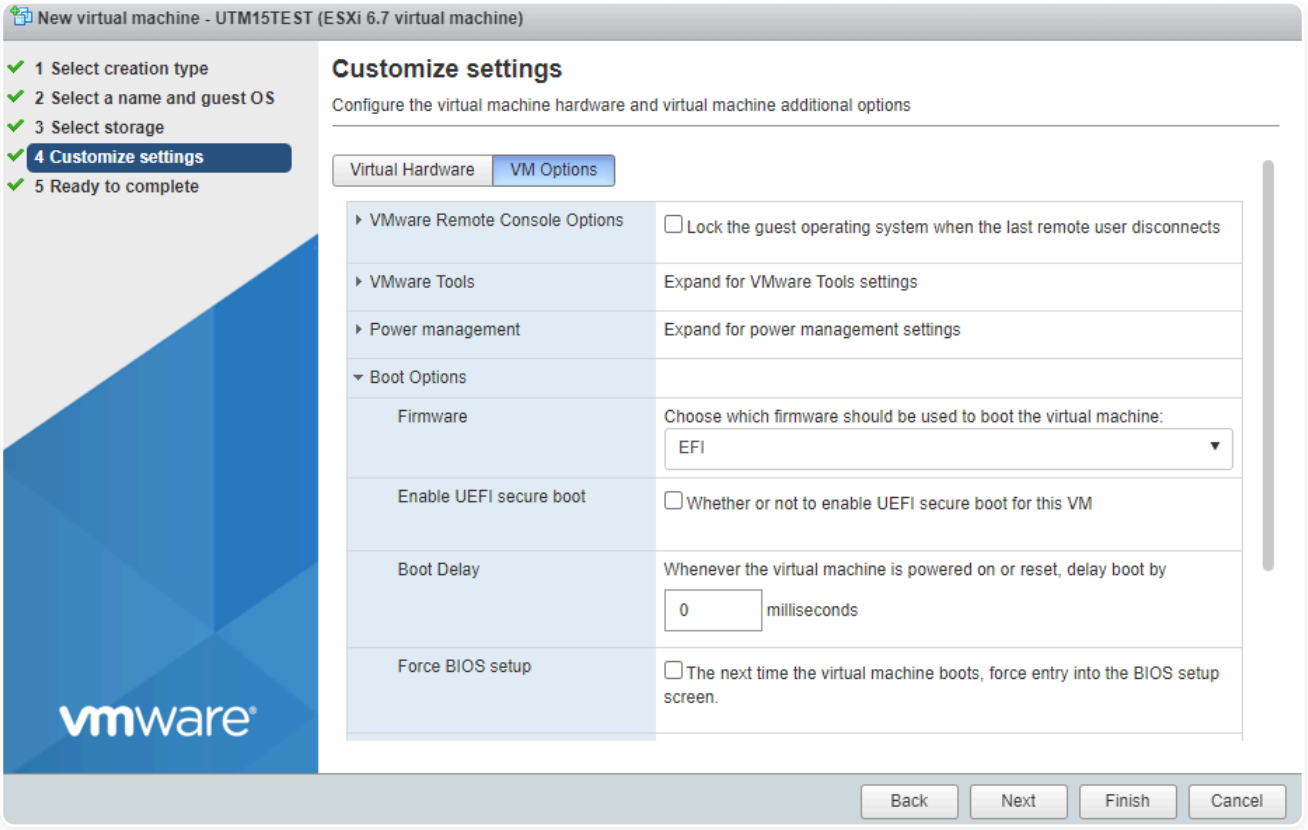


5. Разверните раздел **Memory** и включите опцию **Reserve all guest memory (All locked)**:

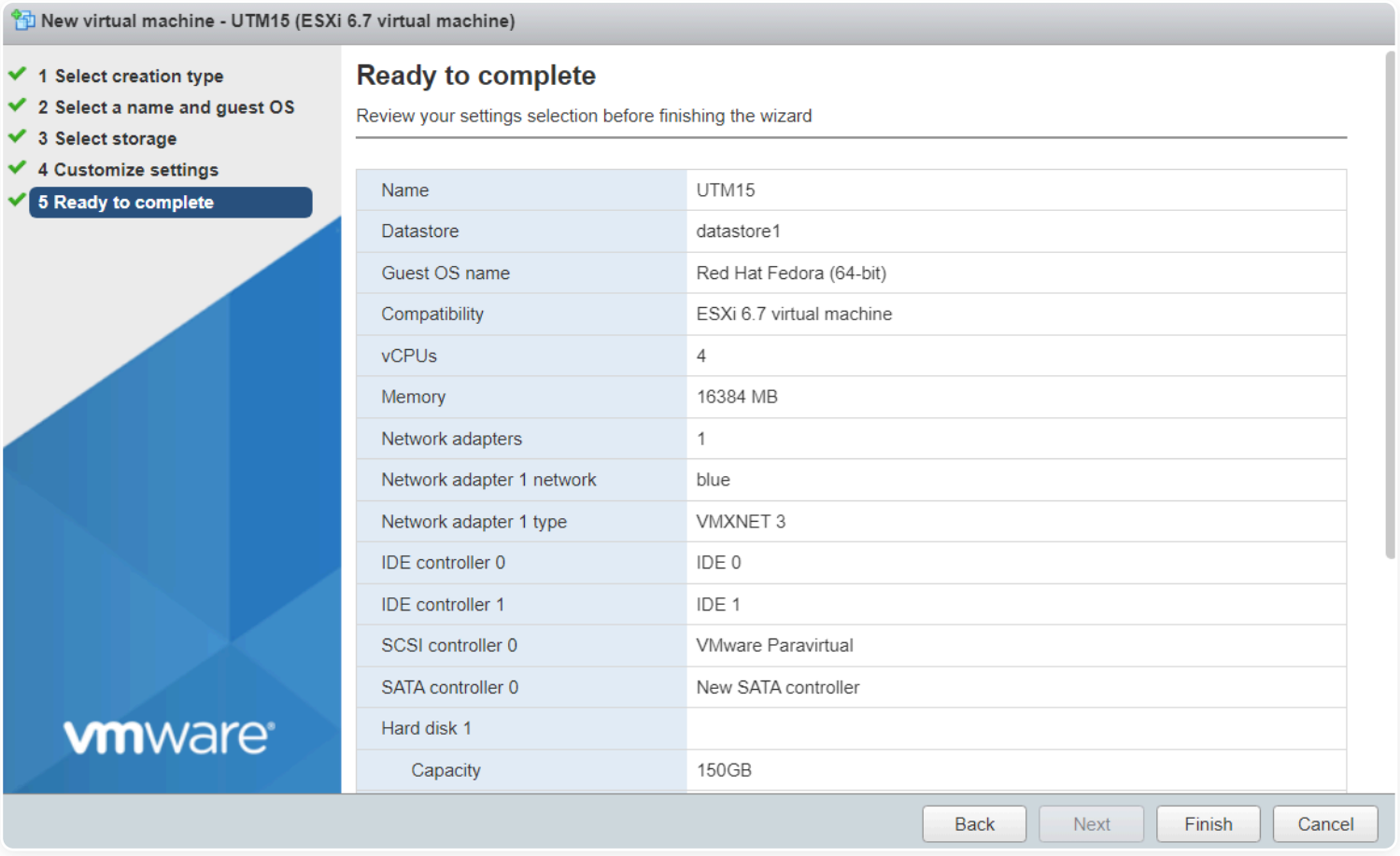


- **Reserve all guest memory (All locked)** - если опция выключена, гипервизор динамически распределяет доступную оперативную память между всеми виртуальными машинами.

6. Включите **UEFI** на вкладке **VM Options**, выбрав в поле **Firmware** EFI:



7. Нажмите **Finish**:



Настройка кластеризации

Для корректной работы кластерной сети требуются дополнительные настройки, так как гостевая ОС программно назначает порту синхронизации MAC-адрес, отличный от аппаратного, заданного в настройках виртуальной машины.

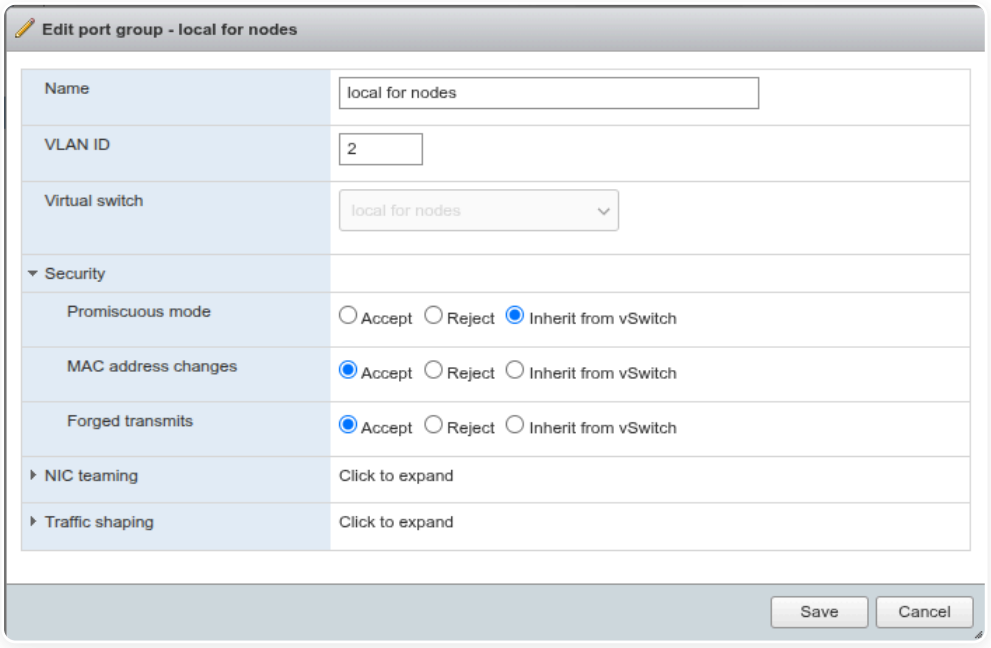
Выполните действия:

1. В интерфейсе VMware ESXi перейдите в **Navigator** → **Networking** → **Port groups**.

2. Выберите группу портов, используемую для сети синхронизации нод, и нажмите **Edit settings**.

3. Раскройте раздел **Security**.

4. Установите значение **Accept** для двух параметров:



- **MAC address changes** - разрешает прием трафика на MAC, отличающийся от заданного в настройках ВМ.
- **Forged transmits** - разрешает отправку кадров с MAC-адресом источника, отличающимся от заданного в настройках ВМ.

5. Нажмите **Save**.

6. Перезапустите NGFW Novum.

> Для синхронизации нод кластера NGFW Novum в виртуальных средах не рекомендуется использовать LACP. Если требуется отказоустойчивость канала между ESXi-хостами, настройте LACP на стороне самих хостов и физических коммутаторов - агрегация будет работать прозрачно для NGFW Novum.

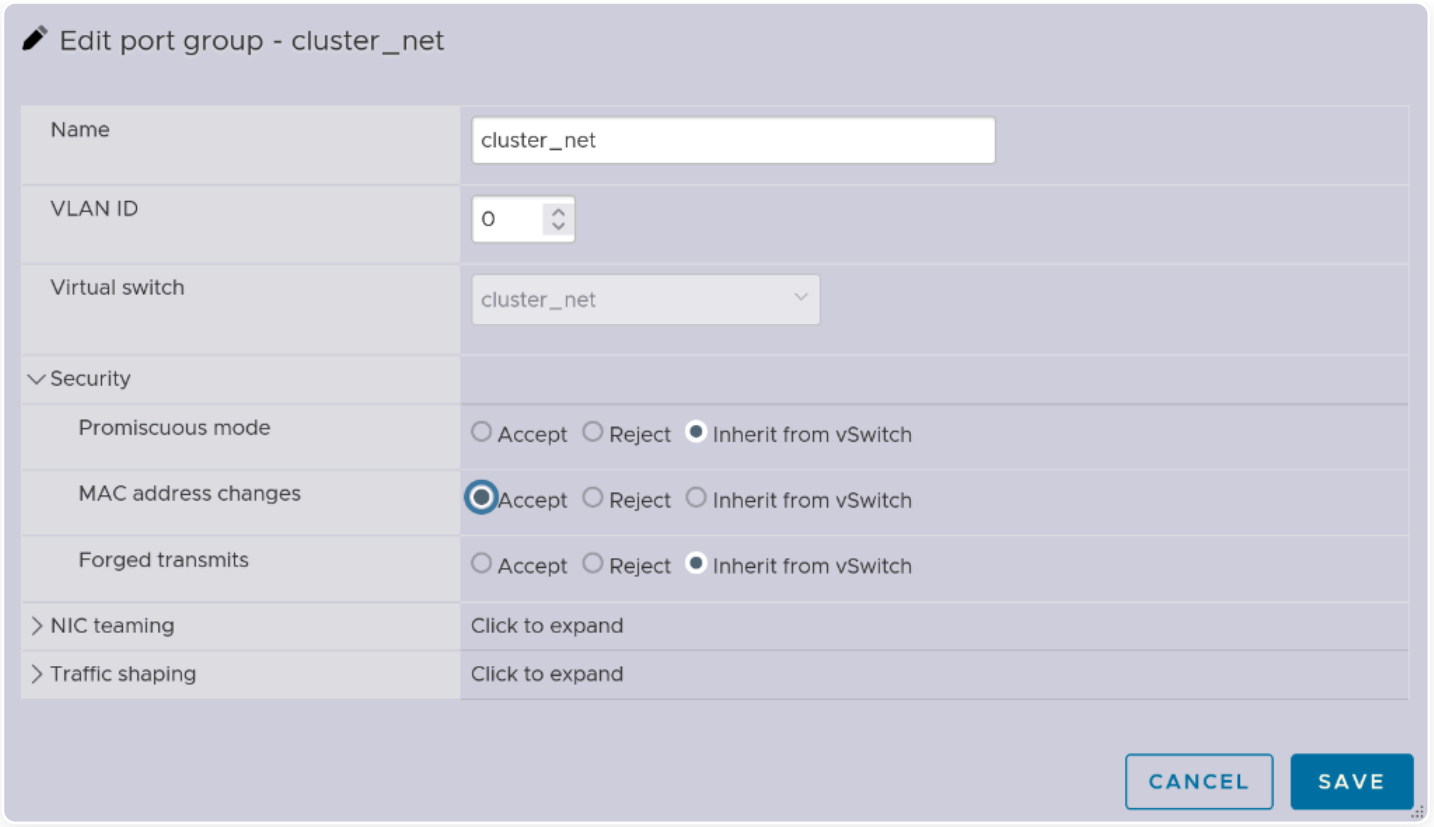
Настройка LACP-интерфейсов

При использовании LACP-интерфейсов требуется настройка группы портов. Для этого:

1. Перейдите в **Networking** → **Port groups**.

2. Выберите группу портов, используемую для LACP.

3. Перейдите в **Edit settings** → **Security** → **MAC address changes** и поменяйте значение на **Accept**:



4. Нажмите **Save**.

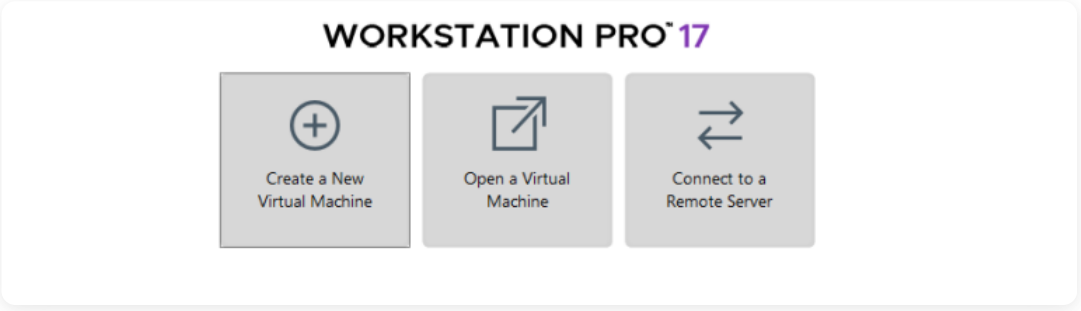
VMware Workstation 17.0

Настройка

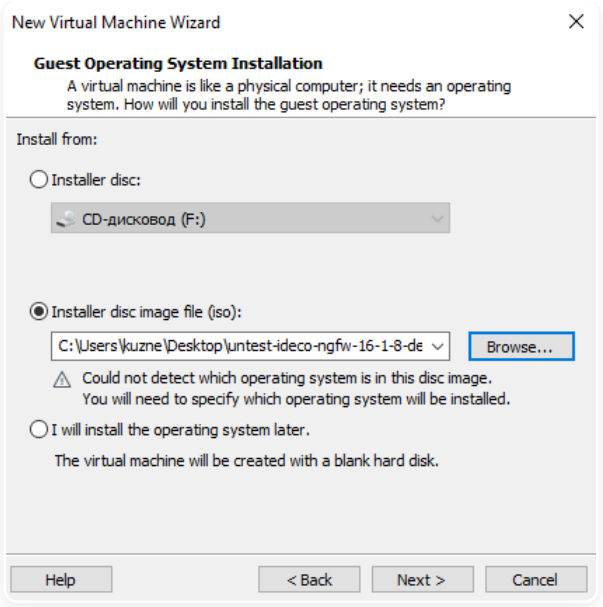
Перед установкой Ideco NGFW Novum:

- Увеличьте размер видеопамяти для виртуальной машины до 16 МБ.
- Используйте виртуальные сетевые адаптеры **vmxnet3**, **e1000e**.

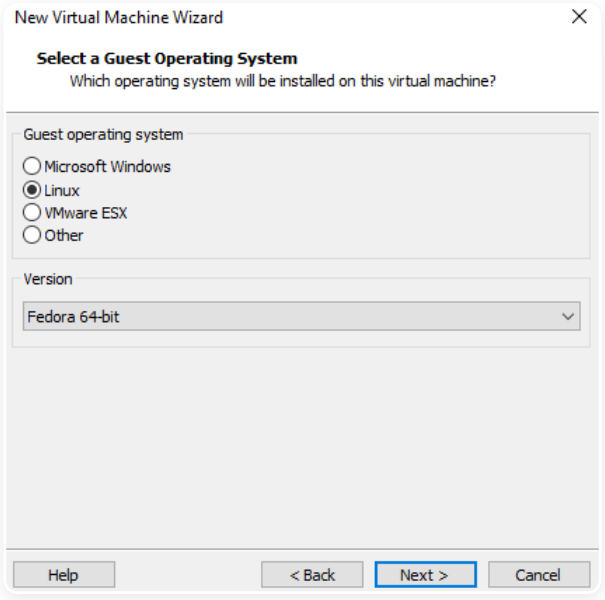
1. Создайте виртуальную машину, нажав **Create a New Virtual Machine**:



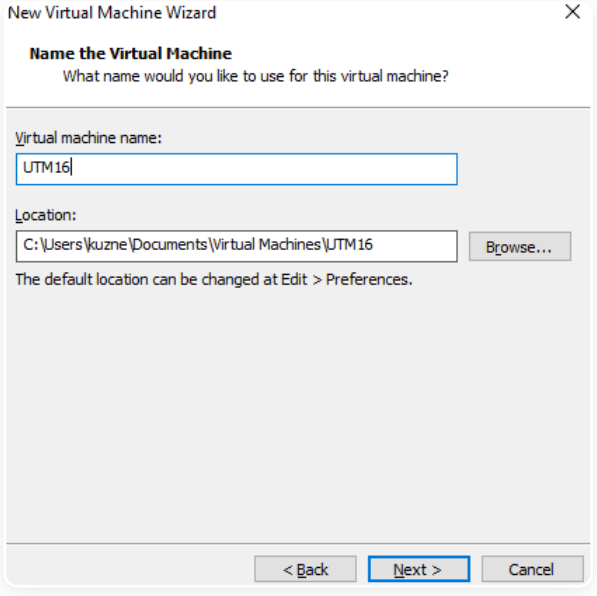
2. Укажите загрузочный ISO-образ:



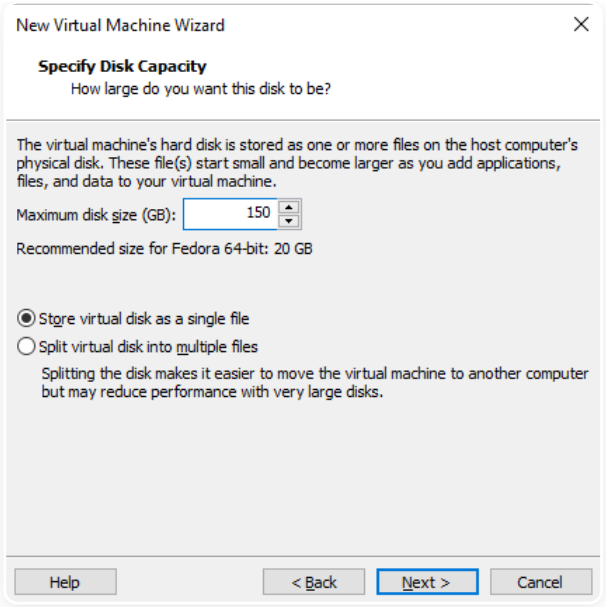
3. Выберите гостевую операционную систему **Linux** и в раскрывающемся списке укажите тип **Fedora 64-bit**:



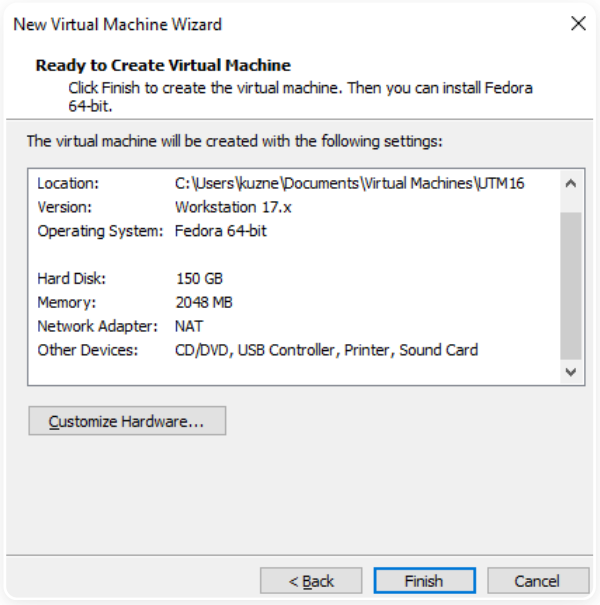
4. Укажите имя виртуальной машины и директорию для создания виртуального диска:



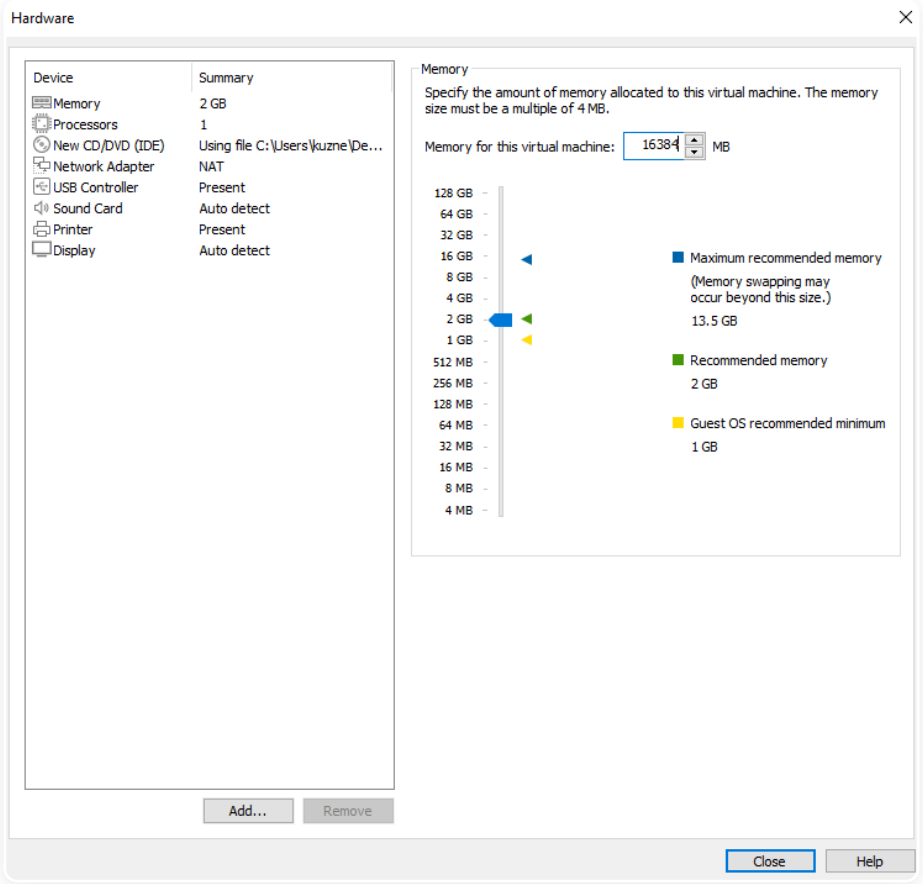
5. Укажите размер виртуального жесткого диска **150 ГБ**:



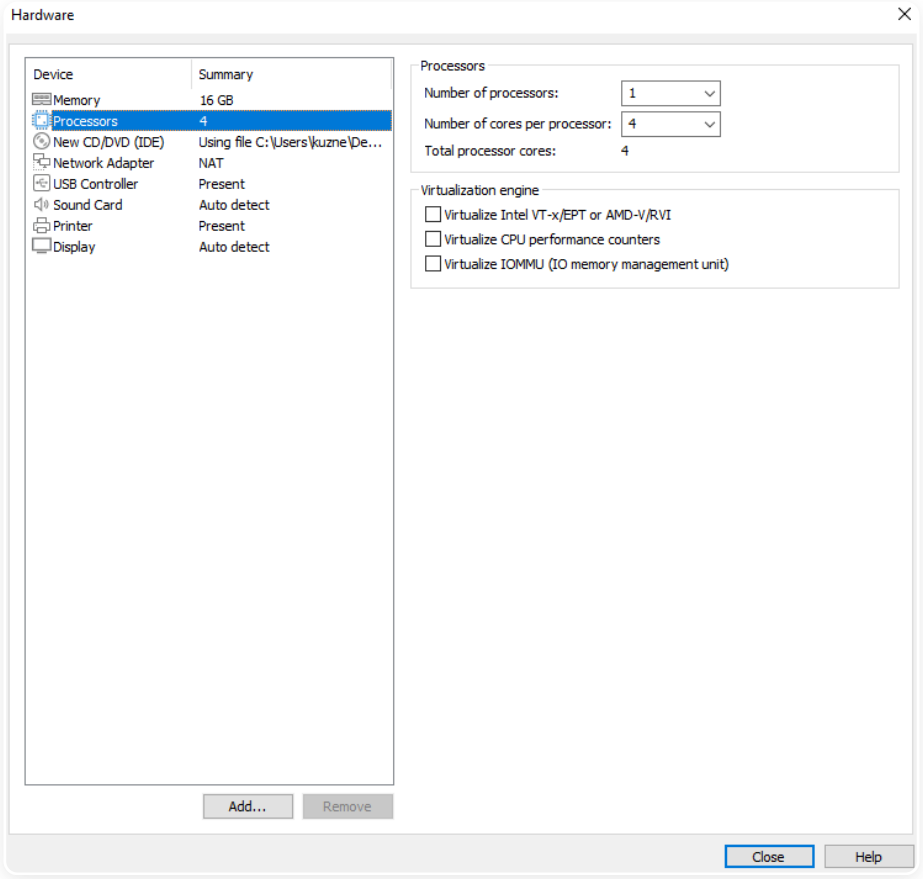
6. Выберите **Customize Hardware** для изменения настроек виртуальной машины:



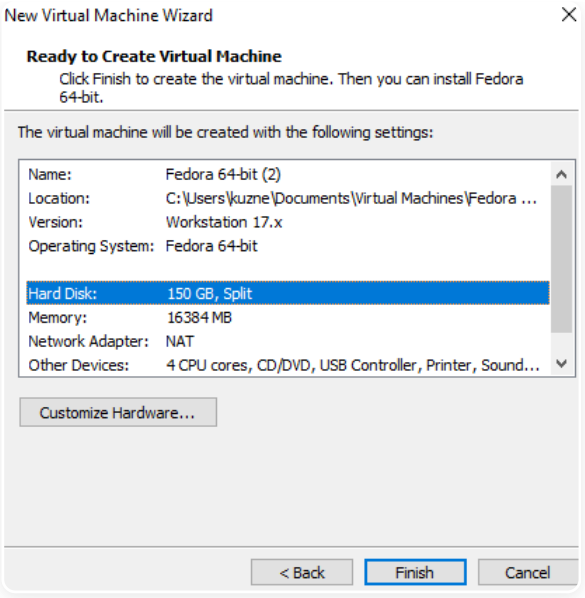
7. Укажите размер виртуальной оперативной памяти **16384 МБ**:



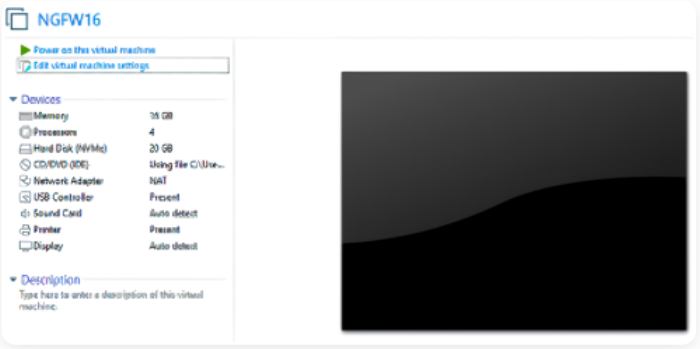
8. Укажите количество ядер процессора, равное 4:



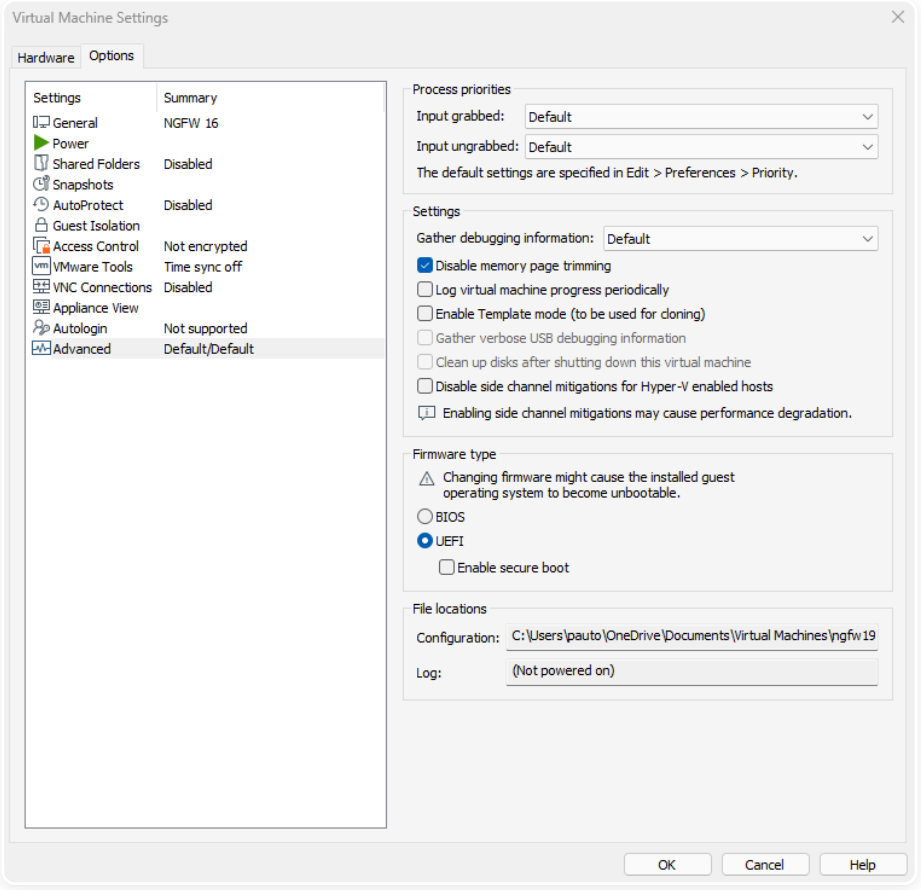
9. Выйдите из меню и нажмите **Finish** для окончания настройки:



10. Откройте окно виртуальной машины и нажмите **Edit virtual machine settings**:



11. Перейдите в **Options** → **Advanced** и активируйте опцию **Disable memory page trimming**. Установите для параметра **Firmware Type** значение **UEFI**:



- **Disable memory page trimming** - если опция выключена, гипервизор динамически распределяет доступную оперативную память между всеми виртуальными машинами.

12. Нажмите **OK** для завершения настройки виртуальной машины.

VirtualBox 7.0.12

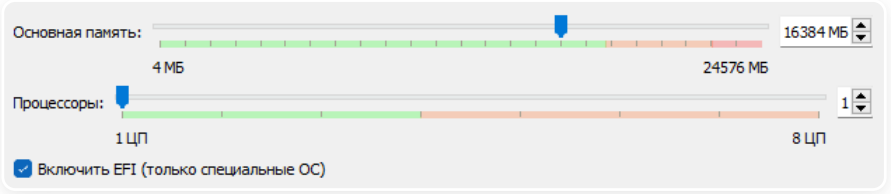
Настройка

> По умолчанию при создании виртуальной машины создается одна сетевая карта с типом подключения **NAT**.

1. Укажите **Имя** виртуальной машины (ВМ), выберите директорию для ВМ и установите путь до загрузочного образа NGFW Novum. Остальные параметры установите как на скриншоте:



2. Установите размер оперативной памяти ВМ (**16 ГБ**), количество ядер процессора **4** и нажмите **Включить EFI**:



3. Создайте виртуальный жесткий диск под ВМ (Объем не меньше **150 ГБ**):

4. Нажмите **Готово**.

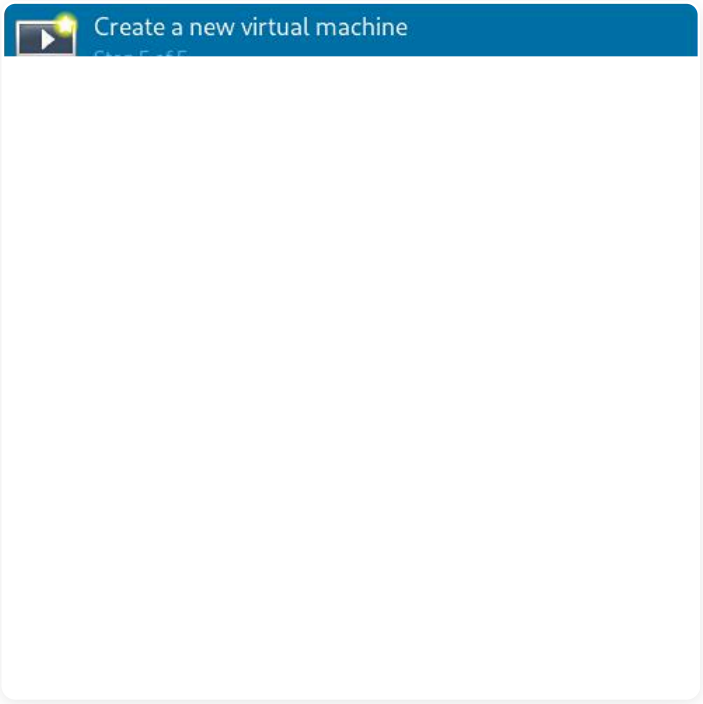
KVM

Настройка

> Минимальные требования к виртуальной машине описаны в статье.

1. При установке Ideco NGFW Novum выберите тип операционной системы - **Fedora**.

2. Включите опцию **Проверить конфигурацию перед установкой** и нажмите кнопку **Готово** на пятом шаге (virtm-manager) установки:



3. Измените интерфейс на **virtio** для дисков и сетевых карт. Изменить тип диска после создания ВМ нельзя.

4. Выберите режим кеширования. Если диски имеют формат qcow2 или raw, используйте **writeback**. Если используется другой формат дисков, проконсультируйтесь с системным администратором или с Технической поддержкой.

5. В появившемся окне на вкладке **Обзор** в поле **Firmware** выберите пункт **UEFI x86_64:/usr/share/OVMF/OVMF_CODE.fd**. Выбор этого пункта включит **UEFI** и выключит опцию **Secure Boot**:

Если пункта **UEFI x86_64:/usr/share/OVMF/OVMF_CODE.fd** нет в списке, доустановите пакет ovmf. В Ubuntu пакет ovmf устанавливается командой `sudo apt install ovmf`.

6. Перейдите в раздел **Memory** → **XML** и измените тег `<memballoon model='virtio'/>` на `<memballoon model='none'/>`, чтобы отключить **Memory Ballooning** и повысить производительность. При включенной опции гипервизор динамически распределяет доступную оперативную память между виртуальными машинами, из-за чего гостевая ОС может видеть больший объем памяти, чем фактически выделено.

Proxmox

Настройка

1. Нажмите **Создать ВМ**, включите опцию **Дополнительно** и введите имя машины:

2. В разделе **ОС** выберите хранилище и заполните поля:

- **ISO-образ** - образ с нужной версией NGFW Novum.
- **Гостевая ОС**:
  - **Тип** - Linux.
  - **Версия** - 6.x - 2.6 Kernel.

3. В разделе **Система** заполните поля:

- **Машина** - q35.
- **BIOS** - OVMF.
- **Хранилище EFI** - хранилище для UEFI-диска.
- **Агент QEMU** - включите опцию, чтобы операционная система могла передавать гипервизору информацию о своих внутренних состояниях.
- **Предварительная загрузка ключей** - отключите опцию.

4. В разделе **Диски** укажите нужный размер диска (не меньше 150 ГБ) и выберите хранилище для NGFW Novum:

- **Шина/Устройство** - VirtIO Block.
- **Отклонить** - включите опцию, если нужно сэкономить дисковое пространство. Она позволяет автоматически очищать освобожденные блоки на диске.

Проверьте свободное место на диске.

5. В разделе **Процессор** укажите количество сокетов и ядер (от четырех ядер) и выберите тип, который поддерживает SSE 4.2:

6. В разделе **Память** укажите объем оперативной памяти (не менее 16 ГБ):

- **Раздувание памяти** - отключите опцию для обеспечения максимальной производительности. При включенной опции гипервизор динамически распределяет доступную оперативную память между виртуальными машинами, из-за чего гостевая ОС может видеть больший объем памяти, чем фактически выделено.

7. В разделе **Сеть** в поле **Сетевой мост** выберите сетевой мост для локального интерфейса:

Рекомендуем отключить опцию **Сетевой экран**, чтобы облегчить настройку и отладку межсетевого экрана в Ideco NGFW Novum и избежать конфликтов обработки трафика.

8. В разделе **Подтверждение** проверьте заданные настройки и нажмите **Готово**:

Рекомендуем отключить опцию **Запуск после создания**, так как потребуется добавить еще одно сетевое устройство.

9. Для работы Ideco NGFW Novum также понадобится мост на сетевой интерфейс, чтобы получить доступ в интернет. Нажмите на созданную виртуальную машину, выберите **Оборудование** → **Добавить** → **Сетевое устройство** и добавьте мост, соответствующий выбранному ранее коммутатору:

Microsoft Hyper-V

Настройка

Сетевые адаптеры Hyper-V не поддерживаются в **Высокопроизводительном контексте**. Исправление планируется в будущих версиях.

Рекомендуем пробрасывать в виртуальную машину физическую сетевую карту на уровне PCI либо использовать эмуляцию сетевых адаптеров Intel (совместимость за счет снижения производительности).

- Поддерживается только второе поколение виртуальных машин под Windows Server 2012 R2 или выше.
- Отключите опцию **Secure Boot (Безопасная загрузка)**.
- Отключите опцию **Dynamic memory (Динамическая память)**.
- Используйте **Network Adapter (Сетевой адаптер)**.

Минимальные требования к виртуальной машине описаны в статье.

Шаги по установке Ideco NGFW Novum после создания загрузочного USB-накопителя можно прочитать в статье Установка.

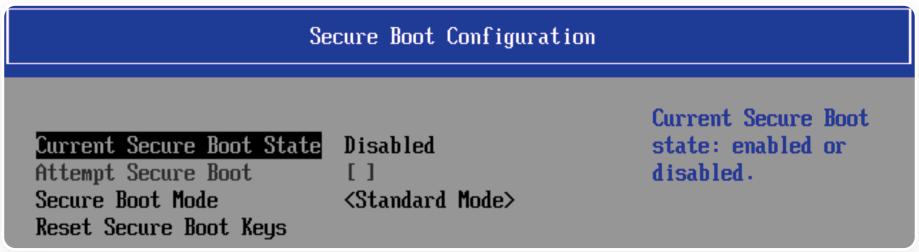
Для корректной работы кластерной сети, а также при использовании LACP-интерфейсов требуется дополнительная настройка на обеих нодах:

1. Перейдите в **Hardware** → **Network Adapter** → **Advanced Features** → **MAC address**.

2. Включите опцию **Enable MAC address spoofing**:

Включение режима совместимости процессора (Processor compatibility) может замедлить работу модуля **Предотвращение вторжений**:

При первом запуске в **BIOS** проверьте, что **Current Secure Boot State** в состоянии **Disabled**:



Полезные ссылки

- **Настройка LACP на Hyper-V**

Создание загрузочного USB-накопителя

При записи ISO-образа вся информация с USB-накопителя будет удалена.

Windows

С помощью программы Rufus

1. Проверьте целостность образа в PowerShell. Хеш-сумма должна совпадать с той, что указана в MY.IDECO → NGFW → Скачать:

```
((Get-FileHash <путь к загрузочному образу> -Algorithm SHA256).hash) -eq "<хеш-сумма>"
```

2. Скачайте программу Rufus и запустите скачанный файл.

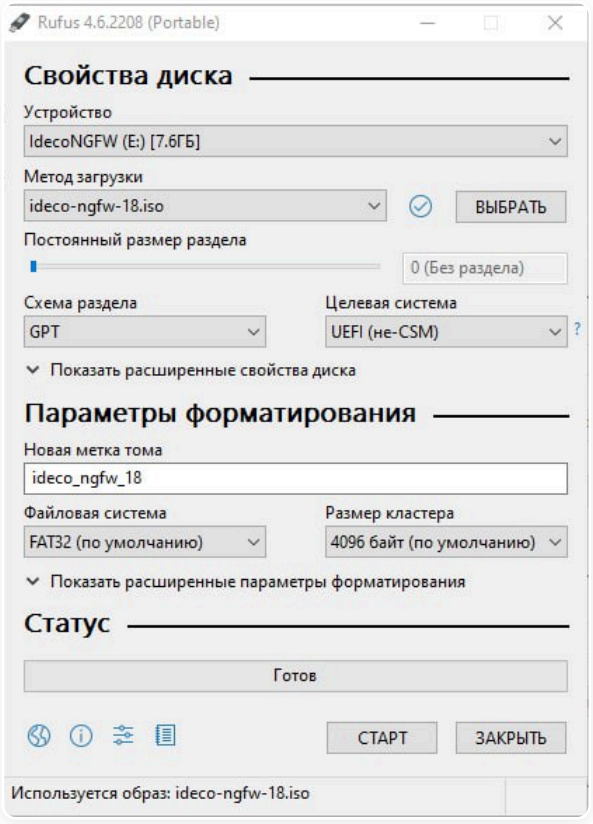
3. Выберите нужный USB-накопитель в пункте **Устройство**.

4. Выберите метод загрузки **Диск или ISO-образ**.

5. Нажмите на кнопку **Выбрать** и откройте скачанный образ Ideco NGFW Novum.

6. Нажмите **Старт** и в появившемся окне выберите пункт **Запись в режиме DD-образ**.

7. В диалоговом окне подтвердите запись:



С помощью программы Win32diskimager

1. Проверьте целостность образа в PowerShell. Хеш-сумма должна совпадать с той, что указана в MY.IDECO → NGFW → Скачать:

```
((Get-FileHash <путь к загрузочному образу> -Algorithm SHA256).hash) -eq "<хеш-сумма>"
```

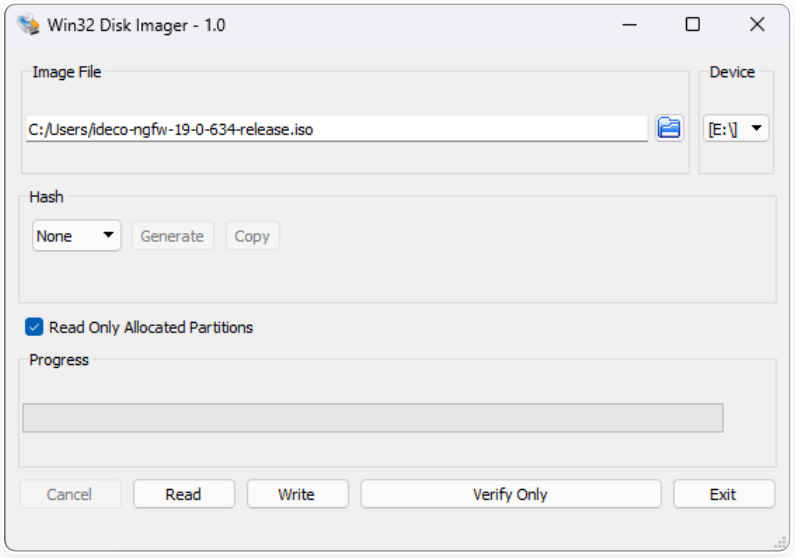
2. Установите программу Win32diskimager и запустите.

3. Нажмите на значок синей папки и выберите ISO-файл, который хотите записать.

По умолчанию все отображаемые файлы в проводнике Windows имеют формат `.img`. Для записи ISO-файла выберите опцию отображения всех файлов в правом нижнем углу.

4. Выберите нужный USB-накопитель рядом с файлом образа.

5. Нажмите **Write** и в появившемся окне подтвердите запись:



Linux

Для создания загрузочного USB-накопителя можно использовать не только терминал, но и программу gnome-disks.

Создание загрузочного накопителя через терминал

1. Проверьте целостность образа. Хеш-сумма должна совпадать с той, что указана в MY.IDECO → NGFW → Скачать:

```
echo "<хеш-сумма>  <путь к загрузочному образу>" | sha256sum -c
```

Пример:

```
echo "bc35a46507908c82ad3b8b75f4bb4f71f21f6d8012ad486aabbbb9a487108400 ideco-ngfw-21-4-26-release.iso" | sha256sum -c
```

2. Найдите USB-носитель в системе:

```
lsblk --nodeps  -o name,size,fstype,tran,model,mountpoint /dev/sd*
```

Вывод:

```
NAME  SIZE FSTYPE TRAN MODEL        MOUNTPOINT
sdx   7,5G        usb  USB_DISK_3.0
sdx1  7,5G vfat                     /run/media/ideco/D661-82E2
```

3. Размонтируйте файловую систему:

```
sudo umount <точка монтирования>
```

Пример:

```
sudo umount /run/media/ideco/D661-82E2
```

4. Запишите образ на носитель:

```
sudo dd if=<путь к загрузочному образу> of=<имя устройства> bs=1M oflag=direct status=progress conv=fdatasync
```

Пример:

```
sudo dd if=/home/ideco/ideco-ngfw-21-4-26-release.iso of=/dev/sdx bs=1M oflag=direct status=progress conv=fdatasync
```

5. Подготовьте носитель к извлечению:

```
sudo eject <имя устройства>
```

Пример:

```
sudo eject /dev/sdx
```

Шаги по установке Ideco NGFW Novum после создания загрузочного USB-накопителя можно прочитать в статье Установка.

Установка

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE



Процесс установки

При установке Ideco NGFW Novum с загрузочного USB-диска выберите загрузку с USB-диска в настройках UEFI сервера.

Если при установке Ideco NGFW Novum появилась ошибка **Требуется не менее 16 ГБ оперативной памяти** и при этом указан рекомендуемый размер оперативной памяти, необходимо уменьшить размер ресурсов, выделенных под видеопамять.

Для установки Ideco NGFW Novum выполните действия:

1. Перейдите к установке, нажав **Install Ideco NGFW Novum**:

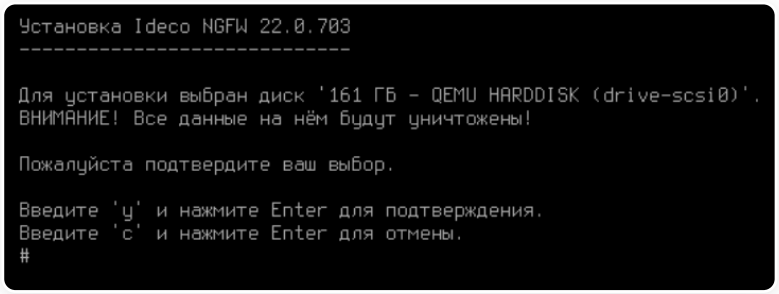


При установке или загрузке сервера Ideco NGFW Novum не рекомендуем нажимать на клавиатуре:

- `-` - нажатие кнопки уменьшает количество секунд в тайм-ауте и может привести к отключению таймера.
- `+` - нажатие кнопки увеличивает количество секунд в тайм-ауте.

При отключении таймера ознакомьтесь со статьей **Как включить таймер при загрузке Ideco NGFW Novum**.

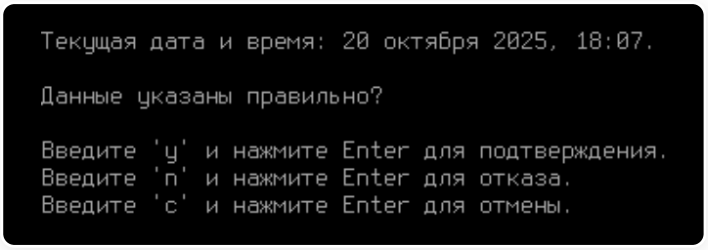
2. Выберите диск и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой находится сервер:

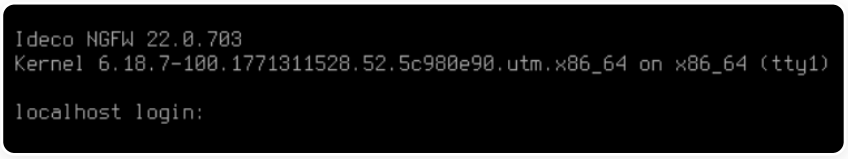


4. **Обязательно проверьте правильность даты и времени.** При необходимости настройте дату и время в соответствии с временной зоной сервера:



Извлеките USB-диск после установки Ideco NGFW Novum, чтобы загрузка с него не началась заново.

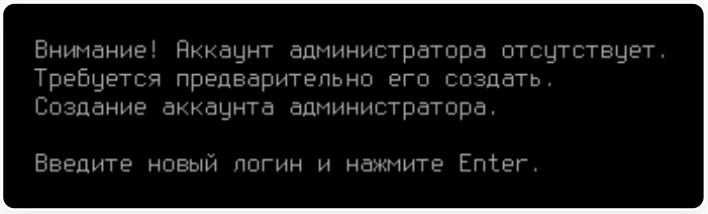
5. Не нажимайте никаких клавиш при появлении окна:



После загрузки система автоматически перейдет к локальному интерфейсу Ideco NGFW Novum.

Создание учетной записи администратора

Создайте учетную запись администратора после уведомления **Создание аккаунта администратора**:



Требования к логину и паролю

Логин:

- Не должен начинаться с цифры.
- Не должен содержать специальных и пробельных символов, кроме дефиса `-`.
- **Длина логина** - от 1 до 31 символа включительно.

Пароль:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.

- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

Если пароль не соответствует требованиям политики безопасности, то появится надпись с информацией, что пароль ненадежен. Потребуется ввести новый пароль с учетом требований к нему.

Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как управляющие символы: `^[[2~;` , `^[[4~;` и так далее.

Настройка интерфейса управления

С версии 21 Ideco NGFW Novum у интерфейсов появились роли:

Control Plane

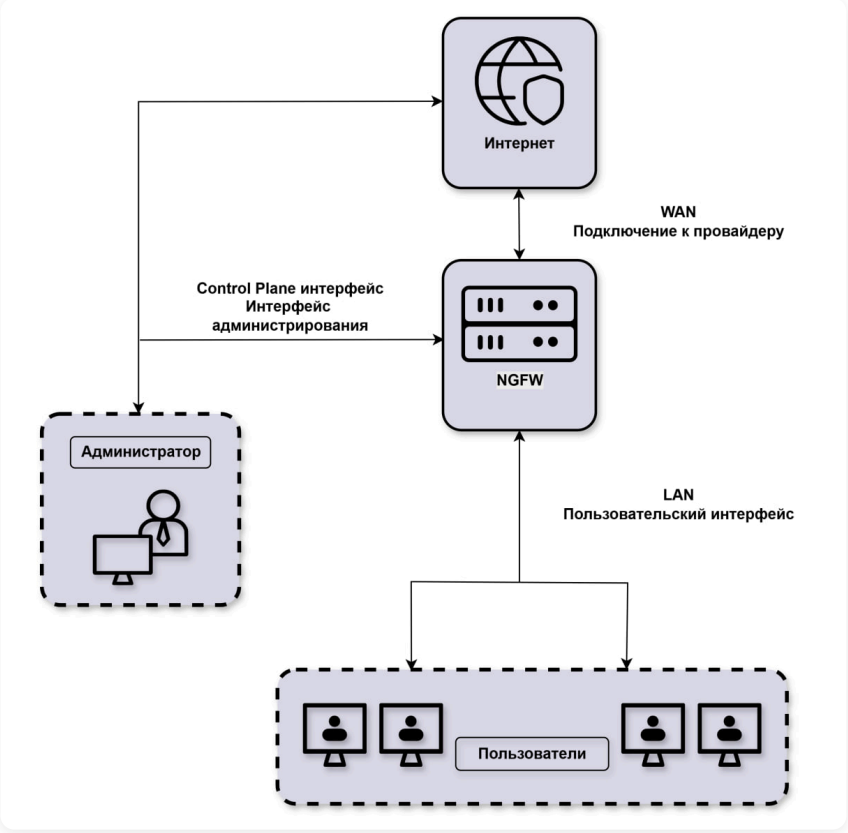
Используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза.

Для доступа пользователей в сеть через NGFW Novum подключайте их к интерфейсу с типом LAN.

Если CP-интерфейс не имеет выхода в интернет, необходимо дополнительно настроить WAN-интерфейс через веб-интерфейс.

Интерфейс Control Plane не обязателен - для администрирования может использоваться LAN-интерфейс.

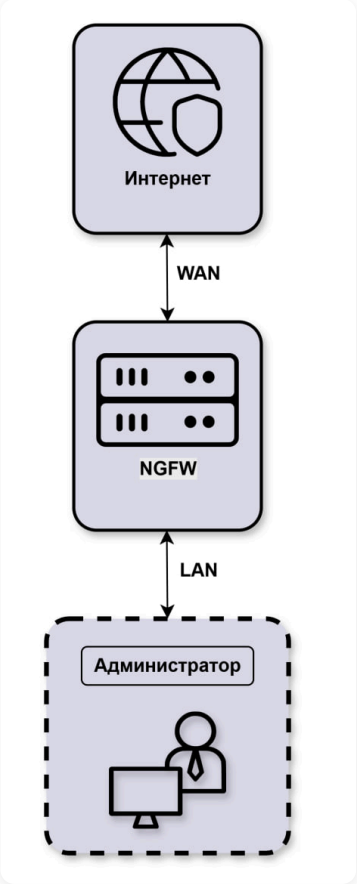
Схема сети с CP-интерфейсом:



LAN

Используется для создания локальных интерфейсов и администрирования NGFW Novum.

Схема сети с LAN-интерфейсом:



WAN

Используется для подключения к провайдеру. WAN-интерфейс для пользовательского трафика настраивается через веб-интерфейс (подробнее - в статье Первоначальная настройка).

При использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса.
Для корректной идентификации сетевой карты используйте MAC-адрес сетевой карты.

Для настройки Ideco NGFW Novum через веб-интерфейс настройте соответствующий интерфейс в локальном меню.

1. Перейдите в раздел **Ethernet-интерфейсы** → **Создать интерфейс**:

```
Управление сервером

1. Консоль
2. Физические порты
3. Ethernet-интерфейсы
4. Отключить все статические маршруты и добавить новый
5. Выбор типа кластерной сети
6. Включить доступ к веб-интерфейсу из внешней сети
7. Включить доступ к серверу по SSH из Интернет
8. Включить доступ к серверу по SSH из локальных сетей
9. Включить режим `Разрешить Интернет всем`
10. Сбросить блокировки по IP
11. Отключить пользовательский межсетевой экран
12. Создать новый бэкап
13. Восстановить из бэкапа
14. Мгновенно восстановить из бэкапа
15. Включить доступ Удаленного Помощника
16. Контакты технической поддержки
17. Восстановиться на предыдущую версию
18. Перезагрузка сервера
19. Отключить сервер
20. Выход

Введите номер пункта и нажмите Enter.
# 3

1. Показать список интерфейсов
2. Включить/Отключить интерфейс
3. Создать интерфейс
4. Изменить интерфейс
5. Удалить интерфейс
```

2. Выберите порт для доступа к веб-интерфейсу:

```
Выберите порт:

-------------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------------
  1    |  eth0_ff  |  bc:24:11:96:55:ff  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  2    |  eth1_c9  |  bc:24:11:26:e3:c9  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  3    |  eth2_e5  |  bc:24:11:9a:ca:e5  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
```

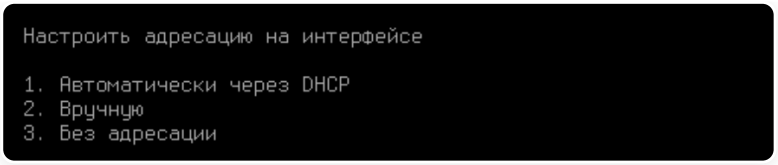
3. Введите имя интерфейса и выберите роль:

```
Введите имя интерфейса (или оставьте пустым) и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# CP

Выберите роль для интерфейса:

1. CP
2. LAN
3. WAN
```

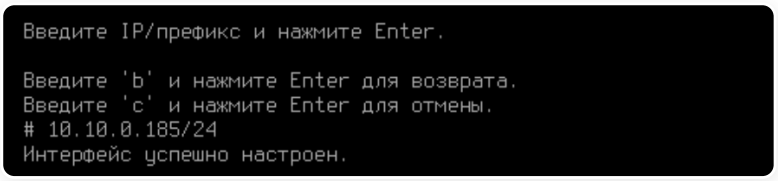
4. Выберите **Системный контекст**:

```
Выберите VCE:

1. Системный контекст
```

5. Настройте локальную сеть **Автоматически через DHCP** или **Вручную**:



6. Если выбрали **Вручную**, введите локальный IP-адрес и маску подсети в формате `ip/маска` и нажмите **Enter**:



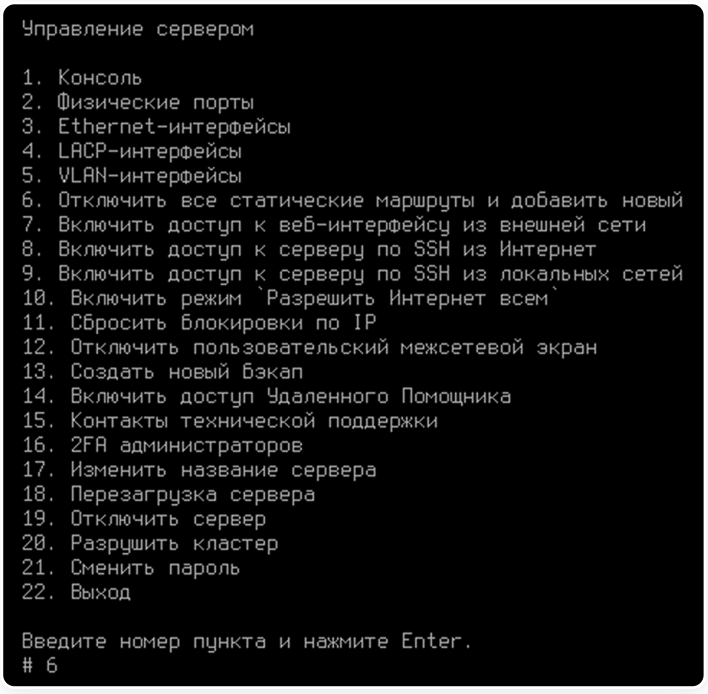
Настройка маршрутов на NGFW Novum для доступа из другой сети

В локальном меню можно настроить статическую маршрутизацию для первичного доступа к веб-интерфейсу, а также в аварийных ситуациях (только через консоль).

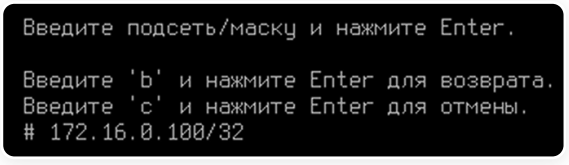
Например, настроен интерфейс `10.10.0.185/24`. Чтобы настроить маршрут до компьютера администратора с IP-адресом `172.16.0.100`, выполните действия:

1. Вернитесь в главное меню, нажав `c`.

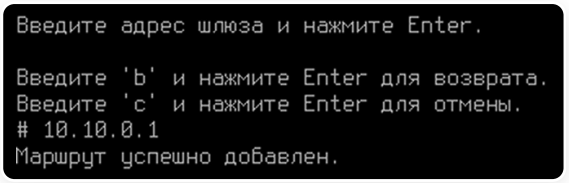
2. Выберите **Отключить все статические маршруты и добавить новый**:



3. Укажите подсеть `172.16.0.100/32`:



4. Введите IP-адрес шлюза:



После этого появится доступ к веб-интерфейсу NGFW Novum.

Можно настроить маршрут по умолчанию для доступа к NGFW Novum из другой сети. Для этого:

1. Укажите подсеть `0.0.0.0/0` - маршрут по умолчанию:

2. Введите IP-адрес шлюза:

```
Введите адрес шлюза и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# 10.10.0.1
Маршрут успешно добавлен.
```

7. После настройки интерфейса можно перейти в веб-интерфейс. Подробная информация о первоначальной настройке в статье.

Если в Ideco NGFW Novum настроен кластер, в локальном меню будет отсутствовать пункт **Восстановиться на предыдущую версию**.

Полезные ссылки

- **Установка Ideco NGFW Novum через COM-порт**

Подключение к Ideco NGFW Novum по COM-порту

Установка Ideco NGFW Novum по COM-порту

COM-порт по умолчанию включен.

Для установки Ideco NGFW Novum через COM-порт на серверы без мониторов и IPMI выполните шаги:

Шаг 1. Создание загрузочного USB-накопителя

Создайте загрузочный USB-накопитель Ideco NGFW Novum. Воспользуйтесь статьей.

Шаг 2. Подготовка BIOS

Этот шаг можно пропустить, если:

- Опция **Console Redirection** включена.
- Опция **SecureBoot** отключена.
- Опция **Hyper-Threading (Intel)** или **SMT (AMD)** отключена, если используется **Высокопроизводительный** контекст.
- Не требуется выбирать загрузочное устройство (BIOS поддерживает загрузку с USB-накопителя по умолчанию).

Если BIOS поддерживает опцию **Console Redirection to Serial Port**, включите ее. Опция находится в разделах, связанных с **Serial Port** или **Supervisor**, и позволяет контролировать процесс установки через COM-порт, начиная с экрана BIOS.

При отсутствии поддержки **Console Redirection to Serial Port** может потребоваться подключение монитора к серверу.

Проведите подготовку BIOS:

1. Выберите USB-накопитель устройством загрузки по умолчанию.
2. Отключите **SecureBoot**.
3. Если используете **Высокопроизводительный** контекст, отключите технологии:

- **Hyper-Threading (Intel)**.
- **SMT (AMD)**.

Шаг 3. Подключение через COM-порт

1. Отключите питание сервера.

2. Подключите компьютер к консольному порту с помощью консольного кабеля.

3. Установите на компьютер программу **PuTTY** или аналогичные утилиты, такие как **tio** или **MobaXterm**, чтобы подключиться к консольному порту.

4. Проверьте, что в используемой утилите заданы параметры:

- **Speed (baud)** - 115200.
- **Data bits** - 8.
- **Stop bits** - 1.
- **Flow control** - XON/XOFF.
- **Terminal-type (или Emulation)** - ANSI.

Пример настройки утилиты PuTTY

1. Перейдите в раздел **Connection** → **Serial** → **Configure the serial line** и укажите значения:

- **Speed (baud)** - 115200.
- **Data bits** - 8.
- **Stop bits** - 1.

- **Flow control** - XON/XOFF.
- **Serial line to connect to**:
  - **Windows** - укажите порт в формате `COMx`, где `x` - номер порта в системе. Например, `COM1`. Чтобы узнать номер порта, откройте **Диспетчер устройств** и найдите раздел **Порты (COM и LPT)**.
  - **Linux** - укажите путь к устройству в формате `/dev/ttyXXXX`. Например, `/dev/ttyUSB0`. Для вывода списка доступных устройств используйте команду `ls /dev/tty`.
  - **macOS** - укажите путь к устройству в формате `/dev/tty.usbserial-XXXXXX`. Например, `/dev/tty.usbserial-DB008OZL`. Для вывода списка доступных устройств используйте команду `ls -l /dev/*usbserial*`.

2. Перейдите в раздел **Connection** → **Data** → **Terminal details** и введите в поле **Terminal-type string** параметр **ANSI**:

3. Нажмите **Open**.

Шаг 4. Процесс установки

1. Запустите терминал, вставьте загрузочный USB-накопитель и включите сервер.

> Через некоторое время после включения на экране терминала отобразится:
>
> - Установщик Ideco NGFW Novum, если опция **Console Redirection** отсутствует в BIOS или выключена.
> - Процесс загрузки сервера, начиная с BIOS и заканчивая установщиком Ideco NGFW Novum, если опция **Console Redirection** включена.

2. Выполните установку Ideco NGFW Novum.

Управление Ideco NGFW Novum по COM-порту

Если подключение по COM-порту ранее не настраивалось, выполните шаги 2 и 3 из инструкции выше. После подключения вы сможете управлять Ideco NGFW Novum через COM-порт посредством локального меню.

Возможные проблемы

Проблема	Возможная причина	Решение
На экране терминала пусто	Не подключен кабель	Подключите кабель COM-порта к серверу
На экране терминала пусто, кабель подключен	Поздно подключен кабель	Нажмите `Ctrl+R` в локальном меню, чтобы обновить дашборд
Не отображается BIOS через COM-порт	BIOS не поддерживает опцию **Console Redirection to Serial Port**	Подключитесь к серверу напрямую
Не отображается BIOS через COM-порт	В BIOS отключена опция **Console Redirection to Serial Port**	Включите опцию **Console Redirection to Serial Port**

Как включить таймер при загрузке Ideco NGFW Novum?

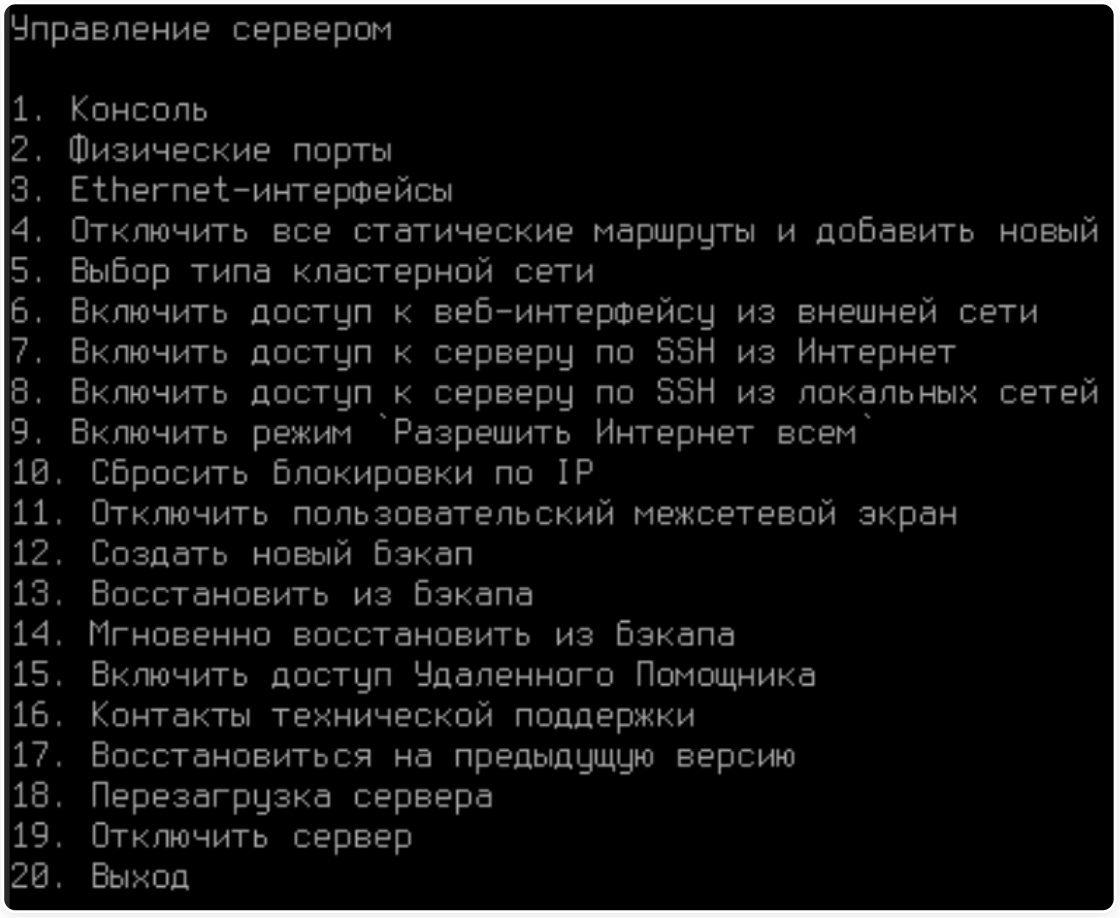
При отключении таймера также отключается автоматический выбор пункта меню. В этом случае система не загрузится сама после обновления, рестарта или переключения ноды в режиме кластеризации до момента нажатия **Enter**.

Для включения таймера выполните действия:

1. При загрузке сервера выберите Ideco NGFW Novum, нажав **Enter**:



2. Дождитесь загрузки, перейдите в локальное меню и выберите **Перезагрузка сервера**:



3. При загрузке сервера выберите необходимое количество секунд в тайм-ауте, нажав **+** на клавиатуре:



4. Подтвердите выбор, нажав **Enter**.

Первоначальная настройка

Перед началом настройки рекомендуем создать бэкап, который позволит восстановить первоначальные настройки в случае необходимости.

Подключение к веб-интерфейсу Ideco NGFW Novum

1. Запустите на любом компьютере в сети интерфейса Control Plane или LAN поддерживаемый браузер (современные версии Firefox, Chrome и браузеров, основанных на Chromium). Подробнее про особенности интерфейсов - в статье.

2. Введите в адресной строке IP-адрес, указанный при настройке интерфейса, и порт 8443.

Пример: `192.168.100.2:8443`

При переходе к учетной записи в браузере отобразится предупреждение безопасности. Необходимо подтвердить подключение, войти в веб-интерфейс и установить сертификат, чтобы исключить появление предупреждения.

3. Введите логин и пароль от учетной записи, созданной при установке Ideco NGFW Novum.

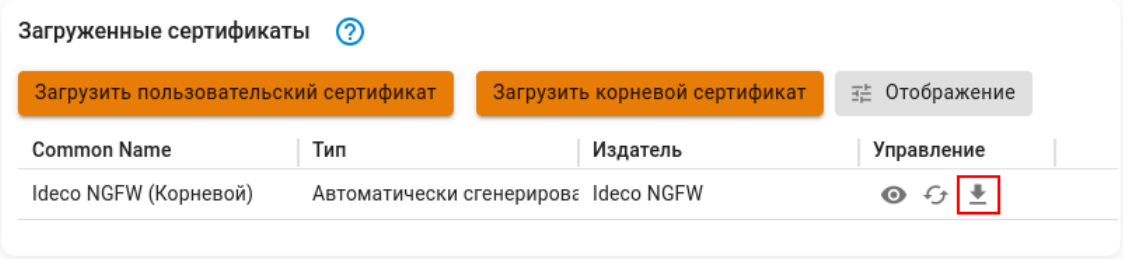
Импорт корневого сертификата Ideco NGFW Novum

Для устранения предупреждения в браузере при входе в веб-интерфейс импортируйте корневой сертификат Ideco NGFW Novum и добавьте в доверенные корневые центры сертификации устройства:

1. Скачайте сертификат одним из способов:

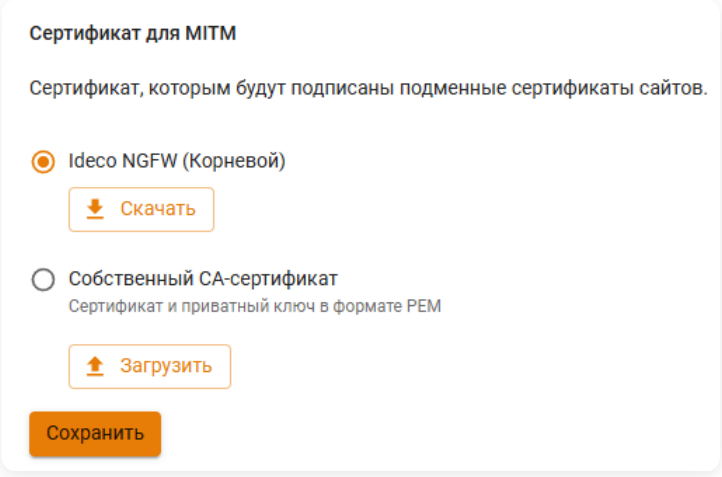
Из раздела Сервисы

В **Сервисы** → **Сертификаты** → **Загруженные сертификаты** нажмите на стрелку для скачивания:



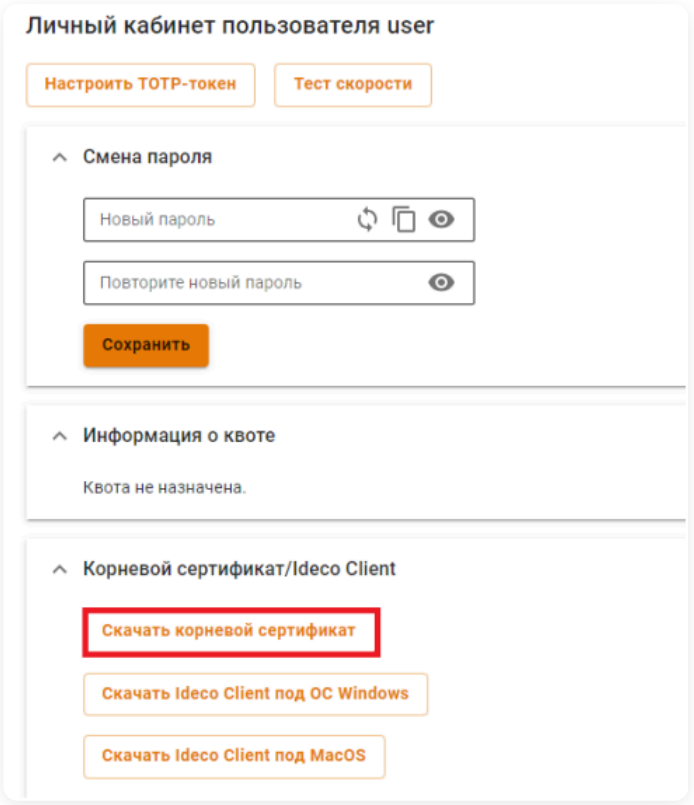
Из раздела Правила трафика

В **Правила трафика** → **Контент-фильтр** → **Настройки** нажмите **Скачать**:



Из личного кабинета пользователя

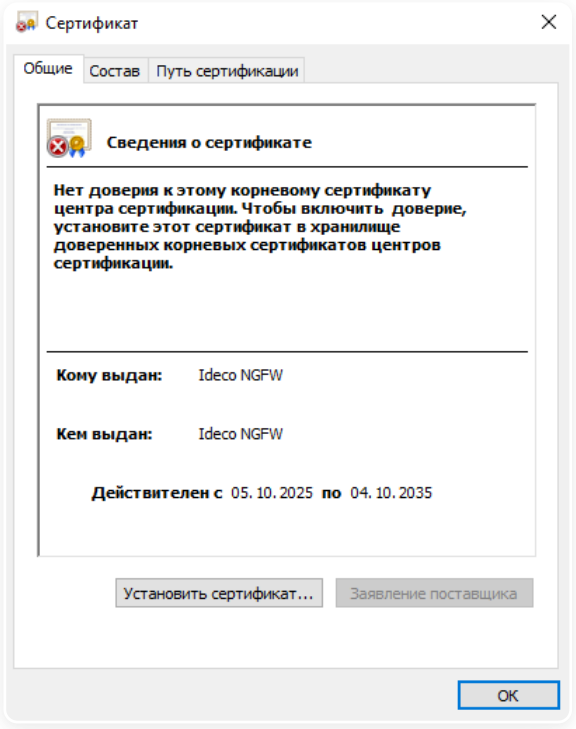
В личном кабинете Ideco NGFW Novum под учетной записью одного из пользователей перейдите на вкладку **Корневой сертификат/Ideco Client** и нажмите **Скачать корневой сертификат**:



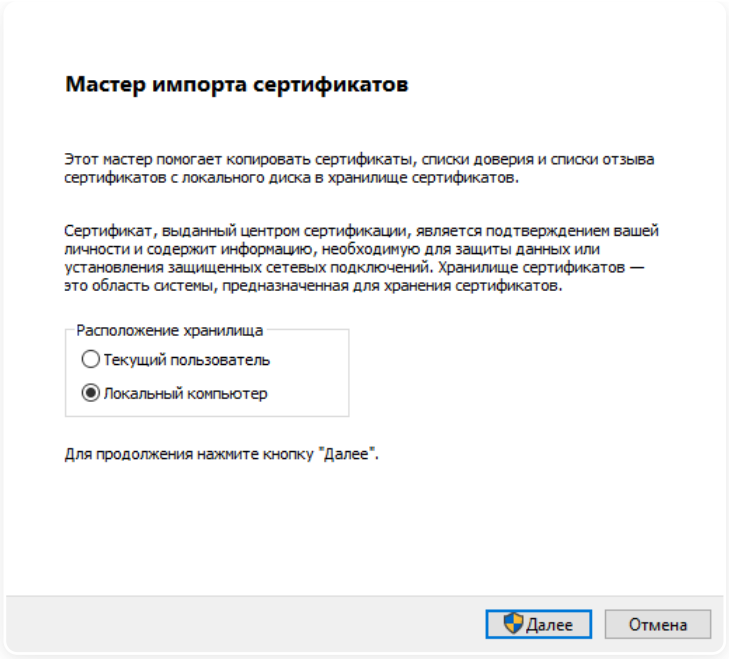
Для публикации личного кабинета пользователя воспользуйтесь статьей.
2. Импортируйте корневой сертификат.

Пример для Windows

1. Откройте скачанный сертификат и нажмите **Установить сертификат**:

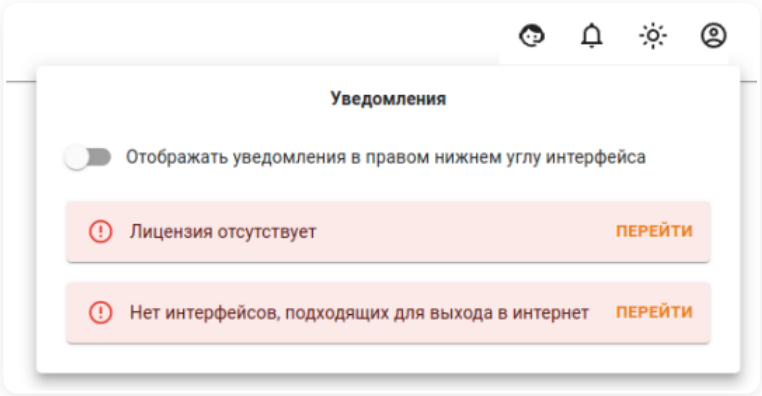


2. Выберите расположение хранилища **Локальный компьютер**:



3. Установите сертификат в **Доверенные корневые центры сертификации**:

После первого входа в веб-интерфейс появятся уведомления, которые помогут настроить подключение к провайдеру и зарегистрировать сервер для корректной работы Ideco NGFW Novum:

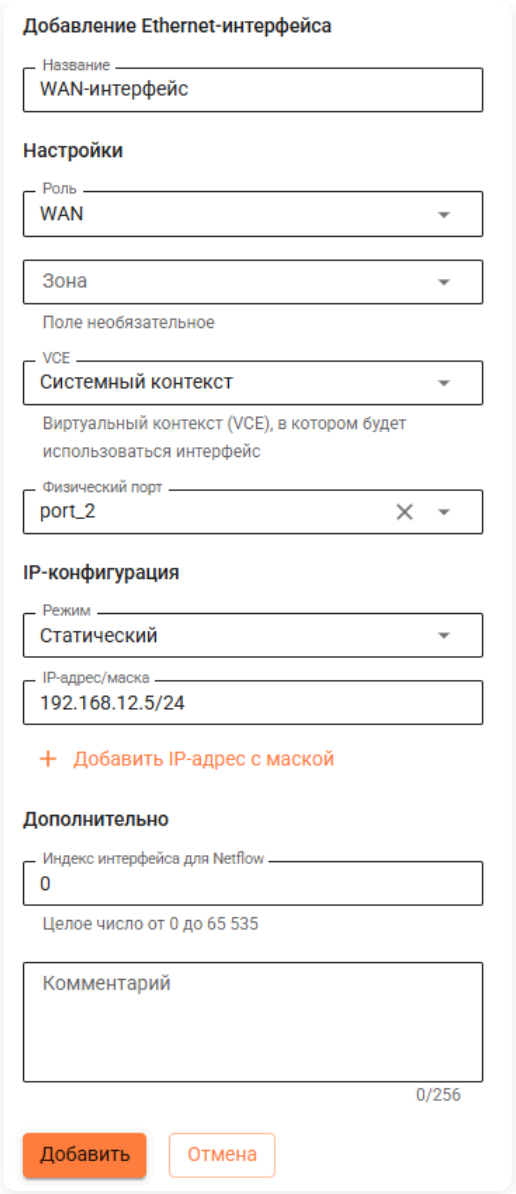


Настройка WAN-интерфейса

Если вы настроили интерфейс (Control Plane или LAN) и у него нет доступа в интернет, настройте WAN-интерфейс, чтобы получить лицензию. Выполните действия:

1. Перейдите в **Сервисы** → **Сетевые интерфейсы**, нажмите **Добавить** и выберите пункт **Ethernet**.

2. Заполните поля:



- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - выберите WAN.
- **Физический порт** - порт на сетевом адаптере, который будет использоваться в созданном интерфейсе.
- **Режим** - выберите Статический и укажите IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.

3. Нажмите **Добавить**. WAN-интерфейс появится в таблице интерфейсов.

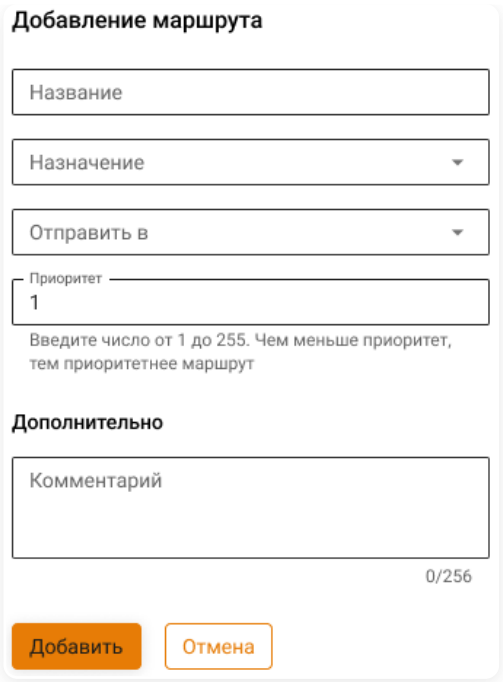
Настройка подключения к провайдеру

Настройте шлюз для WAN-интерфейса, выполнив действия:

Маршрутизация

1. Перейдите в **Маршрутизация** → **Статическая** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

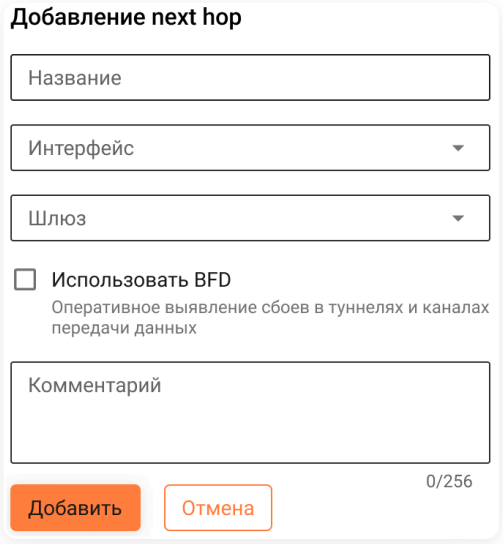


- **Название** - укажите название правила.
- **Назначение** - выберите **Любой**.
- **Отправить в** - введите IP-адрес шлюза.

SD-WAN

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

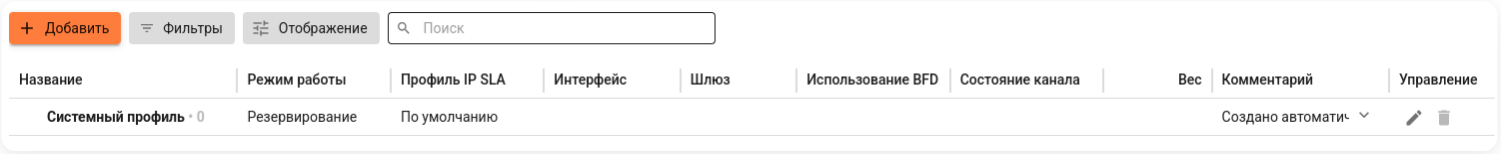


- **Название** - укажите название.
- **Интерфейс** - выберите созданный интерфейс.
- **Шлюз** - укажите IP-адрес следующего узла маршрутизации (next hop), на который будет направляться трафик. Адрес шлюза должен находиться в сети выбранного интерфейса.
- **Использовать BFD** - включите опцию, если поддержка BFD включена на стороне указанного шлюза.

При выборе интерфейса, который получает IP-адрес по DHCP:

- Если оставить поле **Шлюз** пустым, то будет использован шлюз, полученный от DHCP-сервера.
- Если в поле **Шлюз** указать IP-адрес, то в качестве шлюза будет использоваться указанный IP-адрес, а полученный от DHCP-сервера проигнорируется.

3. Перейдите в раздел **Профили Next hop** и нажмите для редактирования **Системного профиля**:



4. Перейдите на вкладку **Next hop**, нажмите **Выбрать next hop** и выберите next hop, созданный на шаге 2.

5. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

После настройки шлюза зарегистрируйте сервер. Подробная информация в статье.

Чтобы получить доступ в интернет и настроить авторизацию, выполните действия. В противном случае доступ в интернет для устройства с установленным Ideco NGFW Novum будет заблокирован.

Настройка других типов подключений

Если провайдер использует другой тип подключения, ознакомиться с остальными инструкциями по настройке можно по ссылкам:

- Сетевые интерфейсы.
- Одновременное подключение к нескольким провайдерам.

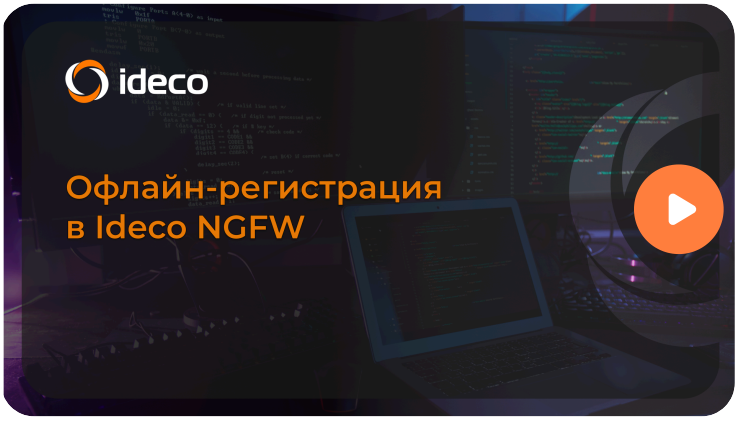
Регистрация сервера

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE



Для активации лицензии необходима обязательная регистрация сервера в MY.IDECO.

NGFW Novum без лицензии по умолчанию не пропускает трафик пользователей в интернет. Для получения лицензии используйте альтернативный (дополнительный) шлюз. Если это невозможно, временно включите опцию **Полный доступ** - для этого перейдите в раздел **Техническая поддержка**, нажав в правом верхнем углу экрана. Подробнее - в статье.

Перед активацией лицензии убедитесь, что в NGFW Novum установлены корректные дата и время, иначе подключиться к серверу лицензирования не получится. Для установки даты и времени воспользуйтесь статьей.

Выберите удобный способ получения лицензии:

- Через **онлайн-регистрацию**.
- Через **офлайн-регистрацию**. Компьютеру администратора должен быть обеспечен собственный выход в интернет.

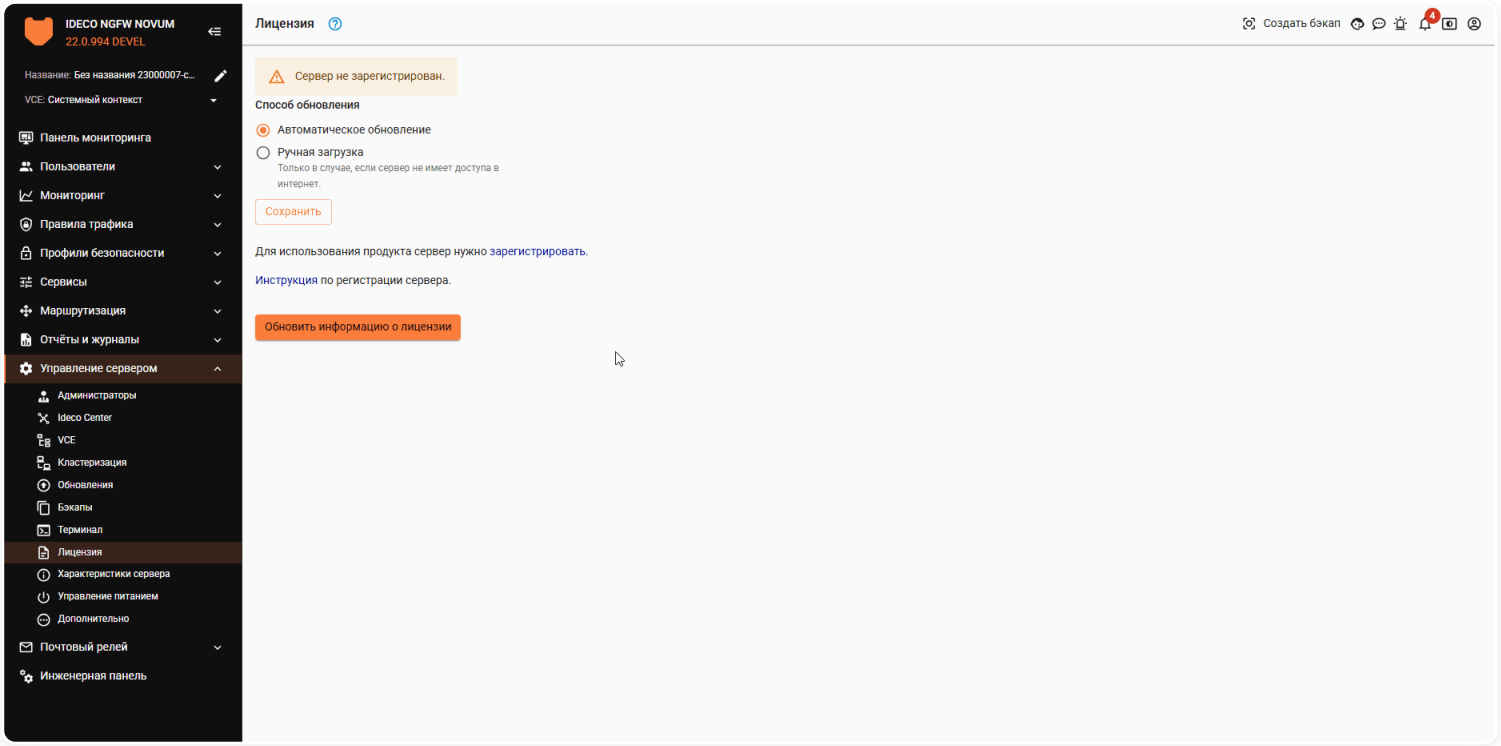
Онлайн-регистрация

Шаги онлайн-регистрации сервера и привязки лицензии:

1. Перейдите в веб-интерфейс Ideco NGFW Novum в **Управление сервером** → **Лицензия**, выберите **Автоматическое обновление** в качестве способа обновления, нажмите **Сохранить**.

2. Перейдите в MY.IDECO, нажав **Зарегистрировать**.

3. В открывшемся окне выберите компанию и нажмите **Добавить**. После добавления нажмите **Обновить информацию о лицензии** для проверки состояния лицензии:



В режиме автоматического обновления сервер ежедневно проверяет статус лицензии на MY.IDECO. В случае отсутствия соединения попытки возобновляются каждую минуту.

Офлайн-регистрация

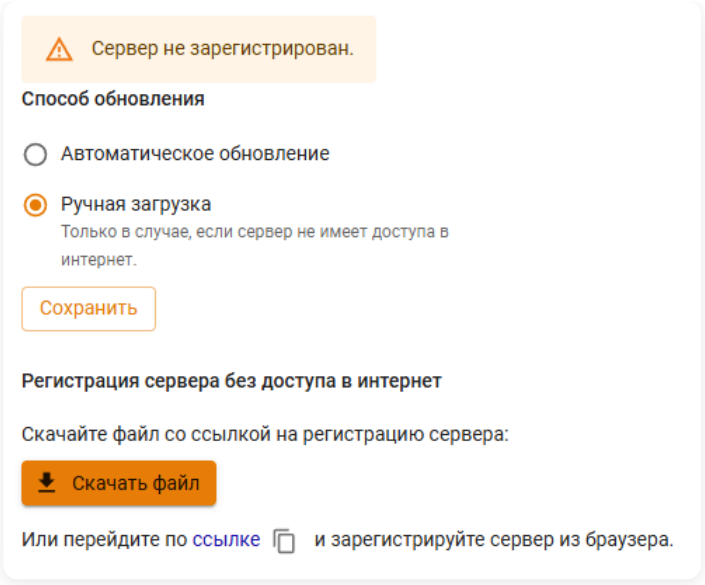
Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

1. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum. Выберите **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Для этого нажмите **Скачать файл** или скопируйте ссылку из веб-интерфейса:

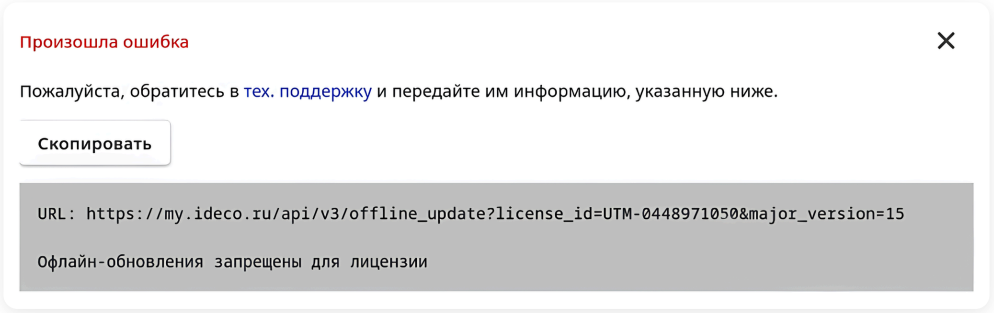


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

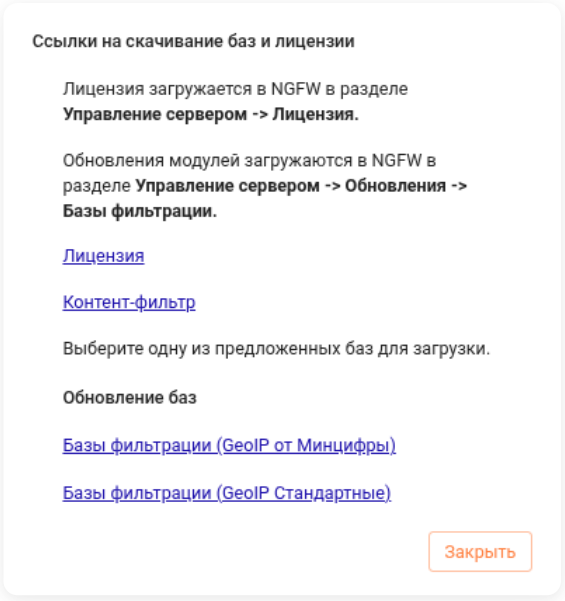
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

5. Перейдите в **NGFW** → **Лицензирование** в MY.IDECO. Нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `UTM (UTM Unknown)`.

Если была выбрана лицензия, не подходящая для офлайн-регистрации сервера, то появится ошибка:

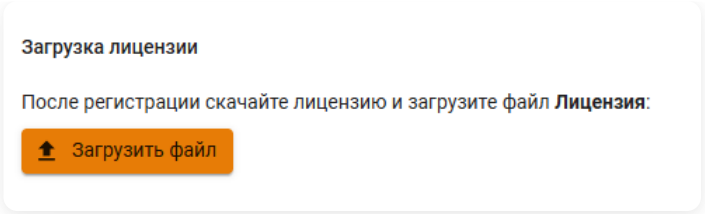


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



Если при скачивании Обновления баз (Предотвращение вторжений, базы GeoIP) через **Google Chrome** возникают проблемы, в настройках браузера разрешите **Небезопасный контент** для MY.IDECO.

7. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum и загрузите файл с лицензией, скачанный в пункте 6:



Повторная регистрация сервера после удаления

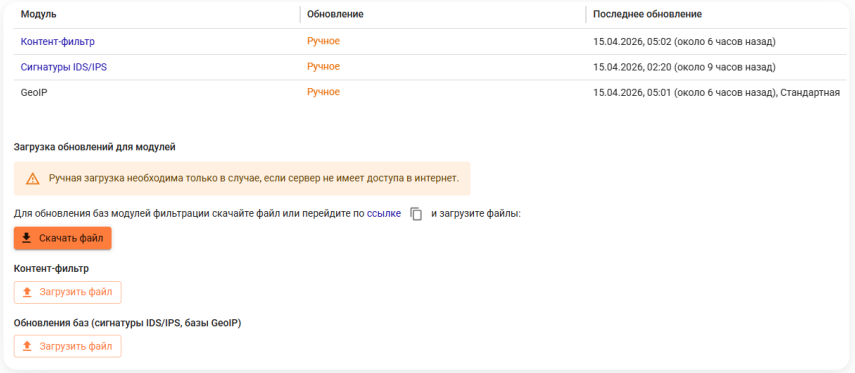
1. Откройте терминал и введите команду:

```
rm /var/cache/ideco/license-backend/license.json
systemctl restart ideco-license-backend.service
```

2. Следуйте пунктам по офлайн-регистрации, которые приведены выше.

Офлайн-обновление баз модулей безопасности

Чтобы обновить базы модулей безопасности в режиме офлайн, перейдите в веб-интерфейс Ideco NGFW Novum в раздел **Управление сервером** → **Обновления** → **Базы фильтрации** и загрузите скачанные в шестом пункте Офлайн-регистрации файлы, нажав на соответствующие кнопки:



Базы фильтрации Ideco NGFW Novum могут меняться ежедневно, поэтому при ручной загрузке обновляйте базы как можно чаще.

Получение доступа в интернет

Для получения доступа в интернет на устройстве пользователя после первоначальной настройки и регистрации сервера выполните действия:

1. Убедитесь, что устройство пользователя настроено одним из способов:

- Устройство находится в одном широковещательном домене с сетевым интерфейсом NGFW: между устройствами только L2-коммутаторы или прямое подключение. В качестве шлюза указан NGFW.
- Интернет-трафик пользователя маршрутизируется на NGFW через промежуточные маршрутизаторы, L3-коммутаторы.

2. Убедитесь, что в веб-интерфейсе NGFW выбран нужный способ авторизации.

3. Выполните действия в зависимости от настроенного способа авторизации пользователя:

- **Веб-аутентификация** - способ авторизации, при котором запрос неавторизованного пользователя переадресуется на NGFW, а после успешной авторизации переходит по указанному пользователем запросу:
  - **Аутентификация через веб-интерфейс**. Зайдите в браузер с устройства пользователя. Введите логин и пароль, указанный при настройке учетной записи пользователя;
  - Для авторизации пользователей Active Directory воспользуйтесь статьей **Аутентификация пользователей AD/Samba DC**.

> При авторизации через **Веб-аутентификацию** проверьте, что у пользователя на сетевой карте в качестве шлюза (объединенных в цепочку нескольких шлюзов) или при прямых подключениях к прокси по умолчанию указан IP-адрес локального сетевого интерфейса NGFW. Убедитесь, что работает DNS-резолвинг адресов.

- **IP и MAC авторизация** - способ авторизации, при котором пользователь получает доступ в интернет без ввода логина и пароля:
  - **Авторизация по IP-адресу**. Проверьте, чтобы IP-адрес устройства пользователя совпадал с IP-адресом, указанным администратором в настройках учетной записи пользователя NGFW. Следуйте рекомендациям статьи **Авторизация по IP-адресу**.
  - Для настройки авторизации переносных устройств (например, рабочих ноутбуков сотрудников) или сетевых устройств, на которых не настроена привязка IP + MAC и выдается IP-адрес через DHCP, воспользуйтесь статьей **Авторизация по MAC-адресу**.

> Для авторизации пользователя по MAC-адресу оба устройства (NGFW и устройство пользователя) должны находиться в одном широковещательном домене, а NGFW должен выступать шлюзом.

- **Авторизация по подсетям** - способ автоматической авторизации большого количества устройств из требуемой подсети без привязки к MAC и/или конкретному IP.

Настройка высокопроизводительного контекста

Высокопроизводительный контекст (VCE VPP) - виртуальный контекст в Ideco NGFW Novum для обработки сетевого трафика с высокой пропускной способностью. Сетевой стек построен на технологиях DPDK (Data Plane Development Kit) и VPP (Vector Packet Processing), работающий в обход стека ядра Linux, который используется в **Классическом контексте** (VCE NGFW).

Ключевые архитектурные отличия:

- Сетевая карта передается в VCE VPP целиком, а не отдельными VLAN. Этим объясняется требование перезагрузки контекста после назначения интерфейсов.
- Контейнерная модель без гипервизора (на базе systemd-nspawn). VCE VPP можно запускать в виртуальных средах без вложенной виртуализации и связанных с ней потерь производительности.
- Жесткая привязка ресурсов - выделенные контексту CPU-ядра, оперативная память и сетевые карты не перераспределяются динамически.

Основные преимущества перед **Классическим контекстом**:

- Поддержка до 100 000 правил **Межсетевого экрана**.
- Фильтрация трафика на любых TCP-портах через **Профили безопасности**.
- Более высокая пропускная способность при обработке трафика.

Ряд функций недоступен, например, DDNS, IPsec и ГОСТ VPN. Полный список различий - в статье.

Подробнее об архитектуре VCE - в статье **Виртуальные контексты в Ideco NGFW: как работают VCE изнутри**.

Статья описывает настройку VCE VPP внутри Ideco NGFW Novum. Входная точка: **Системный контекст** установлен, зарегистрирован и имеет доступ в интернет. Если нет - выполните шаги из статей:

- **Первоначальная настройка**
- **Регистрация сервера**
- **Получение доступа в интернет**

Настройка в Системном контексте

Шаг 1. Создание контекста

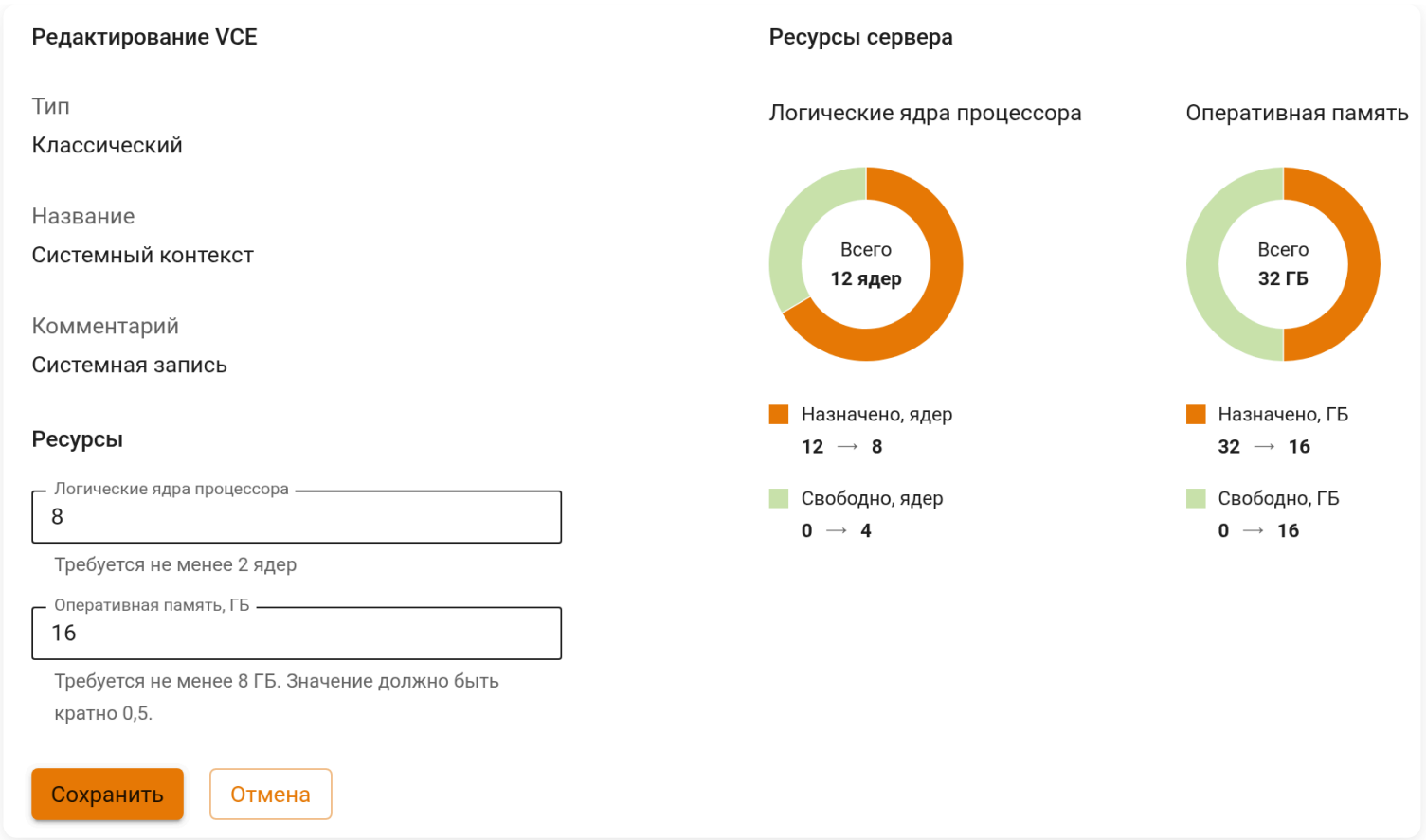
Для **Высокопроизводительного контекста** потребуются:

- Минимум **4 логических ядра**.
- Минимум **8 ГБ оперативной памяти**.

Рекомендуем отключить Hyper-Threading (Intel) и SMT (AMD) в BIOS/UEFI сервера - эти технологии существенно снижают производительность VCE VPP. Не рекомендуем использовать двухпроцессорные системы.

Перейдите в **Управление сервером** → **VCE** и выполните действия:

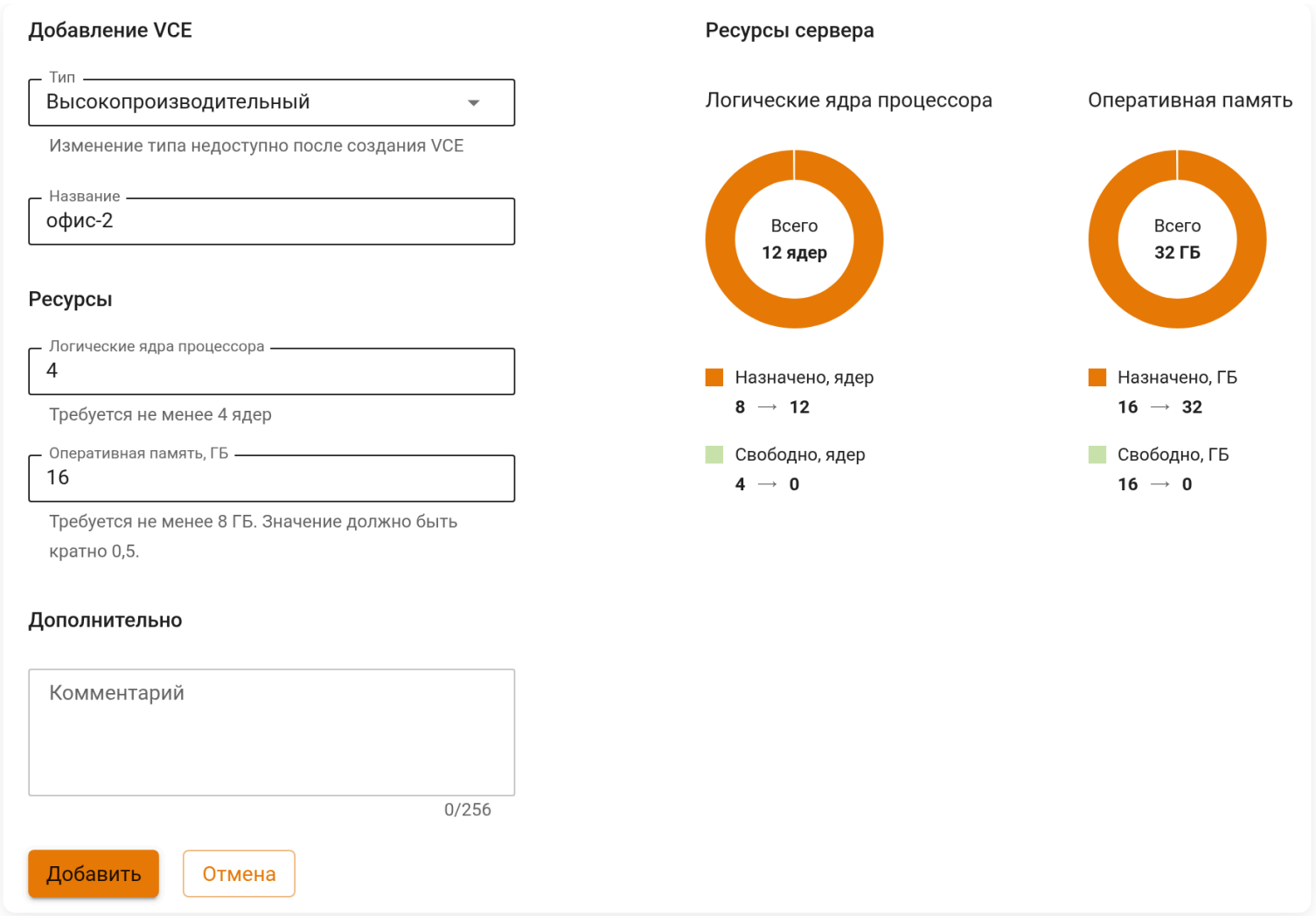
1. Нажмите  в строке **Системного контекста**, освободите в пул **Свободных ресурсов** не менее 4 ядер и 8 ГБ оперативной памяти:



2. Нажмите **Сохранить**.

3. Нажмите **Добавить** для создания нового контекста.

4. Выберите тип контекста **Высокопроизводительный**, укажите название и назначьте ресурсы из пула свободных:



5. Нажмите **Добавить**.

Шаг 2. Создание сетевых интерфейсов

Сетевые интерфейсы для VCE VPP создаются и редактируются только в **Системном контексте**. В **Классических** и **Высокопроизводительных контекстах** таблица интерфейсов доступна только для чтения.

Перейдите в **Сервисы** → **Сетевые интерфейсы** и создайте два интерфейса:

- Интерфейс с ролью **WAN** - для подключения к провайдеру.
- Интерфейс с ролью **LAN** - для пользовательской сети.

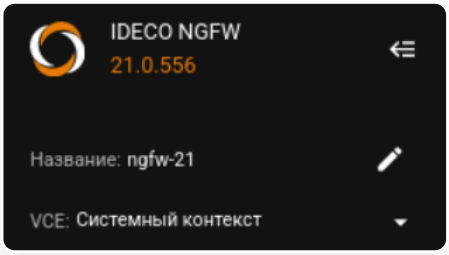
При создании каждого интерфейса укажите его принадлежность к созданному VCE VPP. Пример настройки в статье.

После назначения интерфейсов перезагрузите контекст для корректной работы интерфейсов.

Шаг 3. Подключение к веб-интерфейсу

Перейдите из **Системного контекста** в веб-интерфейс созданного VCE VPP одним из способов:

- В **Управление сервером** → **VCE** нажмите напротив нужного контекста - откроется новая вкладка.
- Нажмите в левом верхнем углу **Системного контекста** и выберите нужный VCE:



Настройка в Высокопроизводительном контексте

Шаг 4. Создание администратора

Только что созданный VCE VPP не содержит администраторов. Учетные записи администраторов **Системного контекста** в VCE VPP не действуют.

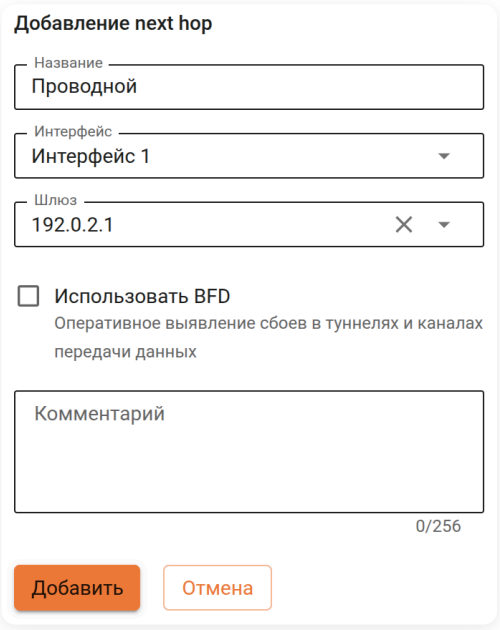
Для дальнейшей работы создайте отдельного администратора по инструкции из статьи **Администраторы**.

Шаг 5. Настройка подключения к провайдеру

Настройте шлюз для выхода в интернет:

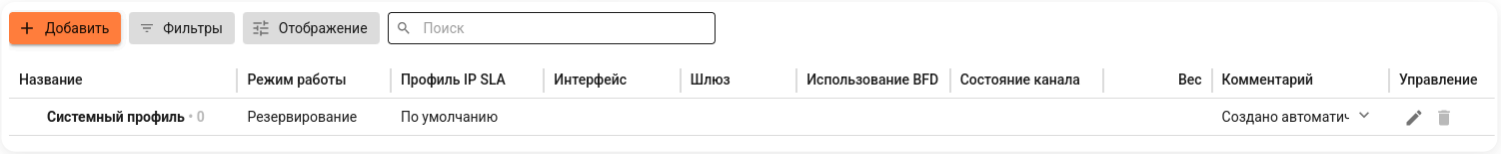
1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:



- **Название** - укажите название.
- **Интерфейс** - выберите WAN-интерфейс, созданный для VCE VPP в шаге 2.
- **Шлюз** - укажите IP-адрес шлюза провайдера. Адрес должен находиться в сети выбранного интерфейса.
- **Использовать BFD** - включите опцию для проверки доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection). Поддержка BFD должна быть включена и на стороне указанного шлюза.

3. Перейдите в **SD-WAN** → **Профили next hop** и нажмите для редактирования **Системного профиля**:



4. Перейдите на вкладку **Next hop**, нажмите **Выбрать next hop** и выберите next hop, созданный на предыдущем шаге.

5. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

Если шлюз не обеспечивает выход в интернет, VCE VPP не получит лицензию и не сможет загрузить обновления баз модулей

безопасности.

Шаг 6. Проверка лицензии

После завершения настройки подключения к провайдеру перейдите в раздел **Лицензия** - данные будут автоматически получены из MY.IDECO.

На Ideco NGFW Novum с лицензией на 100 пользователей каждый созданный VCE поддерживает 100 пользователей. В будущих версиях количество пользователей будет распределяться между **Системным контекстом** и VCE.

Шаг 7. Настройка Межсетевого экрана

В VCE VPP по умолчанию установлено запрещающее FORWARD-правило. Без явного разрешающего правила пользователи не получат доступ в интернет.

Перейдите в **Правила трафика** → **Межсетевой экран** и создайте разрешающее правило для пользовательского трафика в соответствии с политикой безопасности вашей организации.

Шаг 8. Настройка авторизации пользователей

Настройте метод авторизации в разделе **Пользователи** → **Авторизация**. Ниже - базовые методы для быстрого старта:

- **Веб-аутентификация** - пользователь вводит логин и пароль в браузере при попытке выйти в интернет.
- **IP авторизация** - доступ автоматически по IP-адресу без ввода пароля.
- **Авторизация по подсетям** - автоматическая авторизация всех устройств из указанной подсети.

Полный список доступных методов, включая интеграцию с Active Directory, авторизацию через Ideco Client и пользователей терминальных серверов, смотрите в разделе **Авторизация**.

Авторизация по MAC-адресу в VCE VPP недоступна.

Дальнейшие шаги по настройке устройств пользователей аналогичны **Системному контексту**. Инструкция - в статье.

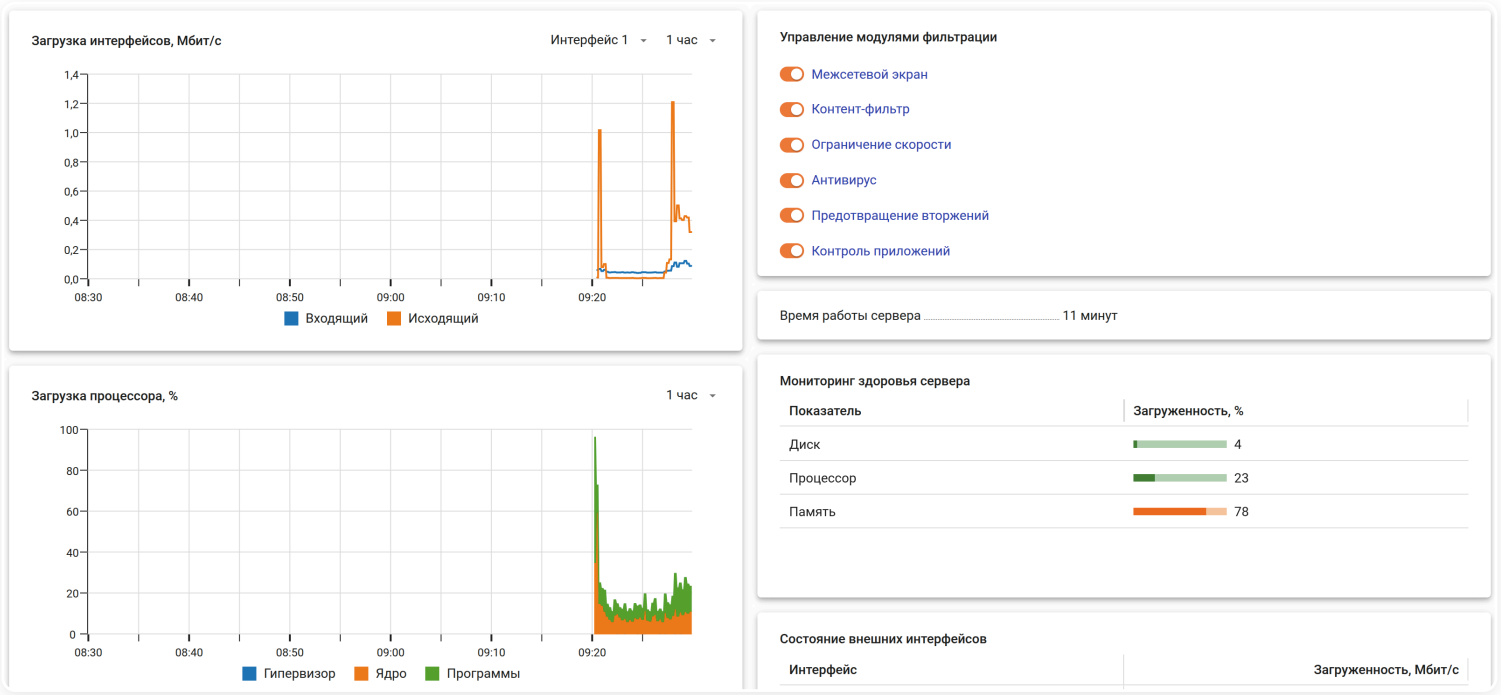
Полезные ссылки

- **VCE**
- **Отличия VCE NGFW и VCE VPP**
- **Лицензия**
- **Межсетевой экран**
- **Веб-аутентификация**
- **IP авторизация**
- **Авторизация по подсетям**
- **Авторизация**
- **Администраторы**
- **Получение доступа в интернет**
- **Первоначальная настройка**
- **Регистрация сервера**

Панель мониторинга

Классический контекст | Высокопроизводительный контекст

Модуль позволяет просматривать информацию о состоянии сервера за определенный промежуток времени:



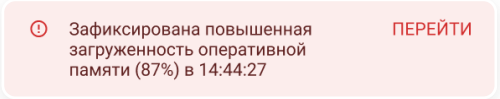
Отображение оперативной информации

- Загрузка интерфейсов, Мбит/с.
- Загрузка процессора, %.
- Занятая оперативная память, ГБ.
- Температура.

Есть возможность выбрать удобный промежуток времени для отображения: 5 минут, 1 час, 6 часов, 1 день, 7 дней.

Мониторинг здоровья сервера

Блок в реальном времени отображает метрики системы при помощи цветовой индикации. Цвет каждого индикатора (зеленый/желтый/красный) зависит от степени превышения пороговых значений. Если показатели остаются в желтой или красной зоне дольше определенного времени, будет отправлено уведомление:



Пороговые значения:

Диск

Зеленый - занято менее 80%.

Желтый - занято от 80% до 90% в течение 5 минут. Уведомление, если дольше 5 минут.

Красный - занято более 90% в течение 5 минут. Уведомление, если дольше 5 минут.

Процессор

Зеленый - нагрузка менее 60%.

Желтый - нагрузка от 60% до 85%. Уведомление, если дольше 1 минуты.

Красный - нагрузка более 85%. Уведомление, если дольше 1 минуты или сразу при нагрузке более 95%.

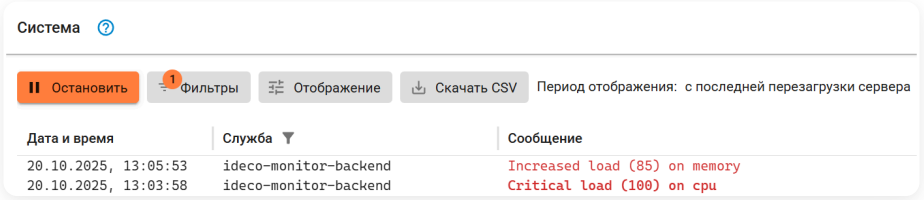
Память

Зеленый - доступно более 15%.

Желтый - доступно от 5% до 15%. Уведомление, если дольше 2 минут.

Красный - доступно менее 5%. Уведомление, если дольше 1 минуты.

При превышении порогов события записываются в логи. Для их просмотра перейдите в раздел **Система** и примените фильтр по службе `ideco-monitor-backend`:



Управление модулями фильтрации

Блок позволяет включить или выключить соответствующие модули фильтрации:

- Межсетевой экран.
- Контент-фильтр.
- Ограничение скорости.
- Антивирусы веб-трафика.
- Предотвращение вторжений.
- Контроль приложений.

Каждый из пунктов является ссылкой на соответствующий модуль.

Отображение статистической информации

- Время работы сервера.
- Состояние внешних интерфейсов.
- Топ хостов (можно выбрать количество в топе: 5, 10, 15, 20).
- Основная информация о лицензии.
- Параметры и загрузка IPsec (есть возможность перейти на страницу IPsec).

Особенности отображения информации

- График загрузки интерфейсов включает весь трафик NGFW, в том числе служебный.
- При выборе разных промежутков времени отображаемые максимальные значения на графике могут отличаться.
- Таблицы **Топ хостов** включают только пользователей с наибольшей скоростью входящего и исходящего трафика. При формировании статистики по хостам учитываются протоколы, определенные модулем **Контроль приложений**. При этом не учитывается служебный трафик NGFW.

Пользователи

Учетные записи

Создание и управление учетными записями пользователей

Перейти

Внешние каталоги

Настройка интеграций Ideco NGFW с Active Directory, ALD Pro, FreeIPA и RADIUS-сервером

Перейти

Аутентификация

Процесс аутентификации пользователей и настройка двухфакторной аутентификации

Перейти

Авторизация

Веб-аутентификация, правила авторизации по IP- и MAC-адресам, возможность авторизации по подсетям

Перейти

VPN-подключение

Настройка VPN-подключения с использованием протоколов: IKEv2/IPsec, SSTP, L2TP/IPsec

Перейти

Ideco Client

Установка и настройка Ideco Client, настройка Device VPN

Перейти

Профили устройств

Использование профилей для проверки устройств, подключаемых к NGFW через Ideco Client

Перейти

Обнаружение устройств

Автоматическое создание пользователя с авторизацией по IP-адресу и MAC-адресу для различных устройств

Перейти

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

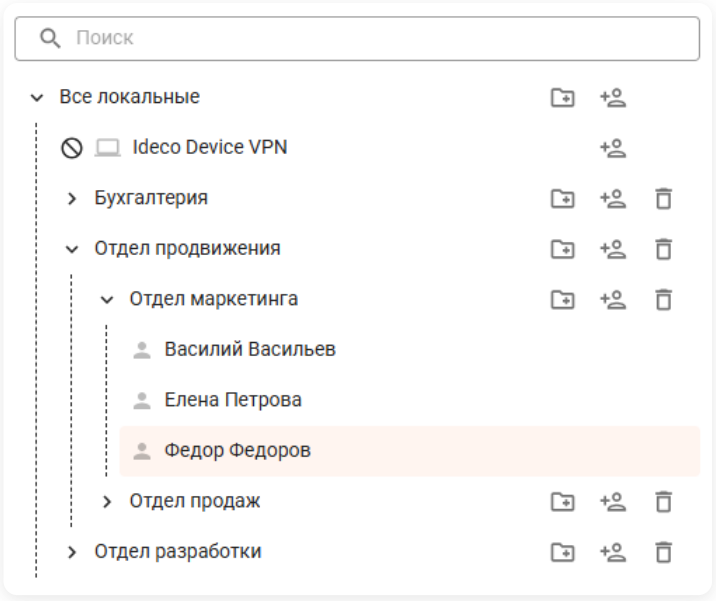
Учетные записи

Классический контекст | Высокопроизводительный контекст | API

С 21 версии Ideco NGFW Novum пользователи разделяются на локальных (сюда же входят импортированные) и пользователей внешних каталогов Active Directory. Пользователи AD более не импортируются в дерево пользователей.

Локальные пользователи

В веб-интерфейсе Ideco NGFW Novum локальные пользователи отображаются в виде дерева и могут быть организованы в группы с неограниченной вложенностью. Пример дерева локальных пользователей:



Группа **Ideco Device VPN** автоматически создается при установке NGFW Novum и объединяет пользователей, подключившихся через Device VPN. Имя пользователя группы импортируется из поля `Common Name` пользовательского сертификата.

Во вкладку **Локальные** попадают пользователи внешних каталогов:

- Импортированные из ALD.
- Импортированные из FreeIPA.
- Пользователи RADIUS, подключившиеся к NGFW Novum, если настроена авторизация через RADIUS.

В Ideco NGFW Novum реализован принцип наследования, который позволяет задавать и изменять общие параметры для всех локальных пользователей группы через родительскую группу.

Все локальные пользователи Ideco NGFW Novum по умолчанию входят в группу **Все локальные**.

Цвет пиктограммы пользователя зависит от состояния учетной записи пользователя:

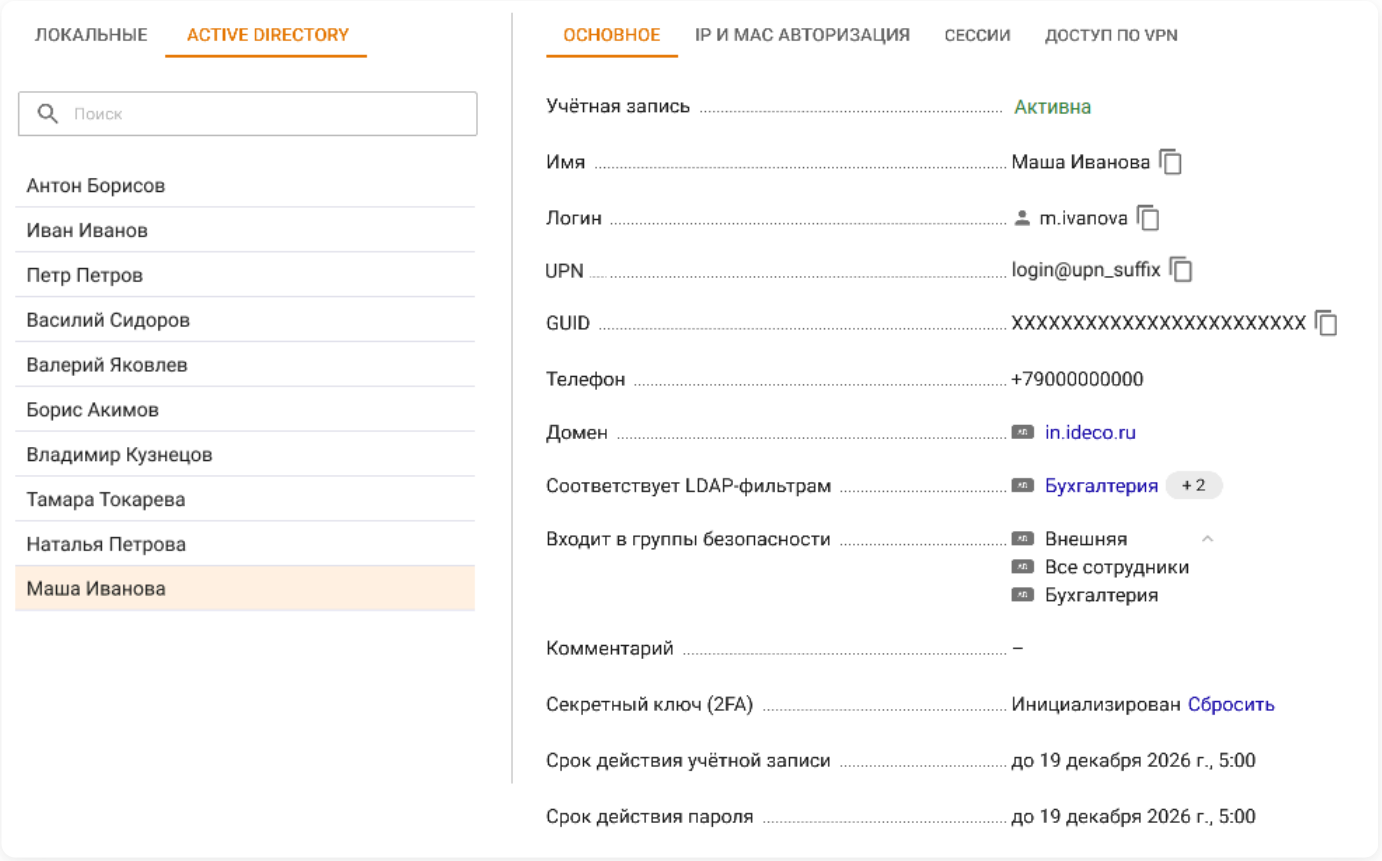
Состояние учетной записи пользователя	Описание
	Пользователь прошел процедуру авторизации, и ему был предоставлен доступ в интернет
	В настройках пользователей выбран запрет на авторизацию
	Пользователь не прошел процедуру авторизации, и ему не был предоставлен доступ в интернет

Элементы управления в дереве пользователей:

Обозначение	Описание
	Создать учетную запись пользователя
	Создать группу
	Удалить учетную запись пользователя или группу

Пользователи внешних каталогов Active Directory

Пользователи внешних каталогов AD отображаются на вкладке **Учетные записи** → **Active Directory**, если настроена интеграция с AD. Данные о пользователе загружаются с контроллеров домена AD:



Расшифровка полей

- **Учетная запись** - Активна/Заблокирована.
- **Имя** - имя пользователя в AD.
- **Логин** - логин пользователя в AD.
- **UPN** - UPN-суффикс пользователя. Можно скопировать в буфер обмена вместе с логином.
- **GUID** - уникальный идентификатор учетной записи.
- **Телефон** - номер телефона, если имеется.
- **Домен** - каталог, к которому принадлежит учетная запись. При нажатии откроется интеграция в разделе **Внешние каталоги** → **Active Directory/Samba DC**.
- **Соответствует LDAP-фильтрам** - список LDAP-фильтров, которым соответствует запись. При нажатии откроется соответствующий фильтр в разделе **Внешние каталоги** → **LDAP-фильтры**. Если запись не соответствует фильтрам, значение будет `Нет`. Если соответствие неизвестно, значение будет `-`.
- **Входит в группы безопасности** - группы безопасности на сервере, в которые входит учетная запись. Если запись не соответствует группам безопасности, значение будет `Нет`. Если соответствие неизвестно, значение будет `-`.
- **Комментарий** - описание (description) пользователя в AD.
- **Секретный ключ (2FA)** - статус TOTP-токена для двухфакторной аутентификации. Чтобы сбросить секретный ключ, нажмите **Сбросить**.

Для принудительного обновления информации о пользователе доступна кнопка **Обновить**. Полученная информация кешируется.

Управление учетными записями и группами

Классический контекст | Высокопроизводительный контекст

В статье описаны создание, удаление и перемещение учетных записей локальных пользователей.

Создание учетной записи пользователя

Не используйте в качестве логина пользователя IP-адрес, так как возникнет ошибка при подключении по IKEv2.

Способы создания учетной записи пользователя и группы:

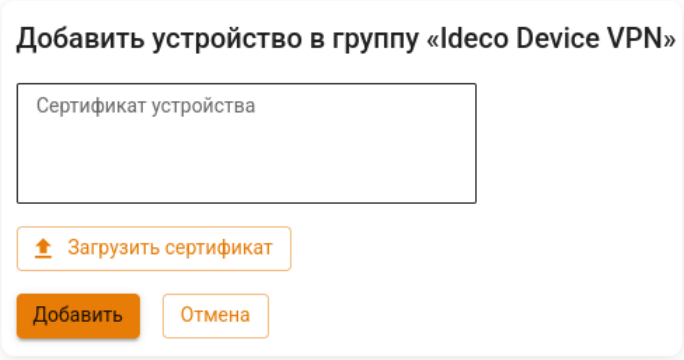
Ideco Device VPN

В группе Ideco Device VPN создаются пользователи Device VPN и терминальные серверы. Для создания пользователя через пользовательский сертификат:

1. Нажмите напротив группы **Ideco Device VPN**:



2. Нажмите **Загрузить сертификат** и выберите сохраненный файл сертификата. Нажмите **Добавить**:



Про создание сертификата для Device VPN смотрите статью.

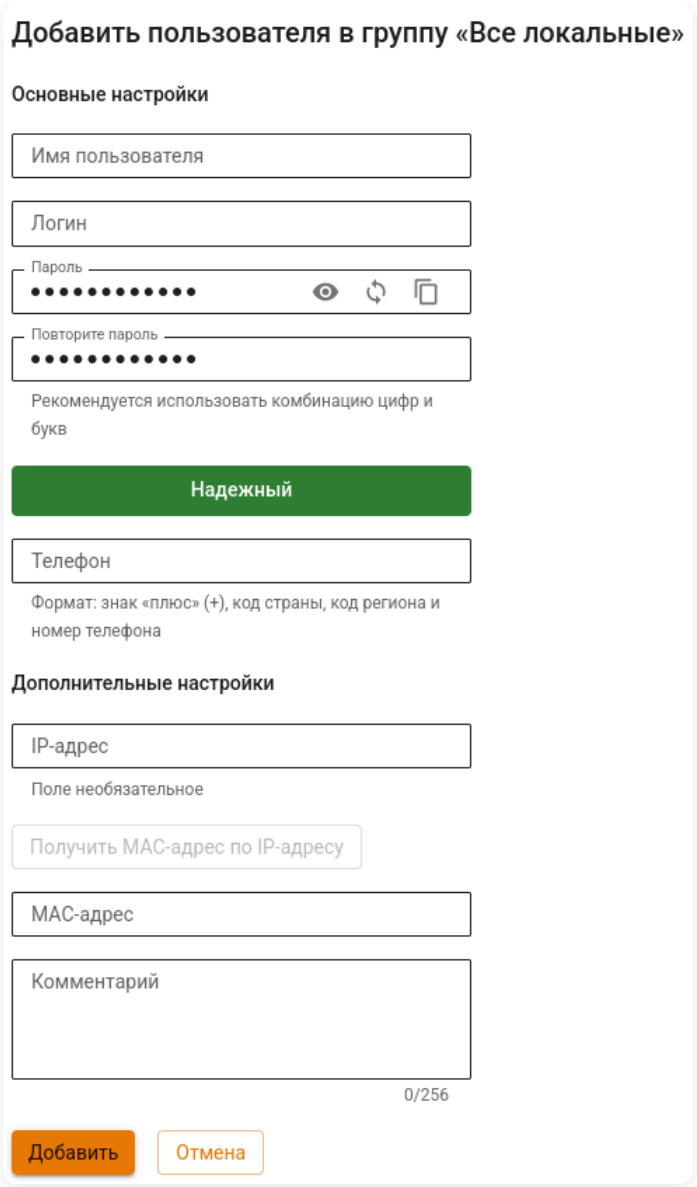
В группе Ideco Device VPN появится пользователь с именем из поля `Common name` пользовательского сертификата.

Группа Все локальные

1. Выберите группу **Все локальные** в дереве пользователей.

2. Нажмите .

3. Заполните поля:



- **Имя пользователя** - введите имя пользователя. Максимальное количество символов - 128.
- **Логин** - введите логин латинскими символами в нижнем регистре. Применяется для авторизации в службах Ideco NGFW Novum. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - введите пароль. Смотрите рекомендации к созданию паролей ниже.
- **Телефон** - телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона.
- **IP-адрес** и **MAC-адрес** - при заполнении этих полей создается правило авторизации в **Пользователи** → **Авторизации** → **IP и MAC** Ideco NGFW Novum.

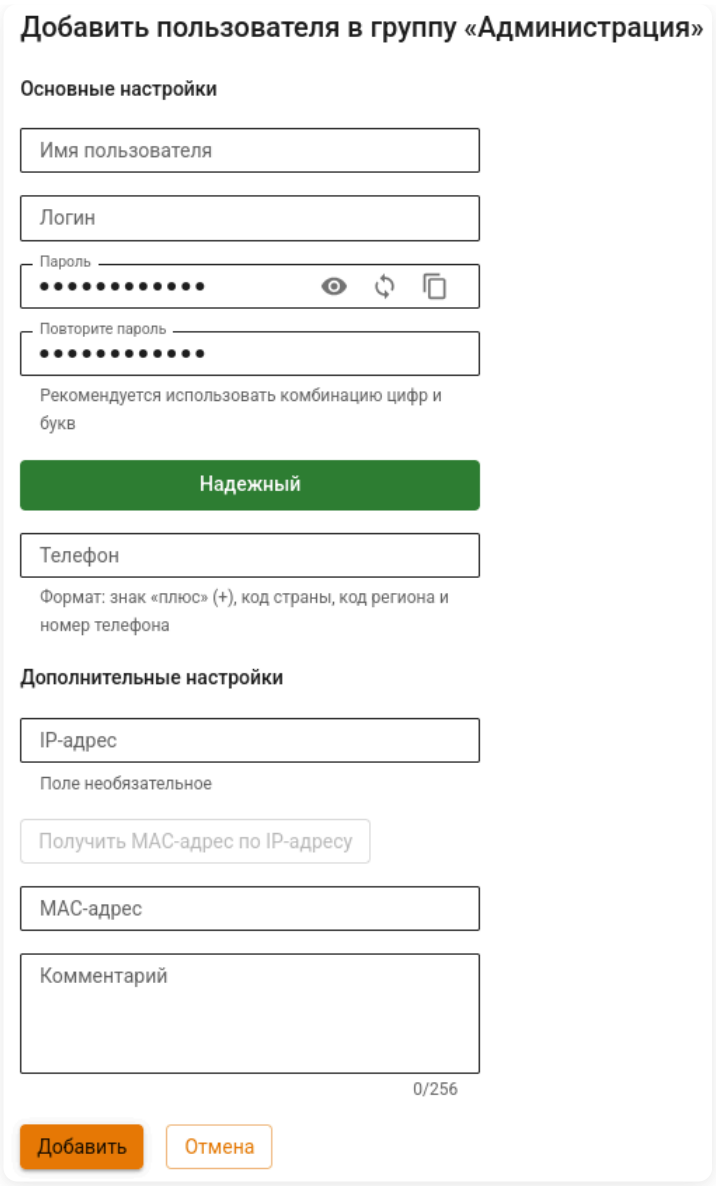
4. Нажмите **Добавить**.

Вложенные группы

1. Выберите группу, в которую добавится пользователь.

2. Нажмите **Создать пользователя** на вкладке **Основное** или рядом с названием группы в дереве.

3. Заполните поля:



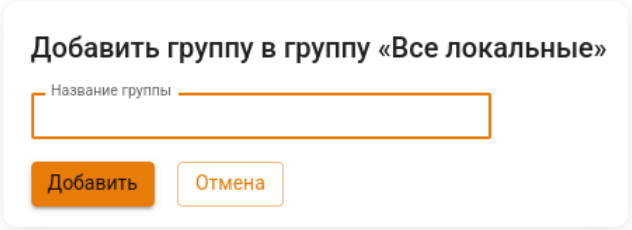
- **Имя пользователя** - введите имя пользователя. Максимальное количество символов - 128.
- **Логин** - введите логин латинскими символами в нижнем регистре. Применяется для авторизации в службах Ideco NGFW Novum. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - введите пароль. Смотрите рекомендации к созданию паролей ниже.
- **Телефон** - введите телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона.
- **IP-адрес** и **MAC-адрес** - при заполнении этих полей создается правило авторизации в **Пользователи** → **Авторизации** → **IP и MAC** Ideco NGFW Novum.

4. Нажмите **Добавить**.

Создание группы

1. Нажмите справа от названия группы.

2. Укажите название и нажмите **Добавить**:



Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;` , `^[[4~;` и т.д.

Посмотреть или восстановить пароль учетной записи пользователя нельзя. Возможна только смена пароля.

Для учетных записей пользователей Active Directory, ALD Pro и RADIUS проверка пароля осуществляется средствами соответствующего каталога или RADIUS-сервера.

Рекомендации к созданию паролей

Доступна автоматическая генерация пароля.

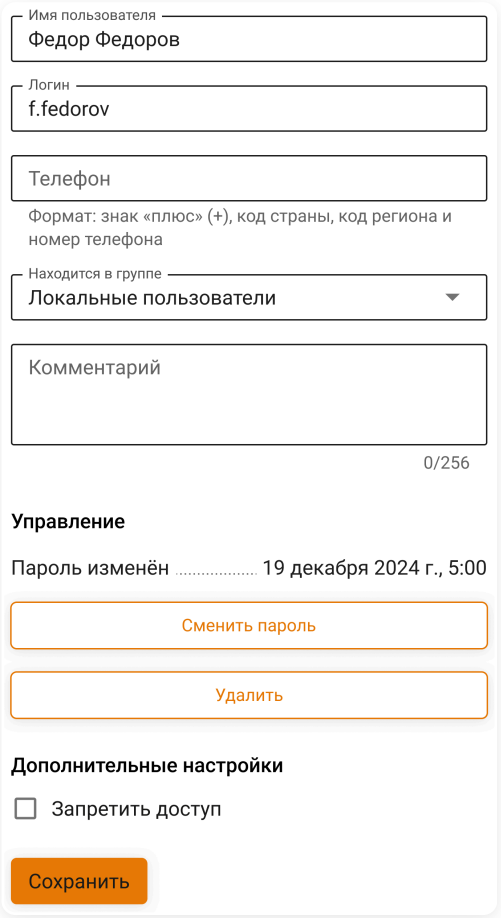
- Минимальная длина - 12 символов.
- Использование строчных и заглавных латинских символов.
- Использование цифр и специальных символов.

Управление пользователями Active Directory (добавление, редактирование или удаление) выполняется на контроллере домена в дереве пользователей.

Удаление учетной записи пользователя или группы

Реализовано два варианта удаления:

- Наведите курсор на пользователя или группу и нажмите на .
- Нажмите на **Удалить** на вкладке **Основное**:



Перемещение учетной записи пользователя

1. Выберите учетную запись или группу.

2. На вкладке **Основное** в поле **Находится в группе** выберите новую группу и нажмите на **Сохранить**.

Редактирование учетной записи пользователя

Редактирование логина и пароля возможно на вкладке **Основное** в разделе **Пользователи** → **Учетные записи** при выделении нужного пользователя.

Полезные ссылки

- **Как безопасно подключить удаленного подрядчика**

Настройка пользователей

Классический контекст | Высокопроизводительный контекст

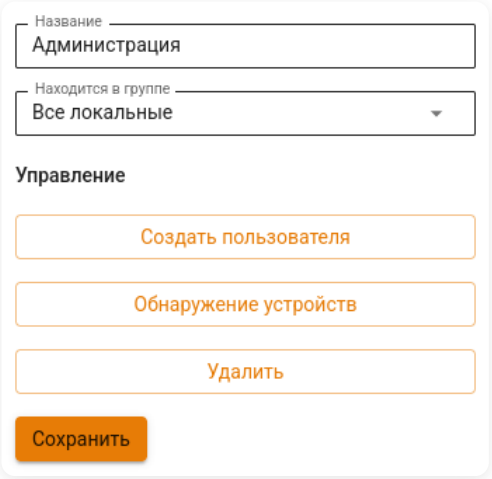
Чтобы изменить параметры учетной записи локального пользователя или группы пользователей, выберите нужный объект в дереве пользователей.

Группы пользователей

В группы можно добавлять как отдельные учетные записи пользователей, так и другие группы, объединяя их вместе. Правила, заданные для группы, автоматически применяются ко всем участникам группы.

Основное

Выберите группу локальных пользователей для редактирования:



- **Название** - введите новое название.
- **Находится в группе** - укажите группу, в которую требуется переместить эту группу.
- **Создать пользователя** - нажмите для создания пользователя в группе.
- **Обнаружение устройств** - нажмите для открытия раздела Обнаружение устройств.
- **Удалить** - нажмите для удаления группы. Вместе с группой удаляются учетные записи пользователей группы.

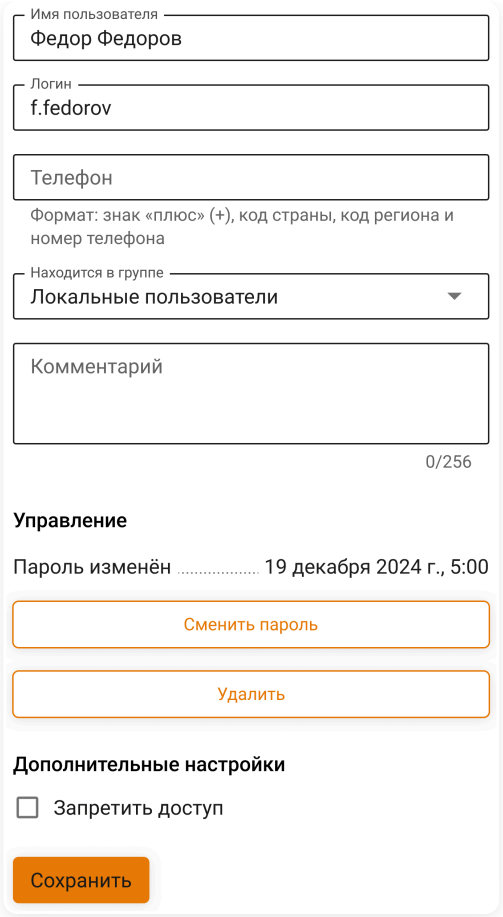
ALD Pro

Категория содержит информацию об имени домена ALD Pro и типе группы. Процесс настройки синхронизации с ALD Pro и импорт пользователей описан в статье Интеграция с ALD Pro.

УЗ локальных пользователей

Основное

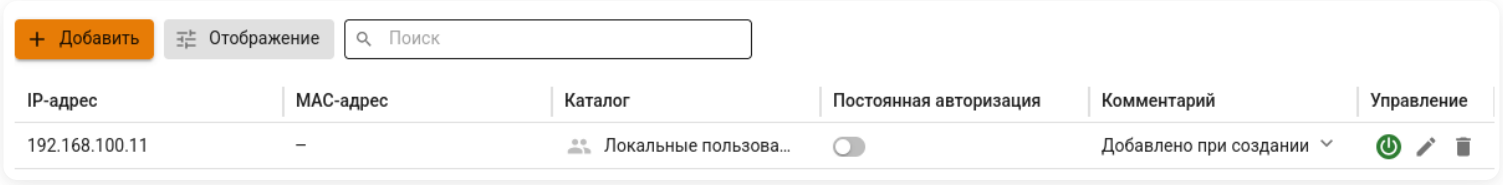
Основные настройки включают параметры, определяющие статус локального пользователя:



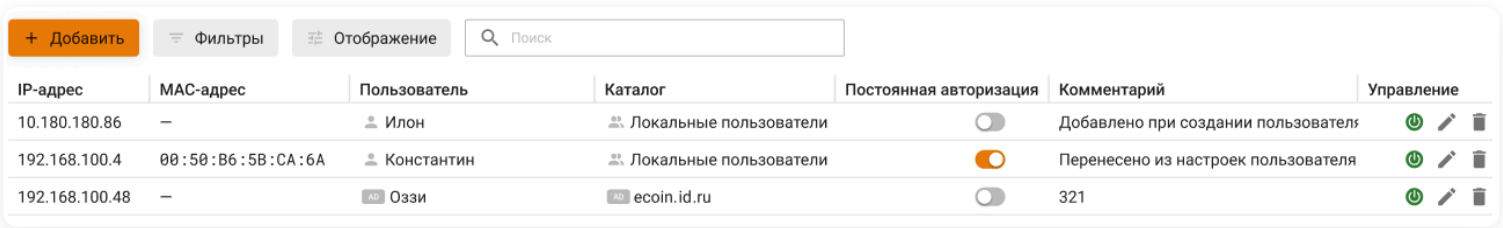
- **Имя пользователя** - введите имя пользователя. Максимальное количество символов - 128.
- **Логин** - введите логин латинскими символами в нижнем регистре. Применяется для авторизации в службах Ideco NGFW Novum. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Телефон** - введите телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона.
- **Находится в группе** - используйте это поле для перемещения пользователя в другую группу.
- **Комментарий** - введите описание пользователя. Необязательное поле.
- **Запретить доступ** - включите опцию, если нужно запретить пользователю авторизацию. Доступ будет закрыт к ресурсам интернета, почте и личному кабинету.

IP и MAC авторизация

На вкладке можно создать правила авторизации по IP и MAC для определенного пользователя:



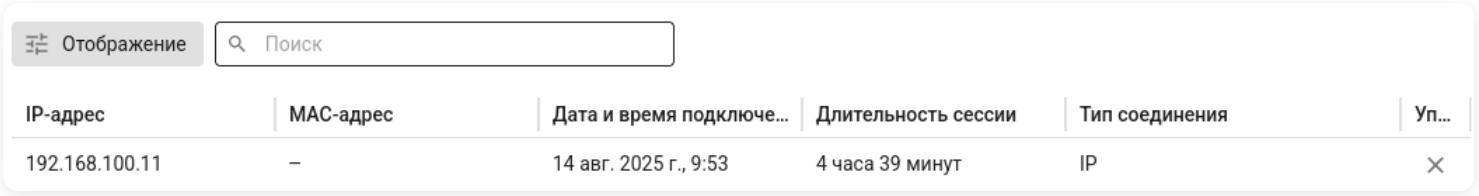
Также создать правила авторизации по IP и MAC для пользователя можно в **Пользователи** → **Авторизация** → **IP и MAC**:



Правила **IP и MAC авторизации** создают аналогичную привязку в DHCP-сервере Ideco NGFW Novum. Однако, если те же адреса указаны во включенных правилах DHCP-сервера, то правила DHCP-сервера будут выполняться в первую очередь.

Сессии

Содержит таблицу с информацией обо всех активных сессиях пользователя:

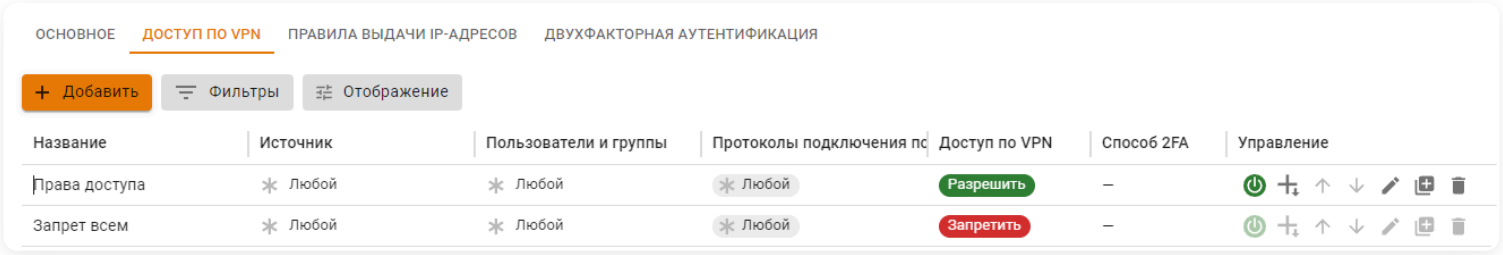


При нажатии на ✕ в столбце **Управление** NGFW разорвет сессию пользователя.

Аналогичная таблица расположена в разделе **Мониторинг** → **Сессии пользователей**.

Доступ по VPN

Категория позволяет просматривать правила доступа VPN, которые настраиваются в **VPN-подключения** → **Доступ по VPN**.



Для перехода к общей таблице доступа VPN из дерева пользователей нажмите на нужное название правила:

Привязанные устройства

Вкладка отображает устройство, привязанное к учетной записи пользователя при подключении через Ideco Client. К одному пользователю может быть привязано только одно устройство:

При отсутствии привязки таблица будет пустой - запись появляется автоматически после первой авторизации пользователя через Ideco Client при включенной опции **Привязать устройство к пользователю** в **Пользователи** → **Ideco Client** → **Основное** или в **Пользователи** → **VPN-подключения** → **Доступ по VPN**.

Для удаления привязки нажмите в колонке **Управление**. После удаления новая привязка будет создана автоматически при следующем подключении пользователя.

Внешние каталоги

Классический контекст | Высокопроизводительный контекст

В Ideco NGFW Novum реализована интеграция с Active Directory (AD), ALD Pro и RADIUS-сервером для получения данных о пользователях, авторизации и управления доступом.

С каталогами AD и ALD Pro выполняется периодическая синхронизация по информации о пользователях:

- AD:
  - Синхронизация списка групп безопасности AD и участия авторизованных пользователей в этих группах - раз в 5 минут.
  - Синхронизация участия авторизованных пользователей в LDAP-фильтрах - раз в 5 минут.
  - Синхронизация списка пользователей с контроллером домена - раз в 15 минут.
  - Проверка на контроллере домена наличия, включенности и соответствия логинов авторизованных пользователей - раз в 15 минут.
- ALD Pro:
  - Синхронизация импорта в дерево пользователей - раз в 15 минут.
  - Синхронизация списка групп пользователей ALD и участия пользователей в этих группах - раз в 5 минут.

Раздел включает пять вкладок:

- **Microsoft Active Directory/Samba DC** - интеграция с Microsoft Active Directory/Samba DC.
- **ALD Pro** - интеграция с ALD Pro.
- **FreeIPA** - интеграция с FreeIPA.
- **RADIUS** - интеграция с RADIUS-сервером (Remote Authentication Dial-In User Service).
- **LDAP-фильтры** - настройка объектов для группировки пользователей каталога AD LDAP (Lightweight Directory Access Protocol).

Active Directory/Samba DC

Классический контекст | Высокопроизводительный контекст | API

Настройка односторонней синхронизации с контроллером домена на базе Microsoft Active Directory (AD) и Samba DC.

Название службы раздела **Active Directory/Samba DC**: `ideco-ad-backend`, `ideco-ad-log-collector`.

Список служб для других разделов доступен по ссылке.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Видеоинструкция актуальна для версий до 20 включительно. С версии 21 не актуален раздел об импорте пользователей.

При интеграции в разделе **Пользователи → Учетные записи → Active Directory** отобразятся данные пользователей AD, исключая пароли. Аутентификация пользователей проверяется средствами Active Directory/Samba DC.

Поддерживаемые контроллеры домена:

- Windows Server 2008 (только R2), 2012, 2016, 2019, 2022, 2025.
- Samba DC с версии 4.0.
- RED ADM / РЕД АДМ 1.10.0.

Для ввода в домен на базе Windows Server 2025 и старше откройте Ideco NGFW Novum, перейдите в раздел **Управление сервером → Терминал** и выполните команду:

```
touch /run/ideco-ad-backend/ldap-passwd
```

Особенности интеграции с несколькими доменами

- Учетные записи пользователей из разных доменов могут иметь одинаковые логины. При аутентификации пользователь будет точно определен по указанному домену. Если домен не был указан пользователем, будет указан каталог по умолчанию.
- Пользователи всех интеграций отображаются в разделе **Пользователи → Учетные записи → Active Directory** в одном списке.
- Пользователи и группы безопасности будут видны и доступны к выбору в правилах трафика, настройках и поиске информации о пользователях AD, со всех интегрированных доменов. При наведении курсора на пользователя или группу безопасности AD выводится информация о принадлежности пользователя домену. Список обновляется каждые 15 минут.

- При SSO-авторизации и первом открытии браузера пользователю будет предложен выбор домена для аутентификации. Выбор сохраняется с помощью cookie и используется при следующей авторизации. Если требуется изменить домен, очистите cookie (для локального IP-адреса NGFW Novum).

Ввод сервера в домен

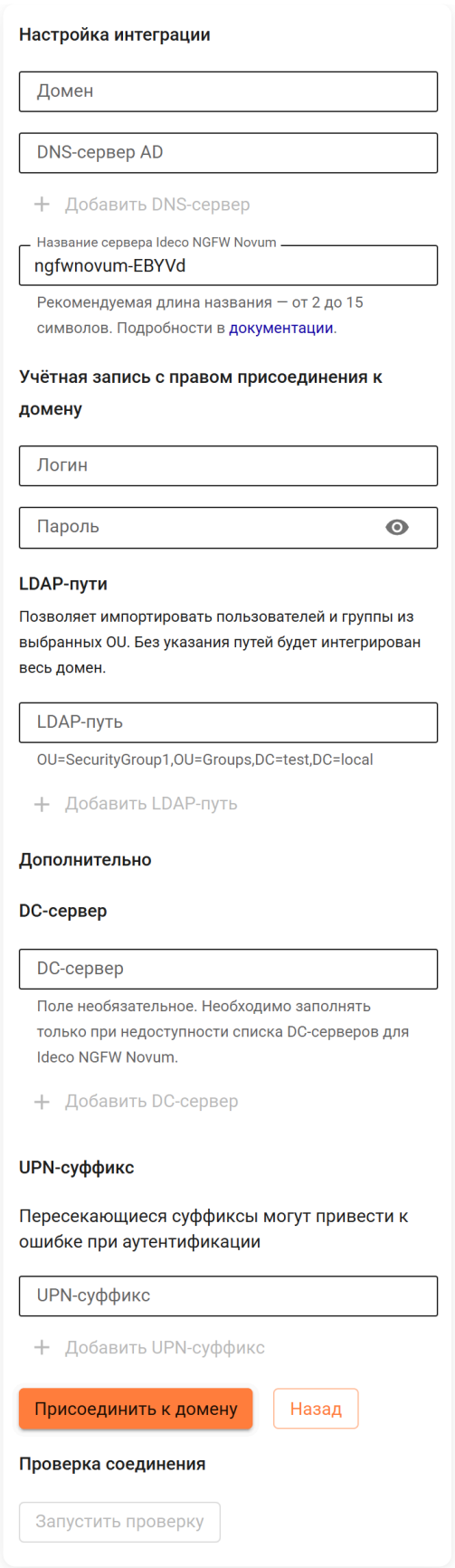
Перед вводом в домен:

- Убедитесь, что время на контроллере домена и NGFW Novum совпадает.
- Убедитесь, что хотя бы один контроллер домена находится в локальной сети NGFW Novum или доступен через локальный интерфейс с помощью настроенной маршрутизации.

Выполните действия:

1. Перейдите в **Пользователи** → **Внешние каталоги** → **Active Directory/Samba DC**.

2. Нажмите **Добавить** и заполните поля:



Если в поле **Название сервера Ideco NGFW Novum** указано более 15 символов, будут недоступны виды аутентификации пользователей AD:

- **SSO через AD и ALD Pro** с токенами NTLM.
- VPN (IKEv2, SSTP, L2TP/IPsec).
- Ideco Client с аутентификаций по логину и паролю.

NetBIOS-имя сервера ограничено 15 символами. При превышении длины название усекается, что вызывает несоответствия при аутентификации, в том числе ошибки SSO из-за некорректного SPN (Service Principal Name).

Расшифровка полей

- **Домен** - полное наименование домена, максимальная длина 64 символа. Например: `mydomain.example`.
- **DNS-сервер AD** - адрес сервера, обладающий ролью DNS-сервера в контроллере домена. Должен быть доступен с любого интерфейса NGFW Novum.
- **Название сервера Ideco NGFW Novum** - имя компьютера, под которым NGFW Novum будет введен в домен. Не более 15 символов.
- **Учетная запись с правом присоединения к домену** - учетная запись AD с правами присоединения к домену (право **Создание объектов: Компьютер**).При заполнении поля домен указывать не требуется. Логин и пароль этой учетной записи используются однократно только для ввода в домен и не сохраняются в Ideco NGFW Novum. После успешного присоединения можно отозвать права, удалить учетную запись или сменить пароль - это не повлияет на дальнейшую работу интеграции.

Чтение домена осуществляется учетной записью типа **Компьютер**. Не удаляйте и не ограничивайте права ни этой учетной записи, ни группе **Доменные компьютеры**. Подробности о необходимых правах для Active Directory можно найти в статье.

- **LDAP-пути** - LDAP-пути для выбора пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет избежать синхронизации с NGFW Novum всего дерева пользователей AD и выбрать только нужные группы.
- **DC-сервер** - контроллер домена. Указывается при недоступности контроллера домена для NGFW Novum или при использовании распределенной корпоративной сети. Можно ввести до 30 DC-серверов.
- **UPN-суффикс** - альтернативные суффиксы `userPrincipalName`. При необходимости можно ввести до 64 UPN-суффиксов. Необходимо указать UPN-суффиксы, если они используются на контроллере домена:

Один и тот же пользователь может войти в NGFW Novum, используя как `sAMAccountName` (SAM), так и дополнительный UPN-суффикс, если он выбран в поле **Имя входа пользователя**:

Указанные UPN-суффиксы отображаются в таблице **Алгоритм аутентификации** в разделе Аутентификация.
3. Нажмите **Присоединить к домену**. Процесс присоединения к домену может занять до одной минуты.

Если в таблице большое количество интеграций, воспользуйтесь кнопкой **Фильтры**.

Алгоритм выбора контроллера домена

Если поле **DC-сервер** не заполнено, NGFW Novum выбирает контроллер домена автоматически:

1. NGFW Novum выполняет DNS-запрос к SRV-записи `_ldap._tcp.<имя домена>` - в ответ возвращается список доступных контроллеров домена.

2. NGFW Novum последовательно проверяет контроллеры домена в случайном порядке на доступность и использует первый ответивший.

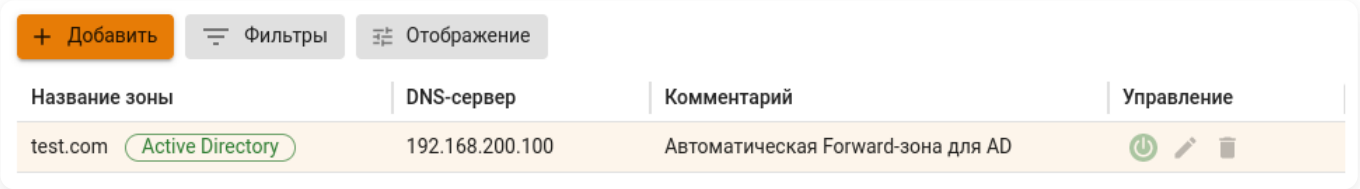
Если в поле **DC-сервер** указаны контроллеры домена, NGFW Novum последовательно проверяет доступность каждого из них и при отсутствии ответа переходит к следующему.

При потере связи с текущим контроллером домена NGFW Novum выполняет новый выбор контроллера в соответствии с алгоритмом.

При использовании распределенной корпоративной сети указывайте контроллеры домена в поле **DC-сервер**, чтобы обеспечить подключение **только к нужным контроллерам** домена.

Настройка DNS для разрешения имен локального домена

В Ideco NGFW Novum Forward-зона DNS создается в **Сервисы** → **DNS** автоматически при вводе сервера в домен:



При настройке компьютеры могут использовать NGFW Novum в качестве основного DNS-сервера. При этом разрешение локальных и интернет-имен будет работать корректно для всех сервисов.

Пользовательские Forward-зоны DNS всегда имеют приоритет над автоматически созданной Forward-зоной для Active Directory.

Удаление интеграции с Active Directory

Для вывода NGFW Novum из домена перейдите в **Пользователи** → **Внешние каталоги** → **Active Directory/Samba DC** и нажмите напротив интеграции. После подтверждения:

- NGFW Novum будет выведен из домена.
- Удалятся все настройки интеграции с контроллером домена.
- Удалятся все пользователи и группы, синхронизированные с доменом.
- В AD созданный для NGFW Novum компьютер не удалится.

После удаления интеграции с Active Directory автоматическая запись в **Сервисы** → **DNS** → **Forward-зоны** должна отсутствовать. Если запись не удалена, обратитесь в Техническую поддержку.

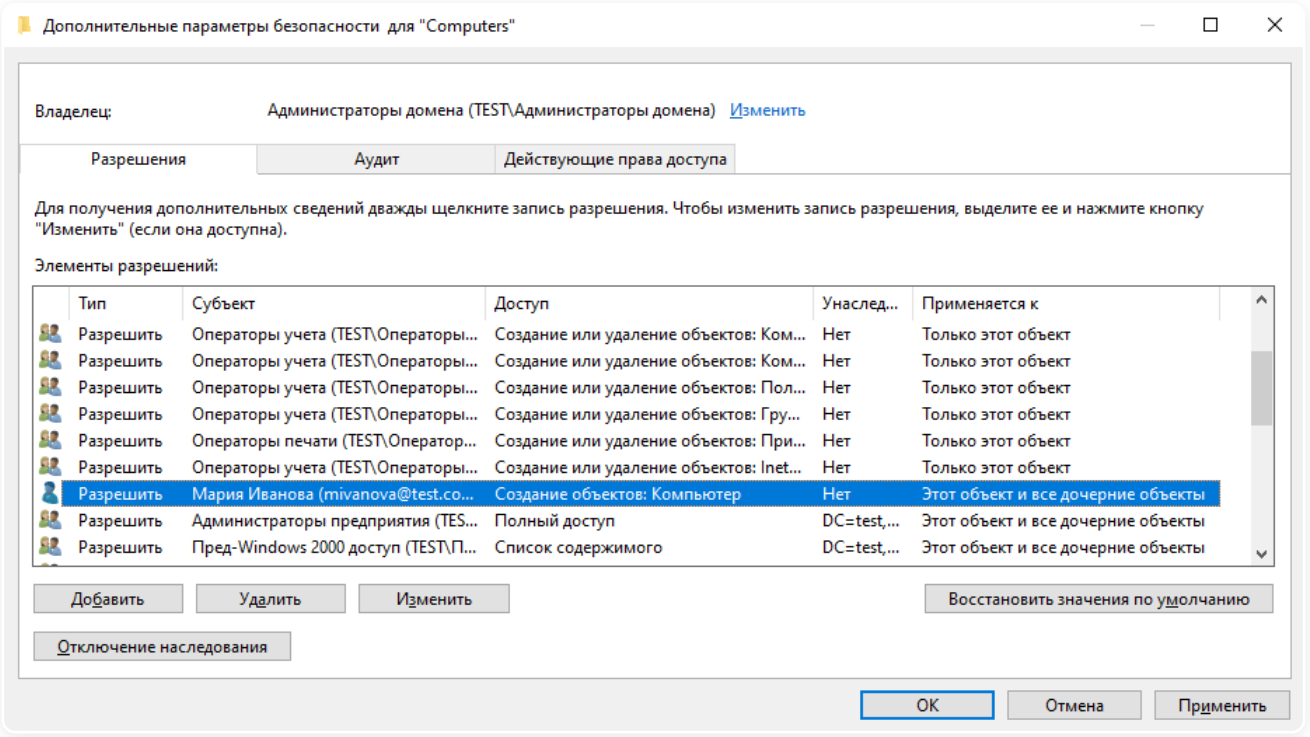
Полезные ссылки

- **Настройка корневого и подчиненного центра сертификации с помощью AD CS**

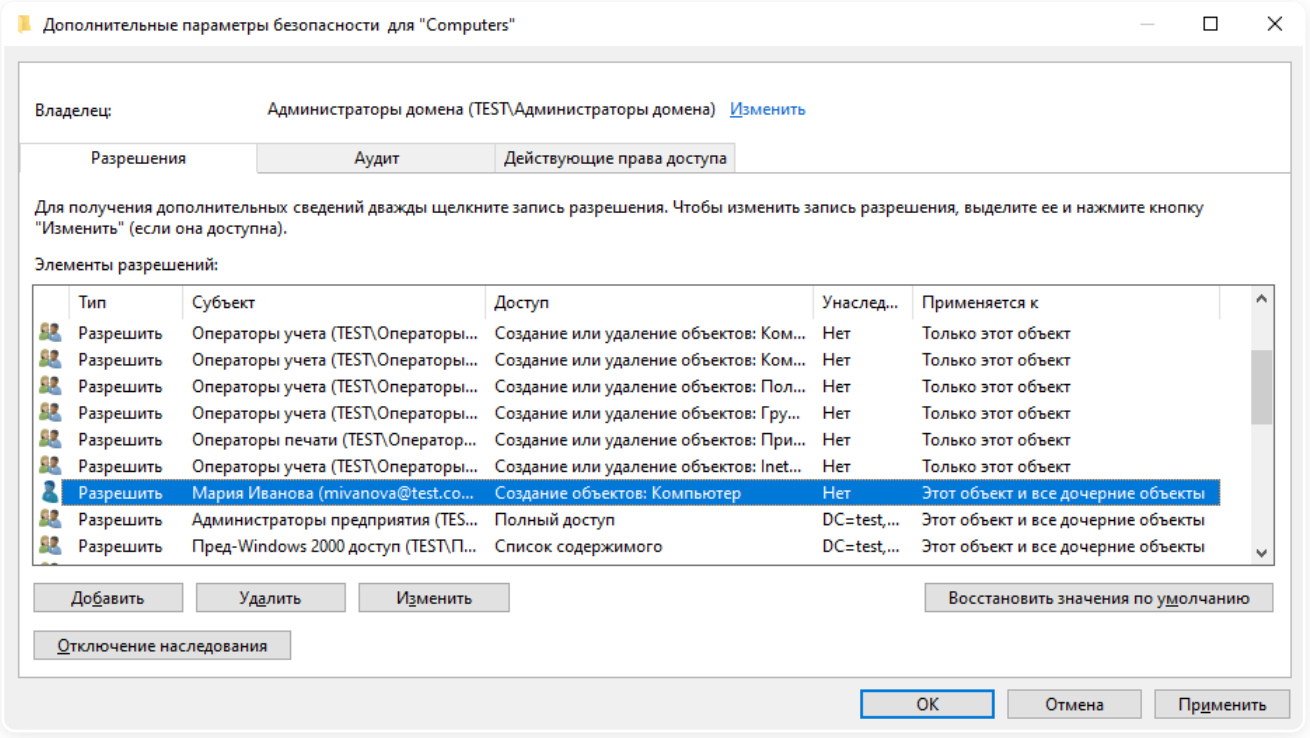
Настройка прав для интеграции Active Directory

Классический контекст | Высокопроизводительный контекст

Для интеграции Ideco NGFW Novum с Active Directory используйте существующую или создайте новую учетную запись с разрешением **Создание объектов: Компьютер**:



Учетная запись используется только при настройке или перенастройке интеграции на NGFW Novum в **Пользователи** → **Active Directory/Samba DC**:



После добавления интеграции на сервере Active Directory будет создана учетная запись компьютера для Ideco NGFW Novum. Она будет использоваться для NGFW Novum в течение всего периода работы и обладает следующими правами:

Область применения	Необходимые права и атрибуты

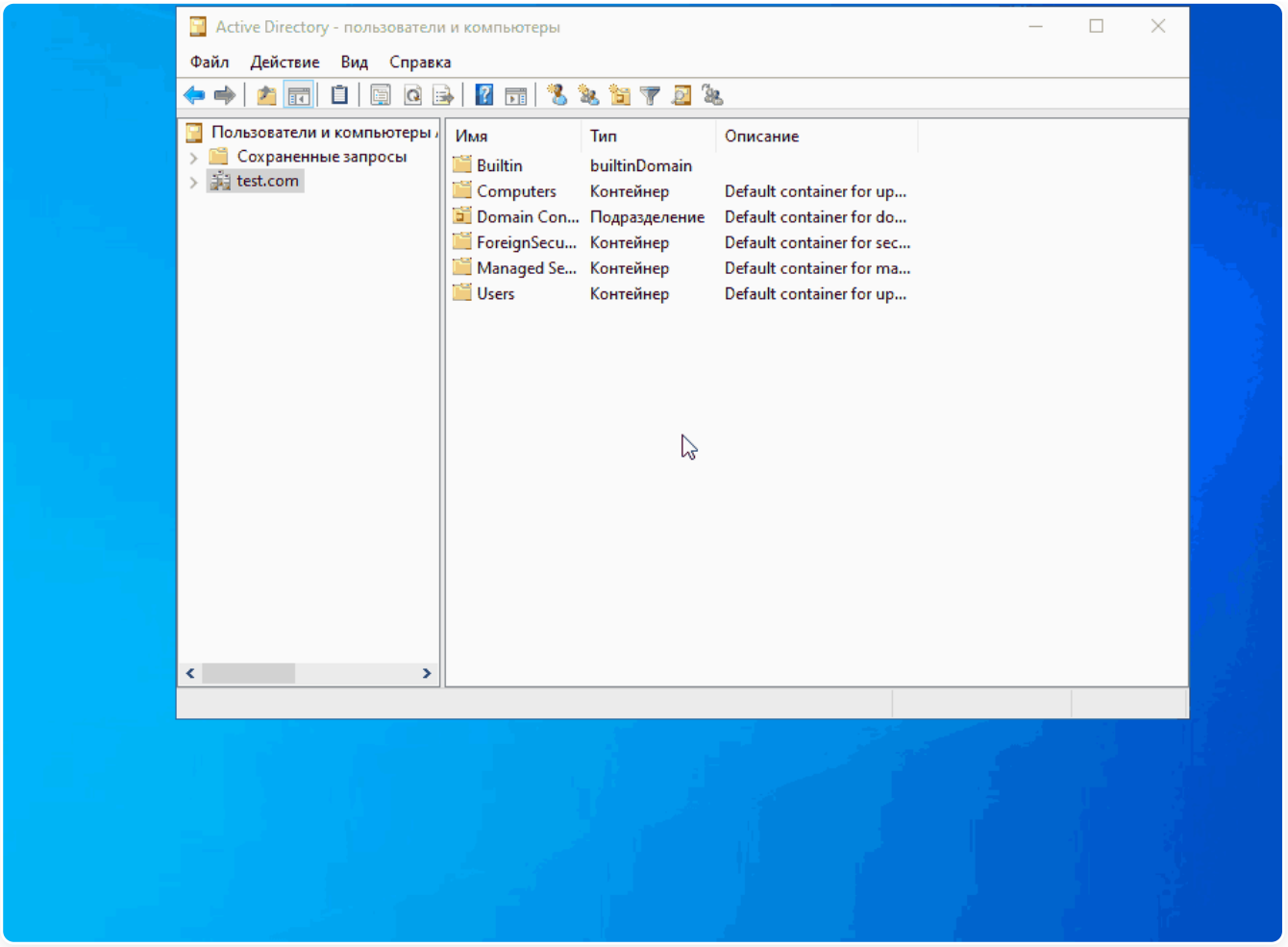
Поиск пользователей	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ name
	  ◦ modifyTimeStamp
	  ◦ objectGUID
	  ◦ objectSid
	  ◦ cn
	  ◦ displayName
	  ◦ login
	  ◦ mobile
	  ◦ objectClass
	  ◦ userAccountControl
	  ◦ sAMAccountName
	  ◦ userPrincipalName
	  ◦ accountExpires
	  ◦ msDS-UserPasswordExpiryTimeComputed
	  ◦ description
	• Предоставляет доступ **ListChildren** просматривать содержимое OU (Organizational Unit).

Поиск групп в OU	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ name
	  ◦ modifyTimeStamp
	  ◦ objectGUID
	  ◦ objectSid
	• Предоставляет доступ **ListChildren** просматривать содержимое OU (Organizational Unit).

Поиск в конфигурации разделов	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ cn (Common Name)
	  ◦ nETBIOSName
	  ◦ nCName
	• Предоставляет доступ к контейнеру **CN=Configuration**.

Проверка текущих прав пользователя через GUI

Откройте **Active Directory Users and Computers** (**Пользователи и Компьютеры Active Directory**) и выполните действия:



1. Включите **View** → **Advanced Features** (**Вид** → **Дополнительные компоненты**).

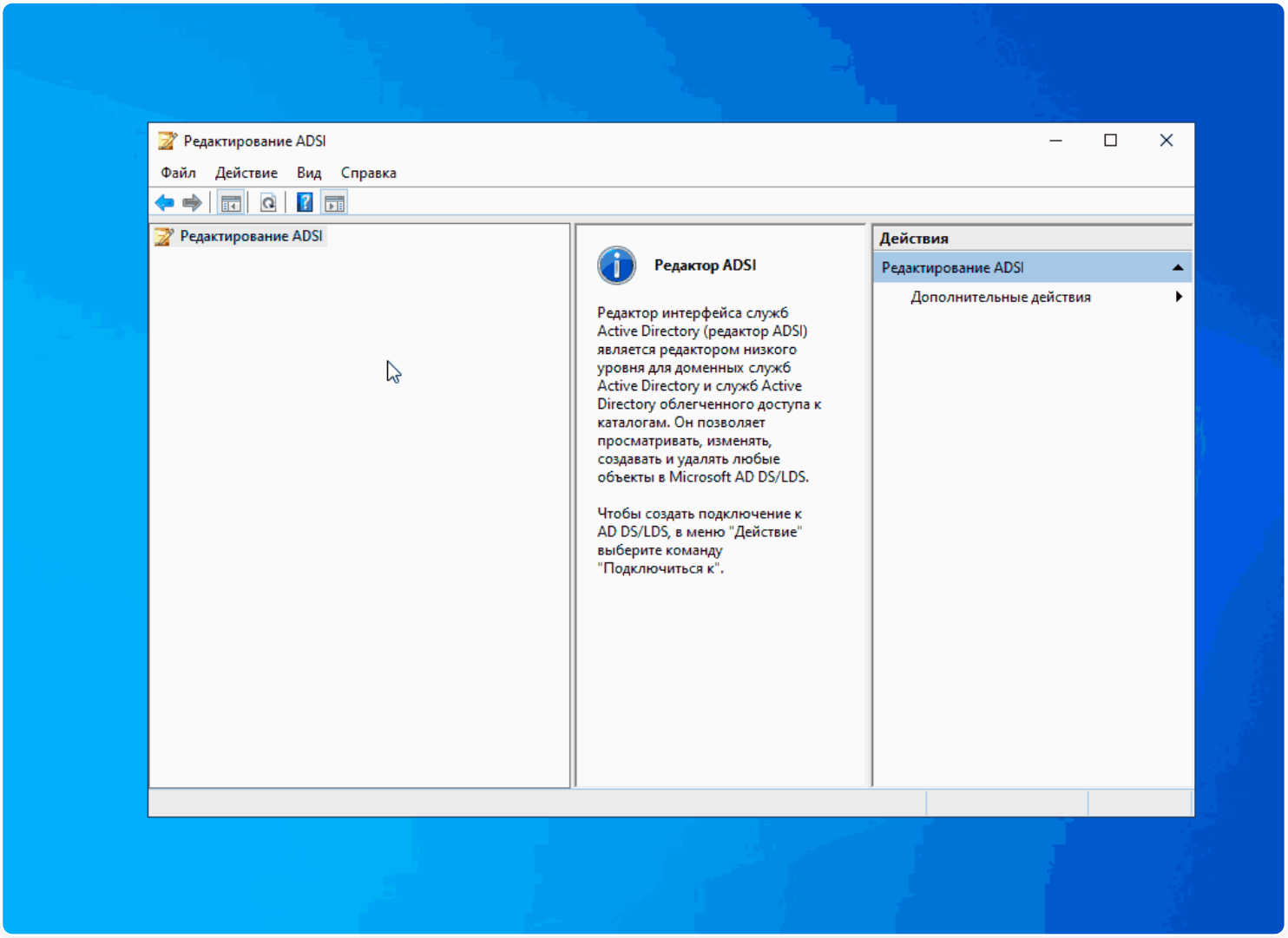
2. Нажмите правой кнопкой на объекте домена, выберите **Properties** → **Security** → **Advanced** (**Свойства** → **Безопасность** → **Дополнительно**).

3. Перейдите на вкладку **Effective Access** (**Действующие права доступа**).

4. Добавьте пользователя/компьютер, чьи права необходимо проверить, и нажмите **View effective access** (**Посмотреть действующие разрешения**).

Проверка прав для конфигурации разделов через GUI

Откройте **ADSI Edit** (**Редактирование ADSI**) командой `adsiedit.msc` в командной строке сервера и выполните действия:



1. Нажмите правой кнопкой на **ADSI Edit** (**Редактирование ADSI**) и выберите **Connect to...** (**Подключиться к...**).

2. Подключитесь к разделу **Configuration** (**Конфигурация**), выбрав **Configuration** (**Конфигурация**) в разделе **Select a well known Naming Context** (**Выберите известный контекст именования**).

3. Перейдите по пути: **CN=Configuration,DC=test1,DC=internal** → **CN=Partitions**.

4. Нажмите правой кнопкой на **CN=Partitions** и выберите **Properties** → **Security** → **Advanced** (**Свойства** → **Безопасность** → **Дополнительно**).

5. Перейдите на вкладку **Effective Access** (**Действующие права доступа**).

6. Добавьте пользователя/компьютер, чьи права необходимо проверить, и нажмите **View effective access** (**Посмотреть действующие разрешения**).

Команды для проверки текущих прав

Через PowerShell

Права для ввода сервера в домен

```
$domain = [ADSI]"LDAP://dc=test1,dc=internal"
$domain.psbase.ObjectSecurity.Access | Format-Table IdentityReference, ActiveDirectoryRights, AccessControlType -AutoSize
```

- `LDAP://dc=test1,dc=internal` - LDAP-путь до корневого домена **test1.internal**.
- `Format-Table IdentityReference, ActiveDirectoryRights, AccessControlType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `AccessControlType` - тип доступа: `allow` (разрешить) или `deny` (запретить).

Поиск пользователей в домене

```
(Get-Acl "AD:\DC=test1,DC=internal").Access |
Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"} |
Format-Table IdentityReference,ActiveDirectoryRights,ObjectType -AutoSize
```

- `AD:\DC=test1,DC=internal` - LDAP-путь до корневого домена **test1.internal**.
- `Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"}` - фильтрация ACL записи, оставляя только те, где **IdentityReference** равен **ngfw-qqtfdk** (имя компьютера, под которым Ideco NGFW Novum будет введен в домен).
- `Format-Table IdentityReference,ActiveDirectoryRights,ObjectType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `ObjectType` - GUID объекта AD, к которому применяются права.

Поиск групп в OU Users и Computers

```
(Get-Acl "AD:\OU=Users,OU=Computers,DC=test1,DC=internal").Access |
Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"} |
Format-Table IdentityReference,ActiveDirectoryRights,ObjectType -AutoSize
```

- `AD:\OU=Users,OU=Computers,DC=test1,DC=internal` - LDAP-путь до организационной единицы **Users**, расположенной внутри **Computers** домена **test1.internal**.
- `Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"}` - фильтрация ACL записи, оставляя только те, где **IdentityReference** равен **ngfw-qqtfdk** (имя компьютера, под которым Ideco NGFW Novum будет введен в домен).
- `Format-Table IdentityReference,ActiveDirectoryRights,ObjectType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `ObjectType` - GUID объекта AD, к которому применяются права.

Поиск в конфигурации разделов

```
(Get-Acl "AD:\CN=Partitions,CN=Configuration,DC=test1,DC=internal").Access |
Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"} |
Format-Table IdentityReference,ActiveDirectoryRights,ObjectType -AutoSize
```

- `AD:\CN=Partitions,CN=Configuration,DC=test1,DC=internal` - LDAP-путь до контейнера **Partitions** в разделе **Configuration** домена **test1.internal**.
- `Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"}` - фильтрация ACL записи, оставляя только те, где **IdentityReference** равен **ngfw-qqtfdk** (имя компьютера, под которым Ideco NGFW Novum будет введен в домен).
- `Format-Table IdentityReference,ActiveDirectoryRights,ObjectType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `ObjectType` - GUID объекта AD, к которому применяются права.

Через Dsacls

Права для ввода сервера в домен и поиск пользователей в домене

```
dsacls "DC=test1,DC=internal"
```

- `DC=test1,DC=internal` - LDAP-путь до корневого домена **test1.internal**.

Поиск групп в OU Users и Computers

```
dsacls "OU=Users,OU=Computers,DC=test1,DC=internal"
```

- `OU=Users,OU=Computers,DC=test1,DC=internal` - LDAP-путь до организационной единицы **Users**, расположенной внутри **Computers** домена **test1.internal**.

Поиск в конфигурации разделов

```
dsacls "CN=Partitions,CN=Configuration,DC=test1,DC=internal"
```

- `CN=Partitions,CN=Configuration,DC=test1,DC=internal` - LDAP-путь до контейнера **Partitions** в разделе **Configuration** домена **test1.internal**.

Аутентификация пользователей AD/Samba DC

Классический контекст | Высокопроизводительный контекст

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE



Видеоинструкция актуальна для всех версий, но с версии 21 потребуется дополнительно настроить **Разрешенные объекты** (см. в этой статье).

Настройка по типам аутентификации пользователей AD/Samba DC описана в статьях:

- **Настройка веб-аутентификации**
- **Настройка SSO-аутентификации**
- **Настройка авторизации через журнал безопасности AD**

Авторизация

Для пользователей Active Directory доступны все типы авторизации. Для пользователей Samba доступны все типы авторизации, кроме авторизации через журнал безопасности.

Чтобы пользователи SambaDC могли использовать VPN-подключение, необходимо включить **NTLM-авторизацию**. Для этого отредактируйте файл с помощью команды `nano /etc/samba/smb.conf`, добавив в секцию `[global]` строку `ntlm auth = yes`.

Способы аутентификации импортированных пользователей:

- **Через Ideco Client** - подходит для SSO-авторизации и для авторизации по логину и паролю из AD. Также используется для авторизации пользователей терминальных серверов Windows.
- **Авторизация по IP-адресу** - подходит для пользователей с фиксированным IP-адресом. IP-адреса на NGFW необходимо прописать вручную каждому пользователю.
- **Авторизация по VPN** - подходит для пользователей удаленных сетей.
- **Авторизация через журналы AD** - прохождение трафика инициирует создание сессии авторизации (так же как IP/MAC).

Особенности авторизации пользователей доверенных доменов

Если у домена, в который введен NGFW Novum, настроено доверие с другим доменом, то пользователи доверенного домена смогут авторизоваться на NGFW Novum при выполнении условий:

- Между доменами настроено доверие Forest - Forest. **Другие типы доверия между доменами не поддерживаются**. Для авторизации пользователей доменов с другим типом доверия необходима настройка интеграции с этими доменами.
- Пользователи доверенного домена могут авторизоваться только с помощью SSO через веб-аутентификацию, другие виды аутентификации и авторизации им недоступны.

- Пользователь доверенного домена должен быть добавлен в AD как ForeignSecurityPrincipal и находиться в локальной группе безопасности, которой разрешена веб-авторизация/аутентификация.

Пользователи доверенного домена отобразятся в разделе **Пользователи** → **Учетные записи** → **Active Directory** наряду с другими пользователями AD.

Полезные ссылки

- **Настройка прав для интеграции Active Directory**
- **Скрипты автоматической разавторизации**

Настройка SSO-аутентификации

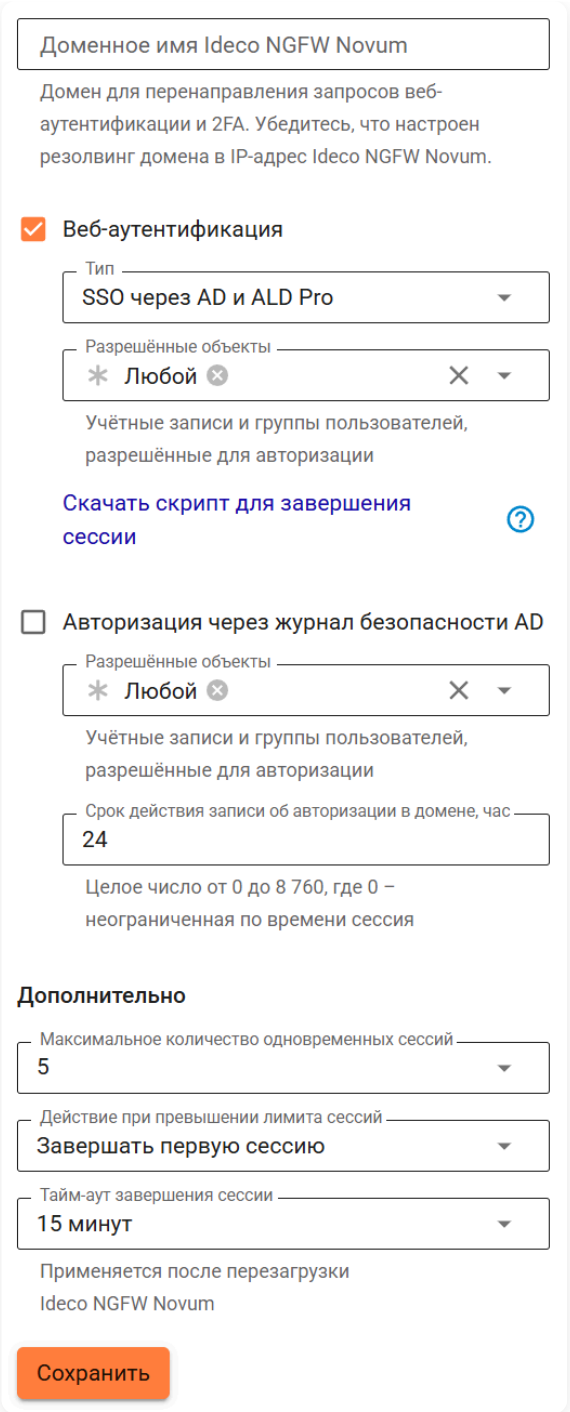
Классический контекст | Высокопроизводительный контекст

Название службы раздела **Веб-аутентификация**: `ideco-web-authd`, `ideco-web-backend`.

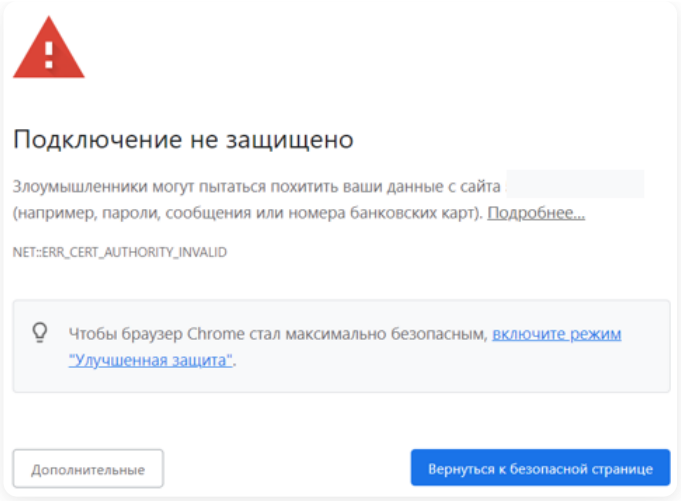
Список служб для других разделов доступен по ссылке.

Настройка SSO-аутентификации на стороне NGFW Novum

Перейдите в **Пользователи** → **Авторизация** → **Настройки** и заполните поля:



- **Доменное имя Ideco NGFW Novum** - укажите доменное имя Ideco NGFW Novum.
- **Веб-аутентификация** - включите настройку и выберите **SSO через AD и ALD Pro** для авторизации с использованием токенов Kerberos или NTLM.
- **Авторизация через журнал безопасности Active Directory** - включите, чтобы Ideco NGFW Novum отслеживал события успешного входа в журнале безопасности AD и авторизовывал пользователя по ним, если трафик идет с того же IP-адреса.
- **Тайм-аут завершения сессии** - установите тайм-аут завершения сессии пользователей. Значение по умолчанию - 15 минут. Диапазон доступных значений - от 10 минут до 1 дня.
  После сохранения настроек будет выдан Let's Encrypt сертификат, пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



Если сертификат для такого домена уже загружен в разделе **Сертификаты**, то будет использоваться загруженный сертификат. Новый сертификат выдаваться не будет.

Выбор каталога при SSO-аутентификации

Каталог для проверки учетных данных выбирается **только среди интеграций с AD и ALD Pro** одним из способов:

- **Неявно** - если настроена только одна интеграция с AD или ALD Pro, она используется автоматически.
- **Явно** - если настроены две или более интеграции, при первом открытии браузера пользователю предлагается выбрать домен для аутентификации. Выбор сохраняется с помощью cookie и используется при последующих авторизациях. Чтобы сменить домен, очистите cookie для локального IP-адреса NGFW Novum.

Каталог выбирается до проверки учетных данных. Если на компьютере не найден SSO-токен и браузер показывает **системное окно ввода логина и пароля** (запрос NTLM), действуют те же правила:

- Учетные данные проверяются **только в уже выбранном каталоге** AD или ALD Pro. Стандартный алгоритм выбора каталога (с **Каталогом по умолчанию** и доменным суффиксом) к этому запросу не применяется.
- В системное окно NTLM можно ввести **только доменную учетную запись** выбранного каталога. Локальная учетная запись не сработает, даже если локальный каталог задан как **Каталог по умолчанию**. Для авторизации локальных пользователей отключите SSO и используйте веб-аутентификацию по логину и паролю - на ее странице доступны локальные и доменные учетные записи.

Пример выбора каталога при двух интеграциях

Настроены две интеграции - домены `example.ru` и `test.ru`. У пользователя `ivanov` есть учетная запись в обоих доменах:

1. Пользователь первый раз открывает браузер и переходит на любой сайт.

2. Ideco NGFW Novum перенаправляет его на страницу выбора домена. Пользователь выбирает `example.ru`.

3. Браузер передает SSO-токен (или, при его отсутствии, запрашивает логин и пароль). Учетные данные проверяются только в каталоге `example.ru`, даже если такой же логин есть в `test.ru`.

4. Выбор `example.ru` сохраняется в cookie. При следующих авторизациях домен не запрашивается. Чтобы авторизоваться в `test.ru`, пользователю нужно очистить cookie для локального IP-адреса NGFW Novum и выбрать другой домен.

Настройка клиентских компьютеров

Настройка зоны интрасети Windows

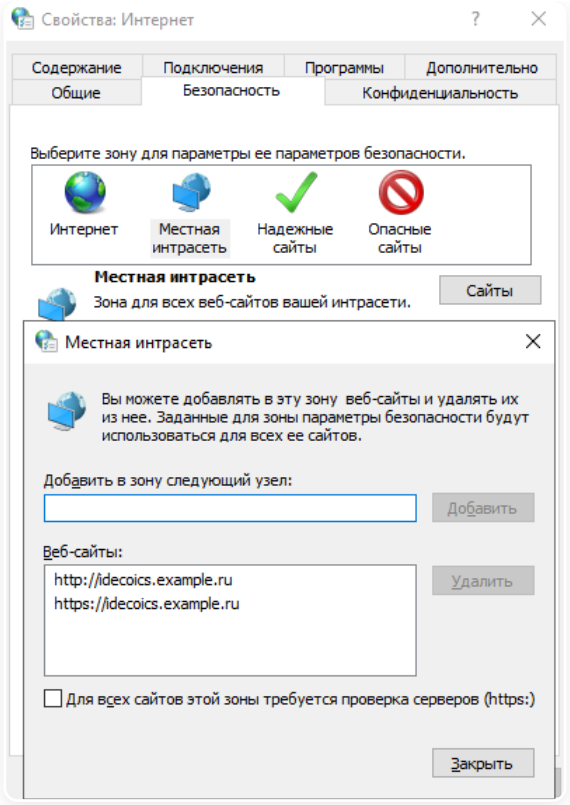
1. В поиск введите **Изменение параметров временных файлов интернета**.

2. В открывшемся окне перейдите на вкладку **Безопасность**.

3. Выберите **Местная интрасеть** → **Сайты**.

4. Добавьте в открывшемся окне ссылку на Ideco NGFW Novum под тем именем, под которым ввели Ideco NGFW Novum в домен. Нужно указывать два URL: с `http://` и с `https://`.

Пример ввода Ideco NGFW Novum в домен `example.ru` под именем `idecoics`:



Настройка браузеров для SSO-аутентификации по протоколам NTLM и Kerberos

В приватных режимах браузеров (**Инкогнито**, **Приватное окно** и аналогичных) SSO-аутентификация по умолчанию не работает: браузеры в таких режимах отключают автоматическую передачу учетных данных по протоколам NTLM и Kerberos. В этом случае пользователю потребуется ввести логин и пароль вручную.

Mozilla Firefox

Порядок настройки

1. В адресной строке Mozilla Firefox введите `about:config` и подтвердите переход.

2. В строке поиска найдите и отредактируйте параметры, установив указанные значения:

Параметр	Значение	Описание
`network.automatic-ntlm-auth.trusted-uris`	Доменное имя Ideco NGFW Novum (например, `idecoics.example.ru`)	Список серверов, для которых разрешена автоматическая NTLM-аутентификация.
`network.negotiate-auth.trusted-uris`	Доменное имя Ideco NGFW Novum (например, `idecoics.example.ru`)	Список серверов, для которых разрешена автоматическая аутентификация Negotiate (Kerberos).
`security.enterprise_roots.enabled`	`true`	Позволяет Mozilla Firefox доверять корневым сертификатам, установленным в операционной системе (необходимо для корректной работы на HTTPS-сайтах).

Важно:

- В значениях необходимо указывать именно доменное имя Ideco NGFW Novum, под которым он доступен в сети (например, `idecoics.example.ru`), а не IP-адрес.
- Доменное имя можно указать с точкой в начале значения, чтобы правило автоматически применялось к домену и всем его поддоменам. Например, `.example.ru` автоматически применит правило к `example.ru` и всем его поддоменам (`sub.example.ru`, `idecoics.example.ru`).
- Если требуется указать несколько адресов, используйте запятую в качестве разделителя.

Как работает аутентификация в Firefox

Mozilla Firefox использует механизм согласования SPNEGO:

1. Браузер пытается выполнить аутентификацию по протоколу Kerberos (более безопасный и быстрый). Аутентификация возможна при условиях:

- Компьютер входит в домен Active Directory.
- Ideco NGFW Novum интегрирован в домен и настроен Service Principal Name (SPN).

2. Если аутентификация по Kerberos невозможна (например, компьютер не в домене или отсутствует билет), браузер автоматически переключается на протокол NTLM.

Для успешной работы обоих механизмов необходимо настроить оба семейства параметров (`negotiate` и `ntlm`). Если настроен только один из протоколов:

- Автоматическая аутентификация будет работать лишь в сценариях, где этот протокол поддерживается и клиентом, и сервером.
- При использовании только Kerberos недоменные компьютеры или машины с проблемами получения билета не смогут авторизоваться.
- При использовании только NTLM в доменной среде не будет задействован Kerberos, хотя аутентификация останется возможной.

Chromium

Порядок настройки

1. Откройте редактор реестра, нажав **Win+R** и введя `regedit`.

2. В редакторе реестра перейдите по одному из путей:

- Для применения ко всем пользователям компьютера - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Chromium`.
- Для применения к текущему пользователю - `HKEY_CURRENT_USER\SOFTWARE\Policies\Chromium`.

Если используется другой браузер, путь может отличаться:

- **Google Chrome** - `...\Policies\Google\Chrome`.
- **Microsoft Edge** - `...\Policies\Microsoft\Edge`.
- **Яндекс Браузер** - `...\Policies\Yandex\Browser`.

3. Создайте новый параметр с типом `REG_SZ`:

Параметр	Значение	Описание
`AuthServerAllowlist`	Доменное имя Ideco NGFW Novum (например, `idecoics.example.ru`)	Список серверов, для которых разрешена автоматическая аутентификация по протоколам NTLM и Kerberos (Negotiate). Если сервер не входит в этот список, браузер будет запрашивать логин и пароль.

Если ранее была выполнена настройка зоны интрасети Windows, параметр `AuthServerAllowlist` подхватывается браузером автоматически. Ручная установка потребуется, если настройка зоны интрасети не применялась.

Важно:

- В значениях необходимо указывать именно доменное имя Ideco NGFW Novum, под которым он доступен в сети (например, `idecoics.example.ru`), а не IP-адрес.
- Доменное имя можно указать с символом `*` в начале значения. Например, `*.example.ru`. Тогда правило будет автоматически применяться к основному домену `example.ru` и ко всем его поддоменам.
- Если требуется указать несколько адресов, используйте запятую в качестве разделителя.

Как работает аутентификация в Chromium

Браузеры Chromium используют механизм согласования SPNEGO:

1. Браузер пытается выполнить аутентификацию по протоколу Kerberos (более безопасный и быстрый). Аутентификация возможна при условиях:

- Компьютер входит в домен Active Directory.
- Ideco NGFW Novum интегрирован в домен и настроен Service Principal Name (SPN).

2. Если аутентификация по Kerberos невозможна (например, компьютер не в домене или отсутствует билет), браузер автоматически переключается на протокол NTLM.

Для успешной работы обоих механизмов необходимо настроить оба семейства параметров (`negotiate` и `ntlm`). Если настроен только один из протоколов:

- Автоматическая аутентификация будет работать лишь в сценариях, где этот протокол поддерживается и клиентом, и сервером.
- При использовании только Kerberos недоменные компьютеры или машины с проблемами получения билета не смогут авторизоваться.
- При использовании только NTLM в доменной среде не будет задействован Kerberos, хотя аутентификация останется возможной.

Настройка на стороне сервера Active Directory

Применение настройки ко всем пользователям Active Directory

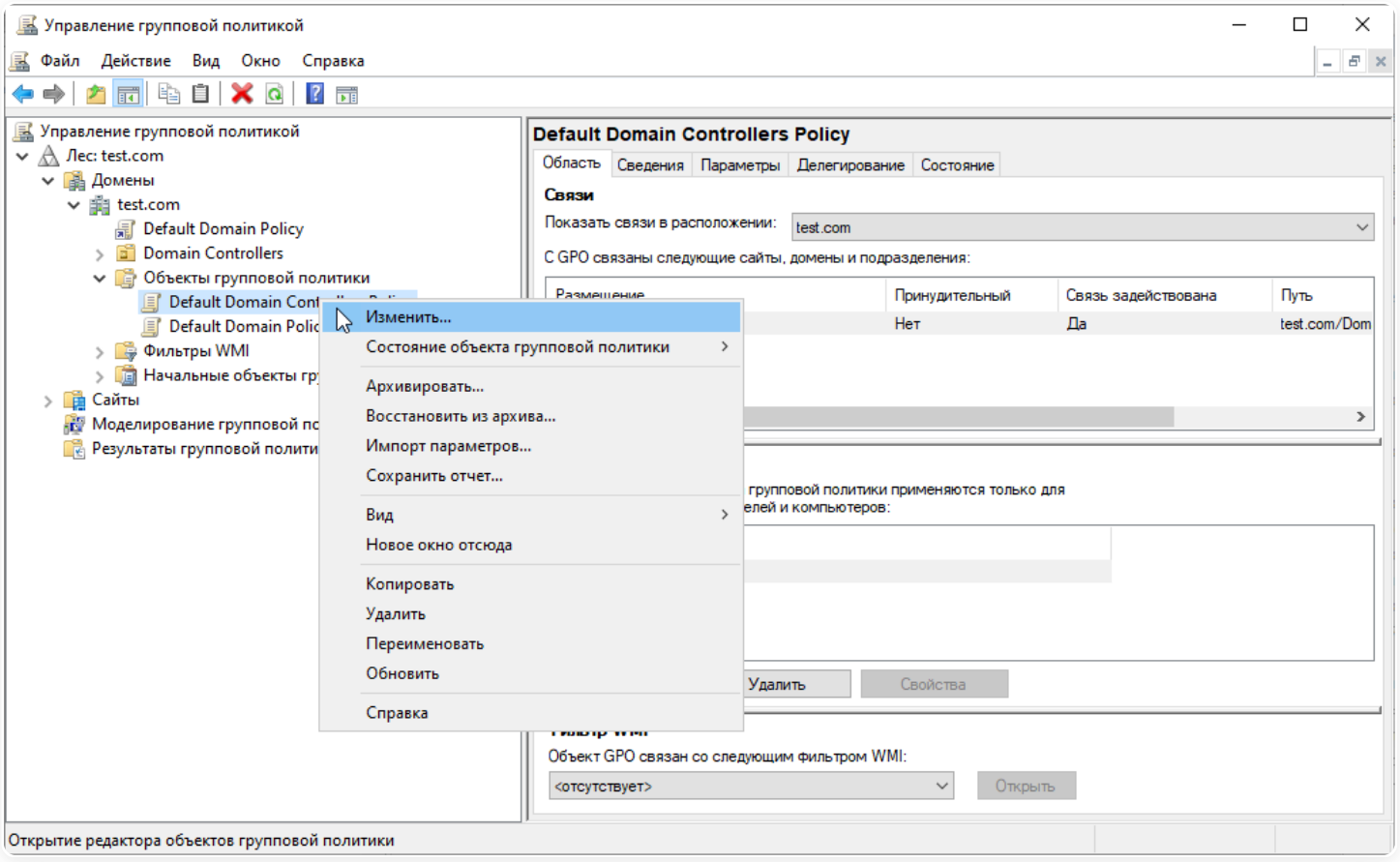
1. Откройте **Управление групповой политикой**. Это можно сделать, нажав клавиши **Win + R** и введя в появившемся окне команду gpmc.msc.

2. Перейдите по пути:

Англоязычная версия

Group Policy Management → Forest → Domains → <ваш домен> → Group Policy Objects.
Русскоязычная версия

Управление групповой политикой → Лес → Домены → <ваш домен> → Объекты групповой политики.
3. Нажмите правой кнопкой на нужный объект групповой политики и выберите **Изменить**:

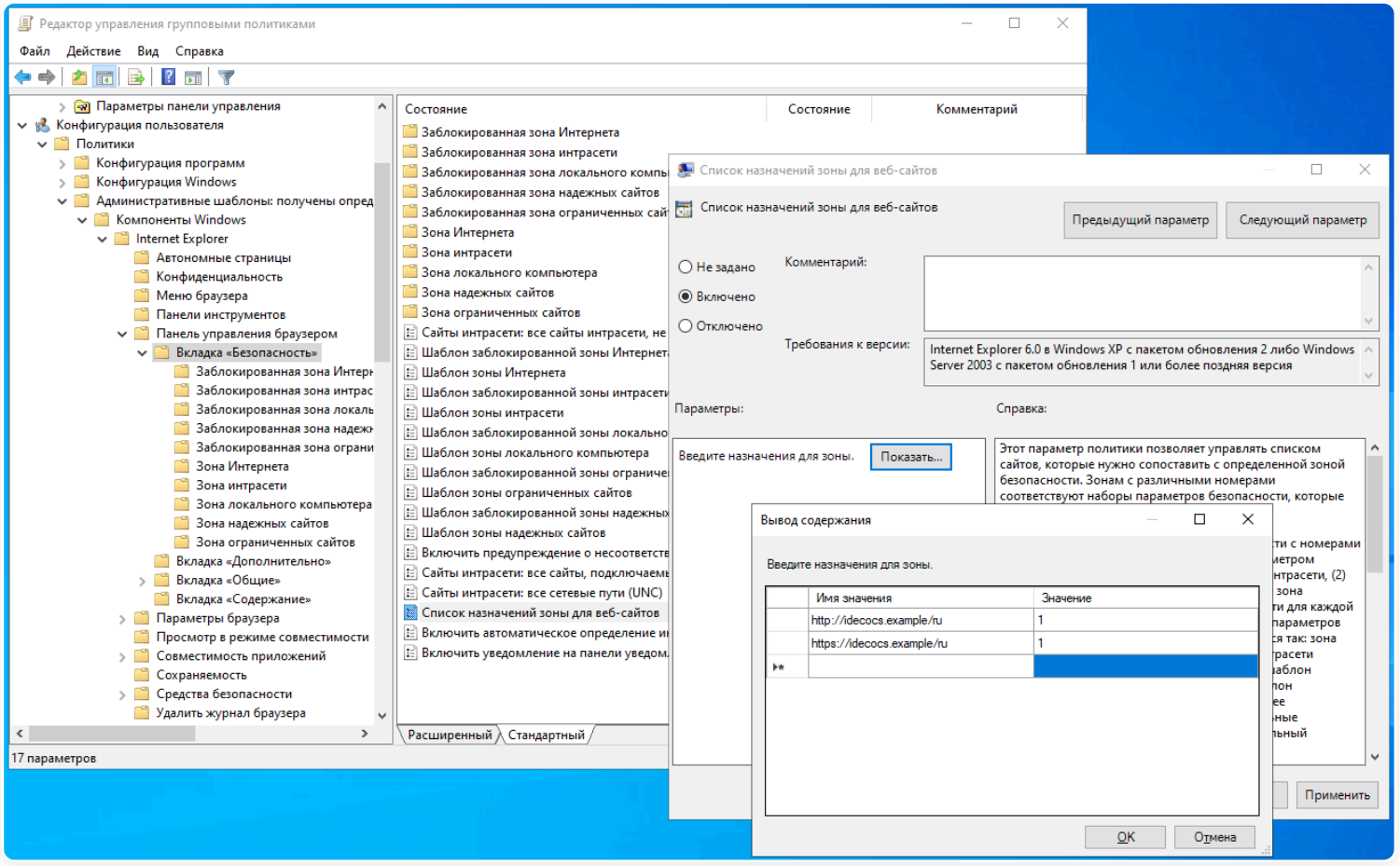


4. Перейдите по пути:

Англоязычная версия

Group Policy Management Editor → User Configuration → Policies → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Security Page → Site to Zone Assignment List.
Русскоязычная версия

Редактор управления групповыми политиками → Конфигурация пользователя → Политики → Административные шаблоны → Компоненты Windows → Internet Explorer → Панель управления браузером → Вкладка «Безопасность» → Список назначений зоны для веб-сайтов.
5. Введите назначение зоны для DNS-имени Ideco NGFW Novum (в примере idecoics.example.ru) со значением `1` (интрасеть). Укажите два назначения для схем работы по `http` и `https`:

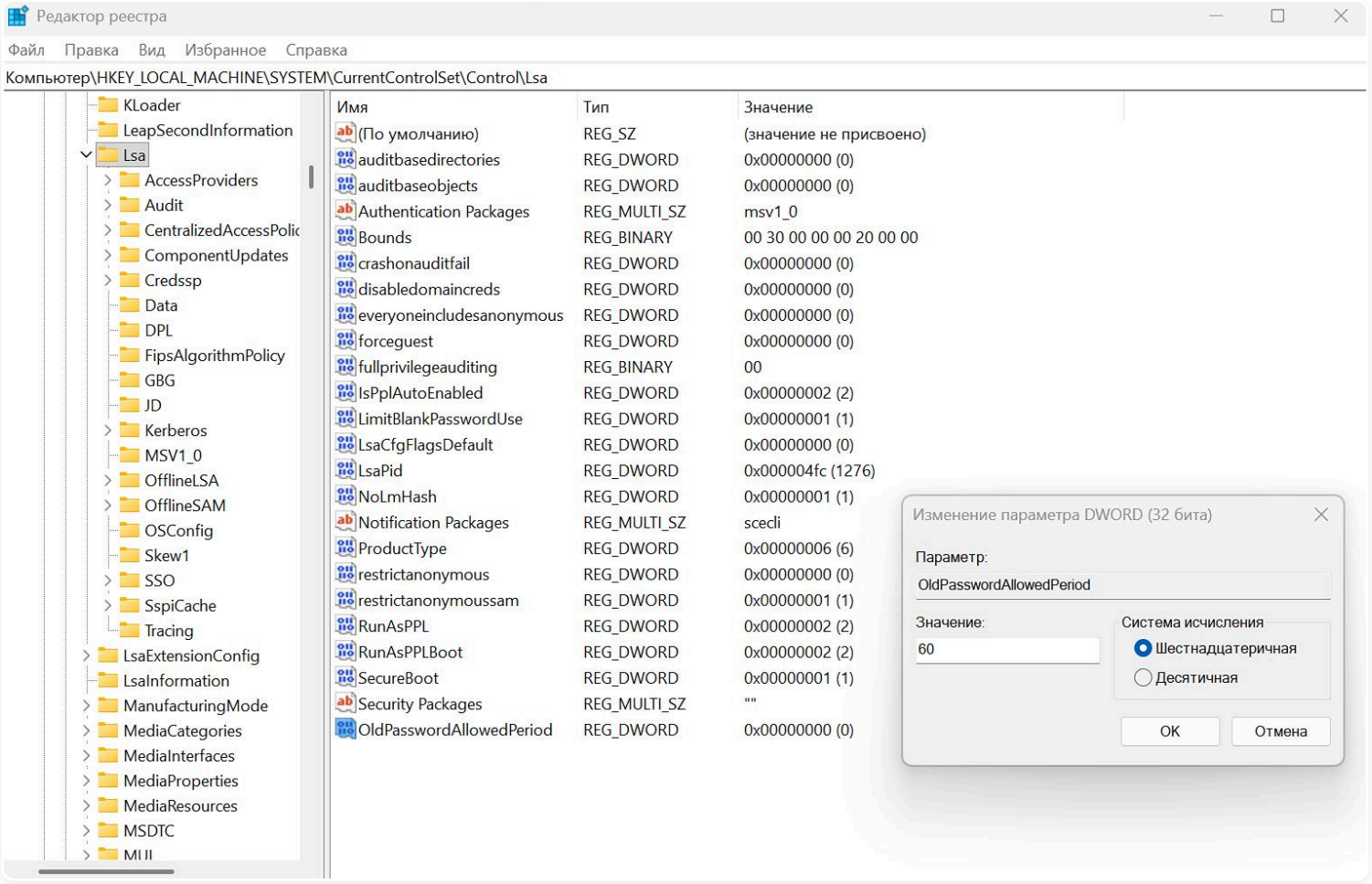


При входе на HTTPS-сайт необходимо разрешить браузеру доверять сертификату Ideco NGFW Novum. Чтобы не делать это каждый раз, можно добавить корневой сертификат Ideco NGFW Novum в доверенные корневые сертификаты устройства.

Особенности использования NTLM-токенов

При использовании NTLM-токенов для веб-аутентификации, а также при VPN авторизации необходимо учитывать период действия старого пароля пользователя. Если политика домена AD **Enforce Password History** установлена на хранение двух и более старых паролей, то контроллеры успешно аутентифицируют через NTLM пользователя с использованием старого пароля еще некоторое время после изменения пароля. По умолчанию в течение **5 минут**.

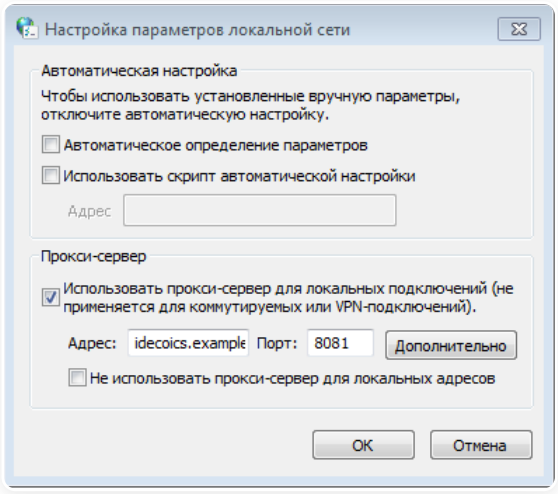
Период действия старого пароля можно настроить с помощью редактирования реестра на контроллере домена. Для этого нужно добавить параметр `DWORD` с именем `OldPasswordAllowedPeriod` в ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`. В поле **Значение** указать период в минутах. Изменение периода действия старого пароля не требует перезагрузки:



Настройка аутентификации пользователей при прямых подключениях к прокси-серверу

Настройка прозрачной аутентификации пользователей при прямых подключениях к прокси-серверу аналогична настройке прозрачной **SSO-аутентификации**.

Единственная особенность - укажите в качестве адреса прокси-сервера **DNS-имя Ideco NGFW Novum**:



При прямых подключениях к прокси **не указывайте** в качестве шлюза IP-адрес Ideco NGFW Novum.

Настройка браузера Mozilla Firefox для аутентификации по NTLM при прямом подключении к прокси-серверу

Для аутентификации компьютеров, которые **не находятся в домене**, под доменным пользовательским аккаунтом на странице настроек браузера **Mozilla Firefox** (введите ***about:config*** в адресной строке) укажите следующие параметры:

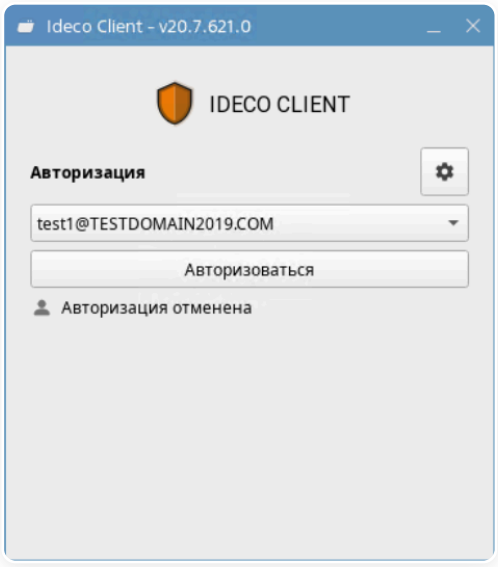
- **network.automatic-ntlm-auth.allow-proxies** = false.
- **network.negotiate-auth.allow-proxies** = false.

Не указывайте в параметрах значение `true` для компьютеров, входящих в домен, т. к. в таком случае будет использоваться устаревший метод авторизации по NTLM.

Возможные проблемы

Авторизация отменена

Проблема: после ввода в домен и настройки SSO-аутентификации попытка авторизации через SSO-профиль не проходит, и Ideco Client выдает ошибку **Авторизация отменена**:



Возникновение такой ошибки может быть связано с неправильной настройкой сети или интеграции NGFW Novum с Active Directory. Ideco Client пытается получить токен для авторизации на NGFW Novum. Но NGFW Novum нет в списках сервисов AD на контроллере домена, и токен получить невозможно.

Для диагностики выполните шаги:

1. Проверьте наличие сети между пользовательской машиной и контроллером домена.

2. Убедитесь, что учетная запись типа **Компьютер** для NGFW Novum на контроллере домена не удалена и имеет необходимые права.

3. Проверьте, что настройки интеграции пользовательского компьютера с AD и NGFW Novum с AD совпадают. Это возможно сделать на контроллере домена или с помощью команды:

```
ldapsearch -H ldap://<имя-контроллера-домена>.<имя-домена> -b "DC=<уровень-домена-(N)>,DC=<уровень-домена-(N-1)>" "(servicePr
```

- `-H ldap://<имя-контроллера-домена>.<имя-домена>` – указывает URL контроллера домена, к которому отправляется запрос;
- `-b "DC=<уровень-домена-(N)>,DC=<уровень-домена-(N-1)>"` – задает базовый DN (Distinguished Name) для поиска. Например, `DC=corp,DC=example,DC=com`;
- `"(servicePrincipalName=*/<имя-NGFW>.<имя-домена>*)"` – ищет объекты, у которых атрибут `servicePrincipalName` содержит строку вида `*/<имя-NGFW>.<имя-домена>*`. Звездочки `*` означают любые символы до и после;
- `servicePrincipalName` – указывает, какой атрибут нужно вывести в результатах поиска.

4. Запустите Ideco Client с опцией `--debug`. Проверьте логи (например, с помощью `journalctl`, `KSystemLog` или `logcheck`) на ошибки получения SSO-токенов вида:

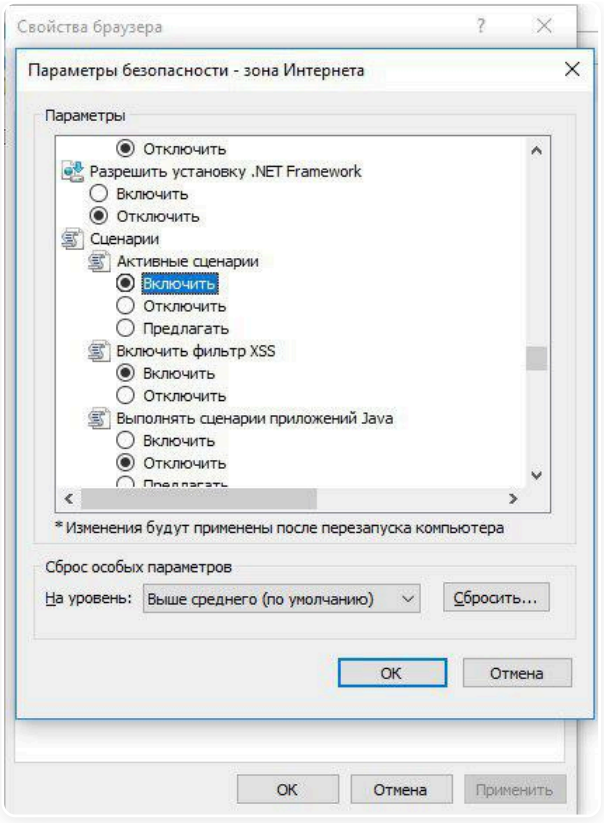
```
SSOGenToken завершился с ошибкой: 'genTokenInternal: <major error string> (<minor error string>)'
```

- `<minor error string>` - описание ошибки, указывающее на причину возникновения ошибки токена SSO.

5. Проверьте состояние интеграции в **Пользователи** → **Active Directory/Samba DC** и при необходимости перенастройте.

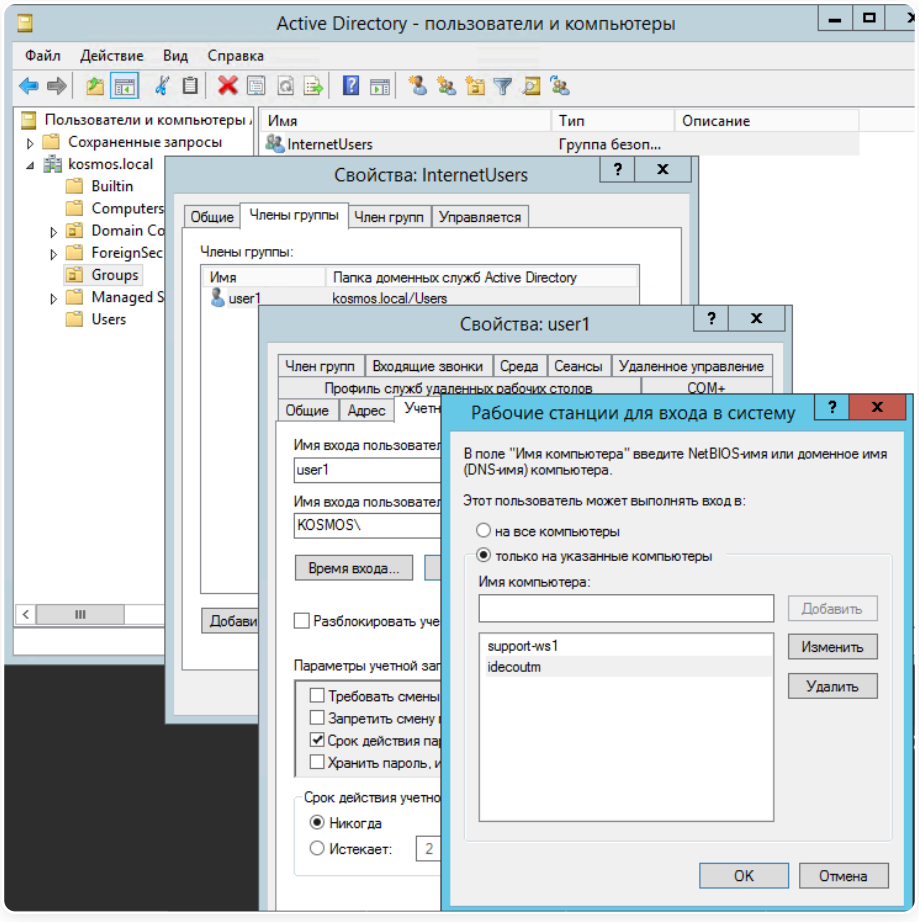
Для получения доступа требуется аутентификация

Если в Internet Explorer появляется окно с текстом **Для получения доступа требуется аутентификация** и аутентификация происходит только при ручном переходе по ссылке, установите параметр **Активные сценарии** в Internet Explorer в значение **Включить**:



Доменному пользователю должно быть разрешено аутентифицироваться на Ideco NGFW Novum. На контроллере домена зайдите в свойства выбранных пользователей в **Учетная запись → Вход на...**, выберите пункт **только на указанные компьютеры** и пропишите имя рабочей станции для входа в систему.

Пример настройки:



Полезные ссылки

- **Авторизация через журнал безопасности AD**
- **Настройка веб-аутентификации**

Настройка авторизации через журнал безопасности

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Настройка авторизации через журнал безопасности**: `ideco-ad-log-collector`.

Список служб для других разделов доступен по ссылке.

Особенности авторизации через журнал безопасности Active Directory

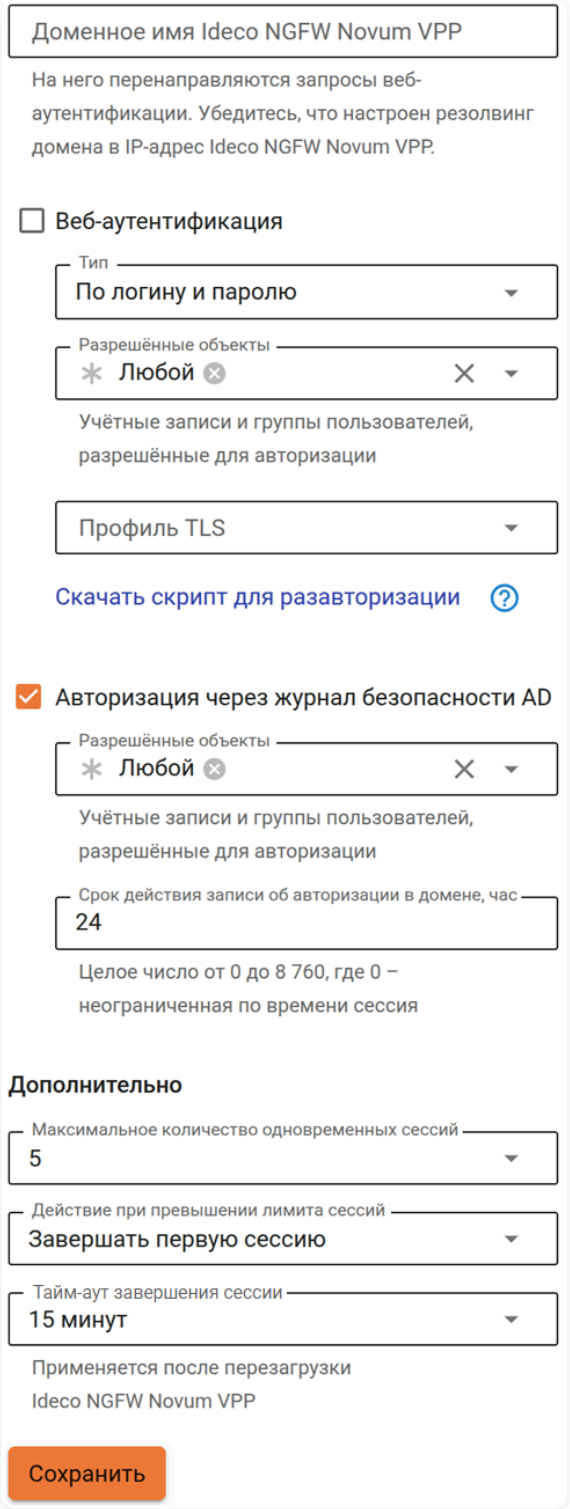
Авторизацию через журнал безопасности Active Directory рекомендуется использовать совместно с SSO-аутентификацией. Авторизация только через журнал безопасности может ограничить возможности управления и настройки прав доступа.

Использование только **Авторизации через журнал безопасности Active Directory** ненадежно по причинам:

- Логи журнала событий безопасности содержат только имя пользователя, IP-адрес и время входа. Журнал не содержит всей информации, необходимой для полноценной авторизации: группы безопасности, права доступа и другие атрибуты пользователя.
- Любые проблемы с журналом, такие как повреждение, потеря данных или задержки в записи, могут привести к проблемам с авторизацией.
- Авторизация через журнал безопасности менее безопасна, так как логи могут быть подделаны или изменены злоумышленниками.
- Авторизация через журнал безопасности требует сложной обработки логов, что повышает риск ошибок и затрудняет поддержку.

Настройка на стороне NGFW Novum

Перейдите в **Пользователи** → **Авторизация** → **Настройки** и заполните поля:

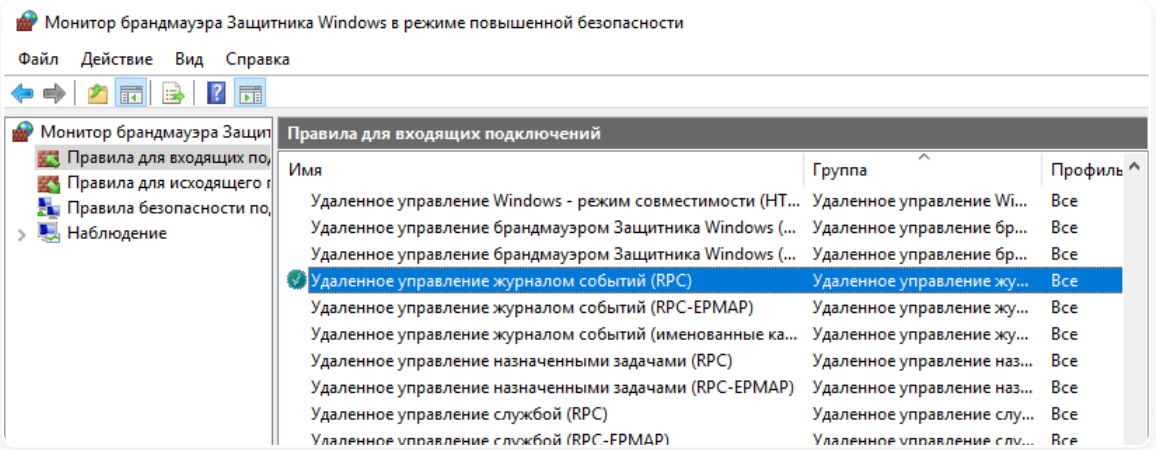


- **Доменное имя Ideco NGFW Novum** - не требуется, если используется только авторизация через журнал безопасности AD.
- **Веб-аутентификация** - не требуется. Авторизация через журнал безопасности AD обеспечивает аутентификацию.
- **Авторизация через журнал безопасности Active Directory** - включите, чтобы Ideco NGFW Novum отслеживал события успешного входа в журнале безопасности AD (события с Event Id `4768`, `4769`, `4624`) и авторизовывал пользователя по ним, если трафик идет с того же IP-адреса.
- **Разрешенные объекты** - выберите разрешенные для авторизации учетные записи или группы пользователей.
- **Срок действия записи об авторизации в домене** - введите время, по истечении которого пользователь деавторизуется в NGFW Novum, если не будет нового входа в домен. При каждом входе пользователя отсчет начинается заново.

Настройка на стороне сервера Active Directory

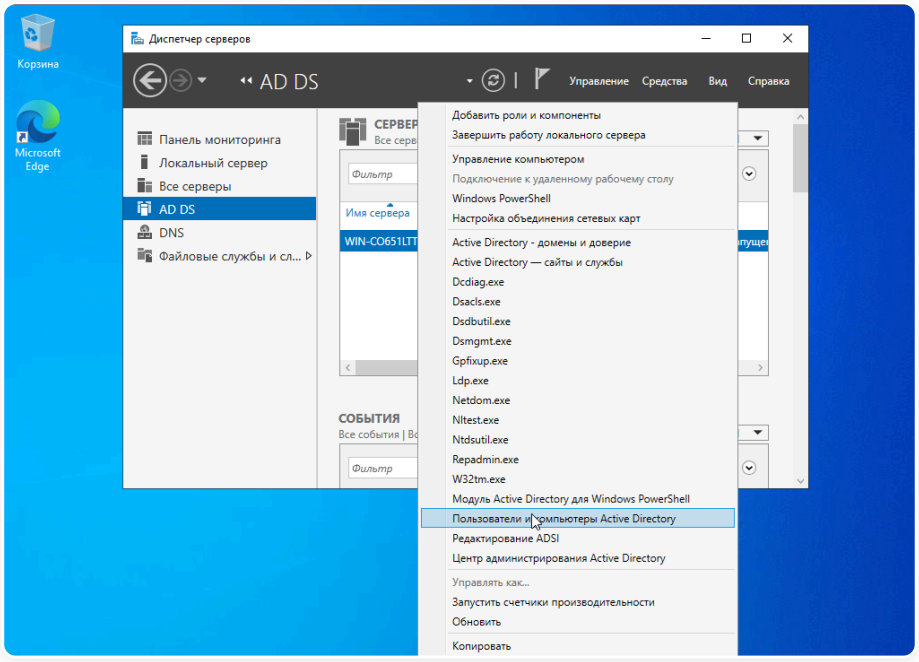
Перед настройкой убедитесь, что Ideco NGFW Novum уже введен в домен.

1. В настройках брандмауэра Windows на всех контроллерах домена разрешите **Удаленное управление журналом событий (Remote Event Log Management)**:

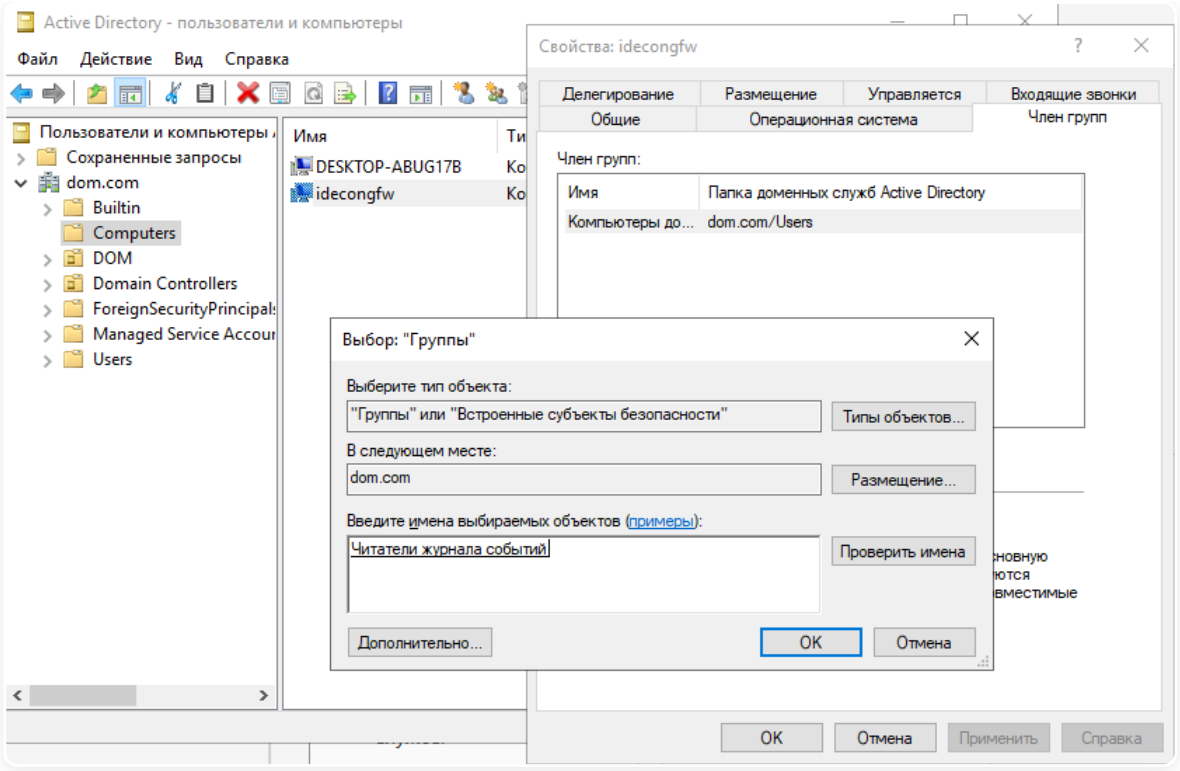


2. Добавьте Ideco NGFW Novum в группу безопасности **Читатели журнала событий (Event Log Readers)**. Чтобы это сделать:

- Зайдите в **Диспетчер серверов**, кликните на **AD DC**, правой кнопкой мыши нажмите на строку с нужным сервером и в выпадающем списке выберите **Пользователи и компьютеры Active Directory**:



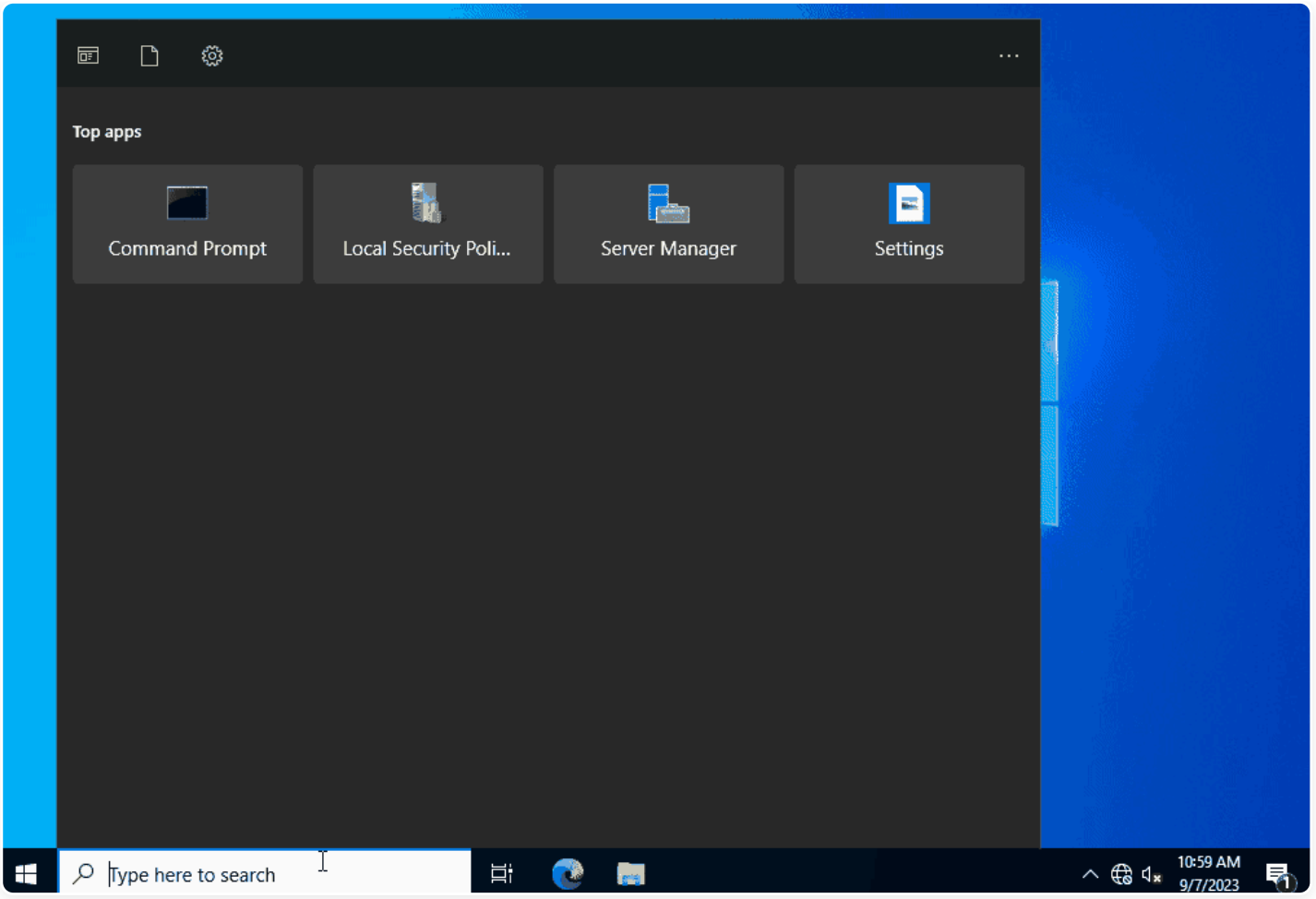
- Откройте **Свойства** объекта **Компьютер**, под которым Ideco NGFW Novum введен в домен (на скриншоте - idecongfw). Перейдите на вкладку **Член групп** и нажмите на кнопку **Добавить**. В появившемся окне нажмите на кнопку **Дополнительно** и добавьте **Читатели журнала событий (Event Log Readers)** через кнопку **Поиск**:



3. Перезапустите службу **Авторизация через журнал безопасности Active Directory** на Ideco NGFW Novum. Для этого отключите эту опцию, а затем снова включите. Либо перезапустите службу `ideco-ad-log-collector` в консоли.

При изменении стандартной политики безопасности контроллеров домена выполните действия:

Англоязычная версия



1. Откройте **Group policy management**.

2. Выберите **Forest: Доменное имя AD** → **Domains** → **Доменное имя AD**.

3. Нажмите правой кнопкой мыши по **Default Domain policy** и выберите **Edit**.

4. В открывшемся окне перейдите по пути **Computer configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies** → **Logon/Logoff**.

5. Дважды кликните по **Audit Logon**.

6. В открывшемся окне на вкладке **Policy** включите **Configure the following audit event** и выберите **Success**.

7. Нажмите **Apply** и **OK**.

8. В папке **Audit Policies** перейдите в **Account Logon**.

9. Дважды кликните по **Audit Kerberos Authentication Service** и повторите действия из пункта 6.

10. Повторите пункты 8 и 9 для **Audit Kerberos Service Ticket Operations**.

Русскоязычная версия

1. Откройте **Управление групповой политикой**.

2. Выберите **Лес: Доменное имя AD** → **Домены** → **Доменное имя AD**.

3. Нажмите правой кнопкой мыши по **Default Domain policy** и выберите **Изменить**.

4. В открывшемся окне перейдите по пути **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Конфигурация расширенной политики аудита** → **Политики аудита** → **Вход/Выход**.

5. Дважды кликните по **Аудит входа в систему**.

6. В открывшемся окне на вкладке **Политика** включите **Настроить следующие события аудита** и выберите **Успех**.

7. Нажмите **Применить** и **OK**.

8. В папке **Политики аудита** перейдите в **Вход учетной записи**.

9. Дважды кликните по **Аудит службы проверки подлинности Kerberos** и повторите действия из пункта 6.

10. Повторите пункты 8 и 9 для **Аудита операций с билетами службы Kerberos**.



Для обновления политик контроллера домена, в терминале выполните команду `gpupdate /force`.

Если авторизация пользователей при входе в систему не происходит, проверьте в журнале безопасности наличие событий 4768, 4769, 4624. Чтобы просмотреть журнал, воспользуйтесь встроенным приложением **Просмотр событий** (Event Viewer). Находится в меню **Пуск** → **Просмотр событий**.

Полезные ссылки

- **Настройка веб-аутентификации**
- **Настройка SSO-аутентификации**

Скрипты автоматического завершения сессии

Классический контекст | Высокопроизводительный контекст

Для автоматического завершения сессий пользователей настройте скрипт (logout), который будет запускаться при выходе пользователей из системы с помощью групповых политик домена (GPO).

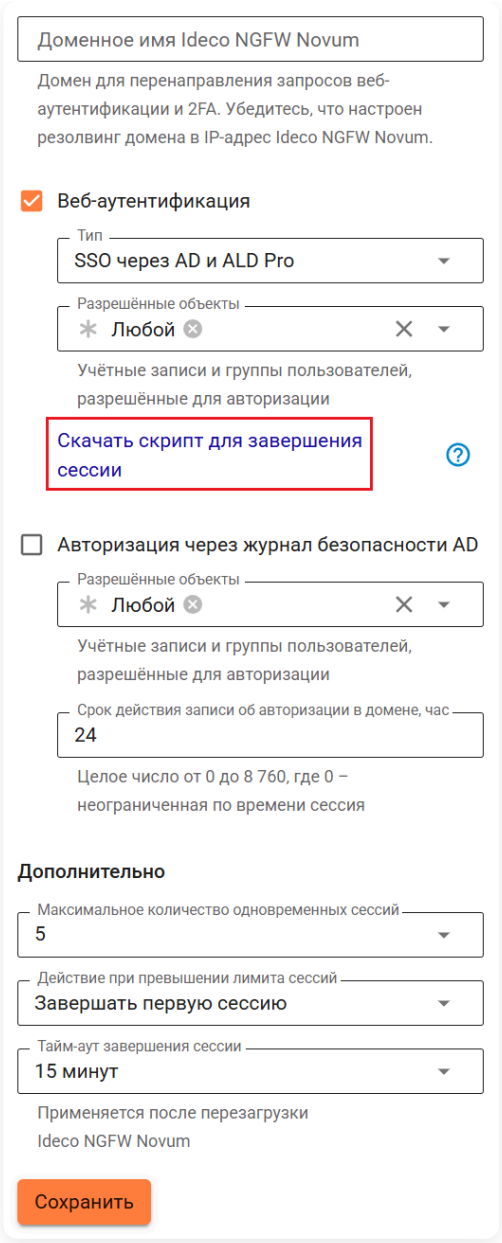
Для работы скрипта выполните настройки политик безопасности домена и браузера, описанные в статье Авторизация пользователей.

Для авторизации по SSO используйте Ideco Client.

Завершение сессии пользователя

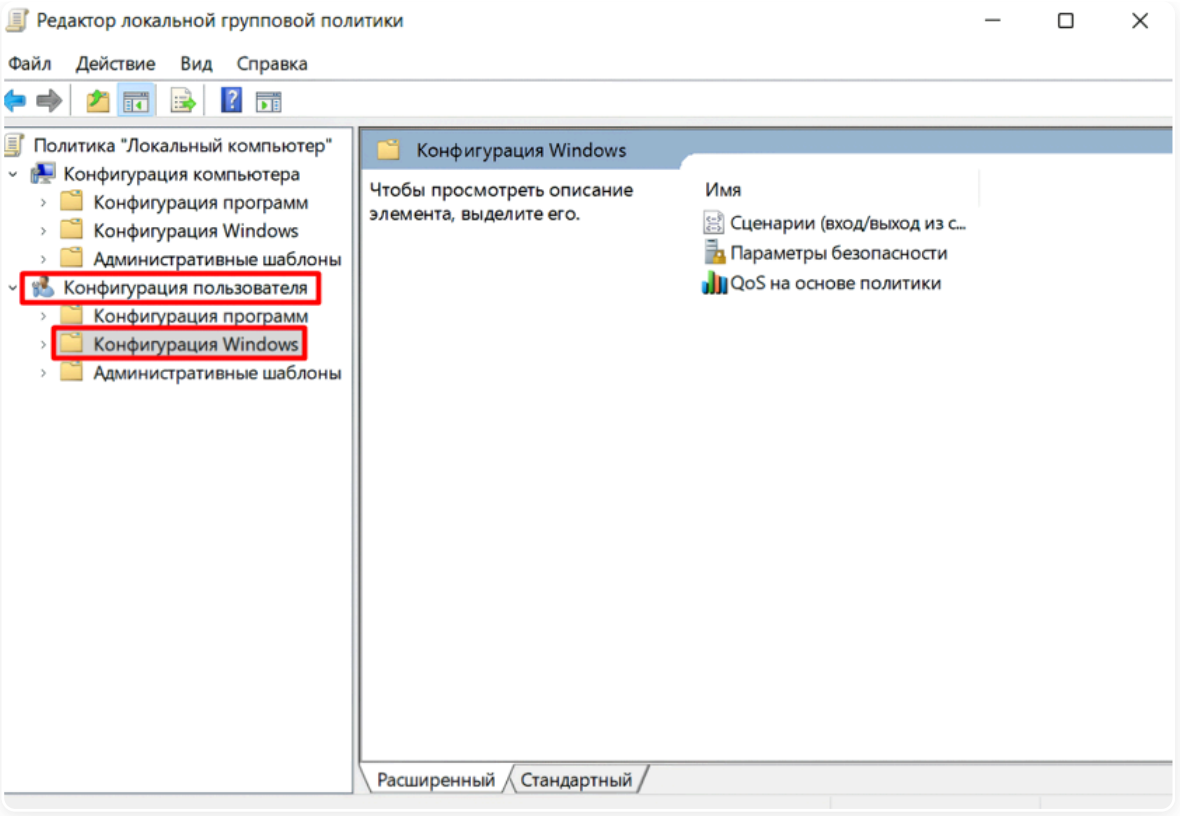
Чтобы скрипт завершения сессии работал корректно, установите на компьютеры пользователей корневой сертификат сервера Ideco NGFW Novum и сделайте сертификат доверенным. Это можно сделать как локально, так и через групповые политики домена, следуя инструкции.

1. Чтобы скачать скрипт, перейдите в **Пользователи** → **Авторизация** → **Настройки**. Включите опцию **Веб-аутентификация**, после чего нажмите **Скачать скрипт для завершения сессии**:



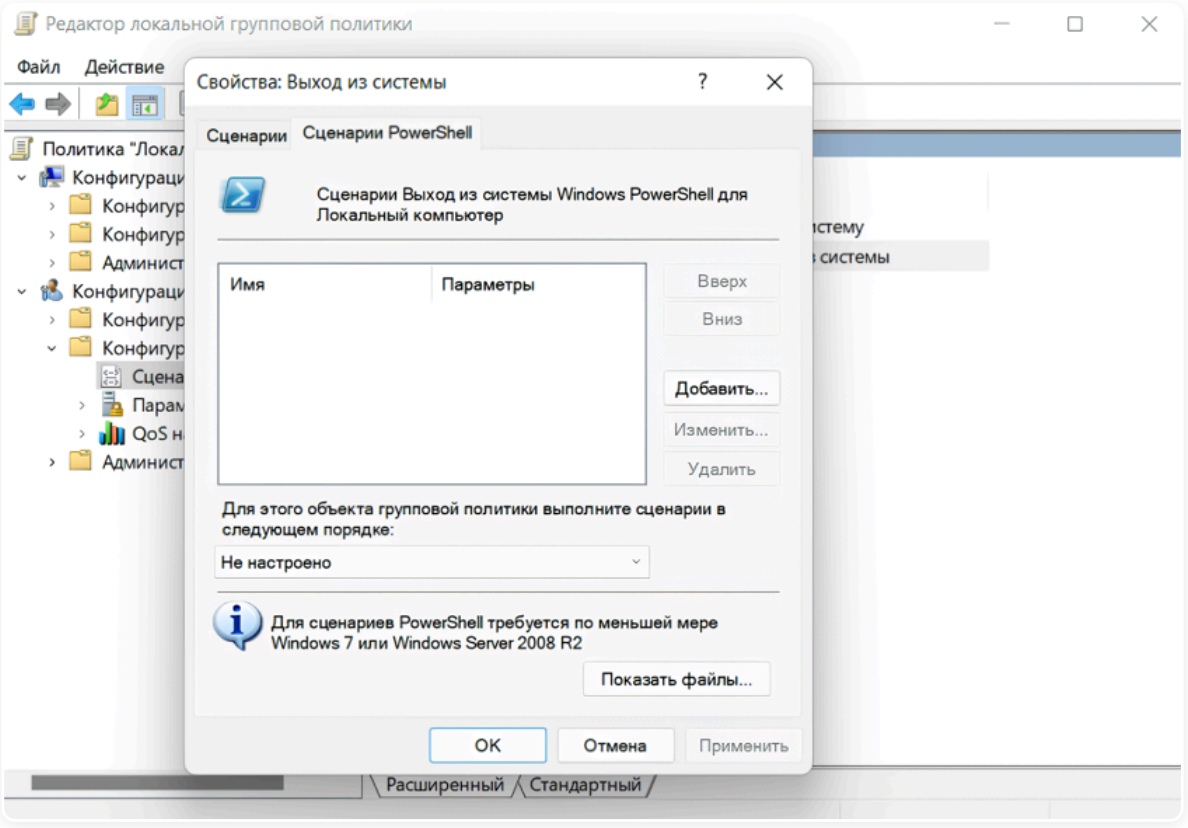
2. Откройте групповые политики `gpedit.msc` от имени администратора на устройстве пользователя.

3. Перейдите в **Конфигурации пользователя** → **Конфигурации Windows**:

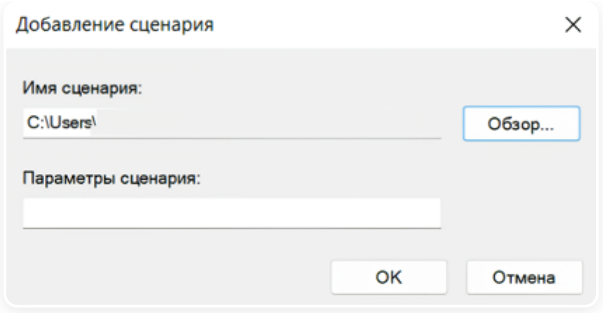


4. Нажмите **Сценарии (вход/выход из системы)**.

5. Откройте **Выход из системы** и перейдите на вкладку **Сценарии PowerShell**:



6. Нажмите **Добавить** и выберите скачанный файл **Ideco_NGFW_logout.ps1**, нажав **Обзор**:



7. Откройте командную строку и обновите групповые политики, введя команду `gpupdate /force`.

Если в вашем браузере появляется окно с текстом **Для получения доступа требуется аутентификация** и авторизация происходит только при ручном переходе по ссылке, включите JavaScript. Ниже представлены настройки для разных браузеров:

Internet Explorer

1. В правом верхнем углу браузера нажмите **Сервис** в виде шестерни или комбинацию клавиш **Alt + X**. В выпадающем меню выберите **Свойства браузера**:

2. В появившемся окне перейдите на вкладку **Безопасность**. Затем нажмите **Другой**:

3. В окне **Параметры** переключите параметр **Активные сценарии** в значение **Включить**:

Google Chrome

1. В правом верхнем углу браузера нажмите на кнопку с тремя точками и выберите **Настройки** в выпадающем меню:

2. В появившемся окне перейдите в раздел **Конфиденциальность и безопасность** и выберите **Настройки сайта**:

3. В настройках **JavaScript** разрешите сайтам использовать JavaScript:

Firefox

1. В адресной строке браузера введите about:config и нажмите **Enter**. Если появится предупреждающее сообщение, нажмите **Принять риск и продолжить**:

2. В поле поиска введите javascript.enabled и переключите настройку параметра, чтобы изменить значение с `false` на `true`:

3. Обновите страницу в браузере.

ALD Pro

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **ALD Pro**: `ideco-ald-rest`; `ideco-ald-backend`.

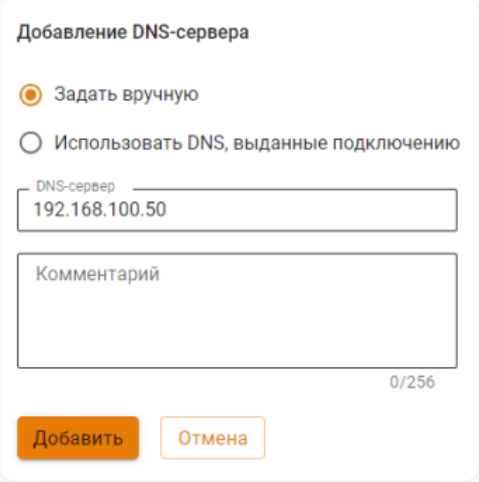
Список служб для других разделов доступен по ссылке.

Система ALD Pro предназначена для централизованного управления ресурсами на базе ОС Astra Linux и может использоваться в организациях различного масштаба.

Ideco NGFW Novum поддерживает версии ALD Pro от 1.4.

Ввод сервера в домен

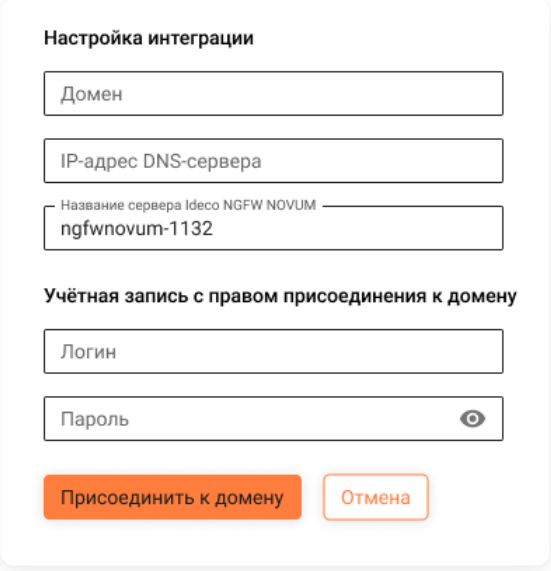
1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы** и добавьте IP-адрес устройства с установленной системой ALD Pro:



2. Перейдите в **Пользователи** → **Внешние каталоги** → **ALD Pro**.

3. Нажмите на кнопку **Добавить**.

4. Заполните поля:



Расшифровка полей

- **Домен** - полное имя домена (не контроллера домена/хоста). Например, `mydomain.example`, а не `astra.mydomain.example`. Домен может содержать только латинские символы, цифры, подчеркивание, дефис и точку.
- **IP-адрес DNS-сервера** - IP-адрес устройства с установленной системой ALD Pro.
- **Название сервера Ideco NGFW Novum** - имя сервера, которое можно сгенерировать в NGFW или указать вручную. Содержит буквенные символы (A-Z), цифры (0-9), а также не может начинаться или заканчиваться на дефис. Максимальное количество символов - 15.
- **Логин и пароль администратора** - данные не сохраняются на сервере и используются один раз для присоединения к домену. Пользователь может не быть администратором домена, но должен обладать правами на присоединение компьютеров к домену.

Если в таблице большое количество интеграций, воспользуйтесь кнопкой **Фильтры**.

Импорт пользователей

ALD Pro поддерживает импорт двух типов групп:

- Группа пользователей - содержит несколько пользователей ALD Pro.
- Подразделение - содержит дерево пользователей ALD Pro, обладающих определенным уровнем доступа.

Из-за особенностей реализации ALD Pro заблокированные пользователи импортируются в Ideco NGFW Novum без блокировки и считаются **активными**.

Для импорта пользователей выполните действия:

1. Перейдите в **Пользователи** → **Учетные записи** и создайте группу, в которую будут импортированы пользователи, нажав на .

2. Перейдите на вкладку **ALD Pro**, выберите домен, тип группы и нажмите **Присоединить к домену**.

Импортированных пользователей можно использовать в качестве объектов для авторизации, настройки VPN-подключений, создания правил трафика (например, в **Межсетевом экране**).

В дальнейшем пользователи будут автоматически синхронизироваться с ALD Pro каждые 15 минут.

Пользователь может быть импортирован только в одну группу Ideco NGFW Novum. Если пользователь находится в нескольких группах ALD Pro то попадет только в ту группу, которая была импортирована последней.

Рекомендуем при создании пользователей указывать в логине домен, например `user@domain.ald`.

Аутентификация пользователей

При аутентификации пользователей проверка осуществляется средствами Kerberos.

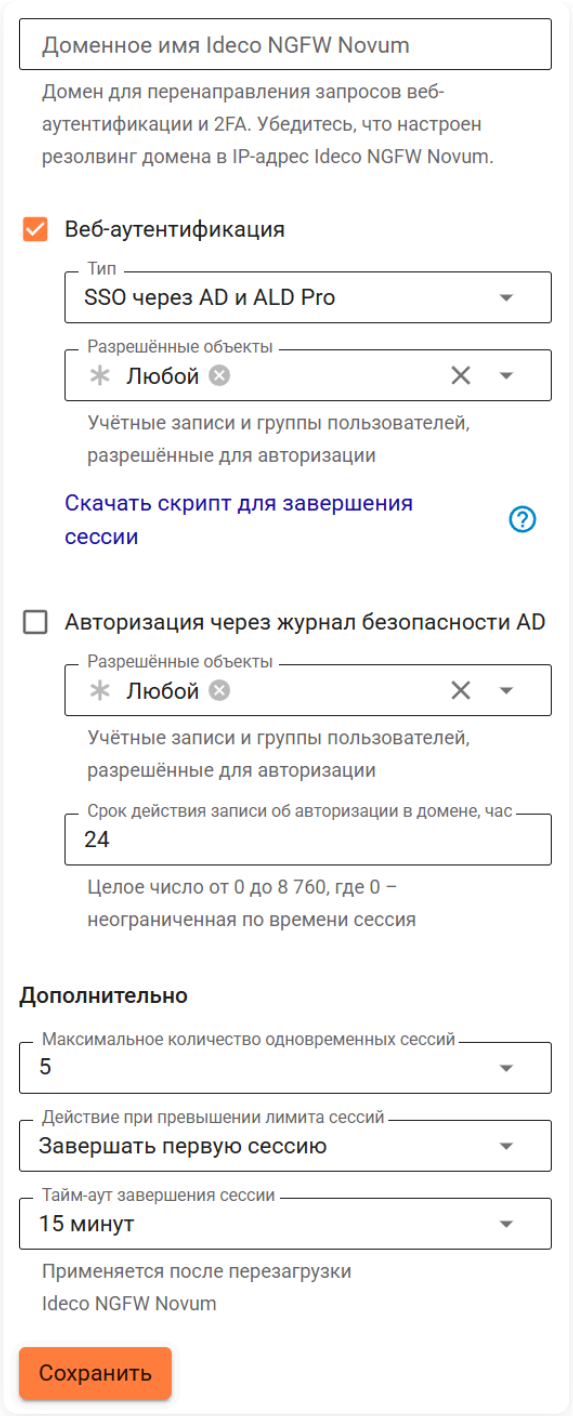
ALD Pro поддерживает два типа входа в систему:

- Вход по логину/паролю.
- Вход через SSO.

Настройка Ideco NGFW Novum

Для настройки аутентификации выполните действия:

1. Перейдите на **Пользователи** → **Авторизация** → **Настройки**:



2. Активируйте опцию **Веб-аутентификация**.

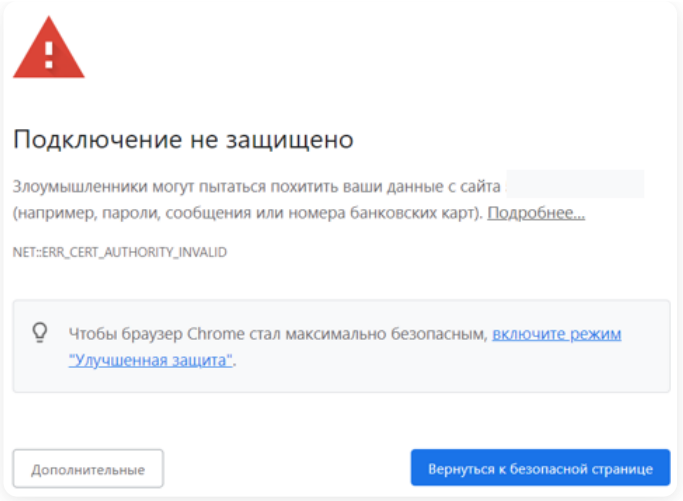
3. Выберите **Тип** входа в систему:

- **По логину и паролю** - вход по логину/паролю.
- **SSO через AD и ALD Pro** - вход через SSO.

4. Выберите разрешенные для авторизации учетные записи или группы пользователей в поле **Разрешенные объекты**.

Настройки в разделе **Дополнительно** описаны в статье.

После заполнения поля **Доменное имя Ideco NGFW Novum** и сохранения настроек будет выдан Let’s Encrypt сертификат, и пользователь перенаправляется на окно авторизации, минуя страницу исключения безопасности:



Если сертификат для такого домена уже загружен в разделе **Сертификаты**, то будет использоваться загруженный сертификат, новый сертификат выдаваться не будет.

> Если NGFW Novum не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW, то страница авторизации будет подписана корневым сертификатом NGFW Novum.

5. Настройте способы авторизации импортированных пользователей. Доступны:

- Авторизация по IP и/или MAC - подходит для пользователей с фиксированными IP- и/или MAC-адресами, на NGFW адреса прописываются вручную каждому пользователю;
- Авторизация по подсетям - подходит, если не требуется регистрировать каждое устройство как отдельного пользователя NGFW. Позволяет автоматически авторизовать большое количество устройств.
- Авторизация по VPN - подходит для аутентификации пользователей удаленных сетей.

Настройка клиентских машин для веб-аутентификации по SSO или NTLM

1. В зависимости от выбранного браузера выполните следующие действия:

Настройка браузера Yandex

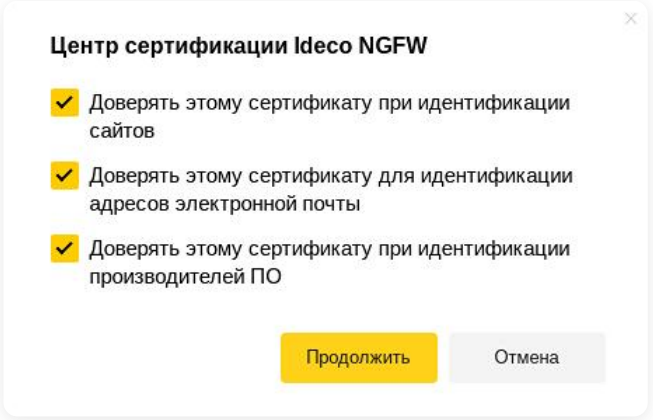
1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.имя_домена",
  "AuthNegotiateDelegateAllowlist": "*.имя_домена"
}
```

2. Скачайте корневой сертификат.

3. В браузере Yandex перейдите в **Настройки** → **Системные** → **Управление сертификатами** → **Центры сертификации** → **Импорт** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:



Настройка браузера Google Chrome

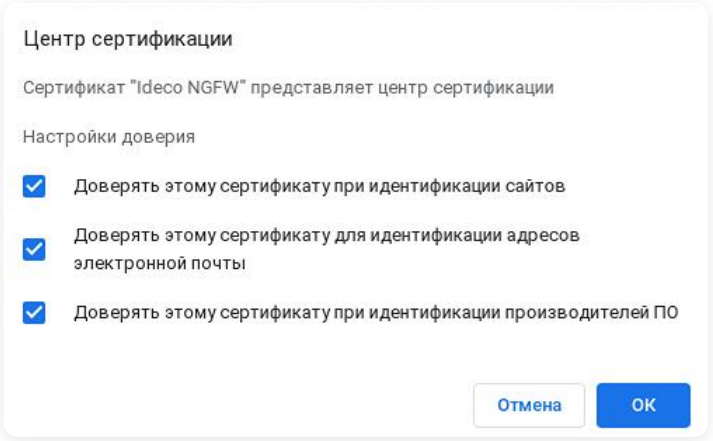
1. Создайте файл **mydomain.json** в директории `/etc/opt/chrome/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.имя_домена",
  "AuthNegotiateDelegateAllowlist": "*.имя_домена"
}
```

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:



Настройка браузера Chromium

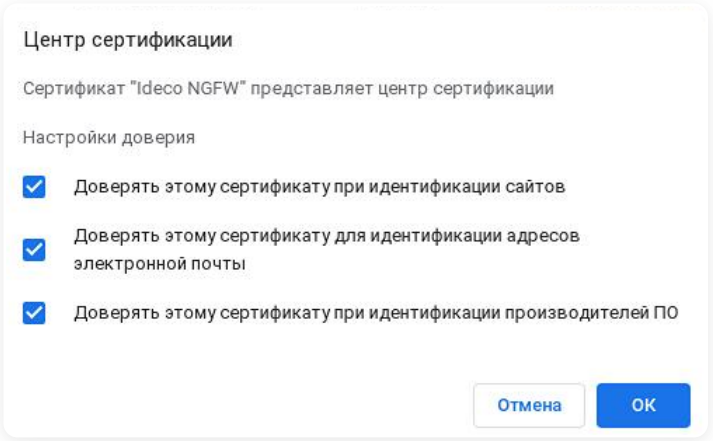
1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и добавьте строки:

```
{
    "AuthServerAllowlist": "*.имя_домена" ,
    "AuthNegotiateDelegateAllowlist": "*.имя_домена"
}
```

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:



Настройка браузера Mozilla Firefox

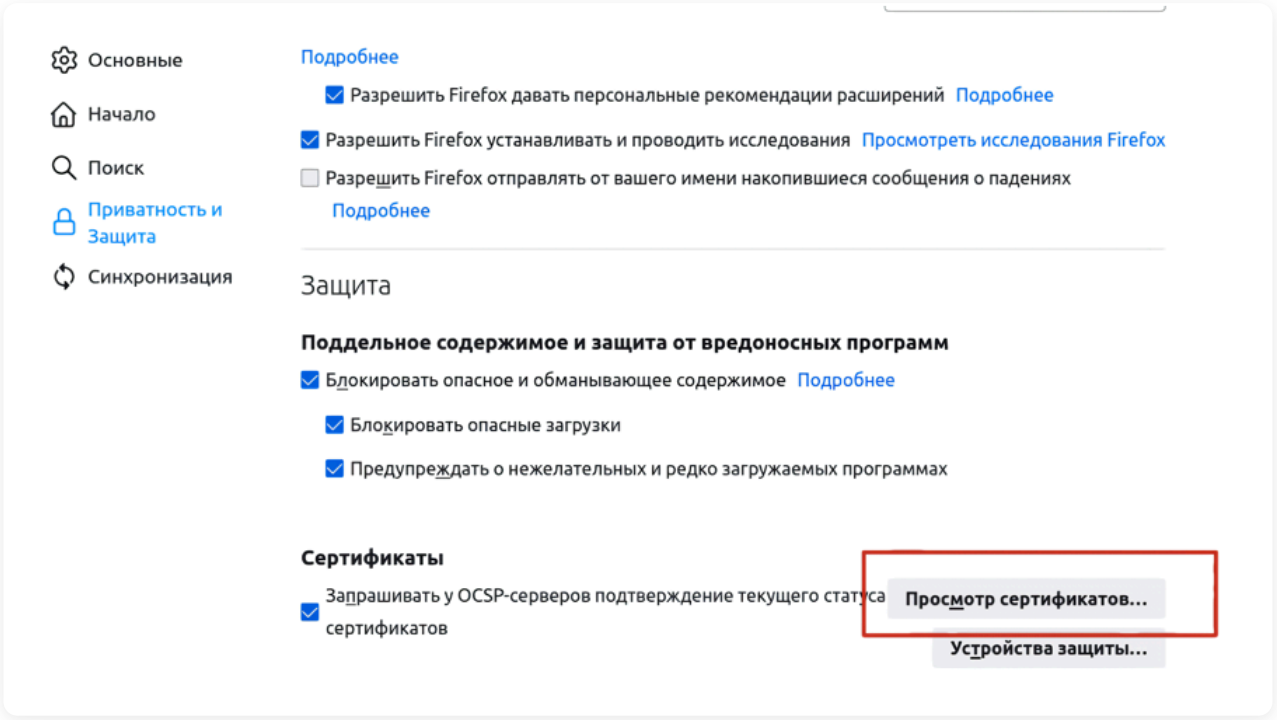
1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

2. Введите параметр `security.enterprise_roots.enabled` и дважды кликните по блоку, чтобы значение изменилось на **True**, что позволит Firefox доверять системным сертификатам и авторизовывать пользователей при переходе на HTTPS-сайты.

3. В параметрах `network.automatic-ntlm-auth.trusted-uris` и `network.negotiate-auth.trusted-uris` укажите `имя_NGFW.имя_домена`.

4. Скачайте корневой сертификат.

5. В настройках браузера Mozilla Firefox в пункте **Приватность и Защита** в разделе **Защита** выберите **Просмотр сертификатов**:



6. На вкладке **Центры сертификации** нажмите **Импортировать** и выберите скачанный с NGFW сертификат.

7. Включите опции доверия для сертификата.
2. На машине ALD-клиента, введенной в домен ALD Pro, добавьте IP-адрес локального интерфейса и доменное имя Ideco NGFW Novum в директорию `/etc/hosts`. Пример: `192.168.100.10 ngfw.domain.ald`.

Руководство по эксплуатации ALD Pro доступно на официальном сайте.

FreeIPA

Классический контекст | Высокопроизводительный контекст | API

FreeIPA - это интегрированное решение для идентификации и аутентификации в сетевых средах Linux/UNIX. Сервер FreeIPA обеспечивает централизованную аутентификацию, авторизацию и доступ к информации об учетных записях.

Предварительная настройка FreeIPA

Для интеграции Ideco NGFW Novum с FreeIPA необходимо на IPA-сервере создать роли:

- **CIFS servers** - предоставляет NGFW Novum права для аутентификации пользователей по протоколу Kerberos, выступая в роли доверенной службы.
- **Organization units** - предоставляет NGFW Novum право на чтение структуры подразделений из каталога для корректного импорта пользователей и групп безопасности.

Для создания ролей выполните действия:

1. Запустите **Терминал Fly** и введите по очереди команды:

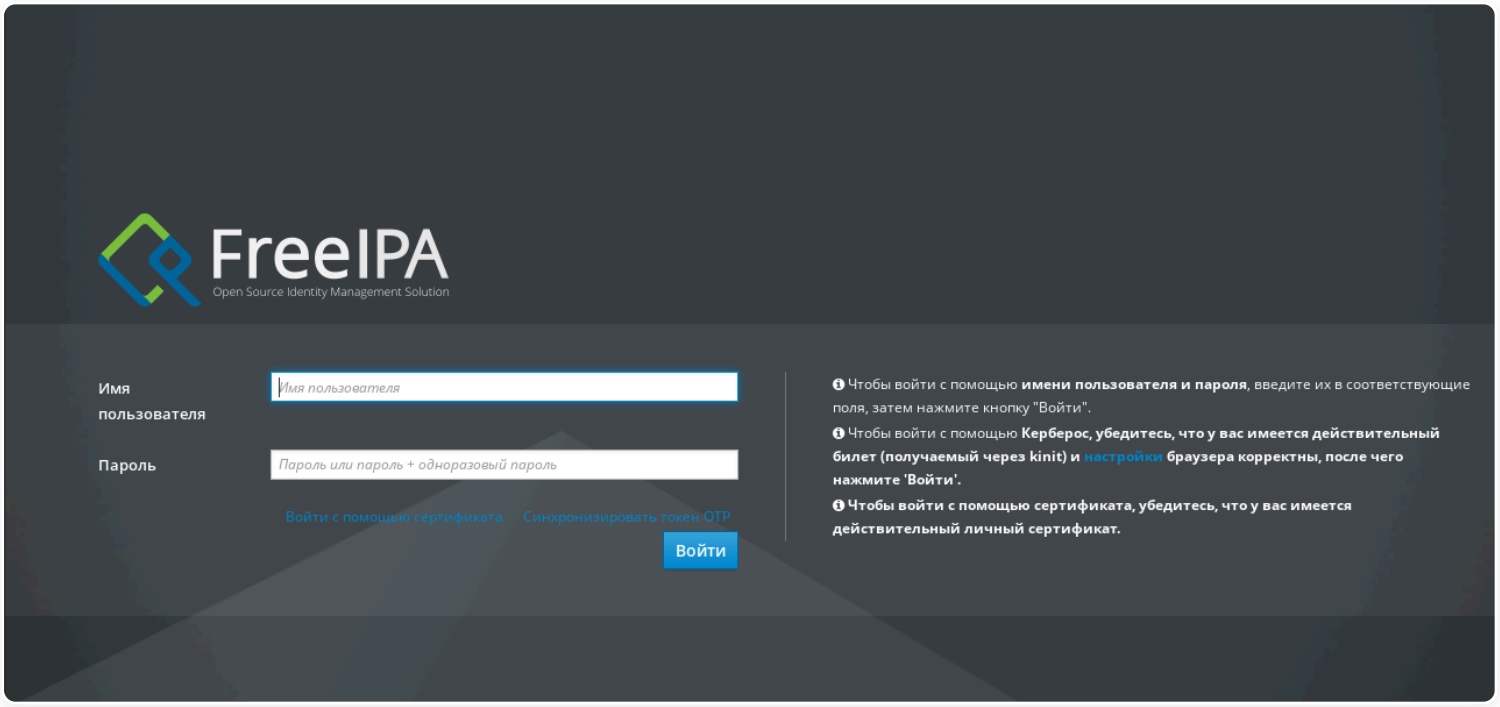
- Для создания роли **CIFS servers**:

```
ipa role-add "CIFS server" --desc="Role for CIFS server"
```

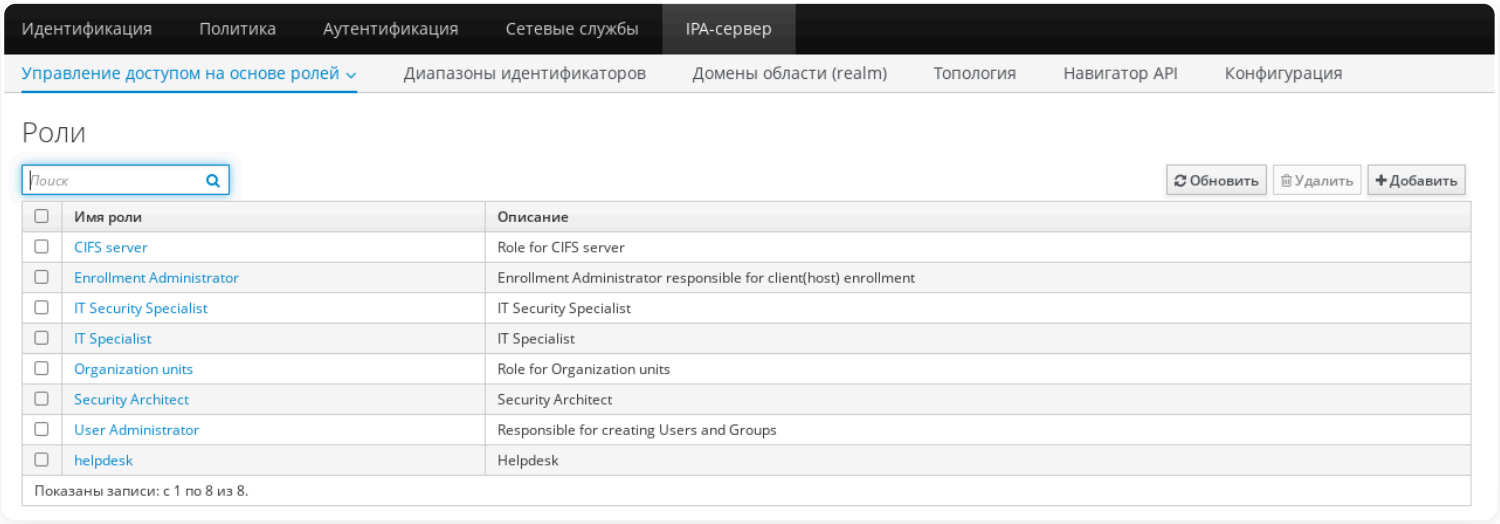
- Для создания **Organization units**:

```
ipa role-add "Organization units" --desc="Role for Organization units"
```

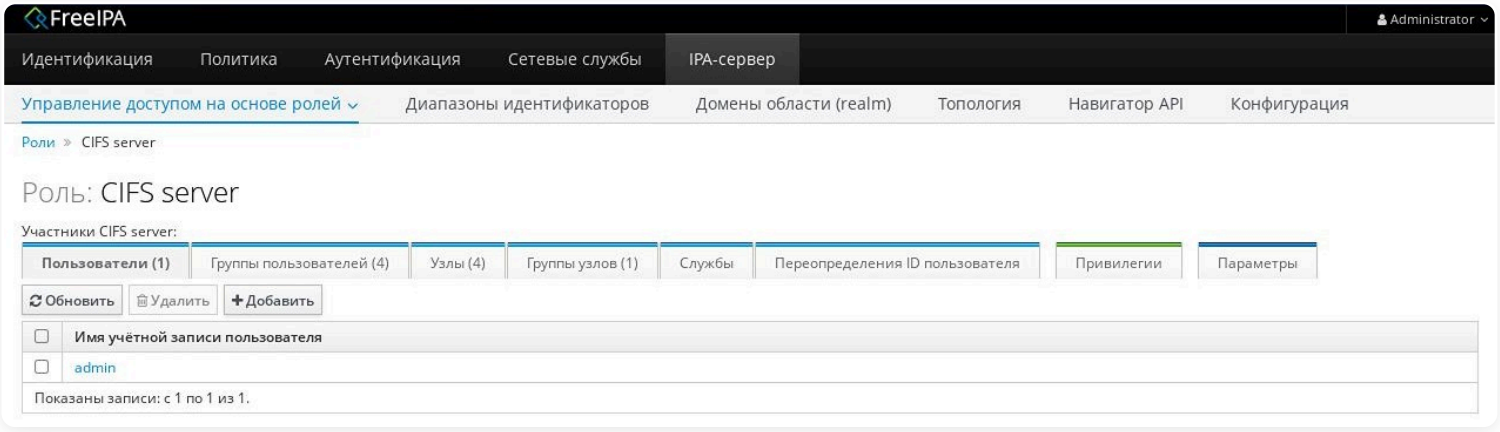
2. Войдите в веб-интерфейс FreeIPA и авторизуйтесь с учетными данными администратора:



3. Перейдите в **IPA-сервер** → **Управление доступом на основе ролей** и убедитесь, что созданные роли появились в списке:



4. Войдите в каждую роль и добавьте объекты:



- **Пользователи** - выберите всех пользователей.
- **Группы пользователей** - выберите все группы.
- **Узлы** - выберите доменный узел.
- **Группы узлов** - выберите все группы.

5. Перезагрузите сервер FreeIPA для активации новых прав.

Дополнительная настройка для VPN-подключений

Для VPN-подключений пользователей FreeIPA необходимо создать разрешение и привилегию на чтение атрибута `ipaNTHash`. Выполните действия одним из способов:

Через терминал

Запустите **Терминал Fly** и введите по очереди команды:

1. Создайте разрешение на чтение NTLM-хэша:

```
ipa permission-add "Read NT Hash Permission" --type=user --permissions="read" --attrs=ipaNTHash
```

2. Создайте привилегию:

```
ipa privilege-add-permission read-ntlm-hashes
```

3. Добавьте разрешение на чтение в созданную привилегию:

```
ipa privilege-add-permission "Read NTLM" --permissions="Read NT Hash Permission"
```

Через веб-интерфейс

1. Для создания разрешения перейдите в **IPA-сервер** → **Управление доступом на основе ролей** → **Разрешения** и нажмите **Добавить**. Заполните поля:

- **Имя разрешения** - укажите имя разрешения.
- **Предоставленные права** - выберите **read**.
- **Тип** - выберите **Пользователь**.
- **Действующие атрибуты** - выберите **ipaNTHash**.

2. Нажмите **Сохранить**.

3. Для создания привилегии перейдите в **IPA-сервер** → **Управление доступом на основе ролей** → **Привилегии** и нажмите **Добавить**:

4. В поле **Имя привилегии** укажите название, например, имя разрешения из шага 1. Нажмите **Добавить**.

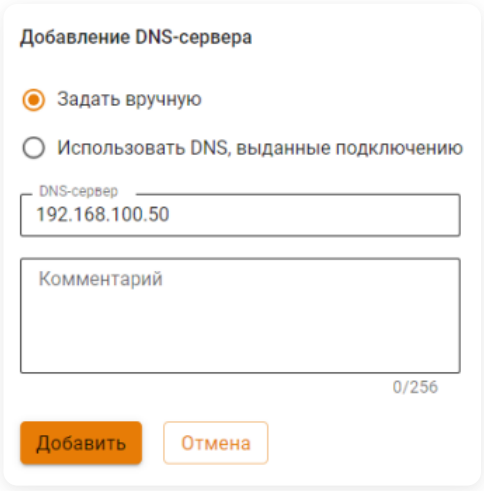
5. Откройте привилегию, созданную на шаге 4, и в блоке **Разрешения** нажмите **Добавить**.

6. Выберите из списка разрешение из шага 1 и подтвердите добавление:

Новую привилегию необходимо добавить в созданные ранее роли **CIFS servers** и **Organization units**, чтобы сервер NGFW Novum получил соответствующие права. Для этого откройте каждую роль и на вкладке **Привилегии** добавьте новую привилегию:

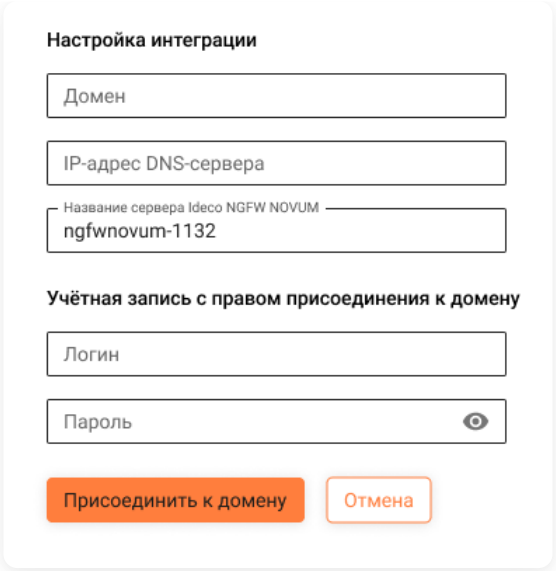
Ввод сервера NGFW Novum в домен FreeIPA

1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы** и добавьте IP-адрес устройства с установленной системой FreeIPA:



2. Перейдите в **Пользователи** → **Внешние каталоги** → **FreeIPA**.

3. Нажмите на кнопку **Добавить** и заполните поля:



Расшифровка полей

- **Домен** - полное имя домена, например, `mydomain.example`. Домен может содержать только латинские символы, цифры, подчеркивание, дефис и точку.
- **IP-адрес DNS-сервера** - IP-адрес устройства с установленной системой FreeIPA.
- **Название сервера Ideco NGFW Novum** - имя сервера, сгенерированное NGFW Novum или указанное вручную. Содержит буквенные символы (A-Z), цифры (0-9), а также не может начинаться или заканчиваться дефисом. Максимальное количество символов - 15.
- **Логин и пароль администратора** - данные не сохраняются на сервере и используются один раз для присоединения к домену. Пользователь может не быть администратором домена, но должен обладать правами на присоединение компьютеров к домену.

Если в таблице большое количество интеграций, воспользуйтесь кнопкой **Фильтры**.

Импорт пользователей

FreeIPA поддерживает импорт двух типов групп:

- Группа пользователей - содержит несколько пользователей FreeIPA.
- Подразделение - содержит дерево пользователей FreeIPA, обладающих определенным уровнем доступа.

Из-за особенностей взаимодействия с FreeIPA при импорте пользователей статус блокировки не передается в Ideco NGFW Novum. В результате учетная запись заблокированного в домене пользователя отображается в NGFW Novum как **активная**.

Однако авторизоваться в NGFW Novum под такой учетной записью невозможно - запрос отклоняет контроллер домена.

Для импорта пользователей выполните действия:

1. Перейдите в **Пользователи** → **Учетные записи** и создайте группу, в которую будут импортированы пользователи, нажав .

2. Перейдите на вкладку **FreeIPA**, выберите домен и созданную группу. Нажмите **Присоединить к домену**.

Импортированных пользователей можно использовать в качестве объектов для авторизации, настройки VPN-подключений, создания правил трафика (например, в **Межсетевом экране**).

В дальнейшем пользователи будут автоматически синхронизироваться с FreeIPA каждые 15 минут.

Пользователь может быть импортирован только в одну группу Ideco NGFW Novum. Если пользователь находится в нескольких группах FreeIPA, то попадет только в ту группу, которая была импортирована последней.

Рекомендуем при создании пользователей указывать в логине домен, например, `user@domain.freeipa`.

Аутентификация пользователей

При аутентификации пользователей проверка осуществляется средствами Kerberos.

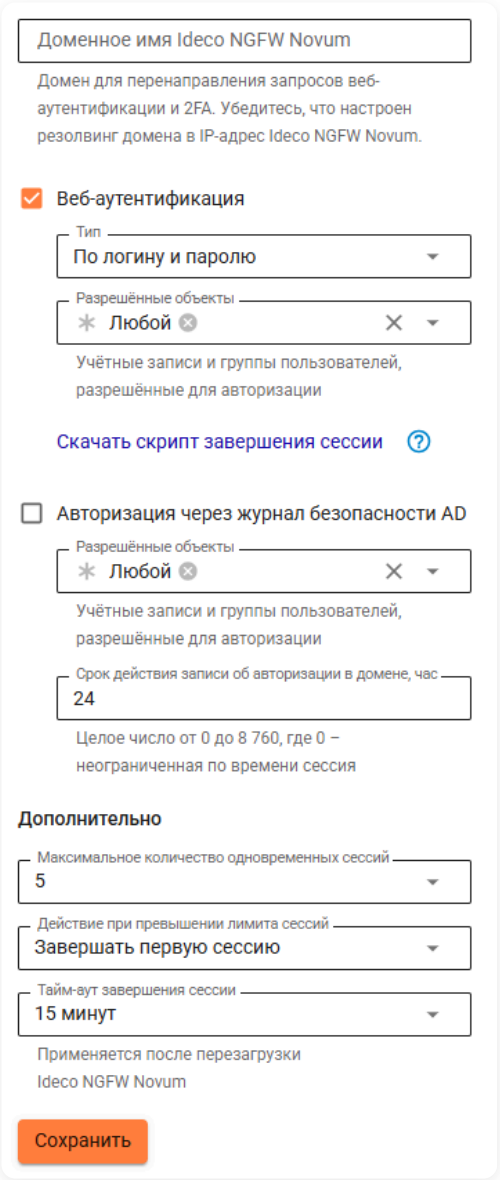
FreeIPA поддерживает два типа входа в систему:

- Вход по логину/паролю.
- Вход через SSO.

Настройка Ideco NGFW Novum

Для настройки аутентификации выполните действия:

1. Перейдите в **Пользователи** → **Авторизация** → **Настройки** и активируйте опцию **Веб-аутентификация**:



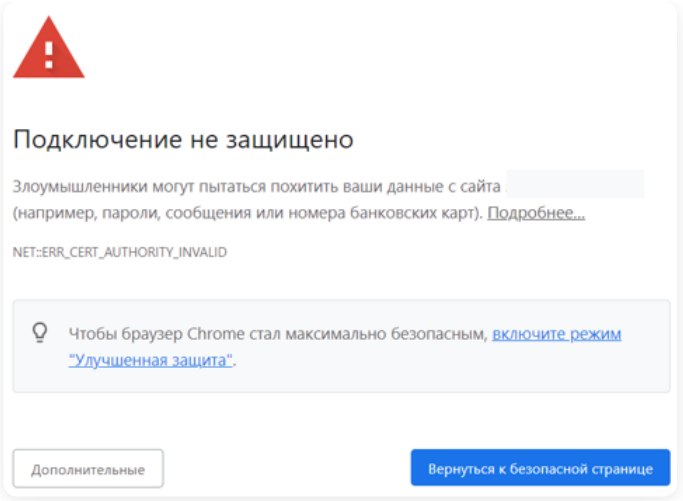
2. Выберите **Тип** входа в систему:

- **По логину и паролю** - вход по логину/паролю.
- **Через SSO** - вход через SSO.

3. Выберите разрешенные для авторизации учетные записи или группы пользователей в поле **Разрешенные объекты**.

Настройки в разделе **Дополнительно** описаны в статье.

После заполнения поля **Доменное имя Ideco NGFW Novum** и сохранения настроек будет выдан Let's Encrypt сертификат. Пользователь перенаправляется на окно авторизации, минуя страницу исключения безопасности:



Если сертификат для такого домена уже загружен в разделе **Сертификаты**, то будет использоваться загруженный сертификат, новый выдаваться не будет.

> Если NGFW Novum не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW Novum, то страница авторизации будет подписана корневым сертификатом NGFW Novum.

4. Настройте способы авторизации импортированных пользователей. Доступны:

- **Авторизация по IP и/или MAC** - подходит для пользователей с фиксированными IP- и/или MAC-адресами, на NGFW Novum адреса прописываются вручную каждому пользователю.
- **Авторизация по подсетям** - подходит, если не требуется регистрировать каждое устройство как отдельного пользователя NGFW Novum. Позволяет автоматически авторизовать большое количество устройств.
- **Авторизация по VPN** - подходит для аутентификации пользователей удаленных сетей.

Настройка клиентских машин для веб-аутентификации по SSO или NTLM

1. В зависимости от выбранного браузера выполните следующие действия:

Настройка браузера Yandex

1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.<имя_домена>",
  "AuthNegotiateDelegateAllowlist": "*.<имя_домена>"
}
```

2. Скачайте корневой сертификат.

3. В браузере Yandex перейдите в **Настройки** → **Системные** → **Управление сертификатами** → **Центры сертификации** → **Импорт** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:

Настройка браузера Google Chrome

1. Создайте файл **mydomain.json** в директории `/etc/opt/chrome/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.<имя_домена>",
  "AuthNegotiateDelegateAllowlist": "*.<имя_домена>"
}
```

2. Скачайте корневой сертификат.

3. В браузере Google Chrome перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:

Настройка браузера Chromium

1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и добавьте строки:

```
{
    "AuthServerAllowlist": "*.<имя_домена>",
    "AuthNegotiateDelegateAllowlist": "*.<имя_домена>"
}
```

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:

Настройка браузера Mozilla Firefox

1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

2. Введите параметр `security.enterprise_roots.enabled` и дважды кликните по блоку, чтобы значение изменилось на **True**, что позволит Firefox доверять системным сертификатам и авторизовывать пользователей при переходе на HTTPS-сайты.

3. В параметрах `network.automatic-ntlm-auth.trusted-uris` и `network.negotiate-auth.trusted-uris` укажите `<имя_NGFW.имя_домена>`.

1. Скачайте корневой сертификат.

2. В настройках браузера Mozilla Firefox перейдите в **Приватность и Защита** → **Защита** и выберите **Просмотр сертификатов**:

3. На вкладке **Центры сертификации** нажмите **Импортировать** и выберите скачанный с NGFW Novum сертификат.

4. Включите опции доверия для сертификата.
2. На машине клиента, введенной в домен FreeIPA, добавьте IP-адрес локального интерфейса и доменное имя Ideco NGFW Novum в файл `/etc/hosts`. Пример: `192.168.100.10 ngfw.domain.freeipa`.

RADIUS

Классический контекст | Высокопроизводительный контекст

> Интеграция с RADIUS-сервером обеспечивает аутентификацию пользователей, данные которых хранятся исключительно на RADIUS-сервере или в базах данных/каталогах, доступных для него.

Особенности интеграции

- Через RADIUS-сервер доступна аутентификация только VPN-пользователей NGFW Novum.
- Пользователи RADIUS могут авторизоваться с помощью Ideco Client без установки VPN-туннеля.
- Если учетные записи в службе каталогов Active Directory/Samba DC совпадают с учетными записями на RADIUS-сервере, авторизация будет производиться с использованием данных из службы каталогов.
- Ideco NGFW Novum поддерживает интеграцию с RADIUS-администраторами. Подробные инструкции по настройке описаны в статье Администраторы.

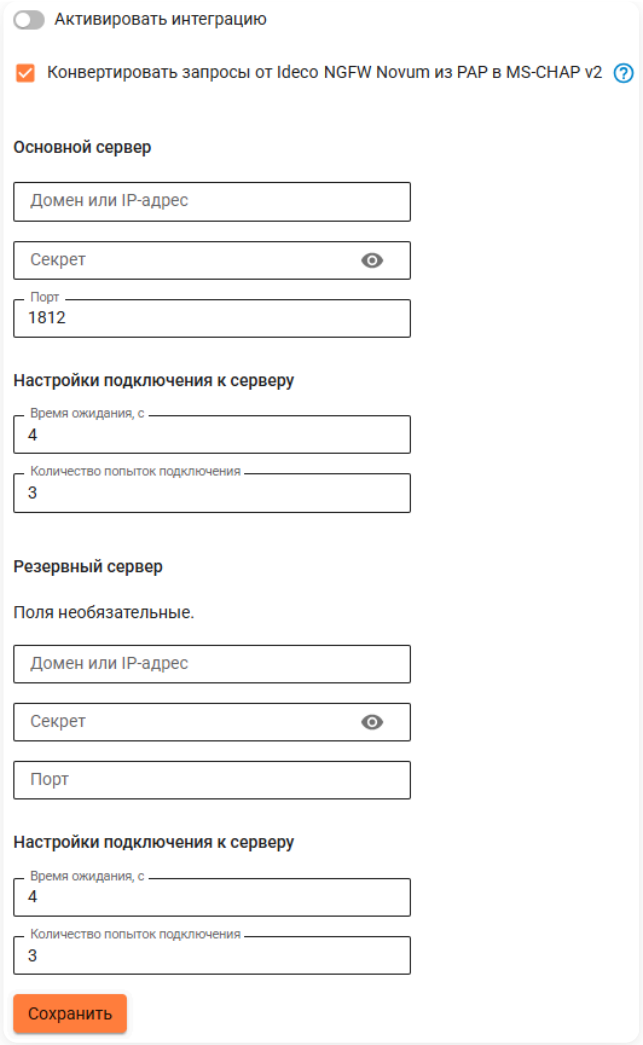
Настройка интеграции

Для настройки интеграции с RADIUS-сервером выполните действия:

1. Перейдите в **Пользователи** → **Внешние каталоги** → **RADIUS** и включите опцию **Активировать интеграцию**.

> При отключенной интеграции с RADIUS-сервером пользователи RADIUS не смогут аутентифицироваться на NGFW Novum.

2. Заполните поля:



- **Конвертировать запросы от Ideco NGFW Novum из PAP в MS-CHAP v2** - выключите опцию, только если необходимо настроить двухфакторную аутентификацию для пользователей RADIUS-сервера. Опция повышает безопасность и защиту:
  - От перехвата паролей между NGFW Novum и RADIUS-сервером.
  - Когда RADIUS-сервер поддерживает только MS-CHAP v2.
- **Основной сервер** - настройте основной RADIUS-сервер:
  - **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
  - **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
  - **Порт** - порт, по которому будет происходить подключение к серверу. Поменяйте при необходимости.
  - **Настройки подключения к серверу**:
    - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
    - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.
- **Резервный сервер** - настройте резервный RADIUS-сервер, если требуется:
  - **Домен или IP-адрес** - домен или адрес резервного RADIUS-сервера.
  - **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
  - **Порт** - порт, по которому будет происходить подключение к серверу. Поменяйте при необходимости.
  - **Настройки подключения к серверу**:
    - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
    - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.

Опция **Порт** влияет только на подключения через Ideco Client. Переключение опции никак не влияет на подключение пользователей по другим типам VPN.

3. Нажмите **Сохранить**.

Добавление пользователей в дерево пользователей Ideco NGFW Novum

1. При подключении пользователя к Ideco NGFW Novum происходит поиск пользователя в дереве пользователей:

- Если пользователь найден - запрос аутентификации сразу будет отправлен на RADIUS-сервер.
- Если пользователь не найден - Ideco NGFW Novum создаст пользователя и отправит запрос аутентификации на RADIUS-сервер.

2. При отсутствии группы **RADIUS** в Ideco NGFW Novum группа будет пересоздаваться при аутентификации пользователей RADIUS-сервера.

3. После аутентификации пользователь будет добавлен в группу **RADIUS** на Ideco NGFW Novum.

Группу и пользователей **RADIUS** можно использовать для создания правил фильтрации трафика и других задач.

Ограничения для группы и пользователей RADIUS:

- Разрешено удалять и переименовывать группу **RADIUS**.
- Запрещено менять параметры пользователя (в том числе поля **Имя** и **Комментарий**), за исключением опции **Запретить доступ**.
- Запрещено перемещать пользователей в другие группы.
- Запрещено перемещать других пользователей NGFW Novum в группу **RADIUS**.
- Запрещена настройка **IP** и **MAC** авторизации для пользователей группы.
- Недоступна авторизация пользователей группы в личном кабинете и веб-почте.

Двухфакторная аутентификация

Двухфакторная аутентификация для пользователей RADIUS-сервера доступна при авторизации через Ideco Client.

По умолчанию Ideco Client использует для аутентификации на внешнем сервере протокол MS-CHAP v2. При отключении опции **Конвертировать запросы от Ideco NGFW Novum из PAP в MS-CHAP v2** запросы аутентификации от Ideco Client к внешнему серверу будут выполняться по протоколу PAP. Для всех прочих VPN-подключений продолжает работать только MS-CHAP v2 независимо от настройки.

Если необходимо обеспечить для пользователей RADIUS-сервера двухфакторную аутентификацию на этом же сервере:

1. В веб-интерфейсе Ideco NGFW Novum в **Пользователи** → **RADIUS** отключите опцию **Конвертировать запросы от Ideco NGFW Novum из PAP в MS-CHAP v2**. Проверку второго фактора с использованием MS-CHAP v2 обеспечить невозможно.

2. Настройте RADIUS-сервер на работу с протоколом PAP.

3. Настройте на RADIUS-сервере механизм двухфакторной аутентификации. Настраивать 2FA на Ideco NGFW Novum не нужно.

При настройке двухфакторной аутентификации на RADIUS-сервере поле сообщения пользователю **Reply-Message** ограничено 253 байтами. Поэтому максимальная длина сообщения ограничена:

- Для латиницы - 253 символа.
- Для кириллицы - 137 символов.

LDAP-фильтры

Классический контекст | Высокопроизводительный контекст

Настройка объектов для группировки пользователей каталога LDAP (Lightweight Directory Access Protocol).

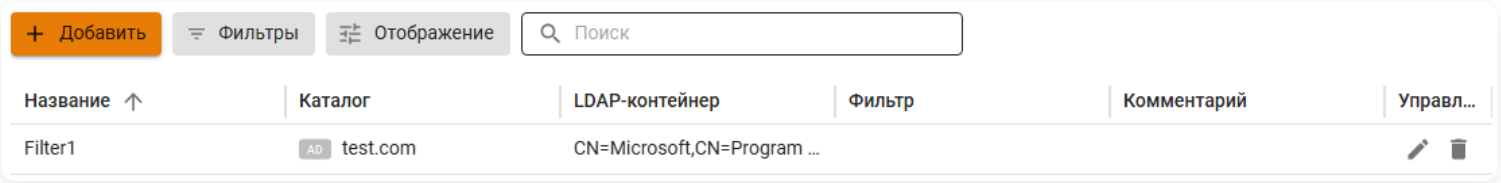
LDAP (Lightweight Directory Access Protocol) - протокол быстрого доступа к каталогам, позволяющий получать и принимать через сеть данные из каталогов с иерархической структурой. LDAP-фильтры - один из способов выборки учетных записей из каталога AD наряду с группами безопасности. С помощью фильтров можно отобрать нужные учетные записи для применения в правилах.

LDAP-фильтры применяются только для каталога Active Directory.

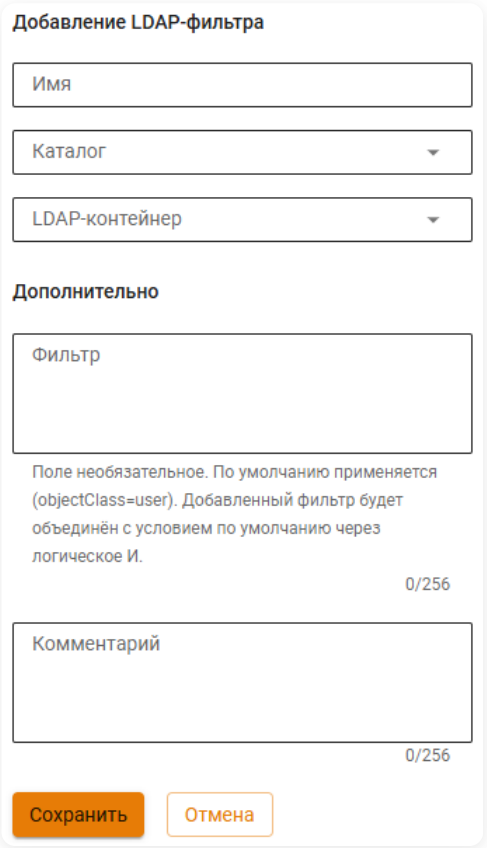
Рекомендуем использовать LDAP-фильтры в правилах только если невозможна настройка с помощью групп безопасности.

Добавление и редактирование LDAP-фильтров

Для добавления LDAP-фильтра перейдите в **Пользователи** → **Внешние каталоги** → **LDAP-фильтры** и нажмите **Добавить**:



1. Заполните форму:



Расшифровка полей

- **Имя** - укажите уникальное название LDAP-фильтра, не более 128 символов.

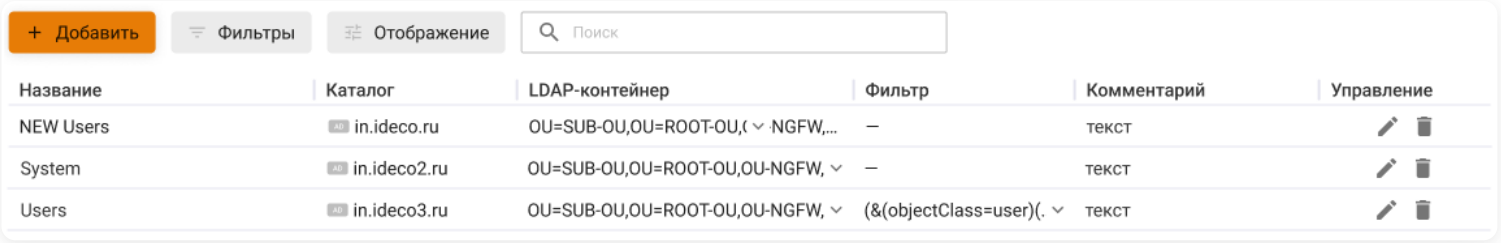
- **Каталог** - выберите каталог AD.
- **LDAP-контейнер** - выберите группу из списка контейнеров каталога.
- **Фильтр** - необязательное поле. Всегда используется `(objectClass=user)` (все пользователи). Фильтр, введенный администратором в поле, объединяется с `(objectClass=user)` через оператор `И`.
- **Комментарий** - необязательное поле.

Примеры фильтров

- `(!userAccountControl:1.2.840.113556.1.4.803:=2)` - только включенные пользователи.
- `(givenName=*)(sn=*)` - все пользователи с заполненными именем и фамилией.
- `(memberOf:1.2.840.113556.1.4.1941:=cn=Test,ou=East,dc=Domain,dc=com)` - все пользователи, принадлежащие группе безопасности `Test`, которая находится в подразделении `East` домена `domain.com`.

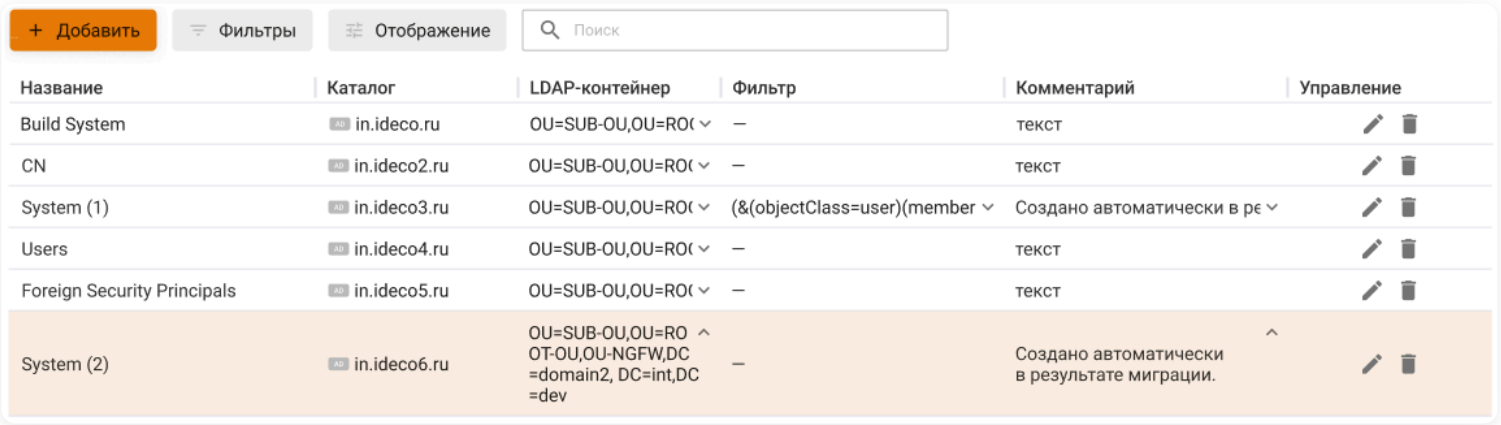
2. Нажмите **Добавить**.

Добавленные LDAP-фильтры отображаются в таблице. Для редактирования записи нажмите :



Миграция LDAP-фильтров

При обновлении Ideco NGFW Novum на версию 21 импортированные ранее в дерево LDAP-группы AD автоматически мигрируют в **LDAP-фильтры**:

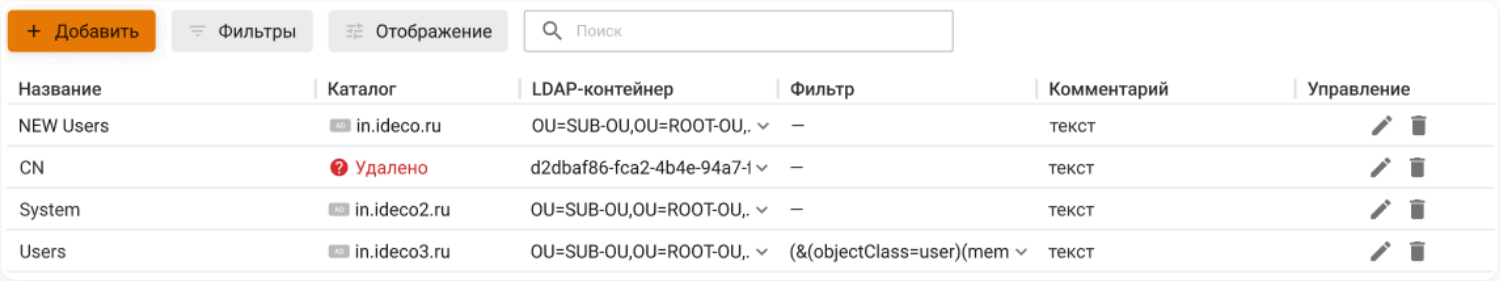


Особенности миграции:

- Если в дерево были импортированы LDAP-группы AD с одинаковым именем, то при миграции в **LDAP-фильтры** к именам фильтров будет добавлен сквозной номер в скобках.
- Автоматически созданные LDAP-фильтры имеют комментарий **Создано автоматически в результате миграции**.

Как восстановить LDAP-фильтры при удалении каталога

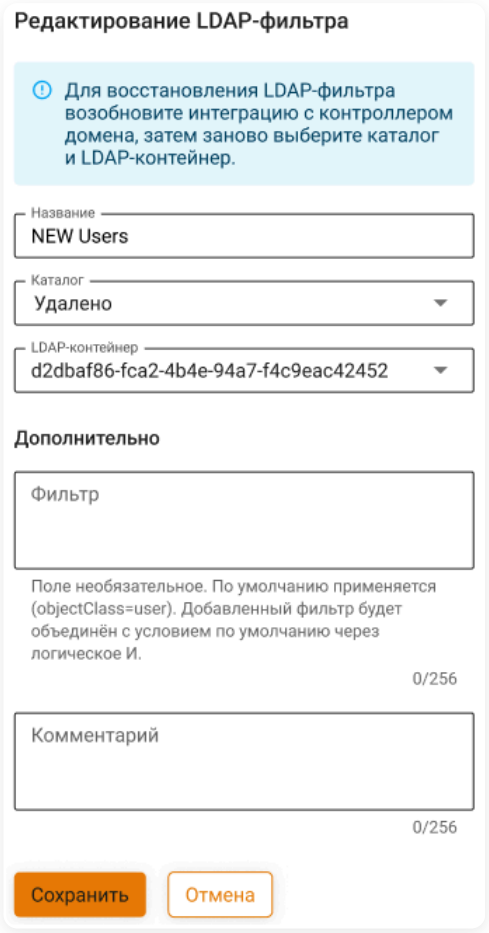
Если действующая интеграция с доменом удалена, каталог LDAP-фильтров, относящийся к такой интеграции, помечается алиасом **Удалено**:



Для восстановления LDAP-фильтра:

1. Восстановите интеграцию с контроллером домена AD. Новая интеграция будет иметь новый ID.

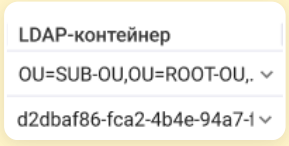
2. Отредактируйте LDAP-фильтр, выбрав каталог и LDAP-контейнер:



3. Нажмите **Сохранить**.

Повторный выбор LDAP-фильтра для возобновления работы правил не требуется.

Если связи с контроллером домена нет или не успела пройти синхронизация, то в поле **LDAP-контейнер** отобразится GUID группы вместо Distinguished Name (DN):



- `OU=SUB-OU,OU=ROOT-OU,DC=test,DC=com` - DN.
- `d2dbaf86-fca2-4b4e-94a7-f305e82c3301` - GUID.

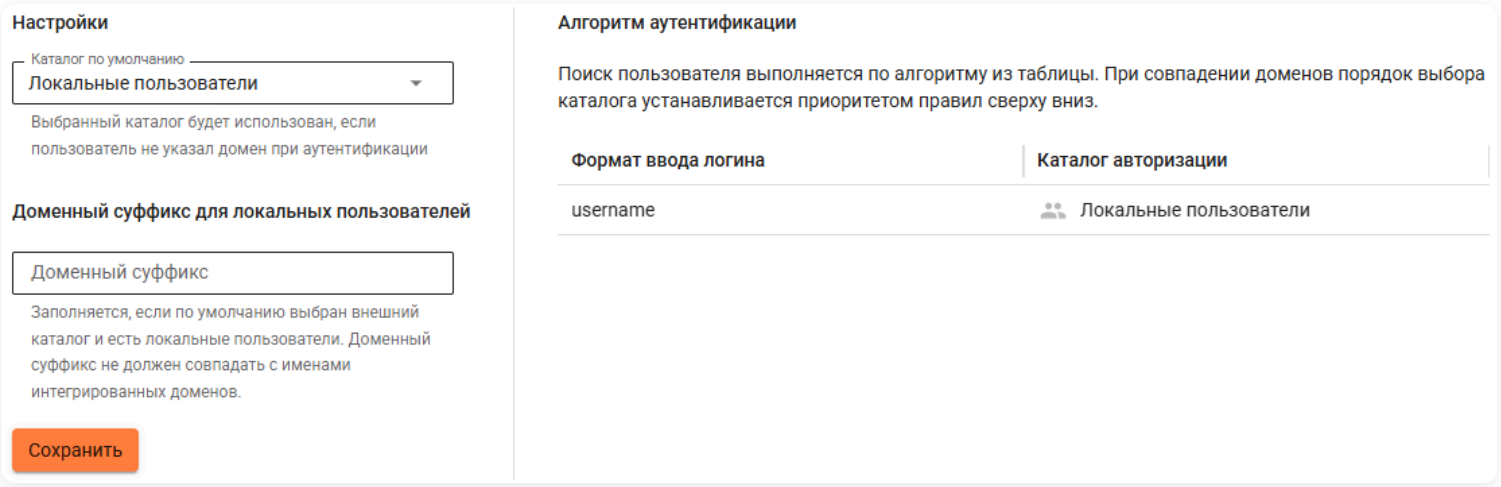
Аутентификация

Классический контекст | Высокопроизводительный контекст | API

Перейдите во вкладку **Основное** для настройки каталогов аутентификации пользователей Ideco NGFW Novum.

Настройки

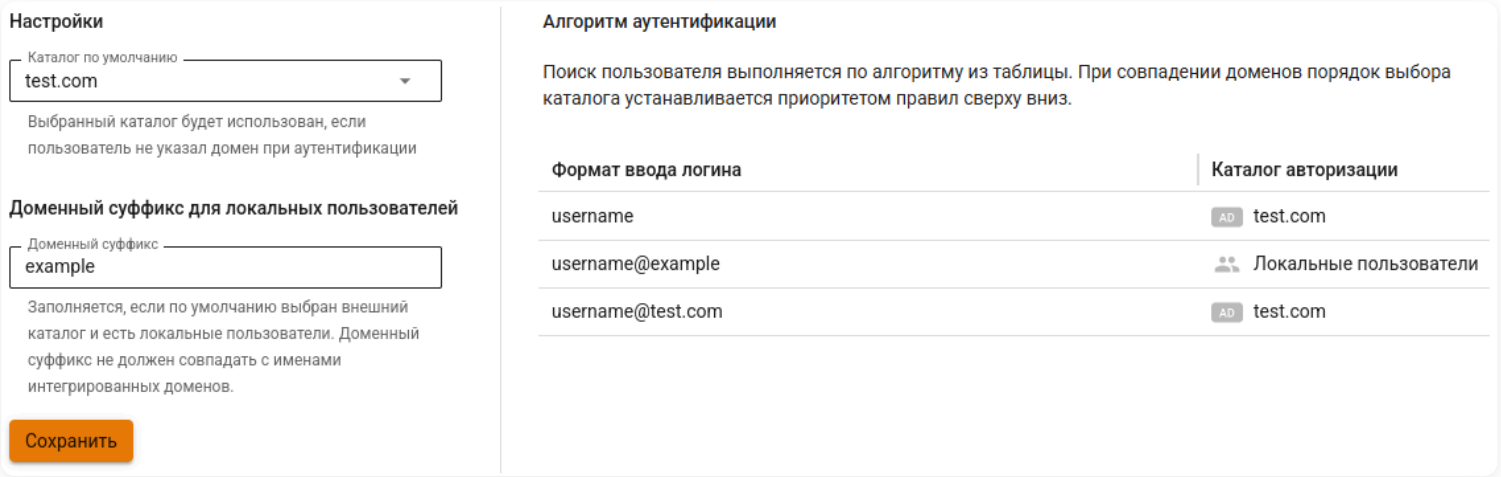
Укажите **Каталог по умолчанию**:



- **Каталог по умолчанию** - определяет каталог для аутентификации пользователей без указания домена. Такой подход позволяет избежать ошибок аутентификации при наличии пользователей с одинаковыми логинами в разных каталогах. Доступные каталоги: локальные пользователи, домен AD/ALD/FreeIPA, интеграция с RADIUS. При интеграции с несколькими доменами AD/ALD/FreeIPA в качестве **Каталога по умолчанию** доступен выбор только одного из них.

Доменный суффикс для локальных пользователей

Введите условный домен, который локальные пользователи будут указывать вместе с логином для аутентификации. Настройка нужна при наличии локальных пользователей и при выборе в качестве **Каталога по умолчанию** домена AD/ALD/FreeIPA или RADIUS. Например, при суффиксе `example` локальный пользователь вводит логин в формате `username@example`:



Условный домен нужен только для выбора каталога **Локальные пользователи** при аутентификации. В ходе поиска по каталогу учитывается только логин пользователя, доменный суффикс отбрасывается.

Алгоритм аутентификации

Описанный ниже алгоритм применяется при аутентификации **по логину и паролю**, когда каталог определяется по доменному суффиксу, указанному в логине после `@`, или по **Каталогу по умолчанию** при отсутствии доменного суффикса в логине.

При **SSO-аутентификации** каталог выбирается иначе - среди интеграций с AD и ALD Pro, без учета **Каталога по умолчанию** и доменного суффикса. Подробнее в разделе **Выбор каталога при SSO-аутентификации**.

В таблице **Алгоритм аутентификации** перечислены все доступные каталоги и формат ввода логина для каждого каталога, включая UPN-суффиксы для Active Directory в порядке добавления.

Не рекомендуется использовать одинаковые наименования доменов в разных интеграциях. При совпадении доменов выбор каталога для поиска пользователя выполняется в приоритете:

1. Локальный каталог, если добавлен доменный суффикс.

2. Каталог AD.

3. Каталог ALD.

4. Каталог FreeIPA.

5. Каталог RADIUS.

Если при аутентификации пользователя не указан домен, поиск осуществляется только в **Каталоге по умолчанию**. Если указан неизвестный Ideco NGFW Novum домен, поиск выполняется в каталоге RADIUS при наличии интеграции.

Примеры настроек при использовании нескольких каталогов одновременно

Аутентификация локальных пользователей без указания домена

1. В поле **Каталог по умолчанию** выберите значение **Локальные пользователи**.

2. Поле **Доменный суффикс для локальных пользователей** можете оставить без изменений.

При такой настройке аутентификация пользователей AD, ALD, FreeIPA и RADIUS выполняется только с указанием домена. Доменный суффикс для RADIUS настраивается только на RADIUS-сервере.

Аутентификация пользователей из каталога AD/ALD/FreeIPA без указания домена

1. В поле **Каталог по умолчанию** выберите конкретный домен AD/ALD/FreeIPA.

2. В поле **Доменный суффикс для локальных пользователей** укажите условный домен, который локальные пользователи будут использовать для аутентификации. Настройка актуальна при наличии локальных пользователей.

Действие настройки:

- Пользователи выбранного каталога могут аутентифицироваться без указания домена или с указанием домена AD/ALD/FreeIPA.
- Аутентификация пользователей в каталогах AD/ALD/FreeIPA, не выбранных как **Каталог по умолчанию**, осуществляется только с указанием домена.
- Локальные пользователи аутентифицируются с указанием условного домена, настроенного в поле **Доменный суффикс для локальных пользователей**.
- Аутентификация пользователей RADIUS осуществляется только с указанием домена. Доменный суффикс для RADIUS настраивается только на RADIUS-сервере.

Аутентификация пользователей RADIUS без указания домена

1. В поле **Каталог по умолчанию** выберите RADIUS.

2. В поле **Доменный суффикс для локальных пользователей** укажите условный домен, который локальные пользователи будут использовать для аутентификации. Настройка актуальна при наличии локальных пользователей.

Действие настройки:

- Пользователи RADIUS могут аутентифицироваться без указания домена или доменом, используемым в RADIUS.
- Аутентификация пользователей AD/ALD/FreeIPA осуществляется только с указанием домена.
- Локальные пользователи аутентифицируются с указанием условного домена, настроенного в поле **Доменный суффикс для локальных пользователей**.

При настройке авторизации в почте проверьте, чтобы основной или дополнительный почтовый домен, указанный в **Почтовый релей** → **Основные настройки**, совпадал с доменом **Каталога авторизации** для успешной аутентификации. В противном случае аутентификация

будет выполняться через **Каталог по умолчанию**: если пользователь есть в каталоге, аутентификация пройдет успешно по логину, указанному до `@`.

Настройку **Доменный суффикс для локальных пользователей** можно использовать совместно с настройкой почтового домена, чтобы для этого почтового домена использовался каталог **Локальные пользователи**.

Двухфакторная аутентификация

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Двухфакторная аутентификация**: `ideco-web-authd`.

Список служб для других разделов доступен по ссылке.

Двухфакторная аутентификация позволяет аутентифицировать локальных и внешних пользователей (в том числе для VPN и для личного кабинета) с использованием второго фактора.

В Ideco NGFW Novum реализовано четыре типа двухфакторной аутентификации:

- **TOTP-токен** - сканированием QR-кода или с помощью токена.
- **SMS Aero** - при помощи ввода кода из SMS.
- **Мультифактор** - путем подтверждения личности в приложении.
- **RADIUS-серверы** - через RADIUS-серверы. Тип двухфакторной аутентификации работает независимо от интеграции с RADIUS.

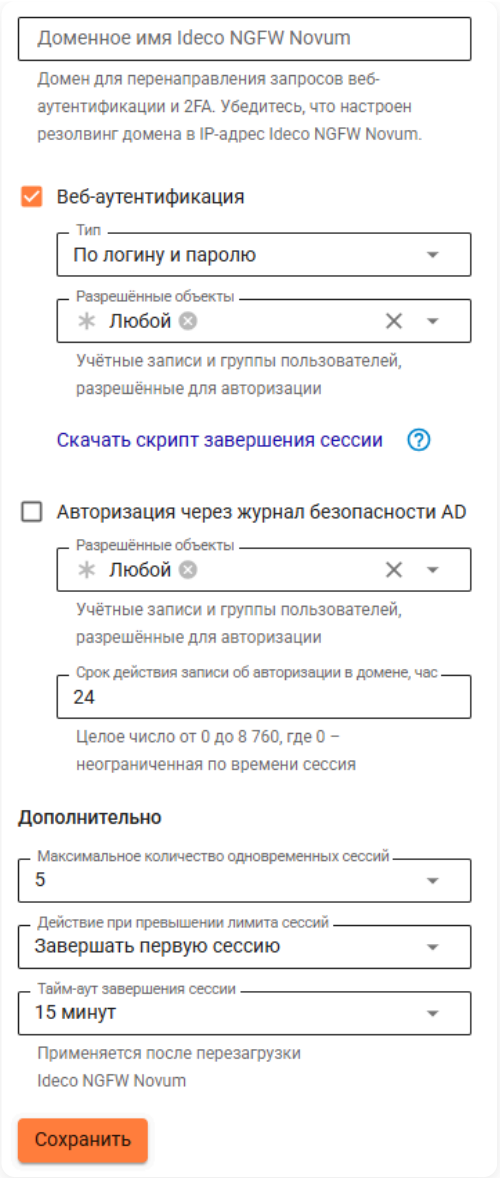
Настройка двухфакторной аутентификации для администраторов Ideco NGFW Novum производится в разделе **Управление сервером** → **Администраторы** → **Двухфакторная аутентификация**.

Для входа в личный кабинет Ideco NGFW Novum с использованием **Мультифактора** необходим доступ в интернет.

Настройки Ideco NGFW Novum с разными типами аутентификации

Для работы двухфакторной аутентификации выполните действия:

1. Перейдите в **Пользователи** → **Авторизация** и включите веб-аутентификацию:



2. Укажите домен Ideco NGFW Novum в поле **Доменное имя Ideco NGFW Novum**, чтобы на сервер перенаправлялись запросы двухфакторной аутентификации.

3. Настройте VPN-подключение в **Пользователи** → **VPN-подключения** → **Основное**, воспользовавшись инструкцией.

4. Перейдите в **Пользователи** → **Аутентификация** → **Двухфакторная аутентификация**. Включите необходимые типы аутентификации:

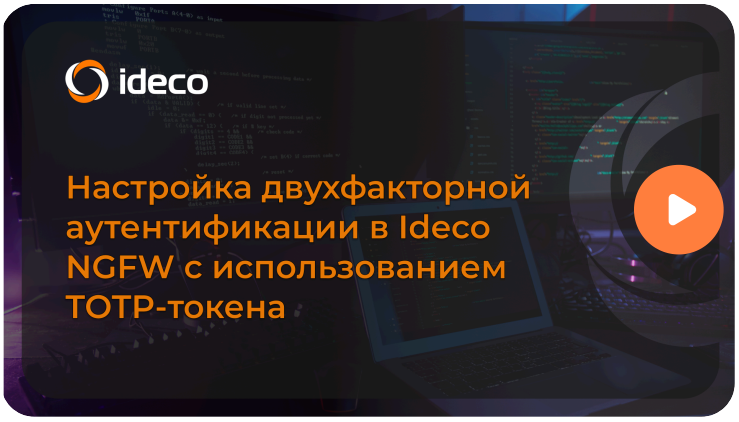
TOTP-токен

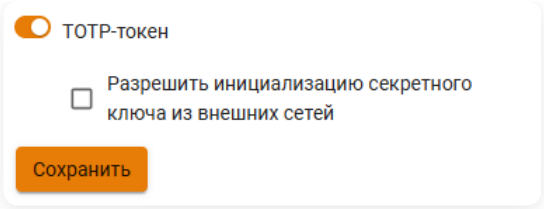
Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE VK Видео





- **Включить** - опция включает TOTP-аутентификацию.
- **Разрешить инициализацию секретного ключа из внешних сетей** - включение опции разрешает пользователям сканировать QR-код в личном кабинете при подключении из внешних сетей.

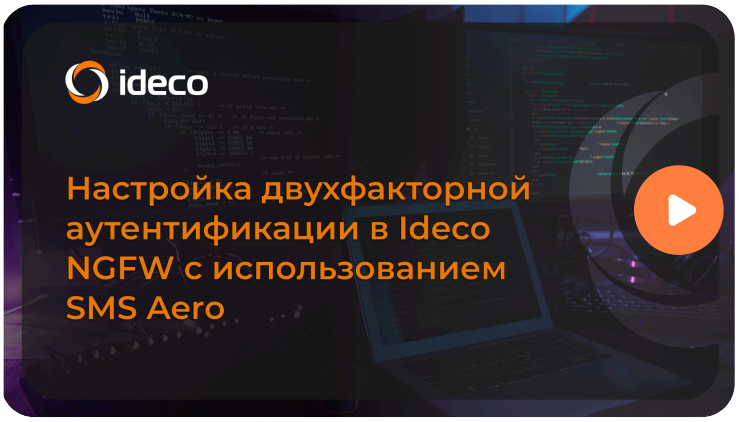
SMS Aero

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

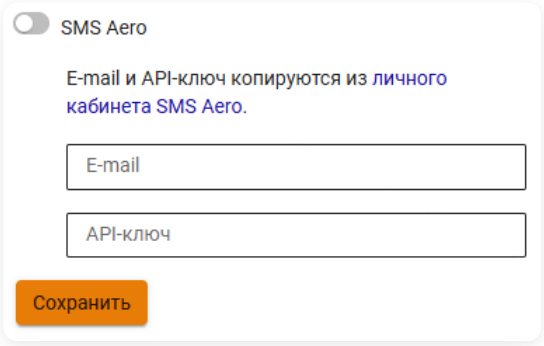
Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Предварительно зарегистрируйтесь в личном кабинете SMS Aero.

1. Введите **e-mail** и **API-ключ** от личного кабинета SMS Aero:



API-ключ можно найти в разделе **Настройки → API и SMPPI**.

2. Если требуется, включите опции:

- **Задать имя отправителя вручную** - рекомендуем использовать, если имя отправителя недоступно.
- **Добавить текст сообщения** - введите текстовое сообщение, которое будет отображаться для получателя. Если опцию не использовать, будет отправлен только код.

3. Нажмите **Сохранить**.

При необходимости можно проверить настройки второго фактора, введя **Номер для тестового СМС** и нажав **Отправить СМС**.

Мультифактор

Видеоинструкция



Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

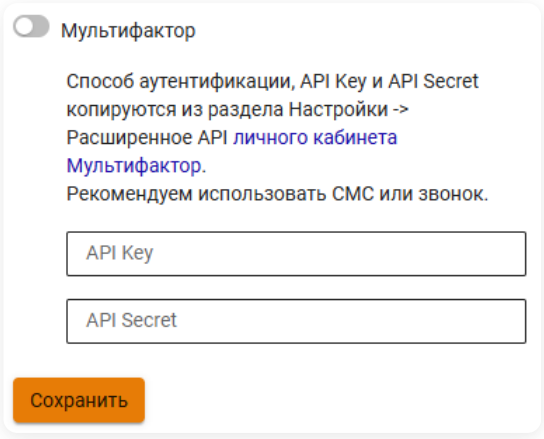
YouTube | RUTUBE | VK Видео

Помимо приложения Multifactor для аутентификации можно использовать Telegram, Яндекс.Ключ, Биометрию и U2F. Подробное описание регистрации и аутентификации этими методами доступно в документации Multifactor.

Предварительно зарегистрируйтесь в системе управления Мультифактором, установите приложение Multifactor и активируйте, отсканировав QR-код.

1. Скопируйте значение полей в личном кабинете пользователя Multifactor в разделе **Настройки** → **Расширенное API** → **Включить API**.

2. Заполните **API Key** и **API Secret**:



3. Нажмите **Сохранить**.

Для дальнейшей аутентификации пользователям потребуется установить и настроить приложения, указанные администратором в настройках группы. Корректировать способы аутентификации для пользователей можно в личном кабинете Multifactor, в разделе **Группы** → **Параметры** → **Редактировать**.

RADIUS-сервер

При необходимости можно настроить несколько RADIUS-серверов для двухфакторной аутентификации. Для каждого выполните шаги:

1. Нажмите **Добавить**.

2. Заполните поля:



- **Название** - уникальное название способа 2FA, которое будет использоваться в настройке доступа. Запрещены названия `TOTP-токен`, `Мультифактор` и `SMS Aero`.
- **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
- **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
- **Порт** - порт, по которому будет происходить подключение к серверу.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
  - **Количество попыток подключения** - число попыток отправки запроса на RADIUS-сервер. В диапазоне от 1 до 5. По умолчанию 3.
- **Режим запроса к RADIUS** - режим запроса на аутентификацию от Ideco NGFW Novum:
  - **Содержимое запроса**:
    - **Логин** - передача в запросе на RADIUS-сервер только логина, пароль остается пустым. В настройках RADIUS-сервера должен быть прописан пропуск проверки пароля в первом запросе. RADIUS-сервер должен проверять только логин для идентификации пользователя.
    - **Логин и OTP-код** - передача логина и OTP-кода. Установите, если RADIUS-сервер не поддерживает запрос без пароля.
  - **Сообщение при вводе OTP-кода** - сообщение, которое увидит пользователь при двухфакторной аутентификации в режиме передачи **Логин и OTP-код**. Должно содержать информацию для пользователя с конкретизацией, откуда он должен взять OTP-код. В режиме передачи **Логин** поле не используется, выводится сообщение от RADIUS-сервера (Reply-Message).
- **Комментарий** - необязательное поле.

3. Нажмите **Сохранить**.

Поддерживается взаимодействие с RADIUS-сервером только по протоколу PAP (Password Authentication Protocol).

5. Разрешите доступ по VPN нужным группам пользователей в **Пользователи** → **VPN-подключения** → **Доступ по VPN**, воспользовавшись инструкцией.

При отключении типа аутентификации, который используется в таблице **Доступ по VPN**, будет выведено предупреждение **Используется для доступа по VPN**. При этом аутентификация пройдет без второго фактора.

Настройка аутентификации на пользовательских устройствах

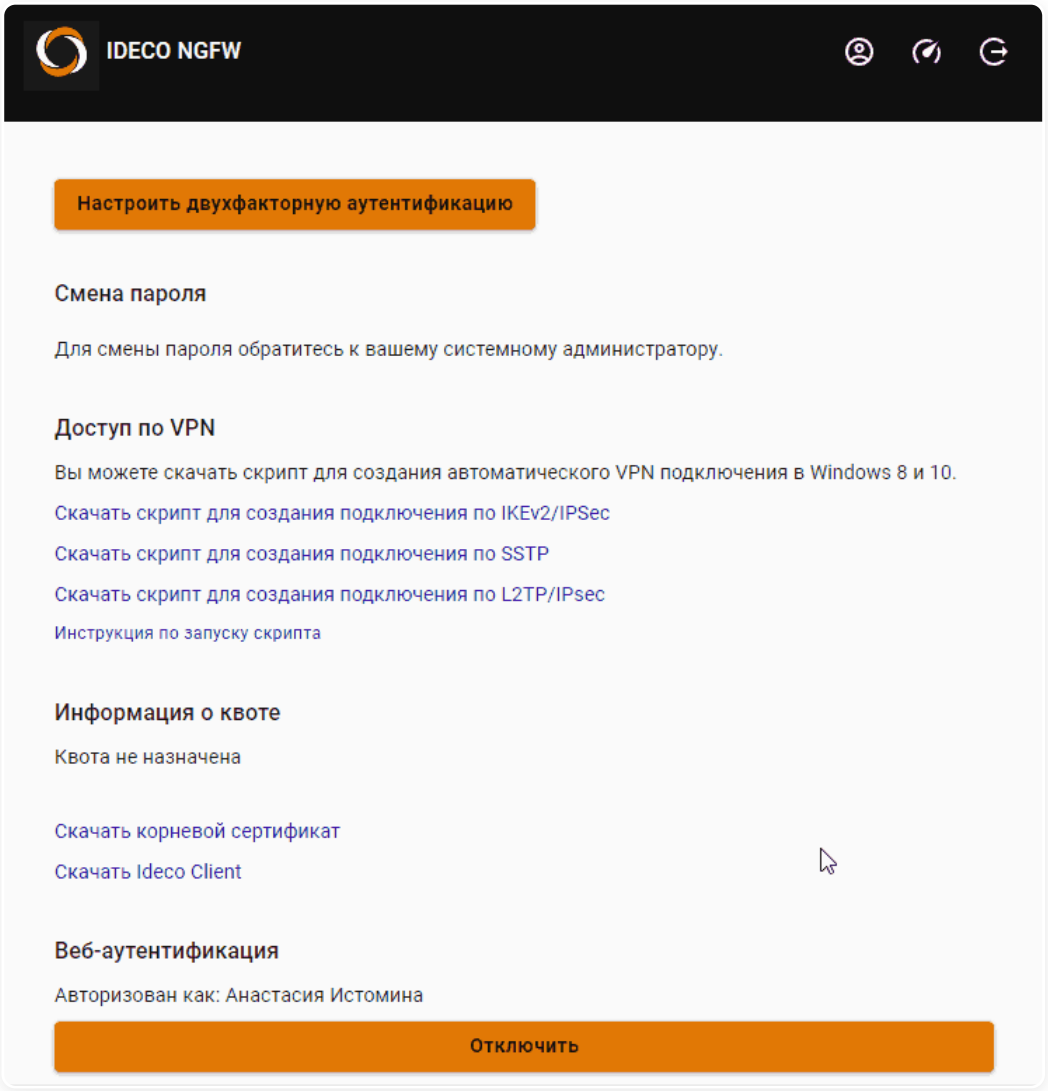
Для настройки двухфакторной аутентификации на устройстве пользователя воспользуйтесь инструкциями:

TOTP-токен

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Войдите в личный кабинет NGFW, указав логин и пароль пользователя.

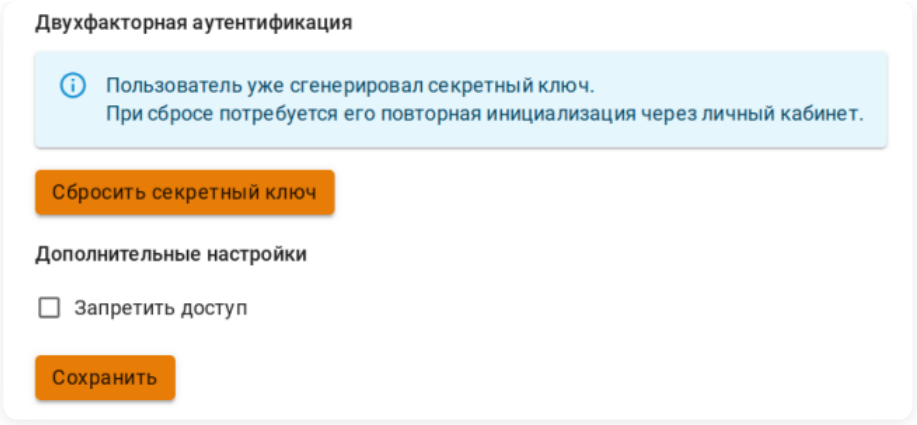
3. Нажмите кнопку **Настроить двухфакторную аутентификацию** и выберите **Сгенерировать QR-код**:



4. Войдите в приложение для аутентификации (например, Яндекс ID, Google Authenticator или Microsoft Authenticator), отсканируйте QR-код или введите секретный ключ, который находится под QR-кодом. При вводе ключа выберите тип ключа **По времени**. Если выбрать тип **По счетчику**, то пользователь не сможет пройти аутентификацию.

Если вернуться в личный кабинет, не отсканировав QR-код, то повторно QR-код появится только после сброса секретного ключа в карточке пользователя.

Чтобы сбросить секретный ключ, перейдите в **Пользователи** → **Учетные записи**. Выберите нужного пользователя и нажмите **Сбросить секретный ключ**:



5. Подключитесь к VPN и откройте любой сайт, не использующий **HSTS** (например, neverssl.com). В появившемся поле введите код, который получили в приложении:

Особенности использования TOTP-токена:

- Для корректной работы необходимо, чтобы время на Ideco NGFW Novum и устройстве пользователя было синхронизировано с точностью до минуты.
- Если секретный ключ был сброшен во время аутентификации пользователя и пользователь не смог пройти аутентификацию, то необходимо удалить сессию пользователя в разделе **Мониторинг → Сессии пользователей**. Сессия будет автоматически завершена по истечении десяти минут бездействия.

SMS Aero

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Если требуется использовать подключение только для ресурсов подключаемой сети, убедитесь, что настройки VPN-подключения соответствуют требованиям:

Для Windows 10:

- Откройте параметры и перейдите в **Сеть и Интернет → VPN → Настройка параметров адаптера**.
- Нажмите правой кнопкой мыши по созданному подключению и выберите **Свойства**.
- Перейдите на вкладку **Сеть**.
- Нажмите на **IP версии 4 (TCP/IPv4) → Свойства → Дополнительно**.
- Снимите флаг с пункта **Использовать основной шлюз в удаленной сети**.
- Нажмите **ОК**.

Для Ubuntu:

- Перейдите в **Настройки → Сеть**.
- Откройте настройки VPN-подключения.
- Перейдите на вкладку **IPv4**.
- Установите флаг в пункте **Использовать это подключение для ресурсов этой сети**.

3. Включите созданное VPN-подключение.

4. Перейдите в браузер, откроется страница аутентификации:

5. Нажмите **Отправить код подтверждения**. На номер телефона, указанный в учетной записи, придет SMS с кодом:

- Если номер телефона в карточке пользователя отсутствует, то на странице аутентификации появится предупреждение:

- Если номер телефона сохранен, то на указанный номер телефона поступит SMS. Введите код из SMS и нажмите **Подтвердить**:

- Если код введен неверно, то появится соответствующее предупреждение:

- Если код введен верно, то появится окно:

Для настройки таймкодов отправки сообщений перейдите в личный кабинет SMS Aero на вкладку **Настройки** и переведите опцию **Исключать множественную отправку** в положение **Включен**. Затем введите лимит и период отправки сообщений:

Мультифактор

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Включите созданное VPN-подключение.

3. При переходе в браузер откроется страница аутентификации:

4. После нажатия **Далее** появится страница с предложением установить приложение на устройство пользователя. Если приложение установлено, нажмите **Далее**.

5. Отсканируйте QR-код или откройте ссылку, которая появится на экране.

6. Нажмите **Выполнить вход**:

7. В окне **Двухфакторная аутентификация** выберите способ аутентификации:

8. В зависимости от выбранного способа подтвердите вход.

RADIUS-сервер

В отличие от остальных способов RADIUS-сервер при настройке двухфакторной аутентификации работает как посредник. RADIUS-сервер только передает код подтверждения в сервис 2FA, а сервис 2FA проверяет его корректность. Настройка второго фактора осуществляется в личном кабинете выбранного сервиса двухфакторной аутентификации. Для настройки используйте документацию соответствующего сервиса.

В зависимости от того, какая система 2FA используется, после ввода логина и пароля в NGFW Novum инициируется запрос на авторизацию через RADIUS-сервер:

- Если от сервера не ожидается код (например, при использовании биометрии), пользователь авторизуется.
- Если от сервера ожидается код подтверждения, введите код и нажмите **Подтвердить**:

- Если доступ запрещен или ответ от RADIUS-сервера не получен, появится окно:

> Предпочтительными являются современные системы с беспарольной аутентификацией (FIDO2-ключи, биометрия). Рекомендуем увеличить время ожидания от RADIUS-сервера в случае использования таких систем.

2FA при помощи БИТ.Аутентификатор

1. Установите клиентский портал БИТ.Аутентификатор по инструкции.

2. В клиентском портале БИТ.Аутентификатор в разделе **Домены проекта** создайте домен. В поле **Название** укажите домен Active Directory и получите API-ключ.

3. Перейдите в раздел **Настройки** и настройте портал на работу с сервером Active Directory и Ideco NGFW Novum, заполнив поля:

- **Служба каталогов** - выберите Active Directory.
- **Адрес службы** - укажите IP-адрес DNS-сервера Active Directory.
- **DN сервисного пользователя** - укажите Distinguished Name учетной записи, от имени которой система будет подключаться к Active Directory для выполнения поиска и проверки данных.
- **Пароль** - укажите пароль Distinguished Name учетной записи.

- **Администраторы** - укажите учетные записи или группы Active Directory, которые будут обладать правами администраторов.
- **Адрес портала** - укажите домен Active Directory.
- **Разрешенные способы проверки второго фактора** - выберите способы проверки второго фактора.
- **Секрет RADIUS** - укажите секрет RADIUS. Поле должно соответствовать секрету RADIUS в Ideco NGFW Novum.

4. Настройте интеграцию Active Directory и Ideco NGFW Novum по инструкции.

5. В Ideco NGFW Novum перейдите в **Пользователи** → **Внешние каталоги** → **Active Directory/Samba DC** и заполните поля:

- **Домен или IP-адрес** - укажите IP-адрес сервера БИТ.Аутентификатор.
- **Секрет** - укажите секрет RADIUS из настроек клиентского портала БИТ.Аутентификатор.
- **Порт** - порт, по которому будет происходить подключение к серверу.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
  - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.

6. Нажмите **Сохранить** и проверьте соединение.

7. Перейдите в **Аутентификация** → **Двухфакторная аутентификация** → **RADIUS-серверы**, нажмите **Добавить** и заполните поля:

- **Название** - укажите название сервера Active Directory.
- **Домен или IP-адрес** - укажите IP-адрес сервера БИТ.Аутентификатор.
- **Порт** - порт, по которому будет происходить подключение к серверу.
  - **Настройки подключения к серверу**:
    - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
    - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.

8. На клиентском портале БИТ.Аутентификатор в разделе **Ресурсы** добавьте ресурс:

- **Название** - укажите название сервера Active Directory.
- **Описание** - необязательное поле.
- **IP-адреса (через ;)** - укажите IP-адрес Ideco NGFW Novum.
- **Разрешен вход (группы через ;)** - пользователи домена.
- **Проверять второй фактор, если настроен (группы через ;)** - пользователи домена.
- **Требовать второй фактор (группы через ;)** - пользователи домена.
- **Второй фактор выключен (группы через ;)** - оставьте поле пустым.
- **LDAP порт** - оставьте значение **Нет**.
- **LDAPS порт** - оставьте значение **Нет**.
- **RADIUS порт** - должен соответствовать полю **Порт** настроек RADIUS-сервера в Ideco NGFW Novum. По умолчанию: `1812`.

9. Создайте VPN-подключение.

10. На вкладке **Доступ по VPN** в поле **Способ 2FA** выберите сервер RADIUS, созданный на шаге 7.

11. Установите VPN-соединение и пройдите проверку второго фактора одним из выбранных способов на шаге 3.

Алгоритм двухфакторной аутентификации с RADIUS-сервером

Алгоритм двухфакторной аутентификации с RADIUS-сервером при любом типе подключении зависит от выбранного режима запроса - **Логин** или **Логин и OTP-код**.

По логину

1. Пользователь указывает логин и пароль и инициирует подключение.

2. NGFW Novum проверяет логин и пароль.

3. При успешной проверке NGFW Novum отправляет на RADIUS-сервер **Access-Request** с логином и пустым паролем.

> RADIUS-сервер должен быть настроен на пропуск проверки пароля и использовать первый запрос только для идентификации

пользователя по логину.

4. После успешной идентификации RADIUS-сервер выбирает тип второго фактора согласно политикам и запрашивает код у пользователя.

5. Пользователь вводит код второго фактора.

6. RADIUS-сервер проверяет второй фактор и завершает аутентификацию.

По логину и OTP-коду

1. Пользователь указывает логин и пароль и инициирует подключение.

2. NGFW Novum проверяет логин и пароль.

3. При успешной проверке NGFW Novum запрашивает у пользователя ввод кода из приложения для аутентификации.

4. NGFW Novum отправляет на RADIUS-сервер **Access-Request**, содержащий логин и введенный пользователем OTP-код.

5. RADIUS-сервер выполняет проверку кода второго фактора и завершает аутентификацию.

Полезные ссылки

- **Как безопасно подключить удаленного подрядчика**

Авторизация

Классический контекст | Высокопроизводительный контекст | API

> Настройка правил авторизации пользователей в Ideco NGFW Novum.

Название службы раздела **Авторизация**: `ideco-auth-backend`.

Список служб для других разделов доступен по ссылке.

Авторизация - необходимое условие для доступа пользователя в интернет. Для работы в пределах локальной сети авторизация не требуется.

Для доступа сетевого устройства (хоста) в интернет через NGFW Novum с возможностью контроля трафика, хост должен быть авторизован в системе под учетной записью пользователя.

Механизм авторизации в Ideco NGFW Novum

Авторизация позволяет системе идентифицировать трафик и применять к нему правила доступа и ограничения, настроенные для конкретного пользователя или группы. Сессия авторизации создается только при наличии разрешающего правила для используемого вида авторизации.

Доступ к сетям для авторизованных и неавторизованных пользователей настраивается через правила межсетевого экрана.

Возможные правила доступа:

- **Авторизация по VPN**. Можно настроить для подключения как из внешних, так и из локальных сетей.
- **Авторизация через Ideco Client без туннеля**. Правила можно настроить для конкретных пользователей, групп пользователей, групп безопасности, специальных объектов **Все пользователи AD**, **Любой** или используя LDAP-фильтры.
- **Авторизация пользователей терминальных серверов**. Правила можно настроить для конкретных пользователей AD, групп безопасности, специального объекта **Любой** или используя LDAP-фильтры. Настраивается для каждого терминального сервера отдельно.
- **Авторизация через журналы AD**. Правила можно настроить для конкретных пользователей AD, групп безопасности, специального объекта **Любой** или используя LDAP-фильтры.
- **Авторизация по WEB, включая SSO**. Правила можно настроить для конкретных пользователей, групп пользователей, групп безопасности, специальных объекстов **Все пользователи AD**, **Все доверенные пользователи**, **Любой** или используя LDAP-фильтры.
- **Авторизация по IP или MAC**. Подробнее в статье.
- **Авторизация по подсети**. Подробнее в статье.

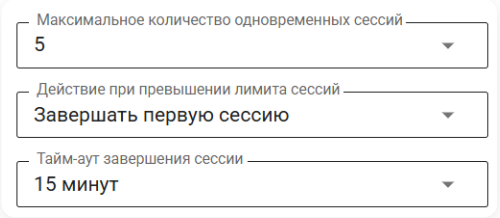
Особенности авторизации пользователей в Ideco NGFW Novum:

- Количество приобретенных по лицензии учетных записей ограничивает число авторизованных пользователей.
- Сессия авторизации учетной записи привязана к IP-адресу или к подсети (при авторизации по подсети) на протяжении действия сессии. У одного пользователя может быть несколько разных сессий.
- Хосты, не прошедшие авторизацию на NGFW Novum, лишены доступа к внешним сетям.
- Сессии авторизации пользователя, не проявляющего активность, завершаются по тайм-ауту и могут быть заняты новыми сессиями пользователей. Исключения:
  - Постоянная авторизация по IP/MAC.
  - Авторизация по подсети.
  - Терминальные пользователи.
  - VPN авторизация.
  - Ideco Client без туннеля.

Для настройки автоматической авторизации пользователей при входе в систему воспользуйтесь статьей.

Дополнительные настройки

Каждая сессия авторизации пользователя привязывается к IP-адресу устройства, с которого была инициирована. Выберите необходимые настройки для сессий:



- **Максимальное количество одновременных сессий** - ограничивает количество активных сессий для одного пользователя (диапазон: 1–6, значение по умолчанию: 5).
- **Действие при превышении лимита сессий** - определяет действие:
  - **Блокировать новую сессию** - авторизация с нового устройства будет невозможна.
  - **Завершать первую сессию** (по умолчанию) - самая старая сессия будет завершена.
- **Тайм-аут завершения сессии** - время до завершения сессии пользователя, если от него не поступает трафик. (диапазон: 10 минут – 24 часа, значение по умолчанию: 15 минут). Не распространяется на VPN. Для применения нового тайм-аута отключения требуется перезагрузка Ideco NGFW Novum.

Трафик может генерировать и сама операционная система без участия пользователя (например, телеметрия Windows). Из-за этого тайм-аут для пользователя будет постоянно сбрасываться.

Полезные ссылки

- **Настройка веб-аутентификации**
- **Настройка SSO-аутентификации**
- **Настройка авторизации через журнал безопасности AD**
- **Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT)**
- **Настройка Wi-Fi-сети**
- **Настройка прозрачной авторизации на Astra Linux**

Веб-аутентификация

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Веб-аутентификация**: `ideco-web-authd`, `ideco-web-backend`.

Список служб для других разделов доступен по ссылке.

Веб-аутентификация в Ideco NGFW Novum - тип авторизации, который предполагает, что отправленный через веб-браузер запрос неавторизованного пользователя будет переадресован на страницу авторизации Ideco NGFW Novum. Переход по указанному запросу произойдет после успешной авторизации.

Для этого типа авторизации должны быть выполнены условия:

- На сетевой карте у пользователя в качестве шлюза/объединенных в цепочку нескольких шлюзов или при прямых подключениях к прокси по умолчанию указан IP-адрес локального сетевого интерфейса Ideco NGFW Novum.
- До подключения к интернету работает **DNS-резолвинг адресов**. Иначе запрос браузера на адрес `example.com` не будет перенаправлен на шлюз, и в браузере не появится запрос логина и пароля.

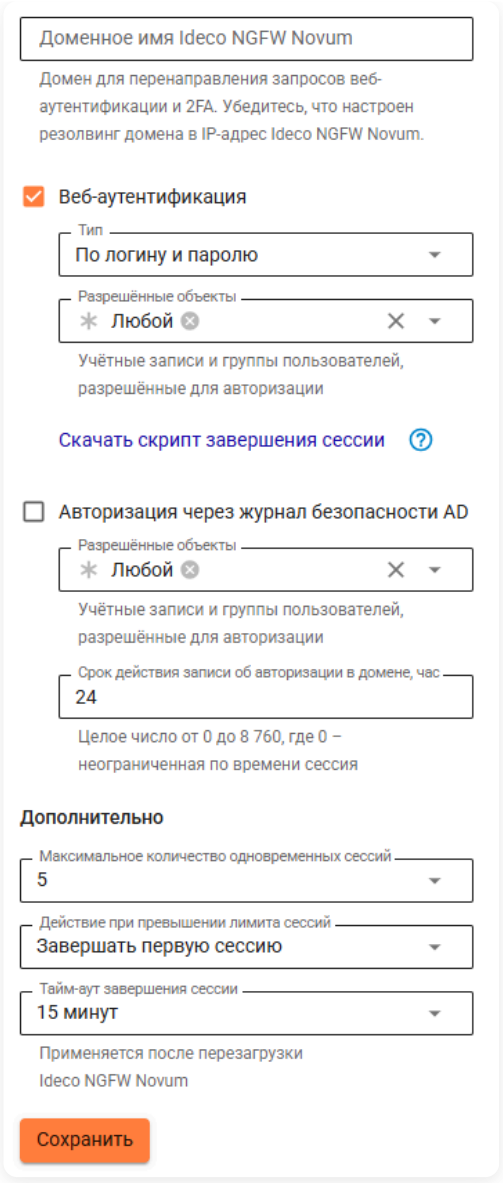
Проверить разрешение имен в Windows можно командой: `nslookup ya.ru`. Вывод данной команды должен содержать IP-адреса.

Рекомендуемые настройки для корректной работы веб-аутентификации:

- Добавьте сертификат Ideco NGFW Novum в доверенные корневые центры сертификации на устройстве (например, через политики домена).
- Укажите в качестве DNS-сервера на компьютерах и устройствах локальной сети IP-адрес локального интерфейса Ideco NGFW Novum.

Настройка авторизации через веб-интерфейс

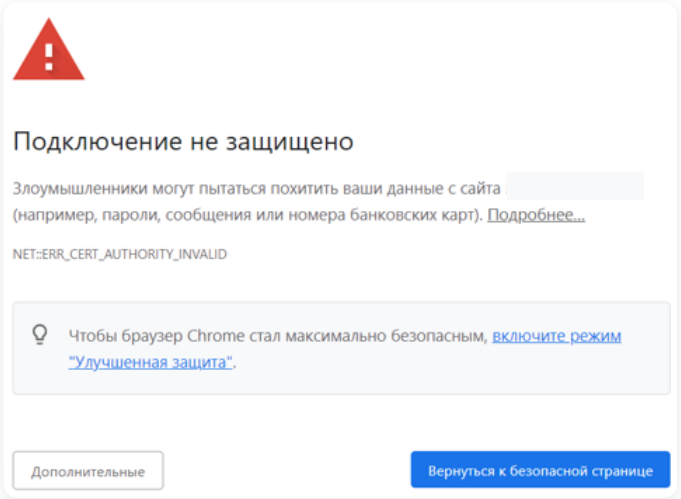
1. Выберите опцию **Веб-аутентификация** на вкладке **Пользователи** → **Авторизация** → **Настройки**:



2. Выберите **По логину и паролю** в поле **Тип**.

3. Выберите разрешенные для авторизации учетные записи или группы пользователей в поле **Разрешенные объекты**.

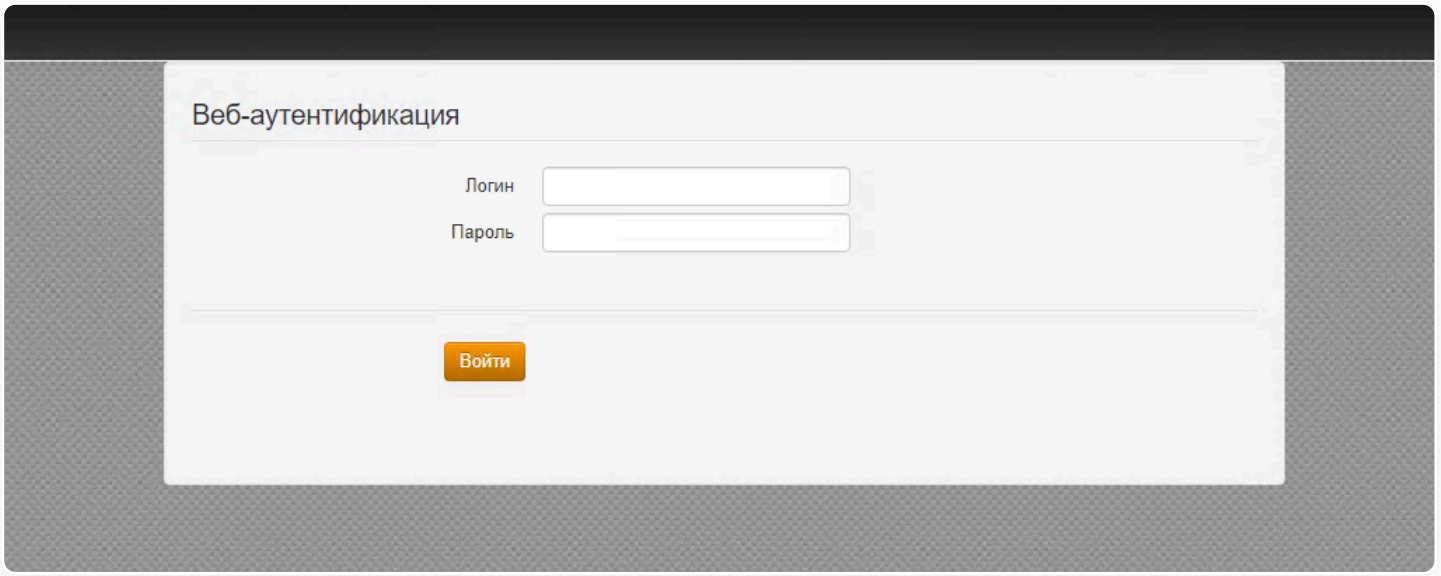
4. Заполните поле **Доменное имя Ideco NGFW Novum** и сохраните настройки, чтобы получить Let's Encrypt сертификат. Пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



Если Ideco NGFW Novum не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW Novum, страница авторизации будет подписана корневым сертификатом NGFW Novum.

Если сертификат для такого домена уже загружен в разделе Сертификаты, то будет использоваться загруженный сертификат, а новый сертификат выдаваться не будет.

5. Откройте веб-браузер с устройства пользователя. Должно появиться окно авторизации, где необходимо ввести логин и пароль от созданной на Ideco NGFW Novum учетной записи пользователя:



После прохождения пользователем веб-аутентификации доступ в интернет будет предоставлен до тех пор, пока авторизация не будет принудительно отменена или прекращена по неактивности пользователя.

Полезные ссылки

- **Настройка SSO-аутентификации**
- **Настройка авторизации через журнал безопасности AD**
- **Настройка автоматической веб-аутентификации на Ideco NGFW на Linux**
- **Настройка прозрачной авторизации на Astra Linux**

IP и MAC

Классический контекст | Высокопроизводительный контекст

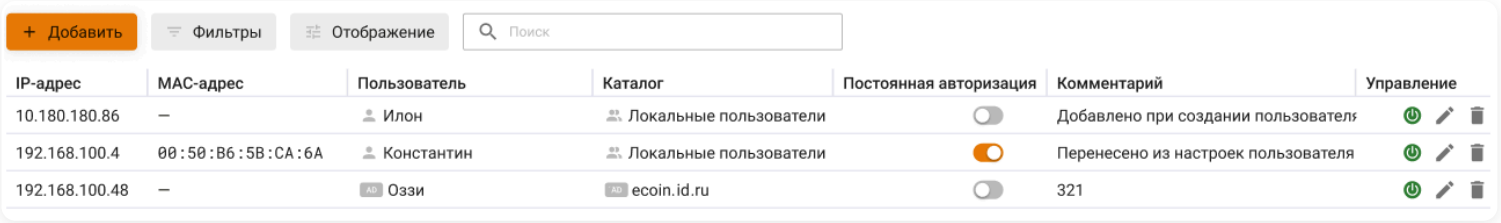
Принцип создания правил авторизации по IP и MAC в Ideco NGFW Novum.

Правила авторизации **IP и MAC** создают аналогичную привязку в **DHCP-сервере** Ideco NGFW Novum. Но если одни и те же IP- и MAC-адреса используются во включенных правилах DHCP-сервера, то правила DHCP-сервера выполняются в первую очередь.

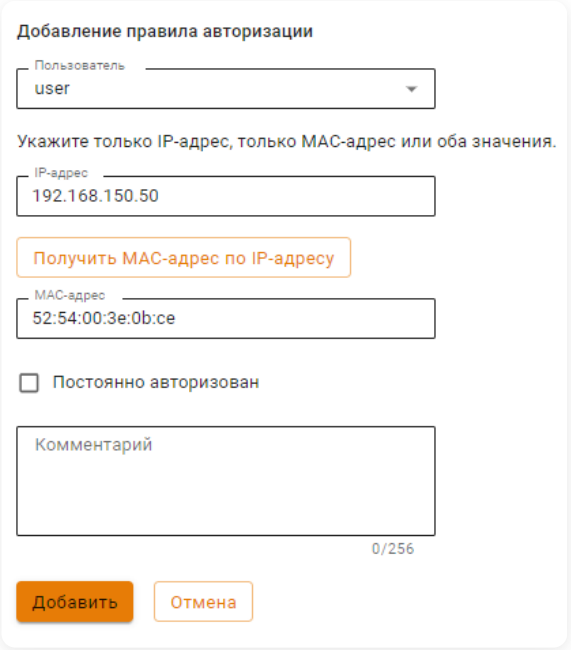
В правилах **IP и MAC** или **По подсетям** нельзя указывать пользователей RADIUS и DeviceVPN.

Настройка правила авторизации

1. Нажмите **Добавить** на вкладке **Авторизация → IP и MAC**:



2. Создайте правило привязки **IP и MAC**:



Расшифровка полей

- **Пользователь** - выберите пользователя из дерева пользователей.
- **IP-адрес** - введите IP-адрес устройства пользователя.
- **Получить MAC-адрес по IP-адресу** - нажмите для заполнения поля **MAC-адрес**. Кнопка активна, если IP-адрес пользователя и IP Ideco NGFW Novum в одной подсети.
- **Постоянно авторизован** - включите опцию, если требуется обеспечить непрерывный доступ в интернет. В этом случае лицензия будет закреплена за IP-адресом, даже если устройство выключено или пользователь неактивен. Настройка полезна для устройств/серверов, если количество пользователей может значительно увеличиться, исчерпав все лицензии.
- **Комментарий** - необязательное поле.

При наличии большого количества правил привязки в таблице воспользуйтесь кнопкой **Фильтры**.

Доступна сортировка по любому из столбцов таблицы.

Созданные на вкладке **Пользователи** → **Авторизация** → **IP и MAC** правила отражаются в карточке пользователя.

Полезные ссылки

Статьи об авторизации пользователей только по IP- или MAC-адресу:

- **Авторизация по MAC-адресу**
- **Авторизация по IP-адресу**

Авторизация по IP-адресу

Классический контекст | Высокопроизводительный контекст

При авторизации по IP пользователь получает доступ в интернет без ввода логина и пароля сразу после инициации подключения.

Доступна авторизация сетевых устройств (камеры видеонаблюдения, сетевые принтеры и прочее), которые находятся в разных с Ideco NGFW Novum широковещательных доменах и требуют доступ в интернет.

Если устройством является маршрутизатор, в котором включен SNAT, то при авторизации внешнего IP маршрутизатора на NGFW Novum, все пользователи за этим маршрутизатором получат доступ в интернет.

Пользователи, которые находятся за маршрутизатором в локальной сети Ideco NGFW Novum, не могут авторизоваться по IP+MAC, так как маршрутизатор не обрабатывает трафик уровня L2.

Если настроена авторизация по IP-адресу, то используемый IP-адрес не будет выдаваться DHCP.

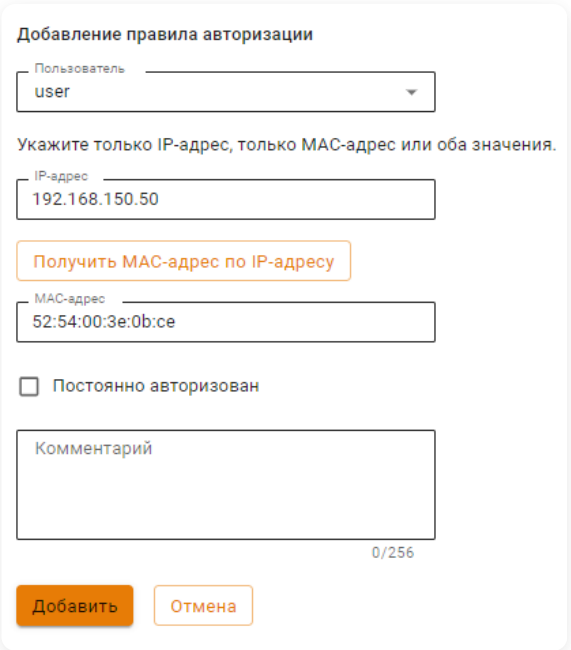
Настройка авторизации по IP

Для авторизации пользователя по IP-адресу:

1. Создайте пользователя.

2. Перейдите в **Пользователи → Учетные записи → Карточка пользователя → IP и MAC авторизация** или на вкладку **Пользователи → Авторизация → IP и MAC**.

3. Создайте правило-связку **IP-адрес <–> Пользователь**:



IP-адрес на устройстве, с которого инициируется сессия, должен совпадать с указанным в правиле. Кнопка **Получить MAC по IP** будет активна, если IP-адрес пользователя и IP Ideco NGFW Novum в одной подсети.

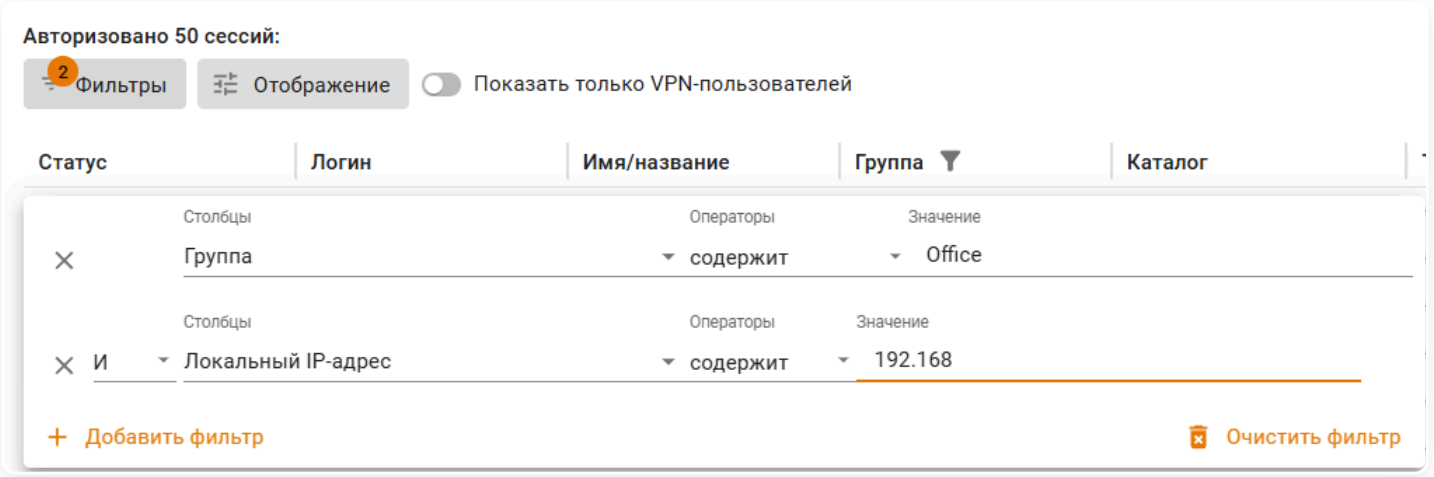
Рекомендации по использованию авторизации по IP-адресу:

- Настройте для пользователя, которым является сетевое оборудование, **Постоянную авторизацию**. Это позволит NGFW Novum создать сессию, а сетевому оборудованию не потребуется делать запрос в интернет.
- Настройте статический IP-адрес или DHCP с привязкой по IP-адресу. Это требуется, например, для ресурсов, опубликованных через DNAT.
- Воспользуйтесь поиском устройств для автоматического создания пользователей при попытке выхода в интернет. Подробнее о настройке в статье Обнаружение устройств.

При использовании авторизации по IP со статической привязкой в DHCP рекомендуем перенести такие правила на авторизацию по MAC-адресу.

Просмотр сессии

После запроса пользователя в интернет на Ideco NGFW Novum в разделе **Мониторинг** → **Сессии пользователей** автоматически создается сессия с типом авторизации `IP`:



У сессий с типом `IP` не заполняется поле **MAC-адрес**, так как уже указан IP-адрес, необходимый для создания сессии.

Авторизация по MAC-адресу

Функциональность доступна в **Классическом** и **Системном контекстах**.

Авторизация по MAC-адресу подойдет для тех устройств, у которых время от времени меняется местоположение между локальными сетями внутри организации (например, рабочие ноутбуки сотрудников), а также сетевых устройств, на которых не настроена привязка IP+MAC и IP-адрес выдается через DHCP.

Для авторизации пользователя на Ideco NGFW Novum по MAC-адресу устройство пользователя и Ideco NGFW Novum должны находиться в одном широковещательном домене, а Ideco NGFW Novum должен выступать шлюзом для этого устройства.

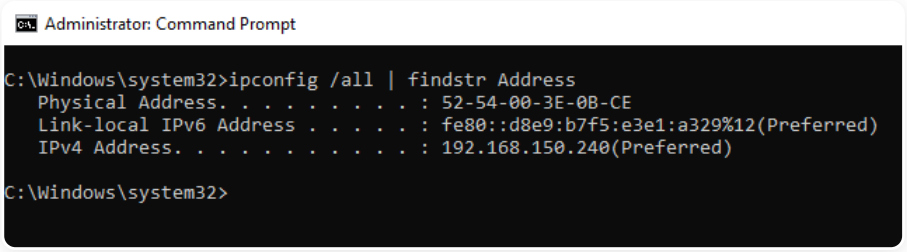
Пользователи, находящиеся за роутером в локальной сети Ideco NGFW Novum, не могут авторизоваться по MAC-адресу, так как роутер разделяет широковещательные домены и не обрабатывает трафик уровня L2. Такие пользователи могут авторизоваться только по IP-адресу.

Для работы MAC-авторизации необходимо, чтобы NGFW Novum и устройство пользователя находились в одном L2-сегменте сети.

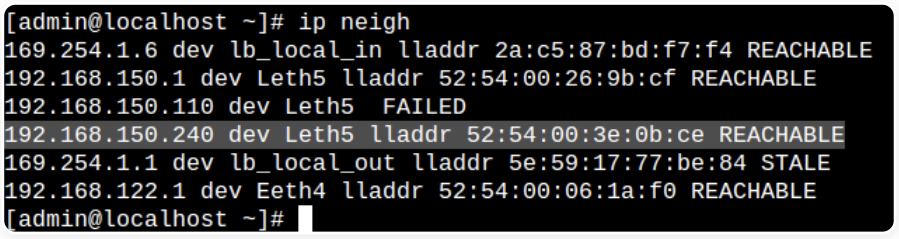
Настройка авторизации по MAC-адресу

Для авторизации пользователя по MAC-адресу:

1. Узнайте MAC-адрес устройства. Для этого в командной строке Windows введите `ipconfig /all | findstr Address` или `ipconfig /all | findstr адрес` (для русскоязычной версии):



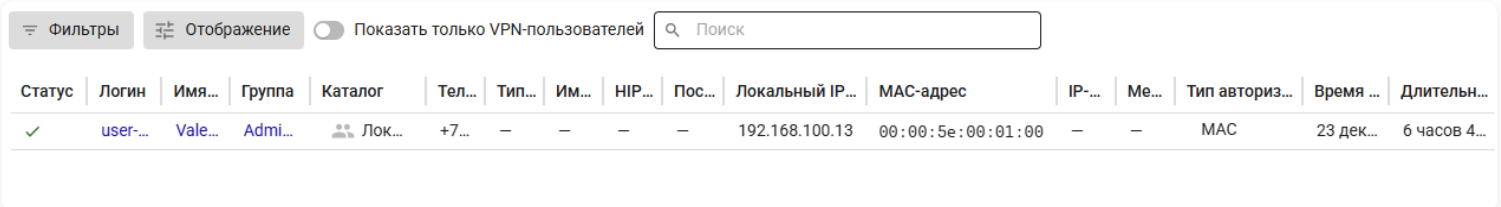
2. Удостоверьтесь, что устройство пользователя и NGFW Novum находятся в одном широковещательном домене. Для этого в **Управление сервером** → **Терминал** веб-интерфейса Ideco NGFW Novum введите команду `ip neigh`:



Эта команда выводит ARP-таблицу Ideco NGFW Novum. Наличие записи с MAC-адресом устройства и статусом REACHABLE - маркер L2-доступности между NGFW Novum и устройством пользователя.

3. Создайте правило-связку **Пользователь <--> MAC-адрес** на вкладке **Пользователи** → **Авторизация** → **IP и MAC**.

Сессия с типом авторизации `MAC` отобразится в разделе **Мониторинг** → **Сессии пользователей**:



Для MAC-адресов невозможно настроить постоянную авторизацию, так как для создания авторизованной сессии необходим IP-адрес. Рекомендуется использовать MAC-авторизацию в комбинации с DHCP-сервером.

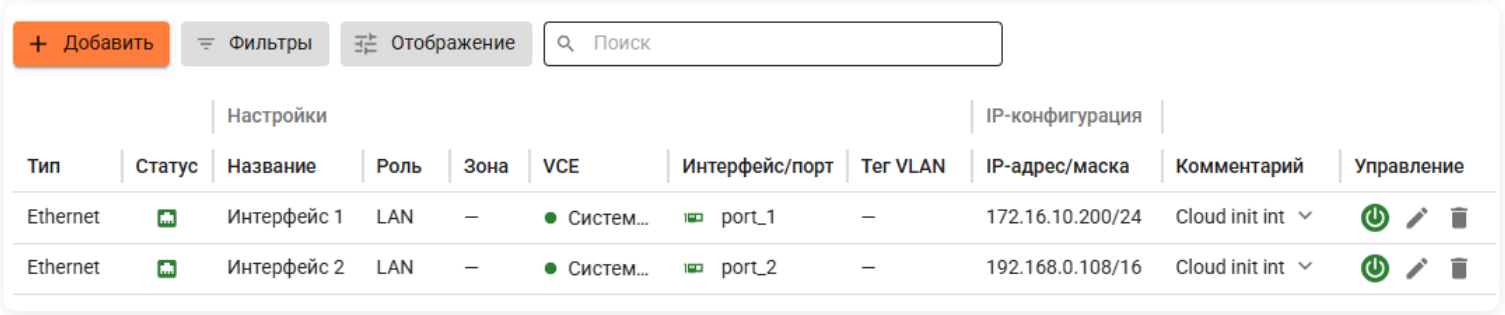
Поведение MAC-авторизации при перемещении устройства между локальными сетями

В организациях часто возникает ситуация, когда необходимо перемещаться между локальными сетями с ноутбуком и при этом всегда оставаться в сети. В таких случаях рекомендуется использовать авторизацию по MAC-адресу.

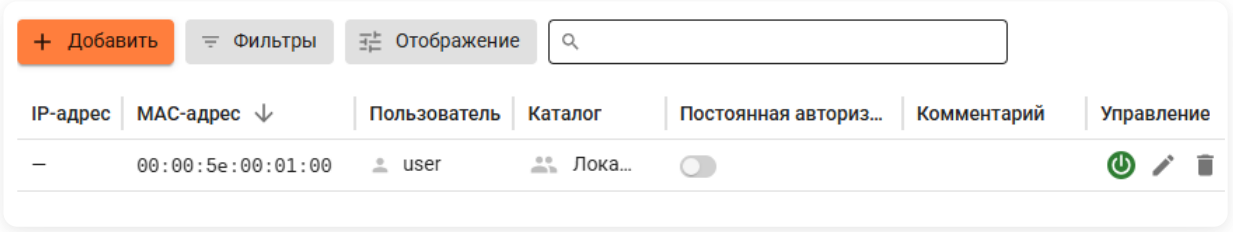
Для авторизации по MAC настройте DHCP-сервер (собственный или на NGFW Novum). В раздаваемых реквизитах шлюзом должен выступать локальный интерфейс NGFW Novum.

Пример. Пользователю `user` понадобилось переместиться с ноутбуком между локальными сетями:

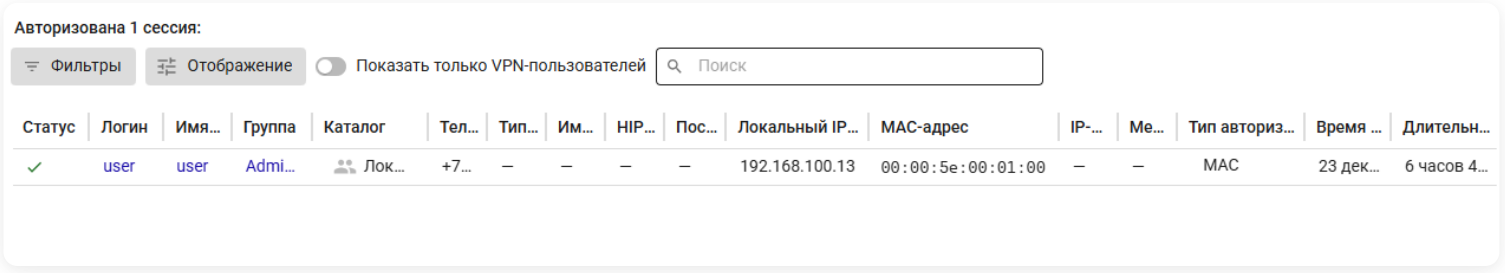
- На NGFW Novum настроены локальные интерфейсы:



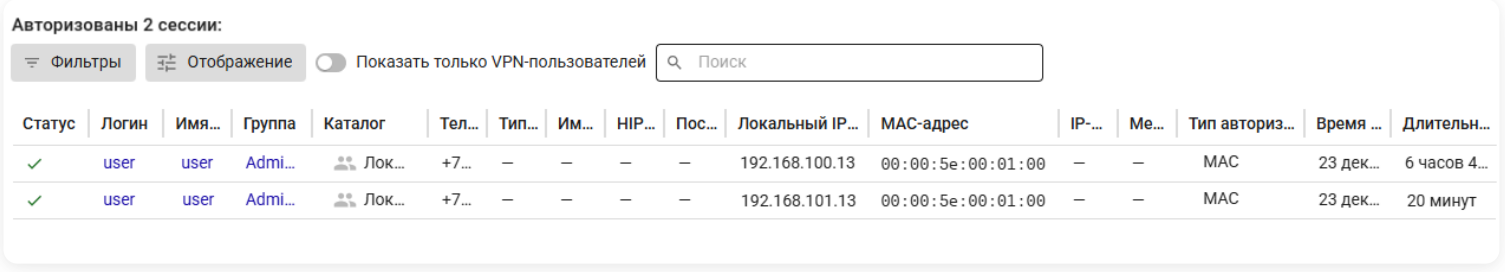
- Настроено правило авторизации пользователя по MAC-адресу:



- У пользователя одна активная сессия в разделе **Сессии пользователей**:



При переходе пользователя из одной локальной сети в другую ему выдаются другие сетевые реквизиты от DHCP-сервера, в которых шлюзом указан NGFW Novum. При обнаружении любой активности пользователя появится вторая сессия авторизации по MAC-адресу:



Если у пользователя не появляется доступ и вторая сессия с авторизацией по MAC-адресу, следует обновить сетевые реквизиты.

Сбросьте старые сетевые настройки от DHCP-сервера и получите новые с помощью команд:

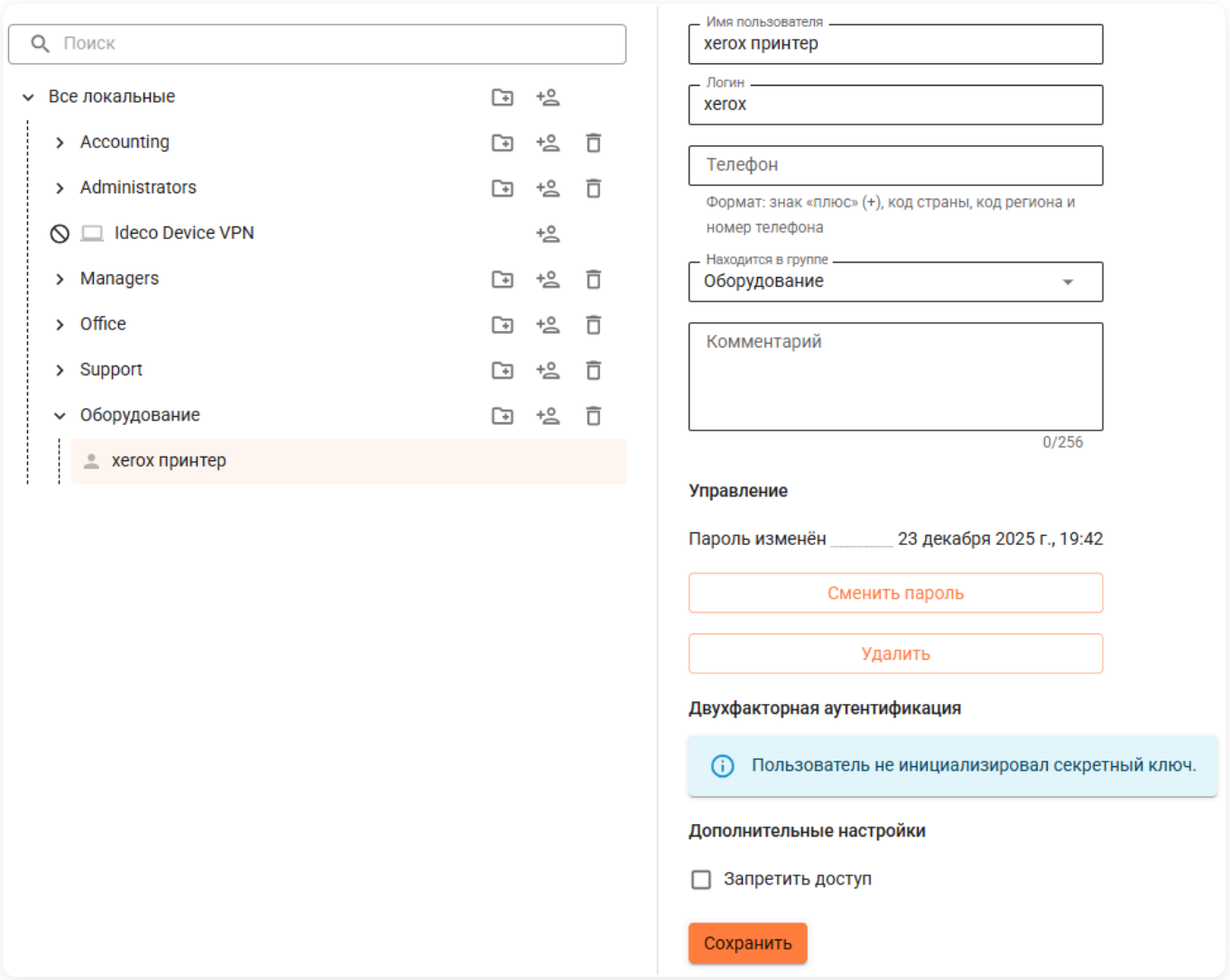
- Windows - `ipconfig /release && ipconfig /renew`;

- Linux - `sudo dhclient -r <имя_интерфейса>`.

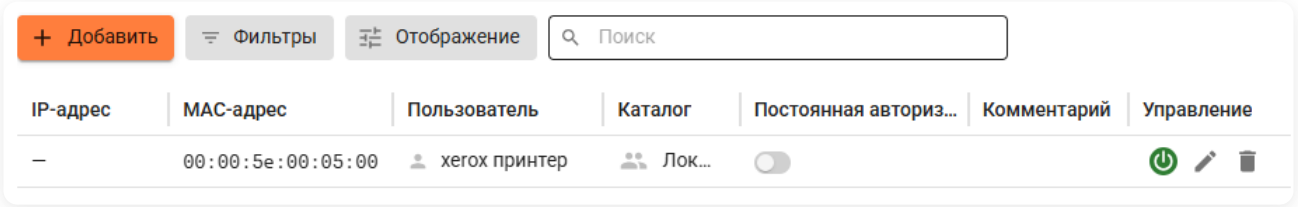
Настройка авторизации по MAC-адресу для сетевого принтера и других сетевых устройств

Сетевые устройства, которым необходим доступ в интернет, должны быть авторизованы на NGFW Novum. Такие устройства можно назвать статическими, для них подойдет авторизация по MAC-адресу.

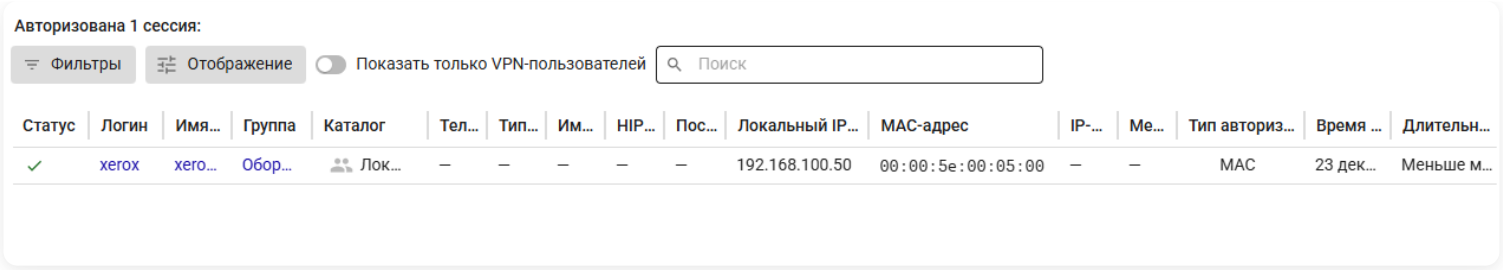
Чтобы авторизовать сетевой принтер, необходимо создать пользователя на NGFW Novum вручную или через Обнаружение устройств:



На вкладке **Пользователи** → **Авторизация** → **IP и MAC** для сетевого принтера необходимо создать правило **Пользователь <--> MAC-адрес**:



При обнаружении активности от сетевого принтера или другого устройства сессия пользователя появится в **Мониторинг** → **Сессии пользователей**:



Опция **Рандомизация MAC-адреса** будет мешать при авторизации мобильного устройства по MAC-адресу. Рекомендуется отключить эту опцию либо использовать другие типы авторизации (например, веб-аутентификацию).

По подсетям

Классический контекст | Высокопроизводительный контекст

Чтобы не регистрировать каждое устройство как отдельного пользователя Ideco NGFW Novum и не задавать для него факторы авторизации, создайте правило в **Пользователи** → **Авторизация** → **По подсетям**. Правила полезны, когда требуется автоматически авторизовать большое количество устройств.

Любой трафик при авторизации по подсетям учитывается как трафик от одного указанного пользователя в указанной подсети. Не допускайте пересечения сетей.

Особенности использования авторизации по подсетям

В правилах **IP и MAC** или **По подсетям** нельзя указывать пользователей RADIUS и DeviceVPN.

Любое **пересечение сетей** при авторизации может привести к проблемам. Например:

- На вкладке **По подсетям** для разных пользователей созданы правила с пересекающимися сетями.
- В **Пользователи** → **Учетные записи** создан пользователь с IP-адресом из подсети в правилах авторизации **По подсетям**.
- В **VPN-подключения** → **Выдача IP-адресов** добавлена привязка к IP-адресам из подсети в правилах авторизации **По подсетям**.
- На вкладке **По подсетям** создано правило с подсетью, частично пересекающейся с диапазоном IP-адресов для выдачи в **Сервисы** → **DHCP**.

Работа DHCP возможна в случае, если диапазон выдачи IP-адресов не превышает количество адресов в подсети, указанной в правиле авторизации **По подсетям**.

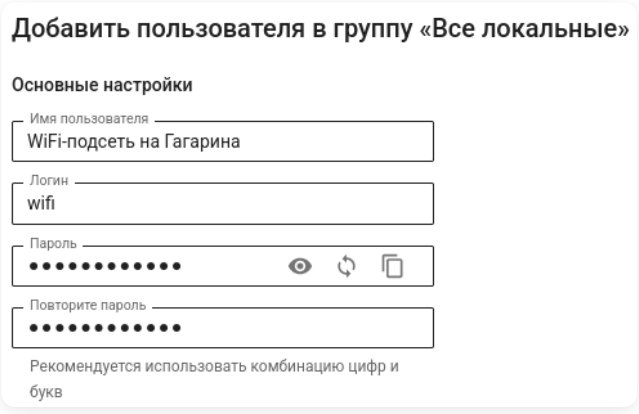
Пример использования

Есть Wi-Fi-подсеть 192.168.10.0/24, для устройств которой требуется авторизация.

Для создания правила авторизации выполните действия:

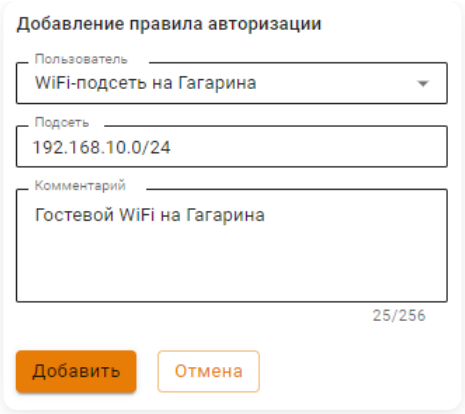
1. Перейдите в **Пользователи** → **Учетные записи** и нажмите .

2. Заполните поля и нажмите **Добавить**:



3. Перейдите в **Пользователи** → **Авторизация** → **По подсетям** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:



- **Пользователь** - выберите созданного в пункте 2 пользователя.
- **Подсеть** - введите IP и маску подсети.
- **Комментарий** - необязательное поле.

При включении или отключении правил авторизации **По подсетям** может наблюдаться задержка в работе Ideco NGFW Novum.

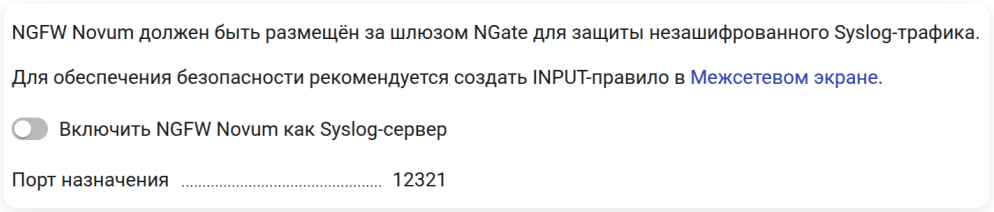
Syslog-сервер

Классический контекст | Высокопроизводительный контекст

На вкладке можно настроить NGFW Novum в роли Syslog-сервера для авторизации пользователей, подключающихся к КриптоПро NGate. NGFW Novum будет принимать Syslog-сообщения, фильтровать их по содержанию и открывать сессии для пользователей NGFW Novum.

На текущий момент интеграция поддерживается только с КриптоПро NGate. В дальнейшем список поддерживаемых вендоров может быть расширен.

Опция **Включить NGFW Novum как Syslog-сервер** позволяет включить или отключить работу NGFW Novum в роли Syslog-сервера:



- **Порт назначения** - порт приема Syslog-сообщений. По умолчанию `12321`.

IP-адрес получателя - по умолчанию `0.0.0.0`. Изменение IP-адреса и порта в интерфейсе не предусмотрено.

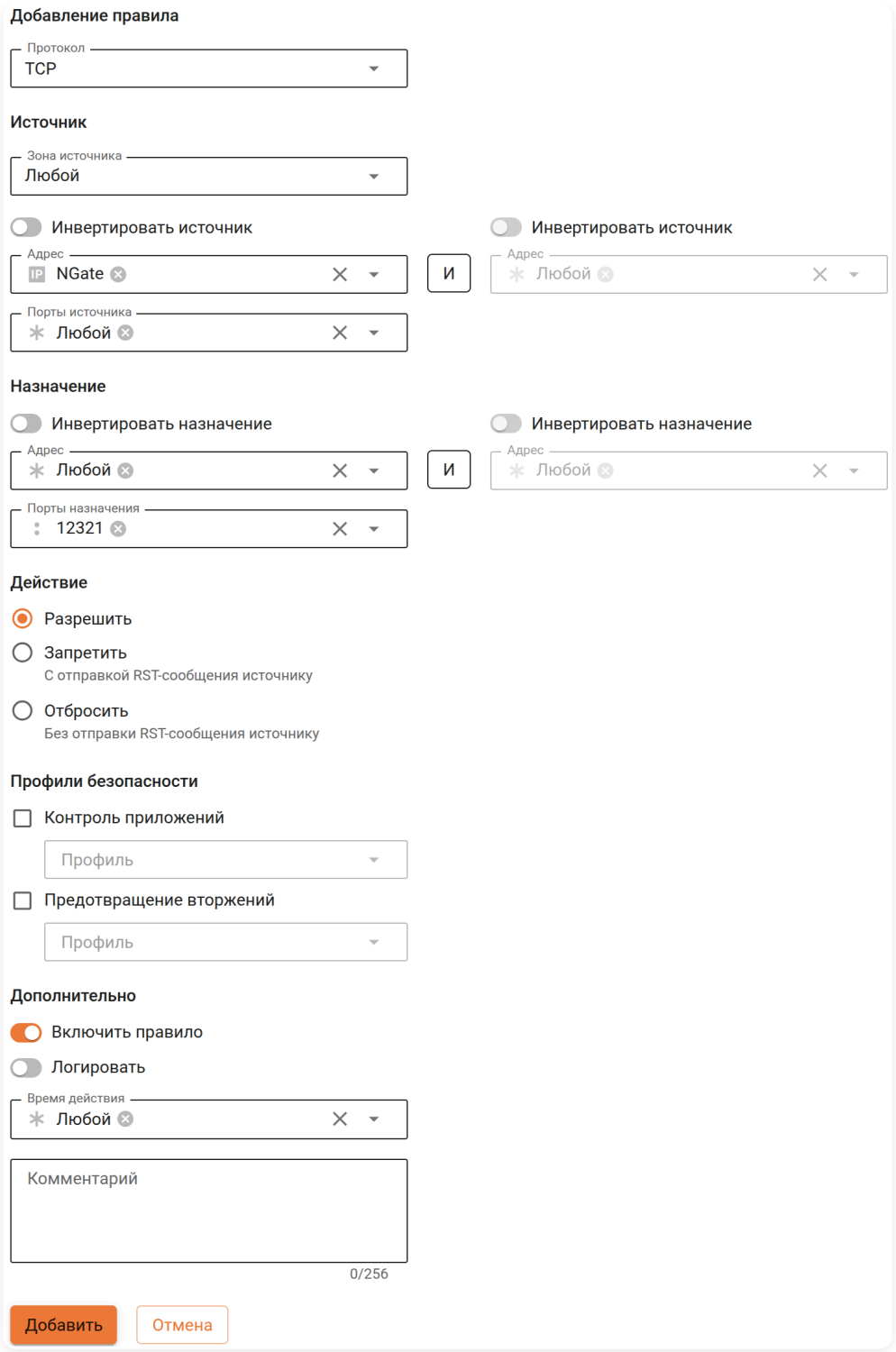
Изменения IP-адреса или порта доступно через API.

Интеграция с NGate открывает незащищенный канал передачи сообщений. Рекомендуем:

1. Разместить NGFW Novum внутри периметра за шлюзом NGate, чтобы предотвратить несанкционированную отправку Syslog-сообщений.

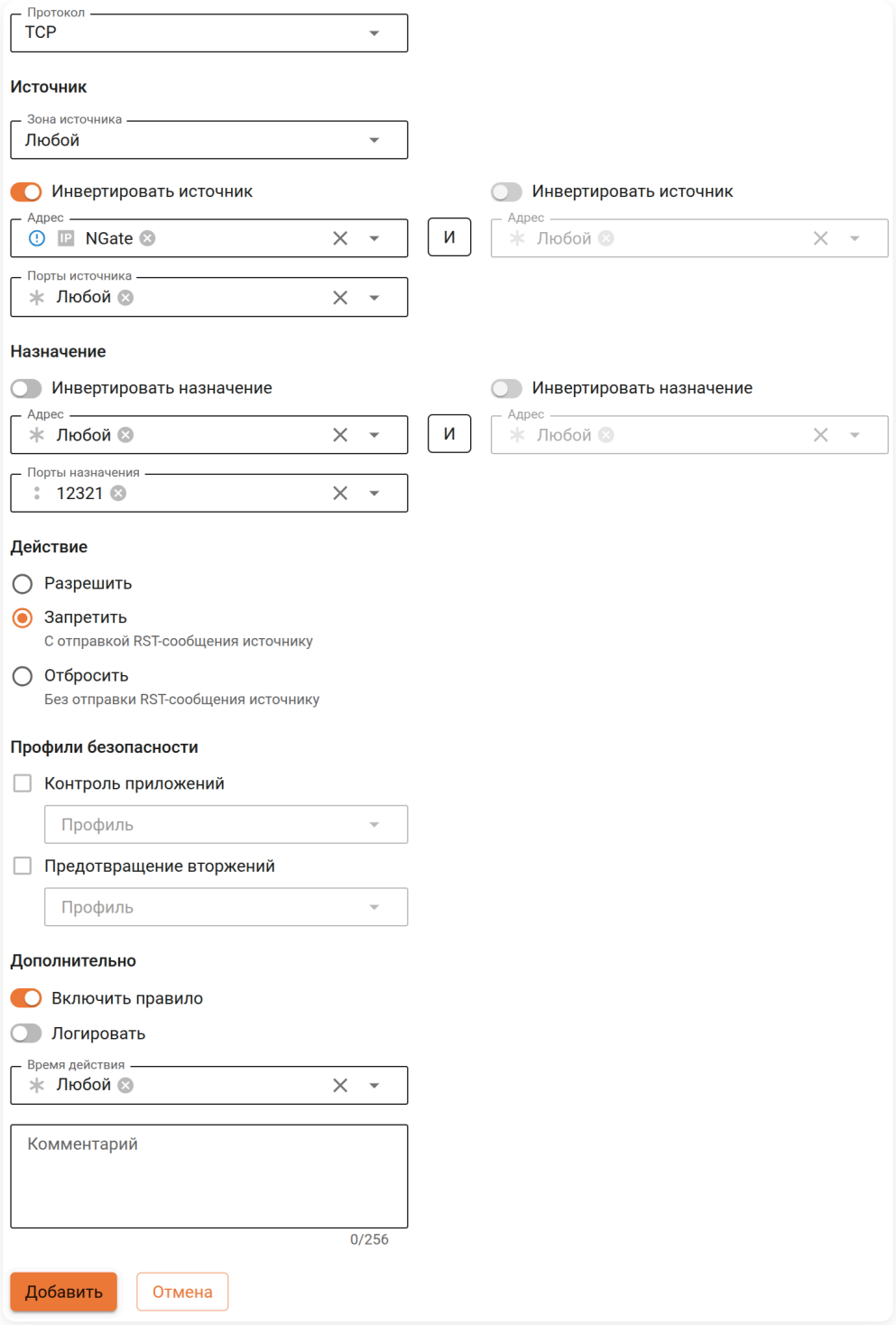
2. Ограничить все запросы на порт `12321` только доверенными источниками. Для этого создайте правило в **Правила трафика** → **Межсетевой экран** → **INPUT** с учетом наличия **запрещающего все** правила:

Запрещающее все правило есть



- **Протокол** - TCP.
- **Источник** - IP-адрес NGate или зона, в которую он входит.
- **Порты назначения** - `12321`.
- **Действие** - Разрешить.

Запрещающее все правило отсутствует



- **Протокол** - TCP.
- **Инвертировать источник** - включите опцию.
- **Источник** - IP-адрес NGate или зона, в которую он входит.
- **Порты назначения** - `12321`.
- **Действие** - Запретить.

Для использования локальной группы пользователей NGFW Novum без интеграции с Active Directory (AD) NGate должен использовать один из способов:

- Подключение к LDAP или RADIUS.
- Аутентификация по сертификатам с именами пользователей.

Подробнее о создании в NGate правил доступа к ресурсам в статье.

Если NGate и NGFW Novum интегрированы с Active Directory, то в **Пользователи** → **Аутентификация** → **Основное** выберите каталог авторизации AD как **Каталог по умолчанию**.

Настройка на NGate

1. Добавьте NGFW Novum в качестве Syslog-сервера на стороне NGate, следуя инструкции:

- NGFW Novum должен быть добавлен отдельным Syslog-сервером, так как NGate поддерживает одновременную отправку логов на несколько Syslog-серверов.
- В настройках Syslog-сервера необходимо выбрать протокол **TCP** и указать порт назначения `12321`.

2. Настройте отправку логов согласно инструкции.

> В конфигурации кластера NGate уровень логирования должен быть установлен не ниже `LOG_INFO`, иначе часть событий не будет передаваться на внешний Syslog-сервер.

VPN-подключения

Классический контекст | Высокопроизводительный контекст | API

С версии 22.0 поддержка протокола PPTP для доступа по VPN отключена, так как протокол устарел.
Рекомендуем использовать Ideco Client, IKEv2/IPsec или SSTP.

Название служб раздела **VPN-подключения**: `ideco-vpn-servers-backend`, `ideco-vpn-authd`, `ideco-vpn-dhcp-backend`, `ideco-vpn-netns`, `ideco-vpn-sessions-sync`.

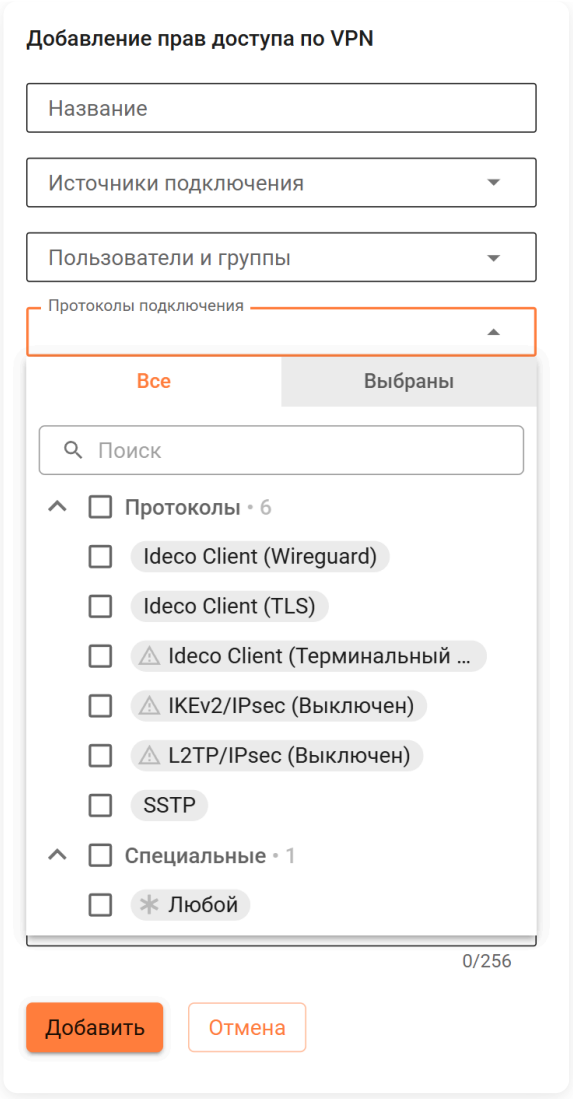
Список служб для других разделов доступен по ссылке.

Для настройки VPN-подключения к Ideco NGFW Novum можно использовать VPN-клиент, который уже есть в операционной системе, или установить отдельный. Как настроить подключение в разных ОС, описано в Инструкции по созданию VPN-подключений.

Настройка VPN-сервера Ideco NGFW Novum происходит в несколько этапов:

- Настройка протоколов, маршрутов и адресации.
- Настройка политик доступа из внешних сетей.
- Настройка двухфакторной аутентификации (опционально).

Поддерживаемые протоколы:



- **WireGuard** - используется Ideco Client с применением шифрования.
- **TLS** (Transport Layer Security) - используется Ideco Client при подключении через TCP.
- **Терминальный сервер** - WireGuard для терминального сервера. Используется Ideco Client с применением шифрования.
- **IKEv2** - рекомендуемый протокол с точки зрения скорости и безопасности.
- **SSTP** - подходит для использования в средах с ограничениями на порты.
- **L2TP/IPsec** - обеспечивает баланс между безопасностью и совместимостью.
- **Любой** - отмечаются все протоколы. Такое соединение может использовать любой из перечисленных протоколов.

Настройка VPN-подключения

Чтобы VPN-подключение работало на устройствах пользователей, необходимо загрузить **корневой сертификат**:

- Корневые сертификаты Ideco NGFW Novum действительны в течение 10 лет.
- Если используется сертификат Let's Encrypt, обновление будет происходить автоматически.

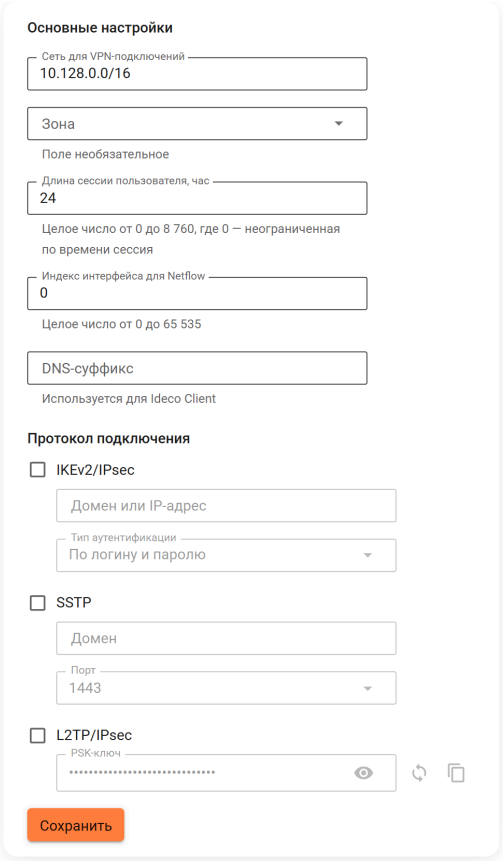
Чтобы пользователь, подключенный к NGFW из локальной сети по VPN или через Ideco Client в режиме VPN, мог выйти в интернет, нужно выполнить одно из следующих действий:

- Настройте вторую сессию авторизации пользователя. Например, через Веб-авторизацию.
- В разделе **Передача маршрутов** для нужных пользователей выберите опцию **Отправлять весь трафик на Ideco NGFW Novum**.

Для настройки VPN-подключения перейдите в **Пользователи** → **VPN-подключения** и создайте правило.

Основное

На вкладке **Основное** настраиваются протоколы и адресация VPN-подключений. Для настройки заполните поля:



Расшифровка полей

- **Сеть для VPN-подключений** - укажите подсеть для динамического назначения IP-адресов. Маска подсети должна быть в диапазоне от 16 до 30 бит.
- **Зона** - добавьте настройку, если необходимо объединить сетевые интерфейсы. Все сетевые интерфейсы, которые создаются при подключении VPN-клиентов, будут автоматически попадать в указанную зону. Трафик пользователей будет обрабатываться по правилам, заданным для этой зоны.

Если требуется настроить VPN-подключение к Loopback-интерфейсу, оставьте поле **Зона** пустым.

- **Длина сессии пользователя, час** - укажите продолжительность сессии пользователя (целое число от 1 до 24). По истечении указанного периода сессия разрывается и требуется переподключение. Настройка распространяется на подключения по протоколам L2TP, SSTP, IKEv2, а также на сессии Ideco Client.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **DNS-суффикс** - укажите DNS-суффикс, если для подключения по VPN используется Ideco Client.
- **Протокол подключения** - выберите, какой протокол будет использоваться.

Для каждого протокола VPN-подключения отображается статус использования. Статусы отображаются в виде подсказок под названиями протоколов:

Зеленый статус: протокол включен и используется.

Оранжевый статус: протокол отключен, но используется в правилах доступа по VPN.

Как увеличить продолжительность сессии пользователя с помощью запроса к API

```
PATCH https://:8443/vpn_servers/settings
```

Json-тело запроса:

```
{
"expired_after_seconds": "integer"
}
```

`expired_after_seconds` - количество секунд от 1 до 31536000, после которого VPN-сессия считается просроченной.

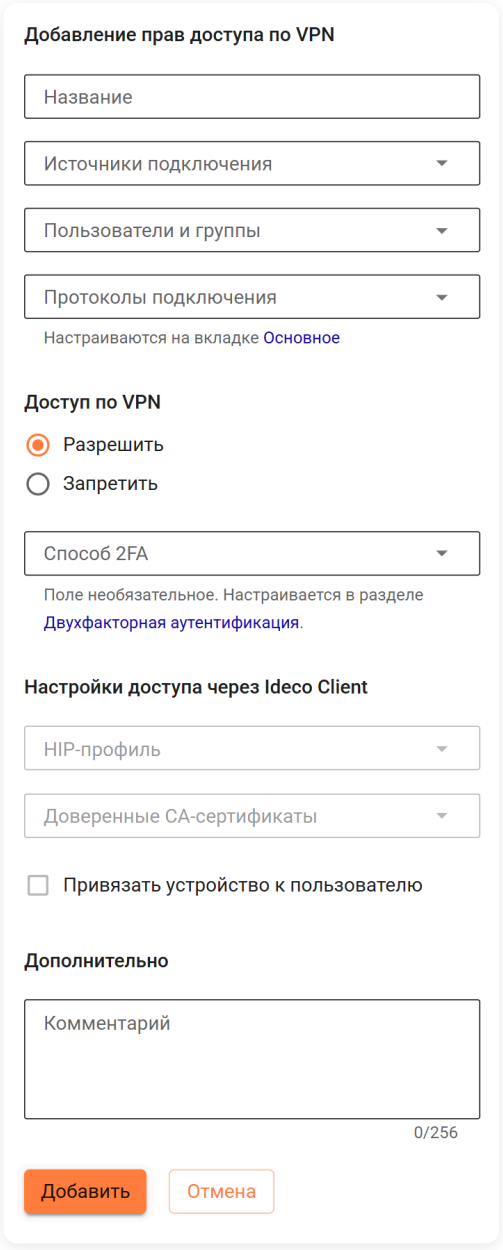
Ответ на успешный запрос: 200 OK

Доступ по VPN

На вкладке **Доступ по VPN** для пользователей и групп на внешние интерфейсы NGFW Novum настраиваются правила доступа. NGFW Novum проверяет таблицу правил сверху вниз до первого совпадения пользователя. При совпадении условий (**Источники подключения**, **Пользователи и группы**, **Протоколы подключения**) выполняется действие, выбранное при создании правил.

В правилах можно использовать как группы пользователей Ideco NGFW Novum, так и группы безопасности AD. Введите Ideco NGFW Novum в домен и при создании правила **Доступ по VPN** в поле **Пользователи и группы** выберите необходимую группу безопасности.

Для настройки правил доступа нажмите **Добавить**:



Расшифровка полей

- **Название** - укажите название правила.
- **Источники подключения** - выберите, откуда будет производиться подключение по VPN (IP-адреса, подсети, страны и континенты).
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.

Для пользователей Device VPN доступно подключение только по протоколам **Ideco Client (Терминальный сервер)**, **Ideco Client (Wireguard)**, и **Ideco Client (TLS)**.

Если в поле **Протоколы подключения** выбраны **Ideco Client (Wireguard)** и **Ideco Client (TLS)** или **Любой**, пользователи будут подключаться по протоколу **Ideco Client (Wireguard)**.

- **Протоколы подключения** - выберите протокол (настраивается на вкладке **Основное**).
- **Доступ по VPN** - разрешите или запретите доступ по созданному правилу.
- **Способ 2FA** - выберите способ двухфакторной аутентификации.

2FA не поддерживается для учетных записей Device VPN.

- **HIP-профиль** - выберите HIP-профиль, если для подключения по VPN используется Ideco Client.
- **Настройки доступа через Ideco Client:**
  - **Доверенные CA-сертификаты** - выберите один или несколько сертификатов CA, которым доверяет Ideco NGFW Novum при проверке сертификата устройства. Загружаются в **Сервисы** → **Сертификаты**. Если поле не заполнено, проверка сертификата устройства не выполняется. Подробнее о выпуске сертификата устройства в статье.
  - **Привязать устройство к пользователю** - если опция включена, при первом подключении пользователя через Ideco Client устройство привязывается к учетной записи. Последующие подключения разрешаются только с привязанного устройства.

Привязка устройств не осуществляется для пользователей **Ideco Device VPN**.

- **Комментарий** - добавьте комментарий (опционально).

Если авторизация Device VPN не требуется, исключите группу **Ideco Device VPN** из разрешающих правил или создайте для нее запрещающее правило.

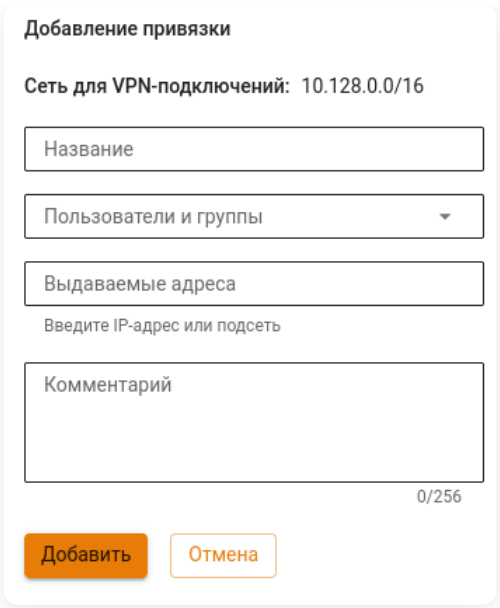
Выдача IP-адресов

На вкладке **Выдача IP-адресов** можно создать правила для выдачи IP-адресов пользователям, подключающимся по VPN.

NGFW Novum проверяет таблицу правил сверху вниз до первого совпадения пользователя. Если пользователь не попал под условия правил, IP-адрес назначается автоматически из пула адресов VPN, настраиваемого в разделе **Пользователи** → **VPN-подключения** (например, 10.128.0.0/16). Из пула исключаются все подсети и одиночные адреса, указанные во всех правилах таблицы выдачи IP-адресов и используемые в текущих сессиях. Если адресов не осталось, соединение разрывается.

- Подсеть, указанная в правиле, должна полностью входить в сеть для VPN-подключений. В противном случае правило считается невалидным, адрес выдать невозможно, соединение разрывается.
- В двух разных правилах нельзя указать одну и ту же сеть.
- Если в разных правилах указаны пересекающиеся сети (например, сеть `10.128.1.0/24` является подсетью сети `10.128.0.0/20`), то:
  - Адреса из сети `10.128.1.0/24` никогда не будут выдаваться.
  - При выдаче адресов сети `10.128.0.0/20` из нее будут исключаться адреса подсети `10.128.1.0/24`.
- Если указать в правилах сеть, совпадающую с сетью для VPN-подключений, то все пользователи VPN, для которых не совпадет ни одно правило таблицы, не смогут получить адрес и подключиться.
- Количество одновременных VPN-подключений от одного пользователя в том числе будет ограничиваться размером сети, указанной для него в правилах.
- Если в правиле указан один IP-адрес, который уже используется в текущей сессии, то указанный в правиле пользователь не сможет установить второе VPN-подключение и не сможет получить адрес.
- Если в правиле указана сеть с префиксом /30 (или маской 255.255.255.252) и более широкие сети (например, `10.128.2.0/24`), то при выдаче адреса из таких сетей адрес самой сети и широковещательный адрес (`10.128.2.0` и `10.128.2.255`) использоваться не будут.

Для создания правила нажмите **Добавить**:



Расшифровка полей

- **Название** - укажите название правила.
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Выдаваемые адреса** - укажите IP-адрес или подсеть, IP-адреса которой будут выдаваться пользователям.
- **Комментарий** - укажите комментарий к правилу (опционально).

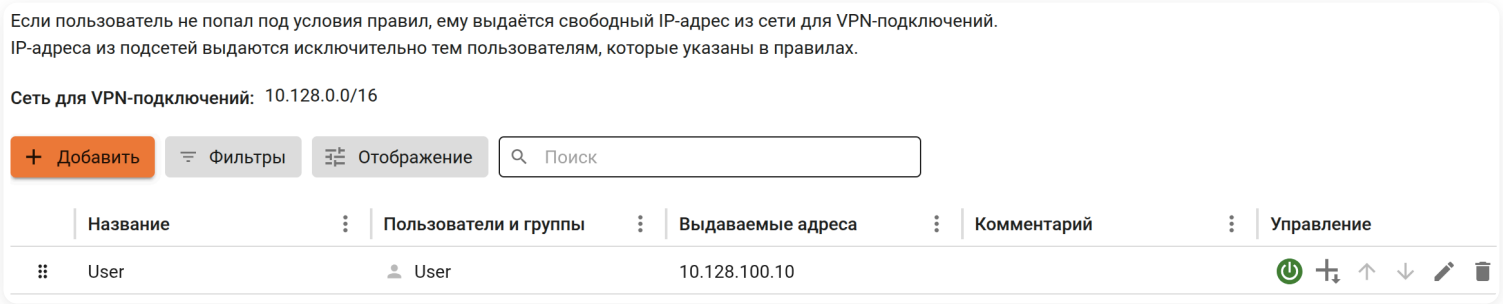
При наличии большого количества правил выдачи IP-адресов в таблице воспользуйтесь кнопкой **Фильтры**.

Чтобы отключить правило, нажмите на в столбце управления. Чтобы удалить правило, нажмите .

Статическая привязка IP-адресов

IP-адрес назначается пользователю автоматически из пула адресов для VPN, настраиваемого в разделе **Пользователи → VPN-подключения** (например, 10.128.0.0/16).

Чтобы настроить **статическую** привязку адресов, выдаваемых определенным пользователям, нужно перейти в **Пользователи → VPN-подключения → Выдача IP-адресов**, нажать **Добавить** и указать нужного пользователя и IP-адрес. Пример настройки фиксированного IP-адреса VPN представлен ниже:



Передача маршрутов

На вкладке **Передача маршрутов** можно настроить правила передачи маршрутов клиентам. Маршруты передаются клиенту в момент установления VPN-подключения. Изменения маршрутов (например, добавление статических маршрутов) после подключения не применяются и становятся доступны пользователю только при повторном подключении к VPN.

Ideco Client поддерживает обновление маршрутов без разрыва соединения.

Маршруты, переданные Ideco NGFW Novum для VPN-клиента, имеют меньшую метрику (т. е. высокий приоритет).

Для настройки правил нажмите **Добавить**:

Расшифровка полей

- **Название** - укажите название правила.
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Отправка маршрутов** - выберите, как будут передаваться маршруты:
  - **Не отправлять** - маршруты не передаются клиенту, трафик не будет проходить через NGFW Novum.
  - **Отправлять весь трафик на Ideco NGFW Novum** - передается маршрут 0.0.0.0/0, весь трафик направляется через NGFW Novum.
  - **Отправлять маршруты до всех сетей, маршрутизируемых через LAN-интерфейсы и IPsec-туннели** - передаются маршруты до всех локальных сетей NGFW Novum, в том числе подключенных через IPsec и маршрутизируемых, кроме маршрутов: **OSPF**, **BGP**, **PBR** и **Маршрутизации внешних сетей**.
  - **Отправлять маршруты до сетей, указанных на LAN-интерфейсах** - передаются маршруты до локальных сетей NGFW Novum, без учета IPsec и маршрутизируемых.
  - **Отправлять только указанные** - выберите сети, до которых будут передаваться маршруты.
- **Исключение адресов из маршрута** - выберите сети, исключенные из маршрута.
- **Комментарий** - укажите комментарий к правилу (опционально).

Если маршруты VPN-клиентов пересекаются с маршрутами, передаваемыми Ideco NGFW Novum, то выберите **Не отправлять** или **Отправлять только указанные**.

Если при подключении по VPN (IKEv2, L2TP, SSTP) не удается получить маршруты до сетей Ideco NGFW Novum, указанное число маршрутов не вмещается в опции DHCP-пакета.

При исключении подсети, IP-адреса, домена из передаваемого маршрута может возникнуть разбиение на несколько маршрутов. Это может привести к тому, что все маршруты не вместятся в опции DHCP-пакета.

Если количество байт в опции маршрутов превышает 255, то маршруты не передаются службой **ideco-vpn-dhcp-backend**.

Если пакет DHCP превышает 576 байт, то пакет может быть проигнорирован клиентом DHCP и применение маршрутов не произойдет (зависит от реализации клиента).

Перемещение правил

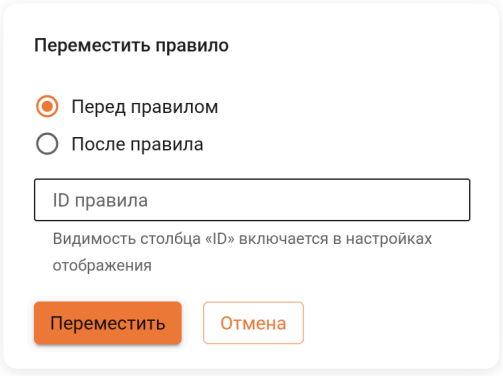
На вкладках **Доступ по VPN**, **Выдача IP-адресов** и **Передача маршрутов** предусмотрено перемещение правил.

Выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Полезные ссылки

- **Инструкции по созданию VPN-подключений**

- **Двухфакторная аутентификация**
- **Сервисы**
- **Создание подключения в Astra Linux**
- **Создание VPN-подключения в Fedora**
- **Создание подключения в Windows**
- **Создание подключения в Mac OS**
- **Как избежать проблем с подключением VPN-клиентов при нескольких серверах**
- **Создание VPN-подключения в Alt Linux**
- **Создание VPN-подключения в Ubuntu**
- **Создание VPN-подключения на мобильных устройствах**

Подключение по IKEv2/IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | VK Видео



IKEv2/IPsec - протокол, который используется для создания защищенного соединения между двумя устройствами в сети.

Рекомендуем использовать IKEv2/IPsec для обеспечения максимальной скорости и безопасности.

Протокол использует корневой сертификат для проверки подлинности участников соединения. Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство пользователя не требуется.

Для аутентификации применяется связка логин и пароль пользователя Ideco NGFW Novum или пользователя из Active Directory.

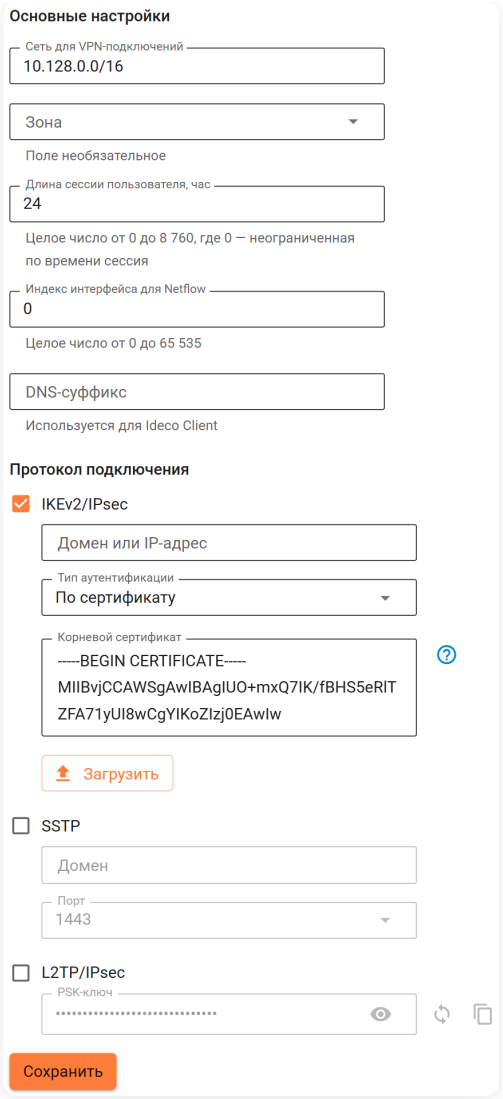
Не применяйте Wildcard-сертификаты для IKEv2/IPsec. Эти сертификаты не поддерживаются IPsec-клиентами из-за ограничений в проверке доменных имен.

Настройка Ideco NGFW Novum

Не рекомендуем использовать для VPN-подключений кириллические логины и пароли, а так же указывать в качестве логина IP-адрес.

Основные настройки

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**, включите опцию **IKEv2/IPsec** и заполните поля:

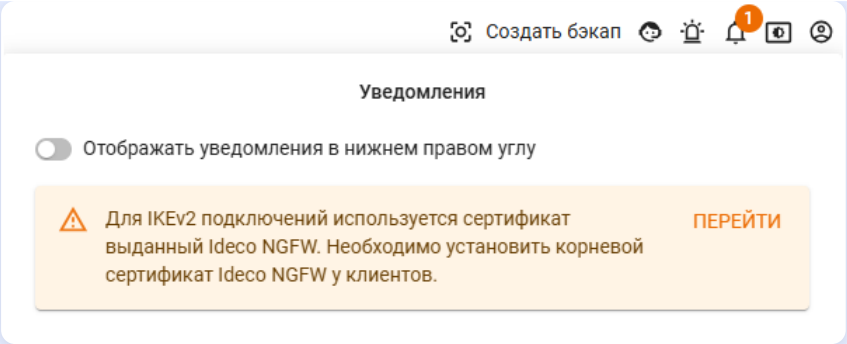


- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

2. Нажмите **Сохранить**.

- Если используется сертификат Let's Encrypt, то дополнительных действий не требуется.
- Если сертификат для VPN-подключений издан NGFW, появится уведомление о необходимости установить корневой сертификат Ideco NGFW Novum у клиентов:



- Если используете сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле **Subject Alternative Name (SAN)**. Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Передача клиентам маршрутов до ваших локальных сетей происходит автоматически. Для управления доступом к сетям используйте Межсетевой экран.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее - в статье VPN-подключения.

Поддержка клиентов IKEv2/IPsec в ОС

- Microsoft **Windows 10** и выше. Требует установки корневого сертификата Let's Encrypt. Инструкция по настройке.
- Apple **MacOS X 10.11** "El Capitan" (2015 г.) и выше. Инструкции по настройке.
- Linux NetworkManager plugin (с 2008 г.). Инструкция по настройке Alt Linux.
- Google **Android 11** (2020 г.) и выше. На более ранних версиях можно использовать приложение StrongSwan. Инструкция по настройке.
- Apple **iOS 9** (iPhone 4S, 2015 г.) и выше. Инструкция по настройке.

Полезные ссылки

- **Создание VPN-подключения в Fedora**
- **Создание подключения в Windows**
- **Создание VPN-подключения на мобильных устройствах**

Подключение по SSTP

Классический контекст | Высокопроизводительный контекст

По возможности не используйте подключение по SSTP. Подключение по SSTP лучше других проходит через NAT, но при нестабильном качестве связи работает значительно хуже, чем другие VPN (особенно при передаче звука/видео), так как инкапсулирует все данные внутри TCP. Рекомендуется использовать IKEv2/IPsec.

SSTP - протокол туннелирования трафика, который обеспечивает безопасное соединение между клиентом и сервером через интернет.

Протокол использует корневой сертификат для проверки подлинности участников соединения. Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство пользователя не требуется.

Для аутентификации применяется связка логин/пароль пользователя Ideco NGFW Novum или пользователя из Active Directory.

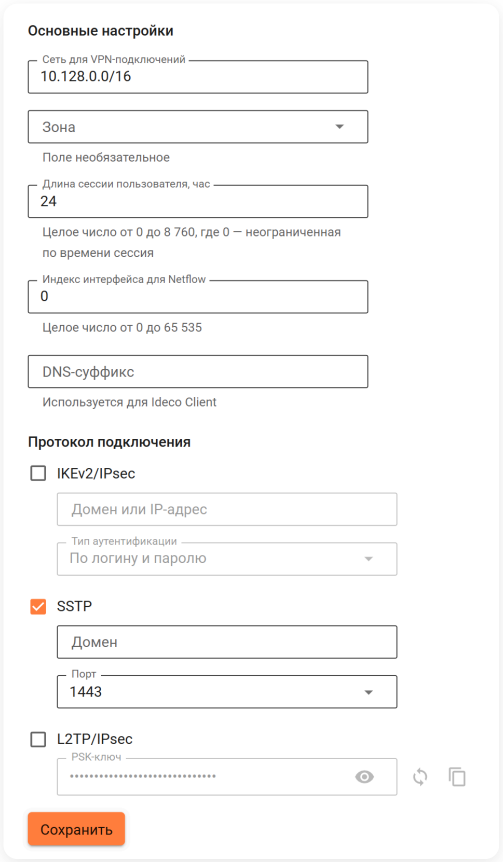
Особенности работы:

- Запрещено использовать домен `.local`. Подключение по SSTP поддерживается только из внешних сетей.
- Не рекомендуется использовать логины на кириллице для VPN-подключений. Это может привести к проблемам с подключением.
- NGFW Novum не поддерживает подключение MikroTik по SSTP, так как MikroTik использует устаревший и небезопасный алгоритм SHA-1.

Настройка Ideco NGFW Novum

Основные настройки

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное** и включите опцию **Подключение SSTP**:



- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

- **Домен** - укажите DNS-имя. IP-адрес внешнего интерфейса Ideco NGFW Novum должен резолвиться в одно из имен вашей внешней доменной зоны. Используйте реальное имя с правильной A-записью, т.к. реальное имя необходимо для выписки сертификата Let's Encrypt.
- **Порт** - выберите предлагаемый порт из вариантов: 1443, 2443, 3443, 4443.

2. Нажмите **Сохранить**.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключения.

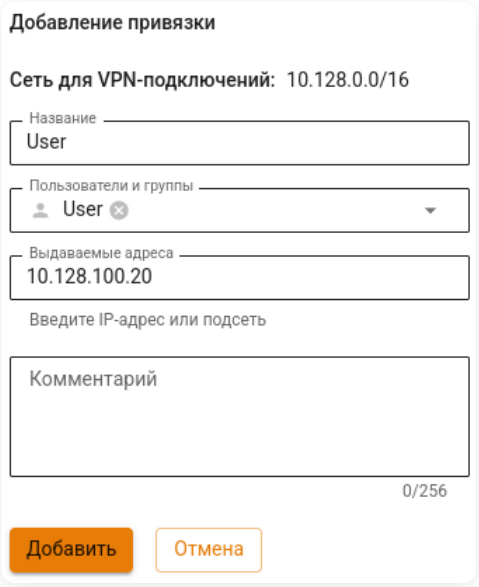
Правила выдачи IP-адресов

IP-адрес пользователю назначается автоматически из пула адресов для VPN, настраиваемого в разделе **Пользователи** → **VPN-подключения** (например, из подсети 10.128.0.0/16).

Настройте **статическую** привязку адресов, выдаваемых по VPN определенным пользователям:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Выдача IP-адресов**.

2. Нажмите **Добавить** и укажите название сети, нужного пользователя и IP-адрес:



3. Нажмите **Добавить** для сохранения изменений.

Правила передачи маршрутов

Выберите режим передачи маршрутов клиентам при добавлении правила в **Пользователи** → **VPN-подключения** → **Передача маршрутов**. Подробнее в статье VPN-подключение.

Полезные ссылки

- В случае, если установлено VPN-соединение, но не удается получить доступ к ресурсам локальной сети, рекомендуется обратиться к статье Особенности маршрутизации и организации доступа.
- Инструкции по настройке VPN-подключений на разных ОС доступны по ссылке.
- **Создание подключения в Windows**
- **Подключение по SSTP Wi-Fi роутеров Keenetic**

Подключение по L2TP/IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Видеоинструкцию смотрите по ссылке:

- Youtube
- docs.ideco.ru

По возможности не используйте L2TP/IPsec-подключение, которое может работать нестабильно, обладает огромной избыточностью, низкой производительностью и поддерживает не самое сильное шифрование. Вместо этого рекомендуется IKEv2/IPsec. Все современные ОС поддерживают IKEv2, либо для них есть приложения.

L2TP/IPsec - протокол позволяет создавать защищенные VPN-соединения между устройствами, обеспечивая конфиденциальность и целостность передаваемых данных.

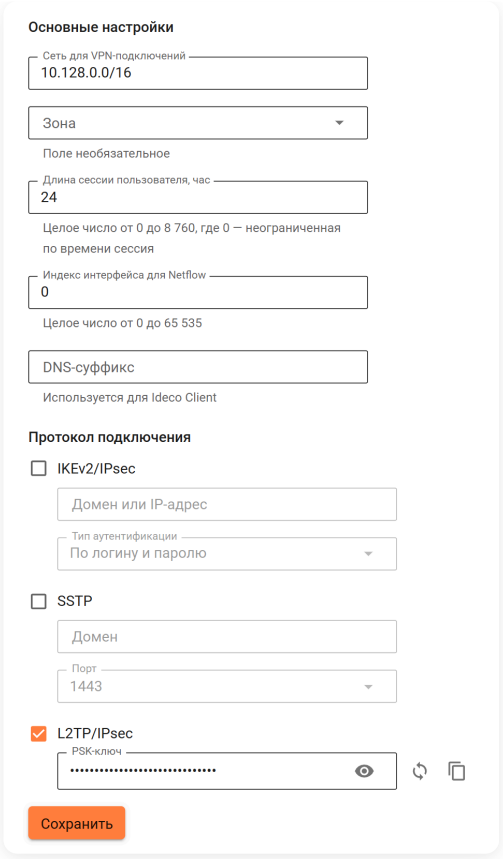
Для аутентификации используется связка логин/пароль пользователя Ideco NGFW Novum или пользователя из Active Directory, а также PSK-ключ, который был указан при настройке соединения.

Не рекомендуем использовать для VPN-подключений кириллические логины. А так же указывать в качестве логина IP-адрес.

Настройка Ideco NGFW Novum

Основные настройки

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное** и включите опцию **Подключение по L2TP/IPsec**:



- **Индекс интерфейса для Netflow** - введите целое число от 0 до 65535 для идентификации интерфейса, если используете Netflow.
- **PSK** - укажите секретную фразу (PSK-ключ).

2. Нажмите **Сохранить**.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключения.

Полезные ссылки

- L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если клиентов больше одного. Решить проблему может помочь инструкция.
- В случае, если установлено VPN-соединение, но не удается получить доступ к ресурсам локальной сети, рекомендуется обратиться к статье Особенности маршрутизации и организации доступа.
- Инструкции по настройке VPN-подключений на разных ОС доступны по ссылке.

Особенности маршрутизации и организации доступа

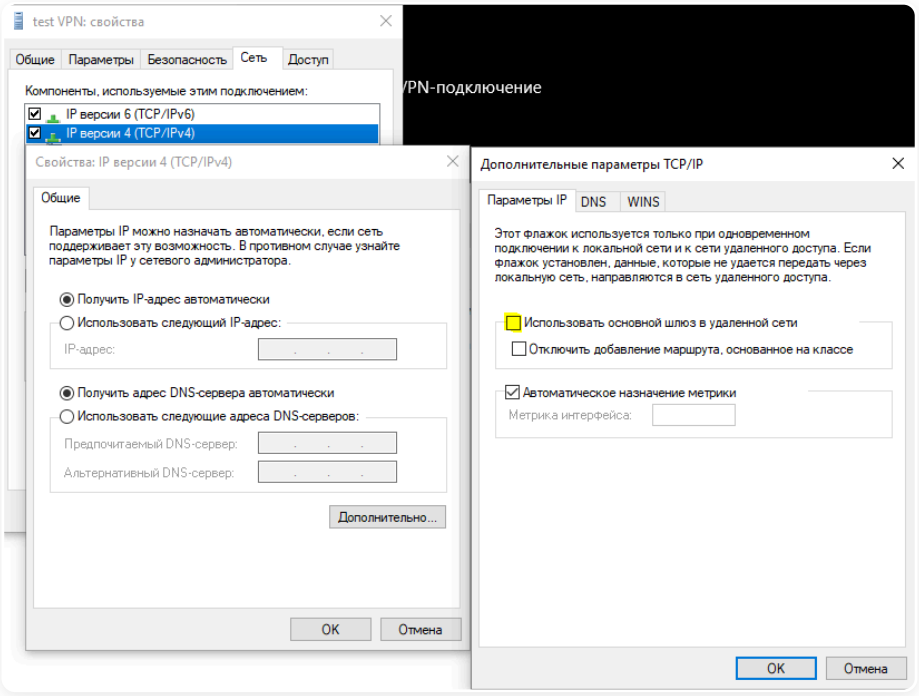
Классический контекст | Высокопроизводительный контекст

В статье рассматриваются потенциальные проблемы, связанные с доступом к ресурсам локальной сети через VPN, и предлагаются решения, такие как настройка маршрутов, исключение определенных сетей в антивирусном ПО и создание правил SNAT на NGFW Novum.

Организация доступа по VPN только к ресурсам локальной сети

Для организации доступа выполните действия:

1. В **Сеть** → **IP версии 4** → **Дополнительно** → **Параметры IP** уберите флаг **Использовать основной шлюз в удаленной сети**:



Особенности VPN-соединения с доступом только к ресурсам локальной сети

При выборе типа передачи маршрутов **Отправлять только указанные сети** маршрут до VPN-сервера и DNS-сервера построен не будет.

Если в NGFW Novum добавить передачу IP-адреса VPN-сервера NGFW Novum (DNS), то маршрут восстановится, а домен будет преобразовываться со следующими особенностями:

- Таблица с включенным шлюзом:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.5      5
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255          On-link         127.0.0.1    331
    192.168.100.2  255.255.255.255          On-link        10.200.0.5      5
  192.168.100.130  255.255.255.255          On-link        10.200.0.5      5
    192.168.122.0    255.255.255.0          On-link    192.168.122.10    281
   192.168.122.10  255.255.255.255          On-link    192.168.122.10    281
  192.168.122.255  255.255.255.255          On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0          On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0          On-link    192.168.122.10    281
  255.255.255.255  255.255.255.255          On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255          On-link    192.168.122.10    281
===========================================================================
```

- Таблица с отключенным шлюзом:

- Таблица с отключенным шлюзом и добавленной публикацией IP NGFW Novum:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.4     26
       10.200.0.4  255.255.255.255          On-link        10.200.0.4    281
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
```

Маршрут до сервера (в примере - 10.200.0.1) добавляется, но имеет более низкий приоритет, чем маршрут по-умолчанию. Соответственно запросы обрабатываются с задержкой и не обрабатываются при перехвате маршрутом по-умолчанию.

Рекомендуем вручную указать маршрут до DNS NGFW Novum, либо добавить маршрут в список публикуемых маршрутов на стороне NGFW Novum. Также можно использовать сторонний DNS-сервер.
2. Пропишите маршрут до корпоративной сети. В Windows 8, 8.1, 10 автоматически создается маршрут на основе класса, в зависимости от адреса, полученного по VPN. Для IPsec-IKEv2 можно настроить автоматическое получение маршрута.

Пример маршрута: если корпоративная сеть имеет адрес `172.16.0.0/16`, а сеть для VPN-подключений, настроенная на Ideco NGFW Novum, имеет адрес `10.128.0.0/16`:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1
```

Маршрут может не работать, когда есть пинг до интерфейса `10.128.0.1`, но нет пинга до хостов в локальной сети. В этом случае при создании маршрута нужно указать номер интерфейса VPN-подключения:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn
```

- `nn` - номер интерфейса VPN-подключения, посмотреть который можно при активном VPN-подключении в выводе в консоли команды `route print` раздел "Список интерфейсов".

Не удается получить доступ к компьютерам в локальной сети Ideco NGFW Novum

Для получения доступа к компьютерам в локальной сети Ideco NGFW Novum убедитесь, что:

1. Локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. В противном случае доступ к сети организации будет невозможен (трафик будет идти через физический интерфейс, а не через VPN).

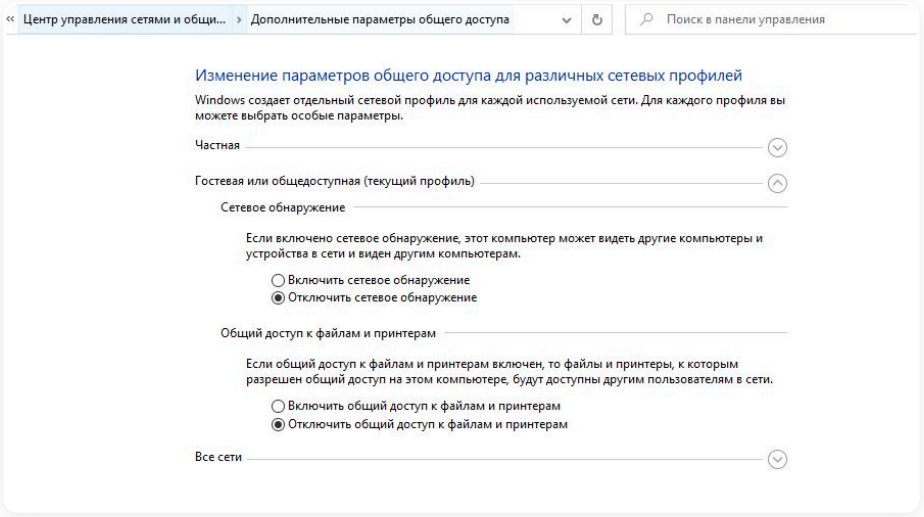
2. На компьютерах локальной сети основным шлюзом должен быть Ideco NGFW Novum. Если это не так, то вручную необходимо прописать соответствующий маршрут, чтобы сетевые пакеты шли на Ideco NGFW Novum для VPN-сети. **Например**:

```
route -p add 10.128.0.0 mask 255.255.0.0 10.1.1.1
```

- `10.128.0.0/16` - адрес VPN-сети Ideco NGFW Novum (настраивается в разделе **Пользователи** → **VPN-подключения**).
- `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW Novum.

3. На Ideco NGFW Novum в разделе **Межсетевой экран** → **FORWARD** нет запрещающих правил.

4. Компьютеры и серверы на Windows не ограничивают доступ к сетевым папкам с помощью правил настроек профилей сети (как на стороне подключающегося по VPN компьютера, так и на стороне компьютеров и серверов локальной сети):



Получение доступа к файлам и принтерам для профиля "Все сети" и "Частные сети"

Для получения доступа выполните действия:

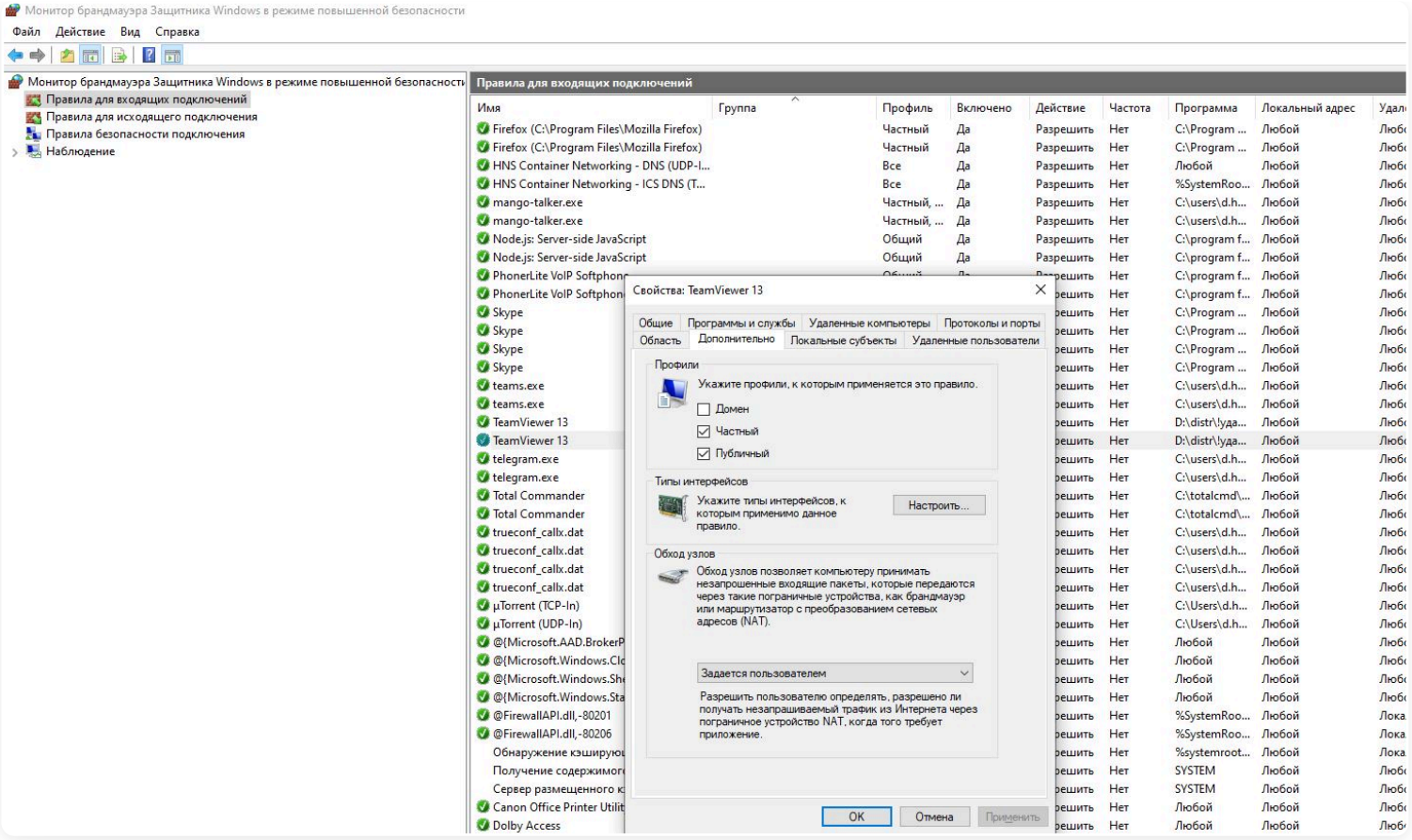
1. Перейдите в PowerShell (запустите PowerShell с повышением прав до администратора).

2. Выполните команду: `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`.

Возможные проблемы:

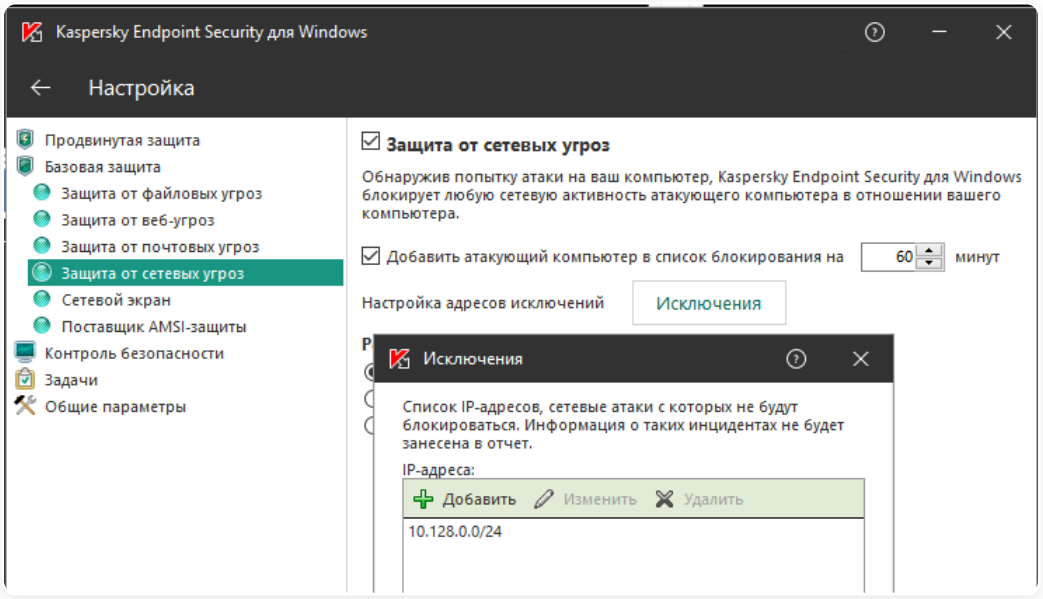
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей.

  Проверьте это в настройках входящих и исходящих подключений (необходимо разрешить доступ из частных и локальных сетей):



- Антивирусное ПО на компьютере может блокировать доступ из нелокальных сетей. Либо блокировать доступ конкретных программ.

  Например, для **Kaspersky Endpoint Security** нужно добавить сеть для VPN-подключений (по умолчанию `10.128.0.0/16`) в исключения:



Получение доступа к локальной сети Филиала

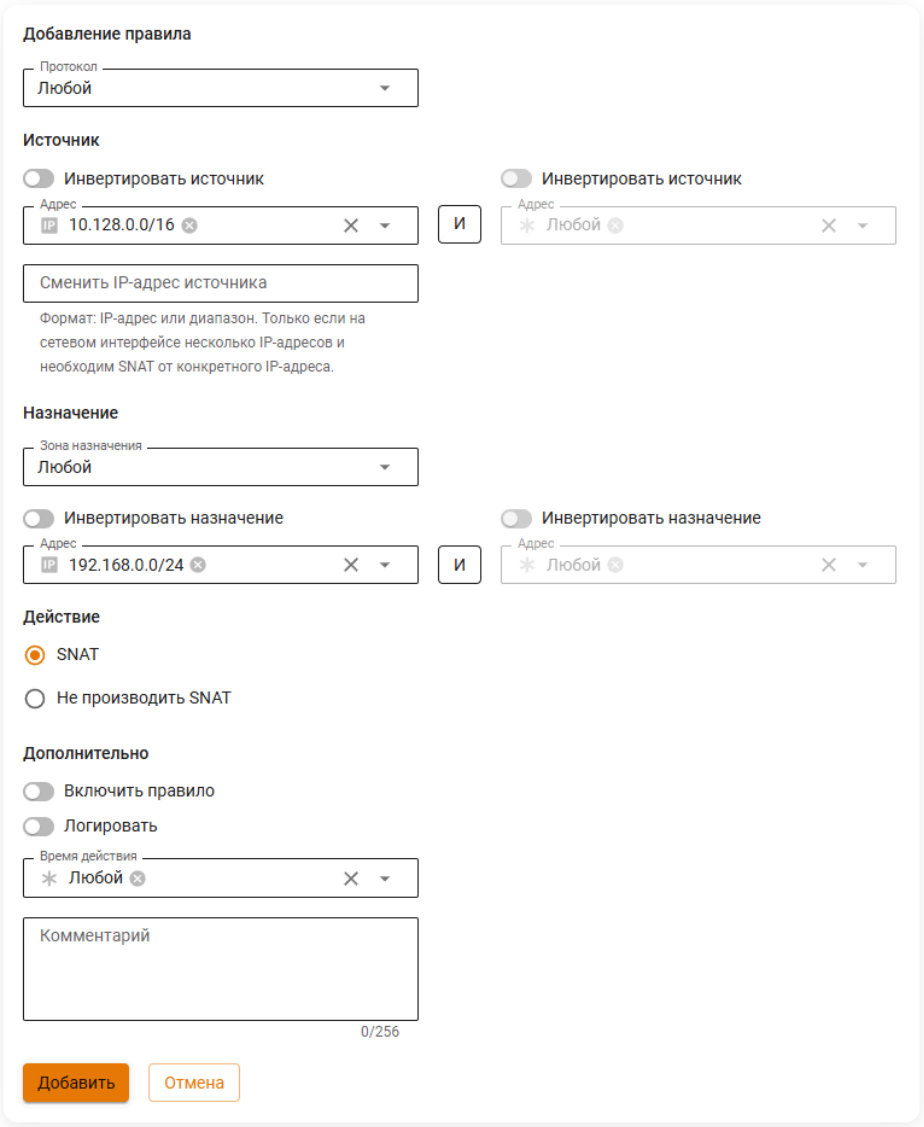
Чтобы обеспечить доступ, убедитесь, что VPN-сети обоих NGFW Novum не пересекаются. Затем проверьте настройки основного NGFW Novum, следуя инструкциям, описанным в статье.

Получение доступа к хостам локальной сети, если за NGFW Novum есть маршрутизатор, выступающий в качестве ядра локальной сети

Чтобы обеспечить доступ, нужно настроить на роутере маршрут от нужной локальной сети до VPN-сети. Для настройки маршрута на роутере укажите в качестве назначения VPN-сеть (`10.128.0.0/16`), в качестве шлюза - NGFW Novum (`172.16.0.1`).

Если настроить на роутере маршрут невозможно, можно создать на NGFW Novum SNAT-правило:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **SNAT**, нажмите **Добавить** и укажите параметры:



- **Источник** - VPN-сеть (`10.128.0.0/16`).
- **Назначение** - сеть за роутером, к которой требуется получить доступ из VPN-сети (`192.168.0.0/24`).

3. Нажмите **Добавить**.

В этом случае при отправке пакетов на роутер NGFW Novum подменит IP-адрес источника своим. За счет этого роутер направит ответ от хоста в локальной сети на NGFW Novum, который затем перенаправит его в VPN-сеть.

У хостов из локальной сети `192.168.0.0/24` не будет доступа к VPN-сети `10.128.0.0/16`.

Полезные ссылки

- **Как избежать проблем с подключением VPN-клиентов при нескольких серверах**

Инструкция по запуску PowerShell скриптов

Классический контекст | Высокопроизводительный контекст

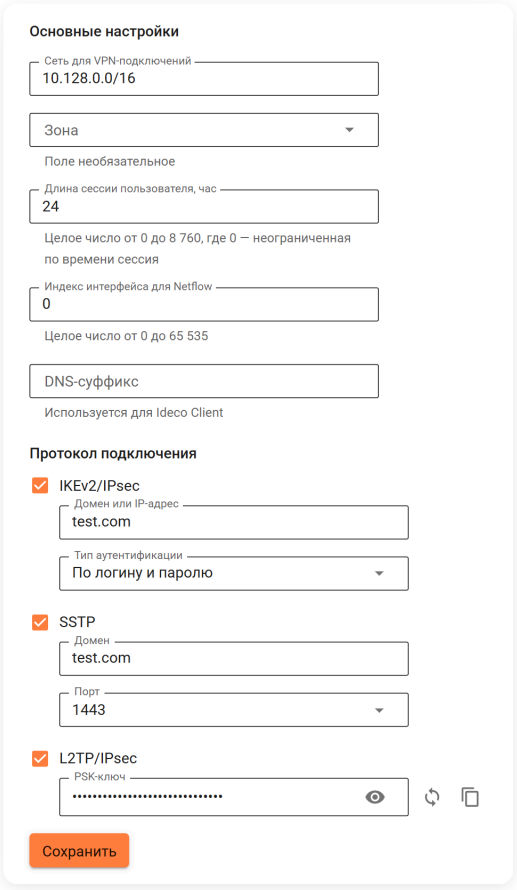
Для подключения по VPN к Ideco NGFW Novum с белым IP адресом достаточно действий, указанных ниже. Если Ideco NGFW Novum выходит в интернет через маршрутизатор, воспользуйтесь пунктом Подключение по VPN к Ideco NGFW Novum с доступом в интернет через маршрутизатор.

Запуск PowerShell-скрипта

1. Скачайте скрипт одним из способов:

Веб-интерфейс Ideco NGFW Novum

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**:



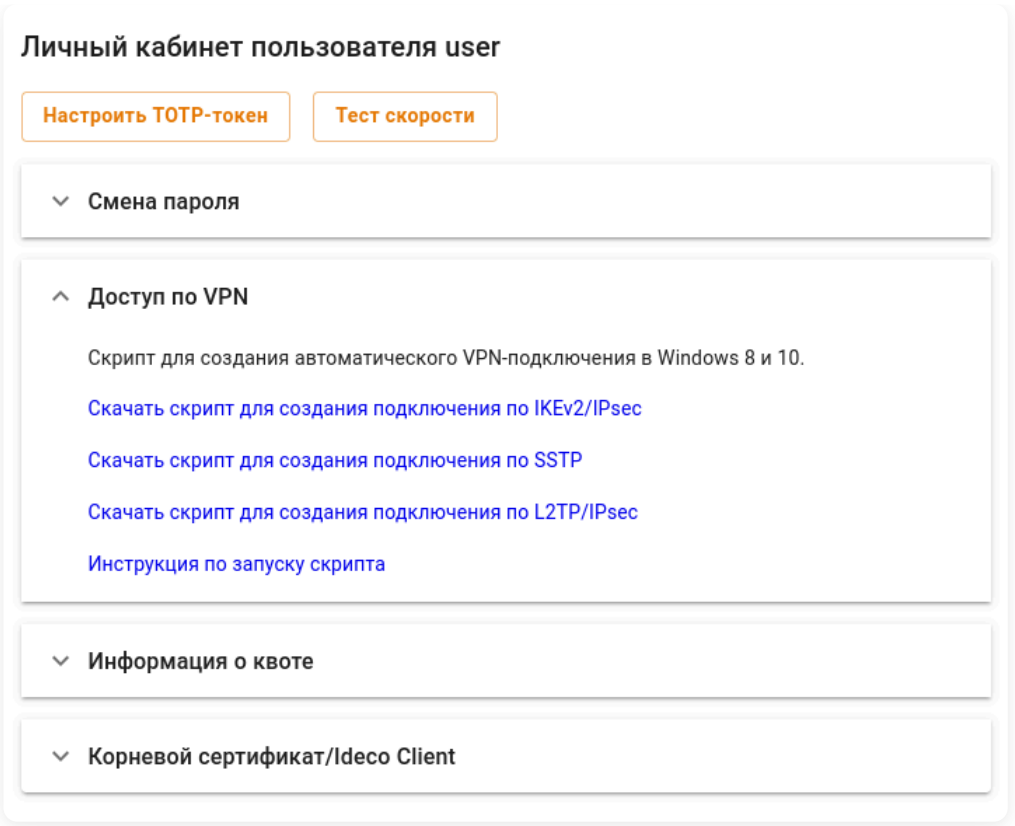
2. Включите и настройте требуемый протокол подключения.

3. Перейдите по ссылке **PowerShell - скрипт для настройки подключений**.

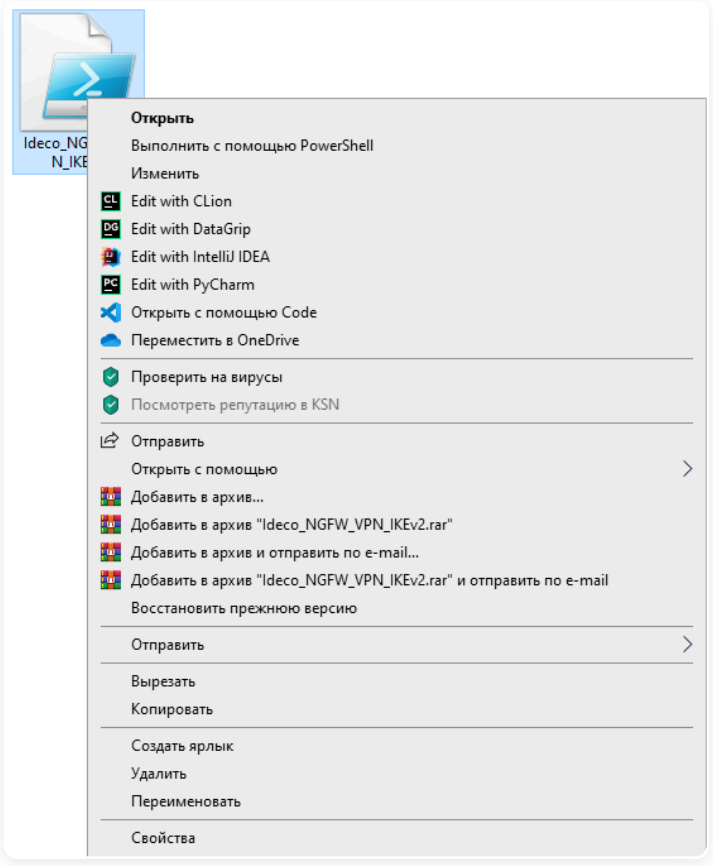
4. Перенесите скачанный файл на устройство, на котором требуется создать VPN-подключение.

Личный кабинет пользователя

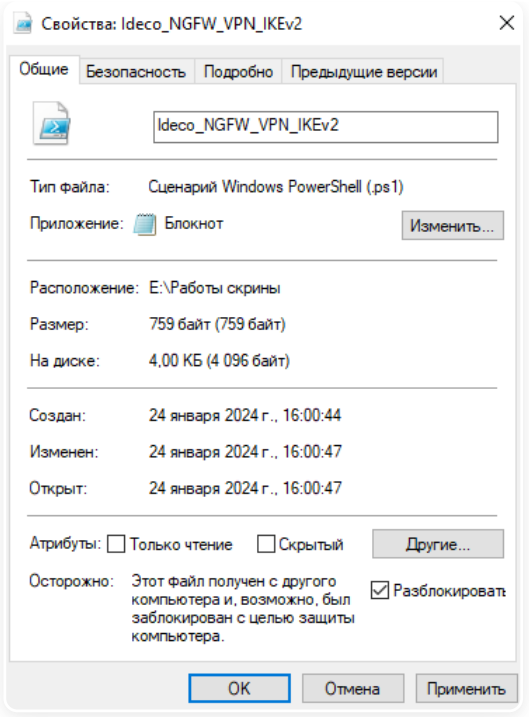
Скачайте скрипт, перейдя по ссылке **Скачать скрипт для создания подключения**:



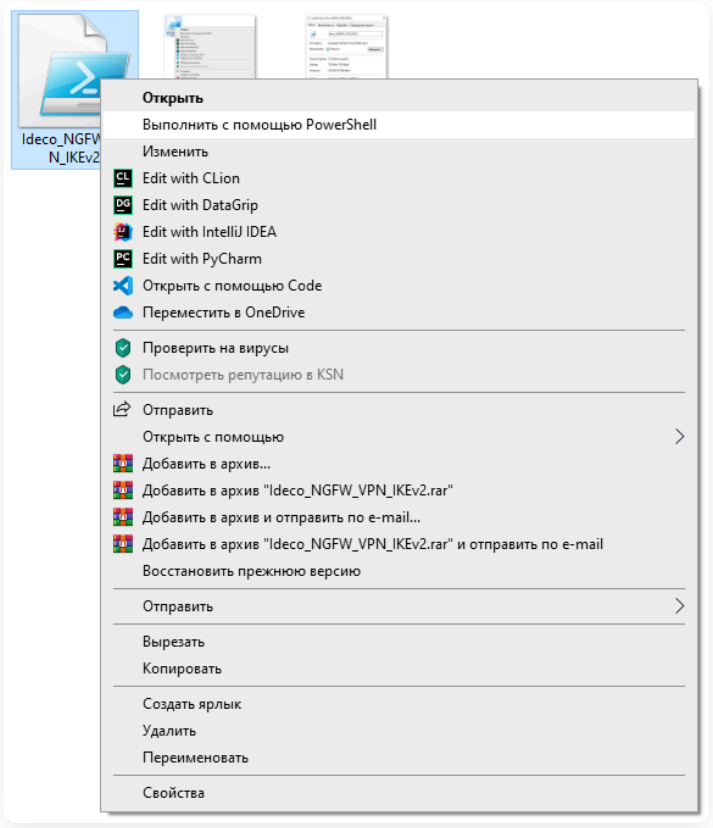
2. Щелкните правой кнопкой мыши по скачанному файлу и в контекстном меню выберите **Свойства**:



3. Включите опцию **Разблокировать** справа в нижнем углу свойств файла (по умолчанию ОС блокирует выполнение скачанных из интернета файлов):

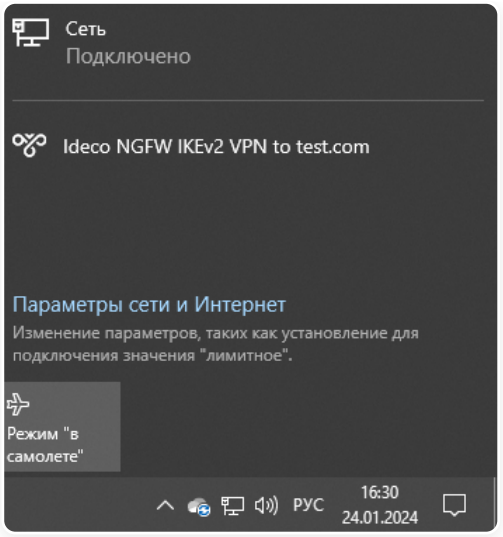


4. Нажмите правой кнопкой мыши на файл и выберите пункт **Выполнить в PowerShell**. Затем подтвердите действие, нажав **Да** на вопрос о внесении изменений в компьютер:



При появлении ошибки **Выполнение сценариев отключено в этой системе** откройте PowerShell с правами администратора, выполните команду для разрешения запуска скриптов `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`, в том же окне заново выполните скрипт для создания подключения и закройте консоль.

5. Когда подключение создано, нажмите **Подключиться** в списке сетей.



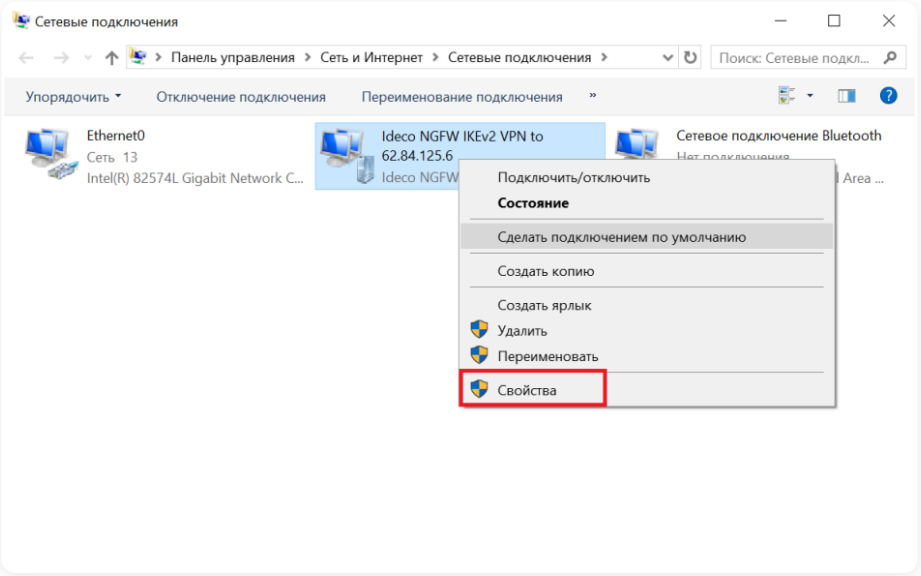
DNS-суффиксы для VPN-подключений

PowerShell-скрипты прописывают основной DNS-суффикс для создаваемого VPN-подключения. DNS-суффикс соответствует домену, в который введен Ideco NGFW Novum, что позволяет обращаться к устройствам за VPN по короткому имени.

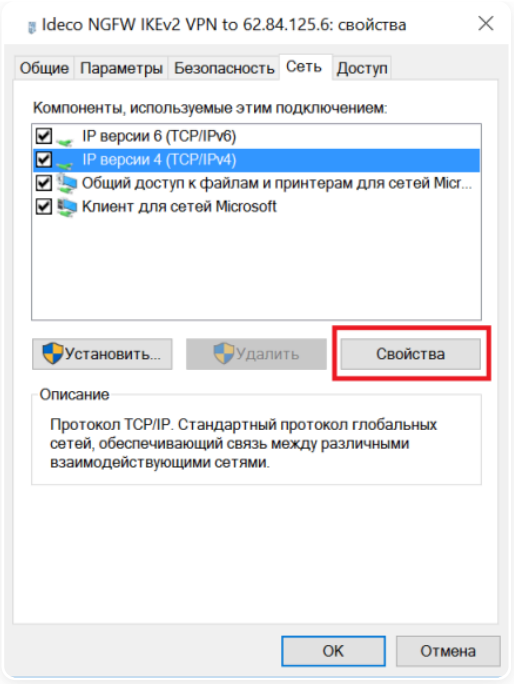
> Если Ideco NGFW Novum введен в несколько доменов, то DNS-суффиксы в PowerShell-скриптах не прописываются. Необходимо настроить DNS-суффиксы вручную на подключенном по VPN устройстве.

Чтобы настроить DNS-суффиксы для созданного VPN-подключения в Windows, выполните действия:

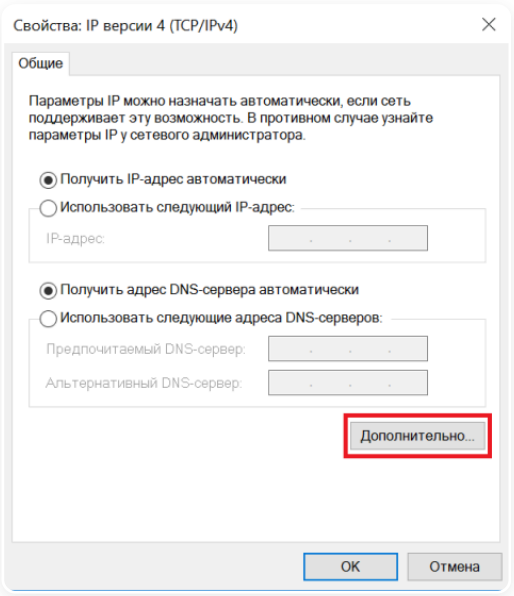
1. Перейдите в **Сетевые подключения**, нажмите правой кнопкой мыши по нужному VPN-подключению и выберите **Свойства**:



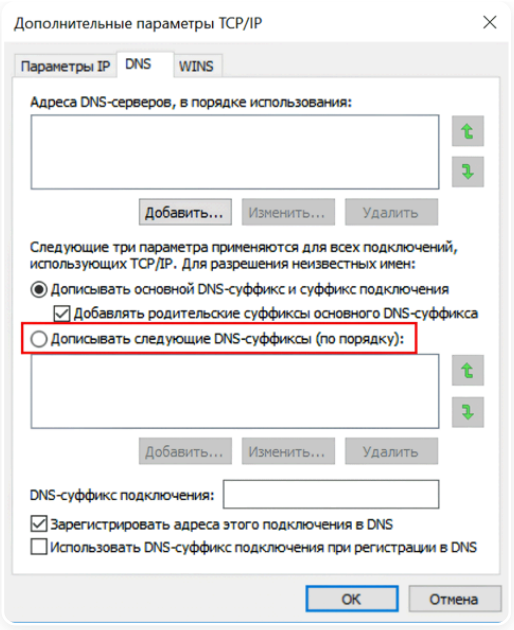
2. В открывшемся окне перейдите на вкладку **Сеть**, выберите компонент **IP версии 4 (TCP/IPv4)** и нажмите **Свойства**:



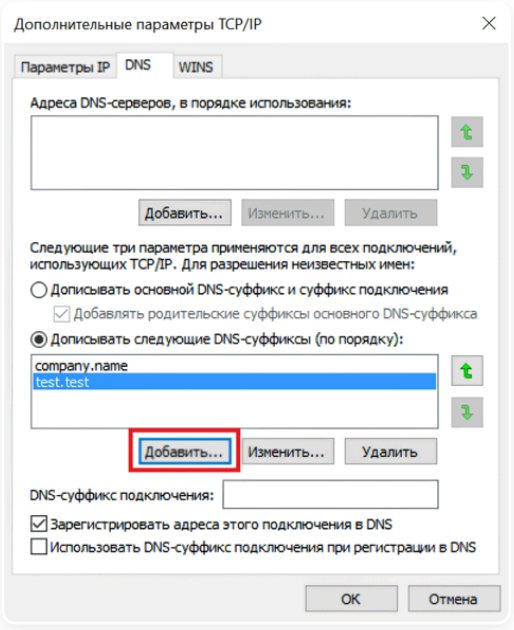
3. В открывшемся окне нажмите **Дополнительно**:



4. Перейдите на вкладку **DNS** и включите опцию **Дописывать следующие DNS-суффиксы (по порядку)**:



5. Нажмите **Добавить** и введите необходимые DNS-суффиксы:



При обращении к компьютеру по короткому имени DNS-суффиксы будут перебираться в порядке расположения. Порядок можно менять стрелками.

Подключение по VPN к Ideco NGFW Novum с доступом в интернет через маршрутизатор

Для работы скрипта подключения по VPN выполните действия:

1. Сделайте проброс портов 4500 и 500 в IP-адрес Ideco NGFW Novum в локальной сети маршрутизатора.

2. Загрузите скрипт на компьютер, воспользовавшись пунктом 1 инструкции Запуск PowerShell-скрипта.

3. Поменяйте в загруженном скрипте IP-адрес Ideco NGFW Novum на внешний IP-адрес маршрутизатора:

```
Add-VpnConnection
    -Force `
    -Name "Ideco NGFW L2TP VPN to 46.36.23.99" `
    -TunnelType L2TP `
    -ServerAddress 46.36.23.99 `
     -AuthenticationMethod MSChapV2 -L2tpPsk 'Jge7b11K_uEO_KYm3ArHcu50wWGjga' `
    -EncryptionLevel "Required" `
    -SplitTunneling $False `
    -RememberCredential
```

- **46.36.23.99** - IP-адрес Ideco NGFW Novum в локальной сети маршрутизатора.
- **5.189.21.1** - внешний IP-адрес маршрутизатора.

4. После выполнения действий следуйте инструкции Запуск PowerShell-скрипта с пункта 4.

Решение проблем запуска PowerShell-скрипта

Для запуска Powershell-скрипта убедитесь, что:

- Вам хватает прав на запуск скрипта.
- PowerShell установлен в системе.

Если не удалось решить проблему запуска PowerShell-скрипта, воспользуйтесь инструкцией для создания подключения в Windows 10 вручную.

Ideco Client

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Ideco Client**: `ideco-agent-backend`, `ideco-agent-websocket`, `ideco-websocket-vpn-server`.

Список служб для других разделов доступен по ссылке.

Ideco Client - программа-клиент, которая управляет авторизацией пользователей при подключении к NGFW Novum. Работает по одному из двух протоколов:

- **Wireguard** - используется собственный коммуникационный протокол, который реализует зашифрованные виртуальные частные сети (VPN). Для его работы используется порт UDP 3051.
- **TCP** - используется современный протокол транспортного уровня безопасности TLS (Transport Layer Security), обеспечивающий функции шифрования, аутентификации и целостности. Для его работы используется порт 443 по умолчанию.

С версии 22 NGFW Novum сессии Ideco Client синхронизируются между нодами кластера. При кратковременных разрывах соединения (до 60 секунд) Ideco Client автоматически восстанавливает подключение без повторного ввода пароля, прохождения 2FA и аутентификации по сертификату. Если соединение не восстановилось за 60 секунд, потребуется повторная авторизация вручную.

Логика выбора протокола Ideco NGFW Novum

С версии 21 для Ideco Client протокол определяется на основе правил в таблице **Пользователи → VPN-подключения → Доступ по VPN**:

- Если в первом сработавшем правиле для пользователя указан протокол подключения **Любой** или **Wireguard (Ideco Client)**, в том числе вместе с **TLS (Ideco Client)**, то используется **Wireguard**.
- Если в первом сработавшем правиле для пользователя указан протокол подключения **TLS (Ideco Client)**, то используется **TLS**.
- Правило применяется ко всем VPN-подключениям, включая терминальный сервер и Device VPN, с любым видом аутентификации. Действует из внешних и локальных сетей при включенной опции **С установлением туннеля**.

Особенности для разных типов подключений:

- Для локальной сети:
  - Если включена опция **С установлением туннеля**, используется протокол из правил **Доступа по VPN**.
  - Если включена опция **Без туннеля**, туннель не устанавливается, таблица **Доступа VPN** не проверяется. Доступ открывается по списку в поле **Пользователи и группы**.
- Для терминального подключения всегда используется **Wireguard**, т.к. **TLS** не поддерживается. При указании в правилах только **TLS (Ideco Client)** соединение будет отклонено с ошибкой, указанной в системном журнале в разделе **Отчеты и журналы → Система**.

Ideco Client недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

Поддерживаемые версии ОС	• Windows 10 22H2 и выше • macOS версии 13.4 и выше. При этом Ideco Client работает с некоторыми ограничениями • Astra Linux 1.7.0 и выше • РЕД ОС 8.0 и выше • Alt OS (Alt Workstation) 9.0 и выше • Fedora 35 и выше • Ubuntu 18.04 LTS (23.04) и выше

Порты для подключения, если NGFW Novum за NAT	• **80 TCP** - используется для работы сертификатов Let's Encrypt • **443 TCP** - используется для авторизации пользователя и установки управляющего соединения (порт по умолчанию) • **14765 TCP** - альтернативный порт для авторизации и управляющего соединения. Чтобы использовать его, укажите адрес сервера в формате `домен:14765` или `IP:14765` • **3051 UDP** - используется для передачи пользовательского трафика через туннель WireGuard. Трафик на этом порту фильтруется правилами таблицы FORWARD, а не INPUT **Межсетевого экрана** Для корректной работы Ideco Client убедитесь, что указанные порты открыты на всех устройствах между пользователем и Ideco NGFW Novum

Возможности Ideco Client

- [x] Авторизация в локальной сети
- [x] VPN-подключение из внешних сетей
- [x] VPN-подключение из локальных сетей
- [x] Режим работы Device VPN
- [x] Двухфакторная аутентификация
- [x] Трехфакторная аутентификация
- [x] Привязка устройств к пользователям по сертификатам
- [x] Сбор данных о подключающихся устройствах

Сбор данных о подключающихся устройствах позволяет задавать критерии проверки - HIP-профили.

HIP-профили помогают реализовать ZTNA (Zero Trust Network Access) - технологию, которая обеспечивает безопасный доступ к сети на основе принципа **нулевого доверия**. ZTNA контролирует и аутентифицирует устройства пользователей перед предоставлением доступа к ресурсам сети.

Скачать Ideco Client

Windows

Скачать Ideco Client

Для версии 10 и новее, Windows Server 2019 и новее.

macOS

Скачать Ideco Client

Для версии 13.4 и новее.

Linux

Скачать Ideco Client

Для Alt Linux, Red OS, Astra Linux.

Каждой версии NGFW Novum соответствует определенная версия Ideco Client. При обнаружении несоответствия Ideco Client автоматически обновляется до требуемой версии при подключении.

Полезные ссылки

- **Настройка Device VPN**
- **Создание сертификатов для Device VPN**
- **Сертификаты**
- **Кастомная настройка Ideco Client**

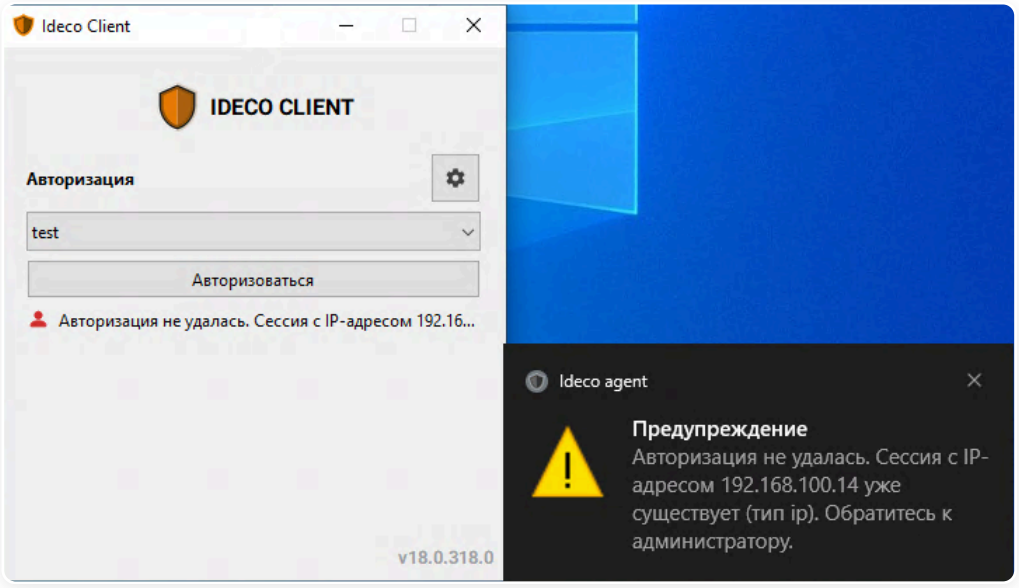
- **Настройки в Ideco NGFW Novum**
- **Как включить режим отладки для Ideco Client**
- **Подключение через Ideco Client к внутреннему DNS**

Особенности работы Ideco Client

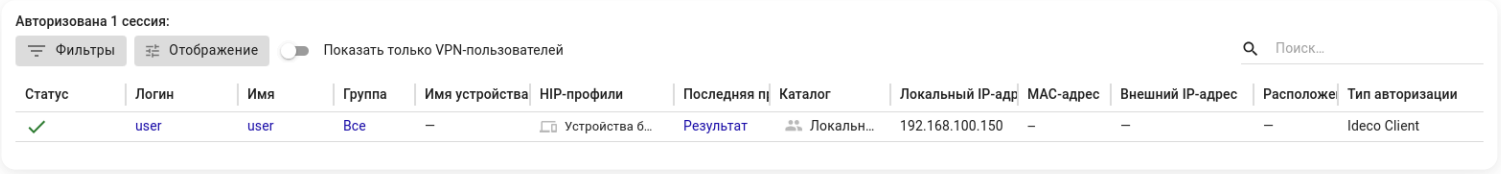
Классический контекст | Высокопроизводительный контекст

Особенности работы Ideco Client, которые важно учитывать при настройке и использовании:

- Только один профиль может быть с опцией автоподключения. Если активировать автоподключение для другого профиля, у предыдущего эта опция отключится.
- Чтобы использовать SSO-профиль с автоподключением, вручную укажите доменное имя в поле **Хост**. Для предварительной настройки адреса подключения используйте групповую политику или запустите файл через командную строку с ключом: `IdecoClient.msi utm_address=адрес_ngfw`.
- При попытке повторной авторизации пользователя, который уже авторизован по IP, появляется предупреждение:



- После каждого обновления приложение Ideco Client запускается автоматически.
- Информация о сессиях пользователей отображается в разделе **Сессии пользователей**:



Особенности работы DNS-запросов при VPN-подключении через Ideco Client

При подключении через Ideco Client DNS-запросы могут не проходить, если выбран тип передачи маршрутов **Отправлять только указанные сети**. При выборе **Отправлять маршруты до локальных сетей Ideco NGFW Novum** сеть до NGFW Novum отправляется автоматически. Это связано с особенностями построения таблицы маршрутизации при подключении через Ideco Client:

- При VPN-подключении без Ideco Client DNS-запросы идут на DNS, прописанный в настройках подключения (как правило, адрес NGFW Novum).
- При VPN-подключении через Ideco Client DNS-запросы идут на адрес NGFW Novum, но в передаваемом на Ideco Client списке нет маршрута до DNS NGFW Novum.

Рекомендуем при выборе типа передачи маршрутов **Отправлять только указанные сети** добавить в список DNS NGFW Novum, чтобы клиент VPN построил таблицу маршрутизации до этой сети.

Особенности маршрутизации и организации доступа по VPN к ресурсам локальной сети описаны в статье.

Как работает перенос настроек с профилями при смене версии

При запуске Ideco Client выполняет последовательность действий:

1. Ideco Client проверяет наличие настроек в json-файле настроек профиля текущей версии.

2. Если настройки найдены, они применяются.

3. Если настройки текущей версии отсутствуют, ищет в json-файлах настроек прошлых версий (от новой к старой).

4. При нахождении настроек в предыдущих версиях они копируются в json-файл настроек текущей версии Ideco Client.

5. Если настройки не найдены, то создается json-файл настроек текущей версии с параметрами по умолчанию.

Файл настроек профиля хранится по пути:

- Linux: `$HOME/.config/Ideco/Agent/<version>/`
- Windows: `C:/Users/<Имя_пользователя>/AppData/Local/Ideco/Agent/<version>/`
- macOS: `$HOME/Library/Preferences/Ideco/Agent/<version>/`

Алгоритм поиска и применения настроек

- Поиск осуществляется последовательно по мажорным и минорным версиям от новой к старой.
- Копирование происходит только вперед с более ранней версии на новую.
- Копируются первые найденные настройки.
- Назад по версиям копирование не осуществляется.
- Если вручную удалить json-файл настроек текущей версии, то при следующем запуске Ideco Client инициирует поиск и копирование настроек. Если настройки не будут найдены в json-файлах настроек предыдущих версий, то будет создан json-файл с настройками по умолчанию.

Примеры работы переноса настроек

Первая установка Ideco Client

Ideco Client не установлен и в каталоге нет json-файла настроек Ideco Client:

1. При запуске Ideco Client создает json-файл настроек текущей версии с параметрами по умолчанию.

2. Копирование не выполняется.

Обновление Ideco Client на следующую версию

Пользователь обновляет Ideco Client с 21.3.2 до 22.0.703:

1. Ideco Client проверяет наличие настроек в json-файле настроек версии 22.0.703.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в json-файлах настроек предыдущих версий от более новой к более старой.

4. Если настройки найдены в json-файле настроек одной из прошлых версий, то они копируются в json-файл настроек версии 22.0.703.

5. Если настройки не найдены, то создается json-файл настроек версии 22.0.703 с параметрами по умолчанию.

Возврат Ideco Client на предыдущую версию

Возврат Ideco Client с версии 22.0.2 на 22.0.1:

1. При запуске Ideco Client ищет настройки в json-файле настроек версии 22.0.1.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в json-файлах настроек предыдущих версий от более новой к более старой.

4. Если настройки найдены, они копируются в json-файл настроек версии 22.0.1.

5. Если настройки не найдены, то создается json-файл настроек версии 22.0.1 с параметрами по умолчанию.



Копирование не происходит назад по версиям, поэтому копирование настроек из версии 22.0.2 на 22.0.1 невозможно.

Повторное обновление Ideco Client после возврата на предыдущую версию

1. Пользователь использовал версию 22.0.2.

2. Выполнен возврат на версию 22.0.1.

3. Пользователь создал новый профиль в версии 22.0.1

4. Выполнено обновление до версии 22.0.2.

5. При запуске Ideco Client настройки и профили из версии 22.0.1 не будут перенесены в версию 22.0.2, поскольку json-файл настроек версии 22.0.2 уже существует, созданный при первом запуске.

Алгоритм работы Ideco Client при редиректах

После формирования списка для подключения Ideco Client пытается подключиться к серверам из списка. Если отправлен редирект с кодом ответа `302`, то Ideco Client продолжит подключение по указанному в редиректе адресу до успешной установки соединения.

Если сервер возвращает редирект с кодом ответа `302`, Ideco Client не ищет SRV-записи для нового адреса. Ideco Client подключится по адресу, полученному в редиректе.

При попытке подключения к хостам из списка могут возникнуть циклические редиректы. На Ideco Client есть ограничение в пять редиректов. При шестом редиректе подключение к текущему серверу считается неуспешным.

Обработка запросов с редиректом позволяет использовать VPN-балансировщик для распределения нагрузки между несколькими NGFW Novum.

Балансировка VPN-подключений происходит на стороне Ideco Client с использованием SRV-записей DNS.

В SRV-записи DNS нельзя указывать IP-адрес, только FQDN (полностью определенное доменное имя, не имеющее неоднозначностей в определении). При указании IP-адреса в SRV-записи IP-адрес будет распознан как поддомен зоны. Подробнее про SRV-записи в RFC-2782.

Если в параметре `target` SRV-записи указан `.`, подключение не сработает. Появится сообщение, что сервис недоступен. Параметр `target` SRV-записи `.` может настраиваться при регистрации доменного имени или при конфигурации записей для доменного имени.

Алгоритм работы Ideco Client при балансировке

При нажатии **Подключиться** Ideco Client проверяет адрес сервера, заданный в настройках профиля, и составляет список для подключения, основываясь на следующих правилах:

1. Если адрес сервера - IP-адрес, то происходит подключение Ideco Client по этому адресу.
2. Если адрес сервера - FQDN, то происходит запрос SRV-записей вида `_ideco-client._tcp.<FQDN домена>` (например: `_ideco-client._tcp.ideco.example.ru`) для указанного FQDN:

- Если для текущего FQDN есть SRV-записи, то происходит добавление SRV-записей в список для подключения. Записи сортируются по параметру `priority`. Если значения совпадают, сортировка продолжается по параметру `weight`. Подробнее про сортировку `weight` в RFC-2782.
- Если для текущего FQDN нет SRV-записей, то происходит разрешение FQDN в IP-адрес с помощью записи типа A и Ideco Client подключается по этому IP-адресу.

Как Ideco Client обрабатывает запросы с редиректом на сервер Ideco NGFW

Ideco Client может обрабатывать запросы с перенаправлением (код ответа 302). Получив ответ от сервера, **Ideco Client** выполняет шаги для подключения к **Ideco NGFW Novum**:

1. Отправляет запрос на адрес https://host:443/connect.
2. Если сервер отвечает статусом 302 с редиректом, **Ideco Client** использует информацию из этого ответа для установления соединения.
3. **Ideco Client** подключается к NGFW, используя имя сервера или IP-адрес, указанный в поле Location.

Важно:

- Адрес обязательно должен включать порт `443`.
- В заголовке Location в ответе 302 должен быть указан полный URL-адрес, из которого будет извлечено только имя сервера или IP-адрес.
- Полученное имя сервера или IP-адрес используются для создания адреса в формате `wss://host_from_location:443/connect`, к которому будет подключаться **Ideco Client**.
- Если ответа со статусом 302 от адреса `https://host:443/connect` нет, то **Ideco Client** подключится к NGFW по адресу `wss://host:443/connect`.

Пример правильного редиректа, полученный с помощью утилиты **curl**:

1. **Запрос**: `curl -il https://host.dev:443/connect`.

2. **Ответ**:

```
HTTP/1.1 302 Found
Server: SERVERNAME
Date: Fri, 15 Nov 2024 04:22:46 GMT
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=15
Location: https://ngfw-host.dev/
cache-control: no-cache
```

Из заголовка `Location: https://ngfw-host.dev/` будет извлечен новый хост `ngfw-host.dev`, и **Ideco Client** будет подключаться к NGFW по адресу `wss://ngfw-host.dev:443/connect`.

3. Если при попытке доступа к URL-адресу `https://host.dev:443/connect` не будет получен ответ с кодом 302, то **Ideco Client** подключится к NGFW по адресу `wss://host.dev:443/connect`.

Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

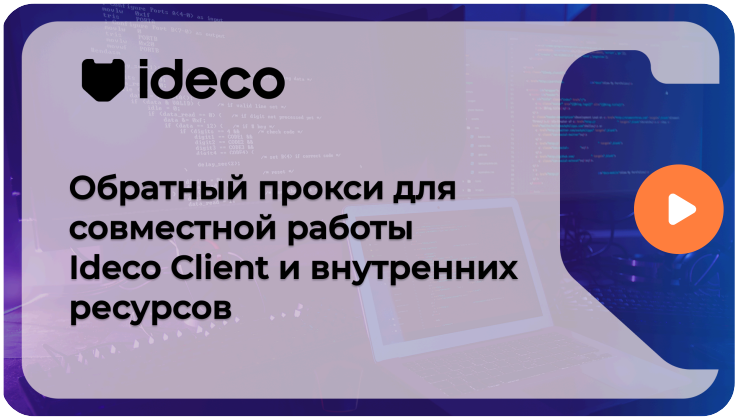
- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Ideco Client не работает, если внутренние ресурсы опубликованы через DNAT

Видеоинструкция

Ссылки на другие ресурсы

YouTube | RUTUBE | VK Видео



Ideco Client для работы использует TCP-порт 443 по умолчанию. Если этот порт занят правилами DNAT для публикации внутренних ресурсов (например, Microsoft Exchange), Ideco Client автоматически переключится на TCP-порт 14765 после неудачной попытки подключения.

Для корректной работы Ideco Client и внутренних ресурсов рекомендуем использовать обратный прокси. Этот способ позволит Ideco Client и внутренним ресурсам работать через один порт при помощи SNI-маршрутизации.

Если использование обратного прокси невозможно, зарезервируйте TCP-порт 443 за Ideco Client, а для публикации внутренних ресурсов назначьте другой TCP-порт.

Аутентификация по сертификату

Классический контекст | Высокопроизводительный контекст

Аутентификация по сертификату - механизм, при котором Ideco NGFW Novum проверяет подлинность устройства пользователя по цифровому сертификату. Сертификат дополняет проверку логина и пароля, а для подключений Device VPN заменяет ее: даже если учетные данные скомпрометированы, подключение с устройства без действующего сертификата не создается.

Аутентификация по сертификату реализована для подключений через Ideco Client и входит в концепцию ZTNA (Zero Trust Network Access). Ideco NGFW Novum сам выпускает сертификаты и управляет привязками пользователей к устройствам - отдельная PKI-инфраструктура не требуется.

Как работает аутентификация по сертификату

Подключение через Ideco Client состоит из двух этапов:

Этап 1. Проверка учетных данных. Пользователь вводит логин и пароль или проходит SSO. Ideco NGFW Novum проверяет учетные данные в локальной базе или во внешнем каталоге. Для Device VPN на этом этапе выполняется идентификация устройства без входа пользователя.

Этап 2. Проверка сертификата устройства. Если сертификат устройства уже установлен (независимо от режима), Ideco NGFW Novum выполняет его проверку:

1. Ideco NGFW Novum запрашивает сертификат устройства.

2. Ideco Client отправляет сертификат с доказательством владения закрытым ключом.

3. Ideco NGFW Novum проверяет сертификат:

- **Доверие к CA** - сертификат должен быть подписан одним из доверенных удостоверяющих центров, указанных в настройках.
- **Срок действия** - сертификат не должен быть просрочен.
- **Статус отзыва** - сертификат не должен быть отозван.

4. Если включена привязка устройства, Ideco NGFW Novum проверяет, совпадает ли сертификат с привязанным устройством.

Проверка сертификата устройства считается включенной:

- **Для туннельных подключений (VPN)** - если в правиле **Пользователи → VPN-подключения → Доступ по VPN** в поле **Доверенные CA-сертификаты** выбран хотя бы один сертификат удостоверяющего центра.
- **Для локальных подключений (без туннеля)** - если в настройках **Пользователи → Ideco Client → Основное** в блоке **Авторизация пользователей** выбран хотя бы один **Доверенный CA-сертификат**.
  Если поле **Доверенные CA-сертификаты** не заполнено, проверка сертификата устройства не выполняется.

Если все проверки пройдены, Ideco NGFW Novum создает VPN-сессию. Если хотя бы одна проверка не пройдена, подключение отклоняется, а причина отказа записывается в журнал **Отчеты и журналы → Аутентификация пользователей** и отображается в разделе **Мониторинг → Сессии пользователей**.

Закрытый ключ сертификата устройства на Ideco NGFW Novum не передается и хранится только на устройстве пользователя.

Привязка пользователя к устройству

Привязка фиксирует за учетной записью пользователя конкретное устройство. После создания привязки подключение с других устройств отклоняется, даже если на них установлен действительный сертификат, подписанный тем же CA.

Привязка появляется при первом удачном входе пользователя, когда в правиле доступа заполнено поле **Доверенные CA-сертификаты**, включена опция **Привязать устройство к пользователю** и с устройства предъявлен действующий сертификат. Работа со списком привязок, удаление и автоматическое пересоздание привязки описаны в статье Настройка Ideco Client.

На учетные записи и группы **Ideco Device VPN** привязка не распространяется.

Режимы управления сертификатом устройства

Способ, которым сертификат попадает на устройство, зависит от режима работы Ideco Client:

- **AUTO** - Ideco NGFW Novum автоматически выпускает сертификат при первом подключении пользователя. Участие администратора не требуется. Сертификат выпускается только после успешной проверки учетных данных и используется при всех последующих подключениях пользователя, включая Device VPN.
- **MANUAL** - сертификат выпускается внешним удостоверяющим центром по CSR от Ideco Client. Режим подходит для корпоративной PKI-инфраструктуры.
- **EXTERNAL** - готовую пару **сертификат + закрытый ключ** предоставляет администратор.

Режимы определяют только способ, которым ключ и сертификат попадают на устройство. После установки ключа и сертификата Ideco Client переходит в готовое состояние и не хранит информацию об источнике. **Любое переключение режима удаляет установленные ранее ключ и сертификат** - переходы AUTO → EXTERNAL, EXTERNAL → AUTO, AUTO → MANUAL, MANUAL → EXTERNAL и обратные работают одинаково: прежнее состояние сбрасывается, и администратор должен установить ключ и сертификат заново в соответствии с выбранным режимом.

Команды CLI для переключения режимов и правила хранения закрытых ключей на разных ОС описаны в статье Настройка Ideco Client.

Работа сертификата с Device VPN

Device VPN не может самостоятельно запустить автоматический выпуск сертификата. Поведение зависит от того, установлен ли на устройстве сертификат от предыдущих подключений пользователя:

- **Сертификат уже установлен** - пользователь ранее авторизовался на Ideco NGFW Novum через Ideco Client и получил сертификат в режиме AUTO. Этот же сертификат используется для подключения Device VPN без дополнительных действий администратора.
- **Сертификата нет** - администратор устанавливает сертификат на устройство вручную в режиме EXTERNAL. Переключение режима удаляет установленные ранее ключ и сертификат.

Порядок настройки Device VPN и выпуска сертификата через OpenSSL описан в статье Создание сертификатов для Device VPN.

Настройка аутентификации по сертификату

Для включения аутентификации по сертификату настройте три раздела:

Что настраивается	Где настраивается
Учетная запись пользователя	**Пользователи → Учетные записи**
Доверенные CA-сертификаты	**Сервисы → Сертификаты → Ideco Client → Реестр**
Правило доступа VPN и привязка устройства	**Пользователи → VPN-подключения → Доступ по VPN** - блок **Настройки доступа через Ideco Client**

Для подключений из локальной сети без туннеля (опция **Без туннеля**) сертификат и привязка настраиваются в **Пользователи → Ideco Client → Основное**.

Ограничения

- Автоматический выпуск сертификата применим только к пользовательским подключениям. Для Device VPN автоматический выпуск не выполняется.
- Поддерживается одна активная привязка на пользователя.
- Автоматическая проверка CRL/OCSP для внешних CA не выполняется.
- Сертификаты должны соответствовать X.509, DN должен однозначно сопоставляться с устройством.

Восстановление доступа после отзыва сертификата устройства

После отзыва сертификата устройства на Ideco NGFW Novum пользователь не сможет подключиться. Отменить отзыв сертификата невозможно.

> Описанный порядок действий применим к режиму AUTO. В режимах MANUAL и EXTERNAL установите новый сертификат в соответствии с выбранным режимом.

Для восстановления доступа выполните действия:

1. На устройстве пользователя удалите файл `device-cert.json`. Путь зависит от ОС и версии Ideco Client:

- **Windows**: `%SystemRoot%\System32\config\systemprofile\Ideco\Agent<версия Ideco Client>\device-cert.json`
- **macOS**: `/Library/Application Support/Ideco/Agent/<версия Ideco Client>/device-cert.json`
- **Linux**: `/root/.config/Ideco/Agent/<версия Ideco Client>/device-cert.json`

2. Перезапустите службу Ideco Service или перезагрузите ОС.

3. Если в настройках включена опция **Привязать устройство к пользователю**, перейдите в **Пользователи** → **Ideco Client** → **Привязанные устройства** и удалите запись привязки для данного пользователя.

При следующем подключении Ideco Client инициирует выпуск нового сертификата в режиме AUTO - сгенерирует закрытый ключ, сформирует CSR и отправит его на Ideco NGFW Novum для подписи. Если опция **Привязать устройство к пользователю** включена, новая привязка создается автоматически при первой успешной аутентификации.

Сценарии использования

- ✅ Удаленный доступ сотрудников к корпоративной сети: подключение идет с корпоративного устройства под учетной записью сотрудника через защищенный туннель
- ✅ Доступ подрядчиков к ограниченному набору ресурсов: сертификат выпускается на конкретное устройство, подключение с личного устройства подрядчика отклоняется
- ✅ Защита привилегированных учетных записей: фишинг логина и пароля не дает доступ без сертификата устройства и без доступа к привязанному устройству
- ✅ Соответствие требованиям регуляторов по многофакторной аутентификации при доступе к системам с персональными данными, КИИ, ГИС
- ✅ Реализация ZTNA в сочетании с HIP-профилями - добавляется проверка состояния устройства (антивирус, обновления ОС, шифрование диска)

Полезные ссылки

- **Ideco Client**
- **Настройка Ideco Client**
- **Device VPN**
- **Создание сертификатов для Device VPN**
- **Доступ по VPN**
- **Сертификаты**
- **HIP-профили**

Пользователи

Настройки в Ideco NGFW Novum

Основные параметры и конфигурация Ideco Client в Ideco NGFW Novum

Перейти >

Установка и настройка Ideco Client на разных ОС

Как установить Ideco Client на Windows, Linux, macOS

Перейти >

Установка и настройка Ideco Client на Windows

Как установить и настроить Ideco Client на Windows

Перейти >

Установка и настройка Ideco Client на macOS

Как установить и настроить Ideco Client на macOS

Перейти >

Установка и настройка Ideco Client на Linux

Как установить и настроить Ideco Client на Linux

Перейти >

Кастомная настройка Ideco Client

Настройка управления профилями и правами пользователей в Ideco Client через JSON-конфигурационный файл.

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройки в Ideco NGFW Novum

Классический контекст | Высокопроизводительный контекст

Подключение пользователей по VPN

Из внешней сети:

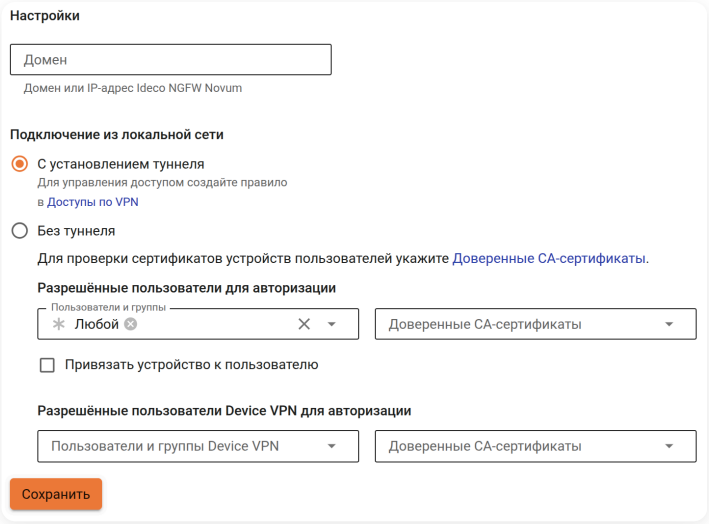
1. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN**.

2. Создайте правило, разрешающее пользователю VPN-подключение.

Из локальной сети:

1. Перейдите в **Ideco Client** → **Основное** и в поле **Домен** укажите доменное имя или IP-адрес Ideco NGFW Novum. Например: `example.ru`, `ideco.example.ru` или `52.251.83.117`.

2. В блоке **Подключение из локальной сети** выберите опцию **С установлением туннеля**:



3. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте правило, разрешающее пользователю VPN-подключение. В правиле настраиваются:

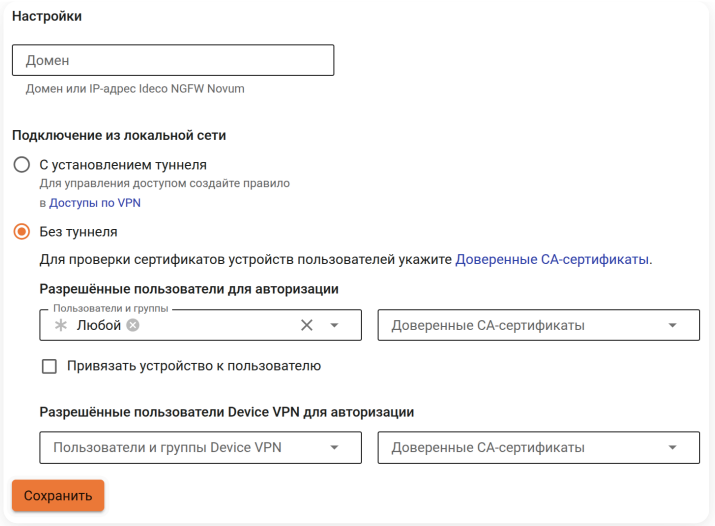
- Проверка сертификата устройства
- Привязка устройства к пользователю
- HIP-профили
- Двухфакторная аутентификация

Чтобы пользователь мог выйти в интернет, нужно выполнить одно из следующих действий:

- Настроить вторую сессию авторизации пользователя. Например, через Веб-аутентификацию.
- На вкладке Передача маршрутов для нужных пользователей выберите опцию **Отправлять весь трафик на Ideco NGFW Novum**.

Подключение пользователей из локальной сети без VPN

1. Перейдите в **Ideco Client** → **Основное** и в блоке **Подключение из локальной сети** выберите опцию **Без туннеля**:



2. Заполните поля:

- **Разрешенные пользователи для авторизации**:
  - **Пользователи и группы** - выберите пользователей или группы, которым разрешена авторизация.
  - **Доверенные CA-сертификаты** - выберите один или несколько сертификатов удостоверяющих центров, которым должно доверять устройство пользователя. Если поле пустое, проверка сертификата не выполняется. Проверка сертификата служит третьим фактором аутентификации, подтверждая подлинность устройства.
  - **Привязать устройство к пользователю** - включите опцию для создания записи в таблице **Привязанные устройства** при первом успешном подключении пользователя с этого устройства. После этого пользователь сможет подключаться только с этого устройства до удаления привязки.
- **Разрешенные пользователи Device VPN для авторизации**:
  - **Пользователи и группы Device VPN** - выберите учетные записи Device VPN (или группу **Ideco Device VPN**), которым разрешена авторизация.
  - **Доверенные CA-сертификаты** - выберите один или несколько сертификатов удостоверяющих центров, которым должно доверять устройство пользователя.

Изменения в настройке **Подключение из локальной сети** разрывает текущие сессии из локальных сетей. Повторное подключение будет соответствовать новому значению настройки.

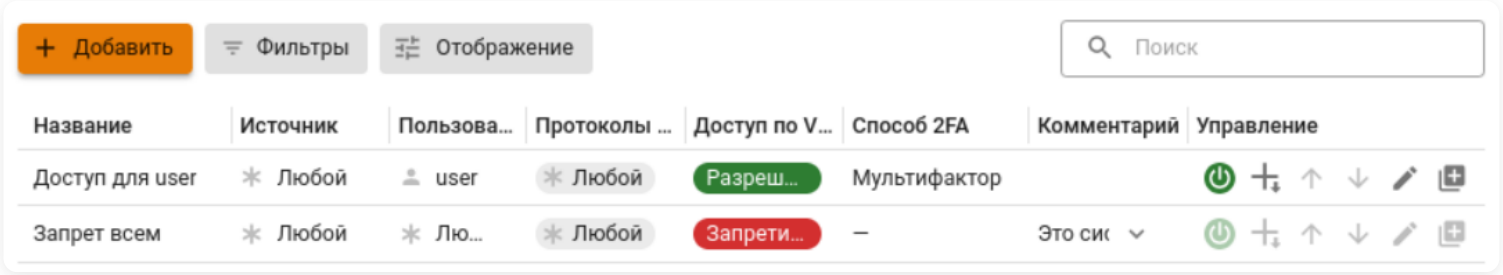
Настройка двухфакторной аутентификации в Ideco Client

В веб-интерфейсе Ideco NGFW Novum:

1. Создайте учетную запись пользователя в **Пользователи** → **Учетные записи**.

2. Перейдите в **Пользователи** → **Двухфакторная аутентификация** и выберите подходящие типы. Настройте двухфакторную аутентификацию способами, указанными в статье.

3. Добавьте правило в **Пользователи** → **VPN-подключения** → **Доступ по VPN**. В настройках правила укажите созданную учетную запись пользователя и тип двухфакторной аутентификации, выбранный в шаге 2. В поле **Протоколы** укажите значение **Любой**:

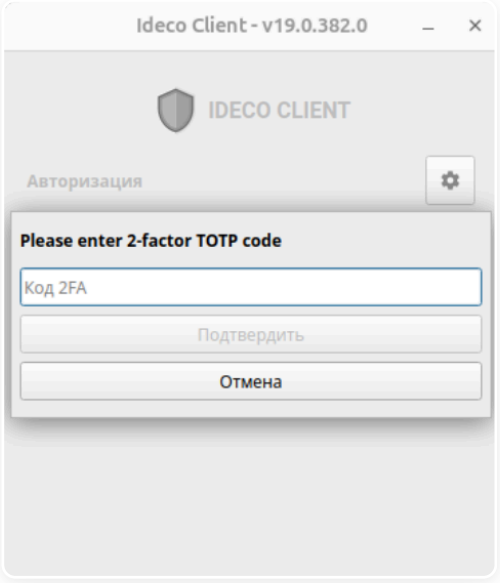


На устройстве пользователя:

1. Установите и запустите приложение Ideco Client. Инструкции по установке: Windows.

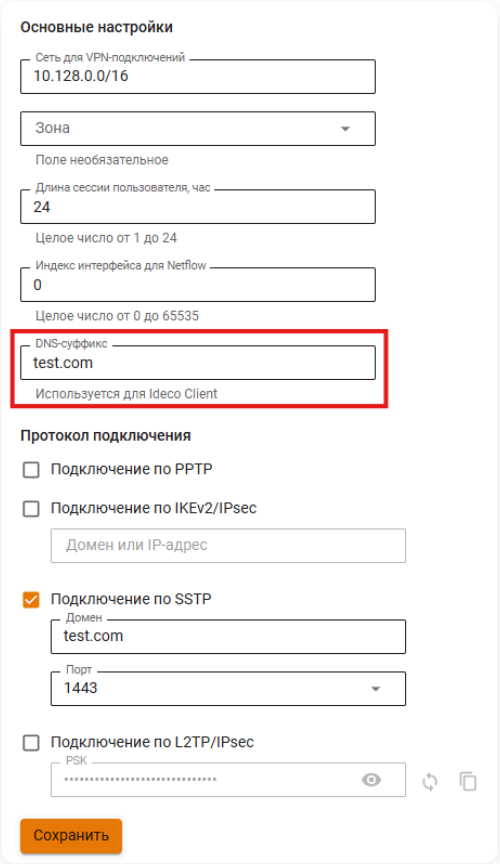
2. Авторизуйтесь через настроенную учетную запись пользователя:

3. Введите код двухфакторной аутентификации:



DNS-суффиксы для VPN-подключений по протоколу Wireguard

Укажите DNS-суффикс внутреннего домена (например, company.lan) в **Пользователи** → **VPN-подключения** → **Основное** → **DNS-суффикс** и нажмите **Сохранить**:



Суффикс будет передан устройствам через Ideco Client и позволит использовать короткие имена серверов (например, server-1c вместо server-1c.company.lan). Без суффикса разрешение таких имен работать не будет.

Ideco NGFW Novum поддерживает только один DNS-суффикс. Не указывайте DNS-суффикс, если NGFW Novum введен в несколько доменов.

Выпуск сертификата устройства

Сертификат устройства подтверждает подлинность устройства при подключении к Ideco NGFW Novum и служит третьим фактором аутентификации. Способ выпуска сертификата зависит от режима управления сертификатом устройства. По умолчанию используется режим AUTO - сертификат выпускается автоматически при первом подключении.

Выпуск сертификата в режиме AUTO недоступен для Device VPN. Если сертификат на устройстве отсутствует, подключение будет отклонено.

Сертификат для Device VPN создается вручную. Процесс описан в статье Создание сертификатов для Device VPN.

Режимы управления сертификатом устройства

Ideco Client поддерживает три режима управления сертификатом устройства: AUTO, MANUAL и EXTERNAL. Режим определяет, каким образом генерируется закрытый ключ, формируется запрос на подпись (CSR) и устанавливается сертификат.

Переключение между режимами выполняется через командную строку (CLI) Ideco Client.

При переключении режима текущий закрытый ключ и сертификат удаляются. Генерируется новый закрытый ключ. Если администратор задал DN, стандартный DN перезаписывается.

Режим AUTO

В режиме AUTO сертификат устройства автоматически выпускается Ideco NGFW Novum при отсутствии сертификата на устройстве. Участие администратора не требуется.

Порядок работы:

1. При первом запуске Ideco Client генерирует закрытый ключ и сохраняет его на устройстве.

2. При подключении к Ideco NGFW Novum пользователь проходит аутентификацию по первому фактору (логин/пароль).

3. Ideco Client формирует запрос на подпись (CSR) и отправляет его на Ideco NGFW Novum.

4. Ideco NGFW Novum подписывает CSR и возвращает сертификат.

5. Ideco Client проверяет соответствие сертификата закрытому ключу и сохраняет его на устройстве.

6. При последующих подключениях сертификат предъявляется Ideco NGFW Novum вместе с доказательством владения закрытым ключом.

Для сброса сертификата и возврата в режим AUTO выполните команду:

```
ideco-client --reset-to-auto-mode
```

Для сброса с указанием нового DN:

```
ideco-client --reset-to-auto-mode --set-dn "CN=hostname-example"
```

Если на устройстве есть сертификат Device VPN, при первом запуске он будет перенесен в хранилище сертификатов Ideco Client и использован как сертификат устройства. Новый закрытый ключ в этом случае не генерируется.

Режим MANUAL

В режиме MANUAL Ideco Client генерирует закрытый ключ и запрос на подпись (CSR), но не отправляет CSR на Ideco NGFW Novum. Администратор самостоятельно передает CSR во внешний удостоверяющий центр, получает подписанный сертификат и загружает его в Ideco Client.

До загрузки подписанного сертификата подключение к Ideco NGFW Novum невозможно.

Получение CSR

Для генерации CSR и вывода его в консоль выполните команду:

```
ideco-client --get-csr
```

Для сохранения CSR в файл укажите путь:

```
ideco-client --get-csr /path/to/output.csr
```

- `/path/to/output.csr` - путь для сохранения файла CSR.

Для генерации CSR с указанием нового DN:

```
ideco-client --get-csr /path/to/output.csr --set-dn "CN=hostname-example,O=MyOrg"
```

Загрузка подписанного сертификата

После получения подписанного сертификата от удостоверяющего центра загрузите его в Ideco Client:

```
ideco-client --set-cert /path/to/certificate.pem
```

- `/path/to/certificate.pem` - путь к файлу подписанного сертификата.

Ideco Client проверит соответствие сертификата закрытому ключу, валидность полей (DN, KU, EKU, срок действия) и сохранит сертификат на устройстве. После этого подключение к Ideco NGFW Novum станет доступно.

Параметр `--set-dn` не может использоваться как отдельная команда - только совместно с `--get-csr`.

Режим EXTERNAL

В режиме EXTERNAL используется заранее подготовленный сертификат устройства и закрытый ключ. Администратор самостоятельно предоставляет оба файла. Ideco Client не генерирует закрытый ключ.

Для загрузки сертификата и ключа одним файлом:

```
ideco-client --set-cert /path/to/cert-and-key.pem
```

- `/path/to/cert-and-key.pem` - путь к файлу, содержащему сертификат и закрытый ключ.

Для загрузки сертификата и ключа разными файлами:

```
ideco-client --set-cert /path/to/certificate.pem --set-key /path/to/private-key.pem
```

- `/path/to/certificate.pem` - путь к файлу сертификата;
- `/path/to/private-key.pem` - путь к файлу закрытого ключа.

Ideco Client проверит:

- Соответствие закрытого ключа сертификату.
- Наличие непустого CN в DN сертификата.
- Отсутствие полей CA и server-auth в расширениях KU/EKU.
- Минимальную стойкость алгоритма (RSA-2048 и выше).

Параметр `--set-dn` не применим к режиму EXTERNAL. При переключении в режим EXTERNAL сохраненный DN не перезаписывается - он будет использован, если администратор вернется в режим AUTO или MANUAL.

В таблице приведено сравнение режимов управления сертификатами:

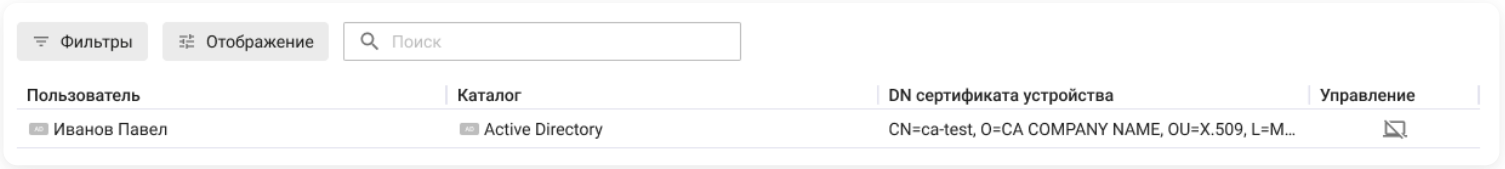
Действие	**AUTO**	**MANUAL**	**EXTERNAL**
Генерация закрытого ключа	Ideco Client	Ideco Client	Администратор
Подпись сертификата	Ideco NGFW Novum	Внешний удостоверяющий центр	Внешний удостоверяющий центр

Участие администратора	Не требуется	Передача CSR и загрузка сертификата	Загрузка ключа и сертификата
Подключение без сертификата	Сертификат выпускается при подключении	Недоступно	Недоступно

Порядок проверки сертификата устройства при подключении описан в статье Аутентификация по сертификату.

Привязанные устройства

В разделе **Пользователи** → **Ideco Client** → **Привязанные устройства** отображается список устройств, привязанных к пользователям. Привязка ограничивает доступ пользователя. После ее создания подключение возможно только с зафиксированного устройства:



Включение опции **Привязать устройство к пользователю** не создает записей в таблице. Записи появляются по мере того, как пользователи авторизуются.

Привязка создается автоматически при первой успешной авторизации пользователя, если:

- В настройках **Пользователи** → **Ideco Client** → **Основное** (для локального подключения без туннеля) или в правиле **Пользователи** → **VPN-подключения** → **Доступ по VPN** включена опция **Привязать устройство к пользователю**.
- Пользователь предоставил действительный сертификат устройства, подписанный доверенным CA.
- Для пользователя еще нет активной привязки.

Привязка не создается для пользователей и групп **Device VPN**.

Для удаления привязки нажмите в колонке **Управление**. Удаление необходимо, если пользователю нужно сменить устройство - новая привязка будет создана автоматически при следующем подключении.

После удаления привязки администратором она будет создана заново при следующей авторизации пользователя.

Если проверка привязки включена, а у пользователя нет привязанного устройства, доступ будет запрещен. При добавлении новых пользователей убедитесь, что для них создана привязка или проверка привязки отключена.

Установка и настройка Ideco Client на разных ОС

Классический контекст | Высокопроизводительный контекст

Поддерживаемые версии ОС и порты подключения

Поддерживаемые версии ОС	• Windows 10 22H2 и выше • macOS версии 13.4 и выше. При этом Ideco Client работает с некоторыми ограничениями • Astra Linux 1.7.0 и выше • РЕД ОС 8.0 и выше • Alt OS (Alt Workstation) 9.0 и выше • Fedora 35 и выше • Ubuntu 18.04 LTS (23.04) и выше
Порты для подключения, если NGFW Novum за NAT	• 80 TCP - используется для работы сертификатов Let's Encrypt • 443 TCP (по умолчанию), 14765 TCP (резервный) и 3051 UDP (для Wireguard) - используются Ideco Client

Возможности Ideco Client на разных ОС

Возможность	Описание	Windows	macOS	Linux
Установка	Установка клиента и службы (демона)	+	+	+
Настройка utm_address при установке	Позволяет настроить адрес сервера по умолчанию. Он будет использован при создании профиля	+		
Удаление	Удаление программы, но не профилей	+	+	+
Ручное обновление поверх	Ручная установка новой или предыдущей версии поверх существующей	+	+	+
Автообновление	Установка новой или предыдущей версии поверх существующей при подключении к NGFW Novum	+	+	+
Копирование профилей	Копирование профилей, если текущая версия меньше устанавливаемой и нет профилей в устанавливаемой версии	+	+	+
Редактирование профилей	Базовая функция	+	+	+
Постоянное хранение профилей в виде конфигурации	Базовая функция	+	+	+
Автоподключение к профилю при логине и запуску	Базовая функция	+	+	+
WireGuard	Подключение по протоколу WireGuard	+	+	+
TLS (443 порт)	Подключение по протоколу TLS	+	+	+
SSO профиль	Автосоздание профиля для SSO, если профилей нет	+	+	+
Device VPN	Подключение до входа пользователя в систему	+	+	+
Терминальный сервер	Поддержка работы терминальных серверов	+		
Балансировка Active-Active302 Редирект	Подключение к Ideco NGFW Novum по выданному балансировщиком адресу или другому серверу	+	+	+
Кастомная настройка	Кастомная настройка конфигурации Ideco Client: автосоздание профилей, запрет редактирования профилей и т.д.	+	+	+
Версия	Проверка актуальной версии Ideco Client	+	+	+
Ввод двухфакторной аутентификации	Показать окно ввода двухфакторной аутентификации при запросе от NGFW Novum и отправить введенный код на проверку	+	+	+

ZTNA. Данные ОС	Тип ОС	+	+	+
	Версия	+	+	+
	Домен	+	+	+
ZTNA. KB	Обновления Windows	+		
ZTNA. Registry	Данные реестра Windows	+		
ZTNA. Services	Проверка запущенных служб Windows	+		
ZTNA. Process	Проверка запущенных процессов	+	+	+
ZTNA. Межсетевой экран	Проверка Межсетевым экраном	+		
ZTNA. Антивирус	Проверка Антивирусами	+	+	

Работа в headless-системах

При необходимости Ideco Client можно запустить в консольном режиме с помощью команды `--console`. В этом случае GUI не отображается, а все команды передаются через командную строку.

На Linux консольный режим активируется автоматически при отсутствии графического интерфейса. На Windows и macOS только вручную.

Межсетевой экран

Windows

Вендор	Продукт
Microsoft	Windows Firewall

Антивирус

Windows

Вендор	Продукт
Microsoft	Windows Defender
Kaspersky Lab	• Kaspersky Free • Kaspersky Endpoint Security Все остальные продукты Kaspersky Lab по умолчанию определяются как Kaspersky Free.
Dr.Web	Dr.Web Security Space
Comodo	Comodo Internet Security

---

macOS

Вендор	Продукт
Kaspersky Lab	• Kaspersky Small Office Security • Kaspersky Endpoint Security • Kaspersky Internet Security
DrWeb	Dr.Web для macOS

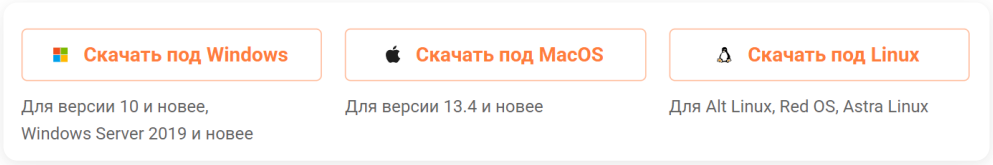
Установка и настройка Ideco Client на Windows

Классический контекст | Высокопроизводительный контекст

Скачивание

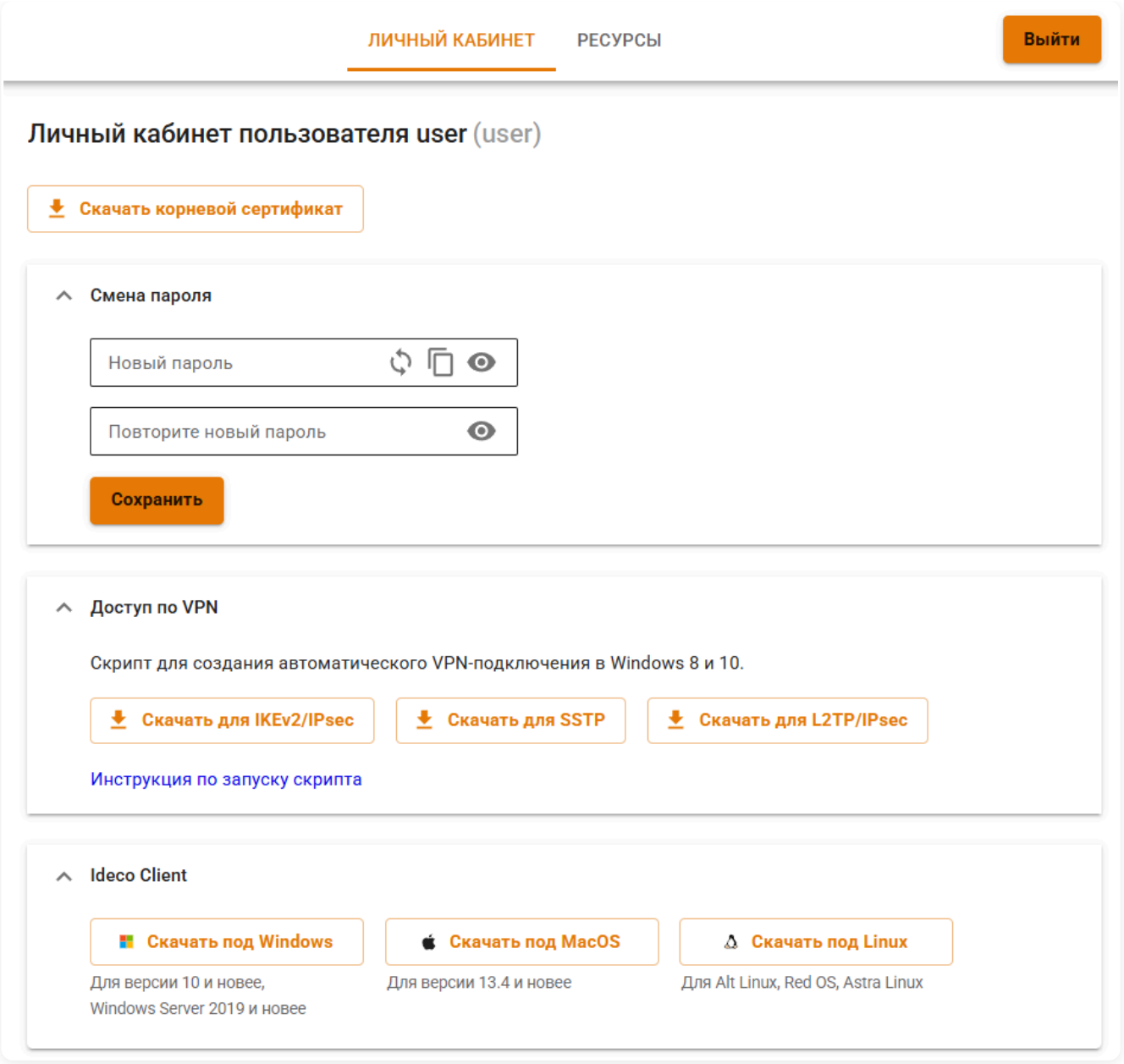
Для администратора

Перейдите в **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Windows** или скачайте по **ссылке**:



Для пользователя

Нажмите на кнопку **Скачать под Windows** в личном кабинете пользователя или скачайте по **ссылке**:



Установка

Сохраните и запустите файл установки `IdecoClient.msi`.

Чтобы заранее задать адрес подключения к Ideco NGFW Novum, запустите установщик с ключом `utm_address` из командной строки:

1. Перейдите в директорию с файлом `cd [путь до файла]`.

2. Откройте файл `IdecoClient.msi` с ключом `utm_address`.

3. Укажите адрес Ideco NGFW Novum (команда: `IdecoClient.msi utm_address=адрес_ngfw`).

Результат зависит от того, входит ли компьютер в домен:

- **Компьютер в домене** - после установки автоматически создается профиль с учетной записью пользователя, под которой выполнялась установка, и с адресом из ключа `utm_address`.
- **Компьютер не в домене** - при создании нового профиля поле с адресом будет автоматически заполнено значением из ключа `utm_address`.

Чтобы оптимизировать процесс установки Ideco Client с помощью GPO, создайте файл трансформации `.mst` с адресом Ideco NGFW Novum и примените его при установке. Для этого воспользуйтесь утилитой Orca.

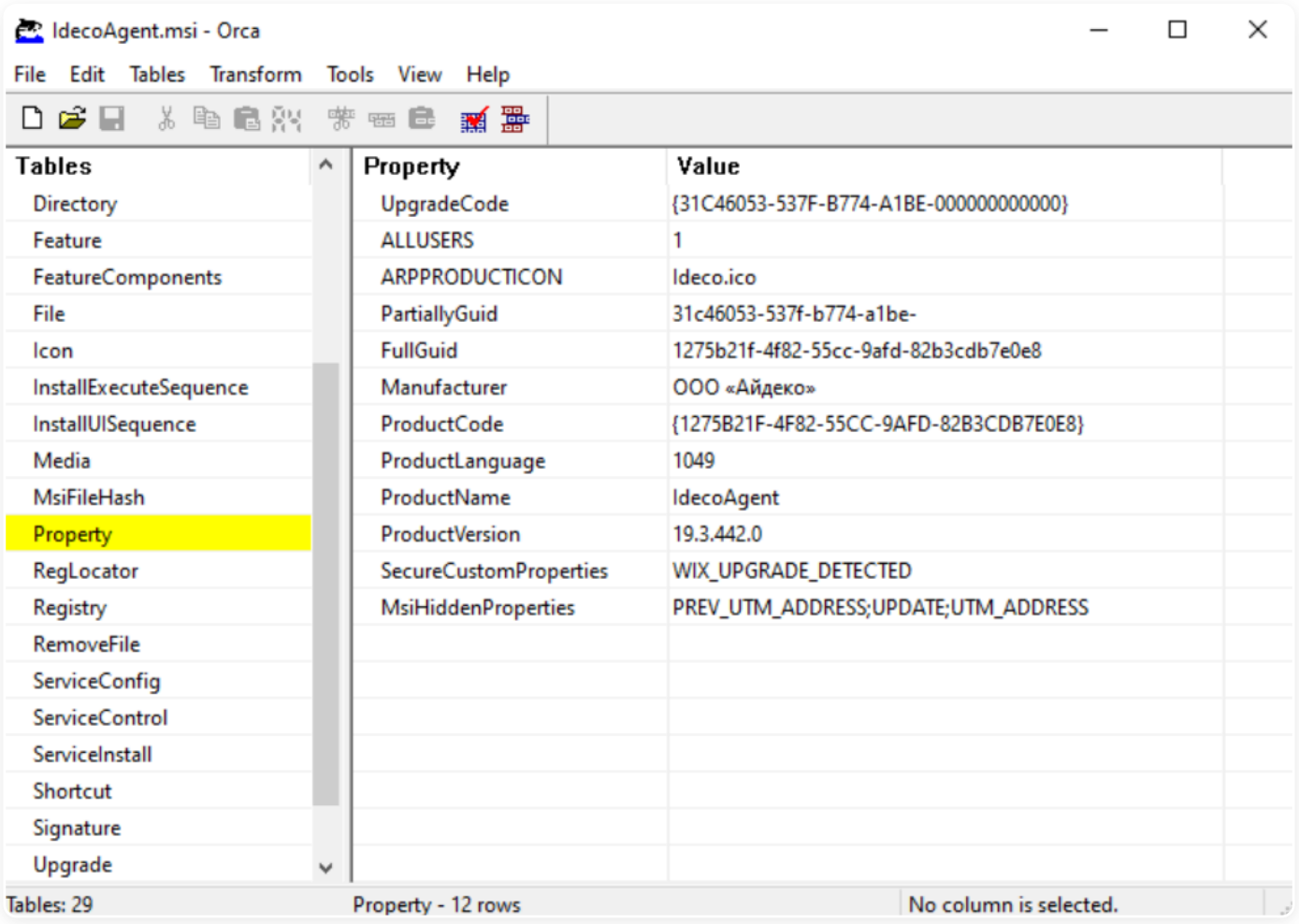
Как создать файл трансформации .mst в Orca

1. Запустите Orca.

2. Нажмите **File** → **Open** и откройте `IdecoClient.msi`.

3. Нажмите **Transform** → **New Transform** для создания файла трансформации. Все дальнейшие изменения будут сохранены в `.mst`-файл, а `IdecoClient.msi` останется неизменным.

4. В дереве таблиц найдите **Property**:



5. Нажмите **Tables** → **Add Row**, чтобы добавить новую запись.

6. В поле **Property** введите `UTM_ADDRESS`, а в поле **Value** - IP-адрес или FQDN Ideco NGFW Novum. Нажмите **Ок**.

7. Нажмите **Transform** → **Generate Transform** и сохраните файл, например `IdecoClient.mst`.

8. Закройте Orca.

При установке через GPO укажите созданный `.mst`-файл в качестве transform-файла для `IdecoClient.msi`. В этом случае Ideco Client будет установлен с уже заполненным полем **Хост**.

Если Kaspersky Plus блокирует установку и обновление

1. Откройте **Настройки** → **Настройки безопасности** → **Исключения и действия с найденными объектами** → **Указать доверенные приложения**:

2. Нажмите **Добавить**, выберите скачанный msi-файл Ideco Client и нажмите **Выбрать**:

3. Включите опции в **Исключения для приложения**:

4. Нажмите **ОК** и не закрывайте окно **Доверенные приложения**.

5. Установите Ideco Client.

6. Нажмите **Добавить** и добавьте файлы `idecoclient.exe` и `idecoservice.exe`. В **Исключения для приложения** укажите опции как в пункте 3:

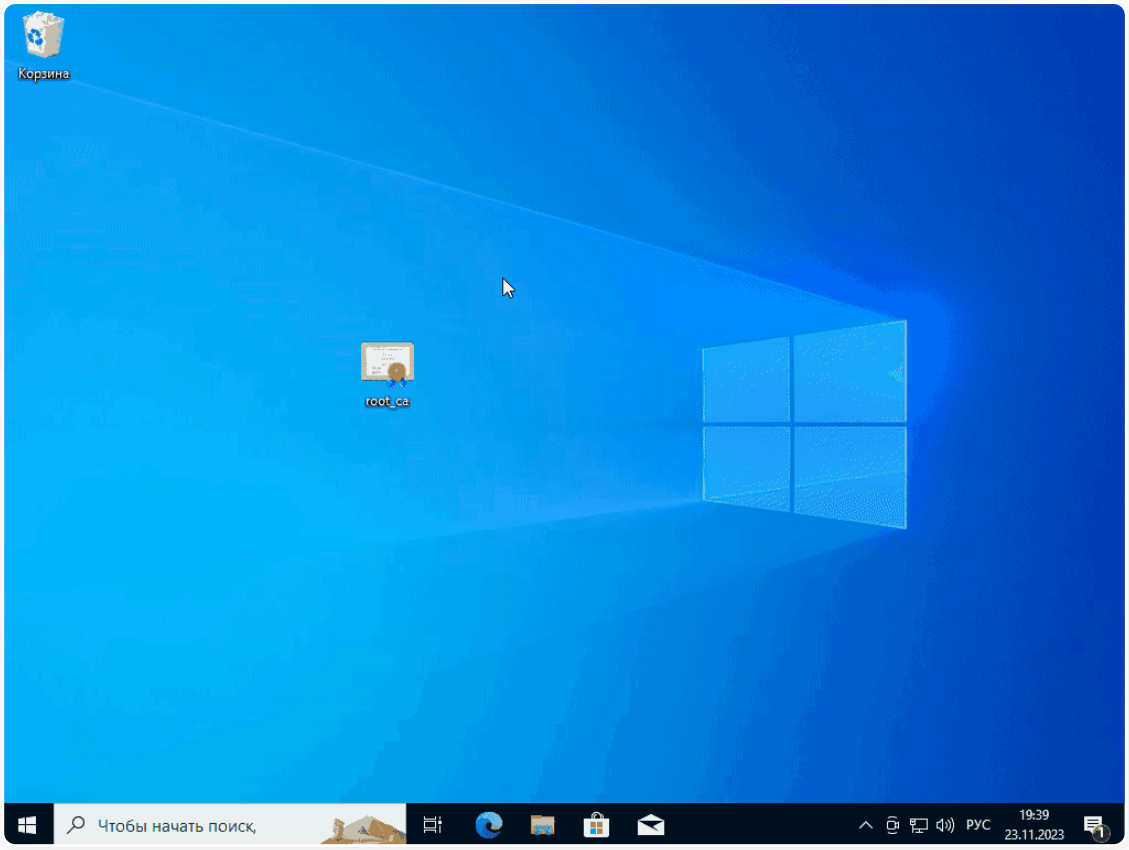
7. Откройте **Настройки** → **Настройки безопасности** → **Настройки сети** и настройте раздел:

8. Нажмите **Сохранить**.

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW Novum по внешнему IP-адресу или доменному имени без сертификата Let’s Encrypt, импортируйте корневой сертификат Ideco NGFW Novum на компьютер.

Для импорта сертификата на компьютер выполните действия:



1. Дважды кликните на скачанный файл сертификата.

2. В открывшемся окне выберите **Установить сертификат**.

3. Откроется **Мастер импорта сертификатов**. В качестве **Расположения хранилища** выберите **Локальный компьютер**.

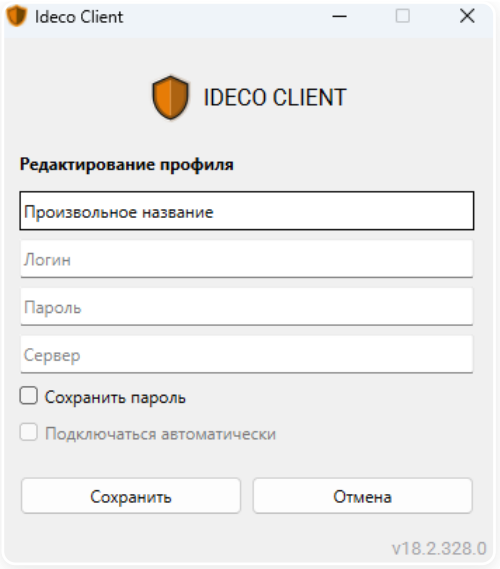
4. Выберите пункт **Поместить все сертификаты в следующее хранилище**, нажмите **Обзор** и выберите папку **Доверенные корневые центры сертификации**.

5. Нажмите **Ок** → **Далее** → **Готово**.

Первый запуск

1. Запустите Ideco Client.

2. Введите данные:



- **Название профиля** - введите произвольное название профиля, который будет доступен для выбора при подключении. Может не совпадать с логином.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Адрес сервера** - укажите логин и адрес сервера. Чтобы использовать резервный порт 14765, адрес необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`). Варианты в зависимости от конфигурации:

NGFW Novum введен в один домен

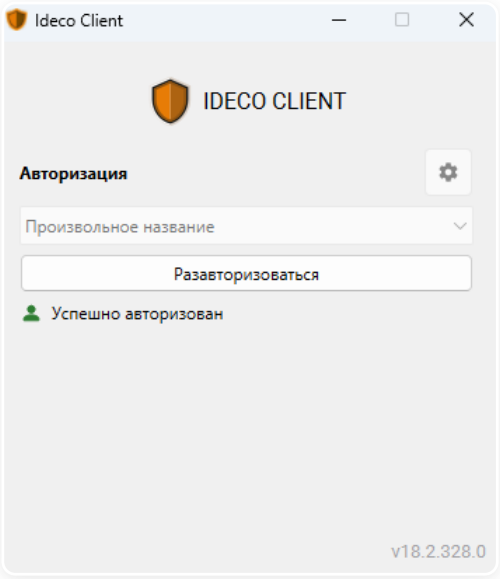
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:

NGFW Novum введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW Novum**:

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Редактирование профиля

1. Перейдите в раздел **Настройки**, нажав  .

2. Выберите профиль для редактирования, нажав  , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

Полезные ссылки

- **Кастомная настройка Ideco Client**
- **Как включить режим отладки для Ideco Client**

Установка и настройка Ideco Client на macOS

Классический контекст | Высокопроизводительный контекст

Особенности работы Ideco Client на macOS

- Ideco Client для macOS требует версии системы 13.4 и выше.
- HIP-профили на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

- ОС
- Процесс
- Антивирус (Kaspersky)

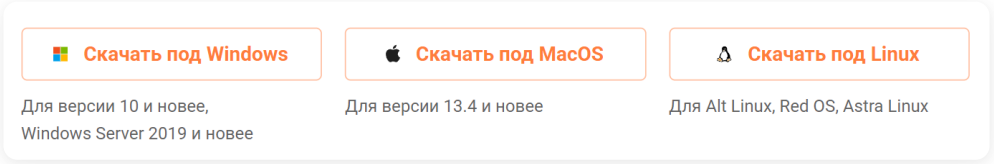
Недоступные HIP-профили

- Домен
- Межсетевой экран
- Реестр (всегда только Windows)
- Службы (всегда только Windows)
- Пакет обновлений Knowledge Base (всегда только Windows)

Скачивание

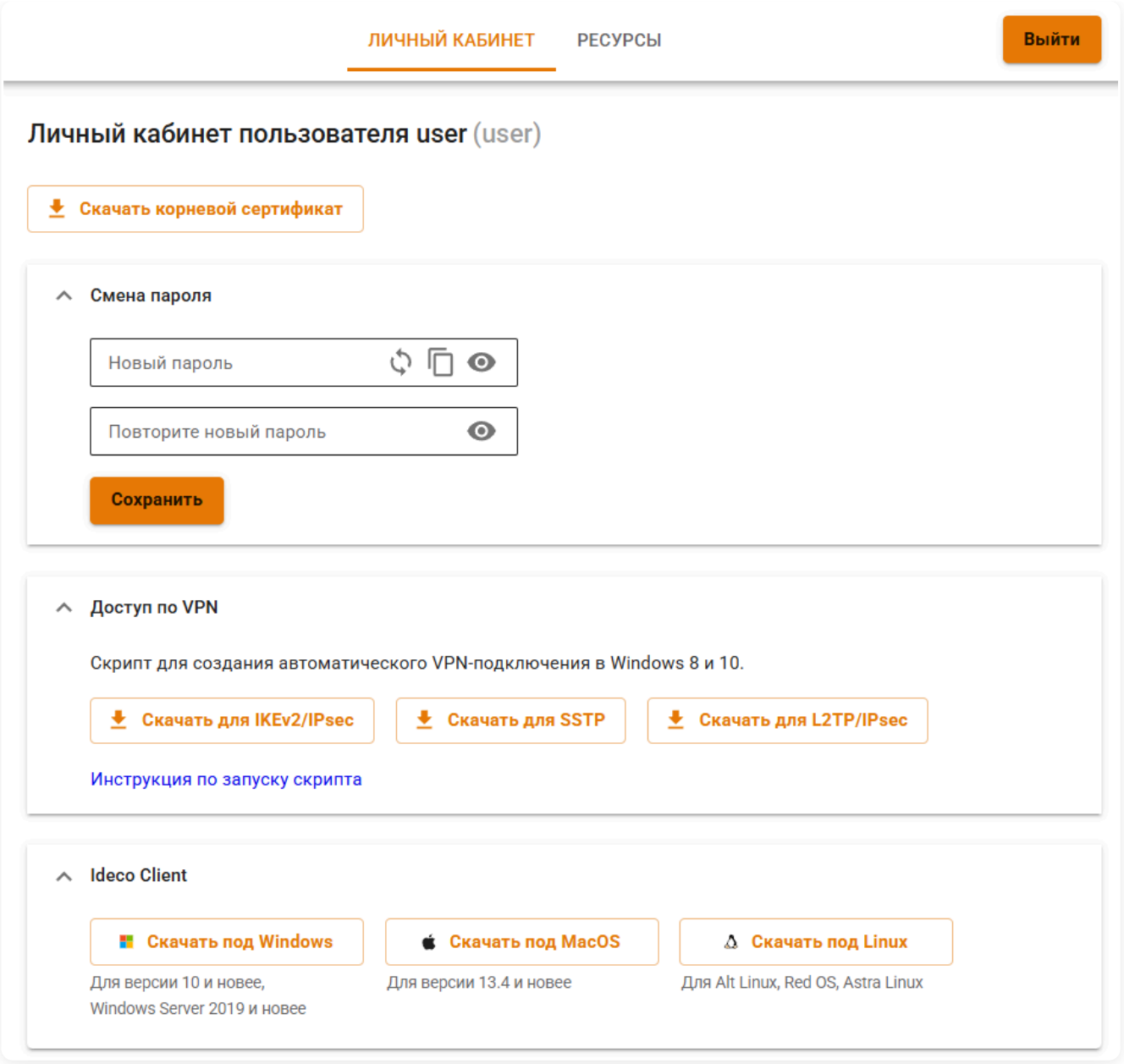
Для администратора

Перейдите в **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под macOS** или скачайте по **ссылке**:



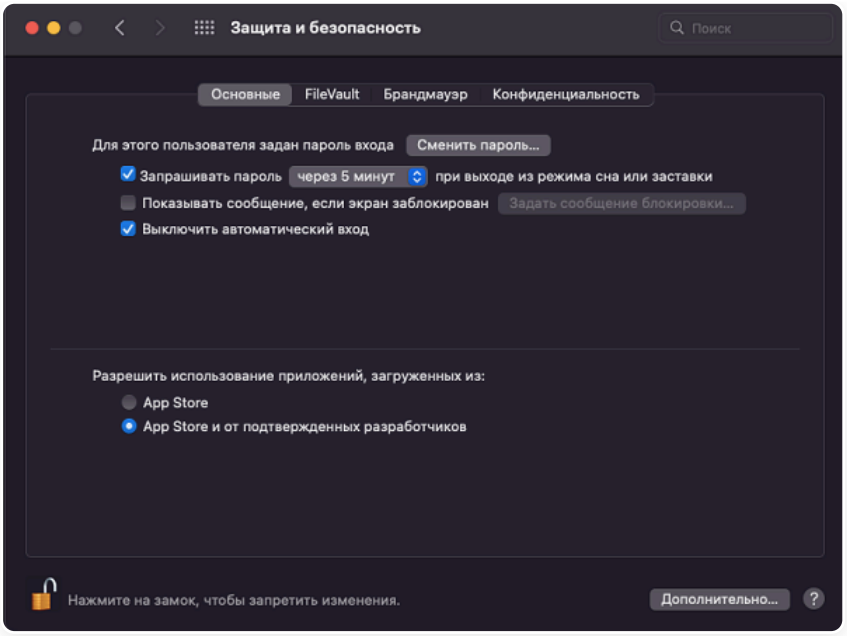
Для пользователя

Нажмите кнопку **Скачать под macOS** или скачайте по **ссылке**:



Установка

В некоторых версиях macOS необходимо явно разрешить установку приложения не из App Store. Для этого перейдите в **Защита и безопасность** → **Основные** и разрешите использование приложений, загруженных из **App Store и от подтвержденных разработчиков**:

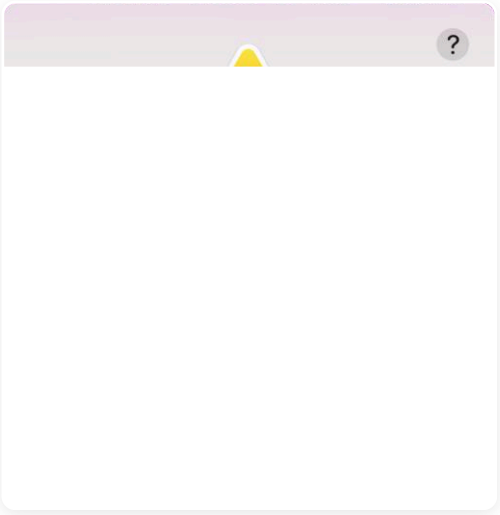


Чтобы установить **Ideco Client** на macOS, выполните действия:

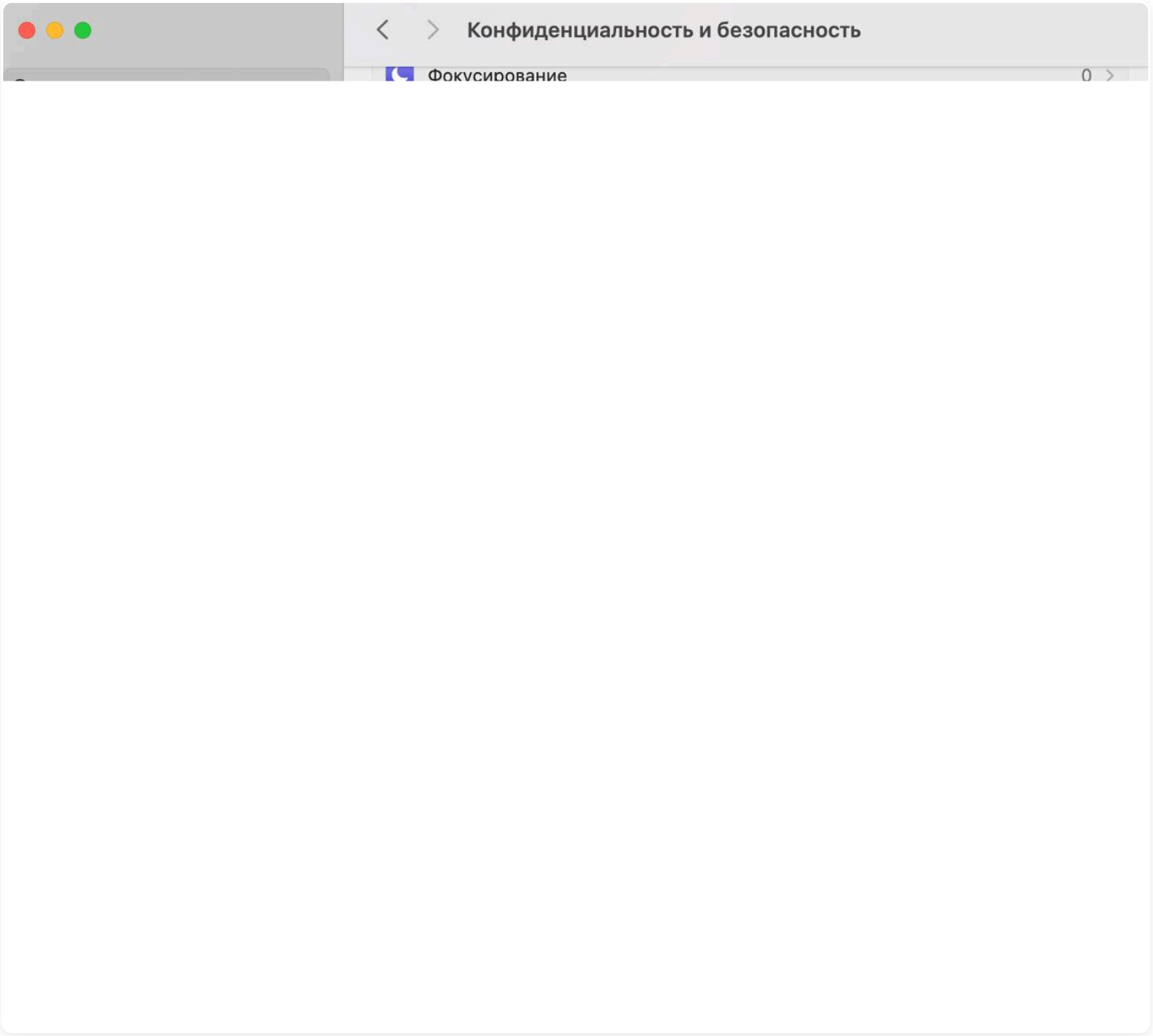
1. Нажмите по файлу **IdecoClient.pkg** правой кнопкой мыши и выберите **Открыть**.

macOS Sequoia

1. При открытии файла **IdecoClient.pkg** система сообщит о потенциальной опасности приложения. Нажмите **Готово**:



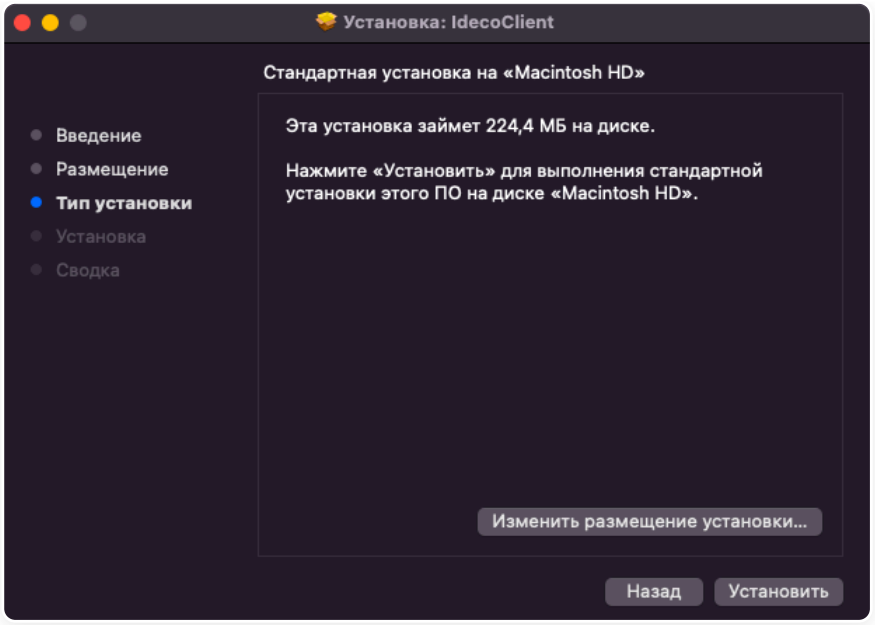
2. Перейдите в раздел **Конфиденциальность и безопасность** и нажмите **Все равно открыть** рядом с именем файла:



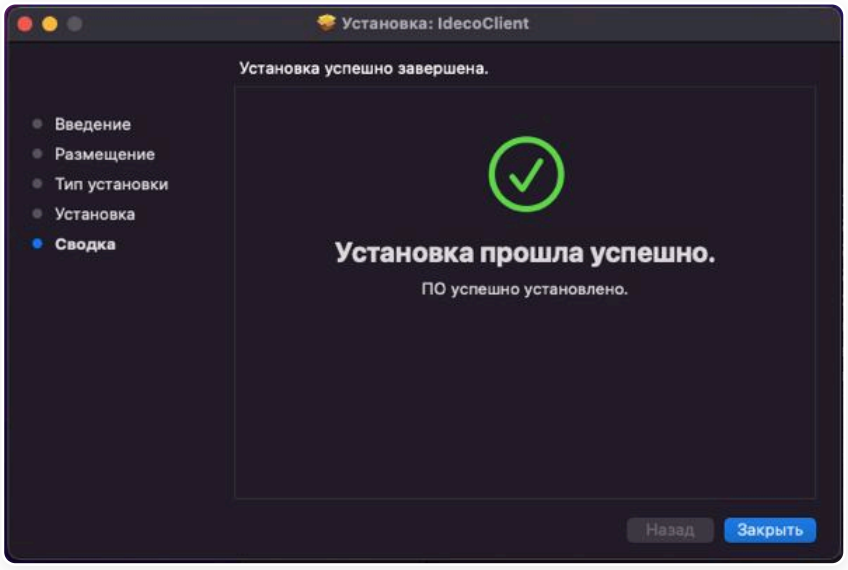
macOS Monterey и macOS Sonoma

При открытии файла **IdecoClient.pkg** система выдаст предупреждение. Подтвердите действие:

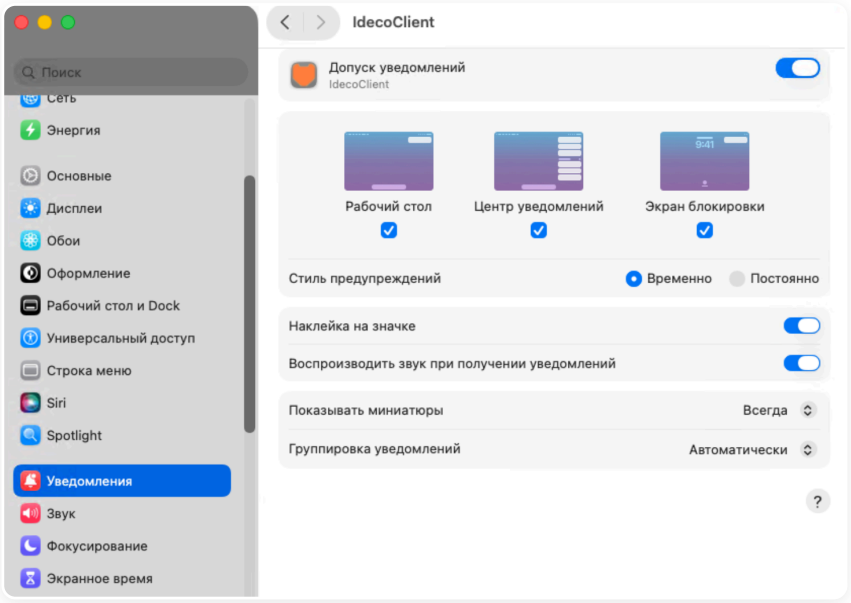
2. Нажмите **Продолжить**. В открывшемся окне нажмите **Установить**:



3. Если установка завершилась успешно, на экране появится соответствующее сообщение:



При первой установке Ideco Client система запросит разрешение на показ уведомлений. Если не дать согласие или проигнорировать запрос, уведомления будут отключены. Включить уведомления можно, установив необходимые разрешения в **Системные настройки** → **Уведомления** → **IdecoClient**:



Настройка профиля для первого запуска

Перед подключением к Ideco NGFW Novum по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt убедитесь, что срок действия оконечного сертификата на домен или IP-адрес составляет не более 825 дней. Если это так, то импортируйте **корневой** сертификат Ideco NGFW Novum на компьютер. Если срок действия оконечного сертификата на домен или IP-адрес превышает 825 дней, загрузите на NGFW Novum свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

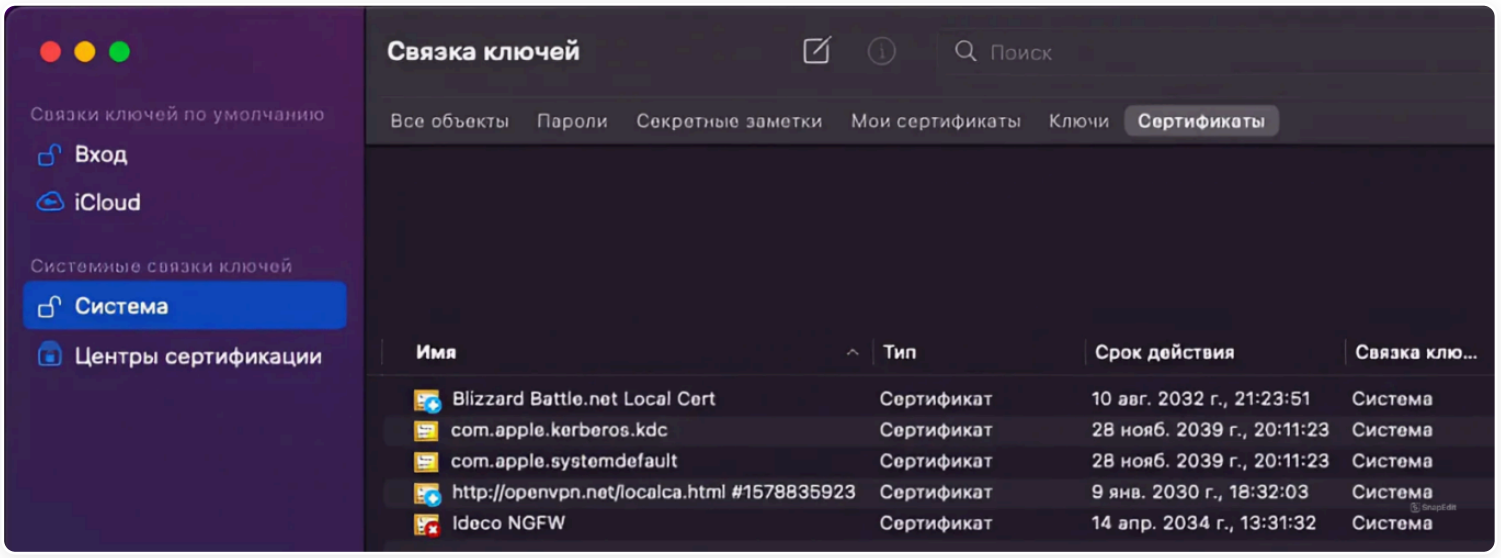
Установка корневого сертификата Ideco NGFW Novum на macOS

Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

> **Не храните** файл сертификата в директориях **Desktop**, **Documents** и **Downloads**: в этом случае Ideco Client не сможет прочитать и получить доступ к этим файлам. Рекомендуем сохранить файлы в другую директорию, например, в корневую директорию домашней папки пользователя.

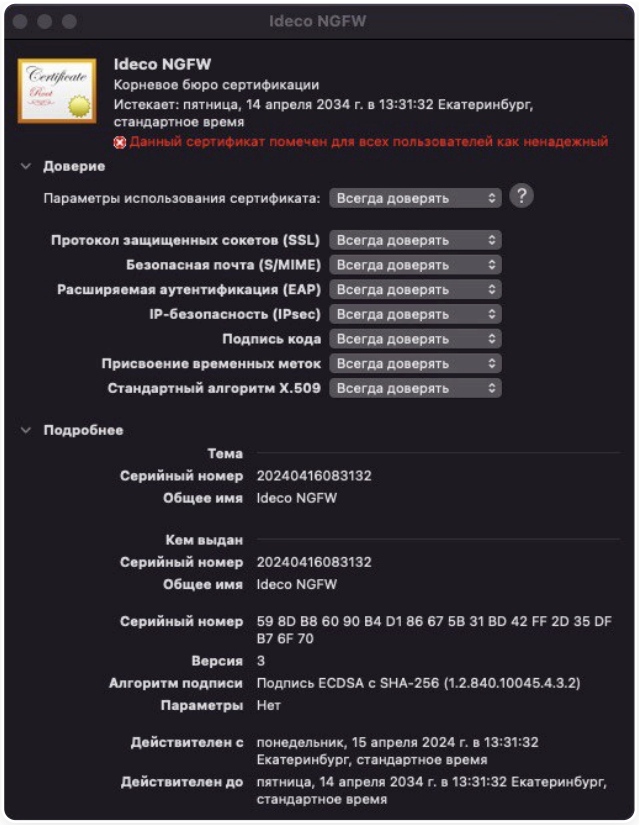
Установка через Связку ключей

1. Откройте скачанный файл **root_ca.crt** в приложении **Связка ключей**, сертификат Ideco NGFW Novum появится в папке **Система**:

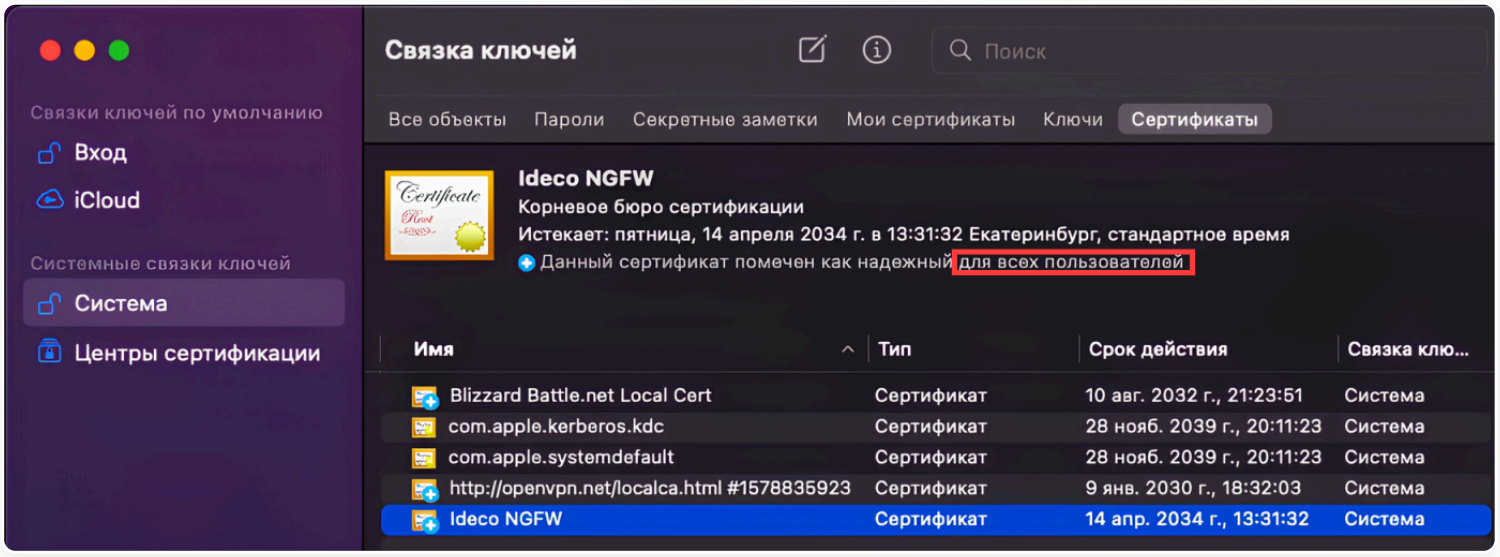


2. Нажмите по сертификату правой кнопкой мыши и выберите **Свойства**.

3. Установите в поле **Параметры использования сертификата** действие **Всегда доверять**:



4. Закройте окно свойств сертификата. Теперь сертификат помечен как надежный **для всех пользователей** устройства:



Сертификат должен быть установлен **для всех пользователей**.

Если сертификат установлен неправильно, то будет только для текущего пользователя. В этом случае проверьте корректность установки сертификата.

5. Перезагрузите компьютер.

Установка через терминал

1. Чтобы добавить корневые сертификаты в список доверенных, выполните в терминале команду:

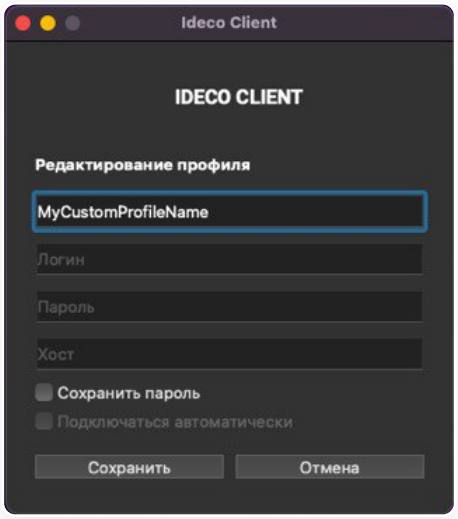
```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <путь к сертификату>/root_ca.crt
```

2. Перезагрузите компьютер.

Первый запуск

1. Запустите Ideco Client.

2. Введите данные:



- **Имя профиля** - может не совпадать с логином и будет использоваться при выборе профиля для авторизации.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Хост** - укажите логин и хост. Чтобы использовать резервный порт 14765, адрес сервера необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`). Варианты в зависимости от конфигурации:

NGFW Novum введен в один домен

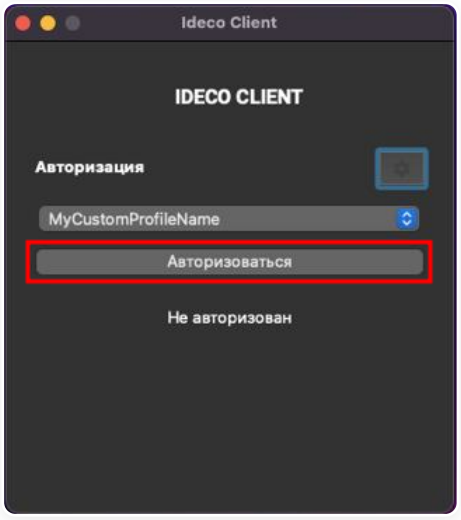
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:

NGFW Novum введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW Novum**:

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Редактирование профиля

1. Перейдите в раздел **Настройки**, нажав по  .

2. Выберите профиль для редактирования, нажав  , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

Установка и настройка Ideco Client на Linux

Классический контекст | Высокопроизводительный контекст

Особенности работы Ideco Client на Linux

- Ideco Client гарантированно работает на Alt Linux, РЕД ОС, Astra Linux, Fedora, Ubuntu. Для остальных дистрибутивов работа не гарантируется.
- HIP-профили на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

- ОС
- Процесс

Недоступные HIP-профили

- Антивирус
- Домен
- Межсетевой экран
- Реестр (всегда только Windows)
- Службы (всегда только Windows)
- Пакет обновлений Knowledge Base (всегда только Windows)

- Для проверки запуска процесса с заданным именем в системе (ZTNA) используется функция:

```
bool os_specific::isProcessExist(const std::string &processName)
```

Длина строки `processName` составляет не более 15 символов. Если название процесса длиннее, то название будет обрезано до максимально доступного числа символов. В этом случае проверка не будет выполнена корректно.

Скачивание

Для администратора

Перейдите в **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Linux** или скачайте по **ссылке**:

Для пользователя

Перейдите в личный кабинет пользователя и нажмите **Скачать под Linux** или скачайте по **ссылке**:

Установка

Для установки Ideco Client на Linux выполните действия:

1. Перейдите в папку со скачанным файлом установки Ideco Client:

```
cd "Путь до директории с установочным файлом"
```

2. Предоставьте файлу разрешение на исполнение, выполнив в терминале команду:

```
chmod +x IdecoClient.sh
```

3. Запустите файл установки Ideco Client:

```
./IdecoClient.sh
```

4. После установки проверьте статус службы IdecoService, выполнив команду:

```
systemctl status IdecoService.service
```

5. Убедитесь, что служба IdecoService запущена и работает:



Для добавления службы в автозагрузку выполните команду:

```
systemctl enable IdecoService.service
```

Для корректной работы Ideco Client:

Astra Linux

1. Проверьте, что установлен пакет `libnss-resolve`. Если нет, установите командой:

```
sudo apt-get install libnss-resolve
```

2. Для резолвинга имен используйте:

```
getent hosts доменное_имя
```

либо

```
resolvectl query доменное_имя
```

Alt Linux

Требуется пакет `systemd-networkd`. Установите командами:

```
sudo apt-get update
sudo apt-get install systemd-networkd
```

Fedora

При использовании SELinux в системе должны быть установлены и доступны в `PATH` утилиты:

- `getenforce`
- `semanage`
- `restorecon`

Команда для установки:

```
sudo dnf install libselinux-utils policycoreutils policycoreutils-python-utils
```

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW Novum по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt убедитесь, что срок действия сертификата на этот домен или IP-адрес составляет не более 825 дней. Если это так, то импортируйте **корневой** сертификат Ideco NGFW Novum на компьютер. Если срок действия сертификата на этот домен или IP-адрес превышает 825 дней, загрузите на NGFW Novum свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

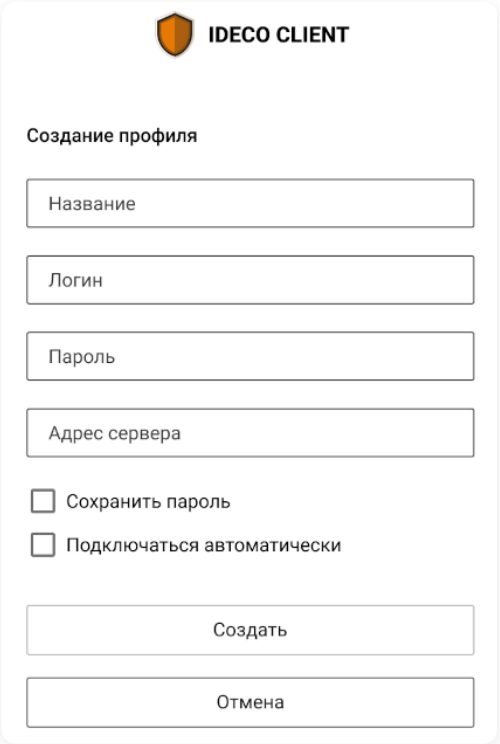
Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

Первый запуск

1. Запустите Ideco Client.

2. Введите данные:



- **Имя профиля** - может не совпадать с логином и будет использоваться при выборе профиля для авторизации.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Адрес сервера** - укажите логин и адрес сервера. Чтобы использовать резервный порт 14765, адрес необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`). Варианты в зависимости от конфигурации:

NGFW Novum введен в один домен

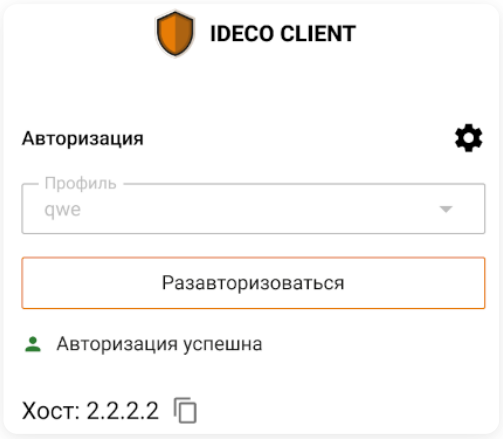
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес.

NGFW Novum введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW Novum**.

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Редактирование профиля

1. Перейдите в раздел **Настройки**, кликнув по .

2. Выберите профиль для редактирования, нажав , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

Удаление

1. Перейдите в каталог, в котором установлен Ideco Client:

```
cd /usr/local/Ideco/Agent/<версия Ideco NGFW Novum>
```

2. Запустите файл удаления Ideco Client:

```
./uninstall.sh
```

Кастомная настройка Ideco Client

Классический контекст | Высокопроизводительный контекст

Для авторизации пользователей Ideco Client использует профили, состоящие из логина и пароля. По умолчанию пользователь может создавать, удалять, редактировать профили и сохранять пароль для автоматической авторизации. Кастомная настройка позволит администратору создавать готовые конфигурации, а также ограничить права пользователей на управление профилями.

Возможности кастомной настройки

- [x] Запрет на создание новых профилей
- [x] Запрет на сохранение пароля
- [x] Запрет на редактирование профиля
- [x] Установка профиля по умолчанию
- [x] Автоматическое подключение выбранного профиля при запуске Ideco Client

Параметры файла конфигурации

Файл конфигурации создается администратором на пользовательской машине в формате .json, устанавливается через командную строку/терминал и поддерживает два типа профилей:

- Password - пользователь подключается по логину и паролю (только для Windows).
- SSO - пользователь для подключения использует данные системы.

Пример файла конфигурации, в котором заданы Password-профиль и SSO-профиль:

Пример файла конфигурации

```
{
    "profiles":
    [

        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90a0ac6",
            "source": "json",
            "name": "some string name 1",
            "data":
            {
                "login": "user1",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options":
            {
                "autoselect": true,
                "autoconnect": false,
                "read_only": false
            }
        },

        {
            "name": "some string name sso",
            "source": "json",
            "data":
            {
                "type": "sso",
                "server": "google.ru"
            },
            "profile_options":
```

```
            {
                "autoselect": false,
                "autoconnect": false,
                "read_only": false
            }
        }
    ],
    "gui_client_options":
    {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

Описание настроек конфигурационного файла

- `"profiles"` - обязательное поле, без него конфигурация не будет работать;
- `"id"` - необязательный идентификатор профиля, используемый для привязки пользовательских данных (например, логина) к конкретному конфигурационному профилю. При отсутствии `"id"` профиль генерируется автоматически. При указании вручную формат должен соответствовать UUID, иначе профиль может быть проигнорирован без отображения ошибки. Только для Password;
- `"source": "json"` - обязательное поле для всех типов профилей;
- `"name"` - уникальное название профиля;
- `"data"` - содержит данные для каждого типа профиля:
  - `"login"` - логин пользователя. Только для Password;
  - `"type"` - определяет тип профиля: Password или SSO;
  - `"server"` - адрес сервера. Для всех типов профилей. Если необходим резервный порт 14765, укажите адрес в формате `домен:14765` или `IP:14765` (например, `server.com:14765`).
- `"profile_options"` - настройки профиля:
  - `"autoselect"` - отвечает за установку профиля по умолчанию:
    - `true` - профиль будет выбран в качестве профиля по умолчанию при запуске Ideco Client;
    - `false` - профиль не выбран в качестве профиля по умолчанию.
  - `"autoconnect"` - отвечает за автоподключение профиля при запуске Ideco Client:
    - `true` - профиль будет автоматически подключаться при запуске Ideco Client;
    - `false` - профиль не будет автоматически подключаться при запуске Ideco Client.
  - `"read_only"` - отвечает за то, может ли пользователь редактировать или удалять профиль:
    - `true` - профиль нельзя редактировать или удалять;
    - `false` - профиль можно редактировать или удалять.
- `"gui_client_options"` - обязательное поле. Управляет поведением графического интерфейса:
  - `"deny_save_profile_password"` - разрешает или запрещает сохранение пароля:
    - `true` - пользователь не сможет сохранить пароль. Ideco Client будет запрашивать пароль при каждом подключении;
    - `false` - пользователь может сохранять пароль в Ideco Client.
  - `"deny_create_profiles"` - разрешает или запрещает создание новых профилей:
    - `true` - пользователь может создавать новые профили в Ideco Client;
    - `false` - пользователь не сможет создавать новые профили в Ideco Client.

Особенности работы профилей:

Password

- Если логин пользователя задан в файле конфигурации в поле `"login"`, то значение логина пользователя будет отображаться в поле **Логин** в Ideco Client.
- Если `"deny_save_profile_password": true`, то автоподключение должно быть запрещено `"autoconnect": false`, так как пароли не хранятся.
- Если `"deny_save_profile_password": true` и `"autoconnect": true`, то служба отклонит конфигурацию и запишет ошибку в логи.
- Если у нескольких профилей будет задан параметр автовыбора `"autoselect": true`, то выбран будет самый нижний профиль в файле конфигурации.
- Связывание пользовательских данных с файлом конфигурации осуществляется по `"id"` пользователя.

SSO

- Для SSO-профиля `"login"` отсутствует в файле конфигурации и поле Логин не отображается в интерфейсе Ideco Client, поскольку аутентификация выполняется автоматически с использованием учетной записи операционной системы.
- Параметры SSO-профиля задаются администратором и не могут быть изменены пользователем.
- Автоподключение возможно `"autoconnect": true`, так как аутентификация не требует ввода пароля.

- Если службе не удается выполнить аутентификацию, то в логи будет записана ошибка, а пользователю - выведено соответствующее уведомление.
- Связывание профиля с учетной записью пользователя выполняется на основе механизма SSO, без сохранения паролей.

Применение файла конфигурации

1. Создайте .json файл на машине пользователя.

2. Задайте необходимую конфигурацию.

3. Завершите все процессы Ideco Client. Это необходимо для корректного запуска с новыми настройками.

4. Установите конфигурацию.

> Путь к .json файлу конфигурации должен быть абсолютным. Например: C:\Program Files\Ideco\test.json

Windows

Откройте командную строку от имени администратора и выполните команду:

```
IdecoClient.exe --set-json-config="путь_до_файла_конфигурации"
```

Linux или macOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --set-json-config="путь_до_файла_конфигурации"
```

---

5. Ideco Client выполнит анализ файла:

- Если нет ошибок - сохранит в реестре данные файла конфигурации.
- Если есть ошибки - отправит в лог службы список ошибок.

Возможные причины ошибок

- Файл недоступен для чтения.
- Файл конфигурации пустой.
- Размер файла превышает 1 Мб.
- Файл содержит неопознанные параметры, например опечатки.
- В файле отсутствуют обязательные поля `"profiles"` и `"gui_client_options"`.
- Более одного профиля имеет опцию автовыбора `"autoselect": true`.
- Более одного профиля имеет опцию автоподключения `"autoconnect": true`.
- Если профиль имеет опцию автоподключения `"autoconnect": true`, но не имеет опции автовыбора `"autoselect": true`.
- В файле конфигурации в рамках Password-профиля указано `"deny_save_profile_password": true` и `"autoconnect": true`.
- Поля `"name"` или `"id"` не уникальны.
- Устройство пользователя не введено в домен, при этом в файле конфигурации прописан SSO-профиль.
- Заполнено поле `"id"` для SSO-профиля.

Работа с конфигурацией

Получить и вывести конфигурацию в консоль:

Windows

Откройте командную строку с правами администратора и выполните команду:

```
IdecoClient.exe --print-json-config True
```

Linux или macOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --print-json-config True
```

Удалить конфигурацию:

Windows

Откройте командную строку с правами администратора и выполните команду:

```
IdecoClient.exe --reset-json-config
```

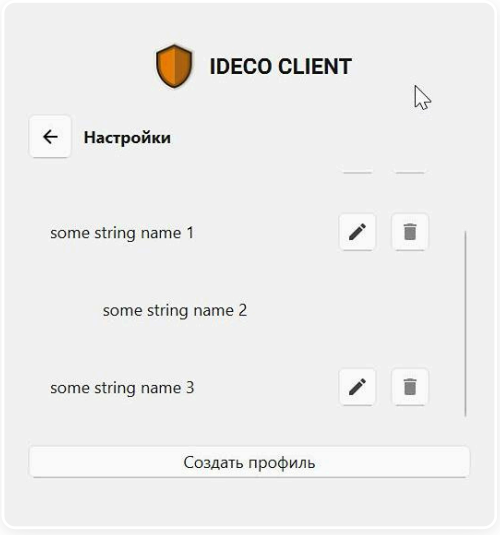
Linux или macOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --reset-json-config
```

Примеры настроек файла конфигурации

Запретить пользователю редактировать преднастроенный профиль



Профиль `some string name 2` создан в файле конфигурации и профиль запрещено редактировать или удалять, так как у него стоит настройка `"read_only": true`.

Профили `some string name 1` и `some string name 3` созданы пользователем самостоятельно, которые можно редактировать или удалять.

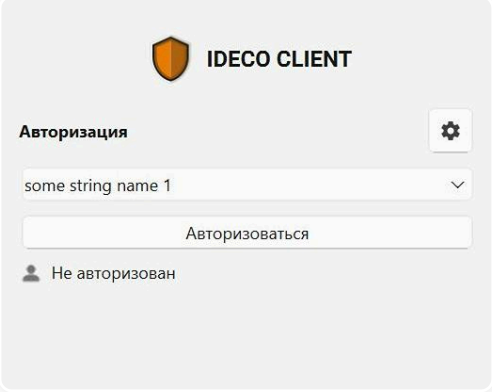
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
```

```
                "autoconnect": false,
                "read_only": true
            }
        }
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса:
  - `"deny_save_profile_password": false` - так как `false`, то пользователь может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": false` - так как `false`, то пользователь может вручную создавать новые профили в Ideco Client.

Задать профиль, который будет выбран по умолчанию при запуске Ideco Client

Файл конфигурации содержит два профиля `some string name 1` и `some string name 2`. Чтобы профилем по умолчанию был выбран `some string name 1`, в файле конфигурации у данного профиля, необходимо указать `"autoselect": true`.



Настройка файла конфигурации:

```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        },

        {
            "id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7",
```

```
            "source": "json",
            "name": "some string name 1",
            "data":
            {
                "login": "user1",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options":
            {
                "autoselect": true,
                "autoconnect": false,
                "read_only": true
            }
        }
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 1"` - название профиля `some string name 1`;
- `"data":` - содержит данные профиля:
  - `"login": "user1"` - логин пользователя `user1`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": true` - так как `true`, профиль будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса:
  - `"deny_save_profile_password": false` - так как `false`, то пользователь может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": false` - так как `false`, то пользователь может вручную создавать новые профили в Ideco Client.

Создать три профиля, которые нельзя изменить или удалить. Запретить создавать новые профили

Файл конфигурации содержит три профиля `some string name 1`, `some string name 2`, `some string name 3`. Чтобы их нельзя было отредактировать или удалить, всем профилям необходимо указать `"read_only": true`.
Чтобы запретить пользователю создавать новые профили необходимо указать: `"deny_create_profiles": true`.



Настройка файла конфигурации:

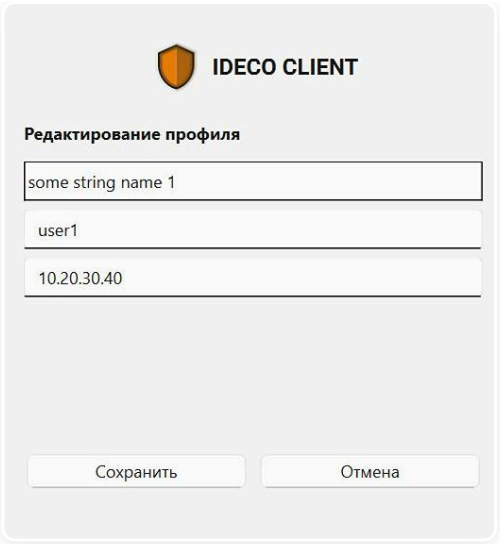
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        },

        {
            "id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7",
            "source": "json",
            "name": "some string name 1",
            "data":
            {
                "login": "user1",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options":
            {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        },

        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7asd4123",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        }
```

```
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": true
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7"` - уникальный идентификатор профиля;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 1"` - название профиля `some string name 1`;
- `"data":` - содержит данные профиля:
  - `"login": "user1"` - логин пользователя `user1`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7asd4123"` - уникальный идентификатор профиля;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 1"` - название профиля `some string name 1`;
- `"data":` - содержит данные профиля:
  - `"login": "user1"` - логин пользователя `user1`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса:
  - `"deny_save_profile_password": false` - так как `false`, то пользователь может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": true` - так как `true`, то пользователь не сможет создавать новые профили в Ideco Client.

Запретить сохранять пароль. Ideco Client будет запрашивать пароль при каждом подключении

Чтобы запретить пользователю сохранять пароль в Ideco Client, необходимо в файле конфигурации указать `"deny_save_profile_password": true`.



Настройка файла конфигурации:

```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": false
            }
        }
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": false` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса;
  - `"deny_save_profile_password": true` - так как `true`, то пользователь не может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": false` - так как `false`, то пользователь может вручную создавать новые профили в Ideco Client.

Управление Ideco Client через CLI

Классический контекст | Высокопроизводительный контекст

С помощью CLI (Command Line Interface) можно настраивать логирование, Device VPN и кастомную конфигурацию, собирать диагностику и управлять запуском без использования графического интерфейса.

Консольный режим без графического окружения (`--console`) поддерживается начиная с Ideco Client версии 22. В более ранних версиях для запуска Ideco Client требуется графическое окружение. Так как мажорная версия Ideco Client соответствует мажорной версии NGFW Novum, для работы в консольном режиме NGFW Novum должен быть версии 22 или выше.

Как вводить команды

Windows

Откройте командную строку (cmd) или PowerShell от имени администратора и введите команду в формате:

```
"C:\Program Files\Ideco\<версия Ideco Client>\IdecoClient.exe" <команда>
```

Linux

Откройте терминал и введите команду в формате:

```
sudo /usr/local/Ideco/Agent/<версия Ideco Client>/IdecoClient.sh <команда>
```

macOS

Откройте терминал и введите команду в формате:

```
sudo /Applications/IdecoClient.app/Contents/MacOS/IdecoClient <команда>
```

Просмотр доступных команд

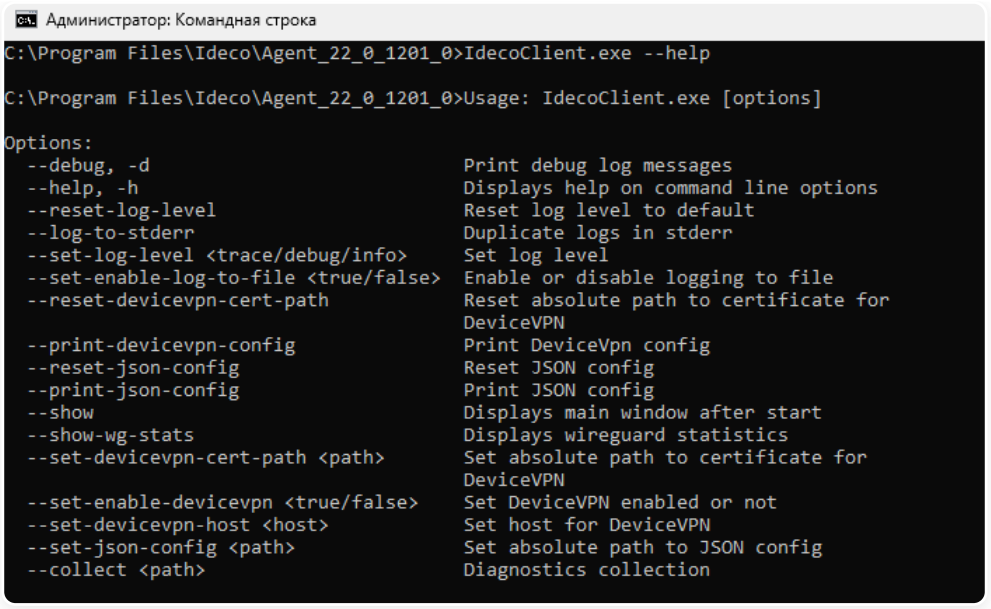
Чтобы вывести список всех доступных команд и их описание, выполните:

Windows

```
IdecoClient.exe --help
```

Или сокращенная форма:

```
IdecoClient.exe -h
```



Linux

```
sudo /usr/local/Ideco/Agent/<версия Ideco Client>/IdecoClient.sh --help
```

Или сокращенная форма:

```
sudo /usr/local/Ideco/Agent/<версия Ideco Client>/IdecoClient.sh -h
```

macOS

```
sudo /Applications/IdecoClient.app/Contents/MacOS/IdecoClient --help
```

Или сокращенная форма:

```
sudo /Applications/IdecoClient.app/Contents/MacOS/IdecoClient -h
```

Справочник команд CLI

Команда	Описание
`--help` или `-h`	Отобразить список доступных команд и их описание
`--debug` или `-d`	Включить вывод отладочных сообщений
`--show`	Отобразить главное окно после запуска
`--show-wg-stats`	Отобразить статистику WireGuard
`--console`	Запустить Ideco Client в консольном режиме без GUI
`--reset-to-auto-mode`	Переключиться на использование автоматически сгенерированных сертификатов
Логирование	
`--set-log-level <trace/debug/info>`	Установить уровень логирования. Доступные значения: • `info` - стандартный • `debug` - расширенный • `trace` - максимальный
`--reset-log-level`	Сбросить уровень логирования до значения `info`
`--set-enable-log-to-file <true/false>`	Включить (`true`) или отключить (`false`) запись логов в файл

`--log-to-stderr`	Дублировать вывод логов в stderr
Device VPN	
`--set-enable-devicevpn <true/false>`	Включить (`true`) или отключить (`false`) Device VPN
`--set-devicevpn-host <адрес NGFW Novum>`	Указать адрес сервера Ideco NGFW Novum для подключения Device VPN. Чтобы использовать резервный порт 14765, адрес необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`)
`--set-devicevpn-cert-path <абсолютный путь до файла сертификата>`	Указать абсолютный путь до PEM-файла сертификата устройства для Device VPN
`--reset-devicevpn-cert-path`	Сбросить путь до сертификата Device VPN
`--print-devicevpn-config`	Вывести в консоль текущую конфигурацию Device VPN
`--set-dn <string>`	Указать DN (Distinguished Name) для нового сертификата
`--get-csr <абсолютный путь к директории или ->`	Создать новый ключ и сформировать запрос на подпись сертификата (CSR). Укажите путь для сохранения CSR в файл или `-` для вывода CSR в терминал без сохранения на диск
`--set-cert <абсолютный путь к файлу>`	Указать путь до подписанного сертификата
`--set-key <абсолютный путь к файлу>`	Указать путь до приватного ключа
Кастомная конфигурация	
`--set-json-config <абсолютный путь к файлу>`	Применить кастомную конфигурацию из JSON-файла по указанному абсолютному пути
`--print-json-config`	Вывести в консоль текущую кастомную конфигурацию
`--reset-json-config`	Удалить текущую кастомную конфигурацию
Диагностика	
`--collect <абсолютный путь к директории>`	Собрать диагностический ZIP-архив и сохранить его по указанному абсолютному пути

Работа в headless-системах

При необходимости Ideco Client можно запустить в консольном режиме с помощью команды `--console`. В этом случае GUI не отображается, а все команды передаются через командную строку.

На Linux консольный режим активируется автоматически при отсутствии графического интерфейса. На Windows и macOS только вручную.

Полезные ссылки

- **Настройка Device VPN**
- **Кастомная настройка Ideco Client**
- **Настройка логирования**
- **Диагностика Ideco Client**

Настройка Device VPN

Классический контекст | Высокопроизводительный контекст

Device VPN - режим работы Ideco Client, в котором клиентское устройство авторизуется на Ideco NGFW Novum без входа пользователя в систему. Такое соединение позволяет:

- ☑ Устанавливать на устройства программы и обновления
- ☑ Получать доступ к внутренней инфраструктуре
- ☑ Применять групповые политики
- ☑ Блокировать/разблокировать устройства и пользователей
- ☑ Отслеживать активность устройств и управлять устройствами за пределами внутренних сетей

Device VPN позволяет получить доступ к устройству даже когда пользователь не использует Ideco Client, и устройство имеет доступ в интернет или до Ideco NGFW Novum. Это позволяет осуществлять удаленное администрирование, обновление ПО и антивирусов, мониторинг.

ⓘ При обновлении Ideco NGFW с версии 21 на версию 22 настройки Device VPN мигрируют автоматически. Результат миграции зависит от исходных параметров: типа подключения из локальной сети, списка разрешенных объектов, состояния опции **Принимать подключения в режиме Device VPN** и наличия доверенного сертификата. Возможные комбинации параметров и результаты их миграции представлены в статье.

Для авторизации через Device VPN используется корневой сертификат с приватным ключом. На основе этого ключа администратор создает пользовательские сертификаты для конечных устройств.

В качестве **Сертификата устройства** Device VPN можно использовать:

- Самоподписанные сертификаты.
- Сертификаты, выданные Центрами сертификации (Certificate Authority, CA).

Чтобы подключить устройство к Ideco NGFW Novum в режиме Device VPN, выполните действия:

1. Перейдите в раздел **Пользователи → Ideco Client**.

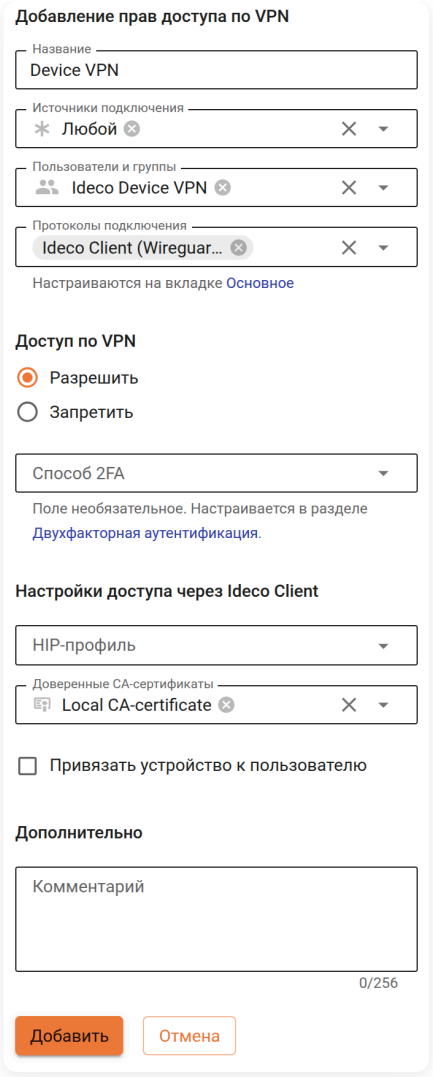
2. Введите домен или IP-адрес Ideco NGFW Novum. Если устройства пользователей находятся в локальной сети, включите одну из опций в блоке **Подключение из локальной сети**:

- **С установлением туннеля** - для авторизации пользователей по VPN.
- **Без туннеля** - для авторизации пользователей в локальной сети без туннеля.

3. Если выбрана опция **Без туннеля**, заполните поля в блоке **Разрешенные пользователи Device VPN для авторизации**:

- **Пользователи и группы Device VPN** - выберите учетные записи Device VPN (или группу **Ideco Device VPN**), которым разрешена авторизация.
- **Доверенные CA-сертификаты** - выберите один или несколько сертификатов удостоверяющих центров, которым должно доверять устройство пользователя. Управлять сертификатами можно в **Сервисы → Сертификаты → Ideco Client**.

4. Если выбрана опция **С установлением туннеля**, блок **Разрешенные пользователи Device VPN для авторизации** не используется - доступ настраивается через правила в **Пользователи → VPN-подключения → Доступ по VPN**. Создайте правило, разрешающее учетным записям или группе Ideco Device VPN подключение по протоколу Wireguard или TLS:



5. Установите Ideco Client на устройство пользователя, затем закройте Ideco Client для дальнейшей конфигурации.

Device VPN не может самостоятельно запустить автоматический выпуск сертификата. Однако, если пользователь ранее авторизовался на Ideco NGFW Novum через Ideco Client и получил сертификат в режиме AUTO, этот же сертификат используется для Device VPN без дополнительных действий - шаги 6 и 7 выполнять не нужно, достаточно задать адрес NGFW Novum и включить Device VPN командами `--set-devicevpn-host` и `--set-enable-devicevpn`.

6. Сгенерируйте на устройстве пользователя приватный ключ и сертификат в формате PEM, подписанный доверенным сертификатом. Процесс создания сертификата описан в статье Создание сертификатов для Device VPN.

Ручная установка сертификата переводит Ideco Client в режим EXTERNAL и удаляет установленные ранее ключ и сертификат, в том числе выпущенные в режиме AUTO. О правилах переключения режимов смотрите в статье Аутентификация по сертификату.

Чтобы уменьшить риск компрометации приватного ключа **Сертификата устройства** рекомендуем хранить его в директории, к которой есть доступ только у администратора. Например:

- Для Linux (Ubuntu) - каталог `/etc/ssl/private`.
- Для Windows - каталог `C:/Users/Пользователь/AppData/Roaming/Microsoft/System/Certificates`, где **Пользователь** - имя вашей учётной записи.

7. Сконфигурируйте установленный Ideco Client с сертификатом для использования Device VPN:

Перед началом ввода команд проверьте, что Ideco Client закрыт.

Чтобы использовать резервный порт 14765, параметр `<адрес NGFW Novum>` необходимо задать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`).

Для Windows

Откройте командную строку от имени администратора и введите:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --set-cert <абсолютный путь до файла сертификата> --set-devicevpn-host <адре
```

Команда `--set-cert` принимает либо файл сертификата, либо объединенный файл с сертификатом и закрытым ключом. Если закрытый ключ хранится в отдельном файле, дополнительно укажите его командой `--set-key <абсолютный путь до файла закрытого ключа>`.

Для вывода заданных параметров в командную строку воспользуйтесь командой:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --print-devicevpn-config
```

Для Linux

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient.sh --set-cert <абсолютный путь до файла сертификата> --set-devicevpn-host <
```

Команда `--set-cert` принимает либо файл сертификата, либо объединенный файл с сертификатом и закрытым ключом. Если закрытый ключ хранится в отдельном файле, дополнительно укажите его командой `--set-key <абсолютный путь до файла закрытого ключа>`.

Для вывода заданных параметров в консоль воспользуйтесь командой:

```
sudo <абсолютный путь до IdecoClient>/ld.so --argv0 IdecoClient --library-path <абсолютный путь до IdecoClient>/lib <абсолютн
```

Для macOS

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient --set-cert <абсолютный путь до файла сертификата> --set-devicevpn-host <адр
```

Команда `--set-cert` принимает либо файл сертификата, либо объединенный файл с сертификатом и закрытым ключом. Если закрытый ключ хранится в отдельном файле, дополнительно укажите его командой `--set-key <абсолютный путь до файла закрытого ключа>`.

Для вывода заданных параметров в консоль воспользуйтесь командой:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient --print-devicevpn-config
```

Если необходимо создать пользователя Device VPN заранее, выполните действия указанные в статье Управление учетными записями и группами. Для создания пользователя Device VPN используется **Сертификат устройства** без приватного ключа, который не хранится на Ideco NGFW Novum в дальнейшем. Ideco NGFW Novum извлекает имя пользователя из поля **Common Name** сертификата.

При неудачной конфигурации Device VPN служба Ideco Client будет постоянно пытаться подключиться к Ideco NGFW Novum. Перезапуск службы не поможет в решении проблемы.

Для решения проблемы необходимо:

- Выключить Device VPN: выполнить команду по настройке Device VPN с единственным параметром `--set-enable-devicevpn false`.
- Исправить конфигурацию подключения (загрузить правильный сертификат, определить корректность пути до него).
- Настроить и активировать Device VPN: выполнить команду по настройке Device VPN с параметром `--set-enable-devicevpn true`.
- В интерфейсе Ideco NGFW Novum убедиться, что подключение Device VPN выполнено.

Если при подключении устройства Device VPN к Ideco NGFW Novum соединение тут же разрывается, то проверьте доступ этого устройства в зависимости от подключения:

- **С установлением туннеля** - перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и проверьте правило, разрешающее учетным записям или группе Ideco Device VPN подключение.
- **Без туннеля** - в поле **Пользователи и группы Device VPN** проверьте учетные записи или группу Ideco Device VPN, которым разрешена авторизация.

Для Device VPN автоматический выпуск сертификата устройства не выполняется. Если сертификат на устройстве отсутствует, подключение будет отклонено. Убедитесь, что сертификат устройства установлен до подключения. Процесс его создания описан в статье Создание сертификатов для Device VPN.

Миграция настроек Device VPN

Классический контекст | Высокопроизводительный контекст

В таблице представлены результаты автоматической миграции настроек Device VPN с версии 21 на версию 22 NGFW Novum в зависимости от исходной конфигурации:

Версия 21				**Версия 22**
Подключение из локальной сети	**Разрешенные объекты**	**Принимать подключения в режиме Device VPN**	**Доверенный сертификат**	**Результат миграции**
Без туннеля	Любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - Любой • **Доверенные CA-сертификаты** - загруженный сертификат • **Пользователи и группы Device VPN** - группа Ideco Device VPN Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
Без туннеля	Не любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN • **Пользователи и группы Device VPN** - объекты, входящие в группу Device VPN • **Доверенные CA-сертификаты** - загруженный сертификат Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN

С установлением туннеля	Любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - Любой • **Доверенные CA-сертификаты** - загруженный сертификат • **Пользователи и группы Device VPN** - группа Ideco Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается разрешающее правило с группой **Ideco Device VPN** и указанным сертификатом Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
С установлением туннеля	Не любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN • **Пользователи и группы Device VPN** - объекты, входящие в группу Device VPN • **Доверенные CA-сертификаты** - загруженный сертификат В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается разрешающее правило с группой **Ideco Device VPN** и указанным сертификатом Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN

С установлением туннеля	Любой	Выключена	Загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы → Сертификаты → Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
Без туннеля	Любой	Выключена	Загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы → Сертификаты → Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
С установлением туннеля	Любой	Выключена	Не загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**
Без туннеля	Любой	Выключена	Не загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**

С установлением туннеля	Не любой	Выключена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
Без туннеля	Не любой	Выключена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
С установлением туннеля	Не любой	Выключена	Не загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**

Без туннеля	Не любой	Выключена	Не загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**

Создание сертификатов для Device VPN

Классический контекст | Высокопроизводительный контекст

> В статье описан процесс создания сертификатов с использованием OpenSSL для подключения по Device VPN между Ideco NGFW Novum и Ideco Client.

Процесс включает два этапа:

1. Создание корневого сертификата с защищенным приватным ключом.

2. Создание сертификатов для пользовательских устройств на основе этого корневого сертификата.

Создание корневого сертификата

1. Сгенерируйте приватный ключ корневого сертификата, защищенный **passphrase**:

> Не рекомендуем копировать приватный ключ корневого сертификата с машины, на который он был создан, во избежание компрометации ключа.
>
> Рекомендуем создавать пользовательские сертификаты сразу на терминальном сервере, чтобы не переносить приватный ключ с машины на машину. Это понизит риск компрометации приватного ключа пользовательского сертификата.

```
openssl genrsa -aes256 -out ideco-dvpn_root-ca.key 4096
```

- `-aes256` - приватный ключ зашифрован алгоритмом AES-256 (более надежен, чем устаревший Triple DES (3DES));
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ.

2. Сгенерируйте корневой сертификат, используя приватный ключ корневого сертификата:

```
openssl req -x509 -new -sha256 -days 1825 -key ideco-dvpn_root-ca.key -out ideco-dvpn_root-ca.pem
```

- `-sha256` - использовать алгоритм SHA256 при создании сертификата;
- `-days 1825` - срок действия сертификата в днях;
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ корневого сертификата;
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат.

3. Заполните параметры сертификата:

```
Country Name (2 letter code) [AU]:Ru
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Test
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:MyName
Email Address []:test@ideco.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

> **Common Name (eg, your name or your server's hostname)** - обязательная строка для заполнения:
>
> - **Common Name** может быть любым, если создается корневой сертификат, который подписывает другие сертификаты.
> - **Common Name** должен быть равен имени пользователя Device VPN на Ideco NGFW Novum, если выпускается клиентский сертификат.
> - **Common Name** должен быть равен домену, на который подключаются клиенты, если выпускается серверный сертификат.

Расшифровка строк

- **Country Name (2 letter code) [XX]** - код страны в формате ISO 3166-1 alpha-2 (например, RU).
- **State or Province Name (full name) [Some-State]** - название региона или области (например, Moscow).
- **Locality Name (eg, city) [Default City]** - название города (например, Saint Petersburg).
- **Organization Name (eg, company) [Internet Widgits Pty Ltd]** - название организации.
- **Organizational Unit Name (eg, section) []** - название подразделения организации.
- **Common Name (e.g. server FQDN or YOUR name) []** - наименование сертификата.
- **Email Address []** - контактный email.

Дополнительные атрибуты:

- **A challenge password []** - пароль для дополнительной аутентификации. Рекомендуем оставить поле пустым.
- **An optional company name []:** - полное юридическое название организации.

4. Проверьте, что сертификат был успешно создан командой:

```
openssl x509 -text -noout -in ideco-dvpn_root-ca.pem
```

- Корневой сертификат должен иметь атрибут `CA:TRUE`.
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат, без приватного ключа.

5. Перейдите в **Сервисы** → **Сертификаты** → **Ideco Client** → **Реестр** и загрузите созданный сертификат `ideco-dvpn_root-ca.pem` без приватного ключа, нажав **Загрузить сертификат**. После загрузки сертификат станет доступен для выбора в поле **Доверенные CA-сертификаты** в **Пользователи** → **Ideco Client** → **Основное** и в правилах **Пользователи** → **VPN-подключения** → **Доступ по VPN**.

Создание пользовательского сертификата для конечного устройства

1. Сгенерируйте приватный ключ без применения шифрования в пользовательском пространстве администратора, куда у пользователей не будет доступа:

```
openssl genrsa -out client1-dvpn.key 4096
```

- `client1-dvpn.key` - файл, содержащий приватный ключ.

2. Сгенерируйте запрос на выпуск пользовательского сертификата с использованием приватного ключа:

```
openssl req -new -key client1-dvpn.key -out client1-dvpn.csr
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.csr` - файл, содержащий зашифрованный запрос на выпуск сертификата.

3. Заполните параметры сертификата:

```
Country Name (2 letter code) [AU]:Ru
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Test
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:MyName
Email Address []:test@ideco.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Common Name (eg, your name or your server's hostname) - обязательная строка для заполнения. Common Name используется в качестве имени пользователя Device VPN на Ideco NGFW Novum, поэтому Common Name у двух пользовательских сертификатов не может совпадать.

Расшифровка строк

- **Country Name (2 letter code) [XX]** - код страны в формате ISO 3166-1 alpha-2 (например, RU).

- **State or Province Name (full name) [Some-State]** - название региона или области (например, Moscow).
- **Locality Name (eg, city) [Default City]** - название города (например, Saint Petersburg).
- **Organization Name (eg, company) [Internet Widgits Pty Ltd]** - название организации.
- **Organizational Unit Name (eg, section) []** - название подразделения организации.
- **Common Name (e.g. server FQDN or YOUR name) []** - наименование сертификата.
- **Email Address []** - контактный email.

Дополнительные атрибуты:

- **A challenge password []** - пароль для дополнительной аутентификации. Рекомендуем оставить поле пустым.
- **An optional company name []:** - полное юридическое название организации.

4. Скопируйте файл `client1-dvpn.csr` на устройство со сгенерированным корневым сертификатом.

5. На устройстве с корневым сертификатом создайте файл **client1-dvpn.ext** для генерации сертификата. Включите в него параметры:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
```

6. На устройстве с корневым сертификатом сгенерируйте сертификат пользовательского устройства от корневого сертификата для Device VPN:

```
openssl x509 -req -in client1-dvpn.csr -CA ideco-dvpn_root-ca.pem -CAkey ideco-dvpn_root-ca.key -CAcreateserial -out client1-
```

- `client1-dvpn.csr` - файл, содержащий зашифрованный запрос на выпуск сертификата;
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат;
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ корневого сертификата;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат.

7. Проверьте, что сертификат был успешно создан командой:

```
openssl x509 -text -noout -in client1-dvpn.crt
```

- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат, без приватного ключа.
- Сертификат должен иметь атрибут `CA:FALSE` и `Subject Key Identifier`.

8. Перенесите полученный CRT-сертификат на клиентскую машину, где находится приватный ключ из шага 1.

9. Объедините приватный ключ и сертификат пользовательского устройства в PEM-файл:

Для Linux и macOS

```
cat client1-dvpn.key client1-dvpn.crt > client1-dvpn.pem
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат;
- `client1-dvpn.pem` - файл, содержащий пользовательский сертификат с приватным ключом внутри.

Для Windows

```
type client1-dvpn.key client1-dvpn.crt > client1-dvpn.pem
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат;
- `client1-dvpn.pem` - файл, содержащий пользовательский сертификат с приватным ключом внутри.

---

10. Сертификат `client1-dvpn.pem` с приватным ключом внутри, полученный на этом этапе, устанавливается на пользовательском устройстве и используется в параметрах Ideco Client.

Авторизация пользователей терминальных серверов

Классический контекст | Высокопроизводительный контекст

Терминальный сервер - сервер, позволяющий множеству пользователей одновременно работать в удаленных сессиях с общими вычислительными ресурсами сервера.

Особенности работы для пользователей терминальных серверов:

- Терминальный сервер должен работать под управлением Microsoft Windows Server версии 2019 и выше. Работа под другим ПО не гарантируется.
- Аутентификация пользователей осуществляется только через Active Directory.
- Для подключения пользователей установите на терминальный сервер Ideco Client.
- Ideco Client устанавливает туннель от терминального сервера до NGFW Novum.
- Каждый пользователь получает отдельный динамический виртуальный IP-адрес из заданной подсети.
- Для каждого пользователя можно настроить правила работы **Межсетевого экрана** и **Контент-фильтра**.
- Правила **Межсетевого экрана** работают только для протоколов TCP и UDP.

Не рекомендуется копировать приватный ключ корневого сертификата с машины, на который он был создан, во избежание компрометации ключа.

Рекомендуем создавать пользовательские сертификаты сразу на терминальном сервере, чтобы не переносить приватный ключ с машины на машину. Это понизит риск компрометации приватного ключа пользовательского сертификата.

Настройка авторизации пользователей

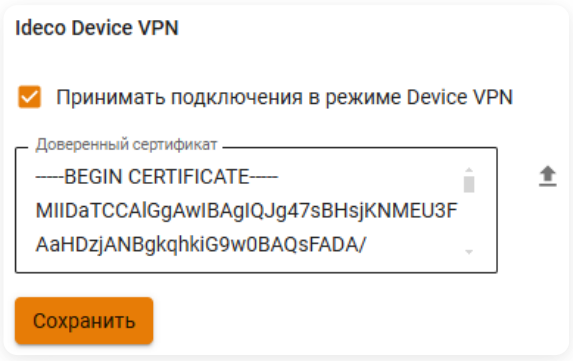
Перед настройкой терминального сервера необходимо:

- Интегрировать Ideco NGFW Novum с Microsoft Active Directory. Если Active Directory и терминальный сервер находятся на **разных физических машинах**, терминальный сервер нужно ввести в домен AD.
- Убедитесь, что нужные пользователи AD доступны для NGFW Novum на вкладке Учетные записи → Active Directory.
- Получить сертификаты или создать самоподписанные сертификаты для подключения. Пример создания самоподписанных сертификатов в статье.

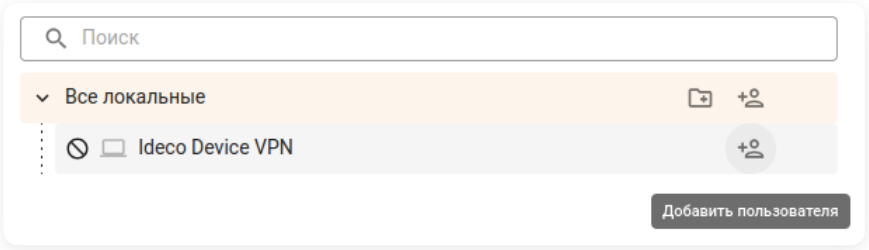
Вместо самоподписанных сертификатов рекомендуем использовать доверенный удостоверяющий центр, например, корпоративный УЦ на базе AD CS.

В Ideco NGFW Novum загружается только корневой или промежуточный сертификат УЦ без приватного ключа, который используется как сертификат Device VPN для проверки сертификата терминального сервера. Сертификат терминального сервера с приватным ключом должен находиться только на самом терминальном сервере и использоваться для аутентификации терминального сервера в Ideco NGFW Novum. Передавать приватные ключи в Ideco NGFW Novum нельзя.

1. Перейдите в **Пользователи** → **Ideco Client**, включите опцию **Принимать подключения в режиме Device VPN** и загрузите корневой сертификат (обязательно без приватного ключа):



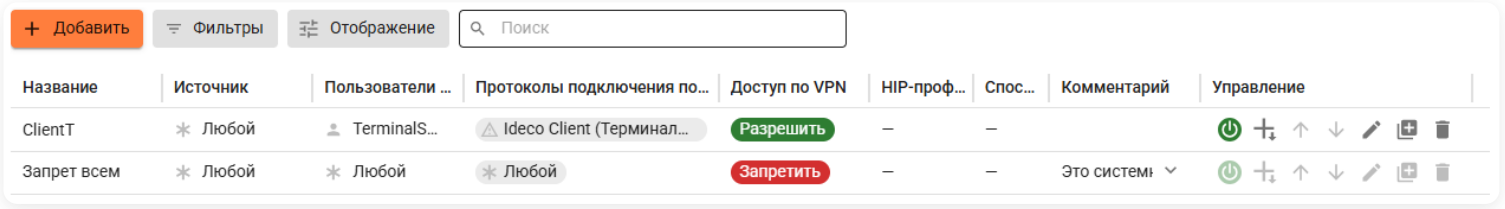
2. Перейдите в **Пользователи** → **Учетные записи** и в группу **Ideco Device VPN** добавьте устройство, загрузив пользовательский сертификат, подписанный корневым сертификатом. Пользовательский сертификат не должен включать в себя приватный ключ, поскольку это повышает шансы компрометации приватного ключа пользовательского сертификата:



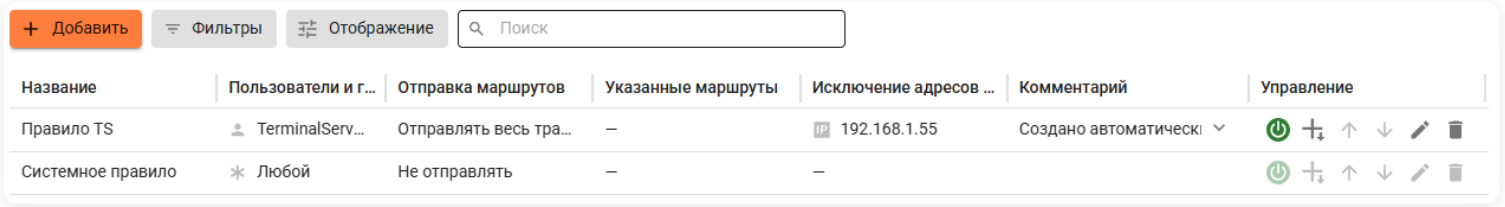
Для добавления нескольких устройств в группу **Ideco Device VPN** убедитесь, что поле **Common Name** во всех пользовательских сертификатах уникальное, т.е. нет двух сертификатов с одинаковым **Common Name**. В противном случае добавить несколько устройств в группу **Device VPN** не выйдет.

Рекомендуем генерировать отдельный пользовательский сертификат для каждого устройства, поскольку в случае компрометации приватного ключа пользовательского сертификата достаточно будет перевыпустить один пользовательский сертификат и поставить на конкретное устройство. В противном случае нужно будет устанавливать новый пользовательский сертификат на все устройства, на которых был скомпрометированный сертификат.

3. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и добавьте правило, разрешающее подключение через Ideco Client:

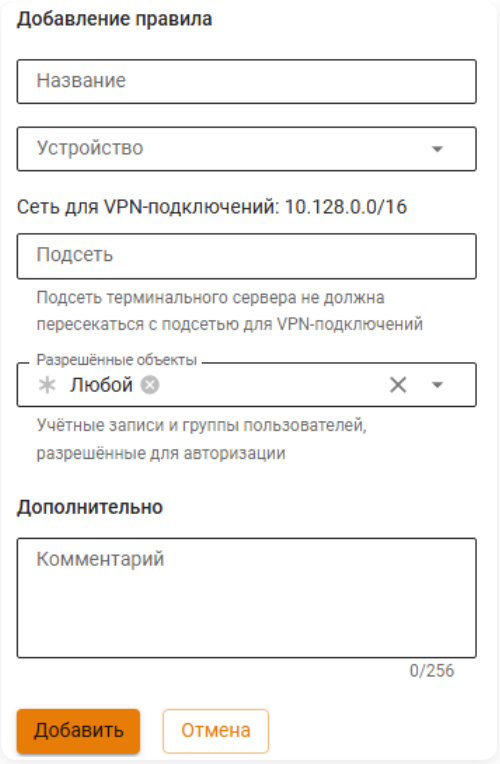


4. Перейдите в **Пользователи** → **VPN-подключения** → **Передача маршрутов** и добавьте правило, перенаправляющее трафик, который нужно проверять на Ideco NGFW Novum. Не стоит перенаправлять служебный трафик до контроллера домена AD или любой другой служебный трафик на Ideco NGFW Novum:



Клиенты терминального сервера будут использовать маршруты, заданные для самого терминального сервера в таблице **Передача маршрутов**.

5. Перейдите в **Пользователи** → **Ideco Client** → **Терминальный доступ** и добавьте правило с подсетью для выдачи IP-адресов пользователям:



- **Название** - укажите название правила.
- **Устройство** - укажите устройство пользователя, добавленное на шаге 2.
- **Подсеть** - укажите подсеть, в которой пользователям будут назначаться IP-адреса. Подсеть должна принадлежать к диапазону локальных подсетей и не должна пересекаться с подсетью для VPN-подключений, указанной в разделе **Пользователи** → **VPN-подключения** → **Основное**.
- **Разрешенные обьекты** - укажите группы пользователей, которым разрешена авторизация. Можно указать объекты: **Любой**, пользователь AD, группа безопасности AD, LDAP-фильтр.
- **Комментарий** - необязательное поле.

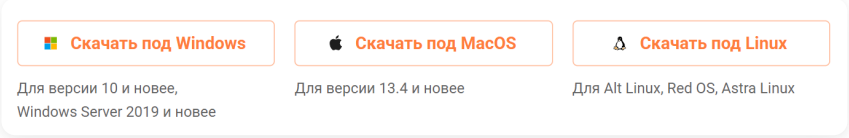
Подсеть для выдачи IP-адресов пользователям терминального сервера не должна пересекаться с уже имеющимися на Ideco NGFW Novum подсетями.

6. Загрузите корневой сертификат Ideco NGFW Novum на терминальный сервер и добавьте его в доверенные центры сертификации. Пользовательский сертификат из шага 1 и 2 также должен находиться на терминальном сервере (с приватным ключом).

Если используется Let`s Encrypt сертификат на доменное имя, к которому подключаются устройства с Ideco Client и терминальный сервер, загружать корневой сертификат NGFW Novum на конечные устройства и терминальный сервер не требуется. Доверие к этому сертификату уже будет на устройствах и терминальном сервере.

Лучше создавать пользовательские сертификаты сразу на терминальном сервере, чтобы не переносить приватный ключ с машины на машину. Это понизит риск компрометации приватного ключа пользовательского сертификата.

7. Установите Ideco Client на терминальный сервер. Для этого перейдите в **Пользователи** → **Ideco Client** и выберите **Скачать под Windows**:



8. Создайте на терминальном сервере `JSON-файл` и добавьте запись:

```
{
  "terminal_data": {
    "type": "terminal",
    "cert_data": "C:\\jsonconfig\\cert.pem",
    "server": "192.168.100.2"
  }
}
```

- `cert_data` - абсолютный путь до сертификата DeviceVPN с приватным ключом в формате `<диск>:\\<путь\\до\\сертификата>`.
- `server` - IP-адрес или FQDN (Fully Qualified Domain Name) сервера Ideco NGFW Novum.

9. Откройте командную строку от имени администратора и выполните команду:

```
"C:\Program Files\Ideco\<Версия Агента>\IdecoClient.exe" --set-json-config="C:\path\to\terminal-conifg.json"
```

- `"C:\Program Files\Ideco\<Версия Агента>\IdecoClient.exe"` - абсолютный путь к `IdecoClient.exe`.
- `"C:\Program Files\Ideco\test.json"` - абсолютный путь к `JSON-файлу` конфигурации.

После настройки конфигурации терминальный сервер должен успешно пройти авторизацию в Ideco NGFW Novum. Для проверки авторизации перейдите в **Мониторинг → Сессии пользователей**. Должна появиться новая запись с названием добавленного терминального сервера, а в столбце **Тип авторизации** указано значение **Терминальный сервер**.

10. Пользователи смогут подключаться к терминальному серверу по протоколу RDP (Remote Desktop Protocol), используя свои учетные данные Active Directory для аутентификации. Система автоматически назначит пользователям динамические виртуальные IP-адреса из указанной подсети, а информация об активных авторизациях появится в таблице **Мониторинг → Сессии пользователей**.

Один и тот же пользователь может авторизоваться со своего компьютера в Ideco NGFW Novum как непосредственно (через VPN, через IP/MAC и т.п.), так и через любой терминальный сервер, к которому у пользователя есть доступ. Терминальный сервер автоматически авторизует пользователя под новым IP (как отдельную сессию). Это позволяет гибко настраивать правила **Межсетевого экрана** и **Контент-фильтра** для каждого способа подключения.

Для управляющего соединения терминального сервера используется порт 443 по умолчанию. Резервный порт 14765 можно указать в поле `server` в формате `IP:14765` или `домен:14765` (например, `server.com:14765`).
В режиме терминального сервера поднимается туннель только через 3051 порт UDP.

Диагностика работы Ideco Client

Как включить режим отладки для Ideco Client

Настройка режима отладки Ideco Client для сбора диагностической информации

Перейти

Диагностика работы Ideco Client при помощи архива с логами и системными данными

Разовый сбор логов и системных данных в один архив

Перейти

Диагностика работы Ideco Client с помощью логирования

Включение логирования позволит анализировать работу Ideco Client для диагностики проблем

Перейти

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Как включить режим отладки для Ideco Client

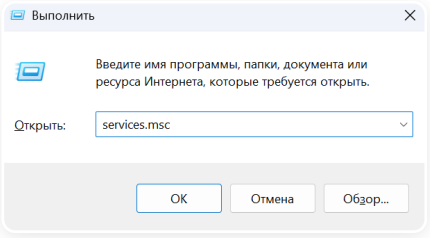
Классический контекст | Высокопроизводительный контекст

Включение режима отладки позволит собрать расширенные диагностические данные.

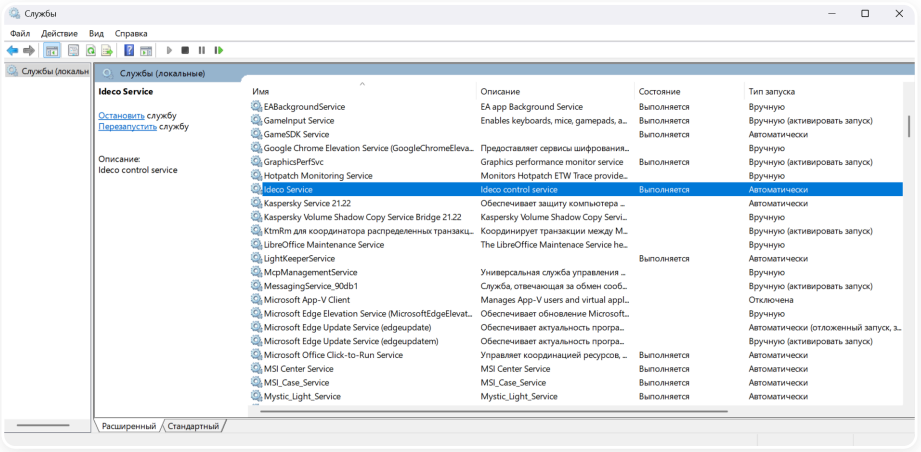
Необходима учетная запись с правами администратора.

Для включения режима:

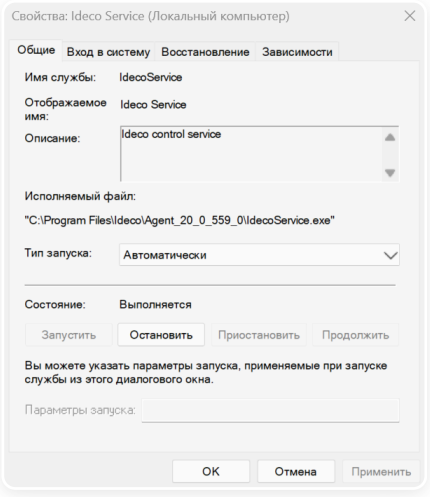
1. Нажмите **Win+R**, введите `services.msc` и нажмите **Ок**:



2. Найдите службу **Ideco Service**:

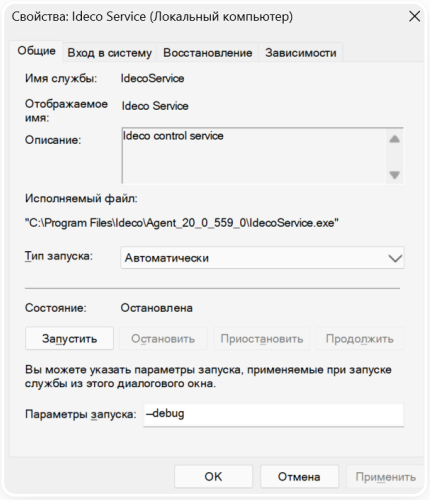


3. Двойным кликом откройте свойства, нажмите **Остановить** и дождитесь остановки службы:



Если произошла ошибка остановки службы, дождитесь запуска службы и остановите службу повторно.

4. В поле **Параметры запуска** введите `--debug` и нажмите **Запустить** для старта службы:



Не закрывайте окно **Свойства: Ideco Service**, иначе режим отладки работать не будет.

5. Запустите Ideco Client, чтобы воспроизвести ошибку.

6. Получите расширенные данные с помощью диагностического архива или системных утилит.

При необходимости обратитесь в техническую поддержку.

Диагностика работы Ideco Client при помощи архива с логами и системными данными

Классический контекст | Высокопроизводительный контекст

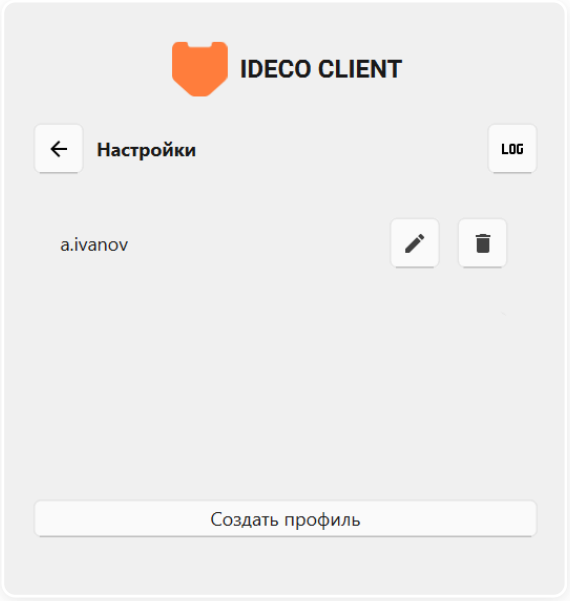
Сбор диагностической информации позволит получить структурированный архив данных для анализа работы Ideco Client. Полученные данные помогут администраторам и специалистам технической поддержки в устранении неполадок.

Запустите сбор данных:

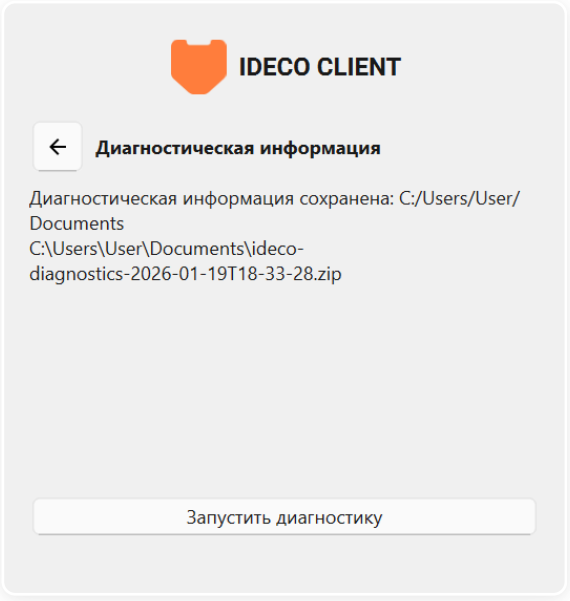
Графический интерфейс

1. Запустите Ideco Client и нажмите .

2. В настройках нажмите LOG и выберите, куда сохранить ZIP-архив с результатами:



3. После окончания сбора данных откроется окно с путем и названием созданного архива с логами:



Командная строка

> В командной строке не отображается ход процесса сбора данных, только итоговый статус.

1. Выполните команду, указав абсолютный путь, куда сохранить ZIP-архив с результатами диагностики:

```
ideco-client --collect <"абсолютный путь к директории">
```

Пример на Windows:

```
ideco-client --collect C:\Users\Username\Desktop\
```

> На Linux и macOS команда аналогична, отличается только синтаксис пути (прямые слеши `/` вместо обратных `\`).

2. Сообщение при успешном завершении:

```
[OK] Diagnostics collected: C:\Users\Username\Desktop\ideco-diagnostics-YYYY-MM-DDTHH-MM.zip
```

Архив содержит данные за последние два дня. Имя файла формируется по шаблону: `ideco-diagnostics-YYYY-MM-DDTHH-MM.zip`, где `YYYY-MM-DD` - дата создания, `THH-MM` - время создания (буква `T` используется как разделитель согласно стандарту ISO 8601). Пример: `ideco-diagnostics-2025-07-31T14-23.zip`.

Содержимое архива

- `logs/`
  - `ideco-client_logs.json` - логи Ideco Client
  - `ideco-service_logs.json` - логи службы Ideco Service
- `system/`
  - `system_info.json` - информация об ОС, имени хоста и DNS-конфигурации
  - `network.json` - список сетевых интерфейсов с основными параметрами

Содержание файлов

ideco-client_logs.json - логи Ideco Client.

```
{
  "ts": "string",
  "comp": "string",
  "lvl": "string",
  "type": "string",
  "msg": "string",
  "data": {
    "eid": "integer",
    "erid": "integer",
    "pid": "integer",
    "tid": "integer",
    "comp_name": "string"
  }
}
```

- `"ts"` - timestamp (ISO 8601, UTC), берется из поля `SystemTime`;
- `"comp"` - источник события:
  - `ideco-service` - служба `ideco-service`;
  - `ideco-client - ProviderName` - Ideco Client.
- `"lvl"` - уровень логирования:

    - `"INFO"` - штатные события работы приложения;
    - `"WARN"` - нештатная ситуация, которая не привела к сбою, но требует внимания;
    - `"ERROR"` - ошибка, которая повлияла на выполнение конкретной операции или запроса, но позволяет приложению продолжать работу;
    - `"DEBUG"` - детальная служебная информация о ходе выполнения;
    - `"TRACE"` - максимально детальная отладочная информация выполнения;
    - `"CRITICAL"` - критическая ошибка, требующая немедленного вмешательства и приводящая к остановке компонента или всего приложения.
- `"type"` - тип события:
    - `"logs"` - логи службы Ideco Service;
    - `"system"` - информация об ОС, имени хоста и DNS-конфигурации;
    - `"network"` - список сетевых интерфейсов с основными параметрами.
- `"msg"` - краткое текстовое описание события;
- `"data"`:
    - `"eid"` - идентификатор события (`EventID`);
    - `"erid"` - идентификатор записи события (`EventRecordID`);
    - `"pid"` - идентификатор процесса (`ProcessID`);
    - `"tid"` - идентификатор потока (`ThreadID`);
    - `"comp_name"` - имя компьютера (`Computer`).

ideco-service_logs.json - логи службы Ideco Service.

```
{
  "ts": "string",
  "comp": "string",
  "lvl": "string",
  "type": "string",
  "msg": "string",
  "data": {
    "eid": "integer",
    "erid": "integer",
    "pid": "integer",
    "tid": "integer",
    "comp_name": "string"
  }
}
```

- `"ts"` - timestamp (ISO 8601, UTC), берется из поля `SystemTime`;
- `"comp"` - источник события:
    - `ideco-service` - служба `ideco-service`;
    - `ideco-client - ProviderName` - Ideco Client.
- `"lvl"` - уровень логирования:
    - `"INFO"` - штатные события работы приложения;
    - `"WARN"` - нештатная ситуация, которая не привела к сбою, но требует внимания;
    - `"ERROR"` - ошибка, которая повлияла на выполнение конкретной операции или запроса, но позволяет приложению продолжать работу;
    - `"DEBUG"` - детальная служебная информация о ходе выполнения;
    - `"TRACE"` - максимально детальная отладочная информация выполнения;
    - `"CRITICAL"` - критическая ошибка, требующая немедленного вмешательства и приводящая к остановке компонента или всего приложения.
- `"type"` - тип события:
    - `"logs"` - логи службы Ideco Service;
    - `"system"` - информация об ОС, имени хоста и DNS-конфигурации;
    - `"network"` - список сетевых интерфейсов с основными параметрами.
- `"msg"` - краткое текстовое описание события;
- `"data"`:
    - `"eid"` - идентификатор события (`EventID`);
    - `"erid"` - идентификатор записи события (`EventRecordID`);
    - `"pid"` - идентификатор процесса (`ProcessID`);
    - `"tid"` - идентификатор потока (`ThreadID`);
    - `"comp_name"` - имя компьютера (`Computer`).

system_info.json - информация об операционной системе, имени хоста и DNS-конфигурации.

```
{
  "ts": "string",
  "type": "string",
  "data": {
    "os_name": "string",
    "os_ver": "string",
    "arch": "string",
    "build": "string",
    "vendor": "string",
    "hostname": "string",
    "dns_srv": ["string"],
    "dns_sfx": ["string"],
    "dns_en": "boolean"
  }
}
```

- `"ts"` - timestamp (ISO 8601, UTC);
- `"type"` - тип данных `system_info`;
- `"data"` - объект с детальной системной информацией:
  - `"os_name"` - название ОС;
  - `"os_ver"` - версия ОС;
  - `"arch"` - архитектура процессора;
  - `"build"` - номер сборки;
  - `"vendor"` - производитель ОС;
  - `"hostname"` - имя хоста;
  - `"dns_srv"` - DNS-серверы;
  - `"dns_sfx"` - DNS-суффиксы поиска;
  - `"dns_en"` - статус службы DNS.

network.json - список сетевых интерфейсов с основными параметрами.

```
{
  "ts": "string",
  "type": "string",
  "data": {
    "name": "string",
    "mac": "string",
    "ipv4": ["string"],
    "netmask": "string",
    "gateway": "string",
    "status": "string",
    "if_type": "string",
    "mtu": "integer",
    "dns_srv": ["string"],
    "dns_sfx": ["string"]
  }
}
```

- `"ts"` - временная метка (ISO 8601, UTC);
- `"type"` - тип данных: `network`;
- `"data"` - объект с информацией о сетевом интерфейсе:
  - `"name"` - имя сетевого интерфейса;
  - `"mac"` - MAC-адрес (формат: `XX:XX:XX:XX:XX:XX`);
  - `"ipv4"` - массив IPv4 адресов;
  - `"netmask"` - маска подсети;
  - `"gateway"` - шлюз по умолчанию;
  - `"status"` - статус интерфейса:
    - `"up"` - подключен;
    - `"down"` - не подключен;
    - `"unknown"` - статус неизвестен.
  - `"if_type"` - тип интерфейса:
    - `"ethernet"` - проводной интерфейс;
    - `"tunnel"` - виртуальный интерфейс, не привязанный к физическому сетевому порту;

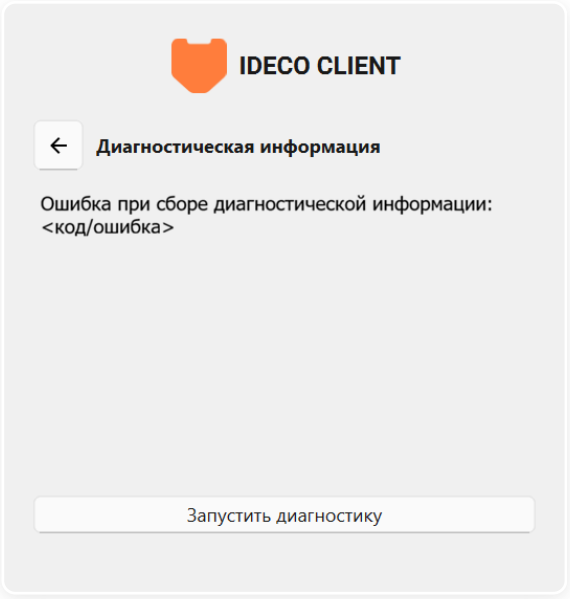
        - `"bridge"` - интерфейс объединяющий несколько интерфейсов в один логический сегмент.
        - `"loopback"` - виртуальный интерфейс, не привязанный к физическому сетевому порту.
    - `"mtu"` - размер пакета MTU;
    - `"dns_srv"` - DNS-серверы, привязанные к интерфейсу;
    - `"dns_sfx"` - DNS-суффиксы поиска.

Данные, которые не собираются:

- Логины
- Пароли
- Электронная почта
- Токены аутентификации
- Приватные ключи
- Пути к домашним директориям пользователей
- Сетевые идентификаторы (SID и аналогичные)

Возможные ошибки при сборе данных

При использовании командной строки текст ошибки будет выведен в командной строке. При использовании графического интерфейса описание и код ошибки будут показаны в окне запуска диагностики:



Список возможных ошибок:

Код ошибки	Сообщение в графическом интерфейсе	Сообщение в командной строке	Как исправить
1	Не указан путь	[ERROR] Invalid command syntax	• Укажите обязательный параметр при вызове команды • Путь должен быть абсолютным. Например: ideco-client --collect C:\Users\Username\Desktop
1	Некорректный путь	[ERROR] Diagnostics collection failed: invalid output path	• Проверьте корректность и существование пути • Путь не должен содержать лишних символов • У пользователя, который запускает диагностику, должны быть права доступа на запись в указанную директорию
2	Сбор уже выполняется	[INFO] Diagnostics collection failed: already running	• Дождитесь завершения текущего процесса сбора диагностики • Если сбор данных завис, перезапустите службу Ideco Service
3	Служба недоступна	[ERROR] Diagnostics collection failed: communication error	• Убедитесь, что служба Ideco Service запущена • Перезапустите службу Ideco Service • Перезапустите Ideco Client
3	Ошибка архивации или сериализации	[ERROR] Diagnostics collection failed: <error_description>	• Убедитесь, что антивирус не блокирует создание архивных файлов

3	Ошибка чтения данных	[ERROR] Diagnostics collection failed: data read error	• Проверьте целостность файлов и повторно запустите сбор данных
3	Недостаточно места на диске	[ERROR] Diagnostics collection failed: not enough disk space	• Проверьте наличие свободного места на диске (требуется минимум 500 МБ) или выберите другой путь для сохранения
3	Внутренняя ошибка службы	[ERROR] Diagnostics collection failed: internal service error	• Перезапустите службу Ideco Service

Полезные ссылки

- **Как включить режим отладки для Ideco Client**
- **Кастомная настройка Ideco Client**

Диагностика работы Ideco Client с помощью логирования

Классический контекст | Высокопроизводительный контекст

Включение логирования позволит анализировать работу Ideco Client для диагностики проблем. Полученные данные помогут администраторам и специалистам технической поддержки в устранении неполадок.

Особенности работы логирования

- Для выполнения команд могут потребоваться права администратора.
- Изменение уровня логирования применяется сразу и не требует перезапуска системы.
- При повторном запуске Ideco Client записи в логах не перезаписываются, а дополняются.
- Доступны логи за последние два дня.

Настройка логирования

1. Откройте командную строку или терминал.

- Windows - командная строка (cmd) или PowerShell.
- Linux и macOS - терминал.

2. Введите команду для перехода к каталогу, где установлен Ideco Client:

ОС	Команда
Windows, Linux, macOS	`cd <путь_к_каталогу_агента>`

Пример: `cd C:\Program Files\Ideco Client`.

3. Выберите необходимый уровень логирования и введите команду:

ОС	Команда
Windows	`.\IdecoClient.exe --set-log-level <уровень_логирования>`
Linux, macOS	`IdecoClient --set-log-level <уровень_логирования>`

Уровни логирования:

- `info` - стандартный уровень детализации.
- `debug` - расширенная отладочная детализация.
- `trace` - максимальный уровень детализации.

Пример: `.\IdecoClient.exe --set-log-level debug`

4. Введите команду, чтобы включить запись логов:

ОС	Команда
Windows	`.\IdecoClient.exe --set-enable-log-to-file true`
Linux, macOS	`IdecoClient --set-enable-log-to-file true`

После включения логирования формируются два файла `IdecoClient_log.txt` и `IdecoService_log.txt` в директории:

ОС	Путь
Windows	`IdecoClient_log.txt` по пути `%TEMP%` `IdecoService_log.txt` по пути `C:\windows\temp`
Linux	`/tmp`
macOS	`/tmp` или `/var/folders/`

Возврат к стандартному уровню логирования

Для возврата логирования к уровню `info` введите команду:

ОС	Команда
Windows	`.\IdecoClient.exe --reset-log-level`
Linux, macOS	`IdecoClient --reset-log-level`

Отключение записи логов

Для отключения записи логов введите команду:

ОС	Команда
Windows	`.\IdecoClient.exe --set-enable-log-to-file false`
Linux, macOS	`IdecoClient --set-enable-log-to-file false`

Профили устройств

Классический контекст | Высокопроизводительный контекст | API

Профили устройств или HIP-профили (Host Information Profile) позволяют задать критерии проверки устройств, которые подключаются к NGFW только через Ideco Client. Для других сессий авторизации профили не назначаются.

С помощью профилей реализуется ZTNA (Zero Trust Network Access) - технология обеспечения безопасного доступа к сети, основанная на **принципе нулевого доверия**. ZTNA позволяет контролировать и аутентифицировать устройства пользователей перед предоставлением доступа к ресурсам сети.

Возможно использование HIP-профилей для терминального сервера. В этом случае HIP-профили определяются только для сессии авторизации сервера, но не для сессий авторизации терминальных пользователей.

В случае несоответствия HIP-профилю терминальная сессия закрывается вместе со всеми сессиями терминальных пользователей.

Информация, собираемая Ideco Client

Данные, которые Ideco Client собирает с устройства пользователя:

- Версия Windows
- Наличие установленного пакета обновлений
- Наличие установленного антивируса
- Наличие актуальной базы антивируса
- Дата последней проверки антивируса
- Версия межсетевого экрана и вендор
- Информация о процессах, запущенных на устройстве
- Информация о запущенных службах
- Информация о ключах реестра
- Добавление устройства в домен

Критерии проверки, доступные на NGFW Novum

Критерии, которые администратор может задать в HIP-объектах для проверки устройств:

- Операционная система
- Пакет обновлений Windows
- Антивирус
- Межсетевой экран
- Процесс, запущенный на устройстве
- Запущенная служба Windows
- Ключ реестра Windows

HIP-объекты

На вкладке создаются объекты, каждый HIP-объект - совокупность критериев проверки устройства. HIP-объекты используются для создания HIP-профиля. Каждый из HIP-объектов возвращает логическое значение. Если критерии HIP-объекта выполнены, то объект возвращает положительный результат.

Для создания HIP-объекта выполните действия:

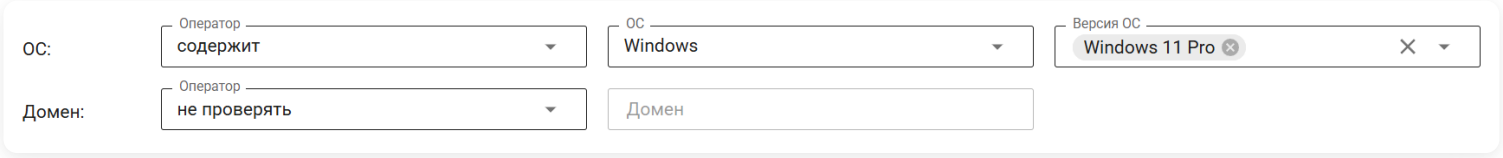
1. Перейдите в **Профили устройств** → **HIP-объекты** и нажмите **Добавить**.

2. Введите название HIP-объекта:



3. Выберите критерии, включив опцию **Включить проверку** для необходимой проверки:

ОС и домен



ОС - проверка по операционной системе.

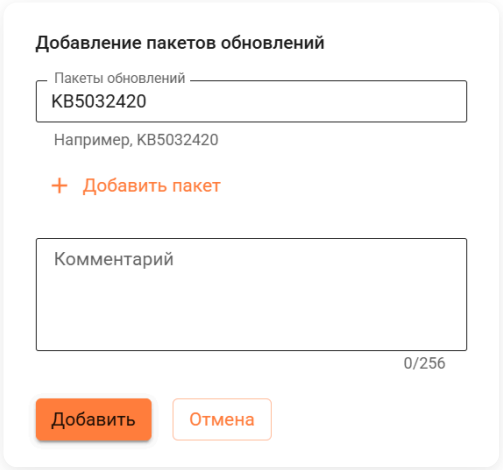
- Оператор:
  - содержит
  - не содержит
  - не проверять
- ОС:
  - Windows
  - Linux
  - macOS
- Версия ОС

Домен - проверка по домену Active Directory, к которому присоединено устройство.

- Оператор:
  - содержит
  - не содержит
  - не проверять
- Домен

Пакеты обновлений (KB)

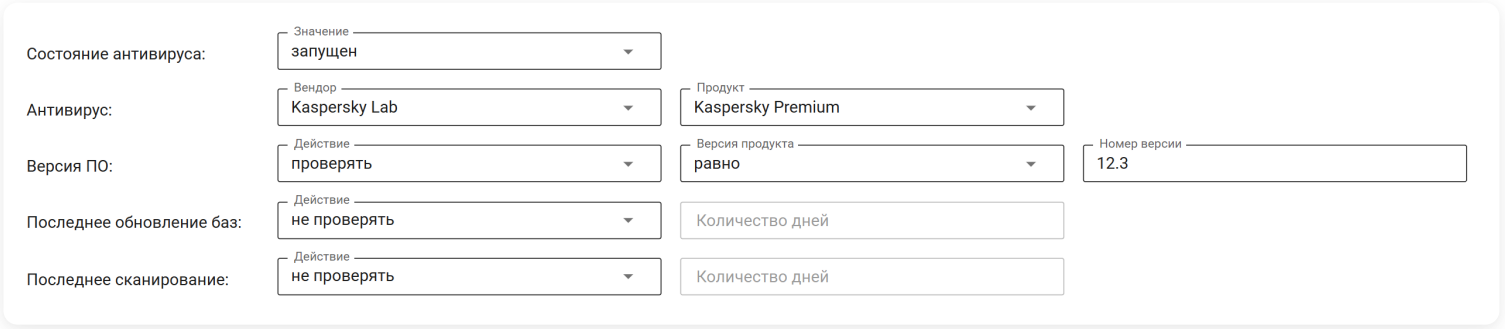
1. Нажмите **Добавить** и укажите пакет обновлений Windows (например, KB5032420):



Для добавления нескольких пакетов обновлений нажмите **Добавить пакет**.

2. Нажмите **Добавить**.

Антивирус



Состояние антивируса - проверка по статусу антивируса.

- Значение:
  - Установлен (антивирус установлен, но не запущен)
  - Запущен (антивирус установлен и запущен)

Антивирус - проверка по антивирусу.

- Вендор (например, Kaspersky Lab)
- Продукт (например, Kaspersky Premium)

Версия ПО - проверка по версии антивируса.

- Действие:
  - Проверять
  - Не проверять
- Версия продукта:
  - Равно
  - Содержит
- Номер версии

Последнее обновление баз - проверка по времени обновления баз.

- Действие:
  - Не проверять
  - Проверять в течение последних дней
- Количество дней (сколько прошло дней с момента обновления баз антивируса)

Последнее сканирование - проверка по времени последнего сканирования антивирусом.

- Действие:
  - Не проверять
  - Проверять в течение последних дней
- Количество дней (сколько прошло дней с момента последнего сканирования)

Межсетевой экран

- Включите опцию **Запущен** для проверки того, запущен ли межсетевой экран.

Продукт - проверка по вендору и продукту межсетевого экрана.

- Оператор:
  - содержит
  - не проверять
- Вендор (например, DrWeb)
- Продукт (например, Dr.Web Security Space)

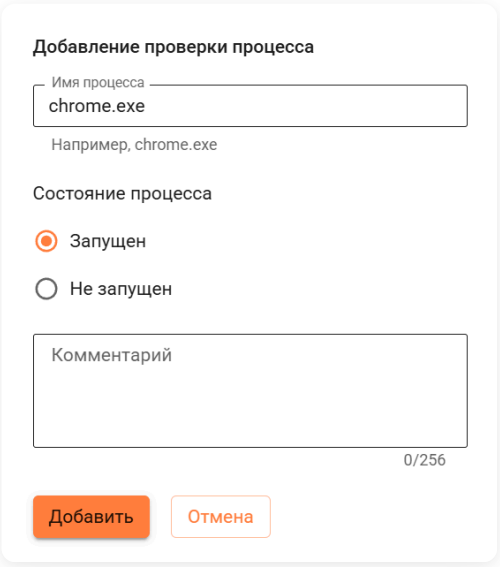
Версия ПО - проверка по версии межсетевого экрана.

- Оператор:
  - содержит

- не проверять
- Версия

Процессы

1. Нажмите **Добавить** и заполните поля:

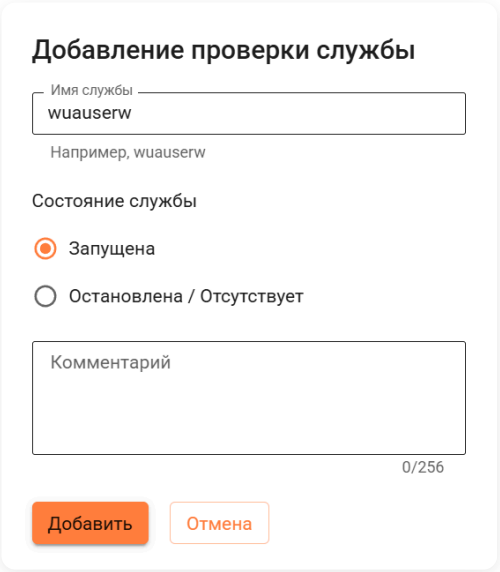


- Имя процесса (например, `chrome.exe`)
- Состояние процесса:
  - Запущен
  - Не запущен

2. Нажмите **Добавить**.

Службы

1. Нажмите **Добавить** и заполните поля:



- Имя службы (например, `wuauserw`)
- Состояние службы:
  - Запущена
  - Остановлена или отсутствует

2. Нажмите **Добавить**.

Ключи реестра

1. Нажмите **Добавить** и заполните поля:

- **Путь** - путь ключа реестра (например, `HKEY_LOCAL_MACHINE\DriverDatabase`).

- **Параметр** - параметр ключа реестра (например, `WallpaperOriginX`).
- **Инвертировать значение** - включите опцию, если необходимо инвертировать значение ключа реестра.
- **Значение** - укажите значение ключа реестра (например, `0x00000000 (0)`).

2. Нажмите **Добавить**.

> При создании критерия проверки **Ключи реестра** используйте корневые разделы реестра Windows:
>
> - `HKEY_LOCAL_MACHINE`
> - `HKEY_CURRENT_USER`
> - `HKEY_CLASSES_ROOT`
> - `HKEY_USERS`
> - `HKEY_CURRENT_CONFIG`

4. Нажмите **Добавить**.

HIP-профили

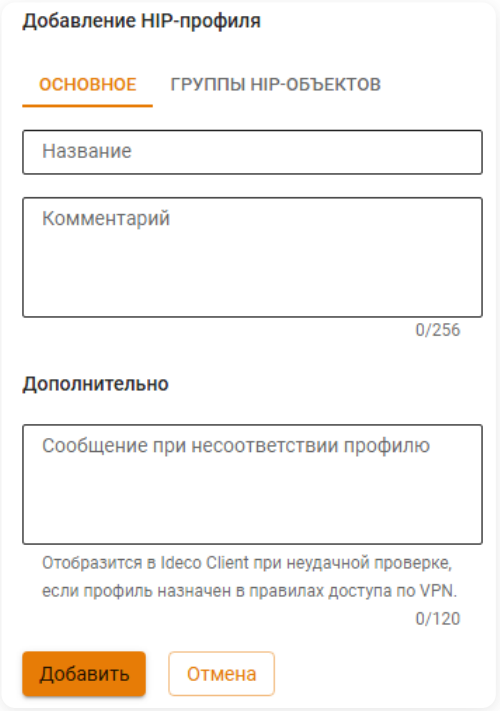
На вкладке создаются HIP-профили, состоящие из сгруппированных с помощью логических операций HIP-объектов И/ИЛИ.

Если при проверке устройства пользователя логическое выражение HIP-профиля возвращает положительный результат, профиль закрепляется за сессией авторизации и отображается в таблице Сессии пользователей. Если ни один HIP-профиль не совпал с сессией авторизации, то на сессию назначается специальный HIP-профиль **Устройство без профиля**. На одну сессию авторизации может быть назначено несколько профилей при совпадении.

Для создания HIP-профиля выполните действия:

1. Перейдите в **Профили устройств** → **HIP-профили** и нажмите **Добавить**.

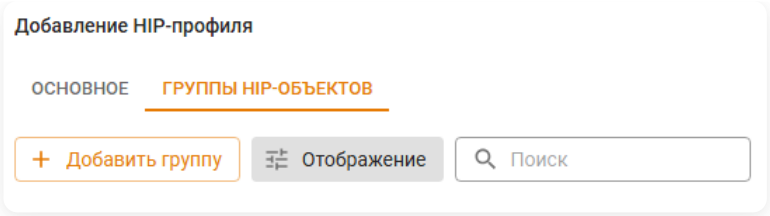
2. Заполните поля на вкладке **Основное**:



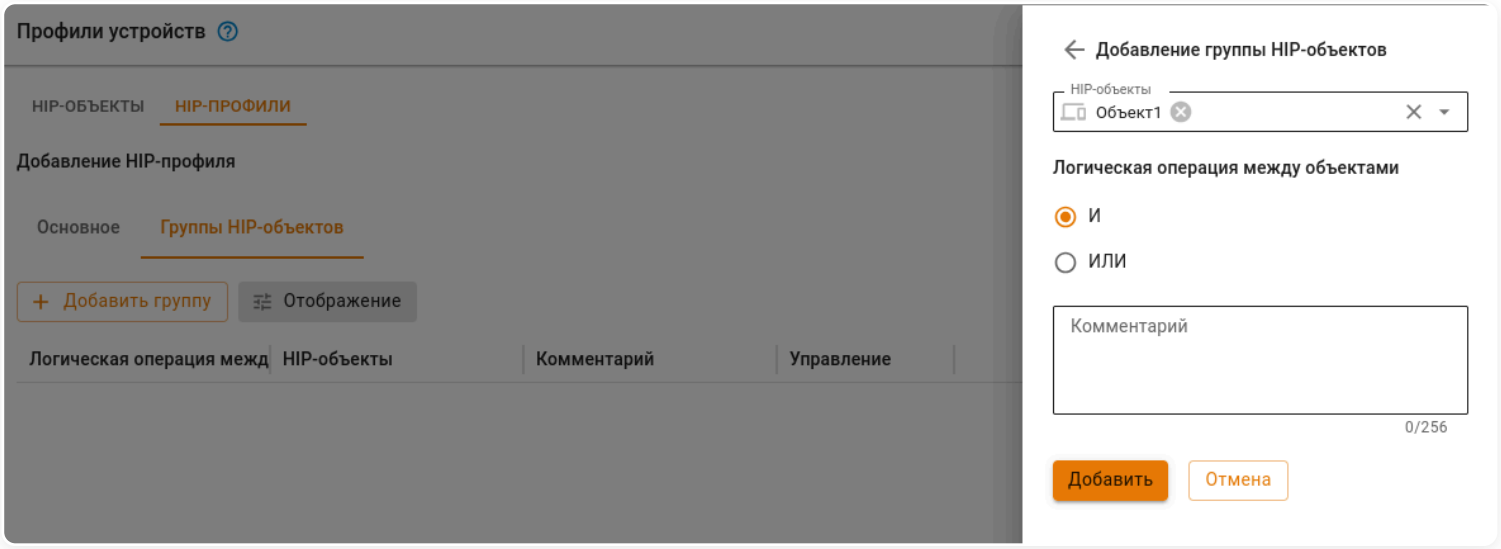
Расшифровка полей

- **Название HIP-профиля** - укажите название HIP-профиля.
- **Комментарий** - произвольный текст. Не более 256 символов.
- **Сообщение при несоответствии профилю** - введите текст, который отобразится в Ideco Client в случае несоответствия устройства назначенному HIP-профилю в правилах доступа по VPN. Максимальная длина - 120 символов. Если поле пустое, то в Ideco Client по умолчанию выводится текст: **Проверка безопасности не пройдена**:

3. Перейдите на вкладку **Группы HIP-объектов**, нажмите **Добавить группу**:



4. Выберите HIP-объекты, указав логическую операцию между объектами И/ИЛИ:



5. Нажмите **Добавить**.

HIP-профили можно использовать в качестве дополнительного условия в правилах **FORWARD**. Правило сработает, если трафик исходит от устройства, которому назначен хотя бы один профиль, указанный в правиле.

Использование HIP-профилей

HIP-объекты и профили не влияют на правила трафика до их применения в правилах **Межсетевого экрана**. Чтобы с помощью профилей ограничить или разрешить доступ к ресурсам сети, необходимо:

1. Создать HIP-объекты.

2. Сгруппировать созданные HIP-объекты в HIP-профили.

3. В **Правила трафика** → **Межсетевой экран** → **FORWARD** создать и включить правило с использованием одного или нескольких профилей, созданных в пункте 2.

Проверка профилей происходит каждые 15 минут.

Примеры использования

Запрет доступа к сети устройствам без профиля

Устройствам, которые не прошли проверку на соответствие ни одному из созданных HIP-профилей, назначается специальный HIP-профиль **Устройство без профиля**. Доступ таких устройств к сети можно ограничить правилом **Межсетевого экрана**. Для этого:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

2. Создайте и включите правило вида:

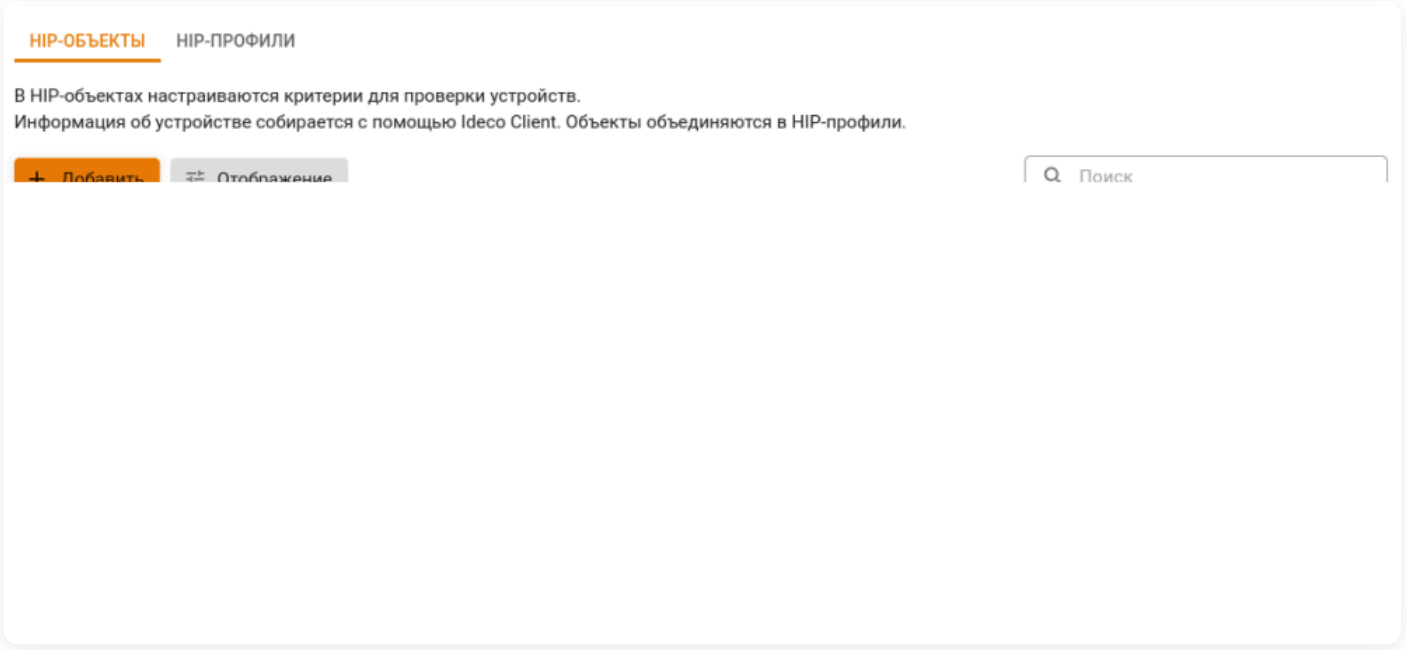
Если в таблице правил **Межсетевого экрана** выше запрещающего правила находится другое правило, которому соответствует трафик одного или нескольких устройств без профиля (например, правило для пользователя или группы пользователей без указания HIP-

профиля), то к трафику будет применено правило, расположенное выше в таблице. Пример:

Ограничение доступа устройств к сети

В качестве примера настроим **Межсетевой экран** так, чтобы пользователи имели доступ к сети, только если устройства пользователей соответствуют HIP-профилю `Profile1`. Для этого:

1. Перейдите в **Пользователи** → **Профили устройств** → **HIP-объекты** и создайте требуемые HIP-объекты:



2. Перейдите на вкладку **HIP-профили** и создайте профиль с созданными ранее HIP-объектами:

3. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**, создайте и включите правило, разрешающее доступ к сети всем пользователям, чьи устройства соответствуют профилю `Profile1`:

4. Ниже создайте и включите правило, запрещающее весь трафик:

В результате трафик всех пользователей, чьи устройства соответствуют HIP-профилю `Profile1`, подпадет под разрешающее правило. Остальной трафик подпадет под запрещающее правило.

Полезные ссылки

- **Как безопасно подключить удаленного подрядчика**

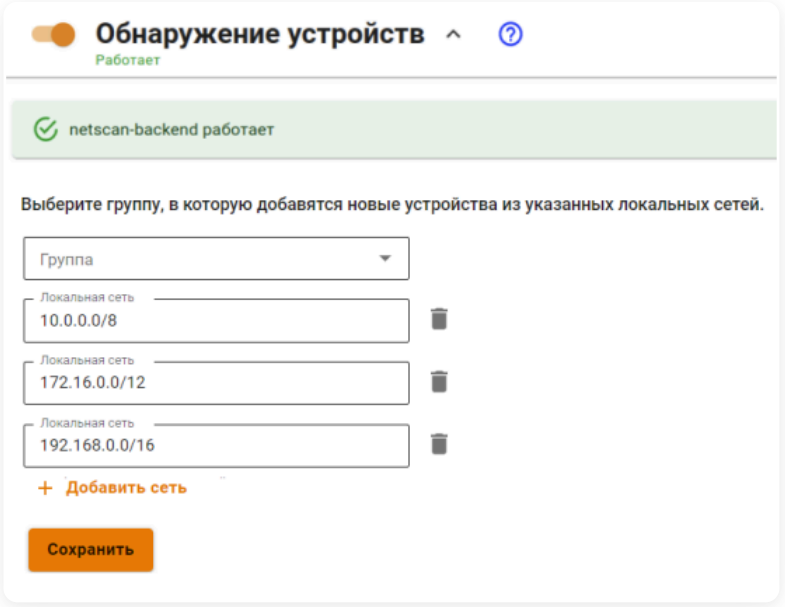
Обнаружение устройств

API

Функциональность доступна в **Классическом** и **Системном контекстах**.

Название службы раздела **Обнаружение устройств**: `ideco-netscan-backend`.
Список служб для других разделов доступен по ссылке.

Модуль **Обнаружение устройств** автоматически создает пользователей с авторизацией по IP-адресу и MAC-адресу. Если модуль включен, то при попытке выхода в интернет будет создана учетная запись с именем, соответствующим NetBIOS-имени устройства:



- **Группа** - группа для автоматически добавленных пользователей.
- **Локальная сеть** - список сетей, для которых попытка выхода в интернет будет активировать создание пользователя.

Примечание

При необходимости можно ограничить локальные сети, пользователи из которых будут автоматически добавлены и авторизованы на Ideco NGFW Novum. Например, так можно авторизовать пользователей, подключающихся по Wi-Fi или другой открытой сети.

Особенности работы модуля **Обнаружение устройств**:

1. Модуль не сканирует сети в поисках устройств, а работает в пассивном режиме.

2. Если NetBIOS-имя определить не удалось, то в поле **Имя пользователя** будет записан IP-адрес найденного устройства.

3. Если в базе пользователей на Ideco NGFW Novum уже есть учетная запись с логином, равным NetBIOS-имени машины, то NGFW использует данные пользователя без обновления параметров пользователя (в том числе IP- или MAC-адреса).

4. Для локальных адресов в одном Ethernet-сегменте модуль создает авторизацию по MAC-адресу. Если устройство находится в локальной сети за роутером, то модуль создает авторизацию по IP-адресу.

Примечание

При подключении к NGFW как к прокси-серверу система обнаружения устройств работать не будет.

Мониторинг

В разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

Сессии администраторов

Список всех сессий администраторов в Ideco NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS

Перейти >

Сессии пользователей

Список всех сессий пользователей, которые авторизовались в NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS

Перейти >

Сессии ЛК

Список активных сессий в личном кабинете Ideco NGFW

Перейти >

Графики загруженности

Статистика по авторизованным пользователям, количеству VPN-подключений, загрузки процессора и диска

Перейти >

Монитор трафика

Таблица, содержащая информацию о трафике, проходящем через Ideco NGFW в режиме реального времени

Перейти >

Проверка IP/домена

Поиск IP-адреса и домена в базах объектов и GeoIP

Перейти >

Telegram-бот

Настройка оповещений от Ideco Monitoring Bot

Перейти >

SNMP

В статье описана настройка доступа к Ideco NGFW по протоколу SNMP

Перейти >

Zabbix-агент

Интеграция Zabbix-агента в Ideco NGFW

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Сессии администраторов

API

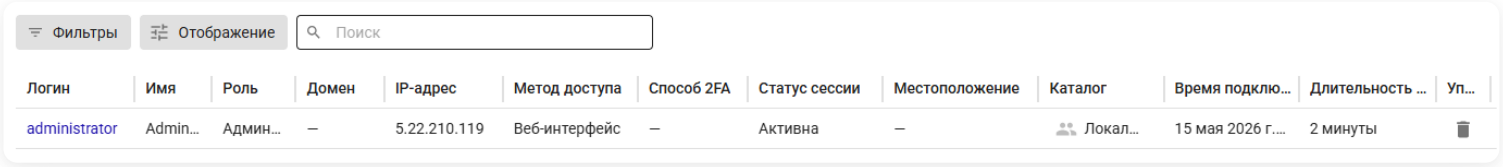
Функциональность доступна в **Классическом** и **Системном контекстах**.

Раздел содержит список всех сессий администраторов в NGFW, включая локальных, из Active Directory, ALD PRO, FreeIPA и RADIUS.

Сессии администраторов, подключенных через Ideco Center, не отображаются в разделе.

Сессия с IP-адресом 127.0.0.1 - сессия администратора, работающего в локальном меню сервера.

Таблица сессий авторизованных администраторов в NGFW:



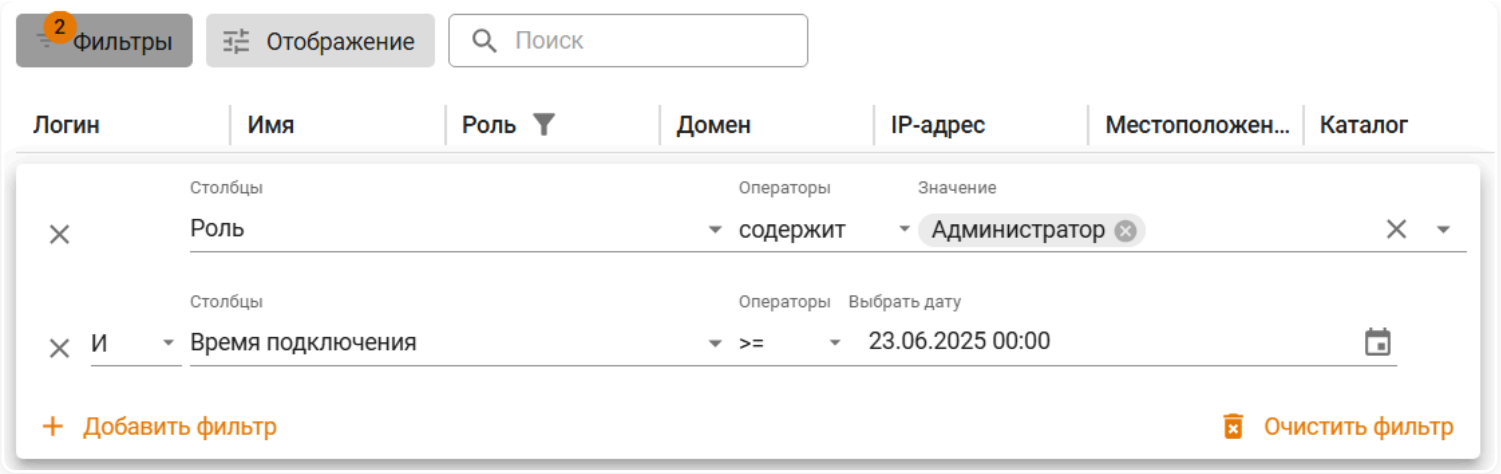
- **Логин** - логин администратора.
- **Имя** - имя администратора.
- **Роль** - возможные роли: Администратор, Только просмотр, Администратор ИБ, Администратор межсетевого экрана, Администратор настройки доступов, Просмотр отчетов, Создание отчетов.
- **Домен** - доменное имя, если администратор импортирован из Active Directory, ALD PRO или FreeIPA. В ином случае в ячейке прочерк.
- **IP-адрес** - IP-адрес устройства, с которого авторизован администратор.
- **Метод доступа** - способ подключения администратора: SSH, Веб-интерфейс или Локальное меню.
- **Способ 2FA** - второй фактор авторизации администратора, если настроен.
- **Местоположение** - географическое местоположение администратора.
- **Каталог** - тип администратора в зависимости от источника добавления: Локальная группа, AD, ALD, IPA, RAD.
- **Время подключения** - момент запуска сессии с указанием даты в формате день/месяц/год и времени в формате час/минута.
- **Длительность сессии** - продолжительность сессии администратора с момента запуска, указанного в столбце **Время подключения**.
- **Управление** - возможность деавторизовать любого администратора из интерфейса Ideco NGFW Novum.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока администратор будет автоматически деавторизован.

В столбце **Управление** администратор может деавторизовать самого себя.

Фильтрация таблицы

При наличии большого количества сессий администраторов воспользуйтесь кнопкой **Фильтры**. Фильтрация возможна по всем столбцам, кроме **Длительность сессии** и **Управление**, а также с использованием нескольких переменных:



При использовании фильтра по **Времени подключения** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные за 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

Полезные ссылки

- **Администраторы**
- **Действия администраторов**

Сессии пользователей

Классический контекст | Высокопроизводительный контекст | API

Раздел содержит список всех сессий пользователей, которые авторизовались в Ideco NGFW Novum, включая локальных, из Active Directory, ALD PRO, FreeIPA и RADIUS.

Количество сессий в мониторинге не является показателем занимаемых лицензий, так как под одной пользовательской учетной записью возможна одновременная авторизация до пяти устройств, что учитывается как одна лицензия.

Таблица сессий авторизованных пользователей в Ideco NGFW Novum:



Статусы подключения пользователей

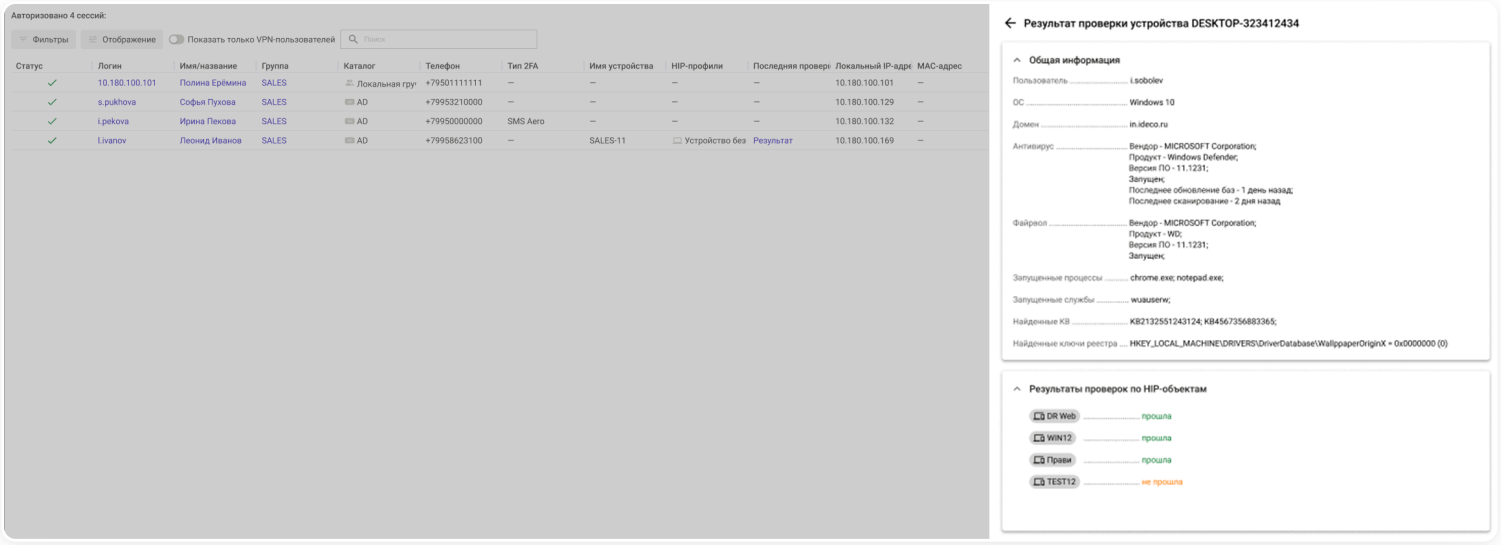
- **Подключено**. Пользователь авторизован.

- **Ожидает второй фактор авторизации**. Пользователь создал и активировал VPN-подключение, но не прошел двухфакторную аутентификацию (подробнее в статье).

- **Превышен лимит лицензии**. Данная сессия заблокирована. Появляется, если превышено количество пользователей по лицензиям или у пользователя уже есть пять активных сессий.

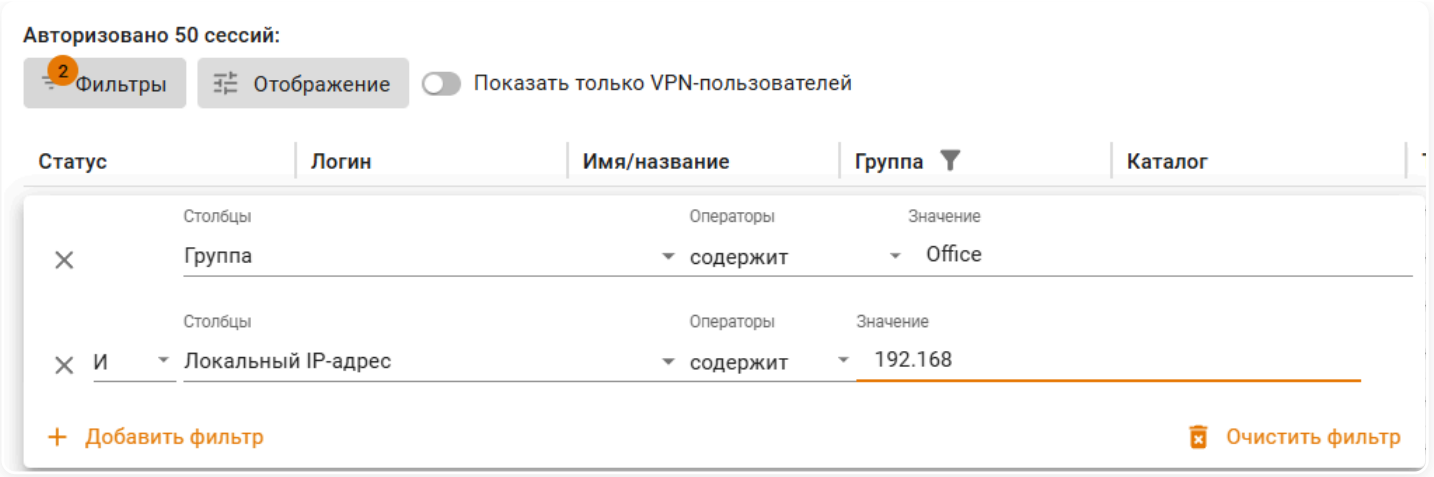
- **Сессия удаляется**. Появляется при разрыве сессии с динамическим IP-адресом. Сессия с таким статусом будет удалена через 30 секунд.

Для просмотра результата проверки устройства, подключенного через Ideco Client, нажмите на **Результат** в столбце **Последняя проверка**. Откроется соответствующее окно с общей информацией и результатами проверок по HIP-объектам:



Фильтрация таблицы

При наличии большого количества авторизованных пользователей в таблице воспользуйтесь кнопкой **Фильтры**. Фильтрация данных возможна по всем столбцам, а также с использованием нескольких переменных:



При использовании фильтра по **Времени подключения** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные за 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

Опция **Показать только VPN-пользователей** отображает в таблице журнала только тех пользователей, которые подключены к NGFW через VPN.

Полезные ссылки

- **Авторизация пользователей**

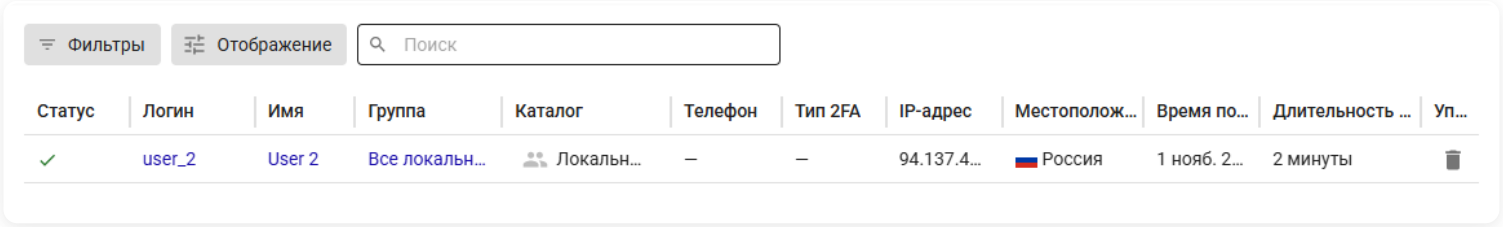
Сессии ЛК

Классический контекст | Высокопроизводительный контекст | API

Сессии ЛК - таблица активных сессий в личном кабинете Ideco NGFW Novum. Для аутентификации пользователей используется логин и пароль, возможно использование технологии 2FA (двухфакторная аутентификация). Доступ к ресурсам в локальной сети пользователи получают через веб-браузер по HTTPS без установки отдельного туннельного соединения (технология SSL VPN).

Записи в журнале появляются после авторизации пользователей в личном кабинете, настроенном в **Сервисы** → **ЛК/Портале SSL VPN**.

Записи доступны для управления и остаются в таблице до завершения сессии:



Помимо общих сведений об учетной записи пользователя (логин, имя, группа, каталог и телефон), таблица активных сессий содержит столбцы:

- **Статус** - доступные значения: авторизован, 2FA (ожидает 2FA, генерация TOTP для прохождения 2FA).
- **Тип 2FA** - метод двухфакторной аутентификации.
- **IP-адрес** - IP-адрес, с которого произведена начальная аутентификация сессии в ЛК.
- **Местоположение** - страна IP-адреса, с которого произведена начальная аутентификация сессии в ЛК. Значение пустое, если:
  - Отсутствует лицензия.
  - Невозможно получить базу GeoIP.
  - IP-адрес локальный.
- **Время подключения** - момент аутентификации в ЛК с указанием даты в формате день/месяц/год и времени в формате час/минута.
- **Время в сети** - длительность сессии аутентификации в ЛК, разница между временем подключения и текущим временем.
- **Управление** - доступно только действие **Отключить** для завершения сессии аутентификации.

IP-адрес и **Местоположение** могут меняться, т.к. сессия авторизации привязана к cookie и браузеру, а не к IP-адресу.

Столбцы в таблице можно отрегулировать кнопкой **Отображение**.

Чтобы найти нужную сессию, воспользуйтесь одним из способов:

- Нажмите кнопку **Фильтры**, выберите один из параметров поиска.

При использовании фильтра по **Времени подключения** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные за 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Графики загруженности

Классический контекст | Высокопроизводительный контекст

Модуль **Графики загруженности** позволяет просматривать данные о состоянии Ideco NGFW Novum в виде графиков в **режиме реального времени**. Горизонтальной шкалой графика всегда является **время** (в зависимости от выбранного интервала). Данные хранятся до 90 дней.

В случае активации резервной ноды кластера, данные с прежней активной ноды остаются доступными (хранятся 90 дней), но не передаются резервной ноде.

При отключении опции **Сбор метрик** в некоторых графиках может наблюдаться несогласованность данных по времени. Это связано с внутренней реализацией модуля.

Раздел **Графики загруженности** состоит из вкладок:

Система

Содержит информацию:

- Количество авторизованных пользователей.
- Процент загрузки процессора (максимальное значение загрузки процессора - 100%).
- Температура процессора.
- Частота процессора.
- Объем используемой оперативной памяти в ГБ.
- Среднее значение загрузки системы.
- Количество всех установленных сетевых соединений.

Сеть

Содержит суммарную информацию о входящем и исходящем трафике, передаваемом через Ideco NGFW по всем интерфейсам раздела Сетевые интерфейсы. Данные отображаются за определенный период времени.

Эта статистика может помочь в настройке резервирования каналов и балансировки.

Диски

Содержит информацию об общей загруженности системного диска (в процентах) и свободном месте в корневой файловой системе (в ГБ) за определенный промежуток времени. Дает оценку интенсивности использования диска.

Информация о свободном и занятом объеме на диске также отображается при создании бэкапа в **Управление сервером → Бэкапы**.

VPN

Содержит информацию о количестве подключений пользователей по протоколам L2TP/IPsec, SSTP, IKEv2 и Ideco Client.
Инструкция по VPN-подключению пользователей доступна по ссылке.

IPsec

Содержит информацию о входящих, исходящих IPsec-подключениях Ideco NFGW. Показывает загрузку входящего и исходящего IPsec-канала.

WCCP GRE

Содержит информацию о входящей скорости GRE-туннелей.
Особенности протокола GRE не позволяют определить исходящую скорость для GRE-туннелей.

ГОСТ VPN

Содержит информацию о входящих и исходящих соединениях ГОСТ VPN в Ideco NFGW. Отображает график входящего и исходящего трафика за выбранный период времени.

Инструкция по настройке ГОСТ VPN доступна по ссылке.

VCE

Содержит информацию о загруженности всех VCE, для которых были назначены ресурсы (ядра процессора и оперативная память).

Инструкция по настройке VCE доступна по ссылке.

Полезные ссылки

- **Сетевые интерфейсы**
- **Профили next hop**
- **Кластеризация**
- **Бэкапы**
- **ГОСТ VPN**
- **Инструкции по созданию VPN-подключений**

Монитор трафика

Классический контекст | Высокопроизводительный контекст | API

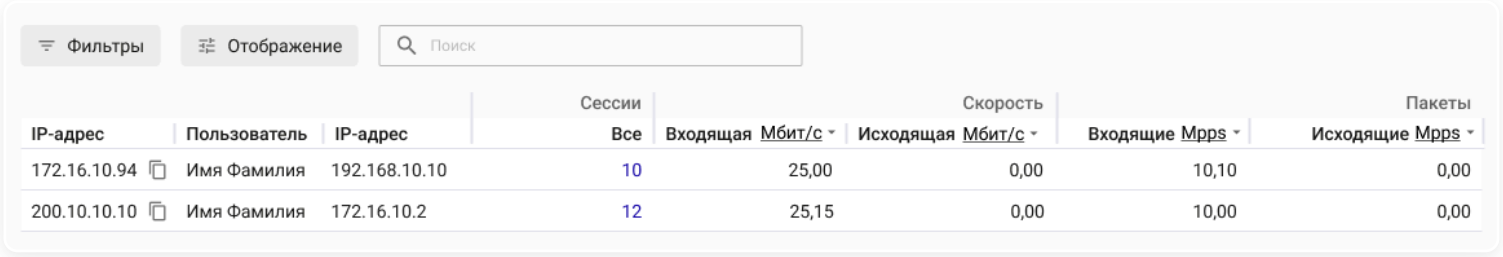
В разделе **Мониторинг → Монитор трафика** можно просматривать данные о трафике (входящая/исходящая скорость, количество сессий), проходящем через Ideco NGFW Novum в режиме реального времени.

Для работы **Монитора трафика** необходимо включить Контроль приложений.

Раздел **Монитор трафика** состоит из вкладок:

По источнику трафика

Вкладка **По источнику трафика** позволяет отслеживать активность пользователей сети и выявлять пользователей, нагружающих канал трафиком:



IP-адрес	Пользователь	IP-адрес	Сессии: Все	Скорость: Входящая Мбит/с	Скорость: Исходящая Мбит/с	Пакеты: Входящие Mpps	Пакеты: Исходящие Mpps
172.16.10.94	Имя Фамилия	192.168.10.10	10	25,00	0,00	10,10	0,00
200.10.10.10	Имя Фамилия	172.16.10.2	12	25,15	0,00	10,00	0,00

Для просмотра информации об активности определенного узла локальной сети нажмите на количество сессий в столбце **Сессии**:

Откроется таблица с подробной информацией:

По приложениям

Вкладка **По приложениям** позволяет отслеживать активность приложений.

Например, если пользователь не загружает канал трафиком, но в таблице **По источнику трафика** присутствует большое количество пакетов данных, то на вкладке **По приложениям** можно выявить приложение с подозрительной активностью:

Для просмотра информации об активности определенного приложения нажмите на **количество сессий** в столбце **Сессии**:

Откроется таблица с подробной информацией:

Фильтрация таблицы

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**. Фильтрация возможна по всем столбцам, кроме **Сессии**, **Скорость** и **Объект**, а также с использованием нескольких переменных.

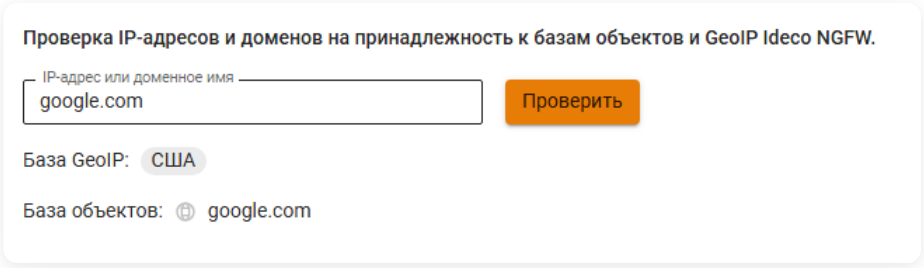
Полезные ссылки

- **Контроль приложений**

Проверка IP/домена

Классический контекст | Высокопроизводительный контекст | API

В разделе можно проверить IP-адрес или домен на принадлежность к базам объектов и GeoIP. Для проверки введите IP-адрес или доменное имя в поиск. Система проверяет в базах объектов и GeoIP. В результатах поиска отображается:



- Страна регистрации.
- Объект, где указан IP-адрес или доменное имя.

Блокировки WAF

Классический контекст | Высокопроизводительный контекст | API

Раздел содержит сведения о текущих IP-адресах, заблокированных правилами Web Application Firewall (WAF). Таблица обновляется каждые 5 секунд:

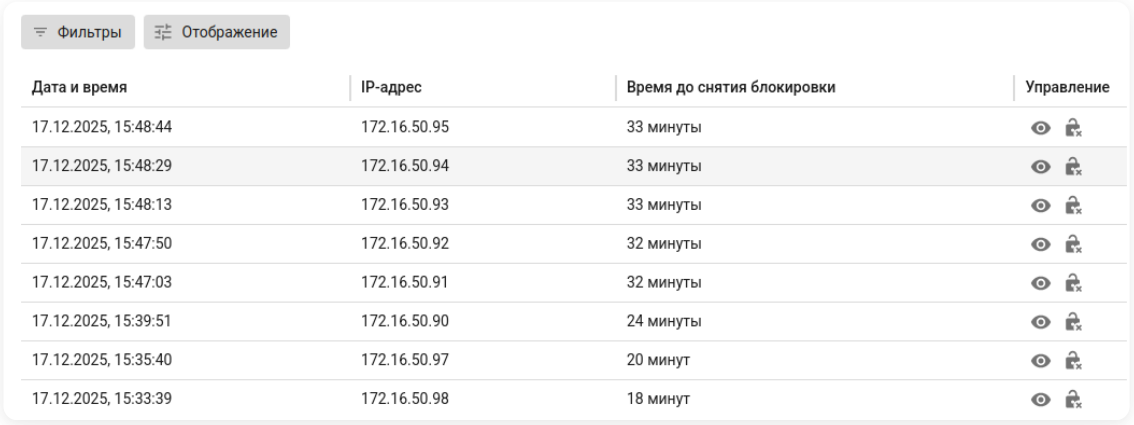


Таблица содержит столбцы:

- **Дата и время** - момент фиксации события блокировки в формате `31 октября 2025, 21:18`.
- **IP-адрес** - заблокированный IP-адрес.
- **Время до снятия блокировки** - оставшийся интервал до автоматического удаления записи из списка в формате `5 минут 35 секунд`.
- **Управление** - доступные действия:
  - - переход к соответствующей записи в журнале События безопасности. При переходе в журнал отображается только запись, вызвавшая блокировку.
  - - снятие блокировки с выбранного IP-адреса. IP-адреса, разблокированные вручную, удаляются из таблицы сразу после снятия блокировки.

IP-адреса, заблокированные WAF, помещаются в список на 40 минут. По истечении этого времени блокировка снимается автоматически и запись удаляется.

Сброшенные ранее блокировки будут восстановлены после перезагрузки NGFW Novum, если критерии блокировки по-прежнему выполняются.

Telegram-бот

Классический контекст | Высокопроизводительный контекст

Ideco Monitoring Bot - это Telegram-бот, который отправляет уведомления о событиях в Ideco NGFW Novum (уведомления из 🔔):

- В личные сообщения.
- В беседы, где два и более участников (groups).

Привязка бота и настройка оповещений Ideco Monitoring Bot осуществляется в MY.IDECO.

Привязка Ideco Monitoring Bot

К личному аккаунту

1. Откройте чат с ботом: @ideco_monitor_bot.
2. Напишите боту `/start`.
3. Скопируйте код привязки к аккаунту.
4. Перейдите в раздел **Ideco Monitoring Bot** в MY.IDECO.
5. Нажмите **Привязать аккаунт**.
6. Введите код в поле **Токен Telegram-аккаунта** и нажмите **Привязать**:



Уведомления начнут приходить в Telegram-аккаунт.

К беседе



При подключении Ideco Monitoring Bot к беседе нельзя использовать подсказки для команд, поскольку требуется ввод команды `/start` вручную.

1. Перейдите в группу в Telegram и добавьте бота: @ideco_monitor_bot.
2. Напишите `/start` в группе.
3. Скопируйте код привязки к аккаунту.
4. Перейдите в раздел **Ideco Monitoring Bot** в MY.IDECO.
5. Нажмите **Привязать аккаунт**.
6. Введите код в поле **Токен Telegram-аккаунта** и нажмите **Привязать**:



Уведомления начнут приходить в Telegram-аккаунт.

Настройка оповещений Ideco Monitoring Bot

В личном кабинете можно настроить оповещения от Ideco Monitoring Bot для каждого привязанного аккаунта или беседы. Для настройки оповещений:

1. Перейдите в раздел **Ideco Monitoring Bot** в MY.IDECO.
2. Выберите аккаунт или группу и нажмите 🔔.
3. Выберите уведомления, которые хотели бы получать.

Если требуется временно отключить отправку уведомлений, нажмите на  . Оповещения перестанут приходить, пока снова не нажмете на эту иконку.

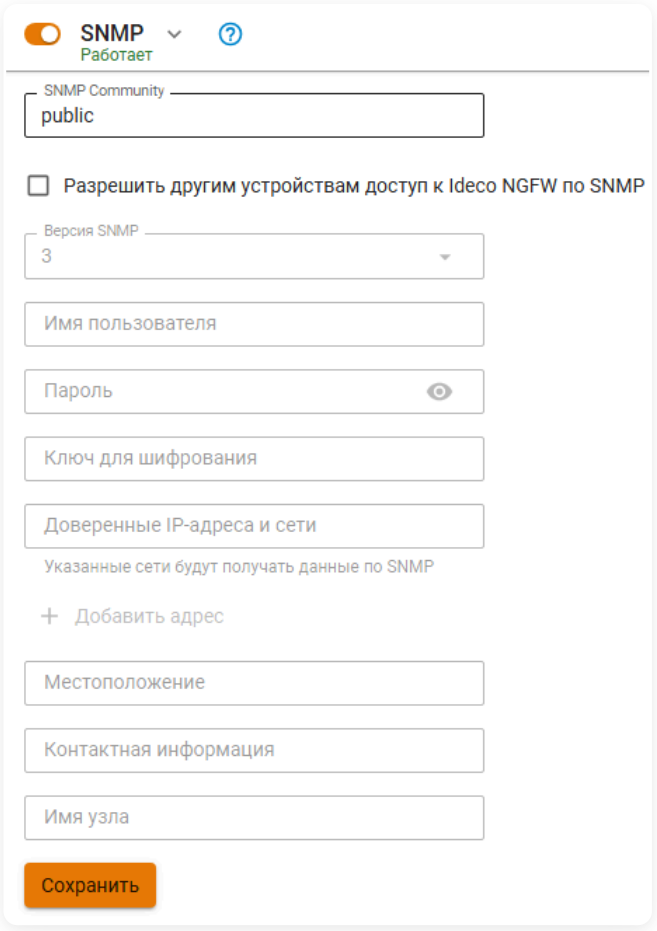
SNMP

Классический контекст | Высокопроизводительный контекст | API

SNMP - это протокол для управления и мониторинга сетевых устройств, таких как маршрутизаторы, коммутаторы и межсетевые экраны. Модуль **SNMP** обеспечивает мониторинг работы Ideco NGFW Novum по протоколу SNMP версий 1/2c и 3.

Настройка подключения

Для подключения по протоколу SNMP в **Мониторинг** → **SNMP** включите опцию и заполните поля:



Версия 1/2c

- **Имя пользователя**.
- **Пароль** (минимальное количество символов - 8).
- **Доверенные IP-адреса и сети**.

Поля **Местоположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.

Версия 3

- **Имя пользователя**.
- **Пароль** (минимальное количество символов - 8).
- **Ключ шифрования**.
- **Доверенные IP-адреса и сети**.

Поля **Местоположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.

Рекомендуем: укажите на сервере, с которым будет установлено соединение по SNMPv3, алгоритмы **Auth Algorithm MD5** и **Crypto Algorithm AES**.

Поле **SNMP community** для SNMPv3 необязательно для заполнения.

Устройства в указанных доверенных сетях получат доступ к данным Ideco NGFW Novum после заполнения поля **Доверенные IP-адреса и сети**.

Как узнать информацию о MIB (Management Information Base)

MIB (Management Information Base) - иерархическая база данных, содержащая описание управляемых объектов сетевого устройства, доступных для мониторинга и управления через протокол SNMP.

После настройки подключения по протоколу SNMP в директории `/usr/share/snmp/mibs/` будут размещены MIB-файлы с описанием всех MIB-модулей.

Список MIB-файлов

- AGENTX-MIB.txt
- IANAifType-MIB.txt
- IPV6-MIB.txt
- NET-SNMP-PASS-MIB.txt
- SMUX-MIB.txt
- SNMP-USM-AES-MIB.txt
- TCP-MIB.txt
- BRIDGE-MIB.txt
- IANA-LANGUAGE-MIB.txt
- IPV6-TCP-MIB.txt
- NET-SNMP-TC.txt
- SNMP-COMMUNITY-MIB.txt
- SNMP-USM-DH-OBJECTS-MIB.txt
- TRANSPORT-ADDRESS-MIB.txt
- DISMAN-EVENT-MIB.txt
- IANA-RTPROTO-MIB.txt
- IPV6-TC.txt
- NET-SNMP-VACM-MIB.txt
- SNMP-FRAMEWORK-MIB.txt
- SNMP-USM-HMAC-SHA2-MIB.txt
- TUNNEL-MIB.txt
- DISMAN-SCHEDULE-MIB.txt
- IF-INVERTED-STACK-MIB.txt
- IPV6-UDP-MIB.txt
- NETWORK-SERVICES-MIB.txt
- SNMP-MPD-MIB.txt
- SNMPv2-CONF.txt
- UCD-DEMO-MIB.txt
- DISMAN-SCRIPT-MIB.txt
- IF-MIB.txt
- LM-SENSORS-MIB.txt
- NOTIFICATION-LOG-MIB.txt
- SNMP-NOTIFICATION-MIB.txt
- SNMPv2-MIB.txt
- UCD-DISKIO-MIB.txt
- EtherLike-MIB.txt
- INET-ADDRESS-MIB.txt
- MTA-MIB.txt
- RFC1155-SMI.txt
- SNMP-PROXY-MIB.txt
- SNMPv2-SMI.txt
- UCD-DLMOD-MIB.txt

- HCNUM-TC.txt
- IP-FORWARD-MIB.txt
- NET-SNMP-AGENT-MIB.txt
- RFC1213-MIB.txt
- SNMP-TARGET-MIB.txt
- SNMPv2-TC.txt
- UCD-IPFWACC-MIB.txt
- HOST-RESOURCES-MIB.txt
- IP-MIB.txt
- NET-SNMP-EXAMPLES-MIB.txt
- RFC-1215.txt
- SNMP-TLS-TM-MIB.txt
- SNMPv2-TM.txt
- UCD-SNMP-MIB.txt
- HOST-RESOURCES-TYPES.txt
- IPV6-FLOW-LABEL-MIB.txt
- NET-SNMP-EXTEND-MIB.txt
- RMON-MIB.txt
- SNMP-TSM-MIB.txt
- SNMP-VIEW-BASED-ACM-MIB.txt
- UDP-MIB.txt
- IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt
- IPV6-ICMP-MIB.txt
- NET-SNMP-MIB.txt
- SCTP-MIB.txt
- SNMP-USER-BASED-SM-MIB.txt
- SQUID-MIB.txt

Каждый MIB-файл написан на специальном языке описания SMI (Structure of Management Information). Этот синтаксис формализован и не всегда человекочитаем. Для удобного просмотра дерева MIB подставьте имя файла без расширения в URL сайта с визуализацией - https://mibs.observium.org/, например:

- https://mibs.observium.org/mib/IF-MIB
- https://mibs.observium.org/mib/SNMP-USER-BASED-SM-MIB
- https://mibs.observium.org/mib/TCP-MIB

Более подробную информацию о конкретном MIB-объекте можно получить через поиск. Можно искать как по имени объекта (например: `sysUpTime`), так и по его числовому OID (например: `.1.3.6.1.2.1.1.3`).

Полезные ссылки

- **Как подключить Ideco NGFW к Zabbix Server по SNMP**

Zabbix-агент

Классический контекст | Высокопроизводительный контекст | API

Zabbix - система с открытым исходным кодом для мониторинга параметров сети, состояния и работоспособности серверов.

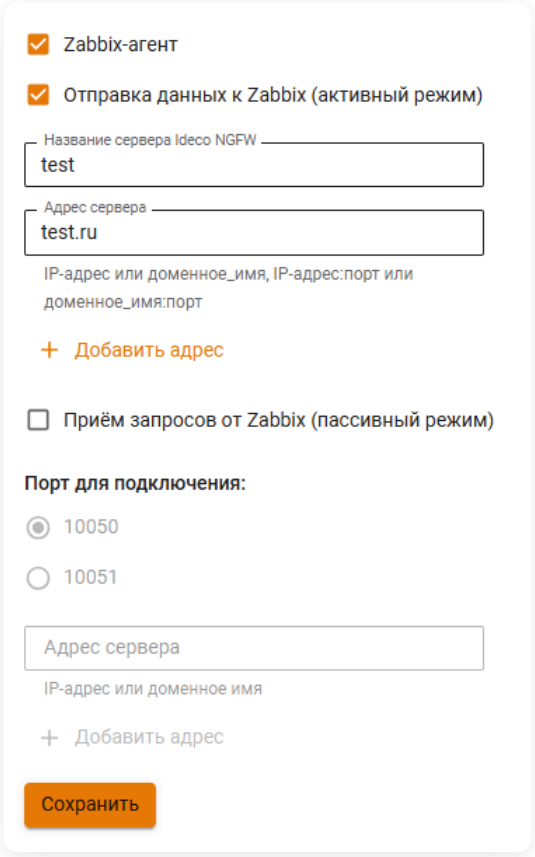
Настройка Zabbix-агента

Для работы системы мониторинга Zabbix в Ideco NGFW Novum активируйте опцию **Zabbix-агент** после настройки интеграции с Zabbix.

Интеграция с системой мониторинга Zabbix возможна в двух режимах: **Активный** и **Пассивный**.

Активный

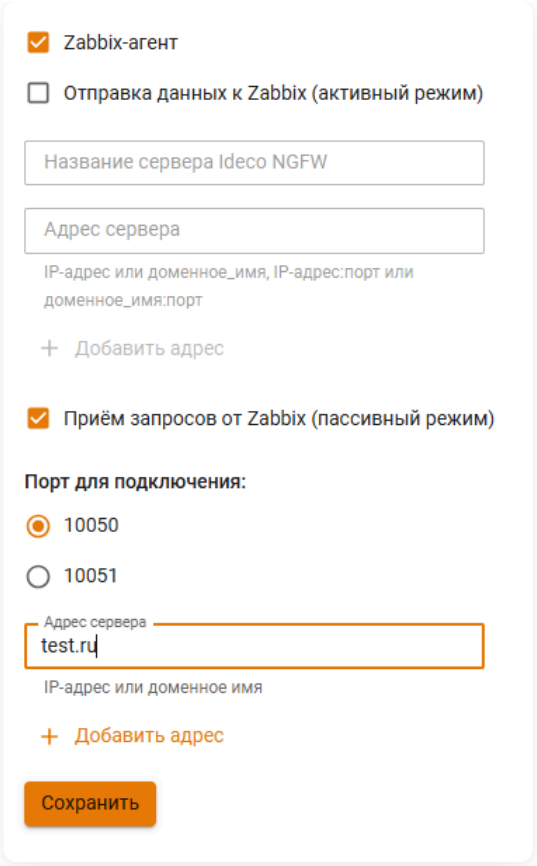
Соединение с Zabbix-сервером происходит со стороны Ideco NGFW Novum. Для настройки заполните поля:



- **Имя сервера Ideco NGFW Novum** - имя, которое будет отображаться на сервере мониторинга.
- **Адрес сервера** - IP-адрес, доменное имя, либо `IP-адрес:порт`, `доменное имя:порт`, если используется нестандартный для Zabbix входящий порт. Для добавления еще одного адреса нажмите **Добавить адрес**.

Пассивный

Подключение происходит со стороны Zabbix-сервера. Для настройки заполните поля:



- **Порт для подключения** - выберите 10050 или 10051 порт.
- **Адрес сервера** - IP-адрес или доменное имя Zabbix-сервера. Для добавления еще одного адреса нажмите **Добавить адрес**.

Zabbix-сервер должен находиться внутри локальной сети Ideco NGFW Novum. Подключение мониторинга возможно только к локальным интерфейсам (с ролью LAN). Это ограничение обусловлено системными правилами **Межсетевого экрана**, которые не отображаются в веб-интерфейсе, но имеют наивысший приоритет. Системные правила разрешают соединения на порты 10050/TCP и 10051/TCP только на локальных интерфейсах и блокируют их на внешних.

Используйте стандартные шаблоны Zabbix для Linux:

- **Linux by Zabbix agent** - для пассивного режима.
- **Linux by Zabbix agent active** - для активного режима.

Zabbix-агент передает стандартный набор метрик, предусмотренный шаблоном Zabbix для Linux. В набор входят данные по процессору, памяти, дискам, файловым системам, сетевым интерфейсам и основным системным параметрам. Количество метрик зависит от количества интерфейсов и дисков.

Полезные ссылки

- **Официальная страница Zabbix**
- **Zabbix как готовое решение**
- **Установка Zabbix**
- **Как подключить Ideco NGFW к Zabbix Server по SNMP**

Правила трафика

В разделе описывается настройка служб, определяющих основные правила фильтрации трафика в Ideco NGFW.

Межсетевой экран

Создание правил Межсетевого экрана, применение профилей безопасности, тестирование правил, настройка предварительной и аппаратной фильтрации

Перейти >

Контент-фильтр

Создание правил Контент-фильтра, пользовательских категорий, морфологический анализ

Перейти >

Ограничение скорости

Настройка ограничения скорости входящего интернет-трафика для пользователей сети

Перейти >

Предотвращение вторжений

Описание групп сигнатур, создание пользовательских сигнатур

Перейти >

Исключения

Настройка исключений для предотвращения обработки трафика в разделах **Предотвращения вторжений**, **Контроля приложений** и **Ограничение скорости**

Перейти >

Объекты

Создание объектов для использования в правилах **Межсетевого экрана**, **Контент-фильтра**, **Контроля приложений**, **Маршрутизации**

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Межсетевой экран

Классический контекст | Высокопроизводительный контекст | API

Для настройки Межсетевого экрана перейдите в раздел Правила трафика → Межсетевой экран.

Название службы раздела **Межсетевой экран**: `ideco-firewall-rest`, `ideco-firewall-backend`, `ideco-apply-manual-blocklist`, `ideco-fw-stats`, `ideco-acl-rest`, `ideco-acl-backend`, `ideco-nflog`.

Список служб для других разделов доступен по ссылке.

Межсетевой экран - средство управления трафиком на сервере (межсетевой экран). Поддерживает фильтрацию пакетов с контролем состояния соединений (Stateful Inspection) - решение о блокировке принимается на все соединение.

Межсетевой экран анализирует заголовки IP-пакетов и TCP-сегментов, проходящих через интерфейсы сервера, и фильтрует трафик на основании параметров заголовков (IP-адреса, TCP/UDP-порты и IP-протокол).

С помощью **Межсетевого экрана** можно создавать наборы правил, которые разграничивают трафик между различными сетями: локальными, VPN и публичными (интернет). В Ideco NGFW Novum предусмотрены преднастроенные и автоматически включаемые системные правила. Пользовательские правила используются для фильтрации трафика локальной сети и публикации ресурсов.

Рекомендуем выпускать весь пользовательский трафик через Ideco NGFW для оптимальной работы политик безопасности (модулей **Контроль приложений** и **Предотвращение вторжений**).

Межсетевой экран не предназначен для решения задач контроля доступа к ресурсам по URL, доменному имени или типу контента на веб-сайтах. Эти задачи решаются с помощью **Контент-фильтра**.

Фильтрация трафика

Межсетевой экран использует для фильтрации трафика как отдельные интерфейсы, так и зоны - логические объединения сетевых интерфейсов. Преимущества такого подхода:

- Гибкость управления правилами при большом количестве интерфейсов.
- Упрощение процесса добавления/удаления интерфейсов без необходимости редактирования множества правил.
- Возможность выбора удобных названий для зон (например, **Разработчики**, **Гости**), что делает правила более читаемыми.

Для работы DPI/IPS в правилах **Межсетевого экрана** можно подключить **Профили безопасности**, создав разрешающее правило с включенной проверкой через **Контроль приложений**, систему **Предотвращения вторжений** . Профили настраиваются в разделе **Профили безопасности**.

Настройка и управление правилами

Настройка производится в **Правила трафика** → **Межсетевой экран**. На вкладках раздела добавляются правила управления трафиком, которые отображаются в таблицах **Межсетевого экрана**. При наличии большого количества правил используйте кнопку **Фильтры**.

Включите опцию **Счетчик срабатываний** для подсчета количества срабатываний правил **Межсетевого экрана**. После включения опции в таблице появится соответствующий столбец.

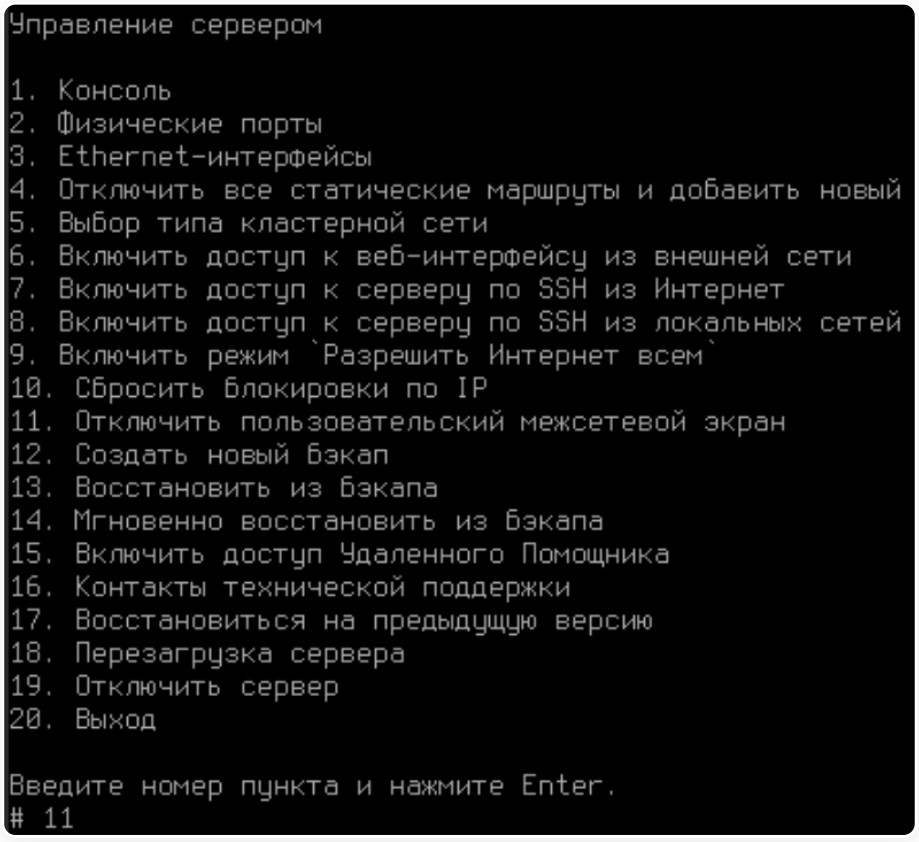
Включить опцию можно, нажав на **Отображение данных**.

Особенности

- Включение режима удаленного помощника изменяет таблицу правил **Межсетевого экрана**, разрешая подключение по SSH из локальных и внешних сетей.
- В Ideco NGFW Novum включены connection tracking helpers для протоколов: ftp, sip, netbios-ns, pptp, h323. Для других протоколов, использующих несколько портов при установлении соединения, работа через NAT не гарантируется.
- При использовании зон в **Межсетевом экране** следует учесть, что одна зона не может содержать более 64 интерфейсов, настроенных в разделе **Сервисы** → **Сетевые интерфейсы**, а также IPsec- и VPN-подключений.

Устранение проблем

В случае создания некорректных правил (например, запрет доступа в веб-интерфейс Ideco NGFW) в локальном меню сервера выберите пункт **Отключить пользовательский межсетевой экран** и нажмите Enter:



При отключении пользовательского межсетевого экрана в веб-интерфейсе системные правила продолжают работу.

Полезные ссылки

- **Таблицы межсетевого экрана (FORWARD, DNAT, INPUT и SNAT)**
- **Примеры создания правил межсетевого экрана**
- **Логирование**
- **Аппаратная фильтрация**
- **Тестирование правил**
- **Предварительная фильтрация**
- **Доступ из внешних сетей без NAT**
- **Блокировка популярных ресурсов**
- **Как разрешить доступ к ресурсам в ограниченной сети**
- **Портмаппинг (проброс портов, DNAT)**
- **Настройка совместной работы ViPNet Координатор с Ideco NGFW**

Профили безопасности

- **Контроль приложений**
- **Предотвращение вторжений**

Таблицы межсетевого экрана (FORWARD, DNAT, INPUT и SNAT)

Классический контекст | Высокопроизводительный контекст

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Для удобства управления в интерфейсе правила разбиты на четыре таблицы:

- **FORWARD** - правила действуют на трафик, проходящий между зонами сервера, т. е. интернетом и локальной сетью, а также между локальными сетями. Это основная таблица, в которую можно добавить правила, ограничивающие трафик пользователей.
- **DNAT** - правила используются для прямого перенаправления портов с внешней зоны на ресурсы во внутренней зоне. Такие правила часто называются правилами проброса портов (port forwarding, port-mapping).
- **INPUT** - правила входящего на сервер трафика. Как правило, это трафик для служб самого Ideco NGFW Novum (например, DNS, DHCP, работающие на Ideco NGFW Novum).
- **SNAT** - правила для управления трансляцией сетевых адресов.

Правила в таблицах имеют приоритет сверху вниз (т. е. **верхнее правило приоритетнее нижнего**).

По умолчанию используется политика **РАЗРЕШИТЬ**. Если не созданы запрещающие правила, все порты и протоколы для пользователей разрешены.

При наличии большого количества правил в таблицах **Межсетевого экрана** воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Создание правил

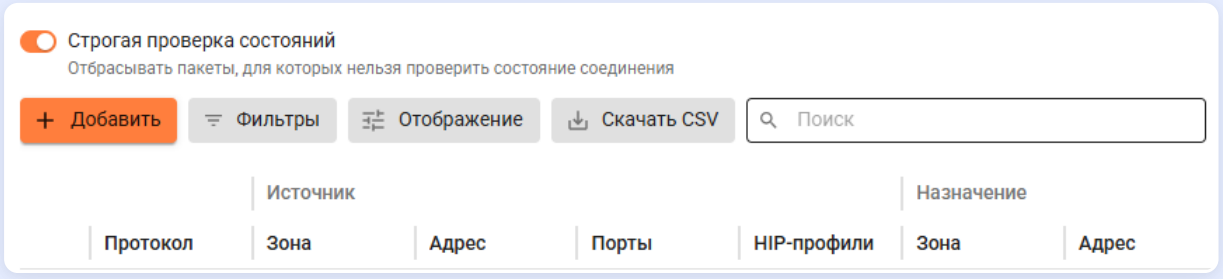
1. В нужной таблице нажмите кнопку **Добавить**.

2. Укажите необходимые параметры, действия правила и нажмите кнопку **Добавить**.

Правило будет добавлено в конец списка. Если необходимо, измените приоритет правила кнопками ↑ и ↓.

FORWARD

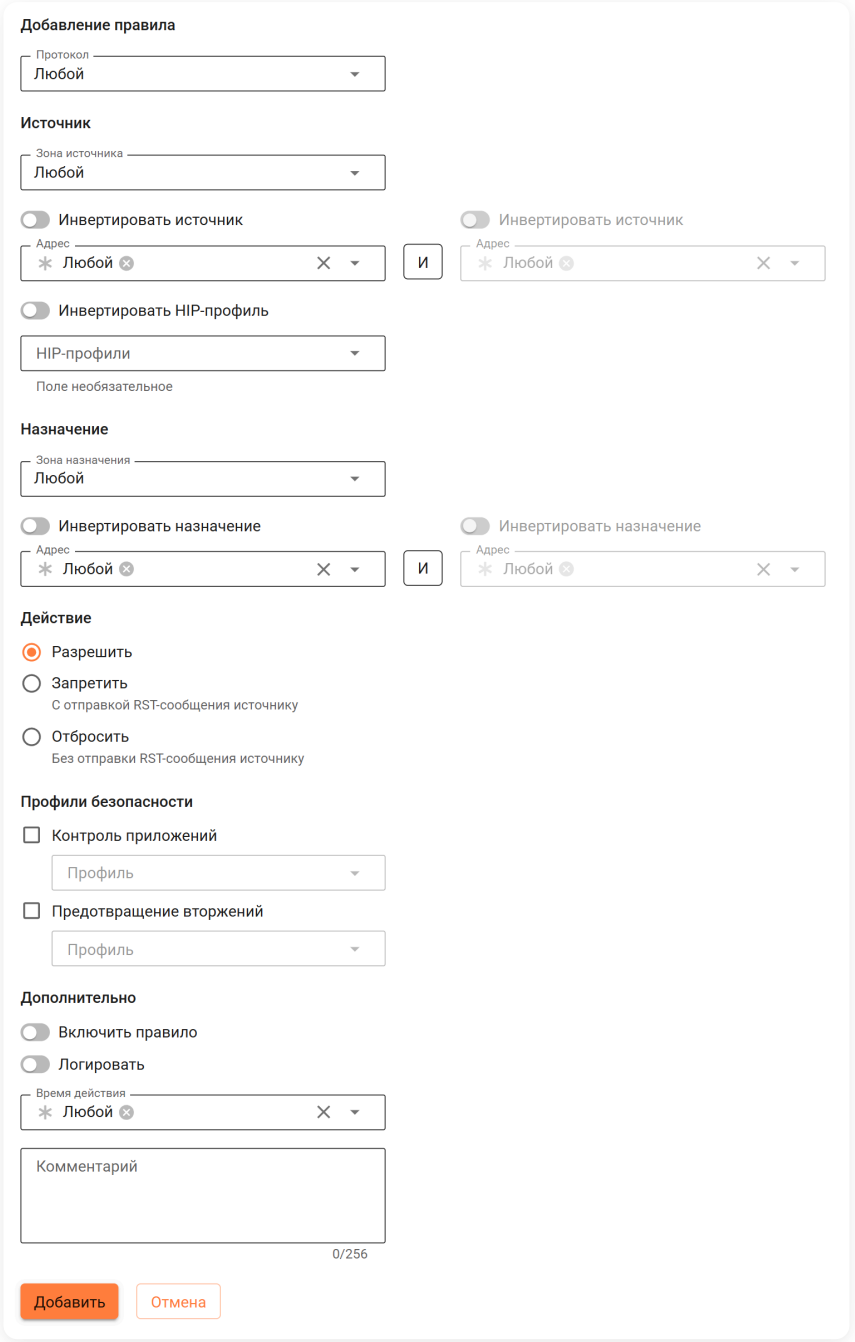
В FORWARD доступна опция **Строгая проверка состояний** (по умолчанию включена):



При включенной опции пакеты, для которых нельзя проверить состояние соединения (со статусом `INVALID`), отбрасываются системным правилом.

Отключение опции снижает уровень защиты, так как система начинает обрабатывать поврежденные, поддельные или не соответствующие логике сетевых протоколов пакеты, которые подсистема отслеживания соединений пометила статусом `INVALID`.

Если в сети используется асимметричная маршрутизация и наблюдаются проблемы с прохождением трафика, отключите опцию **Строгая проверка состояний**. Для устранения причины асимметричной маршрутизации воспользуйтесь инструкцией.



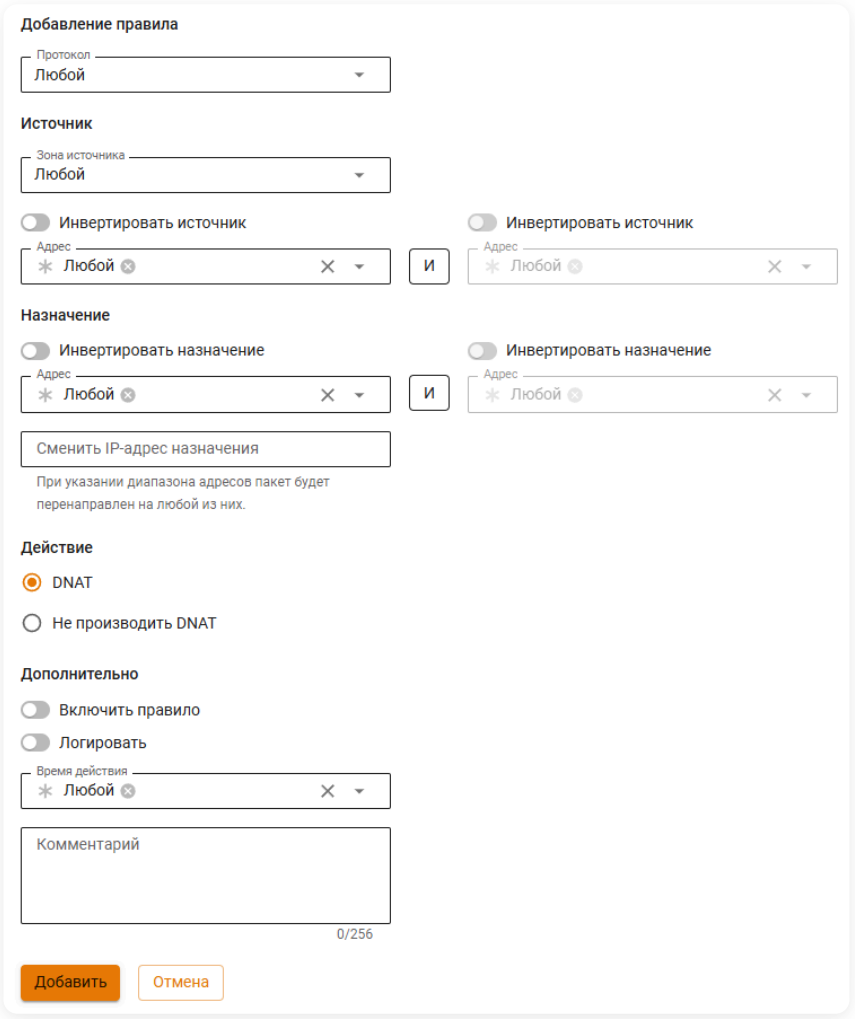
Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.

- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
- **Инвертировать HIP-профиль** - позволяет использовать в правиле все объекты, кроме выбранных в поле **HIP-профили**.
- **HIP-профили** - профиль, соответствующий устройству, от которого исходит трафик.

- **Назначение**:
  - **Зона назначения** - интерфейс или группа интерфейсов, в которые входит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действия**:
  - **Разрешить** - разрешает трафик или направляет трафик в модули фильтрации трафика.
  - **Запретить** - запрещает трафик с отправкой RST-сообщения источнику. Рекомендуем использовать запрет с отправкой RST, так как это позволяет клиенту немедленно завершить попытку соединения, избежать долгих таймаутов и облегчает диагностику.
  - **Отбросить** - запрещает трафик без отправки RST-сообщения источнику.
- **Профили безопасности**:
  - **Контроль приложений** - выберите профиль Контроля приложений, которым требуется фильтровать трафик.
  - **Предотвращение вторжений** - выберите профиль системы Предотвращения вторжений, которым требуется фильтровать трафик.
- **Дополнительно**:
  - **Включить правило** - включите правило. По умолчанию правило выключено.
  - **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
  - **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

DNAT



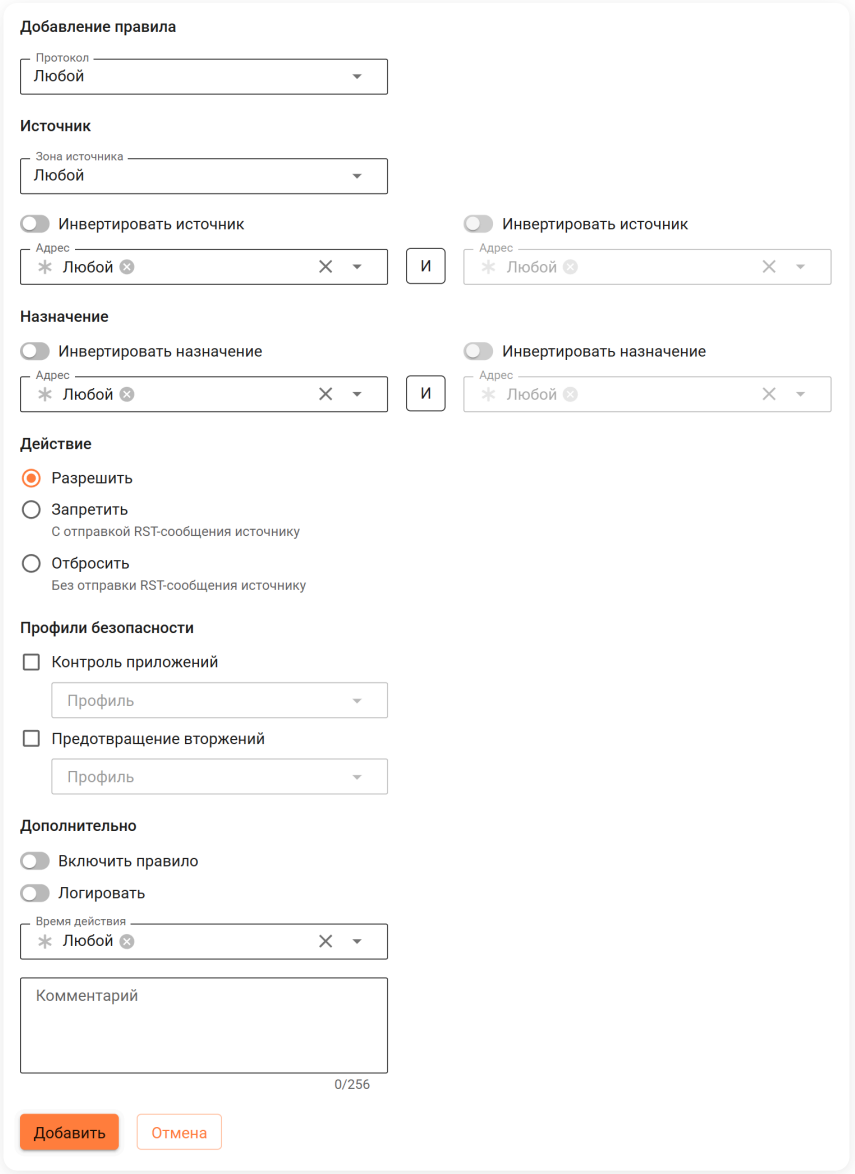
Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
  - **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
- **Назначение**:
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
  - **Сменить IP-адрес назначения** - при указании диапазона адресов пакет будет перенаправлен на любой из них. Диапазон задается в формате `<начальный_IP>-<конечный_IP>`. Например, `192.168.1.1-192.168.1.2`. Выбор конкретного адреса для перенаправления осуществляется по алгоритму **round-robin**: адреса используются последовательно - от первого к последнему, после чего цикл повторяется.

- **Сменить порт назначения** - при указании диапазона портов пакет будет перенаправлен в порт с тем же номером, на который пришел пакет, если этот порт попадает в указанный диапазон.

- **Действие**:
  - **DNAT** - транслирует адреса назначения, перенаправляя входящий трафик. В поле **Сменить IP-адрес назначения** укажите один IP-адрес или диапазон (при указании диапазона IP-адресов пакет будет перенаправлен на любой из них). Если при создании правила были указаны протоколы TCP или UDP, то появится поле **Сменить порт назначения**. Укажите порт, на который будет перенаправлен трафик.
  - **Не производить DNAT** - отменяет действие **DNAT** для трафика, удовлетворяющего критериям правила.
- **Дополнительно**:
  - **Включить правило** - включите правило. По умолчанию правило выключено.
  - **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
  - **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

INPUT



Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене их IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.

- **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.

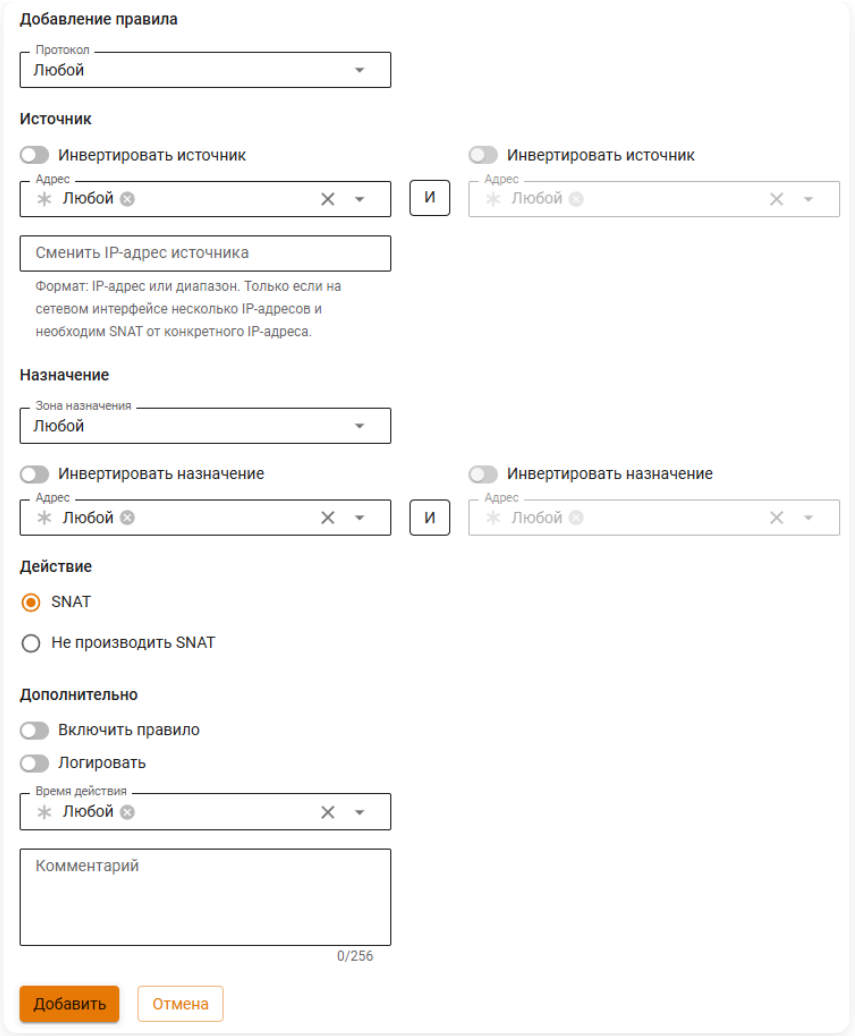
- **Назначение**:
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене их IP-адресов, межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порт назначения** - указывается при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действие**:
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
  - **Запретить** - запрещает трафик с отправкой RST-сообщения источнику. Рекомендуем использовать запрет с отправкой RST, так как это позволяет клиенту немедленно завершить попытку соединения, избежать долгих таймаутов и облегчает диагностику.
  - **Отбросить** - запрещает трафик без отправки RST-сообщения источнику.
- **Профили безопасности**:
  - **Контроль приложений** - выберите профиль **Контроля приложений**, которым требуется фильтровать трафик.
  - **Предотвращение вторжений** - выберите профиль системы **Предотвращения вторжений**, которым требуется фильтровать трафик.
- **Дополнительно**:
  - **Включить правило** - включите правило. По умолчанию правило выключено.
  - **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
  - **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

SNAT

> Правила автоматического **SNAT** работают только для интерфейсов, указанных как внешние.

Чтобы активировать автоматический **SNAT** для локальных сетей, включите опцию **Автоматический SNAT локальных сетей**. Автоматический **SNAT** подменяет адреса источников только для диапазонов: `192.168.0.0/16`, `172.16.0.0/12` и `10.0.0.0/8`.

Чтобы подменять адреса источников из других диапазонов, создайте соответствующее **SNAT** правило. Чтобы допустить устройства в сеть без сетевой трансляции адресов (правилом "не SNAT"), создайте правило **SNAT** с настройкой **Не производить SNAT**.



Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
  - **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
  - **Сменить IP-адрес источника** - заполняется, только если на сетевом интерфейсе несколько IP-адресов и необходим **SNAT** от конкретного IP-адреса. Можно указать IP-адрес или диапазон IP-адресов, например, 192.168.10.2-192.168.10.15.
- **Назначение**:
  - **Зона назначения** - интерфейс или группа интерфейсов, в которые входит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действия**:
  - **SNAT** - транслирует адреса источника.
  - **Не производить SNAT** - отменяет действие **SNAT** для трафика, удовлетворяющего критериям правила.
- **Дополнительно**:

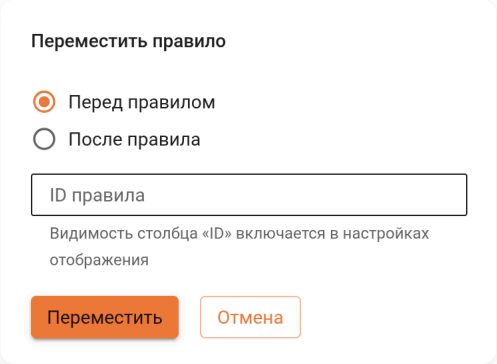
- **Включить правило** - включите правило. По умолчанию правило выключено.
- **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
- **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
- **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

Перемещение правил

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Использование профилей безопасности

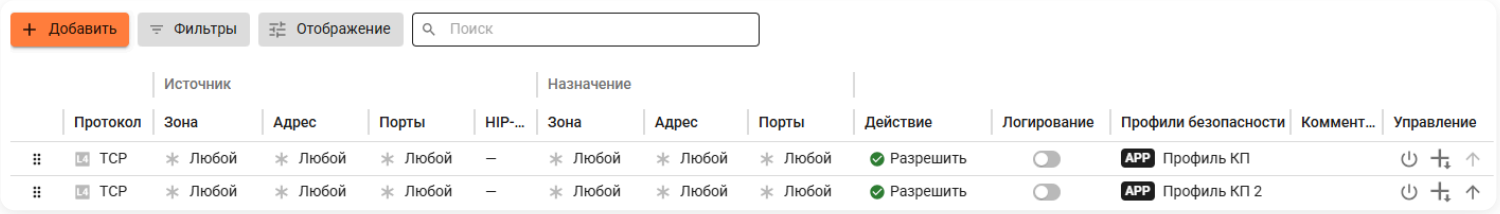
Межсетевой экран Ideco NGFW Novum обрабатывает правила последовательно, сверху вниз. Первое правило, условия которого совпадают с характеристиками проходящего трафика, определяет:

- Разрешить или запретить трафик.
- Включить ли логирование.
- Применить ли профиль безопасности.

Последующие правила, если они регулируют тот же трафик, игнорируются.

Пример. Необходимо ограничить всем сотрудникам доступ к социальным сетям и компьютерным играм. Для этого в таблице **FORWARD** настроено два правила фильтрации:

- С профилем безопасности, запрещающим сотрудникам доступ к социальным сетям, - "Профиль КП".
- С профилем безопасности, запрещающим сотрудникам доступ к компьютерным играм, - "Профиль КП 2".

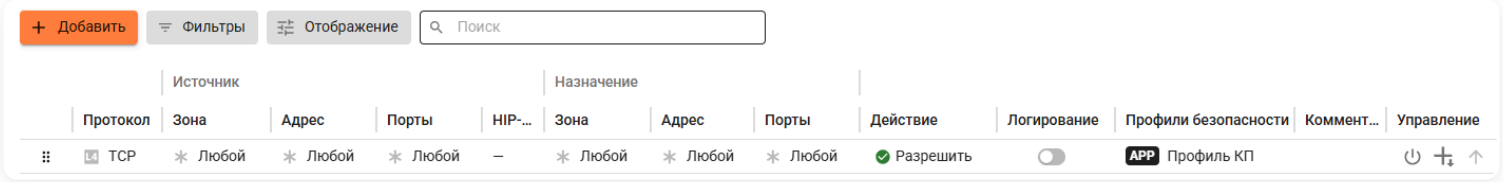


В этом случае при возникновении соответствующего трафика сотрудникам будет ограничен доступ только к социальным сетям - второе правило не будет применено, потому что трафик уже обработан вышестоящим правилом.

Если требуется добавить дополнительные условия фильтрации для определенного типа трафика, рекомендуется скорректировать настройки существующего профиля безопасности.

Рекомендуемые действия:

1. В **Профили безопасности** → **Контроль приложений** создать профиль, запрещающий доступ и к социальным сетям, и компьютерным играм.
2. В **Межсетевой экран** → **FORWARD** создать правило с данным профилем, действие - **Разрешить**:



Больше примеров настройки профилей - в статье.

Подробнее об особенностях настройки профилей - в статьях **Контроль приложений** и **Предотвращение вторжений**.

Важно

При создании правил

- Если в поле **Протокол** выбрать из списка параметр **Любой**, то правило будет действовать для всех протоколов.
- Для доступа из внешней сети в локальную необходимо создать и включить разрешающее правило **FORWARD**. Иначе весь трафик между сетевыми интерфейсами по умолчанию будет заблокирован системным правилом в цепочке **FORWARD**.
- При прямых подключениях к прокси не указывайте в поле **Адрес источника** IP-адрес. В противном случае правило не будет срабатывать, так как при прохождении через прямой прокси IP-адрес источника подменяется на IP-адрес Ideco NGFW.
- Если используется обратный прокси, то для **INPUT**-правила в полях **Адрес назначения** и **Порты назначения** должны указываться внешний IP-адрес и порт Ideco NGFW Novum, так как **INPUT**-правила Межсетевого экрана обрабатывают трафик раньше прокси-сервера.
- Для фильтрации веб-трафика из локальных сетей (80, 443 TCP-порты) для корректной работы правила в поле **Зона источника** должен указываться объект **Любой** либо **зона**, в которую входит интерфейс локальной сети. Если будет указан интерфейс локальной сети, то правило не будет обрабатывать веб-трафик. При инспекции веб-трафика интерфейс источника переназначается на интерфейс Ideco NGFW Novum, но **зона интерфейса источника сохраняется**.
- **DNAT**-правило обрабатывает UDP-трафик, пришедший только с **Внешних** интерфейсов.
- Трафик Ideco Client (порт 3051 UDP) обрабатывается системным правилом цепочки **FORWARD**, а не **INPUT**. Поэтому правила таблицы **INPUT**, запрещающие порт 3051, не блокируют подключения Ideco Client.
- При блокировке TCP-трафика через зону, указанную в **VPN-подключения** → **Основное**, HTTP- и HTTPS-трафик заблокирован не будет. Веб-трафик (порты 80 и 443) перенаправляется на прокси-сервер и далее в таблице **FORWARD** проходит с зоной источника **Исходящий трафик устройства**.

НЕ рекомендуем

- Создавать **FORWARD**- и **INPUT**-правила, запрещающие весь трафик, без предварительного создания разрешающих правил. Это может привести к блокировке доступа к серверу и его функциям.
- При создании правил **Межсетевого экрана** с протоколом TCP или UDP указывать **Порт источника**. Это связано с тем, что:
  - Порт источника выбирается случайно, и лишь некоторые приложения работают с фиксированным портом.
  - Порт источника может подмениться другим при прохождении пакета через NAT.
- В **DNAT**-правилах для обработки UDP-трафика выбирать **Локальный Ethernet** в поле **Источник**. Причина в том, что таблица **DNAT не обрабатывает** UDP-трафик, приходящий с локального интерфейса.
- Публиковать внутренние ресурсы через **DNAT**-правила с использованием TCP-порта 443, это заблокирует работу Ideco Client, использующего тот же порт. Для корректной работы Ideco Client опубликуйте внутренние ресурсы через обратный прокси или зарезервируйте TCP-порт 443 за Ideco Client, а внутренний ресурс опубликуйте на другом порту.

Рекомендуем

- Для предотвращения блокировки клиентского HTTP/HTTPS-трафика создайте правила:
  - Разрешающее трафик от пользователя.
  - Разрешающее трафик для специальной зоны источника **Исходящий трафик устройства**.

Полезные ссылки

- **Объекты**
- **Профили устройств**
- **Логирование**
- **Контроль приложений**
- **Предотвращение вторжений**

Примеры создания правил межсетевого экрана

Настройка правил межсетевого экрана для IPsec-подключений

Чтобы настроить правило **Межсетевого экрана** для IPsec-подключений, выберите в поле **Зона источника** или **Зона назначения** настроенное IPsec-подключение.

Портмаппинг, DNAT, публикация сервера в локальной сети

Примеры данных настроек подробно описаны в статьях раздела Публикация ресурсов.

Блокировка различных ресурсов средствами межсетевого экрана

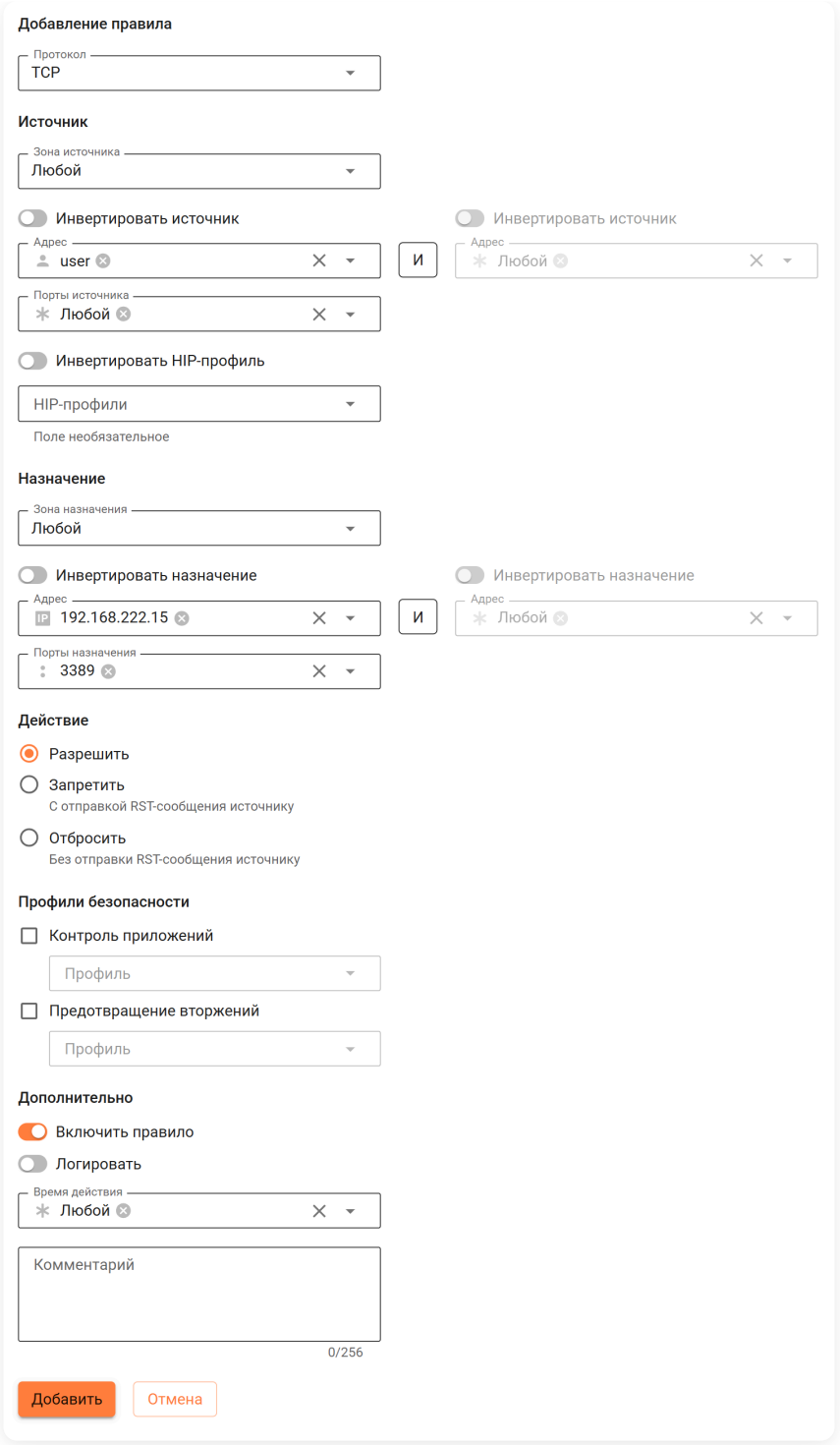
Вопросы блокировки программ удаленного управления (AmmyAdmin и TeamViewer), мессенджеров и другого ПО - описаны в статье Блокировка популярных ресурсов.

Доступ к терминальному серверу для определенного пользователя

1. В **Правила трафика** → **Межсетевой экран** → **FORWARD** нажмите **Добавить**.

2. Заполните поля:

- **Протокол** - выберите TCP.
- **Адрес** - выберите пользователя или группу пользователей.
- **Назначение** - укажите адрес терминального сервера.
- **Порты назначения** - укажите порт 3389.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

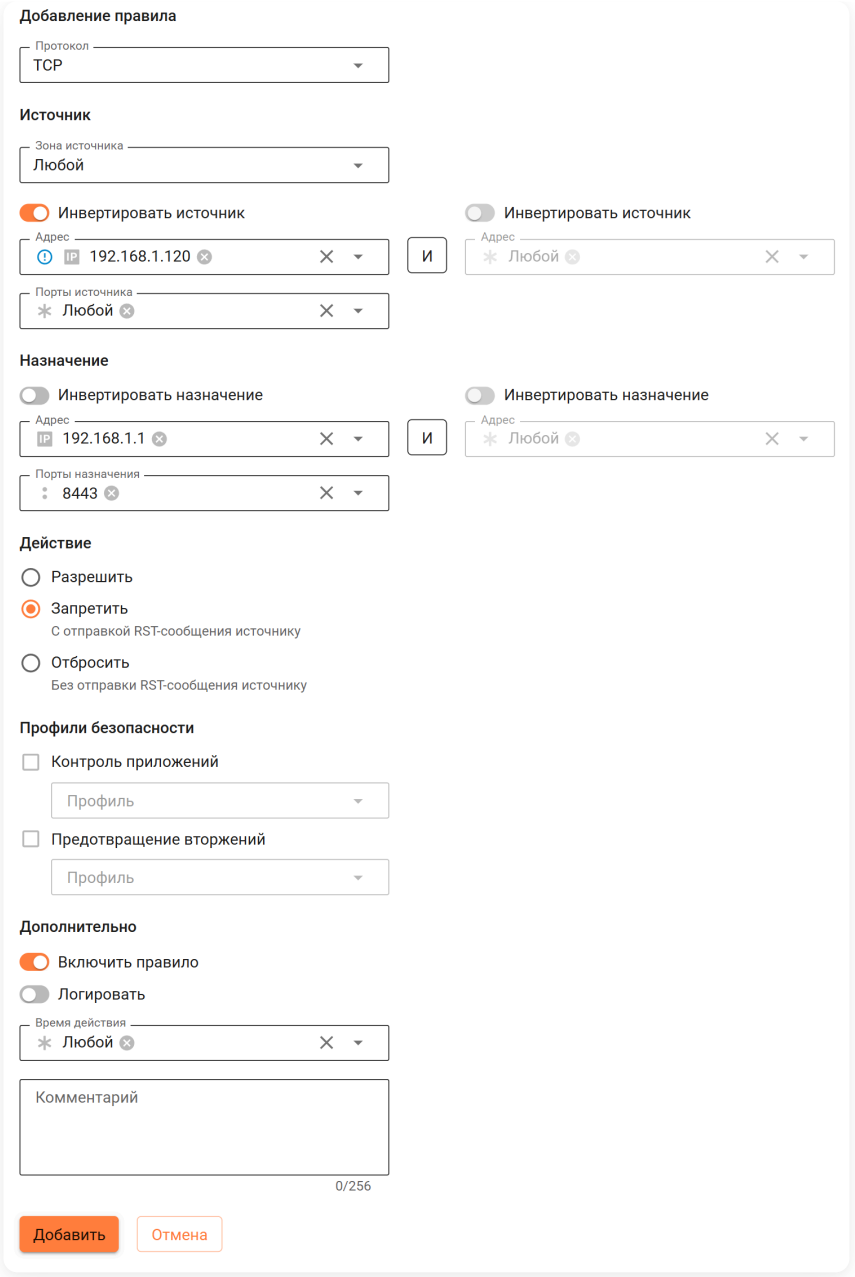


3. Нажмите **Добавить**.

Блокировка доступа к веб-интерфейсу (порт 8443) всем, кроме определенного адреса

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите правило:



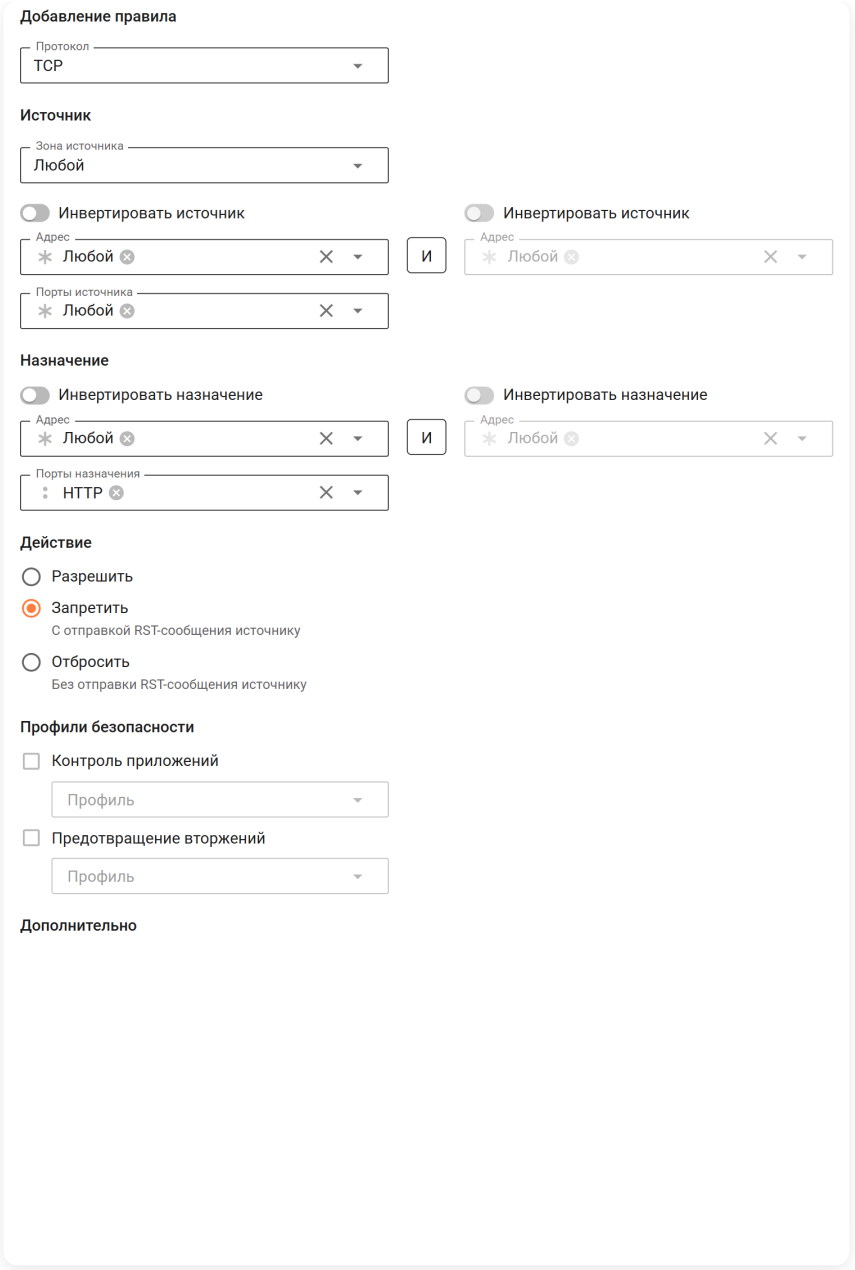
- Доступ к веб-интерфейсу будет разрешен только с IP-адреса **192.168.1.120**.
- **192.168.1.1** - IP-адрес Ideco NGFW Novum в локальной сети.

Блокировка 80 порта Ideco NGFW Novum

80 TCP порт используется для выпуска сертификатов Let`s Encrypt.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите правило:



Разрешение DNS-запросов через внешние DNS

ВАЖНО: Рекомендуем использовать в качестве DNS-сервер Ideco NGFW Novum. Но если необходимо использовать внешний DNS-сервер, то выполните действия:

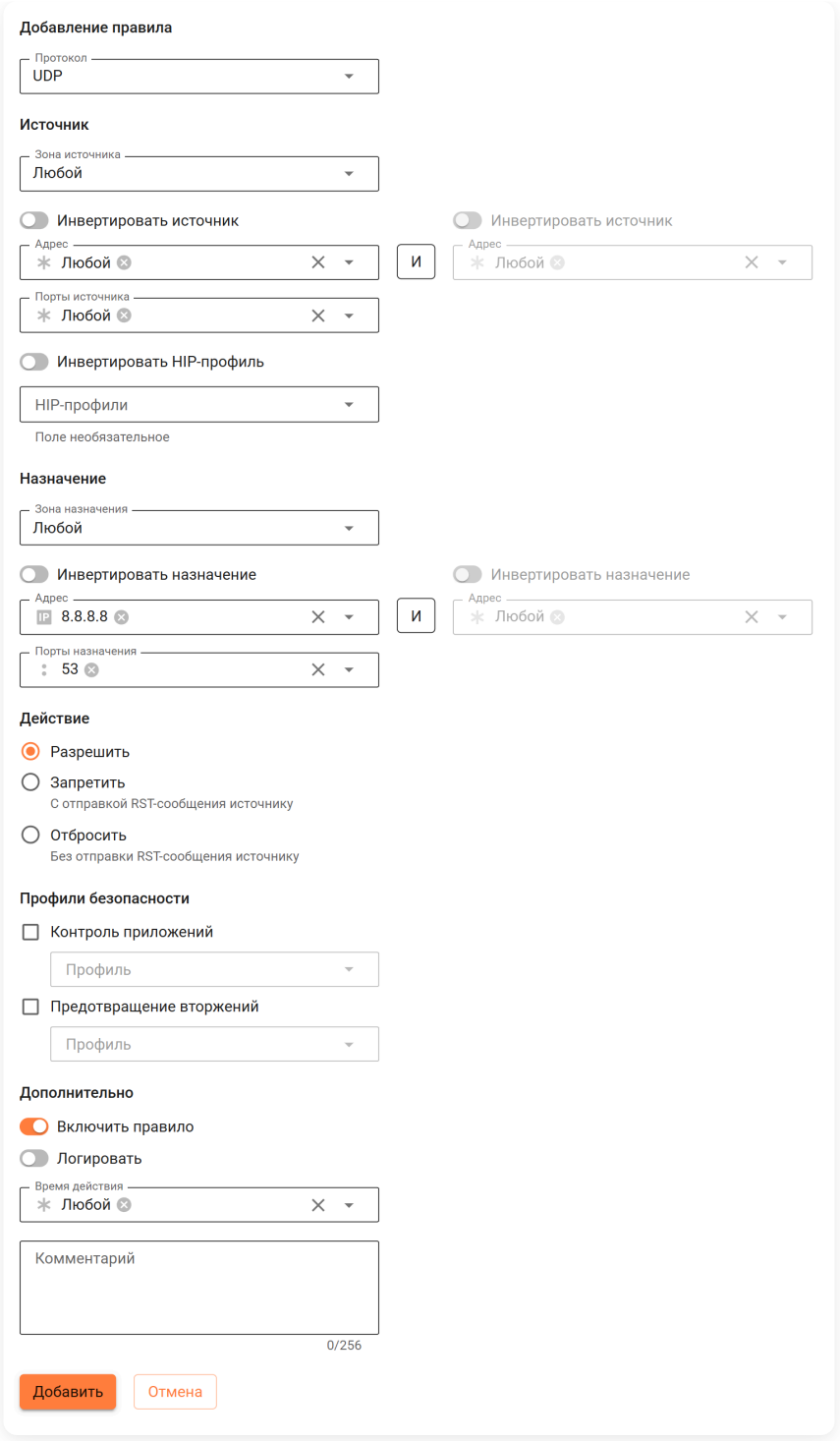
1. В **DNS** → **Внешние DNS** выключите **Перехват пользовательских DNS-запросов**.

2. Добавьте внешний DNS-сервер.

3. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

4. Создайте правило **Запретить все** и включите его.

5. Создайте правило, заполнив поля:



- **Протокол** - выберите UDP.
- **Назначение**:
  - **Адрес** - укажите IP-адрес внешнего DNS-сервера.
  - **Порт назначения** - укажите порт 53.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

Для работы протокола DNS может быть недостаточно правила с протоколом UDP, поскольку DNS использует в качестве транспорта UDP и TCP. Для решения задачи создайте аналогичное правило с протоколом TCP, используя кнопку **Клонировать** в таблице правил.

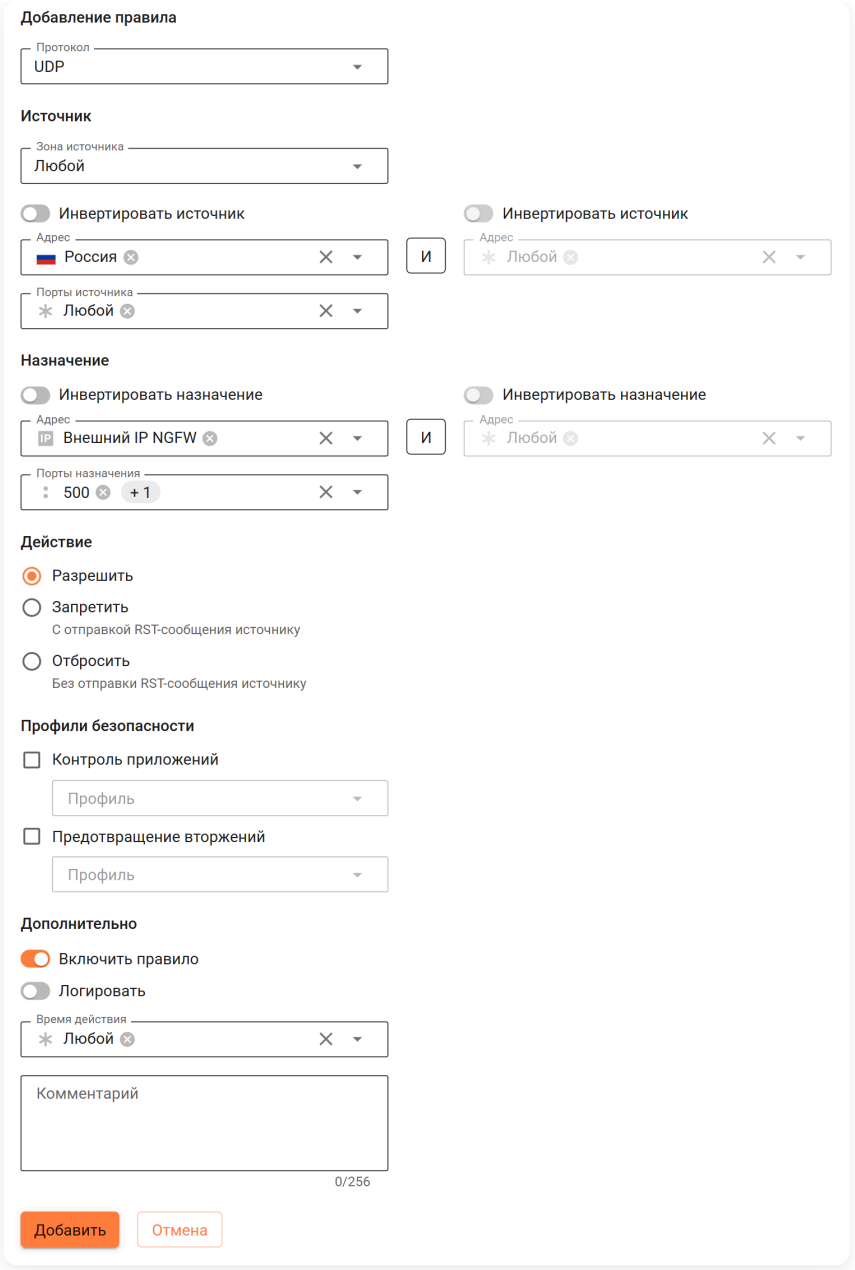
Доступ до Ideco NGFW Novum только из определенной внешней сети по IKEv2/IPsec

Пример: нужно разрешить доступ до Ideco NGFW Novum из России по VPN через IKEv2/IPsec.

ВАЖНО: Правило актуально, если на вкладке **INPUT** есть правило **Запретить все**.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:



- **Протокол** - выберите UDP.
- **Источник**:
  - **Адрес** - выберите страну Россия.
- **Назначение**:
  - **Адрес** - укажите внешний IP-адрес Ideco NGFW Novum.
  - **Порт назначения** - укажите порты 500 и 4500.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

Разрешение доступа к конкретным ресурсам при наличии запрещающего весь трафик правила

Примеры представлены в статье Как разрешить доступ к ресурсам в ограниченной сети.

Настройка одностороннего доступа из подсети к хосту другой подсети

На вкладке **Правила трафика** → **Файрвол** → **FORWARD** создайте два правила:

1. Правило, разрешающее доступ из подсети к хосту:

2. Правило, запрещающее доступ от хоста к подсети:

3. Расположите разрешающее правило выше запрещающего.

- **192.168.112.0/24** - подсеть, из которой требуется разрешить доступ до хоста.
- **192.168.19.119** - хост, который не должен иметь доступ до указанной подсети.

DNAT-правило для работы site-to-site IPsec с устройством в локальной сети

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **DNAT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:

- **5.120.1.25** - IP-адрес Ideco NGFW Novum во внешней сети.
- **192.168.1.50** - IP-адрес устройства в локальной сети.

Для полноценной работы IPsec создайте такое же правило с протоколом AH, нажав Клонировать. Помимо этого, нужно создать **DNAT**-правило с протоколом UDP и портами 500, 4500.

Полезные ссылки

- **Как разрешить доступ к ресурсам в ограниченной сети**

Логирование

Функциональность доступна в **Классическом** и **Системном контекстах**.

Принцип работы

Соединения, установленные до создания правил логирования, залогированы не будут. Если приходит пакет, атрибуты которого (протокол, порты и IP-адрес) соответствуют уже созданному соединению, к нему применяются те же действия, что и к другим пакетам этого соединения.

Первый пакет нового соединения (протокол, порты, IP-адреса не соответствуют атрибутам уже установленного соединения) проходит через правила вкладки **Логирование**. Если атрибуты пакета соответствуют правилу логирования, то на пакет ставится метка логирования. По умолчанию метки нет.

Срабатывают все правила логирования, настроенные на вкладке **Логирование**, по порядку. Если пакет соответствует нескольким правилам логирования, будет применено последнее из них.

Далее трафик проходит через правила в таблицах Межсетевого экрана. Если при срабатывании правила на пакете стояла метка логирования, то в логи попадают следующие данные:

- Атрибуты пакета, с которым произошло событие (протокол, порты и IP-адреса).
- Данные правил **Межсетевого экрана**: идентификатор правила, название таблицы и действие, которое произошло.
- Информация по DNAT: идентификатор правила, измененный IP-адрес и порт назначения.
- Информация по SNAT: идентификатор правила, измененный IP-адрес источника.
- Если в правиле указаны профили безопасности:
  - Данные профиля Контроля приложений: профиль, действие, протокол прикладного уровня, приложение.
  - Данные профиля Предотвращения вторжения: профиль, ID соединения, действие и ID сигнатуры.

Для просмотра логов перейдите в **Отчеты и журналы** → **Межсетевой экран**.

Модули **Контроль приложений** и **Предотвращение вторжений** могут задерживать решение о блокировке или разрешении соединения, поэтому информация в журнале появляется не сразу. После принятия решения запись в журнале **Межсетевой экран** обновляется.

Включите опцию **Логировать срабатывания правил** для начала логирования.

Не рекомендуем включать логирование всего трафика, так как при высоком потоке новых соединений логирование требует дополнительных ресурсов на сервере и возможна потеря части логов. Логирование необходимо, например, для определения модуля, блокирующего доступ в интернет.

Если для работы логирование не требуется, рекомендуем отключить опцию **Логировать срабатывания правил**.

Трафик для логирования

Правила **Логирования** позволяют гибко выбрать трафик для логирования. Создайте и включите в таблице правило логирования. Соединение залогируется и отразится в журнале **Межсетевой экран** при срабатывании правила **Межсетевого экрана**.

Действие **Не логировать** позволяет снять метку логирования.

Пример 1. Настройка логирования всего трафика на yandex.ru, кроме трафика от Иванова Ивана

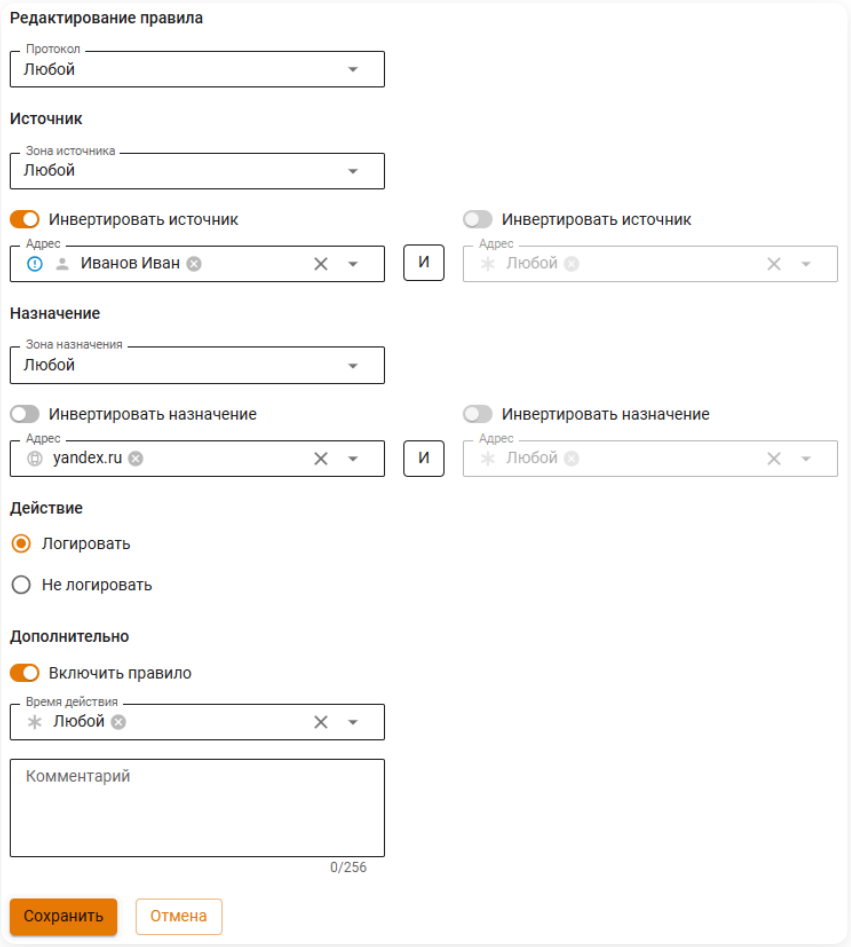
Настройте правило:

1. В поле **Источник** выберите ***Иванова Ивана*** и переведите опцию **Инвертировать источник** в положение **Включен**.

2. В поле **Назначение** выберите `yandex.ru`.

3. Выберите действие **Логировать**.

4. В поле **Дополнительно** включите правило:



Способ настройки через опцию **Инвертировать источник** желательно использовать при небольшом количестве правил логирования. При большом количестве правил логирования более удобен способ, описанный в примере 2.

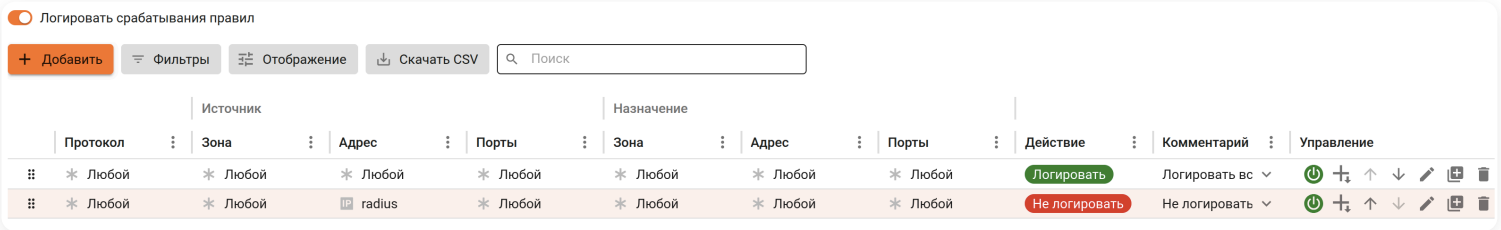
Пример 2. Настройка логирования всего трафика, кроме трафика от RADIUS сервера

Настройте два правила:

1. Правило с действием **Логировать** для всего трафика.

2. Правило с действием **Не логировать** для трафика от источника ***RADIUS***.

Расположите второе ниже:



Предварительная фильтрация

Классический контекст | Высокопроизводительный контекст

Вкладка **Предварительная фильтрация** позволяет заблокировать весь трафик, попадающий под условия таблицы, до просмотра таблиц **Межсетевого экрана** (например, **FORWARD** или **INPUT**). Используйте раздел, если требуется фильтрация пакетов на уровне TCP/IP.

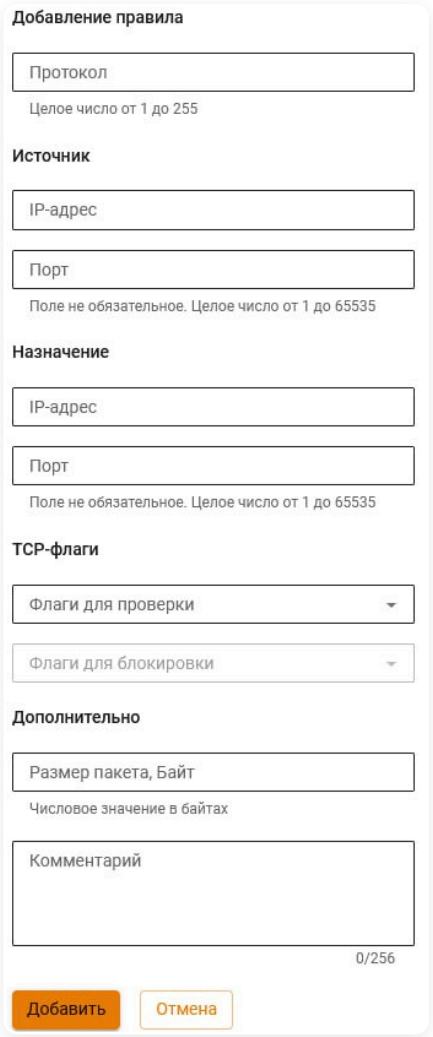
Включение хотя бы одного правила **Предварительной фильтрации** может привести к снижению сетевой производительности NGFW примерно на 20%.
При выключении правила производительность сразу восстановится.

При наличии большого количества правил воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Создание правил

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Предварительная фильтрация** и нажмите **Добавить**.

2. Заполните поля правила:



Расшифровка полей

- **Протокол** - укажите номер протокола из таблицы. Номер может быть в диапазоне от 0 до 255 включительно.

- **Источник**:
  - **IP-адрес** - укажите IP-адрес источника.
  - **Порт** - укажите порт источника.
- **Назначение**:
  - **IP-адрес** - укажите IP-адрес назначения.
  - **Порт** - укажите порт назначения.
- **TCP-флаги**:
  - **Флаги для проверки** - укажите флаги TCP, которые будут проверяться. В этом поле могут быть указаны флаги: **SYN**, **ACK**, **FIN**, **RST**, **URG**, **PSH**.
  - **Флаги для блокировки** - укажите флаги TCP, которые будут заблокированы. Флаг будет доступен для блокировки, только если флаг содержится в поле **Флаги для проверки**.
- **Дополнительно**:
  - **Размер пакета, Байт** - укажите размер пакета в байтах с учетом TCP- и IP-заголовков (40 + N, где N - размер полезных данных в пакете). Пакет указанного размера будет заблокирован.
  - **Комментарий**.

3. Нажмите **Добавить**.

Устранение проблем

При неправильно созданных правилах доступ к веб-интерфейсу может быть заблокирован (например, блокировка протокола TCP с проверкой и блокировкой флага **SYN**). Для возвращения доступа к веб-интерфейсу воспользуйтесь инструкцией или включите режим **Полный доступ**.

Тестирование правил

Классический контекст | Высокопроизводительный контекст

На вкладке создаются тесты для проверки работы правил таблицы **FORWARD** и **INPUT**.

Тест - это конкретный пример, в котором проверяется доступ к определенному IP-адресу с учетом правил таблицы **Межсетевого экрана**. Во время тестирования NGFW Novum генерирует тестовый пакет с заданным источником и назначением, после чего проверяет, как пакет проходит через **Межсетевой экран**.

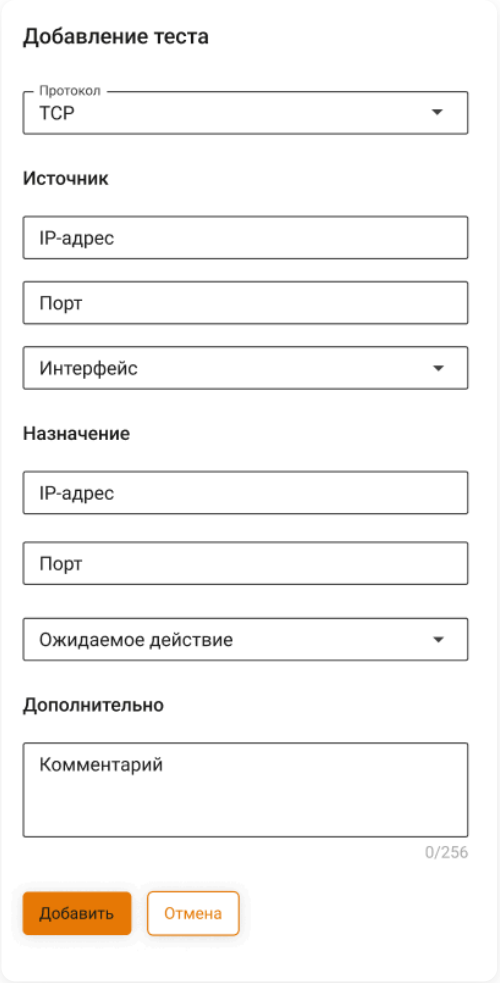
Рекомендуем использовать для источника порты из диапазона 49152 - 65535 (динамически выделяемые или частные порты, которые не регистрируются IANA).

Создание тестов

Для создания теста выполните действия:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Тестирование правил** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Протокол** (**TCP**/**UDP**).
- **IP-адрес** - адрес источника и назначения.

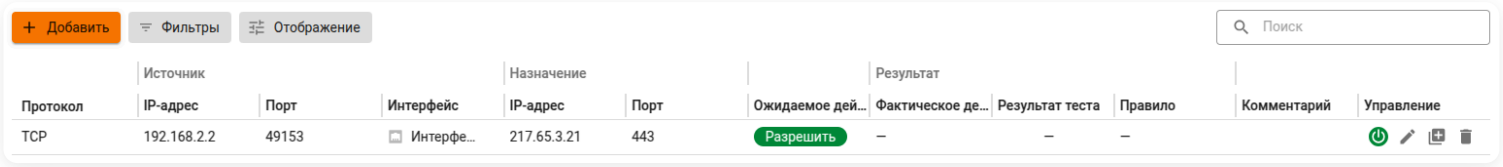
- **Порт** - порт источника и назначения.
- **Интерфейс** - сетевой интерфейс источника.

> Выбранный интерфейс должен быть настроен и подключен. Если интерфейс отключен, Ideco NGFW Novum не сможет выполнить тестирование.

- **Ожидаемое действие** - Разрешить или Запретить.
- **Комментарий** - необязательное поле.

3. Нажмите **Добавить**.

Созданные тесты добавляются в таблицу:



Запуск и результат тестирования

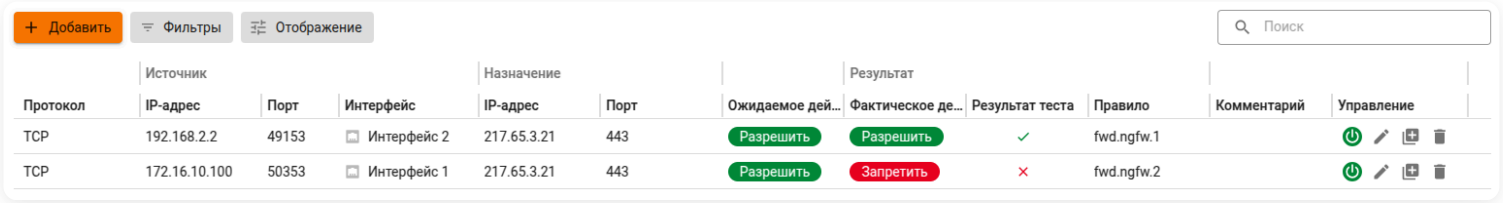
Запуск теста не происходит автоматически при добавлении. Для запуска:

1. Включите нужный тест .

2. Нажмите **Запустить тестирование** в левом нижнем углу вкладки.

> Если тест выключен, то тестирование запускаться не будет.

При совпадении ожидаемого и фактического действия тестирование считается успешным:



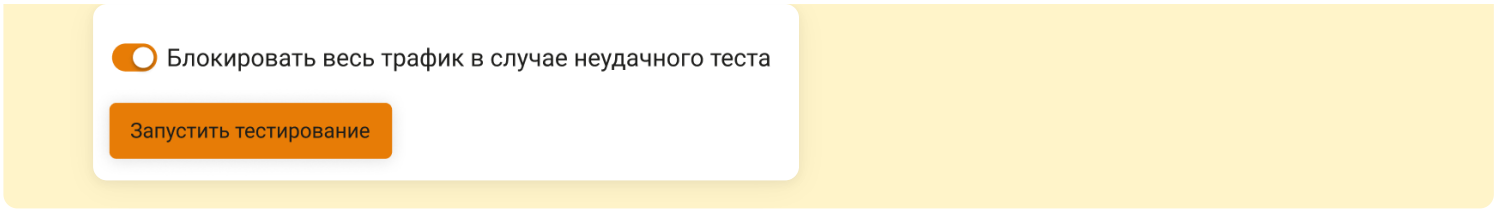
Залогированные правила вида `fwd.sys.xxx`, `inp.sys.xxx`, `out.sys.xxx` в столбце **Правило** - результат срабатывания системного правила, которое разрешило или запретило прохождение трафика в рамках проверки, если не сработало ни одно пользовательское правило. Это правила **Межсетевого экрана**, которыми нельзя управлять из веб-интерфейса Ideco NGFW Novum, правила **Межсетевого экрана** всегда включены.

> Расшифровка элементов системного правила `<name>.sys.xxx`:
>
> - `<name>.sys.` - название правила:
> - `fwd.sys` - Forward System: правило обработки трафика, проходящего между зонами сервера;
> - `inp.sys` - Input System: правило обработки входящего трафика;
> - `out.sys` - Output System: правило обработки исходящего трафика.
> - `xxx` - идентификатор правила. Например, `fwd.sys.22`

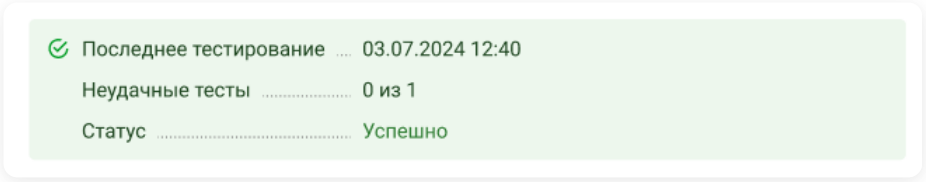
Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Межсетевого экрана**. Посмотреть системное правило, которое сработало, можно через Терминал, введя команду `iptables-save | grep 'sys.<ID правила>'` (смотрите примеры в статье)

Если у выбранного теста **Интерфейс** источника был удален (отображается **Удалено** в столбце **Интерфейс**), тестирование завершится с фактическим действием **Запретить**.

> Не рекомендуем включать опцию **Блокировать весь трафик в случае неудачного теста**, иначе при любом неуспешном результате теста (обозначен) весь трафик через NGFW Novum будет заблокирован. Единственный способ снятия блокировки - тестирование без ошибок. Отключение опции не сработает:



В правом нижнем углу вкладки представлены сведения о последнем тестировании: текущий статус (**Успешно**/**Ошибка**), время проведения и количество неуспешных тестов (из числа включенных в столбце **Управление**):



Повторный запуск сбрасывает результаты предыдущего тестирования.

Аппаратная фильтрация

Функциональность доступна в **Классическом** и **Системном контекстах**.

На вкладке можно настроить пакетную фильтрацию трафика на основе сетевых и физических адресов отправителей и (или) получателей. Пакеты будут блокироваться на аппаратном уровне без участия центрального процессора, с использованием вычислительных мощностей сетевой карты.

В Ideco NGFW Novum блокировка будет происходить в соответствии с выбранным режимом фильтрации. Одновременно может работать фильтрация по MAC-адресу источника или один из видов фильтрации по IP.

Созданные на вкладке правила применяются сразу ко всем поддерживаемым сетевым адаптерам, найденным в системе.

Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

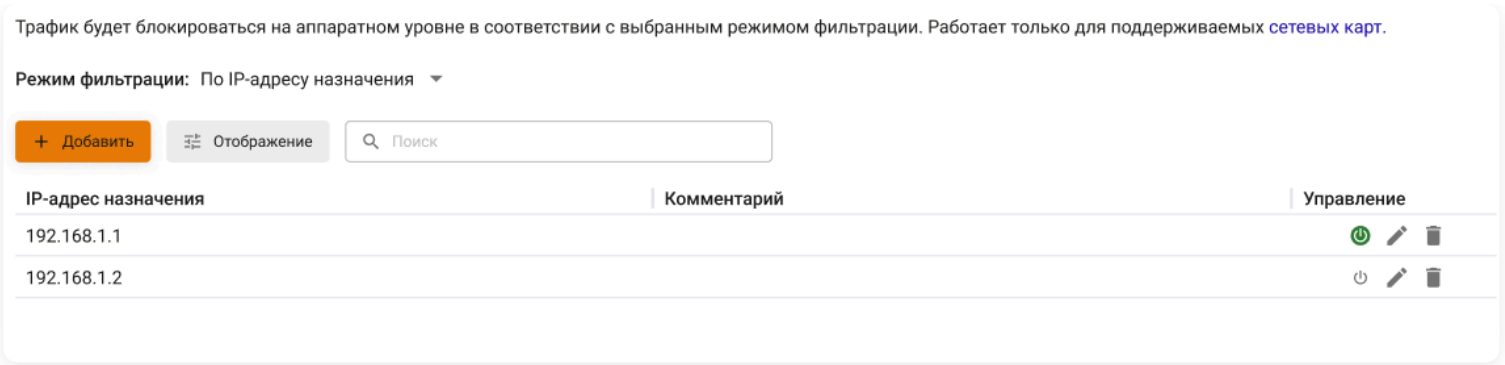
Список поддерживаемых сетевых карт

PCI-идентификатор	Модель адаптера
0x8086:0x0CF8	Ethernet Controller X710 Intel(R) FPGA Programmable Acceleration Card N3000 for Networking
0x8086:0x0D58	Ethernet Controller XXV710 Intel(R) FPGA Programmable Acceleration Card N3000 for Networking
0x8086:0x1572	Ethernet Controller X710 for 10GbE SFP+
0x8086:0x1574	Ethernet Controller XL710 Emulation
0x8086:0x1580	Ethernet Controller XL710 for 40GbE backplane
0x8086:0x1581	Ethernet Controller X710 for 10GbE backplane
0x8086:0x1583	Ethernet Controller XL710 for 40GbE QSFP+
0x8086:0x1584	Ethernet Controller XL710 for 40GbE QSFP+
0x8086:0x1585	Ethernet Controller X710 for 10GbE QSFP+
0x8086:0x1586	Ethernet Controller X710 for 10GBASE-T
0x8086:0x1587	Ethernet Controller XL710 for 20GbE backplane
0x8086:0x1588	Ethernet Controller XL710 for 20GbE backplane
0x8086:0x158A	Ethernet Controller XXV710 for 25GbE backplane
0x8086:0x158B	Ethernet Controller XXV710 for 25GbE SFP28
0x8086:0x15FF	Ethernet Controller X710 for 10GBASE-T
0x8086:0x104F	Ethernet Controller X710 for 10 Gigabit backplane
0x8086:0x104E	Ethernet Controller X710 for 10 Gigabit SFP+
0x8086:0x0DD2	Ethernet Network Adapter I710

Создание правил

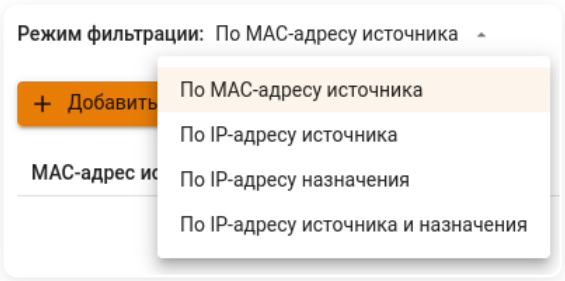
Администратор может создать не более 2500 правил каждого типа фильтрации.

Созданные правила отображаются в таблице в зависимости от выбранного режима фильтрации:



Чтобы создать правило определенного типа, выполните действия:

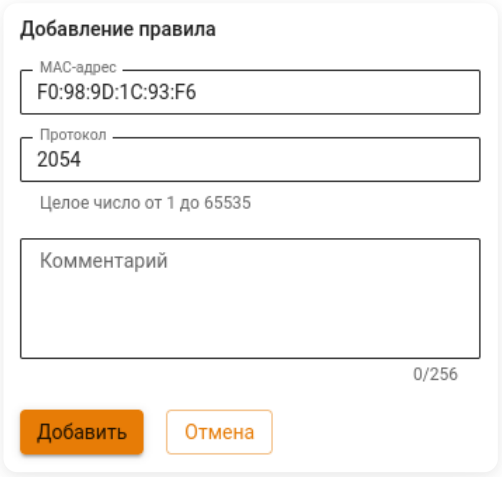
1. Выберите режим фильтрации, нажав на кнопку в левом верхнем углу:



- По MAC-адресу источника.
- По IP-адресу источника.
- По IP-адресу назначения.
- По IP-адресу источника и назначения.

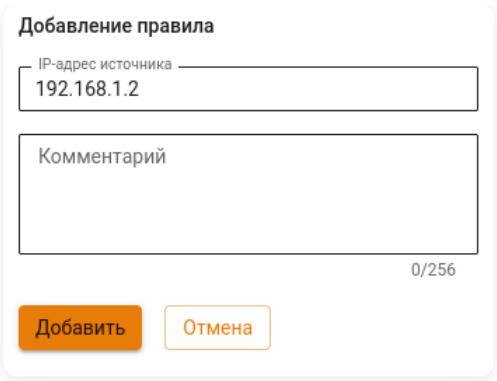
2. Нажмите **Добавить** и заполните поля:

Фильтрация по MAC-адресу источника



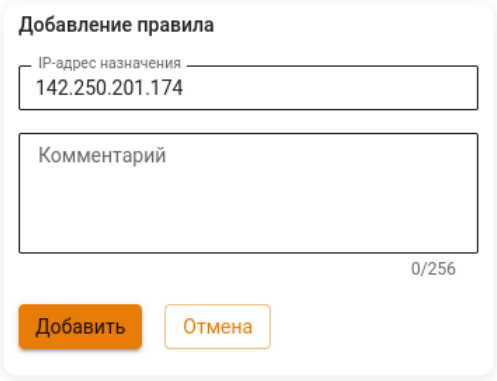
- **MAC-адрес** - введите физический адрес источника трафика.
- **Протокол** - введите номер протокола сетевого уровня. **Не указывайте протокол IPv4** (значение 2048), для фильтрации на сетевом уровне используйте правила ***По IP-адресу источника***, ***По IP-адресу назначения***, ***По IP-адресу источника и назначения***.
- **Комментарий** - поле необязательное.

Фильтрация по IP-адресу источника



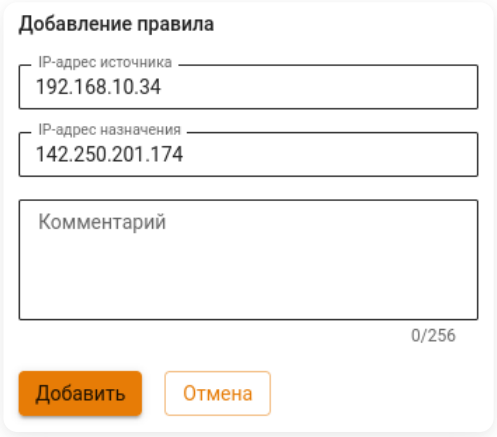
- **IP-адрес источника** - введите IP-адрес источника трафика.
- **Комментарий** - поле необязательное.

Фильтрация по IP-адресу назначения



- IP-адрес назначения - введите IP-адрес назначения трафика.
- Комментарий - поле необязательное.

Фильтрация по IP-адресу источника и назначения



- **IP-адрес источника** - введите IP-адрес источника трафика.
- **IP-адрес назначения** - введите IP-адрес назначения трафика.
- **Комментарий** - поле необязательное.

3. Нажмите **Добавить**.

4. Включите правило или оставьте выключенным.

Отключить аппаратную фильтрацию можно, выключив опцию **Межсетевой экран** в соответствующем разделе.

Настройка ALG

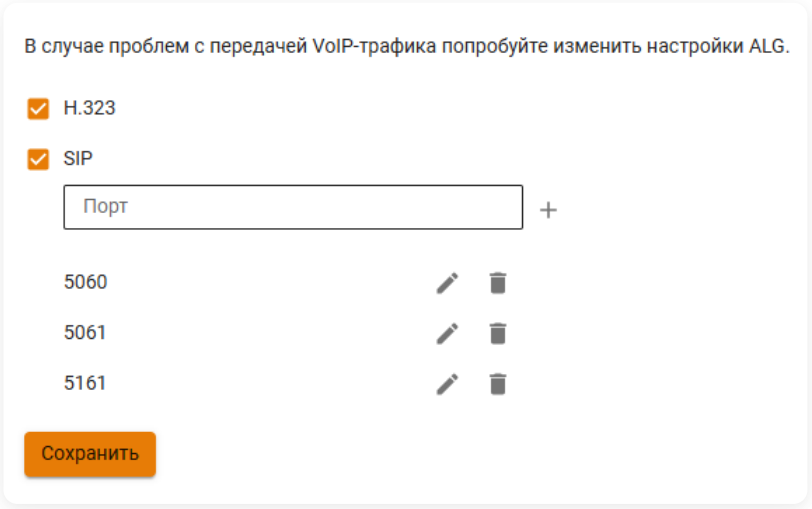
Функциональность доступна в **Классическом** и **Системном контекстах**.

Вкладка **Настройка ALG** позволяет управлять параметрами протоколов VoIP (H.323 и SIP), а также настраивать порты, используемые для передачи голосового трафика. Используйте раздел, если:

- Возникли проблемы с передачей VoIP-трафика, например, отсутствуют гудки или голос при повторных звонках между абонентами.
- Используются нестандартные порты для протокола SIP.

Изменение настроек ALG

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Настройка ALG** и заполните поля:



- **H.323** - активировано по умолчанию. Если протокол не используется, то отключите опцию.
- **SIP** - активировано по умолчанию. Если протокол не используется, то отключите опцию.
- **Порт** - укажите порт для протокола SIP, если используется нестандартный. Максимальное количество портов - 10.

2. Нажмите **Сохранить**.

Контент-фильтр

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Профили контент-фильтра**: `ideco-content-filter-backend`, `ideco-content-filter-backend-rules-file-syncer`, `ideco-content-filter-sky-db-updater`, `ideco-rocks-cf-tool`.

Список имен служб для других разделов доступен по ссылке.

Контент-фильтр проверяет запрашиваемые сайты в базе URL-адресов из пользовательских категорий Ideco NGFW Novum. Если адрес находится в списках, то применяются настроенные правила фильтрации.

Контент-фильтр работает на прикладном уровне (в частности, HTTPS), информация об IP-адресах может быть неточной. Для фильтрации на сетевом уровне по IP-адресам используйте Межсетевой экран.

Контент-фильтр включает пять вкладок:

- Правила - создание и управление правилами фильтрации.
- Пользовательские категории - управление собственных списков.
- Переопределение категорий - проверка и изменение категорий для сайтов из расширенной базы.
- Морфологические словари - фильтрация по ключевым словам.
- Настройки - параметры работы фильтра.

Особенности фильтрации

Контентная фильтрация применяется только к веб-запросам, направленным на внешние интернет-ресурсы через стандартные порты:

- HTTP - порт 80 TCP.
- HTTPS - порт 443 TCP.

Запросы к локальным веб-ресурсам, а также веб-трафик, передаваемый по нестандартным портам, не обрабатываются **Контент-фильтром**.

- **Фильтрация HTTPS**:
  - HTTPS-сайты без расшифровки трафика фильтруются только по домену (не по полному URL). Например, нельзя заблокировать только `http://example.com/page` и оставить доступ к `http://example.com/path` - будет заблокирован весь доступ к `example.com`. Также без расшифровки трафика невозможно применить правила категории **Файлы**: чтобы заблокировать или разрешить загрузку файлов определенных типов, система должна иметь возможность анализировать путь или имя файла в URL (например, `https://example.com/upload/test.pdf`).
  - Для полной фильтрации HTTPS создайте правила расшифровки HTTPS-трафика нужных категорий или всех веб-запросов (категория **Все запросы**).
- **Фильтрация по IP-адресам** работает для:
  - HTTP-запросов к IP-адресам напрямую.
  - Расшифрованных HTTPS-запросов к IP-адресам.
  - HTTPS-запросов к ресурсам, IP-адрес которых содержится в поле Common Name сертификата.

Для записи логов включите опцию **Включить логирование** в **Сервисы** → **Прокси** → **Основное**.

Полезные ссылки

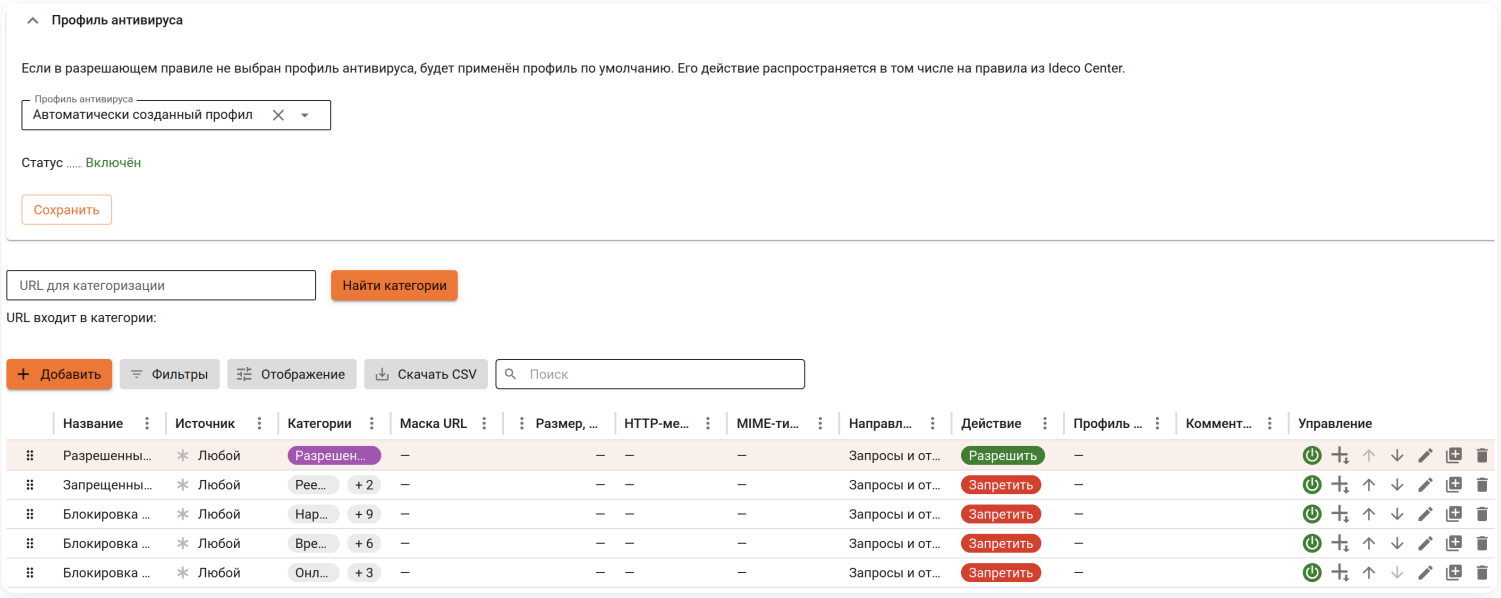
- **Блокировка загрузки файлов в файлообменники**
- **Блокировка популярных ресурсов**
- **Блокировка чат-ботов**

Правила

Функциональность доступна в **Классическом** и **Системном контекстах**.

Правила создаются в **Правила трафика** → **Контент-фильтр** → **Правила**.

Вкладка содержит:



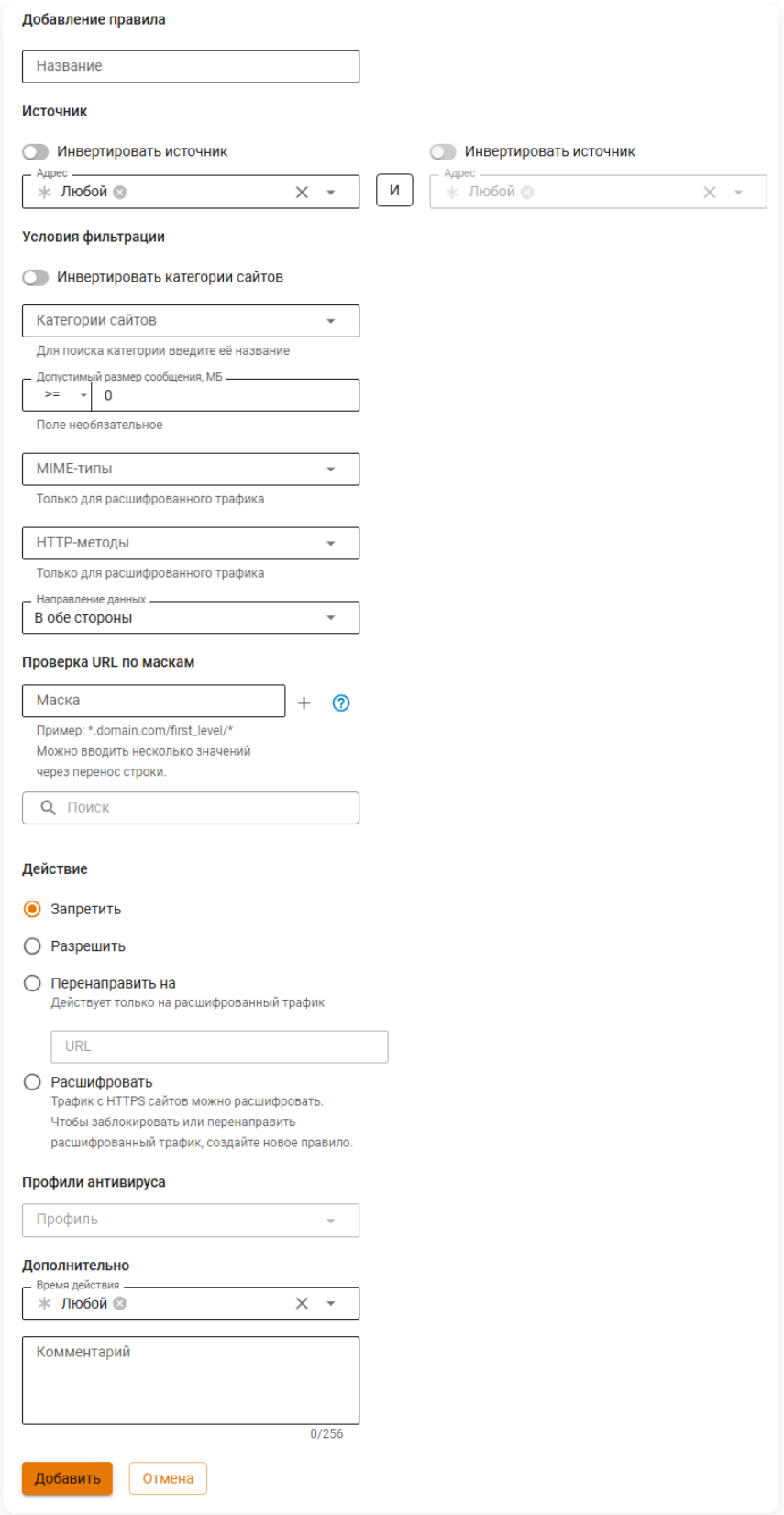
- **Профиль антивируса**. Настройка профиля **Антивируса** по умолчанию, который будет применяться:
  - К разрешающим правилам **Контент-фильтра** (включая правила из Ideco Center), где профиль не задан.
  - К трафику, который не попал ни под одно правило **Контент-фильтра**.
    Статус отображает состояние активности выбранного профиля **Антивируса**.

Чтобы задать профиль для конкретного правила, используйте поле **Профили антивируса** в форме создания или редактирования правила.

- **Строку поиска категории URL для категоризации**. Позволяет найти, к какой категории относится URL для создания правила.
- **Таблицу созданных правил**. Порядок применения правил описан в разделе ниже.

Создание правил

1. Нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Название** - название правила. Значение не должно быть длиннее 42 символов.
- **Источник**:
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), для которых применяется правило. Доступные объекты: IP-адреса, диапазоны IP-адресов, сети, домены, страны или пользователи и группы.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
- **Условия фильтрации**:

- **Инвертировать категории сайтов** - позволяет использовать в правиле все категории, кроме выбранных в поле **Категории сайтов**.
- **Категории сайтов** - поле для выбора предустановленной или пользовательской категории, перечень ресурсов, на которые распространяется действие правила.

Если поле **Категории сайтов** пустое, правило работать не будет.

- **Допустимый размер сообщения** - объем HTTP/HTTPS-сообщений в МБ, только целое число:
  - `>=` - фильтрация сообщений, размер которых больше или равен указанному числу.
  - `<=` - фильтрация сообщений, размер которых меньше или равен указанному числу.
- **MIME-типы** - форматы содержимого, к которым будет применяться правило. Форматы объединены в группы в зависимости от типа контента. Например, Audio (mp4, wav, wave и др.), Video (jpeg, mpeg, jmp и др.), Image (bmp, gif, png и др.). Настройки можно применить как к группе форматов, так и каждому формату отдельно.
- **HTTP-методы** - методы запроса, которые будут применяться для всего HTTP- или HTTPS-трафика. Используются для более точной фильтрации трафика, например, для ограничения скачивания чего-либо на сайтах, заполнения форм и т.п. Доступные методы:
  - GET - извлечение данных ресурса, содержащих тело ответа.
  - HEAD - извлечение данных ресурса, не содержащих тело ответа.
  - POST - отправка данных на определенный ресурс.
  - PUT - замена текущих значений ресурса.
  - DELETE - удаление ресурса.
  - OPTIONS - описание параметров соединения с ресурсом.
  - PATCH - частичное изменение ресурса.
  - TRACE - вызов возвращаемого тестового сообщения с ресурса.
  - CONNECT - установка соединения с ресурсом.
- **Направление данных**:
  - В обе стороны - фильтрация как входящего, так и исходящего трафика.
  - Входящее направление - фильтрация трафика на Ideco NGFW Novum от внешних источников.
  - Исходящее направление - фильтрация трафика от Ideco NGFW Novum к внешним ресурсам.
- **Проверка URL по маскам**:
  - **Маска** - шаблон URL. Значение не должно быть длиннее 255 символов. Максимальное количество URL - 100. Позволяет указать, какие именно URL-адреса внутри выбранной категории должны попадать под действие правила. Правило будет применяться исключительно к тем URL, которые соответствуют хотя бы одной из указанных масок, даже если остальные страницы сайта принадлежат той же категории.

> Для фильтрации по конкретным путям требуется расшифровка трафика - MITM. Это позволит системе анализировать полный URL. Если достаточно проверить весь домен или всю категорию целиком, расшифровка трафика не обязательна.

  - **Поиск** - поиск по введенным значениям **Маски**.
- **Действие**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик и направляет трафик в модули **Морфологический анализ** и **Антивирус**.
  - **Перенаправить на** - перенаправляет расшифрованный трафик на указанный URL.
  - **Расшифровать** - расшифровывает трафик с HTTPS-сайтов.
- **Профили антивируса** - выбор профиля **Антивируса**, которым требуется фильтровать трафик.

> Если выбрать действие **Перенаправить на**, то нужно создать аналогичное правило с действием **Расшифровать** и поместить его выше перенаправляющего правила.
>
> Для расшифрованного трафика при создании и редактировании правила **Контент-фильтра** можно настроить доступ к ресурсам с помощью HTTP-методов запроса и MIME-типов. Проверка не осуществляется по пустым полям.

- **Дополнительно**:
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **Рабочее время**), которые определяются в Объектах. По умолчанию установлено значение **Любой**.
  - **Комментарий** - произвольный текст. Значение не должно быть длиннее 255 символов.

2. Для подтверждения создания правила нажмите **Добавить**.

Порядок применения правил

Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. Если стоящее выше правило разрешает ресурс для определенной группы пользователей, то правила ниже применяться не будут:

- Зашифрованный трафик обрабатывается правилами **Разрешить**, **Запретить** и **Расшифровать**. При срабатывании правила **Расшифровать** трафик расшифровывается и проходит по правилам с начала.
- Расшифрованный трафик обрабатывается правилами **Разрешить**, **Запретить** и **Перенаправить на**.

Можно создавать гибкие настройки фильтрации, исключая нужных пользователей из-под действия блокировок вышестоящими правилами.

Если правила не действуют, проведите диагностику проблем.

Управление правилами

В столбце **Управление** можно:

Включать или выключать правило.
Менять приоритет.
Редактировать правило.
Удалять правило.

Правила **Контентной фильтрации** применяются сразу после создания или включения.

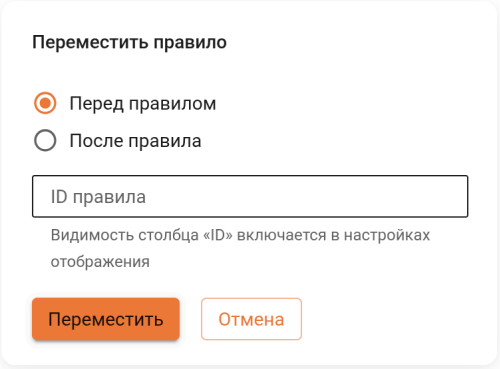
При наличии большого количества правил **Контент-фильтра** в таблице воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Для перемещения правил выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Особенности настройки правил

- При включении оператора `И` значения, выбранные в первом поле **Адрес**, нельзя указать во втором поле **Адрес**.
- Если хотя бы одно из условий **Источника** не выполняется, правило не применяется.
- Для расшифрованного трафика при создании и редактировании правила **Контент-фильтра** доступны более детальные настройки доступа к ресурсам с помощью HTTP-методов запроса, MIME-типов и проверки URL по маскам. Проверка не осуществляется по пустым полям.
- При создании шаблона **Маски** для проверки URL необходимо указывать протокол или использовать символ `*`. Важно учитывать правила:
  - Если `*` отсутствует в начале маски, поиск выполняется по точному совпадению с началом строки.
  - Если `*` отсутствует в конце маски, поиск осуществляется по точному совпадению с концом строки. Браузеры могут добавлять `/` в конце URL, поэтому рекомендуется всегда ставить `*` в конце маски. Например: `*example.com*` или `https://example.com*`.
  - Если в маске отсутствует `*`, поиск выполняется по точному совпадению всей строки.

Примеры использования масок

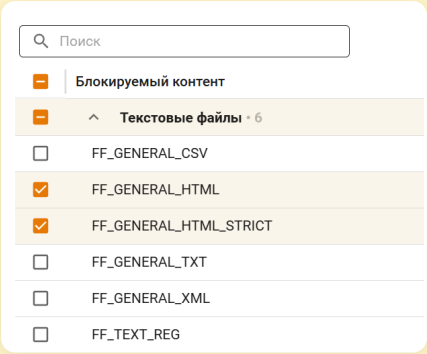
- `*example.com*` - сработает с `https://example.com`, `example.com/test` и `http://sub.example.com`.
- `*example.com` - сработает с `https://test.example.com` и `https://example.com`, не сработает с `https://example.com/path` и `https://example.com/`.

- `*//example.com*` - сработает с `https://example.com`, `http://example.com/path` и `https://sub.example.com/test`, не сработает с `https://sub.example.com`.
- `*//example.com` - сработает с `https://example.com` и `http://example.com`, не сработает с `http://example.com/path`, `https://example.com/` и `https://sub.example.com/`.
- `http*://example.com*` - сработает с `https://example.com`, `http://example.com/page`, не сработает с `ftp://example.com` и `https://sub.example.com/`.
- `https://example.com` - точное совпадение всей строки, которое сработает только с `https://example.com` и не сработает с `http://example.com` и `https://example.com/`.

Без расшифровки трафика (MITM):

- `*example.com*` - сработает с `https://example.com`, не сработает с `https://example.com/path`, `https://example.com/page`.

Антивирус блокирует веб-страницы, если в профиле Антивируса включена блокировка HTML-документов в **Текстовых файлах** и профиль выбран в правиле **Контент-фильтра**:



Полезные ссылки

- **Что делать, если не действуют правила Контент-фильтра**
- **Настройка HTTP-метода**
- **Настройка MIME-типов**
- **Блокировка загрузки файлов в файлообменники**
- **Блокировка популярных ресурсов**
- **Блокировка чат-ботов**

Трекеры и аналитика	Адреса систем учета посещений и веб-аналитики, в том числе системы слежения за пользователями
Туризм	Сайты, посвященные туризму и путешествиям
айл овые архивы	айл овые архивы программного обеспечения, файлообменники
е деральный список Минюста	Материалы, внесенные в список экстремистских Министерством стиции Р
ильмы и видео онлайн	Сайты для онлайн-просмотра фильмов и видео
инансы и финанс овые учреждения	Сайты банков и прочих финансовых организаций
ишинг и по ддельные сайты	ишинг и регистрация доменных имен, б лизких по написанию с адресами популярных сайтов.
ор умы	Сайты, предназначенные для дискуссий и обмена сообщениями между пользователями
о тогалереи	Архивы фотографий, фотостоки
а ты и мессенджеры	Сайты и серверы чатов и мессенджеров
ндик аторы компрометации ин ЕР Т	Адреса из ежедневных бюллетеней ин ЕР Т
мор	мористические и развлекательные сайты

т обы определить категорию сайта перейдите в раздел **Правила траика онтент-иль тр** и введите домен для проверки в поле **L для кате оризаии** :

При нахождении несоответствия сайта и категории обратитесь в техническую поддержку или поменяйте категорию сайта на вкладке Переопределение категорий.

Полезные ссылки

- **локировка зар узки айл ов в айл ообменники**
- **локировка чат-ботов**

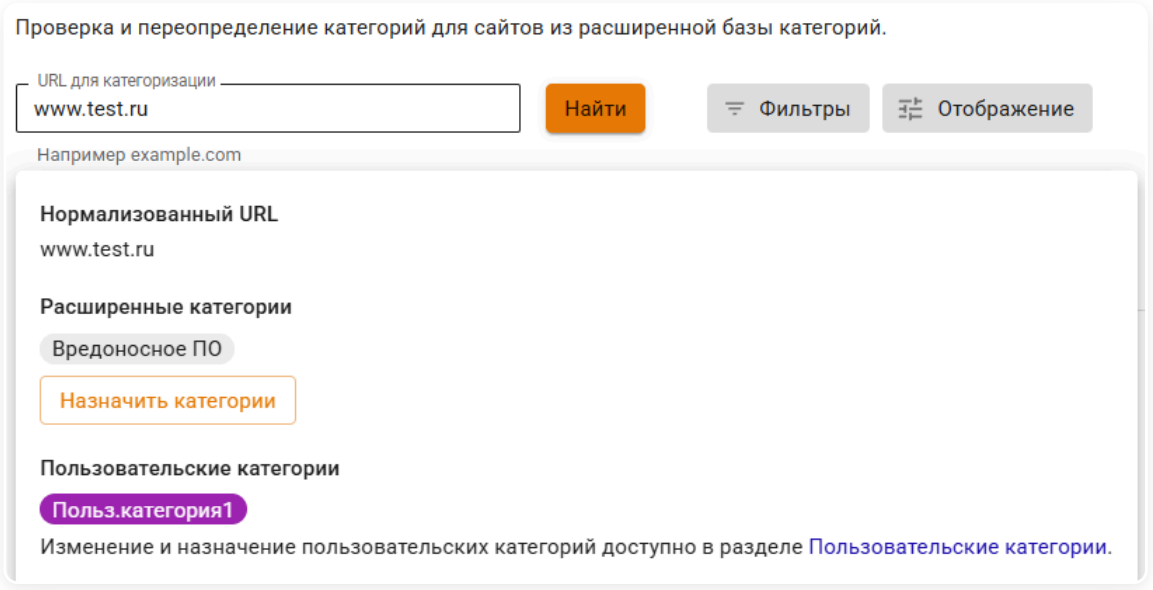
Переопределение категорий

Классический контекст | Высокопроизводительный контекст

На вкладке можно проверить, к каким категориям относится адрес сайта. При необходимости можно удалить некорректную категорию или назначить новую из расширенной базы категорий.

Проверка категорий

Для проверки категорий сайта введите URL в формате `example.com` в поле **URL для категоризации** и нажмите **Найти**. В результатах отобразятся расширенные и пользовательские категории, если URL содержится в них:



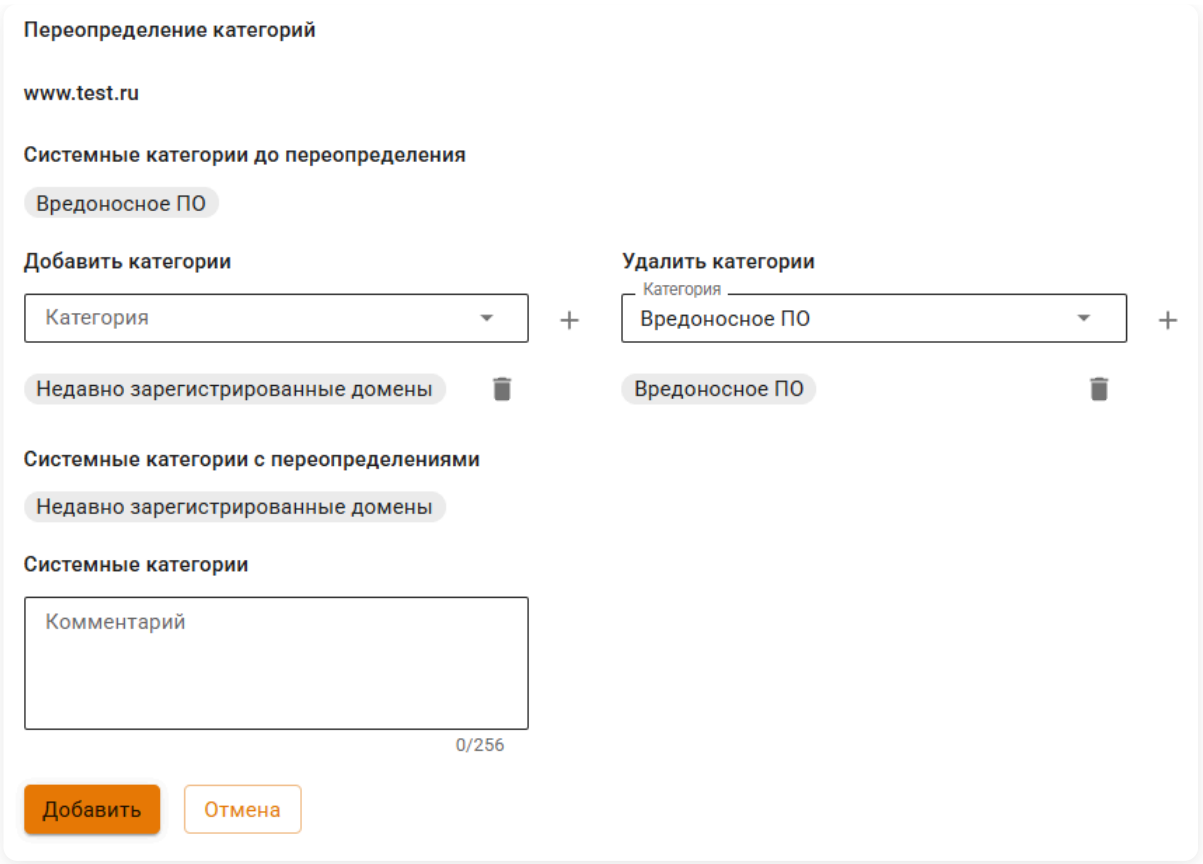
Для редактирования пользовательских категорий перейдите на вкладку **Пользовательские категории**.

Если URL отсутствует в базе расширенных категорий, то добавьте URL в подходящую пользовательскую категорию или создайте новую.

Создание правил переопределения

Для переопределения категорий выполните действия:

1. Нажмите **Переопределить** и заполните поля:

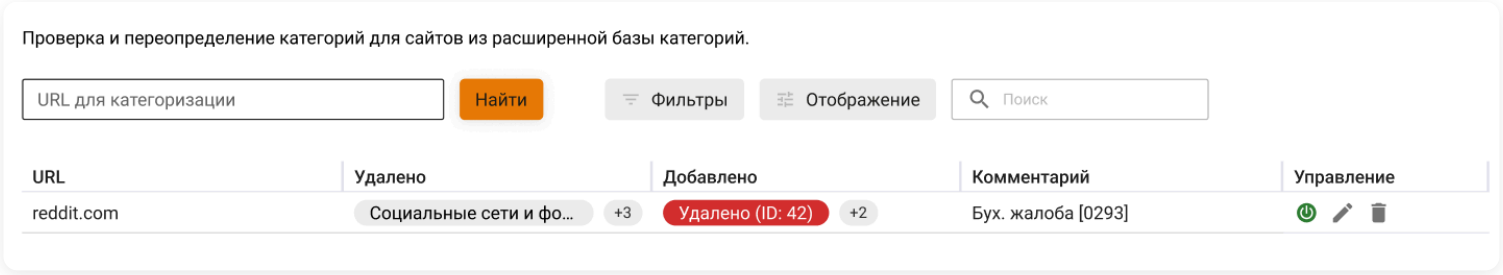


- **Добавить категории** - выберите из списка подходящую категорию и нажмите +. Не должна повторяться с уже назначенной категорией.
- **Удалить категории** - выберите из списка назначенную категорию и нажмите +. Не должна повторяться с добавляемой категорий.
- **Комментарий** - необязательное поле. Не более 256 символов.

2. Нажмите **Добавить**.

Управление правилами

В столбце **Управление** можно включать или выключать правило переопределения, редактировать и удалять. Правила применяются сразу после создания или включения:



При наличии большого количества правил в таблице воспользуйтесь кнопкой **Фильтры**.

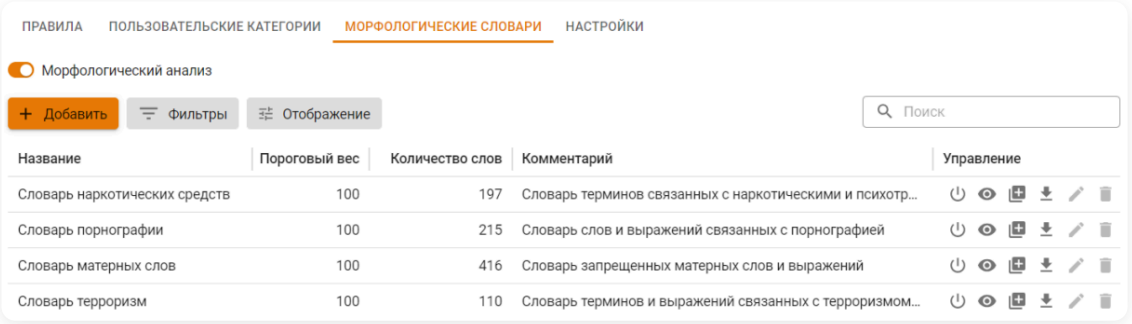
Если в таблице добавленные категории отмечены как удаленные:
1. Удалите неактуальную категорию.
2. При необходимости добавьте близкую по тематике.

Морфологические словари

Функциональность доступна в **Классическом** и **Системном контекстах**.

На вкладке **Морфологические словари** создаются и редактируются словари для проведения морфологического анализа сайтов. Если в тексте анализируемого сайта содержится достаточное для блокировки количество предварительно заданных слов и словосочетаний, доступ к ресурсу блокируется.

Для активации морфологического анализа включите опцию **Морфологический анализ**:



Для работы морфологического анализа требуется:

- Наличие хотя бы одного **включенного словаря**. Если ни один словарь не включен, морфологический анализ не проводится.
- Расшифровка трафика - создайте правило расшифровки в **Контент-фильтре**.

В Ideco NGFW Novum предустановлены четыре словаря (по умолчанию отключены):

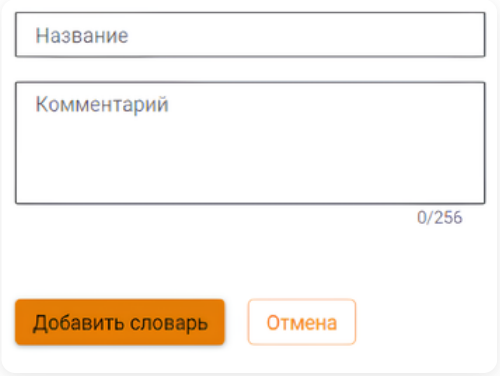
- Словарь наркотических средств
- Словарь порнографии
- Словарь матерных слов
- Словарь терроризм

Предустановленные словари можно включать или отключать, но нельзя редактировать и удалять.

Добавление морфологического словаря

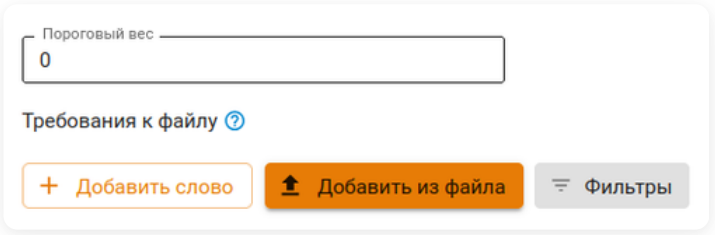
1. Нажмите **Добавить** и заполните поля:

Описание



- **Название** - название добавляемого словаря.
- **Комментарий** - произвольный текст. Значение не должно быть длиннее 255 символов.

Слова



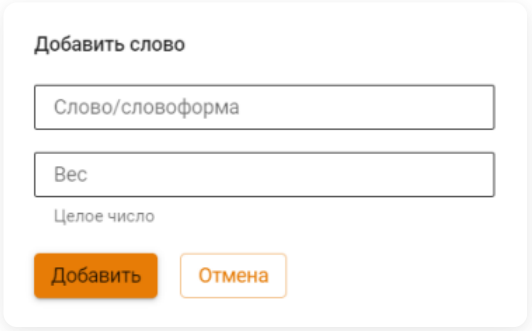
- **Пороговый вес** - общий вес указанных в настройках словаря слов (целое число от 0 до 2 147 483 648).

> Если при проверке сайта общий вес найденных на нем слов превысит пороговый, доступ к сайту будет заблокирован.

Добавьте слова для блокировки трафика вручную или загрузите из файла:

Вручную

Нажмите **Добавить слово** и заполните поля:



- **Слово/словоформа** - введите слово или словосочетание для блокировки трафика.
- **Вес** - укажите целое число.

Загрузка из файла

Нажмите **Добавить из файла** и выберите файл. В один словарь можно загружать несколько файлов. В этом случае дублирующиеся слова будут удалены, останется только одно вхождение с установленным весом.

Требования к загрузке из файла:

- Формат файла - CSV, кодировка - UTF-8.
- В одной строке должно быть одно слово или словосочетание и вес, разделенные точкой с запятой (`;`).
- Допустимо не указывать вес слова. В этом случае по умолчанию к каждому слову/словосочетанию без веса применится значение `20`, а файл будет представлять собой список без разделителей.

При неудачной загрузке файла появится окно с уведомлением **Файл не соответствует требованиям**.

Примеры файлов

- **Файл с указанием веса:**

```
слово;20
словосочетание;20
```

- **Файл без указания веса:**

```
слово
словосочетание
```

Пример работы:

При загрузке файлов и при **Пороговом значении** = `100` доступ к сайту будет заблокирован, если на сайте найдено 5 и более совпадений ("слово" и/или "словосочетание").

> Чтобы снизить вероятность блокировки сайта из-за морфологического анализа, уменьшите вес слов. Для повышения вероятности блокировки - увеличьте вес.

2. Для сохранения настроек нажмите **Добавить словарь**.

Если в таблице большое количество морфологических словарей, воспользуйтесь кнопкой **Фильтры**.

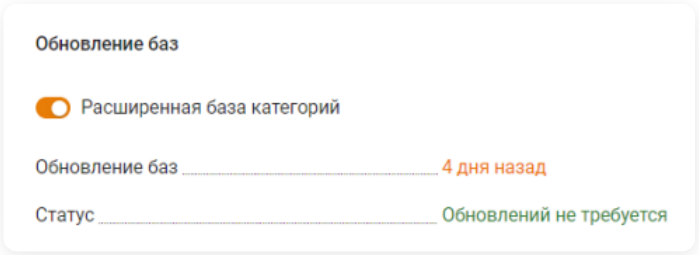
Результат морфологического анализа представлен в разделе **Отчеты и журналы** → **Веб-трафик**:

			Контент-фильтр					Антивирус		Источник				Наз...	
Д...	Резуль...	Причина	Резуль...	Расш...	Названи...	Категории сайта	Категория сработки	Резул...	Проф...	IP-адрес	Польз...	Группа	URL	IP-ад...	Общий, МБ
30.06....	✗	Словарь порнографии	✗	✗	–	Компьютерные и...	–	✓	defau...	192.16...	Mstisl...	Support	safeb...	8.8....	0,00
30.06....	✗	Словарь порнографии	✗	✗	–	Юмор	–	✓	defau...	192.16...	Pavel ...	Office	beac...	7.7....	0,01

Настройки

Обновление баз

Активация опции **Расширенная база категорий** включает автоматически обновляемые Расширенные категории, доступные при активной подписке в платных версиях продукта:



Если отключить опцию **Расширенная база категорий**, то все правила, включающие **Расширенные категории**, перестанут срабатывать.

Настройки безопасности

Блокировать протоколы QUIC и HTTP/3 - протоколы, используемые современными браузерами для доступа к ресурсам (например, Google и YouTube). Рекомендуется заблокировать QUIC и HTTP/3, иначе будет невозможно фильтровать ресурсы, работающие по данным протоколам. Заблокированный трафик нельзя исключить через списки исключений в **Прокси** → **Исключения**.

Безопасный поиск - принудительно включает безопасный поиск в поисковых системах (Google, Yandex, YouTube, Yahoo, Bing, Rambler).

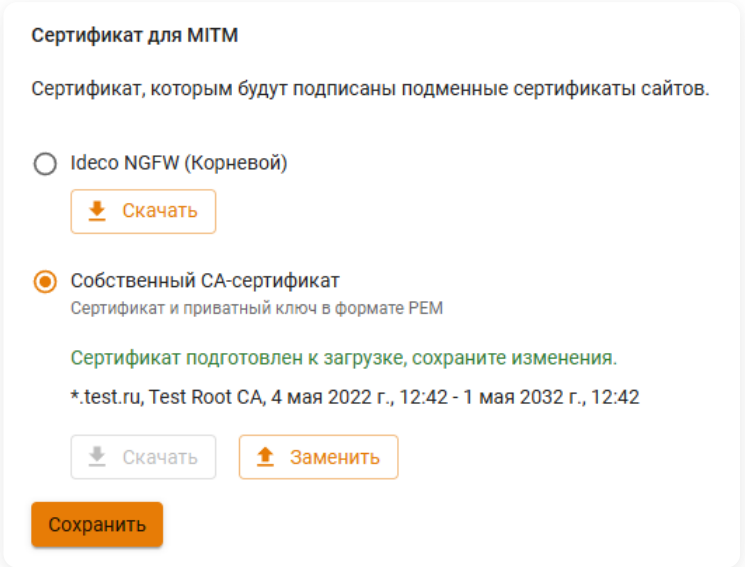
Для корректной работы необходимо включить HTTPS-фильтрацию с подменой сертификата для этих сервисов.

Сертификат для MITM

Если для повторного шифрования требуется использовать сторонний сертификат (не корневой сертификат Ideco NGFW Novum):

1. Нажмите **Загрузить** и выберите нужный сертификат.

2. Сохраните изменения:



Требования к стороннему сертификату:

- Должен быть выдан удостоверяющим центром **Certificate Authority**.
- Имеет расширение **.pem**.
- Содержит приватный ключ.

Настройка фильтрации HTTPS

В Ideco NGFW Novum фильтрация реализуется следующими методами:

- **Анализ заголовков Server Name Indication (SNI)** - благодаря этому методу возможен анализ домена, к которому подключается клиент, без подмены сертификата и вмешательства в HTTPS-трафик. Также анализируются домены, указанные в сертификате. Фильтрация HTTPS по SNI включена по умолчанию.
- **Метод SSL-bump** - фильтрация происходит путем динамической подмены сертификата сайта на **корневой сертификат Ideco NGFW Novum**. Таким образом, передающийся по защищенному HTTPS-соединению трафик становится доступным для обработки всем модулям Ideco NGFW Novum: антивирусу Касперского, внешним ICAP-сервисам и Контент-фильтру (можно категоризировать полный URL запроса и MIME-тип контента).

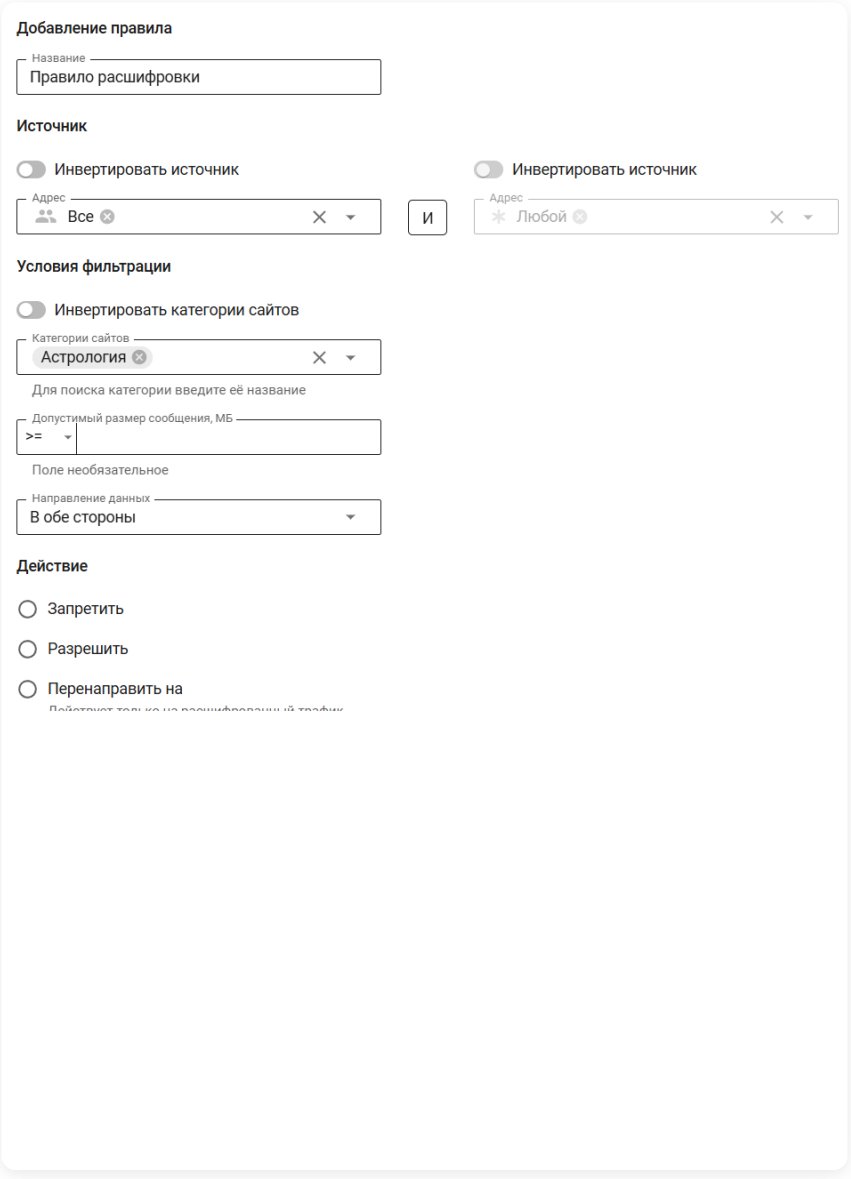
Настройка сервера и рабочих станций

Для работы SSL-bump требуется **настройка на обеих сторонах подключения**: сервера Ideco NGFW Novum и рабочей станции каждого пользователя в локальной сети.

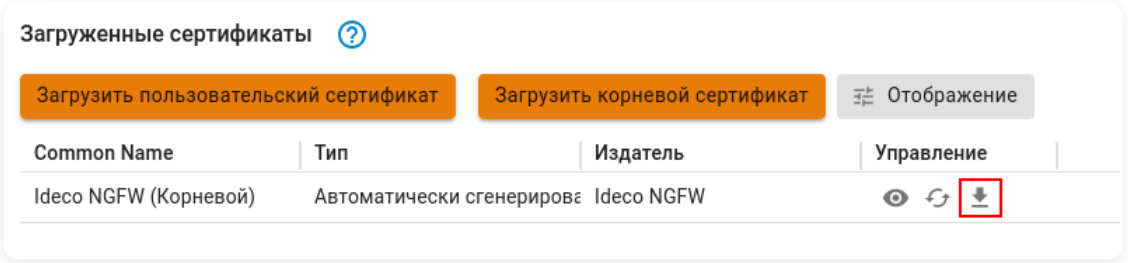
Настройка сервера Ideco NGFW Novum

1. Создайте правило расшифровки HTTPS-трафика в **Правила трафика** → **Контент-фильтр** → **Правила**. Создание правил подробно описано в статье.

Пример правила для расшифровки:



2. Скачайте корневой SSL-сертификат в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



Установка корневого сертификата на рабочей станции

При включенном правиле расшифровки HTTPS-трафика клиентские приложения (браузер, антивирусы, клиенты IM и другое сетевое ПО) потребуют подтверждения для подменного сертификата. Чтобы исключить появление предупреждений безопасности, установите корневой сертификат сервера Ideco NGFW Novum в операционной системе.

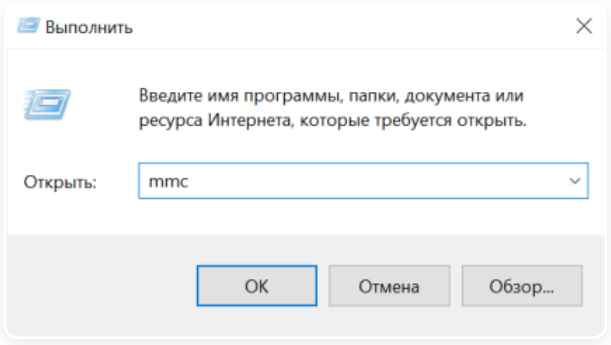
Установка сертификата на Linux

Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

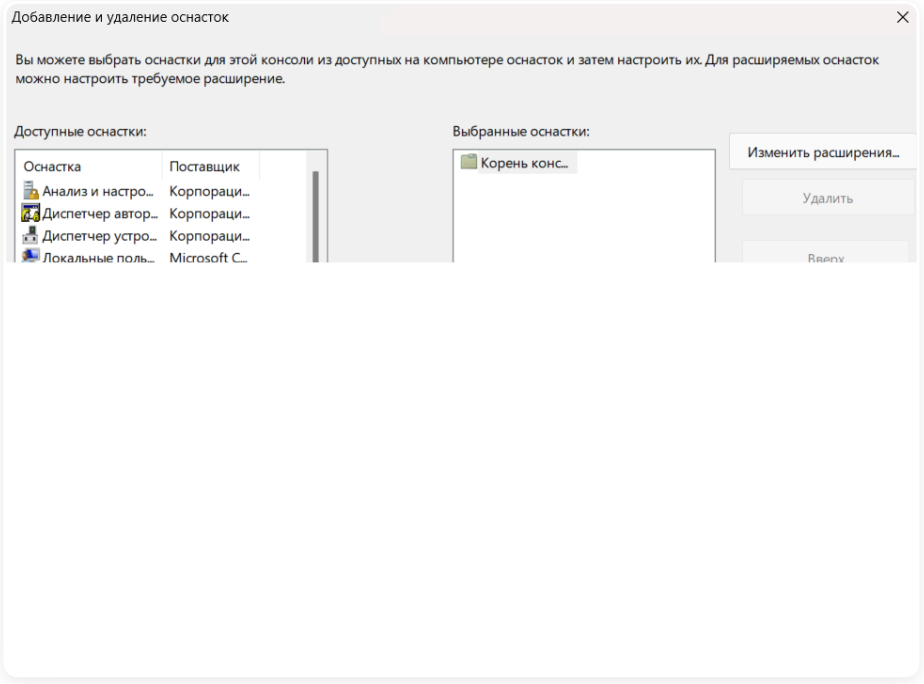
Установка сертификата на Windows

1. Откройте на рабочей станции центр управления сертификатами: **Пуск** → **Выполнить**, выполнив в диалоге команду **mmc**:



2. В меню **Файл** выберите **Добавить или удалить оснастку**:

3. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите кнопку **Добавить**:



4. В открывшемся окне выберите пункт **Учетной записи компьютера** и нажмите кнопку **Далее**:

5. В окне **Выбор компьютера** оставьте флаг **Локальный компьютер** и нажмите кнопку **Готово**.

6. В левой части окна нажмите на стрелку рядом с директорией **Сертификаты (локальный компьютер)** → **Доверенные корневые сертификаты** → **Сертификаты**:

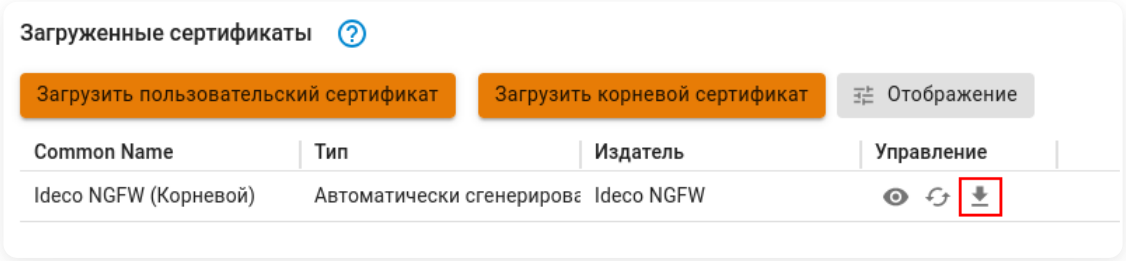
7. В меню **Действие** выберите **Все задачи** → **Импорт**:

8. Следуя инструкциям Мастера импорта сертификатов, импортируйте корневой сертификат сервера Ideco NGFW Novum. Импортированный сертификат появится в списке в правой части окна:

Автоматическая установка сертификата через Active Directory

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, можно установить сертификат Ideco NGFW Novum для всех пользователей автоматически с помощью Active Directory. Для этого необходимо выполнить действия:

1. Скачайте корневой SSL-сертификат в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



2. Зайдите на контроллер домена с правами администратора.

3. Запустите оснастку управления групповой политикой, выполнив команду **gpmc.msc**.

4. Найдите **политику домена**, использующуюся на компьютерах пользователей в **Объектах групповой политики** (Default Domain Policy). Нажмите на нее правой кнопкой мышки и выберите **Изменить**.

5. В открывшемся редакторе управления групповыми политиками выберите: **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Политики открытого ключа** → **Доверенные корневые центры сертификации**.

6. Нажмите правой кнопкой мыши по открывшемуся списку, выберите **Импорт** и импортируйте ключ Ideco NGFW Novum:

7. После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Настройка повторного шифрования трафика

1. В **Сервисы** → **Сертификаты** → **Загруженные сертификаты** загрузите сертификат, который будет использоваться для шифрования.

2. Перейдите в **Правила трафика** → **Контент-фильтр** → **Настройки**.

3. Выберите в пункте **Сертификат для MITM** сертификат, загруженный на шаге 1.

> Клиенты должны иметь загруженный сертификат в доверенных хранилищах. Рекомендации по настройке компьютера пользователя можно найти в разделе **Установка корневого сертификата на рабочей станции**.

Возможные проблемы и методы решения

Проблема	Решение
Включения расшифровки трафика может быть недостаточно для подмены сертификата некоторых сайтов (например, `ya.ru`, `google.com`).	Включить опцию **Блокировать протоколы QUIC и HTTP/3** в **Правила трафика** → **Контент-фильтр** → **Настройки**.

Проблема	Решение
Браузер не использует системное хранилище сертификатов.	1. Добавить сертификат Ideco NGFW Novum в доверенные сертификаты браузера. 2. В Mozilla Firefox присвоить параметру `security.enterprise_roots.enabled` (в **about:config**) значение `true` для доверия системным сертификатам.
На локальной машине используется антивирус, проверяющий HTTPS-трафик методом подмены сертификатов (сайты могут не открываться из-за двойной подмены сертификатов).	Отключить в настройках антивируса проверку HTTPS-трафика.
Обработка HTTPS-трафика по умолчанию (анализ SNI). NGFW Novum не пропускает по HTTPS-порту трафик, отличный от HTTPS.	Разрешить обход прокси-сервера к нужным ресурсам.
Блокировка HTTPS-ресурсов без отображения страницы блокировки.	Настроить доверие корневому SSL-сертификату NGFW Novum (даже при включенной только SNI-фильтрации), так как при блокировке HTTPS-ресурса будет применен SSL-bumping с подстановкой SSL-сертификата NGFW Novum для подмены контента ресурса страницей о блокировке сервером.

Полезные ссылки

- **Установка корневого сертификата на Astra Linux**
- **Установка корневого сертификата на Alt Linux**
- **Установка корневого сертификата на Red OS**
- **Установка корневого сертификата на Ubuntu/Debian**
- **Использование собственного CA-сертификата в Контент-фильтре**
- **Настройка HTTP-метода**
- **Настройка MIME-типов**

Ограничение скорости

Классический контекст | Высокопроизводительный контекст

> Служба предназначена для ограничения скорости входящего интернет-трафика для пользователей сети.

Название службы раздела **Ограничение скорости**: `ideco-shaper-backend`.

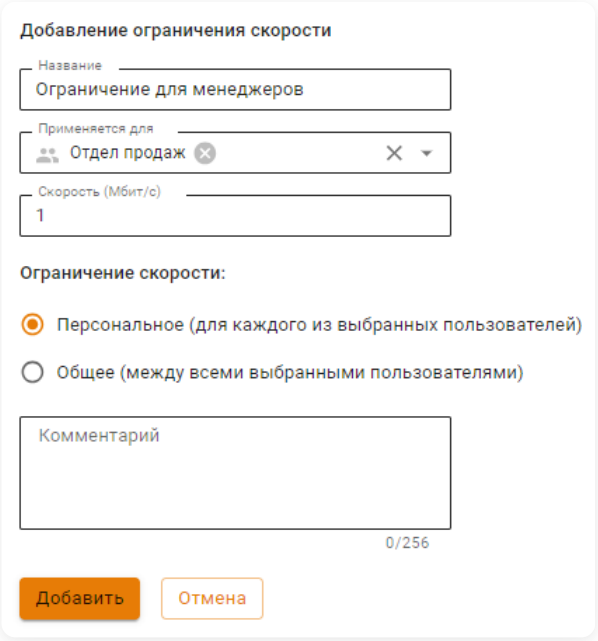
Список имен служб для других разделов доступен по ссылке.

В разделе **Ограничение скорости** создаются правила, позволяющие ограничить скорость входящего интернет-трафика для пользователей сети.

Модуль **Ограничение скорости** работает только при наличии хотя бы одного включенного правила. Если правила не созданы или все отключены, модуль будет находиться в статусе **Остановлен**.

Для исключения пользователя или групп пользователей из обработки правил **Ограничения скорости** добавьте соответствующее правило в разделе **Исключения**.

1. Для создания правила в **Правила трафика** → **Ограничение скорости** нажмите **Добавить** и заполните поля:

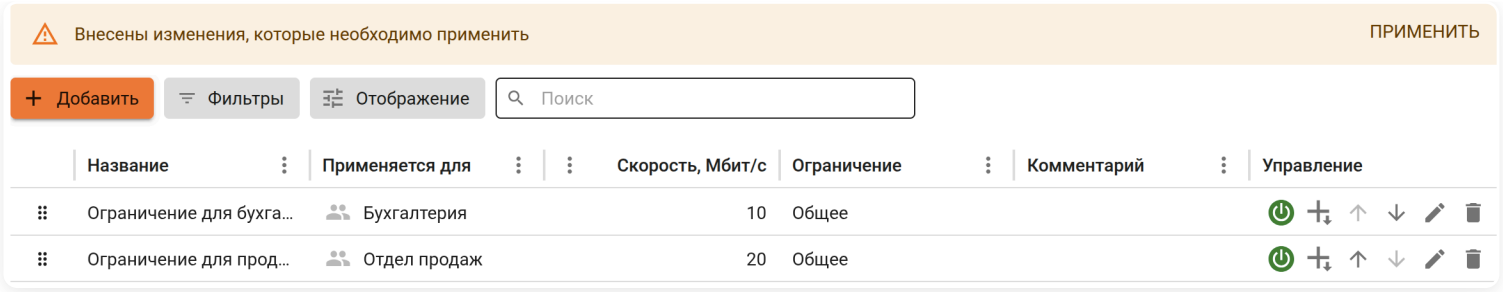


Расшифровка полей

- **Название** - введите название правила, например, Ограничение для менеджеров.
- **Применяется для** - выберите из выпадающего списка пользователя, группу и/или IP-адрес.
- **Скорость (Мбит/с)** - укажите лимит скорости.
- **Ограничение скорости** - выберите тип ограничения скорости:
  - **Персональное** - скорость будет ограничена для каждого из выбранных пользователей. Если под одной учетной записью авторизованы несколько устройств, каждое устройство получает отдельный полный лимит скорости.
  - **Общее** - скорость будет ограничена и разделится между всеми выбранными пользователями. Если под одной учетной записью авторизованы несколько устройств, суммарный лимит распределяется между всеми устройствами.

2. Нажмите **Добавить**.

3. Для применения созданного правила нажмите **Применить** над таблицей:



Если не применить правило и покинуть раздел **Ограничение скорости**, то созданное правило сохранится, но не будет действовать. Для применения правила вернитесь в раздел **Ограничение скорости** и нажмите **Применить**.
Не примененные правила будут удалены:

- При перезагрузке сервера.
- При переключении на другую ноду кластера.

В столбце **Управление** можно:

Включать или выключать правило.
Менять приоритет.
Редактировать правило.
Удалять правило.

При наличии большого количества правил в таблице воспользуйтесь кнопкой **Фильтры**.

Порядок применения правил

Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. То есть, если пользователь одновременно находится в нескольких группах, то к нему применяется правило, которое находится выше в списке правил.

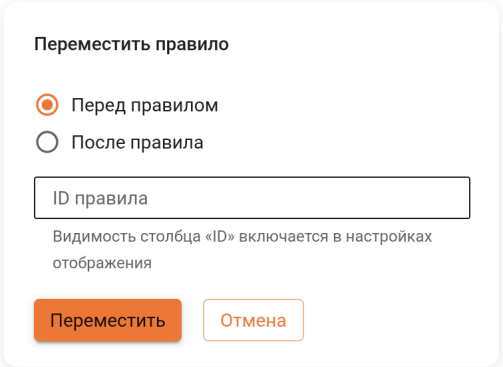
Правила **Ограничения скорости** не обрабатывают трафик между локальными сетями и сетями филиалов. Пользователи VPN приравниваются к пользователям локальных сетей.

Перемещение правил

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



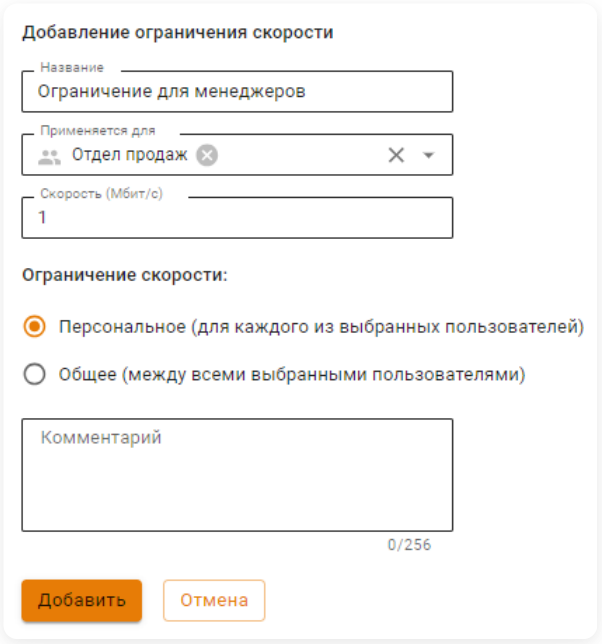
4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Примеры использования

Персональное ограничение

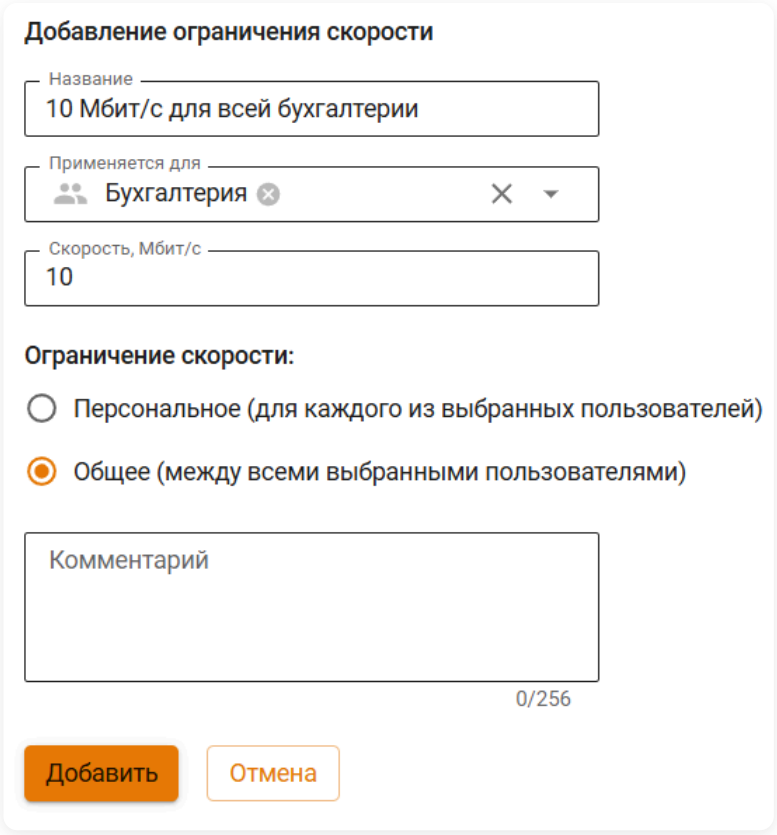
При выборе персонального ограничения скорости лимит скорости для каждого менеджера будет равен 1 Мбит/с:



Если под одной учетной записью авторизованы несколько устройств, каждое устройство получает полный лимит скорости: если задано ограничение 1 Мбит/с и авторизованы три устройства, каждое устройство получит 1 Мбит/с.

Общее ограничение

При выборе общего ограничения ширина канала для всей бухгалтерии будет равна 10 Мбит/с:



Если под одной учетной записью авторизованы несколько устройств, лимит скорости распределяется между всеми устройствами: если задано ограничение 10 Мбит/с и авторизованы три устройства, суммарная скорость для всех трех устройств составит 10 Мбит/с.

Полезные ссылки

- **Исключения**
- **Учетные записи**
- **Объекты**

Предотвращение вторжений

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Предотвращение вторжений**: `ideco-suricata`, `ideco-suricata-backend`, `ideco-suricata-event-syncer`, `ideco-suricata-profiles-syncer`, `ideco-suricata-profiles-syncer-backend`.

Список имен служб для других разделов доступен по ссылке.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE



Система **Предотвращения вторжений** (IDS/IPS, Intrusion detection system / Intrusion prevention system) предназначена для:

- [x] Обнаружения
- [x] Журналирования
- [x] Предотвращения атак злоумышленников на сервер, интегрированные службы и локальную сеть

Раздел состоит из трех вкладок:

- Группы сигнатур - список предустановленных групп сигнатур, распределенных по тактикам согласно матрице MITRE ATT&CK или в табличном виде.
- Пользовательские сигнатуры - позволяет добавить сигнатуры для обработки системой **Предотвращения вторжений**.
- Настройки - информация об обновлениях баз IPS и сетях, защищенных от вторжения.

Требования

Система **Предотвращения вторжений** доступна только в Enterprise-версии Ideco NGFW Novum с активной подпиской на обновления.

- Объем оперативной памяти - от 16 ГБ.
- Процессор - от 4 ядер.

После включения системы проверьте в разделе **Мониторинг** → **Графики загруженности**, что мощности процессора достаточно для анализа всего проходящего трафика.

Особенности настройки Межсетевого экрана и системы Предотвращение вторжений

- **Межсетевой экран** Ideco NGFW Novum анализирует трафик для поиска подходящего правила и применяет правило. Если в таблице есть несколько правил с одними и теми же условиями, применяется правило, стоящее выше по списку. Запрещающие правила **Межсетевого экрана** сразу блокируют соответствующий трафик, который не проходит дополнительную проверку в системе **Предотвращение вторжений**.
- Чтобы через модуль **Предотвращение вторжений** проходил трафик, для которого нет разрешающего правила в таблице **FORWARD** или **INPUT**, рекомендуем создать и включить в **Межсетевой экране** правило с источником **Любой** и назначением **Любой**, разместив правило в конец

таблицы. В этом случае трафик, который не был найден в правилах **Межсетевого экрана**, но соответствует профилям IPS, пройдет проверку системой **Предотвращения вторжений**.

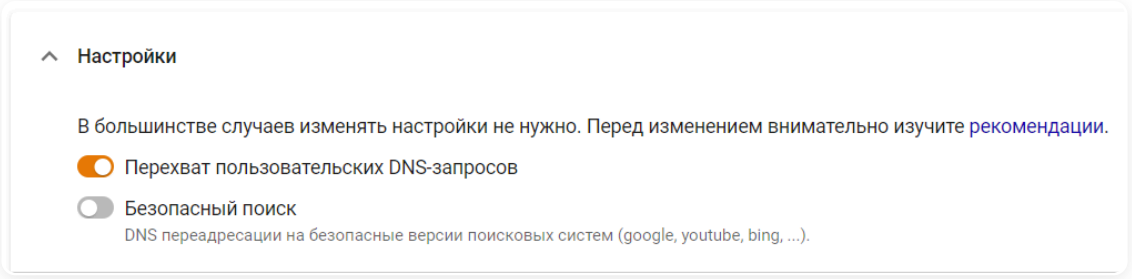
- Если в одном правиле **Межсетевого экрана** включены проверки и **Контролем приложений**, и системой **Предотвращения вторжений**, трафик сначала попадет в обработку DPI, затем - IPS.
- Чтобы трафик фильтровался системой **Предотвращение вторжений**, создайте для всех локальных интерфейсов правило **FORWARD**, содержащее нужный профиль безопасности.

С 18 версии Ideco NGFW Novum механизм работы системы **Предотвращения вторжений** изменился, появились возможности:

- [x] Работать с правилами IPS на уровне сигнатур, фильтровать и просматривать в удобном виде
- [x] Составлять независимые друг от друга наборы правил IPS и применять только к необходимому трафику с помощью профилей системы **Предотвращения вторжений**, которые назначаются в правилах **Межсетевого экрана**

Особенности обработки DNS-запросов

При включенной опции **Перехват пользовательских DNS-запросов** в **Сервисы** → **DNS** → **Внешние DNS-серверы** трафик обрабатывается не как **FORWARD**, а как **INPUT**:



Если опция **Перехват пользовательских DNS-запросов** включена (по умолчанию включена), создайте правила **INPUT** для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

Настройка обработки трафика

Чтобы система **Предотвращения вторжений** обрабатывала трафик:

1. Перейдите в **Правила трафика** → **Предотвращение вторжений** и включите работу системы:



2. Создайте необходимые профили IPS в **Профили безопасности** → **Предотвращение вторжений**.

3. Примените их в правилах Межсетевого экрана.

> В обработку трафика не попадают:
>
> - Сигнатуры, не включенные ни в один профиль.
> - Профили, не используемые в правилах **Межсетевого экрана**.

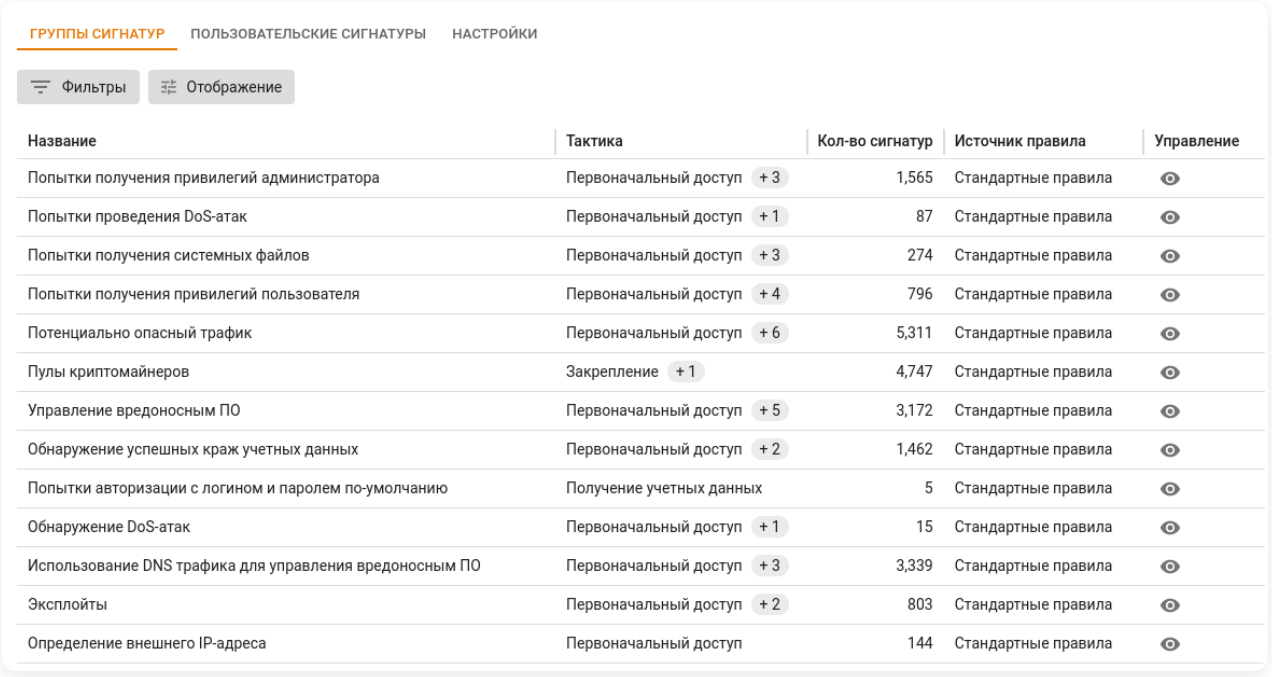
Полезные ссылки

- **Подробнее о Load Average**
- **Блокировка популярных ресурсов**

Группы сигнатур

Классический контекст | Высокопроизводительный контекст

На вкладке **Группы сигнатур** доступны для просмотра пользовательские и предустановленные сигнатуры:



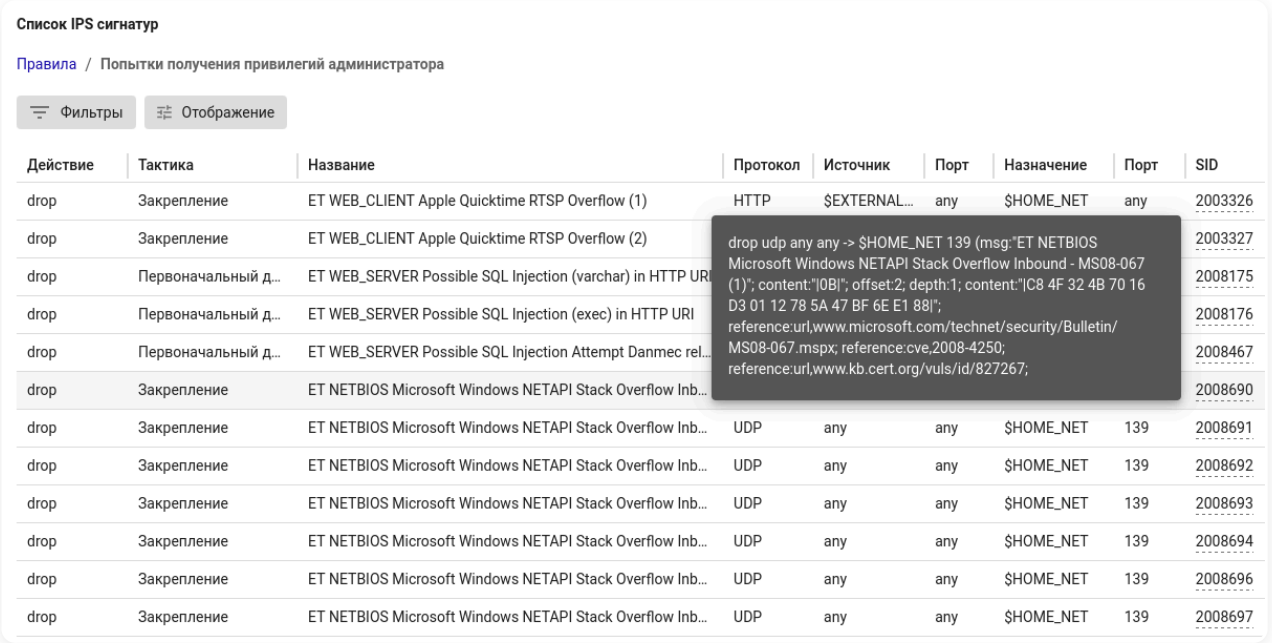
ГРУППЫ СИГНАТУР | ПОЛЬЗОВАТЕЛЬСКИЕ СИГНАТУРЫ | НАСТРОЙКИ

Фильтры | Отображение

Название	Тактика	Кол-во сигнатур	Источник правила	Управление
Попытки получения привилегий администратора	Первоначальный доступ +3	1,565	Стандартные правила	
Попытки проведения DoS-атак	Первоначальный доступ +1	87	Стандартные правила	
Попытки получения системных файлов	Первоначальный доступ +3	274	Стандартные правила	
Попытки получения привилегий пользователя	Первоначальный доступ +4	796	Стандартные правила	
Потенциально опасный трафик	Первоначальный доступ +6	5,311	Стандартные правила	
Пулы криптомайнеров	Закрепление +1	4,747	Стандартные правила	
Управление вредоносным ПО	Первоначальный доступ +5	3,172	Стандартные правила	
Обнаружение успешных краж учетных данных	Первоначальный доступ +2	1,462	Стандартные правила	
Попытки авторизации с логином и паролем по-умолчанию	Получение учетных данных	5	Стандартные правила	
Обнаружение DoS-атак	Первоначальный доступ +1	15	Стандартные правила	
Использование DNS трафика для управления вредоносным ПО	Первоначальный доступ +3	3,339	Стандартные правила	
Эксплойты	Первоначальный доступ +2	803	Стандартные правила	
Определение внешнего IP-адреса	Первоначальный доступ	144	Стандартные правила	

Чтобы увидеть сигнатуры, входящие в группу, нажмите на .

Чтобы увидеть содержание сигнатуры, наведите курсор мыши на SID:



Список IPS сигнатур

Правила / Попытки получения привилегий администратора

Фильтры | Отображение

Действие	Тактика	Название	Протокол	Источник	Порт	Назначение	Порт	SID
drop	Закрепление	ET WEB_CLIENT Apple Quicktime RTSP Overflow (1)	HTTP	$EXTERNAL...	any	$HOME_NET	any	2003326
drop	Закрепление	ET WEB_CLIENT Apple Quicktime RTSP Overflow (2)						2003327
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection (varchar) in HTTP URI						2008175
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection (exec) in HTTP URI						2008176
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection Attempt Danmec rel...						2008467
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...						2008690
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008691
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008692
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008693
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008694
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008696
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008697

drop udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (1)"; content:"|0B|"; offset:2; depth:1; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267;

Описание групп сигнатур

- **DNS поверх HTTPS** - обнаруживает и блокирует попытки скрыть DNS-запросы путем туннелирования через TLS/SSL (DNS поверх HTTPS). Правила анализируют трафик, чтобы выявить характерные для DoH-сессий доменные имена, используемые для обхода стандартных механизмов DNS-фильтрации. Такие методы злоумышленники могут применять для обхода сетевых политик, утечки данных или скрытого управления зараженными системами. Применение этих правил помогает предотвратить несанкционированное использование DoH.

- **SSL-сертификаты, используемые вредоносным ПО и ботнетами** - обнаруживает использование SSL-сертификатов, которые вредоносное ПО и ботнеты применяют для установления защищенных TLS-соединений с командными центрами злоумышленников (C2). Система анализирует отпечатки SSL-сертификатов, присутствующих в трафике, и выявляет попытки скрыть коммуникации посредством легитимно выглядящих шифрованных каналов. При обнаружении совпадений с известными вредоносными отпечатками такие соединения блокируются. Это предотвращает скрытое управление зараженными системами и снижает риск утечки данных и распространения кибератак.
- **Авторизация с подозрительным логином** - обнаруживает попытки авторизации с использованием подозрительных логинов, которые говорят о фишинговых атаках, переборе паролей или применении специализированных эксплойтов для несанкционированного доступа. Выявление таких аномалий позволяет своевременно блокировать соединения, предотвращая компрометацию систем и утечку данных.
- **Анонимайзеры** - обнаруживает использование анонимайзеров для сокрытия истинного источника трафика и возможного обхода систем контроля доступа. Определяются ключевые маркеры, связанные с различными сервисами анонимизации. Злоумышленники могут применять эти технологии для маскировки атак, утечек данных и обхода корпоративных политик безопасности, что делает их важными для своевременного обнаружения и блокировки.
- **Атаки на получение прав пользователя** - обнаруживает попытки получить несанкционированный доступ к учетным данным через эксплуатацию уязвимостей системы и применить специализированные инструменты. Анализируя сетевой трафик, фиксируются характерные маркеры атак, такие как выполнение команд для изменения настроек, обращения к реестру и т.д. Выявление подобной активности позволяет своевременно блокировать подозрительные соединения, предотвращая компрометацию систем и утечку конфиденциальной информации.
- **Атаки на получение привилегий администратора** - обнаруживает попытки получить административные привилегии с использованием уязвимостей и эксплойтов для эскалации прав. Анализируя сетевой трафик, определяет характерные маркеры активности. Такие действия могут указывать на внедрение вредоносного ПО или бэкдоров, что позволяет своевременно блокировать атаки и предотвращать компрометацию критически важных систем.
- **Блокирование активности троянских программ** - обнаруживает попытки эксплуатировать троянские программы, направленные на скрытую передачу данных, удаленно управлять зараженными системами, утечку конфиденциальной информации и др. Анализируя сетевой трафик, выявляет характерные маркеры активности вредоносных троянов - специфичные сигнатуры пакетов, аномальные HTTP-запросы, подозрительные команды и нестандартные DNS-запросы, связанные с ransomware. Блокировка таких соединений предотвращает дальнейшее распространение атак и защищает критически важные данные.
- **Блокирование атак** - обнаруживает попытки атак, направленные на эксплуатацию уязвимостей информационных систем, проведение сканирования портов, удаленное выполнение кода и другие методы вторжения. Анализирует входящий и исходящий сетевой трафик, фиксируя характерные сигнатуры эксплойтов, аномалии в пакетах, нестандартные команды и подозрительные запросы, указывающие на попытки получить несанкционированный доступ, провести DoS-атаки или обойти защитные механизмы. Оценивает репутацию IP-адресов и блокирует трафик, исходящий с адресов, имеющих негативную репутацию или принадлежащих к известным нодам Tor. Это позволяет предотвращать компрометацию инфраструктуры, утечку конфиденциальных данных и нарушение стабильности работы сетевых ресурсов.
- **Блокирование крупных утечек информации** - обнаруживает попытки несанкционированного экспорта данных из систем. Анализируя пакеты, фиксирует характерные маркеры экспорта и специфичные заголовки, свидетельствующие о массовой передаче конфиденциальной информации. Это позволяет оперативно блокировать такие соединения и предотвращать утечку критически важных данных.
- **Блокирование некорректных попыток получения привилегий пользователя** - обнаруживает попытки получить привилегии пользователя посредством некорректных или несанкционированных аутентификаций, которые могут указывать на попытки перебора или взлома учетных записей. Анализируя ответы серверов с сообщениями типа "Login failed", "Invalid login" и другие индикаторы неудачных входов, фиксирует подозрительные активности в протоколах FTP, SSH, RPC, SQL и других службах. Это позволяет оперативно блокировать подобные соединения, снижая риск компрометации учетных данных и предотвращая дальнейшие атаки.
- **Блокирование подозрительных RPC-запросов** - обнаруживает подозрительные RPC-запросы, предназначенные для вызова удаленных функций на сервере. Подозрительные RPC-запросы могут свидетельствовать о попытках эксплуатации уязвимостей или несанкционированного выполнения команд. Анализируя как UDP, так и TCP-трафик, фиксирует аномальные структуры пакетов, неверные параметры и нестандартные последовательности байтов, характерные для вредоносных активностей. Это позволяет оперативно блокировать подозрительные запросы, предотвращая потенциальное выполнение нежелательного кода и компрометацию систем.
- **Блокирование попыток запуска исполняемого кода** - обнаруживает попытки запуска исполняемого кода, направленные на удаленное выполнение команд и получение несанкционированного доступа к системам. Анализирует сетевой трафик на предмет характерных сигнатур RCE, включая специфичные байтовые последовательности, связанные с PHP object deserialization, веб-шеллами, Log4Shell и другими эксплойтами. Фиксирует аномалии в HTTP, TCP и UDP-запросах, что позволяет оперативно блокировать вредоносные попытки выполнения shellcode и предотвращать компрометацию целевых систем.
- **Блокирование утечек информации** - обнаруживает попытки несанкционированного извлечения конфиденциальных данных через сетевые протоколы. Анализируя входящий и исходящий трафик, фиксирует передачу содержимого критически важных файлов, а также различной системной информации. Выявление таких индикаторов утечки позволяет оперативно блокировать подозрительные соединения, предотвращая утечку секретных данных и снижая риск компрометации систем.
- **Запросы на скомпрометированные ресурсы** - обнаруживает нарушения корпоративных политик, связанные с обращениями к ресурсам, имеющим подозрительную репутацию. Правила фиксируют случаи, когда сетевой трафик указывает на несанкционированное использование различных протоколов, автоматизацию браузера или передачу данных в виде незащищенного контента. Такие сигнатуры служат индикаторами потенциального нарушения корпоративной безопасности, позволяя своевременно выявлять и блокировать подобные подключения.
- **Индикаторы компрометации ФинЦЕРТ** - обнаруживает и блокирует трафик с вредоносными файлами, а также попытки обращения к доменным именам, которые включены в бюллетени ФинЦЕРТ.
- **Использование DNS-трафика для управления вредоносным ПО** - обнаруживает попытки использовать DNS-трафик для управления вредоносным ПО, когда зараженные системы обращаются к серверам команд и контроля (C2) для получения инструкций. Анализируя DNS-запросы, TLS SNI и HTTP-заголовки, фиксирует обращения к известным вредоносным доменам и серверам, выявляя характерные паттерны связи с C2-инфраструктурой. Это позволяет оперативно блокировать такие соединения, предотвращая удаленное управление, утечку данных и дальнейшее распространение вредоносного кода.
- **Нежелательное программное обеспечение** - обнаруживает попытки использовать нежелательное программное обеспечение, включая adware и потенциально нежелательные утилиты, которые могут собирать и передавать конфиденциальные данные или связываться с вредоносными серверами. Анализируя HTTP, DNS и TLS-трафик, фиксирует характерные сигнатуры, специфичные запросы и уникальные идентификаторы,

связанные с подобной активностью. Это позволяет блокировать подозрительные соединения, предотвращать утечки информации и снижать риск компрометации конечных устройств.

- **Неизвестный тип трафика** - обнаруживает неопознанный трафик, который не соответствует стандартным протоколам или содержит аномальные, подозрительные шаблоны поведения. Анализирует HTTP-запросы, TLS-соединения и DNS-сообщения на предмет нестандартных User-Agent, специфических JA3-хешей, необычных кодировок, пустых или искаженных заголовков и прочих аномалий. Такие признаки могут указывать на попытки сканирования, обхода защитных механизмов или эксплуатацию уязвимостей. Выявление подобного трафика позволяет оперативно блокировать несанкционированное взаимодействие и снижать риск кибератак.
- **Нецелевое использование стандартных портов** - обнаруживает случаи нецелевого использования стандартных портов, когда сервисы, предназначенные для определенных протоколов, применяются для нелегитимных целей. Анализируя сетевой трафик, фиксирует аномальные подключения, при которых стандартный порт используется для обхода политик безопасности, скрытой передачи данных или запуска вредоносных операций. Это позволяет своевременно блокировать подозрительные соединения и предотвращать попытки эксплуатации инфраструктуры в обход установленных правил.
- **Обнаружение нарушений стандартов сетевых протоколов** - обнаруживает обращения по нестандартным или модифицированным протоколам, отклоняющимся от официальных спецификаций. Анализируя сетевой трафик, фиксирует аномальные баннеры, команды и последовательности данных, которые могут свидетельствовать о попытках обхода стандартных механизмов защиты или эксплуатации уязвимостей. Выявление таких нарушений позволяет оперативно блокировать трафик, не соответствующий протокольным стандартам, и предотвращать несанкционированный доступ и передачу вредоносного кода.
- **Обнаружение подозрительной сетевой активности** - обнаруживает аномалии в сетевом трафике, связанные с нестандартными или подозрительными действиями легитимных пользователей. Анализируя различные протоколы, включая HTTP, TCP, UDP, TLS и DNS, фиксирует отклонения от нормального поведения, такие как частые попытки подключения, необычные запросы или аномальные данные, которые могут свидетельствовать о сканировании сети, автоматизированных атаках или обходе защитных механизмов. Это позволяет своевременно выявлять и блокировать потенциально вредоносный трафик.
- **Обнаружение подозрительных команд** - обнаруживает команды, нехарактерные для стандартного поведения систем, которые злоумышленники могут использовать для обхода защитных мер. Анализируя сетевой трафик, фиксирует аномальные запросы и нестандартные вызовы, например, обращения к зарезервированным ресурсам (COM1, LPT1, LPT4, NULL), что свидетельствует о попытках эксплуатации и несанкционированного доступа. Блокировка таких команд помогает предотвратить возможные атаки и сохранить целостность информационных систем.
- **Обнаружение успешных краж учетных данных** - обнаруживает попытки несанкционированного извлечения учетных данных, направленные на получение логинов, паролей и другой конфиденциальной информации. Анализируя содержимое HTTP-запросов, POST-данные и серверные ответы, фиксирует характерные шаблоны фишинговых атак. Также учитываются сообщения об ошибках аутентификации, указывающие на успешное компрометирование учетных записей, что позволяет оперативно блокировать атаки и предотвращать утечку данных.
- **Определение внешнего IP-адреса** - обнаруживает попытки определения внешнего IP-адреса, когда внутренние системы обращаются к внешним сервисам для получения информации о своей публичной адресации. Анализирует HTTP-запросы, DNS-запросы и TLS SNI, указывающие на обращения к подобным ресурсам. Это позволяет блокировать несанкционированное взаимодействие с внешней инфраструктурой и предотвращать сбор данных для дальнейшей разведки или подготовки атак.
- **Ошибки в сетевых протоколах** - обнаруживает нарушения стандартов сетевых протоколов, фиксируя ошибки в форматировании сообщений, некорректные заголовки и структурные аномалии пакетов. Анализируя входящий и исходящий трафик, система выявляет сбои в реализации протокольных команд, которые могут быть следствием как технических недочетов, так и преднамеренных манипуляций злоумышленников. Это позволяет своевременно блокировать подозрительные соединения, предотвращая атаки, обход защитных механизмов и снижая риск компрометации информационных систем.
- **Подозрительное обращение к файлам** - обнаруживает обращения к файлам, которые не соответствуют обычным операциям системы и могут указывать на несанкционированный доступ или попытки извлечения/модификации критически важных данных. Анализируя сетевой трафик, фиксирует запросы на загрузку, копирование или просмотр файлов с нестандартными расширениями или путями, например, системных конфигураций, резервных копий или скрытых ресурсов. Это позволяет блокировать подозрительную активность, предотвращая утечку данных и возможную компрометацию системы.
- **Попытки авторизации с логином и паролем по-умолчанию** - обнаруживает попытки авторизации с использованием учетных данных по умолчанию, когда злоумышленники применяют стандартные логины и простые пароли для входа в систему. Анализируя трафик, система выявляет запросы, содержащие типичные параметры доступа к различным системам. Такие действия указывают на попытки несанкционированного доступа, что позволяет оперативно блокировать подобные соединения и предотвращать компрометацию сетевой инфраструктуры.
- **Попытки использования социальной инженерии** - обнаруживает попытки социальной инженерии, направленные на обман пользователей и получение конфиденциальной информации, такой как учетные данные/доступ к корпоративным ресурсам. Включает выявление фишинговых сайтов, мошеннических схем с техподдержкой, вредоносных редиректов и подозрительных доменов в DNS-запросах. Эти атаки часто имитируют известные сервисы или компании, побуждая жертву выполнить вредоносные действия, что может привести к утечке данных или компрометации системы.
- **Попытки получения привилегий администратора** - обнаруживает попытки повысить привилегии до уровня администратора и получить учетные данные с использованием различных техник. Включает детектирование эксплойтов, направленных на уязвимости в операционных системах и приложениях, SQL-инъекций, обхода аутентификации, эксплуатации слабых конфигураций сервисов, а также атак на учетные записи через протоколы Telnet, RDP, SMB и другие. Такие действия могут указывать на компрометацию системы или активность злоумышленников, пытающихся расширить контроль над сетью.
- **Попытки получения привилегий пользователя** - обнаруживает попытки повысить привилегии и компрометировать учетные данные пользователей, в том числе - использовать уязвимости в серверных приложениях, базах данных и сетевых сервисах. Включает правила для выявления SQL-инъекций, эксплуатации переполнения буфера, обхода аутентификации и атак на учетные записи пользователей. Используется для защиты от угроз, направленных на несанкционированный доступ и эскалацию привилегий в корпоративных и облачных средах.
- **Попытки получения системных файлов** - обнаруживает попытки получить конфигурационные и системные файлы, включая файлы паролей, журналы, резервные копии и другие критически важные данные. Включает правила для выявления сканирования уязвимостей, запроса конфигураций через веб-интерфейсы, злоупотребления FTP, SMB, SSH и др. Используется для предотвращения утечек данных и сбора информации, которые могут привести к дальнейшей компрометации инфраструктуры.

- **Попытки проведения DoS-атак** - обнаруживает попытки проведения атак типа отказа в обслуживании (DoS), включая флуд, амплификационные атаки и иные методы перегрузки сетевых ресурсов. Анализирует трафик на наличие аномальных запросов и последовательностей, характерных для DDoS-атак в протоколах VoIP, HTTP, NTP, SSDP и других. Фиксирует массовые запросы, некорректные ответы и превышение пороговых значений, что позволяет оперативно блокировать подобные соединения и предотвращать отказ в обслуживании легитимных пользователей.
- **Попытки сканирования сети** - обнаруживает попытки сканирования сети, свидетельствующие о разведке для последующих атак. Анализируя TCP, UDP, ICMP и HTTP-трафик, фиксирует массовые SYN-запросы, сканирование портов, аномальные User-Agent и повторяющиеся обращения к различным сервисам. Такие действия характерны для инструментов вроде Nmap и Zmap, которые злоумышленники используют для поиска уязвимостей. Выявление подобных активностей позволяет оперативно блокировать сканирование и предотвращать потенциальное проникновение в сеть.
- **Потенциально опасный трафик** - обнаруживает трафик с подозрительной шифровкой или запутанными, обфусцированными данными и нестандартными запросами, не характерными для легитимной сетевой активности. Анализируя HTTP, DNS, TLS и IP-заголовки, фиксирует аномальные User-Agent, обращения к подозрительным доменам и C2-серверам, а также другие индикаторы, свидетельствующие о попытках скрыть вредоносную коммуникацию. Это позволяет оперативно блокировать такие соединения, снижая риск проникновения и распространения атак.
- **Пулы криптомайнеров** - обнаруживает попытки взаимодействия с криптомайнинговой инфраструктурой через анализ DNS-запросов, TLS-сессий и TCP-трафика, фиксируя характерные доменные имена и сигнатуры, связанные с известными пулами. Выявляет обращения, используемые криптомайнерами для передачи нагрузки, и блокирует такие соединения, предотвращая несанкционированное использование сетевых ресурсов для майнинга и минимизируя риск утечки вычислительной мощности.
- **Расширенная база правил (от Лаборатории Касперского)** - обнаруживает трафик, который генерируют вредоносные инструменты, используемые злоумышленниками для разведки, атак и несанкционированного доступа. Анализируя HTTP, FTP, SIP, UDP и TCP-запросы, фиксирует аномалии, характерные для SQL-инъекций, эксплойтов, C&C-коммуникаций и других угроз. Правила от Лаборатории Касперского используют сигнатуры и поведенческий анализ для своевременного обнаружения и блокировки подозрительной активности, что помогает предотвратить утечку данных и повысить защиту сети от современных кибератак.
- **Телеметрия Windows** - обнаруживает попытки передать телеметрические данные Windows на серверы Microsoft и связанные сервисы. Анализирует сетевой трафик, включая TLS-сессии с SNI-запросами и DNS-запросы, выявляя характерные строки. Блокирует такие обращения, предотвращая автоматическую отправку телеметрии, что способствует защите конфиденциальности пользователей и снижению объема передаваемой информации.
- **Управление вредоносным ПО** - обнаруживает сетевой трафик инструментов, которые злоумышленники используют для разведки, атак и несанкционированного доступа, включая эксплойты, SQL-инъекции, обход аутентификации и C&C-коммуникации. Использует сигнатуры и поведенческий анализ для выявления характерных HTTP-, FTP-, SIP- и других запросов. Такие инструменты тесно связаны с вредоносным ПО и кибератаками, что позволяет оперативно блокировать их активность.
- **Целевое использование вредоносного ПО** - обнаруживает целевой трафик, связанный с вредоносным программным обеспечением, которое злоумышленники используют для компрометации систем, кражи данных и установления контроля над устройствами. Анализируя HTTP, DNS, TLS и другие протоколы, фиксирует обращения, характерные для APT-активностей и C&C-коммуникаций, а также сигнатуры известных вредоносных семейств. Блокировка таких запросов позволяет предотвратить целевые атаки и снизить риск утечки конфиденциальной информации.
- **Подключения к потенциально уязвимым web-приложениям** - обнаруживает попытки подключения к веб-приложениям с известными уязвимостями.
- **Эксплойты** - обнаруживает попытки эксплуатации системных уязвимостей с использованием эксплойт-китов, зачастую идентифицируемых по стандартным идентификаторам CVE-XXXX-XXXXX. Анализируя трафик в различных протоколах (HTTP, TLS, DNS и других), система фиксирует характерные сигнатуры и аномальные запросы, указывающие на запуск вредоносного кода или несанкционированный доступ. Блокировка таких соединений позволяет оперативно предотвратить компрометацию инфраструктуры и утечку конфиденциальной информации.

Пользовательские сигнатуры

Функциональность доступна в **Классическом** и **Системном контекстах**.

Пользовательская сигнатура - это кастомный шаблон, позволяющий идентифицировать определенные виды вредоносного трафика, аномалий в протоколах или известных атак. Такие сигнатуры можно добавлять на вкладке **Пользовательские сигнатуры**. При корректном добавлении появятся в таблице Группы сигнатур.

В обработке трафика не участвуют:

- Сигнатуры, которые не используются в профилях **Предотвращения вторжений**.
- Профили, которые не используются в правилах **Межсетевого экрана**.

Описание валидной сигнатуры

Валидная сигнатура включает три основные части:

- Действие при совпадении правила.
- Заголовок, определяющий протокол, IP-адреса или сети отправителя и получателя, порты и направление трафика.
- Опции, описывающие специфику сигнатуры.

Пример валидной сигнатуры

Генерирует предупреждение, если обнаружен HTTP GET-запрос, в URI которого встречается слово `rule`:

```
alert http $HOME_NET any → $EXTERNAL_NET any (msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http
```

где:

- `alert` - действие. Перечень валидных действий:
  - `alert` - пропустить пакет и сгенерировать предупреждение.
  - `pass` - пропустить пакет без предупреждения.
  - `drop` - отбросить пакет и сгенерировать предупреждение.
  - `reject` - отправить ошибку `RST/ICMP unreach` отправителю пакета.
  - `rejectdst` - отправить пакет с ошибкой `RST/ICMP error` получателю исходного пакета.
  - `rejectboth` - отправить пакеты с ошибкой `RST/ICMP error` отправителю и получателю исходного пакета.
- `http $HOME_NET any → $EXTERNAL_NET any` - заголовок, в том числе:
  - `http` - протокол. Валидные протоколы: сетевого уровня (`ip`, `icmp`), транспортного уровня (`tcp`, `udp`), уровня представления (`tls`, `ssl`), прикладного уровня (`http`, `dns`, `ssh`, `ftp` и другие).
  - `$HOME_NET` - сети отправителя, указанные в **Правила трафика → Предотвращение вторжений → Настройки → Сети, защищенные от вторжений**.
  - `any` - порты отправителя/получателя.
  - `->` - направление трафика. Два валидных значения: `->` - проверка трафика слева направо, `<>` - проверка трафика в обоих направлениях. Значение `<-` не является валидным. Например, при проверке пакетов, идущих из сети A в сеть B, валидное значение в сигнатуре - `сеть A → сеть B`, невалидное значение - `сеть B <- сеть A`.
  - `$EXTERNAL_NET` - сети получателя (значения, которые не попадают в `$HOME_NET`).
- `(msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1;)` - опции, заключенные в скобки и разделенные точкой с запятой.

Особенности опций валидной сигнатуры

Порядок опций важен, изменение влияет на порядок обработки. Например, указанная в примере опция `content:"GET"` относится к опции `http.method`, а опция `content:"rule"` - к опции `http.uri`.

Опции бывают двух основных видов:

- Влияющие на инспекцию трафика. При добавлении сигнатуры необходимо указать опции. Описание некоторых опций из примера:
  - `flow` - состояние соединения, направление следования пакета и др.;
  - `content` - содержимое пакета, по которому производится сопоставление.
- Метаопции - опции, не влияющие на инспекцию трафика, но влияющие на способ информирования о срабатывании сигнатуры. Список некоторых метаопций из примера:
  - `msg` - информация о сигнатуре и возможном алерте;
  - `classtype` - информация о классе правил и алертов (короткое и длинное название, приоритет);
  - `sid` - уникальный номер сигнатуры;
  - `rev` - версия сигнатуры;
  - `metadata` - дополнительная информация о сигнатуре. Формат `metadata`:

```
metadata: key value;
metadata: key value, key value;
```

Примеры указания тактики MITRE

1. Формат в правилах Касперского - `metadata: MITRE TA0001`:

```
alert http $HOME_NET any → $EXTERNAL_NET any (metadata: MITRE TA0001; msg:""; sid:1;)
```

- `TA0001` - MITRE_ID

2. Формат в Emerging Threats - `metadata: mitre_tactic_id TA0001`:

```
alert http $HOME_NET any → $EXTERNAL_NET any (metadata: mitre_tactic_id TA0001; msg:""; sid:1;)
```

- `TA0001` - MITRE_ID

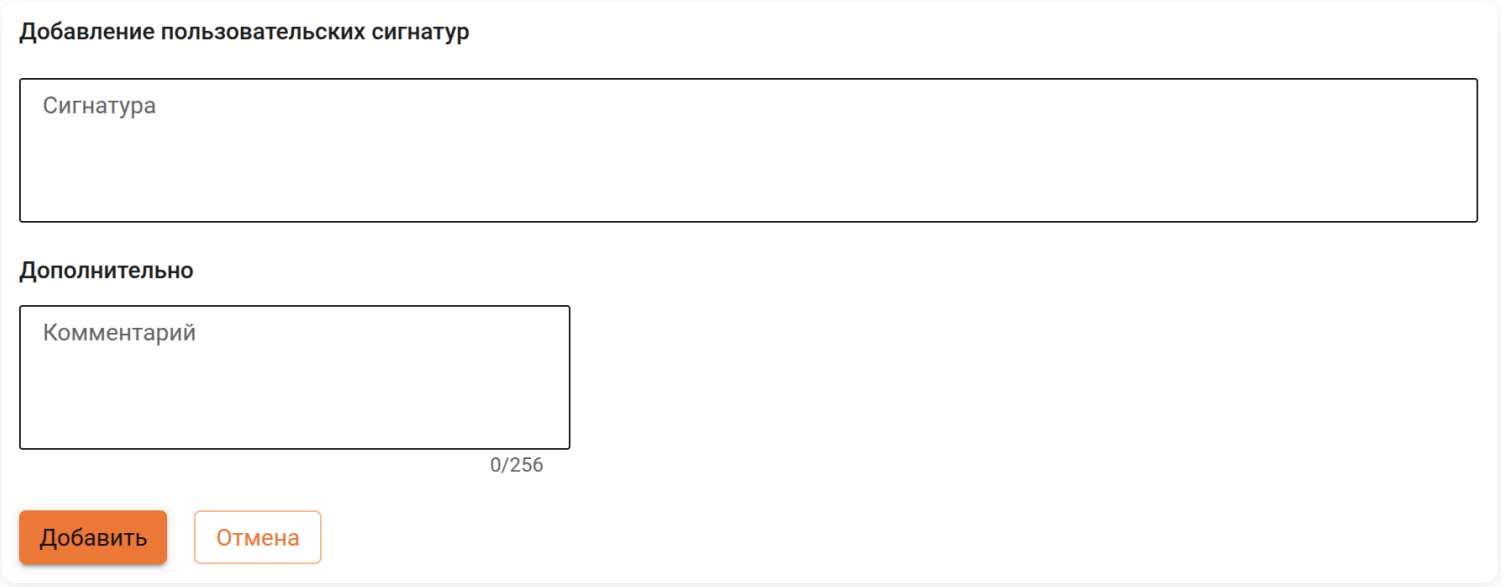
Символы `;` и `"` имеют специальное значение и должны быть экранированы с помощью символа `\` в случае использования в значениях опций.

Создание пользовательской сигнатуры

Нажмите **Добавить** и выберите способ добавления:

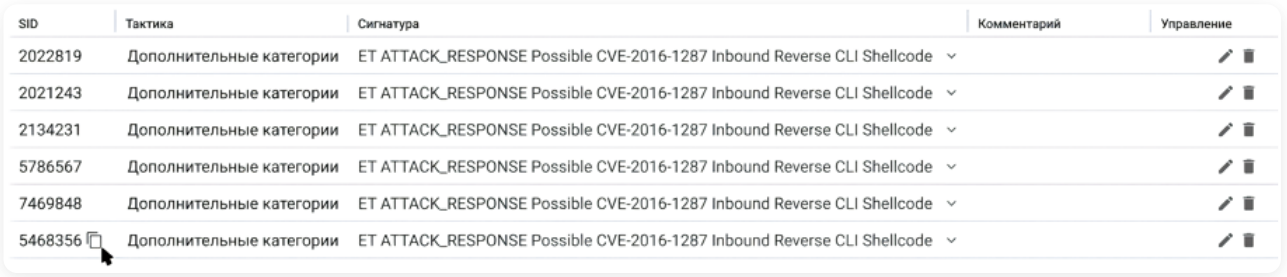
Вручную

В открывшейся форме введите сигнатуру, комментарий и нажмите **Добавить**:



Из файла

Загрузите текстовый файл с валидными сигнатурами (уникальные SID в диапазоне 1-999999). Если в структуре файла есть ошибки, система укажет номера строк с ошибками.



Проверка валидности сигнатур может занять некоторое время. Если одна из сигнатур не пройдет проверку, появится сообщение об ошибке у названия системы **Предотвращения вторжений**. Подробности можно будет увидеть в логах службы.

Пример создания исключения с конкретным адресом и сигнатурой

Пользователю необходимо добавить в исключения передачу трафика, который блокируется конкретной сигнатурой **Предотвращения вторжений** для конкретного отправителя (192.168.10.10) и получателя (1.1.1.1).

Если пользователь добавит в исключения конкретную сигнатуру, то разрешит этот трафик для всех адресов.
Если пользователь создаст исключение в разделе **Правила трафика** → **Исключения**, то исключается конкретный адрес для всех сигнатур.

Пользовательская сигнатура позволит создать исключение для конкретного адреса и конкретной сигнатуры одновременно. Для добавления такой сигнатуры:

1. Перейдите в **Отчеты и журналы** → **События безопасности** и найдите ID сигнатуры, которую необходимо добавить в исключения.

2. Скопируйте содержание сигнатуры (отображается при наведении на ID).

3. Перейдите в **Правила трафика** → **Предотвращение вторжений** → **Пользовательские сигнатуры** и нажмите **Добавить** → **Вручную**.

4. Вставьте скопированный лог в поле **Сигнатура** и измените в нем:

- Действие `drop` на `pass`.
- Значения `$HOME_NET` и/или `$EXTERNAL_NET` на нужный адрес отправителя/получателя.
- Значение `sid` на любое уникальное в диапазоне 1-999999.

Опции, не влияющие на инспекцию трафика, из сигнатуры можно удалить.
Если при добавлении сигнатуры оставить опцию `msg`, то в разделе **Отчеты и журналы** → **События безопасности** будут сохраняться логи по данной сигнатуре.

4. Нажмите **Добавить**.

Пример содержания сигнатуры в разделе **Отчеты и журналы** → **События безопасности**:

```
drop http $EXTERNAL_NET any → $HOME_NET any (msg:"ET HUNTING DDoS-Guard Hosted Content"; flow:established,to_client; http.sta
```

Пример пользовательской сигнатуры:

```
pass http 192.168.10.10 any → 1.1.1.1 any (flow:established,to_client; http.stat_code; content:"200"; http.server; content:"D
```

Полезные ссылки

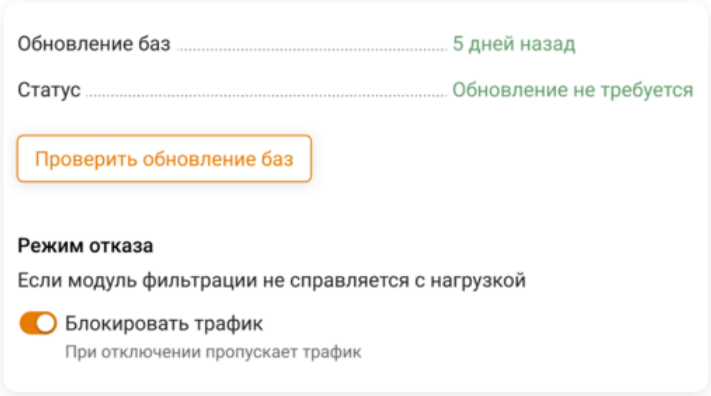
- **Полная документация по форматам сигнатур**.

Настройки

Классический контекст | Высокопроизводительный контекст

> Настройка дополнительных параметров фильтрации системы Предотвращение вторжений.

На вкладке можно проверить статус обновления баз системы **Предотвращение вторжений**, настроить **Режим отказа** и отредактировать список сетей, защищенных от вторжений:



Опция **Блокировать трафик** позволяет заблокировать весь трафик в случае перегрузки модуля **Предотвращение вторжений**.

Для добавления подсети в список защищенных нажмите **Добавить** и в поле **Подсеть** укажите локальные сети, обслуживаемые NGFW (сети локальных интерфейсов NGFW, маршрутизируемые на них сети удаленных сегментов локальной сети предприятия).

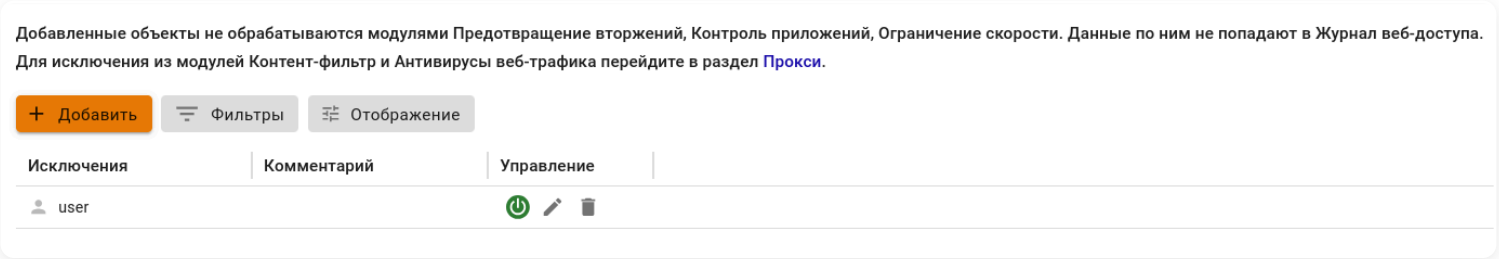
Для корректной работы системы **Предотвращение вторжений**:

- Не указывайте сети, принадлежащие внешним сетевым интерфейсам NGFW и внешним сетям. Указанные на вкладке сети участвуют в правилах системы **Предотвращения вторжений** как локальные.
- Не используйте сторонние DNS-серверы для компьютеров, т.к. служба определяет зараженные устройства по DNS-запросам, проходящим через нее.
- При использовании внутреннего домена AD рекомендуем:
  - В компьютерах указать DNS-сервер Ideco NGFW Novum в качестве единственного DNS-сервера.
  - В настройках DNS-сервера на NGFW указать Forward-зону для локального домена.

Исключения

Функциональность доступна в **Классическом** и **Системном контекстах**.

Правила в разделе **Исключения** отключают трафик из обработки системы Предотвращения вторжений, Контроля приложений, данные по ним не попадают в монитор трафика:



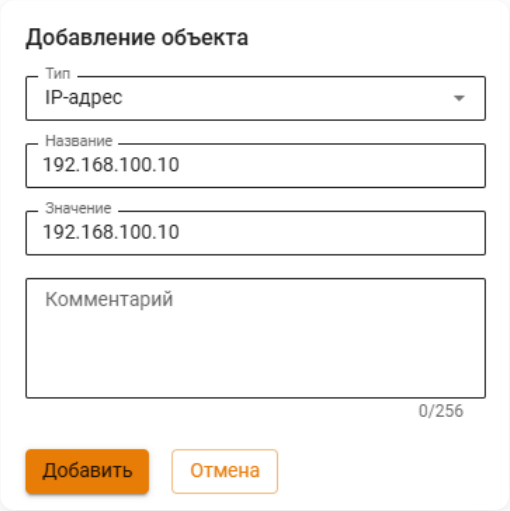
При наличии большого количества исключений в таблице воспользуйтесь кнопкой **Фильтры**.

Добавление исключения

Для предотвращения обработки трафика необходимо добавить объект в исключения:

1. Перейдите в **Правила трафика** → **Исключения** и нажмите **Добавить**.

2. Выберите существующий объект или создайте новый, заполнив поля:



- **Тип** - выберите тип объекта. Список доступных типов объектов приведен в статье.
- **Название** - укажите название объекта.
- **Значение** - укажите значение объекта в соответствии с выбранным типом.
- **Комментарий** - укажите произвольный комментарий. Необязательное поле.

3. Нажмите **Добавить**.

Если в качестве DNS-сервера у пользователя указан локальный адрес сервера Ideco NGFW Novum, то исключения работать не будут. Весь трафик, идущий на адреса локальных и VPN-интерфейсов Ideco NGFW Novum, всегда обрабатывается службой фильтрации трафика.

Объекты

Классический контекст | Высокопроизводительный контекст | API

В Ideco NGFW Novum можно создать объекты для использования в правилах межсетевого экрана, предотвращения вторжений и т.д.

Название службы раздела **Объекты**: `ideco-alias-backend`.

Список имен служб для других разделов доступен по ссылке.

Объектом называется сохраненный в NGFW Novum определенный тип данных, который можно использовать при создании правил.

Типы объектов

- **Зона** - логическое объединение сетевых интерфейсов. Используется для настройки правила межсетевого экрана на несколько интерфейсов.
- **IP-адрес** - IP-адрес IPv4. Пример: `10.0.0.1`.
- **Диапазон IP-адресов** - диапазон IP-адресов от первого до последнего, указанного в диапазоне. Пример: `10.0.0.1-10.0.0.25`.
- **Подсеть** - логический блок IP-адресации. Префикс маршрутизации выражается в нотации CIDR. Пример: `10.0.0.0/24`.
- **Домен** - символьное имя, служащее для идентификации объектов в интернете. Пример: `ideco.ru`.
- **Порт** - номер порта от 1 до 65535. Пример: `3389`.
- **Диапазон портов** - диапазон портов от первого до последнего, указанного в диапазоне. Пример: `1024-65535`.
- **Время** - диапазон времени. Пример: `ПН 9:00-18:00`.
- **Список IP-объектов** - группа объектов, состоящая из отдельных объектов, таких как IP-адрес, диапазон IP-адресов, подсеть, домен, пользователь, группа. При настроенной интеграции Active Directory доступны для выбора пользователи AD, группы безопасности AD, LDAP-фильтры. Пример: `10.0.0.1, 10.0.0.4, 10.0.0.126, test.com, user1`.
- **Список IP-адресов** - объект, состоящий из списка IP-адресов. Для создания объекта требуется загрузить любой текстовый файл (например: TXT/CSV). При этом в одной строке должен быть один адрес. Также допускается использование маски `/24` или `255.255.255.0`.
- **Порты** - группа портов. Пример: `25, 110, 143, 445, 465, 587, 993, 995`.
- **Расписание** - группа диапазонов времени. Пример: `ПН 9:00-12:00, ВТ 13:00-18:00`.
- **Список стран и континентов** - группа объектов, содержащая GeoIP.

При настроенной интеграции с Active Directory в правилах трафика доступны для выбора объекты, импортируемые из каталога.

Объекты, импортируемые из Active Directory

- **Пользователи AD** - учетные записи пользователей интегрированных доменов Active Directory. Становятся доступны для выбора в правилах после настройки интеграции с доменом.
- **Группы безопасности AD** - группы безопасности Active Directory, объединяющие учетные записи пользователей. Позволяют применить правило сразу ко всем пользователям группы.
- **LDAP-фильтры** - выборка учетных записей из каталога Active Directory с помощью фильтров. Подробнее - в статье **LDAP-фильтры**.

Объект **Зона** содержит набор предустановленных алиасов **Специальные**, которые объединяют определенные типы интерфейсов или трафик. Эти зоны нельзя удалить или изменить, но их можно использовать при создании правил фильтрации.

Специальные зоны

- **Внешние интерфейсы** - все интерфейсы с ролью **WAN**.
- **Внешние Ethernet-интерфейсы** - интерфейсы **Ethernet** с ролью **WAN**.
- **Внешние VPN-интерфейсы** - интерфейсы **L2TP**, **PPTP**, **PPPoE** с ролью **WAN**.
- **IPsec-интерфейсы** - соединения site-to-site IPsec.
- **Локальные интерфейсы** - интерфейсы с ролью **LAN**.
- **Туннельные интерфейсы** - интерфейсы **GRE**.
- **ГОСТ VPN-интерфейсы** - соединения, настроенные в **Сервисы** → **ГОСТ VPN**.
- **Исходящий трафик устройства** - исходящий трафик самого NGFW Novum.
- **Клиентский VPN-трафик** - трафик клиентских VPN-соединений.
- **WCCP GRE интерфейсы** - трафик туннелей до WCCP-сервера, созданных в **Сервисы** → **Прокси** → **WCCP**.

Объект **Зона** можно создавать и редактировать только в **Системном контексте**. В других контекстах объект будет доступен **только** для выбора.

Объект **IP-адрес** содержит набор предустановленных алиасов **Специальные**, которые объединяют определенные группы адресов.

Специальные IP-адреса

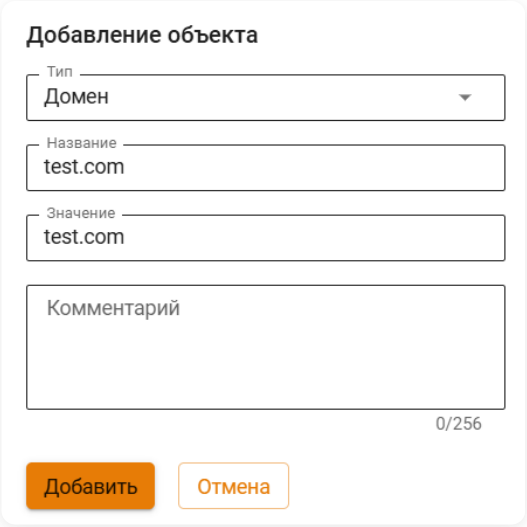
- **Черный список IP-адресов** - IP-адреса, внесенные в централизованные базы угроз (НКЦКИ, открытые источники).
- **Черный список ФинЦЕРТ** - IP-адреса из ежедневных бюллетеней ФинЦЕРТ.
- **Все пользователи AD** - IP-адреса пользователей из Active Directory.
- **Все доверенные пользователи AD** - IP-адреса пользователей из доверенных доменов Active Directory.

Создание объектов

Чтобы создать объект, необходимо выполнить следующие действия:

1. Перейдите в **Правила трафика** → **Объекты** и нажмите кнопку **Добавить** в левом верхнем углу экрана.

2. Выберите тип, название и значение объекта. По желанию можно указать произвольный комментарий не длиннее 128 символов:



3. Нажмите кнопку **Добавить**.

При наличии большого количества объектов в таблице воспользуйтесь кнопкой **Фильтры**.

Важно:

- Для создания групп объектов предварительно необходимо создать сами объекты. К группам объектов относятся: список IP-адресов, порты и расписание.
- Для создания объекта типа **Список IP-адресов** используйте любой текстовый файл (например: TXT/CSV), в котором будут перечислены нужные IP-адреса. Правила заполнения:
  - В строке должен быть один адрес.
  - Допускается использование маски /24 или 255.255.255.0.
- Для создания объекта типа **Зона** необходимо:
  - Создать соответствующий объект в разделе **Правила трафика** → **Объекты**.
  - Перейти в раздел **Сервисы** → **Сетевые интерфейсы** и при редактировании интерфейса добавить его в нужную зону.
- Для IPsec подключения зону можно добавить при создании подключения.
- Объекты типа **IP-адрес** и **Порт** можно создавать непосредственно при создании правил межсетевого экрана, введя нужный IP-адрес или порт в соответствующих полях.

В Ideco NGFW Novum также используется специальный алиас - **Любой**. Если при создании правила в каком-либо из полей выбран алиас **Любой**, правило будет распространяться на все объекты, доступные к выбору в том же поле.

Полезные ссылки

- **Ручная корректировка GeoIP**

Профили безопасности

Профили безопасности это наборы параметров для фильтрации трафика различными модулями и позволяет настраивать разные политики безопасности независимо друг от друга. Профили WAF будут использоваться только в публикациях сервисов в разделе Обратный прокси. Остальные профили - в правилах раздела Межсетевой экран.

Контроль приложений

Создание, настройка и примеры использования **Профилей контроля приложений**

Перейти >

Предотвращение вторжений

Создание, настройка и примеры использования **Профилей предотвращения вторжений**

Перейти >

Web Application Firewall

Создание WAF-профилей для защиты опубликованных веб-ресурсов от атак

Перейти >

Антивирус

Интеграция Kaspersky Anti-Virus Software Development Kit в Ideco NGFW

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Профили контроля приложений

Классический контекст | Высокопроизводительный контекст | API

Названия служб раздела **Профили контроля приложений**: `ideco-app-backend`, `ideco-app-control-nfq`.

Список имен служб для других разделов доступен по ссылке.

В **Профили безопасности** → **Контроль приложений** создаются профили, разрешающие или запрещающие доступ пользователя к заданному администратором набору приложений и протоколов. Созданные профили применяются при настройке правил в разделе **Межсетевой экран**. При наличии большого количества профилей в таблице воспользуйтесь кнопкой **Фильтры**.

Для выявления протоколов приложений осуществляется глубокий анализ трафика (Deep Packet Inspection - DPI). Собранные данные используются для мониторинга трафика. Определение протоколов выполняется системой в зависимости от состояния модуля **Профили контроля приложений**.

- Если включен, то весь трафик проходит через DPI, включая трафик, который обрабатывается правилами **Межсетевого экрана** без выбранного профиля **Контроля приложений**.
- Если выключен, то определение протоколов для трафика не производится.

Контроль приложений фильтрует трафик при условиях:

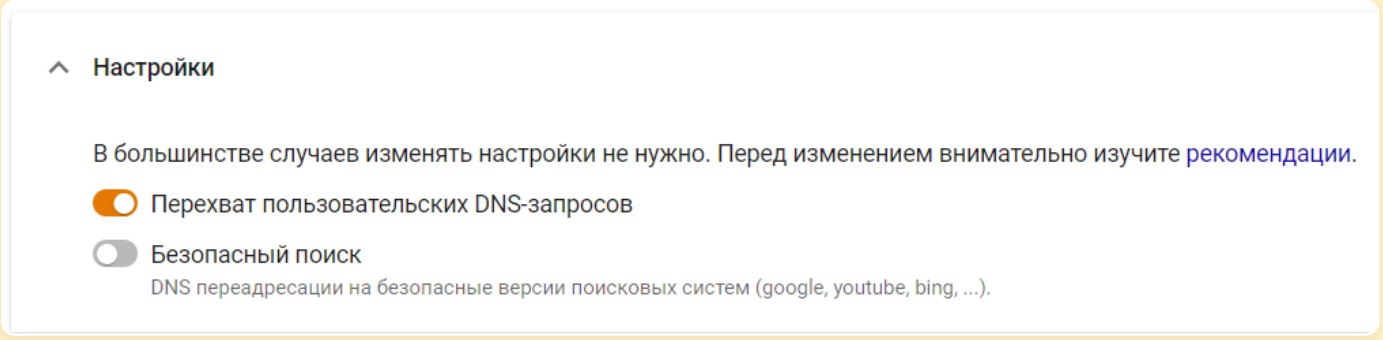
- В правиле **FORWARD** или **INPUT** раздела **Межсетевой экран** включена опция **Контроль приложений**.
- В этом правиле выбран профиль безопасности.

Трафик, не соответствующий условиям, фильтроваться не будет, даже если его протоколы определяются системой.

Принцип создания профилей **Контроля приложений**: все протоколы и приложения, которые не были запрещены, остаются разрешены.

Чтобы трафик фильтровался модулем **Контроль приложений**, создайте для всех локальных интерфейсов правило **FORWARD**, содержащее нужный профиль безопасности.

При включенной опции **Перехват пользовательских DNS-запросов** (по умолчанию включена) в разделе **Сервисы** → **DNS** → **Внешние DNS-серверы** трафик обрабатывается не как FORWARD, а как INPUT:



Создайте правила **INPUT** для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

Особенности обработки трафика с помощью профиля Контроля приложений

Контроль приложений проверяет только тот трафик, который соответствует разрешающему правилу **Межсетевого экрана** с включенной опцией **Профили контроля приложений** и выбранным профилем.

Порядок применения правил Межсетевого экрана

1. **Анализ трафика и поиск подходящего правила. Межсетевой экран** Ideco NGFW Novum проверяет трафик и последовательно (сверху вниз) сравнивает его с правилами из таблицы. Как только находится совпадение, соответствующее правило применяется.

2. **Приоритет правил.** Если **Межсетевой экран** находит несколько правил с одинаковыми условиями, то применяет правило, расположенное выше в списке.

3. **Взаимодействие с Контролем приложений.** Если трафик блокируется запрещающим правилом **Межсетевого экрана**, **Контроль приложений** не проверяет заблокированный трафик.

Доступные приложения и протоколы для создания профилей

Перечень групп приложений и протоколов, доступных для создания профилей

- Стриминговые сервисы
- Веб-ресурсы
- Компьютерные игры
- Видео-контент
- Реклама
- Контент для взрослых
- Передача данных
- Облачные сервисы
- Виртуальные ассистенты
- RPC
- IoT-Scada
- Удаленный доступ
- Обновления ПО
- Сети
- Социальные сети
- Криптовалюты
- Обмен файлами
- Системные
- Базы данных
- VoIP
- VPN
- Кибербезопасность
- Музыка
- Командная работа
- Магазины
- Чаты и мессенджеры
- Почта
- Медиа-контент
- Майнинг

Описание приложений и протоколов, доступных для создания профилей

Приложения и протоколы	**Описание**
1kxun	Китайский видеосервис. На нем представлены различные анимационные фильмы, телевидение, спорт и кино
AccuWeather	Частная американская медиа-компания, предоставляющая коммерческие услуги по прогнозированию погоды по всему миру
Activision	Американская компания по изданию и разработке компьютерных игр, разработчик Call of Duty
AdobeConnect	Платформа веб-конференций, которая позволяет пользователям проводить онлайн-встречи, вебинары
ADS_Analytic_Track	Отслеживание и аналитика рекламы (mobile marketing analytics and attribution platform)
AFP	Протокол представительского и прикладного уровней сетевой модели OSI, предоставляющий доступ к файлам в MacOS X
AJP	Протокол, который может проводить входящие запросы с веб-сервера до сервера приложений
Alibaba	Китайская публичная компания, работающая в сфере интернет-коммерции, владелец веб-порталов Taobao.com, Tmall, Alibaba.com и ряда других
AliCloud	Компания, предоставляющая ресурсы для облачных вычислений, дочерняя компания Alibaba Group
Amazon	Американская компания-разработчик платформ электронной коммерции и публично-облачных вычислений

AmazonAlexa	Облачная голосовая служба Amazon
AmazonAWS	Коммерческое публичное облако, поддерживаемое и развиваемое компанией Amazon
AmazonVideo	Стриминговый сервис компании Amazon
AmongUs	Многопользовательская компьютерная игра
AMQP	Открытый протокол прикладного уровня для передачи сообщений между компонентами системы
ANSI_C1222	Протокол прикладного уровня, предназначенный для использования в сетях электросчетчиков Smart Grid
AnyDesk	Приложение для удаленного рабочего стола, распространяемое AnyDesk Software GmbH
Apple	Компания-производитель смартфонов и компьютерной техники
AppleiCloud	Облачное хранилище от компании Apple, которое предоставляет пользователям доступ к их музыке, фотографиям, документам и другим файлам с любого устройства
AppleiTunes	Медиаплеер для организации и воспроизведения музыки и фильмов, разработанный компанией Apple и бесплатно распространявшийся для платформ MacOS и Windows
ApplePush	Сервис, созданный Apple для отправки уведомлений от сторонних приложений на устройства Apple
AppleSiri	Облачный персональный помощник и вопросно-ответная система компании Apple
AppleStore	Онлайн-магазин техники Apple и аксессуаров к ней
AppleTVPlus	Американский стриминговый сервис, принадлежащий и управляемый компанией Apple
Armagetron	Свободная компьютерная игра для операционных систем Linux, Windows, MacOS, FreeBSD и AmigaOS 4
AVAST	Семейство антивирусных программ, разработанных компанией Avast для операционных систем Windows, MacOS, Android и iOS
AVASTSecureDNS	Сервис защищенных DNS-серверов от компании Avast
Azure	Облачная платформа компании Microsoft. Предоставляет возможность разработки, выполнения приложений и хранения данных на серверах, расположенных в распределенных дата-центрах
BACnet	Сетевой протокол, применяемый в системах автоматизации зданий и сетях управления
Badoo	Приложение для онлайн-знакомств
BeckhoffADS	Открытый протокол обмена данными ADS на базе TCP/IP для общения с контроллером, разработанный BECKHOFF
BFCP	Протокол предназначен для обмена презентациями и демонстрации рабочего стола в рамках видеоконференции
BFD	Протокол обнаружения двунаправленной пересылки, который используется для обнаружения неисправностей между двумя маршрутизаторами или коммутаторами
BGP	Протокол динамической маршрутизации
BITCOIN	Криптовалюта, использующая децентрализованную систему для записи транзакций в блокчейне
BitTorrent	Пиринговый протокол для кооперативного обмена файлами через интернет
BJNP	Протокол обнаружения служб локальной сети, используемый принтерами и сканерами Canon. Компьютерные системы используют этот протокол для автоматического обнаружения устройств Canon в сети
Bloomberg	Американская компания, информационное агентство, один из двух ведущих американских поставщиков финансовой информации для профессиональных участников финансовых рынков
Bluesky	Bluesky Social представляет собой децентрализованную социальную платформу для микроблогов
Cachefly	Поставщик сети доставки контента
CAPWAP	Сетевой протокол с возможностью взаимодействия, который позволяет центральному контроллеру доступа к беспроводной локальной сети управлять набором беспроводных оконечных точек
Cassandra	Распределенная система управления базами данных, относящаяся к классу NoSQL-систем и рассчитанная на создание масштабируемых хранилищ данных, представленных в виде хеша
Ceph	Свободная программная объектная сеть хранения, обеспечивающая как файловый, так и блочный интерфейсы доступа
CHECKMK	Протокол используется для мониторинга серверных и контейнерных систем в ИТ-инфраструктуре
CIP	Информационно-управляющий протокол, который обеспечивает обмен сообщениями ввода/вывода в реальном времени и прямой обмен информационными сообщениями
CiscoSkinny	Корпоративный (проприетарный) VoIP-протокол для управления взаимодействием между оконечными телефонными устройствами и сервером телефонной системы (IP-АТС)
CiscoVPN	Протокол VPN, разработанный компанией Cisco Systems
Citrix	Программа, предоставляющая доступ к приложениям и рабочим столам с удаленного клиентского устройства с помощью ресурсов Citrix Virtual Apps and Desktops и Citrix DaaS
ClickHouse	Система управления базами данных с открытым исходным кодом, построенная на основе колонок
Cloudflare	Американская компания, предоставляющая услуги CDN, защиту от DDoS-атак, безопасный доступ к ресурсам и серверы DNS

CloudflareWarp	Бесплатный VPN от CloudFlare, который проксирует все сетевые запросы в системе (включая обновления Windows и др. ПО, трафик многопользовательских игр, торренты)
CNN	Американский круглосуточный кабельный телеканал новостей
COAP	Протокол для взаимодействия простых устройств, например, датчиков малой мощности, выключателей, клапанов, которые управляются или контролируются удаленно через интернет
CoD_Mobile	Бесплатный шутер для устройств iOS и Android
Collectd	Демон Unix, который собирает, передает и хранит данные о производительности компьютеров и сетевого оборудования
Controller_Area_Network	Стандарт протокола связи, используемый для обмена данными между устройствами в автомобильной промышленности и других промышленных приложениях
Corba	Технологический стандарт написания распределенных приложений, продвигаемый консорциумом OMG, и соответствующая ему информационная технология
CPHA	Алгоритм хеширования, который может использоваться для безопасного хранения паролей в PTC
Crashlytics	Инструмент отчетности о сбоях, который помогает выявлять ошибки
Crossfire	Южнокорейский тактический сетевой шутер от первого лица, разработанный компанией SmileGate
CryNetwork	Составной модуль для создания многопользовательских игр
Cybersec	Компании сферы кибербезопасности: checkpoint.com norton.com, kaspersky.com, fortinet.com
Dailymotion	Французский видеохостинг
DataSaver	Функция для Chrome, которая позволяет значительно сократить использование мобильных данных
Dazn	Спортивный стриминговый сервис
DCERPC	Система удаленного вызова процедур, разработанная для Distributed Computing Environment
Deezer	Французский интернет-сервис потоковой передачи музыки
DHCP	Протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети
DHCPV6	Протокол динамического конфигурирования хостов для межсетевого протокола версии 6
Diameter	Сеансовый протокол, созданный, отчасти, для преодоления некоторых ограничений протокола RADIUS
DirecTV	Компания прямого телерадиовещания в США, сигналы цифрового спутникового телевидения и радио передаются на территорию США и Латинской Америки
Discord	Кроссплатформенная проприетарная система мгновенного обмена сообщениями с поддержкой VoIP и видеоконференций, предназначенная для использования различными сообществами по интересам
DisneyPlus	Американский сервис потокового вещания типа OTT на основе подписки
DLEP	Протокол маршрутизации с учетом радиосвязи (RAR)
DNP3	Протокол передачи данных, используемый для связи между компонентами АСУ ТП
DNS	Протокол, используемый для получения IP адреса хоста по его доменному имени
DNScrypt	Протокол шифрования DNS-трафика
Dofus	Массовая многопользовательская ролевая онлайн-игра (MMORPG), использующая Flash-графику и фэнтезийный сеттинг
DoH_DoT	Протокол защиты DNS-трафика (запросов и ответов) от перехвата и подмены. В том числе включает обычные DNS-запросы адресов DoT/DoH-серверов
Dota2	Многопользовательская командная компьютерная игра в жанре MOBA, разработанная и изданная корпорацией Valve
DRDA	Набор протоколов, обеспечивающих возможность связи между программами и системами баз данных на разных платформах и позволяющих распределять реляционные данные по нескольким платформам
Dropbox	Файловый хостинг компании Dropbox Inc, включающий персональное облачное хранилище, синхронизацию файлов и программу-клиент
DTLS	Протокол передачи данных, обеспечивающий защищенность соединений для протоколов, использующих датаграммы
EAQ	Entitade Aferidora da Qualidade de Banda Larga - эксцентричный протокол VoIP/конференц-связи, который редко встречается в реальной жизни
eBay	Американская компания, предоставляющая услуги в областях интернет-аукционов и интернет-магазинов
Edgecast	Децентрализованное приложение для потоковой передачи видео, построенное на собственной технологии блокчейн THETA со смарт-контрактами
eDonkey	Файлообменная сеть, построенная по принципу P2P на основе сетевого протокола прикладного уровня MFTP
EGP	Устаревший протокол обмена информации между маршрутизаторами нескольких автономных систем
Elasticsearch	Тиражируемая программная поисковая система
ElectronicArts	Американская публичная транснациональная корпорация, занимающаяся распространением и изданием компьютерных игр (FIFA, Battlefield)

EpicGames	Американская компания, занимающаяся разработкой компьютерных игр и программного обеспечения, в частности - Fortnite
ETHEREUM	Криптовалюта и платформа для создания децентрализованных онлайн-сервисов на базе блокчейна
EthernetGlobalData	Протокол связи, разработанный GE Fanuc Automation для обмена данными в реальном времени между устройствами автоматизации и системами управления с использованием стандартной технологии Ethernet
EthernetIP	Промышленный сетевой стандарт, который поддерживает неявный обмен сообщениями (обмен сообщениями ввода/вывода в реальном времени), явный обмен (обмен сообщениями) или оба и использует широко распространенные коммерческие чипы связи Ethernet и физические носители
Ether-S-Bus	Промышленный протокол управления, используемый компанией SAIA Burgess
EtherSIO	Протокол используется для передачи данных между программируемыми логическими контроллерами и удаленными устройствами ввода/вывода производства компании Saia-Burgess Controls Ltd
Facebook	Крупнейшая социальная сеть в мире, которой владеет компания Meta Platforms
FacebookMessenger	Приложение для обмена мгновенными сообщениями и видео, созданное Meta
FacebookVoip	Голосовые и видеозвонки в FaceBook
FastCGI	Клиент-серверный протокол взаимодействия веб-сервера и приложения, дальнейшее развитие технологии CGI
FbookReelStory	Короткие видеоролики на Facebook
FINS	Открытый протокол связи поддерживаемый большинством контроллеров и сетей разработки компании Omron
FIX	Протокол передачи данных, являющийся международным стандартом для обмена данными между участниками биржевых торгов в режиме реального времени
FLUTE	Доставка файлов по однонаправленному транспорту
FortiClient	Комплексное решение безопасности, предназначенное для защиты компьютеров и ноутбуков. Также имеет версии для планшетов и мобильных устройств под управлением Android и Apple iOS
FTP_CONTROL	Протокол, предназначенный для передачи файлов в компьютерных сетях
FTP_DATA	Протокол доступа, предназначенный для удаленной передачи файлов в компьютерных сетях
FTPS	Расширение широко используемого протокола передачи файлов FTP, которое добавляет поддержку для криптографических протоколов уровней транспортной безопасности и защищенных сокетов
Fuze	Файловая система в пользовательском пространстве для Unix-подобных операционных систем, позволяющая непривилегированным пользователям создавать собственные файловые системы без редактирования кода ядра
GaijinEntertainment	Частная компания, разработчик и издатель компьютерных игр, в частности - War Thunder
Gearman	Платформа приложений с открытым исходным кодом, предназначенная для распределения соответствующих компьютерных задач на несколько компьютеров
GeForceNow	Облачный игровой сервис компании Nvidia
GenshinImpact	Компьютерная игра в жанре action-adventure с открытым миром и элементами RPG, разработанная китайской компанией miHoYo Limited
Git	Распределенная система управления версиями
GitHub	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки
GitLab	Веб-инструмент жизненного цикла DevOps с открытым исходным кодом, представляющий систему управления репозиториями кода для Git с собственной вики, системой отслеживания ошибок, CI/CD пайплайном и другими функциями
GMail	Бесплатная почтовая служба от компании Google. Предоставляет доступ к почтовым ящикам через веб-интерфейс и по протоколам POP3, SMTP и IMAP, а также в приложении Gmail на Android
Gnutella	Протокол для распределенного обмена файлами, в основном, музыкальными
Google	Американская технологическая компания, которая специализируется на поисковых технологиях, искусственном интеллекте, онлайн-рекламе, программным обеспечением, бытовой электроникой
GoogleCall	Аудио- и видеозвонки, совершаемые с помощью (любых) приложений Google (например, Google Meet)
GoogleChat	Коммуникационный сервис, разработанный компанией Google
GoogleClassroom	Облачная платформа для организации образовательного процесса
GoogleCloud	Предоставляемый компанией Google набор облачных служб. Выполняются на той же инфраструктуре, которую Google использует для своих продуктов, предназначенных для конечных потребителей
GoogleDocs	Текстовый онлайн-процессор, входящий в состав бесплатного веб-пакета редакторов GoogleDocs
GoogleDrive	Сервис хранения, редактирования и синхронизации файлов, разработанный компанией Google. Его функции включают хранение файлов в интернете, общий доступ к ним и совместное редактирование
GoogleMaps	Набор приложений, построенных на основе бесплатного картографического сервиса и технологии, предоставляемых компанией Google
GoogleMeet	Сервис видео-телефонной связи и видеоконференций, разработанный компанией Google

GoogleServices	Набор приложений и API, которые реализуют дополнительные возможности на устройствах Android. Сервисы Google для мобильных устройств включают основные приложения: Google Play, Gmail, Google Map, YouTube и Chrome
GoTo	Американская компания, предоставляющая услуги телефонных систем для бизнеса, контакт-центров и продукты для ИТ-поддержки
GRE	Протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems
GTP_C	Группа протоколов соединения на основе IP, используемая в сетях GSM, UMTS и LTE
GTP_PRIME	Группа протоколов связи на основе IP, используемых для передачи услуг пакетной радиосвязи общего пользования (GPRS) в сетях GSM, UMTS, LTE
GTP_U	Протокол используется для транспортировки пользовательских данных между пакетной сетью и радиосетью
GTP	Протокол туннелирования GPRS
Guildwars	Фэнтезийная массовая многопользовательская ролевая онлайн-игра, разработанная компанией ArenaNet и выпущенная компанией NCsoft в 2005 году
H323	Набор стандартов для передачи мультимедиа-данных по сетям с пакетной передачей
HalfLife2	Компьютерная игра, научно-фантастический шутер от первого лица
HAProxy	Программное обеспечение для балансировки нагрузки для TCP и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов
HART-IP	Адресуемый по магистрали удаленный преобразователь по IP. В основном используется для обмена данными в качестве стандартного глобального протокола между интеллектуальными устройствами и системой управления и некоторой интеллектуальной системой
HBO	Американский телеканал, принадлежащий компании WarnerMedia
Heroes_of_the_Storm	Онлайн-игра, разработанная Blizzard Entertainment для Microsoft Windows и MacOS
HiSLIP	Коммуникационный протокол для измерительного и тестового оборудования с использованием технологии VISA
HL7	Стандарт обмена, управления и интеграции электронной медицинской информации
HLS	Протокол для потоковой передачи медиа на основе HTTP, разработанный компанией Apple
HotspotShield	Программное обеспечение для организации виртуальной частной сети, обеспечивающей безопасную передачу данных по шифрованному соединению, защищенному от прослушивания
HP_VIRTGRP	Протокол HP Virtual Machine Group Management - часть пакета виртуализации, используемого в серверных средах HP
HSRP	Протокол маршрутизации семейства FHRP (англ. First-hop redundancy protocols), разработанный компанией Cisco и стандартизованный в RFC 2281
HTTP_Connect	Метод HTTP, который запускает двустороннюю связь с запрошенным ресурсом. Метод можно использовать для открытия туннеля
HTTP_Proxy	Тип прокси-сервера, который действует как сервер-посредник между клиентом и веб-сервером
HTTP	Протокол для получения с серверов гипертекстовых документов в формате HTML
HTTP2	Вторая крупная версия сетевого протокола HTTP, используемая для доступа к World Wide Web
Huawei	Трафик устройств Huawei
HuaweiCloud	Мобильное облако Huawei
Hulu	Стриминговый сервис по подписке, принадлежащий The Walt Disney Company
i3D	Протокол с низкой задержкой, используемый в основном игровыми серверами
IAX	Протокол обмена VoIP-данными между IP-АТС Asterisk и другим аналогичным софтсвичом или VoIP-телефоном
IceCast	Протокол для организации потокового цифрового аудиовещания и видеовещания
iCloudPrivateRelay	Сервис для маскировки IP-адреса пользователя с целью сохранения его конфиденциальности
ICMP	Протокол третьего уровня модели OSI, который используется для диагностики проблем со связностью в сети
ICMPV6	Протокол управляющих сообщений для межсетевого протокола версии 6
IEC60870	Набор протоколов для контроля и управления с использованием постоянного соединения
IEC62056	Набор стандартов Международной электротехнической комиссии для обмена данными учета электроэнергии
IEEE-C37118	Потоковый протокол для обмена и передачи данных синхрофазоров (или PMU), которые фиксируют устойчивое состояние или динамический отклик энергосистемы. Обеспечивает высокоскоростную передачу большого количества данных в режиме реального времени
IFLIX	Малайзийский бесплатный видеосервис
IGMP	Протокол управления групповой передачей данных в сетях, основанных на протоколе IP. Используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы
iHeartRadio	Американская платформа бесплатного вещания, подкастов и потокового радио, принадлежащая iHeartMedia
IMAP	Протокол для доступа к электронной почте

IMAPS	Протокол для осуществления доступа к электронной почте, включающий в себя обязательное шифрование
IMO	Веб-сервис и кроссплатформенное приложение для мгновенного обмена сообщениями и VoIP-звонков
Instagram	Американская социальная сеть для обмена фотографиями и видео
IP_in_IP	Протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет
IP_PIM	Семейство многоадресных протоколов маршрутизации для IP сетей, созданное для решения проблем групповой маршрутизации
IPP	Протокол, используемый для передачи документов на печать
IPSec	Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP
iQIYI	Китайская онлайн-видеоплатформа, предлагающая широкий спектр оригинального и лицензионного контента, включая фильмы, драмы, развлекательные шоу и аниме
IRC	Протокол прикладного уровня для обмена сообщениями в режиме реального времени
ISO9506-1-MMS	Протокол передачи данных реального времени и команд диспетчерского управления между сетевыми устройствами и/или программными приложениями
Jabber	Протокол основе на XML, открытый для использования. Предназначен для мгновенного обмена сообщениями и информацией о присутствии в режиме, приближенному к реального времени
JRMI	Протокол удаленного вызова методов Java
JSON-RPC	Протокол удаленного вызова процедур, использующий JSON для кодирования сообщений
Kafka	Распределенный программный брокер сообщений с открытым исходным кодом
KakaoTalk_Voice	Популярный в Южной Корее мессенджер, который поддерживает мгновенную передачу сообщений, позволяет отправлять файлы, а также совершать аудиозвонки и видеозвонки
KakaoTalk	Бесплатное мобильное приложение для мгновенного обмена сообщениями для смартфонов
KCP	Протокол связи, который максимально использует полосу пропускания для надежной связи с низкой задержкой
Kerberos	Протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними
Kismet	Сетевой детектор, анализатор пакетов и система обнаружения вторжений для беспроводных локальных сетей стандарта 802.11
KNXnet_IP	Протокол автоматизации зданий, который обеспечивает обмен данными и управляющей информацией через IP-сети, расширяя стандарт KNX для автоматизации дома и зданий
LastFM	Сервис для прослушивания музыки онлайн
LDAP	Протокол для доступа к службе каталогов X.500
LDP	Протокол маршрутизации, используемый для установления и поддержания путей с коммутацией меток в сети с многопротокольной коммутацией меток (MPLS)
Likee	Социальная сеть, пользователи которой могут создавать и распространять короткие музыкальные видео
Line	Приложение для смартфонов и ПК, средство моментального обмена сообщениями
LineCall	Система звонков/видеоконференций, используемая в популярном мобильном приложении для обмена сообщениями LINE
Linkedin	Американская социальная сеть для поиска и установления деловых контактов
LISP	Протокол маршрутизации, построенный на идее разделения топологического расположения точки присоединения к сети и идентификации узла
Livestream	Платная стриминговая платформа, которая позволяет клиентам загружать живое видео со своих мобильных устройств и компьютерных камер через интернет
LLMNR	Протокол, основанный на формате пакета данных DNS, который позволяет компьютерам выполнять разрешение имен хостов в локальной сети
LoLWildRift	League of Legends: Wild Rift - мобильная игра в жанре MOBA
LotusNotes	Программный продукт, платформа для автоматизации совместной деятельности рабочих групп, содержащий в себе средства электронной почты, персональных и групповых электронных календарей, службы мгновенных сообщений и среду исполнения приложений делового взаимодействия
MapleStory	Бесплатная многопользовательская ролевая онлайн-игра, разработанная южнокорейской компанией Wizet
Mastodon	Бесплатное программное обеспечение с открытым исходным кодом для запуска самостоятельных служб социальных сетей. Mastodon имеет функции микроблогов, аналогичные Twitter
MDNS	Многоадресный протокол DNS, используемый для преобразования имени хостов в IP-адреса в небольших сетях, не включающих локальный сервер имен
Megaco	Протокол для управления функциями шлюза на границе пакетной сети
Memcached	Протокол кеширования, используемый для ускорения динамических веб-приложений путем кеширования данных в памяти

MerakiCloud	Сервис компании Cisco, предоставляющий доступ к облачным технологиям
MGCP	Протокол управления медиашлюзами
Microsoft	Американская корпорация-разработчик в сфере проприетарного программного обеспечения для различного рода вычислительной техники: персональных компьютеров, игровых приставок, КПК, мобильных телефонов и прочего
Microsoft365	Набор веб-сервисов на основе платформы Microsoft Office, электронная почта, функции для общения и управления документами, которые распространяются на основе подписки по схеме программное обеспечение как услуга
Mining	Протоколы, использующиеся программами-майнерами
Modbus	Протокол, основанный на архитектуре ведущий - ведомый, применяется в промышленности для организации связи между электронными устройствами
Monero	Криптовалюта на основе протокола CryptoNote, ориентированная на повышенную конфиденциальность транзакций
MongoDB	Протокол, используемый для взаимодействия клиентов и серверов MongoDB
MPEG_TS	Протокол для передачи аудиоданных и видеоданных, описанных в MPEG2
MpegDash	Протокол потоковой передачи данных, предоставляющий возможность доставки потокового мультимедиа-контента через интернет по протоколу HTTP
MQTT	Упрощенный сетевой протокол, работающий поверх, ориентированный на обмен сообщениями между устройствами по принципу "издатель - подписчик"
MS_OneDrive	Облачное хранилище компании Microsoft. Является частью спектра онлайновых услуг Windows Live
MS-RPCH	Microsoft RPC-over-HTTP (RPC через HTTP) позволяет клиентам RPC подключаться через интернет к программам сервера RPC и выполнять удаленные вызовы процедур
MsSQL-TDS	Протокол прикладного уровня, используемый для передачи данных между сервером базы данных и клиентом
Mullvad	Сервис по поставке услуг виртуальной частной сети (VPN) с открытым исходным кодом, работает с использованием протоколов WireGuard и OpenVPN
Mumble	Свободное кроссплатформенное VoIP-приложение с открытым кодом, включающее особую технологию «позиционирования звука», как основную отличительную особенность
Munin	Бесплатное программное приложение для мониторинга компьютерных систем, сети и инфраструктуры с открытым исходным кодом
MySQL	Протокол, используемый для взаимодействия клиентов и серверов MySQL
Nano	Консольный текстовый редактор для UNIX и Unix-подобных операционных систем
NAT-PMP	Сетевой протокол для автоматической установки параметров преобразования сетевых адресов и конфигураций переадресации портов без участия пользователя
Nats	Система обмена сообщениями с открытым исходным кодом
NestLogSink	Система логирования для домашней системы пожарной безопасности от Google
NetBIOS	Протокол, используемый для обнаружения компьютеров в сети
NetEaseGames	Трафик различных игр NetEase
Netflix	Стриминговый сервис фильмов и сериалов
NetFlow	Протокол, предназначенный для учета сетевого трафика, разработанный компанией Cisco Systems
NFS	Протокол сетевого доступа к файловым системам
Nintendo	Японская компания, специализирующаяся на создании видеоигр и игровых систем
NOE	New Office Environment - протокол VoIP, используемый совместимыми телефонными системами Alcatel-Lucent
NoMachine	Проект итальянской компании Medialogic S.p.A. для дистанционной работы
Ntop	Программное обеспечение, которое исследует компьютерную сеть
NTP	Протокол для синхронизации внутренних часов компьютера
Nvidia	Американская технологическая компания, разработчик графических процессоров и систем на чипе (SoC)
OCS	Спецификация программных интерфейсов класса REST для интеграции социальных интернет-коммуникаций в среды рабочего стола
OCSP	Протокол, используемый для получения статуса отзыва цифрового сертификата X.509
OICQ	Распространенный в Китае сервис мгновенного обмена сообщениями
Ookla	Американская компания, которая владеет сервисом по измерению скорости интернета Speedtest
OPC-UA	Программный интерфейс для промышленного протокола связи и модели данных. Используется для связи между конечными устройствами различных производителей по принципу клиент/сервер
OpenDNS	Протокол, предоставляющий общедоступные DNS-серверы
OpenFlow	Протокол управления процессом обработки данных, передающихся по сети маршрутизаторами и коммутаторами
OpenVPN	Протокол VPN с открытым исходным кодом

OpenWire	Библиотека программирования потоков данных с открытым исходным кодом
OperaVPN	VPN-клиент, встроенный в браузер Opera
Oracle	Американская компания, специализируется на выпуске систем управления базами данных, связующего программного обеспечения, бизнес-приложений
OSPF	Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала
Outlook	Персональный информационный менеджер с функциями почтового клиента, входящий в пакет офисных программ Microsoft Office
Pandora	Тип цифровой криптовалюты
Pastebin	Веб-приложение, которое позволяет загружать отрывки текста, обычно фрагменты исходного кода, для возможности просмотра окружающими
PathofExile	Бесплатная онлайн-ролевая игра в жанре экшен
PFCP	Протокол, используемый для связи между функциями управления (CP) и пользователя (UP) в сетях 4G и 5G
PGM	Протокол надежной многоадресной передачи данных
Pinterest	Социальный интернет-сервис, фотохостинг, позволяющий пользователям добавлять в режиме онлайн-изображения
Playstation	Игровая приставка, разработанная компанией Sony Computer Entertainment
PlayStore	Онлайн-магазин приложений для Android
Pluralsight	Платформа для онлайн-обучения
POP3	Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP
POPS	Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP, включающий в себя обязательное шифрование
PostgreSQL	Протокол, используемый для взаимодействия клиентов и серверов PostgreSQL
PPTP	Туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищенное соединение с сервером за счет создания специального туннеля в стандартной, незащищенной сети
PrivateInternetAccess	Персональная служба VPN
PROFINET_IO	Протокол для связи реального времени (RT) и изохронного реального времени (IRT) с децентрализованной периферией
Protobuf	Протокол сериализации (передачи) структурированных данных, предложенный Google как эффективная бинарная альтернатива текстовому формату XML
ProtonVPN	Сервис по поставке услуг виртуальной частной сети (VPN), управляемый швейцарской компанией Proton AG
Psiphon	Бесплатный инструмент для обхода цензуры в интернете с открытым исходным кодом, в котором используется сочетание технологий защищенной связи и обфускации
PTPv2	Протокол синхронизации для промышленных сетей
QQ	Протокол мгновенного обмена сообщениями
QUIC	Экспериментальный интернет-протокол, позволяющий мультиплексировать несколько потоков данных между двумя компьютерами. Протокол работает поверх протокола UDP и содержит возможности шифрования, эквивалентные TLS и SSL
RADIUS	Протокол удаленной аутентификации пользователей, представляет собой ключевой элемент в обеспечении безопасности и управлении доступом в сетях
Radmin	Программа удаленного администрирования ПК для платформы Windows, которая позволяет полноценно работать на нескольких удаленных компьютерах с помощью графического интерфейса
Raft	Компьютерная игра в жанре симулятор выживания в открытом мире, разработанная шведской компанией Redbeet Interactive и изданная Axolot Games
RakNet	Кроссплатформенный сетевой сервис, разработанный Oculus VR для использования в игровой индустрии
RDP	Протокол удаленного рабочего стола
Reddit	Сайт, сочетающий черты социальной сети и форума, где зарегистрированные пользователи могут размещать ссылки на понравившуюся информацию в интернете и обсуждать ее
RESP	Двоичный протокол, в котором используются управляющие последовательности, закодированные в стандартном ASCII
RiotGames	Американская компания, разработчик видеоигр, издатель и организатор киберспортивных турниров (League of Legends)
RipeAtlas	Протокол зонда RIPE Atlas используется для крупнейшей в мире активной сети измерения интернета
RMCP	Протокол многоадресной передачи с ретрансляцией для предоставления услуг сквозной многоадресной передачи данных по сетям на базе IP-протокола
Roblox	Игровая онлайн-платформа и система создания игр, позволяющая любому пользователю создавать свои собственные и играть в созданные другими игры
Roughtime	Протокол с криптографической защитой на базе UDP, который используется для синхронизации времени серверов
RSH	Протокол, позволяющий подключаться удаленно к устройству и выполнять на нем команды

RSYNC	Утилита для удаленной синхронизации и копирования файлов
RTCP	Протокол управления передачей в реальном времени
RTMP	Проприетарный протокол потоковой передачи данных, в основном используемый для передачи потокового видео и аудиопотоков с веб-камер через интернет
RTP	Протокол, используемый при передаче трафика реального времени
RTPS	Real-Time Publish-Subscribe Protocol - это протокол реального времени для распределенных систем, обеспечивающий обмен структурированными данными
RTSP	Real Time Streaming Protocol - потоковый протокол реального времени - позволяет управлять вещанием: выполнять несколько команд, такие как "старт", "стоп", "переход на определенное время"
RX	Клиент-серверный RPC-протокол, расширенная и объединенная версия старых протоколов R и RFTP
S7Comm	Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400
S7CommPlus	Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400. Сложнее протокола S7Comm и использует двухбайтовое поле под названием ID сессии для защиты от атак воспроизведения
Salesforce	Американская компания, разработчик одноименной CRM-системы, предоставляемой по модели SaaS
SAP	Протокол позволяет сетевым устройствам постоянно корректировать данные о том, какие сервисные услуги имеются сейчас в сети
SCTP	Протокол управления потоком передачи с установлением соединения, как TCP, но передающий данные сообщениями, как UDP
SD-RTN	Software Defined Real-time Network - собственный протокол компании Agora, предназначен для потоковой передачи данных с низкой задержкой
Service_Location_Protocol	Протокол обнаружения сервисов, который позволяет компьютерам и иным устройствам находить сервисы в локальной сети без предварительной конфигурации
sFlow	Протокол, используемый для сбора, отправки и анализа информации о сетевом трафике в целях мониторинга
Showtime	Американский кабельный телевизионный канал
Signal	Криптографический протокол, созданный для обеспечения сквозного шифрования голосовых вызовов, видеозвонков и мгновенных сообщений
SignalVoip	Протокол голосовой связи в мессенджере Signal
Sina	Китайская интернет-компания, владеет аналогом Twitter - сервисом Sina Weibo
SinaWeibo	Китайский сервис микроблогов, запущенный компанией Sina Corp
SIP	Протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения, онлайн-игры)
SiriusXMRadio	Американская радиовещательная компания в сфере спутникового радио и онлайн-радио
Skype_Teams	Сервис Microsoft, предназначенный для командной работы и обмена информацией между участниками проекта или команды
Skype_TeamsCall	Бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее видеосвязь через интернет. Опционально использует технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны
Slack	Корпоративный мессенджер
SMBv1	Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети
SMBv23	Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети
SMPP	Протокол одноранговой передачи коротких сообщений
SMTP	Протокол, предназначенный для передачи электронной почты
SMTPS	Протокол для передачи электронной почты, включающий в себя обязательное шифрование
Snapchat	Мобильное приложение обмена сообщениями с прикрепленными фото и видео
SnapchatCall	Протокол голосовой передачи, основанный на VoIP, в мессенджере Snapchat
SNMP	Протокол для управления устройствами в IP-сетях
SOAP	Протокол обмена структурированными сообщениями в распределенной вычислительной среде
SOCKS	Протокол сеансового уровня модели OSI, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно для них) и таким образом использовать сервисы за межсетевыми экранами (файрволами)

Softether	Бесплатное кроссплатформенное многопротокольное программное обеспечение VPN-клиента и VPN-сервера с открытым исходным кодом
SOMEIP	Автомобильное программное обеспечение, которое может использоваться для передачи управляющих сообщений
SoundCloud	Онлайн-платформа для распространения оцифрованной звуковой информации (например, музыкальных произведений)
Source_Engine	Игровой сервис, разработанный Valve Corporation для собственного использования и лицензирования другим разработчикам
Spotify	Стриминговый сервис, позволяющий легально прослушивать музыкальные композиции, аудиокниги и подкасты, не скачивая их на устройство
SRTP	Протокол, определяющий профиль протокола RTP. Предназначен для шифрования, установления подлинности сообщения, целостности, защиты от подмены данных RTP в однонаправленных и multicast-передачах медиа и приложениях
SSDP	Протокол, служащий для объявления и обнаружения сетевых сервисов
SSH	Протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений
StarCraft	Серия компьютерных игр в жанре стратегии в реальном времени, разработанная компанией Blizzard Entertainment
Steam	Онлайн-сервис цифрового распространения компьютерных игр и программ
SteamDatagramRelay	Закрытая виртуальная игровая сеть Valve. Используя функции API, позволяет перенести игровой трафик на сетевые магистрали Valve
STOMP	Simple Text Oriented Messaging Protocol, протокол обмена сообщениями
STUN	Протокол, который позволяет клиенту, находящемуся за сервером трансляции адресов (или за несколькими такими серверами), определить свой внешний IP-адрес, способ трансляции адреса и порта во внешней сети, связанный с определенным внутренним номером порта
Syncthing	Приложение, позволяющее синхронизировать файлы между несколькими устройствами
Syslog	Протокол отправки и регистрации сообщений о происходящих в системе событиях
Tailscale	VPN-сервис, который работает поверх WireGuard и позволяет получить доступ к контроллеру даже если у вас нет своего VPN-сервера
TargusDataspeed	Проприетарный протокол, используемый для тестирования пропускной способности. Был разработан компанией TARGUSinfo
Teams	Корпоративная платформа, объединяющая в рабочем пространстве чат, встречи, заметки и вложения
TeamSpeak	Компьютерная программа, предназначенная для голосового общения в сети посредством технологии VoIP
TeamViewer	Программное обеспечение для удаленного доступа, удаленного управления и удаленного обслуживания компьютеров и других конечных устройств
Telegram	Кроссплатформенная система мгновенного обмена сообщениями с функциями обмена текстовыми, голосовыми и видеосообщениями, а также стикерами, фотографиями и файлами многих форматов
TelegramVoip	Голосовые и видеозвонки в мессенджере Telegram
Telnet	Протокол для реализации текстового терминального интерфейса по сети
Tencent	Китайский конгломерат, создавший китайский клон ICQ, собственную валюту, отдельную соцсеть, множество игр, торговую площадку и WeChat
TencentGames	Подразделение Tencent Interactive Entertainment, выпускающее видеоигры, разработчик PUPG MOBILE
TencentVideo	Китайская стриминговая платформа, принадлежащая Tencent
Teredo	Сетевой протокол, предназначенный для передачи IPv6-пакетов через сети IPv4, в частности, через устройства, работающие по технологии NAT, путем их инкапсуляции в UDP-дейтаграммы
TES_Online	The Elder Scrolls Online - это MMORPG, действие которой разворачивается в фэнтезийном мире Тамриэля
TeslaServices	Портал с сервисной и диагностической информацией для компаний и частных лиц, занимающихся профессиональным обслуживанием и ремонтом автомобилей Tesla
TFTP	Простой протокол передачи файлов, как правило, используется при загрузке бездисковых систем
Threads	Онлайн-сервис для микроблогинга, разработанный компанией Meta Platforms как дополнение к Instagram
Threema	Кроссплатформенное зашифрованное приложение для обмена мгновенными сообщениями
Thrift	Программный фреймворк Apache Thrift, предназначенный для масштабируемой разработки межъязыковых сервисов
Tidal	Интернет-сервис подписки на музыку, подкасты и потоковое видео, сочетающий в себе звук без потерь и музыкальные видеоролики высокой четкости с эксклюзивным контентом и специальными функциями для музыки
TikTok	Сервис для создания и просмотра коротких видео, принадлежащий пекинской компании ByteDance
TINC	Открытый, самомаршрутизирующийся сетевой протокол и программная реализация, используемая для сжатых и зашифрованных виртуальных частных сетей
TiVoConnect	Протокол TivoConnect обеспечивает автоматическое обнаружение оборудования для двух или более систем медиаплееров Tivo, работающих в одной сети

TLS	Протокол защиты транспортного уровня
TocaBoca	Интерактивная мобильная игра
Tor	Протокол анонимной сети виртуальных туннелей, предоставляющий передачу данных в зашифрованном виде
TPLINK_SHP	Протокол TP-Link Smart Home Protocol используется для подключения устройств "Умного дома" с помощью приложения-компаньона
TruPhone	Глобальная мобильная сеть, которая занимается разработкой технологии eSim, позволяющей подключаться к разным провайдерам без замены сим-карты
Tumblr	Протокол микроблогов, включающий в себя множество картинок, статей, видео и gif-изображений по разным тематикам и позволяющий пользователям публиковать посты в их тамблелог
TuneIn	Американский аудиопотоковый сервис, транслирующий новости, эфиры радиостанций, спортивные мероприятия, музыку и подкасты
TunnelBear	Кроссплатформенный VPN-клиент
TuyaLP	Протокол Tuya LAN используется для взаимодействия многих IoT-устройств, включая светодиодные лампы, лампочки, умные розетки и другое
Twitch	Видеостриминговый сервис, специализирующийся на тематике компьютерных игр, в том числе на трансляциях геймплея и киберспортивных турниров
Twitter	Американский сервис микроблогов и социальная сеть, в которой пользователи публикуют сообщения и взаимодействуют с ними
UBNTAC2	Утилита управления оборудованием Ubiquiti airControl, версия 2
UbuntuONE	Онлайн-хранилище для обмена файлами и синхронизации между компьютерами и мобильными устройствами
UFTP	Протокол передачи файлов на основе UDP
UltraSurf	Бесплатная утилита для обхода цензурных ограничений в интернете
UMAS	Unified Messaging Application Services - проприетарный протокол Schneider Electric, который используется для конфигурации, мониторинга сбора данных и управления промышленными контроллерами Schneider Electric
Unknown	Не распознанные модулем протоколы и приложения
Usenet	Протокол, используемый для общения и публикации файлов
VHUA	Протокол, который использовался для Skype-подобных сервисов в Китае
Viber	Приложение-мессенджер, которое позволяет отправлять сообщения, совершать видео- и голосовые VoIP-звонки через интернет
ViberVoip	Аудио/видеозвонки, совершаемые с помощью приложения Viber
Vimeo	Американский сервис для публикации и просмотра видео
VK	Приложение для взаимодействия с социальной сетью ВКонтакте
VMware	Американская компания-разработчик программного обеспечения для виртуализации
VNC	Протокол удаленного доступа к рабочему столу
VRRP	Протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
Vudu	Потоковый сервис цифрового видео
VXLAN	Протокол инкапсуляции, который обеспечивает подключение центров обработки данных с использованием туннелирования для расширения соединений канального уровня в используемой сети сетевого уровня
Warcraft3	Компьютерная игра в жанре стратегии в реальном времени с элементами RPG
Waze	Бесплатное социальное навигационное приложение для мобильных устройств, позволяющее отслеживать ситуацию на дорогах в режиме реального времени, прокладывать оптимальные маршруты, узнавать о расположении радаров скорости
WebDAV	Набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах
Webex	Американская компания, которая разрабатывает и продает приложения для веб-конференций, видео-конференц-связи и контакт-центра как сервиса
WebSocket	Протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером, используя постоянное соединение
WeChat	Мобильная коммуникационная система для передачи текстовых и голосовых сообщений, разработана китайской компанией Tencent
WhatsApp	Американский бесплатный сервис обмена мгновенными сообщениями и голосовой связи по IP, принадлежащий компании Meta
WhatsAppCall	Протокол голосовой передачи, основанный на VoIP
WhatsAppFiles	Протокол загрузки медиафайлов (изображений, видео, музыки, документов) мессенджера WhatsApp

Whois-DAS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP, применяется для получения регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем
Wikipedia	Самая крупная в мире онлайн-энциклопедия
WindowsUpdate	Сервис обновления операционной системы Windows
WireGuard	Высокоскоростной и безопасный VPN-протокол
WorldOfKungFu	3D MMORPG с боевыми искусствами, основанная на традиционной китайской культуре
WorldOfWarcraft	Массовая многопользовательская ролевая онлайн-игра
WSD	Протокол многоадресного обнаружения для поиска сервисов в локальной сети. Работает через TCP- и UDP-порт 3702 и использует IP-адрес многоадресной рассылки 239.255.255.250 или ff02::c
Xbox	Домашняя игровая консоль, разработанная и выпущенная американской корпорацией Microsoft
XDMCP	Протокол аутентификации между X-сервером и X-клиентом
Xiaomi	Китайская корпорация-производитель смартфонов, компьютерной и бытовой техники
Yahoo	Американская компания, специализирующаяся на проектах и услугах в интернете. Владеет поисковой системой с одноименным названием
Yandex	Российская транснациональная компания в отрасли информационных технологий, владеющая одноименной системой поиска в интернете, интернет-порталом и веб-службами
YandexCloud	Публичная облачная платформа, разработанная российской интернет-компанией Яндекс
YandexDirect	Сервис для размещения объявлений контекстной рекламы на Яндексе и на сайтах-партнерах его рекламной сети
YandexDisk	Сервис для хранения данных в облаке
YandexMail	Почтовый сервис от компании Яндекс
YandexMarket	Сервис заказа товаров онлайн
YandexMetrika	Бесплатный сервис веб-аналитики, предлагаемый Яндексом, который отслеживает и сообщает о трафике веб-сайта
YandexMusic	Стриминговый сервис компании Яндекс, позволяющий слушать музыкальные композиции, их подборки, альбомы
Yojimbo	Менеджер личной информации для MacOS от Bare Bones Software. Позволяет хранить заметки, изображения и медиафайлы, URL-адреса, веб-страницы и пароли
YouTube	Видеохостинг, предоставляющий пользователям услуги хранения, доставки и показа видео
YouTubeUpload	Загрузка файлов на видеохостинг YouTube
Z3950	Клиент-серверный протокол для поиска и получения информации с удаленных компьютерных баз данных
Zabbix	Свободная система мониторинга статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования
Zattoo	Телевизионная платформа, которая предлагает прямые телетрансляции и контент по запросу для компьютеров, мобильных телефонов, планшетов и других сетевых устройств
ZeroMQ	Высокопроизводительная асинхронная библиотека обмена сообщениями, ориентированная на использование в распределенных и параллельных вычислениях
Zoom	Проприетарная программа для организации видеоконференций, разработанная компанией Zoom Video Communications
ZUG	Протокол ZUG является частью консенсусной модели Casper 2.0

Если нужного приложения нет в таблице **Доступ к приложениям** профиля **Контроля приложений**, но необходимо разрешить или заблокировать это приложение, используйте правила **Межсетевого экрана**:

1. Выясните, какие адреса серверов, порты и протоколы использует приложение. Для этого:
   - Обратитесь к разработчикам приложения или найдите информацию в открытых источниках.
   - Используйте логирование трафика и журнал Межсетевой экран.
2. Создайте правило Межсетевого экрана, которое будет разрешать или блокировать трафик по этим параметрам.

Также можно направить в Техническую поддержку запрос на добавление нового протокола, чтобы в будущем приложение появилось в списке **Контроля приложений**.

Полезные ссылки

- **Особенности создания профилей**
- **Пример создания иерархической структуры**
- **Настройка фильтрации трафика**

- **Как разрешить доступ к ресурсам в ограниченной сети**
- **Блокировка популярных ресурсов**

Особенности создания профилей

Классический контекст | Высокопроизводительный контекст

Принцип создания профилей **Контроля приложений** - все протоколы и приложения, которые не были запрещены, остаются разрешены.

Для удобства настройки модуля фильтрации рекомендуем объединить пользователей в несколько групп/подгрупп (например, в соответствии с организационной структурой компании) и настроить профиль **Контроля приложений** отдельно для каждой группы.

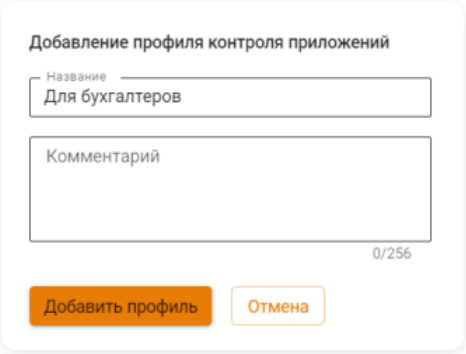
Создание профилей и добавление в правила Межсетевого экрана

Разберем создание профилей и добавление правил **Межсетевого экрана** на примере ограничения доступа к социальным сетям пользователям группы **Бухгалтерия**.

Создание профиля Контроля приложений

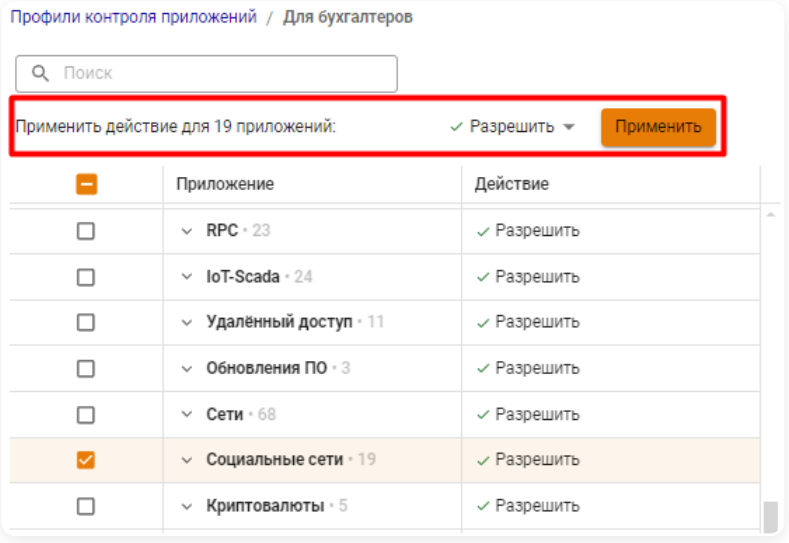
1. Перейдите в **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Заполните **Название**, **Комментарий** (необязательно) и добавьте профиль:

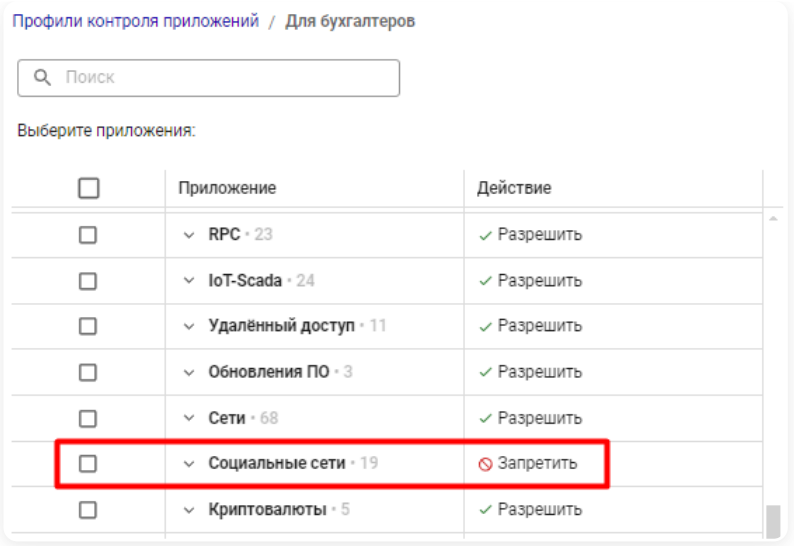


3. Нажмите в столбце **Управление** на  , затем **Доступ к приложениям**.

4. Выберите **Социальные сети** (при необходимости используйте поиск). Появится строка с выбором действия:



5. Примените действие **Запретить** рядом со строкой поиска и нажмите **Применить**. Действие применится к выбранным приложениям:



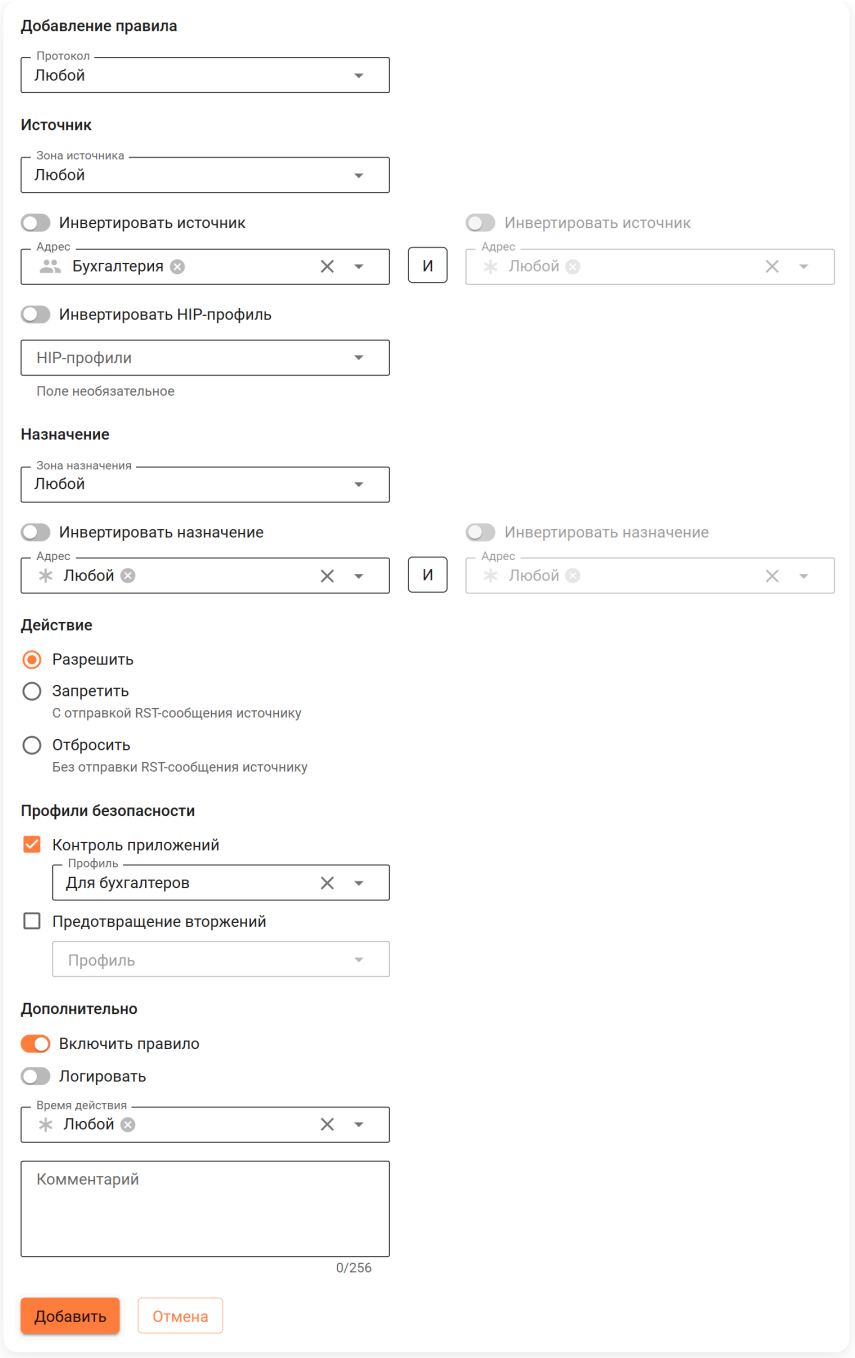
К неизвестным источникам по умолчанию применяется действие **Разрешить** (доступно для редактирования).

6. Нажмите **Сохранить**.

Добавление профиля в правила Межсетевого экрана

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать с помощью профиля **Контроля приложений**.
- **Источник** - выберите **Адрес**, **Зону**, созданную в **Системном контексте**, и **HIP-профиль** источника трафика.
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика, созданную в **Системном контексте**.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** в блоке **Профили безопасности** и из раскрывающегося списка выберите профиль, запрещающий социальные сети сотрудникам бухгалтерии.

4. Включите правило и нажмите **Добавить**.

5. Если в **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правило INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку DNS-трафик направляется в INPUT.

Иерархическая структура Профилей контроля приложений

Один из вариантов корректного применения политик безопасности к вложенной структуре пользователей - построение иерархической структуры профилей **Контроля приложений**:

- Профили для самой большой группы пользователей запрещают наибольшее количество протоколов и приложений.

- Профили для более мелких групп пользователей повторяют запрет для самой большой группы пользователей, но точечно разрешают определенные приложения и протоколы для конкретных подгрупп.
- Профили для конкретных пользователей разрешают определенные протоколы и приложения, необходимые этим конкретным пользователям. В этих профилях также остаются запреты, которые должны сохраниться для этих пользователей.

Полезные ссылки

- **Пример создания иерархической структуры**
- **Настройка фильтрации трафика, для которого в таблице FORWARD нет правил**

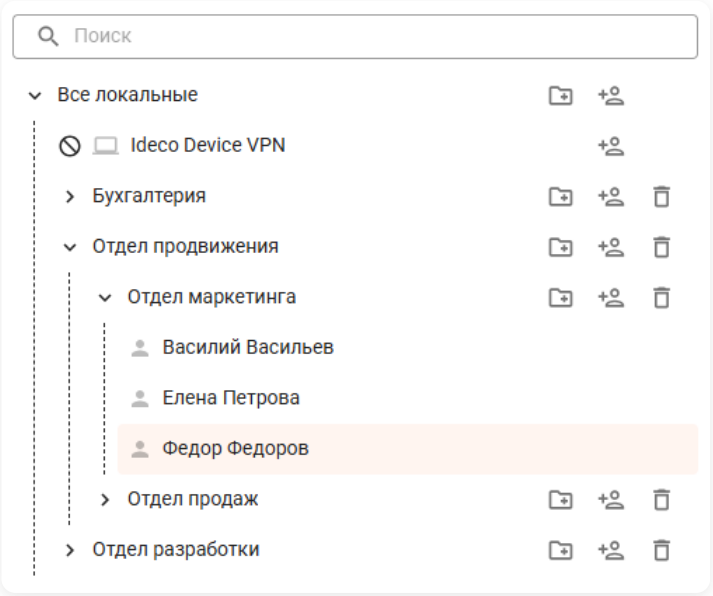
Пример создания иерархической структуры

Классический контекст | Высокопроизводительный контекст

Необходимо настроить профили **Контроля приложений** в соответствии с требованиями:

- Всем пользователям запрещены компьютерные игры, контент для взрослых, майнинг и криптовалюты.
- Доступ к социальным сетям разрешен только **Отделу продвижения**.
- Доступ к стриминговым сервисам разрешен только **Отделу маркетинга**.
- Доступ к музыкальным приложениям разрешен только **Федору Федорову** из **Отдела маркетинга**.

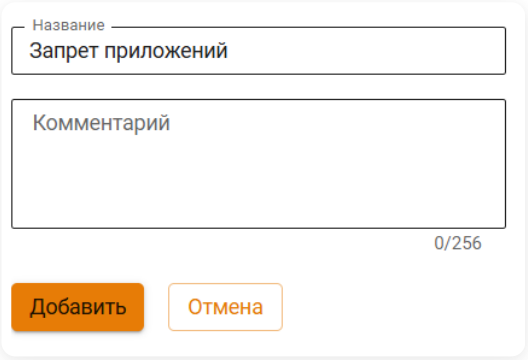
В описанном примере **Федор Федоров** - сотрудник **Отдела маркетинга**, а **Отдел маркетинга** - структурное подразделение **Отдела продвижения**:



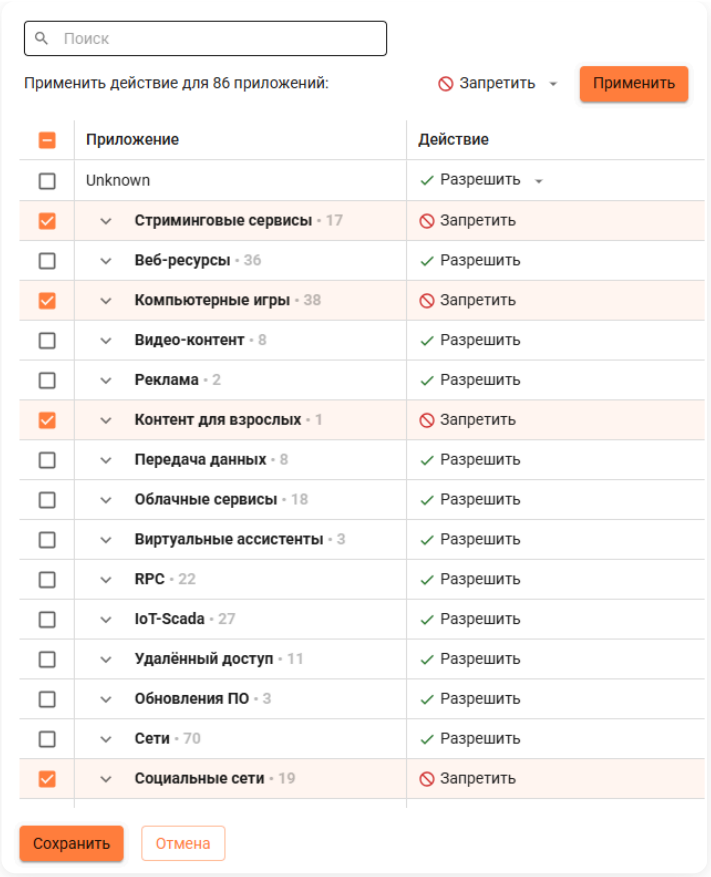
Создание профилей Контроля приложений

Создайте профили в соответствии с условиями примера:

1. Перейдите в **Профили безопасности** → **Контроль приложений**, чтобы создать профиль, запрещающий доступ к социальным сетям, стриминговым сервисам, музыкальным приложениям, компьютерным играм, контенту для взрослых, майнингу и криптовалютам. Нажмите **Добавить** и введите название профиля:



2. Настройте добавленный профиль:



- Перейдите в **Доступ к приложениям** и выберите группы приложений, которые необходимо запретить (перечислены в описании примера).
- Установите настройку **Запретить** и нажмите **Применить** в правом верхнем углу.
- После применения действия нажмите **Сохранить**.

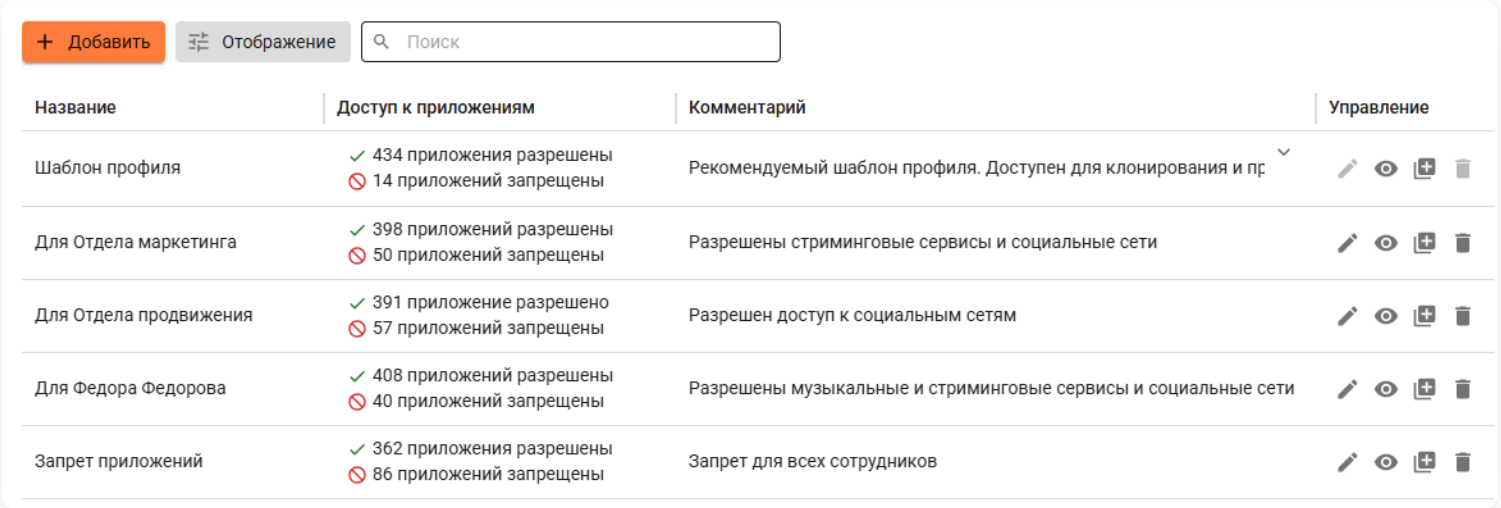
3. Создайте профиль для **Отдела продвижения**, разрешающий доступ к социальным сетям. Для этого:

- Клонируйте созданный профиль, нажав на  в столбце **Управление**.
- Отредактируйте клонированный профиль: поменяйте название (например, на **Для Отдела продвижения**) и настройки доступа к приложениям (разрешите доступ к социальным сетям).

4. Аналогично создайте профиль для Отдела маркетинга, разрешающий доступ к стриминговым сервисам. Для этого клонируйте профиль **Для Отдела продвижения**, введите название (например, **Для Отдела маркетинга**) и разрешите в нем доступ к стриминговым сервисам.

5. Создайте профиль для **Федора Федорова**, разрешающий доступ к музыкальным сервисам. Для этого клонируйте профиль **Для Отдела маркетинга** и установите необходимые настройки.

В итоге должен получиться набор профилей, учитывающий настройки, описанные в примере:

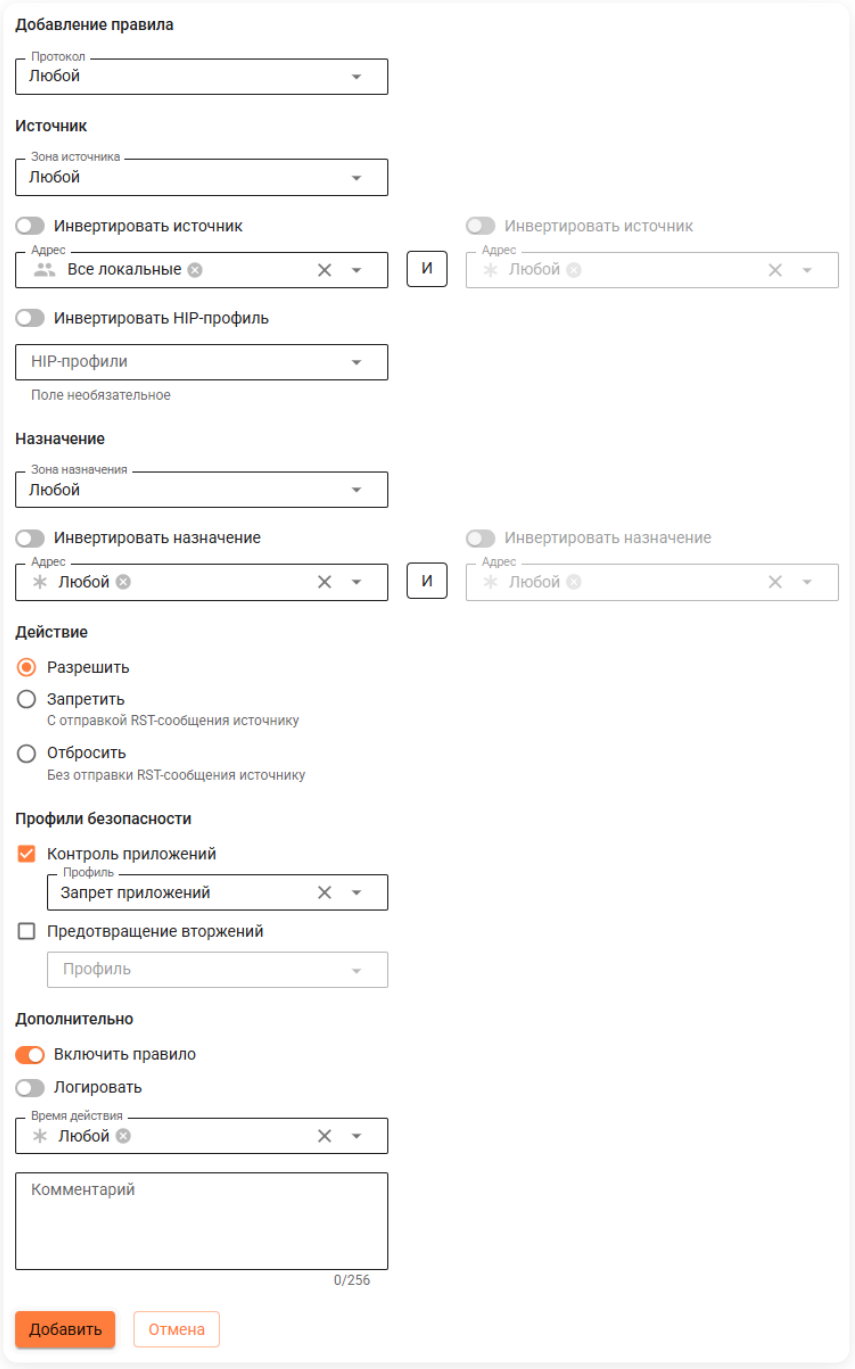


Создание правил Межсетевого экрана

Теперь необходимо создать и включить правила в **Межсетевом экране**, чтобы применить настройки для конкретных групп пользователей и установить приоритет прохождения трафика:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

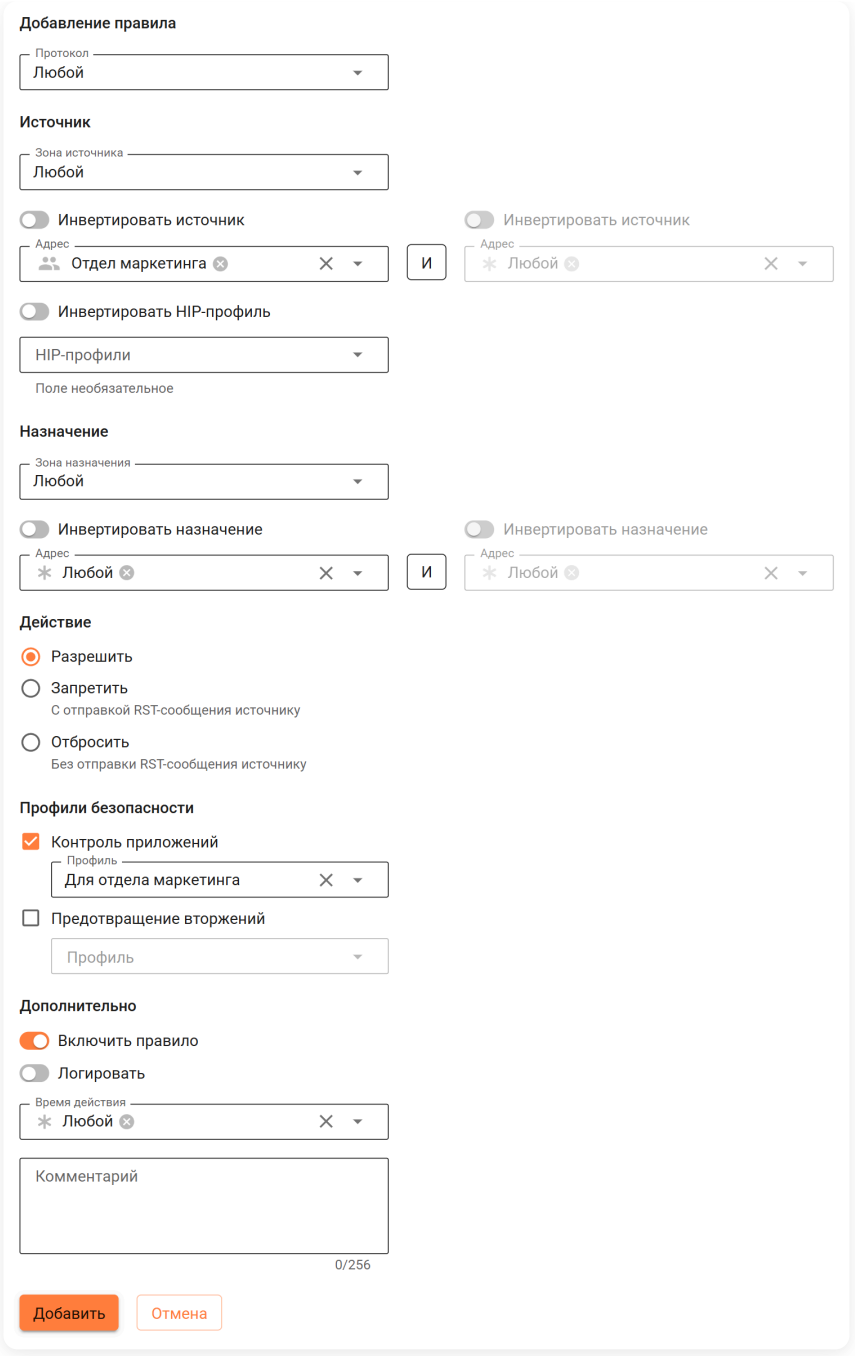
2. Заполните поля:



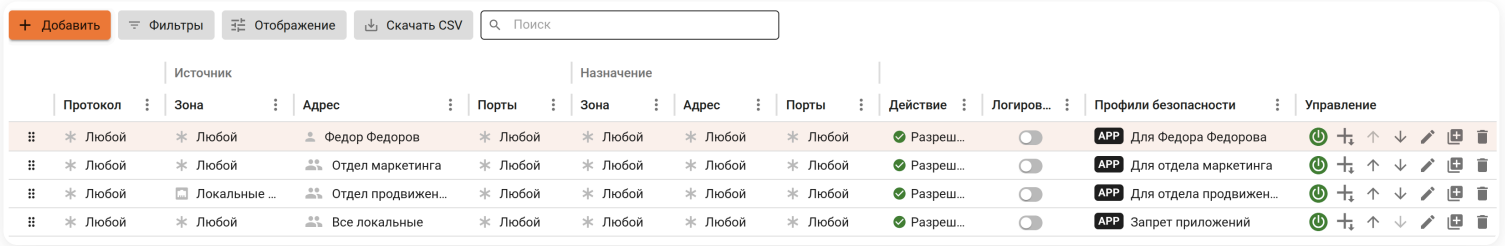
- **Адрес источника** - группа пользователей **Все локальные**.
- **Действие** - **Разрешить**.
- **Профили безопасности** - **Контроль приложений**, профиль **Запрет приложений**.

3. Включите правило и нажмите **Добавить**.

4. Аналогично создайте правила для каждого профиля. При создании правила **Межсетевого экрана** укажите соответствующий профилю адрес источника. Например, при создании правила с профилем фильтрации **Для Отдела маркетинга** выберите в поле **Адрес** блока **Источник** группу **Отдел маркетинга**:



5. Чтобы трафик проходил в соответствии с условиями примера, установите в **Межсетевом экране** следующую последовательность правил:



Чем выше в таблице стоит правило, тем выше его приоритет.

Разрешающее правило для сотрудника не сработает, если выше в таблице **Межсетевого экрана** находится правило, запрещающее трафик для отдела, в котором работает этот сотрудник.

6. Если в **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правила **INPUT** для протоколов **TCP** и **UDP** с теми же профилями безопасности, источником и портом `53` в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку DNS-трафик направляется в **INPUT**.

Настройка фильтрации трафика

Классический контекст | Высокопроизводительный контекст

Создайте профиль **Контроля приложений**, соответствующий нужным правилам:

1. Перейдите в **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Введите **Название** профиля, **Комментарий** и добавьте профиль.

3. Перейдите в **Доступ к приложениям**.

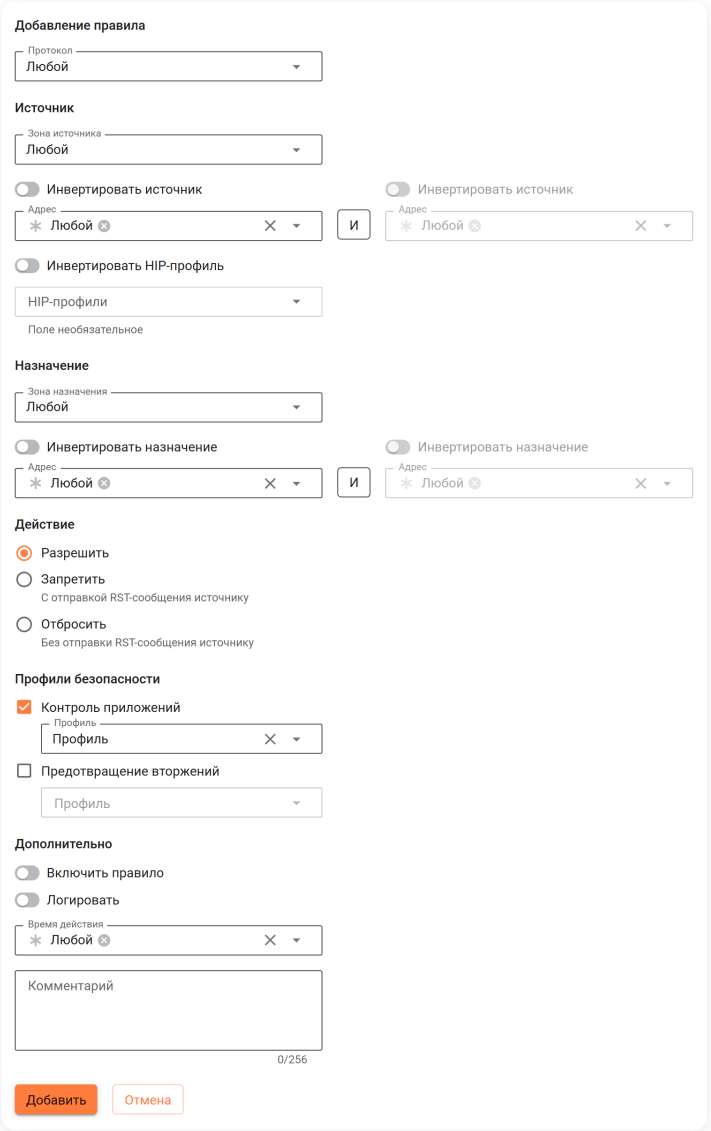
4. Выберите протоколы или группы протоколов и действия (**Запретить** или **Разрешить**), которые будут к ним применяться, затем нажмите **Применить**.

5. Нажмите **Сохранить**.

Далее создайте правило **Межсетевого экрана** с созданным профилем **Контроля приложений**:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите **Любой**.
- **Источник**:

    - **Зона источника** - выберите **Локальные интерфейсы**.
    - **Адрес** - укажите при необходимости адрес источника трафика.
    - **HIP-профиль** - укажите при необходимости профиль, соответствующий устройству, от которого исходит трафик.
- **Назначение**:
    - **Зона назначения** - выберите **Любой**.
    - **Адрес** - укажите при необходимости адрес источника трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** в блоке **Профили безопасности** и из раскрывающегося списка выберите созданный ранее профиль.

4. Включите правило и нажмите **Добавить**.

5. Поместите правило в конец таблицы **Межсетевого экрана**. Если в таблице есть правило, запрещающее все, поместите правило с профилем **Контроля приложений** над ним.

6. Если в **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, зоной источника **Локальные интерфейсы** и портом 53 в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку DNS-трафик направляется в INPUT.

Профили предотвращения вторжений

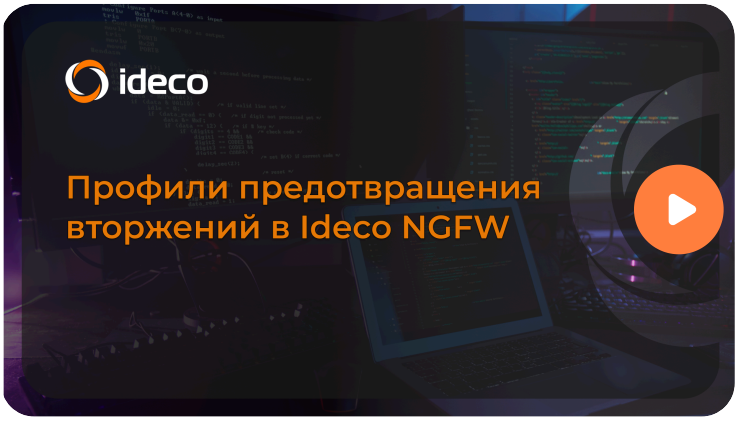
Классический контекст | Высокопроизводительный контекст | API

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



В разделе **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые NGFW Novum будет применять к трафику, соответствующему этим сигнатурам.

Профили предотвращения вторжений применяются при создании правил в разделе **Правила трафика** → **Межсетевой экран**.

Если профиль не добавлен в правила таблицы **FORWARD** или **INPUT** раздела **Правила трафика** → **Межсетевой экран**, трафик не будет фильтроваться модулем **Предотвращение вторжений**.

В обработке трафика не участвуют:

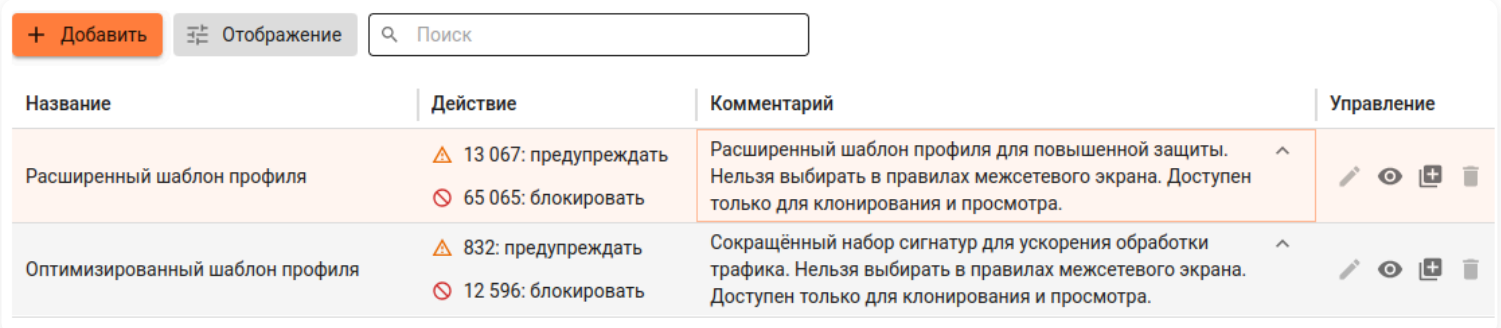
- Сигнатуры, не используемые в профилях.
- Профили, не используемые в правилах **Межсетевого экрана**.

Создание профилей

1. Перейдите в раздел **Профили безопасности** → **Предотвращение вторжений** и нажмите **Добавить**.

Создание профиля через шаблон

1. Для клонирования нажмите :



- **Расширенный шаблон профиля** - подходит для максимальной защиты от кибератак. Он включает динамически обновляемые черные списки хостов и эффективно очищает трафик из внешних сетей.
- **Оптимизированный шаблон профиля** - используется для достижения максимальной производительности. Он почти не содержит правил блокировки по черным спискам, поэтому не подходит для очистки внешнего трафика.

2. Чтобы просмотреть или изменить созданный профиль (описание и правила выбора сигнатур), нажмите на или .

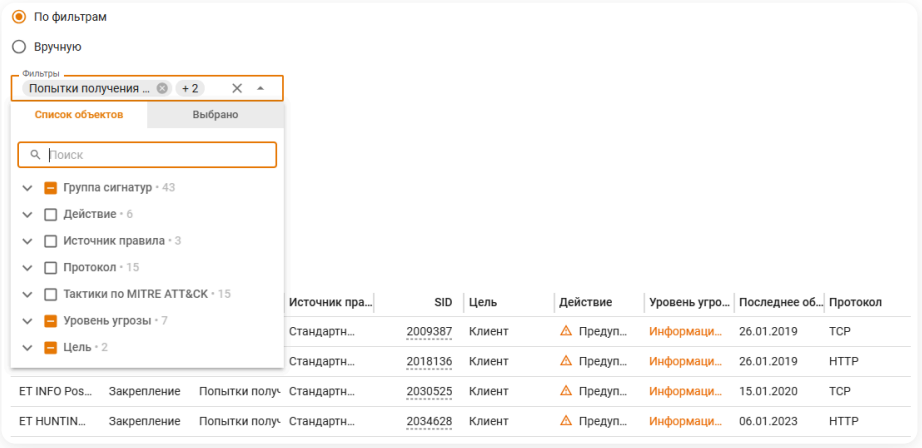
2. Введите название профиля, комментарий и нажмите **Добавить**.

3. Перейдите на вкладку **Сигнатуры** и нажмите **Добавить сигнатуры**.

4. Выберите способ добавления сигнатур в профиль:

По фильтрам

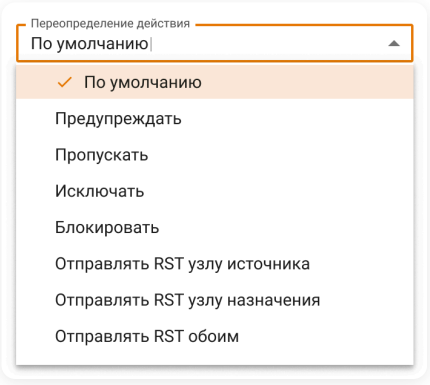
5. Выберите **Фильтры**. В таблице ниже отобразятся сигнатуры, соответствующие каждому из выбранных фильтров:



Доступные фильтры

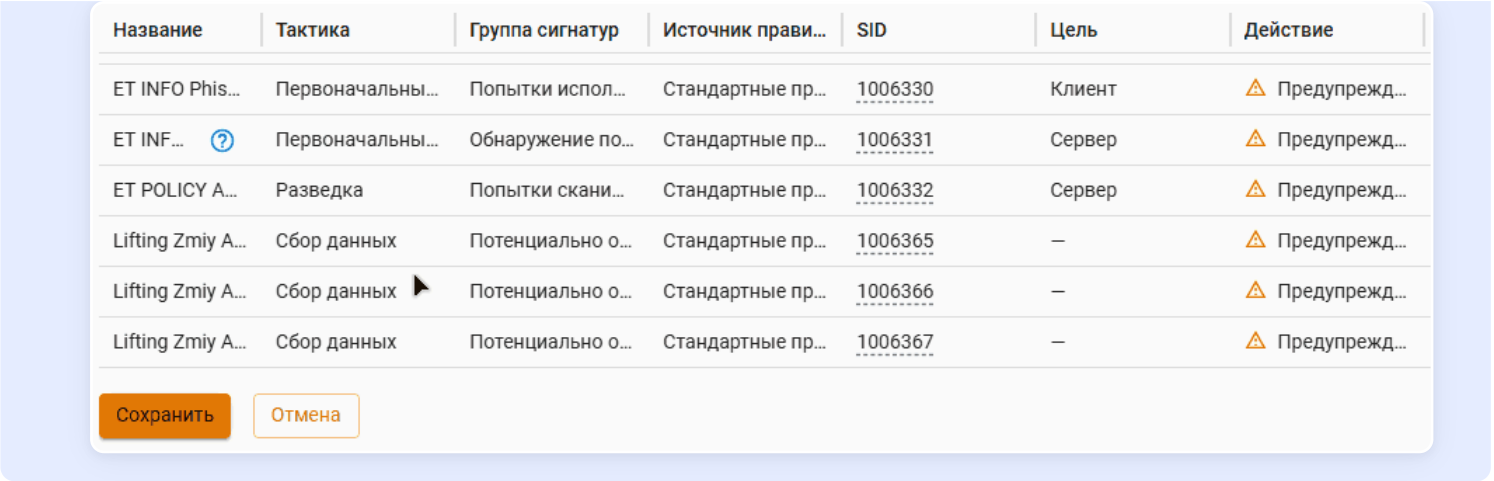
- **Группа сигнатур** - фильтр по готовым наборам сигнатур, сгруппированным по типу угроз.
- **Действие** - фильтр по действию, которое Ideco NGFW Novum применит к трафику, соответствующему сигнатуре.
- **Источник правила** - фильтр по источнику сигнатуры.
- **Протокол** - фильтр по сетевому протоколу, который анализирует сигнатура.
- **Тактики по MITRE ATT&CK** - фильтр по тактикам согласно матрице MITRE ATT&CK.
- **Уровень угрозы** - фильтр по степени опасности сигнатур в соответствии со стандартом CVSS (Common Vulnerability Scoring System).
- **Цель** - фильтр по цели атаки, которую обнаруживает сигнатура.

6. Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие **По умолчанию**:

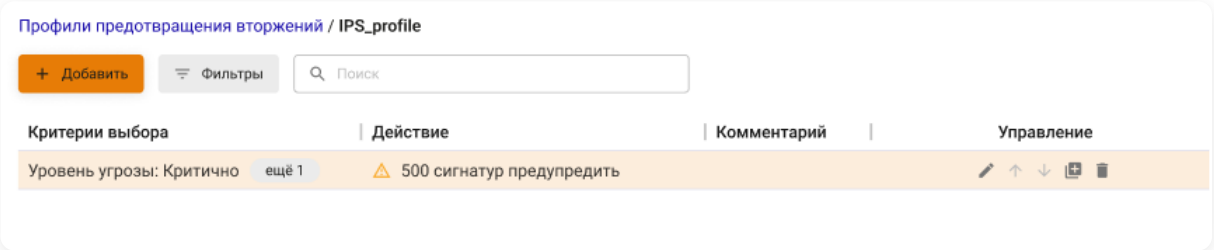


- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения. Система пропускает трафик, как если бы угроза отсутствовала.
- **Исключать** - исключить сигнатуру из профиля. Удаляет сигнатуру из анализа системы IPS, что снижает количество ложных срабатываний и предотвращает анализ по нежелательным правилам.
- **Блокировать** - отбросить пакет и сгенерировать предупреждение.
- **Отправлять RST узлу источника** - отправить ошибку `RST/ICMP unreach` отправителю пакета.
- **Отправлять RST узлу назначения** - отправить пакет с ошибкой `RST/ICMP error` получателю исходного пакета.
- **Отправлять RST обоим** - отправить пакеты с ошибкой `RST/ICMP error` отправителю и получателю исходного пакета.

Flowbit-сигнатуры предназначены для маркировки трафика. К Flowbit-сигнатуре могут быть применены только действия **Пропускать** и **Предупреждать**:

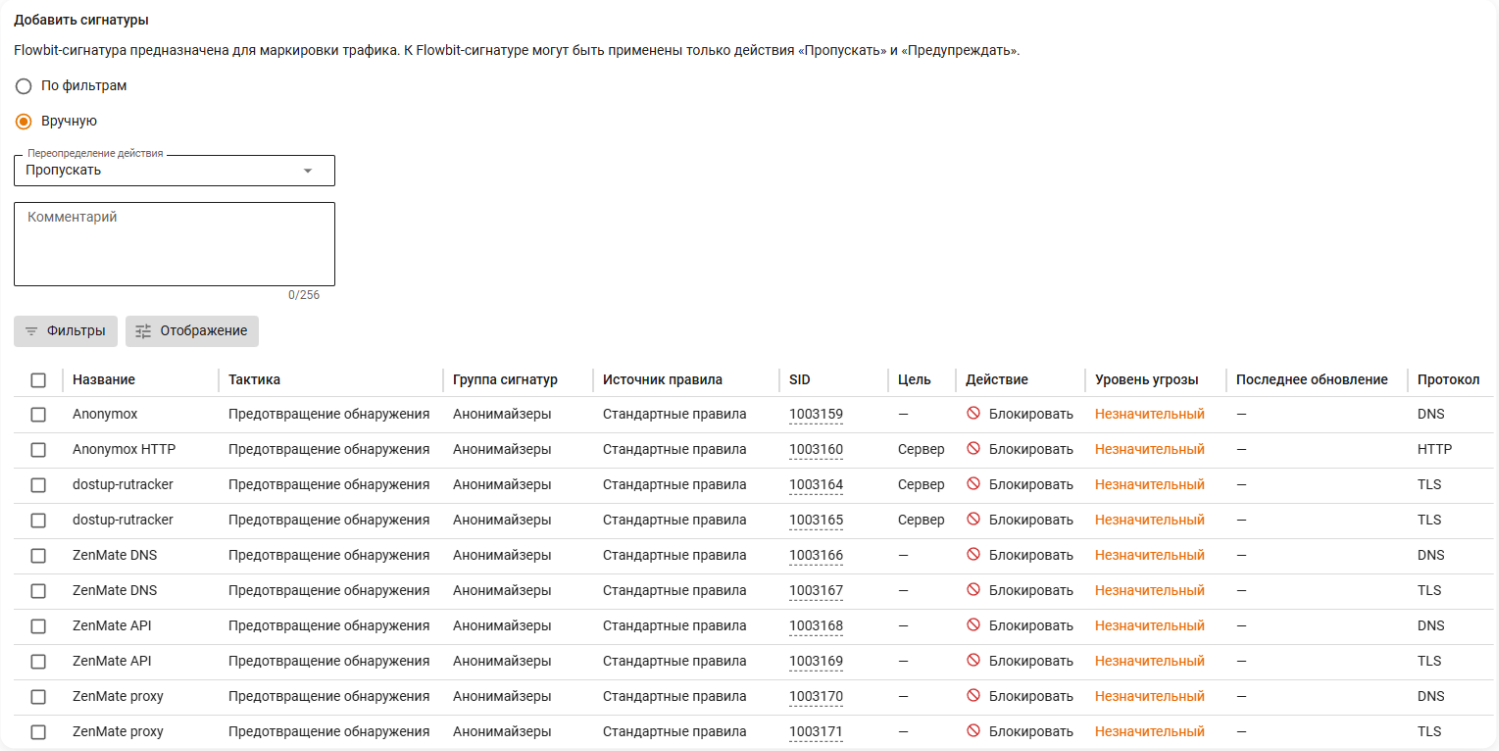


7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

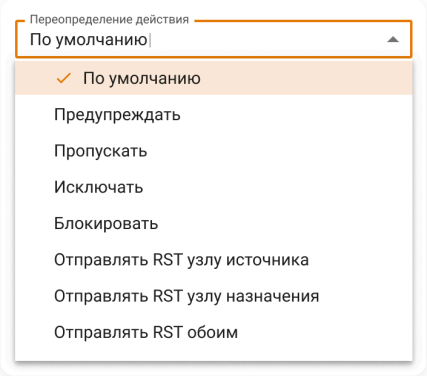


Вручную

5. В таблице отметьте сигнатуры, которые хотите добавить в профиль (при необходимости воспользуйтесь **Фильтром** отображения):

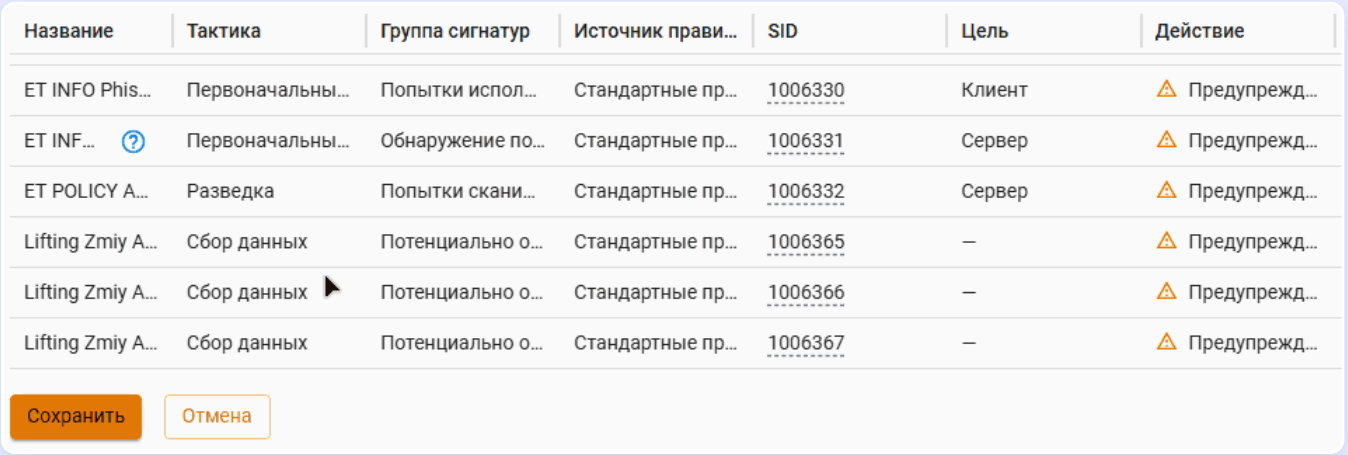


6. Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие **По умолчанию**:

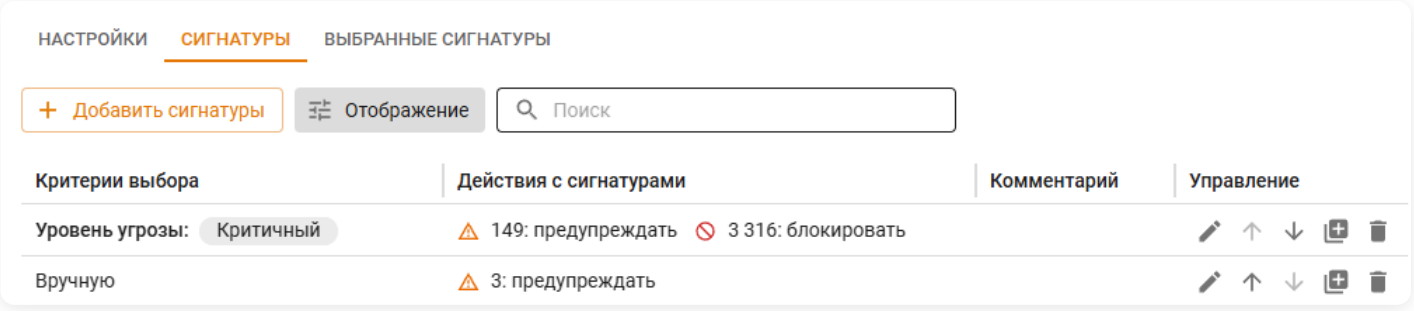


- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения. Система пропускает трафик, как если бы угроза отсутствовала.
- **Исключать** - исключить сигнатуру из профиля. Удаляет сигнатуру из анализа системы IPS, что снижает количество ложных срабатываний и предотвращает анализ по нежелательным правилам.
- **Блокировать** - отбросить пакет и сгенерировать предупреждение.
- **Отправлять RST узлу источника** - отправить ошибку `RST/ICMP unreach` отправителю пакета.
- **Отправлять RST узлу назначения** - отправить пакет с ошибкой `RST/ICMP error` получателю исходного пакета.
- **Отправлять RST обоим** - отправить пакеты с ошибкой `RST/ICMP error` отправителю и получателю исходного пакета.

Flowbit-сигнатуры предназначены для маркировки трафика. К Flowbit-сигнатуре могут быть применены только действия **Пропускать** и **Предупреждать**:



7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

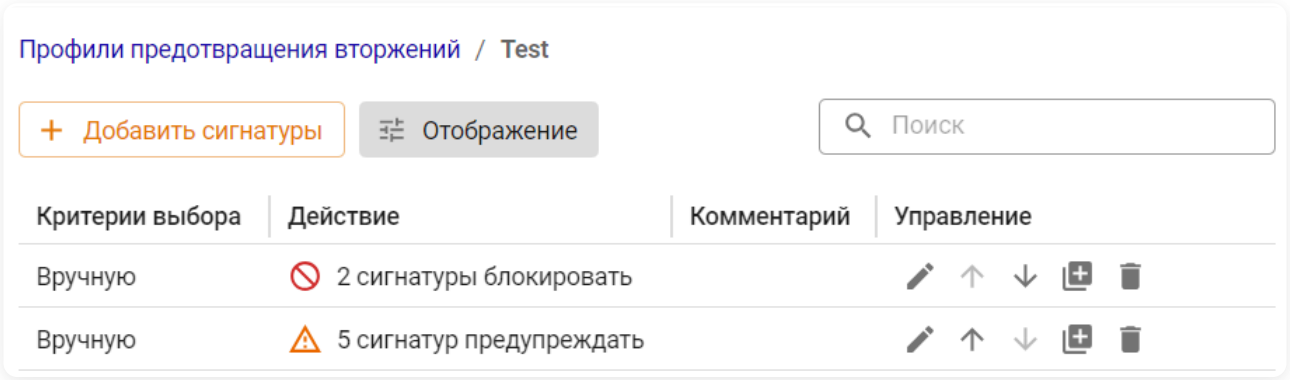


Количество сигнатур, отображаемых в таблице профилей, не всегда соответствует количеству сигнатур, добавленных при создании профиля. Это связано с тем, что для каждой сигнатуры может быть настроено несколько действий, но применяется только приоритетное. Приоритет определяется порядком правил внутри профиля.

В один профиль **Предотвращения вторжений** можно добавить несколько правил выбора сигнатур. Приоритет можно менять в таблице профиля кнопками ↑ и ↓.

Пример отображения профиля при выборе нескольких действий сигнатур

Настройки профиля Test:



- Действие **Блокировать** применяется для сигнатур Anonymox и Anonymox HTTP (2 сигнатуры).
- Действие **Предупреждать** применяется для сигнатур Anonymox, Anonymox HTTP, ZenMate DNS, ZenMate API и ZenMate proxy (5 сигнатур).
- Блокирующее правило приоритетнее предупреждающего.

При переходе в раздел **Профили безопасности** → **Предотвращение вторжений** в профиле Test отображаются 2 сигнатуры с действием **Блокировать** и 3 сигнатуры с действием **Предупреждать**, потому что фактически для дублирующихся сигнатур применяется более приоритетное правило:

Пример добавления сигнатур для исключения из анализа системы

1. Откройте редактирование профиля **Предотвращения вторжений**, нажав .

2. Перейдите на вкладку **Сигнатуры** и нажмите **Добавить сигнатуры**.

3. Выберите сигнатуры для исключения из фильтров или добавьте их вручную:

- Используйте ручной способ добавления и фильтрацию для точного поиска сигнатуры, например, по SID:

4. Выберите действие **Исключать** и нажмите **Добавить**.

5. В таблице измените приоритет сигнатур, переместив сигнатуры с действием **Исключить** выше:

6. Сохраните изменения в профиле.

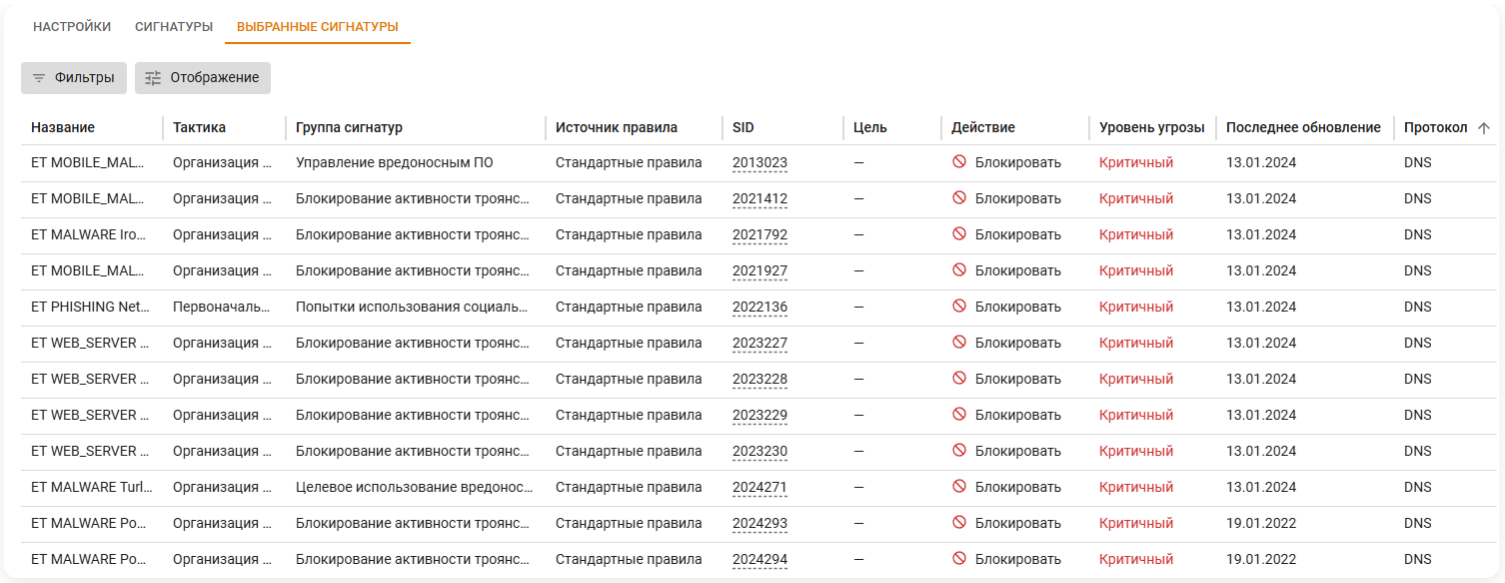
Использование оперативной памяти:

- Шаблоны профилей не потребляют оперативную память.
- Настроенный профиль потребляет оперативную память, даже если не задействован в правилах Межсетевого экрана.
- Объем оперативной памяти, потребляемый одним профилем, зависит от количества сигнатур. Потребление памяти профилями, настроенными по шаблонам:
  - Расширенный: ~450 МБ.
  - Оптимизированный: ~100 МБ.

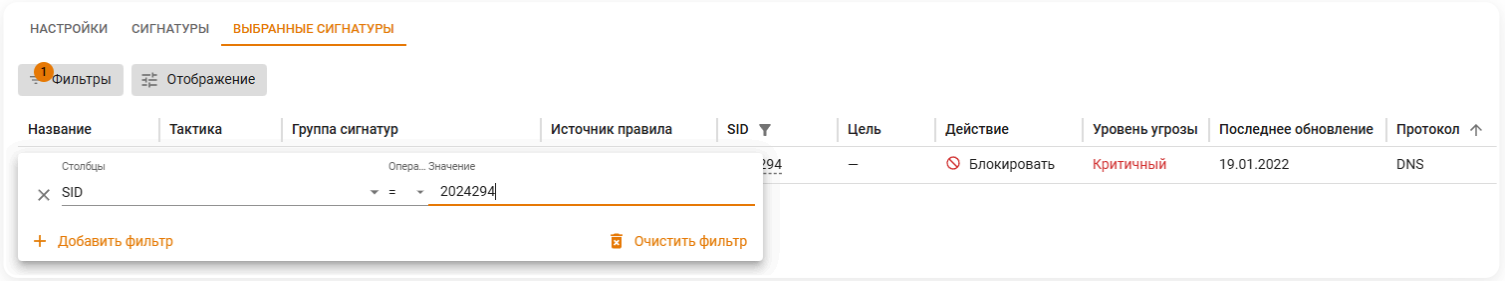
Указаны примерные значения, так как сигнатуры обновляются.

Управление профилями

Чтобы просмотреть или изменить созданный профиль (описание и правила выбора сигнатур), нажмите на или . На вкладке **Выбранные сигнатуры** представлены все сигнатуры, для которых настроено одно или несколько действий:



Для удобного поиска воспользуйтесь **Фильтром**. Например, чтобы найти нужную сигнатуру по идентификатору:

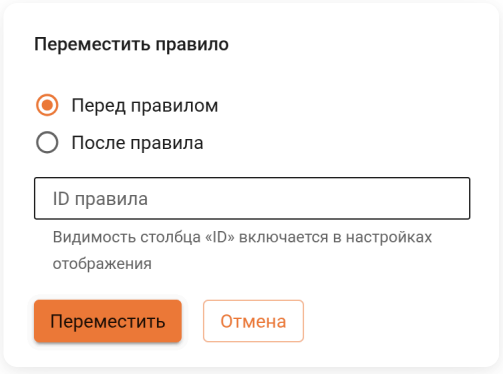


На вкладке **Сигнатуры** доступно перемещение правил. Выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



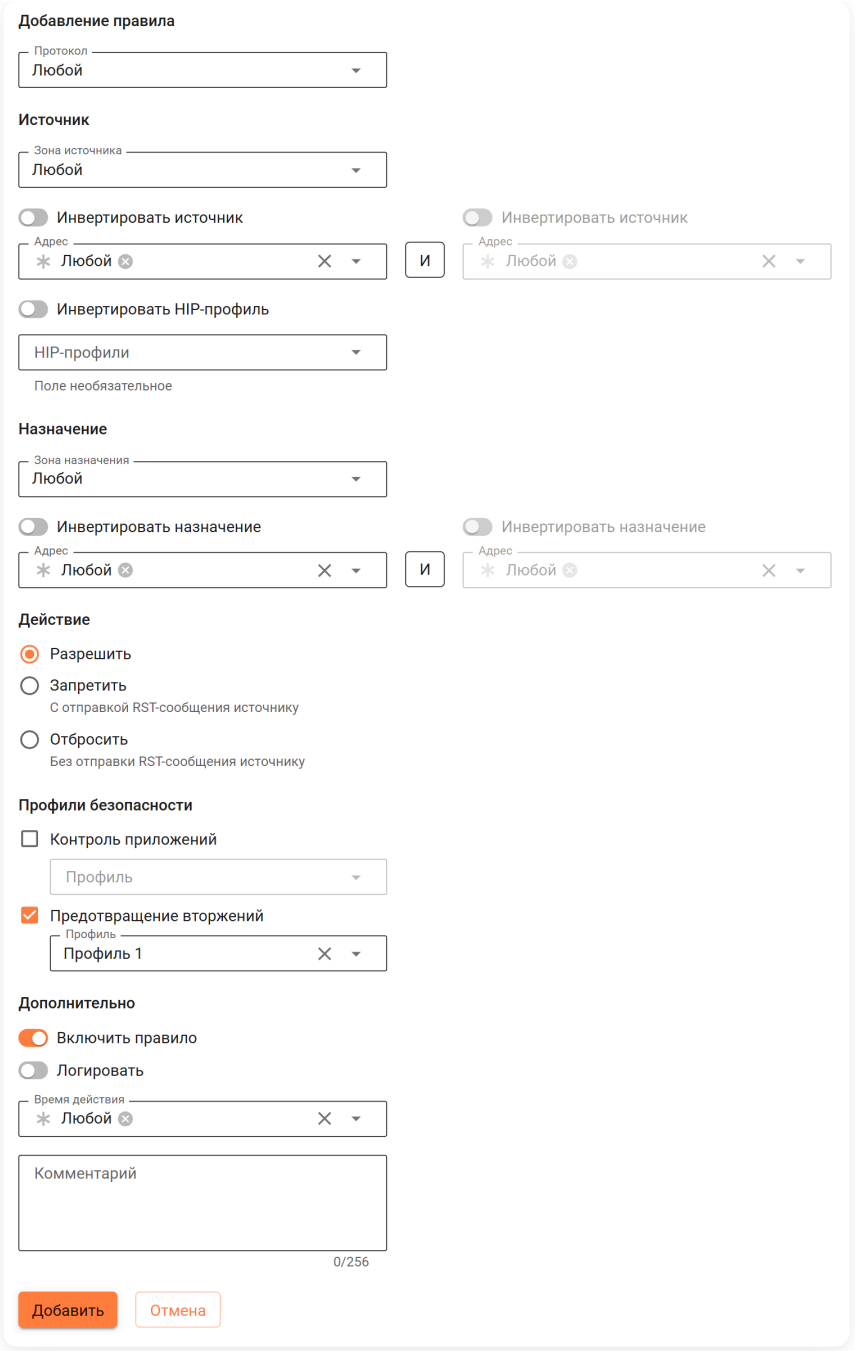
4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Добавление профилей в правила Межсетевого экрана

1. Перейдите в раздел **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать системой **Предотвращения вторжений**.
- **Источник** - выберите **Адрес**, **[Зону](*Зона)**, созданную в **Системном контексте**, и **HIP-профиль** источника трафика.
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика, созданную в **Системном контексте**.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Предотвращение вторжений** в блоке **Профили безопасности** и выберите необходимый профиль из раскрывающегося списка.

4. Включите правило и нажмите **Добавить**.

5. При включенной опции **Перехват пользовательских DNS-запросов** (по умолчанию опция включена) создайте правила **INPUT** с тем же профилем безопасности и портом 53 в разделе **Назначение** для протоколов TCP и UDP.

Полезные ссылки

- **Блокировка популярных ресурсов**

Профили Web Application Firewall

Классический VCE | Высокопроизводительный VCE | API

Название служб раздела **Профили Web Application Firewall**: `ideco-waf-backend`; `ideco-waf-event-syncer`.

Список служб для других разделов доступен по ссылке.

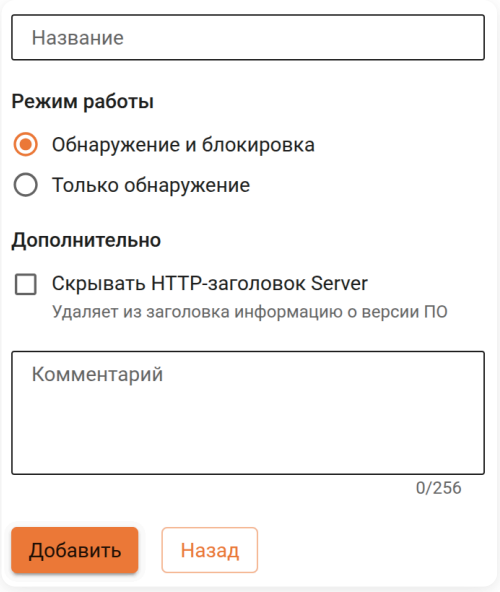
Использование WAF-профилей позволит настроить параметры защиты для опубликованного веб-ресурса. Профиль создается в **Профили безопасности → Web Application Firewall**.

Создание WAF-профилей не влияет на фильтрацию трафика. Чтобы включить фильтрацию, нужно использовать WAF-профили в разделе **Обратный прокси** при создании правила.

Создание профиля WAF

Для создания профиля WAF выполните действия:

1. Нажмите **Добавить** и заполните поля:

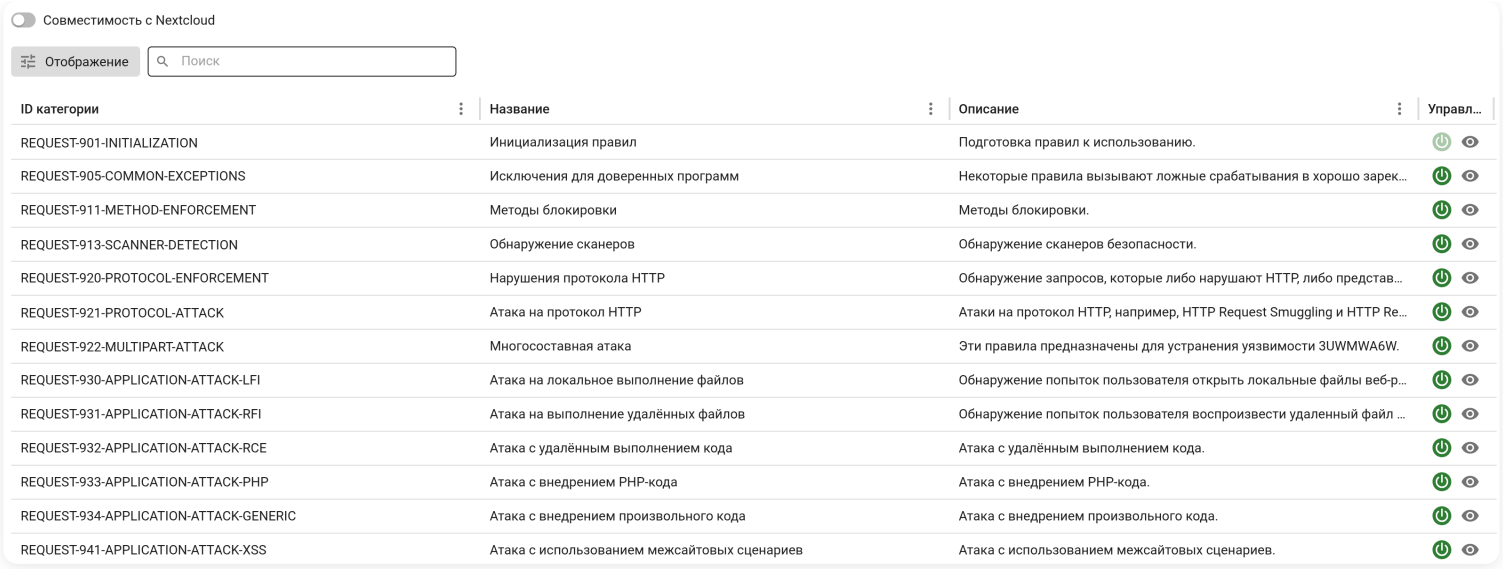


Расшифровка полей

- **Название** - введите название профиля.
- **Режим работы**:
  - **Обнаружение и блокировка** - подозрительные запросы будут блокироваться и логироваться WAF.
  - **Только обнаружение** - подозрительные запросы будут логироваться WAF, но не будут блокироваться.
- **Дополнительно**:
  - **Скрывать HTTP-заголовок Server** - позволяет скрыть данные, идентифицирующие сервер.
  - **Комментарий** - введите пояснение для профиля.

2. Нажмите **Добавить**.

3. На вкладке **Категории** включите или отключите правила:



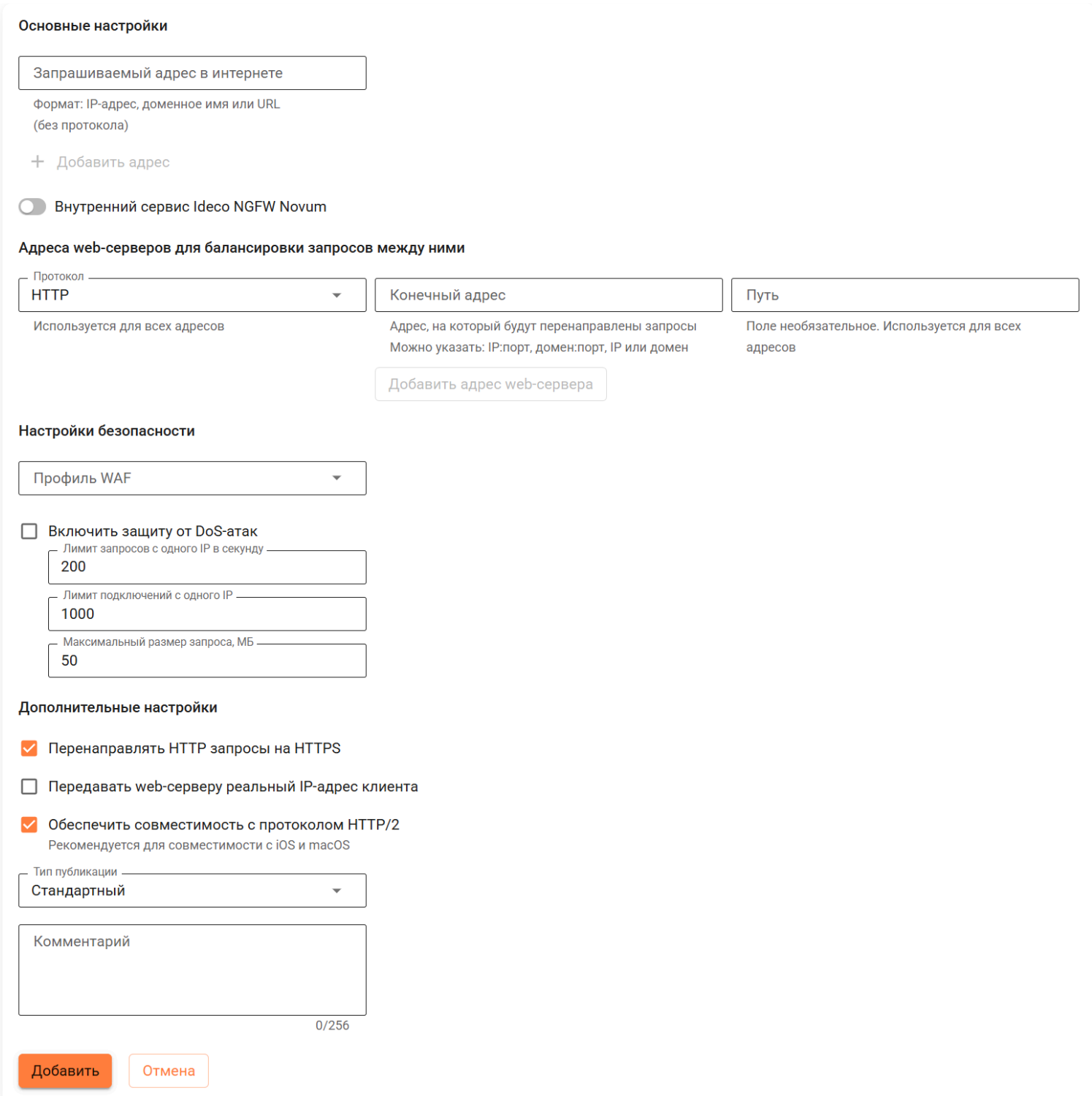
Если сервис Nextcloud работает за WAF, включите опцию **Совместимость с Nextcloud**:



Сигнатуры будут оптимизированы для определения атак на этот сервис. С выключенной опцией **Совместимость с Nextcloud** сервис может работать с ошибками.

Использование профиля WAF в правиле Обратного прокси

1. Перейдите в **Сервисы** → **Обратный прокси**, нажмите **Добавить** и заполните поля:



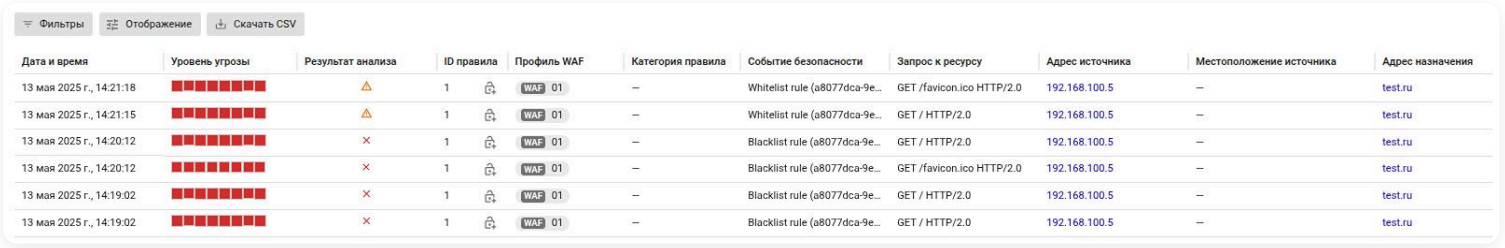
Расшифровка полей

- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных адресов нажмите кнопку **Добавить адрес**.
- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Конечный адрес** - адрес, на который будут перенаправлены запросы.
- **Путь** - поле необязательное и используется для всех адресов.
- **Профиль WAF** - выберите созданный ранее профиль WAF.
- **Перенаправлять HTTP-запросы на HTTPS** - включите настройку, если сайт работает по протоколу HTTPS. Позволяет автоматически переадресовывать пользователей с HTTP-версии.
- **Передавать web-серверу реальный IP-адрес клиента** - при необходимости включите настройку, чтобы публичный IP-адрес клиента при обратном проксировании не заменялся адресом NGFW Novum.

2. Нажмите **Добавить**.

Диагностика и добавление исключений

Срабатывание правил **Web Application Firewall** отображается в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**:



Добавить правило в исключение можно двумя способами:

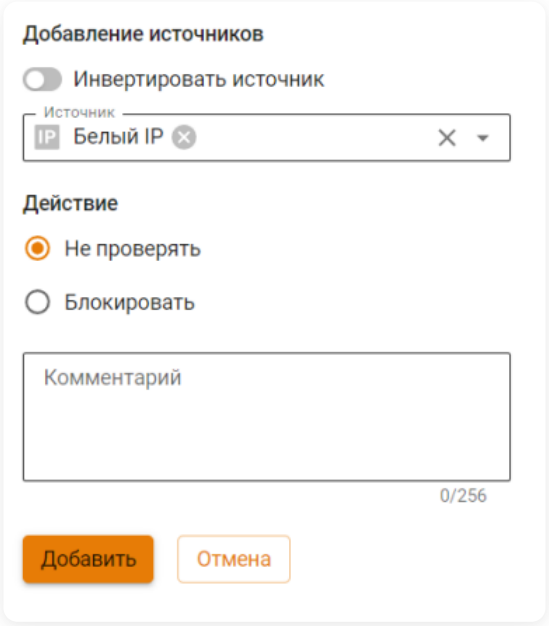
По IP-адресу

1. Перейдите в раздел **Профили Web Application Firewall** и у правила нажмите на .

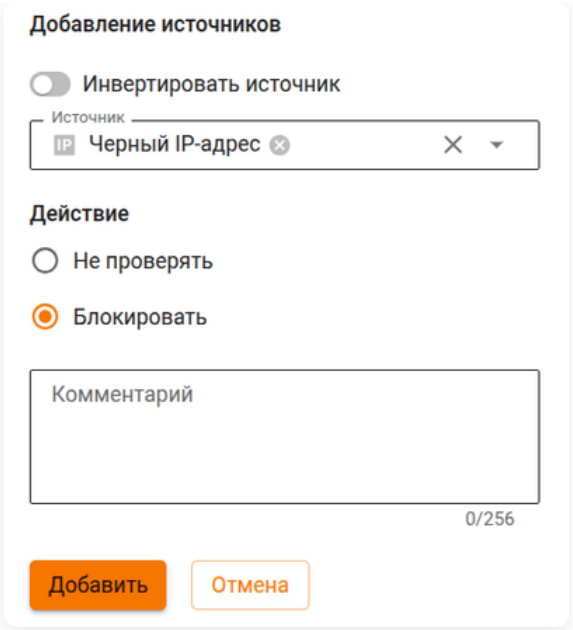
2. В **Белый и черный списки** нажмите **Добавить источник**:

> В каждый профиль WAF можно добавить не более двух тысяч источников в белых и черных списках.
> Если лимит будет превышен, появится сообщение в уведомлениях.

- Для добавления в белый список укажите необходимые IP-адреса и подсети, выберите действие **Не проверять**:



- Для добавления в черный список укажите необходимые IP-адреса и подсети, выберите действие **Блокировать**:



Исключения, добавленные в **Белый и черный списки**, логируются в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

По ID правила

Исключение добавляется двумя способами:

- На вкладке **Исключения**.
- На вкладке **Web Application Firewall**.

Не рекомендуем добавлять исключение по ID правила, так как из обработки исключатся все запросы, попадающие под исключенное правило.

На вкладке Исключения

1. Перейдите в раздел **Профили Web Application Firewall** и у правила нажмите на .

2. На вкладке **Исключения** нажмите **Добавить исключение** и укажите ID правила.

ID правила находится в журнале срабатывания правил в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

На вкладке Web Application Firewall

1. Перейдите в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

2. Нажмите на в столбце ID правила.

Если описанные способы не помогли, обратитесь в Техническую поддержку.

Сохранение правил WAF при обновлении системы

Правила WAF, добавленные в основные файлы конфигурации, перезаписываются при обновлении Ideco NGFW Novum.

Чтобы пользовательские правила WAF сохранялись при обновлении, в Ideco NGFW Novum предусмотрены специальные файлы для пользовательских правил и исключений. Они позволяют встроиться в процесс обработки запроса до или после основных правил WAF:

- **Before-секция** - отключение определенных правил для конкретных IP-адресов или URL до того, как они сработают и заблокируют легитимный запрос (борьба с ложными срабатываниями).
- **After-секция** - добавление пользовательских проверок или изменение поведения системы после того, как стандартные правила отработали.

Пример внесения правил в after-секцию

Требуется, чтобы все срабатывания порогового правила `949110` приводили к ошибке `404`, а не к стандартному ответу CRS.

1. Создайте и откройте для редактирования файл `custom-waf.conf` в `/var/opt/ideco/reverse-backend/`:

```
nano /var/opt/ideco/reverse-backend/custom-waf.conf
```

2. Добавьте в файл необходимое правило. Например:

```
SecRuleUpdateActionById 949110 "t:none,deny,status:404"
```

- `t:none` - не применять трансформаций к данным;
- `deny` - при срабатывании правила заблокировать запрос;
- `status:404` - при блокировке передать клиенту HTTP-статус `404`.

3. Перезапустите службы `ideco-waf-backend`, `ideco-waf-event-syncer` и `ideco-reverse-backend`.

4. Убедитесь, что при срабатывании правила `949110` клиент получает статус ответа `404`.

Пример внесения правил в before-секцию

Требуется для трафика, у которого `Content-Type` начинается с `text/plain` при обращении к `url.path`, начинающемуся с `/api/v1/webhook`, исключить срабатывание правила `920420` и явно указать процессор обработки тела запроса.

1. Создайте и откройте для редактирования файл `custom-waf-before.conf` в `/var/opt/ideco/reverse-backend/`:

```
nano /var/opt/ideco/reverse-backend/custom-waf-before.conf
```

2. Добавьте в файл необходимое правило. Например:

```
SecRule REQUEST_HEADERS:Content-Type "@beginsWith text/plain" \
    "id:10001,\
    phase:1,\
    pass,\
    t:none,\
    nolog,\
    tag:'Custom_Exception',\
    ver:'Custom_Exceptions/1.0',\
    chain"
    SecRule REQUEST_URI "@rx ^/api/v1/webhook" \
        "t:none,\
        ctl:ruleRemoveById=920420,\
        ctl:requestBodyProcessor=JSON"
```

- `SecRule REQUEST_HEADERS:Content-Type "@beginsWith text/plain"` - условие срабатывания. Срабатывает, если `Content-Type` начинается с `text/plain` (например `text/plain; charset=utf-8`);
- `id:10001` - ID пользовательского правила;
- `phase:1` - проверка на фазе 1 (анализ заголовков запроса);
- `pass` - правило не блокирует, только выполняет свои действия (в том числе `ctl` из следующего звена `chain`);
- `t:none` - не применять трансформаций к данным;
- `nolog` - срабатывание этого правила не логируется;
- `tag:'Custom_Exception'`, `ver:'Custom_Exceptions/1.0'` - метки/версия для удобства в логах и управлении;
- `chain` - указывает, что это первое звено цепочки. Действия применяются, только если пройдет и следующее условие;
- `REQUEST_URI` - действие применяется к `url.path`, начинающемуся с `/api/v1/webhook`;
- `t:none` - не применять трансформаций к данным;
- `ctl:ruleRemoveById=920420` - для этого запроса отключается правило с ID `920420`;
- `ctl:requestBodyProcessor=JSON` - принудительно обрабатывает тело запроса как JSON.

3. Перезапустите службы: `ideco-waf-backend`, `ideco-waf-event-syncer` и `ideco-reverse-backend`.

4. Убедитесь в том, что запрос к `/api/v1/webhook` не блокируется правилами из основной базы.

Профили антивируса

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Профили антивируса**: `ideco-av-backend`.

Список имен служб для других разделов доступен по ссылке.

Антивирус в продукте использует технологию Kaspersky Anti-Virus Software Development Kit. Для включения модуля перейдите в **Профили безопасности → Антивирус**.

Опция **Профили антивируса** управляет только проверкой трафика в текущем контексте. Статус **Работает** отображает активность модуля **kav-scanner**, даже если **Антивирус** выключен во всех контекстах. В этом случае NGFW Novum не выполняет проверку трафика. Модуль **kav-scanner** работает всегда при наличии лицензии и ресурсов.

Антивирус приобретается отдельно от Ideco NGFW Novum, использование может быть ограничено условиями лицензии. Для покупки обратитесь в отдел продаж.

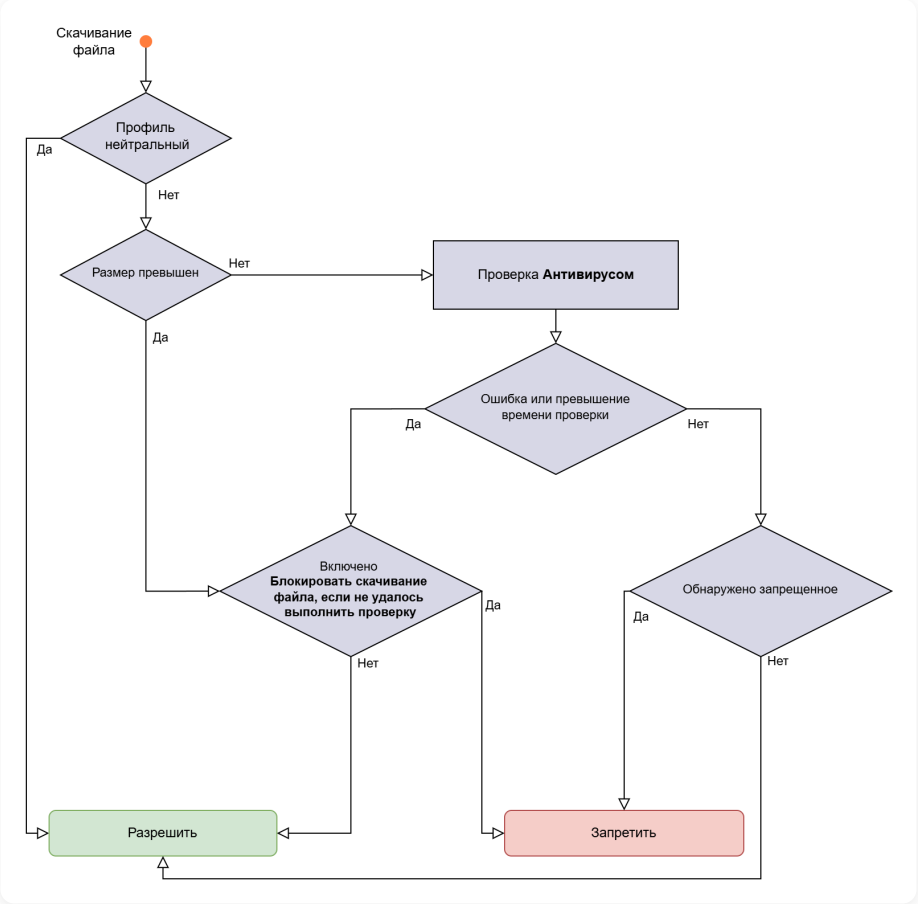
Корпоративные ключи, предназначенные для других продуктов Лаборатории Касперского, нельзя использовать для активации антивируса.

Антивирус связан с прокси-сервером и **Контент-фильтром** и фильтрует веб-трафик при выполнении следующих условий:

- В разделе **Контент-фильтр** настроена расшифровка веб-трафика. HTTPS-сайт проверяется только в случае расшифровки HTTPS-трафика **Контент-фильтром**. Рекомендации по настройке фильтрации HTTPS представлены в статье.
- Веб-ресурс не находится в списках исключений прокси-сервера по назначению.
- Пользователь, к которому поступает трафик, не добавлен в исключения прокси-сервера по источнику.

Для проверки трафика **Антивирусом** создайте правило в разделе **Контент-фильтр** и укажите нужный профиль антивируса. Если профиль не выбран, проверка будет выполняться с использованием профиля по умолчанию в блоке **Настройки**. Если профиль по умолчанию не выбран, проверка трафика не выполняется.

Схема работы профиля антивируса при проверке скачиваемого файла:

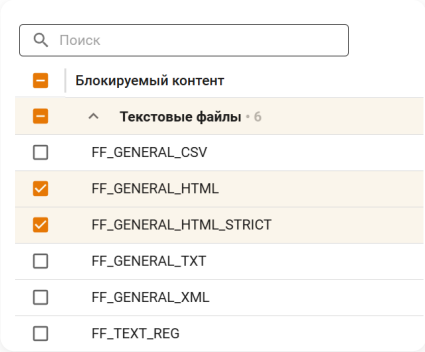


- **Профиль нейтральный** - профиль, в котором не включена блокировка ссылок, ПО и контента.

Результат проверки трафика **Антивирусом** представлен в разделе **Веб-трафик**.

Особенности работы Антивируса

- Ищет файлы заблокированных форматов в архивах. Если находит, то блокирует архив.
- Не блокирует некоторые типы файлов (например, CSV) без фиксированных байтов, используемых для определения типа файла (магических байтов). Все файлы, которые нельзя классифицировать по магическим байтам, Антивирус Касперского относит к TXT. Если необходимо блокировать подобные типы файлов, рекомендуем блокировку по расширению или по MIME-типу через Контент-фильтр.
- Блокирует веб-страницы, если в профиле Антивируса включена блокировка HTML-документов в **Текстовых файлах** и профиль выбран в правиле Контент-фильтра:



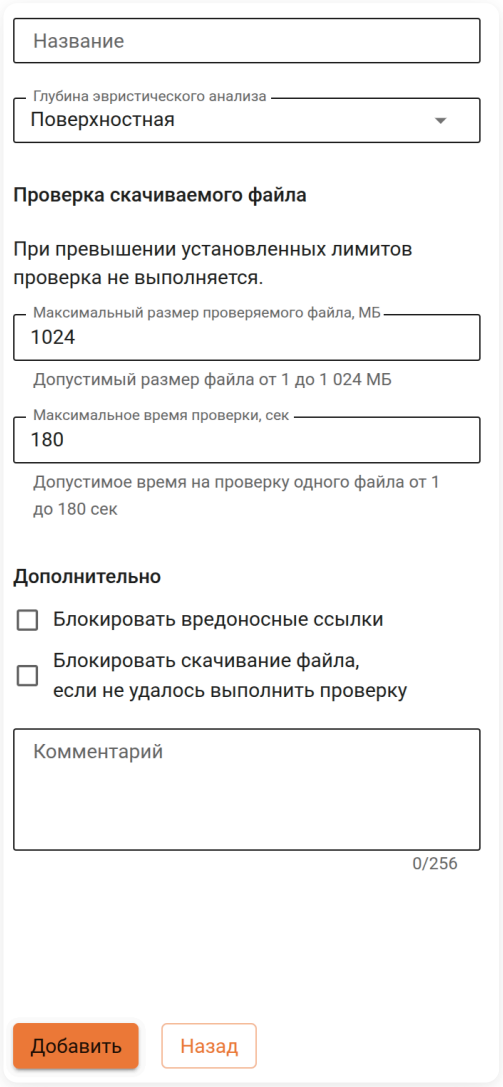
Если файл был загружен при выключенном **Антивирусе**, браузер (например, Google Chrome) может взять файл из кэша при повторной загрузке, минуя фильтрацию NGFW Novum.

Для восстановления антивирусной проверки необходимо очистить кэш браузера.

Профили

Для создания профиля выполните действия:

1. Нажмите **Добавить** и заполните поля на вкладке **Настройки**:



Расшифровка полей

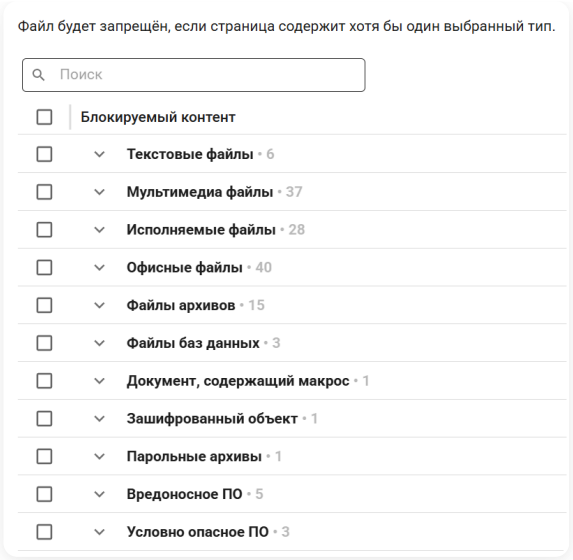
- **Название** - название профиля.
- **Глубина эвристического анализа** - степень обнаружения новых и неизвестных вредоносных программ:
  - **Не проводить проверку**.
  - **Поверхностная**.
  - **Средняя**.
  - **Глубокая**.
  - **Максимальная**.

Повышение уровня сканирования увеличивает глубину проверки, но потребует больше времени и системных ресурсов.

- **Проверка скачиваемого файла** - настройка проверки файлов. При превышении указанных лимитов проверка файлов не выполняется:
  - **Максимальный размер проверяемого файла, МБ** - максимальный объем проверяемого файла (от 1 до 1024 МБ).
  - **Максимальное время проверки, сек** - время на проверку одного файла (от 1 до 180 секунд).
- **Дополнительно:**
  - **Блокировать вредоносные ссылки** - проверка URL по базе вредоносных ссылок Web Malicious URL Filtering (WMUF).
  - **Блокировать скачивание файла, если не удалось выполнить проверку** - блокирование скачивания файла при превышении размера, времени проверки или обнаружении вредоносного контента. Если опция не включена, то файл будет пропущен без проверки.
  - **Комментарий** - произвольный текст. Не более 256 символов.

2. Нажмите **Добавить**.

3. Перейдите на вкладку **Блокировка по контенту** и укажите контент, который должен быть заблокирован:



Тип блокируемого контента

- **Документ, содержащий макрос** - объект, содержащий макросы Microsoft Office.
- **Зашифрованный объект** - объект, защищенный алгоритмом шифрования.
- **Парольные архивы** - запароленный архив.
- **Вредоносное ПО** - вредоносные инструменты, трояны, неопознанное вредоносное ПО высокой или средней опасности и другие категории, указанные в дереве классификации.
- **Условно опасное ПО** - рекламное ПО (Adware), порнографическое (Pornware) или потенциально опасное (Riskware), указанное в дереве классификации.

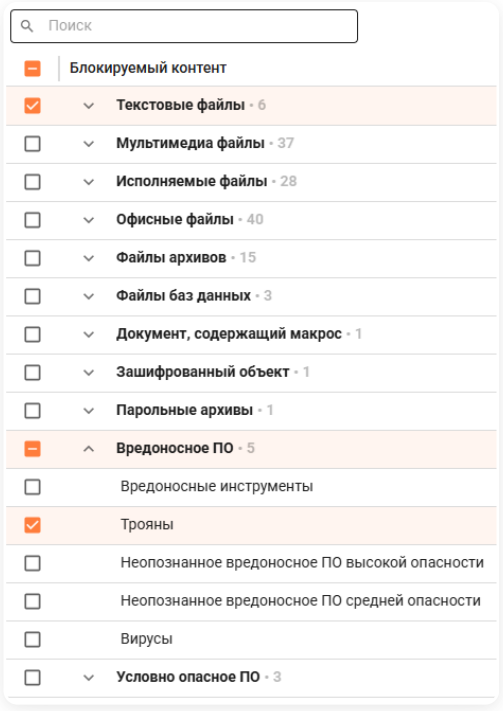
Тип блокируемого контента в файловом формате (**Файлы архивов**, **Исполняемые файлы**, **Мультимедиа файлы**, **Офисные файлы**, **Текстовые файлы**, **Файлы баз данных**, **Файлы веб-архивов**) и **Прочие форматы** указаны в статье.
При настройке блокировки применяется логика **ИЛИ**:

- Если выбрано одно значение, блокируется только трафик с указанным типом.
- Если выбрано несколько значений, блокируется трафик, содержащий любой из выбранных типов или сочетание типов.

Примеры блокировки контента

Пример 1. В профиле выбрана категория **Текстовые файлы**. Результат: будет заблокирован тип контента **Текстовые файлы**.

Пример 2. В профиле выбраны категории **Текстовые файлы** и **Трояны**:

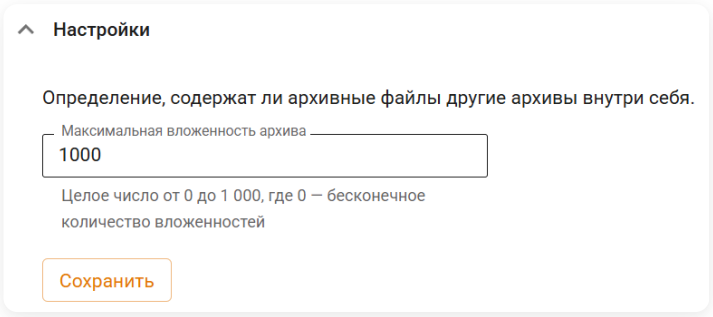


Будут блокироваться три типа контента:

- **Текстовые файлы**.
- **Трояны**.
- **Текстовые файлы**, содержащие **Трояны**.

4. Для подтверждения создания профиля нажмите **Сохранить**.

На вкладке **Основное** можно настроить **Максимальную вложенность архива**:



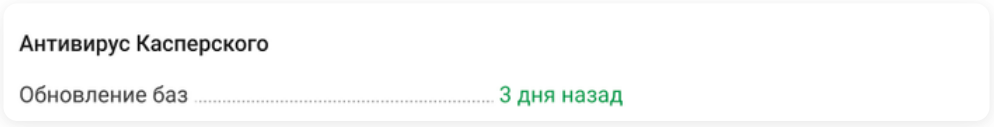
В поле укажите целое число от `0` до `1000`, где `0` - бесконечное количество вложенностей (`0` указано по умолчанию). Для запрета вложенных архивов укажите в поле значение `1`.

> Если включена опция **Блокировать скачивание файла**, попытка скачать архив с превышением указанной вложенности будет заблокирована.

Функция проверки вложенности не работает с запароленными архивами, которые можно заблокировать при создании профиля на вкладке **Блокировка по контенту**.

Обновление баз

На вкладке можно посмотреть информацию о последнем обновлении баз антивируса Касперского:



Проверка работы антивируса

Попробуйте скачать тестовые файлы с сайта: https://www.eicar.org/download-anti-malware-testfile.

В случае правильной настройки браузер выведет ошибку доступа:

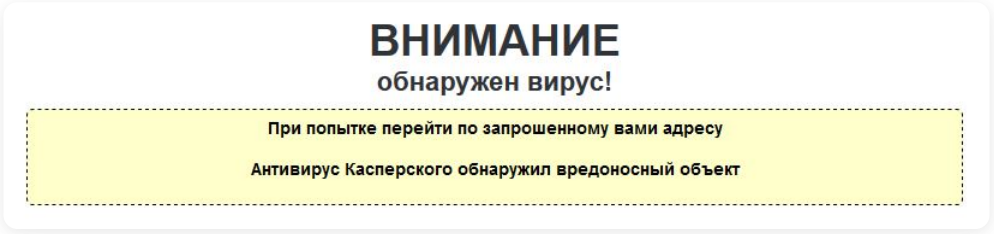


Таблица с описанием типов блокируемого контента модуля Антивирус

Таблица с описанием типов блокируемого контента, обрабатываемых модулем Антивирус:

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Текстовые файлы		FF_GENERAL_CSV	Comma-separated Values	csv	text/csv
Текстовые файлы		FF_GENERAL_HTML	HyperText Markup Language or fragments of HTML	htm; html	text/html
Текстовые файлы		FF_GENERAL_HTML_STRICT	HyperText Markup Language standalone document (generally with doctype or html tags)	htm; html	text/html
Текстовые файлы		FF_GENERAL_TXT	Plain Text	txt	text/plain
Текстовые файлы		FF_GENERAL_XML	Extensible Markup Language (XML)	xml	text/xml; a
Текстовые файлы		FF_TEXT_REG	Windows registry editor script	reg	
Мультимедиа файлы	Audio	FF_AUDIO_AAC	Advanced Audio Coding	aac; m4a	audio/aac
Мультимедиа файлы	Audio	FF_AUDIO_AC3	AC3 multichannel audio	ac3	audio/ac3
Мультимедиа файлы	Audio	FF_AUDIO_APE	Monkey' s Audio (APE)	ape	audio/x-m ape
Мультимедиа файлы	Audio	FF_AUDIO_CDA	CD digital Audio	cda	applicatio
Мультимедиа файлы	Audio	FF_AUDIO_FLAC	Free Lossless Audio Codec (FLAC)	flac	audio/x-fla
Мультимедиа файлы	Audio	FF_AUDIO_MIDI	MIDI	mid; midi	audio/mid
Мультимедиа файлы	Audio	FF_AUDIO_MKA	Matroska Audio	mka	audio/x-m
Мультимедиа файлы	Audio	FF_AUDIO_MP3	MPEG-1 Layer 3	mp3	audio/x-m audio/mpe audio/x-m
Мультимедиа файлы	Audio	FF_AUDIO_OGG	OGG Vorbis Audio	ogg	audio/x-og
Мультимедиа файлы	Audio	FF_AUDIO_RA	RealAudio	rm; ra; ravb	audio/vnd
Мультимедиа файлы	Audio	FF_AUDIO_WAV	Microsoft Wave	wav	audio/x-wa

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Мультимедиа файлы	Audio	FF_AUDIO_WEB_M	WebM Audio	webm; weba	audio/web
Мультимедиа файлы	Audio	FF_AUDIO_WMA	Windows Media Audio	wma	
Мультимедиа файлы	Image	FF_IMAGE_BMP	Windows Bitmap (DIB)	bmp	image/bm
Мультимедиа файлы	Image	FF_IMAGE_CDR	Corel Draw	cdr	
Мультимедиа файлы	Image	FF_IMAGE_EMF	Windows Meta-File	emf; wmf	
Мультимедиа файлы	Image	FF_IMAGE_EPS	Post-Script Format	eps	applicatio
Мультимедиа файлы	Image	FF_IMAGE_GIF	GIF	gif	image/gif
Мультимедиа файлы	Image	FF_IMAGE_JPEG	JPEG/JFIF	jpg; jpe; jpeg; jff	image/jpe
Мультимедиа файлы	Image	FF_IMAGE_PNG	Portable Graphics	png	image/png
Мультимедиа файлы	Image	FF_IMAGE_PSD	Adobe Photoshop	psd	
Мультимедиа файлы	Image	FF_IMAGE_TIFF	Targa Image File Format	tif; tiff	image/tif;
Мультимедиа файлы	Image	FF_IMAGE_WEBP	WebP	webp	image/we
Мультимедиа файлы		FF_MULTIMEDIA_SWF	ShockWave Flash	swf	applicatio
Мультимедиа файлы	Video	FF_VIDEO_3GPP	MPEG4 ISO format	3gp; 3g2; 3gp2; 3p2	
Мультимедиа файлы	Video	FF_VIDEO_ASF	Microsoft Container	asf; wmv	video/x-m
Мультимедиа файлы	Video	FF_VIDEO_AVI	Audio/Video Interleave	avi	video/avi;
Мультимедиа файлы	Video	FF_VIDEO_BIK	Bink Video	bik	
Мультимедиа файлы	Video	FF_VIDEO_DIVX	MPEG4	divx; mp4; m4v	video/mp4
Мультимедиа файлы	Video	FF_VIDEO_F4V	f4v	f4v	video/x-flv
Мультимедиа файлы	Video	FF_VIDEO_FLV	Adobe Flash Video	flv	video/x-flv
Мультимедиа файлы	Video	FF_VIDEO_MKV	Matroska Video	mkv	video/x-m
Мультимедиа файлы	Video	FF_VIDEO_MOV	Apple Quicktime	mov; qt	video/quic
Мультимедиа файлы	Video	FF_VIDEO_RM	RealMedia CB/VB	rm; rmvb	video/vnd
Мультимедиа файлы	Video	FF_VIDEO_RTMP	Real Time Messaging Protocol Message		applicatio
Мультимедиа файлы	Video	FF_VIDEO_VOB	MPEG1 (VCD) / MPEG2 (DVD) format	vob; dat; mpg; mpeg	video/mpe
Мультимедиа файлы	Video	FF_VIDEO_WEB_M	WebM Video	webm	video/web
Исполняемые файлы	Executable	FF_EXECUTABLE_APK	Android Application Package	apk	applicatio

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Исполняемые файлы	Executable	FF_EXECUTABLE_APPLE_SCRIPT	AppleScript Files	scpt; AppleScript	
Исполняемые файлы	Executable	FF_EXECUTABLE_BAT	Command Line Script	cmd; bat	applicatio
Исполняемые файлы	Executable	FF_EXECUTABLE_COM	COM - MS-DOS Application	com	
Исполняемые файлы	Executable	FF_EXECUTABLE_DEB	Debian Software Package	deb	applicatio
Исполняемые файлы	Executable	FF_EXECUTABLE_DEX	Dalvik Executable Format	dex; odex	
Исполняемые файлы	Executable	FF_EXECUTABLE_DOS	"DOS	Win-16	OS/2 - all
Исполняемые файлы	Executable	FF_EXECUTABLE_DOS_NE_RESOURCE	"DOS	Win-16	OS/2 - NE
Исполняемые файлы	Executable	FF_EXECUTABLE_ELF	Executable and Linkable Format	o; so; elf; prx	
Исполняемые файлы	Executable	FF_EXECUTABLE_JAVA	Java Class File	class	
Исполняемые файлы	Executable	FF_EXECUTABLE_JS	JavaScript	js	text/javas
Исполняемые файлы	Executable	FF_EXECUTABLE_MACHO	Mach object file format	; o; dylib	
Исполняемые файлы	Executable	FF_EXECUTABLE_MSI	Microsoft Installer Archive	msi	
Исполняемые файлы	Executable	FF_EXECUTABLE_PYC	Python Bytecode	pyc; pyo	
Исполняемые файлы	Executable	FF_EXECUTABLE_RPM	RPM Package	rpm	applicatio
Исполняемые файлы	Executable	FF_EXECUTABLE_SCRIPTS	Unix Scripts	sh; pl	
Исполняемые файлы	Executable	EFF_XECUTABLE_VBS	Visual Basic Script	vbs; vb	text/vbscri
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE	Win32 PE	exe; dll; ocx; scr	applicatio msdownlo vms/exe;
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_DLL	Win32 PE Dynamic Library	dll; ocx; scr	applicatio msdownlo
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_EXE	Win32 PE Executable File	exe	applicatio applicatio
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_EXEUI	Win32 PE Executable File for Windows GUI/CUI and POSIX Subsystems	exe	applicatio applicatio
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_ILLIBRARY	Win32 PE .Net IL Library	exe; dll; ocx; scr	applicatio msdownlo
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_ILONLY	Win32 PE .Net IL (Only)	exe; dll; ocx; scr	applicatio msdownlo
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_NET	Win32 PE .Net	exe; dll; scr	applicatio msdownlo

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_NET_RESOURCE_WITH_POSSIBLE_TRIVIAL_CODE	Win32 PE .Net Resource Only Library (May contain trival code)	dll	application msdownlo
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_RESOURCE	Win32 PE Resource Only Library	dll	application msdownlo
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_SYS	Win32 PE File for Native Subsystem	sys	application
Исполняемые файлы	Windows	FF_EXECUTABLE_WINDOWS_SHELLLINK	MS Windows shell links	lnk	
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOC	Microsoft Word Document 97-2003	doc	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOCM	Microsoft Word Macro-Enabled Document	docm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOCX	Microsoft Word Document	docx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOT	Microsoft Word Template 97-2003	dot	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOTM	Microsoft Word Macro-Enabled Template	dotm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOTX	Microsoft Word Template	dotx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_POTM	Microsoft PowerPoint Macro-Enabled Template	potm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_POTX	Microsoft PowerPoint Template	potx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPSM	Microsoft PowerPoint Macro-Enabled Slide Show	ppsm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPSX	Microsoft PowerPoint Slide Show	ppsx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPT	Microsoft PowerPoint Presentation 97-2003	ppt; pot; pps	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPTM	Microsoft PowerPoint Macro-Enabled Presentation	pptm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPTX	Microsoft PowerPoint Presentation	pptx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PUB	Microsoft Publisher Document	pub	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_SCRAP	Microsoft Shell Scrap Object	shs; shb	

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLAM	Microsoft Excel Macro-Enabled Add-in	xlam	applicatio
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLS	Microsoft Excel Document 97-2003	xsl	applicatio
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLSB	Microsoft Excel Binary Document	xlsb	applicatio
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLSM	Microsoft Excel Macro-Enabled Document	xlsm	applicatio officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLSX	Microsoft Excel Document	xlsx	applicatio officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLTM	Microsoft Excel Macro-Enabled Template	xltm	applicatio officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLTX	Microsoft Excel Template	xltx	applicatio officedocu
Офисные файлы		FF_OFFICE_EML	Outlook Express Message	eml	message/
Офисные файлы		FF_OFFICE_MSG	Microsoft Outlook Message	msg	applicatio
Офисные файлы		FF_OFFICE_MSOFFICE	MS Office documents	doc; xls; ppt; dot; pot	applicatio applicatio applicatio
Офисные файлы		FF_OFFICE_MSOFFICE_MACRO	Office 2007 macro enabled docs	docm; xlsm; pptm; ppsm; dotm	applicatio
Офисные файлы		FF_OFFICE_ODP	OpenDocument Presentation	odp	applicatio
Офисные файлы		FF_OFFICE_ODS	OpenDocument Spreadsheet	ods	applicatio
Офисные файлы		FF_OFFICE_ODT	OpenDocument Text	odt	applicatio
Офисные файлы		FF_OFFICE_ONE	Microsoft OneNote Document	one	applicatio
Офисные файлы		FF_OFFICE_ONEPKG	Microsoft OneNote Package	onepkg	applicatio
Офисные файлы		FF_OFFICE_OPENXML	Open XML documents	docx; xlsx; pptx; dotx; potx	applicatio ***applicatio*** excel*; ap applicatio
Офисные файлы		FF_OFFICE_PDF	Adobe Acrobat	pdf	applicatio
Офисные файлы		FF_OFFICE_PST	MS Outlook Personal Folders	pst; ost	applicatio
Офисные файлы		FF_OFFICE_RTF	Rich Text Format	rtf	text/rtf; ap
Офисные файлы		FF_OFFICE_SXW	OpenOffice.org 1.0 Writer Document	sxw	applicatio
Офисные файлы		FF_OFFICE_VDX	Microsoft Visio Drawing XML	vdx; vsx; vtx	applicatio

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Офисные файлы		FF_OFFICE_VSD	Microsoft Visio Diagram	vsd; vss; vst	applicatio
Офисные файлы		FF_OFFICE_XPS	Open XML Paper Specification	xps; oxps	applicatio xpsdocum
Офисные файлы		FF_OFFICE_XSN	Microsoft InfoPath Template Form	xsn	applicatio
Файлы архивов		FF_ARCHIVE_ARJ	Arj archive	arj	applicatio
Файлы архивов		FF_ARCHIVE_7Z	7-zip archive	7z*; 7-z	
Файлы архивов		FF_ARCHIVE_ACE	ACE archive	ace	applicatio
Файлы архивов		FF_ARCHIVE_BZIP2	BZIP2 archive	bz; bz2; tbz; tbz2	applicatio
Файлы архивов		FF_ARCHIVE_CAB	Windows Cabinet	cab	
Файлы архивов		FF_ARCHIVE_DMG	Apple Disk Image	dmg; smi; img	applicatio
Файлы архивов		FF_ARCHIVE_GZIP	Gzip archive	gz; tgz	applicatio
Файлы архивов		FF_ARCHIVE_ISO	ISO-9660 CD Disk	iso	
Файлы архивов		FF_ARCHIVE_JAR	Java (ZIP) archive	jar	
Файлы архивов		FF_ARCHIVE_LZIP	Lzip archive	lz	applicatio
Файлы архивов		FF_ARCHIVE_RAR	RAR archive	rar	
Файлы архивов		FF_ARCHIVE_TAR	Tar archive	tar	applicatio
Файлы архивов		FF_ARCHIVE_XAR	Extensible archive format	xar	
Файлы архивов		FF_ARCHIVE_Z	Z (compress) archive	Z	applicatio
Файлы архивов		FF_ARCHIVE_ZIP	ZIP archive	zip	applicatio
Файлы баз данных		FF_DATABASE_ACCDB	Microsoft Access Database	accdb; accde; accdr	applicatio
Файлы баз данных		FF_DATABASE_ACCDC	Microsoft Access Signed Package	accdc	applicatio
Файлы баз данных		FF_DATABASE_MDB	Microsoft Access 2003 Database	mdb	applicatio
Документ, содержащий макрос		OFFICE_MSOFFICE_MACRO	Office 2007 macro enabled docs	docm; xlsm; pptm; ppsm; dotm	applicatio
Зашифрованный объект		ENCRYPTED	Файл с примененным шифрованием, содержимое недоступно без ключа/ пароля		applicatio
Парольные архивы		PASSWORD_PROTECTED_ARCHIVE	Архив, защищенный паролем	zip; rar; 7z; ace; arj; cab; dmg; gz; iso; jar; tar	applicatio applicatio compress
Вредоносное ПО		Вредоносные инструменты			
Вредоносное ПО		Трояны			

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Вредоносное ПО		Неопознанное вредоносное ПО высокой опасности			
Вредоносное ПО		Неопознанное вредоносное ПО средней опасности			
Вредоносное ПО		Вирусы			
Условно опасное ПО		Рекламное (Adware)			
Условно опасное ПО		Порнографическое (Pornware)			
Условно опасное ПО		Потенциально опасное (Riskware)			

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Сервисы

В разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

Сетевые интерфейсы

Настройка сетевых интерфейсов, поддерживаемых Ideco NGFW

Перейти >

IGMP Proxy

IGMP Proxy позволяет принимать мультикаст-трафик от провайдера

Перейти >

Прокси

Настройка прозрачного проксирования веб-трафика в локальной сети

Перейти >

Обратный прокси

Настройка публикация веб-ресурсов локальной сети таким образом, чтобы веб-ресурсы стали доступны потребителям из сети интернет

Перейти >

ЛК/Портал SSL VPN

Настройка личного кабинета пользователя в Ideco NGFW (публикация и управление доступом пользователей)

Перейти >

DNS

Сервер DNS преобразует человекочитаемые имена серверов в IP-адреса. В состав Ideco NGFW входит DNS-сервер, не требующий дополнительной настройки в большинстве случаев.

Перейти >

DHCP-сервер

Настройка DHCP-сервера для автоматического назначения IP-адресов сетевым устройствам в локальной сети

Перейти >

NTP-сервер

Настройка NTP-сервера для синхронизации времени

Перейти >

IPsec

Настройка подключений с помощью защищенного протокола IPsec

Перейти >

ГОСТ VPN

Настройка ГОСТ VPN для соединения двух устройств NGFW

Перейти >

Сертификаты

Создание, загрузка и управление SSL-сертификатами

Перейти >

USB-токены

Настройка USB-токенов для использования на Ideco NGFW

Перейти >

Netflow

В статье описана настройка экспорта статистики трафика на коллектор во внешней или локальной сети по протоколу Netflow.

Перейти >

Syslog

Настройка передачи системных сообщений (syslog) Ideco NGFW в сторонние коллекторы или в SIEM-системы

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

Сетевые интерфейсы

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Сетевые интерфейсы**: `ideco-l2-manager`, `ideco-local-menu`, `ideco-l2manager-rest`, `ideco-l2manager-l2migration`, `ideco-l2manager-dhclient`, `ideco-l2manager-backend`.

Список имен служб для других разделов доступен по ссылке.

Для создания сетевых интерфейсов воспользуйтесь статьями:

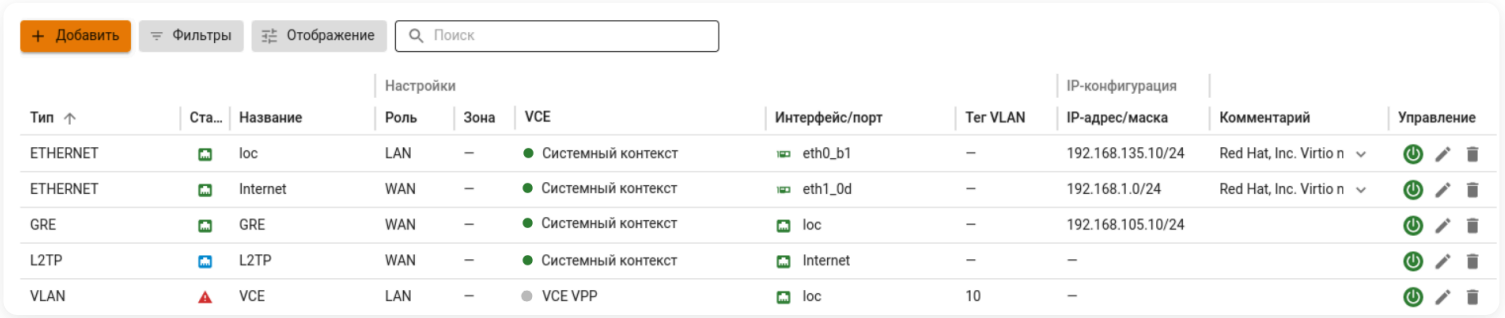
- **Интерфейсы**
- **Физические порты**

Интерфейсы можно создавать и редактировать только в **Системном контексте**. В других контекстах таблица интерфейсов доступна только для чтения.

Возможность передавать в VCE VPP отдельные порты сетевой карты зависит от модели сетевого адаптера:

- Если адаптер поддерживает разделение портов, порты можно передавать по отдельности.
- Если адаптер не поддерживает разделение портов, в VCE VPP необходимо передавать все порты сетевой карты. Иначе интерфейсы этой сетевой карты работать не будут.

Все созданные интерфейсы представлены в виде таблицы:



Статусы соединения

- Подключен

- Подключение

- Не подключен

- Статус неизвестен

Статусы VCE

- Работает

- Выключен

Редактирование сетевых интерфейсов

Интерфейсы можно редактировать, нажав , или удалить, нажав . Удалить интерфейс невозможно, пока на его основе созданы другие.

При создании, редактировании или удалении сетевого интерфейса перевыпускается **SSL-сертификат**, поэтому вероятно снижение скорости работы веб-интерфейса Ideco NGFW Novum. В этом случае рекомендуем нажать **F5**.

Ограничения сетевых интерфейсов

Максимальное количество сетевых интерфейсов, которое может обработать модуль **Ограничение скорости**:

- До 8 ГБ - **14 интерфейсов**.
- От 8 до 16 ГБ - **33 интерфейса**.
- 16 ГБ и более - **66 интерфейсов**.

Интерфейсы

Функциональность доступна в **Классическом** и **Системном контекстах**.

Интерфейсы соединяют устройство пользователя с различными сетевыми сегментами и определяют, как и для чего будут использоваться физические или виртуальные порты.

С версии 21 Ideco NGFW Novum у интерфейсов появились роли:

- **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.

Интерфейс **Control Plane** не обязателен - NGFW Novum можно администрировать и через LAN.

Однако для повышения безопасности рекомендуется ограничить доступ по **LAN** в правилах **Межсетевого экрана** (таблица INPUT, TCP 8443) и использовать для управления только интерфейс **Control Plane**.

- **LAN** – используется для создания локальных интерфейсов.

Для работы служб, зависящих от наличия локального интерфейса (например, **Прокси**), необходим хотя бы один сетевой интерфейс с ролью **LAN**.

- **WAN** – используется для подключения к провайдеру.

Памятка по частным IP-адресам IPv4

Согласно документу RFC 1918, для частных сетей зарезервированы следующие диапазоны адресов IPv4:

- **10.0.0.0/8** IP-адреса: `10.0.0.0 – 10.255.255.255`.
- **172.16.0.0/12** IP-адреса: `172.16.0.0 – 172.31.255.255`.
- **192.168.0.0/16** IP-адреса: `192.168.0.0 – 192.168.255.255`.

Сети, созданные в указанных диапазонах IP-адресов, для NGFW Novum считаются локальными и не подлежат публичной маршрутизации в интернете. Для настройки интерфейсов перейдите в **Сервисы** → **Сетевые интерфейсы**.

Основные интерфейсы

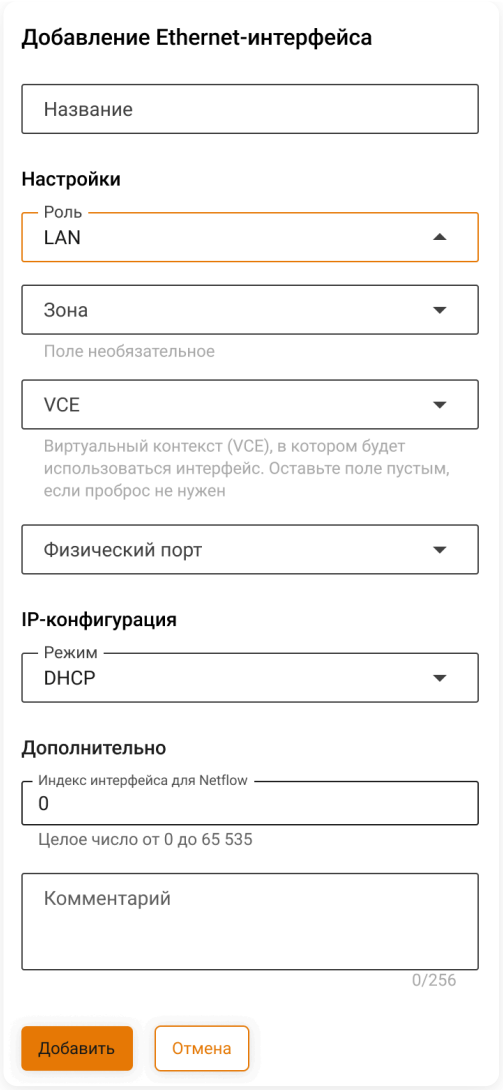
Ethernet

Ethernet - базовая технология проводных сетей, обеспечивающая передачу данных между устройствами. Технология поддерживает как прямое соединение устройств, так и работу через коммутаторы, обеспечивая гибкость и масштабируемость сетевой инфраструктуры.

Для настройки Ethernet-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Ethernet**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для подключения к провайдеру.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Физический порт** - порт на сетевом адаптере, который будет использоваться в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. Ethernet-интерфейс появится в таблице интерфейсов.

VLAN

VLAN (Virtual Local Area Network) - виртуальный сетевой интерфейс, позволяющий создавать и настраивать логические сегменты сети поверх существующей физической инфраструктуры. Данная технология дает возможность эффективно разделять сетевой трафик и организовывать изолированные сетевые сегменты в рамках единой сетевой структуры.

VLAN-интерфейс создается поверх родительского интерфейса и помечает все исходящие пакеты соответствующим тегом.

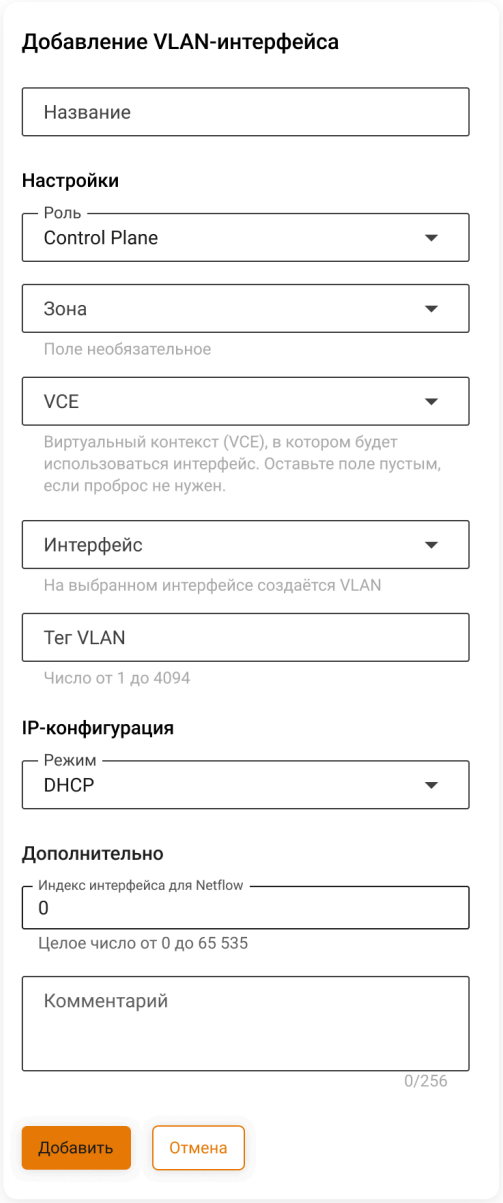
Различия в работе с VCE VPP и NGFW:

- В VCE NGFW можно передать VLAN-интерфейс, не передавая родительский интерфейс: VLAN-интерфейс конфигурируется, если родительский интерфейс отсутствует в контексте.
- В VCE VPP можно передать VLAN-интерфейс, только передав родительский интерфейс: VLAN-интерфейс не конфигурируется, если родительский интерфейс отсутствует в контексте.

Для настройки VLAN-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **VLAN**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для подключения к провайдеру.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.

- **Интерфейс** - родительский интерфейс, на базе которого создается VLAN-интерфейс: физический или агрегированный сетевой интерфейс, через который передается трафик данного VLAN. Доступные варианты: **Ethernet** и **LACP**.
- **Тег VLAN** - числовой идентификатор VLAN (от 1 до 4094), которым помечаются все пакеты VLAN-интерфейса.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. VLAN-интерфейс появится в таблице интерфейсов.

> **Как обрабатываются теги VLAN**
>
> Когда на сетевой интерфейс NGFW Novum приходит кадр с тегом соответствующего VLAN, тег снимается. NGFW Novum анализирует адрес назначения в IP-пакете и отправляет пакет в сетевой интерфейс согласно таблице маршрутизации. При отправке в кадр добавляется тег исходящего сетевого интерфейса (если он задан).
>
> Далее кадр передается на устройство на другом конце кабеля, например, на коммутатор. В зависимости от конфигурации VLAN на коммутаторе кадр либо передается без изменений, либо помещается в Native VLAN (его можно изменить).

LACP

LACP (Link Aggregation Control Protocol) - протокол агрегации каналов, предназначенный для объединения нескольких физических портов в единый логический интерфейс. Основное применение LACP заключается в увеличении общей пропускной способности канала и обеспечении его отказоустойчивости.

> Не рекомендуем использовать **LACP** на виртуальных сетевых адаптерах, так как системы виртуализации некорректно обрабатывают работу **LACP** на таких интерфейсах или вовсе не поддерживают этот режим.

Особенности работы LACP-интерфейсов:

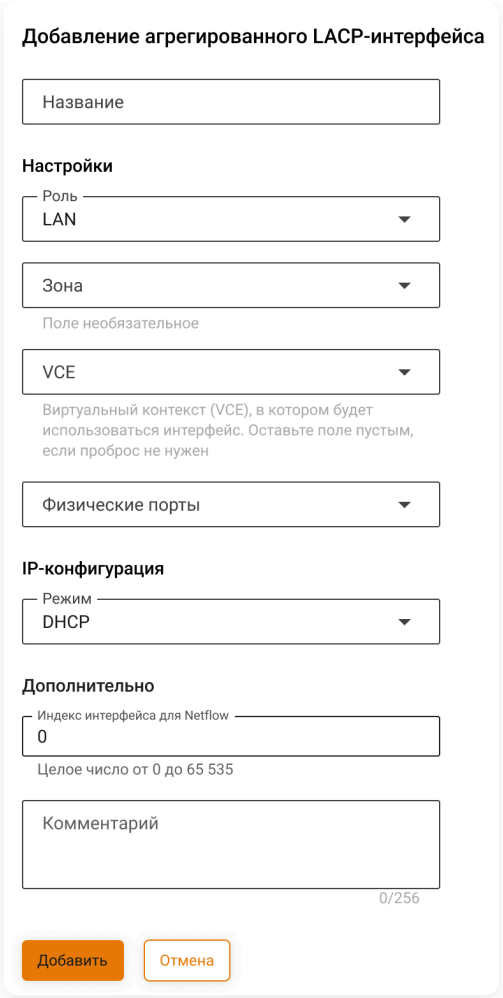
- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active**-режим - постоянная рассылка LACP пакетов.
- Используется режим вычисления хеша для распределения трафика **xmit_hash_policy layer2+3**.
- Проверка соседства осуществляется в режиме **fast** - каждую секунду.
- Количество физических портов, объединяемых в агрегированный интерфейс, не ограничено со стороны NGFW Novum, но также зависит от конфигурации аппаратных решений и организации сети.

> LACP-интерфейсы можно пробрасывать в виртуальные контексты (VCE VPP и VCE NGFW).
>
> Для создания LACP-интерфейса между нодами кластера достаточно указать один физический порт - система автоматически создаст канал между одноименными портами обеих нод. Например, если в кластере есть порт `client`, созданный LACP-интерфейс объединит `client` с первой ноды и `client` со второй ноды. Подробнее о настройке кластера - в статье.

Чтобы объединить несколько физических портов в один агрегированный LACP-интерфейс, выполните действия:

1. Нажмите **Добавить** и выберите **LACP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для подключения к провайдеру.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Физический порт** - порт на сетевом адаптере, который будет использоваться в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. LACP-интерфейс появится в таблице интерфейсов.

SPAN

SPAN (Switch Port Analyzer) - технология зеркалирования трафика, которая позволяет копировать пакеты данных с одного или нескольких портов коммутатора/маршрутизатора на специальный порт мониторинга. В Ideco NGFW Novum SPAN-интерфейс позволяет дублировать трафик локальных и внешних интерфейсов на отдельное внешнее устройство для анализа и выявления угроз.

SPAN-интерфейс должен использовать выделенный физический порт сетевой карты и не может делить его с другими интерфейсами.

Перед обновлением на 22 версию Ideco NGFW Novum убедитесь, что в качестве **Интерфейса назначения** выбран интерфейс, занимающий один физический порт сетевой карты. Если этот порт разделяется с другими интерфейсами, SPAN-интерфейс будет

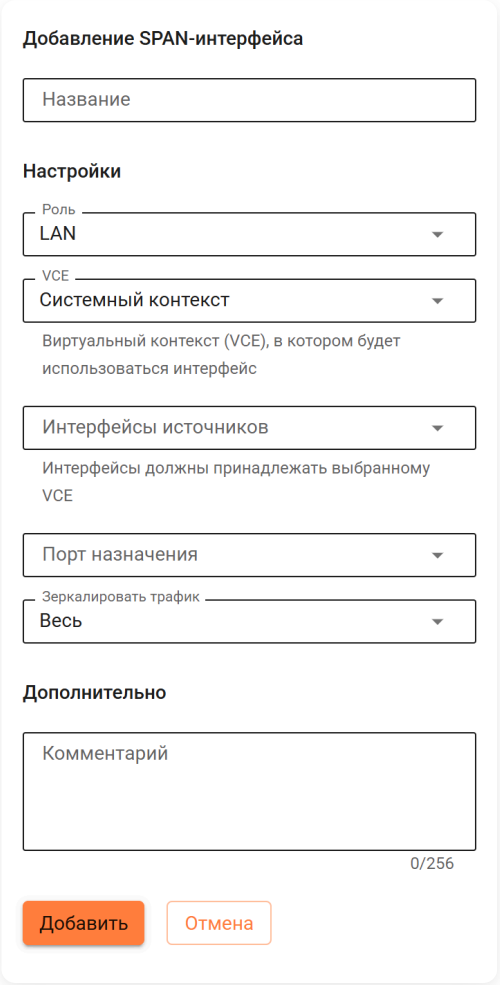
отключен после обновления.

SPAN-интерфейс может быть перегружен при большом количестве наблюдаемых интерфейсов.

Для настройки SPAN-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **SPAN**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для поддержки старых конфигураций Ideco NGFW, если в предыдущих версиях SPAN был настроен на подключении к провайдеру.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейсы источников** - выберите интерфейсы, трафик которых хотите дублировать. Доступные варианты: **Ethernet**, **VLAN** и **LACP**.
- **Порт назначения** - выберите порт, на который будет дублироваться трафик.
- **Зеркалировать трафик** - выберите тип трафика, который хотите дублировать. Доступные варианты: **Весь**, **Только входящий** или **Только исходящий**.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. SPAN-интерфейс появится в таблице интерфейсов.

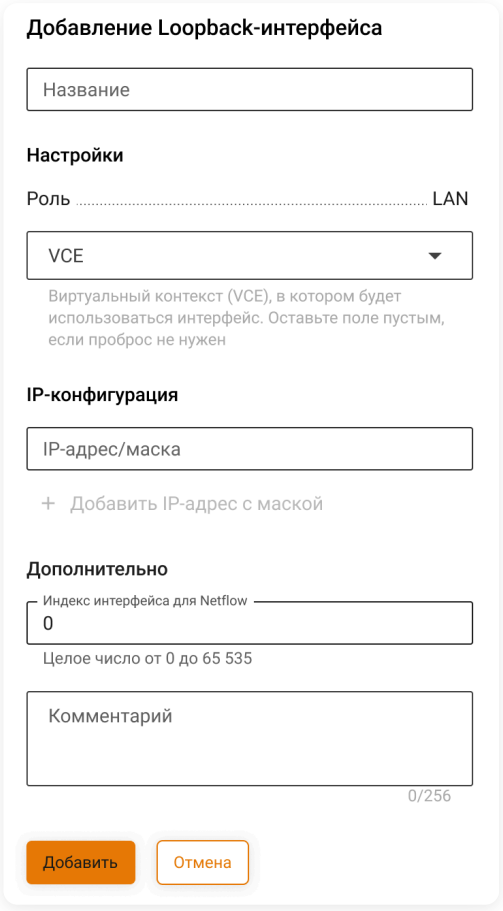
Loopback

Loopback - виртуальный интерфейс, не привязанный к физическому сетевому порту. Основная задача Loopback-интерфейса - обеспечение стабильного IP-адреса для устройства, который остается доступным даже при сбоях физических соединений.

Для настройки Loopback-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Loopback**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - только **LAN** для создания локальных интерфейсов.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

Чтобы избежать проблем с подключением пользователей к Loopback-интерфейсу по VPN, IP-адрес Loopback-интерфейса **не должен** входить в диапазоны адресов, используемые для SNAT. Если включен автоматический SNAT локальных сетей, IP-адрес Loopback-интерфейса не должен входить в диапазоны:

- `10.0.0.0/8`
- `192.168.0.0/16`
- `172.16.0.0/12`

3. Нажмите **Добавить**. Loopback-интерфейс появится в таблице интерфейсов.

Особенности настройки Loopback-интерфейса

При работе с Loopback-интерфейсом используйте правила:

- Для доступа к веб-интерфейсу Ideco NGFW Novum укажите в адресной строке браузера `<IP-адрес Loopback-интерфейса>:8443`.
- Для доступа к серверу по SSH:
  - Разрешите доступ по SSH.
  - Введите в терминале `ssh login@<IP-адрес Loopback-интерфейса>`.
- Для подключения пользователей по VPN на устройстве пользователя при создании VPN-подключения в качестве шлюза укажите домен или IP-адрес Loopback-интерфейса.
- В разделе **BGP** при добавлении **BGP-соседей** укажите в поле **Исходящий интерфейс** Loopback-интерфейс.

- При настройке **OSPF** укажите в поле **Интерфейс** Loopback-интерфейс.
- При создании маршрута Null route укажите Loopback-интерфейс в качестве шлюза для подсети/IP-адресов. В этом случае весь входящий на NGFW трафик, предназначенный для этих адресов, будет отбрасываться.
- При создании DNAT-правила **Межсетевого экрана** в поле **Адрес назначения** укажите IP-адрес, назначенный на Loopback-интерфейс. Опубликованные ресурсы будут доступны по IP-адресу Loopback-интерфейса.
- При создании SNAT-правила **Межсетевого экрана** в поле **Сменить IP-адрес источника** укажите IP-адрес, назначенный на Loopback-интерфейс. Исходный адрес, указанный в поле **Адрес источника**, будет заменен на адрес Loopback-интерфейса.

Для подключения к Loopback-интерфейсу настройте маршрутизацию до IP-адреса, назначенного на этот Loopback-интерфейс.

L2-мост

L2-мост не поддерживается в Классическом и Системном контекстах.

L2-мост используется для соединения двух сегментов сети на уровне канального доступа (L2). Он позволяет:

- Объединять две физические сети в один широковещательный домен для распространения broadcast-трафика (ARP, DHCP и так далее) по объединенной логической сети.
- Обеспечивать видимость всех устройств в обоих сегментах сети, объединенных мостом, как если бы эти устройства находились в одной коммутируемой сети.

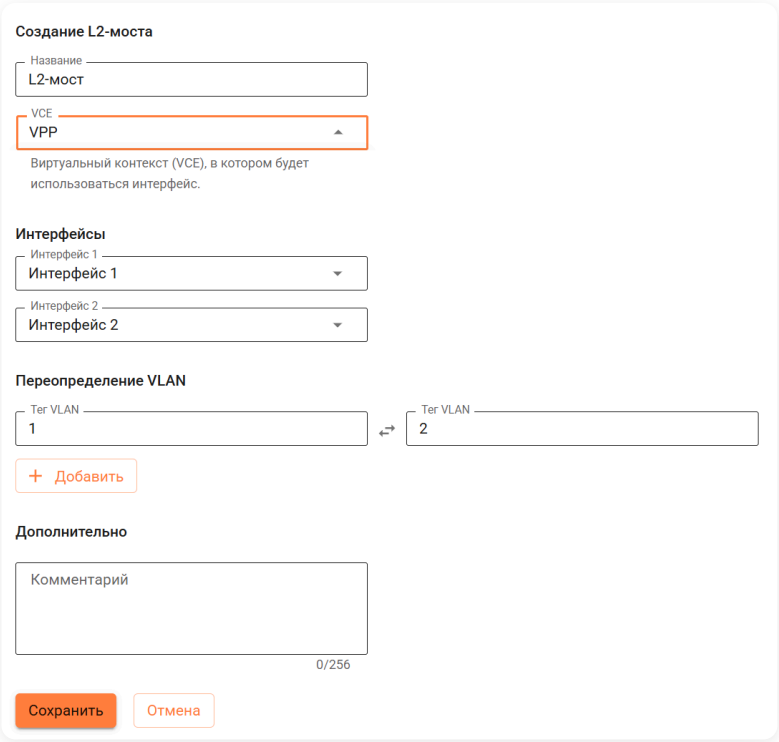
Для создания L2-моста:

1. Создайте два интерфейса. Допустимые интерфейсы:

- **Ethernet** (LAN, WAN).
- **LACP**.
- **VLAN**.

В поле **Физический порт** выберите свободные порты, которые будут объединены L2-мостом, а в поле **VCE** - высокопроизводительный контекст **VPP**.

2. Нажмите **Добавить**, выберите **L2-мост** и заполните поля:



Расшифровка полей

- **Название** - введите название L2-моста.
- **VCE** - выберите VCE VPP.

- **Интерфейсы** - выберите интерфейсы, между которыми будет настроен прозрачный L2-мост. Типы интерфейсов должны совпадать. Нельзя выбрать интерфейсы, имеющие дочерние. При выборе в этих полях VLAN-интерфейсов теги VLAN нельзя будет изменить в настройках моста.
- **Переопределение VLAN** - введите теги VLAN для маппинга или оставьте поля пустыми. Переопределение VLAN работает в обе стороны. При необходимости добавьте несколько пар тегов.
- **Комментарий** - введите описание L2-моста. Максимум 256 символов.

Трафик, проходящий через L2-мост, можно фильтровать политиками безопасности VCE VPP, за временным исключением средств прокси: Контент-фильтра, SSL/TLS-инспекций.

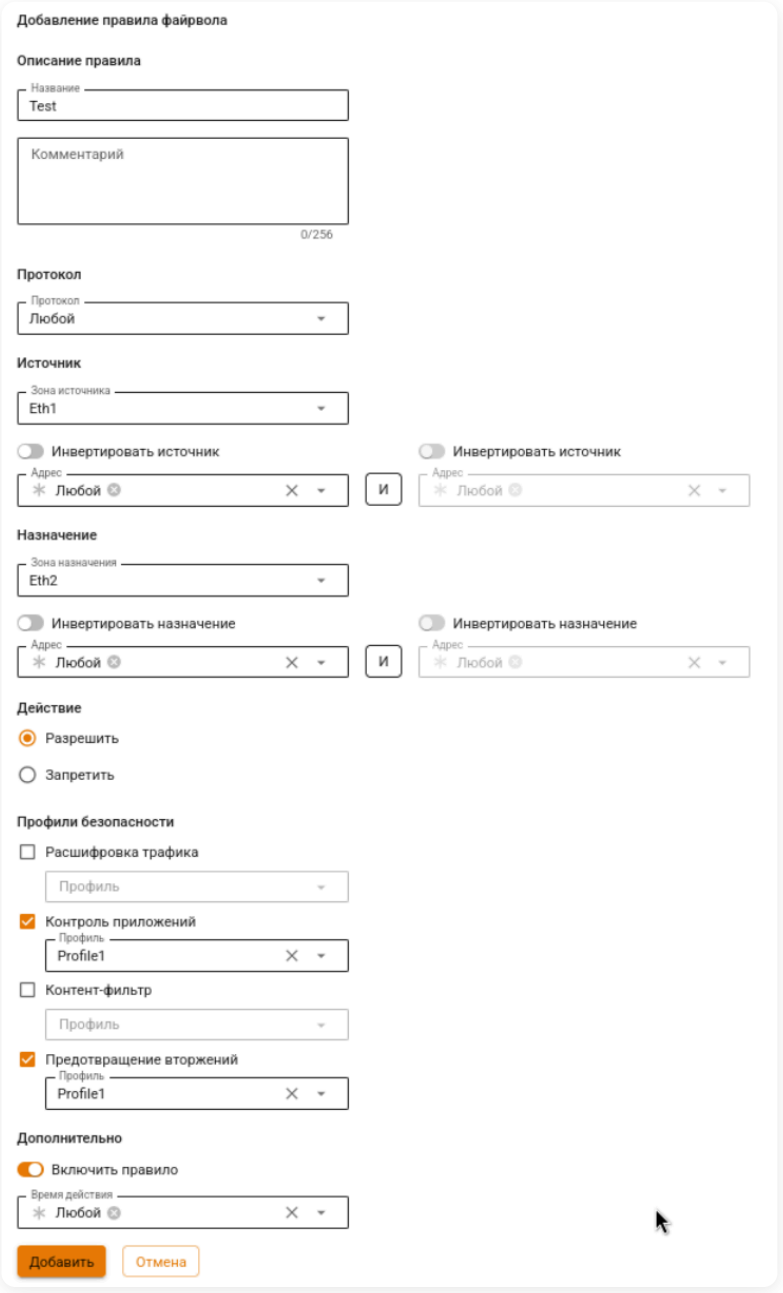
Пример настройки фильтрации

Создан L2-мост между Интерфейсом 1 (зона LAN) и Интерфейсом 2 (зона WAN).

Задача: включить фильтрацию DPI, IPS для трафика из зоны **WAN** в зону **LAN**.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Описание правила** - введите **Название** правила и **Комментарий**.
- **Протокол** - выберите протокол передачи данных: **AH**, **ESP**, **GRE**, **ICMP**, **TCP**, **UDP**, **TCP/UDP** (TCP или UDP) или **Любой**.
- **Источник**:
  - **Зона источника** - выберите Интерфейс 2 (зона WAN).

- **Адрес** - выберите **Любой**.
- **Назначение**:
  - **Зона назначения** - выберите Интерфейс 1 (зона LAN).
  - **Адрес** - выберите **Любой**.
- **Действия** - выберите **Разрешить**.
- **Профили безопасности**:
  - **Расшифровка трафика** - оставьте поле пустым.
  - **Контроль приложений** - выберите профиль Контроля приложений, которым требуется фильтровать трафик.
  - **Контент-фильтр** - оставьте поле пустым.
  - **Предотвращение вторжений** - выберите профиль системы Предотвращения вторжений, которым требуется фильтровать трафик.
- **Дополнительно** - включите правило и задайте время действия. По умолчанию правило выключено.

Подключение по 3G и 4G

В Ideco NGFW Novum поддерживаются модели USB-модемов с Network Communication **CDC-Ethernet**, список модемов представлен в таблице Список поддерживаемых USB-модемов.

Туннельные интерфейсы

GRE

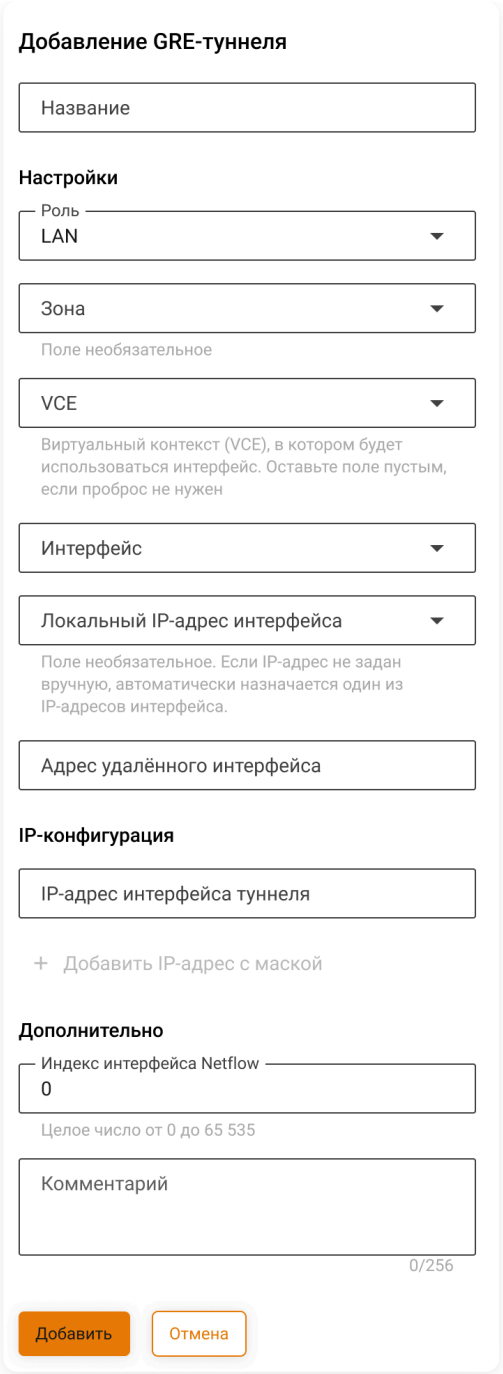
GRE-туннель - соединение, позволяющее передавать широковещательный трафик. Поддерживает работу протокола динамической маршрутизации OSPF. Пакеты, проходящие через GRE-туннель, не подвергаются шифрованию.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

Для настройки GRE-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **GRE**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - доступные роли **WAN** и **LAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN**, **LACP**, **PPTP**, **L2TP** и **PPPoE**.
- **Локальный IP-адрес интерфейса** - укажите IP-адрес родительского интерфейса, на котором запущен туннель.
- **Адрес удаленного интерфейса** - укажите IP-адрес интерфейса для подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес с маской создаваемого туннеля.
- **Шлюз** - укажите шлюз для направления трафика по умолчанию.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. GRE-туннель появится в таблице интерфейсов.

Если GRE-интерфейсу назначена роль **WAN**, для прохождения трафика может потребоваться:

- Авторизация пользователя. Например, по IP-адресу.
- Создание разрешающего правила **FORWARD** для трафика в GRE-туннеле в **Правила трафика** → **Межсетевой экран**.

L2TP

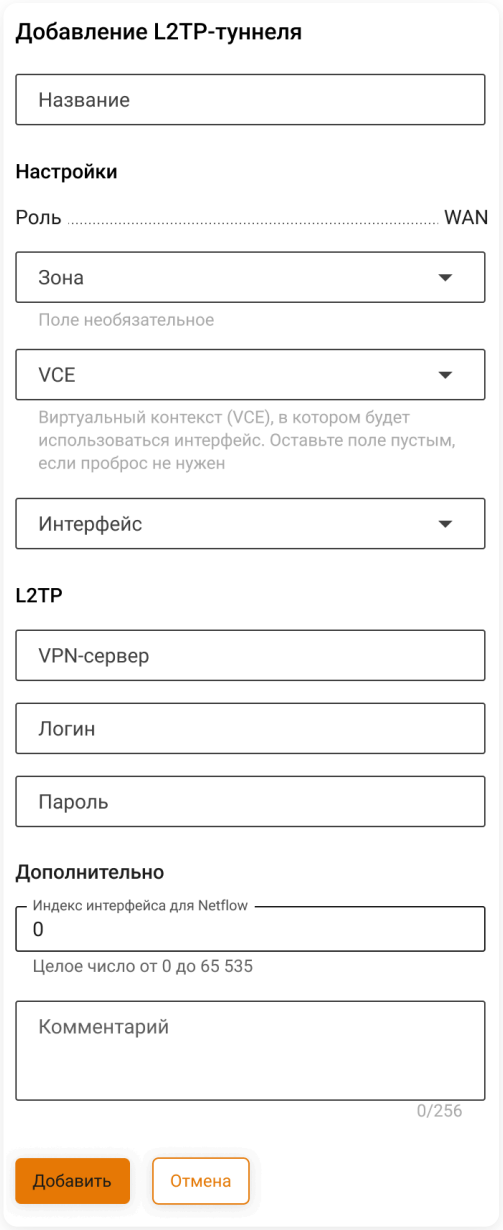
L2TP-туннель - технология подключения, использующая протокол L2TP, которая применяется интернет-провайдерами для повышения надежности процесса авторизации пользователей.

L2TP-туннель можно создать только на интерфейсах, настроенных на режим **Статический** или **DHCP** и роль **WAN**.

Для настройки L2TP-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **L2TP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.

- **Роль** - только **WAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN** и **LACP**.
- **VPN-сервер** - IP-адрес или доменное имя L2TP-сервера.
- **Логин** - имя пользователя для подключения по L2TP.
- **Пароль** - пароль пользователя для подключения по L2TP.
- **DNS-сервер** - укажите, если доменное имя VPN-сервера не резолвится через настроенные в Ideco NGFW Novum DNS-серверы.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. L2TP-туннель появится в таблице интерфейсов.

PPTP

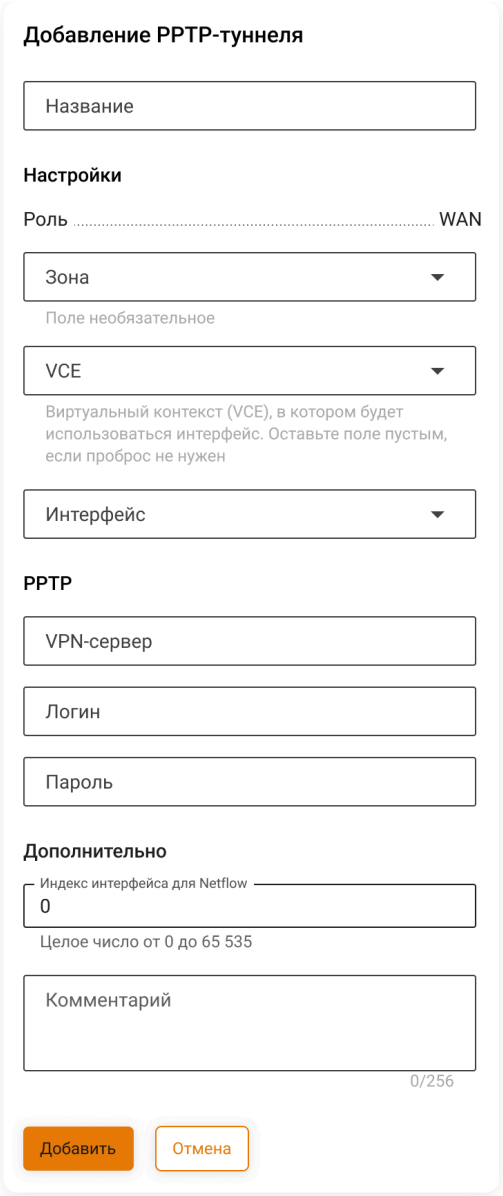
PPTP-туннель - один из первых VPN-протоколов, созданный для обеспечения защищенного доступа через интернет. Работает на базе протокола PPP (Point-to-Point Protocol), который обеспечивает аутентификацию и шифрование данных.

> PPTP-туннель можно создать только на интерфейсах, настроенных на режим **Статический** или **DHCP** и роль **WAN**.

Для настройки PPTP-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **PPTP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - только **WAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN** и **LACP**.
- **VPN-сервер** - IP-адрес или доменное имя PPTP-сервера.
- **Логин** - имя пользователя для подключения по PPTP.
- **Пароль** - пароль пользователя для подключения по PPTP.
- **DNS-сервер** - укажите, если доменное имя VPN-сервера не резолвится через настроенные в Ideco NGFW Novum DNS-серверы.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. PPTP-туннель появится в таблице интерфейсов.

PPPoE

PPPoE-туннель - технология подключения через протокол PPPoE, которая активно применяется интернет-провайдерами при организации доступа в сеть через xDSL-соединения.

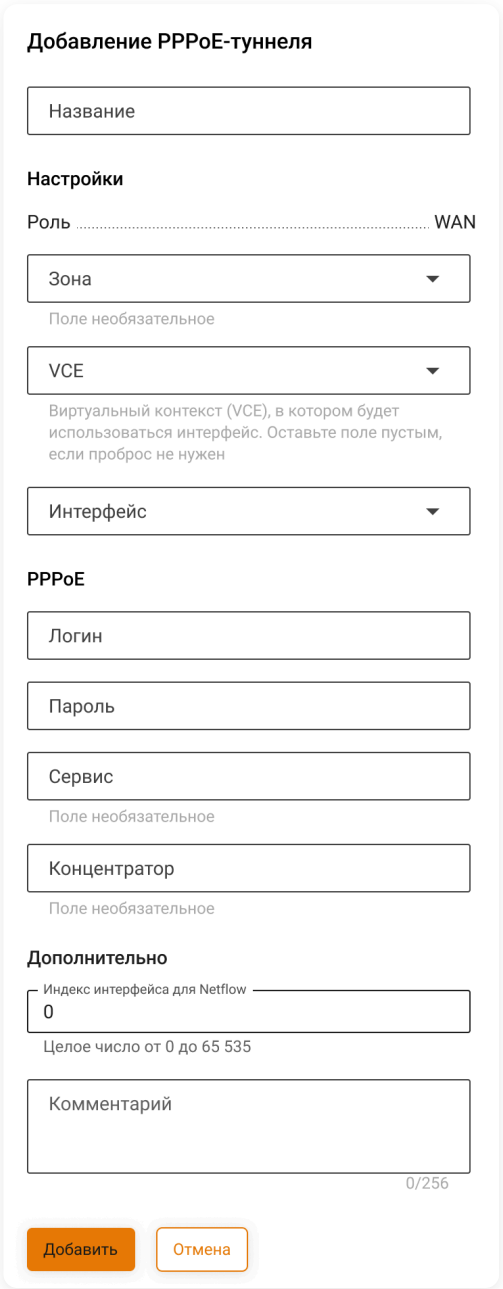
PPPoE-туннель можно создать только на интерфейсах, настроенных на режим **Без конфигурации** и роль **WAN**.

При подключении к провайдеру с использованием протокола PPPoE настройте DNS-сервер вручную, воспользовавшись статьей.

Для настройки PPPoE-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **PPPoE**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - только **WAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN** и **LACP**.
- **Логин** - имя пользователя для подключения по PPPoE.
- **Пароль** - пароль пользователя для подключения по PPPoE.
- **Сервис** - идентификатор сервиса. Необязательное поле.

- **Концентратор** - идентификатор концентратора. Необязательное поле.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. PPPoE-туннель появится в таблице интерфейсов.

Полезные ссылки

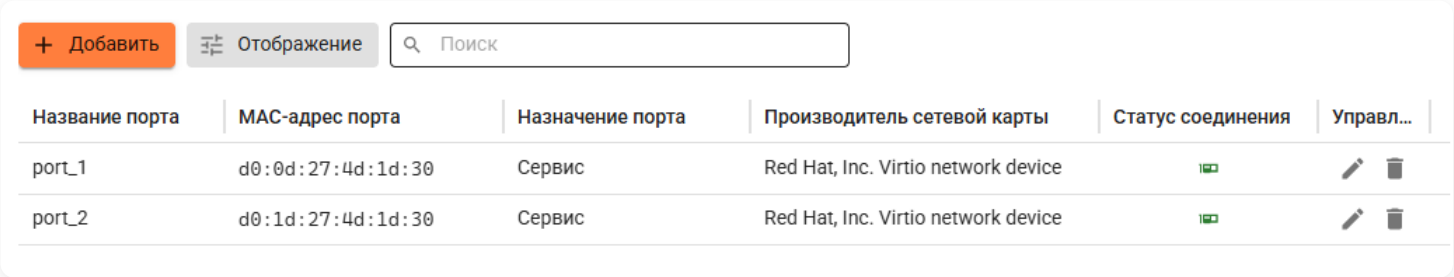
- **Межсетевой экран**
- **Администраторы**
- **BGP**
- **OSPF**
- **Внешние DNS-серверы**

Физические порты

Функциональность доступна в **Классическом** и **Системном контекстах**.

Физические порты связывают сетевую конфигурацию, что позволяет переносить настройки на другой порт без изменения политик безопасности даже при выходе из строя текущего порта.

Сетевые соединения в Ideco NGFW Novum настраиваются в **Сервисы** → **Сетевые интерфейсы** → **Интерфейсы** и ссылаются на **Физические порты**. При первичной установке Ideco NGFW Novum порты автоматически включаются в таблицу и получают название, например, `eth0_b1`. Записи в таблице отражают физические порты на корпусе устройства:



Если **Название порта** не соответствует физическому обозначению, переименуйте порт в соответствии с обозначением на корпусе устройства.

На сетевых картах может быть несколько сетевых портов, каждый из которых имеет свой MAC-адрес.

Возможность передавать в VCE VPP отдельные порты сетевой карты зависит от модели сетевого адаптера:

- Если адаптер поддерживает разделение портов, порты можно передавать по отдельности.
- Если адаптер не поддерживает разделение портов, в VCE VPP необходимо передавать все порты сетевой карты. Иначе интерфейсы этой сетевой карты работать не будут.

В кластеризации используется сетевая конфигурация, общая для обеих нод. Конфигурация ссылается на физические порты по их названию. Соответствие названий конкретным физическим картам хранится:

- Для аппаратных решений - в прошивке сервера (UEFI).
- Для виртуальных машин - внутри образа диска.

Подключение по 3G и 4G

В Ideco NGFW Novum поддерживаются модели USB-модемов с Network Communication **CDC-Ethernet**, список модемов представлен в таблице Список поддерживаемых USB-модемов. При подключении USB-модем будет отображаться в Ideco NGFW Novum как новый ethernet-интерфейс.

Статусы соединения

- Подключен
- Не подключен
- Статус порта неизвестен. Проверьте физический порт, его состояние и совместимость оборудования

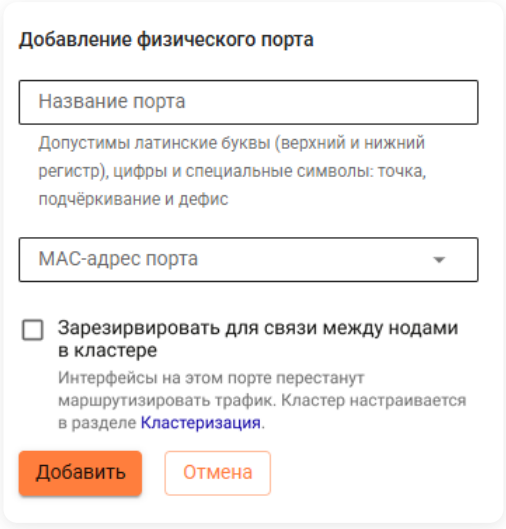
Управление портами

Порты можно редактировать, нажав , или удалить, нажав . При удалении порта созданные на его основе интерфейсы перестанут работать, пока не назначить на них новый порт. Для идентификации порта ориентируйтесь на наименование производителя или MAC-адрес.

Чтобы добавить новый порт, выполните действия:

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и нажмите **Добавить**.

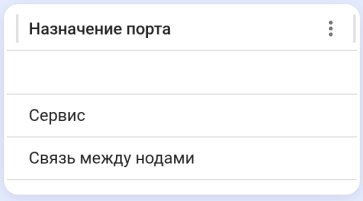
2. Заполните поля:



- **Название порта** - укажите обозначение порта на корпусе устройства.
- **MAC-адрес порта** - выберите свободный порт на сетевой карте.
- **Зарезервировать для связи между нодами в кластере** - включите опцию, если требуется использовать порт для настройки кластеризации. Подробнее в статье Кластеризация. В списке портов в колонке **Связь между нодами** порты со включенной опцией будут иметь значение **Связь между нодами**, а порты с выключенной опцией - значение **Сервис**.

Примеры настройки физических портов

Примеры актуальны для портов с назначением **Сервис**:

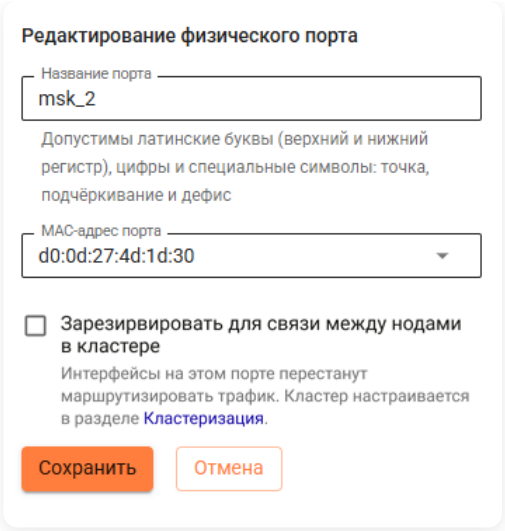


Переименование порта

Наименования всех используемых сетевых портов в кластере должны совпадать на обеих нодах. Подробнее в статье Настройка кластера.

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и нажмите .

2. Отредактируйте **Название порта** и нажмите **Сохранить**:



Перенос сетевого интерфейса на другой порт

Возможные причины переноса сетевого интерфейса на другой порт:

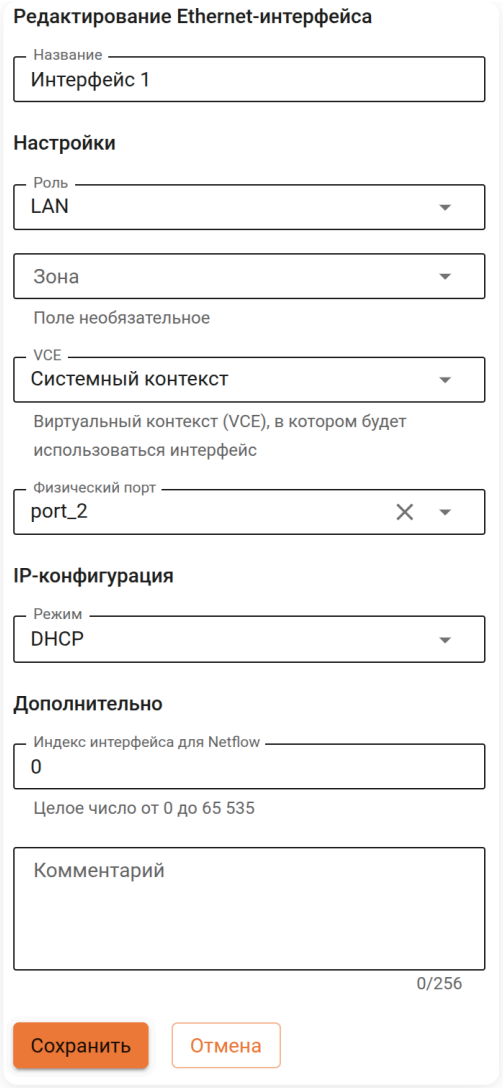
- Замена сетевой карты.
- Выход порта из строя.
- Изменение схемы подключения или порядка портов на устройстве.

> Перенос сетевого интерфейса на другой порт не влияет на настройки правил фильтрации.

Выполните действия:

1. Перейдите в **Сетевые интерфейсы** → **Интерфейсы** и отредактируйте необходимый интерфейс, нажав .

2. Выберите порт в поле **Физический порт** и нажмите **Сохранить**:



3. Если порт занят:

- Отключите интерфейс, порт которого необходимо переназначить на другой интерфейс, нажав .
- Выполните действия из пункта 1.

Перенос сетевых интерфейсов в кластере

Так как в кластеризации используется общая сетевая конфигурация, перенос сетевого интерфейса на другой порт выполняется только на активной ноде. При выходе из строя порта в кластере есть два варианта действий:

Использование другой пары портов

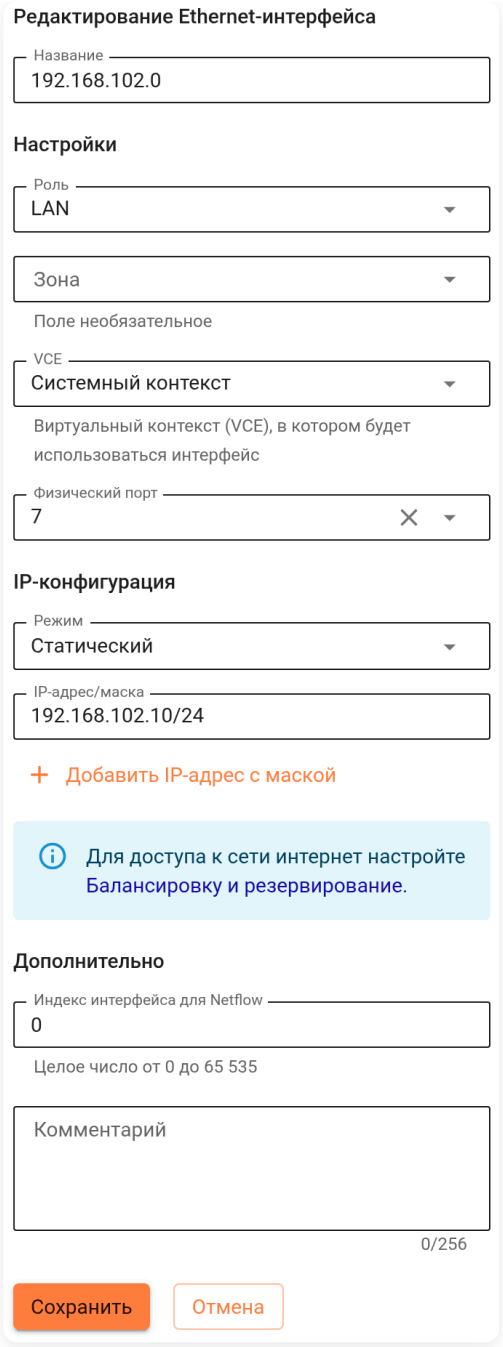
Рекомендуемый вариант, так как обеспечивает соответствие наименований портов физическим обозначениям на сервере.

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и найдите свободную пару портов в активной и пассивной нодах:

Название порта	MAC-адрес порта	Назначение порта	Производитель сетевой карты	Статус соединения	Управление
cluster (Активная) • 7					
1	bc:24:11:08:ee:d0	Сервис	Red Hat, Inc. Virtio network device		
2	bc:24:11:bb:cb:40	Связь между нодами	Red Hat, Inc. Virtio network device		
3	bc:24:11:85:6e:b9	Сервис	Red Hat, Inc. Virtio network device		
4	bc:24:11:df:1b:5a	Сервис	Red Hat, Inc. Virtio network device		
5	bc:24:11:14:6a:a9	Сервис	Red Hat, Inc. Virtio network device		
6	bc:24:11:97:d8:b9	Сервис	Red Hat, Inc. Virtio network device		
7	bc:24:11:19:ad:fb	Сервис	Red Hat, Inc. Virtio network device		
ngfw (Пассивная) • 7					
1	bc:24:11:3f:dd:98	Сервис	Red Hat, Inc. Virtio network device		
4	bc:24:11:14:fe:f3	Сервис	Red Hat, Inc. Virtio network device		
5	bc:24:11:10:67:e5	Сервис	Red Hat, Inc. Virtio network device		
3	bc:24:11:0f:c3:51	Сервис	Red Hat, Inc. Virtio network device		
2	bc:24:11:e4:e0:62	Связь между нодами	Red Hat, Inc. Virtio network device		
7	bc:24:11:10:49:7d	Сервис	Red Hat, Inc. Virtio network device		
6	bc:24:11:45:f2:50	Сервис	–		

2. Перейдите на вкладку **Интерфейсы** и отредактируйте интерфейс, порт которого вышел из строя, нажав .

3. Выберите порт в поле **Физический порт** и нажмите **Сохранить**:



Переименование свободного порта

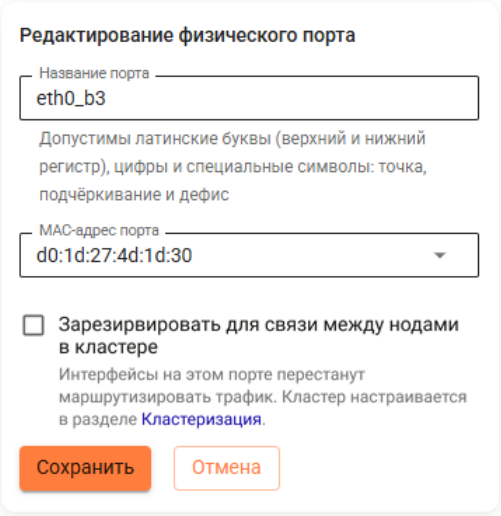
Может вызвать несоответствие между наименованием порта в веб-интерфейсе и физическим обозначением.

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и выберите свободный порт в ноде, порт которой вышел из строя:

Название порта	MAC-адрес порта	Назначение порта	Производитель сетевой карты	Статус соединения	Управление
cluster (Активная) • 7					
eth0_98	bc:24:11:08:ee:d0	Сервис	Red Hat, Inc. Virtio network device		
eth0_b3	bc:24:11:bb:cb:40	Связь между нодами	Red Hat, Inc. Virtio network device		
eth0_51	bc:24:11:85:6e:b9	Сервис	Red Hat, Inc. Virtio network device		
eth1_f3	bc:24:11:df:1b:5a	Сервис	Red Hat, Inc. Virtio network device		
eth0_e5	bc:24:11:14:6a:a9	Сервис	Red Hat, Inc. Virtio network device		
eth2_7d	bc:24:11:32:72:32	Сервис	–		
⚠ eth1_b9	bc:24:11:97:d8:b9	Сервис	Red Hat, Inc. Virtio network device		
ngfw (Пассивная) • 7					
eth0_98	bc:24:11:3f:dd:98	Сервис	Red Hat, Inc. Virtio network device		
eth1_f3	bc:24:11:14:fe:f3	Сервис	Red Hat, Inc. Virtio network device		
eth0_e5	bc:24:11:10:67:e5	Сервис	Red Hat, Inc. Virtio network device		
eth0_51	bc:24:11:0f:c3:51	Сервис	Red Hat, Inc. Virtio network device		
eth0_b3	bc:24:11:e4:e0:62	Связь между нодами	Red Hat, Inc. Virtio network device		
eth2_7d	bc:24:11:10:49:7d	Сервис	Red Hat, Inc. Virtio network device		
⚠ eth3_50	bc:24:11:45:f2:50	Сервис	Red Hat, Inc. Virtio network device		

2. Сохраните **Название порта**, вышедшего из строя, и нажмите для его удаления.

3. Нажмите для редактирования свободного порта и укажите название порта, сохраненное в пункте 2:



4. Нажмите **Сохранить**.

Рекомендуем на корпусе оборудования указать новое название порта, заданное в веб-интерфейсе, и переключить кабель в новый порт.

Перенос бэкапа на другой сервер

Пример настройки подробно описан в статье Бэкапы.

Полезные ссылки

- **Бэкапы**
- **Кластеризация**
- **Настройка кластера**
- **Список поддерживаемых USB-модемов**

IGMP Proxy

Классический контекст | Высокопроизводительный контекст

Название службы раздела **IGMP Proxy**: `ideco-igmpproxy-rest`, `ideco-igmpproxy-backend`, `ideco-igmpproxy`.

Список служб для других разделов доступен по ссылке.

IGMP Proxy - служба, которая позволяет передавать мультикастовый трафик через маршрутизатор. IGMP Proxy работает как посредник между мультикастовыми группами и сетью, оптимизируя передачу данных, что сокращает объем трафика, снижает нагрузку на сеть и повышает скорость работы сети.

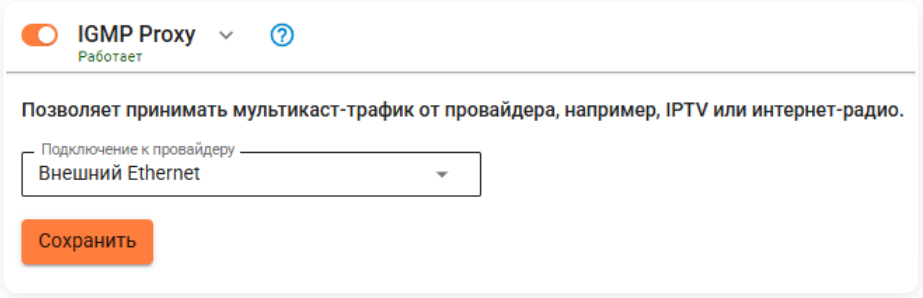
Со стороны клиентов **IGMP Proxy** поддерживает версии IGMPv1 и IGMPv2.

IGMP Proxy работает только с Ethernet-интерфейсами и не работает на интерфейсах VLAN, PPPoE или VPN (L2TP, PPTP).

Настройка в Ideco NGFW Novum

1. Прейдите в **Сервисы** → **IGMP Proxy** и включите опцию **IGMP Proxy**.

2. В поле **Подключение к провайдеру** выберите **Ethernet-подключение**:



Принцип работы

На примере подключения двух пользователей к мультикаст-потоку одного источника:

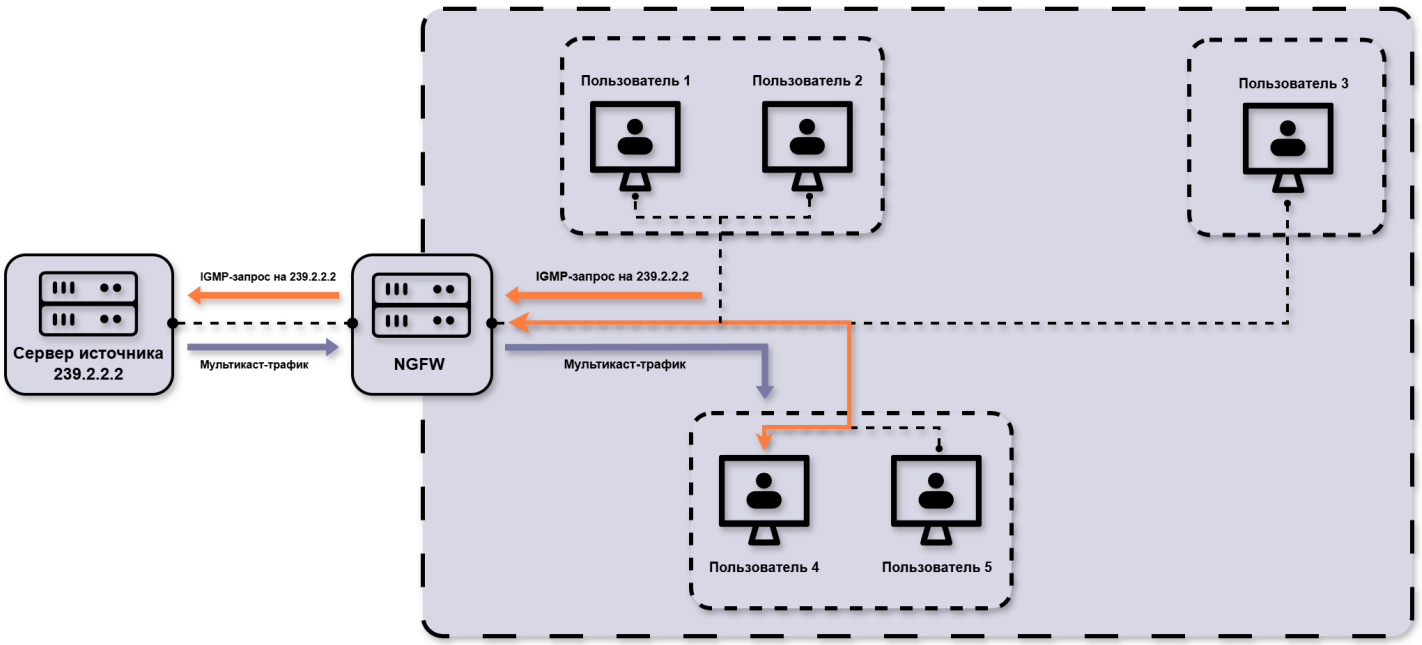
1. **Сервер источника** начинает трансляцию мультикаст-трафика с адреса из диапазона 224.0.0.0/4.

2. **Пользователь 4** хочет подключиться к трафику и генерирует IGMP-запрос (Join) на **Ideco NGFW Novum** для получения мультикаст-трафика от сервера источника.

3. **Ideco NGFW Novum** получает IGMP-запрос и отправляет аналогичный запрос к серверу источника.

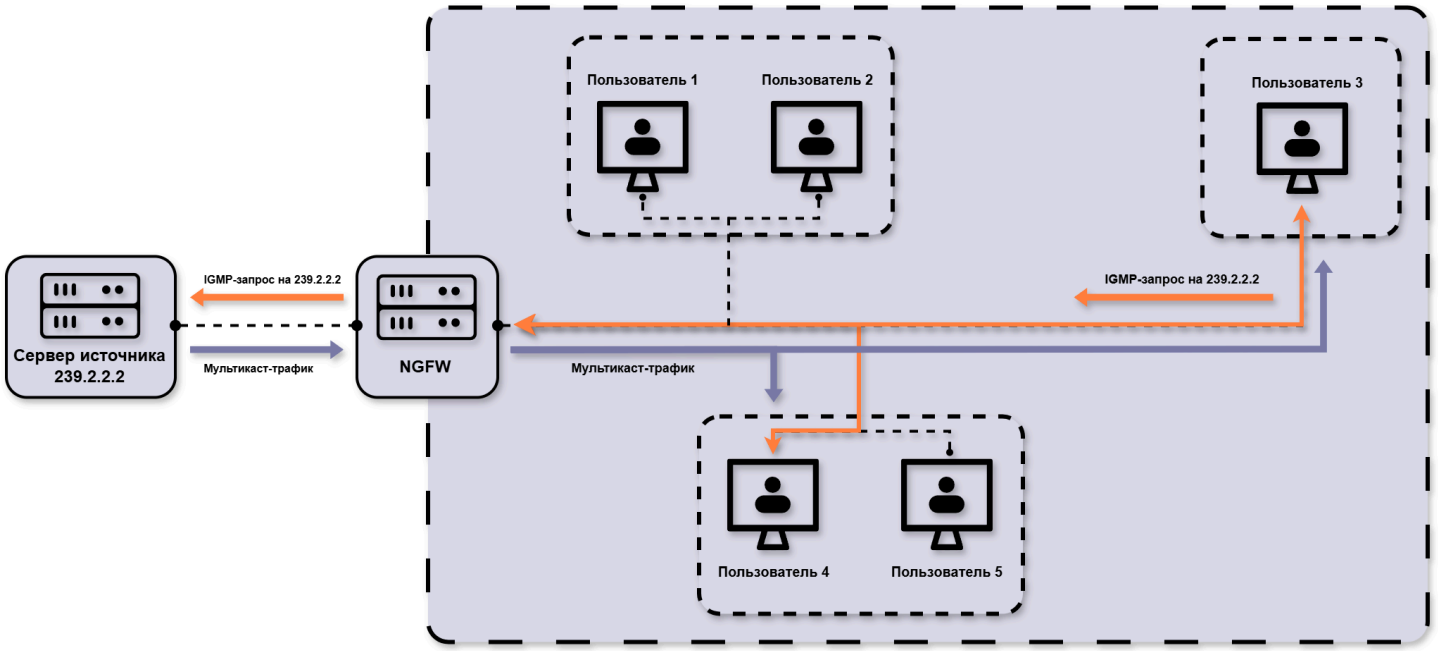
4. Сервер источника получает запрос и начинает транслировать мультикаст-трафик на **Ideco NGFW Novum**.

5. **Ideco NGFW Novum** пропускает трафик с адреса 239.2.2.2 в подсеть с **Пользователем 4**, и **Пользователь 4** становится получателем трафика:



6. **Пользователь 3**, находящийся в другой подсети, также решает подключиться к этой трансляции и генерирует IGMP-запрос (Join) на Ideco NGFW Novum.

7. **Ideco NGFW Novum** получает запрос и дублирует **Пользователю 3** трафик, поступающий **Пользователю 4**:



Ideco NGFW Novum периодически проверяет, есть ли получатели, отправляя пользователям IGMP-запрос (Query). Пользователи в ответ отправляют Join, как при подключении.

Если на Ideco NGFW Novum приходит хотя бы один Join, мультикаст-трафик продолжает транслироваться получателям.

Прокси

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Прокси**: `ideco-proxy-backend`, `squid`.

Список служб для других разделов доступен по ссылке.

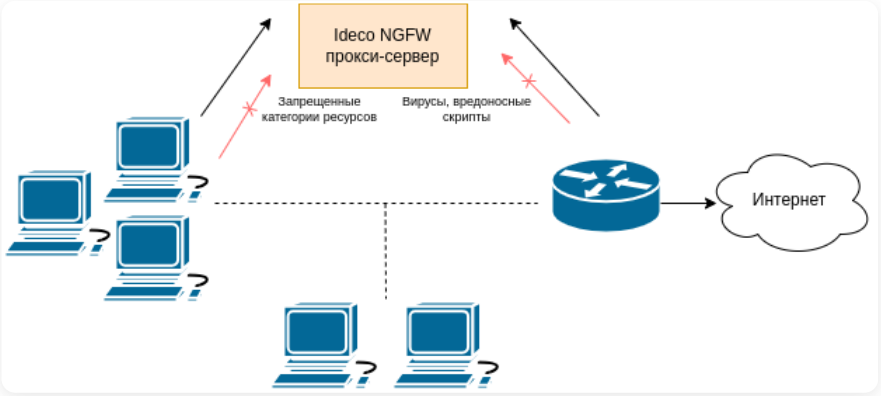
Прокси-сервер используется не только для проксирования веб-трафика, но и для передачи трафика сервисам:

- Антивирус для веб-трафика (Антивирус Касперского).
- Сервис отчетности по веб-трафику пользователей.
- Контент-фильтр.

Порядок обработки веб-трафика подробнее описан в статье.

Не указывайте на хостах локальной сети настройки прокси. Достаточно указания NGFW Novum в качестве шлюза по умолчанию для устройств в сети.

Для настройки фильтрации HTTPS-трафика нужно добавить корневой сертификат NGFW Novum на компьютеры пользователей. Подробнее в статье Настройка фильтрации HTTPS.



При использовании Ideco NGFW Novum в качестве прокси-сервера с прямыми подключениями к прокси большинство функций будет работать с некоторыми особенностями:

- В правилах **Файрвола** для пользователей необходимо указывать цепочки **INPUT** вместо **FORWARD**.
- Глубокий анализ трафика системой **Предотвращение вторжений** и модулем **Контроль приложений** будет осуществляться только для трафика, проходящего через прокси-сервер (часть правил работать не будет).
- Исключения из прокси-сервера необходимо делать средствами браузера или правилами маршрутизации на конечных устройствах. Настройки в разделе **Сервисы** → **Прокси** → **Исключения** применяются только для прозрачного режима работы прокси-сервера.

Для работы прокси-сервера необходим хотя бы один сетевой интерфейс с ролью **LAN**. Если настроен только интерфейс **Control Plane**, служба `squid` не запустится, при этом отобразится сообщение об отсутствии локальных интерфейсов. Для решения проблемы назначьте одному из интерфейсов роль **LAN** в **Сервисы** → **Сетевые интерфейсы**. Подробнее о настройке интерфейсов - в статье.

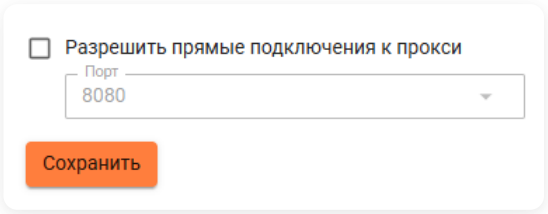
Основное

На вкладке **Основное** предоставлены возможности:

- **Разрешить прямые подключения к прокси** - применяется, когда Ideco NGFW Novum не является шлюзом по умолчанию для клиентов сети. Порт, указанный на стороне NGFW Novum, следует указать на сетевых устройствах локальной сети, веб-трафик которых нужно пропускать через

прокси.

- **Включить журналирование** - применяется для записи логов Антивируса и Контент-фильтра.

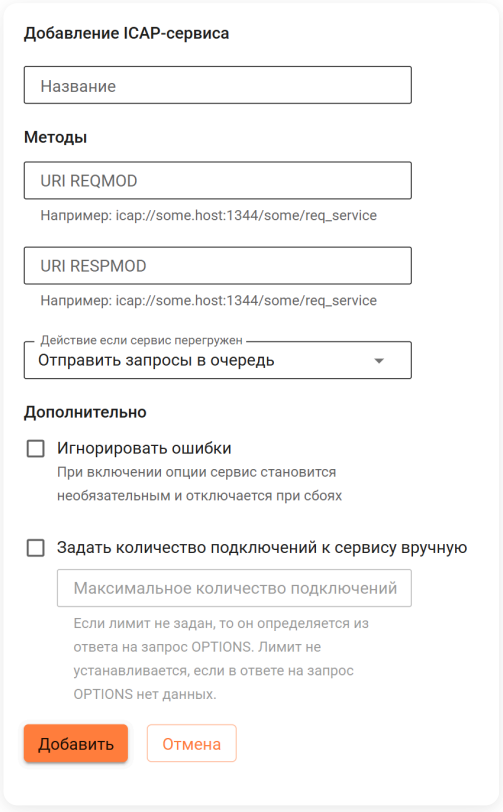


ICAP

ICAP-сервисы обрабатывают исходящий трафик (запросы) после работы Антивируса и Контент-фильтра Ideco NGFW Novum, а входящий (ответы) - перед Антивирусом.

> Для корректной работы ICAP-сервиса должна быть настроена расшифровка HTTPS-трафика в **Контент-фильтре**.

При добавлении ICAP-сервиса доступны настройки:



- **URI REQMOD** - URI для модификации HTTP-запросов перед их отправкой на сервер. Используется для обработки и изменения исходящего трафика.
- **URI RESPMOD** - URI для модификации HTTP-ответов перед их передачей клиенту. Применяется для обработки и изменения входящего трафика.
- **Если сервис перегружен** - опция позволяет выбрать сценарий действий при перегруженности ICAP-сервиса.
- **Игнорировать ошибки** - если включена опция, то сервис будет считаться необязательным. При недоступности или неправильной работе сервис не будет задействован.
- **Установить лимит подключений к сервису** - если значение не задано, максимальное количество подключений берется из ответа сервиса на запрос OPTIONS. Если максимальное количество подключений не указано в ответе на запрос OPTIONS, тогда - без ограничений.

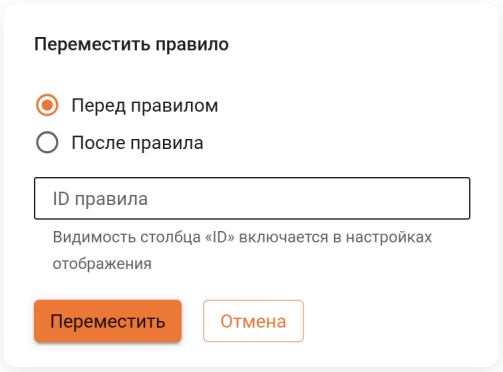
> Если указать в опции **Установить лимит подключений к сервису** значение меньше четырех, то клиентские подключения могут быть нестабильными.

Для перемещения сервисов в таблице выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

WCCP

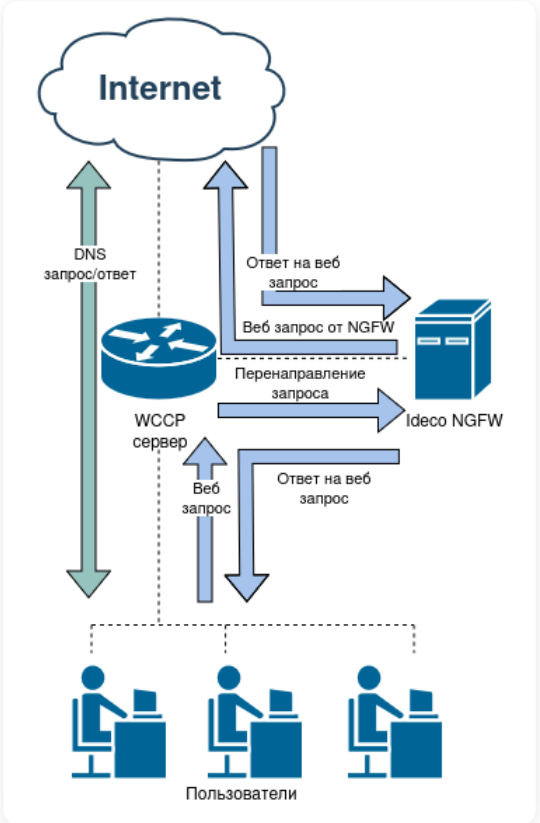
Протокол WCCP используется для перенаправления трафика на Ideco NGFW Novum. По умолчанию перенаправляется только HTTP/HTTPS-трафик.

Для активации WCCP включите опцию **Включить перенаправление трафика с WCCP-серверов на Ideco NGFW Novum**. Запустится процесс согласования параметров с WCCP-сервером.

В NGFW Novum предусмотрено два режима работы WCCP - L2 и GRE:

L2

Режим L2 используется, если WCCP-сервер и Ideco NGFW Novum находятся в одном сетевом сегменте:



Последовательность обработки веб-запросов на уровне L2:

1. Пользователь отправляет веб-запрос.

2. Запрос перенаправляется сервером на Ideco NGFW Novum.

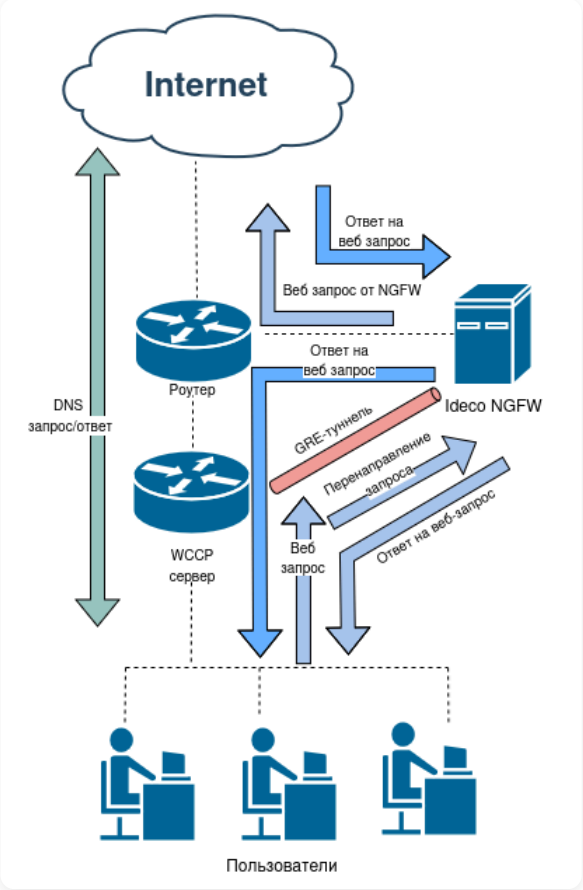
3. Ideco NGFW Novum обрабатывает запрос:

- Если запрос заблокирован, информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW Novum подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается обратно по тому же пути, по которому уходил на внешний сервер.
GRE

Для работы WCCP в GRE-режиме необходимо создать на Ideco NGFW Novum GRE-интерфейс, указав в поле **Адрес удаленного интерфейса** IP-адрес WCCP-сервера.

Режим GRE используется, если WCCP-сервер и Ideco NGFW Novum находятся в разных сетевых сегментах:



Последовательность обработки веб-запросов на уровне GRE:

1. Пользователь отправляет веб-запрос.

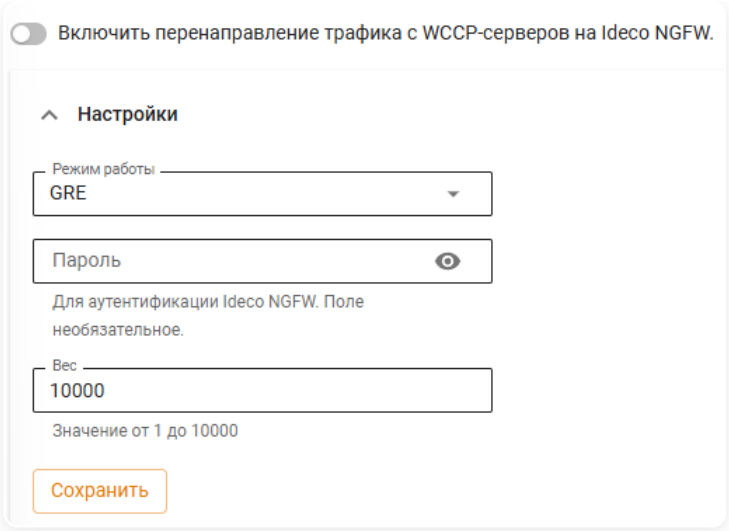
2. Запрос перенаправляется по GRE-туннелю на Ideco NGFW Novum.

3. Ideco NGFW Novum обрабатывает запрос:

- Если запрос заблокирован, то информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW Novum подменяет IP-адрес источника и направляет запрос на внешний сервер.

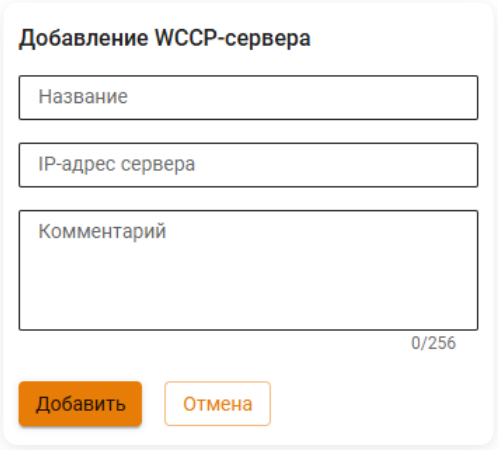
Ответ возвращается напрямую от Ideco NGFW Novum пользователю, минуя GRE-туннель.
Для выбора режима раскройте блок **Настройки**.

Если на WCCP-сервере задан пароль, сохраните пароль в соответствующем поле:



Если WCCP использует несколько Ideco NGFW Novum, настройте распределение трафика с помощью указания приоритета в поле **Вес**. Допустимые значения - от 1 до 10000.

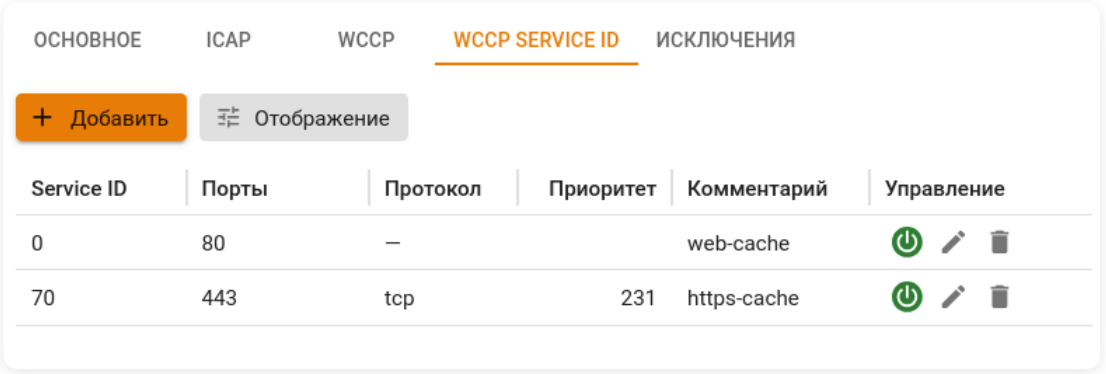
Для добавления WCCP-сервера нажмите кнопку **Добавить** и укажите IP-адрес сервера:



WCCP Service ID

Service ID - идентификаторы сервисной группы. Настройки на этой вкладке позволяют выбрать службы, трафик которых сервер WCCP будет перенаправлять на Ideco NGFW Novum.

По умолчанию настроены сервисы для HTTP/HTTPS-трафика:

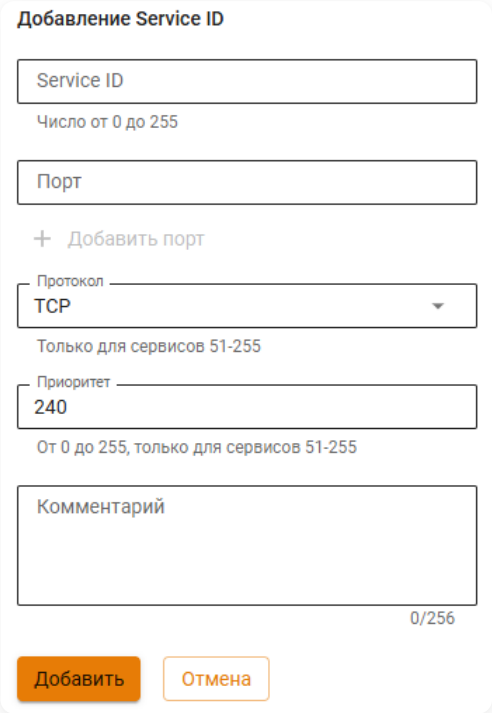


> Service ID с 0 по 50 зарезервированы под фиксированные сервисы. Для них выбирать порты и протоколы нельзя.
>
> Service ID 70 - общепринятое значение для HTTPS-трафика на 443 TCP-порт.

Чтобы настроить Service ID, выполните действия:

1. На вкладке **WCCP Service ID** нажмите кнопку **Добавить**.

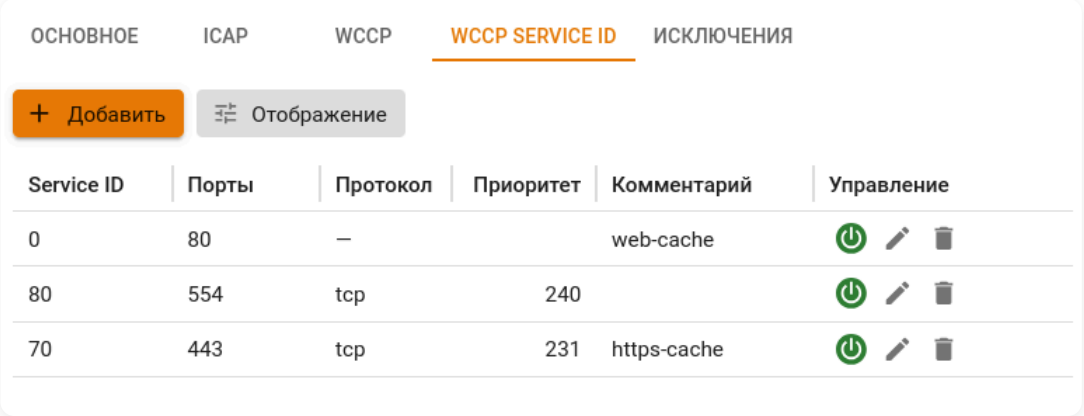
2. В открывшейся форме укажите следующие значения:



- **Service ID** - идентификатор сервисной группы, трафик которой планируется перенаправлять на прокси-сервер. Выбирайте значения от 51 до 255, чтобы избежать проблем со старыми серверами WCCP.
- **Порты** - укажите порты назначения. Максимум 8 значений.
- **Протокол** - укажите протокол для перенаправляемого трафика (TCP, UDP).
- **Приоритет** - укажите приоритет Service ID от 0 до 255. Чем больше число, тем выше приоритет.

Service ID должен соответствовать идентификатору группы, определенному на сервере WCCP.

3. Нажмите **Добавить**. Созданный Service ID появится в таблице:



Исключения

Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

Подробнее о типах исключений в статье Исключения.

Полезные ссылки

- **Настройка Ideco NGFW в качестве прокси с одним интерфейсом**
- **Настройка программы Proxifier для прямых подключений к прокси серверу**

Исключения

Функциональность доступна в **Классическом** и **Системном контекстах**.

Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

На вкладке **Исключения** можно исключить ресурсы из обработки прокси-сервером и всеми связанными службами (контент-фильтр, веб-отчетность, антивирусы):

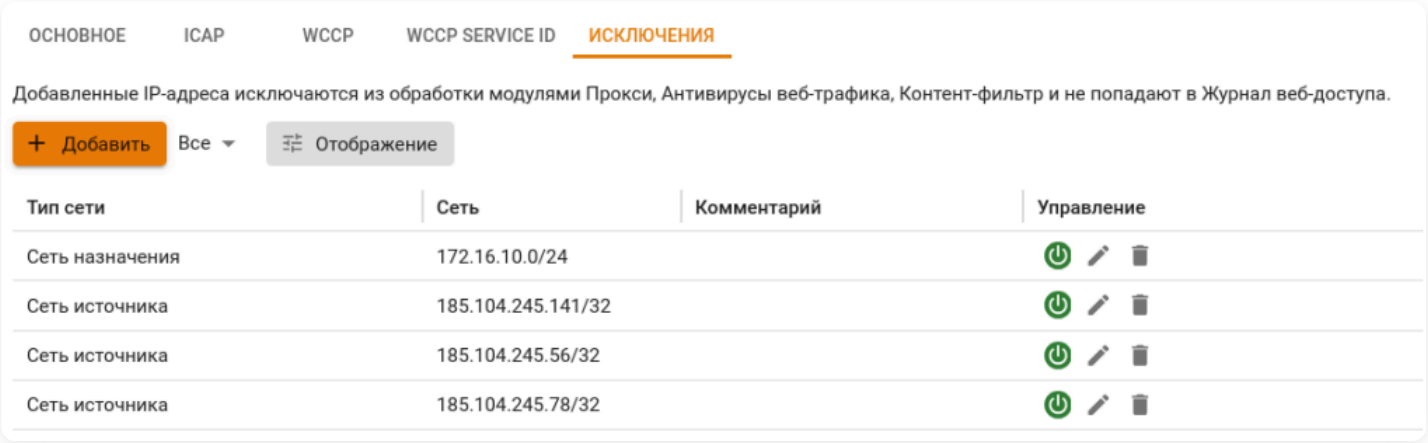
- **Сети источника** - указываются сети, трафик из которых исключается из обработки прокси-сервером.
- **Сети назначения** - указываются внешние сети или IP-адреса (как правило, адреса веб-сайтов или веб-сервисов), трафик до которых из всех локальных сетей NGFW исключается из обработки прокси-сервером.

Настоятельно не рекомендуем исключать из обработки прокси-сервером ВСЮ локальную сеть.

При прямом подключении к прокси-серверу нельзя исключить трафик из обработки прокси. Исключать трафик нужно в настройках прокси-сервера на устройстве (в веб-браузере или системных настройках прокси-сервера).

При создании исключений можно указывать только IP-адреса или IP-сети.

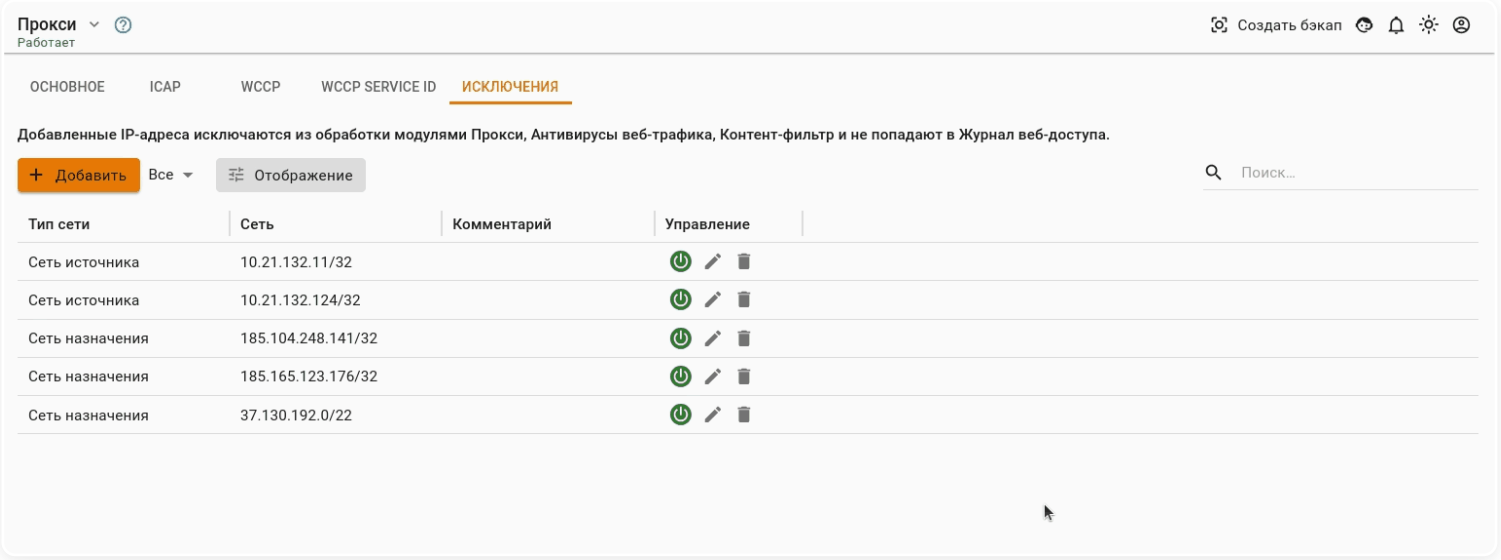
Трафик, исключенный из обработки прокси, не будет участвовать в **Отчетах**, проверяться на вирусы и обрабатываться модулем **Контент-фильтра**. В то же время трафик будет проверен **Межсетевым экраном**, модулями **Предотвращение вторжений** и **Контроль приложений**:



Если добавлено исключение в **Прокси**, соответствующий HTTP(S)-трафик перенаправляется в таблицу **FORWARD** для фильтрации и не попадает в зону **Исходящий трафик устройства**.

Поиск по таблице исключений

Над таблицей исключений расположена строка поиска позволяющая искать среди исключений определенные IP-адреса и сети. Для поиска начните вводить требуемый IP-адрес:



Программы, работающие по отличным от HTTP(S) протоколам через веб-прокси

Некоторые программы, отправляющие трафик на свои серверы по портам 80 и 443, но при этом работающие по протоколам, отличным от HTTP(S), не могут быть обработаны веб-прокси-сервером на NGFW с включенной фильтрацией HTTPS-трафика. Трафик таких программ следует исключать из обработки прокси в поле **Сети назначения**.

1С Коннект

- 185.104.248.141/32
- 185.151.243.218/32
- 185.99.140.108/32
- 185.99.140.101/32
- 185.99.140.102/32
- 185.99.140.103/32
- 185.99.140.104/32
- 185.99.140.105/32
- 185.99.140.106/32
- 185.99.140.107/32
- 185.99.140.108/32
- 185.99.140.114/32
- 185.99.140.115/32
- 193.107.238.195/32
- 77.223.98.83/32
- 77.244.213.204/32
- 78.155.206.40/32
- 78.155.218.78/32
- 80.249.148.135/32
- 88.198.27.15/32
- 88.198.27.27/32
- 88.221.132.128/32
- 92.242.35.35/32
- 46.4.207.211/32
- 2.16.154.81/32
- 185.188.183.87/32
- 185.24.93.122/32
- 185.244.173.25/32
- 185.143.172.61/32

ВЭД-Декларант

- 46.48.116.196/32
- 94.213.21.144/32

- 194.213.21.144/32
- 91.220.57.3/32
- 212.49.126.110/32

MAX

- 104.18.20.226/32
- 104.18.21.226/32
- 155.212.192.0/20
- 185.16.148.119/32
- 185.226.55.94/32
- 5.101.40.2/32

Webinar.ru

- 185.45.80.0/22
- 37.130.192.0/22

vks.samregion.ru

- 195.248.236.141/32

Магазин DNS

- 185.165.123.176/32
- 5.8.69.70/32

СДЭК

- 185.165.123.40/32

Сбербанк Бизнес Онлайн

- 194.54.14.137/32
- 194.54.15.90/32
- 194.186.207.124/32
- 194.186.207.182/32
- 195.8.62.178/32
- 92.38.2.37/32

Яндекс.Телемост

- 37.140.128.0/18
- 37.9.64.0/18
- 5.255.192.0/18
- 5.45.192.0/18
- 37.9.127.0/25
- 5.255.192.0/25
- 5.255.252.0/25
- 37.9.123.192/31
- 5.255.192.176/31
- 5.255.230.32/31

Более подробная информация по настройке Телемоста в корпоративной сети представлена по ссылке.

Обратный прокси

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Обратный прокси**: `ideco-reverse-backend`.

Список служб для других разделов доступен по ссылке.

Технология обратного прокси позволяет перенаправлять веб-трафик из интернета в локальную сеть. Отличия от DNAT:

- Работает на более высоком уровне (используются прикладные протоколы HTTP/HTTPS вместо сетевого протокола IP).
- Позволяет гибко реализовывать публикацию ресурсов.
- Предоставляет дополнительные функции безопасности.
- Позволяет эффективнее управлять трафиком.

Таким образом, имея одну ресурсную A-запись для внешнего сетевого интерфейса Ideco NGFW Novum, можно опубликовать несколько ресурсов в локальной сети, распределив их по нескольким входящим URL.

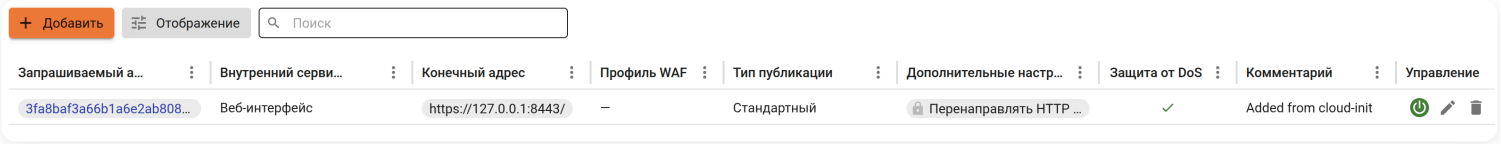
Для публикуемых ресурсов сертификаты не требуют ручной загрузки, Ideco NGFW Novum автоматически отправляет запрос на выпуск сертификата Let's Encrypt. Выпуск сертификата может занять до 20 минут. Сертификаты будут доступны в одноименном разделе.

Создание и настройка правила

Для добавления нового правила:

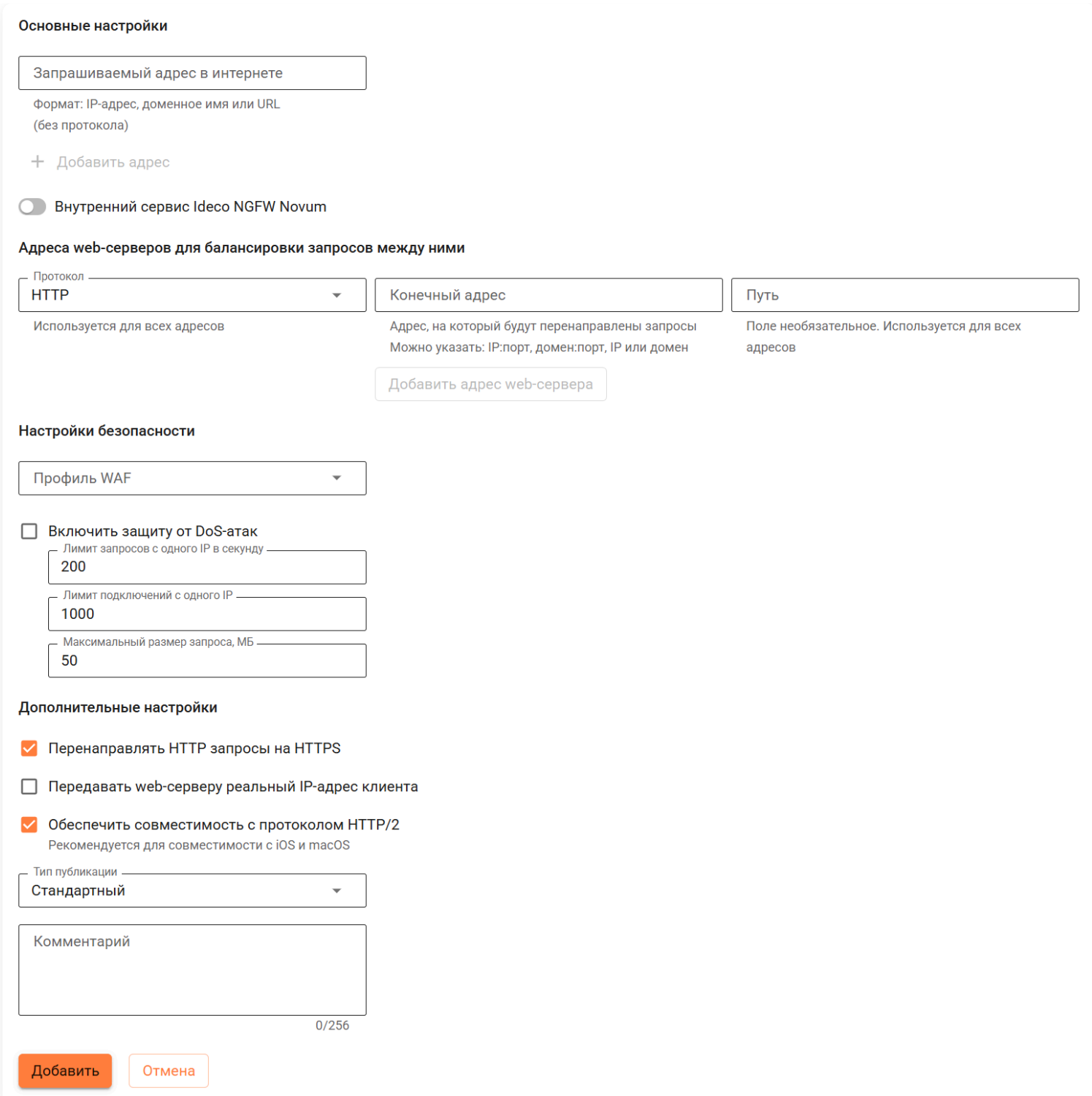
1. Перейдите в раздел **Сервисы → Обратный прокси**.

2. Нажмите **Добавить**:



Форма добавления правила разделена подразделы:

- **Основные настройки**.* **Адреса web-серверов для балансировки запросов между ними**.
- **Настройки безопасности**.
- **Дополнительные настройки**:



Основные настройки

- **Запрашиваемый адрес в интернете** - укажите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями из интернета. Для добавления дополнительных (альтернативных) адресов нажмите кнопку **Добавить адрес**.

При добавлении нескольких правил с одинаковыми значениями в поле **Запрашиваемый адрес в интернете** сработает только одно из созданных правил.

Если требуется опубликовать несколько ресурсов на одном и том же адресе, необходимо указать разные пути после основного IP-адреса/доменного имени/URL.

Пример. Чтобы опубликовать на IP-адресе `192.168.11.1` личный кабинет и почту, при создании правил в поле **Запрашиваемый адрес в интернете** укажите значения:

- Для личного кабинета - `192.168.11.1/cabinet`.

- Для почты - `192.168.11.1/mail`.

- **Внутренний сервис Ideco NGFW Novum** - включите опцию и выберите для публикации один из сервисов Ideco NGFW Novum: Личный кабинет/Портал SSL VPN, Веб-интерфейс или Почта.

Web-серверы для балансировки запросов

- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Конечный адрес** - адрес, на который будут перенаправлены запросы.
- **Путь** - необязательное поле, дописывает путь после **Конечный адрес**.

Если указать в поле **Запрашиваемый адрес в интернете** ***0.0.0.0***, перенаправление будет работать со всех внешних IP-адресов Ideco NGFW Novum на адрес из поля **Конечный адрес**.

Чтобы перенаправление работало с доменов Ideco NGFW Novum на адрес из поля **Конечный адрес**, необходимо явно указать домены в поле **Запрашиваемый адрес в интернете**.

Настройки безопасности

- **Профиль WAF** - позволяет задать параметры защиты веб-ресурса при указании WAF-профиля.
- **Включить защиту от DoS-атак** - опция ограничивает трафик на публикуемый ресурс. Параметры:
  - **Лимит запросов с одного IP в секунду** - от 0 до 4 294 967 295, по умолчанию 200. При превышении будет отправлена ошибка 503 `Service Temporarily Unavailable`. Если число ошибок равно 6 в течение 10 минут, то IP-адрес будет заблокирован на 40 минут. Значение 0 в поле означает, что ограничение по параметру не применяется.
  - **Лимит подключений с одного IP** - от 0 до 65 536, по умолчанию 1000. При превышении будет отправлена ошибка 503 `Service Temporarily Unavailable`. Если число ошибок равно 6 в течение 10 минут, то IP-адрес будет заблокирован на 40 минут. Значение 0 в поле означает, что ограничение по параметру не применяется.
  - **Максимальный размер запроса, МБ** - от 1 до 51 200, по умолчанию 50. Попытка отправить файл или другие данные большего объема приведет к ошибке 413 `Request Entity Too Large`.

При превышении лимита запросов с одного IP или подключений с одного IP после ошибки 503 может возникнуть ошибка `Connection Refused`. Такое поведение является нормальным и ожидаемым результатом совместной работы Nginx и `Fail2Ban`. Эти два механизма работают на разных уровнях сетевого стека и с разной скоростью реагирования.

Пример 1. Настройка строгой защиты от DoS-атак

Защита внутренних административных панелей или критичных API:

- **Лимит запросов с одного IP в секунду** - 50.
- **Лимит подключений с одного IP** - 100.
- **Максимальный размер запроса, МБ** - 10.

Низкие лимиты блокируют атаки, малый размер запроса ограничивает объем данных.

Пример 2. Настройка мягкой защиты от DoS-атак

Публичные API, CDN, сервисы с легитимной высокой нагрузкой:

- **Лимит запросов с одного IP в секунду**: 1000.
- **Лимит подключений с одного IP**: 5000.
- **Максимальный размер запроса, МБ**: 200.

Повышенные лимиты позволяют обрабатывать легитимный трафик, при этом сохраняется защита от явных атак. Увеличенный размер запроса поддерживает загрузку файлов.

Дополнительно

- **Перенаправлять HTTP-запросы на HTTPS** - опция используется, если сайт работает только по протоколу HTTPS. Если опция выключена, посетители, обратившиеся к сайту по HTTP, могут быть потеряны.

Если в поле **Запрашиваемый адрес в интернете** указан URL с путем (например: `example.com/path` или `192.168.111.13/cabinet`), то при включении опции **Перенаправлять HTTP запросы на HTTPS** добавляйте `/` в конец URL (например: `http://example.com/path/` или `192.168.111.13/cabinet/`). Без `/` будет ошибка 404. При использовании HTTPS `/` необязателен.

- **Передавать web-серверу реальный IP-адрес клиента** - при включенной опции для web-сервера передается публичный IP-адрес клиента. Если опция выключена, передается IP-адрес Ideco NGFW Novum. При этом IP-адрес клиента возможно узнать через специальные заголовки в запросах на проксируемые серверы (например, `proxy_set_header X-Forwarded-For $remote_addr`).

> **Web Application Firewall (WAF)** анализирует запросы к сайту и блокирует атаки на уязвимые компоненты веб-приложения (например типы атак OWASP TOP-10). При активации этого модуля также будут блокироваться злоумышленники, ведущие сканирование сайта на уязвимости, с помощью модуля защиты от брутфорс-атак.
>
> Не рекомендуем использовать проброс веб-интерфейса Ideco NGFW Novum через WAF, так как при попытке входа пользователь может быть заблокирован средствами WAF.

- **Обеспечить совместимость с протоколом HTTP/2** - при включении опции будут удалены заголовки `Upgrade`, `Proxy-Connection`, `Keep-Alive` и `Transfer-Encoding`, которые могут вызывать проблемы парсинга у клиентов, строго следующих спецификации `HTTP/2`. Например, встроенные сетевые библиотеки iOS/macOS.
- Поле **Тип публикации** позволяет выбрать один из типов: **Стандартный** или **Outlook Web Access**. Тип **Outlook Web Access** используется для публикации Microsoft Exchange.

В полях **Запрашиваемый адрес в интернете** и **Адрес в локальной сети** для типа **Outlook Web Access** укажите только домены `youdomain.ru` без остальной части URL (она не используется при публикации этим способом).

Если у вас имеется доверенный SSL-сертификат для домена, по которому будет идти обращение извне на публикуемый ресурс, то его можно загрузить в раздел **Сервисы** → **Сертификаты** с помощью кнопки **Добавить**.

Доменные имена, указываемые в поле **Запрашиваемый адрес в интернете**, должны переводиться во внешний IP-адрес сервера Ideco NGFW Novum. Доменные имена, указываемые в поле **Адрес в локальной сети**, должны переводиться в IP-адреса публикуемых ресурсов Ideco NGFW Novum.

> Чтобы исключить IP-адрес из обработки **Защитой от DoS-атак**, обратитесь в Техническую поддержку.

Публикация CMS

Нами протестирована и официально поддерживается публикация сайтов на двух популярных CMS: **Joomla** и **Wordpress**. Подробности публикации каждой CMS описаны ниже.

Joomla

Joomla в текущей реализации публикуется, если настроить перенаправление с внешнего домена на локальный домен без префикса:

- Ассоциировать с внешним адресом Ideco NGFW Novum дополнительное доменное имя специально для публикации Joomla: `joomla.mydomain.ru`.
- Настроить правило публикации `joomla.mydomain.ru` → `joomla.local:port` (порт не обязателен).

WordPress

WordPress в текущей реализации публикуется только в конфигурации, когда в WordPress и в обратном прокси настроен один и тот же домен:

- Для домена компании добавить A-запись `wordpress.mydomain.ru`, указывающую на внешний IP-адрес Ideco NGFW Novum.
- В админ-панели WordPress локального сервера должен быть настроен домен `wordpress.mydomain.ru` на стандартном порту HTTP.
- Добавить в обратный прокси правило публикации `wordpress.mydomain.ru` → `wordpress.mydomain.ru`.

Публикация Nextcloud

Для корректной работы Nextcloud с устройствами Apple добавьте в конфигурацию Nginx следующие строки:

```
location /.well-known/carddav {
    return 301 $scheme://$host/remote.php/dav;
}

location /.well-known/caldav {
    return 301 $scheme://$host/remote.php/dav;
}

location ^~ /.well-known {
    return 301 $scheme://$host/index.php$uri;
}
```

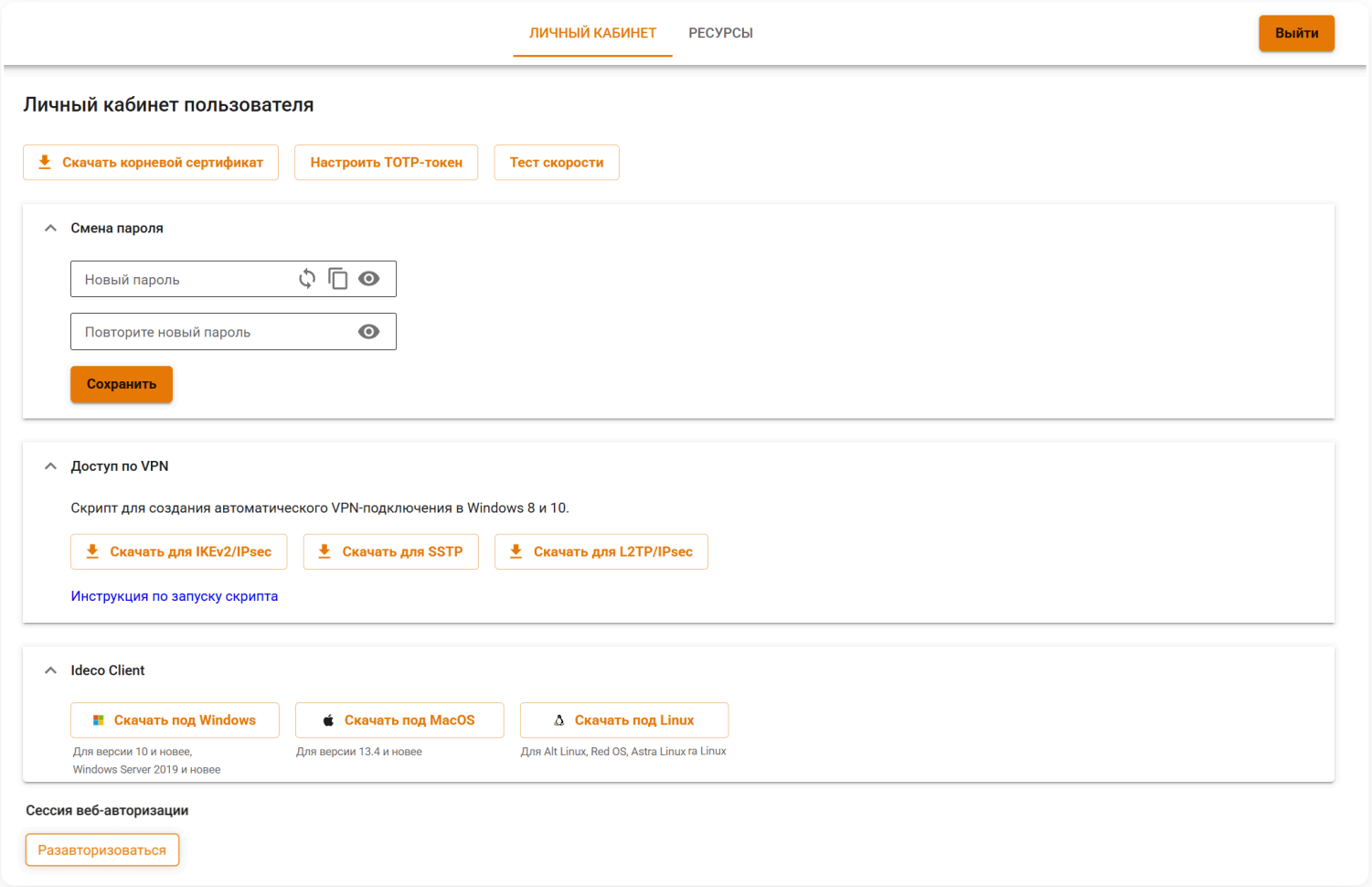
При использовании NGINX Proxy Manager добавьте в **Custom Nginx Configuration** → **Advanced Settings** запись `proxy_hide_header Upgrade;`, иначе мобильные устройства от Apple будут получать сообщение об ошибке **Connection Closed**.

ЛК/Портал SSL VPN

Классический контекст | Высокопроизводительный контекст | API

Портал SSL VPN предоставляет удаленным пользователям безопасный доступ к внутренним ресурсам, выступая в роли защищенной точки входа в корпоративную сеть.
Возможности личного кабинета Ideco NGFW Novum:

- **Скачивание корневого сертификата**.
- **Генерация TOTP-токена**. Для настройки двухфакторной аутентификации воспользуйтесь статьей.
- **Тестирование скорости**. При нажатии на Тест скорости откроется меню тестирования скорости между хостом и NGFW Novum.
- **Смена пароля**.
- **Скачивание скриптов для создания автоматического VPN-подключения в Windows 8 и 10**. Будут доступны скрипты настройки только тех типов подключения, которые указаны для пользователя в таблице **Доступ по VPN** в разделе **Пользователи → VPN-подключения**.
- **Скачивание Ideco Client**. Подробнее о работе в Ideco Client - в статье.
- **Деавторизация**. Деавторизация пользователя в сети NGFW Novum, если пользователь был авторизован через Web/SSO.



Поддерживаемые версии браузеров:

- Google Chrome версия 109 и выше
- Firefox версия 115 и выше
- Safari версия 15.4 и выше

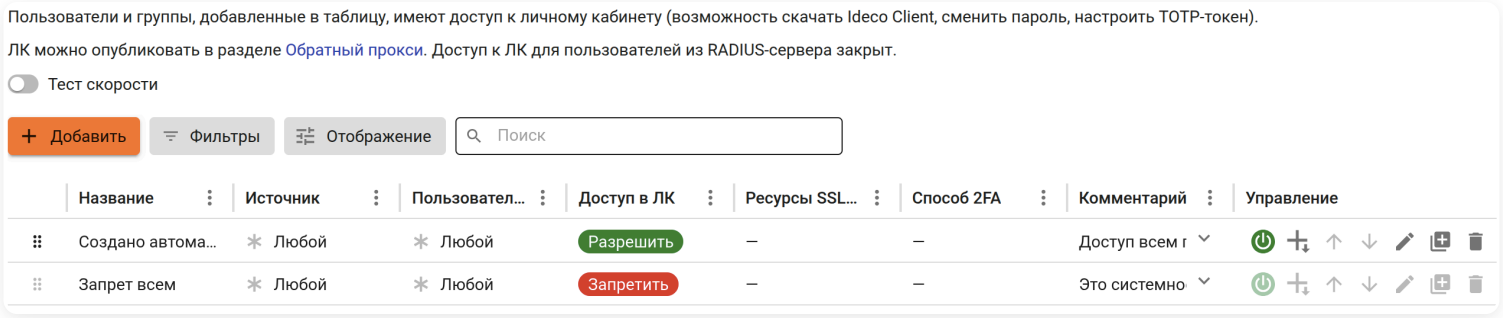
Настроить доступ пользователей в личный кабинет можно в **Сервисы** → **ЛК/Портал SSL VPN** → **Правила доступа**. Для этого необходимо создать **Правило доступа**, а затем опубликовать личный кабинет через **Обратный прокси**, чтобы пользователи получили к нему доступ. VPN-подключение не требуется, пользователь авторизуется через логин и пароль.

Настройка доступа в личный кабинет Ideco NGFW Novum

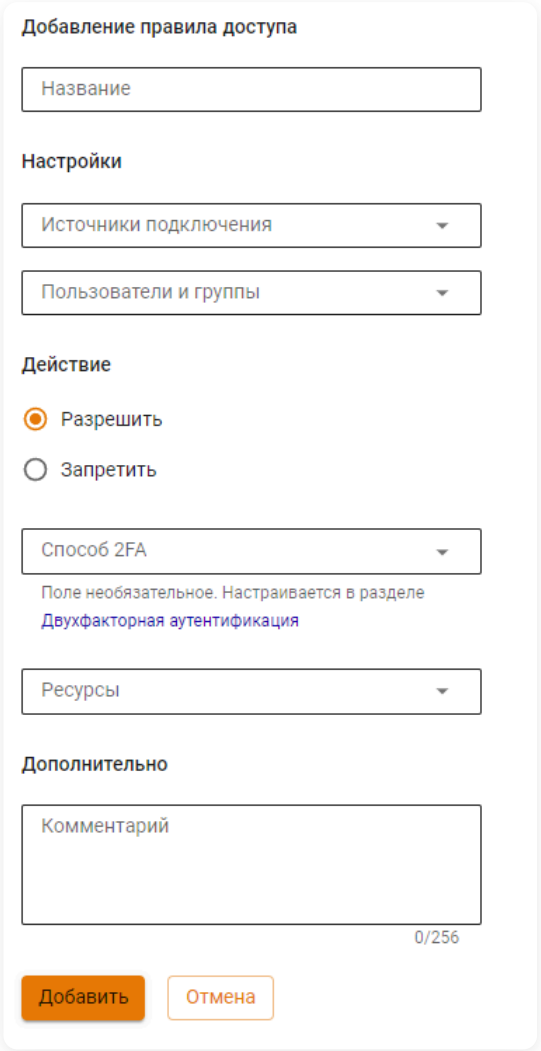
В разделе **Сервисы** → **ЛК/Портал SSL VPN** можно настроить доступ в личный кабинет.

Правила доступа

По умолчанию в таблице настроено правило доступа к личному кабинету для всех пользователей:



Для создания правила нажмите **Добавить** и заполните необходимые поля:



Расшифровка полей

- **Название** - укажите название правила доступа.
- **Источники подключения** - укажите IP-адреса, подсети, страны или домены.
- **Пользователи и группы** - выберите пользователей, группы пользователей, группы безопасности из AD, которым хотите предоставить доступ в личный кабинет.

- **Способ 2FA** - выберите метод двухфакторной аутентификации. Поле может быть пустым.
- **Ресурсы** - укажите необходимые ресурсы, созданные в **ЛК/Портал SSL VPN** → **Ресурсы**. Поле может быть пустым.
- **Комментарий** - произвольный текст, не более 256 символов.

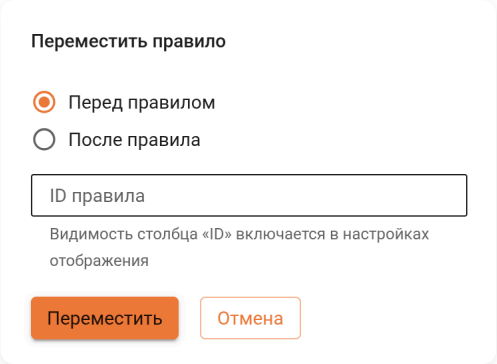
Если у пользователей приватные (серые) IP-адреса, не указывайте в качестве источника страну. Это связано с тем, что такие адреса не относятся к диапазонам IP-адресов ни одной страны и доступ к ним будет запрещен. Рекомендуется использовать диапазон IP-адресов.

Для перемещения правил выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

При наличии большого количества правил доступа в таблице воспользуйтесь кнопкой **Фильтры**.

Как обрабатываются правила:

1. При входе пользователя в ЛК правила проверяются сверху вниз до первого совпадения по полям **Источник** и **Пользователи и группы**.

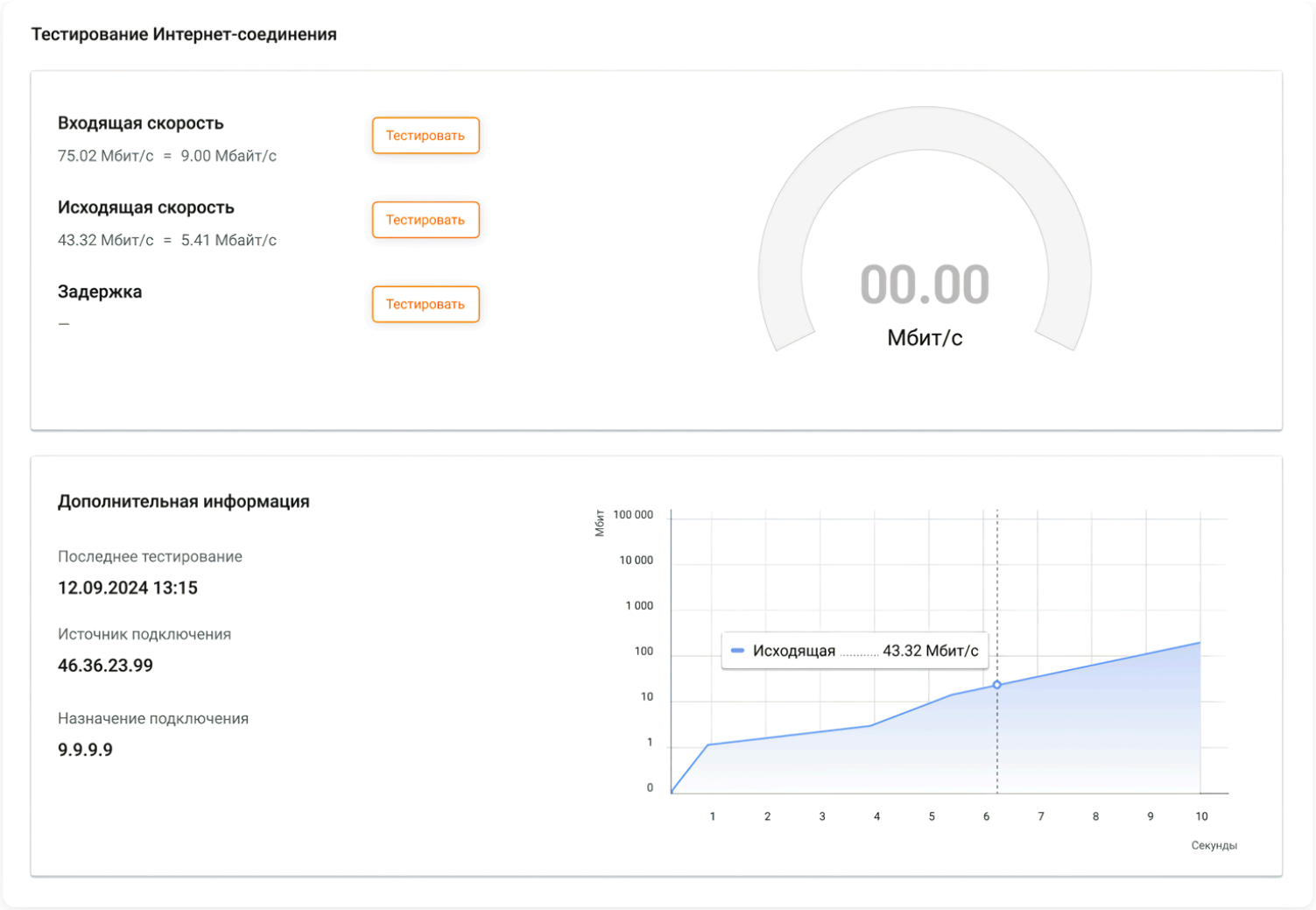
2. Если правило разрешающее, то доступные пользователю в ЛК ресурсы определяются этим правилом. Последующие правила с такими же полями учитываться не будут.

3. Доступ пользователя или группы пользователей к ресурсу определяется заново при изменении таблицы, пользователей и состава групп.

Тест скорости

Опция **Тест скорости** позволяет добавить в личный кабинет функцию проверки скорости интернет-соединения.

В **Тестирование интернет-соединения** пользователь может проверить входящую и исходящую скорость интернет-соединения, а также задержку (ping):



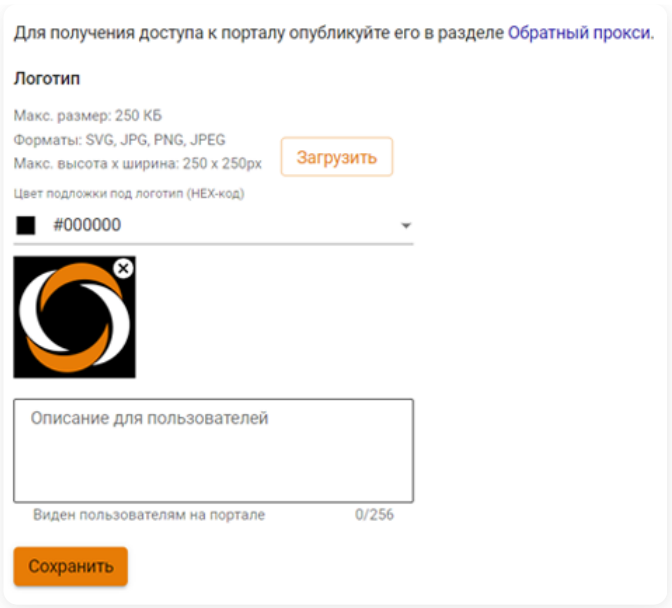
- **Последнее тестирование** - дата и время любого последнего теста.
- **Источник подключения** - IP-адрес пользователя.
- **Назначение подключения** - IP-адрес NGFW Novum.

Особенности работы:

- Продолжительность каждого теста составляет 10 секунд.
- Тесты запускаются последовательно, в каждый момент времени может быть активен только один тест.
- График обнуляется в момент запуска нового теста.

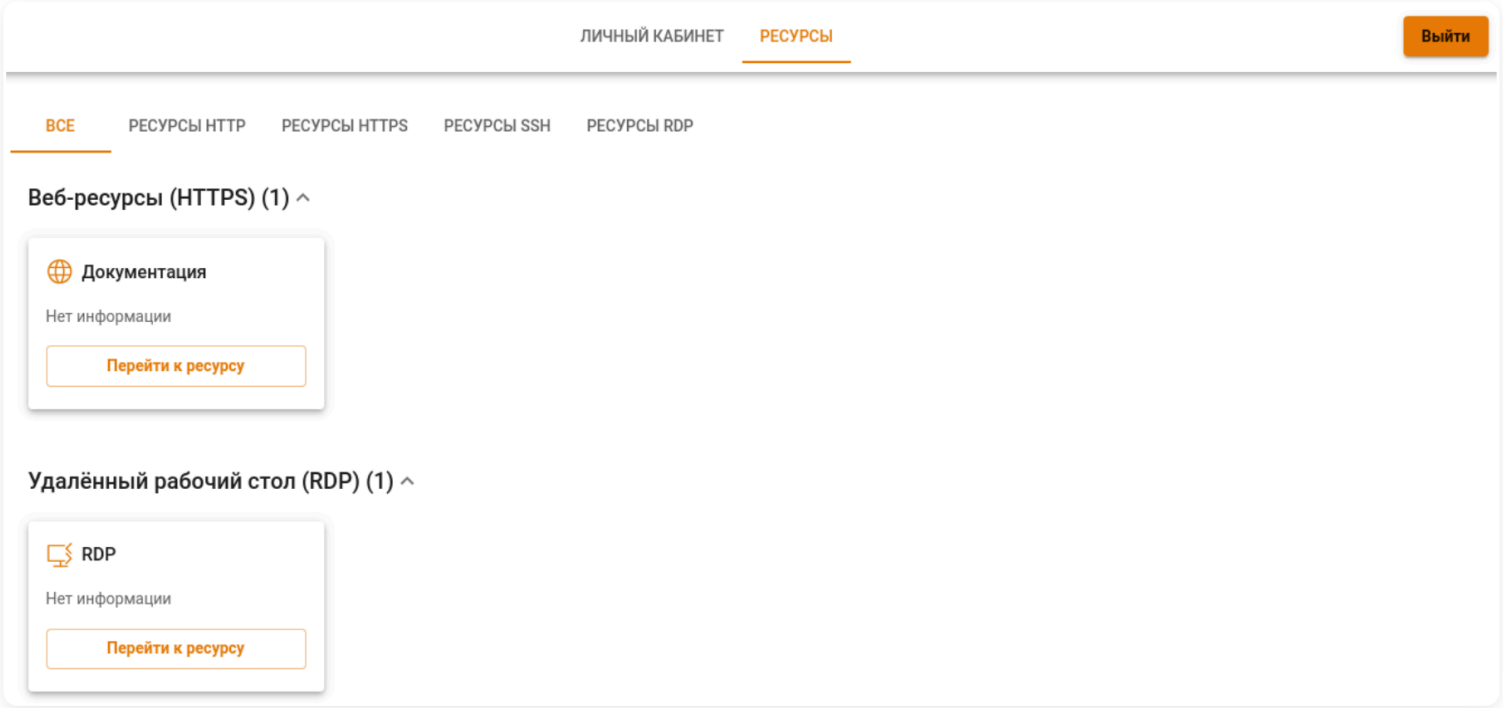
Внешний вид

На вкладке можно настроить внешний вид портала: изменить логотип и добавить описание, которое отображается рядом с логотипом:



Ресурсы

В личном кабинете Ideco NGFW Novum размещаются только внутренние ресурсы, доступные из локальной сети NGFW Novum. Ресурсы становятся доступны пользователям только после успешной авторизации и при наличии соответствующего разрешения в правилах доступа:

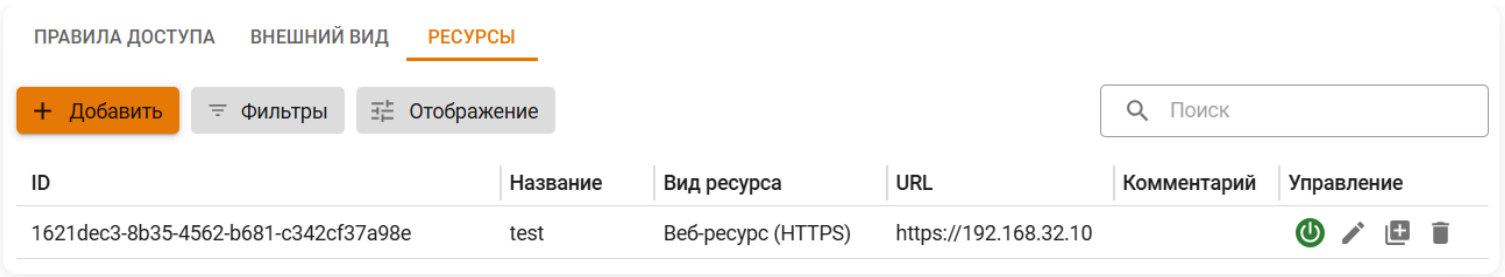


Веб-ресурсы HTTP(S) в SSL VPN работают по принципу **Обратного прокси** ЛК/SSL VPN.

Требования к URL в HTML-коде страниц веб-ресурсов HTTP(S) в ЛК/SSL VPN

URL, которые содержатся в HTML-коде веб-страниц публикуемого внутреннего ресурса (ссылки, картинки, скрипты, стили и т.д.), должны соответствовать одному из требований:

- URL относительные, не зависят от домена и пути. В этом случае браузер дополнит ссылки до полных с учетом домена и пути публикации ЛК.
- URL изначально доступны через интернет. Например, CDN для скриптов и картинок, которые используются ресурсом. Если URL ведут на внешние сайты, то трафик пойдет не через NGFW Novum.
- URL учитывают, что сайт публикуется через ЛК по определенному пути - `https://<домен_порт_публикации_ЛК>/<путь_публикации_ЛК>/resources/<resource_id>/..`. Идентификатор ресурса (`resource_id`) используется для публикации ресурса в ЛК, доступен для просмотра в столбце ID на вкладке **Ресурсы**. По умолчанию столбец в таблице не указан, можно настроить с помощью кнопки **Отображение**:

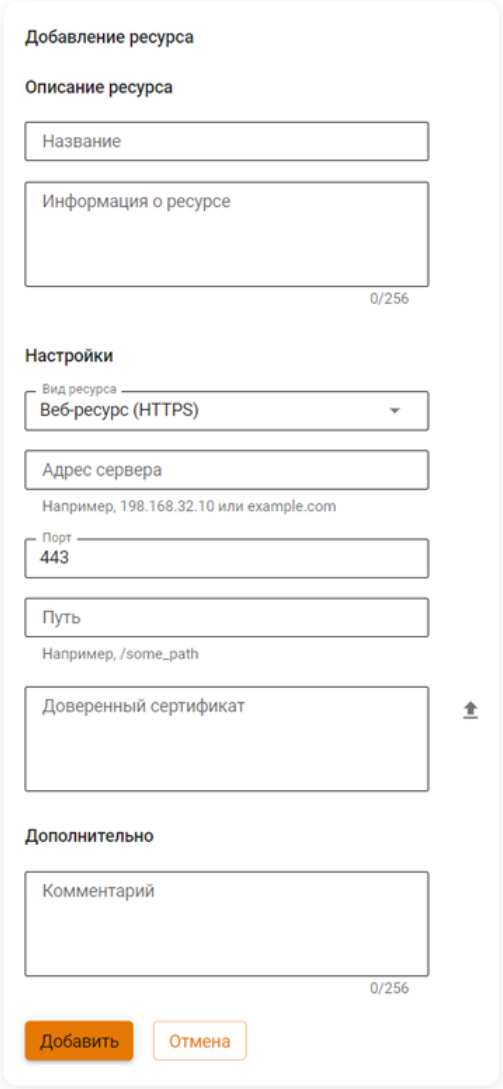


В случае несоответствия URL перечисленным требованиям публикуемый ресурс будет отображаться некорректно, т.к. браузер пользователя не сможет получить некоторые данные с этих URL (например, файлы CSS и JS).

Пример. Личный кабинет опубликован по адресу `example.com/site`, доступен ресурс HTTPS с ID `123`. Адрес, по которому пользователь переходит к ресурсу в личном кабинете - `https://example.com/site/resources/123/`. URL, которые соответствуют требованиям:

- Относительный URL `mysite/main/index.html`. Браузер дополняет ссылку до `https://example.com/site/resources/123/mysite/main/index.html`.
- Абсолютный URL `https://example.com/site/resources/123/mysite/pictures/image.png`. Публикуемый ресурс распознает опубликованные домен и путь, сразу формирует полную ссылку.

Чтобы добавить ресурс, перейдите в **Сервисы** → **ЛК/Портал SSL VPN** → **Ресурсы**, нажмите **Добавить** и заполните поля:



Расшифровка полей

Описание ресурса:

- **Название** - имя ресурса, может содержать до 42 символов.
- **Информация о ресурсе** - укажите текстовое описание, которое будет отображаться в личном кабинете, или оставьте поле пустым.

Настройки:

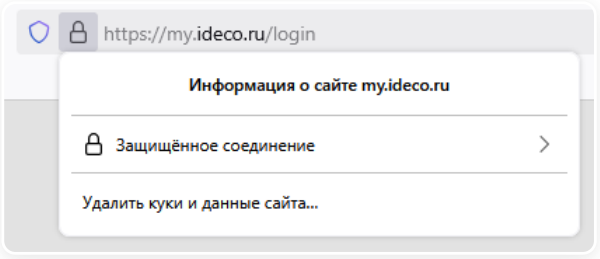
- **Вид ресурса** - **Веб-ресурс (HTTPS)**:

    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `443`.
    - **Путь** - укажите путь. Поле не является обязательным.
    - **Доверенный сертификат** - загрузите доверенный сертификат. Поле не является обязательным.
- **Вид ресурса** - **Веб-ресурс (HTTP)**:
    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `80`.
    - **Путь** - укажите путь. Поле не является обязательным.
- **Вид ресурса** - **Удаленный доступ (SSH)**:
    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `22`.
    - **Отпечаток ключа** - загрузите отпечаток ключа.
- **Вид ресурса** - **Удаленный рабочий стол (RDP)**:
    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `3389`.
- **Дополнительно:**
    - **Комментарий** - поле может быть пустым.

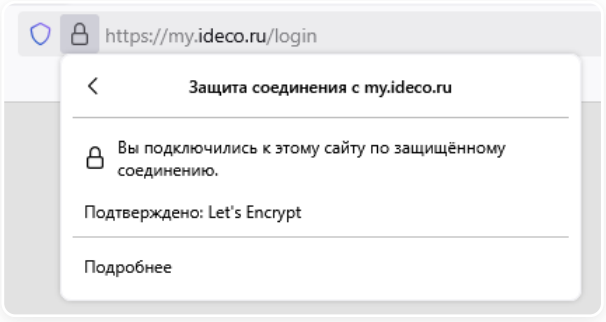
Где скачать доверенный сертификат

Пример скачивания сертификата в браузере Firefox:

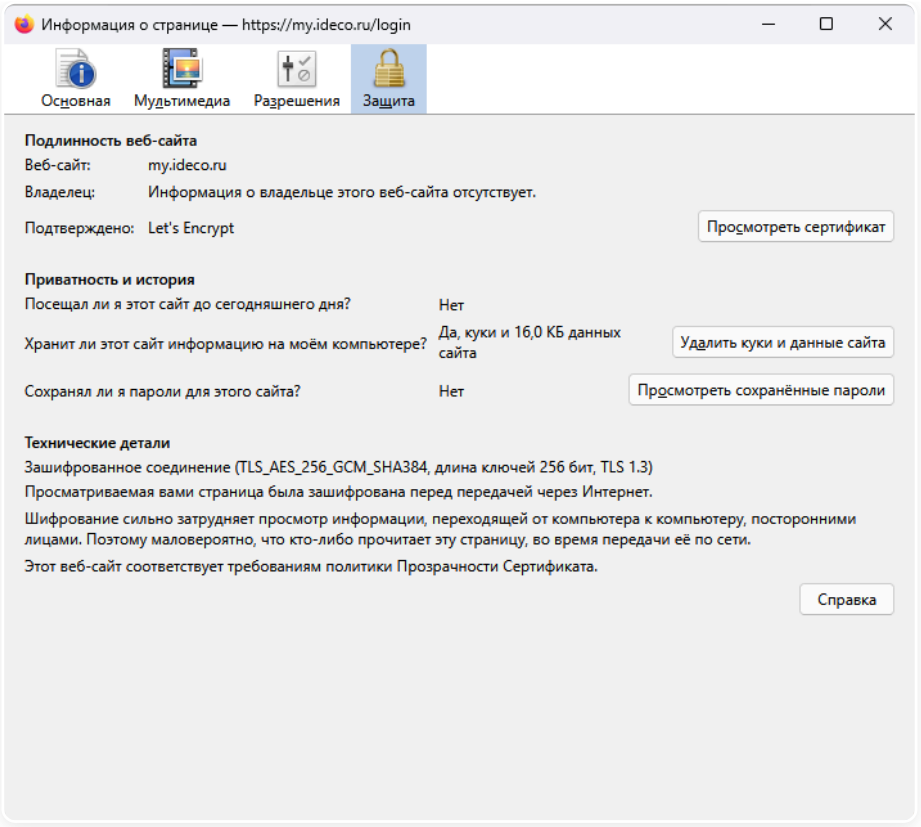
1. Нажмите в адресной строке браузера на значок с замком и выберите **Защищенное соединение**:



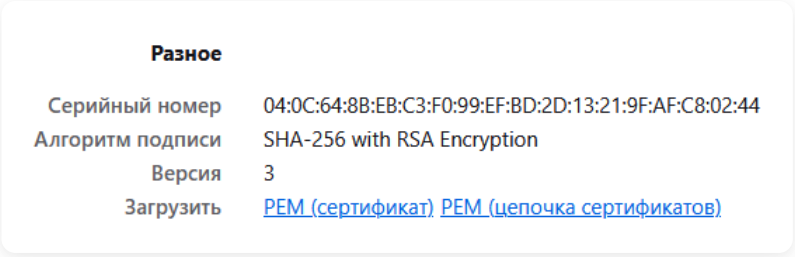
2. Нажмите **Подробнее**:



3. На вкладке **Защита** нажмите **Просмотреть сертификат**:



4. В разделе **Разное** скачайте сертификат из строки **Загрузить**:



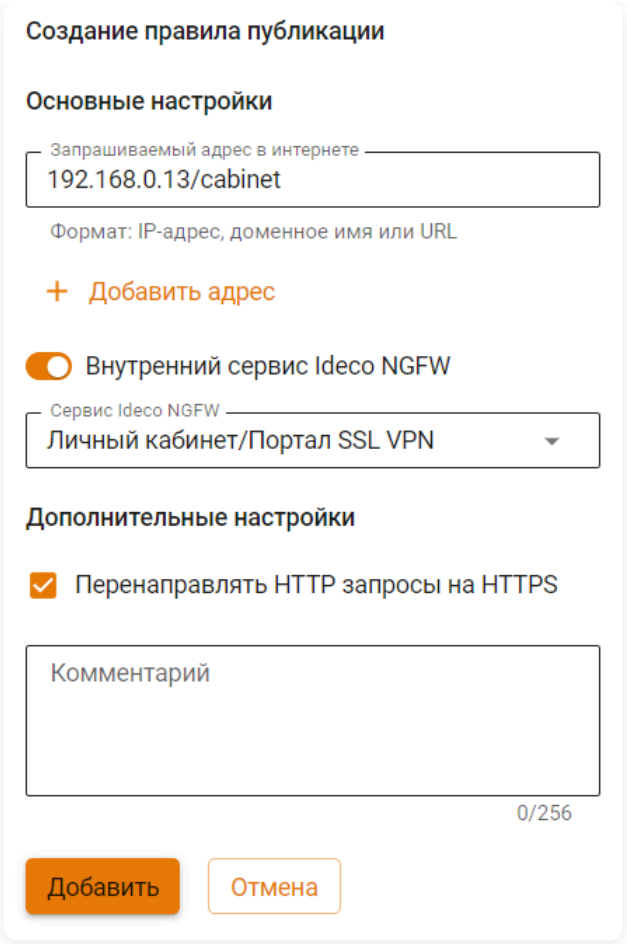
Адреса, на которые ссылается HTTP/HTTPS-ресурс, должны быть относительными во избежание нарушения CORS. Подробнее про CORS.

Публикация личного кабинета

Чтобы пользователи получили доступ в личный кабинет, он должен быть опубликован. Для публикации ЛК перейдите в **Сервисы** → **Обратный прокси** и выполните действия:

1. Нажмите **Добавить** и включите опцию **Внутренний сервис Ideco NGFW Novum**.

2. В поле **Запрашиваемый адрес в интернете** введите адрес, по которому хотите опубликовать личный кабинет:



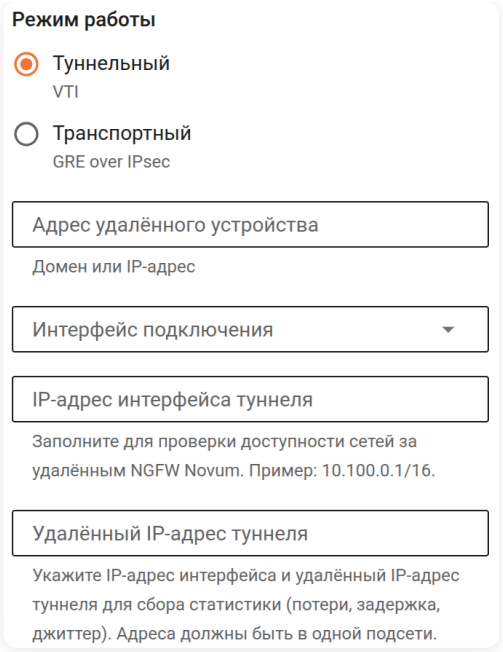
Чтобы система могла отличать личный кабинет от других ресурсов, опубликованных на данном адресе, следует указывать путь после основного IP-адреса/доменного имени/URL - например, `/cabinet`. Это обеспечивает корректную маршрутизацию. Подробнее - в статье.

3. Включите опцию **Перенаправлять HTTP-запросы на HTTPS**. Личный кабинет доступен только по HTTPS. При обращении по HTTP без перенаправления отобразится ошибка подключения.

Если в поле **Запрашиваемый адрес в интернете** указан URL с путем (например: `example.com/path` или `192.168.111.13/cabinet`), то при включении опции **Перенаправлять HTTP запросы на HTTPS** добавляйте `/` в конец URL (например: `http://example.com/path/` или `192.168.111.13/cabinet/`). Без `/` будет ошибка 404. При использовании HTTPS `/` необязателен.

4. Нажмите **Добавить**.

5. Для доступа пользователей к ресурсам в личном кабинете, которые расположены на удаленном хосте за IPsec-туннелем, необходимо заполнить поля в IPsec для входящего и исходящего подключения:



- **IP-адрес туннельного интерфейса** - укажите IP-адрес интерфейса туннеля на сервере, через который требуется получить доступ к ресурсам.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля на удаленном сервере, к ресурсам которого требуется получить доступ.

После этого пользователь сможет зайти в личный кабинет по логину и паролю либо через авторизацию в сети NGFW Novum.

Вход в личный кабинет Ideco NGFW Novum

Личный кабинет пользователя будет доступен по ссылке, указанной при публикации через **Обратный прокси**.

Чтобы зайти в личный кабинет, выполните действия:

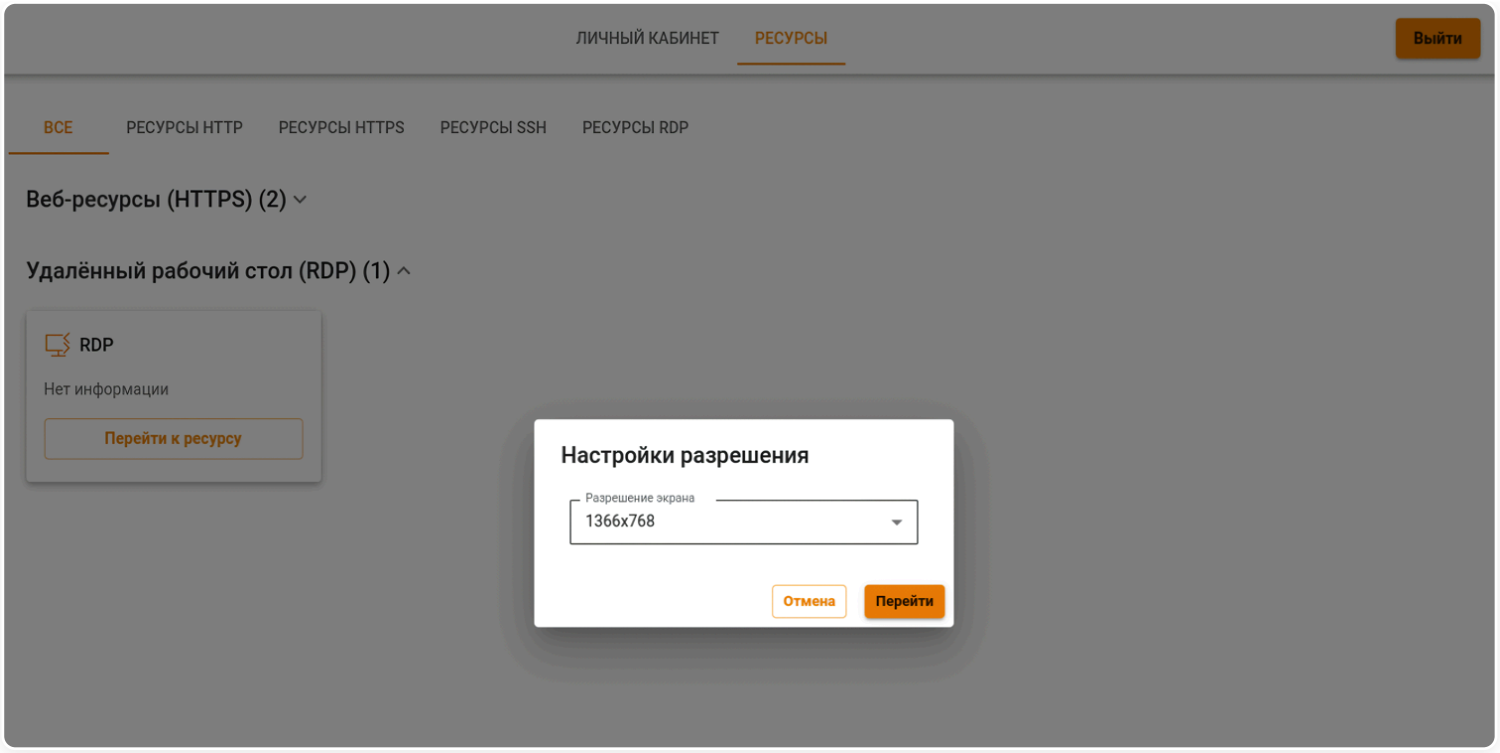
1. Перейдите по ссылке, указанной в правиле публикации личного кабинета.

2. В открывшейся форме авторизации введите логин и пароль пользователя.

Если пользователь уже авторизован в сети NGFW Novum, то логин и пароль вводить не потребуется, личный кабинет откроется сразу.

Настройка разрешения экрана

При подключении пользователя к ресурсу через удаленный рабочий стол (RDP) доступен выбор разрешения экрана:



Доступные настройки разрешения:

- 1920x1080
- 1366x768 (по умолчанию)
- 1024x768

DNS

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **DNS**: `ideco-dns-backend`, `unbound`, `nsd`, `unbound-anchor`, `unbound-keygen`, `ideco-dns-dnstap-reader`.

Список служб для других разделов доступен по ссылке.

Настройка выполняется в **Сервисы** → **DNS** на вкладках:

- **Внешние DNS-серверы** - позволяют указать DNS-серверы во внешних сетях, через которые будут разрешаться доменные имена, запрашиваемые из локальных сетей.
- **Forward-зоны** - позволяют указать сторонние DNS-серверы (в локальных или внешних сетях относительно NGFW) с указанием конкретных DNS-зон, которые эти серверы обслуживают. Перечисленные возможности DNS-сервера могут использоваться одновременно.
- **Master-зоны** - позволяют настроить полнофункциональный DNS-сервер, разрешающий имена в IP-адреса сетевых устройств в локальной сети.
- **DDNS** - обеспечивает доступ по доменному имени к устройствам с изменяющимся IP-адресом. В Ideco NGFW реализован через интеграцию с хостингом RU-CENTER.

При наличии большого количества Forward- и Master-зон в таблицах воспользуйтесь кнопкой **Фильтры**.

Полезные ссылки

- **Интеграция NGFW и SkyDNS**
- **Подключение через Ideco Client к внутреннему DNS**
- **Пример настройки Forward-зоны**

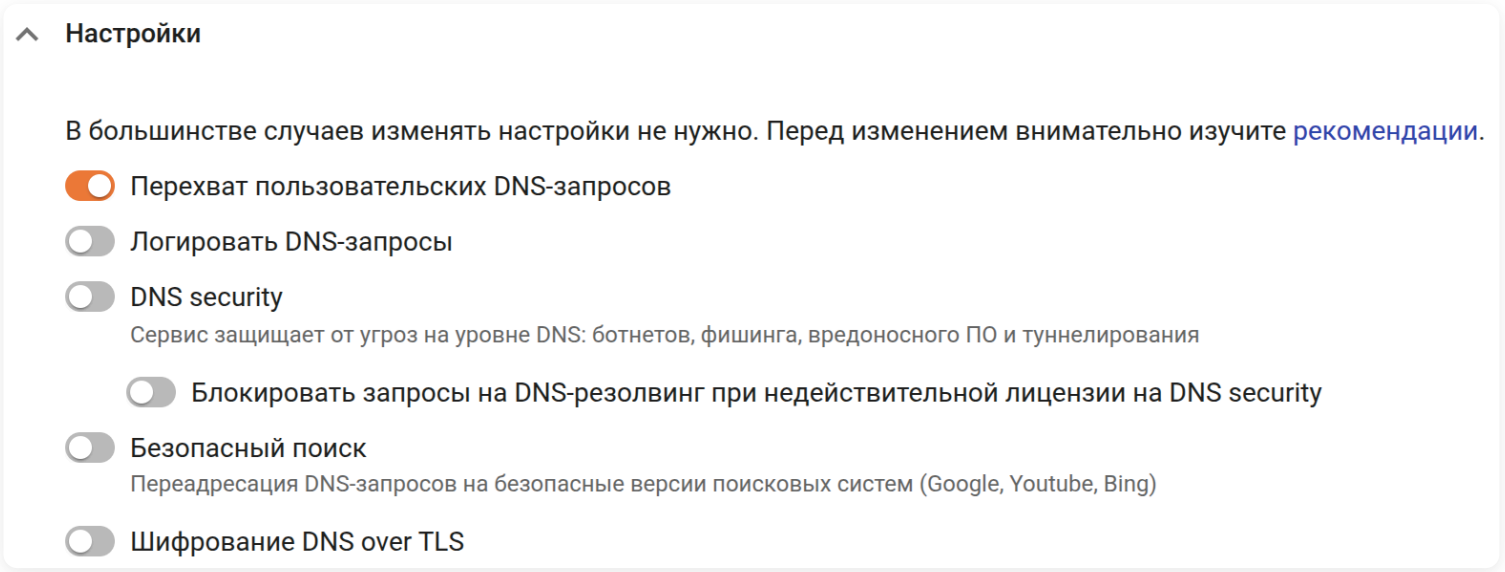
Внешние DNS-серверы

Классический контекст | Высокопроизводительный контекст

По умолчанию внешние DNS-серверы не указаны, и сервер разрешает имена в интернете, используя корневые DNS-серверы. В большинстве случаев изменять настройки не требуется.

Настройки

При необходимости измените настройки работы с внешними DNS-серверами:



Перехват пользовательских DNS-запросов

Включите опцию, чтобы все DNS-запросы пользователей принудительно направлялись на NGFW Novum, даже если на рабочей станции настроен другой DNS-сервер. **Перехват пользовательских DNS-запросов** позволяет контролировать защиту и функциональность DNS централизованно и независимо от потенциально вредоносных настроек.

Для VPN-пользователей опция **Перехват пользовательских DNS-запросов** будет работать только если в настройках VPN включена опция **Отправлять весь трафик на Ideco NGFW Novum**.

Включение перехвата пользовательских DNS-запросов блокирует использование DNS-over-TLS (DoT), DNS-over-QUIC (DoQ) и DNS-over-HTTPS (DoH) для трафика между пользователями и NGFW Novum.

При включенной опции **Перехват пользовательских DNS-запросов** трафик обрабатывается не как FORWARD, а как INPUT. Поэтому для корректной фильтрации трафика модулями **Контроль приложений** создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

Безопасный поиск

При резолвинге NGFW Novum будет возвращать адреса поисковых систем (Google, Youtube, Bing) с включенной фильтрацией нежелательного контента.

Шифрование DNS over TLS (DoT)

Опция включает шифрование DNS-запросов и ответов между NGFW Novum и DNS-сервером с помощью протокола TLS (порт 853). Опция работает только для DNS-серверов, указанных в разделе **Внешние DNS**, и не работает для серверов в FORWARD-зонах, а также корневых серверов. При этом:

- Никто не сможет перехватить и прочитать, какие сайты посещает клиент.
- Никто не сможет изменить DNS-ответ и перенаправить клиента на мошеннический сайт.

Необходимо учитывать, что шифрование добавляет дополнительный слой обработки, что может влиять на скорость резолвинга доменов.

Логировать DNS-запросы

Опция фиксирует обращения к DNS-серверам, которые проходили через Ideco NGFW Novum. Работает при указании адреса NGFW Novum как DNS-сервера либо при включенной опции **Перехват пользовательских DNS-запросов**. События отображаются в журнале DNS-запросы. Настройка полезна для отслеживания и анализа обращений к DNS-серверам, диагностики проблем с доступом к веб-ресурсам или мониторинга использования конкретных доменных имен.

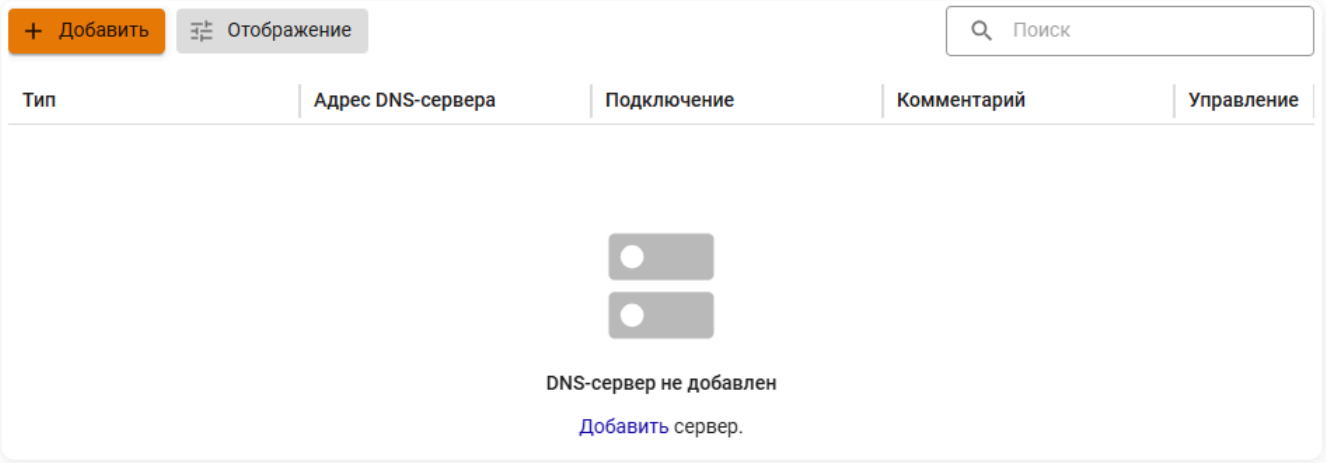
DNS security

Подробная информация в статье DNS security.

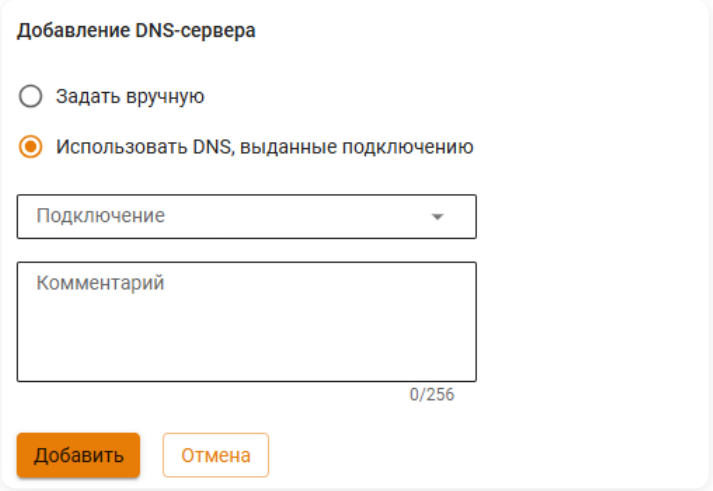
Рекомендации

- В Ideco NGFW Novum встроен кеширующий DNS-сервер. Рекомендуется использовать кеширующий DNS-сервер в качестве DNS-сервера для локальной сети, указав IP-адрес Ideco NGFW Novum в качестве DNS-сервера пользователям.
- Если интернет-провайдер или вышестоящее устройство блокирует DNS-запросы, то использование стандартной конфигурации с корневыми серверами невозможно. Рекомендуем задать серверы вручную или использовать DNS-серверы, выданные провайдером:

1. Нажмите **Добавить**:



2. Выберите **Задать вручную** или **Использовать DNS, выданные подключению**, указав нужное подключение:



- Не указывайте `8.8.8.8`, `1.1.1.1` или подобные известные DNS-серверы без необходимости. Ideco NGFW Novum справится с резолвингом самостоятельно.
- По возможности не используйте DNS, выданные интернет-провайдером, так как DNS, выданные интернет-провайдером, превышают TTL и долго отвечают. Ideco NGFW Novum настроит автоматически все необходимое для подключения к PPTP/L2TP через доменное имя. Если нужна особая внутренняя доменная зона провайдера, то создайте Forward-зону.
- Укажите фильтрующие DNS-серверы, если необходимо (SkyDNS или Яндекс-DNS).
- Не используйте DNS-серверы контроллера домена, даже если домен может самостоятельно разрешать доменные имена в интернете. Это необходимо для эффективного разрешения внутренних имен домена при интеграции с AD. Для резолвинга особых зон, не связанных с AD, создайте Forward-зону вручную.

Сторонние DNS-серверы для дополнительной фильтрации трафика

- SkyDNS при выключенном DNS-over-TLS `193.58.251.251`.
- SkyDNS при включенном DNS-over-TLS `193.58.251.10`.
- Yandex DNS `77.88.8.88`, `77.88.8.2`.
- Google DNS `8.8.8.8`, `8.8.4.4`.
- OpenDNS `208.67.222.222`, `208.67.220.220`, `208.67.222.220`, `208.67.220.222`.
- Cloudflare DNS `1.1.1.1`, `1.0.0.1`.

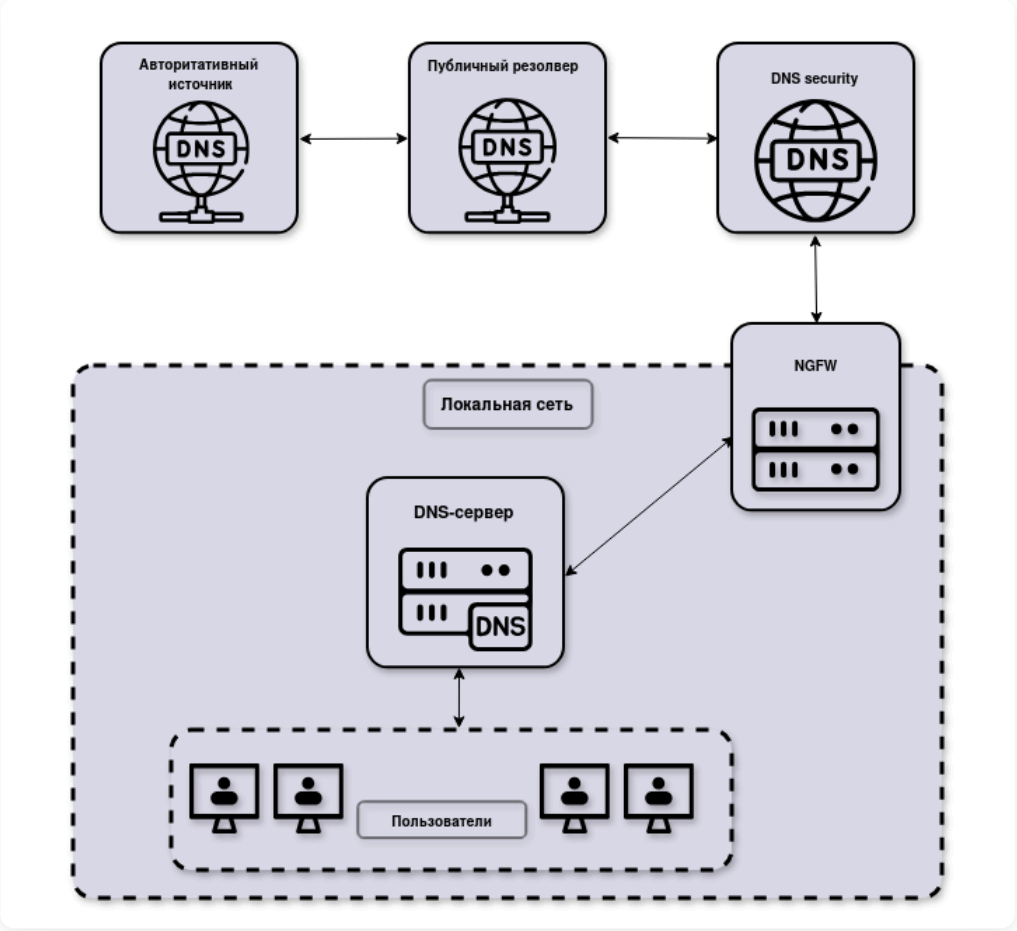
DNS security

Классический контекст | Высокопроизводительный контекст

Модуль должен быть включен в лицензию.

DNS Security - сервис, который защищает от угроз на уровне DNS: ботнетов, фишинга, вредоносного ПО, туннелирования и воровства данных.

Разрешение внешних DNS-доменов всегда работает через сторонние DNS-серверы в интернете. При включении опции **DNS security** облачный сервис выступает посредником между NGFW Novum и этими серверами. Схема DNS-трафика:



Использование функции защиты не делает функциональность NGFW Novum зависимой от интернета, но создает зависимость от облачной инфраструктуры. Отказоустойчивость и высокая доступность обеспечиваются за счет динамической маршрутизации BGP Anycast, которая автоматически направляет трафик к ближайшему доступному облачному узлу. Облачная инфраструктура распределена между узлами, расположенными на территории Российской Федерации.

Доступ к облаку предоставляется исключительно через зашифрованные соединения (DoT), что дополнительно усиливает безопасность.

Сервис **DNS security**:

- Позволяет предиктивно блокировать до 34% угроз на уровне DNS.
- Обеспечивает отказоустойчивость.
- Автоматически блокирует новые и подозрительные домены по мере их появления.
- Постоянно адаптируется к новым угрозам с помощью AI/ML-алгоритмов.
- Сокращает слепые зоны, защищая устройства без антивирусных агентов: промышленные контроллеры, датчики, камеры и офисную периферию.
- Автоматически обнаруживает и блокирует DNS-туннели за 5-10 минут, предотвращая эксфильтрацию данных.
- Блокирует переходы на зараженные сайты по фишинговым ссылкам еще до соединения.

- Автоматически реагирует на компрометацию сети, блокируя подозрительные соединения с C&C-серверами и домены, созданные алгоритмом (DGA).
- Шифрует DNS-запросы через DoH/DoT и использует DNSSEC, исключая перехват, подмену запросов и скрытые перенаправления.
- Обеспечивает глубокую аналитику DNS-трафика, ускоряет расследование инцидентов и снижает риск повторных атак.
- Не имеет доступа к приватной информации и не сохраняет ее.
- Не несет дополнительных рисков безопасности.
- Не вызывает значимой задержки или ухудшения работы.

Защита на уровне DNS выявляет и блокирует следующие угрозы:

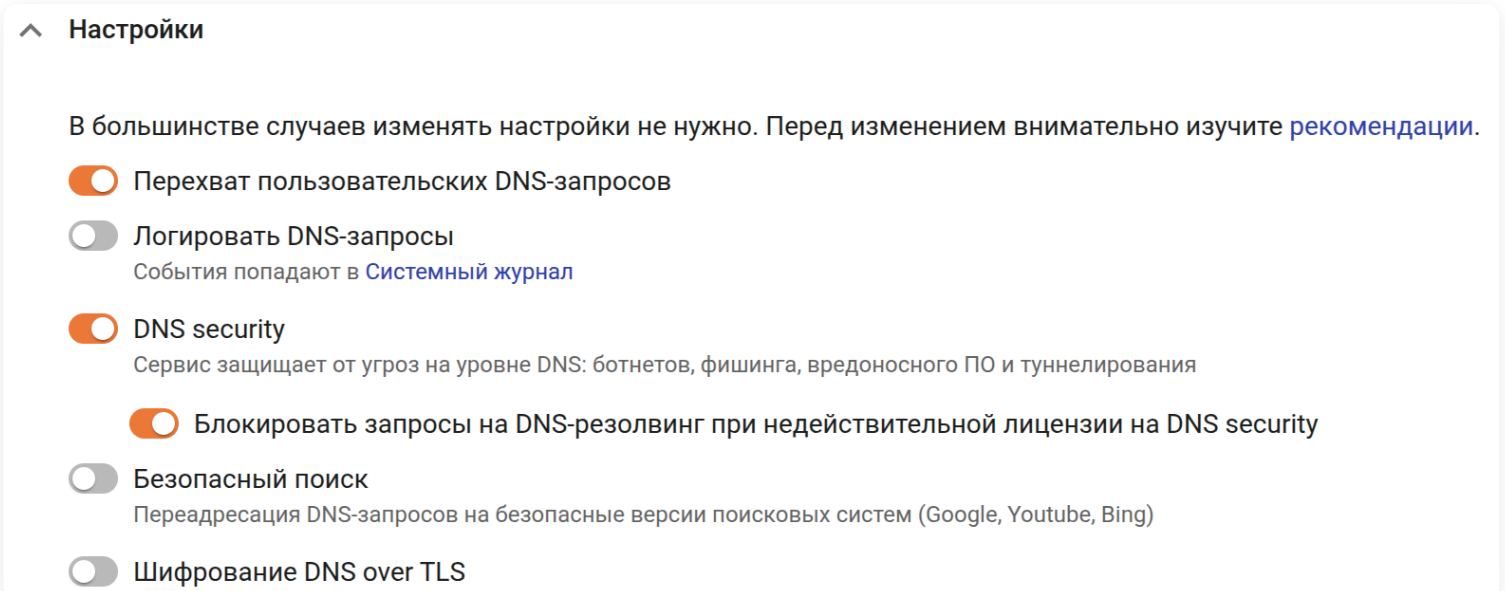
Типы угроз

Тип	Описание
DNS-туннелирование	Скрытая передача данных через DNS-запросы, используемая для кражи информации и управления зараженными системами
Недавно зарегистрированные домены	Домены, созданные менее 90 дней назад вручную или с помощью алгоритмов (DGA), которые не успевают попасть в базы угроз и воспринимаются как легитимные. Активно используются злоумышленниками для фишинга, построения C2-инфраструктуры и распространения вредоносного ПО
Botnets & C2	Распределенная сеть зараженных устройств, управляемых через командные и управляющие серверы (C2) для выполнения вредоносных действий
Cryptojacking	Скрытая атака, при которой ресурсы чужих устройств используются для майнинга криптовалюты без ведома владельца, что замедляет работу устройств и увеличивает энергопотребление
DGA	Алгоритм автоматической генерации доменных имен, используемых злоумышленниками для управления ботнетами, координации атак и распространения вредоносного ПО
Malware (Malicious Software)	Общее название для вредоносных программ, включая вирусы, трояны, шпионское ПО и ransomware, используемых для кражи данных, разрушения систем или получения удаленного доступа к устройствам
Phishing	Мошенничество через поддельные сайты, письма или сообщения с целью кражи логинов, паролей, данных карт или установки вредоносного ПО
Typosquatting	Регистрация доменов, похожих на легитимные, чтобы воспользоваться ошибками пользователей и похищать данные или показывать нежелательную рекламу
Ransomware	Вредоносное ПО, которое шифрует файлы жертвы и требует выкуп за их восстановление. Часто распространяется через фишинг или уязвимости, при этом оплата выкупа не гарантирует возврат данных
Запаркованные домены	Приобретенные, но неиспользуемые домены, которые могут применяться для фишинга, размещения вредоносного ПО или командных серверов злоумышленников

Настройка

1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы**.

2. Включите опцию **DNS Security**:



3. Включите опцию **Перехват пользовательских DNS-запросов** или укажите IP-адрес NGFW Novum как DNS-сервер на клиентских устройствах для фильтрации запросов.

4. Включите опцию **Блокировать запросы на DNS-резолвинг при недействительной лицензии на DNS security** для блокировки DNS-запросов в случае недействительной лицензии.

Важно

Если опция включена и лицензия недействительна:

- Доступ в интернет по доменным именам прекращается.
- Прямые подключения по IP-адресам продолжают работать.

При выключенной опции выполняется откат на обычный DNS-резолвинг без фильтрации **DNS Security**.

Результаты блокировки отображаются в столбце **Результат DNS Security** журнала **DNS-запросы**.

Отключите опцию **DNS Security**, если разрешение внешних доменов через интернет не требуется.

Особенности

При включении **DNS security**:

- Не будут использоваться заданные в таблице **Внешние DNS-серверы** или выданные провайдером DNS-серверы.
- Опция **Шифрование DNS over TLS** не имеет смысла, так как к соответствующим серверам подключений не будет.
- В браузере появится сообщение о недоступности ресурса при его блокировке.
- Если нужная запись есть в DNS-кеше NGFW Novum, резолвинг выполняется из кеша без обращения к облаку.

Если **DNS security** блокирует ресурс, который не должен быть заблокирован, обратитесь в Техническую поддержку.

При включении **DNS security** NGFW Novum обращается к адресу `193.58.251.10` на 853 TCP-порт. Убедитесь, что доступ не блокируется политиками безопасности.

Master-зоны

Классический контекст | Высокопроизводительный контекст

Master-зоны позволяют использовать Ideco NGFW Novum как сервер имен и переводить IP-адреса в доменные имена внутри сети.

DNS-сервер в Ideco NGFW Novum недоступен извне в целях безопасности. Для поддержки внешних DNS-зон рекомендуем использовать сторонние DNS-хостинги.

Формат записей

Формат записей для настройки Master-зоны соответствует формату записей DNS-сервера BIND.

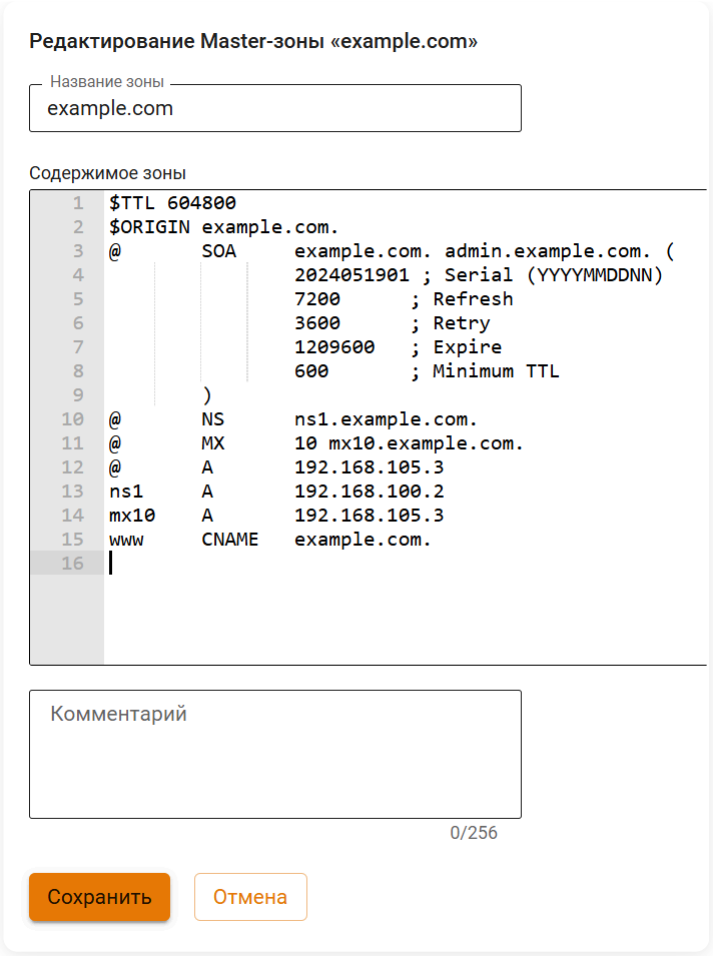
Описание параметров записи

- **TTL** - определяет время кеширования положительных ответов (например, найденного IP-адреса). Задается в секундах или с помощью сокращений: `m` (минуты), `h` (часы), `d` (дни), `w` (недели).
- **ORIGIN** - определяет текущее доменное имя. Значение `ORIGIN` заменяет символ `@` в записях, а также автоматически добавляется к любому имени, не заканчивающемуся точкой (`.`).
- **SOA** - описывает начальные параметры зоны и определяет зону ответственности сервера. Для каждой зоны допустима только одна запись SOA. Включает primary NS-сервер домена и email администратора (с заменой `@` на `.`, например: `admin.example.com`). Включает:
  - **Serial** - серийный номер зоны. Должен увеличиваться при любых изменениях, чтобы вторичные серверы обновили данные. Рекомендуемый формат: `YYYYMMDDnn` (год, месяц, день + двузначный номер изменения, начиная с `00`). Например, первое изменение 15 мая 2025 года будет `2025051500`, следующее в тот же день - `2025051501`.
  - **Refresh** - как часто вторичные серверы должны проверять первичный на наличие обновлений.
  - **Retry** - интервал между повторными попытками при неудачном обновлении.
  - **Expiry** - срок, после которого вторичный сервер прекратит использовать данные зоны, если не сможет обновиться.
  - **TTL** - минимальное время кеширования для вторичных серверов.
- **SRV** - указывает серверы, ответственные за определенные службы в домене (например, Jabber, Active Directory, SIP). Формат: `_служба._протокол.домен`.
- **NS** - указывает авторитетные DNS-серверы для домена. Для каждой `NS`-записи обязательно должны существовать сопоставимые `A` или `AAAA`-записи.
- **PTR** - преобразует IP-адрес в доменное имя (reverse DNS). Используется, например, для проверки почтовых серверов.
- **MX** - указывает почтовые серверы для домена. Формат: `Приоритет Сервер` (например, `10 mx.example.com`). Для каждого `MX` обязательна `A` или `AAAA`-запись.
- **A** - сопоставляет доменное имя с IPv4-адресом (например, `192.0.2.1`). Для каждого интерфейса требуется отдельная запись.
- **AAAA** - аналогична `A`, но для IPv6 (например, `2001:db8::1`).
- **CNAME** - задает алиас (псевдоним) для другого доменного имени. Для алиаса не должно быть других записей (например, `MX` или `TXT`).

Со всеми ресурсными записями можно ознакомиться по ссылке.
Пример записей:

Поле **Название зоны** должно соответствовать записи **$ORIGIN**, но без точки в конце. Например:

- **Имя зоны** - `168.192.in-addr.arpa`
- Запись **$ORIGIN** - `168.192.in-addr.arpa.`



Примеры записей в мастер-зону:

1. Имя зоны: ms:

```
$ORIGIN ms.
$TTL 600
@ SOA ns1.ms. administrator.ms. ( 4 7200 3600 1209600 600 )
@ NS ns1.ms.
@ MX 10 mx10.ms.
@ A 192.168.0.250
ns1 A 192.168.0.250
mx10 A 192.168.0.250
www CNAME @
```

2. Имя зоны: example.com:

```
$TTL 86400
@ SOA localhost. root.localhost. ( 2024120713 28800 14400 3600000 86400 )
@ NS my-dns-server.example.com.
my-dns-server A 1.2.3.4
```

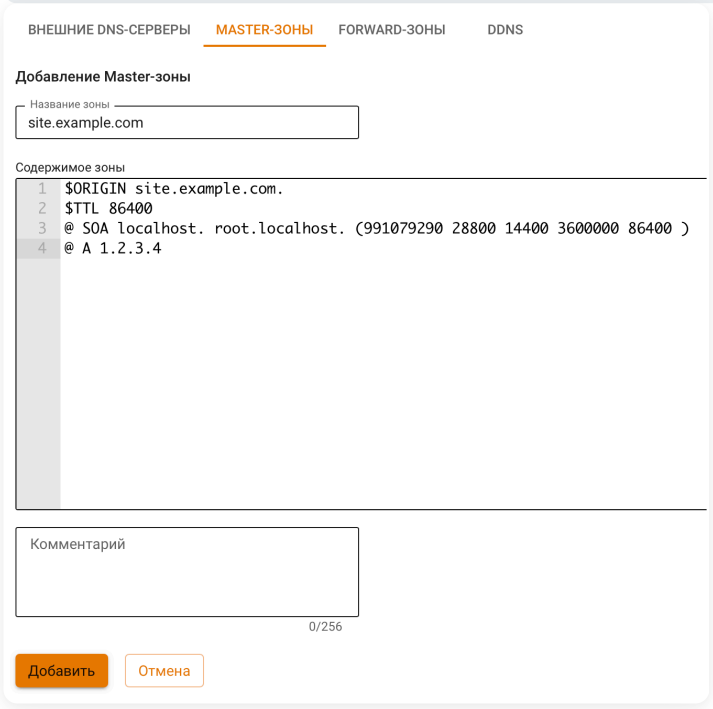
3. Имя зоны: site.example.com:

Если требуется скорректировать Master-зону для конкретного ресурса из зоны example.com, достаточно создать для ресурса отдельную Master-зону. В этом случае NGFW Novum будет управлять только им, а остальной зоной - текущий DNS-хостинг.

Пример описания для ресурса site.example.com из зоны example.com:

```
$ORIGIN site.example.com.
$TTL 86400
```

```
@ SOA localhost. root.localhost. (991079290 28800 14400 3600000 86400 )
@ A 1.2.3.4
```



Работа с IDN-доменами

IDN-домен - домен, составленный из национальных символов алфавита. Например, **дневник.ру**. Для корректной работы Master-зон с IDN-доменами выполните действия:

1. Преобразуйте IDN-домены в формат **Punycode**. Подробнее в RFC.

2. При создании содержимого Master-зоны используйте преобразованное в формат **Punycode** доменное имя.

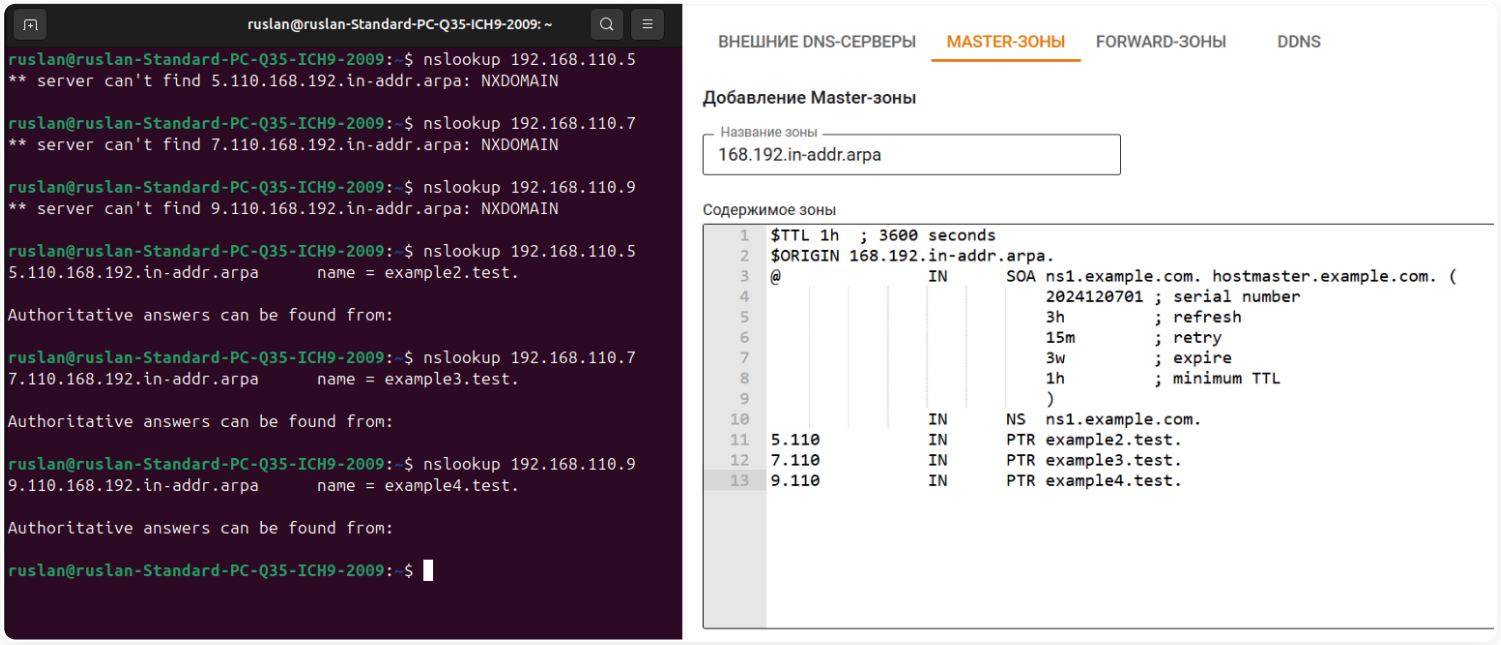
Не используйте Master-зоны для блокировки доступа к сайтам, для этого есть другие средства.

Блокировка таким способом работает неэффективно и не позволяет выборочно запрещать доступ по пользователям или подсетям. Также приводит к проблемам с излишним кешированием.

Обратная Master-зона

Обратная Master-зона используется для распознавания домена по IP-адресу.

Статические Master-зоны требуют ручного создания PTR-записей, динамические - генерируют PTR-записи автоматически. Пример обратной Master-зоны:



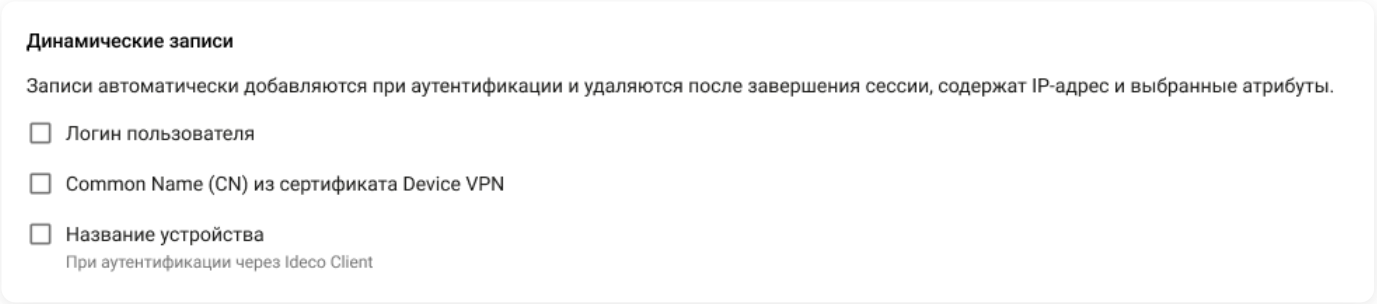
Имя зоны: 168.192.in-addr.arpa

Доменная зона соответствует IP-адресу 192.168.0.0/16. В содержимом зоны указаны три PTR-записи:

```
$TTL 1h  ; 3600 seconds
$ORIGIN 168.192.in-addr.arpa.
@               IN      SOA ns1.example.com. hostmaster.example.com. (
                            2024120701 ; serial number
                            3h         ; refresh
                            15m        ; retry
                            3w         ; expire
                            1h         ; minimum TTL
                            )
                IN      NS  ns1.example.com.
5.110           IN      PTR example2.test.
7.110           IN      PTR example3.test.
9.110           IN      PTR example4.test.
```

Динамические записи

Автоматически обновляемые DNS-записи создаются при аутентификации пользователей в Ideco NGFW, дополняя статические записи зоны. Выберите типы записей для добавления:



- **Логин пользователя** - идентификатор пользователя.
- **Common Name (CN) из сертификата Device VPN** - имя устройства из SSL-сертификата Device VPN.
- **Название устройства** - имя устройства из данных ZTNA (Zero Trust Network Access).

Логика добавления PTR-записей:

- Добавляются только при включении соответствующей опции (логин, CN, название устройства).
- Создаются только в паре с прямыми A-записями.
- Не создаются, если для прямой записи нет зоны.

Примеры динамических DNS-записей, где сессия имеет IP-адрес 192.0.2.2:

Доменное имя сессии	Абсолютное доменное имя сессии	Прямая зона	Прямая запись	Обратная зона	Обратная запись
ivanov.example.com.	ivanov.example.com.	example.com.	ivanov IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.com.
ivanov.example.com	ivanov.example.com.	example.com.	ivanov IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.com.
ivanov.example	ivanov.example.example.com.	example.com.	ivanov.example IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.example.com.
ivanov	ivanov.example.com.	example.com.	ivanov IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.com.

Forward-зоны

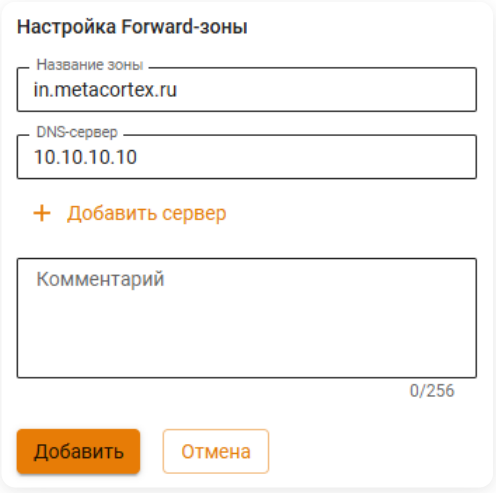
Классический контекст | Высокопроизводительный контекст

Позволяет задать DNS-сервер для разрешения имен конкретной DNS-зоны. Указав доступный в сети DNS-сервер и обслуживаемую зону, клиенты сети Ideco NGFW Novum получают возможность обращаться к ресурсам этой зоны по именам домена.

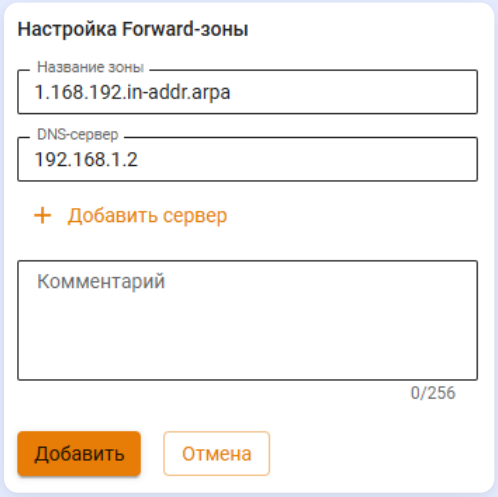
Пользовательские Forward-зоны DNS всегда имеют приоритет над автоматически созданной Forward-зоной для Active Directory.

Например, IT-отдел предприятия предоставляет ресурсы для сотрудников в зоне `in.metacortex.ru` под именами `realm1.in.metacortex.ru`, `sandbox.in.metacortex.ru` и использует для этого DNS-сервер `10.10.10.10`.

Для возможности доступа к этим ресурсам по доменным именам укажите Forward-зону провайдера как isp и далее задайте DNS-сервер `10.10.10.10`:



Для резолвинга PTR при интеграции с Active Directory пропишите обратную Forward-зону. Например, для подсети `192.168.1.0/24` в названии зоны нужно прописать `1.168.192.in-addr.arpa`:



Полезные ссылки

- **Пример настройки Forward-зоны**

- **Подключение через Ideco Client к внутреннему DNS**

DDNS

Функциональность доступна в **Классическом** и **Системном контекстах**.

Название службы раздела **DDNS**: `ideco-dns-backend`.

Список служб для других разделов доступен по ссылке.

DDNS в Ideco NGFW Novum реализован через интеграцию с хостингом RU-CENTER. Перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.

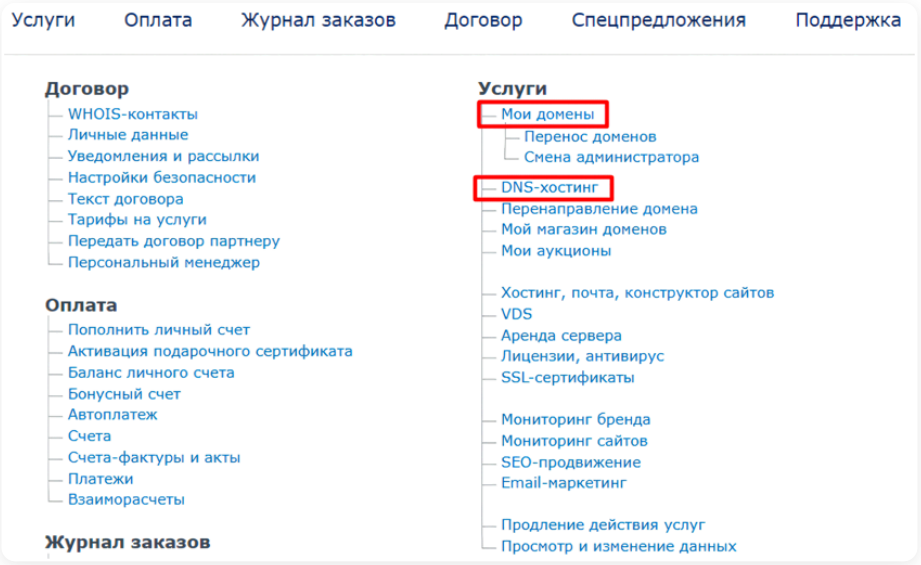
Для решения вопросов по работе с хостингом воспользуйтесь страницей помощи.

Настройка DDNS

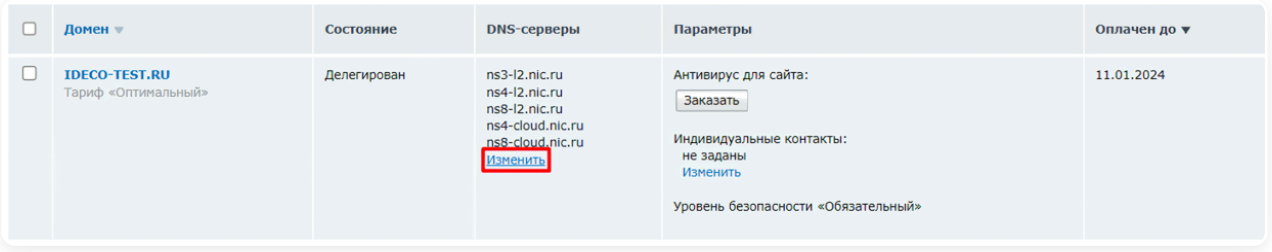
DDNS не будет работать:

- если NGFW находится за NAT.
- если включена балансировка трафика.

1. После входа в личный кабинет RU-CENTER откроется страница Для клиентов. Для дальнейшей работы откройте два раздела - **Мои домены** и **DNS-хостинг**:



2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:

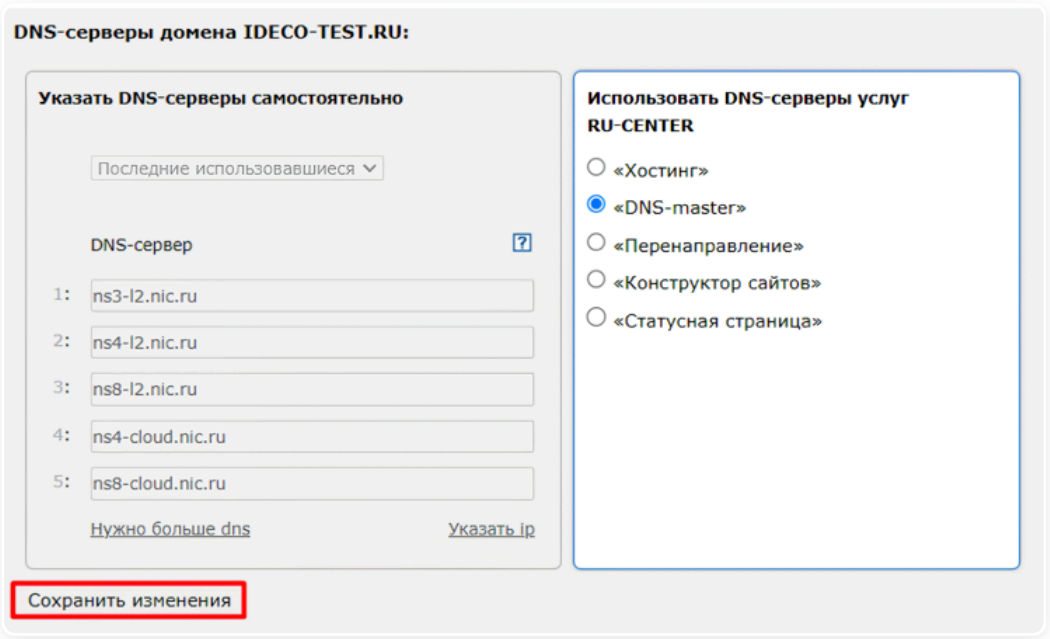


3. Делегируйте домен, отредактировав настройки DNS-серверов:

- **Указать DNS-серверы самостоятельно** - укажите DNS-серверы. Если домен был приобретен на хостинге RU-CENTER, поля заполнятся автоматически.

- **Использовать DNS-серверы услуг RU-CENTER** - выберите **DNS-master**.

Сохраните изменения:



Домен будет делегирован с заданным списком DNS-серверов. Это может занять несколько часов.

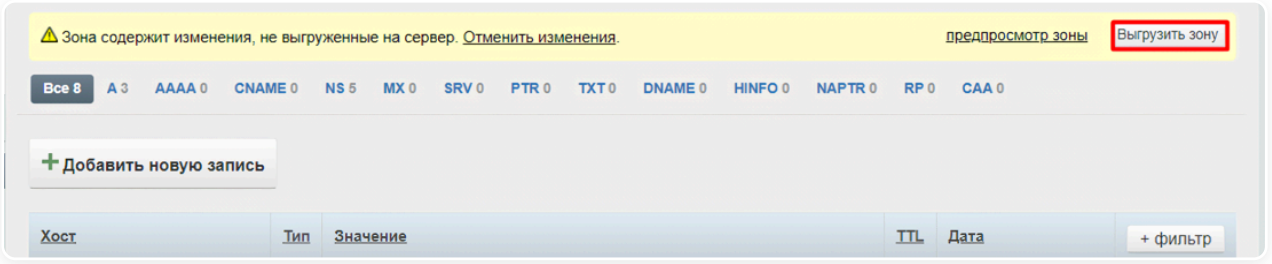
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

5. Выберите нужный домен или добавьте (если домен был приобретен на стороннем ресурсе), нажав соответствующую кнопку.

6. Добавьте две записи по кнопке **Добавить новую запись**:

- Первая запись:
  - Name - укажите знак `@`.
  - Type - выберите тип `A`.
  - IP address - текущий IP-адрес Ideco NGFW Novum (указывается в **Техническая поддержка** → **Информация для технической поддержки**).
  - TTL - оставьте не заполненным.
- Вторая запись:
  - Name - укажите `www`.
  - Type - выберите тип `A`.
  - IP address - текущий IP-адрес Ideco NGFW Novum.
  - TTL - оставьте не заполненным.

7. Нажмите кнопку **Выгрузить зону**:



8. Перейдите в раздел **DDNS** в Ideco NGFW Novum и заполните поля:

- **Домен на DNS-хостинге nic.ru** - укажите приобретенный домен.
- **Логин от API** и **Пароль от API** - для получения логина и пароля перейдите по ссылке Динамический DNS и нажмите **Получить**:



9. Сохраните настройки в Ideco NGFW Novum, нажав соответствующую кнопку.

DHCP-сервер

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **DHCP**: `ideco-dhcp-server-backend`.

Список служб для других разделов доступен по ссылке.

DHCP-сервер автоматически назначает IP-адреса и другие параметры сетевой конфигурации устройствам в сети по протоколу DHCP (Dynamic Host Configuration Protocol).

В Ideco NGFW Novum DHCP-сервер используется для упрощения управления сетевыми настройками:

- Исключает необходимость ручной конфигурации каждого устройства.
- Обеспечивает корректное распределение адресов.
- Предотвращает конфликты IP-адресов.

Это особенно актуально в динамических сетях с большим количеством подключаемых устройств.

Интерфейс Ideco NGFW Novum

- **Настройки** - позволяет настроить диапазон IP-адресов для автоматического назначения.
- **Привязка IP к MAC** - позволяет сформировать статические привязки IP-адресов к MAC-адресам.
- **Мониторинг аренды** - позволяет получить сведения об аренде IP-адреса для устройства.

Сетевые устройства в локальной сети должны быть настроены на автоматическое получение сетевых реквизитов от DHCP-сервера. Таким образом, клиенты отправляют широковещательный запрос в сегмент локальной сети, а сервер перехватывает и отправляет на эти запросы ответы, содержащие необходимые настройки для клиента.

Для сортировки строк таблицы по определенному столбцу нажмите на этот столбец в заголовке таблицы.

Для настройки DHCP-сервера перейдите в **Сервисы** → **DHCP-сервер**. Включите опцию **DHCP-сервер**:



На локальном интерфейсе Ideco NGFW Novum, участвующем в раздаче адресов, должен быть настроен статический IP-адрес.

Настройки

Если Ideco NGFW Novum является шлюзом и DNS-сервером для всех сетевых устройств локальной сети, то настройка службы ограничивается определением диапазона IP-адресов.

Если на Ideco NGFW Novum настроен перехват DNS, то резолвинг имен будет производиться при помощи сервера, указанного в настройках перехвата DNS.

Опция **Выдавать IP-адреса, указанные в авторизациях по IP без MAC** позволяет назначать IP-адреса из правил авторизации (без MAC-адреса) любому устройству в сети, если адрес свободен. Трафик устройства, получившего такой IP-адрес, будет обрабатываться как трафик пользователя из соответствующего правила авторизации.

При отключении опции IP-адреса из правил авторизации (без MAC-адреса) резервируются и не выдаются DHCP-сервером.

Для правил авторизации по IP+MAC резервирование работает всегда, независимо от состояния опции.

Если опция **Выдавать IP-адреса, указанные в авторизациях по IP без MAC** включена, нет гарантий, что устройство получит свой прежний IP-адрес. Если в правиле авторизации не указан MAC-адрес и нет привязки в DHCP, то IP-адрес будет выдан, если свободен на момент запроса. Если адрес занят другим устройством, сервер предложит новый.

Настройка DHCP-сервера делится на три блока:

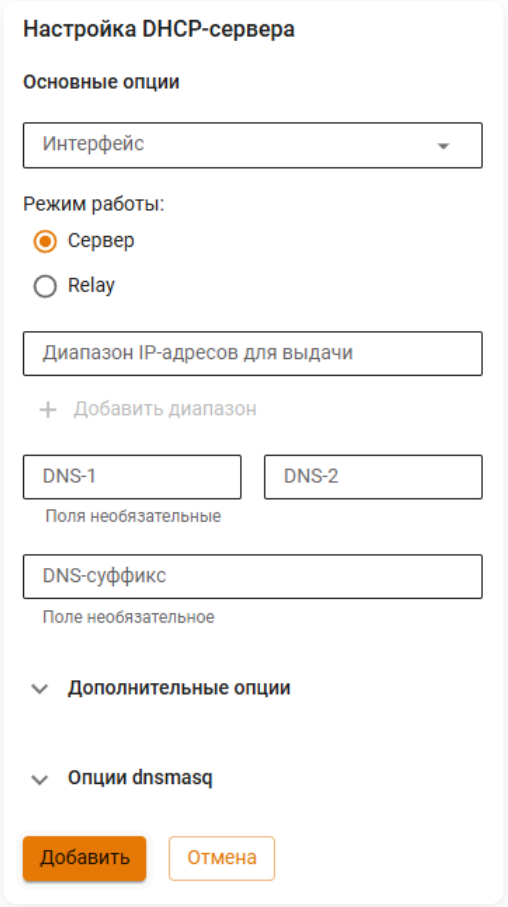
- **Основные опции** - задаются диапазоны IP-адресов и DNS-серверы.
- **Дополнительные опции** - статические маршруты, адреса WINS-серверов, время аренды, PXE Boot и WPAD.
- **Опции dnsmasq** - предназначены для ручного задания опций DHCP, передаваемых сервером клиенту при получении сетевых реквизитов от DHCP-сервера.

Основные опции

Если в разделе **Межсетевой экран** создано правило, которое запрещает весь трафик, то добавьте в таблицу **INPUT** разрешающее правило для UDP-портов 67 и 68, иначе DHCP не сможет раздавать IP-адреса и устройства не получат доступ к сети.

Режим работы Сервер

Выберите режим работы **Сервер**, чтобы настроить выдачу IP-адресов на Ideco NGFW Novum. Заполните поля:



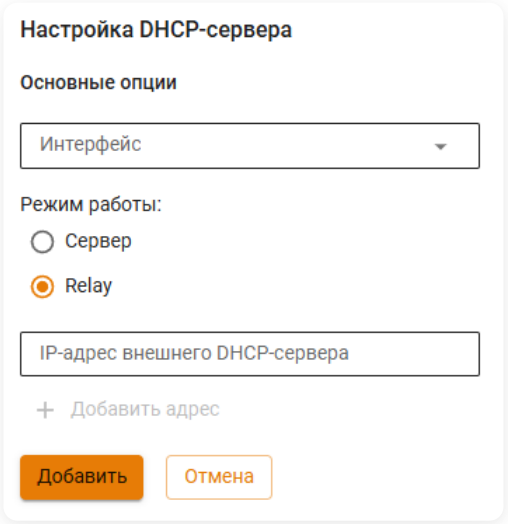
- **Интерфейс** - выберите интерфейс, который будет участвовать в раздаче адресов.

В **Системном контексте** невозможно выбрать интерфейсы, которые используются в VCE.

- **Диапазон IP-адресов для выдачи** - укажите диапазон IP-адресов, которые будут выданы устройствам в локальной сети, должен входить в одну из подсетей выбранного интерфейса. Размер диапазона не должен превышать 256 адресов.
- **DNS-1** и **DNS-2** - укажите IP-адреса DNS-серверов для устройств локальной сети. Если ни одно из полей не заполнено, то DNS-сервером для всех сетевых устройств локальной сети будет Ideco NGFW Novum.
- **DNS-суффикс** - введите домен, прибавляющийся к запрашиваемому имени устройства в локальной сети. Поле не обязательное. Нужен, для того, чтобы в локальной сети вводить не полное имя компьютера вместе с доменом, а только само имя.

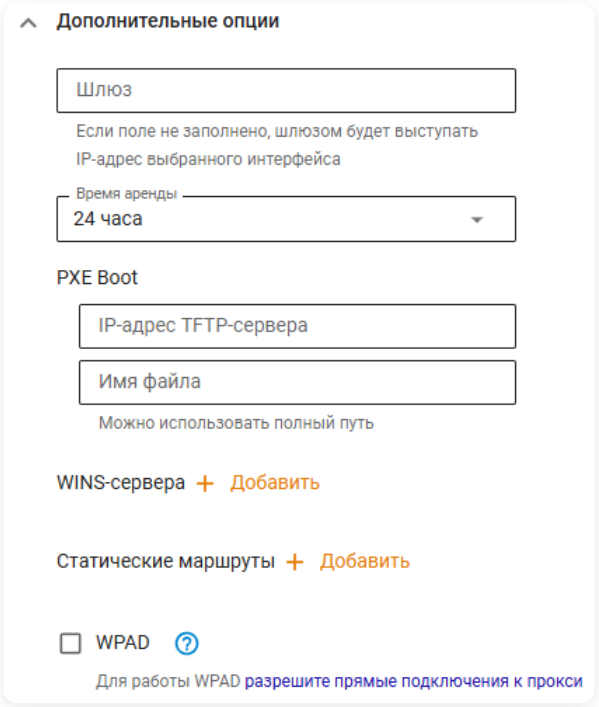
Режим работы Relay

Выберите режим работы **Relay**, если IP-адреса будет выдавать внешний DHCP-сервер. Выберите интерфейс, который будет участвовать в раздаче IP-адресов, и введите IP-адрес внешнего DHCP-сервера:



Включить/выключить, редактировать или удалить правила для выдачи IP-адресов можно кнопками управления в колонке **Управление**.

Дополнительные опции

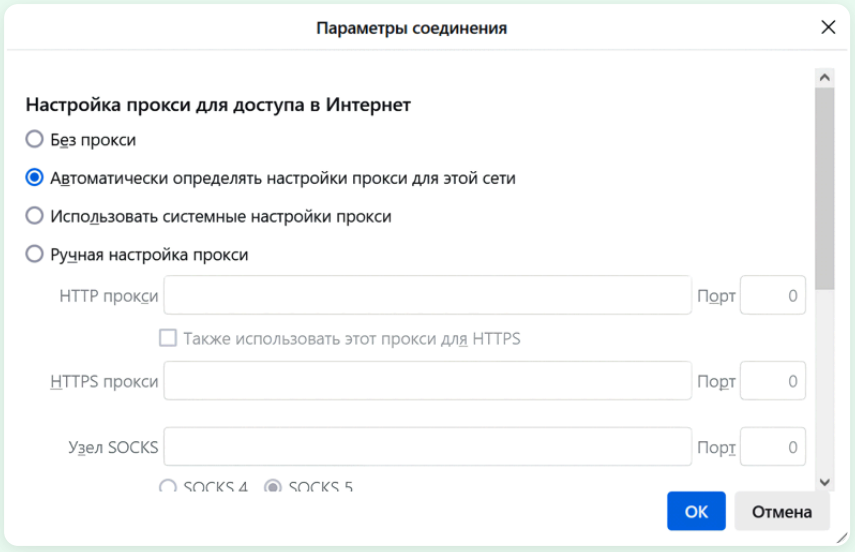


- **Шлюз** - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса.
- **Время аренды** - время, на которое выдается IP-адрес.
- **PXE Boot** - IP-адрес TFTP-сервера для настройки загрузки образа по сети.
- **WINS-сервера** - IP-адрес WINS-сервера.
- **Статические маршруты** - подсеть и шлюз для указания статического маршрута.
- **WPAD** - протокол автоматической настройки прокси.

При включении опции WPAD Ideco NGFW Novum будет автоматически генерировать файл с настройками подключения к прокси и передавать сгенерированный файл хостам в локальной сети, на которых настроено получение IP по DHCP. Локальные сети в файле конфигураций будут добавлены в исключения из прокси.

Для работы WPAD необходимо разрешить прямые подключения к прокси в разделе **Сервисы** → **Прокси**.

Браузеры Google Chrome и Microsoft Edge автоматически примут настройки прокси, переданные хостам по DHCP. В Mozilla Firefox необходимо будет дополнительно зайти в **Настройки браузера** → **Настройки прокси** и выбрать пункт **Автоматически определять настройки прокси для этой сети**:



Опции dnsmasq

Опция **dnsmasq** имеет больший приоритет чем опция, внесенная в блок **Основные опции** или **Дополнительные опции**.

Поле **Значение** может содержать только одну опцию.

Формат записи опции соответствует части записи опции в конфигурации dnsmasq - `[vendor:[<vendor-class>],][<opt>|option:<opt-name>],[<value>[,<value>]]`, где:

- `[vendor:[<vendor-class>],]` - вендор, необязательно.
- `[<opt>|option:<opt-name>]` - числовое или строковое (напр. option:nis-server) обозначение опции.
- `[<value>[,<value>]]` - одно или несколько значений опции через запятую.

Установите флаг **Force** если требуется отправлять опцию DHCP-клиенту, даже если клиент не запрашивал опцию.

Важно: некорректно заданные dnsmasq-опции могут привести к остановке работы раздела **DHCP-сервер**. Статус раздела сменится на **Модуль** `dnsmasq` **не смог запуститься** и **Служба** `ideco-dnsmasq` **остановлена**.

Для поиска некорректно заданной опции выполните действия:

- Перейдите в **Отчеты и журналы** → **Система**.
- В столбце **Сообщение** найдите запись формата `bad option at line 15 of /run/ideco-dhcp-server-backend/dnsmasq.conf`. В записи указано, на какую строку в конфиге нужно обратить внимание.
- Перейдите в **Управление сервером** → **Терминал**.
- Откройте конфиг `/run/ideco-dhcp-server-backend/dnsmasq.conf` и найдите нужную строку.

Расширение базовых опций, отсылаемых DHCP-сервером для конфигурирования IP-телефонов Avaya

Для IP-телефонов Avaya может потребоваться передать оборудованию опции 176 и 242. Для ознакомления со списком опций для конкретной модели обратитесь к документации нужной модели Avaya.

1. Перейдите к созданию настройки DHCP-сервера (**Сервисы** → **DHCP-сервер** → **Настройки** → **Добавить**).

2. Заполните **Основные** и **Дополнительные** опции.

3. Нажмите **Добавить опцию** и заполните 176 опцию. Опция используется для указания голосового сервера:

```
176,"MCIPADD=1.2.3.4,MCPORT=1719"
```

4. После добавления 176 опции добавьте 242, которая используется для серверов передачи данных:

```
242,"MCIPADD=1.1.1.2,MCPORT=1719"
```

После сохранения настроек IP-телефония Avaya будет получать от DHCP-сервера расширенный список опций.

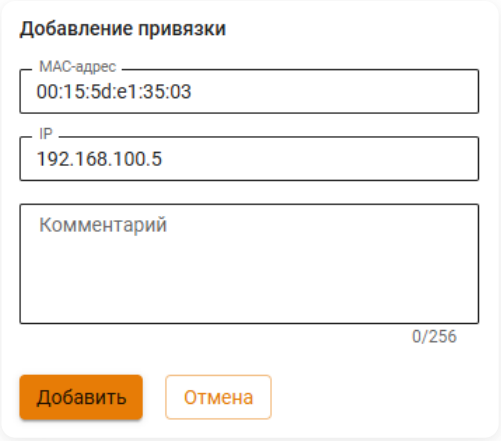
Привязка IP к MAC

IP-адрес, указанный в правиле привязки к MAC, может не входить в диапазон IP-адресов, заданный на вкладке **Настройки**. DHCP-сервер выдаст хосту этот IP-адрес.

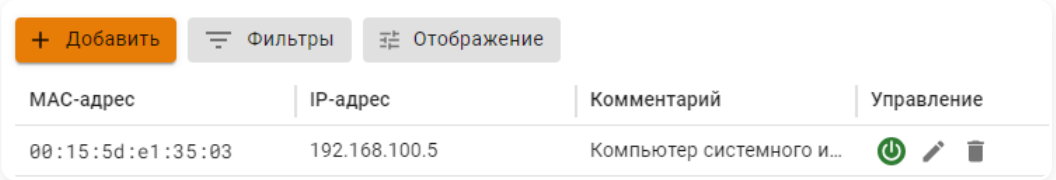
Для настройки в DHCP-сервере привязки IP-адреса к MAC-адресу необходимо:

1. В **Сервисы** → **DHCP** выберите вкладку **Привязка IP к MAC**.

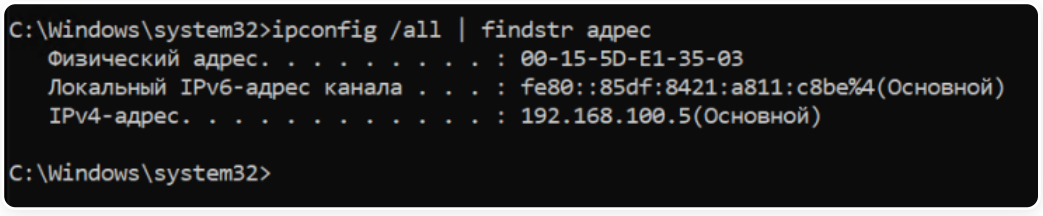
2. Создайте правило привязки **IP к MAC**:



Пример созданного правила привязки показан ниже на скриншоте:



Для проверки созданного правила на компьютере с указанным в правиле MAC-адресом получите IP-адрес по DHCP и проверьте результат с помощью команды `ipconfig /all` (для операционной системы Windows):



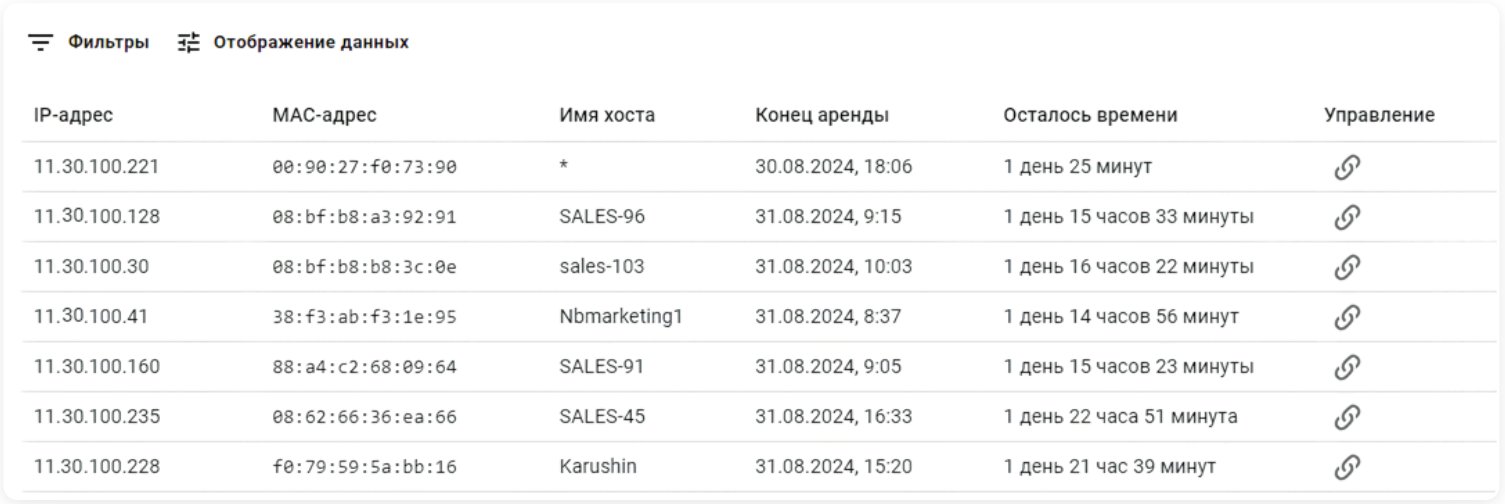
При наличии большого количества привязок в таблице воспользуйтесь кнопкой **Фильтры**.

Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW Novum.

Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (`01-02-03-04-05-06`). В настройках Ideco NGFW Novum октеты MAC-адреса разделяются только двоеточиями (`01:02:03:04:05:06`).

Мониторинг аренды

Содержит информацию об аренде IP-адресов для устройств. Для поиска воспользуйтесь кнопкой **Фильтры**:



IP-адрес	MAC-адрес	Имя хоста	Конец аренды	Осталось времени	Управление
11.30.100.221	00:90:27:f0:73:90	*	30.08.2024, 18:06	1 день 25 минут	
11.30.100.128	08:bf:b8:a3:92:91	SALES-96	31.08.2024, 9:15	1 день 15 часов 33 минуты	
11.30.100.30	08:bf:b8:b8:3c:0e	sales-103	31.08.2024, 10:03	1 день 16 часов 22 минуты	
11.30.100.41	38:f3:ab:f3:1e:95	Nbmarketing1	31.08.2024, 8:37	1 день 14 часов 56 минут	
11.30.100.160	88:a4:c2:68:09:64	SALES-91	31.08.2024, 9:05	1 день 15 часов 23 минуты	
11.30.100.235	08:62:66:36:ea:66	SALES-45	31.08.2024, 16:33	1 день 22 часа 51 минута	
11.30.100.228	f0:79:59:5a:bb:16	Karushin	31.08.2024, 15:20	1 день 21 час 39 минут	

При использовании фильтра по столбцу **Конец аренды** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные по адресам со сроком окончания аренды 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

Для привязки IP к MAC нажмите на в столбце **Управление**.

После завершения срока аренды IP-адреса и повторного подключения устройство запросит у DHCP-сервера свой предыдущий адрес:

- Если предыдущий IP-адрес свободен, сервер выдаст его устройству.
- Если запрошенный IP-адрес занят или зарезервирован, сервер выдаст новый.

Не рекомендуем полностью полагаться на возврат прежнего IP-адреса после истечения срока аренды, так как IP-адрес может быть отдан другому устройству.

Удаление аренды

Чтобы удалить аренду IP-адреса:

1. Перейдите в **Управление сервером** → **Терминал** и введите команду:

```
nano /var/cache/ideco/dhcp-server-backend/dnsmasq.leases
```

2. Удалите строку с нужной арендой IP-адреса и сохраните файл.

Полезные ссылки

- **Настройка Wi-Fi-сети**

NTP-сервер

Классический контекст | Высокопроизводительный контекст

Название службы раздела **NTP**: `chronyd`.

Список служб для других разделов доступен по ссылке.

NTP - протокол для синхронизации времени. Он позволяет установить точное время на компьютере, используя информацию от специальных серверов времени. По умолчанию работает на 123/UDP порте.

Принцип работы

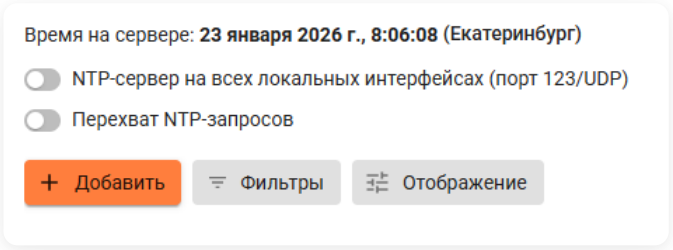
Серверы времени, используемые в NTP, имеют свою иерархию:

- Верхний уровень иерархии занимают официальные источники времени.
- На следующем уровне находятся сервера времени, которые синхронизируют свои часы с официальными источниками времени.
- На последнем уровне находятся клиенты NTP, которые получают информацию от серверов времени.

Ideco NGFW Novum по умолчанию работает как NTP-клиент, получая точное время от эталонных серверов верхнего уровня. При этом Ideco NGFW Novum также может быть настроен как локальный NTP-сервер для устройств во внутренней сети.

Настройка Ideco NGFW Novum

В **Сервисы** → **NTP-сервер** доступны настройки:



- **NTP-сервер на всех локальных интерфейсах (порт 123/UDP)** - при включении опции NGFW Novum будет доступен в качестве NTP-сервера для локальных клиентов. В этом случае NGFW Novum предоставляет время, синхронизированное с внешними эталонными серверами, устройствам в локальной сети, если они настроены на синхронизацию.
- **Перехват NTP-запросов** - при включении опции все запросы локальных клиентов будут обрабатываться NGFW Novum, даже если были отправлены на другой NTP-сервер. В результате все устройства в сети будут получать время только от NGFW Novum, независимо от их собственных настроек.
- Таблица внешних NTP-серверов - в таблице можно вручную указать NTP-серверы, с которыми необходимо синхронизировать время NGFW Novum:
  - Если таблица пуста, NGFW Novum автоматически использует встроенный список доверенных первичных серверов для синхронизации своего времени.
  - Если в таблице есть записи, NGFW Novum будет синхронизироваться только с указанными серверами.

Чтобы создать запись в таблице, нажмите **Добавить** и введите IP-адрес или доменное имя в поле **NTP-сервер**:

Добавление NTP-сервера

NTP-сервер

IP-адрес или доменное имя

Комментарий

0/256

Добавить Отмена

IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Название службы раздела **IPsec**: `ideco-ipsec-backend`.

Список служб для других разделов доступен по ссылке.

IPsec (Internet Protocol Security) - набор протоколов, обеспечивающих безопасную передачу данных в IP-сетях. Обеспечивает аутентификацию, целостность и шифрование данных между узлами.

Воспользуйтесь конфигураторами подключений для MikroTik или Cisco. Конфигураторы позволяют сгенерировать конфиг, запуск которого на удаленном устройстве установит заранее подготовленные настройки IPsec.

Особенности подключений IPsec

В туннельном режиме

- Поддерживается неограниченное число туннелируемых IP-адресов.
- **Туннельный** режим не пропускает широковещательные рассылки, поэтому в таком режиме настроить OSPF не получится.

Необходимо заполнять поле **IP-адрес интерфейса туннеля** для доступа Ideco NGFW Novum к удаленным сетям за другим устройством (например, для доступа к Ideco Center или Active Directory). В будущих версиях без указания IP-адреса доступность удаленных ресурсов для NGFW через IPsec не будет гарантирована.

Следует учесть, что при обновлении на версию 22:

- Существующие конфигурации с несколькими адресами удаленного устройства продолжат работать после миграции. В новой версии допускается только один **Адрес удаленного устройства**.
- **Группа балансировки и резервирования**, выбранная в поле **Интерфейс подключения**, будет перенесена в **Профиль next hop**. В новой версии в поле **Интерфейс подключения** допускается только один интерфейс.

Рекомендуем после обновления указать конкретный **Интерфейс подключения** и конкретный **Адрес удаленного устройства**, так как варианты с множественным выбором или объектом **Любой** будут удалены в следующих версиях.

В транспортном режиме

- Трафик не ограничивается IPSec-политиками, необходимо настраивать маршрутизацию вручную. Для подключения используется выбранный в настройках сетевой интерфейс.
- Пропускаются широковещательные рассылки. Рекомендуем в данном режиме использовать маршрутизацию на основе OSPF.
- Для резервирования канала можно создать несколько IPSec-подключений через разные внешние интерфейсы и определить приоритет направления трафика настройками **OSPF**.

Исходящие и входящие подключения

Настройте исходящее подключение, если Ideco NGFW Novum является инициатором подключения, а удаленное устройство - принимающей стороной. Если удаленное устройство - инициатор подключения, настройте входящее подключение.

Исходящее подключение

Для настройки исходящего подключения подготовьте:

Тип аутентификации	**Требуемые параметры**

Сертификат	• Подписанный удаленным устройством **Запрос на подпись сертификата**. Файл запроса скачивается из веб-интерфейса NGFW Novum при создании подключения, отправляется удаленному устройству и подписанный возвращается для настройки NGFW Novum. • Корневой сертификат удаленного устройства. • Список домашних локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	• PSK-ключ. Генерируется на NGFW Novum при создании подключения. • Идентификатор ключа, который потребуется удаленному устройству для идентификации подключения. • Список локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

Входящее подключение

Для настройки входящего подключения подготовьте:

Тип аутентификации	Требуемые параметры
Сертификат	• Запрос на подпись сертификата (.csr), полученный от удаленного устройства. • Список домашних локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	• PSK-ключ, сгенерированный на удаленном устройстве. • Идентификатор удаленной стороны, заданный в исходящем подключении удаленного устройства. Используется для сопоставления входящего подключения с PSK-ключом. • Список локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

Примеры настройки IPsec

В туннельном режиме:

- **Подключение между двумя Ideco NGFW Novum в туннельном режиме работы**
- **Подключение Ideco NGFW Novum и MikroTik по IPsec в туннельном режиме**
- **Подключение Cisco IOS и Ideco NGFW Novum по IPsec в туннельном режиме**

В транспортном режиме:

- **Подключение между двумя Ideco NGFW Novum в транспортном режиме работы**
- **Подключение Ideco NGFW Novum и MikroTik по IPsec в транспортном режиме**
- **Подключение Cisco IOS и Ideco NGFW Novum по IPsec в транспортном режиме**

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключений. После сохранения изменений произойдет перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

После создания IPsec-подключения в **SD-WAN** → **Next hop** автоматически появляется новый next hop. Для настройки балансировки или резервирования:

1. Создайте несколько IPsec-подключений - для каждого появится свой next hop.

2. В разделе **SD-WAN** → **Профили IP SLA** настройте профиль для проверки доступности и качества канала.

3. В разделе **SD-WAN** → **Профили next hop** создайте профиль и выберите режим работы, добавив:

- **Next hop**, полученные при создании IPsec.
- **Профиль IP SLA**, настроенный на шаге 2.

IPsec использует протокол UDP, порты 500 и 4500. По умолчанию порты открыты, но если настроено запрещающее правило во вкладке **INPUT** раздела **Межсетевой экран**, не забудьте добавить разрешение для IPsec.

Выбор алгоритмов шифрования на удаленных устройствах

При настройке сторонних устройств необходимо явно указать алгоритмы шифрования, используемые для подключения.

Ideco NGFW Novum не поддерживает устаревшие и небезопасные алгоритмы (MD5, SHA1, AES128, DES, 3DES, blowfish и др.) при подключении site-to-site. Все site-to-site используют только IKEv2.

При конфигурировании сторонних устройств можно указать несколько поддерживаемых алгоритмов одновременно, так как не все устройства поддерживают современные алгоритмы.

Список алгоритмов

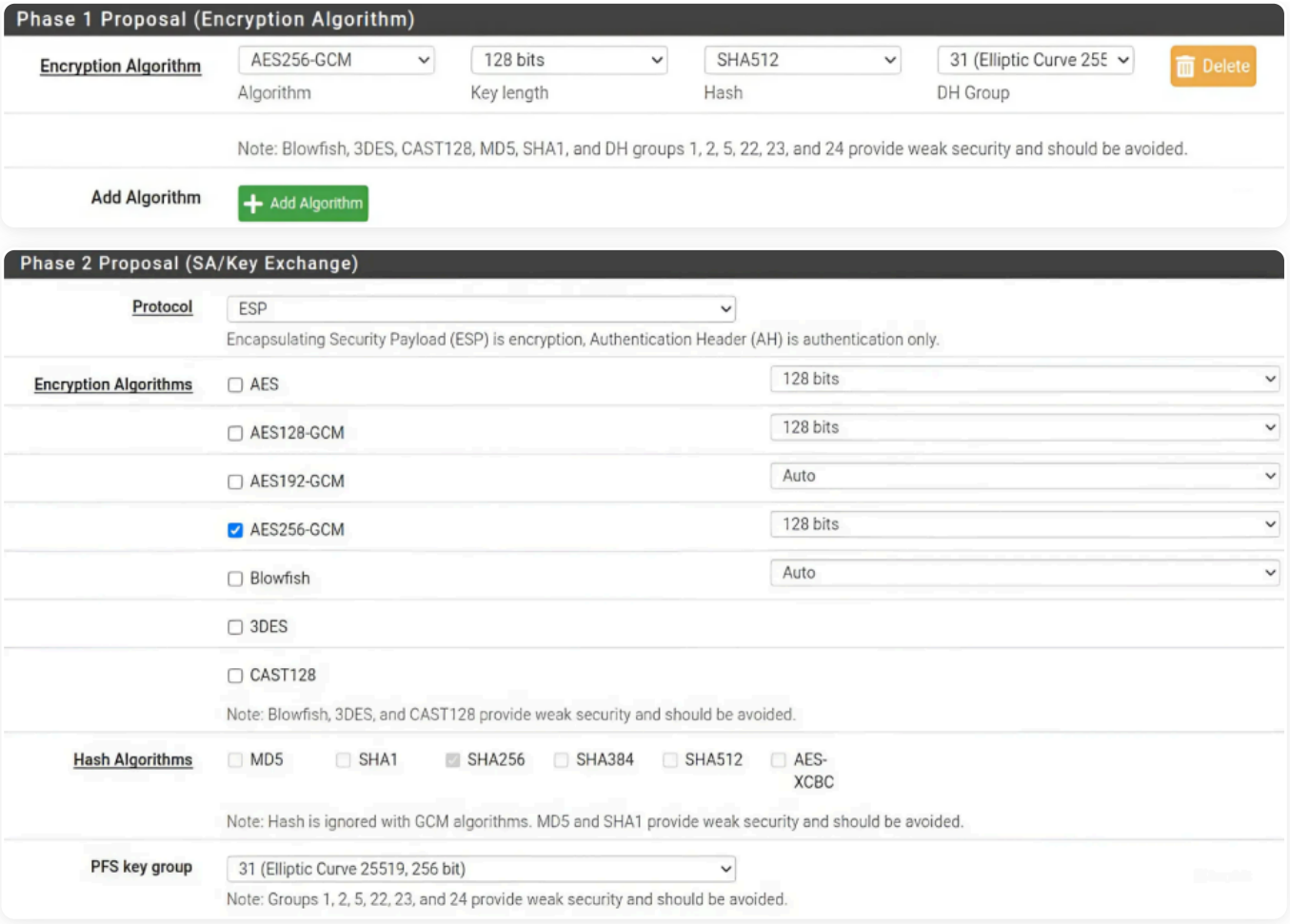
- **Phase 1 (IKE):**
  - encryption (шифрование):
    - **AES256-GCM**.
    - **AES256 (AES256-CBC)**.
  - integrity (hash, целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
    - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
  - prf (функция генерации случайных значений):
    - как правило, настраивается автоматически в зависимости от выбора алгоритмов integrity (пример ниже).
    - для AES-GCM может потребоваться указать явно. В этом случае по приоритету: **AESXCBC, SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman):
    - **Curve25519 (group 31)**.
    - **ECP256 (group 19)**.
    - **modp4096 (group 16)**.
    - **modp2048 (group 14)**.
  - Таймауты:
    - **Lifetime**: 14400 сек.
    - **DPD Timeout** (для L2TP/IPsec): 40 сек.
    - **DPD Delay**: 30 сек.
- **Phase 2 (ESP):**
  - encryption (шифрование):
    - **AES256-GCM**.
    - **AES256 (AES256-CBC)**.
  - integrity (целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
    - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman, PFS). **ВНИМАНИЕ! Если не указать группу, то подключение будет установлено, но через некоторое время не сработает параметр rekey**:
    - **Curve25519 (group 31)**.
    - **ECP256 (group 19)**.
    - **modp4096 (group 16)**.
    - **modp2048 (group 14)**.
  - Таймаут:
    - **Lifetime**: 3600 сек.

Пример использования алгоритмов

Пример:

- **Phase 1 (IKE)** (нужна одна из строк)**:**
  - AES256-GCM\PRF-HMAC-SHA512\Curve25519.
  - AES256(AES256-CBC)\SHA512\PRF-HMAC-SHA512\ECP384.
  - AES256(AES256-CBC)\SHA256\PRF-HMAC-SHA256\MODP2048.
- **Phase 2 (ESP)** (нужна одна из строк)**:**
  - AES256-GCM\ECP384.
  - AES256(AES256-CBC)\SHA256\MODP2048.

Пример настройки подключения pfSense к Ideco NGFW Novum по IPsec:



Мониторинг производительности сети

В Ideco NGFW Novum реализован мониторинг IPsec-соединений, аналогичный IP SLA (Internet Protocol Service Level Agreement). Система позволяет в реальном времени отслеживать ключевые метрики качества сетевого соединения.

В интерфейсе Ideco NGFW Novum для каждого активного соединения отображаются метрики:

- **Вх. скорость, Мбит/с** - скорость приема данных через туннель.
- **Исх. скорость, Мбит/с** - скорость передачи данных через туннель.
- **Средняя задержка, мс** - время, за которое пакет доходит до удаленной стороны туннеля и возвращается обратно.
- **Потеря пакетов, шт.** - количество отправленных, но не дошедших пакетов.
- **Джиттер, мс** - изменение задержки между пакетами.

Для сбора статистики в настройках IPsec-подключения на обеих сторонах заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Указанные IP-адреса должны принадлежать одной подсети.

ГОСТ VPN

Функциональность доступна только в **Системном контексте**.

ГОСТ VPN - это сервис для организации защищенных каналов связи между несколькими Ideco NGFW Novum с использованием технологии виртуальной частной сети. Соединение шифруется согласно требованиям ФСБ по ГОСТ-алгоритмам с применением российского сертифицированного решения от компании Рутокен.

Компания "Айдеко" пока не получила заключение от регулятора и только завершает работы по сертификации интеграции, поэтому использование ГОСТ VPN не закрывает требования регулятора по организации доверенного канала связи для передачи конфиденциальной информации через интернет.

Используются алгоритмы шифрования:

- **ГОСТ Р 34.10-2012** - для создания ключевой пары.
- **ГОСТ Р 34.12-2015** (**Кузнечик** и **Магма**) - для симметричного шифрования.
- **VKO ГОСТ Р 34.10-2012** - для выработки сессионных ключей.

Туннельное соединение можно использовать в **Маршрутизации**.

В разделе **Графики загруженности → ГОСТ VPN** представлена информация о входящих и исходящих соединениях ГОСТ VPN, а также данные мониторинга трафика.

Настройка ГОСТ VPN

Для настройки ГОСТ VPN необходимо подготовить два USB-токена в соответствии с инструкцией, представленной в статье, и подключить токены к USB-портам серверов.

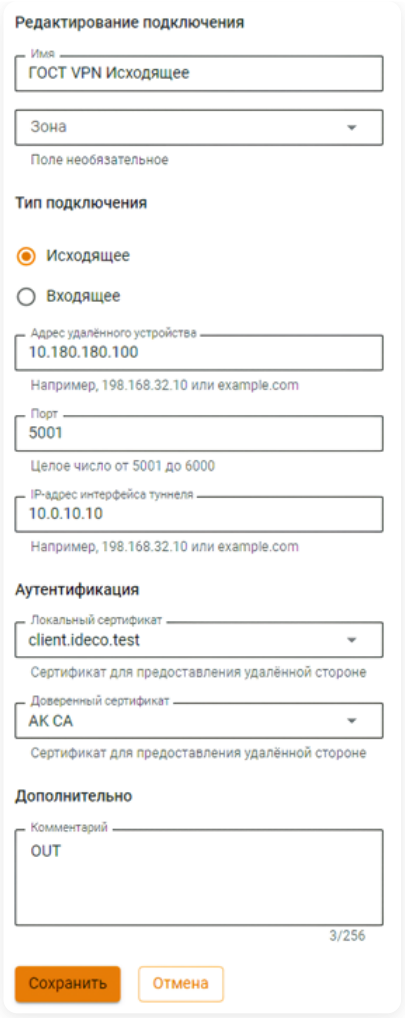
В случае извлечения USB-токена или истечения срока действия сертификатов, хранящихся на USB-токене, VPN-соединение будет разорвано.

Для создания соединения между двумя Ideco NGFW Novum необходимо настроить входящее соединение на одном NGFW и исходящее соединение на другом NGFW.

Настройка исходящего подключения

1. Перейдите в **Сервисы → ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



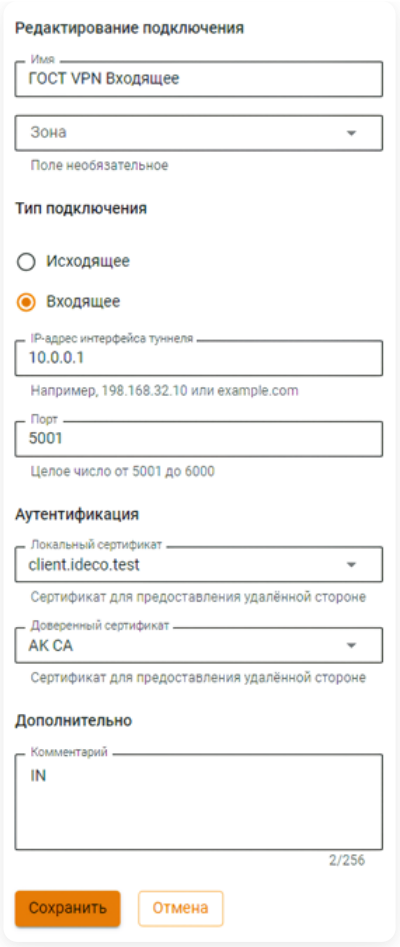
Расшифровка полей

- **Имя** - введите имя подключения, максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Тип подключения** - выберите **Исходящее**.
- **Адрес удаленного устройства** - введите доменное имя или белый IP-адрес удаленного Ideco NGFW Novum.
- **Порт** - введите порт в диапазоне от 5001 до 6000.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля, который будет использоваться для маршрутизации данных на сетевом уровне.
- **Локальный сертификат** - выберите локальный сертификат настраиваемого устройства, который содержит приватный ключ и хранится на USB-токене.
- **Доверенный сертификат** - выберите доверенный сертификат, который хранится на том же USB-токене, где находится локальный сертификат.

Настройка входящего подключения

1. Перейдите в **Сервисы** → **ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Имя** - введите имя подключения, максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Тип подключения** - выберите **Входящее**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля, который будет использоваться для маршрутизации данных на сетевом уровне.
- **Порт** - введите порт в диапазоне от 5001 до 6000.
- **Локальный сертификат** - выберите локальный сертификат настраиваемого устройства, который содержит приватный ключ и хранится на USB-токене.
- **Доверенный сертификат** - выберите доверенный сертификат, который хранится на том же USB-токене, где находится локальный сертификат.

Настройка ГОСТ VPN в кластере

Для корректной работы ГОСТ VPN в кластере необходимо:

1. Подготовить токены:

- Должно быть **два разных USB-токена** - по одному для каждой ноды кластера.
- **Не вставляйте оба токена в одну ноду** - это может привести к ошибкам в работе.

2. Подготовить сертификаты с учетом требований:

- На **каждом токене** необходимо сгенерировать свой сертификат.
- У полученных сертификатов должно быть **одинаковое значение CN (Common Name)**.
- Оба сертификата должны быть подписаны **одним и тем же удостоверяющим центром (Certificate Authority, CA)**.

3. Настроить привязки токенов:

- Для обоих токенов в конфигурации криптопровайдера необходимо прописать привязку **PIN-код - токен**.

Особенности работы в кластере:

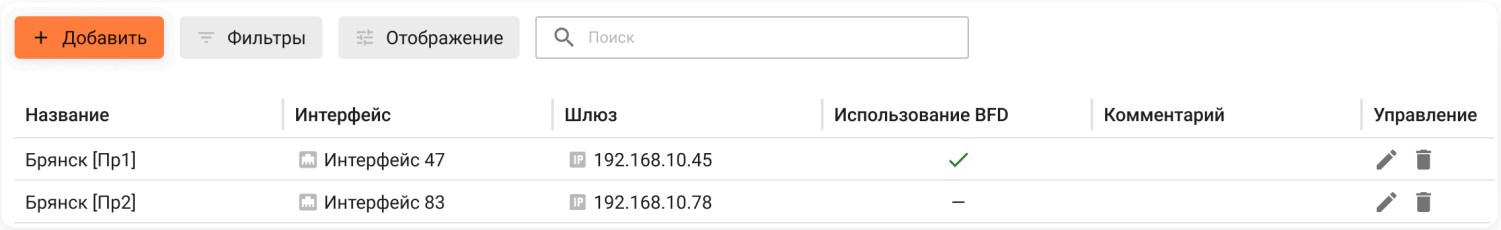
- VPN-соединение работает на **активной** в данный момент ноде.

- При отказе активной ноды кластер переключится на резервную, и использоваться будет сертификат токена, находящийся в резервной ноде. Соединение восстанавливается за счет идентичности сертификатов (CN, подпись CA) на обоих токенах.

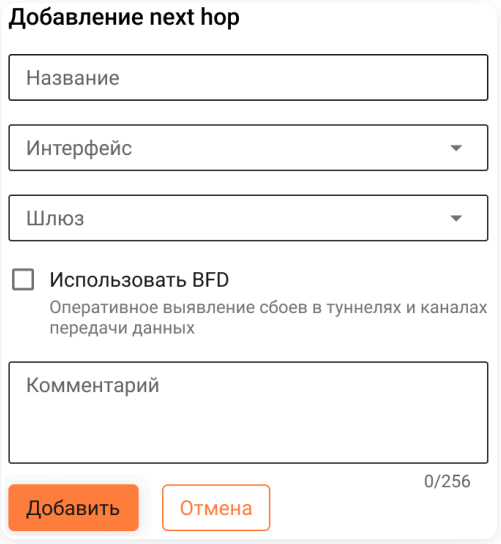
Настройка Next hop

Чтобы использовать туннель в маршрутизации, создайте **Next hop**:

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**:



2. Заполните поля:



- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс **ГОСТ VPN**.
- **Шлюз** - оставьте поле пустым. **ГОСТ VPN** является point-to-point соединением - трафик отправляется напрямую в туннельный интерфейс, минуя шлюз.

Для настройки мониторинга состояния **Next hop** воспользуйтесь статьей.

Статусы подключения

После настройки в таблице **ГОСТ VPN** появится site-to-site соединение, в котором можно отслеживать статус подключения.

Статус подключения ГОСТ VPN	Описание
Подключено	ГОСТ VPN подключен и работает
Соединяется	Происходит установление соединения или ожидание ответа от другого устройства
Отключение	Происходит разъединение подключенных устройств
Не подключено	Отсутствует подключение
Ошибка	Возникла ошибка

Полезные ссылки

- **Поддержка устаревших алгоритмов шифрования**
- **Пример генерации ключей и сертификатов ГОСТ VPN**

Сертификаты

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Сертификаты**: `ideco-cert-backend`.

Список служб для других разделов доступен по ссылке.

В разделе **Сертификаты** отображаются SSL-сертификаты или цепочки сертификатов, список которых формируется модулями:

- [x] Модуль обратного проксирования
- [x] VPN-серверы IKEv2 и SSTP
- [x] Веб-интерфейс
- [x] Веб-аутентификация
- [x] Почта
- [x] Ideco Client

Логика работы

Ideco NGFW Novum позволяет выпустить или загрузить корневые и некорневые (пользовательские) сертификаты:

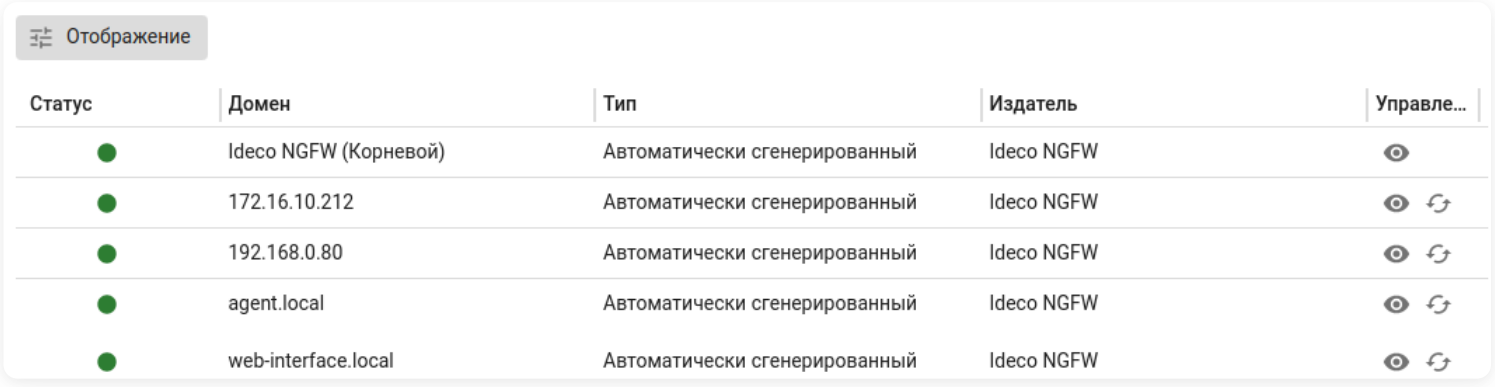
- **Корневые сертификаты** обязательно должны содержать атрибут **X509v3 Basic Constraints: CA: TRUE** для выпуска дочерних сертификатов. При первоначальной установке и запуске Ideco NGFW Novum корневой (самоподписанный) сертификат генерируется автоматически. Сертификат можно скачать, перейдя в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** и нажав .
- **Пользовательские сертификаты** - любые сертификаты на домен. Источником подписи для таких сертификатов могут выступать:
  - Корпоративный корневой сертификат.
  - Центры сертификации (Certificate Authority, CA).

Ideco NGFW Novum автоматически генерирует и подписывает сертификаты на домены, указанные в настройках модулей.

Действующие сертификаты

В таблице **Действующие сертификаты** отображаются:

- Автоматически сгенерированные цепочки сертификатов.
- Загруженные цепочки сертификатов, используемые модулями Ideco NGFW Novum:

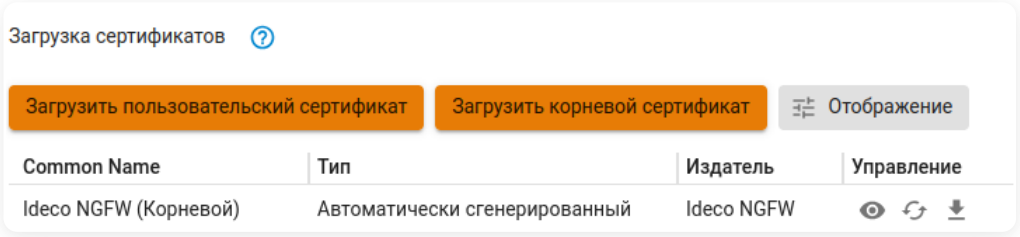


Если в таблице **Действующие сертификаты** одна и та же цепочка сертификатов указана в нескольких строках, значит, она используется несколькими модулями.

Загруженные сертификаты

В таблице **Загруженные сертификаты** отображаются:

- Все загруженные цепочки сертификатов.
- Корневой сертификат Ideco NGFW Novum:



Требования к SSL-сертификатам и инструкция по загрузке в статье.

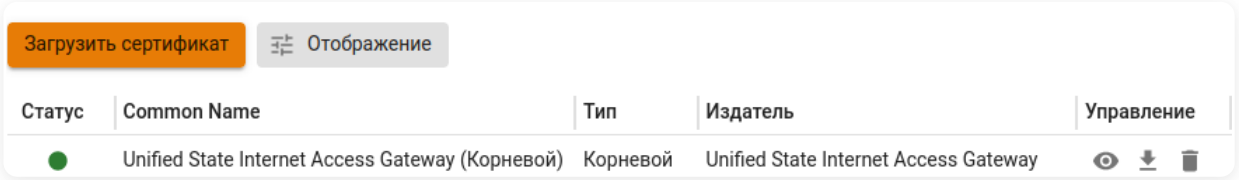
Системные сертификаты

Раздел позволяет загружать свои сертификаты в хранилище доверенных сертификатов ОС Fedora на Ideco NGFW Novum. Подробнее о системных сертификатах - по ссылке.

Загрузка в **Системные сертификаты** необходима, если Ideco NGFW Novum взаимодействует с сервисами, защищенными сертификатом от корпоративного или самоподписанного центра сертификации (CA). Чтобы Ideco NGFW Novum доверял такому сервису, корневой сертификат этого CA необходимо добавить в хранилище.

Если внешний сервис использует сертификат, выпущенный публичным доверенным CA (например, Let's Encrypt), загружать ничего не нужно - такие CA уже включены в стандартное хранилище доверенных сертификатов ОС Fedora.

После добавления сертификата в таблицу **Системные сертификаты** перезагрузите Ideco NGFW Novum. После перезагрузки Ideco NGFW Novum будет доверять загруженному сертификату и всем сертификатам, подписанным загруженным сертификатом:



Ideco Client

Раздел предназначен для управления сертификатами, используемыми для настройки авторизации пользователей и VPN-доступа через Ideco Client. Сертификаты позволяют реализовать привязку устройств к пользователям и третий фактор аутентификации.

Логика работы сертификатов Ideco Client

При подключении через Ideco Client система использует сертификаты устройства для:

- [x] Идентификации и привязки устройства к пользователю
- [x] Проверки подлинности устройства
- [x] Ограничения доступа к VPN только с доверенных устройств

Ideco NGFW Novum поддерживает два источника доверия:

- **Встроенный удостоверяющий центр (CA)**. Создается автоматически при первом запуске системы. Выпускает и подписывает сертификаты для устройств.
- **Сторонние удостоверяющие центры**. Можно загрузить CA-сертификаты сторонних УЦ для проверки сертификатов, выпущенных вне Ideco NGFW Novum.

В Ideco NGFW Novum серверные и клиентские сертификаты подписывают два независимых удостоверяющих центра. Корневой сертификат для выпуска серверных сертификатов Ideco NGFW Novum можно заменить собственным в разделе **Загруженные сертификаты**. **Локальный УЦ** Ideco Client - это отдельный удостоверяющий центр, который подписывает исключительно листовые клиентские сертификаты для устройств Ideco Client.

Замена корневого сертификата в разделе **Загруженные сертификаты** не влияет на **Локальный УЦ** Ideco Client и не заменяет его: он остается прежним и продолжает выпускать клиентские сертификаты для устройств.

Требования к сертификату устройства

Сертификат, выпускаемый на основании CSR-запроса, должен соответствовать следующим требованиям:

- **Тип ключа:** только EC (эллиптическая кривая).
- **Кривая:** только SECP256R1 (P-256).
- **Basic Constraints:** `CA: FALSE`.
- **Key Usage:** `digitalSignature` (critical).
- **Extended Key Usage:** `clientAuth` (critical).
- **Subject DN:** содержит непустой Common Name (CN).
- **Ограничения флагов:** сертификат не должен содержать других флагов, кроме `digitalSignature` и `clientAuth`.

Раздел представлен в виде вкладок:

- **Реестр** - таблица содержит действующие доверенные сертификаты:
  - **Сторонние УЦ** - загруженные администратором CA-сертификаты сторонних удостоверяющих центров в формате `.pem`.
  - **Локальный УЦ** - сертификаты, автоматически сгенерированные локальным удостоверяющим центром Ideco NGFW Novum:
    - **CA-сертификат локального УЦ** - локальный сертификат. Используется для выпуска и подписи сертификатов устройств пользователей.
    - **Выпущенные** - сертификаты устройств, сгенерированные и подписанные локальным УЦ после первой успешной авторизации пользователя через Ideco Client. Такие сертификаты автоматически устанавливаются через Ideco Client на устройство пользователя и обеспечивают идентификацию устройства при последующих подключениях.
- **Отозванные** - сертификаты, которые были отозваны из **Реестра**. Доступны только для редактирования поля **Комментарий**.

Управление сертификатами

В колонке Управление:

- просмотр основной информации о сертификате.
- перевыпуск сертификата.
- скачать сертификат.
- удалить загруженный сертификат.
- отозвать сертификат.

Добавление сертификатов:

- **Загрузить пользовательский сертификат** - позволяет загрузить собственный или приобретенный сертификат как пользовательский, например, на конкретный домен, список доменов (Wildcard) или сервис.
- **Загрузить корневой сертификат** - позволяет загрузить собственный или приобретенный сертификат как корневой, который будет использоваться Ideco NGFW Novum для выпуска и подписания серверных сертификатов. Загруженный корневой сертификат не влияет на **Локальный УЦ** Ideco Client и не заменяет его.
- **Загрузить сертификат** - позволяет загрузить CA-сертификат стороннего удостоверяющего центра в формате `.pem`. Загруженные сертификаты используются как доверенные при проверке сертификатов устройств и могут быть выбраны в настройках авторизации и VPN-доступа.

Процесс выпуска сертификата

Описанный процесс относится к сертификатам, сгенерированным Ideco NGFW Novum (веб-интерфейс, VPN, почта и др.), и не применяется к сертификатам Ideco Client. Сертификаты Ideco Client выпускаются отдельным локальным удостоверяющим центром NGFW Novum. Но для авторизации через Ideco Client используется системный сертификат NGFW Novum на домен, указанный в **Пользователи → Ideco Client → Основное**. О выпуске сертификатов Ideco Client смотрите в статье.

Ideco NGFW Novum выполняет следующие действия:

1. Создает локальную цепочку сертификатов, подписанную корневым (самоподписанным) сертификатом.

2. Параллельно с созданием локальной цепочки сертификатов отправляет запрос на выпуск цепочки в Let's Encrypt.

Условия автоматического выпуска сертификатов Let's Encrypt:

- Наличие доменного имени, зарегистрированного на статический белый IP-адрес, который назначен на внешний интерфейс Ideco NGFW Novum.
- Открытый 80 TCP-порт на внешнем интерфейсе. После установки Ideco NGFW Novum 80 TCP-порт по умолчанию открыт во внешнюю сеть.

Если при соблюдении перечисленных выше условий сертификат Let's Encrypt не выпускается автоматически, перейдите в **Управление сервером** → **Терминал** веб-интерфейса Ideco NGFW Novum и воспользуйтесь командой:

```
systemctl restart ideco-cert-backend.service
```

Команда для просмотра логов:

```
journalctl -u ideco-cert-backend.service -f
```

3. При успешном выпуске цепочки сертификатов Let's Encrypt заменяет локальную цепочку.

4. Если выпуск цепочки сертификатов Let's Encrypt завершился неудачей, NGFW Novum продолжает использовать локальную цепочку сертификатов.

Если требуется повторить попытку получения сертификата Let's Encrypt вместо самоподписанного, то нужно нажать **Перевыпустить** в столбце **Управление**.

Сертификат Let's Encrypt **выпускается на 3 месяца** и будет **автоматически перевыпущен** по окончании срока действия.

С 17 версии Ideco NGFW Novum автоматически сгенерированные NGFW Novum пользовательские сертификаты выпускаются на **825 дней** и будут автоматически перевыпущены по окончании срока действия. В предыдущих версиях срок действия таких сертификатов составлял **10 лет**.

Процесс перевыпуска сертификата

Описанный процесс относится к сертификатам, сгенерированным Ideco NGFW Novum (веб-интерфейс, VPN, почта и др.), и не применяется к сертификатам Ideco Client. Сертификаты Ideco Client выпускаются отдельным локальным удостоверяющим центром NGFW Novum. Но для авторизации через Ideco Client используется сертификат NGFW Novum на домен, указанный в **Пользователи** → **Ideco Client** → **Основное**.

Некорневая цепочка сертификатов

Чтобы перевыпустить некорневую цепочку сертификатов, нажмите в столбце **Управление** таблицы **Действующие сертификаты**. Ideco NGFW Novum будет актуализировать цепочку следующим образом:

- Проверит загруженные сертификаты. Если сертификат найден, заменит действующую цепочку сертификатов на домен новой.
- Если для данного домена новые сертификаты не загружались, Ideco NGFW Novum обратится к Let's Encrypt для выпуска новой цепочки.
- Если цепочка от Let's Encrypt получена, она отобразится в таблице.
- Если получить цепочку сертификатов от Let's Encrypt не удалось, продолжит использовать локальную цепочку сертификатов.

Корневой сертификат

Для перевыпуска корневого сертификата нажмите напротив соответствующей цепочки в таблице **Загруженные сертификаты**. Ideco NGFW Novum заменит цепочку на автоматически сгенерированный корневой сертификат.

Для работы Ideco Client под macOS необходимо, чтобы срок действия сертификата на домен или IP-адрес Ideco NGFW Novum, введенный в разделе **Пользователи** → **Ideco Client**, не превышал 825 дней.

Проверить, что срок действия загруженного пользовательского или сгенерированного Ideco NGFW Novum сертификата не превышает **825 дней**, можно в **Сервисы** → **Сертификаты** → **Действующие сертификаты**, нажав .

Локальная цепочка сертификатов

Чтобы перевыпустить локальную цепочку сертификатов, выполните действия:

1. Перейдите в **Управление сервером** → **Терминал**.

2. Перейдите в директорию `/var/cache/ideco/cert-backend`, выполнив команду:

```
cd /var/cache/ideco/cert-backend
```

3. Выведите содержимое директории, выполнив команду `ls`.

4. Скопируйте название файла сертификата, который требуется перевыпустить. Названия файлов будут иметь вид:

`test.ideco.ru-self-sign_chain_833bcda78229059d2c2886548c75e9e3.pem`, где `test.ideco.ru` - доменное имя или IP-адрес, на который выпущен сертификат.

5. Удалите файл, выполнив команду:

```
rm test.ideco.ru-self-sign_chain_d1f73bf1fcc4d55ca31004ecb13d19b3.pem
```

6. Перейдите в **Сервисы** → **Сертификаты** → **Действующие сертификаты** и перевыпустите сертификат на домен или IP-адрес Ideco NGFW Novum, нажав  .

Чтобы проверить, перевыпустился ли сертификат на новый срок, нажмите  .

Полезные ссылки

- **Использование собственного CA-сертификата в Контент-фильтре**
- **Как установить сертификат Ideco NGFW на Android**
- **Настройка корневого и подчиненного центра сертификации с помощью AD CS**
- **Настройки в Ideco NGFW Novum**

Загрузка SSL-сертификата на сервер

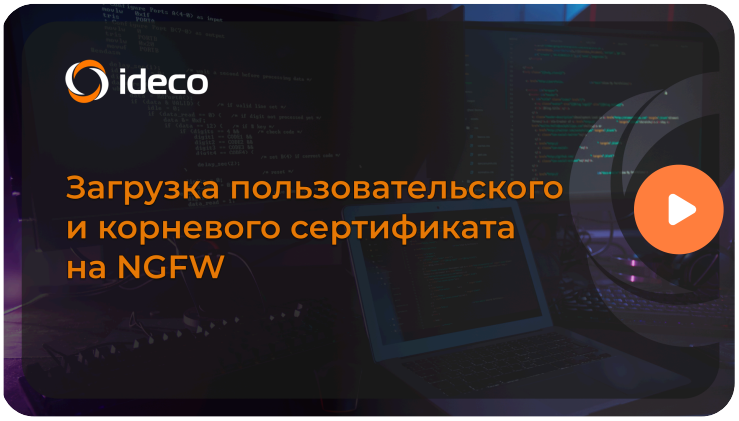
Классический контекст | Высокопроизводительный контекст

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE



Требования к сертификату

Перед загрузкой корневого или пользовательского сертификата на Ideco NGFW Novum убедитесь, что они отвечают следующим требованиям:

- **Формат файла.** Сертификаты должны иметь расширения **.pem**. Если у вашего сертификата другое расширение, конвертируйте сертификат. Как это сделать, описано ниже в разделе **Конвертация сертификата из формата pkcs12 в формат pem с помощью OpenSSL**.
- **Поле Common Name (CN).** В составе сертификата **Издатель** и **Субъект** должны содержать поле **Common Name** (общее имя). При загрузке собственной цепочки сертификатов **CN** последнего сертификата в цепочке должно соответствовать домену, для которого сертификат загружается.
- **Структура цепочки доверия.** Цепочка сертификата должна быть валидной и соответствовать структуре:

```
Приватный ключ
Сертификат на домен (Common Name)
Сертификат из состава бандла vendor-сертификатов (промежуточный сертификат, если есть)
...
Основной (корневой) сертификат
```

- **Уровень безопасности.** Сертификаты должны соответствовать минимально 3 или 4 уровню безопасности (Security Level 3-4) в соответствии со стандартами OpenSSL:
  - **Уровень 3** (128 бит):
    - Длина ключа: RSA - не менее 3072 бит. ECC - не менее 256 бит.
    - Версия TLS: Не ниже TLS 1.1.
    - Алгоритмы хеширования: Запрещено использование MD5 хеша.
    - Дополнительно: Отключены билеты сессии (Session Tickets).
  - **Уровень 4** (192 бита):
    - Длина ключа: RSA - не менее 7680 бит. ECC - не менее 384 бит.
    - Версия TLS: Не ниже TLS 1.2.
    - Алгоритмы хеширования: Запрещено использование SHA-1 для кода аутентификации сообщений (Message Authentication Code, MAC).

Если сертификат самоподписанный, его структура может содержать всего два блока - **Приватный ключ** и **Сертификат на домен (Common Name)**. Если структура сертификата невалидна, переходите к разделу ниже **Подготовка SSL-сертификата для загрузки на Ideco NGFW Novum**.

Если хотите загрузить сертификат как корневой, удостоверьтесь, что сертификат может выдавать дочерние сертификаты: **X509v3 Basic Constraints: CA: TRUE** (это можно проверить в открытом ключе сертификата).

Загрузка SSL-сертификата на Ideco NGFW Novum

Если сертификат удовлетворяет всем перечисленным выше условиям, загрузите его на Ideco NGFW Novum. Для этого:

1. Перейдите в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

2. Нажмите **Загрузить корневой сертификат** или **Загрузить пользовательский сертификат**.

3. Выберите нужный сертификат.

Загруженный корневой сертификат автоматически переподпишет все пользовательские сертификаты на домены, которые ранее автоматически сгенерировал Ideco NGFW Novum. Сертификаты Let's Encrypt и сертификаты, купленные у CA и Центров сертификации, переподписаны не будут.

Если в инфраструктуре компании есть свой корневой центр сертификации, выпустите сертификат с шаблоном **Subordinate Certification Authority** и загрузите его на Ideco NGFW Novum в качестве корневого. Это позволит выстроить цепочку доверия для автоматически выданных сертификатов до корневого центра сертификации. Пользовательские компьютеры будут доверять сертификатам, выданным на стороне Ideco NGFW Novum.

Подготовка SSL-сертификата для загрузки на Ideco NGFW Novum

При покупке доверенного SSL-сертификата на домен у Certificate Authority или Центра сертификации данные для его установки, как правило, высылаются электронным письмом в разрозненном виде. Для корректной загрузки сертификаты на домен промежуточные и корневые сертификаты нужно собрать в один файл в правильном порядке.

Некоторые данные (CSR-запрос и приватный ключ) генерируются только во время покупки SSL-сертификата и не высылаются в письме. Сразу сохраняйте такие данные на своем компьютере.

Корневые (самоподписанные) сертификаты также требуют построения цепочек. Структура таких сертификатов может содержать 2 блока - **Приватный ключ** и **Сертификат на домен (Common Name)** - или более в зависимости от того, есть ли у вас промежуточные сертификаты (из состава бандла vendor-сертификатов).

Для создания корректной цепочки сертификатов выполните действия:

1. Создайте текстовый файл вида:

```
-----BEGIN PRIVATE KEY-----
.....
.....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
```

2. Добавьте в блок (**BEGIN PRIVATE KEY**) ***расшифрованный*** приватный ключ.

Если Центр сертификации выдал приватный ключ в зашифрованном виде, расшифруйте его с помощью passphrase (фразы-пароля).

3. В каждый из блоков (**BEGIN CERTIFICATE**) добавьте сертификат. В начало - сертификат на домен, следом - сертификаты из бандла vendor-сертификатов (если они есть), в самый конец - корневой сертификат. Файл должен получить такую структуру:

```
Приватный ключ
Сертификат на домен
Сертификат из состава бандла vendor-сертификатов (при наличии)
...
Основной (корневой) сертификат
```

4. Сохраните файл с расширением **.pem** и загрузите его на Ideco NGFW Novum.

Конвертация сертификата из формата pkcs12 в формат pem с помощью openssl

> Для конвертации сертификата с помощью openssl на Windows воспользуйтесь ссылкой для загрузки OpenSSL на компьютер.

Для конвертации сертификата из формата **pkcs12** в формат **pem** выполните действия:

1. Откройте командную строку.

2. Введите команду `openssl pkcs12 -in certificate.pkcs12 -out certificate.pem` (сконвертирует сертификат в нужный формат), где:

- **certificate.pkcs12** - исходный сертификат который был получен у центра сертификации.
- **certificate.pem** - результат конвертации.

3. Откройте полученный файл и убедитесь, что файл имеет структуру:

```
-----BEGIN CERTIFICATE-----
..............
..............
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
..............
..............
-----END PRIVATE KEY-----
```

Если в сертификате написано `--BEGIN ENCRYPTED PRIVATE KEY--`, расшифруйте его, введя в OpenSSL команду

`openssl rsa -in certificate.pem -out certificate_decoded.pem`, где:

- **certificate.pem** - файл который был получен после конвертации.
- **certificate_decode.pem** - результат расшифровки.

Слабый ключ RSA в корневом сертификате

При загрузке сертификата с RSA-ключом 1024 бит или меньше возникает ошибка:



Сертификат считается криптографически слабым и небезопасным. Рекомендуется минимум 2048 бит для RSA.

Для изменения RSA-ключа выполните действия:

1. Откройте командную строку.

2. Проверьте размер ключа сертификата:

```
openssl x509 -in client_cert.pem -text -noout | grep "Public-Key"
```

- `client_cert.pem` - имя файла сертификата.

Пример результата:

```
Public-Key: (1024 bit)
```

3. Сгенерируйте новый RSA-ключ:

```
openssl genpkey -algorithm RSA -out client_new.key -pkeyopt rsa_keygen_bits:2048
```

- `client_new.key` - имя файла, в который будет сохранен новый приватный ключ.
- `rsa_keygen_bits` - 2048 или 4096 бит.

4. Создайте запрос на выпуск сертификата - CSR (Certificate Signing Request):

```
openssl req -new -key client_new.key -out client_new.csr -subj "/C=RU/ST=Moscow/L=Moscow/O=Company/OU=IT/CN=client.example.co
```

- `client_new.key` - имя файла с новым приватным ключом.
- `client_new.csr` - имя файла, куда сохранится запрос на сертификат.
- `"/C=RU/ST=Moscow/L=Moscow/O=Company/OU=IT/CN=client.example.com"` - данные субъекта сертификата:
  - `C` - страна.
  - `ST` - регион/штат.
  - `L` - город.
  - `O` - организация.
  - `OU` - подразделение.
  - `CN` - Common Name, имя сертификата.

5. Отправьте CSR в CA (сертификационный центр). В результате будет получен новый сертификат `client_new.crt` с указанным в пункте 3 размером RSA-ключа.

6. Загрузите новый сертификат в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**, нажав кнопку **Загрузить корневой сертификат**.

Создание самоподписанного сертификата с помощью PowerShell

Классический контекст | Высокопроизводительный контекст

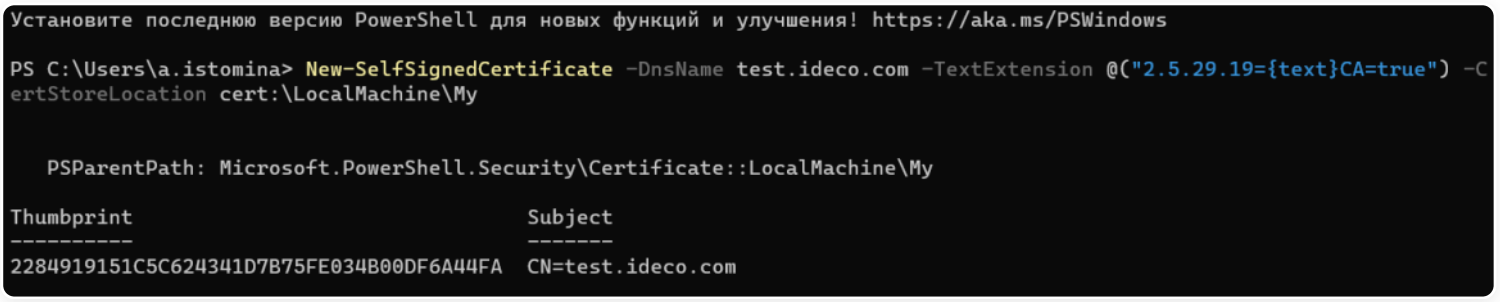
Чтобы создать корневой (самоподписанный) сертификат с помощью PowerShell, выполните следующие действия:

1. Запустите PowerShell от имени администратора.

2. Сгенерируйте сертификат, выполнив команду:

```
New-SelfSignedCertificate -DnsName test.ideco.com -TextExtension @("2.5.29.19={text}CA=true") -CertStoreLocation cert:\LocalM
```

Где `test.ideco.com` - домен.



Для просмотра сгенерированного сертификата выполните команду `certlm.msc`.

3. Сформируйте пароль для сертификата:

```
$CertPassword = ConvertTo-SecureString -String “12345” -Force -AsPlainText
```

Где `12345` - пароль.

4. Экспортируйте сертификат выполнив команду:

```
Export-PfxCertificate -Cert cert:\LocalMachine\My\2284919151C5C624341D7B75FE034B00DF6A44FA -FilePath C:\Users\pende\ssl\test.
```

- `2284919151C5C624341D7B75FE034B00DF6A44FA` - идентификатор сертификата полученный на шаге 2;
- `C:\Users\pende\ssl\test.ideco.pfx` - путь до папки, в которую требуется сохранить сертификат (проверьте корректность сертификата во избежание ошибок).

5. Конвертируйте сертификат в расширение .pem (пример конвертора).

Для загрузки сертификата на сервер воспользуйтесь статьей Загрузка SSL-сертификата на сервер

Создание самоподписанного корневого сертификата с помощью OpenSSL

Классический контекст | Высокопроизводительный контекст

Для генерации самоподписанного корневого сертификата с применением эллиптической кривой (ECC) выполните действия:

1. Сгенерируйте ECDSA-ключ:

```
openssl ecparam -name prime256v1 -genkey -out ecc-key.pem
```

- `ecparam` - работа с параметрами эллиптических кривых.
- `-name prime256v1` - выбор эллиптической кривой **NIST P-256**.
- `-genkey` - генерация нового приватного ключа.
- `-out ecc-key.pem` - сохранение ключа в файле **ecc-key.pem**.

2. Создайте самоподписанный сертификат:

```
openssl req \
-x509 \
-new \
-key ecc-key.pem \
-out cert.pem \
-days 3650 \
-sha256 \
-subj "/CN=MyRootCA/C=RU/ST=SomeState/L=SomeCity/O=MyOrganization/OU=RootCA" \
-nodes \
-addext "authorityKeyIdentifier=keyid,issuer" \
-addext "basicConstraints=CA:TRUE" \
-addext "keyUsage = keyCertSign, cRLSign, digitalSignature"
```

- `req -x509` - создание самоподписанного сертификата.
- `-new` - генерация нового запроса.
- `-key ecc-key.pem` - использование ранее сгенерированного ECC-ключа.
- `-out cert.pem` - сохранение сертификата в файле cert.pem.
- `-days 3650` - установка срока действия сертификата на 10 лет (3650 дней).
- `-sha256` - использование хеш-алгоритма SHA-256 для подписи.
- `-subj` - указание subject. Поле Common Name (CN) требует обязательного заполнения. При необходимости можно указать и другие поля:
  - `/CN=MyRootCA` - наименование сертификата.
  - `C=RU` - код страны в формате ISO 3166-1 alpha-2 (например, RU).
  - `ST=SomeState` - название региона или области (например, Moscow).
  - `L=SomeCity` - название города (например, Saint Petersburg).
  - `O=MyOrganization` - название организации.
  - `OU=RootCA` - название подразделения организации.
- `-nodes` - отсутствие шифрования приватного ключа паролем.
- `-addext "authorityKeyIdentifier=keyid,issuer"` - указание метода идентификации центра сертификации (CA) для цепочки сертификатов.
- `-addext basicConstraints=CA:TRUE"` - присвоение статусу сертификата CA, что позволяет подписывать другие сертификаты.
- `-addext "keyUsage = keyCertSign, cRLSign, digitalSignature"` - разрешение на выполнение цифровых подписей, подписей сертификатов и подписей списков отозванных сертификатов (CRL):
  - `keyCertSign` - может использоваться для подписи других сертификатов.
  - `cRLSign` - может использоваться для подписи CRL (Certificate Revocation List).
  - `digitalSignature` - может использоваться для цифровой подписи данных (параметр необязателен).

Результат: создание самоподписанный сертификата `cert.pem`, который:

- Включает приватный ECDSA-ключ `ecc-key.pem`.

- Действует как центр сертификации (CA) и может подписывать другие сертификаты.
- Включает Common Name: MyRootCA.
- Подписан алгоритмом SHA-256.
- Действителен в течение 10 лет.

Для загрузки сертификата на сервер воспользуйтесь статьей Загрузка SSL-сертификата на сервер

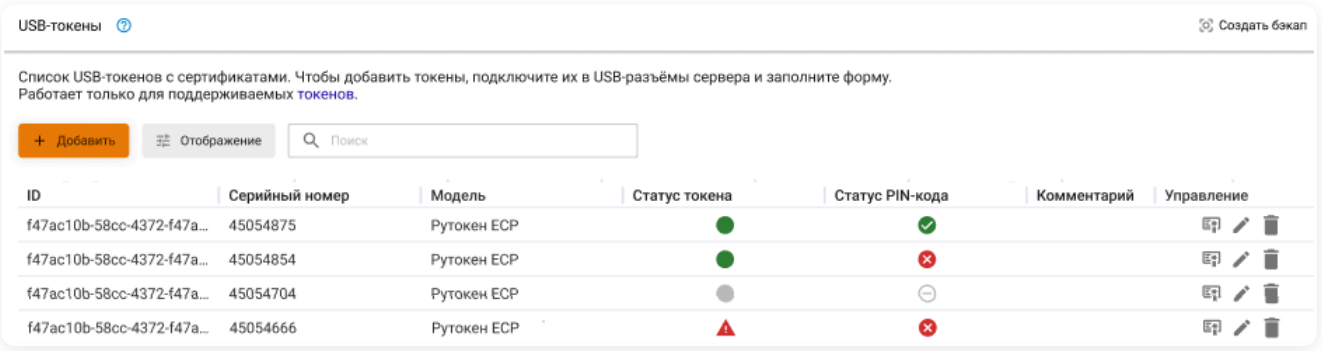
USB-токены

Функциональность доступна только в **Системном контексте**.

USB-токен - это аппаратное устройство для безопасного хранения цифровых сертификатов и работы с приватными ключами.

Ideco NGFW Novum поддерживает только USB-токен модели **Рутокен ЭЦП 3.0**. USB-токены других моделей могут не отображаться в веб-интерфейсе **Ideco NGFW Novum**.

В таблице USB-токенов представлена информация о серийном номере, модели, метке ключа и корректности настройки USB-токена:



Статусы токена

- токен подключен в USB-разъем сервера.

- токен не подключен в USB-разъем сервера.

- возникла ошибка или токен заблокирован.

Статусы PIN-кода

- верный PIN-код.

- неизвестный статус PIN-кода:

- PIN-код был введен, но USB-токен не был установлен в USB-разъем сервера.
- USB-токен с верным PIN-кодом был извлечен из USB-разъема сервера.

- неверный PIN-код.

Чтобы проверить содержимое USB-токенов и убедиться, что на токены загружены все необходимые сертификаты, нажмите на у соответствующего USB-токена.

Подготовка USB-токена

На USB-токен необходимо загрузить два сертификата: доверенный сертификат и сертификат с приватным ключом, который будет использоваться в качестве локального сертификата NGFW. При подготовке USB-токена запишите серийный номер и PIN-код. Это потребуется для дальнейшей настройки.

Пример генерации сертификатов приведен в статье.

Процесс подготовки USB-токена ЭЦП версии 3.0 от компании **Рутокен** подробно описан в документации производителя. В помощь предлагаются статьи, которые помогут разобраться как узнать серийный номер, сменить PIN-код и загрузить сертификаты на USB-токен:

- Панель управления Рутокен для ОС Windows
- Центр Управления Рутокен для ОС GNU/Linux
- Рутокен и OpenSSL
- Рутокен для КриптоПро

Если требуется сгенерировать сертификаты для тестирования ГОСТ VPN, рекомендуем воспользоваться статьей от производителя.

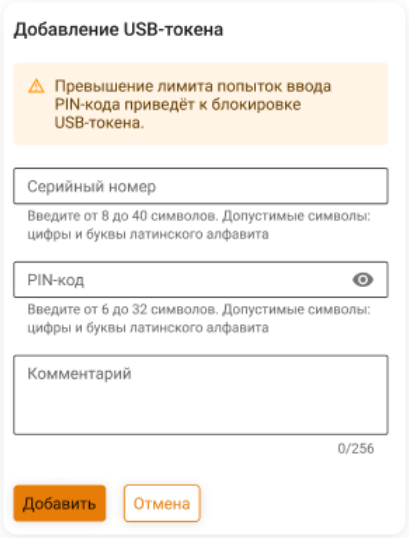
Настройка USB-токена на Ideco NGFW Novum

Перед добавлением USB-токена на Ideco NGFW Novum смените PIN-код пользователя, поскольку изначально на токенах от компании Рутокен установлен PIN-код по умолчанию: `12345678`. Инструкция по смене PIN-кода - по ссылке.

Для работы Ideco NGFW Novum с USB-токеном введите корректный PIN-код. NGFW Novum использует PIN-код для получения доступа к токену сразу после ввода и сохранения параметров токена. Если PIN-код не верный, NGFW Novum остановит попытки получить доступ до ввода и сохранения нового PIN-кода.

При превышении лимита попыток неправильного ввода PIN-кода устройство будет заблокировано. Лимит устанавливается производителем и считается до правильного ввода PIN-кода.

Чтобы добавить новый USB-токен, подключите USB-токен к USB-разъему вашего сервера. Нажмите **Добавить** и заполните поля:



- **Серийный номер** - формат для **Рутокен ЭЦП 3.0** представлен в виде десятизначного числа. Например, `1157977130`. Его можно найти на корпусе USB-токена или:
  - Для Linux - в Центре управления Рутокеном в разделе Об устройстве.
  - Для Windows - в Панели управления Рутокеном
- **PIN-код** - введите установленный ранее PIN-код пользователя.
- **Комментарий** - необязательное поле.

Netflow

Классический контекст | Высокопроизводительный контекст | API

Netflow - проприетарный открытый протокол, разработанный Cisco для мониторинга статистики трафика в сети. Ideco NGFW Novum выступает в качестве сенсора-экспортера, который собирает статистику при прохождении через него трафика.

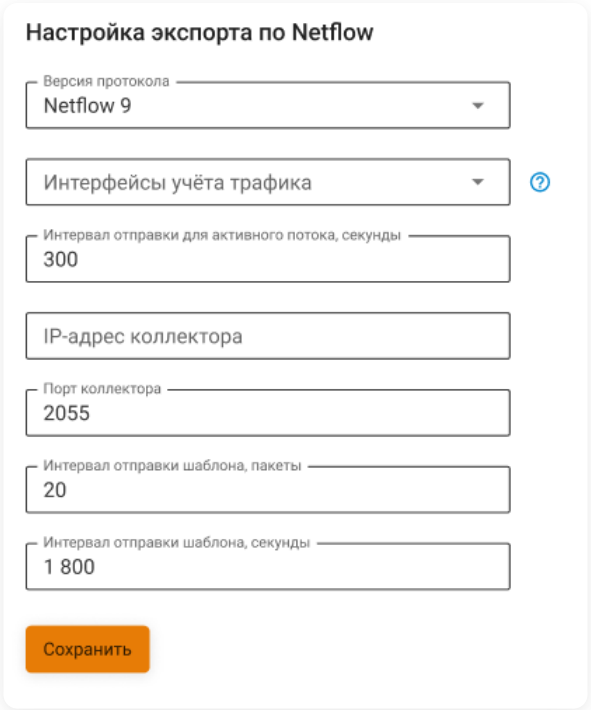
Netflow обеспечивает сбор информации об IP-трафике, обрабатываемом сетевыми устройствами (L3-коммутаторы, маршрутизаторы, сенсоры). Каждый поток является однонаправленным, т.е. каждое двунаправленное соединение **src <–> dst** интерпретируется как два потока: **src → dst** и **dst → src**.

Настройка экспорта по Netflow

При включении Netflow рекомендуем настроить индексы Netflow для интерфейсов, статистику по которым планируется передавать. Это можно сделать в настройках сетевых интерфейсов, значение по умолчанию - 0. Индексы Netflow не меняются при включении/выключении или изменении интерфейса.

Идентификаторами потоков служат индексы Netflow. Потоки с одинаковыми индексами для сбора статистики проходят через один интерфейс учета трафика.

Для настройки Netflow перейдите в **Сервисы → Netflow**:



- **Версия протокола** - выберите версию протокола Netflow. Доступны Netflow 5, Netflow 9 (по умолчанию) и Netflow 10 (IPFIX).
- **Интерфейсы учета трафика** - выберите интерфейсы, трафик которых хотите отслеживать. Если не заполнены, статистика не будет экспортироваться.
- **Интервал отправки для активного потока, секунды** - введите временной интервал, через который Ideco NGFW Novum будет отправлять на коллектор отчеты по потокам, которые не успели завершиться (информация о завершенных потоках отправляется по завершении). Допустимые значения: от 60 до 3600, по умолчанию - 300.
- **IP-адрес коллектора** - введите IP-адрес коллектора данных. Если не заполнен, статистика не будет экспортироваться.
- **Порт коллектора** - введите номер UDP-порта коллектора данных, используемого для приема пакетов Netflow.
- **Интервал отправки шаблона, пакеты** - количество пакетов, через которое на коллектор будет послан шаблон. Допустимые значения: от 10 до 600, по умолчанию - 20. Доступно только при выборе Netflow 9 или Netflow 10 (IPFIX) в поле **Версия протокола**.
- **Интервал отправки шаблона, секунды** - количество секунд, через которое на коллектор будет послан шаблон. Допустимые значения: от 60 до 86400, по умолчанию - 1800. Доступно только при выборе Netflow 9 или Netflow 10 (IPFIX) в поле **Версия протокола**.

При сборе статистики с интерфейсов Ethernet + PPTP/L2TP/PPPoE будет учитываться трафик не на родительском Veth, а на PPP-интерфейсе (Eppp), трафик с которого инкапсулируется в родительский.

Данные в Netflow передаются по протоколу UDP. Поэтому пока коллектор не получит шаблон передаваемых данных, отчеты будут игнорироваться. Правильная настройка полей **Интервал отправки шаблона** позволяет минимизировать потери при перезагрузке или потере связи с коллектором.

Структура передаваемых на коллектор данных

Структура заголовка и записей для Netflow 5 доступна по ссылке.

Структура шаблона для Netflow 9 и Netflow 10 (IPFIX) представлена в таблице:

Поле	Код поля	Длина поля, байт	Описание
IPV4_SRC_ADDR	8	4	IP-адрес источника
IPV4_DST_ADDR	12	4	IP-адрес назначения
INPUT_SNMP	10	2	Индекс входящего интерфейса
OUTPUT_SNMP	14	2	Индекс исходящего интерфейса
IN_BYTES	1	8	Количество байт, переданных в потоке
IN_PKTS	2	8	Количество пакетов, переданных в потоке
FIRST_SWITCHED	22	4	Время начала потока (sys uptime ms)
LAST_SWITCHED	21	4	Время последнего прохождения трафика в потоке (sys uptime ms)
L4_SRC_PORT	7	2	Порт источника
L4_DST_PORT	11	2	Порт назначения
TCP_FLAGS	6	1	Флаги TCP (суммарно зафиксированные за время наблюдения потока)
PROTOCOL	4	1	Код протокола
SRC_MASK	9	1	Маска IP-адреса источника
DST_MASK	13	1	Маска IP-адреса назначения

Syslog

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Syslog**: `ideco-logs-backend`, `ideco-monitor-backend`.

Список служб для других разделов доступен по ссылке.

Syslog - стандартный протокол для сбора, передачи и хранения системных сообщений от устройств и сервисов. Обеспечивает централизованный сбор информации о событиях в сети.

В Ideco NGFW Novum **Syslog** используется для отправки логов на удаленный сервер. Это позволяет администраторам осуществлять мониторинг безопасности, анализировать инциденты, выполнять диагностику проблем.

Пересылка системных сообщений

Чтобы настроить пересылку системных сообщений, перейдите в раздел **Сервисы** → **Syslog** и выполните действия:

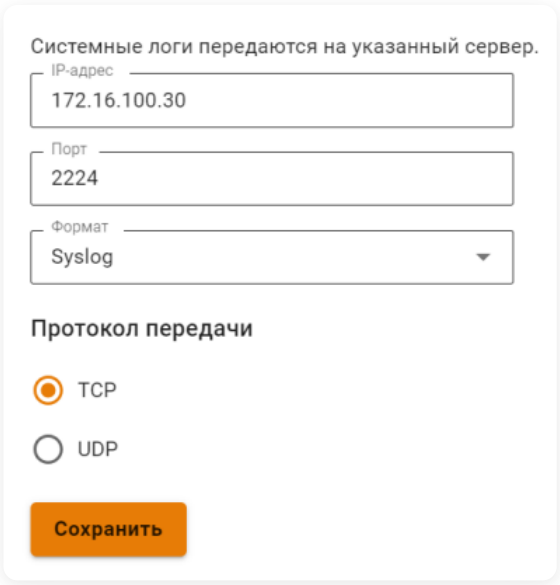
1. Укажите IP-адрес сервера-коллектора (любой локальный или публичный IP-адрес).

2. В поле **Порт** укажите порт, настроенный на сервере-коллекторе (в диапазоне от 1 до 65535).

3. Выберите формат передаваемых системных сообщений (Syslog или CEF).

4. Выберите протокол передачи системных логов - TCP или UDP.

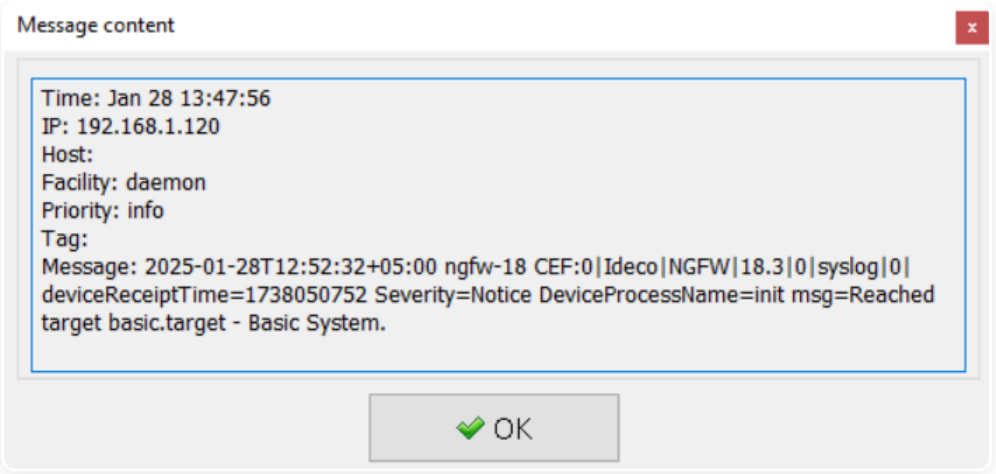
5. Нажмите **Сохранить** и включите опцию Syslog:



Рекомендуется передавать логи по протоколу TCP, так как он гарантирует доставку и соблюдает последовательность сообщений.

Расшифровка передаваемых логов

В статье представлены примеры сообщений (message) в форматах CEF и Syslog (скриншот из Visual Syslog server):



Message начинается со строки вида:

CEF

```
2024-11-18T15:38:54+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1759402874 Severity=Informational
```

где:

- `2024-11-18T15:38:54+05:00` - время события в Ideco NGFW Novum;
- `ideco-ngfw` - hostname сервера NGFW Novum, заданный в левом верхнем углу веб-интерфейса;
- `CEF:0` - версия формата CEF;
- `Ideco` - вендор;
- `NGFW` - название продукта;
- `21.0` - версия продукта;
- `0|syslog|0` - идентификатор лога, постоянный для NGFW Novum. Состоит из трех полей: идентификатор типа события, описание события, важность события.
- `deviceReceiptTime` - время события в системе NGFW Novum, может не совпадать с временем получения события по Syslog;
- `Severity` - уровень значимости события. Возможные значения:
  - `Emergency` - чрезвычайная ситуация;
  - `Alert` - тревога;
  - `Critical` - критическая ошибка;
  - `Error` - ошибка;
  - `Warning` - предупреждение;
  - `Notice` - уведомление;
  - `Informational` - информация;
  - `Debug` - отладка.

Syslog

```
2025-08-27T11:38:13+05:00 ideco-ngfw traffic-journal
```

где:

- `2025-08-27T11:38:13+05:00` - время события в Ideco NGFW Novum;
- `ideco-ngfw` - hostname сервера NGFW Novum, заданный в левом верхнем углу веб-интерфейса.

Уровень значимости события, передаваемый в столбец **Priority**:

- `emerg` - чрезвычайная ситуация;
- `alert` - тревога;
- `crit` - критическая ошибка;
- `err` - ошибка;
- `warning` - предупреждение;
- `notice` - уведомление;
- `info` - информация;

- `debug` - отладка.

Журнал Система

CEF:

```
2026-02-20T14:44:24+05:00 bez-nazvaniya-8fbd0bda-5d9d-4354-8bda-3c49bbcdf23b CEF:0|Ideco|NGFW|21.11|0|syslog|0|deviceReceiptT
```

Syslog:

```
2026-02-20T14:31:30+05:00 bez-nazvaniya-8fbd0bda-5d9d-4354-8bda-3c49bbcdf23b kav-scanner - - - Update in progress, 6 complete
```

Ключ	Описание	
DeviceProcessName	<название_службы>	Название источника журнала. Список всех служб доступен по ссылке

SIEM не сможет извлечь ключевые поля из сообщений журнала для последующего анализа. Такие сообщения доступны только для просмотра в исходном виде. С другими примерами можно ознакомиться по ссылке.

Журнал Трафик

CEF:

```
2025-08-27T11:38:13+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.1|0|syslog|0|deviceReceiptTime=1759385517 Severity=Informational dev
```

Syslog:

```
2025-08-27T11:38:13+05:00 ideco-ngfw traffic-journal - - - result:accept, rule_id:2, table:inp, action:l7_inspection, ips_pro
```

Ключ CEF	Ключ Syslog	Описание
deviceProcessName	traffic-journal	Название источника журнала
outcome	result	Общий результат проверки. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет
deviceEventClassId	rule_id	Идентификатор правила **Межсетевого экрана**. Пустая строка означает отсутствие значения.
name	table	Название таблицы, в которой сработало правило. Возможные значения: • `absent` - отсутствие значения; • `fwd` - таблица **FORWARD** раздела **Межсетевой экран** Ideco NGFW Novum; • `fwd_a` - постправило FORWARD Ideco Center; • `fwd_b` - предправило FORWARD Ideco Center; • `fwd_s` - системное правило FORWARD; • `inp` - таблица **INPUT** раздела **Межсетевой экран** Ideco NGFW Novum; • `inp_a` - постправило INPUT Ideco Center; • `inp_b` - предправило INPUT Ideco Center; • `inp_s` - системное правило INPUT.
act	action	Действие правила **Межсетевого экрана**. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет • `l7_inspection` - перенаправление в профиль безопасности
cs1	ips_profile	Название IPS профиля

cn1	ips_action	Действие IPS профиля. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет
cn2	ips_signature_id	Идентификатор сигнатуры, сработавшей в профиле
cs2	dpi_profile	Название DPI профиля
cn3	dpi_action	Действие DPI профиля. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет
destinationServiceName	dpi_app	Название приложения
app	dpi_protocol	Название протокола прикладного уровня
proto	protocol	Название протокола
sourceAddress	src_ip	IP-адрес источника
sourcePort	src_port	Порт источника. Значение `0` - отсутствие данных
sourceZoneExternalID	src_zone	Название зоны источника
suser	src_user_name	Имя пользователя источника
suid	src_user_login	Логин пользователя источника
spriv	src_group	Название группы источника
cs3	src_location_name	Название локации источника
-	src_location_code	Код локации источника
destinationAddress	dst_ip	IP-адрес назначения
destinationPort	dst_port	Порт назначения. Значение `0` - отсутствие данных
destinationZoneExternalID	dst_zone	Название зоны назначения
duser	dst_user_name	Имя пользователя назначения
duid	dst_user_login	Логин пользователя назначения
dpriv	dst_group	Название группы назначения
cs4	dst_location_name	Название локации назначения
-	dst_location_code	Код локации назначения
cs5	dnat_rule_id	Идентификатор DNAT-правила. Пустая строка - отсутствие значения
destinationTranslatedAddress	dnat_ip	IP-адрес, на который был изменен адрес назначения
destinationTranslatedPort	dnat_port	Порт, на который был изменен порт назначения
cs6	snat_rule_id	Идентификатор SNAT-правила. Пустая строка - отсутствие значения
sourceTranslatedAddress	snat_ip	IP-адрес, на который был изменен адрес источника
deviceExternalId	cluster_id	Идентификатор кластера
-	cluster_name	Название кластера
externalId	vce_id	Идентификатор VCE
-	vce_name	Название VCE
eventId	flow_id	Идентификатор соединения. Уникален для каждой записи
start	nflog_timestamp	Служебная информация

Журнал Веб-трафик

CEF:

```
2025-10-02T16:01:14+05:00 ngfw CEF:0|Ideco|NGFW|21.1|0|syslog|0|deviceReceiptTime=1759402874 Severity=Informational DevicePro
```

Syslog:

```
2025-08-27T11:43:05+05:00 ideco-ngfw web-proxy - - - domain:st3-24.vk.com, uri:, categories:['РЎРѕС†РёР°Р»СЊРЅС‹Рµ СЃРµС‚Рё']
```

Ключ CEF	**Ключ Syslog**	**Описание**

DeviceProcessName	web-proxy	Название источника журнала
DestinationHostName	domain	Домен сайта
RequestUrl	uri	URI сайта, включающий все, кроме доменного имени и якорей
cat	categories	Список категорий, по которым был классифицирован сайт
in	incoming_traffic	Входящий трафик, байт
out	outgoing_traffic	Исходящий трафик, байт
FlexNumber1	traffic_amount	Общий трафик, байт
deviceAction	action	Результат проверки Контент-фильтра. Возможные значения: • `bump` - расшифровать • `allow` - разрешить • `deny` - запретить • `redirect` - перенаправить на другой сайт. Действует только на расшифрованный трафик
reason	blocked_reason	Причины блокировки: имя категории, имя словаря, HTTP-метод или MIME-тип, по которым был запрещен доступ к сайту
cs1	redirected_to	Если запрос попал под правило перенаправления, отображает url куда перенаправило, если нет - пустая строка
cs2	rule_name	Название правила Контент-фильтра
SourceAddress	source_ip	IP-адрес источника
SourcePort	source_port	Порт источника, число
DestinationAddress	destination_ip	IP-адрес назначения. Значение `0.0.0.0` означает отсутствие адреса назначения
DestinationPort	destination_port	Порт назначения, число. Значение `0` - отсутствие данных
ApplicationProtocol	proto_info	Версия HTTP-протокола. Отсутствие данных отображается пустой строкой
requestMethod	method	Метод, с которым был произведен запрос. Отсутствие данных отображается пустой строкой. При отображении в таблице GET-запрос - скачивание, остальные запросы - загрузка
Code	status_code	Код HTTP-ответа. Значение `0` - отсутствие данных
cs3	mime	Content-Type HTTP-запроса. Отсутствие данных отображается пустой строкой
requestClientApplication	useragent	User-Agent HTTP-запроса. Отсутствие данных отображается пустой строкой
cs4	user_name	Имя пользователя, который авторизован с IP источника
-	login	Логин пользователя
cs5	group_name	Имя группы, в которую входит пользователь
cs6	referer	Referer HTTP-запроса. Отсутствие данных отображается пустой строкой
cs7	vce_id	Идентификатор VCE
cs8	vce_name	Название VCE

Предотвращение вторжений

CEF:

```
2025-10-03T14:06:02+05:00 ngfw CEF:0|Ideco|NGFW|21.1|0|syslog|0|deviceReceiptTime=1759482362 Severity=Warning DeviceCustomStr
```

Syslog:

```
2025-10-03T14:01:38+05:00 ngfw suricata - - - flow_id:2113278673659098, in_iface:, sensor_name:ideco-ips, event_type:alert, s
```

Ключ CEF	**Ключ Syslog**	**Описание**
-	suricata	Название источника журнала
DeviceCustomString1	flow_id	Внутренний идентификатор системы **Предотвращения вторжений** flow (сессии)
DeviceInboundInterface	in_iface	Идентификатор входящего интерфейса
DeviceProcessName	sensor_name	Имя экземпляра системы **Предотвращения вторжений**
DeviceCustomString5	event_type	Тип события
SourceAddress	src_ip	IP-адрес источника

DeviceCustomString1	src_ip_type	Принадлежность адреса источника. Возможные значения: • `local` - локальный • `external` - внешний • `unknown` - принадлежность не определена
SourcePort	src_port	Порт источника
SourceCountry	src_country	Название местоположения источника
DeviceCustomString2	src_country_code	ISO-код страны источника
DeviceCustomString3	src_session_uuid	Внутренний идентификатор сессии Ideco NGFW Novum источника
SourceUserID	src_user_id	Идентификатор пользователя источника
SourceUserName	src_user_name	Имя пользователя источника
DestinationAddress	dest_ip	IP-адрес назначения
DeviceCustomString4	dest_ip_type	Принадлежность адреса назначения. Возможные значения: • `local` - локальный • `external` - внешний • `unknown` - принадлежность не определена
DestinationPort	dest_port	Порт назначения
DestinationCountry	dest_country	Название местоположения назначения
DeviceCustomString5	dest_country_code	ISO-код страны назначения
DeviceCustomString6	dest_session_uuid	Внутренний идентификатор сессии Ideco NGFW Novum назначения
DestinationUserID	dest_user_object_id	Идентификатор пользователя назначения
DestinationUserName	dest_user_name	Имя пользователя назначения
TransportProtocol	proto	Протокол
DeviceEventClassID	alert.signature_id	Идентификатор правила системы предотвращения вторжений
Message	alert.signature	Сообщение из сработавшего правила
DeviceEventCategory	alert.category	Описание колонки в веб-интерфейсе **События безопасности**. Соответствие `alert.category` → `alert.signature` описаны в файле.
Severity	alert.severity	Уровень угрозы, может принимать значения `1`, `2`, `3` и `256`, где `1` - самый высокий уровень угрозы
DeviceCustomString8	alert.gid	GID угрозы
DeviceCustomString9	alert.action	Действие по отношению к угрозе. Возможные значения: • `blocked` - блокировать • `allowed` - разрешить

Служебные поля результата анализа HTTP-трафика. Заполняются, если в процессе анализа трафика был определен HTTP-протокол:

DestinationHostName	http.hostname	Идентификатор хоста
RequestUrl	http.url	URL, на который был запрос
RequestClientApplication	http.http_user_agent	Информация, идентифицирующая HTTP-клиента

Служебные поля flow (сессии):

FlexNumber1	flow.pkts_toserver	Количество пакетов, переданное от клиента к серверу
FlexNumber2	flow.pkts_toclient	Количество пакетов, переданное от сервера к клиенту
BytesIn	flow.bytes_toserver	Количество байт, переданное от клиента к серверу
BytesOut	flow.bytes_toclient	Количество байт, переданное от сервера к клиенту
StartTime	flow.start	Начало сессии
EndTime	flow.end	Окончание сессии
FlexNumber3	flow.age	Возраст сессии
DeviceCustomString11	flow.state	Текущее состояние
DeviceCustomString12	flow.reason	Запущен ли IPsec в режиме отладки
FlexNumber4	flow.alerted	Сгенерировался ли поток `alert`

Состояние флага TCP flow(сессии):

DeviceCustomString14	tcp.tcp_flags	Значение поля flags в заголовке TCP
DeviceCustomString15	tcp.tcp_flags_ts	Timestamp флаги.
DeviceCustomString16	tcp.tcp_flags_tc	Флаг Truncated response
FlexNumber5	tcp.cwr	Флаг TCP-пакета, информирующий отправителя, что получен пакет с установленным флагом ECE (Подробнее в RFC 3186)
FlexNumber6	tcp.ecn	Флаг TCP-пакета, информирующий получателя, что узел способен на явное уведомление о перегрузке сети
FlexNumber7	tcp.urg	Флаг TCP-пакета, указывающий важность пакета
FlexNumber8	tcp.ack	Флаг получения TCP-пакета
FlexNumber9	tcp.psh	Флаг TCP-пакета, информирующий получателя, что все данные переданы и можно передать их приложению
FlexNumber10	tcp.rst	Флаг TCP-пакета, указывающий, что соединение завершено в аварийном режиме
FlexNumber11	tcp.syn	Флаг TCP-пакета, отвечающий за установку соединения
FlexNumber12	tcp.fin	Флаг TCP-пакета, указывающий на завершение соединения в штатном порядке
DeviceCustomString17	tcp.state	Состояние сеанса TCP

Ключ	**Описание**	
DeviceCustomString18	vce_id	Идентификатор VCE
DeviceCustomString19	vce_name	Название VCE

Журнал Web Application Firewall

CEF:

```
2026-04-03T15:36:50+05:00 ideco-ngfw CEF:0|Ideco|NGFW|22.0|0|syslog|0|rt=1775212610 deviceProcessName=modsecurity act=allowed
```

Syslog:

```
2026-04-03T15:32:10+05:00 ideco-ngfw waf - - - id:01KN9ED1B23GT115YHSM406MKJ, blocked:true, rule_file:/run/ideco-reverse-back
```

Ключ CEF	**Ключ Syslog**	**Описание**
deviceProcessName	waf	Название источника журнала
rt	-	Время события в формате Unix Timestamp
act	blocked	Действие, выполненное WAF. Возможные значения: • `allowed` - запрос пропущен • `blocked` - запрос заблокирован
msg	message	Текстовое сообщение из сработавшего правила
reason	nginx_message	Описание причины срабатывания правила
cat	category_name	Название категории правила
externalId	unique_id	Уникальный идентификатор HTTP-запроса
deviceExternalId	vce_id	Идентификатор VCE
requestMethod	-	HTTP-метод запроса: `GET`, `POST`
request	uri	URI запроса с параметрами строки запроса
src	nginx_client	IP-адрес источника
dst	nginx_server	IP-адрес назначения
dhost	nginx_host	Имя хоста защищаемого ресурса
filePath	rule_file	Путь к файлу с правилом, по которому сработал WAF
cs1	profile_id	Идентификатор профиля WAF
cs2	profile_name	Название профиля WAF
cs3	category_id	Идентификатор категории правила
cs4	ruleset_ver	Версия набора правил
cs5	ref	Координаты совпадения в запросе
cs6	data	Данные, которые послужили причиной срабатывания правила
cn1	rule_id	Идентификатор правила

cn2	rule_line	Номер строки в файле правил
cn3	severity	Уровень критичности правила. Возможные значения: • `0` - EMERGENCY • `1` - ALERT • `2` - CRITICAL • `3` - ERROR • `4` - WARNING • `5` - NOTICE • `6` - INFO • `7` - DEBUG
flexString1	nginx_client_country	Название местоположения источника
flexString2	tags	Теги правила, разделенные пробелом
sproc	vce_name	Название VCE
-	id	Идентификатор события в журнале WAF
-	hostname	Имя защищаемого ресурса
-	nginx_client_country_code	ISO-код страны источника
-	nginx_request	Стартовая строка HTTP-запроса (метод, URI, версия протокола)

Журнал Действия администраторов

CEF:

```
2026-01-21T12:52:57+05:00 bez-nazvaniya-2a6874b3-8156-4591-af99-4edc1e9f24d9 CEF:0|Ideco|NGFW|21.11|0|syslog|0|deviceProcessN
```

Syslog:

```
2026-01-21T12:48:59+05:00 bez-nazvaniya-2a6874b3-8156-4591-af99-4edc1e9f24d9 admin-audit - - - admin_id:6b17b3ce-2727-4318-95
```

Ключ CEF	**Ключ Syslog**	**Описание**
deviceProcessName	admin-audit	Название источника журнала
rt	-	Время события в формате Unix Timestamp
suid	admin_id	Идентификатор администратора
cs1	admin_login	Логин администратора
suser	admin_name	Имя администратора
dproc	backend	Название службы
src	ip	IP-адрес администратора
requestMethod	request_method	HTTP-метод запроса (GET, POST и т.д.)
cs2	request_body	Тело входящего запроса
request	request_url	URL, на который отправлен запрос
outcome	response_code	Код HTTP-ответа
cs3	response_body	Тело ответа
msg	message	Текстовое сообщение или описание события
cs4	target_id	Идентификатор целевого объекта (ресурса, сущности, операции)
deviceExternalId	vce_id	Идентификатор VCE
cs5	vce_name	Название VCE

Журнал DNS-запросы

CEF:

```
2026-02-04T11:00:15+05:00 bez-nazvaniya-23000007-c6d3-f255-a811-03c1a64d3b0e CEF: 0|Ideco|NGFW|21.12|0|syslog|0|deviceReceipt
```

Syslog:

```
2026-02-04T10:28:41+05:00 bez-nazvaniya-23000007-c6d3-f255-a811-03c1a64d3b0e dns-journal action:reply, protocol:UDP, src_ip:1
```

Ключ CEF	Ключ Syslog	Описание
deviceProcessName	dns-journal	Название источника журнала
act	action	Результат обработки DNS-запроса: • `query` - перехват запроса к серверу • `reply` - успешно • `cache` - из кэша • `fail` - ошибка
proto	protocol	Название протокола
src	src_ip	IP-адрес источника
request	qname	Доменное имя, указанное в DNS-запросе
cs1	qtype	Тип DNS-запроса (например, A, AAAA, MX, TXT)
cs2	qclass	Класс DNS-запроса (обычно IN - Internet)
cs3	opcode	Код операции DNS (например, стандартный запрос, обновление)
outcome	rcode	Код ответа DNS (результат обработки запроса)
cs4	id_wire	Идентификатор DNS-транзакции
cs5	flags	Флаги DNS-пакета (например, RD, RA, AA, TC)
cs6	answer	Раздел ответов DNS (ресурсные записи ответа)
flexString1	authority	Ресурсные записи секции Authority, указывающие на полномочный источник
flexString2	additional	Ресурсные записи секции Additional с дополнительной информацией
suid	src_user_login	Логин пользователя
suser	src_user_name	Имя пользователя
spriv	src_group	Группа пользователя
externalId	cluster_id	Идентификатор кластера
-	cluster_name	Название кластера
deviceExternalId	vce_id	Идентификатор VCE
sproc	vce_name	Название VCE

Примеры сообщений журнала Система

Авторизация через журнал безопасности AD

CEF:

```
2024-07-18T17:20:22+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1721305222 Severity=Notice DeviceProc
```

Syslog:

```
2024-07-18T16:19:39+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.205.254/32 is authorized as user 'Sanek'. Connec
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.205.254/32 is authorized as user 'Sanek'. Connection made from None, type 'log'.` - сообщение об авторизации пользователя `'Sanek'` через журнал безопасности AD (`type 'log'`).

Веб-авторизация

CEF:

```
2024-11-18T14:54:21+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731923661 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T14:47:11+05:00 ideco-ngfw ideco-web-authd - - - Subnet 192.168.101.25/32 is authorized as user 'user'. Connection
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-web-authd	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.25/32 is authorized as user 'user'. Connection made from None, type 'web'.` - сообщение об авторизации пользователя `'user'` через веб-авторизацию (`type 'web'`).

Авторизация по IP

CEF:

```
2024-11-18T18:51:43+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731937903 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T18:42:45+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.101.25/32 is authorized as user 'user'. Connecti
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.25/32 is authorized as user 'user'. Connection made from None, type 'ip'.` - сообщение об авторизации пользователя `'user'` по IP-адресу (`type 'ip'`).

Авторизация по MAC

CEF:

```
2024-11-18T18:54:21+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731938061 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:01:14+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.101.25/32 is authorized as user 'user'. Connecti
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.25/32 is authorized as user 'user'. Connection made from None, type 'mac'.` - сообщение об авторизации пользователя `'user'` по MAC-адресу (`type 'mac'`).

Авторизация по подсетям

CEF:

```
2024-11-18T19:07:54+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731938874 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:06:08+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.101.0/24 is authorized as user 'user'. Connectio
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.0/24 is authorized as user 'user'. Connection made from None, type 'net'.` - сообщение об авторизации пользователя `'user'` по подсети (`type 'net'`).

Авторизация по VPN

CEF:

```
2024-11-18T19:16:18+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731939378 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:17:56+05:00 ideco-ngfw ideco-vpn-authd - - - Subnet 10.128.0.5/32 is authorized as user 'user'. Connection made
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-vpn-authd	Название источника журнала

Информация в сообщении:

- `Subnet 10.128.0.5/32 is authorized as user 'user'. Connection made from '192.168.1.25', type 'pptp'` - сообщение об авторизации пользователя `'user'` по VPN (`type 'pptp'`).

Авторизация администратора

CEF:

```
2026-02-06T11:58:25+05:00 ngfw-21-server CEF:0|Ideco|NGFW|21.11|0|syslog|0|deviceReceiptTime=1770361105 Severity=Notice Devic
```

Syslog:

```
2026-02-05T16:14:47+05:00 ngfw-21-server ideco-web-backend - - - Admin 'admin' (session: AuthSessionInfo(auth_type='local', a
```

Ключ CEF	Ключ Syslog	Описание
deviceProcessName	ideco-web-backend	Название источника журнала

Информация в сообщении:

- `Admin 'admin' (session: AuthSessionInfo) has been successfully authorized for REST from IP '192.168.101.102'` - сообщение об авторизации администратора `'admin'` через веб-интерфейс с IP-адреса `'192.168.101.102'`.

Описание полей `AuthSessionInfo`:

- `auth_type` - тип авторизации;
- `auth_rule_id` - идентификатор правила, по которому авторизовался администратор;
- `auth_group_alias_id` - идентификатор группы безопасности или группы пользователей, по которой авторизовался администратор AD/ALD/FreeIPA;
- `admin_id` - идентификатор администратора;
- `competence` - список прав доступа администратора;
- `role_id` - идентификатор роли администратора;
- `role_name` - название роли администратора;
- `login` - логин администратора;
- `name` - имя администратора;
- `system_session` - признак системной сессии;
- `domain_name` - название домена при авторизации администратора AD/ALD/FreeIPA;
- `login_timestamp` - время события в формате Unix Timestamp;
- `ip` - IP-адрес, с которого выполнена авторизация;
- `access_method` - способ доступа;
- `remote_cc_session` - подключение к NGFW Novum из Ideco Center;
- `country_code` - ISO-код страны;
- `pid` - идентификатор процесса.

Служба fail2ban

CEF:

```
2024-11-18T19:26:57+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:21:54+05:00 ideco-ngfw fail2ban - - - INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-18 19:21:54
```

Ключ	**Описание**	
DeviceProcessName	fail2ban	Название источника журнала

Информация в сообщении:

- `INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-18 19:21:54` - факт обнаружения правил безопасности с указанием группы правил (`[utm-vpn-authd]`), IP-адреса и даты/времени.
- `NOTICE [utm-vpn-authd] Ban 192.168.1.25` - факт блокировки или разблокировки IP-адреса с указанием группы правил (`[utm-vpn-authd]`).
- Список групп правил:
  - `utm-dovecot` - авторизация на почтовом сервере через почтовые клиенты;
  - `utm-postfix-connrate` - превышение лимита подключения к почтовому серверу;
  - `utm-postscreen-prgrt` - отслеживание нежелательных подключений (PREGREET) к почтовому серверу;
  - `utm-reverse-proxy-conn` - защита от DoS (лимит подключений);
  - `utm-reverse-proxy-req` - защита от DoS (лимит запросов в секунду);
  - `utm-reverse-proxy` - Web Application Firewall (WAF);
  - `utm-roundcube` - авторизация в веб-интерфейсе почтового сервера;
  - `utm-smtp` - авторизация по smtp;
  - `utm-smtp-rcpt` - защита от перебора почтовых ящиков;
  - `utm-ssh` - авторизация по ssh;
  - `utm-two-factor-codes` - прохождение двухфакторной аутентификации;
  - `utm-vpn-authd` - авторизация по VPN;
  - `utm-web-interface` - авторизация в административном веб-интерфейсе;
  - `utm-user-cabinet` - авторизация в пользовательском веб-интерфейсе.

SD-WAN

Классический контекст | Высокопроизводительный контекст | API

SD-WAN (Software-Defined Wide Area Network) - технология программно-определяемых распределенных сетей, которая управляет WAN-каналами на основе политик и обеспечивает интеллектуальную маршрутизацию трафика между филиалами, центрами обработки данных и облачными сервисами.

В разделе **SD-WAN** доступны настройки:

- **Next hop** - следующий узел маршрутизации, задающий интерфейс и шлюз, через которые будет отправляться трафик.
- **Профили next hop** - объединение нескольких next hop в одну логическую группу. В профиле задаются режим работы (резервирование или балансировка), приоритет и способ проверки доступности.
- **Профили IP SLA** - набор параметров для мониторинга качества канала: допустимые пороги задержки, джиттера и потери пакетов. Используется в **Профилях next hop** для оценки доступности канала.

Миграция при обновлении

Балансировка и резервирование

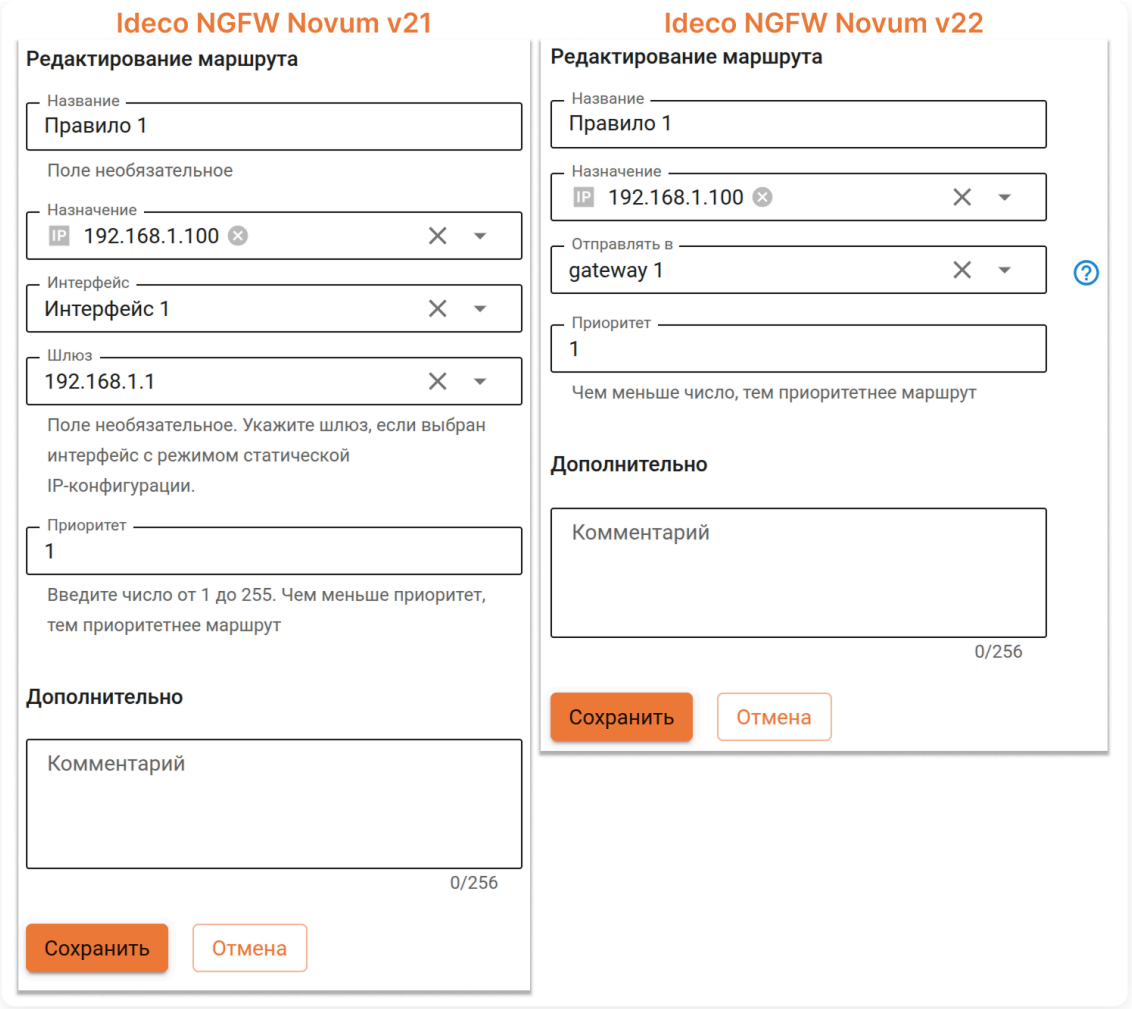
С версии 22 Ideco NGFW Novum раздел **Балансировка и резервирование** вошел в состав **SD-WAN**. При обновлении настройки будут перенесены автоматически. Миграция настроек:

- Все шлюзы, добавленные ранее на вкладке **Основное**, будут перенесены в **Next hop**.
- Выбранный ранее режим **Балансировки** или **Резервирования** будет преобразован в системный **Профиль next hop**. Помимо системного профиля, теперь можно создавать несколько пользовательских профилей.
- **Адреса для проверки связи** будут перенесены в системный **Профиль IP SLA**. Этот профиль будет выбран в системном профиле next hop при миграции.

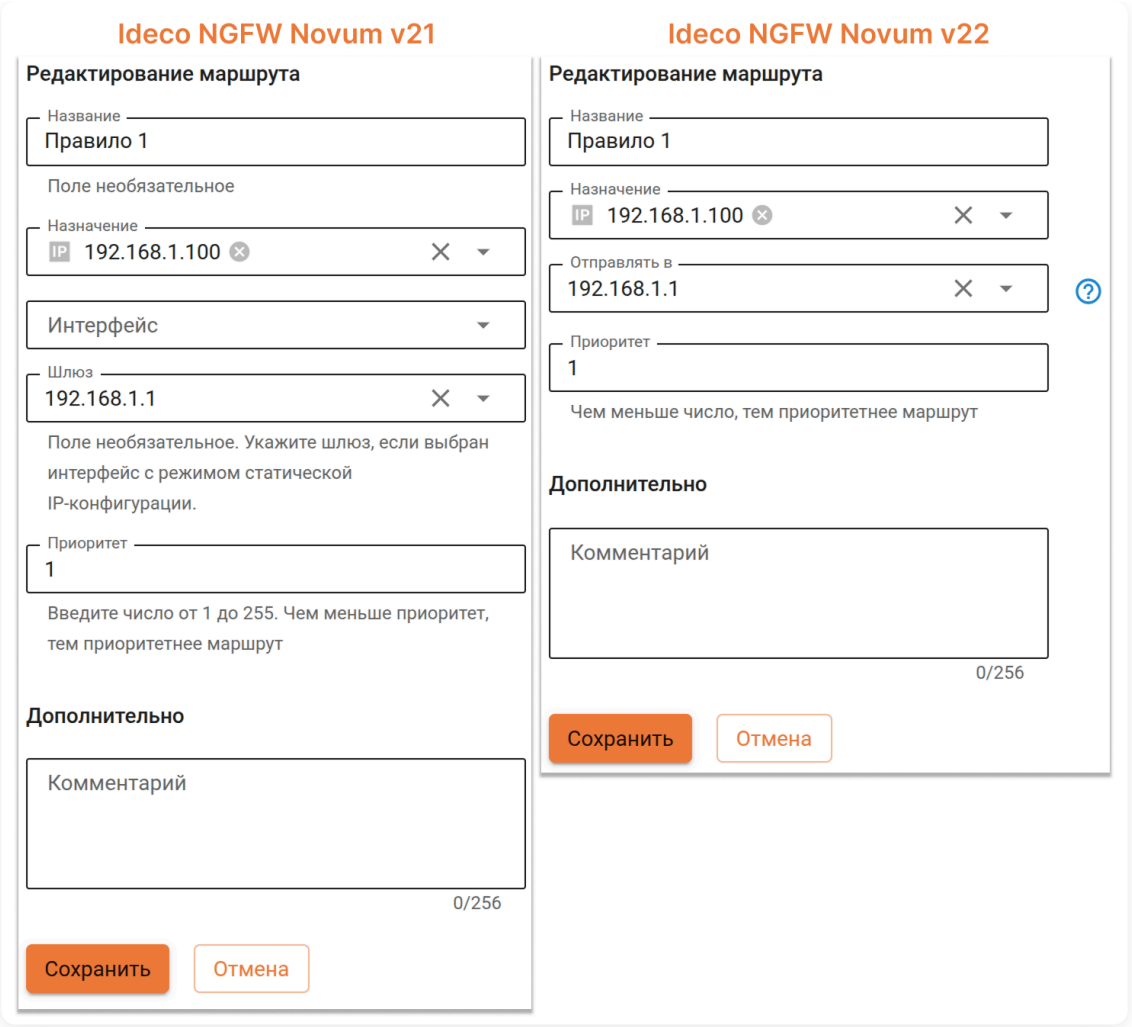
Маршрутизация (PBR, Статическая, Внешних сетей)

Логика создания **Next hop** при миграции маршрутов зависит от исходной конфигурации:

- Если в маршруте был указан **Интерфейс** - автоматически создается **Next hop**. Пример правила статической маршрутизации:



- Если в маршруте не был указан **Интерфейс** - **Next hop** не создается, маршрут сохраняется в прежнем виде. Пример правила статической маршрутизации:



Если в правиле маршрутизации **Внешних сетей** была включена опция **Использовать маршрут только при доступности шлюза (адаптивность)** - при миграции автоматически создается **Профиль next hop** с настроенной проверкой доступности шлюза. Это необходимо для корректной работы адаптивности после обновления.

С версии 22 Ideco NGFW Novum не поддерживает указание пользователя в поле **Шлюз** правил **Статической** маршрутизации. Если в правиле был указан пользователь, перед обновлением замените его на IP-адрес вручную.

IPsec

Следует учесть, что при обновлении на версию 22:

- Существующие конфигурации с несколькими адресами удаленного устройства продолжат работать после миграции. В новой версии допускается только один **Адрес удаленного устройства**.
- **Группа балансировки и резервирования**, выбранная в поле **Интерфейс подключения**, будет перенесена в **Профиль next hop**. В новой версии в поле **Интерфейс подключения** допускается только один интерфейс.

Рекомендуем после обновления указать конкретный **Интерфейс подключения** и конкретный **Адрес удаленного устройства**, так как варианты с множественным выбором или объектом **Любой** будут удалены в следующих версиях.

Next hop

Классический контекст | Высокопроизводительный контекст | API

Next hop - это следующий узел маршрутизации, на который передается сетевой трафик для дальнейшей доставки к целевой сети. В рамках **SD-WAN** next hop определяется после выбора маршрута до точки назначения и задает, через какой интерфейс и шлюз будет отправляться трафик.

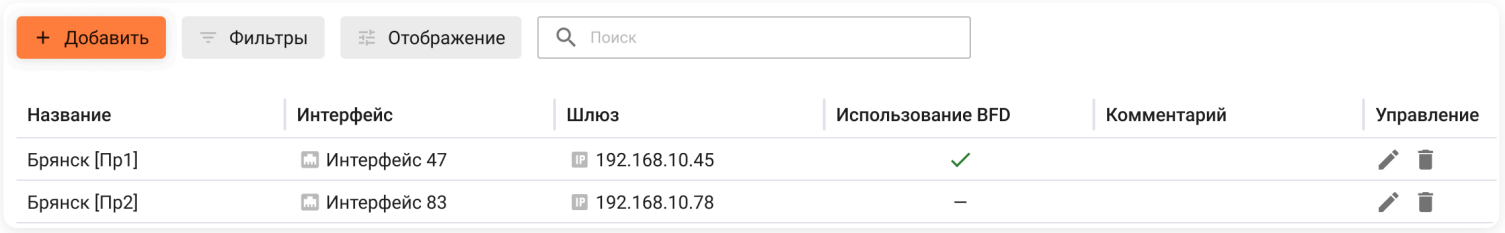
Next hop используется при настройке маршрутизации: **Статическая**, **PBR** и **Внешних сетей**.

Если нет необходимости в проверке доступности шлюза или резервировании, в поле **Отправить в** достаточно указать IP-адрес как **Объект** или **Значение**. Создайте **Next hop**, если:

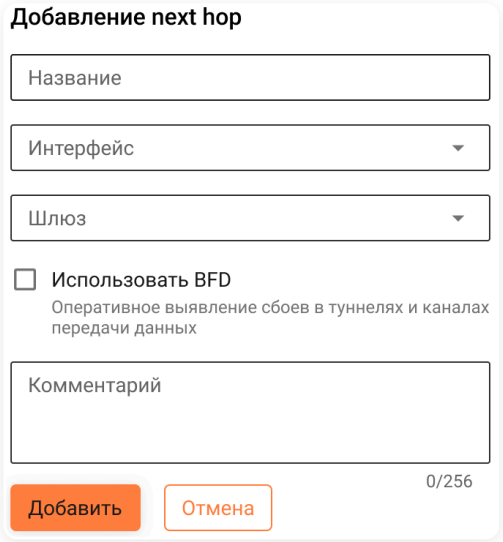
- Нужна проверка доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection).
- Планируется объединить несколько шлюзов в **Профиль next hop** для резервирования или балансировки трафика.
- При настройке **Статического** маршрута, правила **PBR** или **Внешних сетей** необходимо указать интерфейс.

Для добавления **Next hop** выполните действия:

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**:



2. Заполните поля:



- **Название** - укажите название.
- **Интерфейс** - выберите сетевой интерфейс, через который будет отправляться трафик к следующему узлу.
- **Шлюз** - укажите IP-адрес следующего узла маршрутизации (next hop), на который будет направляться трафик. Адрес шлюза должен находиться в сети выбранного интерфейса.

При выборе интерфейса, который получает IP-адрес по DHCP:

- Если оставить поле **Шлюз** пустым, то будет использован шлюз, полученный от DHCP-сервера.
- Если в поле **Шлюз** указать IP-адрес, то в качестве шлюза будет использоваться указанный IP-адрес, а полученный от DHCP-сервера проигнорируется.

- **Использовать BFD** - включите опцию для проверки доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection). Поддержка BFD должна быть включена и на стороне указанного шлюза.
- **Комментарий** - необязательное поле для описания **Next hop**.

> Интерфейс с ролью **Control Plane** используется только для настройки и администрирования NGFW Novum. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.

Добавленные **Next hop** можно редактировать, удалять и объединять в **Профили next hop**. Подробности в статье.

Мониторинг состояния Next hop

Для настройки проверки работоспособности **Next hop** выполните действия:

1. Создайте **Профиль IP SLA**, указав требования к качеству сетевого соединения и IP-адрес для проверки связи.

2. Создайте **Профиль next hop**:

- На вкладке **Настройки** выберите **Профиль IP SLA**, созданный на шаге 1.
- На вкладке **Next hop** выберите **Next hop**, для которого нужна проверка работоспособности.

> Уведомления о недоступности будут отображаться в **Отчеты и журналы** → **Система**.

Полезные ссылки

- **Статическая маршрутизация**
- **PBR**
- **Внешних сетей**
- **Профили next hop**

Профили next hop

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Профили next hop**: `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

Профили next hop - объединение нескольких шлюзов (next hop) в одну логическую группу. В профиле задаются режим работы шлюзов (резервирование или балансировка), их приоритет и способ проверки доступности.

Профили next hop используются при настройке маршрутизации: **Статическая**, **PBR** и **Внешних сетей**.

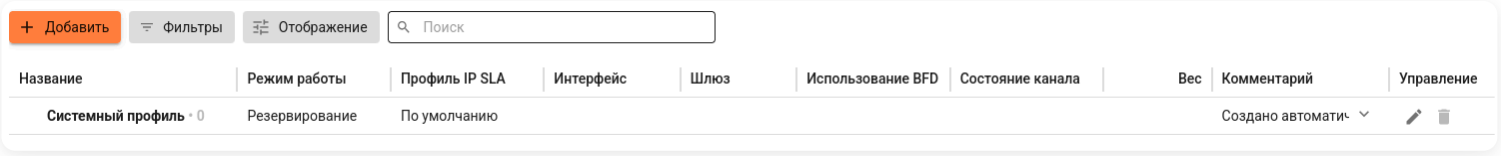
Режимы работы профилей:

- **Резервирование** - NGFW Novum использует шлюзы по приоритету. При недоступности основного шлюза трафик переходит через резервные.
- **Балансировка** - трафик распределяется между несколькими шлюзами по мере установления новых сетевых сессий, что позволяет равномерно распределять нагрузку. Режим использует механизм **ECMP** (Equal-Cost Multi-Path). Сессии одного пользователя могут проходить через разные шлюзы:
  - **Балансировка со стабильной привязкой** - сетевые сессии закрепляются за определенным шлюзом и всегда проходят через него. Рекомендуется, если на внешних интерфейсах не используется NAT.

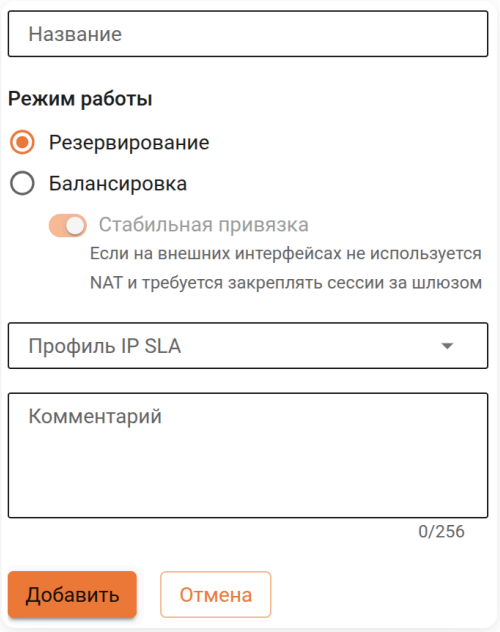
Добавление профиля

Для добавления **Профиля next hop** выполните действия:

1. Перейдите в **SD-WAN** → **Профили next hop** и нажмите **Добавить**:



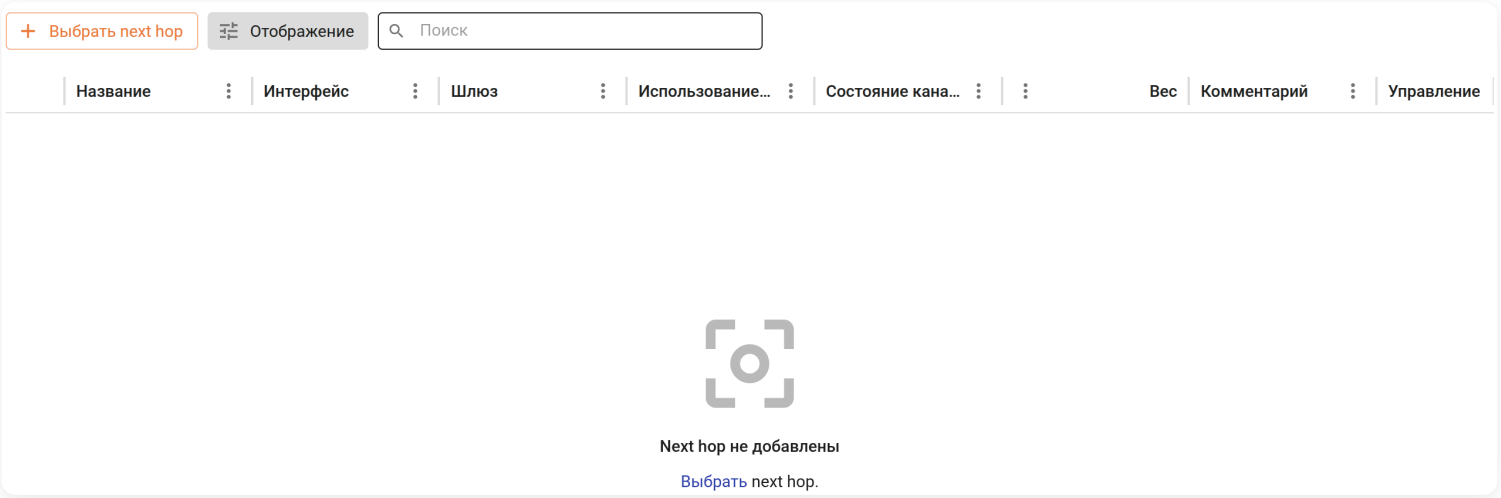
2. Заполните поля и нажмите **Добавить**:



Расшифровка полей

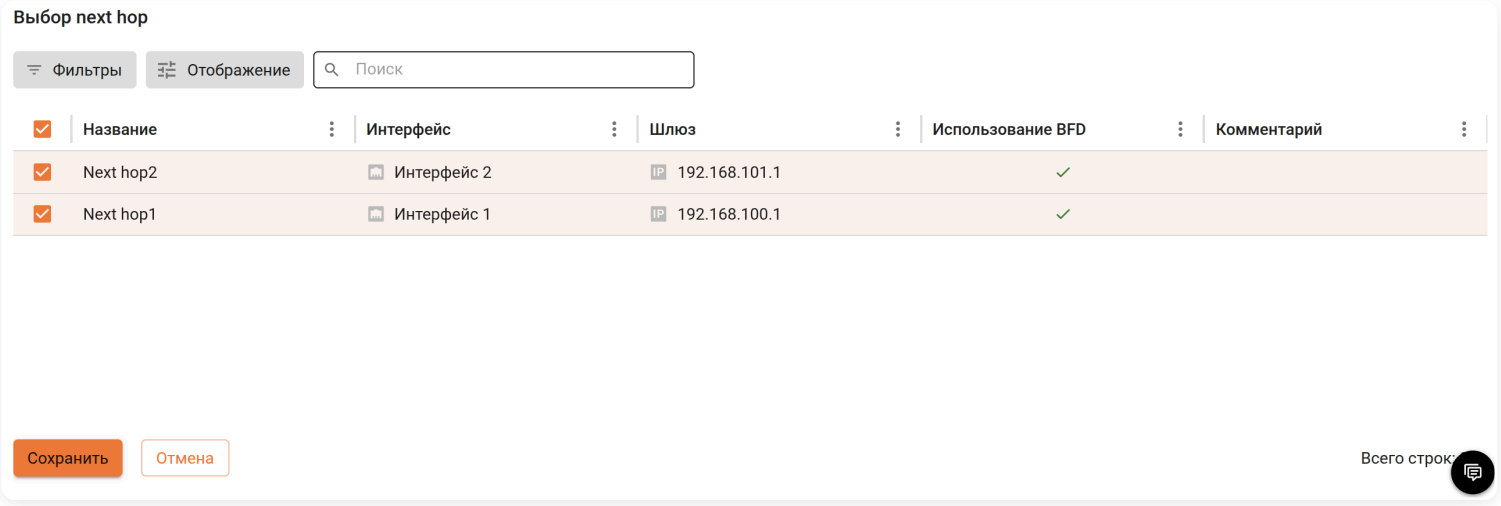
- **Название** - укажите название профиля.
- **Режим работы** - выберите способ использования шлюзов в профиле:
  - **Резервирование** - используется один основной шлюз, а остальные применяются как резервные при его недоступности.
  - **Балансировка** - трафик распределяется между несколькими шлюзами:
    - **Стабильная привязка** - включите опцию для закрепления сетевых сессий за определенным шлюзом. Рекомендуем включать, если на внешних интерфейсах не используется NAT и важно, чтобы трафик одной сессии всегда проходил через один шлюз.
- **Профиль IP SLA** - выберите профиль, который будет использоваться для проверки доступности шлюзов и качества канала.
- **Комментарий** - необязательное поле для описания профиля.

3. Перейдите на вкладку **Next hop**, нажмите **Выбрать next hop** и выполните действия в зависимости от выбранного режима работы:



Балансировка

4. Выберите нужные next hop и нажмите **Сохранить**:

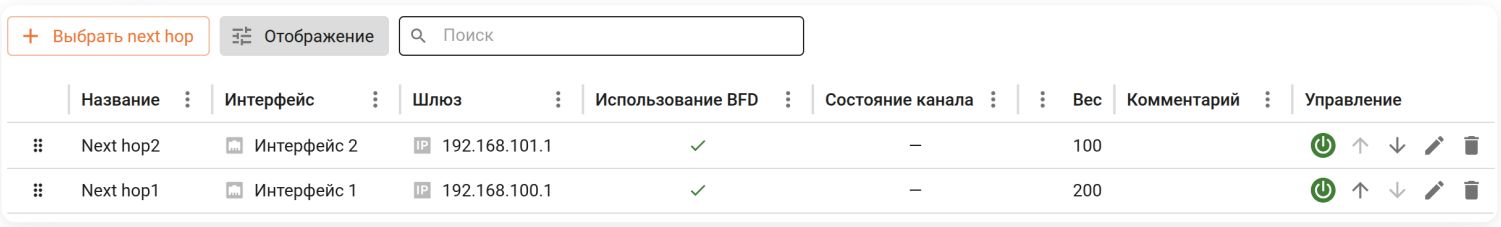


Изменение веса у next hop в профиле

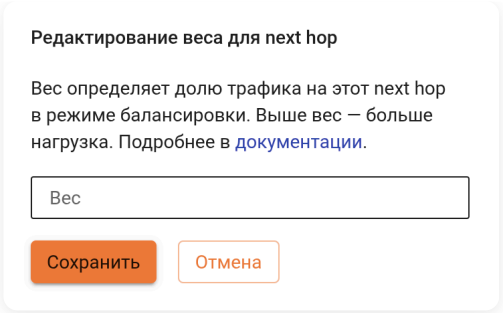
Вес - числовой коэффициент, определяющий долю трафика, направляемую на конкретный next hop при балансировке нагрузки. Чем выше вес относительно других узлов, тем больше запросов получит этот шлюз.

В поле **Вес** у выбранного next hop рекомендуем указывать пропускную способность интернет-провайдера. Балансировщик распределит трафик пропорционально весам всех активных узлов.

5. Нажмите напротив нужного next hop:



6. Введите вес и нажмите **Сохранить**:

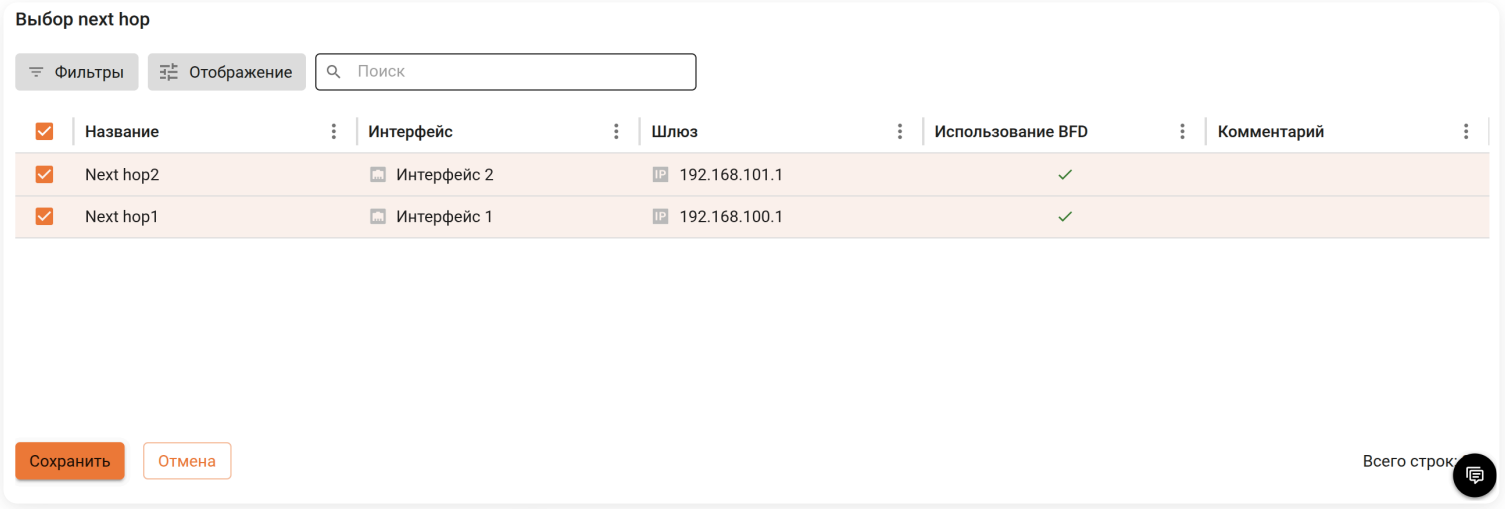


Next hop без указанного веса в балансировке не участвует.

Резервирование

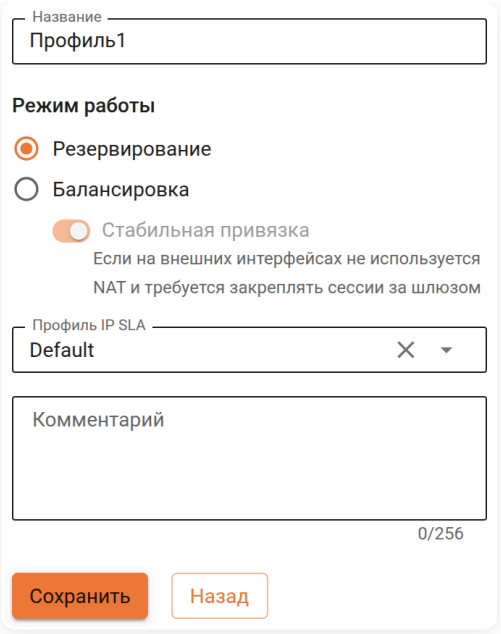
При **Резервировании** Ideco NGFW Novum использует шлюзы в соответствии с приоритетом. Приоритет задается порядком next hop в таблице, сверху вниз. Если интернет стал недоступен через используемый шлюз, то NGFW Novum будет перебирать подключения сверху вниз (до первого доступного шлюза).

4. Выберите нужные next hop и нажмите **Сохранить**:



5. Смените приоритет при необходимости, нажав ↑ ↓.

Вернитесь на вкладку **Настройки** и нажмите **Сохранить**:

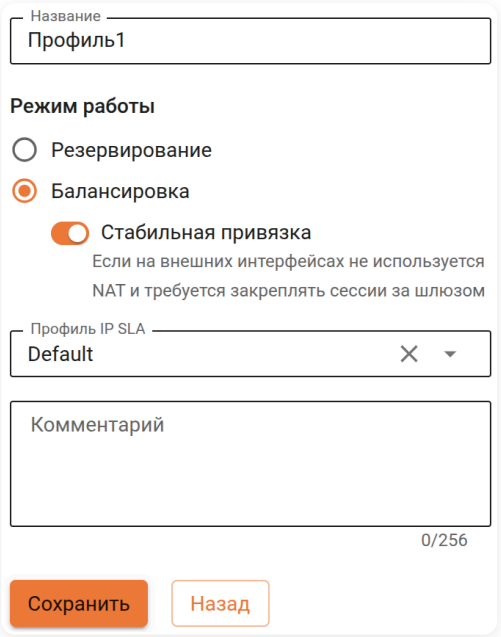


Изменение профиля

Для изменения режима профиля выполните действия:

1. Нажмите  напротив нужного профиля.

2. Выберите новый режим и нажмите **Сохранить**:



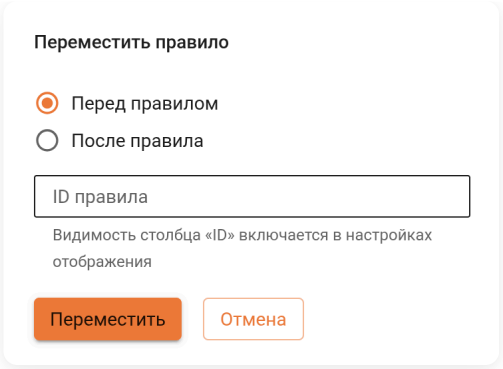
Если переключаете режим с **Резервирование** на **Балансировка**, настройте значение веса у next hop в профиле.

При изменении профиля на вкладке **Next hop** доступно перемещение добавленных next hop. Выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Полезные ссылки

- **Статическая маршрутизация**
- **PBR**
- **Внешних сетей**
- **Next hop**
- **Профили IP SLA**

Профили IP SLA

Классический контекст | Высокопроизводительный контекст | API

Профили IP SLA - набор параметров, определяющих требования к качеству сетевого соединения и правила мониторинга доступности канала. Профиль используется при создании **Профилей next hop** для оценки состояния канала и принятия решений о его доступности на основе измеряемых сетевых показателей.

В рамках **Профиля IP SLA** настраиваются параметры качества обслуживания:

- **Задержка** - максимально допустимое время передачи данных по сети.
- **Джиттер** - максимально допустимое колебание времени задержки пакетов, характеризующее стабильность соединения.
- **Потеря пакетов** - максимально допустимый процент потерянных пакетов в канале связи.

Если в одном из параметров значение превышает заданный порог, соединение не соответствует требованиям SLA.

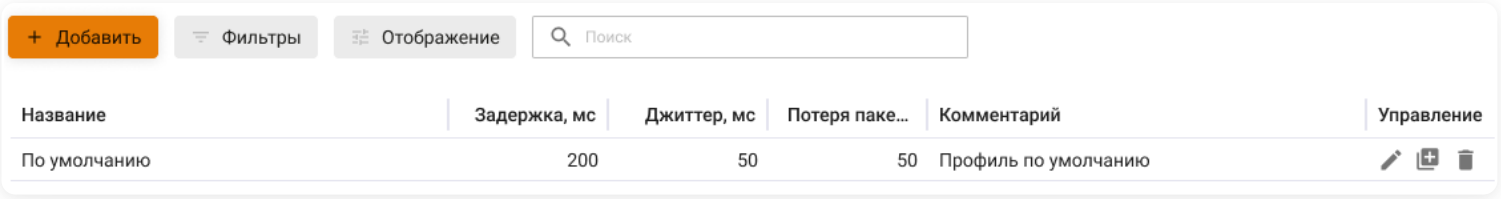
Для определения доступности канала в профиле используется протокол ICMP. Система отправляет ICMP-запросы на указанные IP-адреса. По результатам ответов оцениваются:

- Наличие или отсутствие соединения.
- Количество последовательных неудачных проверок.
- Количество последовательных успешных проверок.
- Минимальное время стабильной работы канала, необходимое для признания его активным.

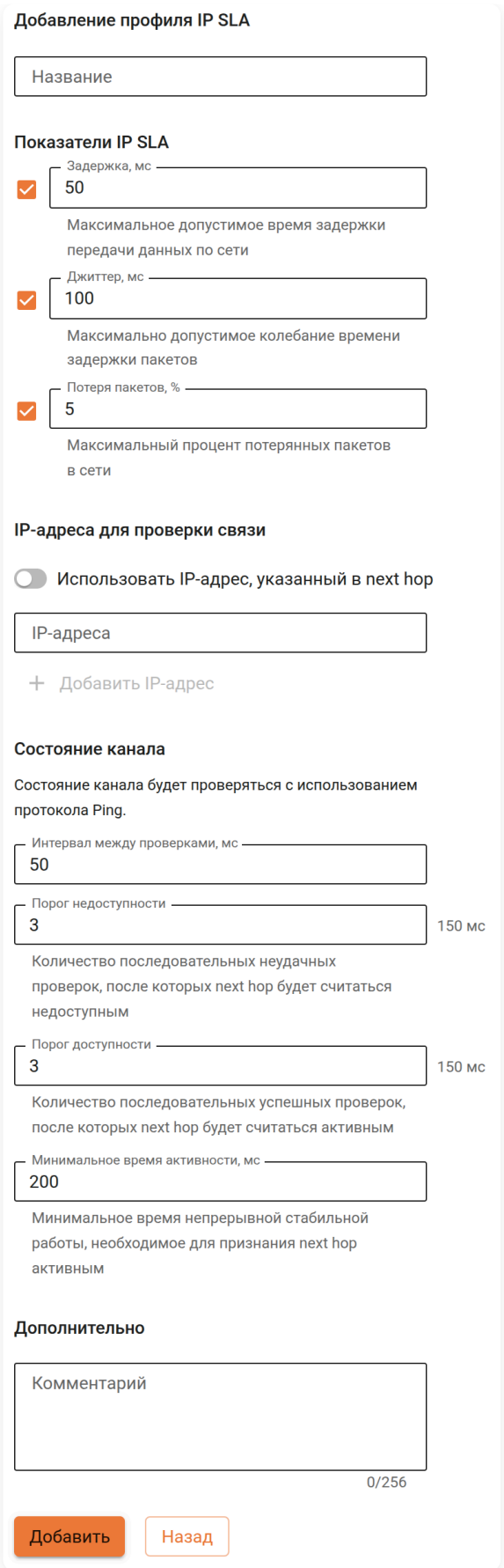
Если число неуспешных проверок превышает заданный порог, канал помечается как недоступный. Канал считается восстановленным после достижения порога успешных проверок и выдержки минимального времени активности.

Для добавления профиля выполните действия:

1. Перейдите в **SD-WAN** → **Профили IP SLA** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - укажите название профиля.
- **Показатели SLA** - включите опции:
  - **Задержка, мс** - задайте максимально допустимое время задержки передачи данных по сети.
  - **Джиттер, мс** - укажите максимально допустимое колебание времени задержки пакетов.

    - **Потеря пакетов, %** - укажите максимально допустимый процент потерянных пакетов в сети.
- **IP-адреса для проверки связи**:
    - **Использовать IP-адрес, указанный в next hop** - включите опцию для проверки доступности следующего узла (next hop), указанного в маршруте.
    - **IP-адрес** - укажите IP-адрес узла, до которого выполняется проверка доступности канала. Можно указать несколько адресов для проверки.
- **Состояние канала**:
    - **Интервал между проверками, мс** - определите периодичность выполнения проверок доступности канала.
    - **Порог недоступности** - укажите количество последовательных неудачных проверок, после которых next hop считается недоступным.
    - **Порог доступности** - укажите количество последовательных успешных проверок, после которых next hop считается активным (но не раньше, чем **Минимальное время активности, мс**).
    - **Минимальное время активности, мс** - укажите минимальное время непрерывной стабильной работы канала, необходимое для признания next hop активным.
- **Дополнительно**:
    - **Комментарий** - необязательное поле для описания профиля.

Маршрутизация

Классический контекст | Высокопроизводительный контекст

Маршрутизация - механизм определения пути сетевого пакета от источника к назначению. Модуль позволяет:

- Обеспечить сетевую связность между подсетями, филиалами и внешними сетями.
- Управлять направлением трафика в зависимости от адресов источника, назначения и других условий.
- Организовать отказоустойчивость и балансировку нагрузки между несколькими каналами связи.
- Обеспечить корректную доставку как исходящего, так и ответного трафика.

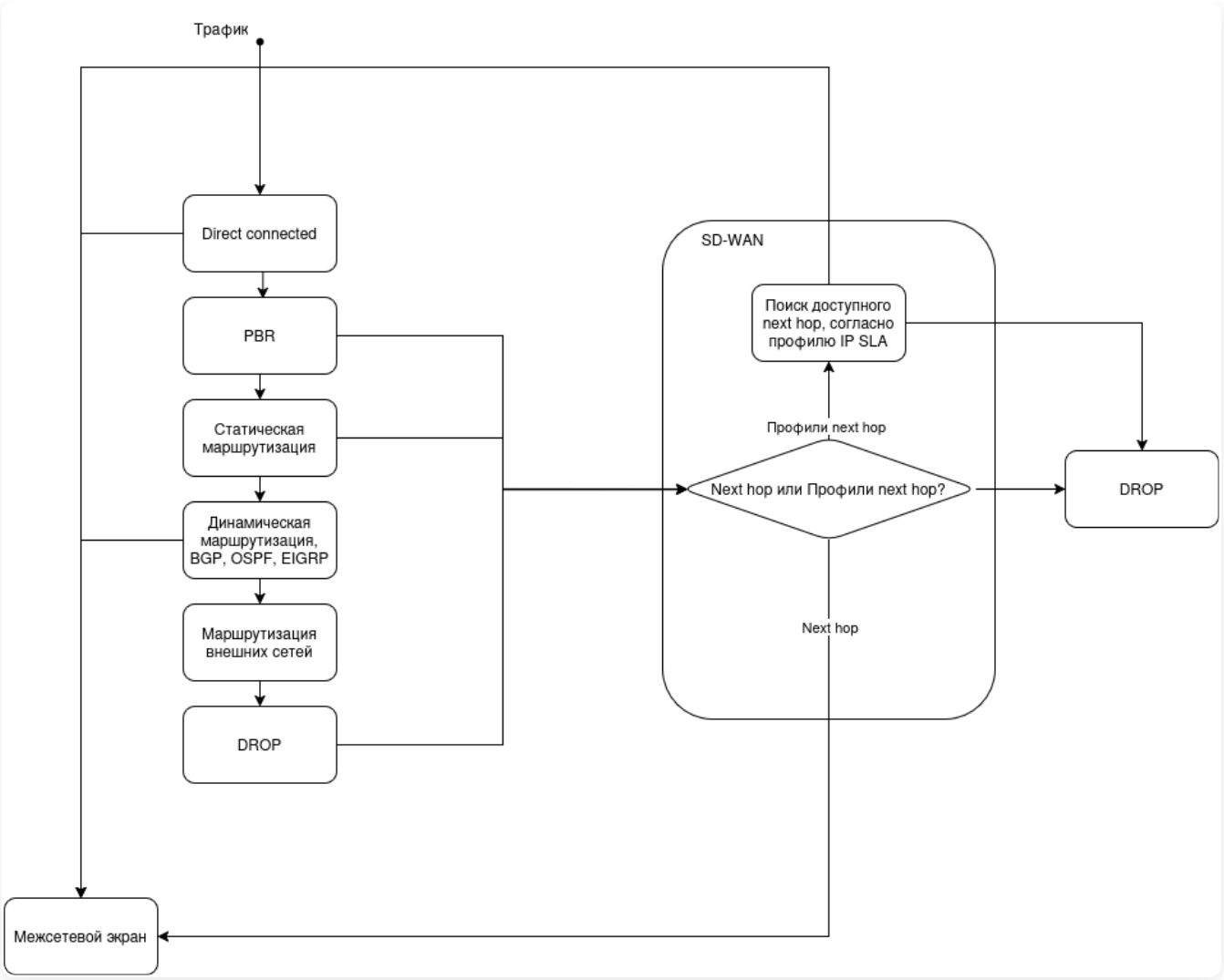
В разделе доступны настройки:

- **PBR** - маршрутизация на основе политик, которые устанавливаются администратором.
- **Статическая** - маршрутизация на основе заданных вручную маршрутов с фиксированными шлюзами и интерфейсами.
- **BGP** - динамическая маршрутизация на основе протокола прикладного уровня, обеспечивающая обмен маршрутами между сетями и автономными системами.
- **OSPF** - динамическая маршрутизация на основе протокола состояния каналов, определяющая оптимальные пути передачи данных внутри сети.
- **EIGRP** - динамическая маршрутизация на основе гибридного протокола. Он сочетает особенности дистанционно-векторного подхода и протоколов состояния каналов, что обеспечивает быструю сходимость и актуальность таблиц маршрутизации.
- **Внешних сетей** - маршрутизация, позволяющая направлять трафик от разных пользователей или групп пользователей по заданным маршрутам.

Обработка трафика

Трафик последовательно проходит этапы поиска маршрута. Путь пакета после его определения зависит от того, в какой таблице найден маршрут:

- Для маршрутов из таблиц **PBR**, **Статической** маршрутизации и маршрутизации **Внешних сетей** требуется дополнительный выбор next hop через **SD-WAN**.
- Маршруты из Direct connected и динамической маршрутизации направляются напрямую в **Межсетевой экран**:



После определения маршрута результат маршрутизации сохраняется. Путь пакета фиксируется, но может измениться при недоступности ранее выбранного next hop.

Этап 1. Поиск маршрута

Трафик проверяется на пяти уровнях в строгой последовательности. В зависимости от действия происходит переход:

Уровень	**Если маршрут найден**	**Если не найден**
Direct connected	Межсетевой экран	PBR
PBR	SD-WAN	Статическая маршрутизация
Статическая маршрутизация	SD-WAN	Динамическая маршрутизация
Динамическая маршрутизация (BGP, OSPF, EIGRP)	Межсетевой экран	Маршрутизация внешних сетей
Маршрутизация внешних сетей	SD-WAN	DROP

Этап 2. Выбор next hop

Когда маршрут найден в таблицах **PBR**, **Статической маршрутизации** или **Маршрутизации внешних сетей**, пакет направляется в **SD-WAN** для выбора next hop:

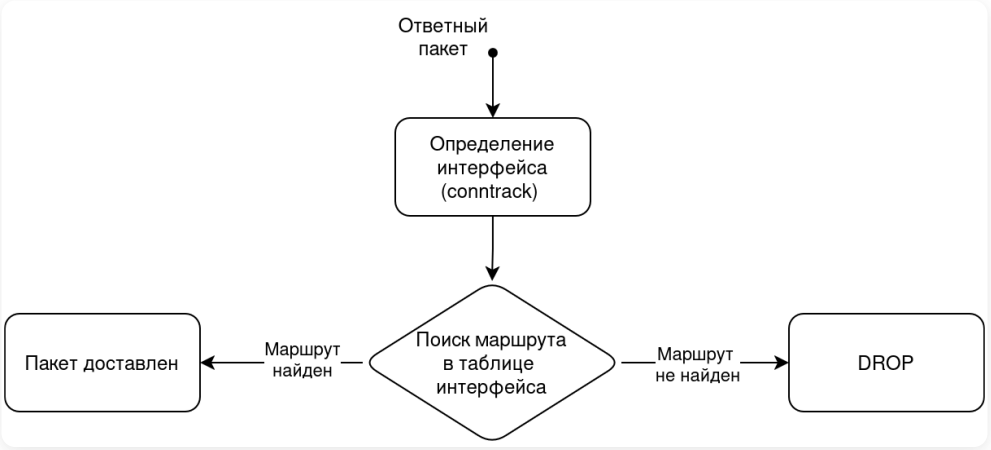
- Если используется конкретный **Next hop**, то проверяется его доступность:
  - Если доступен - пакет направляется в **Межсетевой экран**.
  - Если недоступен - пакет отбрасывается.
- Если используются **Профили next hop**:
  - Пакет направляется на этап **Поиск доступного next hop, согласно профилю IP SLA**. Выбранный next hop фиксируется и пакет направляется в **Межсетевой экран**.
  - Если в **Профиле next hop** следующие узлы недоступны - пакет отбрасывается.

Маршруты в таблицах **PBR** и **Внешних сетей** имеют приоритет сверху вниз, то есть **верхний маршрут приоритетнее нижнего**.

Для трафика не будут применяться нижестоящие правила, если хотя бы одно условие совпадает с вышестоящим правилом.

Обработка ответного трафика

Для пакетов, относящихся к уже установленному соединению, NGFW использует механизм Connection tracking (conntrack): ответный пакет отправляется через тот же интерфейс, с которого поступил исходный запрос, если для этого интерфейса существует подходящий маршрут:



Если маршрут в сторону интерфейса-источника отсутствует, ответный пакет не будет отправлен. Рекомендуем добавить явный маршрут (например, статический) в сеть источника через соответствующий интерфейс.

Полезные ссылки

- **Как избавиться от асимметричной маршрутизации трафика**

PBR

Классический контекст | Высокопроизводительный контекст | API

PBR (Policy-based Routing) - маршрутизация на основе политик, которые устанавливаются администратором. Позволяет направлять трафик по различным условиям, например, от конкретных пользователей или по протоколу. Применяется первой до всех остальных видов маршрутизации.

Способы применения:

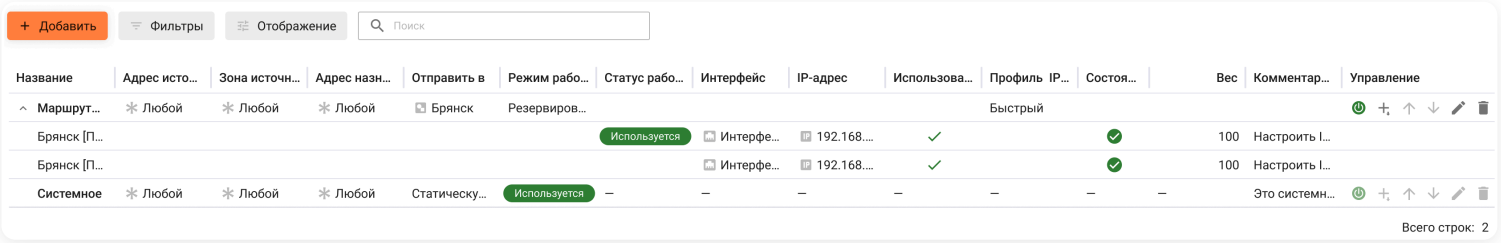
- Направление части трафика через интернет-провайдера с наименьшей стоимостью этого трафика.
- Предоставление доступа в интернет через одного из провайдеров для определенных пользователей/групп пользователей.

> Маршруты в таблице имеют приоритет сверху вниз, то есть **верхний маршрут приоритетнее нижнего**.

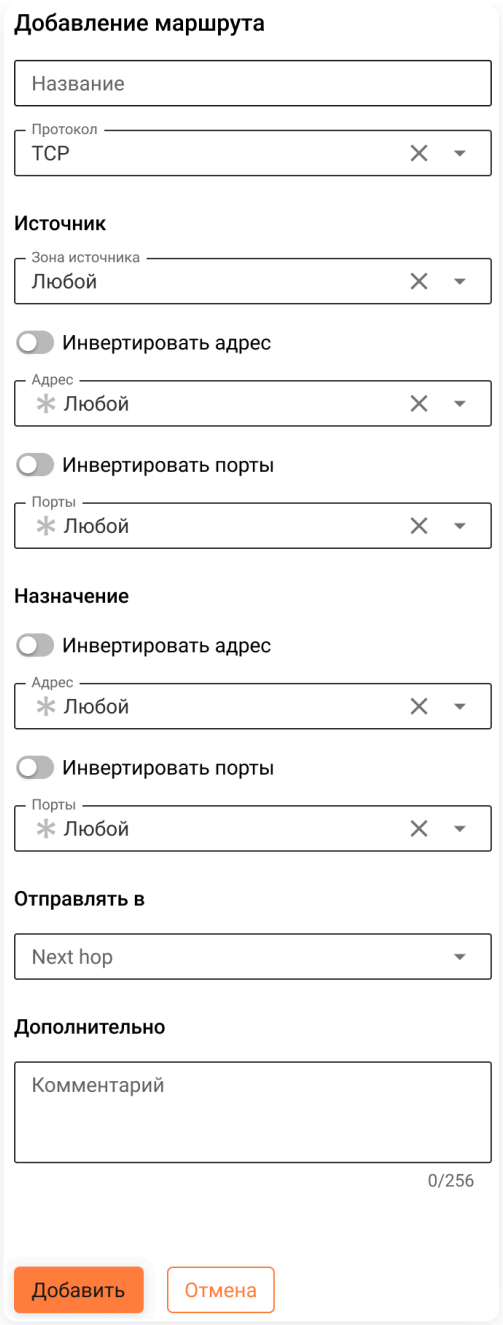
Перед обновлением на Ideco NGFW Novum версии 22 ознакомьтесь с информацией по ссылке.

Действия для настройки:

1. Перейдите в **Маршрутизация** → **PBR** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - введите название маршрута.
- **Протокол** - выберите протокол передачи данных: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP).
- **Источник**:
  - **Зона*** - выберите интерфейс или группу интерфейсов Ideco NGFW Novum, на которые приходит трафик от источника. Объект типа **Зона** можно создавать и редактировать только в **Системном контексте**.
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - выберите объект, трафик от которого нужно маршрутизировать. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
  - **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.
  - **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

Не рекомендуем указывать порт источника, так как он обычно выбирается случайным образом. Исключение - протоколы с фиксированными портами источника и назначения (например, DNS).

- **Назначение**:
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.

- **Адрес** - выберите объекты, при обращении к которым будет применяться этот маршрут. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
- **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.
- **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

- **Отправлять в** - выберите вариант, через который будет направляться трафик. В поле могут быть выбраны: Next hop, Профили next hop, IP-адреса или Статическая маршрутизация. IP-адрес можно указать как **Объект** или **Значение**. При выборе Статической маршрутизации NGFW Novum трафик перенаправляется в таблицу **Статической маршрутизации**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

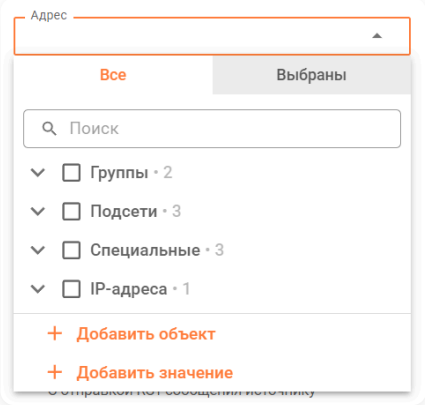
Отличие значений от объектов:

- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

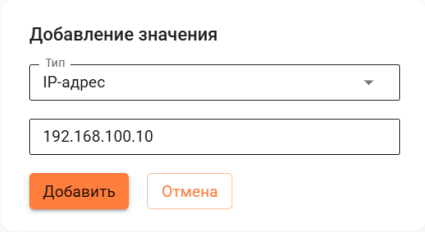
Управление значениями

Добавление

1. В поле нажмите **Добавить значение**:



2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:

Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:

2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

- **Дополнительно**:
  - **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

В столбце **Управление** можно:

 Включать или выключать правило.

 Менять приоритет.

 Редактировать правило.

 Удалять правило.

Полезные ссылки

- **Объекты**
- **Статическая маршрутизация**
- **Next hop**
- **Профили next hop**

Статическая маршрутизация

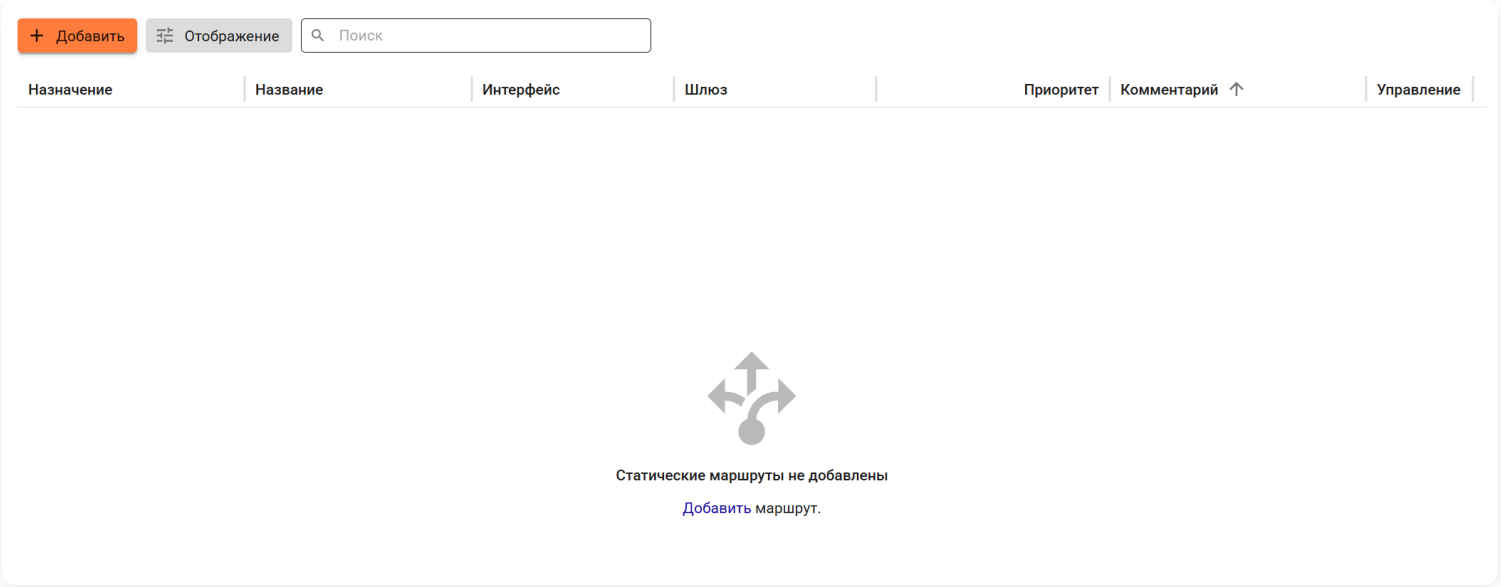
Классический контекст | Высокопроизводительный контекст | API

Статическая маршрутизация применяется в сценариях, где нет необходимости в сложной логике маршрутизации. Обработка статических маршрутов происходит после PBR, но до динамической маршрутизации и маршрутизации внешних сетей.

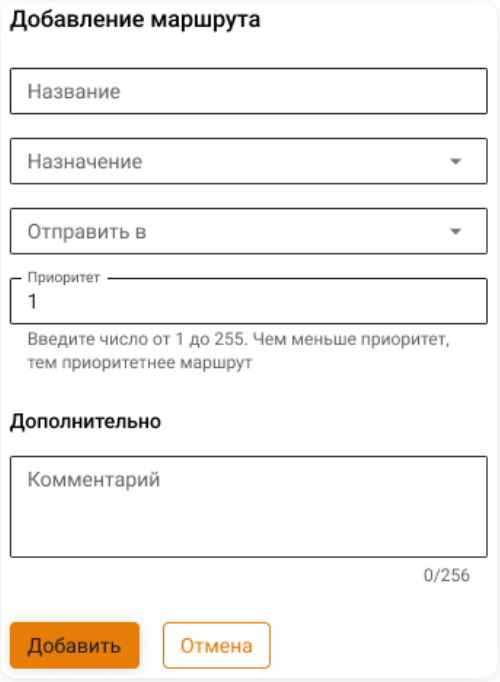
Перед обновлением на Ideco NGFW Novum версии 22 ознакомьтесь с информацией по ссылке.

Для добавления статического маршрута выполните действия:

1. Перейдите в раздел **Маршрутизация** → **Статическая** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - укажите название правила.

- **Назначение** - выберите объекты, при обращении к которым будет применяться это правило. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
- **Отправить в** - выберите IP-адрес, Next hop или профиль Next hop, через который будет отправлен трафик. IP-адрес можно указать как **Объект** или **Значение**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

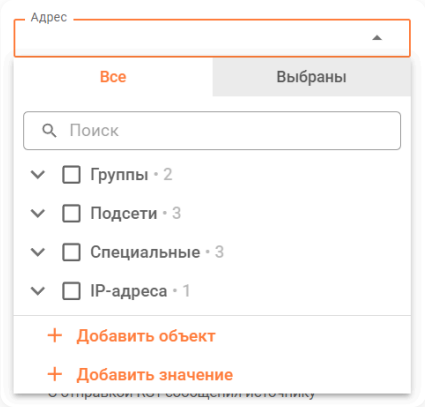
Отличие значений от объектов:

- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

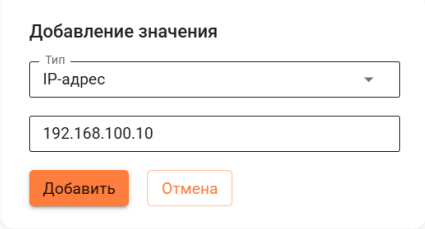
Управление значениями

Добавление

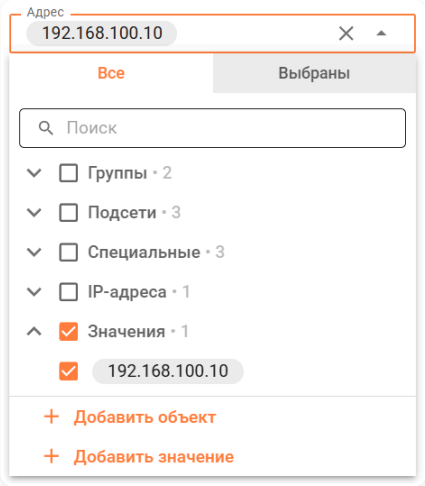
1. В поле нажмите **Добавить значение**:



2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:

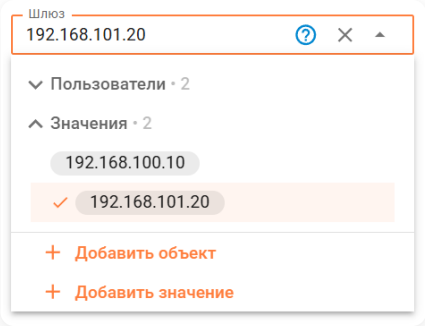


Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:



2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

Интерфейс с ролью **Control Plane** используется только для настройки и администрирования NGFW Novum. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.

- **Приоритет** - укажите приоритет маршрута. Чем меньше число, тем выше приоритет. При значении 255 трафик по этому маршруту будет заблокирован.
- **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

С версии 22 Ideco NGFW Novum не поддерживает указание пользователя в поле **Шлюз**. Если в правиле был указан пользователь, перед обновлением замените его на IP-адрес вручную.

Особенности

- **Порядок обработки маршрутов:**
  Статические маршруты обрабатываются после PBR, но до динамической маршрутизации (BGP, OSPF и EIGRP). Если в статической маршрутизации задан шлюз по умолчанию, трафик будет отправлен через него и не дойдет до динамической маршрутизации и правил маршрутизации внешних сетей.
- **Резервные маршруты через приоритет:**
  Если установить приоритет статического маршрута в диапазоне от 200 до 254, он станет менее приоритетным, чем маршруты, полученные через протоколы динамической маршрутизации. Это позволяет использовать статические маршруты как резервные:
  - Если динамическая маршрутизация предоставляет путь к сети, будет использован динамический маршрут.
  - Если динамический маршрут отсутствует, трафик пойдет по статическому маршруту.
- **Балансировка нагрузки (ECMP):**
  Если создать два маршрута к одному назначению с одинаковым приоритетом, трафик будет распределен между ними по принципу ECMP (Equal-Cost Multi-Path).
- **Блокировка трафика:**
  При значении приоритета 255 трафик по маршруту блокируется.

Полезные ссылки

- **Доступ из внешних сетей без NAT**
- **Как избавиться от асимметричной маршрутизации трафика**

BGP

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **BGP**: `frr`; `ideco-routing-backend`, `ideco-routing-rest`.

Список служб для других разделов доступен по ссылке.

Border Gateway Protocol (BGP) - это основной динамический протокол прикладного уровня, используемый для маршрутизации пакетов между автономными системами (сеть или группа сетей, работающих по единой политике маршрутизации).

Для запуска модуля необходимо предварительно настроить BGP:

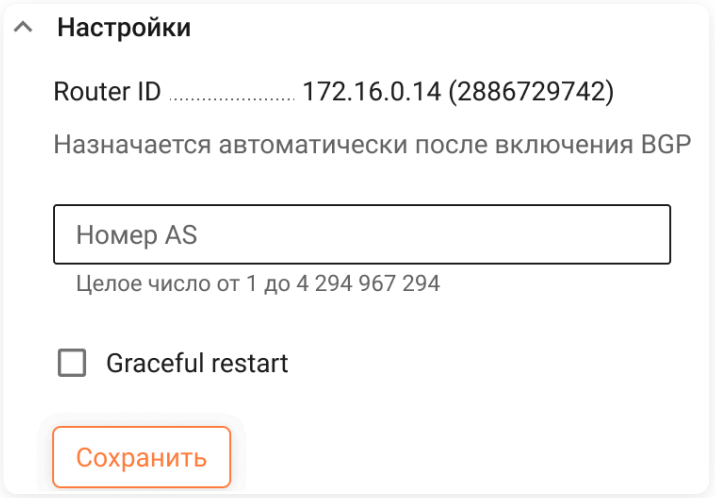
- Указать номер автономной системы.
- Создать и включить как минимум одного BGP-соседа.

На Ideco NGFW Novum по умолчанию включен **BGP Multipath** - механизм, позволяющий устанавливать несколько путей BGP к одному месту назначения в таблице IP-маршрутизации. **BGP Multipath** не влияет на процесс выбора лучшего пути.

Ideco NGFW Novum автоматически заполняет поле **Router ID** значением наибольшего IP-адреса локальной сети, указанного в разделе **Сетевые интерфейсы**. При необходимости измените IP-адрес в разделе **Сетевые интерфейсы**.

Настройка автономной системы

1. Перейдите в **Маршрутизация** → **BGP** и введите номер автономной системы в поле **Номер AS** в блоке **Настройки**:



2. Нажмите **Сохранить** и включите модуль **BGP**.

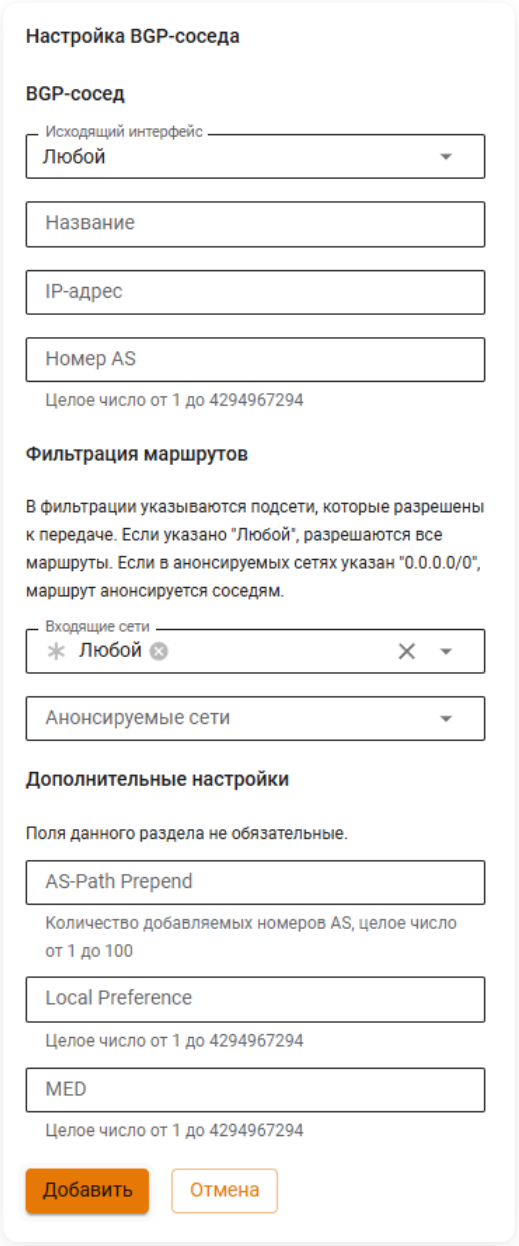
Graceful Restart - механизм обеспечения непрерывности маршрутизации, позволяющий сетевому устройству временно перезапустить управляющую плоскость (например, при обновлении ПО или восстановлении после сбоя) без немедленного перерасчета маршрутов у соседних устройств.

При включении **Graceful Restart** соседние маршрутизаторы не рассматривают кратковременный разрыв управления как отказ и продолжают использовать ранее полученные маршруты в течение ограниченного периода ожидания (120 секунд). Это позволяет избежать частых изменений состояния маршрутов и снижает влияние плановых или аварийных перезапусков на работу сети.

Graceful Restart работает только при поддержке со стороны соседних маршрутизаторов.

Настройка BGP-соседей

Для добавления BGP-соседа нажмите **Добавить** и заполните поля:

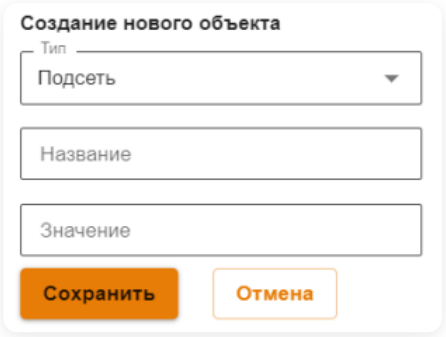


Расшифровка полей

- **Исходящий интерфейс** - интерфейс Ideco NGFW Novum, IP-адрес которого будет использован для обмена маршрутами. Для надежности и стабильности работы службы рекомендуем выбрать Loopback-интерфейс. Если выбран **Любой**, будет использоваться ближайший к соседу интерфейс. Для динамической маршрутизации поверх VPN-туннеля можно выбрать туннельный интерфейс **IPsec** или **IPsec GRE**.
- **Название** - любое значение.
- **IP-адрес** - IP-адрес BGP-соседа. Рекомендуем указать адрес Loopback-интерфейса соседа.
- **Номер AS** - номер автономной системы BGP-соседа.
- **Входящие сети** - сети, информацию от которых хотите получать. Если нужного объекта для фильтрации нет, то нажмите **Создать новый объект**. Если выбран объект **Любой**, то фильтрация будет отключена и будут приниматься все сети от BGP-соседа. Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру **0.0.0.0/0**.
- **Анонсируемые сети** - сети, информацию о которых хотите отправлять. Если нужного объекта для фильтрации нет, то нажмите **Создать новый объект**. Если выбран объект **Любой**, то фильтрация будет отключена и будет передаваться информация обо всех маршрутах, известных NGFW Novum (redistribute static, connected, ospf). Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру **0.0.0.0/0**.
- **AS-Path Prepend** - чем больше значение, тем менее приоритетным становится канал.
- **Local Preference** - определяет приоритет пути для выхода трафика. Чем больше значение, тем более приоритетным становится канал.
- **MED** - определяет приоритет пути для входа трафика. Чем меньше значение, тем приоритетнее путь.

Создание нового объекта

В поле **Входящие сети** или **Анонсируемые сети** нажмите **Создать новый объект** и заполните поля:



- **Тип** - значение **Подсеть**.
- **Название** - любое значение.
- **Значение** - значение подсети в формате: `подсеть/маска подсети`, например, `192.168.100.0/24`.

После настройки можно проверить состояние BGP-сессий с помощью утилиты `vtysh`. Примеры использования утилиты смотрите в статье.

Для динамической маршрутизации сетей двух NGFW Novum, соединенных по IPsec в туннельном режиме, воспользуйтесь BGP. Подробнее про настройку подключения двух NGFW Novum по IPsec - в статье.

Для **Входящих сетей** и **Анонсируемых сетей** объект **Любой** не может быть установлен одновременно с другими фильтрами.

OSPF

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **OSPF**: `frr`; `ideco-routing-backend`, `ideco-routing-rest`.

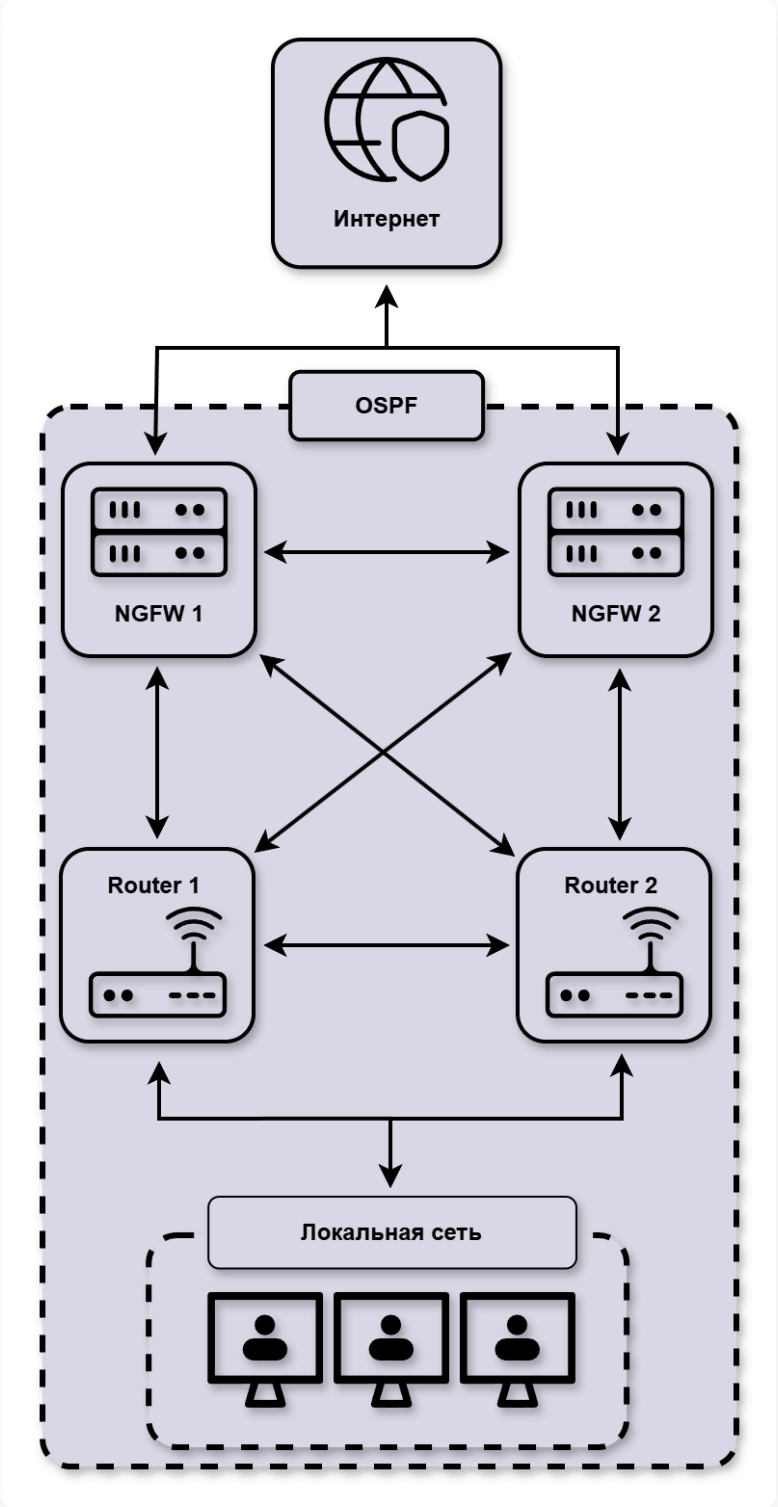
Список служб для других разделов доступен по ссылке.

Ideco NGFW Novum поддерживает OSPFv2 (Open Shortest Path First) - протокол динамической маршрутизации, который определяет оптимальные пути передачи данных на основе состояния каналов (интерфейсов маршрутизаторов или сетевых сегментов).

Рекомендуем использовать модуль в сетях, где применяется балансировка нагрузки на сеть и резервирование каналов.

При одинаковой стоимости нескольких путей до одного назначения используется ECMP (Equal-Cost Multi-Path) для балансировки нагрузки.

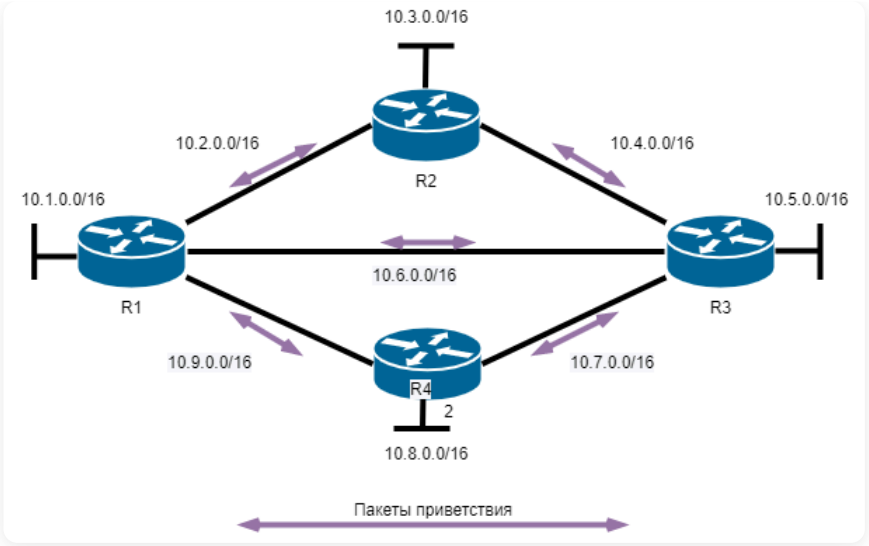
Пример топологии с использованием OSPF представлен на схеме



Принцип работы маршрутизации по состоянию канала

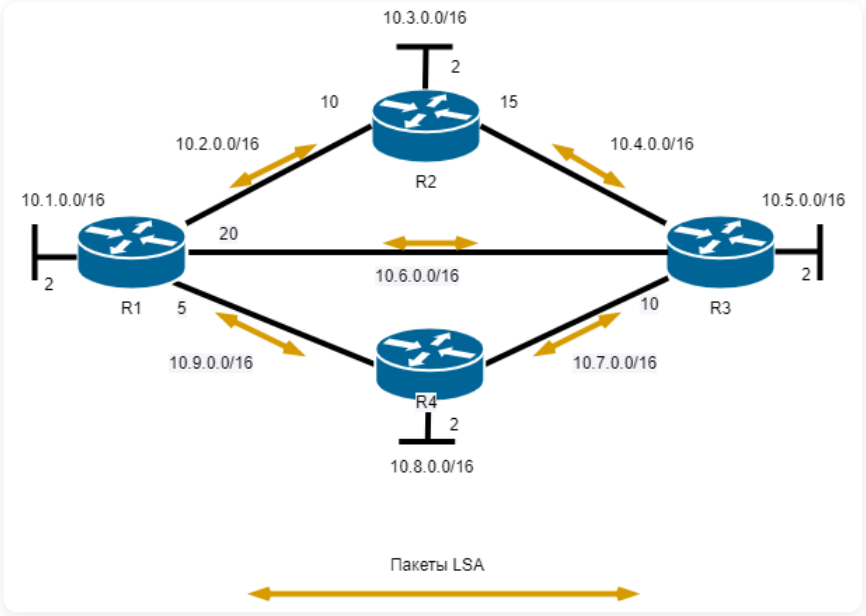
1. Установление отношений смежности с соседними устройствами

Маршрутизатор, использующий OSPF, отправляет hello-пакеты на мультикастовый адрес 224.0.0.5 со всех интерфейсов, где запущен OSPF. При наличии соседнего устройства маршрутизатор пытается установить с ним отношения смежности.



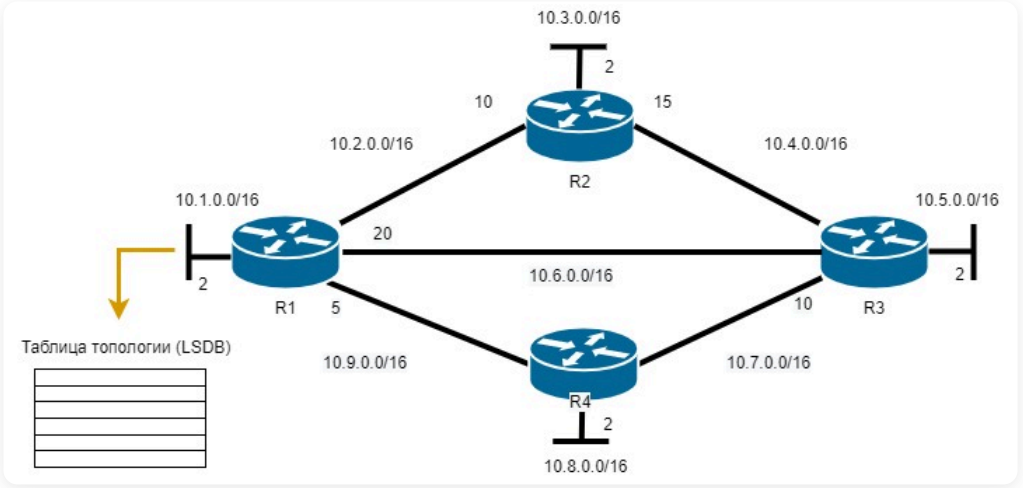
2. Обмен объявлениями о состоянии каналов

После установления смежности устройства выполняют обмен LSA. Пакеты LSA содержат информацию о состоянии и стоимости каждого канала с прямым подключением.



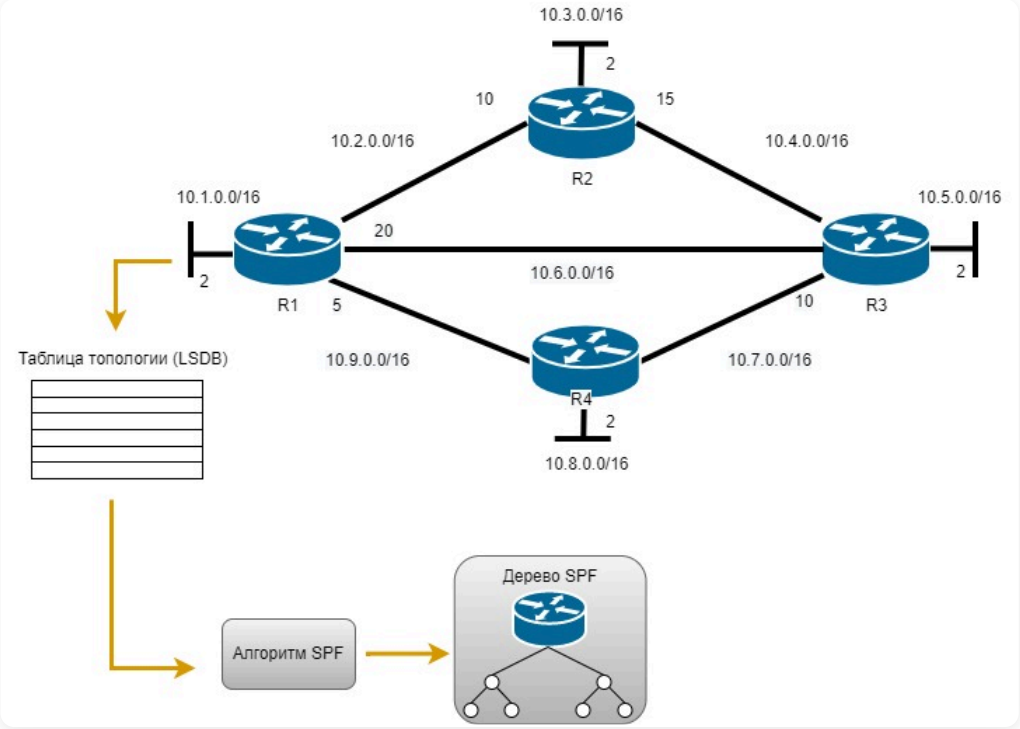
3. Создание базы данных состояния связи

На основе объявления LSA маршрутизаторы собирают базу данных, в которой содержатся данные о топологии сети в области.



4. Исполнение алгоритма SPF

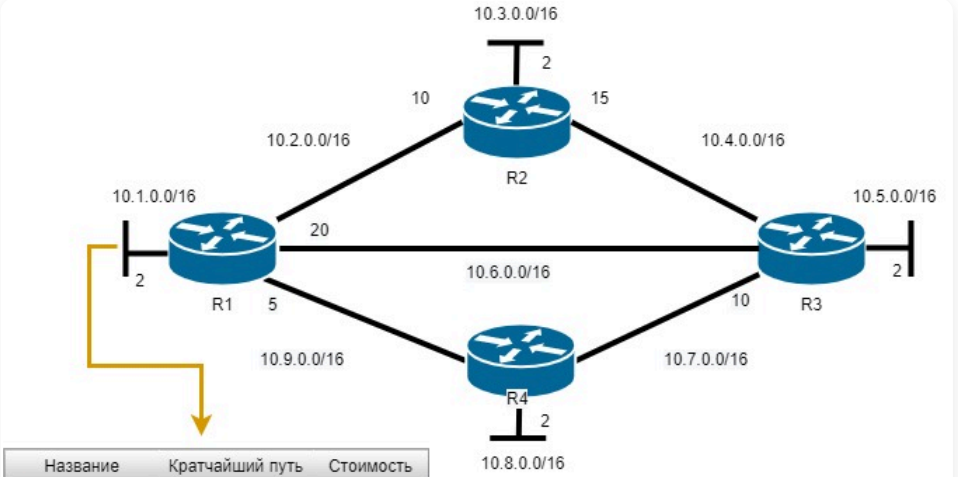
На устройствах выполняется алгоритм SPF, результатом которого является создание дерева кратчайших путей.



5. Выбор лучшего маршрута

На основании данных дерева SPF обновляются данные в таблице IP-маршрутизации.
Маршрут добавляется в таблицу маршрутизации, если отсутствует источник маршрута к той же сети с меньшим административным расстоянием, например, статический маршрут.

Решения по маршрутизации пакетов принимаются на основе записей в таблице маршрутизации.



Название	Кратчайший путь	Стоимость
10.3.0.0/16	R1 -> R2	12
10.4.0.0/16	R1 -> R2	25
10.5.0.0/16	R1 -> R3	22
10.7.0.0/16	R1 -> R4	17
10.8.0.0/16	R1 -> R4	7

Для настройки OSPF в Ideco NGFW Novum перейдите в **Маршрутизация** → **OSPF** и выполните действия на вкладках:

Основные

Ideco NGFW Novum автоматически заполняет поле **Router ID** значением наибольшего IP-адреса локальной сети, указанного в разделе **Сетевые интерфейсы**. При необходимости измените IP-адрес в разделе **Сетевые интерфейсы**.

Аутентификация соседей применяется для всех настроенных OSPF-интерфейсов. Важна для защиты маршрутной информации от несанкционированного вмешательства:

- Предотвращение подмены соседей (Spoofing) - злоумышленник не сможет подключиться к OSPF-домену, представившись легальным маршрутизатором, и передавать фальшивые LSA (Link-State Advertisements).
- Перехват и изменение OSPF-пакетов (например, подмена метрик или топологии).

Если пакет изменен, то хеш не будет совпадать и пакет будет отброшен. Хеш вычисляется на основе:

- Содержимого пакета (заголовок и данные).
- Секретного ключа, известного только доверенным маршрутизаторам.

Принцип работы MD5-аутентификации

На всех маршрутизаторах в одной зоне OSPF задается:

- Идентификатор ключа (Key ID).
- Секретный ключ (пароль).

При отправке OSPF-пакета маршрутизатор добавляет к нему:

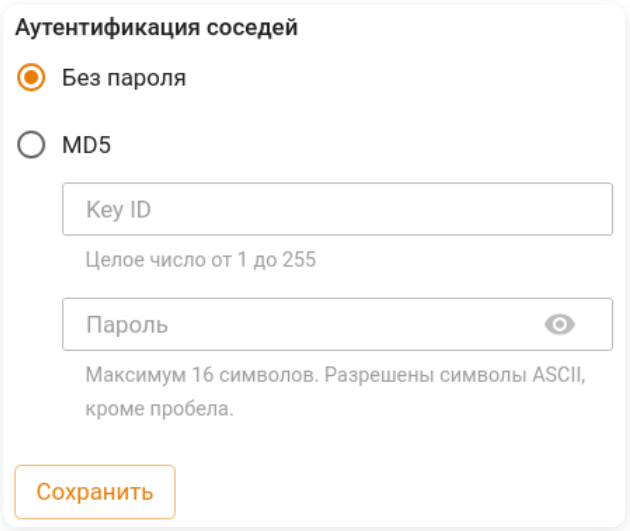
- Key ID.
- MD5-хеш, вычисленный по формуле: `MD5(OSPF_пакет + Секретный_ключ + Key_ID)`.

Принимающая сторона (получатель):
1. Берет Key ID из пакета.
2. Находит у себя секретный ключ, соответствующий переданному Key ID.
3. Вычисляет MD5-хеш по той же формуле и сравнивает с полученным:

- Если хеши совпали, пакет принимается.
- Если хеши не совпали, пакет отбрасывается с ошибкой.

> Все маршрутизаторы в зоне OSPF должны использовать MD5-аутентификацию, а также одинаковые Key ID и секретный ключ.

Настройка аутентификации



- **Без пароля** - вариант, если не нужно использовать аутентификацию. Выбран по умолчанию после миграции с Ideco NGFW Novum 19 версии.
- **MD5**:
  - **Key ID** - идентификатор ключа. Число в диапазоне от 1 до 255.
  - **Пароль** - секретный ключ.

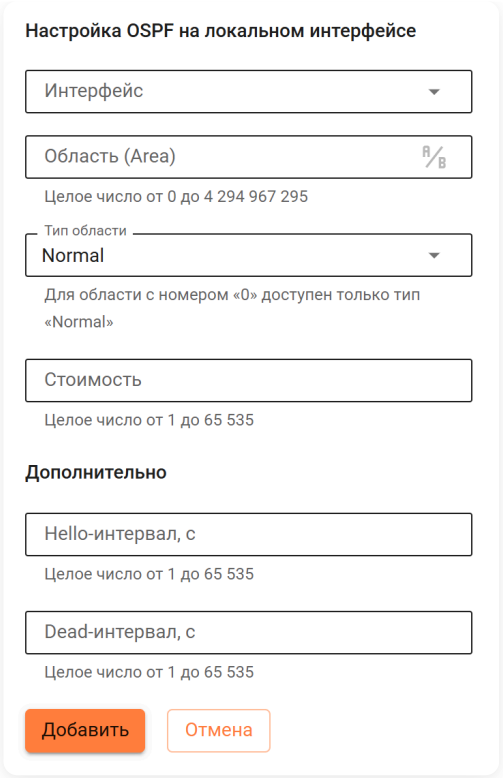
Требования к паролю

- **Максимальная длина пароля** - 16 символов.
- **Символы** - любые ASCII-символы, за исключением пробелов.

Настройка OSPF

1. Перейдите в **Маршрутизация** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



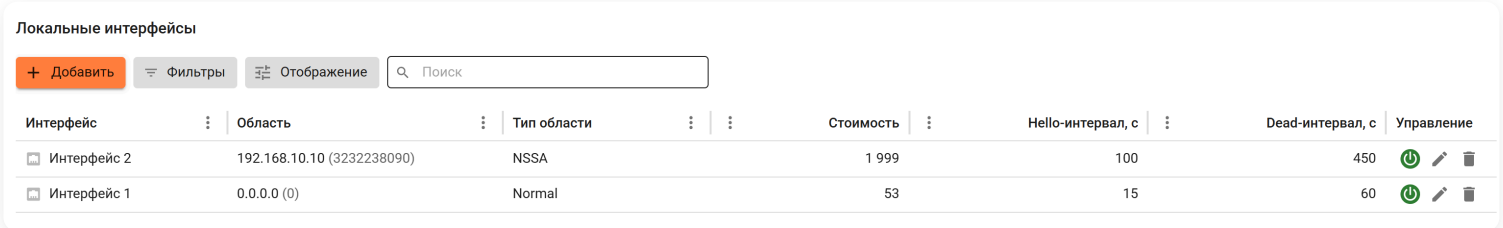
- **Интерфейс** - локальный или Loopback-интерфейс Ideco NGFW Novum, IP-адрес которого будет использован для обмена маршрутами.
- **Область (Area)** - номер области (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Тип области** - для области с указанным номером `area` должен быть выбран одинаковый тип при настройке всех OSPF-соседей. Для области с номером 0 (`0.0.0.0`) допустимо указывать только один тип - **Normal**. Допустимые значения: **Normal**, **Stub**, **NSSA**:
  - **Normal Area** (обычная зона) - стандартная зона OSPF, которая получает полную информацию о маршрутах как внутри автономной системы, так и за ее пределами. В такой зоне могут находиться как маршрутизаторы, так и конечные устройства.
  - **Stub Area** (усеченная зона) - зона, в которой не принимаются внешние маршруты (Type 5 LSA), но принимаются маршруты других зон. Вместо полной информации о внешних маршрутах используется маршрут по умолчанию.
  - **NSSA** (Not-So-Stubby Area) - разновидность Stub-зоны, которая может получать маршруты по умолчанию и отправлять свои маршруты в другие зоны через **ABR** (Area Border Router). В **NSSA** зоне используется специальный тип LSA (Type 7), который преобразуется в Type 5 на ABR.
- **Стоимость** - стоимость маршрута.
- **Hello-интервал** - время между отправкой Hello-пакетов, которое варьируется от 1 до 65535 секунд. Если поле не заполнено, по умолчанию используется значение 10 секунд. Для установления соседства между устройствами интервал должен быть одинаковым для всех участников сети.
- **Dead-интервал** - время, через которое сосед считается недоступным, если не получает Hello-пакеты. Диапазон значений - от 1 до 65535 секунд. Если поле не заполнено, по умолчанию в 4 раза больше, чем Hello-интервал. Для успешного соседства значение должно быть одинаковым у всех устройств в сегменте сети.

3. Нажмите **Добавить**.

4. Включите модуль **OSPF**.

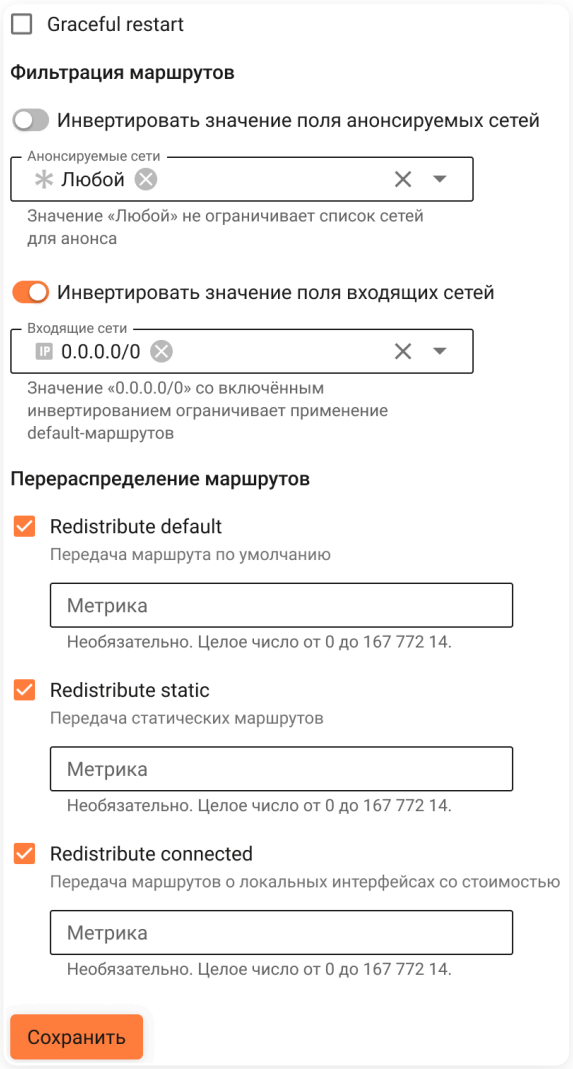
> Добавьте в таблицу OSPF **Loopback-интерфейс**, если на вкладке **Дополнительно** отключена опция **Redistribute connected** (по умолчанию включена), чтобы сети **Loopback-интерфейсов** анонсировались.

Пример готовой таблицы:



При наличии большого количества настроек OSPF в таблице воспользуйтесь кнопкой **Фильтры**.

Дополнительные



Graceful Restart - механизм обеспечения непрерывности маршрутизации, позволяющий сетевому устройству временно перезапустить управляющую плоскость (например, при обновлении ПО или восстановлении после сбоя) без немедленного перерасчета маршрутов у соседних устройств.

При включении **Graceful Restart** соседние маршрутизаторы не рассматривают кратковременный разрыв управления как отказ и продолжают использовать ранее полученные маршруты в течение ограниченного периода ожидания (120 секунд). Это позволяет избежать частых изменений состояния маршрутов и снижает влияние плановых или аварийных перезапусков на работу сети.

> **Graceful Restart** работает только при поддержке со стороны соседних маршрутизаторов.

Фильтрация маршрутов - фильтр для маршрутов, передаваемых и принимаемых от OSPF-соседей:

- **Анонсируемые сети** - маршруты, которые отправляются OSPF-соседям. По умолчанию используется значение **Любой**. Поле также фильтрует сети из блока **Перераспределение маршрутов**:
  - **Инвертировать значение поля анонсируемых сетей** - если опция включена, то OSPF-соседям будут отправлены маршруты ко всем сетям, кроме тех, что указаны в поле **Анонсируемые сети**.
- **Входящие сети** - маршруты, которые принимаются от OSPF-соседей. По умолчанию используется значение **Любой**, кроме `0.0.0.0/0`:
  - **Инвертировать значение поля входящих сетей** - если опция включена, то от OSPF-соседей будут приняты маршруты ко всем сетям, кроме указанных в поле **Входящие сети**.

Перераспределение маршрутов:

- **Redistribute default** - при включении опции для других устройств NGFW Novum будет являться шлюзом по умолчанию.
- **Redistribute static** - при включении опции будут анонсироваться статические маршруты, указанные в разделе **Маршрутизация** → **Статическая**, а также маршруты до VPN-сетей.

- **Redistribute connected** - при включении опции будут анонсироваться маршруты подсетей, подключенных напрямую, в том числе и Loopback-интерфейсов.

> Если **Redistribute connected** отключить, сети Loopback-интерфейсов будут анонсироваться при добавлении в таблицу OSPF **Loopback-интерфейса**.

Подробнее о значении поля **Метрика** - в статье.

Примеры работы фильтрации маршрутов

При включении опции:

- **Redistribute default** - чтобы NGFW Novum анонсировал себя как шлюз по умолчанию, в поле **Анонсируемые сети** укажите **Любой** или `0.0.0.0/0`.
- **Redistribute static** - если в **Маршрутизация** → **Статическая** задано шесть маршрутов, но в поле **Анонсируемые сети** указаны только три из них, то **OSPF** будет анонсировать только указанные **Анонсированные сети** OSPF-соседям.
- **Redistribute connected** - для исключения части подключенных напрямую сетей в поле **Анонсируемые сети** пропишите список сетей, которые необходимо анонсировать. Остальные подключенные сети анонсироваться не будут.

Настройка MikroTik

1. Авторизуйтесь на MikroTik и выполните команду:

```
routing ospf area add area-id=x.x.x.x default-cost=1 disabled=no inject-summary-lsa=no name=area1 type=default
```

- `x.x.x.x` - название зоны, которое указали при настройке Ideco NGFW Novum. ID должен быть уникален для каждого роутера.

2. Для передачи любых других сетей соседним устройствам по динамической маршрутизации введите команду:

```
routing ospf network add network=(другая подсеть)/24 area=area1
```

3. Повторите команду из пункта 1 для добавления каждой подсети.

4. Для вывода таблицы маршрутизации введите команду: `ip route print`.

Настройка Cisco

1. Запустите на Cisco процесс OSPF:

```
enable
conf t
router ospf 1
```

2. По умолчанию отключите отправку hello-пакетов на всех интерфейсах и включите на нужных интерфейсах:

```
passive-interface default
no passive-interface GigabitEthernet0/0
```

- `GigabitEthernet0/0` - название интерфейса.

3. Укажите сети, маршруты до которых хотите анонсировать:

```
network <IP-адрес подсети> <wildcart-маска подсети> area <номер зоны, указанный при настройке Ideco NGFW Novum>
```

Пример команды:

```
network 192.168.100.0 0.0.255.255 area 0
```

4. Если Cisco получил уведомление вида `*Dec 18 10:02:03.628: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.122.73 on GigabitEthernet0/0 from LOADING to FULL, Loading Done`, соседские отношения установлены.

5. Для просмотра списка соседей воспользуйтесь командой `show ip ospf neighbor`:

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.122.73    1   FULL/DR         00:00:38    192.168.102.11  GigabitEthernet0/0
Router#
```

6. Для вывода таблицы маршрутизации введите команду `show ip route` (в таблице должны появиться маршруты до сетей NGFW Novum):

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.102.11 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      10.0.0.0/16 is subnetted, 1 subnets
O E2     10.128.0.0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.100.0/32 is subnetted, 1 subnets
O E2     192.168.100.100
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.102.0/24 is directly connected, GigabitEthernet0/0
L        192.168.102.79/32 is directly connected, GigabitEthernet0/0
      192.168.103.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.103.0/24 is directly connected, GigabitEthernet0/1
L        192.168.103.130/32 is directly connected, GigabitEthernet0/1
O E2  192.168.122.0/24
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
```

Особенности работы OSPF в Ideco NGFW Novum

- В предустановленной конфигурации Ideco NGFW Novum - шлюз по умолчанию для других устройств.
- OSPF работает на локальных Ethernet-интерфейсах и на ГОСТ, GRE, GRE over IPsec интерфейсах.
- Значение **Типа сети** (**Network Type**) в Ideco NGFW Novum устанавливается автоматически в зависимости от типа интерфейса, используемого для OSPF:
  - GRE-интерфейсы - значение `p2p`.
  - Ethernet-интерфейсы - значение `broadcast`.

Примеры использования

Объединение филиальной сети с резервированием и/или балансировкой

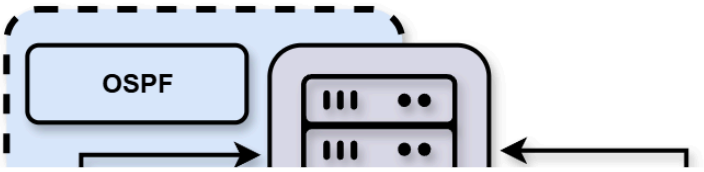


- Между **NGFW Novum-1** в Филиале 1 и **NGFW Novum-2** в Филиале 2 настраивается GRE-over-IPsec и OSPF.
- Каждый NGFW Novum подключен к двум провайдерам (**Провайдер-1** и **Провайдер-2**).

Преимущества настройки:

- Трафик будет автоматически балансироваться между **Провайдером-1** и **Провайдером-2**.
- При неисправности одного из провайдеров трафик автоматически смаршрутизируется через другое соединение.
- Отсутствует необходимость вручную настраивать маршруты до локальных сетей филиалов.

Схема с балансировкой доступа из локальной сети в интернет или другую сеть



- И **NGFW Novum-1**, и **NGFW Novum-2** используются в качестве шлюза по умолчанию.
- Между балансировщиком и каждым из NGFW Novum настроена OSPF.

Преимущества настройки:

- Трафик балансируется между **NGFW Novum-1** и **NGFW Novum-2**: часть пользователей из Локальной сети выходят в интернет через **NGFW Novum-1**, часть - через **NGFW Novum-2**.
- При неисправности одного из NGFW Novum трафик автоматически смаршрутизируется через другое соединение.
- Отсутствует необходимость вручную настраивать маршруты для хостов в Локальной сети.

Анонс конкретного хоста (/32)

Необходимо анонсировать конкретный хост `192.168.0.100/32` и обеспечить его распространение через OSPF на **NGFW Novum-2**, не передавая при этом всю сеть `192.168.0.0/24`.

Схема сети:

- **NGFW Novum-1** подключен к локальной сети `192.168.0.0/24`.
- **NGFW Novum-2** подключен к локальной сети `192.168.2.0/24`.
- Между ними настроен GRE-over-IPsec, в котором работает OSPF.

Выполните действия:

1. Перейдите в **Маршрутизация** → **Статическая** и добавьте маршрут:

- **Название** - укажите название маршрута.
- **Назначение** - выберите `192.168.0.100`.
- **Отправлять в** - выберите `192.168.0.1`.
- **Приоритет** - укажите необходимый приоритет маршруту.

2. Перейдите в **Маршрутизация** → **OSPF** → **Дополнительно** и настройте **Фильтрацию маршрутов**:

- **Анонсируемые сети** - выберите подсеть `192.168.0.100/32`.
- **Redistribute static** - включите опцию.

3. Нажмите **Сохранить**.

EIGRP

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **EIGRP**: `frr`; `ideco-routing-backend`, `ideco-routing-rest`.

Список служб для других разделов доступен по ссылке.

EIGRP (Enhanced Interior Gateway Routing Protocol) - продвинутый дистанционно-векторный протокол маршрутизации, разработанный компанией Cisco. EIGRP поддерживает высокую скорость обмена информацией о маршрутах для обеспечения актуальности таблиц маршрутизации.

Настройка модуля EIGRP на Ideco NGFW Novum состоит из шагов:

Шаг 1. Настройка аутентификации (MD5)

Для маршрутизаторов с EIGRP MD5-аутентификацию можно не настраивать только в доверенной и контролируемой среде, где уже есть защита или нет рисков.

Маршрутизаторы с разными или неверными ключами не будут устанавливать соседство - снижается риск подмены и несанкционированного участия в EIGRP.

Принцип работы MD5-аутентификации

На всех маршрутизаторах в одной зоне EIGRP задается:

- Идентификатор ключа (Key ID).
- Секретный ключ (пароль).

При отправке EIGRP-пакета маршрутизатор добавляет к нему:

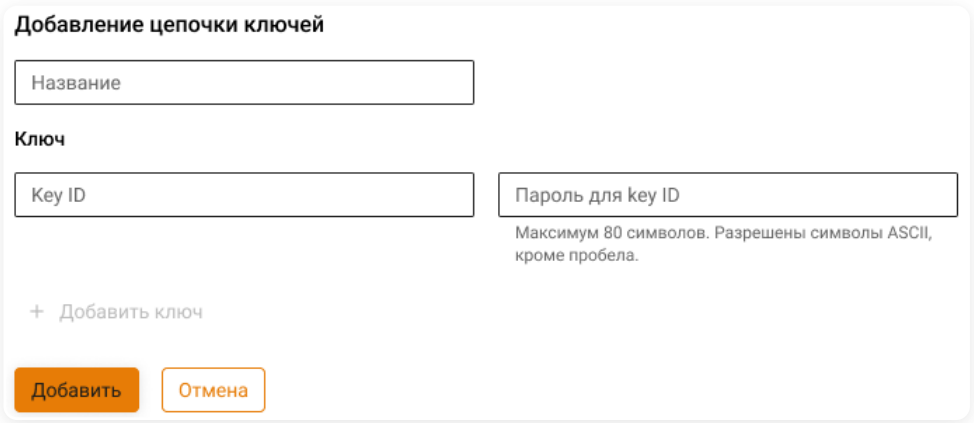
- Key ID.
- MD5-хеш, вычисленный по формуле: `MD5(EIGRP_пакет + Секретный_ключ + Key_ID)`.

Принимающая сторона (получатель):

1. Берет Key ID из пакета.
2. Находит у себя секретный ключ, соответствующий переданному Key ID.
3. Вычисляет MD5-хеш по той же формуле и сравнивает с полученным:

- Если хеши совпали, пакет принимается.
- Если хеши не совпали, пакет отбрасывается с ошибкой.

1. Перейдите в **Маршрутизация** → **EIGRP** → **Ключи** и нажмите **Добавить**:



- **Название** - введите название цепочки ключей. Название может быть неуникальным.
- **Key ID** - введите идентификатор ключа. Число в диапазоне от 1 до 255.
- **Пароль для key ID** - введите пароль для ключа.

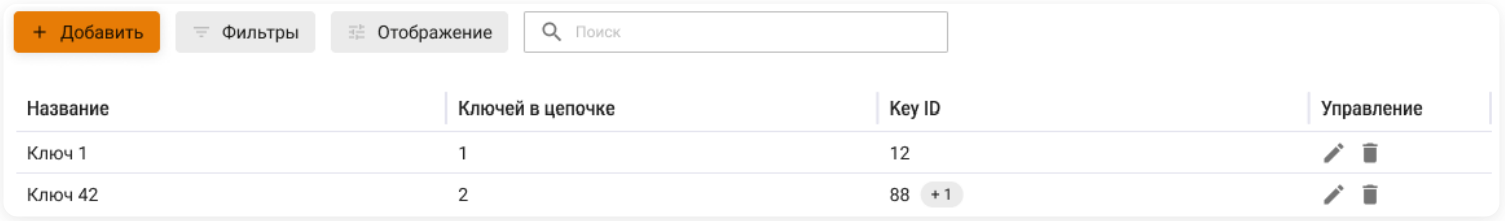
Требования к паролю

- **Максимальная длина пароля** - 80 символов.
- **Символы** - любые ASCII-символы, за исключением пробелов.

2. При необходимости добавьте в цепочку дополнительные ключи, нажав **Добавить ключ**.

3. Нажмите **Добавить**.

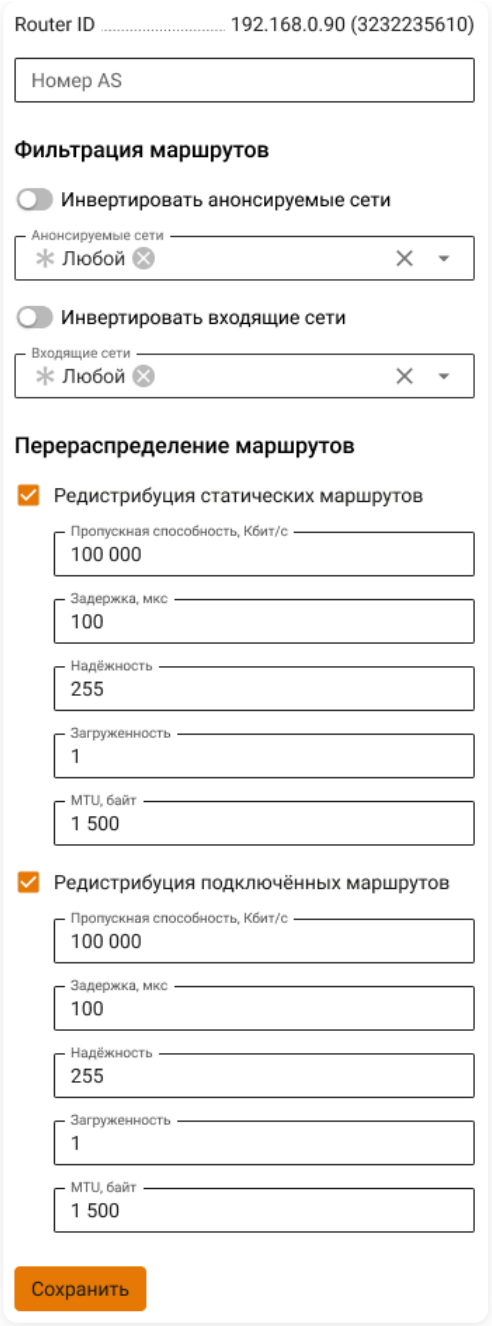
Созданные цепочки ключей отображаются в таблице:



Шаг 2. Настройка автономной системы EIGRP

Перед настройкой соседей необходимо на Ideco NGFW Novum указать номер автономной системы (AS) и активировать модуль.

1. Перейдите в **Маршрутизация** → **EIGRP** → **Настройки**:



2. Введите **Номер AS**. Маршрутизаторы с одной автономной системой обмениваются маршрутами и устанавливают соседство. Маршрутизаторы с разными AS друг с другом по EIGRP не взаимодействуют.

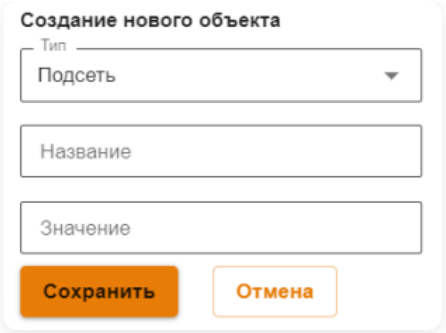
3. Настройте **Фильтрацию маршрутов**:

- **Анонсируемые сети** - список сетей, которые разрешено отправлять в EIGRP другим соседям.
- **Входящие сети** - список сетей, которые разрешено принимать от соседей по EIGRP и добавлять в таблицу маршрутизации.

Опции инвертирования позволяют использовать списки анонсируемых и входящих сетей наоборот, когда разрешено все, кроме указанных сетей.

Создание нового объекта

В поле **Анонсируемые сети** или **Входящие сети** нажмите **Создать новый объект** и заполните поля:



- **Тип** - значение **Подсеть**.
- **Название** - любое значение.
- **Значение** - значение подсети в формате: `подсеть/маска подсети`, например, `192.168.100.0/24`.

4. При необходимости настройте **Перераспределение маршрутов**:

- **Редистрибуция статических маршрутов** - при включении опции будут анонсироваться статические маршруты, указанные в разделе **Маршрутизация** → **Статическая**, а также маршруты до VPN-сетей.
- **Редистрибуция подключенных маршрутов** - при включении опции будут анонсироваться маршруты подсетей, подключенных напрямую, в том числе и Loopback-интерфейсов.

> Если **Редистрибуция подключенных маршрутов** отключена, сети Loopback-интерфейсов будут анонсироваться при добавлении **Loopback-интерфейса** в таблицу **Интерфейсы**.

При необходимости для каждого типа перераспределения задайте метрики:

- **Пропускная способность** - минимальная пропускная способность на всем пути к сети (Кбит/с). Чем выше пропускная способность, тем предпочтительнее маршрут. По умолчанию 100 000 Кбит/с.
- **Задержка** - сумма задержек интерфейсов на пути, в десятках микросекунд. По умолчанию 100.
- **Надежность** - оценка надежности канала (0–255), обычно от статистики потерь пакетов. По умолчанию 255.
- **Загруженность** - загрузка канала (0–255). По умолчанию 1.
- **MTU** - максимальный размер пакета на пути, в байтах. По умолчанию 1500.

> Обычно значений метрик по умолчанию достаточно для большинства сценариев. EIGRP использует композитную метрику (одно число), которая рассчитывается из указанных параметров. Задавайте их явно только при необходимости тонко управлять выбором пути.

5. Нажмите **Сохранить**.

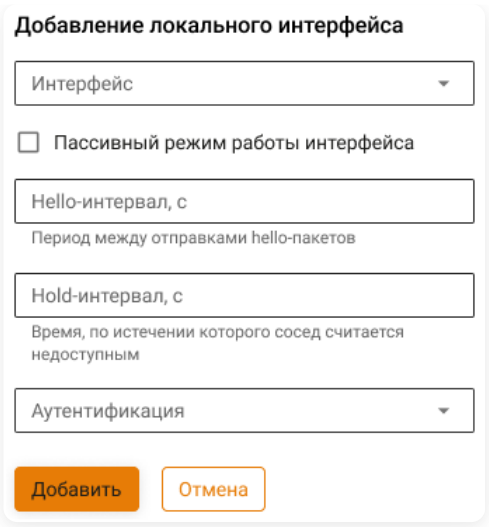
6. Включите модуль **EIGRP**.

Шаг 3. Настройка интерфейсов, участвующих в процессе EIGRP

> Если интерфейс не добавлен в таблицу или не активен, EIGRP на нем работать не будет.

Для каждого из сетевых интерфейсов, участвующих в EIGRP, на Ideco NGFW Novum выполните шаги:

1. Перейдите в **Маршрутизация** → **EIGRP** → **Интерфейсы** и нажмите **Добавить**:



2. Выберите интерфейс, на котором запускается протокол EIGRP в поле **Интерфейс**.

3. Включите опцию **Пассивный режим работы интерфейса**, если нужно, чтобы выбранный интерфейс участвовал в EIGRP, но не отправлял и не принимал EIGRP-пакеты. Интерфейс будет анонсировать свою сеть, но соседство с другими маршрутизаторами через него не устанавливается. При выборе пассивного режима остальные параметры интерфейса станут недоступны.

Пассивный режим работы интерфейса полезен, когда требуется подключить сеть в EIGRP, не создавая лишнего трафика и соседства (например, stub-сети).

4. Установите параметры интерфейса, если требуется:

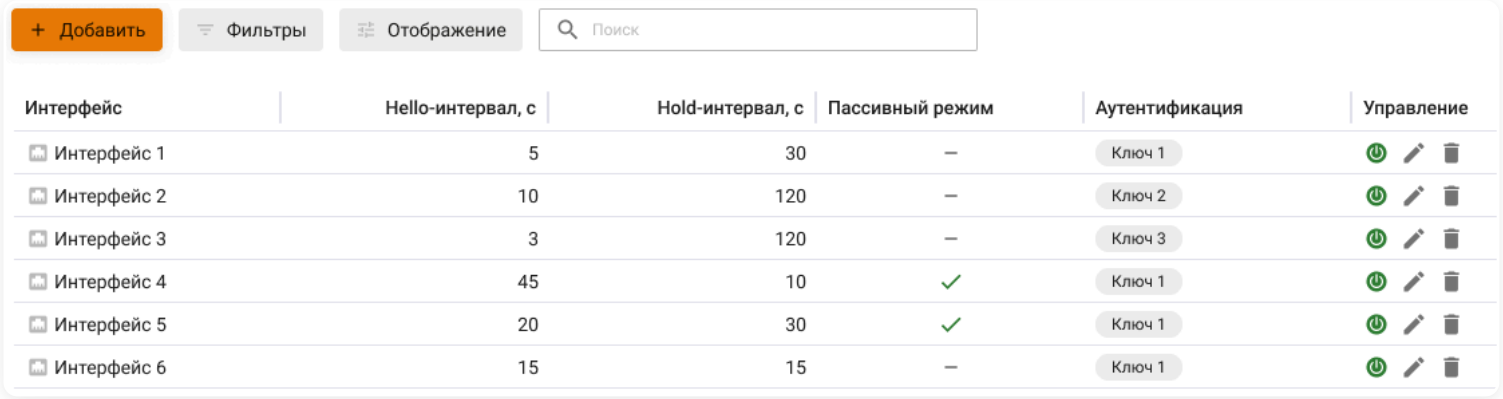
- **Hello-интервал** - интервал в секундах, с которым маршрутизатор отправляет пакеты Hello на multicast-адрес.
- **Hold-интервал** - максимальное время (в секундах) без пакетов Hello, после которого сосед считается потерянным и соседство сбрасывается.
- **Аутентификация** - выберите цепочку ключей, если используете MD5-аутентификацию.

5. Нажмите **Сохранить**.

Если соседство не устанавливается при включенной MD5, проверьте, что:

- Имя цепочки ключей привязано к интерфейсу.
- На соседнем устройстве настроен тот же ключ (ID и пароль).
- В логах системы нет ошибки `authentication mismatch`.

Интерфейсы, участвующие в маршрутизации EIGRP, отображаются в таблице:



При перенастройке EIGRP на Ideco NGFW Novum возможна кратковременная потеря связи с соседями.

Если после изменения настроек EIGRP перестал работать (например, соседи долго не появляются), выключите и включите модуль **EIGRP** вручную.

Маршрутизация внешних сетей

Классический контекст | Высокопроизводительный контекст | API

Позволяет направлять трафик от разных пользователей или групп пользователей по заданным маршрутам. Маршрутизация внешних сетей применяется после PBR, статической и динамической маршрутизации.

Способы применения:

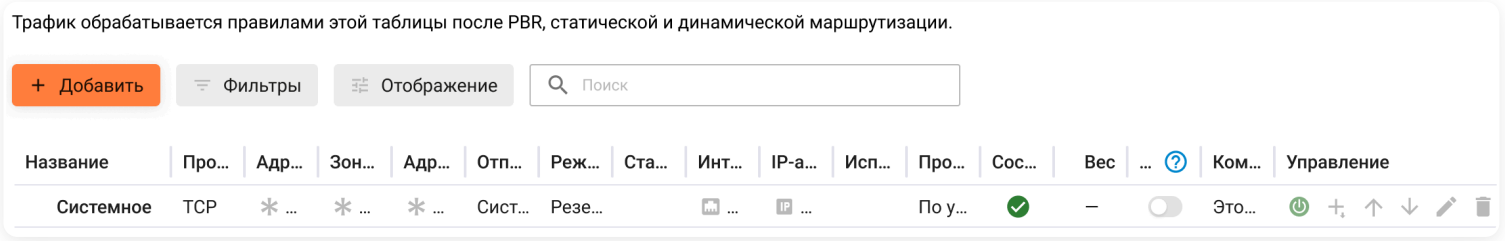
- Направление части трафика через интернет-провайдера с наименьшей стоимостью этого трафика.
- Предоставление доступа в интернет через одного из провайдеров для определенных пользователей/групп пользователей.

Маршруты в таблице имеют приоритет сверху вниз, то есть **верхний маршрут приоритетнее нижнего**.

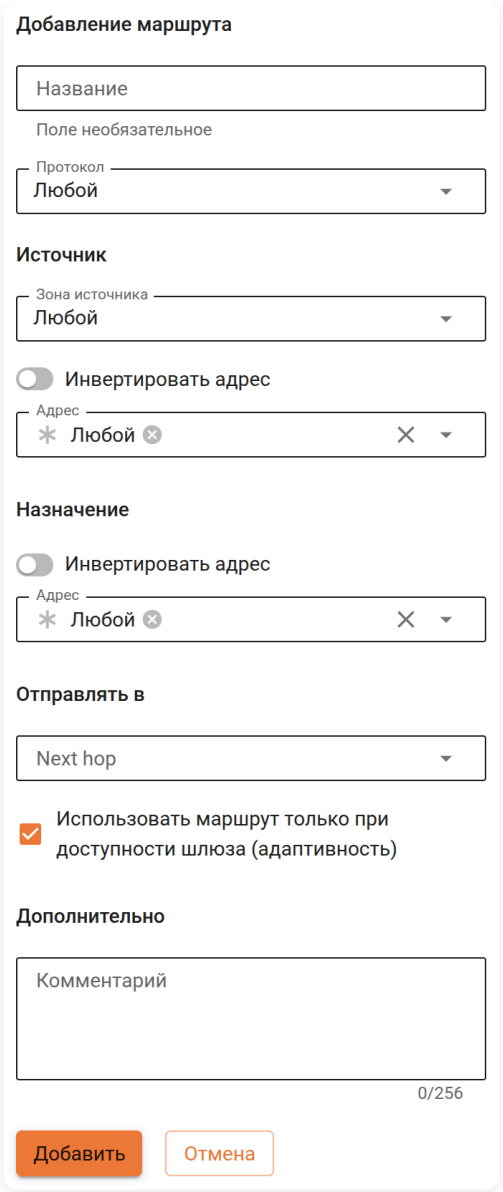
Перед обновлением на Ideco NGFW Novum версии 22 ознакомьтесь с информацией по ссылке.

Действия для настройки:

1. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - введите название маршрута.
- **Протокол** - выберите протокол передачи данных: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP).
- **Источник**:
  - **Зона** - выберите интерфейс или группу интерфейсов Ideco NGFW Novum, на которые приходит трафик от источника. Объект типа **Зона** можно создавать и редактировать только в **Системном контексте**.
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - выберите объект, трафик от которого нужно маршрутизировать. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
  - **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.
  - **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

Не рекомендуем указывать порт источника, так как он обычно выбирается случайным образом. Исключение - протоколы с фиксированными портами источника и назначения (например, DNS).

- **Назначение**:
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - выберите объекты, при обращении к которым будет применяться этот маршрут. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
  - **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.

- **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

- **Отправлять в** - выберите вариант, через который будет направляться трафик. В поле могут быть выбраны: Next hop, Профили next hop, IP-адреса или Статическая маршрутизация. IP-адрес можно указать как **Объект** или **Значение**. При выборе Статической маршрутизации NGFW Novum трафик перенаправляется в таблицу **Статической маршрутизации**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

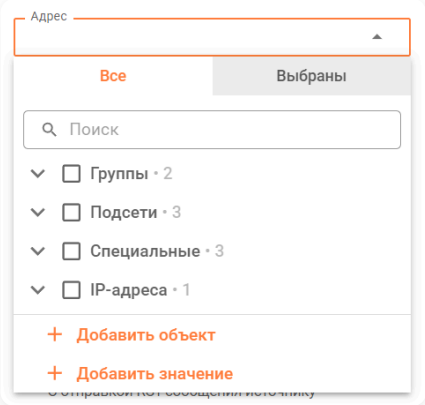
Отличие значений от объектов:

- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

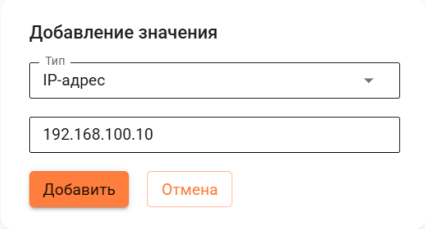
Управление значениями

Добавление

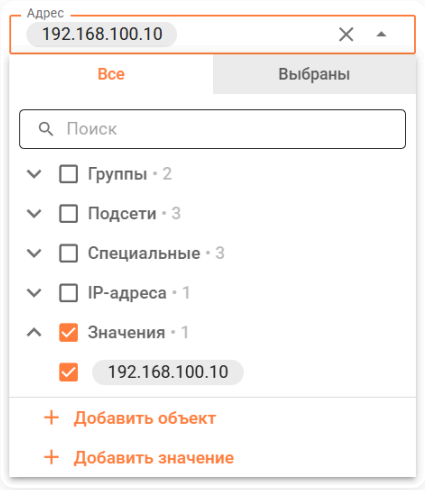
1. В поле нажмите **Добавить значение**:



2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:

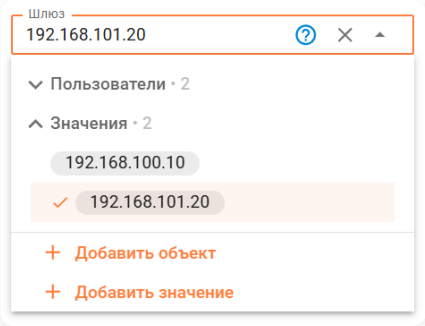


Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:



2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

- **Использовать маршрут только при доступности шлюза (адаптивность)** - включите опцию, чтобы маршрутизатор при недоступности **Next hop** продолжал поиск маршрута по нижестоящим правилам. Если опция отключена, трафик отбрасывается, а отправителю возвращается ошибка `destination unreachable`.
- **Дополнительно**:
  - **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

Адаптивность

Опция **Использовать маршрут только при доступности шлюза (адаптивность)** требует настроенной проверки доступности шлюза. Без проверки доступности NGFW Novum не сможет определить, что шлюз недоступен, и адаптивность не сработает.

Настроить проверку доступности можно одним из способов:

Next hop

Используйте этот способ, если в поле **Отправлять в** указан **Next hop**.

1. Перейдите в **SD-WAN** → **Next hop**.

2. Нажмите напротив нужного next hop.

3. Включите опцию **Использовать BFD**.

4. Нажмите **Сохранить**.

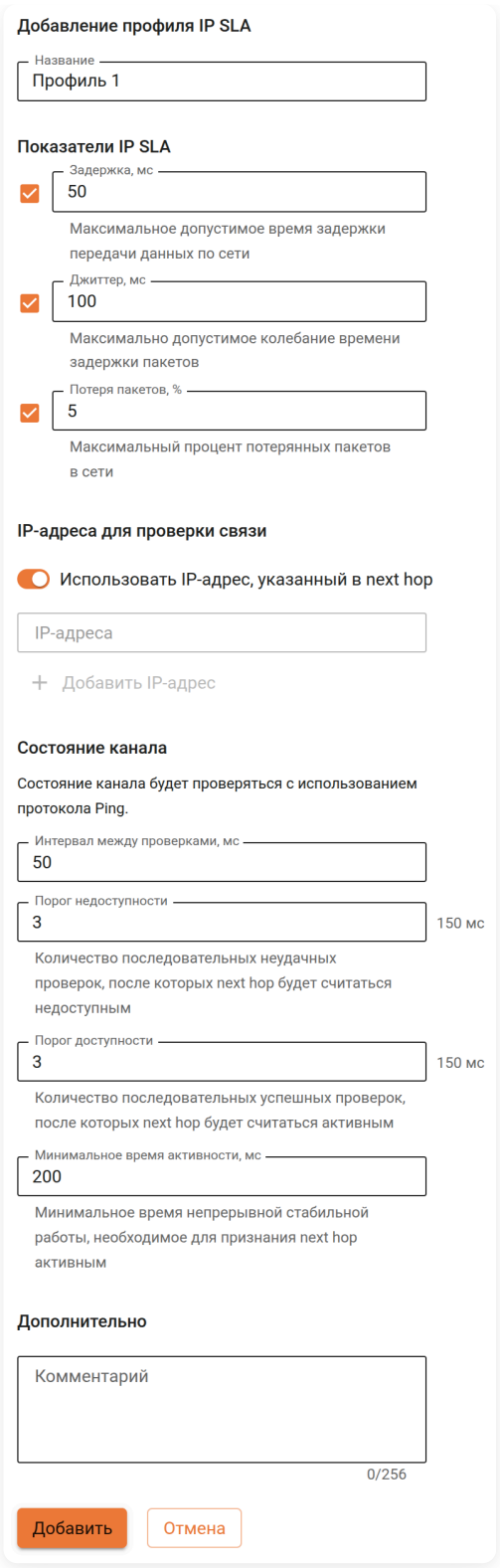
Поддержка BFD должна быть настроена и на стороне указанного шлюза. Без этого проверка доступности работать не будет.

Профили next hop

Используйте этот способ, если в поле **Отправлять в** указан **Профиль next hop**.

1. Перейдите в **SD-WAN** → **Профили IP SLA** и нажмите **Добавить**.

2. Заполните параметры профиля. В блоке **IP-адреса для проверки связи** включите опцию **Использовать IP-адрес, указанный в next hop**:



3. Нажмите **Сохранить**.

4. Перейдите в **SD-WAN** → **Профили next hop** и нажмите напротив нужного профиля.

5. В поле **Профиль IP SLA** выберите созданный профиль.

6. Нажмите **Сохранить**.

Автоматическое перенаправление трафика при недоступности шлюза можно реализовать без опции **Использовать маршрут только при доступности шлюза (адаптивность)**. Для этого в поле **Отправлять в** выберите **Профиль next hop** с режимом **Резервирование**. В этом случае трафик будет направляться через доступный next hop с учетом приоритета.

В столбце **Управление** можно:

 Включать или выключать правило.

 Менять приоритет.

 Редактировать правило.

 Удалять правило.

Полезные ссылки

- **Объекты**
- **Статическая маршрутизация**
- **Next hop**
- **Профили next hop**

Отчеты и журналы

Настройте получение данных об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени

Трафик

Статистика из **Контроля приложений** и **Контент-фильтра**

Перейти >

Система

Таблица логов работы служб

Перейти >

Веб-трафик

Статистика из проверки трафика антивирусом и модулем **Контент-фильтр**

Перейти >

Межсетевой экран

Таблица срабатываний правил **Межсетевого экрана**

Перейти >

События безопасности

Статистика событий модулей WAF и IPS, а также графики событий IPS

Перейти >

Действия администраторов

Таблица действий администраторов в Ideco NGFW

Перейти >

Аутентификация администраторов

Таблица аутентифицированных на Ideco NGFW администраторов

Перейти >

Аутентификация пользователей

Таблица аутентифицированных на Ideco NGFW пользователей

Перейти >

Аутентификация пользователей ЛК

Таблица сессий пользователей, авторизованных в личном кабинете Ideco NGFW

Перейти >

Конструктор отчетов

Создание шаблонов отчетов и настройка рассылки на электронную почту

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Трафик

Классический контекст | Высокопроизводительный контекст

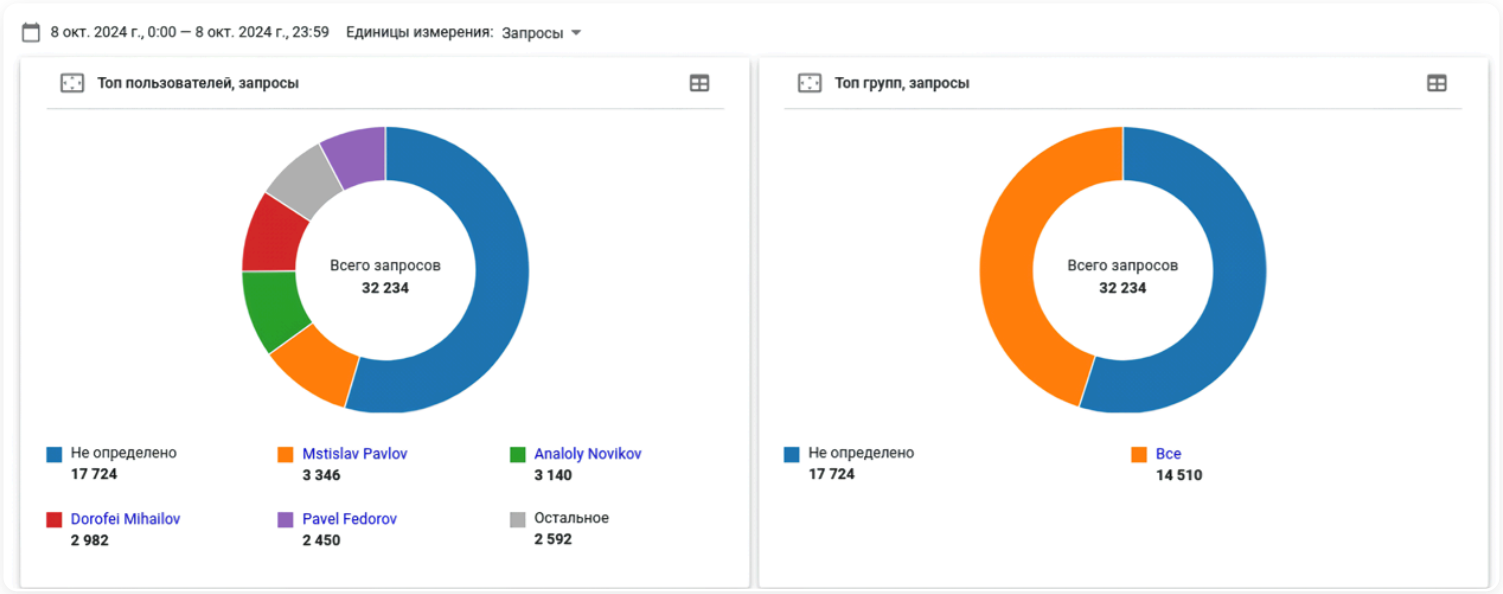
При включении опции **Трафик** в левом верхнем углу раздел начинает собирать статистику из Контент-фильтра и отображается в виде виджетов.

Способы отображения информации:

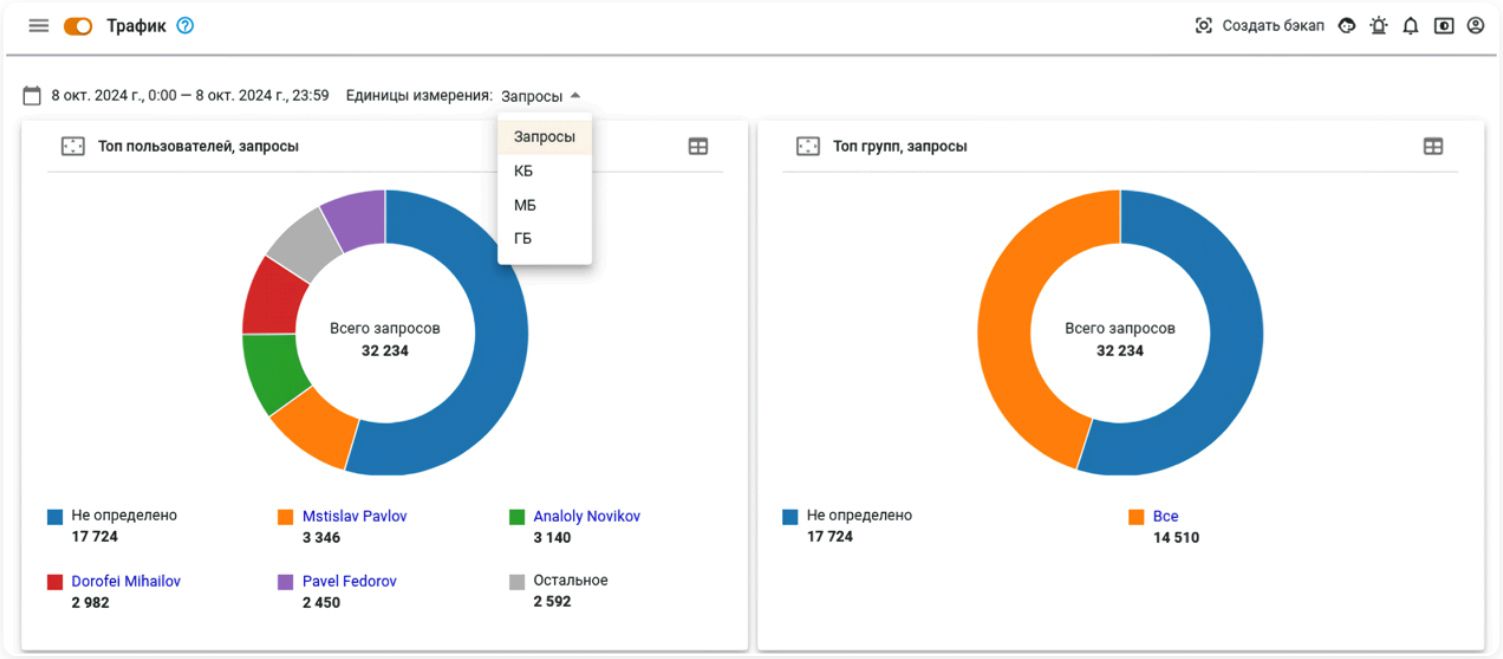
- Круговая диаграмма ( ) и таблица ( ).
- Развернутый режим ( ).

Диаграмма и таблица

Содержат топ-6 объектов. Каждый объект кликабелен и ведет на страницу с виджетами, в которых статистика фильтруется по этому объекту:



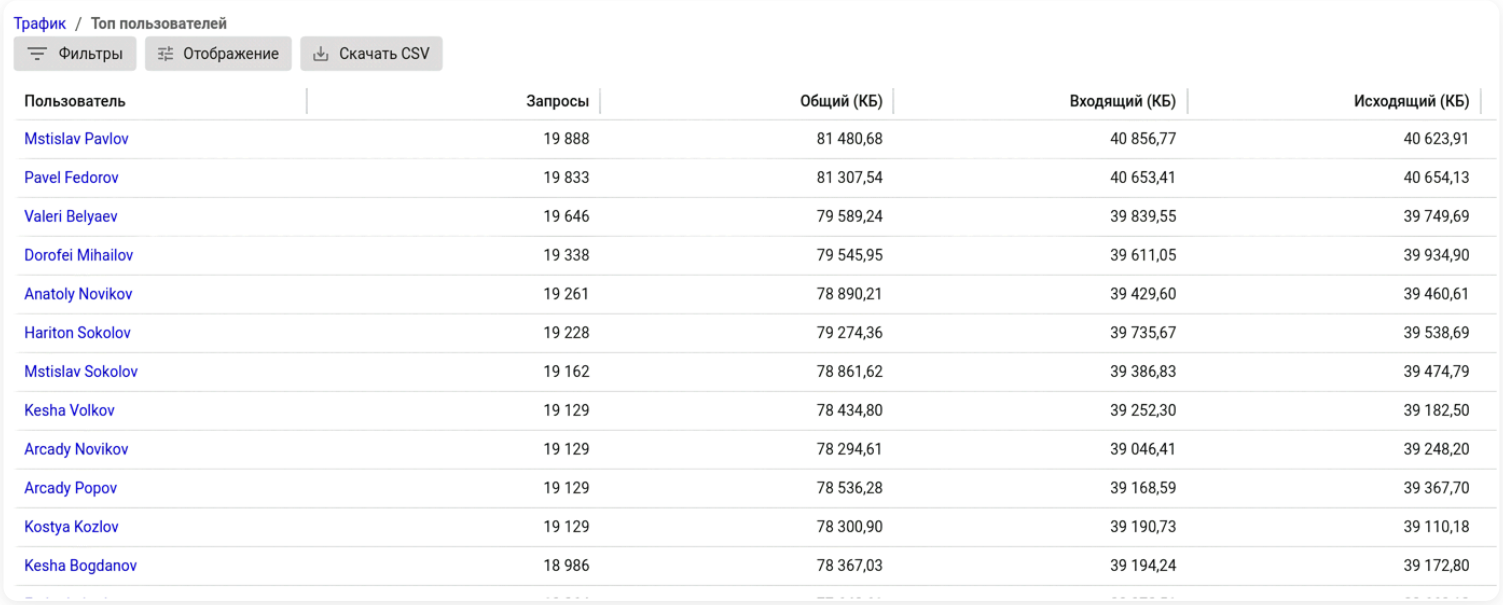
Единицу измерения можно изменить по кнопке над виджетами:



Не определено (трафик с неизвестным адресом и пользователем) - это любой трафик от самого Ideco NGFW Novum. Например, скачивание баз Контент-фильтра, GeoIP, сигнатур и т.д.

Развернутый режим

Содержит данные по всем объектам из топа. Для поиска по объектам воспользуйтесь кнопкой **Фильтры**.



Пользователь	Запросы	Общий (КБ)	Входящий (КБ)	Исходящий (КБ)
Mstislav Pavlov	19 888	81 480,68	40 856,77	40 623,91
Pavel Fedorov	19 833	81 307,54	40 653,41	40 654,13
Valeri Belyaev	19 646	79 589,24	39 839,55	39 749,69
Dorofei Mihailov	19 338	79 545,95	39 611,05	39 934,90
Anatoly Novikov	19 261	78 890,21	39 429,60	39 460,61
Hariton Sokolov	19 228	79 274,36	39 735,67	39 538,69
Mstislav Sokolov	19 162	78 861,62	39 386,83	39 474,79
Kesha Volkov	19 129	78 434,80	39 252,30	39 182,50
Arcady Novikov	19 129	78 294,61	39 046,41	39 248,20
Arcady Popov	19 129	78 536,28	39 168,59	39 367,70
Kostya Kozlov	19 129	78 300,90	39 190,73	39 110,18
Kesha Bogdanov	18 986	78 367,03	39 194,24	39 172,80

Если в левом верхнем углу установлен флаг в строке **Запросы**, то объекты отфильтруются по убыванию по колонке **Запросы**. Если **Трафик** - по убыванию в колонке **Входящий**.

Время и дата в виджете отображается в часовом поясе сервера.

Примеры использования:

На какие запрещенные сайты переходил определенный пользователь

- Откройте раздел **Отчеты и журналы** → **Трафик**.
- В виджете **Топ пользователей** найдите нужного пользователя и нажмите по нему. Если пользователя нет в списке, то нажмите **Развернуть** ( ) в левом верхнем углу виджета (откроется список всех пользователей).
- В виджете **Топ заблокированных сайтов** Ideco NGFW Novum покажет топ-5 блокировок. Для просмотра полного списка блокировок нажмите **Развернуть** ( ).

Каким пользователям заблокировали определенное приложение

- Откройте раздел **Отчеты и журналы** → **Трафик**.
- В виджете **Топ заблокированных протоколов** найдите требуемый протокол и нажмите по нему. Если протокола нет в списке, то нажмите **Развернуть** ( ).
- Чтобы увидеть список всех пользователей, у которых был заблокирован протокол, на открывшейся странице найдите виджет **Топ пользователей** и нажмите **Развернуть** ( ).

Подробнее о создании собственных шаблонов со статистикой - в статье Конструктор отчетов.

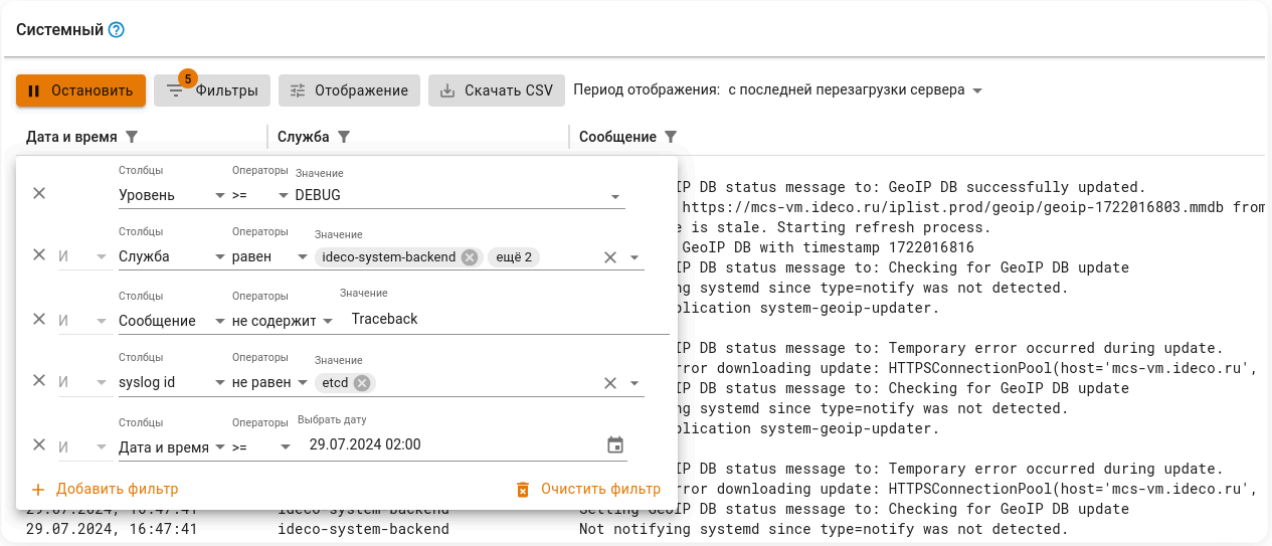
Система

Классический контекст | Высокопроизводительный контекст

Время хранения логов в разделе **Система** - 90 дней.

Для просмотра логов определенной службы воспользуйтесь строкой поиска или фильтром.

Для фильтрации логов по нескольким параметрам нажмите **Добавить фильтр** и выберите соответствующий критерий, значение и оператор в форме. Фильтрация по нескольким критериям:



По кнопке **Скачать CSV** сохраняются те строки логов, которые заданы фильтрацией.

Полный список служб смотрите в статье.

Удаление заблокированных соединений

Служба `ideco-conndrop` принудительно завершает сетевые соединения, запрещенные правилами **Межсетевого экрана**.

Алгоритм работы службы:

1. Присваивает соединению метку `ideco-irreversible-drop` при срабатывании запрещающего правила **Межсетевого экрана**.
2. Каждую минуту выполняет фильтрацию записей с меткой `ideco-irreversible-drop` и удаляет их.

Защита от брутфорс-атак (fail2ban)

Для просмотра логов службы `fail2ban` задайте фильтр `fail2ban` в строке поиска.

Как посмотреть заблокированные адреса и управлять белым списком, описано в статье **Защита от брутфорс-атак (fail2ban)**

Полезные ссылки

- **Ручная корректировка GeoIP**

Список служб

Классический контекст | Высокопроизводительный контекст

Логи представленных служб доступны в разделе Сервис:

Модуль	Имя службы
ALD Pro	ideco-ald-rest, ideco-ald-backend
Active Directory	ideco-ad-log-collector, ideco-ad-backend
BGP, OSPF	ideco-routing-rest, ideco-routing-backend, frr
Control Plane	nginx-control-plane
DNS	unbound-keygen, unbound-anchor, unbound, nsd, ideco-dns-backend, ideco-dns-dnstap-reader
DDNS	ideco-dns-backend
DHCP	ideco-dnsmasq, ideco-dhcp-server-backend
Data Plane	nginx-data-plane
IGMP Proxy	ideco-igmpproxy-rest, ideco-igmpproxy-backend, ideco-igmpproxy
IPsec	ideco-ipsec-backend
Ideco Center	ideco-central-console-backend
Ideco Client	ideco-websocket-vpn-server, ideco-agent-websocket, ideco-agent-backend
NTP	chronyd
Syslog	ideco-monitor-backend, ideco-logs-backend
VCE	ideco-vce-rest, ideco-vce-backend, ideco-vce-vpp
VPN-подключения	pcscd, ideco-vpn-sessions-sync, ideco-vpn-servers-backend, ideco-vpn-netns, ideco-vpn-dhcp-backend, ideco-vpn-authd, ideco-gost-vpn-rest, ideco-gost-vpn-backend, ideco-accel-sstp, ideco-accel-l2tp, strongswan, ideco-vpn-authd-dhcp-auth-server
Web Application Firewall	ideco-waf-event-syncer, ideco-waf-backend
Авторизация	ideco-auth-backend
Антивирус	klmsinit, kav-scanner, ideco-av-backend
Антиспам и антивирус	klms_postgres
Профили next hop, Маршрутизация	ideco-routing-backend
Бэкапы	ideco-backup-rotate, ideco-backup-restore, ideco-backup-create, ideco-backup-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-backend, ideco-web-authd
Дополнительно	ideco-system-swap, ideco-system-backend
Кластеризация	ideco-cluster-backup-pusher, ideco-cluster-backend
Контент-фильтр	ideco-content-filter-backend, ideco-content-filter-sky-db-updater, ideco-content-filter-backend-rules-file-syncer, ideco-rocks-cf-tool
Лицензия	ideco-license-backend
Межсетевой экран	ideco-fw-stats, ideco-firewall-rest, ideco-firewall-backend, ideco-apply-manual-blocklist, ideco-acl-rest, ideco-acl-backend, ideco-nflog
Обновления	ideco-sysupdate-backend
Обнаружение устройств	ideco-netscan-backend
Объекты	ideco-alias-backend
Обратный прокси	ideco-reverse-backend
Ограничение скорости	ideco-shaper-backend
Отчеты и журналы	ideco-reports-backend, ideco-logs-syncer, ideco-logs-backend, ideco-audit-backend

Модуль	Имя службы
Предотвращение вторжений	ideco-suricata-profiles-syncer, ideco-suricata-profiles-syncer-backend, ideco-suricata-event-syncer, ideco-suricata-backend, ideco-suricata
Прокси	squid, ideco-proxy-backend
Профили контроля приложений	ideco-app-stats, ideco-app-control-nfq, ideco-app-backend
Сертификаты	ideco-cert-backend
Сетевые интерфейсы	ideco-local-menu, ideco-l2manager-rest, ideco-l2manager-l2migration, ideco-l2manager-dhclient, ideco-l2manager-backend, ideco-l2-manager

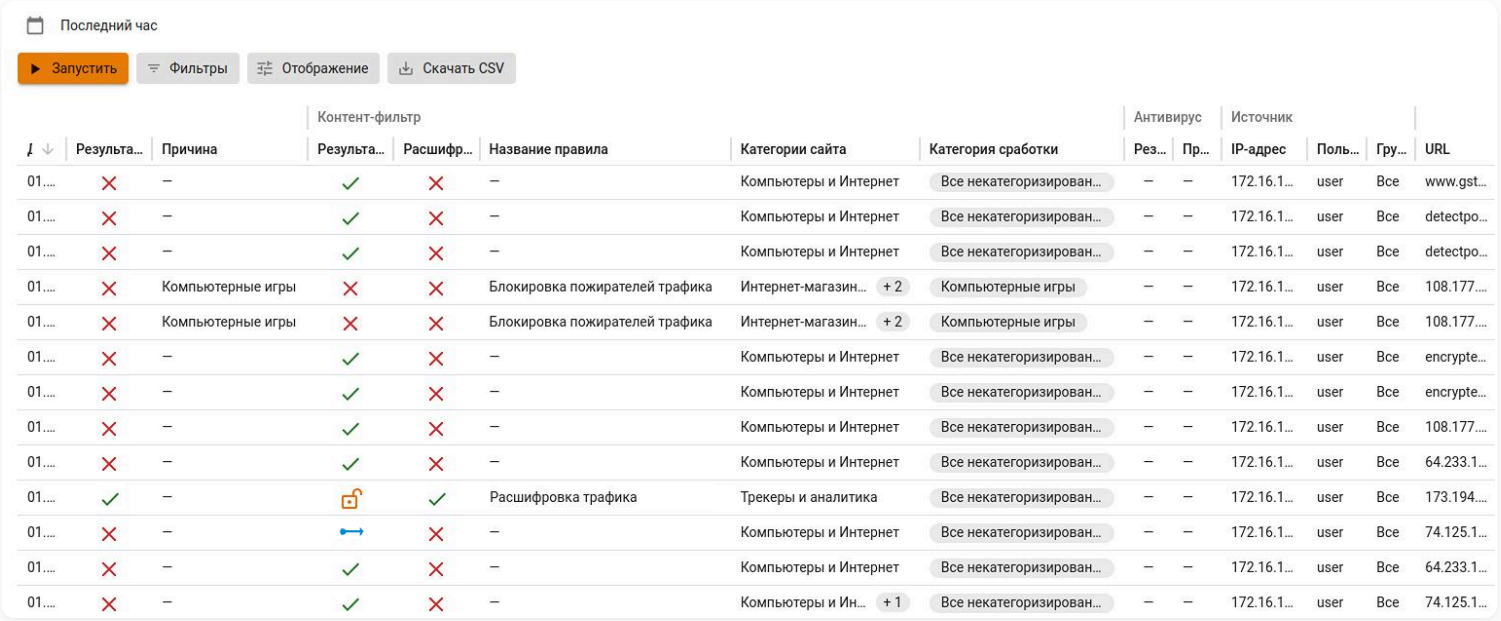
Служебные:

Модуль	Имя службы
API	ideco-rest-api-backend
MY.IDECO	ideco-mir-alerts
Авторизация и межсетевой экран	ideco-auth-backend-vpn-ipset-syncer
Базовая система и менеджер сессий (systemd)	user, var-log-journal, systemd-udevd, systemd-tmpfiles-setup, systemd-sysctl, systemd-oomd, systemd-nsresourced, systemd-modules-load, systemd-machined, systemd-logind, systemd-journald, systemd-hostnamed, systemd-homed, systemd-coredump, systemd-boot-random-seed, init, login, su
Демон для работы RDP в SSL VPN	guacd
Инженерная панель	ideco-engineering-panel-backend
Контроль целостности системы	ideco-check-sums
Локальная база данных	ideco-etcd-runtime-defrag, ideco-etcd-runtime, ideco-etcd-permanent-defrag, ideco-etcd-permanent
Настройка системы в облачных развертываниях	ideco-vk-cloud-license, ideco-cloud-init-backend
Ограничение скорости	ideco-netmap-loader, ideco-netmap-backend
Отчеты и журналы	ideco-clickhouse-enrichment
Проверка прав пользователей на перезапуск служб systemd	ideco-policy-backend
Ранняя инициализация системы	dracut-initqueue, dracut-cmdline
Сбор метрик и статистики	prometheus-node-exporter, prometheus, ideco-gatherstat-backend
Сервер базы данных	clickhouse-server
Системная шина	dbus-broker
Создание дампов ядра в случае падения	kdump
Управление томами	lvm2-monitor, lvm-activate-utm_421259

Веб-трафик

Классический контекст | Высокопроизводительный контекст

В разделе представлен результат проверки трафика антивирусом и модулем **Контент-фильтр**. Для просмотра отчета перейдите в **Отчеты и Журналы → Веб-трафик**:



Для настройки столбцов журнала нажмите **Отображение**.

Столбец	Описание
Общие	
Дата и время	Дата и время записи в формате `ДД.ММ.ГГГГ, ЧЧ:ММ:СС`
Результат проверки	Разрешено/расшифровано/запрещено/перенаправлено
Причина	Причины блокировки: название категории, имя словаря, HTTP-метод или MIME-тип, по которым был запрещен доступ к сайту
URL	Адрес запроса
Домен	Домен запроса
Путь	URL без домена
Перенаправлено на	Адрес, на который перенаправлен запрос
Referer	Заголовок Referer HTTP-запроса
Общий, МБ	Общий трафик
Входящий, МБ	Входящий трафик для запроса
Исходящий, МБ	Исходящий трафик для запроса
Тип/версия протокола	HTTP/HTTPS и версия протокола
Код ответа	Код ответа на запрос
Метод	Метод запроса
Тип контента	Заголовок Content-Type HTTP-запроса
Агент пользователя	Браузер или другой агент пользователя и его версия с указанием ОС
Контент-фильтр	

Результат	Результат работы Контент-фильтра:  - **Разрешено**  - **Расшифровано**  - **Запрещено** - **Перенаправлено на**
Расшифровка	 - **Трафик расшифрован**  - **Трафик не расшифрован**
Правило из Ideco Center	При наличии Ideco Center - постправило/предправило/локальное правило или прочерк
ID правила	Идентификатор правила контент-фильтра
Название правила	Название правила, под которое попадает запрос
Категории сайта	Категории из классификации сайтов, к которым относится запрос
Категория сработки	Категория из классификации сайтов контент-фильтром, по которой сайт был заблокирован
Антивирус	
Результат	Результат работы Антивируса: разрешено/расшифровано/запрещено/перенаправлено
ID	Идентификатор профиля антивируса
Профиль	Название профиля антивируса
Серьезность угрозы	Указанная антивирусом серьезность угрозы: информационный, низкий, средний, высокий
Тип обнаруженной угрозы	Указанный антивирусом тип угрозы: Рекламное (Adware), Вредоносные инструменты, Порнографическое (Pornware), Потенциально опасное (Riskware), Трояны, Неопознанное вредоносное ПО высокой опасности, Неопознанное вредоносное ПО средней опасности, Вирусы
Название объекта	Путь к файлу. Для простых файлов имеет неинформативное техническое значение, типа `Memory region 123`. Для архивов и других контейнеров содержит также путь к проверенному объекту внутри контейнера, типа `Memory region 123//virus.exe`
Тип объекта	Файл/URL (для вредоносных ссылок)
Формат объекта	Формат файла для функции блокировки по формату
Источник	
IP-адрес	Адрес источника
Порт	Порт источника запроса
Пользователь	Пользователь, от имени которого идет запрос
Группа	Группа, к которой относится пользователь
Назначение	
IP-адрес	Адрес назначения
Порт	Порт назначения
Кластер	
ID	Идентификатор кластера
Название	Название кластера
VCE	
ID	Идентификатор контекста
Название	Название контекста

Если с устройства пользователя недоступен какой-либо интернет-ресурс, в **Отчеты и журналы** → **Веб-трафик** можно найти правило, блокирующее ресурс.

Для просмотра блокировок по конкретному правилу воспользуйтесь кнопкой **Фильтры**, указав в форме наименование правила и оператор.

Межсетевой экран

Классический контекст | Высокопроизводительный контекст | API

В журнале отображается информация о срабатывании правил **Межсетевого экрана** (таблицы FORWARD и INPUT), а также о профилях **Предотвращения вторжений** и **Контроля приложений**.

Раздел позволяет быстро выявить модуль фильтрации, который блокирует трафик, и выявить DDoS-атаки.

В таблицу попадают соединения, которые подошли под правила в таблице Логирования. Фильтрация наиболее быстро работает с полями **Пользователь источника**.

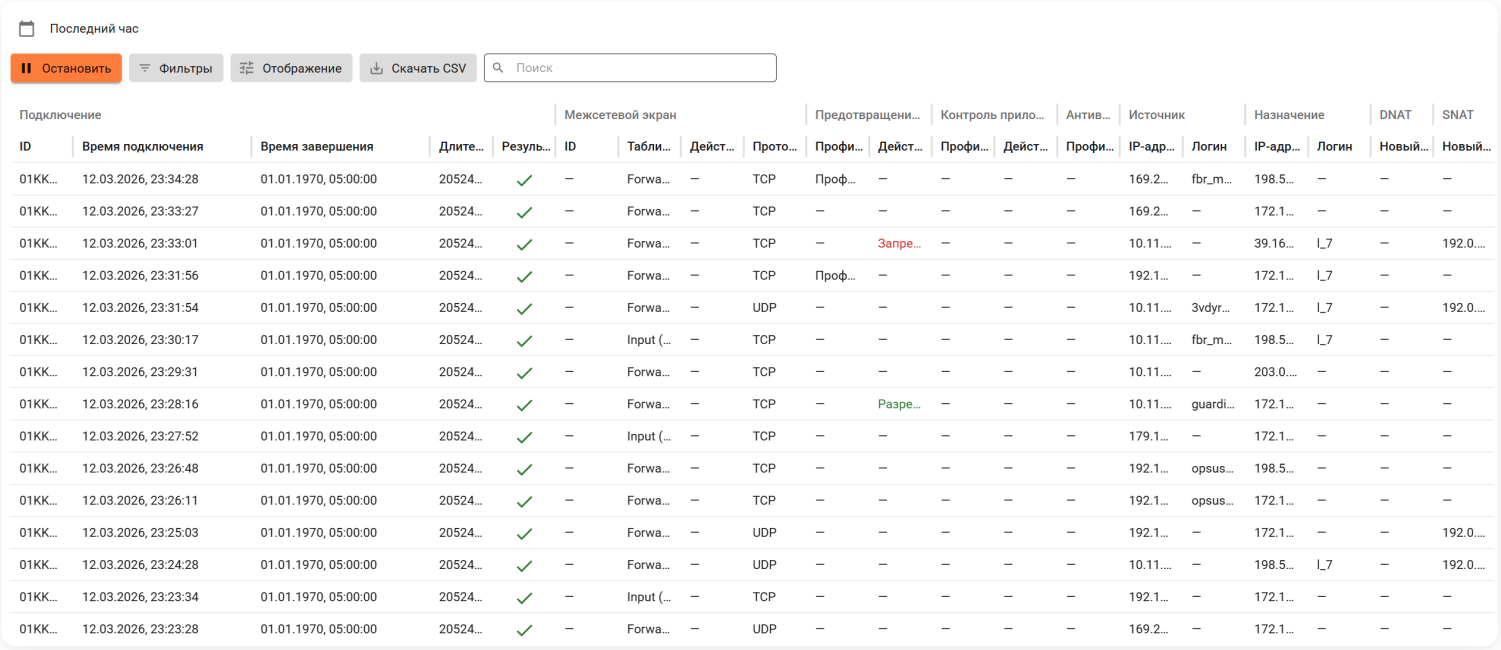
Соединения, которые были установлены до включения правил в таблице Логирование или не попали ранее под эти правила, не будут отображены в журнале.

Будьте внимательны: объем данных в журнале **Межсетевой экран** может кратно превысить объем данных любого другого журнала. Журнал хранит данные за три месяца, но при превышении размера журнала 15 ГБ старые записи будут удалены.

Чтобы отрегулировать столбцы, отображаемые в таблице, воспользуйтесь кнопкой **Отображение**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**.

При фильтрации по **Таблице правил (Межсетевой экран)** можно вывести срабатывания системных правил (Forward System и Input System). Это правила **Межсетевого экрана**, которыми нельзя управлять из веб-интерфейса Ideco NGFW Novum, они всегда включены. Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Межсетевого экрана**. По вопросам срабатывания системных правил обращайтесь в Техническую поддержку.



Столбец	Описание
Подключение	
ID	Идентификатор сессии
Время подключения	Дата начала сессии
Время завершения	Дата завершения сессии
Длительность	Длительность сессии

Результат	Результат проверки трафика тремя модулями фильтрации: Межсетевой экран, Предотвращение вторжений, Контроль приложений. Результат проверки:  - **Разрешено**  - **Расшифровано**  - **Запрещено** - **Перенаправлено на**
Межсетевой экран	
ID	Идентификатор правила Межсетевого экрана
Таблица правил	Правила, которые сработали: • FORWARD - таблица FORWARD раздела Межсетевой экран Ideco NGFW Novum • DNAT - таблица DNAT раздела Межсетевой экран Ideco NGFW Novum • INPUT - таблица INPUT раздела Межсетевой экран Ideco NGFW Novum • SNAT - таблица SNAT раздела Межсетевой экран Ideco NGFW Novum • FORWARD BEFORE - предправило FORWARD Ideco Center • FORWARD AFTER - постправило FORWARD Ideco Center • INPUT BEFORE - предправило INPUT Ideco Center • INPUT AFTER - постправило INPUT Ideco Center • FORWARD SYSTEM - системное правило FORWARD • INPUT SYSTEM - системное правило INPUT Информацию по системному правилу можно просмотреть через Терминал, введя команду `iptables-save / grep 'sys.<ID правила>'`. Смотрите примеры в статье
Действие	Действие, определенное для трафика, подпадающего под сработавшее правило. Возможные действия: Разрешить, Запретить, Перенаправить в профиль
Протокол	Протокол соединения
Предотвращение вторжений	
ID	Идентификатор профиля Предотвращения вторжений
Профиль	Название профиля Предотвращения вторжений, использованного в правиле Межсетевого экрана
ID сигнатуры	Идентификатор сигнатуры, которой соответствует трафик
Действие	Действие для трафика, определенное профилем
Контроль приложений	
ID	Идентификатор профиля Контроля приложений
Профиль	Название профиля Контроля приложений, использованного в правиле Межсетевого экрана
Действие	Действие для трафика, определенное профилем
Приложение	Приложение, действие для которого определено профилем
Протокол прикладного уровня	Протокол, к которому применяется действие, определенное профилем
Антивирус	
ID	Идентификатор профиля Антивируса
Профиль	Название профиля Антивируса
Источник	
IP-адрес	IP-адрес источника трафика
Порт	Порт источника трафика
Зона	Интерфейс или группа интерфейсов, из которых пришел трафик
Логин	Логин пользователя источника
Пользователь	Имя пользователя источника
Группа	Группа, в которую входит пользователь
Местоположение	Страна источника трафика (GeoIP)
Внешний IP-адрес	Внешний IP-адрес источника трафика
Назначение	

IP-адрес	IP-адрес назначения трафика
Порт	Порт назначения трафика
Зона	Интерфейс или группа интерфейсов, в которые вошел трафик
Логин	Логин пользователя назначения
Пользователь	Имя пользователя назначения
Группа	Группа, в которую входит пользователь
Местоположение	Страна назначения трафика (GeoIP)
DNAT	
ID	Идентификатор сработавшего правила таблицы DNAT
Новый IP назначения	IP-адрес, на который межсетевой экран поменял IP-адрес назначения
Новый порт назначения	Порт, на который межсетевой экран поменял Порт назначения
SNAT	
ID	Идентификатор сработавшего правила таблицы SNAT
Новый IP источника	IP-адрес, на который межсетевой экран поменял IP-адрес источника
Кластер	
ID	Идентификатор кластера, если кластер настроен на NGFW Novum
Название	Название кластера, если кластер настроен на NGFW Novum
VCE	
ID	Идентификатор VCE
Название	Название VCE

События безопасности

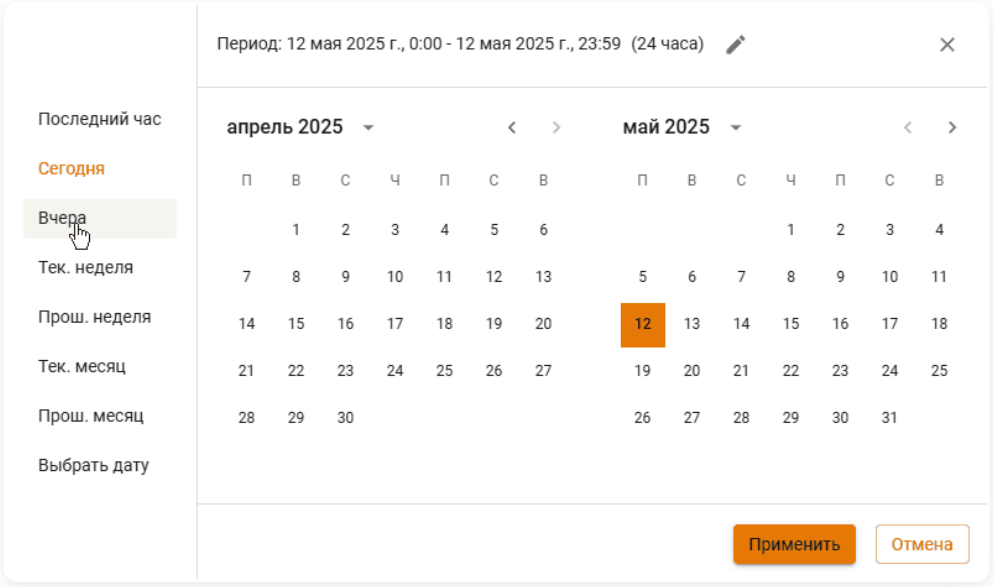
Классический контекст | Высокопроизводительный контекст | API

Все графики формируются в часовом поясе сервера.

В разделе **События безопасности** представлены события модулей WAF и IPS, а также графики событий IPS.

Выбор периода

Все отображаемые данные фильтруются по дате и времени. Например, выберите определенный временной период (по кнопке) или воспользуйтесь одним из предустановленных фильтров:



Если не выбран ни один фильтр по дате и времени, то по умолчанию устанавливается интервал **Сегодня** (Графики IPS) или **Последний час** (Журнал IPS, Web Application Firewall) в часовом поясе сервера.

Графики IPS

В этом разделе представлены графики, содержащие краткую информацию раздела **Предотвращение вторжений**. Подробные сведения обо всех срабатываниях правил **Предотвращение вторжений** можно найти на вкладке **Журнал IPS** в виде таблицы.

График Количество атак по уровню угрозы

Информация представлена в виде графика со значениями угрозы безопасности:

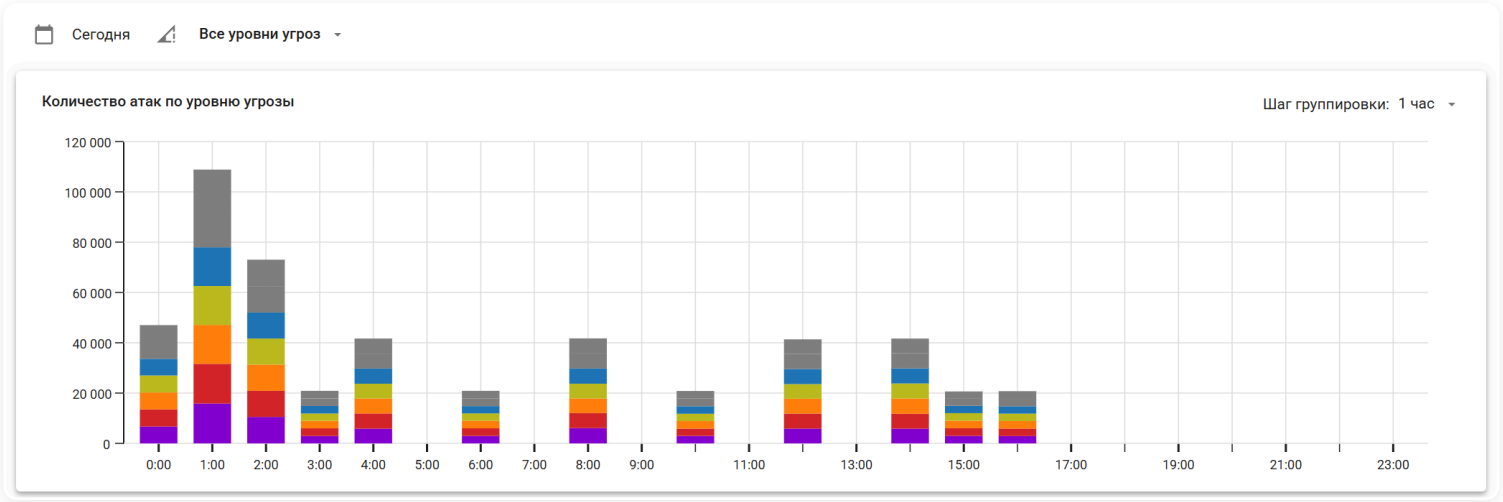
- **Не обнаружен** - уровень угрозы 0. Не удалось обнаружить уровень угрозы для сигнатуры
- **Критичный** - уровень угрозы 1
- **Опасный** - уровень угрозы 2
- **Незначительный** - уровень угрозы 3
- **Информационный** - уровень угрозы 4
- **Неопределенный** - уровень угрозы 255. Сигнатуры, явно не отнесенные ни к одной из категорий

Уровни угроз определяются в соответствии с характеристиками сигнатур в порядке убывания приоритета:

- Severity metadata - метаданные серьезности угрозы, явно заданные в сигнатуре. Если это поле присутствует, оно имеет наивысший приоритет при определении уровня угрозы.
- Priority - приоритет сигнатуры, указанный в ее описании. Используется, если поле Severity metadata отсутствует.
- Classtype - тип класса атаки (например, `trojan-activity` или `attempted-admin`). Используется для определения уровня угрозы, если ни Severity metadata, ни Priority не заданы.

Если нажать на уровень угрозы в правом списке, все графики будут отфильтрованы в соответствии с этим уровнем. Чтобы отменить фильтрацию, нажмите еще раз на выбранный уровень.

Пример графика **Количество атак по уровню угрозы**:



Описание дополнительных графиков

Топ атакованных адресов

В топ атакованных попадают как внешние, так и внутренние адреса. Один из примеров, когда атакованный адрес является внешним, - работа трояна изнутри защищаемой сети.

Топ заблокированных типов атак

График подсчитывает статистику типов атак (например, типы атак **Черный список IP-адресов** или **Попытки получения привилегий администратора**) по количеству срабатываний с этим типом атаки.

Топ внешних узлов по количеству блокировок

График содержит информацию о внешних адресах и количестве блокировок по ним.

Топ атакующих стран

Топ атакующих стран строится по IP-адресам, полученным при срабатывании правил в разделе **Предотвращение вторжений**. Если IP-адрес не геокодируется в наименование страны, адрес не будет отображается в виджете.

По этой причине локальные IP-адреса не отображаются в виджете.

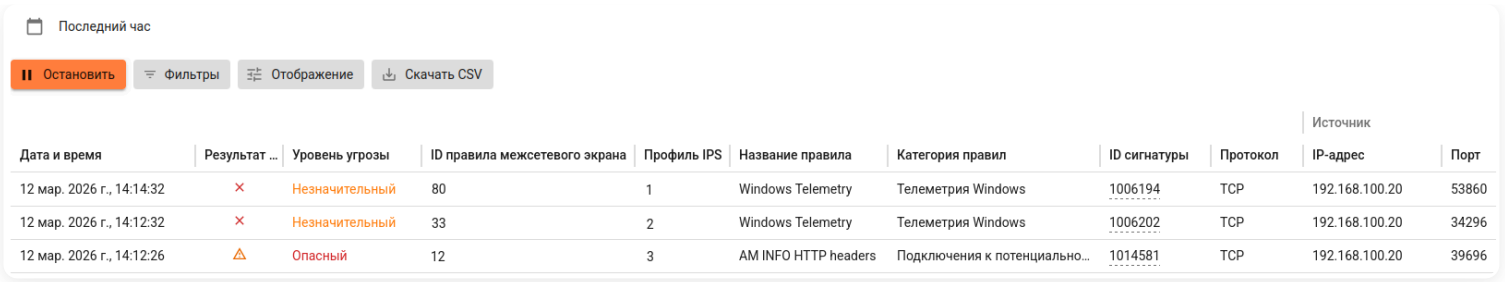
Топ подозрительных локальных узлов

Виджет отображает локальные IP-адреса, являющиеся источниками срабатываний правил системы **Предотвращение вторжений**. В топ попадают как авторизованные, так и неавторизованные пользователи, запросы которых блокировались. Если для IP-адреса не найдено соответствие с учетной записью пользователя, то имя пользователя отображаться не будет.

> Топ строится только по данным источника (src), данные назначения (dest) не учитываются. Источник локальный, если присутствует условие `src_ip_type == 'local'`.

Журнал IPS

В **Отчеты и журналы** → **События безопасности** → **Журнал IPS** можно просмотреть логи системы **Предотвращения вторжений**:



- Поле **Результат анализа** отображает действие системы:
  - `Blocked` - пакет блокирован.
  - Любая другая информация в этом поле - `Allowed`, информирование.
- В поле **Уровень угрозы** могут отображаться следующие значения:
  - **Критичный**
  - **Опасный**
  - **Незначительный**
  - **Информационный**
  - **Неопределенный**
  - **Не обнаружен**

Для проверки IP-адресов в столбцах **Источник** и **Назначение** скопируйте адрес и выполните его поиск в сервисе Whois.

Для корректного отображения информации из CSV-файла

1. Скачайте CSV-файл с логами системы **Предотвращения вторжений** за определенный период по соответствующей кнопке.

2. Откройте CSV-файл в MS Excel и выделите весь первый столбец.

3. Перейдите на вкладку **Данные** и нажмите кнопку **Текст по столбцам**.

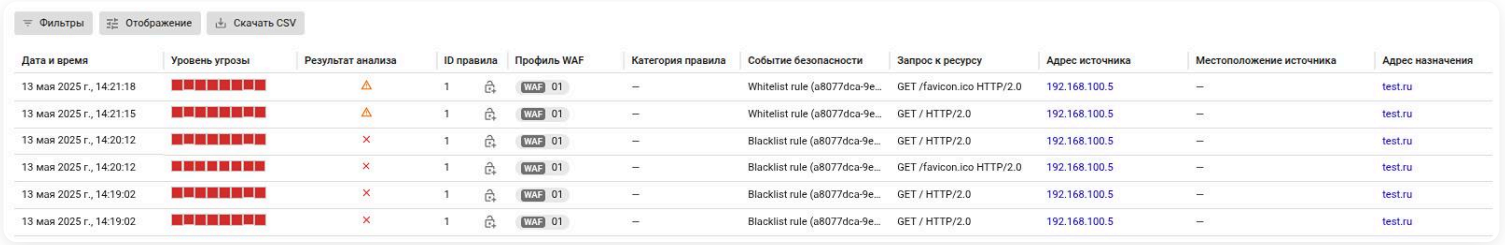
4. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:

5. В блоке **Символом-разделителем является:** выберите **запятая** и нажмите **Далее**:

6. В блоке **Формат данных столбца** выберите **Текстовый** и нажмите **Готово**:

Web Application Firewall

Вкладка **Отчеты и журналы** → **События безопасности** → **Web Application Firewall** содержит информацию о срабатывании правил Web Application Firewall в виде таблицы:



Для проверки IP-адресов в столбцах **Адрес источника** и **Адрес назначения** скопируйте адрес и выполните его поиск в сервисе Whois.

На вкладке **Web Application Firewall** отображается профиль WAF, параметры которого вызвали блокировку доступа к ресурсу.

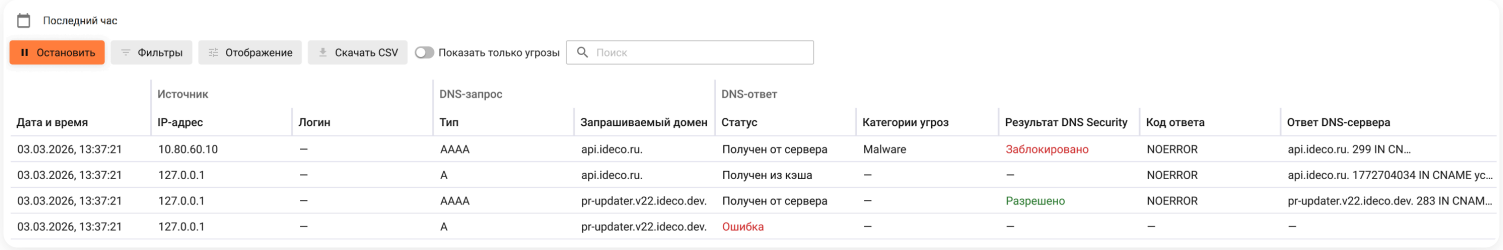
DNS-запросы

Классический контекст | Высокопроизводительный контекст | API

Время хранения данных в журнале **DNS-запросы** - 3 месяца.

В разделе отображается информация об обмене DNS-сообщениями, обработанными Ideco NGFW Novum при включенной опции **Логировать DNS-запросы** в **Сервисы → DNS → Внешние DNS-серверы**.

Журнал предназначен для анализа DNS-активности, выявления обращений к опасным и нежелательным доменам, а также просмотра DNS-запросов и результатов их обработки с привязкой к источнику:



Чтобы отрегулировать столбцы, отображаемые в таблице, воспользуйтесь кнопкой **Отображение**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**.

При включении опции **Показать только угрозы** в таблице остаются только те записи, у которых в столбце **Результат DNS Security** указано **Заблокировано**. Опция позволяет отфильтровать DNS-запросы, заблокированные сервисом DNS Security.

Описание столбцов

Столбец	Описание
	Общие
Дата и время	Дата и время записи в формате `ДД.ММ.ГГГГ, ЧЧ:ММ:СС`
	Источник
IP-адрес	IP-адрес источника DNS-запроса
Логин	Логин пользователя
Пользователь	Имя пользователя
Группа	Группа, в которую входит пользователь
	DNS-запрос
Код операции	Возможные значения: • QUERY - стандартный запрос • IQUERY - обратный запрос • STATUS - запрос состояния сервера • NOTIFY - уведомление вторичных серверов • UPDATE - динамическое обновление зоны
Класс	Класс запроса, определяющий тип сети: • IN (Internet) - основной класс • CH (Chaos) - для служебных или экспериментальных запросов • HS (Hesiod) - специальный класс для систем Hesiod

Тип	Тип DNS-запроса: • A (Address Record) - сопоставляет доменное имя с IPv4-адресом (например, example.com → 93.184.216.34) • AAAA (Quad-A Record) - сопоставляет доменное имя с IPv6-адресом (например, example.com → 2606:2800:220:1:248:1893:25c8:1946) • CNAME (Canonical Name Record) - перенаправляет одно доменное имя на другое (например, www.example.com → example.com) • MX (Mail Exchange Record) - указывает серверы, обрабатывающие почту для домена (например, example.com → mail.example.com) • TXT (Text Record) - содержит произвольный текст, часто используется для проверок (SPF, DKIM, DMARC) • NS (Name Server Record) - указывает DNS-серверы, отвечающие за домен (например, example.com → ns1.example.com) • SOA (Start of Authority) - содержит служебную информацию о зоне (первичный DNS-сервер, email администратора, TTL и другое) • PTR (Pointer Record) - используется для обратного DNS-запроса (например, 93.184.216.3 → example.com) • SRV (Service Record) - указывает серверы для определенных сервисов (например, SIP, XMPP) • CAA (Certification Authority Authorization) - определяет, какие центры сертификации могут выпускать SSL-сертификаты для домена
Протокол	Протокол соединения
Запрашиваемый домен	Доменное имя, указанное в DNS-запросе
Флаги	Свойства, отражающие особенности формирования и обработки запроса: • QR - запись является запросом • AA - авторитетный ответ, подтверждает, что сервер является авторитетным для зоны • TC - усеченный ответ, превышен размер пакета DNS • RD - рекурсия запрошена клиентом • RA - рекурсия доступна на сервере • Z - зарезервировано • AD - данные проверены DNSSEC, достоверность подтверждена • CD - проверка DNSSEC отключена
DNS-ответ	
Статус	Результат обработки DNS-запроса: • Получен от сервера - ответ на запрос получен от сервера • Получен из кэша - ответ на запрос сформирован из кэша • Ошибка - ошибка обработки
Результат DNS Security	Статус блокировки запроса сервисом DNS Security: • Заблокировано - домен заблокирован • Разрешено - категория угроз не найдена • Прочерк - сервис DNS Security был отключен при обработке запроса • Неизвестно - состояние сервиса DNS Security при обработке запроса неизвестно (значение для записей до версии NGFW Novum 21.1)
Категории угроз	Названия категорий из группы **Security**. Перечень категорий приведен в статье DNS security
Код ответа	Возможные значения: • NXDOMAIN - домен не существует • SERVFAIL - ошибка при обработке запроса сервером • REFUSED - сервер отклонил запрос • NOANSWER - нет данных для ответа • NOERROR - запрос обработан успешно • FORMERR - ошибка формата DNS-запроса • NOTIMPL - операция не поддерживается сервером • YXDOMAIN - домен уже существует (ошибка при создании или обновлении зоны) • YXRRSET - запись уже существует • NXRRSET - запись не существует • NOTAUTH - сервер не является авторитетным для зоны • NOTZONE - домен не относится к указанной зоне
Ответ DNS-сервера	Данные, возвращенные DNS-сервером в ответ на запрос (IP-адрес, имя сервера или иная информация)
Кластер	

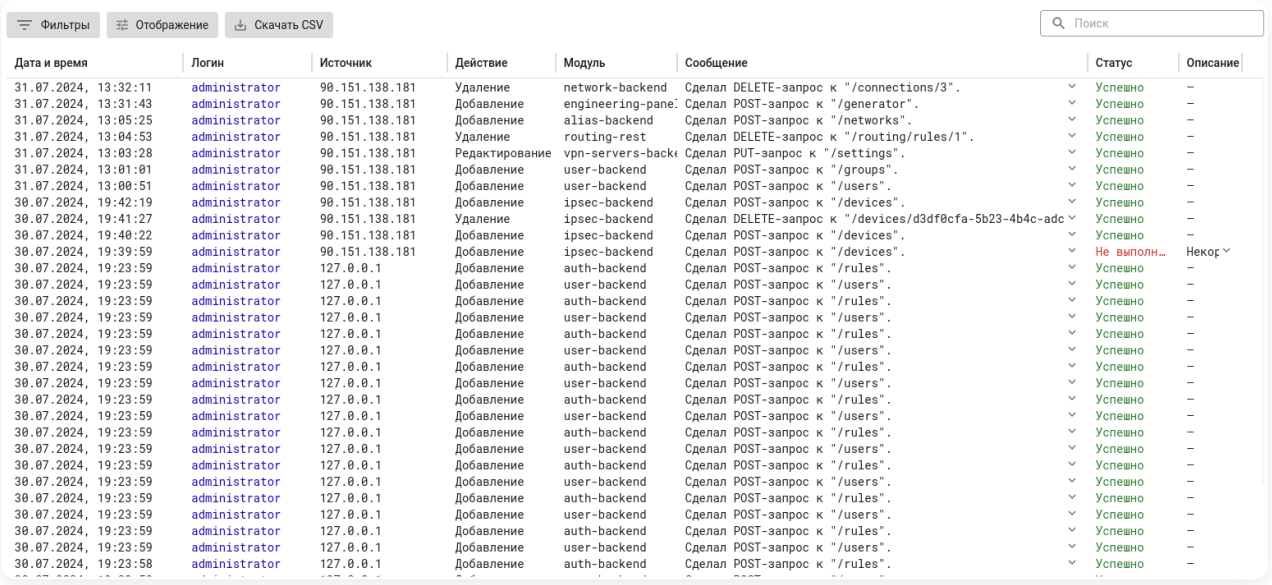
ID	Идентификатор кластера
Название	Название кластера
VCE	
ID	Идентификатор контекста
Название	Название контекста

Названия категорий в столбце **Категории угроз** отображаются при наличии лицензии сервиса **DNS-Security** и включенной опции в **Сервисы → DNS → Внешние DNS-серверы**.

Действия администраторов

Классический контекст | Высокопроизводительный контекст

Ideco NGFW Novum логирует действия администраторов, которые вносят изменения в конфигурацию NGFW Novum из веб-интерфейса, локального интерфейса и терминала. Действия, осуществляемые через локальное меню Ideco NGFW Novum, отображаются в журнале действий администраторов с источником `127.0.0.1`:



Дата и время	Логин	Источник	Действие	Модуль	Сообщение	Статус	Описание
31.07.2024, 13:32:11	administrator	90.151.138.181	Удаление	network-backend	Сделал DELETE-запрос к "/connections/3".	Успешно	–
31.07.2024, 13:31:43	administrator	90.151.138.181	Добавление	engineering-panel	Сделал POST-запрос к "/generator".	Успешно	–
31.07.2024, 13:05:25	administrator	90.151.138.181	Добавление	alias-backend	Сделал POST-запрос к "/networks".	Успешно	–
31.07.2024, 13:04:53	administrator	90.151.138.181	Удаление	routing-rest	Сделал DELETE-запрос к "/routing/rules/1".	Успешно	–
31.07.2024, 13:03:28	administrator	90.151.138.181	Редактирование	vpn-servers-backe	Сделал PUT-запрос к "/settings".	Успешно	–
31.07.2024, 13:01:01	administrator	90.151.138.181	Добавление	user-backend	Сделал POST-запрос к "/groups".	Успешно	–
31.07.2024, 13:00:51	administrator	90.151.138.181	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:42:19	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Успешно	–
30.07.2024, 19:41:27	administrator	90.151.138.181	Удаление	ipsec-backend	Сделал DELETE-запрос к "/devices/d3df0cfa-5b23-4b4c-adc	Успешно	–
30.07.2024, 19:40:22	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Успешно	–
30.07.2024, 19:39:59	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Не выполн…	Некор
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:58	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–

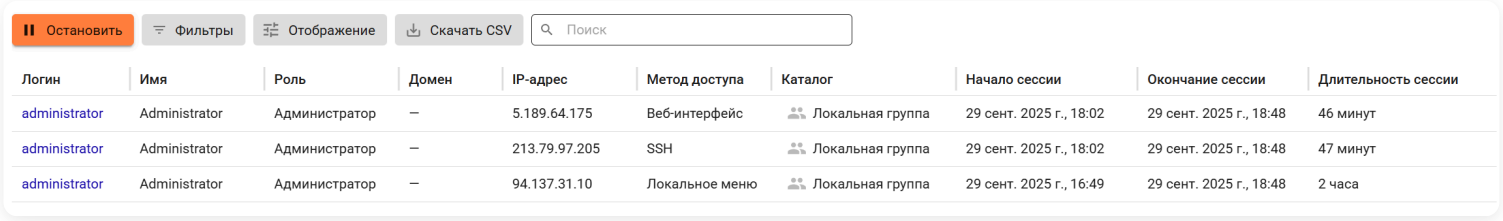
Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

При работе Ideco NGFW в режиме кластера логи действия администраторов не передаются резервной ноде.

Аутентификация администраторов

Классический контекст | Высокопроизводительный контекст

Время хранения данных в журнале **Аутентификация администраторов** составляет 1 год.



Логин	Имя	Роль	Домен	IP-адрес	Метод доступа	Каталог	Начало сессии	Окончание сессии	Длительность сессии
administrator	Administrator	Администратор	–	5.189.64.175	Веб-интерфейс	Локальная группа	29 сент. 2025 г., 18:02	29 сент. 2025 г., 18:48	46 минут
administrator	Administrator	Администратор	–	213.79.97.205	SSH	Локальная группа	29 сент. 2025 г., 18:02	29 сент. 2025 г., 18:48	47 минут
administrator	Administrator	Администратор	–	94.137.31.10	Локальное меню	Локальная группа	29 сент. 2025 г., 16:49	29 сент. 2025 г., 18:48	2 часа

Для поиска авторизованных администраторов нажмите **Фильтры** и укажите:

- В поле **Столбец** - требуемый параметр поиска.
- В последнем поле - значение.

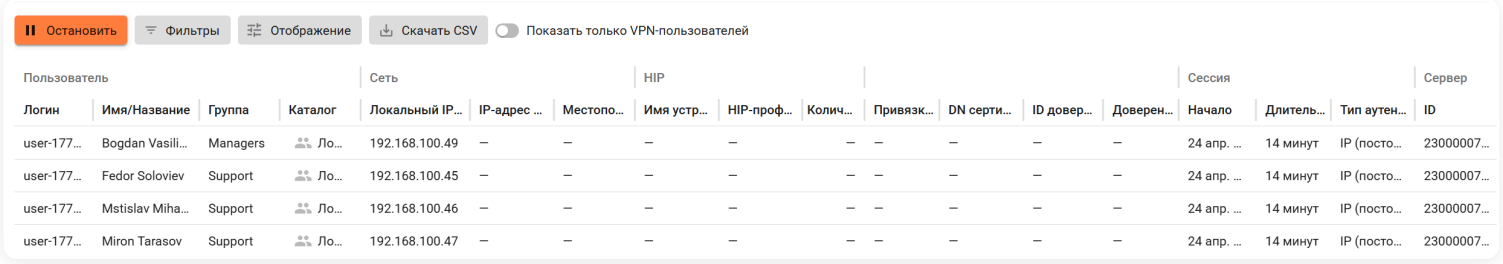
Особенности работы Журнала аутентификации администраторов

- Время жизни сессии администратора обновляется каждые 5 минут, поскольку происходит запись текущего времени в поле **Окончание сессии**. Если запрос на поиск будет отправлен до момента синхронизации буфера, то время окончания будет одно, в ином случае - другое.
- При завершении сессии администратора информация о разрыве сессии в журнале появляется сразу. Время окончания завершенной сесси больше не меняется.

Аутентификация пользователей

Классический контекст | Высокопроизводительный контекст | API

Время хранения данных в журнале **Аутентификации пользователей** составляет 180 дней.

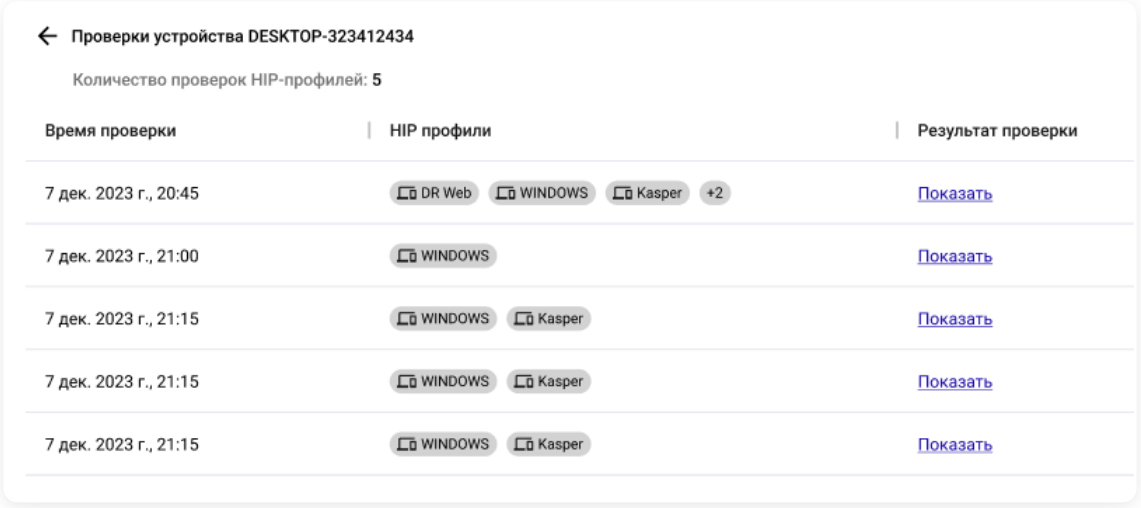


Для поиска авторизованных пользователей нажмите на **Фильтры**, укажите в поле **Столбец** требуемый параметр поиска и в последнем поле - значение.

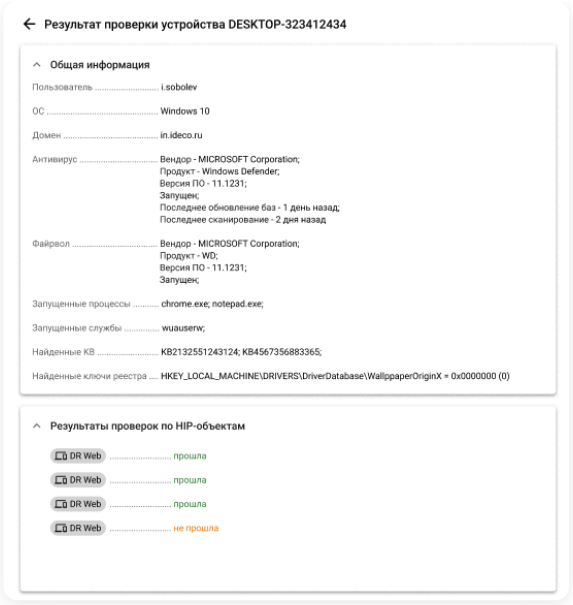
В столбце **Кол-во изменений профилей** указано количество изменений HIP-профилей, зафиксированных в результате проверок устройств, подключенных через Ideco Client. Изменения фиксируются при редактировании HIP-профиля в веб-интерфейсе или при смене профиля у устройств.

Для просмотра результатов проверок устройств, подключенных через Ideco Client, выполните действия:

1. Нажмите на число в столбце **Кол-во изменений профилей**. Откроется список проверок:



2. Нажмите **Показать** в столбце **Результат**, чтобы увидеть общую информацию и результат проверки по **HIP-объектам**:



Особенности работы Журнала аутентификации пользователей:

- Время окончания открытой сессии пользователя меняется каждые 5 минут, поскольку происходит запись текущего времени в поле **Окончание сессии**. Если запрос на поиск будет отправлен до момента синхронизации буфера, то время окончания будет одно, в ином случае - другое.
- Для завершенной сессии информация о времени закрытия не меняется.

Включение опции **Показать VPN-пользователей** отфильтрует в таблице журнала информацию обо всех VPN-сессиях по всем протоколам.

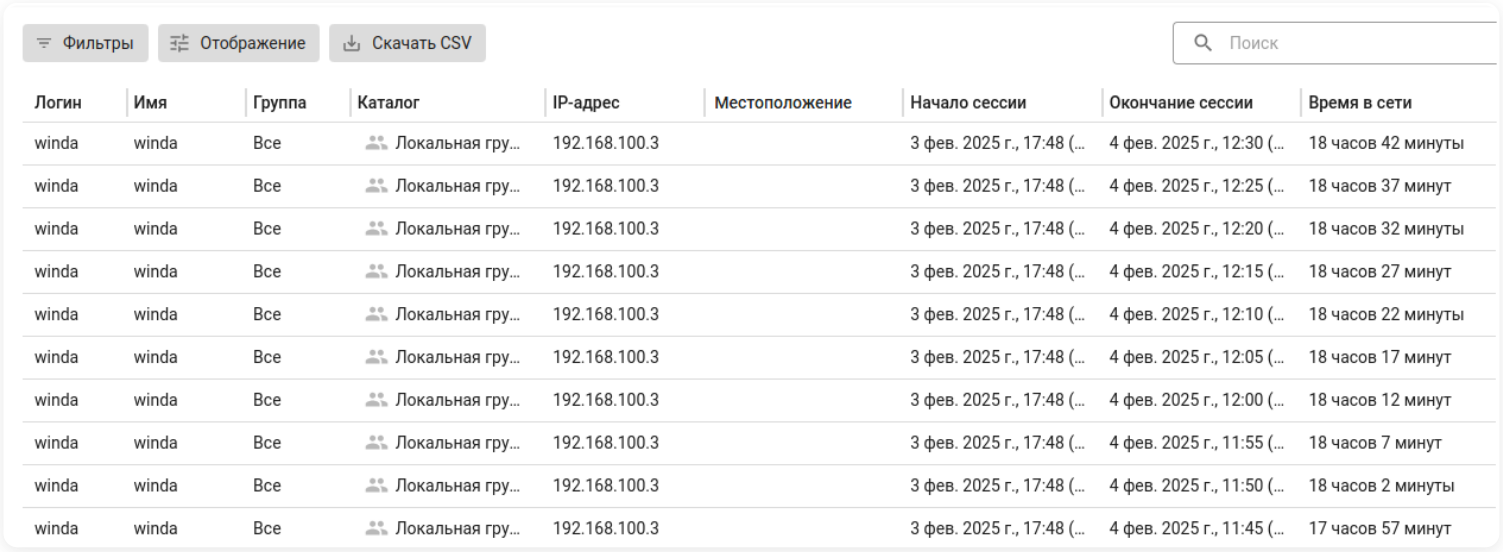
Аутентификация пользователей ЛК

Классический контекст | Высокопроизводительный контекст | API

Раздел представляет собой историю сессий пользователей, авторизованных в личном кабинете пользователя Ideco NGFW Novum.

Записи в журнале отображаются после настройки **Обратного прокси**. Технология SSL VPN используется пользователями для получения доступа к ресурсам в локальной сети через веб-браузер по HTTPS. При этом не устанавливается отдельное туннельное соединение.

Таблицу сессий можно скачать в формате CSV, воспользовавшись соответствующей кнопкой:



Логин	Имя	Группа	Каталог	IP-адрес	Местоположение	Начало сессии	Окончание сессии	Время в сети
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:30 (...	18 часов 42 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:25 (...	18 часов 37 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:20 (...	18 часов 32 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:15 (...	18 часов 27 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:10 (...	18 часов 22 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:05 (...	18 часов 17 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:00 (...	18 часов 12 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 11:55 (...	18 часов 7 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 11:50 (...	18 часов 2 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 11:45 (...	17 часов 57 минут

Помимо общих сведений об учетной записи пользователя (логин, имя, группа и каталог), список сессий включает столбцы:

- **IP-адрес** - IP-адрес, с которого произведена аутентификация.
- **Местоположение** - страна IP-адреса, с которого произведена аутентификация. Значение пустое, если:
  - Отсутствует лицензия.
  - Невозможно получить базу GeoIP.
  - IP-адрес локальный.
- **Начало сессии** - момент запуска сессии с указанием даты в формате день/месяц/год и времени в формате час/минута.
- **Окончание сессии** - момент завершения сессии с указанием даты в формате день/месяц/год и времени в формате час/минута. Пустое значение, если сессия активна.
- **Время в сети** - продолжительность сессии с момента запуска.

Наличие столбцов в таблице регулируется кнопкой **Отображение**. По каждому столбцу доступна фильтрация и сортировка.

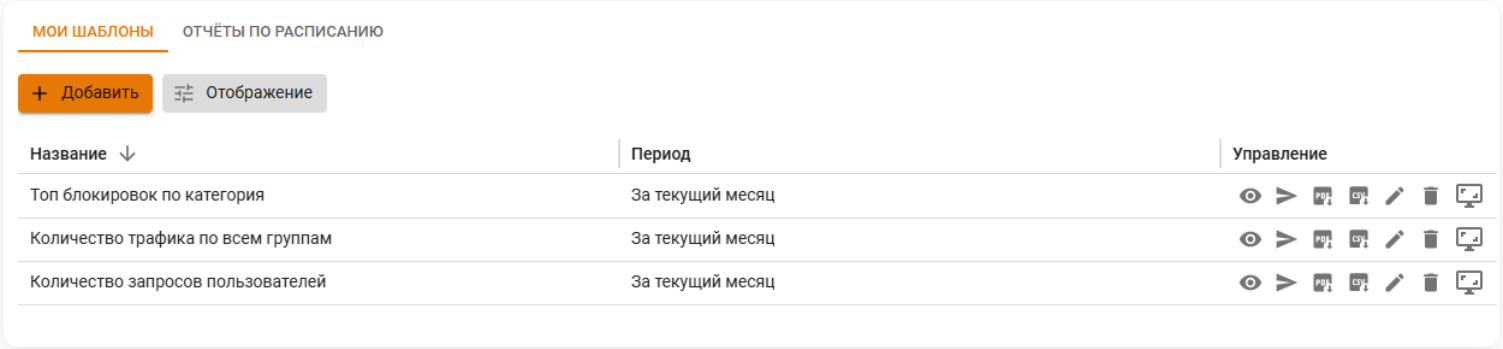
Для поиска нужной сессии воспользуйтесь одним из способов:

- Нажмите кнопку **Фильтры**, установите параметр поиска (все наименования доступных столбцов) и значение.
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Конструктор отчетов

Классический контекст | Высокопроизводительный контекст | API

В разделе **Отчеты и журналы** → **Конструктор отчетов** доступно создание шаблонов отчетов со статистическими данными и настройка автоматической отправки по email в форматах PDF и/или CSV по расписанию:



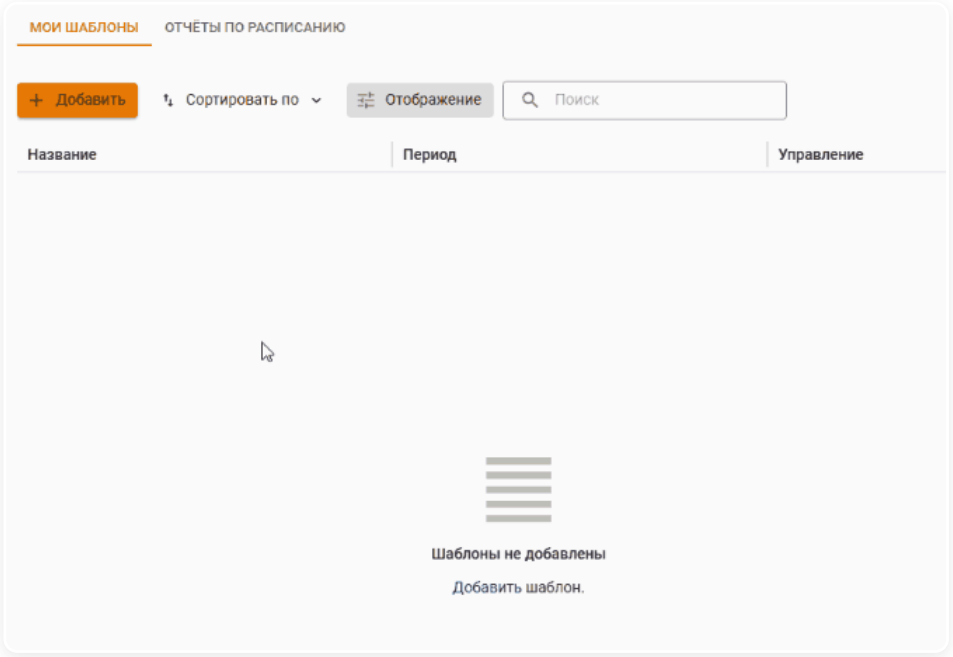
Ideco NGFW Novum хранит данные в течение определенного времени, по прошествии которого данные безвозвратно удаляются.

Сроки хранения данных по разделам:

- Система - 90 дней.
- Логи служб - 14 дней.
- Данные веб-трафика (Веб-трафик, а также посещенные сайты) - 1 месяц.
- События безопасности (Журнал IPS и Web application firewall) - 3 месяца.
- Действия администраторов и Аутентификация администраторов - 1 год.
- Аутентификация пользователей - 180 дней.

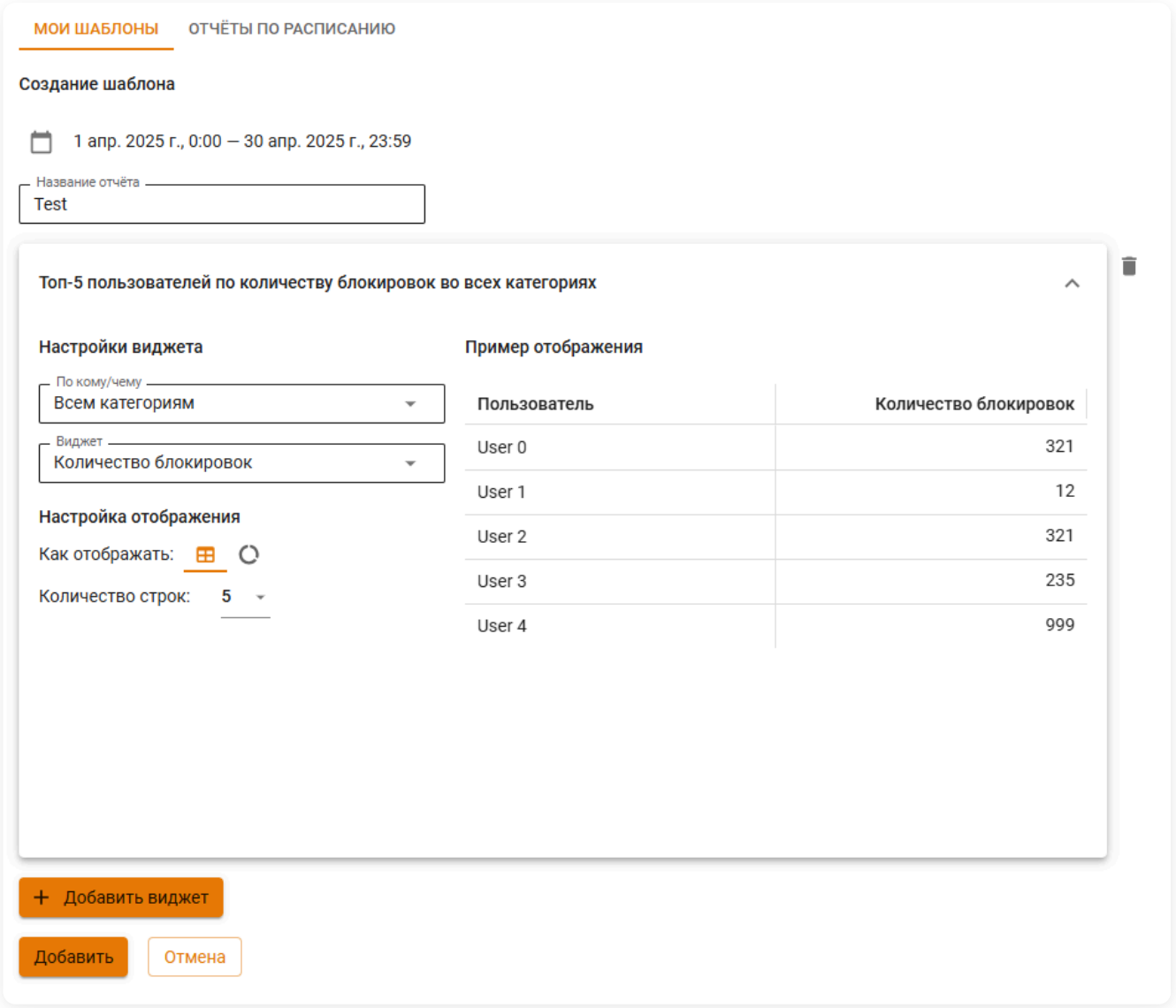
Создание шаблона

1. На вкладке **Мои шаблоны** нажмите **Добавить** и заполните поля:



- **Период** - укажите временной промежуток, за который следует сформировать отчет, из предложенных фильтров или укажите даты, нажав **Выбрать дату**.
- **Название отчета** - укажите название отчета.

2. Нажмите **Добавить виджет** и заполните поля:



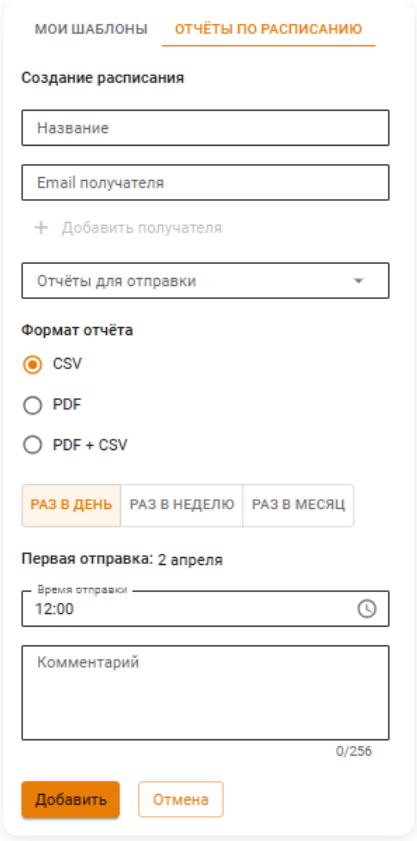
- **По кому/чему** - выберите объект, по которому будет собираться статистика. Если выбираете **Определенный** объект (например, ***Определенный пользователь*** или ***Определенная группа***), то появится дополнительное поле **Объекты**, где можно выбрать несколько объектов.
- **Виджет** - выберите, какую информацию хотите видеть по выбранному объекту. Один шаблон может содержать несколько виджетов. Некоторые виджеты позволяют настроить отображение данных в шаблоне отчета:
  - **Настройки отображения** - настройте, как должны отображаться данные в отчете.

3. Для сохранения шаблона нажмите **Добавить**.

Созданный шаблон можно редактировать, просмотреть в браузере, отправить на почту или скачать в формате PDF или CSV, нажав соответствующую кнопку в столбце **Управление**.

Настройка расписания

1. На вкладке **Отчеты по расписанию** нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Название** - укажите название расписания.
- **Email получателя** - укажите адрес электронной почты. Можно указать несколько почтовых адресов через кнопку **Добавить получателя**.
- **Отчеты для отправки** - выберите шаблон отчета для отправки.
- **Формат отчета** - выберите вариант формата для отправки отчета.
- **Периодичность рассылки отчетов**:
  - **Раз в день** - укажите время. Если при создании настройки время отправки меньше текущего на сервере, то отправка отчетов произойдет на следующий день.
  - **Раз в неделю** - укажите день и время отправки.
  - **Раз в месяц** - укажите необходимый день месяца. Если выбрано 31 число, но в месяце меньше дней, то выбирается последнее число месяца.
- **Комментарий** - произвольный текст, поясняющий назначение расписания отправки отчетов.
  Текст отображается только в Ideco NGFW Novum и не будет отправляться в отчетах.

2. Сохраните расписание, нажав **Добавить**.

3. Включите расписание, нажав на (по умолчанию выключено).

NGFW Novum сохранит все пользовательские настройки времени отправки во всех фильтрах (раз в день, раз в неделю и раз в месяц), но шаблон отчета будет отправляться автоматически после включения расписания и только в период, выбранный пользователем.

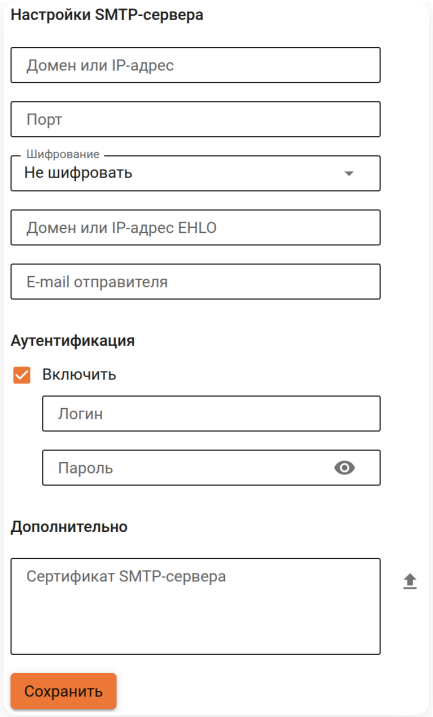
Если в таблице большое количество правил, воспользуйтесь кнопкой **Фильтры**:

Настройка отправки

1. На вкладке **Настройки отправки** выберите **Метод доставки**:

- **my.ideco.ru** - доставка писем с помощью MY.IDECO.
- **SMTP-сервер** - доставка писем с помощью SMTP-сервера.

При выборе метода **SMTP-сервер** заполните поля:



Расшифровка полей

Настройки SMTP-сервера:

- **Домен или IP-адрес** - домен или адрес SMTP-сервера, с помощью которого будут отправляться письма.
- **Порт** - порт SMTP-сервера.
- **Шифрование** - тип шифрования, используемый при соединении с SMTP-сервером. Доступные варианты: Не шифровать, TLS, STARTTLS.
- **Домен или IP-адрес EHLO** - домен или адрес, которые устройство указывает SMTP-серверу в команде EHLO.
- **E-mail отправителя** - адрес, от имени которого будут отправляться письма.

Аутентификация:

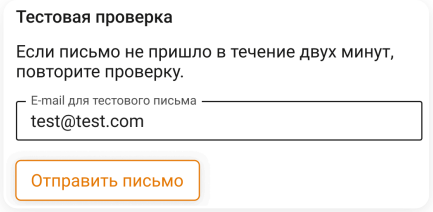
- **Включить** - при включении опции заполняются поля **Логин** и **Пароль** пользователя для аутентификации на SMTP-сервере.

Дополнительно:

- **Сертификат SMTP-сервера** - загрузка сертификата сервера. Используется, если SMTP-сервер применяет собственный сертификат и необходимо доверие со стороны Ideco NGFW Novum.

2. Нажмите **Сохранить**.

3. Для выполнения **Тестовой проверки** укажите e-mail получателя и нажмите **Отправить письмо**:



Пример настройки ежемесячного отчета

Необходимо настроить отправку отчета с информацией о заблокированных сайтах по всем пользователям. Периодичность - ежемесячно, каждое первое число месяца.

Создайте шаблон отчета, на основании которого будет собрана статистика для отправки:

1. Нажмите **Добавить** на вкладке **Мои шаблоны**.

2. Выберите временной период, за который следует сформировать отчет.

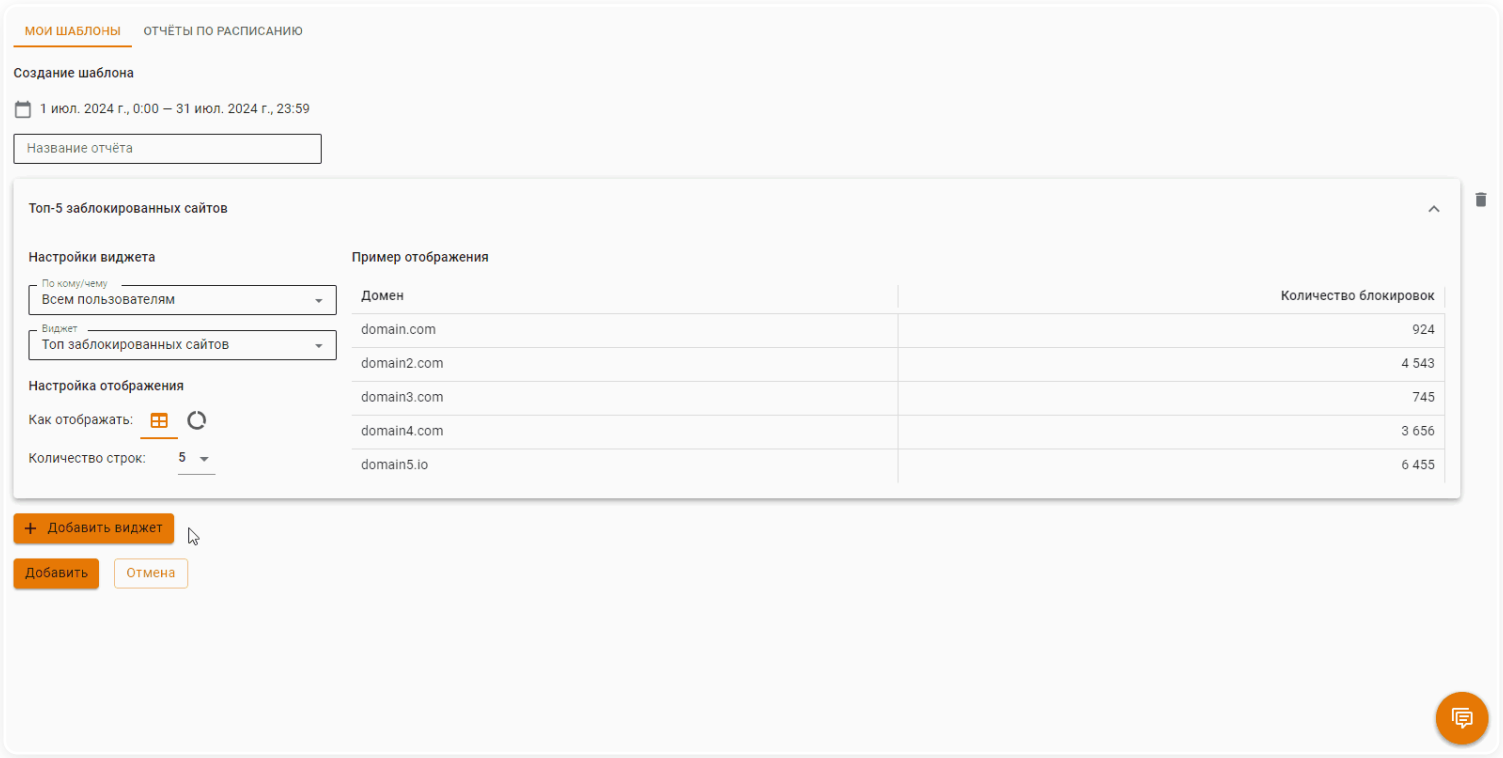
3. Укажите название в поле **Название отчета**.

4. Нажмите **Добавить виджет**.

5. Заполните поля:

- **По кому/чему** - выберите **Всем пользователям**.
- **Виджет** - выберите **Топ заблокированных сайтов**.

6. Укажите **Настройки отображения** в виде таблицы или круговой диаграммы:



7. Сохраните шаблон, нажав **Добавить**.

Создайте расписание, по которому шаблон отчета будет отправляться на электронную почту:

1. Нажмите **Добавить** на вкладке **Отчеты по расписанию**.

2. Заполните поля:

- **Название** - любое название, которое поможет идентифицировать правило расписания.
- **Email получателя** - электронная почта получателя отчета. Если нужно укажите дополнительные адреса, нажав **Добавить получателя**.

3. Выберите нужный шаблон в поле **Отчеты для отправки**.

4. Выберите формат, в котором хотите получать отчет.

5. Укажите настройки даты/дня и времени отправки отчета получателю (раз в месяц, каждый 1-й день месяца).

6. Сохраните расписание, нажав **Добавить**.

7. Включите расписание.

8. Перейдите на вкладку **Настройки отправки** и выберите **Метод доставки** отчета.

Управление сервером

Администраторы

Создание локальных администраторов, интеграция администраторов из сервисов Active Directory, ALD PRO, RADIUS

Перейти >

Ideco Center

Настройка интеграции Ideco NGFW к Ideco Center

Перейти >

VCE

Настройка VCE в Ideco NGFW, чтобы разделить одну локальную сеть на несколько независимых подсетей

Перейти >

Кластеризация

Настройка кластера, состоящего из двух серверов Ideco NGFW

Перейти >

Обновления

Настройка параметров автоматического обновления в Ideco NGFW

Перейти >

Бэкапы

Процесс создания и восстановления бэкапа Ideco NGFW

Перейти >

Терминал

Терминал для диагностики проблем на Ideco NGFW

Перейти >

Лицензия

Онлайн- Офлайн-привязка лицензии к серверу Ideco NGFW

Перейти >

Дополнительно

Настройка часового пояса и сбор анонимной статистики

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Администраторы

Классический контекст | Высокопроизводительный контекст | API

В Ideco NGFW Novum можно создать локальных администраторов или интегрировать администраторов из сервисов Active Directory, ALD PRO, FreeIPA, RADIUS.

При обновлении на версию 21 убедитесь, что логины локальных администраторов соответствуют требованиям:

- Не начинаются с цифры.
- Не содержат специальных и пробельных символов, кроме дефиса `-`.
- **Длина логина** - от 1 до 31 символа включительно.

Учетные записи администраторов, чьи логины не соответствуют требованиям, будут отключены.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока администратор будет автоматически деавторизован.

Сведения об авторизованных администраторах представлены в **Отчеты и журналы** → **Аутентификация администраторов** и **Сессии администраторов**.

Роли администраторов

Роль	Возможности
Администратор	• Полный доступ ко всем настройкам NGFW Novum, возможность создания новых настроек, правил, учетных записей других пользователей NGFW Novum, а также редактирования, управления и удаления их • Создание пользователей с правами администратора
Только просмотр	• Полный доступ к просмотру всех настроек NGFW Novum без возможности создания новых настроек, правил, учетных записей других пользователей NGFW Novum, а также редактирования, управления и удаления их

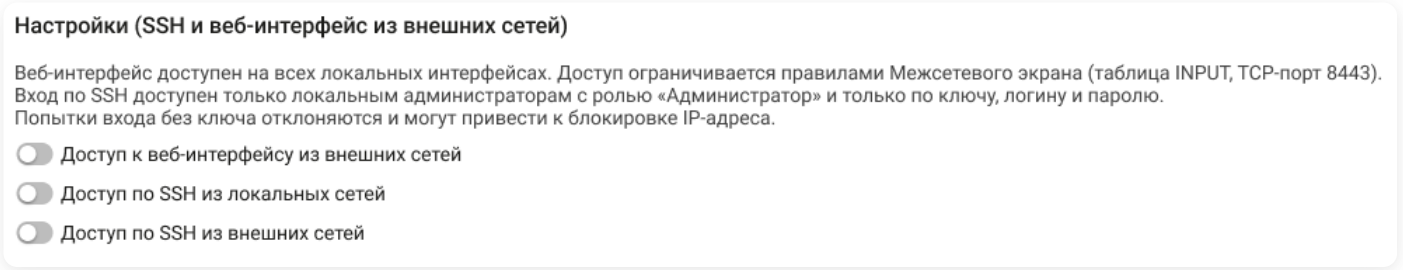
Администратор ИБ	• Выбор событий безопасности, подлежащих регистрации в журнале **События безопасности**
	• Чтение журнала **События безопасности**
	• Настройка параметров выгрузки информации о событиях безопасности, зарегистрированных в NGFW Novum
	• Формирование отчетов в формате `.csv` с учетом заданных критериев отбора и выгрузка их из журнала событий безопасности NGFW Novum
	• Настройка и получение оповещений в веб-интерфейсе NGFW Novum в случае:
	  ◦ выявления признаков вредоносного программного обеспечения в передаваемых файлах
	  ◦ выявления сетевого трафика, в котором обнаружен признак компьютерной атаки
	• Получение уведомлений о непройденной проверке контрольных сумм

Администратор межсетевого экрана	• Создание учетных записей других пользователей NGFW Novum.
	• Управление учетными записями пользователей NGFW Novum, в том числе возможность создания, изменения или удаления идентификаторов, а именно: логин пользователя, имя пользователя, IP-адрес пользователя, MAC-адрес пользователя, телефон пользователя
	• Назначение полномочий пользователям NGFW Novum, определяемых их ролями
	• Определение периода неактивности пользователя, по истечении которого сессия пользователя будет завершена (10 минут, 15 минут, 30 минут, 1 час, 2 часа, 8 часов, 12 часов, 1 день)
	• Установка правил фильтрации, позволяющих настроить разрешение или запрет (блокирование) прохождения сетевого трафика с использованием атрибутов фильтрации сетевого трафика, а также результатов обнаружения компьютерных атак и вредоносного программного обеспечения
	• Изменение и удаление правил фильтрации NGFW Novum
	• Применение правил фильтрации к:
	  ◦ сетевым интерфейсам NGFW Novum
	  ◦ идентифицированным пользователям NGFW Novum
	  ◦ идентифицированным приложениям, используемым при сетевом взаимодействии
	• Управление приоритетами применения правил фильтрации
	• Включение и отключение отдельных правил фильтрации при настройке анализа сетевого трафика на наличие признаков компьютерных атак
	• Установка собственных правил фильтрации при настройке анализа сетевого трафика на наличие признаков компьютерных атак
	• Управление режимами работы NGFW Novum
	• Изменение конфигурации NGFW Novum
	• Тестирование NGFW Novum

Администратор настройки доступов	• Создание учетных записей других пользователей NGFW Novum • Управление учетными записями пользователей NGFW Novum, в том числе возможность создания, изменения или удаления идентификаторов, а именно: логин пользователя, имя пользователя, IP-адрес пользователя, MAC-адрес пользователя, телефон пользователя • Назначение полномочий пользователям NGFW Novum, определяемых их ролями • Определение периода неактивности пользователя, по истечении которого сессия пользователя будет завершена (10 минут, 15 минут, 30 минут, 1 час, 2 часа, 8 часов, 12 часов, 1 день) • Создание, управление и удаление правил в разделах **Обратный прокси**, **Сертификаты**, **Почтовый релей** и **Ограничение скорости**
Просмотр отчетов	• Просмотр отчетов для следующих журналов: **Трафик**, **Система**, **Веб-трафик**, **Межсетевой экран**, **События безопасности**, **Аутентификация пользователей** и **Аутентификация пользователей ЛК**
Создание отчетов	• Просмотр, настройка и выгрузка отчетов в формате `.csv` для следующих журналов: **Трафик**, **Система**, **Веб-трафик**, **Межсетевой экран**, **События безопасности**, **Аутентификация пользователей**, **Аутентификация пользователей ЛК** и **Конструктор отчетов**

Доступ к веб-интерфейсу из внешней сети и удаленный доступ по SSH

Для настройки перейдите в **Управление сервером** → **Администраторы** → **Настройки**:



- **Доступ к веб-интерфейсу из внешней сети** - включите опцию для получения доступа к Ideco NGFW Novum из внешней сети. Это позволяет администрировать Ideco NGFW Novum удаленно. Попытки подбора паролей блокируются автоматически.
- **Доступ по SSH из локальных сетей** - включите для получения доступа к Ideco NGFW Novum по SSH из локальной сети (порт 22 TCP). Попытки подбора паролей блокируются автоматически.
- **Доступ по SSH из внешних сетей** - включите для получения доступа к Ideco NGFW Novum по SSH из внешних сетей (порт 22 TCP). Попытки подбора паролей блокируются автоматически.

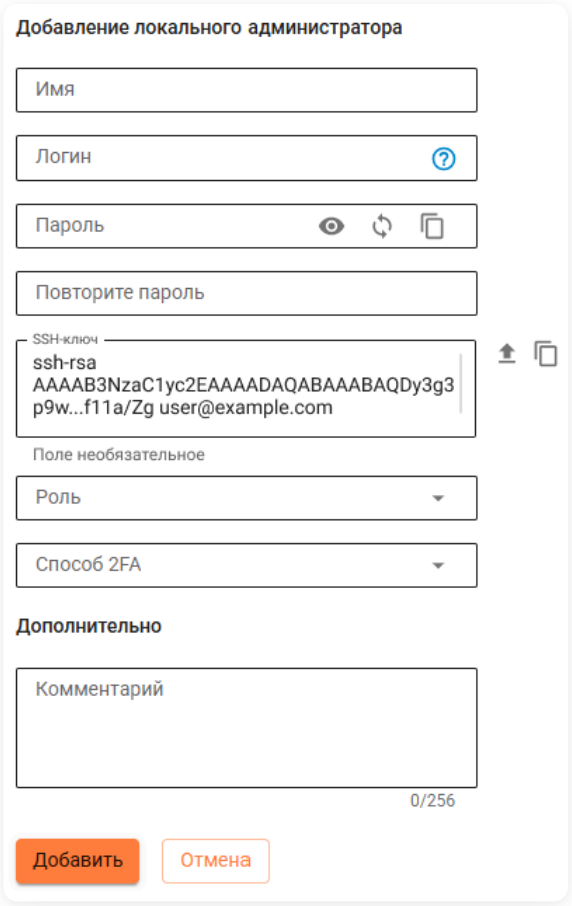
Подробнее о настройке подключения к веб-интерфейсу при удаленном доступе смотрите в статье Удаленный доступ для управления сервером.

Управление локальными администраторами

Чтобы добавить нового локального администратора выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **Администраторы** → **Локальные** и нажмите **Добавить**.

2. Заполните поля:



- **Имя** - введите имя нового администратора. Значение не должно быть длиннее 42 символов.
- **Логин** - введите логин нового администратора. Значение не должно начинаться с цифры, содержать специальные и пробельные символы, кроме дефиса `-`. Длина логина - от 1 до 31 символа.
- **Пароль/повторите пароль** - введите пароль нового администратора. Требования к паролю:
  - Минимальная длина пароля - 12 символов.
  - Содержит строчные и заглавные латинские буквы.
  - Содержит цифры.
  - Содержит специальные символы (! # $ % & ' * + и другие).
- **SSH-ключ** - вставьте SSH-ключ. Должна быть включена хотя бы одна из опций доступа по SSH.
- **Роль** - выберите роль.
- **Способ 2FA** - выберите второй фактор для авторизации администратора. Доступны TOTP-токен и RADIUS 2FA, настраиваемые на вкладке **Двухфакторная аутентификация**.

3. Нажмите **Добавить**.

Чтобы изменить имя и пароль администратора, нажмите  в столбце **Управление**.

Подробнее о восстановлении пароля администратора смотрите в статье по ссылке.

Если в таблице большое количество администраторов, воспользуйтесь кнопкой **Фильтры**.

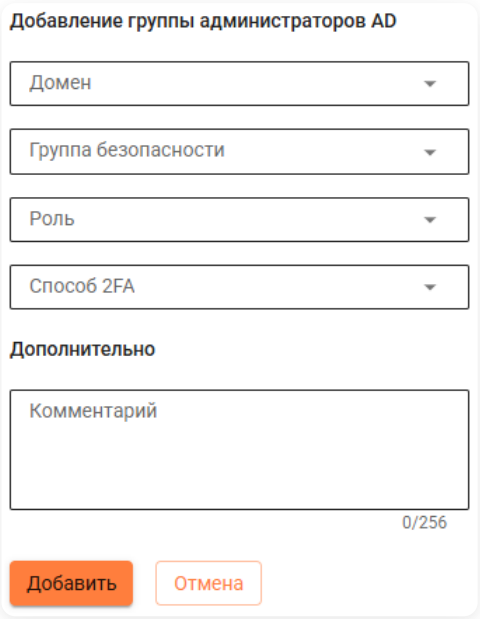
Управление AD/ALD/FreeIPA администраторами

Чтобы добавить администраторов, необходимо ввести NGFW Novum в домен Active Directory. При удалении домена AD/ALD/FreeIPA из Ideco NGFW Novum будут удалены сессии администраторов.

Чтобы интегрировать администраторов Active Directory, ALD Pro или FreeIPA с Ideco NGFW Novum, выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **Администраторы**, выберите нужную вкладку и нажмите **Добавить**.

2. Заполните поля:



- **Домен** - выберите доменное имя.
- **Группа безопасности** - выберите созданную группу безопасности.
- **Роль** - выберите роль. Роли AD/ALD/FreeIPA администраторов идентичны ролям локальных администраторов.
- **Способ 2FA** - выберите второй фактор для авторизации администратора. Доступны TOTP-токен и RADIUS 2FA, настраиваемые на вкладке **Двухфакторная аутентификация**.

3. Нажмите **Добавить**.

Особенности работы:

- Если администратор был авторизован по правилу или группе безопасности, которые были удалены, то сессия администратора будет удалена. Это произойдет только после синхронизации групп безопасности на Ideco NGFW Novum, которая выполняется каждые 5 минут.
- Если администратора исключить из группы безопасности, то администратор не будет удален сразу. Сессия завершится через некоторое время, и при следующей попытке авторизации администратор не сможет войти в систему.
- Если администратор соответствует нескольким правилам при авторизации, например, входит в несколько выбранных групп безопасности, ему будет отказано в доступе. Это необходимо, чтобы избежать проблем в определении прав доступа для администратора.

Управление RADIUS-администраторами

Особенности настройки RADIUS-сервера

В Ideco NGFW Novum используется **Vendor Code** 39410. Для авторизации через RADIUS укажите атрибуты:

```
ATTRIBUTE   Ideco-Administrator-Role           30  string
ATTRIBUTE   Ideco-Administrator-Name           31  string
```

`Ideco-Administrator-Role` обязателен для авторизации, а `Ideco-Administrator-Name` опционален. Атрибуты передают ID роли и ФИО администратора соответственно. Роли RADIUS-администраторов идентичны ролям локальных администраторов.

ID роли администраторов

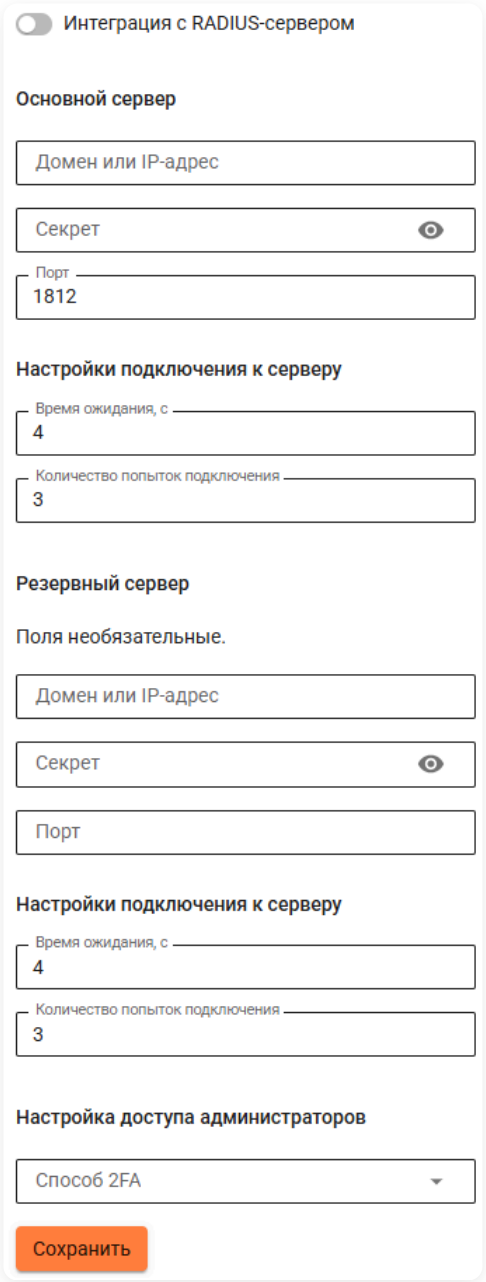
- `predefined_admin_write` - Администратор.
- `predefined_admin_readonly` - Только просмотр.
- `predefined_security_admin` - Администратор информационной безопасности.
- `predefined_firewall_admin` - Администратор межсетевого экрана.

- `predefined_access_settings_admin` - Администратор настройки доступов.
- `predefined_reports_view` - Просмотр отчетов.
- `predefined_reports_change` - Создание отчетов.

Интеграция администраторов RADIUS с Ideco NGFW Novum

Выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **Администраторы** → **RADIUS** и включите опцию **Интеграция с RADIUS-сервером**:



2. Укажите параметры соединения для основного RADIUS-сервера:

- **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
- **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
- **Порт** - порт, по которому будет происходить подключение к серверу. Поменяйте при необходимости.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
  - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.
- **Способ 2FA** - выберите второй фактор для авторизации администратора. Доступны TOTP-токен и RADIUS 2FA, настраиваемые на вкладке **Двухфакторная аутентификация**.

3. При наличии в сети двух RADIUS-серверов настройте резервный с указанием порта подключения. При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.

4. Нажмите **Сохранить**.

Особенности удаления администраторов

- Если администратора удалить из раздела **Администраторы**, то сессия будет автоматически завершена, и администратор потеряет доступ к веб-интерфейсу.
- Если администратора удалить из группы безопасности, то сессия будет автоматически завершена через 24 часа после авторизации.

Чтобы удалить администратора, нажмите напротив нужной учетной записи. Можно удалить и собственный аккаунт.

Не рекомендуем удалять или отключать всех администраторов с ролью **Администратор**, это приведет к тому, что доступ к настройке Ideco NGFW Novum будет потерян. Если это произошло, обратитесь в Техническую поддержку.

Аутентификация администраторов

Ideco NGFW Novum не только блокирует попытки авторизации с неправильными логином или паролем, но и обнаруживает случаи, когда не удается получить информацию об администраторе из контроллера домена.
Если администратор не соответствует ни одному из правил авторизации, Ideco NGFW Novum считает попытку авторизации неудачной.
Доступ блокируется, если количество неудачных попыток превышает шесть, а для версии ФСТЭК - четыре.

Чтобы получить доступ к веб-интерфейсу Ideco NGFW Novum, администратору нужно выполнить процедуру аутентификации, указав логин и пароль.

Для разных групп администраторов предусмотрены разные логины:

- **Локальный администратор** - логин в формате `User`.
- **AD/ALD администратор** - логин в формате `User@test.com`, где `test.com` домен.
- **RADIUS администратор** - логин в формате `User@radius`, где `@radius` обязательная часть логина.

Двухфакторная аутентификация администраторов

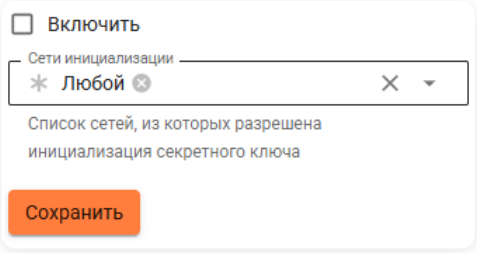
Для настройки двухфакторной аутентификации для администраторов перейдите в **Управление сервером → Администраторы → Двухфакторная аутентификация**. Для администраторов доступны два способа двухфакторной аутентификации:

- **TOTP-токен** - сканирование QR-кода или ручной ввод ключа (доступен только один токен).
- **RADIUS-серверы** - через RADIUS-серверы (может быть несколько).

Выберите необходимую вкладку:

TOTP-токен

Настройте использование TOTP-токена:



- **Включить** - опция активирует этот способ аутентификации.
- **Сети инициализации** - список сетей, из которых разрешена инициализация секретного ключа.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW Novum с использованием TOTP-токена смотрите по ссылкам:

- Rutube
- Youtube

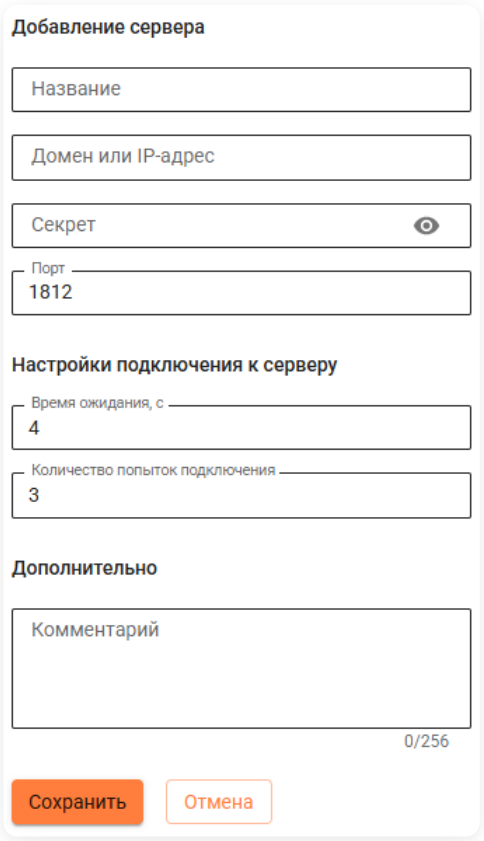
- docs.ideco.ru

RADIUS-сервер

При необходимости можно настроить несколько RADIUS-серверов для двухфакторной аутентификации. Для каждого сервера выполните шаги:

1. Нажмите **Добавить**.

2. Заполните поля:



- **Название** - уникальное название способа 2FA, которое будет использоваться в настройке доступа. Запрещены названия `TOTP-токен`, `Мультифактор` и `SMS Aero`.
- **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
- **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
- **Порт** - порт, по которому будет происходить подключение к серверу.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию `4`.
  - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию `3`.
- **Комментарий** - необязательное поле.

3. Нажмите **Сохранить**.

Реестр 2FA

На вкладке отображаются все администраторы (локальные, AD, ALD, RADIUS) с инициализированным TOTP-токеном.

Если требуется сбросить TOTP-токен администратора (например, при потере телефона), нажмите напротив соответствующей записи:

Фильтры | Отображение | Поиск

ID	Логин	Имя	Домен	Каталог	Управление
43e4ed4c-832b-40c9-b8bd-ec9e4f…	z3vs101	Алексей	AD in.ideco	AD Active Directory	
78b43d57-5d0a-4681-8d6c-775bb…	i.petr0v14	Иван	AD in.ideco	ALD ALD Pro	
c078e196-1218-4cac-a0bf-b1a6d9…	-	-	AD in.ideco	RAD RAD	
c5dc4ef5-8067-4ec7-850d-03c143…	jup1ter	Константин	AD in.ideco	Локальные	

Удаленный доступ к серверу

Доступ по SSH к локальному меню сервера

Для подключения по SSH из внешних или локальных сетей выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы**.

2. Активируйте необходимую настройку:

- **Доступ по SSH из внешних сетей**.
- **Доступ по SSH из локальных сетей**.

3. Подключитесь к серверу с помощью любого SSH-клиента (для Windows, например, PuTTY), используя 22 порт. Необходимо указать логин и пароль **Администратора**.

4. Используйте `ideco-local-menu --debug` для доступа к локальному меню или `ls` для вывода каталогов текущей директории.

Пример подключения при помощи OpenSSH через консоль:

```
[test@My-PC home]$ ssh admin@192.168.100.183
admin@192.168.100.183's password:
Last login: Wed Sep  6 11:51:38 2023 from 192.168.100.1
[admin@localhost ~]#
```

Доступ к веб-интерфейсу сервера из интернета

Доступ из внешней сети:

- Включите функцию **Доступ к веб-интерфейсу из внешней сети** в **Управление сервером** → **Администраторы**. Для доступа введите внешний IP-адрес Ideco NGFW Novum и порт 8443.

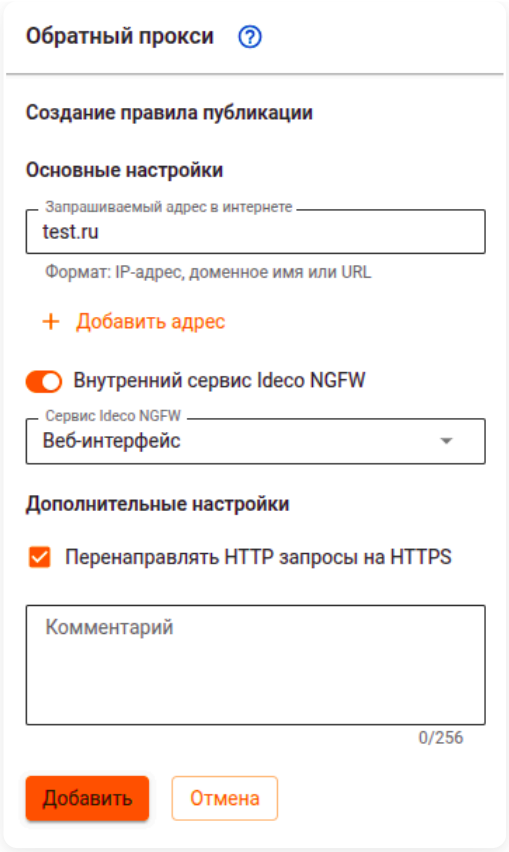
Доступ по VPN:

- Создайте VPN-подключение к серверу, например, по IKEv2 или SSTP. После подключения перейдите в веб-интерфейс по IP-адресу любого локального интерфейса с указанием порта 8443 (в том числе по IP-адресу из диапазона для VPN-подключений. Адрес по умолчанию - 10.128.0.1).

Публикация через обратный прокси:

1. Перейдите в **Сервисы** → **Обратный прокси**.

2. Добавьте новое правило, заполнив поля:



3. Укажите в качестве запрашиваемого адреса IP-адрес, доменное имя или URL, который будет запрашиваться пользователями.

4. Нажмите **Добавить** и перейдите по одному из адресов, которые были указаны в поле **Запрашиваемый адрес в интернете**.

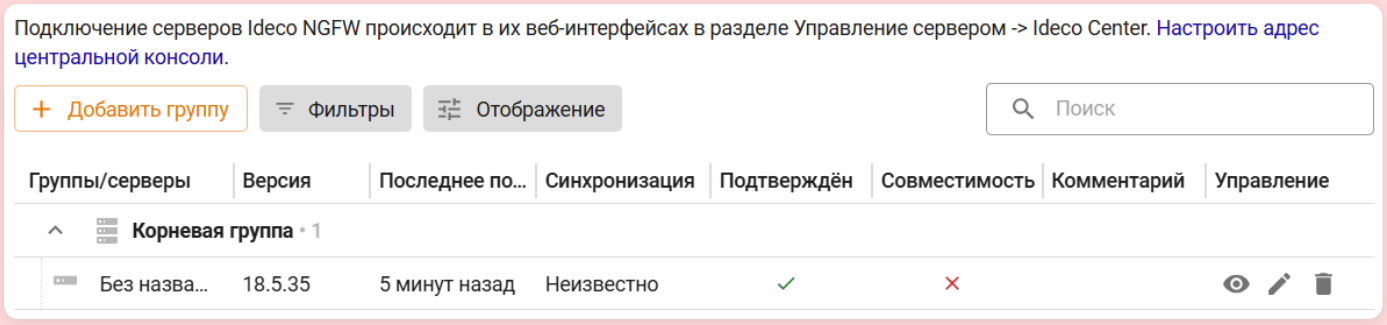
Ideco Center

Классический контекст | Высокопроизводительный контекст | API

Ideco Center - центральная консоль, помогающая в администрировании нескольких серверов Ideco NGFW Novum. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW Novum.

Подключение Ideco NGFW Novum к Ideco Center

При синхронизации Ideco Center и Ideco NGFW Novum с разными мажорными версиями передача правил с Ideco Center происходить не будет. При этом в разделе **Серверы** будет информация о том, что Ideco Center и Ideco NGFW Novum несовместимы:

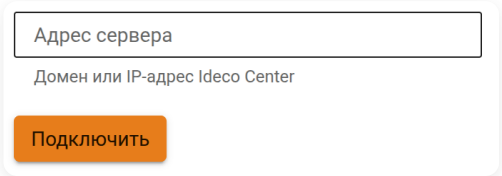


Особенности работы:

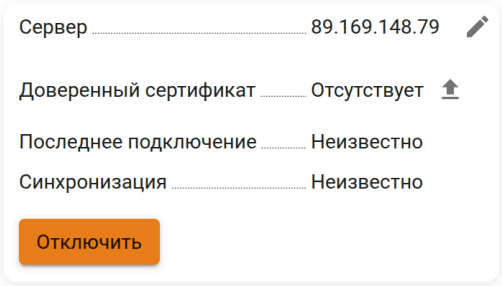
- Сетевое подключение производится в направлении от Ideco NGFW Novum к Ideco Center, т. е. возможна связь и когда Ideco NGFW Novum за NAT.
- Если сервер Ideco Center находится за NAT, в Ideco Center укажите IP-адрес NAT-устройства или доменное имя в **Управление сервером → Дополнительно → Адрес Ideco Center**.
- Для синхронизации базы данных отчетов и журналов между серверами используется WireGuard.
- Для остальных коммуникаций между серверами используется WebSocket.
- Соединение между серверами шифруется по протоколу TLS 1.3. Старые версии протокола (TLS 1.0, TLS 1.1, TLS 1.2) отключены.

1. Перейдите в **Управление сервером → Ideco Center**.

2. Введите IP-адрес или доменное имя в поле **Адрес сервера** и нажмите **Подключить**:

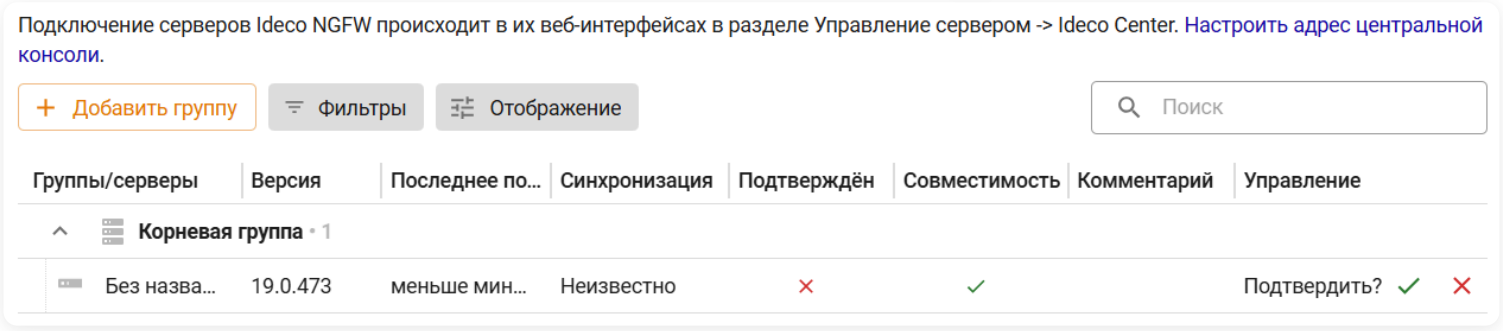


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW Novum или VCE:

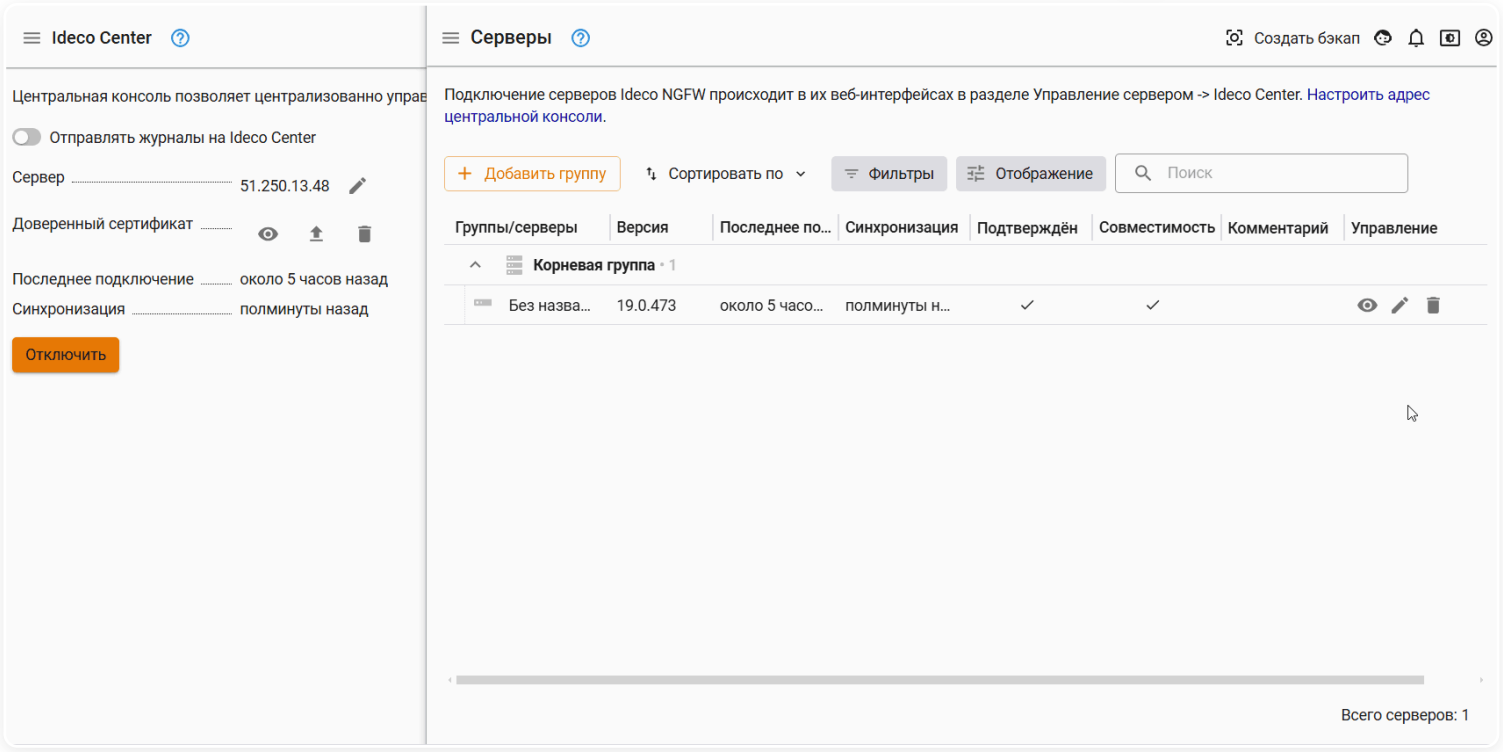


Скачать корневой сертификат можно в Ideco Center в разделе **Сервисы** → **Сертификаты**.

3. В интерфейсе Ideco Center перейдите в раздел **Серверы** и подтвердите подключение, нажав ✓:



Для удаления сервера Ideco NGFW Novum из Ideco Center разорвите привязку в интерфейсе Ideco Center, нажав 🗑:



VCE

API

Функциональность доступна в **Системном контексте**.

Название службы раздела **VCE**: `ideco-vce-backend`, `ideco-vce-rest`, `ideco-vce-vpp`.

Список служб для других разделов доступен по ссылке.

VCE (virtual context engine) - функциональность Ideco NGFW Novum, реализованная с помощью контейнеров Linux на базе systemd-nspawn, которая позволяет создавать виртуальные серверы (контексты) на одном системном NGFW Novum. Это дает возможность:

- Разбить одну локальную сеть на несколько независимых сетей с полной изоляцией трафика между ними. Коммуникация корневого сервера с виртуальными контекстами осуществляется через внешние сетевые мосты.
- Индивидуально создавать для каждой сети политики безопасности и объекты.
- Разграничивать доступ и независимо управлять дочерними VCE.

При этом нет необходимости устанавливать и настраивать для этого отдельные физические серверы.

Архитектура виртуальных контекстов не является Multitenancy.

Виртуальные контексты изолированы по ресурсам процессора и памяти, независимо обрабатывают трафик и имеют собственные конфигурации. Но интерфейсы и сетевые зоны контекстов конфигурируются из системного контекста, и администраторы системного контекста имеют доступ к конфиграции внутри VCE.

В 21 версии появилась возможность создавать два типа виртуальных контекстов:

- **Классический (VCE NGFW)** - контекст на основе решения NGFW. Настройки разделов в VCE NGFW идентичны настройкам в продукте Ideco NGFW Novum.
- **Высокопроизводительный (VCE VPP)** - контекст с обработкой трафика в VPP. Документация по настройке разделов VCE VPP доступна по ссылке.

Таблица с различиями между VCE NGFW и VCE VPP в статье.

Не предоставляйте доступ к VCE сторонним организациям, поскольку полная изоляция VCE не реализована и не предусмотрена. Предоставление доступа сторонним организациям может привести к угрозе безопасности сервера.

Платформы Ideco SX+ и Ideco SMX в текущих версиях не поддерживают запуск VCE. Поддержка планируется в следующих версиях.

Возможности VCE:

- Создание виртуальных контекстов и настройка независимых сетевых интерфейсов.
- Независимая настройка политик безопасности и прав доступа различным виртуальным контекстам.
- Связь с Ideco Center.
- Запуск и остановка виртуальных контекстов с одного **Системного контекста**.

Лицензия между **Системным контекстом** и всеми виртуальными контекстами общая. Это значит, что на Ideco NGFW Novum с лицензией на 100 пользователей можно создать неограниченное количество VCE, каждый из которых будет поддерживать 100 пользователей. В будущих версиях количество пользователей, ограниченное числом в лицензии, будет распределяться между **Системным контекстом** и всеми VCE.

В интерфейсе VCE недоступно:

- Создание кластера.
- Обновление.
- Переход в **Профиль** через иконку в шапке веб-интерфейса (настраивается в системном контексте).
- Возможность выключения и перезагрузки (настраивается в системном контексте).
- Энергосберегающий режим (настраивается в системном контексте).
- Изменение настроек часового пояса и языка (настраивается в системном контексте).
- Создание и редактирование Сетевых интерфейсов. В дочерних контекстах доступ ограничен интерфейсами текущего VCE в режиме только для чтения.
- Создание зон. Чтобы просмотреть доступные зоны в дочерних контекстах, перейдите в раздел **Правила трафика** → **Объекты**.

Важные моменты работы VCE:

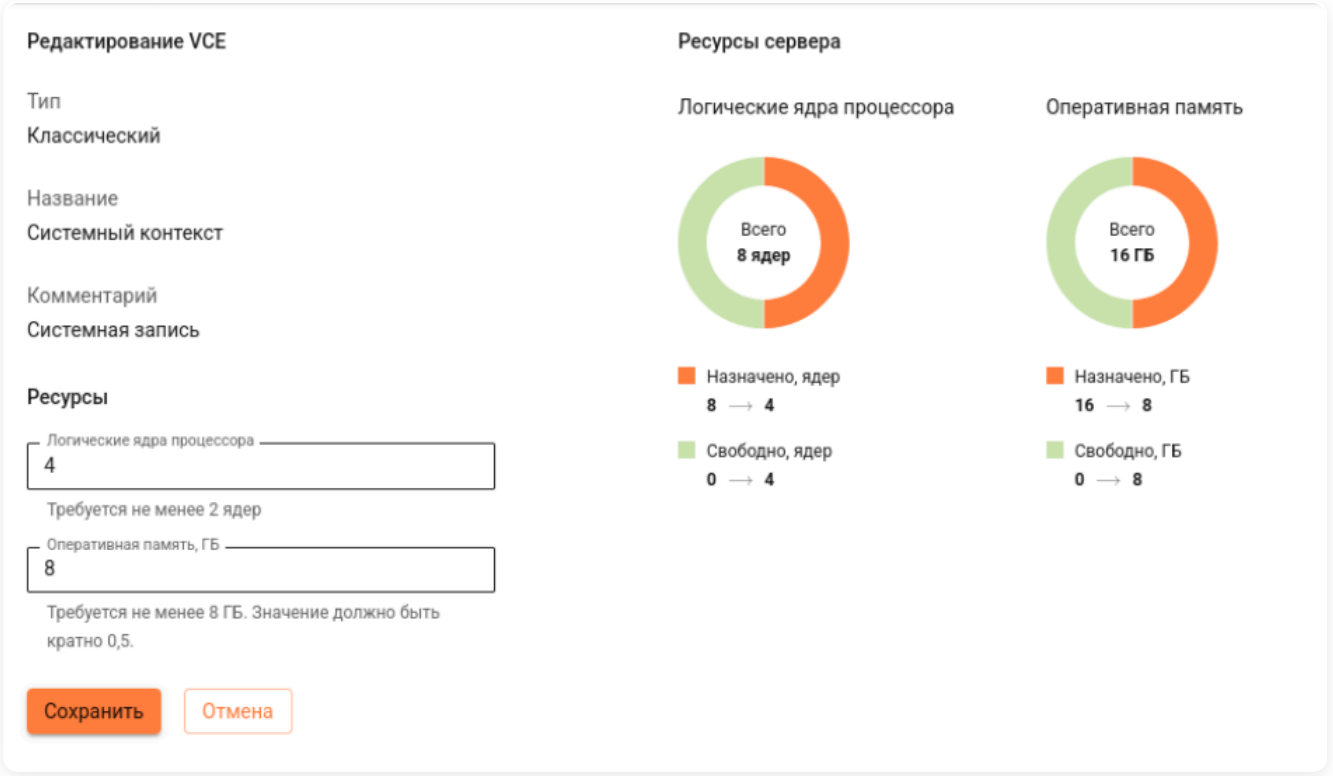
- В бэкап системного VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте бэкапы корневого NGFW и каждого из дочерних VCE.
- При восстановлении системы все настроенные VCE и их данные также откатятся к исходному состоянию.
- Если VCE исчерпает выделенные ресурсы:
  - При нехватке оперативной памяти система начнет выгружать данные на диск, что может привести к завершению процессов и нестабильной работе контекста.
  - При недостатке мощности выделенных ядер CPU возможны задержки и потеря пакетов.
- Каждый контекст использует собственные ресурсы и не влияет на другие.
- **Не рекомендуем использовать двухпроцессорные системы**, так как оптимизация для такого оборудования отсутствует. Поддержка планируется в следующих версиях.
- Рекомендуем отключить технологии при использовании **Высокопроизводительного** контекста, так как они могут существенно снижать производительность:
  - Hyper-Threading (Intel).
  - SMT (AMD).

Создание VCE

С 21 версии поддержка VCE без выделенных ресурсов прекращена.

Чтобы создать виртуальный контекст в рамках VCE, перейдите в **Управление сервером** → **VCE** и выполните действия:

1. Освободите ресурсы, назначенные в **Системном контексте**, и перенесите в список **Свободных ресурсов**. Для этого откройте редактирование VCE, нажав на , и перераспределите ресурсы:

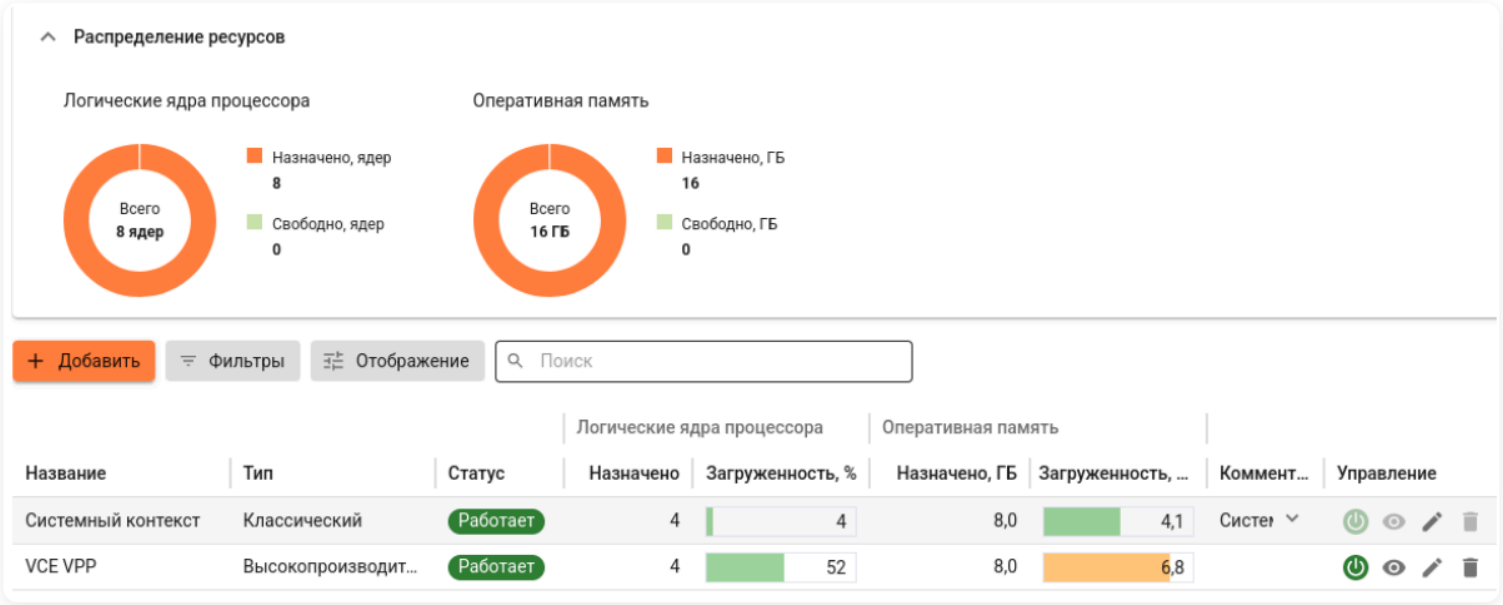


2. Нажмите **Добавить**.

3. Выберите тип создаваемого контекста: **Классический** или **Высокопроизводительный**. Укажите название контекста и назначьте ресурсы:

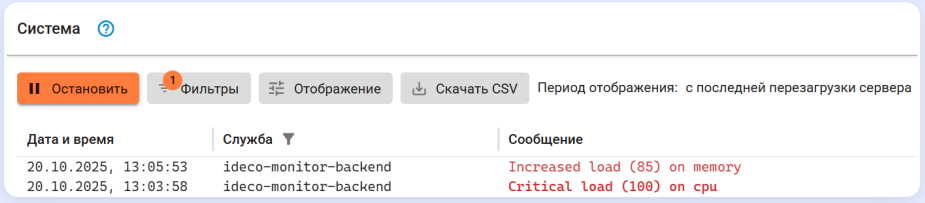
- Для работы классического контекста (VCE NGFW) потребуются минимум 8 ГБ оперативной памяти и 2 логических ядра.
- Для высокопроизводительного контекста (VCE VPP) потребуются минимум 8 ГБ оперативной памяти и 4 логических ядра.

4. Нажмите **Добавить** - виртуальный конктест появится в таблице:



5. Перейдите в **Сервисы → Сетевые интерфейсы** и на вкладке **Интерфейсы** создайте интерфейс для виртуального контекста. Для работы VCE нужен минимум один сетевой интерфейс. Пример настройки.

В 21 версии доступен **Мониторинг здоровья сервера**. Данные о состоянии сервера отображаются в разделе **Панель мониторинга**. При превышении пороговых значений Ideco NGFW Novum отправит уведомление и запишет событие в логи. Для просмотра этих записей перейдите в раздел **Система** и примените фильтр по службе `ideco-monitor-backend`:



Если для VCE выделены минимально возможные ресурсы, то они будут использоваться полностью, а пороговые значения будут всегда превышены. Это штатная работа Ideco NGFW Novum в таких условиях и не считается ошибкой.

Редактирование VCE

Чтобы отредактировать VCE, нажмите на . При редактировании можно менять:

- Название виртуального контекста.
- Выделенные ресурсы.

Изменение VCE приведет к перезапуску контекста и следующих служб:

- **Прокси** - в `ideco-proxy-backend` будет перезапущена служба `squid`.
- **Предотвращение вторжений** - в `ideco-suricata-backend` будет перезапущена служба `ideco-suricata`.
- **Антивирус** - в `ideco-av-backend` будут перезапущены службы `av4web` и `kav-scanner`.

Если в таблице большое количество VCE, воспользуйтесь кнопкой **Фильтры**.

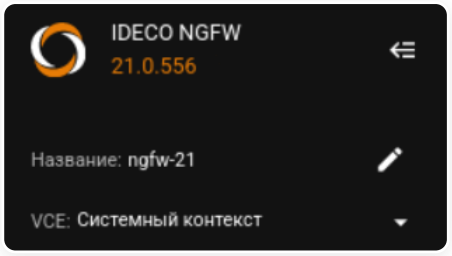
Удаление VCE

Удалить VCE можно, нажав на в системном VCE.

После удаления VCE все его настройки, журналы и внутренние данные будут безвозвратно утеряны. Восстановить их будет невозможно.

Переход в веб-интерфейс VCE

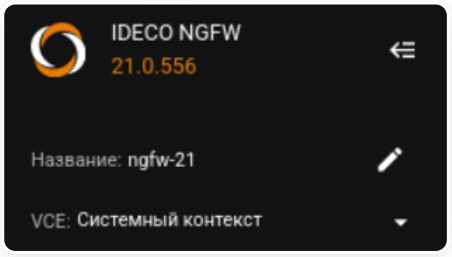
После создания VCE текущий сервер, в котором VCE был создан, будет обозначен как **Системный контекст**:



Перейти в веб-интерфейс созданного VCE из веб-интерфейса NGFW Novum можно двумя способами:

1. Перейдите в **Управление сервером** → **VCE** и нажмите на . В новой вкладке откроется веб-интерфейс VCE.

2. Нажмите на в левом верхнем углу и выберите нужный VCE:



Дополнительно

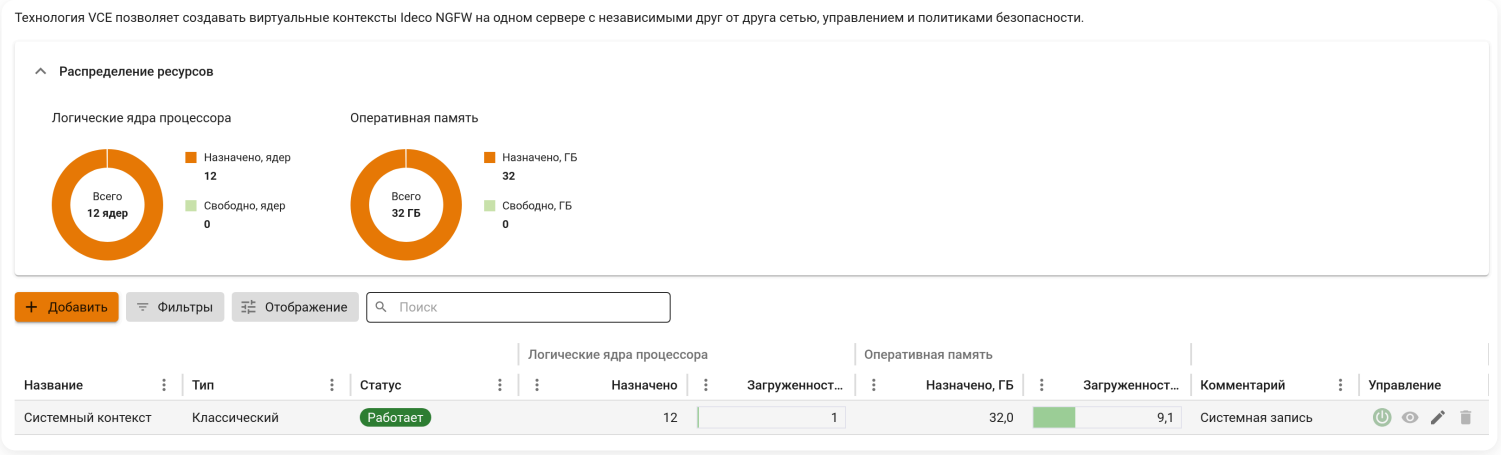
Пример распределения ресурсов для создания виртуального контекста

Настройка виртуального контекста для разделения основного и дочернего офисов, чтобы создавать и настраивать индивидуальные политики безопасности и объекты для каждого офиса.

Создание контекста состоит из двух этапов:

1. Распределение назначенных ресурсов в пул свободных.
2. Выделение свободных ресурсов новому виртуальному контексту.

Рассмотрим процесс на примере системы с конфигурацией: 12 логических ядер процессора и 32 ГБ оперативной памяти:



1. Перейдите в раздел редактирования **Системного контекста**, нажав на .

2. Распределите **Назначенные ресурсы** в пул **Свободных ресурсов** и нажмите **Сохранить**. Если физический сервер оснащен 12 ядрами и 32 ГБ оперативной памяти, а для **Системного контекста** выделено 8 ядер и 16 ГБ, то оставшиеся ресурсы будут перераспределены в свободные ресурсы:

- Для работы классического контекста (VCE NGFW) потребуются минимум 8 ГБ оперативной памяти и 2 логических ядра.
- Для высокопроизводительного контекста (VCE VPP) потребуются минимум 8 ГБ оперативной памяти и 4 логических ядра.

3. Нажмите **Добавить** и выберите тип создаваемого контекста: **Классический** или **Высокопроизводительный**. Укажите название контекста и назначьте свободные ресурсы:

4. Нажмите **Добавить** - виртуальный контекст появится в таблице:

Пример создания интерфейсов

1. Перейдите в **Сервисы** → **Сетевые интерфейсы Системного контекста** и создайте два интерфейса с ролью WAN и LAN, которые будут использоваться в виртуальном контексте:

2. В виртуальном контексте перейдите в **SD-WAN** → **Next hop** и добавьте шлюз для интерфейса с ролью WAN:

3. В виртуальном контексте в **Управление сервером** → **Лицензия** появится информация о лицензии:

Для высокопроизводительного контекста в **Правила трафика** → **Межсетевой экран** по умолчанию установлено запрещающее FORWARD-правило. Если не создать разрешающие правила, все порты и протоколы для пользователей будут запрещены.

Полезные ссылки

- **Настройка высокопроизводительного контекста**
- **Отличия VCE NGFW и VCE VPP**

Отличия VCE NGFW и VCE VPP

Функции, не описанные в таблице, присутствуют и в VCE NGFW, и в VCE VPP.

ГОСТ VPN, **USB-токены**, **Кластеризация** и **VCE** доступны только в **Системном контексте**.
Почтовый релей доступен в **Классическом** и **Системном** контекстах.

В таблице представлены отличия VCE NGFW и VCE VPP:

Функциональность	**NGFW**	**VPP**
Пользователи		
VPN-подключения через IKEv2/IPsec, L2TP/IPsec	✅	❌
Авторизация по MAC-адресу	✅	❌
Использование Профилей TLS в настройках авторизации	❌	✅
Обнаружение устройств	✅	❌
Мониторинг		
Сессии администраторов	✅	❌
Графики загруженности IPsec	✅	❌
Графики загруженности WCCP GRE	✅	❌
Графики загруженности ГОСТ VPN	✅	❌
Графики загруженности VCE	✅	❌
Правила трафика		
Межсетевой экран, функционал: • Аппаратная фильтрация • Настройка ALG • Логирование • Строгая проверка состояний в FORWARD	✅	❌
Персональное ограничение скорости	✅	❌
Исключения	✅	❌
Пользовательские сигнатуры в **Предотвращение вторжений**	✅	❌
Профили безопасности		
Контент-фильтр	Модуль в разделе **Правила трафика**. Функциональность: • Создание правил для запрета, разрешения и фильтрации веб-трафика • Фильтрация трафика только на 80 и 443 TCP-портах • Морфологические словари • Настройки безопасности и выбор сертификатов для MITM	Профили в разделе **Профили безопасности**. Функциональность: • Использование профилей в правилах Межсетевого экрана • Фильтрация трафика на любых TCP-портах

Профили TLS/SSL-инспекции	Модуля в **Профилях безопасности** нет. Доступно: • Расшифровка трафика правилами **Контент-фильтра** • Расшифровка трафика только на 80 и 443 TCP-портах	Профили в разделе **Профили безопасности**. Функциональность: • Использование профилей в правилах Межсетевого экрана • Расшифровка трафика на любых TCP-портах
Сетевые интерфейсы (все интерфейсы создаются, редактируются и удаляются только в системном контексте)		
Loopback	✅	❌
L2TP	✅	❌
PPPoE	✅	❌
PPTP	✅	❌
L2-мост	❌	✅
Сервисы		
Прокси, функции: • WCCP • Прямые подключения	✅	❌
Обратный прокси, функции: • Настройка web-серверов для балансировки запросов • Передача web-серверу реального IP-адреса клиента • Выбор типа публикации	✅	❌
ЛК/Портал SSL VPN, функции: • Публикация ресурсов SSL VPN	✅	❌
Перехват пользовательских DNS-запросов	Встроенная опция	Можно настроить вручную с помощью правил DNAT
DDNS	✅	❌
Перехват пользовательских NTP-запросов	✅	❌
IPsec	✅	❌
Маршрутизация		
Опция адаптивности при настройке маршрутизации Внешних сетей	✅	❌
Отчеты и журналы		
Трафик, виджеты: • Топ категорий • Топ сайтов • Топ заблокированных сайтов • Топ заблокированных категорий	✅	❌
Управление сервером		
Опция отправки журналов на Ideco Center	✅	❌
Обновления: • Вкладка **Система** • Выбор источника баз GeoIP	✅	❌
Перезагрузка сервера	✅	❌
Энергосберегающий режим	✅	❌

Полезные ссылки

- **Настройка высокопроизводительного контекста**
- **VCE**

Кластеризация

Функциональность доступна в **Системном контексте**.

Название службы раздела **Кластеризация**: `ideco-cluster-backend`, `ideco-cluster-backup-pusher`.

Список служб для других разделов доступен по ссылке.

Для настройки требуется активная лицензия с режимом кластеризации. Подробную информацию о лицензировании кластера можно найти в статье.

Каждое из двух устройств Ideco NGFW Novum, объединенных в кластер, называется нодой.

Кластер работает в режиме active-passive:

- **Активной** является нода, обрабатывающая трафик в данный момент.
- **Резервная** нода находится в предзагруженном состоянии и непрерывно отслеживает состояние активной ноды, а при отсутствии связи с ней переводит текущие задачи обработки трафика на себя.

При переключении нод резервная нода становится активной.

В любой момент обрабатывать трафик может только одна из нод.

Административно переключить ноды нельзя.

Если IP-адреса кластера настроены вручную, то кластер имеет один общий IP на внутреннем интерфейсе и другой общий IP на внешнем интерфейсе. В случае автоматической конфигурации по DHCP адреса будут отличаться в зависимости от ноды.

Межкластерное соединение

Сетевое взаимодействие между нодами осуществляется по одному или нескольким физическим каналам, для которых на каждой ноде резервируется один или несколько физических портов.

Для корректной работы кластера необходимо постоянное наличие связи между нодами посредством прямого сетевого соединения, без использования моста или коммутатора.

При настройке кластера доступен выбор типа соединения:

- **Ethernet** - для связи между нодами может быть настроен только один физический порт. При наличии нескольких портов для связи между нодами настроить этот тип соединения нельзя. Настроить второй порт для связи между нодами в созданном кластере с типом соединения **Ethernet** нельзя.
- **LACP** - для связи между нодами должно быть настроено несколько физических портов. При выходе из строя одного физического порта связь между нодами будет работать через другой. При этом кластер продолжит работать штатно. В кластере с типом **LACP** можно добавить порт для связи между нодами без потери связности.

VCE в кластере

При создании VCE на активной ноде:

- На резервной ноде создается VCE, который синхронизирует конфигурацию с VCE на активной ноде.
- Пользовательские сессии синхронизируются только в кластере **С синхронизацией сессий**.

При переключении нод VCE запускается с последней имеющейся конфигурацией.

При обновлении Ideco NGFW Novum с 20 версии кластеры получат тип соединения **Ethernet**.

Чтобы изменить тип кластерного соединения, нужно разрушить кластер.

Процесс синхронизации нод в кластере

- При синхронизации двух NGFW данные активной ноды копируются в резервную ноду.
- Синхронизация данных происходит автоматически в фоновом режиме.
- Автоматические бэкапы отключены на резервной ноде. Все бэкапы с активной ноды передаются на резервную в момент обмена данными и заменяют те бэкапы, которые там присутствовали ранее.

Обмен данными между нодами кластера происходит раз в минуту. Все несинхронизированные пользовательские изменения настроек и бэкапы **могут быть потеряны, если с момента внесения изменений на активной ноде до переключения нод не было обмена данными**.

Диагностика нод кластера

Проверить статус текущей ноды

Если подключение к серверу выполнено через веб-интерфейс или SSH - это активная нода.

Имя сервера можно посмотреть:

- В веб-интерфейсе - в левом верхнем углу, под именем кластера.
- В локальном меню - на стартовом экране в строке **Название сервера**.

Для проверки статуса текущей ноды используйте один из способов:

Локальное меню

На стартовом экране локального меню отображается статус ноды в строке **Состояние кластера**:

```
Название кластера:                      Без названия b42c0cae-9d59-4efa-a1ca-e635f3d45d67
Название сервера:                       Без названия b42c0cae-9d59-4efa-a1ca-e635f3d45d67
Тип кластера:                           С синхронизацией сессий
Тип соединения:                         LACP
Состояние кластера:                     Активная нода
Состояние локальных интерфейсов:        Настроены
Доступ Удаленного Помощника:            Отключено
Режим `Разрешить Интернет всем`:        Отключено
Доступ в веб-интерфейс:                 Доступен
Доступ к веб-интерфейсу из внешней сети:  Отключено

Адреса веб-интерфейса:
    https://192.168.1.10:8443
    https://192.168.101.10:8443

В случае возникновения ошибок на сервере, пожалуйста,
обратитесь в техподдержку:

Email: help@ideco.ru
Портал тех. поддержки: help.ideco.ru
Время работы тех. поддержки: ideco.ru/support


Нажмите любую клавишу для перехода к локальному меню.
Press Ctrl+R if you don't see the symbols above.
```

Команда в терминале

1. Откройте терминал одним из способов:

- В веб-интерфейсе перейдите в **Управление сервером** → **Терминал**.
- В локальном меню выберите **Консоль**.

2. Введите команду:

```
etcdctl_rt get /cluster/status/v1/record
```

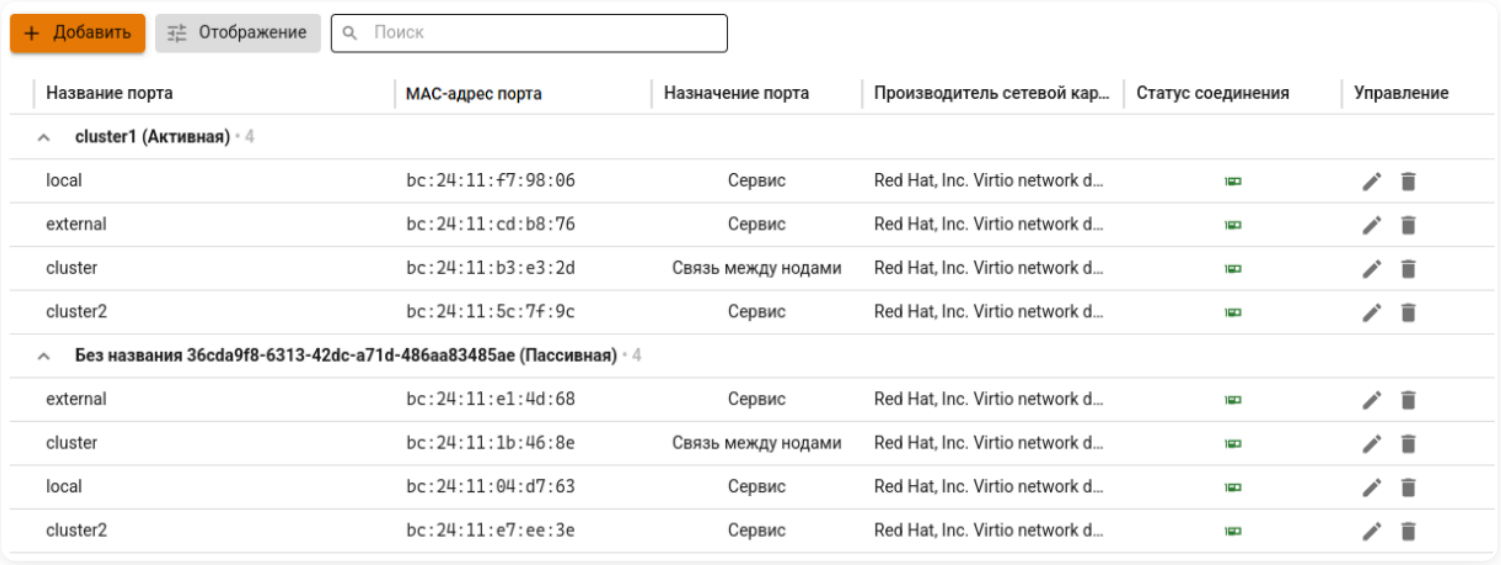
Возможные значения вывода:

- `{"state": "ACTIVE"}` - текущая нода - активная;
- `{"state": "RESERVE"}` - текущая нода - резервная. Статус не отобразится в выводе команды, так как проверка выполняется на активной ноде;
- `{"state": "NOT_CONFIGURED"}` - кластер не настроен.

Проверить состояние резервной ноды

Резервная нода доступна, если в разделе **Управление сервером** → **Кластеризация** присутствует сообщение о том, что связь с сервером установлена.

Проверить статусы физических портов резервной ноды можно в веб-интерфейсе активной ноды в таблице **Сервисы** → **Сетевые интерфейсы** → **Физические порты** в столбце **Статусы соединения**:



Проверить статусы сетевых интерфейсов и модулей резервной ноды можно, подключившись к ней по ssh (это возможно только в кластере **С синхронизацией сессий**). Для этого:

1. На активной ноде перейдите в **Управление сервером** → **Терминал**.

2. Введите команду `ideco-ssh-another-node` для подключения по ssh к резервной ноде.

3. Воспользуйтесь командами:

- `ip a` - для проверки статуса сетевых интерфесов резервной ноды.
- `systemctl status <название службы Ideco NGFW Novum>` - для проверки статуса служб Ideco NGFW Novum.

Особенности работы кластера

Особенности работы кластера с синхронизацией сессий

- При переключении на резервную ноду изменения с активной ноды применяются к бэкапам и базам данных на резервной ноде. Изменения не применяются к логам journald и мониторинга, а также аппаратным данным.
- Если активная нода теряет соединение (carrier down), переключение происходит моментально. Если нода перестает отвечать на запросы, переключение произойдет через 8 секунд.

- При переключении происходит синхронизация данных приложений с активной ноды на резервную.
- Нода, на которой есть внесенные администратором изменения, будет оставаться активной до синхронизации данных с резервной нодой.
- При отключении интерфейса локальной/внешней сети активная нода становится резервной, а резервная - активной.
- При отключении интерфейса локальной/внешней сети активной становится нода, у которой больше активных интерфейсов. Резервной - нода, у которой меньше активных интерфейсов.
- При одинаковом количестве отключенных интерфейсов на обеих нодах активной становится нода, у которой было меньше всего деградации сети (разрывов). Резервной - нода, у которой было больше всего разрывов.
- При одинаковом количестве отключенных/включенных интерфейсов на обеих нодах и одинаковом количестве разрывов сети активной становится нода, у которой больше uptime (запущена раньше). Резервной - нода, у которой uptime меньше (запущена позднее).
- При офлайн-обновлении кластера с синхронизацией сессий обновления баз **Предотвращения вторжений**, **Контент-фильтра** и **Антивирусов веб-трафика** не синхронизируются, каждая нода обновляется отдельно. Вторая нода обновится после того, как станет активной.

Особенности работы кластера без синхронизации сессий

- При переключении на резервную ноду синхронизируются все данные с диска активной ноды (синхронизация осуществляется за счет копирования файлов в файловой системе).
- При отключении интерфейса локальной/внешней сети механизм переключения нод в этом режиме кластера не предусмотрен.
- Время переключения нод - 15 секунд + загрузка резервной ноды.
- При переключении нод не синхронизируются логи мониторинга и journald, а также аппаратные данные.

Особенности работы с бэкапами при кластеризации

- Невозможно полное восстановление из бэкапов. При этом можно создать резервную копию и после разрушения кластера восстановить копию на ноде, которая была активной.
- На активной ноде доступно **Мгновенное восстановление из бэкапа**. Восстанавливаются все настройки, кроме статистики в отчетах. Данные на второй ноде также придут в соответствие с восстановленными настройками после синхронизации нод.

Особенности работы кластера в облачных сервисах

- Кластер в облаке можно поднять, только если облако поддерживает L2-связность.
- Если облако не поддерживает L2-связность, то отказоустойчивости можно достичь средствами самого облака.

Особенности работы кластера в гипервизорах

Для корректной работы кластерной сети в гипервизоре требуется дополнительная настройка сетевых адаптеров:

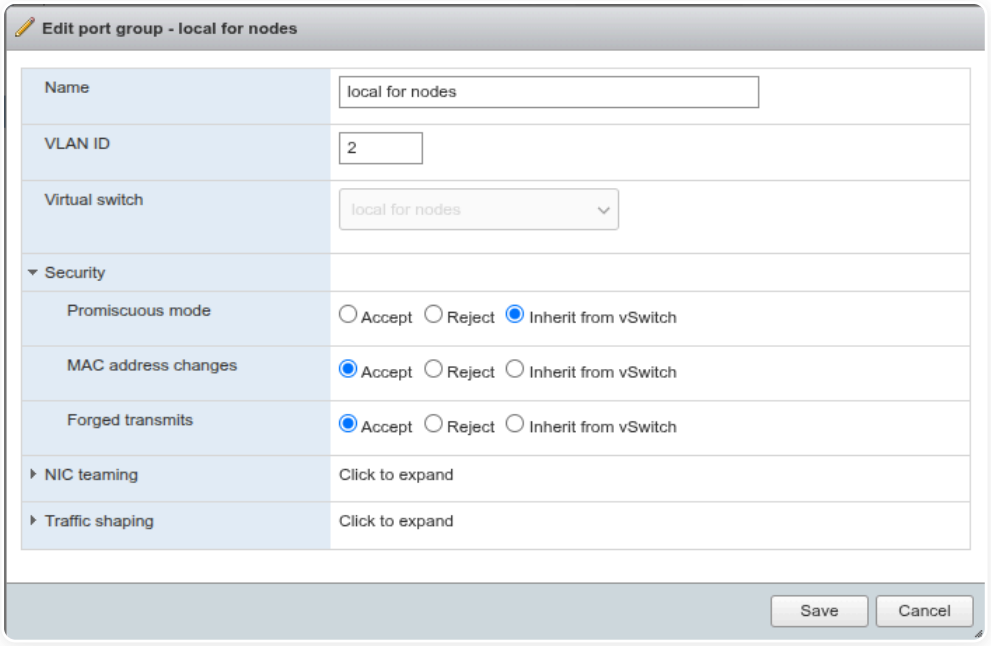
VMware ESXi:

1. В интерфейсе VMware ESXi перейдите в **Navigator** → **Networking** → **Port groups**.

2. Выберите группу портов, используемую для сети синхронизации нод, и нажмите **Edit settings**.

3. Раскройте раздел **Security**.

4. Установите значение **Accept** для двух параметров:



- **MAC address changes** - разрешает прием трафика на MAC, отличающийся от заданного в настройках ВМ.
- **Forged transmits** - разрешает отправку кадров с MAC-адресом источника, отличающимся от заданного в настройках ВМ.

5. Нажмите **Save**.

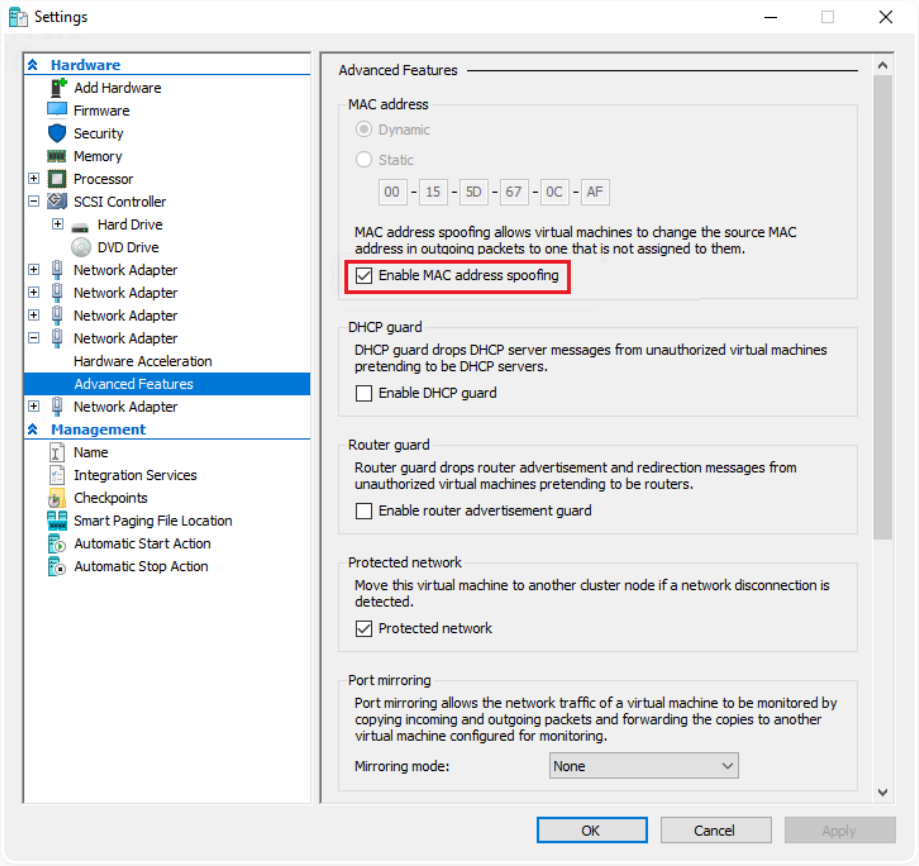
6. Перезапустите NGFW Novum.

> Для синхронизации нод кластера NGFW Novum в виртуальных средах не рекомендуется использовать LACP. Если требуется отказоустойчивость канала между ESXi-хостами, настройте LACP на стороне самих хостов и физических коммутаторов - агрегация будет работать прозрачно для NGFW Novum.

Microsoft Hyper-V:

1. Перейдите в **Hardware** → **Network Adapter** → **Advanced Features** → **MAC address**.

2. Включите опцию **Enable MAC address spoofing**:



Без этих настроек связь между нодами не будет установлена. Подробнее в статье Настройка гипервизора.

Возможные проблемы при работе двух Ideco NGFW Novum в кластере

- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.
- Два NGFW с разными версиями не синхронизируются.
- При обновлении Ideco NGFW Novum в кластере сначала обновится активная нода, затем резервная нода с младшей версией принудительно станет активной для обновления до версии активной ноды. Подробнее смотрите статью Обновление кластера.
- При различных размерах жестких дисков могут возникнуть проблемы синхронизации из-за нехватки места.
- Если у провайдера имеется привязка по MAC-адресу, то при переключении нод будет отсутствовать доступ в интернет.
- Если с момента создания бэкапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения этот бэкап будет потерян.
- Если с момента мгновенного восстановления из бэкапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения вторая нода окажется в состоянии до восстановления.

> **Кластерный режим совместим с агрегацией интерфейсов (LACP)**.

Полезные ссылки

- **Настройка кластера**
- **Обновление кластера**
- **Основные интерфейсы**
- **VCE**
- **Терминал**
- **Физические порты**
- **Предотвращение вторжений**
- **Контент-фильтр**
- **Настройка гипервизора**
- **Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG**

Настройка кластера

Функциональность доступна в **Классическом** и **Системном контекстах**.

Если на момент создания кластера у вас уже есть настроенный Ideco NGFW Novum, рекомендуем выбрать настроенный Ideco NGFW Novum в качестве активной ноды. Все настройки резервной ноды в процессе создания кластера будут удалены.

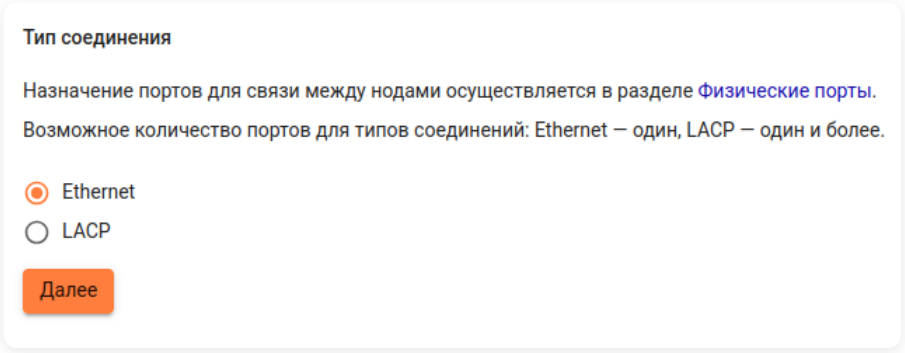
Требования

Для создания кластера необходимо соблюдение следующих требований:

- В кластере может быть только две ноды Ideco NGFW Novum.
- Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки, и один тип кластерного соединения.
- Сетевые порты для использования в кластере желательно соединять напрямую, т.к. на основе интерфейса происходит ускоренное переключение нод, поэтому не рекомендуется использовать коммутаторы для кластерной сети. Как минимум сеть должна быть изолирована.
- Для типа соединения **LACP** промежуточное оборудование (свитч между нодами) должно поддерживать LACP.
- В NGFW Novum нет возможности использовать геораспределенные ноды.
- При работе NGFW Novum в гипервизорах используйте средства отказоустойчивости гипервизора. Перед созданием кластера выполните дополнительную настройку сетевых адаптеров. Без нее связь между нодами не будет установлена. Подробнее - в разделе Особенности работы кластера в гипервизорах.

- Физические порты для связи между нодами на каждом Ideco NGFW Novum должны быть в одном сегменте локальной сети, в котором нет других устройств. Не используйте в качестве кластерной сети общедоступную сеть, используемую для передачи стороннего трафика. Обмен данными между нодами не защищен от подмены и прослушивания.
- При настройке кластеризации с использованием гипервизора убедитесь, что сетевые порты, предназначенные для связи между нодами, подключены к изолированной IPv6-сети.
- Не рекомендуем добавлять или удалять физические порты. При несовпадении количества портов на разных нодах кластер будет работать некорректно. Удаление физического порта, используемого для связи между нодами, разрушит кластер.
- Можно менять сетевые карты при редактировании физических портов в кластере, но не рекомендуется переименовывать их. При несовпадении названий портов на разных нодах кластер будет работать некорректно.

В кластере можно удалять, редактировать и создавать новые сетевые интерфейсы. Выполните действия в зависимости от **Типа соединения**:



Убедитесь, что все требования для создания кластера соблюдены:

- Если на сервере нет физических портов для связи между нодами, перейдите в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** и настройте один или несколько портов.
- Если названия и/или количество физических портов на нодах отличаются, отредактируйте порты в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** или в локальном меню сервера.

Ethernet

Ethernet - для связи между нодами может быть настроен только один физический порт. При наличии нескольких портов для связи между нодами настроить этот тип соединения нельзя.

Шаг 1 - Конфигурация резервной ноды

Конфигурация из локального меню Ideco NGFW Novum

1. В локальном меню резервной ноды выберите пункт **Физические порты** → **Показать список и отредактировать порт**:

```
Выберите порт:

-------------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------------
  1    |  eth0_d8  |  bc:24:11:48:49:d8  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  2    |  eth1_73  |  bc:24:11:84:eb:73  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  3    |  eth2_63  |  bc:24:11:de:13:63  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
```

2. Выберите физический порт, который планируете использовать для связи между нодами.

3. Введите название физического порта.

4. Оставьте прежние настройки сетевой карты.

5. Укажите режим работы порта **Для связи между нодами кластера**:

```
Текущий режим работы порта: Сервис
Выберите режим работы порта:

1. Для связи между нодами кластера
2. Сервисный порт (для построение интерфейсов на базе этого порта)

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1
Физический порт успешно обновлен.
```

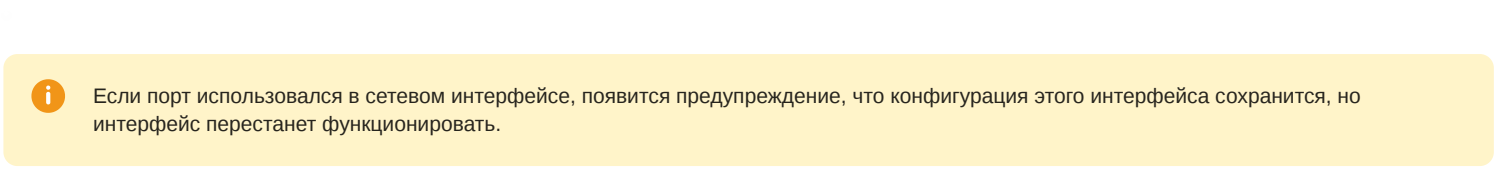
6. Перейдите в веб-интерфейс активной ноды и выполните настройки раздела **Шаг 2 - Конфигурация активной ноды**.

Конфигурация из веб-интерфейса Ideco NGFW Novum

1. Перейдите в **Сервисы** → **Сетевые интерфейсы** → **Физические порты**.

2. Выберите физический порт, который планируете использовать для связи между нодами, и нажмите  .

3. Включите опцию **Зарезервировать для связи между нодами в кластере** и нажмите **Сохранить**:



Если порт использовался в сетевом интерфейсе, появится предупреждение, что конфигурация этого интерфейса сохранится, но интерфейс перестанет функционировать.

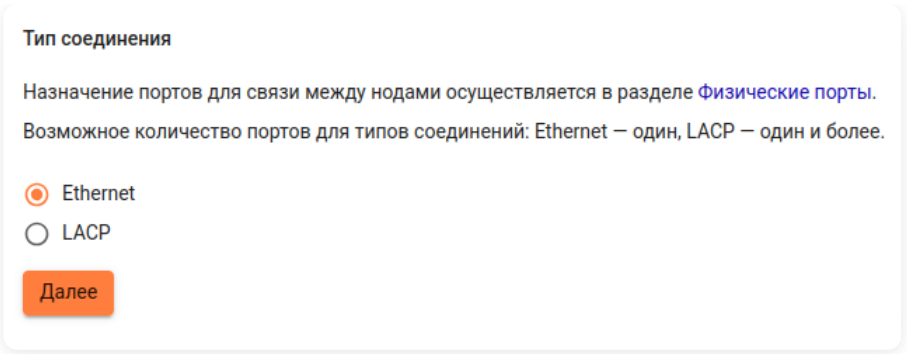
4. Перейдите в веб-интерфейс активной ноды и выполните настройки раздела **Шаг 2 - Конфигурация активной ноды**.

Шаг 2 - Конфигурация активной ноды

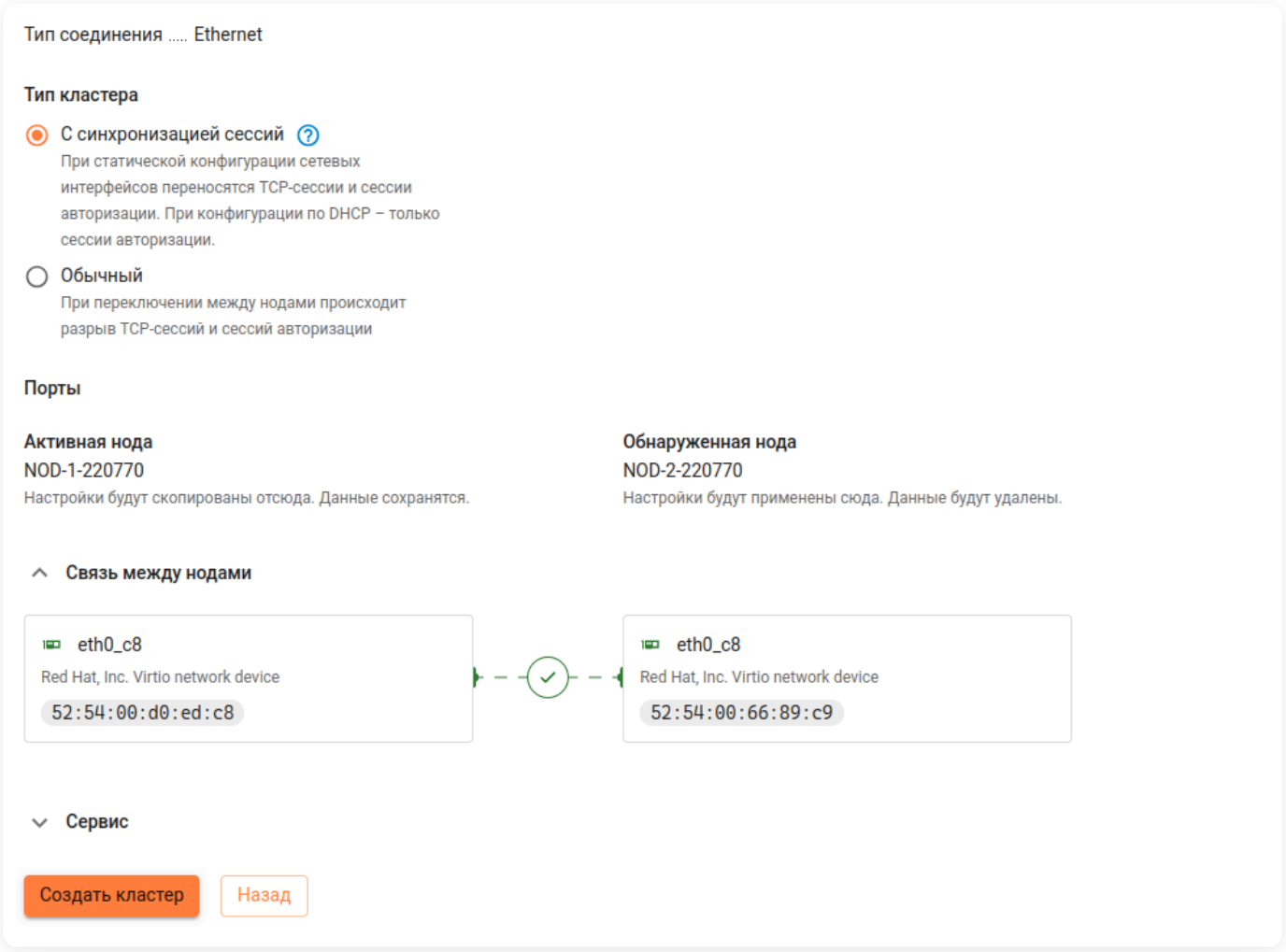
Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW Novum выполните действия:

1. Перейдите в **Управление сервером** → **Кластеризация**.

2. Выберите тип кластерного соединения **Ethernet** и нажмите **Далее**:



3. Выберите тип кластера и нажмите **Создать кластер**. Сетевые порты нод будут сопоставлены автоматически:



LACP

LACP - для связи между нодами должно быть настроено несколько физических портов. При выходе из строя одного физического порта связь между нодами будет работать через другой. При этом кластер продолжит работать штатно.

При создании LACP-интерфейса между нодами кластера достаточно указать один физический порт - система автоматически создаст канал между одноименными портами обеих нод. Например, если в кластере есть порт `client`, созданный LACP-интерфейс объединит `client` с первой ноды и `client` со второй ноды. Подробнее о создании LACP-интерфейса - в статье.

Шаг 1 - Конфигурация резервной ноды

Конфигурация из локального меню Ideco NGFW Novum

1. Выберите пункт **Физические порты** → **Показать список и отредактировать порт**:

```
Выберите порт:

-------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------
  1    |  eth0_d8  |  bc:24:11:48:49:d8  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------
  2    |  eth1_73  |  bc:24:11:84:eb:73  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------
  3    |  eth2_63  |  bc:24:11:de:13:63  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------
```

2. Выберите физический порт, который планируете использовать для связи между нодами.

3. Введите имя физического порта.

4. Оставьте прежние настройки сетевой карты.

5. Укажите режим работы порта **Для связи между нодами кластера**:

```
Текущий режим работы порта: Сервис
Выберите режим работы порта:

1. Для связи между нодами кластера
2. Сервисный порт (для построение интерфейсов на базе этого порта)

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1
Физический порт успешно обновлен.
```

6. В локальном меню резервной ноды выберите пункт **Выбор типа кластерной сети** и режим **LACP**:

```
Управление сервером

1. Консоль
2. Физические порты
3. Ethernet-интерфейсы
4. LACP-интерфейсы
5. VLAN-интерфейсы
6. Отключить все статические маршруты и добавить новый
7. Выбор типа кластерной сети
8. Включить доступ к веб-интерфейсу из внешней сети
9. Включить доступ к серверу по SSH из Интернет
10. Включить доступ к серверу по SSH из локальных сетей
11. Включить режим `Разрешить Интернет всем`
12. Сбросить блокировки по IP
13. Отключить пользовательский межсетевой экран
14. Создать новый бэкап
15. Восстановить из бэкапа
16. Мгновенно восстановить из бэкапа
17. Включить доступ Удаленного Помощника
18. Контакты технической поддержки
19. 2FA администраторов
20. Восстановиться на предыдущую версию
21. Перезагрузка сервера
22. Отключить сервер
23. Сменить пароль
24. Выход

Введите номер пункта и нажмите Enter.
# 7

1. Ethernet
2. LACP

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 2
```

7. Повторите пункты 1-5 для другого порта.

8. Перейдите в веб-интерфейс активной ноды и выполните настройки раздела **Шаг 2 - Конфигурация активной ноды**.

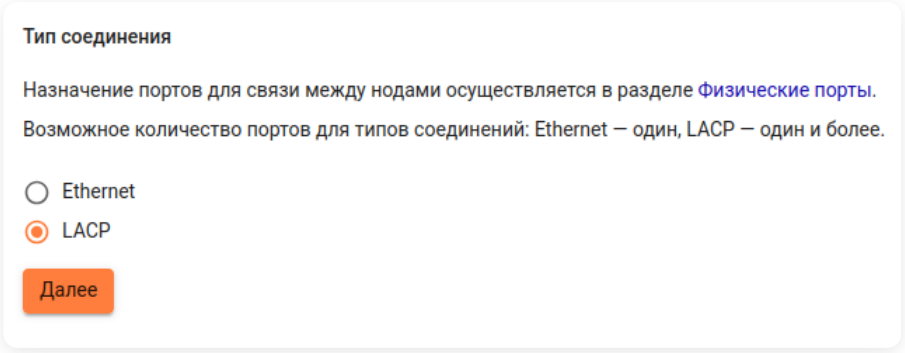
Конфигурация из веб-интерфейса Ideco NGFW Novum

1. Перейдите в **Сервисы → Сетевые интерфейсы → Физические порты**.

2. Выберите физический порт, который планируете использовать для связи между нодами, и нажмите  .

3. Включите опцию **Зарезервировать для связи между нодами в кластере** и нажмите **Сохранить**:

4. Перейдите в **Управление сервером** → **Кластеризация** и выберите тип кластерного соединения - **LACP**:



5. Нажмите **Далее** - тип кластерного соединения будет сохранен.

6. Вернитесь в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** и повторите действия из пункта 2-3 для другого порта.

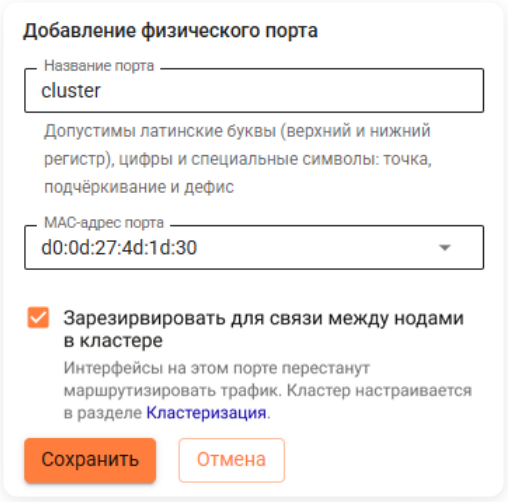
Шаг 2 - Конфигурация активной ноды

Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW Novum выполните действия:

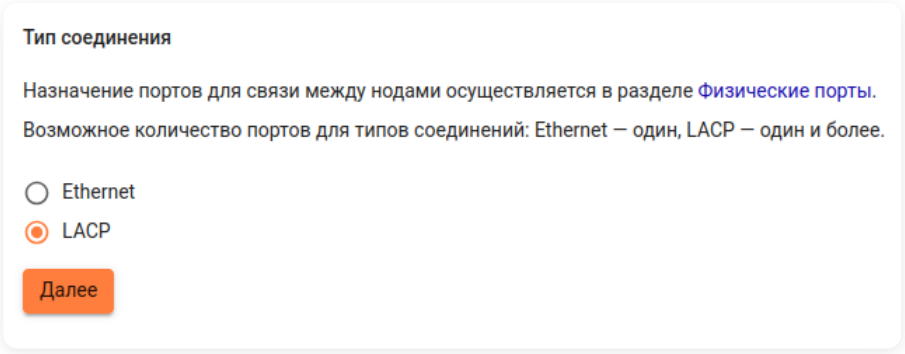
1. Перейдите в **Сервисы** → **Сетевые интерфейсы** → **Физические порты**.

2. Выберите физический порт, который планируете использовать для связи между нодами, и нажмите .

3. Включите опцию **Зарезервировать для связи между нодами в кластере** и нажмите **Сохранить**:



4. Перейдите в **Управление сервером** → **Кластеризация** и выберите тип кластерного соединения - **LACP**:

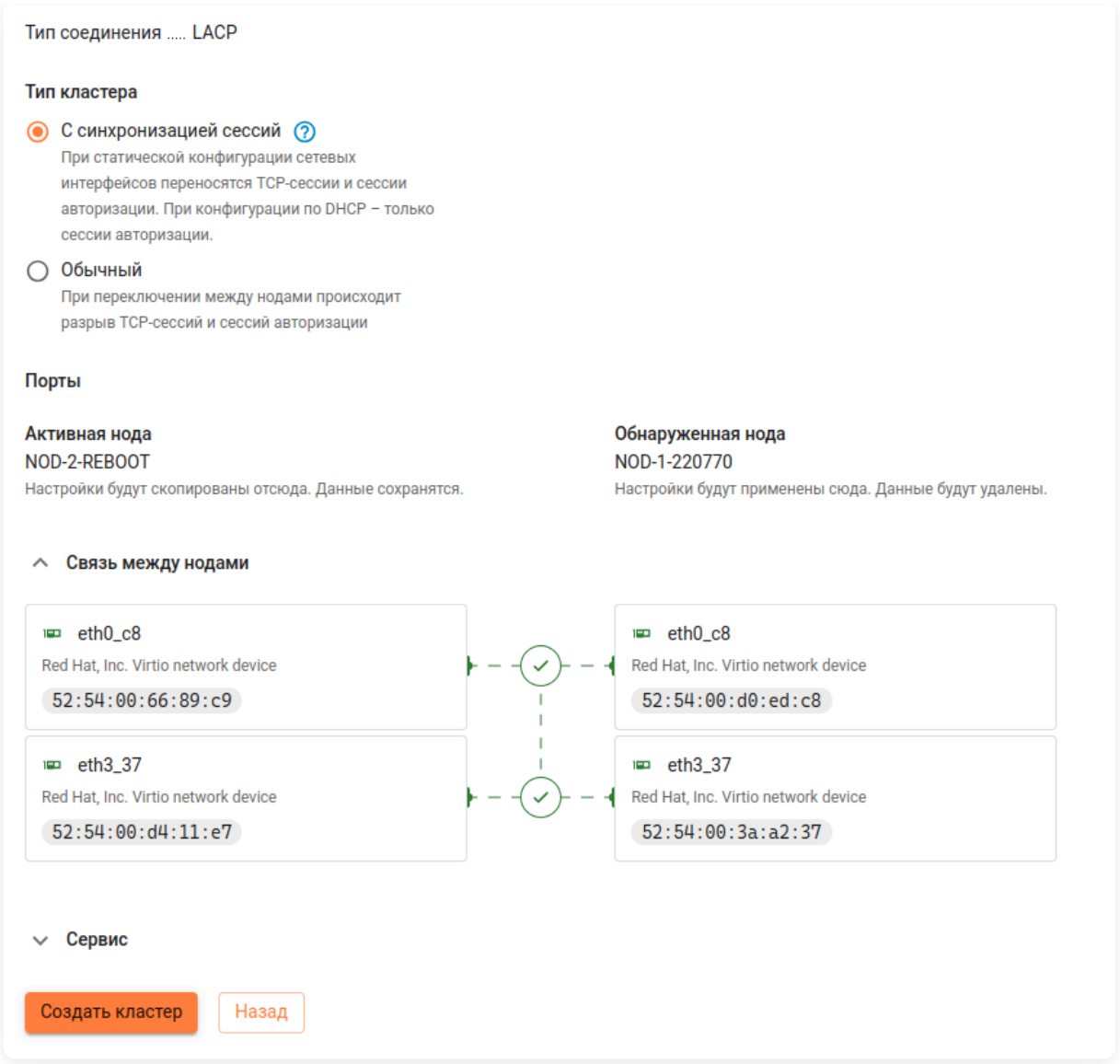


5. Нажмите **Далее** - тип кластерного соединения будет сохранен.

6. Вернитесь в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** и повторите действия из пункта 2-3 для другого порта.

7. Перейдите в **Управление сервером** → **Кластеризация** и нажмите **Далее**.

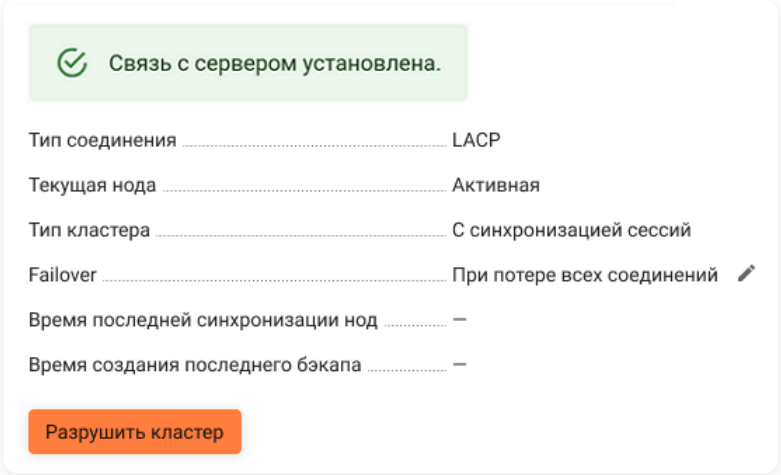
8. Выберите тип кластера и нажмите **Создать кластер**. Сетевые порты нод будут сопоставлены автоматически:



Если был настроен **Обычный** тип кластера, то при переключении между нодами происходит разрыв TCP-сессий пользователей и сессий авторизации.

Если был настроен тип кластера **С синхронизацией сессий**, то при статической конфигурации сетевых интерфейсов все TCP-сессии пользователей и сессии авторизации перенесутся на резервную ноду. При конфигурации по DHCP - перенесутся только сессии авторизации.

После применения настроек резервная нода перезагрузится, и в веб-интерфейсе активной ноды отобразится информация, что кластер создан:



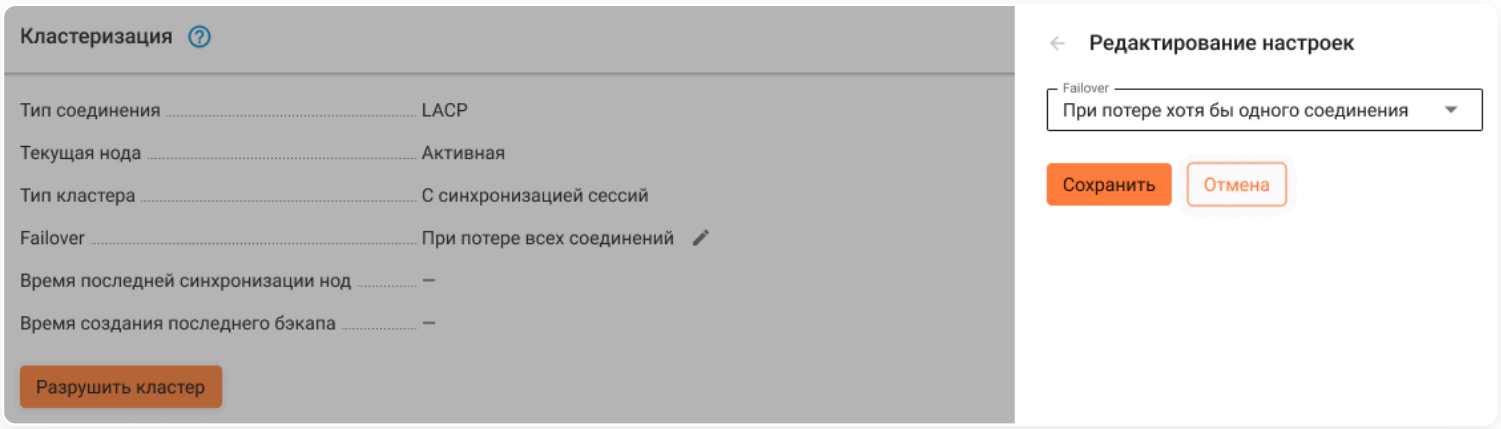
Во время перезагрузки резервной ноды в веб-интерфейсе активной ноды может временно отображаться статус о потере связи. Соединение восстановится автоматически после завершения загрузки резервной ноды.

Локальное меню резервной ноды доступно только в кластере **С синхронизацией сессий**.

В кластере **С синхронизацией сессий** доступна настройка **Failover**, которая определяет условие переключения на резервную ноду:

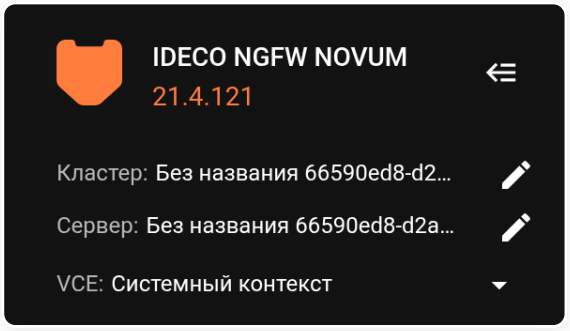
- При потере хотя бы одного соединения.
- При потере всех соединений.

По умолчанию установлено значение **При потере всех соединений**. Чтобы изменить значение, нажмите и отредактируйте настройку:



Изменение названия кластера и сервера

Название кластера или сервера можно изменить через веб-интерфейс активной ноды. Для этого нажмите на рядом с названием кластера или сервера в левом верхнем углу экрана:



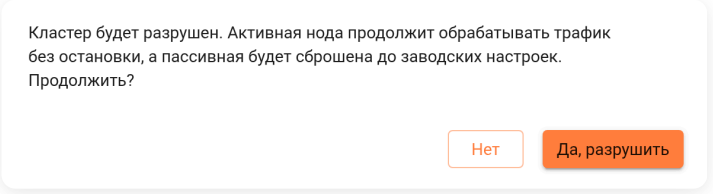
Разрушение кластера

Разрушить кластер можно только из активной ноды. При этом нода продолжит работать, а вторая нода (резервная) сбросит настройки до состояния только что установленного Ideco NGFW Novum. Для разрушения кластера:

В Веб-интерфейсе

1. Перейдите в **Управление сервером** → **Кластеризация** и нажмите кнопку **Разрушить кластер**.

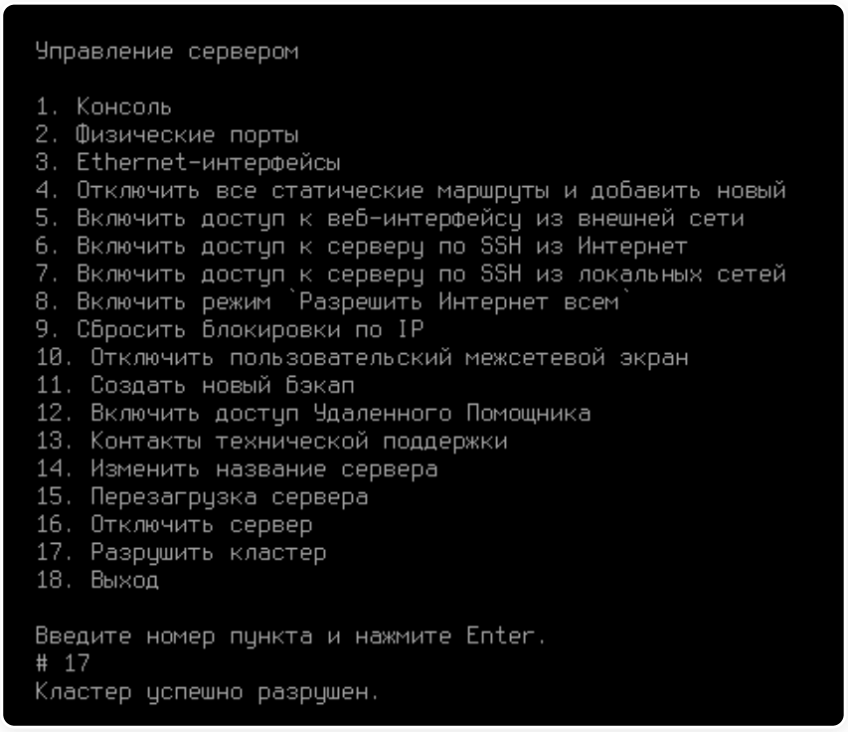
2. Появится окно с предупреждением:



3. Нажмите **Да, разрушить**.

В Локальном меню

В локальном меню резервной ноды выберите пункт **Разрушить кластер**:



Обновление кластера

Функциональность доступна в **Классическом** и **Системном контекстах**.

Процесс обновления Ideco NGFW Novum описан в статье **Обновления**.

Убедитесь в наличии лицензии на кластер.

Чтобы обновить NGFW до последней версии в режиме кластера, выполните действия:

1. Запустите обновление активной (первой) ноды в **Управление сервером** → **Обновление**. Сработает алгоритм обновления кластера Ideco NGFW Novum:

- Активная нода проверит время последней синхронизации и наличие лицензии на кластер.
- Если условия выполнены, активная нода установит обновление, перезагрузится и станет резервной.
- Вторая нода станет активной принудительно, скачает и установит обновления в автоматическом режиме.

Обновление активной ноды кластера будет заблокировано, если нода не синхронизирована с резервной нодой или с момента последней синхронизации прошло более 30 минут. Нода с младшей версией сможет обновиться без синхронизации. Это позволяет минимизировать потерю данных.

Для синхронизации оба устройства должны иметь одну версию системы, идентичную вплоть до номера сборки.

2. Дождитесь, пока вторая нода скачает и установит обновление. После завершения обновления кластер вновь будет работоспособен.

Обновления

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Обновления**: `ideco-sysupdate-backend`.

Список служб для других разделов доступен по ссылке.

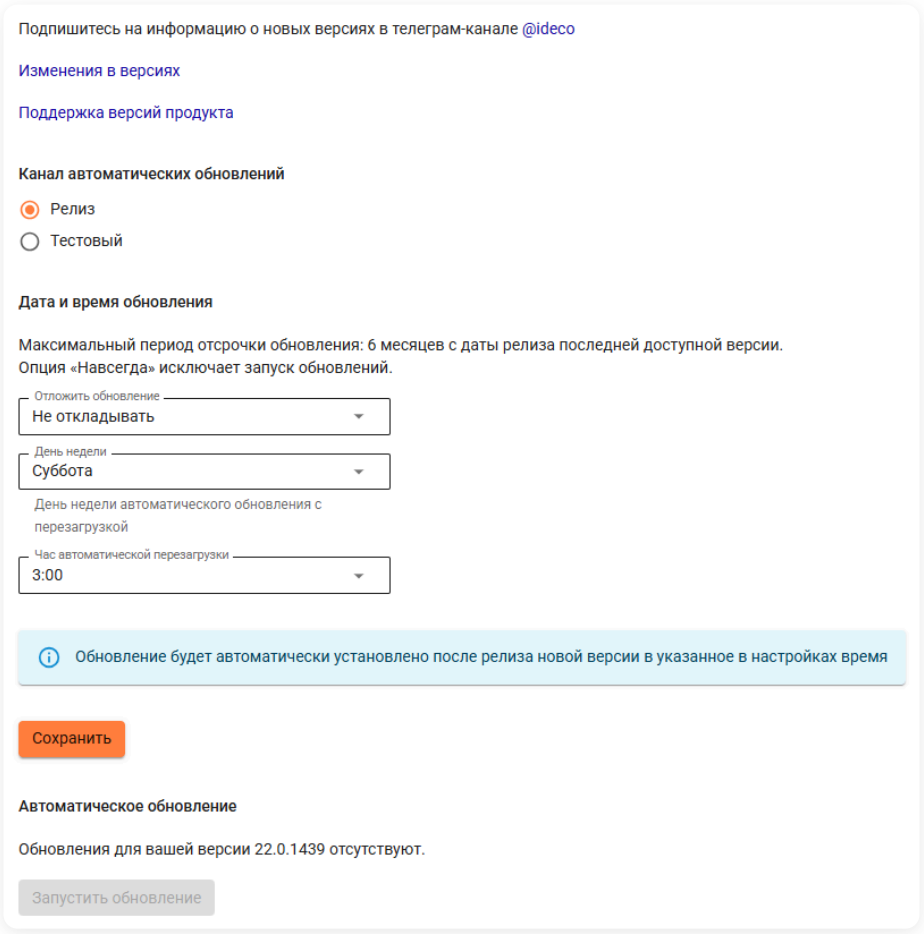
Система

Механизм обновления с версий Ideco UTM 7.9.9 - 14 описан в инструкции.

Обновить систему Ideco NGFW Novum можно как в офлайн-режиме, так и через интернет. Выбрать режим обновления можно в разделе **Управление сервером → Лицензия**.

Автоматическое обновление

Доступны настройки:



Расшифровка полей

- **Канал обновлений**:
  - **Релиз** - позволяет обновляться на стабильно работающие версии. Выбран по умолчанию.

    - **Тестовый** - позволяет быстрее обновляться как на релизные версии, так и на последние бета-версии продукта во время коротких периодов бета-тестирования новых мажорных версий.
- **Отложить обновления** - время, на которое будет отложено обновление. Максимальный срок - шесть месяцев с даты релиза последней версии, до которой доступно обновление.
- **День недели** - день недели запуска автоматического обновления.
- **Час автоматической перезагрузки** - час запуска автоматического обновления.
- **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

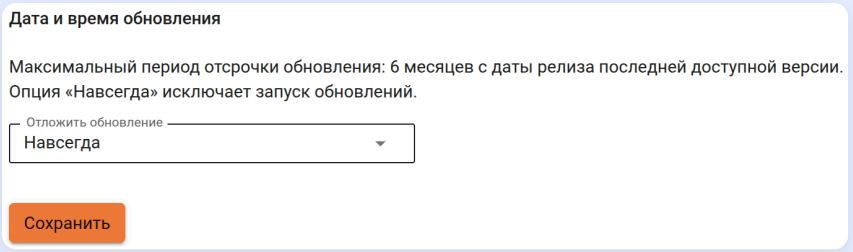
Кнопка **Запустить обновление** активна и только применяет обновление, когда оно уже скачано. Инициировать скачивание нельзя.

После принудительного обновления потребуется полная перезагрузка сервера.

По умолчанию сервер обновляется по субботам в 3:00 по часовому поясу, выбранному в настройках.

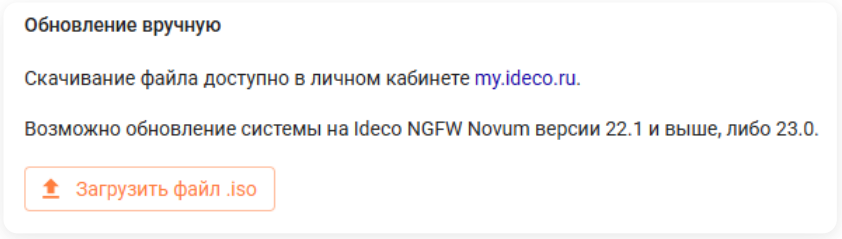
Обновление вручную

Чтобы обновлять Ideco NGFW Novum только вручную, в поле **Отложить обновление** выберите **Навсегда**:



Не рекомендуем отключать обновления, так как это приведет к пропуску важных улучшений и критических исправлений безопасности. Если автоматическое обновление отключено, регулярно проверяйте наличие новых версий.

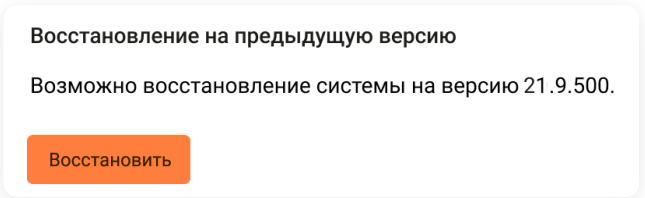
Для обновления необходимо скачать ISO-образ новой версии Ideco NGFW Novum в MY.IDECO и загрузить образ с внешнего носителя:



После проведения процедуры обновления новая версия будет отображаться в верхнем левом углу веб-интерфейса NGFW Novum.

Для обновления серверов Ideco NGFW Novum, подключенных к Ideco Center, перейдите в интерфейс NGFW Novum одним из способов, указанных в разделе Ideco Center.

Восстановление на предыдущую версию



Кнопка **Восстановить** позволяет вернуться к предыдущей версии NGFW Novum. Система будет перезагружена, при этом текущие настройки будут потеряны. После восстановления отложите автоматическое обновление.

При восстановлении системы все настроенные VCE с данными также откатятся к исходному состоянию.

Если в **Ideco NGFW Novum** настроен кластер, то в веб-интерфейсе будет отсутствовать пункт **Восстановление на предыдущую версию**.

При восстановлении на предыдущую версию данные перенесены не будут. NGFW Novum вернется в состояние, в котором был на момент обновления. Все изменения, внесенные после обновления, будут утеряны. Сохраните информацию на внешнем носителе, NGFW предоставляет возможность выгружать бэкапы на:

- Сетевое файловое хранилище по протоколу FTP.
- Сетевое файловое хранилище по протоколу NetBIOS (CIFS).
- ПК через кнопку **Скачать** в таблице бэкапов ( ) для переноса с сервера на иной внешний носитель вручную.

Бэкап можно восстановить только на версию NGFW Novum не ниже той, на которой был создан.

Процесс выхода релизов в каналы обновлений

Тестовый канал обновлений позволяет быстрее обновляться до новых версий (релизных или бета-версий во время активного тестирования). После выхода бета-версии NGFW Novum в **Тестовый** канал ожидается обратная связь от пользователей по использованию новой версии продукта. Обратная связь позволяет выявить недочеты и уязвимости в продукте. После исправления происходит выкладка в канал **Релиз**.

Если в версии NGFW Novum, вышедшей в канал **Релиз**, в ходе использования выявляются недочеты, то исправляются ближайшими обновлениями версии. Обновление в канале **Релиз** появляется постепенно.

Особенности обновления

NGFW Novum

- Обновление будет автоматически установлено в указанное в настройках время после релиза новой версии.
- Обновления можно отложить на срок до шести месяцев или навсегда. Если отложить обновление на определенный срок, то период будет отсчитываться от **даты релиза** последнего доступного обновления и корректироваться в соответствии с указанным для обновления днем недели.
- Даты релизов можно посмотреть на сайте или в документации в разделе Release notes.
- Номер мажорной версии NGFW Novum - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7).
- Автоматическое обновление Ideco NGFW Novum до следующей мажорной версии возможно только после установки последней минорной версии, выпущенной в релиз. Например, можно обновить NGFW Novum 17.2 до версии 17.9, а затем до версии 18.6.
- Ручное обновление Ideco NGFW Novum до следующей мажорной версии можно выполнить с любой версии. Например, можно обновить NGFW Novum 17.2 до версии 18.5.

Если обновление было отложено на шесть месяцев, но за это время вышел новый минорный релиз, дата обновления сдвигается. Шесть месяцев отсчитываются с даты выхода последнего доступного минорного релиза.

VCE

- При обновлении корневого NGFW Novum все включенные VCE автоматически обновляются вместе с корневым NGFW Novum.
- Если в системе есть выключенные VCE, которые созданы в младшей версии корневого NGFW Novum и не запускались после обновления, то обновление корневого NGFW Novum на следующую мажорную версию будет заблокировано.

Пример. Если в NGFW Novum версии 18.3 создали VCE, затем выключили его и обновили корневой NGFW Novum до 19.0, но сам VCE на 19.0 не включали, то переход с 19.0 на 20.0 будет заблокирован.

Включите все VCE для автоматического обновления до версии корневого NGFW Novum.

- Если VCE не включался после обновления корневого NGFW Novum, то:
  - VCE останется на предыдущей версии.
  - Корневой NGFW Novum можно обновить в рамках текущей мажорной версии.

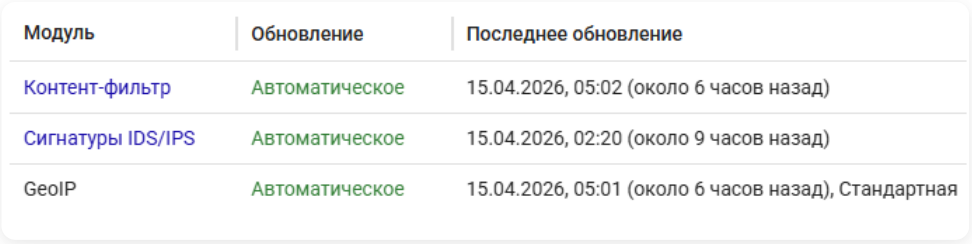
Пример. Корневой NGFW Novum можно обновить с 18.3 до 18.6, но выключенный VCE останется на 18.3.

Кластер

- Если активная нода кластера не синхронизирована с резервной или с момента последней синхронизации прошло более 30 минут, ее обновления будут заблокированы. Произойдет переключение нод кластера. Нода с младшей версией сможет обновиться без синхронизации.
- При офлайн-обновлении кластера с синхронизацией сессий обновления баз **Предотвращения вторжений**, **Контент-фильтра** и **Антивирусов веб-трафика** не синхронизируются, каждая нода обновляется отдельно. Вторая нода обновится после того, как станет активной.

Базы фильтрации

На вкладке **Базы фильтрации** отображается информация о последнем обновлении баз модулей фильтрации Ideco NGFW Novum: **Контент-фильтра**, **Предотвращения вторжений**, а также GeoIP (соответствия подсетей и стран):



Модуль	Обновление	Последнее обновление
Контент-фильтр	Автоматическое	15.04.2026, 05:02 (около 6 часов назад)
Сигнатуры IDS/IPS	Автоматическое	15.04.2026, 02:20 (около 9 часов назад)
GeoIP	Автоматическое	15.04.2026, 05:01 (около 6 часов назад), Стандартная

Обновить базы фильтрации Ideco NGFW Novum можно как в офлайн-режиме, так и по сети. Выбрать режим обновления можно в разделе **Управление сервером** → **Лицензия**.

Изменение источника баз GeoIP доступно только в **Системном контексте**.

Автоматическое обновление

1. В режиме **Автоматического обновления** выберите источник обновления баз GeoIP:

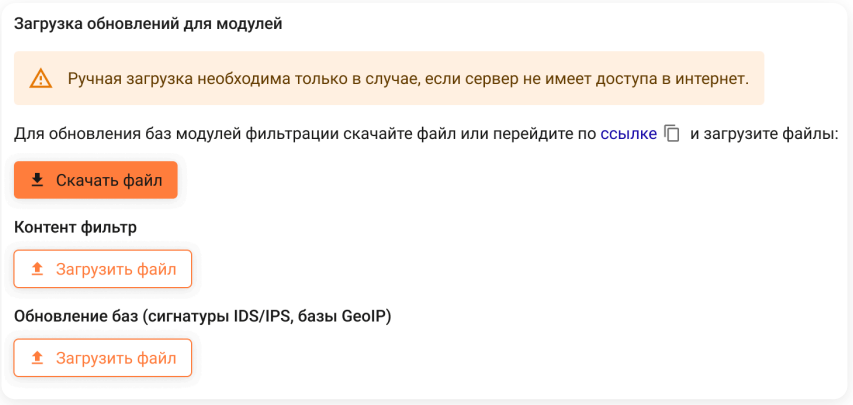


- **Стандартная** - международная база данных для определения геолокации по IP-адресам. Используется по умолчанию.
- **Минцифры** - база данных для определения стран, разработанная Министерством цифрового развития РФ.

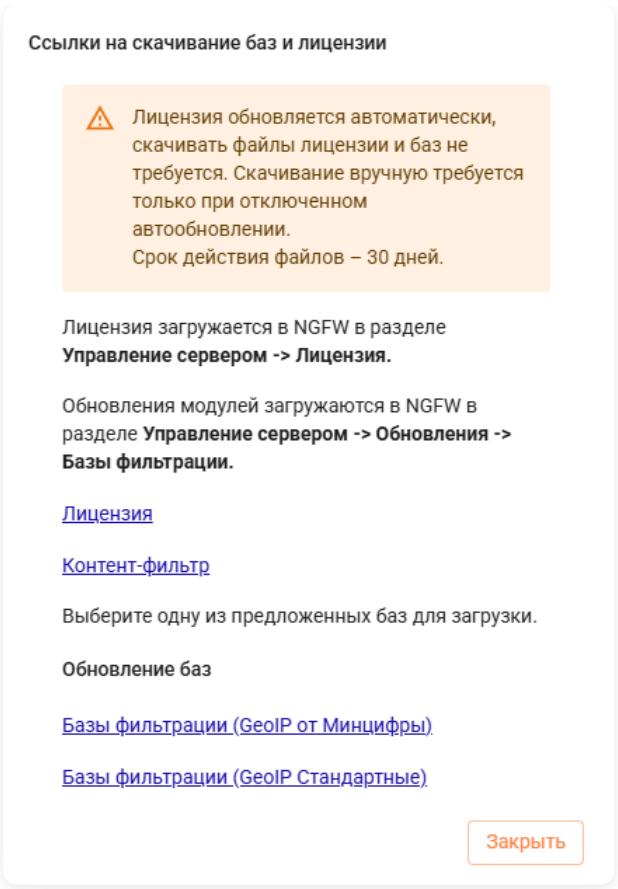
2. Нажмите **Сохранить**.

Изменения источника вступят в силу после подгрузки выбранной базы, источник отобразится в сведениях об обновлении в строке **GeoIP**.

В автоматическом режиме также доступно скачивание файлов для ручного обновления:



При переходе к скачиванию отобразится уведомление:



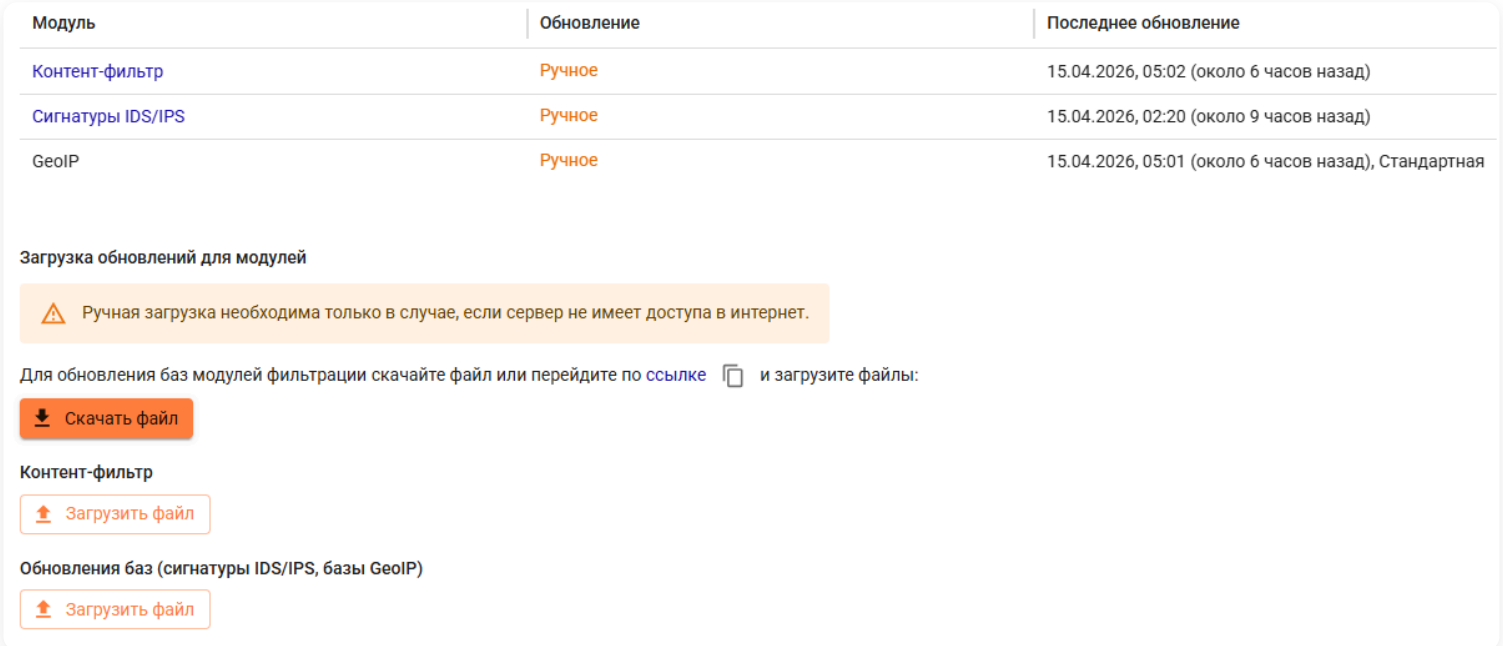
Ручное обновление

Базы фильтрации Ideco NGFW Novum могут меняться ежедневно, поэтому при ручной загрузке обновляйте базы как можно чаще.

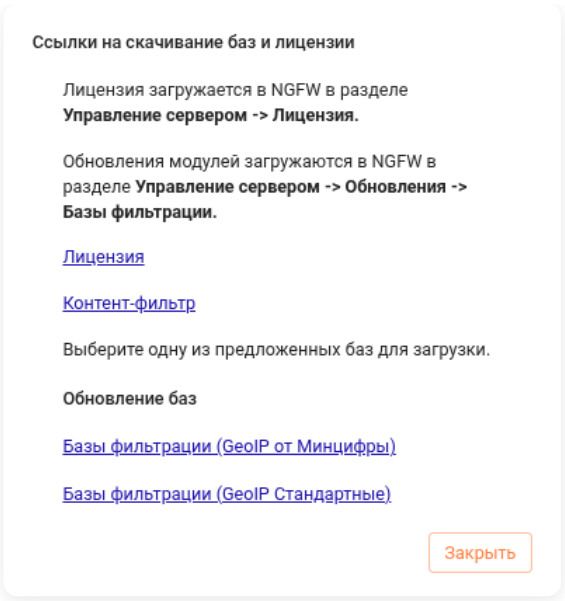
Ручная загрузка необходима только в случае, если сервер не имеет доступа в интернет, а в разделе **Управление сервером** → **Лицензия** выбран способ обновления **Ручная загрузка**.

Для загрузки файлов обновления баз на Ideco NGFW Novum выполните действия:

1. В интерфейсе Ideco NGFW Novum на вкладке **Управление сервером** → **Обновления** → **Базы фильтрации** скачайте файл или перейдите по ссылке:



2. Скачайте и загрузите файлы:



Если при скачивании Обновления баз (Предотвращение вторжений, базы GeoIP) через **Google Chrome** возникают проблемы, в настройках браузера разрешите **Небезопасный контент** для MY.IDECO.

Полезные ссылки

- **Источники данных**

Как восстановиться на прошлую версию после обновления Ideco NGFW Novum

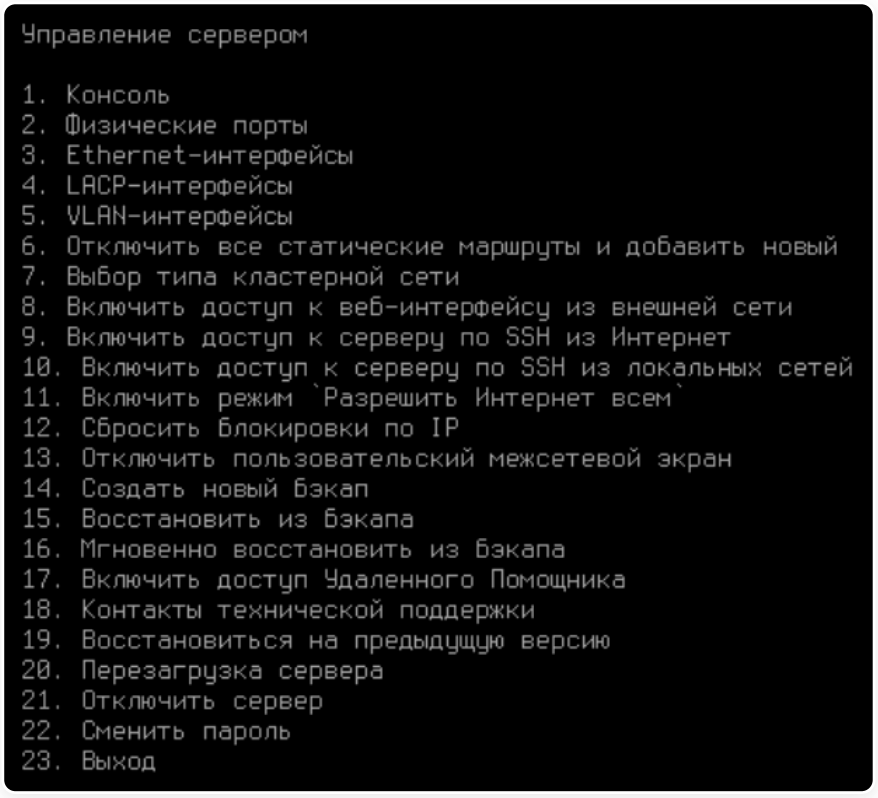
При восстановлении на предыдущую версию данные перенесены не будут. Сохраните бэкап на внешнем носителе. Информация о работе с API бэкапа описана в статье Бэкап.

Для восстановления на предыдущую версию выполните действия:

1. Перейдите в локальное меню Ideco NGFW Novum.

2. Введите логин и пароль администратора.

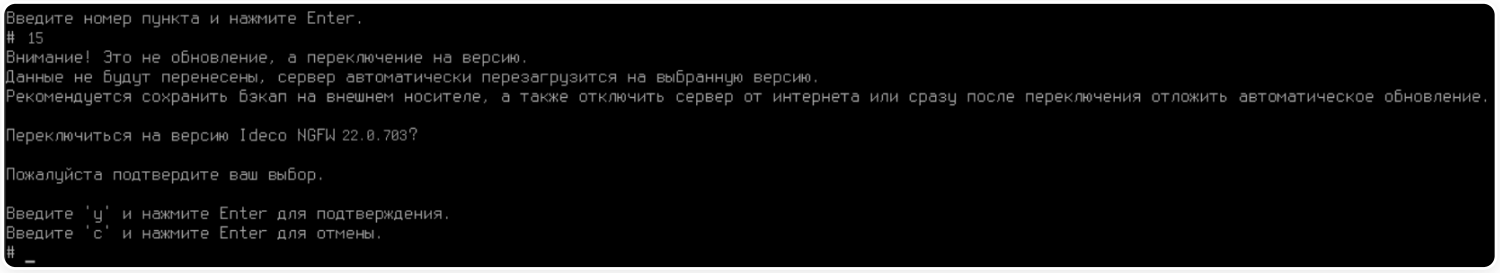
3. Укажите номер пункта **Восстановиться на предыдущую версию** и нажмите Enter:



Появится окно с предупреждением и описанием версии, на которую произойдет переключение.

> Если в Ideco NGFW Novum настроен кластер, то в локальном меню будет отсутствовать пункт **Восстановиться на предыдущую версию**.

3. Подтвердите выбор, введя y и нажав Enter:



4. После перезагрузки Ideco NGFW Novum переключится на предыдущую версию.

Бэкапы

Классический контекст | Высокопроизводительный контекст | API

Название служб раздела **Бэкапы**: `ideco-backup-backend`, `ideco-backup-create`, `ideco-backup-restore`, `ideco-backup-rotate`.

Список служб для других разделов доступен по ссылке.

Бэкап - это предварительно созданная резервная копия данных, позволяющая восстановить большинство настроек и сохраненной информации.

В NGFW Novum создается только полный бэкап, который включает все настройки, созданные администратором в веб-интерфейсе.

Бэкапы не включают:

- Системный журнал.
- Почту.
- Статистику web-трафика и другие отчеты.
- Любые кешируемые данные, базы антивирусов, правила IPS и т. п.
- Настройки созданных VCE.
- Любые данные, генерируемые в процессе работы системы автоматически.

В бэкап системного VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте отдельный бэкап системного VCE и каждого из дочерних VCE.

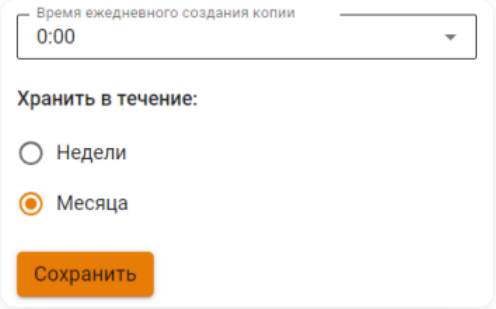
В NGFW Novum бэкап создается как автоматически, так и вручную.

Не рекомендуем использовать один и тот же бэкап для клонирования серверов. Это приведет к конфликту идентификаторов серверов и проблемам с подключением к Ideco Center, интеграцией с внешними системами (например, Active Directory, ALD), корректностью отчетности и т.д.

Интеграция с AD, ALD может перестать работать, если вы производите откат на предыдущую версию или разворачиваете старый бэкап, в котором присутствует устаревшая информация для аутентификации NGFW Novum на контроллере домена. При каждом изменении настроек интеграции информация для аутентификации NGFW Novum обновляется. Для решения проблемы интеграции NGFW Novum с AD, ALD сделайте переинтеграцию NGFW Novum с соответствующим сервисом.

Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в **Управление сервером** → **Бэкапы** → **Настройки**:



Установите время ежедневного создания и продолжительность хранения бэкапа на локальном жестком диске. При настройке выгрузки на сетевое файловое хранилище автоматический бэкап будет также дублироваться туда.

- **Время ежедневного создания копии** - укажите в настройках час. Рекомендуется выбирать ночное время для создания бэкапа.
- **Хранить в течение** - выберите срок хранения. Хранить бэкапы на локальном жестком диске можно в течение недели или месяца.

> Каждый автоматически созданный бэкап сохраняется в таблице бэкапов с комментарием **Автоматическая резервная копия**.

Рекомендуется хранить бэкапы не только на локальном жестком диске, но и на внешних носителях. NGFW Novum предоставляет возможность выгружать бэкапы на:

- Сетевое файловое хранилище по протоколу FTP.
- Сетевое файловое хранилище по протоколу NetBIOS (CIFS).
- ПК через кнопку **Скачать** в таблице бэкапов для переноса с сервера на иной внешний носитель вручную.

Для проверки корректности настройки сохранения бэкапов на FTP-сервере или в общей папке CIFS введите команду `ideco-backup-create` в терминале Ideco NGFW Novum. Команда создает автоматический бэкап в соответствии с заданными настройками сохранения.

> При настройке бэкапов указывайте путь к каталогу в UNIX-формате. Например, если в ОС Windows каталог открывается по пути `\\192.168.1.1\dir_1\dir_2\backup`, то в поле **Путь к каталогу** пропишите `dir_1/dir_2/backup`.

Бэкапы на удаленное файловое хранилище по протоколу FTP

Ключевые параметры, необходимые для настройки бэкапа на FTP-сервер, описаны в таблице:

Параметр	Описание
Адрес сервера	IP-адрес удаленного FTP-сервера, на котором будут размещаться бэкапы
Логин	Имя пользователя для авторизации на FTP-сервере
Пароль	Пароль для авторизации на FTP-сервере
Путь к каталогу	Каталог, в который будут записываться бэкапы

Бэкапы на сетевое файловое хранилище по протоколу NetBIOS (CIFS)

Ключевые параметры, необходимые для настройки бэкапа на NetBIOS-сервер, описаны в таблице:

Параметр	Описание
Адрес сервера	IP-адрес удаленного NetBIOS-сервера, на котором будут размещаться бэкапы
Логин	Имя пользователя для авторизации на сетевом ресурсе Windows
Пароль	Пароль для авторизации на сетевом ресурсе Windows
Путь к каталогу	Каталог, в который будут записываться бэкапы

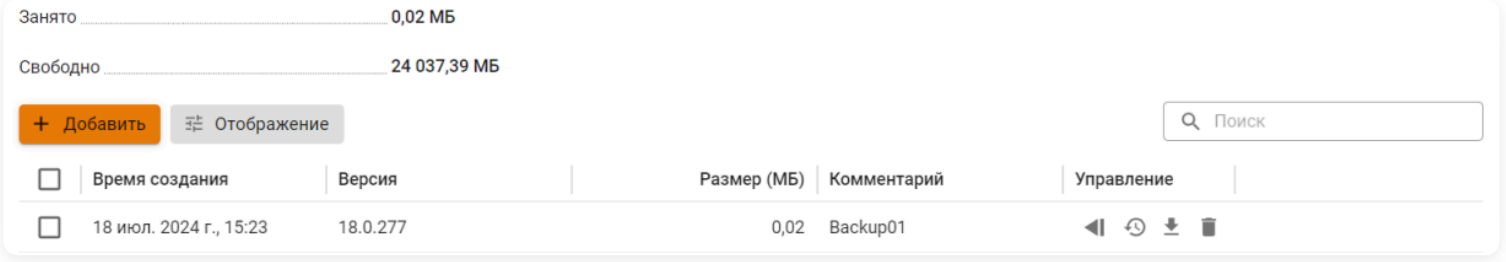
Ручное создание бэкапа

Через веб-интерфейс

Для создания бэкапа через интерфейс Ideco NGFW Novum выполните одно из действий:

- Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и нажмите **Добавить** → **Создать**.
- Нажмите **Создать бэкап** в правом верхнем углу веб-интерфейса.

Введите комментарий или оставьте поле пустым, нажмите **Создать**. Новый бэкап появится в таблице:



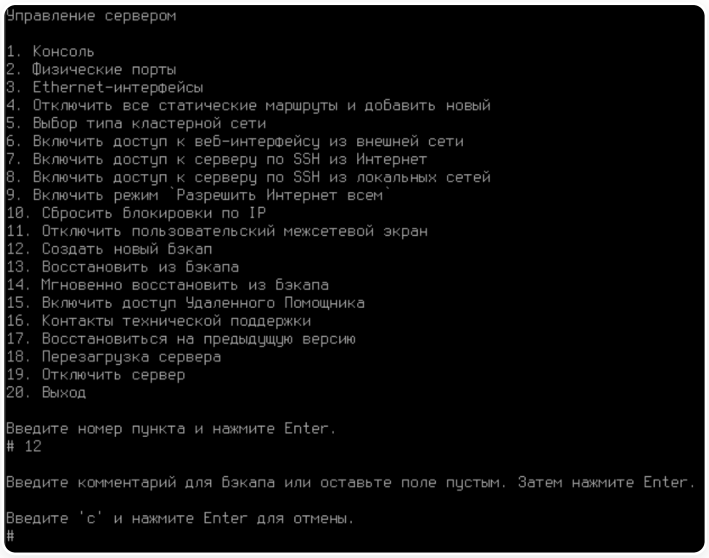
Через локальное меню

Чтобы создать новый бэкап через локальное меню Ideco NGFW Novum, выполните действия:

1. Выберите пункт **Создать новый бэкап** и нажмите **Enter**.

2. Введите комментарий для бэкапа и нажмите **Enter**.

Пример создания бэкапа через локальное меню приведен на скриншоте ниже:



Настройка сохранения бэкапа в сетевом файловом хранилище возможна только через веб-интерфейс Ideco NGFW Novum. Выгрузка на внешние сетевые хранилища производится только при автоматическом создании бэкапа.

Полезные ссылки

- **Восстановление конфигурации из бэкапа**

Терминал

Классический контекст | Высокопроизводительный контекст

Используйте терминал только для диагностики. Воздержитесь от команд, изменяющих файлы. Система рассчитана на настройку только через веб-интерфейс. Компания "Айдеко" не несет ответственности за негативные последствия работы с Ideco NGFW из терминала. Техническая поддержка вправе отказать в обслуживании, если окажется, что работа системы была нарушена из-за действий пользователя в терминале.

Основные команды

- **Утилиты сетевой диагностики:** `ping`, `host`, `nslookup`, `tracepath`, `tcpdump`, `arping`, `ss` (аналог `netstat`).
- **Файловый редактор:** `nano`.
- **Просмотр логов:** `journalctl -u <название службы>` (например, `journalctl -u ideco-routing-backend`).
- **Разблокировка в случае срабатывания защиты от брутфорс-атак:**
  - `fail2ban-client unban --all` - команда используется для снятия всех блокировок.
  - `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса. Укажите нужный IP-адрес в качестве аргумента.
- **Просмотр конфигурации FRR:** `vtysh`.
- **Просмотр системных правил Межсетевого экрана:**
  - `iptables -L |grep fwd.sys.<id правила>` - для просмотра системных правил FORWARD.
  - `iptables -L |grep inp.sys.<id правила>` - для просмотра системных правил INPUT.
  - `iptables -L -v` - для полного вывода всех цепочек системных правил со статистикой по каждому правилу.

Перечень цепочек системных правил

- `Chain forward_sys_rules` - системные FORWARD-правила, находятся перед пользовательскими.
- `Chain forward_user_rules_before` - пользовательские FORWARD-предправила от Ideco Center, находятся перед локальными пользовательскими.
- `Chain forward_user_rules` - пользовательские FORWARD-правила.
- `Chain forward_user_acl_rules` - правила списков ACL (через API).
- `Chain forward_user_rules_after` - пользовательские FORWARD-постправила от Ideco Center, находятся после локальных пользовательских.
- `Chain input_sys_rules` - системные INPUT-правила.
- `Chain input_sys_rules_E` - системные правила фильтрации для WAN-интерфейсов.
- `Chain input_user_rules_before` - пользовательские INPUT-предправила от Ideco Center, находятся перед локальными пользовательскими.
- `Chain input_user_rules` - пользовательские INPUT-правила.
- `Chain input_user_rules_after` - пользовательские INPUT-постправила от Ideco Center, находятся после локальных пользовательских.
- `Chain input_reject` - цепочка для отправки RST- или ICMP-ответа при блокировке.
- `Chain input_drop` - цепочка для дропа пакета при блокировке.
- `Chain preinput_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК перед INPUT.
- `Chain preinput_fstek_rules_log_bf` - опциональные правила по нормативам ФСТЭК для логирования BADFLAGS.
- `Chain input_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК на INPUT.
- `Chain forward_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК на FORWARD.
- `Chain output_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК на OUTPUT.
- `Chain ips_nfq_rules` - цепочка для работы профилей IPS.
- `Chain l7_inspection` - цепочка, в которую перенаправляется трафик при срабатывании правила с действием **Разрешить**, если к нему применены профили DPI/IPS для проверки.
- `Chain fail2ban` - блокировки fail2ban по IP-адресу.
- `Chain filter_dns` - функциональность перехвата DNS-запросов.
- `Chain filter_log_user_rules` - пользовательские правила логирования соединения.
- `Chain set_log_mark_chain` - настройка логирования соединения.
- `Chain clear_log_mark_chain` - очистка логирования соединения.

- `Chain log_accept` - цепочка для разрешающего правила или разрешающей политики.
- `Chain smart_drop` - цепочка, в которую перенаправляется трафик при срабатывании правила с действием **Отбросить** (без отправки RST).
- `Chain smart_reject` - цепочка, в которую перенаправляется трафик при срабатывании правила с действием **Запретить** (с отправкой RST).
- **Вызов локального меню:** `ideco-local-menu --debug` - команда используется для доступа к локальному меню Ideco NGFW Novum.

Для просмотра подсказки по всем командам введите : `ideco-vppctl ?`

- **Просмотр списка всех физических интерфейсов, соответствующих сетевой карте:** `ideco-vppctl show hardware-interface brief`.
- **Просмотр списка всех сетевых интерфейсов, через которые проходит трафик:** `ideco-vppctl show interface`.
- **Просмотр списка всех IP-адресов интерфейсов:** `ideco-vppctl show interface addr`.
- **Просмотр таблицы маршрутизации:** `ideco-vppctl show ip fib`.
- **Запись последних 100 сетевых пакетов, прошедших через шлюз:** `ideco-vppctl pcap trace rx tx intfc any file capture.pcap`.
- **Просмотр ARP-таблицы:** `ip neigh show`.

Таблица служб

Модуль	Имя службы
ALD Pro	ideco-ald-rest, ideco-ald-backend
Active Directory	ideco-ad-log-collector, ideco-ad-backend
BGP, OSPF	ideco-routing-rest, ideco-routing-backend, frr
Веб-интерфейс администратора	nginx-control-plane (порты 8443 и 82)
DNS	unbound-keygen, unbound-anchor, unbound, nsd, ideco-dns-backend
DDNS	ideco-dns-backend
DHCP	ideco-dhcp-server-backend
Обратный прокси	nginx-data-plane (порты 443 и 80)
IGMP Proxy	ideco-igmpproxy-rest, ideco-igmpproxy-backend
IPsec	ideco-ipsec-backend
Ideco Center	ideco-central-console-backend
Ideco Client	ideco-websocket-vpn-server, ideco-agent-websocket, ideco-agent-backend
NTP	chronyd
Syslog	ideco-monitor-backend, ideco-logs-backend
VCE	ideco-vce-rest, ideco-vce-backend
VPN-подключения	pcscd, ideco-vpn-sessions-sync, ideco-vpn-servers-backend, ideco-vpn-netns, ideco-vpn-dhcp-backend, ideco-vpn-authd, ideco-gost-vpn-rest, ideco-gost-vpn-backend, ideco-accel-sstp, ideco-accel-l2tp, strongswan
Web Application Firewall	ideco-waf-event-syncer, ideco-waf-backend
Авторизация	ideco-auth-backend
Антивирус	klmsinit, kav-scanner, ideco-av-backend
Профили next hop, Маршрутизация	ideco-routing-backend
Бэкапы	ideco-backup-rotate, ideco-backup-restore, ideco-backup-create, ideco-backup-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-backend, ideco-web-authd
Дополнительно	ideco-system-swap, ideco-system-backend
Кластеризация	ideco-cluster-backup-pusher, ideco-cluster-backend
Контент-фильтр	ideco-content-filter-backend
Лицензия	ideco-license-backend
Межсетевой экран	ideco-fw-stats, ideco-firewall-rest, ideco-firewall-backend, ideco-apply-manual-blocklist, ideco-acl-rest, ideco-acl-backend, ideco-nflog
Обновления	ideco-sysupdate-backend
Обнаружение устройств	ideco-netscan-backend
Объекты	ideco-alias-backend
Обратный прокси	ideco-reverse-backend

Модуль	Имя службы
Ограничение скорости	ideco-shaper-backend
Отчеты и журналы	ideco-reports-backend, ideco-logs-syncer, ideco-logs-backend, ideco-audit-backend
Предотвращение вторжений	ideco-suricata-profiles-syncer, ideco-suricata-event-syncer, ideco-suricata-backend, ideco-suricata
Прокси	squid, ideco-proxy-backend
Профили контроля приложений	ideco-app-stats, ideco-app-control-nfq, ideco-app-backend
Сертификаты	ideco-cert-backend
Сетевые интерфейсы	ideco-l2manager-rest, ideco-l2manager-l2migration, ideco-l2manager-dhclient, ideco-l2manager-backend, ideco-l2-manager

Служебные:

Модуль	Имя службы
API	ideco-rest-api-backend
MY.IDECO	ideco-mir-alerts
Базовая система и менеджер сессий (systemd)	user, var-log-journal, systemd-udevd, systemd-tmpfiles-setup, systemd-sysctl, systemd-oomd, systemd-nsresourced, systemd-modules-load, systemd-machined, systemd-logind, systemd-journald, systemd-hostnamed, systemd-homed, systemd-coredump, systemd-boot-random-seed, init
Демон для работы RDP в SSL VPN	guacd
Инженерная панель	ideco-engineering-panel-backend
Контроль целостности системы	ideco-check-sums
Локальная база данных	ideco-etcd-runtime-defrag, ideco-etcd-runtime, ideco-etcd-permanent-defrag, ideco-etcd-permanent
Локальное меню	ideco-local-menu
Настройка системы в облачных развертываниях	ideco-vk-cloud-license, ideco-cloud-init-backend
Проверка прав пользователей на перезапуск служб systemd	ideco-policy-backend
Ранняя инициализация системы	dracut-initqueue, dracut-cmdline
Сбор метрик и статистики	prometheus-node-exporter, prometheus, ideco-gatherstat-backend
Сервер базы данных	clickhouse-server
Системная шина	dbus-broker
Создание дампов ядра в случае падения	kdump
Управление томами	lvm2-monitor, lvm-activate-utm_421259

Примеры использования утилит

Классический контекст | Высокопроизводительный контекст

Примеры использования утилиты vtysh

Просмотр таблицы маршрутизации

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра таблицы маршрутизации введите:

```
show ip route
```

Пример вывода утилиты:

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 1.1.1.1/32 [1/0] via 10.10.10.1, Leth1, weight 1, 00:02:32
O   10.10.10.0/24 [110/1] is directly connected, Leth1, weight 1, 00:02:28
C>* 10.10.10.0/24 is directly connected, Leth1, 00:02:33
C>* 10.11.12.0/25 is directly connected, Eeth2, 00:02:33
O>* 10.20.40.0/24 [110/21] via 10.10.10.201, Leth1, weight 1, 00:02:18
S>* 10.128.0.0/16 [1/0] is directly connected, Lvpn0, weight 1, 00:02:32
C>* 169.254.1.0/29 is directly connected, lb_local_in, 00:02:33
C>* 169.254.1.0/29 is directly connected, lb_local_out, 00:02:33
C>* 169.254.1.4/32 is directly connected, Lvpn0, 00:02:33
C>* 169.254.254.254/32 is directly connected, lo, 00:02:33
```

Полезная информация:

- Не все маршруты могут быть выгружены в ядро, поэтому при просмотре таблицы маршрутизации без утилиты `vtsyh` некоторые маршруты могут не отображаться.
- Для просмотра примененных маршрутов введите:

```
ip route show table 230
```

Просмотр конфигурации FRR

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра конфигурации введите:

```
show running-config
```

Пример вывода утилиты:

```
Building configuration...

Current configuration:
!
frr version 8.5.3
frr defaults traditional
hostname bez-nazvaniya-23000007-c6d8-01c2-a572-d68497c66441
no ipv6 forwarding
service integrated-vtysh-config
!
ip route 10.128.0.0/16 Lvpn0
!
interface Leth1
 ip ospf cost 125
exit
!
interface lo
 ip ospf passive
exit
!
router ospf
 ospf router-id 192.168.0.200
 redistribute connected
 redistribute static
 network 172.16.10.0/24 area 0.0.0.200
 default-information originate always
exit
!
ip prefix-list DEFAULT seq 5 deny 0.0.0.0/0
ip prefix-list DEFAULT seq 10 permit 0.0.0.0/0 le 32
!
route-map DEFMAP permit 10
 match ip address prefix-list DEFAULT
exit
!
ip protocol ospf route-map DEFMAP
!
end
```

Просмотр OSPF соседства

Убедитесь, что включен модуль OSPF.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей OSPF введите:

```
show ip ospf neighbor
```

Пример вывода утилиты:

```
Neighbor ID     Pri State           Up Time         Dead Time Address         Interface                         RXmtL RqstL DB
10.10.10.201      1 Full/DR         6m35s             34.709s 10.10.10.201    Leth1:10.10.10.126                    0     0
```

Просмотр BGP соседства

> Убедитесь, что включен модуль BGP.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей BGP введите:

```
show ip bgp neighbors
```

Пример вывода утилиты:

```
BGP neighbor is 10.10.10.2, remote AS 123, local AS 123, internal link
  Local Role: undefined
  Remote Role: undefined
 Member of peer-group V4_AS123_10_10_10_2 for session parameters
  BGP version 4, remote router ID 10.11.12.2, local router ID 10.11.12.71
  BGP state = Established, up for 00:00:10
  Last read 00:00:10, Last write 00:00:09
  Hold time is 180 seconds, keepalive interval is 60 seconds
  Configured hold time is 180 seconds, keepalive interval is 60 seconds
  Configured conditional advertisements interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Extended Message: advertised
    AddPath:
      IPv4 Unicast: RX advertised
    Long-lived Graceful Restart: advertised
    Route refresh: advertised and received(new)
    Enhanced Route Refresh: advertised
    Address Family IPv4 Unicast: advertised and received
    Hostname Capability: advertised (name: bez-nazvaniya-5f3323c3-6462-4981-b8a0-2b4397e3448a,domain name: n/a) not received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 0 seconds
      Address families by peer:
        none
  Graceful restart information:
    End-of-RIB send: IPv4 Unicast
    End-of-RIB received:
    Local GR Mode: Helper*

    Remote GR Mode: Helper

    R bit: False
    N bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
    IPv4 Unicast:
      F bit: False
      End-of-RIB sent: Yes
      End-of-RIB sent after update: Yes
      End-of-RIB received: No
      Timers:
        Configured Stale Path Time(sec): 360
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
```

```
    Opens:                  1         1
    Notifications:          0         0
    Updates:                1         3
    Keepalives:             1         2
    Route Refresh:          0         0
    Capability:             0         0
    Total:                  3         6
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  V4_AS123_10_10_10_2 peer-group member
  Update group 1, subgroup 1
  Packet Queue length 0
  NEXT_HOP is always this router
  Community attribute sent to this neighbor(all)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *IMPORT_V4_AS123_10_10_10_2
  Route map for outgoing advertisements is *EXPORT_V4_AS123_10_10_10_2
  12 accepted prefixes

  Connections established 1; dropped 0
  Last reset 00:05:26,  No AFI/SAFI activated for peer
  Internal BGP neighbor may be up to 255 hops away.
Local host: 10.10.10.126, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 38445
Nexthop: 10.10.10.126
Nexthop global: ::
Nexthop local: ::
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Estimated round trip time: 1 ms
Read thread: on  Write thread: on  FD used: 25
```

Примеры использования утилиты iptables

Просмотр системного правила INPUT

Пример просмотра правила с `id=59` для опции **Полный доступ**.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
iptables -L |grep inp.sys.59
```

3. Пример ответа на запрос:

```
-A INPUT -m condition --condition emergency_internet_access -m logger --mask 268435456 --value 268435456 --prefix inp.sys.59,
```

- `-A INPUT` - цепочка правил INPUT (для соединений с самим NGFW);
- `-m condition --condition emergency_internet_access` - условие для активации правила. Специфичное для Ideco NGFW Novum;
- `-m logger --mask 268435456 --value 268435456 --prefix inp.sys.59,accept` - уникальная метка правила, отличающая его от других в модуле **Тестирование правил**. Специфичное для Ideco NGFW Novum;
- `-j` - действие, специфичное для Ideco NGFW Novum. Возможные варианты:
  - `log_accept` - если включено логирование, залогировать и разрешить;
  - `smart_reject` - отбросить.

Правила могут быть более сложными. При необходимости дополнительную информацию можно найти в документации к iptables.

Просмотр системного правила FORWARD

Пример просмотра правила с `id=15` для опции **Блокировать протоколы QUIC и HTTP/3**.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
iptables -L |grep fwd.sys.15
```

3. Пример ответа на запрос:

```
-A forward_sys_rules -p udp -m multiport --dports 80,443 -m condition --condition "quic_reject"  -m logger --mask 268435456 -
```

- `-A forward_sys_rules` - системное правило FORWARD;
- `-p udp` - протокол UDP;
  - `--dports 80,443` - порт назначения `80` или `443`;
- `-m condition --condition "quic_reject"` - условие для активации правила. Специфичное для Ideco NGFW Novum;
- `-m logger --mask 268435456 --value 268435456 --prefix fwd.sys.15,drop` - уникальная метка правила, отличающая его от других в модуле **Тестирование правил**. Специфичное для Ideco NGFW Novum;
- `-j` - действие, специфичное для Ideco NGFW Novum. Возможные варианты:
  - `log_accept` - если включено логирование, залогировать и разрешить;
  - `smart_reject` - отбросить.

Правила могут быть более сложными. При необходимости дополнительную информацию можно найти в документации к iptables.

Анализ трафика

Используйте утилиту `tcpdump` для анализа трафика на NGFW в разделе **Управление сервером → Терминал**.

Утилита `tcpdump` предустановлена в продукт Ideco NGFW Novum.

При запуске утилиты без каких-либо ключей/параметров произойдет перехват всех пакетов через первый доступный сетевой интерфейс (петлевые интерфейсы игнорируются). Отобразить список интерфейсов можно командой `tcpdump -D`. Для просмотра всех ключей утилиты введите `tcpdump -h`.

Для более гибкого использования утилиты используйте комбинацию ключей. **Например**, чтобы вывести пять пакетов с интерфейса `eth1`, введите:

```
tcpdump -i eth1 -c 5
```

Ключи и примеры команд для утилиты tcpdump

Использование tcpdump с применением ключей

Просмотр списка сетевых интерфейсов

Введите в терминале:

```
tcpdump -D
```

Пример вывода утилиты:

```
1.eth0
2.nflog (Linux netfilter log (NFLOG) interface)
3.nfqueue (Linux netfilter queue (NFQUEUE) interface)
4.eth1
5.any (Pseudo-device that captures on all interfaces)
6.lo [Loopback]
```

Захват пакетов, проходящих через определенный интерфейс

Введите в терминале для просмотра пакетов с интерфейса `eth1`:

```
tcpdump -i eth1
```

Пример вывода утилиты:

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
01:06:09.278817 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761, seq 1, length 64
01:06:09.279374 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 4761, seq 1, length 64
01:06:10.281142 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761, seq 2, length 6
```

Полезная информация:

- Ключ `-v` увеличивает количество отображаемой информации о пакетах (добавляется протокол, флаги пакета).
- Ключ `-vv` дает еще более подробную информацию (полный разбора пакета и вывод в терминал).

Пример использования с ключами:

```
tcpdump -i eth1 -v
```

```
tcpdump -i eth1 -vv
```

Вывод и захват только определенного числа пакетов

Введите в терминале для разбора пяти пакетов с интерфейса по-умолчанию:

```
tcpdump -c 5
```

Пример вывода утилиты:

```
04:19:07.675216 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 2186733178:2186733278, ack 204106815, win 37232, length 100
04:19:07.675497 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 100, win 65535, length 0
04:19:07.675747 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 100:136, ack 1, win 37232, length 36
04:19:07.675902 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 136, win 65535, length 0
04:19:07.676142 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 136:236, ack 1, win 37232, length 100
5 packets captured
```

Использование tcpdump с применением фильтров

Список часто используемых фильтров `tcpdump`:

- `port` - фильтрация пакетов по номеру порта.
- `host` - фильтрация исходящих и входящих пакетов по IP-адресу.
- `src` - фильтрация пакетов по IP-адресу источника.
- `dst` - фильтрация пакетов по IP-адресу назначения.

Для фильтрации по определенному протоколу укажите протокол в качестве фильтра:

- `tcp` - фильтрация пакетов `TCP`.
- `udp` - фильтрация пакетов `UDP`.
- `icmp` - фильтрация пакетов `ICMP`.
- `arp` - фильтрация пакетов `ARP`.

Для комбинирования фильтров используйте логические операторы:

- `and` - пакет выведется при совпадении условий у всех указанных фильтров.
- `or` - пакет выведется при совпадении условий у одного указанного фильтра.
- `not` - инвертирует условие фильтра.

Фильтрация пакетов по 80 порту

Введите в терминале:

```
tcpdump port 80
```

Пример вывода утилиты:

```
23:54:24.978612 IP 10.0.0.1.53971 > 10.0.0.50.80: Flags [SEW], seq 53967733, win 65535, options [mss 1460,nop,wscale 5,nop,no
23:54:24.978650 IP 10.0.0.50.80 > 10.0.0.1.53971: Flags [S.E], seq 996967790, ack 53967734, win 28960, options [mss 1460,sack
23:54:24.978699 IP 10.0.0.1.53972 > 10.0.0.50.80: Flags [SEW], seq 226341105, win 65535, options [mss 1460,nop,wscale 5,nop,n
23:54:24.978711 IP 10.0.0.50.80 > 10.0.0.1.53972: Flags [S.E], seq 1363851389, ack 226341106, win 28960, options [mss 1460,sa
```

Фильтрация пакетов по хосту с IP-адресом 10.0.2.15

Введите в терминале:

```
tcpdump host 10.0.2.15
```

Пример вывода утилиты:

```
03:48:06.087509 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 3862934963:3862934999, ack 65355639, win 37232, length 36
03:48:06.087806 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 36, win 65535, length 0
03:48:06.088087 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 36:72, ack 1, win 37232, length 36
```

```
03:48:06.088274 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 72, win 65535, length 0
03:48:06.088440 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 72:108, ack 1, win 37232, length 36
```

Фильтрация пакетов по IP-адресу назначения 8.8.8.8

Введите в терминале:

```
tcpdump dst 8.8.8.8
```

Пример вывода утилиты:

```
17:32:19.642154 IP desktop > dns.google: ICMP echo request, id 1, seq 1, length 64
17:32:20.644231 IP desktop > dns.google: ICMP echo request, id 1, seq 2, length 64
17:32:21.645715 IP desktop > dns.google: ICMP echo request, id 1, seq 3, length 64
17:32:22.647387 IP desktop > dns.google: ICMP echo request, id 1, seq 4, length 64
17:32:23.648814 IP desktop > dns.google: ICMP echo request, id 1, seq 5, length 64
```

Фильтрация пакетов по протоколу ICMP

Введите в терминале:

```
tcpdump icmp
```

Пример вывода утилиты:

```
04:03:47.408545 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812, seq 75, length 64
04:03:47.408999 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812, seq 75, length 64
04:03:48.408697 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812, seq 76, length 64
04:03:48.409208 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812, seq 76, length 64
04:03:49.411287 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812, seq 77, length 64
```

Фильтрация пакетов с интерфеса eth1 с IP-адресом источника 10.0.0.1 и 80 портом назначения

Введите в терминале:

```
tcpdump -i eth1 src 10.0.0.1 and dst port 80
```

Пример вывода утилиты:

```
00:18:17.155066 IP 10.0.0.1.54222 > 10.0.0.50.80: Flags [F.], seq 500773341, ack 2116767648, win 4117, options [nop,nop,TS va
00:18:17.155104 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [S], seq 904045691, win 65535, options [mss 1460,nop,wscale 5,nop,nop
00:18:17.157337 IP 10.0.0.1.54221 > 10.0.0.50.80: Flags [P.], seq 4282813257:4282813756, ack 1348066220, win 4111, options [n
00:18:17.157366 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [.], ack 1306947508, win 4117, options [nop,nop,TS val 257786174 ecr
```

Фильтрация пакетов по всем доступным протоколам, кроме ICMP

Введите в терминале:

```
tcpdump not icmp
```

Пример вывода утилиты:

```
17:45:34.847882 IP desktop.48552 > 149.154.167.41.https: Flags [P.], seq 3991504547:3991504748, ack 499514727, win 248, optio
17:45:34.918383 IP 149.154.167.41.https > desktop.48552: Flags [.], ack 201, win 7509, options [nop,nop,TS val 4205203056 ecr
17:45:34.919444 IP 149.154.167.41.https > desktop.48552: Flags [.], seq 1:1229, ack 201, win 7509, options [nop,nop,TS val 42
17:45:34.919475 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 1229, win 239, options [nop,nop,TS val 1585771377 ecr
17:45:34.919778 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 1229:2457, ack 201, win 7509, options [nop,nop,TS va
17:45:34.919804 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2457, win 239, options [nop,nop,TS val 1585771377 ecr
17:45:34.923322 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 2457:2845, ack 201, win 7509, options [nop,nop,TS va
17:45:34.923351 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2845, win 239, options [nop,nop,TS val 1585771381 ecr
17:45:35.644804 IP desktop.49669 > _gateway.domain: 65295+ PTR? 41.167.154.149.in-addr.arpa. (45)
```

Сохранение дампа захваченных пакетов в файл в формате .pcap

Введите в терминале:

```
tcpdump -w out.pcap
```

Для анализа захваченных пакетов в формате `.pcap` используйте Wireshark.

Использование в Ideco NGFW Novum

Проверка работы IPsec-туннелей

Команды помогут понять причину неработоспособности IPsec-туннеля:

1. Для проверки прохождения трафика на всех интерфейсах головного офиса по порту 4500 введите:

```
tcpdump -i any port 4500
```

2. Для проверки прохождения трафика на всех интерфейсах филиала по порту 500 введите:

```
tcpdump -i any port 500
```

Защита от брутфорс-атак (fail2ban)

Классический контекст | Высокопроизводительный контекст

Служба `fail2ban` отслеживает повторяющиеся неудачные попытки аутентификации с одного IP-адреса.

После шести неудачных попыток ввода пароля в течение 15 минут IP-адрес отправителя запросов блокируется на 45 минут.

Список служб, защищаемых от брутфорс-атак:

Модуль	Имя службы
VPN	ideco-vpn-authd
SSH	ideco-ssh, sshd
Веб-интерфейс	ideco-web-interface
Двухфакторная аутентификация	ideco-two-factor-codes
Обратный прокси	ideco-reverse-proxy, ideco-reverse-proxy-conn, ideco-reverse-proxy-req
Личный кабинет пользователя	ideco-user-cabinet, ideco-user-cabinet-backend, ideco-user-cabinet-proxy, ideco-user-cabinet-reports
Почтовые службы	ideco-dovecot, ideco-postfix-connrate, ideco-postscreen-prgrt, ideco-roundcube, ideco-smtp, ideco-smtp-rcpt

Просмотр логов

Логи службы `fail2ban` можно просмотреть двумя способами:

- В веб-интерфейсе в **Отчеты и журналы** → **Система**, задав фильтр `fail2ban`.
- В **Управление сервером** → **Терминал**, введя команду `journalctl -u fail2ban`.

Просмотр заблокированных адресов

Для получения списка IP-адресов, заблокированных `fail2ban`, используйте команды:

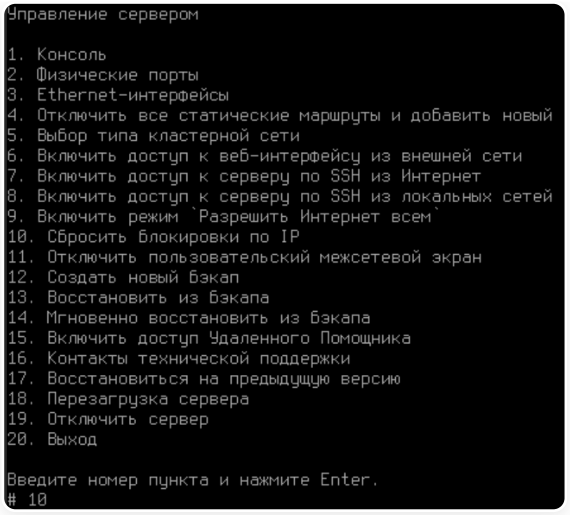
- `fail2ban-client status` - просмотр списка доступных Jail.
- `fail2ban-client get [Jail] banned` - просмотр списка адресов в указанном Jail. Например: `fail2ban-client get utm-ssh banned`.
- `fail2ban-client banned` - просмотр заблокированных адресов сразу по всем Jail (формат `python dict/json`).

Разблокировка IP-адресов

Для разблокировки через терминал используйте команды:

- `fail2ban-client unban --all` - снятие всех блокировок.
- `fail2ban-client unban <IP-адрес>` - разблокировка конкретного IP-адреса.

Блокировки можно сбросить из локального меню шлюза, выбрав опцию **Сбросить блокировки по IP**:



Добавление IP-адреса в белый список

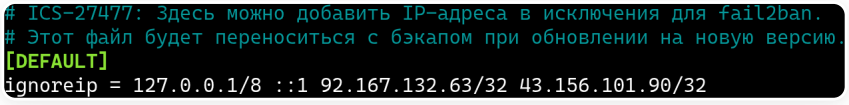
Если доверенный IP-адрес был заблокирован, добавьте его в белый список, чтобы предотвратить повторную блокировку. Для этого:

1. Перейдите в **Управление сервером** → **Терминал** и выполните команду:

```
nano /var/opt/ideco/fail2ban/excluded_ip_addresses.local
```

2. Найдите в файле параметр `ignoreip` и раскомментируйте строку, убрав символ `#` в начале.

3. Добавьте IP-адрес с маской `/32` или подсеть с нужной маской в конец строки через пробел. Для нескольких адресов укажите их последовательно через пробел:



4. Сохраните файл, нажав **Ctrl+O**, затем **Enter**.

5. Выйдите из редактора, нажав **Ctrl+X**.

6. Выполните команду `systemctl restart fail2ban` для перезагрузки службы и применения изменений.

Лицензия

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Лицензия**: `ideco-license-backend`.

Список служб для других разделов доступен по ссылке.

В разделе **NGFW** MY.IDECO находится информация о зарегистрированных серверах и имеющихся лицензиях. Подробнее о видах лицензий в статье Лицензирование.

Доступные действия для управления лицензиями:

- Регистрация сервера.
- Добавление коммерческой или бесплатной лицензии.
- Привязка лицензии к серверу.
- Просмотр информации об имеющихся лицензиях.
- Офлайн-обновление лицензии и баз модулей фильтрации.

Лицензия между **Системным контекстом** и всеми виртуальными контекстами общая. Это значит, что на Ideco NGFW Novum с лицензией на 100 пользователей можно создать неограниченное количество VCE, каждый из которых будет поддерживать 100 пользователей. В будущих версиях количество пользователей, ограниченное числом в лицензии, будет распределяться между **Системным контекстом** и всеми VCE.

Добавление коммерческой (Enterprise) лицензии

1. Скопируйте токен лицензии из письма, отправленного после покупки лицензии. Формат токена: `owhYLGvT6Xmt819JyinSxREkJfvjVO63`.

2. В MY.IDECO перейдите в раздел **NGFW → Лицензирование**, нажмите **Добавить лицензию** и выберите **Коммерческую**.

3. Введите токен в поле **Токен лицензии** и нажмите **Добавить**.

Токен станет недействительным, а в таблице **Непривязанные лицензии** отобразится купленная лицензия.

Если требуется перепривязать купленную лицензию к серверу с уже установленной тестовой лицензией, воспользуйтесь статьей.

Добавление FREE (бесплатной) лицензии

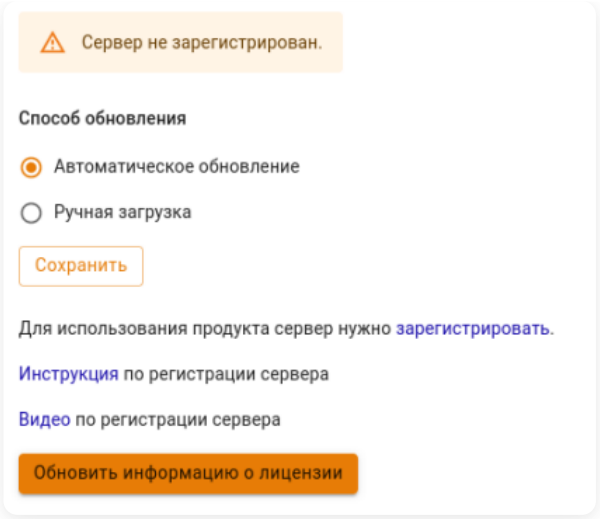
Для добавления FREE-лицензии в MY.IDECO перейдите в раздел **NGFW → Лицензирование**, нажмите **Добавить лицензию** и выберите **Бесплатную**. Добавленная лицензия отобразится в таблице **Непривязанные лицензии**.

Подробнее о бесплатной лицензии в статье Лицензирование.

Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн. Онлайн проводится только в MY.IDECO. Офлайн потребует доступ к веб-интерфейсу сервера.

Для онлайн-привязки лицензии в разделе **Управление сервером → Лицензия** веб-интерфейса Ideco NGFW Novum выберите способ обновления **Автоматическое обновление**. Для офлайн-привязки выберите **Ручную загрузку**:



Назначьте имеющиеся коммерческие лицензии на любой зарегистрированный сервер Ideco NGFW Novum с учетом следующих ограничений:

- Одна лицензия может быть привязана только к одному серверу.
- Демо-лицензию нельзя привязать к другому серверу.
- Демо-лицензию нельзя отвязать от сервера. Доступна только замена на другую лицензию.
- Демо-лицензию нельзя повторно получить на одну и ту же инсталляцию сервера.
- При удалении сервера с демо-лицензией также удаляется и лицензия.

После активации лицензия привязывается к оборудованию, на котором установлено программное обеспечение Ideco NGFW Novum. При замене оборудования или частей оборудования лицензия отвязывается и требует повторной привязки. Демо-лицензия при этом теряется.

Онлайн-привязка лицензии

Выберите удобный вариант привязки:

- В MY.IDECO на вкладке **Лицензирование** нажмите **Привязать лицензию**. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения.
- В MY.IDECO на вкладке **Лицензирование** выберите **Непривязанные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

Особенности работы онлайн-лицензии:

- При наличии доступа в интернет обновление данных о лицензии происходит один раз в сутки.
- Если связь с серверами лицензирования отсутствует, Ideco NGFW Novum предпринимает попытки соединения каждые 60 секунд до восстановления доступа.
- Если у Ideco NGFW Novum отсутствует связь с серверами лицензирования более 30 дней, то Ideco NGFW Novum перейдет в нелицензионный режим.
- Для использования Ideco NGFW Novum в закрытом контуре (без доступа к интернету) необходимо использовать офлайн-лицензию.

Офлайн-привязка лицензии

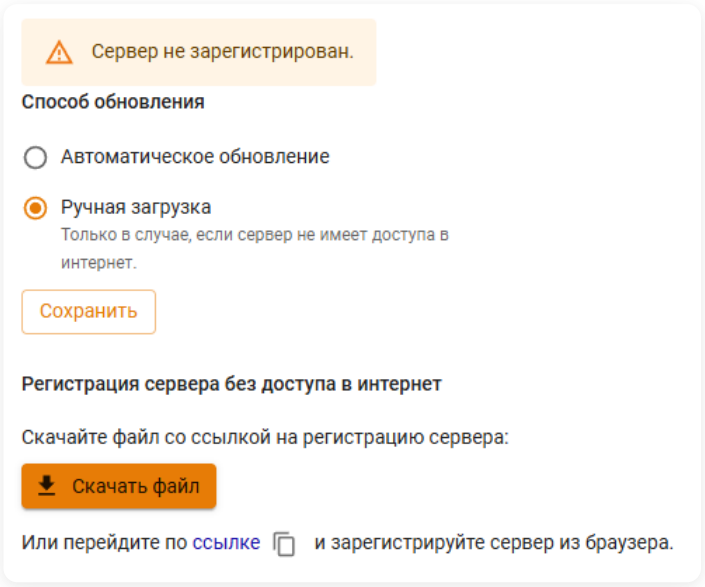
Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

1. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum. Выберите **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Для этого нажмите **Скачать файл** или скопируйте ссылку из веб-интерфейса:

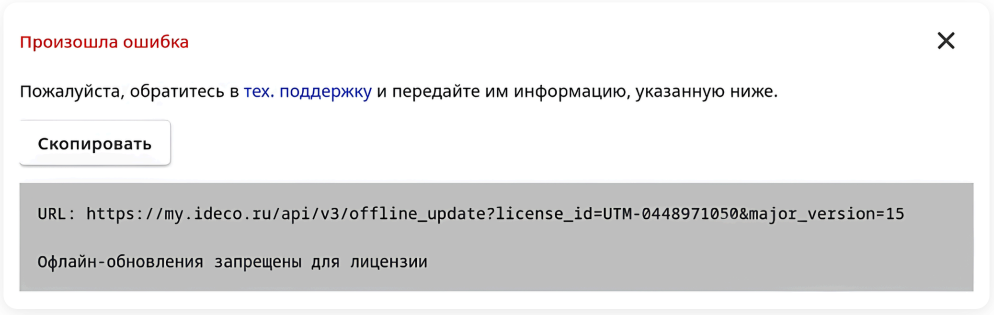


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

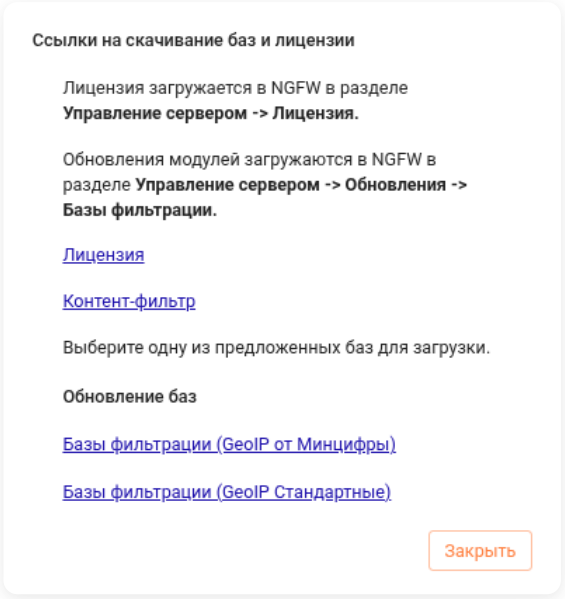
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

5. Перейдите в **NGFW** → **Лицензирование** в MY.IDECO. Нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `UTM (UTM Unknown)`.

Если была выбрана лицензия, не подходящая для офлайн-регистрации сервера, то появится ошибка:

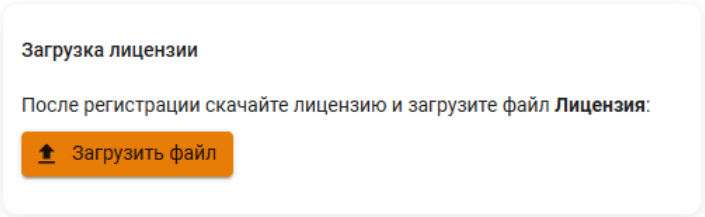


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



Если при скачивании Обновления баз (Предотвращение вторжений, базы GeoIP) через **Google Chrome** возникают проблемы, в настройках браузера разрешите **Небезопасный контент** для MY.IDECO.

7. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum и загрузите файл с лицензией, скачанный в пункте 6:



Повторная регистрация сервера после удаления

1. Откройте терминал и введите команду:

```
rm /var/cache/ideco/license-backend/license.json
systemctl restart ideco-license-backend.service
```

2. Следуйте пунктам по офлайн-регистрации, которые приведены выше.

Просмотр информации о лицензиях

Посмотреть информацию о модулях и лицензии можно:

- В MY.IDECO напротив нужного сервера.
- В разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum.

Информация о лицензии содержит сведения о количестве пользователей, сроках действия лицензии, окончания обновлений и технической поддержки и других параметрах.

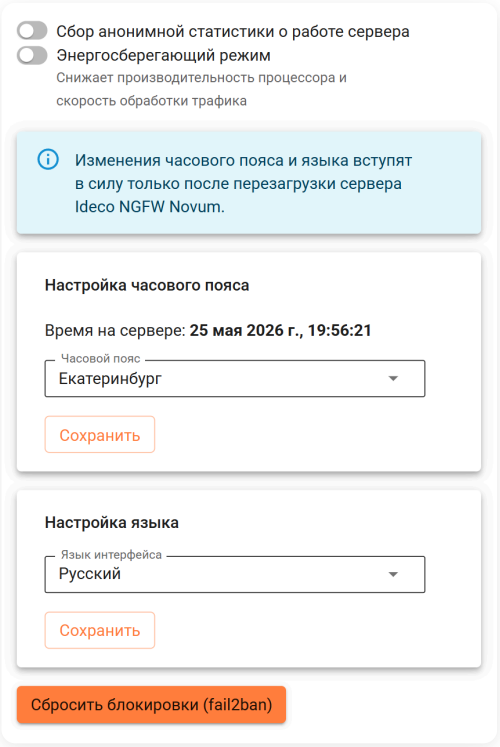
Дополнительно

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Дополнительно**: `ideco-system-backend`, `ideco-system-swap`.

Список служб для других разделов доступен по ссылке.

Настройка часового пояса и сбор анонимной статистики через веб-интерфейс в разделе **Управление сервером** → **Дополнительно**:



- **Сбор анонимной статистики о работе сервера** - включите опцию, чтобы сервер мог отправлять информацию об используемых модулях. При этом исключается передача следующих данных:
  - Пользователи.
  - Проходящий через сервер трафик.
  - Сетевые интерфейсы.
  - Идентификаторы сервера и лицензии.
- **Энергосберегающий режим** - включите опцию для снижения производительности процессора и скорости обработки трафика.
- **Настройка часового пояса** - установите часовой пояс для корректного сбора логов и статистики.
- **Настройка языка** - укажите язык, удобный для работы в веб-интерфейсе.
- **Сбросить блокировки (fail2ban)** - используйте для сброса всех IP-адресов, заблокированных службой `fail2ban`. Если требуется разблокировать какой-то конкретный IP-адрес, воспользуйтесь командой `fail2ban-client unban <IP-адрес>` в терминале.

Служба `fail2ban` отслеживает повторяющиеся неудачные попытки аутентификации с одного IP-адреса.

После шести неудачных попыток ввода пароля в течение 15 минут IP-адрес отправителя запросов блокируется на 45 минут.

Почтовый релей

API

Функциональность доступна только в **Системном контексте**.

Все возможности по фильтрации почтового трафика можно также применить к внутреннему почтовому серверу, опубликовав сервер через почтовый релей.

Для фильтрации почтового трафика от вирусов, спама и фишинга рекомендуется покупка лицензии на антиспам Касперского.

Для настройки почтового сервера перейдите в раздел **Почтовый релей**. Настройка ключевых параметров выполняется в следующих разделах:

- **Основные настройки** - базовые параметры, необходимые для настройки почтового сервера, почтового релея и веб-почты.
- **Расширенные настройки** - параметры маршрутизации и ограничения почты, механизмы безопасности, а также DKIM-подпись исходящей почты для подтверждения легитимности отправителя.
- **Антиспам и антивирус** - управление работой службы антиспама и антивируса почтового сервера, а также настройка фильтрации.
- **Правила** - управление пересылкой писем, а также списками доверенных и заблокированных отправителей.
- **Почтовая очередь** - управление очередью отложенной входящей и исходящей почты.

Если используется почтовый сервер Ideco NGFW Novum, обязательно подключите дополнительный SSD. В настройках почтового сервера можно указать максимальный размер почтового ящика и максимальный размер письма. Подробнее в статье.

Параметры подключения и примеры настройки почтового клиента описаны в статье Настройка почтового клиента.

При настройке кластера почта доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.

Схема фильтрации почтового трафика

Полная схема и последовательность фильтрации:



Модуль **Антиспама и антивируса** Касперского использует собственный набор методик для фильтрации и обеспечивает высокий уровень детектирования спама при низких значениях ложных срабатываний (0,003-0,005% от общего количества сообщений).

Для защиты пользователей применяется набор технологий распознавания спама с использованием внешних облачных сервисов (DNSBL, SPF и SURBL) и собственных алгоритмов:

- Сигнатурный анализ текста и графики.
- Лингвистическая эвристика.
- Использование UDS-запросов в режиме реального времени.

Также для защиты проверяются все ссылки в почтовых сообщениях и письма со ссылками на фишинговые ресурсы блокируются.

Разрешенные адреса в настройках почты обеспечивают прохождение писем без фильтрации, начиная с уровня **Фильтрации по серым спискам**. **Предварительный спам-фильтр** срабатывает для любых адресатов.

Полезные ссылки

- **Основные настройки**
- **Расширенные настройки**
- **Антиспам и антивирус**
- **Правила**
- **Почтовая очередь**
- **Настройка почтового клиента**

Основные настройки

В разделе представлены базовые параметры, необходимые для настройки почтового сервера, почтового релея и веб-почты.

Настройка почтового сервера

Перейти >

Настройка почтового релея

Перейти >

Web-почта

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка почтового сервера

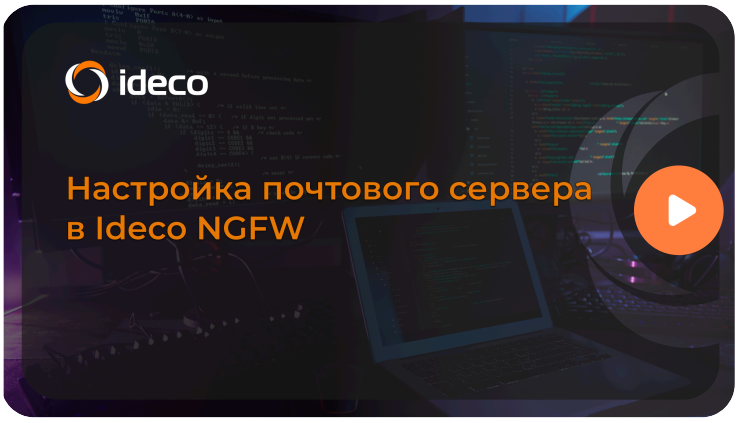
Функциональность доступна только в **Системном контексте**.

Видеоинструкция

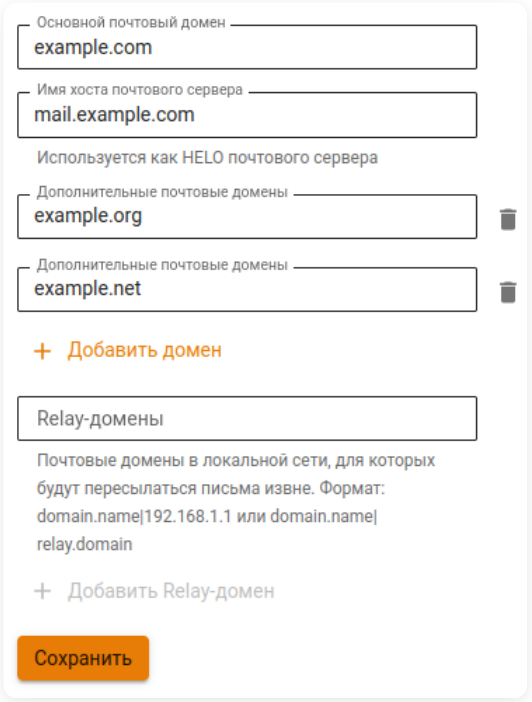
Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE



1. Перейдите в **Почтовый релей** → **Основные настройки** и заполните поля:



Расшифровка полей

- **Основной почтовый домен** - указывает серверу, для какого домена сервер принимает и обрабатывает электронную почту. Все пользовательские почтовые ящики закреплены за этим доменом. Переписка с внешними получателями осуществляется от имени указанного домена.
- **Имя хоста почтового сервера** - должно разрешаться из интернета во внешний IP-адрес NGFW. Указанное имя используется в качестве идентификатора при передаче почты между почтовыми серверами. Необходимо для корректной работы почтового сервера в интернете.
- **Дополнительные почтовые домены** - домены, которые почтовый сервер будет считать своими. Электронная почта, отправляемая с ящиков в этих почтовых доменах, будет обрабатываться сервером при условии правильной установки MX-записей.

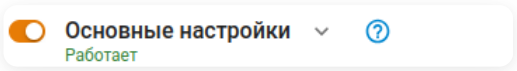
Имя хоста почтового сервера, как правило, совпадает с MX-записью для вашего домена.

При настройке авторизации в почте проверьте, чтобы основной или дополнительный почтовый домен совпадал с доменами **Каталога авторизации** в **Пользователи** → **Аутентификация**. В противном случае аутентификация будет выполняться через **Каталог по**

умолчанию: если пользователь есть в каталоге, аутентификация пройдет успешно по логину, указанному до `@`.

Настройку **Доменный суффикс для локальных пользователей** можно использовать совместно с настройкой почтового домена, чтобы для данного почтового домена использовался каталог **Локальные пользователи**.

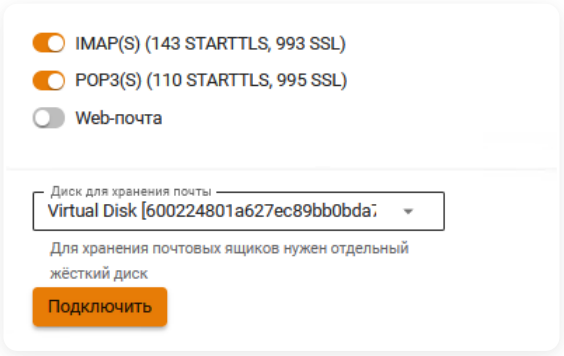
2. Включите почтовый сервер Ideco NGFW Novum:



3. Выберите протокол получения электронной почты:

- **IMAP(S) (143 STARTTLS, 993 SSL)** - подключение к почтовым ящикам с сохранением писем на сервере. Изменения (прочтение, перемещение, удаление) синхронизируются между устройствами. Удобен для использования с нескольких устройств.
- **POP3(S) (110 STARTTLS, 995 SSL)** - загрузка писем с сервера на клиент с последующим удалением с сервера. Настроить сохранение копий можно на почтовом клиенте. Подходит для проверки почты с одного устройства.

4. Подключите к серверу дополнительный жесткий диск:



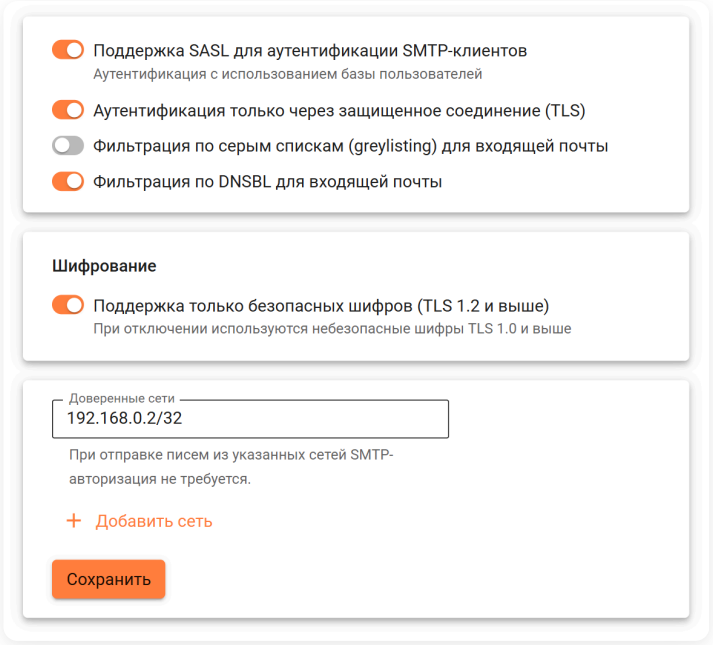
Если диск после подключения не отображается:

- Проверьте, стерты ли с диска все данные, в том числе таблица разделов.
- Обратитесь в техническую поддержку, если проблему не удалось решить самостоятельно.

Хранение почты на дополнительном HDD/SSD-диске обязательно. Рекомендуем использовать SSD-диск.

Поддерживаются SATA/SAS- и NVMe-накопители. Дополнительное устройство используется только для работы почтового сервера, другие данные на нем храниться не будут.

5. Чтобы разрешить прием входящей почты на порт 25 от сторонних доменов с серых IP-подсетей, внесите подсети в список доверенных. Для этого перейдите в **Почтовый релей** → **Расширенные настройки** → **Безопасность** и укажите в поле **Доверенные сети** адрес почтового сервера для подключения к NGFW Novum:



Подробнее о расширенных настройках - в статье.

SSL-сертификат для почтового домена

После сохранения настроек почтового сервера Ideco NGFW Novum создает локальный сертификат, подписанный корневым (самоподписанным) сертификатом. Параллельно с созданием локального сертификата отправляется запрос на выпуск сертификата Let's Encrypt:

- Если сертификат Let's Encrypt успешно выпущен, то Let's Encrypt заменит собой локальный сертификат.
- Если выпуск сертификата Let's Encrypt завершился неудачей, то будет использоваться локальный сертификат.

Для замены автоматически выпущенного сертификата перейдите в **Сервисы → Сертификаты → Загруженные сертификаты** и загрузите собственную цепочку сертификатов. **CN (Общее имя)** последнего сертификата в цепочке должно соответствовать домену, для которого загружается сертификат. Подробнее в инструкции.

Проверка настроек почтового сервера

Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса check.smtp.bz.

При правильной настройке почтовый сервер на Ideco NGFW Novum должен получить результат **Отлично**.

Создание копии диска с почтой

1. Подключите второй физический диск, на который будете клонировать почту.

2. В терминале выполните команду `lsblk` и посмотрите название дисков:

```
NAME                   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sr0                     11:0     1   1,8G  0 rom
nvme01                  259:0    0   150G  0 disk
├─nvme01p1              259:1    0   512M  0 part
├─nvme01p2              259:2    0     2M  0 part
└─nvme01p3              259:3    0 149,5G  0 part
  ├─utm_72874-root_one 253:0    0     4G  0 lvm  /run/ideco-erofs
  ├─utm_72874-data     253:1    0  63,7G  0 lvm  /run/ideco-overlay-dir
  ├─utm_72874-logs     253:2    0     2G  0 lvm  /var/log/journal
  ├─utm_72874-root_two 253:3    0     4G  0 lvm
  └─utm_72874-swap     253:4    0  15,3G  0 lvm  [SWAP]
nvme02                  259:4    0    50G  0 disk /var/spool/mail
nvme03                  259:5    0    55G  0 disk
```

- В примере используются диски:
  - `nvme01` - для работы NGFW.
  - `nvme02` - для хранения почты.
  - `nvme03` - новый диск.

3. Выполните поблочное копирование с помощью утилиты dd, введя команду:

```
dd if=/dev/nvme02 of=/dev/nvme03 bs=4M status=progress
```

- `if=/dev/nvme02` - источник данных для копирования.
- `of=/dev/nvme03` - место назначения для скопированных данных.

После выполнения команды все данные на диске `nvme03` будут перезаписаны. Если размер диска `nvme02` превышает размер диска `nvme03`, то копирование завершится неудачно.

Web-почта

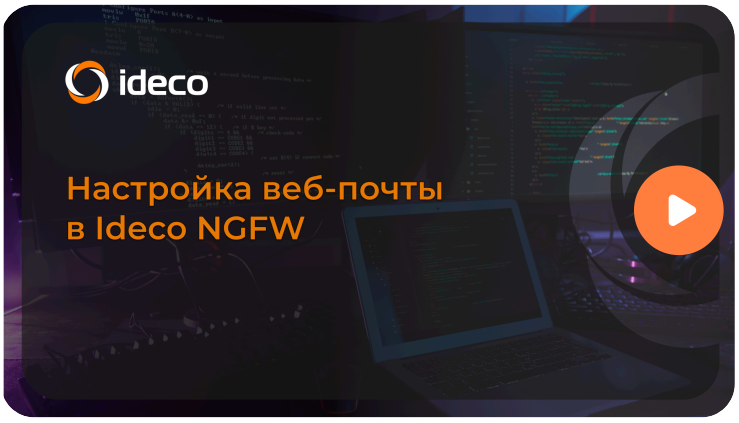
Функциональность доступна только в **Системном контексте**.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

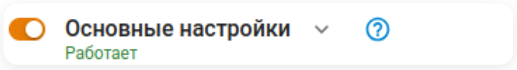
YouTube | RUTUBE | VK Видео



Веб-интерфейс встроенного почтового клиента работает с почтовым сервером по протоколу IMAP и обладает возможностями:

- Создание и отправка писем с поддержкой загрузки нескольких вложений.
- Просмотр, удаление, перемещение письма, а также управление IMAP-папками почтового ящика.
- Персональная (для конкретного ящика) адресная книга, работающая только в рамках веб-приложения.
- Поддержка формата VCARD в адресной книге с возможностью экспорта или сохранения контактов на компьютер.
- Календарь для создания событий и отправки уведомлений сотрудникам по электронной почте.
- Цветные метки писем, аналогично клиенту Thunderbird. Проставляются клавишами от 1 до 5, при этом метки сохраняются на сервере и отображаются в других почтовых клиентах.

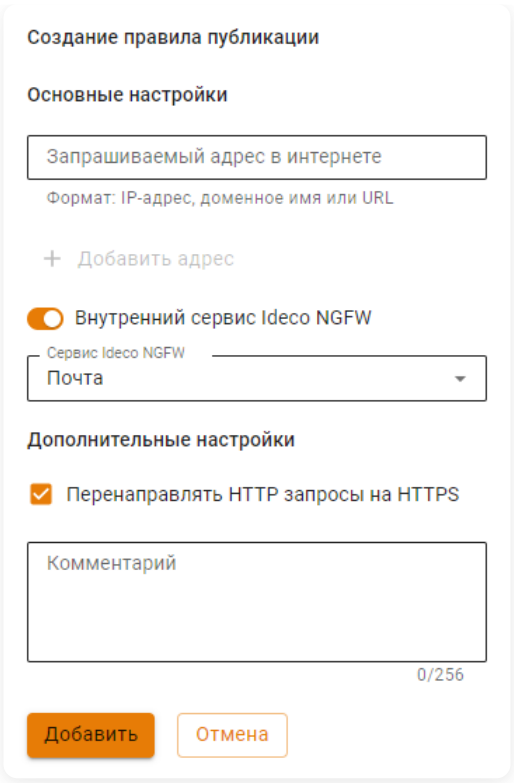
Перед настройкой веб-почты убедитесь, что на Ideco NGFW Novum включен почтовый сервер:



Для работы веб-почты необходимо:

1. Активировать опцию **Web-почта** в **Почтовый релей** → **Основные настройки**.

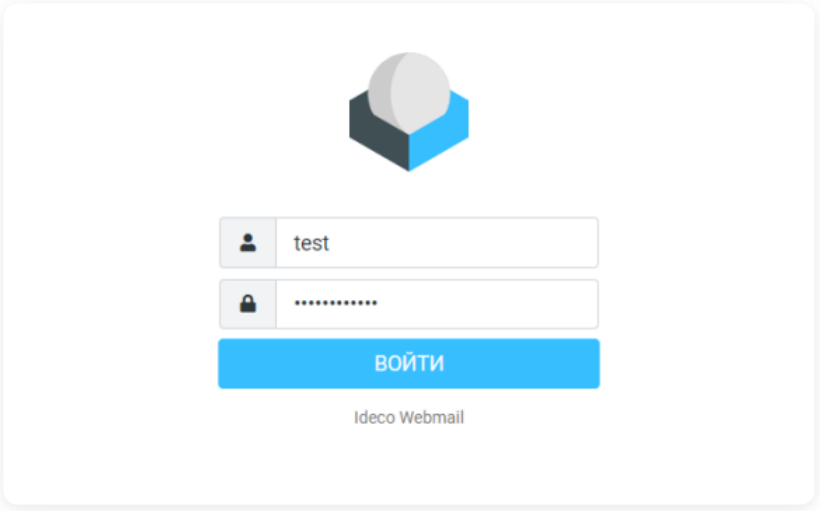
2. Создать и добавить правило публикации в **Сервисы** → **Обратный прокси**:



- В поле **Запрашиваемый адрес в интернете** введите домен, IP-адрес или URL, по которому должна быть доступна веб-почта (например, `webmail.example.com`, `192.168.100.40` или `192.168.100.20/webmail`).
- Включите опцию **Внутренний сервис Ideco NGFW Novum**.
- В качестве сервиса выберите **Почта**.
- В блоке **Дополнительные настройки** включите опцию **Перенаправлять HTTP запросы на HTTPS**.

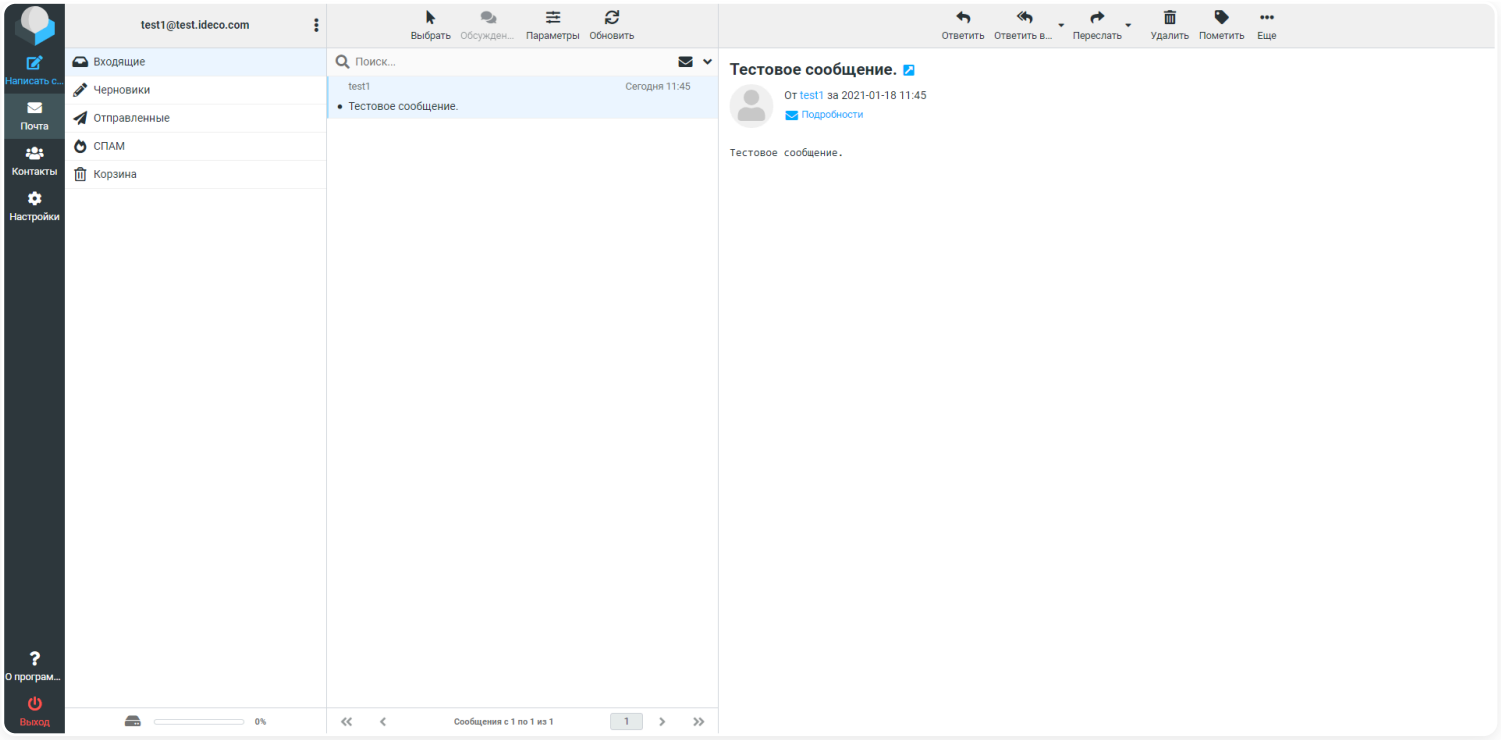
- Чтобы пользователи имели доступ к веб-почте из внешней сети, в правиле публикации в поле **Запрашиваемый адрес в интернете** укажите **белый IP-адрес или зарегистрированный домен**.
- Для подключения обязательно используйте HTTPS.
- С версии 17 Ideco NGFW Novum веб-почта не доступна через `IP-адрес_или_домен_веб-интерфейса:8443/webmail`, так как не связана с административным веб-интерфейсом NGFW.

После создания правила из локальной или внешней сети в браузере наберите: `https://<IP-адрес>`, `https://<домен>` или `https://<URL>`:



- В качестве логина укажите логин от учетной записи пользователя.
- В качестве пароля пропишите пароль от учетной записи пользователя. **Установить отдельный пароль на почту нельзя.**

При успешном входе в браузере откроется веб-интерфейс почтового ящика пользователя:



В правом верхнем углу в разделе **Еще...** находится расширенный поиск по всем письмам ящика.

Настройка почтового релея

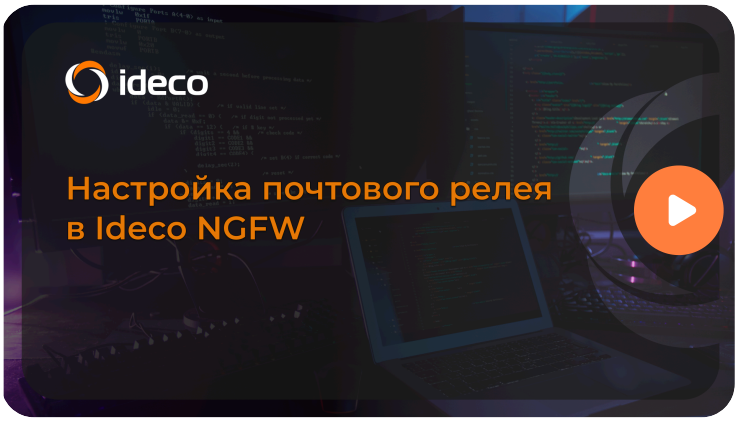
Функциональность доступна только в **Системном контексте**.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Работа в режиме открытого почтового релея невозможна, поэтому Ideco NGFW Novum в режиме Relay может принимать почту только в следующих случаях:

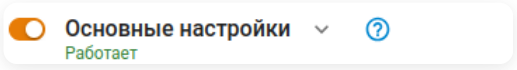
- Когда почта адресована исключительно указанному Relay-домену.
- Из сетей, которые входят в список доверенных в **Почтовый релей** → **Расширенные настройки** → **Безопасность**.

Остальная почта будет отвергнута сервером.

Все почтовые домены должны быть ассоциированы с внешним адресом сервера Ideco NGFW Novum (A- и MX-записи в DNS-зоне).

NGFW Novum не поддерживает кириллические почтовые домены.

Перед настройкой почтового релея убедитесь, что на Ideco NGFW Novum включен почтовый сервер:



Настройка пересылки почты

Для пересылки почты с почтового сервера в локальной сети через Ideco NGFW Novum выполните действия:

Входящая

1. Перейдите в **Почтовый релей** → **Основные настройки** и заполните поля **Основной почтовый домен** и **Имя хоста почтового сервера**:

Основной почтовый домен Ideco NGFW Novum и имя хоста почтового сервера должны отличаться от Relay-доменов. Если Ideco NGFW Novum используется только в режиме Relay:

- В поле **Основной почтовый домен** укажите любой валидный несуществующий домен.
- В поле **Имя хоста почтового сервера** укажите реальное доменное имя с соответствующими DNS-записями.

2. Заполните поле **Relay-домены** в формате `corp-domain.ru|10.20.30.40`:

- `corp-domain.ru` - почтовый домен, зарегистрированный в интернете на публичный адрес Ideco NGFW Novum.
- `10.20.30.40` - адрес почтового сервера в локальной сети.

3. Если требуется проверка почты на спам и вирусы, перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

Исходящая

Для пересылки исходящей почты дополнительных настроек на стороне NGFW Novum не требуется, но почта не будет проверяться на спам и вирусы. Если нужна такая проверка, выполните действия:

1. Перейдите в **Почтовый релей** → **Основные настройки** и заполните поля **Основной почтовый домен** и **Имя хоста почтового сервера**:

2. Перейдите в **Почтовый релей** → **Расширенные настройки** → **Безопасность** и укажите в поле **Доверенные сети** адрес почтового сервера для подключения к NGFW Novum:

3. Перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

4. На почтовом сервере клиента в настройках отправки исходящей почты по протоколу SMTP укажите внешний IP-адрес Ideco NGFW Novum.

Настройка доступа почтовых клиентов

Доступ из внешней сети

Для подключения почтовых клиентов из внешней сети, перейдите в **Правила трафика** → **Межсетевой экран** → **DNAT**, создайте и включите правило проброса портов, используемых вашим почтовым сервером для клиентских подключений: POP3(S), IMAP(S), SMTPS (465), SUBMISSION (587):

Расшифровка полей

- **Протокол** - укажите TCP.
- **Назначение**:
  - **Адрес** - внешний IP-адрес Ideco NGFW Novum.
  - **Порты назначения** - порты, которые использует ваш почтовый клиент: POP3, IMAP, SMTPS (465), SUBMISSION (587), POP3S или IMAPS.
  - **Сменить IP-адрес назначения** - IP-адрес почтового сервера в локальной сети.
- **Действие** - DNAT.
- **Дополнительно** - включите правило.

SMTP, в отличие от SMTPS, нельзя пробрасывать через DNAT, так как трафик не попадет на почтовый релей и поэтому:

- Не пройдет проверку Антиспамом.
- Не будет направляться на нужный почтовый сервер в сети, если серверов несколько.

Доступ по VPN

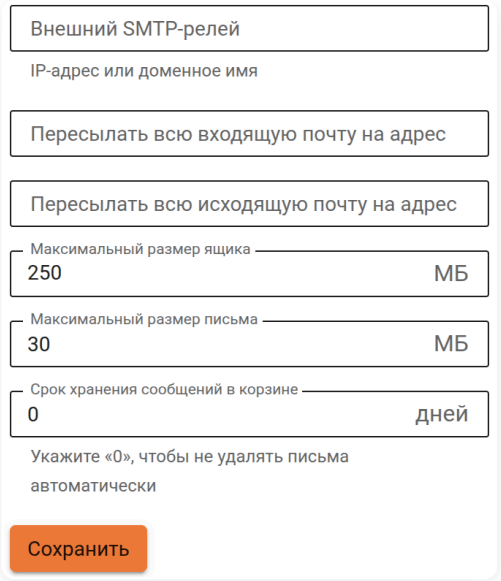
Пользователи смогут подключаться к почтовому серверу по IP-адресу почтового сервера в локальной сети.
Убедитесь, что VPN-подключение корректно настроено и есть разрешающее правило доступа.

Расширенные настройки

Функциональность доступна только в **Системном контексте**.

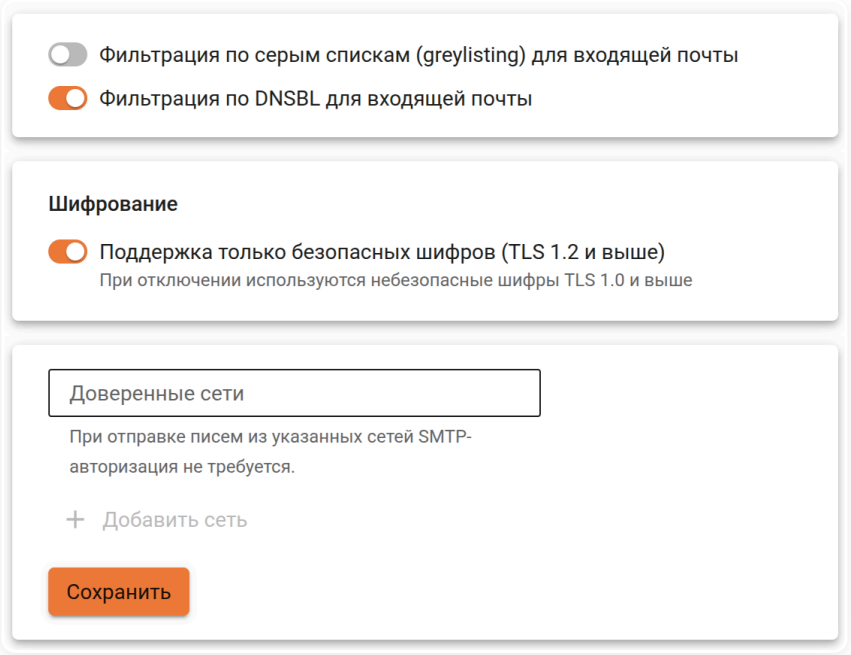
Раздел **Расширенные настройки** состоит из трех подразделов: **Основное, Безопасность, DKIM-подпись**.

Основное



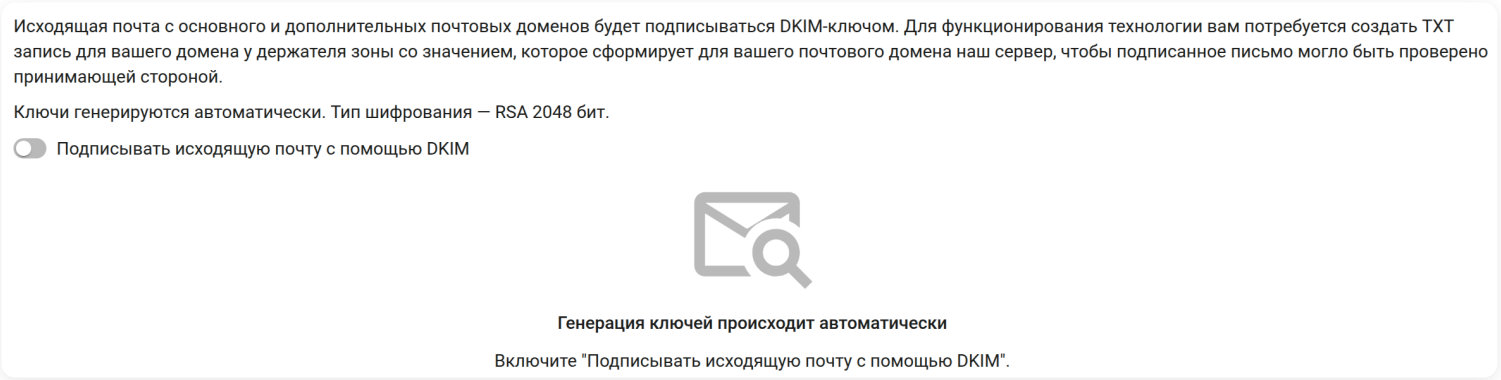
- **Внешний SMTP-релей.** Вся исходящая почта будет отправляться на указанный адрес. Используется, например, если почта должна проходить через вышестоящий сервер провайдера перед отправкой в интернет.
- **Пересылать всю исходящую почту на адрес.** Вся исходящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости.
- **Пересылать всю входящую почту на адрес.** Вся входящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости.
- **Максимальный размер ящика.** Ограничение на максимальный размер почтового ящика в Мбайтах (**100 ГБ - максимальное значение**).
- **Максимальный размер письма.** Ограничение на максимальный размер формируемого сервером письма в Мбайтах (**150 МБ - максимальное значение**).
- **Срок хранения сообщений в корзине.** Количество дней, в течение которых почта хранится в корзине перед удалением. Максимальный срок хранения - 60 дней.

Безопасность



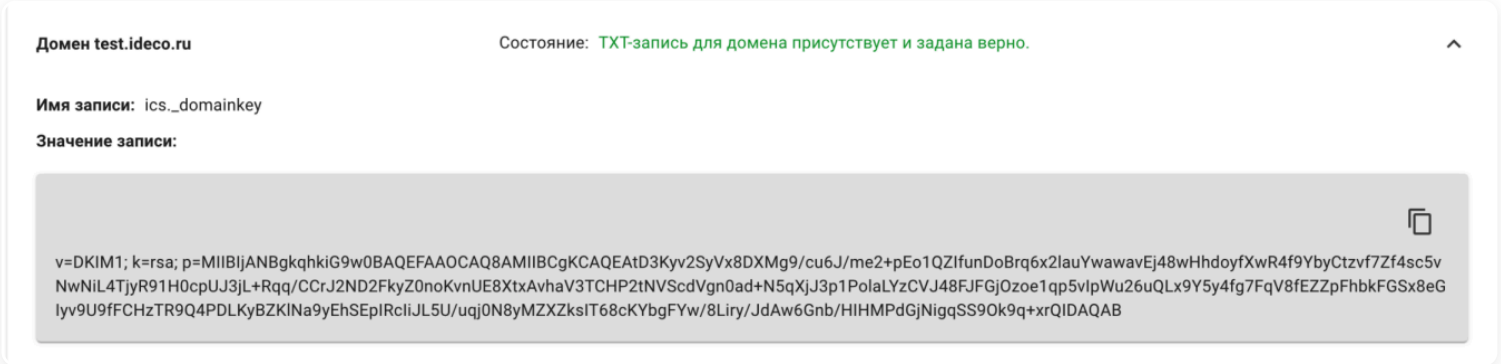
- **Фильтрация по серым спискам (greylisting) для входящей почты.** Включает фильтрацию по серым спискам (greylisting) для входящей почты. При этом почта от неизвестных доменов отправителей может приходить с небольшой задержкой.
- **Фильтрация по DNSBL для входящей почты.** Включает фильтрацию по DNSBL для входящей почты.
- **Поддержка только безопасных шифров (TLS 1.2 и выше)**. При отключении используются небезопасные шифры TLS 1.0 и выше.
- **Доверенные сети.** Авторизация на сервере для доступа к почтовому ящику не требуется при попытке доступа из этих сетей. Указываются IP-сети и хосты в нотации CIDR или с префиксом сети, например, `10.0.0.5/255.255.255.255` или `192.168.0.0/16`.

DKIM-подпись



Настраивается в **Почтовый релей → Расширенные настройки → DKIM-подпись.** Подписывает исходящую с сервера корреспонденцию уникальной для почтового домена подписью так, что другие почтовые серверы в сети интернет могут убедиться, что почта легитимна и заслуживает доверия.

Для функционирования технологии потребуется создать TXT-запись для домена у держателя зоны со значением, которое сформирует для этого почтового домена наш сервер. TXT-записи будут сформированы для основного почтового домена, настроенного на Ideco NGFW Novum, и дополнительных почтовых доменов (если указаны). Сервер также проверит, правильно ли была указана запись и резолвится ли запись в интернет:



Объем TXT-записи достаточно велик и многие регистраторы/держатели зон испытывают сложности с предоставлением интерфейса клиентам для указания TXT-записей длиннее 255 символов. Зачастую регистраторы/держатели зон предоставляют возможность указания TXT-записей длиной до 256 символов, согласно стандарту RFC1035. Но другой стандарт, RFC4408, предполагает объединение строк в случаях, когда нужно использовать длинные TXT-записи при настройке SPF и DKIM. Оперируйте этой информацией в диалоге с держателем доменной зоны. Как правило, держатели зон находят способ создания длинных TXT-записей.

Подпись содержит сочетание кавычек (кавычка-пробел-кавычка: **" "**).

Если хостинг не воспринимает такой формат записи, удалите эти символы.

Настройка домена у регистратора/держателя зоны

Для создания почтового сервера потребуется доменное имя. Зарегистрируйте доменное имя у интернет-провайдера или напрямую у регистратора, например, в RUcenter.

После того как было зарегистрировано доменное имя, потребуется внести изменения в описание зоны на DNS-сервере (у держателя доменной зоны, которой зачастую является регистратор).

1. Создайте ресурсную запись типа A с именем для почтового сервера в домене, указывающую на внешний IP-адрес Ideco NGFW Novum. **Убедитесь, что на внешнем интерфейсе NGFW назначен публичный адрес, доступный из сети интернет.**

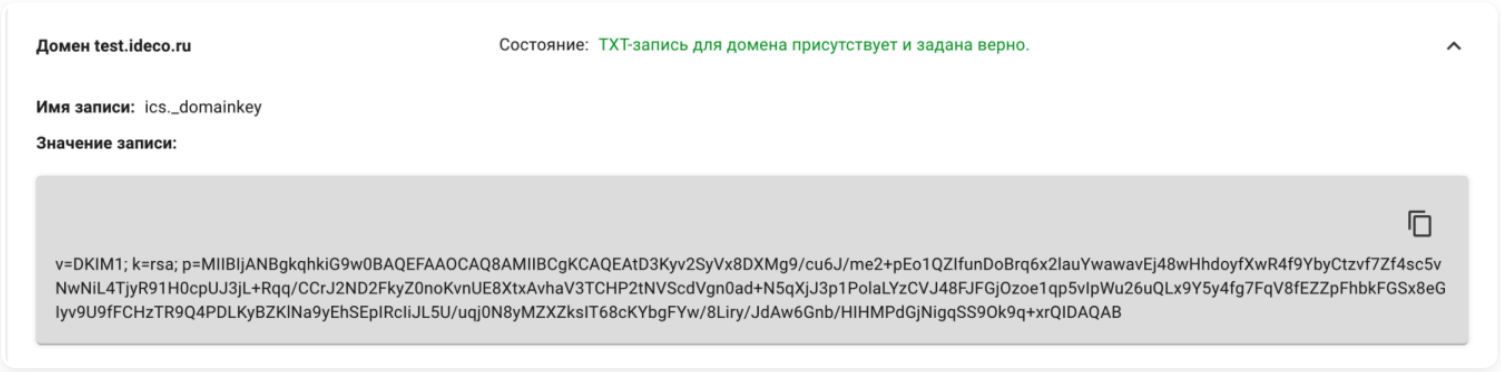
2. Добавьте ресурсную запись типа MX, указывающую на A-запись, которая была создана на предыдущем шаге. MX-запись указывает на сетевой узел, который занимается обработкой почтовых сообщений для домена, и должна ссылаться на доменное имя почтового сервера, а не на IP-адрес.

Рекомендуем:

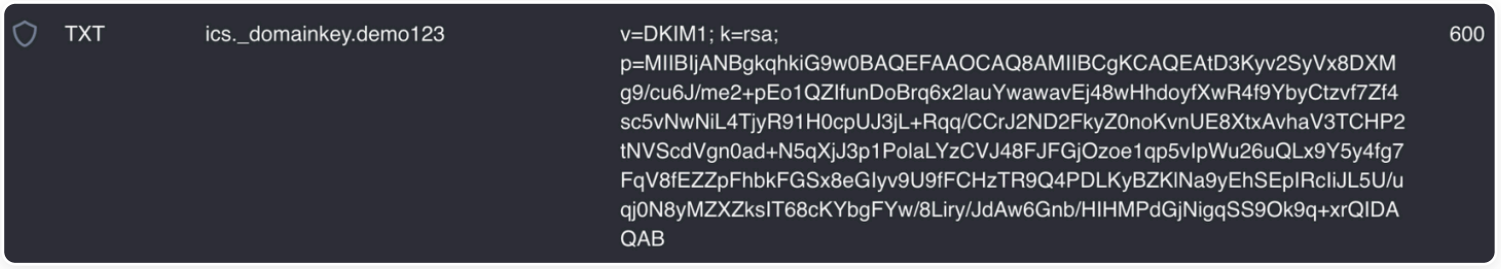
3. Добавить обратную ресурсную запись типа PTR. Эта запись должна быть прописана в файле обратной зоны. Эти изменения должны быть сделаны на стороне интернет-провайдера. Обратитесь к нему с просьбой прописать обратную ресурсную запись для IP-адреса, которая должна ссылаться на запись типа MX.

4. Настроить SPF-запись для почтового сервера.

5. После настройки почтового сервера настроить также DKIM-подпись почтовых сообщений. Для этого перейдите в **Почтовый релей** → **Расширенные настройки** → **DKIM-подпись** и активируйте пункт **Подписывать исходящую почту с помощью DKIM**:



Также создайте TXT-запись для домена у держателя зоны с именем из строки ***Имя записи*** и с содержимым, которое было сформировано Ideco NGFW Novum в **Значение записи**:



Рассмотрим набор необходимых записей на примере вымышленного домена `example.net`:

- A-запись вида: `mail.example.net. IN A 23.45.67.89`, где 23.45.67.89 - это внешний IP-адрес Ideco NGFW Novum.
- MX-запись вида: `example.net. MX 10 mail.example.net`.
- Обратитесь на хостинг для регистрации PTR-записи для нужного IP-адреса вида: `89.67.45.23.in-addr.arpa IN PTR mail.example.net`.
- SPF-запись, объявляющая другим почтовым серверам в интернет, что отправка писем с домена разрешена только с хоста почтового сервера, указанного в MX-записи: `example.net. IN TXT "v=spf1 a mx -all"`.

Синтаксис SPF:

- "v=spf1" - версия SPF, обязательный параметр, всегда spf1, никакие другие версии не работают;
- "+" - принимать письма (по умолчанию);
- "-" - отклонить;
- "~" - "мягкое" отклонение (письмо будет принято, но будет помечено как спам);

- "?" - нейтральное отношение;
- "mx" - включает все адреса серверов, указанные в MX-записях домена;

При использовании почтового сервера на NGFW в качестве почтового релея ресурсные записи будут выглядеть так же, так как в интернете почтовый сервер в локальной сети будет представлен SMTP-релеем на NGFW.

Антиспам и антивирус

Функциональность доступна только в **Системном контексте**.

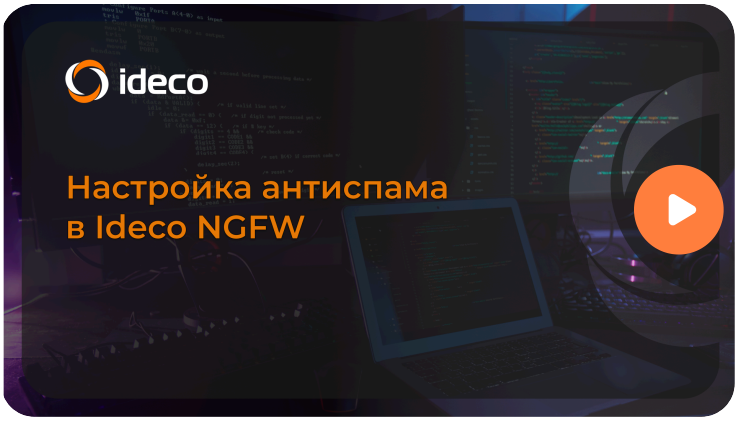
API

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE VK Видео



Раздел **Антиспам и антивирус** состоит из вкладок: **Основное** и **Настройки фильтрации**.

Основное



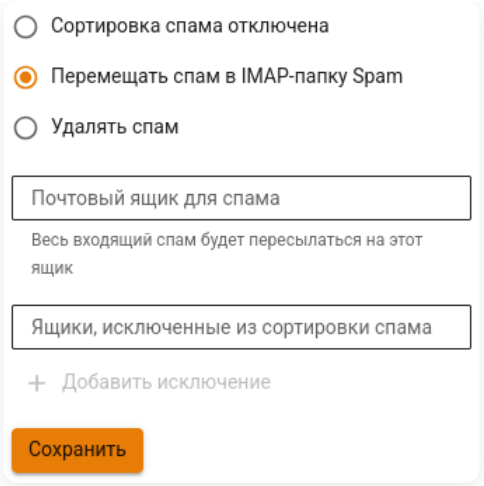
Позволяет управлять работой службы антиспама и антивируса почтового сервера на базе Kaspersky Security for Linux Mail Server с функцией машинного обучения и искусственного интеллекта. Также на вкладке предоставлена возможность добавления лицензионного ключа антиспама. Ключ поставляется в файле, имеющем расширение `.key`.

Если приобретена лицензия на антиспам, но нет в распоряжении лицензионного ключа, проверьте переписку с отделом продаж нашей компании (`sales@ideco.ru`) на наличие вложений. В случае отсутствия вложений запросите ключ заново, выслав письмо на `sales@ideco.ru` с указанием наименования организации или номера лицензии.

Для работы антиспама и антивируса Касперского необходимо включить почтовый сервер. Перед загрузкой ключа обязательно включите модуль **Антиспам и антивирус**.

Настройки фильтрации

Позволяет задать правила обработки и сортировки нежелательных сообщений:



- **Сортировка спама отключена** - отключение сортировки.
- **Перемещать спам в IMAP-папку Spam** - перемещение нежелательных писем в папку Spam, созданную почтовым сервером/релеем. По умолчанию опция включена.
- **Удалять спам** - удаление нежелательных писем с сервера.
- **Почтовый ящик для спама** - пересылка всего входящего спама на указанный ящик. Не указывайте ящик Spam.
- **Ящики, исключенные из сортировки спама** - указание почтовых адресов, которые не будут проверяться на спам.

Правила для разрешенных адресов в Антиспаме формируются автоматически на основе правил, добавленных на NGFW Novum в **Правила** → **Разрешенные адреса**. Адреса, добавленные на вкладке **Запрещенные адреса**, обрабатываются только NGFW Novum.

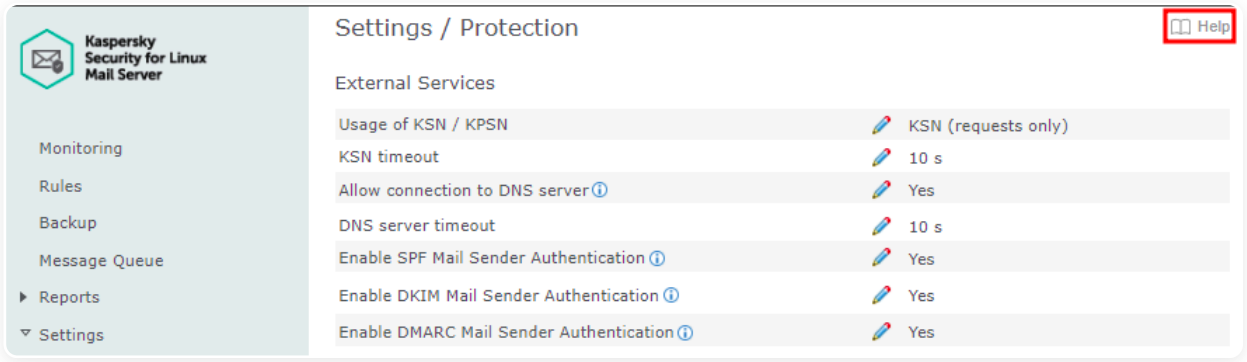
Веб-интерфейс для Антиспама

> Для включения веб-интерфейса Антиспама требуется, чтобы модуль **Антиспам и антивирус** был включен.

Веб-интерфейс имеет следующие преимущества:

- Отображает детальную статистику по категориям Антиспама Касперского.
- Генерирует отчеты по работе за определенный период.
- Отображает очередь обрабатываемых сообщений.
- Ведет аудит всех действий, производимых с Антиспамом.

Документацию по продукту Kaspersky Security for Linux Mail Server можно посмотреть по ссылке. Также перейти в документацию можно через веб-интерфейс, нажав на кнопку **Help**:



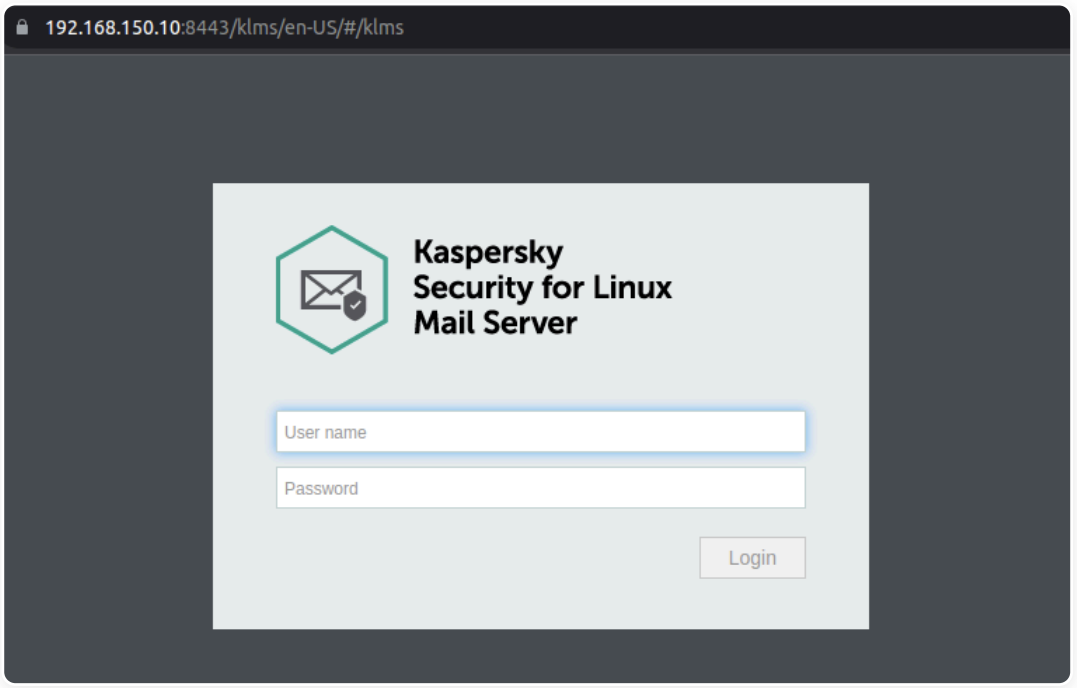
Чтобы включить веб-интерфейс для Антиспама:

1. Перейдите в **Управление сервером** → **Терминал** и выполните команду `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`

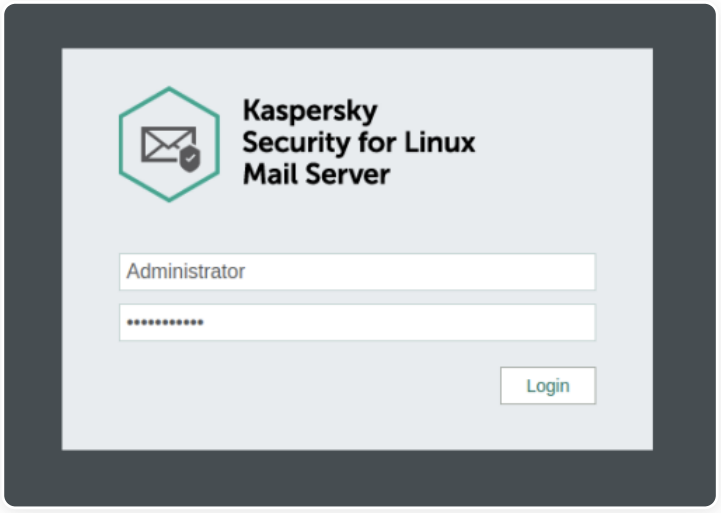
2. Задайте пароль для стандартного аккаунта **Administrator**, состоящий минимум из 8 символов: строчных букв, заглавных букв, специальных символов, чисел:

```
[admin@localhost ~]# /opt/kaspersky/klms/bin/klms-control --set-web-admin-password
Password must satisfy three of four requirements:
       (1) Contains an uppercase letter;
       (2) Contains a lowercase letter;
       (3) Contains a special symbol;
       (4) Contains a number.
       And it must at least contain 8 characters

Enter new WEB console password for Administrator:
Retype new WEB console password for Administrator:
[admin@localhost ~]#
```

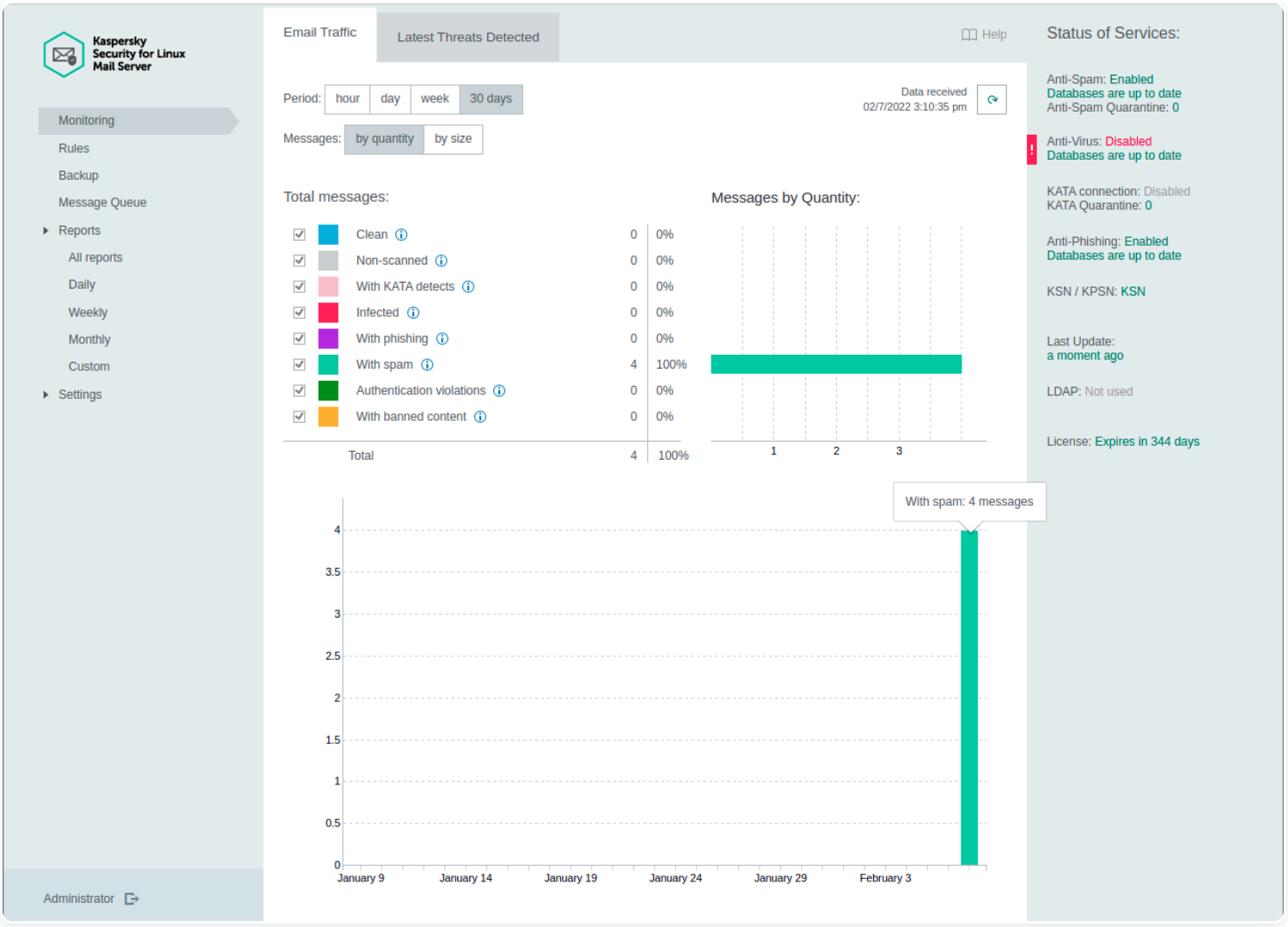
3. Перейдите в адресной строке по пути `ngfw_ip_address:8443/klms/` чтобы получить доступ к веб-интерфейсу:



4. Войдите в веб-интерфейс с учетной записью **Administrator** и ранее заданным в терминале паролем:



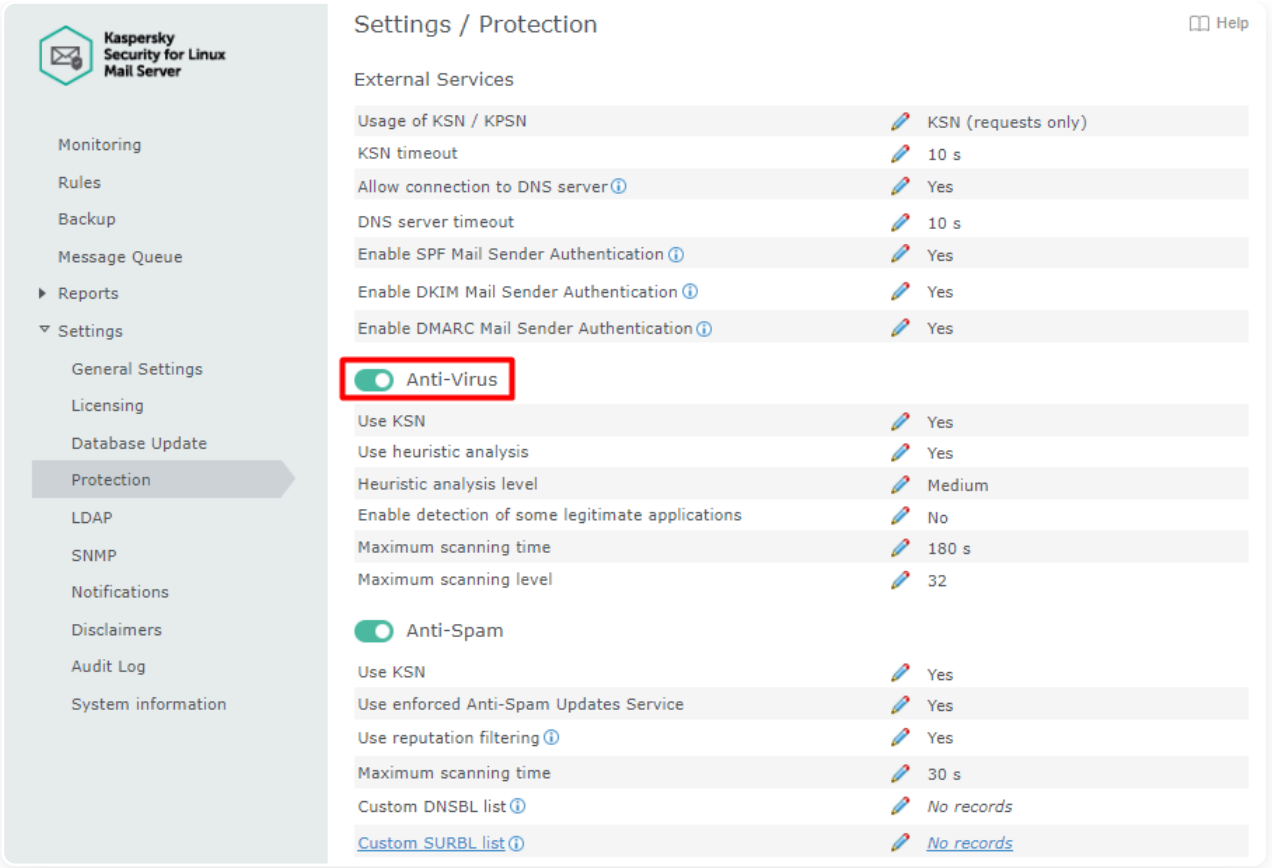
После успешного входа будет отображен дашборд со статистикой работы Антиспама:



Включение Антивируса почтового сервера

1. Перейдите в веб-интерфейс Антиспама.

2. Включите антивирус почтового сервера, перейдите в **Settings** → **Protection** и активируйте опцию **Anti-Virus**:



Службы антиспама и антивируса почтового сервера преднастроены для оптимальной работы в составе Ideco NGFW Novum. Не рекомендуем вносить какие-либо изменения в раздел **Settings**. Веб-интерфейс решения Kaspersky Security for Linux Mail Server предусмотрен только для работы с отчетностью и для внесения изменений, описанных в этой статье.

Правила

API

Функциональность доступна только в **Системном контексте**.

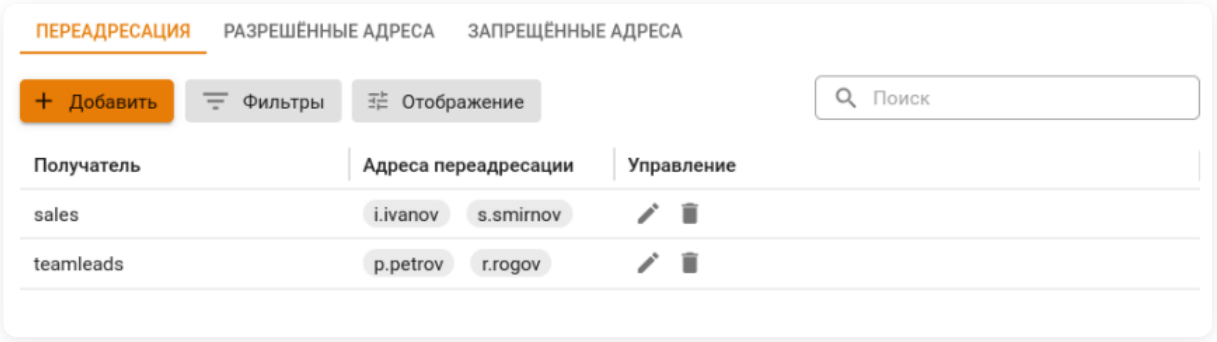
Раздел **Правила** состоит из трех вкладок: **Переадресация, Разрешенные адреса, Запрещенные адреса**. На каждой вкладке доступна фильтрация по кнопке **Фильтры**.

Переадресация

Позволяет настроить переадресацию почты на сервере с помощью почтовых алиасов.

Алиасы, в отличие от почтовых ящиков, не требуют логинов и паролей, алиасы закрепляются за ящиком и служат копией ящика с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, может служить группой рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в графе **Получатель**, должен реально существовать.

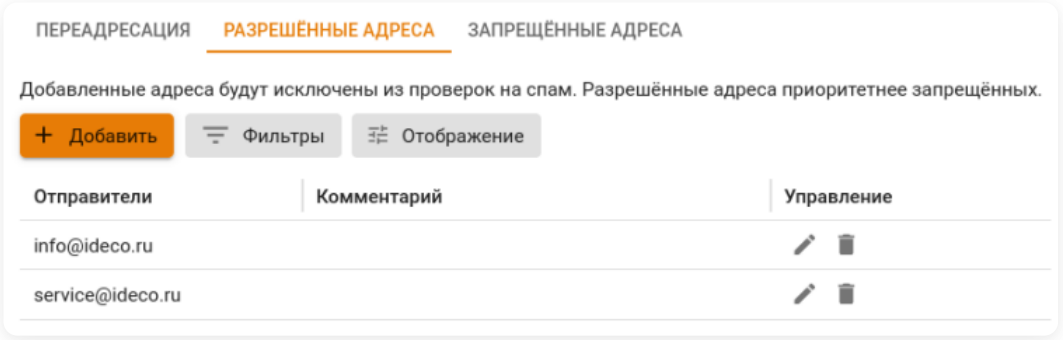
Подробнее с документацией по настройке почтовых алиасов на Ideco NGFW Novum ознакомьтесь в статье Переадресация почты:



Разрешенные адреса

Позволяет указывать почтовые домены, IP-адреса почтовых серверов и почтовые ящики, отправления с которых не будут проверяться на спам.

Если ящик одновременно указан в **Запрещенном адресе** и в **Разрешенном адресе**, то наивысший приоритет имеет **Разрешенный адрес**.



При занесении пересекающихся источников в оба списка корреляции между источниками не происходит. Приоритет будет отдан сначала IP-адресам, затем ящикам и затем доменам. То есть, если запрещен IP-адрес почтового сервера и разрешен домен, который IP-адрес

обслуживает, то письма от него будут блокироваться (блокировка по IP-адресу имеет приоритет). Обратный пример: разрешен IP-адрес, но запрещен домен. Письма блокируются, просто на более поздней стадии, при проверке почтового домена.

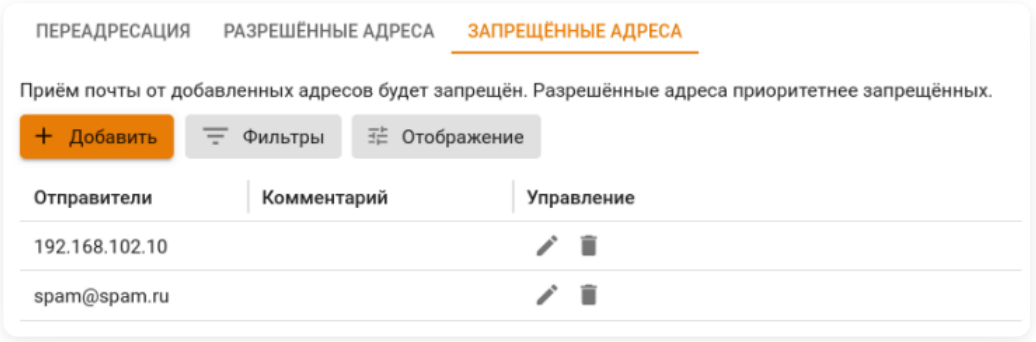
Еще один пример: в **Разрешенные адреса** внесен домен, в **Запрещенные адреса** - ящик из этого домена. Тогда письма с ящика будут заблокированы.

Обратный пример: письма от ящика, занесенного в **Разрешенные адреса**, будут разрешены, даже если домен, которому принадлежит ящик, занесен в **Запрещенные адреса**.

Схема обработки писем в почтовом сервере представлена в статье Схема фильтрации почтового трафика. Обратите внимание, что Разрешенные и Запрещенные адреса срабатывают после нескольких предварительных этапов фильтрации.

Запрещенные адреса

Позволяет указывать почтовые домены и ящики, отправления с которых не будут приниматься сервером:



Переадресация почты

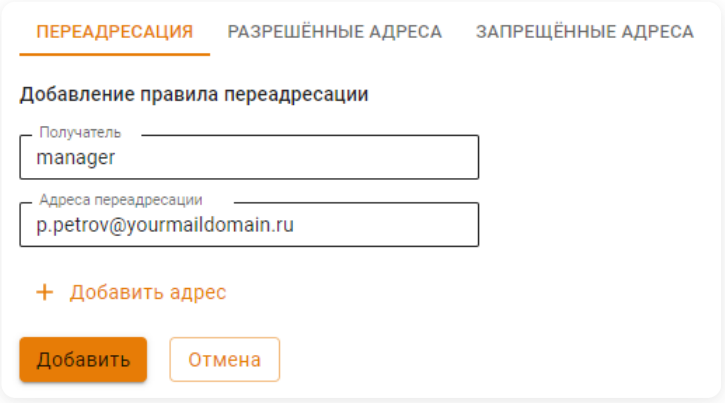
Функциональность доступна только в **Системном контексте**.

Чтобы создавать и редактировать почтовые правила переадресации (алиасы), перейдите в **Почтовый релей → Правила → Переадресация**.

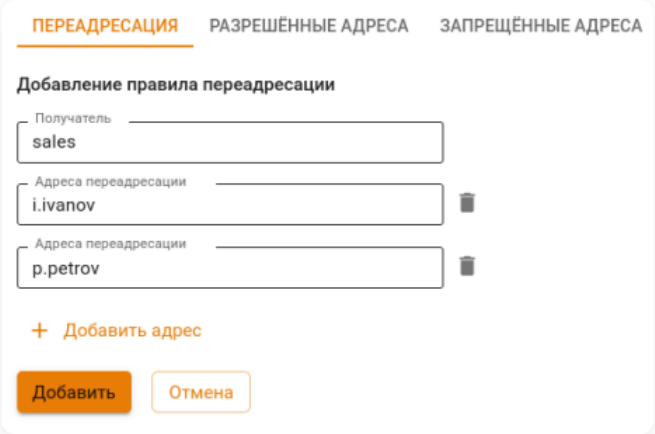
Почтовые алиасы отличаются от почтовых ящиков тем, что не требуют логинов и паролей. Алиасы закрепляются за ящиком и служат копией ящика с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, можно сказать что алиас - это группа почтовых ящиков или группа рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Часть адреса `@yourdomain.com` можно не указывать при создании правил, если ящик расположен на почтовом сервере Ideco NGFW Novum. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в поле **Получатель**, должен реально существовать.

Примеры

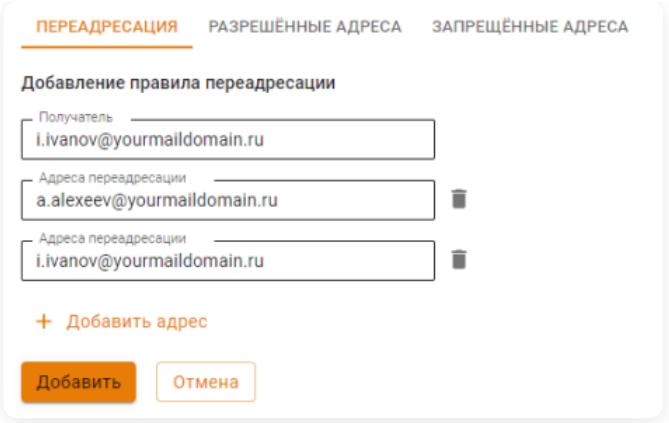
- Создать алиас `manager@yourdomain.ru` для ящика менеджера компании для связи с клиентами и партнерами, у которого реальный почтовый ящик имеет имя `p.petrov@yourmaildomain.ru`:



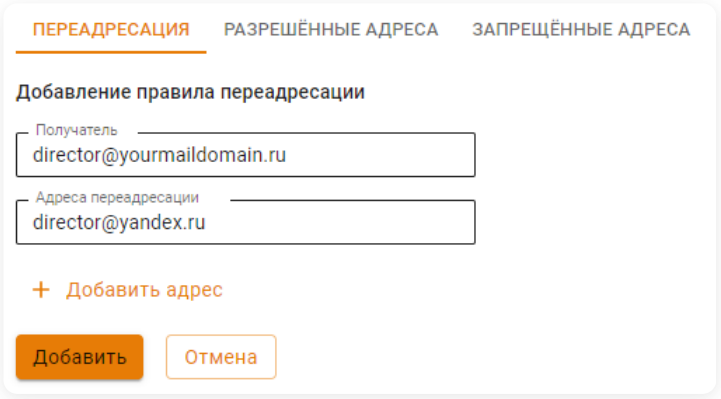
- Создать корпоративный алиас для отдела продаж `sales@yourmaildomail.ru`, чтобы почта пересылалась на всех сотрудников этого отдела:



- Создать временный алиас для переадресации почты сотрудника, который находится в отпуске `i.ivanov@yourmaildomail.ru`, на ящик коллеги `a.alexeev@yourmaildomain.ru` с сохранением почты на ящике `i.ivanov@yourmaildomail.ru`:



- Создать алиас `director@yourmaildomain.ru`, который будет перенаправлять почту на реальный ящик `director@yandex.ru`:



Работа почты при настроенных правилах переадресации

Письма, приходящие на несуществующий ящик (алиас) `manager@yourdomain.ru`, будут попадать на реальный `p.petrov@yourmaildomain.ru`. Также есть алиас для отдела продаж `sales@yourmaildomail.ru`, который, по сути, служит алиасом для рассылки почты и сам писем не хранит. Это удобно, если есть информация для отдела продаж, которую надо распространить на каждого сотрудника. Все то же самое можно сделать, если просто указать в письме всех получателей, но использовать алиас намного удобнее. Также сотрудник с почтой `i.ivanov@yourmaildomail.ru` сейчас находится в отпуске, вся приходящая к нему почта попадает на его ящик и дублируется на `a.alexeev@yourmaildomain.ru`. Последнее правило позволяет директору получать почту не на корпоративный ящик, а на его личную почту на Яндексе.

Алиас не является действительным почтовым ящиком. К нему нельзя подключиться почтовым клиентом, используя логин и пароль, как в обычном почтовом аккаунте. Таким образом, создание алиасов не увеличивает максимально возможное количество реальных почтовых аккаунтов на Ideco NGFW Novum.

Почтовая очередь

API

Функциональность доступна только в **Системном контексте**.

Модуль позволяет управлять входящей и исходящей отложенной корреспонденцией. Для анализа возможных причин задержки корреспонденции в очереди можно использовать информацию из соответствующего столбца таблицы для каждого письма. По кнопке **Фильтры** доступна фильтрация по каждому столбцу.

Почтовая очередь позволяет выполнять следующие выборочные и групповые действия с отправлениями:

- Очистка очереди
- Повторная отправка отдельного письма
- Удаление отдельных писем из очереди
- Повторная отправка всей корреспонденции из очереди

Значение в столбце **Время доставки** соответствует времени поступления письма в очередь. Если письмо не будет отправлено в течение 7 дней, то письмо будет удалено из почтовой очереди и не будет доставлено получателю.

При обновлении Ideco NGFW Novum почтовая очередь очищается.

Проверка настроек почтового сервера

Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса check.smtp.bz.

При правильной настройке почтовый сервер на Ideco NGFW Novum должен получить результат **Отлично**.

Настройка почтовых клиентов

Функциональность доступна в **Системном контексте**.

Примечание

В Ideco NGFW Novum нет ограничений по количеству почтовых клиентов для одного почтового адреса по протоколу IMAP.

Настройка почтового клиента при работе из локальной сети

1. Сервер входящей почты работает на 995 TCP-порту (POP3) и на 143 TCP-порту (IMAP) с шифрованием STARTTLS/SSL:

- В качестве логина прописывается логин от учетной записи пользователя.
- В качестве пароля всегда прописывается пароль от учетной записи пользователя (в том числе для пользователей, импортированных из Active Directory). Задать отдельный пароль на почтовый ящик нельзя.

2. Сервер исходящей почты работает на 587 порту TCP с шифрованием STARTTLS/SSL. Без авторизации возможна отправка почты только из доверенных сетей (настройте доверенные сети в **Почтовый релей** → **Расширенные настройки** → **Безопасность**).

Настройка почтового клиента при работе из внешней сети

Важно

Начиная с версии UTM 7.0.0, подключиться из внешней сети клиентом Microsoft Outlook (любой версии) по протоколу POP3 можно только с типом шифрования SSL. Подключение к почтовому серверу извне без шифрования запрещено.

Остается возможность подключаться по протоколу IMAP с использованием STARTTLS или SSL. Для этого выберите соответствующий тип шифрования в Outlook.

1. Сервер входящей почты работает на 995 TCP-порту (POP3S) и на 143 TCP-порту (IMAP-STARTTLS/SSL), шифрование обязательно:

- В качестве логина прописывается логин от учетной записи пользователя.
- В качестве пароля всегда прописывается пароль от учетной записи пользователя. Задать отдельный пароль на почтовый ящик нельзя.

2. Сервер исходящей почты работает только с авторизацией и шифрованием. Необходимо использовать 587 порт для подключения (а не 25). Тип шифрования, логин и пароль указываются аналогично серверу входящей почты.

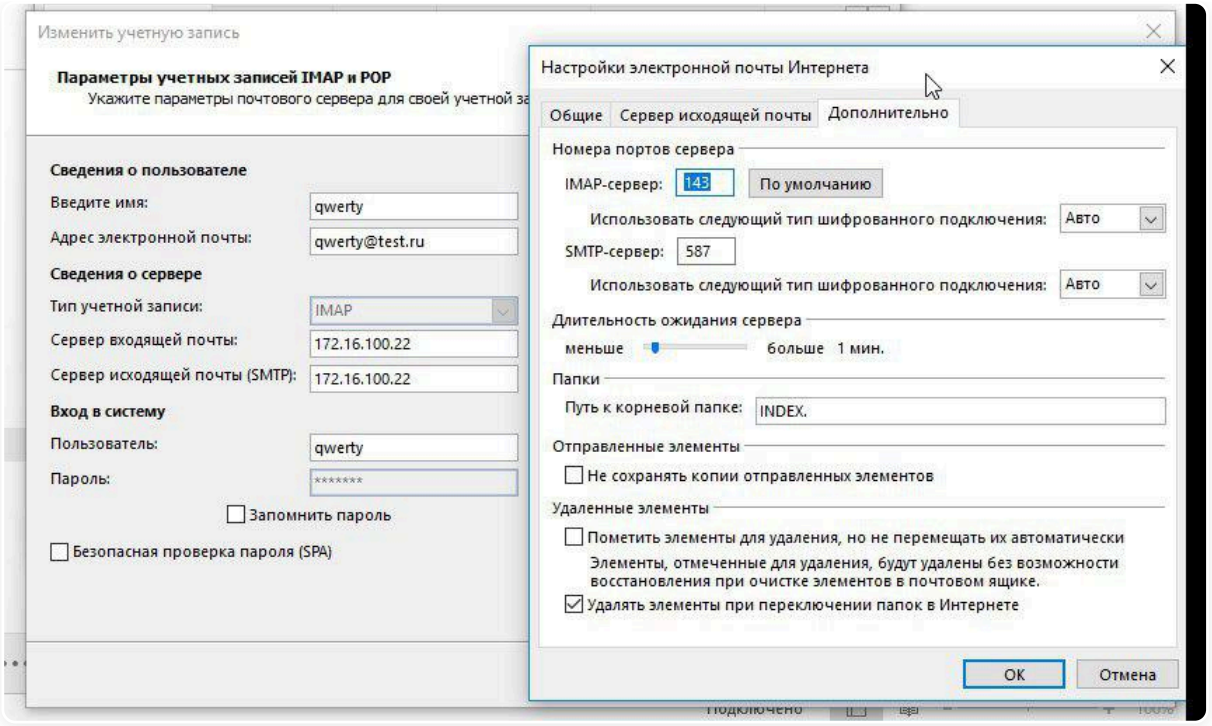
Для любого почтового клиента, кроме веб-почты в составе NGFW, установите корневой сертификат сервера NGFW. Сертификат можно скачать в **Сервисы** → **Сертификаты**.

Примеры настроек популярных почтовых клиентов

Outlook 2013 и 2016

Пример настроек клиента Microsoft Outlook 2013 по протоколу IMAP:

Пример настроек клиента Microsoft Outlook 2016 по протоколу IMAP:



Для отображения IMAP-папок отключите опцию **При просмотре дерева в Outlook показывать только подписанные папки** в свойствах IMAP-папок:

---

iPhone

Установка корневого SSL-сертификат NGFW

1. Скачайте сертификат в **Сервисы** → **Сертификаты** и перенесите на настраиваемое устройство (например, отправив по почте).

2. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством**.

3. Выберите сертификат и нажмите кнопку **Установить**:

4. Зайдите в **Настройки** → **Основные** → **Об этом устройстве** и выберите **Доверие сертификатов**.

5. Включите опцию **Доверять корневым сертификатам полностью**:

Настройка почтового ящика

1. Перейдите в Учетную запись почты и нажмите **Дополнительно**:

2. Скорректируйте настройки:

Thunderbird

1. Перейдите в **Настройки** → **Параметры ученой записи**.

2. Заполните обязательные поля:

- **Имя сервера**.
- **Порт**.
- **Имя пользователя**.
- **Защита соединения**.
- **Метод аутентификации** (рекомендуем указать **Обычный пароль**).

При необходимости заполните **Параметры сервера** и **Хранилище сообщений**.

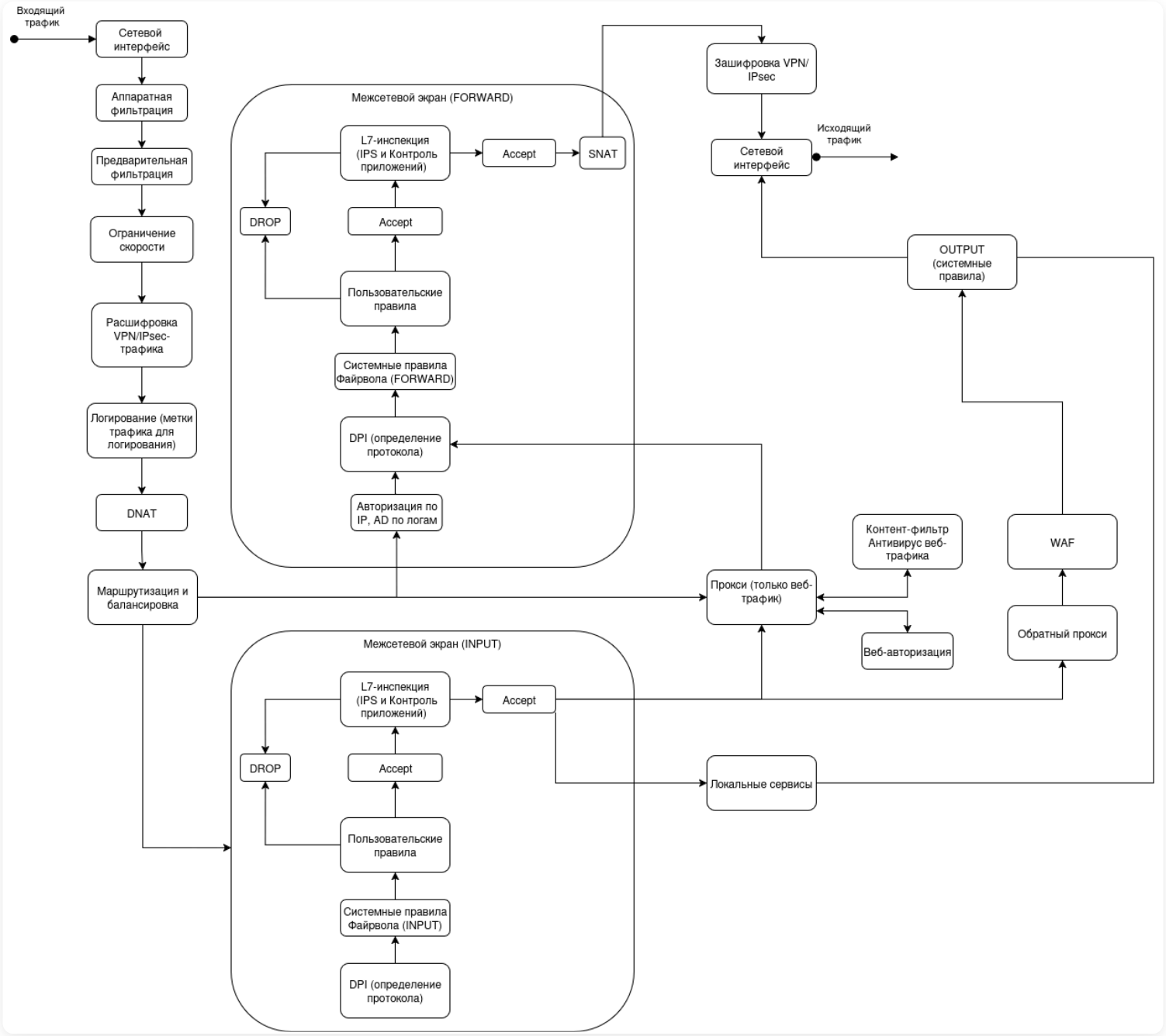
Полный цикл обработки трафика в Ideco NGFW Novum

Классический контекст | Высокопроизводительный контекст

Статья описывает цикл, который проходят пакеты трафика в Ideco NGFW Novum, в зависимости от сценария.

Обработку трафика условно можно разделить на три стадии:

- Предварительная.
- Межсетевой экран.
- Завершающая.



К **Предварительной стадии** можно отнести **Аппаратную** и **Предварительную фильтрацию**.

На второй стадии трафик проходит либо таблицу **INPUT**, либо таблицу **FORWARD** **Межсетевого экрана**:

- В первом случае - одно из двух:
  - Трафик проходит таблицу **INPUT** (пользовательские правила и L7-фильтрацию) и направляется в локальные сервисы NGFW (например, DNS, NTP).
  - Трафик направляется в **Прокси** или **Обратный прокси**, обрабатывается соответствующими модулями и направляется в таблицу **FORWARD** (от **Прокси**) или в **OUTPUT** (от **Обратного прокси**).
- Во втором случае трафик проходит таблицу **FORWARD** (пользовательские правила, L7-фильтрацию, **Прокси** с **Расшифровкой TLS**, **Контент-фильтром** и **Антивирусом**).

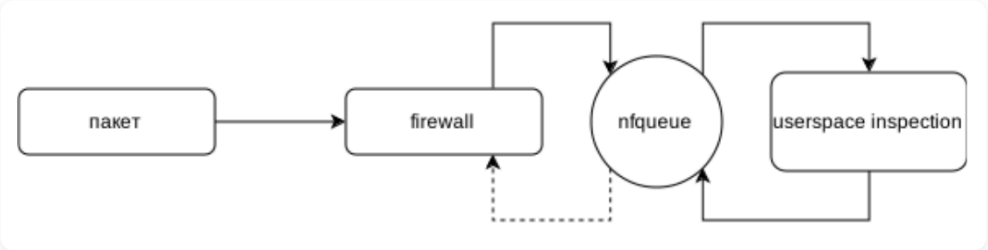
На **Завершающей стадии** трафик после обработки зашифровывается (при необходимости) и направляется получателю.

Принцип работы L7-инспекций

Межсетевой экран работает по принципу stateful-фильтрации - решение о пропуске или блокировке принимается один раз при установлении соединения. L7-инспекции анализируют каждый пакет в рамках этого соединения и могут инициировать блокировку на любом этапе.

Трафик на обработку **Предотвращением вторжений** из **Межсетевого экрана** передается через NFQUEUE.

NFQUEUE - это технология интеграции межсетевого экрана linux с userspace-процессами, выполняющими инспекцию, которая позволяет выполнять L7-инспекции после L3-правил **Межсетевого экрана**:



Примеры прохождения трафика

Транзит трафика с фильтрацией и прозрачным прокси

1. Трафик пользователя попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию**, **Ограничение скорости** (если трафик подпадает под правила, то может быть заблокирован и дальше не пойдет).

2. Если пользователь подключился через VPN, трафик будет расшифрован.

3. Будет проверена DNAT-таблица **Межсетевого экрана**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

4. Веб-трафик направляется в **Прокси** для веб-авторизации, проверки **Контент-фильтром** и **Антивирусом веб-трафика**.

5. Трафик направляется в **FORWARD**-таблицу **Межсетевого экрана**:

- Если трафик подпадает под запрещающее правило, он блокируется.
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию при включенных модулях **Предотвращение вторжений** и/или **Контроль приложений**.

6. Трафик проверяется на соответствие правилам таблицы **SNAT**. При необходимости подменяется IP-адрес источника.

7. Если пользователь подключился через VPN, трафик будет зашифрован.

Прямое подключение к прокси

1. Трафик пользователя попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию**, **Ограничение скорости** (если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет).

2. Будет проверена **DNAT**-таблица **Межсетевого экрана**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT**, веб-трафик оттуда захватывается **Прокси**, где обрабатывается **Контент-фильтром** и **Антивирусом веб-трафика**. Пользователь проходит веб-авторизацию (если веб-авторизация настроена).

4. Трафик направляется в **FORWARD**-таблицу **Межсетевого экрана**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию при включенных модулях **Предотвращение вторжений** и/или **Контроль приложений**.

5. Запрос направляется ресурсу, на который обратился пользователь, ответ направляется пользователю (трафик вновь проходит пункт 1 - пункт 4).

Публикация ресурсов через обратный прокси

1. Трафик из внешней сети попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию** (если трафик подпадает под их правила, то он может быть заблокирован и дальше не пойдет).

2. Будет проверена **DNAT**-таблица **Межсетевого экрана**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT Межсетевого экрана**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию при включенных модулях **Предотвращение вторжений** и/или **Контроль приложений**.

3. Трафик попадает в **Обратный прокси**, где проходит через **Web Application Firewall**. Если трафик подпадает под правила WAF, он может быть отброшен.

4. Трафик направляется ресурсу в локальной сети, который был опубликован через **Обратный прокси**, и возвращает ответ.

Полный доступ

1. Трафик пользователя попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию**, **Ограничение скорости**. Если трафик подпадает под правила - он будет заблокирован и дальше не пойдет.

2. Пользователи могут подключаться через VPN, включая шифрованные подключения.

3. **DNAT**-таблица **Межсетевого экрана** не проверяется: даже если трафик подпадет под правила - IP-адрес или порт назначения не изменится.

4. Трафик, минуя стадию авторизации, пройдет таблицу **FORWARD** и не будет отброшен вне зависимости от созданных там правил фильтрации.

Порядок обработки веб-трафика в Ideco NGFW Novum

Порядок обработки веб-трафика:

1. Ограничение скорости.

2. DNS.

3. Захват трафика для фильтрации (прокси-сервер):

- Контент-фильтр.
- Антивирус веб-трафика.

4. Межсетевой экран.

5. Контроль приложений.

6. Система Предотвращения вторжений.

INPUT-правила Межсетевого экрана обрабатывают трафик раньше DNS (если включен перехват DNS-запросов) и прокси-сервера.

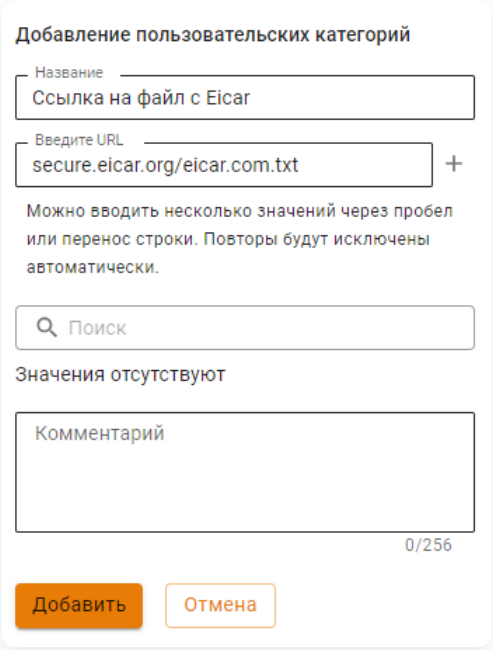
В модули **Контроль приложений** и **Предотвращение вторжений** отправится только трафик, который попадает под разрешающее правило **Межсетевого экрана** с включенной проверкой через профиль контроля приложений и профиль предотвращения вторжений соответственно.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика?

Для примера использовался тестовый файл с Eicar, доступный для скачивания по ссылке.

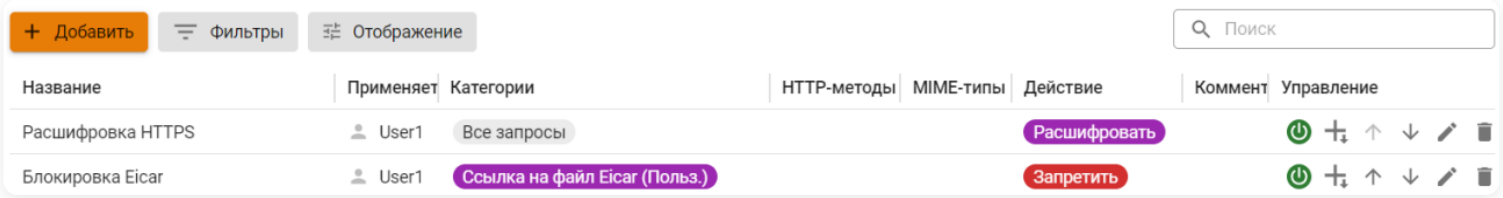
1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Пользовательские категории**. Нажмите **Добавить**.

2. Введите ссылку на ресурс и нажмите + :



3. Перейдите на вкладку **Правила** и создайте два правила для **User1**:

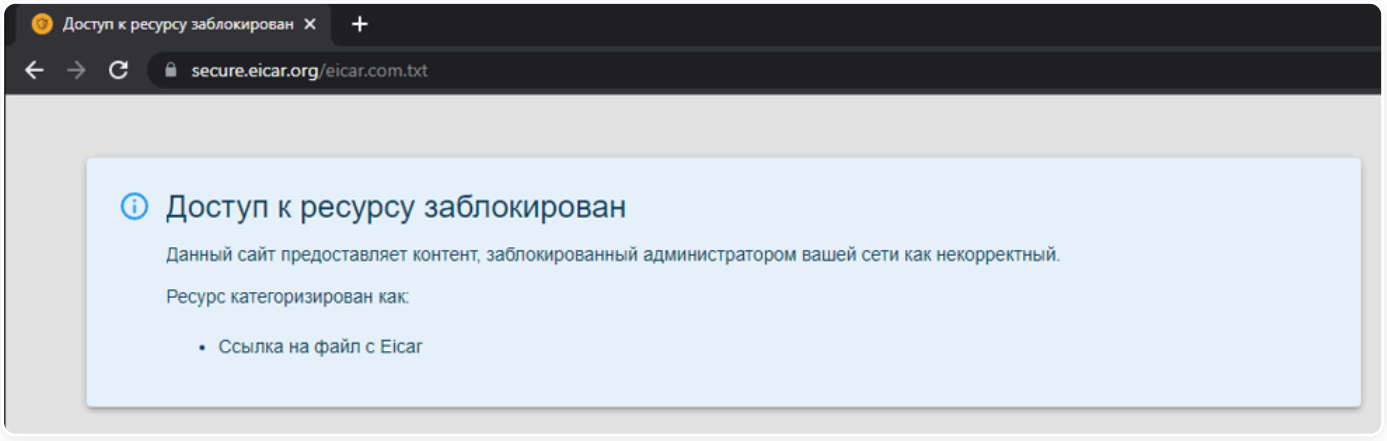
- Правило расшифровки всех HTTPS-запросов, чтобы антивирус мог работать с HTTPS-трафиком.
- Правило блокировки созданной пользовательской категории:



4. Убедитесь, что опция **Антивирус** переведена в положение **Включен**.

5. Авторизуйте пользователя и перейдите по ссылке на скачивание Eicar.

Откроется страница блокировки **Контент-фильтра**:



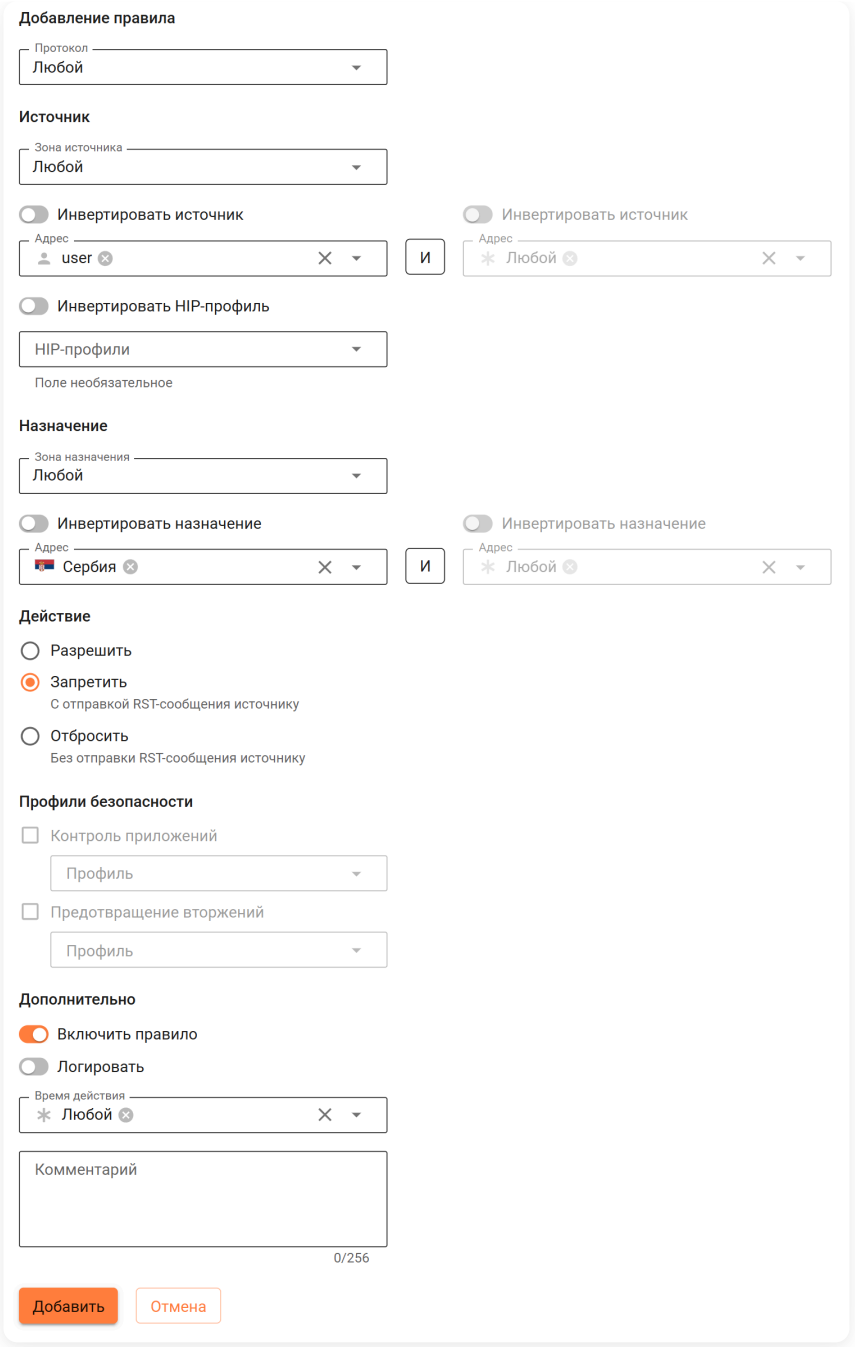
Контент-фильтр обрабатывает трафик приоритетнее, чем антивирусы. Просмотреть информацию о срабатывании правил **Контент-фильтра** можно в **Отчеты** → **Трафик** → **Топ сайтов**.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Межсетевой экран?

Для примера заблокируем пользователю `user` сайт `rts.rs`.

1. Перейдите в **Правила трафика** → **Межсетевой экран**, на вкладку **FORWARD** и нажмите **Добавить**.

2. Заполните поля:

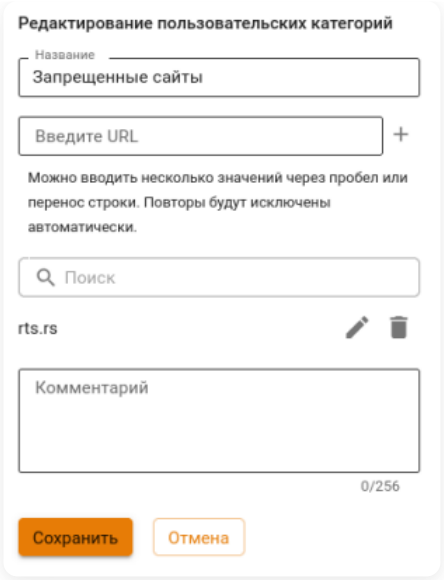


- **Протокол** - выберите **Любой**.
- **Адрес** источника - выберите пользователя `user`.
- **Адрес** назначения - выберите страну **Сербия**.
- **Действие** - выберите **Запретить**.

3. Нажмите **Добавить**.

4. Перейдите в **Правила трафика** → **Контент-фильтр** → **Пользовательские категории** и нажмите на  напротив категории **Запрещенные сайты**.

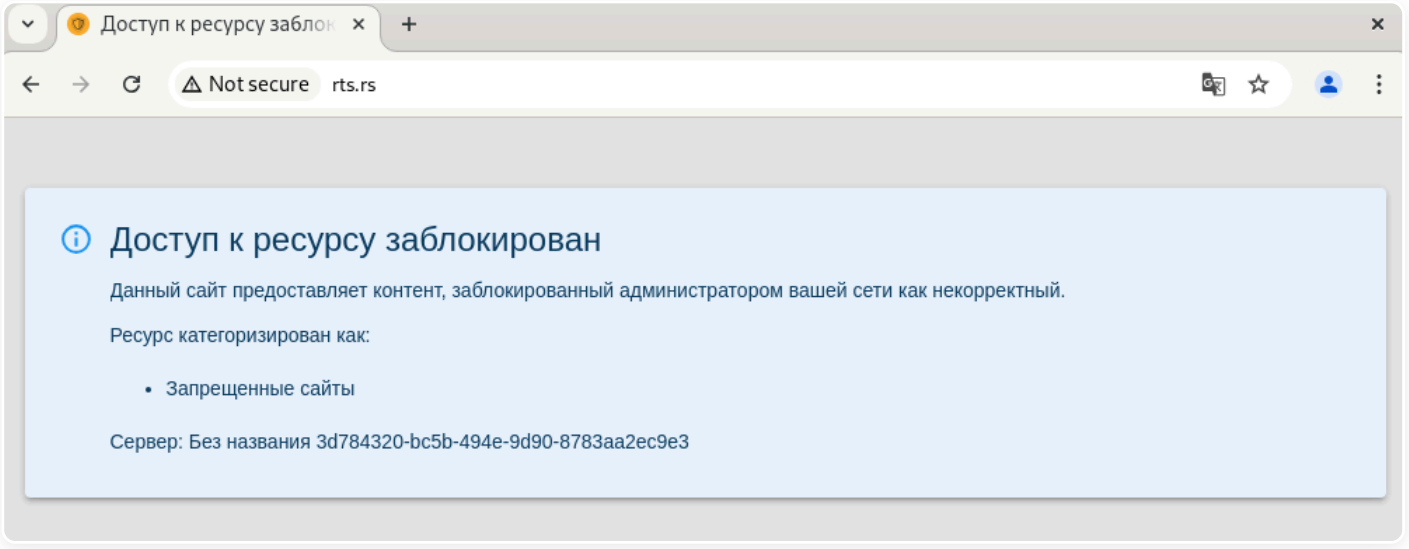
5. Добавьте ссылку на сайт `rts.rs` и нажмите **Сохранить**:



6. Убедитесь, что в таблице правил **Контент-фильтра** включено правило запрета для категории **Запрещенные сайты**.

7. Авторизуйте пользователя и перейдите на сайт `rts.rs`.

Откроется страница блокировки **Контент-фильтра**:



Контент-фильтр обрабатывает трафик приоритетнее, чем **Межсетевой экран**.

В статье представлен полный перечень видеоинструкций по продуктам Ideco

Ссылки на другие ресурсы

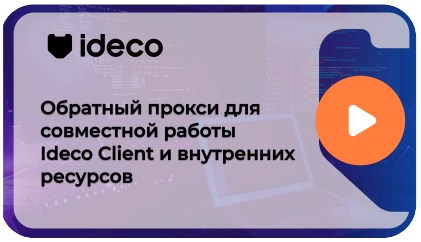
YouTube | RUTUBE | VK Видео



Последние видео







Видеоинструкции NGFW

Список видеоинструкции разбитые по разделам

Пользователи | Правила трафика | Профили безопасности | Сервисы | Маршрутизация | Управление сервером | Почтовый релей

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Вопросы и ответы

Как заблокировать чат-боты?

Заблокировать чат-боты можно, создав правило в Контент-фильтре. О том, как это сделать, написано в статье Блокировка чат-ботов.

Как настроить совместную работу ViPNet-Координатора с Ideco NGFW Novum ?

Процесс настройки подробно описан в статье.

Как настроить автоматическую аутентификацию на Linux через веб-интерфейс ?

Процесс настройки подробно описан в статье Настройка автоматической аутентификации на NGFW на Linux. Скрипт подходит для всех Linux-систем с Python 3.5 и выше.

Есть ли возможность добавлять сигнатуры IPS?

Да, добавьте сигнатуру вручную в файл `/var/opt/ideco/suricata-backend/custom.rules`. Важно: sid правила не должен совпадать с существующими.

Подробнее о добавлении в статье Как исключить узел из обработки системой IDS/IPS через терминал.

Как настроить кластеризацию Active/Active?

Для настройки кластеризации Active/Active воспользуйтесь решением наших партнеров АО "НПП "Цифровые решения". Инструкция по интеграции Ideco NGFW Novum и брокера сетевых пакетов DS Integrity NG - по ссылке.

Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW Novum?

Порядок обработки веб-трафика и примеры проверки работоспособности модулей описаны в статье.

Хочу работать из дома, подключившись по RDP к своем компьютеру в офисе. Можно ли опубликовать RDP, чтобы RDP был доступен из интернета?

Не рекомендуем так делать. В такой ситуации существуют риски успешного взлома с помощью RDP. Даже сложный пароль и актуальные обновления не гарантируют того, что злоумышленники не смогут проникнуть внутрь сети через опубликованный RDP. Не рекомендуем публиковать RDP и подобные сервисы "наружу" (SSH, FTP и т.д.), так как это увеличивает количество потенциальных точек входа для злоумышленников. Рекомендуем использовать подключение по VPN к своей сети.

Как создать VPN-подключение?

В зависимости от операционной системы выберите подходящую инструкцию из Инструкций по созданию VPN-подключений.

Что делать, если ваш IP попал в черные списки DNSBL?

Если используете белый статический IP-адрес, то попадание IP-адреса в черные списки может означать, что в сети зафиксирована бот-активность, участие в DDoS-атаках, либо рассылка спама.

Наличие в черных списках динамического IP-адреса из "домашних" диапазонов IP-адресов провайдеров в целом нормальное явление, т. к. вредоносная активность в таком случае может исходить не из вашей сети.

Порядок действий при попадании в черный список описан в статье.

Утрачен пароль администратора, как восстановить?

При утере пароля администратора можно восстановить, имея физический доступ к серверу. Подробнее о процессе восстановления в статье Как восстановить доступ к Ideco NGFW Novum.

После обновления потребовалось вернуть предыдущую версию со всеми настройками. Как это сделать?

Возможность восстановиться на предыдущую версию после обновления Ideco NGFW Novum доступна с 12.X версий. Подробнее о процессе восстановления в статье Как восстановиться на прошлую версию после обновления Ideco NGFW Novum.

Как подобрать аппаратную платформу для Ideco NGFW Novum?

Ideco NGFW Novum представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW Novum основан на Fedora 42 и содержит ядро Linux с набором драйверов от этой ОС с небольшими изменениями с нашей стороны. Таким образом, Ideco NGFW Novum можно установить на большую часть оборудования, поддерживающего Fedora 42. Подробнее в статье Выбор аппаратной платформы для Ideco NGFW Novum.

Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW Novum?

Для настройки Ideco NGFW Novum воспользуйтесь рекомендациями из статьи Поддержка устаревших алгоритмов шифрования.

Как настроить прямое подключение к прокси-серверу, если ПО его не поддерживает?

При использовании прямых подключений к прокси-серверу выход в интернет будет поддерживаться всеми программами, имеющими настройки прокси-сервера, либо программами, применяющими системные настройки прокси.

Некоторое ПО не имеет настроек прокси-сервера, поэтому необходимо использовать специализированное ПО на конечных рабочих станциях для вывода в интернет таких программ. Одно из таких ПО - Proxifier.

Инструкция по настройке программы Proxifier для прямых подключений к прокси-серверу доступна по ссылке.

Как эффективно заблокировать Ammyy Admin, Анонимайзеры, BitTorrent и т. д.?

Примеры блокировки программ удаленного доступа, анонимайзеров, торрентов и др. описаны в статье Блокировка популярных ресурсов.

Как настроить SSO-авторизацию для Astra Linux в домене AD?

Описание процесса настройки можно найти в статье Настройка прозрачной авторизации на Astra linux. Это решение подходит для браузеров Chromium и Firefox.

Как восстановить Ideco NGFW Novum до первоначальных настроек?

Для возврата к первоначальным настройкам используйте бэкап, созданный после установки Ideco NGFW Novum. Если бэкапа нет - переустановите Ideco NGFW Novum.

Пример настройки Forward-зоны

Как настроить сеть, чтобы пользователи локальной сети могли обращаться к ресурсам, опубликованным на Ideco NGFW Novum. Ресурсы находятся в защищенной сети, и доступ к ним должен осуществляться напрямую, без выхода через внешний интерфейс. Подробнее в статье.

Как публиковать веб-приложения



Функциональность доступна в **Классическом** и **Системном контекстах**.

Публикация веб-серверов возможна через обратный прокси-сервер.

Как настроить публичный IP-адрес на компьютере в локальной сети

Для версии Ideco UTM 7.9.0 и старше настройка публичного IP-адреса для компьютеров, находящихся в локальной сети, невозможна.

Используйте портмаппинг, чтобы пробросить весь диапазон портов от 0 до 65535 для получения эффекта присутствия локального сервера на внешнем IP-адресе.

Практические руководства

Пошаговые инструкции по настройке и использованию возможностей Ideco NGFW

VPN-подключения

Создание VPN-подключений в различных операционных системах и устройствах

Перейти >

Аутентификация

Настройка сертификатов и аутентификации пользователей в Ideco NGFW

Перейти >

Сервисы

Практические руководства по настройке сервисов Ideco NGFW

Перейти >

Правила трафика

Настройка блокировок, межсетевого экрана и фильтрации трафика в Ideco NGFW

Перейти >

SD-WAN

Практические руководства по настройке SD-WAN в Ideco NGFW Novum

Перейти >

Маршрутизация

Практические руководства по настройке маршрутизации в Ideco NGFW Novum

Перейти >

Управление сервером

Практические руководства по управлению сервером Ideco NGFW

Перейти >

Интеграции

Практические руководства по интеграции Ideco NGFW со сторонними решениями

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Пользователи

Практические руководства по настройке VPN-подключений и аутентификации пользователей

VPN-подключения

Инструкции по созданию VPN-подключений на различных операционных системах и устройствах

Перейти >

Аутентификация

Настройка сертификатов, прозрачной авторизации и веб-аутентификации

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Инструкции по созданию VPN-подключений

Создание VPN-подключения в Ubuntu

Перейти >

Инструкция по созданию подключения в Fedora

Перейти >

Инструкция по созданию подключения в Astra Linux

Перейти >

Инструкция по созданию подключения в Windows

Перейти >

Инструкция по созданию VPN-подключения на мобильных устройствах

Перейти >

Инструкция по созданию подключения в Mac OS

Перейти >

Подключение по SSTP Wi-Fi-роутеров Keenetic

Перейти >

Создание VPN-подключения в Alt Linux

Перейти >

Как избежать проблем с подключением VPN-клиентов при нескольких серверах

Перейти >

Подключение Keenetic по SSTP или IPsec

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Создание VPN-подключения в Alt Linux

Функциональность доступна в **Классическом** и **Системном контекстах**.

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее правило для VPN-подключения.

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

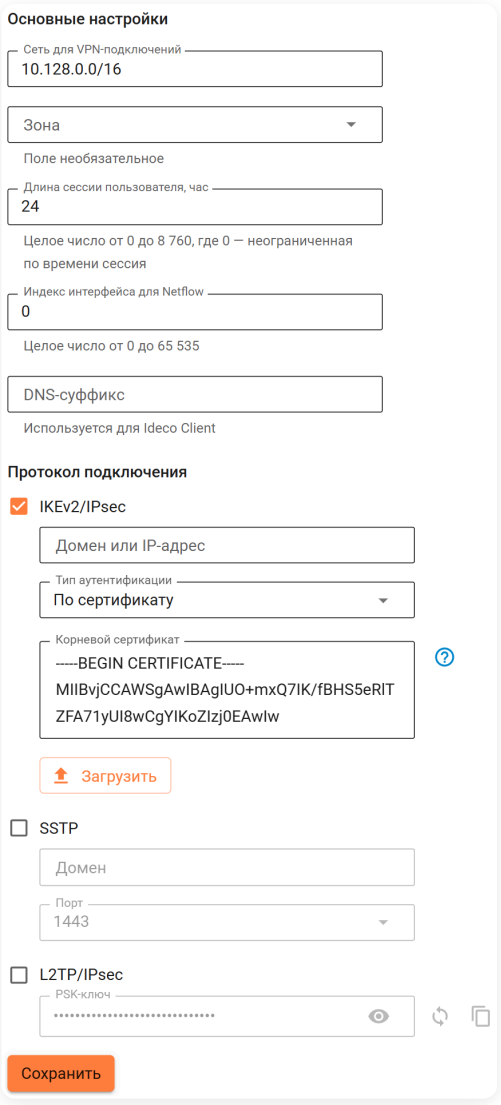
Не рекомендуем использовать для VPN-подключений кириллические логины.

Настройка подключения по протоколу IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Выберите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы → Сертификаты → Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя, нажав **Скачать корневой сертификат**.

Применение сертификатов для VPN-подключений:

- Если сертификат издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority):
  - Убедитесь, что домен указан в поле Subject Alternative Name (SAN).
  - Загрузите сертификат в **Сервисы → Сертификаты → Загруженные сертификаты**, нажав **Загрузить пользовательский сертификат**.

Создание подключения в Alt Linux:

1. Откройте терминал сочетанием клавиш **Ctrl+Alt+T** или из **Меню** и установите необходимые пакеты:

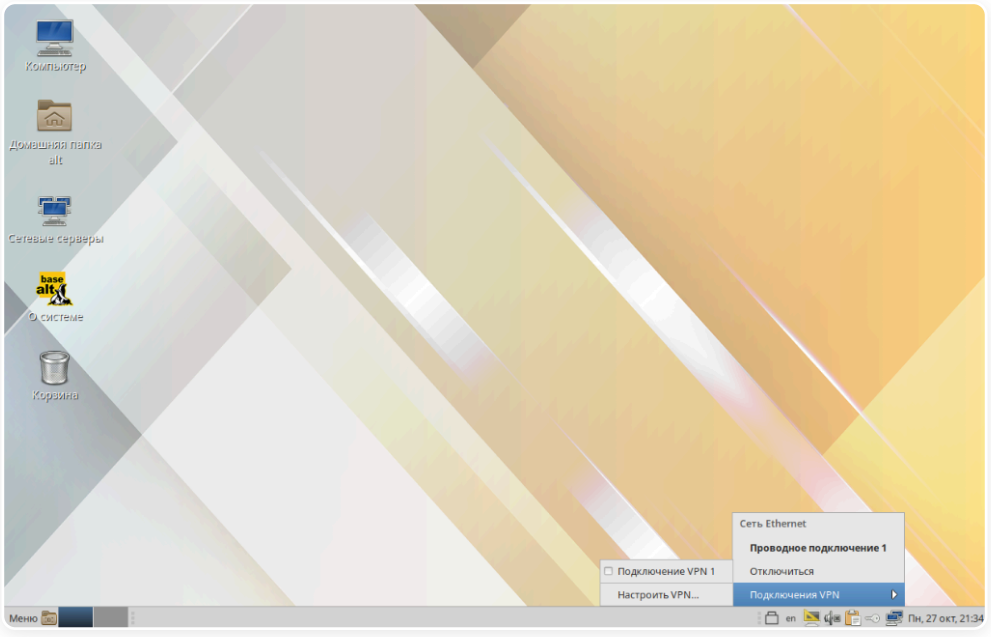
```
apt-get update && apt-get dist-upgrade && apt-get install NetworkManager-strongswan NetworkManager-strongswan-gnome strongswa
```

2. Установите корневой сертификат на рабочую станцию:

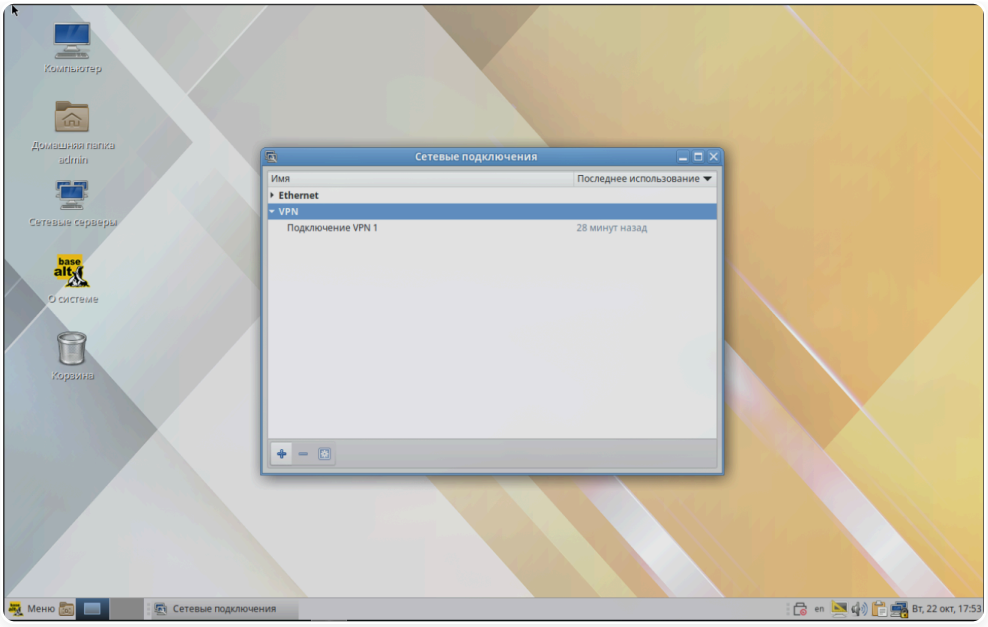
```
cp root-ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

- `root-ca.crt` - расположение сертификата/имя файла сертификата.

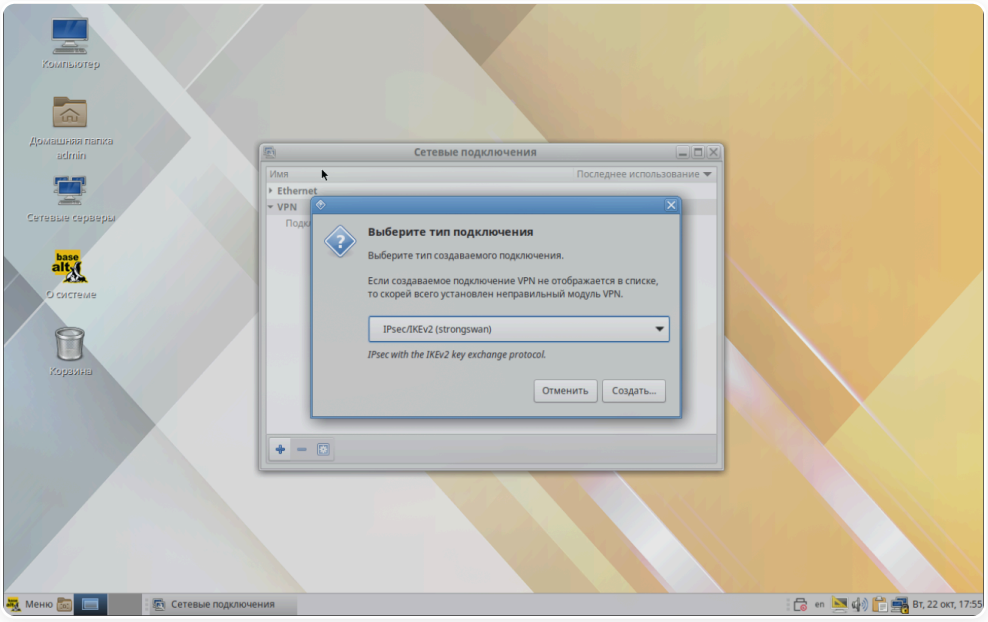
3. Перейдите в **Подключения VPN** и нажмите **Настроить VPN**:



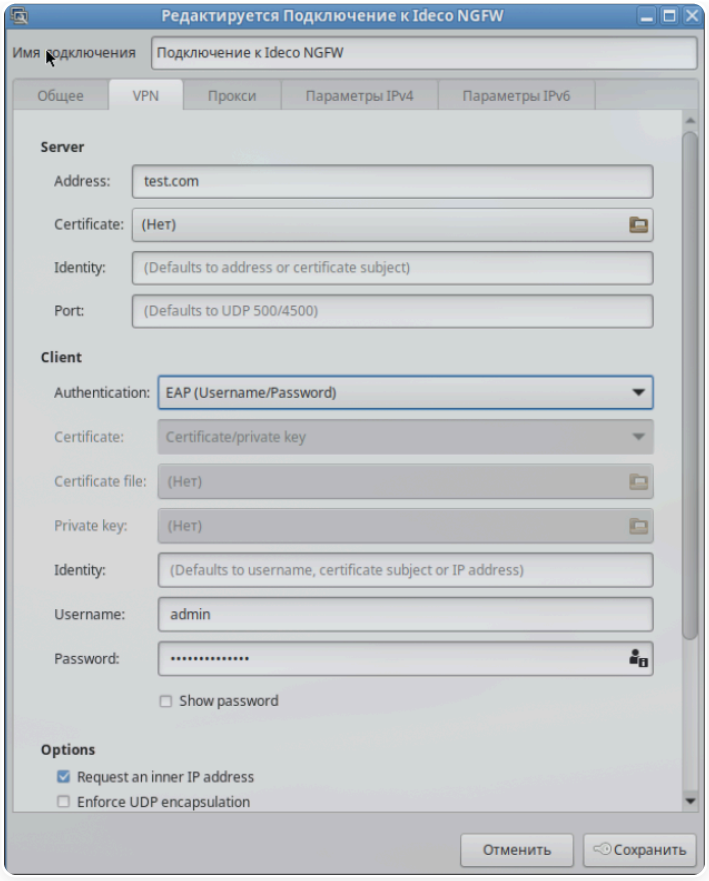
4. Добавьте новое VPN-подключение, нажав :



5. Выберите тип VPN-подключения `IPsec/IKEv2 (strongswan)` и нажмите **Создать**:

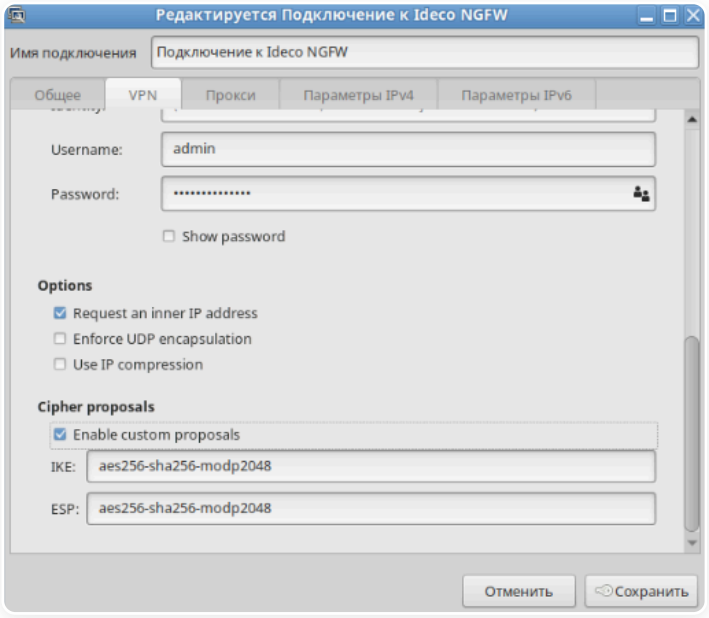


6. Заполните необходимые поля для создания VPN-подключения, как на скриншоте:



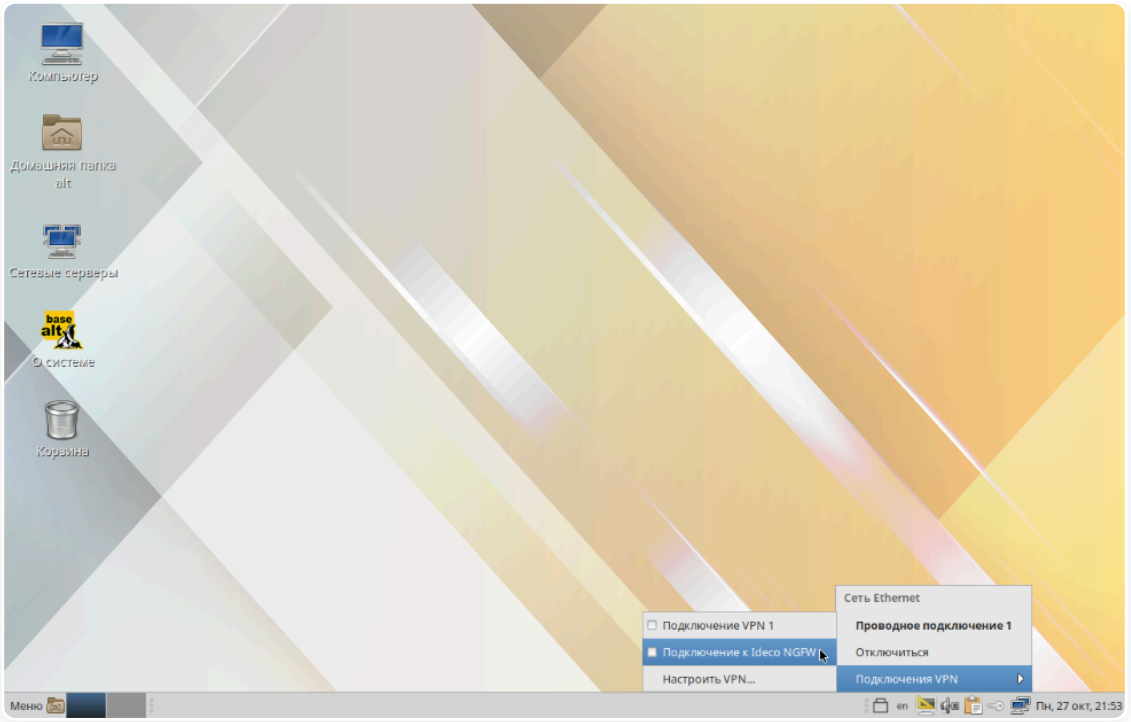
- **Address** - адрес шлюза.
- **Authentication** - тип аутентификации.
- **Username** - логин пользователя в Ideco NGFW Novum.
- **Password** - пароль пользователя в Ideco NGFW Novum.

7. Заполните параметры шифрования, как на скриншоте, и нажмите **Сохранить**:



- В блоке **Options** включите опцию **Request an inner IP address**.
- В блоке **Cipher proposals** включите опцию **Enable custom proposals** и заполните поля:
  - **IKE** - aes256-sha256-modp2048.
  - **ESP** - aes256-sha256-modp2048.

8. Запустите созданное VPN-подключение:



Полезные ссылки

- VPN-подключения

Создание VPN-подключения в Ubuntu

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

Не рекомендуем использовать для VPN-подключений кириллические логины.

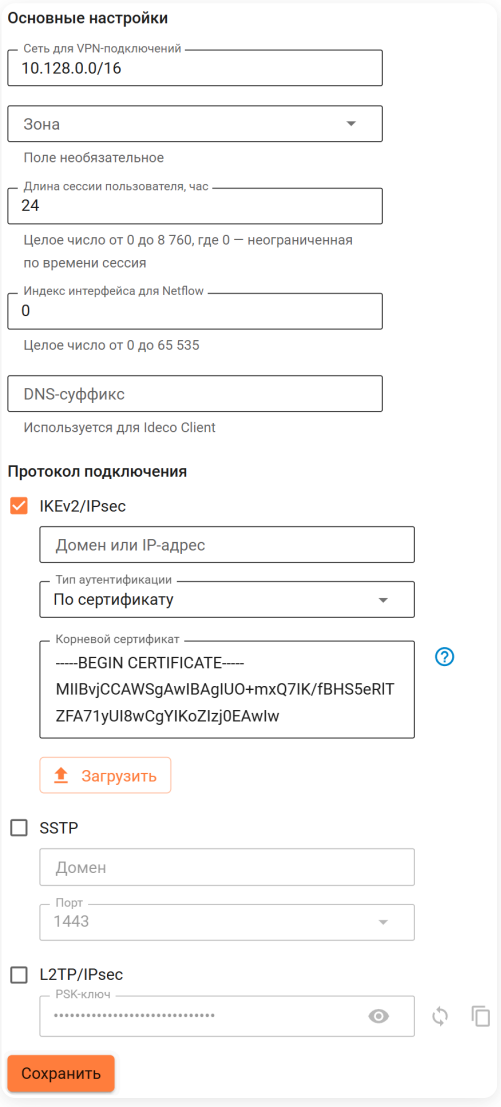
Инструкция актуальна для версии Ubuntu 24.04 LTS.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:

- **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
- **По сертификату** - вход по сертификату пользователя.

- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Ubuntu:

1. Откройте терминал и выполните команду:

```
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-extra-plugins
```

2. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

3. Перейдите в терминале в директорию с загруженным корневым сертификатом (если на доменное имя NGFW выпущен Let`s Encrypt сертификат, сразу перейдите к пункту 6).

4. Установите корневой сертификат NGFW Novum в хранилище доверенных сертификатов Ubuntu:

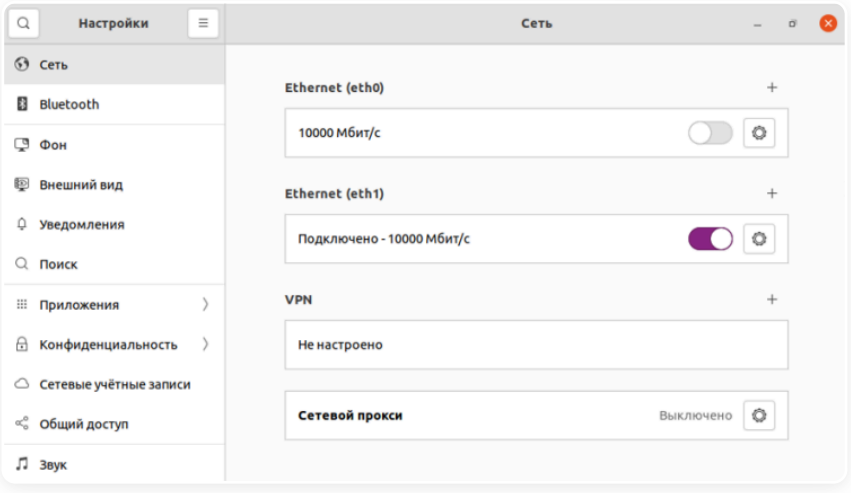
```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

- `ca.crt` - имя скачанного сертификата.

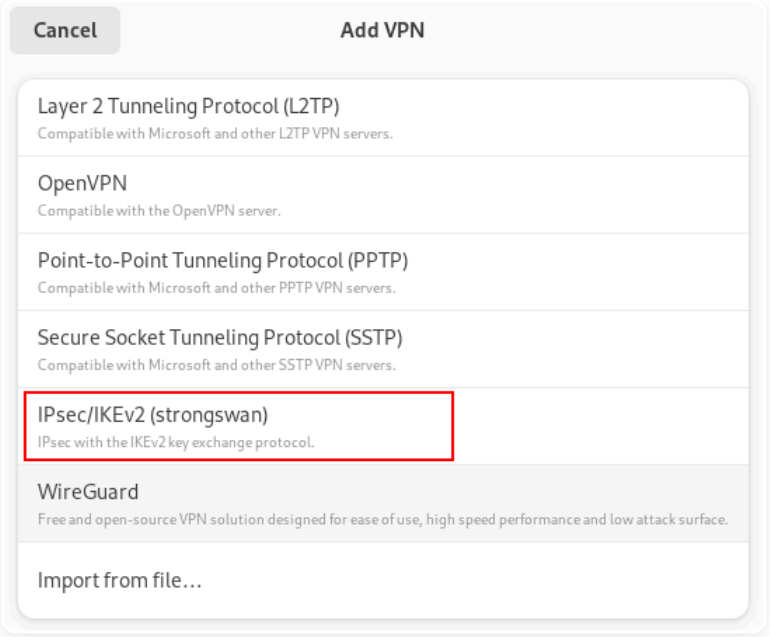
5. Для обновления сертификатов устройства выполните команду:

```
sudo update-ca-certificates
```

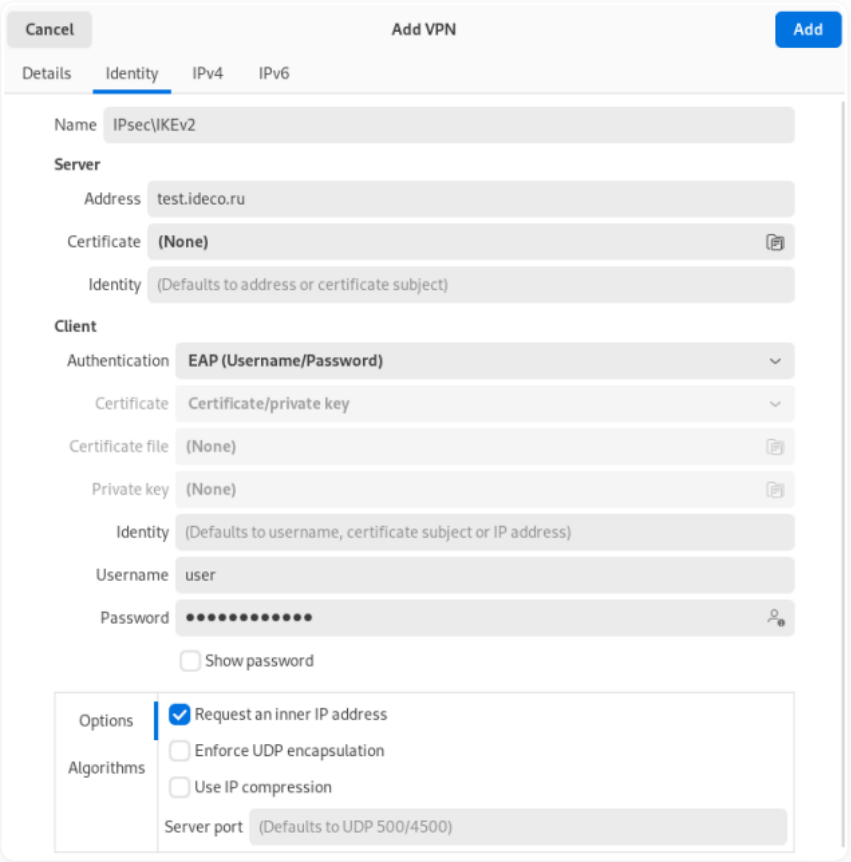
6. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите +:



7. В появившемся окне выберите **IPsec\IKEv2 (strongswan)**:



8. На вкладке **Identity (Идентификация)** заполните поля:



- **Название** - имя подключения.
- **Address** - домен, который указан в настройках **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Authentication** - рекомендуем выбрать EAP.
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.

Установите флаг **Request an inner IP address** и нажмите **Добавить**.

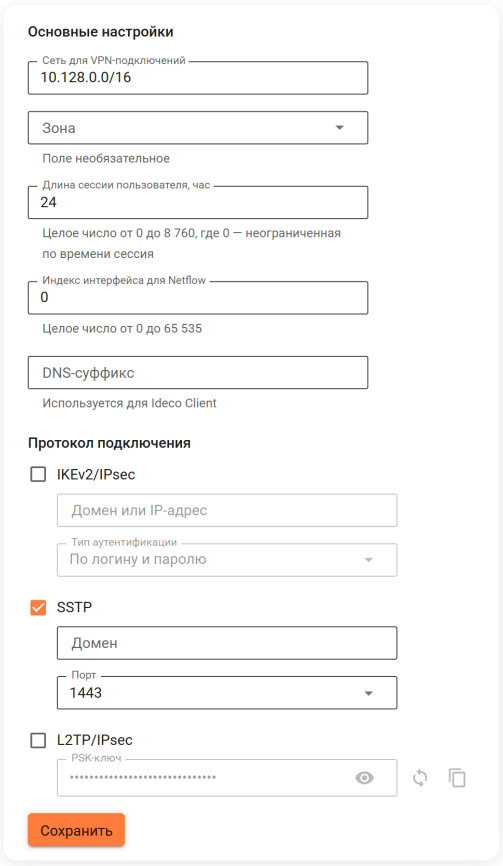
9. Включите созданное VPN-подключение.

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Ubuntu:

1. Откройте терминал и выполните команды:

```
sudo apt-add-repository ppa:eivnaes/network-manager-sstp
sudo apt install -y network-manager-sstp sstp-client
```

2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. Перейдите в терминале в директорию с загруженным корневым сертификатом (если на доменное имя NGFW выпущен Let`s Encrypt сертификат, сразу перейдите к пункту 6).

4. Установите корневой сертификат NGFW в хранилище доверенных сертификатов Ubuntu:

```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

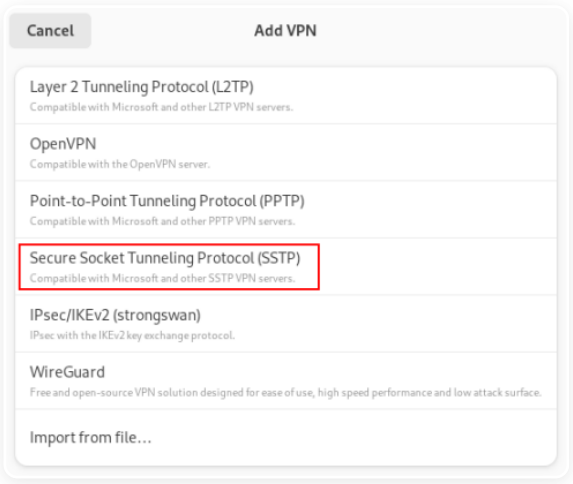
- `ca.crt` - имя скачанного сертификата.

5. Для обновления сертификатов устройства выполните команду:

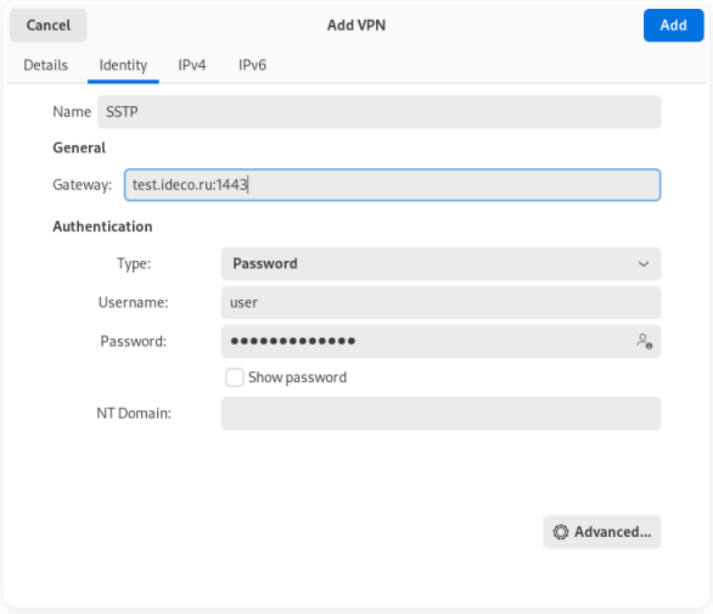
```
sudo update-ca-certificates
```

6. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋.

7. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)** (**Туннельный протокол типа точка-точка (SSTP)**):



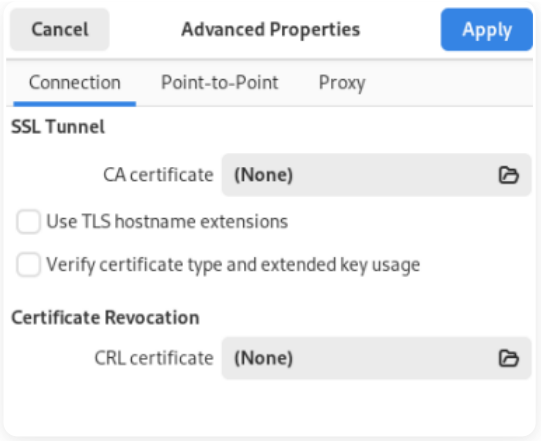
8. На вкладке **Identity (Идентификация)** заполните поля:



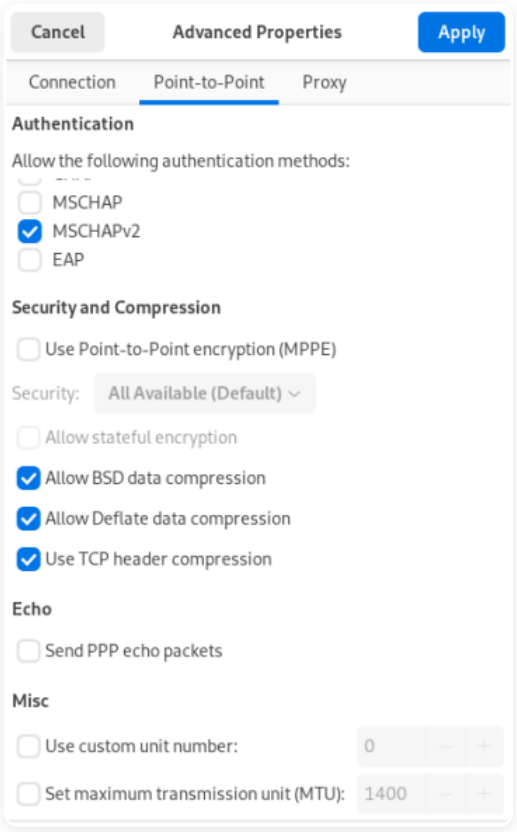
- **Название** - имя подключения.
- **Шлюз** - укажите в формате `домен:<порт, выбранный на NGFW>`.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.
- **NT-домен** - оставьте поле пустым.

9. Нажмите **Advanced**:

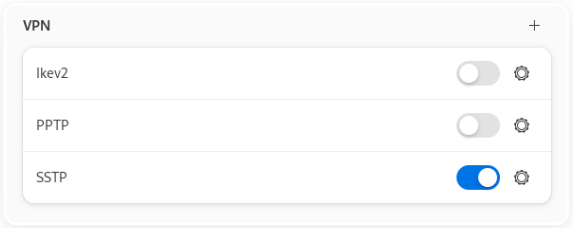
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**.
  - **Verify certificate type and extended key usage**:



- На вкладке **Point-to-Point** установите флаги на пунктах:
  - **Разрешить следующие методы аутентификации** - установите флаг только на ***MSCHAPv2***.
  - **Использовать для данных сжатие BSD**.
  - **Использовать для данных сжатие Deflate**.
  - **Использовать сжатие заголовков TCP**:



10. Нажмите **Добавить** и включите созданное VPN-подключение:



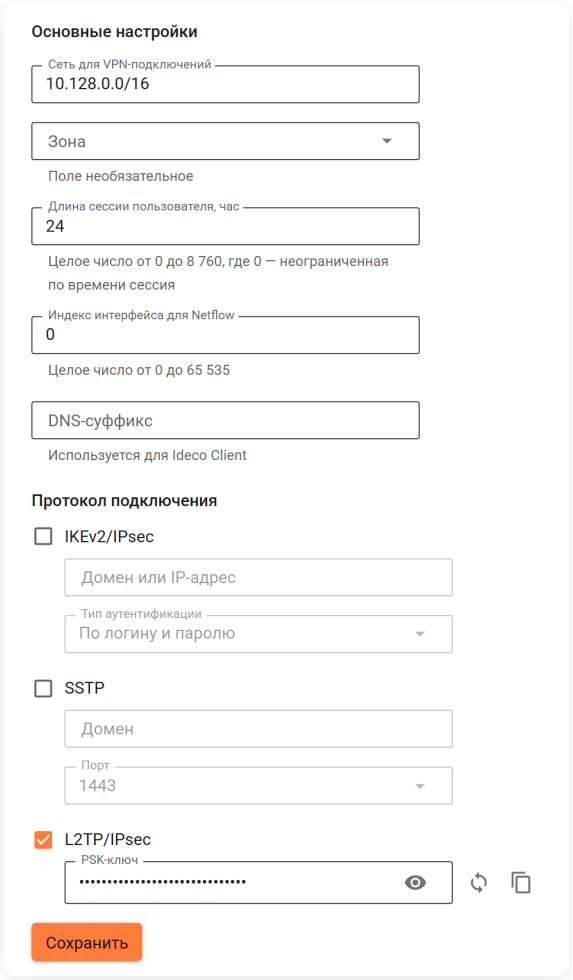
L2TP/IPsec

Важно: L2TP/IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если клиентов более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Ubuntu:

1. Подключите репозиторий, в котором находятся необходимые пакеты для создания L2TP VPN-соединения, а затем обновите информацию о репозиториях. Для этого выполните команды:

```
sudo add-apt-repository ppa:nm-l2tp/network-manager-l2tp
sudo apt update
```

2. Установите дополнение к стандартному NetworkManager с помощью двух пакетов:

```
sudo apt install -y network-manager-l2tp network-manager-l2tp-gnome
```

3. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

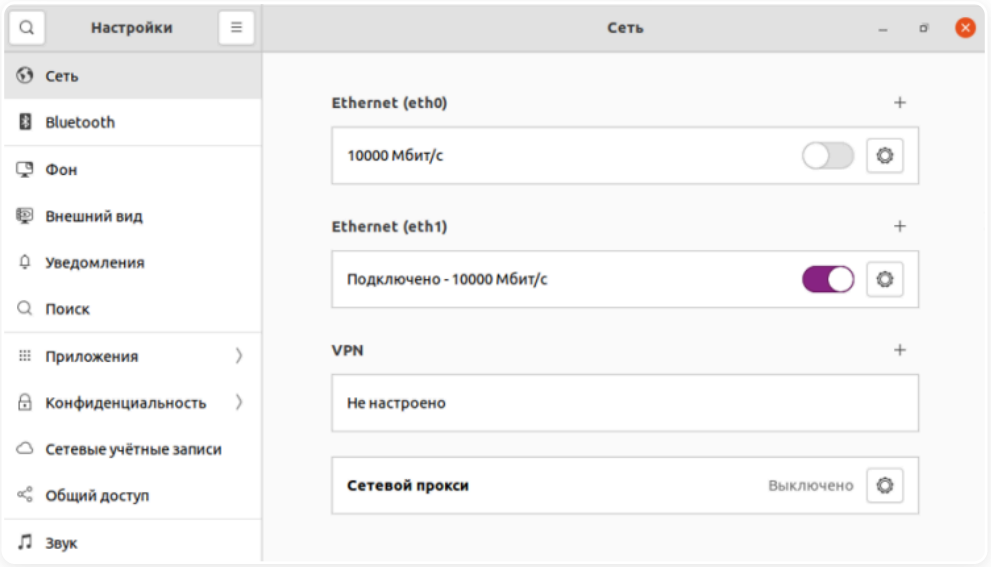
4. Проверьте установленные пакеты:

```
dpkg --get-selections | grep l2tp
```

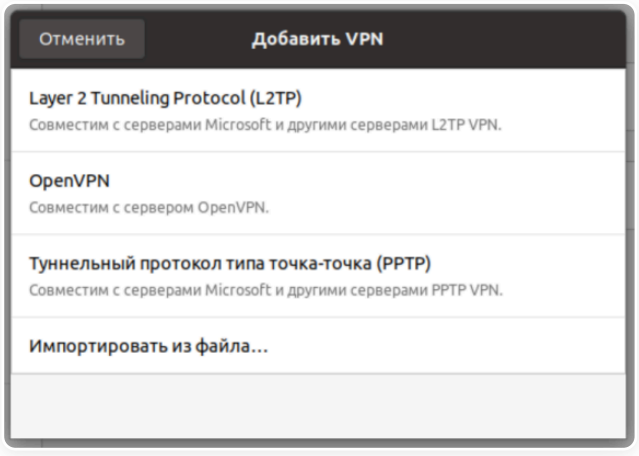
Важно: если в списке пакетов находится `go-l2tp`, удалите пакет и установите `xl2tpd`:

```
sudo apt purge go-l2tp
sudo apt install xl2tpd
```

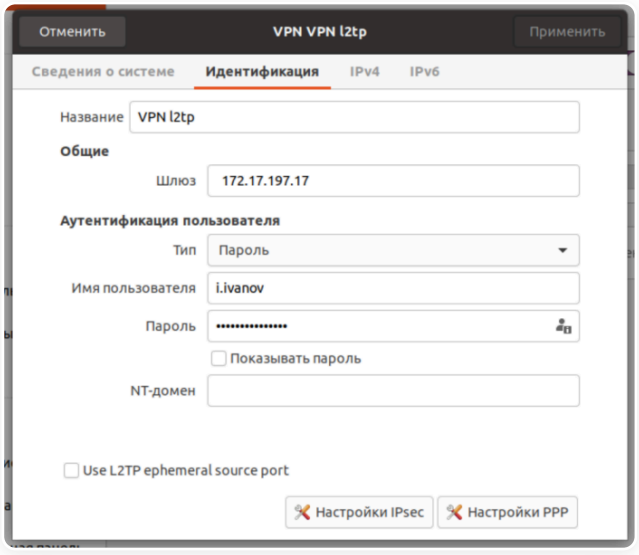
5. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋:



6. В появившемся окне выберите пункт **Layer 2 Tunneling Protocol (L2TP)**:

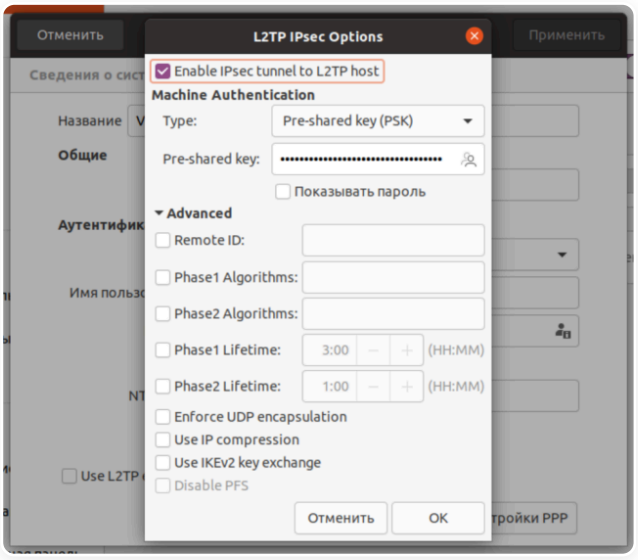


7. На вкладке **Идентификация** заполните поля:



- **Название** - имя подключения.
- **Шлюз** - домен или IP-адрес Ideco NGFW Novum.
- **Тип** - Password (аутентификация по имени пользователя и паролю).
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.
- **NT-домен** - оставьте поле пустым.

8. Перейдите в **Настройки IPsec** и включите настройку **Enable IPsec tunnel to L2TP host**, чтобы активировалась возможность настраивать остальные параметры:

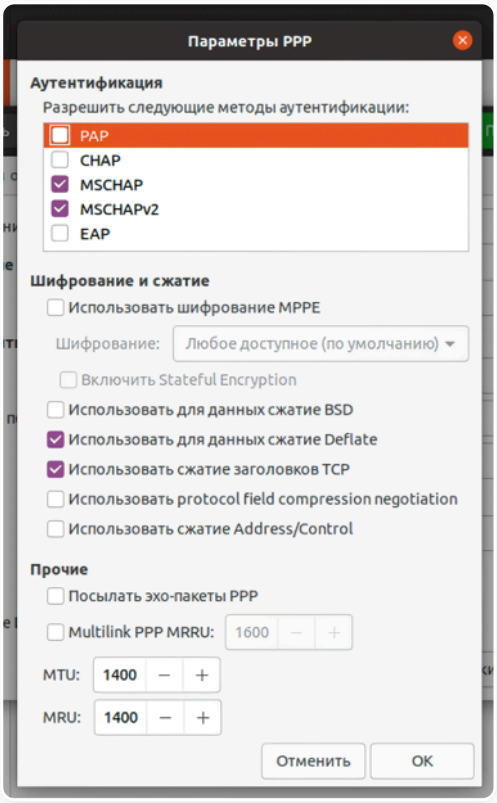


- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу.
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи** → **VPN-подключения** → **Основное** из поля **PSK**.

Раздел **Advanced** необязателен для заполнения.

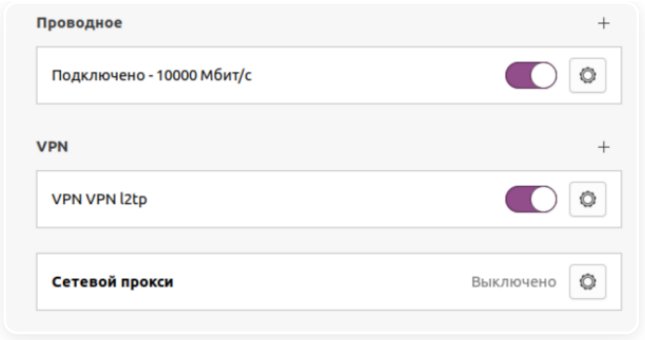
После окончания настройки **L2TP IPsec Options** нажмите **OK**.

9. При необходимости перейдите в **Настройки PPP** и настройте раздел **Аутентификация**, **Шифрование и сжатие** и **Прочие**:



После настройки **Параметры PPP** нажмите **OK** и **Применить**.

10. Включите созданное VPN-подключение:



Полезные ссылки

- VPN-подключения

Инструкция по созданию подключения в Fedora

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

Инструкция актуальна для Fedora 41. Рекомендуемый протокол подключения - IKEv2/IPsec.

Перед настройкой

1. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте правило разрешающее VPN-подключение.

2. Загрузите на устройство корневой сертификат Ideco NGFW Novum. Файл сертификата должен находиться в общедоступном каталоге.

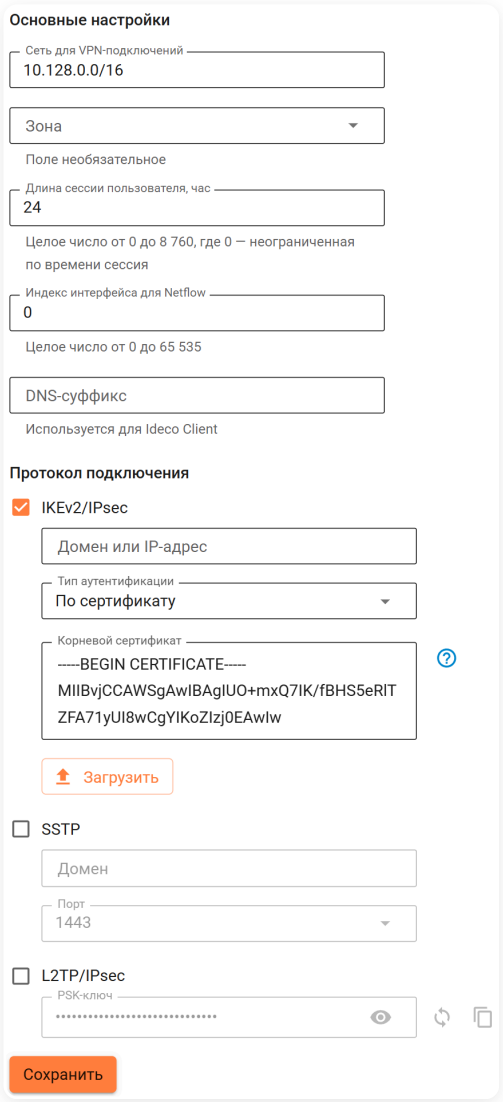
Загружать сертификат **ISRG_ROOT_X1** не требуется, так как сертификат уже есть в Fedora 41 и находится в каталоге `/etc/ssl/certs`.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.

- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Создание подключения в Fedora:

1. Для поддержки подключения по IPsec для NetworkManager установите пакет **NetworkManager-strongswan**:

```
sudo dnf -y install NetworkManager-strongswan
```

2. Установите пакет для настройки IPsec-подключения через графический интерфейс:

- Окружение рабочего стола GNOME:

```
sudo dnf -y install NetworkManager-strongswan-gnome
```

- Окружение рабочего стола KDE:

```
sudo dnf -y install plasma-nm-strongswan
```

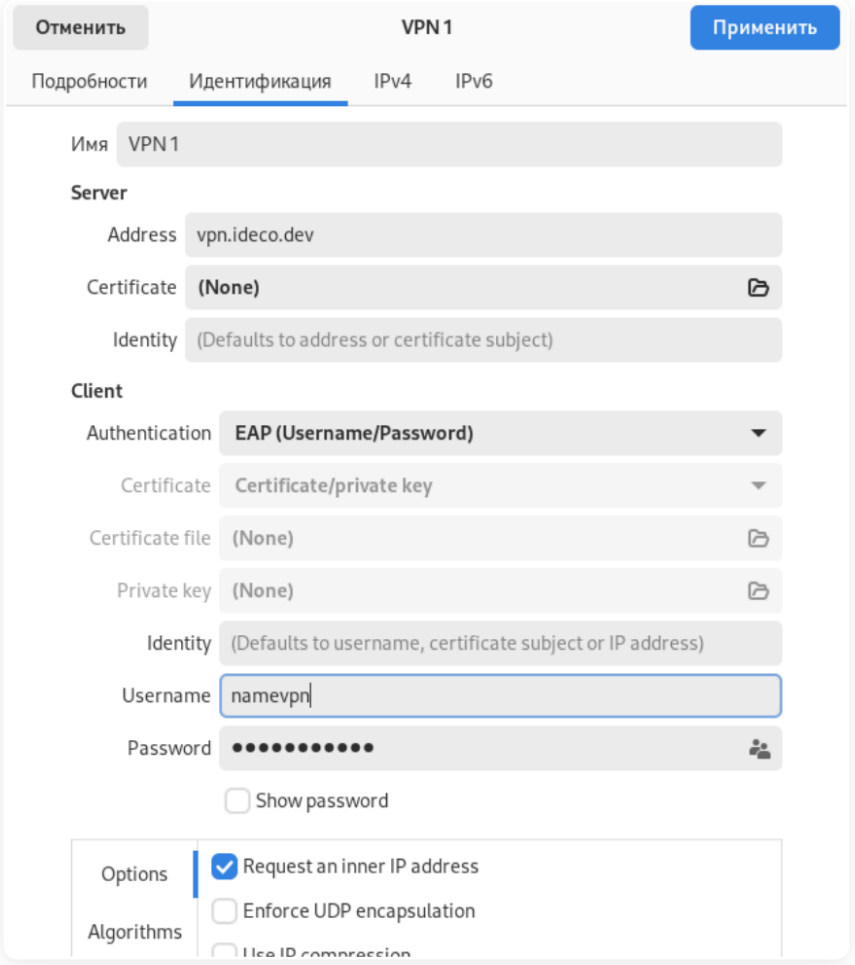
Создание подключения в Fedora:

1. Загрузите корневой сертификат NGFW Novum, включая всю цепочку доверия, в каталог `/etc/strongswan/ipsec.d/cacerts`.

2. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите  .

3. В появившемся окне выберите **IPsec\IKEv2 (strongswan)**.

4. В **Идентификация** заполните поля:



- **Имя** - название VPN-подключения.
- **Address** - доменное имя шлюза для VPN-подключения.
- **Authentication** - EAP (Username/Password).
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

5. Установите флаг **Request an inner IP address**.

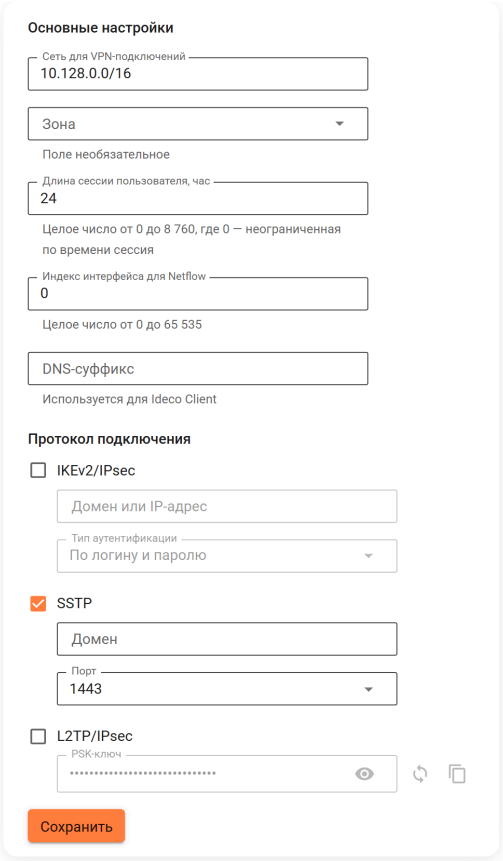
6. Нажмите **Применить** и включите созданное VPN-подключение.

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Создание подключения в Fedora:

1. Откройте терминал и установите необходимые пакеты, выполнив команду:

- Окружение рабочего стола GNOME:

```
sudo dnf install NetworkManager-sstp.x86_64 NetworkManager-sstp-gnome.x86_64 sstp-client.x86_64
```

- Окружение рабочего стола KDE:

```
sudo dnf install NetworkManager-sstp.x86_64 plasma-nm-sstp.x86_64 sstp-client.x86_64
```

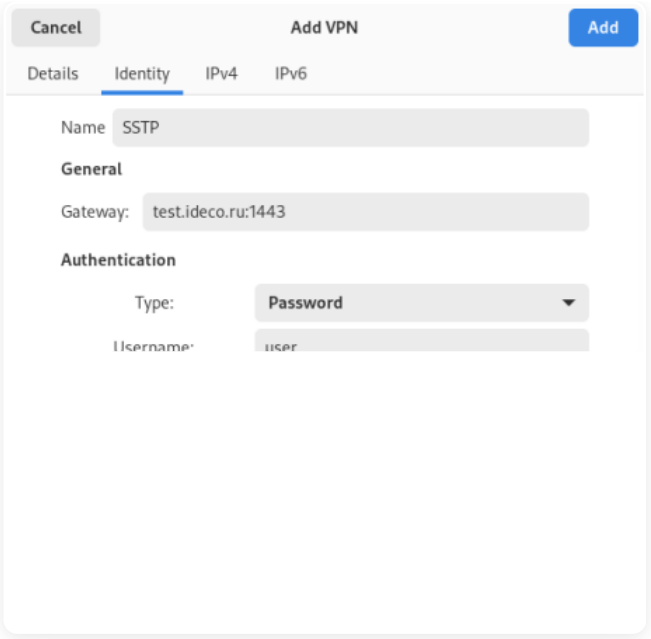
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите +.

4. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)**.

5. В разделе **Идентификация** заполните поля:

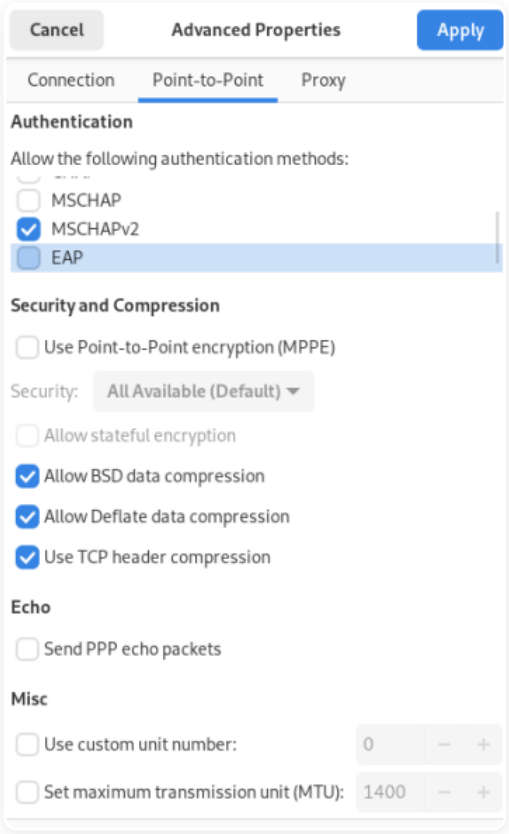


- **Name** - название VPN-подключения.
- **Gateway** - укажите в формате `домен:<порт, выбранный на NGFW>`.
- **Username** - имя пользователя на Ideco NGFW Novum.
- **Password** - пароль пользователя на Ideco NGFW Novum.

6. Нажмите **Advanced**:

- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**.
  - **Verify certificate type and extended key usage**:

- На вкладке **Point-to-Point** рекомендуем установить флаги на пунктах:



- **Allow the following authentication methods** - установите флаг на ***MSCHAPv2***.
- **Allow BSD data compression**.

- **Allow Deflate data compression**.
- **Allow TCP header compression**.

7. Нажмите **Добавить** и включите созданное VPN-подключение.

> Если подключение по SSTP не устанавливается:
>
> 1. Выполните команду `sestatus`, чтобы узнать текущий режим SELinux. Если режим **Enforcing**, SELinux может блокировать работу SSTP.
>
> 2. Переведите SELinux в режим **Permissive**. Для этого выполните команду `sudo setenforce 0`. Это до перезагрузки отключит принудительный контроль доступа SELinux.
>
> 3. Попробуйте подключиться к VPN через SSTP. Если проблема была в SELinux, подключение должно заработать.
>
> 4. Если заработало, то измените файл `sudo nano /etc/selinux/config` и установите `SELINUX=permissive` или `SELINUX=disabled`. После этого перезагрузите систему.
>
> Рекомендуем режим **Permissive** (setenforce 0) использовать только для диагностики и не оставлять SELinux в этом режиме на постоянной основе, так как это снижает уровень безопасности системы.

L2TP/IPsec

L2TP/IPsec клиенты, находящиеся за одним NAT, могут испытывать проблемы подключения, если клиентов более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

Создание подключения в Fedora:

1. Установите необходимые пакеты для создания L2TP VPN-соединения, выполнив команду:

- Окружение рабочего стола GNOME:

```
sudo dnf install NetworkManager-l2tp.x86_64 NetworkManager-l2tp-gnome.x86_64 xl2tpd.x86_64
```

- Окружение рабочего стола KDE:

```
sudo dnf install NetworkManager-l2tp.x86_64 plasma-nm-l2tp.x86_64 xl2tpd.x86_64
```

2. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

4. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите +.

5. В окне создания подключений по VPN выберите пункт **Layer 2 Tunneling Protocol (L2TP)**.

6. На вкладке **Идентификация** заполните поля:

- **Name** - название VPN-подключения.
- **Gateway** - доменное имя или IP-адрес NGFW.
- **Type** - Password.
- **User Name** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

7. Перейдите в **Настройки IPsec** и включите настройку **Enable IPsec tunnel to L2TP host**, чтобы активировалась возможность настраивать остальные параметры:

- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу.
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи** → **VPN-подключения** → **Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения.

После окончания настройки **L2TP IPsec Options** нажмите **OK**.

8. При необходимости перейдите в **Настройки PPP** и настройте раздел **Аутентификация**, **Шифрование и сжатие** и **Прочие**:

После настройки **Параметров PPP** нажмите **OK** и **Применить**.

9. Включите созданное VPN-подключение.

Полезные ссылки

- **VPN-подключения**
- **Подключение по IKEv2/IPsec**

Инструкция по созданию подключения в Astra Linux

Функциональность доступна в **Классическом** и **Системном контекстах**.

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

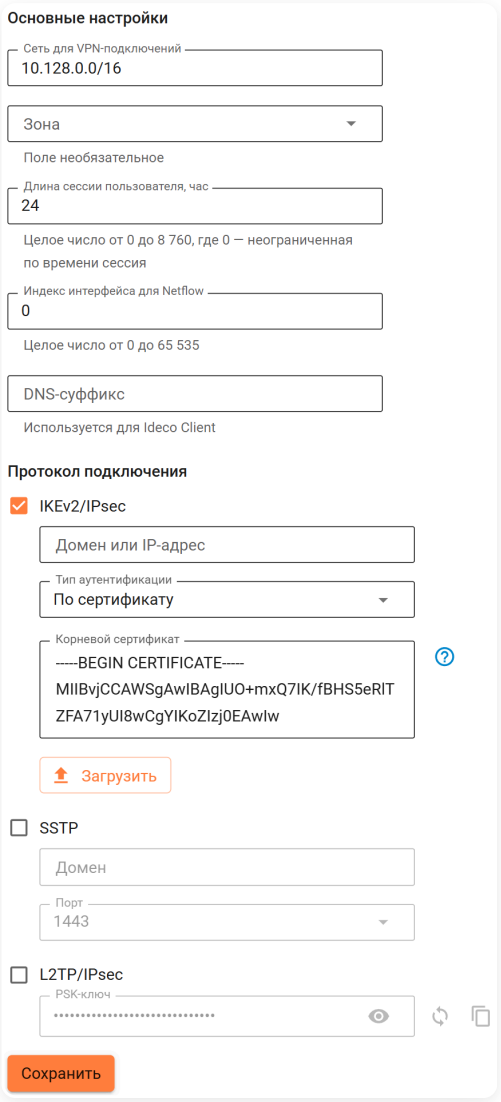
Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.

- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Astra Linux:

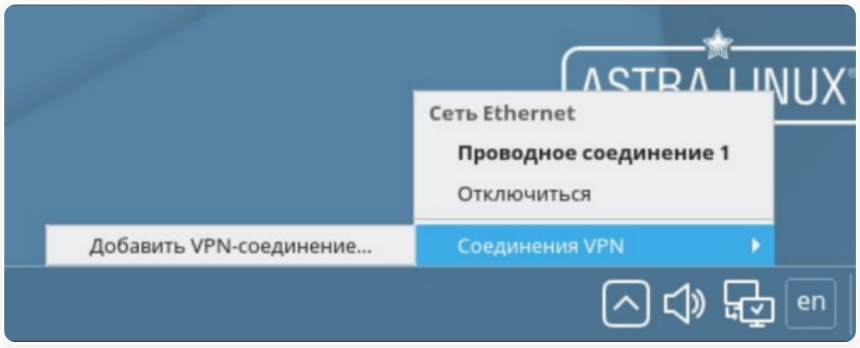
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt install libcharon-extra-plugins
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-extra-plugins
```

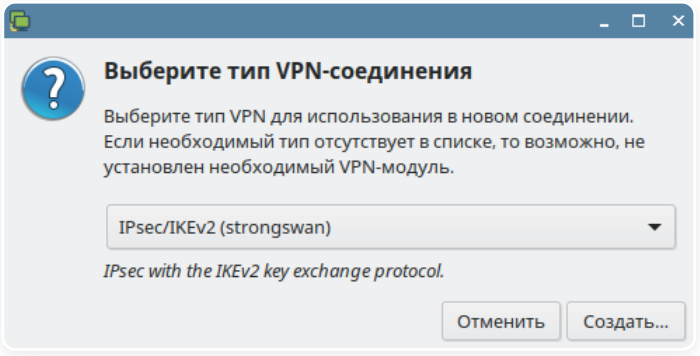
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

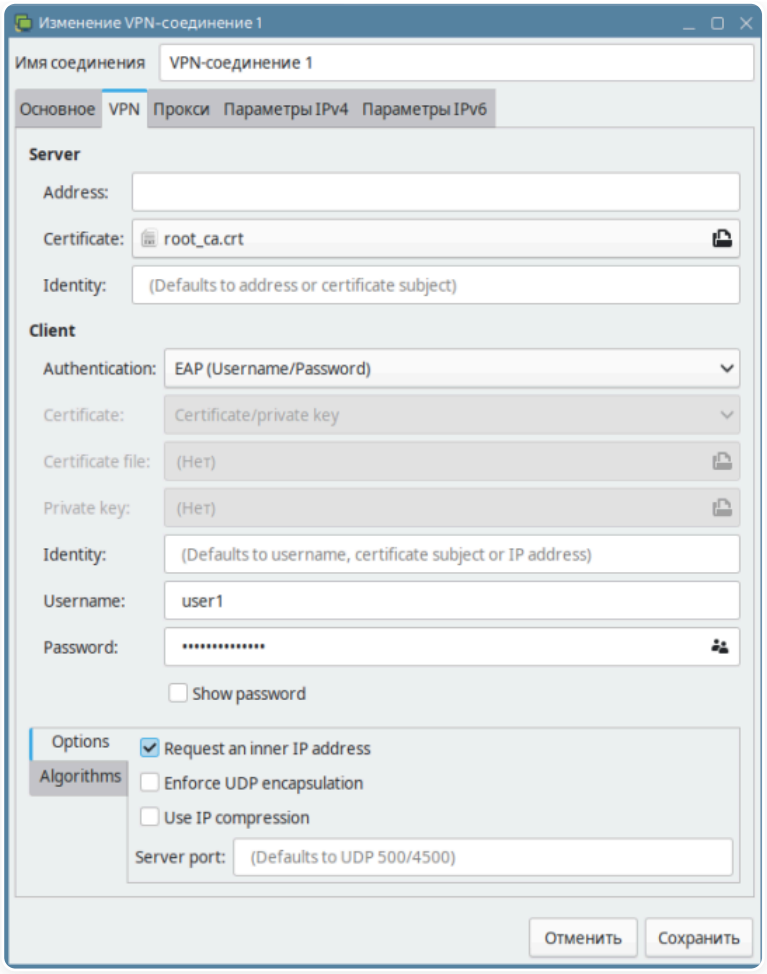
3. В настройках сети выберите **Соединения VPN** → **Добавить VPN-соединение**:



4. Выберите тип соединения **IPsec/IKEv2 (strongswan)** и нажмите **Создать**:



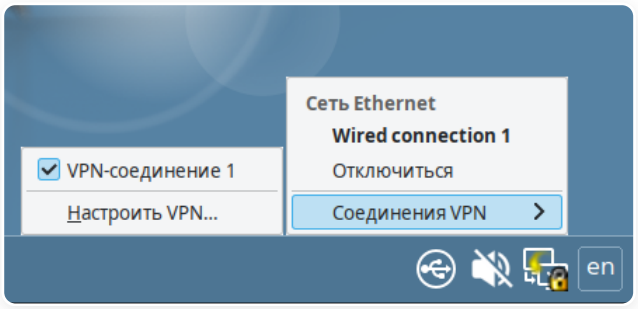
5. На вкладке **VPN** заполните поля:



- **Имя соединения** - имя подключения.
- **Address** - введите домен или IP-адрес, который указан в настройках **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Certificate** - выберите корневой сертификат NGFW или оставьте поле пустым, если используется сертификат Let's Encrypt.
- **Authentication** - рекомендуем выбрать EAP (Username/Password).
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.

Установите флаг **Request an inner IP address** и нажмите **Добавить**.

6. В настройках сети выберите **Соединения VPN** и установите флаг в строке с созданным соединением:



Проверить способы шифрования можно в конфигурации NGFW. Для этого откройте терминал NGFW и введите команду:

```
cat /run/ideco-ipsec-backend/strongswan/swanctl/conf.d/rw_ikev2.conf
```

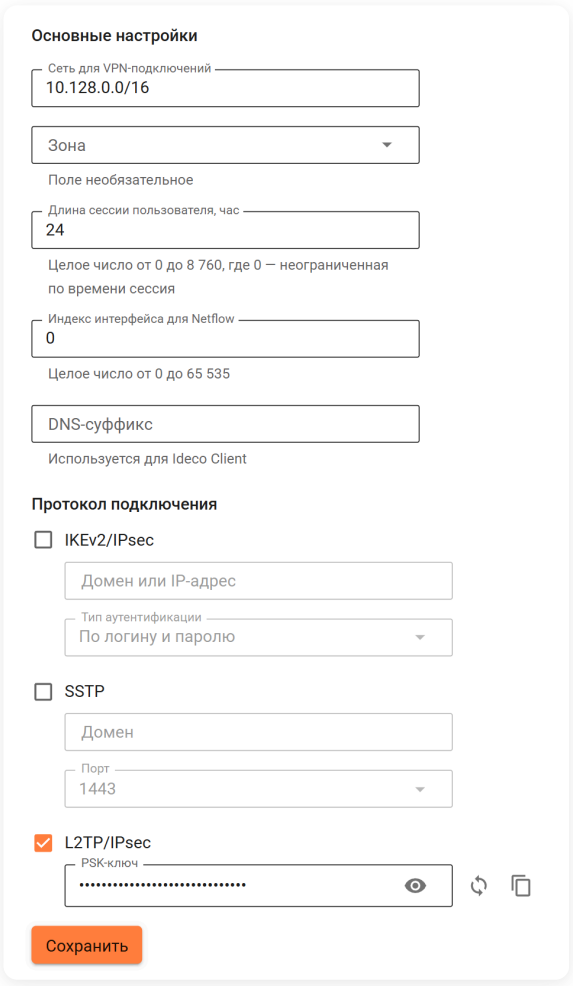
- для Phase1 Algorithm ищите значения **proposals=**;
- для Phase2 Algorithms ищите значения **esp_proposals=**.

L2TP/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи → VPN-подключения → Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Astra Linux:

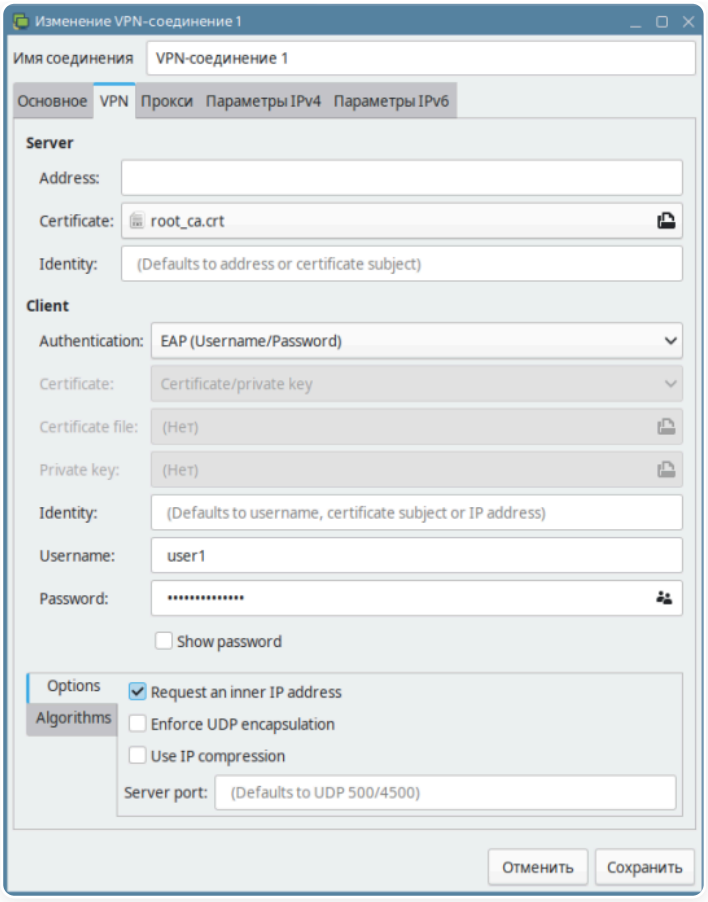
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt update
sudo apt install network-manager-l2tp-gnome
```

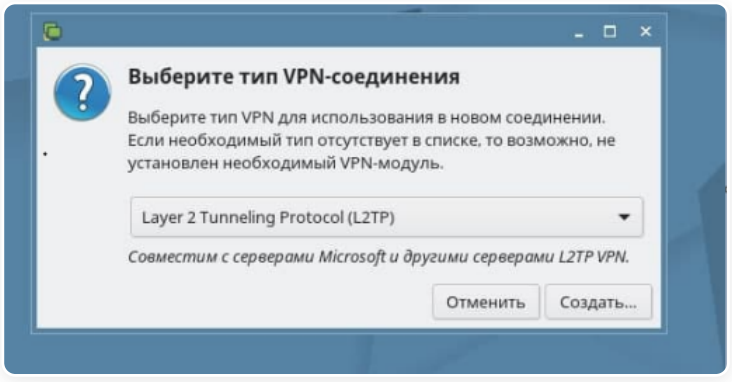
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

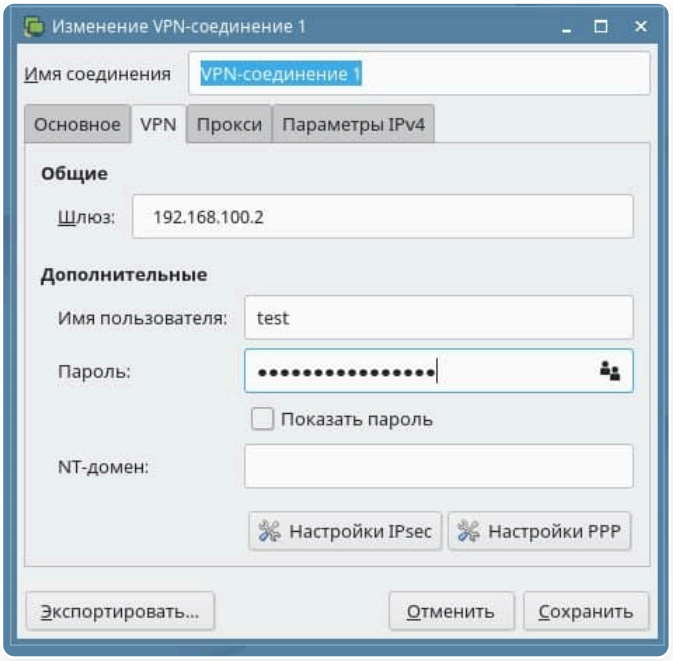
3. В настройках сети выберите **Соединения VPN → Добавить VPN-соединение**:



4. Выберите тип соединения **Layer 2 Tunneling Protocol (L2TP)** и нажмите **Создать**:



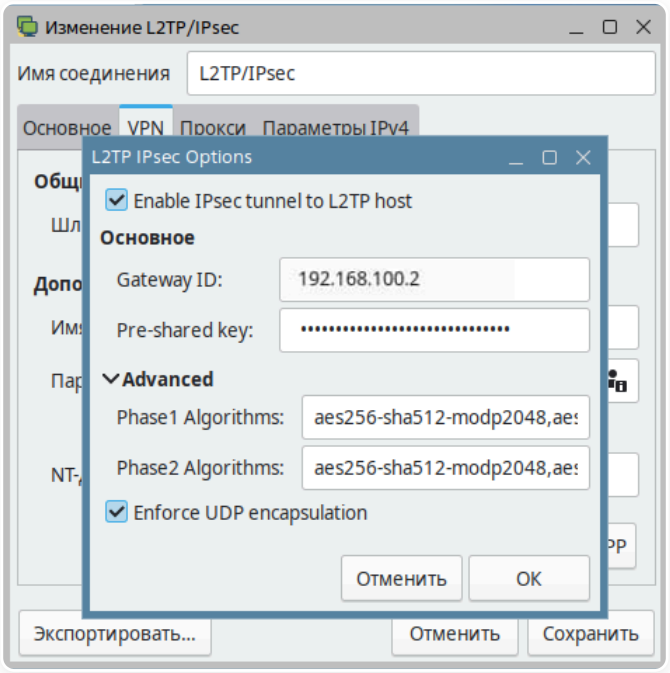
5. На вкладке **VPN** заполните поля:



- **Шлюз** - IP-адрес или домен внешнего интерфейса Ideco NGFW Novum.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.

6. Нажмите **Настройки IPsec**.

7. Заполните поля:

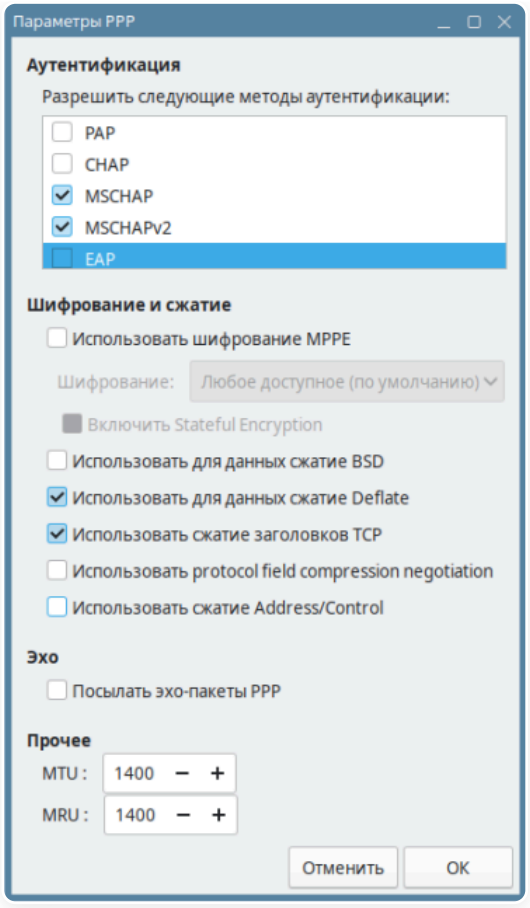


- **Gateway ID** - IP-адрес интерфейса, к которому осуществляется подключение.
- **Pre-shared key** - PSK-ключ из настроек Ideco NGFW Novum (**Пользователи** → **VPN-подключения** → **Основное**).
- **Phase1 Algorithm** - `aes256-sha512-modp2048,aes256-sha512-modp1024,aes256-sha1-ecp256,aes256-sha1-modp2048,aes256-sha1-modp1024!`. *
- **Phase2 Algorithms** - `aes256-sha512-modp2048,aes256-sha256-modp2048,aes256-sha1-modp2048,aes128-sha1-modp2048,aes256-sha512-modp1024,aes256-sha256-modp1024,aes256-sha1-modp1024,aes128-sha1-modp1024,aes256-sha512,aes256-sha256,aes256-sha1,aes128-sha1!`.*

* Обязательно поставьте восклицательный знак в конце строки.

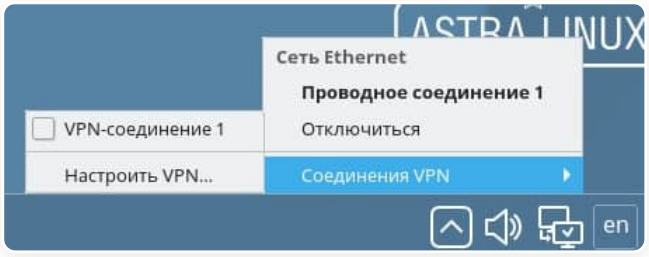
Так как Astra Linux по умолчанию запрашивает не самые защищенные алгоритмы, рекомендуем заполнить поля **Phase1 Algorithm** и **Phase2 Algorithms** самостоятельно.

8. При необходимости перейдите в **Настройки PPP** и настройте разделы **Аутентификация**, **Шифрование и сжатие**, **Прочее**:



9. Нажмите **ОК**, затем **Сохранить**.

Далее в настройках сети **Соединения VPN** появится VPN-подключение. Для активации включите опцию **VPN-соединение**:



Полезные ссылки

- **VPN-подключения**

Инструкция по созданию подключения в Windows

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Не рекомендуем использовать для VPN-подключений кириллические логины.

Создание VPN-подключения в Windows

Для корректной передачи маршрутов клиенту убедитесь, что опция **Использовать основной шлюз удаленной сети** выключена. Для отключения опции перейдите в **Панель управления** → **Сеть и интернет** → **Центр управления сетями и общим доступом** → **Изменение параметров адаптера** → **Свойства**. После этого перейдите в **Сеть** → **IP версии 4 (TCP/IPv4)** → **Дополнительно**.

IKEv2/IPsec

Выберите тип аутентификации пользователей и выполните действия:

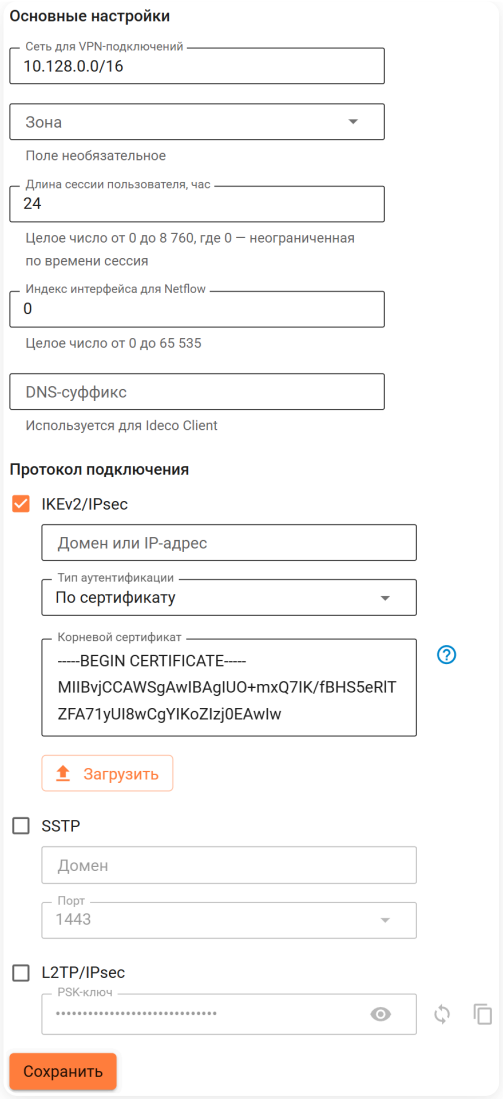
По логину и паролю **По сертификату**

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Домен и IP-адрес** - укажите доменное имя или IP-адрес, по которому будут подключаться пользователи.
- **Тип аутентификации** - выберите тип **По логину и паролю**.

3. Нажмите **Сохранить**.

4. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

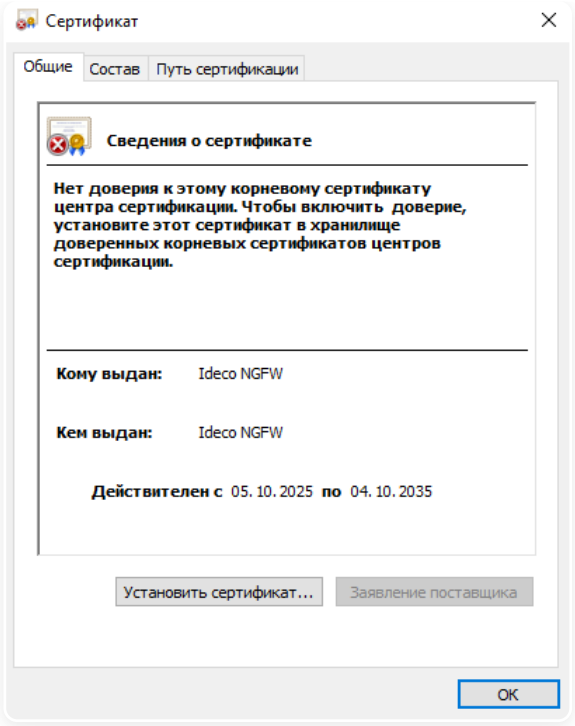
- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Windows:

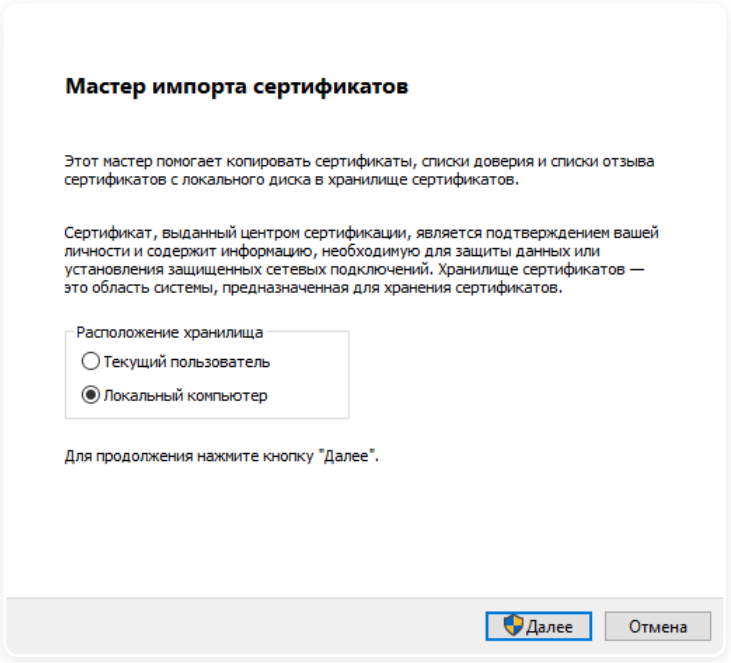
1. Импортируйте сертификат Ideco NGFW Novum:

Пример для Windows

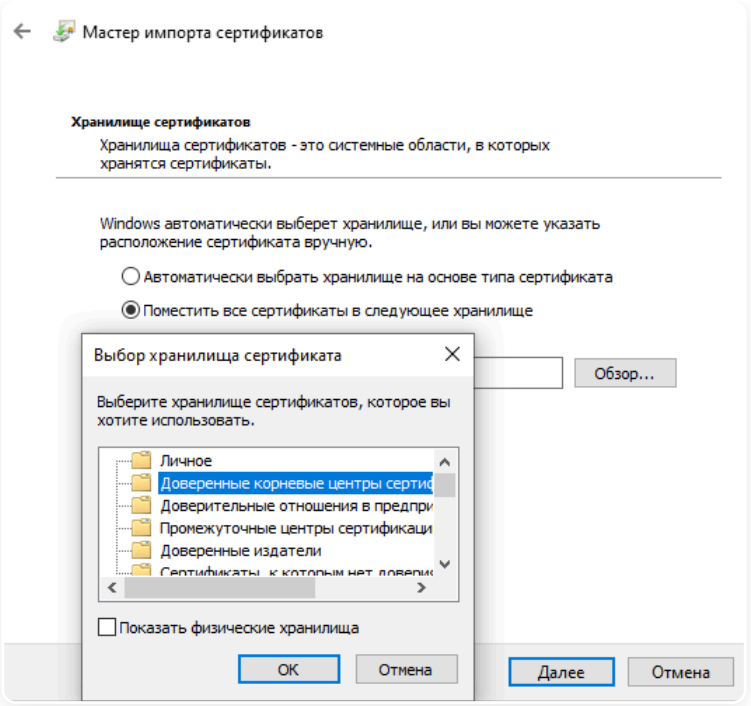
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



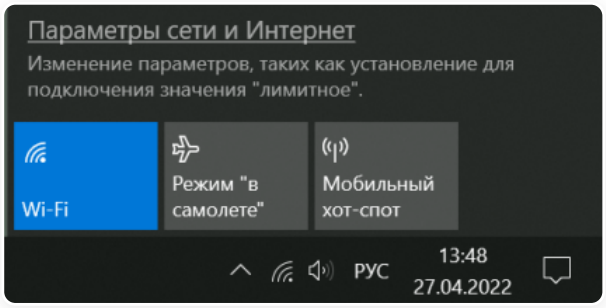
2. Выберите расположение хранилища **Локальный компьютер**:



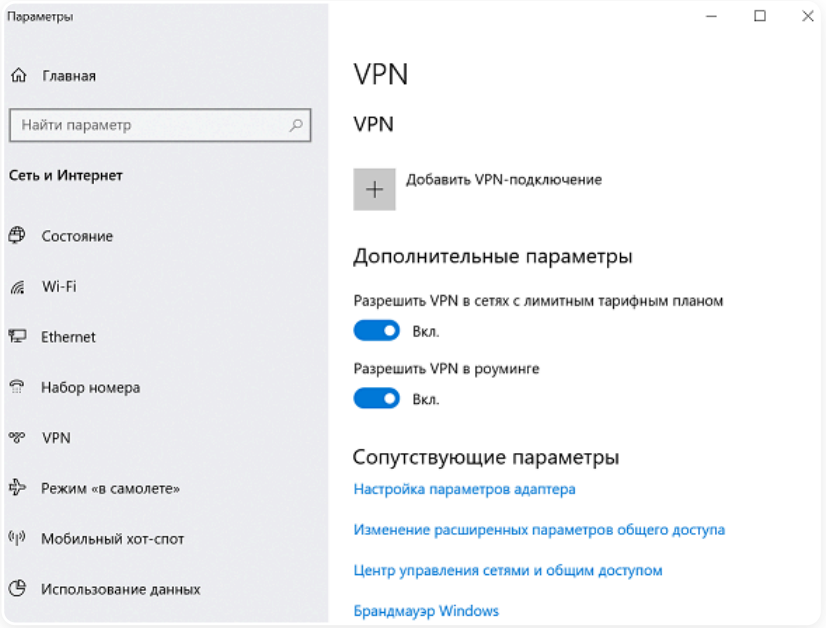
3. Установите сертификат в **Доверенные корневые центры сертификации**:



2. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



3. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



4. Заполните соответствующие поля и нажмите **Сохранить**:



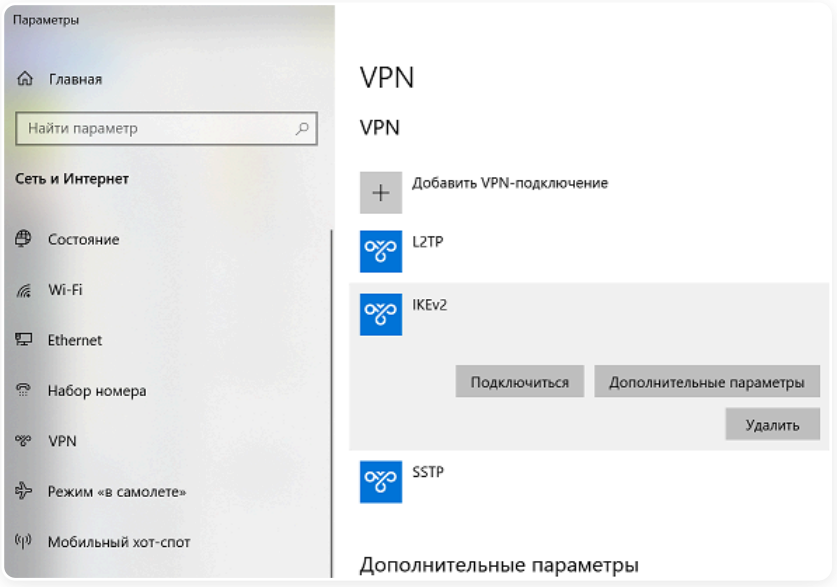
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера.
- **Тип VPN** - протокол IKEv2.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

5. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

6. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).
- **Протокол расширенной проверки подлинности (EAP)** - Microsoft защищенный пароль (EAP MSCHAPV2).

7. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



8. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры** → **Изменить**.

L2TP/IPsec

Подготовка:

Для аутентификации пользователей по сертификату необходимо экспортировать:

- **Корневой сертификат** Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя.
- **Полную цепочку промежуточных сертификатов**, если сертификат пользователя выпущен промежуточным УЦ.
- **Пользовательский сертификат**.

Требования к сертификатам

Алгоритмы хеширования:

- Для подписи сертификатов рекомендуется использовать алгоритм SHA-256 или более стойкий (например, SHA-384, SHA-512).
- Алгоритм SHA-1 не поддерживается.

Ключевые расширения:

- **Для промежуточного сертификата:**
- `basicConstraints=critical,CA:TRUE` - используется для указания, что сертификат может подписывать другие сертификаты.
- **Для пользовательского сертификата:**
- `subjectAltName=DNS:...` - используется для указания альтернативных имен (например, DNS или IP-адреса).

Примеры генерации сертификатов УЦ:

Создание корневого и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **CN** - укажите логин учетной записи пользователя для авторизации.

3. Подписание пользовательского сертификата корневым:

```
openssl x509 -req -in client.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

4. Создание PFX-архива для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile rootCA.crt -passout pass:1234
```

Создание корневого, промежуточного и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание промежуточного сертификата:

```
openssl genrsa -out interCA.key 4096
openssl req -new -key interCA.key -out interCA.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"

openssl x509 -req -in interCA.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out interCA.crt -days 1825 -sha256 \
-extfile <(printf "basicConstraints=critical,CA:TRUE")
```

3. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **Common Name (CN)** - укажите логин учетной записи пользователя для авторизации.

4. Подписание пользовательского сертификата промежуточным:

```
openssl x509 -req -in client.csr -CA interCA.crt -CAkey interCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

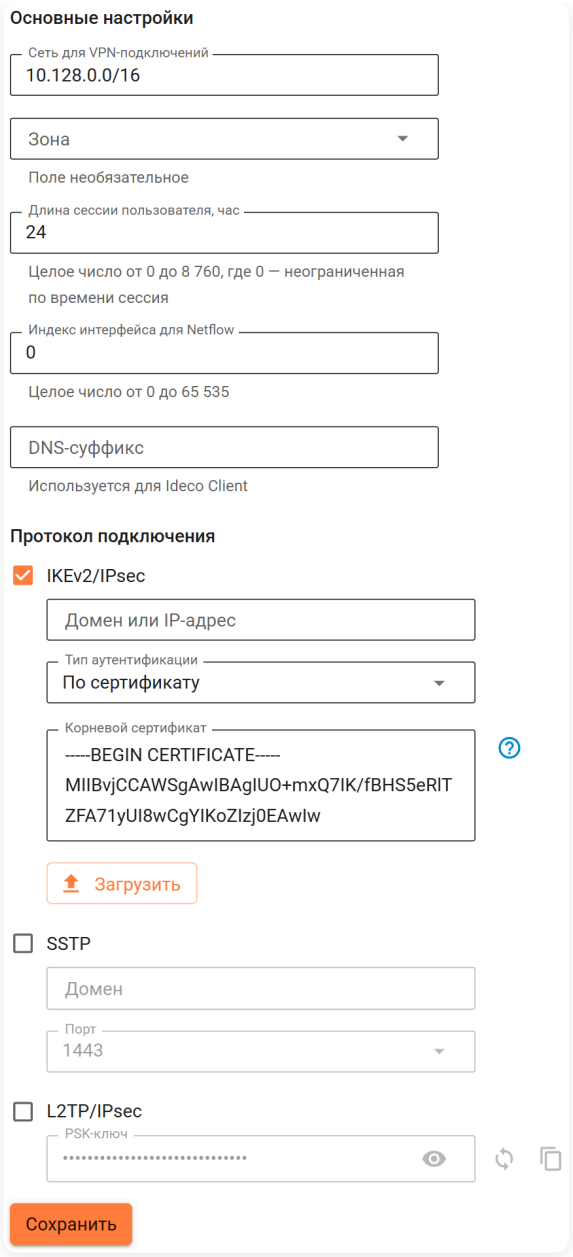
5. Создание PFX-архива с полной цепочкой доверия для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile <(cat interCA.crt rootCA.crt) -passout pass:1234
```

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Домен и IP-адрес** - укажите доменное имя или IP-адрес, по которому будут подключаться пользователи.
- **Тип аутентификации** - выберите тип **По сертификату**.
- **Корневой сертификат** - загрузите корневой сертификат УЦ или объединенный в один файл корневой и все промежуточные сертификаты.

3. Нажмите **Сохранить**.

4. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

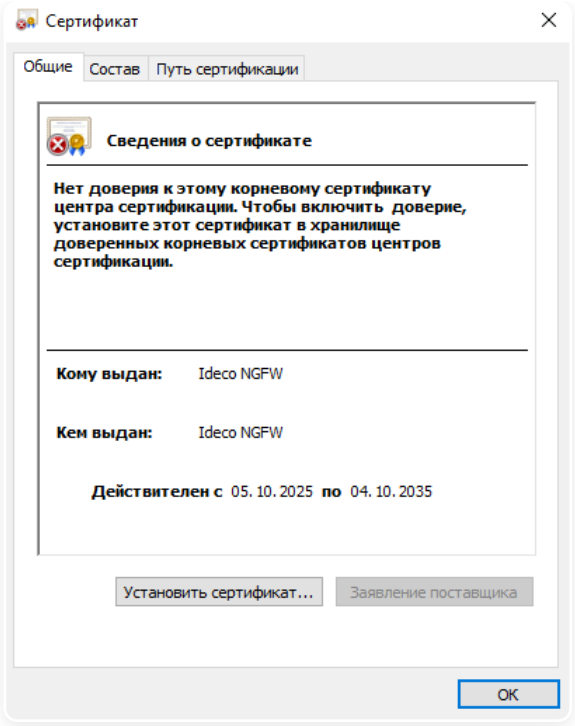
- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Windows:

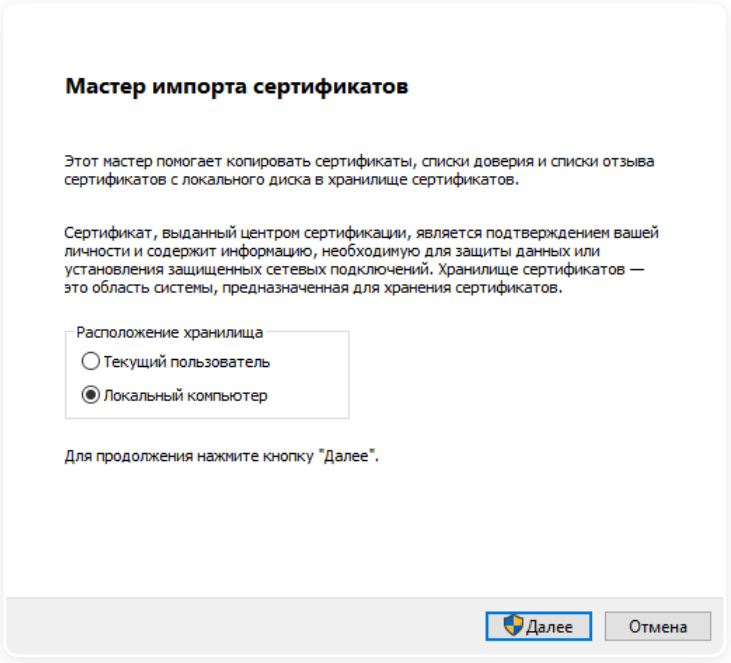
1. Импортируйте корневой сертификат Ideco NGFW Novum:

Пример для Windows

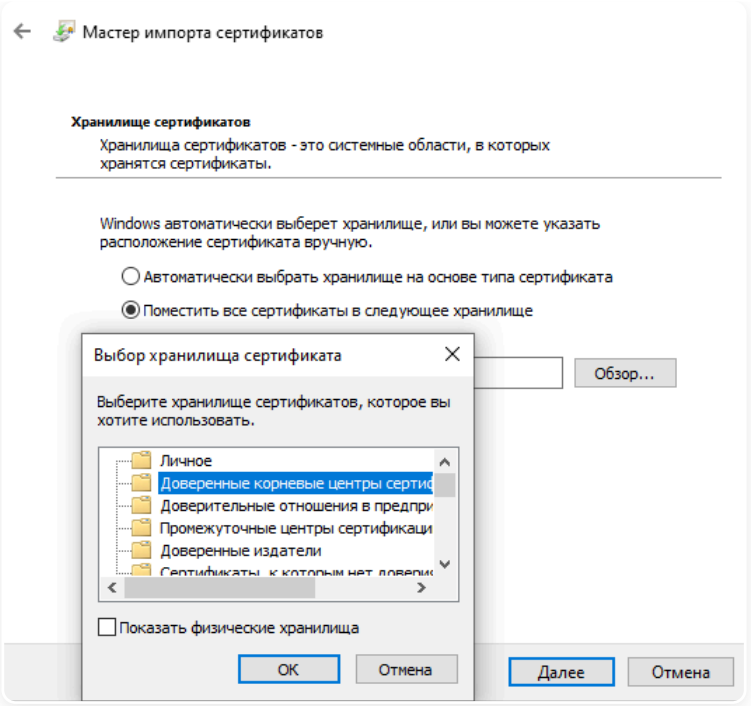
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



2. Выберите расположение хранилища **Локальный компьютер**:



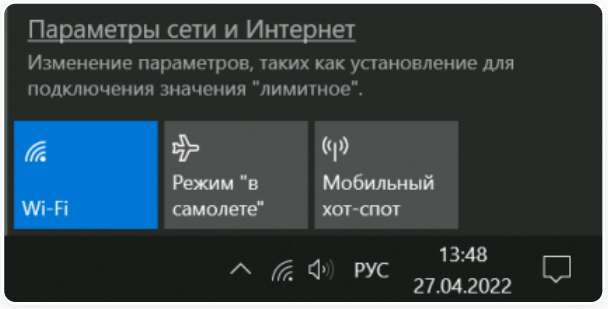
3. Установите сертификат в **Доверенные корневые центры сертификации**:



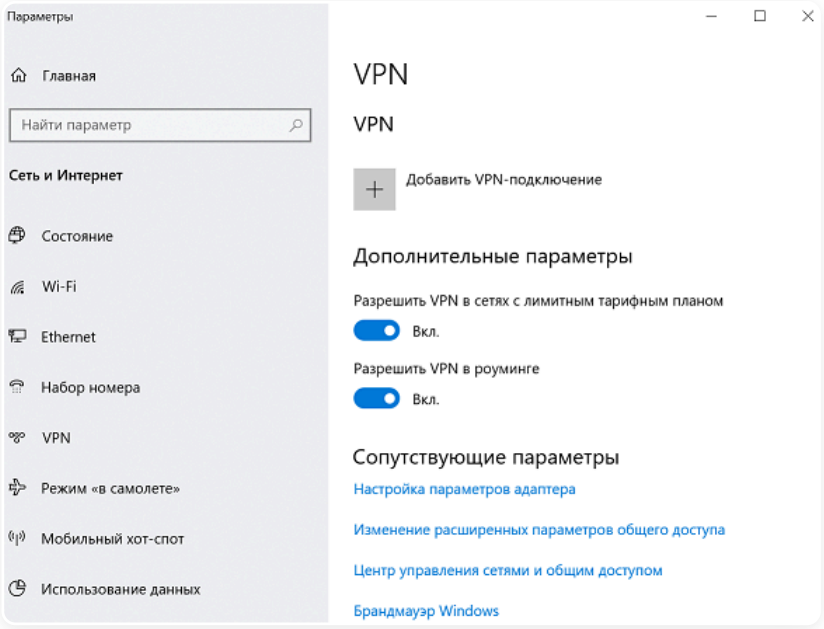
2. Импортируйте пользовательский сертификат:

- Расположение хранилище - **Текущий пользователь**.
- Выбор хранилища - **Личное**.

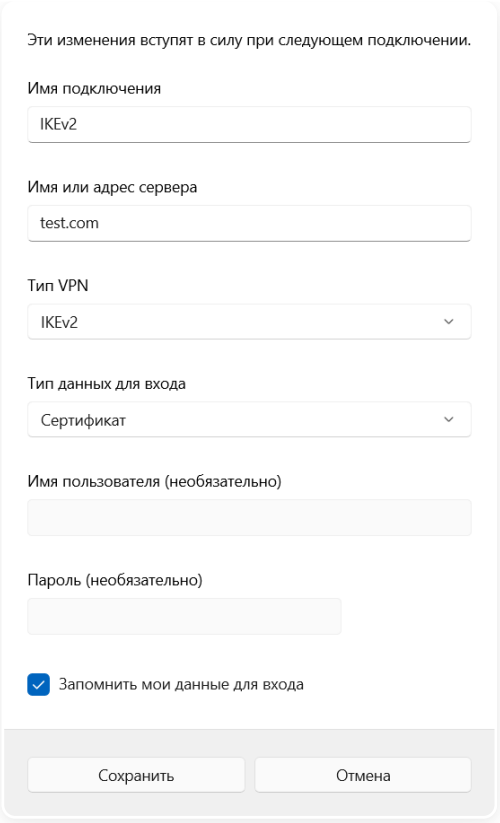
3. Кликните на иконку сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



4. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



5. Заполните соответствующие поля и нажмите **Сохранить**:



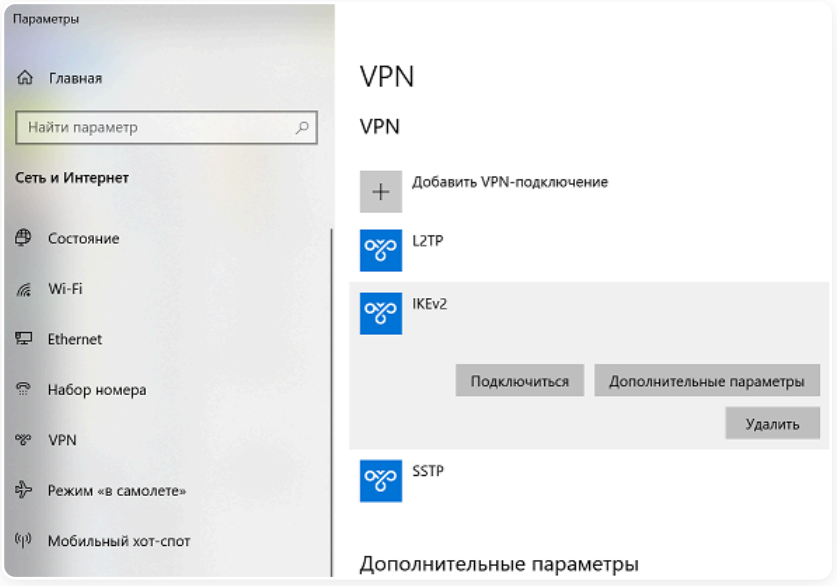
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера.
- **Тип VPN** - протокол IKEv2.
- **Тип данных для входа** - сертификат.

6. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

7. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).
- **Протокол расширенной проверки подлинности (EAP)** - Microsoft: Смарт-карта или другой сертификат (EAP-TLS).

8. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



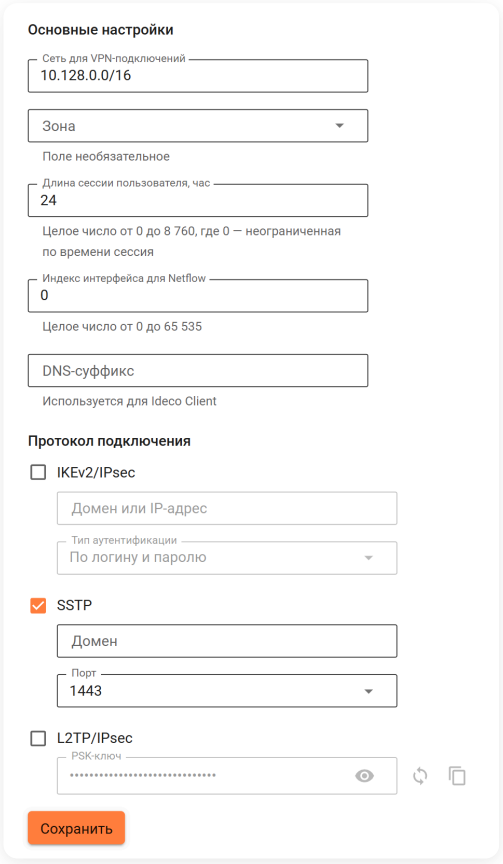
9. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры → Изменить**.

Вкладка 4

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи → VPN-подключения → Основное**.

2. Включите опцию **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы → Сертификаты → Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

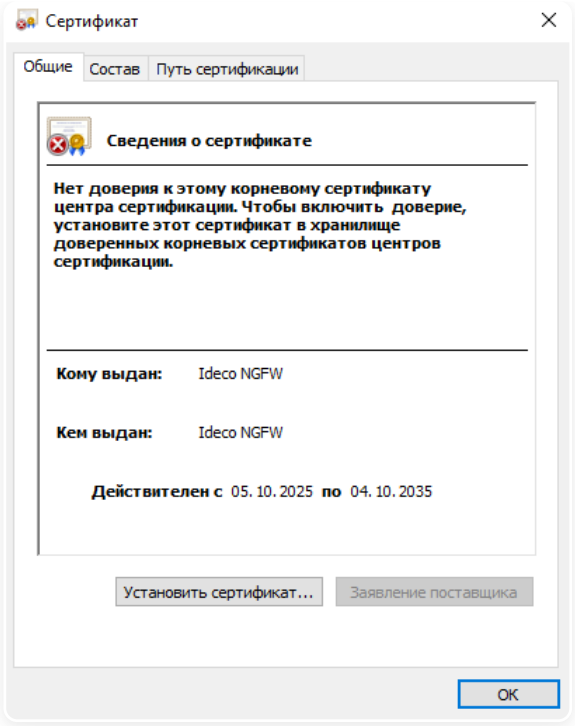
Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы → Сертификаты → Загруженные сертификаты**.

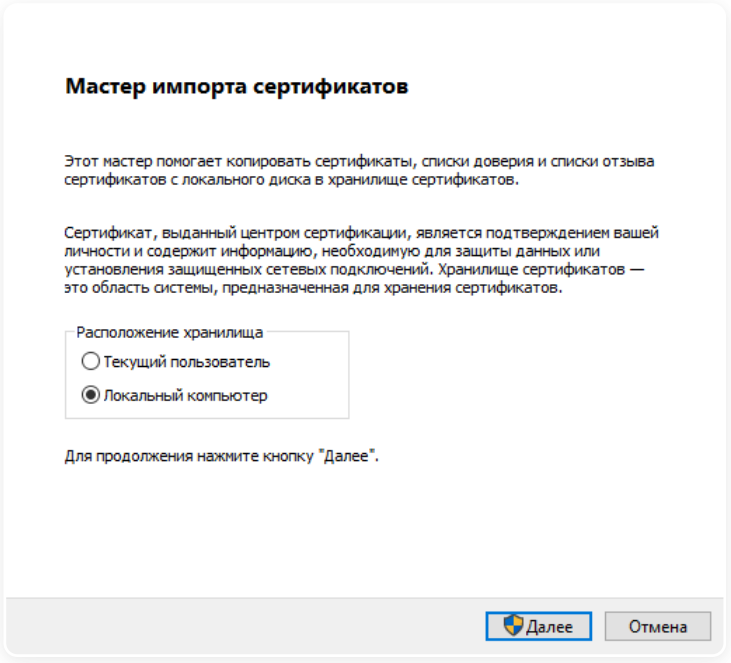
4. Импортируйте сертификат Ideco NGFW Novum:

Пример для Windows

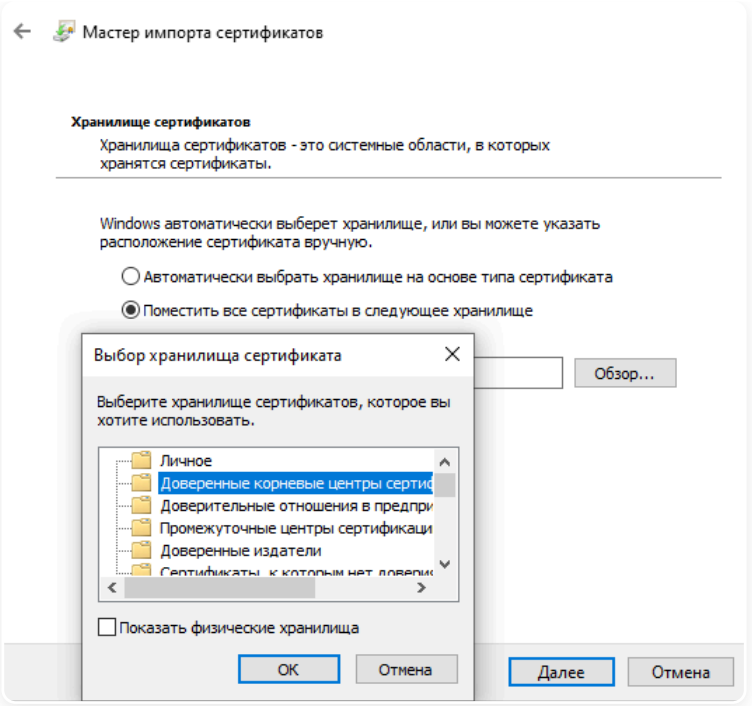
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



2. Выберите расположение хранилища **Локальный компьютер**:

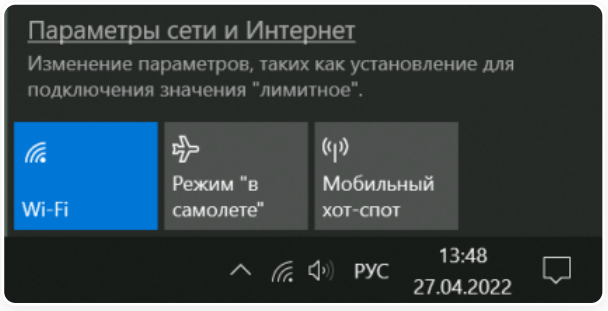


3. Установите сертификат в **Доверенные корневые центры сертификации**:

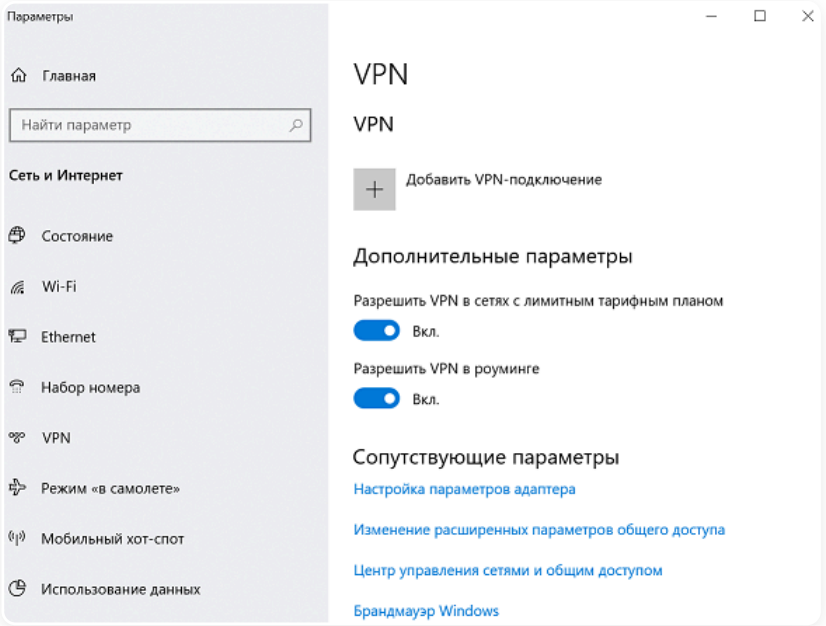


Создание подключения в Windows:

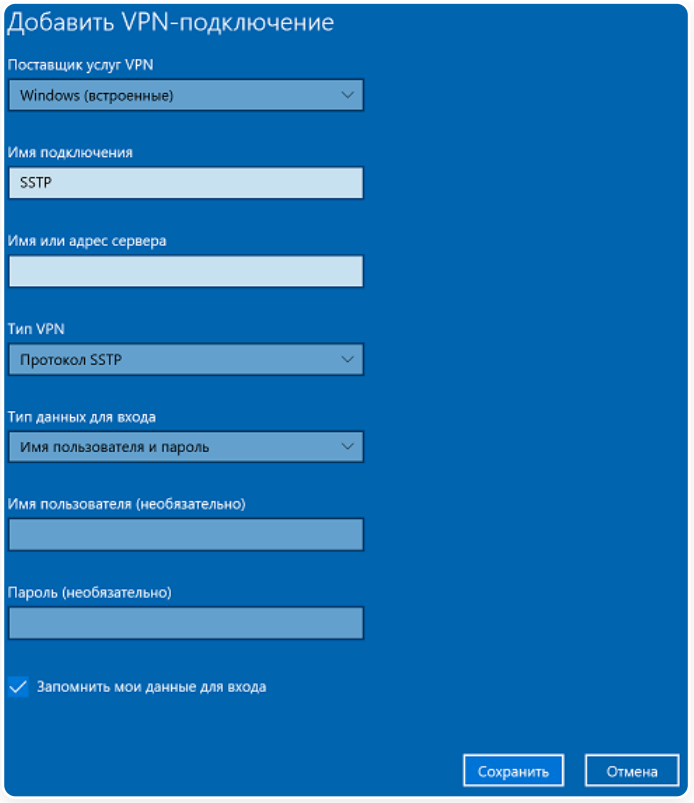
1. Кликните на иконку сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



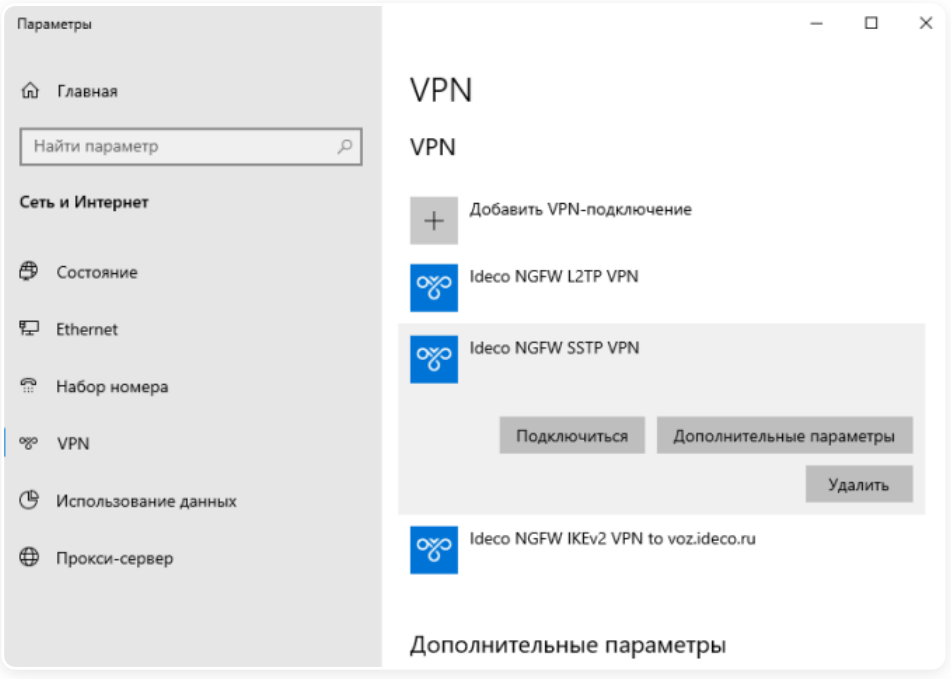
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера в формате ***адрес_VPN_сервера:порт***.
- **Тип VPN** - протокол SSTP.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).
- **Разрешить следующие протоколы** - протокол Microsoft CHAP версии 2 (MS-CHAP v2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры → Изменить**.

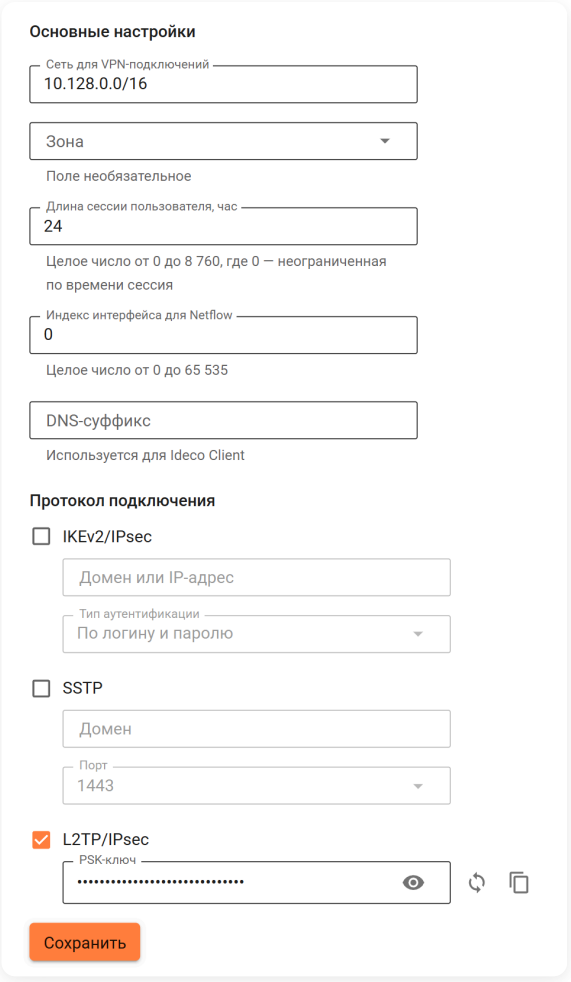
Вкладка 5

> **Важно:** L2TP/IPsec клиенты, находящиеся за одним NAT, могут испытывать проблемы подключения, если клиентов более одного. В решении проблемы поможет инструкция. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

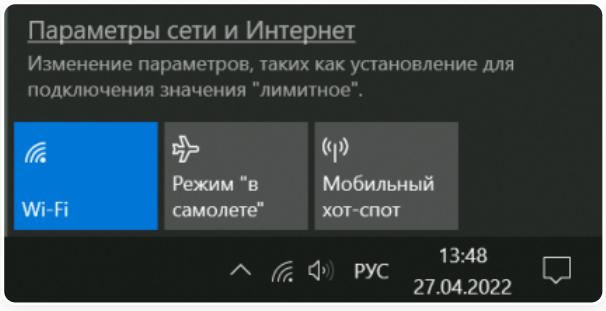
1. Перейдите в **Пользователи → VPN-подключения → Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

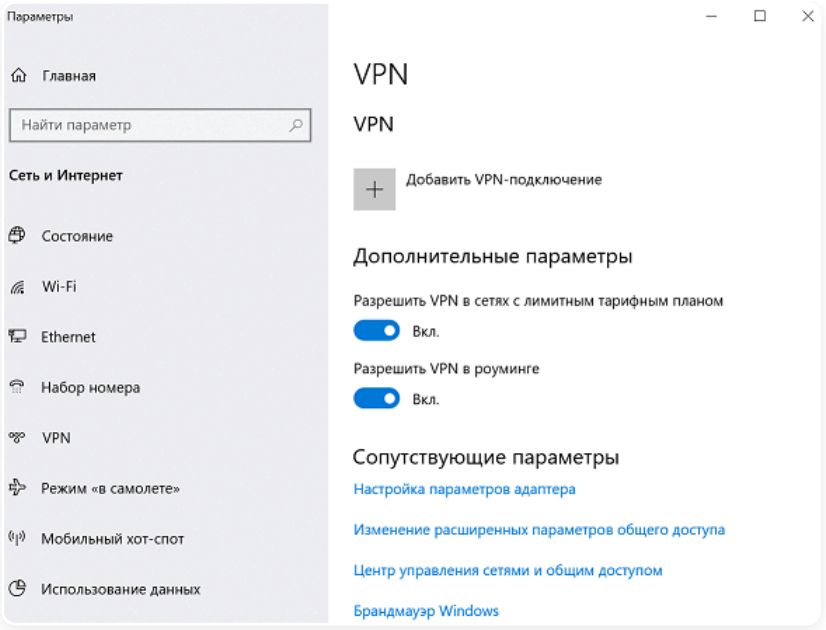


Создание подключения в Windows:

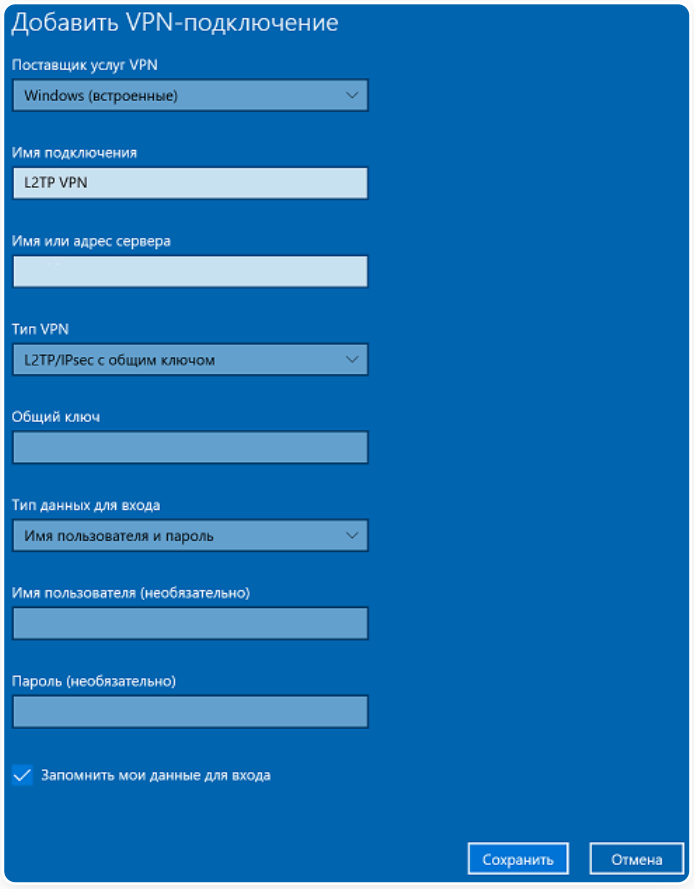
1. Кликните на иконку сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера.
- **Тип VPN** - протокол L2TP/IPsec с общим ключом.
- **Общий ключ** - значение поля **PSK** в разделе **Пользователи → VPN-подключения → Основное → Подключение по L2TP/IPsec**.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

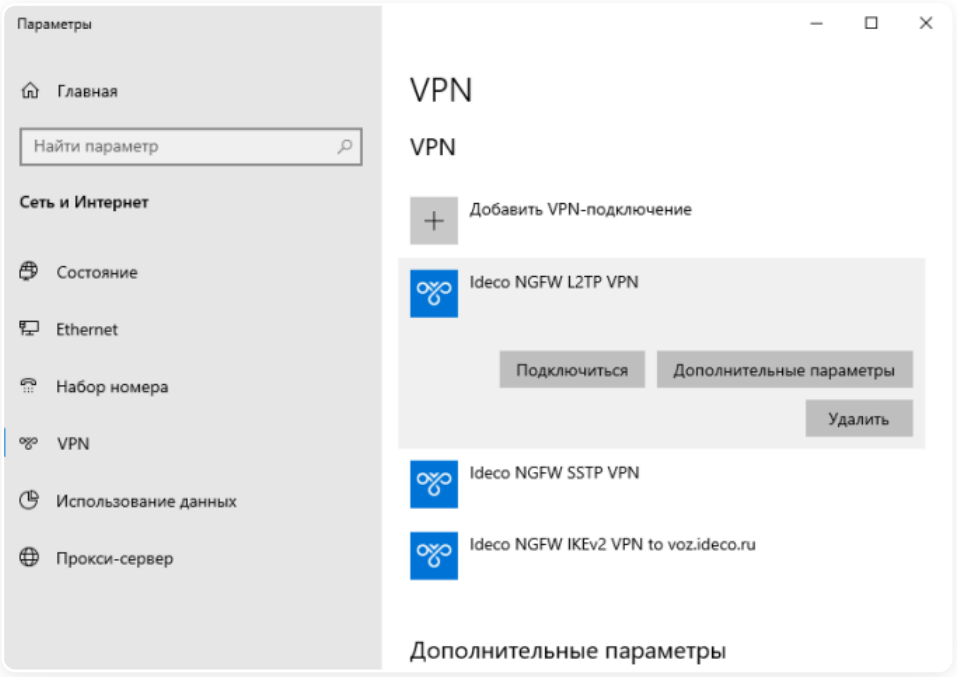
4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).

- **Разрешить следующие протоколы** - протокол Microsoft CHAP версии 2 (MS-CHAP v2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры** → **Изменить**.

Если создается VPN-подключение к NGFW через проброс портов:

1. Откройте **Редактор реестра**.

2. Перейдите в `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent` и создайте DWORD-параметр с именем AssumeUDPEncapsulationContextOnSendRule и значением `2`.

3. Перезагрузите Windows.

Возможные неполадки:

1. Неправильно указан логин или пароль пользователя. Часто при повторном соединении предлагается указать домен. Старайтесь создавать для учетных записей цифро-буквенные пароли, желательно на латинице. Если есть сомнения в этом пункте, то временно установите логин и пароль пользователю `user` и `123456`.

2. Чтобы пакеты пошли через VPN-туннель, надо убедиться, что в настройках этого подключения стоит чекбокс **Использовать основной шлюз в удаленной сети** в **Настройка параметров адаптера** → **Правой кнопкой мыши по подключению** → **Свойства** → **Сеть** → **Свойства опции "Протокол интернета версии 4 (TCP/IPv4)"** → **Дополнительно**. Если же маршрутизировать все пакеты в этот интерфейс не обязательно, то маршрут надо прописать вручную.

3. Подключение происходит через DNAT, т.е. внешний интерфейс Ideco NGFW Novum не имеет "белого" IP-адреса, а необходимые для работы порты (500 и 4500) "проброшены" на внешний интерфейс устройства, расположенного перед Ideco NGFW Novum и имеющего "белый" IP-адрес. В данном случае VPN-подключение либо вообще не будет устанавливаться, либо будут периодические обрывы. Решение - исключить устройство перед Ideco NGFW Novum и указать на внешнем интерфейсе Ideco NGFW Novum "белый" IP-адрес, к которому в итоге и будут осуществляться L2TP/IPsec-подключения. Либо используйте протокол SSTP, который проще опубликовать с помощью проброса портов.

4. Если в ОС Windows 10 повторно подключиться по L2TP, но при этом использовать **невалидный** ключ PSK (введя его в дополнительных параметрах), подключение все равно будет установлено успешно. Это связано с особенностями работы ОС.

Убедитесь, что локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. Если пересекается, то доступа к сети организации не будет (трафик по таблице маршрутизации пойдет в физический интерфейс, а не в VPN). Адресацию необходимо менять.

Ошибки работы VPN-подключений

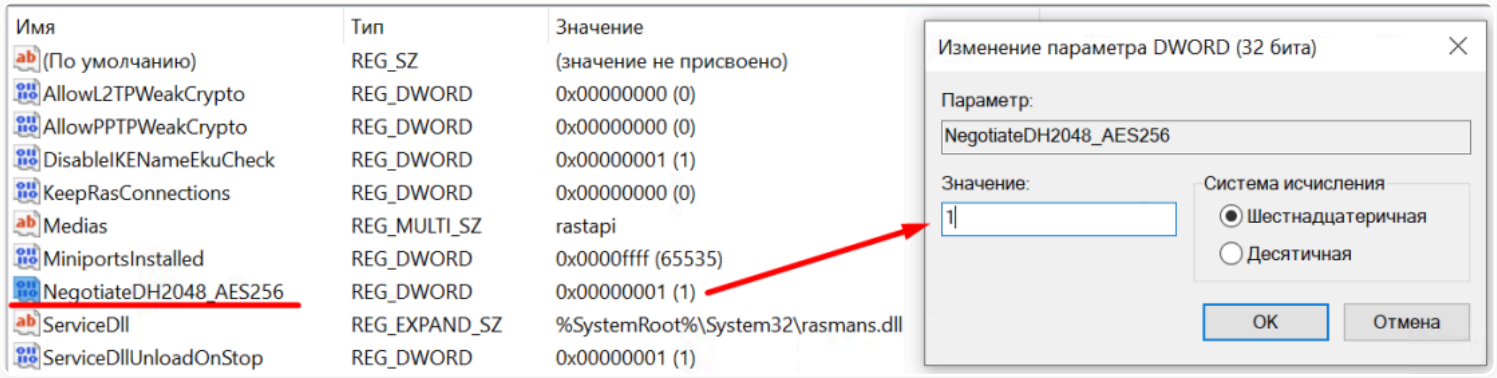
Если при подключении по IKEv2 возникает "Ошибка сопоставления групповой политики" или ошибка с кодом "13868"

Если VPN-подключение по протоколам IPSec в Windows автоматически разрывается через 7 часов 45 минут, для восстановления связи подойдут следующие действия:

1. Переподключите соединение. Соединение восстановится, но через 7 часов 45 минут вновь будет автоматически разорвано. Если требуется, чтобы подключение не разрывалось автоматически, то выполните действия из следующего пункта.

2. Внесите изменения в реестр:

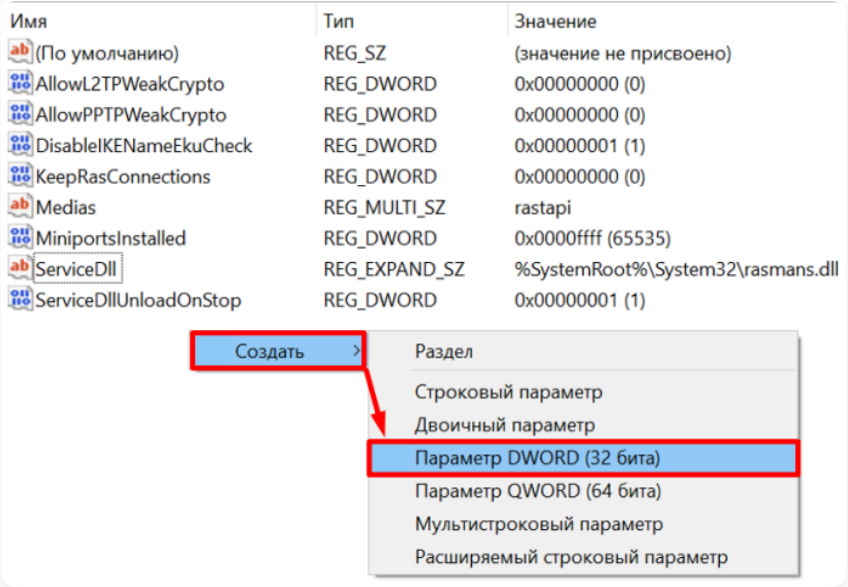
- Откройте **Редактор реестра**.
- Перейдите по пути `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters`.
- Нажмите правой кнопкой мыши по параметру с именем **NegotiateDH2048_AES256** и нажмите **Изменить**.
- В строке **Значение** укажите значение `1`:



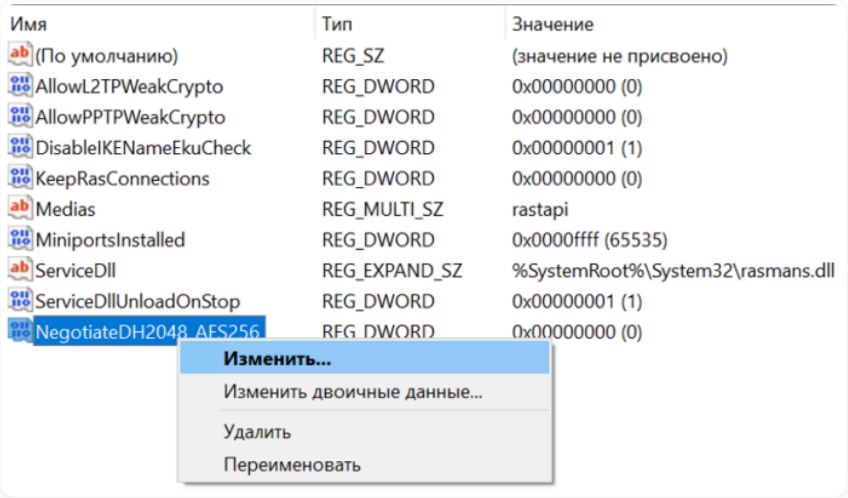
- Нажмите **OK**.
- Перезагрузите Windows.

Если параметра с именем **NegotiateDH2048_AES256** нет, то создайте его. Для этого:

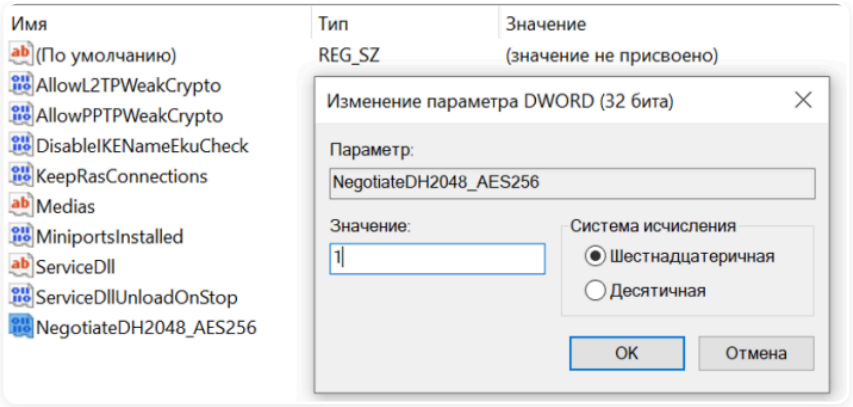
- Нажмите правой кнопкой мыши по свободному месту реестра в **Parameters** и выберите **Создать** → **DWORD**:



- Задайте имя **NegotiateDH2048_AES256**.
- Нажмите правой кнопкой мыши по созданному файлу и выберите **Изменить**:



- В строке **Значение** укажите значение `1`:



- Нажмите **OK**.

3. Перезагрузите Windows.

В Ideco NGFW Novum также есть возможность загрузить с сервера готовые скрипты для создания VPN-подключения в ОС Windows версий 8.1 и 10. Для загрузки и запуска скриптов воспользуйтесь инструкцией.

Создание VPN-подключения на мобильных устройствах

> В статье описана настройка VPN-подключения к Ideco NGFW Novum на мобильных устройствах по протоколам IKEv2/IPsec, L2TP/IPsec, SSTP.

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** в Ideco NGFW Novum и создайте разрешающее правило для VPN-подключения.

Применение сертификатов в протоколе IKEv2/IPsec и SSTP:

- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Скачать сертификат можно в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя, нажав **Скачать корневой сертификат**.

Не рекомендуем использовать для VPN-подключений кириллические логины.

Android

Android

Если в вашей версии Android возникают проблемы при подключении VPN описанными ниже способами, рекомендуем использовать сторонние приложения (например, StrongSwan).

1. Перейдите в **Настройки** → **Подключения** → **Другие настройки** → **VPN** и добавьте подключение. При необходимости воспользуйтесь строкой поиска по настройкам.

2. Выберите тип подключения и заполните поля:

IKEv2/IPsec MSCHAPv2

- **Название сети** - имя подключения.
- **Адрес сервера** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Идентификатор IPsec** - логин пользователя, которому разрешено подключение по VPN.
- **Сертификат ЦС IPsec** - не проверять сервер.
- **Сертификат сервера** - принято от сервера.
- **Имя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

L2TP/IPsec PSK

Начиная с версии Android 12 прекращена поддержка протокола L2TP. Не рекомендуем использовать L2TP, так как подключение крайне небезопасно.

- **Имя** - имя подключения.
- **Адрес сервера** - домен или IP-адрес Ideco NGFW Novum.

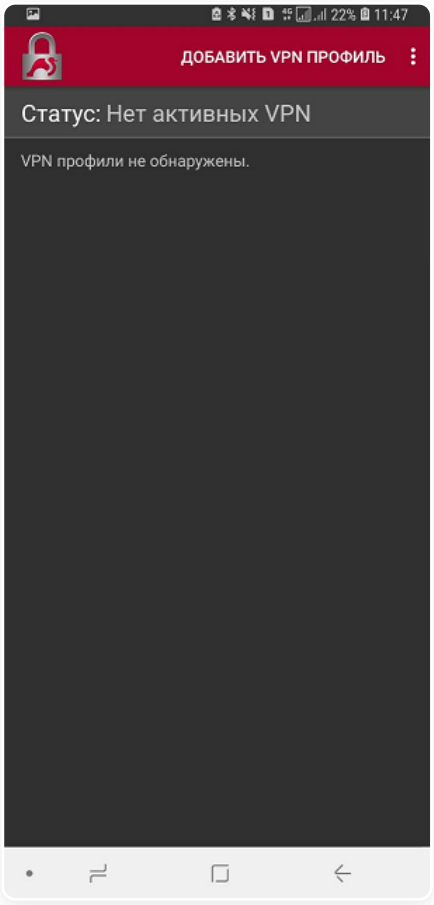
- **Общий ключ IPsec** - значение поля **PSK** в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по L2TP/IPsec** в Ideco NGFW Novum.

3. Нажмите **Сохранить** и активируйте подключение.

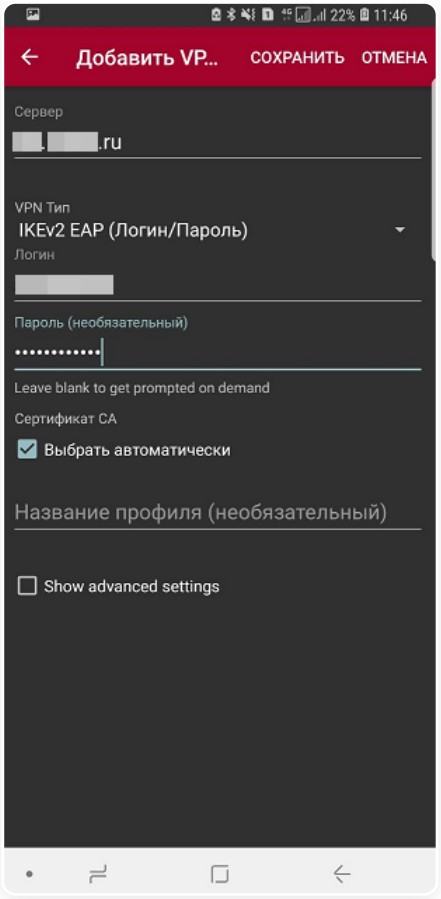
StrongSwan

> Приложение StrongSwan позволяет создавать VPN-подключение только через протокол IKEv2.

1. Нажмите **Добавить VPN профиль**:



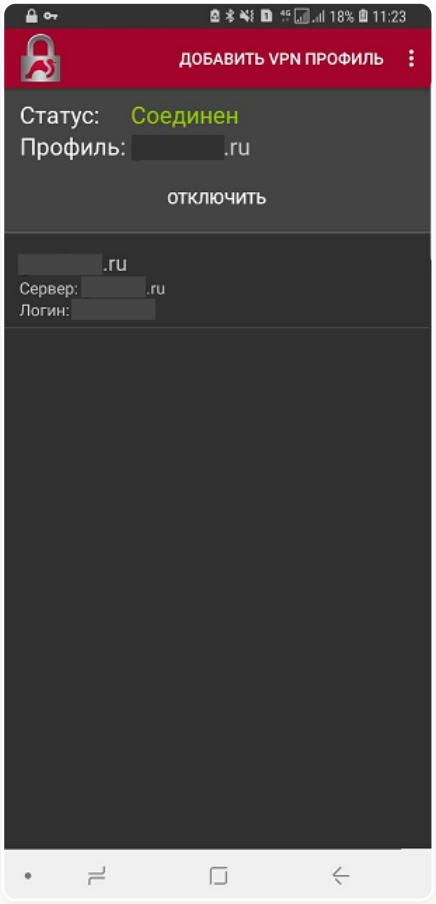
2. Заполните поля:



Расшифровка полей

- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **VPN тип** - IKEv2 EAP (Логин/Пароль).
- **Логин** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

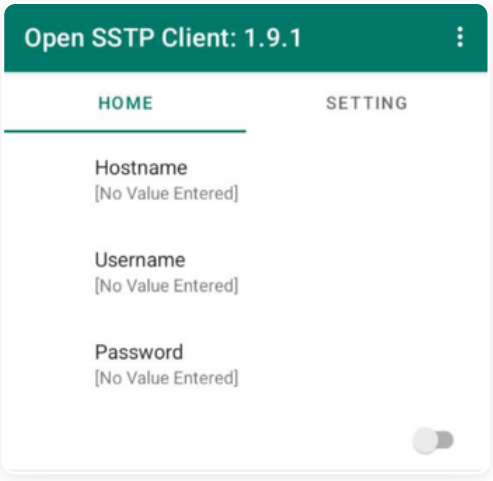
3. Нажмите **Сохранить** и перейдите по созданному подключению:



Open SSTP Client

Приложение Open SSTP Client позволяет создавать VPN-подключение через протокол SSTP.

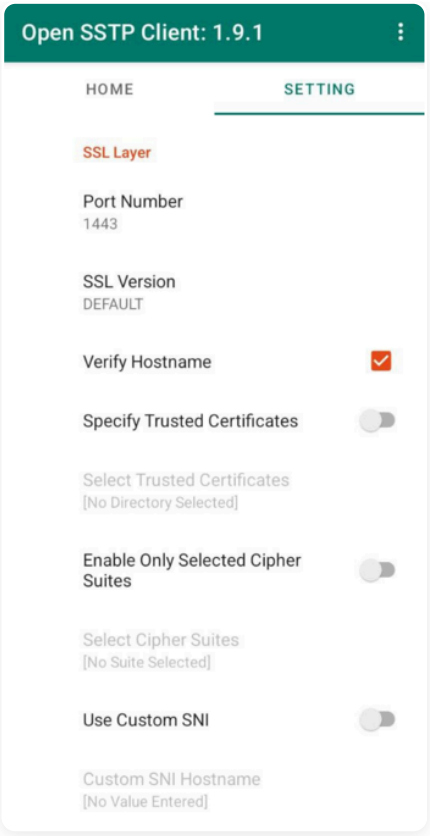
1. Откройте приложение и заполните поля:



Расшифровка полей

- **Hostname** - домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по SSTP**.
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

2. На вкладке **SETTING** укажите в поле **Port Number** порт подключения, указанный в NGFW. По умолчанию порт 1443.



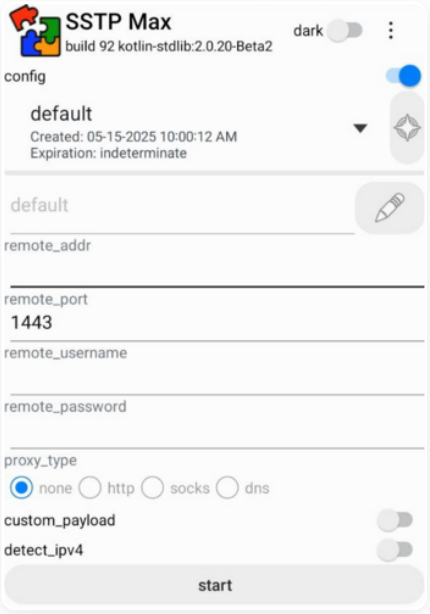
Для автоматического подключения включите опцию **Enable Reconnection** на вкладке **SETTING**.

3. На вкладке **HOME** переключите опцию в правом нижнем углу в положение включено.

SSTP Max

Приложение SSTP Max позволяет создавать VPN-подключение через протокол SSTP. Но рекомендуем к использованию приложение Open SSTP Client.

1. Откройте приложение и заполните поля:



Расшифровка полей

- **remote_addr** - домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по SSTP**.

- **remote_port** - порт подключения, указанный в NGFW. По умолчанию порт 1443.
- **remote_username** - логин пользователя, которому разрешено подключение по VPN.
- **remote_password** - пароль пользователя.

2. Нажмите start.

---

iOS

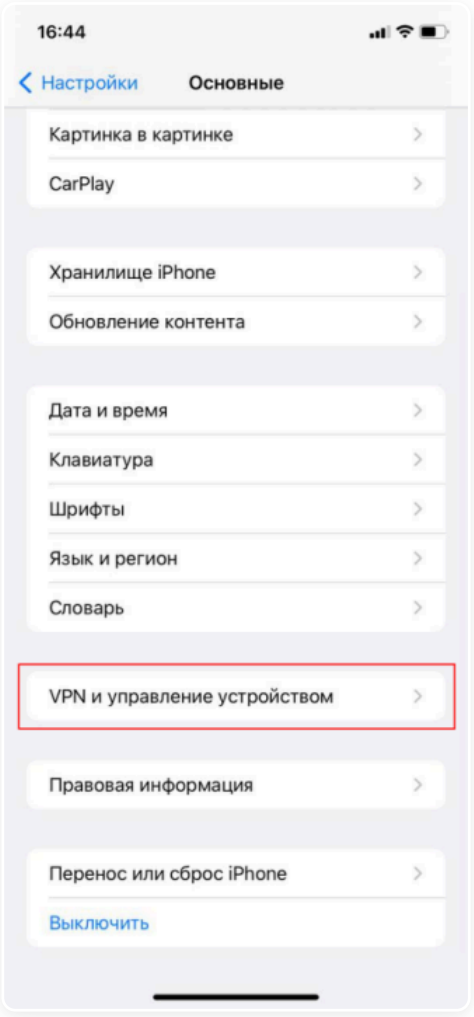
iOS

Выберите тип аутентификации пользователей и выполните действия:

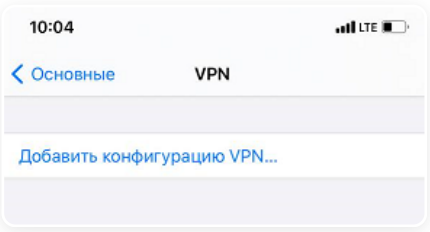
По логину и паролю **По сертификату**

Brooog IKEv2

1. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством** → **VPN**:

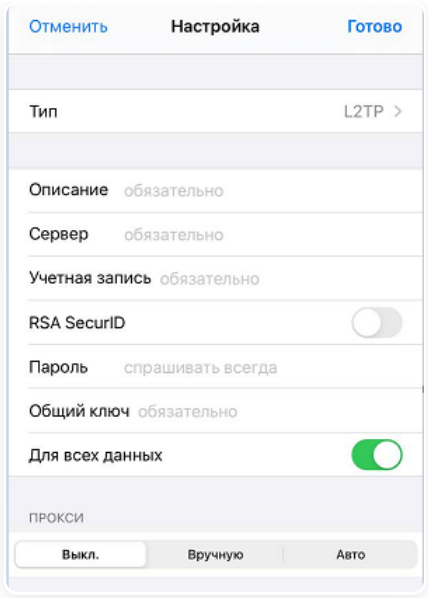


2. Нажмите **Добавить конфигурацию VPN**:



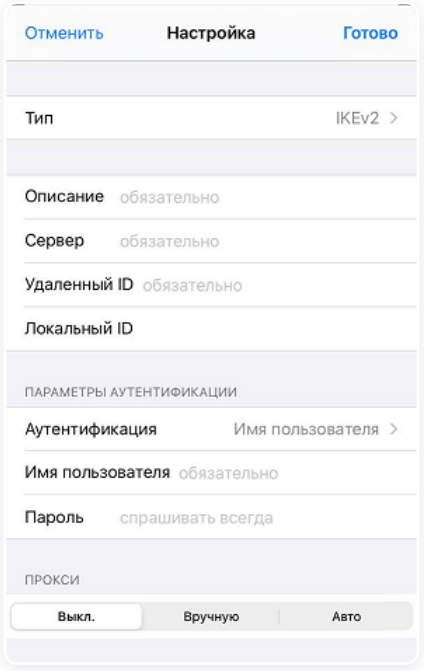
3. Выберите **Тип** подключения и заполните поля:

L2TP



- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес Ideco NGFW Novum.
- **Учетная запись** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.
- **Общий ключ** - значение поля **PSK** в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по L2TP/IPsec** в Ideco NGFW Novum.

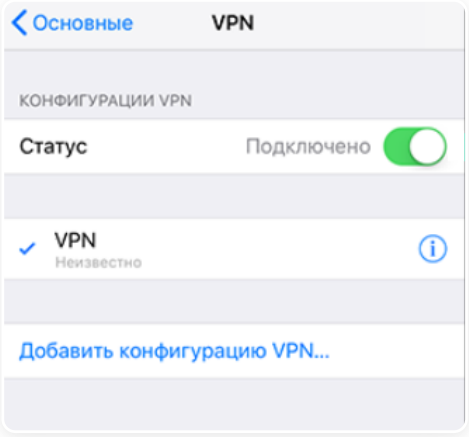
IKEv2



- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Удаленный ID** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

4. Нажмите **Готово**.

5. Включите опцию **Статус**:



Вкладка 3

Подготовка:

Для аутентификации пользователей по сертификату необходимо экспортировать:

- **Корневой сертификат** Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя.
- **Полную цепочку промежуточных сертификатов**, если сертификат пользователя выпущен промежуточным УЦ.
- **Пользовательский сертификат**.

Требования к сертификатам

Алгоритмы хеширования:

- Для подписи сертификатов рекомендуется использовать алгоритм SHA-256 или более стойкий (например, SHA-384, SHA-512).
- Алгоритм SHA-1 не поддерживается.

Ключевые расширения:

- **Для промежуточного сертификата:**
- `basicConstraints=critical,CA:TRUE` - используется для указания, что сертификат может подписывать другие сертификаты.
- **Для пользовательского сертификата:**
- `subjectAltName=DNS:...` - используется для указания альтернативных имен (например, DNS или IP-адреса).

Примеры генерации сертификатов УЦ:

Создание корневого и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **CN** - укажите логин учетной записи пользователя для авторизации.

3. Подписание пользовательского сертификата корневым:

```
openssl x509 -req -in client.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

4. Создание PFX-архива для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile rootCA.crt -passout pass:1234
```

Создание корневого, промежуточного и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание промежуточного сертификата:

```
openssl genrsa -out interCA.key 4096
openssl req -new -key interCA.key -out interCA.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"

openssl x509 -req -in interCA.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out interCA.crt -days 1825 -sha256 \
-extfile <(printf "basicConstraints=critical,CA:TRUE")
```

3. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **Common Name (CN)** - укажите логин учетной записи пользователя для авторизации.

4. Подписание пользовательского сертификата промежуточным:

```
openssl x509 -req -in client.csr -CA interCA.crt -CAkey interCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

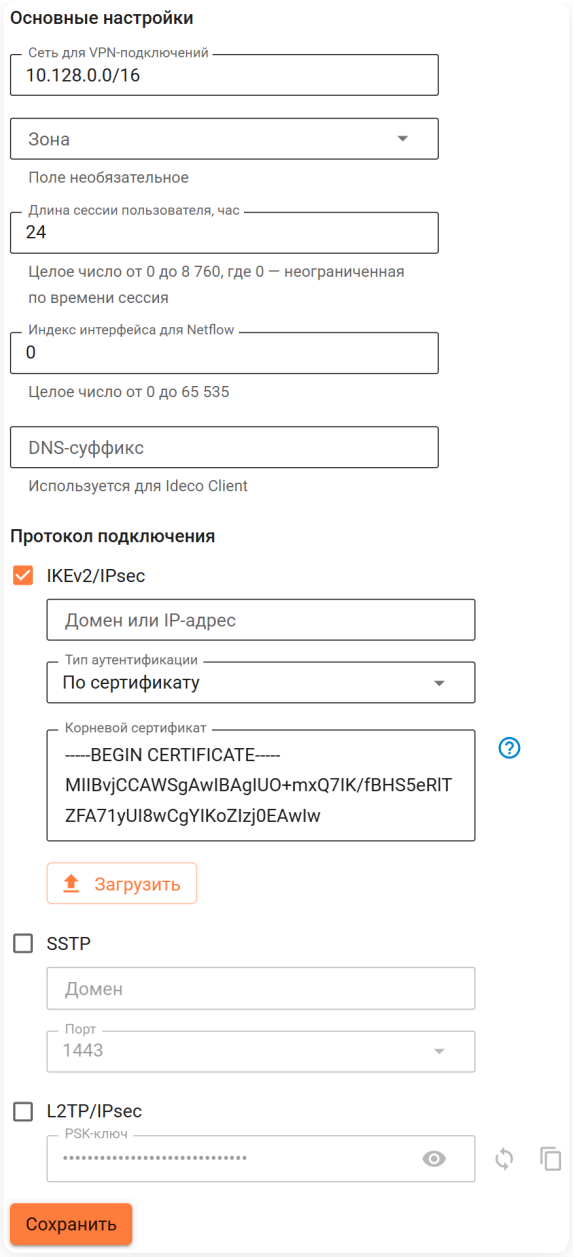
5. Создание PFX-архива с полной цепочкой доверия для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile <(cat interCA.crt rootCA.crt) -passout pass:1234
```

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Домен и IP-адрес** - укажите доменное имя или IP-адрес, по которому будут подключаться пользователи.
- **Тип аутентификации** - выберите тип **По сертификату**.
- **Корневой сертификат** - загрузите корневой сертификат УЦ или объединенный в один файл корневой и все промежуточные сертификаты.

3. Нажмите **Сохранить**.

4. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

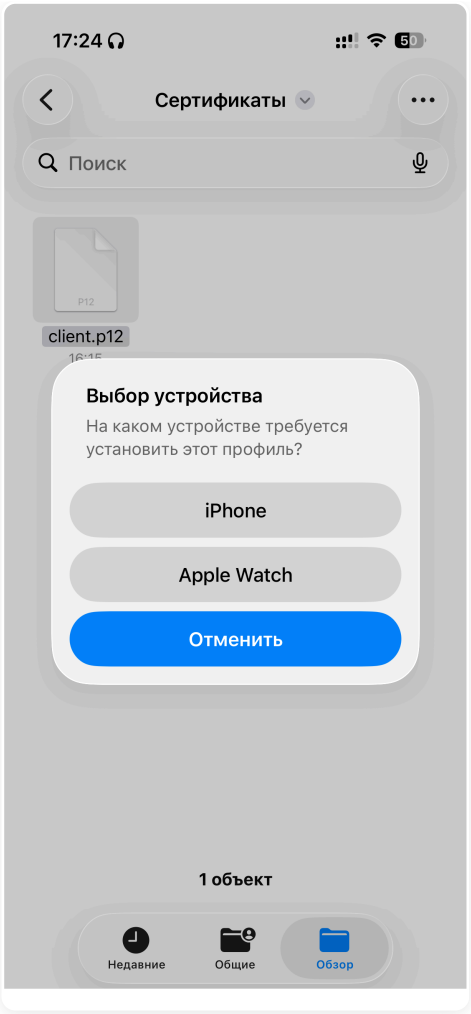
Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в IOS:

1. Загрузите пользовательский сертификат на устройство пользователя.

2. Нажмите на сертификат и выберите устройство, на которое требуется установить профиль:

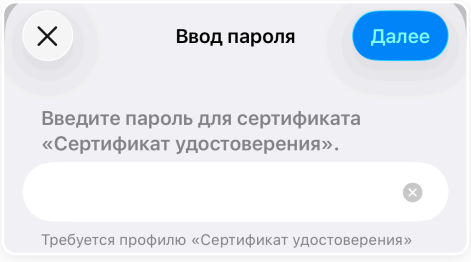


3. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством**.

4. В блоке **Загруженный профиль** выберите **Сертификат удостоверения** и нажмите **Установить**:

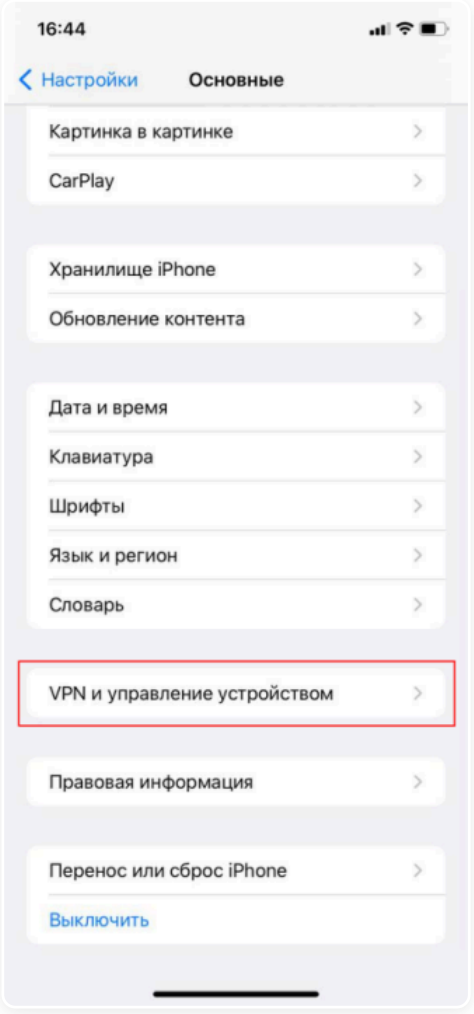
5. Введите код-пароль, используемый для разблокировки устройства, и нажмите **Установить**.

6. Введите пароль для сертификата и нажмите **Далее**:

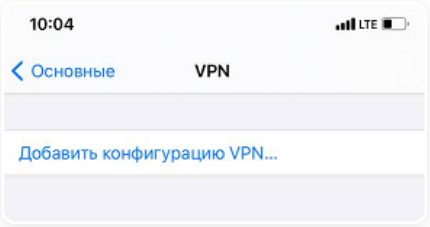


7. Нажмите .

8. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством** → **VPN**:



9. Нажмите **Добавить конфигурацию VPN**:

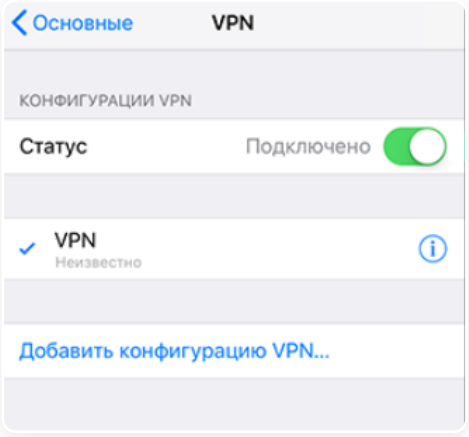


10. Заполните поля:

- **Тип** - выберите IKEv2.
- **Описание** - введите название соединения.
- **Сервер** - укажите домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Удаленный ID** - укажите домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Локальный ID** - введите логин пользователя.
- **Аутентификация** - выберите **Сертификат**.
- **Сертификат** - выберите сертификат.

11. Нажмите .

12. Включите опцию **Статус**:



Вкладка 4

1. Нажмите **Add VPN Connection**:

2. Заполните поля и включите опцию **Connect on Demand**:

Расшифровка полей

- **Server** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

3. Нажмите **Save** и переведите опцию в режим **CONNECTED**:

Полезные ссылки

- **VPN-подключения**
- **Подключение по IKEv2/IPsec**

Инструкция по созданию подключения в macOS

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Не рекомендуем использовать для VPN-подключений кириллические логины.

При проблемах с подключением на IOS требуется:

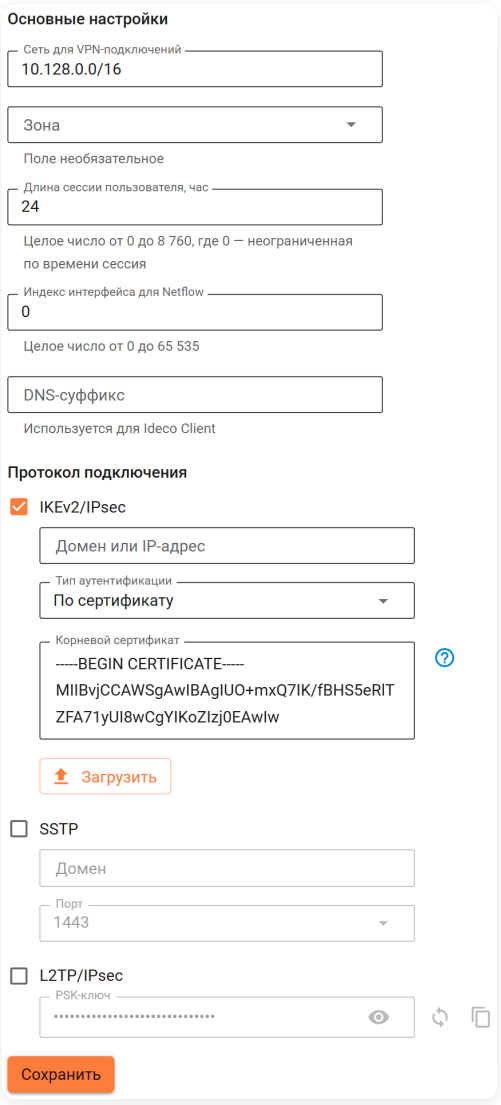
1. Проверить, что в качестве VPN-сервера указано доменное имя VPN-сервера в разделе **Пользователи** → **VPN-подключения**.
2. Проверить, что на доменное имя VPN-сервера выдан сертификат Let's Encrypt.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.

- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

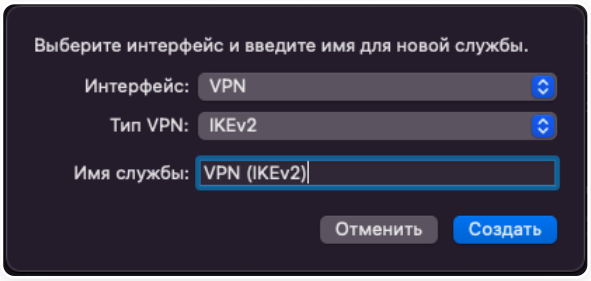
- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в macOS:

1. Перейдите в **Системные настройки** → **Сеть**.

2. Нажмите **Добавить** в левом нижнем углу (иконка +).

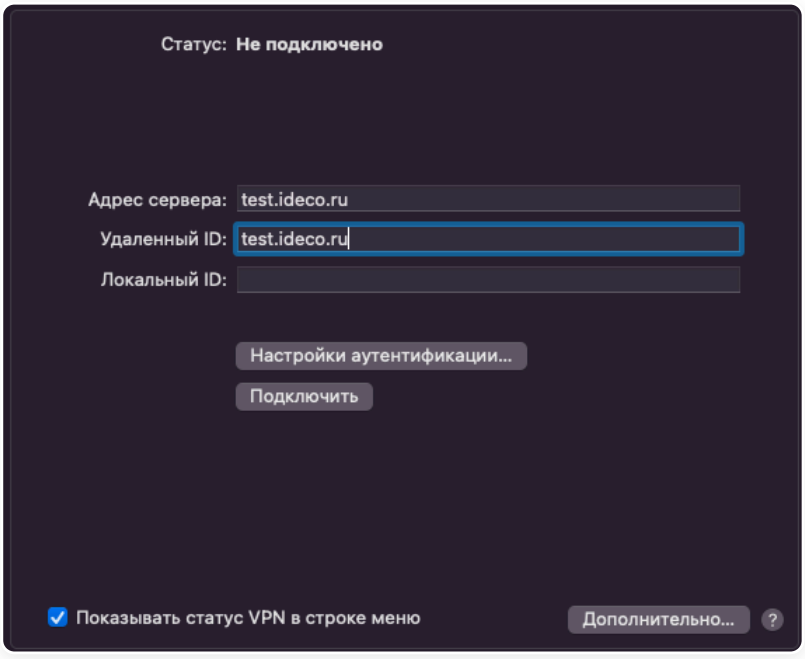
3. Заполните поля:



- **Интерфейс** - VPN.
- **Тип VPN** - IKEv2.
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

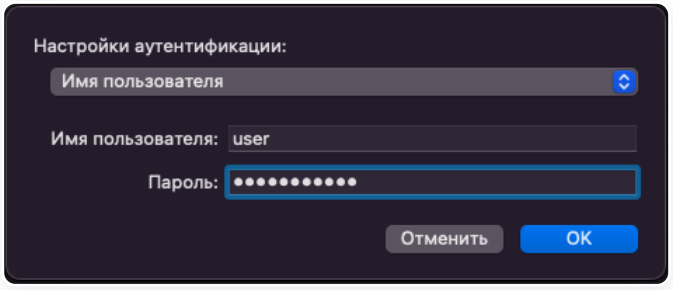
5. Установите параметры подключения:



- **Адрес сервера** - адрес VPN-сервера.
- **Удаленный ID** - продублируйте адрес VPN-сервера.

6. Выберите **Настройки аутентификации**.

7. Укажите идентификационные данные и нажмите **OK**:



- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

8. Нажмите **OK**.

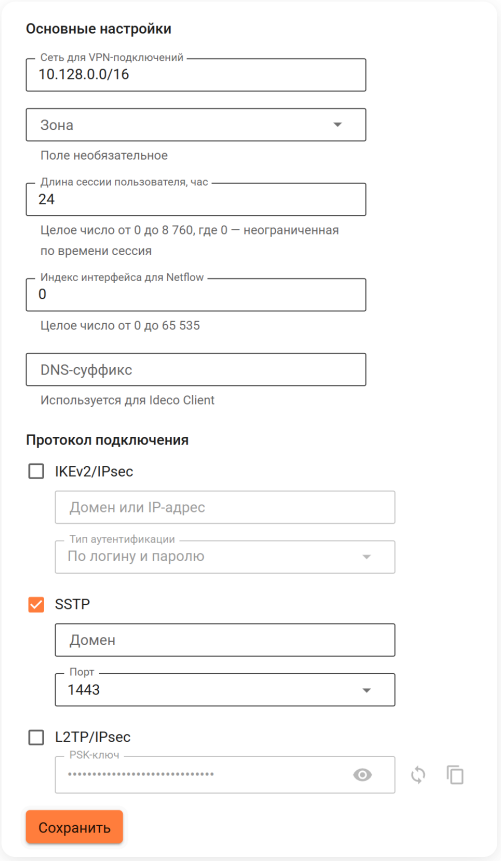
9. Включите опцию **Показывать статус VPN в строке меню**, нажмите **Применить** и включите соединение.

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в macOS:

1. Откройте терминал и установите `sstp-client`, выполнив команды:

```
brew update
brew install sstp-client
```

2. Создайте и включите SSTP-подключение. Путь к утилите `sstpc` зависит от процессора Mac:

> Узнать архитектуру процессора можно командой `uname -m`:
>
> - `arm64` - Apple Silicon.
> - `x86_64` - Intel.
>
> Также путь установки Homebrew покажет команда `brew --prefix`.

- **Для Mac с процессорами Apple Silicon (M1/M2/M3/M4)** - каталог `/opt/homebrew`:

```
sudo /opt/homebrew/sbin/sstpc --cert-warn --tls-ext --user <логин пользователя Ideco NGFW Novum> --password <пароль польз
```

- **Для Mac с процессорами Intel** - каталог `/usr/local`:

```
sudo /usr/local/sbin/sstpc --cert-warn --tls-ext --user <логин пользователя Ideco NGFW Novum> --password <пароль пользова
```

Если указан параметр `defaultroute`, в VPN-туннель будет заворачиваться весь трафик.

Чтобы через VPN-туннель проходил только трафик до определенных сетей, используйте параметр `nodefaultroute` и добавьте маршруты в таблицу маршрутизации вручную, например: `sudo route add -net "172.16.0.0/12" -interface ppp0`.

3. Для проверки подключения откройте новую вкладку или окно терминала и введите команду `ifconfig -a`. Если в выводе присутствует строка вида `ppp0: flags=8051 mtu 1500 inet 10.128.0.0 → 10.128.0.1 netmask 0xff000000`, подключение установлено.

4. Чтобы отключить соединение, перейдите в терминал, из которого соединение было установлено, и нажмите **Ctrl+C**.

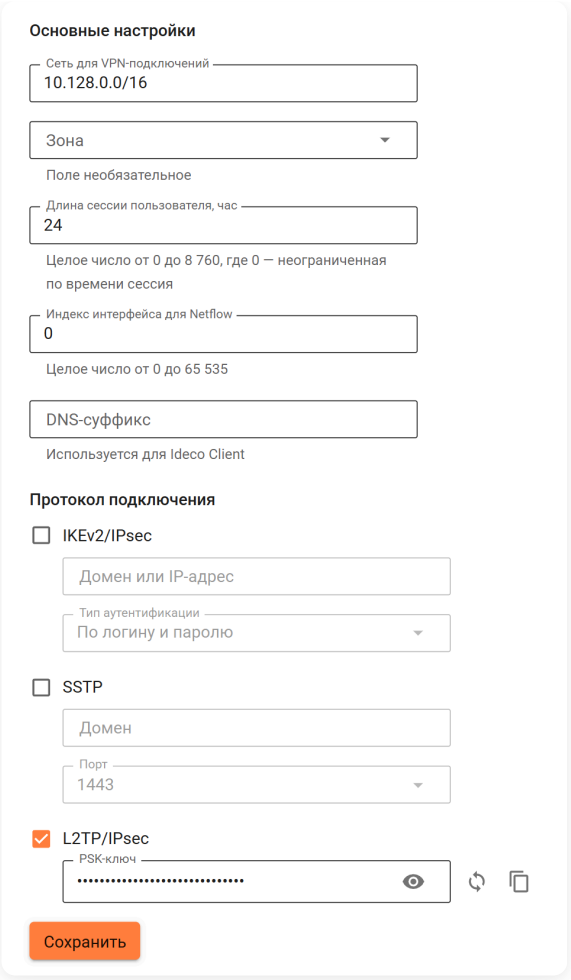
L2TP/IPsec

Важно: L2TP/IPsec-клиенты, находящиеся за одним NAT, могут испытывать проблемы с подключением, если клиентов более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

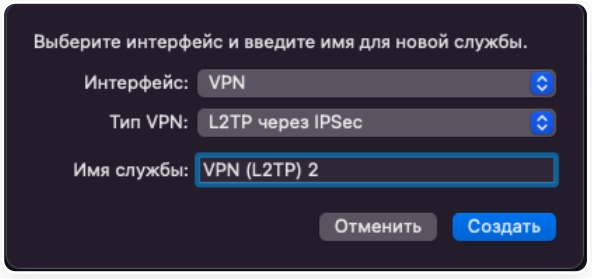
2. Включите опцию **L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в macOS:

1. Перейдите в **Системные настройки** → **Сеть** и нажмите **Добавить** в левом нижнем углу (иконка (+)).

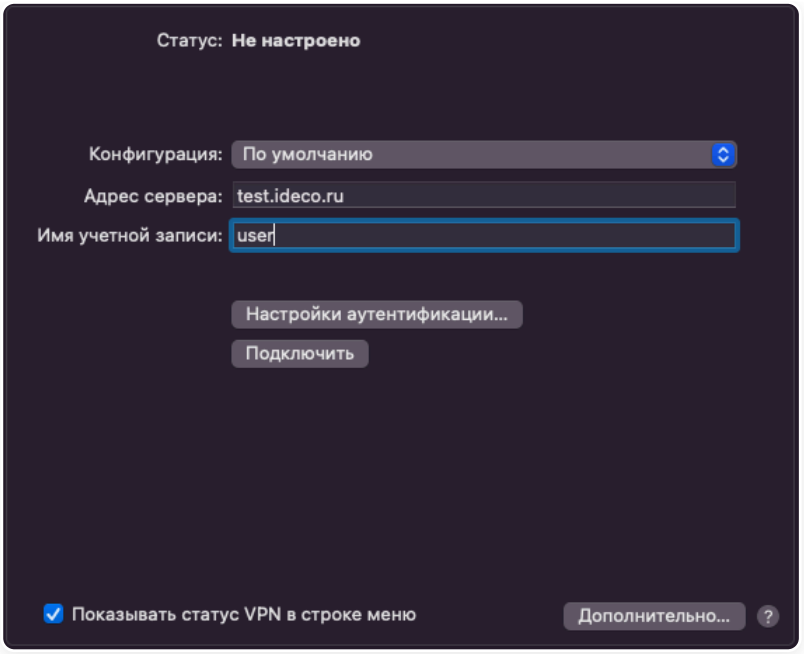
3. Заполните поля:



- **Интерфейс** - VPN.
- **Тип VPN** - L2TP через IPsec.
- **Имя службы** - имя подключения.

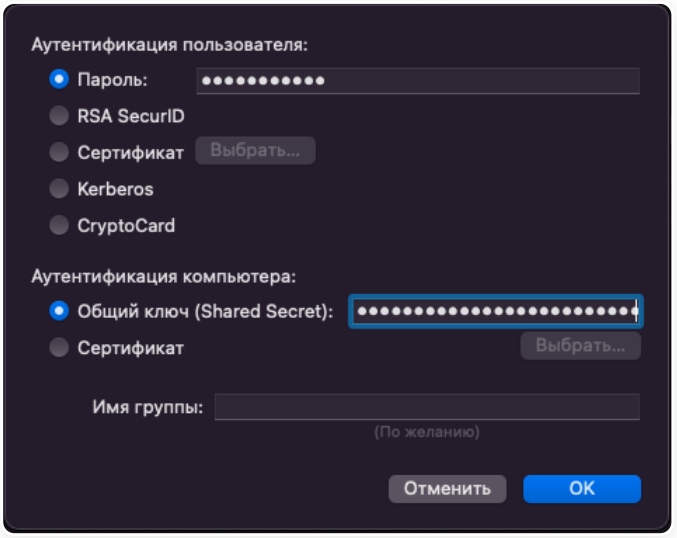
4. Нажмите **Создать**.

5. Заполните **Адрес сервера** и **Имя учетной записи**:



6. Включите опцию **Показывать статус VPN в строке меню** и выберите **Настройки аутентификации**.

7. В **Аутентификации пользователя** заполните **Пароль**, в **Аутентификации компьютера** - **Общий ключ (Shared Secret)**:



8. Нажмите **ОК** → **Применить** и включите соединение.

Полезные ссылки

- **VPN-подключения**

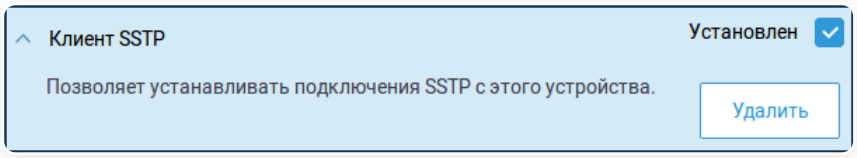
Подключение по SSTP Wi-Fi-роутеров Keenetic

Поддерживаются все роутеры на базе KeeneticOS 3.x.x.

1. Выполните настройку пользователей в Ideco NGFW Novum и включите SSTP в **Пользователи** → **VPN-подключения** → **Основное**.

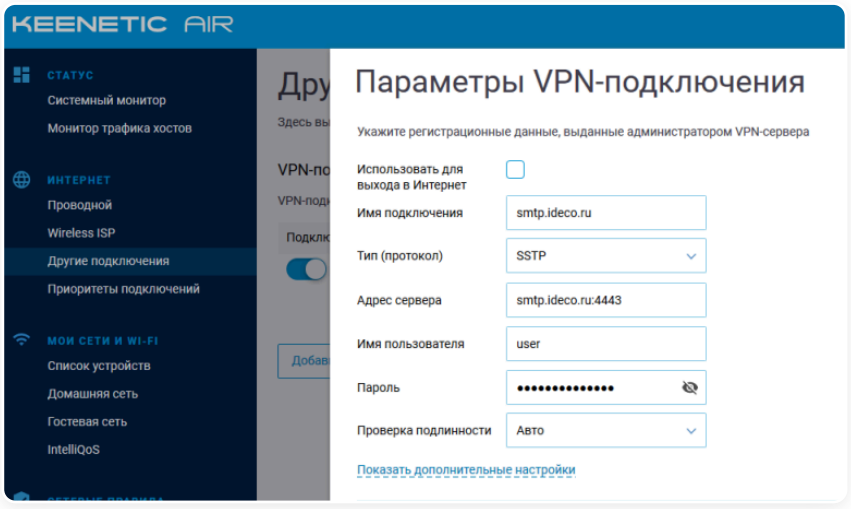
2. Зайдите в веб-интерфейс управления Keenetic: `http://my.keenetic.net`.

3. Установите компонент системы **Клиент SSTP** на странице **Общие настройки** в разделе **Обновления и компоненты**, нажмите **Изменить набор компонентов**:



Подробнее о настройках в документации Keenetic.

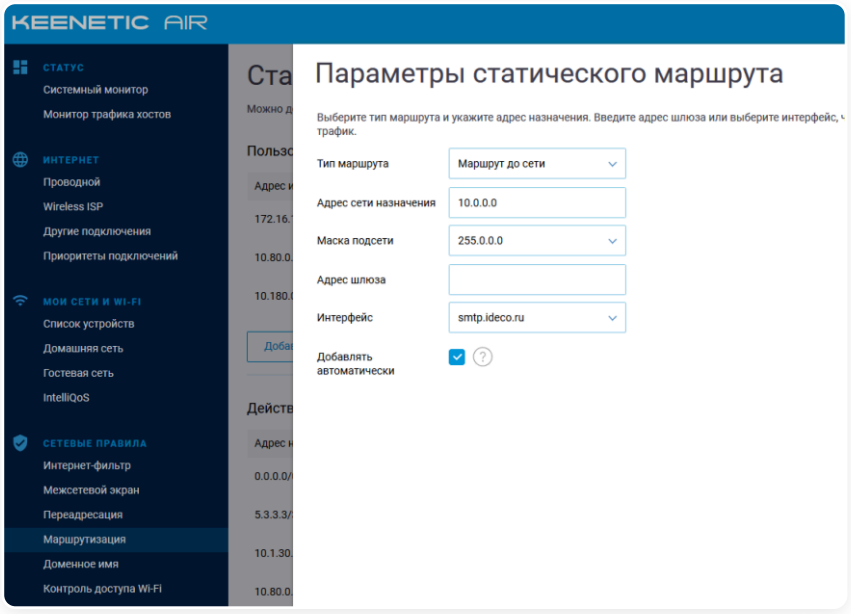
4. Создайте подключение в **Интернет** → **Другие подключения** нажмите кнопку **Добавить подключение**



Не устанавливайте флаг **Использовать для выхода в интернет**.

Введите имя подключения, протокол SSTP, адрес сервера (**обязательно укажите в адресе порт через двоеточие**), имя пользователя и пароль.

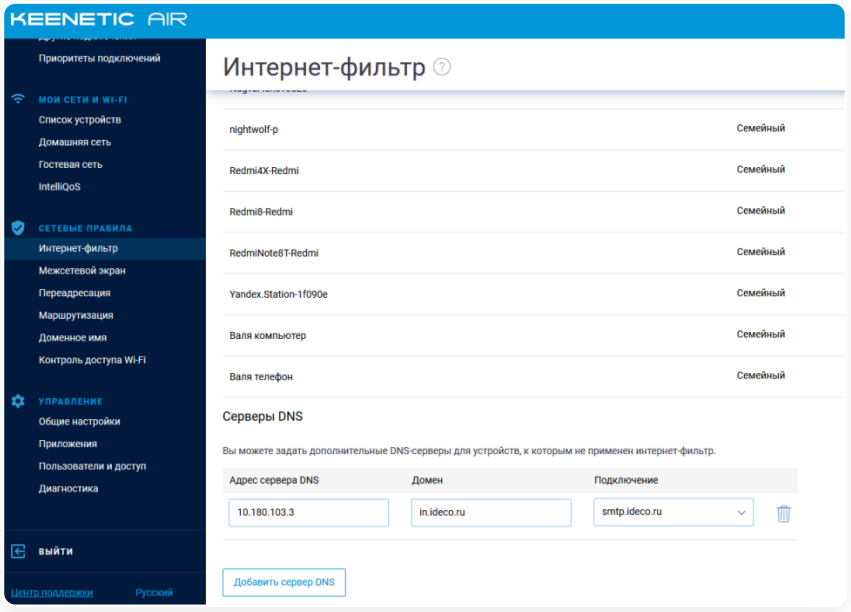
5. В **Сетевые правила** → **Маршруты** добавьте маршруты в рабочую сеть. Например, если сеть офиса `10.0.0.0/8`, добавьте маршрут:



Выберите в качестве **Интерфейса** созданное VPN-подключение и установите флаг **Добавлять автоматически**, чтобы маршрут действовал только при активном VPN-подключении.

6. Настройте DNS для локального домена (например, Active Directory), чтобы обращаться к ресурсам (файловым и иным серверам) по DNS-именам.

В **Сетевые правила** → **Интернет-фильтр** → **Серверы DNS** укажите DNS-сервер контроллера домена и имя домена:



Настройка закончена.

7. Используйте утилиту **ping** в командной строке для проверки связи и маршрутизации.

`nslookup` - для проверки резолвинга локальных имен рабочей сети.

Если VPN работает, но с некоторыми ресурсами (например, файловыми или RDP) нет связи, воспользуйтесь инструкцией для диагностики проблем.

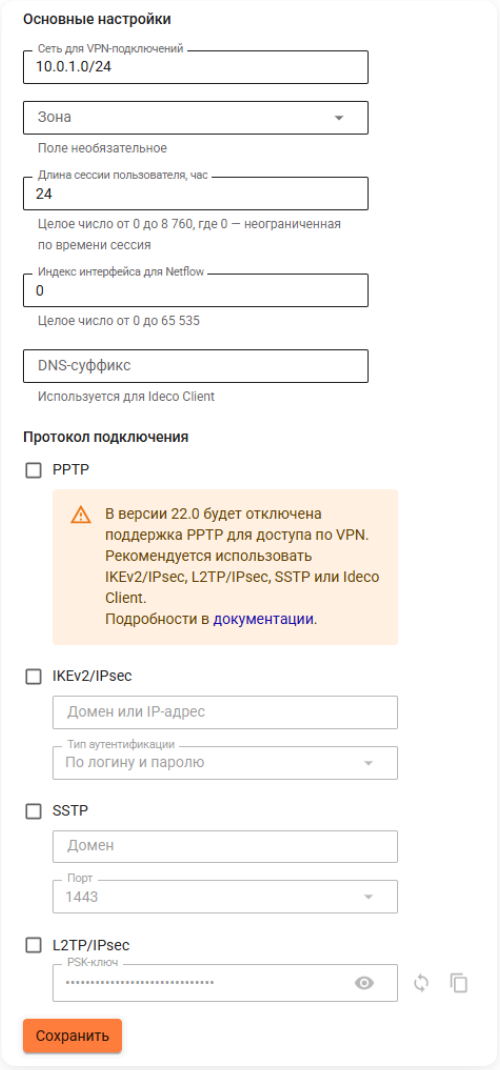
Полезные ссылки

- **Подключение по SSTP**

Как избежать проблем с подключением VPN-клиентов при использовании нескольких серверов Ideco NGFW Novum

При использовании нескольких серверов Ideco NGFW Novum могут возникнуть проблемы с подключением VPN-клиентов. Частая причина - пересечение подсетей, используемых для выдачи IP-адресов удаленным пользователям.

Для решения проблемы настройте изолированные подсети для каждого сервера в **Пользователи** → **VPN-подключения** → **Основное**:



В поле **Сеть для VPN-подключений** укажите уникальные значения, например:

- Для ideco1 - `10.0.1.0/24`.
- Для ideco2 - `10.0.2.0/24`.

Подробнее о настройке VPN-подключений - в статье.

Избегайте пересечений подсетей с другими сервисами внутри одного сервера. Убедитесь, что подсеть для VPN не пересекается с:

- Диапазонами IP-адресов для выдачи в **Сервисы** → **DHCP**.
- Правилами авторизации **По подсетям**. Подробнее - в статье.
- Статическими привязками в **Пользователи** → **VPN-подключения** → **Выдача IP-адресов**.

Если проблема сохраняется, обратитесь в Техническую поддержку.

Полезные ссылки

- **VPN-подключения**
- **Особенности маршрутизации и организации доступа**

Подключение Keenetic по SSTP или IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Для создания подключения используются протоколы:

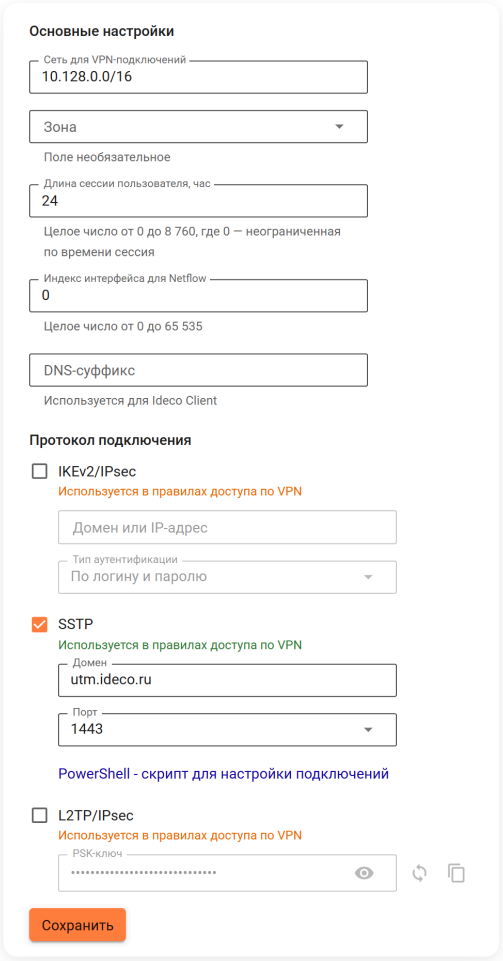
- **SSTP** - для безопасного соединения между клиентом и сервером.
- **IPsec** - для безопасной передачи данных в IP-сетях.

Подключение по SSTP

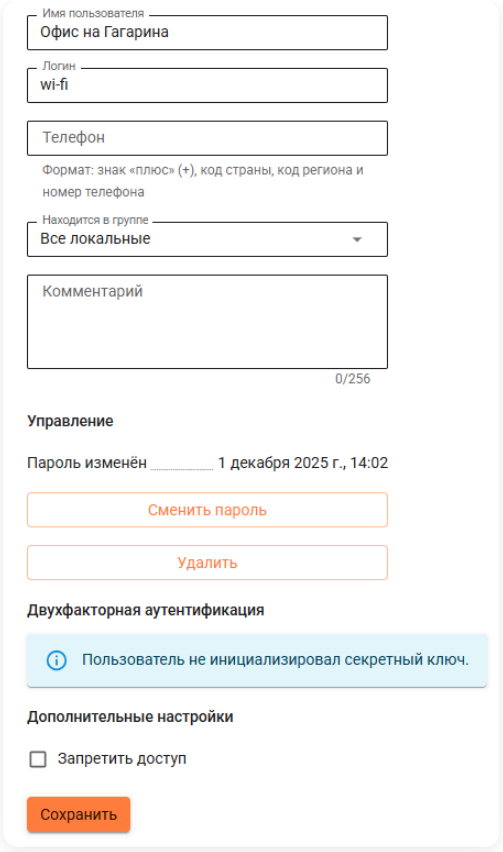
Если доступ из центрального офиса в сеть за Keenetic не нужен, воспользуйтесь инструкцией по подключению в режиме client-to-site.

Настройка Ideco NGFW Novum

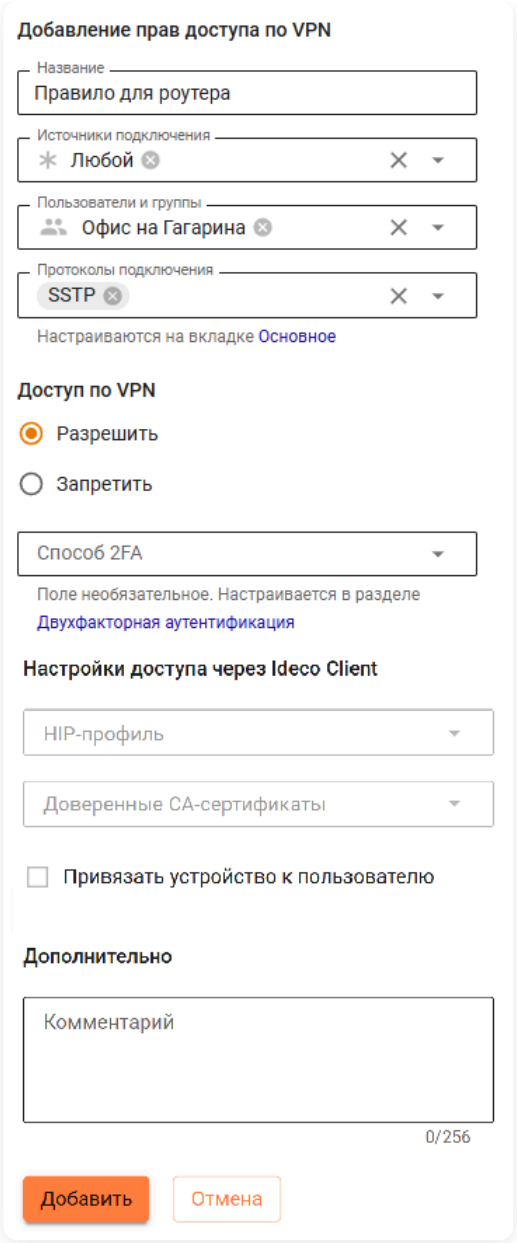
1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**, включите настройку SSTP, укажите домен и порт для подключения:



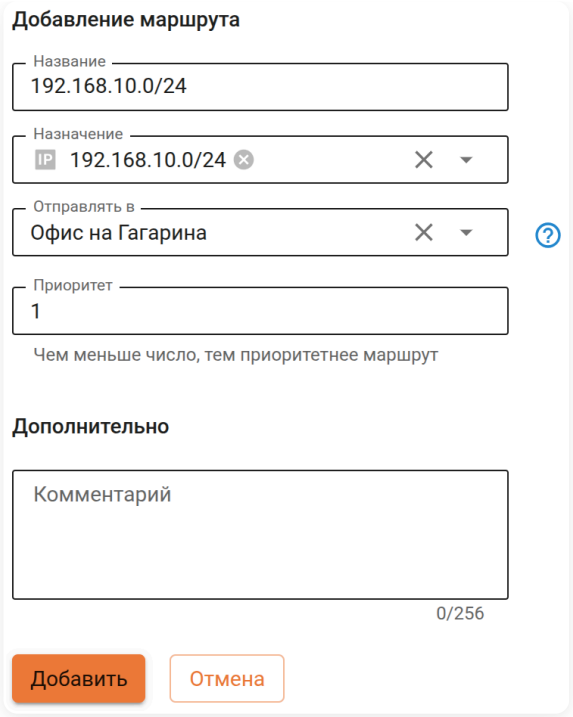
2. Перейдите в **Пользователи** → **Учетные записи** и создайте специального пользователя для удаленного роутера. Логин и пароль пользователя будут использоваться на роутере:



3. Перейдите в **VPN-подключения** → **Доступ по VPN** и создайте правило доступа по VPN для этого пользователя:



4. Пропишите маршруты в удаленную сеть. Например, если сеть за роутером `192.168.10.0/24`, необходимо добавить маршрут в **Маршрутизация** → **Статическая**:



Настройка роутера Keenetic

Настройте VPN-подключение роутера Keenetic по инструкции для client-to-site подключений.

Необходимо выполнить все три пункта:

1. Настроить VPN-подключение.

2. Настроить маршруты.

3. Настроить DNS для резолвинга локального домена (если используете Active Directory).

Для проверки связи используйте утилиты ping и traceroute.

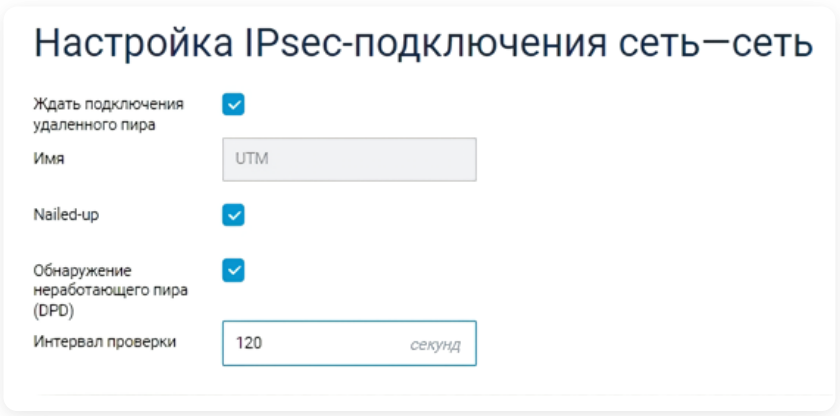
Доступ часто блокируется в Windows из-за настроек сетевых профилей.

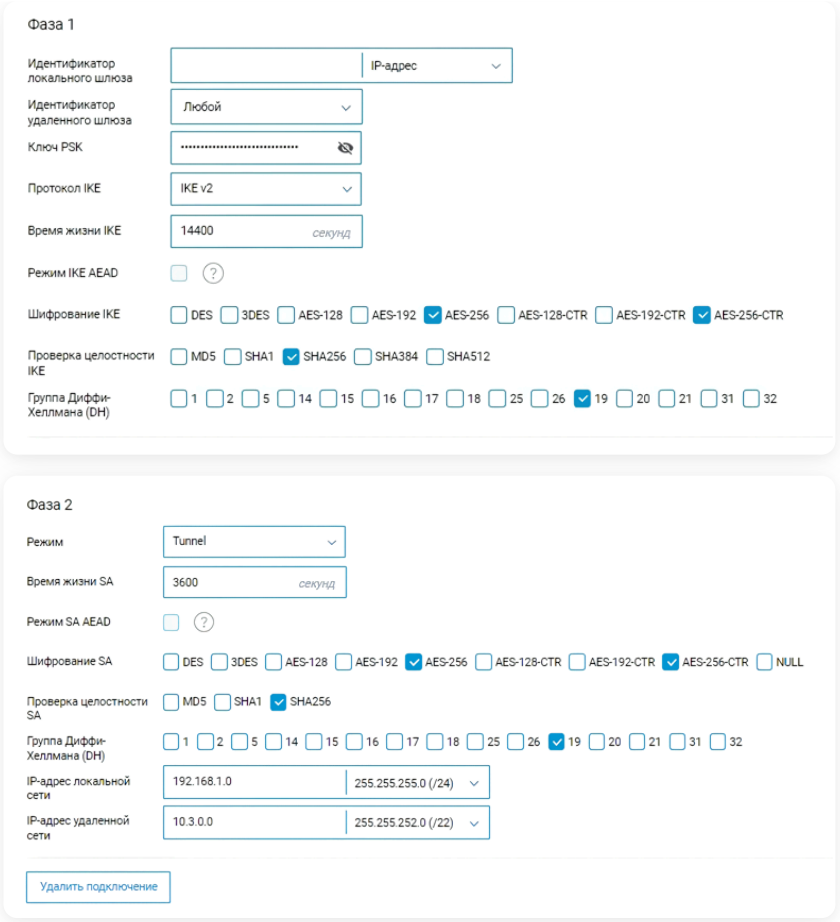
Разрешите доступ до внешних сетей во всех профилях, выполнив команду в PowerShell (запущенного с правами администратора):
`Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`

Подключение по IPsec

На стороне Ideco NGFW Novum настройте подключения в **Сервисы** → **IPsec** → **Исходящие подключения** или в **Сервисы** → **IPsec** → **Входящие подключения**.

На стороне устройства Keenetic при создании подключения в **Интернет** → **Другие подключения** используйте следующие настройки протоколов шифрования:





В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **Подключение по SSTP Wi-Fi-роутеров Keenetic**
- **IPsec**

Аутентификация

Настройка сертификатов и аутентификации пользователей в Ideco NGFW

Настройка корневого и подчиненного центра сертификации с помощью AD CS

Перейти >

Использование собственного CA-сертификата в Контент-фильтре

Перейти >

Как установить сертификат Ideco NGFW на Android

Перейти >

Настройка прозрачной авторизации на Astra Linux

Перейти >

Настройка автоматической веб-аутентификации на Ideco NGFW на Linux

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка корневого и подчиненного центра сертификации с помощью AD CS

Как подготовить и настроить корневой центр сертификации (Root CA), а затем на его основе создать подчиненный центр сертификации (Subordinate CA) через Active Directory Certificate Services (AD CS) для работы с NGFW Novum.

Предварительные требования:

- Необходимо развернуть две виртуальные машины в одной сети с правами администратора:
  - Корневой центр сертификации (Root CA) - Windows Server 2022 без роли контроллера домена (рекомендуется).
  - Подчиненный центр сертификации (Subordinate CA) - Windows Server 2022 с ролью контроллера домена (DC).

Настройка корневого центра сертификации (Root CA)

Шаг 1. Подготовка конфигурационного файла

На сервере, претендующем на роль корневого центра сертификации, необходимо создать INF-файл с именем `CAPolicy.inf` по пути `C:\Windows\CAPolicy.inf`. В файле укажите:

```
[Version]
Signature="$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
CRLPeriod=Years
CRLPeriodUnits=1
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=30
CRLOverlapPeriod=Weeks
CRLOverlapUnits=1
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=0

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=True
```

Расшифровка полей

Version

- `Signature="$Windows NT$"` - файл предназначен для операционной системы Windows NT и совместимых версий. Этот маркер обязателен для правильного распознавания системы.

Certsrv Server

- `RenewalKeyLength=2048` - длина нового ключа шифрования для сертификата самого Центра сертификации (CA) при его обновлении;
- `RenewalValidityPeriod=Years` - единица измерения срока действия для нового сертификата CA;
- `RenewalValidityPeriodUnits=20` - значение срока действия нового сертификата CA;
- `CRLPeriod=Years` - единица измерения интервала публикации основного списка отозванных сертификатов (CRL);
- `CRLPeriodUnits=1` - значение интервала публикации основного CRL;
- `CRLDeltaPeriod=Days` - единица измерения интервала публикации дельта-CRL (разностного списка отзыва);
- `CRLDeltaPeriodUnits=30` - значение интервала публикации дельта-CRL;
- `CRLOverlapPeriod=Weeks` - единица измерения интервала перекрытия (времени жизни) старого CRL;
- `CRLOverlapUnits=1` - значение интервала перекрытия CRL;
- `LoadDefaultTemplates=0` - значение определяет, будут ли шаблоны сертификатов загружаться по умолчанию при установке корпоративного центра сертификации:

- Если значение `0`, шаблоны не загружаются;
- Если значение `1`, шаблоны загружаются.

- `AlternateSignatureAlgorithm=0` - значение управляет алгоритмом подписи сертификатов от центра сертификации:
  - Если значение `0`, будет использоваться стандартный алгоритм (обычно SHA256RSA, где сначала создается хэш SHA256, а затем применяется подпись RSA);
  - Если значение `1`, будет применяться альтернативный алгоритм для совместимости с устаревшими системами, например, SHA1RSA. Рекомендуется выбрать значение `0`, так как оно более безопасное.

CRLDistributionPoint

- `Empty=True` - исключает URL-адреса точек распространения CRL из сертификатов, выпущенных центром сертификации.

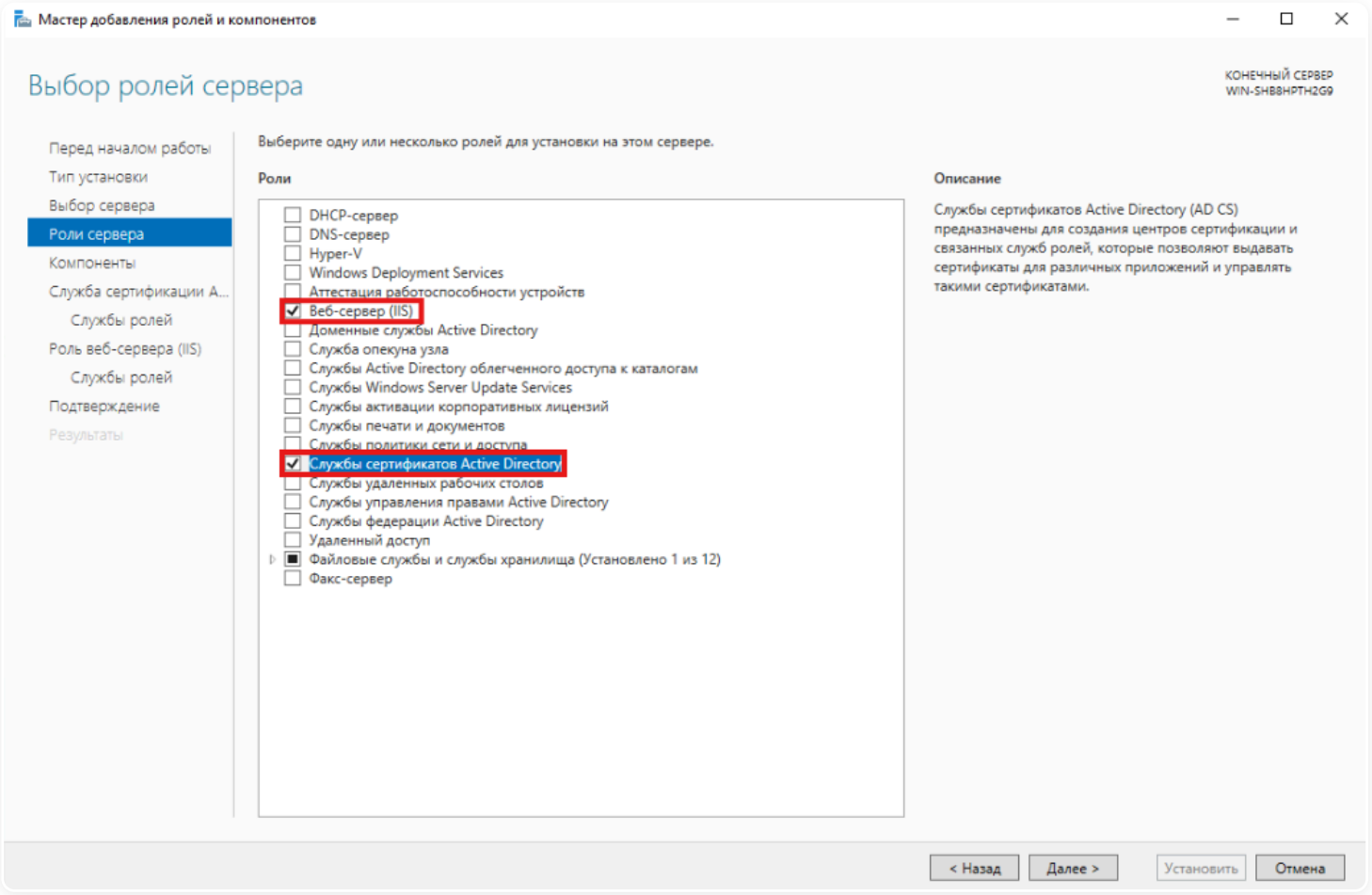
AuthorityInformationAccess

- `Empty=True` - не добавляет URL-адрес AIA в сертификаты, выданные центром сертификации.

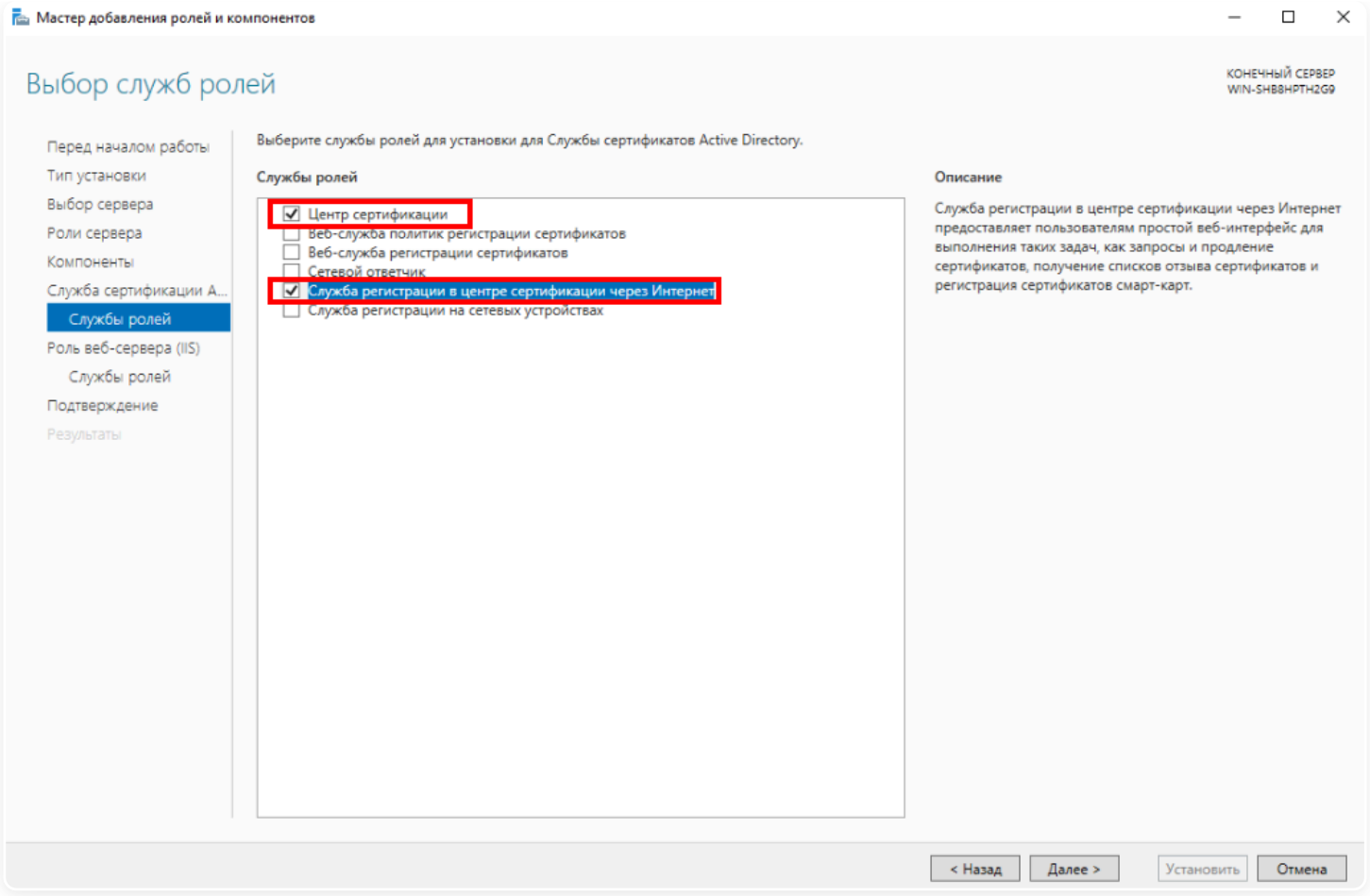
Шаг 2. Установка ролей служб сертификации

1. Откройте **Диспетчер серверов** и перейдите в **Управление** → **Добавление ролей и компонентов**.

2. На этапе **Роли сервера** выберите роль **Службы сертификатов Active Directory** и **Веб-сервер (IIS)**:



3. В окне **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:

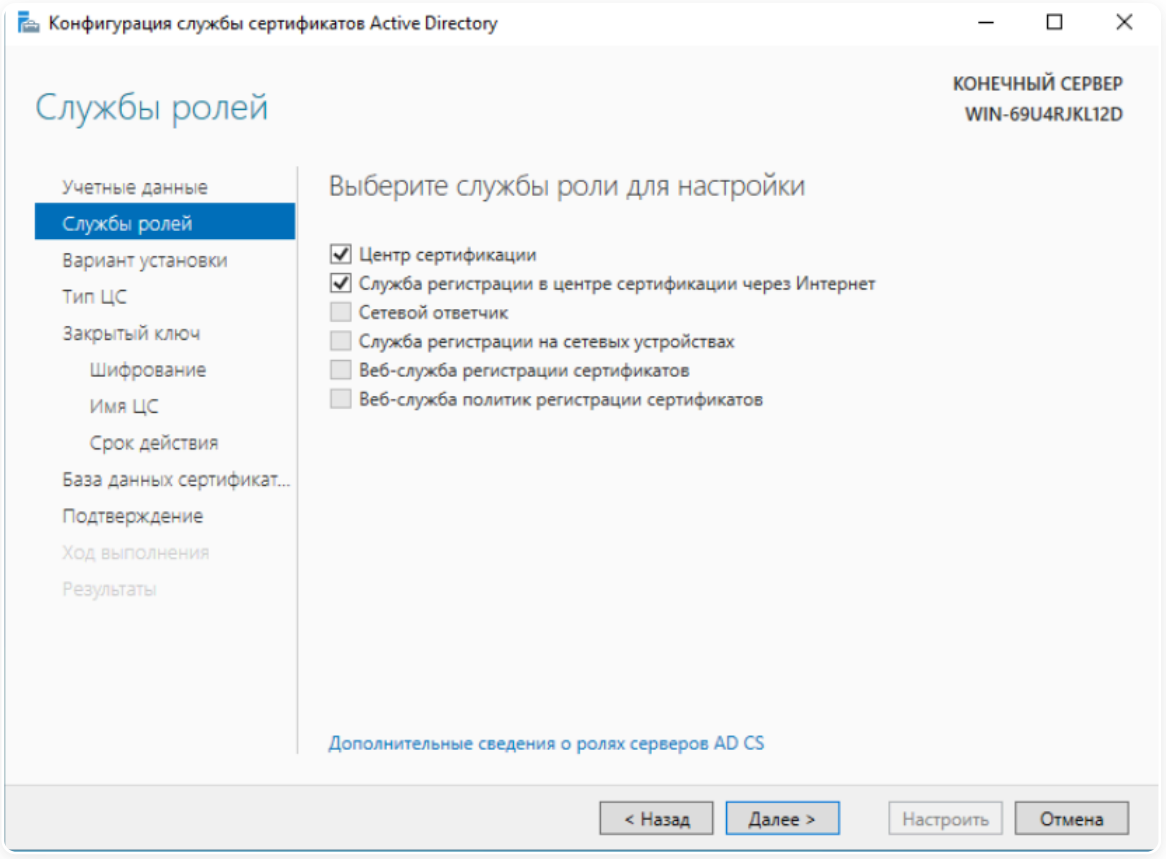


4. Завершите установку.

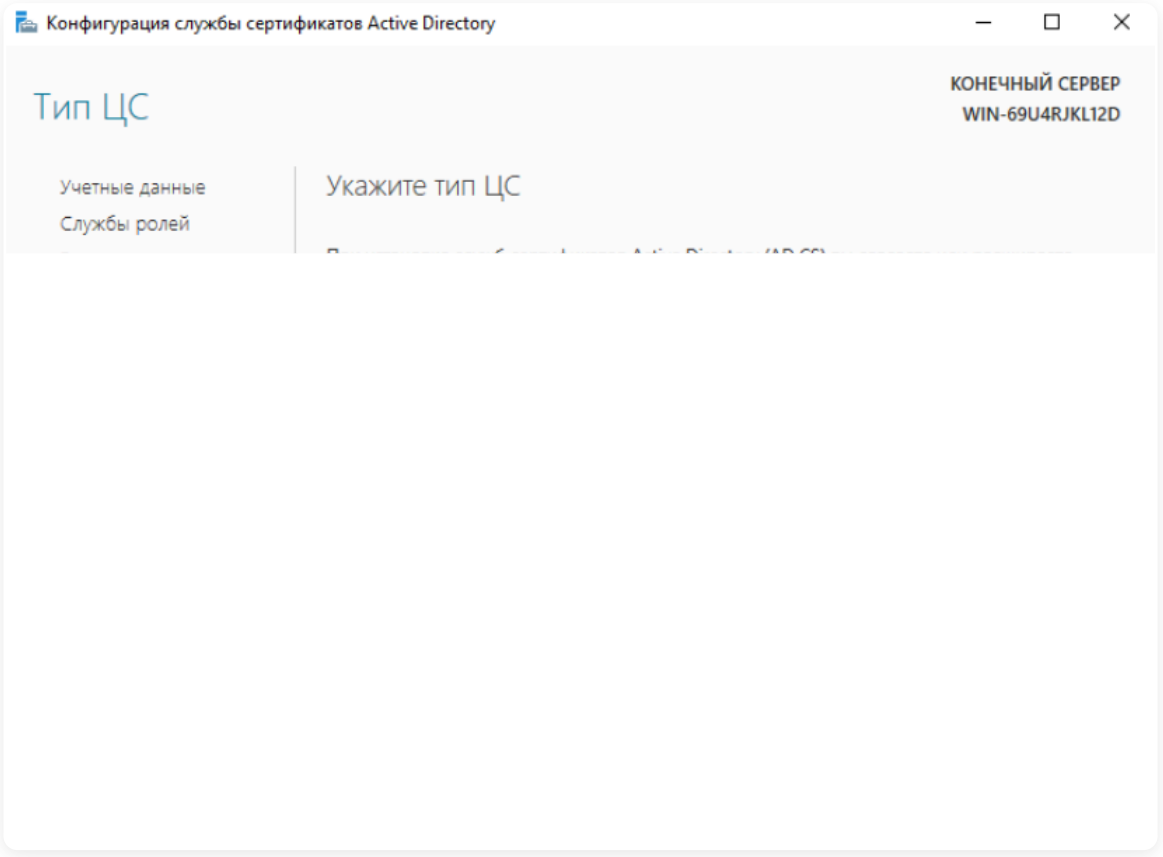
Шаг 3. Настройка служб сертификации

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

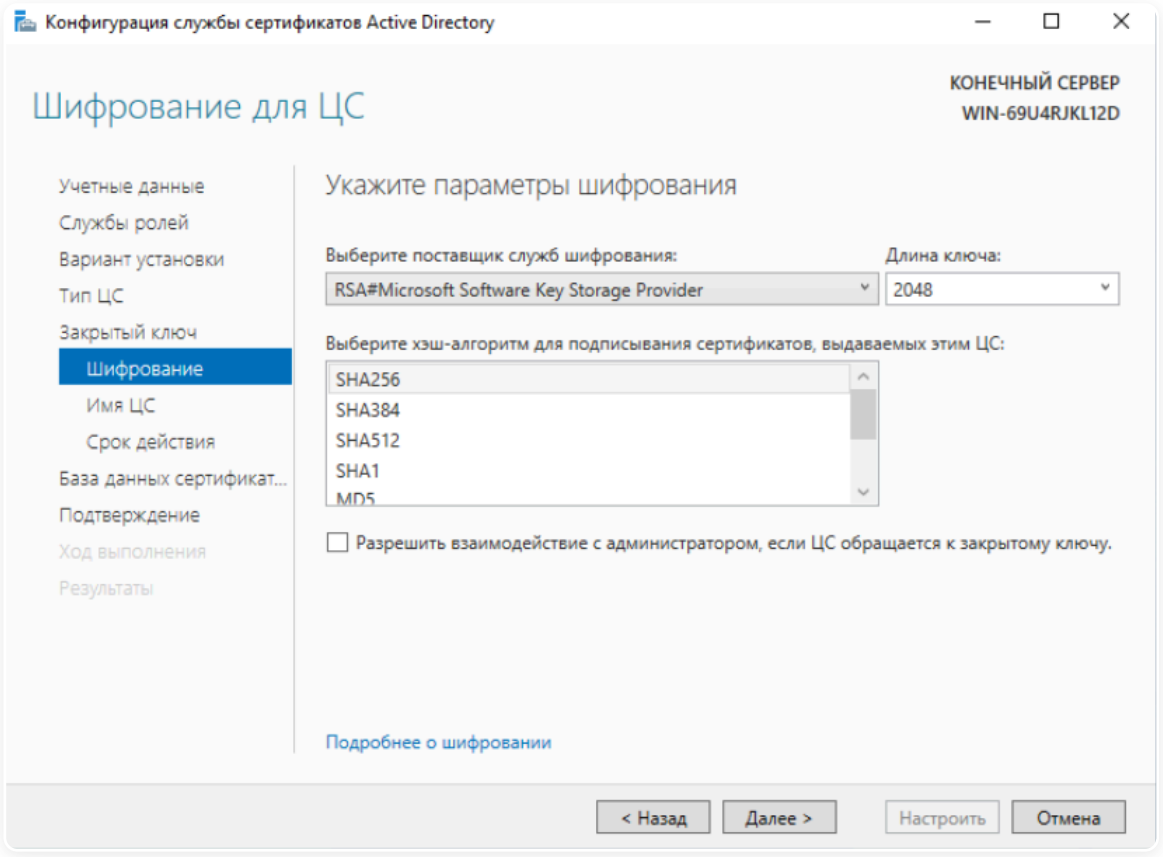
2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



3. На этапе **Тип ЦС** выберите **Корневой ЦС**:



4. На этапе **Шифрование** убедитесь, что выбран алгоритм **SHA256**:



5. На этапе **Имя ЦС** задайте имя (например, `TestRootCA`):

6. Завершите настройку:

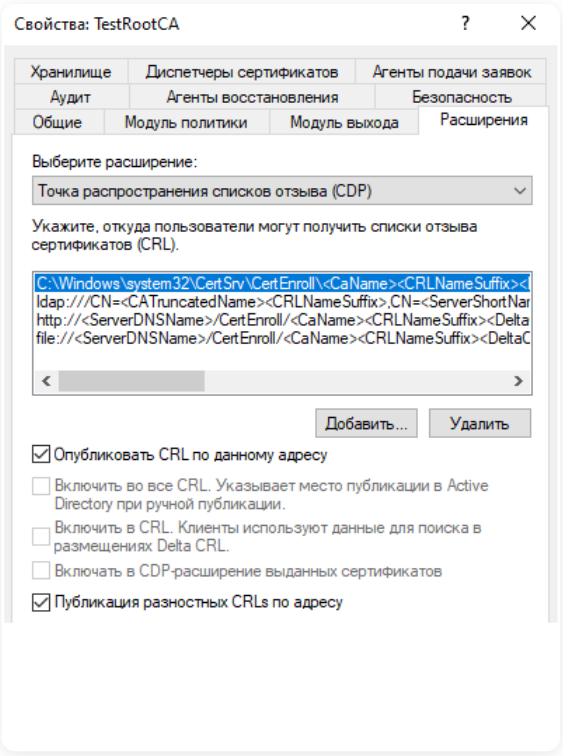
Шаг 4. Настройка точек распространения (CDP/AIA)

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**.

2. Нажмите правой кнопкой мыши по имени созданного центра сертификации `TestRootCA` и перейдите в **Свойства**.

3. На вкладке **Расширения** выберите расширение **Точка распространения списков отзыва (CDP)**.

4. Удалите пути, начинающиеся с `ldap://`, `file://` и `http://`:



5. Нажмите **Добавить** и введите URL `http://<домен-сервера>/Certs/`. Затем добавьте переменные `<CaName>`, `<CRLNameSuffix>` и `<DeltaCRLAllowed>` после `Certs/`. Конечный путь будет выглядеть так: `http://test.com/Certs/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.

6. Выберите добавленный URL и активируйте опции **Включить в CRL** и **Включать в CDP-расширение выданных сертификатов**:

7. На вкладке **Расширения** выберите расширение **Доступ к сведениям о центрах сертификации (AIA)**.

8. Удалите пути, начинающиеся с `ldap://`, `file://` и `http://`:

9. Нажмите **Добавить** и введите URL `http://<домен-сервера>/CertsAIA/`. Затем добавьте переменные `<ServerDNSName>`, `<CaName>` и `<CertificateName>` после `Certs/`. Конечный путь будет выглядеть так: `http://test.com/CertsAIA/<ServerDNSName>_<CaName><CertificateName>.crt`.

10. Выберите добавленный URL и активируйте опции **Включать в AIA-расширение выданных сертификатов**.

11. Примените изменения и перезапустите службу.

Шаг 5. Экспорт корневого сертификата

1. Откройте консоль управления. Для этого нажмите **Win + R**, введите команду `mmc` и нажмите **Enter**.

2. Перейдите в **Файл** → **Добавить или удалить оснастку**.

3. Выберите **Сертификаты** и нажмите **Добавить**.

4. Выберите опцию **учетной записи компьютера** и нажмите **Далее** → **Готово** → **ОК**.

5. Перейдите в **Сертификаты (локальный компьютер)** → **Личное** → **Сертификаты**. Нажмите правой кнопкой мыши по корневому сертификату `TestRootCA` и выберите **Все задачи** → **Экспорт**.

6. Выберите **Нет, не экспортировать закрытый ключ** и нажмите **Далее**.

7. Выберите формат **Файлы X.509 (.CER) в кодировке DER** и нажмите **Далее**.

8. Сохраните файл (например, `Root_CA.cer`) и перенесите этот файл на сервер подчиненного центра сертификации.

Настройка подчиненного центра сертификации (Subordinate CA)

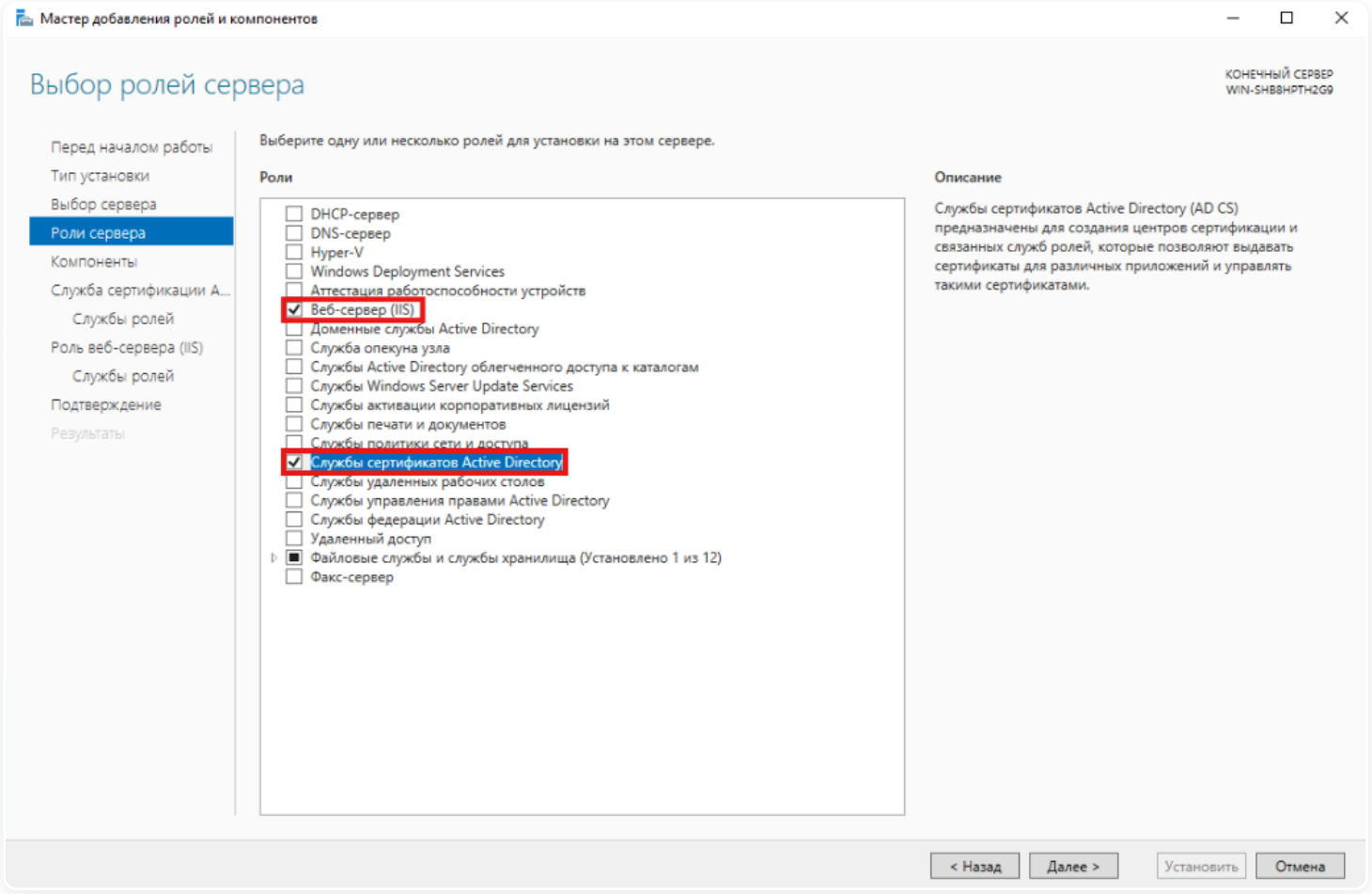
Шаг 1. Установка доверия к корню и установка ролей

На подчиненном центре сертификации (контроллере домена):

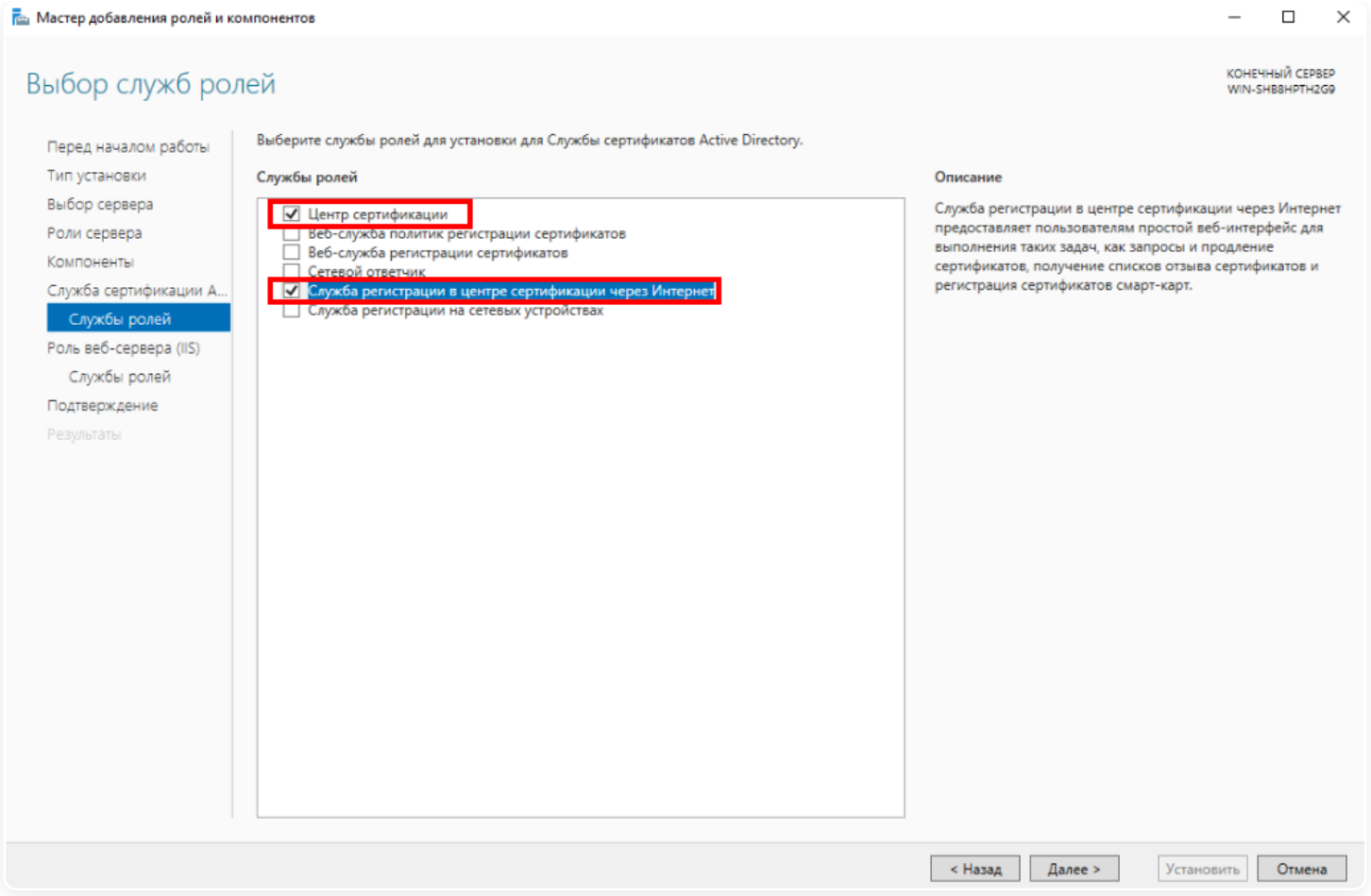
1. Установите сертификат `Root_CA.cer` в хранилище **Доверенные корневые центры сертификации** для локального компьютера.

2. Откройте **Диспетчер серверов** и перейдите в **Управление → Добавление ролей и компонентов**.

3. На этапе **Роли сервера** выберите роль **Службы сертификатов Active Directory** и **Веб-сервер (IIS)**:



4. В окне **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



5. Завершите установку.

Шаг 2. Настройка подчиненного центра сертификации и создание запроса (CSR)

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:

3. На этапе **Тип ЦС** выберите **Подчиненный ЦС**:

4. На этапе **Имя ЦС** задайте имя (например, `SubCAcert`):

5. На этапе **Запрос сертификата** сохраните запрос в файл `.req`. Скопируйте путь к файлу:

6. Завершите настройку. По завершении настройки система выдаст информационное предупреждение, которое является стандартным.

Шаг 3. Завершение настройки подчиненного центра сертификации

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. На подчиненном центре сертификации нажмите правой кнопкой мыши **Установить сертификат ЦС** и выберите скачанный файл. Установите файл в папку **Доверенные корневые центры сертификации**.

2. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на центр сертификации и выберите **Все задачи** → **Запуск службы**.

Шаг 4. Настройка IIS для публикации CRL и сертификатов

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Диспетчер служб IIS**.

2. Нажмите правой кнопкой мыши по узлу сервера, выберите **Добавить веб-сайт** и заполните поля:

- **Имя сайта** - введите `CertAU`.

- **Физический путь** - создайте новую папку `CA_site` по пути `C:\CA_site`.
- **Имя узла** - укажите доменное имя, по которому будет доступен сайт, например, `marketing.contoso.com`.

3. После добавления веб-сайта перейдите в раздел **Просмотр каталогов** и нажмите **Включить**:

4. Нажмите правой кнопкой мыши по созданному в пункте 3 веб-сайту, выберите **Добавить виртуальный каталог** и заполните поля:

- **Псевдоним** - укажите `Certs`.
- **Физический путь** - создайте новую папку `CDP` по пути `C:\CA_site\CDP`.

5. Повторите пункт 4. Создайте новый виртуальный каталог с псевдонимом `certsAIA` и укажите путь `C:\CA_site\AIA`.

6. Для каждого созданного каталога перейдите в раздел **Просмотр каталогов** и нажмите **Включить**.

7. Скопируйте файлы `.crl` и `.crt` с корневого центра сертификации в соответствующие папки на подчиненном.

8. Для сайта `CertAU` откройте раздел **Фильтрация запросов**. Выберите действие **Изменить параметры** и включите опцию **Разрешить двойное преобразование**.

Шаг 5. Настройка CDP и AIA на подчиненном центре сертификации

1. Откройте **Диспетчер серверов** и перейдите в **Средства → Центр сертификации**.

2. Нажмите правой кнопкой мыши по центру сертификации и перейдите в **Свойства**.

3. На вкладке **Расширения** удалите пути, начинающиеся с `ldap://`, `file://` и `http://`.

4. Добавьте новые пути:

- Для CDP конечный путь будет выглядеть так: `http://<домен-сервера>/Certs/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.
- Для AIA конечный путь будет выглядеть так: `http://<домен-сервера>/CertsAIA/<ServerDNSName>_<CaName><CertificateName>.crt`.

5. Выберите добавленный URL и активируйте опции:

- Для CDP: **Включить в CRL** и **Включать в CDP-расширение выданных сертификатов**.
- Для AIA: **Включать в AIA-расширение выданных сертификатов**.

Шаг 6. Получение сертификата от корневого центра сертификации

1. Откройте файл `.req` в блокноте и скопируйте текст.

2. Откройте в браузере `http://<IP-адрес-корневого-центра-сертификации>/certsrv`.

3. Перейдите в **Запросить сертификат → Расширенный запрос сертификата**:

4. Вставьте текст запроса в поле и нажмите **Выдать**:

5. В корневом центре сертификации откройте **Диспетчер серверов** и перейдите в **Средства → Центр сертификации**.

6. Перейдите в папку **Запросы в ожидании**, найдите запрос, нажмите правой кнопкой мыши **Все задачи → Выдать**.

7. С подчиненного центра сертификации вернитесь на страницу браузера `http://<IP-адрес-корневого-центра-сертификации>/certsrv`, выберите **Просмотр состояния ожидаемого запроса сертификата** и скачайте выданный сертификат.

Шаг 7. Настройка путей для публикации подчиненного центра сертификации (CRLDelta)

1. Откройте **Диспетчер серверов** и перейдите в **Средства → Диспетчер служб IIS**.

2. Создайте виртуальный каталог `subCA/CDP`. Для этого нажмите правой кнопкой мыши по веб-сайту `CertAU`, выберите **Добавить виртуальный каталог** и заполните поля:

- **Псевдоним** - укажите `subCA/CDP`.
- **Физический путь** - создайте новую папку `CDP` по пути `C:\CA_site\subCA\CDP`.

3. Повторите шаги из пункта 2 для создания виртуального каталога `subCA/AIA`:

- **Псевдоним** - укажите `subCA/AIA`.
- **Физический путь** - создайте новую папку `CDP` по пути `C:\CA_site\subCA\AIA`.

4. Откройте **Свойства** центра сертификации и на вкладке **Расширения** добавьте физические пути для публикации:

- Для CDP конечный путь будет выглядеть так: `C:\CA_site\subCA\CDP\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.
- Для AIA конечный путь будет выглядеть так: `C:\CA_site\subCA\AIA\<ServerDNSName>_<CaName><CertificateName>.crt`.

5. Выберите добавленный путь для CDP и активируйте опции **Опубликовать CRL по данному адресу** и **Публикация разностных CRL по адресу**.

6. Скопируйте сертификат подчиненного центра сертификации из папки `C:\Windows\System32\certsrv\CertEnroll` в папку `C:\CA_site\subCA\AIA`.

7. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на центр сертификации и выберите **Все задачи** → **Публикация**, чтобы обновить CRL.

Создание шаблона сертификата и тестовая выдача

Шаг 1. Создание шаблона сертификата

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на папку **Шаблоны сертификатов** и выберите **Управление**.

2. Найдите шаблон **Пользователь**, нажмите правой кнопкой мыши и выберите **Скопировать шаблон**.

3. Настройте шаблон в соответствии с вашими требованиями (имя, срок действия, криптопровайдеры и так далее):

4. На вкладке **Безопасность** добавьте группу **Компьютеры домена** и/или **Пользователи домена** с разрешениями **Чтение** и **Заявка**:

5. Вернитесь в раздел **Центр сертификации** → **Шаблоны сертификатов**. Нажмите правой кнопкой мыши в пустой области **Создать** → **Выдаваемый шаблон сертификата** и выберите созданный шаблон.

Шаг 2. Тестовая выдача сертификата на клиентском устройстве

1. На клиентском устройстве установите корневой сертификат `Root_CA.cer` и сертификаты от подчиненного центра в хранилище **Доверенные корневые центры сертификации**.

2. Откройте консоль управления. Для этого нажмите **Win + R**, введите команду `mmc` и нажмите **Enter**.

3. Перейдите в **Файл** → **Добавить или удалить оснастку**.

4. Выберите **Сертификаты** и нажмите **Добавить**.

5. Выберите опцию **моей учетной записи компьютера** и нажмите **Готово** → **ОК**.

6. Перейдите в **Сертификаты - текущий пользователь**. Нажмите правой кнопкой мыши по папке **Личное** и выберите **Все задачи** → **Запросить новый сертификат**.

7. Выберите созданный шаблон и нажмите **Заявка**.

8. Убедитесь, что сертификат появился в личном хранилище:

Полезные ссылки

- **Active Directory/Samba DC**
- **Сертификаты**

Использование собственного CA-сертификата в Контент-фильтре

В **Контент-фильтре** возможно использование не корневого сертификата Ideco NGFW Novum, а собственного CA-сертификата. Процедура настройки такого сертификата включает этапы:

1. Генерация приватного ключа и CA-сертификата.

2. Подготовка CA-сертификата для загрузки на сервер NGFW Novum.

3. Загрузка CA-сертификата на сервер NGFW Novum.

4. Установка CA-сертификата на устройство пользователя.

Шаг 1. Генерация приватного ключа и CA-сертификата

1. Сгенерируйте приватный ключ корневого сертификата без применения **passphrase**, фразы-пароля:

```
openssl genrsa -aes256 -out ideco-cf_root-ca.key 4096
```

- `-aes256` - приватный ключ зашифрован алгоритмом AES-256;
- `ideco-cf_root-ca.key` - название файла, содержащего приватный ключ.

2. Сгенерируйте корневой сертификат, используя приватный ключ корневого сертификата:

```
openssl req -x509 -new -sha256 -days 1825 -key ideco-cf_root-ca.key -out ideco-cf_root-ca.pem
```

- `-sha256` - использование алгоритма SHA256 при создании сертификата;
- `-days 1825` - срок действия сертификата в днях;
- `ideco-cf_root-ca.key` - название файла, содержащего приватный ключ сертификата;
- `ideco-cf_root-ca.pem` - название файла, содержащего сам сертификат.

3. Заполните параметры сертификата:

```
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Moscow
Locality Name (eg, city) [Default City]:Moscow
Organization Name (eg, company) [Default Company Ltd]:Test
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:MyName
Email Address []:test@ideco.ru
```

Расшифровка строк

- `Country Name (2 letter code) [XX]` - код страны в формате ISO 3166-1 alpha-2 (например, `RU`).
- `State or Province Name (full name) [Some-State]` - название региона или области (например, `Moscow`).
- `Locality Name (eg, city) [Default City]` - название города (например, `Saint Petersburg`).
- `Organization Name (eg, company) [Internet Widgits Pty Ltd]` - название организации.
- `Organizational Unit Name (eg, section) []` - название подразделения организации.
- `Common Name (e.g. server FQDN or YOUR name) []` - наименование сертификата, например `Ideco`.
- `Email Address []` - контактный email.

Дополнительные атрибуты:

- **A challenge password []** - пароль для дополнительной аутентификации. Поле должно быть пустым.
- **An optional company name []:** - полное юридическое название организации.

4. Проверьте, что сертификат был успешно создан:

```
openssl x509 -text -noout -in ideco-cf_root-ca.pem
```

Требования к CA-сертификату:

- Должен иметь атрибут `CA:TRUE`.
- Для RSA длина ключа должна быть не менее 1024 бит. Рекомендуем использовать длину ключа не менее 2048 бит.

После генерации вы должны получить ключ и сертификат в файлах:

- `ideco-cf_root-ca.key` - файл, содержащий приватный ключ сертификата;
- `ideco-cf_root-ca.pem` - файл, содержащий CA-сертификат.

Шаг 2. Подготовка сертификата для загрузки на сервер

Для корректной загрузки на сервер Ideco NGFW Novum CA-сертификат нужно собрать в один файл, называемый бандлом, в правильном порядке. Структура файла должна содержать два блока - **Приватный ключ** и **CA-сертификат**.

Для создания бандла выполните действия:

1. Создайте текстовый файл вида:

```
-----BEGIN PRIVATE KEY-----
.....
.....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
```

2. Добавьте в блок `BEGIN PRIVATE KEY` приватный ключ.

3. В блок `BEGIN CERTIFICATE` добавьте сгенерированный CA-сертификат. Файл бандла должен получить такую структуру:

```
-----BEGIN PRIVATE KEY-----
Приватный ключ
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
CA-сертификат
-----END CERTIFICATE-----
```

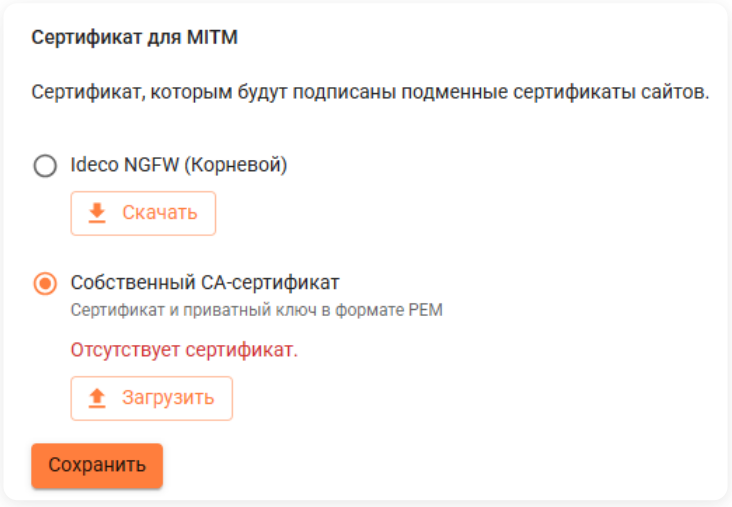
4. Сохраните файл бандла с именем, отличным от PEM-файла CA-сертификата, и расширением **.pem**, например, `ideco-cf_root-ca-key.pem`.

Шаг 3. Загрузка сертификата на сервер

Загрузите файл бандла на Ideco NGFW Novum. Для этого:

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Настройки**.

2. В поле **Сертификат для MITM** выберите опцию **Собственный CA-сертификат**:



3. Нажмите **Загрузить** и выберите созданный файл бандла `ideco-cf_root-ca-key.pem`.

Шаг 4. Установка CA-сертификата на устройство пользователя

На устройства пользователей необходимо установить только CA-сертификат, без приватного ключа.

Установите на устройства пользователей файл CA-сертификата (без приватного ключа), в нашем примере `ideco-cf_root-ca.pem`. Варианты установки:

Установка CA-сертификата вручную

Установка сертификата на Linux

Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

Установка сертификата на Windows

1. Откройте на рабочей станции центр управления сертификатами: **Пуск** → **Выполнить**, введите **mmc** и нажмите **Enter**:

2. В меню **Файл** выберите **Добавить или удалить оснастку**:

3. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите **Добавить**:

4. В открывшемся окне выберите пункт **Учетной записи компьютера** и нажмите **Далее**:

5. В окне **Выбор компьютера** оставьте флаг **Локальный компьютер** и нажмите **Готово**.

6. В левой части окна нажмите на стрелку рядом с директорией **Сертификаты (локальный компьютер)** → **Доверенные корневые сертификаты** → **Сертификаты**:

7. В меню **Действие** выберите **Все задачи** → **Импорт**:

8. Следуя инструкциям **Мастера импорта сертификатов**, импортируйте CA-сертификат. Импортированный сертификат появится в списке в правой части окна:

Автоматическая установка CA-сертификата через Active Directory

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, можно установить сертификат Ideco NGFW Novum для всех пользователей автоматически:

1. Зайдите на контроллер домена с правами администратора.

2. Запустите оснастку **Управление групповой политикой**, выполнив команду **gpmc.msc**.

3. Найдите **политику домена**, использующуюся на компьютерах пользователей в **Объектах групповой политики** (Default Domain Policy). Нажмите на нее правой кнопкой мыши и выберите **Изменить**:

4. В открывшемся редакторе управления групповыми политиками выберите: **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Политики открытого ключа** → **Доверенные корневые центры сертификации**.

5. Нажмите правой кнопкой мыши по открывшемуся списку, выберите **Импорт** и импортируйте ключ Ideco NGFW Novum:

6. После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Полезные ссылки

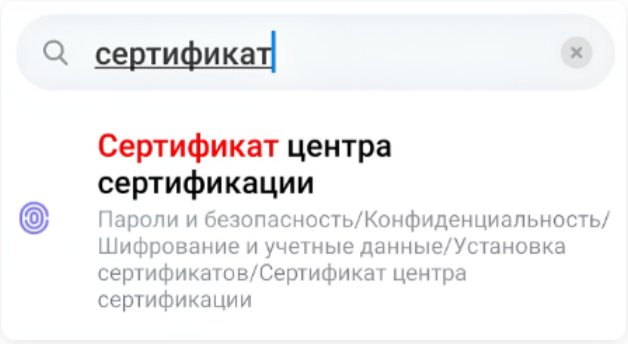
- **Настройка фильтрации HTTPS**
- **Сертификаты**

Как установить сертификат Ideco NGFW Novum на Android

1. Скачайте сертификат Ideco NGFW Novum на Android-устройство.

2. Перейдите в **Настройки**.

3. В поиске введите `Сертификат`:

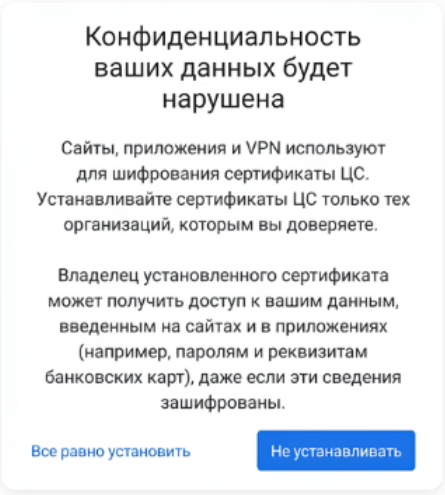


4. Выберите **Сертификат центра сертификации**.

> В зависимости от версии Android и версии оболочки путь может отличаться. Ориентируйтесь на расположение **Пароли и безопасность/ Конфиденциальность/Шифрование и учетные данные**.

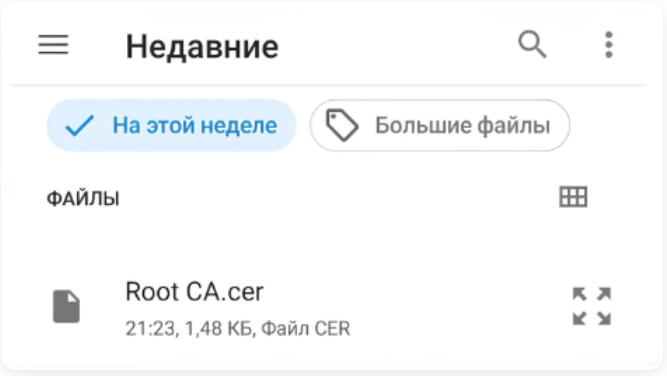
5. Если появится окно **Укажите название сертификата**, введите удобное вам название.

6. Выберите **Сертификат центра сертификации** и нажмите **ОК**. Если откроется предупреждение, нажмите **Все равно установить** или **Установить в любом случае**:



7. Введите пароль или PIN-код от устройства. Нажмите **Подтвердить**.

8. В загрузках выберите скачанный сертификат `Root CA.cer`:



После установки в нижней части экрана появится уведомление **Сертификат установлен**.

Полезные ссылки

- **Сертификаты**

Настройка прозрачной авторизации на Astra Linux

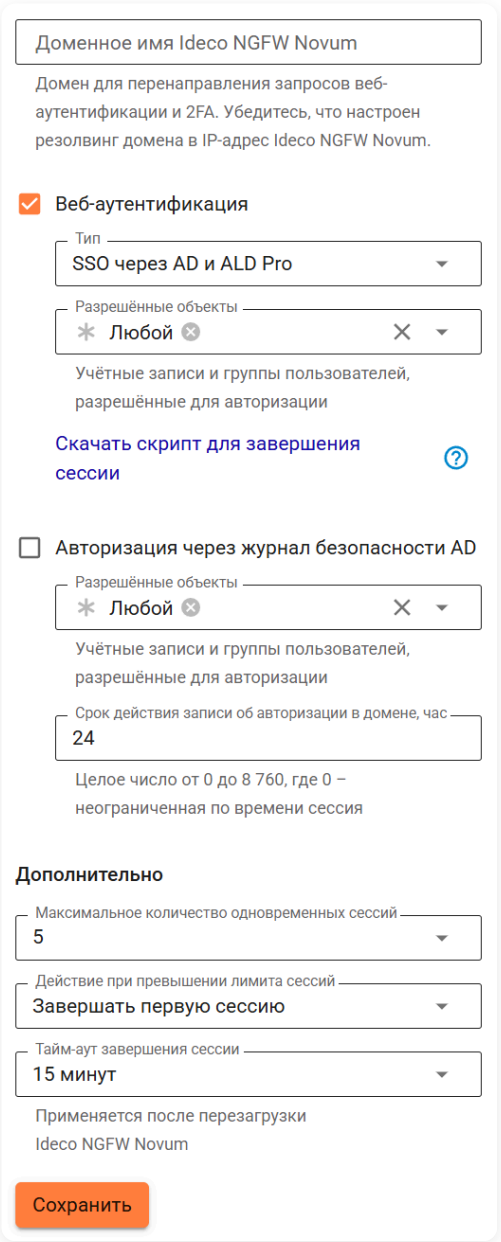
Решение подходит для браузеров **Yandex**, **Chromium** и **Firefox.**

1. Установите и настройте NGFW на устройстве администратора, получите лицензию.

2. Введите Astra Linux в домен (например, через Active Directory).

3. Введите NGFW в домен, что и Astra Linux, и импортируйте пользователей (в том числе Astra Linux) в группу.

4. Выберите **SSO через AD и ALD Pro** на вкладке **Пользователи** → **Авторизация** → **Настройки** в Ideco NGFW Novum:



5. Зайдите под доменной учетной записью на Astra Linux.

6. В зависимости от выбранного браузера, выполните действия:

Для браузера Yandex

1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и впишите в него строку:

```
{
  "AuthServerAllowlist": "имя_NGFW.имя_домена",
  "AuthNegotiateDelegateAllowlist": "имя_NGFW.имя_домена"
}
```

2. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.

Для браузера Chromium

1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и впишите в него строку:

```
{
    "AuthServerAllowlist": "имя_NGFW.имя_домена" ,
    "AuthNegotiateDelegateAllowlist": "имя_NGFW.имя_домена"
}
```

2. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.

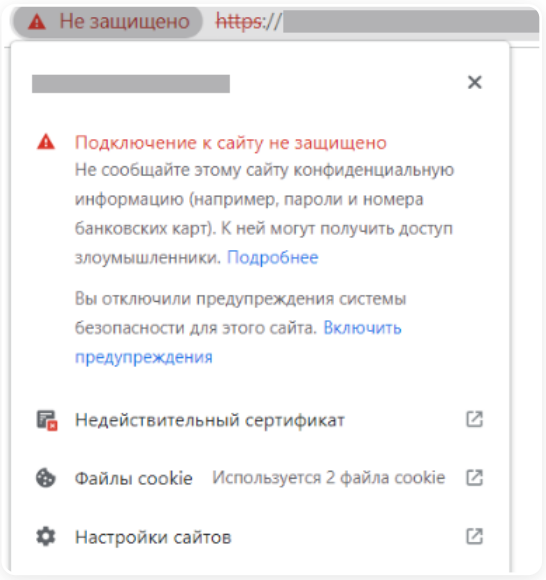
Для браузера Firefox

1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

2. Введите параметр `security.enterprise_roots.enabled` и дважды кликните по блоку, чтобы значение изменилось на **True**, что позволит Firefox доверять системным сертификатам и авторизовывать пользователей при переходе на HTTPS-сайты.

3. В параметрах `network.automatic-ntlm-auth.trusted-uris` и `network.negotiate-auth.trusted-uris` укажите `имя_NGFW.имя_домена`.

4. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.
7. При возникновении проблемы с доверенным сертификатом установите корневой сертификат NGFW. Пример проблемы:

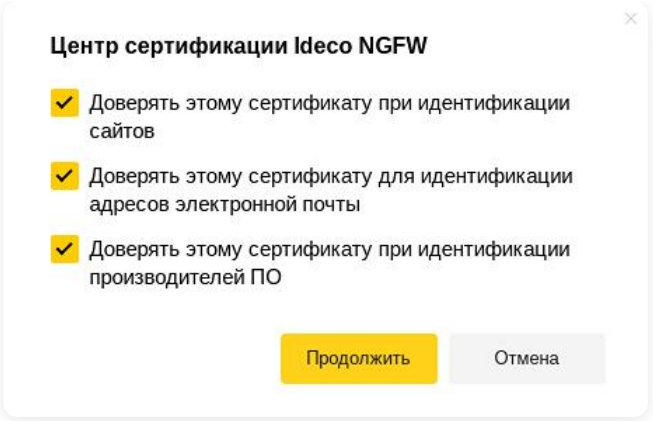


Для браузера Yandex

1. Скачайте корневой сертификат.

2. В браузере Yandex перейдите в **Настройки** → **Системные** → **Управление сертификатами** → **Центры сертификации** → **Импорт** и добавьте сертификат в список доверенных.

3. Включите опции доверия для сертификата:

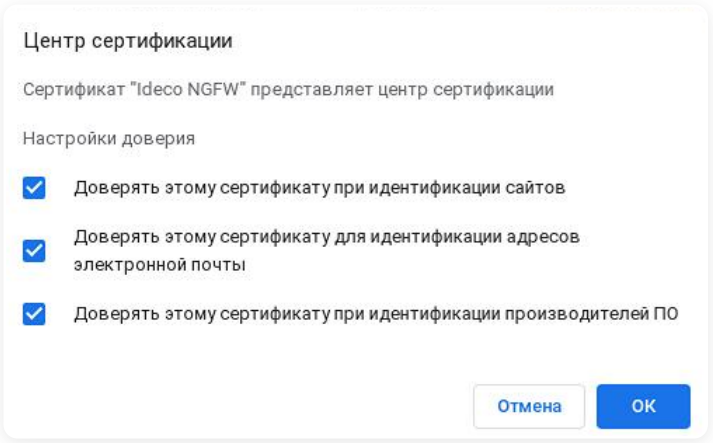


Для браузера Chromium

1. Скачайте корневой сертификат.

2. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

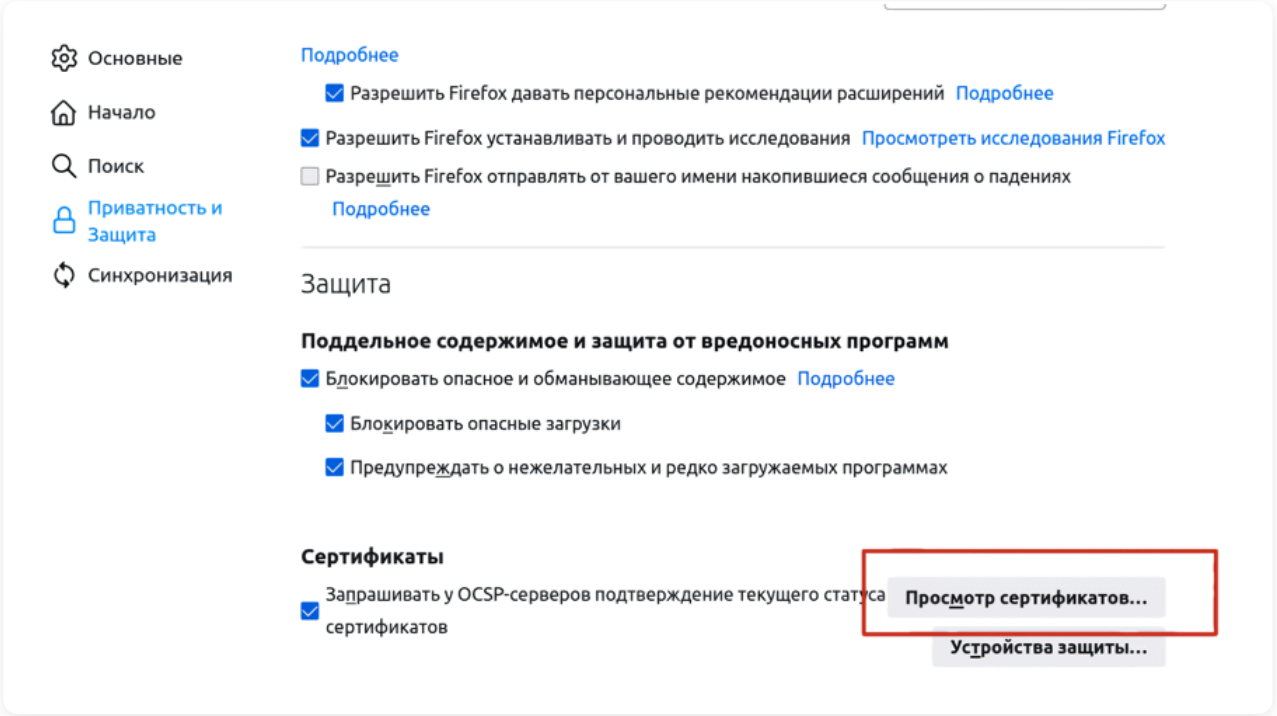
3. Включите опции доверия для сертификата:



Для браузера Firefox

1. Скачайте корневой сертификат.

2. В настройках браузера Mozilla Firefox в пункте **Приватность и Защита** в разделе **Защита** выберите **Просмотр сертификатов**:



3. На вкладке **Центры сертификации** нажмите **Импортировать** и выберите скачанный с NGFW сертификат.

4. Отметьте пункт **Доверять при идентификации веб-сайтов** и подтвердите.

Полезные ссылки

- **Авторизация**
- **Веб-аутентификация**

Настройка автоматической веб-аутентификации на Ideco NGFW Novum на Linux

Для настройки автоматической аутентификации выполните действия:

1. Перейдите в домашнюю директорию пользователя (Home) и включите отображение скрытых файлов.

2. Перейдите в папку `.config` и создайте там каталог `ideco-utm`.

3. Скачайте корневой сертификат NGFW. Подробнее в статье и поместите сертификат в каталог, созданный на предыдущем шаге.

4. Создайте в папке `ideco-utm` файл `auth.conf`. Откройте его, введите логин и пароль пользователя по образцу:

```
login=логин_пользователя
password=пароль_пользователя
```

5. Скачайте скрипт на компьютер пользователя, перейдя по ссылке, и настройте автозагрузку в соответствии с описанным ниже алгоритмом. Чтобы сохранить файл, кликните правой кнопкой мыши в любом месте страницы и выберите пункт **Сохранить как**.

Для корректной работы скрипта имя корневого сертификата должно быть `root_ca.crt`.

Настройка автозагрузки скрипта

Для настройки выясните возможность добавления приложений в автозагрузку через графический интерфейс. При отсутствии такой возможности настройте автозагрузку через терминал.

Для настройки через терминал потребуются права администратора.

Настройка через терминал

Если сделать скрипт исполняемым файлом с помощью команды `chmod +x <путь до скрипта>`, можно не указывать путь до python.

1. Откройте терминал и введите команду:

```
sudo nano /etc/systemd/system/auto-authorization.service
```

2. Заполните файл следующим образом:

```
[Unit]
Description=Auto-Authorization

[Service]
Type=simple
User=имя_пользователя_в_системе
ExecStart=полный_путь_до_python полный_путь_до_скрипта --check-timeout=60

[Install]
WantedBy=multi-user.target
```

Введите имя пользователя Linux и полный путь до скрипта.

3. Сохраните файл и выйдите из редактора.

4. Добавьте службу в автозагрузку командой `systemctl enable auto-authorization`.

Скрипт поддерживает множество ключей, с помощью которых можно менять путь к файлам и другие параметры. Для вывода справки утилиты используйте ключ `-h`.

Для проверки статуса ранее настроенной службы введите `systemctl status auto-authorization.service`

Проверить работу настройки можно с помощью интерфейса Ideco NGFW Novum. Зайдите в раздел **Мониторинг** → **Сессии пользователей** и завершите сессию пользователя, для которого настраивалась автоматическая аутентификация. Чтобы удалить авторизованную сессию, нажмите на соответствующую пиктограмму и подтвердите выбор.

Если выйти из сессии на устройстве пользователя и повторно открыть браузер, то запрос на авторизацию не должен появиться.

Полезные ссылки

- **Веб-аутентификация**

Как безопасно подключить удаленного подрядчика

> Статья описывает полный цикл настройки Ideco NGFW Novum для безопасного подключения внешнего подрядчика к внутренним ресурсам компании. Конфигурация строится по принципу минимально необходимого доступа и охватывает сетевую изоляцию, аутентификацию, проверку устройства и аудит сессий.

Пример. Финансовый отдел компании привлекает внешнего подрядчика для работы в системе 1С. Подрядчик должен подключаться удаленно к RDP-серверу финансового отдела, на котором развернута 1С, до завершения контракта. Задача администратора - предоставить строго ограниченный доступ и обеспечить контроль подключения на каждом уровне.

Требования к безопасности:

- Доступ только к RDP-серверу финансового отдела с системой 1С.
- Доступ исключительно по протоколу RDP (порт 3389). Весь остальной трафик запрещен через **Межсетевой экран** и модуль **Контроль приложений**.
- Аутентификация через Ideco Client: логин/пароль и обязательная двухфакторная аутентификация (MFA).
- Подключение разрешено только с территории России и только в рабочее время (с 09:00 до 18:00 по будням).
- Устройство подрядчика должно соответствовать требованиям: Windows 11, активный антивирус Касперского.
- Постоянный контроль защищенности точки подключения: проверка IPS на RDP-уязвимости.
- Подрядчик не должен иметь доступа к смежным сегментам сети (другие отделы, внутренняя инфраструктура) для исключения горизонтального перемещения в случае компрометации доступа.
- Полная запись всех сессий подрядчика для последующего аудита.
- Автоматическое отключение сессии по истечении рабочего времени или времени бездействия.
- Запрет split-tunneling: трафик подрядчика в интернет не должен проходить через корпоративные ресурсы.
- Доступ предоставляется на ограниченный срок с ручным отключением учетной записи по его истечении.

Модель угроз

Таблица описывает потенциальные угрозы при подключении удаленного подрядчика и механизмы защиты от каждой из них.

Вектор угрозы	Описание	Механизм защиты
Несанкционированный доступ к смежным сегментам сети	Подрядчик получает доступ к ресурсам за пределами RDP-сервера финансового отдела	Правила FORWARD в **Межсетевом экране**: разрешен только трафик к IP-адресу RDP-сервера по порту 3389. Запрещающее правило блокирует весь остальной трафик
Использование протоколов, отличных от RDP	Попытка передачи данных через HTTP, SSH, SMB и другие протоколы	Профиль **Контроля приложений** запрещает все протоколы, кроме RDP
Эксплуатация RDP-уязвимостей	Атака на RDP-сервер через известные уязвимости (BlueKeep, DejaBlue и другие)	Профиль **Предотвращения вторжений** с включенными группами сигнатур для RDP-уязвимостей и атак на получение привилегий
Компрометация учетных данных	Перехват или подбор логина и пароля	Двухфакторная аутентификация (TOTP-токен) при подключении через Ideco Client
Подключение с зараженного устройства	Устройство без антивируса или с устаревшими базами используется как точка входа в сеть	HIP-профиль в правиле доступа по VPN проверяет наличие Windows 11 и активного антивируса Касперского. Устройства, не прошедшие проверку, блокируются при подключении
Подключение из-за пределов России	Попытка подключения из нетипичной геолокации, указывающая на компрометацию учетной записи	GeoIP-фильтрация в правиле **Межсетевого экрана**: разрешены подключения только с территории России
Подключение в нерабочее время	Несанкционированная активность вне контролируемого периода	Поле **Время действия** в правиле **Межсетевого экрана** ограничивает доступ рабочими часами (09:00-18:00, будни) на основе объекта временного интервала
Утечка данных через интернет	Подрядчик пытается передать корпоративные данные через интернет-ресурсы, используя VPN-туннель	Запрет split-tunneling: в правиле передачи маршрутов указана только подсеть RDP-сервера, интернет-трафик подрядчика не маршрутизируется через NGFW Novum
Сохранение доступа после завершения контракта	Учетная запись остается активной после окончания срока работ	Ручное включение опции **Запретить доступ** в карточке пользователя по завершении контракта. Чек-лист завершения работ

Настройка в Ideco NGFW Novum

Подрядчик подключается к NGFW Novum из внешней сети через Ideco Client. NGFW Novum выполняет аутентификацию, проверяет устройство по **HIP-профилю** и применяет правила **Межсетевого экрана**. Трафик подрядчика проходит через профили **Контроля приложений** и **Предотвращения вторжений**, после чего маршрутизируется к RDP-серверу финансового отдела.

Пример адресации:

- Внешний IP-адрес Ideco NGFW Novum - `203.0.113.1`.
- Пул VPN-адресов Ideco Client - `10.128.0.0/16` (по умолчанию).
- RDP-сервер финансового отдела (1С) - `192.168.10.50`.
- Порт RDP - `3389/TCP`.

Задействованные модули NGFW Novum

Настройка безопасного доступа для подрядчика выполняется с помощью модулей:

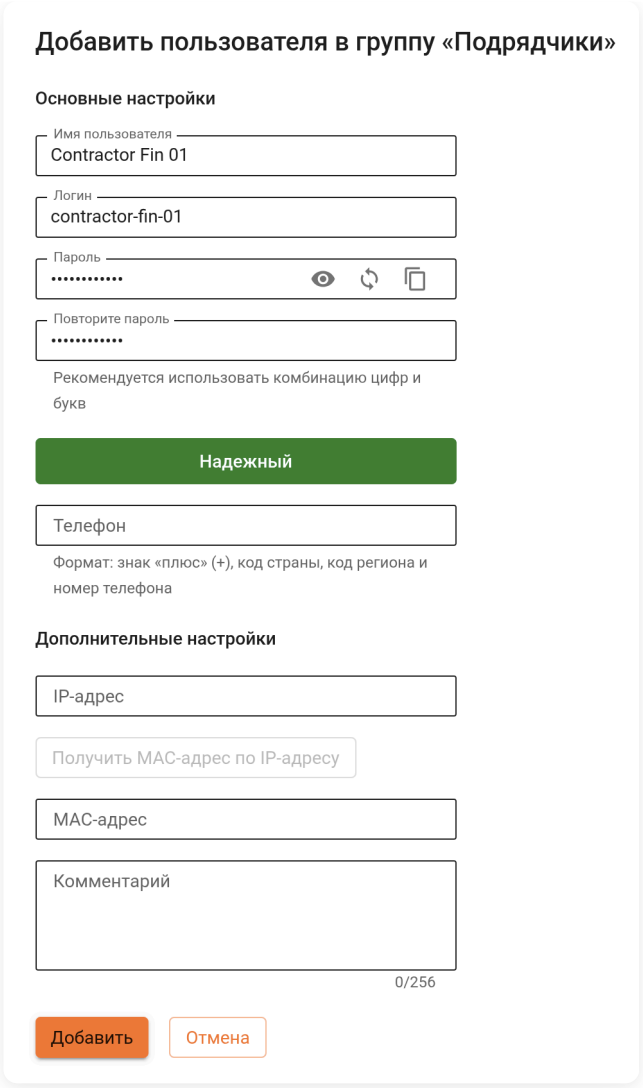
- **Ideco Client** - VPN-клиент для подключения подрядчика к NGFW Novum. Обеспечивает шифрованный туннель и передает информацию о состоянии устройства для проверки HIP-профилем.
- **Двухфакторная аутентификация (TOTP-токен)** - второй фактор при подключении через Ideco Client. Подрядчик вводит одноразовый код из приложения-аутентификатора.
- **Межсетевой экран (FORWARD)** - правила, ограничивающие доступ подрядчика одним IP-адресом и одним портом. GeoIP-фильтрация и ограничение по времени действия применяются в этих же правилах.
- **Профиль контроля приложений** - разрешает только протокол RDP.
- **Профиль предотвращения вторжений** - анализирует трафик подрядчика на предмет эксплойтов и RDP-уязвимостей.
- **HIP-профиль (профиль устройства)** - проверяет соответствие устройства подрядчика требованиям: операционная система Windows 11 и активный антивирус Касперского. Назначается в правиле доступа по VPN и блокирует подключение при несоответствии.
- **Логирование** - запись сессий подрядчика в журналы NGFW Novum для аудита.
- **Syslog** - передача журналов в SIEM-систему для долгосрочного хранения и анализа.

Создание учетной записи подрядчика

1. Перейдите в **Пользователи** → **Учетные записи**.

2. Выберите группу **Все локальные** в дереве пользователей. Нажмите на  для создания группы, введите название **Подрядчики** и нажмите **Добавить**.

3. Выберите созданную группу **Подрядчики** в дереве пользователей. На вкладке **Основное** нажмите **Создать пользователя** и заполните поля:



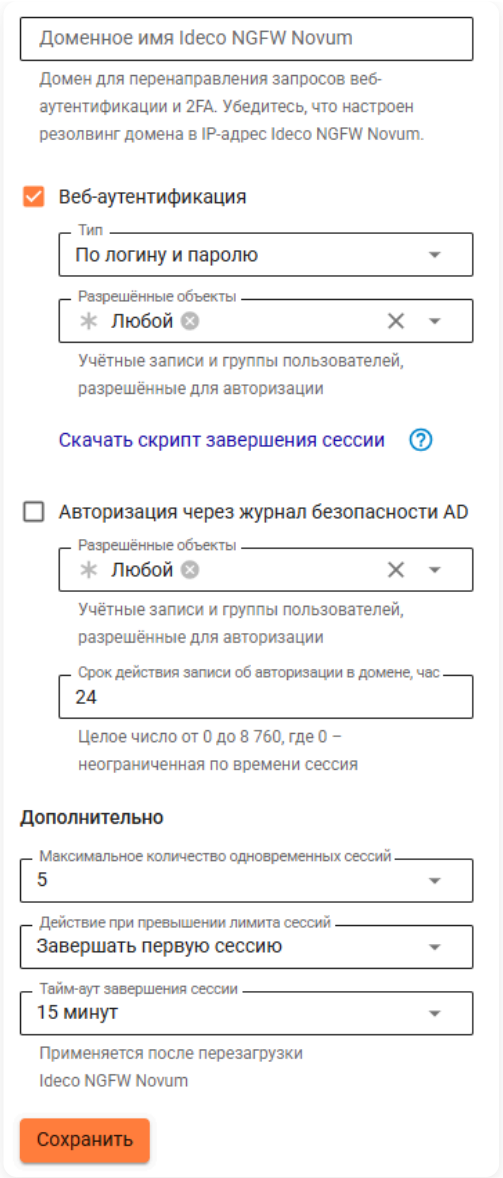
- **Имя пользователя** - введите отображаемое имя. Например, `Contractor Fin 01`.
- **Логин** - укажите логин. Например, `contractor-fin-01`.
- **Пароль** и **Повторите пароль** - задайте сложный пароль длиной не менее 12 символов.

4. Нажмите **Добавить**.

> По завершении контракта включите опцию **Запретить доступ** в карточке пользователя - это заблокирует учетную запись немедленно.

Настройка двухфакторной аутентификации

1. Перейдите в **Пользователи** → **Авторизация** и убедитесь, что опция **Веб-аутентификация** включена:



2. Укажите доменное имя Ideco NGFW Novum в поле **Доменное имя Ideco NGFW Novum**, чтобы на сервер перенаправлялись запросы двухфакторной аутентификации.

3. Перейдите в **Пользователи** → **Аутентификация** → **Двухфакторная аутентификация**.

4. Включите опцию **TOTP-токен**.

5. Включите опцию **Разрешить инициализацию секретного ключа из внешних сетей**, если подрядчик будет генерировать QR-код из внешней сети.

6. Нажмите **Сохранить**.

Создание HIP-профиля для проверки устройства подрядчика

HIP-профили позволяют задать критерии проверки устройств, подключающихся через Ideco Client. Для подрядчика настройте проверку операционной системы и антивируса.

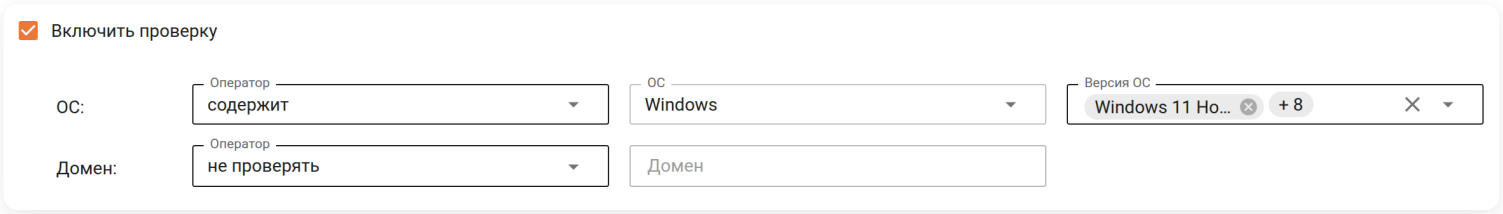
Создание HIP-объекта

1. Перейдите в **Пользователи** → **Профили устройств** → **HIP-объекты** и нажмите **Добавить**.

2. Введите название. Например, `Contractor-Device-Requirements`.

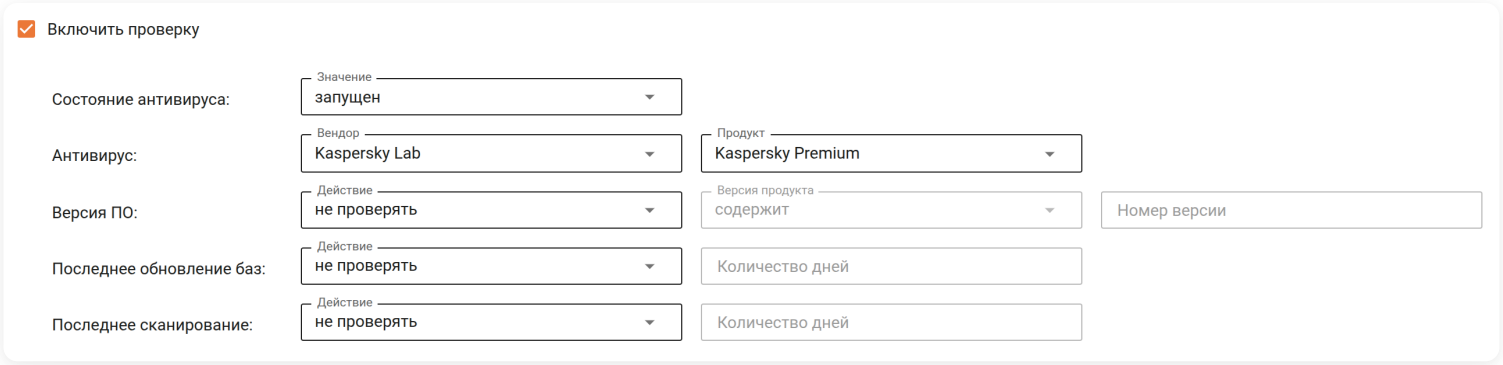
3. Включите проверки, нажав **Включить проверку** для каждого критерия:

ОС и домен



- Оператор - **содержит**.
- ОС - **Windows**.
- Версия ОС - **11**.

Антивирус



- Состояние антивируса - **Запущен**.
- Вендор - `Kaspersky Lab`.

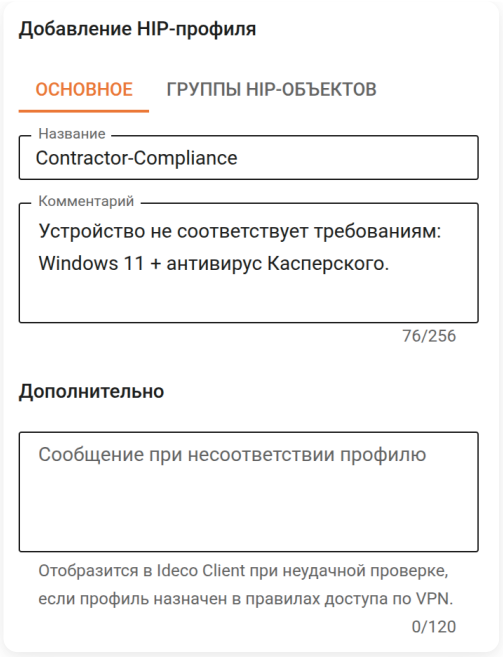
> Для большей детализации можно добавить версию установленного пакета обновлений.

4. Нажмите **Добавить**.

Создание HIP-профиля

1. Перейдите на вкладку **HIP-профили** и нажмите **Добавить**.

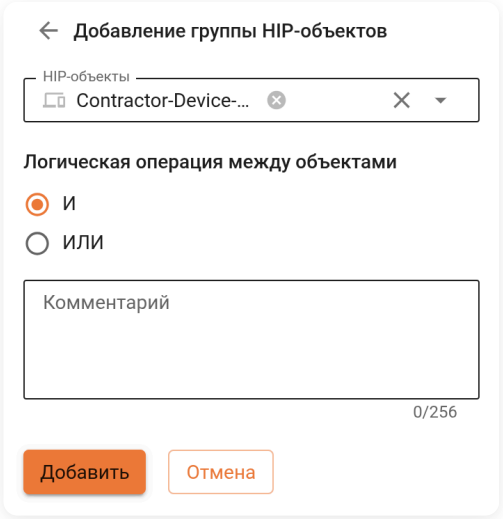
2. Заполните поля на вкладке **Основное**:



- **Название HIP-профиля** - `Contractor-Compliance`.
- **Сообщение при несоответствии профилю** - `Устройство не соответствует требованиям: Windows 11 + антивирус Касперского`.

3. Перейдите на вкладку **Группы HIP-объектов**.

4. Нажмите **Добавить группу**, заполните поля и нажмите **Добавить**:



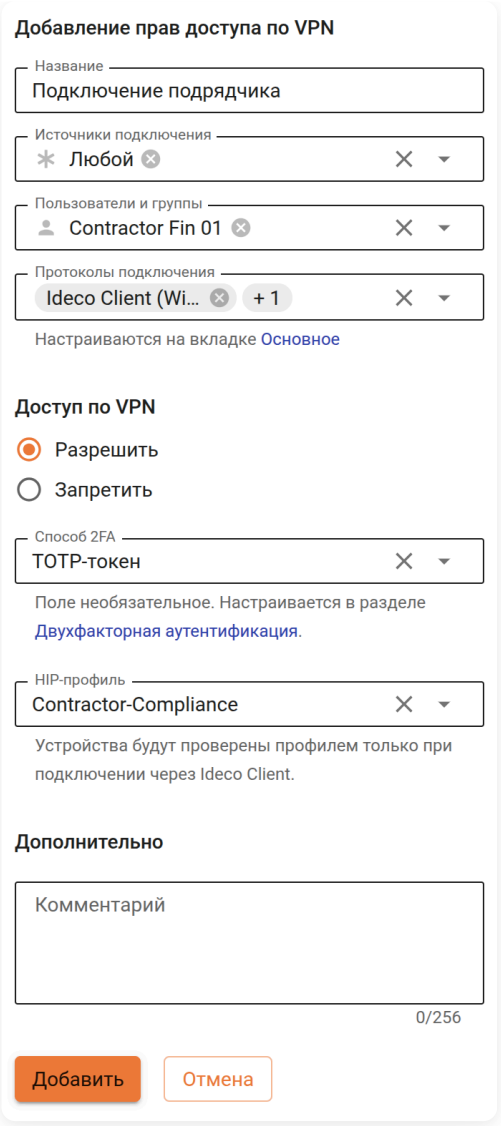
- **HIP-объекты** - выберите созданный объект `Contractor-Device-Requirements`.
- **Логическая операция между объектами** - укажите логическую операцию **И**.

4. Нажмите **Добавить**.

Настройка VPN-подключения через Ideco Client

1. Перейдите в **Пользователи** → **Ideco Client** и убедитесь, что служба включена.

2. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и нажмите **Добавить**. Заполните поля:

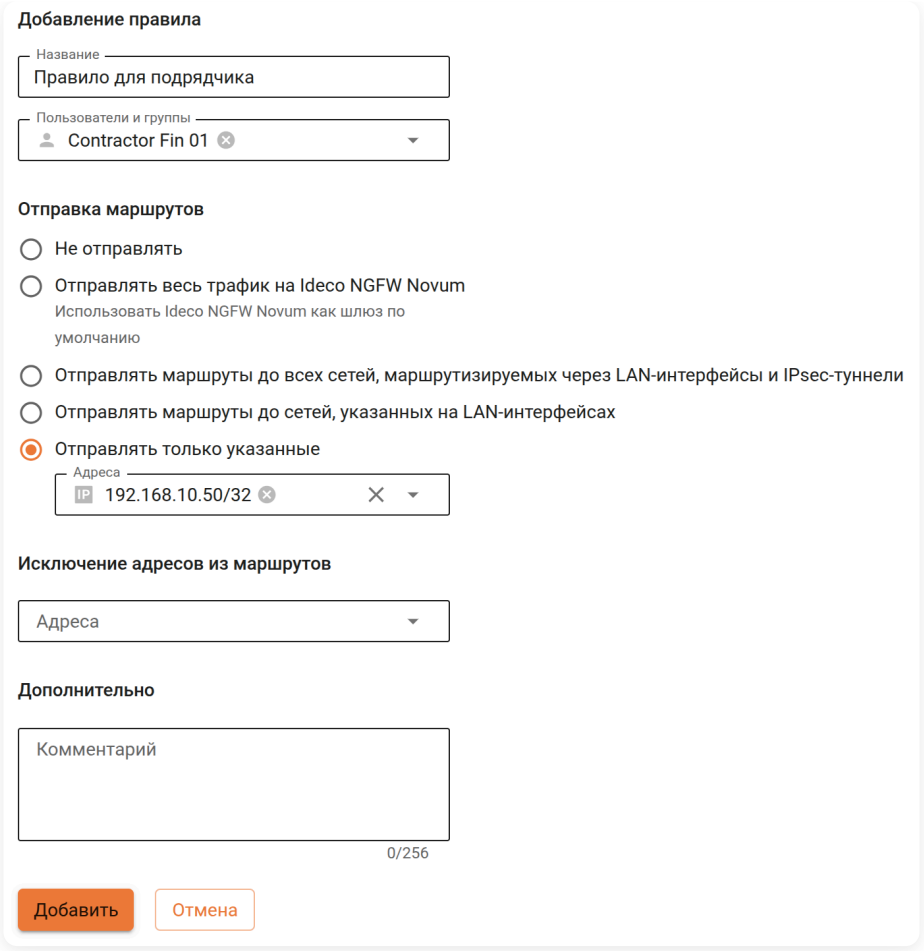


- **Пользователи и группы** - выберите пользователя `contractor-fin-01`.
- **Способ 2FA** - выберите **TOTP-токен**.
- **HIP-профиль** - выберите `Contractor-Compliance`.

> Именно здесь HIP-профиль блокирует само VPN-подключение при несоответствии устройства требованиям - с сообщением, заданным в профиле.

3. Нажмите **Добавить**.

4. Перейдите на вкладку **Передача маршрутов** и нажмите **Добавить**. Заполните поля:



- **Пользователи и группы** - выберите пользователя `contractor-fin-01`.
- **Тип передачи** - выберите **Отправлять только указанные**.
- **Сети** - укажите `192.168.10.50/32`.

5. Нажмите **Добавить**.

Эта настройка ограничит маршрутизацию на стороне VPN-клиента: на устройство подрядчика будет передан только маршрут до RDP-сервера. Интернет-трафик подрядчика не будет проходить через NGFW Novum (запрет split-tunneling).

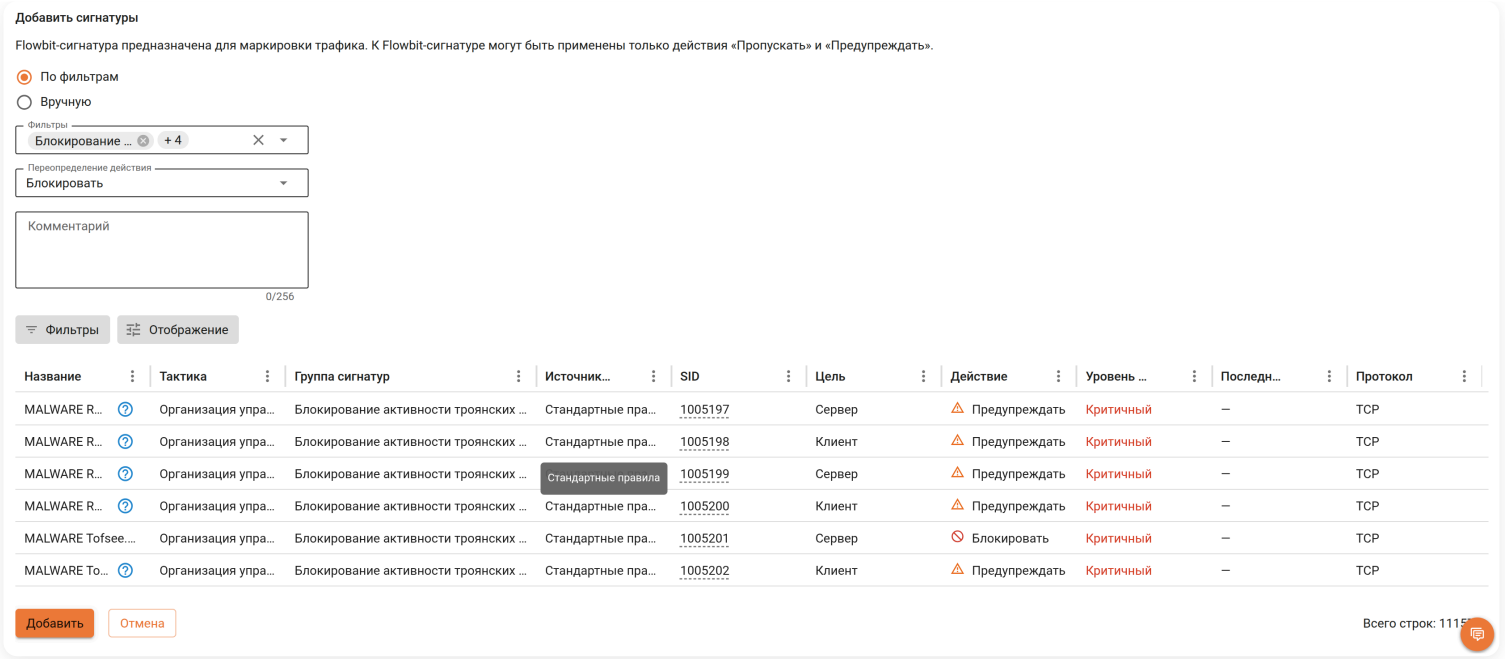
Создание профиля Предотвращения вторжений

1. Перейдите в **Профили безопасности** → **Предотвращение вторжений** и нажмите **Добавить**.

2. Введите название профиля, например, `IPS-Contractor-RDP`, и нажмите **Добавить**.

3. Перейдите на вкладку **Сигнатуры** созданного профиля и нажмите **Добавить сигнатуры**.

4. Выберите способ **По фильтрам**. Последовательно добавьте каждую из групп сигнатур, связанных с защитой RDP-соединений. Для каждой группы выберите действие **Блокировать** и нажмите **Добавить**:



- **Блокирование атак** - обнаружение эксплойтов, сканирования портов и попыток удаленного выполнения кода.
- **Атаки на получение прав пользователя** - выявление попыток получить несанкционированный доступ к учетным данным.
- **Атаки на получение привилегий администратора** - защита от эскалации привилегий.
- **Блокирование активности троянских программ** - обнаружение вредоносной активности в канале подключения.
- **Блокирование крупных утечек информации** - предотвращение несанкционированного экспорта данных.

5. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

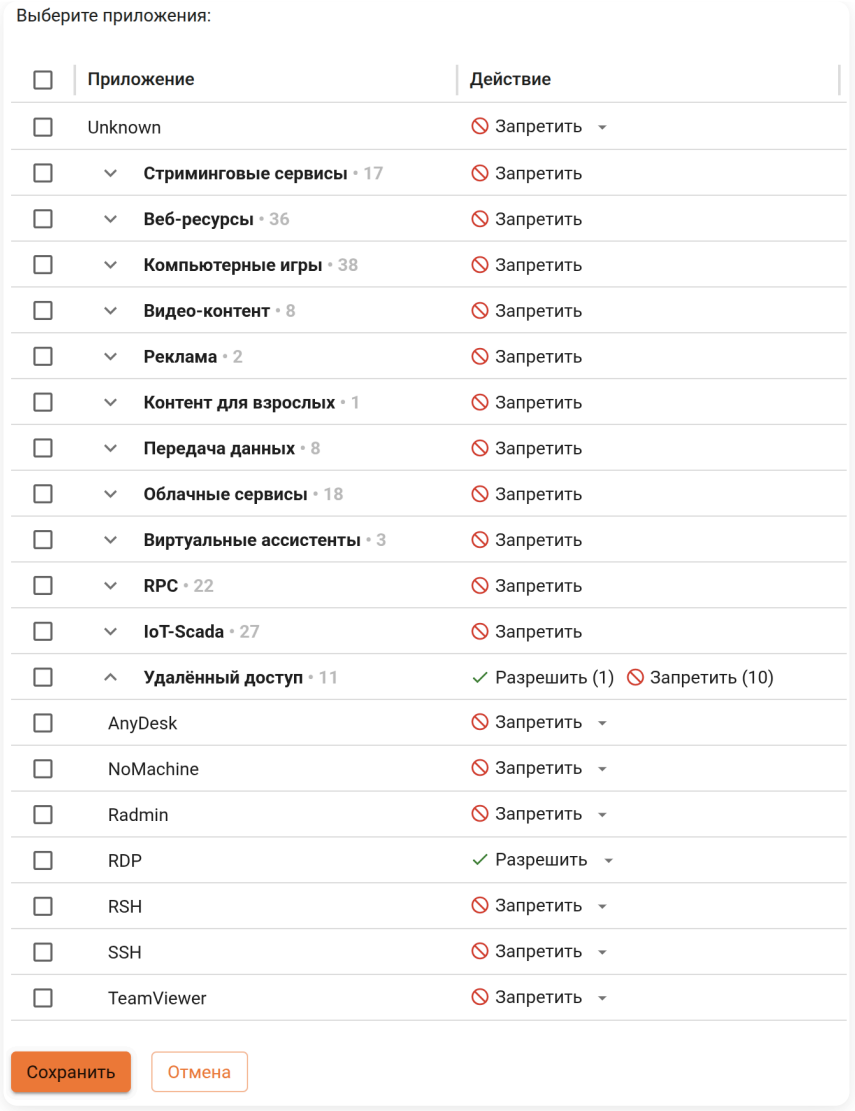
Создание профиля Контроля приложений

1. Перейдите в **Профили безопасности → Контроль приложений** и нажмите **Добавить**.

2. Введите название профиля, например `AppControl-RDP-Only`, и нажмите **Добавить**.

3. Перейдите на вкладку **Доступ к приложениям**.

4. Выберите все протоколы и приложения, которые необходимо заблокировать (например, HTTP, HTTPS, SMB, SSH, FTP и другие). Примените к ним действие **Запретить**:



5. Нажмите **Сохранить**.

Принцип работы по умолчанию: все протоколы и приложения, которые явно не запрещены, остаются разрешены. Создавать отдельное разрешающее правило для RDP не нужно - он разрешен автоматически, пока не попадет под запрет.

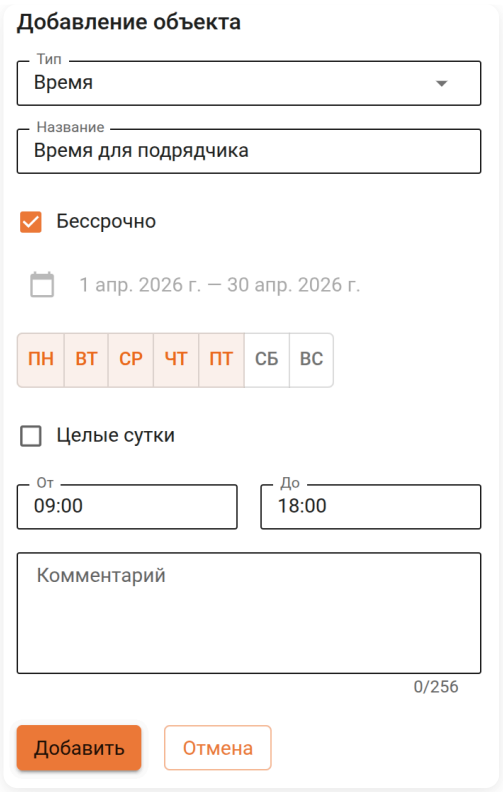
Настройка правил Межсетевого экрана

Правила **Межсетевого экрана** обеспечивают сетевую изоляцию подрядчика. Создайте правила в порядке, указанном ниже, и убедитесь, что разрешающее правило расположено выше запрещающего в таблице.

Создание объекта Время

Перед настройкой правила необходимо создать объект временного интервала, который будет использован в поле **Время действия** правила **Межсетевого экрана**.

1. Перейдите в **Правила трафика** → **Объекты**, нажмите **Добавить** и заполните поля:



- **Тип** - выберите тип объекта **Время**.
- **Название** - укажите название. Например, `Время для подрядчика`.

Укажите временные промежутки: **понедельник–пятница**, с **09:00** до **18:00**.

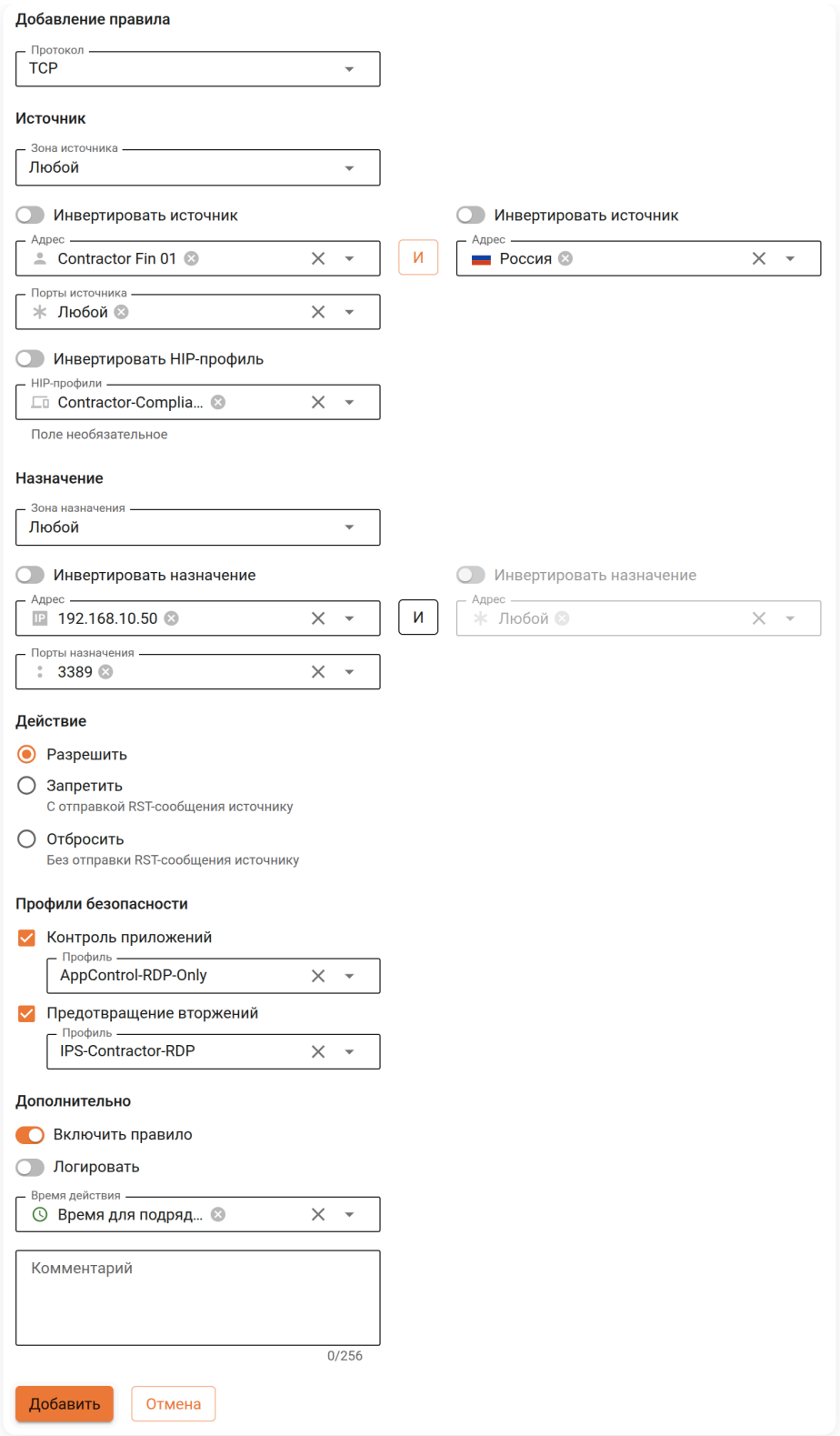
2. Нажмите **Добавить**.

Время задается по часовому поясу сервера, так как сервер не знает локального времени клиента.

Разрешающее правило для доступа к RDP-серверу

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - TCP.
- **Источник**:
  - **Адрес** - пользователь `contractor-fin-01`.
  - С помощью оператора **И** добавьте второе условие: **Страна** - Россия (GeoIP-фильтрация).
  - **HIP-профили** - `Contractor-Compliance` для дополнительной проверки соответствия устройства на уровне трафика.
- **Назначение**:
  - **Адрес** - IP-адрес RDP-сервера `192.168.10.50`.
  - **Порты назначения** - `3389`.
- **Действие** - Разрешить.
- **Профили безопасности**:
  - **Контроль приложений** - `AppControl-RDP-Only`.
  - **Предотвращение вторжений** - `IPS-Contractor-RDP`.

- **Дополнительно**:
  - **Время действия** - объект `Время для подрядчика`.
  - **Включить правило** - включите опцию.

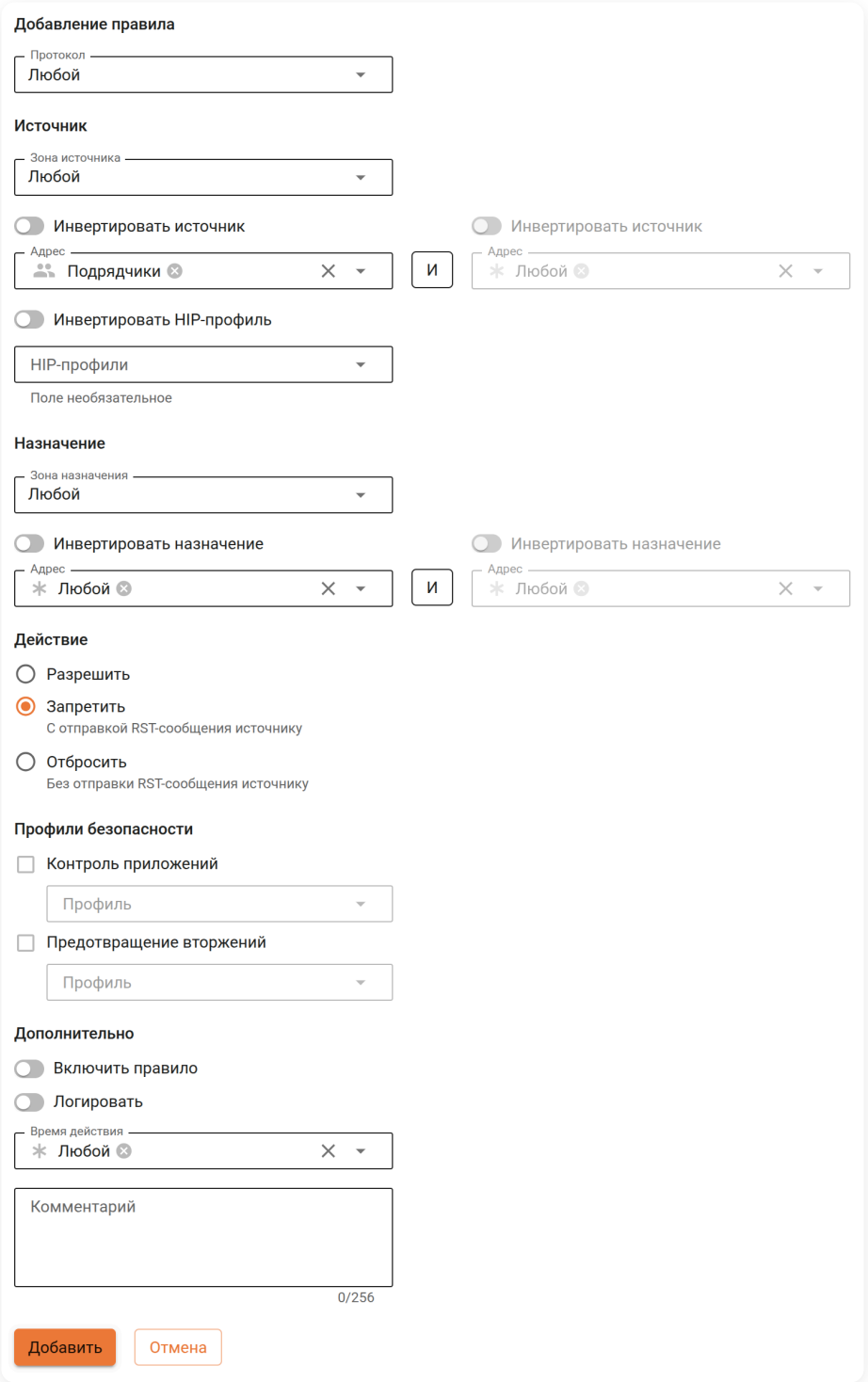
3. Нажмите **Добавить**.

> В зависимости от используемой версии протокола RDP также может потребоваться правило с UDP. Создайте аналогичное правило с протоколом UDP, используя кнопку **Клонировать** в таблице правил.

Запрещающее правило для блокировки остального трафика

1. На вкладке **FORWARD** нажмите **Добавить**.

2. Заполните поля:



- **Источник**:

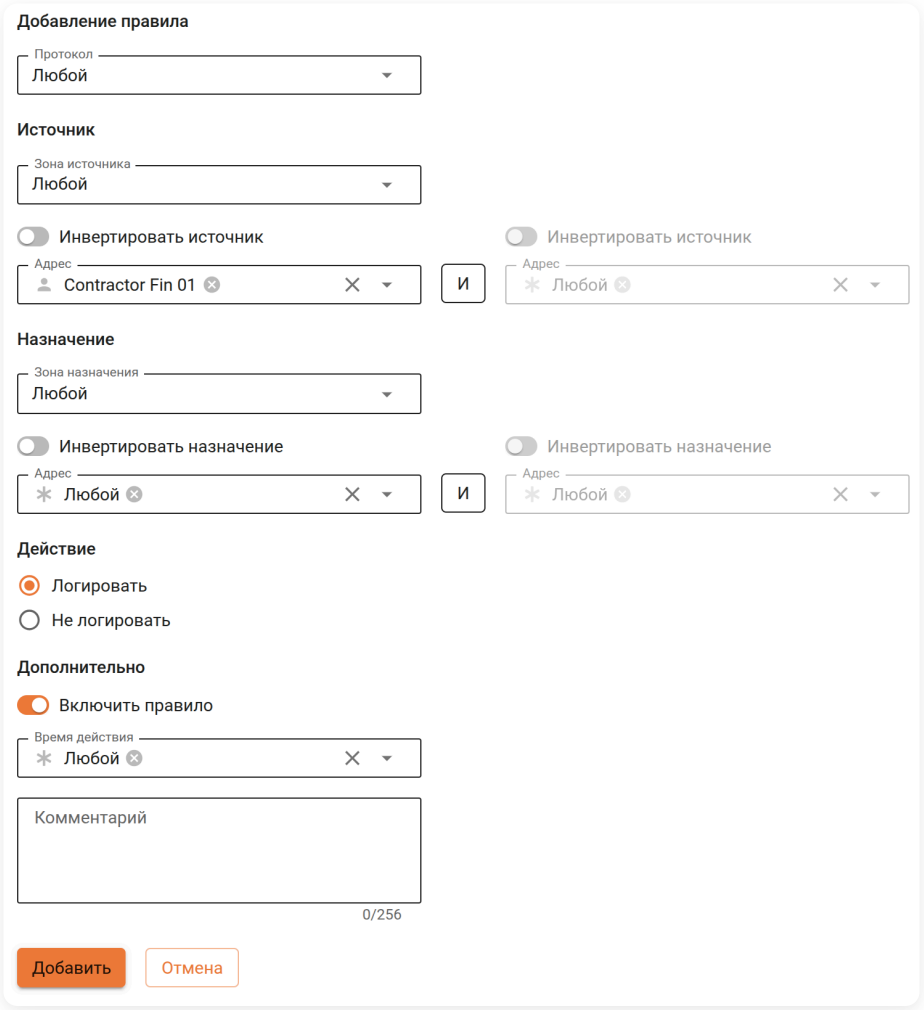
- **Адрес** - пользователь `contractor-fin-01` или группа **Подрядчики**.
- **Дополнительно**:
  - **Действие** - Запретить.
  - **Включить правило** - включите опцию.

3. Нажмите **Добавить**.

Настройка логирования

Для записи всех сессий подрядчика настройте логирование трафика.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Логирование**, нажмите **Добавить** и заполните поля:



- **Источник** - выберите пользователя `contractor-fin-01` или группу **Подрядчики**.
- **Действие** - Логировать.
- **Включить правило** - включите опцию.

2. Нажмите **Добавить**.

3. Включите опцию **Логировать срабатывания правил**.

> Записи доступны в **Отчеты и журналы** → **Межсетевой экран**. Информация о срабатывании профилей **Контроля приложений** и **Предотвращения вторжений** также фиксируется в журнале.

Передача журналов в SIEM-систему

Для долгосрочного хранения и анализа настройте передачу логов через Syslog:

1. Перейдите в **Сервисы** → **Syslog** и включите модуль.

2. Укажите адрес и порт SIEM-системы или Syslog-коллектора.

3. Выберите **Протокол передачи**.

4. Нажмите **Сохранить**.

Все события, включая сессии подрядчика, срабатывания системы **Предотвращения вторжений** и действия **Межсетевого экрана**, будут передаваться в указанную систему.

Установка Ideco Client на устройство подрядчика

1. Передайте подрядчику ссылку для скачивания Ideco Client. Скачать клиент можно в веб-интерфейсе Ideco NGFW Novum или в личном кабинете пользователя.

2. Подрядчик устанавливает Ideco Client на устройство с Windows 11.

3. При первом подключении подрядчик указывает:

- **Адрес сервера** - внешний IP-адрес или доменное имя Ideco NGFW Novum.
- **Логин** - `contractor-fin-01`.
- **Пароль** - пароль, заданный при создании учетной записи.

4. После ввода логина и пароля подрядчик перенаправляется на страницу двухфакторной аутентификации. При первом подключении необходимо войти в личный кабинет NGFW Novum, нажать **Настроить двухфакторную аутентификацию** и отсканировать QR-код в приложении-аутентификаторе (Яндекс ID, Google Authenticator или Microsoft Authenticator).

5. При последующих подключениях подрядчик вводит одноразовый код из приложения для прохождения двухфакторной аутентификации.

После успешной аутентификации Ideco Client устанавливает VPN-туннель. NGFW Novum проверяет устройство по HIP-профилю `Contractor-Compliance`. Если устройство не соответствует требованиям (отсутствует Windows 11 или антивирус Касперского не активен), подключение блокируется с сообщением **Устройство не соответствует требованиям: Windows 11 + антивирус Касперского**.

Чек-лист: проверка настройки

После завершения настройки выполните проверку:

- ☑ Убедитесь, что подрядчик подключается через Ideco Client и проходит двухфакторную аутентификацию
- ☑ Проверьте, что в **Мониторинг** → **Сессии пользователей** отображается сессия подрядчика с назначенным HIP-профилем `Contractor-Compliance`
- ☑ Убедитесь, что подрядчик имеет доступ только к RDP-серверу по адресу `192.168.10.50:3389`, весь остальной трафик должен быть заблокирован
- ☑ Проверьте **Отчеты и журналы** → **События безопасности** → **Журнал IPS** на наличие записей по трафику подрядчика
- ☑ Проверьте записи в **Отчеты и журналы** → **Межсетевой экран** для аудита сессий
- ☑ Попробуйте подключиться за пределами рабочего времени (после 18:00 или в выходной) и убедитесь, что доступ запрещен

Чек-лист: действия при завершении работы с подрядчиком

По окончании контрактного периода выполните действия:

- ☑ Завершите активную сессию подрядчика в **Мониторинг** → **Сессии пользователей**, если она активна
- ☑ Откройте карточку пользователя `contractor-fin-01` в **Пользователи** → **Учетные записи** и на вкладке **Основное** включите опцию **Запретить доступ**
- ☑ Отключите правило `Contractor-Allow-RDP` в **Правила трафика** → **Межсетевой экран** → **FORWARD**
- ☑ Отключите правило `Contractor-Deny-All` в **Правила трафика** → **Межсетевой экран** → **FORWARD**
- ☑ Удалите запись пользователя `contractor-fin-01` из таблицы **Доступ по VPN** в **Пользователи** → **VPN-подключения**
- ☑ Сбросьте секретный ключ двухфакторной аутентификации в карточке пользователя `contractor-fin-01` в **Пользователи** → **Учетные записи**
- ☑ Сохраните журналы сессий подрядчика из **Отчеты и журналы** → **Межсетевой экран** и **Отчеты и журналы** → **Аутентификация пользователей** для архива либо убедитесь, что они уже имеются в SIEM-системе
- ☑ При необходимости удалите учетную запись, группу, HIP-профиль и профили безопасности, если они больше не используются

Полезные ссылки

- **Двухфакторная аутентификация**
- **Пользователи**
- **Профили устройств**
- **Управление учетными записями и группами**

Сервисы

Практические руководства по настройке сервисов Ideco NGFW

DNS

Настройка DNS-сервера и Forward-зон

Перейти >

Сетевые интерфейсы

Настройка Wi-Fi-сети и LACP

Перейти >

IPsec

Подключение различных устройств к Ideco NGFW по IPsec

Перейти >

ГОСТ VPN

Генерация ключей и сертификатов ГОСТ VPN

Перейти >

Прокси

Настройка прямых подключений к прокси-серверу

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

DNS

Практические руководства по настройке DNS в Ideco NGFW

Подключение через Ideco Client к внутреннему DNS

Перейти >

Пример настройки Forward-зоны

Перейти >

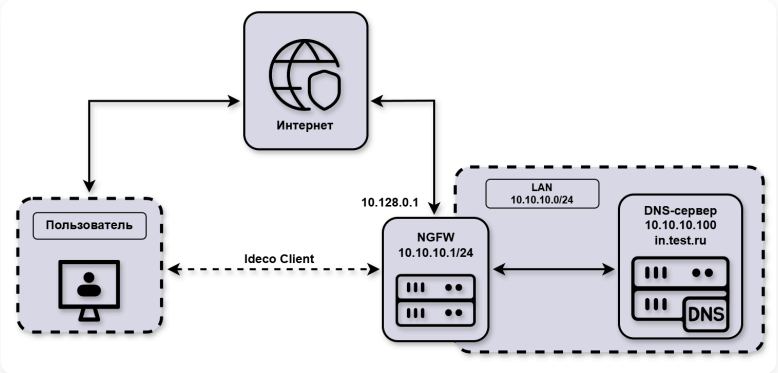
Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Подключение через Ideco Client к внутреннему DNS

Клиенты, подключающиеся к NGFW Novum из внешней сети через Ideco Client, изначально не видят внутренний DNS-сервер.

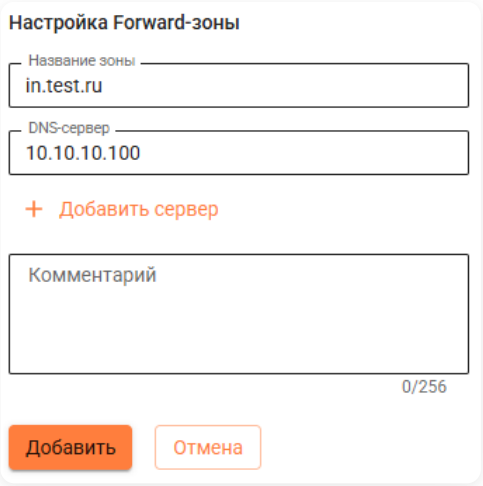
Схема сети:



Для настройки подключения к внутреннему DNS-серверу выполните действия:

1. Перейдите в **Сервисы** → **DNS** → **FORWARD-ЗОНЫ** и нажмите **Добавить**.

2. Заполните форму и нажмите **Добавить**:



После настройки NGFW Novum клиенты, подключающиеся к NGFW Novum с помощью Ideco Client из интернета, смогут использовать внутренний DNS-сервер.

Полезные ссылки

- **DNS**
- **Forward-зоны**
- **Ideco Client**

Пример настройки Forward-зоны

Как настроить сеть, чтобы пользователи локальной сети могли обращаться к ресурсам, опубликованным на Ideco NGFW Novum. Ресурсы находятся в защищенной сети, и доступ к ним должен осуществляться напрямую, без выхода через внешний интерфейс.

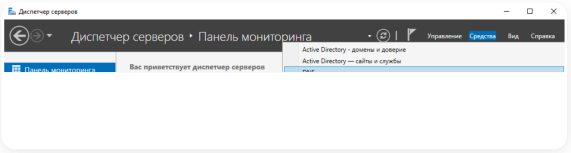
Если в сети уже есть DNS-сервер

1. На DNS-сервере, например, в AD, создайте новую зону прямого просмотра, на которую будут перенаправляться запросы пользователей. В зоне прямого просмотра создайте необходимые DNS-записи с приватными IP-адресами.

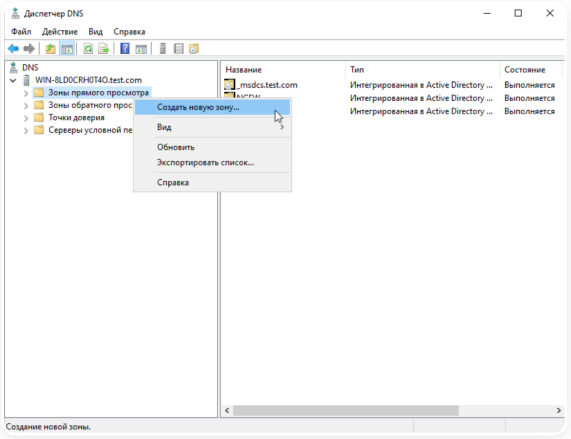
2. На Ideco NGFW Novum настройте Forwad-зону для перенаправления пользователей на зону прямого просмотра в AD.

Пример с настройкой DNS-сервера в AD

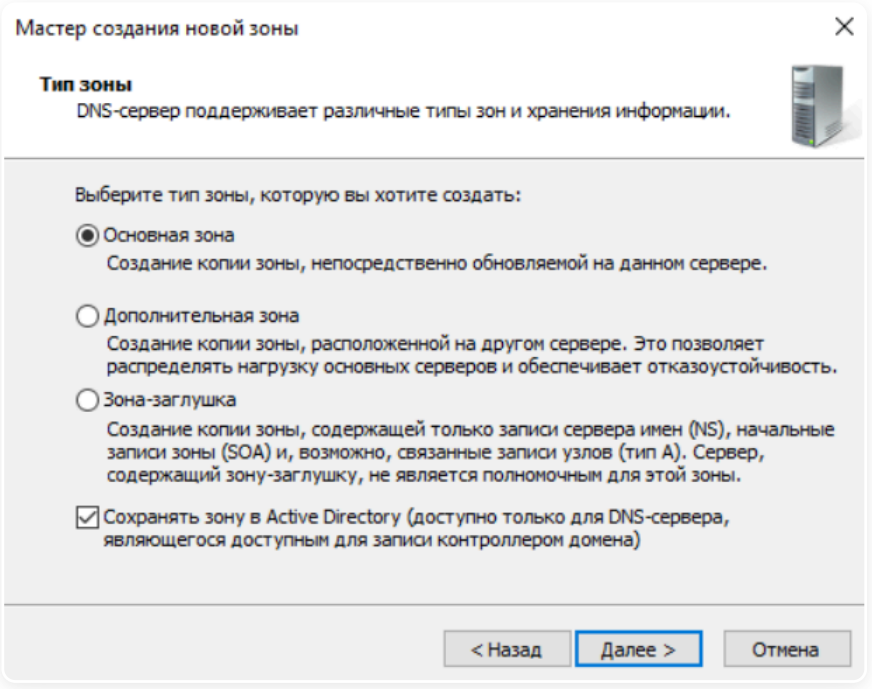
1. На контроллере домена откройте **Диспетчер сервера** → **Средства** → **DNS**:



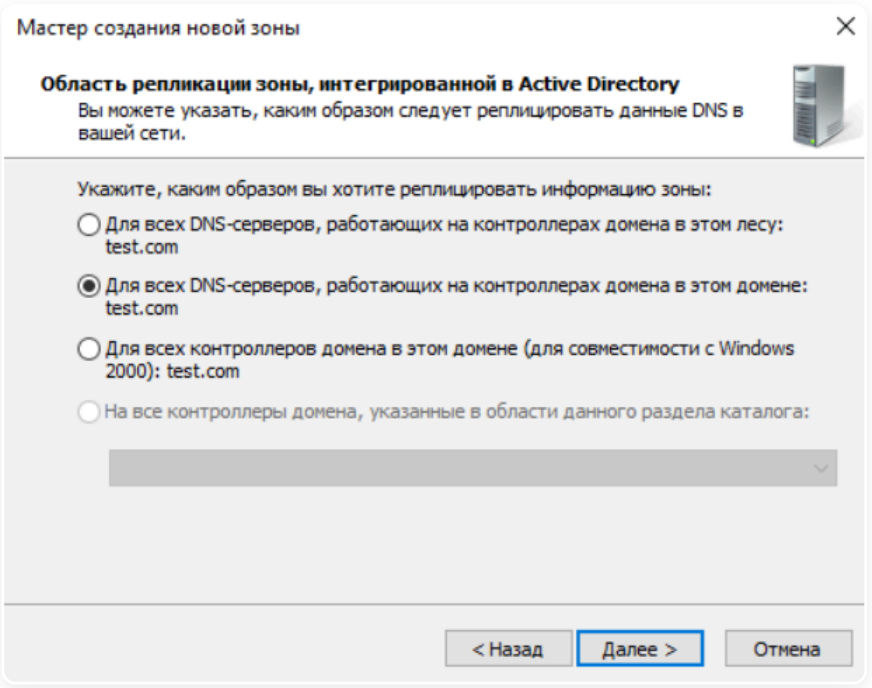
2. В новом окне разверните узел сервера, нажмите правой кнопкой мыши на **Зоны прямого просмотра** и выберите **Создать новую зону**:



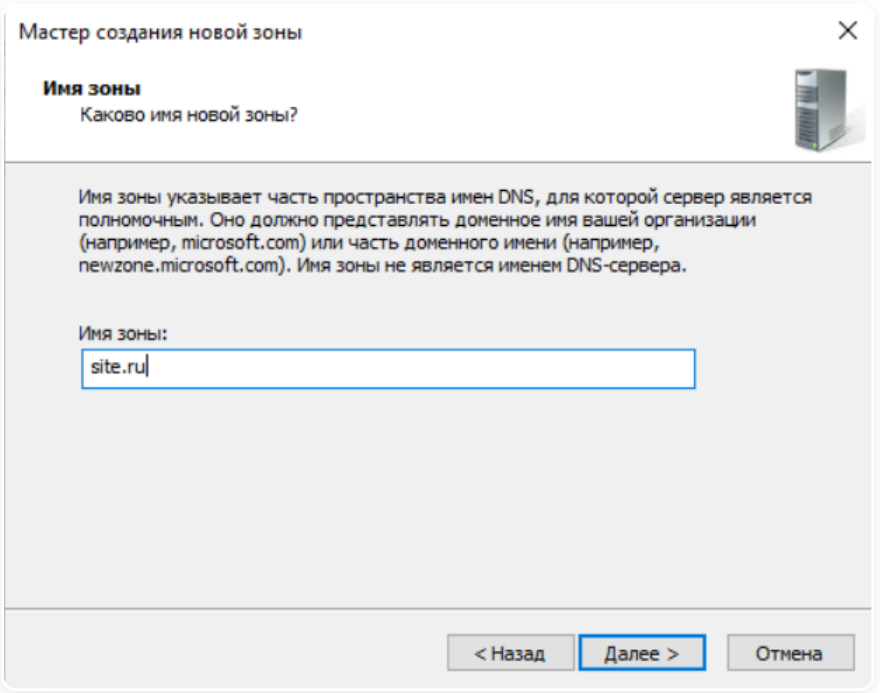
3. Нажмите **Далее** и выберите тип **Основная зона**. Для интеграции с AD убедитесь, что включена опция **Хранить зону в Active Directory**:



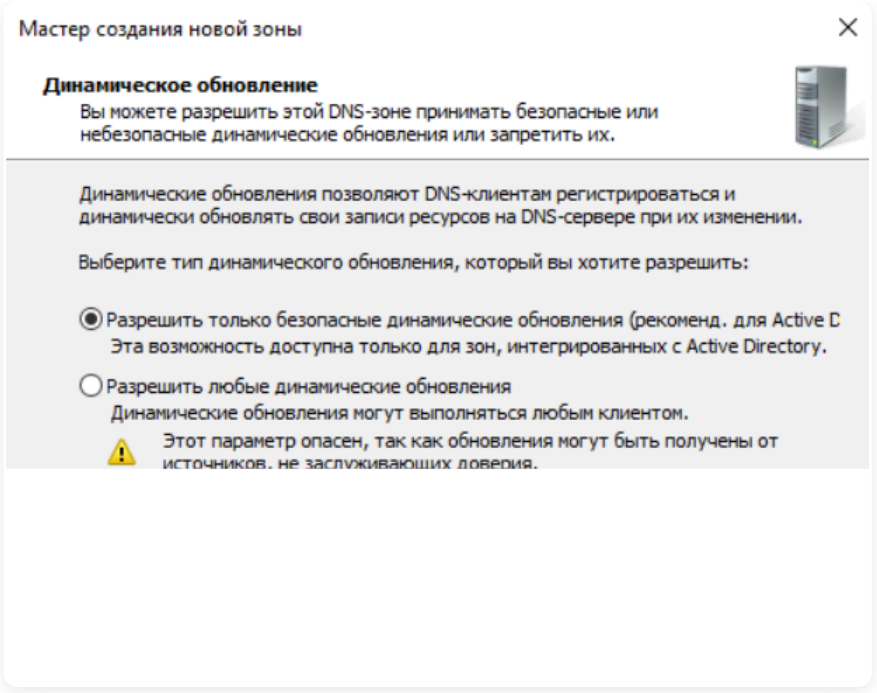
4. Выберите область репликации для зоны (например, **На все DNS-серверы, работающие на контроллерах домена в этом домене**), чтобы зона автоматически реплицировалась:



5. Укажите имя зоны:



6. Настройте динамические обновления. Для безопасности в доменной среде рекомендуется выбрать **Разрешать только безопасные динамические обновления**:



7. Нажмите **Готово**.

8. Создайте новую A-запись. В DNS-менеджере нажмите правой кнопкой мыши по созданной зоне и выберите **Создать узел (A или AAAA)**:

9. Заполните поля:

- **Имя** - введите имя хоста (например, `in` для полного доменного имени `in.site.ru`).
- **IP-адрес** - введите внутренний IP-адрес сервера.
- **Создать связанную запись (PTR)** - по желанию можно включить опцию для автоматического создания соответствующей PTR-записи в зоне обратного просмотра.

10. Сохраните запись, нажав **Добавить узел**.

11. Перейдите в Ideco NGFW Novum в раздел **Сервисы** → **DNS** → **FORWARD-зоны** и нажмите **Добавить**.

12. Заполните поля:

- **Название зоны** - укажите имя зоны из пункта 5.
- **DNS-сервер** - укажите IP-адрес из пункта 9.

13. Нажмите **Добавить**.

Полезные ссылки

- **DNS**
- **Forward-зоны**

Сетевые интерфейсы

Практические руководства по настройке сетевых интерфейсов в Ideco NGFW

Настройка Wi-Fi-сети

Перейти >

Настройка LACP на Hyper-V

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка Wi-Fi-сети

В текущей версии Ideco NGFW Novum не поддерживает Wi-Fi-адаптеры. Для работы беспроводных клиентов необходимо использовать беспроводные точки доступа или Wi-Fi-маршрутизаторы.

Для выхода в интернет пользователей, подключающихся по Wi-Fi, необходима авторизация пользователей или Wi-Fi-роутера в Ideco NGFW Novum. Способ авторизации зависит от режима работы маршрутизатора.

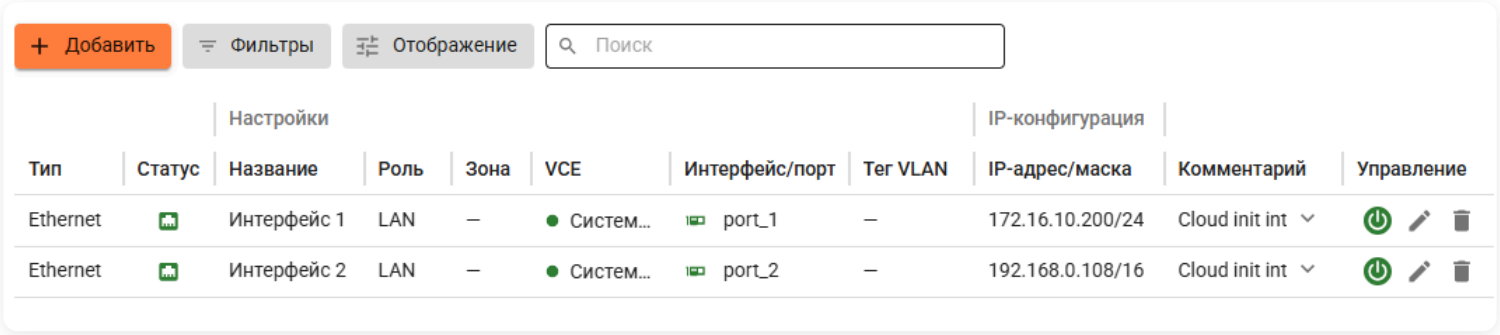
Режим точки доступа или bridge

В режиме точки доступа или bridge устройство Wi-Fi позволяет беспроводным клиентам подключаться к локальной сети.

Для этого индивидуально авторизуйте всех беспроводных клиентов на Ideco NGFW Novum с помощью IP-авторизации. Воспользуйтесь рекомендациями по настройке:

- Используйте отдельную логическую сеть для клиентов Wi-Fi с настроенным DHCP-сервером.
- Создайте в **Сервисы** → **Сетевые интерфейсы** новый интерфейс, в IP-конфигурации выберите режим **Статический**, добавьте IP-адрес, служащий шлюзом для этой сети.
- Создайте группу пользователей, подключающихся по Wi-Fi.
- С помощью Контент-фильтра настройте необходимые ограничения для пользователей Wi-Fi.
- Если Wi-Fi-роутер подключен к отдельному физическому интерфейсу Ideco NGFW Novum, то в **Межсетевом экране** запретите доступ из беспроводной сети в локальную сеть.

Пример настройки интерфейса для клиентов, подключающихся по Wi-Fi:



- `172.16.10.200/24` - интерфейс для беспроводной Wi-Fi-сети.
- `192.168.0.108/16` - интерфейс для локальной Ethernet-сети.

Настройка DHCP

1. Создайте в **Сервисы** → **Сетевые интерфейсы** новый интерфейс, в IP-конфигурации выберите режим **DHCP**.

2. Перейдите в **Сервисы** → **DHCP-сервер** и выберите сетевой интерфейс, настроенный на прошлом шаге.

3. Назначьте диапазон IP-адресов для DHCP-сервера и нажмите **Сохранить**.

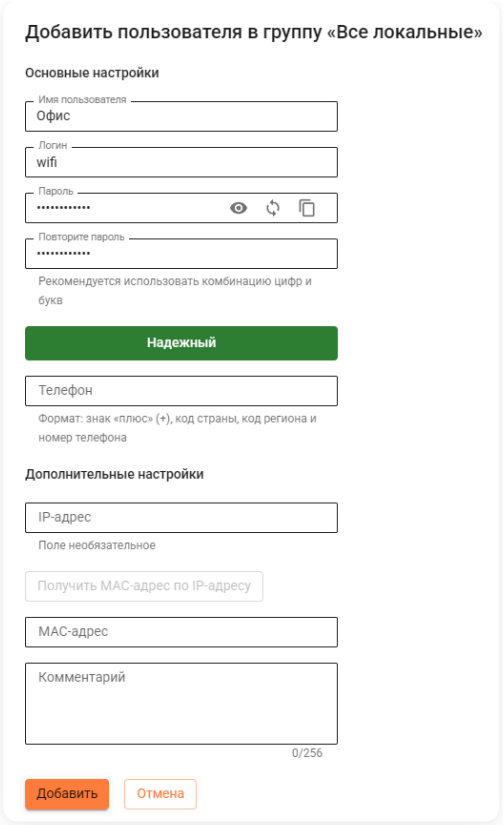
Для индивидуальной авторизации Wi-Fi-пользователей и учета их трафика и статистики воспользуйтесь Веб-аутентификацией. При таком способе авторизации Ideco NGFW Novum будет учитывать каждого пользователя, подключившегося по Wi-Fi. Это следует принять во внимание при планировании лицензирования Ideco NGFW Novum.

Режим роутера

В режиме роутера устройство Wi-Fi скрывает за NAT устройства беспроводной сети. Таким образом, для Ideco NGFW Novum достаточно будет авторизовать только точку доступа как одного из пользователей.

Пример настройки пользователя в режиме роутера:

1. В **Пользователи** → **Учетные записи** создайте пользователя для Wi-Fi-роутера:



2. Перейдите к настройкам пользователя, выберите **IP и MAC авторизация**, добавьте правило и укажите IP-адрес. Правило также можно добавить в **Пользователи** → **Авторизация** → **IP и MAC**.

К пользователю необходимо применить общие ограничения **Контент-фильтра** для Wi-Fi-сети.

Настройка DHCP

При работе маршрутизатора в режиме роутера не требуется дополнительной настройки DHCP-сервера Ideco NGFW Novum, так как работает встроенный DHCP-сервер маршрутизатора. Если у вас не получилось подключиться к Wi-Fi-сети, нужно проверить работу DHCP-сервера маршрутизатора.

При этом способе авторизации в Ideco NGFW Novum будет использоваться одна лицензия на точку доступа Wi-Fi. Отдельно настроить фильтрацию трафика и считать статистику по трафику в отчетах для отдельных клиентов Wi-Fi будет невозможно.

Полезные ссылки

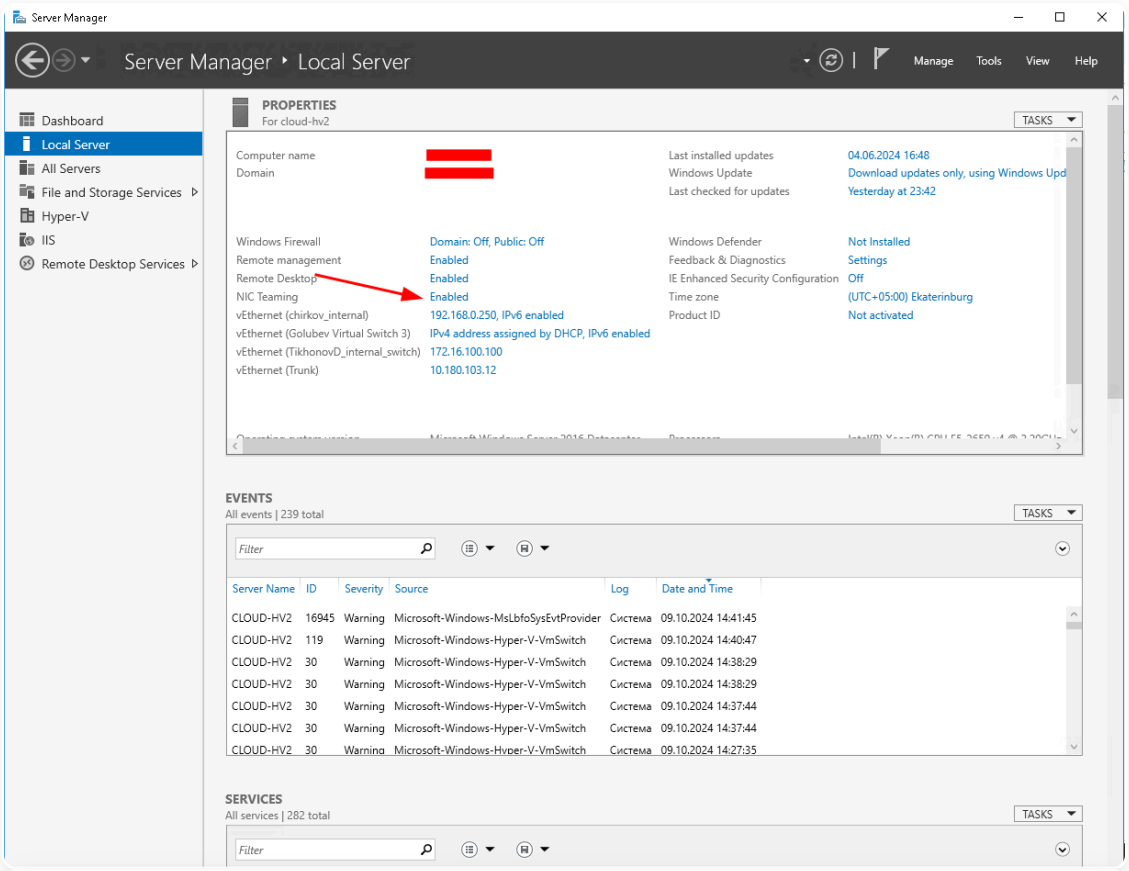
- **DHCP-сервер**
- **Авторизация**
- **Интерфейсы**

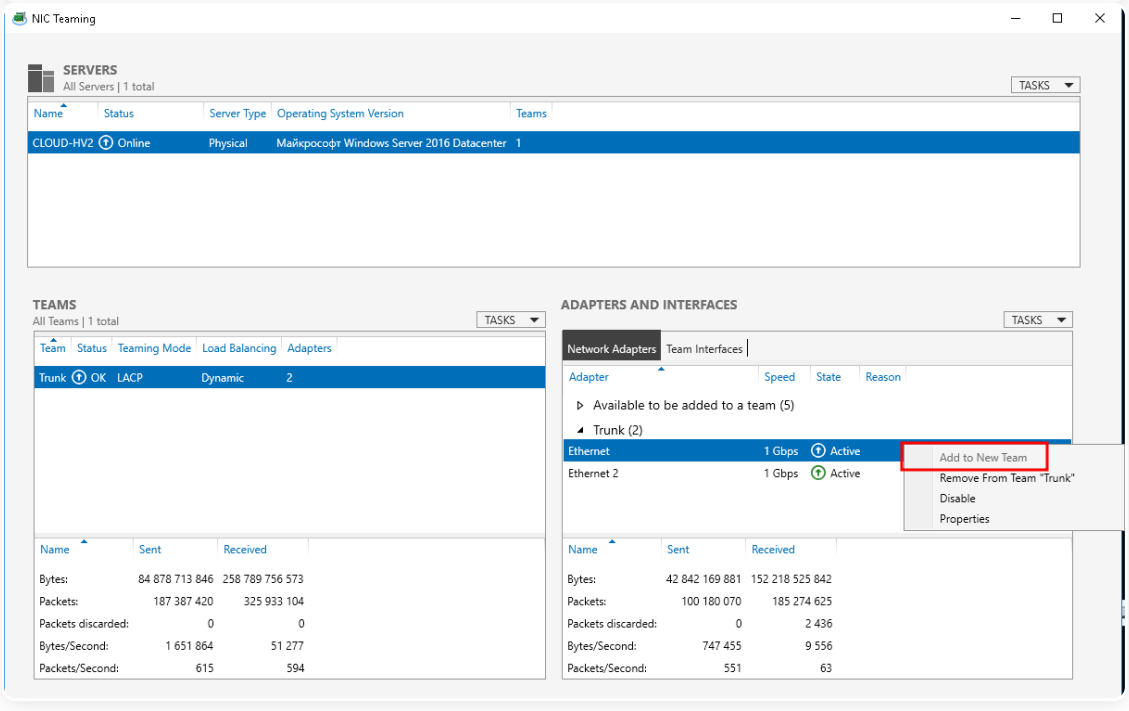
Настройка LACP в Hyper-V

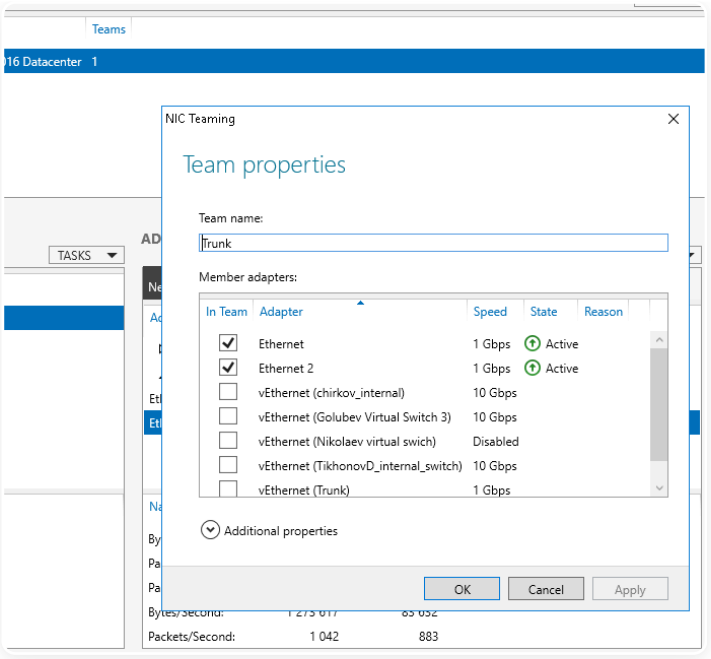
Для настройки LACP в гипервизоре Hyper-V существуют два способа:

Настройка на хост системе

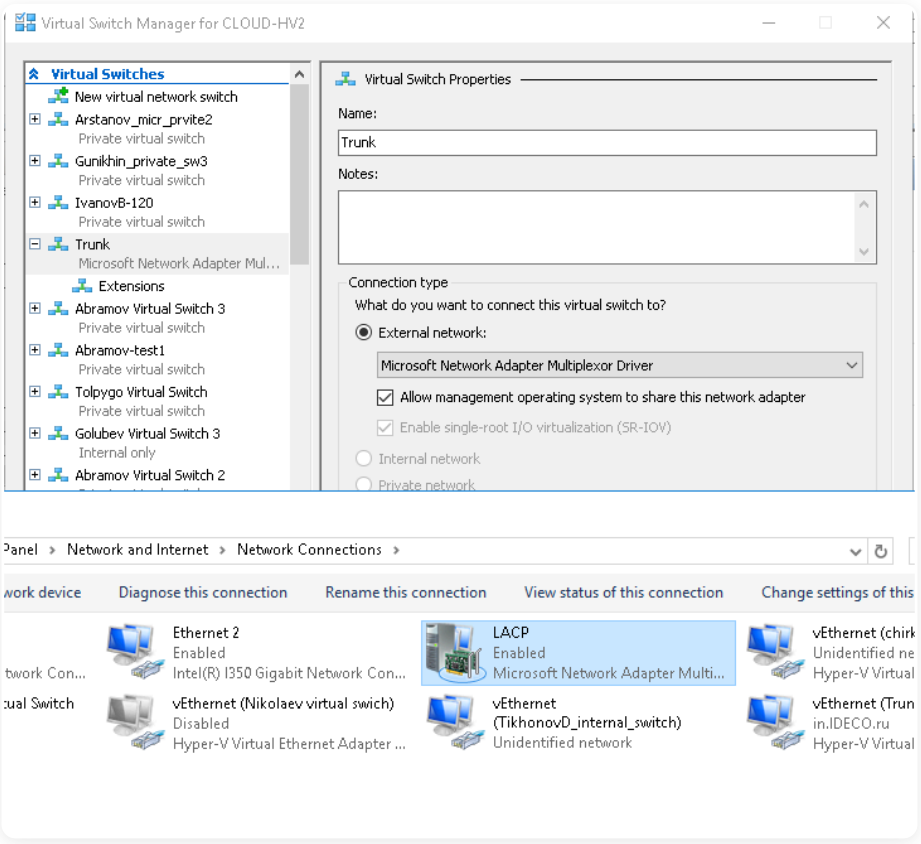
1. Объедините физические интерфейсы:







2. Выберите созданный интерфейс при настройке виртуального свитча:



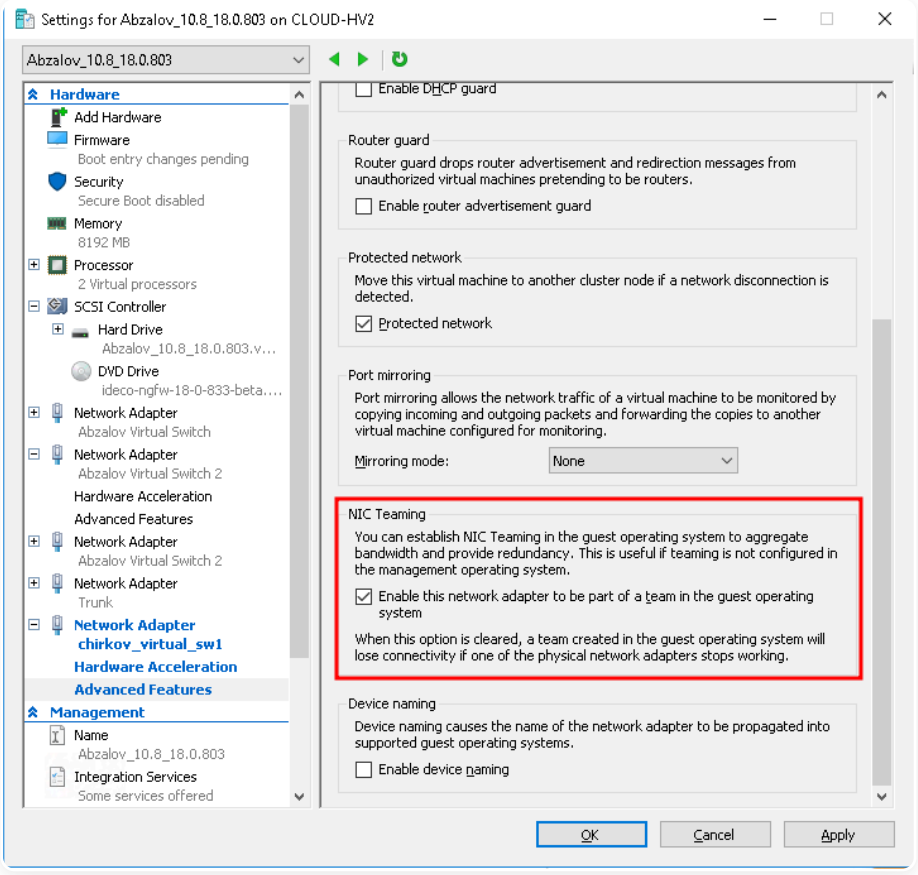
Получившийся виртуальный свитч можно использовать для добавления новых интерфейсов в LACP на гостевую систему.

3. Настройте подключение в **Сетевые интерфейсы → Внешние и локальные** для вновь созданного LACP-интерфейса, как для обычного сетевого интерфейса NGFW.

Настройка на гостевой системе

1. Добавьте необходимое количество интерфейсов на гостевую систему, на основе виртуального свитча, например, с названием **Virtual Switch 1**.

2. На каждом добавляемом интерфейсе включите опцию NIC Teaming:



3. Добавьте вновь созданные интерфейсы в LACP-интерфейсы NGFW в **Сетевые интерфейсы → Агрегированные(LACP)**.

4. Настройте подключения в **Сетевые интерфейсы → Внешние и локальные**.

Полезные ссылки

- **Настройка гипервизора**
- **Интерфейсы**

IPsec

Практические руководства по подключению устройств к Ideco NGFW по IPsec

Подключение между двумя Ideco NGFW в туннельном режиме работы

Перейти >

Подключение между двумя Ideco NGFW в транспортном режиме работы

Перейти >

Подключение Ideco NGFW и Mikrotik по IPsec в туннельном режиме

Перейти >

Подключение Ideco NGFW и Mikrotik по IPsec в транспортном режиме

Перейти >

Подключение MikroTik и Ideco NGFW по L2TP/IPsec

Перейти >

Подключение Cisco IOS и Ideco NGFW по IPsec в туннельном режиме

Перейти >

Подключение Cisco IOS и Ideco NGFW по IPsec в транспортном режиме

Перейти >

Подключение Cisco IOS и Ideco NGFW по route-based IPsec

Перейти >

Подключение pfSense к Ideco NGFW по IPsec

Перейти >

Подключение Kerio Control и Ideco NGFW по IPsec

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Подключение между двумя Ideco NGFW Novum в туннельном режиме работы

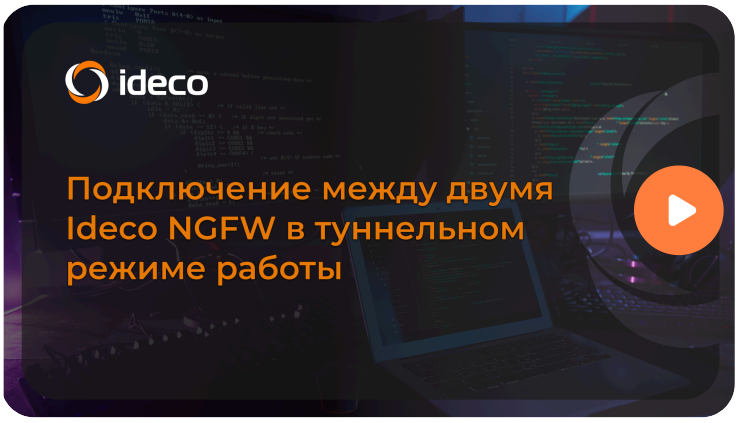
Функциональность доступна в **Классическом** и **Системном контекстах**.

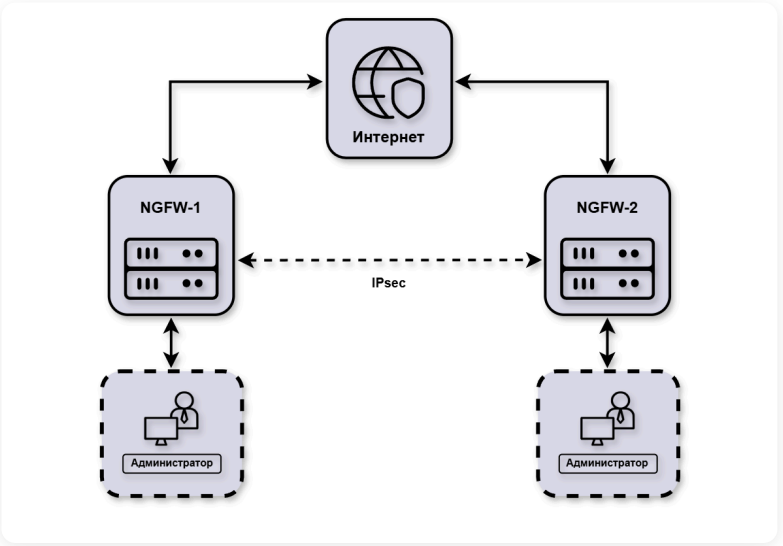
Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео





Для создания IPsec-подключения между Ideco NGFW Novum нужно настроить на одном NGFW Novum входящее подключение, а на другом NGFW Novum - исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключение, а на **NGFW-2** - входящее подключение.

Шаг 1. Проверка условий подключения

Перед созданием подключения убедитесь, что:

- На **NGFW-1** и **NGFW-2 правильно настроены временные зоны**. Без этого подключение не установится.
- Для работы IPsec все подсети, участвующие в соединениях, не пересекаются.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. **Входящее подключение должно настраиваться на сервере с белым IP-адресом**.
- Пользовательские правила из раздела **Правила трафика** → **Межсетевой экран** → **INPUT** не блокируют входящий трафик для протоколов ESP и UDP (порты 500 и 4500), поступающий на внешние интерфейсы **NGFW-2**.
- Сети для VPN-подключений у **NGFW-1** и **NGFW-2** не пересекаются.

Шаг 2. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в **Сервисы → IPsec → Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:

Добавление подключения

Название подключения

Зона

Режим работы

- Туннельный
  VTI
- Транспортный
  GRE over IPsec

Адрес удалённого устройства

Домен или IP-адрес

Интерфейс подключения

IP-адрес интерфейса туннеля

Заполните для проверки доступности сетей за удалённым NGFW Novum. Пример: 10.100.0.1/16.

Удалённый IP-адрес туннеля

Укажите IP-адрес интерфейса и удалённый IP-адрес туннеля для сбора статистики (потери, задержка, джиттер). Адреса должны быть в одной подсети.

IPsec-политики

- [x] Автоматическое создание маршрутов
  При выборе подсети 0.0.0.0/0 маршрут создаваться не будет

Домашние локальные сети

Удалённые локальные сети

Тип аутентификации

- Сертификат
  Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
- PSK
  Обеспечивает низкий уровень безопасности, поддерживается большинством устройств

Запрос на подпись сертификата

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBuAIBADBWMQ4wDAYDVQQKDAVJZG
VjbzEMMAoGA1UECwwDVVRNMTYwNAYD
```

Подписанный сертификат NGFW Novum

Загрузить

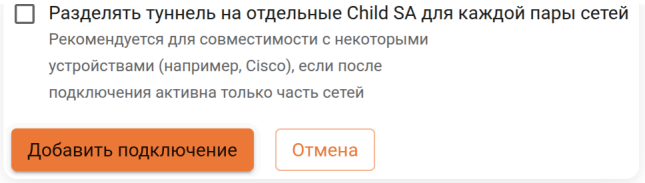
Корневой сертификат удалённого устройства

Загрузить

Дополнительно

Индекс интерфейса для Netflow

0



Расшифровка полей

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW Novum или белый IP-адрес другого Ideco NGFW Novum. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля:
  - При настройке BGP-соседства для динамической маршрутизации и сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**:
  - Для сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW Novum.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW Novum или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW Novum.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW Novum.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните сертификат для настройки входящего подключения.
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните ключ для настройки входящего подключения. Заполните поле **Идентификатор UTM**.

> Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.
>
> Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно настроить статические маршруты до удаленных локальных сетей NGFW в **Сервисы → Маршрутизация** или динамическую маршрутизацию через BGP в **Сервисы → BGP**.

3. Выполните действие для нужного типа аутентификации:

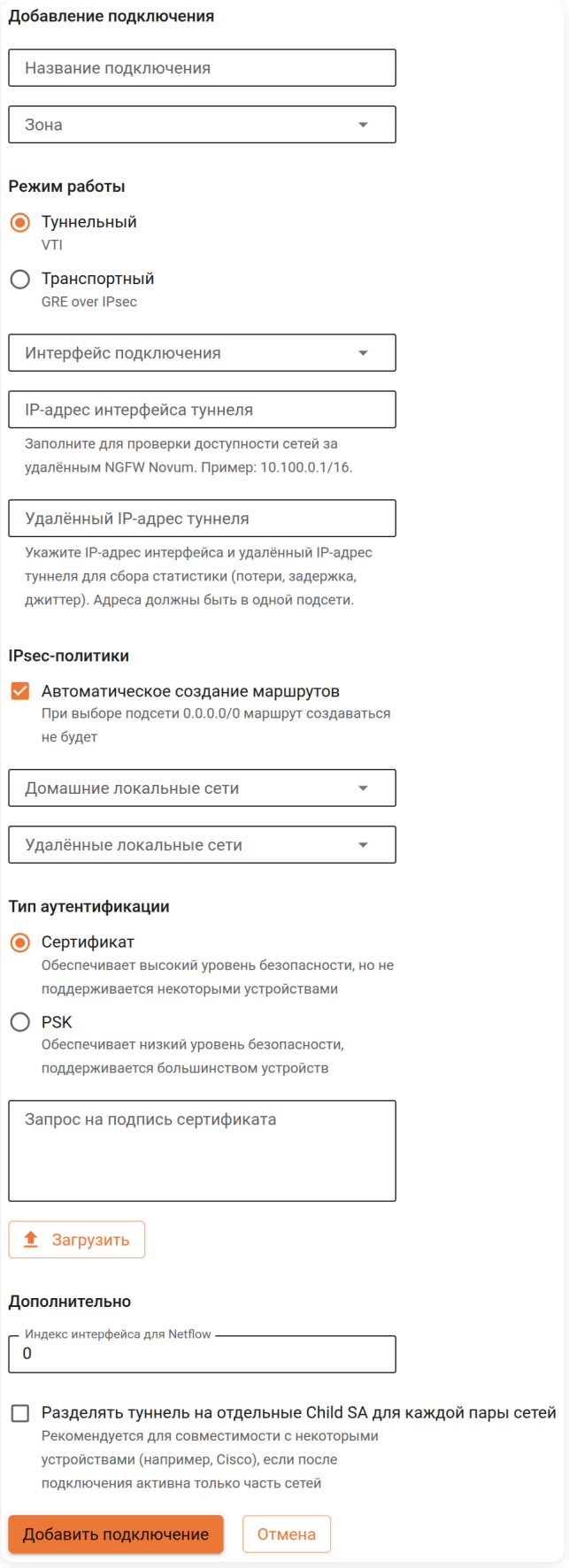
- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 3**.
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 3** для настройки входящего подключения на **NGFW-2**.

Шаг 3. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в **Сервисы → IPsec → Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля:
  - При настройке BGP-соседства для динамической маршрутизации и сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**:
  - Для сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW Novum.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW Novum или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW Novum.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW Novum.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - **Сертификат** - заполните поле **Запрос на подпись сертификата**, вставив значение сохраненное при первоначальной настройке исходящего подключения.
  - **PSK** - заполните поле **PSK ключ**, вставив значение сохраненное при первоначальной настройке исходящего подключения. Заполните поле **Идентификатор удаленной стороны**.

> Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно настроить статические маршруты до удаленных локальных сетей NGFW Novum в **Сервисы** → **Маршрутизация** или динамическую маршрутизацию через BGP в **Сервисы** → **BGP**.

3. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

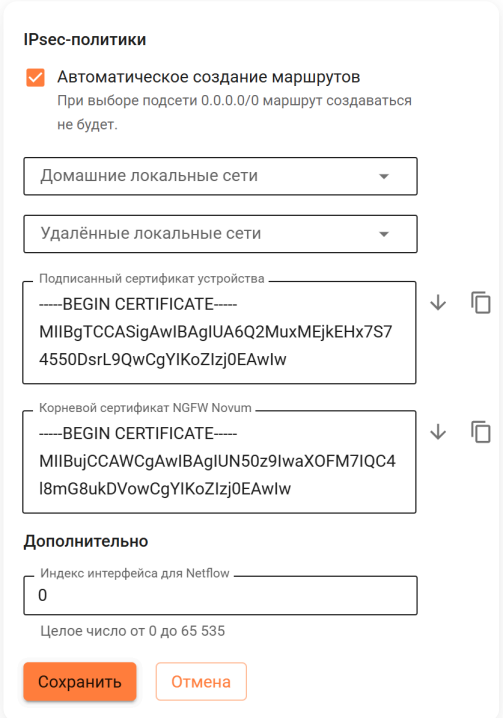
Если был выбран тип аутентификации **PSK**, то настройка завершена.

Если был выбран тип аутентификации **Сертификат**, то выполните **Шаг 4**.

Шаг 4. Донастройка исходящего подключения с типом аутентификации Сертификат

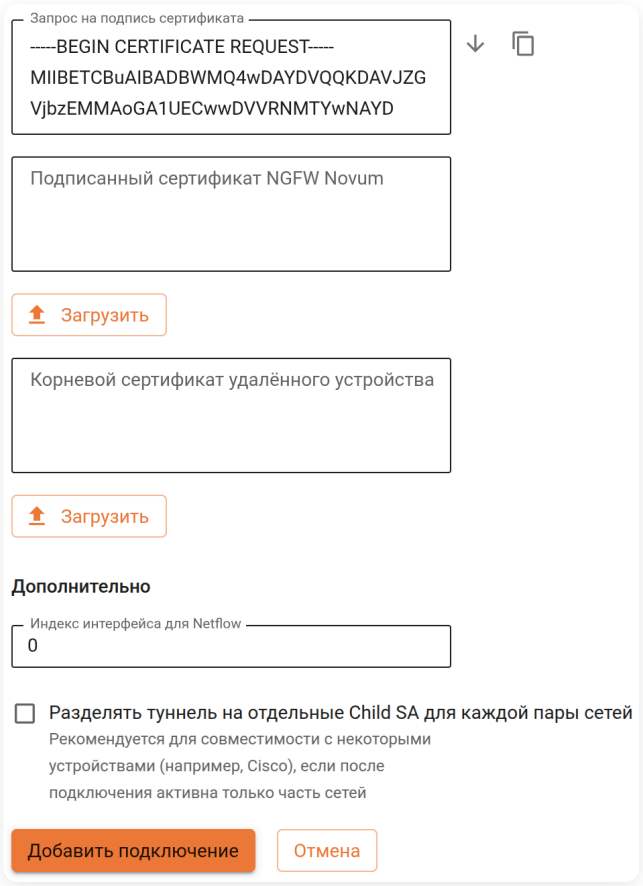
1. В **NGFW-2** перейдите в **Сервисы** → **IPsec** → **Входящие подключения** и нажмите  по ранее созданному входящему подключению.

2. Скопируйте поля **Подписанный сертификат устройства** и **Корневой сертификат NGFW**:



3. В **NGFW-1** перейдите в **Сервисы** → **IPsec** → **Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** значениями, ранее скопированными из **NGFW-2**:



5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

> Если соединение по IPsec не устанавливается, воспользуйтесь статьей.

Настройка доступа к локальным сетям по VPN из NGFW-1 к NGFW-2

Для доступа к локальным сетям по VPN из **NGFW-1** к **NGFW-2** выполните действия:

1. Перейдите к редактированию настроенного IPsec-подключения на **NGFW-2**.

2. Укажите в поле **Домашние локальные сети** сеть, используемую для VPN в **NGFW-2**.

> В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение между двумя Ideco NGFW Novum в транспортном режиме работы

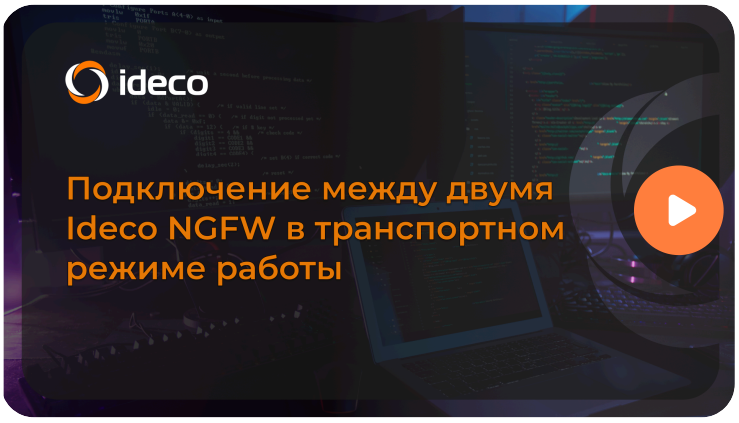
Функциональность доступна в **Классическом** и **Системном контекстах**.

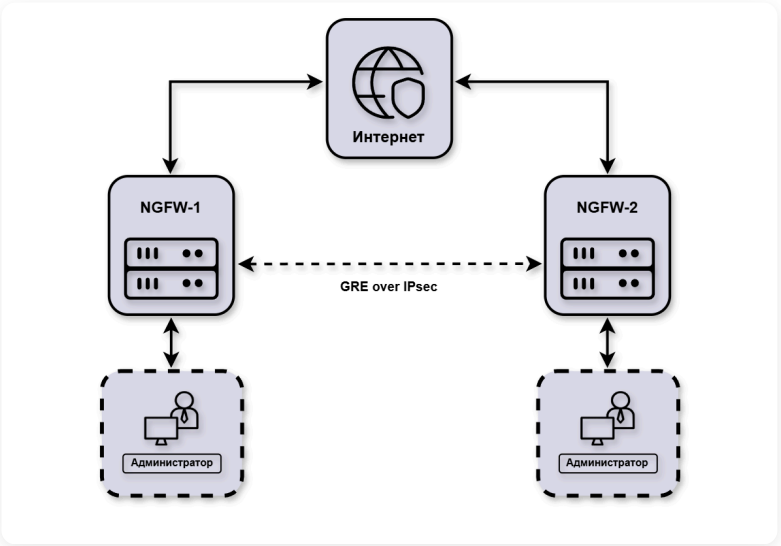
Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео





GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

При замене/перевыпуске корневого сертификата в разделе Сертификаты, IPsec-подключения перестанут работать и необходимо будет пересоздать.

Перед настройкой убедитесь, что:

- В каждой из подключаемых сторон **правильно настроена временная зона**. Без этого установить подключение невозможно.
- Пользовательские правила из раздела **Правила трафика** → **Межсетевой экран** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW Novum для протоколов ESP и UDP (порты 500 и 4500).
- Пользовательские правила из раздела **Правила трафика** → **Межсетевой экран** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW Novum для протокола GRE.
- Ни один Ideco NGFW Novum не находится за NAT, так как в таком случае подключение двух Ideco NGFW Novum в транспортном режиме недоступно.
- Все IP-подсети, участвующие в соединениях не должны пересекаться и, тем более, не должны совпадать.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. Входящее подключение должно настраиваться на сервере с белым IP-адресом.

- Сети для VPN-подключений у двух NGFW не пересекаются.

Для создания IPsec подключения между Ideco NGFW Novum нужно настроить на одном NGFW входящее подключение, а на другом NGFW исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключение, а на **NGFW-2** входящее подключение.

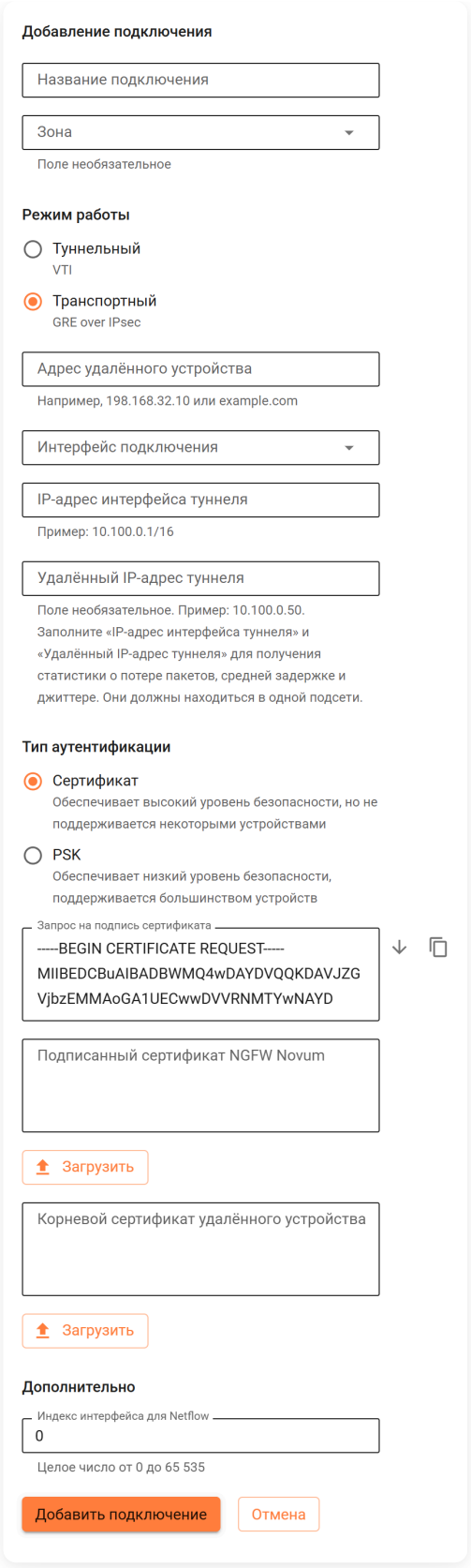
Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

Шаг 1. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в **Сервисы** → **IPsec** → **Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Название подключения** - максимальное количество символов 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW Novum или белый IP-адрес другого Ideco NGFW Novum. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните его для настройки входящего подключения.
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните его для настройки входящего подключения. Заполните поле **Идентификатор NGFW**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Если тип аутентификации:

- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 2**.
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 2** для настройки входящего подключения на другом NGFW.



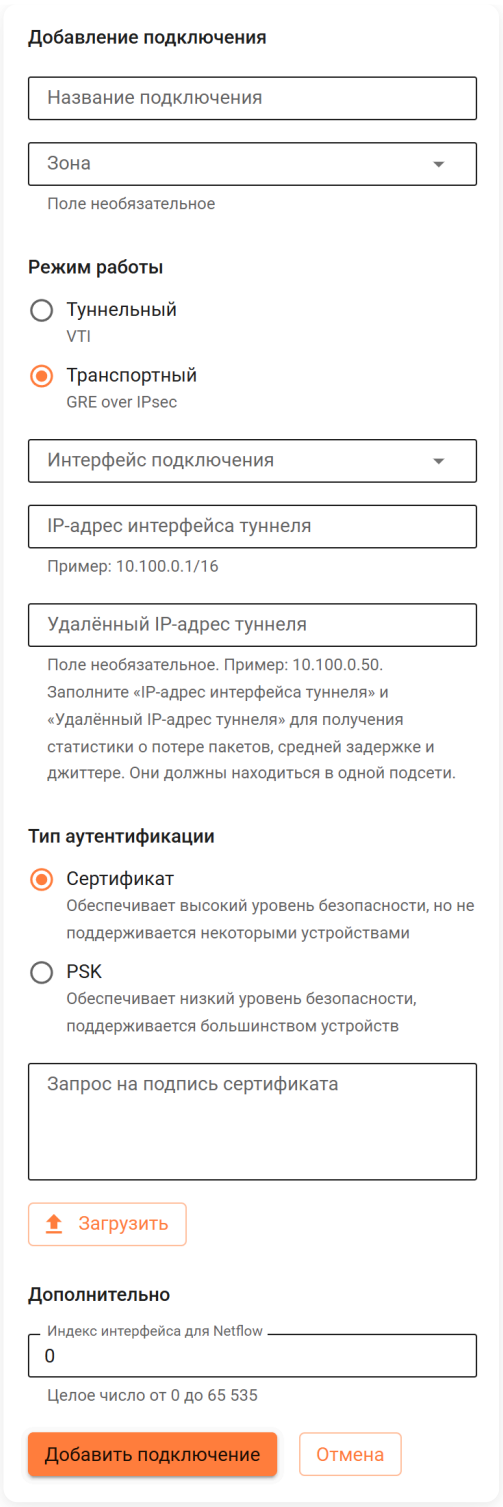
В поле **Интерфейс подключения** при выборе Loopback-интерфейса обеспечьте сетевой доступ к IP-адресу этого интерфейса настройками маршрутизации.

Шаг 2. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в **Сервисы** → **IPsec** → **Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - **Сертификат** - заполните поле **Запрос на подпись сертификата**, вставив значение сохраненное при первоначальной настройке исходящего подключения.
  - **PSK** - заполните поле **PSK ключ**, вставив значение сохраненное при первоначальной настройке исходящего подключения.Заполните поле **Идентификатор удаленной стороны**.

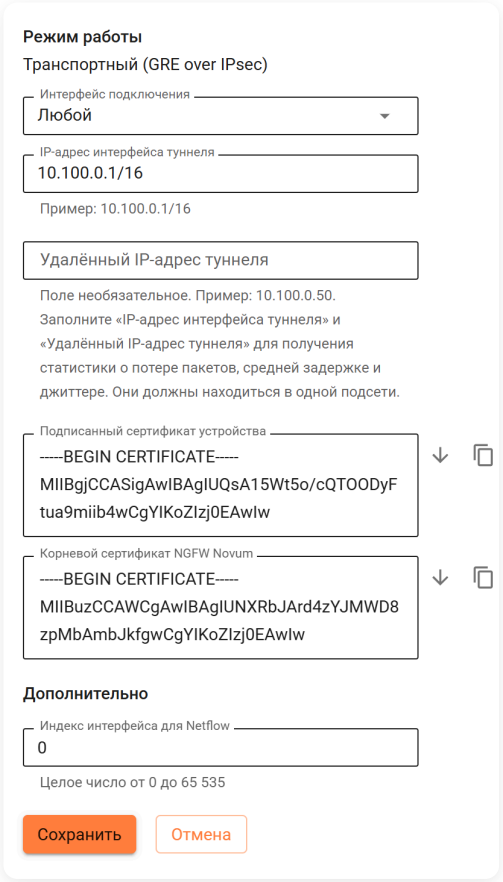
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Шаг 3. Донастройка исходящего подключения с типом аутентификации Сертификат

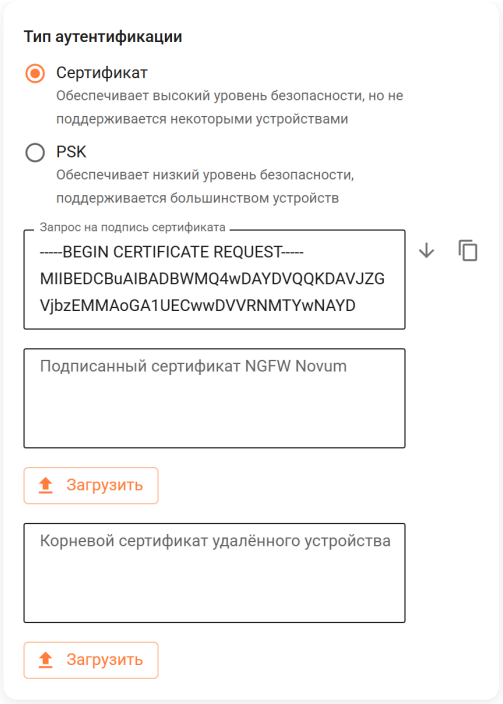
1. В **NGFW-2** перейдите в **Сервисы** → **IPsec** → **Входящие подключения** и нажмите по ранее созданному входящему подключению.

2. Скопируйте поля **Подписанный сертификат устройства** и **Корневой сертификат NGFW**:



3. В **NGFW-1** перейдите в **Сервисы** → **IPsec** → **Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** ранее скопированным значением при редактировании входящего подключения:



5. Нажмите **Сохранить**.

Шаг 4. Настройка маршрутизации

Маршрутизацию можно настроить тремя способами:

- Статические маршруты до локальных сетей удаленного NGFW в разделе **Сервисы** → **Маршрутизация**.
- Динамическая маршрутизация через BGP в разделе **Сервисы** → **BGP**.
- Динамическая маршрутизация через OSPF в разделе **Сервисы** → **OSPF**.

Рекомендуем для настройки маршрутизации использовать OSPF, в этом случае нет необходимости вручную настраивать маршруты до локальных сетей филиалов.

Также настройками OSPF можно определить приоритет направления трафика для резервирования каналов при создании нескольких IPSec-подключений.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Ideco NGFW Novum и MikroTik по IPsec в туннельном режиме

Функциональность доступна в **Классическом** и **Системном контекстах**.

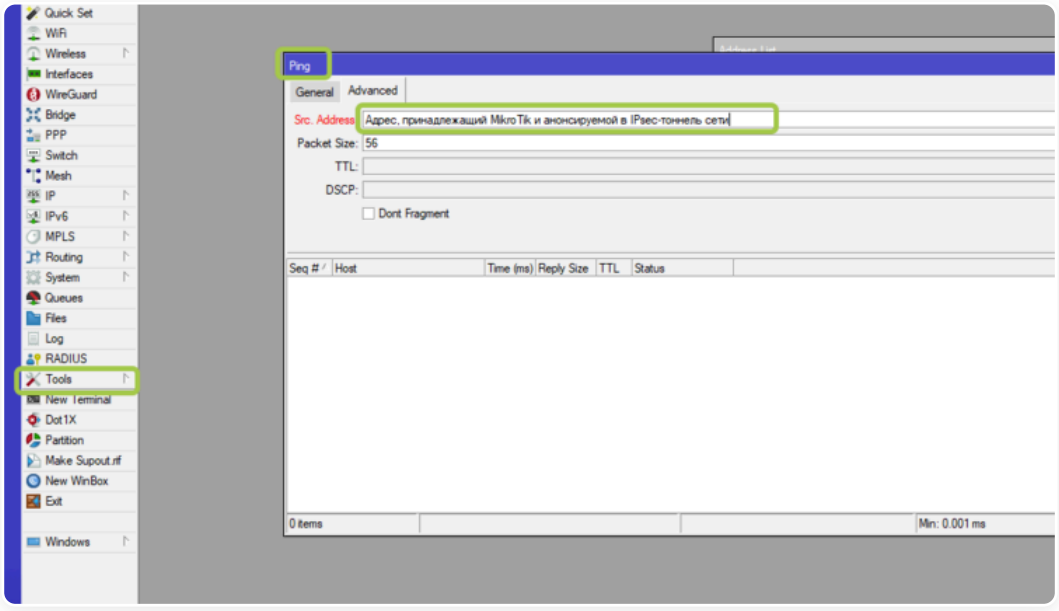
В статье описана настройка IPsec-подключения между Ideco NGFW Novum и MikroTik с аутентификацией по сертификатам или PSK. Локальные сети в разных офисах не должны пересекаться.

Требования и подготовка

Основные требования:

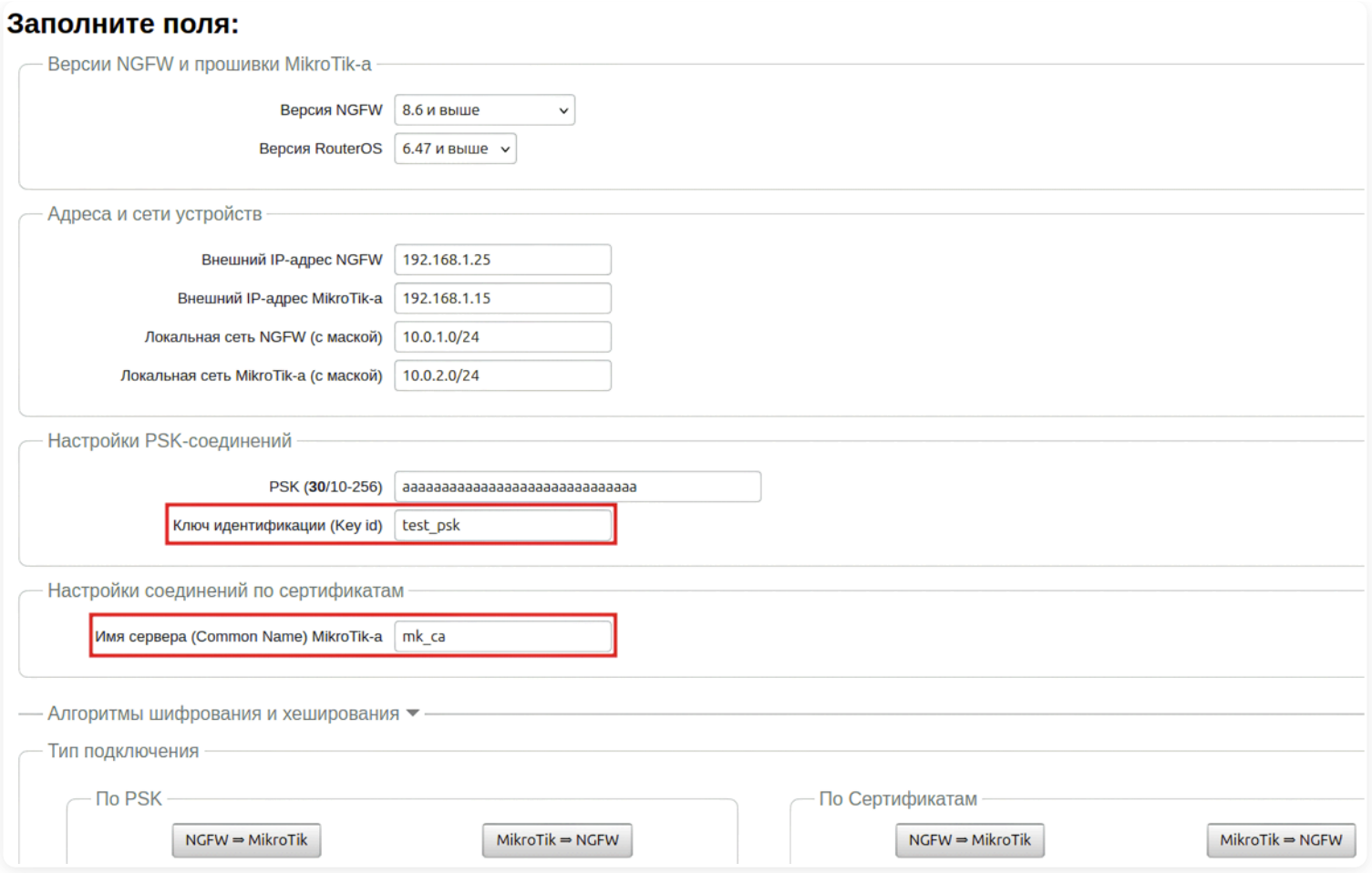
- Локальные сети в разных офисах не должны пересекаться.
- Для корректной работы подключений по сертификатам убедитесь, что время на Ideco NGFW Novum и MikroTik совпадает. Расхождение времени между устройствами приведет к ошибкам аутентификации. Рекомендуется настроить NTP-клиент на каждом из устройств.
- IPsec-подключения от Ideco NGFW Novum к MikroTik версии 6.45 и ниже по сертификатам не работают, так как нельзя использовать современные криптоалгоритмы.

Для проверки доступности анонсируемых сетей Ideco NGFW Novum с MikroTik указывайте IP-адрес источника:



При подключении нескольких устройств MikroTik к одному Ideco NGFW Novum **в туннельном режиме** через конфигуратор скриптов для MikroTik рекомендуем:

- Для PSK - укажите разные **Идентификаторы ключа (key-id)** для каждого устройства.
- Для сертификатов - укажите разные **Имена сервера (Common Name)** для каждого устройства:



Подключение от Ideco NGFW Novum к MikroTik

Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

Шаг 1. Настройка Ideco NGFW Novum (исходящее подключение)

Сгенерируйте запрос на подпись сертификата:

1. В Ideco NGFW Novum откройте **Сервисы** → **IPsec** → **Исходящие подключения**, нажмите **Добавить** и заполните поля:

Добавление подключения

Название подключения

Зона

Режим работы

- Туннельный
  VTI
- Транспортный
  GRE over IPsec

Адрес удалённого устройства

Домен или IP-адрес

Интерфейс подключения

IP-адрес интерфейса туннеля

Заполните для проверки доступности сетей за удалённым NGFW Novum. Пример: 10.100.0.1/16.

Удалённый IP-адрес туннеля

Укажите IP-адрес интерфейса и удалённый IP-адрес туннеля для сбора статистики (потери, задержка, джиттер). Адреса должны быть в одной подсети.

IPsec-политики

- [x] Автоматическое создание маршрутов
  При выборе подсети 0.0.0.0/0 маршрут создаваться не будет

Домашние локальные сети

Удалённые локальные сети

Тип аутентификации

- Сертификат
  Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
- PSK
  Обеспечивает низкий уровень безопасности, поддерживается большинством устройств

Запрос на подпись сертификата

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBuAIBADBWMQ4wDAYDVQQKDAVJZG
VjbzEMMAoGA1UECwwDVVRNMTYwNAYD
```

Подписанный сертификат NGFW Novum

Загрузить

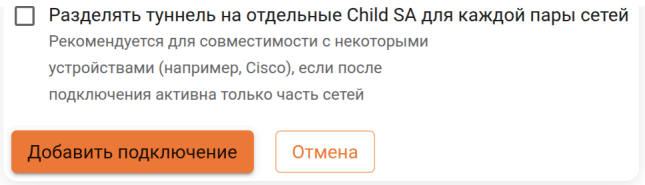
Корневой сертификат удалённого устройства

Загрузить

Дополнительно

Индекс интерфейса для Netflow

0



Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - укажите внешний IP-адрес MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **Сертификат**.
- **Запрос на подпись сертификата** - будет сгенерирован **запрос, который необходимо отправить для подписи на MikroTik**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. После подписания запроса необходимо продолжить настройку подключения в Ideco NGFW Novum.

> **Не закрывайте вкладку с настройками.** При закрытии вкладки **Запрос на подпись сертификата** изменит значение и процесс подписания файла **NGFW.csr** потребуется повторить.

Шаг 2. Настройка MikroTik (входящее подключение)

Файл **NGFW.csr**, полученный из Ideco NGFW Novum, необходимо загрузить в файловое хранилище MikroTik:

1. Откройте раздел **File**.

2. Нажмите кнопку **Browse**.

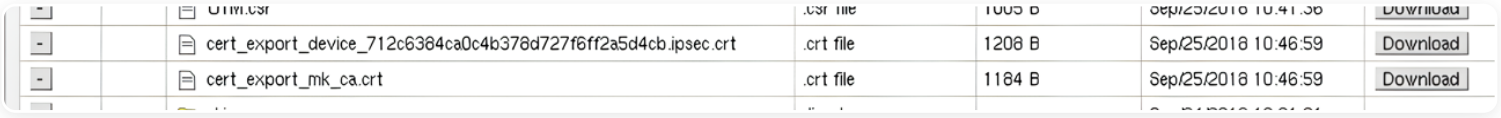
3. Выберите и загрузите файл.

Настроить MikroTik можно через:

- GUI.
- Консоль устройства.
- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт. Вставьте в скрипт код, сгенерированный конфигуратором, затем запустите.

В файловой системе MikroTik появятся два файла, которые необходимо скачать, чтобы впоследствии загрузить на NGFW:



Файл `cert_export_device_<случайный набор символов>.ipsec.crt` - подписанный сертификат NGFW.

Файл `cert_export_mk_ca.crt` - корневой сертификат MikroTik.

Шаг 3. Завершение настройки Ideco NGFW Novum

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW Novum.

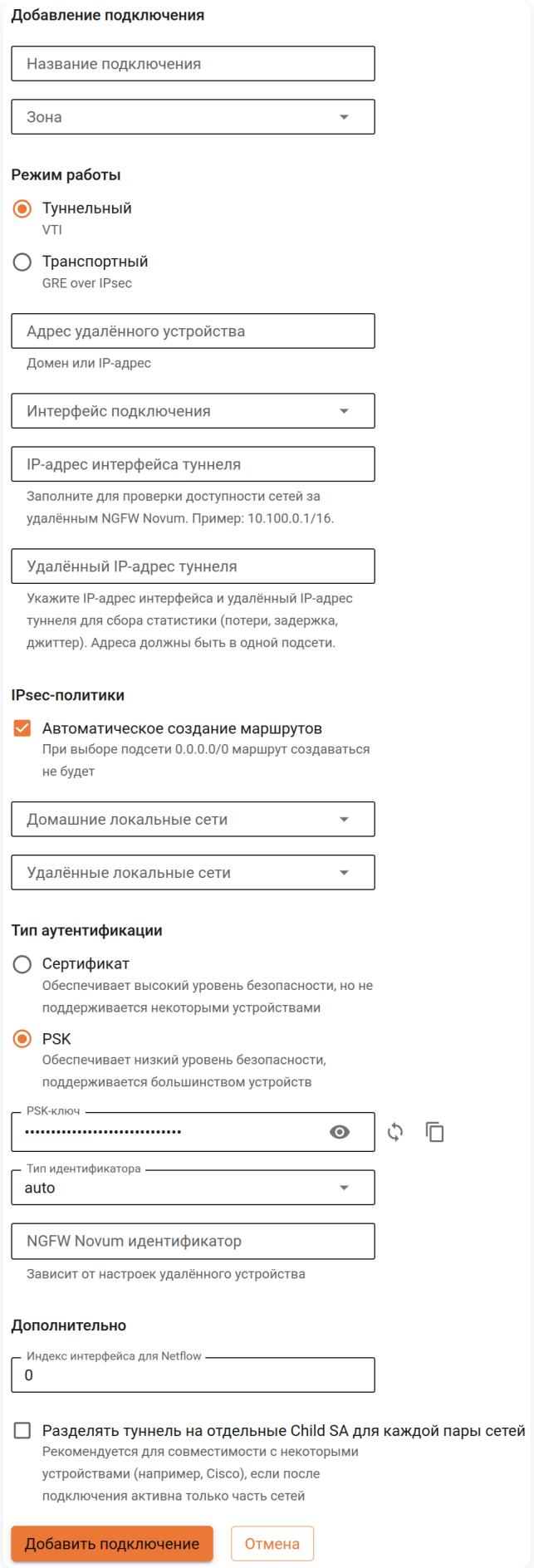
1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

PSK

Шаг 1. Настройка Ideco NGFW Novum (исходящее подключение)

1. Откройте **Сервисы** → **IPsec** → **Исходящие подключения**, нажмите **Добавить** и заполните поля:

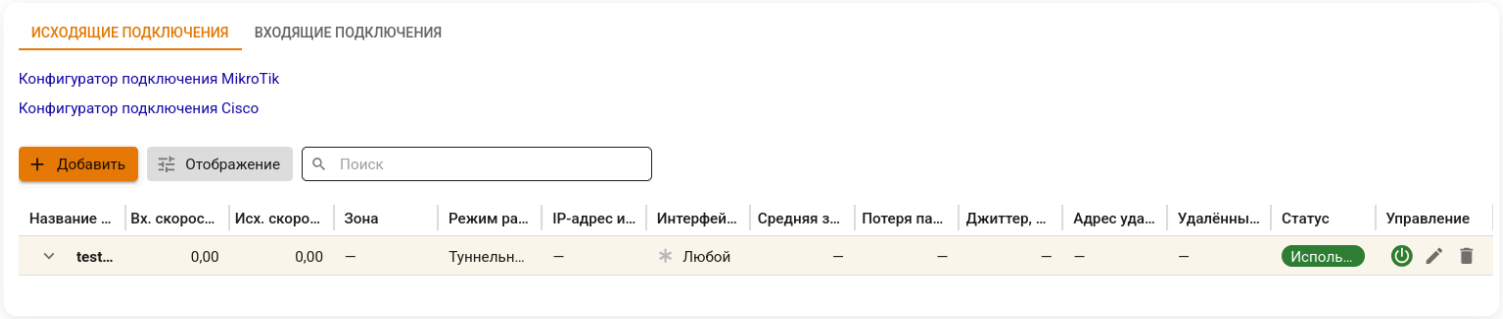


Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.

- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - укажите внешний IP-адрес MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **PSK**. В поле **PSK-ключ** будет сгенерирован случайный PSK-ключ для настройки подключения в MikroTik.
- **Тип идентификатора** - выберите **auto**.
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего IPsec-подключения в MikroTik.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. После заполнения всех полей нажмите **Добавить подключение**. В списке подключений появится созданное подключение:



Шаг 2. Настройка MikroTik (входящее подключение)

Настроить MikroTik можно через:

- GUI.
- Консоль устройства.
- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт. Вставьте в скрипт код, сгенерированный конфигуратором, и запустите.

Подключение от MikroTik к Ideco NGFW Novum

Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

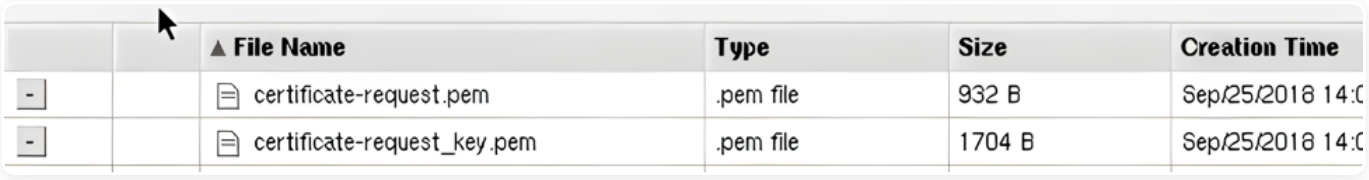
Шаг 1. Предварительная настройка MikroTik

Настроить MikroTik можно через:

- GUI.
- Консоль устройства.
- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт для генерации запроса на подпись сертификата. Вставьте в скрипт код, сгенерированный конфигуратором, и запустите. Конфигуратором генерируется два скрипта, поэтому в MikroTik также создайте два скрипта.

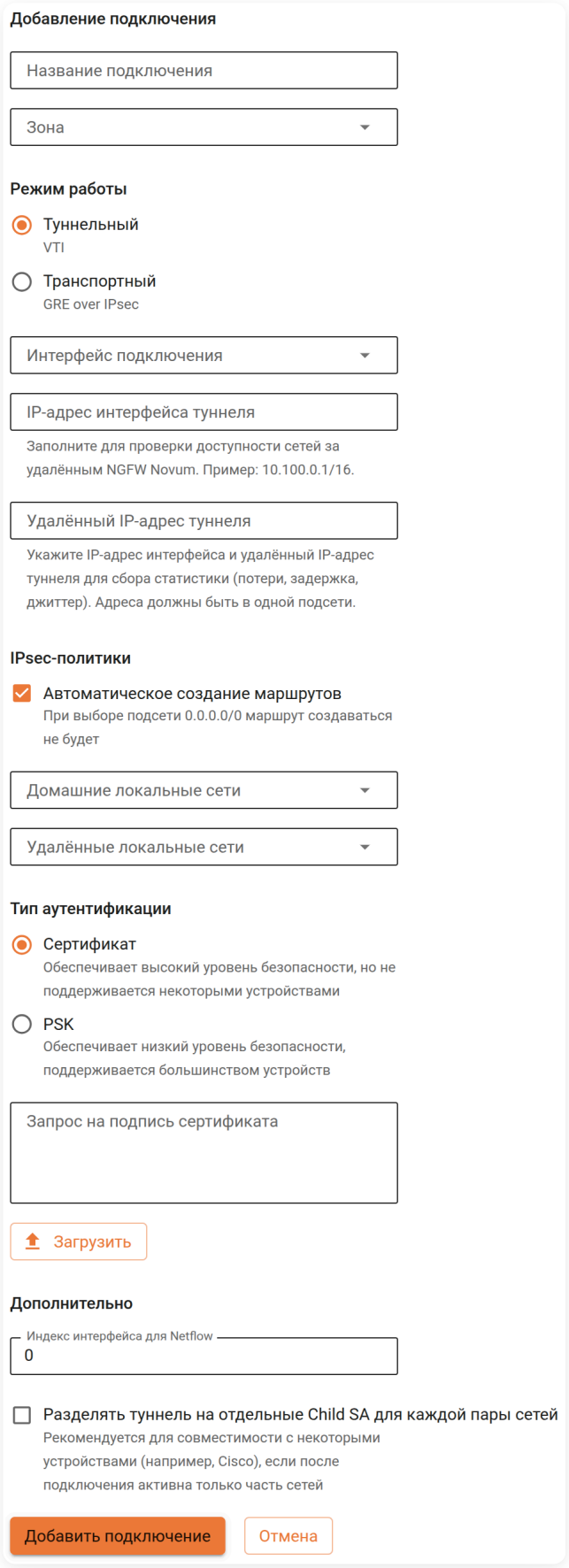
Перед настройкой необходимо запустить первый скрипт для запроса на подпись сертификата. После чего в файловом хранилище MikroTik появятся два файла, которые необходимо скачать. Файлы потребуются для дальнейшей настройки:



- Файл `certificate-request.pem` - запрос на подпись сертификата.
- Файл `certificate-request_key.pem` - приватный ключ.

Шаг 2. Настройка Ideco NGFW Novum (входящее подключение)

1. В Ideco NGFW Novum откройте **Сервисы** → **IPsec** → **Входящие подключения**, нажмите **Добавить** и заполните поля:

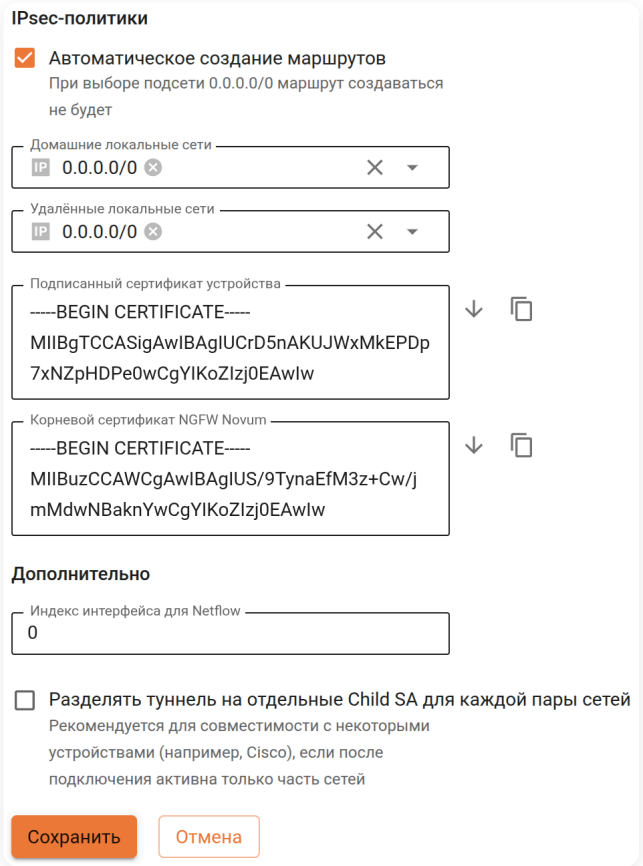


Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону, в которую требуется добавить IPsec-подключение. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **Сертификат**.
- **Запрос на подпись сертификата** - загрузите запрос на подпись, **полученный от MikroTik**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Нажмите кнопку **Добавить подключение**. Нажмите на кнопку редактирования соединения ( ), чтобы продолжить настройку.

3. Откройте созданное IPsec-соединение, нажав на , и скачайте файлы **Подписанного сертификата устройства** (`device.crt`) и **Корневого сертификата NGFW** (`NGFW.crt`):



Шаг 3. Настройка MikroTik (исходящее подключение)

1. Загрузите на MikroTik скачанные ранее файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`) через WinBox или по SSH.

2. Запустите второй сгенерированный конфигуратором скрипт.

PSK

Шаг 1. Настройка MikroTik (исходящее подключение)

Настроить устройство MikroTik можно через:

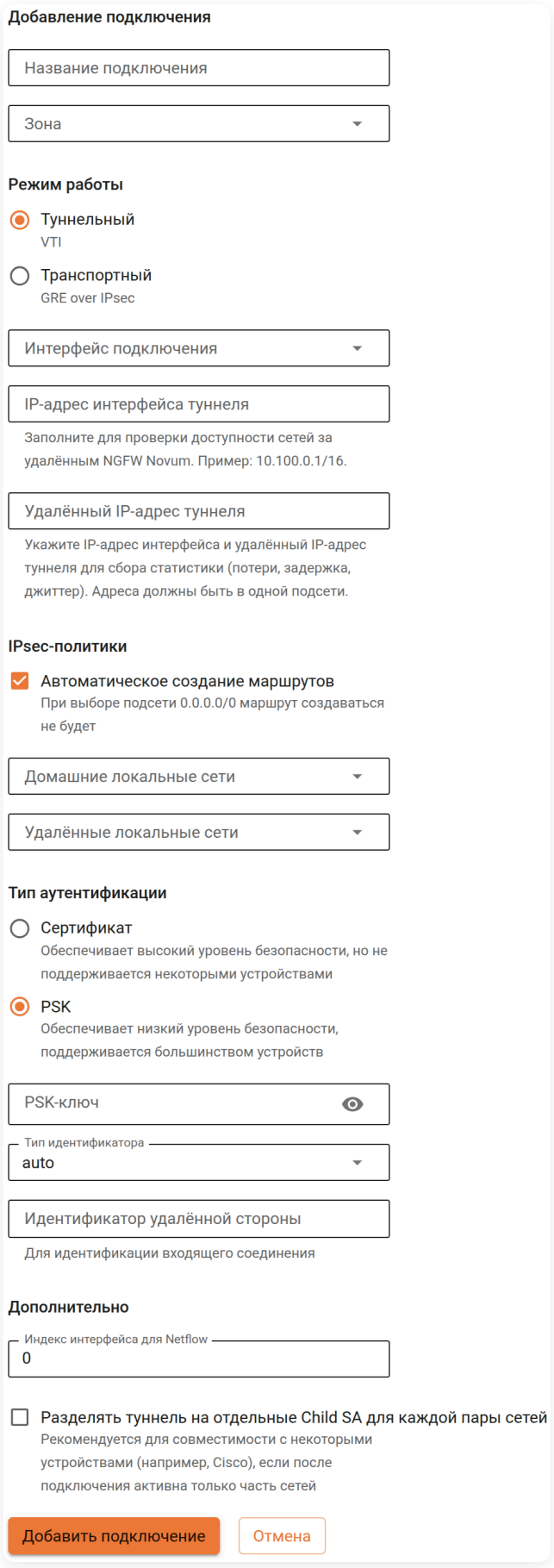
- GUI.
- Консоль устройства.

- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт. Вставьте в скрипт код, сгенерированный конфигуратором, и запустите.

Шаг 2. Настройка Ideco NGFW Novum (входящее подключение)

1. В Ideco NGFW Novum откройте **Сервисы** → **IPsec** → **Входящие подключения**, нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - вставьте PSK-ключ, полученный от MikroTik.
- **Тип идентификатора** - выберите **keyid**.
- **Идентификатор удаленной стороны** - вставьте идентификатор MikroTik (параметр key-id в `/ip ipsec peers`).
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Нажмите кнопку **Добавить подключение**.

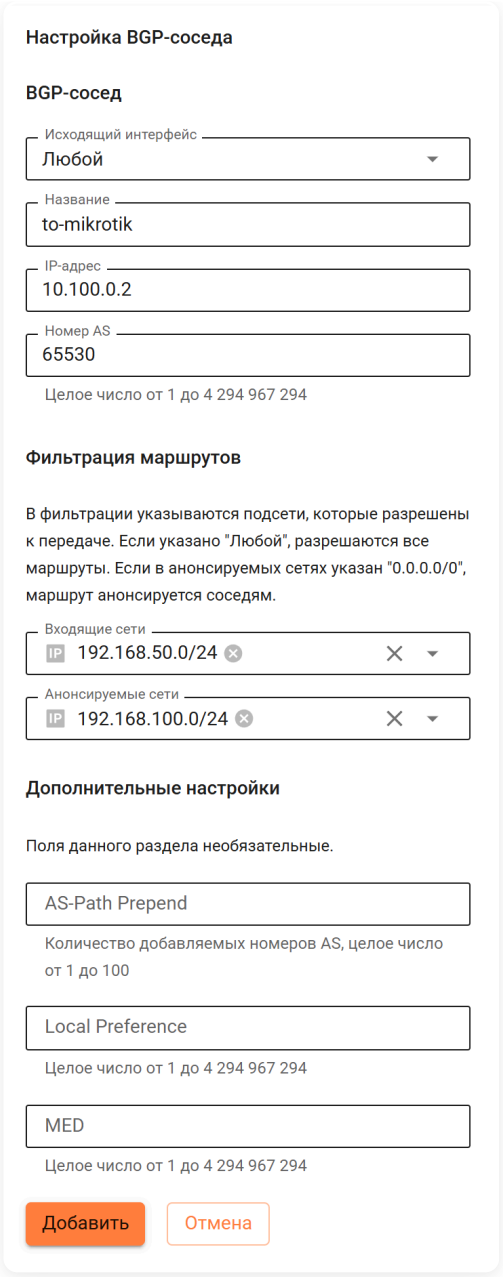
Настройка динамической маршрутизации (BGP)

Настройка Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в поле **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:



Расшифровка полей

- **Исходящий интерфейс** - выберите **Любой**.
- **Название** - любое значение.
- **IP-адрес** - укажите IP-адрес интерфейса туннеля MikroTik.
- **Номер AS** - номер автономной системы MikroTik.
- **Входящие сети** - укажите локальные сети MikroTik.
- **Анонсируемые сети** - укажите локальные сети Ideco NGFW Novum.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

5. Включите модуль **BGP**.

Настройка MikroTik

1. Настройте общий шаблон BGP:

```
/routing bgp template set default address-families=ip disabled=no output.default-originate=always router-id=<Router-ID MikroT
```

2. Добавьте BGP-сессию с Ideco NGFW Novum:

```
/routing bgp connection add address-families=ip as=<AS MikroTik> disabled=no local.role=ebgp-peer name=<Имя подключения> outp
```

Возможные проблемы

Соединение не устанавливается при повторной активации

Если после отключения VPN-подключение не восстанавливается, удаленное устройство заблокировано fail2ban. Сбросьте блокировки по IP на Ideco NGFW Novum. Подробнее в статье Защита от брутфорс-атак.

Fail2ban отслеживает в log-файлах попытки обратиться к сервисам и, если находит повторяющиеся неудачные попытки авторизации с одного и того же IP-адреса или хоста, блокирует IP-адрес.

Соединение периодически разрывается

При работе туннеля между Ideco NGFW Novum и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW Novum.

Для автоматизации процесса поддержания соединения создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW Novum:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в **System** → **Scripts**.

3. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



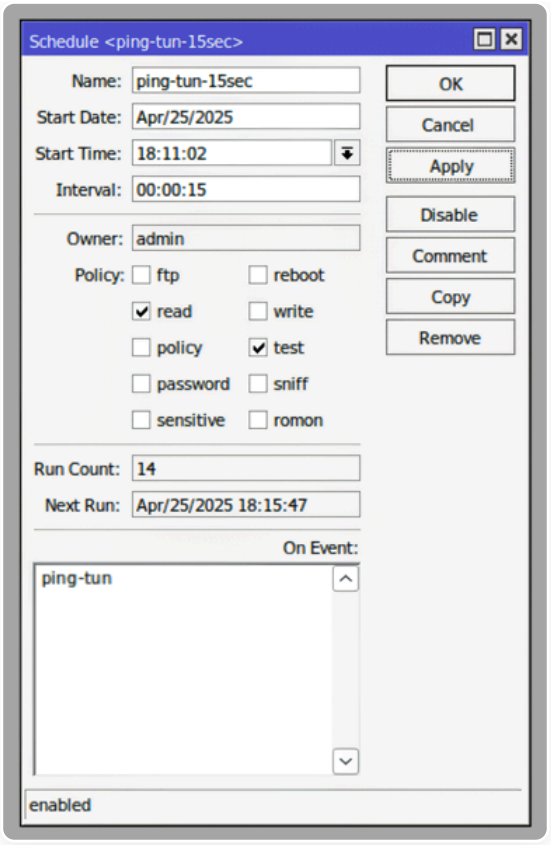
- **Name** - название скрипта (не поддерживаются пробелы и нижние подчеркивания).
- **Policy** - включите опции **read** и **test**.
- **Source** - введите команду `ping <IP-адрес Ideco NGFW Novum> count=3`.

4. Нажмите **Apply**, затем **Ok**.

Далее настройте запуск скрипта по расписанию в планировщике заданий:

1. Перейдите в **System** → **Scheduler**.

2. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



- **Name** - название задания (не поддерживаются пробелы и нижние подчеркивания).
- **Interval** - интервал 00:00:15 (каждые 15 секунд).
- **Policy** - включите опции **read** и **test**.
- **On Event** - введите название созданного ранее скрипта.

3. Нажмите **Apply**, затем **Ok**.

По завершению настройки MikroTik каждые 15 секунд будет отправлять три ICMP-запроса на адрес Ideco NGFW Novum. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Ideco NGFW Novum и MikroTik по IPsec в транспортном режиме

Функциональность доступна в **Классическом** и **Системном контекстах**.

При объединении сетей с помощью VPN локальные сети в разных офисах не должны пересекаться.

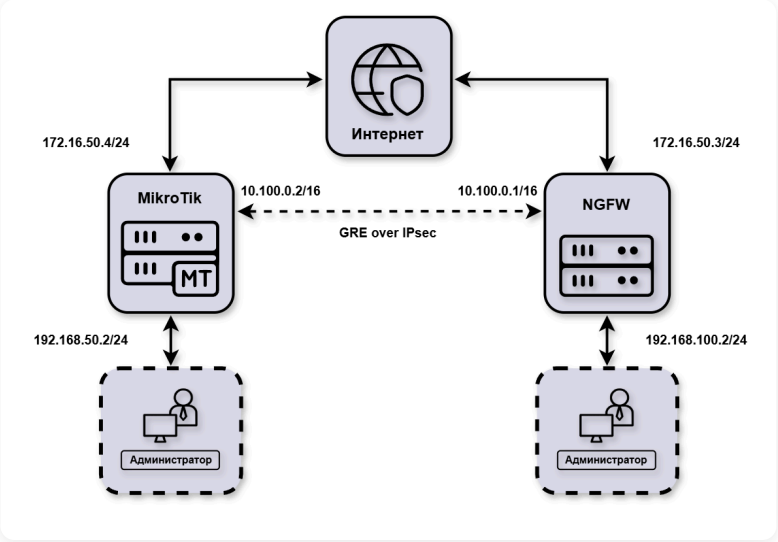
Для корректной работы подключений по сертификатам убедитесь, что время на Ideco NGFW Novum и MikroTik совпадает. Расхождение времени между устройствами приведет к ошибкам аутентификации. Рекомендуется настроить NTP-клиент на каждом из устройств.

IPsec-подключения от Ideco NGFW Novum к MikroTik по сертификатам к MikroTik версии 6.45 и ниже не работают, так как нельзя использовать современные криптоалгоритмы.

GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

Рассмотрим настройку подключения по схеме:



- `172.16.50.3/24` - внешний IP-адрес NGFW.
- `192.168.100.2/24` - локальный IP-адрес NGFW.
- `10.100.0.1/30` - IP-адрес GRE-туннеля NGFW.
- `172.16.50.4/24` - внешний IP-адрес MikroTik.
- `192.168.50.2/24` - локальный IP-адрес MikroTik.
- `10.100.0.2/30` - IP-адрес GRE-туннеля MikroTik.

Для настройки подключения MikroTik и Ideco NGFW Novum следуйте инструкции в каждом из пунктов.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

PSK-ключ

Для PSK-ключа допустимы все печатные ASCII-символы (коды от 0x20 до 0x7E), включая:

- **Латинские буквы в верхнем и нижнем регистре** (A–Z, a–z).
- **Цифры** (0–9).
- **Пробел и специальные символы** (! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ { | } ~).

Подключение от Ideco NGFW Novum к MikroTik

Предварительная настройка MikroTik

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

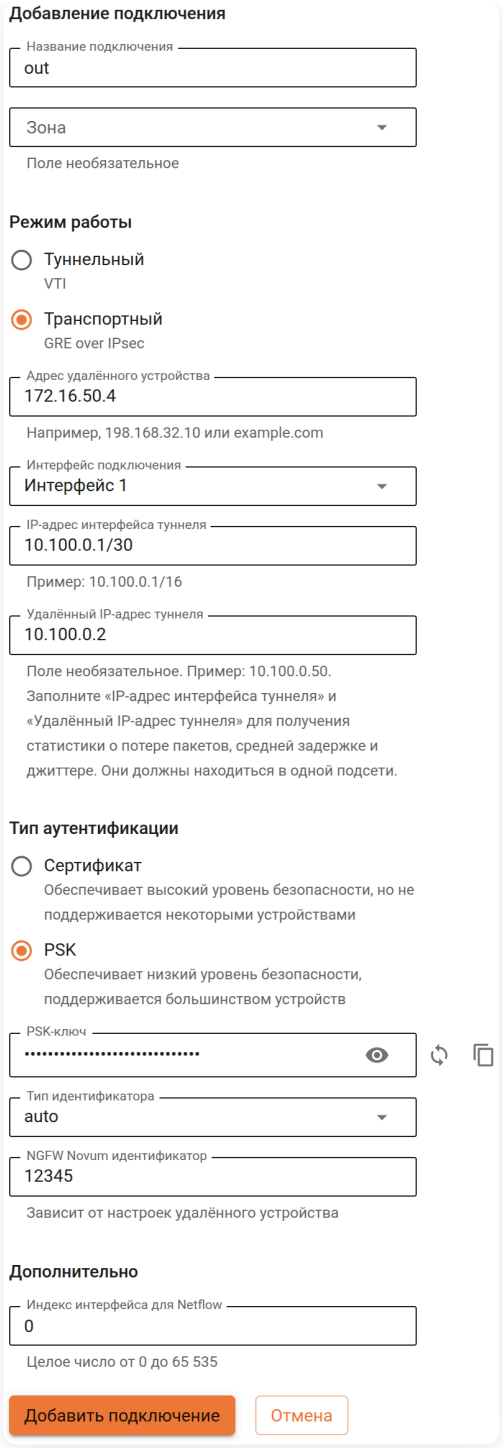
2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1 remote-address=172.16.50.3
/ip address add address=10.100.0.2/30 interface=gre-tunnel1 network=10.100.0.0
```

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на Ideco NGFW Novum

1. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - будет сгенерирован случайный PSK-ключ для настройки подключения в MikroTik.
- **Тип идентификатора** - выберите **keyid**.
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего подключения в MikroTik.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Настройка входящего IPsec-подключения на MikroTik

1. Настройте IPsec-подключение со стороны MikroTik:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256 name=from_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=from_192.168.100.0/24 enc-algorithms=aes-256-cbc name=172.16.50.3 pfs-g

/ip ipsec peer add address=172.16.50.3/32 comment=from_192.168.100.0/24 exchange-mode=ike2 name=from_192.168.100.0/24 passive

/ip ipsec identity add comment=from_192.168.100.0/24 peer=from_192.168.100.0/24 secret="<Сгенерированный NGFW PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.
```

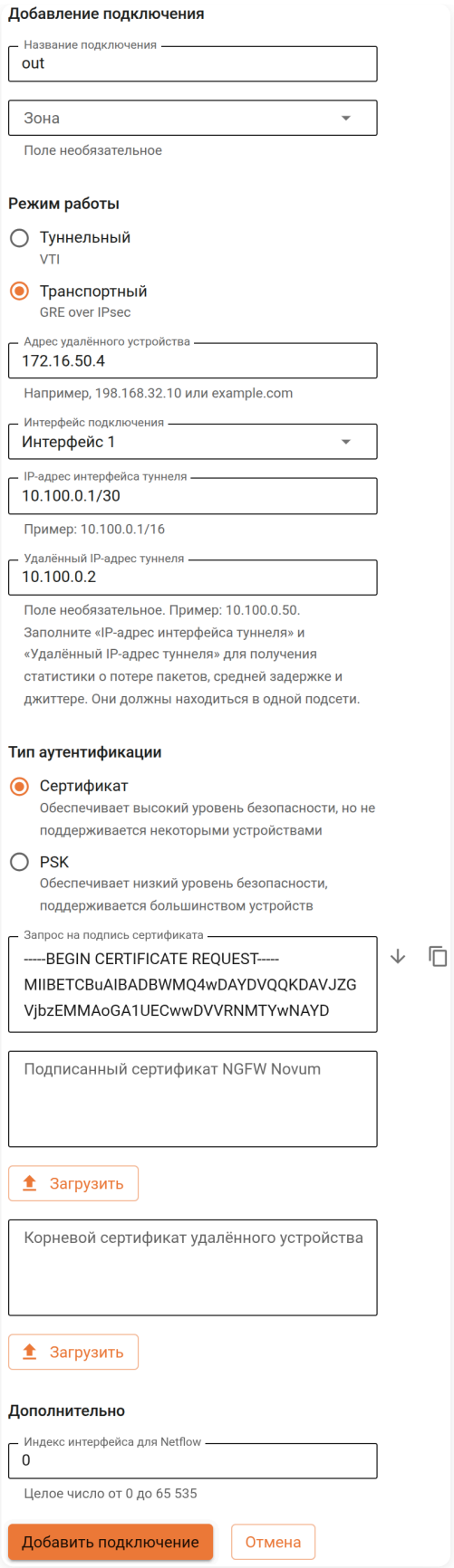
2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Тип аутентификации Сертификат

Настройка исходящего IPsec-подключения на Ideco NGFW Novum

1. Перейдите в **IPsec** → **Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.

- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Скачайте **Запрос на подпись сертификата**.

4. Не закрывая форму создания исходящего подключения NGFW, перейдите к настройке Mikrotik.

Настройка входящего IPsec-подключения на MikroTik

1. Загрузите скачанный ранее файл с **Запросом на подпись сертификата** (`NGFW.crt`) на MikroTik через WinBox или по SSH.

2. Создайте корневой сертификат MikroTik:

```
/certificate add common-name=mk_ca name=mk_ca_template key-usage=key-cert-sign,crl-sign,digital-signature,content-commitment
/certificate sign mk_ca_template ca-crl-host=172.16.50.4 name=mk_ca
```

3. Подпишите сертификат Ideco NGFW Novum и сделайте сертификат доверенным:

```
/certificate sign-certificate-request file-name=NGFW.csr ca=mk_ca
/certificate set [find name~"^device_.+\\.ipsec\$"] trusted=yes
```

4. Экспортируйте корневой сертификат MikroTik и подписанный сертификат NGFW в формат `.pem`:

```
/certificate export-certificate mk_ca type=pem
/certificate export-certificate [find name~"^device_.+\\.ipsec\$"] type=pem
```

5. Загрузите с MikroTik корневой сертификат MikroTik и подписанный сертификат NGFW через WinBox или по SSH. Названия файлов содержат `cert_export`.

6. Настройте входящее IPsec-соединение на MikroTik:

```
/ip ipsec profile add name=from_192.168.100.0/24 hash-algorithm=sha256 enc-algorithm=aes-256 dh-group=modp4096 dpd-interval=1

/ip ipsec peer add name=from_192.168.100.0/24 address=172.16.50.3/32 profile=from_192.168.100.0/24 exchange-mode=ike2 passive

/ip ipsec identity add peer=from_192.168.100.0/24 auth-method=digital-signature certificate=mk_ca remote-certificate=[: put [

/ip ipsec proposal add name=172.16.50.3 enc-algorithms=aes-256-cbc auth-algorithms=sha256 pfs-group=modp4096 comment=from_192

/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.
```

7. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Донастройка исходящего IPsec-подключение на Ideco NGFW Novum

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW Novum.

1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

3. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Подключение от MikroTik к Ideco NGFW Novum

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на MikroTik

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1 remote-address=172.16.50.3
/ip address add address=10.100.0.2/30 interface=gre-tunnel1 network=10.100.0.0
```

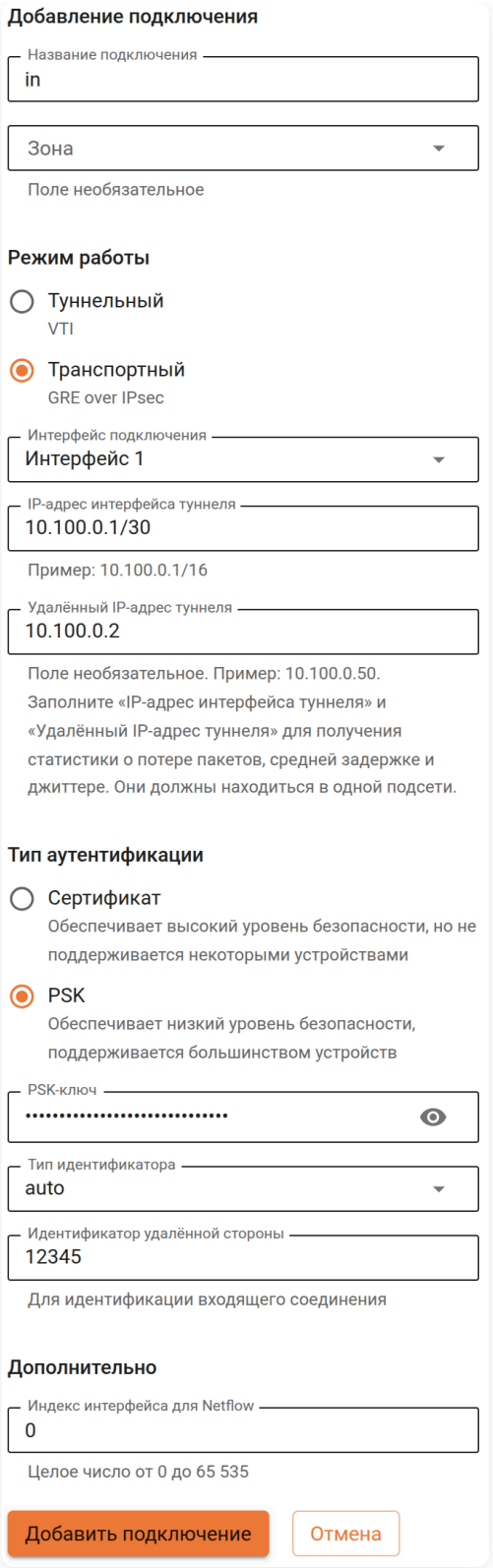
3. Настройте IPsec-подключение со стороны MikroTik:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256 name=to_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-algorithms=aes-256-cbc name=172.16.50.3 pfs-gro

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-mode=ike2 name=to_192.168.100.0/24 profile=to_

/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 my-id=key-id:"test_psk" secret="<PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.16
```

4. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Настройка входящего IPsec-подключения на Ideco NGFW Novum

1. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - введите PSK-ключ, указанный при настройке исходящего IPsec-подключения в MikroTik.
- **Тип идентификатора** - выберите **keyid**.

- **NGFW идентификатор** - введите **key-id**, использованный при настройке исходящего IPsec-подключения в MikroTik.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Тип аутентификации Сертификат

Предварительная настройка MikroTik

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1 remote-address=172.16.50.3
/ip address add address=10.100.0.2/30 interface=gre-tunnel1 network=10.100.0.0
```

3. Сгенерируйте запрос на подпись сертификата:

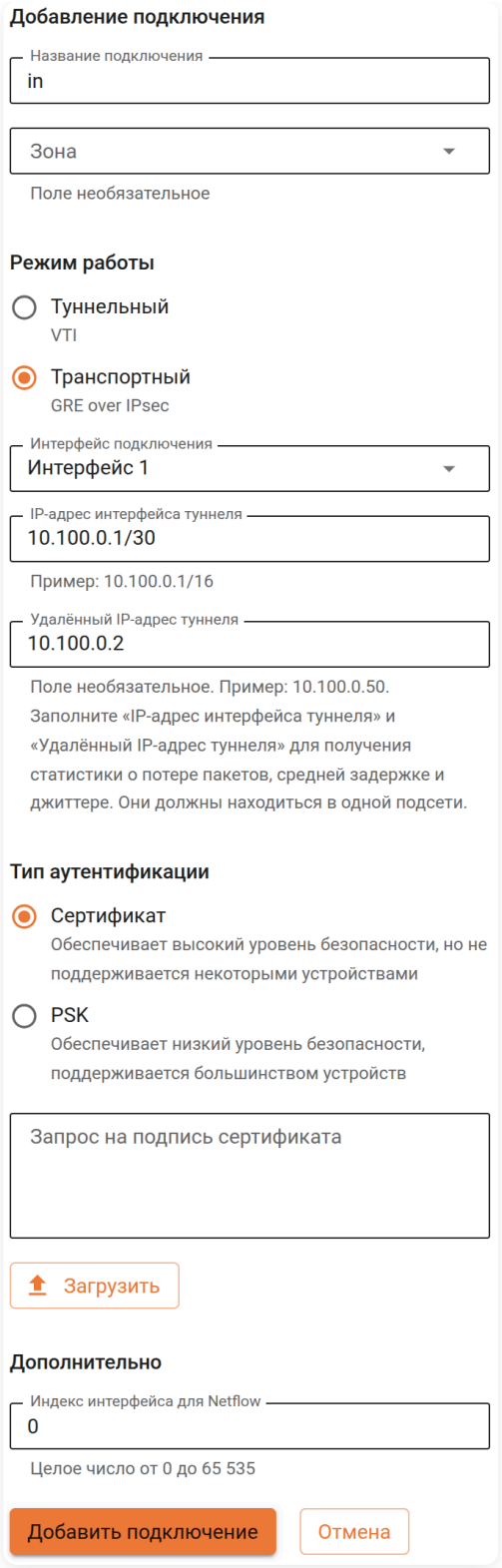
```
/certificate add name=mk_ca common-name=mk_ca key-usage=digital-signature,content-commitment
/certificate create-certificate-request key-passphrase="" template=mk_ca
```

4. Загрузите файл `certificate-request.pem` с MikroTik через WinBox или по SHH.

Настройка входящего IPsec-подключения на Ideco NGFW Novum

1. Перейдите в **IPsec** → **Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Загрузите скачанный ранее с MikroTik файл `certificate-request.pem` в поле **Запрос на подпись сертификата**.

4. Нажмите **Добавить подключение**.

5. Откройте созданное IPsec-соединение, нажав на , и загрузите файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`).

6. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Настройка исходящего IPsec-подключение на MikroTik

1. Загрузите на MikroTik скачанные ранее файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`) через WinBox или по SSH.

2. Импортируйте сертификаты:

```
/certificate import file-name=NGFW.crt passphrase=""
/certificate import file-name=device.crt passphrase=""
/certificate import file-name=certificate-request_key.pem passphrase=""
```

3. Настройте IPsec-соединение:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256 name=to_192.168.100.0/24 dpd-interval=120

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-mode=ike2 name=to_192.168.100.0/24 profile=to_

/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 auth-method=digital-signature certificate=device.

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-algorithms=aes-256-cbc name=172.16.50.3 pfs-gro

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.16
```

4. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

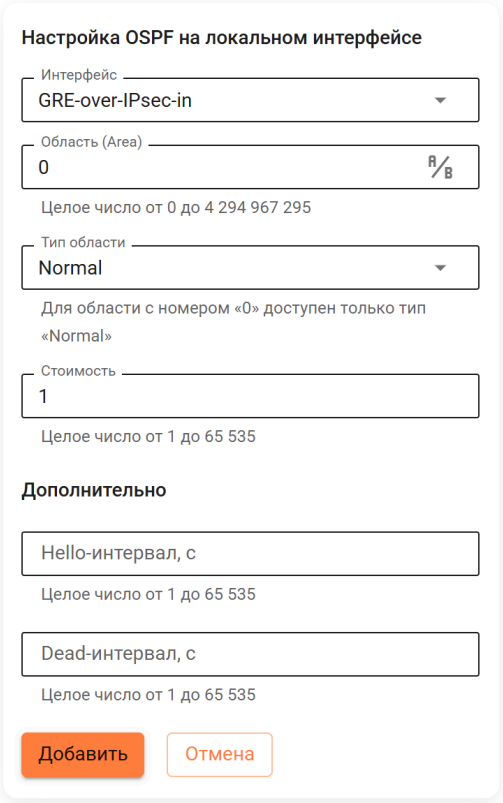
Настройка динамической маршрутизации

OSPF

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW Novum, настроенный ранее.
- **Область (Area)** - введите номер области (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Тип области** - для области с указанным номером `area` должен быть выбран одинаковый тип на всех OSPF-соседях. Для области с номером 0 (`0.0.0.0`) допустимо указывать только один тип - **Normal**. Допустимые значения: **Normal**, **Stub**, **NSSA**:
  - **Normal Area** (обычная зона) - стандартная зона OSPF, которая получает полную информацию о маршрутах как внутри автономной системы, так и за ее пределами. В такой зоне могут находиться как маршрутизаторы, так и конечные устройства.
  - **Stub Area** (усеченная зона) - зона, в которой не принимаются внешние маршруты (Type 5 LSA), но принимаются маршруты других зон. Вместо полной информации о внешних маршрутах используется маршрут по умолчанию.
  - **NSSA** (Not-So-Stubby Area) - разновидность stub-зоны, которая может получать маршруты по умолчанию и отправлять свои маршруты в другие зоны через **ABR** (Area Border Router). В **NSSA** зоне используется специальный тип LSA (Type 7), который преобразуется в Type 5 на ABR.
- **Стоимость** - введите стоимость маршрута.
- **Hello-интервал** - укажите время между отправкой Hello-пакетов, которое варьируется от 1 до 65535 секунд. Если поле не заполнено, по умолчанию используется значение 10 секунд. Для установления соседства между устройствами интервал должен быть одинаковым для всех участников сети.
- **Dead-интервал** - укажите время, через которое сосед считается недоступным, если не получает Hello-пакеты. Диапазон значений - от 1 до 65535 секунд. Если поле не заполнено, по умолчанию в 4 раза больше, чем Hello-интервал. Для успешного соседства значение должно быть одинаковым у всех устройств в сегменте сети.

3. Нажмите **Сохранить**.

4. Включите модуль **OSPF**.

Настройка на MikroTik (RouterOS 6.48.6)

1. Настройте область (значение `area`, должно совпадать на NGFW и Mikrotik):

```
/routing ospf area
add name=backbone area-id=0.0.0.0 type=default default-cost=1 inject-summary-lsa=no
```

3. Объявите сети, участвующие в OSPF:

```
/routing ospf network
add network=192.168.50.0/24 area=backbone
add network=10.100.0.0/16 area=backbone
```

Настройка на MikroTik (RouterOS 7.18.2)

1. Настройте OSPF Instance (процесс OSPF, управляющий определенной группой маршрутов и интерфейсов):

```
/routing ospf instance
add name=<Название Instance> router-id=<Router-ID Mikrotik> redistribute=connected in-filter-chain=ospf-in out-filter-chain=o
```

2. Настройте магистральную зону (значение `area`, должно совпадать на NGFW и Mikrotik):

```
/routing ospf area
add name=backbone area-id=0.0.0.0 instance=<Название Instance>
```

3. Настройте интерфейсы:

```
/routing ospf interface-template
add interfaces=<Название GRE-интерфейса> area=backbone type=ptp network=10.100.0.0/16 cost=10
add interfaces=<Название интерфейса локальной сети> area=backbone type=broadcast network=192.168.50.0/24 cost=1
```

4. Настройте фильтрацию:

```
/routing filter rule
add chain=ospf-in rule="accept" disabled=no comment="Разрешаем все входящие маршруты"
add chain=ospf-out rule="accept" disabled=no comment="Разрешаем все исходящие маршруты"
```

Разрешение всех маршрутов без фильтрации допустимо в тестовых средах, простых или полностью контролируемых топологиях. В

распределенных сетях рекомендуем применять фильтрацию OSPF-маршрутов.

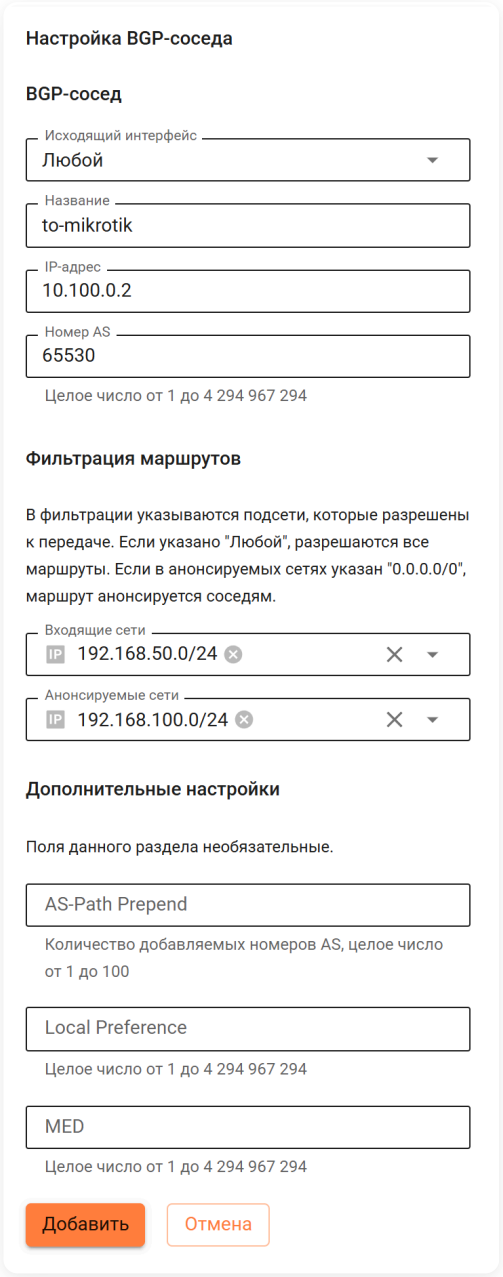
BGP

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. Введите номер автономной системы в поле **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:



- **Исходящий интерфейс** - выберите **Любой**.
- **Название** - любое значение.
- **IP-адрес** - IP-адрес GRE-интерфейса MikroTik.
- **Номер AS** - введите номер автономной системы MikroTik.
- **Входящие сети** - введите сети MikroTik, информацию от которых хотите получать. Если нужного объекта для фильтрации нет, нажмите **Создать новый объект**. Если выбран объект **Любой**, фильтрация будет отключена. Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру `0.0.0.0/0`.
- **Анонсируемые сети** - введите сети Ideco NGFW Novum, информацию о которых хотите отправлять. Если нужного объекта для фильтрации нет, нажмите **Создать новый объект**. Если выбран объект **Любой**, будет передаваться информация обо всех маршрутах, известных NGFW Novum. Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру `0.0.0.0/0`.
- **AS-Path Prepend** - введите число. Чем больше значение, тем менее приоритетным становится канал.

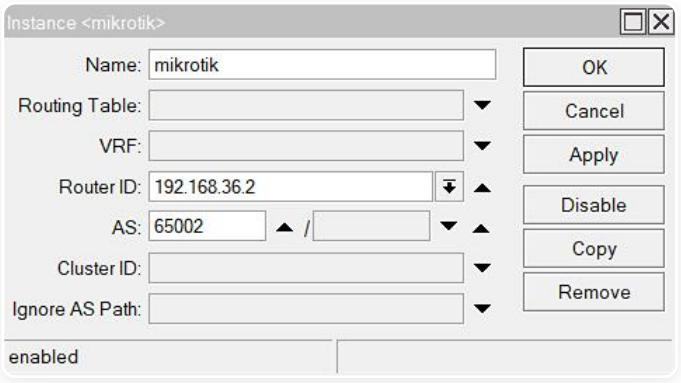
- **Local Preference** - введите число. Определяет приоритет пути для выхода трафика. Чем больше значение, тем более приоритетным становится канал.
- **MED** - введите число. Определяет приоритет пути для входа трафика. Чем меньше значение, тем приоритетнее путь.

3. Нажмите **Сохранить**.

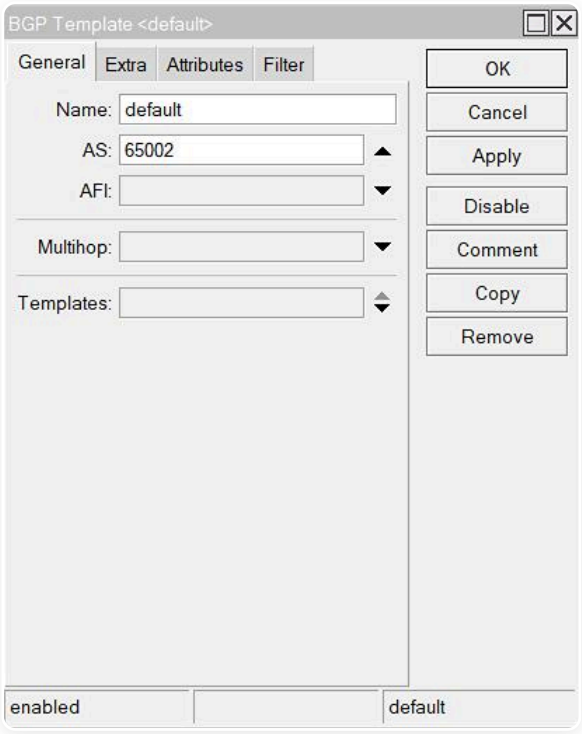
Настройка на MikroTik (RouterOS 7.20.6) через Winbox

Откройте Winbox и подключитесь к MikroTik. Все дальнейшие настройки BGP выполняются в разделе **Routing** → **BGP**.

1. На вкладке **Templates** откройте предустановленный шаблон **default** и задайте номер автономной системы в поле **AS**:



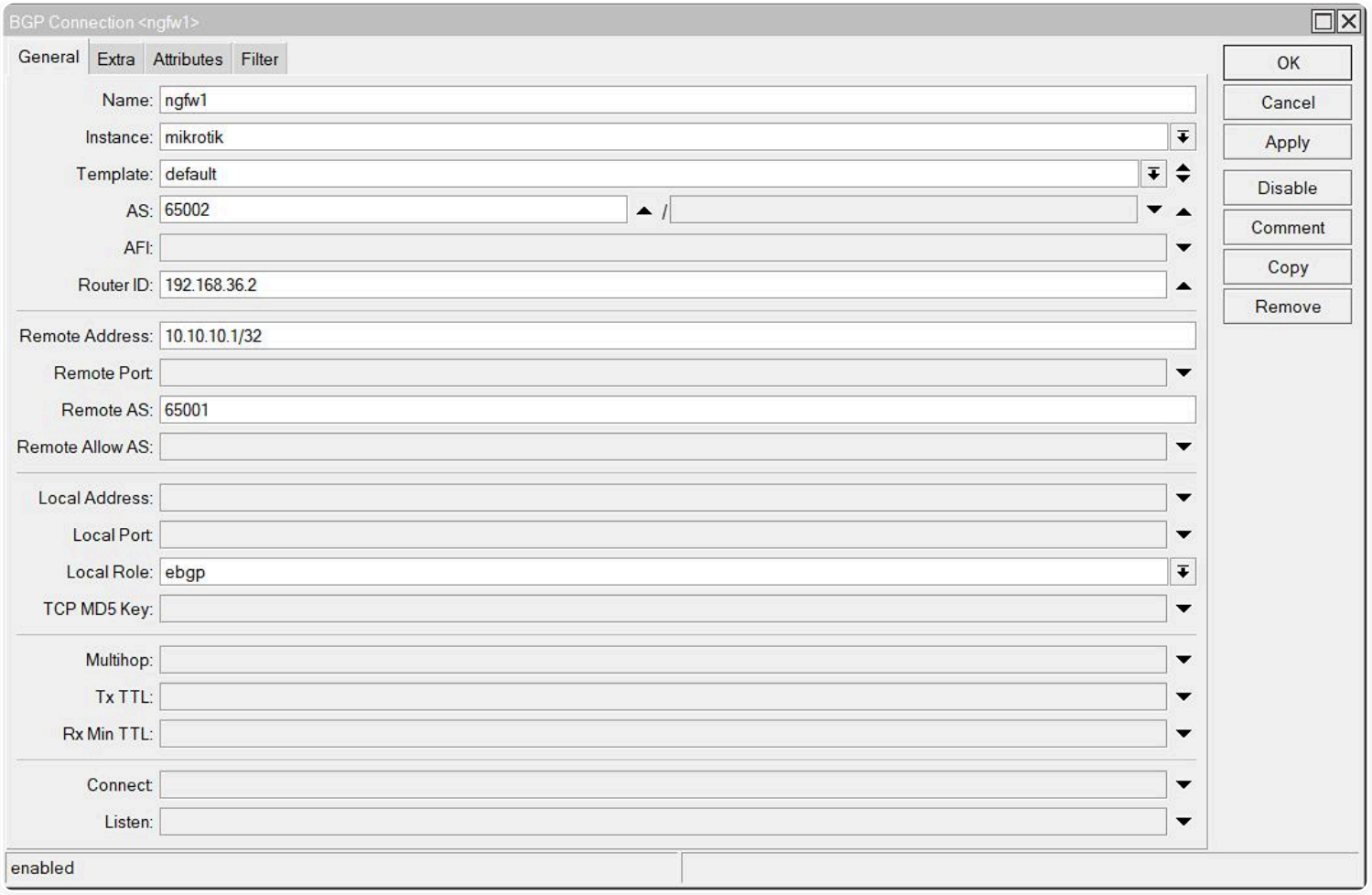
2. На вкладке **Instances** создайте экземпляр BGP с параметрами:



- **Name** - введите произвольное имя.
- **Router ID** - введите IP-адрес одного из локальных интерфейсов MikroTik, например, LAN-интерфейса.
- **AS** - введите номер автономной системы MikroTik.

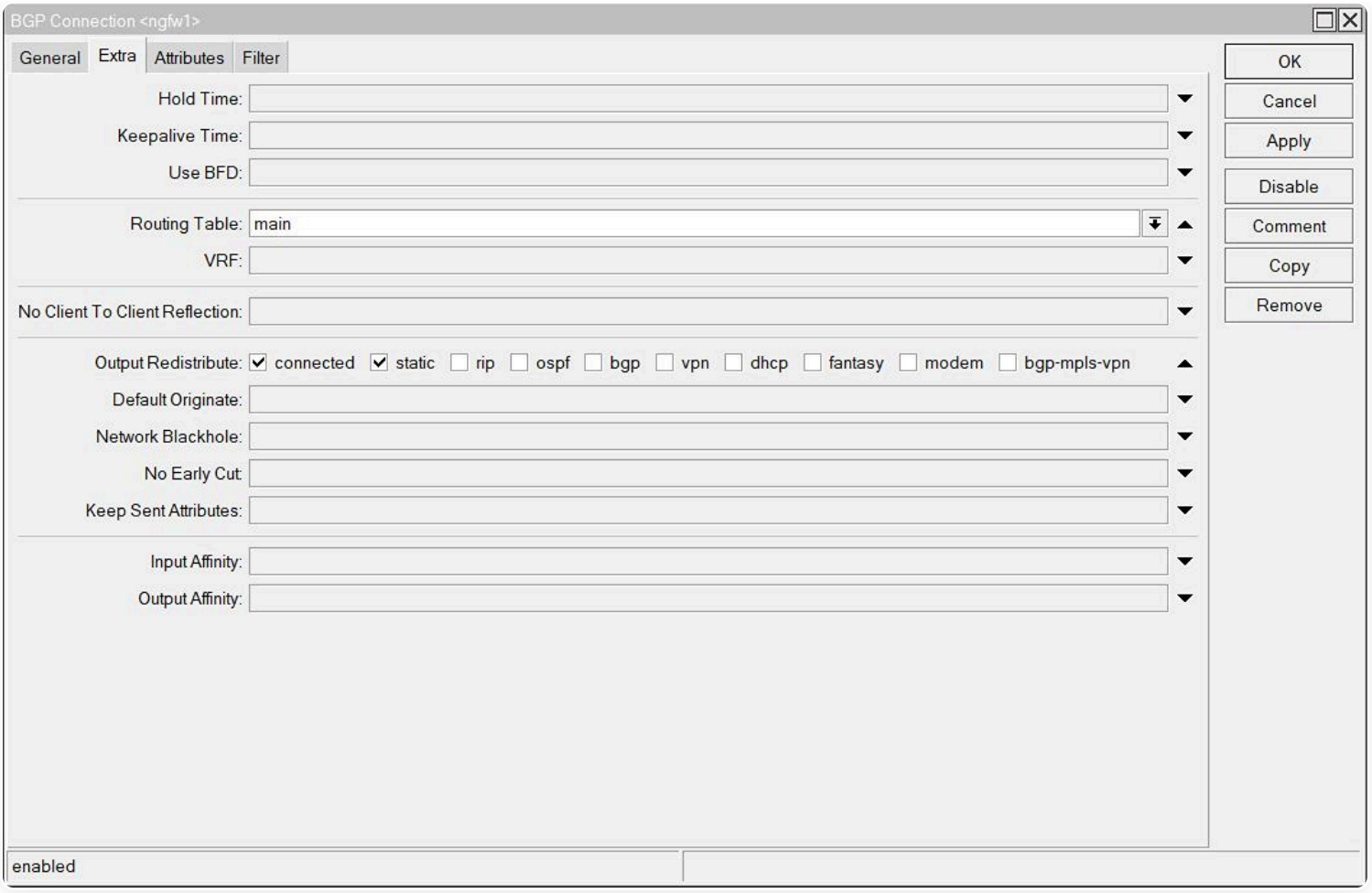
3. Нажмите **OK**.

4. Перейдите на вкладку **Connections**, создайте новое BGP-соединение и заполните поля на вкладке **General**:



- **Name** - введите произвольное имя.
- **Instance** - выберите экземпляр BGP, созданный на шаге 2.
- **Template** - выберите шаблон **default**, отредактированный на шаге 1.
- **AS** - введите номер автономной системы MikroTik.
- **Router ID** - введите IP-адрес одного из локальных интерфейсов MikroTik. Значение должно совпадать с указанным в экземпляре BGP на шаге 2 - здесь оно переопределяется для конкретного соединения.
- **Remote Address** - введите IP-адрес GRE-интерфейса NGFW Novum с маской `/32`.
- **Remote AS** - введите номер автономной системы NGFW Novum.
- **Local Role** - определяет роль данного узла в BGP-сессии. Укажите `ebgp`, так как соединение устанавливается между разными автономными системами (внешний BGP).

5. Перейдите на вкладку **Extra** и заполните поля:



- **Routing Table** - таблица маршрутизации, в которую будут помещаться маршруты, полученные от BGP-соседа. Укажите `main` для использования основной таблицы.
- **Output Redistribute** - отметьте `connected` и `static`, чтобы передавать BGP-соседу подключенные и статические маршруты MikroTik.

6. Нажмите **OK**.

Настройка на MikroTik через CLI

1. Настройте общий шаблон BGP, укажите номер автономной системы и основную таблицу маршрутизации:

```
/routing bgp template set default as=<номер AS MikroTik> disabled=no router-id=<IP-адрес локального интерфейса MikroTik> rout
```

2. Добавьте BGP-соединение с NGFW Novum:

```
/routing bgp connection add name=ngfw remote.address=<IP-адрес GRE-интерфейса NGFW Novum>/32 remote.as=<номер AS NGFW Novum>
```

Проверка результата

Проверка маршрутов на MikroTik

Перейдите в **IP** → **Routes**. В таблице маршрутизации должна появиться подсеть NGFW Novum со статусом `b` (получена по BGP) и шлюзом - IP-адрес GRE-интерфейса NGFW Novum.

Проверка через CLI:

```
/ip route print where bgp
```

Проверка статуса BGP-сессии на MikroTik

Через CLI проверьте, что BGP-сессия установлена:

```
/routing bgp session print
```

В выводе статус соединения должен быть `established`.

Проверка статуса IPsec на MikroTik

Перейдите в **IP** → **IPsec** → **Active Peers**. Должна отображаться запись с внешним IP-адресом NGFW Novum - это подтвердит, что IPsec-сессия установлена.

Перейдите в **IP** → **IPsec** → **Installed SAs**. Должны присутствовать активные записи SA - это подтвердит, что шифрование работает.

Проверка через CLI:

```
/ip ipsec active-peers print
/ip ipsec installed-sa print
```

Проверка на стороне Ideco NGFW Novum

Перейдите в **Управление сервером** → **Терминал** и выполните команды:

1. Проверьте статус IPsec-подключения:

```
ipsec status
```

Подключение должно быть в статусе **Established**.

2. Проверьте таблицы маршрутизации:

```
ip route show proto bgp
```

В выводе должна присутствовать подсеть MikroTik.

Проверка связи между хостами

С хоста в подсети NGFW Novum выполните:

```
ping <хост в подсети MikroTik>
```

С хоста в подсети MikroTik выполните:

```
/ping <хост в подсети NGFW Novum>
```

Обе проверки должны пройти успешно. Убедитесь, что NAT не применяется - в ответах должны фигурировать реальные IP-адреса хостов, а не транслированные.

Возможные проблемы

Соединение не устанавливается при повторной активации

Если подключение было отключено и при попытке включения соединение не установилось, удаленное устройство попало в fail2ban. Для установки соединения сбросьте блокировки по IP на Ideco NGFW Novum. О сбросе блокировки читайте в статье Защита от брутфорс-атак.

Fail2ban отслеживает в log-файлах попытки обратиться к сервисам, и, если находит повторяющиеся неудачные попытки авторизации с одного и того же IP-адреса или хоста, блокирует IP-адрес.

Соединение периодически разрывается

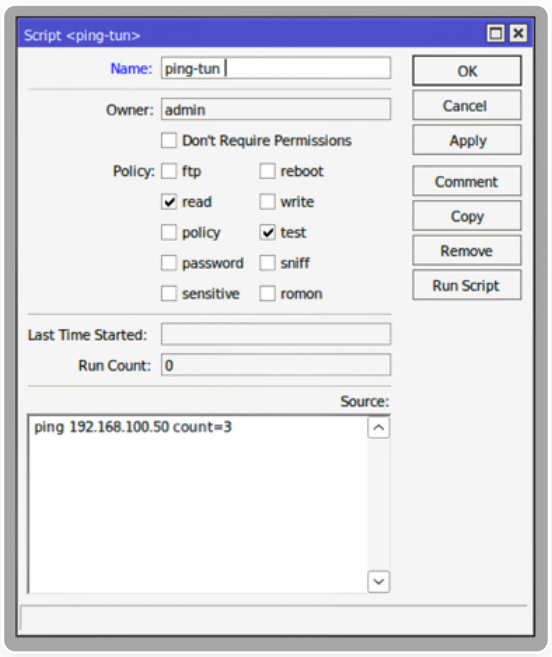
При работе туннеля между Ideco NGFW Novum и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW Novum.

Для автоматизации процесса поддержания соединения, создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW Novum:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в **System** → **Scripts**.

3. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



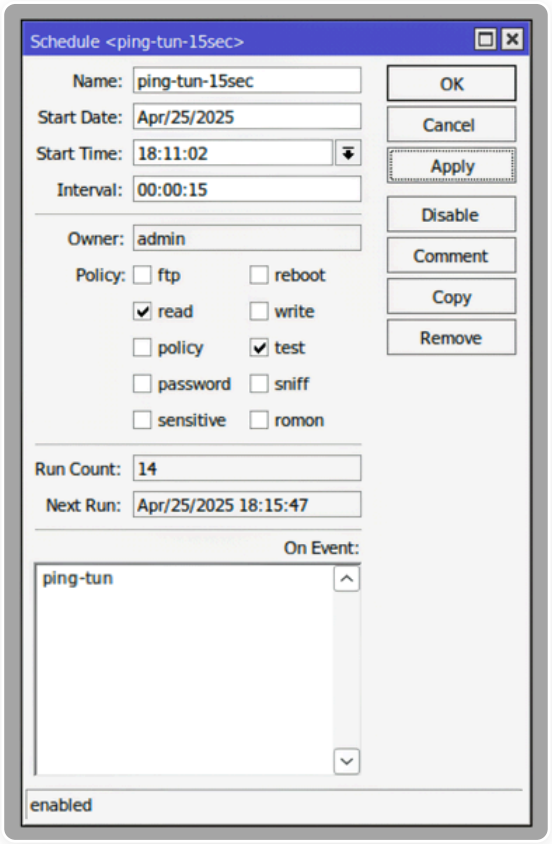
- **Name** - название скрипта (не поддерживаются пробелы и нижние подчеркивания).
- **Policy** - оставьте флаги на **read** и **test**.
- **Source** - введите команду `ping <ID-адрес Ideco NGFW Novum> count=3`.

4. Нажмите **Apply**, затем **Ok**.

Далее настройте запуск скрипта по расписанию в планировщике заданий:

1. Перейдите в **System** → **Scheduler**.

2. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



- **Name** - название задания (не поддерживаются пробелы и нижние подчеркивания).

- **Interval** - интервал 00:00:15 (каждые 15 секунд).
- **Policy** - оставьте флаги на **read** и **test**.
- **On Event** - введите название созданного ранее скрипта.

3. Нажмите **Apply**, затем **Ok**.

По завершению настройки MikroTik каждые 15 секунд будет отправлять три ICMP-запроса на адрес Ideco NGFW Novum. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.



В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение MikroTik и Ideco NGFW Novum по L2TP/IPsec

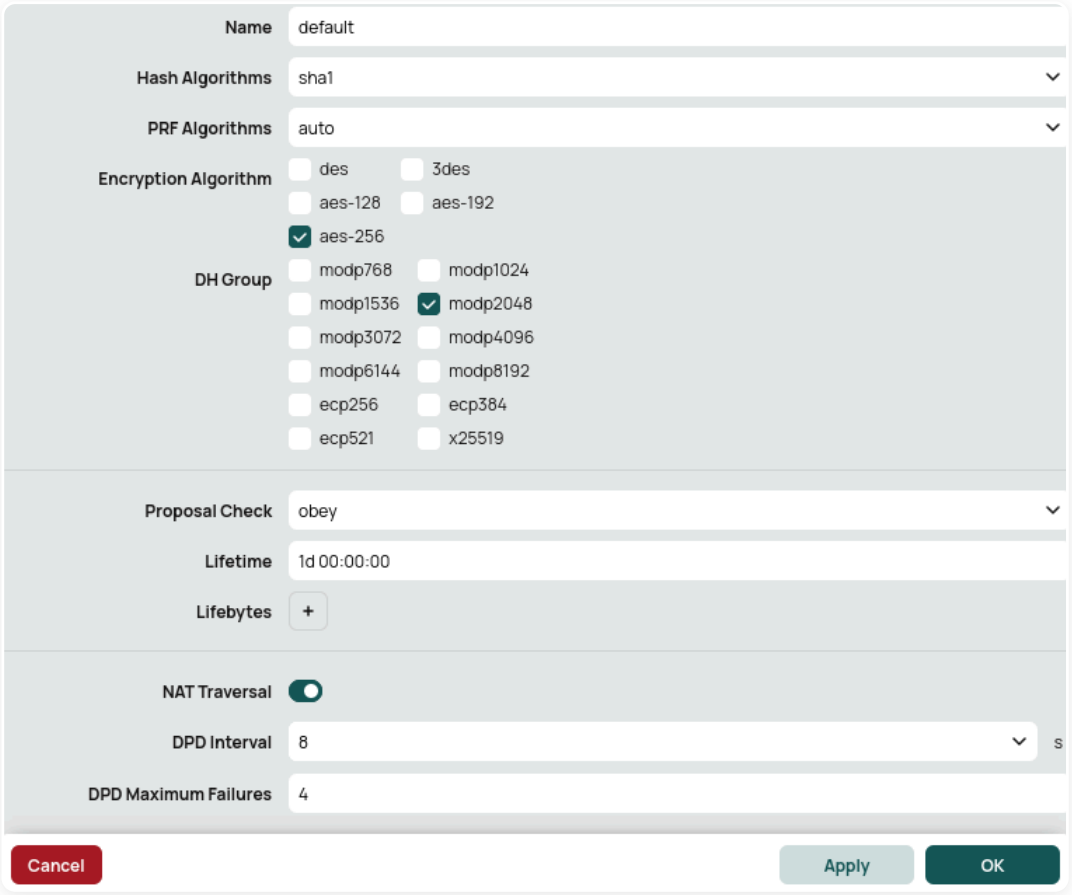
Функциональность доступна в **Классическом** и **Системном контекстах**.

Подключение MikroTik к Ideco NGFW Novum по L2TP/IPsec

- Настройте VPN-сервер на Ideco NGFW Novum в **Пользователи** → **VPN-подключения**. Подробная инструкция по настройке - в статье Подключение по L2TP/IPsec.
- Настройте подключение на MikroTik:

Веб-интерфейс

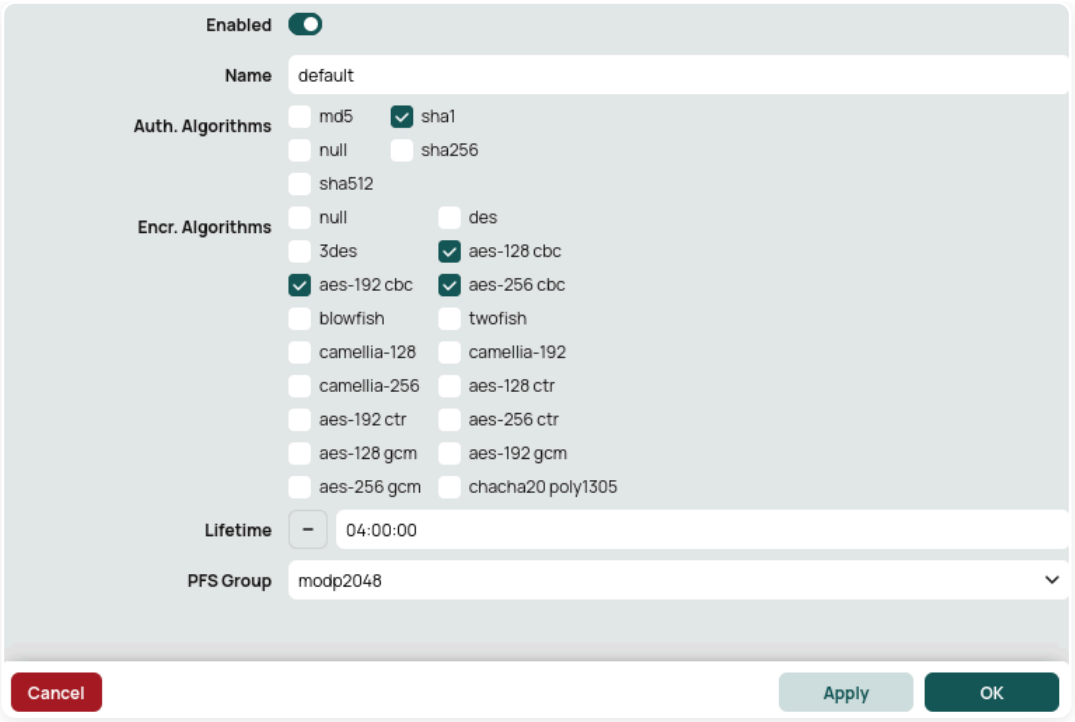
1. Перейдите в **IP** → **IPsec** → **Profiles**, выберите профиль **default** и заполните поля:



- **Hash Algorithms** - `sha1`.
- **Encryption Algorithm** - `aes-256`.
- **DH Group** - `modp2048`.

2. Нажмите **OK**.

3. Перейдите в **IP** → **IPsec** → **Proposals**, выберите профиль **default** и заполните поля:

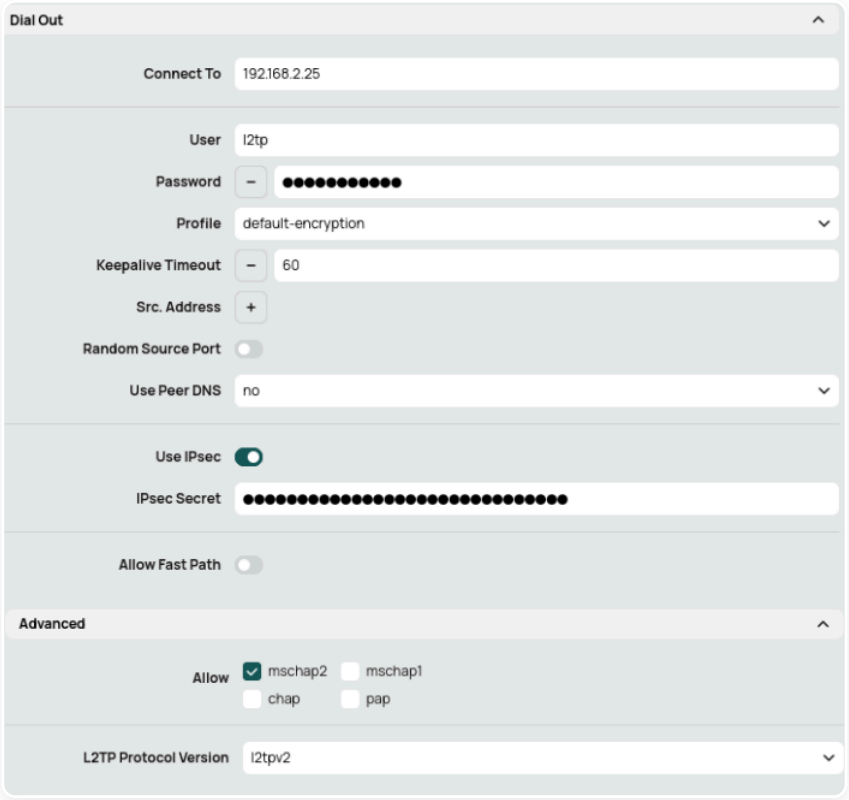


- **Auth. Algorithms** - `sha1`.
- **Encr. Algorithms** - `aes-256-cbc`, `aes-192-cbc`, `aes-128-cbc`.
- **PFS Group** - `modp2048`.

4. Нажмите **OK**.

5. Перейдите в **Interfaces**, нажмите **New** и выберите **L2TP Client**.

6. Заполните поля:



Расшифровка полей

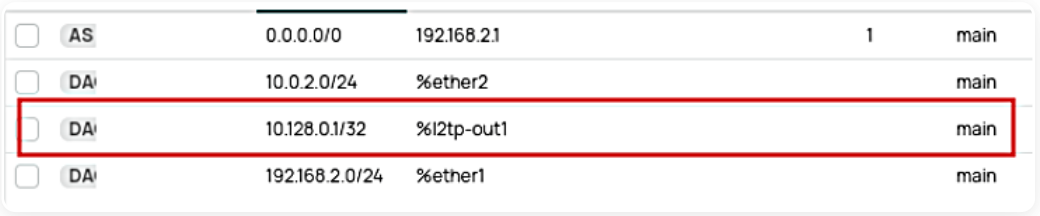
- **Dial Out**:
  - **Connect To** - IP-адрес Ideco NGFW Novum.
  - **User** - логин пользователя, которому разрешено подключение по VPN.

- **Password** - пароль пользователя.
- **Use IPsec** - включите опцию.
- **IPsec Secret** - ключ, скопированный по пути **Пользователи** → **VPN-подключения** → **Основное** из поля **PSK**.

- **Advanced**:
  - **Allow** - `mschap2`.

7. Нажмите **OK**.

8. Перейдите в **IP** → **Routes** и проверьте, что маршрут создан:



Терминал

1. Отредактируйте IPsec profile:

```
ip ipsec profile set default hash-algorithm=sha1 enc-algorithm=aes-256 dh-group=modp2048
```

2. Отредактируйте IPsec proposals:

```
ip ipsec proposal set default auth-algorithms=sha1 enc-algorithms=aes-256-cbc,aes-192-cbc,aes-128-cbc pfs-group=modp2048
```

3. Создайте подключение к Ideco NGFW Novum:

```
interface l2tp-client add connect-to=<server> profile=default disabled=no name=<interface_name> password="<password>" user="<
```

4. Добавьте маршрут до первого адреса VPN-сети NGFW (remote VPN subnet):

```
ip route add dst-address=<remote VPN subnet> gateway=l2tp-out1
```

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

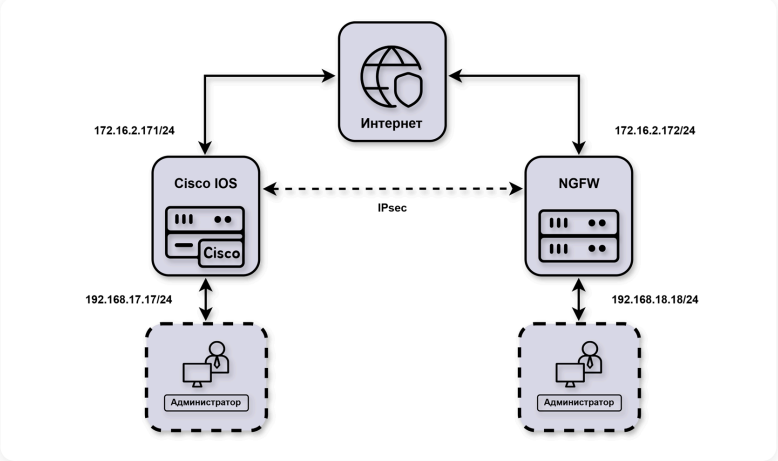
Полезные ссылки

- **IPsec**

Подключение Cisco IOS и Ideco NGFW Novum по IPsec в туннельном режиме

Функциональность доступна в **Классическом** и **Системном контекстах**.

Рассмотрим настройку подключения по схеме ниже:



Адресация:

- `172.16.2.172/24` - внешний IP-адрес NGFW.
- `192.168.18.18/24` - локальный IP-адрес NGFW.
- `172.16.2.171/24` - внешний IP-адрес Cisco.
- `192.168.17.17/24` - локальный IP-адрес Cisco.

Для настройки подключения Cisco IOS к Ideco NGFW Novum следуйте инструкции ниже.

Первоначальная настройка Ideco NGFW Novum и Cisco IOS

Настройка Ideco NGFW Novum

Настройте на Ideco NGFW Novum локальный и внешний интерфейсы. Инструкция по настройке - в статье.

Настройка Cisco IOS XE

Настроить Cisco можно, воспользовавшись нашими конфигурационными скриптами, сгенерированными по адресу https://cisco.ideco.ru/.

Для настройки Cisco через консоль выполните действия:

1. Настройте локальный интерфейс:

```
enable
conf t
interface GigabitEthernet2
ip address <локальный IP Cisco> <маска подсети>
no shutdown
ip nat inside
exit
```

2. Настройте внешний интерфейс:

```
interface GigabitEthernet1
ip address <внешний IP Cisco> <маска подсети>
no shutdown
```

```
ip nat outside
exit
```

3. Проверьте наличие связи между внешними интерфейсами Ideco NGFW Novum и Cisco. Для этого в консоли Cisco используйте команду `ping <внешний IP NGFW>`. Результат вывода команды - наличие ICMP-ответов.

4. Создайте access-list с адресацией локальной сети:

```
ip access-list extended NAT
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit
```

5. Настройте NAT:

```
ip nat inside source list NAT interface GigabitEthernet1 overload
exit
```

6. Сохраните настройки конфигурации:

```
write memory
```

7. **После сохранения настроек проверьте, что из локальной сети Cisco присутствует доступ в интернет.**

Для этого перейдите на какой-нибудь сайт (например: https://www.cisco.com/) с устройства в локальной сети Cisco.

Особенности работы Cisco в некоторых версиях:

- Cisco передает внешний IP-адрес вместо **KeyID** (проверьте, включив расширенный лог IPsec на Cisco). При настройке подключения от таких роутеров к Ideco NGFW Novum в качестве **Идентификатора удаленной стороны** укажите внешний IP-адрес Cisco, в качестве **Типа идентификатора** - auto.
- Если в подключении site2site активную сторону представляет Cisco и Child_SA закрывается, то пассивная сторона не сможет отправить пакет в сторону Cisco, пока Cisco не создаст новый Child_SA.

Инструкция проверена на **Cisco IOS XE версии 17.3.5**. При использовании других версий Cisco IOS синтаксис отдельных команд может отличаться.

Подключение от Ideco NGFW Novum к Cisco

Настройка IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
exit
```

3. Создайте peer:

```
crypto ikev2 keyring key
peer strongswan
```

```
address <внешний IP NGFW>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile:

```
crypto ikev2 profile ikev2profile
match identity remote key-id <key-id>
authentication remote pre-share
authentication local pre-share
keyring local key
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode tunnel
exit
```

6. Создайте ipsec-isakmp:

```
crypto map cmap 10 ipsec-isakmp
set peer <внешний IP NGFW>
set transform-set TS
set ikev2-profile ikev2profile
match address cryptoacl
reverse-route
exit
```

7. Настройте crypto map на внешнем интерфейсе:

```
interface GigabitEthernet1
crypto map cmap
exit
```

8. Создайте access-list для трафика между локальными сетями Cisco и NGFW:

```
ip access-list extended cryptoacl
permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
exit
```

9. Добавьте в access-list NAT исключения трафика между локальными сетями Cisco и NGFW (правило `deny` должно оказаться выше, чем `permit`):

```
ip access-list extended NAT
no permit ip <локальная подсеть Cisco> <обратная маска подсети> any
deny ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit

end
```

10. Сохраните настройки конфигурации:

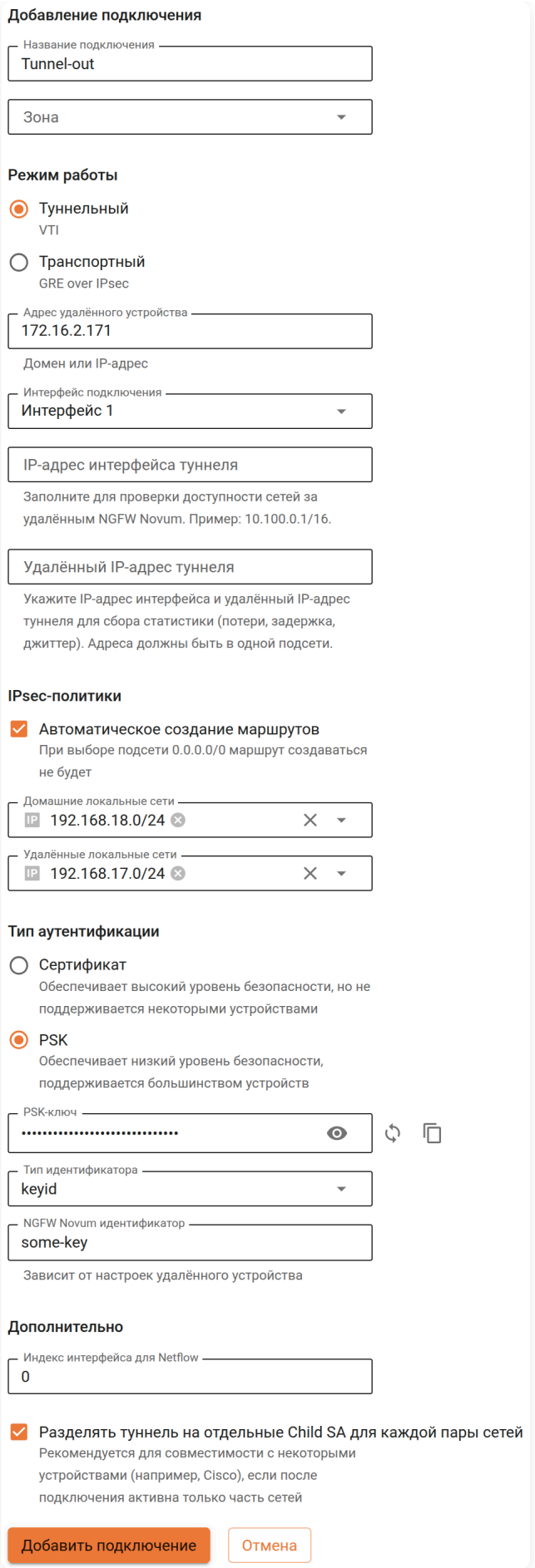
```
write memory
```

Настройка исходящего подключения на Ideco NGFW Novum

Для настройки исходящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPsec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.

- **Адрес удаленного устройства** - введите IP-адрес Cisco. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное. Заполняется при настройке BGP-соседства для динамической маршрутизации, получения статистики обмена пакетами или для обеспечения доступа Ideco NGFW Novum к удаленным сетям за другим устройством.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Поле необязательное. Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.
- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - будет сгенерирован случайный PSK-ключ для подключения в Cisco.
- **Идентификатор NGFW** - введенный ключ будет использоваться для идентификации исходящего подключения. Введите также этот идентификатор в Cisco.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Разделять туннель на отдельные Child SA для каждой пары сетей** - включите опцию для создания отдельного Child SA на каждую пару локальной и удаленной подсети, обеспечивая доступность всех сетей сразу после установления VPN. Актуально для совместимости с некоторыми типами устройств (например, Cisco), которые не поддерживают несколько селекторов трафика в одном Child SA.

3. Сохраните созданное подключение, затем нажмите на кнопку **Включить**.

4. Проверьте, что подключение установлено и используется (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Используется**).

5. Проверьте наличие трафика между локальными сетями.
Итоговая конфигурация IKEv2 IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Ideco NGFW Novum к Cisco

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy ikev2policy
 match fvrf any
 proposal ikev2proposal

crypto ikev2 keyring key
  peer strongswan
   address <внешний IP NGFW>
   pre-shared-key local <psk>
   pre-shared-key remote <psk>

crypto ikev2 profile ikev2profile
  match identity remote key-id <key-id>
  authentication remote pre-share
  authentication local pre-share
  keyring local key

crypto ipsec transform-set TS esp-gcm 256
 mode tunnel

crypto map cmap 10 ipsec-isakmp
 set peer <внешний IP NGFW>
 set transform-set TS
 set ikev2-profile ikev2profile
 match address cryptoacl
 reverse-route

interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
 crypto map cmap
```

```
interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid

ip nat inside source list NAT interface GigabitEthernet1 overload

ip access-list extended NAT
 deny   ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
ip access-list extended cryptoacl
 permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
```

Подключение от Cisco к Ideco NGFW Novum

Настройка IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
exit
```

3. Создайте peer:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP NGFW>
identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile:

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP NGFW> 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local key
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode tunnel
exit
```

6. Создайте ipsec-isakmp:

```
crypto map cmap 10 ipsec-isakmp
set peer <внешний IP NGFW>
set transform-set TS
set ikev2-profile ikev2profile
match address cryptoacl
reverse-route
exit
```

7. Настройте crypto map на внешнем интерфейсе:

```
interface GigabitEthernet1
crypto map cmap
exit
```

8. Создайте access-list для трафика между локальными сетями Cisco и NGFW:

```
ip access-list extended cryptoacl
permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
exit
```

9. Добавьте в access-list NAT исключения трафика между локальными сетями Cisco и NGFW (правило `deny` должно оказаться выше чем `permit`):

```
ip access-list extended NAT
no permit ip <локальная подсеть Cisco> <обратная маска подсети> any
deny ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit

end
```

10. Сохраните настройки конфигурации:

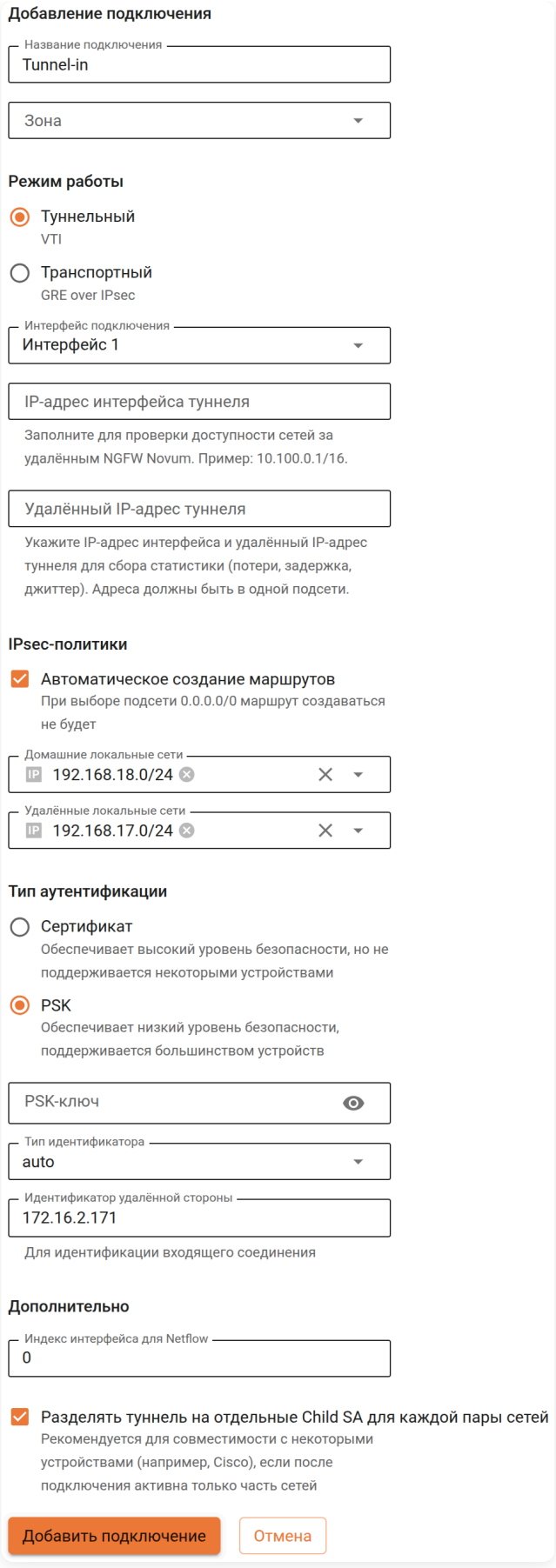
```
write memory
```

Настройка входящего подключения на Ideco NGFW Novum

Для настройки входящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы → IPsec → Устройства (входящие подключения)**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPSec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное. Заполняется при настройке BGP-соседства для динамической маршрутизации, получения статистики обмена пакетами или для обеспечения доступа Ideco NGFW Novum к удаленным сетям за другим устройством.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Поле необязательное. Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. IP-адреса должны находиться в одной подсети. Заполняется для получения статистики обмена пакетами.
- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ.
- **Тип идентификатора** - keyid или auto, если Cisco передает IP-адрес вместо key-id.
- **Идентификатор удаленной стороны** - вставьте идентификатор Cisco (параметр Key ID) или IP-адрес Cisco, если Cisco передает IP-адрес вместо key-id.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Разделять туннель на отдельные Child SA для каждой пары сетей** - включите опцию для создания отдельного Child SA на каждую пару локальной и удаленной подсети, обеспечивая доступность всех сетей сразу после установления VPN. Актуально для совместимости с некоторыми типами устройств (например, Cisco), которые не поддерживают несколько селекторов трафика в одном Child SA.

3. Сохраните созданное подключение, затем нажмите на кнопку **Включить**.

4. Проверьте, что подключение установлено и используется (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Используется**).

5. Проверьте наличие трафика между локальными сетями.
Итоговая конфигурация IKEv2 IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW Novum

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy ikev2policy
 match fvrf any
 proposal ikev2proposal

crypto ikev2 keyring key
  peer strongswan
   address <внешний IP NGFW>
   identity key-i <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
   pre-shared-key local <psk>
   pre-shared-key remote <psk>

crypto ikev2 profile ikev2profile
  match identity remote address <внешний IP NGFW> 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local key

crypto ipsec transform-set TS esp-gcm 256
 mode tunnel

crypto map cmap 10 ipsec-isakmp
 set peer <внешний IP NGFW>
 set transform-set TS
 set ikev2-profile ikev2profile
 match address cryptoacl
 reverse-route

interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
 crypto map cmap
```

```
interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid

ip nat inside source list NAT interface GigabitEthernet1 overload

ip access-list extended NAT
 deny   ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
ip access-list extended cryptoacl
 permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
```

Настройка динамической маршрутизации (BGP)

Настройка на Cisco

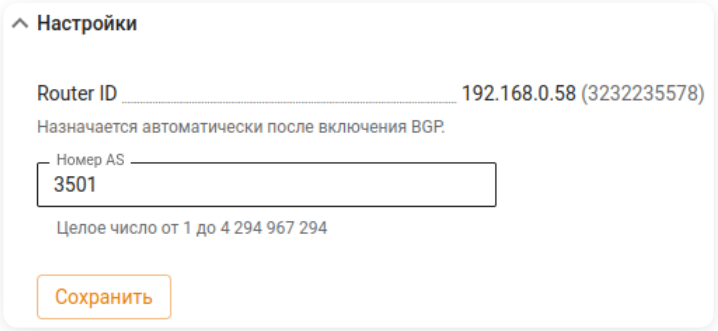
Настройте BGP на роутере:

```
conf t
router bgp 3500
 neighbor <внешний IP NGFW> remote-as 3501
 neighbor <внешний IP NGFW> ebgp-multihop 2
 !
 address-family ipv4
 network <локальная подсеть Cisco> mask <маска подсети>
 neighbor <внешний IP NGFW> activate
 exit-address-family
```

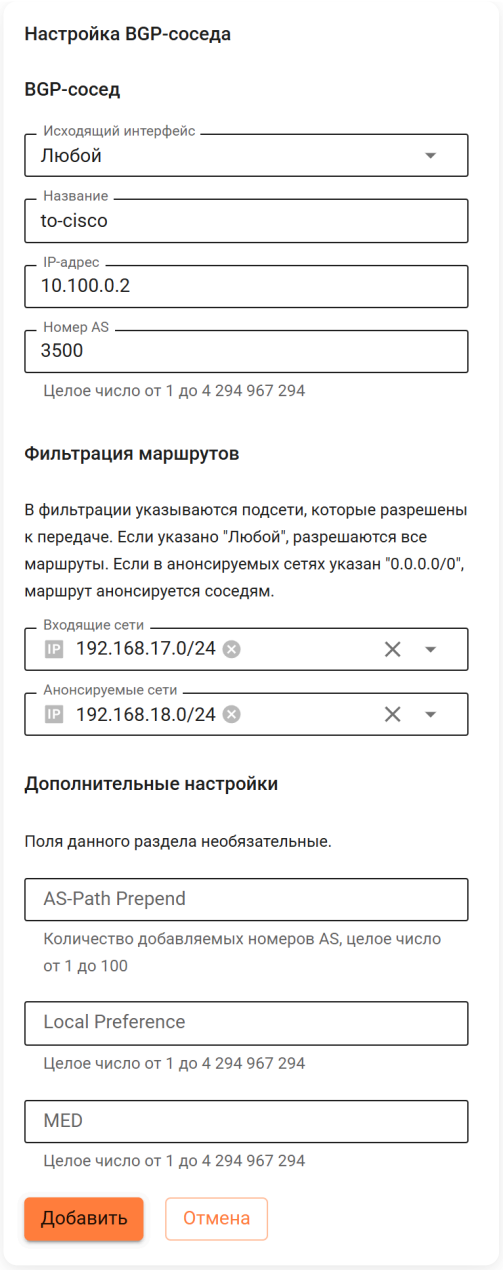
Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. Введите в блоке **Настройки** номер автономной системы в поле **Номер AS** и нажмите **Сохранить**:



3. Заполните поля:



Расшифровка полей

- **Исходящий интерфейс** - выберите **Любой**.
- **IP-адрес** - укажите внешний IP-адрес Cisco.
- **Номер AS** - номер AS Cisco (указанный в команде `router bgp 3500`).
- **Входящие сети** - укажите локальные сети Cisco.
- **Анонсируемые сети** - укажите локальные сети Ideco NGFW Novum.
- **Дополнительные настройки** при необходимости:
  - **AS-Path Prepend** - укажите приоритетность канала.
  - **Local Preference** - определите приоритет пути для выхода трафика. Чем больше значение, тем более приоритетным становится канал.
  - **MED** - определите приоритет пути для входа трафика. Чем меньше значение, тем приоритетнее путь.

4. Включите модуль **BGP**.



В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Cisco IOS и Ideco NGFW Novum по IPsec в транспортном режиме

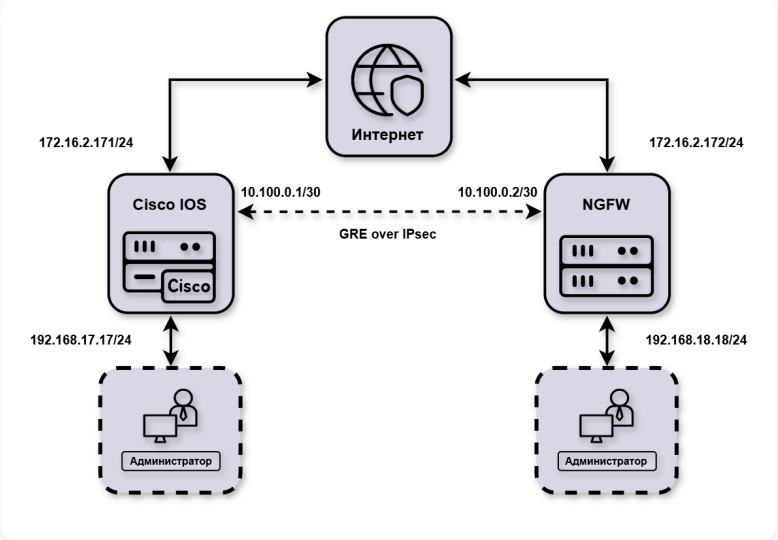
Функциональность доступна в **Классическом** и **Системном контекстах**.

GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

В GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

Для доступности локальных сетей NGFW и Cisco с удаленного устройства при подключении по GRE over IPsec настройте на обоих устройствах статические маршруты или динамическую маршрутизацию через **BGP**.

Рассмотрим настройку подключения по схеме ниже:



Адресация:

- `172.16.2.172/24` - внешний IP-адрес NGFW.
- `192.168.18.18/24` - локальный IP-адрес NGFW.
- `172.16.2.171/24` - внешний IP-адрес Cisco.
- `192.168.17.17/24` - локальный IP-адрес Cisco.
- `10.100.0.1/30` - IP-адрес интерфейса туннеля NGFW.
- `10.100.0.2/30` - IP-адрес интерфейса туннеля Cisco.

Для настройки подключения Cisco IOS к Ideco NGFW Novum следуйте инструкции ниже.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

Первоначальная настройка Ideco NGFW Novum и Cisco IOS

Настройка Ideco NGFW Novum

Настройте на Ideco NGFW Novum локальный и внешний интерфейсы. Инструкция по настройке - в статье.

Настройка Cisco IOS через консоль

1. Настройте локальный интерфейс:

```
enable
conf t
interface GigabitEthernet2
ip address <локальный IP Cisco> <маска подсети>
no shutdown
ip nat inside
exit
```

2. Настройте внешний интерфейс:

```
interface GigabitEthernet1
ip address <внешний IP Cisco> <маска подсети>
no shutdown
ip nat outside
exit
```

3. Проверьте наличие связи между внешними интерфейсами Ideco NGFW Novum и Cisco. Для этого в консоли Cisco используйте команду `ping <внешний IP NGFW>`. Результат вывода команды - наличие ICMP-ответов.

4. Создайте access-list и NAT для доступа из локальной сети в интернет:

```
ip access-list extended NAT
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit
ip nat inside source list NAT interface gigabitEthernet 1 overload
```

5. Сохраните настройки конфигурации:

```
write memory
```

5. **После сохранения настроек проверьте, что из локальной сети Cisco присутствует доступ в интернет.**

Для этого перейдите на какой-нибудь сайт (например: https://www.cisco.com/) с устройства в локальной сети Cisco.

Особенности работы Cisco в некоторых версиях:

- Cisco передает внешний IP-адрес вместо **KeyID** (проверьте, включив расширенный лог IPsec на Cisco). При настройке подключения от таких роутеров к Ideco NGFW Novum в качестве **Идентификатора удаленной стороны** укажите внешний IP-адрес Cisco, в качестве **Типа идентификатора** - auto.
- Если в подключении site2site активную сторону представляет Cisco и Child_SA закрывается, то пассивная сторона не сможет отправить пакет в сторону Cisco, пока Cisco не создаст новый Child_SA.

Подключение от Ideco NGFW Novum к Cisco

Настройка IKEv2+GRE-over-IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
```

```
proposal ikev2proposal
exit
```

3. Создайте peer (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

- Для подключения от Ideco NGFW Novum к Cisco:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP-адрес NGFW>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

- Для подключения от Cisco к Ideco NGFW Novum:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP NGFW>
identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

- Для подключения от Ideco NGFW Novum к Cisco:

```
crypto ikev2 profile ikev2profile
match identity remote key-id <key-id>
authentication remote pre-share
authentication local pre-share
keyring local key
dpd 10 3 periodic
exit
```

- Для подключения от Cisco к Ideco NGFW Novum:

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP NGFW> 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local key
dpd 10 3 periodic
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode transport
exit
```

6. Настройте профиль IPsec:

```
crypto ipsec profile ikev2TSprofile
set transform-set TS
set pfs group19
set ikev2-profile ikev2profile
exit
```

7. Создайте туннельный интерфейс:

```
interface Tunnel0
ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
ip mtu 1400
tunnel source GigabitEthernet 1
tunnel destination <внешний IP-адрес NGFW>
tunnel protection ipsec profile ikev2TSprofile
exit
```

8. Настройте динамическую маршрутизацию (BGP или OSPF) или статический маршрут до локальных сетей Ideco NGFW Novum:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

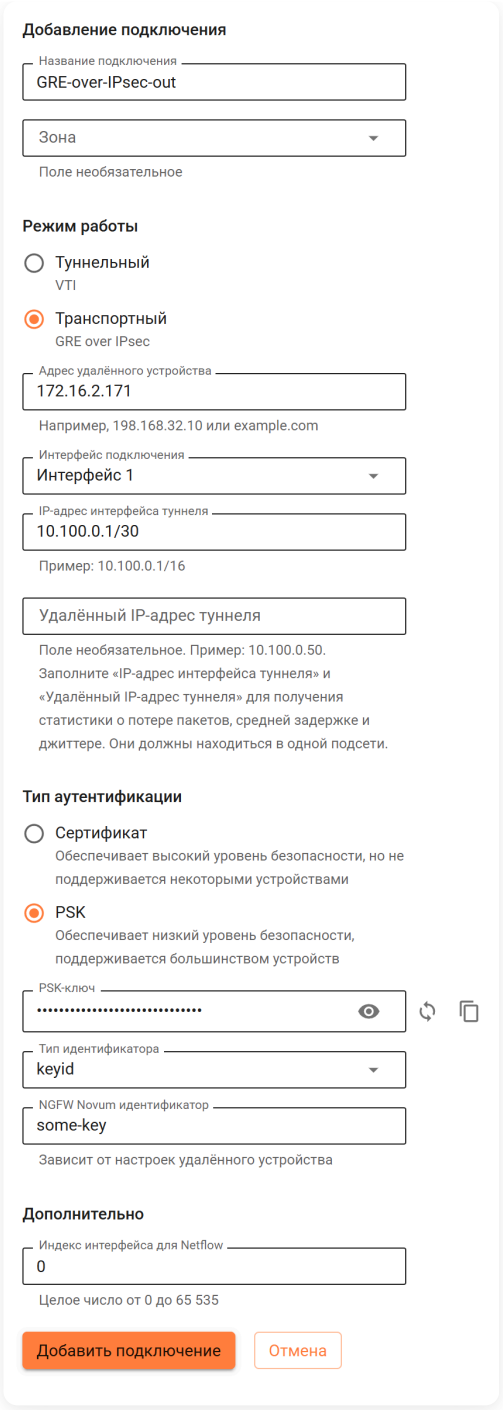
```
write memory
```

Настройка исходящего подключения на Ideco NGFW Novum

Для настройки исходящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPSec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **Адрес удаленного устройства** - введите IP-адрес Cisco. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля Cisco. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере.
- **Тип аутентификации** - PSK.
- **PSK** - будет сгенерирован случайный PSK-ключ для подключения в Cisco.
- **NGFW идентификатор** - введенный ключ будет использоваться для идентификации исходящего подключения. Введите также идентификатор в Cisco.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Проверьте, что подключение установилось (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

4. Проверьте наличие трафика между туннельными интерфейсами NGFW и Cisco. Для этого в консоли Cisco или терминале NGFW используйте утилиту `ping`.
Итоговая конфигурация IKEv2 GRE over IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Ideco NGFW Novum к Cisco

```
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 2

!
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
!
!
crypto ikev2 keyring key
 peer strongswan
  address <внешний IP-адрес NGFW>
  pre-shared-key local <psk>
  pre-shared-key remote <psk>
!
!
crypto ikev2 profile ikev2profile
 match identity remote key-id <key-id>
 authentication remote pre-share
 authentication local pre-share
 keyring local key
 dpd 10 3 periodic
!
!
crypto ipsec transform-set TS esp-gcm 256
 mode transport
!
!
crypto ipsec profile ikev2TSprofile
 set transform-set TS
 set pfs group2
 set ikev2-profile ikev2profile
!
!
interface Tunnel0
 ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
 ip mtu 1400
 tunnel source GigabitEthernet 1
 tunnel destination <внешний IP-адрес NGFW>
 tunnel protection ipsec profile ikev2TSprofile
!
interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid

interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid
!
ip nat inside source list NAT interface GigabitEthernet1 overload
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
!
ip access-list extended NAT
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
```

Подключение от Cisco к Ideco NGFW Novum

Настройка IKEv2+GRE-over-IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
exit
```

3. Создайте peer (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP NGFW>
identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP NGFW> 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local key
dpd 10 3 periodic
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode transport
exit
```

6. Настройте профиль IPsec:

```
crypto ipsec profile ikev2TSprofile
set transform-set TS
set pfs group19
set ikev2-profile ikev2profile
exit
```

7. Создайте туннельный интерфейс:

```
interface Tunnel0
ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
ip mtu 1400
tunnel source GigabitEthernet 1
```

```
tunnel destination <внешний IP-адрес NGFW>
tunnel protection ipsec profile ikev2TSprofile
exit
```

8. Настройте динамическую маршрутизацию (BGP или OSPF) или статический маршрут до локальных сетей Ideco NGFW Novum:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

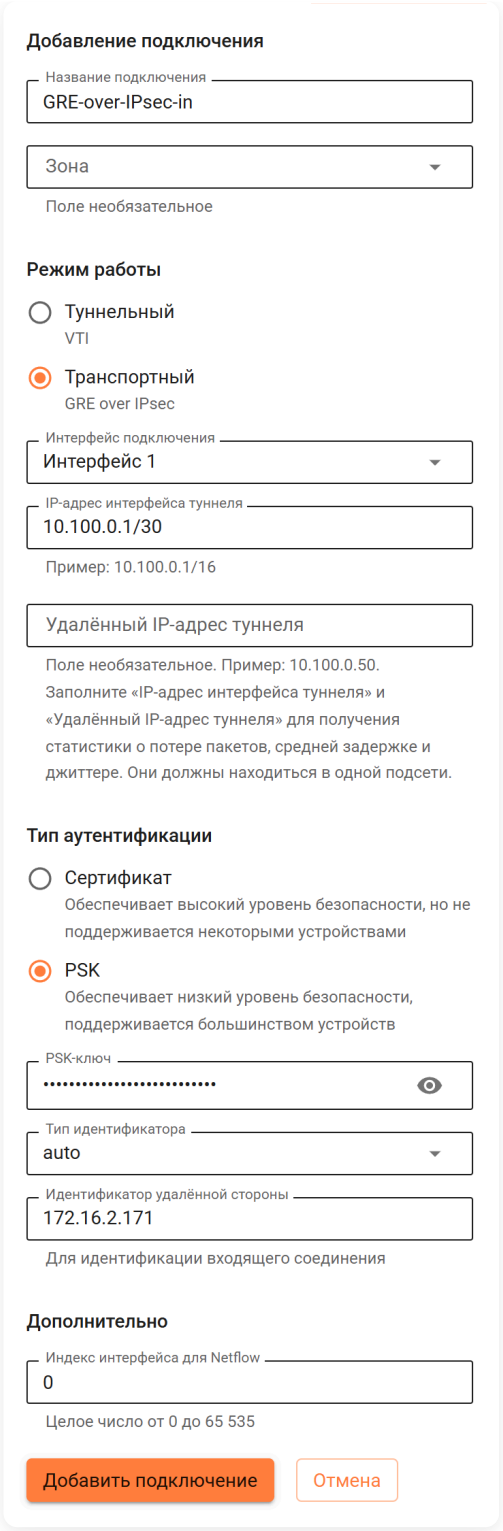
```
write memory
```

Настройка входящего подключения на Ideco NGFW Novum

Для настройки входящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Устройства(входящие подключения)**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля Cisco. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ.
- **Тип идентификатора** - keyid или auto, если Cisco передает IP-адрес вместо key-id.
- **Идентификатор удаленной стороны** - вставьте идентификатор Cisco (параметр Key ID) или IP-адрес Cisco, если Cisco передает IP-адрес вместо key-id.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Сохраните созданное подключение, затем нажмите на кнопку **Включить**.

4. Проверьте, что подключение установлено (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

5. Проверьте наличие трафика между туннельными интерфейсами NGFW и Cisco. Для этого в консоли Cisco или терминале NGFW используйте утилиту `ping`.
Итоговая конфигурация IKEv2 GRE over IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW Novum

```
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 2

!
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
!
!
crypto ikev2 keyring key
 peer strongswan
  address <внешний IP NGFW>
  identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
  pre-shared-key local <psk>
  pre-shared-key remote <psk>
!
!
crypto ikev2 profile ikev2profile
 match identity remote address <внешний IP NGFW> 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local key
!
!
crypto ipsec transform-set TS esp-gcm 256
 mode transport
!
!
crypto ipsec profile ikev2TSprofile
 set transform-set TS
 set pfs group2
 set ikev2-profile ikev2profile
!
!
interface Tunnel0
 ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
 ip mtu 1400
 tunnel source GigabitEthernet 1
 tunnel destination <внешний IP-адрес NGFW>
 tunnel protection ipsec profile ikev2TSprofile
!
interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid

interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid
!
ip nat inside source list NAT interface GigabitEthernet1 overload
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

```
!
ip access-list extended NAT
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
```

Настройка динамической маршрутизации

OSPF

Настройка на Cisco

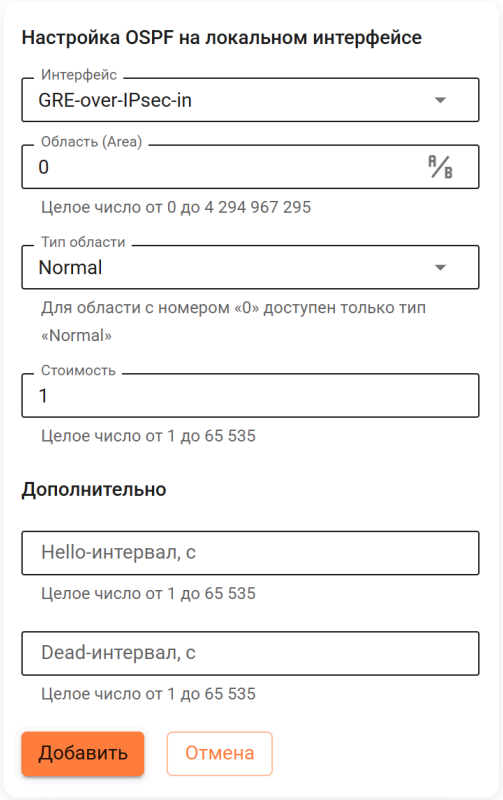
Настройте процесс OSPF на роутере (значение `area` должно совпадать на Cisco и NGFW):

```
conf t
router ospf 1
passive-interface default
 no passive-interface Tunnel0
 network <подсеть туннельного интерфейса Cisco> <обратная маска> area 0
 network <локальная подсеть Cisco> <обратная маска> area 0
exit
```

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW Novum, настроенный ранее.
- **Область (Area)** - введите номер области (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Тип области** - для области с указанным номером `area` должен быть выбран одинаковый тип на всех OSPF-соседях. Для области с номером 0 (`0.0.0.0`) допустимо указывать только один тип - **Normal**. Допустимые значения: **Normal**, **Stub**, **NSSA**:
  - **Normal Area** (обычная зона) - стандартная зона OSPF, которая получает полную информацию о маршрутах как внутри автономной системы, так и за ее пределами. В такой зоне могут находиться как маршрутизаторы, так и конечные устройства.
  - **Stub Area** (усеченная зона) - зона, в которой не принимаются внешние маршруты (Type 5 LSA), но принимаются маршруты других зон. Вместо полной информации о внешних маршрутах используется маршрут по умолчанию.
  - **NSSA** (Not-So-Stubby Area) - разновидность stub-зоны, которая может получать маршруты по умолчанию и отправлять свои маршруты в другие зоны через **ABR** (Area Border Router). В **NSSA** зоне используется специальный тип LSA (Type 7), который преобразуется в Type 5 на ABR.

- **Стоимость** - введите стоимость маршрута.
- **Hello-интервал** - укажите время между отправкой Hello-пакетов, которое варьируется от 1 до 65535 секунд. Если поле не заполнено, по умолчанию используется значение 10 секунд. Для установления соседства между устройствами интервал должен быть одинаковым для всех участников сети.
- **Dead-интервал** - укажите время, через которое сосед считается недоступным, если не получает Hello-пакеты. Диапазон значений - от 1 до 65535 секунд. Если поле не заполнено, по умолчанию в 4 раза больше, чем Hello-интервал. Для успешного соседства значение должно быть одинаковым у всех устройств в сегменте сети.

3. Нажмите **Сохранить**.

4. Включите модуль **OSPF**.

Для подключения нескольких устройств Cisco к одному Ideco NGFW Novum и передачи маршрутов между всеми устройствами:

1. Создайте для каждого Cisco Gre-over-IPsec подключение к Ideco NGFW Novum.

2. Подключите каждое устройство Cisco по OSPF.

При такой конфигурации локальные сети каждого Cisco будут доступны с Ideco NGFW Novum и других устройств Cisco.

BGP

Настройка на Cisco

Настройте процесс BGP на роутере:

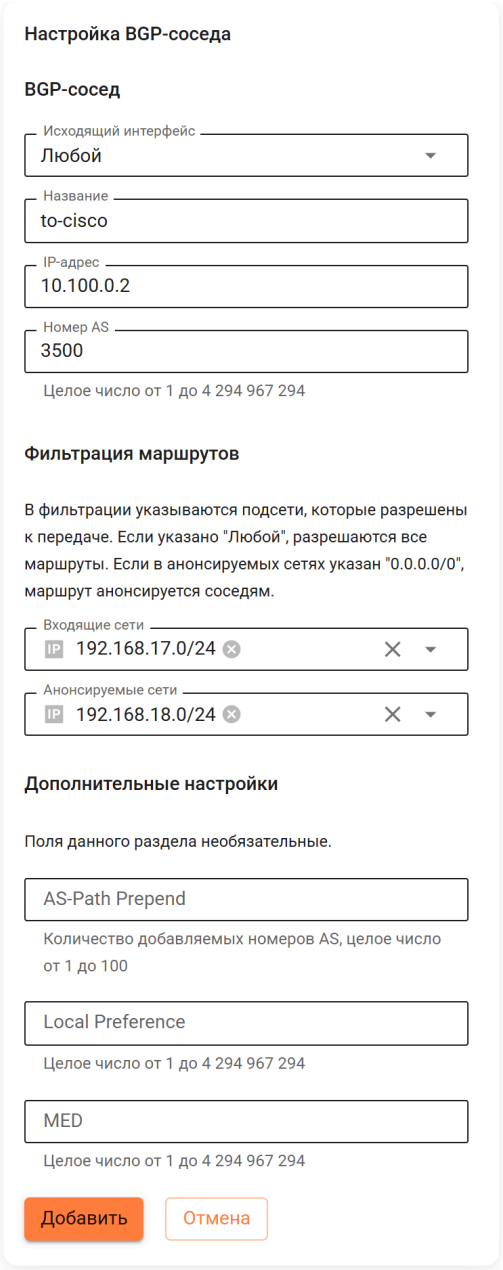
```
conf t
router bgp 3500
 neighbor <IP интерфейса туннеля NGFW> remote-as 3501
 neighbor <IP интерфейса туннеля NGFW> ebgp-multihop 2
 neighbor <IP интерфейса туннеля NGFW> update-source Tunnel0
 !
 address-family ipv4
  network <локальная подсеть Cisco> mask <маска подсети>
  neighbor <IP интерфейса туннеля NGFW> activate
 exit-address-family
```

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в поле **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:



- **Исходящий интерфейс** - выберите **Любой**.
- **IP-адрес** - укажите IP-адрес интерфейса туннеля Cisco.
- **Номер AS** - номер AS Cisco (указанный в команде `router bgp 3500`).
- **Входящие сети** - укажите локальные сети Cisco.
- **Анонсируемые сети** - укажите локальные сети Ideco NGFW Novum.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

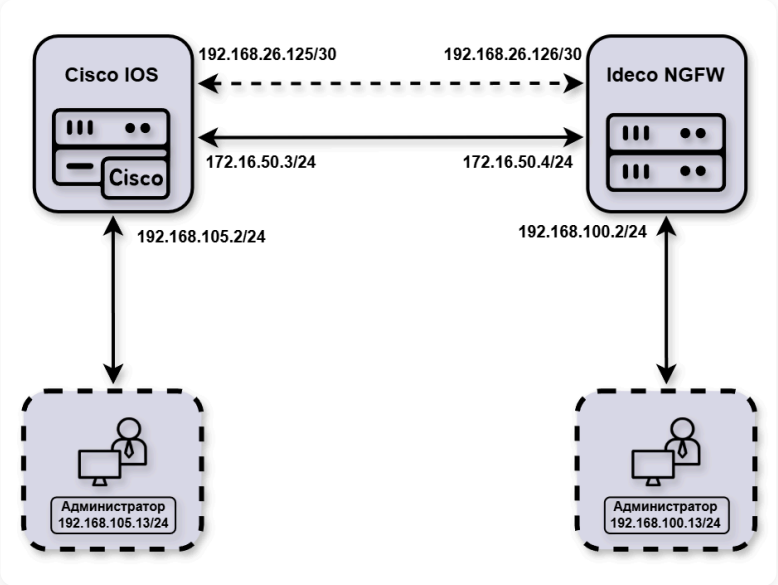
5. Включите модуль **BGP**.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Cisco IOS и Ideco NGFW Novum по route-based IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Рассмотрим процесс настройки подключения в туннельном режиме по следующей схеме:



Адресация:

- `192.168.26.125/30` - IP-адрес интерфейса туннеля NGFW.
- `192.168.26.126/30` - IP-адрес интерфейса туннеля Cisco.
- `172.16.50.3/24` - внешний IP-адрес NGFW.
- `192.168.100.2/24` - локальный IP-адрес NGFW.
- `172.16.50.4/24` - внешний IP-адрес Cisco.
- `192.168.105.2/24` - локальный IP-адрес Cisco.

Инструкция проверена на **Cisco IOS XE версии 17.3.5**. При использовании других версий Cisco IOS синтаксис отдельных команд может отличаться.

Первоначальная настройка Ideco NGFW Novum и Cisco IOS

Настройка Ideco NGFW Novum

Настройте на Ideco NGFW Novum локальный и внешний интерфейсы. Подробная информация находится в статье Первоначальная настройка.

Настройка Cisco

Для настройки Cisco через консоль выполните действия:

1. Настройка локального и внешнего интерфейса:

```
enable
configure terminal
interface gigabitEthernet 1
ip address <внешний IP-адрес Cisco> <маска подсети>
no shutdown
ip nat outside
exit
```

```
interface gigabitEthernet 2
ip address <локальный IP-адрес Cisco> <маска подсети>
no shutdown
ip nat inside
exit
```

2. Настройка DNS и добавление маршрута по умолчанию для доступа в интернет:

```
configure terminal
ip name-server <IP-адрес DNS-сервера>
ip route 0.0.0.0 0.0.0.0 <IP-адрес провайдера>
```

3. Создание access-list и NAT для доступа из локальной сети в интернет:

```
ip access-list extended NAT
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit
ip nat inside source list NAT interface gigabitEthernet 1 overload
```

4. Добавление локального администратора и настройка доступа по SSH:

```
configure terminal
username admin privilege 15 secret <пароль>
hostname <имя роутера>
ip domain name <имя домена>
crypto key generate rsa
ip ssh version 2
aaa new-model
line vty 0 4
transport input ssh
privilege level 15
exit
```

5. Сохранение настроек конфигурации:

```
write
```

Настройка route-based IPsec на Cisco

1. Создание proposal:

```
configure terminal
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создание policy:

```
crypto ikev2 policy ikev2policy
proposal ikev2proposal
exit
```

3. Создание peer:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP-адрес NGFW>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создание IKEv2 profile:

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP-адрес NGFW> <маска подсети>
identity local address <внешний IP-адрес Cisco>
authentication remote pre-share
authentication local pre-share
keyring local key
no config-exchange set send
no config-exchange set accept
no config-exchange request
exit
```

5. Настройка шифрования в esp:

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
exit
```

6. Создание ipsec profile:

```
crypto ipsec profile ikev2TSprofile
set transform-set TS
set pfs group19
set ikev2-profile ikev2profile
exit
```

7. Создание туннельного интерфейса:

```
interface Tunnel3000
ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
tunnel source gigabitEthernet 1
tunnel mode ipsec ipv4
tunnel destination <внешний IP-адрес NGFW>
tunnel protection ipsec profile ikev2TSprofile
exit
```

8. Сохранение настроек конфигурации:

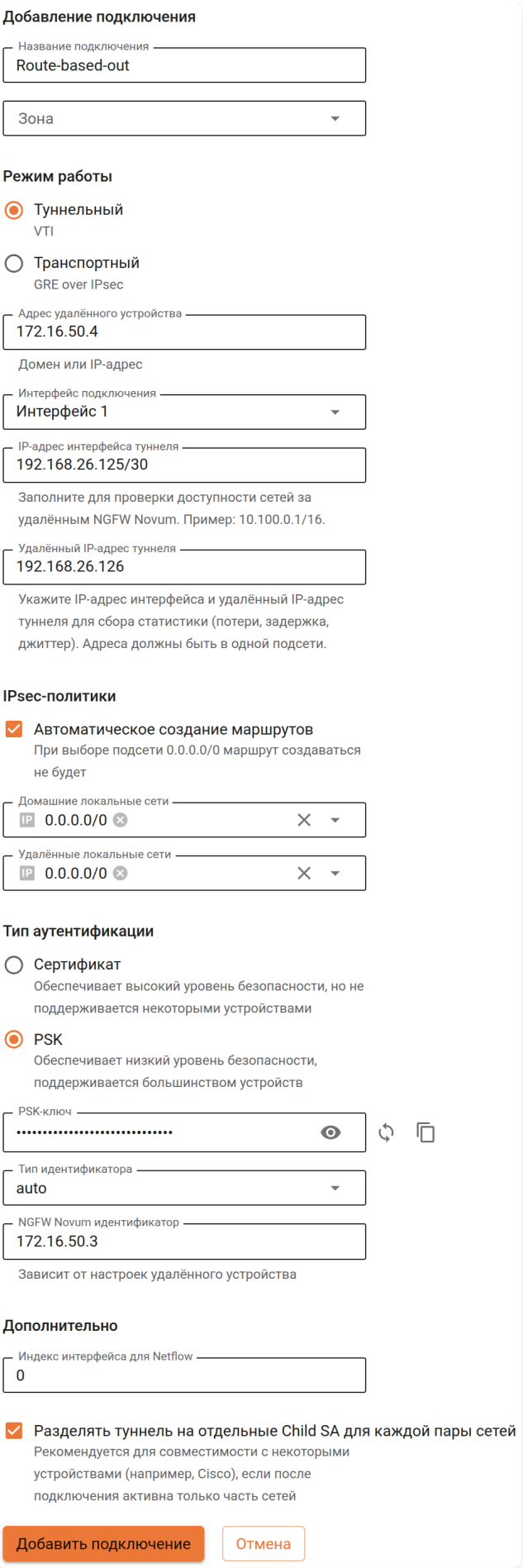
```
write
```

Настройка исходящего подключения на Ideco NGFW Novum

Для настройки исходящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы → IPsec → Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPsec подключения. Список предустановленных зон приведен в статье.

- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - введите IP-адрес Cisco. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля NGFW Novum.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Адреса должны находиться в одной подсети.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ созданный на третьем этапе в разделе **Настройка route-based IPsec на Cisco**.
- **NGFW идентификатор** - укажите внешний IP-адрес NGFW Novum.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Разделять туннель на отдельные Child SA для каждой пары сетей** - включите опцию для создания отдельного Child SA на каждую пару локальной и удаленной подсети, обеспечивая доступность всех сетей сразу после установления VPN. Актуально для совместимости с некоторыми типами устройств (например, Cisco), которые не поддерживают несколько селекторов трафика в одном Child SA.

3. Проверьте, что подключение установилось (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

4. Проверьте наличие трафика между локальными сетями (TCP и web).
Итоговая конфигурация route-based IPsec на Cisco должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW Novum

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy ikev2policy
 proposal ikev2proposal

crypto ikev2 keyring key
 peer strongswan
  address <внешний IP-адрес NGFW>
  pre-shared-key local <psk>
  pre-shared-key remote <psk>

crypto ikev2 profile ikev2profile
 match identity remote address <внешний IP-адрес NGFW> <маска подсети>
 identity local address <внешний IP-адрес Cisco>
 authentication remote pre-share
 authentication local pre-share
 keyring local key
 no config-exchange set send
 no config-exchange set accept
 no config-exchange request

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile ikev2TSprofile
 set transform-set TS
 set pfs group19
 set ikev2-profile ikev2profile
```



В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **IPsec**

Подключение pfSense к Ideco NGFW Novum по IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

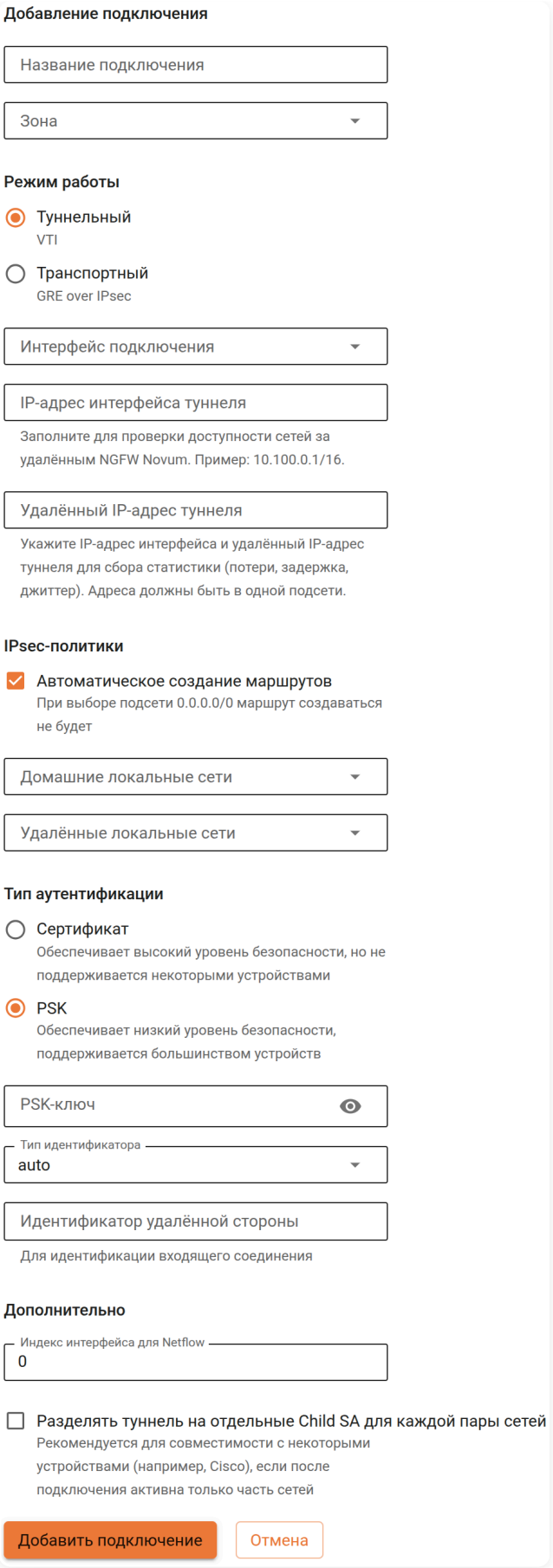
Объединяемые локальные сети не должны пересекаться!

Настройка входящего подключения

Для настройки Ideco NGFW Novum следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Входящие подключения**.

2. Добавьте новое подключение:



- **Название подключения** - любое.
- **Зона** - укажите зону для добавления IPSec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Тип аутентификации** - выберите PSK.
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения.
- **Идентификатор удаленной стороны** - введите значение, которое будет использоваться для идентификации pfSense.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW Novum.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

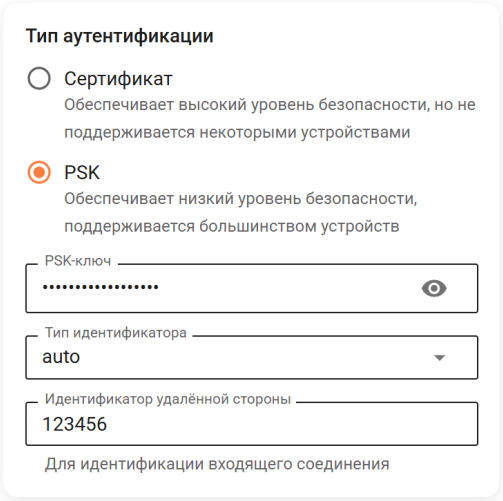
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.

3. Сохраните созданное подключение, нажмите на кнопку **Включить**.

4. Скопируйте значение идентификатора удаленной стороны одним из способов:

В интерфейсе NGFW

В **Сервисы** → **IPsec** → **Входящие подключения** в поле **Идентификатор удаленной стороны**:



Через терминал

На Ideco NGFW Novum в папке `/run/ideco-ipsec-backend/strongswan/swanctl/conf.d/` будет сгенерирован конфигурационный файл. Необходимо перейти в консоль и открыть на редактирование файл вида `device_<номер>.conf`. Из этого файла необходимо скопировать значение строки `id` (идентификатор удаленной стороны):

```
        children {
            device2utm_1_fqdn-0 {

                policies = no

                start_action = none
                esp_proposals = aes256gcm16-curve25519-ecp256-modp4096-modp2048-modp1024,aes256-sha512-sha384-sha256-curve25519-ecp256-modp4096-modp2048-modp1024

                local_ts = 192.168.101.0/24
                remote_ts = 192.168.201.0/24

                dpd_action = clear
                close_action = clear

                # ICS-24156 Вместо дефолтных 10% от 1ч, увеличиваем rand_time до 20%,
                # чтобы уменьшить вероятность одновременного рекеинга и появления дубликатов CHILD_SA
                rand_time = 720s

                updown = /usr/bin/ideco-ipsec-updown
            }
        }
        local {
            auth = psk
        }
        remote {
            # Во входящих подключениях нам не известен заранее IP удаленного устройства,
            # поэтому в качестве идентификатора подключения используем указанный идентификатор.
            # В исходящих подключениях мы таким образом даем себя идентифицировать.
            # ( https://wiki.strongswan.org/projects/strongswan/wiki/IdentityParsing )
            id = 123456
            auth = psk
        }
    }
}
secrets {
    ike-device2utm_1_fqdn-0 {
        # Hex encoded PSK aaaaaaaaa:',
        id = 123456
        secret = 0x61616161616161616161
    }
}
```

5. Перейдите к настройке pfSense, предварительно записав значение строки `id` (идентификатор удаленной стороны).

Настройка pfSense

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите в **VPN** → **IPsec** → **Tunnels**.

2. Добавьте новое подключение:

- **Description** - любое.
- **Key Exchange version** - IKEv2.
- **Internet Protocol** - IPv4.
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW Novum.
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW Novum.
- **Authentication Method** - Mutual PSK.
- **My identifier и Peer identifier** - сюда вставьте значение строки `id` на Ideco NGFW Novum (см. шаг 4 в настройке Ideco NGFW Novum).
- **Pre-Shared Key** - вставьте PSK-ключ, который ранее прописывали на Ideco NGFW Novum.
- **Encryption Algorithm** - используйте следующие параметры:
  - **Algorithm** - AES256-GCM.
  - **Key length** - 128 bit.
  - **Hash** - SHA256.
  - **DH Group** - Elliptic Curve 25519-256.

Все остальные значения можно оставить по умолчанию.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2. Здесь укажите:

- **Encryption Algorithm** - используйте следующие параметры:
  - **Algorithm** - AES256-GCM.
  - **Key length** - 128 bit.
  - **Hash** - SHA256.
  - **DH Group** - Elliptic Curve 25519-256.
- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW Novum.
- **Remote Network** - локальную сеть Ideco NGFW Novum, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. Разрешите хождение трафика между локальными сетями pfSense и Ideco NGFW Novum в настройках файрвола pfSense (перейдите в **Firewall** → **Rules** → **IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW Novum и pfSense).

Обращаем внимание на раздел файрвола WAN - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

7. Теперь перейдите в **Status** → **IPsec** (там должно появиться созданное подключение), нажмите **Connect VPN**.

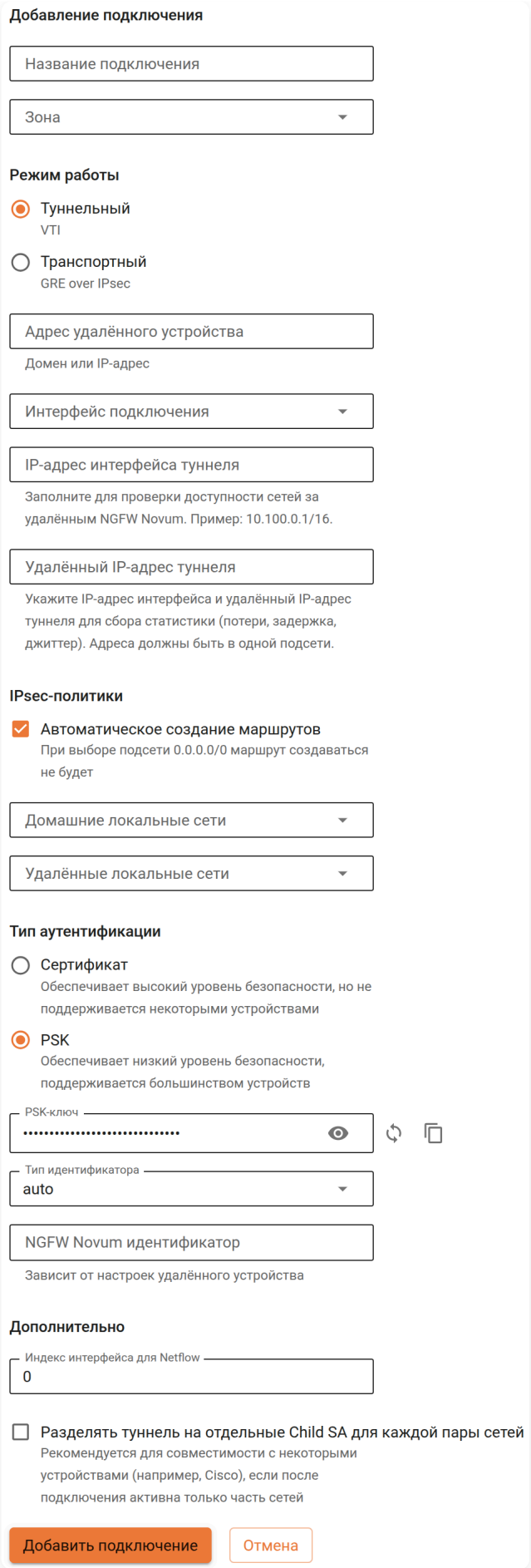
Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое указано в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

Настройка исходящего подключения

Для настройки Ideco NGFW Novum следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPSec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.

- **Адрес удаленного устройства** - укажите внешний IP-адрес pfSense. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW Novum, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW Novum.
- **Тип аутентификации** - выберите тип PSK.
- **PSK-ключ** - укажите PSK-ключ, который будет использоваться для подключения.
- **Тип идентификатора** - выберите auto.
- **Идентификатор NGFW** - введите значение, которое будет использоваться для идентификации Ideco NGFW Novum на pfSense.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Настройка pfSense

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите в **VPN > IPsec > Advanced Options** и в поле **Child SA Start Action** выберите параметр **None (Responder Only)**.

2. Добавьте новое подключение:

- **Key Exchange version** - IKEv2.
- **Internet Protocol** - IPv4.
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW Novum.
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW Novum.
- **Description** - любое.
- **Authentication Method** - Mutual PSK.
- **My identifier** - My ip address.
- **Peer identifier** - KeyID tag. Введите идентификатор удаленной стороны, т. е. Ideco NGFW Novum.
- **Pre-Shared Key** - введите PSK-ключ.
- **Encryption Algorithm**:
  - Для **Ideco UTM версии 10.0 и Ideco NGFW Novum версии 16.0 и новее** используйте следующие параметры:
    - **Algorithm** - AES256-GCM.
    - **Key length** - 128 bit.
    - **Hash** - SHA256.
    - **DH Group** - Elliptic Curve 25519-256.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2 и укажите следующие значения:

- **Encryption Algorithm**:
  - **Для Ideco UTM версии 10.0 и Ideco NGFW Novum версии 16.0 и новее** используйте следующие параметры:
    - **Algorithm** - AES256-GCM.
    - **Key length** - 128 bit.
    - **Hash** - SHA256.
    - **DH Group** - Elliptic Curve 25519-256.
- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW Novum.
- **Remote Network** - локальную сеть Ideco NGFW Novum, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. В настройках файрвола pfSense перейдите в **Firewall → Rules → IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW Novum и pfSense.

7. Обратите внимание на раздел файрвола **WAN** - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

8. Перейдите в **Status → IPsec** (там должно появиться созданное подключение), нажмите на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое указали в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **IPsec**

Подключение Kerio Control и Ideco NGFW Novum по IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Объединяемые локальные сети не должны пересекаться!

Предварительная настройка Kerio Control

1. По умолчанию Kerio Control использует IKEv1 для создания подключений к сторонним устройствам. Включить IKEv2 можно через консоль, выполнив действия:

- Подключиться к Kerio Control по SSH.
- Перейти в папку `/var/winroute`.
- Открыть на редактирование файл `winroute.cfg`.
- В нем найти раздел, начинающийся с текста `<table name="Firewall">`.
- В этом разделе найти строку `<variable name="IKEVersion">ikev1</variable>` и изменить в ней `ikev1` на `ikev2`.
- После этого требуется перезагрузить сервер и убедиться, что изменения в настройках сохранились.

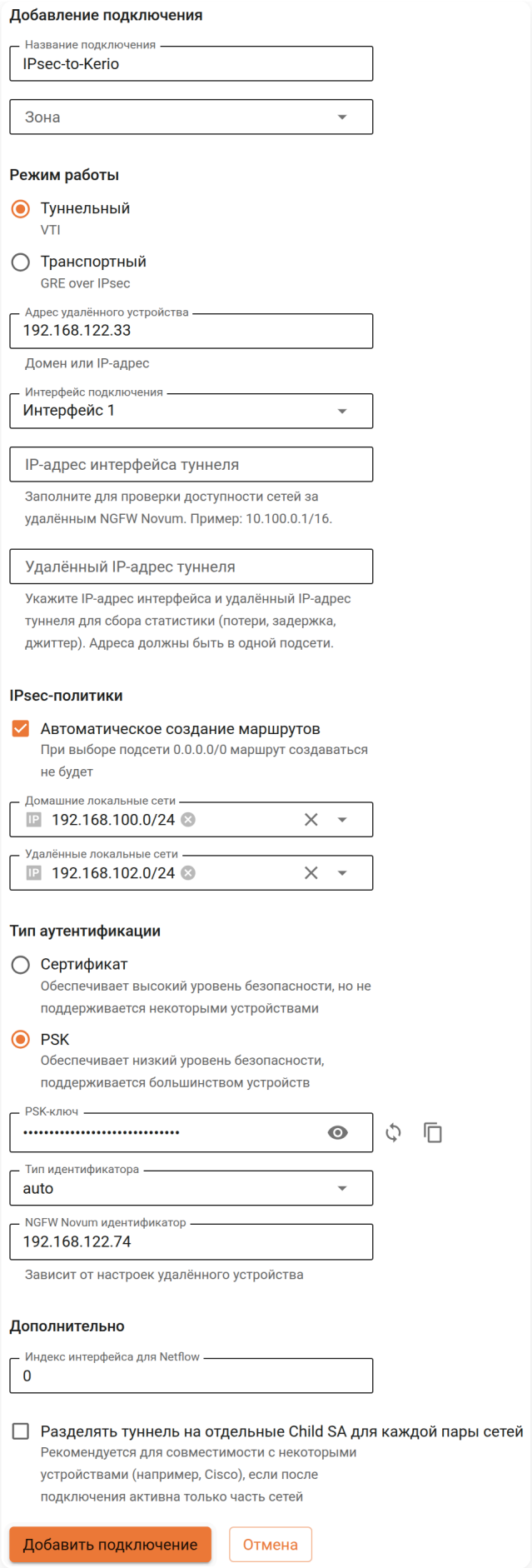
2. В разделе **Правила трафика** разрешите трафик VPN-служб.

Подключение от Ideco NGFW Novum к Kerio Control

Настройка исходящего подключения на Ideco NGFW Novum

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение и заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPsec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.

- **Адрес удаленного устройства** - укажите внешний IP-адрес Kerio Control. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW Novum, которая будет видна из подсети Kerio Control.
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW Novum.
- **Тип аутентификации** - выберите тип PSK.
- **PSK-ключ** - укажите PSK-ключ, который будет использоваться для подключения.
- **Тип идентификатора** - выберите auto.
- **Идентификатор NGFW** - укажите IP-адрес внешнего интерфейса Ideco NGFW Novum, который будет использоваться для подключения.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

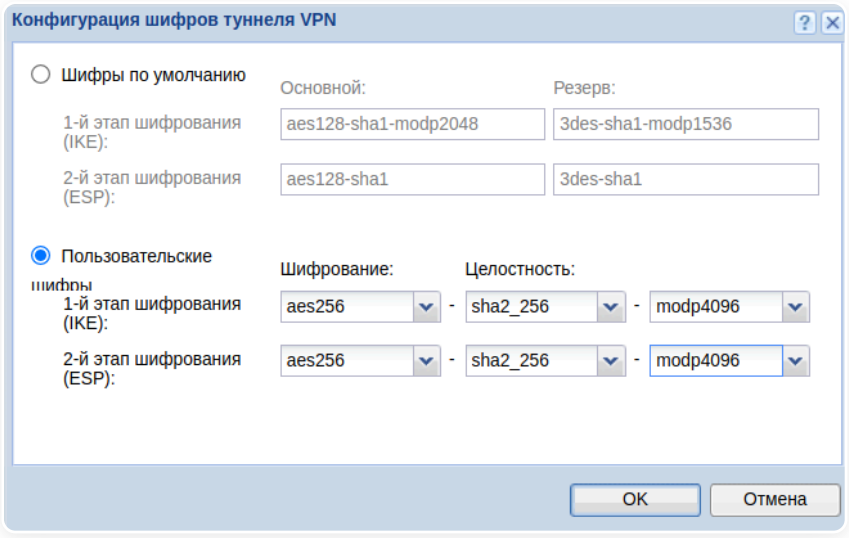
Настройка завершена, теперь переходим к настройке Kerio Control.

Настройка входящего подключения на Kerio Control

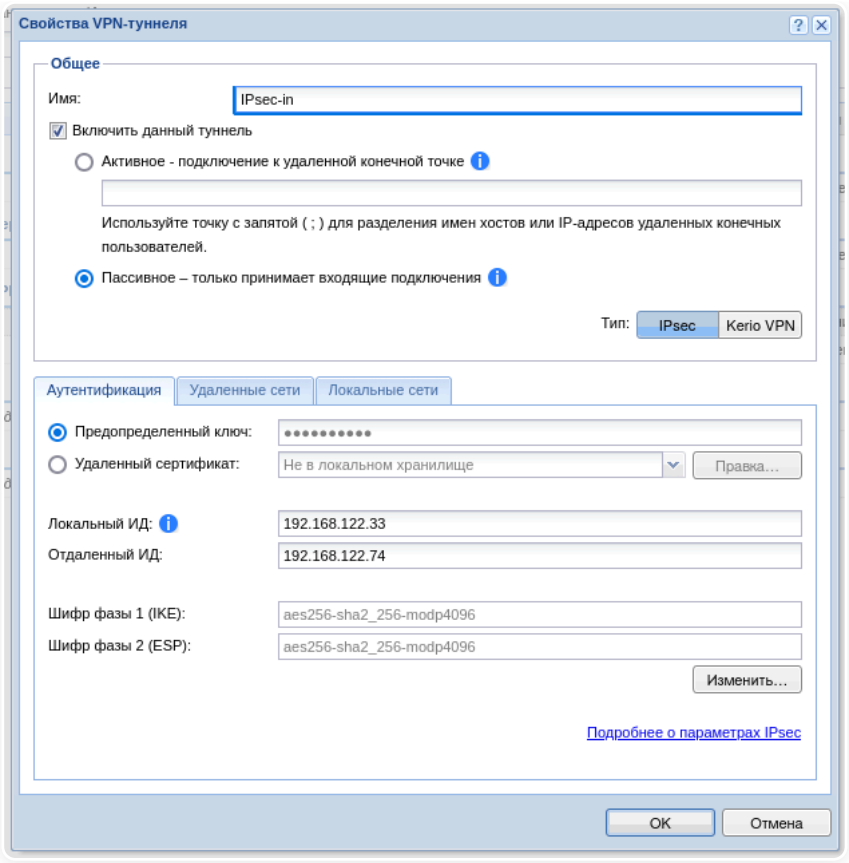
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель...**.

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec.
- **Имя** - произвольное.
- **Включить данный туннель**.
- Тип **Пассивное**.
- **Предопределенный ключ** - введите PSK-ключ, который был указан при создании подключения на Ideco NGFW Novum.
- **Локальный ИД** - укажите IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения.
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW Novum.
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



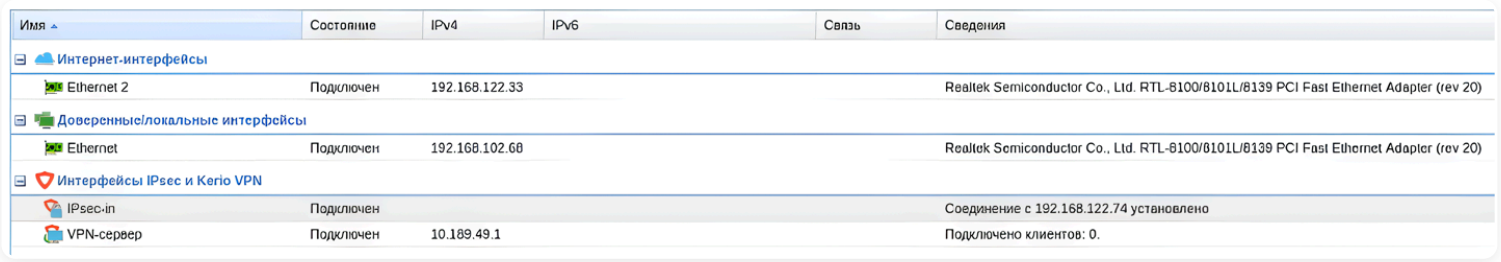
Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW Novum, которая будет видна из подсети Kerio Control.

4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW Novum, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице:



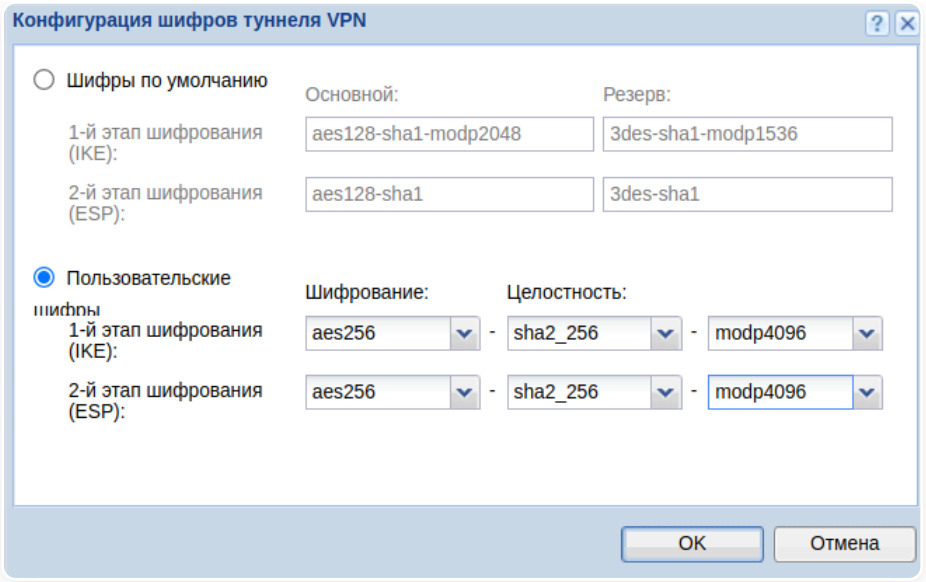
Подключение от Kerio Control к Ideco NGFW Novum

Настройка исходящего подключения на Kerio Control

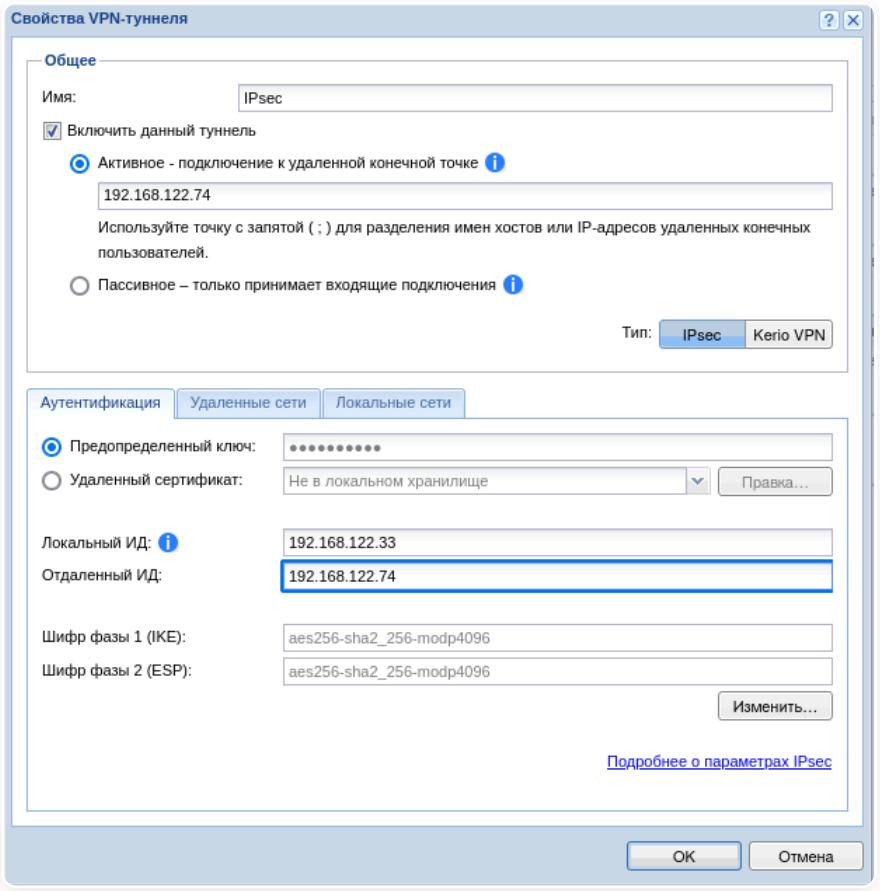
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель...**.

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec.
- **Имя** - произвольное.
- **Включить данный туннель**.
- Выберите тип **Активное** и в поле под ним пропишите IP-адрес внешнего интерфейса Ideco NGFW Novum, который будет использоваться для подключения.
- **Предопределенный ключ** - введите PSK-ключ, который будет использоваться для подключения.
- **Локальный ИД** - укажите ключ, который будет задан в поле **Идентификатор NGFW** при настройке входящего подключения на Ideco NGFW Novum, или IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения. **Предпочтительное значение - имя хоста Kerio**.
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW Novum, который будет использоваться для подключения.
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW Novum, которая будет видна из подсети Kerio Control.

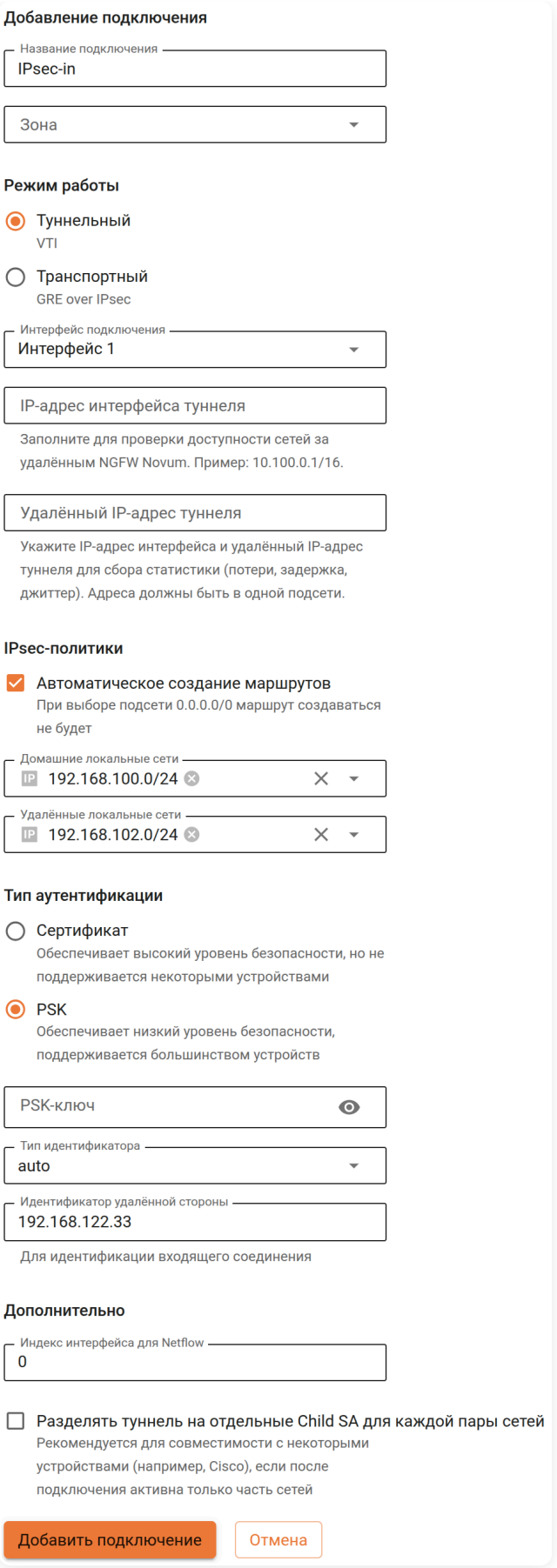
4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW Novum, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице.

Настройка входящего подключения на Ideco NGFW Novum

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Входящие подключения**.

2. Добавьте новое подключение и заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW Novum, которая будет видна из подсети Kerio Control.
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW Novum.
- **Тип аутентификации** - выберите тип PSK.
- **PSK-ключ** - введите PSK-ключ, который был указан при создании подключения в Kerio.
- **Тип идентификатора** - выберите auto.
- **Идентификатор удаленной стороны** - укажите **Локальный ИД**, указанный при настройке исходящего подключения на Kerio.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. IP-адреса должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

Настройка завершена.

При возникновении проблем обратите внимание на настройки файрвола Kerio Control.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **IPsec**

ГОСТ VPN

Практические руководства по работе с ГОСТ VPN в Ideco NGFW

Пример генерации ключей и сертификатов ГОСТ VPN

Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Пример генерации ключей и сертификатов ГОСТ VPN

Выполните команды:

1. Установите OpenSC (pkcs11-tool):

```
dnf install opensc
```

2. Создайте в текущей директории файл `openssl.conf`:

```
openssl_conf = openssl_init

[ openssl_init ]
engines = engine_section

[ engine_section ]
gost = gost_section

[ gost_section ]
dynamic_path = /usr/lib64/librtengine.so
pkcs11_path = /usr/lib64/librtpkcs11ecp.so
default_algorithms = CIPHERS, DIGEST, PKEY

[ crypto_policy ]
MinProtocol = TLSv1.2
MaxProtocol = TLSv1.3
Ciphersuites =  TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_SHA256:TLS_GOSTR34
CipherString = @SECLEVEL=1:kEECDH:kRSA:kEDH:kPSK:kDHEPSK:kECDHEPSK:kRSAPSK:-aDSS:-3DES:!DES:!RC4:!RC2:!IDEA:-SEED:!eNULL:!aNU
```

3. Включите поддержку ГОСТ в openssl:

```
export OPENSSL_CONF=openssl.conf
```

Далее введите команды для работы с сертификатами (в примере пин-код токена `12345678`).

4. Создайте закрытый ключ и CA сертификат:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out ca.key
openssl req -addext basicConstraints=CA:TRUE,pathlen:0 -x509 -new -nodes -days 3650 -key ca.key -out ca.crt -subj "/C=RU/ST=M
```

Здесь и далее в примере используются:

- `id = 3231 (hex) = 21 (dec)` - для локальных сертификатов;
- `id = 3230 (hex) = 20 (dec)` - для CA сертификатов.

5. Установите сертификат на токен:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l --pin 12345678 -y cert -w ca.crt --id 3230 --label GOST_CA_Cert
```

6. Сгенерируйте ключевую пару на токене:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen --key-type GOSTR3410-2012-256:A -l --pin 12345678 --id 3231 --
```

Важные параметры:

- `usage-derive`;
- `usage-decrypt`;
- `key-type GOSTR3410-2012-256:A`.

7. Сделайте запрос на сертификат (система запросит пин-код):

```
openssl req -addext basicConstraints=CA:FALSE,pathlen:0 -new -keyform engine -key "pkcs11:id=21" -engine rtengine -out server
```

Вместо домена `.test` указывайте реальный домен.

8. Подпишите сертификат:

```
openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -md_gost12_256
```

9. Установите сертификат на токен:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l --pin 12345678 -y cert -w server.crt --id 3231 --label GOST_Server_Cert
```

10. Если требуется протестировать, выгрузите сертификат из токена:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -p 12345678 -r --type cert --id 3231 | openssl x509 -inform der > server
```

Полезные ссылки

- **ГОСТ VPN**

Прокси

Практические руководства по настройке прокси-сервера в Ideco NGFW

Настройка Ideco NGFW в качестве прокси с одним интерфейсом

Перейти ›

Настройка программы Proxifier для прямых подключений к прокси-серверу

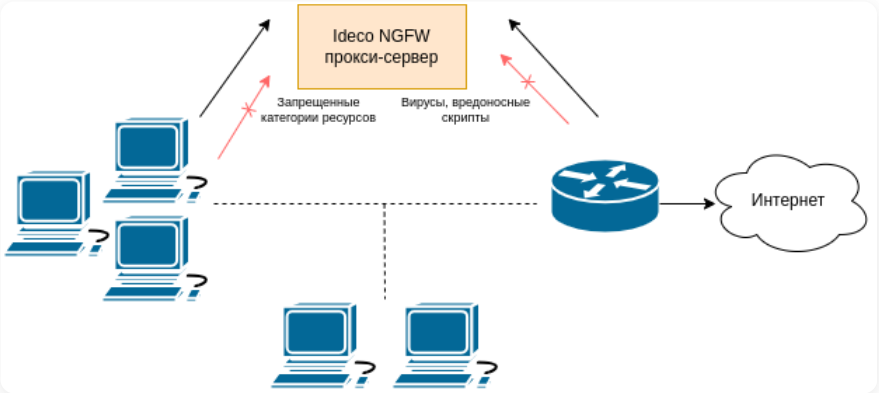
Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка Ideco NGFW Novum в качестве прокси с одним интерфейсом

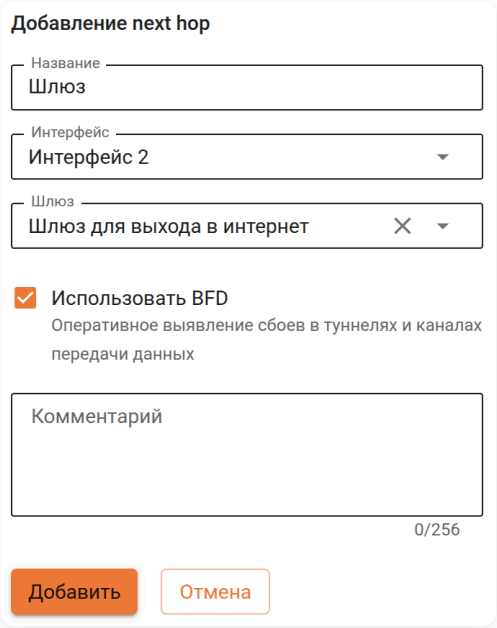
Функциональность доступна в **Классическом** и **Системном контекстах**.



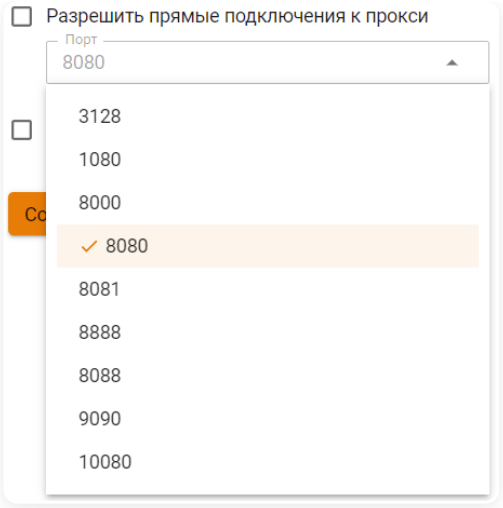
При необходимости можно использовать Ideco NGFW Novum в качестве прокси-сервера с прямыми подключениями клиентов к прокси. Для этого выполните действия:

1. Создайте интерфейс с ролью LAN через локальное меню сервера. Подробнее в статье.

2. Перейдите в **SD-WAN** → **Next hop** и добавьте шлюз для настроенного интерфейса:



3. Разрешите прямые подключения к прокси-серверу в разделе **Сервисы** → **Прокси**, выбрав нужный порт из списка:



Если прямое подключение к прокси требуется только части клиентских устройств или части локальных интерфейсов, то создайте INPUT-правило **Межсетевого экрана**. Пример приведен ниже.

При использовании запрещающих все правил:

- Убедитесь, что разрешающие правила для прокси расположены выше в таблице.
- Проверьте, что трафик служебной подсети `169.254.1.0/30` не ограничен FORWARD-правилами **Межсетевого экрана**.

Для учета, контроля и проверки веб-трафика на вирусы, требуется соблюдение следующих условий:

- Локальная подсеть не пересекается с внешним интерфейсом NGFW Novum.
- У сервера Ideco NGFW Novum есть доступ в интернет.
- На клиентских устройствах указан адрес веб-прокси (в настройках прокси-сервера в браузерах).

Пример настройки INPUT-правила

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**, создайте **разрешающее** правило и включите:

- **Протокол** - TCP.
- **Источник**:
  - **Зона источника** - локальный интерфейс или конкретные интерфейсы.
  - **Адрес** - IP-адреса или подсети разрешенных пользовательских устройств.
- **Назначение**:
  - **Адрес** - IP-адрес локального интерфейса NGFW.
  - **Порт назначения** - порт, указанный в настройках **Прокси**.
- **Действия** - **Разрешить**.

2. Если необходимо ограничить доступ к прокси, создайте **запрещающее** INPUT-правило и поместите под разрешающим:

- **Протокол** - TCP.
- **Источник**:
  - **Зона источника** - локальный интерфейс или конкретные интерфейсы.
  - **Адрес** - **Любой**. Доступ будет запрещен всем, кроме адресов в разрешающем правиле.
- **Назначение**:
  - **Адрес** - IP-адрес локального интерфейса NGFW.
  - **Порт назначения** - порт, указанный в настройках **Прокси**.
- **Действия** - **Запретить**.

Настройка прямого подключения к прокси на клиентских устройствах

Для настройки выполните действия:

1. Укажите IP-адрес локального интерфейса Ideco NGFW Novum в качестве веб-прокси в локальной сети на клиентских устройствах.

2. В настройках прокси на клиентской машине укажите порт для прямых подключений к прокси (возможен выбор портов из списка: 3128, 1080, 8000, 8080, 8888, 8081, 8088, 10080).

Если в настройках программы под ОС Windows или macOS X нет возможности указать прокси-сервер, воспользуйтесь сторонним ПО для маршрутизации всего трафика рабочей станции на прокси-сервер. Такую возможность предоставляет программа **Proxifier**, которую можно настроить для прямых подключений к прокси. Для настройки воспользуйтесь статьей.

Полезные ссылки

- **Прокси**

Настройка программы Proxifier для прямых подключений к прокси серверу

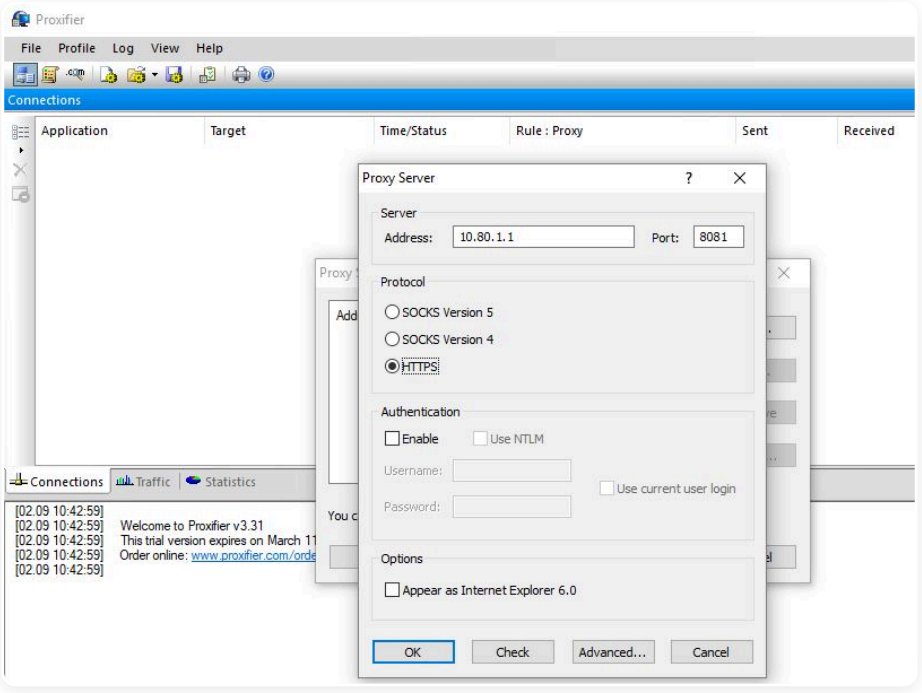
Функциональность доступна в **Классическом** и **Системном контекстах**.

Скачать Proxifier можно с сайта разработчика.

Настройка

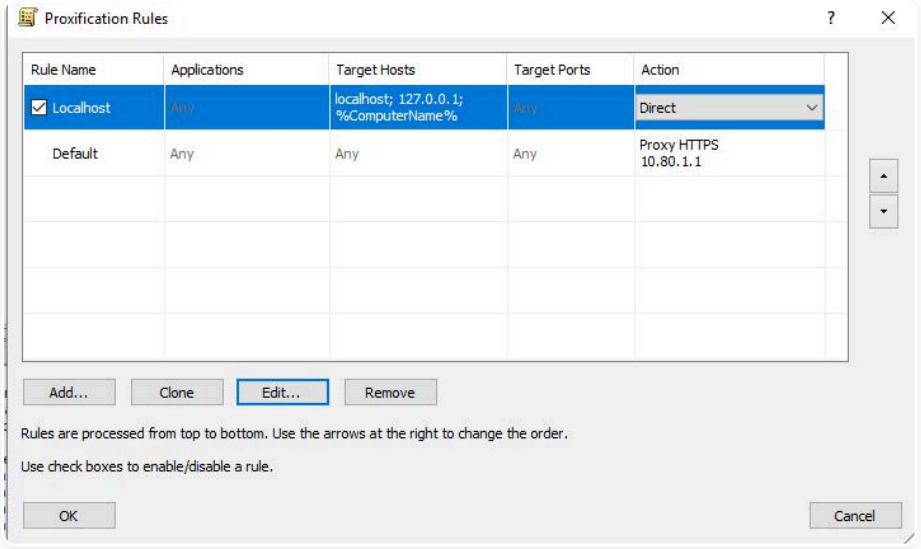
Выполните стандартные настройки браузера для прямых подключений к прокси-серверу, а затем настройте программу для перенаправления остального трафика на прокси-сервер.

Пропишите в настройках прокси-сервера в Proxyfier IP-адрес локального интерфейса Ideco NGFW Novum и порт, указанный в настройке прокси для прямых подключений (см. документацию по прокси-серверу). Тип протокола: HTTPS. Настройки авторизации указывать необязательно:



После добавления прокси-сервера ответьте утвердительно на вопросы о создании правил перенаправления трафика на него.

Либо эти настройки можно отредактировать позже:



Настройка закончена, программы будут выходить в интернет через заданный прокси-сервер.

Полезные ссылки

- **Прокси**

Правила трафика

Практические руководства по настройке правил трафика в Ideco NGFW

Блокировка популярных ресурсов

Настройка блокировки популярных интернет-ресурсов

Перейти >

Контент-фильтр

Настройка блокировки через Контент-фильтр

Перейти >

Межсетевой экран

Настройка правил Межсетевого экрана

Перейти >

Ручная корректировка GeoIP

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Контент-фильтр

Практические руководства по настройке Контент-фильтра в Ideco NGFW

Блокировка чат-ботов

Настройка блокировки чат-ботов в Контент-фильтре

Перейти >

Настройка HTTP-метода

Пример настройки HTTP-метода в Контент-фильтре

Перейти >

Настройка MIME-типов

Пример настройки MIME-типов в Контент-фильтре

Перейти >

Блокировка загрузки файлов в файлообменники

Настройка блокировки загрузки файлов в файлообменники в Контент-фильтре

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

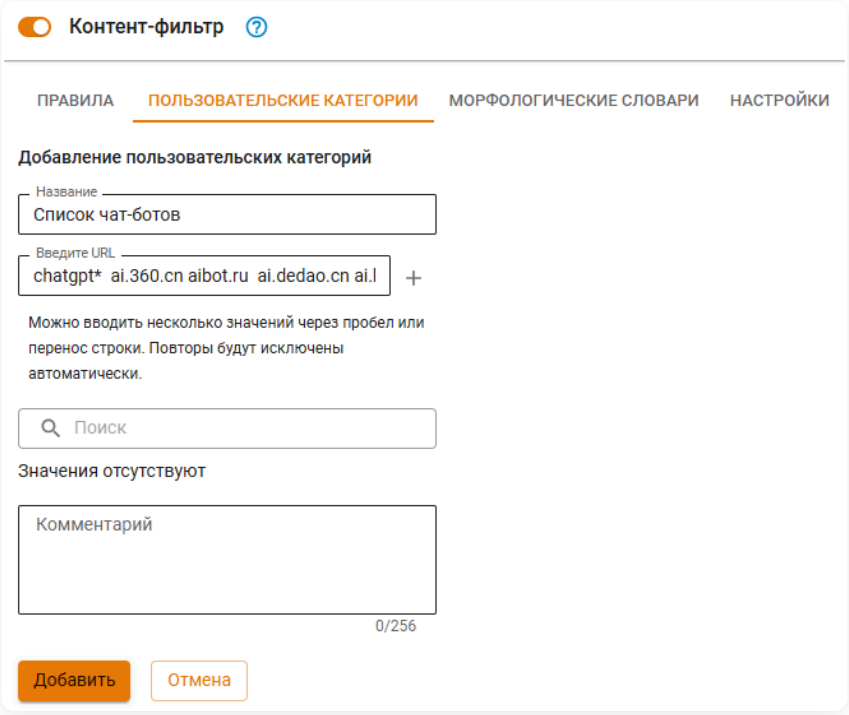
OK

Блокировка чат-ботов

Для блокировки ресурсов, которые взаимодействуют с чат-ботами, необходимо создать правило в **Контент-фильтре**:

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Пользовательские категории**.

2. Добавьте новую категорию и заполните поля:



- **Название** - введите любое название.
- **URL** - скопируйте и вставьте список URL из блока ниже.
- **Комментарий** - заполнение не обязательно.

Список URL

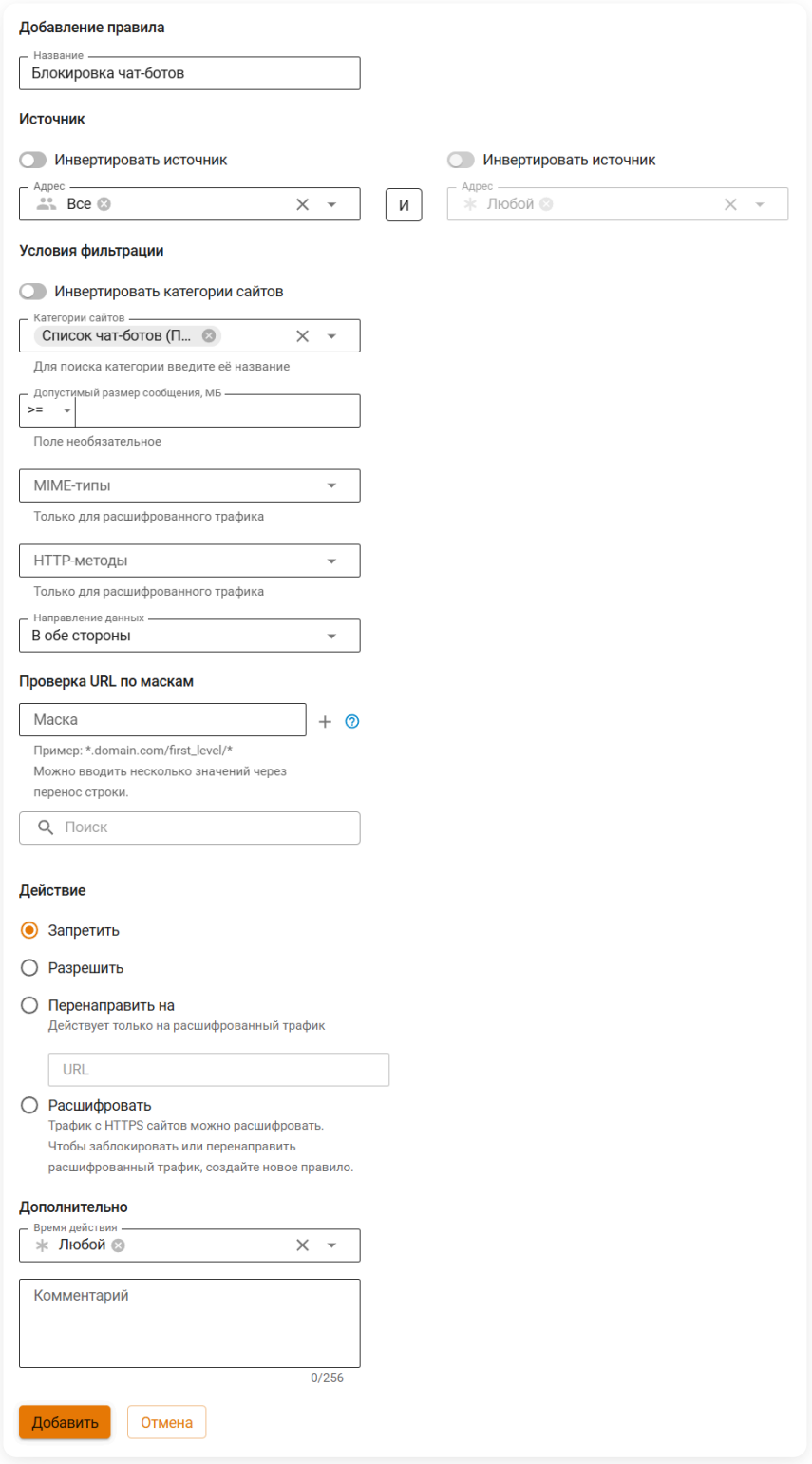
```
chatgpt*
ai.360.cn
aibot.ru
ai.dedao.cn
ai.ls
aiservice.vercel.app
aitianhu.com
anse.app
anthropic.com
b.ai-huan.xyz
bard.google.com
bettergpt.chat
bing.com
chadgpt.ru
character.ai
chat4gpt.ru
chat9.yqcloud.top
chat.acytoo.com
chataigpt.org
chat.ai-open.ru
chatboxai.app
chat.dfehub.com
chat.getgpt.world
chatglm.cn
chatgp.ru
chat.gpt4free.io
```

```
chatgpt4rus.ru
chatgpt.ai
chatgptbot.ru
chat-gpt.com
chatgptfree.ai
chat-gpt-free.ru
chatgptlogin.ac
chatgpt-me.ru
chat-gpt-na.ru
chatgptnarusskom.ru
chat-gpt.org
chatgpt.org
chatgpt.pro
chat-gpt.ru
chatgpt-telegram.com
chatgptweb.ru
chathub.gg
chatinfo.ru
chat.lmsys.org
chat.openai.com
chat.ramxn.dev
chat.su
claude.ai
crfm.stanford.edu
deepai.org
easychat-ai.app
itbabushka.com
forefront.com
freechatgpt.chat
free-chatgpt.ru
free.easychat.work
gpt2.ru
gpt4all.io
gpt-chatbot.ru
gptchatbot.ru
gptchatly.com
gpt-gm.h2o.ai
gptgo.ai
gpt-open.ru
gptschat.ru
gradio.app
h2o.ai
huggingface.co
iask.ai
liaobots.com
liftweb.ru
lmsys.org
macgpt.com
mashagpt.ru
moss.fastnlp.top
neice.tiangong.cn
openai.ru
openai-gpt.ru
openai-chat-gpt.ru
open-assistant.io
opencat.app
petals.ml
play.vercel.ai
poe.com
ru-chatgpt.ru
rugpt.chat
sdk.vercel.ai
supertest.lockchat.app
tenchat.ru
theb.ai
timeai.ru
tongyi.aliyun.com
tools.zmo.ai
trychatgpt.ru
wewordle.org
xinghuo.xfyun.cn
```

```
yandex-gpt.com
yandex-gpt.ru
yiyan.baidu.com
you.com
zhpt.tech
```

4. Сохраните категорию.

3. Перейдите в **Правила** и добавьте новое правило с действием **Запретить**:



Полезные ссылки

- **Правила**
- **Описание категорий Контент-фильтра**

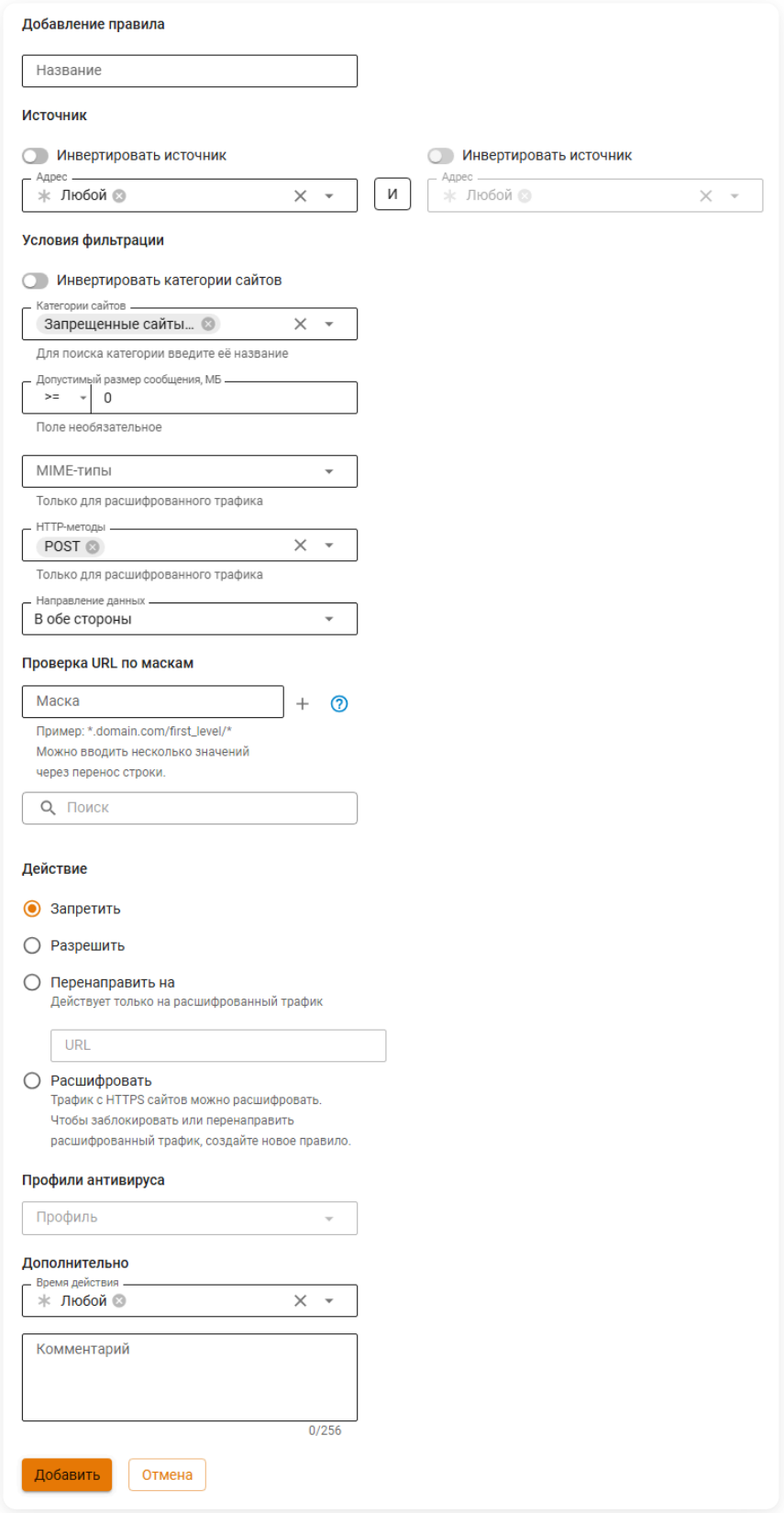
- **Контент-фильтр**

Настройка HTTP-метода

Пример. Необходимо запретить пользователям вводить данные на запрещенных сайтах.

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**.

2. Заполните поля:



- **Адрес** - выберите пользователей, для которых будет работать правило.
- **Категории сайтов** - выберите категорию сайтов, для которых должно работать правило, например, **Запрещенные сайты**.
- **HTTP-методы** - выберите метод `POST`, чтобы запретить отправку данных на определенный ресурс.
- Выберите **Запретить**, чтобы правило работало как запрещающее.

При сохранении правила сайты будут открываться, но пользователь не сможет отправить данные (например, заполнить форму обратной связи или ввести логин и пароль).

Полезные ссылки

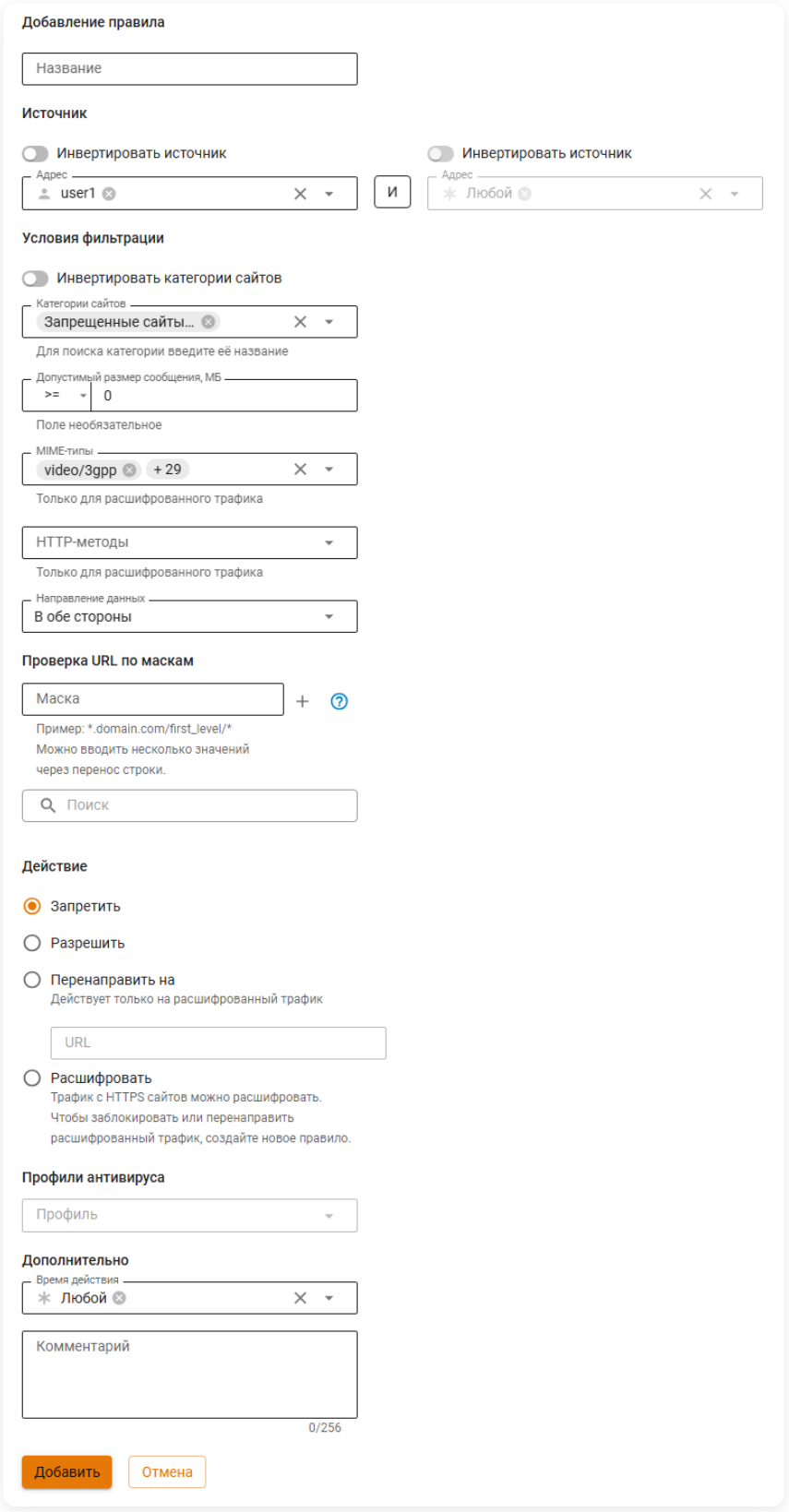
- **Настройка фильтрации HTTPS**

Настройка MIME-типов

Пример. Необходимо запретить конкретному пользователю (например, user1) воспроизводить видеоконтент на запрещенных сайтах.

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**.

2. Заполните поля, как на скриншоте:



- В поле **Категории сайтов** укажите предварительно созданную пользовательскую категорию **Запрещенные сайты**.
- В поле **MIME-типы** выберите все форматы группы **Video**.
- Примените действие правила **Запретить**.

При сохранении правила сайт откроется, если трафик не заблокирован другим правилом, но видеоконтент не воспроизведется.

Полезные ссылки

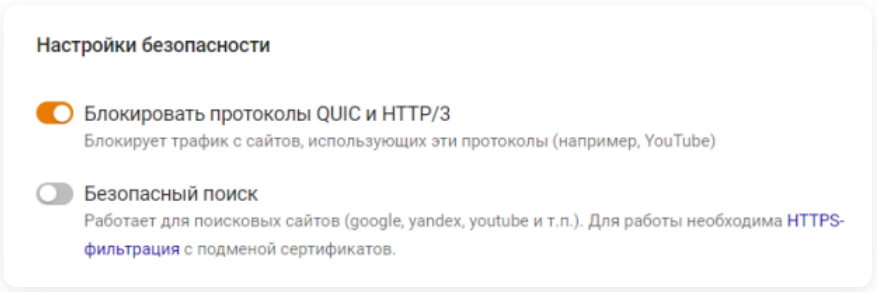
- **Настройка фильтрации HTTPS**

Блокировка загрузки файлов в файлообменники

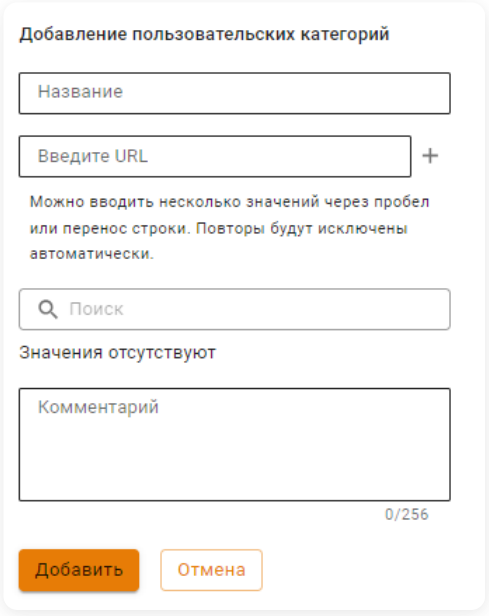
Блокирование этой категории требует особой настройки правил **Контент-фильтра**. В случае с файлообменниками расшифровки трафика может быть недостаточно у категорий: **Файлообменники, Файловые хранилища, Файловые архивы** и **Загрузка файлов в файлообменники**.

Чтобы заблокировать загрузку файлов в облака через браузер, выполните действия:

1. Включите **Блокировку протоколов Quic/HTTP3** в **Контент-фильтр** → **Настройки**:



2. Создайте пользовательскую категорию для расшифровки трафика и укажите домены нужных файлообменников, используя маску `example.com`:



3. Создайте правило, расшифровывающее трафик созданной в пункте 2 категории:



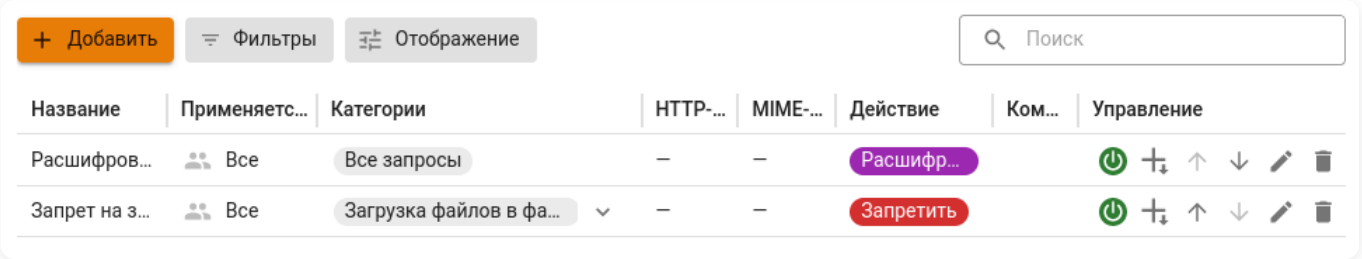
4. Ниже создайте запрещающее правило для категории **Загрузка файлов в файлообменник**:



5. Проверьте, работает ли блокировка: с устройства пользователя, для которого настроена, зайдите на сайты нужных файлообменников и попробуйте загрузить файлы.

Если загрузка проходит, то:

- Добавьте в пользовательскую категорию домены файлообменников, используя любые варианты масок: `subdomain.example.com`, `*.subdomain.example.com`, `subdomain.example.com/home`, `*.example.com`.
- Создайте в **Контент-фильтре** правило, расшифровывающее весь трафик пользователя, а ниже - правило, запрещающее загрузку файлов в файлообменники:



Если не удалось выполнить настройку, то обратитесь в Техническую поддержку.

Полезные ссылки

- **Контент-фильтр**
- **Описание категорий Контент-фильтра**

Межсетевой экран

Практические руководства по настройке правил Межсетевого экрана в Ideco NGFW

Как разрешить доступ к ресурсам в ограниченной сети

Примеры настройки правил для разрешения доступа к конкретным ресурсам при ограниченном интернете

Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

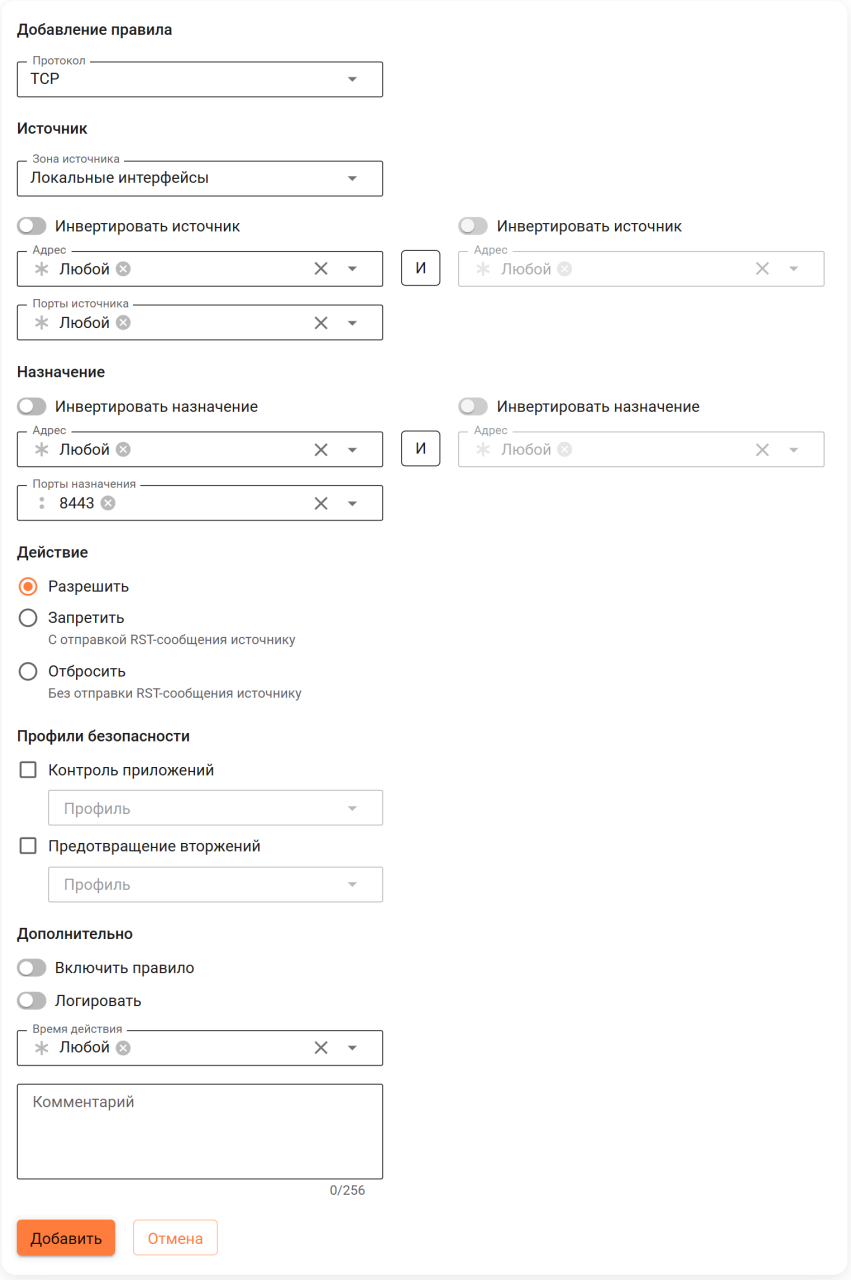
OK

Как разрешить доступ к ресурсам в ограниченной сети

Разрешить доступ к веб-интерфейсу Ideco NGFW Novum из локальной сети

Пример. Необходимо ограничить доступ ко всем внутренним ресурсам Ideco NGFW Novum, кроме веб-интерфейса администратора Ideco NGFW Novum.

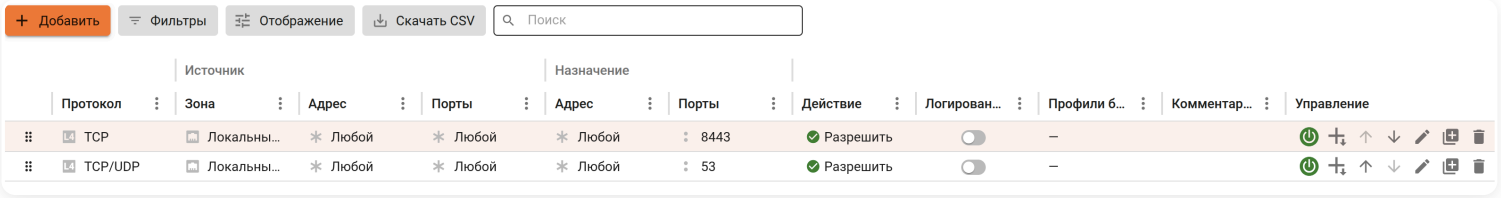
1. В **Правила трафика** → **Межсетевой экран** → **INPUT** создайте разрешающее правило, заполнив поля:



- **Протокол** - протокол транспортного уровня TCP.
- **Зона источника** - можно выбрать только один источник, для каждого источника создается отдельное правило. Выберите значение **Локальные интерфейсы**, чтобы разрешить доступ из локальной сети.
- **Адрес источника** - при необходимости укажите учетную запись пользователя или IP-адрес, которому необходимо разрешить доступ к веб-интерфейсу Ideco NGFW Novum.
- **Порт** - 8443.

Включите правило и нажмите **Добавить**.

2. Если Ideco NGFW Novum используется как DNS-сервер или включен перехват пользовательских DNS-запросов, необходимо в таблице INPUT создать правила для протоколов TCP и UDP, разрешающие подключение из локальной сети на порт 53:



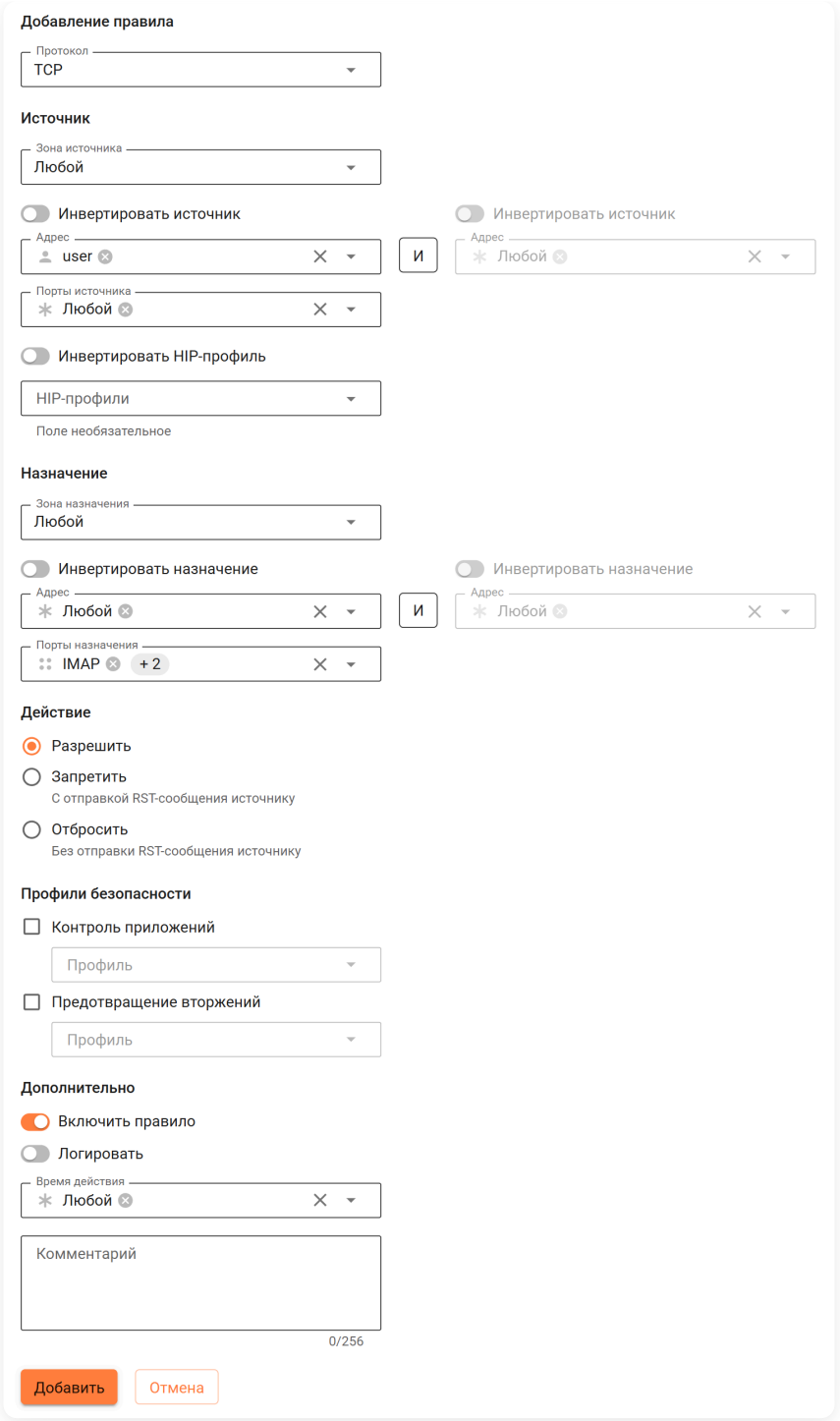
3. Создайте запрещающее весь трафик правило INPUT. При создании правила доступна опция **Включить правило** в разделе **Дополнительно**. Не включайте правило, пока не убедитесь, что в таблице разрешающее правило находится выше запрещающего.

При потере доступа к веб-интерфейсу Ideco NGFW Novum воспользуйтесь опцией **Полный доступ**.

Разрешить доступ к почтовым сервисам конкретному пользователю

Пример. Необходимо ограничить весь транзитный трафик всем пользователям, но разрешить доступ к внешним почтовым сервисам пользователю user.

1. В **Правила трафика** → **Межсетевой экран** → **FORWARD** создайте разрешающее правило, заполнив поля:



- **Протокол** - протокол транспортного уровня TCP.
- **Адрес источника** - user.
- **Порты назначения** - IMAP, POP3, MAIL (порты, используемые для передачи почты по протоколам POP3, IMAP, SMTP в т.ч. защищенных версий).

Включите правило и нажмите **Добавить**.

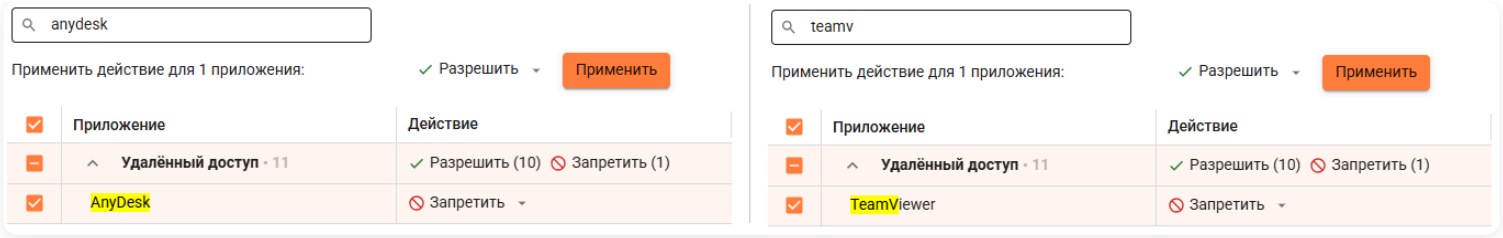
2. Создайте запрещающее весь трафик правило FORWARD. В таблице поместите разрешающее правило выше запрещающего.

Разрешить трафик из локальной во внешнюю сеть, но запретить конкретные приложения

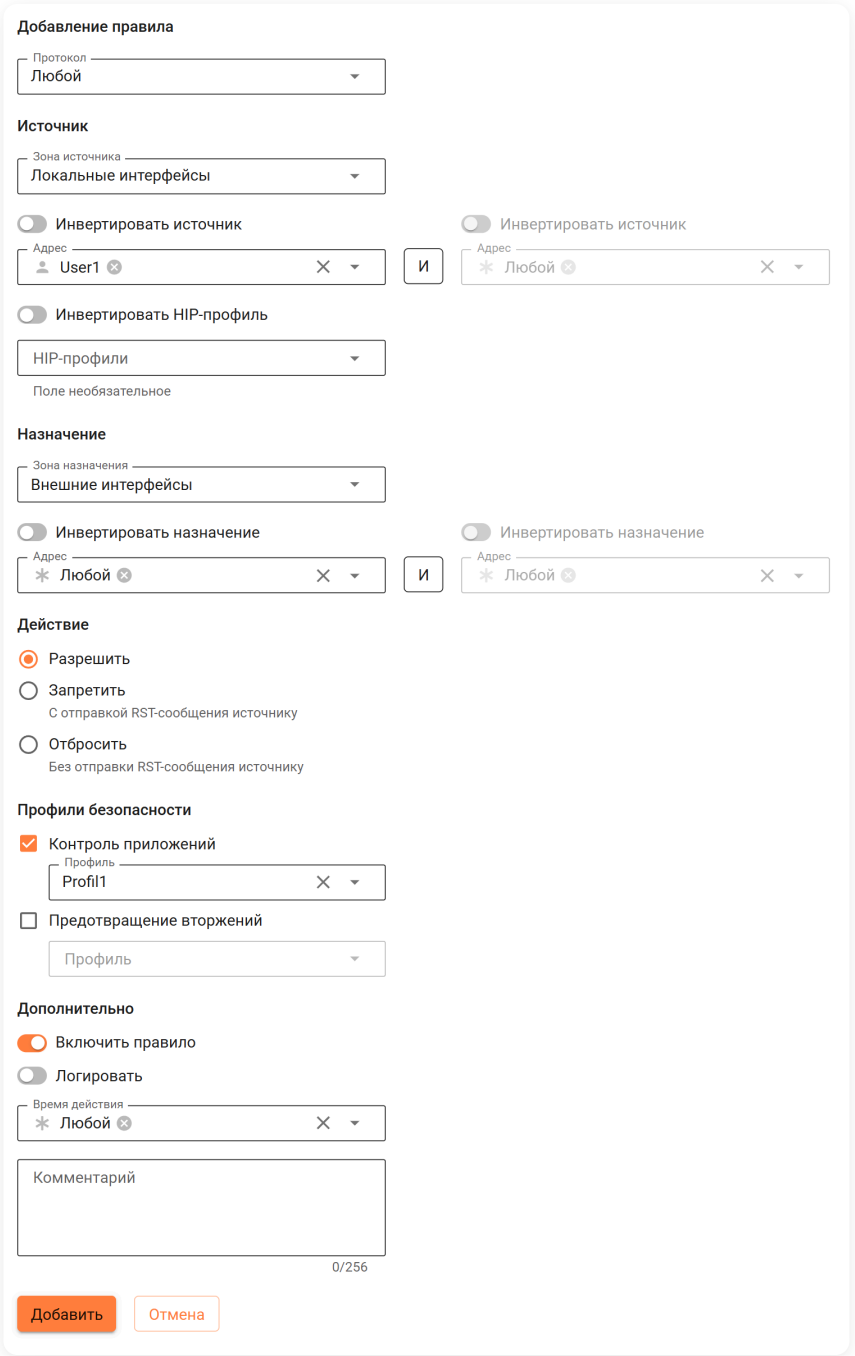
Пример. Необходимо ограничить весь транзитный трафик, но разрешить трафик из локальной во внешнюю сеть. При этом нужно запретить доступ пользователю `User1` к приложению удаленного доступа AnyDesk, а пользователю `User2` - к TeamViewer.

Выполните действия:

1. В разделе **Профили безопасности** → **Контроль приложений** создайте профили (например, `Profil1` и `Profil2`), запрещающие доступ к AnyDesk и TeamViewer:



2. В разделе **Правила трафика** → **Межсетевой экран** → **FORWARD** добавьте разрешающее правило для `User1`, заполнив поля:

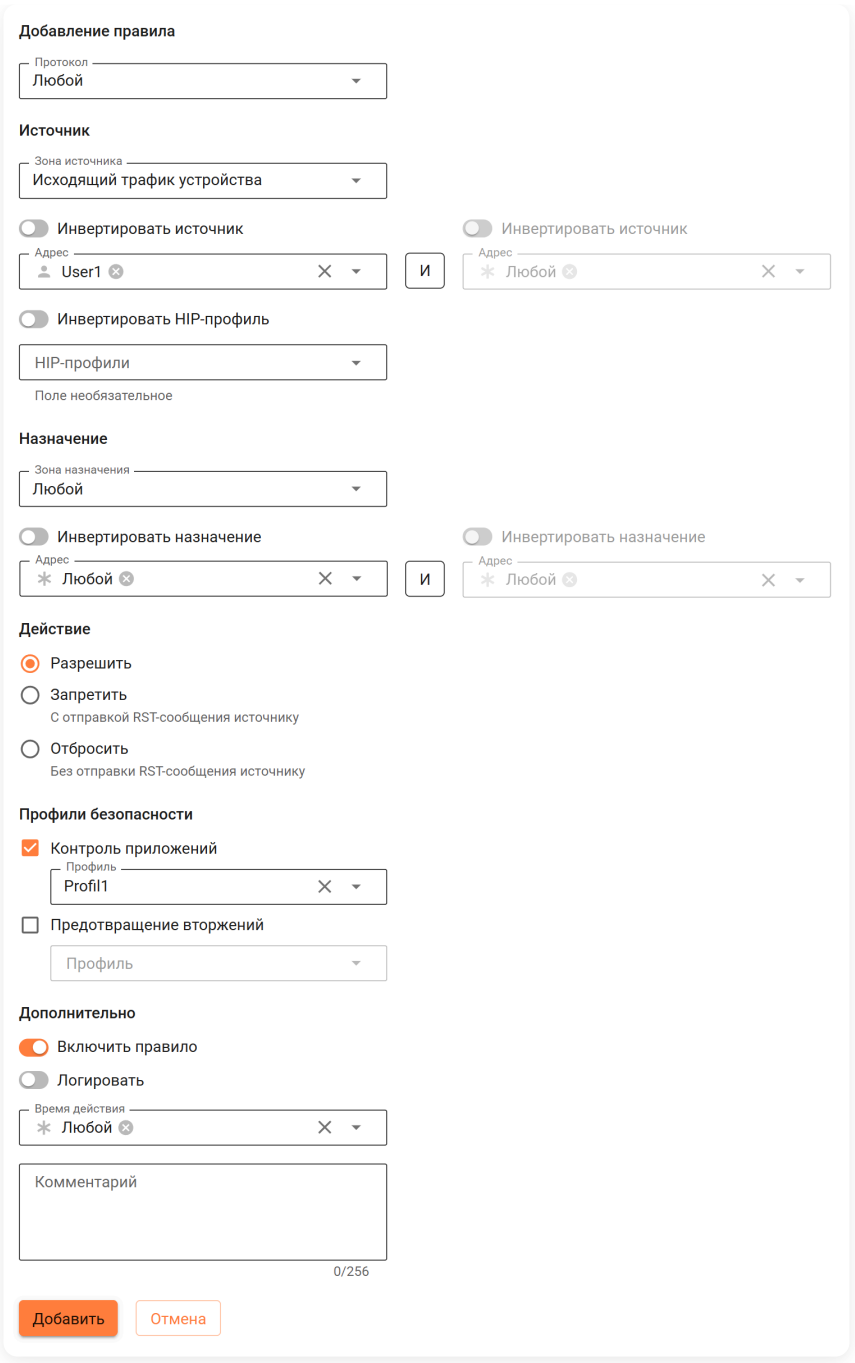


- **Протокол** - выберите **Любой**.
- **Зона источника** - выберите **Локальные интерфейсы**, чтобы разрешить доступ из локальной сети.
- **Адрес** - выберите пользователя `User1`.
- **Зона назначения** - выберите **Внешние интерфейсы**, чтобы разрешить доступ во внешнюю сеть.
- **Профили безопасности** - укажите профиль **Контроля приложений** `Profil1`, созданный в шаге 1.

Включите правило и нажмите **Добавить**.

3. По аналогии с шагом 2 добавьте разрешающее правило для `User2` с профилем **Контроля приложений** `Profil2`.

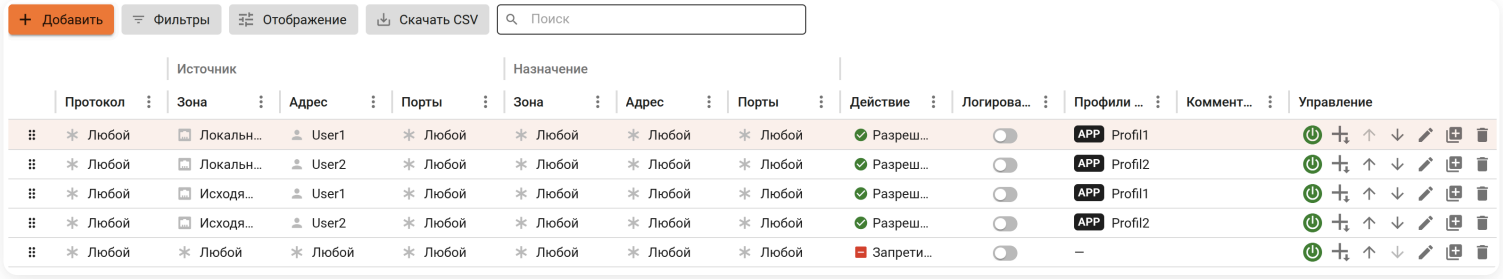
4. Добавьте правило, разрешающее трафик для специальной зоны источника **Исходящий трафик устройства** для `User1`:



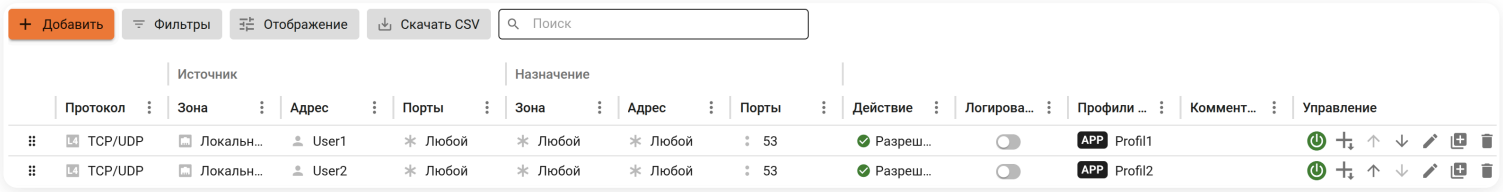
- **Протокол** - выберите **Любой**.
- **Зона источника** - выберите **Исходящий трафик устройства**, необходимо для работы прямого и прозрачного прокси, веб-трафика.
- **Адрес** - выберите пользователя `User1`.
- **Зона назначения** - выберите **Любой**.
- **Профили безопасности** - укажите профиль **Контроля приложений** `Profil1`.

5. По аналогии с шагом 4 добавьте разрешающее правило для `User2` с профилем **Контроля приложений** `Profil2`.

6. Создайте запрещающее весь трафик правило FORWARD. В таблице поместите разрешающие правила выше запрещающего:



7. Если в разделе **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку он направляется в INPUT:



Полезные ссылки

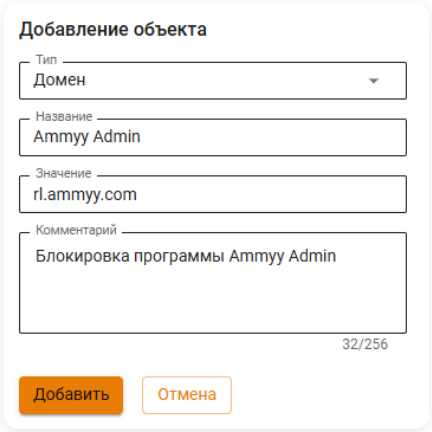
- **Межсетевой экран**
- **Примеры создания правил межсетевого экрана**

Блокировка популярных ресурсов

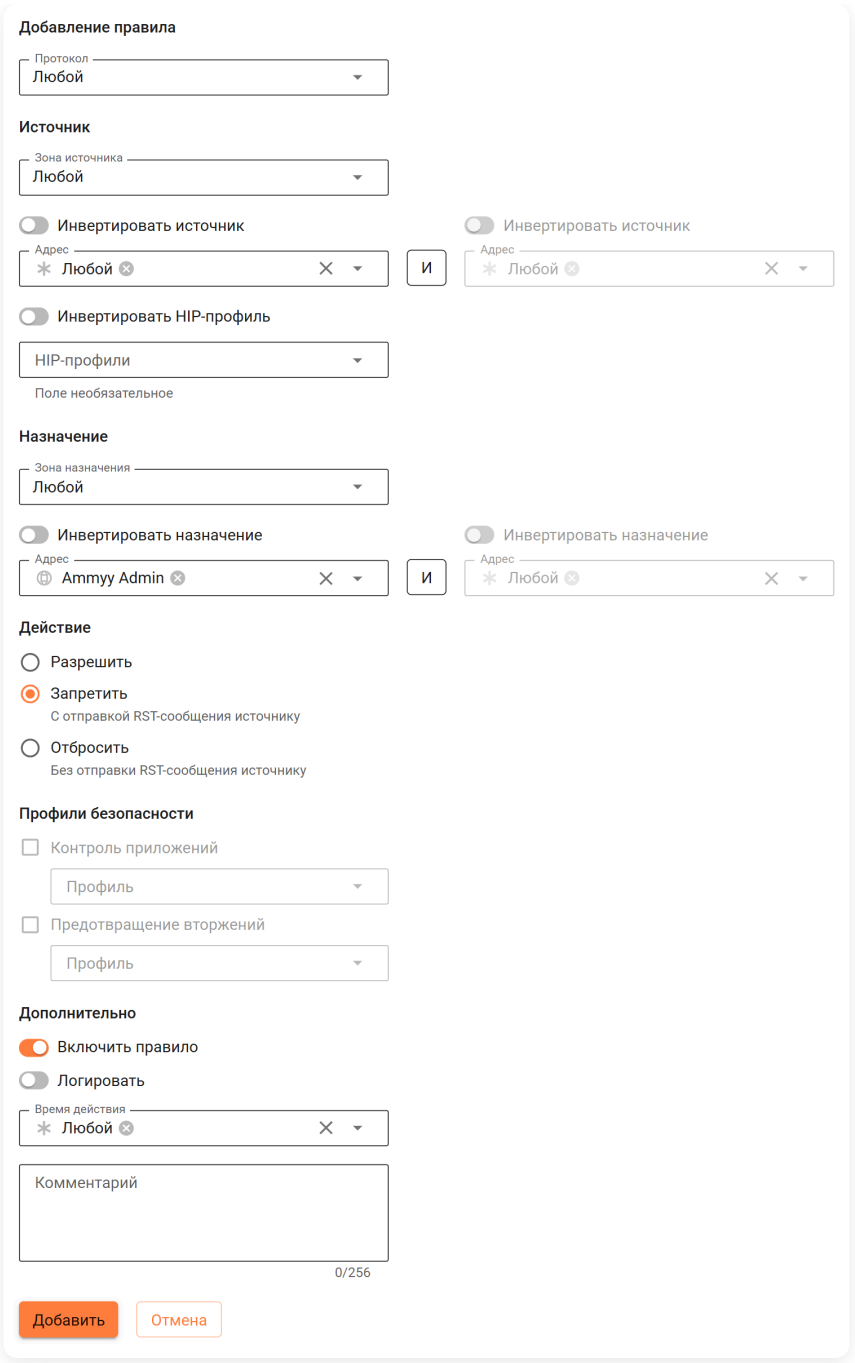
Блокировка Ammyy Admin

Ammyy Admin - это система удаленного доступа и администрирования. Чтобы заблокировать систему, выполните следующие настройки:

1. Откройте раздел **Правила трафика** → **Объекты** и создайте объект типа **Домен** с доменным именем rl.ammyy.com:



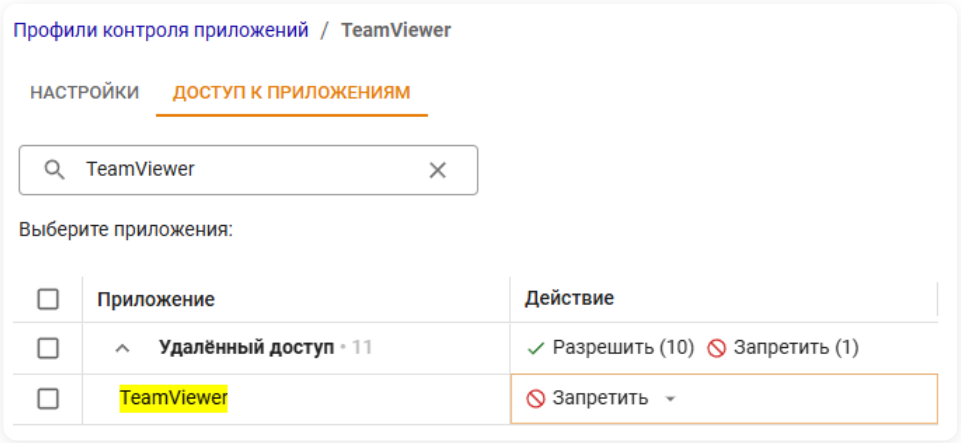
2. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**, создайте и включите правило запрета для нужных пользователей или групп. В поле **Назначение** выберите объект, созданный в пункте 1:



Блокировка TeamViewer

TeamViewer - это программное обеспечение для удаленного доступа и управления компьютерами. TeamViewer можно заблокировать с помощью Контроля приложений.

1. Перейдите в **Профили безопасности** → **Контроль приложений**. Создайте новый профиль для TeamViewer с действием **Запретить**:

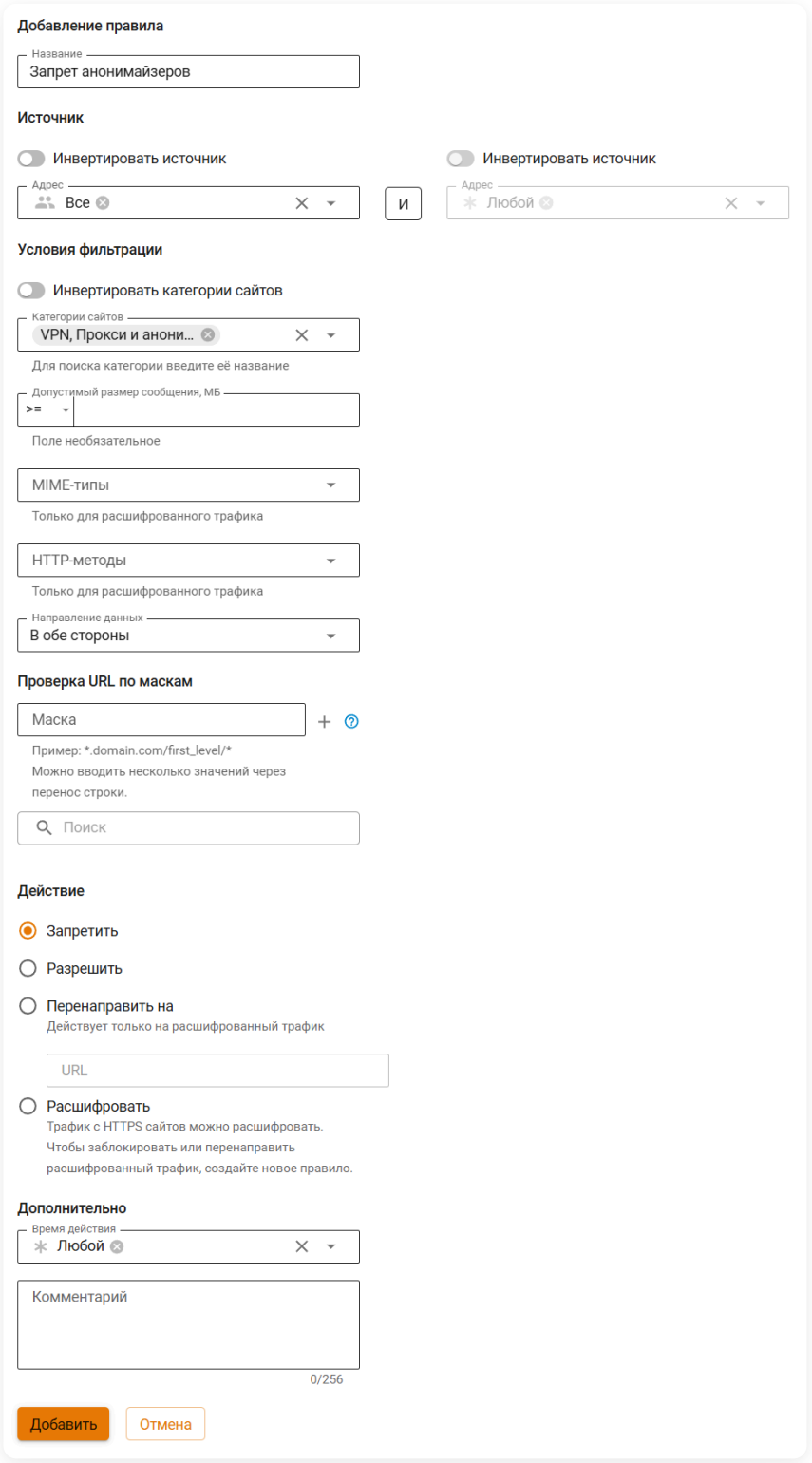


2. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

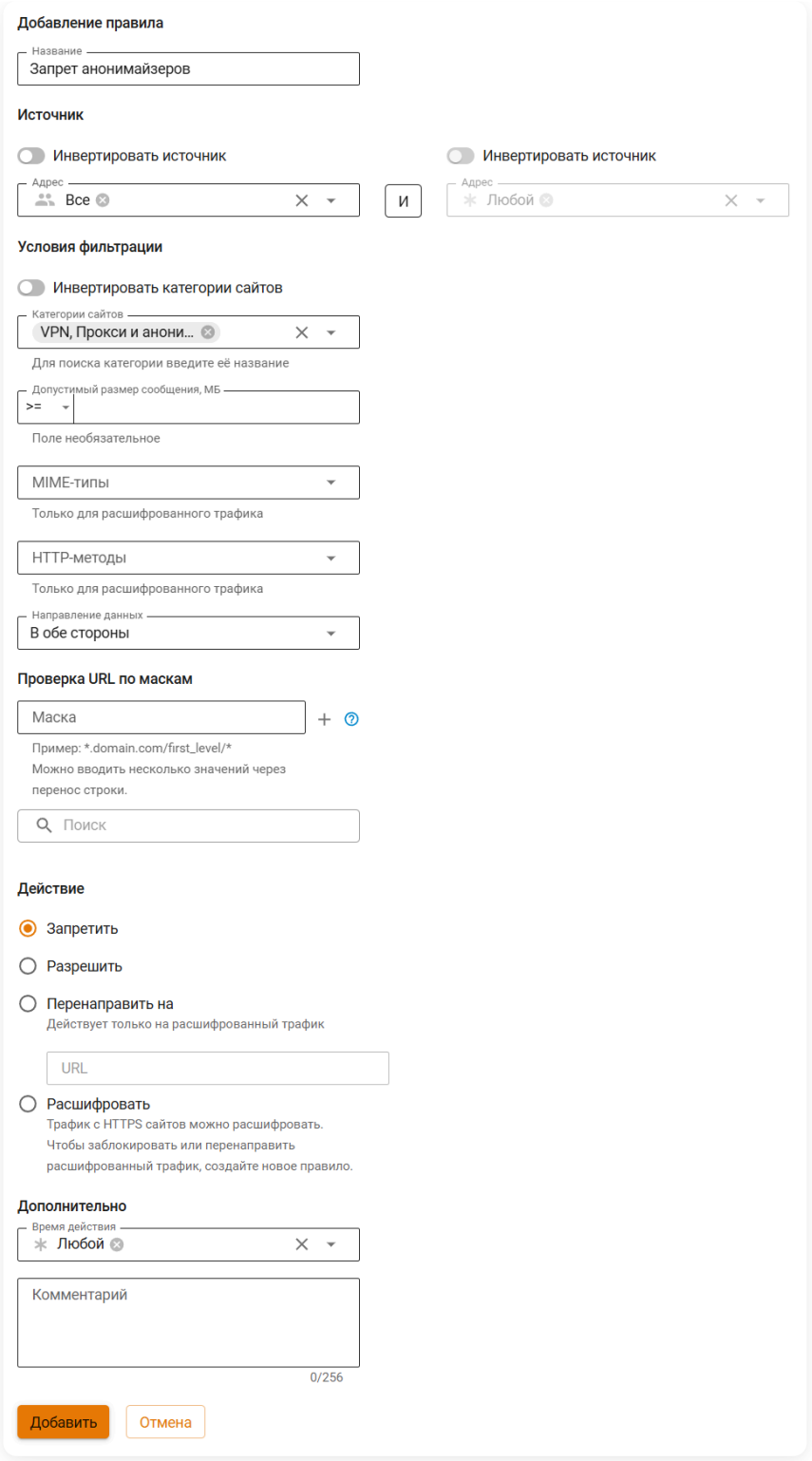
Блокировка анонимайзеров

Заблокировать анонимайзеры можно в разделе **Правила трафика** тремя способами:

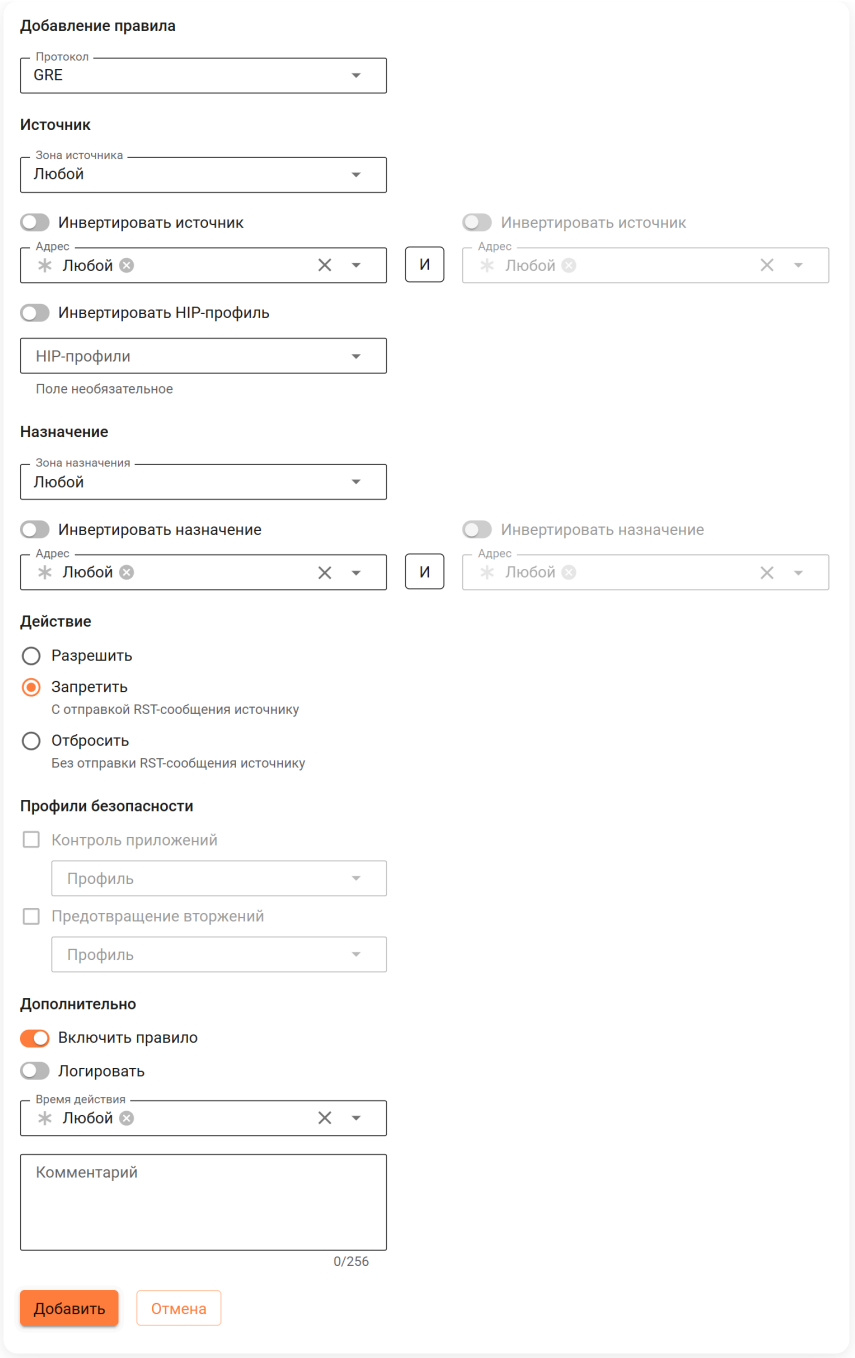
1. Анонимайзеры, работающие по протоколам HTTP(S), блокируются в **Правила трафика** → **Контент-фильтр**. Для этого создайте правило, в котором запретите категорию сайтов **Анонимайзеры**:



2. Чтобы предотвратить обход **Контент-фильтра**, создайте правило, которое будет блокировать прямые обращения по IP-адресам в Контент-фильтре:



3. Для блокировки VPN-анонимайзеров, использующих протокол PPTP, достаточно заблокировать протокол GRE в правилах **Межсетевого экрана**:

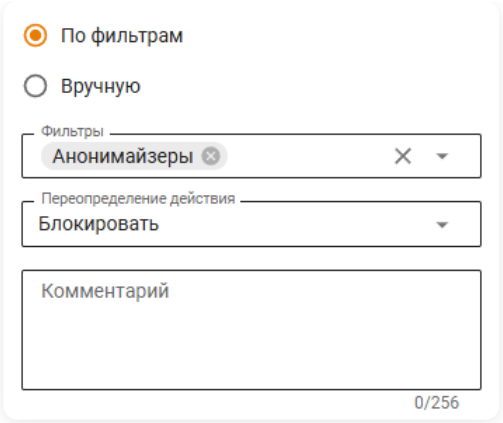


Блокировка Opera.Turbo, Opera VPN, Yandex.Turbo, friGate, Anonymox

Чтобы заблокировать функции браузеров, которые используются для обхода контентной фильтрации, воспользуйтесь модулем Предотвращение вторжений.

1. Перейдите в **Профили безопасности** → **Предотвращение вторжений**. Создайте новый профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило, блокирующее группу сигнатур **Анонимайзеры**:



3. Нажмите **Добавить**.

4. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилем, созданным ранее.

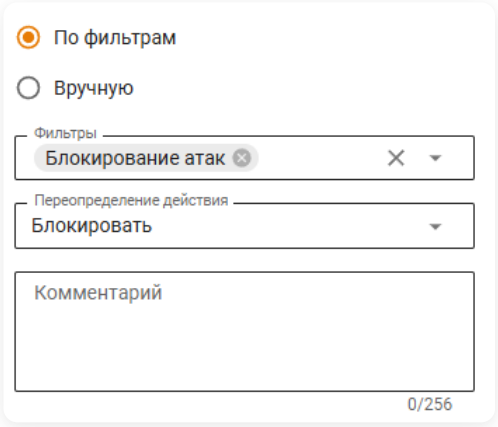
Блокировка Tor

Tor - специально разработанное программное обеспечение и среда прокси-серверов, предназначенная для обхода различного рода блокировок, поэтому полностью заблокировать Tor сейчас невозможно.

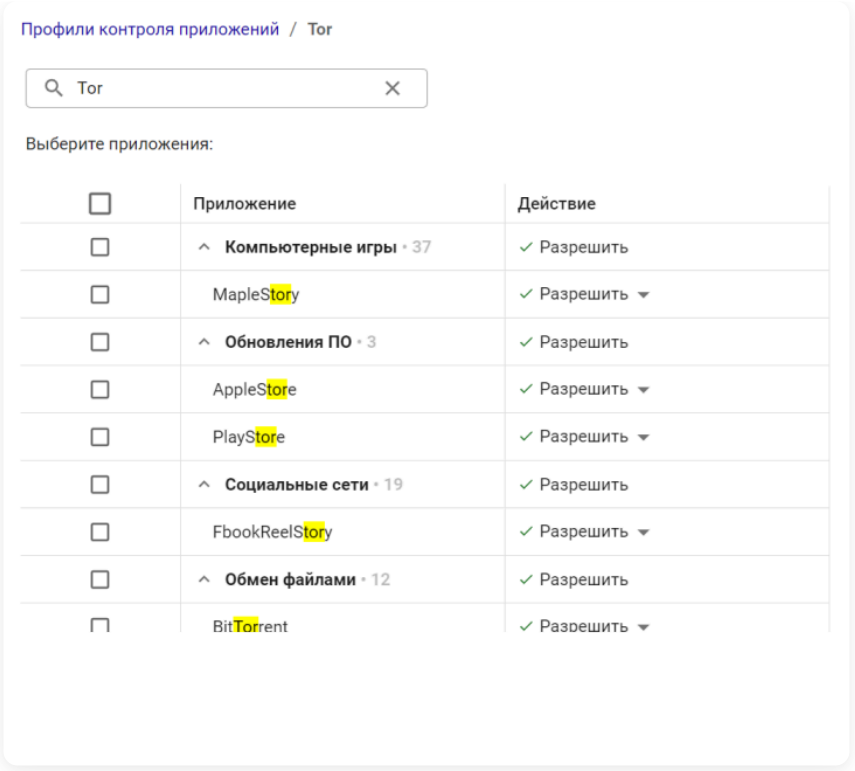
Для противодействия использованию сети Tor, а также для журналирования попыток подключения и использования сети Tor, выполните следующие настройки:

1. В **Профили безопасности** → **Предотвращение вторжений** создайте профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило для группы сигнатур **Блокирование атак**:



3. В **Профили безопасности** → **Контроль приложений** добавьте профиль, запрещающий приложение Tor:



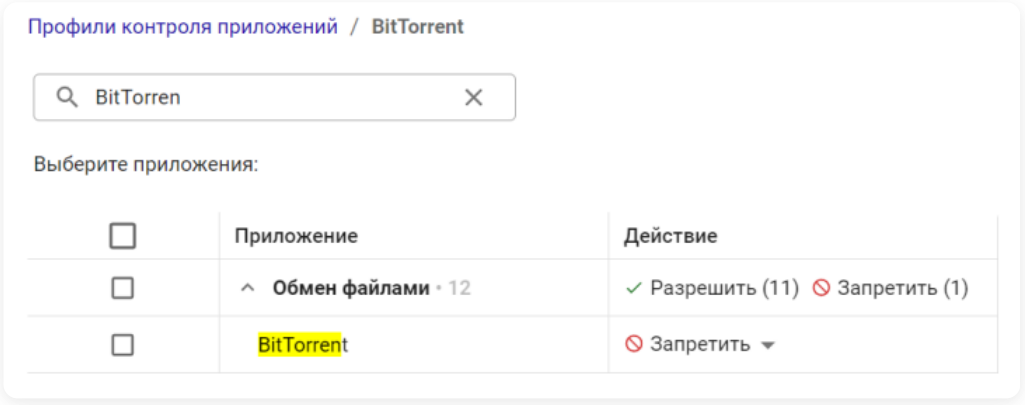
4. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилями **Предотвращения вторжений** и **Контроля приложений**, созданными ранее.

Блокировка торрентов

BitTorrent - P2P-протокол, предназначенный для обмена файлами через интернет.

Для ограничения возможности использования торрентов выполните следующие настройки:

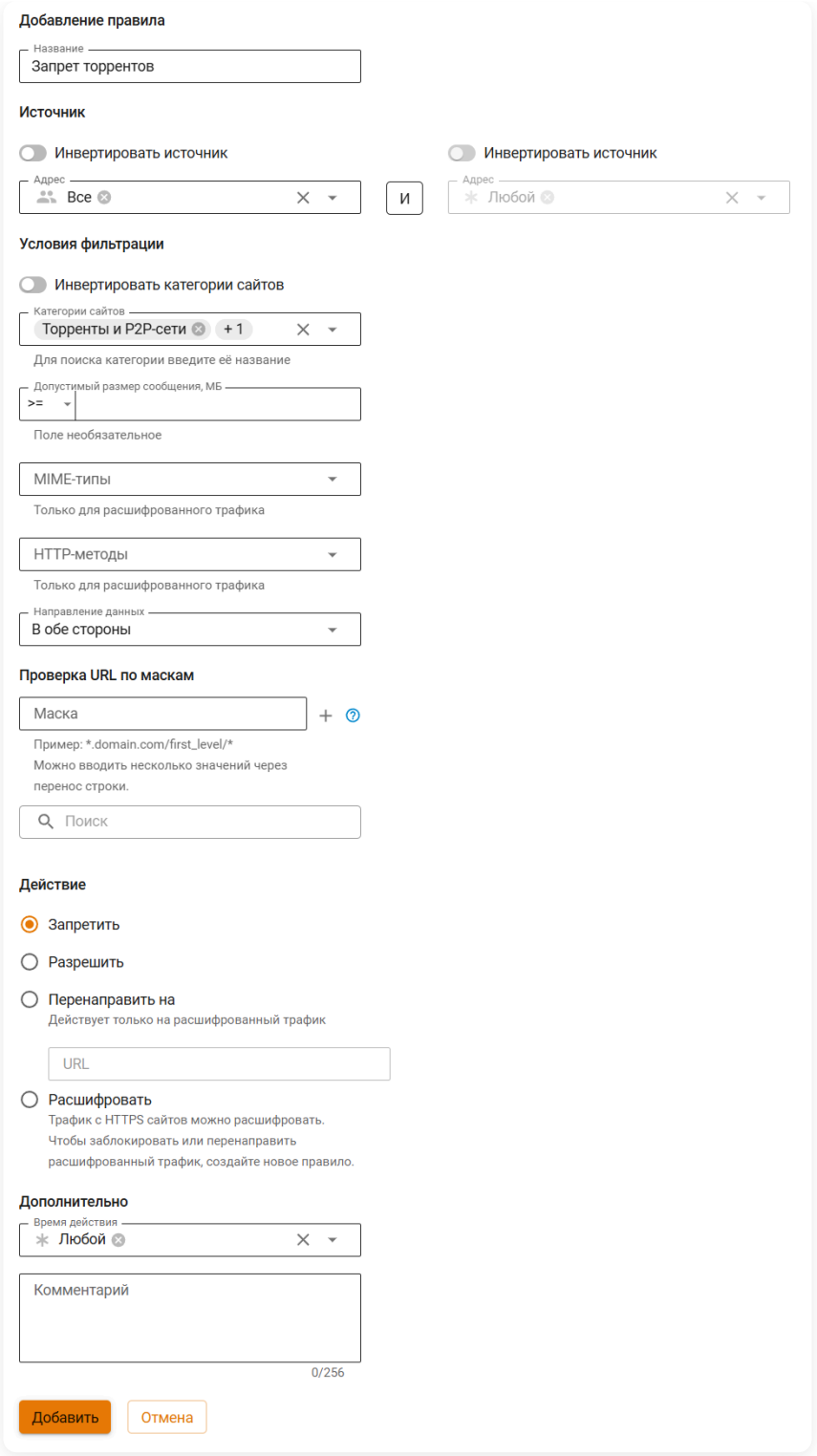
1. Запретите протокол BitTorrent с помощью правила в **Профили безопасности** → **Контроль приложений**:



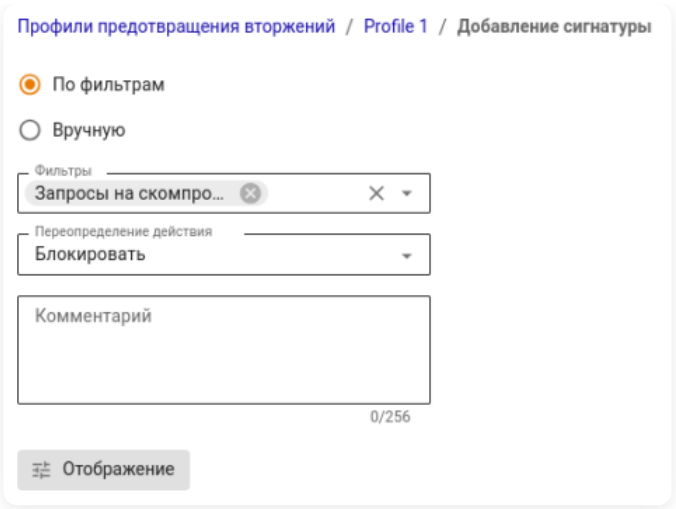
2. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

3. Разрешите нужные TCP и UDP порты пользователям. Затем создайте и включите в **Правила трафика** → **Межсетевой экран** → **FORWARD** правило, которое запрещает все протоколы (правила действуют сверху вниз).

4. В **Контент-фильтр** заблокируйте доступ к сайтам-каталогам и торрент-файлам. Для этого запретите категории **Торрент-трекеры** и **Torrent-файлы**:



5. В **Профили безопасности** → **Предотвращение вторжений** создайте профиль, блокирующий группу сигнатур **Запросы на скомпрометированные ресурсы**, которая позволяет блокировать активность P2P-программ:



Блокировка Telegram

Telegram - облачный мессенджер для мобильных устройств и компьютеров (приложение и веб-версия).

Telegram не блокируется **Контролем приложений**, если в приложении настроить опцию **Использовать собственный прокси** в **Настройки** → **Продвинутые настройки** → **Тип соединения**:

При необходимости рекомендуем блокировать доступ к приложению Telegram на рабочих станциях: запрещать установку и запуск приложения политиками безопасности или антивирусом.

Веб-версию Telegram можно заблокировать с помощью **Контент-фильтра**. Для этого выполните следующие действия:

1. Создайте пользовательскую категорию, включающую значение `web.telegram.org`, или отредактируйте уже существующую:

2. Укажите созданную или отредактированную пользовательскую категорию при добавлении правила **Контент-фильтра** с действием **Запретить**:

Полезные ссылки

- **Контент-фильтр**
- **Контроль приложений**
- **Межсетевой экран**
- **Правила**
- **Предотвращение вторжений**
- **Предотвращение вторжений**

Ручная корректировка GeoIP

Чтобы изменить привязку IP-адреса или сети к стране, добавьте необходимую запись в файл `/var/opt/ideco/system-backend/geoip.override`. Можно добавлять IP-адреса и сети в формате CIDR для привязки к указанной стране.

Информация о корректировке GeoIP отображается в журнале Система.

Формат записи файла

```
<network> <country>
```

- `network` - сеть в CIDR-нотации (например, 109.70.184.0/21).

> Индивидуальные IP-адреса должны быть оформлены как сеть с маской подсети `/32`.

- `country` - ISO-код (Alpha-2) страны, в которую будет помещен IP-адрес или сеть.

```
1.2.9.10/32 us
1.2.10.0/24 ru
104.28.130.178/32 ru
```

- `1.2.9.10/32 us` - перемещение IP-адреса `1.2.9.10/32` в список **Соединенные Штаты**, остальные IP-адреса подсети `1.2.9.0/24` останутся в списке **Российская Федерация**.
- `1.2.10.0/24 ru` - подсеть `1.2.10.0/24` добавится к списку **Российская Федерация**.
- `104.28.130.178/32 ru` - IP-адрес `104.28.130.178/32` исключится из списка **Соединенные Штаты** и добавится в список **Российская Федерация**.

Порядок действий

Для изменения привязки IP-адреса или сети к стране:

1. Перейдите в **Управление сервером** → **Терминал**.

2. Отредактируйте файл: `/var/opt/ideco/system-backend/geoip.override`:

```
nano /var/opt/ideco/system-backend/geoip.override
```

Изменение GeoIP базы произойдет в течение минуты.

> Некорректные записи в файле игнорируются и сведения об ошибках фиксируются в журнале Система в формате `Invalid IpList Patch line "<СТРОКА>": <ОШИБКА>`.

Список зон IpList

> **Важно**: ручное добавление IP-адреса в список определенной страны не добавляет IP-адрес автоматически в список группы стран или континента. Для добавления IP-адреса во все необходимые списки пропишите эти группы в файле:
>
> ```
> 123.123.123.123/32 at
> 123.123.123.123/32 eu_group
> 123.123.123.123/32 eu_union_group
> ```
>
> В этом примере IP-адрес будет одновременно добавлен в списки: **Австрия**, **Европа** и **Европейский союз**.

Зона (country)	Местоположение
ad	Андорра
ae	Объединенные Арабские Эмираты
af	Афганистан
af_group	Африка
ag	Антигуа и Барбуда
ai	Ангилья
al	Албания
am	Армения
an_group	Антарктика
ao	Ангола
aq	Антарктида
ar	Аргентина
as	Американское Самоа
as_group	Азия
at	Австрия
au	Австралия
aw	Аруба
ax	Аланды
az	Азербайджан
ba	Босния
bb	Барбадос
bd	Бангладеш
be	Бельгия
bf	Буркина Фасо
bg	Болгария
bh	Бахрейн
bi	Бурунди
bj	Бенин
bl	Сен-Бартельми
bm	Бермудские острова
bn	Бруней Даруссалам
bo	Боливия
bq	Бонайре, Синт-Эстатиус и Саба
br	Бразилия
bs	Багамские острова
bt	Бутан
bv	Остров Буве
bw	Ботсвана
by	Беларусь
bz	Белиз
ca	Канада
cc	Кокосовые острова
cd	Конго, Демократическая Республика
cf	Центрально-Африканская Республика
cg	Республика Конго
ch	Швейцария
ci	Кот-д'Ивуар
ck	Острова Кука

Зона (country)	Местоположение
cl	Чили
cm	Камерун
cn	Китай
co	Колумбия
cr	Коста-Рика
cu	Куба
cv	Кабо-Верде
cw	Кюрасао
cx	Остров Рождества
cy	Кипр
cz	Чешская Республика
de	Германия
dj	Джибути
dk	Дания
dm	Остров Доминика
do	Доминиканская Республика
dz	Алжир
ec	Эквадор
ee	Эстония
eg	Египет
eh	Западная Сахара
er	Эритрея
es	Испания
et	Эфиопия
eu_group	Европа
eu_union_group	Европейский Союз
fi	Финляндия
fj	Фиджи
fk	Фолклендские острова
fm	Федеративные Штаты Микронезии
fo	Фарерские острова
fr	Франция
ga	Габон
gb	Великобритания
gd	Гренада
ge	Грузия
gf	Французская Гвиана
gg	Гернси
gh	Гана
gi	Гибралтар
gl	Гренландия
gm	Гамбия
gn	Гвинея
gp	Гваделупа
gq	Экваториальная Гвинея
gr	Греция
gs	Южная Георгия и Южные Сандвичевы острова
gt	Гватемала

Зона (country)	Местоположение
gu	Гуам
gw	Гвинея-Биссау
gy	Гайана
hk	Гонконг
hm	Острова Херд и Макдональд
hn	Гондурас
hr	Хорватия
ht	Гаити
hu	Венгрия
id	Индонезия
ie	Ирландия
il	Израиль
im	Остров Мэн
in	Индия
io	Британская территория в Индийском океане
iq	Ирак
ir	Иран
is	Исландия
it	Италия
je	Джерси
jm	Ямайка
jo	Иордания
jp	Япония
ke	Кения
kg	Кыргызстан
kh	Камбоджа
ki	Кирибати
km	Коморские острова
kn	Сент-Киттс и Невис
kp	КНДР
kr	Южная Корея
kw	Кувейт
ky	Каймановы Острова
kz	Казахстан
la	Лаос
lb	Ливан
lc	Сент-Люсия
li	Лихтенштейн
lk	Шри-Ланка
lr	Либерия
ls	Лесото
lt	Литва
lu	Люксембург
lv	Латвия
ly	Ливия
ma	Марокко
mc	Монако
md	Молдова

Зона (country)	Местоположение
me	Черногория
mf	Сен-Мартен
mg	Мадагаскар
mh	Маршалловы Острова
mk	Македония
ml	Мали
mm	Мьянма (Бирма)
mn	Монголия
mo	Макао
mp	Северные Марианские острова
mq	Мартиника
mr	Мавритания
ms	Монтсеррат
mt	Мальта
mu	Маврикий
mv	Мальдивы
mw	Малави
mx	Мексика
my	Малайзия
mz	Мозамбик
na	Намибия
na_group	Северная Америка
nc	Новая Каледония
ne	Нигер
nf	Остров Норфолк
ng	Нигерия
ni	Никарагуа
nl	Нидерланды
no	Норвегия
np	Непал
nr	Науру
nu	Ниуэ
nz	Новая Зеландия
oc_group	Океания
om	Оман
pa	Панама
pe	Перу
pf	Французская Полинезия
pg	Папуа - Новая Гвинея
ph	Филиппины
pk	Пакистан
pl	Польша
pm	Сен-Пьер и Микелон
pn	Острова Питкэрн
pr	Пуэрто-Рико
ps	Палестина
pt	Португалия
pw	Палау

Зона (country)	Местоположение
py	Парагвай
qa	Катар
re	Реюньон
ro	Румыния
rs	Сербия
ru	Российская Федерация
rw	Руанда
sa	Саудовская Аравия
sa_group	Южная Америка
sb	Соломоновы Острова
sc	Сейшельские острова
sd	Судан
se	Швеция
sg	Сингапур
sh	Остров Св. Елены
si	Словения
sj	Шпицберген и Ян-Майен
sk	Словакия
sl	Сьерра-Леоне
sm	Сан-Марино
sn	Сенегал
so	Сомали
sr	Суринам
ss	Южный Судан
st	Сан-Томе и Принсипи
sv	Сальвадор
sx	Синт-Мартен
sy	Сирийская Арабская Республика
sz	Эсватини
tc	Острова Теркс и Кайкос
td	Чад
tf	Французские Южные территории
tg	Того
th	Таиланд
tj	Таджикистан
tk	Токелау
tl	Тимор-Лесте
tm	Туркменистан
tn	Тунис
to	Тонга
tr	Турция
tt	Тринидад и Тобаго
tv	Тувалу
tw	Тайвань
tz	Танзания
ua	Украина
ug	Уганда
um	Внешние малые острова (США)

Зона (country)	Местоположение
us	Соединенные Штаты
uy	Уругвай
uz	Узбекистан
va	Государство-город Ватикан
vc	Сент-Винсент и Гренадины
ve	Венесуэла
vg	Виргинские острова (Великобритания)
vi	Виргинские острова (США)
vn	Вьетнам
vu	Вануату
wf	Острова Уоллис и Футуна
ws	Самоа
xk	Косово
ye	Йемен
yt	Майотта
za	ЮАР
zm	Замбия
zw	Зимбабве

Полезные ссылки

- **Объекты**
- **Система**

SD-WAN

Практические руководства по настройке SD-WAN в Ideco NGFW Novum

Резервирование трех WAN-каналов через SD-WAN

Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Резервирование трех WAN-каналов через SD-WAN

Классический контекст | Высокопроизводительный контекст

Руководство описывает настройку каскадного резервирования WAN на удаленной площадке с тремя каналами доступа в интернет:

- **Интерфейс 1** - проводной провайдер, шлюз 192.0.2.1 (основной канал).
- **Интерфейс 2** - LTE-модем в Ethernet-режиме, шлюз 10.0.0.1 (первый резервный канал).
- **Интерфейс 3** - спутниковый терминал, шлюз 10.0.1.1 (второй резервный канал).
- **Локальная сеть** - 172.16.0.0/24.

После настройки при обрыве проводного канала трафик автоматически перейдет на LTE, при обрыве LTE - на спутник. После восстановления канала с более высоким приоритетом трафик вернется на него автоматически.

Что нужно учесть перед настройкой

Каналы имеют принципиально разные характеристики:

Тип канала	Ориентировочная задержка	Джиттер	Особенности
Проводной провайдер	5-30 мс	низкий	Стабильный, предсказуемый
LTE-модем	30-80 мс	средний	Зависит от загруженности сети и уровня сигнала
Спутниковый терминал (GEO)	500-700 мс	высокий	Большая задержка из-за расстояния до спутника. Непригоден для VoIP и видеозвонков. Трафик значительно дороже проводного и LTE

Значения задержки и джиттера ориентировочные. Реальные показатели зависят от оборудования и условий работы канала.

Настройка

Шаг 1. Настройте интерфейсы

Убедитесь, что все три внешних интерфейса настроены и получают адреса от своих провайдеров. Подробнее о настройке интерфейсов в статье.

Шаг 2. Создайте Next hop для каждого канала

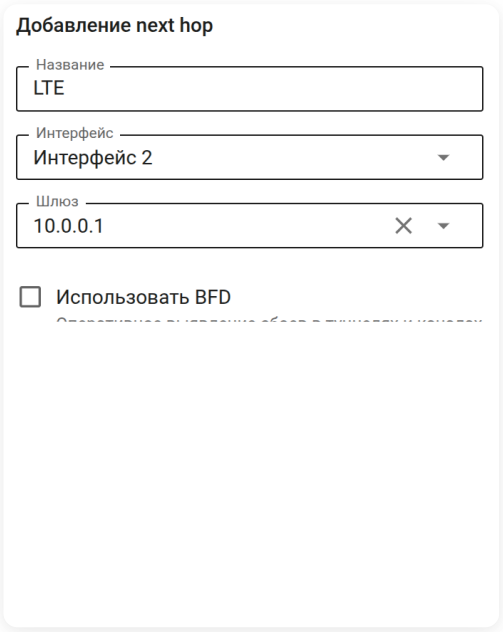
1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля:

Проводной провайдер

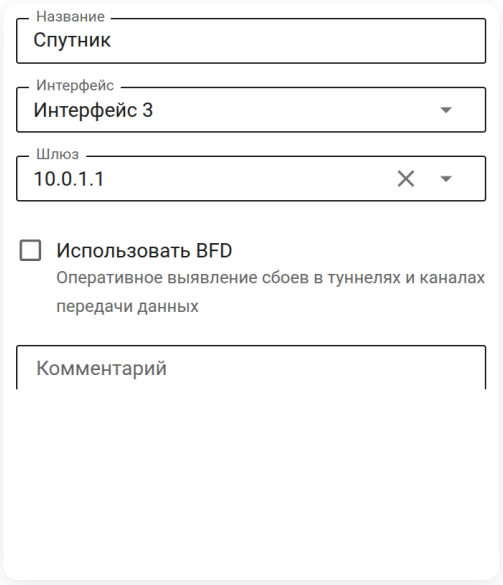
- **Название** - укажите `Проводной`.
- **Интерфейс** - выберите `Интерфейс 1`.
- **Шлюз** - укажите `192.0.2.1`.
- **Использовать BFD** - оставьте опцию выключенной.

LTE



- **Название** - укажите `LTE`.
- **Интерфейс** - выберите `Интерфейс 2`.
- **Шлюз** - укажите `10.0.0.1`.
- **Использовать BFD** - оставьте опцию выключенной.

Спутник



- **Название** - укажите `Спутник`.
- **Интерфейс** - выберите `Интерфейс 3`.
- **Шлюз** - укажите `10.0.1.1`.
- **Использовать BFD** - оставьте опцию выключенной.

---

3. Нажмите **Добавить**.

BFD требует поддержки на стороне шлюза провайдера. Операторы LTE и спутниковые операторы, как правило, BFD не поддерживают, поэтому для проверки доступности каналов используйте профили IP SLA на следующем шаге.

Шаг 3. Создайте профиль IP SLA

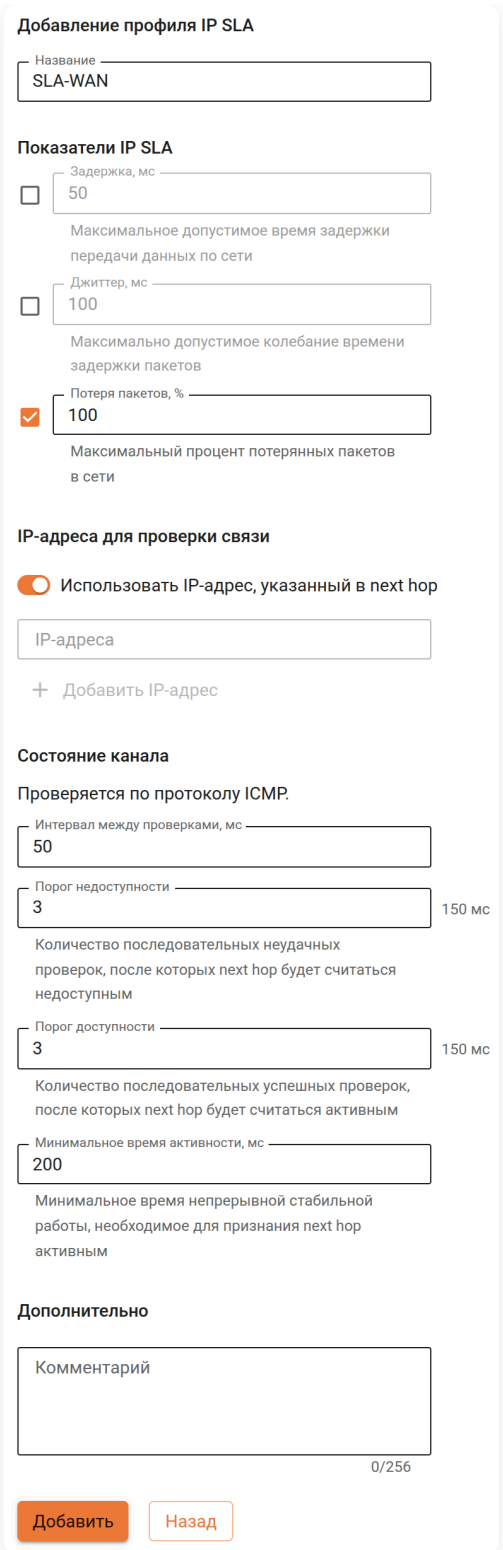
Профиль IP SLA применяется ко всем узлам в **Профиле next hop**.

Поскольку каналы различаются по задержке, в особенности спутниковый (с базовой задержкой ~500-700 мс), использовать пороги задержки и джиттера в общем профиле нецелесообразно: канал с высокой задержкой будет постоянно считаться недоступным. Для резервирования достаточно проверять только доступность шлюза по ICMP.

Выполните действия:

1. Перейдите в **SD-WAN** → **Профили IP SLA** и нажмите **Добавить**.

2. Заполните поля:



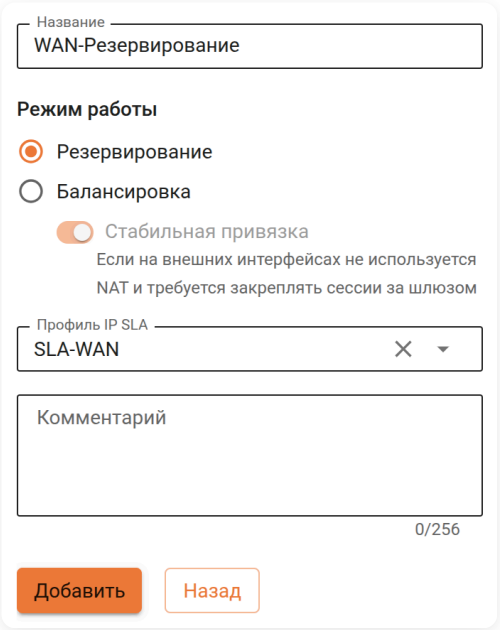
- **Название** - укажите `SLA-WAN`.
- **Показатели SLA**:
  - **Задержка, мс** - оставьте опцию выключенной. Базовая задержка спутникового канала (~500-700 мс) превысит любой разумный порог.
  - **Джиттер, мс** - оставьте опцию выключенной по той же причине.
  - **Потеря пакетов, %** - включите опцию и укажите `100`.
- **Использовать IP-адрес, указанный в next hop** - включите опцию. Система будет проверять шлюз каждого next hop по его собственному IP-адресу.
- **Интервал между проверками, мс** - задайте частоту проверок, например, `50`.
- **Порог недоступности** - задайте количество последовательных неудачных проверок для признания канала недоступным, например, `3`.
- **Порог доступности** - задайте количество последовательных успешных проверок для признания канала восстановленным, например, `3`.
- **Минимальное время активности, мс** - задайте минимальное время стабильной работы перед тем, как канал будет признан активным, например, `200`.

3. Нажмите **Добавить**.

Шаг 4. Создайте профиль next hop в режиме Резервирование

1. Перейдите в **SD-WAN** → **Профили next hop** и нажмите **Добавить**.

2. На вкладке **Настройки** заполните поля:

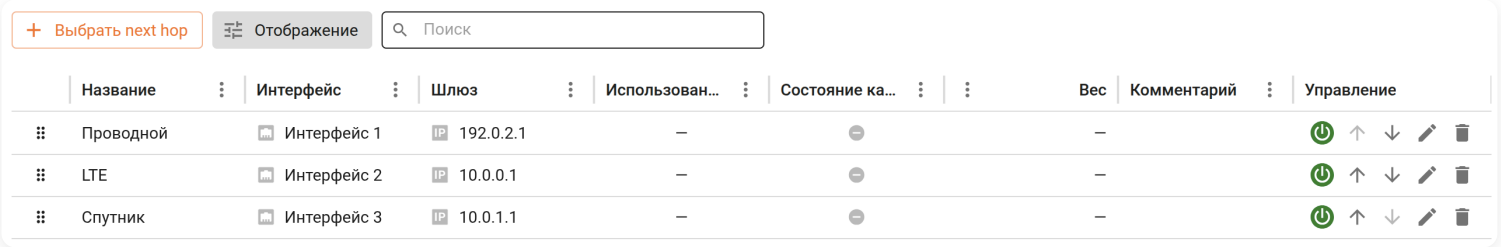


- **Название** - укажите `WAN-Резервирование`.
- **Режим работы** - выберите **Резервирование**.
- **Профиль IP SLA** - выберите `SLA-WAN`.

3. Нажмите **Добавить** и перейдите на вкладку **Next hop**.

4. Нажмите **Выбрать next hop**, отметьте `Проводной`, `LTE` и `Спутник`, нажмите **Выбрать**.

5. Расставьте приоритет с помощью ↑ ↓ - порядок должен быть сверху вниз:

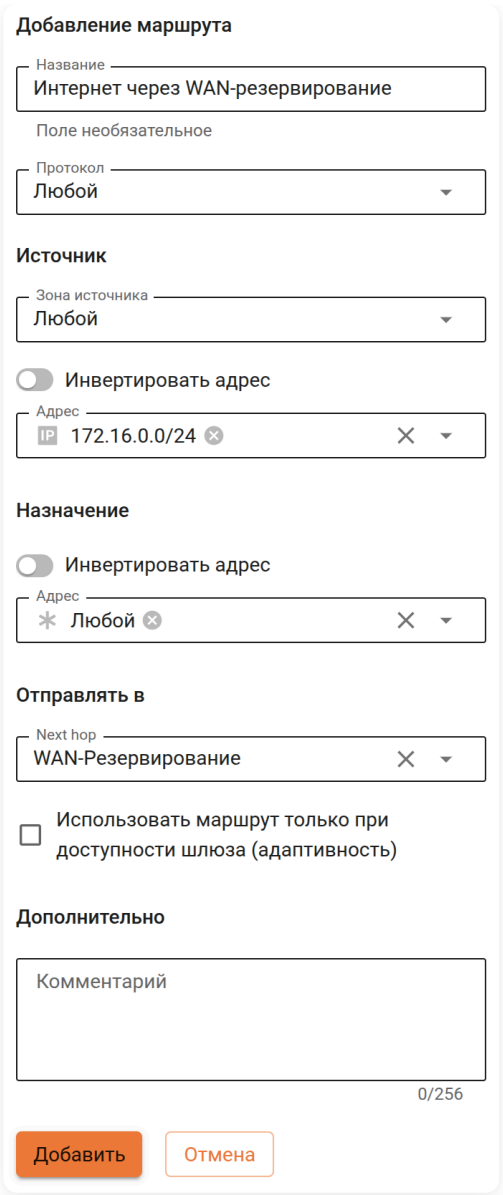


6. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

Шаг 5. Примените профиль в правиле маршрутизации

1. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**.

2. Заполните поля:



- **Название** - укажите `Интернет через WAN-резервирование`.
- **Источник**:
  - **Адрес** - выберите подсеть `172.16.0.0/24`.
- **Отправлять в** - выберите профиль `WAN-Резервирование`.

3. Нажмите **Добавить**.

Проверка каскадного переключения

1. Убедитесь, что трафик идет через проводной канал: проверьте доступность интернета с устройства в сети `172.16.0.0/24`.

2. Отключите проводной канал (физически или на стороне провайдера). Дождитесь срабатывания порога недоступности в профиле `SLA-WAN`.

3. Убедитесь, что трафик переключился на LTE: проверьте доступность интернета. События переключения отображаются в **Отчеты и журналы** → **Система**.

4. Не восстанавливая проводной канал, отключите LTE. Дождитесь срабатывания порога недоступности в профиле `SLA-WAN`.

5. Убедитесь, что трафик переключился на спутник.

6. Восстановите LTE. После достижения порога доступности и минимального времени активности в профиле `SLA-WAN` трафик должен вернуться на LTE.

7. Восстановите проводной канал. После достижения порога доступности в профиле `SLA-WAN` трафик должен вернуться на проводной канал.

Если переключение не произошло, проверьте события в **Отчеты и журналы** → **Система** и убедитесь, что пороги IP SLA выставлены корректно для вашего оборудования.

Если все три канала признаны недоступными, маршрут до внешних сетей исчезнет и трафик будет отброшен. При восстановлении любого из каналов трафик автоматически направится через него после достижения порога доступности и минимального времени активности в профиле `SLA-WAN`.

Полезные ссылки

- **Next hop**
- **Профили next hop**
- **Профили IP SLA**
- **Маршрутизация внешних сетей**
- **Интерфейсы**

Маршрутизация

Практические руководства по настройке маршрутизации в Ideco NGFW

Как избавиться от асимметричной маршрутизации трафика

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Как избавиться от асимметричной маршрутизации трафика

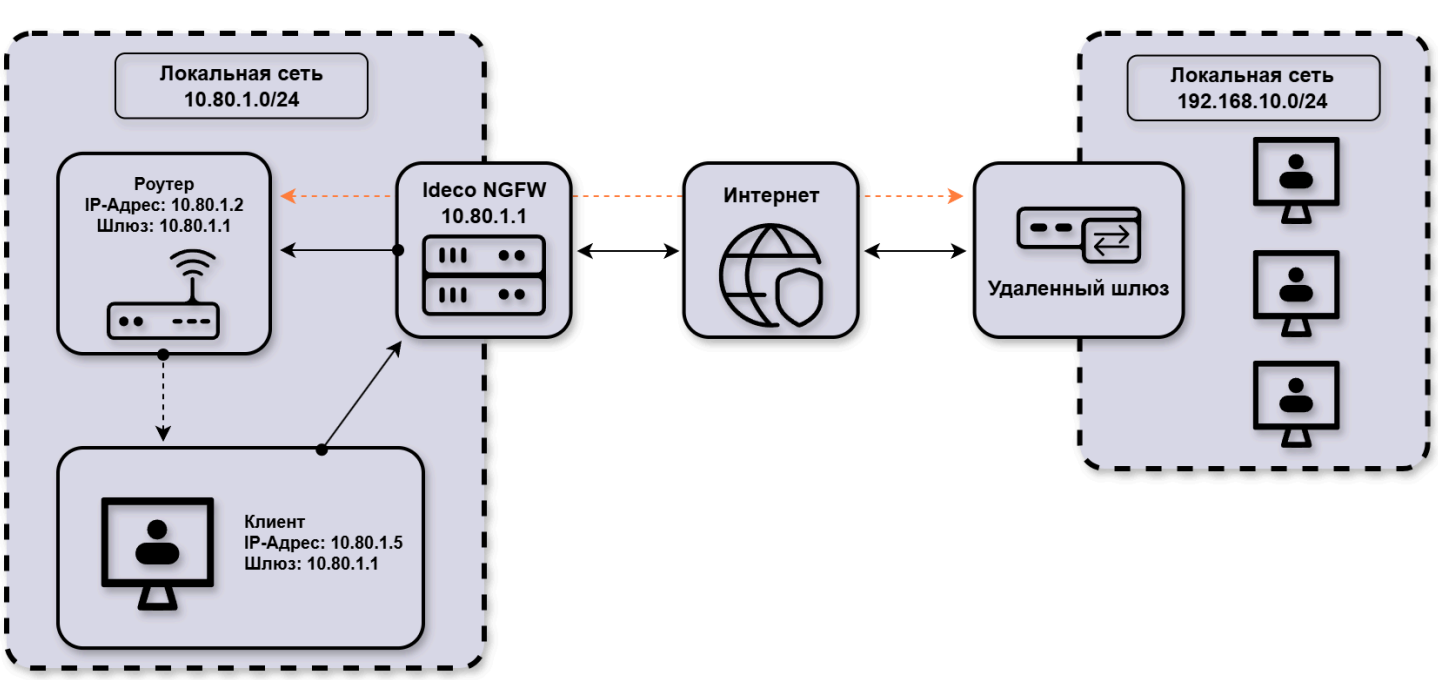
Классический контекст | Высокопроизводительный контекст

При настройке доступа в удаленные сети через маршрутизатор в локальной сети может возникнуть асимметричная маршрутизация, препятствующая прохождению пакетов между двумя локальными сетями. В этой статье описаны случаи возникновения асимметричной маршрутизации и способы предотвращения.

Пример. В локальной сети NGFW Novum используется маршрутизатор, устанавливающий связь с другими сетями. NGFW Novum - шлюз по умолчанию для клиентов сети. Требуется настроить маршрутизацию на NGFW Novum так, чтобы клиенты сети `10.80.1.0/24` получали доступ к удаленной сети `192.168.10.0/24` и обратно через маршрутизатор.

Асимметричная маршрутизация при наличии маршрутизатора в локальной сети

Неправильная топология сети, способствующая асимметричной маршрутизации:

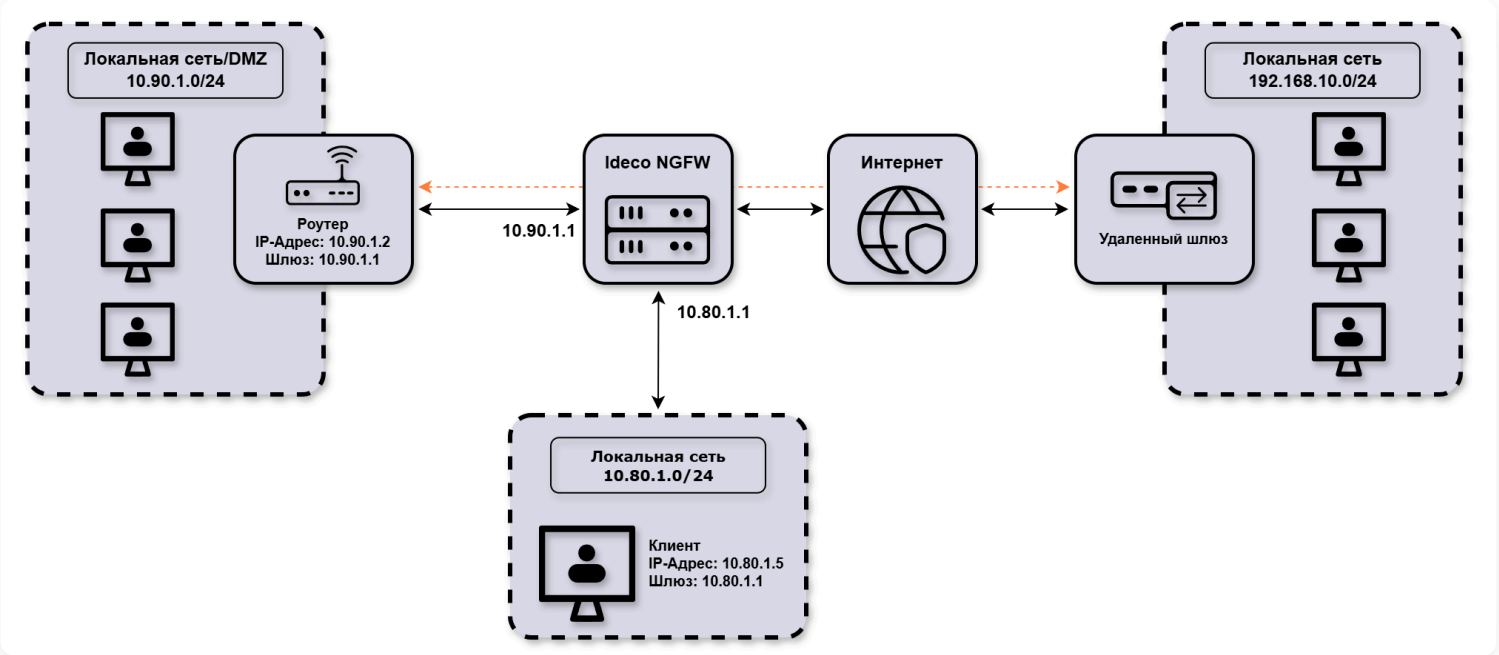


- `10.80.1.1` - шлюз для локальной сети `10.80.1.0/24`.
- `10.80.1.2` - маршрутизатор, имеющий доступ к удаленной сети `192.168.10.0/24`.
- `10.80.1.5` - адрес хоста в локальной сети.
- **Оранжевая стрелка** - двусторонняя связь маршрутизатора с удаленным шлюзом или маршрутизатором, обеспечивающая доступ к удаленной сети `192.168.10.0/24` (туннель к шлюзу, маршрут до маршрутизатора в соседнюю сеть предприятия).
- **Черные стрелки** - трафик от хостов локальной сети `10.80.1.0/24` до удаленной сети `192.168.10.0/24` через шлюз NGFW Novum (`10.80.1.1`) и маршрутизатор (`10.80.1.2`).
- **Пунктирная стрелка** - трафик, который маршрутизатор возвращает хостам локальной сети в обход NGFW Novum, поэтому хосты этот трафик обратно не принимают.

Часть трафика от клиентов до маршрутизатора идет через шлюз, а часть - непосредственно от маршрутизатора до абонентов сети. Разная маршрутизация на разных участках делает прохождение пакетов между двумя локальными сетями невозможным.

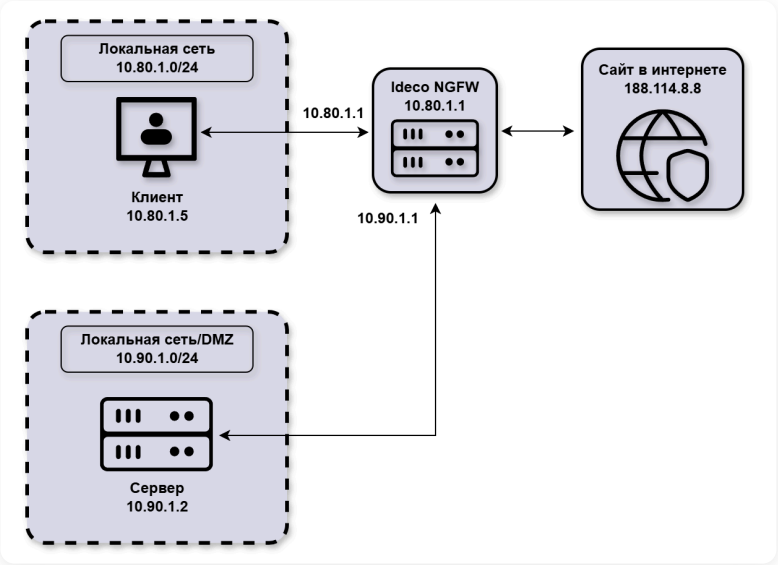
Решение: Изоляция маршрутизатора в отдельную сеть (DMZ)

Правильная топология сети:



Для правильной работы схемы потребуется:

1. Вынести маршрутизатор в отдельную локальную сеть (DMZ `10.90.1.0/24`), чтобы избежать асимметричной маршрутизации между маршрутизатором и клиентами локальной сети:



2. Настроить DMZ на NGFW Novum, добавив на локальный интерфейс NGFW Novum еще один IP-адрес (`10.90.1.0/24`), к локальной сети которого подключен маршрутизатор.

3. Настроить IP-адрес на маршрутизаторе из адресного пространства новой сети `10.90.1.2`. Шлюзом указать дополнительный IP-адрес, настроенный на локальном интерфейсе NGFW Novum из этой сети `10.90.1.1`.

Физически маршрутизатор и клиенты локальной сети будут находиться в одном сегменте сети, имея при этом разную IP-адресацию и шлюзы. Как правило, схемы с виртуальной изоляцией сетей на основе одного физического интерфейса достаточно.

Для физической изоляции локальной сети клиентов NGFW Novum и маршрутизатора:

- Подключите к NGFW Novum дополнительную сетевую карту.
- Настройте на подключенной сетевой карте дополнительный локальный интерфейс и отдельную IP-адресацию в этой сети.
- Укажите в качестве шлюза для маршрутизатора адрес, настроенный на дополнительном локальном интерфейсе.

Физически маршрутизатор будет находиться в сегменте дополнительной сетевой карты.

Шаг 1. Настройка сетевого интерфейса

Для настройки нескольких IP-подсетей на одном локальном интерфейсе NGFW Novum перейдите в **Сервисы** → **Сетевые интерфейсы** и выполните действия:

1. Откройте Ethernet-интерфейс с ролью **LAN** для локальной сети `10.80.1.1/24`, нажав на .

2. В поле **Режим** выберите **Статический** и введите IP-адрес вручную.

3. Нажмите **Добавить IP-адрес с маской** и введите IP-адрес `10.90.1.1/24` для изоляции маршрутизатора:

4. Нажмите **Сохранить**.

Шаг 2. Настройка маршрутизации

После изоляции маршрутизатора в DMZ нужно указать маршрут на NGFW Novum до удаленной сети. Для этого выполните действия:

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс для локальной сети.
- **Шлюз** - введите адрес маршрутизатора в DMZ `10.90.1.2`.

3. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:

- **Название** - укажите название.
- **Источник** - введите адрес локальной сети `10.80.1.0/24`.
- **Назначение** - введите адрес внешней сети `192.168.10.0/24`.
- **Отправлять в** - выберите созданный на шаге 2 **Next hop**.

В результате трафик между сетями `10.80.1.0/24` и `192.168.10.0/24` во всех направлениях будет направляться через NGFW Novum и маршрутизатор.

Шаг 3. Настройка клиентских машин

Хосты сетей, которые теперь обслуживает NGFW Novum (`10.80.1.0/24` и `10.90.1.0/24`), физически включены в один Ethernet-сегмент. Чтобы шлюзом и DNS-сервером для хостов этих сетей был соответствующий адрес на локальном интерфейсе NGFW Novum, укажите:

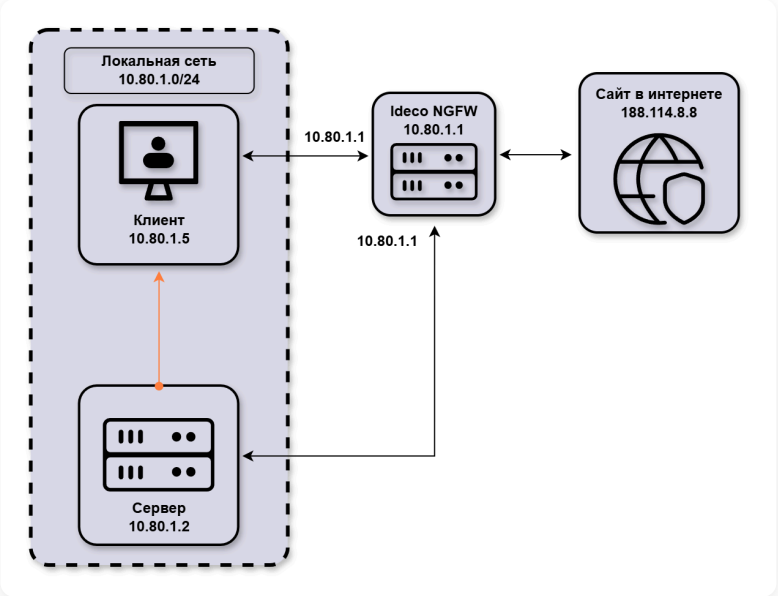
1. Для хостов из подсети `10.80.1.0/24` значение шлюза и DNS-сервера - `10.80.1.1`.

2. Для хостов из подсети `10.90.1.0/24` значение шлюза и DNS-сервера - `10.90.1.1`.

Если по какой-то причине изолировать сервер в DMZ невозможно, создайте на NGFW Novum специальное **SNAT**-правило.

Асимметричная маршрутизация при публикации ресурсов через DNAT

Асимметричная маршрутизация также возникает, когда в одной локальной сети находятся хост и сервер, на котором расположен опубликованный при помощи **DNAT**-правила ресурс:

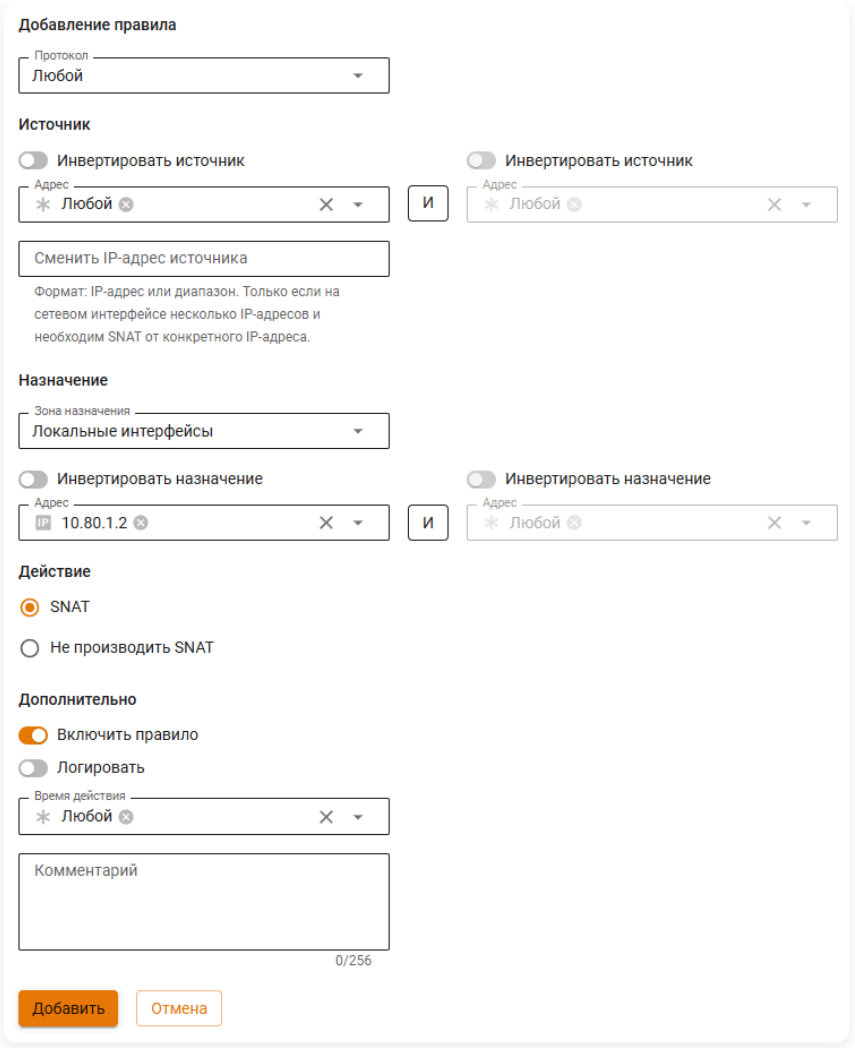


- `10.80.1.1` - адрес Ideco NGFW Novum в локальной сети.
- `10.80.1.2` - адрес сервера в локальной сети.
- `10.80.1.5` - адрес хоста в локальной сети.
- `188.114.8.8` - адрес ресурса в интернете.
- **Оранжевая стрелка** - ответ напрямую от сервера хосту в локальной сети.

Когда хост `10.80.1.5` обращается к ресурс по внешнему адресу `188.114.8.8` (например, в случае обращения по доменному имени, которое разрешено во внешнем IP), трафик проходит через NGFW Novum. На NGFW Novum срабатывает правило **DNAT** и перенаправляет трафик на сервер `10.80.1.2`, а сервер отвечает хосту, минуя NGFW Novum.

Решение: Принудительное направление ответного трафика через NGFW Novum с помощью SNAT-правила

Чтобы сервер `10.80.1.2` не отвечал напрямую на `10.80.1.5`, а отправлял ответ на NGFW Novum `10.80.1.1`, нужно в **Правила трафика** → **Межсетевой экран** → **SNAT** создать и включить правило:



- **Назначение:**
  - **Зона назначения** - укажите **Локальные интерфейсы**.
  - **Адрес** - укажите IP-адрес `10.80.1.2`.

Трафик хоста `10.80.1.5` на внешний адрес ресурса `188.114.8.8` будет перенаправлен на адрес сервера `10.80.1.2` правилом **DNAT**. При этом созданное правило **SNAT** заменит адрес источника `10.80.1.5` на адрес NGFW Novum - пакет приобретет вид: `src 10.80.1.1 dst 10.80.1.2`. Ответ от сервера также пройдет через NGFW Novum - пакет `src 10.80.1.2 dst 10.80.1.1`.

Полезные ссылки

- **Маршрутизация**
- **Статическая маршрутизация**

Управление сервером

Практические руководства по управлению сервером Ideco NGFW

Тестирование оперативной памяти сервера

Перейти >

Как настроить автоматическое включение после сбоя питания

Перейти >

Сброс пароля IPMI на сервере NGFW Novum

Перейти >

Поддержка устаревших алгоритмов шифрования

Перейти >

Восстановление конфигурации из бэкапа

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Как подключить Ideco NGFW Novum к Zabbix Server по SNMP

Классический контекст | Высокопроизводительный контекст

Протокол SNMP используется для сбора данных с сетевых устройств. Подключение Ideco NGFW Novum к Zabbix по SNMP позволяет централизованно мониторить его состояние и получать оповещения о проблемах.

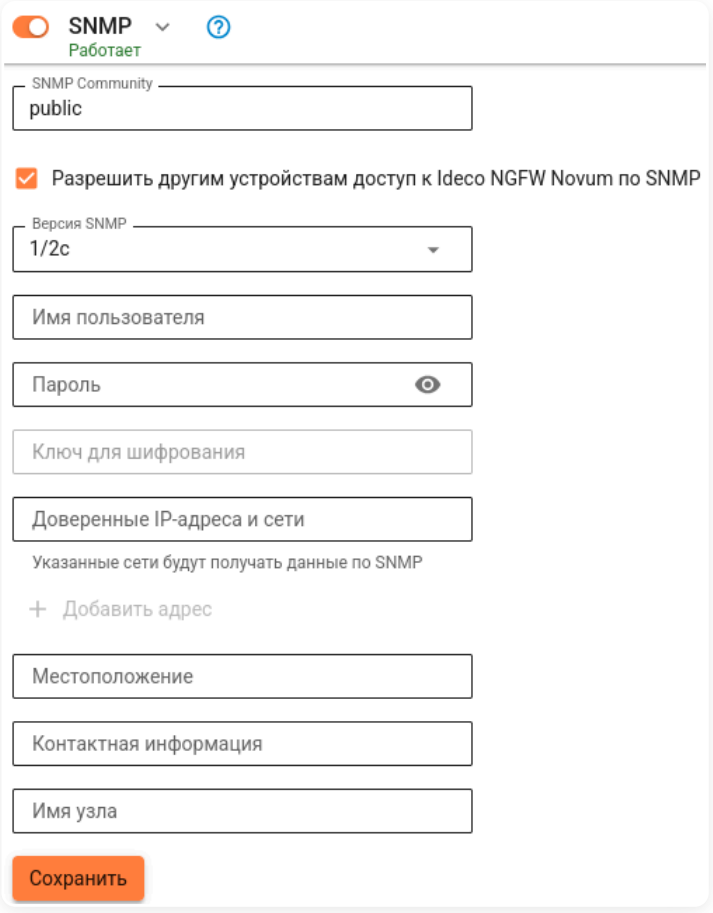
В статье - пошаговая инструкция по настройке SNMP на Ideco NGFW Novum и добавлению устройства в Zabbix Server.

Предусловия:

- Zabbix Server установлен и работает.
- Наличие сетевой доступности между Zabbix Server и Ideco NGFW Novum по UDP 161.

Настройка Ideco NGFW Novum

1. Перейдите в **Мониторинг** → **SNMP**, включите опцию **Разрешить другим устройствам доступ к Ideco NGFW Novum по SNMP** и заполните поля:



- **SNMP community** - введите название.
- **Версия SNMP** - выберите **1/2c**.
- **Доверенные IP-адреса и сети** - введите адрес Zabbix-сервера.

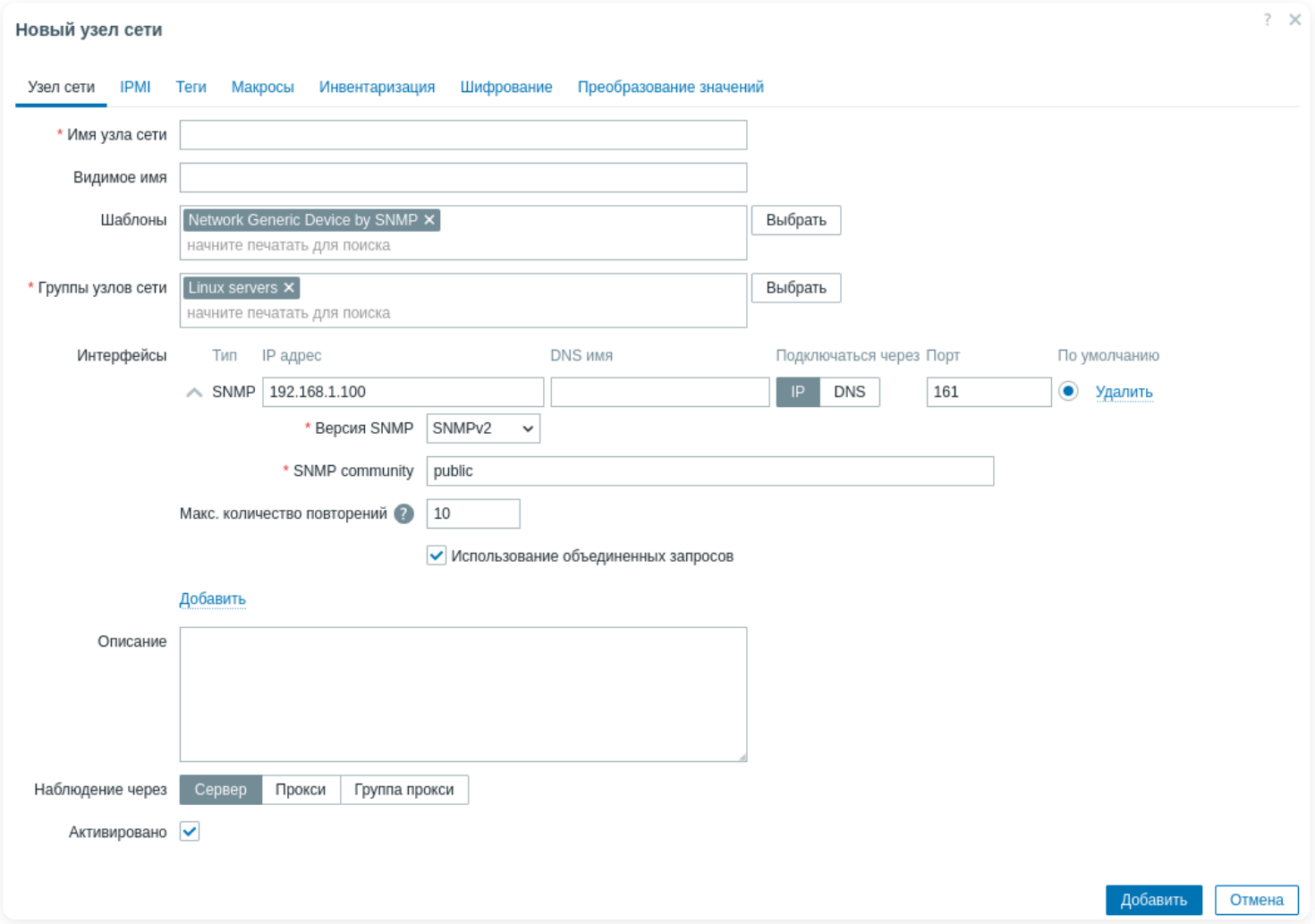
2. Нажмите **Сохранить**.

Настройка Zabbix-сервера

Инструкция актуальна для Zabbix версии 7.0.

1. Перейдите в **Сбор данных** → **Узлы сети** и в правом верхнем углу нажмите **Создать узел сети**.

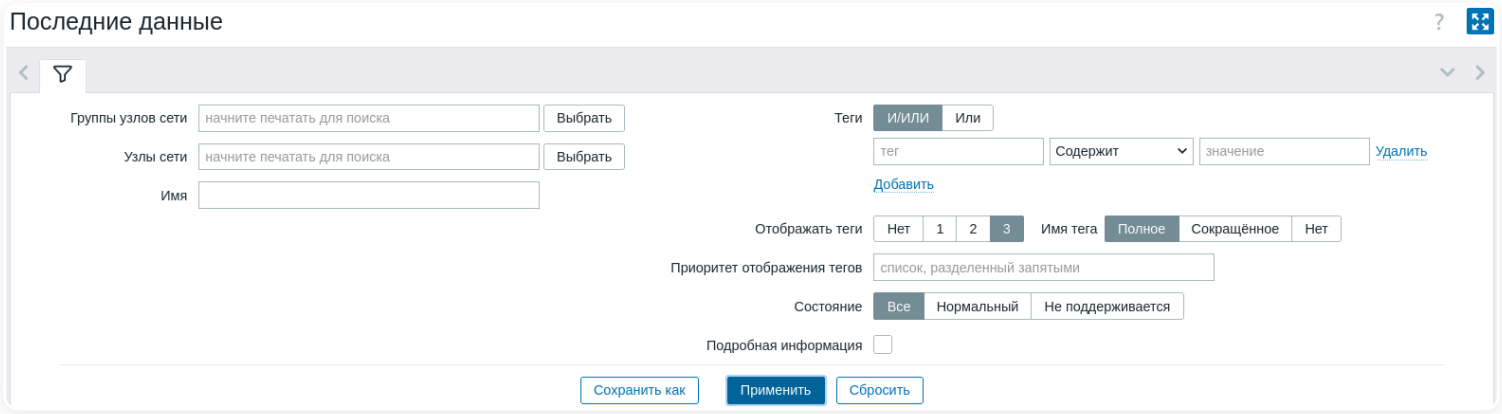
2. Заполните поля:



- **Имя узла сети** - введите название узла.
- **Шаблоны** - выберите в группе шаблонов **Templates/Network devices** → **Network Generic Device by SNMP**.
- **Группы узлов сети** - выберите **Linux servers**.
- **Интерфейсы** - нажмите **Добавить** и выберите **SNMP**:
  - **IP адрес** - введите IP-адрес NGFW Novum.
  - **Версия SNMP** - выберите **SNMPv2**.
  - **SNMP community** - введите название, указанное в настройках NGFW Novum.

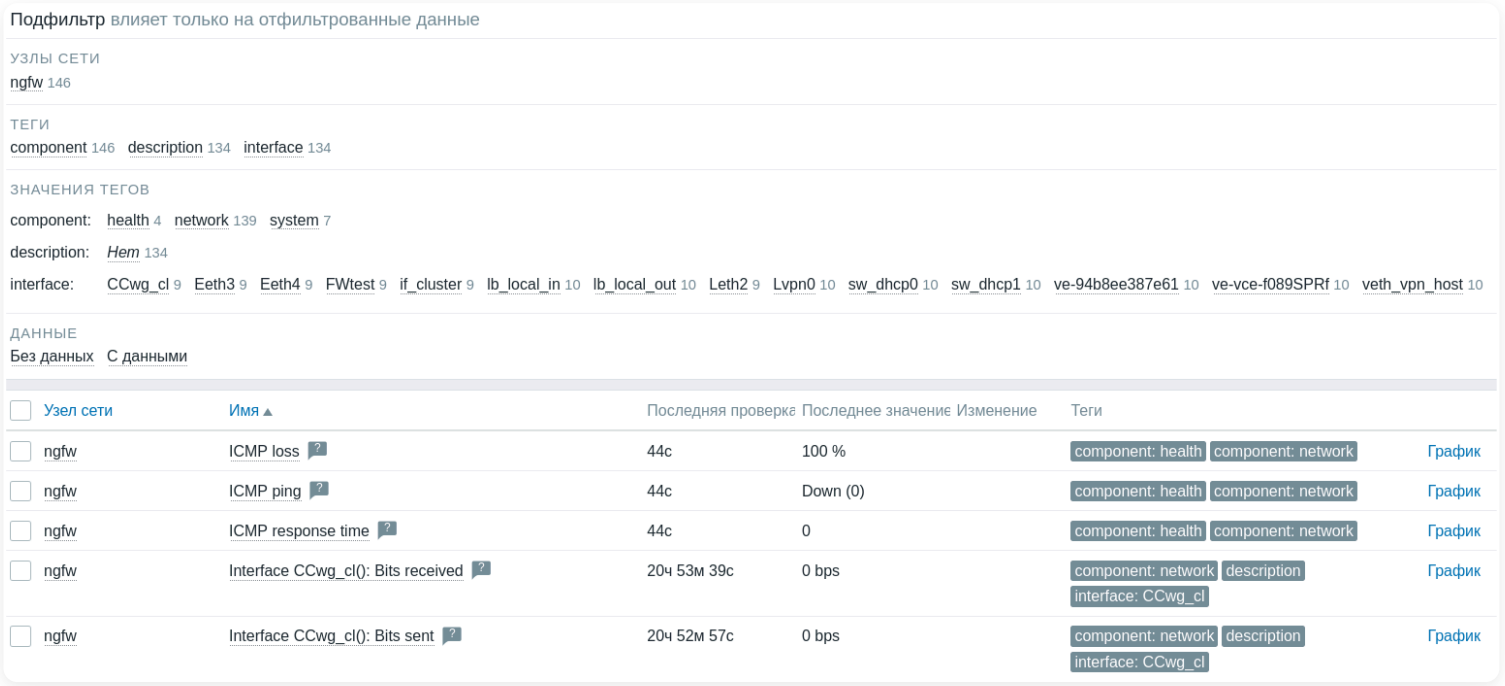
3. Нажмите **Добавить**.

4. Перейдите в **Мониторинг** → **Последние данные** и заполните поля:



- **Группы узлов сети** - выберите **Linux servers**.
- **Узлы сети** - выберите узел, созданный ранее.

5. Нажмите **Применить**. В таблице отобразятся данные NGFW Novum:



Подробнее об отображаемых данных шаблона **Network Generic Device by SNMP** можно посмотреть в статье.

Полезные ссылки

- **SNMP**
- **Zabbix-агент**

Тестирование оперативной памяти сервера

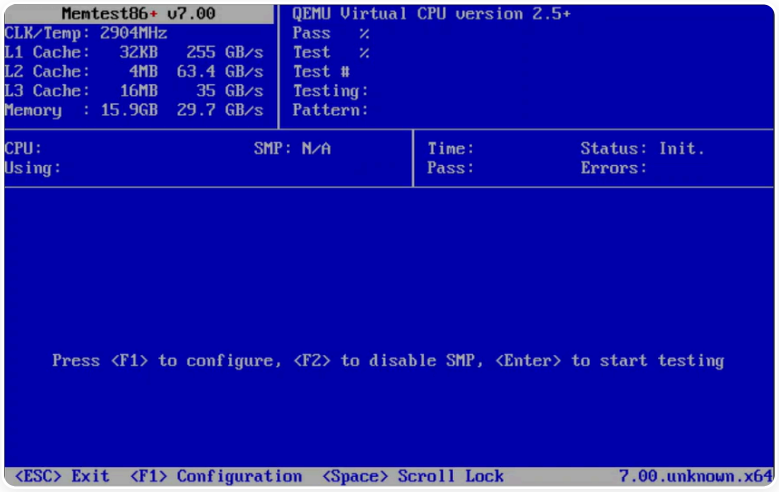
Для нормальной работы сервера все аппаратные компоненты сервера должны функционировать исправно.
Тестирование памяти помогает выявить и исключить проблемы с оперативной памятью сервера при поиске неисправностей.

При загрузке GRUB используйте Memtest86+ для тестирования оперативной памяти.
Для запуска тестирования выполните действия:

1. При загрузке сервера выберите **Memory test**:

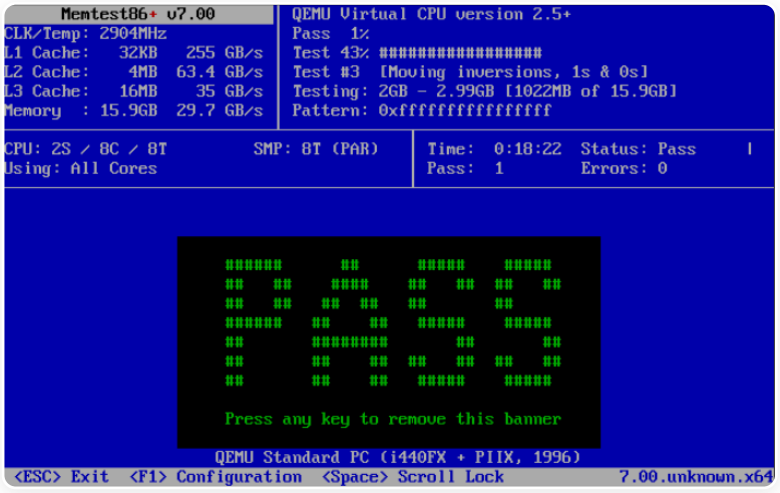


2. Нажмите **Enter** или подождите 5 секунд для автоматического запуска тестирования:

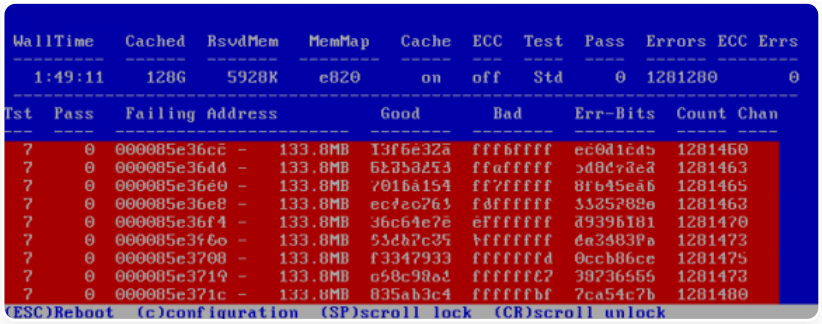


> Для выбора режима диагностики **Fail-Safe Mode** нажмите **F1**.
>
> Для выбора режима диагностики **Multi-Threading(SMP)** нажмите **F2**.

- Если появится запись **PASS**, тесты памяти пройдены успешно:



- При ошибке памяти появится запись вида:



Полезные ссылки

- Выбор аппаратной платформы

Как настроить автоматическое включение аппаратного комплекса Ideco NGFW Novum после сбоя питания

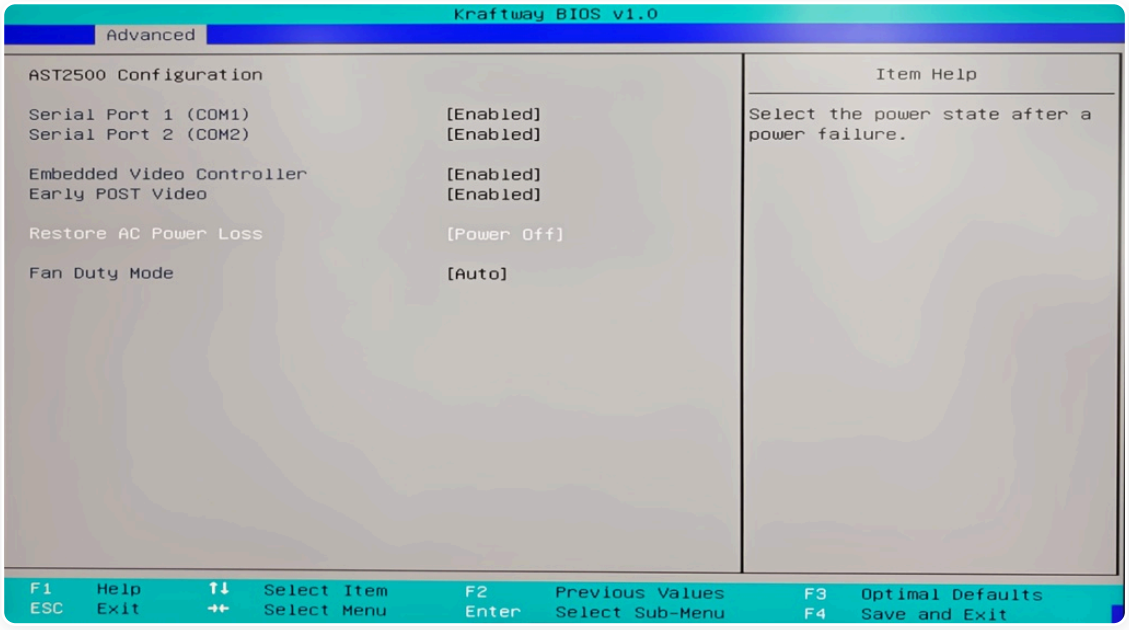
Решение подходит для всех моделей аппаратных комплексов Ideco NGFW Novum.

Для автоматического восстановления работы аппаратного комплекса Ideco NGFW Novum после сбоя электропитания необходимо активировать опцию **Restore AC Power Loss (Восстановления питания после сбоя)** в BIOS. Для включения опции:

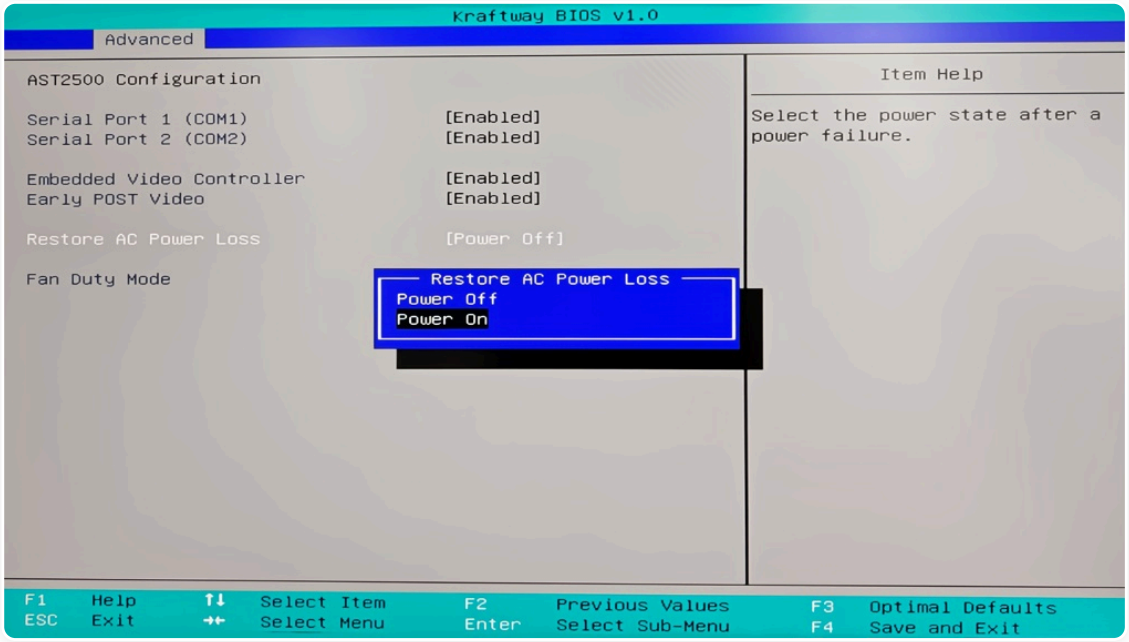
1. Запустите перезагрузку сервера.

2. Во время начальной загрузки нажмите `Delete`, чтобы зайти в BIOS.

3. В BIOS перейдите на вкладку **Advanced (Настройки)** и выберите **AST2500 Configuration (Настройка контроллера AST2500)**.



4. В меню найдите параметр **Restore AC Power Loss (Восстановления питания после сбоя)** и установите для него значение **Power ON (Включать питание)**.



5. Для сохранения настроек и выхода из BIOS нажмите `F4` и подтвердите действие.

После активации опции сервер будет автоматически запускаться при восстановлении электропитания.

Поддержка устаревших алгоритмов шифрования

Ideco NGFW Novum основан на операционной системе Fedora. В Ideco NGFW Novum используется Fedora 42. Подробнее об изменениях политики алгоритмов можно прочитать в статье.

Устаревшие алгоритмы, как (криптографическое) хеширование и шифрование, обычно имеют время жизни, по истечении которого считаются либо слишком рискованными для использования, либо просто небезопасными.

Могут возникнуть неполадки, связанные с работой HTTPS, например, при пробросе OWA (веб-интерфейс для доступа к Microsoft Exchange). Столкнувшись с этим, выполните следующие действия для перехода в режим совместимости уровней политики шифрования:

1. Зайдите в консоль Ideco NGFW Novum. Это можно сделать из локального меню, по ssh или через веб-интерфейс Ideco NGFW Novum.

2. Введите в терминале команду `update-crypto-policies --set DEFAULT:FEDORA32`.

3. Перезагрузите Ideco NGFW Novum.



Настоятельно не рекомендуем использовать данную настройку, так как при следующем обновлении Ideco NGFW Novum настройки режима совместимости будут сброшены. В более новых версиях данная возможность будет отключена.

Полезные ссылки

- **ГОСТ VPN**

Восстановление конфигурации из бэкапа

Восстановление в рамках одного сервера

В NGFW Novum возможно полное и мгновенное восстановление из бэкапа.

При выполнении полного восстановления система будет перезагружена для применения настроек сервера.

При мгновенном восстановлении бэкап применяется без перезагрузки. При этом логи журнала **Система** не входят в бэкап, поэтому содержимое журнала не изменяется при восстановлении.

При восстановлении системы из резервной копии информация о лицензии не будет восстановлена, поскольку это может привести к использованию устаревшей лицензии.

После завершения процесса восстановления Ideco NGFW Novum автоматически отправит запрос в личный кабинет для обновления лицензии. Офлайн-лицензию необходимо загрузить самостоятельно.

Если резервное копирование используется для переноса настроек с одного сервера на другой, выполните "перепривязку" лицензии.

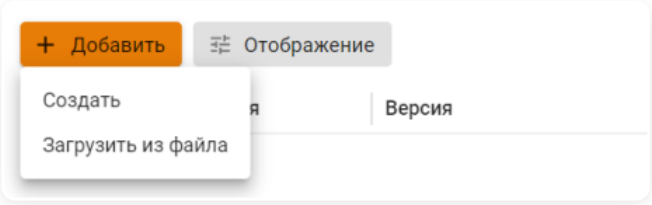
Полное восстановление конфигурации возможно только из бэкапов, версия которых не превышает версию текущей установленной системы.
Например, для Ideco NGFW Novum версии 20 подойдут бэкапы с 19 или 20 версии. При этом важно учитывать минорные версии: например, в версии 19.13 невозможно восстановление из бэкапа, созданного в 19.14.

Мгновенное восстановление возможно только из бэкапа, созданного в той же версии, что и текущая версия на сервере.

Через веб-интерфейс

Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и нажмите кнопку **Полное восстановление** или **Мгновенное восстановление** в столбце **Управление**.

Также можно загрузить бэкап из файла. Например, в случае переноса с другого сервера. Для восстановления конфигураций бэкапа, который находится на внешнем носителе, перейдите на **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

- **Восстановить из бэкапа** - восстановятся все настройки и перезагрузится сервер.
- **Мгновенно восстановить из бэкапа** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

Нажмите **Enter**.

2. Выберите из списка бэкап, введя пункт нужной копии, и нажмите **Enter**.

3. Перезагрузите сервер при запуске полного восстановления, введя **y**, а затем **Enter**. При мгновенном восстановлении перезагрузка не нужна.

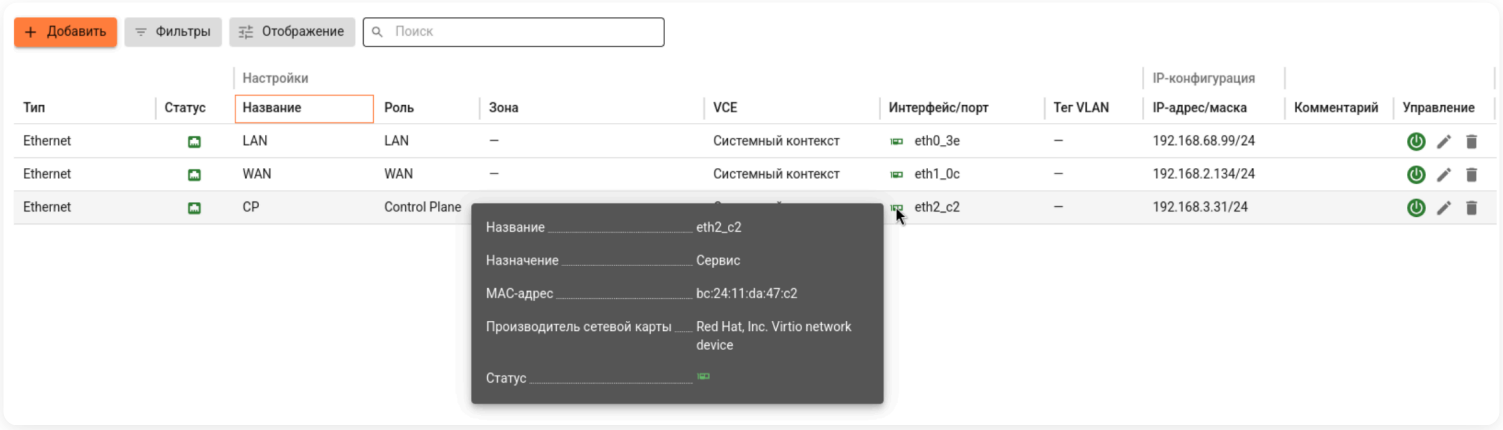
Пример восстановления из бэкапа через локальное меню:

```
Введите номер пункта и нажмите Enter.
# 13

Выберите бэкап для восстановления:

1.
Время:          12.01.2026 14:29:26
Версия:         Ideco NGFW 22.9.297
Комментарий:    backup01
2.
Время:          12.01.2026 14:26:01
Версия:         Ideco NGFW 22.9.297
Комментарий:

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1

Выбран бэкап

Время:          12.01.2026 14:29:26
Версия:         Ideco NGFW 22.9.297
Комментарий:    backup01

Для восстановления из бэкапа необходима перезагрузка.
Перезагрузить сервер и восстановить настройки сейчас?

Пожалуйста подтвердите ваш выбор.

Введите 'y' и нажмите Enter для подтверждения.
Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# y
```

Восстановление на другом сервере

Если необходимо восстановить конфигурацию из бэкапа на другом сервере, установите Ideco NGFW Novum на новый сервер и выполните шаги по восстановлению данных:

1. На новом сервере перейдите в **Сервисы** → **Сетевые интерфейсы**, наведите курсор на значение в столбце **Интерфейс/Порт** и запишите MAC-адрес Control Plane интерфейса:



2. Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите **Добавить** → **Загрузить из файла** и выберите бэкап, скачанный со старого сервера.

3. Нажмите в столбце **Управление** для перезагрузки сервера и применения настроек.

> После перезагрузки веб-интерфейс будет недоступен, так как настройки сетевых интерфейсов были заменены настройками из бэкапа.

4. Зайдите в локальное меню Ideco NGFW Novum, введите логин и пароль.

5. Перейдите в **Ethernet-интерфейсы** → **Изменить интерфейс**:

```
Управление сервером

1. Консоль
2. Физические порты
3. Ethernet-интерфейсы
4. Отключить все статические маршруты и добавить новый
5. Выбор типа кластерной сети
6. Отключить доступ к веб-интерфейсу из внешней сети
7. Включить доступ к серверу по SSH из Интернет
8. Включить доступ к серверу по SSH из локальных сетей
9. Включить режим `Разрешить Интернет всем`
10. Сбросить блокировки по IP
11. Отключить пользовательский межсетевой экран
12. Создать новый бэкап
13. Восстановить из бэкапа
14. Мгновенно восстановить из бэкапа
15. Включить доступ Удаленного Помощника
16. Контакты технической поддержки
17. Восстановиться на предыдущую версию
18. Перезагрузка сервера
19. Отключить сервер
20. Выход

Введите номер пункта и нажмите Enter.
# 3

1. Показать список интерфейсов
2. Создать интерфейс
3. Изменить интерфейс
4. Удалить интерфейс

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 3
```

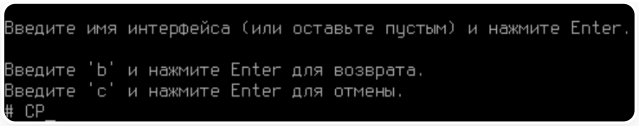
6. Выберите Control Plane интерфейс:

```
Выберите порт

-------------------------------------------------------------------------------------------------
  N    |  Название    |  Роль    |  VCE                |  Порт    |  IP                 |  Статус
-------------------------------------------------------------------------------------------------
  1    |  LAN         |  LAN     |  Корневой контекст  |          |  192.168.155.55/24  |  unknown
-------------------------------------------------------------------------------------------------
  2    |  WAN         |  WAN     |  Корневой контекст  |          |  192.168.1.81/24    |  unknown
-------------------------------------------------------------------------------------------------
  3    |  CP          |  CP      |  Корневой контекст  |          |  192.168.2.83/24    |  unknown
-------------------------------------------------------------------------------------------------

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 3_
```

7. Выберите порт, MAC-адрес которого был записан на шаге 1:

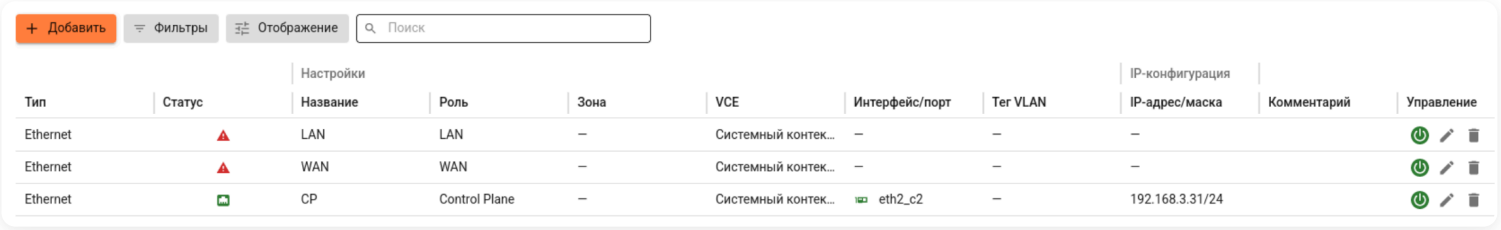
```
Выберите порт

-------------------------------------------------------------------------------------------------
  N    |  Порт                       |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------------
  1    |  Оставить прежние настройки |                     |                |
-------------------------------------------------------------------------------------------------
  2    |  eth0_3e                    |  bc:24:11:1a:f6:3e  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  3    |  eth1_0c                    |  bc:24:11:b2:48:0c  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  4    |  eth2_c2                    |  bc:24:11:da:47:c2  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 4_
```

8. Введите имя интерфейса или оставьте пустым:



9. Настройте Control Plane интерфейс, следуя инструкции с шага 3 в статье Установка в разделе **Настройка интерфейса управления**.

10. Перейдите в веб-интерфейс в **Сервисы** → **Сетевые интерфейсы** и настройте интерфейсы, привязав к ним физические порты:



11. Проверьте корректность настроек в разделах:

- **Сервисы** → **DNS** - внешние DNS-серверы.
- **Сервисы** → **DHCP-сервер** - опции DHCP-сервера.
- **Правила трафика** → **Файрвол** - зоны источника и зоны назначения в правилах.
- **Маршрутизация** → **OSPF** - настройку интерфейсов.
- **Маршрутизация** → **Внешних сетей** - правила маршрутизации.
- **Маршрутизация** → **Балансировка и резервирование** - настройку балансировки и адрес шлюза.

Перенос лицензии

Если сервер переносится из-за неисправности старого, необходимо перепривязать лицензию. Для этого:

1. Перейдите в MY.IDECO.

2. Отвяжите лицензию от старого сервера, нажав на .

3. Отвяжите demo-лицензию от нового сервера, нажав на .

4. Привяжите enterprise-лицензию к новому серверу, нажав **Свободные лицензии** → **Привязать к серверу**.

> В случае возникновения проблем при привязке лицензий обратитесь в Техническую поддержку.

Перенос данных почтового сервера

1. Скопируйте всю почту из папки `/var/mail/` на внешнее хранилище. Это можно сделать с помощью различных программ для копирования файлов между локальным компьютером и удаленным сервером (например: rsync, WinSCP, scp от ssh и др.).

2. Установите с загрузочного образа последнюю версию Ideco NGFW Novum на физический диск.

3. Подключите второй физический диск, который будет использоваться для хранения почты.

4. В веб-интерфейсе Ideco NGFW Novum перейдите в **Почтовый релей** → **Основные настройки**, выберите диск для хранения почты и отформатируйте диск.

5. Разрешите доступ по SSH из локальных сетей в **Управление сервером** → **Администраторы**.

6. Подключитесь к NGFW Novum, например, с помощью программы WinSCP и выгрузите всю скопированную почту по пути `/var/spool/mail/`.

7. По окончании выгрузки файлов почты выполните команду:

```
chown -R ideco-mail-backend:ideco-mail-backend /var/spool/mail/
```

> Команда выше меняет владельца и группу для файлов почты, чтобы почтовый демон `dovecot` мог иметь доступ к этим файлам.

> Если на Ideco NGFW Novum настроен кластер, то перед работой с бэкапами нужно ознакомиться с особенностями работы бэкапов:

- Невозможно полное восстановление из бэкапов. При этом можно создать резервную копию и после разрушения кластера восстановить копию на ноде, которая была активной.
- На активной ноде доступно **Мгновенное восстановление из бэкапа**. Восстанавливаются все настройки, кроме статистики в отчетах. Данные на второй ноде также придут в соответствие с восстановленными настройками после синхронизации нод.

Полезные ссылки

- **Бэкапы**

Публикация ресурсов

Доступ из внешних сетей без NAT

Перейти >

Портмаппинг (проброс портов, DNAT)

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

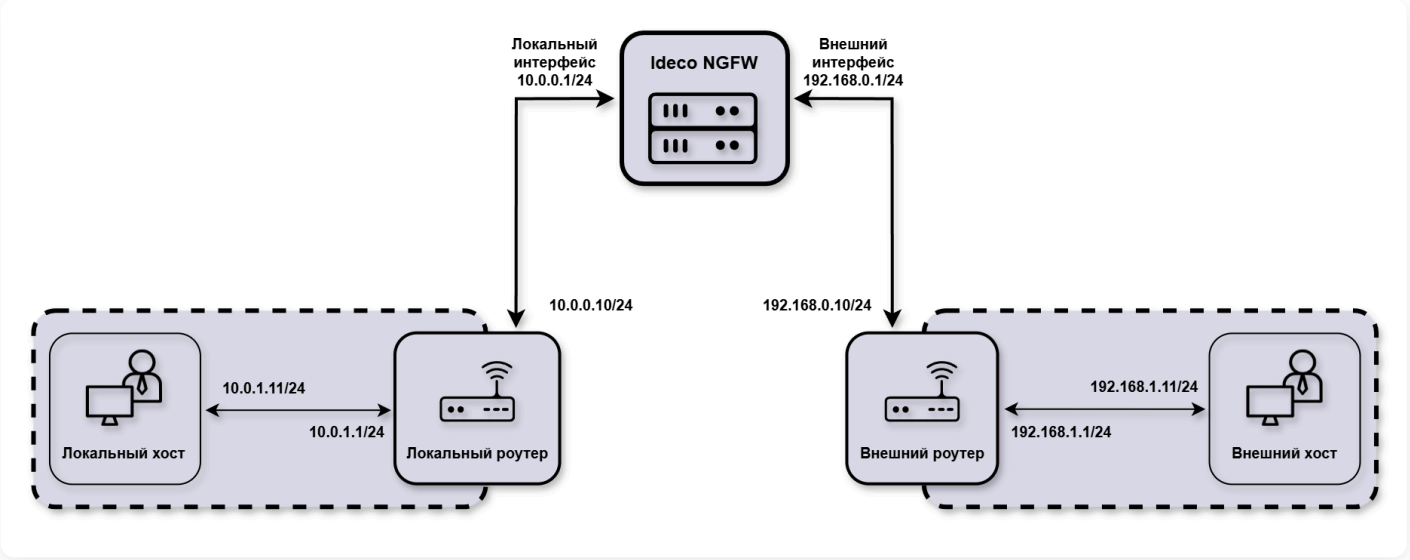
Доступ из внешних сетей без NAT

Классический контекст | Высокопроизводительный контекст

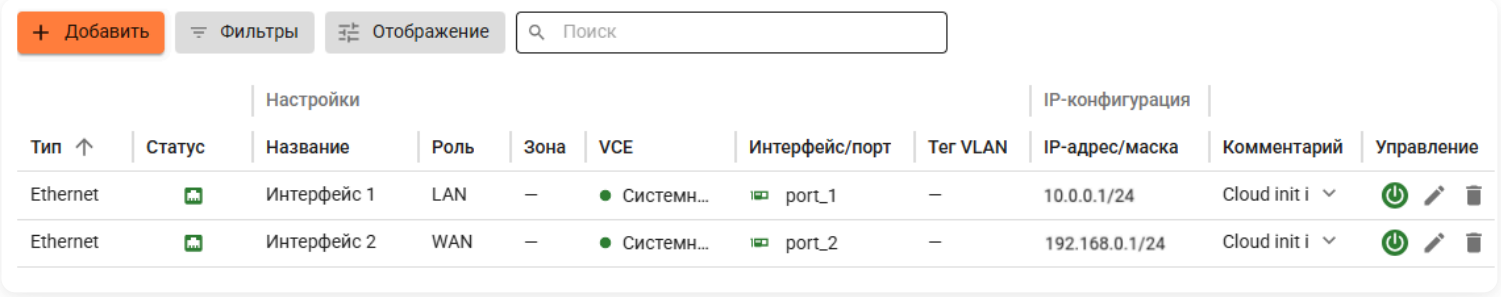
Если Ideco NGFW Novum расположен не на границе с интернетом, а внутри локальной сети, и при этом одна из подключенных сетей считается внешней, доступны действия:

- Организовать прямой доступ к ресурсам внешних по отношению к Ideco NGFW Novum сетей без использования NAT.
- Разрешить доступ из внешних относительно Ideco NGFW Novum сетей в локальную сеть с прямым обращением к локальным IP-адресам.

Пример. Настройка Ideco NGFW Novum для доступа без NAT в следующей конфигурации сети:



1. Настройте сетевые интерфейсы в **Сервисы** → **Сетевые интерфейсы** → **Интерфейсы** на Ideco NGFW Novum:



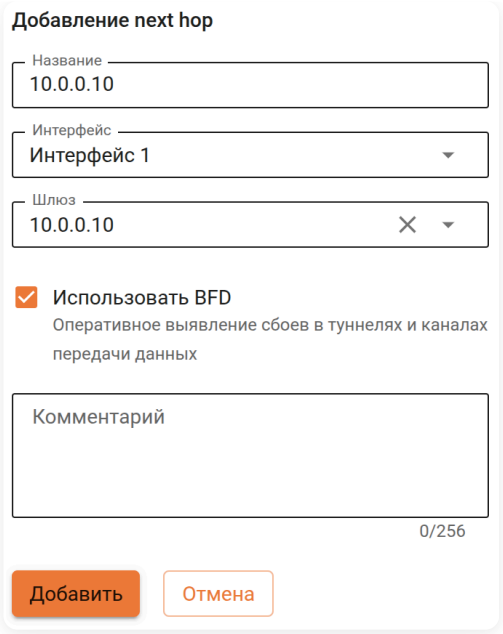
- С ролью **LAN** - интерфейс для доступа в пользовательскую локальную сеть.
- С ролью **WAN** - интерфейс для доступа в пользовательскую внешнюю сеть.

2. В разделе **Маршрутизация** создайте правила для доступа к IP-адресам пользователей, которые находятся за маршрутизаторами:

Для Локальных сетей

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

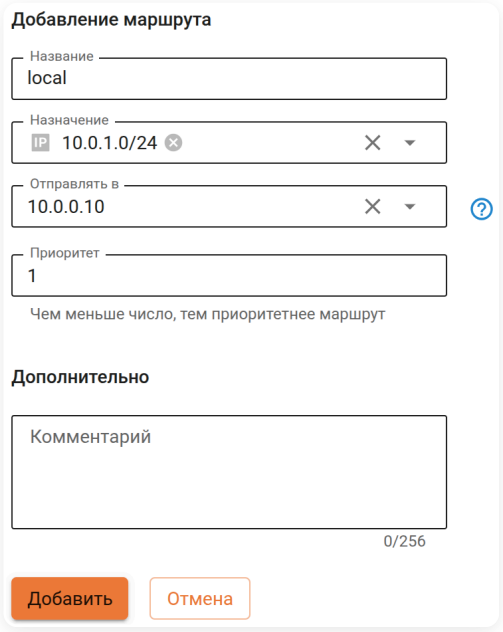
2. Заполните поля и нажмите **Добавить**:



- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс для доступа в пользовательскую локальную сеть.
- **Шлюз** - укажите адрес маршрутизатора (`10.0.0.10`).

3. Перейдите в **Маршрутизация** → **Статическая** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:



- **Название** - укажите название.
- **Назначение** - выберите адрес локальной сети за маршрутизатором (`10.0.1.0/24`).
- **Отправлять в** - выберите созданный на шаге 2 **Next hop**.

Для Внешних сетей

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

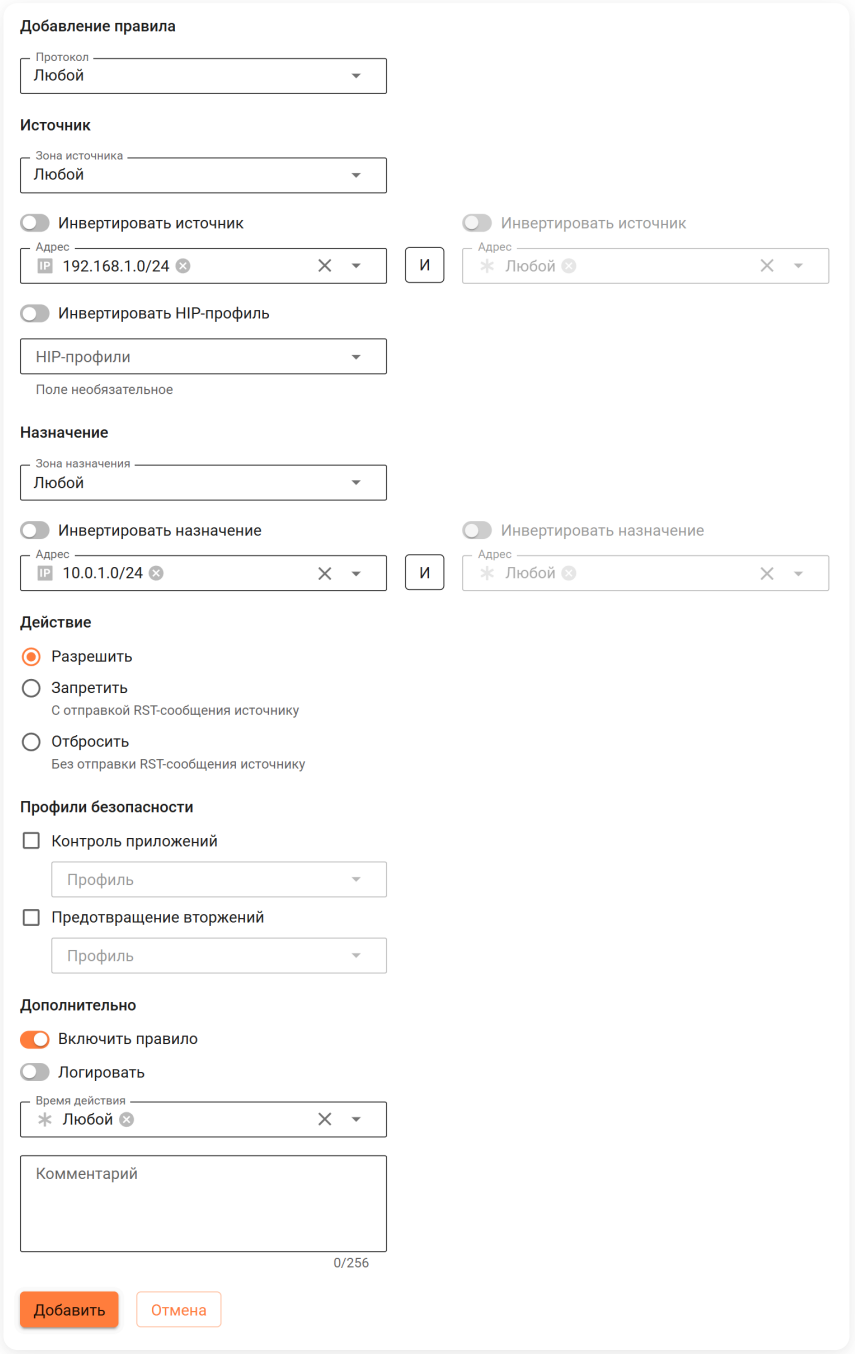
- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс для доступа в пользовательскую внешнюю сеть.
- **Шлюз** - укажите адрес маршрутизатора (`192.168.0.10`).

3. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:

- **Название** - укажите название.
- **Назначение** - выберите адрес внешней сети за маршрутизатором (`192.168.1.0/24`).
- **Отправлять в** - выберите созданный на шаге 2 **Next hop**.

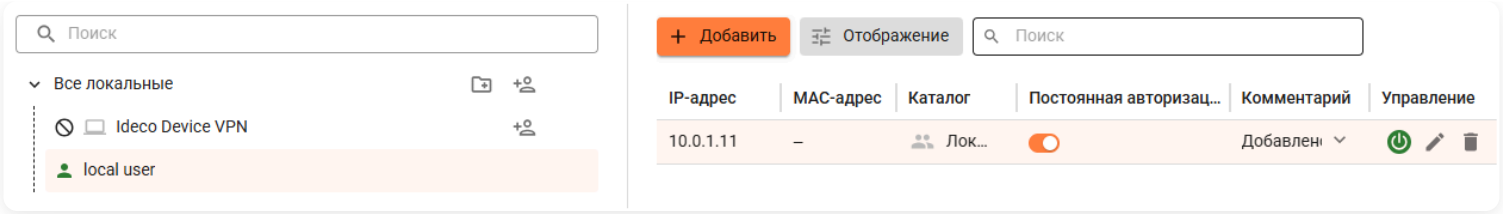
3. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**, создайте и включите правило для доступа хостов из внешней сети `192.168.1.0/24` до IP-адресов пользователей локальной сети `10.0.1.0/24`:



Правило необходимо, чтобы разрешить трафик в пользовательской цепочке **FORWARD**. Трафик из внешних сетей в локальные, не указанный в таблице **FORWARD**, будет заблокирован системным правилом.

4. Перейдите в **Правила трафика** → **Межсетевой экран** → **SNAT** и отключите опцию **Автоматический SNAT локальных сетей**.

5. Перейдите в **Пользователи** → **Учетные записи** и включите опцию **Постоянная авторизация** для пользователей локальной сети `10.0.1.0/24` на вкладке **IP и MAC авторизация**. Устройства локальной сети должны быть авторизованы на NGFW:



Учитывайте риски подобного доступа с точки зрения информационной безопасности. Не предоставляйте доступ для внешних сетей и хостов, в безопасности которых не уверены.

Полезные ссылки

- **Межсетевой экран**
- **Статическая маршрутизация**

Портмаппинг (проброс портов, DNAT)

Сервер предоставляет доступ к опубликованному в интернете веб-ресурсу (сервису, сетевой службе) на устройстве в локальной сети с серым IP-адресом. Ресурс публикуется путем трансляции (проброса) любого неиспользуемого сетевого порта на публичном IP-адресе сервера Ideco NGFW Novum на порт ресурса, работающего на устройстве в локальной сети. При этом все обращения из внешних сетей на публичный адрес сервера Ideco по транслируемому порту перенаправляются на публикуемый порт данного ресурса. Эта технология называется DNAT, portmapper или port forwarding.

Для настройки портмаппинга в Ideco NGFW Novum добавьте правило в **Правила трафика** → **Межсетевой экран** → **DNAT**. При создании правила укажите адреса сервера, публикуемой машины и сетевого порта, с которого и на который осуществляется трансляция сетевых запросов извне.

Создайте разрешающее FORWARD-правило, если:

- В таблице FORWARD есть запрещающее прохождение трафика правило. В этом случае поместите созданное правило выше запрещающего.
- Нужна проверка трафика профилями безопасности. В этом случае укажите в правиле нужные профили **Контроля приложений** или **Предотвращения вторжений**.
  Укажите при создании правила назначение (адрес устройства в локальной сети) и порт назначения.

> **Не рекомендуется использовать проброс портов для публикации веб- и почтовых серверов (80, 443 порты).** Для публикации портов воспользуйтесь обратным прокси-сервером.

Особенности создания правил DNAT с версии 18

- В предыдущих версиях профили безопасности настраивались в отдельных разделах. С версии 18 **Контроль приложений** настраиваются в правилах **Межсетевого экрана**.
- Для проверки трафика модулем **Контроль приложений** и системой **Предотвращения вторжений** необходимо создать FORWARD-правило с включенными настройками профилей безопасности.
- В случае проблем с доступом до публикуемой службы проверьте **Отчеты и журналы** → **События безопасности** → **Журнал IPS** и при необходимости отредактируйте правила нужного профиля **Предотвращения вторжений**.

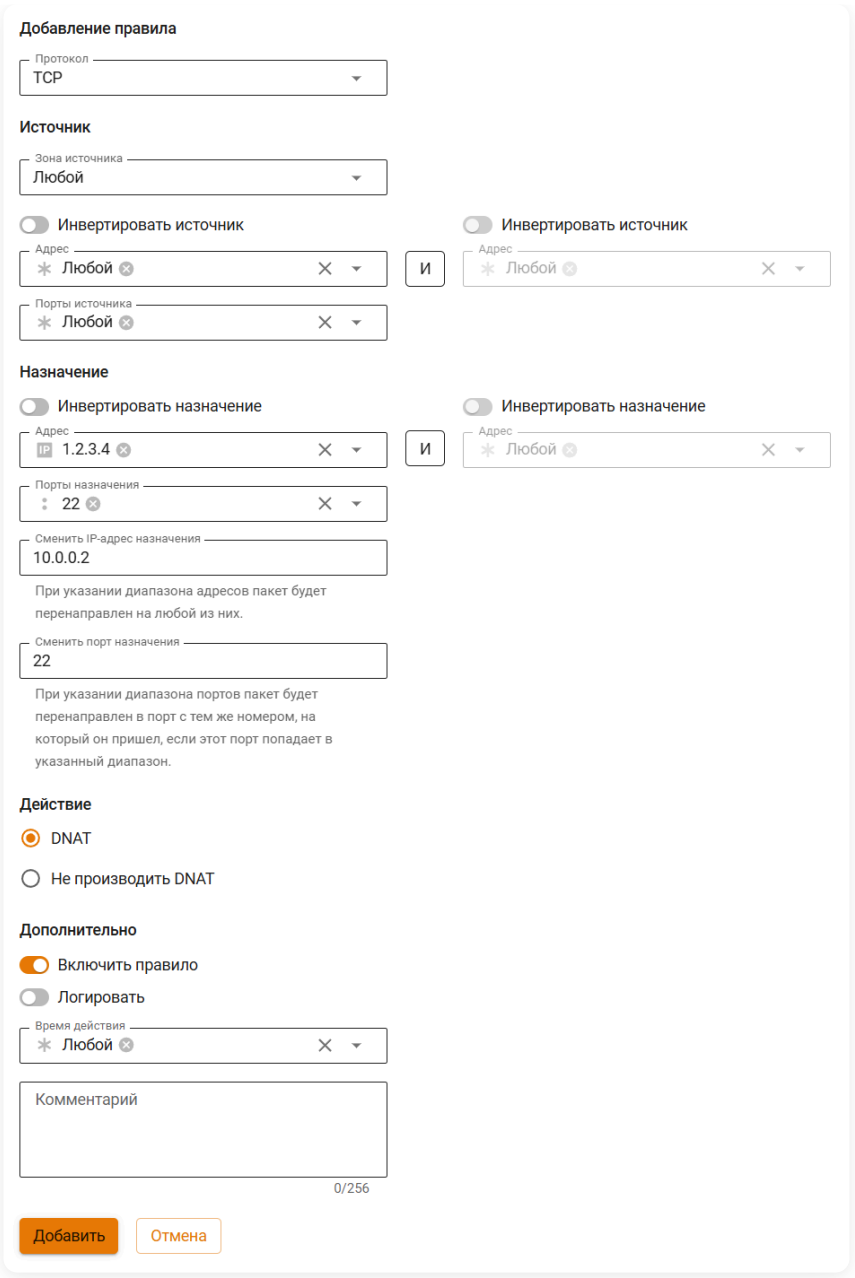
Создание правил DNAT и FORWARD в Межсетевом экране Ideco NGFW Novum

Пример:

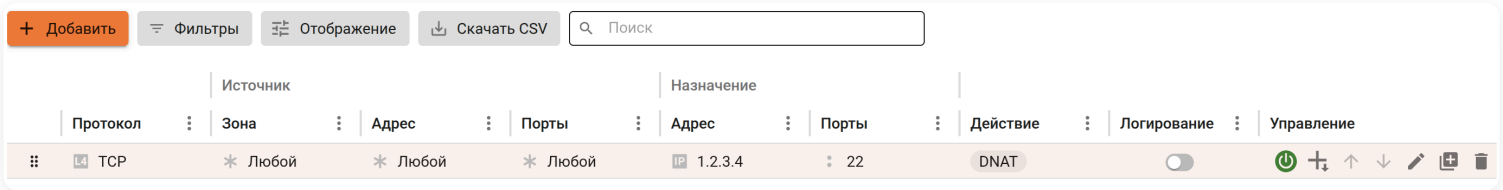
- Публичный адрес сервера Ideco - `1.2.3.4`.
- Публикуемая служба - SSH, работающая на 22 TCP-порте.
- Адрес компьютера в локальной сети, где запущена служба, к которой нужен доступ извне - `10.0.0.2`.

Для настройки трансляции запросов к службе извне через сервер Ideco NGFW Novum на устройство в локальной сети перейдите в **Правила трафика** → **Межсетевой экран** → **DNAT** и нажмите **Добавить**.

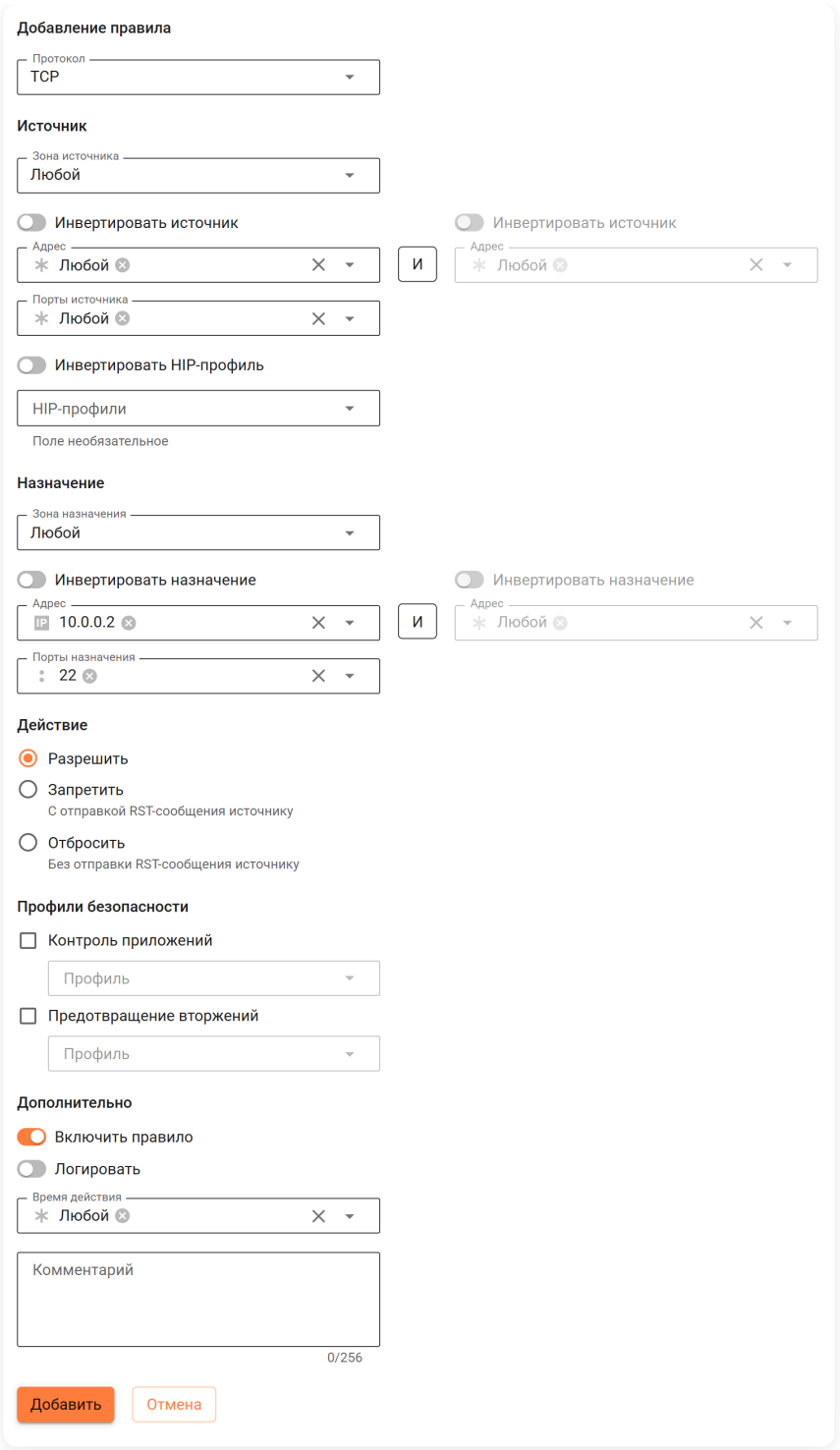
Заполните поля в соответствии с характеристиками, указанными в примере:



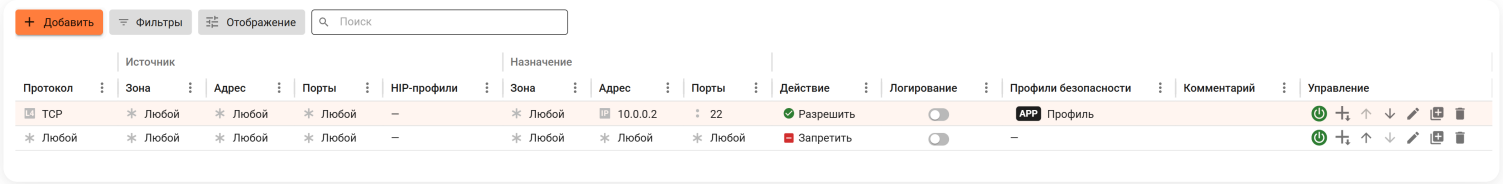
Вид правила в таблице после сохранения:



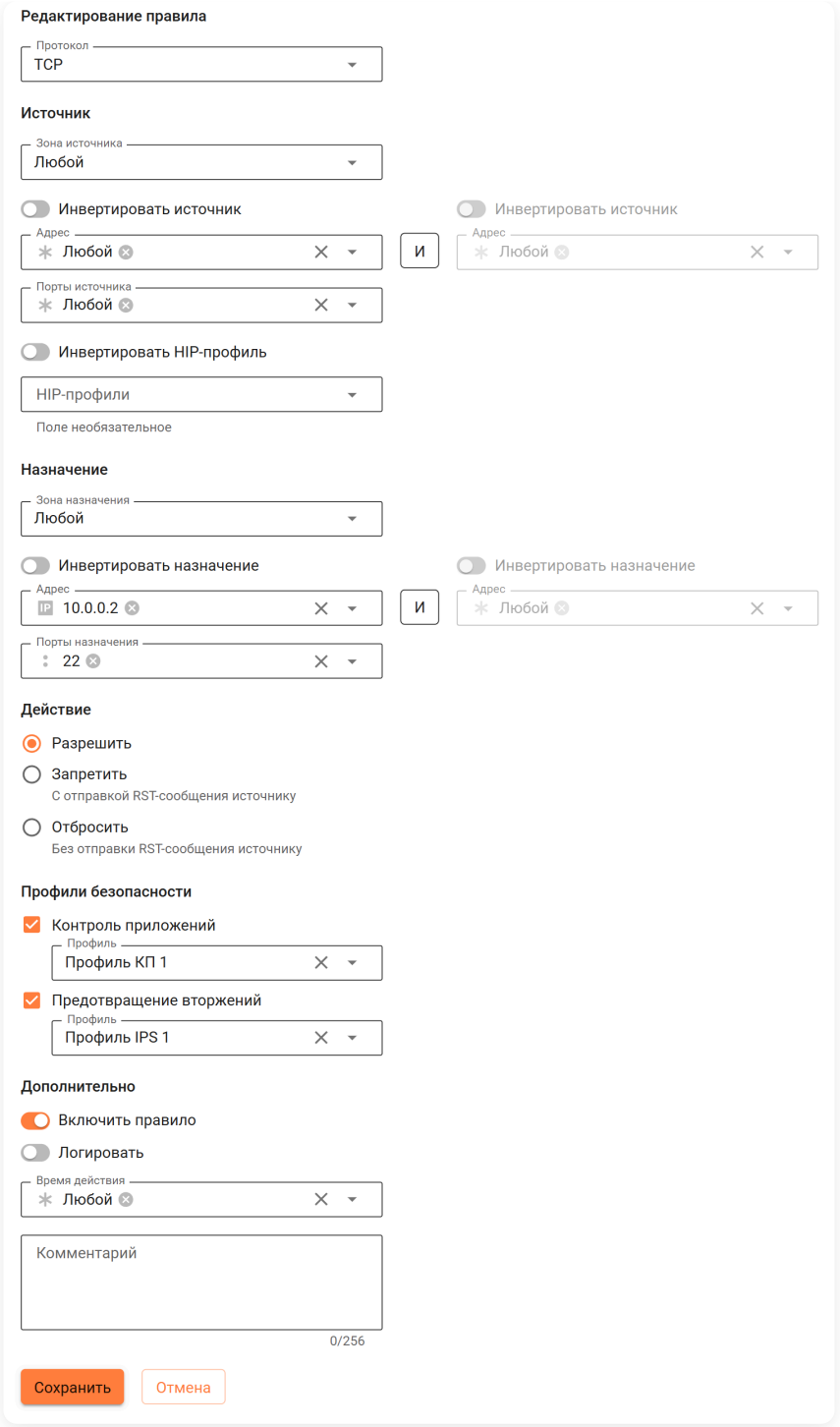
Проверьте наличие запрещающих правил в таблице **FORWARD**. При необходимости создайте правило, разрешающее трафик:



Поместите созданное правило выше запрещающего трафик:



Если хотите, чтобы трафик проверялся профилями безопасности, включите в созданном правиле соответствующие настройки:



Настройки **Межсетевого экрана** применяются сразу при создании правил.

Частые ошибки

- Если включен режим **Полный доступ**, правила **Межсетевого экрана**, включая таблицу **DNAT**, не работают. При этом трафик пользователя проходит Аппаратную и Предварительную фильтрацию. Если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет.

Рекомендации

- Проверять работу правила **DNAT** следует из внешней сети. Если необходим доступ из локальной сети, используйте обратный прокси-сервер для публикации веб-ресурсов.
- Порт на внешнем интерфейсе сервера, с которого транслируются запросы, не всегда совпадает с публикуемым портом самой службы. Например, для предотвращения автоматических попыток подключения вредоносного ПО на популярный сервис внешние запросы транслируются на порт 4489, а в локальную сеть - на порт 3389.
- Для защиты от нежелательных подключений к публикуемой службе при создании правила укажите в поле **Источник** IP-адрес или подсеть, с которой разрешено подключаться к этой службе.
- Если осуществляется трансляция на один и тот же номер порта локального сервера, заполнять поле **Сменить порт назначения** не обязательно. Система автоматически переадресует запрос на соответствующий порт устройства в локальной сети.

Устранение неполадок

- Убедитесь, что клиент, на которого осуществляется проброс портов, отвечает на эхо-запросы ping к внешним ресурсам. Основным шлюзом на данном устройстве следует указать локальный IP-адрес Ideco NGFW Novum, либо прописать маршрут.
- При правильной настройке публикуемая служба отвечает клиенту во внешней сети через тот же внешний интерфейс сервера, с которого изначально пришел запрос. Настройте правильный адрес SNAT для опубликованного сервиса с помощью создания правил в таблице SNAT, если в созданном правиле в поле **Назначение** указан публичный IP-адрес сервера для приема подключений извне, а также в случае переопределения автоматических правил NAT.
- Правило трансляции запросов на сервере не работает, если брандмауэр Windows или другие программы защиты блокируют соединения с внешних адресов в интернете. Для диагностики убедитесь, что настройки встроенного брандмауэра Windows или сторонних файрволов и антивирусов разрешают целевое соединение. Например, для проверки настроек брандмауэра на устройстве Windows перейдите в **Панель управления → Брандмауэр Защитника Windows → Дополнительные параметры → Правила для входящих подключений / Правила для исходящих подключений**.
- Правило портмаппинга пробрасывает трафик из внешней сети на хост в локальной сети. Трафик запроса ресурса из этой же локальной сети при обращении на внешний адрес не будет проброшен правильно. Во избежание асимметричной маршрутизации при диагностике сетевыми утилитами подключайтесь из внешних для NGFW сетей, а внутри локальной сети обращайтесь к сервису по IP-адресу сервиса в локальной сети. Альтернативный вариант - вынесите ресурс в отдельную локальную сеть, DMZ и обращайтесь к ресурсу из локальной сети клиентов по внешнему IP-адресу.

Полезные ссылки

- **Межсетевой экран**

Интеграции

Практические руководства по интеграции Ideco NGFW со сторонними решениями

Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG

Перейти >

Настройка совместной работы ViPNet Координатор с Ideco NGFW

Перейти >

Интеграция NGFW и SkyDNS

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка кластера Active/Active с брокером сетевых пакетов DS Integrity NG

В Ideco NGFW Novum реализована кластеризация Active/Passive. Повысить отказоустойчивость можно, создав кластер Active/Active. Для этого воспользуйтесь решением наших партнеров АО "НПП "Цифровые решения" - брокером сетевых пакетов DS Integrity NG.

Расположите брокер сетевых пакетов перед Ideco NGFW Novum. Брокер будет самостоятельно балансировать трафик устройств в локальной сети между нодами созданного кластера.

При падении одной ноды трафик перебалансируется между остальными Ideco NGFW Novum без перерыва в связи. Это реализует схему кластера Active/Active.

Объединять в кластер устройства Ideco NGFW Novum между собой не нужно.

Для корректной работы нод установите одинаковые настройки.

Для централизованного управления нодами Ideco NGFW Novum воспользуйтесь Ideco Center.

Особенности использования схемы:

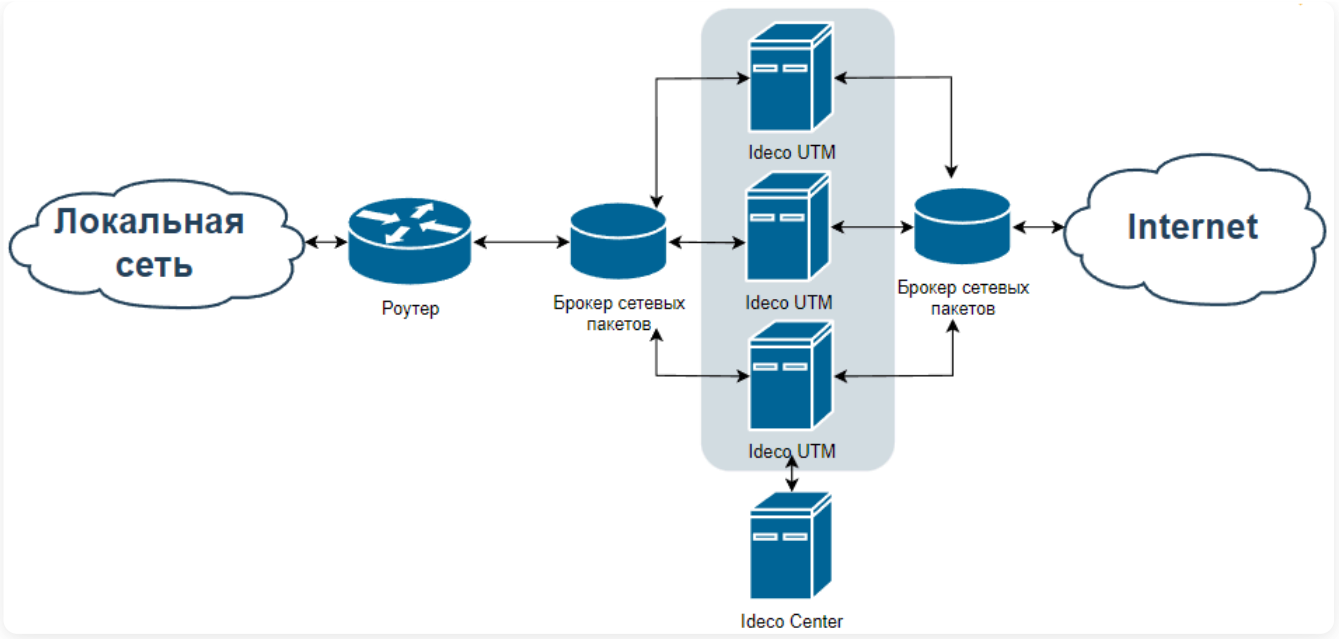
- Настройки, которые нельзя распространить через Ideco Center, придется вручную изменять на каждом Ideco NGFW Novum.
- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.
- Данные отчетности, логов и мониторинга не синхронизируются между нодами. В каждой ноде хранятся свои данные.
- Восстановление из бэкапа и обновление системы будет затрагивать только одну ноду. Каждую ноду потребуется обновлять отдельно.
- Между локальной сетью и брокером сетевых пакетов потребуется расположить роутер с настроенной динамической маршрутизацией (OSPF) для обмена маршрутами.
- На каждую ноду Ideco NGFW Novum потребуется отдельная лицензия. По вопросам условий лицензирования при использовании такой конфигурации обратитесь к менеджерам.

Примеры трех типовых схем совместного использования брокера сетевых пакетов DS Integrity NG и Ideco NGFW Novum ниже. На этой основе встройте оба решения в свою сеть.

На каждом Ideco NGFW Novum для обмена маршрутами необходимо настроить OSPF для всех локальных интерфейсов. Название зоны и вес должны быть идентичными настроенным ранее на роутере. Информация о настройке OSPF описана в статье OSPF. Там же находятся инструкции для настройки OSPF для MikroTik, который можно использовать в качестве роутера.

По вопросам настройки брокера обращайтесь в техническую поддержку АО "НПП "Цифровые решения".

Пример 1 - Два брокера, по одному со стороны локальной и внешней сетей



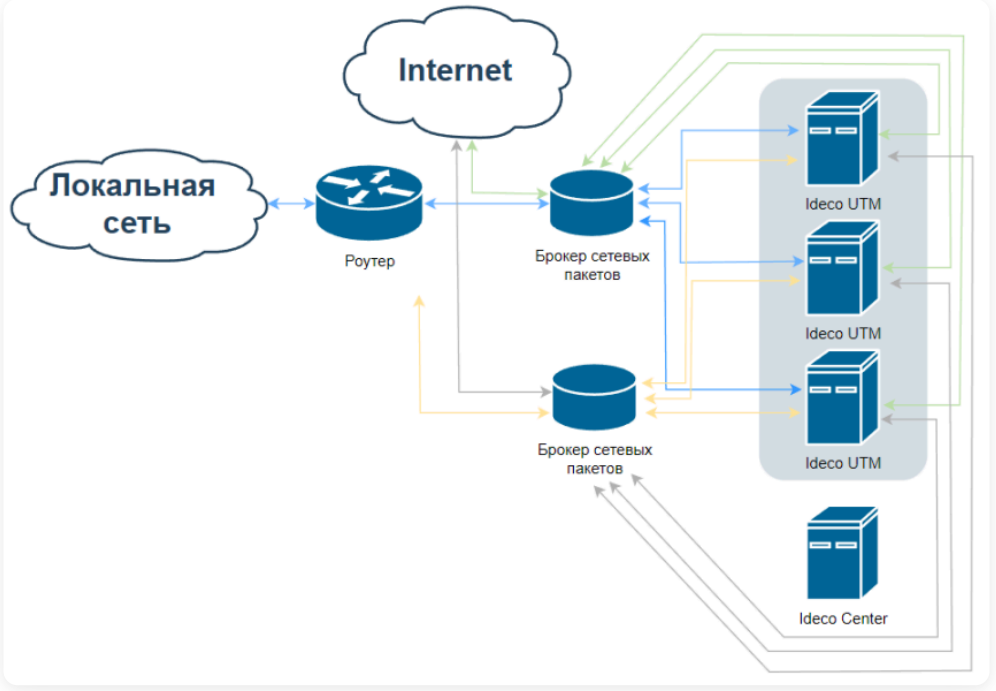
Настройка Ideco NGFW Novum:

На каждом устройстве Ideco NGFW Novum необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW Novum.

На каждом Ideco NGFW Novum в качестве шлюза внешнего интерфейса нужно использовать IP-адрес, полученный от провайдера.

Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW Novum



Настройка Ideco NGFW Novum

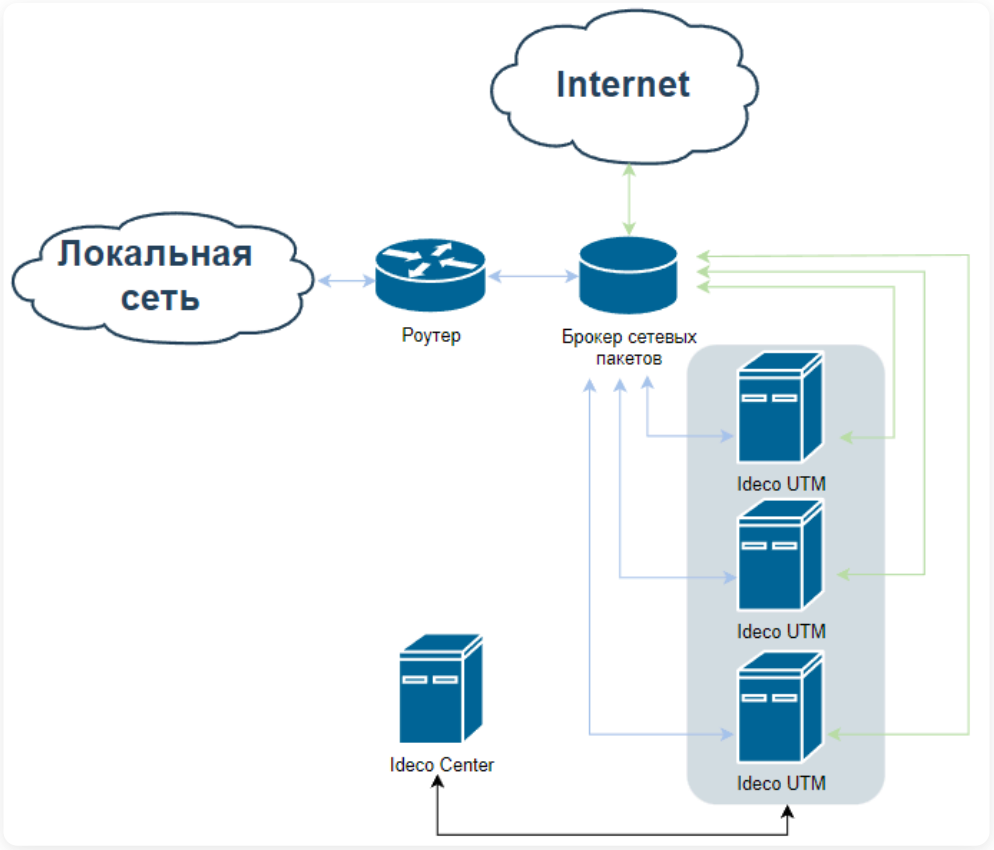
На каждом устройстве Ideco NGFW Novum необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW Novum.
- На каждом NGFW будет два локальных и два внешних интерфейса. Шлюзом внешних интерфейсов нужно указать IP-адрес, полученный от провайдера.

На Ideco NGFW Novum в этой конфигурации в разделе **SD-WAN** → **Профили next hop** должен быть активирован режим резервирования. Приоритетным внешним интерфейсом должен быть выбран интерфейс, который идет к основному брокеру сетевых пакетов.

Пример 3 - Один брокер, расположенный перед Ideco NGFW Novum



Настройка Ideco NGFW Novum

На каждом устройстве Ideco NGFW Novum необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW Novum.
- Шлюзом внешнего интерфейса нужно указать IP-адрес, полученный от провайдера.

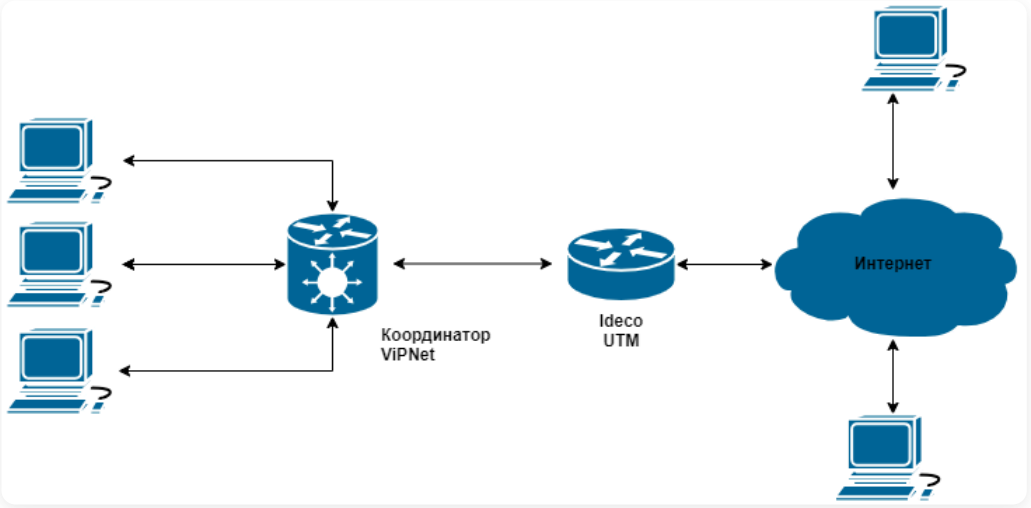
Полезные ссылки

- **Кластеризация**

Рекомендации по настройке NGFW для работы совместно с ViPNet-координатором

ViPNet-координатор используется для шифрования трафика подсети, в которой является шлюзом. Шифрование позволяет обеспечить конфиденциальность информации, передаваемой по незащищенному каналу.

Схема совместной работы Ideco NGFW Novum с ViPNet-координатором:



Настройка Ideco NGFW Novum и ViPNet-координатора

Для корректной работы Координатора совместно с NGFW выполните действия:

1. Настройте проброс порта udp 55777 на IP адрес координатора в **Межсетевой экран → DNAT (перенаправление портов)**.

2. Переведите Координатор в режим **Со статической трансляцией адресов**.

Работа Координатора в режиме динамической трансляции адресов совместно с Ideco NGFW Novum не гарантируется.

Более подробно о настройке ViPNet можно узнать в статье.

Полезные ссылки

- **Межсетевой экран**

Интеграция NGFW и SkyDNS

Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

Чем может быть полезна интеграция

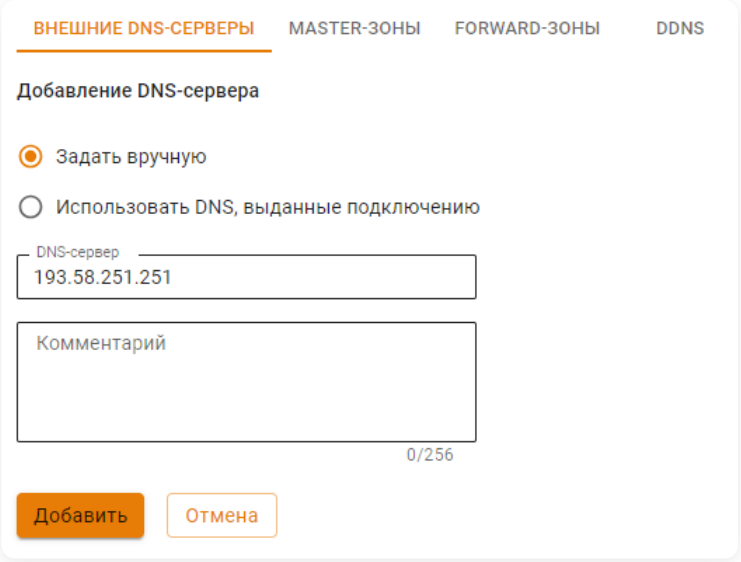
- **Защита от зараженных сайтов**. Вредоносные скрипты могут содержать сайты, как взломанные злоумышленниками, так и созданные специально для распространения вредоносного ПО.
- **Защита от бот-сетей**. Созданные из зараженных вредоносными программами компьютеров сети используются в DDoS-атаках на серверы, рассылках спама, похищениях паролей от интернет-банков и сервисов и в других целях. DNS-фильтрация ограничивает доступ к выявленным серверам для управления бот-сетями. В результате злоумышленники не смогут управлять компьютером, даже если компьютер заражен вредоносной программой.
- **Защита от нежелательных сайтов**. SkyDNS фильтрует интернет-ресурсы по более чем 50 категориям, что повышает качество фильтрации нежелательного контента.
- **Соблюдение 436-ФЗ О защите детей от информации, причиняющей вред их здоровью и развитию**. Сервис SkyDNS полностью соответствует требованиям Правил подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети интернет Минобрнауки РФ.

Настройка интеграции Ideco NGFW Novum и SkyDNS

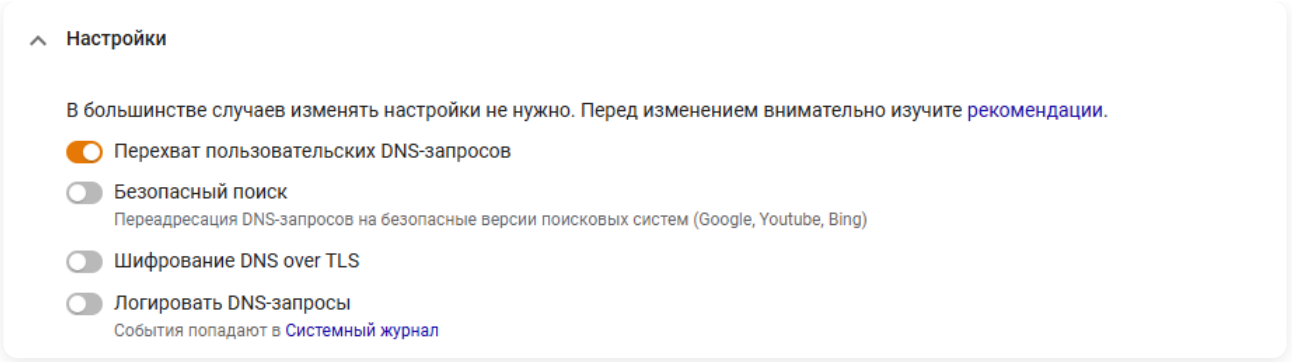
Чтобы настроить интеграцию со SkyDNS, выполните действия:

1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы** и нажмите **Добавить**.

2. Выберите пункт **Задать вручную** и в поле **DNS-сервер** введите IP-адрес DNS-сервера SkyDNS (`193.58.251.251`) и нажмите **Добавить**:

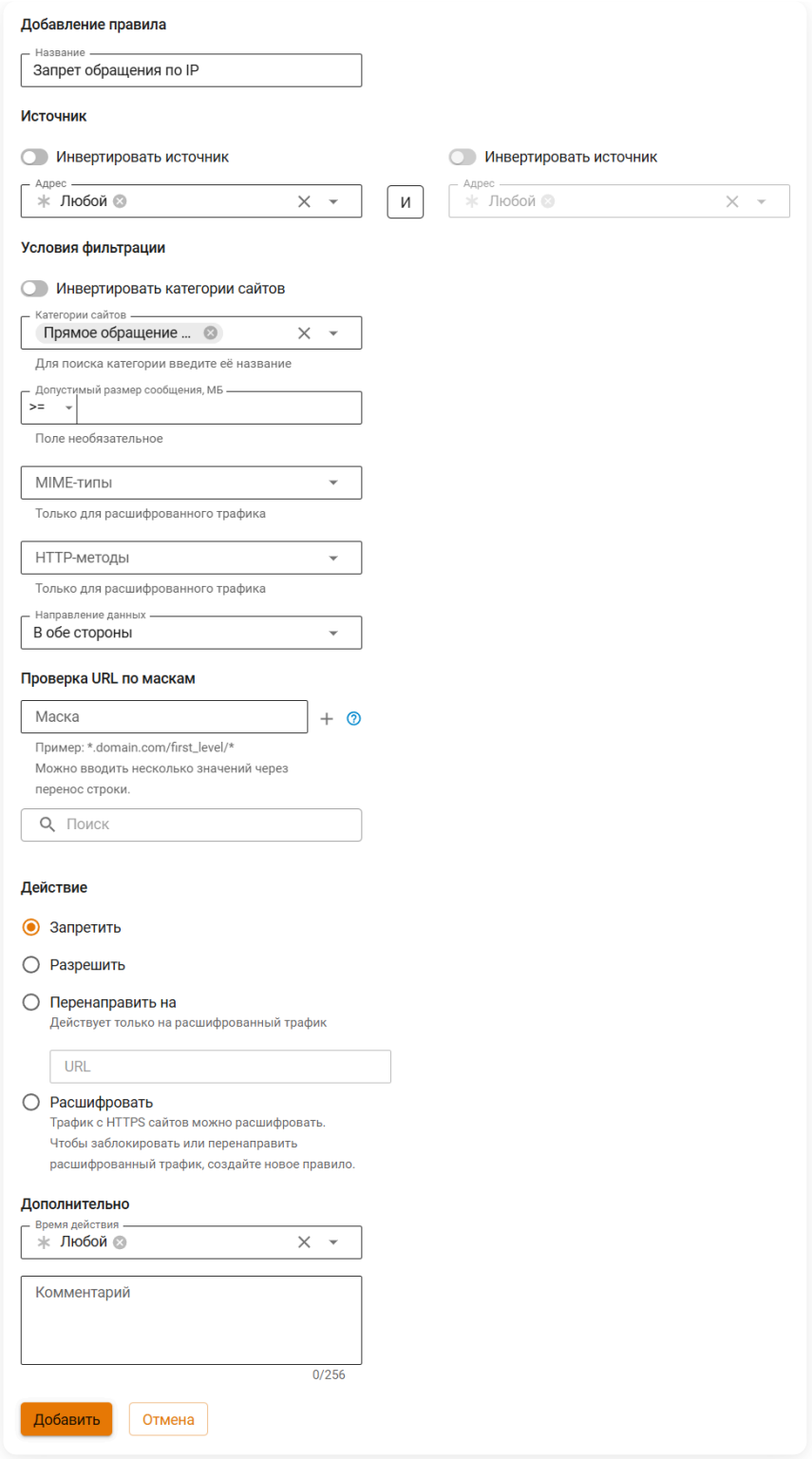


3. В настройках DNS включите опцию **Перехват пользовательских DNS-запросов** для запрета обращения к другим DNS-серверам (если фильтрация через SkyDNS обязательна для всей сети):



4. Если внутри локальной сети или внутри сети провайдера есть внутренняя DNS-зона, не обслуживаемая внешними DNS-серверами (например, домен Active Directory), укажите внутреннюю DNS-зону в разделе **DNS** → **FORWARD-ЗОНЫ**.

5. Перейдите в **Правила трафика** → **Контент-фильтр** и создайте правило запрета прямого обращения к сайтам по IP-адресу:



6. Пропишите IP-адрес локального интерфейса Ideco NGFW Novum в качестве единственного DNS-сервера в сетевых настройках на всех устройствах, которые требуется защитить.

Пользователи, получающие адреса автоматически через DHCP-сервер Ideco NGFW Novum или подключающиеся по VPN, получают нужные настройки автоматически.

Чтобы исключить некоторые компьютеры из фильтрации, пропишите на них другой внешний DNS-сервер (например, 8.8.8.8) и не включайте **Перехват пользовательских DNS-запросов**.

7. При наличии у Ideco NGFW Novum статического белого IP-адреса привяжите адрес к аккаунту SkyDNS в личном кабинете на сайте SkyDNS (в разделе **Настройки → Сети**).

8. Настройте запрет доступа к сайтам по категориям безопасного поиска и другие сервисы в личном кабинете на сайте SkyDNS.

Документация по настройке и активации сервиса SkyDNS

Документация доступна на сайте сервиса.

По вопросам настройки сервиса обращайтесь в техническую поддержку SkyDNS.

Схема фильтрации веб-трафика при использовании SkyDNS



Полезные ссылки

- **DNS**

Решение проблем

Диагностика и устранение типичных проблем при работе с Ideco NGFW

Доступ в интернет

Решение проблем с доступом в интернет через Ideco NGFW

Перейти >

VPN

Решение проблем с VPN-подключениями в Ideco NGFW

Перейти >

Ошибки при авторизации

Устранение ошибок при авторизации пользователей в Ideco NGFW

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Доступ в интернет

Решение проблем с доступом в интернет через Ideco NGFW

Что делать, если IP попал в черные списки DNSBL

Перейти >

Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Перейти >

Что делать, если не работает интернет

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Что делать, если IP попал в черные списки DNSBL

Если используется белый статический IP-адрес, то попадание IP-адреса в черные списки может означать, что в сети зафиксирована бот-активность, участие в DDoS-атаках либо рассылка спама.

Наличие в черных списках динамического IP-адреса из "домашних" диапазонов IP-адресов провайдеров в целом нормальное явление, т. к. вредоносная активность в таком случае может исходить не из вашей сети.

Порядок действий при попадании в черный список

1. Узнайте причину попадания в DNSBL-список. Часто сервис называет конкретный вирус или сетевой червь и особенности - используемые порты, протоколы. Выполните рекомендации сервиса.

2. Активируйте систему предотвращения вторжений на шлюзе. Проанализируйте логи, наличие обращений к командным центрам ботнетов.

3. Проверьте все компьютеры сети антивирусом. Убедитесь, что антивирусная защита активирована, базы обновлены (как правило, вирусы мешают обновлению баз или работе антивирусного ПО).

4. После лечения зараженных компьютеров отправьте в DNSBL-сервис сообщение с просьбой исключить IP из черного списка.

Ideco NGFW Novum

Наше решение обладает всей функциональностью, обеспечивающей максимальную защиту от спам-ботов, ботнет-клиентов и предотвращение вирусной активности в сети.

До 22 пользователей - решение предоставляется бесплатно. Для 10000 пользователей доступна 40-дневная пробная версия.

Скачать Ideco NGFW Novum

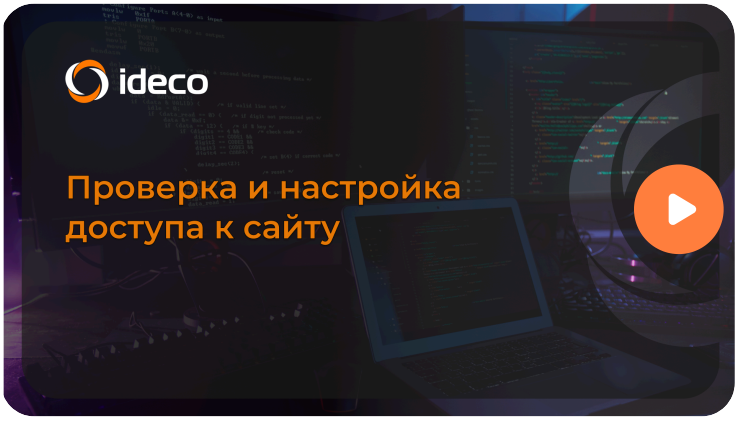
Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube



Перед проверкой модулей фильтрации NGFW убедитесь, что на работу сайта не влияют:

- Технические проблемы на самом ресурсе.
- Блокировка со стороны провайдера.
- Некорректная работа устройства пользователя и т.д.

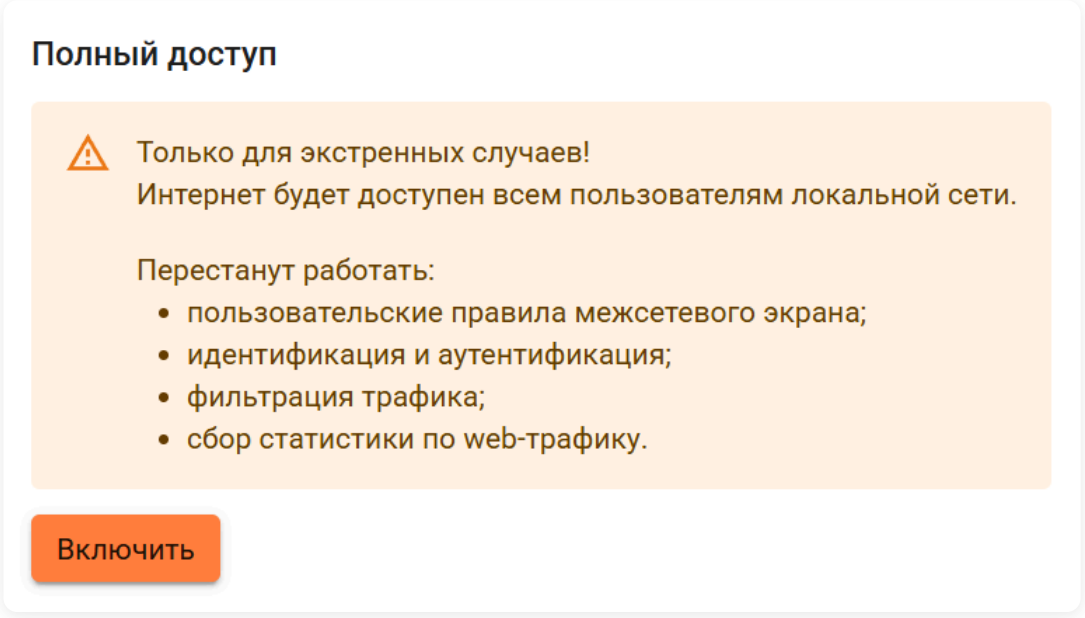
Откройте сайт с устройства вне локальной сети NGFW. Например, со смартфона через мобильный интернет. Если сайт доступен, перейдите в веб-интерфейс NGFW.

Для определения модуля фильтрации, блокирующего сайт, можно проверить логи в разделах Системный журнал. Это может помочь определить причину возникшей проблемы и более точно диагностировать.

Шаг 1. Проверьте, открывается ли сайт в режиме **Полный доступ**

1. Нажмите на в верхней правой части веб-интерфейса NGFW.

2. Нажмите **Включить** в блоке **Полный доступ**:



3. Откройте сайт.

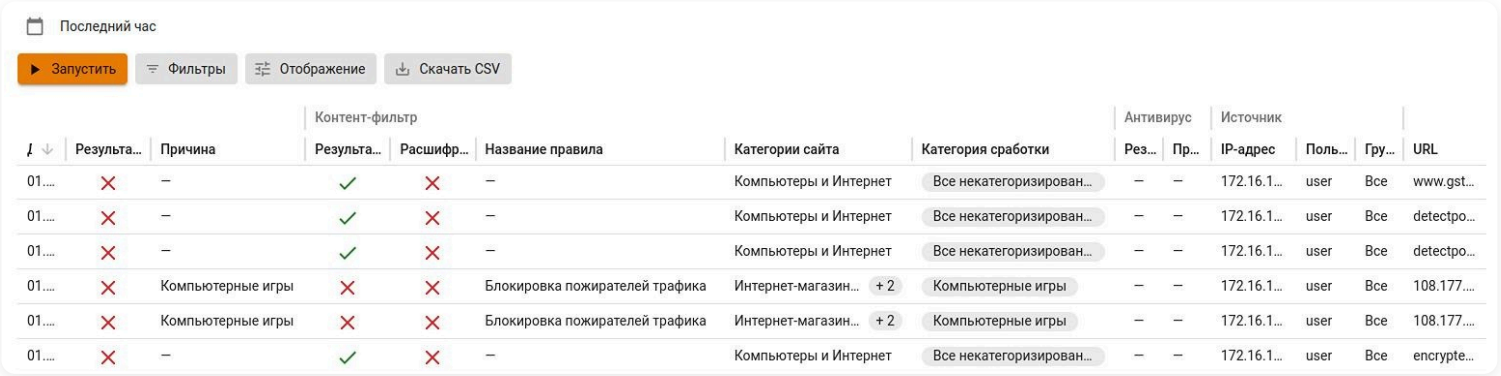
Если сайт не открывается, проверьте, откроется ли сайт на другом устройстве с того же IP-адреса:

- Если не открывается, рекомендуем обратиться к провайдеру. Скорее всего, провайдер блокирует IP-адрес или адрес сайта.
- Если сайт открывается, проверьте настройки устройства пользователя.

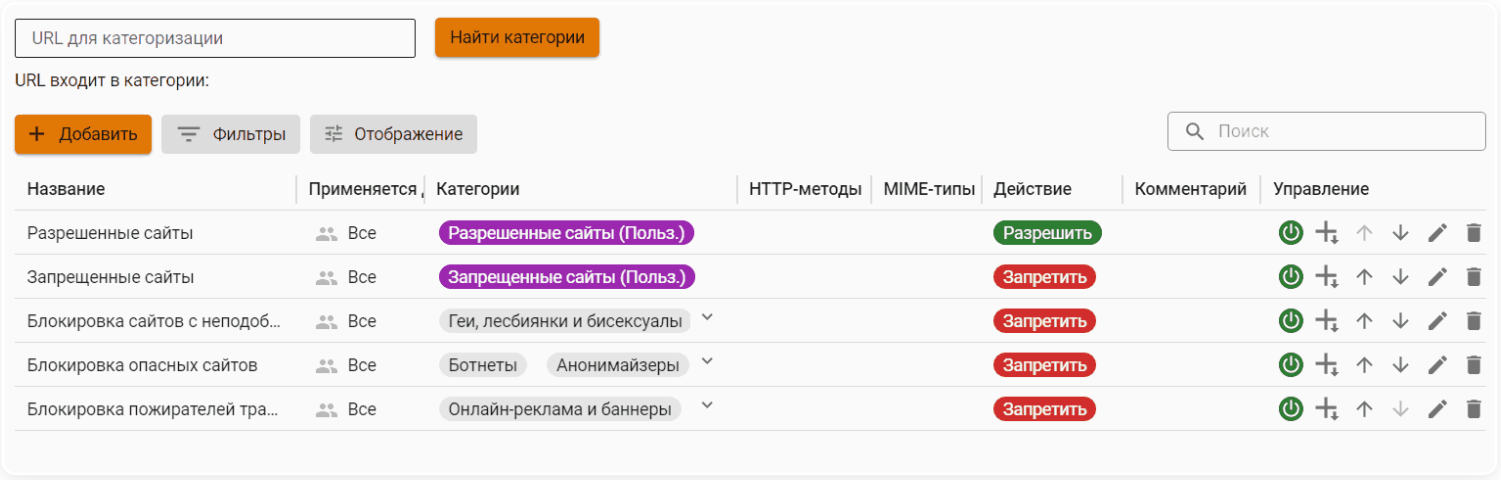
Шаг 2. Проверьте, не блокируется ли сайт правилом Контент-фильтра

1. Откройте сайт с устройства пользователя.

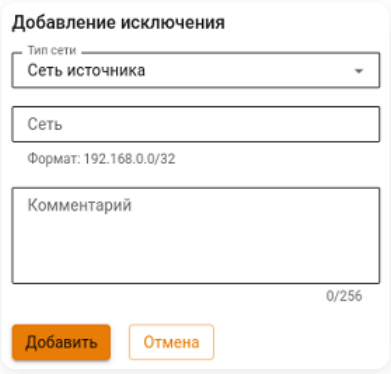
2. В NGFW перейдите в **Отчеты и журналы** → **Веб-трафик** и посмотрите, какое правило блокирует сайт:



3. Для поиска блокирующего правила также можно ввести URL сайта в строку поиска категорий **Контент-фильтра** в **Правила трафика** → **Контент-фильтр** → **Правила**:



4. Если сайт блокируется правилом **Контент-фильтра**, измените настройки **Контент-фильтра** или добавьте сайт в исключения в разделе **Сервисы** → **Прокси** на вкладке **Исключения**:



В **Сервисы** → **Прокси** → **Исключения** рекомендуем добавлять заведомо надежные сервисы.

Добавлять в исключения адреса клиентов вашей сети не рекомендуется, так как в этом случае веб-трафик клиентов не будет фильтроваться правилами **Контент-фильтра** и не будет попадать в отчеты.

Шаг 3. Проверьте, не блокирует ли сайт правило **Межсетевого экрана**

Найдите блокирующее правило одним из способов:

Первый способ. Счетчик срабатываний

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

2. Нажмите на **Отображение** и включите **Счетчик срабатываний**:

3. Откройте сайт с устройства пользователя.

4. Найдите в таблице FORWARD правило с заметным увеличением количества срабатываний.

Второй способ. Тестовое правило

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

2. Создайте тестовое правило, разрешающее любой трафик:

3. Правило добавится в конец таблицы. Поместите созданное правило на одну позицию вверх, нажав на кнопку .

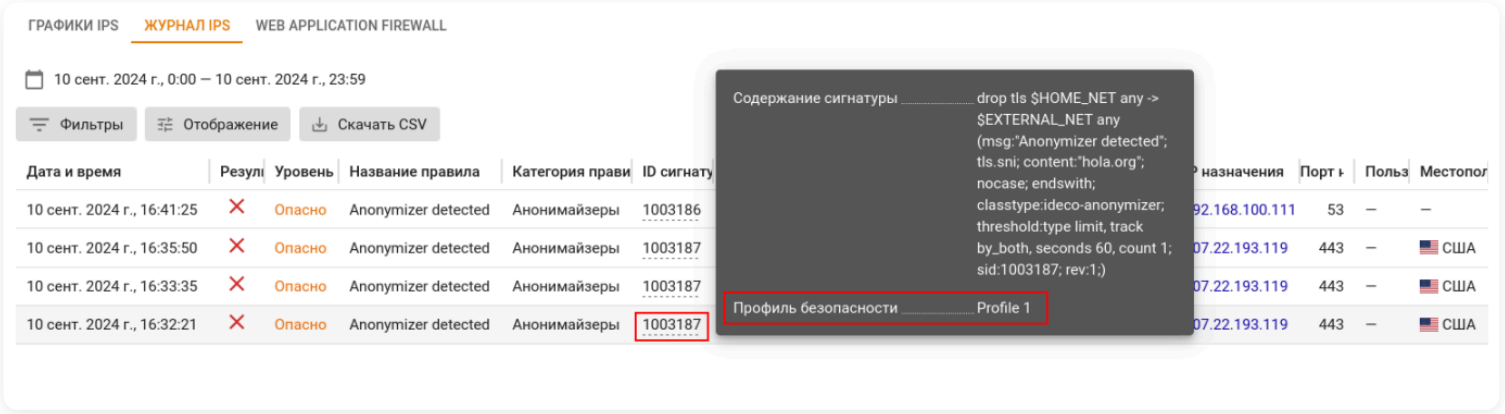
4. Откройте сайт с устройства пользователя.

5. Если сайт не открывается, поднимите тестовое правило на позицию выше и повторно откройте сайт с устройства пользователя. Повторяйте эти действия до тех пор, пока сайт не откроется.

6. Если сайт открывается, блокирующее правило расположено ниже тестового.

Если блокирующее правило направляет трафик через систему Предотвращения вторжений

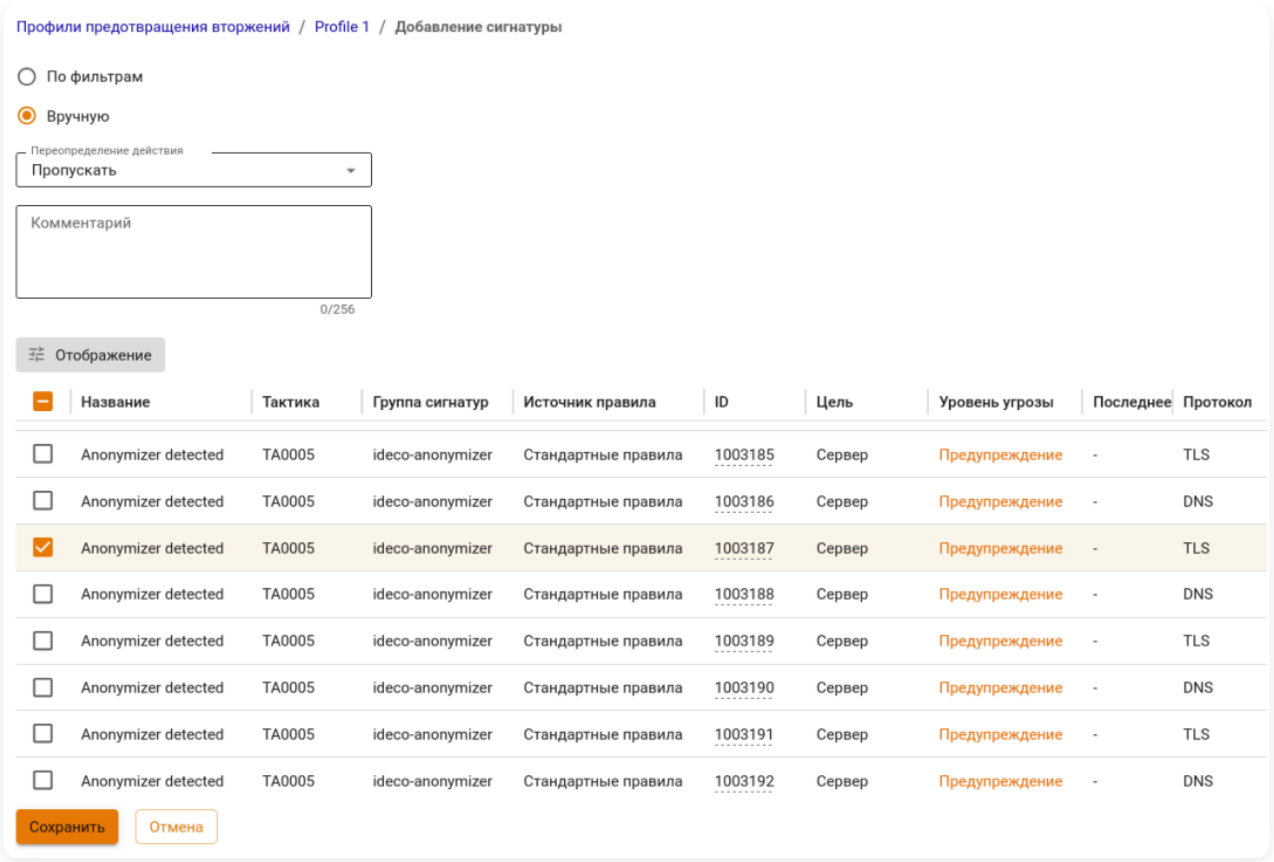
1. Перейдите в раздел **Отчеты и журналы** → **События безопасности** на вкладку **Журнал IPS** и найдите в таблице ID сигнатуры, заблокировавшей сайт, и название профиля, к которому относится сигнатура:



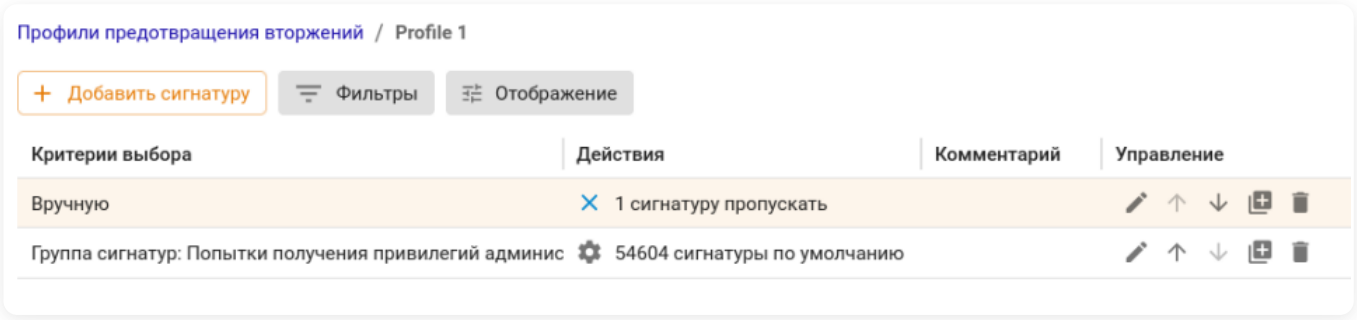
2. Перейдите в **Профили безопасности** → **Предотвращение вторжений**, нажмите на напротив профиля, заблокировавшего сайт, и выберите **Сигнатуры**.

3. Нажмите **Добавить сигнатуру** и выберите способ **Вручную**.

4. В таблице сигнатур по ID найдите сигнатуру (или сигнатуры), заблокировавшую сайт, и переопределите действие для нее:



5. Нажмите **Добавить** и переместите только что созданное правило на самый верх таблицы правил профиля:



Если блокирующее правило направляет трафик через Контроль приложений

1. Перейдите в **Отчеты и журналы** → **Трафик**.

2. В виджете **Топ заблокированных протоколов** найдите протоколы, которые блокируются **Контролем приложений**.

3. Перейдите в **Профили безопасности** → **Контроль приложений** и отредактируйте профиль, разрешив заблокированные протоколы.

Шаг 4. Определите блокируемый домен или IP-адрес (рассмотрим на примере FireFox)

1. Откройте в браузере нужный сайт.

2. Откройте инструменты веб-разработчика одним из способов:

- Нажмите Ctrl+Shift+I.
- Нажмите на ☰ в правом верхнем углу браузера, перейдите в **Другие инструменты** → **Инструменты веб-разработчика**.

3. Выберите вкладку **Сеть**.

4. Обновите страницу.

5. Отсортируйте столбец **Статус** левой кнопкой мыши. Обратите внимание на коды состояния 4xx и 5xx. Часто именно эти запросы блокируются NGFW.

Если решить проблему не удалось

Отправьте в техподдержку:

1. Скриншот ошибки в браузере.

2. Скриншот отсортированных ошибок из браузера, чтобы было видно проблемные домены или IP-адреса.

Что делать, если не работает интернет

Если при первоначальной настройке Ideco NGFW Novum у пользователей отсутствует интернет, выполните шаги для диагностики и решения проблемы.

Шаг 1. Проверьте лицензию

Перейдите в **Управление сервером** → **Лицензия** и проверьте, привязана ли лицензия к серверу.

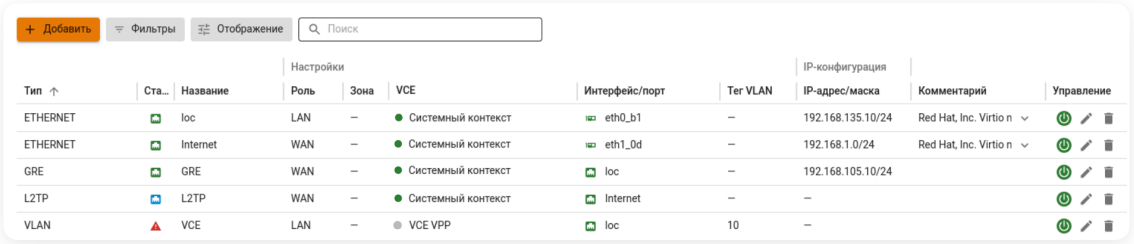
Шаг 2. Проверьте настройки межсетевого экрана

Перейдите в **Правила трафика** → **Межсетевой экран** и отключите в разделах **FORWARD** и **INPUT** правила, запрещающие все.

Шаг 3. Проверьте настройки интерфейсов

Проверьте, правильно ли настроен интерфейс

Перейдите в **Сервисы** → **Сетевые интерфейсы**. Если Ideco NGFW Novum использует выделенный интерфейс для подключения к провайдеру и работает не только как прокси, то проверьте тип подключения и роль:



- Тип подключения должен соответствовать требованиям провайдера.
- Роль должна быть **WAN**.

Проверьте подключение

1. Если провайдер требует VLAN, проверьте настройку VLAN-интерфейса. Убедитесь, что тег указан корректно.

2. Проверьте ICMP-запросы. Выполните команду `ping` до шлюза провайдера. Если отвечает, добавьте шлюз в список адресов для проверки связи.

Проверьте IP-адреса локального интерфейса

Внутренняя сеть должна относиться к приватным диапазонам. Если используются публичные IP-адреса:

- Рекомендуем перейти на приватную адресацию.
- В качестве временного решения создайте правило **SNAT**, где источник - ваша локальная сеть, назначение - внешний интерфейс.

Шаг 4. Включите режим Полный доступ

> Используйте опцию только для диагностики.

В правой верхней части окна Ideco NGFW Novum нажмите на иконку технической поддержки, а затем нажмите **Включить** в блоке **Полный доступ**. После включения:

- Сбор веб-статистики будет отключен.
- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включен автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Межсетевого экрана**.

Цикл обработки трафика в Ideco NGFW Novum описан в статье.

Если интернет появился, то проблема в неверно настроенной авторизации, правилах Межсетевого экрана или маршрутизации.

Шаг 5. Проверьте настройки пользователей

Проверьте авторизацию пользователей

- В Ideco NGFW Novum для авторизации пользователей обязательно требуется сопоставление IP-адреса с пользователем.
- На этапе первоначальной настройки не рекомендуем использовать настройку **Постоянная авторизация пользователя** и **Обнаружение устройств**.
- Пользователи ALD должны быть выгружены в Ideco NGFW Novum.
- Проверьте, что связь установлена с внешними каталогами ALD Pro, Active Directory и RADIUS.

Проверьте тип авторизации

- Если используется **MAC и IP+MAC авторизация**, то на компьютере клиента шлюзом по умолчанию должен быть указан Ideco NGFW Novum. В случае некорректной настройки шлюза, авторизация не будет работать.
- Если используется **Веб-аутентификация**, в поле **Разрешенные объекты** должны быть указаны учетные записи или группы пользователей, которым разрешена авторизация. Пользователю необходимо открыть браузер и попытаться перейти на любой внешний сайт (например, google.com).
- Если используется **Авторизация через журнал безопасности AD**, то:
  - В поле **Разрешенные объекты** должны быть указаны учетные записи или группы пользователей, которым разрешена авторизация.
  - Настройки на стороне контроллера домена.

Не рекомендуем использовать авторизацию через журнал безопасности AD.

Шаг 6. Проверьте работу DNS

Перейдите в **Управление сервером** → **Терминал** и выполните команду `nslookup ya.ru`.

Если разрешение имен работает, то укажите IP-адрес Ideco NGFW Novum в качестве DNS-сервера на рабочих станциях (в одноранговой сети) или в настройках внутреннего DNS-сервера, в разделе серверов перенаправления (в доменной сети).

Если не указать серверы DNS, Ideco NGFW Novum использует корневые серверы DNS, которые может блокировать провайдер. В таких случаях попробуйте указать в качестве DNS `8.8.8.8`, `1.1.1.1` и `77.88.8.8`. Если провайдер блокирует доступ и к ним тоже, используйте серверы провайдера в качестве серверов DNS.



Если не удалось решить проблему, обратитесь в Техническую поддержку

VPN

Решение проблем с VPN-подключениями в Ideco NGFW

Что делать, если не работает VPN-подключение на Windows

Перейти >

Если соединение по IPsec не устанавливается

Перейти >

Особенности маршрутизации и организации доступа (VPN)

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Что делать, если не работает VPN-подключение на Windows

В статье собраны основные методы диагностики для проверки работы VPN-подключения.

Шаг 1. Проверьте параметры VPN-подключения

1. Откройте **Параметры Windows (Win + I)** → **Сеть и Интернет** → **VPN**.

2. Выберите **VPN-подключение** и нажмите **Дополнительные параметры** → **Изменить**.

3. В открывшемся окне проверьте соответствие данным в Ideco NGFW Novum:

IKEv2/IPsec

- **Имя или адрес сервера** - должны соответствовать полю **Домен или IP-адрес** настроек IKEv2/IPsec.
- **Тип VPN** - IKEv2.
- **Тип данных для входа** - должен соответствовать полю **Тип аутентификации**. Если соответствует, проверьте настройки:
  - **Имя пользователя и пароль** - должны соответствовать данным пользователя.
  - **Сертификат** - проверьте, что в Ideco NGFW Novum загружен корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то должна быть загружена полная цепочка доверия: все промежуточные и корневой сертификаты.

SSTP

- **Имя или адрес сервера** - должны соответствовать полям **Домен** и **Порт** настроек SSTP. Проверьте, что в поле указаны данные в формате `example.ru:1443`, а домен не содержит кириллицу и `.local`.
- **Тип VPN** - SSTP.
- **Имя пользователя** и **Пароль** - должны соответствовать данным пользователя.

L2TP/IPsec

- **Имя или адрес сервера** - должны соответствовать домену или IP-адресу настроек L2TP/IPsec.
- **Тип VPN** - L2TP/IPsec с общим ключом.
- **Общий ключ** - должен соответствовать ключу из настроек L2TP/IPsec.
- **Имя пользователя** и **Пароль** - должны соответствовать данным пользователя.



Не используйте кириллические логины, а также не указывайте в качестве логина IP-адрес.

4. Проверьте, что на компьютер пользователя корректно установлен корневой сертификат.

5. Проверьте настройки VPN-подключения на стороне Ideco NGFW Novum:

- В разделе **Пользователи** → **VPN-подключения** модуль VPN-подключения активен.
- На вкладке **Пользователи** → **VPN-подключения** → **Основное** настроено и активно необходимое VPN-подключение.
- На вкладке **Пользователи** → **VPN-подключения** → **Доступ по VPN** добавлено правило, разрешающее подключение пользователю.

Шаг 2. Проверьте доступность VPN-сервера

1. Нажмите **Win + R**, введите `cmd` и нажмите **Enter**.

2. В командной строке выполните команду `ping <адрес_сервера>`. Например, `ping vpn.example.com`.

3. Проверьте ответ:

- Если есть ответы со временем отклика - сервер доступен. Переходите к следующему шагу.
- Если отображается сообщение `Превышен интервал ожидания` - есть проблема с сетевым путем или адресом.

4. Если ping не проходит, но вы уверены в правильности адреса, выполните альтернативную проверку с помощью команды `tracert <адрес_сервера>`. Она покажет, на каком участке сети обрывается связь.

Шаг 3. Проверьте информацию из журнала событий

1. Нажмите **Win + R**, введите `eventvwr.msc` и нажмите **Enter**, чтобы открыть журнал событий.

2. В левой колонке перейдите к **Журналы Windows** → **Система**.

3. В правой части окна нажмите **Фильтр текущего журнала**.

4. В поле **Источник** выберите **RasClient**.

5. Изучите события с уровнем **Ошибка** и **Предупреждение**. Информация из вкладок **Общие** и **Подробности** поможет определить причину и найти способ устранения.

Шаг 4. Сбросьте и перезагрузите сетевые компоненты Windows

Запустите командную строку от имени администратора и выполните команды по порядку, дожидаясь завершения каждой команды:

1. `netsh winsock reset` - сбрасывает каталог сетевых сокетов.

2. `netsh int ip reset` - сбрасывает настройки TCP/IP.

3. `ipconfig /flushdns` - очищает кэш DNS-клиента.

> Дальнейшие команды предназначены для сетей, где IP-адрес назначается автоматически (DHCP). Если на компьютере настроен статический IP-адрес, выполнение этих команд приведет к потере сетевого подключения, и интернет не восстановится автоматически.

4. `ipconfig /release` - освобождает текущий IP-адрес.

5. `ipconfig /renew` - запрашивает новый IP-адрес.

После выполнения команд перезагрузите компьютер.

Шаг 5. Проверьте состояние необходимых служб Windows

1. Нажмите **Win + R**, введите `services.msc` и нажмите **Enter**.

2. Найдите следующие службы и убедитесь, что тип запуска этих служб - **Автоматически**, а состояние - **Выполняется**:

- `Диспетчер подключений удаленного доступа` (Remote Access Connection Manager) - отвечает за управление подключениями удаленного доступа, включая VPN-подключения. Без этой службы Windows не сможет установить туннель.
- `Служба сетевых подключений` (Network Connections) - управляет объектами в папке **Сетевые подключения**, отвечает за отображение сетевых адаптеров (включая VPN-адаптеры) в интерфейсе Windows. Если служба остановлена, VPN-профиль не будет отображаться и его не получится создать.
- `Служба списка сетей` (Network List Service) - определяет характеристики сетевого подключения, собирает и хранит информацию о сетях.

3. Если служба остановлена, нажмите на ее название правой кнопкой мыши и выберите **Запустить**. Если тип запуска не **Автоматически**, дважды кликните по службе и в выпадающем списке **Тип запуска** выберите **Автоматически**. Нажмите **Применить**, затем **Запустить**.

4. Если ключевые службы отсутствуют или не запускаются, то системные компоненты Windows повреждены. Для восстановления выполните проверку целостности системных файлов (сначала `sfc /scannow`, затем `DISM /Online /Cleanup-Image /RestoreHealth` в командной строке от имени администратора) и перезагрузите компьютер.

5. Если это не помогает, используйте точку восстановления системы или другие средства восстановления Windows, так как без этих служб создание и работа VPN-подключения невозможны.

Шаг 6. Проверьте настройки брандмауэра и антивируса

Брандмауэр Windows

1. Временно отключите брандмауэр Windows. Для этого откройте **Параметры Windows (Win + I)** → **Конфиденциальность и защита** → **Безопасность Windows** → **Брандмауэр и защита сети**.

2. Отключите брандмауэр для частных и публичных сетей.

3. Установите VPN-соединение.

Антивирус

1. Найдите иконку антивируса в системном трее.

2. Перейдите в настройки, временно отключите антивирус и его функции сетевого экрана.

3. Установите VPN-соединение.

Шаг 7. Пересоздайте VPN-подключение

1. Откройте раздел **Параметры Windows (Win + I)** → **Сеть и Интернет** → **VPN**.

2. Выберите подключение и нажмите **Удалить**.

3. Нажмите **Добавить VPN-подключение** и создайте новое подключение.

4. Заполните все поля. Рекомендуем заполнять поля вручную и проверить раскладку клавиатуры.

5. Установите VPN-соединение.

Шаг 8. Проверьте драйверы сетевого адаптера

1. Нажмите **Win + X** и выберите **Диспетчер устройств**.

2. Раскройте **Сетевые адаптеры**.

3. Найдите основной адаптер и выберите **Обновить драйвер** → **Автоматический поиск обновленных драйверов**.

4. Если система найдет новый драйвер - установите его и перезагрузите компьютер.

Шаг 9. Если ничего не помогло

Если ни один из вариантов решения не помог, обратитесь в Техническую поддержку.

Если соединение по IPsec не устанавливается

1. Перезагрузите сервисы двух NGFW, выполнив команду `systemctl restart ideco-ipsec-backend.service && systemctl restart strongswan.service`.

2. Проверьте работоспособность перезагруженных сервисов:

- выполните команду `systemctl status strongswan.service`;
- перейдите в **Сервисы** → **IPsec**.

Если при переходе в раздел **IPsec** и выполнении команды возникли ошибки, то перейдите к пункту 3.

3. Пересоздайте соединение из веб-интерфейса по инструкции Настройка подключения между Филиалом и Главным офисом.

Если пересоздание соединения не помогло, перейдите к пункту 4.

4. Проверьте, ходит ли трафик по портам 500 и 4500, выполнив команды `tcpdump -i any port 4500 -ttttnnn` и `tcpdump -i any port 500 -ttttnnn` в головном офисе и филиале.

Если трафик уходит с одного NGFW и приходит на второй NGFW, то обратитесь в техническую поддержку.

Если трафик уходит с одного NGFW и не приходит на второй NGFW, обратитесь к провайдеру.

Особенности маршрутизации и организации доступа

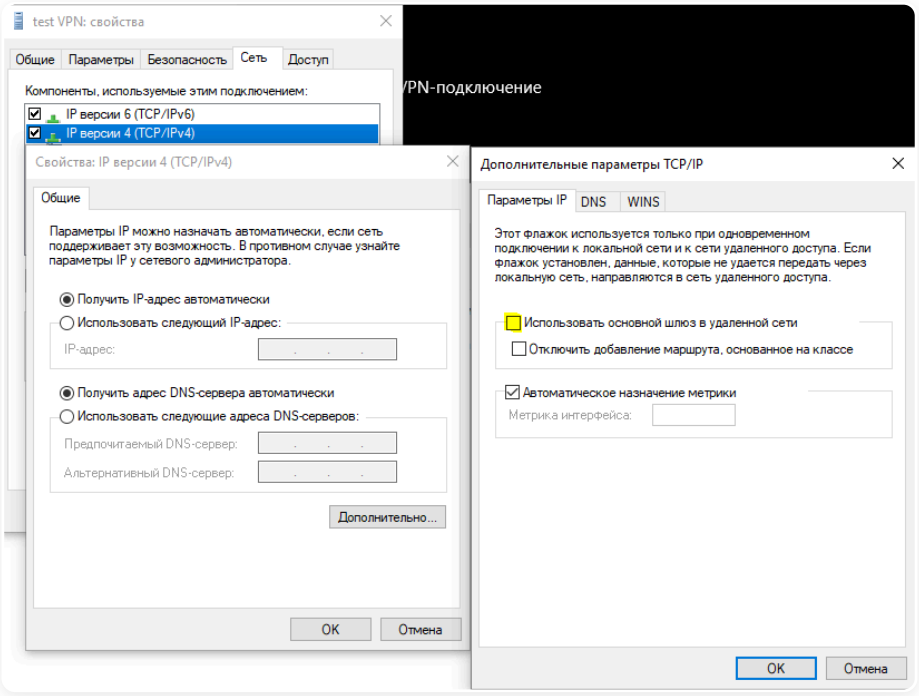
Классический контекст | Высокопроизводительный контекст

В статье рассматриваются потенциальные проблемы, связанные с доступом к ресурсам локальной сети через VPN, и предлагаются решения, такие как настройка маршрутов, исключение определенных сетей в антивирусном ПО и создание правил SNAT на NGFW Novum.

Организация доступа по VPN только к ресурсам локальной сети

Для организации доступа выполните действия:

1. В **Сеть** → **IP версии 4** → **Дополнительно** → **Параметры IP** уберите флаг **Использовать основной шлюз в удаленной сети**:



Особенности VPN-соединения с доступом только к ресурсам локальной сети

При выборе типа передачи маршрутов **Отправлять только указанные сети** маршрут до VPN-сервера и DNS-сервера построен не будет.

Если в NGFW Novum добавить передачу IP-адреса VPN-сервера NGFW Novum (DNS), то маршрут восстановится, а домен будет преобразовываться со следующими особенностями:

- Таблица с включенным шлюзом:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.5      5
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255          On-link         127.0.0.1    331
    192.168.100.2  255.255.255.255          On-link        10.200.0.5      5
  192.168.100.130  255.255.255.255          On-link        10.200.0.5      5
    192.168.122.0    255.255.255.0          On-link    192.168.122.10    281
   192.168.122.10  255.255.255.255          On-link    192.168.122.10    281
  192.168.122.255  255.255.255.255          On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0          On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0          On-link    192.168.122.10    281
  255.255.255.255  255.255.255.255          On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255          On-link    192.168.122.10    281
===========================================================================
```

- Таблица с отключенным шлюзом:

- Таблица с отключенным шлюзом и добавленной публикацией IP NGFW Novum:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.4     26
       10.200.0.4  255.255.255.255          On-link        10.200.0.4    281
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
```

Маршрут до сервера (в примере - 10.200.0.1) добавляется, но имеет более низкий приоритет, чем маршрут по-умолчанию. Соответственно запросы обрабатываются с задержкой и не обрабатываются при перехвате маршрутом по-умолчанию.

Рекомендуем вручную указать маршрут до DNS NGFW Novum, либо добавить маршрут в список публикуемых маршрутов на стороне NGFW Novum. Также можно использовать сторонний DNS-сервер.
2. Пропишите маршрут до корпоративной сети. В Windows 8, 8.1, 10 автоматически создается маршрут на основе класса, в зависимости от адреса, полученного по VPN. Для IPsec-IKEv2 можно настроить автоматическое получение маршрута.

Пример маршрута: если корпоративная сеть имеет адрес `172.16.0.0/16`, а сеть для VPN-подключений, настроенная на Ideco NGFW Novum, имеет адрес `10.128.0.0/16`:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1
```

Маршрут может не работать, когда есть пинг до интерфейса `10.128.0.1`, но нет пинга до хостов в локальной сети. В этом случае при создании маршрута нужно указать номер интерфейса VPN-подключения:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn
```

- `nn` - номер интерфейса VPN-подключения, посмотреть который можно при активном VPN-подключении в выводе в консоли команды `route print` раздел "Список интерфейсов".

Не удается получить доступ к компьютерам в локальной сети Ideco NGFW Novum

Для получения доступа к компьютерам в локальной сети Ideco NGFW Novum убедитесь, что:

1. Локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. В противном случае доступ к сети организации будет невозможен (трафик будет идти через физический интерфейс, а не через VPN).

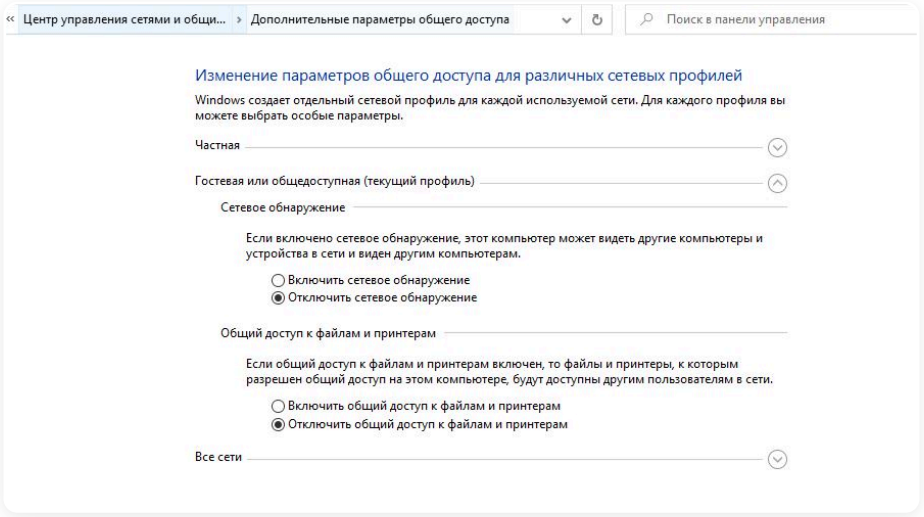
2. На компьютерах локальной сети основным шлюзом должен быть Ideco NGFW Novum. Если это не так, то вручную необходимо прописать соответствующий маршрут, чтобы сетевые пакеты шли на Ideco NGFW Novum для VPN-сети. **Например**:

```
route -p add 10.128.0.0 mask 255.255.0.0 10.1.1.1
```

- `10.128.0.0/16` - адрес VPN-сети Ideco NGFW Novum (настраивается в разделе **Пользователи** → **VPN-подключения**).
- `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW Novum.

3. На Ideco NGFW Novum в разделе **Межсетевой экран** → **FORWARD** нет запрещающих правил.

4. Компьютеры и серверы на Windows не ограничивают доступ к сетевым папкам с помощью правил настроек профилей сети (как на стороне подключающегося по VPN компьютера, так и на стороне компьютеров и серверов локальной сети):



Получение доступа к файлам и принтерам для профиля "Все сети" и "Частные сети"

Для получения доступа выполните действия:

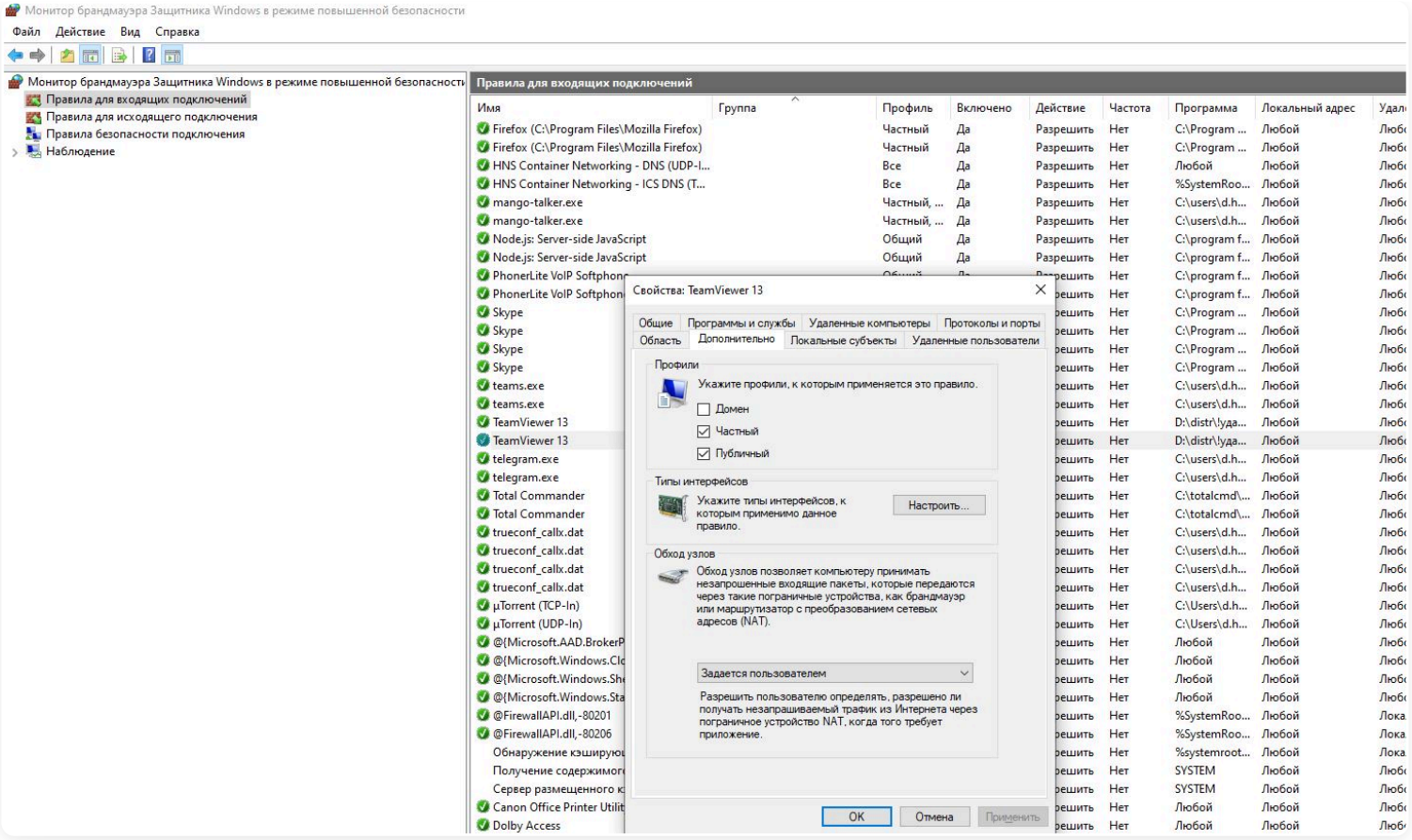
1. Перейдите в PowerShell (запустите PowerShell с повышением прав до администратора).

2. Выполните команду: `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`.

Возможные проблемы:

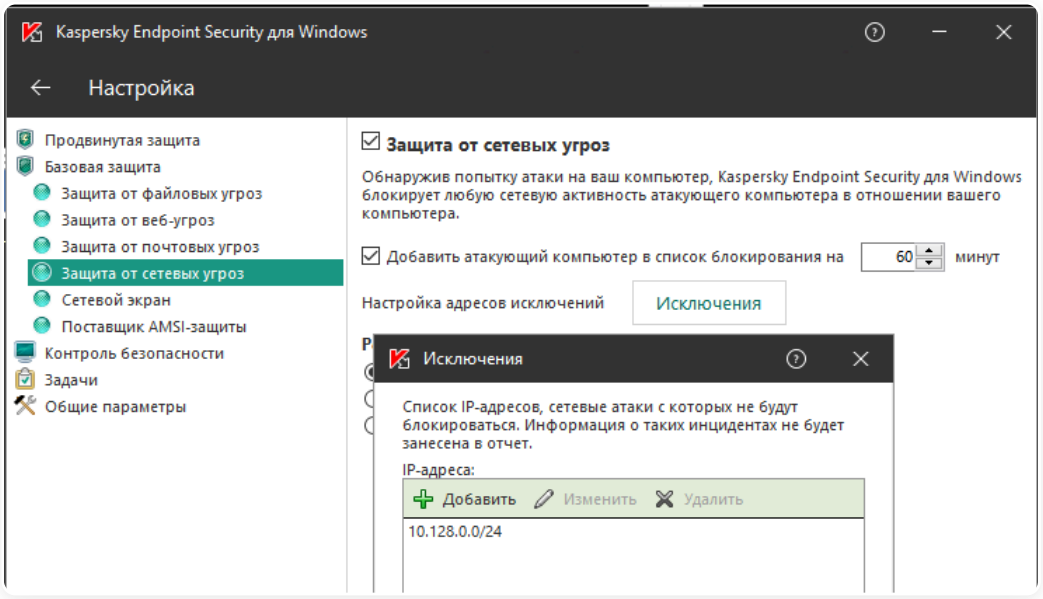
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей.

  Проверьте это в настройках входящих и исходящих подключений (необходимо разрешить доступ из частных и локальных сетей):



- Антивирусное ПО на компьютере может блокировать доступ из нелокальных сетей. Либо блокировать доступ конкретных программ.

  Например, для **Kaspersky Endpoint Security** нужно добавить сеть для VPN-подключений (по умолчанию `10.128.0.0/16`) в исключения:



Получение доступа к локальной сети Филиала

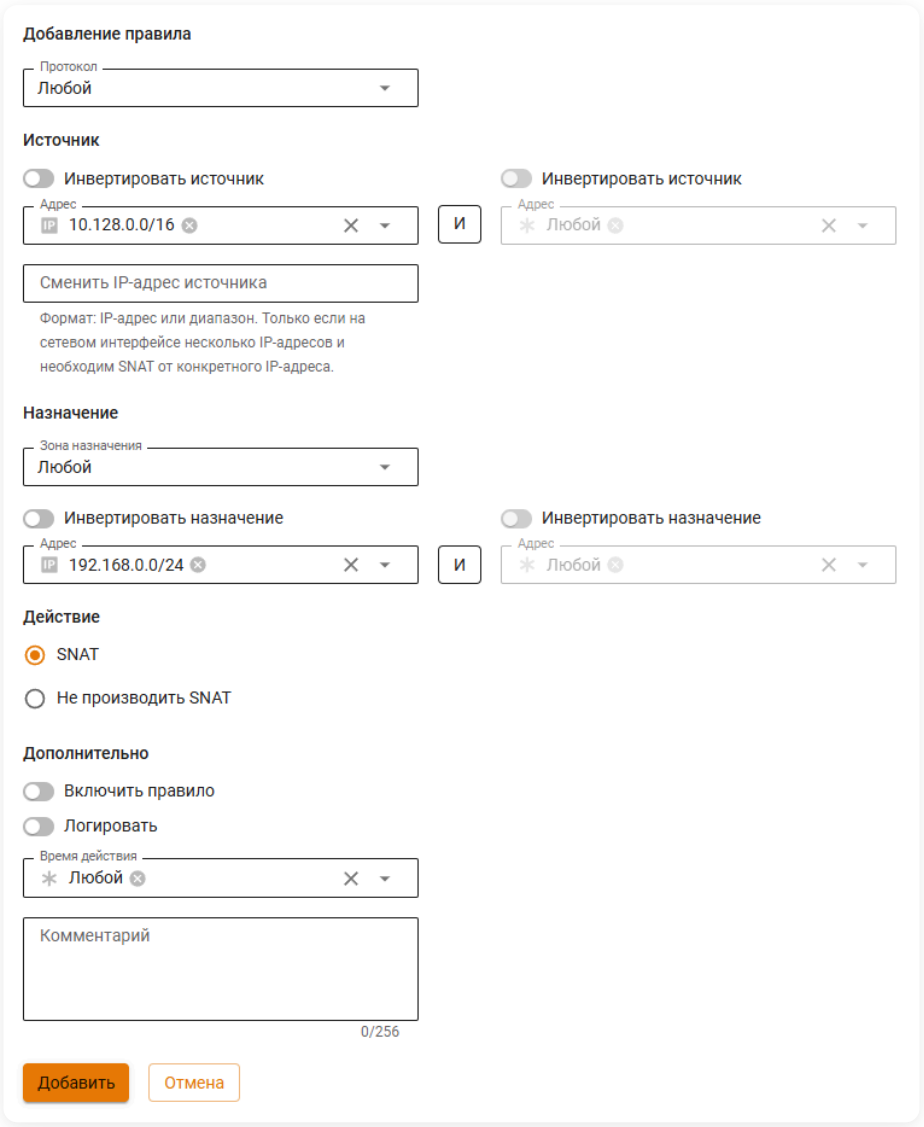
Чтобы обеспечить доступ, убедитесь, что VPN-сети обоих NGFW Novum не пересекаются. Затем проверьте настройки основного NGFW Novum, следуя инструкциям, описанным в статье.

Получение доступа к хостам локальной сети, если за NGFW Novum есть маршрутизатор, выступающий в качестве ядра локальной сети

Чтобы обеспечить доступ, нужно настроить на роутере маршрут от нужной локальной сети до VPN-сети. Для настройки маршрута на роутере укажите в качестве назначения VPN-сеть (`10.128.0.0/16`), в качестве шлюза - NGFW Novum (`172.16.0.1`).

Если настроить на роутере маршрут невозможно, можно создать на NGFW Novum SNAT-правило:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **SNAT**, нажмите **Добавить** и укажите параметры:



- **Источник** - VPN-сеть (`10.128.0.0/16`).
- **Назначение** - сеть за роутером, к которой требуется получить доступ из VPN-сети (`192.168.0.0/24`).

3. Нажмите **Добавить**.

В этом случае при отправке пакетов на роутер NGFW Novum подменит IP-адрес источника своим. За счет этого роутер направит ответ от хоста в локальной сети на NGFW Novum, который затем перенаправит его в VPN-сеть.

У хостов из локальной сети `192.168.0.0/24` не будет доступа к VPN-сети `10.128.0.0/16`.

Полезные ссылки

- **Как избежать проблем с подключением VPN-клиентов при нескольких серверах**

Ошибки при авторизации

Решение проблем с авторизацией в Ideco NGFW

Ошибка при авторизации "The browser is outdated"

Перейти >

Ошибка 400 Bad Request Request Header Or Cookie Too Large при авторизации в браузерах

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Ошибка при авторизации "The browser is outdated"

Если используется браузер, который не поддерживает NGFW, при авторизации появится ошибка **Your browser is outdated. This version of browser is unsecure and unsupported by modern web-technologies. Please, install the latest version of one of the listed browsers**.

Поддерживаемые версии браузеров:

- Google Chrome версия >= 109;
- Firefox версия >= 115;
- Safari версия >= 15.4.

Рекомендуем обновить браузер до минимально поддерживаемой версии.

Для продолжения авторизации несмотря на риски потребуется нажать **I understand the risks and wish to continue**.

Ошибка 400 Bad Request Request Header Or Cookie Too Large при авторизации в браузерах

Ошибка возникает на Windows 7, 8, 11, Windows Server 2008 R2, 2012, 2022 из-за большого количества групп безопасности и неспособности токена Kerberos вместить все данные.

По умолчанию размер токена Kerberos:

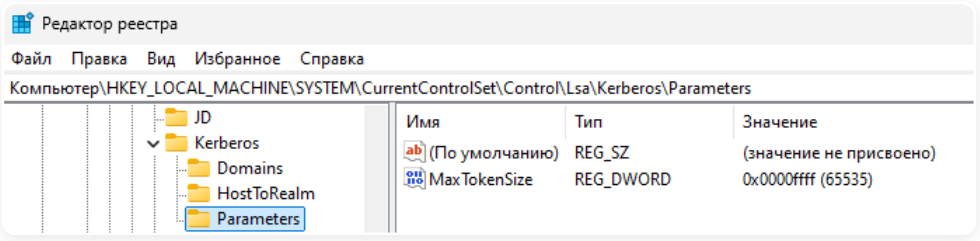
- **Windows 7 и Windows Server 2008R2** - 12000 байт.
- **Windows 8 и Windows Server 2012 (включая Windows Server 2022 и Windows 11)** - 48000 байт.

Для решения проблемы нужно увеличить размер токена на пользовательской ОС. Для этого:

1. Откройте редактор реестра и перейдите в раздел **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters**.

2. Создайте новый параметр типа **DWORD (32-bit)** с именем **MaxTokenSize**.

3. Задайте максимальное значение размера буфера - 65535 байт в десятичной системе счисления:



4. Перезагрузите компьютер.

Чтобы узнать текущее значение параметра **MaxTokenSize**, выполните следующую команду в **PowerShell**:

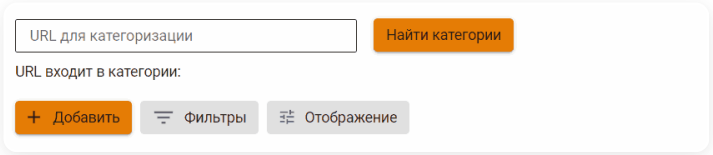
```
Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters|select MaxTokenSize
```

Что делать, если не действуют правила Контент-фильтра

Если правила контентной фильтрации не действуют, проверьте следующие параметры в настройках:

- IP-адрес пользователя должен соответствовать его адресу в авторизации (раздел **Мониторинг** → **Сессии пользователей**), пользователь должен находиться в группе, на которую назначено правило.
- IP-адрес пользователя и ресурса, к которому обращается, не должен входить в исключения прокси-сервера.
- В браузере и на компьютере пользователя не должны использоваться функции или плагины VPN, не прописаны сторонние прокси-серверы.

Дополнительно проверьте настройки категоризации ресурса, к которому обращаетесь, в поле **URL для категоризации** на вкладке **Правила**:



Если сайт неправильно категоризирован, поменяйте категорию на вкладке Переопределение категорий или воспользуйтесь формой обратной связи SkyDNS.

Как восстановить доступ к Ideco NGFW Novum

Для этого нужно выполнить следующие действия:

1. Перезагрузите сервер. При появлении меню загрузчика GRUB с выбором ядра Linux для загрузки системы нажмите англоязычную клавишу **E** на клавиатуре:

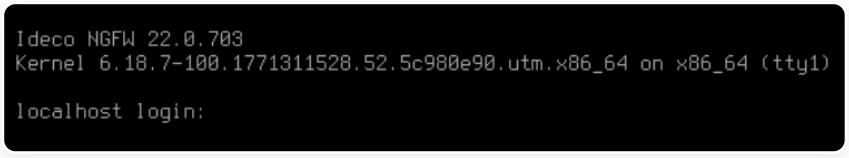


2. Откроется окно параметров ядра с возможностью редактирования. Переместите указатель стрелками на клавиатуре вправо до слова `quiet` и допишите текст `p=1`:



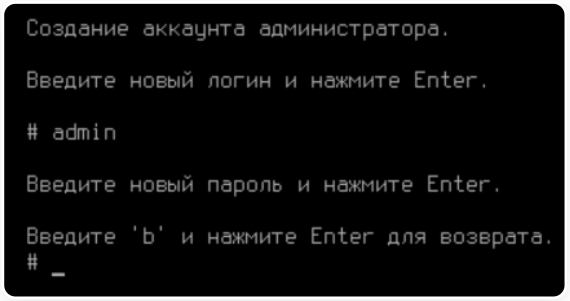
3. Нажмите `Enter`.

4. Не нажимайте никаких клавиш при появлении окна:



Дождитесь появления локальной консоли.

5. После повторной загрузки системы появится окно создания аккаунта администратора. Задайте новый логин и пароль администратора:



Требования к логину и паролю

Логин:

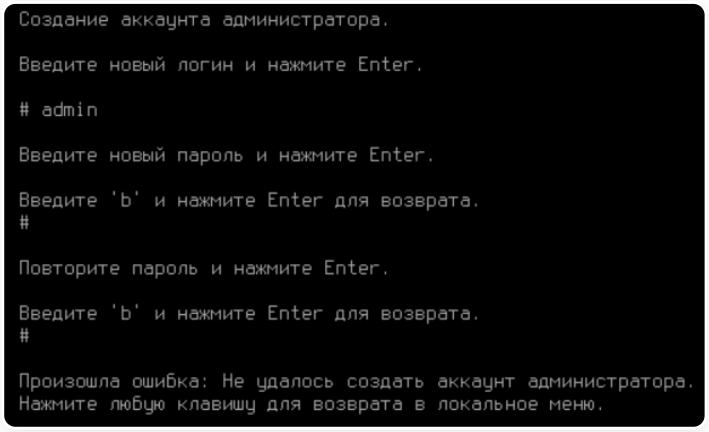
- Не должен начинаться с цифры.
- Не должен содержать специальных и пробельных символов, кроме дефиса `-`.
- **Длина логина** - от 1 до 31 символа включительно.

Пароль:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.
- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

Если при создании нового логина администратора логин будет совпадать с предыдущим логином, то будет выведена ошибка. Создайте имя администратора, отличное от предыдущего.

Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;`, `^[[4~;` и т.д.



Как изменить дату и время в Ideco NGFW Novum

Если дата и время в Ideco NGFW Novum установлены неверно, сервер не сможет получить лицензию. Для установки корректных значений:

1. Перейдите в раздел **Управление сервером** → **Терминал**.

2. Остановите службу `chronyd`, которая автоматически синхронизирует системные часы с NTP-серверами:

```
systemctl stop chronyd
```



Без отключения службы изменить дату и время не получится.

3. Убедитесь, что служба остановлена:

```
systemctl status chronyd
```

В строке `Active` должно отображаться значение `inactive (dead)`.

4. Установите корректную дату и время в формате `ГГГГ-ММ-ДД ЧЧ:ММ:СС`:

```
timedatectl set-time "2026-04-22 12:33:14"
```

5. Проверьте, что изменения применились:

```
timedatectl
```

6. Выполните регистрацию сервера и привяжите лицензию. Подробнее в статье.

7. После регистрации сервера вернитесь в **Управление сервером** → **Терминал** и запустите службу `chronyd`, чтобы восстановить автоматическую синхронизацию времени:

```
systemctl start chronyd
```

8. Убедитесь, что служба успешно запустилась:

```
systemctl status chronyd
```

В строке `Active` должно отображаться значение `active (running)`.

При необходимости добавьте адрес NTP-сервера. Подробнее в статье.

Ideco NGFW Novum 22.0.1629

Примечания к релизу

Дата выхода версии: 05.05.2026.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в Telegram-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Электронная почта: support@ideco.ru
- Telegram: ideco.bot
- MAX: id6670208848_bot
- Интерактивный онлайн-чат со специалистом технической поддержки - https://my.ideco.ru/, https://ideco.ru/, веб-интерфейс Ideco NGFW Novum

Скачать Ideco NGFW 22

Автоматическая регистрация тестовой лицензии: my.ideco.ru (полная функциональность на 42 дня и 10 000 пользователей).

Критические изменения и особенности обновления

Обратите внимание на изменения в 22 версии NGFW Novum при обновлении с версии 21:

- Поддержка PPTP-сервера для доступа по VPN прекращена, так как протокол устарел. Рекомендуем использовать **Ideco Client**, **IKEv2/IPsec** или **SSTP**.
- Группа сигнатур GeoIP будет исключена из обработки модулем IPS, однако по-прежнему останется в **Межсетевом экране**. Рекомендуем заранее создать необходимые правила в **Межсетевом экране**.
- Отключена возможность отправки почты через почтовые клиенты на 25 порту. Для аутентифицированной отправки используйте порт 587 (TLS).
- При подключения Ideco Client порт 14765 больше не используется как резервный для порта 443.
- Раздел **Балансировка и резервирование** перенесен в **SD-WAN**. Внедрение раздела **SD-WAN** затронет настройки маршрутизации: **Next hop** создаются только для маршрутов с указанным интерфейсом и шлюзом.
- При настройке **IPsec** в поле **Адрес удаленного устройства** допускается только одно значение. В поле **Интерфейс подключения** требуется указать конкретный интерфейс - значение **Любой** и группа балансировки больше не поддерживаются. Подключения, не соответствующие этим требованиям, после обновления работают, но не будут поддерживаться в последующих версиях.
- В правилах **Статической** маршрутизации больше не поддерживается указание пользователя в поле **Шлюз**. Если в правиле был указан пользователь, перед обновлением замените его на IP-адрес вручную. При обновлении система попытается выполнить замену автоматически, но без привязки к IP-адресу объект отобразится как **Удалено** и правило перестанет работать.

Новые возможности

Функциональность	**Описание**
SD-WAN	Добавлен раздел SD-WAN для управления распределенными сетями на основе политик. Технология обеспечивает интеллектуальную маршрутизацию трафика между филиалами, ЦОД и облачными сервисами с поддержкой резервирования и балансировки каналов. В разделе доступны настройки next hop, профилей next hop и профилей IP SLA для мониторинга качества каналов по задержке, джиттеру и потере пакетов Подробности в статье
Аутентификация по сертификату	Добавлена возможность привязывать пользователя к конкретному устройству и использовать сертификат как дополнительный фактор авторизации в VPN. NGFW может автоматически выпускать сертификаты для устройств и управлять привязками - без необходимости разворачивать отдельную PKI-инфраструктуру Подробности в статье
Журнал DNS-запросов	В журнале отображается информация об обмене DNS-сообщениями, обработанными Ideco NGFW Novum при включенной опции **Логировать DNS-запросы** в **Сервисы → DNS → Внешние DNS-серверы** Подробности в статье
Двухфакторная аутентификация для администраторов	Добавлена поддержка 2FA при входе в веб-интерфейс для администраторов всех типов (локальные, AD, ALD, RADIUS). Поддерживаются методы: TOTP-токен и RADIUS 2FA. Настройка в разделе **Управление сервером → Администраторы** на вкладке **Двухфакторная аутентификация** Подробности в статье

Маршрутизация по протоколу EIGRP	**EIGRP** - динамическая маршрутизация на основе гибридного протокола. Он сочетает особенности дистанционно-векторного подхода и протоколов состояния каналов, что обеспечивает быструю сходимость и актуальность таблиц маршрутизации Подробности в статье
Логирование в Ideco Client	В программу добавлены инструменты диагностики: режим отладки и сбор логов с системными данными в один архив. Это упрощает выявление и устранение проблем с подключением без привлечения технической поддержки Подробности в статье
Исключение сигнатур из профиля IPS	В профилях IPS появилась возможность исключать отдельные сигнатуры из анализа. Это позволяет снизить количество ложных срабатываний и убрать нежелательные правила без изменения всего профиля Подробности в статье
Управление сервером через последовательный порт	Добавлена возможность устанавливать NGFW через COM-порт, а также включен постоянный доступ через COM-порт к локальному меню Подробности в статье

Безопасность

- Добавлена интеграция с базой данных ФинЦЕРТ - центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Новый источник доступен в настройках: групп сигнатур Предотвращения вторжений, а также правил Межсетевого экрана и Контент-фильтра через объект **Черный список ФинЦЕРТ**.

Улучшения и оптимизации

- Реализована возможность интеграции со сторонними ZTNA агентами.
- В профилях системы **Предотвращения вторжений** отображается уровень угрозы пользовательских сигнатур.
- В журнале **Межсетевой экран** добавлены разделы столбцов:
  - **Подключение** (ID, Время подключения, Время завершения, Длительность).
  - **Антивирус** (ID, Профиль).
  - **TLS/SSL-инспекция** (ID, Профиль, Результат) в высокопроизводительном контексте.
  - **Контент-фильтр** (ID, Профиль) в высокопроизводительном контексте.
- Повышена производительность обработки трафика.
- В высокопроизводительный контекст добавлены:
  - **Профили устройств**.
  - **Двухфакторная аутентификация**.
  - **Обратный прокси**.
  - **Личный кабинет пользователя**.
  - **Сессии ЛК**.
  - **Аутентификация пользователей ЛК**.
  - Возможность подключения SPAN-интерфейса.
  - Интеграция с RADIUS-сервером.
- При синхронизации активной и резервной ноды данные на резервной ноде больше не перезаписываются.
- В IPsec добавлена опция **Разделять туннель на отдельные Child SA для каждой пары сетей** для создания отдельного Child SA на каждую пару локальной и удаленной подсети, обеспечивающая доступность всех сетей сразу после установления VPN.
- Улучшение сбора статистики и работы **Монитора трафика** под большой нагрузкой.
- Оптимизирована загрузка данных журналов для снижения нагрузки на диск и ускорения отображения.
- Добавлена поддержка Graceful Restart для протоколов OSPF и BGP.
- Добавлена возможность выбора интерфейсов GRE-over-IPSec, IPSec VTI и ГОСТ VPN в качестве интерфейсов BGP.
- Добавлены столбцы **Профиль IPS** и **ID правила межсетевого экрана** в разделе **Отчеты и журналы → События безопасности**. При нажатии на ID правила выполняется переход в раздел **Межсетевой экран** с подсветкой соответствующего правила.
- В раздел **Отчеты и журналы → Межсетевой экран** добавлена группа колонок **Подключение**. В высокопроизводительном контексте появились группы колонок **Антивирус** и **Контент-фильтр**.
- Добавлена возможность загрузки баз фильтрации из файла при любом типе лицензии - как онлайн, так и офлайн.
- Добавлена возможность выбора портов для связи между нодами при настройке кластера.
- Добавлена возможность сохранения состояния таблицы при создании и редактировании объектов: автоматическая прокрутка к измененной строке, ее подсветка и раскрытие группы.

Исправленные ошибки (Resolved Issues)

ID задачи	Описание	Модуль

ICS-42696	Исправлена ошибка авторизации Ideco Client при использовании BGP-подключения от провайдера	Ideco Client
ICS-55312	Исправлена проверка статуса Secure Boot на этапе предзагрузки - система теперь останавливает загрузку при обнаружении включенного Secure Boot	-
ICS-29314	Исправлено местоположение иконки чата с технической поддержкой	-
ICS-51952	Устранена ошибка, приводившая к циклической перезагрузке NGFW после обновления	-

Ideco NGFW Novum 22.1.108

Примечания к релизу

Дата выхода версии: 15.05.2026.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в Telegram-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Электронная почта: support@ideco.ru
- Telegram: ideco.bot
- MAX: id6670208848_bot
- Интерактивный онлайн-чат со специалистом технической поддержки - https://my.ideco.ru/, https://ideco.ru/, веб-интерфейс Ideco NGFW Novum

Скачать Ideco NGFW 22

Автоматическая регистрация тестовой лицензии: my.ideco.ru (полная функциональность на 42 дня и 10 000 пользователей).

Безопасность

- Исправлена уязвимость ядра CVE-2026−31 431, связанная с локальным повышением привилегий до root (не эксплуатируется удаленно, не критична для системы).

Улучшения и оптимизация

- Журнал **Блокировки по IP** доступен в высокопроизводительном контексте.
- В логах журнала **DNS-запросы** отображается статус DNS Security.
- **Рекомендуемый** профиль предотвращения вторжений переименован в **Расширенный**.
- При подключении к Ideco Client можно указывать резервный порт 14765 в формате `домен:14765` или `IP:14765` (поле `server`).
- Повышена стабильность работы EIGRP.
- Косметические изменения веб-интерфейса.

Исправленные ошибки

ID задачи	Описание	Модуль
ICS-64653	Исправлена установка IPsec-подключений через неверный исходящий интерфейс	IPsec
ICS-63490	Исправлена ошибка, при которой в журнале **Межсетевой экран** трафик по правилу deny any any отображается как разрешенный	Межсетевой экран

Ideco NGFW Novum 22.3.52

Примечания к релизу

Дата выхода версии: 29.05.2026.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в Telegram-канале с разработчиками: @idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Электронная почта: support@ideco.ru
- Telegram: @ideco_support_bot
- MAX: id6670208848_bot
- Интерактивный онлайн-чат со специалистом технической поддержки - https://my.ideco.ru/, https://ideco.ru/, веб-интерфейс Ideco NGFW Novum

Скачать Ideco NGFW 22

Автоматическая регистрация тестовой лицензии: my.ideco.ru (полная функциональность на 42 дня и 10 000 пользователей).

Безопасность

- Обновлён модуль **Предотвращения вторжений** (с исправлениями CVE-2026-45764, CVE-2026-45766, CVE-2026-45769, CVE-2026-46387, CVE-2026-45759, CVE-2026-45762, CVE-2026-45765, CVE-2026-45747, CVE-2026-45767, CVE-2026-45751, CVE-2026-45761).
- Обновлены правила WAF.
- Исправлена уязвимость CVE-2026-1642 в модуле Обратный прокси, связанная с внедрением данных в ответы проксируемых TLS-серверов при MITM-атаке (не эксплуатируется удалённо без позиции MITM, средний уровень критичности).

Улучшения и оптимизация

- Журнал **Блокировки по IP** переименован в **Блокировки WAF**.
- В **Управление сервером** → **Дополнительно** кнопка **Сбросить блокировки по IP** переименована в **Сбросить блокировки (fail2ban)**.
- В **Управление сервером** → **Ideco Center** появился блок **Доверенные сертификаты** - сертификаты добавляются кнопкой **Загрузить**.
- В форме добавления/редактирования **Внешнего DNS-сервера** доступны все сетевые интерфейсы.
- Повышена производительность обработки веб-трафика под большой нагрузкой.

Исправленные ошибки

ID задачи	Описание	Модуль
ICS-32784	Восстановлен учет аренды DHCP-адресов при наличии нескольких VLAN на одном интерфейсе с одним MAC-адресом: сохранялась только последняя выданная аренда.	DHCP
ICS-65477	Восстановлена работа журнала **Межсетевой экран** при срабатывании правил с профилями безопасности в высокопроизводительном контексте	Отчеты и журналы
ICS-65405	Исправлена потеря доступа извне после обновления на 22.x: шлюз с профилем проверки без заданных адресов больше не помечается ошибочно недоступным	SD-WAN
ICS-65100	Исправлено падение службы Ideco Client после быстрых многократных циклов авторизации и деавторизации	Ideco Client
ICS-65551	Восстановлено логирование срабатываний правил **Межсетевого** экрана с действием **Запретить** и правил **SNAT**	Межсетевой экран

Новое в документации

Май 2026

Практические руководства

Резервирование трех WAN-каналов через SD-WAN

Настройка Ideco NGFW Novum

Настройка высокопроизводительного контекста

Аутентификация по сертификату

Диагностика работы Ideco Client с помощью логирования

Управление Ideco Client через CLI

DNS-запросы

EIGRP

Next hop

Профили next hop

Профили IP SLA

Объекты

05.06.26

Межсетевой экран

05.06.26

Настройка фильтрации трафика

05.06.26

Особенности создания профилей

05.06.26

Пример создания иерархической структуры

05.06.26

Профили предотвращения вторжений

05.06.26

Терминал

05.06.26

Прокси

05.06.26

Полный цикл обработки трафика в Ideco NGFW Novum

05.06.26

Syslog

05.06.26

Установка и настройка Ideco Client на Windows

05.06.26

Кластеризация

05.06.26

Настройка высокопроизводительного контекста

05.06.26

Сетевые интерфейсы

05.06.26

Интерфейсы

05.06.26

Аутентификация

05.06.26

Настройка SSO-аутентификации

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

05.06.26

Сертификаты

04.06.26

Настройка Device VPN

04.06.26

Инструкция по созданию подключения в macOS

03.06.26

VPN-подключения

29.05.26

Миграция настроек Device VPN

29.05.26

Резервирование трех WAN-каналов через SD-WAN

29.05.26

Ideco NGFW Novum 22.3.52

29.05.26

Доступ из внешних сетей без NAT

28.05.26

Управление Ideco Client через CLI

28.05.26

Ограничение скорости

28.05.26

События безопасности

21.05.26

Active Directory/Samba DC

21.05.26

EIGRP

20.05.26

DNS-запросы

18.05.26

Ideco Client

16.05.26

Блокировки WAF

16.05.26

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

Ideco NGFW Novum 22.1.108

15.05.26

Аутентификация по сертификату

13.05.26

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

Об Ideco NGFW Novum

> Ideco NGFW Novum - многофункциональный межсетевой экран с фильтрацией до уровня L7, поддержкой VPN, ZTNA и кластеризации. Обеспечивает защиту и контроль трафика в компаниях уровня enterprise.

Возможности Ideco NGFW Novum

- ☑ Межсетевой экран
- ☑ Система предотвращения вторжений
- ☑ Контент-фильтр
- ☑ Контроль приложений
- ☑ Антивирусная и антиспам-проверка трафика
- ☑ Защита от ботнетов, фишинга и шпионского ПО
- ☑ Поддержка работы до 100 тысяч правил Файрвола
- ☑ Производительность ядра сети: до 200 Гбит/с, поддержка до 25 миллионов сессий и 1 миллиона новых TCP-сессий в секунду.
- ☑ Настройка физических портов и перенос настроек на другой порт без изменения политик безопасности
- ☑ Внедрение без перестройки сети и быстрый запуск пилотных проектов благодаря L2-мосту
- ☑ VPN site-to-site (GRE, IPSec, ГОСТ VPN) и client-to-site (IKEv2/IPSec, L2TP/IPSec, SSTP, Wireguard, TLS в Ideco Client) с 2FA
- ☑ Логирование действий администратора
- ☑ Создание высокопроизводительного виртуального контекста с функциями NGFW Novum
- ☑ Управление через Ideco Center
- ☑ Отчетность по трафику пользователей и событиям безопасности
- ☑ Интеграция с Microsoft Active Directory, ALD Pro, Samba DC, SIEM, Zabbix и DLP-системами

И это далеко не полный список возможностей и сервисов Ideco NGFW Novum, которые позволяют создать надежный барьер для защиты локальной сети от современных угроз безопасности.

Техническое описание Ideco NGFW Novum доступно по ссылке.

Скачать Ideco NGFW Novum можно в личном кабинете.

Видеодокументация доступна на YouTube и Rutube.

О документации

Документация содержит подробные инструкции, описания функций и рекомендации по устранению проблем. Как эффективно использовать документацию:

Навигация по разделам

Слева на странице расположены блоки с разделами:

- **Общая информация** - блок содержит информацию о доступных в Ideco NGFW Novum лицензиях, системных требованиях, режимах работы технической поддержки и информацию о продуктах, которые могут интегрироваться в инфраструктуре с продуктами Ideco.
- **Быстрый старт** - блок статей поможет произвести первоначальные настройки Ideco NGFW Novum, включая создание загрузочного USB-накопителя, установку и подключение к веб-интерфейсу, импорт корневого сертификата, настройку Ethernet-подключения и активацию лицензии.
- **Настройка Ideco NGFW Novum** - включает разделы с подробными статьями по настройке Ideco NGFW Novum. Разделы повторяют структуру веб-интерфейса Ideco NGFW Novum, обеспечивая удобство и простоту использования.
- **Популярные инструкции и диагностика проблем** - содержит по тематике диагностики проблем и ответы на часто задаваемые вопросы.
- **API** - документация по API перенесена и доступна по ссылке. Блок описывает API-запросы, которые управляют функциями и настройками Ideco NGFW Novum. Среди них - авторизация, работа с объектами, настройка правил и многое другое.

Поиск информации

Введите запрос в строку поиска в правом верхнем углу страницы. Поиск выполняется по документации, относящейся к текущему продукту.

Документация высокопроизводительного контекста

В документации Ideco NGFW Novum добавлена новая функция - возможность переключаться между виртуальными контекстами. Подробнее о VCE в статье:

- **Классический контекст** - документация для **Системного контекста** и всех его дочерних контекстов, созданных с использованием классического типа.
- **Высокопроизводительный контекст** - документация, специально разработанная для высокопроизводительного контекста, учитывающая его уникальные особенности и отличия.

Переключение между контекстами осуществляется с помощью кнопок в верхней части статьи. Типы кнопок и их назначение:

- **Оранжевая кнопка** - подсвечивает, документация какого контекста сейчас активна.
- **Белая кнопка** - переключает на документацию другого контекста. Например, если активна кнопка **Классический контекст**, то белая кнопка **Высокопроизводительный контекст** откроет соответствующую статью в документации по высокопроизводительному контексту.

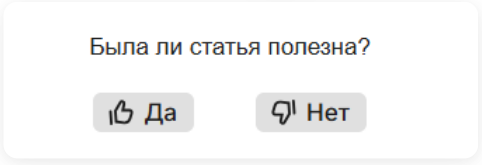
Поиск по документации осуществляется только в пределах выбранного контекста.

Обратная связь

Мы постоянно совершенствуем нашу документацию и всегда рады вашим отзывам.

Как оставить отзыв:

- Поставить реакцию в правом верхнем углу или в конце любой статьи:

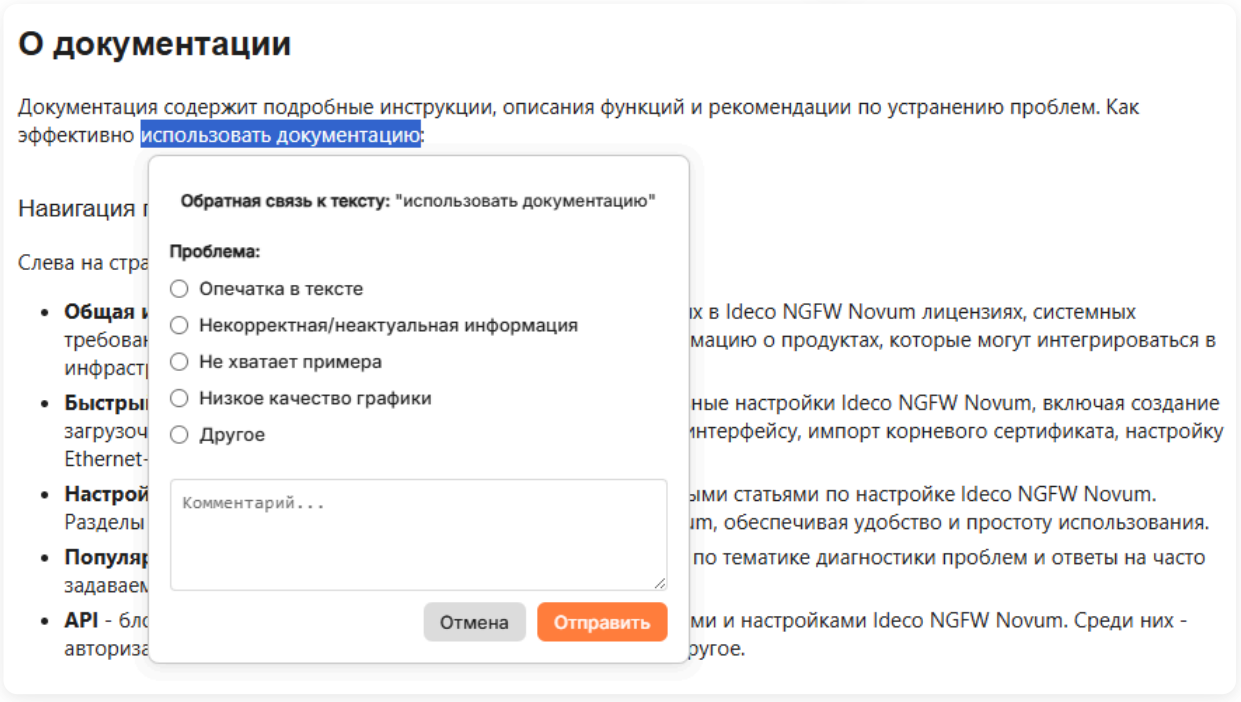


- Написать комментарий к фрагменту текста внутри статьи.

Если рекомендации из статьи не помогли, нажмите , заполните форму обратной связи, нажмите **Отправить**, а затем - **Обратиться в техподдержку**.

Чтобы написать комментарий:

1. Выделите фрагмент, который хотите прокомментировать, и нажмите на иконку . Иконка появляется при выделении фрагмента от 5 символов:



2. Выберите проблему и при необходимости опишите ее в поле **Комментарий** (не менее 5 символов).

3. Нажмите **Отправить**.

Лицензирование

> В статье представлено описание доступных в Ideco NGFW Novum лицензий.

Лицензирование позволяет передать программное обеспечение в пользование на условиях лицензии: пользователь получает возможность использовать продукт, а владелец продукта сохраняет за собой право собственности.

У лицензии Ideco NGFW Novum есть три основные характеристики:

- **Количество пользователей Ideco NGFW Novum** - авторизованные пользователи локальной сети или подключенные по VPN пользователи, трафик которых проверяется и контролируется шлюзом.
- **Редакция Ideco NGFW Novum (вид лицензии)** - набор доступных к использованию модулей в системе и особенности работы модулей.
- **Срок действия лицензии** - часть функций остается доступной после завершения срока.

Особенности лицензирования:

- Количество приобретенных по лицензии учетных записей ограничивает число авторизованных пользователей.
- Под одной учетной записью пользователя на Ideco NGFW Novum можно авторизовать до пяти устройств с помощью различных методов авторизации. При авторизации шестого устройства будет разорвана самая старая сессия.
- При изменении вида лицензирования некоторые модули могут работать некорректно в течение суток до автоматического обновления информации о лицензии. Для обновления информации о лицензии перейдите в **Управление сервером** → **Лицензия** веб-интерфейса NGFW и нажмите **Обновить информацию о лицензии**.

Подробнее об управлении лицензиями - в статье.

Виды лицензий

В Ideco NGFW Novum доступны лицензии:

Enterprise

Enterprise - коммерческая лицензия.

- [x] Бессрочное право на использование Ideco NGFW Novum
- [x] Включает в себя годовую подписку **Security Update**
- [x] Лицензирование по числу активных пользователей или по количеству ядер виртуальной машины
- [x] Для программно-аппаратных комплексов Ideco доступно лицензирование без ограничения по количеству пользователей

В период действия подписки **Security Update** доступны следующие преимущества:

- Обновления на новые версии Ideco NGFW Novum.
- Расширенная база категорий **Контент-фильтра**.
- Модуль **Предотвращение вторжений**.
- Модуль **Контроль приложений**.
- Автоматическое обновление баз модулей.
- Техническая поддержка.

По истечении срока подписки **Security Update** для сервера Ideco NGFW Novum:

- **Контроль приложений** - модуль отключается.
- **Контент-фильтр** - становятся доступны только пользовательские категории.
- **Предотвращение вторжений** - остается доступна старая отчетность, но анализ трафика отключается.
- **Техническая поддержка** - недоступна.
- Обновление баз модулей - недоступно.
- Обновление на версии, вышедшие после даты окончания подписки - недоступно.



Для использования кластера и/или модуля **DNS security** Ideco NGFW Novum потребуются дополнительные лицензии.

Enterprise-demo

Enterprise-demo - бесплатная лицензия сроком на 44 дня.

- ☑ Авторизация до 10 000 пользователей
- ☑ Включены все модули, кроме технологий Касперского для фильтрации почтового трафика
- ☑ Техническая поддержка

Лицензию нельзя переназначить на другой сервер или переместить в свободные лицензии. Выдается автоматически один раз при регистрации сервера в разделе **Управление сервером** → **Лицензия** веб-интерфейса NGFW.

По истечении срока действия лицензии для сервера Ideco NGFW Novum:

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокирован FORWARD- и INPUT-трафик. Кроме доступа к MY.IDECO.
- Доступен перехват DNS-запросов и подключение по SSH при включении удаленного помощника.

Free

Free - свободная лицензия с ограниченным набором функций, сроком на 5 лет.

- ☑ Авторизация до 22 пользователей
- ☑ Интеграция с **Active Directory** на 2 года
- ☑ **Контроль приложений**, **Предотвращение вторжений** и расширенный **Контент-фильтр** доступны на 2 года с даты создания лицензии

Техническая поддержка не предоставляется. Недоступно: **Кластеризация**, **Расширенная база правил** (от Лаборатории Касперского) для модуля **Предотвращение вторжений**, **Антивирус Касперского** и **Антиспам Касперского**.

Чтобы добавить лицензию **Free** в личный кабинет, нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Непривязанные лицензии**.

При отсутствии/окончании срока действия лицензии для сервера Ideco NGFW Novum:

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокирован FORWARD- и INPUT-трафик. Кроме доступа к MY.IDECO.
- Доступен перехват DNS-запросов и подключение по SSH при включении удаленного помощника.

Более подробная информация о видах лицензий в Ideco доступна на сайте.

Лицензия с режимом кластеризации и технологии Лаборатории Касперского приобретаются отдельно в отделе продаж.

> NGFW Novum без лицензии по умолчанию не пропускает трафик пользователей в интернет. Для получения лицензии используйте альтернативный (дополнительный) шлюз. Если это невозможно, временно включите опцию **Полный доступ** - для этого перейдите в раздел **Техническая поддержка**, нажав  в правом верхнем углу экрана. Подробнее - в статье.

Лицензирование с режимом кластеризации

- Если право использования ПО было приобретено до 01.08.2024, все Enterprise-лицензии с действующей подпиской (Security Update) включают в себя право использования ПО для всех нод кластера со сроком использования до 01.07.2029.
- Право использования ПО для ноды кластера нужно приобретать дополнительно.
- Если приобретается право использования ПО для нод кластера, то при продлении подписки Security Update возможно только совокупное продление подписки Security Update для всех нод кластера. Продление подписки Security Update для основной лицензии и для ноды кластера по отдельности не осуществляется.
- Функциональная возможность использования ПО в кластере после приобретения права на использование для ноды кластера является бессрочной, однако подписка Security Update остается срочной.
- После окончания срока действия подписки Security Update работа кластера не нарушается.

Просмотр информации о лицензиях

Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др. Посмотреть информацию о лицензии и доступных модулях можно:

- На MY.IDECO.RU. Здесь также можно получить лицензию, посмотреть информацию о зарегистрированных серверах и настроить связь лицензий с серверами.
- В разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum.

Подробная информация об управлении лицензиями и привязке лицензии к серверу представлена в статье.

Особенности работы онлайн-лицензии:

- При наличии доступа в интернет обновление данных о лицензии происходит один раз в сутки.
- Если связь с серверами лицензирования отсутствует, Ideco NGFW Novum предпринимает попытки соединения каждые 60 секунд до восстановления доступа.
- Если у Ideco NGFW Novum отсутствует связь с серверами лицензирования более 30 дней, то Ideco NGFW Novum перейдет в нелицензионный режим.
- Для использования Ideco NGFW Novum в закрытом контуре (без доступа к интернету) необходимо использовать офлайн-лицензию.

Классический контекст | Высокопроизводительный контекст

Системные требования

Перед регистрацией и загрузкой образа Ideco NGFW Novum с MY.IDECO ознакомьтесь с системными требованиями к платформе, на которую будет установлен Ideco NGFW Novum:

- Выбор аппаратной платформы
- Виртуальная платформа

Для ФСТЭК версий Ideco UTM используются платформы:

- Программно-аппаратный комплекс (ПАК) - для межсетевых экранов типа А четвертого класса защиты.
- Виртуальная платформа - для межсетевых экранов типа Б четвертого класса защиты.

Для ФСТЭК версии Ideco NGFW Novum четвертого класса защиты используется только ПАК.

Производительность платформы

Рекомендуем использовать физический сервер, так как производительность на сервере выше по сравнению с работой в гипервизоре при сопоставимых параметрах.

Частота процессора, а также объем и частота ОЗУ сервера сильно зависят от нагрузки на Ideco NGFW Novum. При подсчете нагрузки нужно учитывать два фактора:

- Задействованные компоненты NGFW Novum (**Контроль приложений**, **Прокси** с подключенными сервисами, проверка трафика на спам/вирусы, обширность настройки модуля **Контентной фильтрации** или **Межсетевого экрана**).
- **Система предотвращения вторжений** - при скорости подключения к провайдеру от 100 Мбит/с эта служба может потребовать значительных ресурсов процессора и памяти. Рекомендуется использовать многоядерные процессоры (4 и более ядер с частотой более 3 ГГц) и от 16 ГБ оперативной памяти.

При туннелировании по типу site-to-site с небольшим количеством соединений (от 3 до 5) допустимо использовать процессор с меньшим количеством ядер, но с большей частотой. Если Ideco NGFW Novum планируется использовать как VPN-сервер для S2S и C2S с большим количеством соединений, то лучше выбрать процессор и с большим количеством ядер, и с большей частотой. Это обусловлено тем, что соединения могут распределяться по ядрам.

Выбор аппаратной платформы

> В статье представлен набор требований для корректной работы Ideco NGFW Novum на аппаратной платформе.

Программно-аппаратный комплекс

Работа Ideco NGFW Novum с конечными устройствами гарантирована только на программно-аппаратных комплексах (ПАК). Для выбора ПАК обратитесь в отдел продаж.

Сертифицированные ПАК не имеют автономного управления платформой (IPMI).

ПАК имеют регистрацию в реестре Минпромторга на базе сетевых устройств Рубеж от компании АО "КРАФТВЭЙ КОРПОРЭЙШН ПЛС":

- Для Ideco NGFW Novum MX2/LX/LX+ - номер записи 10465633, ссылка.
- Для Ideco NGFW Novum EX - номер записи 10549715, ссылка.

Собственный сервер

Минимальные системные требования

Корректная работа на стороннем оборудовании не гарантируется.

Минимальные системные требования удовлетворяют низкой загруженности служб NGFW, обслуживающих небольшое количество авторизованных пользователей (до 50 человек).

Платформы Ideco SX+ и Ideco SMX в текущих версиях не поддерживают запуск VCE. Поддержка планируется в следующих версиях.

Требования	Характеристики
Процессор	• Intel i3/i5/i7/i9/Xeon минимум 4 поколения Haswell (2013г.) • AMD FX/Ryzen/EPYC. • Поддержка SSE 4.2. • От 4 ядер.
Объем оперативной памяти	• От 16 ГБ (16-64 ГБ в зависимости от количества пользователей, от 32 ГБ с созданием VCE).
Накопитель	• Объем 150 ГБ или более. • Запись 4K блоками в один поток, с синхронизацией каждой записи не менее 1000 IOPS. • SSD с интерфейсом SATA, mSATA, SAS, NVMe. • Дополнительный SSD при использовании почтового сервера. • Не гарантируется работа с аппаратными RAID-контроллерами (программные контроллеры, интегрированные в чипсет, не поддерживаются).
Сеть	• Две сетевые карты (или два сетевых порта) 100/1000 Mbps на чипах Intel.
BIOS	• Поддержка UEFI. • Отключенная опция Secure Boot в UEFI. • Отключенный режим Legacy, может называться CSM (Compatibility Support Module).
Дополнительно	• Монитор и клавиатура (не требуется, если используется IPMI).

Высокопроизводительный контекст поддерживает работу до 100 000 правил **Межсетевого экрана**.

Минимальные требования (для 10K-100K правил):

- Процессор: от 8 ядер.
- Оперативная память: от 64 ГБ.

Полная загрузка правил в интерфейсе может занять несколько минут.

На каждый VCE требуется:

- Классический контекст: не менее 2 ядер CPU и 8 ГБ оперативной памяти.
- Высокопроизводительный контекст: не менее 4 ядер CPU и 8 ГБ оперативной памяти.
- Дисковое пространство: дополнительное место на SSD в зависимости от нагрузки.

Рекомендации

Ознакомьтесь с требованиями к производительности платформы по ссылке.

Чипсеты и производители

- Рекомендуем чипсеты, контроллеры и сетевые карты компании Intel.
- Не гарантируем стабильную работу и заявленную производительность, а также поддержку работоспособности сети при использовании встроенных сетевых карт, особенно интерфейсов на бюджетных/редких/устаревших/noname чипсетах.
- Не рекомендуем использовать RAID-контроллеры, так как они официально не поддерживаются нашим продуктом.
- Материнские платы могут использоваться как серверные, так и десктопные. Рекомендуем использовать процессоры Intel и AMD.

Дисковая подсистема

- Рекомендуем использовать серверные SSD с технологией защиты от сбоев питания (Power Loss Protection (PLP)).
- В большинстве конфигураций достаточно одного SSD объемом от 200 ГБ.
- Если на NGFW развернут почтовый сервер, для хранения электронной почты необходимо подключить отдельный накопитель.
- Рекомендуемые производители: Micron, Transcend, Kingston, Samsung.

Виртуальная платформа

В статье представлен набор требований для корректной работы Ideco NGFW Novum на виртуальной платформе.

Минимальные системные требования

Минимальные системные требования удовлетворяют низкой загруженности служб NGFW, обслуживающих небольшое количество авторизованных пользователей (до 50 человек).

Требования	Характеристики
Платформы виртуализации	• VMware (Workstation и ESXi) версии не ниже 6.5.0. • Microsoft Hyper-V (виртуальные машины 2-го поколения). • VirtualBox версии не ниже 7.0.0. • KVM версии не ниже 1.2.0. • Citrix XenServer. • Proxmox VE.
Тип ОС для создания виртуальной машины	• Linux Fedora 64 bit.
Процессор	• Поддержка SSE 4.2. • От 4 ядер.
Объем оперативной памяти	• 16 ГБ (16-64 ГБ в зависимости от количества пользователей).
Накопитель	• Объем 150 ГБ или более. • Запись 4К блоками в один поток, с синхронизацией каждой записи не менее 1000 IOPS. • Дополнительный диск при использовании почтового сервера. • KVM: virtio для дисков.
Сеть	• WMWare: vmxnet3. • VirtualBox: сетевая карта с типом подключения NAT. • KVM: virtio. • Microsoft Hyper-V: виртуальный сетевой адаптер (Network Adapter).
BIOS	• Поддержка UEFI. • Отключенная опция Secure Boot в UEFI. • Отключенный режим Legacy, может называться CSM (Compatibility Support Module).
Дополнительно	• Внутренние часы виртуальной машины должны быть настроены на хранение времени во временной зоне UTC.

Высокопроизводительный контекст поддерживает работу до 100 000 правил **Межсетевого экрана**.

Минимальные требования (для 10К-100К правил):

- Процессор: от 8 ядер.
- Оперативная память: от 64 ГБ.

Полная загрузка правил в интерфейсе может занять несколько минут.

На каждый VCE требуется:

- Классический контекст: не менее 2 ядер CPU и 8 ГБ оперативной памяти.
- Высокопроизводительный контекст: не менее 4 ядер CPU и 8 ГБ оперативной памяти.

- Дисковое пространство: дополнительное место на SSD в зависимости от нагрузки.

Для максимальной производительности рекомендуем:

- Режим работы кэша виртуального диска: writeback. Хранилище должно гарантировать сохранность данных после завершения команды фиксации кэша.
- Настроить паравиртуализованный источник энтропии (Random Number Generator (RNG)).
- Настроить паравиртуализованные часы и таймер.
- Убедиться, что виртуальные процессоры, использующиеся для виртуальной машины, располагаются на одной физической NUMA-ноде.
- Гипервизор с аппаратной виртуализацией (вложенная виртуализация не требуется).

Ознакомьтесь с требованиями к производительности платформы по ссылке.

Информация по настройке гипервизора доступна по ссылке.

Техническая поддержка

Одним из главных приоритетов компании Ideco является высокий уровень удовлетворенности наших клиентов.

Техническая поддержка предоставляется в период действия подписки на сервис. Подписка включена в стоимость лицензии и действует в течение года с момента приобретения продукта. После окончания срока действия подписка может быть продлена на срок от 1 года и более.

Подробнее о подписке на техническую поддержку и обновления можно посмотреть на сайте компании Ideco.

График работы

Дни недели	Время работы (московское)
понедельник-пятница	04:00 - 21:00
суббота	09:00 - 16:00
воскресенье и праздничные дни	выходной/особое расписание

В рамках расширенной технической поддержки на договорных условиях техподдержка оказывается круглосуточно 24x7x365.

Способы обращения

Способ	Обращаться через
Портал поддержки. Для получения доступа к порталу отправьте запрос на электронную почту support@ideco.ru	support.ideco.ru
Телефон	+7 (495) 662-87-34
Telegram	ideco_support_bot
MAX	id6670208848_bot
Интерактивный онлайн-чат со специалистом технической поддержки	https://my.ideco.ru/, https://ideco.ru/, веб-интерфейс Ideco NGFW Novum

Правила обращения

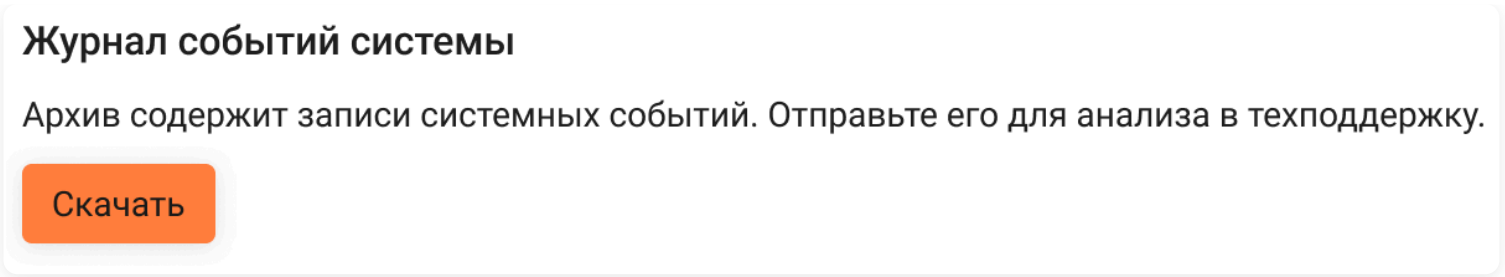
Техническая поддержка пользователей осуществляется в соответствии с регламентом.

- Техническая поддержка оказывается по вопросам настройки продуктов компании "Айдеко";
- Специалисты службы техподдержки не занимаются обучением пользователей продукту в рамках оказания услуг по поддержке.

При обращении необходимо предоставить следующую информацию: название организации, ваши контактные данные, номер лицензии.

Скачивание журнала системных событий

В веб-интерфейсе Ideco NGFW Novum доступно скачивание журнала системных событий для передачи в техническую поддержку.
Для скачивания нажмите в правом верхнем углу экрана, а затем **Скачать** в блоке **Журнал событий системы**:



Начнется загрузка архива в формате **zst** с файлом логов:

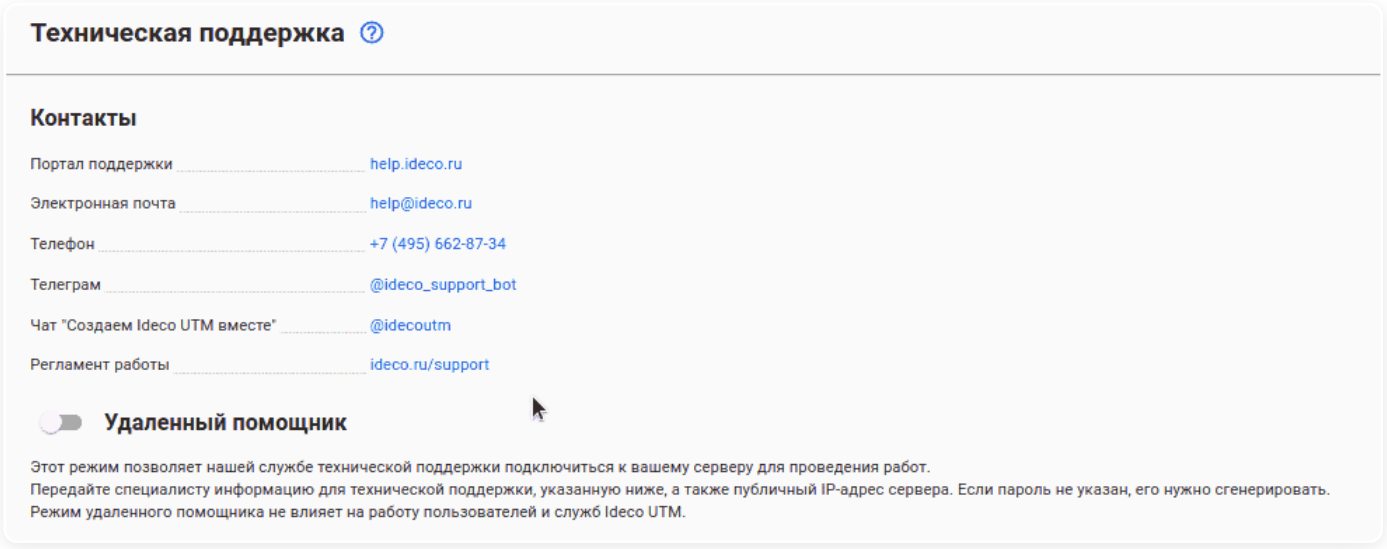
- Если установка первичная или не было возврата к предыдущей версии, файл будет содержать события текущей версии.
- Если был возврат к предыдущей версии, файл будет содержать события версии, с которой произошел возврат, и события текущей версии, записанные до возврата.

Режим удаленного помощника

Чтобы служба технической поддержки могла подключиться к серверу удаленно, необходимо включить режим удаленного помощника. Работа сервера в этом режиме не влияет на работу пользователей.

Для включения режима удаленного помощника нажмите на значок в правом верхнем углу экрана и переведите ползунок около пункта **Удаленный помощник** в статус **Включен**.

Включение режима удаленного помощника изменяет таблицу правил **Межсетевого экрана**. При этом становится доступно подключение по SSH: из WAN-зоны - только для ограниченного списка адресов Технической поддержки, из локальных сетей - для любого источника.



Включение режима удаленного помощника из веб-интерфейса

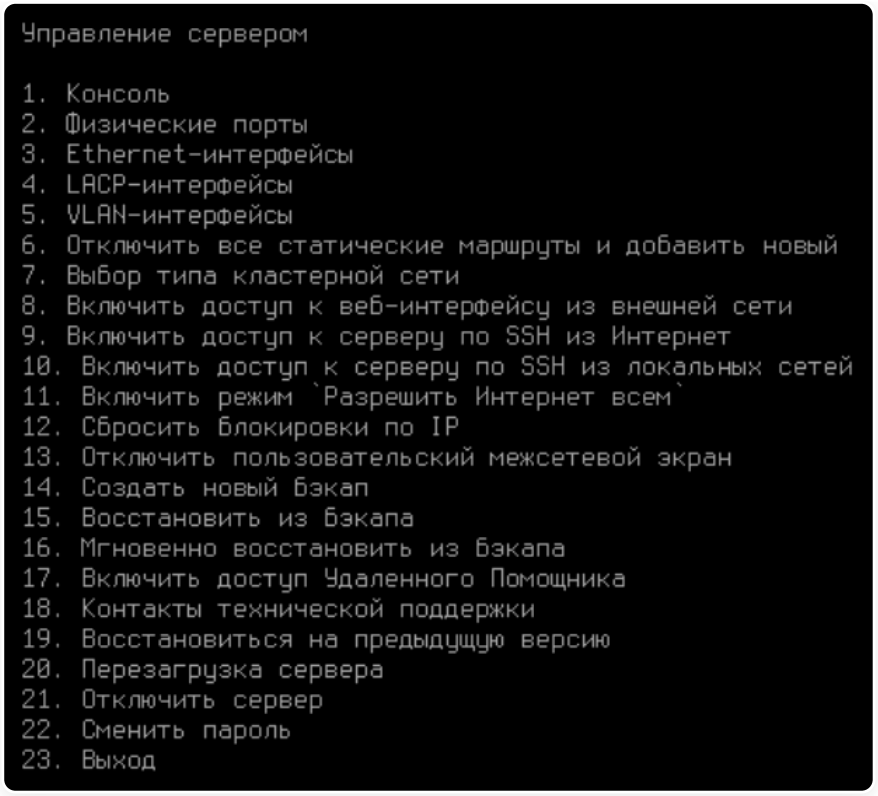
Для подключения специалиста технической поддержки сообщите ему **Информацию для технической поддержки**, нажав кнопку **Скопировать**. Также нужно отдельно передать публичный IP-адрес сервера. Если сервер подключен не напрямую к Ideco NGFW Novum, выполните проброс с внешнего маршрутизатора до 22-го порта на NGFW.

Режим удаленного помощника остается включенным даже при перезагрузке сервера. Отключайте режим удаленного помощника, когда использовать режим нет необходимости. **Крайне не рекомендуется постоянная эксплуатация сервера Ideco NGFW Novum в этом режиме.**

Включение режима удаленного помощника из локального меню сервера

Чтобы включить режим удаленного помощника, в локальном меню Ideco NGFW Novum введите номер пункта **Включить доступ Удаленного помощника**, затем нажмите **Enter**.

Сгенерируется пароль, который необходимо сообщить технической поддержке для подключения по SSH:



Работа с сервером по протоколу SSH в режиме удаленного помощника

Чтобы организовать работу с локальной консолью сервера удаленно по протоколу SSH от пользователя **root** в режиме удаленного помощника, необходимо выполнить следующие действия:

1. Подключитесь к серверу с помощью SSH-клиента **PuTTY**. Программа бесплатна, скачать можно на сайте разработчиков (https://www.putty.org/).

2. При подключении из локальной сети используйте адрес, который настроен на локальной сетевой карте Ideco. Введите необходимые параметры для подключения:

- **порт** - 22;
- **логин** - remsup;
- **пароль, указанный при включении удаленного помощника.**

Символ "#" свидетельствует, что работа ведется от имени суперпользователя.

Полный доступ

Классический контекст | Высокопроизводительный контекст

Используйте режим только для диагностики.

Режим **Полный доступ** не отключается автоматически и продолжает работать, пока режим не отключить вручную.

При включении:

- Сбор веб-статистики будет отключен.
- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включен автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Межсетевого экрана**.

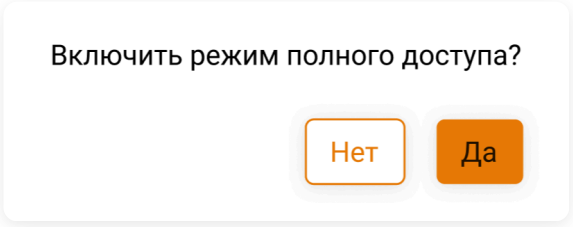
Цикл обработки трафика в Ideco NGFW Novum описан в статье.

Включить режим можно через:

Веб-интерфейс

Нажмите на иконку технической поддержки в верхней правой части окна, а затем в блоке **Полный доступ** нажмите **Включить**:

Подтвердите выбор, нажав **Да**:



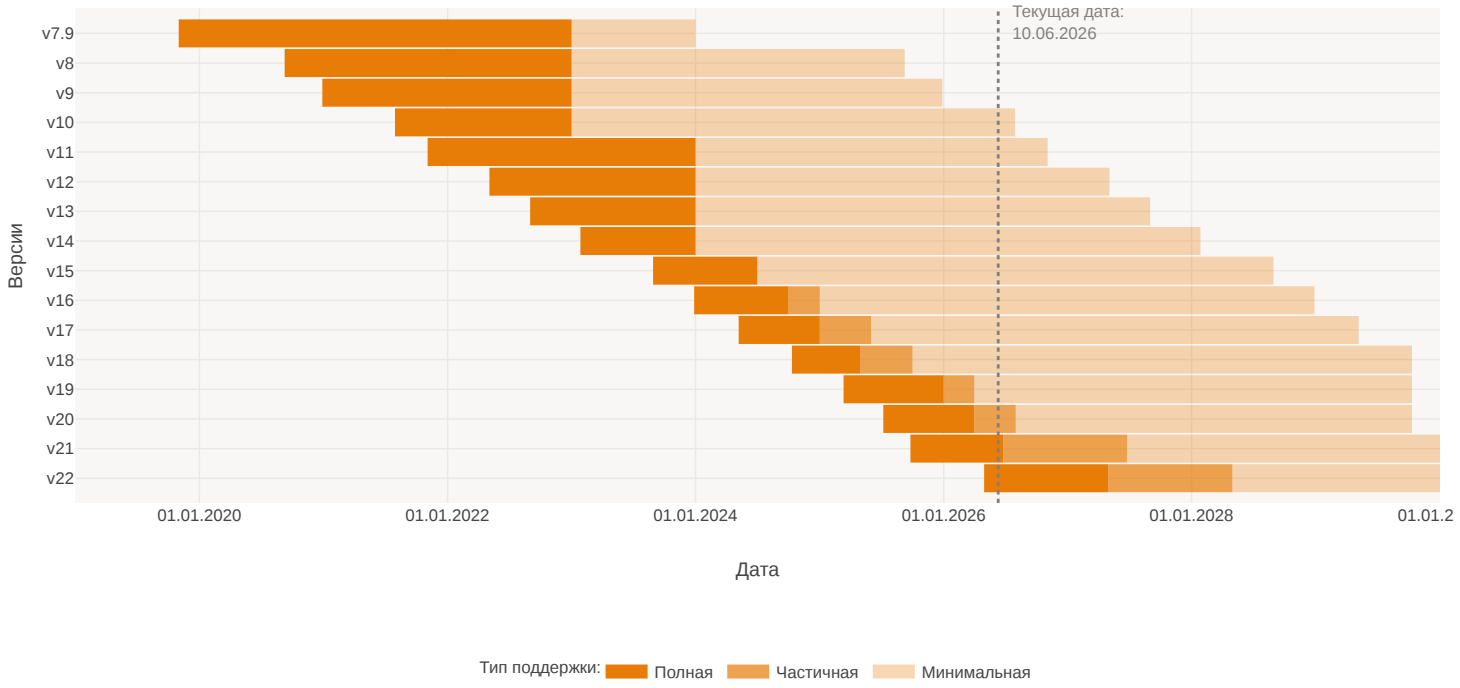
Локальное меню

Выберите **Включить режим Разрешить интернет всем** и нажмите **Enter** для применения настройки:

Информация о поддержке версий Ideco NGFW Novum

В статье описываются типы поддержки Ideco NGFW Novum и сроки поддержки по каждой версии.

Сроки поддержки



Что входит в типы поддержки

✅ Поддержка гарантируется.

❓ Поддержка не гарантируется. Стараемся поддерживать максимально долго, но гарантий нет.

Тип	Полная	Частичная	Минимальная
Автообновление системы	✅	✅	✅
Обновление баз: • Предотвращение вторжений • Контент-фильтр • IpList • GeoIP	✅	❓	❓
Антивирус Касперского	✅	❓	❓
Антивирус и антиспам Касперского для почты	✅	❓	❓
Сигнатуры IPS от Лаборатории Касперского	✅	❓	❓
Исправление некритичных багов (например, ошибка в тексте)	✅	❓	❓
Баги безопасности (CVE)	✅	✅	❓
Исправление критических багов (влияют на работу продукта в целом или отдельного модуля)	✅	✅	❓

Техническая поддержка (простое обращение)	✅	✅	❓
Техническая поддержка (сложное обращение)	✅	❓	❓
Документация	✅	✅	❓

Настройка двухфакторной аутентификации с использованием TOTP-токенов

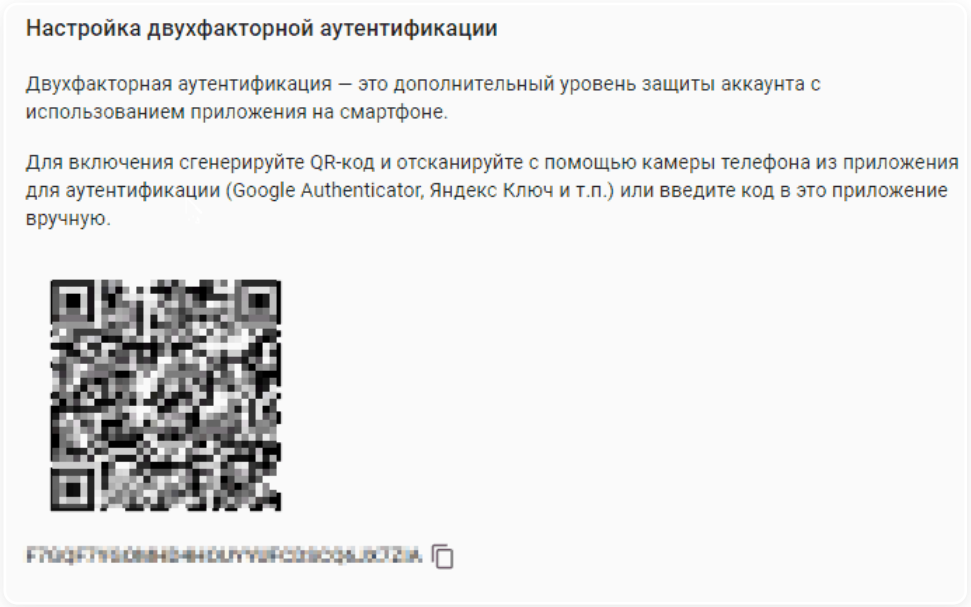
TOTP (Time-based One-Time Password) - это временные одноразовые пароли, которые меняются каждые 30 секунд. Метод аутентификации с использованием TOTP-токенов обеспечивает дополнительный уровень безопасности для ваших аккаунтов.

Для настройки выполните действия:

1. Установите приложение:

- Для смартфонов (Android/iOS):
  - Google Authenticator: Play Market (Android), App Store (iOS).
  - Яндекс ID: Play Market (Android), App Store (iOS).
  - Другое аналогичное приложение.
- Браузерное расширение для компьютеров, например:
  - Аутентификатор для Chrome.
  - Authenticator для Firefox.

2. Активируйте 2FA на NGFW Novum. Подробнее - в статье. Система отобразит QR-код и секретный ключ (строка букв и цифр):

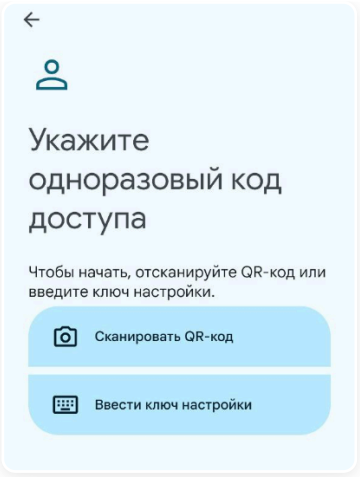


3. Добавьте аккаунт в приложение.

Google Authenticator

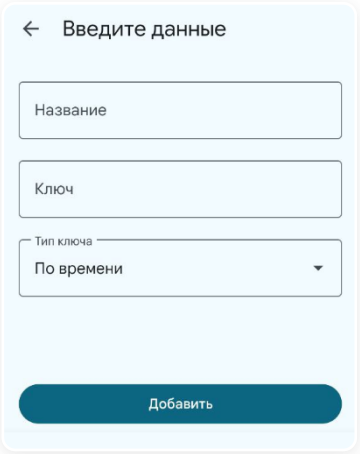
1. Запустите приложение и нажмите **Начать**.

2. Нажмите **Добавить код**:



3. Выберите опцию:

- **Сканировать QR-код** - наведите камеру и сканируйте код на сайте.
- **Ввести ключ настройки**:



- **Название** - укажите название аккаунта.
- **Ключ** - вставьте секретный ключ с сайта.
- **Тип ключа** - оставьте **По времени**.

4. Нажмите **Добавить**.

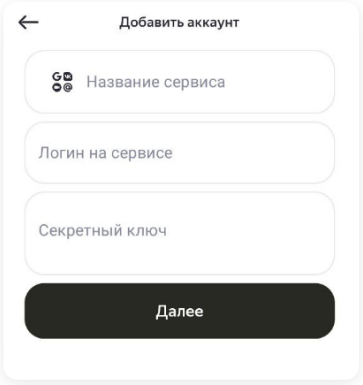
В приложении отобразится шестизначный код и таймер обратного отсчета (30 секунд). Код автоматически обновляется.

Яндекс ID

1. Запустите приложение и нажмите **Добавить аккаунт**.

2. Выберите опцию:

- **Сканировать QR** - наведите камеру и сканируйте код на сайте.
- **Добавить вручную**:



- **Название сервиса** - укажите название сервиса.
- **Логин на сервисе** - укажите логин на сервисе.
- **Секретный ключ** - укажите секретный ключ с сайта.

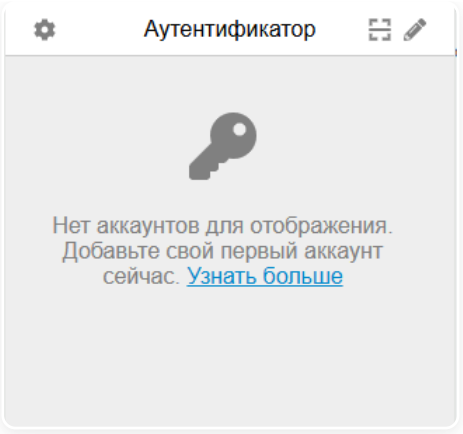
3. Нажмите **Далее**.

В приложении отобразится шестизначный код и таймер обратного отсчета (30 секунд). Код автоматически обновляется.

Расширение Аутентификатор

Для Chrome

1. Для сканирования QR-кода нажмите на иконку расширения в правом верхнем углу браузера, выберите установленное расширение, нажмите и выделите область с QR-кодом на сайте.



2. Для ручного ввода ключа нажмите , а затем - , из меню выберите **Ручной ввод** и укажите:

- Название сервиса.
- Секретный ключ с сайта.

Для Firefox

Процесс настройки аналогичен Chrome-расширению.

Технологические партнеры

> В статье представлена информация о продуктах других вендоров, совместимость с которыми была протестирована.

В таблице указаны продукты, которые могут интегрироваться в инфраструктуре с продуктами Ideco.

Продукт	Компания	Класс продукта
Alertix	ООО «ЭнДжиАр софтлаб»	SIEM-система
ALD Pro	ООО "РусБИТех-Астра"	Служба каталога для Linux
Astra Linux	ООО "РусБИТех-Астра"	Операционная система
DS Proxima	АО "НПП "Цифровые решения"	Аппаратный балансировщик нагрузки. Интеграция NGFW Novum и DS Integrity NG
Efros DefOps	ООО "Газинформсервис"	Многофункциональный комплекс по защите ИТ-инфраструктуры (сетевых и оконечных устройств, компонентов сред виртуализации), а также прикладного ПО: SCADA, RPA, СУБД, NAC, NA, VC, FA, CM
IVA MCU	ПАО "ИВА"	Платформа видеоконференцсвязи
IVA ONE	ПАО "ИВА"	Платформа бизнес-коммуникаций
JaCarta Management System 4LX (включает JaCarta Authentication Server и Aladdin 2FA)	АО "Аладдин Р.Д."	Корпоративная система централизованного управления для Linux
Kaspersky Anti-Spam	ЗАО "Лаборатория Касперского"	Антиспам
Kaspersky Anti Targeted Attack Platform (KATA Sandbox)	ЗАО "Лаборатория Касперского"	Сетевая песочница
Kaspersky Threat Intelligence	ЗАО "Лаборатория Касперского"	Сигнатуры
Microsoft Active Directory	Microsoft	Служба каталога для Windows
MIST Insight	ООО "МИСТ"	NSPM (Network Security Policy Management)
Multifactor	ООО "Мультифактор"	Система двухфакторной аутентификации и контроля доступа
Netopia	ООО "Нетопия"	Мониторинг и контроль сетевой безопасности
Securitm	ООО "СЕКЪЮРИТМ"	Система управления информационной безопасностью
SKY DNS	"СкайДНС"	Решение DNS Security и фильтрация контента. Интеграция NGFW Novum и SkyDNS
SMS Aero	ООО "СМС Аэро"	SMS-рассылка
UDV DATAPK Industrial Kit	ООО "СайберЛимфа"	Система обнаружения вторжений в промышленных сетях
UDV ITM	ООО "СайберЛимфа"	Единое решение для мониторинга на базе Zabbix. Подходит для мониторинга АСУ ТП, серверов, каналов связи и ИТ-услуг
VK Cloud	ООО "Цифровое Облако"	Платформа сетевого доступа к вычислительным ресурсам и различным облачным сервисам
Альт Домен	ООО "Базальт СПО"	Служба каталогов
Альт Рабочая станция	ООО "Базальт СПО"	Операционная система
Альт Сервер	ООО "Базальт СПО"	Серверный дистрибутив с широкой функциональностью
АльтерОС	ООО "Алми Партнер"	Сертифицированная российская операционная система на Linux последнего поколения
Антивирус Касперского	ЗАО "Лаборатория Касперского"	Антивирус
БИТ.Аутентификатор	ООО "Первый Бит"	Система двухфакторной аутентификации
MFASOFT	ООО «СИС разработка»	Система двухфакторной аутентификации
Indeed Access Manager	ООО «Индид»	Система двухфакторной аутентификации
Контур Staffcop Enterprise	ООО "АТОМ Безопасность"	Система расследования инцидентов внутренней информационной безопасности

КриптоПро NGate	ООО "КРИПТО-ПРО"	Универсальное высокопроизводительное средство криптографической защиты сетевого трафика (TLS- и VPN-сервер)
ОСОН "ОСнова"	АО "НППКТ"	Операционная система для рабочих станций и серверов
Ред АДМ	ООО "РЕД СОФТ"	Система централизованного управления ИТ-инфраструктурой
Ред Виртуализация	ООО "РЕД СОФТ"	Система управления виртуализацией серверов и рабочих станций
Ред ОС	ООО "РЕД СОФТ"	Операционная система
Рутокен ЭЦП 3.0	АО "Актив-софт"	Электронный идентификатор
СёрчИнформ КИБ	ООО "СёрчИнформ"	DLP-система

Источники данных

Классический контекст | Высокопроизводительный контекст

Ideco NGFW Novum может обращаться к адресам для получения данных:

Тип запроса	Адрес	Используемые порты
Отправка уведомлений в личный кабинет/телеграм-бот	api.ideco.ru	443 TCP-порт
Обновление баз Контент-фильтра	content-filter.v22.ideco.dev	443 TCP-порт
Отправка анонимной статистики	gatherstat.v22.ideco.dev	443 TCP-порт
Обновления баз GeoIP	ip-list.v22.ideco.dev	443 TCP-порт
Обмен информацией о лицензии	api.ideco.ru	443 TCP-порт
Отправка отчетов по почте	api.ideco.ru	443 TCP-порт
Обновления сигнатур IDS/IPS	suricata.v22.ideco.dev	443 TCP-порт
Обновления системы	api.ideco.ru	443 TCP-порт
Синхронизация времени	ntp.ideco.ru	123 UDP-порт
Получение сертификатов Let's Encrypt	acme-v02.api.letsencrypt.org	443 и 80 TCP-порты
Антивирус Касперского (обновление баз)	Серверы с официального сайта Лаборатории Касперского	443 и 80 TCP-порты
DNS security	193.58.251.10	853 TCP-порт

Часть запросов к указанным выше серверам может быть перенаправлена на `mcs-vm.ideco.ru`, `update.ideco.ru`, `storage.yandexcloud.net` (443 порт).

Для корректной работы всех модулей фильтрации Ideco NGFW Novum необходимо, чтобы доступ к вышеуказанным ресурсам был разрешен настройками фильтрации.

Учитывайте при обновлении, что `v22` в домене соответствует версии Ideco NGFW Novum. Эту часть можно заменить символом `*` при настройке фильтрации. Например: `license.*.ideco.dev`.

Таблица портов Ideco NGFW Novum, доступных из локальной и внешних сетей

- Протокол ICMP разрешен на внешних и локальных интерфейсах.
- TCP-порт 8443, предназначенный для веб-интерфейса, находится в состоянии **Listen** постоянно. Порт открыт в локальную сеть сразу после установки Ideco NGFW Novum и настройки интерфейсов.
- TCP-порты 80 и 443, открытые во внешнюю и локальную сеть сразу после установки Ideco NGFW Novum и настройки интерфейсов, находятся в состоянии **Listen** постоянно.

Доступные из внешней сети

Включенная служба	Порты
Доступ к веб-интерфейсу из внешних сетей	8443 TCP
Доступ по SSH из внешних сетей	22 TCP
VPN IPSec	500, 4500 UDP
VPN L2TP	500, 4500 UDP
VPN PPTP	1723 TCP
VPN SSTP	1443 TCP (порт настраивается пользователем)
Ideco Client	443 TCP (по умолчанию), 14765 TCP (резервный), 3051 UDP (для Wireguard)
SMTP(S)	25, 587 TCP
Веб-почта	443 TCP
Обратный прокси	443, 80 TCP
POP3(S)	110, 995 TCP
IMAP(S)	143, 993 TCP
BGP	179 TCP

Доступные из локальной сети

Включенная служба	Порты
Доступ к веб-интерфейсу из локальной сети	8443 TCP
Прокси	8080 TCP (порт настраивается пользователем)
DNS	53 TCP, UDP
DHCP-сервер	67, 68 UDP
NTP-сервер	123 UDP
Тест скорости	18080 TCP
OSPF	-
Zabbix-сервер	10050, 10051 TCP
Let's Encrypt	80 TCP
Веб-аутентификация	443 TCP
Двухфакторная аутентификация	443 TCP
Ideco Client	443 TCP (по умолчанию), 14765 TCP (резервный)
Обратный прокси (Веб-почта, Веб-интерфейс, Личный кабинет/Портал SSL VPN)	443 TCP

Как проверить, открыт ли порт

Чтобы проверить, открыт ли порт, воспользуйтесь инструментом nmap, выполнив команду:

```
nmap -v 192.168.0.150
```

- 192.168.0.150 - адрес локального или внешнего интерфейса Ideco NGFW Novum.

Рекомендации при первоначальной настройке

Рекомендуемая последовательность шагов для минимальной настройки Ideco NGFW Novum:

1. Зарегистрируйтесь в MY.IDECO. Подробнее в статье О личном кабинете MY.IDECO.

2. Скачайте загрузочный образ продукта. Дистрибутивы также доступны в личном кабинете MY.IDECO.

3. Определитесь с устройством, на которое собираетесь устанавливать Ideco NGFW Novum, и выполните предварительные действия. Ideco NGFW Novum можно устанавливать как на виртуальную машину, так и на физический сервер.

4. Установите Ideco NGFW Novum на устройство, создайте учетную запись администратора. Для этого воспользуйтесь статьей Установка.

5. Выполните первоначальную настройку Ideco NGFW Novum. Воспользуйтесь статьей Первоначальная настройка.

6. Зарегистрируйте сервер в MY.IDECO и получите лицензию.

7. Создайте учетные записи пользователей и настройте авторизацию, чтобы получить доступ в интернет через Ideco NGFW Novum. Более подробная информация представлена в статье Получение доступа в интернет.

Подготовка платформы к установке

Установка в гипервизоре

Перейти >

Создание загрузочного USB-накопителя

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка гипервизора

Если при установке Ideco NGFW Novum появилось окно с текстом **Installation in BIOS mode is not supported**, необходимо проверить включение режима UEFI в настройках.

Методы обеспечения отказоустойчивости:

- Встроенные технологии гипервизора:
  - High Availability (HA) - автоматический перезапуск виртуальных машин на другом узле при сбое.
  - Fault Tolerance (FT) - синхронное дублирование виртуальной машины для нулевого простоя.
- Кластеризация.

Не рекомендуется применять два метода одновременно.

VMware ESXi 6.7

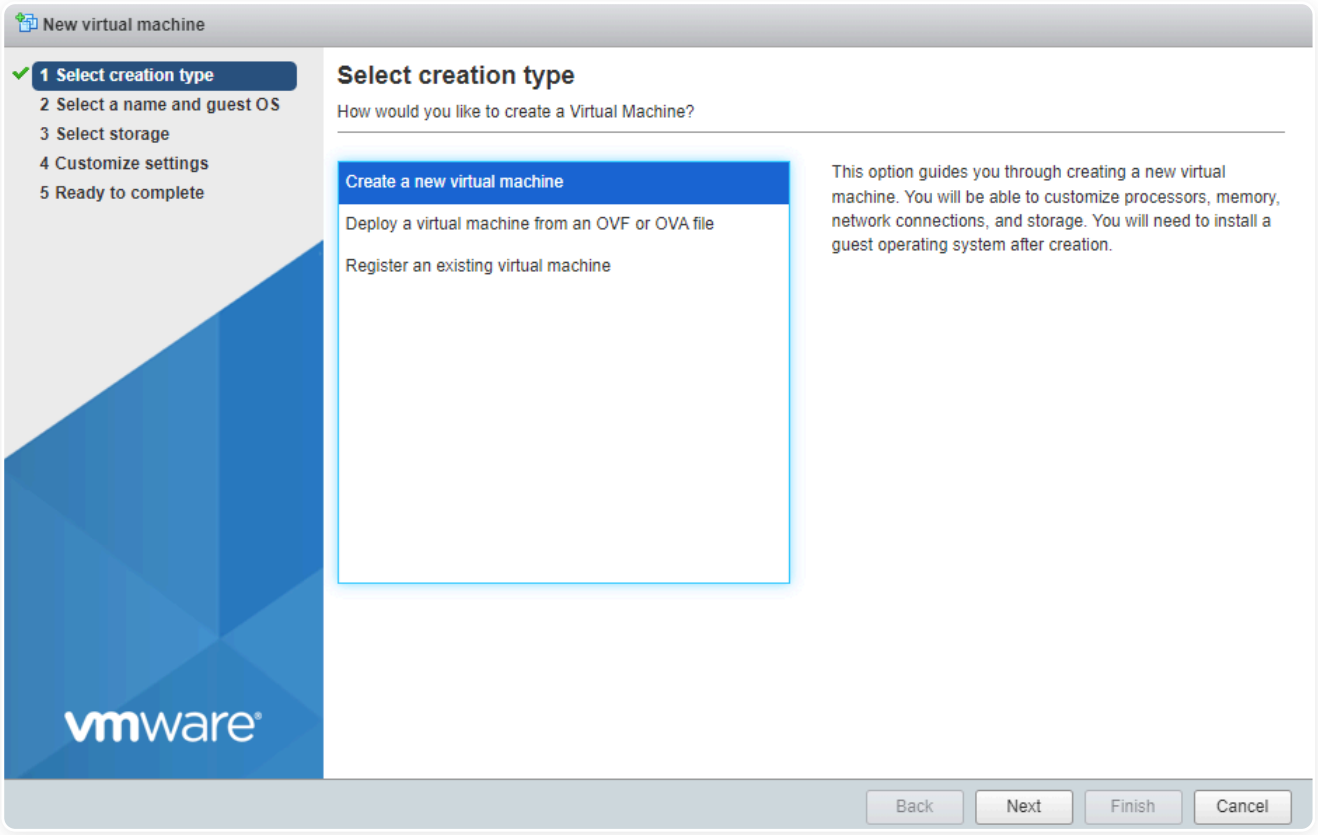
При установке Ideco NGFW Novum на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

Настройка

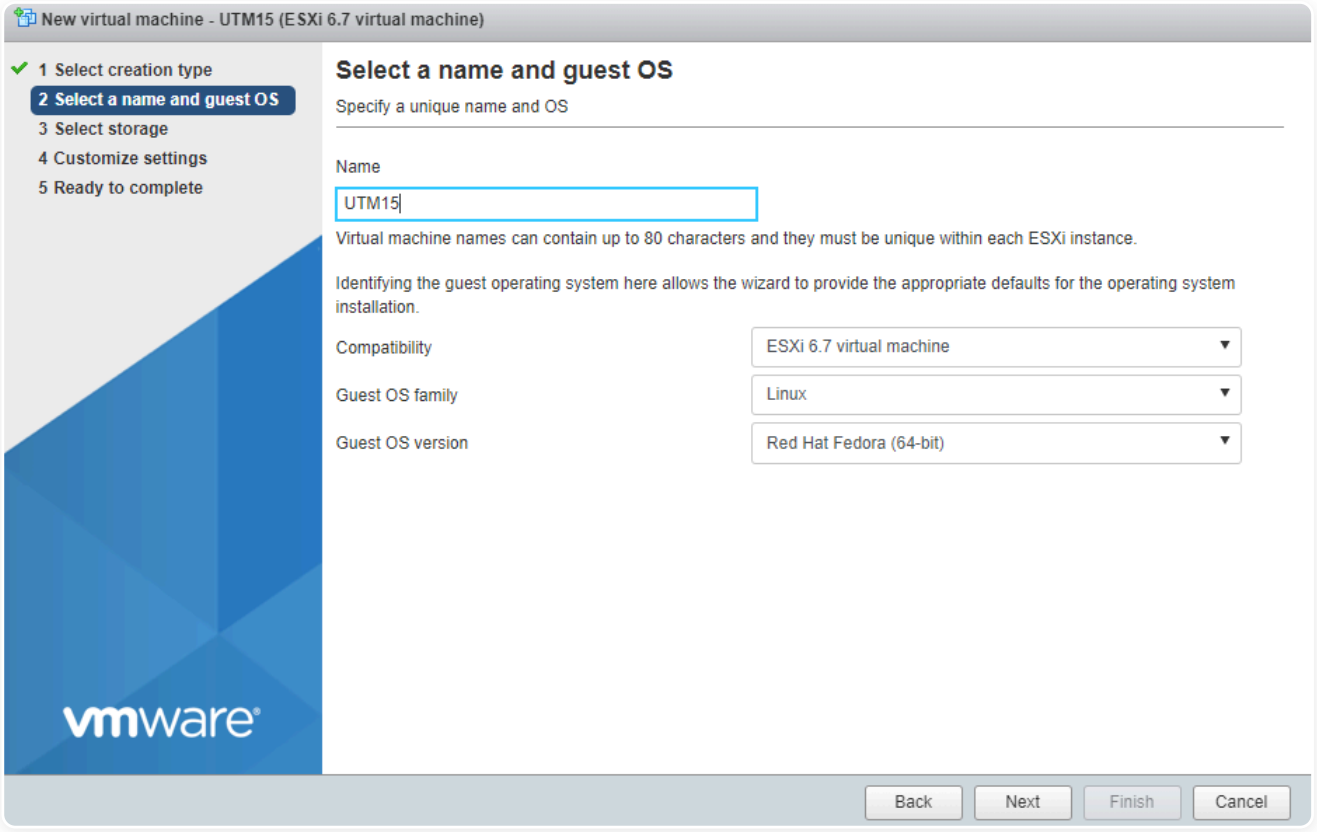
Перед установкой Ideco NGFW Novum:

- Загрузите образ, скачанный в MY.IDECO, на VMware ESXi. При настройке виртуальной машины потребуется указать путь к образу.
- Увеличьте размер видеопамяти для виртуальной машины до 16 МБ.
- Используйте виртуальные сетевые адаптеры **vmxnet3**, **e1000e**.

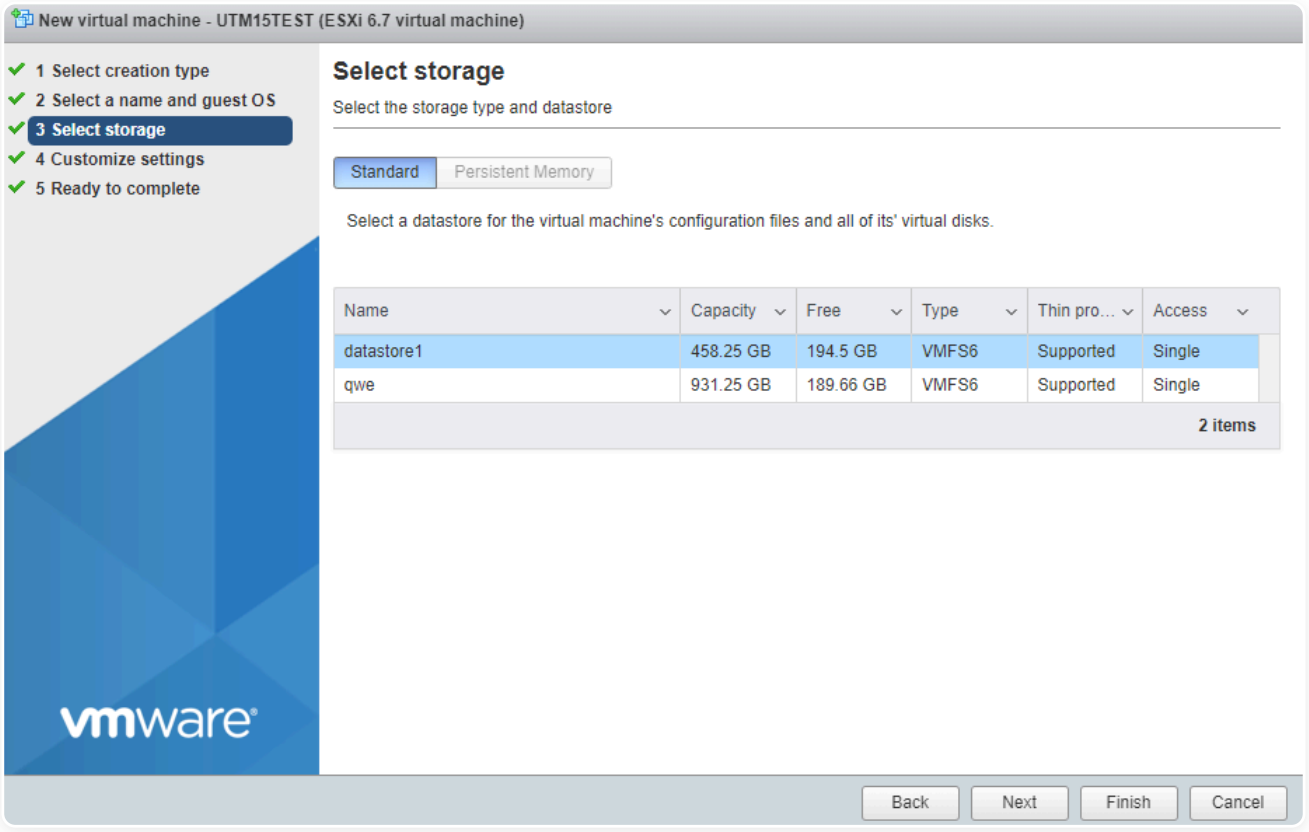
1. Создайте виртуальную машину:



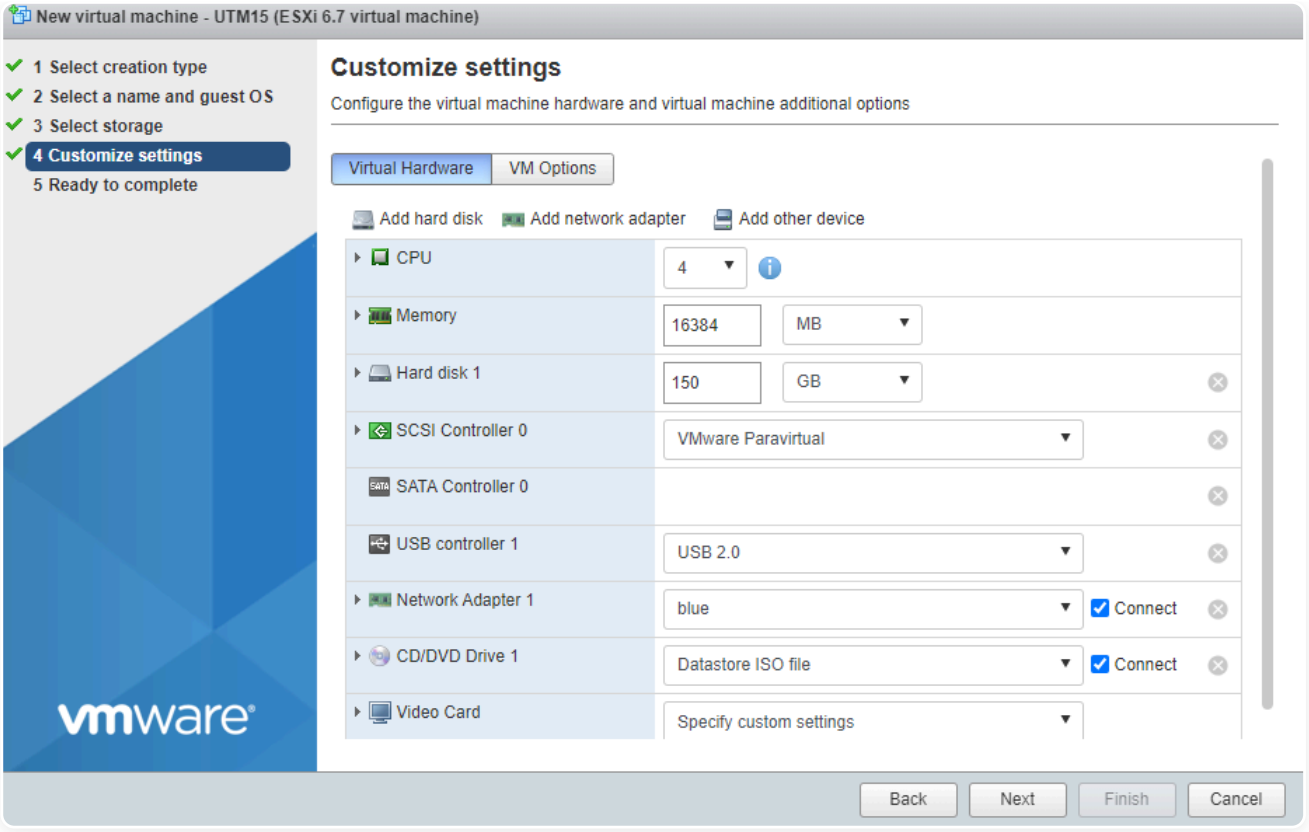
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



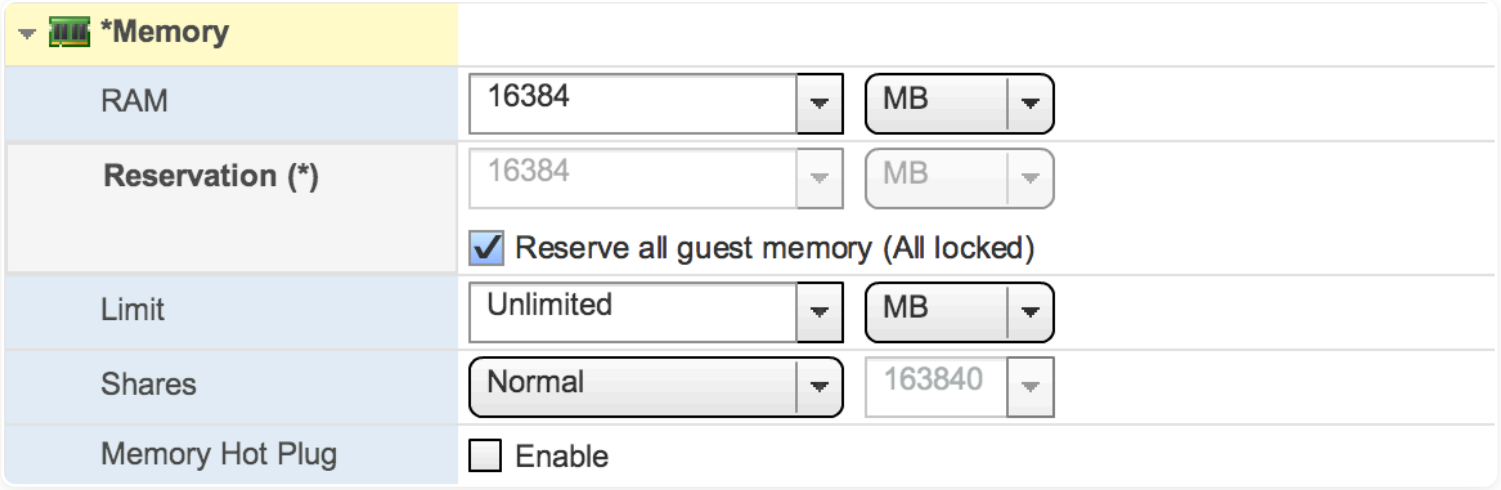
3. Выберите хранилище для виртуальной машины:



4. Установите размер оперативной памяти **16 ГБ**, количество ядер процессора **4** и размер диска **150 ГБ**. После выберите в поле **CD/DVD Drive** Datastore ISO file и укажите путь к загрузочному образу:

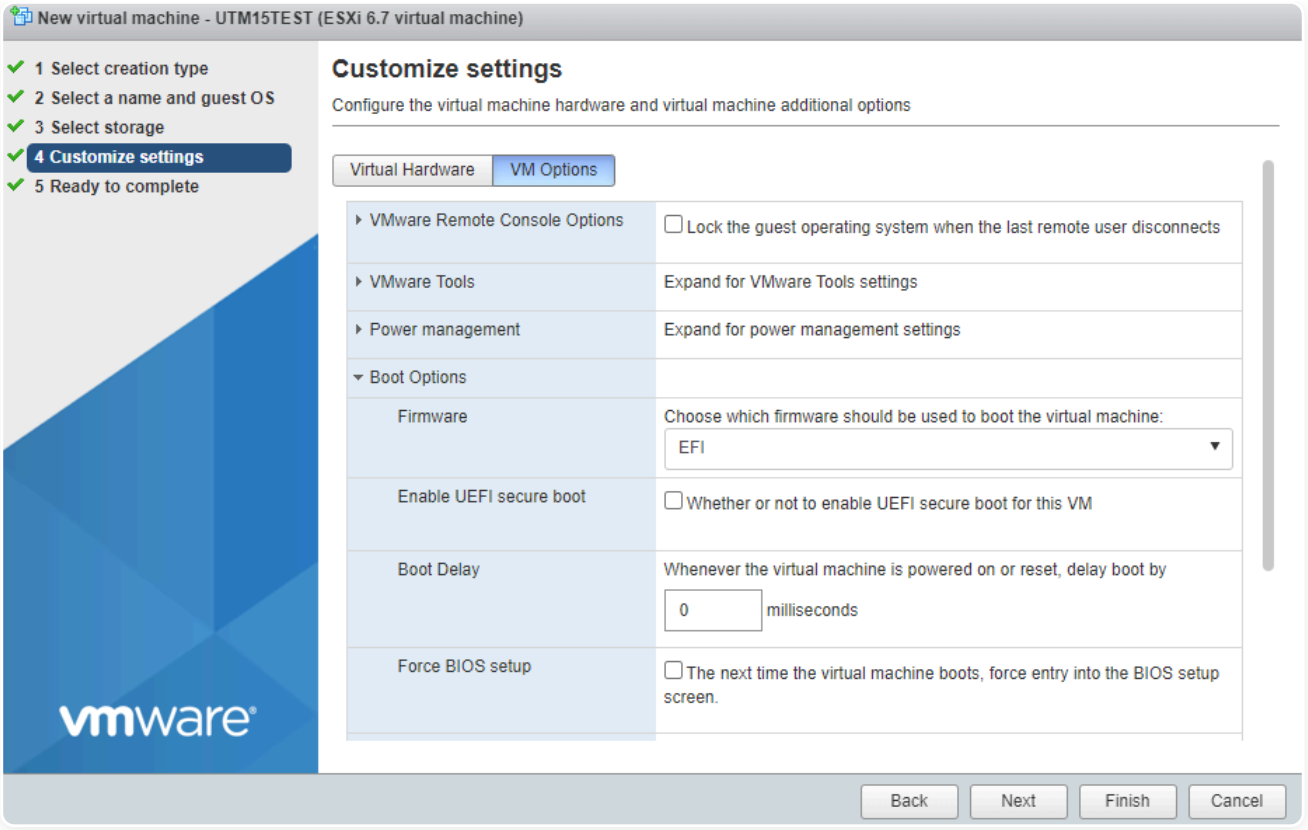


5. Разверните раздел **Memory** и включите опцию **Reserve all guest memory (All locked)**:

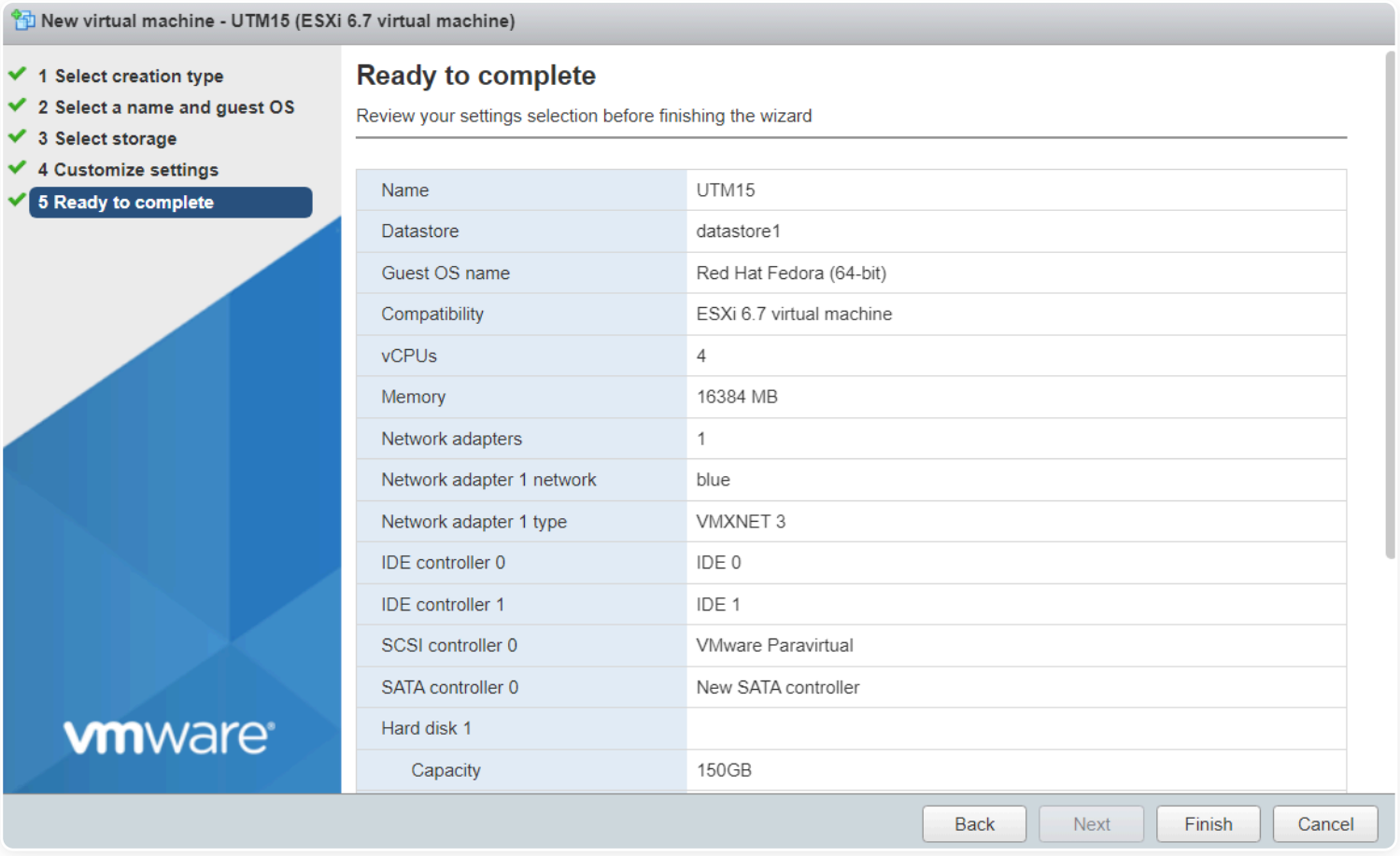


- **Reserve all guest memory (All locked)** - если опция выключена, гипервизор динамически распределяет доступную оперативную память между всеми виртуальными машинами.

6. Включите **UEFI** на вкладке **VM Options**, выбрав в поле **Firmware** EFI:



7. Нажмите **Finish**:



Настройка кластеризации

Для корректной работы кластерной сети требуются дополнительные настройки, так как гостевая ОС программно назначает порту синхронизации MAC-адрес, отличный от аппаратного, заданного в настройках виртуальной машины.

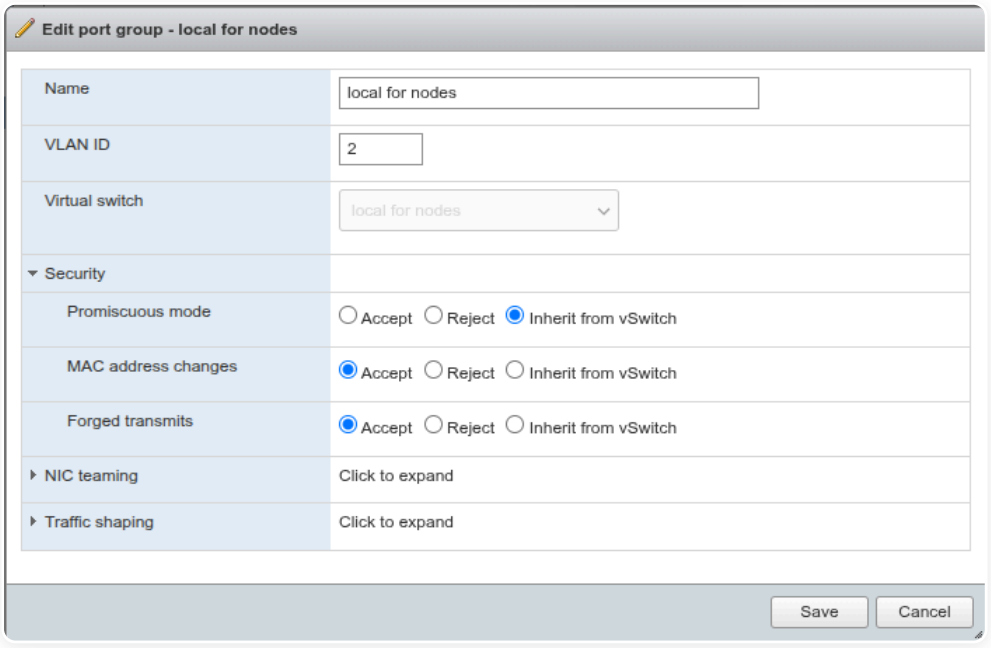
Выполните действия:

1. В интерфейсе VMware ESXi перейдите в **Navigator** → **Networking** → **Port groups**.

2. Выберите группу портов, используемую для сети синхронизации нод, и нажмите **Edit settings**.

3. Раскройте раздел **Security**.

4. Установите значение **Accept** для двух параметров:



- **MAC address changes** - разрешает прием трафика на MAC, отличающийся от заданного в настройках ВМ.
- **Forged transmits** - разрешает отправку кадров с MAC-адресом источника, отличающимся от заданного в настройках ВМ.

5. Нажмите **Save**.

6. Перезапустите NGFW Novum.

> Для синхронизации нод кластера NGFW Novum в виртуальных средах не рекомендуется использовать LACP. Если требуется отказоустойчивость канала между ESXi-хостами, настройте LACP на стороне самих хостов и физических коммутаторов - агрегация будет работать прозрачно для NGFW Novum.

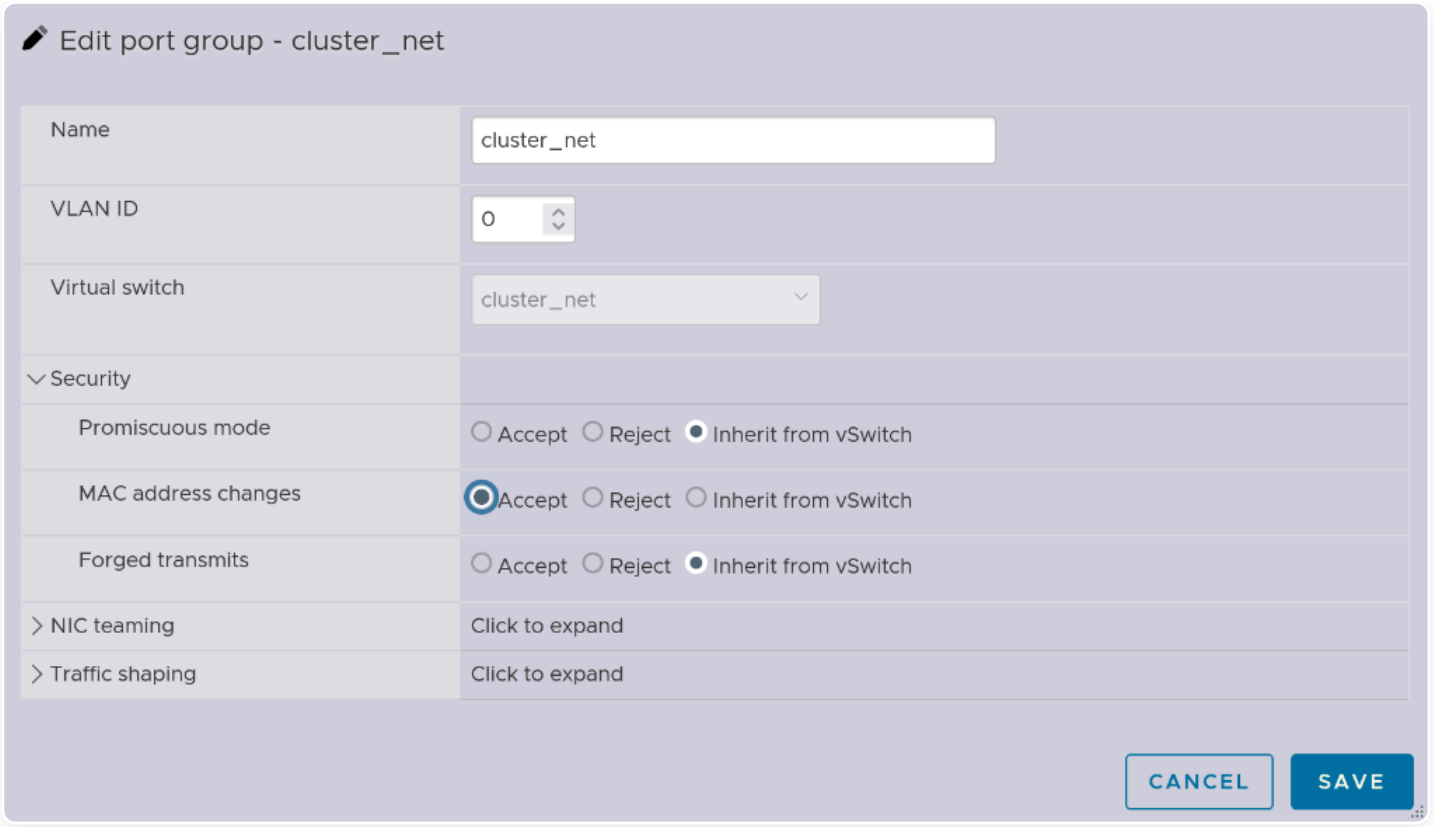
Настройка LACP-интерфейсов

При использовании LACP-интерфейсов требуется настройка группы портов. Для этого:

1. Перейдите в **Networking** → **Port groups**.

2. Выберите группу портов, используемую для LACP.

3. Перейдите в **Edit settings** → **Security** → **MAC address changes** и поменяйте значение на **Accept**:



4. Нажмите **Save**.

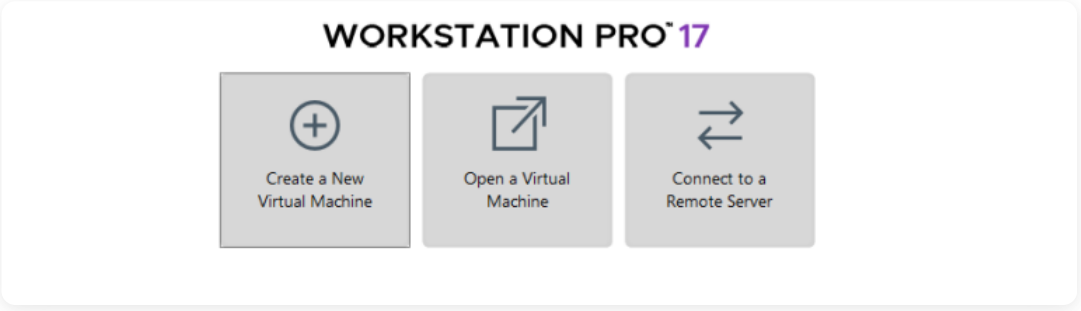
VMware Workstation 17.0

Настройка

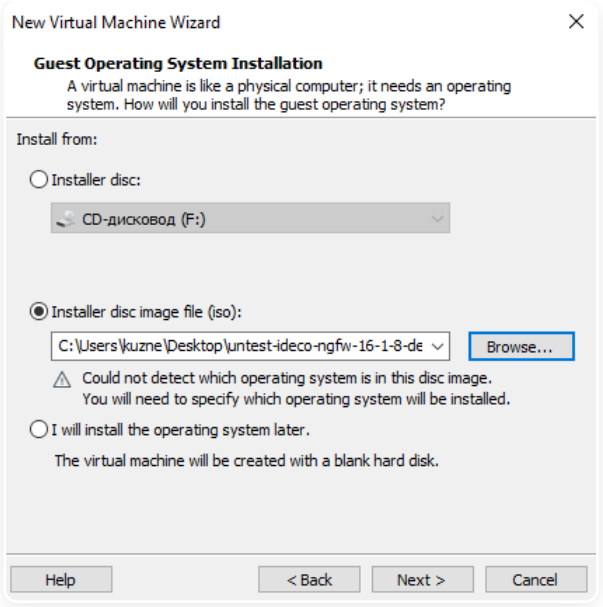
Перед установкой Ideco NGFW Novum:

- Увеличьте размер видеопамяти для виртуальной машины до 16 МБ.
- Используйте виртуальные сетевые адаптеры **vmxnet3**, **e1000e**.

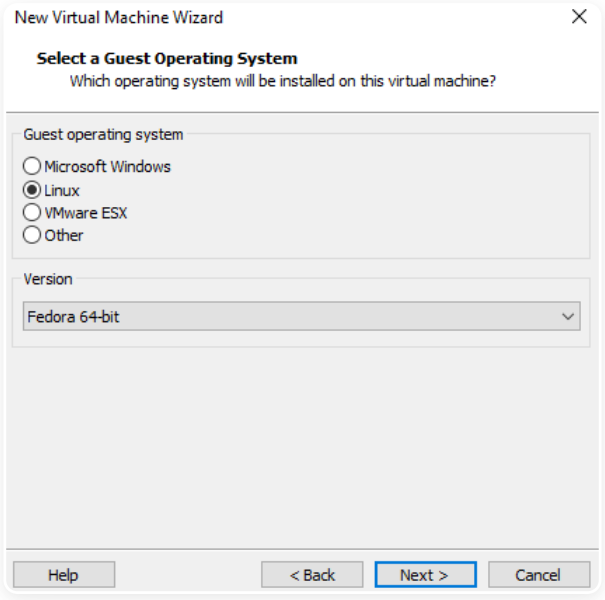
1. Создайте виртуальную машину, нажав **Create a New Virtual Machine**:



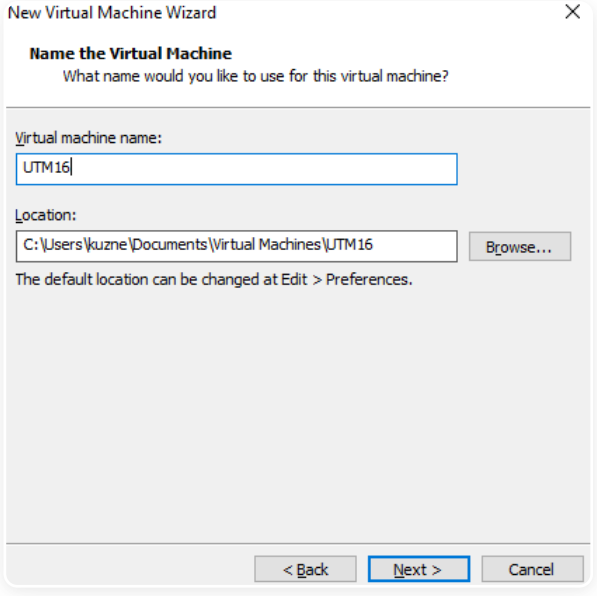
2. Укажите загрузочный ISO-образ:



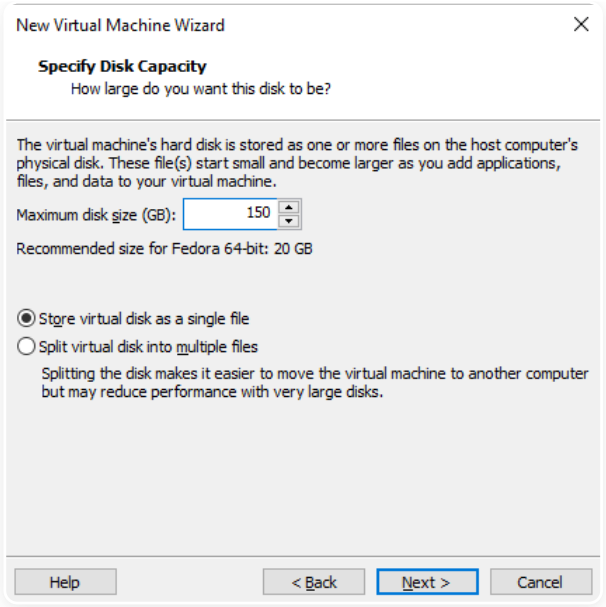
3. Выберите гостевую операционную систему **Linux** и в раскрывающемся списке укажите тип **Fedora 64-bit**:



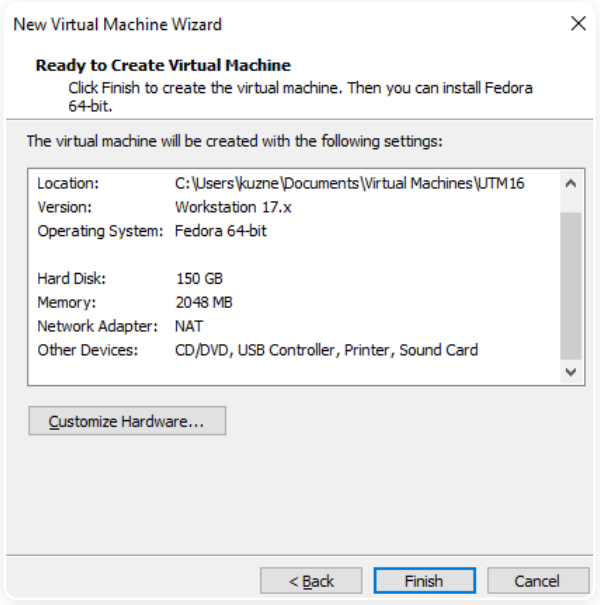
4. Укажите имя виртуальной машины и директорию для создания виртуального диска:



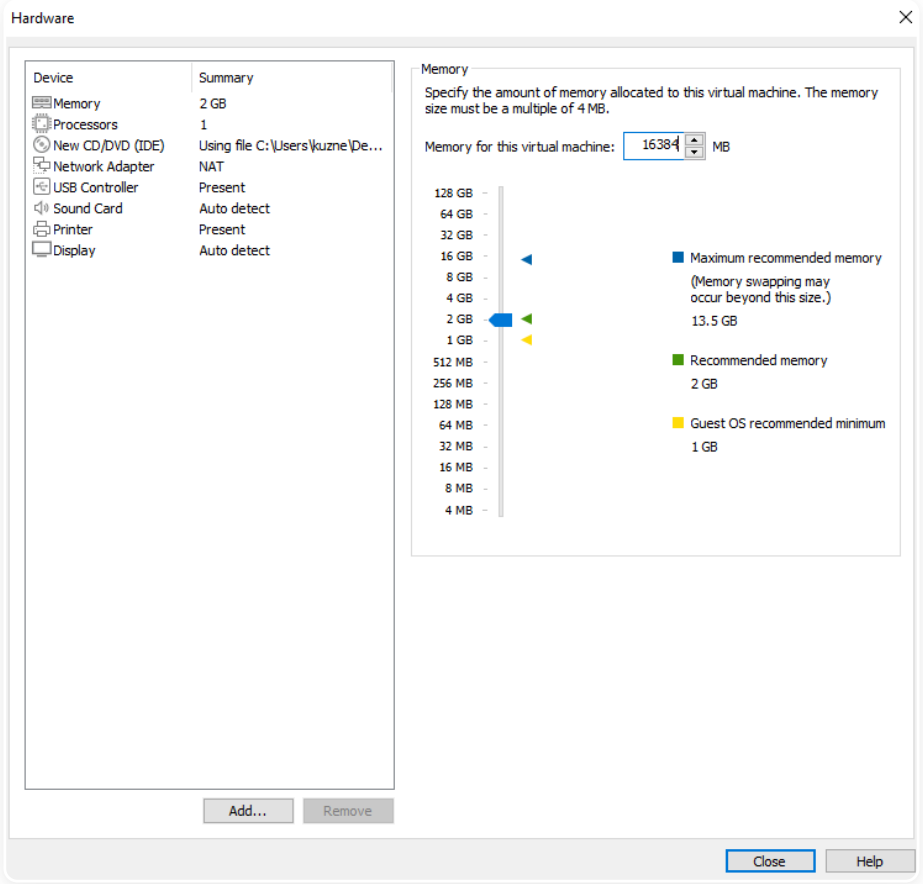
5. Укажите размер виртуального жесткого диска **150 ГБ**:



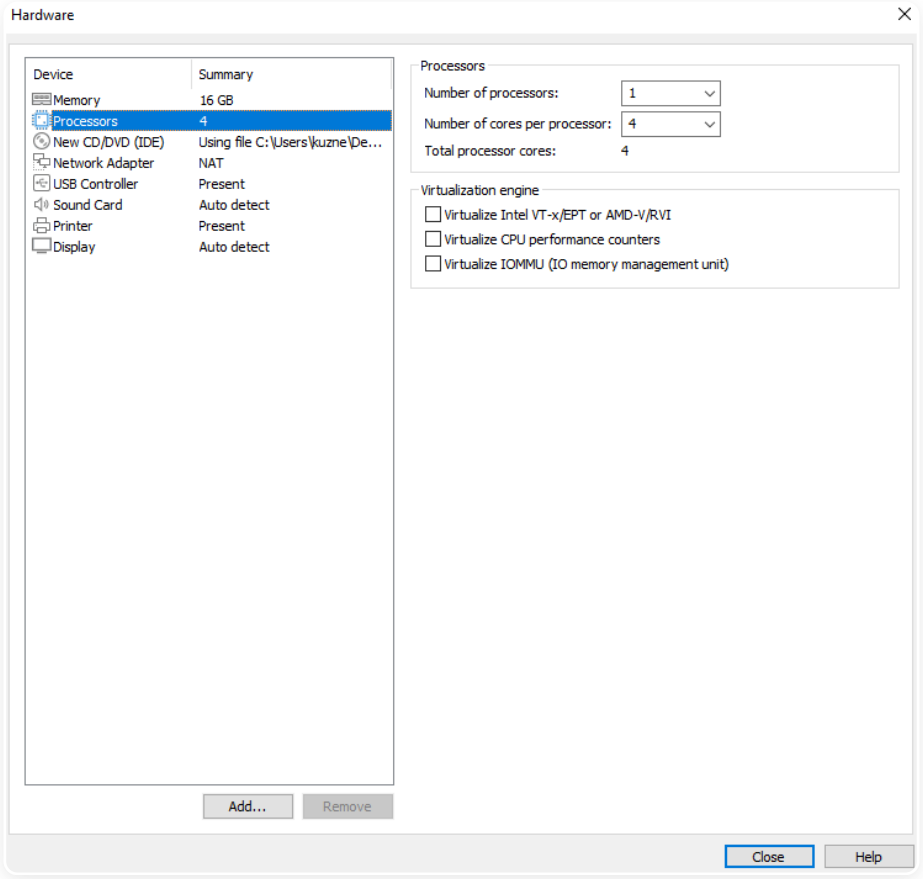
6. Выберите **Customize Hardware** для изменения настроек виртуальной машины:



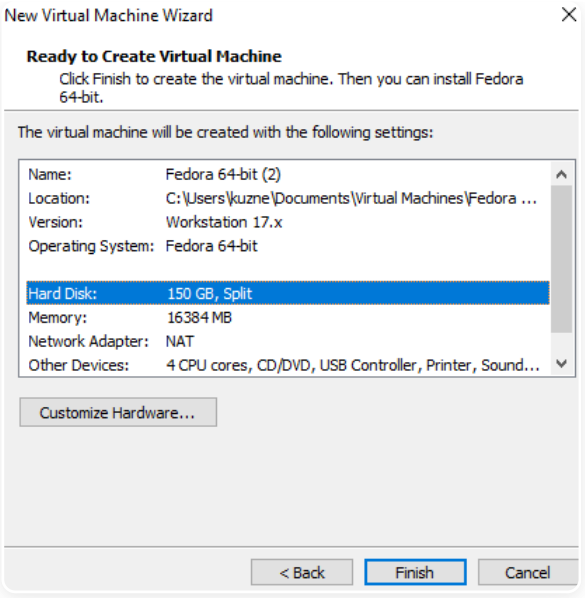
7. Укажите размер виртуальной оперативной памяти **16384 МБ**:



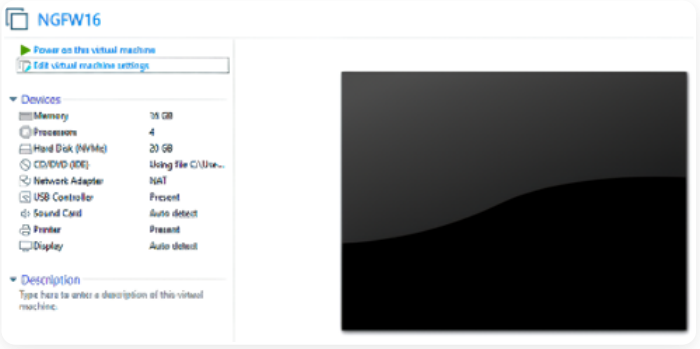
8. Укажите количество ядер процессора, равное 4:



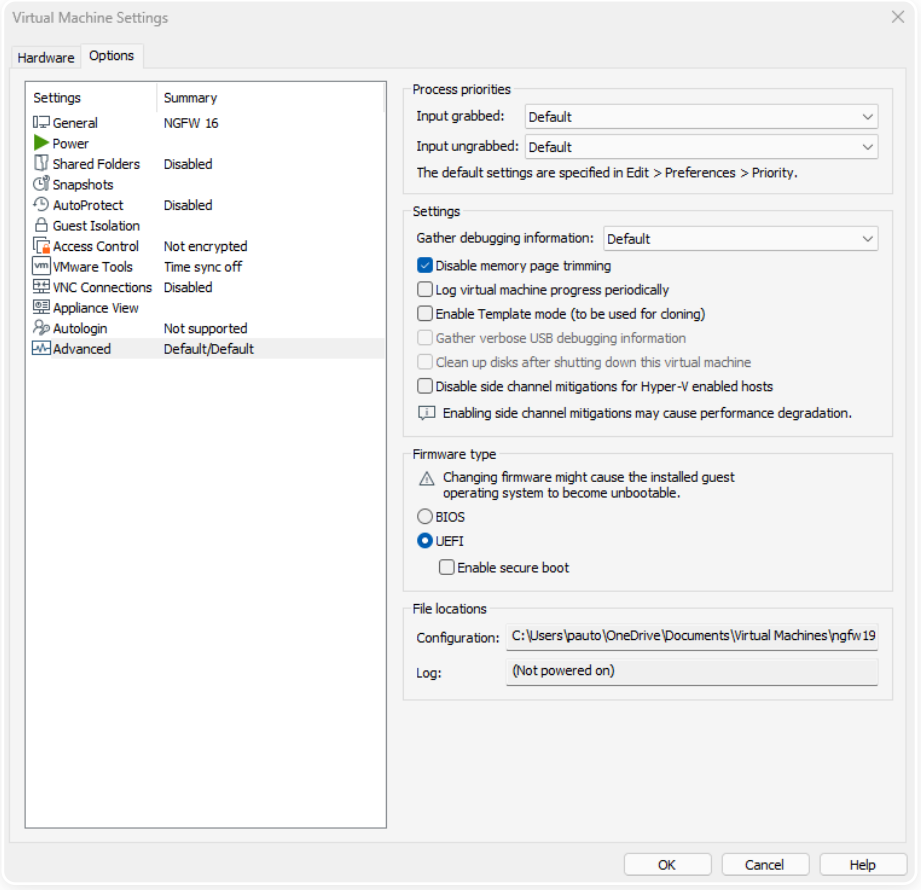
9. Выйдите из меню и нажмите **Finish** для окончания настройки:



10. Откройте окно виртуальной машины и нажмите **Edit virtual machine settings**:



11. Перейдите в **Options** → **Advanced** и активируйте опцию **Disable memory page trimming**. Установите для параметра **Firmware Type** значение **UEFI**:



- **Disable memory page trimming** - если опция выключена, гипервизор динамически распределяет доступную оперативную память между всеми виртуальными машинами.

12. Нажмите **OK** для завершения настройки виртуальной машины.

VirtualBox 7.0.12

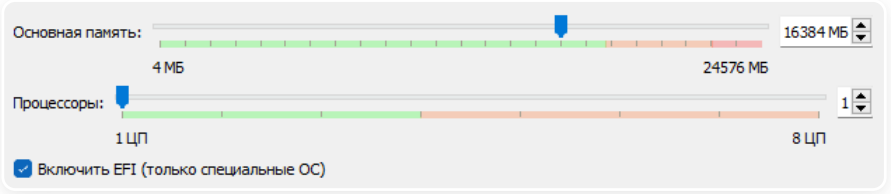
Настройка

> По умолчанию при создании виртуальной машины создается одна сетевая карта с типом подключения **NAT**.

1. Укажите **Имя** виртуальной машины (ВМ), выберите директорию для ВМ и установите путь до загрузочного образа NGFW Novum. Остальные параметры установите как на скриншоте:



2. Установите размер оперативной памяти ВМ (**16 ГБ**), количество ядер процессора **4** и нажмите **Включить EFI**:



3. Создайте виртуальный жесткий диск под ВМ (Объем не меньше **150 ГБ**):

4. Нажмите **Готово**.

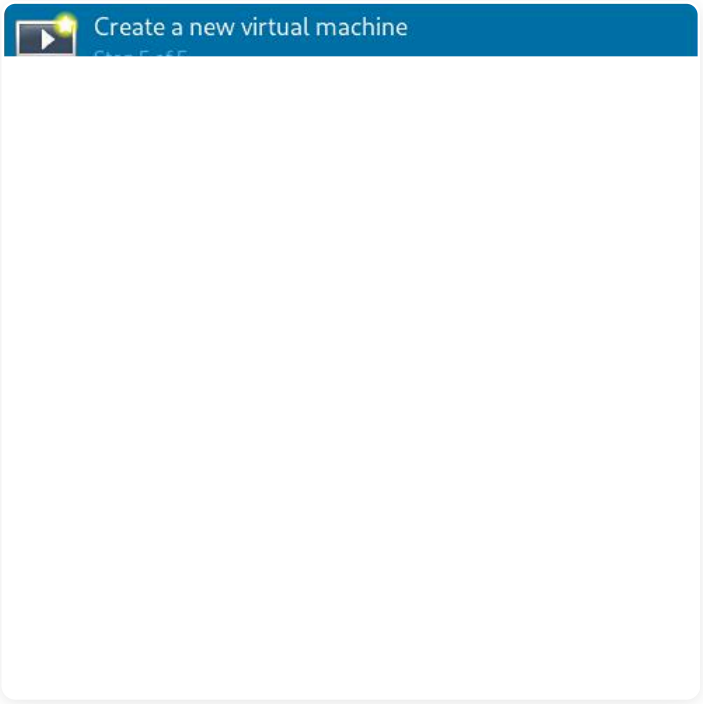
KVM

Настройка

> Минимальные требования к виртуальной машине описаны в статье.

1. При установке Ideco NGFW Novum выберите тип операционной системы - **Fedora**.

2. Включите опцию **Проверить конфигурацию перед установкой** и нажмите кнопку **Готово** на пятом шаге (virtm-manager) установки:



3. Измените интерфейс на **virtio** для дисков и сетевых карт. Изменить тип диска после создания ВМ нельзя.

4. Выберите режим кеширования. Если диски имеют формат qcow2 или raw, используйте **writeback**. Если используется другой формат дисков, проконсультируйтесь с системным администратором или с Технической поддержкой.

5. В появившемся окне на вкладке **Обзор** в поле **Firmware** выберите пункт **UEFI x86_64:/usr/share/OVMF/OVMF_CODE.fd**. Выбор этого пункта включит **UEFI** и выключит опцию **Secure Boot**:

Если пункта **UEFI x86_64:/usr/share/OVMF/OVMF_CODE.fd** нет в списке, доустановите пакет ovmf. В Ubuntu пакет ovmf устанавливается командой `sudo apt install ovmf`.

6. Перейдите в раздел **Memory** → **XML** и измените тег `<memballoon model='virtio'/>` на `<memballoon model='none'/>`, чтобы отключить **Memory Ballooning** и повысить производительность. При включенной опции гипервизор динамически распределяет доступную оперативную память между виртуальными машинами, из-за чего гостевая ОС может видеть больший объем памяти, чем фактически выделено.

Proxmox

Настройка

1. Нажмите **Создать ВМ**, включите опцию **Дополнительно** и введите имя машины:

2. В разделе **ОС** выберите хранилище и заполните поля:

- **ISO-образ** - образ с нужной версией NGFW Novum.
- **Гостевая ОС**:
  - **Тип** - Linux.
  - **Версия** - 6.x - 2.6 Kernel.

3. В разделе **Система** заполните поля:

- **Машина** - q35.
- **BIOS** - OVMF.
- **Хранилище EFI** - хранилище для UEFI-диска.
- **Агент QEMU** - включите опцию, чтобы операционная система могла передавать гипервизору информацию о своих внутренних состояниях.
- **Предварительная загрузка ключей** - отключите опцию.

4. В разделе **Диски** укажите нужный размер диска (не меньше 150 ГБ) и выберите хранилище для NGFW Novum:

- **Шина/Устройство** - VirtIO Block.
- **Отклонить** - включите опцию, если нужно сэкономить дисковое пространство. Она позволяет автоматически очищать освобожденные блоки на диске.

Проверьте свободное место на диске.

5. В разделе **Процессор** укажите количество сокетов и ядер (от четырех ядер) и выберите тип, который поддерживает SSE 4.2:

6. В разделе **Память** укажите объем оперативной памяти (не менее 16 ГБ):

- **Раздувание памяти** - отключите опцию для обеспечения максимальной производительности. При включенной опции гипервизор динамически распределяет доступную оперативную память между виртуальными машинами, из-за чего гостевая ОС может видеть больший объем памяти, чем фактически выделено.

7. В разделе **Сеть** в поле **Сетевой мост** выберите сетевой мост для локального интерфейса:

Рекомендуем отключить опцию **Сетевой экран**, чтобы облегчить настройку и отладку межсетевого экрана в Ideco NGFW Novum и избежать конфликтов обработки трафика.

8. В разделе **Подтверждение** проверьте заданные настройки и нажмите **Готово**:

Рекомендуем отключить опцию **Запуск после создания**, так как потребуется добавить еще одно сетевое устройство.

9. Для работы Ideco NGFW Novum также понадобится мост на сетевой интерфейс, чтобы получить доступ в интернет. Нажмите на созданную виртуальную машину, выберите **Оборудование** → **Добавить** → **Сетевое устройство** и добавьте мост, соответствующий выбранному ранее коммутатору:

Microsoft Hyper-V

Настройка

Сетевые адаптеры Hyper-V не поддерживаются в **Высокопроизводительном контексте**. Исправление планируется в будущих версиях.

Рекомендуем пробрасывать в виртуальную машину физическую сетевую карту на уровне PCI либо использовать эмуляцию сетевых адаптеров Intel (совместимость за счет снижения производительности).

- Поддерживается только второе поколение виртуальных машин под Windows Server 2012 R2 или выше.
- Отключите опцию **Secure Boot (Безопасная загрузка)**.
- Отключите опцию **Dynamic memory (Динамическая память)**.
- Используйте **Network Adapter (Сетевой адаптер)**.

Минимальные требования к виртуальной машине описаны в статье.

Шаги по установке Ideco NGFW Novum после создания загрузочного USB-накопителя можно прочитать в статье Установка.

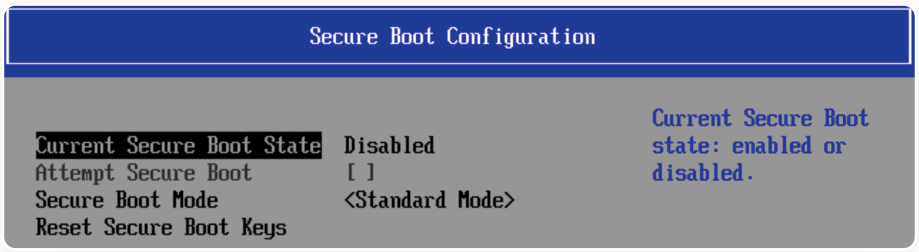
Для корректной работы кластерной сети, а также при использовании LACP-интерфейсов требуется дополнительная настройка на обеих нодах:

1. Перейдите в **Hardware** → **Network Adapter** → **Advanced Features** → **MAC address**.

2. Включите опцию **Enable MAC address spoofing**:

Включение режима совместимости процессора (Processor compatibility) может замедлить работу модуля **Предотвращение вторжений**:

При первом запуске в **BIOS** проверьте, что **Current Secure Boot State** в состоянии **Disabled**:



Полезные ссылки

- **Настройка LACP на Hyper-V**

Создание загрузочного USB-накопителя

При записи ISO-образа вся информация с USB-накопителя будет удалена.

Windows

С помощью программы Rufus

1. Проверьте целостность образа в PowerShell. Хеш-сумма должна совпадать с той, что указана в MY.IDECO → NGFW → Скачать:

```
((Get-FileHash <путь к загрузочному образу> -Algorithm SHA256).hash) -eq "<хеш-сумма>"
```

2. Скачайте программу Rufus и запустите скачанный файл.

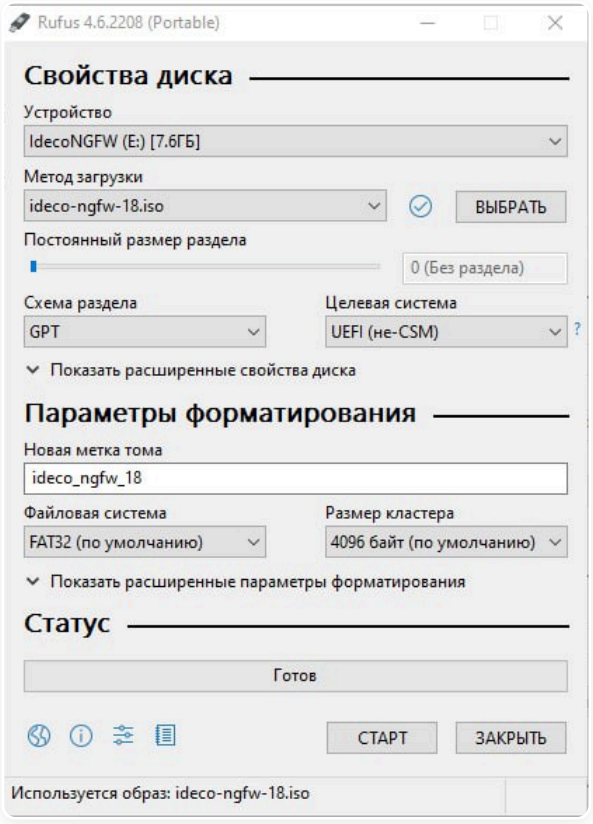
3. Выберите нужный USB-накопитель в пункте **Устройство**.

4. Выберите метод загрузки **Диск или ISO-образ**.

5. Нажмите на кнопку **Выбрать** и откройте скачанный образ Ideco NGFW Novum.

6. Нажмите **Старт** и в появившемся окне выберите пункт **Запись в режиме DD-образ**.

7. В диалоговом окне подтвердите запись:



С помощью программы Win32diskimager

1. Проверьте целостность образа в PowerShell. Хеш-сумма должна совпадать с той, что указана в MY.IDECO → NGFW → Скачать:

```
((Get-FileHash <путь к загрузочному образу> -Algorithm SHA256).hash) -eq "<хеш-сумма>"
```

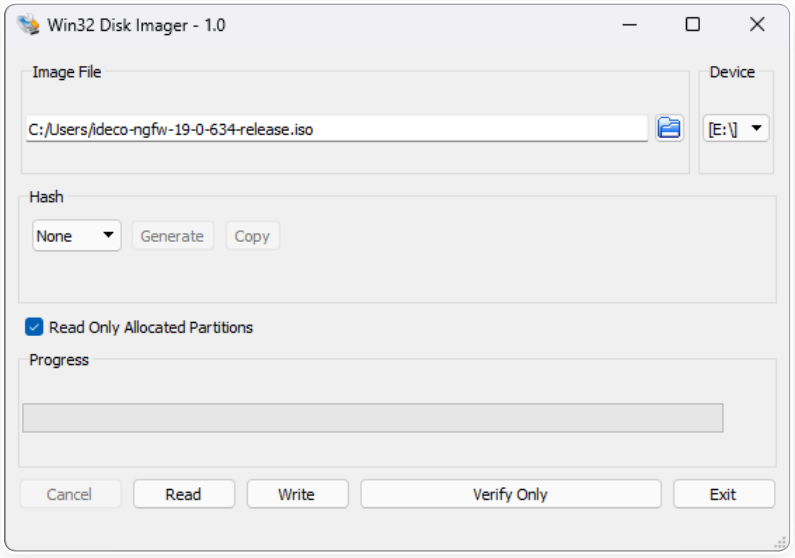
2. Установите программу Win32diskimager и запустите.

3. Нажмите на значок синей папки и выберите ISO-файл, который хотите записать.

По умолчанию все отображаемые файлы в проводнике Windows имеют формат `.img`. Для записи ISO-файла выберите опцию отображения всех файлов в правом нижнем углу.

4. Выберите нужный USB-накопитель рядом с файлом образа.

5. Нажмите **Write** и в появившемся окне подтвердите запись:



Linux

Для создания загрузочного USB-накопителя можно использовать не только терминал, но и программу gnome-disks.

Создание загрузочного накопителя через терминал

1. Проверьте целостность образа. Хеш-сумма должна совпадать с той, что указана в MY.IDECO → NGFW → Скачать:

```
echo "<хеш-сумма>  <путь к загрузочному образу>" | sha256sum -c
```

Пример:

```
echo "bc35a46507908c82ad3b8b75f4bb4f71f21f6d8012ad486aabbbb9a487108400 ideco-ngfw-21-4-26-release.iso" | sha256sum -c
```

2. Найдите USB-носитель в системе:

```
lsblk --nodeps  -o name,size,fstype,tran,model,mountpoint /dev/sd*
```

Вывод:

```
NAME  SIZE FSTYPE TRAN MODEL        MOUNTPOINT
sdx   7,5G        usb  USB_DISK_3.0
sdx1  7,5G vfat                     /run/media/ideco/D661-82E2
```

3. Размонтируйте файловую систему:

```
sudo umount <точка монтирования>
```

Пример:

```
sudo umount /run/media/ideco/D661-82E2
```

4. Запишите образ на носитель:

```
sudo dd if=<путь к загрузочному образу> of=<имя устройства> bs=1M oflag=direct status=progress conv=fdatasync
```

Пример:

```
sudo dd if=/home/ideco/ideco-ngfw-21-4-26-release.iso of=/dev/sdx bs=1M oflag=direct status=progress conv=fdatasync
```

5. Подготовьте носитель к извлечению:

```
sudo eject <имя устройства>
```

Пример:

```
sudo eject /dev/sdx
```

Шаги по установке Ideco NGFW Novum после создания загрузочного USB-накопителя можно прочитать в статье Установка.

Установка

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE



Процесс установки

При установке Ideco NGFW Novum с загрузочного USB-диска выберите загрузку с USB-диска в настройках UEFI сервера.

Если при установке Ideco NGFW Novum появилась ошибка **Требуется не менее 16 ГБ оперативной памяти** и при этом указан рекомендуемый размер оперативной памяти, необходимо уменьшить размер ресурсов, выделенных под видеопамять.

Для установки Ideco NGFW Novum выполните действия:

1. Перейдите к установке, нажав **Install Ideco NGFW Novum**:

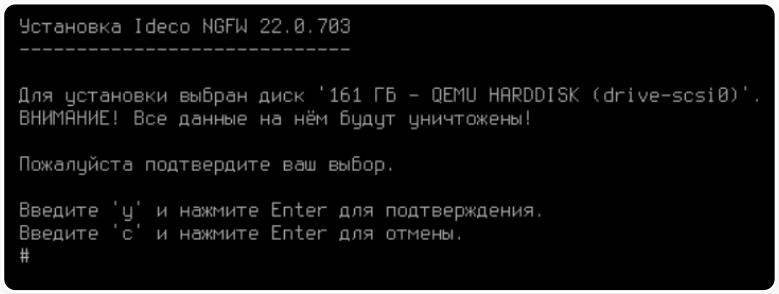


При установке или загрузке сервера Ideco NGFW Novum не рекомендуем нажимать на клавиатуре:

- `-` - нажатие кнопки уменьшает количество секунд в тайм-ауте и может привести к отключению таймера.
- `+` - нажатие кнопки увеличивает количество секунд в тайм-ауте.

При отключении таймера ознакомьтесь со статьей **Как включить таймер при загрузке Ideco NGFW Novum**.

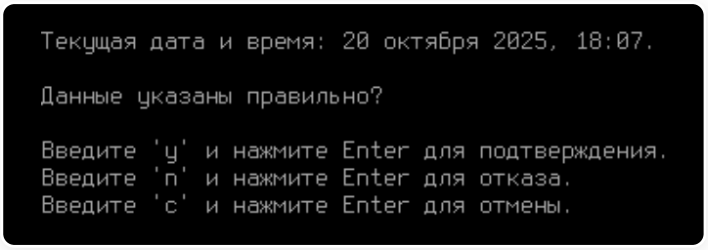
2. Выберите диск и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой находится сервер:

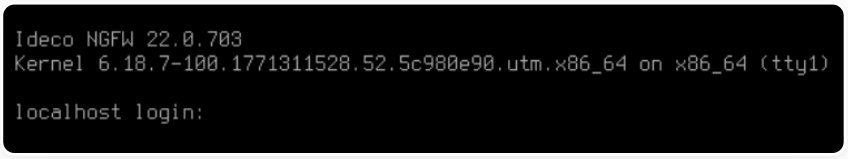


4. **Обязательно проверьте правильность даты и времени.** При необходимости настройте дату и время в соответствии с временной зоной сервера:



Извлеките USB-диск после установки Ideco NGFW Novum, чтобы загрузка с него не началась заново.

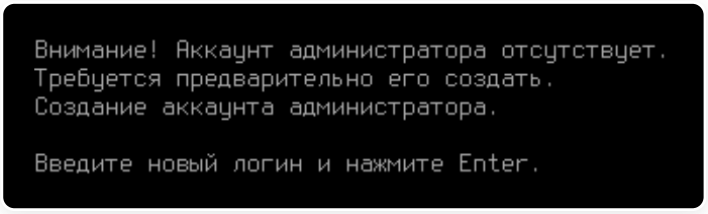
5. Не нажимайте никаких клавиш при появлении окна:



После загрузки система автоматически перейдет к локальному интерфейсу Ideco NGFW Novum.

Создание учетной записи администратора

Создайте учетную запись администратора после уведомления **Создание аккаунта администратора**:



Требования к логину и паролю

Логин:

- Не должен начинаться с цифры.
- Не должен содержать специальных и пробельных символов, кроме дефиса `-`.
- **Длина логина** - от 1 до 31 символа включительно.

Пароль:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.

- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

Если пароль не соответствует требованиям политики безопасности, то появится надпись с информацией, что пароль ненадежен. Потребуется ввести новый пароль с учетом требований к нему.

Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как управляющие символы: `^[[2~;` , `^[[4~;` и так далее.

Настройка интерфейса управления

С версии 21 Ideco NGFW Novum у интерфейсов появились роли:

Control Plane

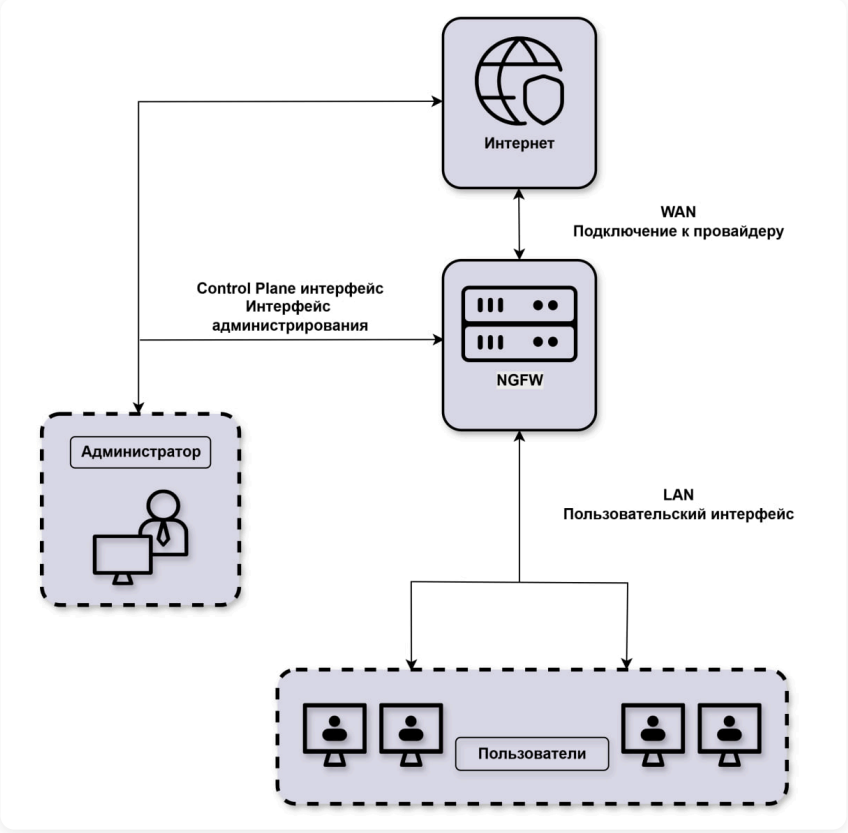
Используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза.

Для доступа пользователей в сеть через NGFW Novum подключайте их к интерфейсу с типом LAN.

Если CP-интерфейс не имеет выхода в интернет, необходимо дополнительно настроить WAN-интерфейс через веб-интерфейс.

Интерфейс Control Plane не обязателен - для администрирования может использоваться LAN-интерфейс.

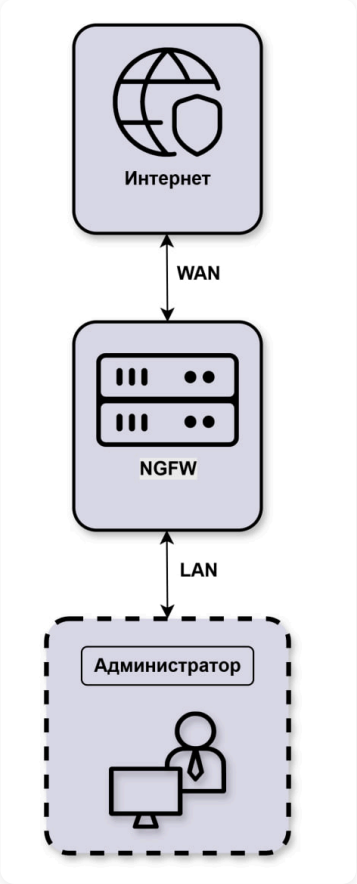
Схема сети с CP-интерфейсом:



LAN

Используется для создания локальных интерфейсов и администрирования NGFW Novum.

Схема сети с LAN-интерфейсом:



WAN

Используется для подключения к провайдеру. WAN-интерфейс для пользовательского трафика настраивается через веб-интерфейс (подробнее - в статье Первоначальная настройка).

При использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса.
Для корректной идентификации сетевой карты используйте MAC-адрес сетевой карты.

Для настройки Ideco NGFW Novum через веб-интерфейс настройте соответствующий интерфейс в локальном меню.

1. Перейдите в раздел **Ethernet-интерфейсы** → **Создать интерфейс**:

```
Управление сервером

1. Консоль
2. Физические порты
3. Ethernet-интерфейсы
4. Отключить все статические маршруты и добавить новый
5. Выбор типа кластерной сети
6. Включить доступ к веб-интерфейсу из внешней сети
7. Включить доступ к серверу по SSH из Интернет
8. Включить доступ к серверу по SSH из локальных сетей
9. Включить режим `Разрешить Интернет всем`
10. Сбросить блокировки по IP
11. Отключить пользовательский межсетевой экран
12. Создать новый бэкап
13. Восстановить из бэкапа
14. Мгновенно восстановить из бэкапа
15. Включить доступ Удаленного Помощника
16. Контакты технической поддержки
17. Восстановиться на предыдущую версию
18. Перезагрузка сервера
19. Отключить сервер
20. Выход

Введите номер пункта и нажмите Enter.
# 3

1. Показать список интерфейсов
2. Включить/Отключить интерфейс
3. Создать интерфейс
4. Изменить интерфейс
5. Удалить интерфейс
```

2. Выберите порт для доступа к веб-интерфейсу:

```
Выберите порт:

-------------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------------
  1    |  eth0_ff  |  bc:24:11:96:55:ff  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  2    |  eth1_c9  |  bc:24:11:26:e3:c9  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  3    |  eth2_e5  |  bc:24:11:9a:ca:e5  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
```

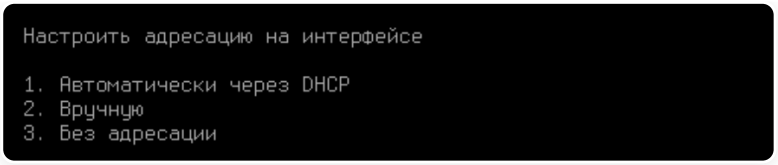
3. Введите имя интерфейса и выберите роль:

```
Введите имя интерфейса (или оставьте пустым) и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# CP

Выберите роль для интерфейса:

1. CP
2. LAN
3. WAN
```

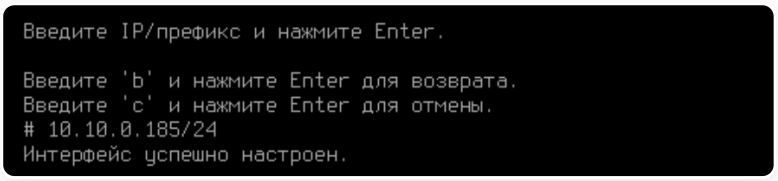
4. Выберите **Системный контекст**:

```
Выберите VCE:

1. Системный контекст
```

5. Настройте локальную сеть **Автоматически через DHCP** или **Вручную**:



6. Если выбрали **Вручную**, введите локальный IP-адрес и маску подсети в формате `ip/маска` и нажмите **Enter**:



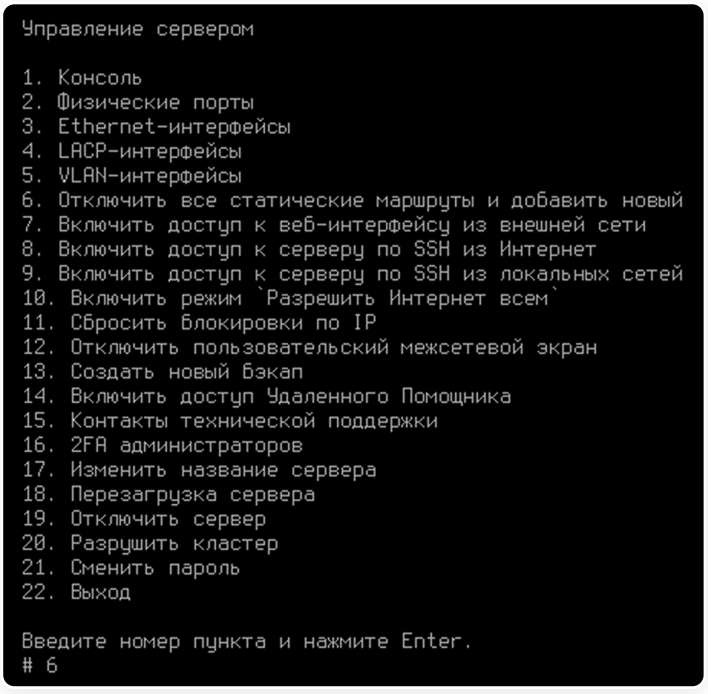
Настройка маршрутов на NGFW Novum для доступа из другой сети

В локальном меню можно настроить статическую маршрутизацию для первичного доступа к веб-интерфейсу, а также в аварийных ситуациях (только через консоль).

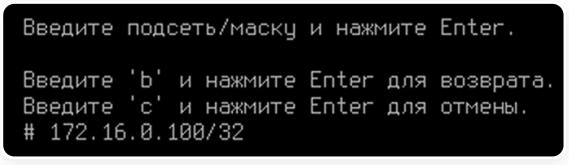
Например, настроен интерфейс `10.10.0.185/24`. Чтобы настроить маршрут до компьютера администратора с IP-адресом `172.16.0.100`, выполните действия:

1. Вернитесь в главное меню, нажав `c`.

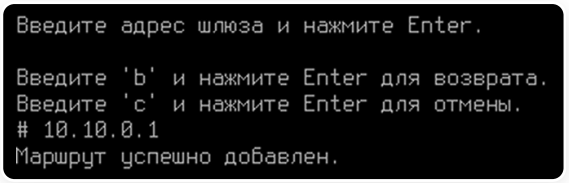
2. Выберите **Отключить все статические маршруты и добавить новый**:



3. Укажите подсеть `172.16.0.100/32`:



4. Введите IP-адрес шлюза:



После этого появится доступ к веб-интерфейсу NGFW Novum.

Можно настроить маршрут по умолчанию для доступа к NGFW Novum из другой сети. Для этого:

1. Укажите подсеть `0.0.0.0/0` - маршрут по умолчанию:

2. Введите IP-адрес шлюза:

```
Введите адрес шлюза и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# 10.10.0.1
Маршрут успешно добавлен.
```

7. После настройки интерфейса можно перейти в веб-интерфейс. Подробная информация о первоначальной настройке в статье.

Если в Ideco NGFW Novum настроен кластер, в локальном меню будет отсутствовать пункт **Восстановиться на предыдущую версию**.

Полезные ссылки

- **Установка Ideco NGFW Novum через COM-порт**

Подключение к Ideco NGFW Novum по COM-порту

Установка Ideco NGFW Novum по COM-порту

COM-порт по умолчанию включен.

Для установки Ideco NGFW Novum через COM-порт на серверы без мониторов и IPMI выполните шаги:

Шаг 1. Создание загрузочного USB-накопителя

Создайте загрузочный USB-накопитель Ideco NGFW Novum. Воспользуйтесь статьей.

Шаг 2. Подготовка BIOS

Этот шаг можно пропустить, если:

- Опция **Console Redirection** включена.
- Опция **SecureBoot** отключена.
- Опция **Hyper-Threading (Intel)** или **SMT (AMD)** отключена, если используется **Высокопроизводительный** контекст.
- Не требуется выбирать загрузочное устройство (BIOS поддерживает загрузку с USB-накопителя по умолчанию).

Если BIOS поддерживает опцию **Console Redirection to Serial Port**, включите ее. Опция находится в разделах, связанных с **Serial Port** или **Supervisor**, и позволяет контролировать процесс установки через COM-порт, начиная с экрана BIOS.

При отсутствии поддержки **Console Redirection to Serial Port** может потребоваться подключение монитора к серверу.

Проведите подготовку BIOS:

1. Выберите USB-накопитель устройством загрузки по умолчанию.
2. Отключите **SecureBoot**.
3. Если используете **Высокопроизводительный** контекст, отключите технологии:

- **Hyper-Threading (Intel)**.
- **SMT (AMD)**.

Шаг 3. Подключение через COM-порт

1. Отключите питание сервера.

2. Подключите компьютер к консольному порту с помощью консольного кабеля.

3. Установите на компьютер программу **PuTTY** или аналогичные утилиты, такие как **tio** или **MobaXterm**, чтобы подключиться к консольному порту.

4. Проверьте, что в используемой утилите заданы параметры:

- **Speed (baud)** - 115200.
- **Data bits** - 8.
- **Stop bits** - 1.
- **Flow control** - XON/XOFF.
- **Terminal-type (или Emulation)** - ANSI.

Пример настройки утилиты PuTTY

1. Перейдите в раздел **Connection** → **Serial** → **Configure the serial line** и укажите значения:

- **Speed (baud)** - 115200.
- **Data bits** - 8.
- **Stop bits** - 1.

- **Flow control** - XON/XOFF.
- **Serial line to connect to**:
  - **Windows** - укажите порт в формате `COMx`, где `x` - номер порта в системе. Например, `COM1`. Чтобы узнать номер порта, откройте **Диспетчер устройств** и найдите раздел **Порты (COM и LPT)**.
  - **Linux** - укажите путь к устройству в формате `/dev/ttyXXXX`. Например, `/dev/ttyUSB0`. Для вывода списка доступных устройств используйте команду `ls /dev/tty`.
  - **macOS** - укажите путь к устройству в формате `/dev/tty.usbserial-XXXXXX`. Например, `/dev/tty.usbserial-DB008OZL`. Для вывода списка доступных устройств используйте команду `ls -l /dev/*usbserial*`.

2. Перейдите в раздел **Connection** → **Data** → **Terminal details** и введите в поле **Terminal-type string** параметр **ANSI**:

3. Нажмите **Open**.

Шаг 4. Процесс установки

1. Запустите терминал, вставьте загрузочный USB-накопитель и включите сервер.

> Через некоторое время после включения на экране терминала отобразится:
>
> - Установщик Ideco NGFW Novum, если опция **Console Redirection** отсутствует в BIOS или выключена.
> - Процесс загрузки сервера, начиная с BIOS и заканчивая установщиком Ideco NGFW Novum, если опция **Console Redirection** включена.

2. Выполните установку Ideco NGFW Novum.

Управление Ideco NGFW Novum по COM-порту

Если подключение по COM-порту ранее не настраивалось, выполните шаги 2 и 3 из инструкции выше. После подключения вы сможете управлять Ideco NGFW Novum через COM-порт посредством локального меню.

Возможные проблемы

Проблема	Возможная причина	Решение
На экране терминала пусто	Не подключен кабель	Подключите кабель COM-порта к серверу
На экране терминала пусто, кабель подключен	Поздно подключен кабель	Нажмите `Ctrl+R` в локальном меню, чтобы обновить дашборд
Не отображается BIOS через COM-порт	BIOS не поддерживает опцию **Console Redirection to Serial Port**	Подключитесь к серверу напрямую
Не отображается BIOS через COM-порт	В BIOS отключена опция **Console Redirection to Serial Port**	Включите опцию **Console Redirection to Serial Port**

Как включить таймер при загрузке Ideco NGFW Novum?

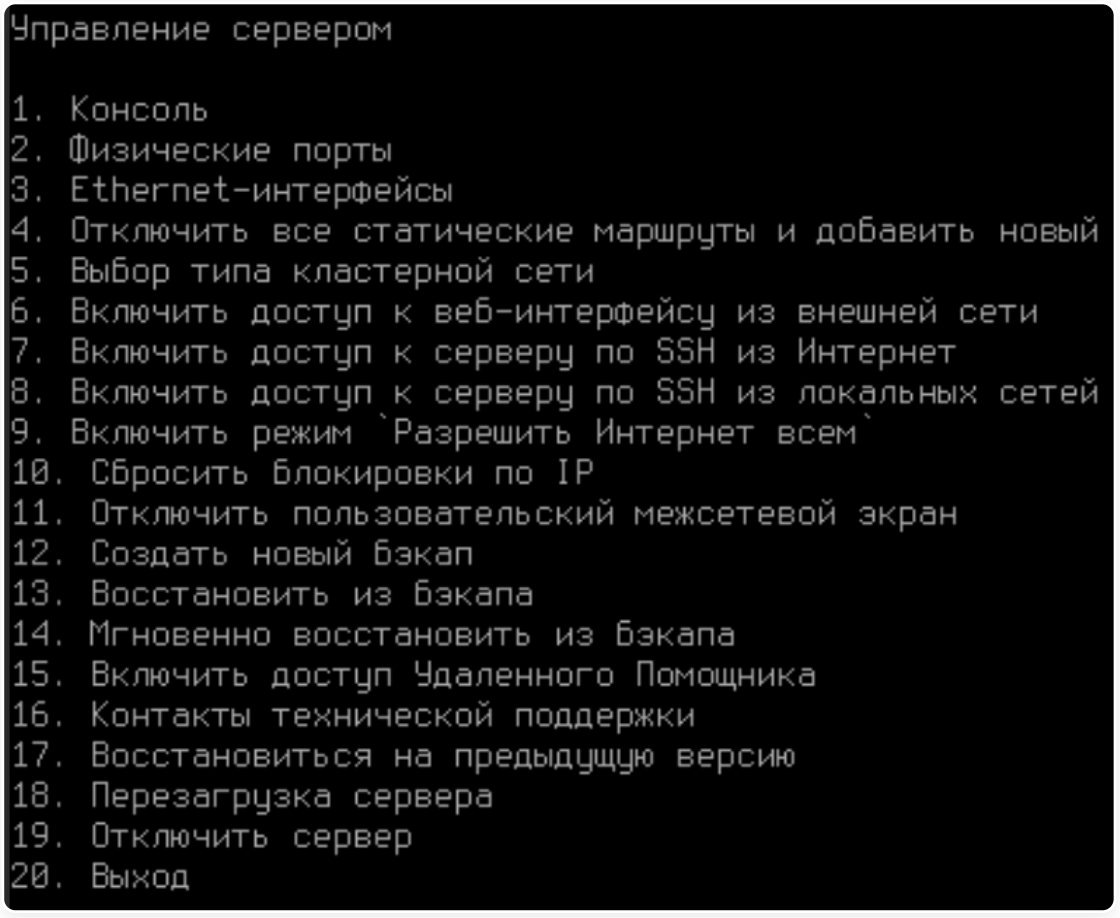
При отключении таймера также отключается автоматический выбор пункта меню. В этом случае система не загрузится сама после обновления, рестарта или переключения ноды в режиме кластеризации до момента нажатия **Enter**.

Для включения таймера выполните действия:

1. При загрузке сервера выберите Ideco NGFW Novum, нажав **Enter**:



2. Дождитесь загрузки, перейдите в локальное меню и выберите **Перезагрузка сервера**:



3. При загрузке сервера выберите необходимое количество секунд в тайм-ауте, нажав **+** на клавиатуре:



4. Подтвердите выбор, нажав **Enter**.

Первоначальная настройка

Перед началом настройки рекомендуем создать бэкап, который позволит восстановить первоначальные настройки в случае необходимости.

Подключение к веб-интерфейсу Ideco NGFW Novum

1. Запустите на любом компьютере в сети интерфейса Control Plane или LAN поддерживаемый браузер (современные версии Firefox, Chrome и браузеров, основанных на Chromium). Подробнее про особенности интерфейсов - в статье.

2. Введите в адресной строке IP-адрес, указанный при настройке интерфейса, и порт 8443.

Пример: `192.168.100.2:8443`

При переходе к учетной записи в браузере отобразится предупреждение безопасности. Необходимо подтвердить подключение, войти в веб-интерфейс и установить сертификат, чтобы исключить появление предупреждения.

3. Введите логин и пароль от учетной записи, созданной при установке Ideco NGFW Novum.

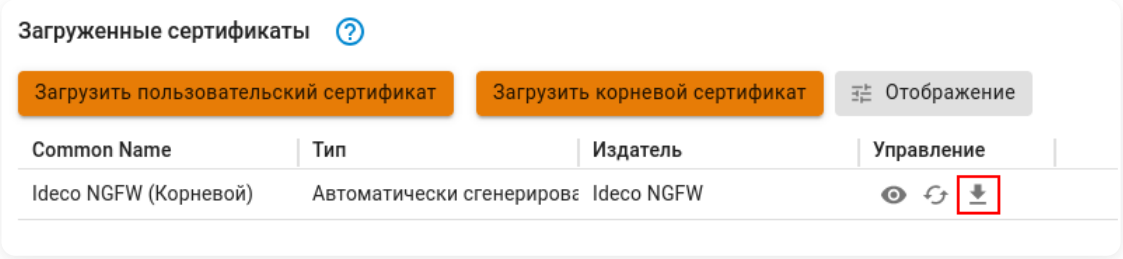
Импорт корневого сертификата Ideco NGFW Novum

Для устранения предупреждения в браузере при входе в веб-интерфейс импортируйте корневой сертификат Ideco NGFW Novum и добавьте в доверенные корневые центры сертификации устройства:

1. Скачайте сертификат одним из способов:

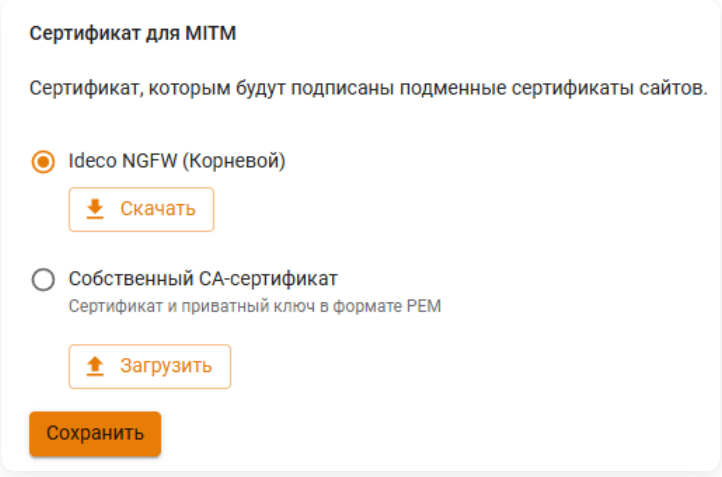
Из раздела Сервисы

В **Сервисы** → **Сертификаты** → **Загруженные сертификаты** нажмите на стрелку для скачивания:



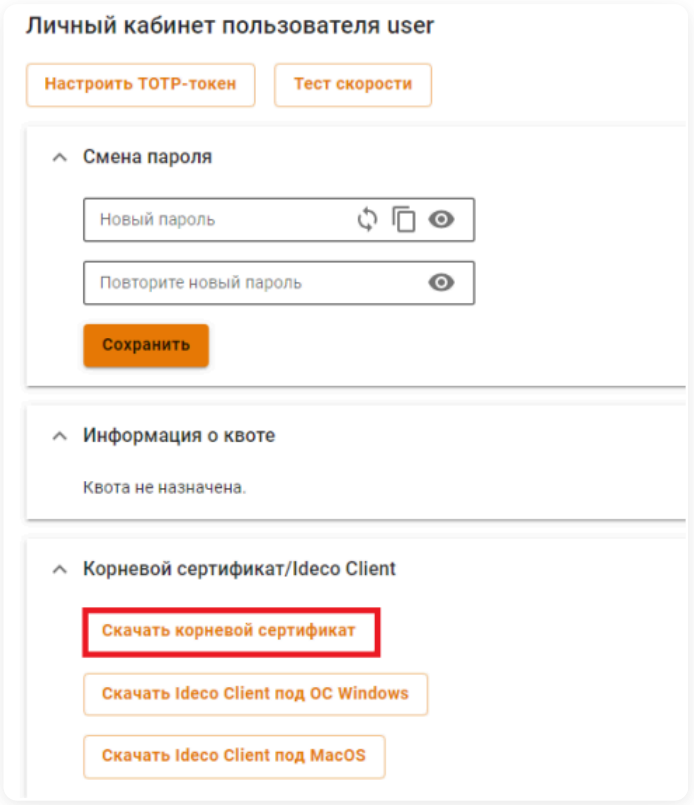
Из раздела Правила трафика

В **Правила трафика** → **Контент-фильтр** → **Настройки** нажмите **Скачать**:



Из личного кабинета пользователя

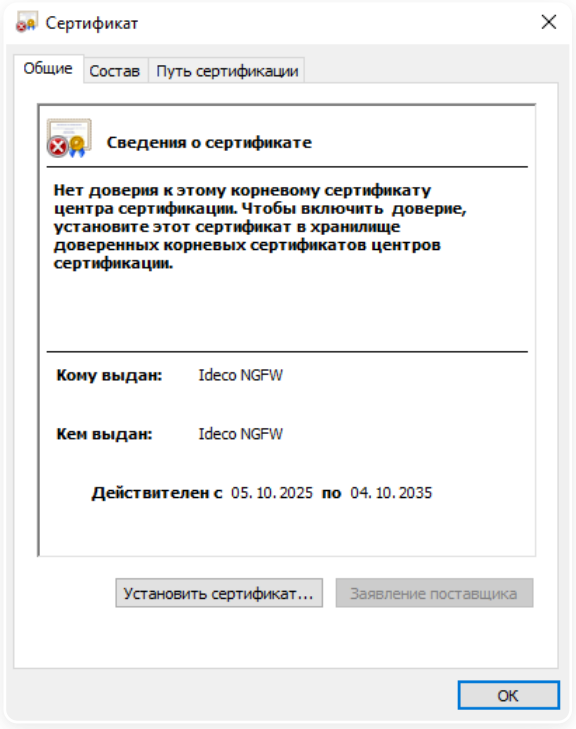
В личном кабинете Ideco NGFW Novum под учетной записью одного из пользователей перейдите на вкладку **Корневой сертификат/Ideco Client** и нажмите **Скачать корневой сертификат**:



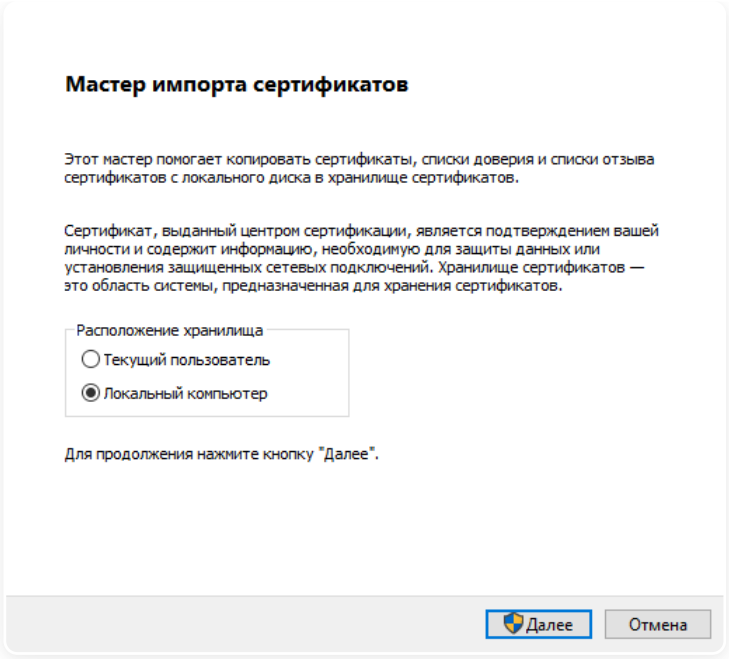
Для публикации личного кабинета пользователя воспользуйтесь статьей.
2. Импортируйте корневой сертификат.

Пример для Windows

1. Откройте скачанный сертификат и нажмите **Установить сертификат**:

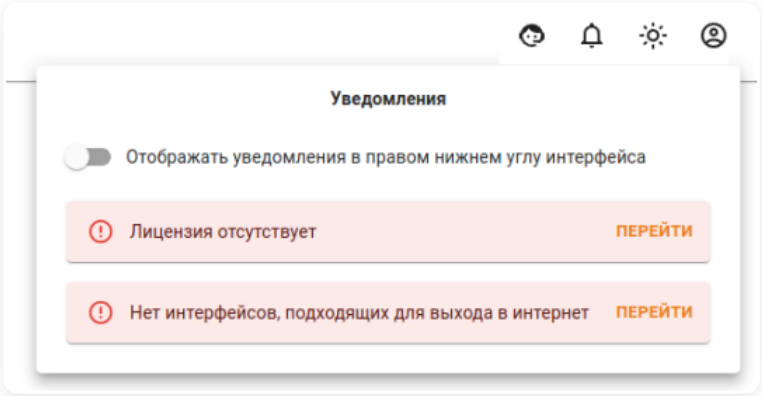


2. Выберите расположение хранилища **Локальный компьютер**:



3. Установите сертификат в **Доверенные корневые центры сертификации**:

После первого входа в веб-интерфейс появятся уведомления, которые помогут настроить подключение к провайдеру и зарегистрировать сервер для корректной работы Ideco NGFW Novum:

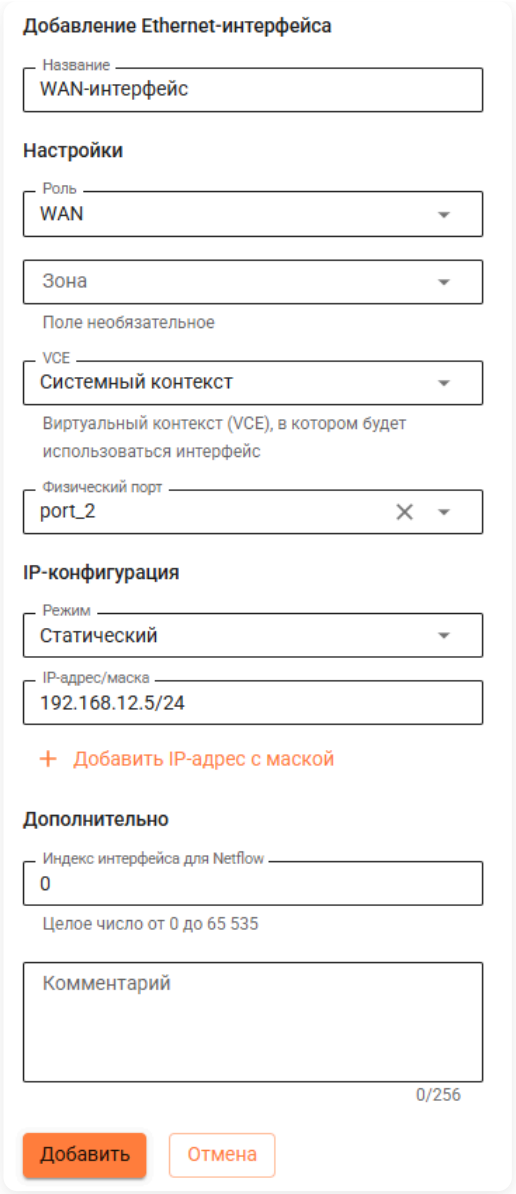


Настройка WAN-интерфейса

Если вы настроили интерфейс (Control Plane или LAN) и у него нет доступа в интернет, настройте WAN-интерфейс, чтобы получить лицензию. Выполните действия:

1. Перейдите в **Сервисы** → **Сетевые интерфейсы**, нажмите **Добавить** и выберите пункт **Ethernet**.

2. Заполните поля:



- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - выберите WAN.
- **Физический порт** - порт на сетевом адаптере, который будет использоваться в созданном интерфейсе.
- **Режим** - выберите Статический и укажите IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.

3. Нажмите **Добавить**. WAN-интерфейс появится в таблице интерфейсов.

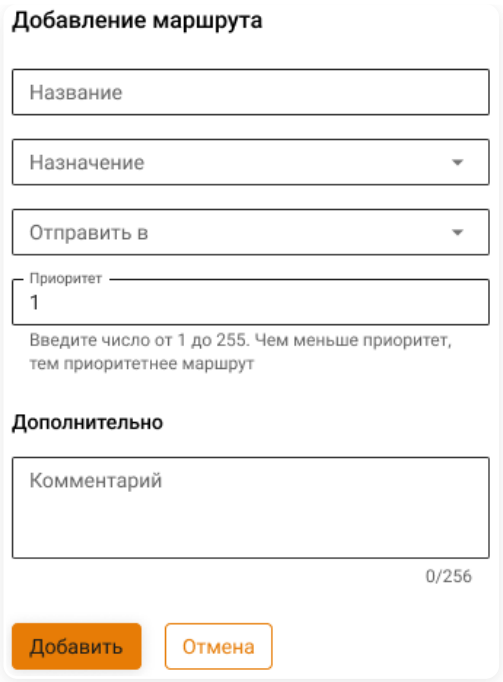
Настройка подключения к провайдеру

Настройте шлюз для WAN-интерфейса, выполнив действия:

Маршрутизация

1. Перейдите в **Маршрутизация** → **Статическая** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

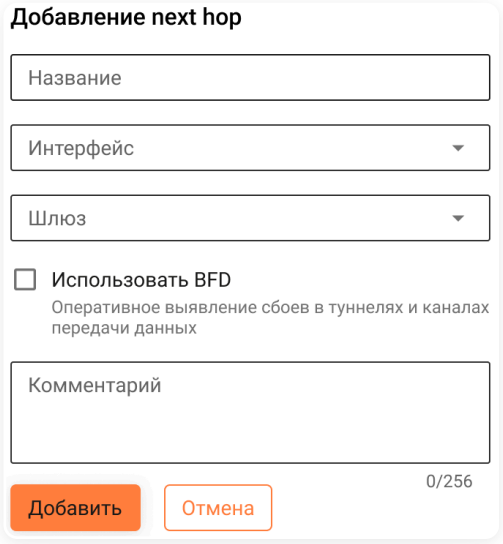


- **Название** - укажите название правила.
- **Назначение** - выберите **Любой**.
- **Отправить в** - введите IP-адрес шлюза.

SD-WAN

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

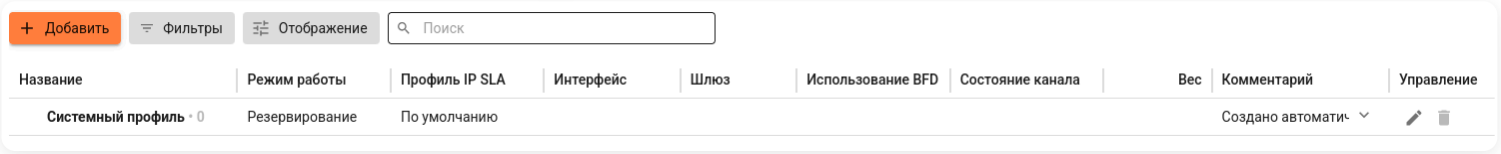


- **Название** - укажите название.
- **Интерфейс** - выберите созданный интерфейс.
- **Шлюз** - укажите IP-адрес следующего узла маршрутизации (next hop), на который будет направляться трафик. Адрес шлюза должен находиться в сети выбранного интерфейса.
- **Использовать BFD** - включите опцию, если поддержка BFD включена на стороне указанного шлюза.

При выборе интерфейса, который получает IP-адрес по DHCP:

- Если оставить поле **Шлюз** пустым, то будет использован шлюз, полученный от DHCP-сервера.
- Если в поле **Шлюз** указать IP-адрес, то в качестве шлюза будет использоваться указанный IP-адрес, а полученный от DHCP-сервера проигнорируется.

3. Перейдите в раздел **Профили Next hop** и нажмите для редактирования **Системного профиля**:



4. Перейдите на вкладку **Next hop**, нажмите **Выбрать next hop** и выберите next hop, созданный на шаге 2.

5. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

После настройки шлюза зарегистрируйте сервер. Подробная информация в статье.

Чтобы получить доступ в интернет и настроить авторизацию, выполните действия. В противном случае доступ в интернет для устройства с установленным Ideco NGFW Novum будет заблокирован.

Настройка других типов подключений

Если провайдер использует другой тип подключения, ознакомиться с остальными инструкциями по настройке можно по ссылкам:

- Сетевые интерфейсы.
- Одновременное подключение к нескольким провайдерам.

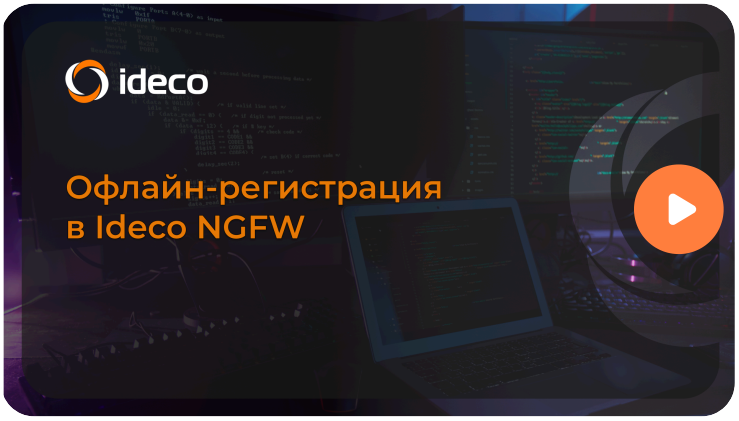
Регистрация сервера

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE



Для активации лицензии необходима обязательная регистрация сервера в MY.IDECO.

NGFW Novum без лицензии по умолчанию не пропускает трафик пользователей в интернет. Для получения лицензии используйте альтернативный (дополнительный) шлюз. Если это невозможно, временно включите опцию **Полный доступ** - для этого перейдите в раздел **Техническая поддержка**, нажав в правом верхнем углу экрана. Подробнее - в статье.

Перед активацией лицензии убедитесь, что в NGFW Novum установлены корректные дата и время, иначе подключиться к серверу лицензирования не получится. Для установки даты и времени воспользуйтесь статьей.

Выберите удобный способ получения лицензии:

- Через **онлайн-регистрацию**.
- Через **офлайн-регистрацию**. Компьютеру администратора должен быть обеспечен собственный выход в интернет.

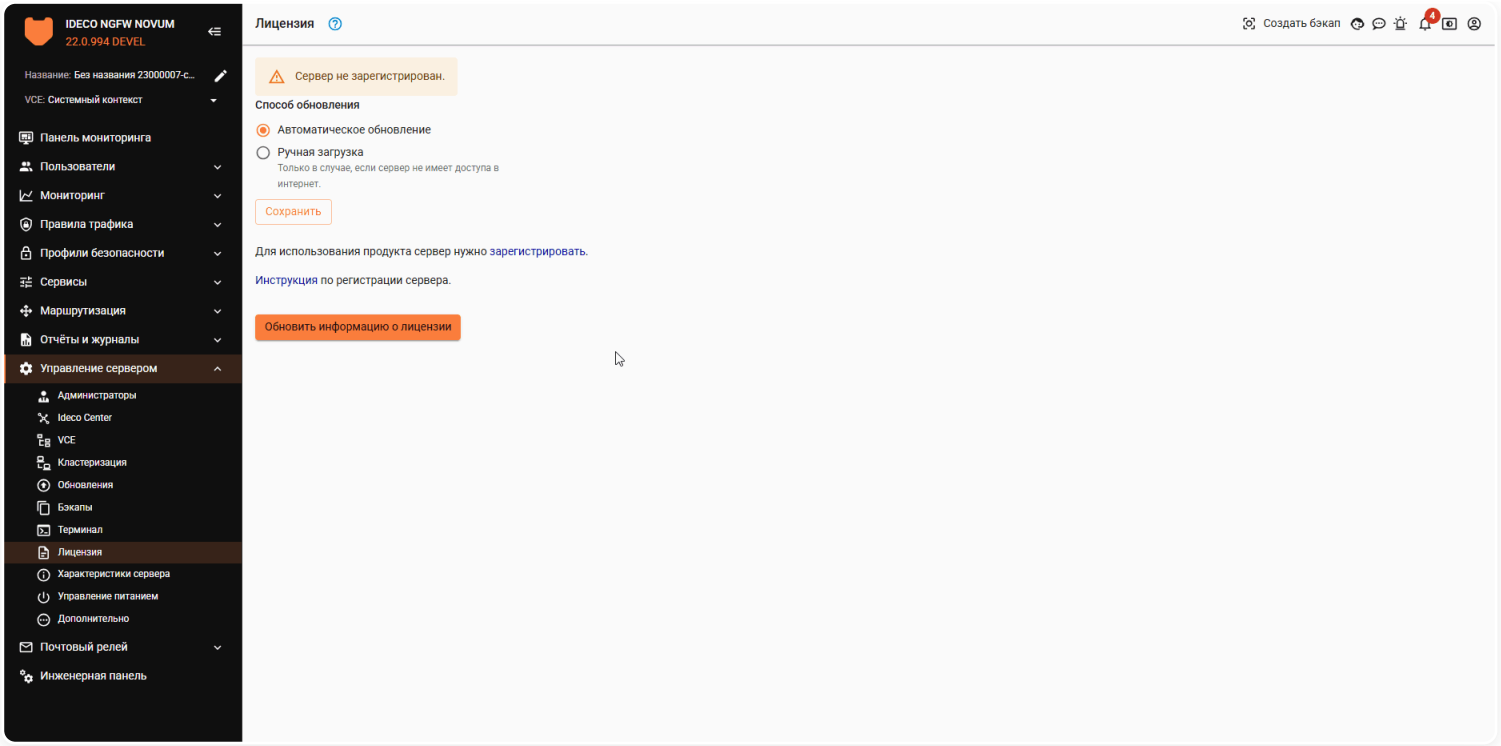
Онлайн-регистрация

Шаги онлайн-регистрации сервера и привязки лицензии:

1. Перейдите в веб-интерфейс Ideco NGFW Novum в **Управление сервером** → **Лицензия**, выберите **Автоматическое обновление** в качестве способа обновления, нажмите **Сохранить**.

2. Перейдите в MY.IDECO, нажав **Зарегистрировать**.

3. В открывшемся окне выберите компанию и нажмите **Добавить**. После добавления нажмите **Обновить информацию о лицензии** для проверки состояния лицензии:



В режиме автоматического обновления сервер ежедневно проверяет статус лицензии на MY.IDECO. В случае отсутствия соединения попытки возобновляются каждую минуту.

Офлайн-регистрация

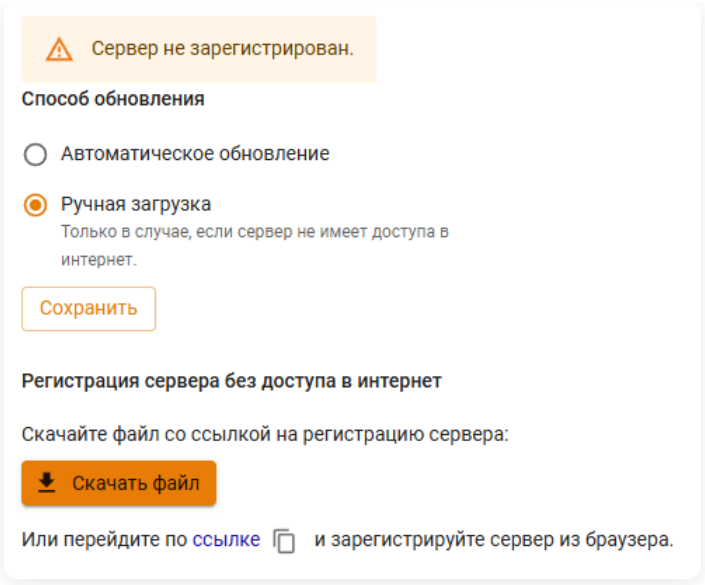
Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

1. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum. Выберите **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Для этого нажмите **Скачать файл** или скопируйте ссылку из веб-интерфейса:

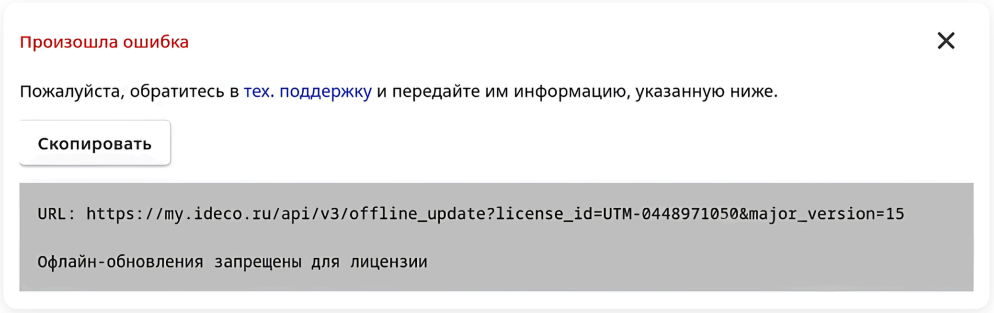


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

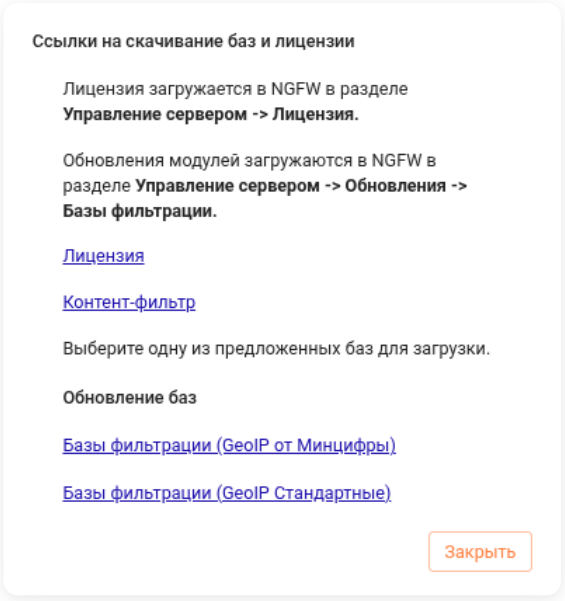
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

5. Перейдите в **NGFW** → **Лицензирование** в MY.IDECO. Нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `UTM (UTM Unknown)`.

Если была выбрана лицензия, не подходящая для офлайн-регистрации сервера, то появится ошибка:

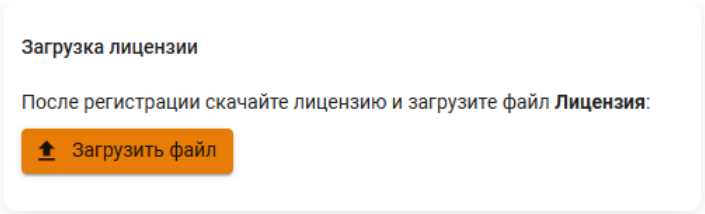


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



Если при скачивании Обновления баз (Предотвращение вторжений, базы GeoIP) через **Google Chrome** возникают проблемы, в настройках браузера разрешите **Небезопасный контент** для MY.IDECO.

7. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum и загрузите файл с лицензией, скачанный в пункте 6:



Повторная регистрация сервера после удаления

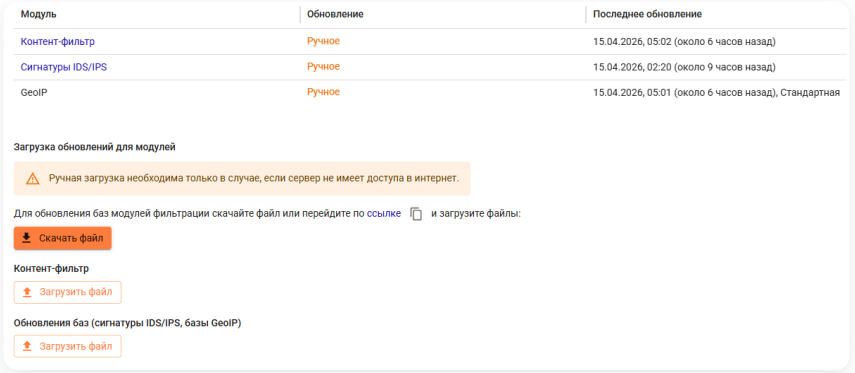
1. Откройте терминал и введите команду:

```
rm /var/cache/ideco/license-backend/license.json
systemctl restart ideco-license-backend.service
```

2. Следуйте пунктам по офлайн-регистрации, которые приведены выше.

Офлайн-обновление баз модулей безопасности

Чтобы обновить базы модулей безопасности в режиме офлайн, перейдите в веб-интерфейс Ideco NGFW Novum в раздел **Управление сервером** → **Обновления** → **Базы фильтрации** и загрузите скачанные в шестом пункте Офлайн-регистрации файлы, нажав на соответствующие кнопки:



Базы фильтрации Ideco NGFW Novum могут меняться ежедневно, поэтому при ручной загрузке обновляйте базы как можно чаще.

Получение доступа в интернет

Для получения доступа в интернет на устройстве пользователя после первоначальной настройки и регистрации сервера выполните действия:

1. Убедитесь, что устройство пользователя настроено одним из способов:

- Устройство находится в одном широковещательном домене с сетевым интерфейсом NGFW: между устройствами только L2-коммутаторы или прямое подключение. В качестве шлюза указан NGFW.
- Интернет-трафик пользователя маршрутизируется на NGFW через промежуточные маршрутизаторы, L3-коммутаторы.

2. Убедитесь, что в веб-интерфейсе NGFW выбран нужный способ авторизации.

3. Выполните действия в зависимости от настроенного способа авторизации пользователя:

- **Веб-аутентификация** - способ авторизации, при котором запрос неавторизованного пользователя переадресуется на NGFW, а после успешной авторизации переходит по указанному пользователем запросу:
  - **Аутентификация через веб-интерфейс**. Зайдите в браузер с устройства пользователя. Введите логин и пароль, указанный при настройке учетной записи пользователя;
  - Для авторизации пользователей Active Directory воспользуйтесь статьей **Аутентификация пользователей AD/Samba DC**.

> При авторизации через **Веб-аутентификацию** проверьте, что у пользователя на сетевой карте в качестве шлюза (объединенных в цепочку нескольких шлюзов) или при прямых подключениях к прокси по умолчанию указан IP-адрес локального сетевого интерфейса NGFW. Убедитесь, что работает DNS-резолвинг адресов.

- **IP и MAC авторизация** - способ авторизации, при котором пользователь получает доступ в интернет без ввода логина и пароля:
  - **Авторизация по IP-адресу**. Проверьте, чтобы IP-адрес устройства пользователя совпадал с IP-адресом, указанным администратором в настройках учетной записи пользователя NGFW. Следуйте рекомендациям статьи **Авторизация по IP-адресу**.
  - Для настройки авторизации переносных устройств (например, рабочих ноутбуков сотрудников) или сетевых устройств, на которых не настроена привязка IP + MAC и выдается IP-адрес через DHCP, воспользуйтесь статьей **Авторизация по MAC-адресу**.

> Для авторизации пользователя по MAC-адресу оба устройства (NGFW и устройство пользователя) должны находиться в одном широковещательном домене, а NGFW должен выступать шлюзом.

- **Авторизация по подсетям** - способ автоматической авторизации большого количества устройств из требуемой подсети без привязки к MAC и/или конкретному IP.

Настройка высокопроизводительного контекста

Высокопроизводительный контекст (VCE VPP) - виртуальный контекст в Ideco NGFW Novum для обработки сетевого трафика с высокой пропускной способностью. Сетевой стек построен на технологиях DPDK (Data Plane Development Kit) и VPP (Vector Packet Processing), работающий в обход стека ядра Linux, который используется в **Классическом контексте** (VCE NGFW).

Ключевые архитектурные отличия:

- Сетевая карта передается в VCE VPP целиком, а не отдельными VLAN. Этим объясняется требование перезагрузки контекста после назначения интерфейсов.
- Контейнерная модель без гипервизора (на базе systemd-nspawn). VCE VPP можно запускать в виртуальных средах без вложенной виртуализации и связанных с ней потерь производительности.
- Жесткая привязка ресурсов - выделенные контексту CPU-ядра, оперативная память и сетевые карты не перераспределяются динамически.

Основные преимущества перед **Классическим контекстом**:

- Поддержка до 100 000 правил **Межсетевого экрана**.
- Фильтрация трафика на любых TCP-портах через **Профили безопасности**.
- Более высокая пропускная способность при обработке трафика.

Ряд функций недоступен, например, DDNS, IPsec и ГОСТ VPN. Полный список различий - в статье.

Подробнее об архитектуре VCE - в статье **Виртуальные контексты в Ideco NGFW: как работают VCE изнутри**.

Статья описывает настройку VCE VPP внутри Ideco NGFW Novum. Входная точка: **Системный контекст** установлен, зарегистрирован и имеет доступ в интернет. Если нет - выполните шаги из статей:

- **Первоначальная настройка**
- **Регистрация сервера**
- **Получение доступа в интернет**

Настройка в Системном контексте

Шаг 1. Создание контекста

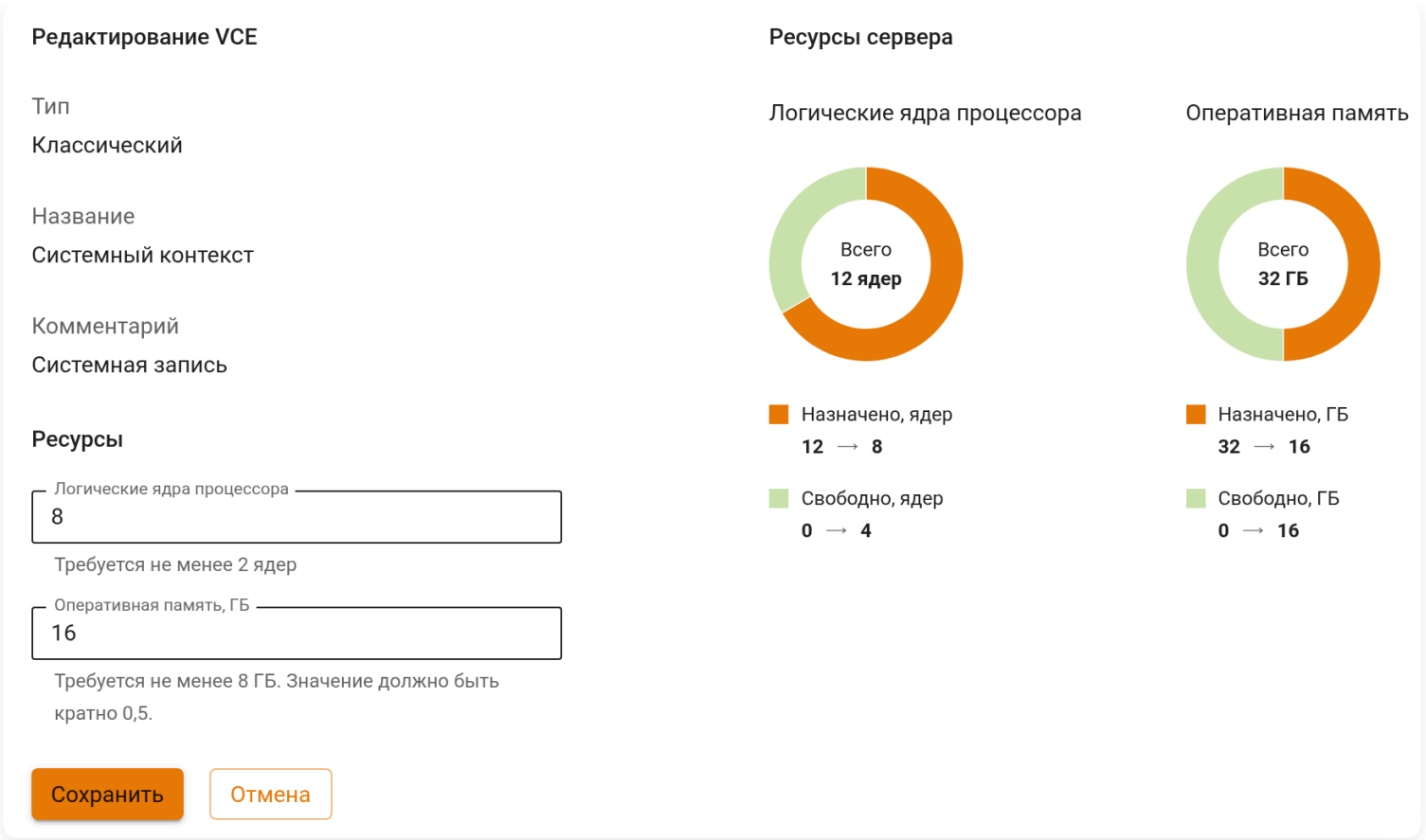
Для **Высокопроизводительного контекста** потребуются:

- Минимум **4 логических ядра**.
- Минимум **8 ГБ оперативной памяти**.

Рекомендуем отключить Hyper-Threading (Intel) и SMT (AMD) в BIOS/UEFI сервера - эти технологии существенно снижают производительность VCE VPP. Не рекомендуем использовать двухпроцессорные системы.

Перейдите в **Управление сервером** → **VCE** и выполните действия:

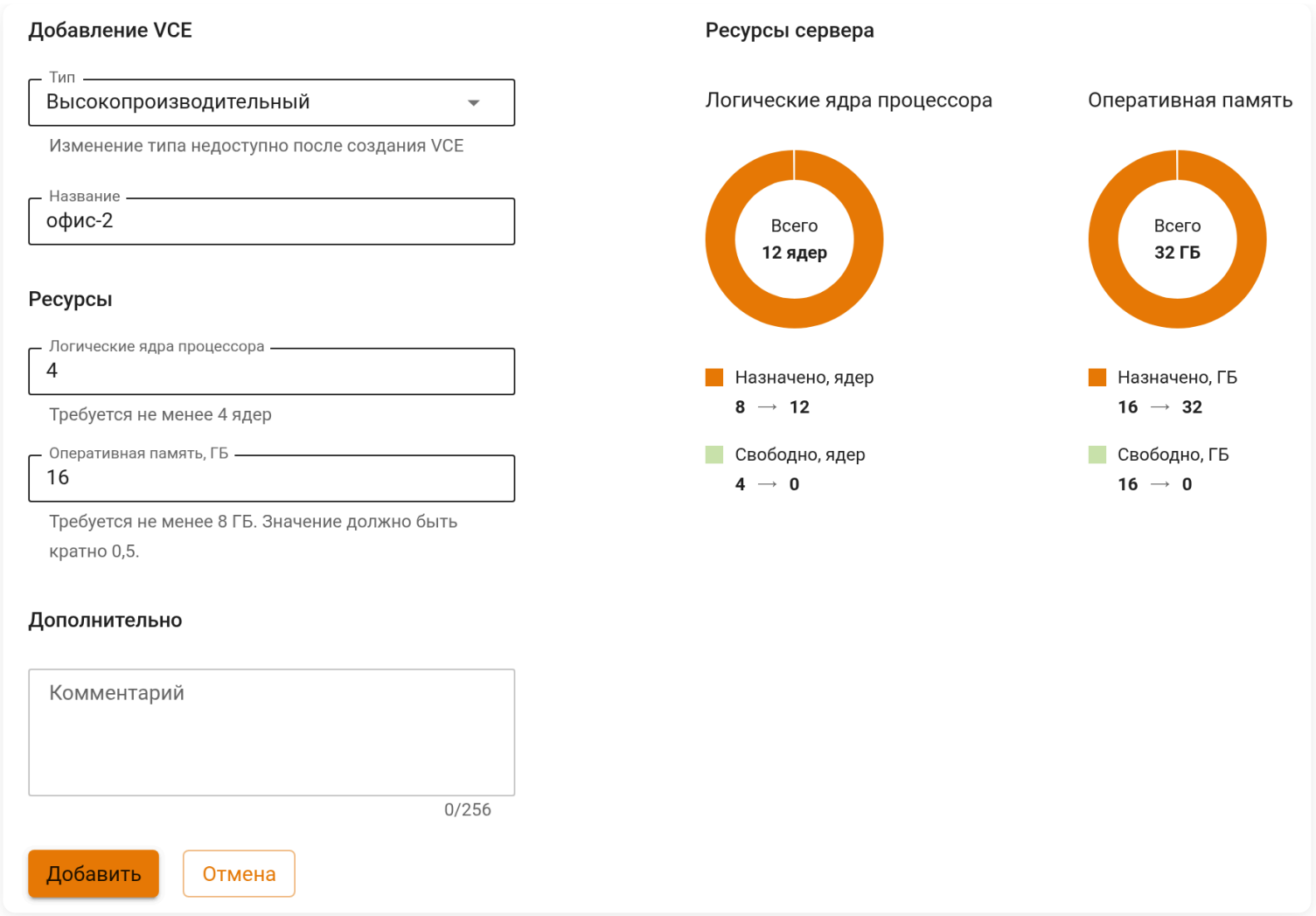
1. Нажмите  в строке **Системного контекста**, освободите в пул **Свободных ресурсов** не менее 4 ядер и 8 ГБ оперативной памяти:



2. Нажмите **Сохранить**.

3. Нажмите **Добавить** для создания нового контекста.

4. Выберите тип контекста **Высокопроизводительный**, укажите название и назначьте ресурсы из пула свободных:



5. Нажмите **Добавить**.

Шаг 2. Создание сетевых интерфейсов

Сетевые интерфейсы для VCE VPP создаются и редактируются только в **Системном контексте**. В **Классических** и **Высокопроизводительных контекстах** таблица интерфейсов доступна только для чтения.

Перейдите в **Сервисы** → **Сетевые интерфейсы** и создайте два интерфейса:

- Интерфейс с ролью **WAN** - для подключения к провайдеру.
- Интерфейс с ролью **LAN** - для пользовательской сети.

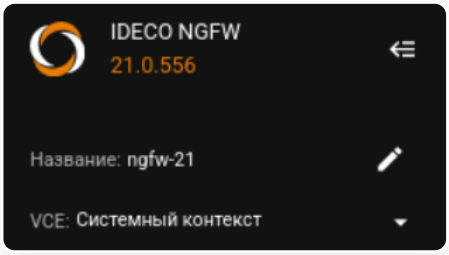
При создании каждого интерфейса укажите его принадлежность к созданному VCE VPP. Пример настройки в статье.

После назначения интерфейсов перезагрузите контекст для корректной работы интерфейсов.

Шаг 3. Подключение к веб-интерфейсу

Перейдите из **Системного контекста** в веб-интерфейс созданного VCE VPP одним из способов:

- В **Управление сервером** → **VCE** нажмите напротив нужного контекста - откроется новая вкладка.
- Нажмите в левом верхнем углу **Системного контекста** и выберите нужный VCE:



Настройка в Высокопроизводительном контексте

Шаг 4. Создание администратора

Только что созданный VCE VPP не содержит администраторов. Учетные записи администраторов **Системного контекста** в VCE VPP не действуют.

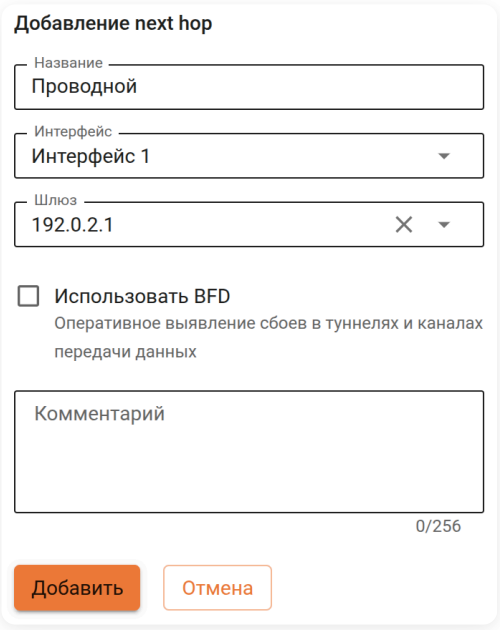
Для дальнейшей работы создайте отдельного администратора по инструкции из статьи **Администраторы**.

Шаг 5. Настройка подключения к провайдеру

Настройте шлюз для выхода в интернет:

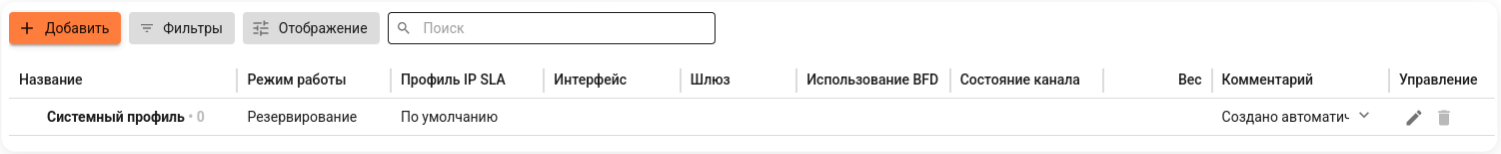
1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:



- **Название** - укажите название.
- **Интерфейс** - выберите WAN-интерфейс, созданный для VCE VPP в шаге 2.
- **Шлюз** - укажите IP-адрес шлюза провайдера. Адрес должен находиться в сети выбранного интерфейса.
- **Использовать BFD** - включите опцию для проверки доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection). Поддержка BFD должна быть включена и на стороне указанного шлюза.

3. Перейдите в **SD-WAN** → **Профили next hop** и нажмите для редактирования **Системного профиля**:



4. Перейдите на вкладку **Next hop**, нажмите **Выбрать next hop** и выберите next hop, созданный на предыдущем шаге.

5. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

Если шлюз не обеспечивает выход в интернет, VCE VPP не получит лицензию и не сможет загрузить обновления баз модулей

безопасности.

Шаг 6. Проверка лицензии

После завершения настройки подключения к провайдеру перейдите в раздел **Лицензия** - данные будут автоматически получены из MY.IDECO.

На Ideco NGFW Novum с лицензией на 100 пользователей каждый созданный VCE поддерживает 100 пользователей. В будущих версиях количество пользователей будет распределяться между **Системным контекстом** и VCE.

Шаг 7. Настройка Межсетевого экрана

В VCE VPP по умолчанию установлено запрещающее FORWARD-правило. Без явного разрешающего правила пользователи не получат доступ в интернет.

Перейдите в **Правила трафика** → **Межсетевой экран** и создайте разрешающее правило для пользовательского трафика в соответствии с политикой безопасности вашей организации.

Шаг 8. Настройка авторизации пользователей

Настройте метод авторизации в разделе **Пользователи** → **Авторизация**. Ниже - базовые методы для быстрого старта:

- **Веб-аутентификация** - пользователь вводит логин и пароль в браузере при попытке выйти в интернет.
- **IP авторизация** - доступ автоматически по IP-адресу без ввода пароля.
- **Авторизация по подсетям** - автоматическая авторизация всех устройств из указанной подсети.

Полный список доступных методов, включая интеграцию с Active Directory, авторизацию через Ideco Client и пользователей терминальных серверов, смотрите в разделе **Авторизация**.

Авторизация по MAC-адресу в VCE VPP недоступна.

Дальнейшие шаги по настройке устройств пользователей аналогичны **Системному контексту**. Инструкция - в статье.

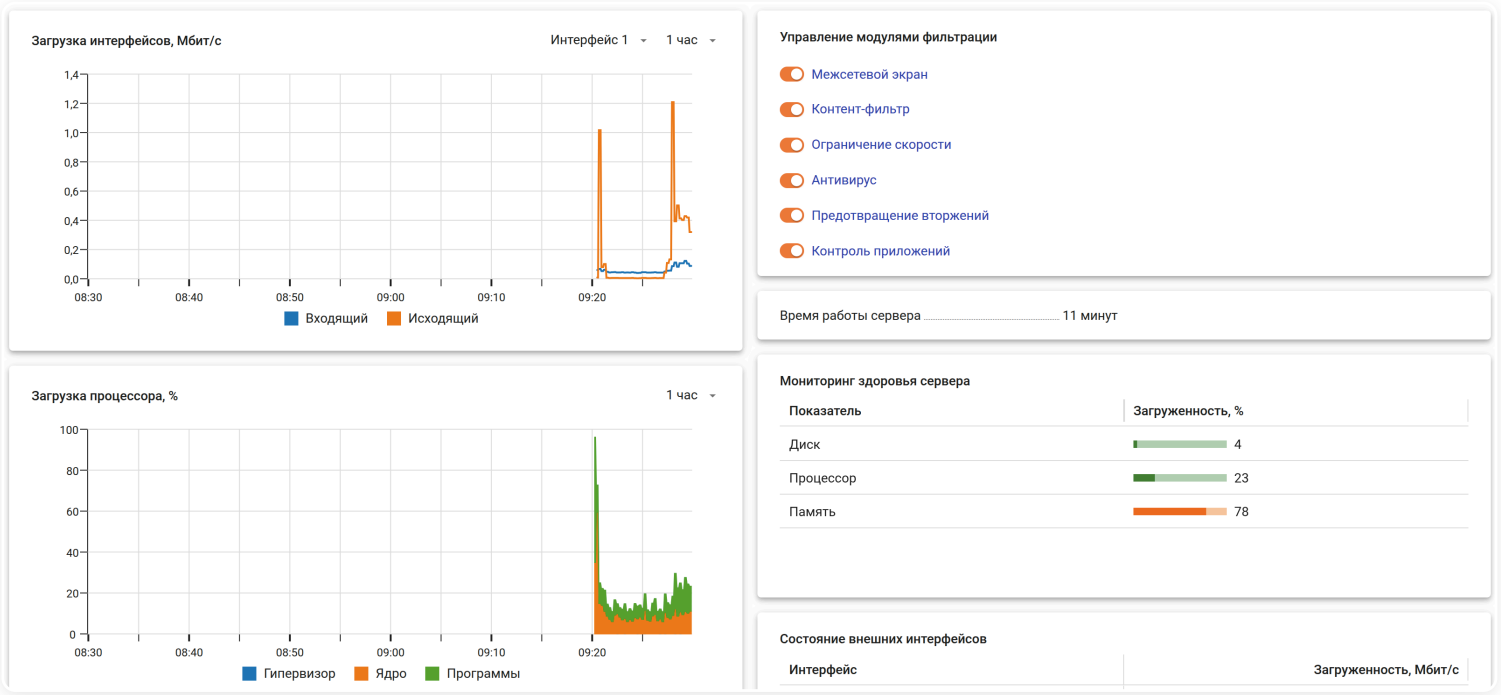
Полезные ссылки

- **VCE**
- **Отличия VCE NGFW и VCE VPP**
- **Лицензия**
- **Межсетевой экран**
- **Веб-аутентификация**
- **IP авторизация**
- **Авторизация по подсетям**
- **Авторизация**
- **Администраторы**
- **Получение доступа в интернет**
- **Первоначальная настройка**
- **Регистрация сервера**

Панель мониторинга

Классический контекст | Высокопроизводительный контекст

Модуль позволяет просматривать информацию о состоянии сервера за определенный промежуток времени:



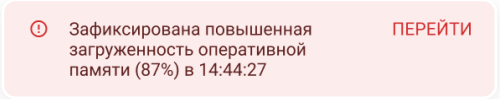
Отображение оперативной информации

- Загрузка интерфейсов, Мбит/с.
- Загрузка процессора, %.
- Занятая оперативная память, ГБ.
- Температура.

Есть возможность выбрать удобный промежуток времени для отображения: 5 минут, 1 час, 6 часов, 1 день, 7 дней.

Мониторинг здоровья сервера

Блок в реальном времени отображает метрики системы при помощи цветовой индикации. Цвет каждого индикатора (зеленый/желтый/красный) зависит от степени превышения пороговых значений. Если показатели остаются в желтой или красной зоне дольше определенного времени, будет отправлено уведомление:



Пороговые значения:

Диск

Зеленый - занято менее 80%.

Желтый - занято от 80% до 90% в течение 5 минут. Уведомление, если дольше 5 минут.

Красный - занято более 90% в течение 5 минут. Уведомление, если дольше 5 минут.

Процессор

Зеленый - нагрузка менее 60%.

Желтый - нагрузка от 60% до 85%. Уведомление, если дольше 1 минуты.

Красный - нагрузка более 85%. Уведомление, если дольше 1 минуты или сразу при нагрузке более 95%.

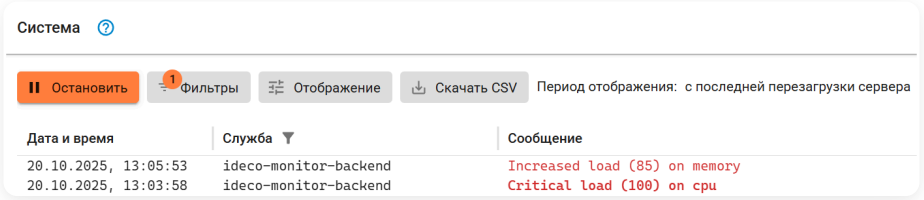
Память

Зеленый - доступно более 15%.

Желтый - доступно от 5% до 15%. Уведомление, если дольше 2 минут.

Красный - доступно менее 5%. Уведомление, если дольше 1 минуты.

При превышении порогов события записываются в логи. Для их просмотра перейдите в раздел **Система** и примените фильтр по службе `ideco-monitor-backend`:



Управление модулями фильтрации

Блок позволяет включить или выключить соответствующие модули фильтрации:

- Межсетевой экран.
- Контент-фильтр.
- Ограничение скорости.
- Антивирусы веб-трафика.
- Предотвращение вторжений.
- Контроль приложений.

Каждый из пунктов является ссылкой на соответствующий модуль.

Отображение статистической информации

- Время работы сервера.
- Состояние внешних интерфейсов.
- Топ хостов (можно выбрать количество в топе: 5, 10, 15, 20).
- Основная информация о лицензии.
- Параметры и загрузка IPsec (есть возможность перейти на страницу IPsec).

Особенности отображения информации

- График загрузки интерфейсов включает весь трафик NGFW, в том числе служебный.
- При выборе разных промежутков времени отображаемые максимальные значения на графике могут отличаться.
- Таблицы **Топ хостов** включают только пользователей с наибольшей скоростью входящего и исходящего трафика. При формировании статистики по хостам учитываются протоколы, определенные модулем **Контроль приложений**. При этом не учитывается служебный трафик NGFW.

Пользователи

Учетные записи

Создание и управление учетными записями пользователей

Перейти

Внешние каталоги

Настройка интеграций Ideco NGFW с Active Directory, ALD Pro, FreeIPA и RADIUS-сервером

Перейти

Аутентификация

Процесс аутентификации пользователей и настройка двухфакторной аутентификации

Перейти

Авторизация

Веб-аутентификация, правила авторизации по IP- и MAC-адресам, возможность авторизации по подсетям

Перейти

VPN-подключение

Настройка VPN-подключения с использованием протоколов: IKEv2/IPsec, SSTP, L2TP/IPsec

Перейти

Ideco Client

Установка и настройка Ideco Client, настройка Device VPN

Перейти

Профили устройств

Использование профилей для проверки устройств, подключаемых к NGFW через Ideco Client

Перейти

Обнаружение устройств

Автоматическое создание пользователя с авторизацией по IP-адресу и MAC-адресу для различных устройств

Перейти

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

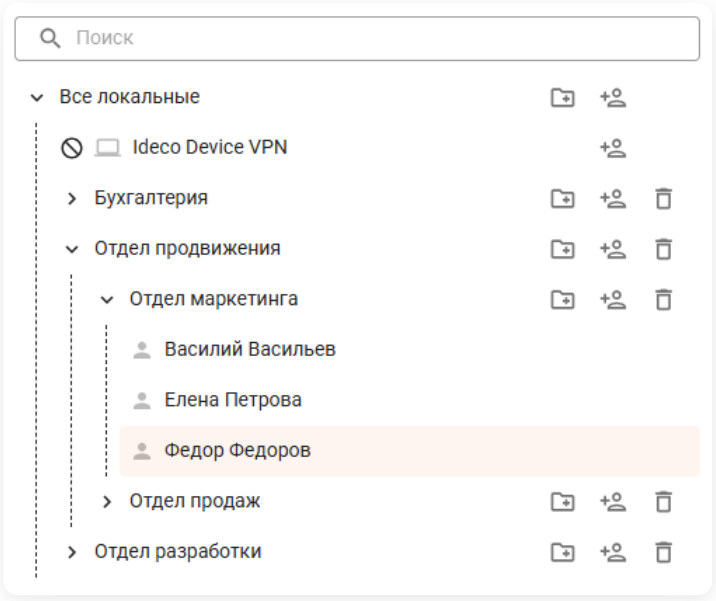
Учетные записи

Классический контекст | Высокопроизводительный контекст | API

С 21 версии Ideco NGFW Novum пользователи разделяются на локальных (сюда же входят импортированные) и пользователей внешних каталогов Active Directory. Пользователи AD более не импортируются в дерево пользователей.

Локальные пользователи

В веб-интерфейсе Ideco NGFW Novum локальные пользователи отображаются в виде дерева и могут быть организованы в группы с неограниченной вложенностью. Пример дерева локальных пользователей:



Группа **Ideco Device VPN** автоматически создается при установке NGFW Novum и объединяет пользователей, подключившихся через Device VPN. Имя пользователя группы импортируется из поля `Common Name` пользовательского сертификата.

Во вкладку **Локальные** попадают пользователи внешних каталогов:

- Импортированные из ALD.
- Импортированные из FreeIPA.
- Пользователи RADIUS, подключившиеся к NGFW Novum, если настроена авторизация через RADIUS.

В Ideco NGFW Novum реализован принцип наследования, который позволяет задавать и изменять общие параметры для всех локальных пользователей группы через родительскую группу.

Все локальные пользователи Ideco NGFW Novum по умолчанию входят в группу **Все локальные**.

Цвет пиктограммы пользователя зависит от состояния учетной записи пользователя:

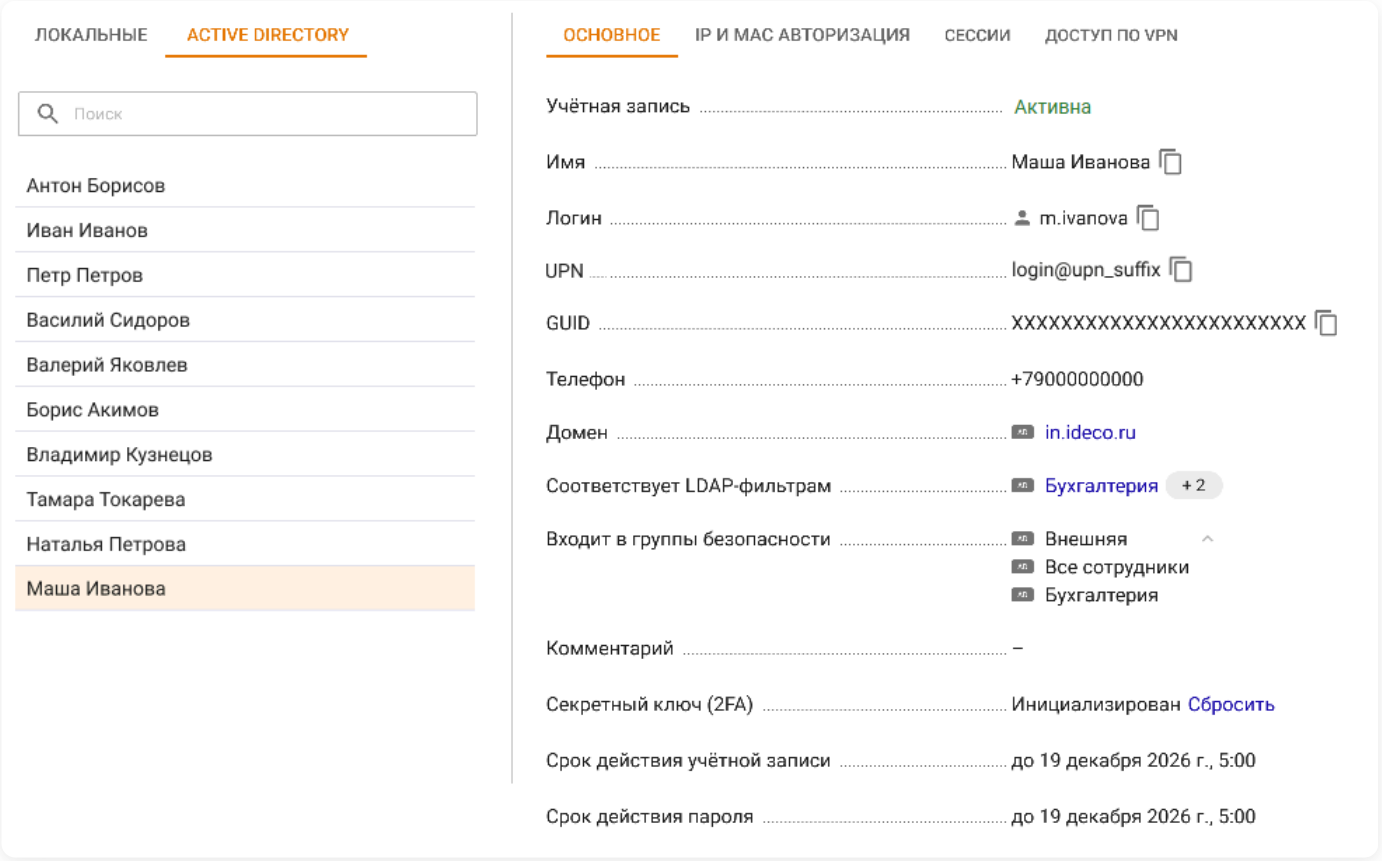
Состояние учетной записи пользователя	Описание
	Пользователь прошел процедуру авторизации, и ему был предоставлен доступ в интернет
	В настройках пользователей выбран запрет на авторизацию
	Пользователь не прошел процедуру авторизации, и ему не был предоставлен доступ в интернет

Элементы управления в дереве пользователей:

Обозначение	Описание
	Создать учетную запись пользователя
	Создать группу
	Удалить учетную запись пользователя или группу

Пользователи внешних каталогов Active Directory

Пользователи внешних каталогов AD отображаются на вкладке **Учетные записи** → **Active Directory**, если настроена интеграция с AD. Данные о пользователе загружаются с контроллеров домена AD:



Расшифровка полей

- **Учетная запись** - Активна/Заблокирована.
- **Имя** - имя пользователя в AD.
- **Логин** - логин пользователя в AD.
- **UPN** - UPN-суффикс пользователя. Можно скопировать в буфер обмена вместе с логином.
- **GUID** - уникальный идентификатор учетной записи.
- **Телефон** - номер телефона, если имеется.
- **Домен** - каталог, к которому принадлежит учетная запись. При нажатии откроется интеграция в разделе **Внешние каталоги** → **Active Directory/Samba DC**.
- **Соответствует LDAP-фильтрам** - список LDAP-фильтров, которым соответствует запись. При нажатии откроется соответствующий фильтр в разделе **Внешние каталоги** → **LDAP-фильтры**. Если запись не соответствует фильтрам, значение будет `Нет`. Если соответствие неизвестно, значение будет `-`.
- **Входит в группы безопасности** - группы безопасности на сервере, в которые входит учетная запись. Если запись не соответствует группам безопасности, значение будет `Нет`. Если соответствие неизвестно, значение будет `-`.
- **Комментарий** - описание (description) пользователя в AD.
- **Секретный ключ (2FA)** - статус TOTP-токена для двухфакторной аутентификации. Чтобы сбросить секретный ключ, нажмите **Сбросить**.

Для принудительного обновления информации о пользователе доступна кнопка **Обновить**. Полученная информация кешируется.

Управление учетными записями и группами

Классический контекст | Высокопроизводительный контекст

В статье описаны создание, удаление и перемещение учетных записей локальных пользователей.

Создание учетной записи пользователя

Не используйте в качестве логина пользователя IP-адрес, так как возникнет ошибка при подключении по IKEv2.

Способы создания учетной записи пользователя и группы:

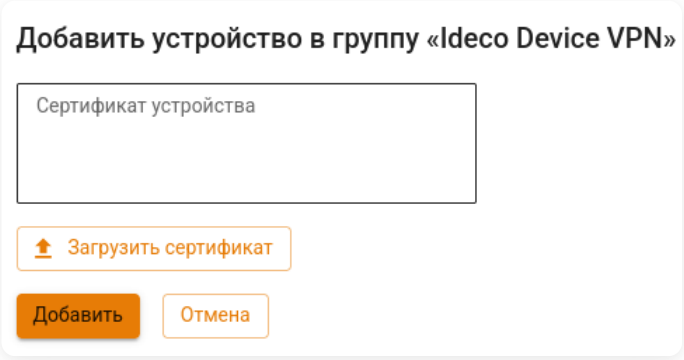
Ideco Device VPN

В группе Ideco Device VPN создаются пользователи Device VPN и терминальные серверы. Для создания пользователя через пользовательский сертификат:

1. Нажмите напротив группы **Ideco Device VPN**:



2. Нажмите **Загрузить сертификат** и выберите сохраненный файл сертификата. Нажмите **Добавить**:



Про создание сертификата для Device VPN смотрите статью.

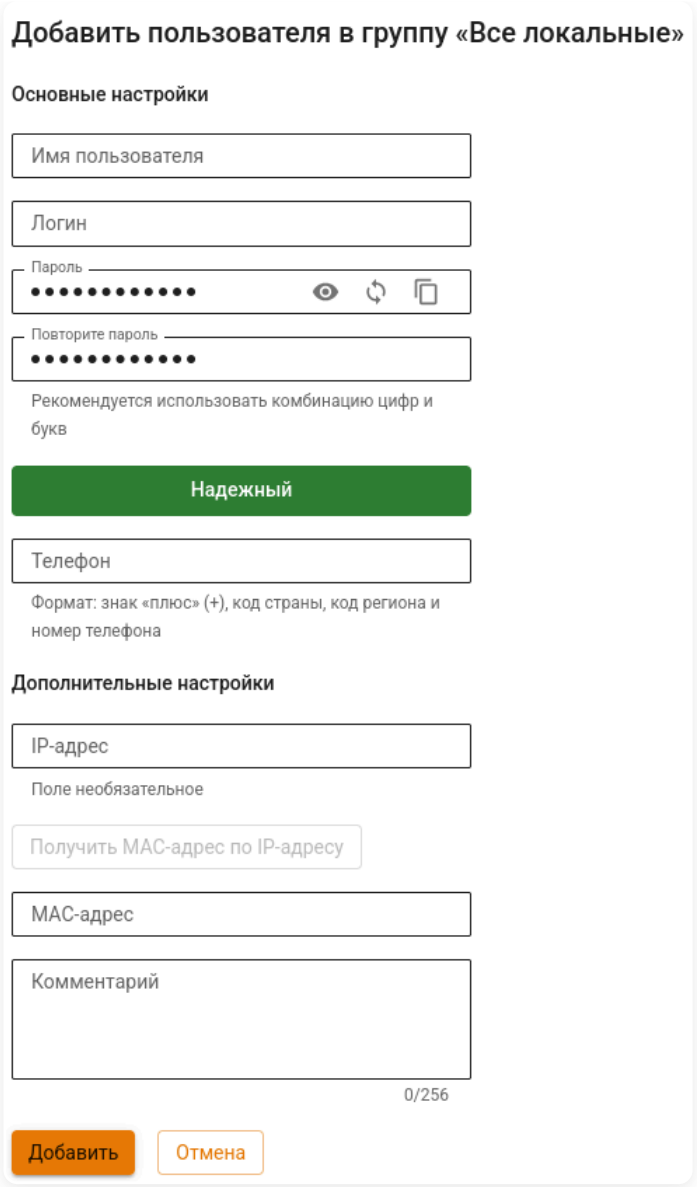
В группе Ideco Device VPN появится пользователь с именем из поля `Common name` пользовательского сертификата.

Группа Все локальные

1. Выберите группу **Все локальные** в дереве пользователей.

2. Нажмите .

3. Заполните поля:



- **Имя пользователя** - введите имя пользователя. Максимальное количество символов - 128.
- **Логин** - введите логин латинскими символами в нижнем регистре. Применяется для авторизации в службах Ideco NGFW Novum. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - введите пароль. Смотрите рекомендации к созданию паролей ниже.
- **Телефон** - телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона.
- **IP-адрес** и **MAC-адрес** - при заполнении этих полей создается правило авторизации в **Пользователи** → **Авторизации** → **IP и MAC** Ideco NGFW Novum.

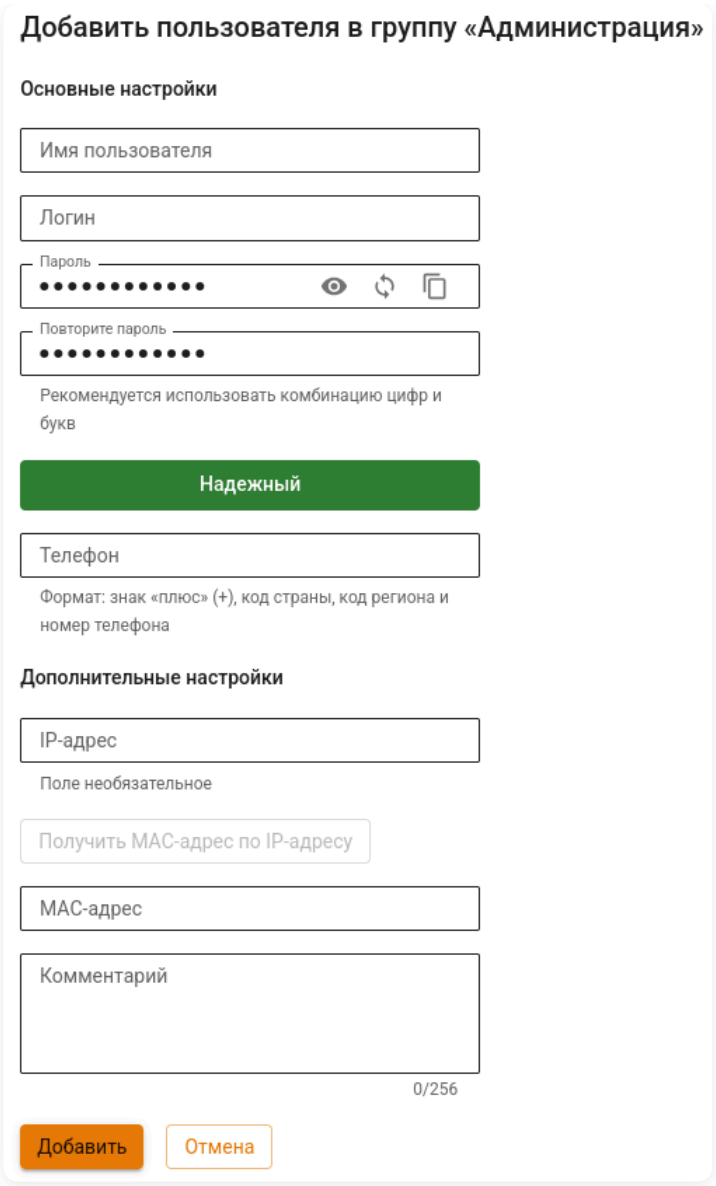
4. Нажмите **Добавить**.

Вложенные группы

1. Выберите группу, в которую добавится пользователь.

2. Нажмите **Создать пользователя** на вкладке **Основное** или рядом с названием группы в дереве.

3. Заполните поля:



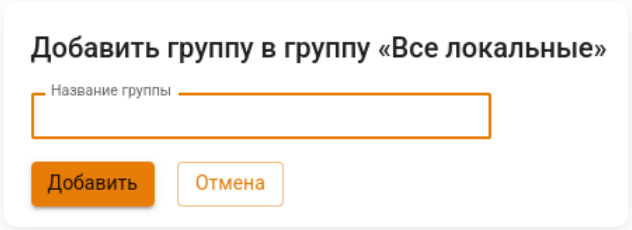
- **Имя пользователя** - введите имя пользователя. Максимальное количество символов - 128.
- **Логин** - введите логин латинскими символами в нижнем регистре. Применяется для авторизации в службах Ideco NGFW Novum. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - введите пароль. Смотрите рекомендации к созданию паролей ниже.
- **Телефон** - введите телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона.
- **IP-адрес** и **MAC-адрес** - при заполнении этих полей создается правило авторизации в **Пользователи** → **Авторизации** → **IP и MAC** Ideco NGFW Novum.

4. Нажмите **Добавить**.

Создание группы

1. Нажмите справа от названия группы.

2. Укажите название и нажмите **Добавить**:



Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;` , `^[[4~;` и т.д.

Посмотреть или восстановить пароль учетной записи пользователя нельзя. Возможна только смена пароля.

Для учетных записей пользователей Active Directory, ALD Pro и RADIUS проверка пароля осуществляется средствами соответствующего каталога или RADIUS-сервера.

Рекомендации к созданию паролей

Доступна автоматическая генерация пароля.

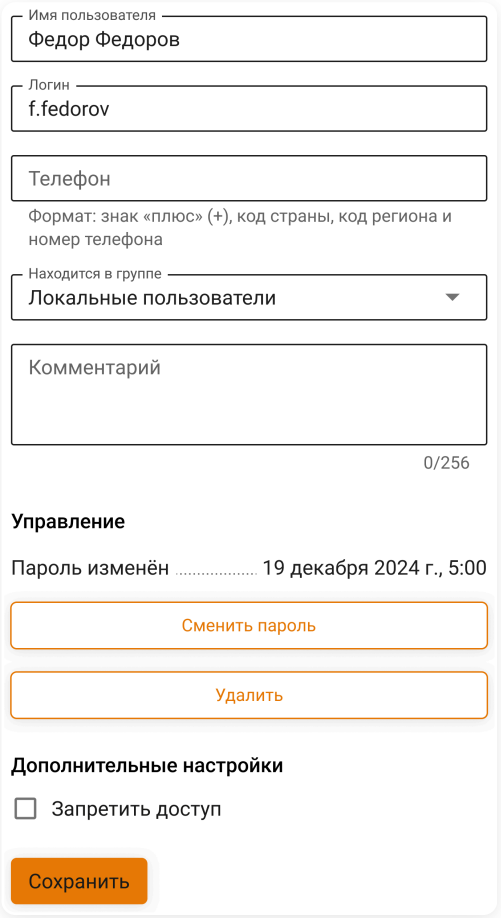
- Минимальная длина - 12 символов.
- Использование строчных и заглавных латинских символов.
- Использование цифр и специальных символов.

Управление пользователями Active Directory (добавление, редактирование или удаление) выполняется на контроллере домена в дереве пользователей.

Удаление учетной записи пользователя или группы

Реализовано два варианта удаления:

- Наведите курсор на пользователя или группу и нажмите на .
- Нажмите на **Удалить** на вкладке **Основное**:



Перемещение учетной записи пользователя

1. Выберите учетную запись или группу.

2. На вкладке **Основное** в поле **Находится в группе** выберите новую группу и нажмите на **Сохранить**.

Редактирование учетной записи пользователя

Редактирование логина и пароля возможно на вкладке **Основное** в разделе **Пользователи** → **Учетные записи** при выделении нужного пользователя.

Полезные ссылки

- **Как безопасно подключить удаленного подрядчика**

Настройка пользователей

Классический контекст | Высокопроизводительный контекст

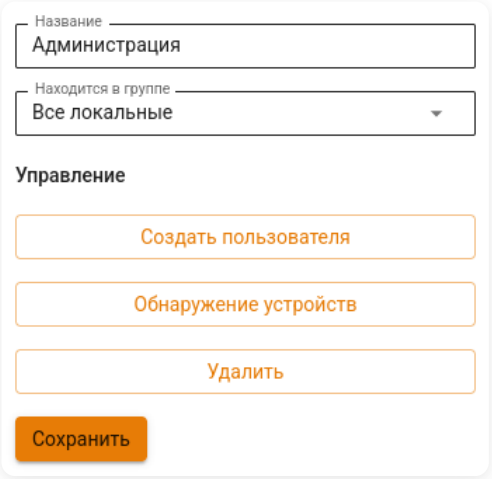
Чтобы изменить параметры учетной записи локального пользователя или группы пользователей, выберите нужный объект в дереве пользователей.

Группы пользователей

В группы можно добавлять как отдельные учетные записи пользователей, так и другие группы, объединяя их вместе. Правила, заданные для группы, автоматически применяются ко всем участникам группы.

Основное

Выберите группу локальных пользователей для редактирования:



- **Название** - введите новое название.
- **Находится в группе** - укажите группу, в которую требуется переместить эту группу.
- **Создать пользователя** - нажмите для создания пользователя в группе.
- **Обнаружение устройств** - нажмите для открытия раздела Обнаружение устройств.
- **Удалить** - нажмите для удаления группы. Вместе с группой удаляются учетные записи пользователей группы.

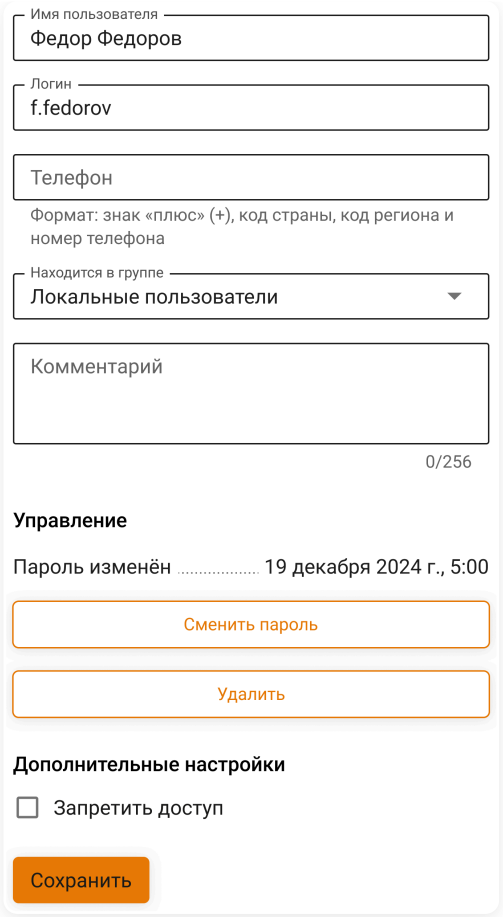
ALD Pro

Категория содержит информацию об имени домена ALD Pro и типе группы. Процесс настройки синхронизации с ALD Pro и импорт пользователей описан в статье Интеграция с ALD Pro.

УЗ локальных пользователей

Основное

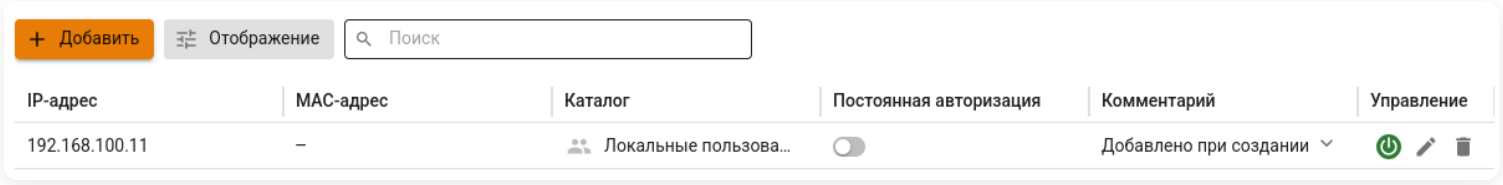
Основные настройки включают параметры, определяющие статус локального пользователя:



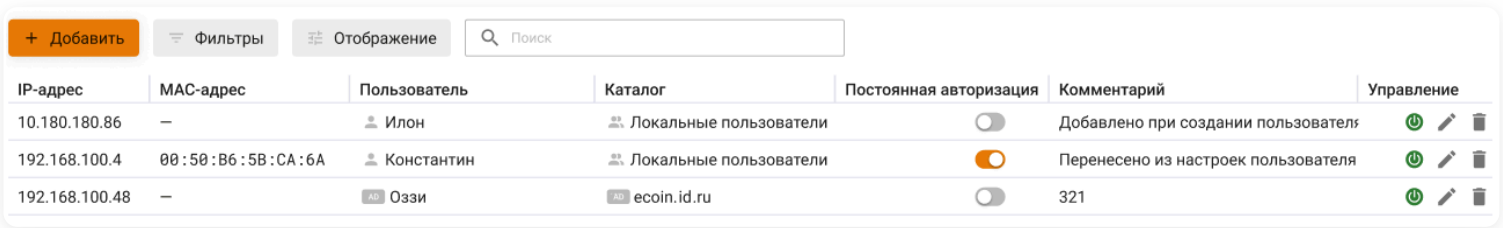
- **Имя пользователя** - введите имя пользователя. Максимальное количество символов - 128.
- **Логин** - введите логин латинскими символами в нижнем регистре. Применяется для авторизации в службах Ideco NGFW Novum. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Телефон** - введите телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона.
- **Находится в группе** - используйте это поле для перемещения пользователя в другую группу.
- **Комментарий** - введите описание пользователя. Необязательное поле.
- **Запретить доступ** - включите опцию, если нужно запретить пользователю авторизацию. Доступ будет закрыт к ресурсам интернета, почте и личному кабинету.

IP и MAC авторизация

На вкладке можно создать правила авторизации по IP и MAC для определенного пользователя:



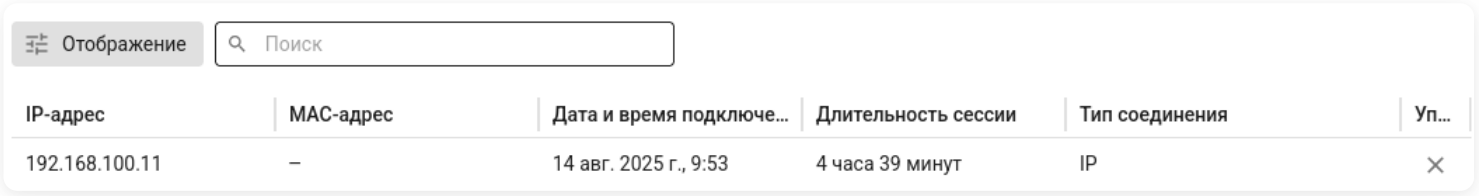
Также создать правила авторизации по IP и MAC для пользователя можно в **Пользователи** → **Авторизация** → **IP и MAC**:



Правила **IP и MAC авторизации** создают аналогичную привязку в DHCP-сервере Ideco NGFW Novum. Однако, если те же адреса указаны во включенных правилах DHCP-сервера, то правила DHCP-сервера будут выполняться в первую очередь.

Сессии

Содержит таблицу с информацией обо всех активных сессиях пользователя:

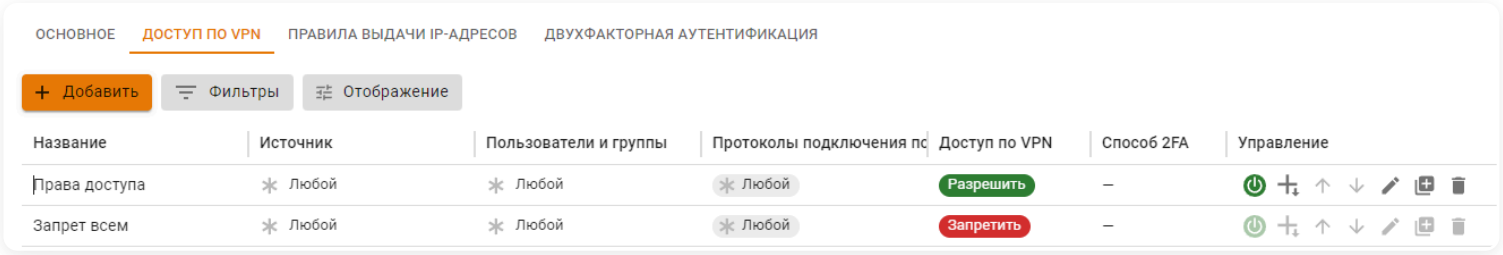


При нажатии на ✕ в столбце **Управление** NGFW разорвет сессию пользователя.

Аналогичная таблица расположена в разделе **Мониторинг** → **Сессии пользователей**.

Доступ по VPN

Категория позволяет просматривать правила доступа VPN, которые настраиваются в **VPN-подключения** → **Доступ по VPN**.



Для перехода к общей таблице доступа VPN из дерева пользователей нажмите на нужное название правила:

Привязанные устройства

Вкладка отображает устройство, привязанное к учетной записи пользователя при подключении через Ideco Client. К одному пользователю может быть привязано только одно устройство:

При отсутствии привязки таблица будет пустой - запись появляется автоматически после первой авторизации пользователя через Ideco Client при включенной опции **Привязать устройство к пользователю** в **Пользователи** → **Ideco Client** → **Основное** или в **Пользователи** → **VPN-подключения** → **Доступ по VPN**.

Для удаления привязки нажмите в колонке **Управление**. После удаления новая привязка будет создана автоматически при следующем подключении пользователя.

Внешние каталоги

Классический контекст | Высокопроизводительный контекст

В Ideco NGFW Novum реализована интеграция с Active Directory (AD), ALD Pro и RADIUS-сервером для получения данных о пользователях, авторизации и управления доступом.

С каталогами AD и ALD Pro выполняется периодическая синхронизация по информации о пользователях:

- AD:
  - Синхронизация списка групп безопасности AD и участия авторизованных пользователей в этих группах - раз в 5 минут.
  - Синхронизация участия авторизованных пользователей в LDAP-фильтрах - раз в 5 минут.
  - Синхронизация списка пользователей с контроллером домена - раз в 15 минут.
  - Проверка на контроллере домена наличия, включенности и соответствия логинов авторизованных пользователей - раз в 15 минут.
- ALD Pro:
  - Синхронизация импорта в дерево пользователей - раз в 15 минут.
  - Синхронизация списка групп пользователей ALD и участия пользователей в этих группах - раз в 5 минут.

Раздел включает пять вкладок:

- **Microsoft Active Directory/Samba DC** - интеграция с Microsoft Active Directory/Samba DC.
- **ALD Pro** - интеграция с ALD Pro.
- **FreeIPA** - интеграция с FreeIPA.
- **RADIUS** - интеграция с RADIUS-сервером (Remote Authentication Dial-In User Service).
- **LDAP-фильтры** - настройка объектов для группировки пользователей каталога AD LDAP (Lightweight Directory Access Protocol).

Active Directory/Samba DC

Классический контекст | Высокопроизводительный контекст | API

Настройка односторонней синхронизации с контроллером домена на базе Microsoft Active Directory (AD) и Samba DC.

Название службы раздела **Active Directory/Samba DC**: `ideco-ad-backend`, `ideco-ad-log-collector`.

Список служб для других разделов доступен по ссылке.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Видеоинструкция актуальна для версий до 20 включительно. С версии 21 не актуален раздел об импорте пользователей.

При интеграции в разделе **Пользователи → Учетные записи → Active Directory** отобразятся данные пользователей AD, исключая пароли. Аутентификация пользователей проверяется средствами Active Directory/Samba DC.

Поддерживаемые контроллеры домена:

- Windows Server 2008 (только R2), 2012, 2016, 2019, 2022, 2025.
- Samba DC с версии 4.0.
- RED ADM / РЕД АДМ 1.10.0.

Для ввода в домен на базе Windows Server 2025 и старше откройте Ideco NGFW Novum, перейдите в раздел **Управление сервером → Терминал** и выполните команду:

```
touch /run/ideco-ad-backend/ldap-passwd
```

Особенности интеграции с несколькими доменами

- Учетные записи пользователей из разных доменов могут иметь одинаковые логины. При аутентификации пользователь будет точно определен по указанному домену. Если домен не был указан пользователем, будет указан каталог по умолчанию.
- Пользователи всех интеграций отображаются в разделе **Пользователи → Учетные записи → Active Directory** в одном списке.
- Пользователи и группы безопасности будут видны и доступны к выбору в правилах трафика, настройках и поиске информации о пользователях AD, со всех интегрированных доменов. При наведении курсора на пользователя или группу безопасности AD выводится информация о принадлежности пользователя домену. Список обновляется каждые 15 минут.

- При SSO-авторизации и первом открытии браузера пользователю будет предложен выбор домена для аутентификации. Выбор сохраняется с помощью cookie и используется при следующей авторизации. Если требуется изменить домен, очистите cookie (для локального IP-адреса NGFW Novum).

Ввод сервера в домен

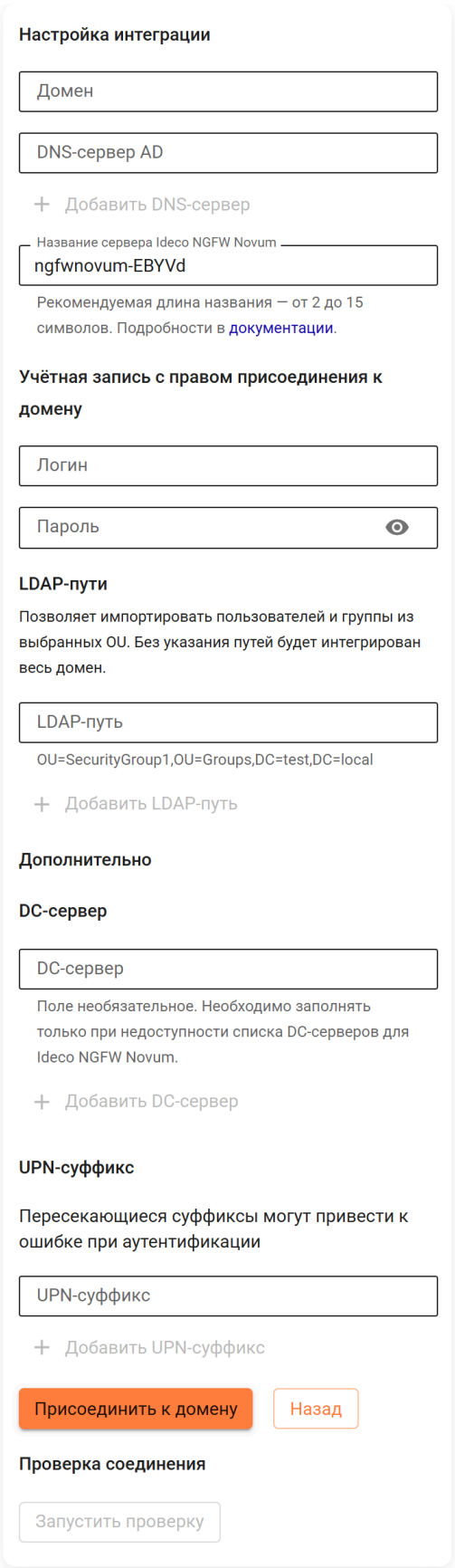
Перед вводом в домен:

- Убедитесь, что время на контроллере домена и NGFW Novum совпадает.
- Убедитесь, что хотя бы один контроллер домена находится в локальной сети NGFW Novum или доступен через локальный интерфейс с помощью настроенной маршрутизации.

Выполните действия:

1. Перейдите в **Пользователи** → **Внешние каталоги** → **Active Directory/Samba DC**.

2. Нажмите **Добавить** и заполните поля:



Если в поле **Название сервера Ideco NGFW Novum** указано более 15 символов, будут недоступны виды аутентификации пользователей AD:

- **SSO через AD и ALD Pro** с токенами NTLM.
- VPN (IKEv2, SSTP, L2TP/IPsec).
- Ideco Client с аутентификаций по логину и паролю.

NetBIOS-имя сервера ограничено 15 символами. При превышении длины название усекается, что вызывает несоответствия при аутентификации, в том числе ошибки SSO из-за некорректного SPN (Service Principal Name).

Расшифровка полей

- **Домен** - полное наименование домена, максимальная длина 64 символа. Например: `mydomain.example`.
- **DNS-сервер AD** - адрес сервера, обладающий ролью DNS-сервера в контроллере домена. Должен быть доступен с любого интерфейса NGFW Novum.
- **Название сервера Ideco NGFW Novum** - имя компьютера, под которым NGFW Novum будет введен в домен. Не более 15 символов.
- **Учетная запись с правом присоединения к домену** - учетная запись AD с правами присоединения к домену (право **Создание объектов: Компьютер**).При заполнении поля домен указывать не требуется. Логин и пароль этой учетной записи используются однократно только для ввода в домен и не сохраняются в Ideco NGFW Novum. После успешного присоединения можно отозвать права, удалить учетную запись или сменить пароль - это не повлияет на дальнейшую работу интеграции.

Чтение домена осуществляется учетной записью типа **Компьютер**. Не удаляйте и не ограничивайте права ни этой учетной записи, ни группе **Доменные компьютеры**. Подробности о необходимых правах для Active Directory можно найти в статье.

- **LDAP-пути** - LDAP-пути для выбора пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет избежать синхронизации с NGFW Novum всего дерева пользователей AD и выбрать только нужные группы.
- **DC-сервер** - контроллер домена. Указывается при недоступности контроллера домена для NGFW Novum или при использовании распределенной корпоративной сети. Можно ввести до 30 DC-серверов.
- **UPN-суффикс** - альтернативные суффиксы `userPrincipalName`. При необходимости можно ввести до 64 UPN-суффиксов. Необходимо указать UPN-суффиксы, если они используются на контроллере домена:

Один и тот же пользователь может войти в NGFW Novum, используя как `sAMAccountName` (SAM), так и дополнительный UPN-суффикс, если он выбран в поле **Имя входа пользователя**:

Указанные UPN-суффиксы отображаются в таблице **Алгоритм аутентификации** в разделе Аутентификация.
3. Нажмите **Присоединить к домену**. Процесс присоединения к домену может занять до одной минуты.

Если в таблице большое количество интеграций, воспользуйтесь кнопкой **Фильтры**.

Алгоритм выбора контроллера домена

Если поле **DC-сервер** не заполнено, NGFW Novum выбирает контроллер домена автоматически:

1. NGFW Novum выполняет DNS-запрос к SRV-записи `_ldap._tcp.<имя домена>` - в ответ возвращается список доступных контроллеров домена.

2. NGFW Novum последовательно проверяет контроллеры домена в случайном порядке на доступность и использует первый ответивший.

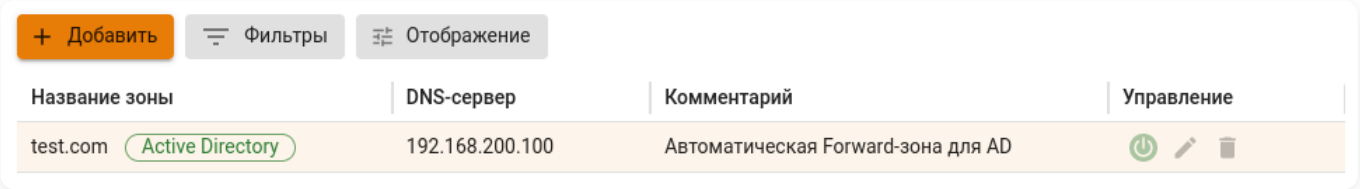
Если в поле **DC-сервер** указаны контроллеры домена, NGFW Novum последовательно проверяет доступность каждого из них и при отсутствии ответа переходит к следующему.

При потере связи с текущим контроллером домена NGFW Novum выполняет новый выбор контроллера в соответствии с алгоритмом.

При использовании распределенной корпоративной сети указывайте контроллеры домена в поле **DC-сервер**, чтобы обеспечить подключение **только к нужным контроллерам** домена.

Настройка DNS для разрешения имен локального домена

В Ideco NGFW Novum Forward-зона DNS создается в **Сервисы** → **DNS** автоматически при вводе сервера в домен:



При настройке компьютеры могут использовать NGFW Novum в качестве основного DNS-сервера. При этом разрешение локальных и интернет-имен будет работать корректно для всех сервисов.

Пользовательские Forward-зоны DNS всегда имеют приоритет над автоматически созданной Forward-зоной для Active Directory.

Удаление интеграции с Active Directory

Для вывода NGFW Novum из домена перейдите в **Пользователи** → **Внешние каталоги** → **Active Directory/Samba DC** и нажмите напротив интеграции. После подтверждения:

- NGFW Novum будет выведен из домена.
- Удалятся все настройки интеграции с контроллером домена.
- Удалятся все пользователи и группы, синхронизированные с доменом.
- В AD созданный для NGFW Novum компьютер не удалится.

После удаления интеграции с Active Directory автоматическая запись в **Сервисы** → **DNS** → **Forward-зоны** должна отсутствовать. Если запись не удалена, обратитесь в Техническую поддержку.

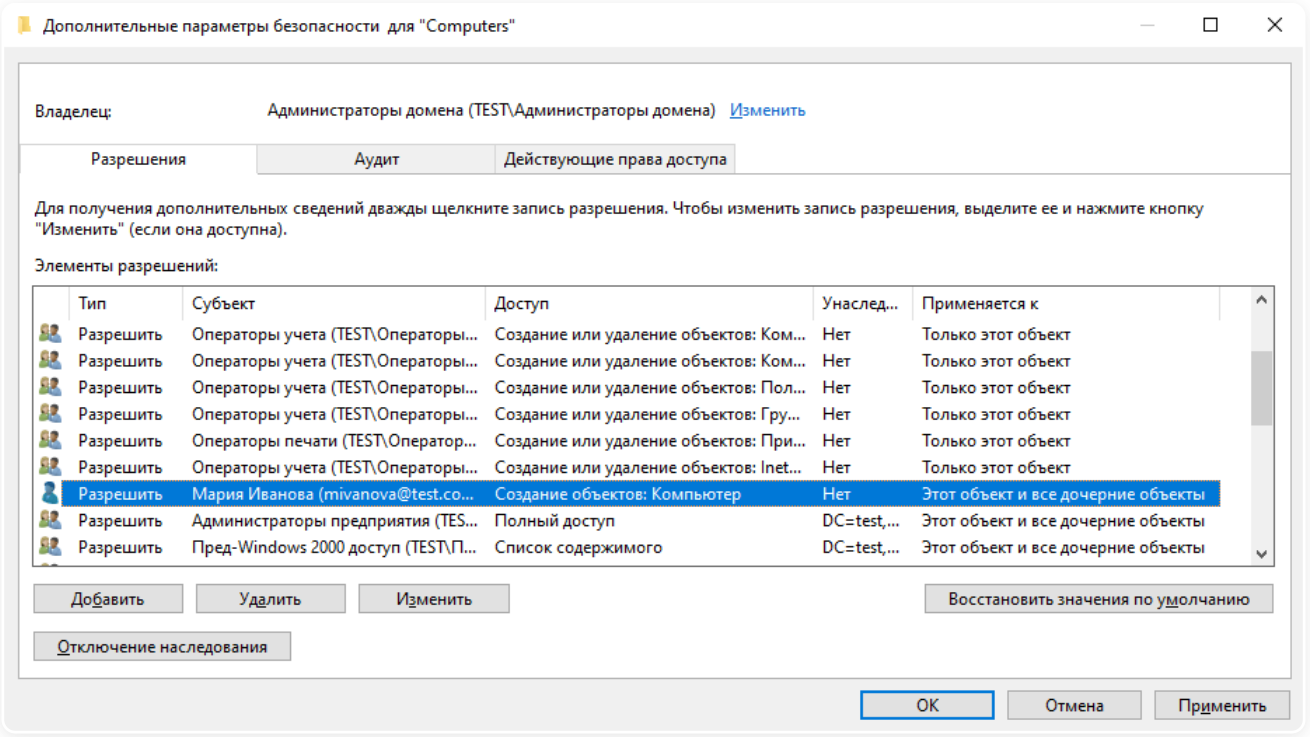
Полезные ссылки

- **Настройка корневого и подчиненного центра сертификации с помощью AD CS**

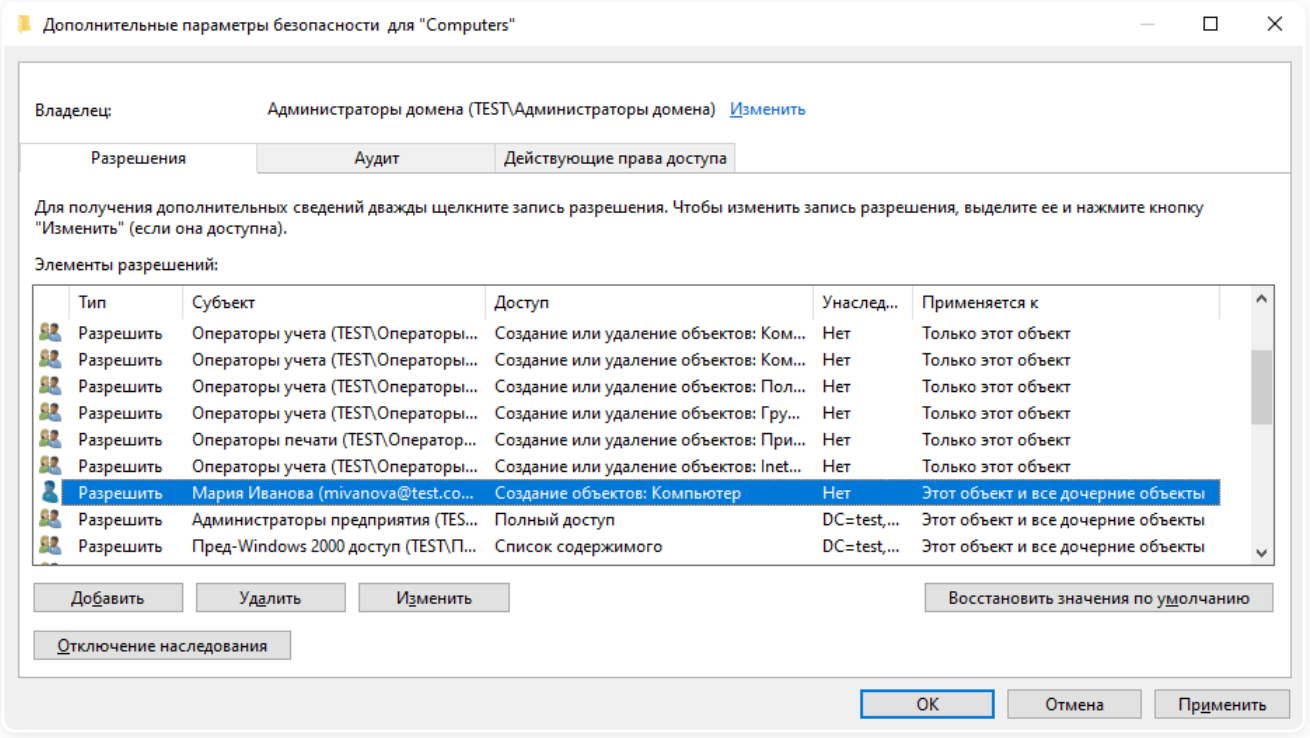
Настройка прав для интеграции Active Directory

Классический контекст | Высокопроизводительный контекст

Для интеграции Ideco NGFW Novum с Active Directory используйте существующую или создайте новую учетную запись с разрешением **Создание объектов: Компьютер**:



Учетная запись используется только при настройке или перенастройке интеграции на NGFW Novum в **Пользователи** → **Active Directory/Samba DC**:



После добавления интеграции на сервере Active Directory будет создана учетная запись компьютера для Ideco NGFW Novum. Она будет использоваться для NGFW Novum в течение всего периода работы и обладает следующими правами:

Область применения	Необходимые права и атрибуты

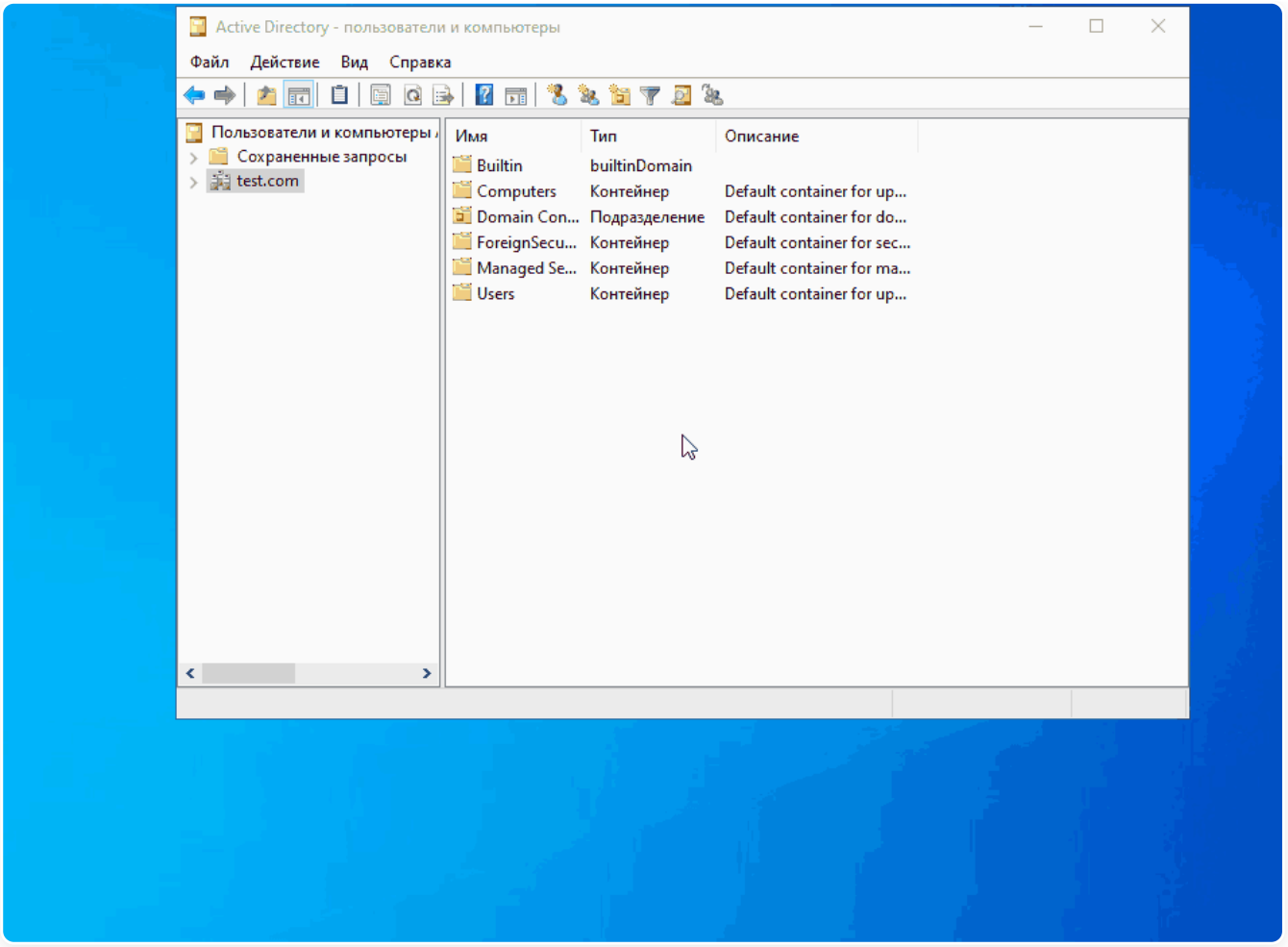
Поиск пользователей	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ name
	  ◦ modifyTimeStamp
	  ◦ objectGUID
	  ◦ objectSid
	  ◦ cn
	  ◦ displayName
	  ◦ login
	  ◦ mobile
	  ◦ objectClass
	  ◦ userAccountControl
	  ◦ sAMAccountName
	  ◦ userPrincipalName
	  ◦ accountExpires
	  ◦ msDS-UserPasswordExpiryTimeComputed
	  ◦ description
	• Предоставляет доступ **ListChildren** просматривать содержимое OU (Organizational Unit).

Поиск групп в OU	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ name
	  ◦ modifyTimeStamp
	  ◦ objectGUID
	  ◦ objectSid
	• Предоставляет доступ **ListChildren** просматривать содержимое OU (Organizational Unit).

Поиск в конфигурации разделов	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ cn (Common Name)
	  ◦ nETBIOSName
	  ◦ nCName
	• Предоставляет доступ к контейнеру **CN=Configuration**.

Проверка текущих прав пользователя через GUI

Откройте **Active Directory Users and Computers** (**Пользователи и Компьютеры Active Directory**) и выполните действия:



1. Включите **View** → **Advanced Features** (**Вид** → **Дополнительные компоненты**).

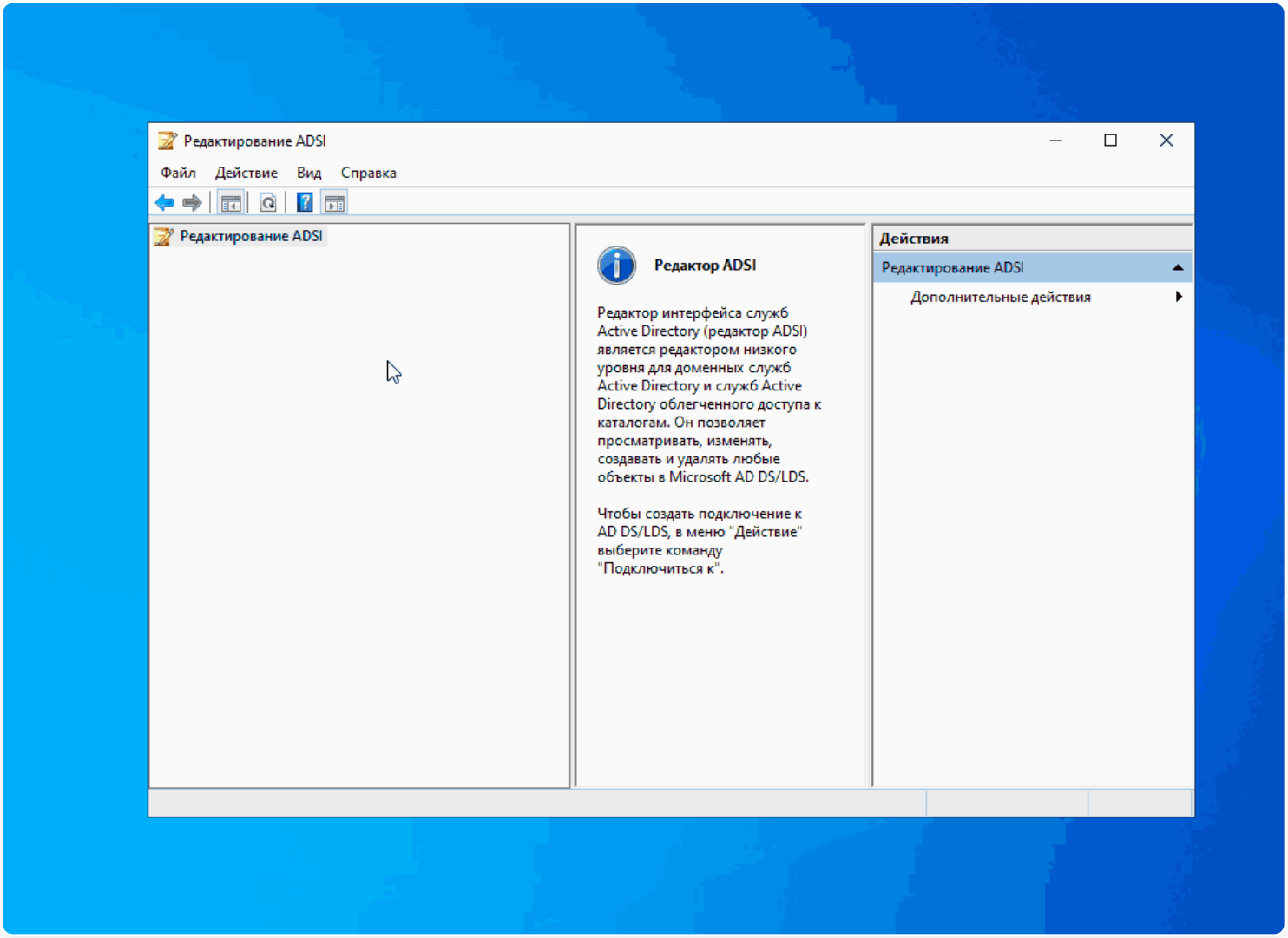
2. Нажмите правой кнопкой на объекте домена, выберите **Properties** → **Security** → **Advanced** (**Свойства** → **Безопасность** → **Дополнительно**).

3. Перейдите на вкладку **Effective Access** (**Действующие права доступа**).

4. Добавьте пользователя/компьютер, чьи права необходимо проверить, и нажмите **View effective access** (**Посмотреть действующие разрешения**).

Проверка прав для конфигурации разделов через GUI

Откройте **ADSI Edit** (**Редактирование ADSI**) командой `adsiedit.msc` в командной строке сервера и выполните действия:



1. Нажмите правой кнопкой на **ADSI Edit** (**Редактирование ADSI**) и выберите **Connect to...** (**Подключиться к...**).

2. Подключитесь к разделу **Configuration** (**Конфигурация**), выбрав **Configuration** (**Конфигурация**) в разделе **Select a well known Naming Context** (**Выберите известный контекст именования**).

3. Перейдите по пути: **CN=Configuration,DC=test1,DC=internal** → **CN=Partitions**.

4. Нажмите правой кнопкой на **CN=Partitions** и выберите **Properties** → **Security** → **Advanced** (**Свойства** → **Безопасность** → **Дополнительно**).

5. Перейдите на вкладку **Effective Access** (**Действующие права доступа**).

6. Добавьте пользователя/компьютер, чьи права необходимо проверить, и нажмите **View effective access** (**Посмотреть действующие разрешения**).

Команды для проверки текущих прав

Через PowerShell

Права для ввода сервера в домен

```
$domain = [ADSI]"LDAP://dc=test1,dc=internal"
$domain.psbase.ObjectSecurity.Access | Format-Table IdentityReference, ActiveDirectoryRights, AccessControlType -AutoSize
```

- `LDAP://dc=test1,dc=internal` - LDAP-путь до корневого домена **test1.internal**.
- `Format-Table IdentityReference, ActiveDirectoryRights, AccessControlType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `AccessControlType` - тип доступа: `allow` (разрешить) или `deny` (запретить).

Поиск пользователей в домене

```
(Get-Acl "AD:\DC=test1,DC=internal").Access |
Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"} |
Format-Table IdentityReference,ActiveDirectoryRights,ObjectType -AutoSize
```

- `AD:\DC=test1,DC=internal` - LDAP-путь до корневого домена **test1.internal**.
- `Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"}` - фильтрация ACL записи, оставляя только те, где **IdentityReference** равен **ngfw-qqtfdk** (имя компьютера, под которым Ideco NGFW Novum будет введен в домен).
- `Format-Table IdentityReference,ActiveDirectoryRights,ObjectType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `ObjectType` - GUID объекта AD, к которому применяются права.

Поиск групп в OU Users и Computers

```
(Get-Acl "AD:\OU=Users,OU=Computers,DC=test1,DC=internal").Access |
Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"} |
Format-Table IdentityReference,ActiveDirectoryRights,ObjectType -AutoSize
```

- `AD:\OU=Users,OU=Computers,DC=test1,DC=internal` - LDAP-путь до организационной единицы **Users**, расположенной внутри **Computers** домена **test1.internal**.
- `Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"}` - фильтрация ACL записи, оставляя только те, где **IdentityReference** равен **ngfw-qqtfdk** (имя компьютера, под которым Ideco NGFW Novum будет введен в домен).
- `Format-Table IdentityReference,ActiveDirectoryRights,ObjectType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `ObjectType` - GUID объекта AD, к которому применяются права.

Поиск в конфигурации разделов

```
(Get-Acl "AD:\CN=Partitions,CN=Configuration,DC=test1,DC=internal").Access |
Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"} |
Format-Table IdentityReference,ActiveDirectoryRights,ObjectType -AutoSize
```

- `AD:\CN=Partitions,CN=Configuration,DC=test1,DC=internal` - LDAP-путь до контейнера **Partitions** в разделе **Configuration** домена **test1.internal**.
- `Where-Object {$_.IdentityReference -eq "test1\ngfw-qqtfdk$"}` - фильтрация ACL записи, оставляя только те, где **IdentityReference** равен **ngfw-qqtfdk** (имя компьютера, под которым Ideco NGFW Novum будет введен в домен).
- `Format-Table IdentityReference,ActiveDirectoryRights,ObjectType` - форматирует вывод в таблицу, где:
  - `IdentityReference` - пользователь/группа, которым назначены права.
  - `ActiveDirectoryRights` - тип прав, например, **ReadProperty**.
  - `ObjectType` - GUID объекта AD, к которому применяются права.

Через Dsacls

Права для ввода сервера в домен и поиск пользователей в домене

```
dsacls "DC=test1,DC=internal"
```

- `DC=test1,DC=internal` - LDAP-путь до корневого домена **test1.internal**.

Поиск групп в OU Users и Computers

```
dsacls "OU=Users,OU=Computers,DC=test1,DC=internal"
```

- `OU=Users,OU=Computers,DC=test1,DC=internal` - LDAP-путь до организационной единицы **Users**, расположенной внутри **Computers** домена **test1.internal**.

Поиск в конфигурации разделов

```
dsacls "CN=Partitions,CN=Configuration,DC=test1,DC=internal"
```

- `CN=Partitions,CN=Configuration,DC=test1,DC=internal` - LDAP-путь до контейнера **Partitions** в разделе **Configuration** домена **test1.internal**.

Аутентификация пользователей AD/Samba DC

Классический контекст | Высокопроизводительный контекст

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE



Видеоинструкция актуальна для всех версий, но с версии 21 потребуется дополнительно настроить **Разрешенные объекты** (см. в этой статье).

Настройка по типам аутентификации пользователей AD/Samba DC описана в статьях:

- **Настройка веб-аутентификации**
- **Настройка SSO-аутентификации**
- **Настройка авторизации через журнал безопасности AD**

Авторизация

Для пользователей Active Directory доступны все типы авторизации. Для пользователей Samba доступны все типы авторизации, кроме авторизации через журнал безопасности.

Чтобы пользователи SambaDC могли использовать VPN-подключение, необходимо включить **NTLM-авторизацию**. Для этого отредактируйте файл с помощью команды `nano /etc/samba/smb.conf`, добавив в секцию `[global]` строку `ntlm auth = yes`.

Способы аутентификации импортированных пользователей:

- **Через Ideco Client** - подходит для SSO-авторизации и для авторизации по логину и паролю из AD. Также используется для авторизации пользователей терминальных серверов Windows.
- **Авторизация по IP-адресу** - подходит для пользователей с фиксированным IP-адресом. IP-адреса на NGFW необходимо прописать вручную каждому пользователю.
- **Авторизация по VPN** - подходит для пользователей удаленных сетей.
- **Авторизация через журналы AD** - прохождение трафика инициирует создание сессии авторизации (так же как IP/MAC).

Особенности авторизации пользователей доверенных доменов

Если у домена, в который введен NGFW Novum, настроено доверие с другим доменом, то пользователи доверенного домена смогут авторизоваться на NGFW Novum при выполнении условий:

- Между доменами настроено доверие Forest - Forest. **Другие типы доверия между доменами не поддерживаются**. Для авторизации пользователей доменов с другим типом доверия необходима настройка интеграции с этими доменами.
- Пользователи доверенного домена могут авторизоваться только с помощью SSO через веб-аутентификацию, другие виды аутентификации и авторизации им недоступны.

- Пользователь доверенного домена должен быть добавлен в AD как ForeignSecurityPrincipal и находиться в локальной группе безопасности, которой разрешена веб-авторизация/аутентификация.

Пользователи доверенного домена отобразятся в разделе **Пользователи** → **Учетные записи** → **Active Directory** наряду с другими пользователями AD.

Полезные ссылки

- **Настройка прав для интеграции Active Directory**
- **Скрипты автоматической разавторизации**

Настройка SSO-аутентификации

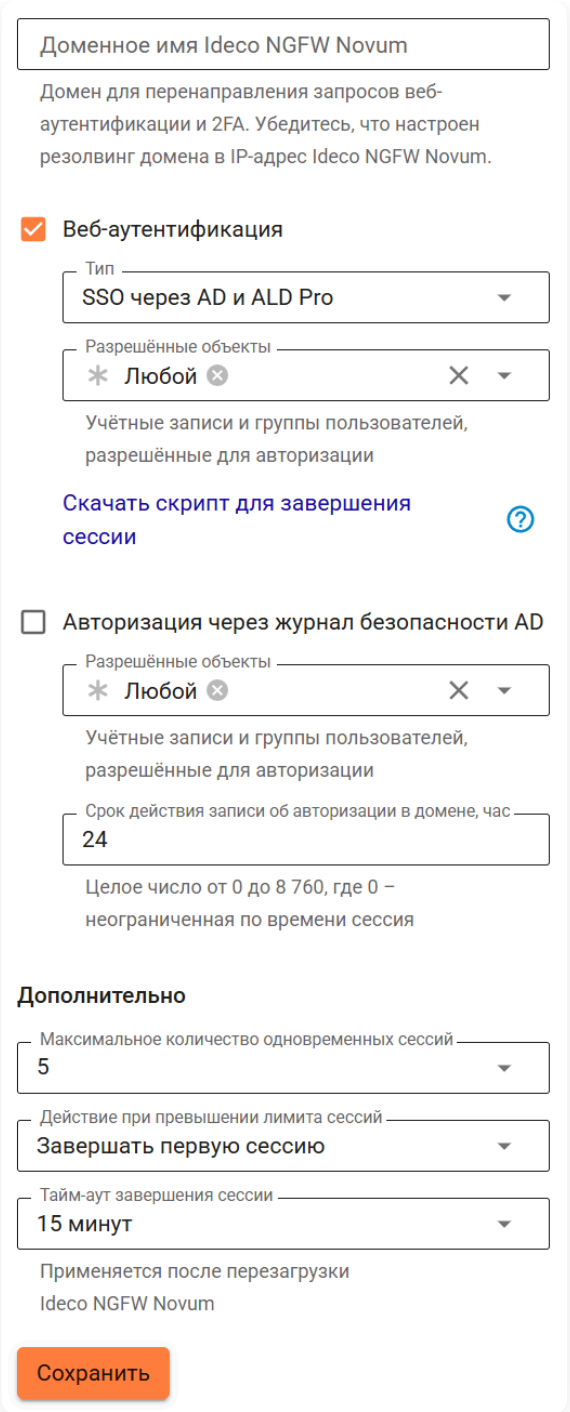
Классический контекст | Высокопроизводительный контекст

Название службы раздела **Веб-аутентификация**: `ideco-web-authd`, `ideco-web-backend`.

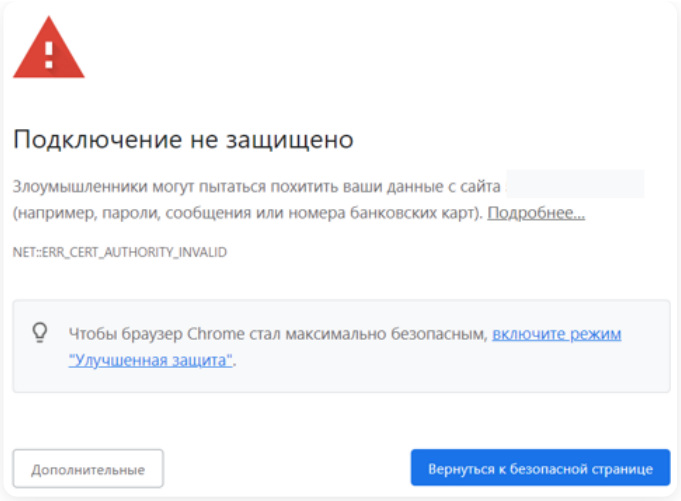
Список служб для других разделов доступен по ссылке.

Настройка SSO-аутентификации на стороне NGFW Novum

Перейдите в **Пользователи** → **Авторизация** → **Настройки** и заполните поля:



- **Доменное имя Ideco NGFW Novum** - укажите доменное имя Ideco NGFW Novum.
- **Веб-аутентификация** - включите настройку и выберите **SSO через AD и ALD Pro** для авторизации с использованием токенов Kerberos или NTLM.
- **Авторизация через журнал безопасности Active Directory** - включите, чтобы Ideco NGFW Novum отслеживал события успешного входа в журнале безопасности AD и авторизовывал пользователя по ним, если трафик идет с того же IP-адреса.
- **Тайм-аут завершения сессии** - установите тайм-аут завершения сессии пользователей. Значение по умолчанию - 15 минут. Диапазон доступных значений - от 10 минут до 1 дня.
  После сохранения настроек будет выдан Let's Encrypt сертификат, пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



Если сертификат для такого домена уже загружен в разделе **Сертификаты**, то будет использоваться загруженный сертификат. Новый сертификат выдаваться не будет.

Выбор каталога при SSO-аутентификации

Каталог для проверки учетных данных выбирается **только среди интеграций с AD и ALD Pro** одним из способов:

- **Неявно** - если настроена только одна интеграция с AD или ALD Pro, она используется автоматически.
- **Явно** - если настроены две или более интеграции, при первом открытии браузера пользователю предлагается выбрать домен для аутентификации. Выбор сохраняется с помощью cookie и используется при последующих авторизациях. Чтобы сменить домен, очистите cookie для локального IP-адреса NGFW Novum.

Каталог выбирается до проверки учетных данных. Если на компьютере не найден SSO-токен и браузер показывает **системное окно ввода логина и пароля** (запрос NTLM), действуют те же правила:

- Учетные данные проверяются **только в уже выбранном каталоге** AD или ALD Pro. Стандартный алгоритм выбора каталога (с **Каталогом по умолчанию** и доменным суффиксом) к этому запросу не применяется.
- В системное окно NTLM можно ввести **только доменную учетную запись** выбранного каталога. Локальная учетная запись не сработает, даже если локальный каталог задан как **Каталог по умолчанию**. Для авторизации локальных пользователей отключите SSO и используйте веб-аутентификацию по логину и паролю - на ее странице доступны локальные и доменные учетные записи.

Пример выбора каталога при двух интеграциях

Настроены две интеграции - домены `example.ru` и `test.ru`. У пользователя `ivanov` есть учетная запись в обоих доменах:

1. Пользователь первый раз открывает браузер и переходит на любой сайт.

2. Ideco NGFW Novum перенаправляет его на страницу выбора домена. Пользователь выбирает `example.ru`.

3. Браузер передает SSO-токен (или, при его отсутствии, запрашивает логин и пароль). Учетные данные проверяются только в каталоге `example.ru`, даже если такой же логин есть в `test.ru`.

4. Выбор `example.ru` сохраняется в cookie. При следующих авторизациях домен не запрашивается. Чтобы авторизоваться в `test.ru`, пользователю нужно очистить cookie для локального IP-адреса NGFW Novum и выбрать другой домен.

Настройка клиентских компьютеров

Настройка зоны интрасети Windows

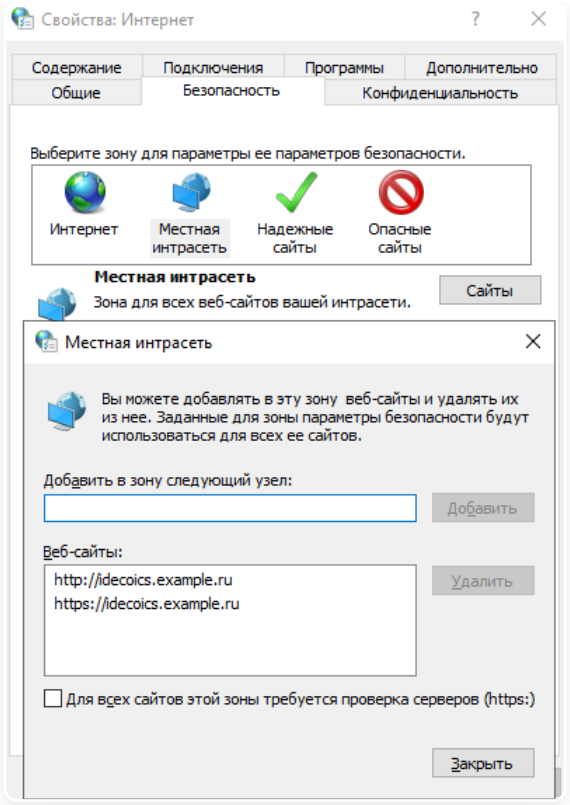
1. В поиск введите **Изменение параметров временных файлов интернета**.

2. В открывшемся окне перейдите на вкладку **Безопасность**.

3. Выберите **Местная интрасеть** → **Сайты**.

4. Добавьте в открывшемся окне ссылку на Ideco NGFW Novum под тем именем, под которым ввели Ideco NGFW Novum в домен. Нужно указывать два URL: с `http://` и с `https://`.

Пример ввода Ideco NGFW Novum в домен `example.ru` под именем `idecoics`:



Настройка браузеров для SSO-аутентификации по протоколам NTLM и Kerberos

В приватных режимах браузеров (**Инкогнито**, **Приватное окно** и аналогичных) SSO-аутентификация по умолчанию не работает: браузеры в таких режимах отключают автоматическую передачу учетных данных по протоколам NTLM и Kerberos. В этом случае пользователю потребуется ввести логин и пароль вручную.

Mozilla Firefox

Порядок настройки

1. В адресной строке Mozilla Firefox введите `about:config` и подтвердите переход.

2. В строке поиска найдите и отредактируйте параметры, установив указанные значения:

Параметр	Значение	Описание
`network.automatic-ntlm-auth.trusted-uris`	Доменное имя Ideco NGFW Novum (например, `idecoics.example.ru`)	Список серверов, для которых разрешена автоматическая NTLM-аутентификация.
`network.negotiate-auth.trusted-uris`	Доменное имя Ideco NGFW Novum (например, `idecoics.example.ru`)	Список серверов, для которых разрешена автоматическая аутентификация Negotiate (Kerberos).
`security.enterprise_roots.enabled`	`true`	Позволяет Mozilla Firefox доверять корневым сертификатам, установленным в операционной системе (необходимо для корректной работы на HTTPS-сайтах).

Важно:

- В значениях необходимо указывать именно доменное имя Ideco NGFW Novum, под которым он доступен в сети (например, `idecoics.example.ru`), а не IP-адрес.
- Доменное имя можно указать с точкой в начале значения, чтобы правило автоматически применялось к домену и всем его поддоменам. Например, `.example.ru` автоматически применит правило к `example.ru` и всем его поддоменам (`sub.example.ru`, `idecoics.example.ru`).
- Если требуется указать несколько адресов, используйте запятую в качестве разделителя.

Как работает аутентификация в Firefox

Mozilla Firefox использует механизм согласования SPNEGO:

1. Браузер пытается выполнить аутентификацию по протоколу Kerberos (более безопасный и быстрый). Аутентификация возможна при условиях:

- Компьютер входит в домен Active Directory.
- Ideco NGFW Novum интегрирован в домен и настроен Service Principal Name (SPN).

2. Если аутентификация по Kerberos невозможна (например, компьютер не в домене или отсутствует билет), браузер автоматически переключается на протокол NTLM.

Для успешной работы обоих механизмов необходимо настроить оба семейства параметров (`negotiate` и `ntlm`). Если настроен только один из протоколов:

- Автоматическая аутентификация будет работать лишь в сценариях, где этот протокол поддерживается и клиентом, и сервером.
- При использовании только Kerberos недоменные компьютеры или машины с проблемами получения билета не смогут авторизоваться.
- При использовании только NTLM в доменной среде не будет задействован Kerberos, хотя аутентификация останется возможной.

Chromium

Порядок настройки

1. Откройте редактор реестра, нажав **Win+R** и введя `regedit`.

2. В редакторе реестра перейдите по одному из путей:

- Для применения ко всем пользователям компьютера - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Chromium`.
- Для применения к текущему пользователю - `HKEY_CURRENT_USER\SOFTWARE\Policies\Chromium`.

Если используется другой браузер, путь может отличаться:

- **Google Chrome** - `...\Policies\Google\Chrome`.
- **Microsoft Edge** - `...\Policies\Microsoft\Edge`.
- **Яндекс Браузер** - `...\Policies\Yandex\Browser`.

3. Создайте новый параметр с типом `REG_SZ`:

Параметр	Значение	Описание
`AuthServerAllowlist`	Доменное имя Ideco NGFW Novum (например, `idecoics.example.ru`)	Список серверов, для которых разрешена автоматическая аутентификация по протоколам NTLM и Kerberos (Negotiate). Если сервер не входит в этот список, браузер будет запрашивать логин и пароль.

Если ранее была выполнена настройка зоны интрасети Windows, параметр `AuthServerAllowlist` подхватывается браузером автоматически. Ручная установка потребуется, если настройка зоны интрасети не применялась.

Важно:

- В значениях необходимо указывать именно доменное имя Ideco NGFW Novum, под которым он доступен в сети (например, `idecoics.example.ru`), а не IP-адрес.
- Доменное имя можно указать с символом `*` в начале значения. Например, `*.example.ru`. Тогда правило будет автоматически применяться к основному домену `example.ru` и ко всем его поддоменам.
- Если требуется указать несколько адресов, используйте запятую в качестве разделителя.

Как работает аутентификация в Chromium

Браузеры Chromium используют механизм согласования SPNEGO:

1. Браузер пытается выполнить аутентификацию по протоколу Kerberos (более безопасный и быстрый). Аутентификация возможна при условиях:

- Компьютер входит в домен Active Directory.
- Ideco NGFW Novum интегрирован в домен и настроен Service Principal Name (SPN).

2. Если аутентификация по Kerberos невозможна (например, компьютер не в домене или отсутствует билет), браузер автоматически переключается на протокол NTLM.

Для успешной работы обоих механизмов необходимо настроить оба семейства параметров (`negotiate` и `ntlm`). Если настроен только один из протоколов:

- Автоматическая аутентификация будет работать лишь в сценариях, где этот протокол поддерживается и клиентом, и сервером.
- При использовании только Kerberos недоменные компьютеры или машины с проблемами получения билета не смогут авторизоваться.
- При использовании только NTLM в доменной среде не будет задействован Kerberos, хотя аутентификация останется возможной.

Настройка на стороне сервера Active Directory

Применение настройки ко всем пользователям Active Directory

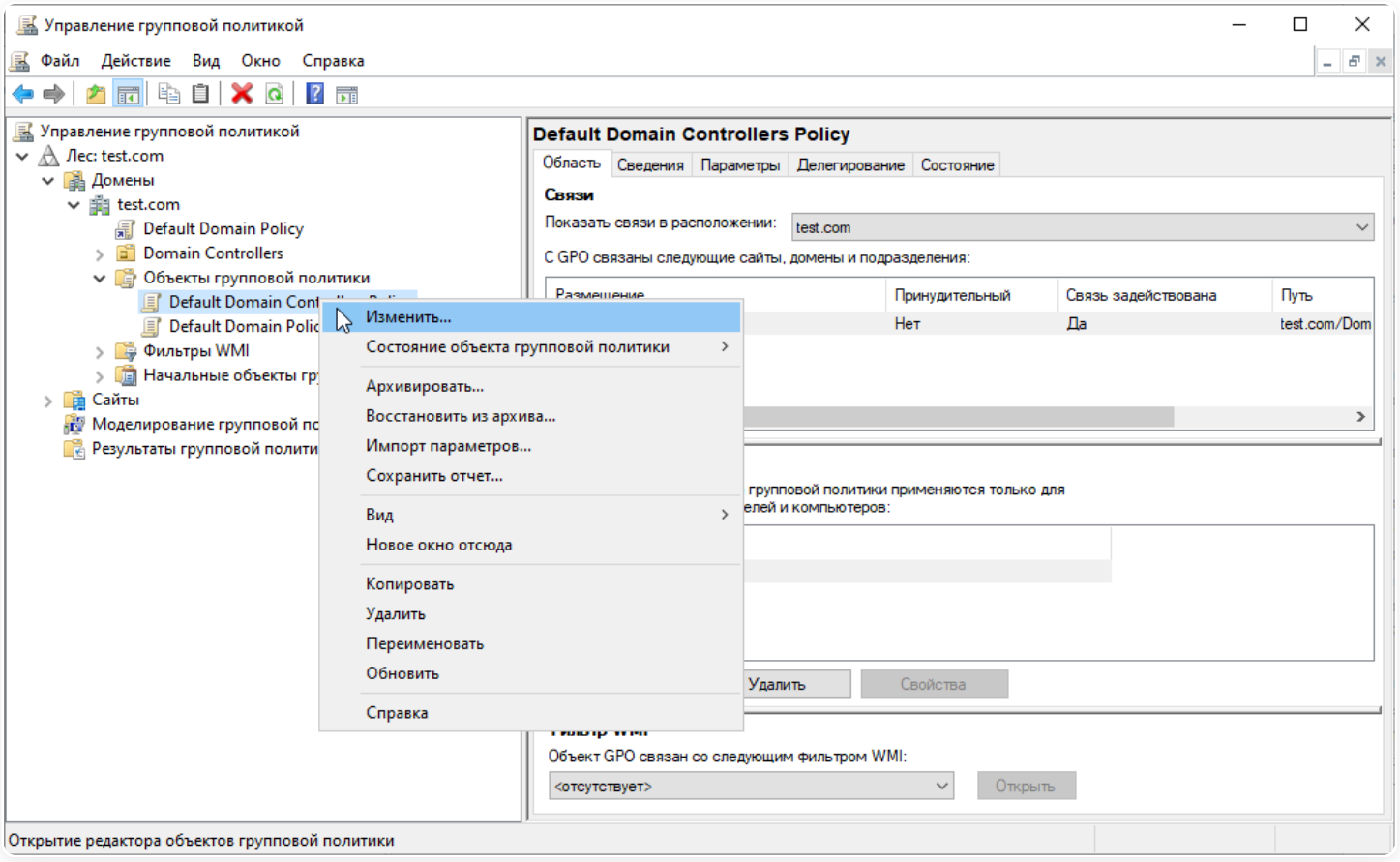
1. Откройте **Управление групповой политикой**. Это можно сделать, нажав клавиши **Win + R** и введя в появившемся окне команду gpmc.msc.

2. Перейдите по пути:

Англоязычная версия

Group Policy Management → Forest → Domains → <ваш домен> → Group Policy Objects.
Русскоязычная версия

Управление групповой политикой → Лес → Домены → <ваш домен> → Объекты групповой политики.
3. Нажмите правой кнопкой на нужный объект групповой политики и выберите **Изменить**:

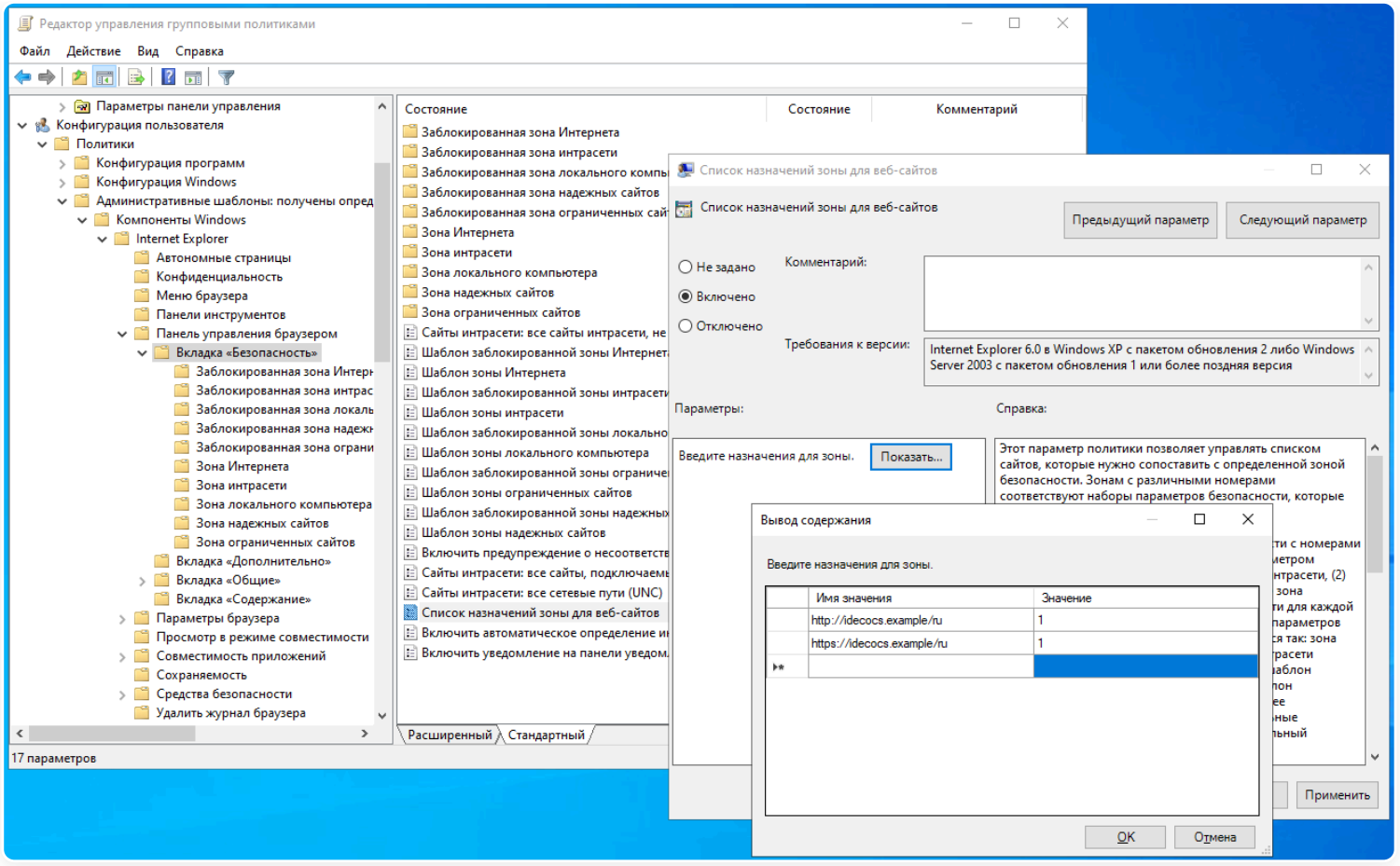


4. Перейдите по пути:

Англоязычная версия

Group Policy Management Editor → User Configuration → Policies → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Security Page → Site to Zone Assignment List.
Русскоязычная версия

Редактор управления групповыми политиками → Конфигурация пользователя → Политики → Административные шаблоны → Компоненты Windows → Internet Explorer → Панель управления браузером → Вкладка «Безопасность» → Список назначений зоны для веб-сайтов.
5. Введите назначение зоны для DNS-имени Ideco NGFW Novum (в примере idecoics.example.ru) со значением `1` (интрасеть). Укажите два назначения для схем работы по `http` и `https`:

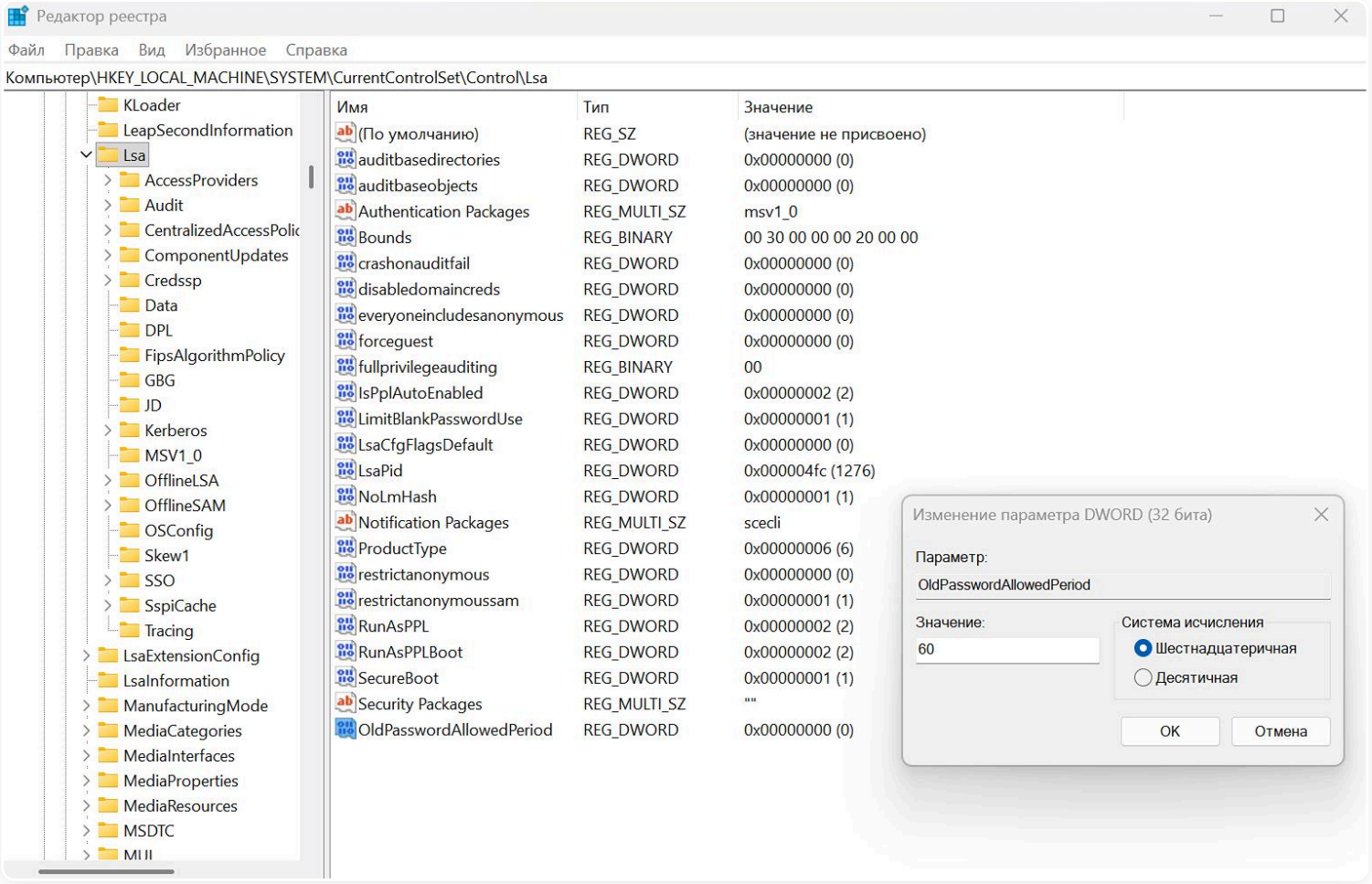


При входе на HTTPS-сайт необходимо разрешить браузеру доверять сертификату Ideco NGFW Novum. Чтобы не делать это каждый раз, можно добавить корневой сертификат Ideco NGFW Novum в доверенные корневые сертификаты устройства.

Особенности использования NTLM-токенов

При использовании NTLM-токенов для веб-аутентификации, а также при VPN авторизации необходимо учитывать период действия старого пароля пользователя. Если политика домена AD **Enforce Password History** установлена на хранение двух и более старых паролей, то контроллеры успешно аутентифицируют через NTLM пользователя с использованием старого пароля еще некоторое время после изменения пароля. По умолчанию в течение **5 минут**.

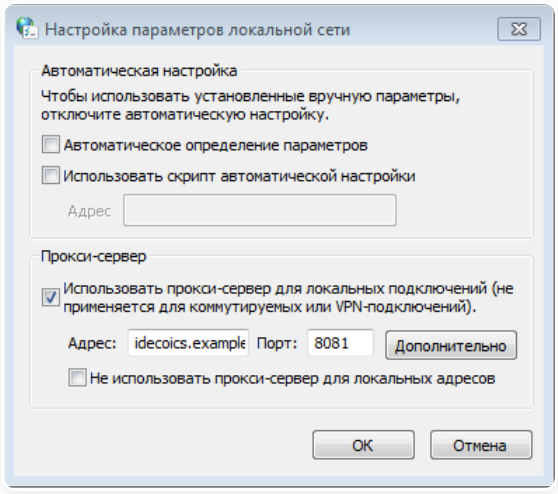
Период действия старого пароля можно настроить с помощью редактирования реестра на контроллере домена. Для этого нужно добавить параметр `DWORD` с именем `OldPasswordAllowedPeriod` в ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`. В поле **Значение** указать период в минутах. Изменение периода действия старого пароля не требует перезагрузки:



Настройка аутентификации пользователей при прямых подключениях к прокси-серверу

Настройка прозрачной аутентификации пользователей при прямых подключениях к прокси-серверу аналогична настройке прозрачной **SSO-аутентификации**.

Единственная особенность - укажите в качестве адреса прокси-сервера **DNS-имя Ideco NGFW Novum**:



При прямых подключениях к прокси **не указывайте** в качестве шлюза IP-адрес Ideco NGFW Novum.

Настройка браузера Mozilla Firefox для аутентификации по NTLM при прямом подключении к прокси-серверу

Для аутентификации компьютеров, которые **не находятся в домене**, под доменным пользовательским аккаунтом на странице настроек браузера **Mozilla Firefox** (введите ***about:config*** в адресной строке) укажите следующие параметры:

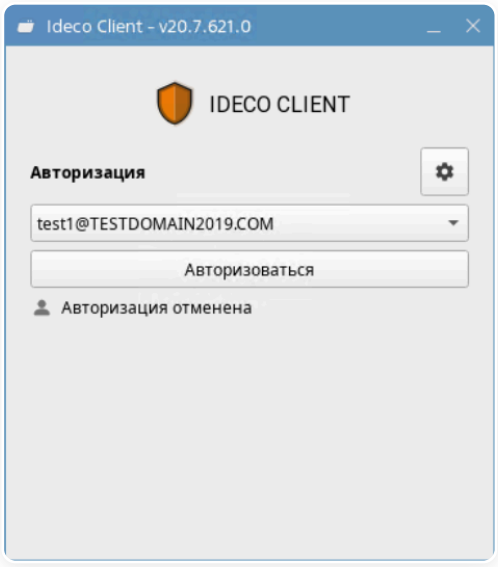
- **network.automatic-ntlm-auth.allow-proxies** = false.
- **network.negotiate-auth.allow-proxies** = false.

Не указывайте в параметрах значение `true` для компьютеров, входящих в домен, т. к. в таком случае будет использоваться устаревший метод авторизации по NTLM.

Возможные проблемы

Авторизация отменена

Проблема: после ввода в домен и настройки SSO-аутентификации попытка авторизации через SSO-профиль не проходит, и Ideco Client выдает ошибку **Авторизация отменена**:



Возникновение такой ошибки может быть связано с неправильной настройкой сети или интеграции NGFW Novum с Active Directory. Ideco Client пытается получить токен для авторизации на NGFW Novum. Но NGFW Novum нет в списках сервисов AD на контроллере домена, и токен получить невозможно.

Для диагностики выполните шаги:

1. Проверьте наличие сети между пользовательской машиной и контроллером домена.

2. Убедитесь, что учетная запись типа **Компьютер** для NGFW Novum на контроллере домена не удалена и имеет необходимые права.

3. Проверьте, что настройки интеграции пользовательского компьютера с AD и NGFW Novum с AD совпадают. Это возможно сделать на контроллере домена или с помощью команды:

```
ldapsearch -H ldap://<имя-контроллера-домена>.<имя-домена> -b "DC=<уровень-домена-(N)>,DC=<уровень-домена-(N-1)>" "(servicePr
```

- `-H ldap://<имя-контроллера-домена>.<имя-домена>` – указывает URL контроллера домена, к которому отправляется запрос;
- `-b "DC=<уровень-домена-(N)>,DC=<уровень-домена-(N-1)>"` – задает базовый DN (Distinguished Name) для поиска. Например, `DC=corp,DC=example,DC=com`;
- `"(servicePrincipalName=*/<имя-NGFW>.<имя-домена>*)"` – ищет объекты, у которых атрибут `servicePrincipalName` содержит строку вида `*/<имя-NGFW>.<имя-домена>*`. Звездочки `*` означают любые символы до и после;
- `servicePrincipalName` – указывает, какой атрибут нужно вывести в результатах поиска.

4. Запустите Ideco Client с опцией `--debug`. Проверьте логи (например, с помощью `journalctl`, `KSystemLog` или `logcheck`) на ошибки получения SSO-токенов вида:

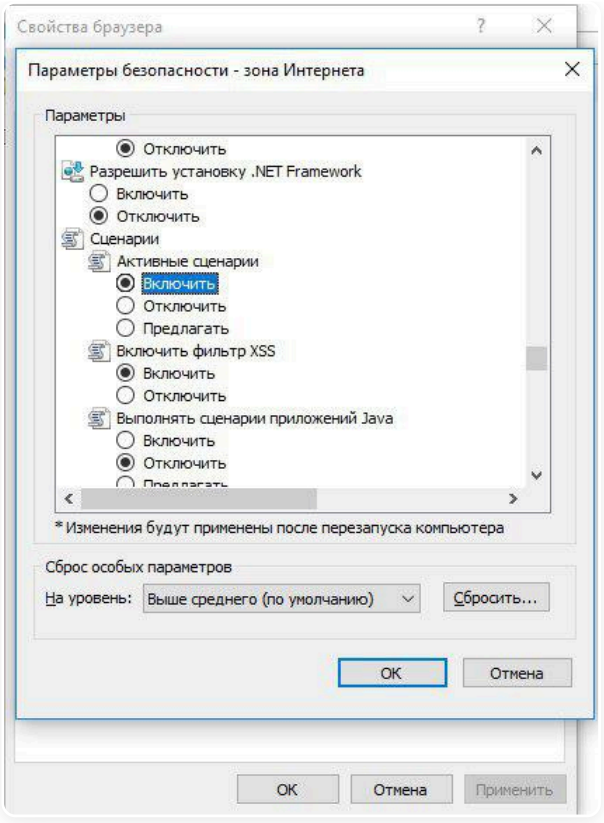
```
SSOGenToken завершился с ошибкой: 'genTokenInternal: <major error string> (<minor error string>)'
```

- `<minor error string>` - описание ошибки, указывающее на причину возникновения ошибки токена SSO.

5. Проверьте состояние интеграции в **Пользователи** → **Active Directory/Samba DC** и при необходимости перенастройте.

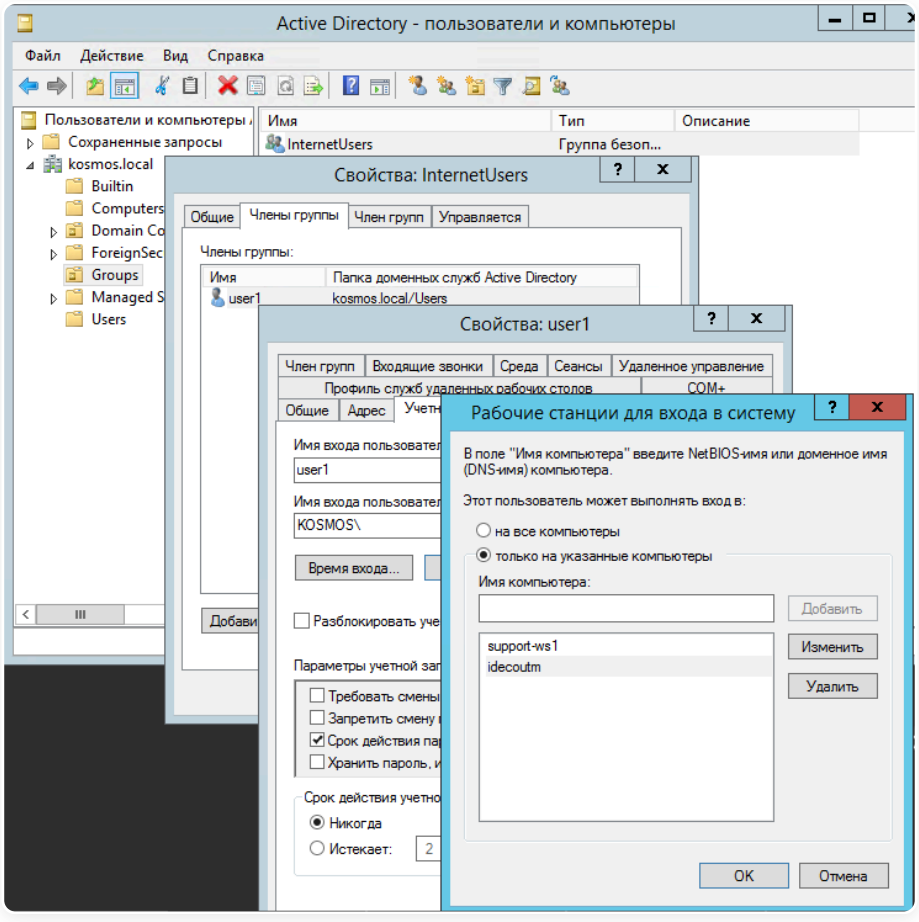
Для получения доступа требуется аутентификация

Если в Internet Explorer появляется окно с текстом **Для получения доступа требуется аутентификация** и аутентификация происходит только при ручном переходе по ссылке, установите параметр **Активные сценарии** в Internet Explorer в значение **Включить**:



Доменному пользователю должно быть разрешено аутентифицироваться на Ideco NGFW Novum. На контроллере домена зайдите в свойства выбранных пользователей в **Учетная запись → Вход на...**, выберите пункт **только на указанные компьютеры** и пропишите имя рабочей станции для входа в систему.

Пример настройки:



Полезные ссылки

- **Авторизация через журнал безопасности AD**
- **Настройка веб-аутентификации**

Настройка авторизации через журнал безопасности

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Настройка авторизации через журнал безопасности**: `ideco-ad-log-collector`.

Список служб для других разделов доступен по ссылке.

Особенности авторизации через журнал безопасности Active Directory

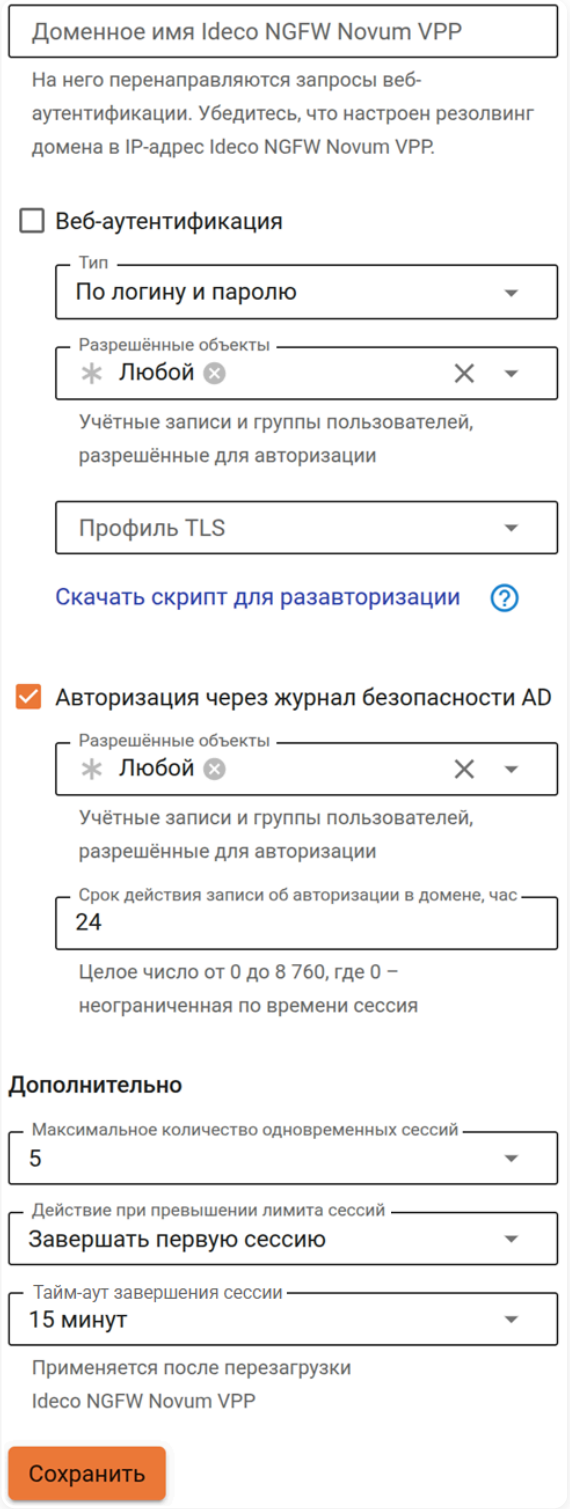
Авторизацию через журнал безопасности Active Directory рекомендуется использовать совместно с SSO-аутентификацией. Авторизация только через журнал безопасности может ограничить возможности управления и настройки прав доступа.

Использование только **Авторизации через журнал безопасности Active Directory** ненадежно по причинам:

- Логи журнала событий безопасности содержат только имя пользователя, IP-адрес и время входа. Журнал не содержит всей информации, необходимой для полноценной авторизации: группы безопасности, права доступа и другие атрибуты пользователя.
- Любые проблемы с журналом, такие как повреждение, потеря данных или задержки в записи, могут привести к проблемам с авторизацией.
- Авторизация через журнал безопасности менее безопасна, так как логи могут быть подделаны или изменены злоумышленниками.
- Авторизация через журнал безопасности требует сложной обработки логов, что повышает риск ошибок и затрудняет поддержку.

Настройка на стороне NGFW Novum

Перейдите в **Пользователи** → **Авторизация** → **Настройки** и заполните поля:

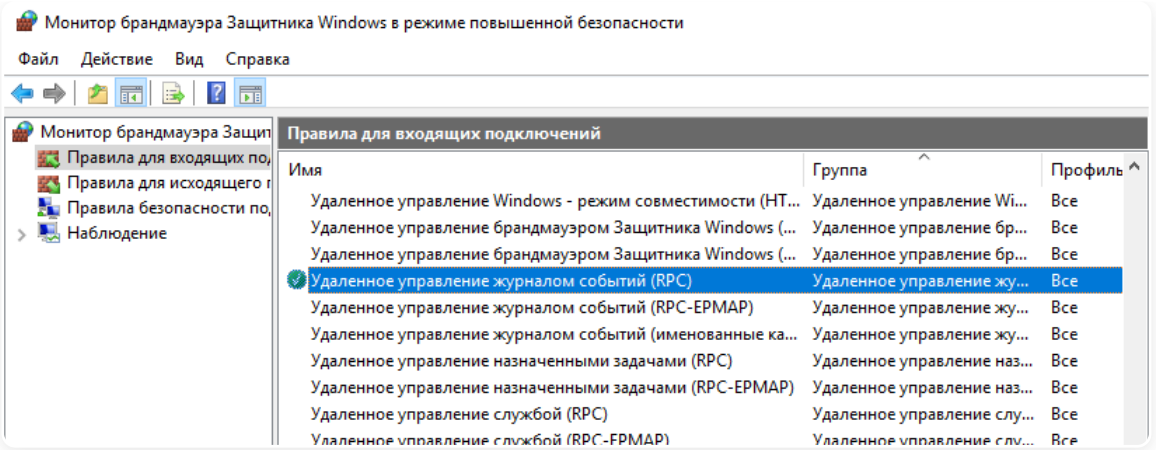


- **Доменное имя Ideco NGFW Novum** - не требуется, если используется только авторизация через журнал безопасности AD.
- **Веб-аутентификация** - не требуется. Авторизация через журнал безопасности AD обеспечивает аутентификацию.
- **Авторизация через журнал безопасности Active Directory** - включите, чтобы Ideco NGFW Novum отслеживал события успешного входа в журнале безопасности AD (события с Event Id `4768`, `4769`, `4624`) и авторизовывал пользователя по ним, если трафик идет с того же IP-адреса.
- **Разрешенные объекты** - выберите разрешенные для авторизации учетные записи или группы пользователей.
- **Срок действия записи об авторизации в домене** - введите время, по истечении которого пользователь деавторизуется в NGFW Novum, если не будет нового входа в домен. При каждом входе пользователя отсчет начинается заново.

Настройка на стороне сервера Active Directory

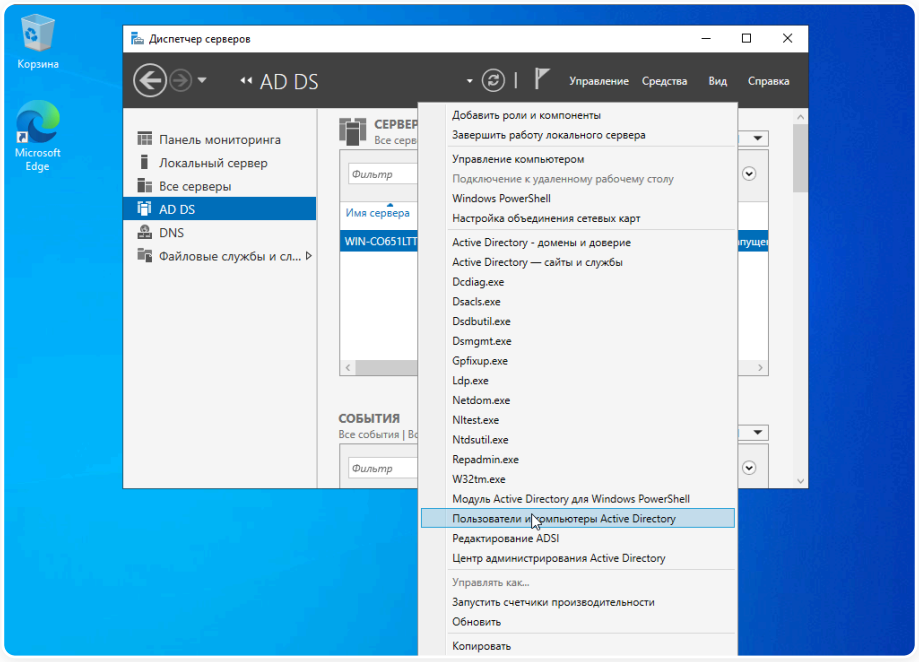
Перед настройкой убедитесь, что Ideco NGFW Novum уже введен в домен.

1. В настройках брандмауэра Windows на всех контроллерах домена разрешите **Удаленное управление журналом событий (Remote Event Log Management)**:

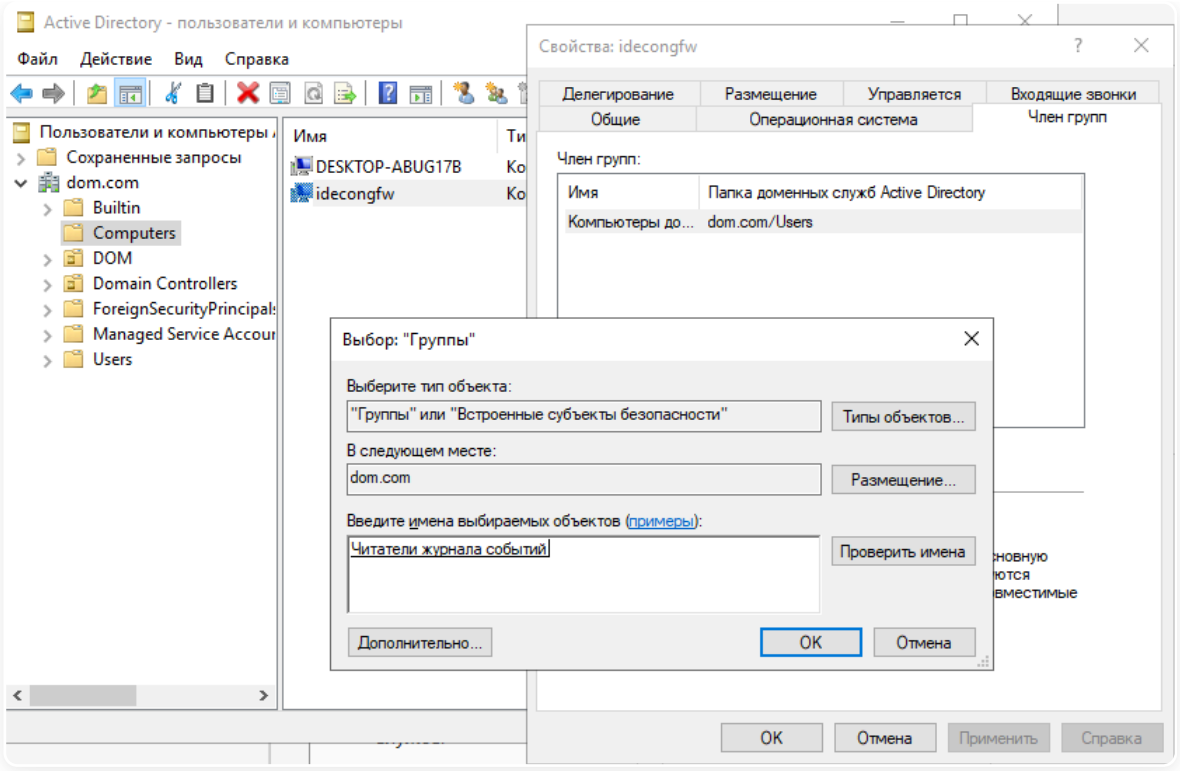


2. Добавьте Ideco NGFW Novum в группу безопасности **Читатели журнала событий (Event Log Readers)**. Чтобы это сделать:

- Зайдите в **Диспетчер серверов**, кликните на **AD DC**, правой кнопкой мыши нажмите на строку с нужным сервером и в выпадающем списке выберите **Пользователи и компьютеры Active Directory**:



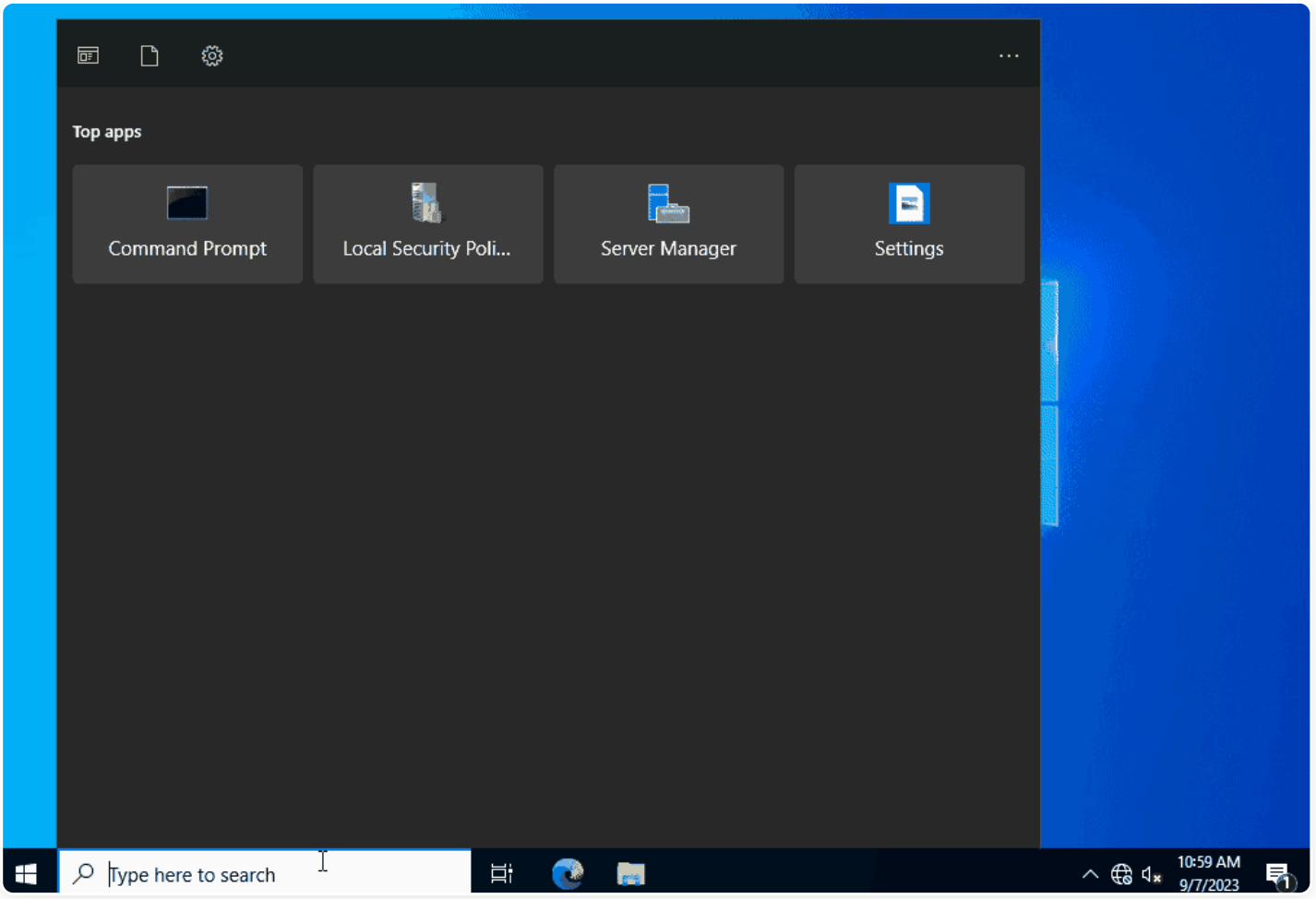
- Откройте **Свойства** объекта **Компьютер**, под которым Ideco NGFW Novum введен в домен (на скриншоте - idecongfw). Перейдите на вкладку **Член групп** и нажмите на кнопку **Добавить**. В появившемся окне нажмите на кнопку **Дополнительно** и добавьте **Читатели журнала событий (Event Log Readers)** через кнопку **Поиск**:



3. Перезапустите службу **Авторизация через журнал безопасности Active Directory** на Ideco NGFW Novum. Для этого отключите эту опцию, а затем снова включите. Либо перезапустите службу `ideco-ad-log-collector` в консоли.

При изменении стандартной политики безопасности контроллеров домена выполните действия:

Англоязычная версия



1. Откройте **Group policy management**.

2. Выберите **Forest: Доменное имя AD** → **Domains** → **Доменное имя AD**.

3. Нажмите правой кнопкой мыши по **Default Domain policy** и выберите **Edit**.

4. В открывшемся окне перейдите по пути **Computer configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies** → **Logon/Logoff**.

5. Дважды кликните по **Audit Logon**.

6. В открывшемся окне на вкладке **Policy** включите **Configure the following audit event** и выберите **Success**.

7. Нажмите **Apply** и **OK**.

8. В папке **Audit Policies** перейдите в **Account Logon**.

9. Дважды кликните по **Audit Kerberos Authentication Service** и повторите действия из пункта 6.

10. Повторите пункты 8 и 9 для **Audit Kerberos Service Ticket Operations**.

Русскоязычная версия

1. Откройте **Управление групповой политикой**.

2. Выберите **Лес: Доменное имя AD** → **Домены** → **Доменное имя AD**.

3. Нажмите правой кнопкой мыши по **Default Domain policy** и выберите **Изменить**.

4. В открывшемся окне перейдите по пути **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Конфигурация расширенной политики аудита** → **Политики аудита** → **Вход/Выход**.

5. Дважды кликните по **Аудит входа в систему**.

6. В открывшемся окне на вкладке **Политика** включите **Настроить следующие события аудита** и выберите **Успех**.

7. Нажмите **Применить** и **OK**.

8. В папке **Политики аудита** перейдите в **Вход учетной записи**.

9. Дважды кликните по **Аудит службы проверки подлинности Kerberos** и повторите действия из пункта 6.

10. Повторите пункты 8 и 9 для **Аудита операций с билетами службы Kerberos**.



Для обновления политик контроллера домена, в терминале выполните команду `gpupdate /force`.

Если авторизация пользователей при входе в систему не происходит, проверьте в журнале безопасности наличие событий 4768, 4769, 4624. Чтобы просмотреть журнал, воспользуйтесь встроенным приложением **Просмотр событий** (Event Viewer). Находится в меню **Пуск** → **Просмотр событий**.

Полезные ссылки

- **Настройка веб-аутентификации**
- **Настройка SSO-аутентификации**

Скрипты автоматического завершения сессии

Классический контекст | Высокопроизводительный контекст

Для автоматического завершения сессий пользователей настройте скрипт (logout), который будет запускаться при выходе пользователей из системы с помощью групповых политик домена (GPO).

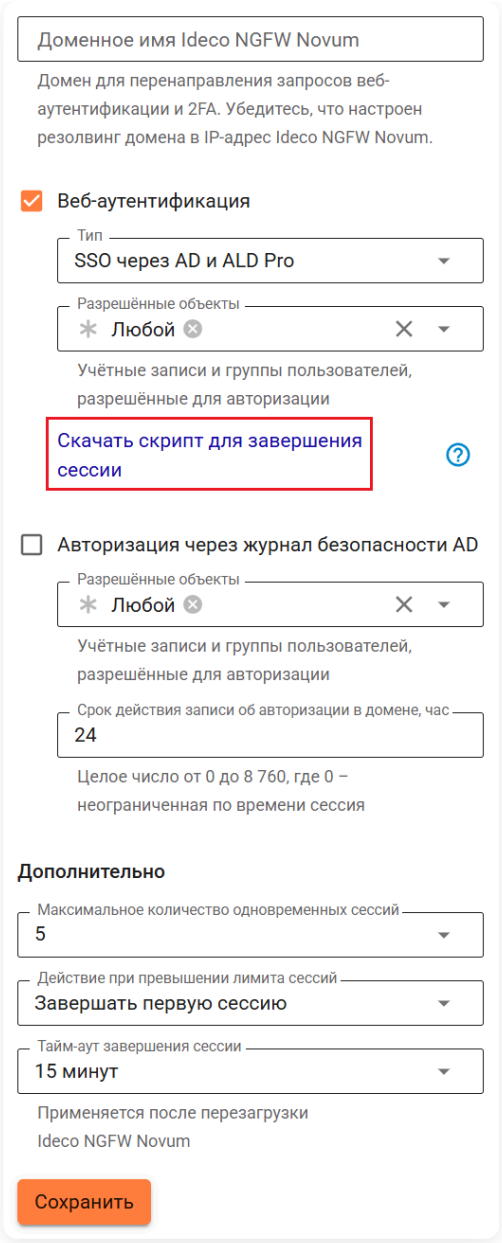
Для работы скрипта выполните настройки политик безопасности домена и браузера, описанные в статье Авторизация пользователей.

Для авторизации по SSO используйте Ideco Client.

Завершение сессии пользователя

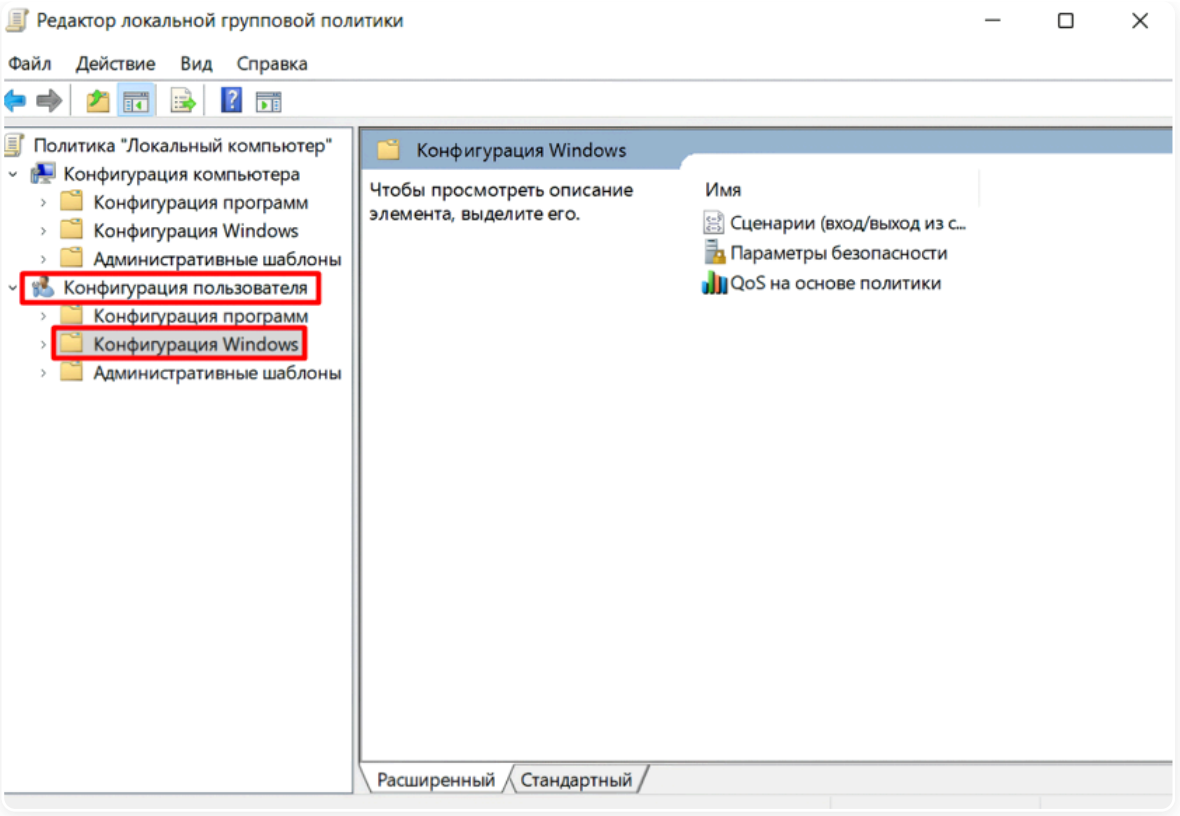
Чтобы скрипт завершения сессии работал корректно, установите на компьютеры пользователей корневой сертификат сервера Ideco NGFW Novum и сделайте сертификат доверенным. Это можно сделать как локально, так и через групповые политики домена, следуя инструкции.

1. Чтобы скачать скрипт, перейдите в **Пользователи** → **Авторизация** → **Настройки**. Включите опцию **Веб-аутентификация**, после чего нажмите **Скачать скрипт для завершения сессии**:



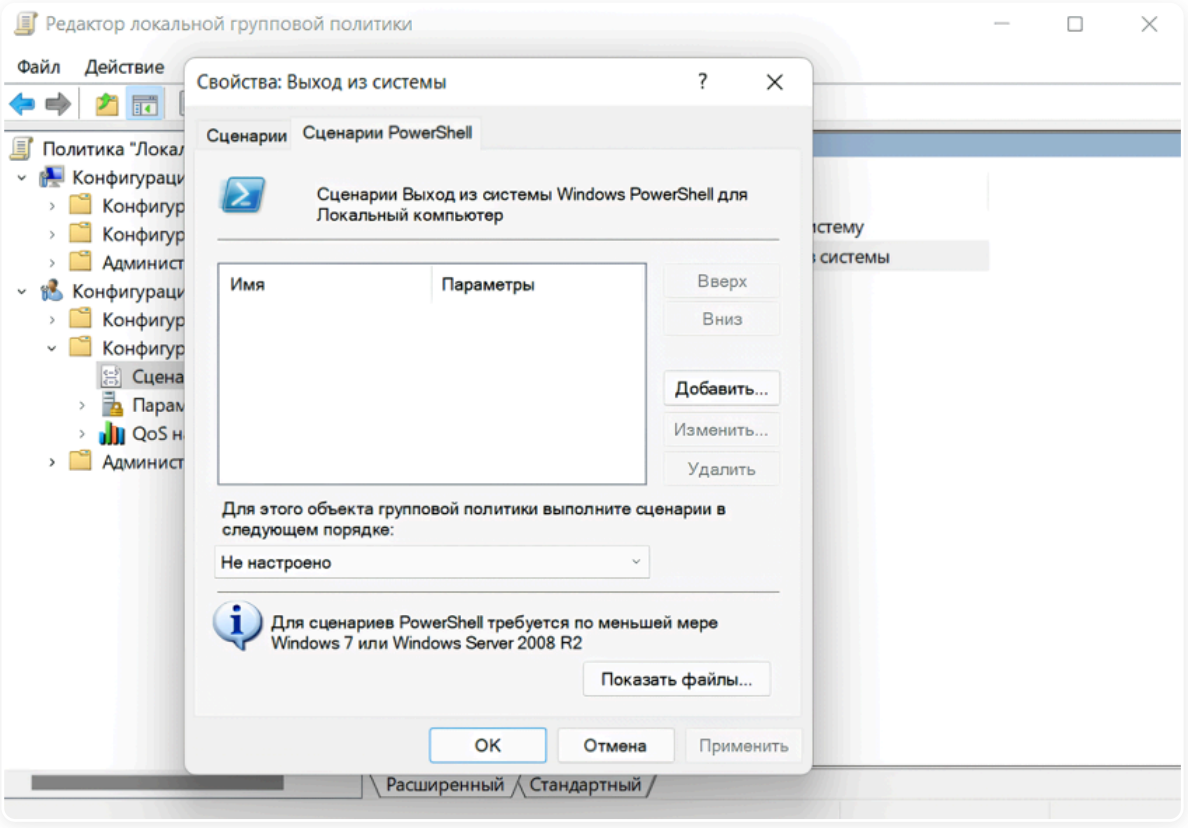
2. Откройте групповые политики `gpedit.msc` от имени администратора на устройстве пользователя.

3. Перейдите в **Конфигурации пользователя** → **Конфигурации Windows**:

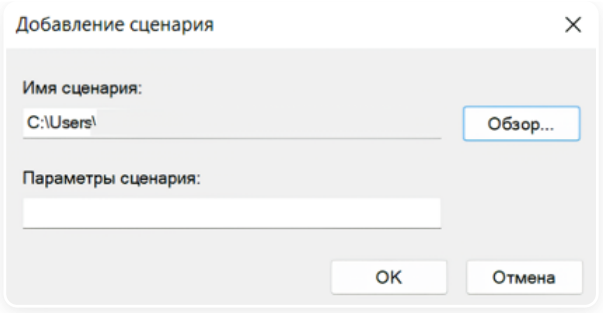


4. Нажмите **Сценарии (вход/выход из системы)**.

5. Откройте **Выход из системы** и перейдите на вкладку **Сценарии PowerShell**:



6. Нажмите **Добавить** и выберите скачанный файл **Ideco_NGFW_logout.ps1**, нажав **Обзор**:



7. Откройте командную строку и обновите групповые политики, введя команду `gpupdate /force`.

Если в вашем браузере появляется окно с текстом **Для получения доступа требуется аутентификация** и авторизация происходит только при ручном переходе по ссылке, включите JavaScript. Ниже представлены настройки для разных браузеров:

Internet Explorer

1. В правом верхнем углу браузера нажмите **Сервис** в виде шестерни или комбинацию клавиш **Alt + X**. В выпадающем меню выберите **Свойства браузера**:

2. В появившемся окне перейдите на вкладку **Безопасность**. Затем нажмите **Другой**:

3. В окне **Параметры** переключите параметр **Активные сценарии** в значение **Включить**:

Google Chrome

1. В правом верхнем углу браузера нажмите на кнопку с тремя точками и выберите **Настройки** в выпадающем меню:

2. В появившемся окне перейдите в раздел **Конфиденциальность и безопасность** и выберите **Настройки сайта**:

3. В настройках **JavaScript** разрешите сайтам использовать JavaScript:

Firefox

1. В адресной строке браузера введите about:config и нажмите **Enter**. Если появится предупреждающее сообщение, нажмите **Принять риск и продолжить**:

2. В поле поиска введите javascript.enabled и переключите настройку параметра, чтобы изменить значение с `false` на `true`:

3. Обновите страницу в браузере.

ALD Pro

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **ALD Pro**: `ideco-ald-rest`; `ideco-ald-backend`.

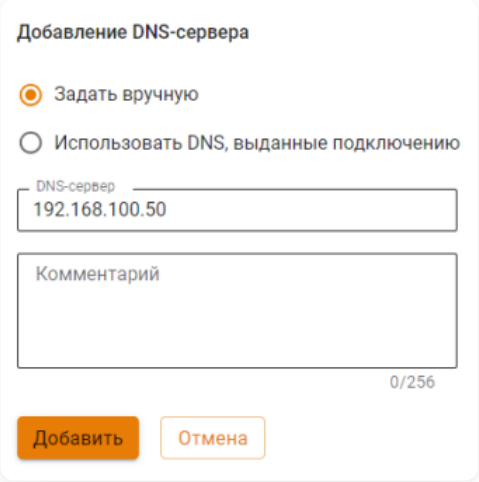
Список служб для других разделов доступен по ссылке.

Система ALD Pro предназначена для централизованного управления ресурсами на базе ОС Astra Linux и может использоваться в организациях различного масштаба.

Ideco NGFW Novum поддерживает версии ALD Pro от 1.4.

Ввод сервера в домен

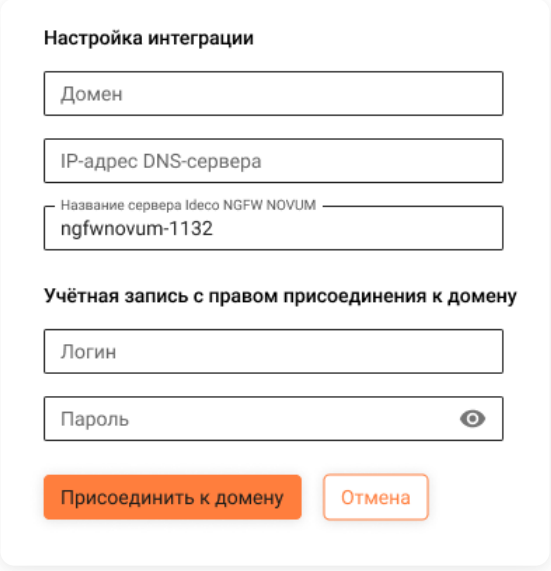
1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы** и добавьте IP-адрес устройства с установленной системой ALD Pro:



2. Перейдите в **Пользователи** → **Внешние каталоги** → **ALD Pro**.

3. Нажмите на кнопку **Добавить**.

4. Заполните поля:



Расшифровка полей

- **Домен** - полное имя домена (не контроллера домена/хоста). Например, `mydomain.example`, а не `astra.mydomain.example`. Домен может содержать только латинские символы, цифры, подчеркивание, дефис и точку.
- **IP-адрес DNS-сервера** - IP-адрес устройства с установленной системой ALD Pro.
- **Название сервера Ideco NGFW Novum** - имя сервера, которое можно сгенерировать в NGFW или указать вручную. Содержит буквенные символы (A-Z), цифры (0-9), а также не может начинаться или заканчиваться на дефис. Максимальное количество символов - 15.
- **Логин и пароль администратора** - данные не сохраняются на сервере и используются один раз для присоединения к домену. Пользователь может не быть администратором домена, но должен обладать правами на присоединение компьютеров к домену.

Если в таблице большое количество интеграций, воспользуйтесь кнопкой **Фильтры**.

Импорт пользователей

ALD Pro поддерживает импорт двух типов групп:

- Группа пользователей - содержит несколько пользователей ALD Pro.
- Подразделение - содержит дерево пользователей ALD Pro, обладающих определенным уровнем доступа.

Из-за особенностей реализации ALD Pro заблокированные пользователи импортируются в Ideco NGFW Novum без блокировки и считаются **активными**.

Для импорта пользователей выполните действия:

1. Перейдите в **Пользователи** → **Учетные записи** и создайте группу, в которую будут импортированы пользователи, нажав на .

2. Перейдите на вкладку **ALD Pro**, выберите домен, тип группы и нажмите **Присоединить к домену**.

Импортированных пользователей можно использовать в качестве объектов для авторизации, настройки VPN-подключений, создания правил трафика (например, в **Межсетевом экране**).

В дальнейшем пользователи будут автоматически синхронизироваться с ALD Pro каждые 15 минут.

Пользователь может быть импортирован только в одну группу Ideco NGFW Novum. Если пользователь находится в нескольких группах ALD Pro то попадет только в ту группу, которая была импортирована последней.

Рекомендуем при создании пользователей указывать в логине домен, например `user@domain.ald`.

Аутентификация пользователей

При аутентификации пользователей проверка осуществляется средствами Kerberos.

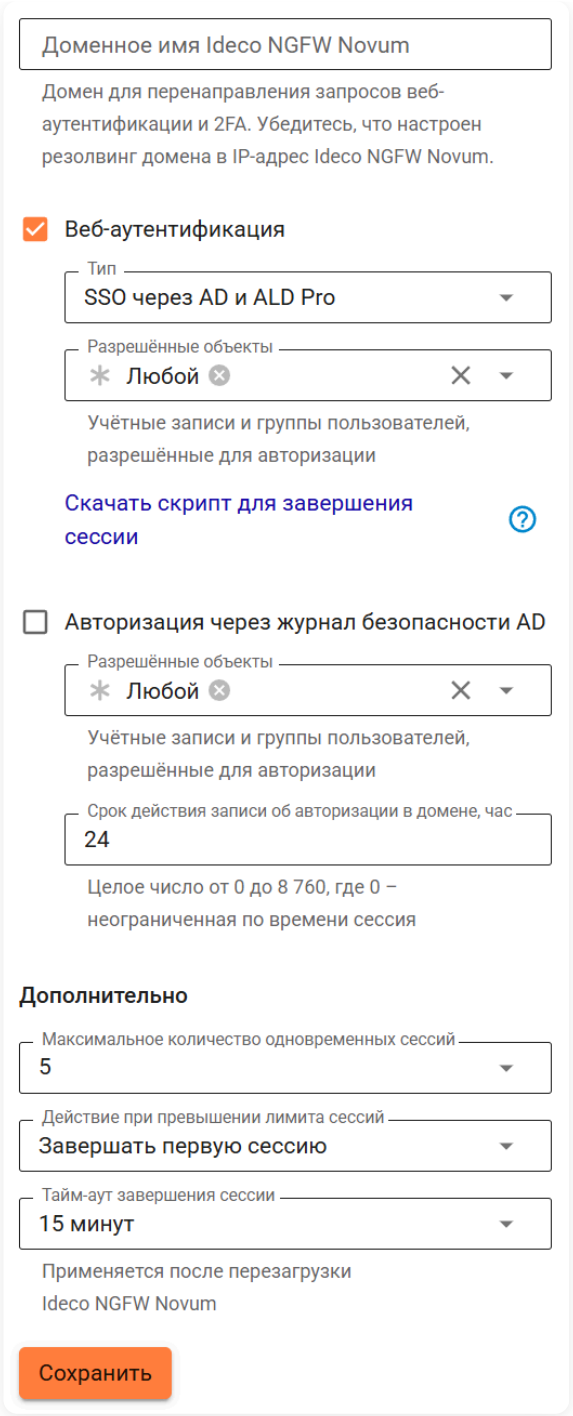
ALD Pro поддерживает два типа входа в систему:

- Вход по логину/паролю.
- Вход через SSO.

Настройка Ideco NGFW Novum

Для настройки аутентификации выполните действия:

1. Перейдите на **Пользователи** → **Авторизация** → **Настройки**:



2. Активируйте опцию **Веб-аутентификация**.

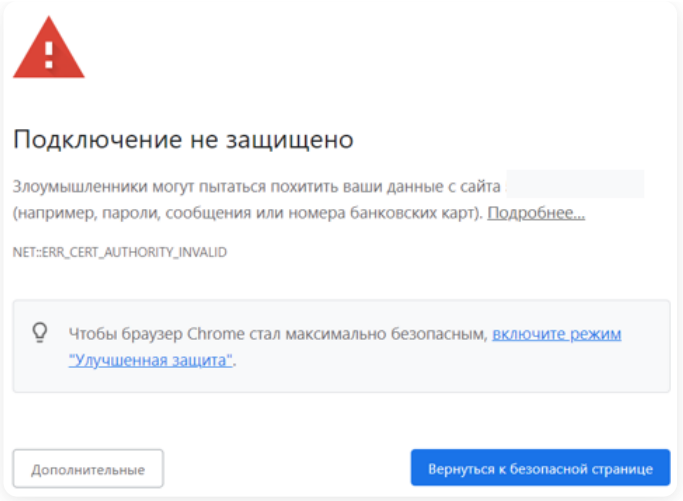
3. Выберите **Тип** входа в систему:

- **По логину и паролю** - вход по логину/паролю.
- **SSO через AD и ALD Pro** - вход через SSO.

4. Выберите разрешенные для авторизации учетные записи или группы пользователей в поле **Разрешенные объекты**.

Настройки в разделе **Дополнительно** описаны в статье.

После заполнения поля **Доменное имя Ideco NGFW Novum** и сохранения настроек будет выдан Let’s Encrypt сертификат, и пользователь перенаправляется на окно авторизации, минуя страницу исключения безопасности:



Если сертификат для такого домена уже загружен в разделе **Сертификаты**, то будет использоваться загруженный сертификат, новый сертификат выдаваться не будет.

> Если NGFW Novum не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW, то страница авторизации будет подписана корневым сертификатом NGFW Novum.

5. Настройте способы авторизации импортированных пользователей. Доступны:

- Авторизация по IP и/или MAC - подходит для пользователей с фиксированными IP- и/или MAC-адресами, на NGFW адреса прописываются вручную каждому пользователю;
- Авторизация по подсетям - подходит, если не требуется регистрировать каждое устройство как отдельного пользователя NGFW. Позволяет автоматически авторизовать большое количество устройств.
- Авторизация по VPN - подходит для аутентификации пользователей удаленных сетей.

Настройка клиентских машин для веб-аутентификации по SSO или NTLM

1. В зависимости от выбранного браузера выполните следующие действия:

Настройка браузера Yandex

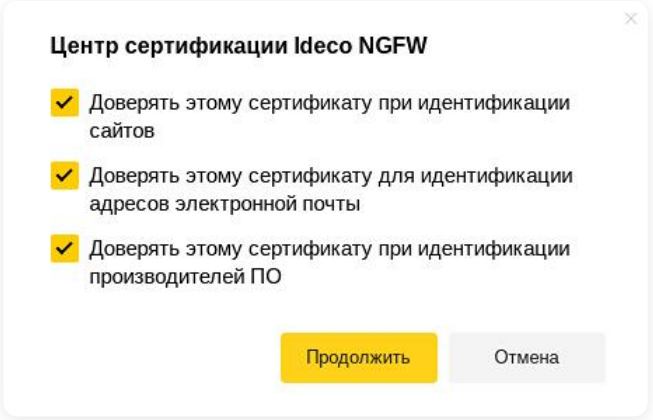
1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.имя_домена",
  "AuthNegotiateDelegateAllowlist": "*.имя_домена"
}
```

2. Скачайте корневой сертификат.

3. В браузере Yandex перейдите в **Настройки** → **Системные** → **Управление сертификатами** → **Центры сертификации** → **Импорт** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:



Настройка браузера Google Chrome

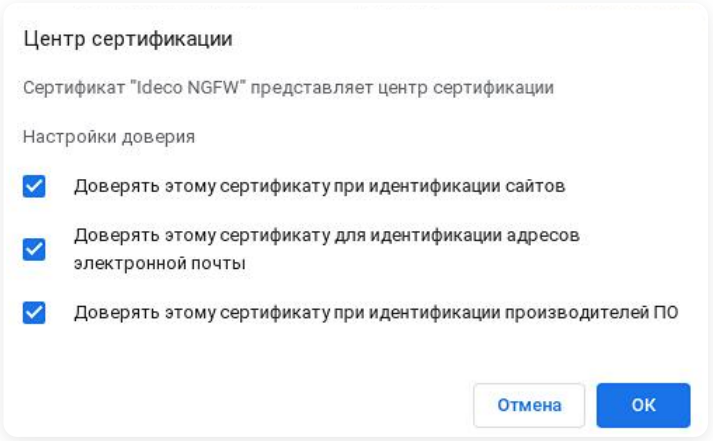
1. Создайте файл **mydomain.json** в директории `/etc/opt/chrome/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.имя_домена",
  "AuthNegotiateDelegateAllowlist": "*.имя_домена"
}
```

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:



Настройка браузера Chromium

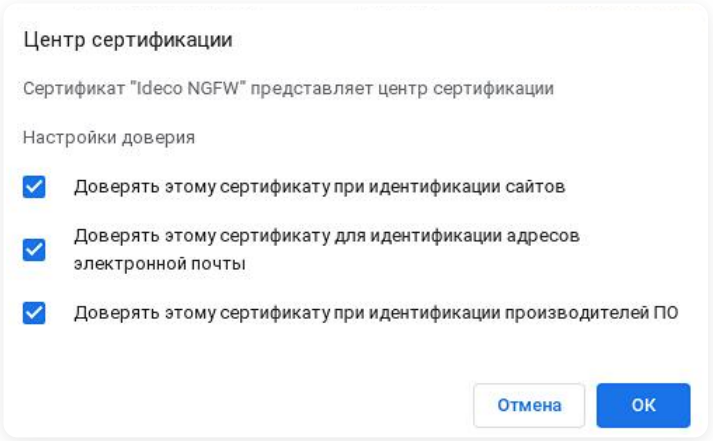
1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и добавьте строки:

```
{
    "AuthServerAllowlist": "*.имя_домена" ,
    "AuthNegotiateDelegateAllowlist": "*.имя_домена"
}
```

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:



Настройка браузера Mozilla Firefox

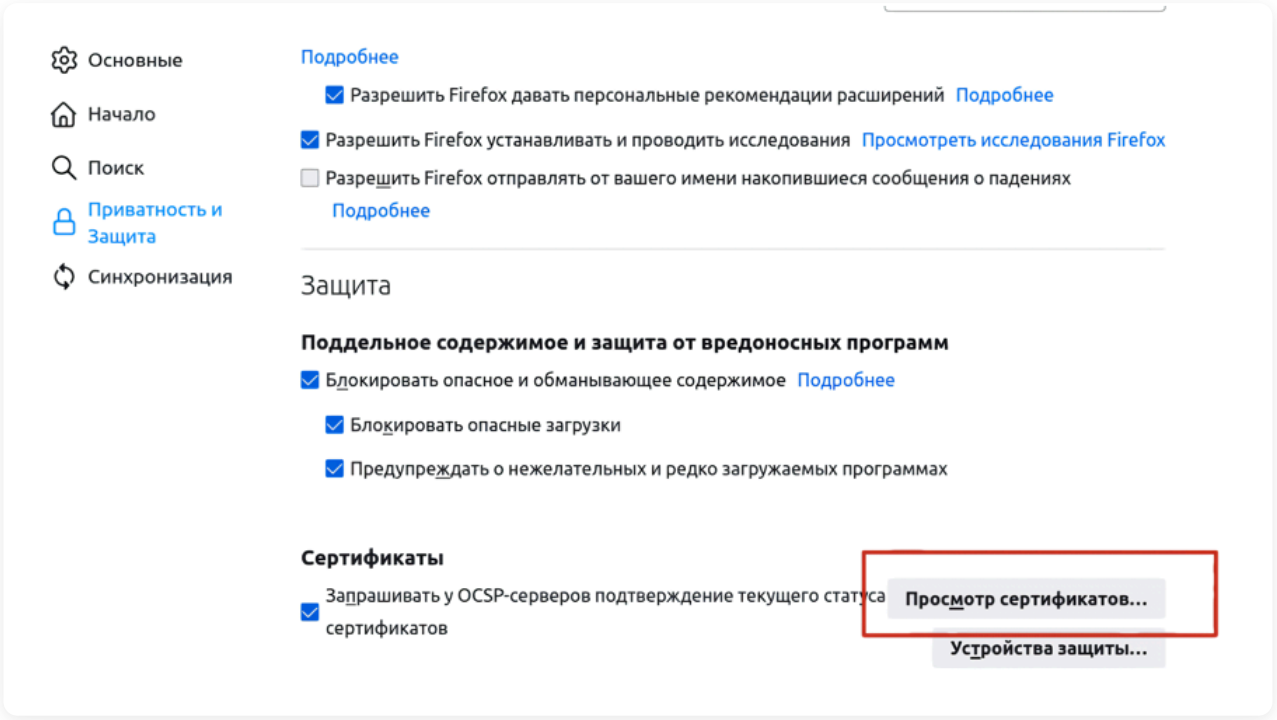
1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

2. Введите параметр `security.enterprise_roots.enabled` и дважды кликните по блоку, чтобы значение изменилось на **True**, что позволит Firefox доверять системным сертификатам и авторизовывать пользователей при переходе на HTTPS-сайты.

3. В параметрах `network.automatic-ntlm-auth.trusted-uris` и `network.negotiate-auth.trusted-uris` укажите `имя_NGFW.имя_домена`.

4. Скачайте корневой сертификат.

5. В настройках браузера Mozilla Firefox в пункте **Приватность и Защита** в разделе **Защита** выберите **Просмотр сертификатов**:



6. На вкладке **Центры сертификации** нажмите **Импортировать** и выберите скачанный с NGFW сертификат.

7. Включите опции доверия для сертификата.
2. На машине ALD-клиента, введенной в домен ALD Pro, добавьте IP-адрес локального интерфейса и доменное имя Ideco NGFW Novum в директорию `/etc/hosts`. Пример: `192.168.100.10 ngfw.domain.ald`.

Руководство по эксплуатации ALD Pro доступно на официальном сайте.

FreeIPA

Классический контекст | Высокопроизводительный контекст | API

FreeIPA - это интегрированное решение для идентификации и аутентификации в сетевых средах Linux/UNIX. Сервер FreeIPA обеспечивает централизованную аутентификацию, авторизацию и доступ к информации об учетных записях.

Предварительная настройка FreeIPA

Для интеграции Ideco NGFW Novum с FreeIPA необходимо на IPA-сервере создать роли:

- **CIFS servers** - предоставляет NGFW Novum права для аутентификации пользователей по протоколу Kerberos, выступая в роли доверенной службы.
- **Organization units** - предоставляет NGFW Novum право на чтение структуры подразделений из каталога для корректного импорта пользователей и групп безопасности.

Для создания ролей выполните действия:

1. Запустите **Терминал Fly** и введите по очереди команды:

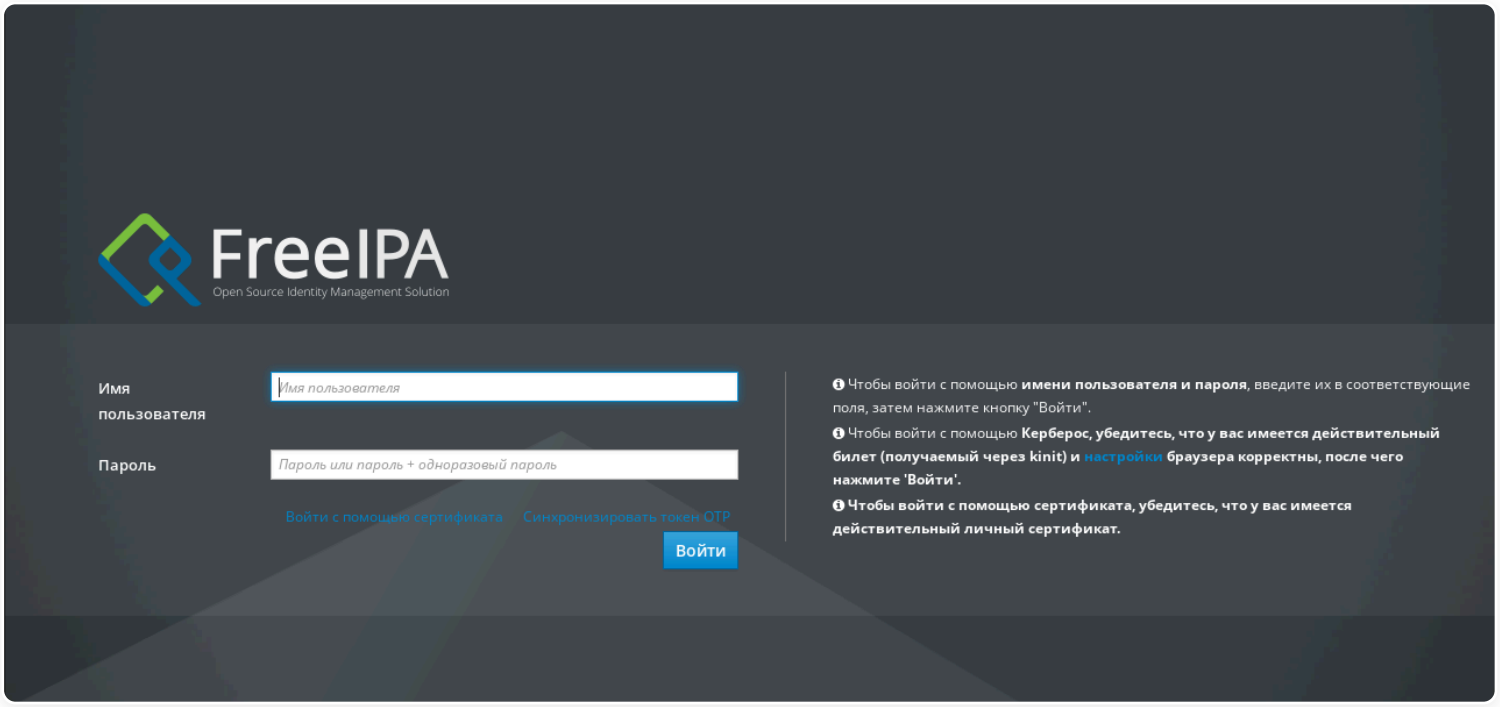
- Для создания роли **CIFS servers**:

```
ipa role-add "CIFS server" --desc="Role for CIFS server"
```

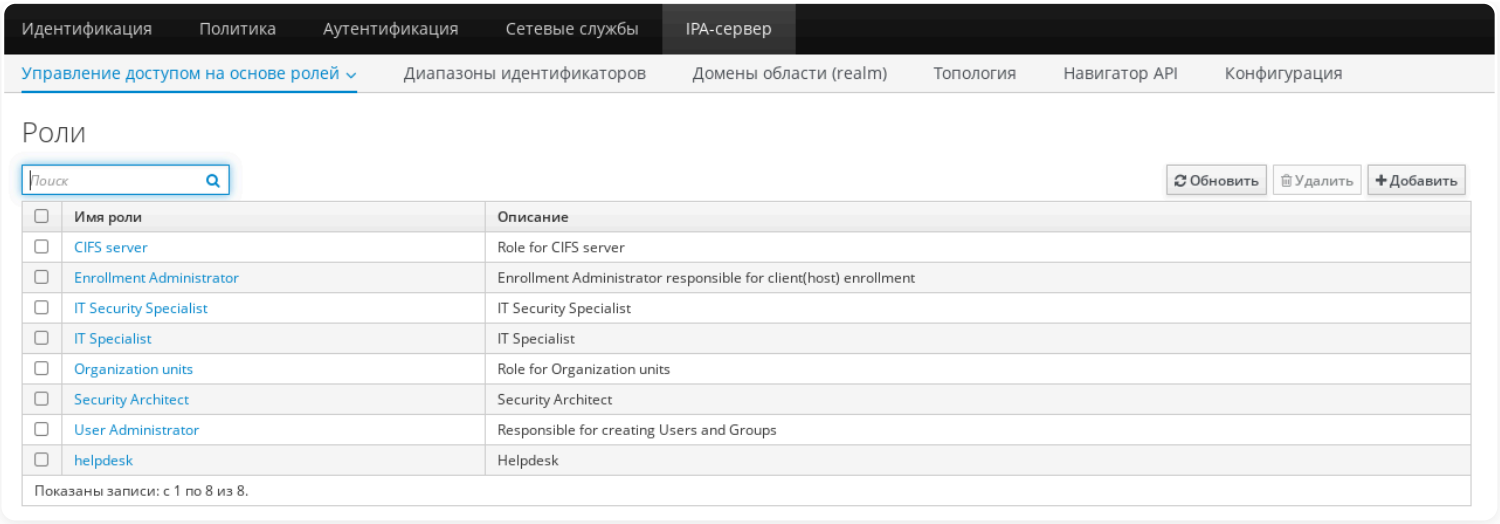
- Для создания **Organization units**:

```
ipa role-add "Organization units" --desc="Role for Organization units"
```

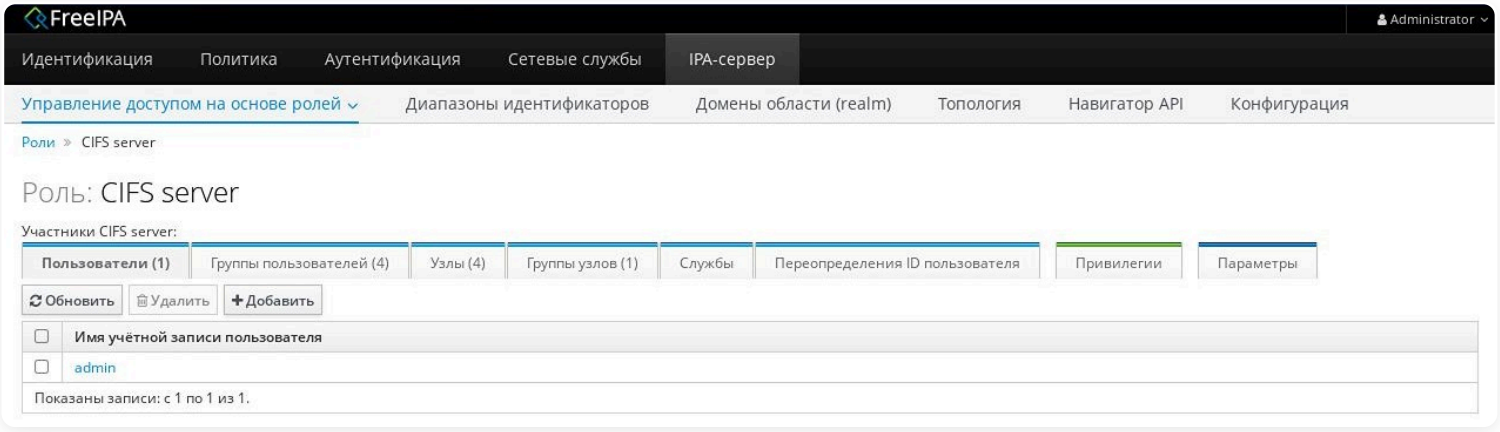
2. Войдите в веб-интерфейс FreeIPA и авторизуйтесь с учетными данными администратора:



3. Перейдите в **IPA-сервер** → **Управление доступом на основе ролей** и убедитесь, что созданные роли появились в списке:



4. Войдите в каждую роль и добавьте объекты:



- **Пользователи** - выберите всех пользователей.
- **Группы пользователей** - выберите все группы.
- **Узлы** - выберите доменный узел.
- **Группы узлов** - выберите все группы.

5. Перезагрузите сервер FreeIPA для активации новых прав.

Дополнительная настройка для VPN-подключений

Для VPN-подключений пользователей FreeIPA необходимо создать разрешение и привилегию на чтение атрибута `ipaNTHash`. Выполните действия одним из способов:

Через терминал

Запустите **Терминал Fly** и введите по очереди команды:

1. Создайте разрешение на чтение NTLM-хэша:

```
ipa permission-add "Read NT Hash Permission" --type=user --permissions="read" --attrs=ipaNTHash
```

2. Создайте привилегию:

```
ipa privilege-add-permission read-ntlm-hashes
```

3. Добавьте разрешение на чтение в созданную привилегию:

```
ipa privilege-add-permission "Read NTLM" --permissions="Read NT Hash Permission"
```

Через веб-интерфейс

1. Для создания разрешения перейдите в **IPA-сервер** → **Управление доступом на основе ролей** → **Разрешения** и нажмите **Добавить**. Заполните поля:

- **Имя разрешения** - укажите имя разрешения.
- **Предоставленные права** - выберите **read**.
- **Тип** - выберите **Пользователь**.
- **Действующие атрибуты** - выберите **ipaNTHash**.

2. Нажмите **Сохранить**.

3. Для создания привилегии перейдите в **IPA-сервер** → **Управление доступом на основе ролей** → **Привилегии** и нажмите **Добавить**:

4. В поле **Имя привилегии** укажите название, например, имя разрешения из шага 1. Нажмите **Добавить**.

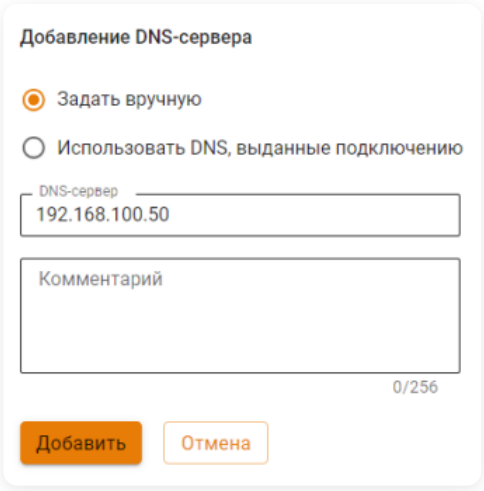
5. Откройте привилегию, созданную на шаге 4, и в блоке **Разрешения** нажмите **Добавить**.

6. Выберите из списка разрешение из шага 1 и подтвердите добавление:

Новую привилегию необходимо добавить в созданные ранее роли **CIFS servers** и **Organization units**, чтобы сервер NGFW Novum получил соответствующие права. Для этого откройте каждую роль и на вкладке **Привилегии** добавьте новую привилегию:

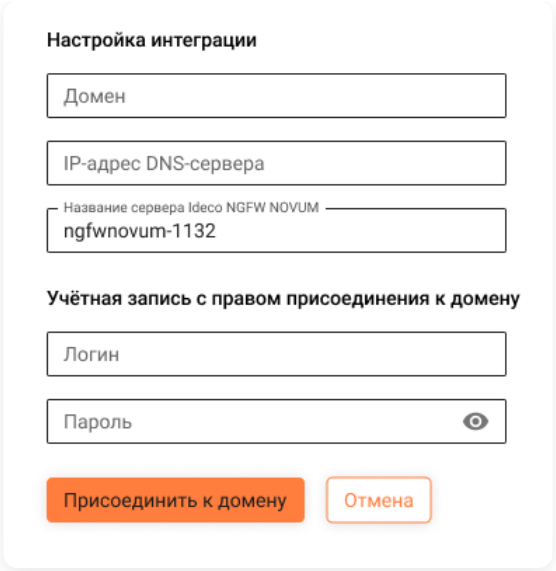
Ввод сервера NGFW Novum в домен FreeIPA

1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы** и добавьте IP-адрес устройства с установленной системой FreeIPA:



2. Перейдите в **Пользователи** → **Внешние каталоги** → **FreeIPA**.

3. Нажмите на кнопку **Добавить** и заполните поля:



Расшифровка полей

- **Домен** - полное имя домена, например, `mydomain.example`. Домен может содержать только латинские символы, цифры, подчеркивание, дефис и точку.
- **IP-адрес DNS-сервера** - IP-адрес устройства с установленной системой FreeIPA.
- **Название сервера Ideco NGFW Novum** - имя сервера, сгенерированное NGFW Novum или указанное вручную. Содержит буквенные символы (A-Z), цифры (0-9), а также не может начинаться или заканчиваться дефисом. Максимальное количество символов - 15.
- **Логин и пароль администратора** - данные не сохраняются на сервере и используются один раз для присоединения к домену. Пользователь может не быть администратором домена, но должен обладать правами на присоединение компьютеров к домену.

Если в таблице большое количество интеграций, воспользуйтесь кнопкой **Фильтры**.

Импорт пользователей

FreeIPA поддерживает импорт двух типов групп:

- Группа пользователей - содержит несколько пользователей FreeIPA.
- Подразделение - содержит дерево пользователей FreeIPA, обладающих определенным уровнем доступа.

Из-за особенностей взаимодействия с FreeIPA при импорте пользователей статус блокировки не передается в Ideco NGFW Novum. В результате учетная запись заблокированного в домене пользователя отображается в NGFW Novum как **активная**.

Однако авторизоваться в NGFW Novum под такой учетной записью невозможно - запрос отклоняет контроллер домена.

Для импорта пользователей выполните действия:

1. Перейдите в **Пользователи** → **Учетные записи** и создайте группу, в которую будут импортированы пользователи, нажав .

2. Перейдите на вкладку **FreeIPA**, выберите домен и созданную группу. Нажмите **Присоединить к домену**.

Импортированных пользователей можно использовать в качестве объектов для авторизации, настройки VPN-подключений, создания правил трафика (например, в **Межсетевом экране**).

В дальнейшем пользователи будут автоматически синхронизироваться с FreeIPA каждые 15 минут.

Пользователь может быть импортирован только в одну группу Ideco NGFW Novum. Если пользователь находится в нескольких группах FreeIPA, то попадет только в ту группу, которая была импортирована последней.

Рекомендуем при создании пользователей указывать в логине домен, например, `user@domain.freeipa`.

Аутентификация пользователей

При аутентификации пользователей проверка осуществляется средствами Kerberos.

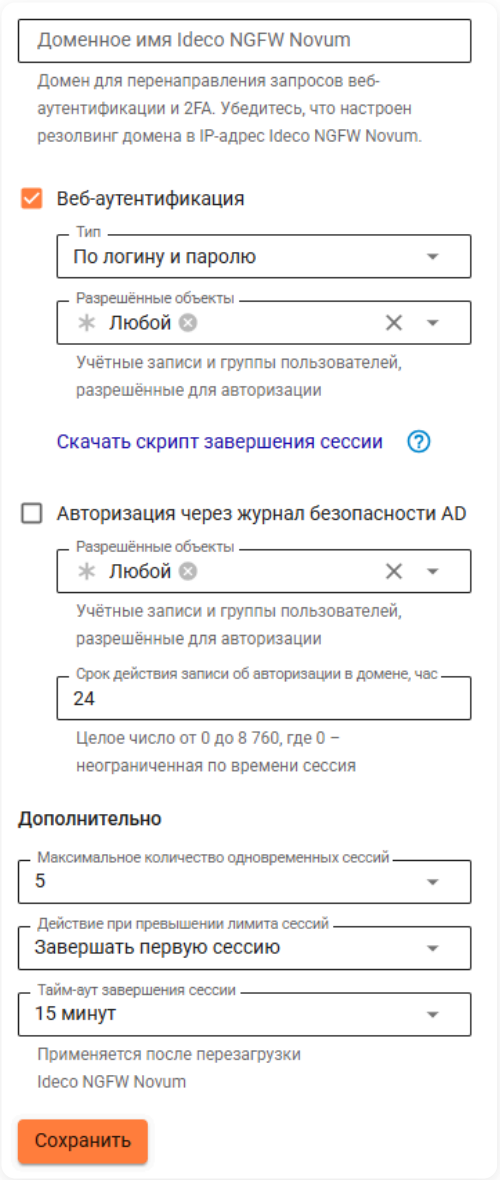
FreeIPA поддерживает два типа входа в систему:

- Вход по логину/паролю.
- Вход через SSO.

Настройка Ideco NGFW Novum

Для настройки аутентификации выполните действия:

1. Перейдите в **Пользователи** → **Авторизация** → **Настройки** и активируйте опцию **Веб-аутентификация**:



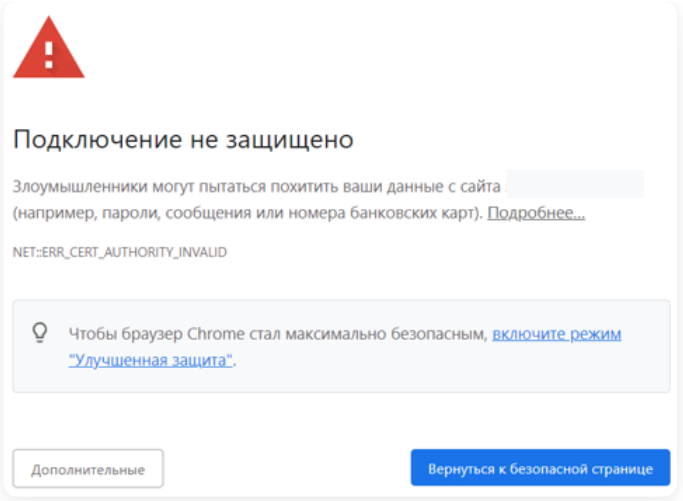
2. Выберите **Тип** входа в систему:

- **По логину и паролю** - вход по логину/паролю.
- **Через SSO** - вход через SSO.

3. Выберите разрешенные для авторизации учетные записи или группы пользователей в поле **Разрешенные объекты**.

Настройки в разделе **Дополнительно** описаны в статье.

После заполнения поля **Доменное имя Ideco NGFW Novum** и сохранения настроек будет выдан Let's Encrypt сертификат. Пользователь перенаправляется на окно авторизации, минуя страницу исключения безопасности:



Если сертификат для такого домена уже загружен в разделе **Сертификаты**, то будет использоваться загруженный сертификат, новый выдаваться не будет.

> Если NGFW Novum не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW Novum, то страница авторизации будет подписана корневым сертификатом NGFW Novum.

4. Настройте способы авторизации импортированных пользователей. Доступны:

- **Авторизация по IP и/или MAC** - подходит для пользователей с фиксированными IP- и/или MAC-адресами, на NGFW Novum адреса прописываются вручную каждому пользователю.
- **Авторизация по подсетям** - подходит, если не требуется регистрировать каждое устройство как отдельного пользователя NGFW Novum. Позволяет автоматически авторизовать большое количество устройств.
- **Авторизация по VPN** - подходит для аутентификации пользователей удаленных сетей.

Настройка клиентских машин для веб-аутентификации по SSO или NTLM

1. В зависимости от выбранного браузера выполните следующие действия:

Настройка браузера Yandex

1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.<имя_домена>",
  "AuthNegotiateDelegateAllowlist": "*.<имя_домена>"
}
```

2. Скачайте корневой сертификат.

3. В браузере Yandex перейдите в **Настройки** → **Системные** → **Управление сертификатами** → **Центры сертификации** → **Импорт** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:

Настройка браузера Google Chrome

1. Создайте файл **mydomain.json** в директории `/etc/opt/chrome/policies/managed/` и добавьте строки:

```
{
  "AuthServerAllowlist": "*.<имя_домена>",
  "AuthNegotiateDelegateAllowlist": "*.<имя_домена>"
}
```

2. Скачайте корневой сертификат.

3. В браузере Google Chrome перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:

Настройка браузера Chromium

1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и добавьте строки:

```
{
    "AuthServerAllowlist": "*.<имя_домена>",
    "AuthNegotiateDelegateAllowlist": "*.<имя_домена>"
}
```

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

4. Включите опции доверия для сертификата:

Настройка браузера Mozilla Firefox

1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

2. Введите параметр `security.enterprise_roots.enabled` и дважды кликните по блоку, чтобы значение изменилось на **True**, что позволит Firefox доверять системным сертификатам и авторизовывать пользователей при переходе на HTTPS-сайты.

3. В параметрах `network.automatic-ntlm-auth.trusted-uris` и `network.negotiate-auth.trusted-uris` укажите `<имя_NGFW.имя_домена>`.

1. Скачайте корневой сертификат.

2. В настройках браузера Mozilla Firefox перейдите в **Приватность и Защита** → **Защита** и выберите **Просмотр сертификатов**:

3. На вкладке **Центры сертификации** нажмите **Импортировать** и выберите скачанный с NGFW Novum сертификат.

4. Включите опции доверия для сертификата.
2. На машине клиента, введенной в домен FreeIPA, добавьте IP-адрес локального интерфейса и доменное имя Ideco NGFW Novum в файл `/etc/hosts`. Пример: `192.168.100.10 ngfw.domain.freeipa`.

RADIUS

Классический контекст | Высокопроизводительный контекст

> Интеграция с RADIUS-сервером обеспечивает аутентификацию пользователей, данные которых хранятся исключительно на RADIUS-сервере или в базах данных/каталогах, доступных для него.

Особенности интеграции

- Через RADIUS-сервер доступна аутентификация только VPN-пользователей NGFW Novum.
- Пользователи RADIUS могут авторизоваться с помощью Ideco Client без установки VPN-туннеля.
- Если учетные записи в службе каталогов Active Directory/Samba DC совпадают с учетными записями на RADIUS-сервере, авторизация будет производиться с использованием данных из службы каталогов.
- Ideco NGFW Novum поддерживает интеграцию с RADIUS-администраторами. Подробные инструкции по настройке описаны в статье Администраторы.

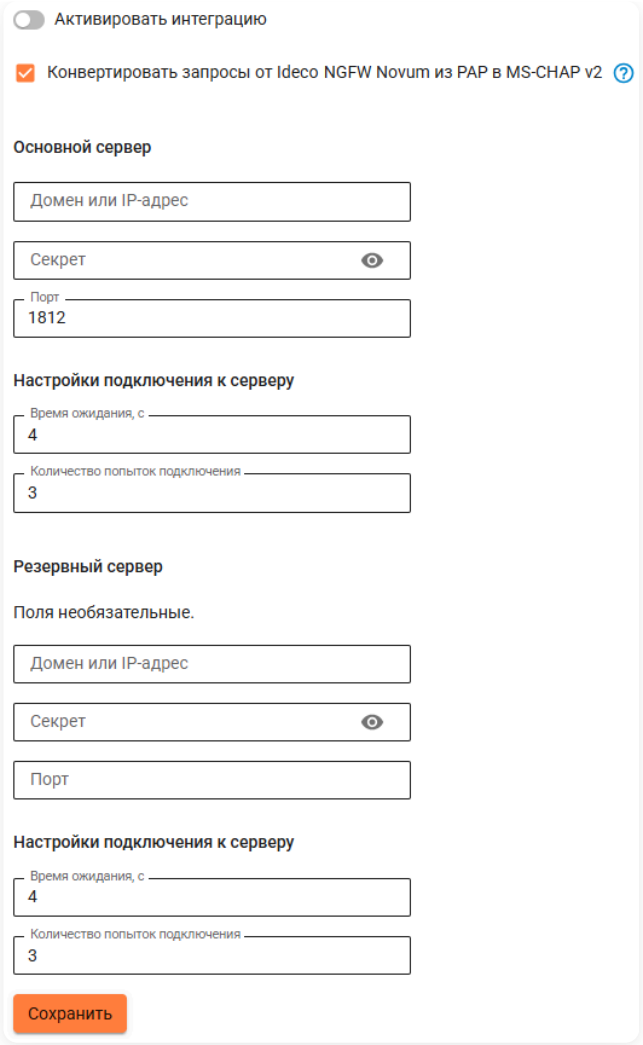
Настройка интеграции

Для настройки интеграции с RADIUS-сервером выполните действия:

1. Перейдите в **Пользователи** → **Внешние каталоги** → **RADIUS** и включите опцию **Активировать интеграцию**.

> При отключенной интеграции с RADIUS-сервером пользователи RADIUS не смогут аутентифицироваться на NGFW Novum.

2. Заполните поля:



- **Конвертировать запросы от Ideco NGFW Novum из PAP в MS-CHAP v2** - выключите опцию, только если необходимо настроить двухфакторную аутентификацию для пользователей RADIUS-сервера. Опция повышает безопасность и защиту:
  - От перехвата паролей между NGFW Novum и RADIUS-сервером.
  - Когда RADIUS-сервер поддерживает только MS-CHAP v2.
- **Основной сервер** - настройте основной RADIUS-сервер:
  - **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
  - **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
  - **Порт** - порт, по которому будет происходить подключение к серверу. Поменяйте при необходимости.
  - **Настройки подключения к серверу**:
    - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
    - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.
- **Резервный сервер** - настройте резервный RADIUS-сервер, если требуется:
  - **Домен или IP-адрес** - домен или адрес резервного RADIUS-сервера.
  - **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
  - **Порт** - порт, по которому будет происходить подключение к серверу. Поменяйте при необходимости.
  - **Настройки подключения к серверу**:
    - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
    - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.

Опция **Порт** влияет только на подключения через Ideco Client. Переключение опции никак не влияет на подключение пользователей по другим типам VPN.

3. Нажмите **Сохранить**.

Добавление пользователей в дерево пользователей Ideco NGFW Novum

1. При подключении пользователя к Ideco NGFW Novum происходит поиск пользователя в дереве пользователей:

- Если пользователь найден - запрос аутентификации сразу будет отправлен на RADIUS-сервер.
- Если пользователь не найден - Ideco NGFW Novum создаст пользователя и отправит запрос аутентификации на RADIUS-сервер.

2. При отсутствии группы **RADIUS** в Ideco NGFW Novum группа будет пересоздаваться при аутентификации пользователей RADIUS-сервера.

3. После аутентификации пользователь будет добавлен в группу **RADIUS** на Ideco NGFW Novum.

Группу и пользователей **RADIUS** можно использовать для создания правил фильтрации трафика и других задач.

Ограничения для группы и пользователей RADIUS:

- Разрешено удалять и переименовывать группу **RADIUS**.
- Запрещено менять параметры пользователя (в том числе поля **Имя** и **Комментарий**), за исключением опции **Запретить доступ**.
- Запрещено перемещать пользователей в другие группы.
- Запрещено перемещать других пользователей NGFW Novum в группу **RADIUS**.
- Запрещена настройка **IP** и **MAC** авторизации для пользователей группы.
- Недоступна авторизация пользователей группы в личном кабинете и веб-почте.

Двухфакторная аутентификация

Двухфакторная аутентификация для пользователей RADIUS-сервера доступна при авторизации через Ideco Client.

По умолчанию Ideco Client использует для аутентификации на внешнем сервере протокол MS-CHAP v2. При отключении опции **Конвертировать запросы от Ideco NGFW Novum из PAP в MS-CHAP v2** запросы аутентификации от Ideco Client к внешнему серверу будут выполняться по протоколу PAP. Для всех прочих VPN-подключений продолжает работать только MS-CHAP v2 независимо от настройки.

Если необходимо обеспечить для пользователей RADIUS-сервера двухфакторную аутентификацию на этом же сервере:

1. В веб-интерфейсе Ideco NGFW Novum в **Пользователи** → **RADIUS** отключите опцию **Конвертировать запросы от Ideco NGFW Novum из PAP в MS-CHAP v2**. Проверку второго фактора с использованием MS-CHAP v2 обеспечить невозможно.

2. Настройте RADIUS-сервер на работу с протоколом PAP.

3. Настройте на RADIUS-сервере механизм двухфакторной аутентификации. Настраивать 2FA на Ideco NGFW Novum не нужно.

При настройке двухфакторной аутентификации на RADIUS-сервере поле сообщения пользователю **Reply-Message** ограничено 253 байтами. Поэтому максимальная длина сообщения ограничена:

- Для латиницы - 253 символа.
- Для кириллицы - 137 символов.

LDAP-фильтры

Классический контекст | Высокопроизводительный контекст

Настройка объектов для группировки пользователей каталога LDAP (Lightweight Directory Access Protocol).

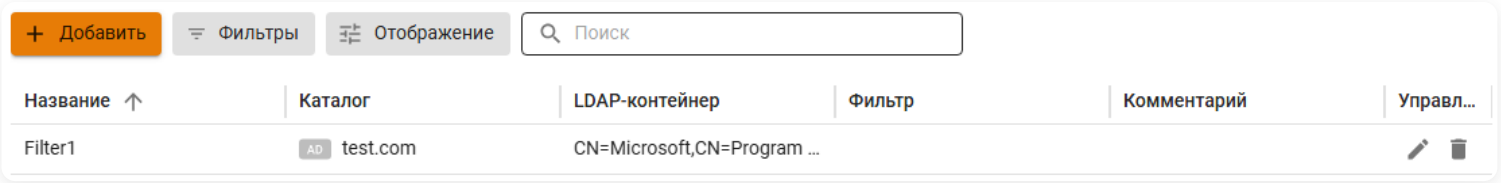
LDAP (Lightweight Directory Access Protocol) - протокол быстрого доступа к каталогам, позволяющий получать и принимать через сеть данные из каталогов с иерархической структурой. LDAP-фильтры - один из способов выборки учетных записей из каталога AD наряду с группами безопасности. С помощью фильтров можно отобрать нужные учетные записи для применения в правилах.

LDAP-фильтры применяются только для каталога Active Directory.

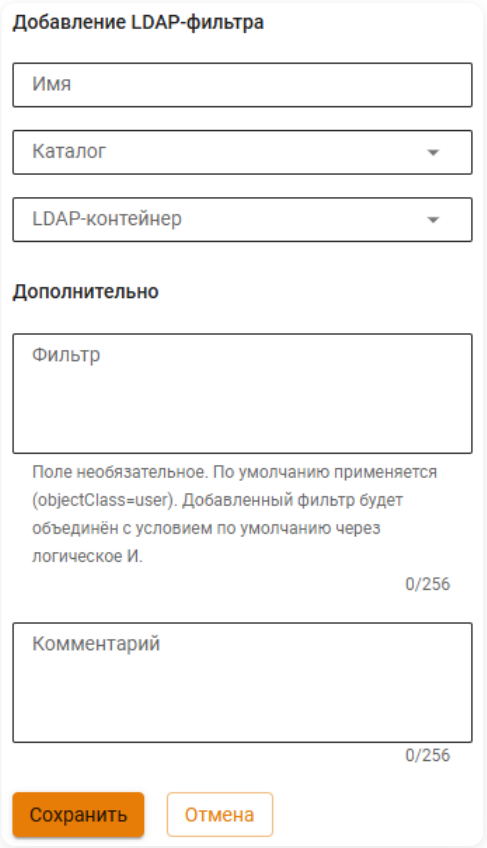
Рекомендуем использовать LDAP-фильтры в правилах только если невозможна настройка с помощью групп безопасности.

Добавление и редактирование LDAP-фильтров

Для добавления LDAP-фильтра перейдите в **Пользователи** → **Внешние каталоги** → **LDAP-фильтры** и нажмите **Добавить**:



1. Заполните форму:



Расшифровка полей

- **Имя** - укажите уникальное название LDAP-фильтра, не более 128 символов.

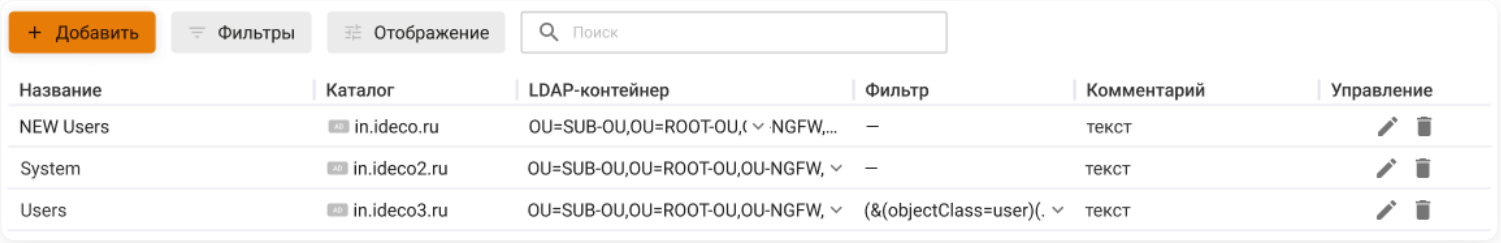
- **Каталог** - выберите каталог AD.
- **LDAP-контейнер** - выберите группу из списка контейнеров каталога.
- **Фильтр** - необязательное поле. Всегда используется `(objectClass=user)` (все пользователи). Фильтр, введенный администратором в поле, объединяется с `(objectClass=user)` через оператор `И`.
- **Комментарий** - необязательное поле.

Примеры фильтров

- `(!userAccountControl:1.2.840.113556.1.4.803:=2)` - только включенные пользователи.
- `(givenName=*)(sn=*)` - все пользователи с заполненными именем и фамилией.
- `(memberOf:1.2.840.113556.1.4.1941:=cn=Test,ou=East,dc=Domain,dc=com)` - все пользователи, принадлежащие группе безопасности `Test`, которая находится в подразделении `East` домена `domain.com`.

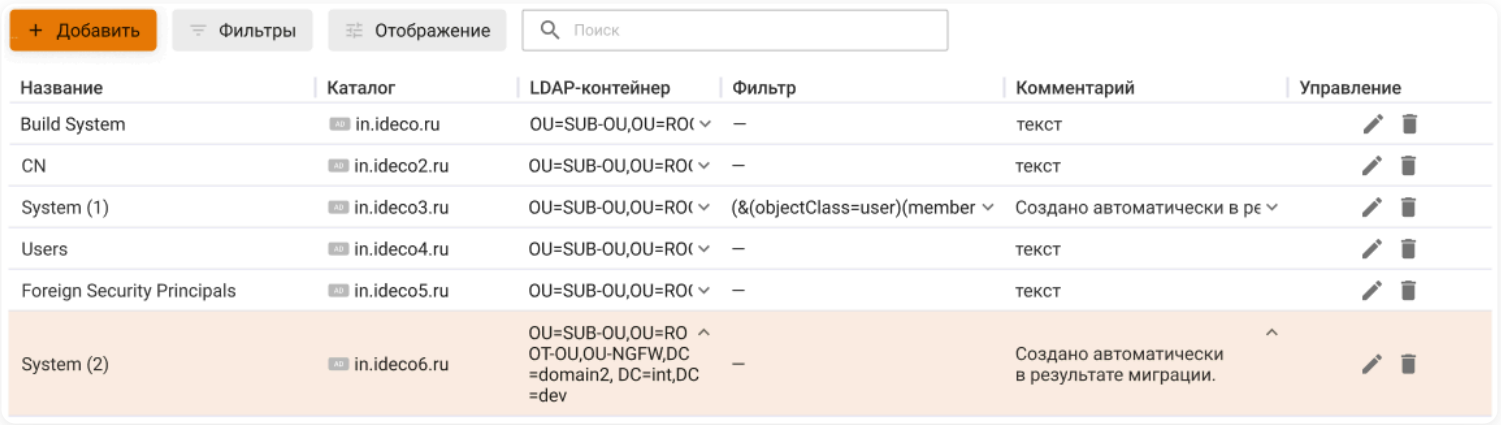
2. Нажмите **Добавить**.

Добавленные LDAP-фильтры отображаются в таблице. Для редактирования записи нажмите :



Миграция LDAP-фильтров

При обновлении Ideco NGFW Novum на версию 21 импортированные ранее в дерево LDAP-группы AD автоматически мигрируют в **LDAP-фильтры**:

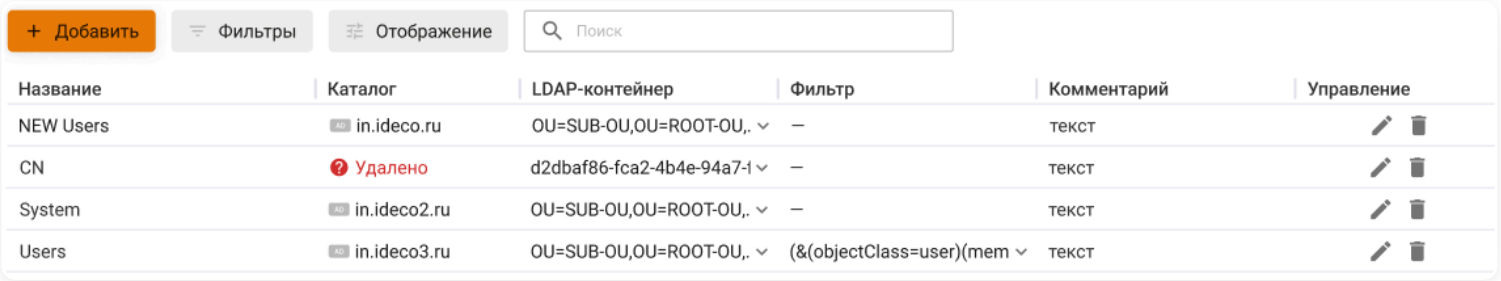


Особенности миграции:

- Если в дерево были импортированы LDAP-группы AD с одинаковым именем, то при миграции в **LDAP-фильтры** к именам фильтров будет добавлен сквозной номер в скобках.
- Автоматически созданные LDAP-фильтры имеют комментарий **Создано автоматически в результате миграции**.

Как восстановить LDAP-фильтры при удалении каталога

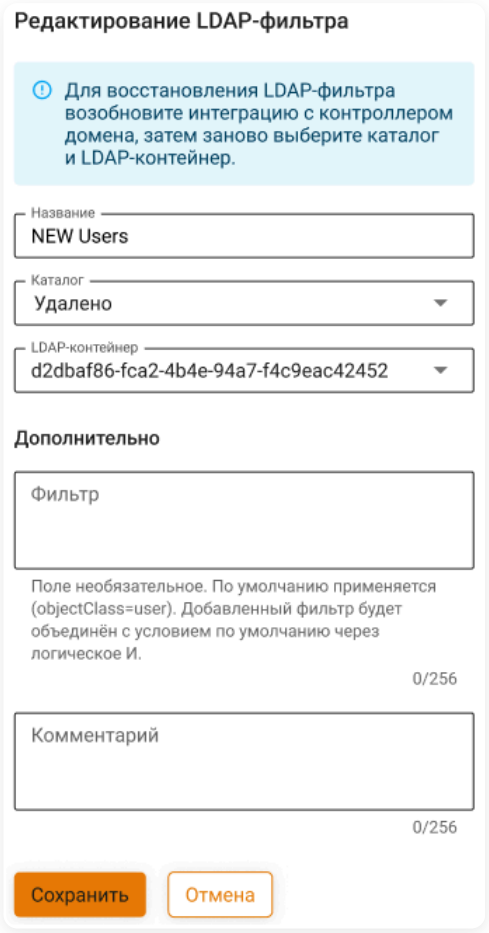
Если действующая интеграция с доменом удалена, каталог LDAP-фильтров, относящийся к такой интеграции, помечается алиасом **Удалено**:



Для восстановления LDAP-фильтра:

1. Восстановите интеграцию с контроллером домена AD. Новая интеграция будет иметь новый ID.

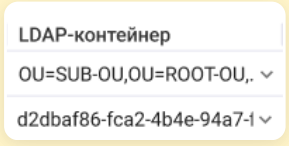
2. Отредактируйте LDAP-фильтр, выбрав каталог и LDAP-контейнер:



3. Нажмите **Сохранить**.

Повторный выбор LDAP-фильтра для возобновления работы правил не требуется.

Если связи с контроллером домена нет или не успела пройти синхронизация, то в поле **LDAP-контейнер** отобразится GUID группы вместо Distinguished Name (DN):



- `OU=SUB-OU,OU=ROOT-OU,DC=test,DC=com` - DN.
- `d2dbaf86-fca2-4b4e-94a7-f305e82c3301` - GUID.

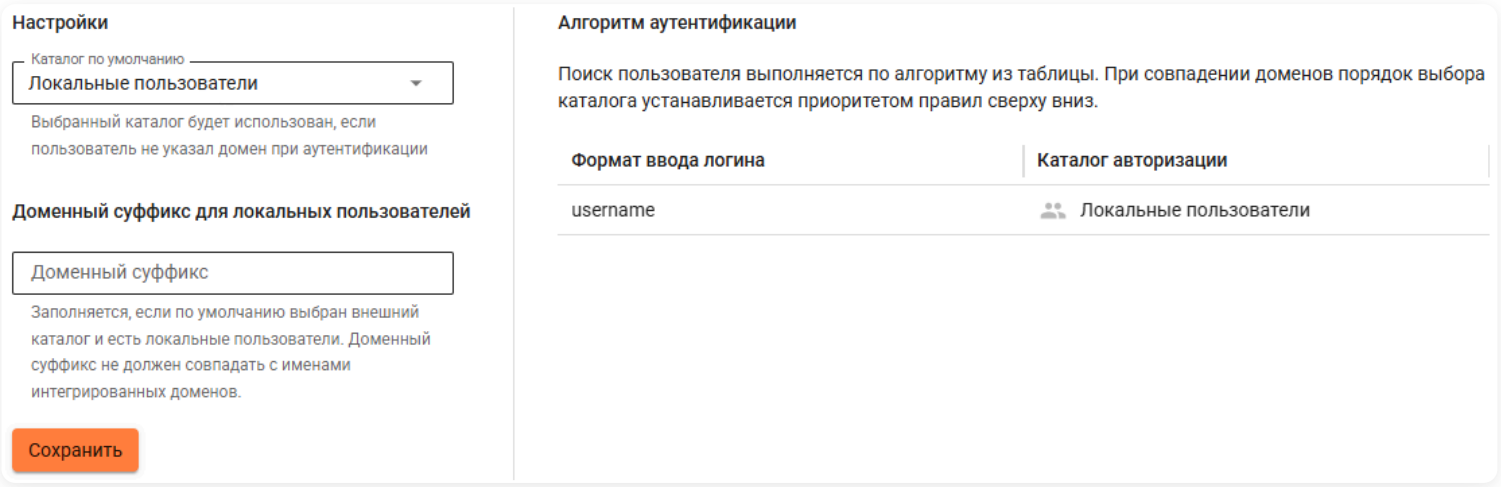
Аутентификация

Классический контекст | Высокопроизводительный контекст | API

Перейдите во вкладку **Основное** для настройки каталогов аутентификации пользователей Ideco NGFW Novum.

Настройки

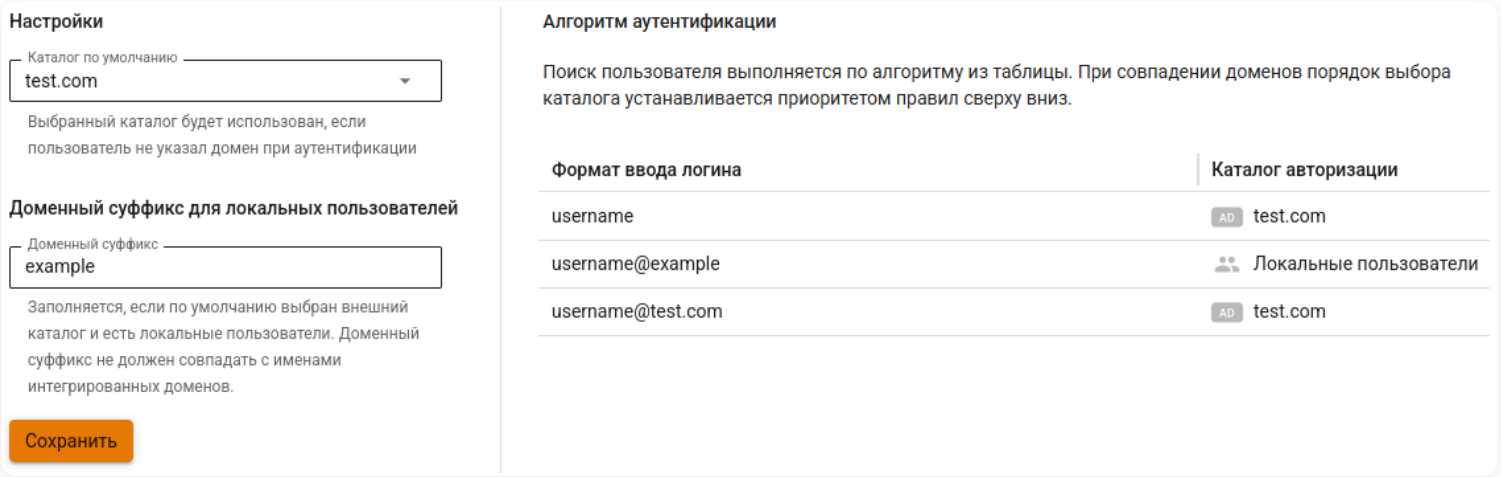
Укажите **Каталог по умолчанию**:



- **Каталог по умолчанию** - определяет каталог для аутентификации пользователей без указания домена. Такой подход позволяет избежать ошибок аутентификации при наличии пользователей с одинаковыми логинами в разных каталогах. Доступные каталоги: локальные пользователи, домен AD/ALD/FreeIPA, интеграция с RADIUS. При интеграции с несколькими доменами AD/ALD/FreeIPA в качестве **Каталога по умолчанию** доступен выбор только одного из них.

Доменный суффикс для локальных пользователей

Введите условный домен, который локальные пользователи будут указывать вместе с логином для аутентификации. Настройка нужна при наличии локальных пользователей и при выборе в качестве **Каталога по умолчанию** домена AD/ALD/FreeIPA или RADIUS. Например, при суффиксе `example` локальный пользователь вводит логин в формате `username@example`:



Условный домен нужен только для выбора каталога **Локальные пользователи** при аутентификации. В ходе поиска по каталогу учитывается только логин пользователя, доменный суффикс отбрасывается.

Алгоритм аутентификации

Описанный ниже алгоритм применяется при аутентификации **по логину и паролю**, когда каталог определяется по доменному суффиксу, указанному в логине после `@`, или по **Каталогу по умолчанию** при отсутствии доменного суффикса в логине.

При **SSO-аутентификации** каталог выбирается иначе - среди интеграций с AD и ALD Pro, без учета **Каталога по умолчанию** и доменного суффикса. Подробнее в разделе **Выбор каталога при SSO-аутентификации**.

В таблице **Алгоритм аутентификации** перечислены все доступные каталоги и формат ввода логина для каждого каталога, включая UPN-суффиксы для Active Directory в порядке добавления.

Не рекомендуется использовать одинаковые наименования доменов в разных интеграциях. При совпадении доменов выбор каталога для поиска пользователя выполняется в приоритете:

1. Локальный каталог, если добавлен доменный суффикс.

2. Каталог AD.

3. Каталог ALD.

4. Каталог FreeIPA.

5. Каталог RADIUS.

Если при аутентификации пользователя не указан домен, поиск осуществляется только в **Каталоге по умолчанию**. Если указан неизвестный Ideco NGFW Novum домен, поиск выполняется в каталоге RADIUS при наличии интеграции.

Примеры настроек при использовании нескольких каталогов одновременно

Аутентификация локальных пользователей без указания домена

1. В поле **Каталог по умолчанию** выберите значение **Локальные пользователи**.

2. Поле **Доменный суффикс для локальных пользователей** можете оставить без изменений.

При такой настройке аутентификация пользователей AD, ALD, FreeIPA и RADIUS выполняется только с указанием домена. Доменный суффикс для RADIUS настраивается только на RADIUS-сервере.

Аутентификация пользователей из каталога AD/ALD/FreeIPA без указания домена

1. В поле **Каталог по умолчанию** выберите конкретный домен AD/ALD/FreeIPA.

2. В поле **Доменный суффикс для локальных пользователей** укажите условный домен, который локальные пользователи будут использовать для аутентификации. Настройка актуальна при наличии локальных пользователей.

Действие настройки:

- Пользователи выбранного каталога могут аутентифицироваться без указания домена или с указанием домена AD/ALD/FreeIPA.
- Аутентификация пользователей в каталогах AD/ALD/FreeIPA, не выбранных как **Каталог по умолчанию**, осуществляется только с указанием домена.
- Локальные пользователи аутентифицируются с указанием условного домена, настроенного в поле **Доменный суффикс для локальных пользователей**.
- Аутентификация пользователей RADIUS осуществляется только с указанием домена. Доменный суффикс для RADIUS настраивается только на RADIUS-сервере.

Аутентификация пользователей RADIUS без указания домена

1. В поле **Каталог по умолчанию** выберите RADIUS.

2. В поле **Доменный суффикс для локальных пользователей** укажите условный домен, который локальные пользователи будут использовать для аутентификации. Настройка актуальна при наличии локальных пользователей.

Действие настройки:

- Пользователи RADIUS могут аутентифицироваться без указания домена или доменом, используемым в RADIUS.
- Аутентификация пользователей AD/ALD/FreeIPA осуществляется только с указанием домена.
- Локальные пользователи аутентифицируются с указанием условного домена, настроенного в поле **Доменный суффикс для локальных пользователей**.

При настройке авторизации в почте проверьте, чтобы основной или дополнительный почтовый домен, указанный в **Почтовый релей** → **Основные настройки**, совпадал с доменом **Каталога авторизации** для успешной аутентификации. В противном случае аутентификация

будет выполняться через **Каталог по умолчанию**: если пользователь есть в каталоге, аутентификация пройдет успешно по логину, указанному до `@`.

Настройку **Доменный суффикс для локальных пользователей** можно использовать совместно с настройкой почтового домена, чтобы для этого почтового домена использовался каталог **Локальные пользователи**.

Двухфакторная аутентификация

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Двухфакторная аутентификация**: `ideco-web-authd`.

Список служб для других разделов доступен по ссылке.

Двухфакторная аутентификация позволяет аутентифицировать локальных и внешних пользователей (в том числе для VPN и для личного кабинета) с использованием второго фактора.

В Ideco NGFW Novum реализовано четыре типа двухфакторной аутентификации:

- **TOTP-токен** - сканированием QR-кода или с помощью токена.
- **SMS Aero** - при помощи ввода кода из SMS.
- **Мультифактор** - путем подтверждения личности в приложении.
- **RADIUS-серверы** - через RADIUS-серверы. Тип двухфакторной аутентификации работает независимо от интеграции с RADIUS.

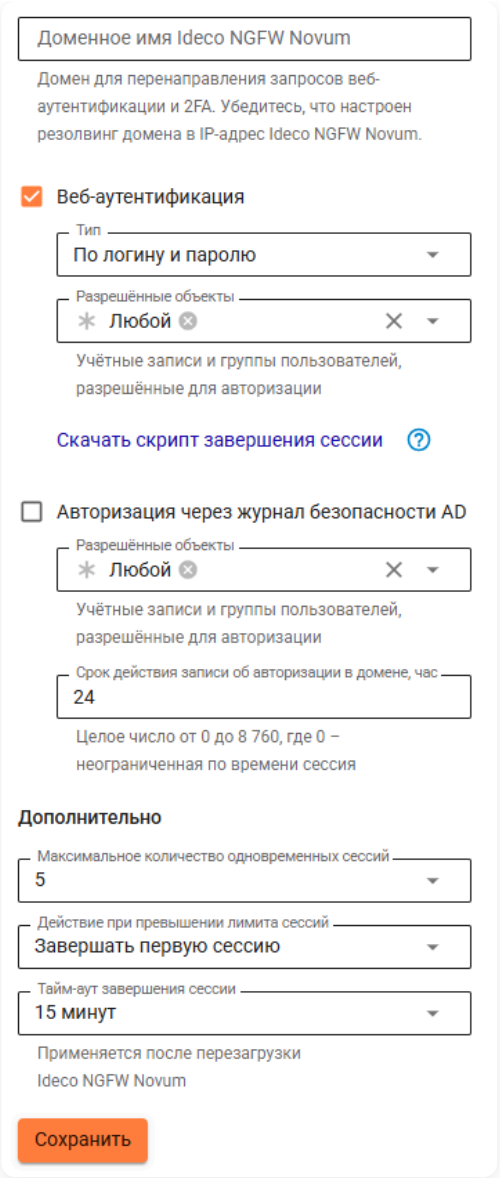
Настройка двухфакторной аутентификации для администраторов Ideco NGFW Novum производится в разделе **Управление сервером** → **Администраторы** → **Двухфакторная аутентификация**.

Для входа в личный кабинет Ideco NGFW Novum с использованием **Мультифактора** необходим доступ в интернет.

Настройки Ideco NGFW Novum с разными типами аутентификации

Для работы двухфакторной аутентификации выполните действия:

1. Перейдите в **Пользователи** → **Авторизация** и включите веб-аутентификацию:



2. Укажите домен Ideco NGFW Novum в поле **Доменное имя Ideco NGFW Novum**, чтобы на сервер перенаправлялись запросы двухфакторной аутентификации.

3. Настройте VPN-подключение в **Пользователи** → **VPN-подключения** → **Основное**, воспользовавшись инструкцией.

4. Перейдите в **Пользователи** → **Аутентификация** → **Двухфакторная аутентификация**. Включите необходимые типы аутентификации:

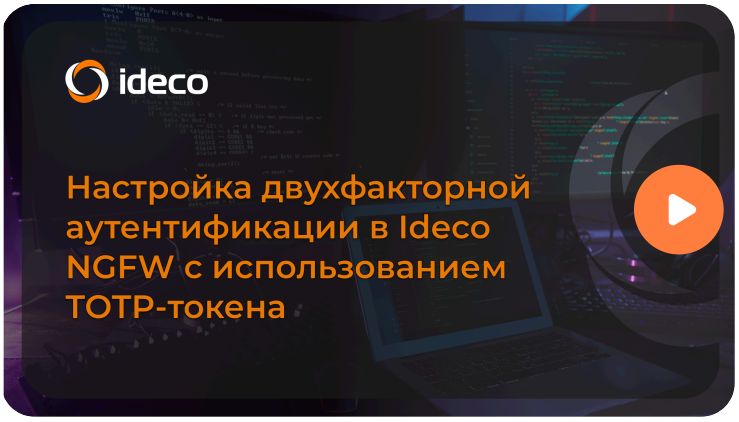
TOTP-токен

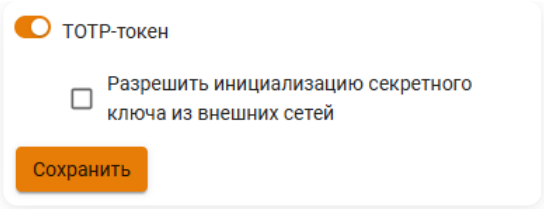
Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE VK Видео





- **Включить** - опция включает TOTP-аутентификацию.
- **Разрешить инициализацию секретного ключа из внешних сетей** - включение опции разрешает пользователям сканировать QR-код в личном кабинете при подключении из внешних сетей.

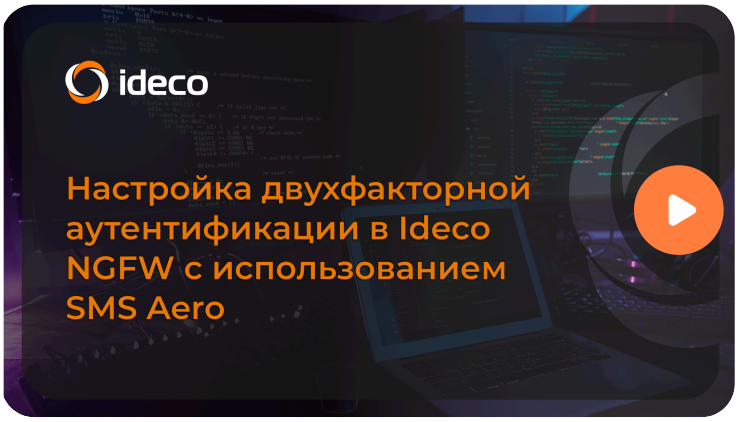
SMS Aero

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

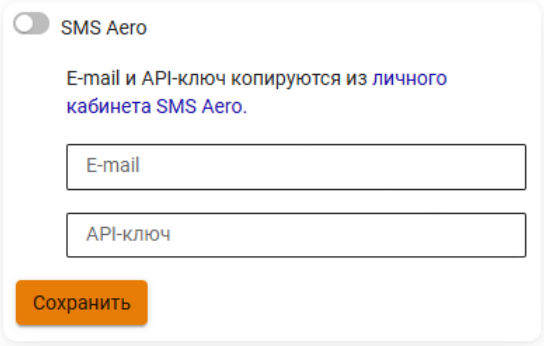
Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Предварительно зарегистрируйтесь в личном кабинете SMS Aero.

1. Введите **e-mail** и **API-ключ** от личного кабинета SMS Aero:



API-ключ можно найти в разделе **Настройки → API и SMPPI**.

2. Если требуется, включите опции:

- **Задать имя отправителя вручную** - рекомендуем использовать, если имя отправителя недоступно.
- **Добавить текст сообщения** - введите текстовое сообщение, которое будет отображаться для получателя. Если опцию не использовать, будет отправлен только код.

3. Нажмите **Сохранить**.

При необходимости можно проверить настройки второго фактора, введя **Номер для тестового СМС** и нажав **Отправить СМС**.

Мультифактор

Видеоинструкция



Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

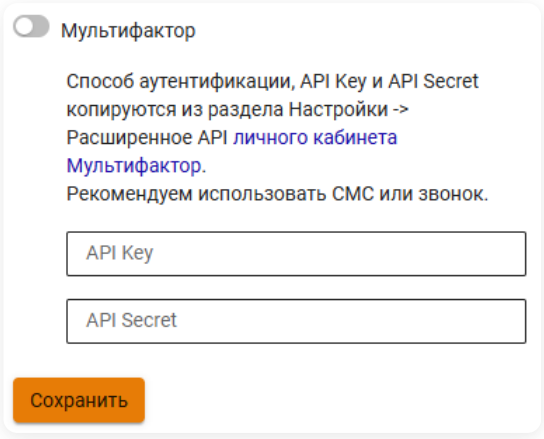
YouTube | RUTUBE | VK Видео

Помимо приложения Multifactor для аутентификации можно использовать Telegram, Яндекс.Ключ, Биометрию и U2F. Подробное описание регистрации и аутентификации этими методами доступно в документации Multifactor.

Предварительно зарегистрируйтесь в системе управления Мультифактором, установите приложение Multifactor и активируйте, отсканировав QR-код.

1. Скопируйте значение полей в личном кабинете пользователя Multifactor в разделе **Настройки** → **Расширенное API** → **Включить API**.

2. Заполните **API Key** и **API Secret**:



3. Нажмите **Сохранить**.

Для дальнейшей аутентификации пользователям потребуется установить и настроить приложения, указанные администратором в настройках группы. Корректировать способы аутентификации для пользователей можно в личном кабинете Multifactor, в разделе **Группы** → **Параметры** → **Редактировать**.

RADIUS-сервер

При необходимости можно настроить несколько RADIUS-серверов для двухфакторной аутентификации. Для каждого выполните шаги:

1. Нажмите **Добавить**.

2. Заполните поля:



- **Название** - уникальное название способа 2FA, которое будет использоваться в настройке доступа. Запрещены названия `TOTP-токен`, `Мультифактор` и `SMS Aero`.
- **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
- **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
- **Порт** - порт, по которому будет происходить подключение к серверу.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
  - **Количество попыток подключения** - число попыток отправки запроса на RADIUS-сервер. В диапазоне от 1 до 5. По умолчанию 3.
- **Режим запроса к RADIUS** - режим запроса на аутентификацию от Ideco NGFW Novum:
  - **Содержимое запроса**:
    - **Логин** - передача в запросе на RADIUS-сервер только логина, пароль остается пустым. В настройках RADIUS-сервера должен быть прописан пропуск проверки пароля в первом запросе. RADIUS-сервер должен проверять только логин для идентификации пользователя.
    - **Логин и OTP-код** - передача логина и OTP-кода. Установите, если RADIUS-сервер не поддерживает запрос без пароля.
  - **Сообщение при вводе OTP-кода** - сообщение, которое увидит пользователь при двухфакторной аутентификации в режиме передачи **Логин и OTP-код**. Должно содержать информацию для пользователя с конкретизацией, откуда он должен взять OTP-код. В режиме передачи **Логин** поле не используется, выводится сообщение от RADIUS-сервера (Reply-Message).
- **Комментарий** - необязательное поле.

3. Нажмите **Сохранить**.

Поддерживается взаимодействие с RADIUS-сервером только по протоколу PAP (Password Authentication Protocol).

5. Разрешите доступ по VPN нужным группам пользователей в **Пользователи** → **VPN-подключения** → **Доступ по VPN**, воспользовавшись инструкцией.

При отключении типа аутентификации, который используется в таблице **Доступ по VPN**, будет выведено предупреждение **Используется для доступа по VPN**. При этом аутентификация пройдет без второго фактора.

Настройка аутентификации на пользовательских устройствах

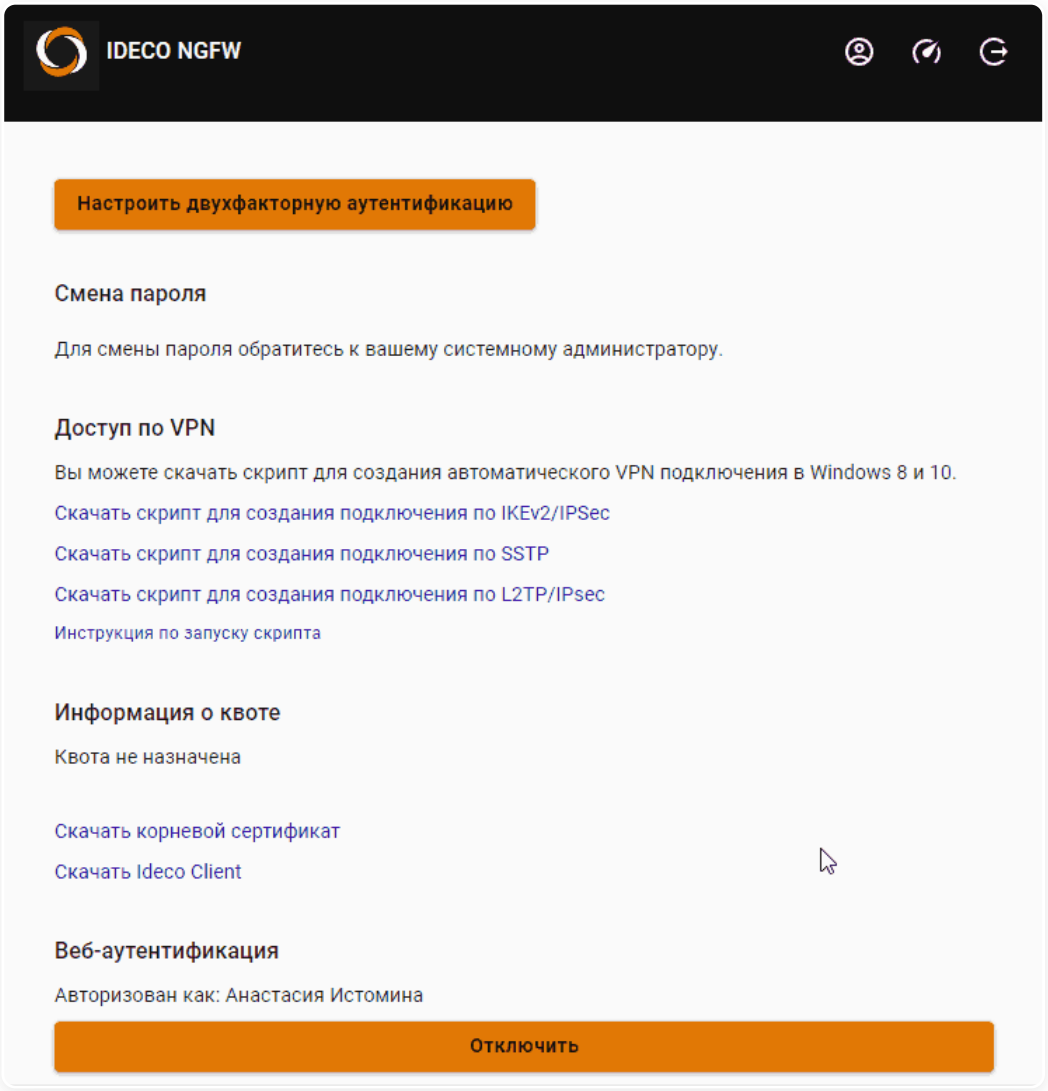
Для настройки двухфакторной аутентификации на устройстве пользователя воспользуйтесь инструкциями:

TOTP-токен

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Войдите в личный кабинет NGFW, указав логин и пароль пользователя.

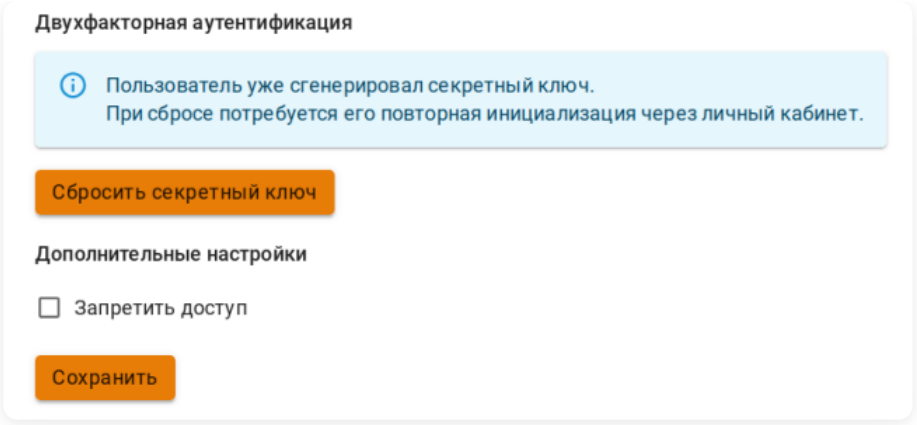
3. Нажмите кнопку **Настроить двухфакторную аутентификацию** и выберите **Сгенерировать QR-код**:



4. Войдите в приложение для аутентификации (например, Яндекс ID, Google Authenticator или Microsoft Authenticator), отсканируйте QR-код или введите секретный ключ, который находится под QR-кодом. При вводе ключа выберите тип ключа **По времени**. Если выбрать тип **По счетчику**, то пользователь не сможет пройти аутентификацию.

Если вернуться в личный кабинет, не отсканировав QR-код, то повторно QR-код появится только после сброса секретного ключа в карточке пользователя.

Чтобы сбросить секретный ключ, перейдите в **Пользователи** → **Учетные записи**. Выберите нужного пользователя и нажмите **Сбросить секретный ключ**:



5. Подключитесь к VPN и откройте любой сайт, не использующий **HSTS** (например, neverssl.com). В появившемся поле введите код, который получили в приложении:

Особенности использования TOTP-токена:

- Для корректной работы необходимо, чтобы время на Ideco NGFW Novum и устройстве пользователя было синхронизировано с точностью до минуты.
- Если секретный ключ был сброшен во время аутентификации пользователя и пользователь не смог пройти аутентификацию, то необходимо удалить сессию пользователя в разделе **Мониторинг → Сессии пользователей**. Сессия будет автоматически завершена по истечении десяти минут бездействия.

SMS Aero

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Если требуется использовать подключение только для ресурсов подключаемой сети, убедитесь, что настройки VPN-подключения соответствуют требованиям:

Для Windows 10:

- Откройте параметры и перейдите в **Сеть и Интернет → VPN → Настройка параметров адаптера**.
- Нажмите правой кнопкой мыши по созданному подключению и выберите **Свойства**.
- Перейдите на вкладку **Сеть**.
- Нажмите на **IP версии 4 (TCP/IPv4) → Свойства → Дополнительно**.
- Снимите флаг с пункта **Использовать основной шлюз в удаленной сети**.
- Нажмите **ОК**.

Для Ubuntu:

- Перейдите в **Настройки → Сеть**.
- Откройте настройки VPN-подключения.
- Перейдите на вкладку **IPv4**.
- Установите флаг в пункте **Использовать это подключение для ресурсов этой сети**.

3. Включите созданное VPN-подключение.

4. Перейдите в браузер, откроется страница аутентификации:

5. Нажмите **Отправить код подтверждения**. На номер телефона, указанный в учетной записи, придет SMS с кодом:

- Если номер телефона в карточке пользователя отсутствует, то на странице аутентификации появится предупреждение:

- Если номер телефона сохранен, то на указанный номер телефона поступит SMS. Введите код из SMS и нажмите **Подтвердить**:

- Если код введен неверно, то появится соответствующее предупреждение:

- Если код введен верно, то появится окно:

Для настройки таймкодов отправки сообщений перейдите в личный кабинет SMS Aero на вкладку **Настройки** и переведите опцию **Исключать множественную отправку** в положение **Включен**. Затем введите лимит и период отправки сообщений:

Мультифактор

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Включите созданное VPN-подключение.

3. При переходе в браузер откроется страница аутентификации:

4. После нажатия **Далее** появится страница с предложением установить приложение на устройство пользователя. Если приложение установлено, нажмите **Далее**.

5. Отсканируйте QR-код или откройте ссылку, которая появится на экране.

6. Нажмите **Выполнить вход**:

7. В окне **Двухфакторная аутентификация** выберите способ аутентификации:

8. В зависимости от выбранного способа подтвердите вход.

RADIUS-сервер

В отличие от остальных способов RADIUS-сервер при настройке двухфакторной аутентификации работает как посредник. RADIUS-сервер только передает код подтверждения в сервис 2FA, а сервис 2FA проверяет его корректность. Настройка второго фактора осуществляется в личном кабинете выбранного сервиса двухфакторной аутентификации. Для настройки используйте документацию соответствующего сервиса.

В зависимости от того, какая система 2FA используется, после ввода логина и пароля в NGFW Novum инициируется запрос на авторизацию через RADIUS-сервер:

- Если от сервера не ожидается код (например, при использовании биометрии), пользователь авторизуется.
- Если от сервера ожидается код подтверждения, введите код и нажмите **Подтвердить**:

- Если доступ запрещен или ответ от RADIUS-сервера не получен, появится окно:

> Предпочтительными являются современные системы с беспарольной аутентификацией (FIDO2-ключи, биометрия). Рекомендуем увеличить время ожидания от RADIUS-сервера в случае использования таких систем.

2FA при помощи БИТ.Аутентификатор

1. Установите клиентский портал БИТ.Аутентификатор по инструкции.

2. В клиентском портале БИТ.Аутентификатор в разделе **Домены проекта** создайте домен. В поле **Название** укажите домен Active Directory и получите API-ключ.

3. Перейдите в раздел **Настройки** и настройте портал на работу с сервером Active Directory и Ideco NGFW Novum, заполнив поля:

- **Служба каталогов** - выберите Active Directory.
- **Адрес службы** - укажите IP-адрес DNS-сервера Active Directory.
- **DN сервисного пользователя** - укажите Distinguished Name учетной записи, от имени которой система будет подключаться к Active Directory для выполнения поиска и проверки данных.
- **Пароль** - укажите пароль Distinguished Name учетной записи.

- **Администраторы** - укажите учетные записи или группы Active Directory, которые будут обладать правами администраторов.
- **Адрес портала** - укажите домен Active Directory.
- **Разрешенные способы проверки второго фактора** - выберите способы проверки второго фактора.
- **Секрет RADIUS** - укажите секрет RADIUS. Поле должно соответствовать секрету RADIUS в Ideco NGFW Novum.

4. Настройте интеграцию Active Directory и Ideco NGFW Novum по инструкции.

5. В Ideco NGFW Novum перейдите в **Пользователи** → **Внешние каталоги** → **Active Directory/Samba DC** и заполните поля:

- **Домен или IP-адрес** - укажите IP-адрес сервера БИТ.Аутентификатор.
- **Секрет** - укажите секрет RADIUS из настроек клиентского портала БИТ.Аутентификатор.
- **Порт** - порт, по которому будет происходить подключение к серверу.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
  - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.

6. Нажмите **Сохранить** и проверьте соединение.

7. Перейдите в **Аутентификация** → **Двухфакторная аутентификация** → **RADIUS-серверы**, нажмите **Добавить** и заполните поля:

- **Название** - укажите название сервера Active Directory.
- **Домен или IP-адрес** - укажите IP-адрес сервера БИТ.Аутентификатор.
- **Порт** - порт, по которому будет происходить подключение к серверу.
  - **Настройки подключения к серверу**:
    - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
    - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.

8. На клиентском портале БИТ.Аутентификатор в разделе **Ресурсы** добавьте ресурс:

- **Название** - укажите название сервера Active Directory.
- **Описание** - необязательное поле.
- **IP-адреса (через ;)** - укажите IP-адрес Ideco NGFW Novum.
- **Разрешен вход (группы через ;)** - пользователи домена.
- **Проверять второй фактор, если настроен (группы через ;)** - пользователи домена.
- **Требовать второй фактор (группы через ;)** - пользователи домена.
- **Второй фактор выключен (группы через ;)** - оставьте поле пустым.
- **LDAP порт** - оставьте значение **Нет**.
- **LDAPS порт** - оставьте значение **Нет**.
- **RADIUS порт** - должен соответствовать полю **Порт** настроек RADIUS-сервера в Ideco NGFW Novum. По умолчанию: `1812`.

9. Создайте VPN-подключение.

10. На вкладке **Доступ по VPN** в поле **Способ 2FA** выберите сервер RADIUS, созданный на шаге 7.

11. Установите VPN-соединение и пройдите проверку второго фактора одним из выбранных способов на шаге 3.

Алгоритм двухфакторной аутентификации с RADIUS-сервером

Алгоритм двухфакторной аутентификации с RADIUS-сервером при любом типе подключении зависит от выбранного режима запроса - **Логин** или **Логин и OTP-код**.

По логину

1. Пользователь указывает логин и пароль и инициирует подключение.

2. NGFW Novum проверяет логин и пароль.

3. При успешной проверке NGFW Novum отправляет на RADIUS-сервер **Access-Request** с логином и пустым паролем.

> RADIUS-сервер должен быть настроен на пропуск проверки пароля и использовать первый запрос только для идентификации

пользователя по логину.

4. После успешной идентификации RADIUS-сервер выбирает тип второго фактора согласно политикам и запрашивает код у пользователя.

5. Пользователь вводит код второго фактора.

6. RADIUS-сервер проверяет второй фактор и завершает аутентификацию.

По логину и OTP-коду

1. Пользователь указывает логин и пароль и инициирует подключение.

2. NGFW Novum проверяет логин и пароль.

3. При успешной проверке NGFW Novum запрашивает у пользователя ввод кода из приложения для аутентификации.

4. NGFW Novum отправляет на RADIUS-сервер **Access-Request**, содержащий логин и введенный пользователем OTP-код.

5. RADIUS-сервер выполняет проверку кода второго фактора и завершает аутентификацию.

Полезные ссылки

- **Как безопасно подключить удаленного подрядчика**

Авторизация

Классический контекст | Высокопроизводительный контекст | API

> Настройка правил авторизации пользователей в Ideco NGFW Novum.

Название службы раздела **Авторизация**: `ideco-auth-backend`.

Список служб для других разделов доступен по ссылке.

Авторизация - необходимое условие для доступа пользователя в интернет. Для работы в пределах локальной сети авторизация не требуется.

Для доступа сетевого устройства (хоста) в интернет через NGFW Novum с возможностью контроля трафика, хост должен быть авторизован в системе под учетной записью пользователя.

Механизм авторизации в Ideco NGFW Novum

Авторизация позволяет системе идентифицировать трафик и применять к нему правила доступа и ограничения, настроенные для конкретного пользователя или группы. Сессия авторизации создается только при наличии разрешающего правила для используемого вида авторизации.

Доступ к сетям для авторизованных и неавторизованных пользователей настраивается через правила межсетевого экрана.

Возможные правила доступа:

- **Авторизация по VPN**. Можно настроить для подключения как из внешних, так и из локальных сетей.
- **Авторизация через Ideco Client без туннеля**. Правила можно настроить для конкретных пользователей, групп пользователей, групп безопасности, специальных объектов **Все пользователи AD**, **Любой** или используя LDAP-фильтры.
- **Авторизация пользователей терминальных серверов**. Правила можно настроить для конкретных пользователей AD, групп безопасности, специального объекта **Любой** или используя LDAP-фильтры. Настраивается для каждого терминального сервера отдельно.
- **Авторизация через журналы AD**. Правила можно настроить для конкретных пользователей AD, групп безопасности, специального объекта **Любой** или используя LDAP-фильтры.
- **Авторизация по WEB, включая SSO**. Правила можно настроить для конкретных пользователей, групп пользователей, групп безопасности, специальных объекстов **Все пользователи AD**, **Все доверенные пользователи**, **Любой** или используя LDAP-фильтры.
- **Авторизация по IP или MAC**. Подробнее в статье.
- **Авторизация по подсети**. Подробнее в статье.

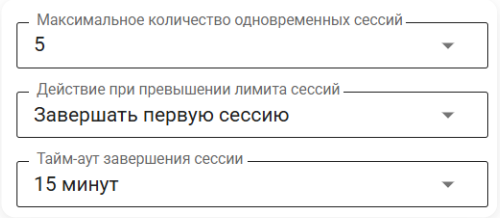
Особенности авторизации пользователей в Ideco NGFW Novum:

- Количество приобретенных по лицензии учетных записей ограничивает число авторизованных пользователей.
- Сессия авторизации учетной записи привязана к IP-адресу или к подсети (при авторизации по подсети) на протяжении действия сессии. У одного пользователя может быть несколько разных сессий.
- Хосты, не прошедшие авторизацию на NGFW Novum, лишены доступа к внешним сетям.
- Сессии авторизации пользователя, не проявляющего активность, завершаются по тайм-ауту и могут быть заняты новыми сессиями пользователей. Исключения:
  - Постоянная авторизация по IP/MAC.
  - Авторизация по подсети.
  - Терминальные пользователи.
  - VPN авторизация.
  - Ideco Client без туннеля.

Для настройки автоматической авторизации пользователей при входе в систему воспользуйтесь статьей.

Дополнительные настройки

Каждая сессия авторизации пользователя привязывается к IP-адресу устройства, с которого была инициирована. Выберите необходимые настройки для сессий:



- **Максимальное количество одновременных сессий** - ограничивает количество активных сессий для одного пользователя (диапазон: 1–6, значение по умолчанию: 5).
- **Действие при превышении лимита сессий** - определяет действие:
  - **Блокировать новую сессию** - авторизация с нового устройства будет невозможна.
  - **Завершать первую сессию** (по умолчанию) - самая старая сессия будет завершена.
- **Тайм-аут завершения сессии** - время до завершения сессии пользователя, если от него не поступает трафик. (диапазон: 10 минут – 24 часа, значение по умолчанию: 15 минут). Не распространяется на VPN. Для применения нового тайм-аута отключения требуется перезагрузка Ideco NGFW Novum.

Трафик может генерировать и сама операционная система без участия пользователя (например, телеметрия Windows). Из-за этого тайм-аут для пользователя будет постоянно сбрасываться.

Полезные ссылки

- **Настройка веб-аутентификации**
- **Настройка SSO-аутентификации**
- **Настройка авторизации через журнал безопасности AD**
- **Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT)**
- **Настройка Wi-Fi-сети**
- **Настройка прозрачной авторизации на Astra Linux**

Веб-аутентификация

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Веб-аутентификация**: `ideco-web-authd`, `ideco-web-backend`.

Список служб для других разделов доступен по ссылке.

Веб-аутентификация в Ideco NGFW Novum - тип авторизации, который предполагает, что отправленный через веб-браузер запрос неавторизованного пользователя будет переадресован на страницу авторизации Ideco NGFW Novum. Переход по указанному запросу произойдет после успешной авторизации.

Для этого типа авторизации должны быть выполнены условия:

- На сетевой карте у пользователя в качестве шлюза/объединенных в цепочку нескольких шлюзов или при прямых подключениях к прокси по умолчанию указан IP-адрес локального сетевого интерфейса Ideco NGFW Novum.
- До подключения к интернету работает **DNS-резолвинг адресов**. Иначе запрос браузера на адрес `example.com` не будет перенаправлен на шлюз, и в браузере не появится запрос логина и пароля.

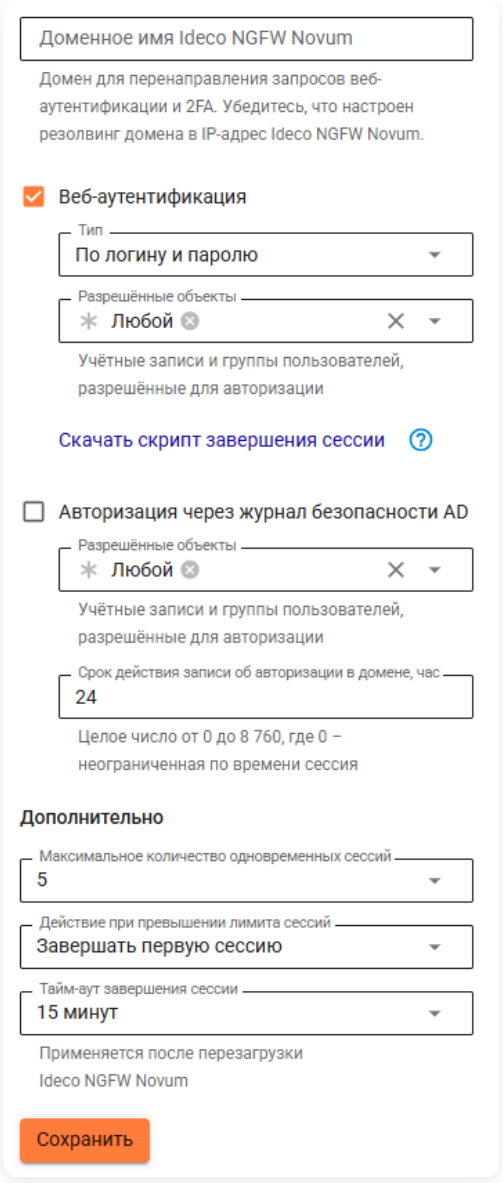
Проверить разрешение имен в Windows можно командой: `nslookup ya.ru`. Вывод данной команды должен содержать IP-адреса.

Рекомендуемые настройки для корректной работы веб-аутентификации:

- Добавьте сертификат Ideco NGFW Novum в доверенные корневые центры сертификации на устройстве (например, через политики домена).
- Укажите в качестве DNS-сервера на компьютерах и устройствах локальной сети IP-адрес локального интерфейса Ideco NGFW Novum.

Настройка авторизации через веб-интерфейс

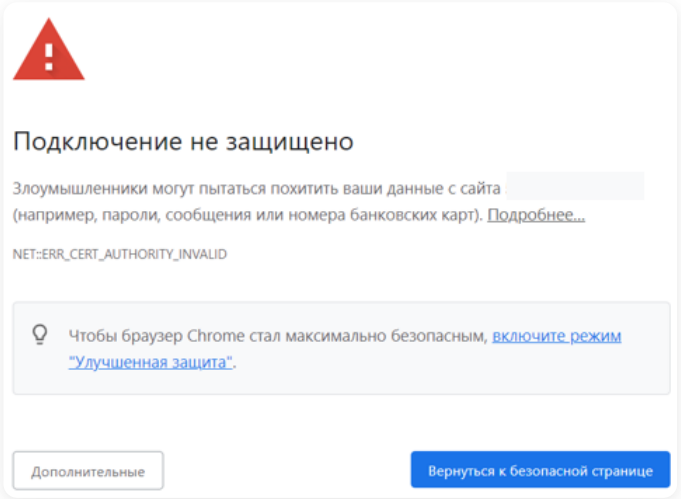
1. Выберите опцию **Веб-аутентификация** на вкладке **Пользователи** → **Авторизация** → **Настройки**:



2. Выберите **По логину и паролю** в поле **Тип**.

3. Выберите разрешенные для авторизации учетные записи или группы пользователей в поле **Разрешенные объекты**.

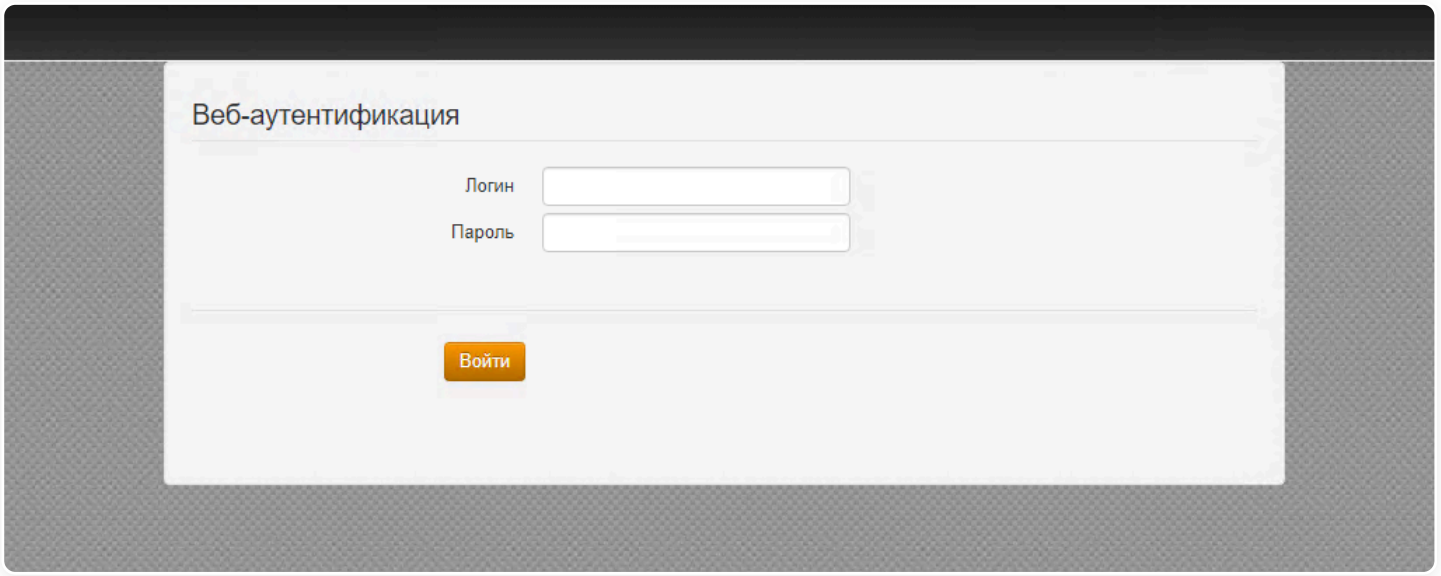
4. Заполните поле **Доменное имя Ideco NGFW Novum** и сохраните настройки, чтобы получить Let's Encrypt сертификат. Пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



Если Ideco NGFW Novum не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW Novum, страница авторизации будет подписана корневым сертификатом NGFW Novum.

Если сертификат для такого домена уже загружен в разделе Сертификаты, то будет использоваться загруженный сертификат, а новый сертификат выдаваться не будет.

5. Откройте веб-браузер с устройства пользователя. Должно появиться окно авторизации, где необходимо ввести логин и пароль от созданной на Ideco NGFW Novum учетной записи пользователя:



После прохождения пользователем веб-аутентификации доступ в интернет будет предоставлен до тех пор, пока авторизация не будет принудительно отменена или прекращена по неактивности пользователя.

Полезные ссылки

- **Настройка SSO-аутентификации**
- **Настройка авторизации через журнал безопасности AD**
- **Настройка автоматической веб-аутентификации на Ideco NGFW на Linux**
- **Настройка прозрачной авторизации на Astra Linux**

IP и MAC

Классический контекст | Высокопроизводительный контекст

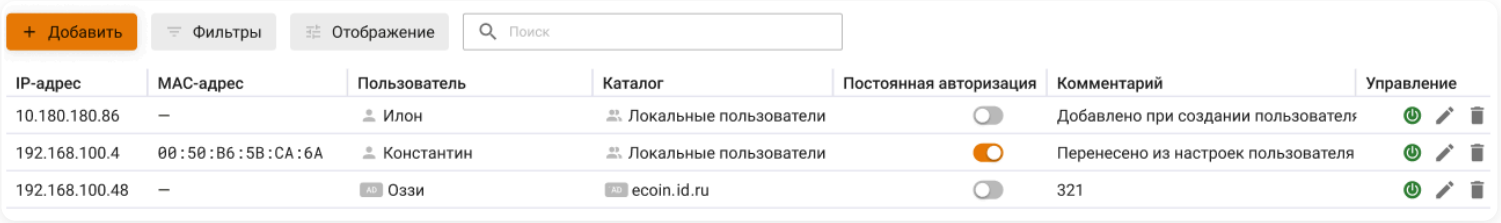
Принцип создания правил авторизации по IP и MAC в Ideco NGFW Novum.

Правила авторизации **IP и MAC** создают аналогичную привязку в **DHCP-сервере** Ideco NGFW Novum. Но если одни и те же IP- и MAC-адреса используются во включенных правилах DHCP-сервера, то правила DHCP-сервера выполняются в первую очередь.

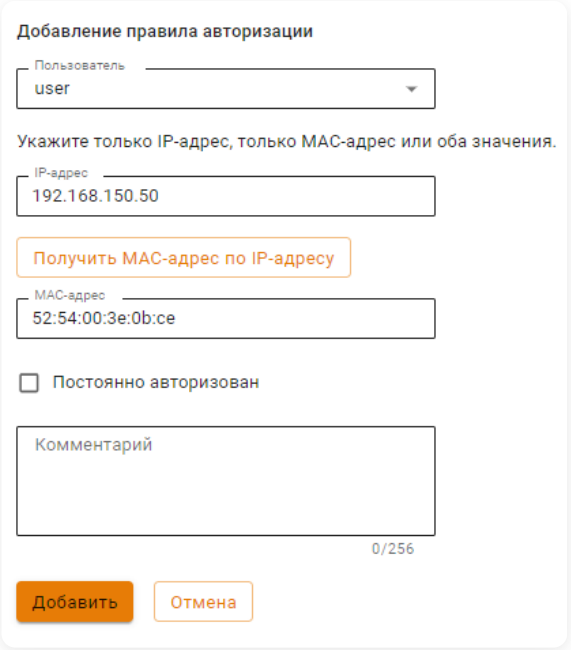
В правилах **IP и MAC** или **По подсетям** нельзя указывать пользователей RADIUS и DeviceVPN.

Настройка правила авторизации

1. Нажмите **Добавить** на вкладке **Авторизация → IP и MAC**:



2. Создайте правило привязки **IP и MAC**:



Расшифровка полей

- **Пользователь** - выберите пользователя из дерева пользователей.
- **IP-адрес** - введите IP-адрес устройства пользователя.
- **Получить MAC-адрес по IP-адресу** - нажмите для заполнения поля **MAC-адрес**. Кнопка активна, если IP-адрес пользователя и IP Ideco NGFW Novum в одной подсети.
- **Постоянно авторизован** - включите опцию, если требуется обеспечить непрерывный доступ в интернет. В этом случае лицензия будет закреплена за IP-адресом, даже если устройство выключено или пользователь неактивен. Настройка полезна для устройств/серверов, если количество пользователей может значительно увеличиться, исчерпав все лицензии.
- **Комментарий** - необязательное поле.

При наличии большого количества правил привязки в таблице воспользуйтесь кнопкой **Фильтры**.

Доступна сортировка по любому из столбцов таблицы.

Созданные на вкладке **Пользователи** → **Авторизация** → **IP и MAC** правила отражаются в карточке пользователя.

Полезные ссылки

Статьи об авторизации пользователей только по IP- или MAC-адресу:

- **Авторизация по MAC-адресу**
- **Авторизация по IP-адресу**

Авторизация по IP-адресу

Классический контекст | Высокопроизводительный контекст

При авторизации по IP пользователь получает доступ в интернет без ввода логина и пароля сразу после инициации подключения.

Доступна авторизация сетевых устройств (камеры видеонаблюдения, сетевые принтеры и прочее), которые находятся в разных с Ideco NGFW Novum широковещательных доменах и требуют доступ в интернет.

Если устройством является маршрутизатор, в котором включен SNAT, то при авторизации внешнего IP маршрутизатора на NGFW Novum, все пользователи за этим маршрутизатором получат доступ в интернет.

Пользователи, которые находятся за маршрутизатором в локальной сети Ideco NGFW Novum, не могут авторизоваться по IP+MAC, так как маршрутизатор не обрабатывает трафик уровня L2.

Если настроена авторизация по IP-адресу, то используемый IP-адрес не будет выдаваться DHCP.

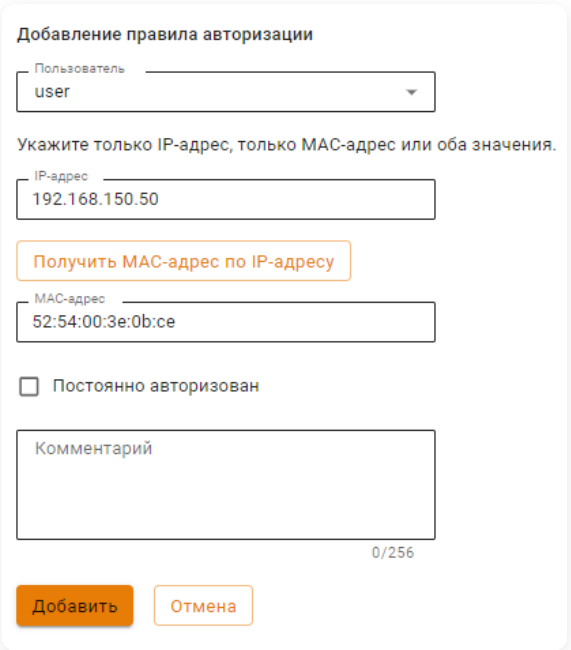
Настройка авторизации по IP

Для авторизации пользователя по IP-адресу:

1. Создайте пользователя.

2. Перейдите в **Пользователи → Учетные записи → Карточка пользователя → IP и MAC авторизация** или на вкладку **Пользователи → Авторизация → IP и MAC**.

3. Создайте правило-связку **IP-адрес <–> Пользователь**:



IP-адрес на устройстве, с которого инициируется сессия, должен совпадать с указанным в правиле. Кнопка **Получить MAC по IP** будет активна, если IP-адрес пользователя и IP Ideco NGFW Novum в одной подсети.

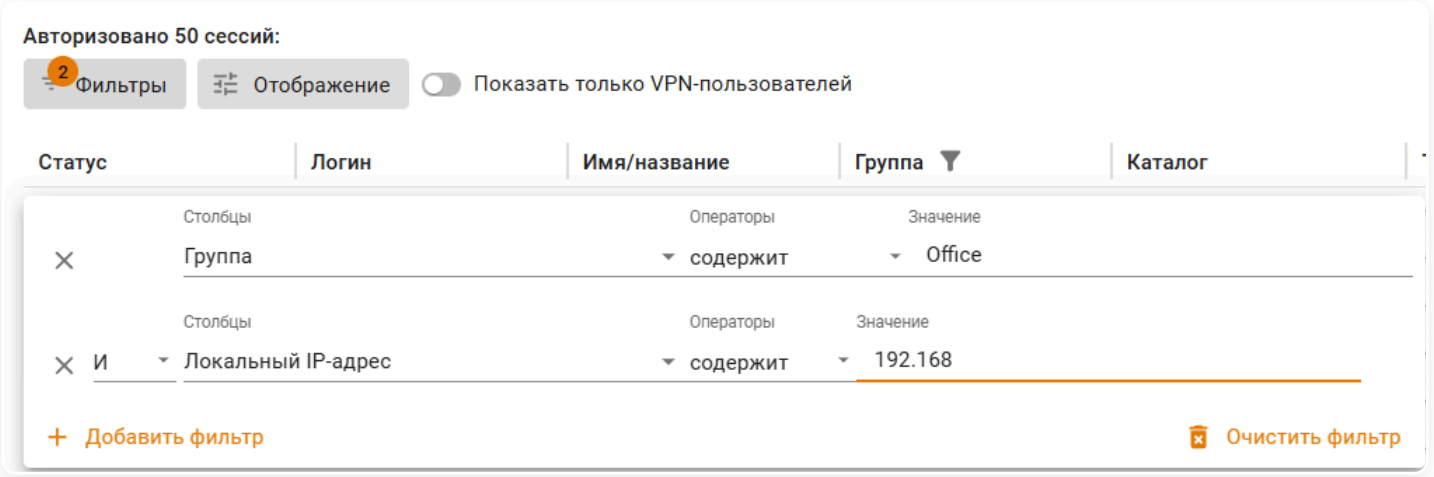
Рекомендации по использованию авторизации по IP-адресу:

- Настройте для пользователя, которым является сетевое оборудование, **Постоянную авторизацию**. Это позволит NGFW Novum создать сессию, а сетевому оборудованию не потребуется делать запрос в интернет.
- Настройте статический IP-адрес или DHCP с привязкой по IP-адресу. Это требуется, например, для ресурсов, опубликованных через DNAT.
- Воспользуйтесь поиском устройств для автоматического создания пользователей при попытке выхода в интернет. Подробнее о настройке в статье Обнаружение устройств.

При использовании авторизации по IP со статической привязкой в DHCP рекомендуем перенести такие правила на авторизацию по MAC-адресу.

Просмотр сессии

После запроса пользователя в интернет на Ideco NGFW Novum в разделе **Мониторинг** → **Сессии пользователей** автоматически создается сессия с типом авторизации `IP`:



У сессий с типом `IP` не заполняется поле **MAC-адрес**, так как уже указан IP-адрес, необходимый для создания сессии.

Авторизация по MAC-адресу

Функциональность доступна в **Классическом** и **Системном контекстах**.

Авторизация по MAC-адресу подойдет для тех устройств, у которых время от времени меняется местоположение между локальными сетями внутри организации (например, рабочие ноутбуки сотрудников), а также сетевых устройств, на которых не настроена привязка IP+MAC и IP-адрес выдается через DHCP.

Для авторизации пользователя на Ideco NGFW Novum по MAC-адресу устройство пользователя и Ideco NGFW Novum должны находиться в одном широковещательном домене, а Ideco NGFW Novum должен выступать шлюзом для этого устройства.

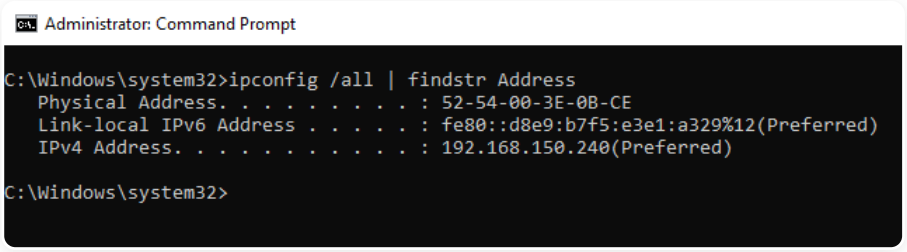
Пользователи, находящиеся за роутером в локальной сети Ideco NGFW Novum, не могут авторизоваться по MAC-адресу, так как роутер разделяет широковещательные домены и не обрабатывает трафик уровня L2. Такие пользователи могут авторизоваться только по IP-адресу.

Для работы MAC-авторизации необходимо, чтобы NGFW Novum и устройство пользователя находились в одном L2-сегменте сети.

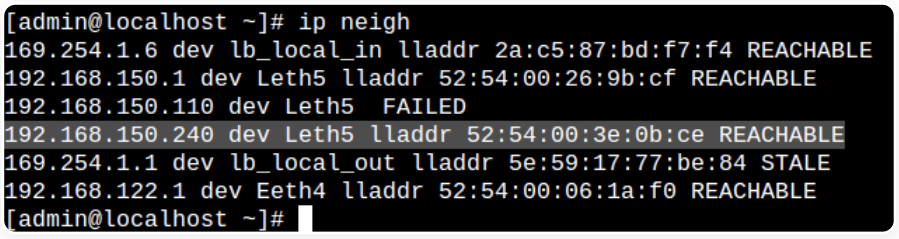
Настройка авторизации по MAC-адресу

Для авторизации пользователя по MAC-адресу:

1. Узнайте MAC-адрес устройства. Для этого в командной строке Windows введите `ipconfig /all | findstr Address` или `ipconfig /all | findstr адрес` (для русскоязычной версии):



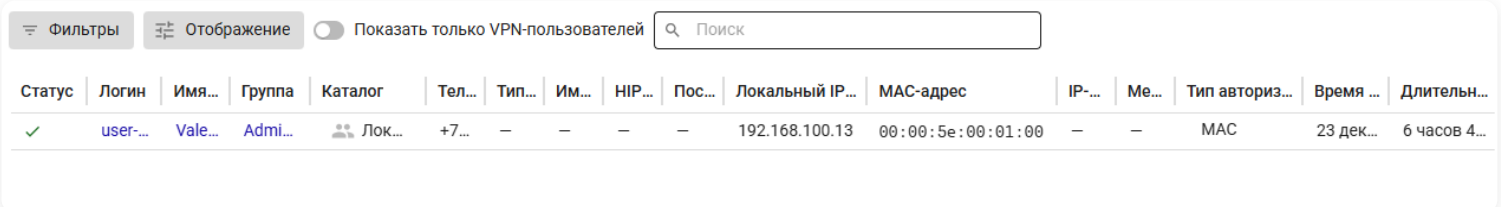
2. Удостоверьтесь, что устройство пользователя и NGFW Novum находятся в одном широковещательном домене. Для этого в **Управление сервером** → **Терминал** веб-интерфейса Ideco NGFW Novum введите команду `ip neigh`:



Эта команда выводит ARP-таблицу Ideco NGFW Novum. Наличие записи с MAC-адресом устройства и статусом REACHABLE - маркер L2-доступности между NGFW Novum и устройством пользователя.

3. Создайте правило-связку **Пользователь <--> MAC-адрес** на вкладке **Пользователи** → **Авторизация** → **IP и MAC**.

Сессия с типом авторизации `MAC` отобразится в разделе **Мониторинг** → **Сессии пользователей**:



Для MAC-адресов невозможно настроить постоянную авторизацию, так как для создания авторизованной сессии необходим IP-адрес. Рекомендуется использовать MAC-авторизацию в комбинации с DHCP-сервером.

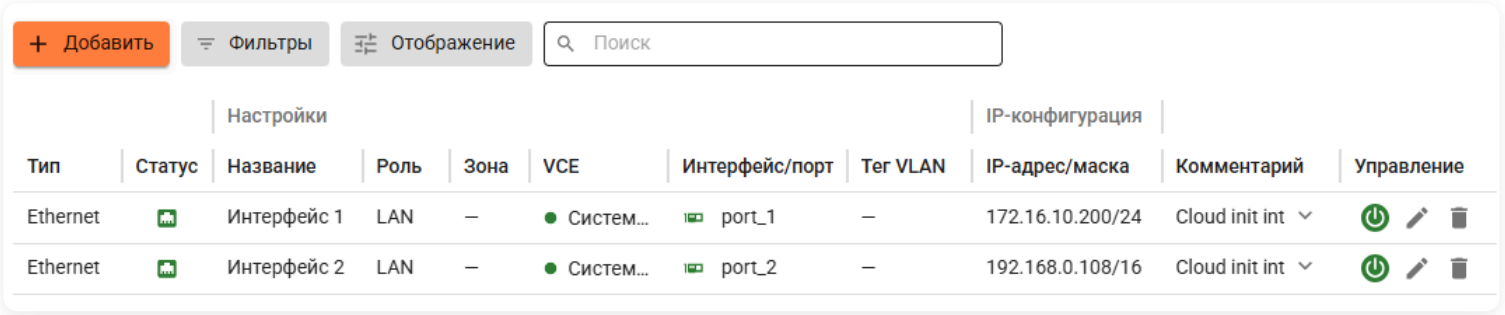
Поведение MAC-авторизации при перемещении устройства между локальными сетями

В организациях часто возникает ситуация, когда необходимо перемещаться между локальными сетями с ноутбуком и при этом всегда оставаться в сети. В таких случаях рекомендуется использовать авторизацию по MAC-адресу.

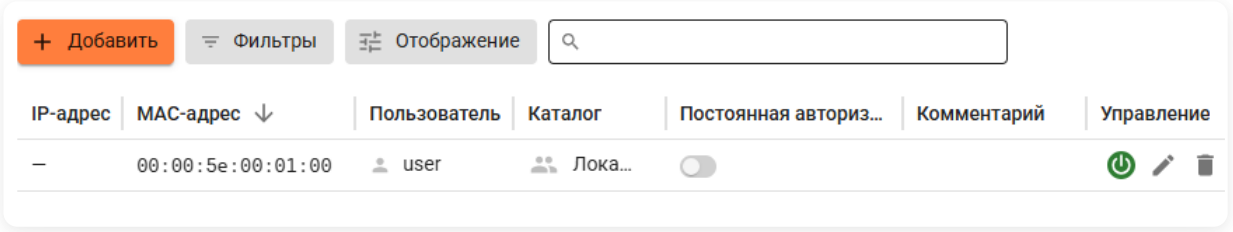
Для авторизации по MAC настройте DHCP-сервер (собственный или на NGFW Novum). В раздаваемых реквизитах шлюзом должен выступать локальный интерфейс NGFW Novum.

Пример. Пользователю `user` понадобилось переместиться с ноутбуком между локальными сетями:

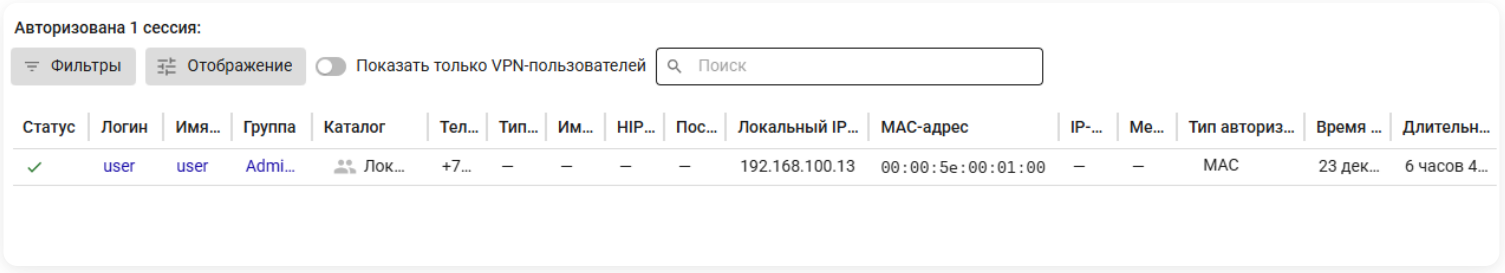
- На NGFW Novum настроены локальные интерфейсы:



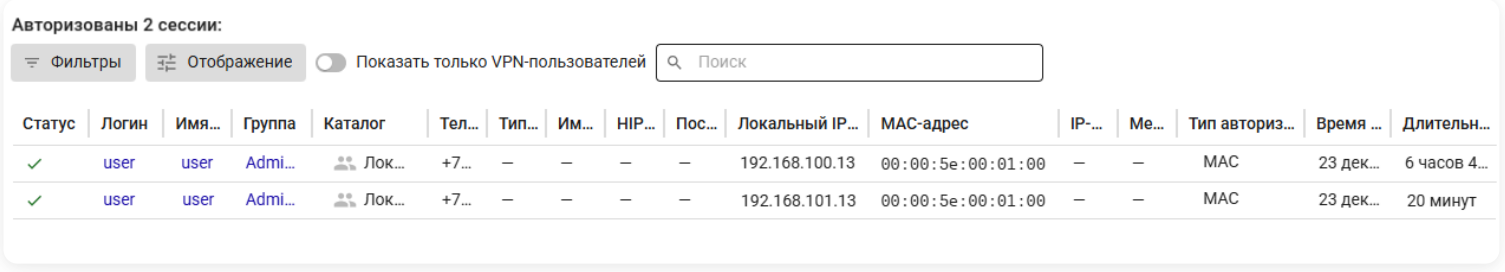
- Настроено правило авторизации пользователя по MAC-адресу:



- У пользователя одна активная сессия в разделе **Сессии пользователей**:



При переходе пользователя из одной локальной сети в другую ему выдаются другие сетевые реквизиты от DHCP-сервера, в которых шлюзом указан NGFW Novum. При обнаружении любой активности пользователя появится вторая сессия авторизации по MAC-адресу:



Если у пользователя не появляется доступ и вторая сессия с авторизацией по MAC-адресу, следует обновить сетевые реквизиты.

Сбросьте старые сетевые настройки от DHCP-сервера и получите новые с помощью команд:

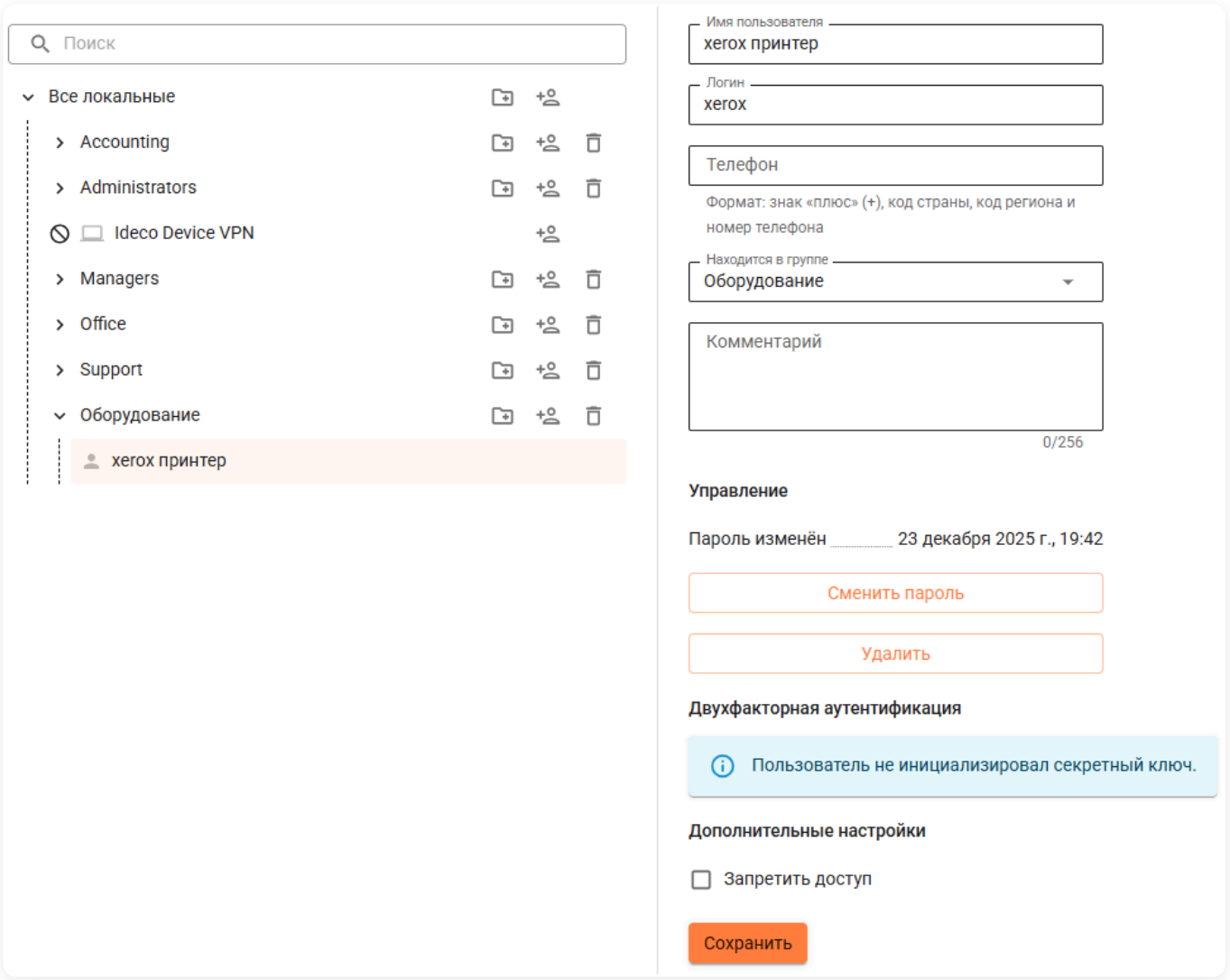
- Windows - `ipconfig /release && ipconfig /renew`;

- Linux - `sudo dhclient -r <имя_интерфейса>`.

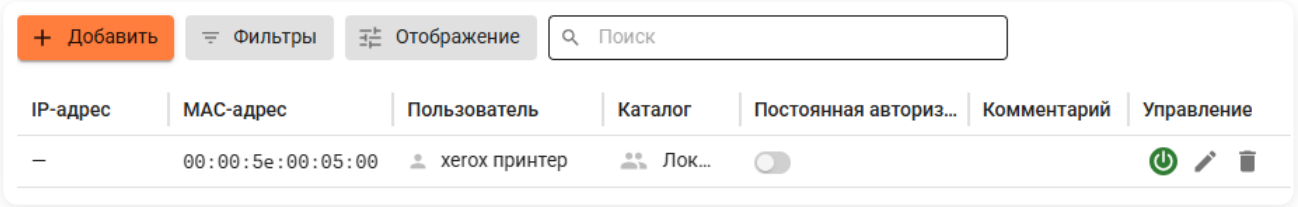
Настройка авторизации по MAC-адресу для сетевого принтера и других сетевых устройств

Сетевые устройства, которым необходим доступ в интернет, должны быть авторизованы на NGFW Novum. Такие устройства можно назвать статическими, для них подойдет авторизация по MAC-адресу.

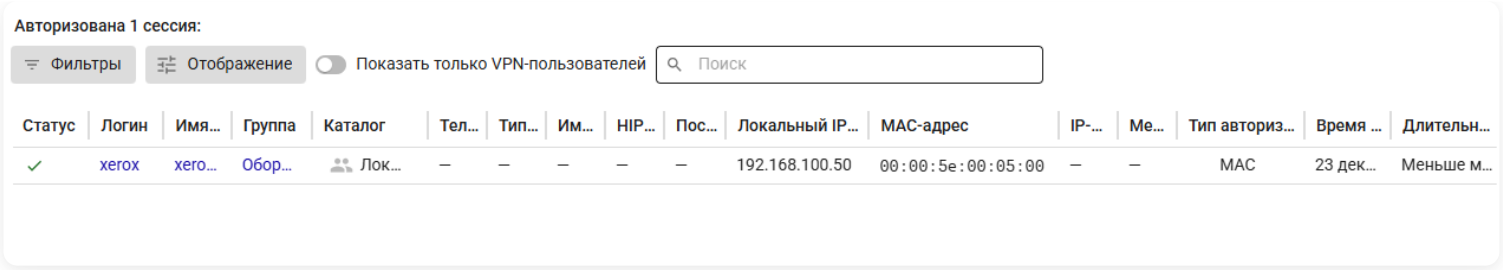
Чтобы авторизовать сетевой принтер, необходимо создать пользователя на NGFW Novum вручную или через Обнаружение устройств:



На вкладке **Пользователи** → **Авторизация** → **IP и MAC** для сетевого принтера необходимо создать правило **Пользователь <--> MAC-адрес**:



При обнаружении активности от сетевого принтера или другого устройства сессия пользователя появится в **Мониторинг** → **Сессии пользователей**:



Опция **Рандомизация MAC-адреса** будет мешать при авторизации мобильного устройства по MAC-адресу. Рекомендуется отключить эту опцию либо использовать другие типы авторизации (например, веб-аутентификацию).

По подсетям

Классический контекст | Высокопроизводительный контекст

Чтобы не регистрировать каждое устройство как отдельного пользователя Ideco NGFW Novum и не задавать для него факторы авторизации, создайте правило в **Пользователи** → **Авторизация** → **По подсетям**. Правила полезны, когда требуется автоматически авторизовать большое количество устройств.

Любой трафик при авторизации по подсетям учитывается как трафик от одного указанного пользователя в указанной подсети. Не допускайте пересечения сетей.

Особенности использования авторизации по подсетям

В правилах **IP и MAC** или **По подсетям** нельзя указывать пользователей RADIUS и DeviceVPN.

Любое **пересечение сетей** при авторизации может привести к проблемам. Например:

- На вкладке **По подсетям** для разных пользователей созданы правила с пересекающимися сетями.
- В **Пользователи** → **Учетные записи** создан пользователь с IP-адресом из подсети в правилах авторизации **По подсетям**.
- В **VPN-подключения** → **Выдача IP-адресов** добавлена привязка к IP-адресам из подсети в правилах авторизации **По подсетям**.
- На вкладке **По подсетям** создано правило с подсетью, частично пересекающейся с диапазоном IP-адресов для выдачи в **Сервисы** → **DHCP**.

Работа DHCP возможна в случае, если диапазон выдачи IP-адресов не превышает количество адресов в подсети, указанной в правиле авторизации **По подсетям**.

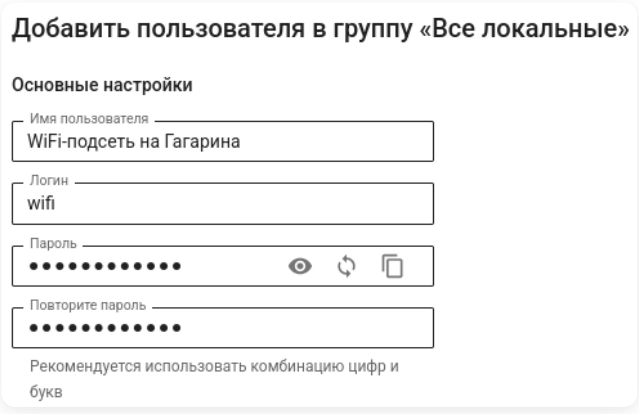
Пример использования

Есть Wi-Fi-подсеть 192.168.10.0/24, для устройств которой требуется авторизация.

Для создания правила авторизации выполните действия:

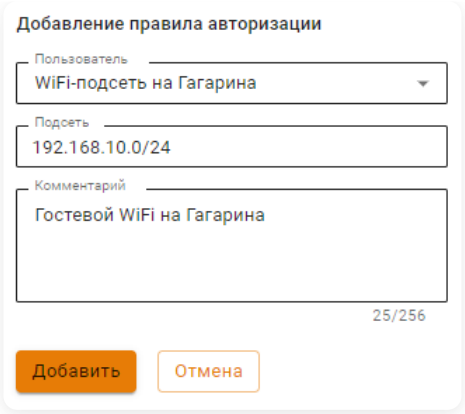
1. Перейдите в **Пользователи** → **Учетные записи** и нажмите .

2. Заполните поля и нажмите **Добавить**:



3. Перейдите в **Пользователи** → **Авторизация** → **По подсетям** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:



- **Пользователь** - выберите созданного в пункте 2 пользователя.
- **Подсеть** - введите IP и маску подсети.
- **Комментарий** - необязательное поле.

При включении или отключении правил авторизации **По подсетям** может наблюдаться задержка в работе Ideco NGFW Novum.

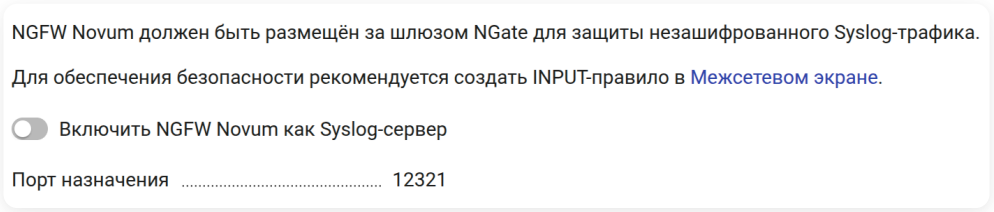
Syslog-сервер

Классический контекст | Высокопроизводительный контекст

На вкладке можно настроить NGFW Novum в роли Syslog-сервера для авторизации пользователей, подключающихся к КриптоПро NGate. NGFW Novum будет принимать Syslog-сообщения, фильтровать их по содержанию и открывать сессии для пользователей NGFW Novum.

На текущий момент интеграция поддерживается только с КриптоПро NGate. В дальнейшем список поддерживаемых вендоров может быть расширен.

Опция **Включить NGFW Novum как Syslog-сервер** позволяет включить или отключить работу NGFW Novum в роли Syslog-сервера:



- **Порт назначения** - порт приема Syslog-сообщений. По умолчанию `12321`.

IP-адрес получателя - по умолчанию `0.0.0.0`. Изменение IP-адреса и порта в интерфейсе не предусмотрено.

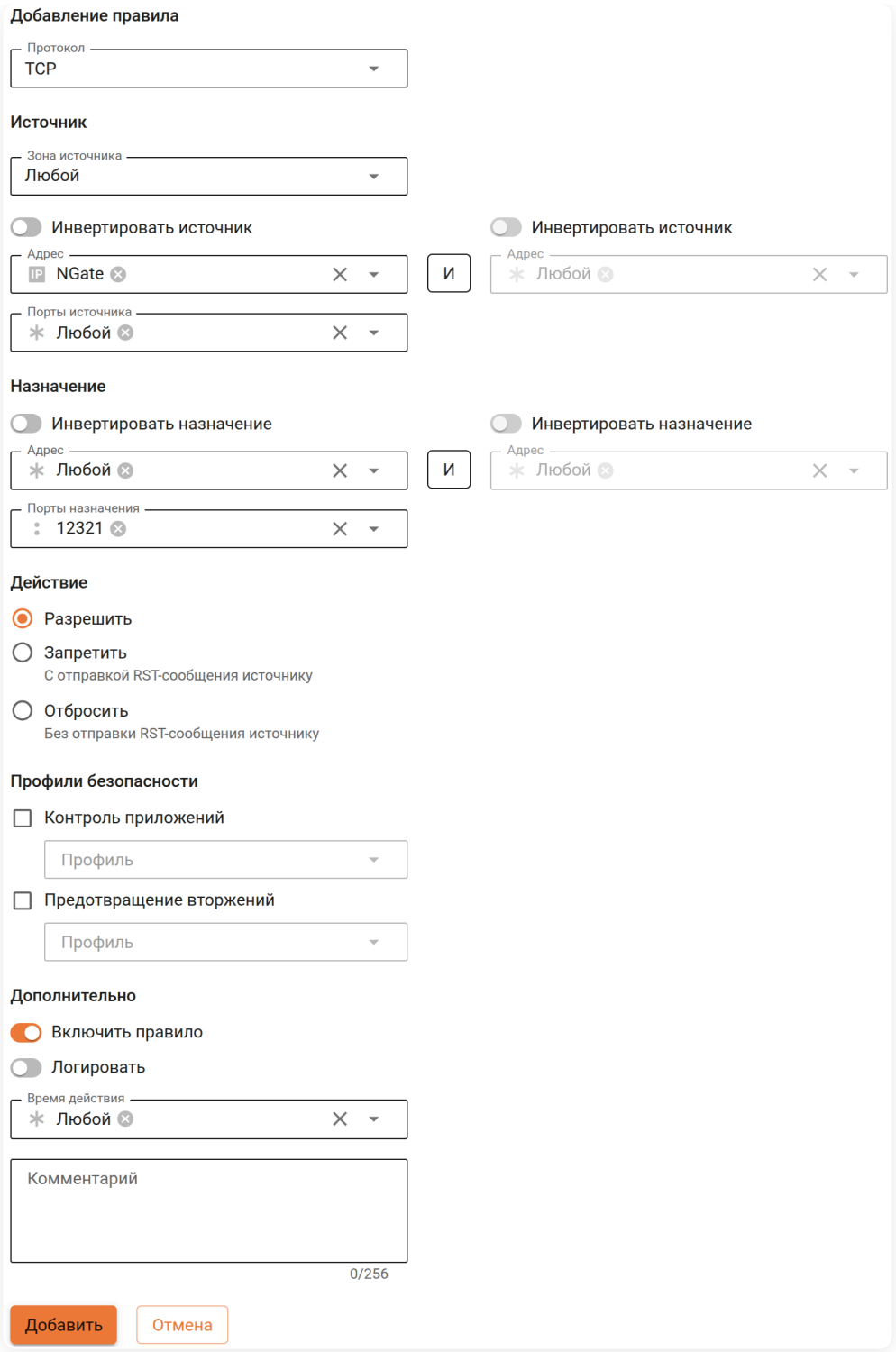
Изменения IP-адреса или порта доступно через API.

Интеграция с NGate открывает незащищенный канал передачи сообщений. Рекомендуем:

1. Разместить NGFW Novum внутри периметра за шлюзом NGate, чтобы предотвратить несанкционированную отправку Syslog-сообщений.

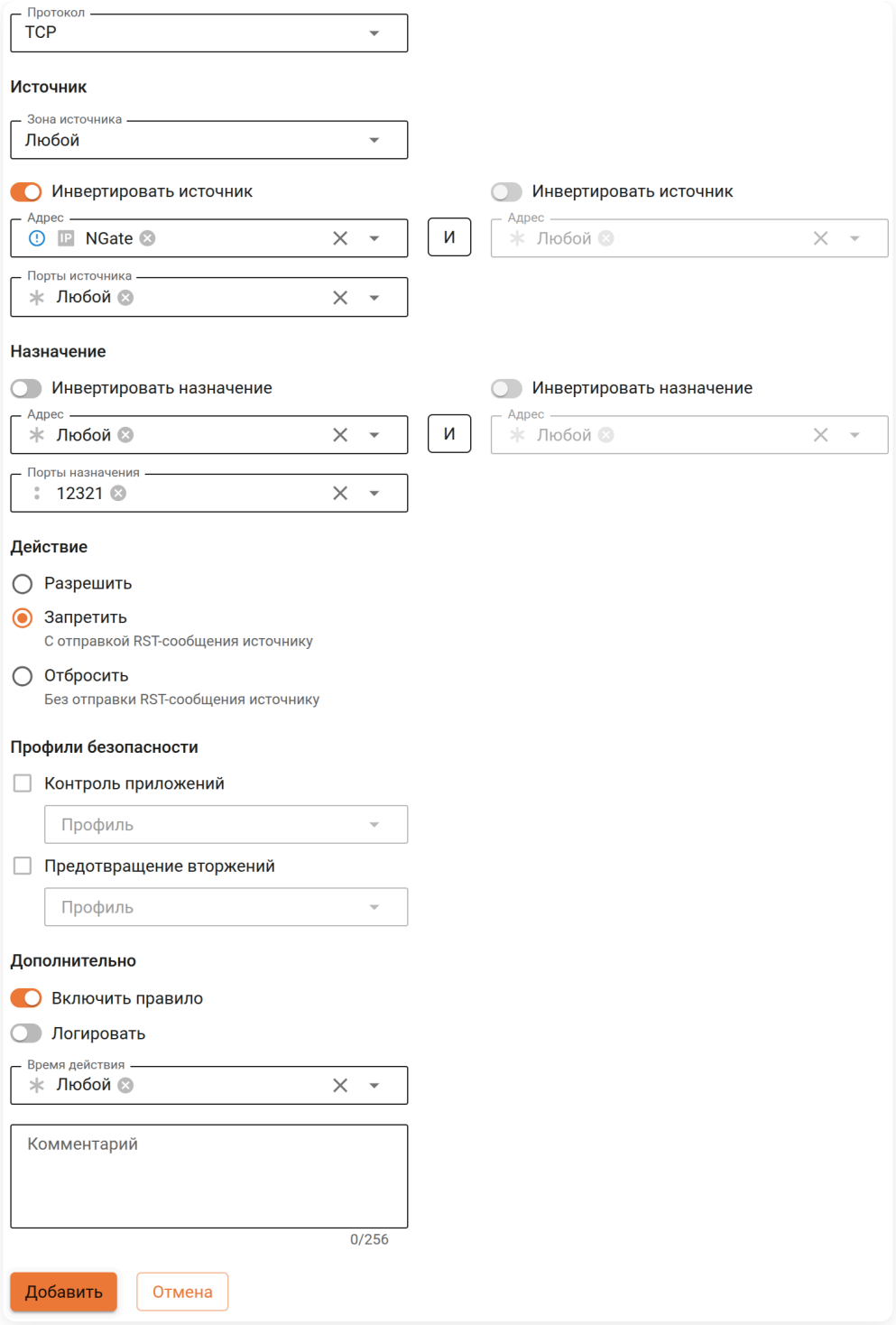
2. Ограничить все запросы на порт `12321` только доверенными источниками. Для этого создайте правило в **Правила трафика** → **Межсетевой экран** → **INPUT** с учетом наличия **запрещающего все** правила:

Запрещающее все правило есть



- **Протокол** - TCP.
- **Источник** - IP-адрес NGate или зона, в которую он входит.
- **Порты назначения** - `12321`.
- **Действие** - Разрешить.

Запрещающее все правило отсутствует



- **Протокол** - TCP.
- **Инвертировать источник** - включите опцию.
- **Источник** - IP-адрес NGate или зона, в которую он входит.
- **Порты назначения** - `12321`.
- **Действие** - Запретить.

Для использования локальной группы пользователей NGFW Novum без интеграции с Active Directory (AD) NGate должен использовать один из способов:

- Подключение к LDAP или RADIUS.
- Аутентификация по сертификатам с именами пользователей.

Подробнее о создании в NGate правил доступа к ресурсам в статье.

Если NGate и NGFW Novum интегрированы с Active Directory, то в **Пользователи** → **Аутентификация** → **Основное** выберите каталог авторизации AD как **Каталог по умолчанию**.

Настройка на NGate

1. Добавьте NGFW Novum в качестве Syslog-сервера на стороне NGate, следуя инструкции:

- NGFW Novum должен быть добавлен отдельным Syslog-сервером, так как NGate поддерживает одновременную отправку логов на несколько Syslog-серверов.
- В настройках Syslog-сервера необходимо выбрать протокол **TCP** и указать порт назначения `12321`.

2. Настройте отправку логов согласно инструкции.

> В конфигурации кластера NGate уровень логирования должен быть установлен не ниже `LOG_INFO`, иначе часть событий не будет передаваться на внешний Syslog-сервер.

VPN-подключения

Классический контекст | Высокопроизводительный контекст | API

С версии 22.0 поддержка протокола PPTP для доступа по VPN отключена, так как протокол устарел.
Рекомендуем использовать Ideco Client, IKEv2/IPsec или SSTP.

Название служб раздела **VPN-подключения**: `ideco-vpn-servers-backend`, `ideco-vpn-authd`, `ideco-vpn-dhcp-backend`, `ideco-vpn-netns`, `ideco-vpn-sessions-sync`.

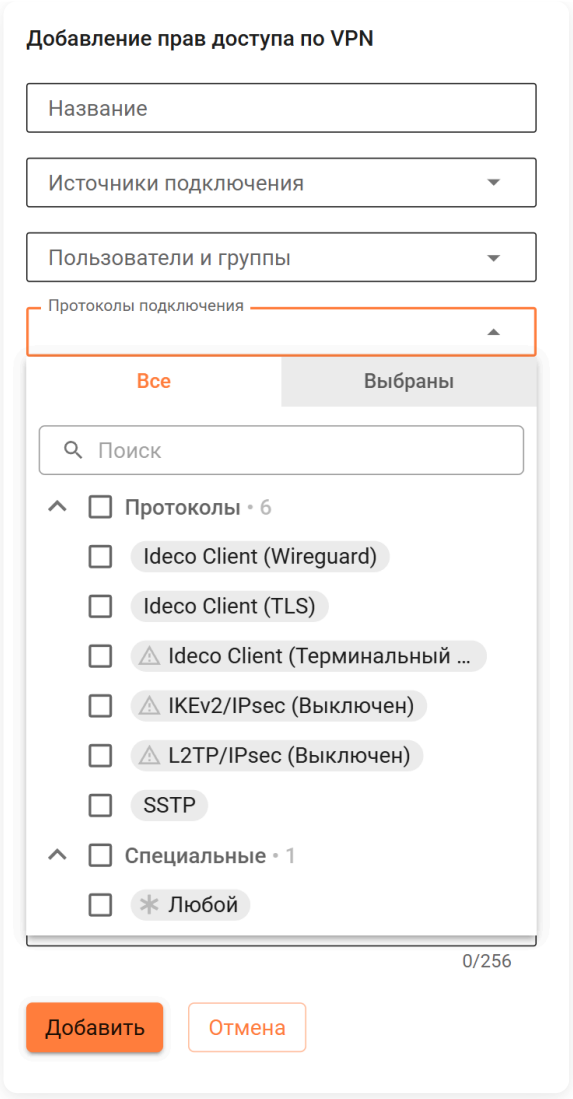
Список служб для других разделов доступен по ссылке.

Для настройки VPN-подключения к Ideco NGFW Novum можно использовать VPN-клиент, который уже есть в операционной системе, или установить отдельный. Как настроить подключение в разных ОС, описано в Инструкции по созданию VPN-подключений.

Настройка VPN-сервера Ideco NGFW Novum происходит в несколько этапов:

- Настройка протоколов, маршрутов и адресации.
- Настройка политик доступа из внешних сетей.
- Настройка двухфакторной аутентификации (опционально).

Поддерживаемые протоколы:



- **WireGuard** - используется Ideco Client с применением шифрования.
- **TLS** (Transport Layer Security) - используется Ideco Client при подключении через TCP.
- **Терминальный сервер** - WireGuard для терминального сервера. Используется Ideco Client с применением шифрования.
- **IKEv2** - рекомендуемый протокол с точки зрения скорости и безопасности.
- **SSTP** - подходит для использования в средах с ограничениями на порты.
- **L2TP/IPsec** - обеспечивает баланс между безопасностью и совместимостью.
- **Любой** - отмечаются все протоколы. Такое соединение может использовать любой из перечисленных протоколов.

Настройка VPN-подключения

Чтобы VPN-подключение работало на устройствах пользователей, необходимо загрузить **корневой сертификат**:

- Корневые сертификаты Ideco NGFW Novum действительны в течение 10 лет.
- Если используется сертификат Let's Encrypt, обновление будет происходить автоматически.

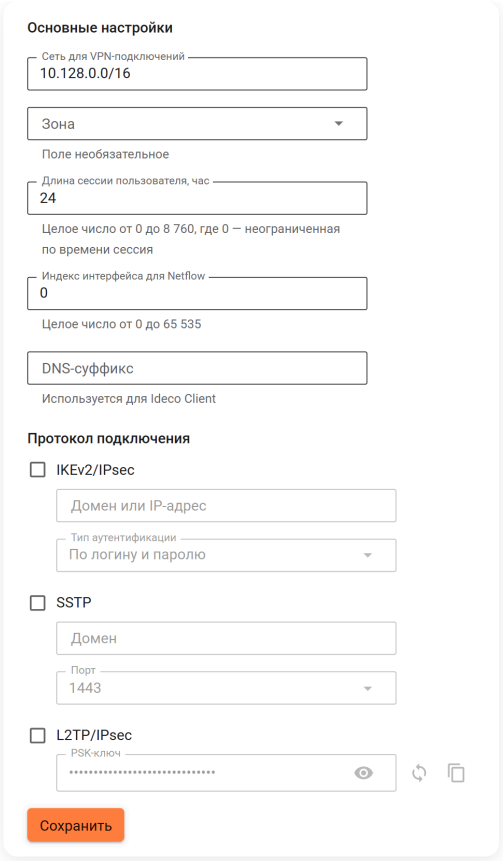
Чтобы пользователь, подключенный к NGFW из локальной сети по VPN или через Ideco Client в режиме VPN, мог выйти в интернет, нужно выполнить одно из следующих действий:

- Настройте вторую сессию авторизации пользователя. Например, через Веб-авторизацию.
- В разделе **Передача маршрутов** для нужных пользователей выберите опцию **Отправлять весь трафик на Ideco NGFW Novum**.

Для настройки VPN-подключения перейдите в **Пользователи** → **VPN-подключения** и создайте правило.

Основное

На вкладке **Основное** настраиваются протоколы и адресация VPN-подключений. Для настройки заполните поля:



Расшифровка полей

- **Сеть для VPN-подключений** - укажите подсеть для динамического назначения IP-адресов. Маска подсети должна быть в диапазоне от 16 до 30 бит.
- **Зона** - добавьте настройку, если необходимо объединить сетевые интерфейсы. Все сетевые интерфейсы, которые создаются при подключении VPN-клиентов, будут автоматически попадать в указанную зону. Трафик пользователей будет обрабатываться по правилам, заданным для этой зоны.

Если требуется настроить VPN-подключение к Loopback-интерфейсу, оставьте поле **Зона** пустым.

- **Длина сессии пользователя, час** - укажите продолжительность сессии пользователя (целое число от 1 до 24). По истечении указанного периода сессия разрывается и требуется переподключение. Настройка распространяется на подключения по протоколам L2TP, SSTP, IKEv2, а также на сессии Ideco Client.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **DNS-суффикс** - укажите DNS-суффикс, если для подключения по VPN используется Ideco Client.
- **Протокол подключения** - выберите, какой протокол будет использоваться.

Для каждого протокола VPN-подключения отображается статус использования. Статусы отображаются в виде подсказок под названиями протоколов:

Зеленый статус: протокол включен и используется.

Оранжевый статус: протокол отключен, но используется в правилах доступа по VPN.

Как увеличить продолжительность сессии пользователя с помощью запроса к API

```
PATCH https://:8443/vpn_servers/settings
```

Json-тело запроса:

```
{
"expired_after_seconds": "integer"
}
```

`expired_after_seconds` - количество секунд от 1 до 31536000, после которого VPN-сессия считается просроченной.

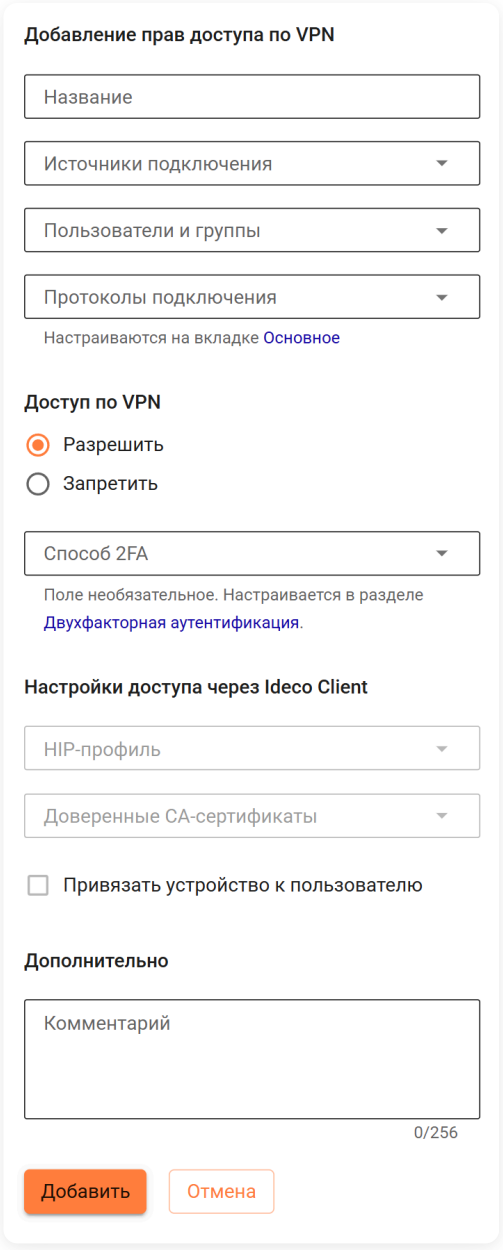
Ответ на успешный запрос: 200 OK

Доступ по VPN

На вкладке **Доступ по VPN** для пользователей и групп на внешние интерфейсы NGFW Novum настраиваются правила доступа. NGFW Novum проверяет таблицу правил сверху вниз до первого совпадения пользователя. При совпадении условий (**Источники подключения**, **Пользователи и группы**, **Протоколы подключения**) выполняется действие, выбранное при создании правил.

В правилах можно использовать как группы пользователей Ideco NGFW Novum, так и группы безопасности AD. Введите Ideco NGFW Novum в домен и при создании правила **Доступ по VPN** в поле **Пользователи и группы** выберите необходимую группу безопасности.

Для настройки правил доступа нажмите **Добавить**:



Расшифровка полей

- **Название** - укажите название правила.
- **Источники подключения** - выберите, откуда будет производиться подключение по VPN (IP-адреса, подсети, страны и континенты).
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.

Для пользователей Device VPN доступно подключение только по протоколам **Ideco Client (Терминальный сервер)**, **Ideco Client (Wireguard)**, и **Ideco Client (TLS)**.

Если в поле **Протоколы подключения** выбраны **Ideco Client (Wireguard)** и **Ideco Client (TLS)** или **Любой**, пользователи будут подключаться по протоколу **Ideco Client (Wireguard)**.

- **Протоколы подключения** - выберите протокол (настраивается на вкладке **Основное**).
- **Доступ по VPN** - разрешите или запретите доступ по созданному правилу.
- **Способ 2FA** - выберите способ двухфакторной аутентификации.

2FA не поддерживается для учетных записей Device VPN.

- **HIP-профиль** - выберите HIP-профиль, если для подключения по VPN используется Ideco Client.
- **Настройки доступа через Ideco Client:**
  - **Доверенные CA-сертификаты** - выберите один или несколько сертификатов CA, которым доверяет Ideco NGFW Novum при проверке сертификата устройства. Загружаются в **Сервисы** → **Сертификаты**. Если поле не заполнено, проверка сертификата устройства не выполняется. Подробнее о выпуске сертификата устройства в статье.
  - **Привязать устройство к пользователю** - если опция включена, при первом подключении пользователя через Ideco Client устройство привязывается к учетной записи. Последующие подключения разрешаются только с привязанного устройства.

Привязка устройств не осуществляется для пользователей **Ideco Device VPN**.

- **Комментарий** - добавьте комментарий (опционально).

Если авторизация Device VPN не требуется, исключите группу **Ideco Device VPN** из разрешающих правил или создайте для нее запрещающее правило.

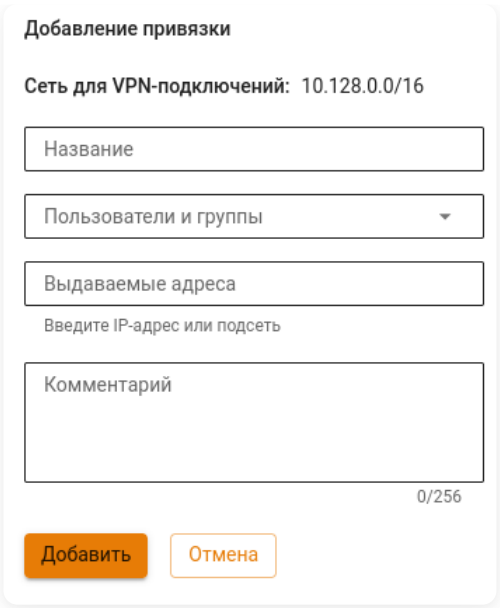
Выдача IP-адресов

На вкладке **Выдача IP-адресов** можно создать правила для выдачи IP-адресов пользователям, подключающимся по VPN.

NGFW Novum проверяет таблицу правил сверху вниз до первого совпадения пользователя. Если пользователь не попал под условия правил, IP-адрес назначается автоматически из пула адресов VPN, настраиваемого в разделе **Пользователи** → **VPN-подключения** (например, 10.128.0.0/16). Из пула исключаются все подсети и одиночные адреса, указанные во всех правилах таблицы выдачи IP-адресов и используемые в текущих сессиях. Если адресов не осталось, соединение разрывается.

- Подсеть, указанная в правиле, должна полностью входить в сеть для VPN-подключений. В противном случае правило считается невалидным, адрес выдать невозможно, соединение разрывается.
- В двух разных правилах нельзя указать одну и ту же сеть.
- Если в разных правилах указаны пересекающиеся сети (например, сеть `10.128.1.0/24` является подсетью сети `10.128.0.0/20`), то:
  - Адреса из сети `10.128.1.0/24` никогда не будут выдаваться.
  - При выдаче адресов сети `10.128.0.0/20` из нее будут исключаться адреса подсети `10.128.1.0/24`.
- Если указать в правилах сеть, совпадающую с сетью для VPN-подключений, то все пользователи VPN, для которых не совпадет ни одно правило таблицы, не смогут получить адрес и подключиться.
- Количество одновременных VPN-подключений от одного пользователя в том числе будет ограничиваться размером сети, указанной для него в правилах.
- Если в правиле указан один IP-адрес, который уже используется в текущей сессии, то указанный в правиле пользователь не сможет установить второе VPN-подключение и не сможет получить адрес.
- Если в правиле указана сеть с префиксом /30 (или маской 255.255.255.252) и более широкие сети (например, `10.128.2.0/24`), то при выдаче адреса из таких сетей адрес самой сети и широковещательный адрес (`10.128.2.0` и `10.128.2.255`) использоваться не будут.

Для создания правила нажмите **Добавить**:



Расшифровка полей

- **Название** - укажите название правила.
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Выдаваемые адреса** - укажите IP-адрес или подсеть, IP-адреса которой будут выдаваться пользователям.
- **Комментарий** - укажите комментарий к правилу (опционально).

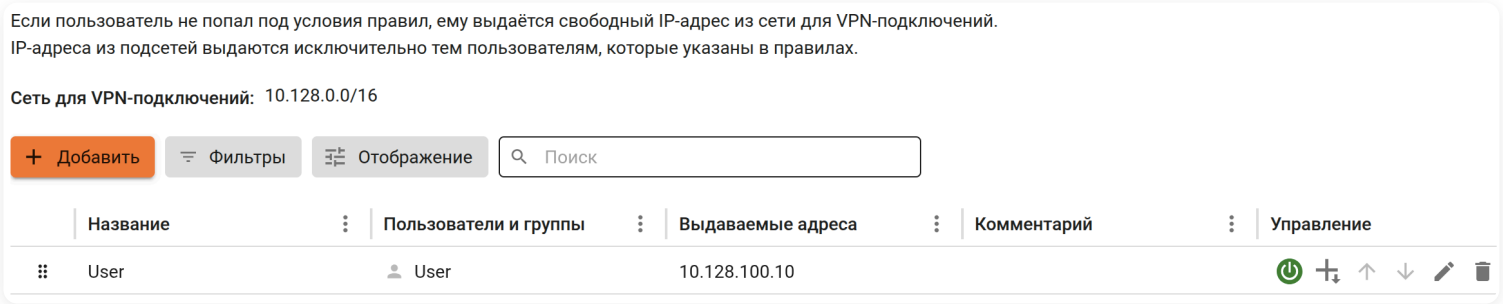
При наличии большого количества правил выдачи IP-адресов в таблице воспользуйтесь кнопкой **Фильтры**.

Чтобы отключить правило, нажмите на в столбце управления. Чтобы удалить правило, нажмите .

Статическая привязка IP-адресов

IP-адрес назначается пользователю автоматически из пула адресов для VPN, настраиваемого в разделе **Пользователи → VPN-подключения** (например, 10.128.0.0/16).

Чтобы настроить **статическую** привязку адресов, выдаваемых определенным пользователям, нужно перейти в **Пользователи → VPN-подключения → Выдача IP-адресов**, нажать **Добавить** и указать нужного пользователя и IP-адрес. Пример настройки фиксированного IP-адреса VPN представлен ниже:



Передача маршрутов

На вкладке **Передача маршрутов** можно настроить правила передачи маршрутов клиентам. Маршруты передаются клиенту в момент установления VPN-подключения. Изменения маршрутов (например, добавление статических маршрутов) после подключения не применяются и становятся доступны пользователю только при повторном подключении к VPN.

Ideco Client поддерживает обновление маршрутов без разрыва соединения.

Маршруты, переданные Ideco NGFW Novum для VPN-клиента, имеют меньшую метрику (т. е. высокий приоритет).

Для настройки правил нажмите **Добавить**:

Расшифровка полей

- **Название** - укажите название правила.
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Отправка маршрутов** - выберите, как будут передаваться маршруты:
  - **Не отправлять** - маршруты не передаются клиенту, трафик не будет проходить через NGFW Novum.
  - **Отправлять весь трафик на Ideco NGFW Novum** - передается маршрут 0.0.0.0/0, весь трафик направляется через NGFW Novum.
  - **Отправлять маршруты до всех сетей, маршрутизируемых через LAN-интерфейсы и IPsec-туннели** - передаются маршруты до всех локальных сетей NGFW Novum, в том числе подключенных через IPsec и маршрутизируемых, кроме маршрутов: **OSPF**, **BGP**, **PBR** и **Маршрутизации внешних сетей**.
  - **Отправлять маршруты до сетей, указанных на LAN-интерфейсах** - передаются маршруты до локальных сетей NGFW Novum, без учета IPsec и маршрутизируемых.
  - **Отправлять только указанные** - выберите сети, до которых будут передаваться маршруты.
- **Исключение адресов из маршрута** - выберите сети, исключенные из маршрута.
- **Комментарий** - укажите комментарий к правилу (опционально).

Если маршруты VPN-клиентов пересекаются с маршрутами, передаваемыми Ideco NGFW Novum, то выберите **Не отправлять** или **Отправлять только указанные**.

Если при подключении по VPN (IKEv2, L2TP, SSTP) не удается получить маршруты до сетей Ideco NGFW Novum, указанное число маршрутов не вмещается в опции DHCP-пакета.

При исключении подсети, IP-адреса, домена из передаваемого маршрута может возникнуть разбиение на несколько маршрутов. Это может привести к тому, что все маршруты не вместятся в опции DHCP-пакета.

Если количество байт в опции маршрутов превышает 255, то маршруты не передаются службой **ideco-vpn-dhcp-backend**.

Если пакет DHCP превышает 576 байт, то пакет может быть проигнорирован клиентом DHCP и применение маршрутов не произойдет (зависит от реализации клиента).

Перемещение правил

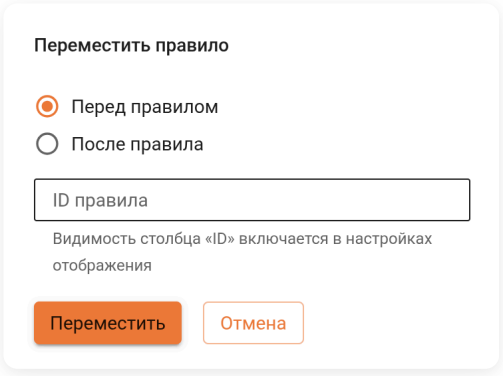
На вкладках **Доступ по VPN**, **Выдача IP-адресов** и **Передача маршрутов** предусмотрено перемещение правил.

Выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Полезные ссылки

- **Инструкции по созданию VPN-подключений**

- **Двухфакторная аутентификация**
- **Сервисы**
- **Создание подключения в Astra Linux**
- **Создание VPN-подключения в Fedora**
- **Создание подключения в Windows**
- **Создание подключения в Mac OS**
- **Как избежать проблем с подключением VPN-клиентов при нескольких серверах**
- **Создание VPN-подключения в Alt Linux**
- **Создание VPN-подключения в Ubuntu**
- **Создание VPN-подключения на мобильных устройствах**

Подключение по IKEv2/IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | VK Видео



IKEv2/IPsec - протокол, который используется для создания защищенного соединения между двумя устройствами в сети.

Рекомендуем использовать IKEv2/IPsec для обеспечения максимальной скорости и безопасности.

Протокол использует корневой сертификат для проверки подлинности участников соединения. Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство пользователя не требуется.

Для аутентификации применяется связка логин и пароль пользователя Ideco NGFW Novum или пользователя из Active Directory.

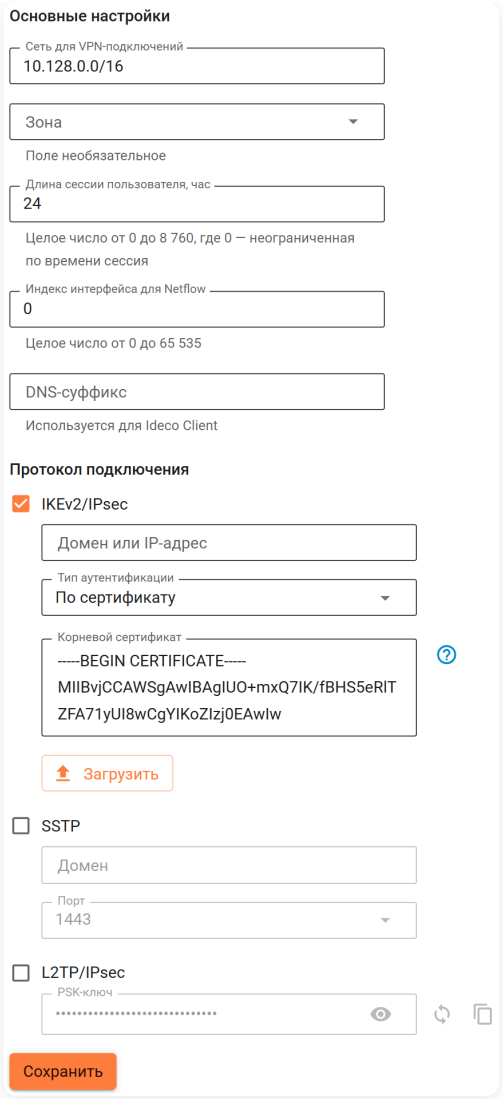
Не применяйте Wildcard-сертификаты для IKEv2/IPsec. Эти сертификаты не поддерживаются IPsec-клиентами из-за ограничений в проверке доменных имен.

Настройка Ideco NGFW Novum

Не рекомендуем использовать для VPN-подключений кириллические логины и пароли, а так же указывать в качестве логина IP-адрес.

Основные настройки

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**, включите опцию **IKEv2/IPsec** и заполните поля:

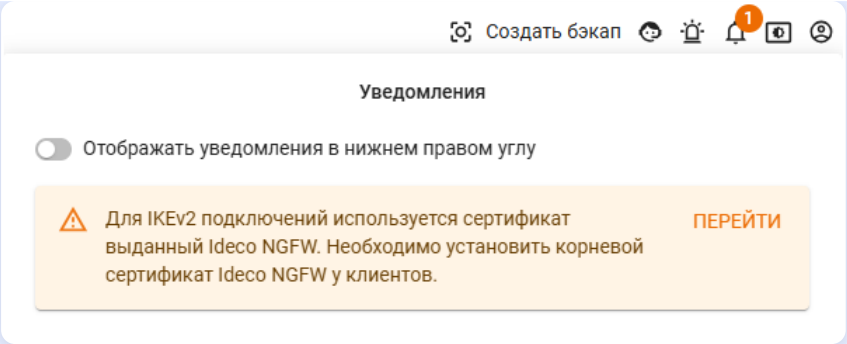


- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

2. Нажмите **Сохранить**.

- Если используется сертификат Let's Encrypt, то дополнительных действий не требуется.
- Если сертификат для VPN-подключений издан NGFW, появится уведомление о необходимости установить корневой сертификат Ideco NGFW Novum у клиентов:



- Если используете сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле **Subject Alternative Name (SAN)**. Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Передача клиентам маршрутов до ваших локальных сетей происходит автоматически. Для управления доступом к сетям используйте Межсетевой экран.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее - в статье VPN-подключения.

Поддержка клиентов IKEv2/IPsec в ОС

- Microsoft **Windows 10** и выше. Требует установки корневого сертификата Let's Encrypt. Инструкция по настройке.
- Apple **MacOS X 10.11** "El Capitan" (2015 г.) и выше. Инструкции по настройке.
- Linux NetworkManager plugin (с 2008 г.). Инструкция по настройке Alt Linux.
- Google **Android 11** (2020 г.) и выше. На более ранних версиях можно использовать приложение StrongSwan. Инструкция по настройке.
- Apple **iOS 9** (iPhone 4S, 2015 г.) и выше. Инструкция по настройке.

Полезные ссылки

- **Создание VPN-подключения в Fedora**
- **Создание подключения в Windows**
- **Создание VPN-подключения на мобильных устройствах**

Подключение по SSTP

Классический контекст | Высокопроизводительный контекст

По возможности не используйте подключение по SSTP. Подключение по SSTP лучше других проходит через NAT, но при нестабильном качестве связи работает значительно хуже, чем другие VPN (особенно при передаче звука/видео), так как инкапсулирует все данные внутри TCP. Рекомендуется использовать IKEv2/IPsec.

SSTP - протокол туннелирования трафика, который обеспечивает безопасное соединение между клиентом и сервером через интернет.

Протокол использует корневой сертификат для проверки подлинности участников соединения. Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство пользователя не требуется.

Для аутентификации применяется связка логин/пароль пользователя Ideco NGFW Novum или пользователя из Active Directory.

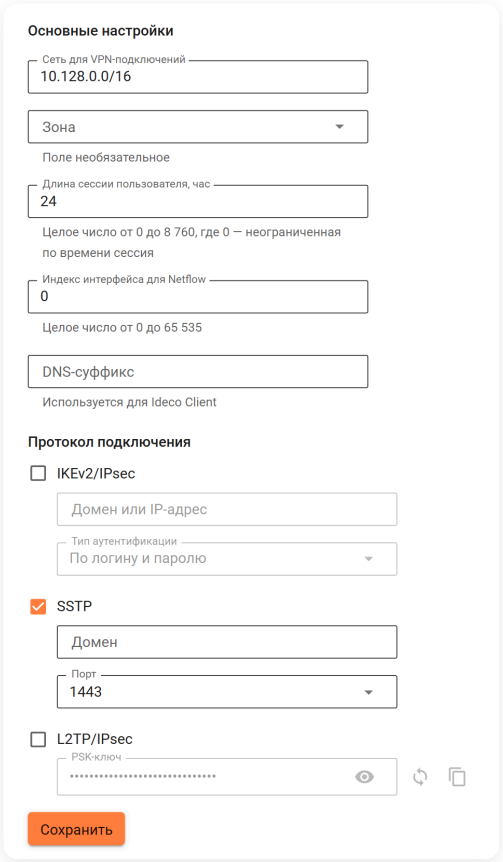
Особенности работы:

- Запрещено использовать домен `.local`. Подключение по SSTP поддерживается только из внешних сетей.
- Не рекомендуется использовать логины на кириллице для VPN-подключений. Это может привести к проблемам с подключением.
- NGFW Novum не поддерживает подключение MikroTik по SSTP, так как MikroTik использует устаревший и небезопасный алгоритм SHA-1.

Настройка Ideco NGFW Novum

Основные настройки

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное** и включите опцию **Подключение SSTP**:



- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

- **Домен** - укажите DNS-имя. IP-адрес внешнего интерфейса Ideco NGFW Novum должен резолвиться в одно из имен вашей внешней доменной зоны. Используйте реальное имя с правильной A-записью, т.к. реальное имя необходимо для выписки сертификата Let's Encrypt.
- **Порт** - выберите предлагаемый порт из вариантов: 1443, 2443, 3443, 4443.

2. Нажмите **Сохранить**.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключения.

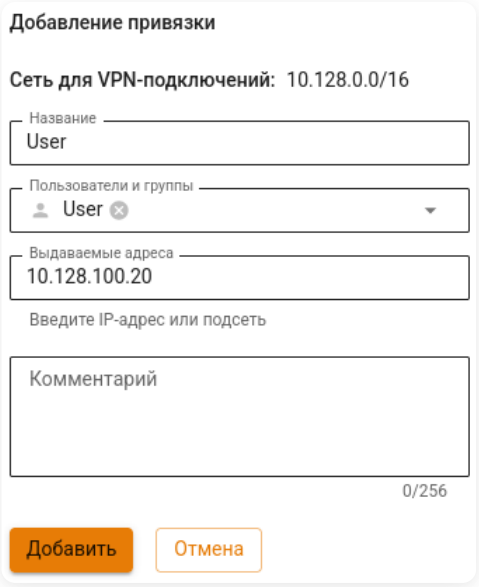
Правила выдачи IP-адресов

IP-адрес пользователю назначается автоматически из пула адресов для VPN, настраиваемого в разделе **Пользователи** → **VPN-подключения** (например, из подсети 10.128.0.0/16).

Настройте **статическую** привязку адресов, выдаваемых по VPN определенным пользователям:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Выдача IP-адресов**.

2. Нажмите **Добавить** и укажите название сети, нужного пользователя и IP-адрес:



3. Нажмите **Добавить** для сохранения изменений.

Правила передачи маршрутов

Выберите режим передачи маршрутов клиентам при добавлении правила в **Пользователи** → **VPN-подключения** → **Передача маршрутов**. Подробнее в статье VPN-подключение.

Полезные ссылки

- В случае, если установлено VPN-соединение, но не удается получить доступ к ресурсам локальной сети, рекомендуется обратиться к статье Особенности маршрутизации и организации доступа.
- Инструкции по настройке VPN-подключений на разных ОС доступны по ссылке.
- **Создание подключения в Windows**
- **Подключение по SSTP Wi-Fi роутеров Keenetic**

Подключение по L2TP/IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Видеоинструкцию смотрите по ссылке:

- Youtube
- docs.ideco.ru

По возможности не используйте L2TP/IPsec-подключение, которое может работать нестабильно, обладает огромной избыточностью, низкой производительностью и поддерживает не самое сильное шифрование. Вместо этого рекомендуется IKEv2/IPsec. Все современные ОС поддерживают IKEv2, либо для них есть приложения.

L2TP/IPsec - протокол позволяет создавать защищенные VPN-соединения между устройствами, обеспечивая конфиденциальность и целостность передаваемых данных.

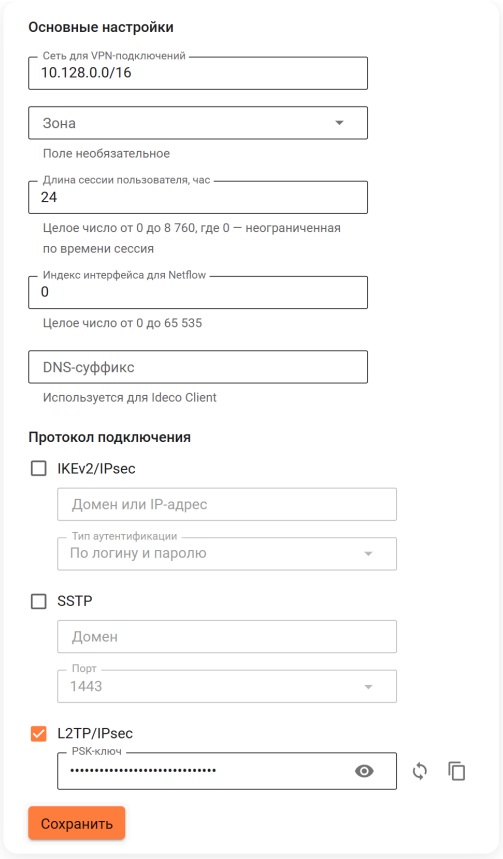
Для аутентификации используется связка логин/пароль пользователя Ideco NGFW Novum или пользователя из Active Directory, а также PSK-ключ, который был указан при настройке соединения.

Не рекомендуем использовать для VPN-подключений кириллические логины. А так же указывать в качестве логина IP-адрес.

Настройка Ideco NGFW Novum

Основные настройки

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное** и включите опцию **Подключение по L2TP/IPsec**:



- **Индекс интерфейса для Netflow** - введите целое число от 0 до 65535 для идентификации интерфейса, если используете Netflow.
- **PSK** - укажите секретную фразу (PSK-ключ).

2. Нажмите **Сохранить**.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключения.

Полезные ссылки

- L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если клиентов больше одного. Решить проблему может помочь инструкция.
- В случае, если установлено VPN-соединение, но не удается получить доступ к ресурсам локальной сети, рекомендуется обратиться к статье Особенности маршрутизации и организации доступа.
- Инструкции по настройке VPN-подключений на разных ОС доступны по ссылке.

Особенности маршрутизации и организации доступа

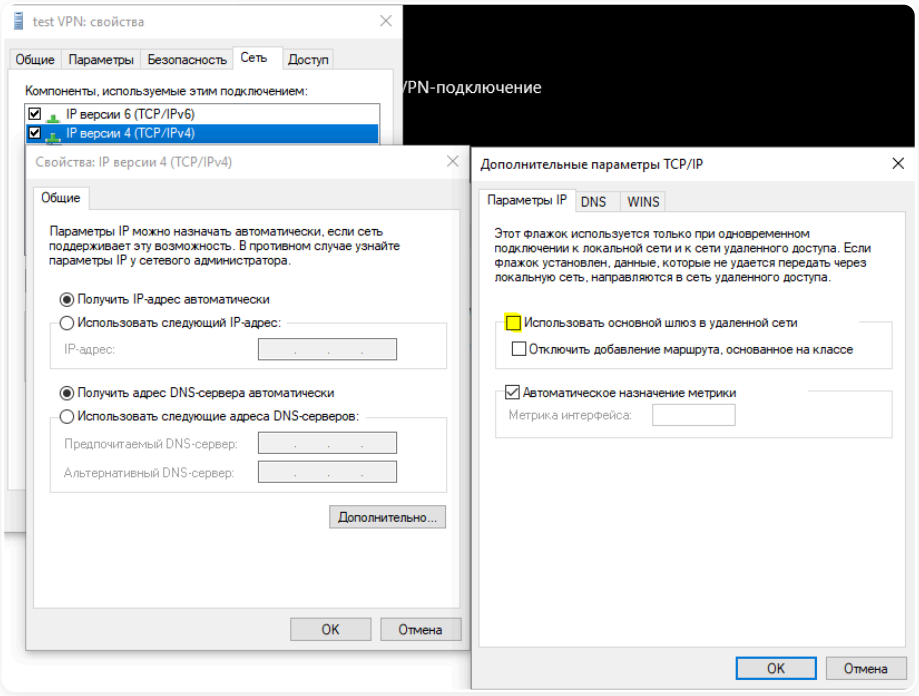
Классический контекст | Высокопроизводительный контекст

В статье рассматриваются потенциальные проблемы, связанные с доступом к ресурсам локальной сети через VPN, и предлагаются решения, такие как настройка маршрутов, исключение определенных сетей в антивирусном ПО и создание правил SNAT на NGFW Novum.

Организация доступа по VPN только к ресурсам локальной сети

Для организации доступа выполните действия:

1. В **Сеть** → **IP версии 4** → **Дополнительно** → **Параметры IP** уберите флаг **Использовать основной шлюз в удаленной сети**:



Особенности VPN-соединения с доступом только к ресурсам локальной сети

При выборе типа передачи маршрутов **Отправлять только указанные сети** маршрут до VPN-сервера и DNS-сервера построен не будет.

Если в NGFW Novum добавить передачу IP-адреса VPN-сервера NGFW Novum (DNS), то маршрут восстановится, а домен будет преобразовываться со следующими особенностями:

- Таблица с включенным шлюзом:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.5      5
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255          On-link         127.0.0.1    331
    192.168.100.2  255.255.255.255          On-link        10.200.0.5      5
  192.168.100.130  255.255.255.255          On-link        10.200.0.5      5
    192.168.122.0    255.255.255.0          On-link    192.168.122.10    281
   192.168.122.10  255.255.255.255          On-link    192.168.122.10    281
  192.168.122.255  255.255.255.255          On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0          On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0          On-link    192.168.122.10    281
  255.255.255.255  255.255.255.255          On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255          On-link    192.168.122.10    281
===========================================================================
```

- Таблица с отключенным шлюзом:

- Таблица с отключенным шлюзом и добавленной публикацией IP NGFW Novum:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.4     26
       10.200.0.4  255.255.255.255          On-link        10.200.0.4    281
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
```

Маршрут до сервера (в примере - 10.200.0.1) добавляется, но имеет более низкий приоритет, чем маршрут по-умолчанию. Соответственно запросы обрабатываются с задержкой и не обрабатываются при перехвате маршрутом по-умолчанию.

Рекомендуем вручную указать маршрут до DNS NGFW Novum, либо добавить маршрут в список публикуемых маршрутов на стороне NGFW Novum. Также можно использовать сторонний DNS-сервер.
2. Пропишите маршрут до корпоративной сети. В Windows 8, 8.1, 10 автоматически создается маршрут на основе класса, в зависимости от адреса, полученного по VPN. Для IPsec-IKEv2 можно настроить автоматическое получение маршрута.

Пример маршрута: если корпоративная сеть имеет адрес `172.16.0.0/16`, а сеть для VPN-подключений, настроенная на Ideco NGFW Novum, имеет адрес `10.128.0.0/16`:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1
```

Маршрут может не работать, когда есть пинг до интерфейса `10.128.0.1`, но нет пинга до хостов в локальной сети. В этом случае при создании маршрута нужно указать номер интерфейса VPN-подключения:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn
```

- `nn` - номер интерфейса VPN-подключения, посмотреть который можно при активном VPN-подключении в выводе в консоли команды `route print` раздел "Список интерфейсов".

Не удается получить доступ к компьютерам в локальной сети Ideco NGFW Novum

Для получения доступа к компьютерам в локальной сети Ideco NGFW Novum убедитесь, что:

1. Локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. В противном случае доступ к сети организации будет невозможен (трафик будет идти через физический интерфейс, а не через VPN).

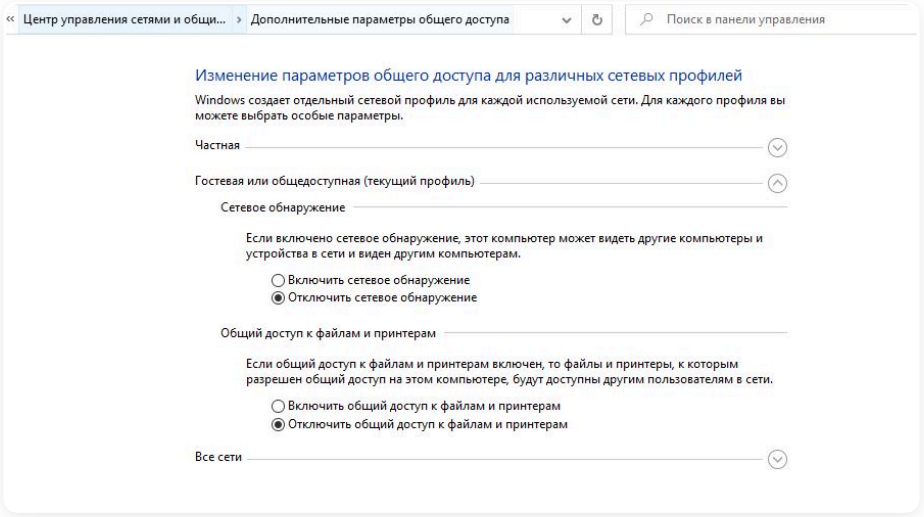
2. На компьютерах локальной сети основным шлюзом должен быть Ideco NGFW Novum. Если это не так, то вручную необходимо прописать соответствующий маршрут, чтобы сетевые пакеты шли на Ideco NGFW Novum для VPN-сети. **Например**:

```
route -p add 10.128.0.0 mask 255.255.0.0 10.1.1.1
```

- `10.128.0.0/16` - адрес VPN-сети Ideco NGFW Novum (настраивается в разделе **Пользователи** → **VPN-подключения**).
- `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW Novum.

3. На Ideco NGFW Novum в разделе **Межсетевой экран** → **FORWARD** нет запрещающих правил.

4. Компьютеры и серверы на Windows не ограничивают доступ к сетевым папкам с помощью правил настроек профилей сети (как на стороне подключающегося по VPN компьютера, так и на стороне компьютеров и серверов локальной сети):



Получение доступа к файлам и принтерам для профиля "Все сети" и "Частные сети"

Для получения доступа выполните действия:

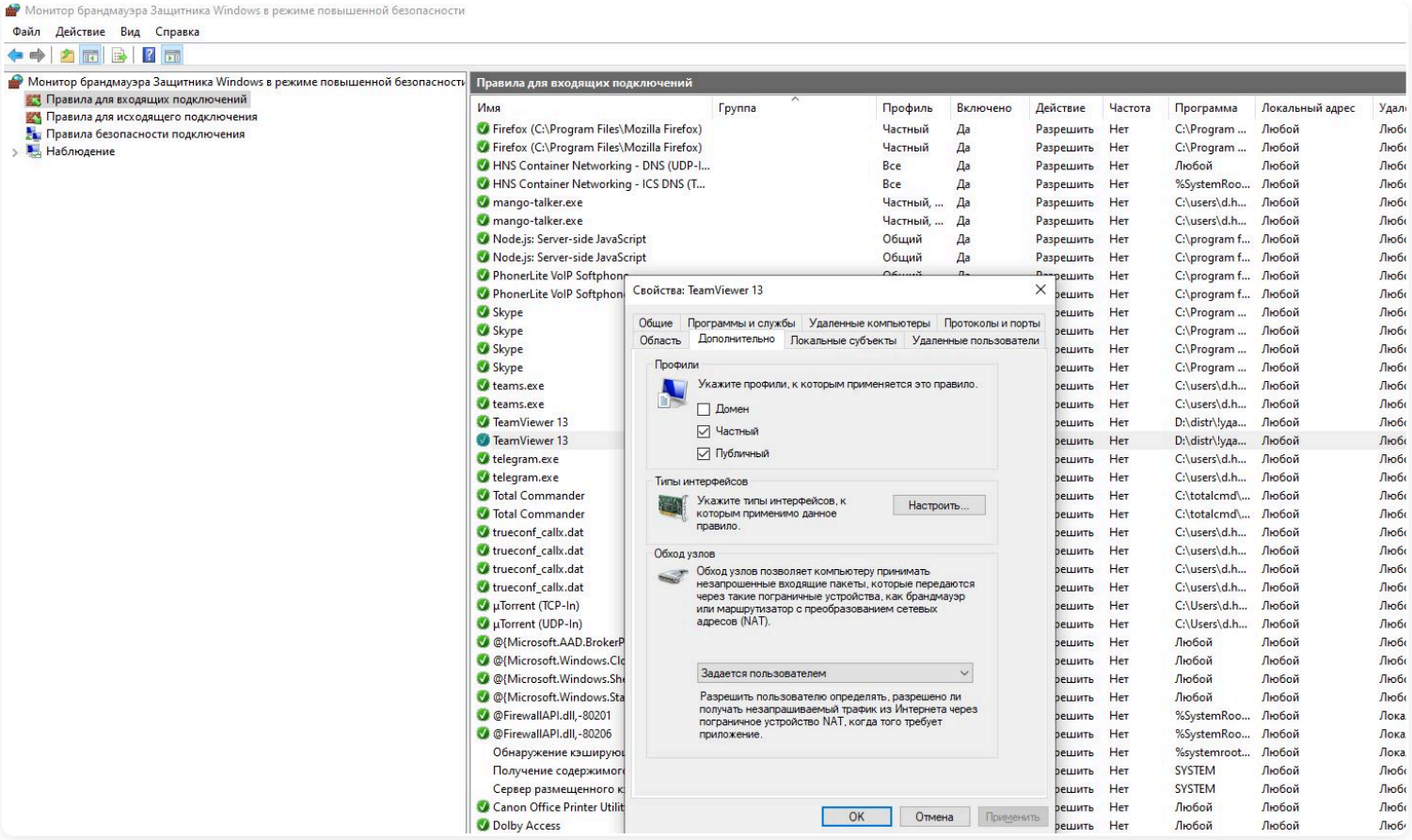
1. Перейдите в PowerShell (запустите PowerShell с повышением прав до администратора).

2. Выполните команду: `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`.

Возможные проблемы:

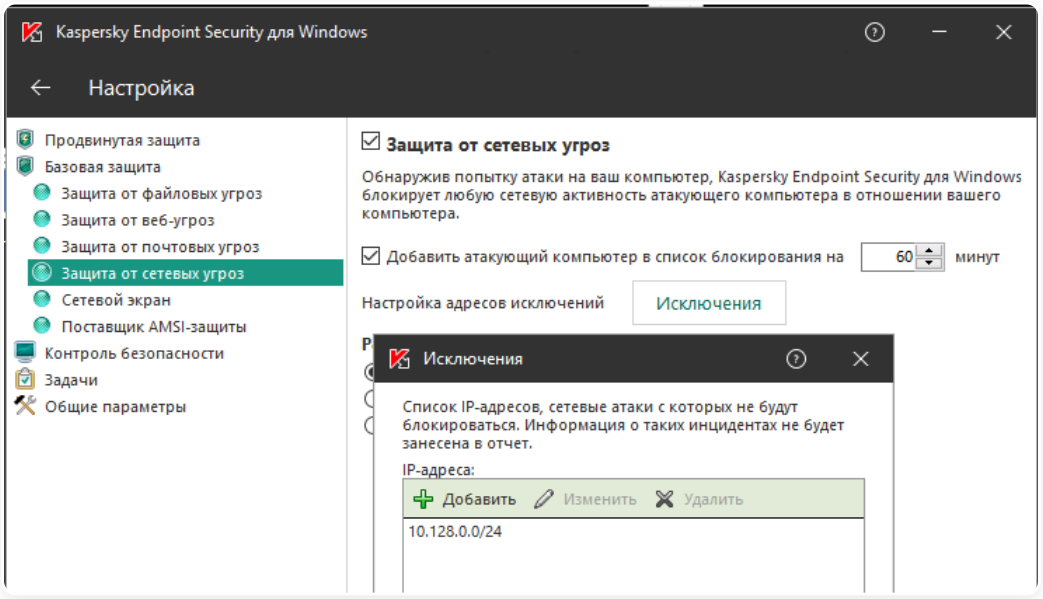
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей.

  Проверьте это в настройках входящих и исходящих подключений (необходимо разрешить доступ из частных и локальных сетей):



- Антивирусное ПО на компьютере может блокировать доступ из нелокальных сетей. Либо блокировать доступ конкретных программ.

  Например, для **Kaspersky Endpoint Security** нужно добавить сеть для VPN-подключений (по умолчанию `10.128.0.0/16`) в исключения:



Получение доступа к локальной сети Филиала

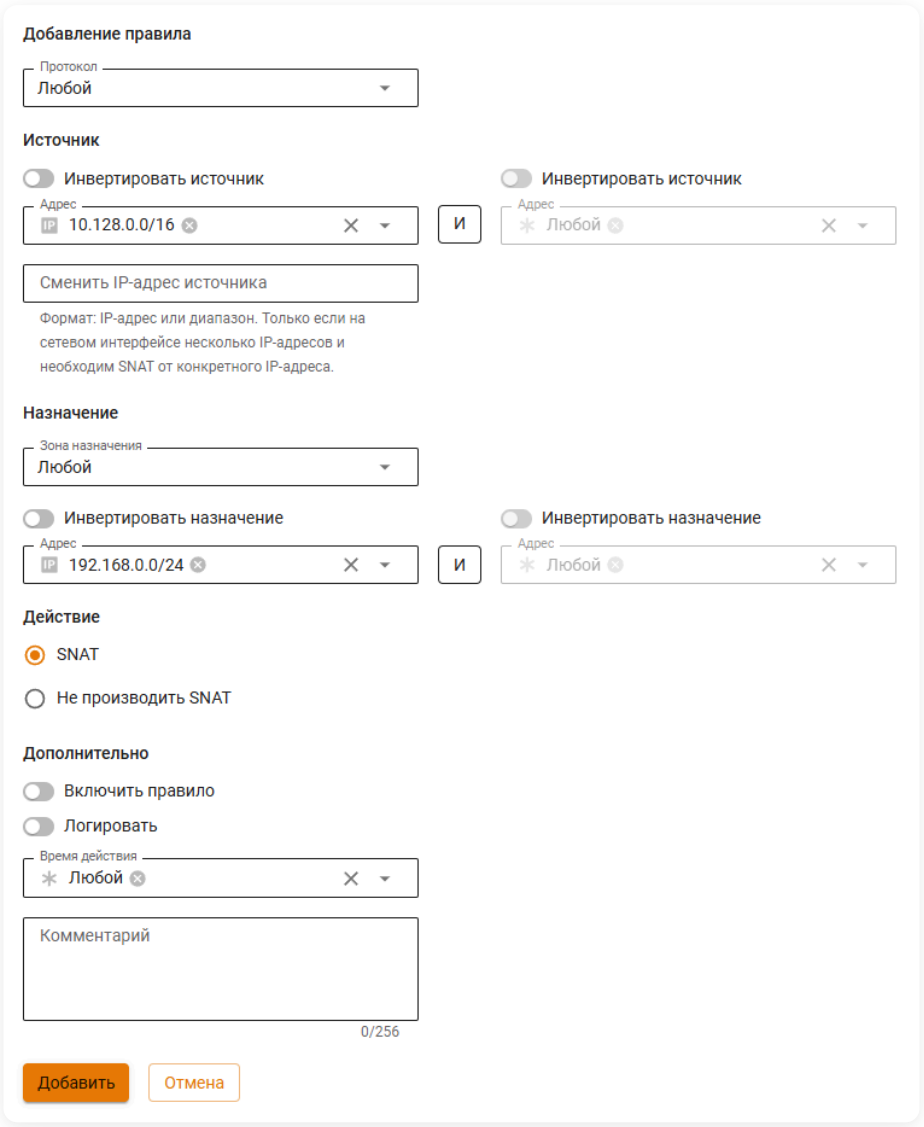
Чтобы обеспечить доступ, убедитесь, что VPN-сети обоих NGFW Novum не пересекаются. Затем проверьте настройки основного NGFW Novum, следуя инструкциям, описанным в статье.

Получение доступа к хостам локальной сети, если за NGFW Novum есть маршрутизатор, выступающий в качестве ядра локальной сети

Чтобы обеспечить доступ, нужно настроить на роутере маршрут от нужной локальной сети до VPN-сети. Для настройки маршрута на роутере укажите в качестве назначения VPN-сеть (`10.128.0.0/16`), в качестве шлюза - NGFW Novum (`172.16.0.1`).

Если настроить на роутере маршрут невозможно, можно создать на NGFW Novum SNAT-правило:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **SNAT**, нажмите **Добавить** и укажите параметры:



- **Источник** - VPN-сеть (`10.128.0.0/16`).
- **Назначение** - сеть за роутером, к которой требуется получить доступ из VPN-сети (`192.168.0.0/24`).

3. Нажмите **Добавить**.

В этом случае при отправке пакетов на роутер NGFW Novum подменит IP-адрес источника своим. За счет этого роутер направит ответ от хоста в локальной сети на NGFW Novum, который затем перенаправит его в VPN-сеть.

У хостов из локальной сети `192.168.0.0/24` не будет доступа к VPN-сети `10.128.0.0/16`.

Полезные ссылки

- **Как избежать проблем с подключением VPN-клиентов при нескольких серверах**

Инструкция по запуску PowerShell скриптов

Классический контекст | Высокопроизводительный контекст

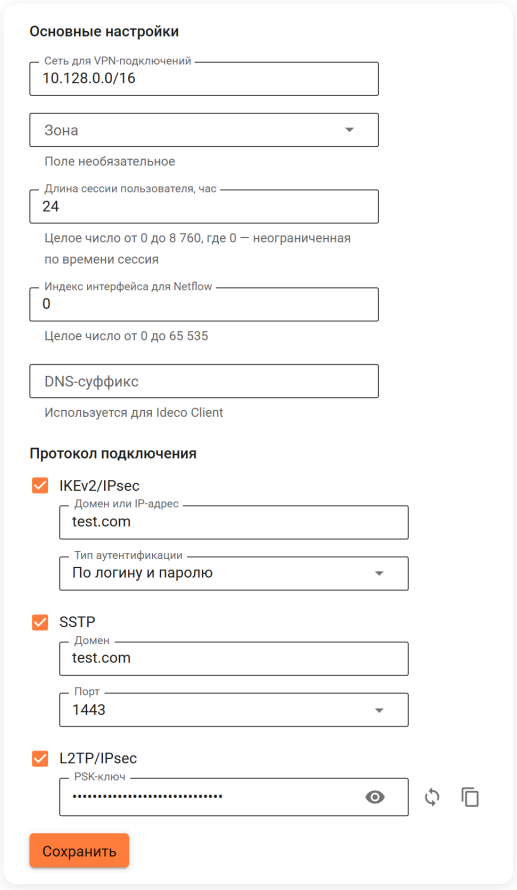
Для подключения по VPN к Ideco NGFW Novum с белым IP адресом достаточно действий, указанных ниже. Если Ideco NGFW Novum выходит в интернет через маршрутизатор, воспользуйтесь пунктом Подключение по VPN к Ideco NGFW Novum с доступом в интернет через маршрутизатор.

Запуск PowerShell-скрипта

1. Скачайте скрипт одним из способов:

Веб-интерфейс Ideco NGFW Novum

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**:



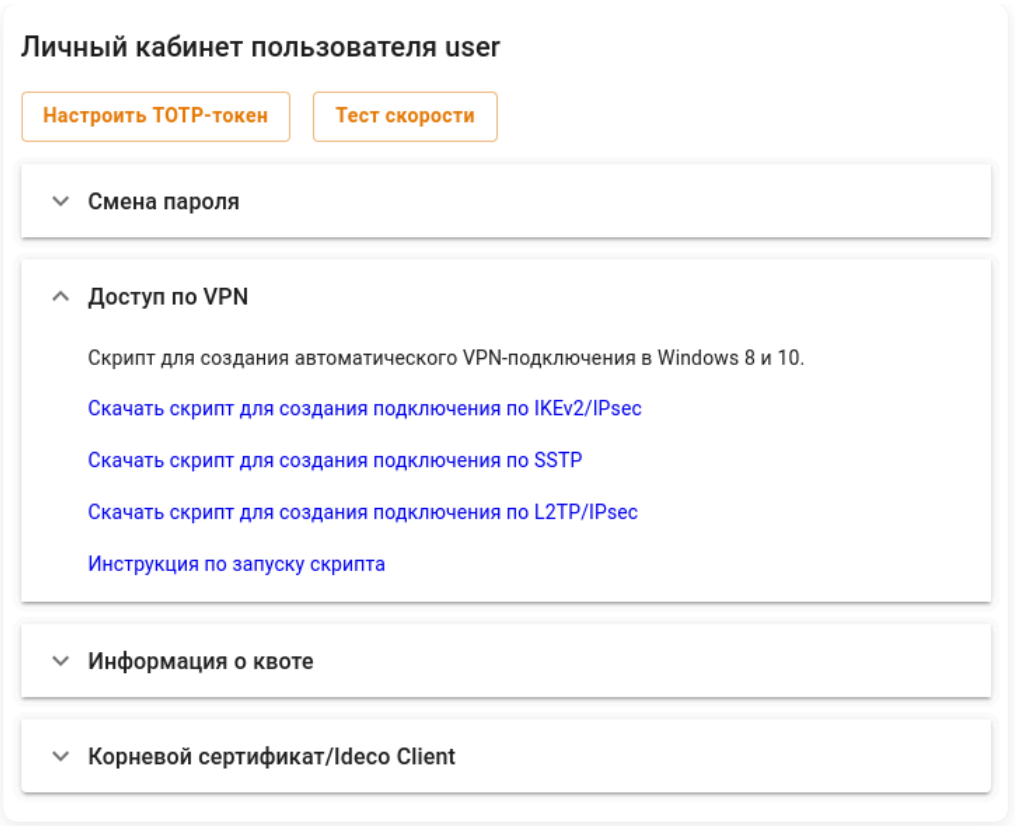
2. Включите и настройте требуемый протокол подключения.

3. Перейдите по ссылке **PowerShell - скрипт для настройки подключений**.

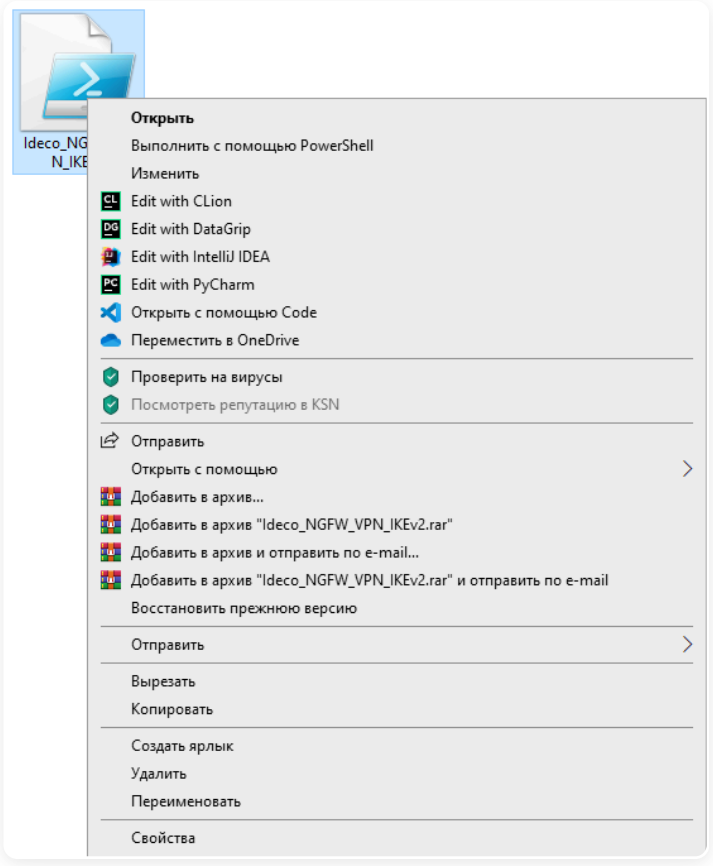
4. Перенесите скачанный файл на устройство, на котором требуется создать VPN-подключение.

Личный кабинет пользователя

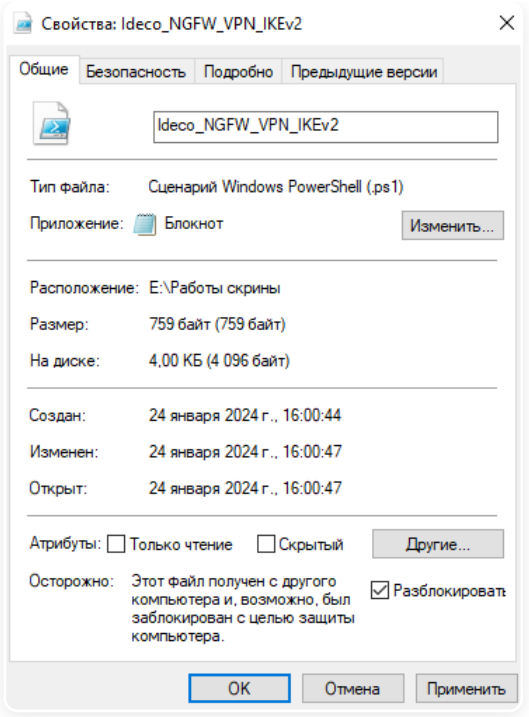
Скачайте скрипт, перейдя по ссылке **Скачать скрипт для создания подключения**:



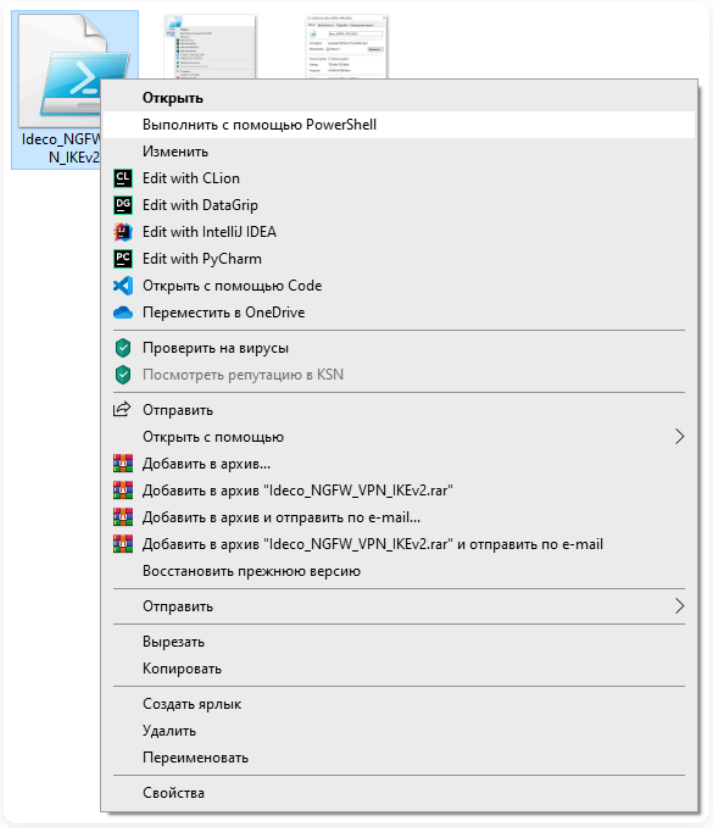
2. Щелкните правой кнопкой мыши по скачанному файлу и в контекстном меню выберите **Свойства**:



3. Включите опцию **Разблокировать** справа в нижнем углу свойств файла (по умолчанию ОС блокирует выполнение скачанных из интернета файлов):

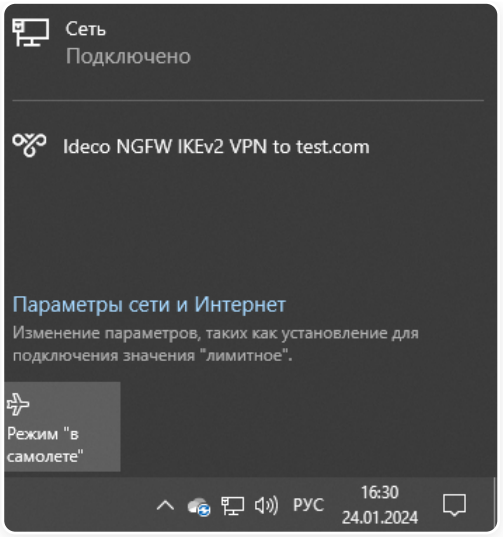


4. Нажмите правой кнопкой мыши на файл и выберите пункт **Выполнить в PowerShell**. Затем подтвердите действие, нажав **Да** на вопрос о внесении изменений в компьютер:



При появлении ошибки **Выполнение сценариев отключено в этой системе** откройте PowerShell с правами администратора, выполните команду для разрешения запуска скриптов `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`, в том же окне заново выполните скрипт для создания подключения и закройте консоль.

5. Когда подключение создано, нажмите **Подключиться** в списке сетей.



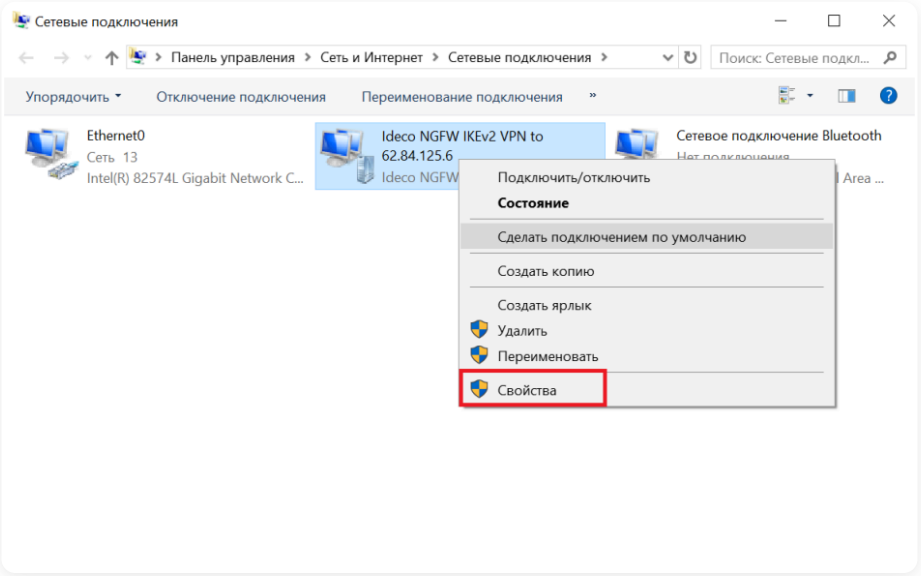
DNS-суффиксы для VPN-подключений

PowerShell-скрипты прописывают основной DNS-суффикс для создаваемого VPN-подключения. DNS-суффикс соответствует домену, в который введен Ideco NGFW Novum, что позволяет обращаться к устройствам за VPN по короткому имени.

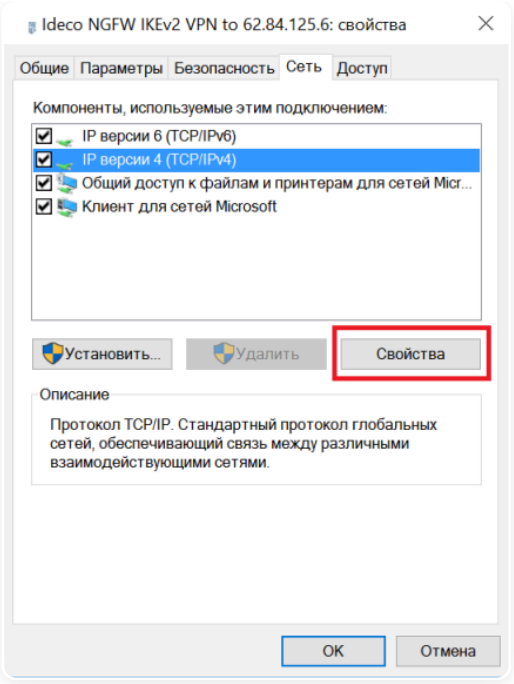
> Если Ideco NGFW Novum введен в несколько доменов, то DNS-суффиксы в PowerShell-скриптах не прописываются. Необходимо настроить DNS-суффиксы вручную на подключенном по VPN устройстве.

Чтобы настроить DNS-суффиксы для созданного VPN-подключения в Windows, выполните действия:

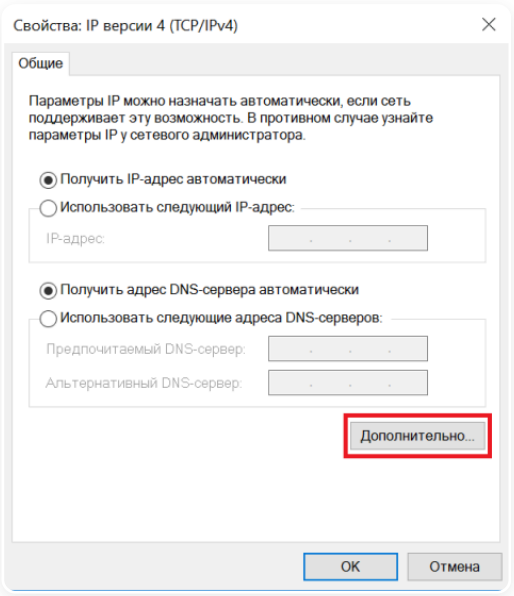
1. Перейдите в **Сетевые подключения**, нажмите правой кнопкой мыши по нужному VPN-подключению и выберите **Свойства**:



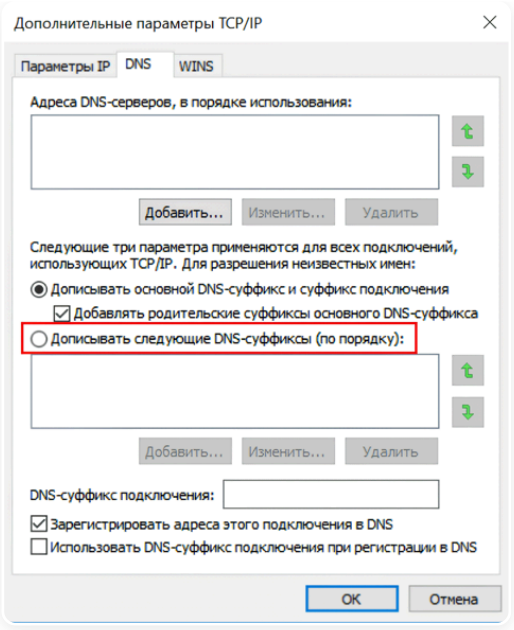
2. В открывшемся окне перейдите на вкладку **Сеть**, выберите компонент **IP версии 4 (TCP/IPv4)** и нажмите **Свойства**:



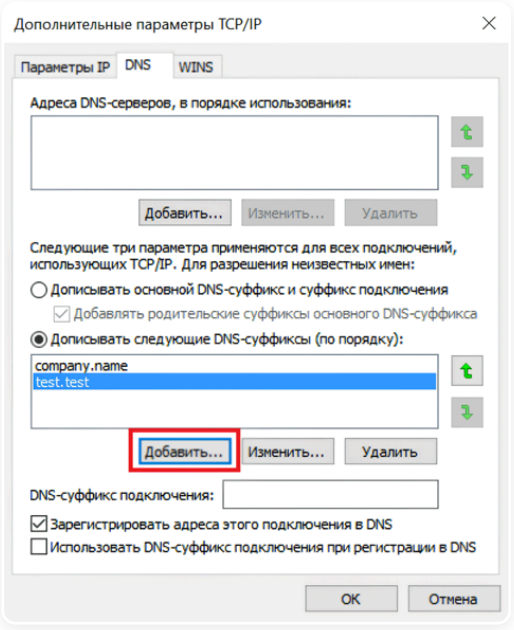
3. В открывшемся окне нажмите **Дополнительно**:



4. Перейдите на вкладку **DNS** и включите опцию **Дописывать следующие DNS-суффиксы (по порядку)**:



5. Нажмите **Добавить** и введите необходимые DNS-суффиксы:



При обращении к компьютеру по короткому имени DNS-суффиксы будут перебираться в порядке расположения. Порядок можно менять стрелками.

Подключение по VPN к Ideco NGFW Novum с доступом в интернет через маршрутизатор

Для работы скрипта подключения по VPN выполните действия:

1. Сделайте проброс портов 4500 и 500 в IP-адрес Ideco NGFW Novum в локальной сети маршрутизатора.

2. Загрузите скрипт на компьютер, воспользовавшись пунктом 1 инструкции Запуск PowerShell-скрипта.

3. Поменяйте в загруженном скрипте IP-адрес Ideco NGFW Novum на внешний IP-адрес маршрутизатора:

```
Add-VpnConnection
    -Force `
    -Name "Ideco NGFW L2TP VPN to 46.36.23.99" `
    -TunnelType L2TP `
    -ServerAddress 46.36.23.99 `
     -AuthenticationMethod MSChapV2 -L2tpPsk 'Jge7b11K_uEO_KYm3ArHcu50wWGjga' `
    -EncryptionLevel "Required" `
    -SplitTunneling $False `
    -RememberCredential
```

- **46.36.23.99** - IP-адрес Ideco NGFW Novum в локальной сети маршрутизатора.
- **5.189.21.1** - внешний IP-адрес маршрутизатора.

4. После выполнения действий следуйте инструкции Запуск PowerShell-скрипта с пункта 4.

Решение проблем запуска PowerShell-скрипта

Для запуска Powershell-скрипта убедитесь, что:

- Вам хватает прав на запуск скрипта.
- PowerShell установлен в системе.

Если не удалось решить проблему запуска PowerShell-скрипта, воспользуйтесь инструкцией для создания подключения в Windows 10 вручную.

Ideco Client

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Ideco Client**: `ideco-agent-backend`, `ideco-agent-websocket`, `ideco-websocket-vpn-server`.

Список служб для других разделов доступен по ссылке.

Ideco Client - программа-клиент, которая управляет авторизацией пользователей при подключении к NGFW Novum. Работает по одному из двух протоколов:

- **Wireguard** - используется собственный коммуникационный протокол, который реализует зашифрованные виртуальные частные сети (VPN). Для его работы используется порт UDP 3051.
- **TCP** - используется современный протокол транспортного уровня безопасности TLS (Transport Layer Security), обеспечивающий функции шифрования, аутентификации и целостности. Для его работы используется порт 443 по умолчанию.

С версии 22 NGFW Novum сессии Ideco Client синхронизируются между нодами кластера. При кратковременных разрывах соединения (до 60 секунд) Ideco Client автоматически восстанавливает подключение без повторного ввода пароля, прохождения 2FA и аутентификации по сертификату. Если соединение не восстановилось за 60 секунд, потребуется повторная авторизация вручную.

Логика выбора протокола Ideco NGFW Novum

С версии 21 для Ideco Client протокол определяется на основе правил в таблице **Пользователи → VPN-подключения → Доступ по VPN**:

- Если в первом сработавшем правиле для пользователя указан протокол подключения **Любой** или **Wireguard (Ideco Client)**, в том числе вместе с **TLS (Ideco Client)**, то используется **Wireguard**.
- Если в первом сработавшем правиле для пользователя указан протокол подключения **TLS (Ideco Client)**, то используется **TLS**.
- Правило применяется ко всем VPN-подключениям, включая терминальный сервер и Device VPN, с любым видом аутентификации. Действует из внешних и локальных сетей при включенной опции **С установлением туннеля**.

Особенности для разных типов подключений:

- Для локальной сети:
  - Если включена опция **С установлением туннеля**, используется протокол из правил **Доступа по VPN**.
  - Если включена опция **Без туннеля**, туннель не устанавливается, таблица **Доступа VPN** не проверяется. Доступ открывается по списку в поле **Пользователи и группы**.
- Для терминального подключения всегда используется **Wireguard**, т.к. **TLS** не поддерживается. При указании в правилах только **TLS (Ideco Client)** соединение будет отклонено с ошибкой, указанной в системном журнале в разделе **Отчеты и журналы → Система**.

Ideco Client недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

Поддерживаемые версии ОС	• Windows 10 22H2 и выше • macOS версии 13.4 и выше. При этом Ideco Client работает с некоторыми ограничениями • Astra Linux 1.7.0 и выше • РЕД ОС 8.0 и выше • Alt OS (Alt Workstation) 9.0 и выше • Fedora 35 и выше • Ubuntu 18.04 LTS (23.04) и выше

Порты для подключения, если NGFW Novum за NAT	• **80 TCP** - используется для работы сертификатов Let's Encrypt • **443 TCP** - используется для авторизации пользователя и установки управляющего соединения (порт по умолчанию) • **14765 TCP** - альтернативный порт для авторизации и управляющего соединения. Чтобы использовать его, укажите адрес сервера в формате `домен:14765` или `IP:14765` • **3051 UDP** - используется для передачи пользовательского трафика через туннель WireGuard. Трафик на этом порту фильтруется правилами таблицы FORWARD, а не INPUT **Межсетевого экрана** Для корректной работы Ideco Client убедитесь, что указанные порты открыты на всех устройствах между пользователем и Ideco NGFW Novum

Возможности Ideco Client

- [x] Авторизация в локальной сети
- [x] VPN-подключение из внешних сетей
- [x] VPN-подключение из локальных сетей
- [x] Режим работы Device VPN
- [x] Двухфакторная аутентификация
- [x] Трехфакторная аутентификация
- [x] Привязка устройств к пользователям по сертификатам
- [x] Сбор данных о подключающихся устройствах

Сбор данных о подключающихся устройствах позволяет задавать критерии проверки - HIP-профили.

HIP-профили помогают реализовать ZTNA (Zero Trust Network Access) - технологию, которая обеспечивает безопасный доступ к сети на основе принципа **нулевого доверия**. ZTNA контролирует и аутентифицирует устройства пользователей перед предоставлением доступа к ресурсам сети.

Скачать Ideco Client

Windows

Скачать Ideco Client

Для версии 10 и новее, Windows Server 2019 и новее.

macOS

Скачать Ideco Client

Для версии 13.4 и новее.

Linux

Скачать Ideco Client

Для Alt Linux, Red OS, Astra Linux.

Каждой версии NGFW Novum соответствует определенная версия Ideco Client. При обнаружении несоответствия Ideco Client автоматически обновляется до требуемой версии при подключении.

Полезные ссылки

- **Настройка Device VPN**
- **Создание сертификатов для Device VPN**
- **Сертификаты**
- **Кастомная настройка Ideco Client**

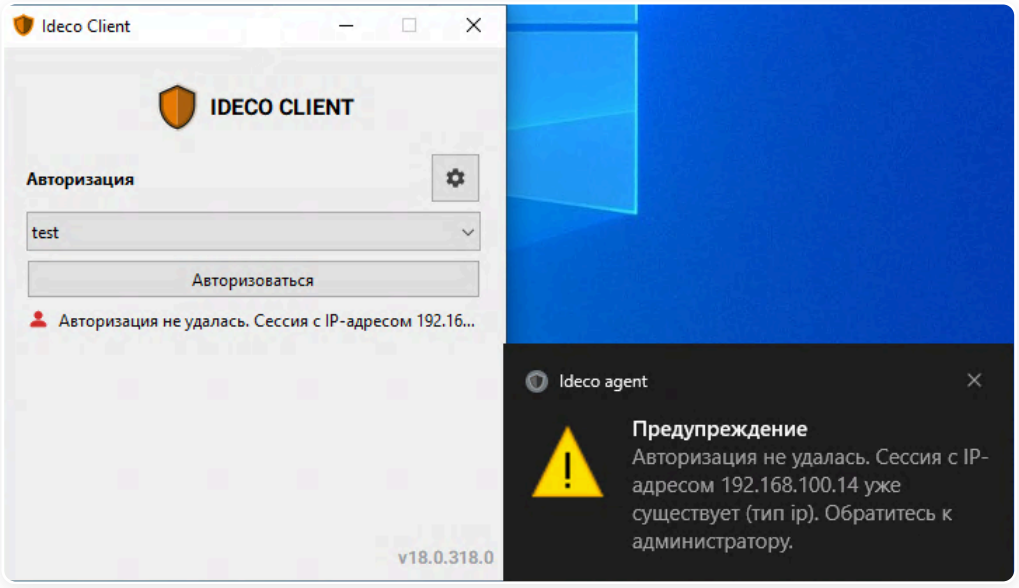
- **Настройки в Ideco NGFW Novum**
- **Как включить режим отладки для Ideco Client**
- **Подключение через Ideco Client к внутреннему DNS**

Особенности работы Ideco Client

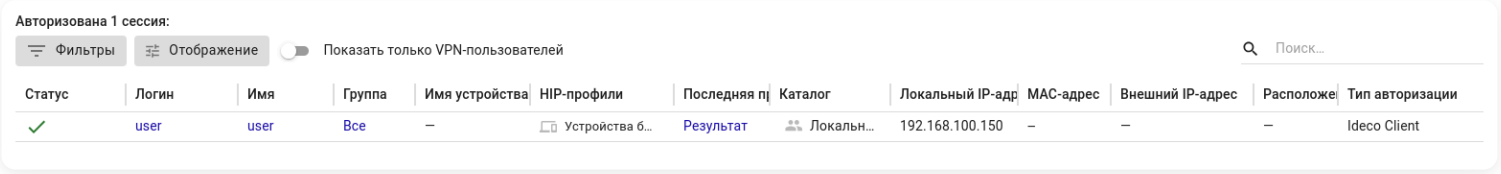
Классический контекст | Высокопроизводительный контекст

Особенности работы Ideco Client, которые важно учитывать при настройке и использовании:

- Только один профиль может быть с опцией автоподключения. Если активировать автоподключение для другого профиля, у предыдущего эта опция отключится.
- Чтобы использовать SSO-профиль с автоподключением, вручную укажите доменное имя в поле **Хост**. Для предварительной настройки адреса подключения используйте групповую политику или запустите файл через командную строку с ключом: `IdecoClient.msi utm_address=адрес_ngfw`.
- При попытке повторной авторизации пользователя, который уже авторизован по IP, появляется предупреждение:



- После каждого обновления приложение Ideco Client запускается автоматически.
- Информация о сессиях пользователей отображается в разделе **Сессии пользователей**:



Особенности работы DNS-запросов при VPN-подключении через Ideco Client

При подключении через Ideco Client DNS-запросы могут не проходить, если выбран тип передачи маршрутов **Отправлять только указанные сети**. При выборе **Отправлять маршруты до локальных сетей Ideco NGFW Novum** сеть до NGFW Novum отправляется автоматически. Это связано с особенностями построения таблицы маршрутизации при подключении через Ideco Client:

- При VPN-подключении без Ideco Client DNS-запросы идут на DNS, прописанный в настройках подключения (как правило, адрес NGFW Novum).
- При VPN-подключении через Ideco Client DNS-запросы идут на адрес NGFW Novum, но в передаваемом на Ideco Client списке нет маршрута до DNS NGFW Novum.

Рекомендуем при выборе типа передачи маршрутов **Отправлять только указанные сети** добавить в список DNS NGFW Novum, чтобы клиент VPN построил таблицу маршрутизации до этой сети.

Особенности маршрутизации и организации доступа по VPN к ресурсам локальной сети описаны в статье.

Как работает перенос настроек с профилями при смене версии

При запуске Ideco Client выполняет последовательность действий:

1. Ideco Client проверяет наличие настроек в json-файле настроек профиля текущей версии.

2. Если настройки найдены, они применяются.

3. Если настройки текущей версии отсутствуют, ищет в json-файлах настроек прошлых версий (от новой к старой).

4. При нахождении настроек в предыдущих версиях они копируются в json-файл настроек текущей версии Ideco Client.

5. Если настройки не найдены, то создается json-файл настроек текущей версии с параметрами по умолчанию.

Файл настроек профиля хранится по пути:

- Linux: `$HOME/.config/Ideco/Agent/<version>/`
- Windows: `C:/Users/<Имя_пользователя>/AppData/Local/Ideco/Agent/<version>/`
- macOS: `$HOME/Library/Preferences/Ideco/Agent/<version>/`

Алгоритм поиска и применения настроек

- Поиск осуществляется последовательно по мажорным и минорным версиям от новой к старой.
- Копирование происходит только вперед с более ранней версии на новую.
- Копируются первые найденные настройки.
- Назад по версиям копирование не осуществляется.
- Если вручную удалить json-файл настроек текущей версии, то при следующем запуске Ideco Client инициирует поиск и копирование настроек. Если настройки не будут найдены в json-файлах настроек предыдущих версий, то будет создан json-файл с настройками по умолчанию.

Примеры работы переноса настроек

Первая установка Ideco Client

Ideco Client не установлен и в каталоге нет json-файла настроек Ideco Client:

1. При запуске Ideco Client создает json-файл настроек текущей версии с параметрами по умолчанию.

2. Копирование не выполняется.

Обновление Ideco Client на следующую версию

Пользователь обновляет Ideco Client с 21.3.2 до 22.0.703:

1. Ideco Client проверяет наличие настроек в json-файле настроек версии 22.0.703.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в json-файлах настроек предыдущих версий от более новой к более старой.

4. Если настройки найдены в json-файле настроек одной из прошлых версий, то они копируются в json-файл настроек версии 22.0.703.

5. Если настройки не найдены, то создается json-файл настроек версии 22.0.703 с параметрами по умолчанию.

Возврат Ideco Client на предыдущую версию

Возврат Ideco Client с версии 22.0.2 на 22.0.1:

1. При запуске Ideco Client ищет настройки в json-файле настроек версии 22.0.1.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в json-файлах настроек предыдущих версий от более новой к более старой.

4. Если настройки найдены, они копируются в json-файл настроек версии 22.0.1.

5. Если настройки не найдены, то создается json-файл настроек версии 22.0.1 с параметрами по умолчанию.



Копирование не происходит назад по версиям, поэтому копирование настроек из версии 22.0.2 на 22.0.1 невозможно.

Повторное обновление Ideco Client после возврата на предыдущую версию

1. Пользователь использовал версию 22.0.2.

2. Выполнен возврат на версию 22.0.1.

3. Пользователь создал новый профиль в версии 22.0.1

4. Выполнено обновление до версии 22.0.2.

5. При запуске Ideco Client настройки и профили из версии 22.0.1 не будут перенесены в версию 22.0.2, поскольку json-файл настроек версии 22.0.2 уже существует, созданный при первом запуске.

Алгоритм работы Ideco Client при редиректах

После формирования списка для подключения Ideco Client пытается подключиться к серверам из списка. Если отправлен редирект с кодом ответа `302`, то Ideco Client продолжит подключение по указанному в редиректе адресу до успешной установки соединения.

Если сервер возвращает редирект с кодом ответа `302`, Ideco Client не ищет SRV-записи для нового адреса. Ideco Client подключится по адресу, полученному в редиректе.

При попытке подключения к хостам из списка могут возникнуть циклические редиректы. На Ideco Client есть ограничение в пять редиректов. При шестом редиректе подключение к текущему серверу считается неуспешным.

Обработка запросов с редиректом позволяет использовать VPN-балансировщик для распределения нагрузки между несколькими NGFW Novum.

Балансировка VPN-подключений происходит на стороне Ideco Client с использованием SRV-записей DNS.

В SRV-записи DNS нельзя указывать IP-адрес, только FQDN (полностью определенное доменное имя, не имеющее неоднозначностей в определении). При указании IP-адреса в SRV-записи IP-адрес будет распознан как поддомен зоны. Подробнее про SRV-записи в RFC-2782.

Если в параметре `target` SRV-записи указан `.`, подключение не сработает. Появится сообщение, что сервис недоступен. Параметр `target` SRV-записи `.` может настраиваться при регистрации доменного имени или при конфигурации записей для доменного имени.

Алгоритм работы Ideco Client при балансировке

При нажатии **Подключиться** Ideco Client проверяет адрес сервера, заданный в настройках профиля, и составляет список для подключения, основываясь на следующих правилах:

1. Если адрес сервера - IP-адрес, то происходит подключение Ideco Client по этому адресу.
2. Если адрес сервера - FQDN, то происходит запрос SRV-записей вида `_ideco-client._tcp.<FQDN домена>` (например: `_ideco-client._tcp.ideco.example.ru`) для указанного FQDN:

- Если для текущего FQDN есть SRV-записи, то происходит добавление SRV-записей в список для подключения. Записи сортируются по параметру `priority`. Если значения совпадают, сортировка продолжается по параметру `weight`. Подробнее про сортировку `weight` в RFC-2782.
- Если для текущего FQDN нет SRV-записей, то происходит разрешение FQDN в IP-адрес с помощью записи типа A и Ideco Client подключается по этому IP-адресу.

Как Ideco Client обрабатывает запросы с редиректом на сервер Ideco NGFW

Ideco Client может обрабатывать запросы с перенаправлением (код ответа 302). Получив ответ от сервера, **Ideco Client** выполняет шаги для подключения к **Ideco NGFW Novum**:

1. Отправляет запрос на адрес https://host:443/connect.
2. Если сервер отвечает статусом 302 с редиректом, **Ideco Client** использует информацию из этого ответа для установления соединения.
3. **Ideco Client** подключается к NGFW, используя имя сервера или IP-адрес, указанный в поле Location.

Важно:

- Адрес обязательно должен включать порт `443`.
- В заголовке Location в ответе 302 должен быть указан полный URL-адрес, из которого будет извлечено только имя сервера или IP-адрес.
- Полученное имя сервера или IP-адрес используются для создания адреса в формате `wss://host_from_location:443/connect`, к которому будет подключаться **Ideco Client**.
- Если ответа со статусом 302 от адреса `https://host:443/connect` нет, то **Ideco Client** подключится к NGFW по адресу `wss://host:443/connect`.

Пример правильного редиректа, полученный с помощью утилиты **curl**:

1. **Запрос**: `curl -il https://host.dev:443/connect`.

2. **Ответ**:

```
HTTP/1.1 302 Found
Server: SERVERNAME
Date: Fri, 15 Nov 2024 04:22:46 GMT
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=15
Location: https://ngfw-host.dev/
cache-control: no-cache
```

Из заголовка `Location: https://ngfw-host.dev/` будет извлечен новый хост `ngfw-host.dev`, и **Ideco Client** будет подключаться к NGFW по адресу `wss://ngfw-host.dev:443/connect`.

3. Если при попытке доступа к URL-адресу `https://host.dev:443/connect` не будет получен ответ с кодом 302, то **Ideco Client** подключится к NGFW по адресу `wss://host.dev:443/connect`.

Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

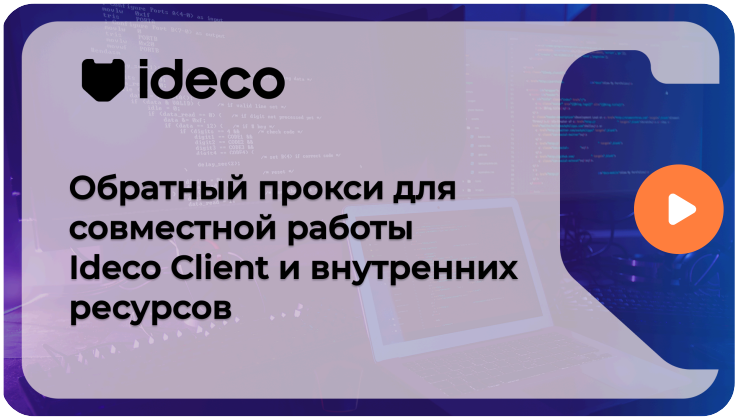
- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Ideco Client не работает, если внутренние ресурсы опубликованы через DNAT

Видеоинструкция

Ссылки на другие ресурсы

YouTube | RUTUBE | VK Видео



Ideco Client для работы использует TCP-порт 443 по умолчанию. Если этот порт занят правилами DNAT для публикации внутренних ресурсов (например, Microsoft Exchange), Ideco Client автоматически переключится на TCP-порт 14765 после неудачной попытки подключения.

Для корректной работы Ideco Client и внутренних ресурсов рекомендуем использовать обратный прокси. Этот способ позволит Ideco Client и внутренним ресурсам работать через один порт при помощи SNI-маршрутизации.

Если использование обратного прокси невозможно, зарезервируйте TCP-порт 443 за Ideco Client, а для публикации внутренних ресурсов назначьте другой TCP-порт.

Аутентификация по сертификату

Классический контекст | Высокопроизводительный контекст

Аутентификация по сертификату - механизм, при котором Ideco NGFW Novum проверяет подлинность устройства пользователя по цифровому сертификату. Сертификат дополняет проверку логина и пароля, а для подключений Device VPN заменяет ее: даже если учетные данные скомпрометированы, подключение с устройства без действующего сертификата не создается.

Аутентификация по сертификату реализована для подключений через Ideco Client и входит в концепцию ZTNA (Zero Trust Network Access). Ideco NGFW Novum сам выпускает сертификаты и управляет привязками пользователей к устройствам - отдельная PKI-инфраструктура не требуется.

Как работает аутентификация по сертификату

Подключение через Ideco Client состоит из двух этапов:

Этап 1. Проверка учетных данных. Пользователь вводит логин и пароль или проходит SSO. Ideco NGFW Novum проверяет учетные данные в локальной базе или во внешнем каталоге. Для Device VPN на этом этапе выполняется идентификация устройства без входа пользователя.

Этап 2. Проверка сертификата устройства. Если сертификат устройства уже установлен (независимо от режима), Ideco NGFW Novum выполняет его проверку:

1. Ideco NGFW Novum запрашивает сертификат устройства.

2. Ideco Client отправляет сертификат с доказательством владения закрытым ключом.

3. Ideco NGFW Novum проверяет сертификат:

- **Доверие к CA** - сертификат должен быть подписан одним из доверенных удостоверяющих центров, указанных в настройках.
- **Срок действия** - сертификат не должен быть просрочен.
- **Статус отзыва** - сертификат не должен быть отозван.

4. Если включена привязка устройства, Ideco NGFW Novum проверяет, совпадает ли сертификат с привязанным устройством.

Проверка сертификата устройства считается включенной:

- **Для туннельных подключений (VPN)** - если в правиле **Пользователи → VPN-подключения → Доступ по VPN** в поле **Доверенные CA-сертификаты** выбран хотя бы один сертификат удостоверяющего центра.
- **Для локальных подключений (без туннеля)** - если в настройках **Пользователи → Ideco Client → Основное** в блоке **Авторизация пользователей** выбран хотя бы один **Доверенный CA-сертификат**.
  Если поле **Доверенные CA-сертификаты** не заполнено, проверка сертификата устройства не выполняется.

Если все проверки пройдены, Ideco NGFW Novum создает VPN-сессию. Если хотя бы одна проверка не пройдена, подключение отклоняется, а причина отказа записывается в журнал **Отчеты и журналы → Аутентификация пользователей** и отображается в разделе **Мониторинг → Сессии пользователей**.

Закрытый ключ сертификата устройства на Ideco NGFW Novum не передается и хранится только на устройстве пользователя.

Привязка пользователя к устройству

Привязка фиксирует за учетной записью пользователя конкретное устройство. После создания привязки подключение с других устройств отклоняется, даже если на них установлен действительный сертификат, подписанный тем же CA.

Привязка появляется при первом удачном входе пользователя, когда в правиле доступа заполнено поле **Доверенные CA-сертификаты**, включена опция **Привязать устройство к пользователю** и с устройства предъявлен действующий сертификат. Работа со списком привязок, удаление и автоматическое пересоздание привязки описаны в статье Настройка Ideco Client.

На учетные записи и группы **Ideco Device VPN** привязка не распространяется.

Режимы управления сертификатом устройства

Способ, которым сертификат попадает на устройство, зависит от режима работы Ideco Client:

- **AUTO** - Ideco NGFW Novum автоматически выпускает сертификат при первом подключении пользователя. Участие администратора не требуется. Сертификат выпускается только после успешной проверки учетных данных и используется при всех последующих подключениях пользователя, включая Device VPN.
- **MANUAL** - сертификат выпускается внешним удостоверяющим центром по CSR от Ideco Client. Режим подходит для корпоративной PKI-инфраструктуры.
- **EXTERNAL** - готовую пару **сертификат + закрытый ключ** предоставляет администратор.

Режимы определяют только способ, которым ключ и сертификат попадают на устройство. После установки ключа и сертификата Ideco Client переходит в готовое состояние и не хранит информацию об источнике. **Любое переключение режима удаляет установленные ранее ключ и сертификат** - переходы AUTO → EXTERNAL, EXTERNAL → AUTO, AUTO → MANUAL, MANUAL → EXTERNAL и обратные работают одинаково: прежнее состояние сбрасывается, и администратор должен установить ключ и сертификат заново в соответствии с выбранным режимом.

Команды CLI для переключения режимов и правила хранения закрытых ключей на разных ОС описаны в статье Настройка Ideco Client.

Работа сертификата с Device VPN

Device VPN не может самостоятельно запустить автоматический выпуск сертификата. Поведение зависит от того, установлен ли на устройстве сертификат от предыдущих подключений пользователя:

- **Сертификат уже установлен** - пользователь ранее авторизовался на Ideco NGFW Novum через Ideco Client и получил сертификат в режиме AUTO. Этот же сертификат используется для подключения Device VPN без дополнительных действий администратора.
- **Сертификата нет** - администратор устанавливает сертификат на устройство вручную в режиме EXTERNAL. Переключение режима удаляет установленные ранее ключ и сертификат.

Порядок настройки Device VPN и выпуска сертификата через OpenSSL описан в статье Создание сертификатов для Device VPN.

Настройка аутентификации по сертификату

Для включения аутентификации по сертификату настройте три раздела:

Что настраивается	Где настраивается
Учетная запись пользователя	**Пользователи → Учетные записи**
Доверенные CA-сертификаты	**Сервисы → Сертификаты → Ideco Client → Реестр**
Правило доступа VPN и привязка устройства	**Пользователи → VPN-подключения → Доступ по VPN** - блок **Настройки доступа через Ideco Client**

Для подключений из локальной сети без туннеля (опция **Без туннеля**) сертификат и привязка настраиваются в **Пользователи → Ideco Client → Основное**.

Ограничения

- Автоматический выпуск сертификата применим только к пользовательским подключениям. Для Device VPN автоматический выпуск не выполняется.
- Поддерживается одна активная привязка на пользователя.
- Автоматическая проверка CRL/OCSP для внешних CA не выполняется.
- Сертификаты должны соответствовать X.509, DN должен однозначно сопоставляться с устройством.

Восстановление доступа после отзыва сертификата устройства

После отзыва сертификата устройства на Ideco NGFW Novum пользователь не сможет подключиться. Отменить отзыв сертификата невозможно.

> Описанный порядок действий применим к режиму AUTO. В режимах MANUAL и EXTERNAL установите новый сертификат в соответствии с выбранным режимом.

Для восстановления доступа выполните действия:

1. На устройстве пользователя удалите файл `device-cert.json`. Путь зависит от ОС и версии Ideco Client:

- **Windows**: `%SystemRoot%\System32\config\systemprofile\Ideco\Agent<версия Ideco Client>\device-cert.json`
- **macOS**: `/Library/Application Support/Ideco/Agent/<версия Ideco Client>/device-cert.json`
- **Linux**: `/root/.config/Ideco/Agent/<версия Ideco Client>/device-cert.json`

2. Перезапустите службу Ideco Service или перезагрузите ОС.

3. Если в настройках включена опция **Привязать устройство к пользователю**, перейдите в **Пользователи** → **Ideco Client** → **Привязанные устройства** и удалите запись привязки для данного пользователя.

При следующем подключении Ideco Client инициирует выпуск нового сертификата в режиме AUTO - сгенерирует закрытый ключ, сформирует CSR и отправит его на Ideco NGFW Novum для подписи. Если опция **Привязать устройство к пользователю** включена, новая привязка создается автоматически при первой успешной аутентификации.

Сценарии использования

- ✅ Удаленный доступ сотрудников к корпоративной сети: подключение идет с корпоративного устройства под учетной записью сотрудника через защищенный туннель
- ✅ Доступ подрядчиков к ограниченному набору ресурсов: сертификат выпускается на конкретное устройство, подключение с личного устройства подрядчика отклоняется
- ✅ Защита привилегированных учетных записей: фишинг логина и пароля не дает доступ без сертификата устройства и без доступа к привязанному устройству
- ✅ Соответствие требованиям регуляторов по многофакторной аутентификации при доступе к системам с персональными данными, КИИ, ГИС
- ✅ Реализация ZTNA в сочетании с HIP-профилями - добавляется проверка состояния устройства (антивирус, обновления ОС, шифрование диска)

Полезные ссылки

- **Ideco Client**
- **Настройка Ideco Client**
- **Device VPN**
- **Создание сертификатов для Device VPN**
- **Доступ по VPN**
- **Сертификаты**
- **HIP-профили**

Пользователи

Настройки в Ideco NGFW Novum

Основные параметры и конфигурация Ideco Client в Ideco NGFW Novum

Перейти >

Установка и настройка Ideco Client на разных ОС

Как установить Ideco Client на Windows, Linux, macOS

Перейти >

Установка и настройка Ideco Client на Windows

Как установить и настроить Ideco Client на Windows

Перейти >

Установка и настройка Ideco Client на macOS

Как установить и настроить Ideco Client на macOS

Перейти >

Установка и настройка Ideco Client на Linux

Как установить и настроить Ideco Client на Linux

Перейти >

Кастомная настройка Ideco Client

Настройка управления профилями и правами пользователей в Ideco Client через JSON-конфигурационный файл.

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройки в Ideco NGFW Novum

Классический контекст | Высокопроизводительный контекст

Подключение пользователей по VPN

Из внешней сети:

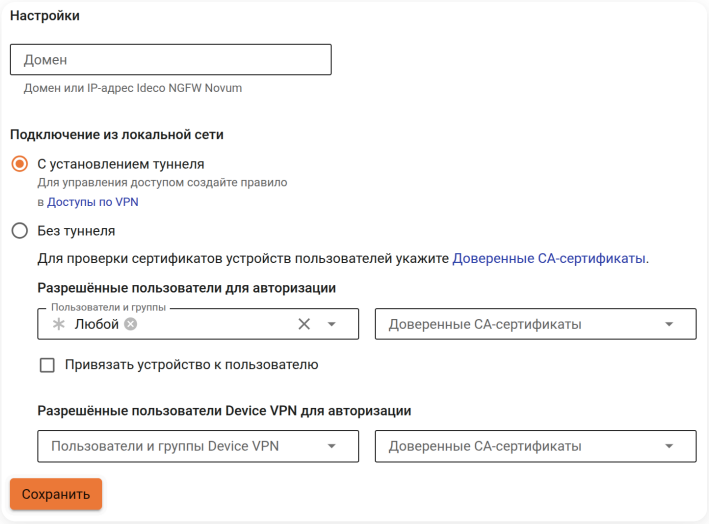
1. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN**.

2. Создайте правило, разрешающее пользователю VPN-подключение.

Из локальной сети:

1. Перейдите в **Ideco Client** → **Основное** и в поле **Домен** укажите доменное имя или IP-адрес Ideco NGFW Novum. Например: `example.ru`, `ideco.example.ru` или `52.251.83.117`.

2. В блоке **Подключение из локальной сети** выберите опцию **С установлением туннеля**:



3. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте правило, разрешающее пользователю VPN-подключение. В правиле настраиваются:

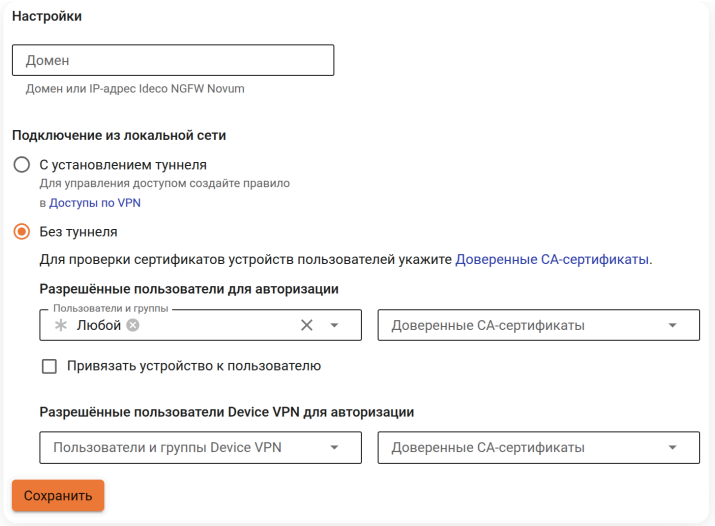
- Проверка сертификата устройства
- Привязка устройства к пользователю
- HIP-профили
- Двухфакторная аутентификация

Чтобы пользователь мог выйти в интернет, нужно выполнить одно из следующих действий:

- Настроить вторую сессию авторизации пользователя. Например, через Веб-аутентификацию.
- На вкладке Передача маршрутов для нужных пользователей выберите опцию **Отправлять весь трафик на Ideco NGFW Novum**.

Подключение пользователей из локальной сети без VPN

1. Перейдите в **Ideco Client** → **Основное** и в блоке **Подключение из локальной сети** выберите опцию **Без туннеля**:



2. Заполните поля:

- **Разрешенные пользователи для авторизации**:
  - **Пользователи и группы** - выберите пользователей или группы, которым разрешена авторизация.
  - **Доверенные CA-сертификаты** - выберите один или несколько сертификатов удостоверяющих центров, которым должно доверять устройство пользователя. Если поле пустое, проверка сертификата не выполняется. Проверка сертификата служит третьим фактором аутентификации, подтверждая подлинность устройства.
  - **Привязать устройство к пользователю** - включите опцию для создания записи в таблице **Привязанные устройства** при первом успешном подключении пользователя с этого устройства. После этого пользователь сможет подключаться только с этого устройства до удаления привязки.
- **Разрешенные пользователи Device VPN для авторизации**:
  - **Пользователи и группы Device VPN** - выберите учетные записи Device VPN (или группу **Ideco Device VPN**), которым разрешена авторизация.
  - **Доверенные CA-сертификаты** - выберите один или несколько сертификатов удостоверяющих центров, которым должно доверять устройство пользователя.

Изменения в настройке **Подключение из локальной сети** разрывает текущие сессии из локальных сетей. Повторное подключение будет соответствовать новому значению настройки.

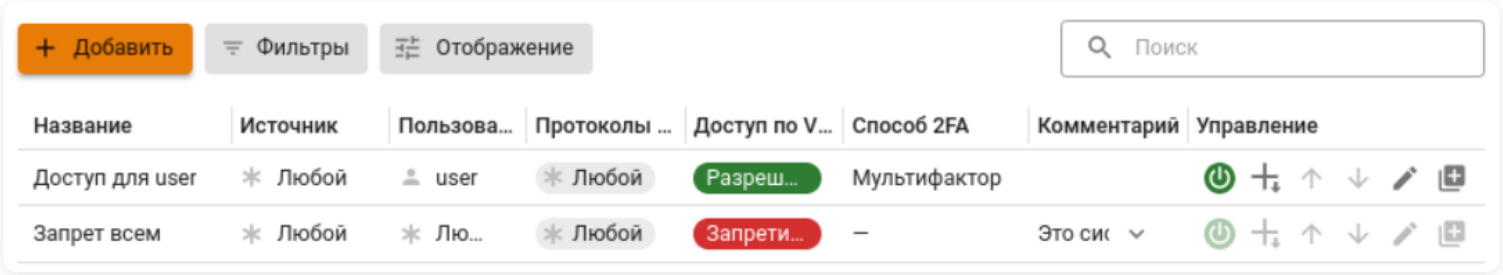
Настройка двухфакторной аутентификации в Ideco Client

В веб-интерфейсе Ideco NGFW Novum:

1. Создайте учетную запись пользователя в **Пользователи** → **Учетные записи**.

2. Перейдите в **Пользователи** → **Двухфакторная аутентификация** и выберите подходящие типы. Настройте двухфакторную аутентификацию способами, указанными в статье.

3. Добавьте правило в **Пользователи** → **VPN-подключения** → **Доступ по VPN**. В настройках правила укажите созданную учетную запись пользователя и тип двухфакторной аутентификации, выбранный в шаге 2. В поле **Протоколы** укажите значение **Любой**:

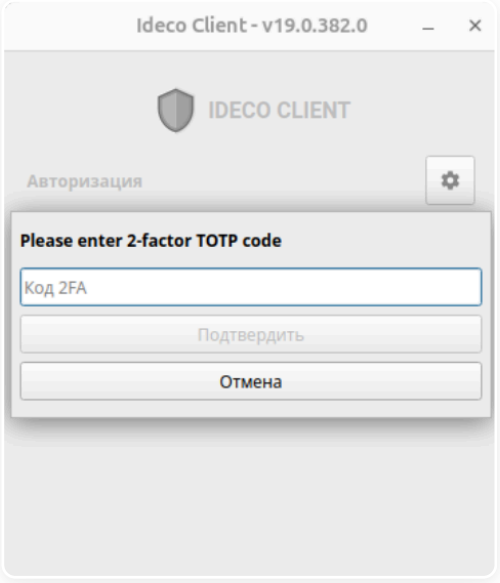


На устройстве пользователя:

1. Установите и запустите приложение Ideco Client. Инструкции по установке: Windows.

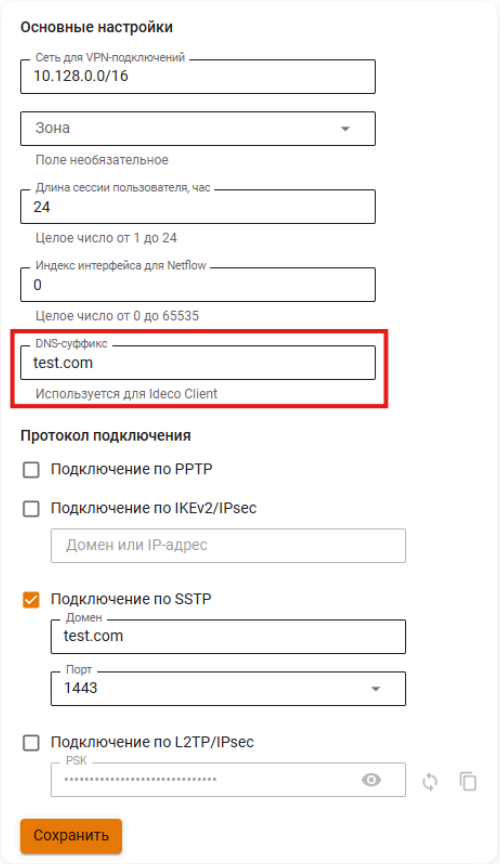
2. Авторизуйтесь через настроенную учетную запись пользователя:

3. Введите код двухфакторной аутентификации:



DNS-суффиксы для VPN-подключений по протоколу Wireguard

Укажите DNS-суффикс внутреннего домена (например, company.lan) в **Пользователи** → **VPN-подключения** → **Основное** → **DNS-суффикс** и нажмите **Сохранить**:



Суффикс будет передан устройствам через Ideco Client и позволит использовать короткие имена серверов (например, server-1c вместо server-1c.company.lan). Без суффикса разрешение таких имен работать не будет.

Ideco NGFW Novum поддерживает только один DNS-суффикс. Не указывайте DNS-суффикс, если NGFW Novum введен в несколько доменов.

Выпуск сертификата устройства

Сертификат устройства подтверждает подлинность устройства при подключении к Ideco NGFW Novum и служит третьим фактором аутентификации. Способ выпуска сертификата зависит от режима управления сертификатом устройства. По умолчанию используется режим AUTO - сертификат выпускается автоматически при первом подключении.

Выпуск сертификата в режиме AUTO недоступен для Device VPN. Если сертификат на устройстве отсутствует, подключение будет отклонено.

Сертификат для Device VPN создается вручную. Процесс описан в статье Создание сертификатов для Device VPN.

Режимы управления сертификатом устройства

Ideco Client поддерживает три режима управления сертификатом устройства: AUTO, MANUAL и EXTERNAL. Режим определяет, каким образом генерируется закрытый ключ, формируется запрос на подпись (CSR) и устанавливается сертификат.

Переключение между режимами выполняется через командную строку (CLI) Ideco Client.

При переключении режима текущий закрытый ключ и сертификат удаляются. Генерируется новый закрытый ключ. Если администратор задал DN, стандартный DN перезаписывается.

Режим AUTO

В режиме AUTO сертификат устройства автоматически выпускается Ideco NGFW Novum при отсутствии сертификата на устройстве. Участие администратора не требуется.

Порядок работы:

1. При первом запуске Ideco Client генерирует закрытый ключ и сохраняет его на устройстве.

2. При подключении к Ideco NGFW Novum пользователь проходит аутентификацию по первому фактору (логин/пароль).

3. Ideco Client формирует запрос на подпись (CSR) и отправляет его на Ideco NGFW Novum.

4. Ideco NGFW Novum подписывает CSR и возвращает сертификат.

5. Ideco Client проверяет соответствие сертификата закрытому ключу и сохраняет его на устройстве.

6. При последующих подключениях сертификат предъявляется Ideco NGFW Novum вместе с доказательством владения закрытым ключом.

Для сброса сертификата и возврата в режим AUTO выполните команду:

```
ideco-client --reset-to-auto-mode
```

Для сброса с указанием нового DN:

```
ideco-client --reset-to-auto-mode --set-dn "CN=hostname-example"
```

Если на устройстве есть сертификат Device VPN, при первом запуске он будет перенесен в хранилище сертификатов Ideco Client и использован как сертификат устройства. Новый закрытый ключ в этом случае не генерируется.

Режим MANUAL

В режиме MANUAL Ideco Client генерирует закрытый ключ и запрос на подпись (CSR), но не отправляет CSR на Ideco NGFW Novum. Администратор самостоятельно передает CSR во внешний удостоверяющий центр, получает подписанный сертификат и загружает его в Ideco Client.

До загрузки подписанного сертификата подключение к Ideco NGFW Novum невозможно.

Получение CSR

Для генерации CSR и вывода его в консоль выполните команду:

```
ideco-client --get-csr
```

Для сохранения CSR в файл укажите путь:

```
ideco-client --get-csr /path/to/output.csr
```

- `/path/to/output.csr` - путь для сохранения файла CSR.

Для генерации CSR с указанием нового DN:

```
ideco-client --get-csr /path/to/output.csr --set-dn "CN=hostname-example,O=MyOrg"
```

Загрузка подписанного сертификата

После получения подписанного сертификата от удостоверяющего центра загрузите его в Ideco Client:

```
ideco-client --set-cert /path/to/certificate.pem
```

- `/path/to/certificate.pem` - путь к файлу подписанного сертификата.

Ideco Client проверит соответствие сертификата закрытому ключу, валидность полей (DN, KU, EKU, срок действия) и сохранит сертификат на устройстве. После этого подключение к Ideco NGFW Novum станет доступно.

Параметр `--set-dn` не может использоваться как отдельная команда - только совместно с `--get-csr`.

Режим EXTERNAL

В режиме EXTERNAL используется заранее подготовленный сертификат устройства и закрытый ключ. Администратор самостоятельно предоставляет оба файла. Ideco Client не генерирует закрытый ключ.

Для загрузки сертификата и ключа одним файлом:

```
ideco-client --set-cert /path/to/cert-and-key.pem
```

- `/path/to/cert-and-key.pem` - путь к файлу, содержащему сертификат и закрытый ключ.

Для загрузки сертификата и ключа разными файлами:

```
ideco-client --set-cert /path/to/certificate.pem --set-key /path/to/private-key.pem
```

- `/path/to/certificate.pem` - путь к файлу сертификата;
- `/path/to/private-key.pem` - путь к файлу закрытого ключа.

Ideco Client проверит:

- Соответствие закрытого ключа сертификату.
- Наличие непустого CN в DN сертификата.
- Отсутствие полей CA и server-auth в расширениях KU/EKU.
- Минимальную стойкость алгоритма (RSA-2048 и выше).

Параметр `--set-dn` не применим к режиму EXTERNAL. При переключении в режим EXTERNAL сохраненный DN не перезаписывается - он будет использован, если администратор вернется в режим AUTO или MANUAL.

В таблице приведено сравнение режимов управления сертификатами:

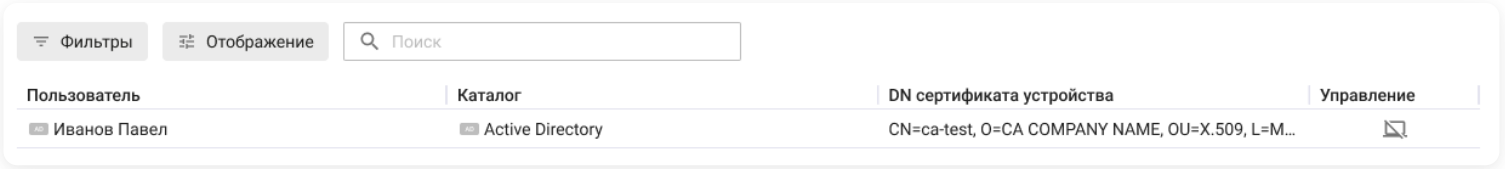
Действие	**AUTO**	**MANUAL**	**EXTERNAL**
Генерация закрытого ключа	Ideco Client	Ideco Client	Администратор
Подпись сертификата	Ideco NGFW Novum	Внешний удостоверяющий центр	Внешний удостоверяющий центр

Участие администратора	Не требуется	Передача CSR и загрузка сертификата	Загрузка ключа и сертификата
Подключение без сертификата	Сертификат выпускается при подключении	Недоступно	Недоступно

Порядок проверки сертификата устройства при подключении описан в статье Аутентификация по сертификату.

Привязанные устройства

В разделе **Пользователи** → **Ideco Client** → **Привязанные устройства** отображается список устройств, привязанных к пользователям. Привязка ограничивает доступ пользователя. После ее создания подключение возможно только с зафиксированного устройства:



Включение опции **Привязать устройство к пользователю** не создает записей в таблице. Записи появляются по мере того, как пользователи авторизуются.

Привязка создается автоматически при первой успешной авторизации пользователя, если:

- В настройках **Пользователи** → **Ideco Client** → **Основное** (для локального подключения без туннеля) или в правиле **Пользователи** → **VPN-подключения** → **Доступ по VPN** включена опция **Привязать устройство к пользователю**.
- Пользователь предоставил действительный сертификат устройства, подписанный доверенным CA.
- Для пользователя еще нет активной привязки.

Привязка не создается для пользователей и групп **Device VPN**.

Для удаления привязки нажмите в колонке **Управление**. Удаление необходимо, если пользователю нужно сменить устройство - новая привязка будет создана автоматически при следующем подключении.

После удаления привязки администратором она будет создана заново при следующей авторизации пользователя.

Если проверка привязки включена, а у пользователя нет привязанного устройства, доступ будет запрещен. При добавлении новых пользователей убедитесь, что для них создана привязка или проверка привязки отключена.

Установка и настройка Ideco Client на разных ОС

Классический контекст | Высокопроизводительный контекст

Поддерживаемые версии ОС и порты подключения

Поддерживаемые версии ОС	• Windows 10 22H2 и выше • macOS версии 13.4 и выше. При этом Ideco Client работает с некоторыми ограничениями • Astra Linux 1.7.0 и выше • РЕД ОС 8.0 и выше • Alt OS (Alt Workstation) 9.0 и выше • Fedora 35 и выше • Ubuntu 18.04 LTS (23.04) и выше
Порты для подключения, если NGFW Novum за NAT	• 80 TCP - используется для работы сертификатов Let's Encrypt • 443 TCP (по умолчанию), 14765 TCP (резервный) и 3051 UDP (для Wireguard) - используются Ideco Client

Возможности Ideco Client на разных ОС

Возможность	Описание	Windows	macOS	Linux
Установка	Установка клиента и службы (демона)	+	+	+
Настройка utm_address при установке	Позволяет настроить адрес сервера по умолчанию. Он будет использован при создании профиля	+		
Удаление	Удаление программы, но не профилей	+	+	+
Ручное обновление поверх	Ручная установка новой или предыдущей версии поверх существующей	+	+	+
Автообновление	Установка новой или предыдущей версии поверх существующей при подключении к NGFW Novum	+	+	+
Копирование профилей	Копирование профилей, если текущая версия меньше устанавливаемой и нет профилей в устанавливаемой версии	+	+	+
Редактирование профилей	Базовая функция	+	+	+
Постоянное хранение профилей в виде конфигурации	Базовая функция	+	+	+
Автоподключение к профилю при логине и запуску	Базовая функция	+	+	+
WireGuard	Подключение по протоколу WireGuard	+	+	+
TLS (443 порт)	Подключение по протоколу TLS	+	+	+
SSO профиль	Автосоздание профиля для SSO, если профилей нет	+	+	+
Device VPN	Подключение до входа пользователя в систему	+	+	+
Терминальный сервер	Поддержка работы терминальных серверов	+		
Балансировка Active-Active302 Редирект	Подключение к Ideco NGFW Novum по выданному балансировщиком адресу или другому серверу	+	+	+
Кастомная настройка	Кастомная настройка конфигурации Ideco Client: автосоздание профилей, запрет редактирования профилей и т.д.	+	+	+
Версия	Проверка актуальной версии Ideco Client	+	+	+
Ввод двухфакторной аутентификации	Показать окно ввода двухфакторной аутентификации при запросе от NGFW Novum и отправить введенный код на проверку	+	+	+

ZTNA. Данные ОС	Тип ОС	+	+	+
	Версия	+	+	+
	Домен	+	+	+
ZTNA. KB	Обновления Windows	+		
ZTNA. Registry	Данные реестра Windows	+		
ZTNA. Services	Проверка запущенных служб Windows	+		
ZTNA. Process	Проверка запущенных процессов	+	+	+
ZTNA. Межсетевой экран	Проверка Межсетевым экраном	+		
ZTNA. Антивирус	Проверка Антивирусами	+	+	

Работа в headless-системах

При необходимости Ideco Client можно запустить в консольном режиме с помощью команды `--console`. В этом случае GUI не отображается, а все команды передаются через командную строку.

На Linux консольный режим активируется автоматически при отсутствии графического интерфейса. На Windows и macOS только вручную.

Межсетевой экран

Windows

Вендор	Продукт
Microsoft	Windows Firewall

Антивирус

Windows

Вендор	Продукт
Microsoft	Windows Defender
Kaspersky Lab	• Kaspersky Free • Kaspersky Endpoint Security Все остальные продукты Kaspersky Lab по умолчанию определяются как Kaspersky Free.
Dr.Web	Dr.Web Security Space
Comodo	Comodo Internet Security

---

macOS

Вендор	Продукт
Kaspersky Lab	• Kaspersky Small Office Security • Kaspersky Endpoint Security • Kaspersky Internet Security
DrWeb	Dr.Web для macOS

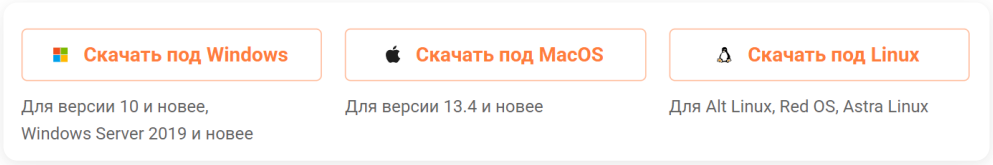
Установка и настройка Ideco Client на Windows

Классический контекст | Высокопроизводительный контекст

Скачивание

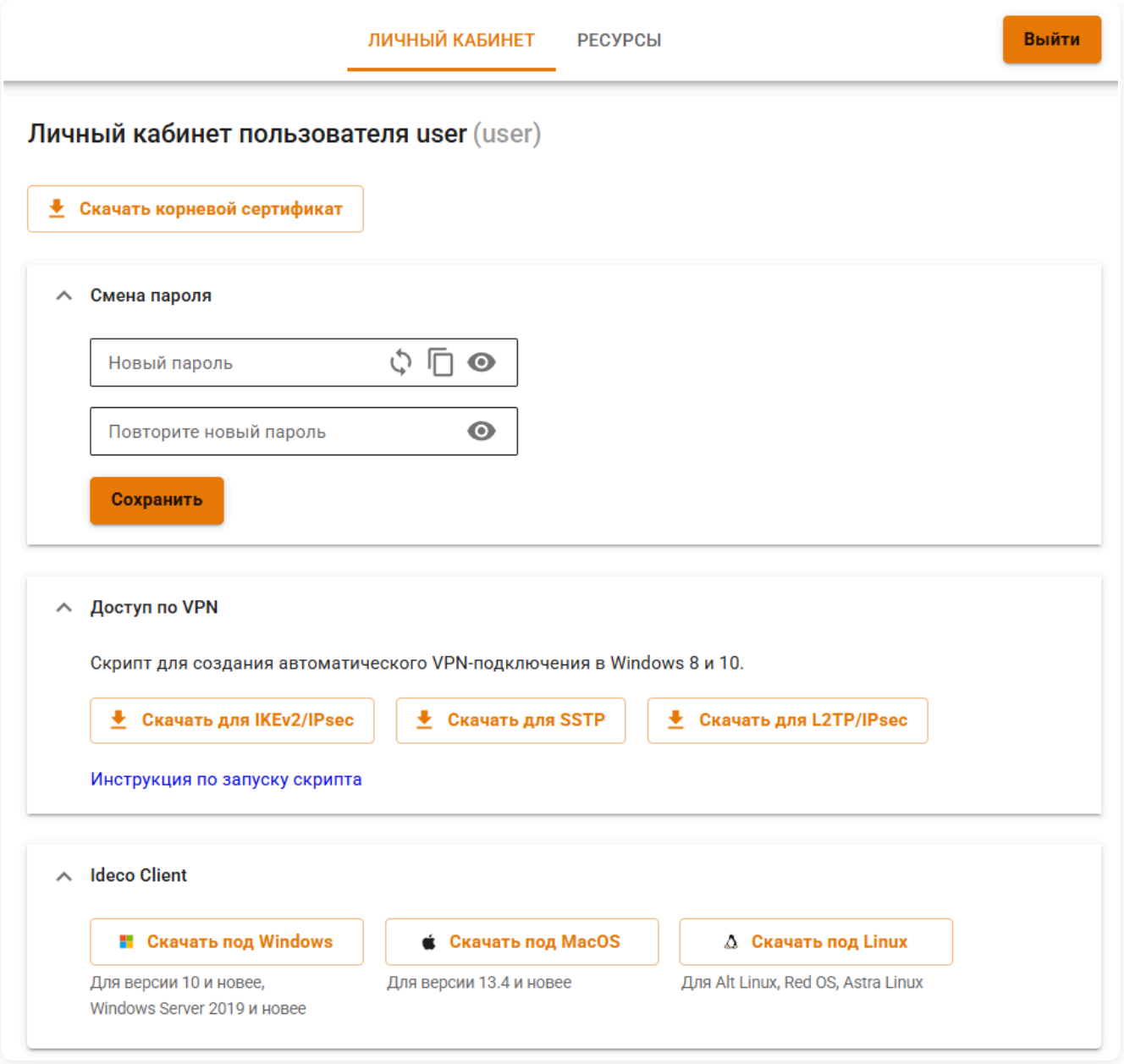
Для администратора

Перейдите в **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Windows** или скачайте по **ссылке**:



Для пользователя

Нажмите на кнопку **Скачать под Windows** в личном кабинете пользователя или скачайте по **ссылке**:



Установка

Сохраните и запустите файл установки `IdecoClient.msi`.

Чтобы заранее задать адрес подключения к Ideco NGFW Novum, запустите установщик с ключом `utm_address` из командной строки:

1. Перейдите в директорию с файлом `cd [путь до файла]`.

2. Откройте файл `IdecoClient.msi` с ключом `utm_address`.

3. Укажите адрес Ideco NGFW Novum (команда: `IdecoClient.msi utm_address=адрес_ngfw`).

Результат зависит от того, входит ли компьютер в домен:

- **Компьютер в домене** - после установки автоматически создается профиль с учетной записью пользователя, под которой выполнялась установка, и с адресом из ключа `utm_address`.
- **Компьютер не в домене** - при создании нового профиля поле с адресом будет автоматически заполнено значением из ключа `utm_address`.

Чтобы оптимизировать процесс установки Ideco Client с помощью GPO, создайте файл трансформации `.mst` с адресом Ideco NGFW Novum и примените его при установке. Для этого воспользуйтесь утилитой Orca.

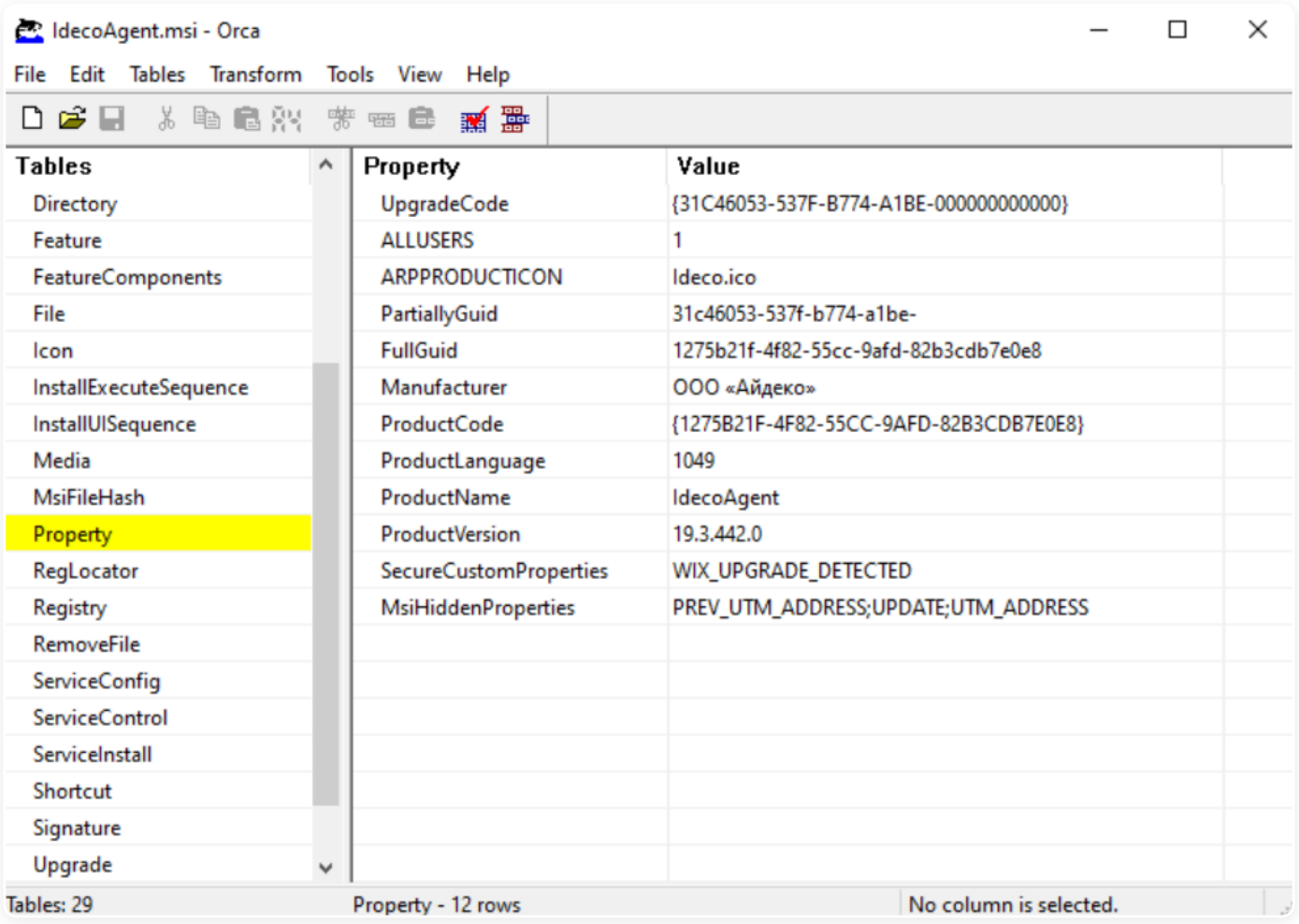
Как создать файл трансформации .mst в Orca

1. Запустите Orca.

2. Нажмите **File** → **Open** и откройте `IdecoClient.msi`.

3. Нажмите **Transform** → **New Transform** для создания файла трансформации. Все дальнейшие изменения будут сохранены в `.mst`-файл, а `IdecoClient.msi` останется неизменным.

4. В дереве таблиц найдите **Property**:



5. Нажмите **Tables** → **Add Row**, чтобы добавить новую запись.

6. В поле **Property** введите `UTM_ADDRESS`, а в поле **Value** - IP-адрес или FQDN Ideco NGFW Novum. Нажмите **Ок**.

7. Нажмите **Transform** → **Generate Transform** и сохраните файл, например `IdecoClient.mst`.

8. Закройте Orca.

При установке через GPO укажите созданный `.mst`-файл в качестве transform-файла для `IdecoClient.msi`. В этом случае Ideco Client будет установлен с уже заполненным полем **Хост**.

Если Kaspersky Plus блокирует установку и обновление

1. Откройте **Настройки** → **Настройки безопасности** → **Исключения и действия с найденными объектами** → **Указать доверенные приложения**:

2. Нажмите **Добавить**, выберите скачанный msi-файл Ideco Client и нажмите **Выбрать**:

3. Включите опции в **Исключения для приложения**:

4. Нажмите **ОК** и не закрывайте окно **Доверенные приложения**.

5. Установите Ideco Client.

6. Нажмите **Добавить** и добавьте файлы `idecoclient.exe` и `idecoservice.exe`. В **Исключения для приложения** укажите опции как в пункте 3:

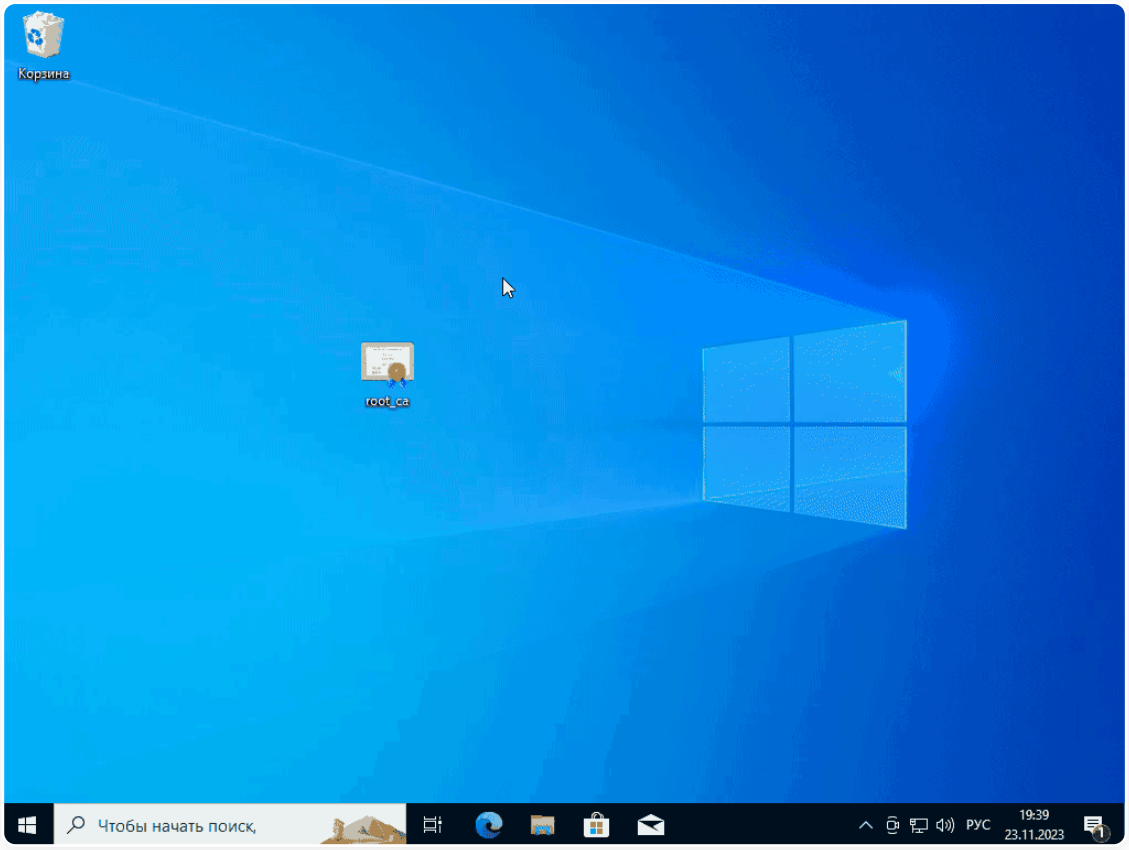
7. Откройте **Настройки** → **Настройки безопасности** → **Настройки сети** и настройте раздел:

8. Нажмите **Сохранить**.

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW Novum по внешнему IP-адресу или доменному имени без сертификата Let’s Encrypt, импортируйте корневой сертификат Ideco NGFW Novum на компьютер.

Для импорта сертификата на компьютер выполните действия:



1. Дважды кликните на скачанный файл сертификата.

2. В открывшемся окне выберите **Установить сертификат**.

3. Откроется **Мастер импорта сертификатов**. В качестве **Расположения хранилища** выберите **Локальный компьютер**.

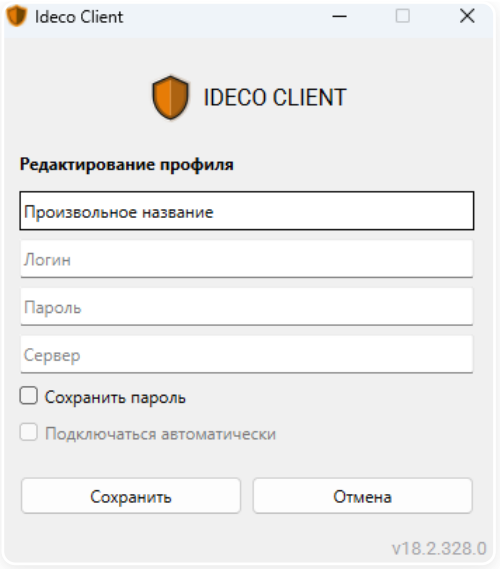
4. Выберите пункт **Поместить все сертификаты в следующее хранилище**, нажмите **Обзор** и выберите папку **Доверенные корневые центры сертификации**.

5. Нажмите **Ок** → **Далее** → **Готово**.

Первый запуск

1. Запустите Ideco Client.

2. Введите данные:



- **Название профиля** - введите произвольное название профиля, который будет доступен для выбора при подключении. Может не совпадать с логином.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Адрес сервера** - укажите логин и адрес сервера. Чтобы использовать резервный порт 14765, адрес необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`). Варианты в зависимости от конфигурации:

NGFW Novum введен в один домен

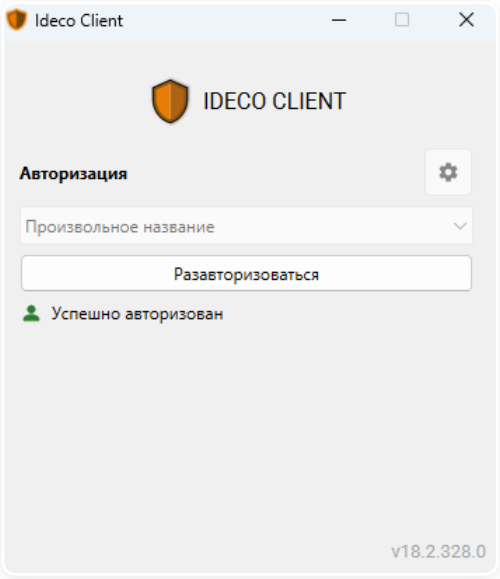
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:

NGFW Novum введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW Novum**:

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Редактирование профиля

1. Перейдите в раздел **Настройки**, нажав  .

2. Выберите профиль для редактирования, нажав  , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

Полезные ссылки

- **Кастомная настройка Ideco Client**
- **Как включить режим отладки для Ideco Client**

Установка и настройка Ideco Client на macOS

Классический контекст | Высокопроизводительный контекст

Особенности работы Ideco Client на macOS

- Ideco Client для macOS требует версии системы 13.4 и выше.
- HIP-профили на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

- ОС
- Процесс
- Антивирус (Kaspersky)

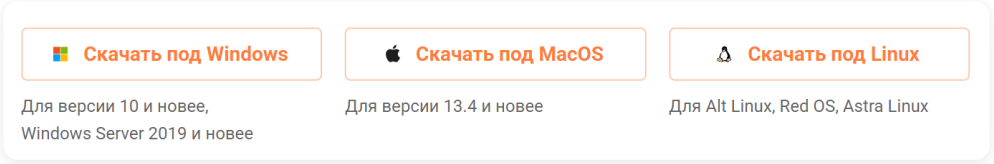
Недоступные HIP-профили

- Домен
- Межсетевой экран
- Реестр (всегда только Windows)
- Службы (всегда только Windows)
- Пакет обновлений Knowledge Base (всегда только Windows)

Скачивание

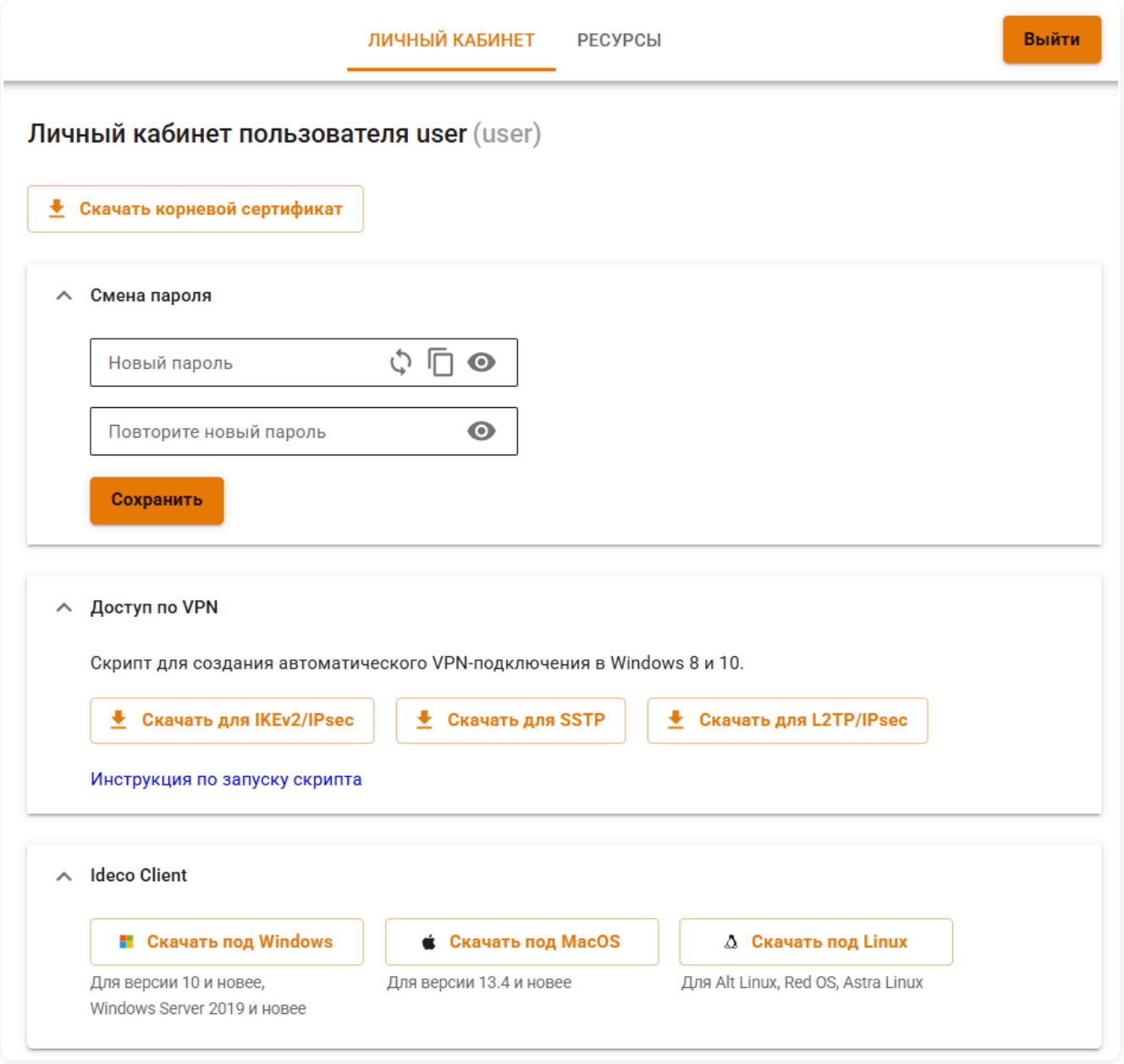
Для администратора

Перейдите в **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под macOS** или скачайте по **ссылке**:



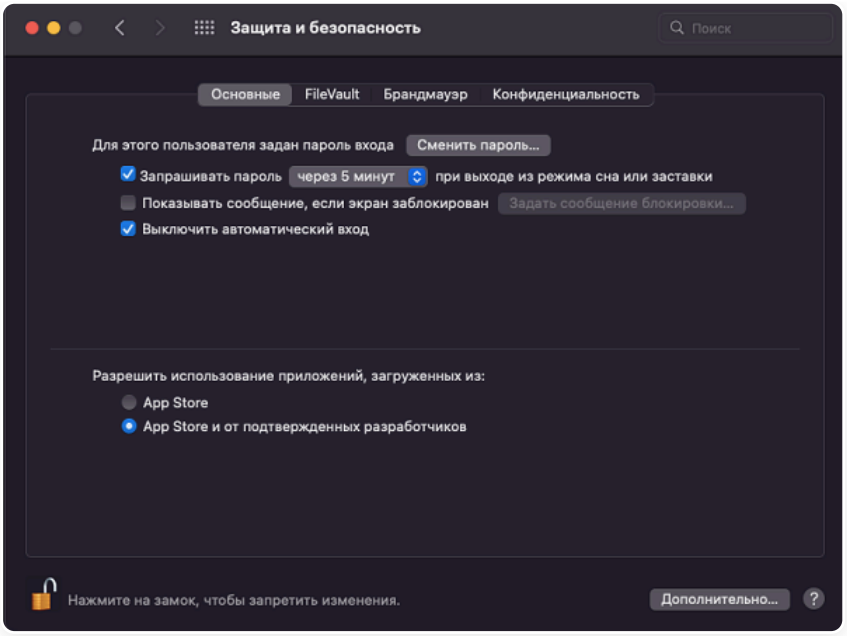
Для пользователя

Нажмите кнопку **Скачать под macOS** или скачайте по **ссылке**:



Установка

В некоторых версиях macOS необходимо явно разрешить установку приложения не из App Store. Для этого перейдите в **Защита и безопасность** → **Основные** и разрешите использование приложений, загруженных из **App Store и от подтвержденных разработчиков**:

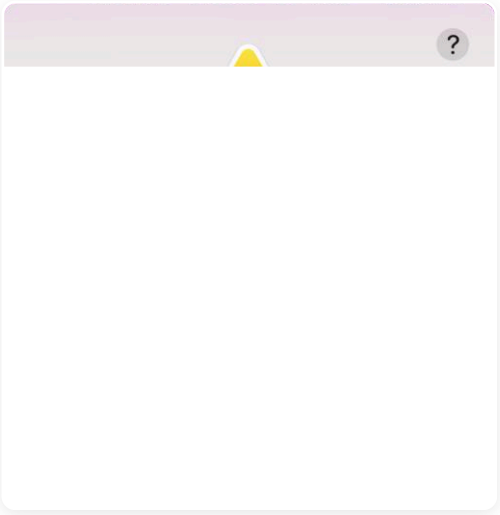


Чтобы установить **Ideco Client** на macOS, выполните действия:

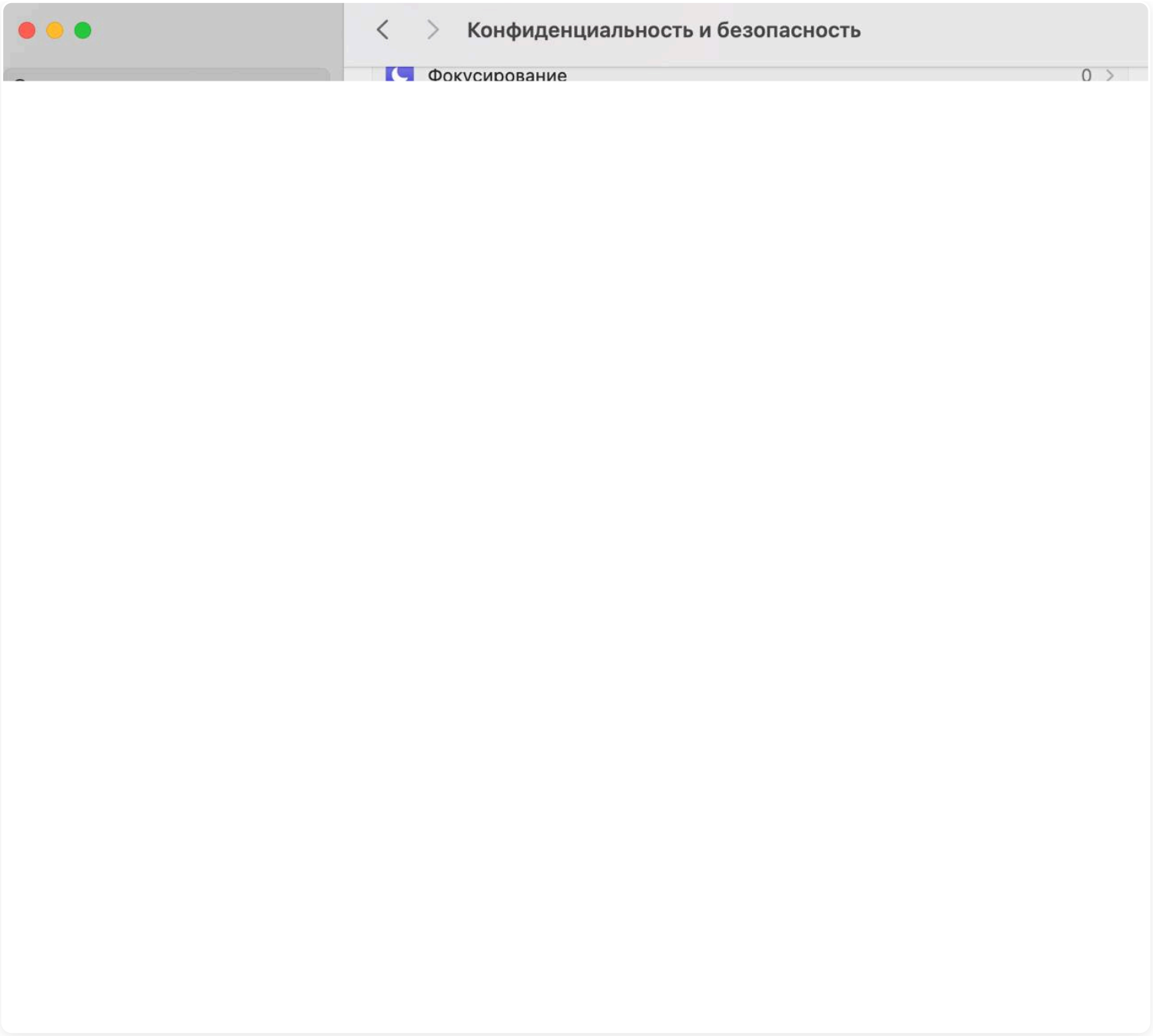
1. Нажмите по файлу **IdecoClient.pkg** правой кнопкой мыши и выберите **Открыть**.

macOS Sequoia

1. При открытии файла **IdecoClient.pkg** система сообщит о потенциальной опасности приложения. Нажмите **Готово**:



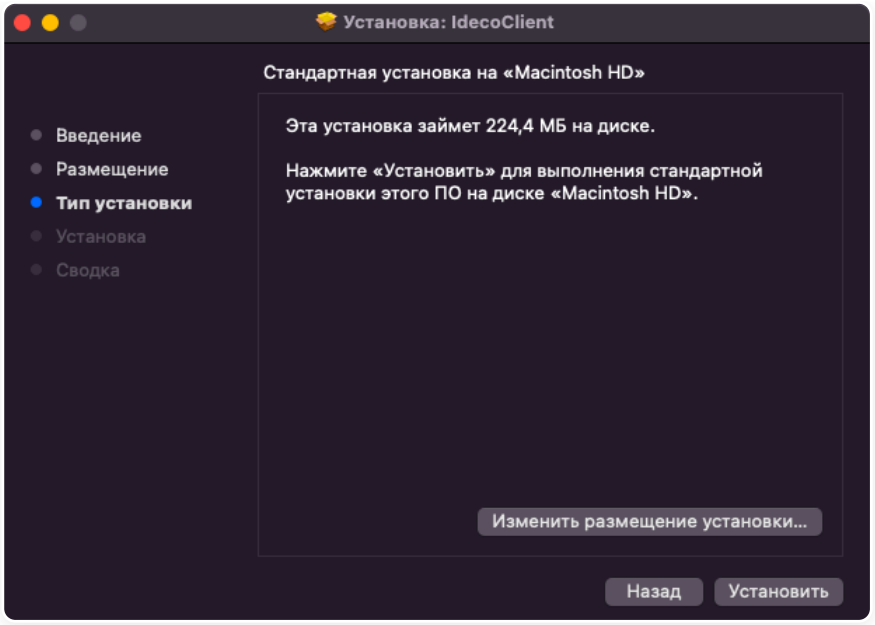
2. Перейдите в раздел **Конфиденциальность и безопасность** и нажмите **Все равно открыть** рядом с именем файла:



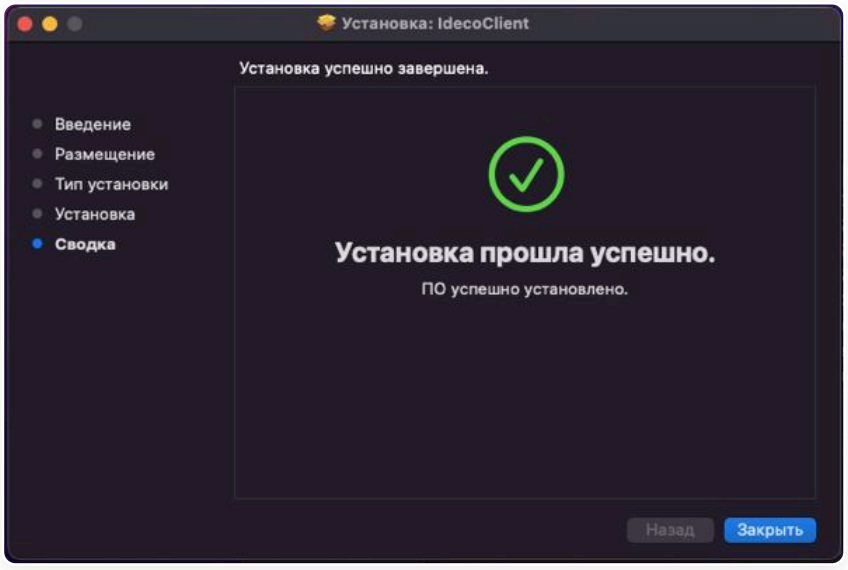
macOS Monterey и macOS Sonoma

При открытии файла **IdecoClient.pkg** система выдаст предупреждение. Подтвердите действие:

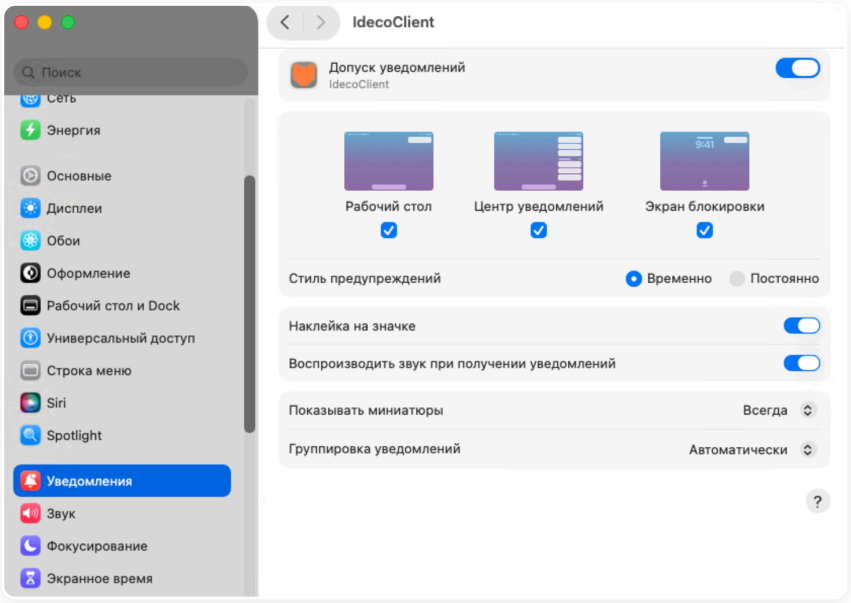
2. Нажмите **Продолжить**. В открывшемся окне нажмите **Установить**:



3. Если установка завершилась успешно, на экране появится соответствующее сообщение:



При первой установке Ideco Client система запросит разрешение на показ уведомлений. Если не дать согласие или проигнорировать запрос, уведомления будут отключены. Включить уведомления можно, установив необходимые разрешения в **Системные настройки** → **Уведомления** → **IdecoClient**:



Настройка профиля для первого запуска

Перед подключением к Ideco NGFW Novum по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt убедитесь, что срок действия оконечного сертификата на домен или IP-адрес составляет не более 825 дней. Если это так, то импортируйте **корневой** сертификат Ideco NGFW Novum на компьютер. Если срок действия оконечного сертификата на домен или IP-адрес превышает 825 дней, загрузите на NGFW Novum свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

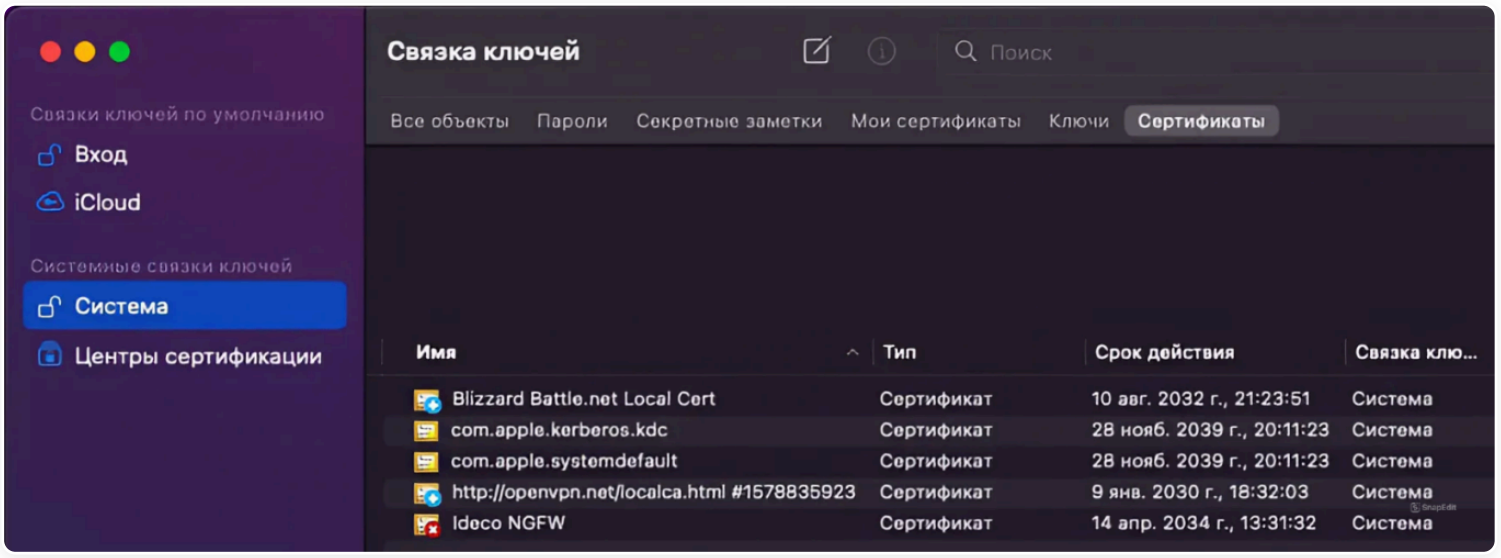
Установка корневого сертификата Ideco NGFW Novum на macOS

Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

> **Не храните** файл сертификата в директориях **Desktop**, **Documents** и **Downloads**: в этом случае Ideco Client не сможет прочитать и получить доступ к этим файлам. Рекомендуем сохранить файлы в другую директорию, например, в корневую директорию домашней папки пользователя.

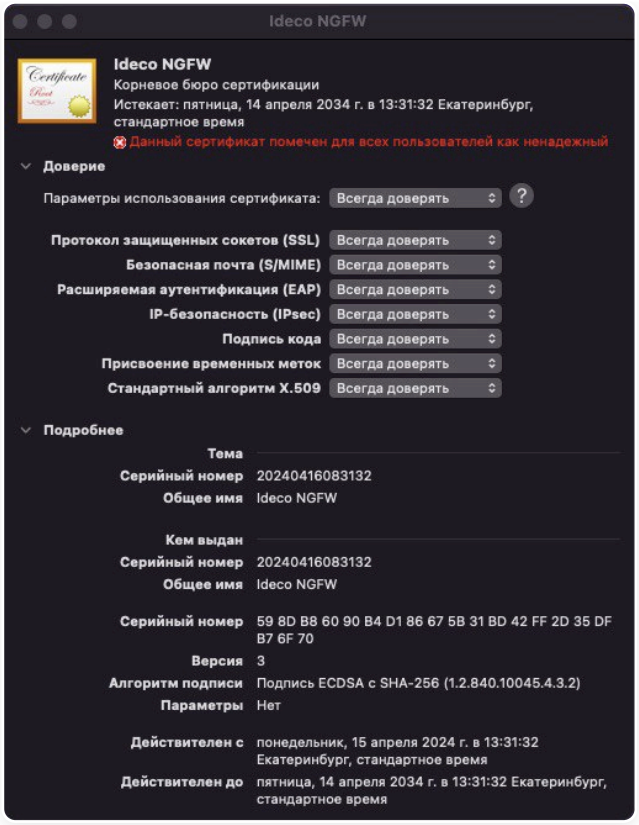
Установка через Связку ключей

1. Откройте скачанный файл **root_ca.crt** в приложении **Связка ключей**, сертификат Ideco NGFW Novum появится в папке **Система**:

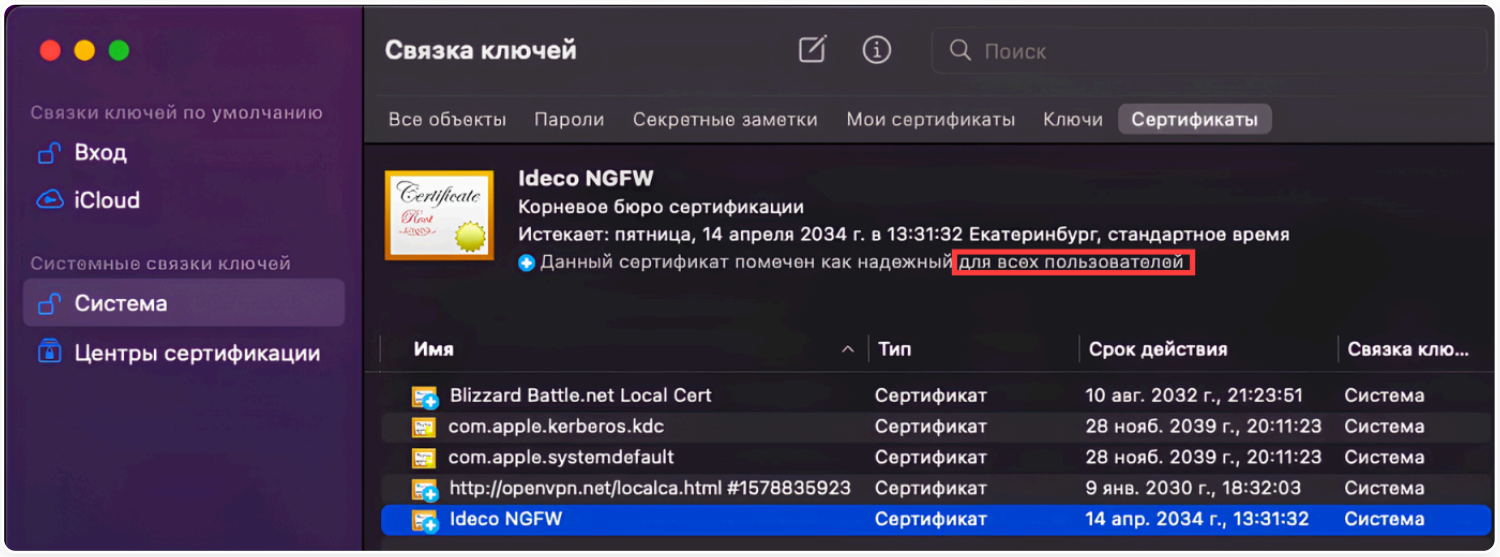


2. Нажмите по сертификату правой кнопкой мыши и выберите **Свойства**.

3. Установите в поле **Параметры использования сертификата** действие **Всегда доверять**:



4. Закройте окно свойств сертификата. Теперь сертификат помечен как надежный **для всех пользователей** устройства:



Сертификат должен быть установлен **для всех пользователей**.

Если сертификат установлен неправильно, то будет только для текущего пользователя. В этом случае проверьте корректность установки сертификата.

5. Перезагрузите компьютер.

Установка через терминал

1. Чтобы добавить корневые сертификаты в список доверенных, выполните в терминале команду:

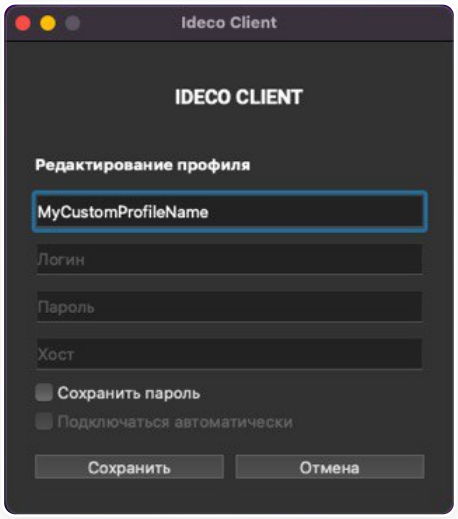
```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <путь к сертификату>/root_ca.crt
```

2. Перезагрузите компьютер.

Первый запуск

1. Запустите Ideco Client.

2. Введите данные:



- **Имя профиля** - может не совпадать с логином и будет использоваться при выборе профиля для авторизации.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Хост** - укажите логин и хост. Чтобы использовать резервный порт 14765, адрес сервера необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`). Варианты в зависимости от конфигурации:

NGFW Novum введен в один домен

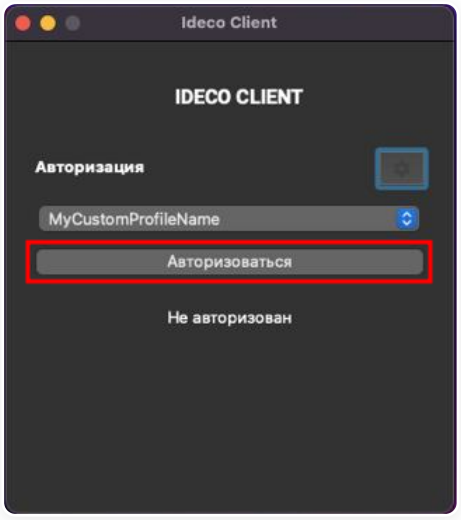
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:

NGFW Novum введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW Novum**:

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Редактирование профиля

1. Перейдите в раздел **Настройки**, нажав по  .

2. Выберите профиль для редактирования, нажав  , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

Установка и настройка Ideco Client на Linux

Классический контекст | Высокопроизводительный контекст

Особенности работы Ideco Client на Linux

- Ideco Client гарантированно работает на Alt Linux, РЕД ОС, Astra Linux, Fedora, Ubuntu. Для остальных дистрибутивов работа не гарантируется.
- HIP-профили на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

- ОС
- Процесс

Недоступные HIP-профили

- Антивирус
- Домен
- Межсетевой экран
- Реестр (всегда только Windows)
- Службы (всегда только Windows)
- Пакет обновлений Knowledge Base (всегда только Windows)

- Для проверки запуска процесса с заданным именем в системе (ZTNA) используется функция:

```
bool os_specific::isProcessExist(const std::string &processName)
```

Длина строки `processName` составляет не более 15 символов. Если название процесса длиннее, то название будет обрезано до максимально доступного числа символов. В этом случае проверка не будет выполнена корректно.

Скачивание

Для администратора

Перейдите в **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Linux** или скачайте по **ссылке**:

Для пользователя

Перейдите в личный кабинет пользователя и нажмите **Скачать под Linux** или скачайте по **ссылке**:

Установка

Для установки Ideco Client на Linux выполните действия:

1. Перейдите в папку со скачанным файлом установки Ideco Client:

```
cd "Путь до директории с установочным файлом"
```

2. Предоставьте файлу разрешение на исполнение, выполнив в терминале команду:

```
chmod +x IdecoClient.sh
```

3. Запустите файл установки Ideco Client:

```
./IdecoClient.sh
```

4. После установки проверьте статус службы IdecoService, выполнив команду:

```
systemctl status IdecoService.service
```

5. Убедитесь, что служба IdecoService запущена и работает:



Для добавления службы в автозагрузку выполните команду:

```
systemctl enable IdecoService.service
```

Для корректной работы Ideco Client:

Astra Linux

1. Проверьте, что установлен пакет `libnss-resolve`. Если нет, установите командой:

```
sudo apt-get install libnss-resolve
```

2. Для резолвинга имен используйте:

```
getent hosts доменное_имя
```

либо

```
resolvectl query доменное_имя
```

Alt Linux

Требуется пакет `systemd-networkd`. Установите командами:

```
sudo apt-get update
sudo apt-get install systemd-networkd
```

Fedora

При использовании SELinux в системе должны быть установлены и доступны в `PATH` утилиты:

- `getenforce`
- `semanage`
- `restorecon`

Команда для установки:

```
sudo dnf install libselinux-utils policycoreutils policycoreutils-python-utils
```

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW Novum по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt убедитесь, что срок действия сертификата на этот домен или IP-адрес составляет не более 825 дней. Если это так, то импортируйте **корневой** сертификат Ideco NGFW Novum на компьютер. Если срок действия сертификата на этот домен или IP-адрес превышает 825 дней, загрузите на NGFW Novum свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

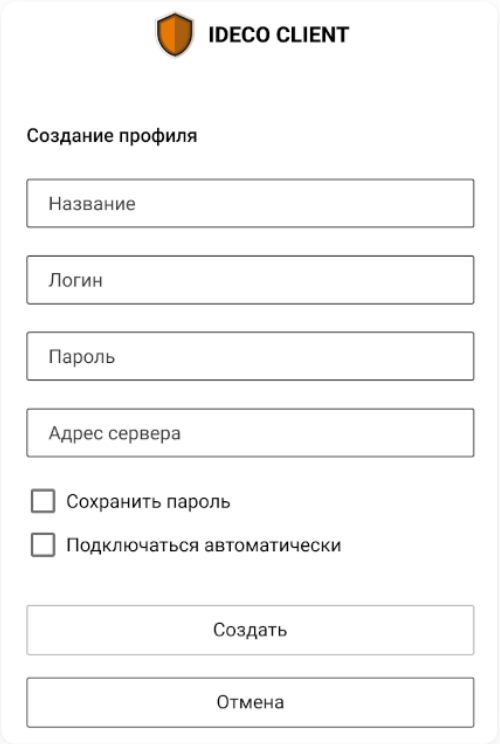
Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

Первый запуск

1. Запустите Ideco Client.

2. Введите данные:



- **Имя профиля** - может не совпадать с логином и будет использоваться при выборе профиля для авторизации.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Адрес сервера** - укажите логин и адрес сервера. Чтобы использовать резервный порт 14765, адрес необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`). Варианты в зависимости от конфигурации:

NGFW Novum введен в один домен

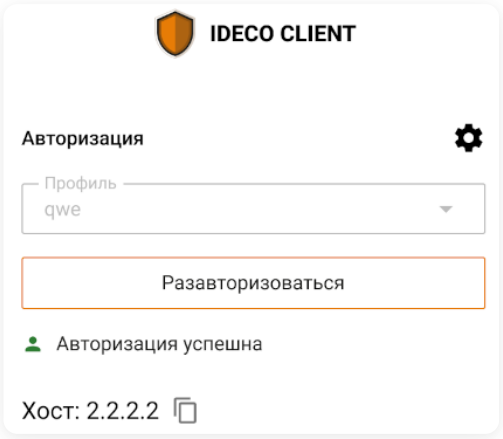
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес.

NGFW Novum введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW Novum**.

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



Статусы подключения в Ideco Client

При установке соединения Ideco Client последовательно отображает статусы, позволяющие отслеживать этапы подключения:

1. **Подключение (Connecting)** - инициализация соединения с сервером.

2. **Авторизация (Authorization)** - проверка имени пользователя и пароля.

3. **Проверка второго фактора (2FA checking)** - подтверждение аутентификации с помощью проверки второго фактора.

4. **Запрошен сертификат для устройства (Device certificate requested)** - отправка запроса на получение сертификата устройства.

5. **Проверка сертификата (Certificate verification)** - проверка сертификата устройства.

6. **Создание туннеля (Creating a tunnel)** - установка зашифрованного канала.

7. **Соединение установлено (Connection established)** - успешное подключение.

Подключение может быть заблокировано с сообщениями:

- **Требуется ручная установка сертификата (Manual certificate installation pending)** - на этапе **Подключение (Connecting)**, если ранее был отправлен запрос на подпись сертификата (CSR), но подписанный сертификат не был установлен на устройство. Подключение невозможно до завершения установки сертификата.
- **Действительный сертификат отсутствует (No valid certificate)** - на этапе **Проверка сертификата (Certificate verification)**, если сертификат устройства истек или не прошел проверку, а также при рассинхронизации времени между компьютером с Ideco Client и Ideco NGFW Novum (сертификат может считаться еще не вступившим в силу или просроченным). Убедитесь, что время на устройстве совпадает со временем сервера.

Редактирование профиля

1. Перейдите в раздел **Настройки**, кликнув по .

2. Выберите профиль для редактирования, нажав , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

Удаление

1. Перейдите в каталог, в котором установлен Ideco Client:

```
cd /usr/local/Ideco/Agent/<версия Ideco NGFW Novum>
```

2. Запустите файл удаления Ideco Client:

```
./uninstall.sh
```

Кастомная настройка Ideco Client

Классический контекст | Высокопроизводительный контекст

Для авторизации пользователей Ideco Client использует профили, состоящие из логина и пароля. По умолчанию пользователь может создавать, удалять, редактировать профили и сохранять пароль для автоматической авторизации. Кастомная настройка позволит администратору создавать готовые конфигурации, а также ограничить права пользователей на управление профилями.

Возможности кастомной настройки

- [x] Запрет на создание новых профилей
- [x] Запрет на сохранение пароля
- [x] Запрет на редактирование профиля
- [x] Установка профиля по умолчанию
- [x] Автоматическое подключение выбранного профиля при запуске Ideco Client

Параметры файла конфигурации

Файл конфигурации создается администратором на пользовательской машине в формате .json, устанавливается через командную строку/терминал и поддерживает два типа профилей:

- Password - пользователь подключается по логину и паролю (только для Windows).
- SSO - пользователь для подключения использует данные системы.

Пример файла конфигурации, в котором заданы Password-профиль и SSO-профиль:

Пример файла конфигурации

```
{
    "profiles":
    [

        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90a0ac6",
            "source": "json",
            "name": "some string name 1",
            "data":
            {
                "login": "user1",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options":
            {
                "autoselect": true,
                "autoconnect": false,
                "read_only": false
            }
        },

        {
            "name": "some string name sso",
            "source": "json",
            "data":
            {
                "type": "sso",
                "server": "google.ru"
            },
            "profile_options":
```

```
            {
                "autoselect": false,
                "autoconnect": false,
                "read_only": false
            }
        }
    ],
    "gui_client_options":
    {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

Описание настроек конфигурационного файла

- `"profiles"` - обязательное поле, без него конфигурация не будет работать;
- `"id"` - необязательный идентификатор профиля, используемый для привязки пользовательских данных (например, логина) к конкретному конфигурационному профилю. При отсутствии `"id"` профиль генерируется автоматически. При указании вручную формат должен соответствовать UUID, иначе профиль может быть проигнорирован без отображения ошибки. Только для Password;
- `"source": "json"` - обязательное поле для всех типов профилей;
- `"name"` - уникальное название профиля;
- `"data"` - содержит данные для каждого типа профиля:
  - `"login"` - логин пользователя. Только для Password;
  - `"type"` - определяет тип профиля: Password или SSO;
  - `"server"` - адрес сервера. Для всех типов профилей. Если необходим резервный порт 14765, укажите адрес в формате `домен:14765` или `IP:14765` (например, `server.com:14765`).
- `"profile_options"` - настройки профиля:
  - `"autoselect"` - отвечает за установку профиля по умолчанию:
    - `true` - профиль будет выбран в качестве профиля по умолчанию при запуске Ideco Client;
    - `false` - профиль не выбран в качестве профиля по умолчанию.
  - `"autoconnect"` - отвечает за автоподключение профиля при запуске Ideco Client:
    - `true` - профиль будет автоматически подключаться при запуске Ideco Client;
    - `false` - профиль не будет автоматически подключаться при запуске Ideco Client.
  - `"read_only"` - отвечает за то, может ли пользователь редактировать или удалять профиль:
    - `true` - профиль нельзя редактировать или удалять;
    - `false` - профиль можно редактировать или удалять.
- `"gui_client_options"` - обязательное поле. Управляет поведением графического интерфейса:
  - `"deny_save_profile_password"` - разрешает или запрещает сохранение пароля:
    - `true` - пользователь не сможет сохранить пароль. Ideco Client будет запрашивать пароль при каждом подключении;
    - `false` - пользователь может сохранять пароль в Ideco Client.
  - `"deny_create_profiles"` - разрешает или запрещает создание новых профилей:
    - `true` - пользователь может создавать новые профили в Ideco Client;
    - `false` - пользователь не сможет создавать новые профили в Ideco Client.

Особенности работы профилей:

Password

- Если логин пользователя задан в файле конфигурации в поле `"login"`, то значение логина пользователя будет отображаться в поле **Логин** в Ideco Client.
- Если `"deny_save_profile_password": true`, то автоподключение должно быть запрещено `"autoconnect": false`, так как пароли не хранятся.
- Если `"deny_save_profile_password": true` и `"autoconnect": true`, то служба отклонит конфигурацию и запишет ошибку в логи.
- Если у нескольких профилей будет задан параметр автовыбора `"autoselect": true`, то выбран будет самый нижний профиль в файле конфигурации.
- Связывание пользовательских данных с файлом конфигурации осуществляется по `"id"` пользователя.

SSO

- Для SSO-профиля `"login"` отсутствует в файле конфигурации и поле Логин не отображается в интерфейсе Ideco Client, поскольку аутентификация выполняется автоматически с использованием учетной записи операционной системы.
- Параметры SSO-профиля задаются администратором и не могут быть изменены пользователем.
- Автоподключение возможно `"autoconnect": true`, так как аутентификация не требует ввода пароля.

- Если службе не удается выполнить аутентификацию, то в логи будет записана ошибка, а пользователю - выведено соответствующее уведомление.
- Связывание профиля с учетной записью пользователя выполняется на основе механизма SSO, без сохранения паролей.

Применение файла конфигурации

1. Создайте .json файл на машине пользователя.

2. Задайте необходимую конфигурацию.

3. Завершите все процессы Ideco Client. Это необходимо для корректного запуска с новыми настройками.

4. Установите конфигурацию.

> Путь к .json файлу конфигурации должен быть абсолютным. Например: C:\Program Files\Ideco\test.json

Windows

Откройте командную строку от имени администратора и выполните команду:

```
IdecoClient.exe --set-json-config="путь_до_файла_конфигурации"
```

Linux или macOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --set-json-config="путь_до_файла_конфигурации"
```

---

5. Ideco Client выполнит анализ файла:

- Если нет ошибок - сохранит в реестре данные файла конфигурации.
- Если есть ошибки - отправит в лог службы список ошибок.

Возможные причины ошибок

- Файл недоступен для чтения.
- Файл конфигурации пустой.
- Размер файла превышает 1 Мб.
- Файл содержит неопознанные параметры, например опечатки.
- В файле отсутствуют обязательные поля `"profiles"` и `"gui_client_options"`.
- Более одного профиля имеет опцию автовыбора `"autoselect": true`.
- Более одного профиля имеет опцию автоподключения `"autoconnect": true`.
- Если профиль имеет опцию автоподключения `"autoconnect": true`, но не имеет опции автовыбора `"autoselect": true`.
- В файле конфигурации в рамках Password-профиля указано `"deny_save_profile_password": true` и `"autoconnect": true`.
- Поля `"name"` или `"id"` не уникальны.
- Устройство пользователя не введено в домен, при этом в файле конфигурации прописан SSO-профиль.
- Заполнено поле `"id"` для SSO-профиля.

Работа с конфигурацией

Получить и вывести конфигурацию в консоль:

Windows

Откройте командную строку с правами администратора и выполните команду:

```
IdecoClient.exe --print-json-config True
```

Linux или macOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --print-json-config True
```

Удалить конфигурацию:

Windows

Откройте командную строку с правами администратора и выполните команду:

```
IdecoClient.exe --reset-json-config
```

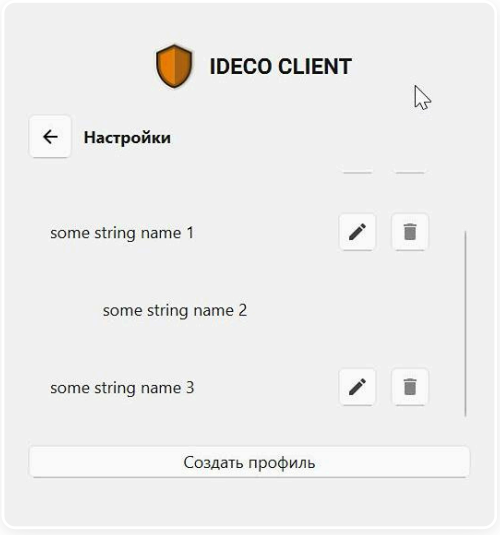
Linux или macOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --reset-json-config
```

Примеры настроек файла конфигурации

Запретить пользователю редактировать преднастроенный профиль



Профиль `some string name 2` создан в файле конфигурации и профиль запрещено редактировать или удалять, так как у него стоит настройка `"read_only": true`.

Профили `some string name 1` и `some string name 3` созданы пользователем самостоятельно, которые можно редактировать или удалять.

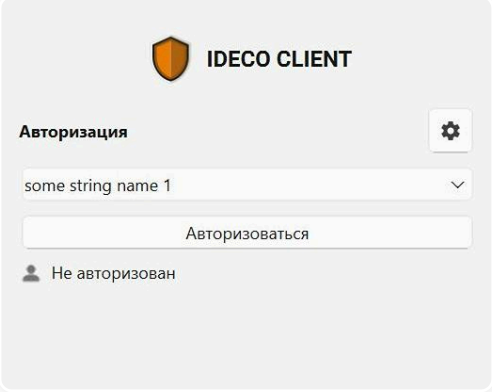
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
```

```
                "autoconnect": false,
                "read_only": true
            }
        }
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса:
  - `"deny_save_profile_password": false` - так как `false`, то пользователь может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": false` - так как `false`, то пользователь может вручную создавать новые профили в Ideco Client.

Задать профиль, который будет выбран по умолчанию при запуске Ideco Client

Файл конфигурации содержит два профиля `some string name 1` и `some string name 2`. Чтобы профилем по умолчанию был выбран `some string name 1`, в файле конфигурации у данного профиля, необходимо указать `"autoselect": true`.



Настройка файла конфигурации:

```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        },

        {
            "id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7",
```

```
            "source": "json",
            "name": "some string name 1",
            "data":
            {
                "login": "user1",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options":
            {
                "autoselect": true,
                "autoconnect": false,
                "read_only": true
            }
        }
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 1"` - название профиля `some string name 1`;
- `"data":` - содержит данные профиля:
  - `"login": "user1"` - логин пользователя `user1`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": true` - так как `true`, профиль будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса:
  - `"deny_save_profile_password": false` - так как `false`, то пользователь может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": false` - так как `false`, то пользователь может вручную создавать новые профили в Ideco Client.

Создать три профиля, которые нельзя изменить или удалить. Запретить создавать новые профили

Файл конфигурации содержит три профиля `some string name 1`, `some string name 2`, `some string name 3`. Чтобы их нельзя было отредактировать или удалить, всем профилям необходимо указать `"read_only": true`.
Чтобы запретить пользователю создавать новые профили необходимо указать: `"deny_create_profiles": true`.



Настройка файла конфигурации:

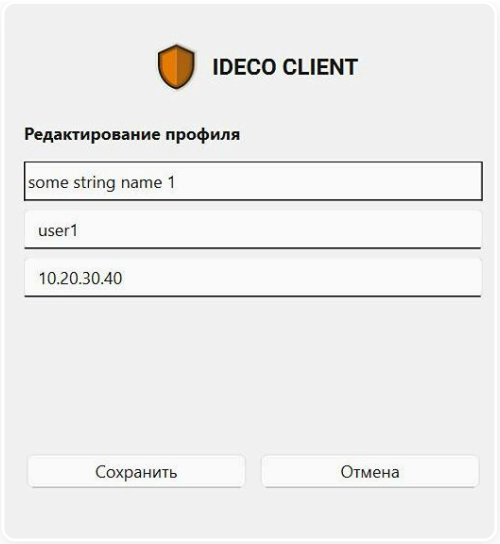
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        },

        {
            "id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7",
            "source": "json",
            "name": "some string name 1",
            "data":
            {
                "login": "user1",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options":
            {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        },

        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7asd4123",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": true
            }
        }
```

```
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": true
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"id": "a78cb502-f0d5-4ce5-84ab-a127a90a0ac7"` - уникальный идентификатор профиля;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 1"` - название профиля `some string name 1`;
- `"data":` - содержит данные профиля:
  - `"login": "user1"` - логин пользователя `user1`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7asd4123"` - уникальный идентификатор профиля;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 1"` - название профиля `some string name 1`;
- `"data":` - содержит данные профиля:
  - `"login": "user1"` - логин пользователя `user1`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": true` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса:
  - `"deny_save_profile_password": false` - так как `false`, то пользователь может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": true` - так как `true`, то пользователь не сможет создавать новые профили в Ideco Client.

Запретить сохранять пароль. Ideco Client будет запрашивать пароль при каждом подключении

Чтобы запретить пользователю сохранять пароль в Ideco Client, необходимо в файле конфигурации указать `"deny_save_profile_password": true`.



Настройка файла конфигурации:

```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "profile_options": {
                "autoselect": false,
                "autoconnect": false,
                "read_only": false
            }
        }
    ],
    "gui_client_options": {
        "deny_save_profile_password": true,
        "deny_create_profiles": false
    }
}
```

- `"profiles":` - обязательное поле, без него конфигурация не будет работать;
- `"id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6"` - уникальный идентификатор профиля. Только для Password;
- `"source": "json"` - обязательное поле, без него конфигурация не будет работать;
- `"name": "some string name 2"` - название профиля `some string name 2`;
- `"data":` - содержит данные профиля:
  - `"login": "user2"` - логин пользователя `user2`;
  - `"type": "password"` - тип профиля Password;
  - `"server": "10.20.30.40"` - IP-адрес сервера Ideco NGFW Novum.
- `"profile_options":` - настройки профиля:
  - `"autoselect": false` - так как `false`, профиль не будет профилем по умолчанию;
  - `"autoconnect": false` - так как `false`, профиль не будет подключаться автоматически при запуске Ideco Client;
  - `"read_only": false` - так как `true`, запрещает редактировать и удалять профиль.
- `"gui_client_options":` - управляет поведением графического интерфейса;
  - `"deny_save_profile_password": true` - так как `true`, то пользователь не может сохранять пароль в Ideco Client;
  - `"deny_create_profiles": false` - так как `false`, то пользователь может вручную создавать новые профили в Ideco Client.

Управление Ideco Client через CLI

Классический контекст | Высокопроизводительный контекст

С помощью CLI (Command Line Interface) можно настраивать логирование, Device VPN и кастомную конфигурацию, собирать диагностику и управлять запуском без использования графического интерфейса.

Консольный режим без графического окружения (`--console`) поддерживается начиная с Ideco Client версии 22. В более ранних версиях для запуска Ideco Client требуется графическое окружение. Так как мажорная версия Ideco Client соответствует мажорной версии NGFW Novum, для работы в консольном режиме NGFW Novum должен быть версии 22 или выше.

Как вводить команды

Windows

Откройте командную строку (cmd) или PowerShell от имени администратора и введите команду в формате:

```
"C:\Program Files\Ideco\<версия Ideco Client>\IdecoClient.exe" <команда>
```

Linux

Откройте терминал и введите команду в формате:

```
sudo /usr/local/Ideco/Agent/<версия Ideco Client>/IdecoClient.sh <команда>
```

macOS

Откройте терминал и введите команду в формате:

```
sudo /Applications/IdecoClient.app/Contents/MacOS/IdecoClient <команда>
```

Просмотр доступных команд

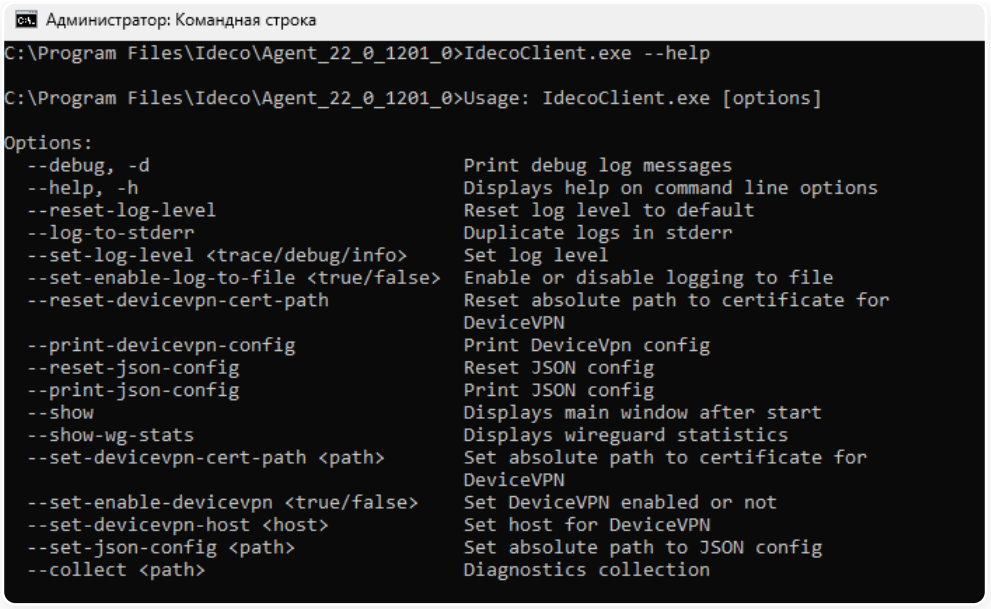
Чтобы вывести список всех доступных команд и их описание, выполните:

Windows

```
IdecoClient.exe --help
```

Или сокращенная форма:

```
IdecoClient.exe -h
```



Linux

```
sudo /usr/local/Ideco/Agent/<версия Ideco Client>/IdecoClient.sh --help
```

Или сокращенная форма:

```
sudo /usr/local/Ideco/Agent/<версия Ideco Client>/IdecoClient.sh -h
```

macOS

```
sudo /Applications/IdecoClient.app/Contents/MacOS/IdecoClient --help
```

Или сокращенная форма:

```
sudo /Applications/IdecoClient.app/Contents/MacOS/IdecoClient -h
```

Справочник команд CLI

Команда	Описание
`--help` или `-h`	Отобразить список доступных команд и их описание
`--debug` или `-d`	Включить вывод отладочных сообщений
`--show`	Отобразить главное окно после запуска
`--show-wg-stats`	Отобразить статистику WireGuard
`--console`	Запустить Ideco Client в консольном режиме без GUI
`--reset-to-auto-mode`	Переключиться на использование автоматически сгенерированных сертификатов
Логирование	
`--set-log-level <trace/debug/info>`	Установить уровень логирования. Доступные значения: • `info` - стандартный • `debug` - расширенный • `trace` - максимальный
`--reset-log-level`	Сбросить уровень логирования до значения `info`
`--set-enable-log-to-file <true/false>`	Включить (`true`) или отключить (`false`) запись логов в файл

`--log-to-stderr`	Дублировать вывод логов в stderr
Device VPN	
`--set-enable-devicevpn <true/false>`	Включить (`true`) или отключить (`false`) Device VPN
`--set-devicevpn-host <адрес NGFW Novum>`	Указать адрес сервера Ideco NGFW Novum для подключения Device VPN. Чтобы использовать резервный порт 14765, адрес необходимо указать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`)
`--set-devicevpn-cert-path <абсолютный путь до файла сертификата>`	Указать абсолютный путь до PEM-файла сертификата устройства для Device VPN
`--reset-devicevpn-cert-path`	Сбросить путь до сертификата Device VPN
`--print-devicevpn-config`	Вывести в консоль текущую конфигурацию Device VPN
`--set-dn <string>`	Указать DN (Distinguished Name) для нового сертификата
`--get-csr <абсолютный путь к директории или ->`	Создать новый ключ и сформировать запрос на подпись сертификата (CSR). Укажите путь для сохранения CSR в файл или `-` для вывода CSR в терминал без сохранения на диск
`--set-cert <абсолютный путь к файлу>`	Указать путь до подписанного сертификата
`--set-key <абсолютный путь к файлу>`	Указать путь до приватного ключа
Кастомная конфигурация	
`--set-json-config <абсолютный путь к файлу>`	Применить кастомную конфигурацию из JSON-файла по указанному абсолютному пути
`--print-json-config`	Вывести в консоль текущую кастомную конфигурацию
`--reset-json-config`	Удалить текущую кастомную конфигурацию
Диагностика	
`--collect <абсолютный путь к директории>`	Собрать диагностический ZIP-архив и сохранить его по указанному абсолютному пути

Работа в headless-системах

При необходимости Ideco Client можно запустить в консольном режиме с помощью команды `--console`. В этом случае GUI не отображается, а все команды передаются через командную строку.

На Linux консольный режим активируется автоматически при отсутствии графического интерфейса. На Windows и macOS только вручную.

Полезные ссылки

- **Настройка Device VPN**
- **Кастомная настройка Ideco Client**
- **Настройка логирования**
- **Диагностика Ideco Client**

Настройка Device VPN

Классический контекст | Высокопроизводительный контекст

Device VPN - режим работы Ideco Client, в котором клиентское устройство авторизуется на Ideco NGFW Novum без входа пользователя в систему. Такое соединение позволяет:

- ☑ Устанавливать на устройства программы и обновления
- ☑ Получать доступ к внутренней инфраструктуре
- ☑ Применять групповые политики
- ☑ Блокировать/разблокировать устройства и пользователей
- ☑ Отслеживать активность устройств и управлять устройствами за пределами внутренних сетей

Device VPN позволяет получить доступ к устройству даже когда пользователь не использует Ideco Client, и устройство имеет доступ в интернет или до Ideco NGFW Novum. Это позволяет осуществлять удаленное администрирование, обновление ПО и антивирусов, мониторинг.

ⓘ При обновлении Ideco NGFW с версии 21 на версию 22 настройки Device VPN мигрируют автоматически. Результат миграции зависит от исходных параметров: типа подключения из локальной сети, списка разрешенных объектов, состояния опции **Принимать подключения в режиме Device VPN** и наличия доверенного сертификата. Возможные комбинации параметров и результаты их миграции представлены в статье.

Для авторизации через Device VPN используется корневой сертификат с приватным ключом. На основе этого ключа администратор создает пользовательские сертификаты для конечных устройств.

В качестве **Сертификата устройства** Device VPN можно использовать:

- Самоподписанные сертификаты.
- Сертификаты, выданные Центрами сертификации (Certificate Authority, CA).

Чтобы подключить устройство к Ideco NGFW Novum в режиме Device VPN, выполните действия:

1. Перейдите в раздел **Пользователи → Ideco Client**.

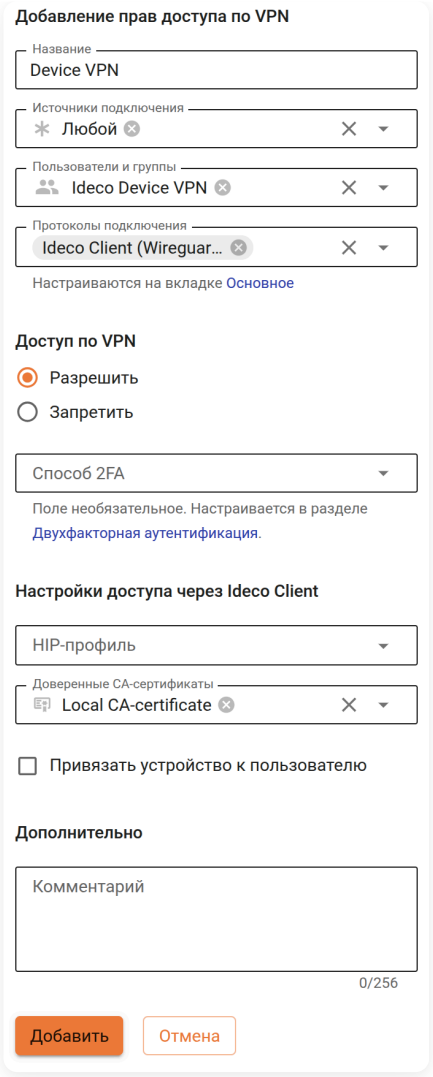
2. Введите домен или IP-адрес Ideco NGFW Novum. Если устройства пользователей находятся в локальной сети, включите одну из опций в блоке **Подключение из локальной сети**:

- **С установлением туннеля** - для авторизации пользователей по VPN.
- **Без туннеля** - для авторизации пользователей в локальной сети без туннеля.

3. Если выбрана опция **Без туннеля**, заполните поля в блоке **Разрешенные пользователи Device VPN для авторизации**:

- **Пользователи и группы Device VPN** - выберите учетные записи Device VPN (или группу **Ideco Device VPN**), которым разрешена авторизация.
- **Доверенные CA-сертификаты** - выберите один или несколько сертификатов удостоверяющих центров, которым должно доверять устройство пользователя. Управлять сертификатами можно в **Сервисы → Сертификаты → Ideco Client**.

4. Если выбрана опция **С установлением туннеля**, блок **Разрешенные пользователи Device VPN для авторизации** не используется - доступ настраивается через правила в **Пользователи → VPN-подключения → Доступ по VPN**. Создайте правило, разрешающее учетным записям или группе Ideco Device VPN подключение по протоколу Wireguard или TLS:



5. Установите Ideco Client на устройство пользователя, затем закройте Ideco Client для дальнейшей конфигурации.

Device VPN не может самостоятельно запустить автоматический выпуск сертификата. Однако, если пользователь ранее авторизовался на Ideco NGFW Novum через Ideco Client и получил сертификат в режиме AUTO, этот же сертификат используется для Device VPN без дополнительных действий - шаги 6 и 7 выполнять не нужно, достаточно задать адрес NGFW Novum и включить Device VPN командами `--set-devicevpn-host` и `--set-enable-devicevpn`.

6. Сгенерируйте на устройстве пользователя приватный ключ и сертификат в формате PEM, подписанный доверенным сертификатом. Процесс создания сертификата описан в статье Создание сертификатов для Device VPN.

Ручная установка сертификата переводит Ideco Client в режим EXTERNAL и удаляет установленные ранее ключ и сертификат, в том числе выпущенные в режиме AUTO. О правилах переключения режимов смотрите в статье Аутентификация по сертификату.

Чтобы уменьшить риск компрометации приватного ключа **Сертификата устройства** рекомендуем хранить его в директории, к которой есть доступ только у администратора. Например:

- Для Linux (Ubuntu) - каталог `/etc/ssl/private`.
- Для Windows - каталог `C:/Users/Пользователь/AppData/Roaming/Microsoft/System/Certificates`, где **Пользователь** - имя вашей учётной записи.

7. Сконфигурируйте установленный Ideco Client с сертификатом для использования Device VPN:

Перед началом ввода команд проверьте, что Ideco Client закрыт.

Чтобы использовать резервный порт 14765, параметр `<адрес NGFW Novum>` необходимо задать в формате `домен:14765` или `IP:14765` (например, `server.com:14765`).

Для Windows

Откройте командную строку от имени администратора и введите:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --set-cert <абсолютный путь до файла сертификата> --set-devicevpn-host <адре
```

Команда `--set-cert` принимает либо файл сертификата, либо объединенный файл с сертификатом и закрытым ключом. Если закрытый ключ хранится в отдельном файле, дополнительно укажите его командой `--set-key <абсолютный путь до файла закрытого ключа>`.

Для вывода заданных параметров в командную строку воспользуйтесь командой:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --print-devicevpn-config
```

Для Linux

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient.sh --set-cert <абсолютный путь до файла сертификата> --set-devicevpn-host <
```

Команда `--set-cert` принимает либо файл сертификата, либо объединенный файл с сертификатом и закрытым ключом. Если закрытый ключ хранится в отдельном файле, дополнительно укажите его командой `--set-key <абсолютный путь до файла закрытого ключа>`.

Для вывода заданных параметров в консоль воспользуйтесь командой:

```
sudo <абсолютный путь до IdecoClient>/ld.so --argv0 IdecoClient --library-path <абсолютный путь до IdecoClient>/lib <абсолютн
```

Для macOS

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient --set-cert <абсолютный путь до файла сертификата> --set-devicevpn-host <адр
```

Команда `--set-cert` принимает либо файл сертификата, либо объединенный файл с сертификатом и закрытым ключом. Если закрытый ключ хранится в отдельном файле, дополнительно укажите его командой `--set-key <абсолютный путь до файла закрытого ключа>`.

Для вывода заданных параметров в консоль воспользуйтесь командой:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient --print-devicevpn-config
```

Если необходимо создать пользователя Device VPN заранее, выполните действия указанные в статье Управление учетными записями и группами. Для создания пользователя Device VPN используется **Сертификат устройства** без приватного ключа, который не хранится на Ideco NGFW Novum в дальнейшем. Ideco NGFW Novum извлекает имя пользователя из поля **Common Name** сертификата.

При неудачной конфигурации Device VPN служба Ideco Client будет постоянно пытаться подключиться к Ideco NGFW Novum. Перезапуск службы не поможет в решении проблемы.

Для решения проблемы необходимо:

- Выключить Device VPN: выполнить команду по настройке Device VPN с единственным параметром `--set-enable-devicevpn false`.
- Исправить конфигурацию подключения (загрузить правильный сертификат, определить корректность пути до него).
- Настроить и активировать Device VPN: выполнить команду по настройке Device VPN с параметром `--set-enable-devicevpn true`.
- В интерфейсе Ideco NGFW Novum убедиться, что подключение Device VPN выполнено.

Если при подключении устройства Device VPN к Ideco NGFW Novum соединение тут же разрывается, то проверьте доступ этого устройства в зависимости от подключения:

- **С установлением туннеля** - перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и проверьте правило, разрешающее учетным записям или группе Ideco Device VPN подключение.
- **Без туннеля** - в поле **Пользователи и группы Device VPN** проверьте учетные записи или группу Ideco Device VPN, которым разрешена авторизация.

Для Device VPN автоматический выпуск сертификата устройства не выполняется. Если сертификат на устройстве отсутствует, подключение будет отклонено. Убедитесь, что сертификат устройства установлен до подключения. Процесс его создания описан в статье Создание сертификатов для Device VPN.

Миграция настроек Device VPN

Классический контекст | Высокопроизводительный контекст

В таблице представлены результаты автоматической миграции настроек Device VPN с версии 21 на версию 22 NGFW Novum в зависимости от исходной конфигурации:

Версия 21				**Версия 22**
Подключение из локальной сети	**Разрешенные объекты**	**Принимать подключения в режиме Device VPN**	**Доверенный сертификат**	**Результат миграции**
Без туннеля	Любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - Любой • **Доверенные CA-сертификаты** - загруженный сертификат • **Пользователи и группы Device VPN** - группа Ideco Device VPN Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
Без туннеля	Не любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN • **Пользователи и группы Device VPN** - объекты, входящие в группу Device VPN • **Доверенные CA-сертификаты** - загруженный сертификат Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN

С установлением туннеля	Любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - Любой • **Доверенные CA-сертификаты** - загруженный сертификат • **Пользователи и группы Device VPN** - группа Ideco Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается разрешающее правило с группой **Ideco Device VPN** и указанным сертификатом Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
С установлением туннеля	Не любой	Включена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN • **Пользователи и группы Device VPN** - объекты, входящие в группу Device VPN • **Доверенные CA-сертификаты** - загруженный сертификат В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается разрешающее правило с группой **Ideco Device VPN** и указанным сертификатом Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN

С установлением туннеля	Любой	Выключена	Загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы → Сертификаты → Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
Без туннеля	Любой	Выключена	Загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы → Сертификаты → Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
С установлением туннеля	Любой	Выключена	Не загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**
Без туннеля	Любой	Выключена	Не загружен	В **Пользователи → Ideco Client → Основное**: • **Пользователи и группы** - Любой В **Пользователи → VPN-подключения → Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**

С установлением туннеля	Не любой	Выключена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
Без туннеля	Не любой	Выключена	Загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN** Сертификат Device VPN мигрирует в **Сервисы** → **Сертификаты** → **Ideco Client**. После миграции он доступен для выбора в настройках Ideco Client и в правилах доступа по VPN
С установлением туннеля	Не любой	Выключена	Не загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**

Без туннеля	Не любой	Выключена	Не загружен	В **Пользователи** → **Ideco Client** → **Основное**: • **Пользователи и группы** - объекты, не входящие в группу Device VPN В **Пользователи** → **VPN-подключения** → **Доступ по VPN** создается запрещающее правило с группой **Ideco Device VPN**

Создание сертификатов для Device VPN

Классический контекст | Высокопроизводительный контекст

> В статье описан процесс создания сертификатов с использованием OpenSSL для подключения по Device VPN между Ideco NGFW Novum и Ideco Client.

Процесс включает два этапа:

1. Создание корневого сертификата с защищенным приватным ключом.

2. Создание сертификатов для пользовательских устройств на основе этого корневого сертификата.

Создание корневого сертификата

1. Сгенерируйте приватный ключ корневого сертификата, защищенный **passphrase**:

> Не рекомендуем копировать приватный ключ корневого сертификата с машины, на который он был создан, во избежание компрометации ключа.
>
> Рекомендуем создавать пользовательские сертификаты сразу на терминальном сервере, чтобы не переносить приватный ключ с машины на машину. Это понизит риск компрометации приватного ключа пользовательского сертификата.

```
openssl genrsa -aes256 -out ideco-dvpn_root-ca.key 4096
```

- `-aes256` - приватный ключ зашифрован алгоритмом AES-256 (более надежен, чем устаревший Triple DES (3DES));
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ.

2. Сгенерируйте корневой сертификат, используя приватный ключ корневого сертификата:

```
openssl req -x509 -new -sha256 -days 1825 -key ideco-dvpn_root-ca.key -out ideco-dvpn_root-ca.pem
```

- `-sha256` - использовать алгоритм SHA256 при создании сертификата;
- `-days 1825` - срок действия сертификата в днях;
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ корневого сертификата;
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат.

3. Заполните параметры сертификата:

```
Country Name (2 letter code) [AU]:Ru
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Test
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:MyName
Email Address []:test@ideco.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

> **Common Name (eg, your name or your server's hostname)** - обязательная строка для заполнения:
>
> - **Common Name** может быть любым, если создается корневой сертификат, который подписывает другие сертификаты.
> - **Common Name** должен быть равен имени пользователя Device VPN на Ideco NGFW Novum, если выпускается клиентский сертификат.
> - **Common Name** должен быть равен домену, на который подключаются клиенты, если выпускается серверный сертификат.

Расшифровка строк

- **Country Name (2 letter code) [XX]** - код страны в формате ISO 3166-1 alpha-2 (например, RU).
- **State or Province Name (full name) [Some-State]** - название региона или области (например, Moscow).
- **Locality Name (eg, city) [Default City]** - название города (например, Saint Petersburg).
- **Organization Name (eg, company) [Internet Widgits Pty Ltd]** - название организации.
- **Organizational Unit Name (eg, section) []** - название подразделения организации.
- **Common Name (e.g. server FQDN or YOUR name) []** - наименование сертификата.
- **Email Address []** - контактный email.

Дополнительные атрибуты:

- **A challenge password []** - пароль для дополнительной аутентификации. Рекомендуем оставить поле пустым.
- **An optional company name []:** - полное юридическое название организации.

4. Проверьте, что сертификат был успешно создан командой:

```
openssl x509 -text -noout -in ideco-dvpn_root-ca.pem
```

- Корневой сертификат должен иметь атрибут `CA:TRUE`.
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат, без приватного ключа.

5. Перейдите в **Сервисы** → **Сертификаты** → **Ideco Client** → **Реестр** и загрузите созданный сертификат `ideco-dvpn_root-ca.pem` без приватного ключа, нажав **Загрузить сертификат**. После загрузки сертификат станет доступен для выбора в поле **Доверенные CA-сертификаты** в **Пользователи** → **Ideco Client** → **Основное** и в правилах **Пользователи** → **VPN-подключения** → **Доступ по VPN**.

Создание пользовательского сертификата для конечного устройства

1. Сгенерируйте приватный ключ без применения шифрования в пользовательском пространстве администратора, куда у пользователей не будет доступа:

```
openssl genrsa -out client1-dvpn.key 4096
```

- `client1-dvpn.key` - файл, содержащий приватный ключ.

2. Сгенерируйте запрос на выпуск пользовательского сертификата с использованием приватного ключа:

```
openssl req -new -key client1-dvpn.key -out client1-dvpn.csr
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.csr` - файл, содержащий зашифрованный запрос на выпуск сертификата.

3. Заполните параметры сертификата:

```
Country Name (2 letter code) [AU]:Ru
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Test
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:MyName
Email Address []:test@ideco.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Common Name (eg, your name or your server's hostname) - обязательная строка для заполнения. Common Name используется в качестве имени пользователя Device VPN на Ideco NGFW Novum, поэтому Common Name у двух пользовательских сертификатов не может совпадать.

Расшифровка строк

- **Country Name (2 letter code) [XX]** - код страны в формате ISO 3166-1 alpha-2 (например, RU).

- **State or Province Name (full name) [Some-State]** - название региона или области (например, Moscow).
- **Locality Name (eg, city) [Default City]** - название города (например, Saint Petersburg).
- **Organization Name (eg, company) [Internet Widgits Pty Ltd]** - название организации.
- **Organizational Unit Name (eg, section) []** - название подразделения организации.
- **Common Name (e.g. server FQDN or YOUR name) []** - наименование сертификата.
- **Email Address []** - контактный email.

Дополнительные атрибуты:

- **A challenge password []** - пароль для дополнительной аутентификации. Рекомендуем оставить поле пустым.
- **An optional company name []:** - полное юридическое название организации.

4. Скопируйте файл `client1-dvpn.csr` на устройство со сгенерированным корневым сертификатом.

5. На устройстве с корневым сертификатом создайте файл **client1-dvpn.ext** для генерации сертификата. Включите в него параметры:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
```

6. На устройстве с корневым сертификатом сгенерируйте сертификат пользовательского устройства от корневого сертификата для Device VPN:

```
openssl x509 -req -in client1-dvpn.csr -CA ideco-dvpn_root-ca.pem -CAkey ideco-dvpn_root-ca.key -CAcreateserial -out client1-
```

- `client1-dvpn.csr` - файл, содержащий зашифрованный запрос на выпуск сертификата;
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат;
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ корневого сертификата;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат.

7. Проверьте, что сертификат был успешно создан командой:

```
openssl x509 -text -noout -in client1-dvpn.crt
```

- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат, без приватного ключа.
- Сертификат должен иметь атрибут `CA:FALSE` и `Subject Key Identifier`.

8. Перенесите полученный CRT-сертификат на клиентскую машину, где находится приватный ключ из шага 1.

9. Объедините приватный ключ и сертификат пользовательского устройства в PEM-файл:

Для Linux и macOS

```
cat client1-dvpn.key client1-dvpn.crt > client1-dvpn.pem
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат;
- `client1-dvpn.pem` - файл, содержащий пользовательский сертификат с приватным ключом внутри.

Для Windows

```
type client1-dvpn.key client1-dvpn.crt > client1-dvpn.pem
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат;
- `client1-dvpn.pem` - файл, содержащий пользовательский сертификат с приватным ключом внутри.

---

10. Сертификат `client1-dvpn.pem` с приватным ключом внутри, полученный на этом этапе, устанавливается на пользовательском устройстве и используется в параметрах Ideco Client.

Авторизация пользователей терминальных серверов

Классический контекст | Высокопроизводительный контекст

Терминальный сервер - сервер, позволяющий множеству пользователей одновременно работать в удаленных сессиях с общими вычислительными ресурсами сервера.

Особенности работы для пользователей терминальных серверов:

- Терминальный сервер должен работать под управлением Microsoft Windows Server версии 2019 и выше. Работа под другим ПО не гарантируется.
- Аутентификация пользователей осуществляется только через Active Directory.
- Для подключения пользователей установите на терминальный сервер Ideco Client.
- Ideco Client устанавливает туннель от терминального сервера до NGFW Novum.
- Каждый пользователь получает отдельный динамический виртуальный IP-адрес из заданной подсети.
- Для каждого пользователя можно настроить правила работы **Межсетевого экрана** и **Контент-фильтра**.
- Правила **Межсетевого экрана** работают только для протоколов TCP и UDP.

Не рекомендуется копировать приватный ключ корневого сертификата с машины, на который он был создан, во избежание компрометации ключа.

Рекомендуем создавать пользовательские сертификаты сразу на терминальном сервере, чтобы не переносить приватный ключ с машины на машину. Это понизит риск компрометации приватного ключа пользовательского сертификата.

Настройка авторизации пользователей

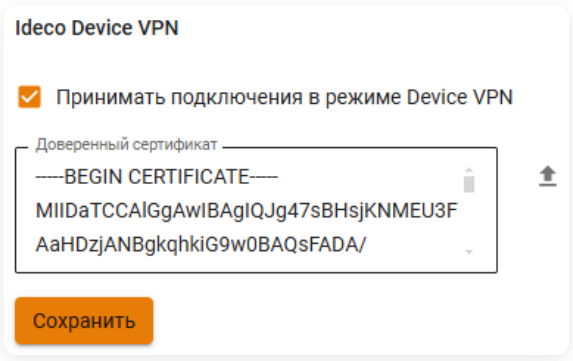
Перед настройкой терминального сервера необходимо:

- Интегрировать Ideco NGFW Novum с Microsoft Active Directory. Если Active Directory и терминальный сервер находятся на **разных физических машинах**, терминальный сервер нужно ввести в домен AD.
- Убедитесь, что нужные пользователи AD доступны для NGFW Novum на вкладке Учетные записи → Active Directory.
- Получить сертификаты или создать самоподписанные сертификаты для подключения. Пример создания самоподписанных сертификатов в статье.

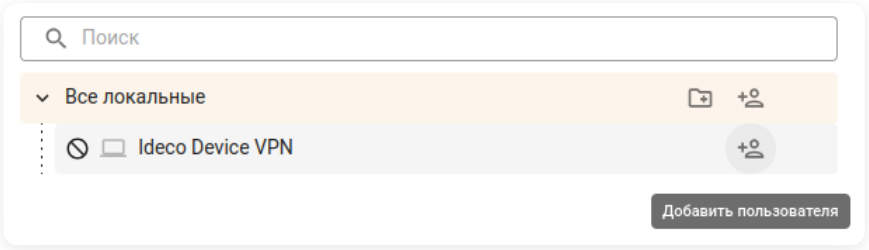
Вместо самоподписанных сертификатов рекомендуем использовать доверенный удостоверяющий центр, например, корпоративный УЦ на базе AD CS.

В Ideco NGFW Novum загружается только корневой или промежуточный сертификат УЦ без приватного ключа, который используется как сертификат Device VPN для проверки сертификата терминального сервера. Сертификат терминального сервера с приватным ключом должен находиться только на самом терминальном сервере и использоваться для аутентификации терминального сервера в Ideco NGFW Novum. Передавать приватные ключи в Ideco NGFW Novum нельзя.

1. Перейдите в **Пользователи** → **Ideco Client**, включите опцию **Принимать подключения в режиме Device VPN** и загрузите корневой сертификат (обязательно без приватного ключа):



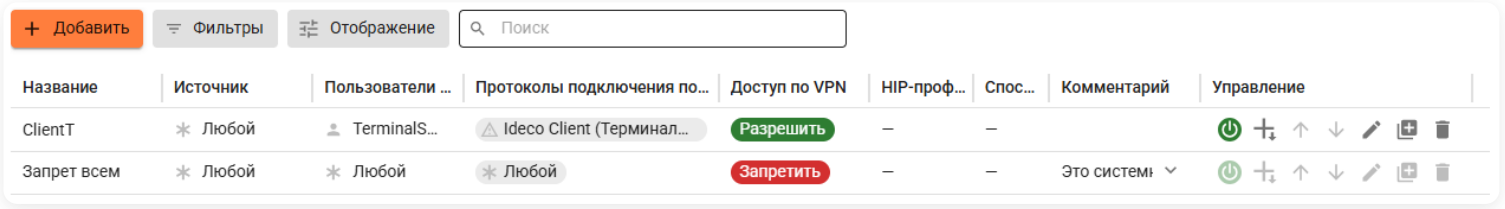
2. Перейдите в **Пользователи** → **Учетные записи** и в группу **Ideco Device VPN** добавьте устройство, загрузив пользовательский сертификат, подписанный корневым сертификатом. Пользовательский сертификат не должен включать в себя приватный ключ, поскольку это повышает шансы компрометации приватного ключа пользовательского сертификата:



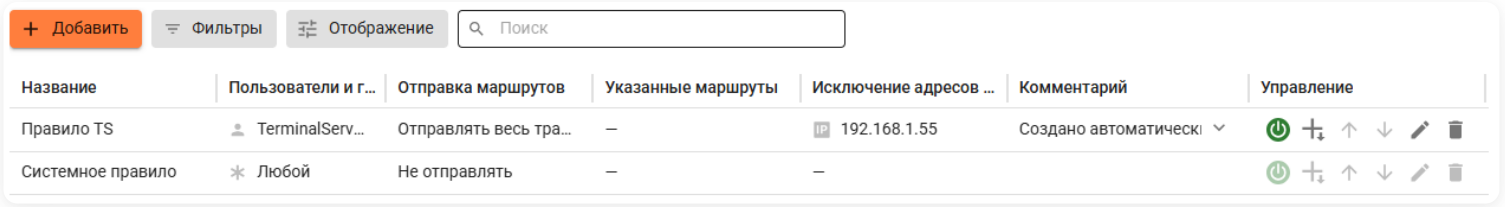
Для добавления нескольких устройств в группу **Ideco Device VPN** убедитесь, что поле **Common Name** во всех пользовательских сертификатах уникальное, т.е. нет двух сертификатов с одинаковым **Common Name**. В противном случае добавить несколько устройств в группу **Device VPN** не выйдет.

Рекомендуем генерировать отдельный пользовательский сертификат для каждого устройства, поскольку в случае компрометации приватного ключа пользовательского сертификата достаточно будет перевыпустить один пользовательский сертификат и поставить на конкретное устройство. В противном случае нужно будет устанавливать новый пользовательский сертификат на все устройства, на которых был скомпрометированный сертификат.

3. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и добавьте правило, разрешающее подключение через Ideco Client:

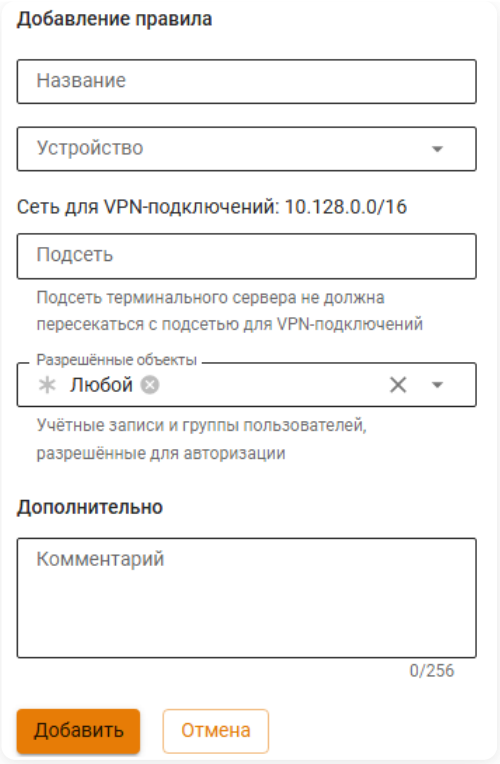


4. Перейдите в **Пользователи** → **VPN-подключения** → **Передача маршрутов** и добавьте правило, перенаправляющее трафик, который нужно проверять на Ideco NGFW Novum. Не стоит перенаправлять служебный трафик до контроллера домена AD или любой другой служебный трафик на Ideco NGFW Novum:



Клиенты терминального сервера будут использовать маршруты, заданные для самого терминального сервера в таблице **Передача маршрутов**.

5. Перейдите в **Пользователи** → **Ideco Client** → **Терминальный доступ** и добавьте правило с подсетью для выдачи IP-адресов пользователям:



- **Название** - укажите название правила.
- **Устройство** - укажите устройство пользователя, добавленное на шаге 2.
- **Подсеть** - укажите подсеть, в которой пользователям будут назначаться IP-адреса. Подсеть должна принадлежать к диапазону локальных подсетей и не должна пересекаться с подсетью для VPN-подключений, указанной в разделе **Пользователи** → **VPN-подключения** → **Основное**.
- **Разрешенные обьекты** - укажите группы пользователей, которым разрешена авторизация. Можно указать объекты: **Любой**, пользователь AD, группа безопасности AD, LDAP-фильтр.
- **Комментарий** - необязательное поле.

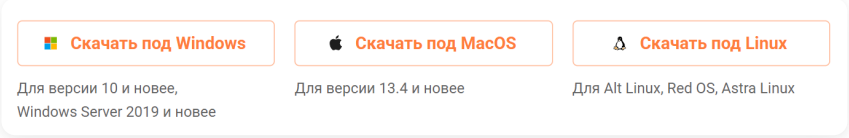
Подсеть для выдачи IP-адресов пользователям терминального сервера не должна пересекаться с уже имеющимися на Ideco NGFW Novum подсетями.

6. Загрузите корневой сертификат Ideco NGFW Novum на терминальный сервер и добавьте его в доверенные центры сертификации. Пользовательский сертификат из шага 1 и 2 также должен находиться на терминальном сервере (с приватным ключом).

Если используется Let`s Encrypt сертификат на доменное имя, к которому подключаются устройства с Ideco Client и терминальный сервер, загружать корневой сертификат NGFW Novum на конечные устройства и терминальный сервер не требуется. Доверие к этому сертификату уже будет на устройствах и терминальном сервере.

Лучше создавать пользовательские сертификаты сразу на терминальном сервере, чтобы не переносить приватный ключ с машины на машину. Это понизит риск компрометации приватного ключа пользовательского сертификата.

7. Установите Ideco Client на терминальный сервер. Для этого перейдите в **Пользователи** → **Ideco Client** и выберите **Скачать под Windows**:



8. Создайте на терминальном сервере `JSON-файл` и добавьте запись:

```
{
  "terminal_data": {
    "type": "terminal",
    "cert_data": "C:\\jsonconfig\\cert.pem",
    "server": "192.168.100.2"
  }
}
```

- `cert_data` - абсолютный путь до сертификата DeviceVPN с приватным ключом в формате `<диск>:\\<путь\\до\\сертификата>`.
- `server` - IP-адрес или FQDN (Fully Qualified Domain Name) сервера Ideco NGFW Novum.

9. Откройте командную строку от имени администратора и выполните команду:

```
"C:\Program Files\Ideco\<Версия Агента>\IdecoClient.exe" --set-json-config="C:\path\to\terminal-conifg.json"
```

- `"C:\Program Files\Ideco\<Версия Агента>\IdecoClient.exe"` - абсолютный путь к `IdecoClient.exe`.
- `"C:\Program Files\Ideco\test.json"` - абсолютный путь к `JSON-файлу` конфигурации.

После настройки конфигурации терминальный сервер должен успешно пройти авторизацию в Ideco NGFW Novum. Для проверки авторизации перейдите в **Мониторинг → Сессии пользователей**. Должна появиться новая запись с названием добавленного терминального сервера, а в столбце **Тип авторизации** указано значение **Терминальный сервер**.

10. Пользователи смогут подключаться к терминальному серверу по протоколу RDP (Remote Desktop Protocol), используя свои учетные данные Active Directory для аутентификации. Система автоматически назначит пользователям динамические виртуальные IP-адреса из указанной подсети, а информация об активных авторизациях появится в таблице **Мониторинг → Сессии пользователей**.

Один и тот же пользователь может авторизоваться со своего компьютера в Ideco NGFW Novum как непосредственно (через VPN, через IP/MAC и т.п.), так и через любой терминальный сервер, к которому у пользователя есть доступ. Терминальный сервер автоматически авторизует пользователя под новым IP (как отдельную сессию). Это позволяет гибко настраивать правила **Межсетевого экрана** и **Контент-фильтра** для каждого способа подключения.

Для управляющего соединения терминального сервера используется порт 443 по умолчанию. Резервный порт 14765 можно указать в поле `server` в формате `IP:14765` или `домен:14765` (например, `server.com:14765`).
В режиме терминального сервера поднимается туннель только через 3051 порт UDP.

Диагностика работы Ideco Client

Как включить режим отладки для Ideco Client

Настройка режима отладки Ideco Client для сбора диагностической информации

Перейти

Диагностика работы Ideco Client при помощи архива с логами и системными данными

Разовый сбор логов и системных данных в один архив

Перейти

Диагностика работы Ideco Client с помощью логирования

Включение логирования позволит анализировать работу Ideco Client для диагностики проблем

Перейти

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Как включить режим отладки для Ideco Client

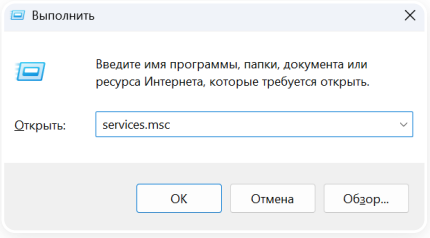
Классический контекст | Высокопроизводительный контекст

Включение режима отладки позволит собрать расширенные диагностические данные.

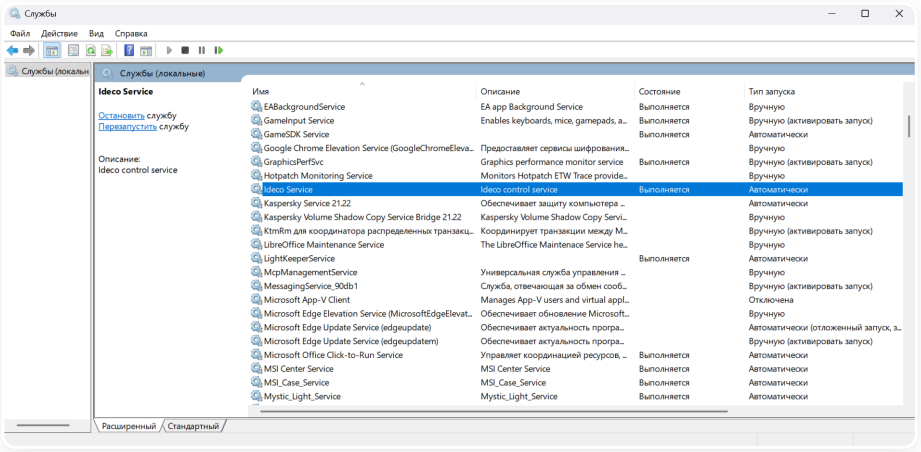
Необходима учетная запись с правами администратора.

Для включения режима:

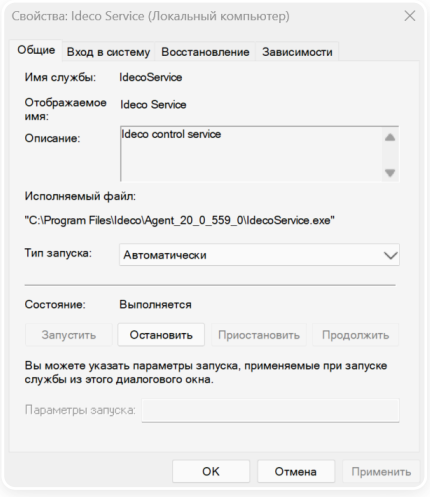
1. Нажмите **Win+R**, введите `services.msc` и нажмите **Ок**:



2. Найдите службу **Ideco Service**:

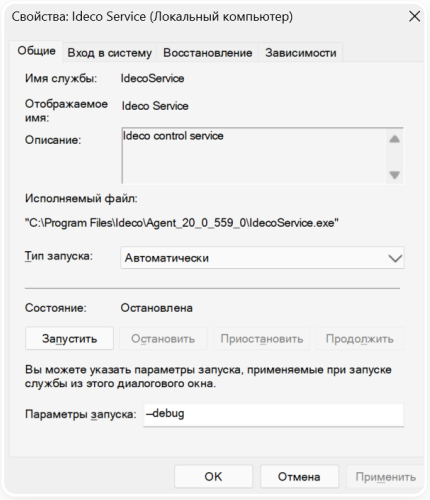


3. Двойным кликом откройте свойства, нажмите **Остановить** и дождитесь остановки службы:



Если произошла ошибка остановки службы, дождитесь запуска службы и остановите службу повторно.

4. В поле **Параметры запуска** введите `--debug` и нажмите **Запустить** для старта службы:



Не закрывайте окно **Свойства: Ideco Service**, иначе режим отладки работать не будет.

5. Запустите Ideco Client, чтобы воспроизвести ошибку.

6. Получите расширенные данные с помощью диагностического архива или системных утилит.

При необходимости обратитесь в техническую поддержку.

Диагностика работы Ideco Client при помощи архива с логами и системными данными

Классический контекст | Высокопроизводительный контекст

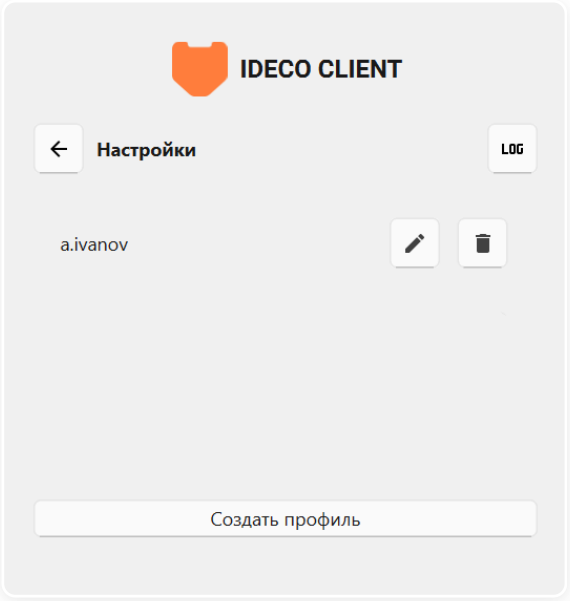
Сбор диагностической информации позволит получить структурированный архив данных для анализа работы Ideco Client. Полученные данные помогут администраторам и специалистам технической поддержки в устранении неполадок.

Запустите сбор данных:

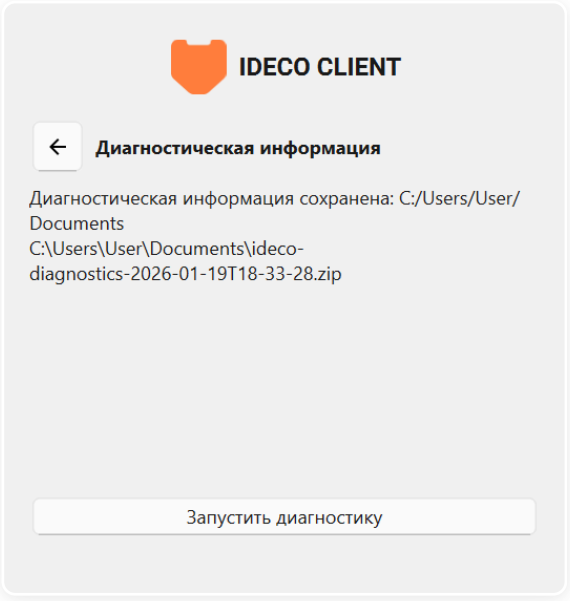
Графический интерфейс

1. Запустите Ideco Client и нажмите .

2. В настройках нажмите LOG и выберите, куда сохранить ZIP-архив с результатами:



3. После окончания сбора данных откроется окно с путем и названием созданного архива с логами:



Командная строка

> В командной строке не отображается ход процесса сбора данных, только итоговый статус.

1. Выполните команду, указав абсолютный путь, куда сохранить ZIP-архив с результатами диагностики:

```
ideco-client --collect <"абсолютный путь к директории">
```

Пример на Windows:

```
ideco-client --collect C:\Users\Username\Desktop\
```

> На Linux и macOS команда аналогична, отличается только синтаксис пути (прямые слеши `/` вместо обратных `\`).

2. Сообщение при успешном завершении:

```
[OK] Diagnostics collected: C:\Users\Username\Desktop\ideco-diagnostics-YYYY-MM-DDTHH-MM.zip
```

Архив содержит данные за последние два дня. Имя файла формируется по шаблону: `ideco-diagnostics-YYYY-MM-DDTHH-MM.zip`, где `YYYY-MM-DD` - дата создания, `THH-MM` - время создания (буква `T` используется как разделитель согласно стандарту ISO 8601). Пример: `ideco-diagnostics-2025-07-31T14-23.zip`.

Содержимое архива

- `logs/`
  - `ideco-client_logs.json` - логи Ideco Client
  - `ideco-service_logs.json` - логи службы Ideco Service
- `system/`
  - `system_info.json` - информация об ОС, имени хоста и DNS-конфигурации
  - `network.json` - список сетевых интерфейсов с основными параметрами

Содержание файлов

ideco-client_logs.json - логи Ideco Client.

```
{
  "ts": "string",
  "comp": "string",
  "lvl": "string",
  "type": "string",
  "msg": "string",
  "data": {
    "eid": "integer",
    "erid": "integer",
    "pid": "integer",
    "tid": "integer",
    "comp_name": "string"
  }
}
```

- `"ts"` - timestamp (ISO 8601, UTC), берется из поля `SystemTime`;
- `"comp"` - источник события:
  - `ideco-service` - служба `ideco-service`;
  - `ideco-client - ProviderName` - Ideco Client.
- `"lvl"` - уровень логирования:

    - `"INFO"` - штатные события работы приложения;
    - `"WARN"` - нештатная ситуация, которая не привела к сбою, но требует внимания;
    - `"ERROR"` - ошибка, которая повлияла на выполнение конкретной операции или запроса, но позволяет приложению продолжать работу;
    - `"DEBUG"` - детальная служебная информация о ходе выполнения;
    - `"TRACE"` - максимально детальная отладочная информация выполнения;
    - `"CRITICAL"` - критическая ошибка, требующая немедленного вмешательства и приводящая к остановке компонента или всего приложения.
- `"type"` - тип события:
    - `"logs"` - логи службы Ideco Service;
    - `"system"` - информация об ОС, имени хоста и DNS-конфигурации;
    - `"network"` - список сетевых интерфейсов с основными параметрами.
- `"msg"` - краткое текстовое описание события;
- `"data"`:
    - `"eid"` - идентификатор события (`EventID`);
    - `"erid"` - идентификатор записи события (`EventRecordID`);
    - `"pid"` - идентификатор процесса (`ProcessID`);
    - `"tid"` - идентификатор потока (`ThreadID`);
    - `"comp_name"` - имя компьютера (`Computer`).

ideco-service_logs.json - логи службы Ideco Service.

```
{
  "ts": "string",
  "comp": "string",
  "lvl": "string",
  "type": "string",
  "msg": "string",
  "data": {
    "eid": "integer",
    "erid": "integer",
    "pid": "integer",
    "tid": "integer",
    "comp_name": "string"
  }
}
```

- `"ts"` - timestamp (ISO 8601, UTC), берется из поля `SystemTime`;
- `"comp"` - источник события:
    - `ideco-service` - служба `ideco-service`;
    - `ideco-client - ProviderName` - Ideco Client.
- `"lvl"` - уровень логирования:
    - `"INFO"` - штатные события работы приложения;
    - `"WARN"` - нештатная ситуация, которая не привела к сбою, но требует внимания;
    - `"ERROR"` - ошибка, которая повлияла на выполнение конкретной операции или запроса, но позволяет приложению продолжать работу;
    - `"DEBUG"` - детальная служебная информация о ходе выполнения;
    - `"TRACE"` - максимально детальная отладочная информация выполнения;
    - `"CRITICAL"` - критическая ошибка, требующая немедленного вмешательства и приводящая к остановке компонента или всего приложения.
- `"type"` - тип события:
    - `"logs"` - логи службы Ideco Service;
    - `"system"` - информация об ОС, имени хоста и DNS-конфигурации;
    - `"network"` - список сетевых интерфейсов с основными параметрами.
- `"msg"` - краткое текстовое описание события;
- `"data"`:
    - `"eid"` - идентификатор события (`EventID`);
    - `"erid"` - идентификатор записи события (`EventRecordID`);
    - `"pid"` - идентификатор процесса (`ProcessID`);
    - `"tid"` - идентификатор потока (`ThreadID`);
    - `"comp_name"` - имя компьютера (`Computer`).

system_info.json - информация об операционной системе, имени хоста и DNS-конфигурации.

```
{
  "ts": "string",
  "type": "string",
  "data": {
    "os_name": "string",
    "os_ver": "string",
    "arch": "string",
    "build": "string",
    "vendor": "string",
    "hostname": "string",
    "dns_srv": ["string"],
    "dns_sfx": ["string"],
    "dns_en": "boolean"
  }
}
```

- `"ts"` - timestamp (ISO 8601, UTC);
- `"type"` - тип данных `system_info`;
- `"data"` - объект с детальной системной информацией:
  - `"os_name"` - название ОС;
  - `"os_ver"` - версия ОС;
  - `"arch"` - архитектура процессора;
  - `"build"` - номер сборки;
  - `"vendor"` - производитель ОС;
  - `"hostname"` - имя хоста;
  - `"dns_srv"` - DNS-серверы;
  - `"dns_sfx"` - DNS-суффиксы поиска;
  - `"dns_en"` - статус службы DNS.

network.json - список сетевых интерфейсов с основными параметрами.

```
{
  "ts": "string",
  "type": "string",
  "data": {
    "name": "string",
    "mac": "string",
    "ipv4": ["string"],
    "netmask": "string",
    "gateway": "string",
    "status": "string",
    "if_type": "string",
    "mtu": "integer",
    "dns_srv": ["string"],
    "dns_sfx": ["string"]
  }
}
```

- `"ts"` - временная метка (ISO 8601, UTC);
- `"type"` - тип данных: `network`;
- `"data"` - объект с информацией о сетевом интерфейсе:
  - `"name"` - имя сетевого интерфейса;
  - `"mac"` - MAC-адрес (формат: `XX:XX:XX:XX:XX:XX`);
  - `"ipv4"` - массив IPv4 адресов;
  - `"netmask"` - маска подсети;
  - `"gateway"` - шлюз по умолчанию;
  - `"status"` - статус интерфейса:
    - `"up"` - подключен;
    - `"down"` - не подключен;
    - `"unknown"` - статус неизвестен.
  - `"if_type"` - тип интерфейса:
    - `"ethernet"` - проводной интерфейс;
    - `"tunnel"` - виртуальный интерфейс, не привязанный к физическому сетевому порту;

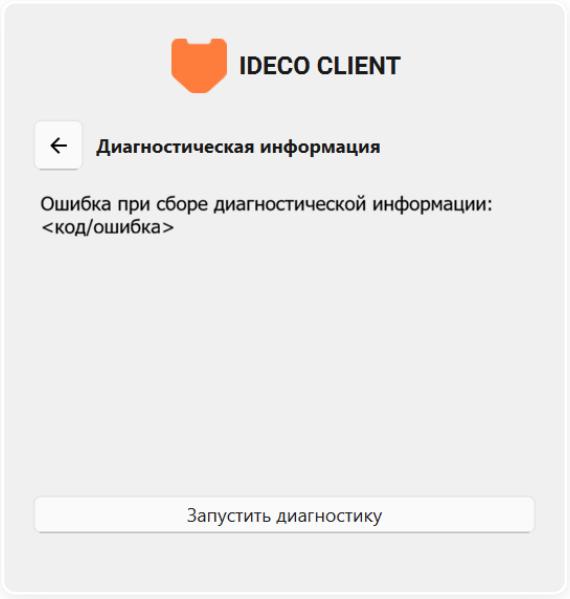
        - `"bridge"` - интерфейс объединяющий несколько интерфейсов в один логический сегмент.
        - `"loopback"` - виртуальный интерфейс, не привязанный к физическому сетевому порту.
    - `"mtu"` - размер пакета MTU;
    - `"dns_srv"` - DNS-серверы, привязанные к интерфейсу;
    - `"dns_sfx"` - DNS-суффиксы поиска.

Данные, которые не собираются:

- Логины
- Пароли
- Электронная почта
- Токены аутентификации
- Приватные ключи
- Пути к домашним директориям пользователей
- Сетевые идентификаторы (SID и аналогичные)

Возможные ошибки при сборе данных

При использовании командной строки текст ошибки будет выведен в командной строке. При использовании графического интерфейса описание и код ошибки будут показаны в окне запуска диагностики:



Список возможных ошибок:

Код ошибки	Сообщение в графическом интерфейсе	Сообщение в командной строке	Как исправить
1	Не указан путь	[ERROR] Invalid command syntax	• Укажите обязательный параметр при вызове команды • Путь должен быть абсолютным. Например: ideco-client --collect C:\Users\Username\Desktop
1	Некорректный путь	[ERROR] Diagnostics collection failed: invalid output path	• Проверьте корректность и существование пути • Путь не должен содержать лишних символов • У пользователя, который запускает диагностику, должны быть права доступа на запись в указанную директорию
2	Сбор уже выполняется	[INFO] Diagnostics collection failed: already running	• Дождитесь завершения текущего процесса сбора диагностики • Если сбор данных завис, перезапустите службу Ideco Service
3	Служба недоступна	[ERROR] Diagnostics collection failed: communication error	• Убедитесь, что служба Ideco Service запущена • Перезапустите службу Ideco Service • Перезапустите Ideco Client
3	Ошибка архивации или сериализации	[ERROR] Diagnostics collection failed: <error_description>	• Убедитесь, что антивирус не блокирует создание архивных файлов

3	Ошибка чтения данных	[ERROR] Diagnostics collection failed: data read error	• Проверьте целостность файлов и повторно запустите сбор данных
3	Недостаточно места на диске	[ERROR] Diagnostics collection failed: not enough disk space	• Проверьте наличие свободного места на диске (требуется минимум 500 МБ) или выберите другой путь для сохранения
3	Внутренняя ошибка службы	[ERROR] Diagnostics collection failed: internal service error	• Перезапустите службу Ideco Service

Полезные ссылки

- **Как включить режим отладки для Ideco Client**
- **Кастомная настройка Ideco Client**

Диагностика работы Ideco Client с помощью логирования

Классический контекст | Высокопроизводительный контекст

Включение логирования позволит анализировать работу Ideco Client для диагностики проблем. Полученные данные помогут администраторам и специалистам технической поддержки в устранении неполадок.

Особенности работы логирования

- Для выполнения команд могут потребоваться права администратора.
- Изменение уровня логирования применяется сразу и не требует перезапуска системы.
- При повторном запуске Ideco Client записи в логах не перезаписываются, а дополняются.
- Доступны логи за последние два дня.

Настройка логирования

1. Откройте командную строку или терминал.

- Windows - командная строка (cmd) или PowerShell.
- Linux и macOS - терминал.

2. Введите команду для перехода к каталогу, где установлен Ideco Client:

ОС	Команда
Windows, Linux, macOS	`cd <путь_к_каталогу_агента>`

Пример: `cd C:\Program Files\Ideco Client`.

3. Выберите необходимый уровень логирования и введите команду:

ОС	Команда
Windows	`.\IdecoClient.exe --set-log-level <уровень_логирования>`
Linux, macOS	`IdecoClient --set-log-level <уровень_логирования>`

Уровни логирования:

- `info` - стандартный уровень детализации.
- `debug` - расширенная отладочная детализация.
- `trace` - максимальный уровень детализации.

Пример: `.\IdecoClient.exe --set-log-level debug`

4. Введите команду, чтобы включить запись логов:

ОС	Команда
Windows	`.\IdecoClient.exe --set-enable-log-to-file true`
Linux, macOS	`IdecoClient --set-enable-log-to-file true`

После включения логирования формируются два файла `IdecoClient_log.txt` и `IdecoService_log.txt` в директории:

ОС	Путь
Windows	`IdecoClient_log.txt` по пути `%TEMP%` `IdecoService_log.txt` по пути `C:\windows\temp`
Linux	`/tmp`
macOS	`/tmp` или `/var/folders/`

Возврат к стандартному уровню логирования

Для возврата логирования к уровню `info` введите команду:

ОС	Команда
Windows	`.\IdecoClient.exe --reset-log-level`
Linux, macOS	`IdecoClient --reset-log-level`

Отключение записи логов

Для отключения записи логов введите команду:

ОС	Команда
Windows	`.\IdecoClient.exe --set-enable-log-to-file false`
Linux, macOS	`IdecoClient --set-enable-log-to-file false`

Профили устройств

Классический контекст | Высокопроизводительный контекст | API

Профили устройств или HIP-профили (Host Information Profile) позволяют задать критерии проверки устройств, которые подключаются к NGFW только через Ideco Client. Для других сессий авторизации профили не назначаются.

С помощью профилей реализуется ZTNA (Zero Trust Network Access) - технология обеспечения безопасного доступа к сети, основанная на **принципе нулевого доверия**. ZTNA позволяет контролировать и аутентифицировать устройства пользователей перед предоставлением доступа к ресурсам сети.

Возможно использование HIP-профилей для терминального сервера. В этом случае HIP-профили определяются только для сессии авторизации сервера, но не для сессий авторизации терминальных пользователей.

В случае несоответствия HIP-профилю терминальная сессия закрывается вместе со всеми сессиями терминальных пользователей.

Информация, собираемая Ideco Client

Данные, которые Ideco Client собирает с устройства пользователя:

- Версия Windows
- Наличие установленного пакета обновлений
- Наличие установленного антивируса
- Наличие актуальной базы антивируса
- Дата последней проверки антивируса
- Версия межсетевого экрана и вендор
- Информация о процессах, запущенных на устройстве
- Информация о запущенных службах
- Информация о ключах реестра
- Добавление устройства в домен

Критерии проверки, доступные на NGFW Novum

Критерии, которые администратор может задать в HIP-объектах для проверки устройств:

- Операционная система
- Пакет обновлений Windows
- Антивирус
- Межсетевой экран
- Процесс, запущенный на устройстве
- Запущенная служба Windows
- Ключ реестра Windows

HIP-объекты

На вкладке создаются объекты, каждый HIP-объект - совокупность критериев проверки устройства. HIP-объекты используются для создания HIP-профиля. Каждый из HIP-объектов возвращает логическое значение. Если критерии HIP-объекта выполнены, то объект возвращает положительный результат.

Для создания HIP-объекта выполните действия:

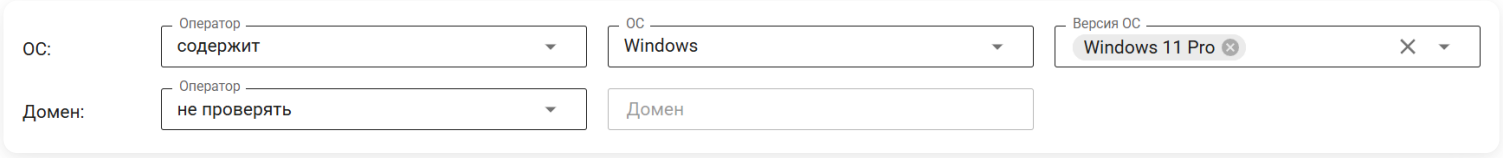
1. Перейдите в **Профили устройств** → **HIP-объекты** и нажмите **Добавить**.

2. Введите название HIP-объекта:



3. Выберите критерии, включив опцию **Включить проверку** для необходимой проверки:

ОС и домен



ОС - проверка по операционной системе.

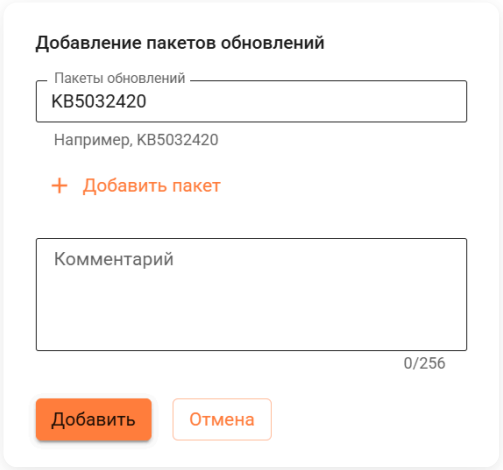
- Оператор:
  - содержит
  - не содержит
  - не проверять
- ОС:
  - Windows
  - Linux
  - macOS
- Версия ОС

Домен - проверка по домену Active Directory, к которому присоединено устройство.

- Оператор:
  - содержит
  - не содержит
  - не проверять
- Домен

Пакеты обновлений (KB)

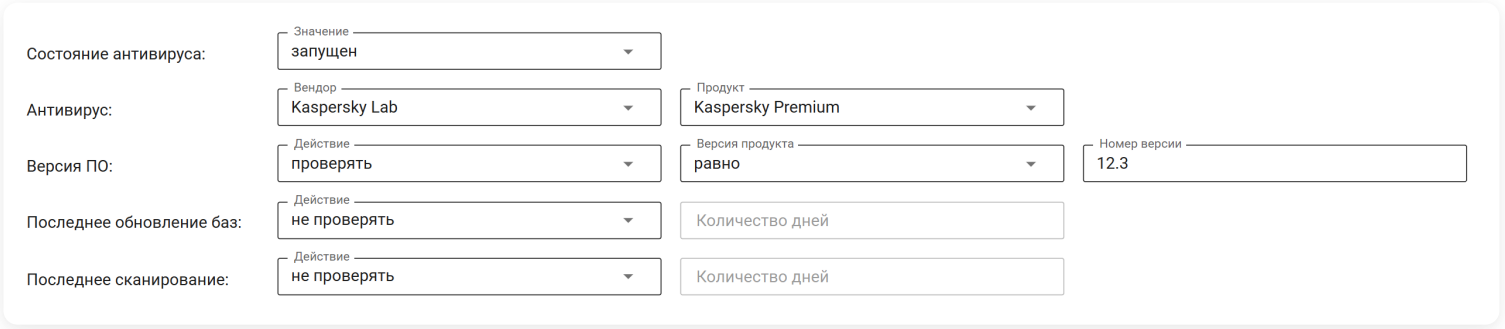
1. Нажмите **Добавить** и укажите пакет обновлений Windows (например, KB5032420):



Для добавления нескольких пакетов обновлений нажмите **Добавить пакет**.

2. Нажмите **Добавить**.

Антивирус



Состояние антивируса - проверка по статусу антивируса.

- Значение:
  - Установлен (антивирус установлен, но не запущен)
  - Запущен (антивирус установлен и запущен)

Антивирус - проверка по антивирусу.

- Вендор (например, Kaspersky Lab)
- Продукт (например, Kaspersky Premium)

Версия ПО - проверка по версии антивируса.

- Действие:
  - Проверять
  - Не проверять
- Версия продукта:
  - Равно
  - Содержит
- Номер версии

Последнее обновление баз - проверка по времени обновления баз.

- Действие:
  - Не проверять
  - Проверять в течение последних дней
- Количество дней (сколько прошло дней с момента обновления баз антивируса)

Последнее сканирование - проверка по времени последнего сканирования антивирусом.

- Действие:
  - Не проверять
  - Проверять в течение последних дней
- Количество дней (сколько прошло дней с момента последнего сканирования)

Межсетевой экран

- Включите опцию **Запущен** для проверки того, запущен ли межсетевой экран.

Продукт - проверка по вендору и продукту межсетевого экрана.

- Оператор:
  - содержит
  - не проверять
- Вендор (например, DrWeb)
- Продукт (например, Dr.Web Security Space)

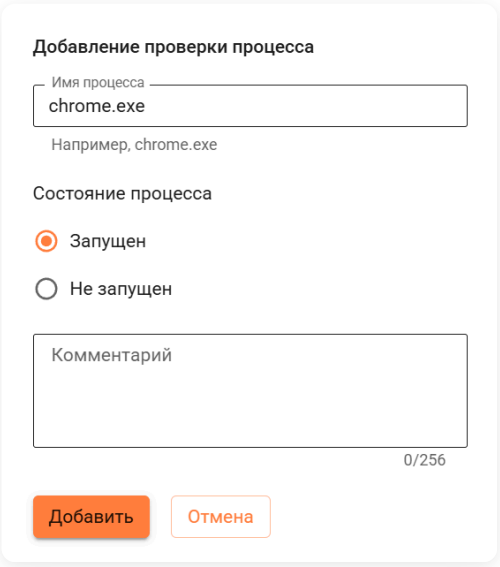
Версия ПО - проверка по версии межсетевого экрана.

- Оператор:
  - содержит

- не проверять
- Версия

Процессы

1. Нажмите **Добавить** и заполните поля:

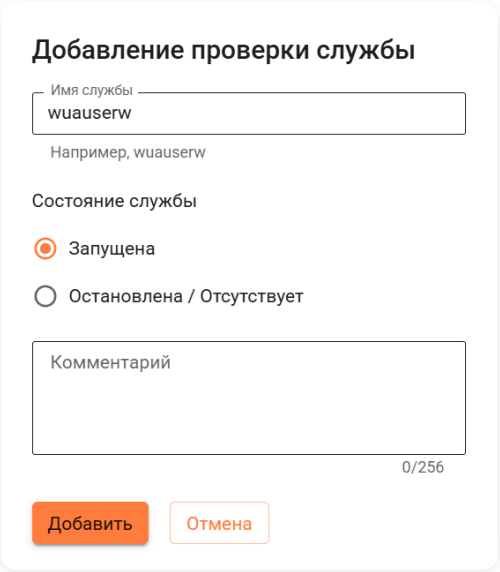


- Имя процесса (например, `chrome.exe`)
- Состояние процесса:
  - Запущен
  - Не запущен

2. Нажмите **Добавить**.

Службы

1. Нажмите **Добавить** и заполните поля:



- Имя службы (например, `wuauserw`)
- Состояние службы:
  - Запущена
  - Остановлена или отсутствует

2. Нажмите **Добавить**.

Ключи реестра

1. Нажмите **Добавить** и заполните поля:

- **Путь** - путь ключа реестра (например, `HKEY_LOCAL_MACHINE\DriverDatabase`).

- **Параметр** - параметр ключа реестра (например, `WallpaperOriginX`).
- **Инвертировать значение** - включите опцию, если необходимо инвертировать значение ключа реестра.
- **Значение** - укажите значение ключа реестра (например, `0x00000000 (0)`).

2. Нажмите **Добавить**.

> При создании критерия проверки **Ключи реестра** используйте корневые разделы реестра Windows:
>
> - `HKEY_LOCAL_MACHINE`
> - `HKEY_CURRENT_USER`
> - `HKEY_CLASSES_ROOT`
> - `HKEY_USERS`
> - `HKEY_CURRENT_CONFIG`

4. Нажмите **Добавить**.

HIP-профили

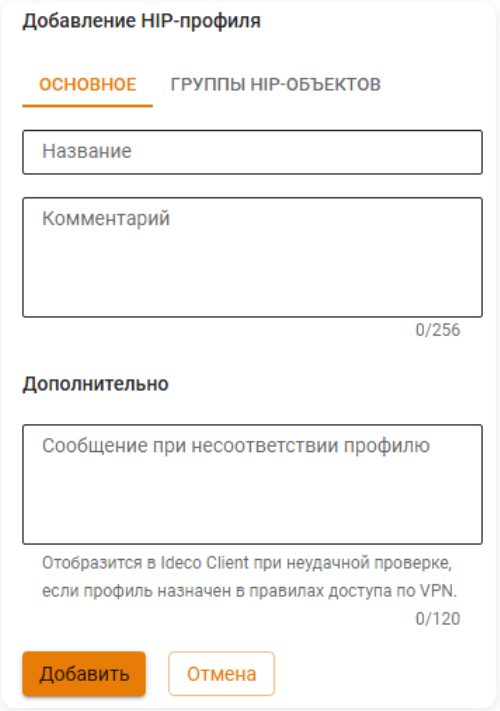
На вкладке создаются HIP-профили, состоящие из сгруппированных с помощью логических операций HIP-объектов И/ИЛИ.

Если при проверке устройства пользователя логическое выражение HIP-профиля возвращает положительный результат, профиль закрепляется за сессией авторизации и отображается в таблице Сессии пользователей. Если ни один HIP-профиль не совпал с сессией авторизации, то на сессию назначается специальный HIP-профиль **Устройство без профиля**. На одну сессию авторизации может быть назначено несколько профилей при совпадении.

Для создания HIP-профиля выполните действия:

1. Перейдите в **Профили устройств** → **HIP-профили** и нажмите **Добавить**.

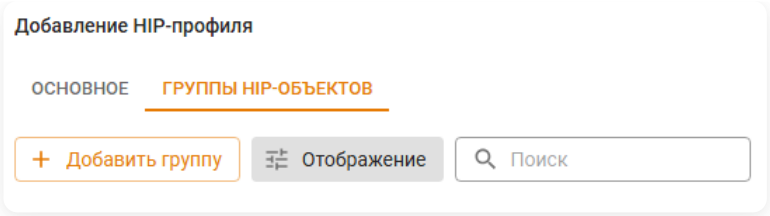
2. Заполните поля на вкладке **Основное**:



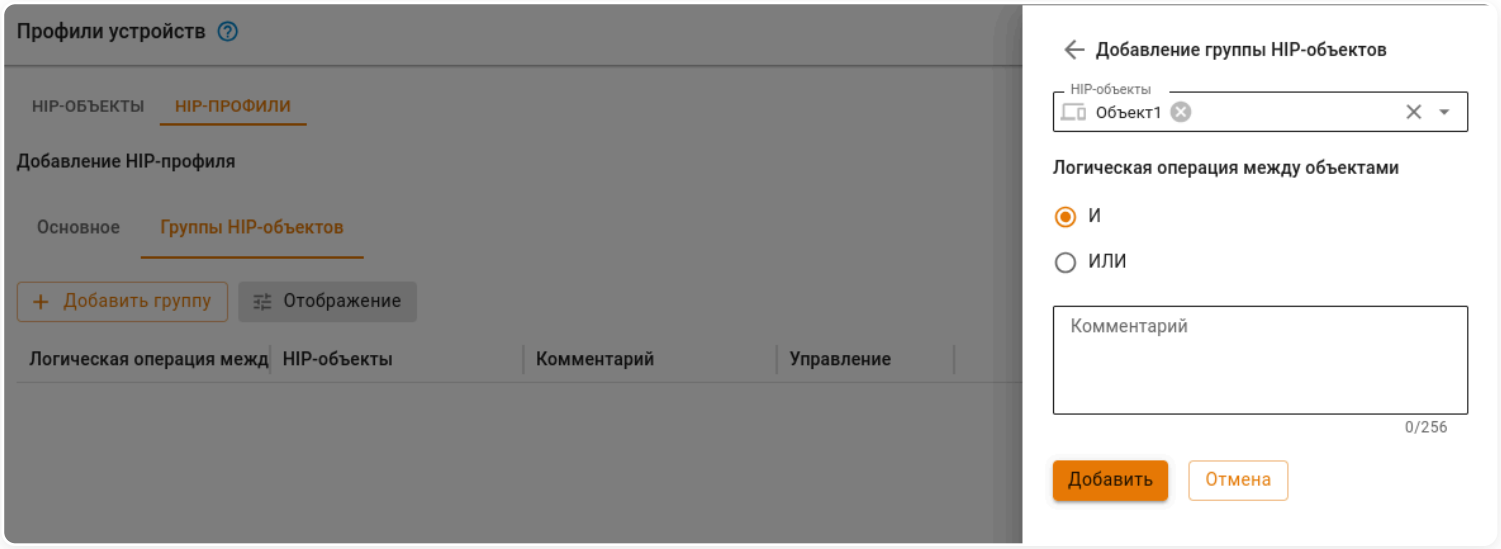
Расшифровка полей

- **Название HIP-профиля** - укажите название HIP-профиля.
- **Комментарий** - произвольный текст. Не более 256 символов.
- **Сообщение при несоответствии профилю** - введите текст, который отобразится в Ideco Client в случае несоответствия устройства назначенному HIP-профилю в правилах доступа по VPN. Максимальная длина - 120 символов. Если поле пустое, то в Ideco Client по умолчанию выводится текст: **Проверка безопасности не пройдена**:

3. Перейдите на вкладку **Группы HIP-объектов**, нажмите **Добавить группу**:



4. Выберите HIP-объекты, указав логическую операцию между объектами И/ИЛИ:



5. Нажмите **Добавить**.

HIP-профили можно использовать в качестве дополнительного условия в правилах **FORWARD**. Правило сработает, если трафик исходит от устройства, которому назначен хотя бы один профиль, указанный в правиле.

Использование HIP-профилей

HIP-объекты и профили не влияют на правила трафика до их применения в правилах **Межсетевого экрана**. Чтобы с помощью профилей ограничить или разрешить доступ к ресурсам сети, необходимо:

1. Создать HIP-объекты.

2. Сгруппировать созданные HIP-объекты в HIP-профили.

3. В **Правила трафика** → **Межсетевой экран** → **FORWARD** создать и включить правило с использованием одного или нескольких профилей, созданных в пункте 2.

Проверка профилей происходит каждые 15 минут.

Примеры использования

Запрет доступа к сети устройствам без профиля

Устройствам, которые не прошли проверку на соответствие ни одному из созданных HIP-профилей, назначается специальный HIP-профиль **Устройство без профиля**. Доступ таких устройств к сети можно ограничить правилом **Межсетевого экрана**. Для этого:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

2. Создайте и включите правило вида:

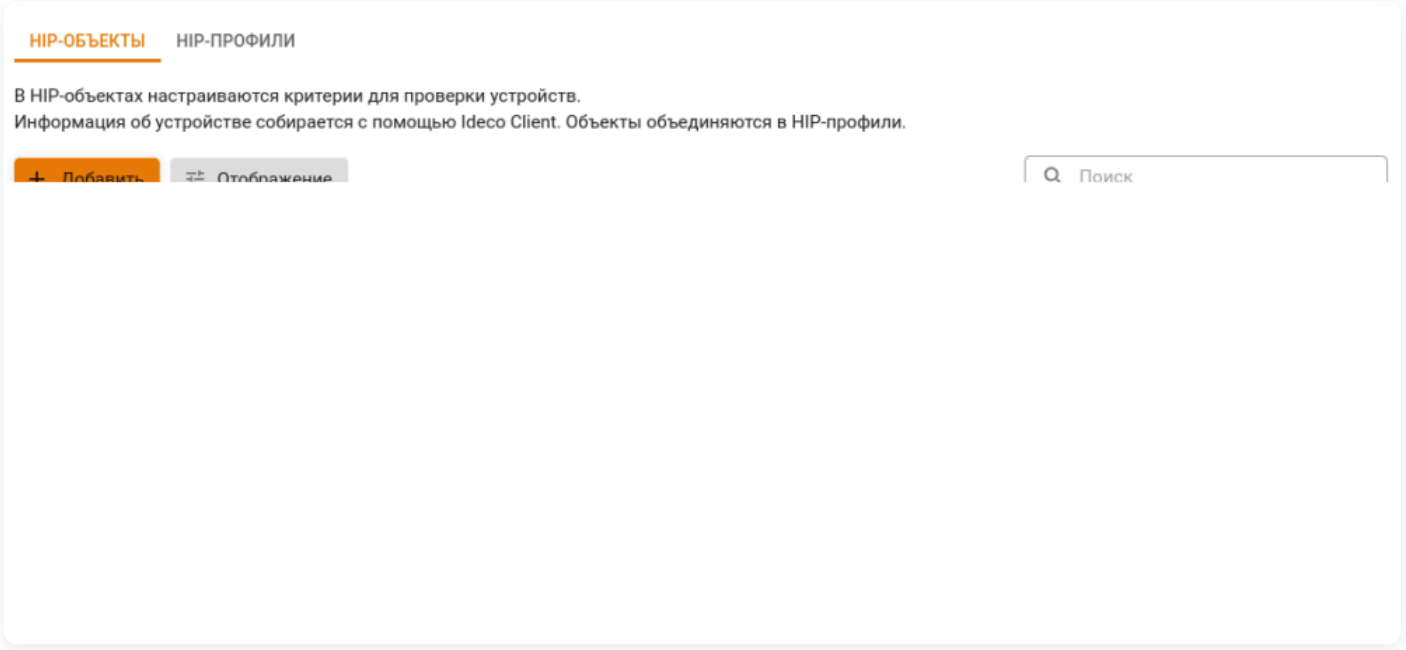
Если в таблице правил **Межсетевого экрана** выше запрещающего правила находится другое правило, которому соответствует трафик одного или нескольких устройств без профиля (например, правило для пользователя или группы пользователей без указания HIP-

профиля), то к трафику будет применено правило, расположенное выше в таблице. Пример:

Ограничение доступа устройств к сети

В качестве примера настроим **Межсетевой экран** так, чтобы пользователи имели доступ к сети, только если устройства пользователей соответствуют HIP-профилю `Profile1`. Для этого:

1. Перейдите в **Пользователи** → **Профили устройств** → **HIP-объекты** и создайте требуемые HIP-объекты:



2. Перейдите на вкладку **HIP-профили** и создайте профиль с созданными ранее HIP-объектами:

3. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**, создайте и включите правило, разрешающее доступ к сети всем пользователям, чьи устройства соответствуют профилю `Profile1`:

4. Ниже создайте и включите правило, запрещающее весь трафик:

В результате трафик всех пользователей, чьи устройства соответствуют HIP-профилю `Profile1`, подпадет под разрешающее правило. Остальной трафик подпадет под запрещающее правило.

Полезные ссылки

- **Как безопасно подключить удаленного подрядчика**

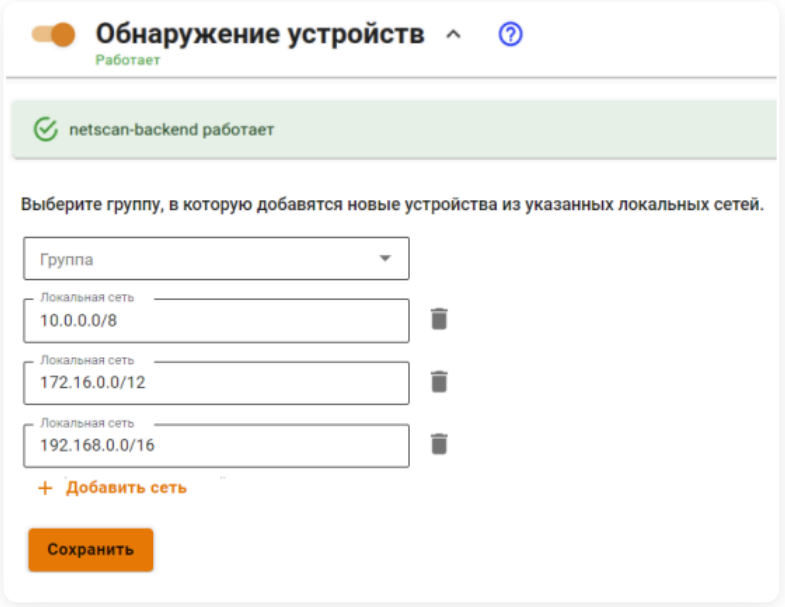
Обнаружение устройств

API

Функциональность доступна в **Классическом** и **Системном контекстах**.

Название службы раздела **Обнаружение устройств**: `ideco-netscan-backend`.
Список служб для других разделов доступен по ссылке.

Модуль **Обнаружение устройств** автоматически создает пользователей с авторизацией по IP-адресу и MAC-адресу. Если модуль включен, то при попытке выхода в интернет будет создана учетная запись с именем, соответствующим NetBIOS-имени устройства:



- **Группа** - группа для автоматически добавленных пользователей.
- **Локальная сеть** - список сетей, для которых попытка выхода в интернет будет активировать создание пользователя.

Примечание

При необходимости можно ограничить локальные сети, пользователи из которых будут автоматически добавлены и авторизованы на Ideco NGFW Novum. Например, так можно авторизовать пользователей, подключающихся по Wi-Fi или другой открытой сети.

Особенности работы модуля **Обнаружение устройств**:

1. Модуль не сканирует сети в поисках устройств, а работает в пассивном режиме.

2. Если NetBIOS-имя определить не удалось, то в поле **Имя пользователя** будет записан IP-адрес найденного устройства.

3. Если в базе пользователей на Ideco NGFW Novum уже есть учетная запись с логином, равным NetBIOS-имени машины, то NGFW использует данные пользователя без обновления параметров пользователя (в том числе IP- или MAC-адреса).

4. Для локальных адресов в одном Ethernet-сегменте модуль создает авторизацию по MAC-адресу. Если устройство находится в локальной сети за роутером, то модуль создает авторизацию по IP-адресу.

Примечание

При подключении к NGFW как к прокси-серверу система обнаружения устройств работать не будет.

Мониторинг

В разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

Сессии администраторов

Список всех сессий администраторов в Ideco NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS

Перейти >

Сессии пользователей

Список всех сессий пользователей, которые авторизовались в NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS

Перейти >

Сессии ЛК

Список активных сессий в личном кабинете Ideco NGFW

Перейти >

Графики загруженности

Статистика по авторизованным пользователям, количеству VPN-подключений, загрузки процессора и диска

Перейти >

Монитор трафика

Таблица, содержащая информацию о трафике, проходящем через Ideco NGFW в режиме реального времени

Перейти >

Проверка IP/домена

Поиск IP-адреса и домена в базах объектов и GeoIP

Перейти >

Telegram-бот

Настройка оповещений от Ideco Monitoring Bot

Перейти >

SNMP

В статье описана настройка доступа к Ideco NGFW по протоколу SNMP

Перейти >

Zabbix-агент

Интеграция Zabbix-агента в Ideco NGFW

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Сессии администраторов

API

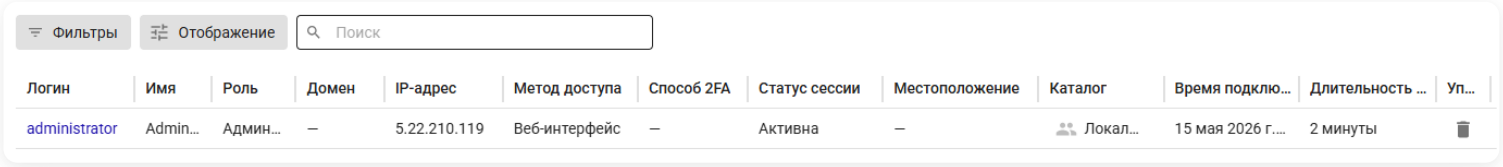
Функциональность доступна в **Классическом** и **Системном контекстах**.

Раздел содержит список всех сессий администраторов в NGFW, включая локальных, из Active Directory, ALD PRO, FreeIPA и RADIUS.

Сессии администраторов, подключенных через Ideco Center, не отображаются в разделе.

Сессия с IP-адресом 127.0.0.1 - сессия администратора, работающего в локальном меню сервера.

Таблица сессий авторизованных администраторов в NGFW:



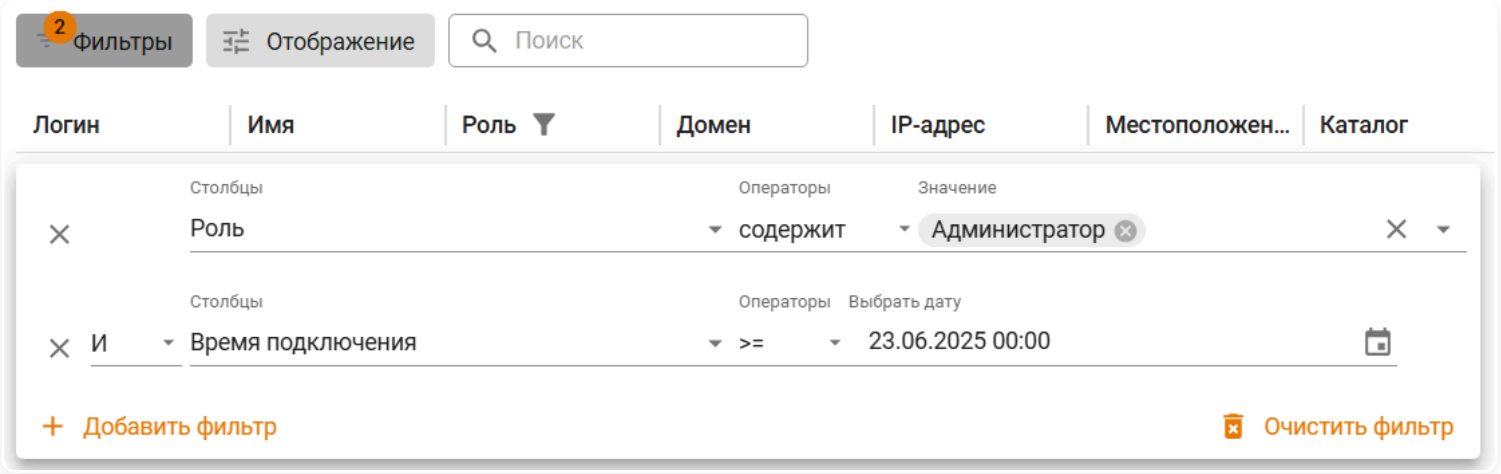
- **Логин** - логин администратора.
- **Имя** - имя администратора.
- **Роль** - возможные роли: Администратор, Только просмотр, Администратор ИБ, Администратор межсетевого экрана, Администратор настройки доступов, Просмотр отчетов, Создание отчетов.
- **Домен** - доменное имя, если администратор импортирован из Active Directory, ALD PRO или FreeIPA. В ином случае в ячейке прочерк.
- **IP-адрес** - IP-адрес устройства, с которого авторизован администратор.
- **Метод доступа** - способ подключения администратора: SSH, Веб-интерфейс или Локальное меню.
- **Способ 2FA** - второй фактор авторизации администратора, если настроен.
- **Местоположение** - географическое местоположение администратора.
- **Каталог** - тип администратора в зависимости от источника добавления: Локальная группа, AD, ALD, IPA, RAD.
- **Время подключения** - момент запуска сессии с указанием даты в формате день/месяц/год и времени в формате час/минута.
- **Длительность сессии** - продолжительность сессии администратора с момента запуска, указанного в столбце **Время подключения**.
- **Управление** - возможность деавторизовать любого администратора из интерфейса Ideco NGFW Novum.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока администратор будет автоматически деавторизован.

В столбце **Управление** администратор может деавторизовать самого себя.

Фильтрация таблицы

При наличии большого количества сессий администраторов воспользуйтесь кнопкой **Фильтры**. Фильтрация возможна по всем столбцам, кроме **Длительность сессии** и **Управление**, а также с использованием нескольких переменных:



При использовании фильтра по **Времени подключения** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные за 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

Полезные ссылки

- **Администраторы**
- **Действия администраторов**

Сессии пользователей

Классический контекст | Высокопроизводительный контекст | API

Раздел содержит список всех сессий пользователей, которые авторизовались в Ideco NGFW Novum, включая локальных, из Active Directory, ALD PRO, FreeIPA и RADIUS.

Количество сессий в мониторинге не является показателем занимаемых лицензий, так как под одной пользовательской учетной записью возможна одновременная авторизация до пяти устройств, что учитывается как одна лицензия.

Таблица сессий авторизованных пользователей в Ideco NGFW Novum:



Статусы подключения пользователей

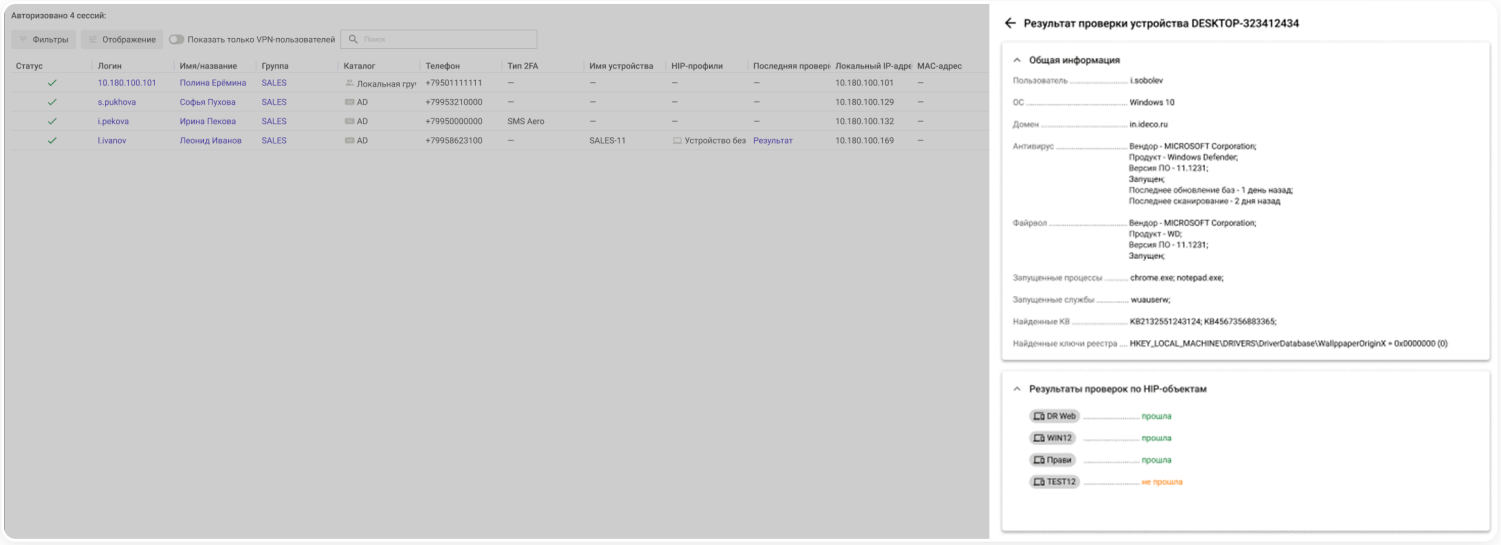
- **Подключено**. Пользователь авторизован.

- **Ожидает второй фактор авторизации**. Пользователь создал и активировал VPN-подключение, но не прошел двухфакторную аутентификацию (подробнее в статье).

- **Превышен лимит лицензии**. Данная сессия заблокирована. Появляется, если превышено количество пользователей по лицензиям или у пользователя уже есть пять активных сессий.

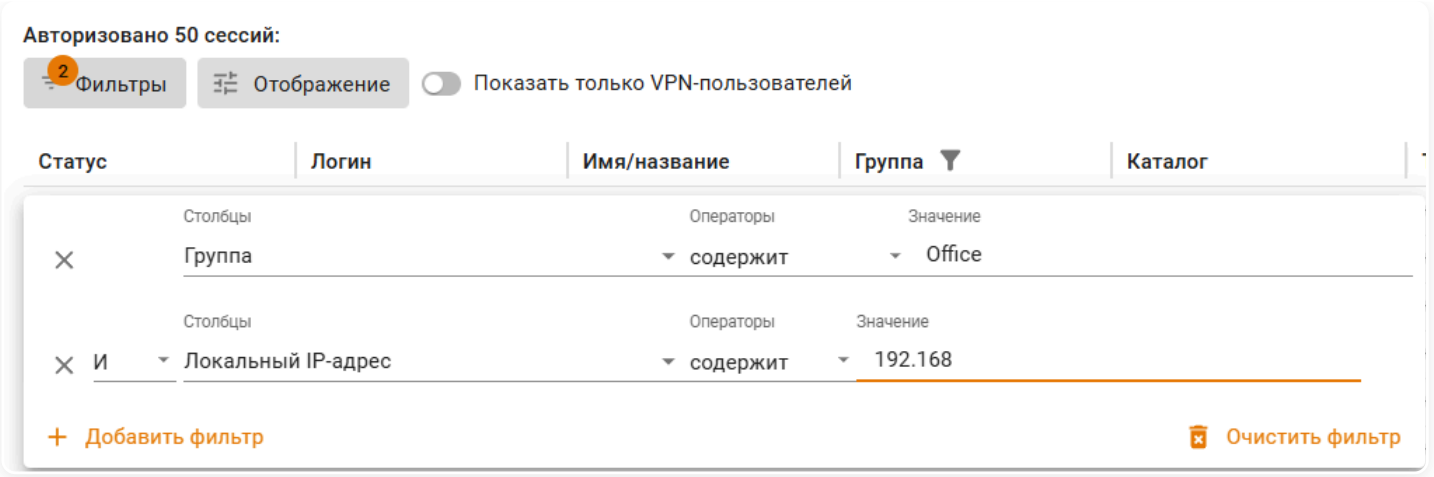
- **Сессия удаляется**. Появляется при разрыве сессии с динамическим IP-адресом. Сессия с таким статусом будет удалена через 30 секунд.

Для просмотра результата проверки устройства, подключенного через Ideco Client, нажмите на **Результат** в столбце **Последняя проверка**. Откроется соответствующее окно с общей информацией и результатами проверок по HIP-объектам:



Фильтрация таблицы

При наличии большого количества авторизованных пользователей в таблице воспользуйтесь кнопкой **Фильтры**. Фильтрация данных возможна по всем столбцам, а также с использованием нескольких переменных:



При использовании фильтра по **Времени подключения** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные за 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

Опция **Показать только VPN-пользователей** отображает в таблице журнала только тех пользователей, которые подключены к NGFW через VPN.

Полезные ссылки

- **Авторизация пользователей**

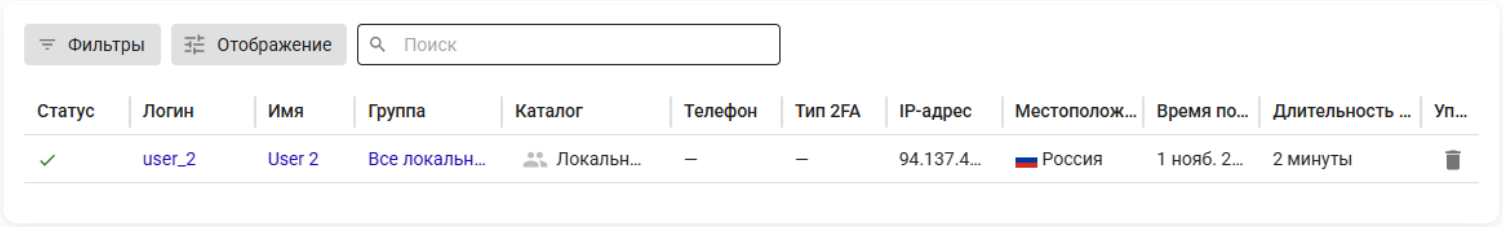
Сессии ЛК

Классический контекст | Высокопроизводительный контекст | API

Сессии ЛК - таблица активных сессий в личном кабинете Ideco NGFW Novum. Для аутентификации пользователей используется логин и пароль, возможно использование технологии 2FA (двухфакторная аутентификация). Доступ к ресурсам в локальной сети пользователи получают через веб-браузер по HTTPS без установки отдельного туннельного соединения (технология SSL VPN).

Записи в журнале появляются после авторизации пользователей в личном кабинете, настроенном в **Сервисы** → **ЛК/Портале SSL VPN**.

Записи доступны для управления и остаются в таблице до завершения сессии:



Помимо общих сведений об учетной записи пользователя (логин, имя, группа, каталог и телефон), таблица активных сессий содержит столбцы:

- **Статус** - доступные значения: авторизован, 2FA (ожидает 2FA, генерация TOTP для прохождения 2FA).
- **Тип 2FA** - метод двухфакторной аутентификации.
- **IP-адрес** - IP-адрес, с которого произведена начальная аутентификация сессии в ЛК.
- **Местоположение** - страна IP-адреса, с которого произведена начальная аутентификация сессии в ЛК. Значение пустое, если:
  - Отсутствует лицензия.
  - Невозможно получить базу GeoIP.
  - IP-адрес локальный.
- **Время подключения** - момент аутентификации в ЛК с указанием даты в формате день/месяц/год и времени в формате час/минута.
- **Время в сети** - длительность сессии аутентификации в ЛК, разница между временем подключения и текущим временем.
- **Управление** - доступно только действие **Отключить** для завершения сессии аутентификации.

IP-адрес и **Местоположение** могут меняться, т.к. сессия авторизации привязана к cookie и браузеру, а не к IP-адресу.

Столбцы в таблице можно отрегулировать кнопкой **Отображение**.

Чтобы найти нужную сессию, воспользуйтесь одним из способов:

- Нажмите кнопку **Фильтры**, выберите один из параметров поиска.

При использовании фильтра по **Времени подключения** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные за 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Графики загруженности

Классический контекст | Высокопроизводительный контекст

Модуль **Графики загруженности** позволяет просматривать данные о состоянии Ideco NGFW Novum в виде графиков в **режиме реального времени**. Горизонтальной шкалой графика всегда является **время** (в зависимости от выбранного интервала). Данные хранятся до 90 дней.

В случае активации резервной ноды кластера, данные с прежней активной ноды остаются доступными (хранятся 90 дней), но не передаются резервной ноде.

При отключении опции **Сбор метрик** в некоторых графиках может наблюдаться несогласованность данных по времени. Это связано с внутренней реализацией модуля.

Раздел **Графики загруженности** состоит из вкладок:

Система

Содержит информацию:

- Количество авторизованных пользователей.
- Процент загрузки процессора (максимальное значение загрузки процессора - 100%).
- Температура процессора.
- Частота процессора.
- Объем используемой оперативной памяти в ГБ.
- Среднее значение загрузки системы.
- Количество всех установленных сетевых соединений.

Сеть

Содержит суммарную информацию о входящем и исходящем трафике, передаваемом через Ideco NGFW по всем интерфейсам раздела Сетевые интерфейсы. Данные отображаются за определенный период времени.

Эта статистика может помочь в настройке резервирования каналов и балансировки.

Диски

Содержит информацию об общей загруженности системного диска (в процентах) и свободном месте в корневой файловой системе (в ГБ) за определенный промежуток времени. Дает оценку интенсивности использования диска.

Информация о свободном и занятом объеме на диске также отображается при создании бэкапа в **Управление сервером → Бэкапы**.

VPN

Содержит информацию о количестве подключений пользователей по протоколам L2TP/IPsec, SSTP, IKEv2 и Ideco Client.
Инструкция по VPN-подключению пользователей доступна по ссылке.

IPsec

Содержит информацию о входящих, исходящих IPsec-подключениях Ideco NFGW. Показывает загрузку входящего и исходящего IPsec-канала.

WCCP GRE

Содержит информацию о входящей скорости GRE-туннелей.
Особенности протокола GRE не позволяют определить исходящую скорость для GRE-туннелей.

ГОСТ VPN

Содержит информацию о входящих и исходящих соединениях ГОСТ VPN в Ideco NFGW. Отображает график входящего и исходящего трафика за выбранный период времени.

Инструкция по настройке ГОСТ VPN доступна по ссылке.

VCE

Содержит информацию о загруженности всех VCE, для которых были назначены ресурсы (ядра процессора и оперативная память).

Инструкция по настройке VCE доступна по ссылке.

Полезные ссылки

- **Сетевые интерфейсы**
- **Профили next hop**
- **Кластеризация**
- **Бэкапы**
- **ГОСТ VPN**
- **Инструкции по созданию VPN-подключений**

Монитор трафика

Классический контекст | Высокопроизводительный контекст | API

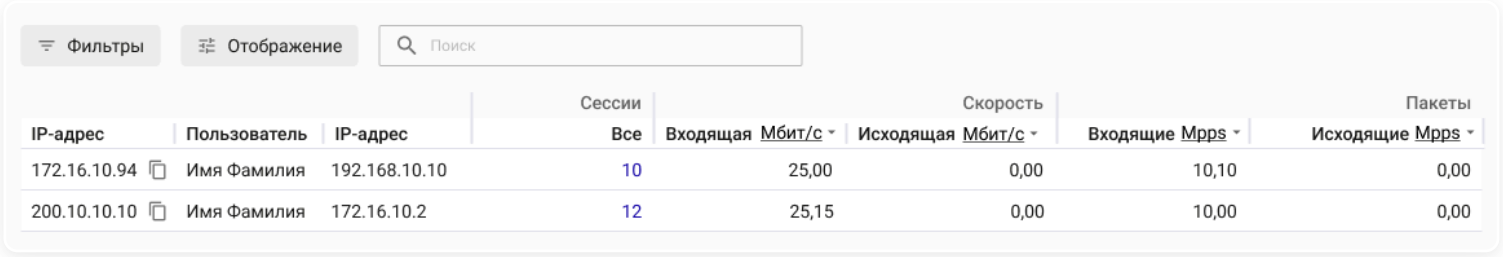
В разделе **Мониторинг → Монитор трафика** можно просматривать данные о трафике (входящая/исходящая скорость, количество сессий), проходящем через Ideco NGFW Novum в режиме реального времени.

Для работы **Монитора трафика** необходимо включить Контроль приложений.

Раздел **Монитор трафика** состоит из вкладок:

По источнику трафика

Вкладка **По источнику трафика** позволяет отслеживать активность пользователей сети и выявлять пользователей, нагружающих канал трафиком:



IP-адрес	Пользователь	IP-адрес	Сессии: Все	Скорость: Входящая Мбит/с	Скорость: Исходящая Мбит/с	Пакеты: Входящие Mpps	Пакеты: Исходящие Mpps
172.16.10.94	Имя Фамилия	192.168.10.10	10	25,00	0,00	10,10	0,00
200.10.10.10	Имя Фамилия	172.16.10.2	12	25,15	0,00	10,00	0,00

Для просмотра информации об активности определенного узла локальной сети нажмите на количество сессий в столбце **Сессии**:

Откроется таблица с подробной информацией:

По приложениям

Вкладка **По приложениям** позволяет отслеживать активность приложений.

Например, если пользователь не загружает канал трафиком, но в таблице **По источнику трафика** присутствует большое количество пакетов данных, то на вкладке **По приложениям** можно выявить приложение с подозрительной активностью:

Для просмотра информации об активности определенного приложения нажмите на **количество сессий** в столбце **Сессии**:

Откроется таблица с подробной информацией:

Фильтрация таблицы

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**. Фильтрация возможна по всем столбцам, кроме **Сессии**, **Скорость** и **Объект**, а также с использованием нескольких переменных.

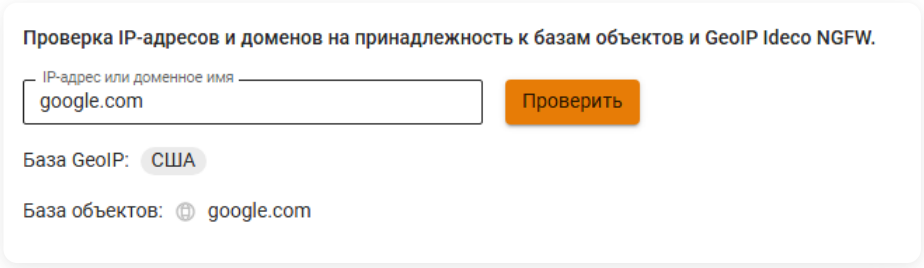
Полезные ссылки

- **Контроль приложений**

Проверка IP/домена

Классический контекст | Высокопроизводительный контекст | API

В разделе можно проверить IP-адрес или домен на принадлежность к базам объектов и GeoIP. Для проверки введите IP-адрес или доменное имя в поиск. Система проверяет в базах объектов и GeoIP. В результатах поиска отображается:



- Страна регистрации.
- Объект, где указан IP-адрес или доменное имя.

Блокировки WAF

Классический контекст | Высокопроизводительный контекст | API

Раздел содержит сведения о текущих IP-адресах, заблокированных правилами Web Application Firewall (WAF). Таблица обновляется каждые 5 секунд:

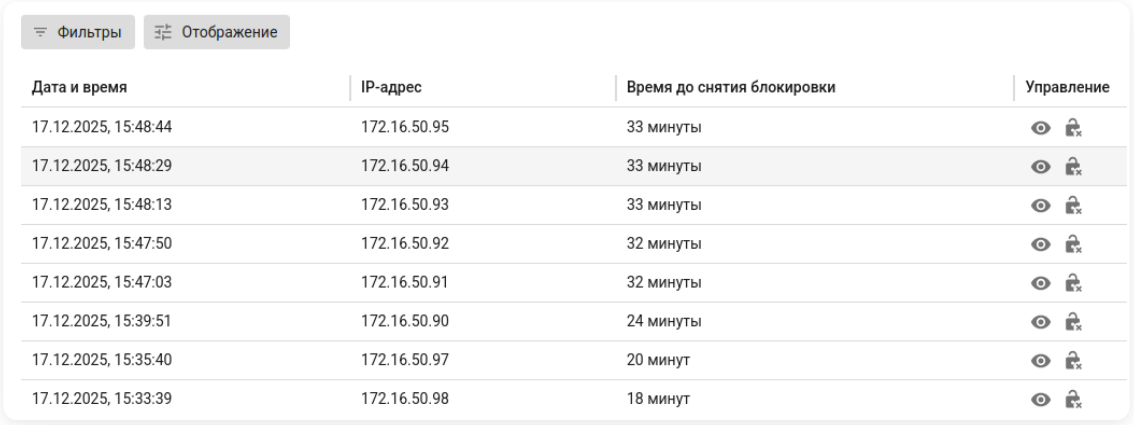


Таблица содержит столбцы:

- **Дата и время** - момент фиксации события блокировки в формате `31 октября 2025, 21:18`.
- **IP-адрес** - заблокированный IP-адрес.
- **Время до снятия блокировки** - оставшийся интервал до автоматического удаления записи из списка в формате `5 минут 35 секунд`.
- **Управление** - доступные действия:
  - - переход к соответствующей записи в журнале События безопасности. При переходе в журнал отображается только запись, вызвавшая блокировку.
  - - снятие блокировки с выбранного IP-адреса. IP-адреса, разблокированные вручную, удаляются из таблицы сразу после снятия блокировки.

IP-адреса, заблокированные WAF, помещаются в список на 40 минут. По истечении этого времени блокировка снимается автоматически и запись удаляется.

Сброшенные ранее блокировки будут восстановлены после перезагрузки NGFW Novum, если критерии блокировки по-прежнему выполняются.

Telegram-бот

Классический контекст | Высокопроизводительный контекст

Ideco Monitoring Bot - это Telegram-бот, который отправляет уведомления о событиях в Ideco NGFW Novum (уведомления из 🔔):

- В личные сообщения.
- В беседы, где два и более участников (groups).

Привязка бота и настройка оповещений Ideco Monitoring Bot осуществляется в MY.IDECO.

Привязка Ideco Monitoring Bot

К личному аккаунту

1. Откройте чат с ботом: @ideco_monitor_bot.
2. Напишите боту `/start`.
3. Скопируйте код привязки к аккаунту.
4. Перейдите в раздел **Ideco Monitoring Bot** в MY.IDECO.
5. Нажмите **Привязать аккаунт**.
6. Введите код в поле **Токен Telegram-аккаунта** и нажмите **Привязать**:



Уведомления начнут приходить в Telegram-аккаунт.

К беседе



При подключении Ideco Monitoring Bot к беседе нельзя использовать подсказки для команд, поскольку требуется ввод команды `/start` вручную.

1. Перейдите в группу в Telegram и добавьте бота: @ideco_monitor_bot.
2. Напишите `/start` в группе.
3. Скопируйте код привязки к аккаунту.
4. Перейдите в раздел **Ideco Monitoring Bot** в MY.IDECO.
5. Нажмите **Привязать аккаунт**.
6. Введите код в поле **Токен Telegram-аккаунта** и нажмите **Привязать**:



Уведомления начнут приходить в Telegram-аккаунт.

Настройка оповещений Ideco Monitoring Bot

В личном кабинете можно настроить оповещения от Ideco Monitoring Bot для каждого привязанного аккаунта или беседы. Для настройки оповещений:

1. Перейдите в раздел **Ideco Monitoring Bot** в MY.IDECO.
2. Выберите аккаунт или группу и нажмите 🔔.
3. Выберите уведомления, которые хотели бы получать.

Если требуется временно отключить отправку уведомлений, нажмите на  . Оповещения перестанут приходить, пока снова не нажмете на эту иконку.

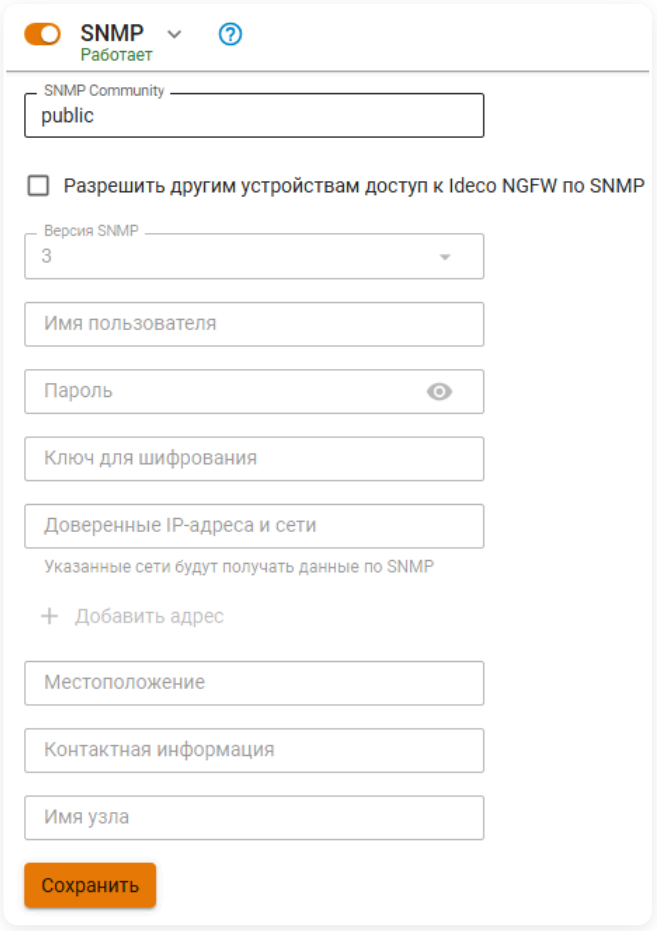
SNMP

Классический контекст | Высокопроизводительный контекст | API

SNMP - это протокол для управления и мониторинга сетевых устройств, таких как маршрутизаторы, коммутаторы и межсетевые экраны. Модуль **SNMP** обеспечивает мониторинг работы Ideco NGFW Novum по протоколу SNMP версий 1/2c и 3.

Настройка подключения

Для подключения по протоколу SNMP в **Мониторинг** → **SNMP** включите опцию и заполните поля:



Версия 1/2c

- **Имя пользователя**.
- **Пароль** (минимальное количество символов - 8).
- **Доверенные IP-адреса и сети**.

Поля **Местоположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.

Версия 3

- **Имя пользователя**.
- **Пароль** (минимальное количество символов - 8).
- **Ключ шифрования**.
- **Доверенные IP-адреса и сети**.

Поля **Местоположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.

Рекомендуем: укажите на сервере, с которым будет установлено соединение по SNMPv3, алгоритмы **Auth Algorithm MD5** и **Crypto Algorithm AES**.

Поле **SNMP community** для SNMPv3 необязательно для заполнения.

Устройства в указанных доверенных сетях получат доступ к данным Ideco NGFW Novum после заполнения поля **Доверенные IP-адреса и сети**.

Как узнать информацию о MIB (Management Information Base)

MIB (Management Information Base) - иерархическая база данных, содержащая описание управляемых объектов сетевого устройства, доступных для мониторинга и управления через протокол SNMP.

После настройки подключения по протоколу SNMP в директории `/usr/share/snmp/mibs/` будут размещены MIB-файлы с описанием всех MIB-модулей.

Список MIB-файлов

- AGENTX-MIB.txt
- IANAifType-MIB.txt
- IPV6-MIB.txt
- NET-SNMP-PASS-MIB.txt
- SMUX-MIB.txt
- SNMP-USM-AES-MIB.txt
- TCP-MIB.txt
- BRIDGE-MIB.txt
- IANA-LANGUAGE-MIB.txt
- IPV6-TCP-MIB.txt
- NET-SNMP-TC.txt
- SNMP-COMMUNITY-MIB.txt
- SNMP-USM-DH-OBJECTS-MIB.txt
- TRANSPORT-ADDRESS-MIB.txt
- DISMAN-EVENT-MIB.txt
- IANA-RTPROTO-MIB.txt
- IPV6-TC.txt
- NET-SNMP-VACM-MIB.txt
- SNMP-FRAMEWORK-MIB.txt
- SNMP-USM-HMAC-SHA2-MIB.txt
- TUNNEL-MIB.txt
- DISMAN-SCHEDULE-MIB.txt
- IF-INVERTED-STACK-MIB.txt
- IPV6-UDP-MIB.txt
- NETWORK-SERVICES-MIB.txt
- SNMP-MPD-MIB.txt
- SNMPv2-CONF.txt
- UCD-DEMO-MIB.txt
- DISMAN-SCRIPT-MIB.txt
- IF-MIB.txt
- LM-SENSORS-MIB.txt
- NOTIFICATION-LOG-MIB.txt
- SNMP-NOTIFICATION-MIB.txt
- SNMPv2-MIB.txt
- UCD-DISKIO-MIB.txt
- EtherLike-MIB.txt
- INET-ADDRESS-MIB.txt
- MTA-MIB.txt
- RFC1155-SMI.txt
- SNMP-PROXY-MIB.txt
- SNMPv2-SMI.txt
- UCD-DLMOD-MIB.txt

- HCNUM-TC.txt
- IP-FORWARD-MIB.txt
- NET-SNMP-AGENT-MIB.txt
- RFC1213-MIB.txt
- SNMP-TARGET-MIB.txt
- SNMPv2-TC.txt
- UCD-IPFWACC-MIB.txt
- HOST-RESOURCES-MIB.txt
- IP-MIB.txt
- NET-SNMP-EXAMPLES-MIB.txt
- RFC-1215.txt
- SNMP-TLS-TM-MIB.txt
- SNMPv2-TM.txt
- UCD-SNMP-MIB.txt
- HOST-RESOURCES-TYPES.txt
- IPV6-FLOW-LABEL-MIB.txt
- NET-SNMP-EXTEND-MIB.txt
- RMON-MIB.txt
- SNMP-TSM-MIB.txt
- SNMP-VIEW-BASED-ACM-MIB.txt
- UDP-MIB.txt
- IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt
- IPV6-ICMP-MIB.txt
- NET-SNMP-MIB.txt
- SCTP-MIB.txt
- SNMP-USER-BASED-SM-MIB.txt
- SQUID-MIB.txt

Каждый MIB-файл написан на специальном языке описания SMI (Structure of Management Information). Этот синтаксис формализован и не всегда человекочитаем. Для удобного просмотра дерева MIB подставьте имя файла без расширения в URL сайта с визуализацией - https://mibs.observium.org/, например:

- https://mibs.observium.org/mib/IF-MIB
- https://mibs.observium.org/mib/SNMP-USER-BASED-SM-MIB
- https://mibs.observium.org/mib/TCP-MIB

Более подробную информацию о конкретном MIB-объекте можно получить через поиск. Можно искать как по имени объекта (например: `sysUpTime`), так и по его числовому OID (например: `.1.3.6.1.2.1.1.3`).

Полезные ссылки

- **Как подключить Ideco NGFW к Zabbix Server по SNMP**

Zabbix-агент

Классический контекст | Высокопроизводительный контекст | API

Zabbix - система с открытым исходным кодом для мониторинга параметров сети, состояния и работоспособности серверов.

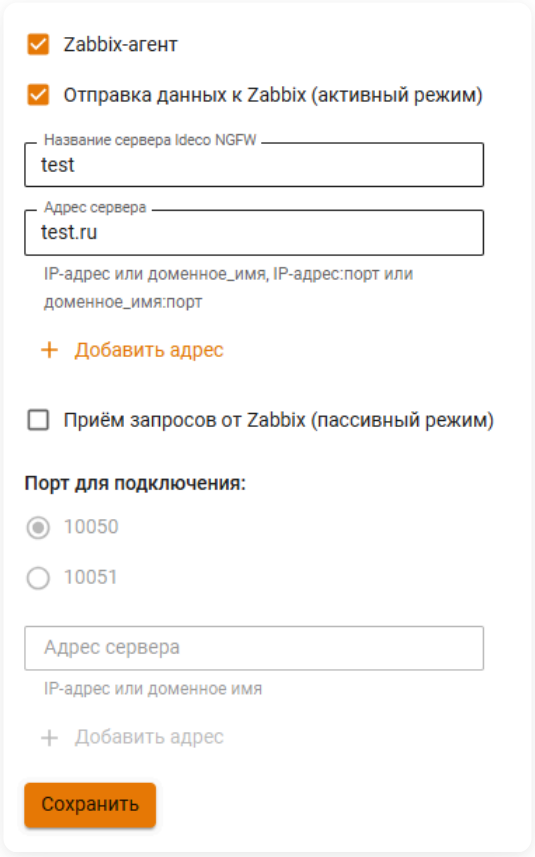
Настройка Zabbix-агента

Для работы системы мониторинга Zabbix в Ideco NGFW Novum активируйте опцию **Zabbix-агент** после настройки интеграции с Zabbix.

Интеграция с системой мониторинга Zabbix возможна в двух режимах: **Активный** и **Пассивный**.

Активный

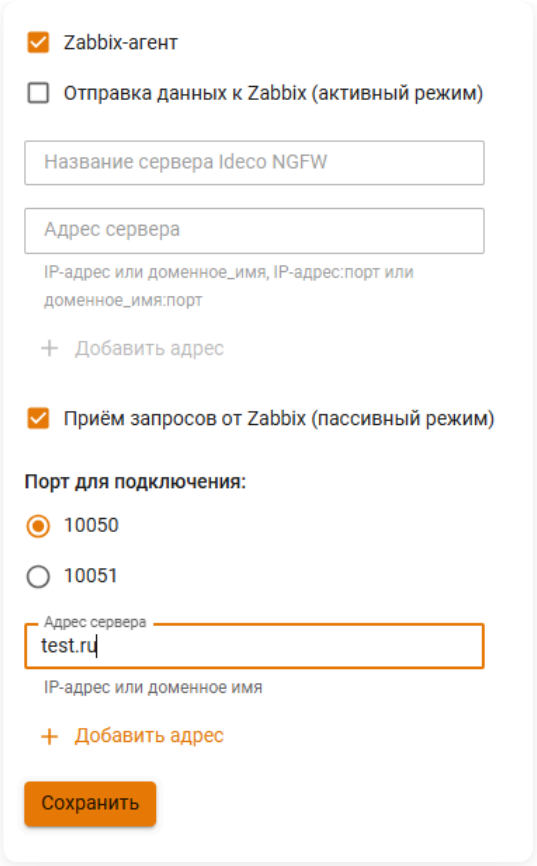
Соединение с Zabbix-сервером происходит со стороны Ideco NGFW Novum. Для настройки заполните поля:



- **Имя сервера Ideco NGFW Novum** - имя, которое будет отображаться на сервере мониторинга.
- **Адрес сервера** - IP-адрес, доменное имя, либо `IP-адрес:порт`, `доменное имя:порт`, если используется нестандартный для Zabbix входящий порт. Для добавления еще одного адреса нажмите **Добавить адрес**.

Пассивный

Подключение происходит со стороны Zabbix-сервера. Для настройки заполните поля:



- **Порт для подключения** - выберите 10050 или 10051 порт.
- **Адрес сервера** - IP-адрес или доменное имя Zabbix-сервера. Для добавления еще одного адреса нажмите **Добавить адрес**.

Zabbix-сервер должен находиться внутри локальной сети Ideco NGFW Novum. Подключение мониторинга возможно только к локальным интерфейсам (с ролью LAN). Это ограничение обусловлено системными правилами **Межсетевого экрана**, которые не отображаются в веб-интерфейсе, но имеют наивысший приоритет. Системные правила разрешают соединения на порты 10050/TCP и 10051/TCP только на локальных интерфейсах и блокируют их на внешних.

Используйте стандартные шаблоны Zabbix для Linux:

- **Linux by Zabbix agent** - для пассивного режима.
- **Linux by Zabbix agent active** - для активного режима.

Zabbix-агент передает стандартный набор метрик, предусмотренный шаблоном Zabbix для Linux. В набор входят данные по процессору, памяти, дискам, файловым системам, сетевым интерфейсам и основным системным параметрам. Количество метрик зависит от количества интерфейсов и дисков.

Полезные ссылки

- **Официальная страница Zabbix**
- **Zabbix как готовое решение**
- **Установка Zabbix**
- **Как подключить Ideco NGFW к Zabbix Server по SNMP**

Правила трафика

В разделе описывается настройка служб, определяющих основные правила фильтрации трафика в Ideco NGFW.

Межсетевой экран

Создание правил Межсетевого экрана, применение профилей безопасности, тестирование правил, настройка предварительной и аппаратной фильтрации

Перейти >

Контент-фильтр

Создание правил Контент-фильтра, пользовательских категорий, морфологический анализ

Перейти >

Ограничение скорости

Настройка ограничения скорости входящего интернет-трафика для пользователей сети

Перейти >

Предотвращение вторжений

Описание групп сигнатур, создание пользовательских сигнатур

Перейти >

Исключения

Настройка исключений для предотвращения обработки трафика в разделах **Предотвращения вторжений**, **Контроля приложений** и **Ограничение скорости**

Перейти >

Объекты

Создание объектов для использования в правилах **Межсетевого экрана**, **Контент-фильтра**, **Контроля приложений**, **Маршрутизации**

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Межсетевой экран

Классический контекст | Высокопроизводительный контекст | API

Для настройки Межсетевого экрана перейдите в раздел Правила трафика → Межсетевой экран.

Название службы раздела **Межсетевой экран**: `ideco-firewall-rest`, `ideco-firewall-backend`, `ideco-apply-manual-blocklist`, `ideco-fw-stats`, `ideco-acl-rest`, `ideco-acl-backend`, `ideco-nflog`.

Список служб для других разделов доступен по ссылке.

Межсетевой экран - средство управления трафиком на сервере (межсетевой экран). Поддерживает фильтрацию пакетов с контролем состояния соединений (Stateful Inspection) - решение о блокировке принимается на все соединение.

Межсетевой экран анализирует заголовки IP-пакетов и TCP-сегментов, проходящих через интерфейсы сервера, и фильтрует трафик на основании параметров заголовков (IP-адреса, TCP/UDP-порты и IP-протокол).

С помощью **Межсетевого экрана** можно создавать наборы правил, которые разграничивают трафик между различными сетями: локальными, VPN и публичными (интернет). В Ideco NGFW Novum предусмотрены преднастроенные и автоматически включаемые системные правила. Пользовательские правила используются для фильтрации трафика локальной сети и публикации ресурсов.

Рекомендуем выпускать весь пользовательский трафик через Ideco NGFW для оптимальной работы политик безопасности (модулей **Контроль приложений** и **Предотвращение вторжений**).

Межсетевой экран не предназначен для решения задач контроля доступа к ресурсам по URL, доменному имени или типу контента на веб-сайтах. Эти задачи решаются с помощью **Контент-фильтра**.

Фильтрация трафика

Межсетевой экран использует для фильтрации трафика как отдельные интерфейсы, так и зоны - логические объединения сетевых интерфейсов. Преимущества такого подхода:

- Гибкость управления правилами при большом количестве интерфейсов.
- Упрощение процесса добавления/удаления интерфейсов без необходимости редактирования множества правил.
- Возможность выбора удобных названий для зон (например, **Разработчики**, **Гости**), что делает правила более читаемыми.

Для работы DPI/IPS в правилах **Межсетевого экрана** можно подключить **Профили безопасности**, создав разрешающее правило с включенной проверкой через **Контроль приложений**, систему **Предотвращения вторжений** . Профили настраиваются в разделе **Профили безопасности**.

Настройка и управление правилами

Настройка производится в **Правила трафика** → **Межсетевой экран**. На вкладках раздела добавляются правила управления трафиком, которые отображаются в таблицах **Межсетевого экрана**. При наличии большого количества правил используйте кнопку **Фильтры**.

Включите опцию **Счетчик срабатываний** для подсчета количества срабатываний правил **Межсетевого экрана**. После включения опции в таблице появится соответствующий столбец.

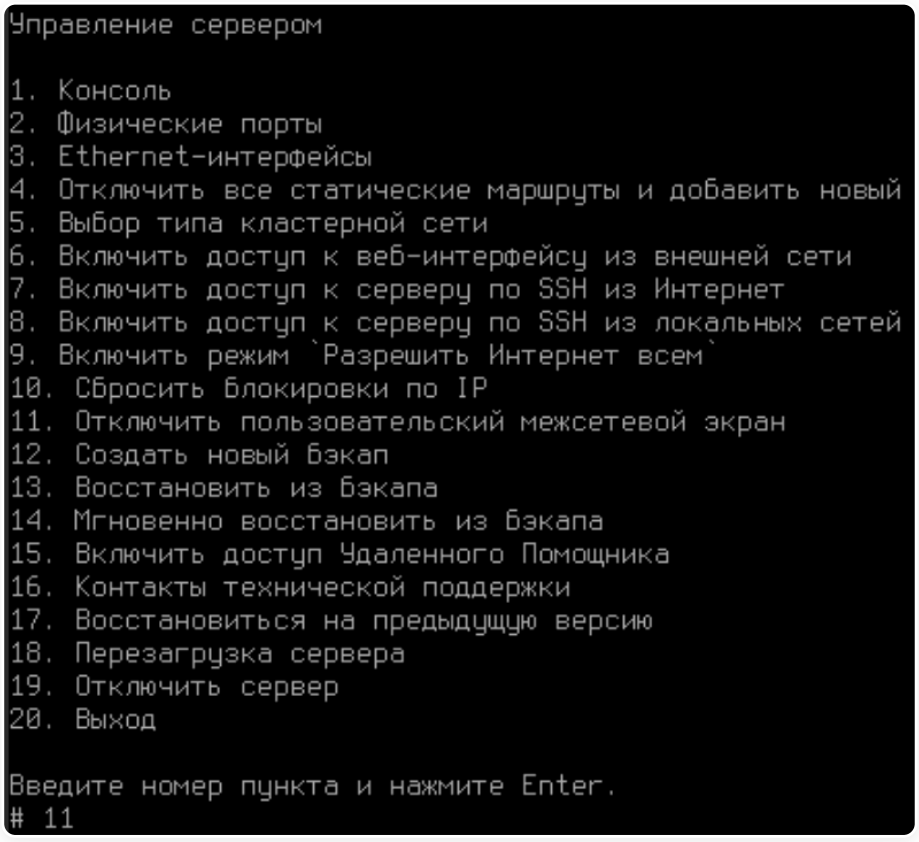
Включить опцию можно, нажав на **Отображение данных**.

Особенности

- Включение режима удаленного помощника изменяет таблицу правил **Межсетевого экрана**, разрешая подключение по SSH из локальных и внешних сетей.
- В Ideco NGFW Novum включены connection tracking helpers для протоколов: ftp, sip, netbios-ns, pptp, h323. Для других протоколов, использующих несколько портов при установлении соединения, работа через NAT не гарантируется.
- При использовании зон в **Межсетевом экране** следует учесть, что одна зона не может содержать более 64 интерфейсов, настроенных в разделе **Сервисы** → **Сетевые интерфейсы**, а также IPsec- и VPN-подключений.

Устранение проблем

В случае создания некорректных правил (например, запрет доступа в веб-интерфейс Ideco NGFW) в локальном меню сервера выберите пункт **Отключить пользовательский межсетевой экран** и нажмите Enter:



При отключении пользовательского межсетевого экрана в веб-интерфейсе системные правила продолжают работу.

Полезные ссылки

- **Таблицы межсетевого экрана (FORWARD, DNAT, INPUT и SNAT)**
- **Примеры создания правил межсетевого экрана**
- **Логирование**
- **Аппаратная фильтрация**
- **Тестирование правил**
- **Предварительная фильтрация**
- **Доступ из внешних сетей без NAT**
- **Блокировка популярных ресурсов**
- **Как разрешить доступ к ресурсам в ограниченной сети**
- **Портмаппинг (проброс портов, DNAT)**
- **Настройка совместной работы ViPNet Координатор с Ideco NGFW**

Профили безопасности

- **Контроль приложений**
- **Предотвращение вторжений**

Таблицы межсетевого экрана (FORWARD, DNAT, INPUT и SNAT)

Классический контекст | Высокопроизводительный контекст

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Для удобства управления в интерфейсе правила разбиты на четыре таблицы:

- **FORWARD** - правила действуют на трафик, проходящий между зонами сервера, т. е. интернетом и локальной сетью, а также между локальными сетями. Это основная таблица, в которую можно добавить правила, ограничивающие трафик пользователей.
- **DNAT** - правила используются для прямого перенаправления портов с внешней зоны на ресурсы во внутренней зоне. Такие правила часто называются правилами проброса портов (port forwarding, port-mapping).
- **INPUT** - правила входящего на сервер трафика. Как правило, это трафик для служб самого Ideco NGFW Novum (например, DNS, DHCP, работающие на Ideco NGFW Novum).
- **SNAT** - правила для управления трансляцией сетевых адресов.

Правила в таблицах имеют приоритет сверху вниз (т. е. **верхнее правило приоритетнее нижнего**).

По умолчанию используется политика **РАЗРЕШИТЬ**. Если не созданы запрещающие правила, все порты и протоколы для пользователей разрешены.

При наличии большого количества правил в таблицах **Межсетевого экрана** воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Создание правил

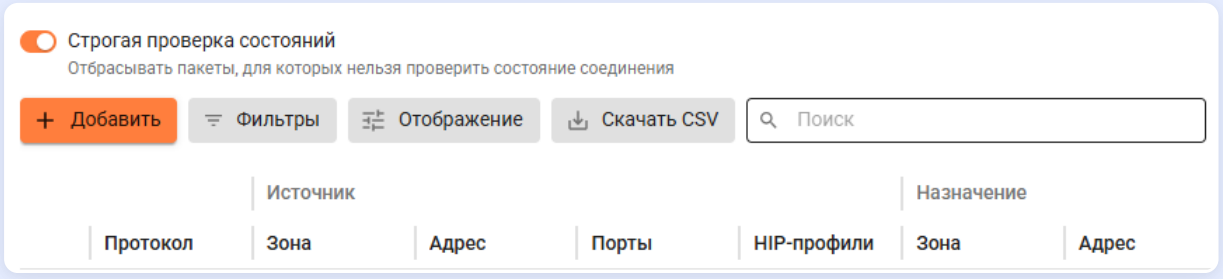
1. В нужной таблице нажмите кнопку **Добавить**.

2. Укажите необходимые параметры, действия правила и нажмите кнопку **Добавить**.

Правило будет добавлено в конец списка. Если необходимо, измените приоритет правила кнопками ↑ и ↓.

FORWARD

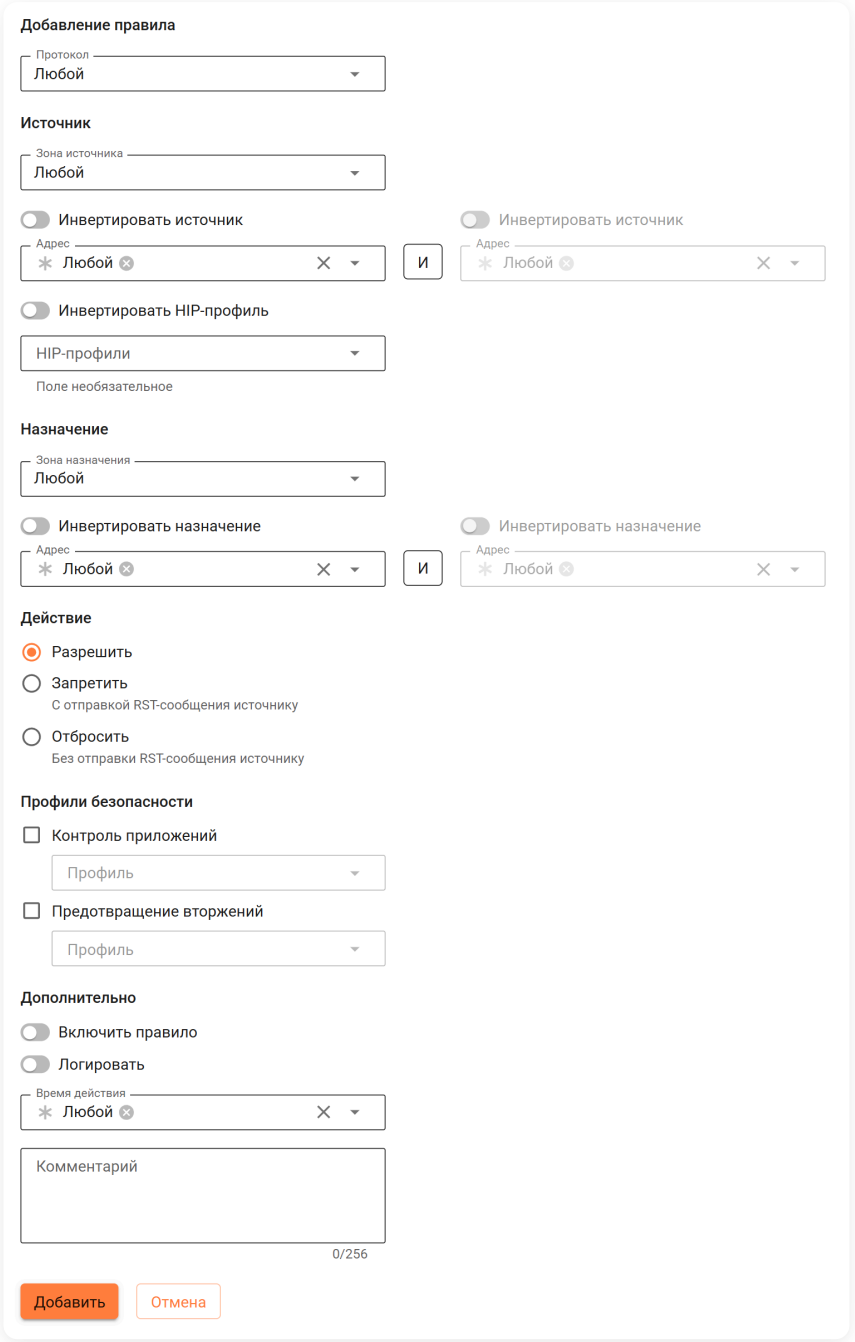
В FORWARD доступна опция **Строгая проверка состояний** (по умолчанию включена):



При включенной опции пакеты, для которых нельзя проверить состояние соединения (со статусом `INVALID`), отбрасываются системным правилом.

Отключение опции снижает уровень защиты, так как система начинает обрабатывать поврежденные, поддельные или не соответствующие логике сетевых протоколов пакеты, которые подсистема отслеживания соединений пометила статусом `INVALID`.

Если в сети используется асимметричная маршрутизация и наблюдаются проблемы с прохождением трафика, отключите опцию **Строгая проверка состояний**. Для устранения причины асимметричной маршрутизации воспользуйтесь инструкцией.



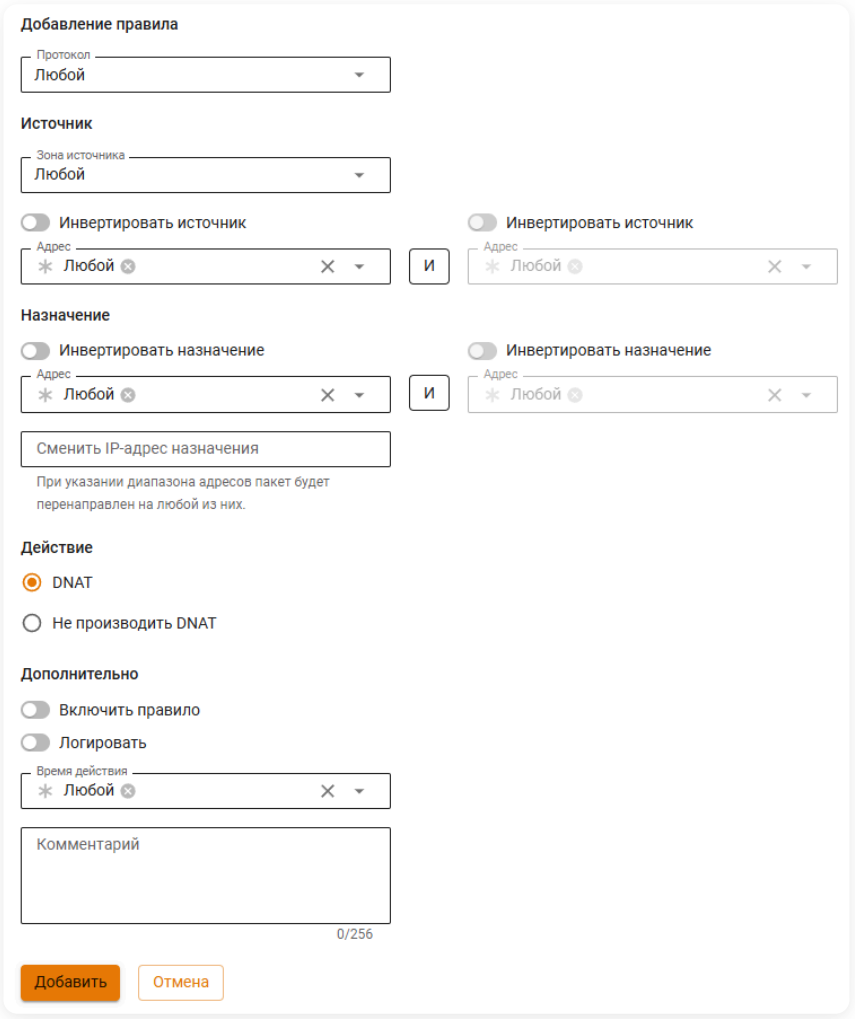
Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.

- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
- **Инвертировать HIP-профиль** - позволяет использовать в правиле все объекты, кроме выбранных в поле **HIP-профили**.
- **HIP-профили** - профиль, соответствующий устройству, от которого исходит трафик.

- **Назначение**:
  - **Зона назначения** - интерфейс или группа интерфейсов, в которые входит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действия**:
  - **Разрешить** - разрешает трафик или направляет трафик в модули фильтрации трафика.
  - **Запретить** - запрещает трафик с отправкой RST-сообщения источнику. Рекомендуем использовать запрет с отправкой RST, так как это позволяет клиенту немедленно завершить попытку соединения, избежать долгих таймаутов и облегчает диагностику.
  - **Отбросить** - запрещает трафик без отправки RST-сообщения источнику.
- **Профили безопасности**:
  - **Контроль приложений** - выберите профиль Контроля приложений, которым требуется фильтровать трафик.
  - **Предотвращение вторжений** - выберите профиль системы Предотвращения вторжений, которым требуется фильтровать трафик.
- **Дополнительно**:
  - **Включить правило** - включите правило. По умолчанию правило выключено.
  - **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
  - **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

DNAT



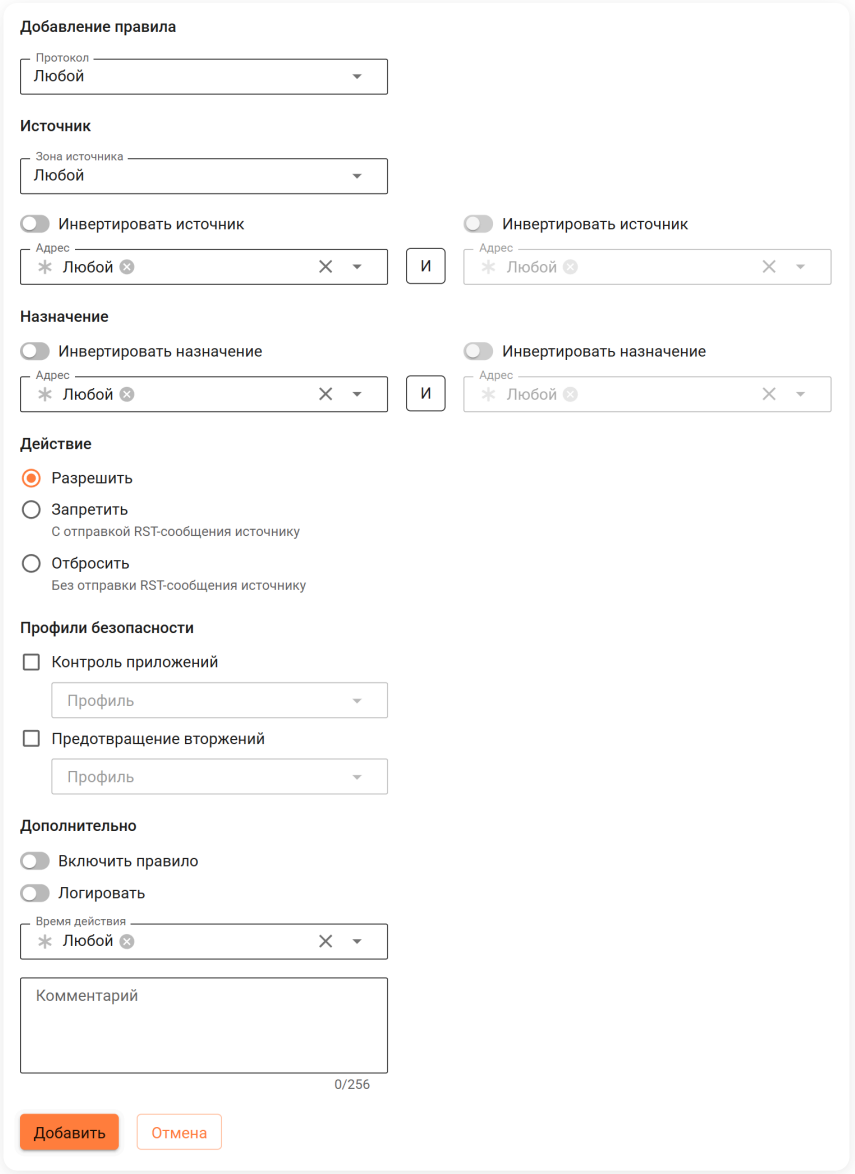
Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
  - **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
- **Назначение**:
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
  - **Сменить IP-адрес назначения** - при указании диапазона адресов пакет будет перенаправлен на любой из них. Диапазон задается в формате `<начальный_IP>-<конечный_IP>`. Например, `192.168.1.1-192.168.1.2`. Выбор конкретного адреса для перенаправления осуществляется по алгоритму **round-robin**: адреса используются последовательно - от первого к последнему, после чего цикл повторяется.

- **Сменить порт назначения** - при указании диапазона портов пакет будет перенаправлен в порт с тем же номером, на который пришел пакет, если этот порт попадает в указанный диапазон.

- **Действие**:
  - **DNAT** - транслирует адреса назначения, перенаправляя входящий трафик. В поле **Сменить IP-адрес назначения** укажите один IP-адрес или диапазон (при указании диапазона IP-адресов пакет будет перенаправлен на любой из них). Если при создании правила были указаны протоколы TCP или UDP, то появится поле **Сменить порт назначения**. Укажите порт, на который будет перенаправлен трафик.
  - **Не производить DNAT** - отменяет действие **DNAT** для трафика, удовлетворяющего критериям правила.
- **Дополнительно**:
  - **Включить правило** - включите правило. По умолчанию правило выключено.
  - **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
  - **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

INPUT



Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене их IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.

- **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.

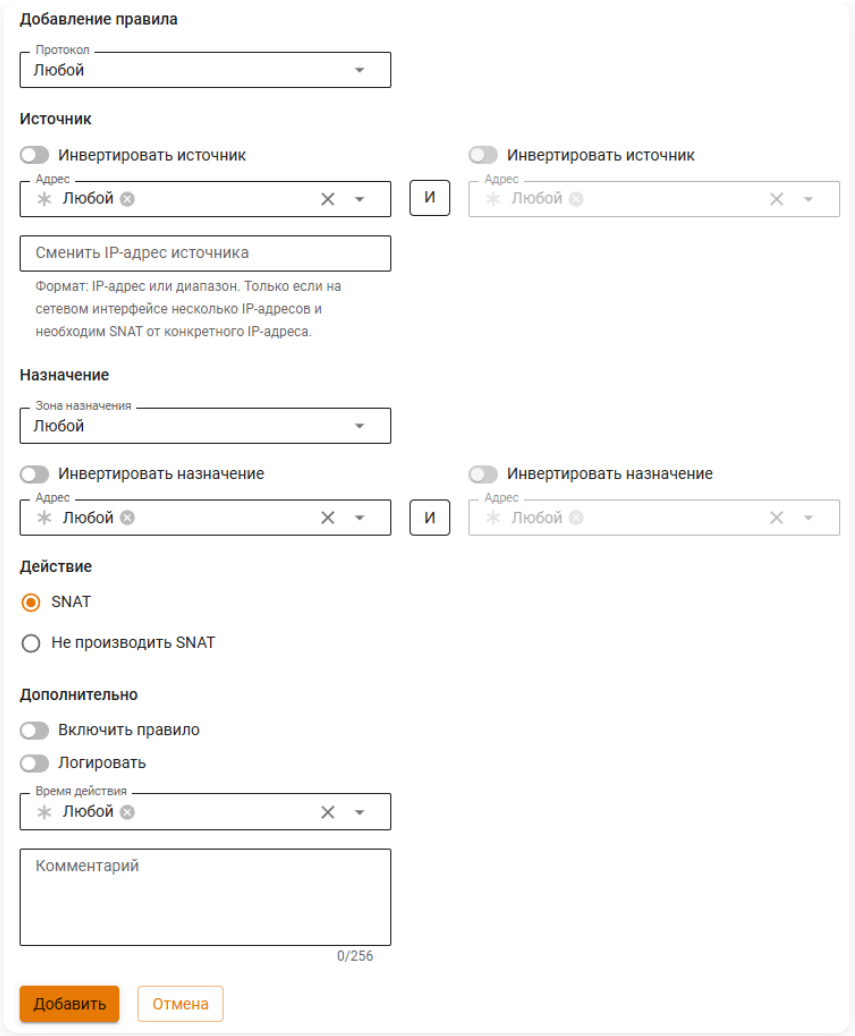
- **Назначение**:
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене их IP-адресов, межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порт назначения** - указывается при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действие**:
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
  - **Запретить** - запрещает трафик с отправкой RST-сообщения источнику. Рекомендуем использовать запрет с отправкой RST, так как это позволяет клиенту немедленно завершить попытку соединения, избежать долгих таймаутов и облегчает диагностику.
  - **Отбросить** - запрещает трафик без отправки RST-сообщения источнику.
- **Профили безопасности**:
  - **Контроль приложений** - выберите профиль **Контроля приложений**, которым требуется фильтровать трафик.
  - **Предотвращение вторжений** - выберите профиль системы **Предотвращения вторжений**, которым требуется фильтровать трафик.
- **Дополнительно**:
  - **Включить правило** - включите правило. По умолчанию правило выключено.
  - **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
  - **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

SNAT

> Правила автоматического **SNAT** работают только для интерфейсов, указанных как внешние.

Чтобы активировать автоматический **SNAT** для локальных сетей, включите опцию **Автоматический SNAT локальных сетей**. Автоматический **SNAT** подменяет адреса источников только для диапазонов: `192.168.0.0/16`, `172.16.0.0/12` и `10.0.0.0/8`.

Чтобы подменять адреса источников из других диапазонов, создайте соответствующее **SNAT** правило. Чтобы допустить устройства в сеть без сетевой трансляции адресов (правилом "не SNAT"), создайте правило **SNAT** с настройкой **Не производить SNAT**.



Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP), либо **Любой**.
- **Источник**:
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
  - **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
  - **Сменить IP-адрес источника** - заполняется, только если на сетевом интерфейсе несколько IP-адресов и необходим **SNAT** от конкретного IP-адреса. Можно указать IP-адрес или диапазон IP-адресов, например, 192.168.10.2-192.168.10.15.
- **Назначение**:
  - **Зона назначения** - интерфейс или группа интерфейсов, в которые входит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны в **Системном контексте** или **Специальные типы**.
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика (dst), к которому обращается источник. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**), страны или пользователи и группы (при смене IP-адресов межсетевой экран автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действия**:
  - **SNAT** - транслирует адреса источника.
  - **Не производить SNAT** - отменяет действие **SNAT** для трафика, удовлетворяющего критериям правила.
- **Дополнительно**:

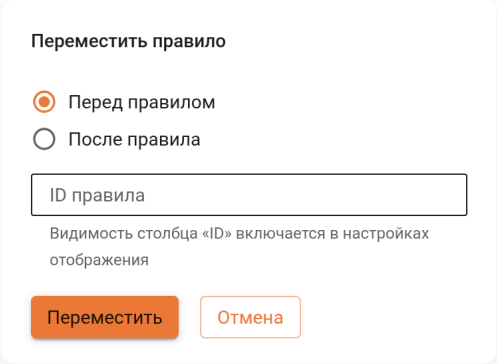
- **Включить правило** - включите правило. По умолчанию правило выключено.
- **Логировать** - включите логирование для записи срабатывания правила в журнале **Межсетевой экран**.
- **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в **Объектах**.
- **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

Перемещение правил

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Использование профилей безопасности

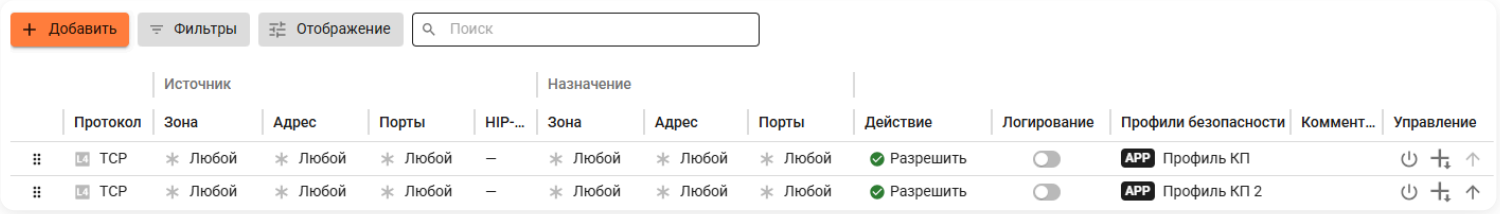
Межсетевой экран Ideco NGFW Novum обрабатывает правила последовательно, сверху вниз. Первое правило, условия которого совпадают с характеристиками проходящего трафика, определяет:

- Разрешить или запретить трафик.
- Включить ли логирование.
- Применить ли профиль безопасности.

Последующие правила, если они регулируют тот же трафик, игнорируются.

Пример. Необходимо ограничить всем сотрудникам доступ к социальным сетям и компьютерным играм. Для этого в таблице **FORWARD** настроено два правила фильтрации:

- С профилем безопасности, запрещающим сотрудникам доступ к социальным сетям, - "Профиль КП".
- С профилем безопасности, запрещающим сотрудникам доступ к компьютерным играм, - "Профиль КП 2".

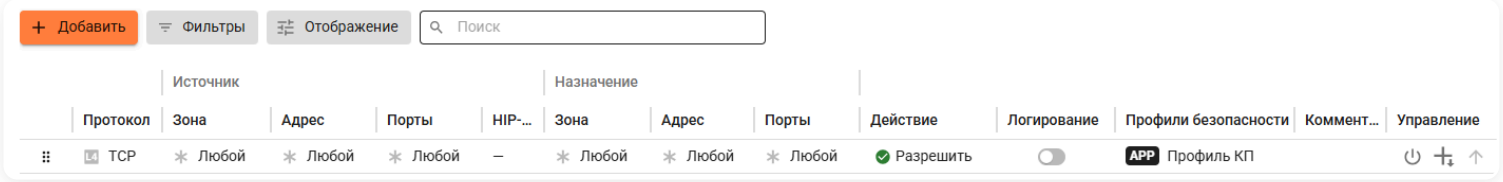


В этом случае при возникновении соответствующего трафика сотрудникам будет ограничен доступ только к социальным сетям - второе правило не будет применено, потому что трафик уже обработан вышестоящим правилом.

Если требуется добавить дополнительные условия фильтрации для определенного типа трафика, рекомендуется скорректировать настройки существующего профиля безопасности.

Рекомендуемые действия:

1. В **Профили безопасности** → **Контроль приложений** создать профиль, запрещающий доступ и к социальным сетям, и компьютерным играм.
2. В **Межсетевой экран** → **FORWARD** создать правило с данным профилем, действие - **Разрешить**:



Больше примеров настройки профилей - в статье.

Подробнее об особенностях настройки профилей - в статьях **Контроль приложений** и **Предотвращение вторжений**.

Важно

При создании правил

- Если в поле **Протокол** выбрать из списка параметр **Любой**, то правило будет действовать для всех протоколов.
- Для доступа из внешней сети в локальную необходимо создать и включить разрешающее правило **FORWARD**. Иначе весь трафик между сетевыми интерфейсами по умолчанию будет заблокирован системным правилом в цепочке **FORWARD**.
- При прямых подключениях к прокси не указывайте в поле **Адрес источника** IP-адрес. В противном случае правило не будет срабатывать, так как при прохождении через прямой прокси IP-адрес источника подменяется на IP-адрес Ideco NGFW.
- Если используется обратный прокси, то для **INPUT**-правила в полях **Адрес назначения** и **Порты назначения** должны указываться внешний IP-адрес и порт Ideco NGFW Novum, так как **INPUT**-правила Межсетевого экрана обрабатывают трафик раньше прокси-сервера.
- Для фильтрации веб-трафика из локальных сетей (80, 443 TCP-порты) для корректной работы правила в поле **Зона источника** должен указываться объект **Любой** либо **зона**, в которую входит интерфейс локальной сети. Если будет указан интерфейс локальной сети, то правило не будет обрабатывать веб-трафик. При инспекции веб-трафика интерфейс источника переназначается на интерфейс Ideco NGFW Novum, но **зона интерфейса источника сохраняется**.
- **DNAT**-правило обрабатывает UDP-трафик, пришедший только с **Внешних** интерфейсов.
- Трафик Ideco Client (порт 3051 UDP) обрабатывается системным правилом цепочки **FORWARD**, а не **INPUT**. Поэтому правила таблицы **INPUT**, запрещающие порт 3051, не блокируют подключения Ideco Client.
- При блокировке TCP-трафика через зону, указанную в **VPN-подключения** → **Основное**, HTTP- и HTTPS-трафик заблокирован не будет. Веб-трафик (порты 80 и 443) перенаправляется на прокси-сервер и далее в таблице **FORWARD** проходит с зоной источника **Исходящий трафик устройства**.

НЕ рекомендуем

- Создавать **FORWARD**- и **INPUT**-правила, запрещающие весь трафик, без предварительного создания разрешающих правил. Это может привести к блокировке доступа к серверу и его функциям.
- При создании правил **Межсетевого экрана** с протоколом TCP или UDP указывать **Порт источника**. Это связано с тем, что:
  - Порт источника выбирается случайно, и лишь некоторые приложения работают с фиксированным портом.
  - Порт источника может подмениться другим при прохождении пакета через NAT.
- В **DNAT**-правилах для обработки UDP-трафика выбирать **Локальный Ethernet** в поле **Источник**. Причина в том, что таблица **DNAT не обрабатывает** UDP-трафик, приходящий с локального интерфейса.
- Публиковать внутренние ресурсы через **DNAT**-правила с использованием TCP-порта 443, это заблокирует работу Ideco Client, использующего тот же порт. Для корректной работы Ideco Client опубликуйте внутренние ресурсы через обратный прокси или зарезервируйте TCP-порт 443 за Ideco Client, а внутренний ресурс опубликуйте на другом порту.

Рекомендуем

- Для предотвращения блокировки клиентского HTTP/HTTPS-трафика создайте правила:
  - Разрешающее трафик от пользователя.
  - Разрешающее трафик для специальной зоны источника **Исходящий трафик устройства**.

Полезные ссылки

- **Объекты**
- **Профили устройств**
- **Логирование**
- **Контроль приложений**
- **Предотвращение вторжений**

Примеры создания правил межсетевого экрана

Настройка правил межсетевого экрана для IPsec-подключений

Чтобы настроить правило **Межсетевого экрана** для IPsec-подключений, выберите в поле **Зона источника** или **Зона назначения** настроенное IPsec-подключение.

Портмаппинг, DNAT, публикация сервера в локальной сети

Примеры данных настроек подробно описаны в статьях раздела Публикация ресурсов.

Блокировка различных ресурсов средствами межсетевого экрана

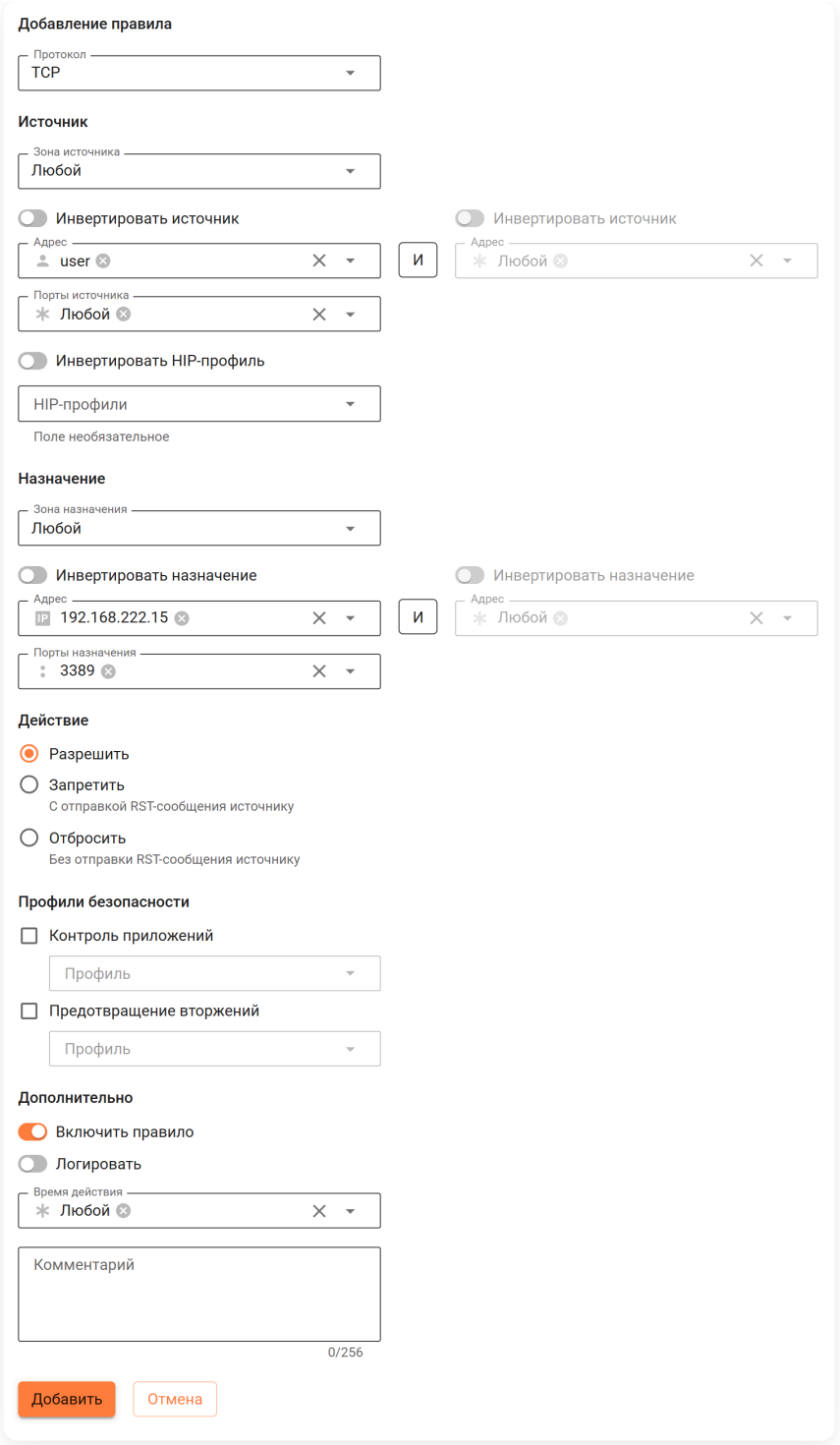
Вопросы блокировки программ удаленного управления (AmmyAdmin и TeamViewer), мессенджеров и другого ПО - описаны в статье Блокировка популярных ресурсов.

Доступ к терминальному серверу для определенного пользователя

1. В **Правила трафика** → **Межсетевой экран** → **FORWARD** нажмите **Добавить**.

2. Заполните поля:

- **Протокол** - выберите TCP.
- **Адрес** - выберите пользователя или группу пользователей.
- **Назначение** - укажите адрес терминального сервера.
- **Порты назначения** - укажите порт 3389.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

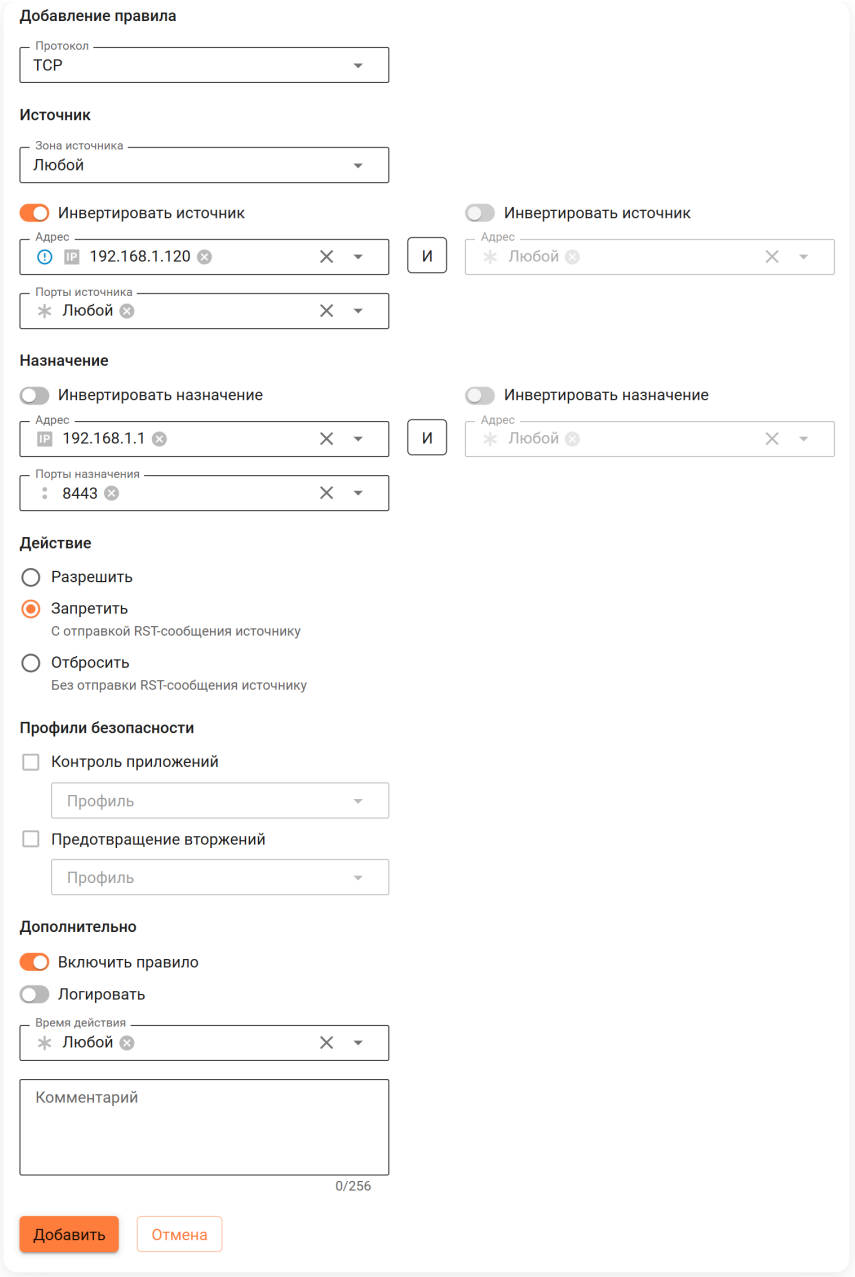


3. Нажмите **Добавить**.

Блокировка доступа к веб-интерфейсу (порт 8443) всем, кроме определенного адреса

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите правило:



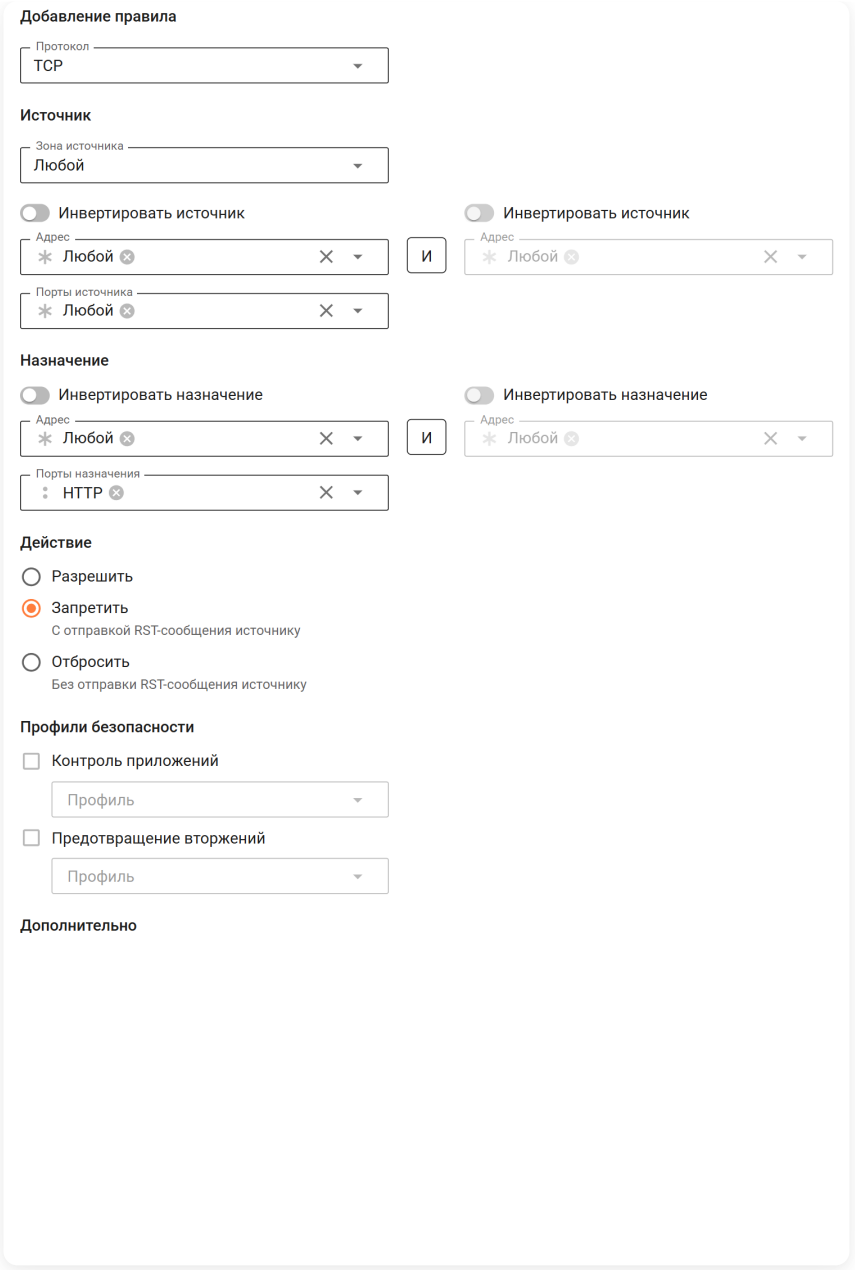
- Доступ к веб-интерфейсу будет разрешен только с IP-адреса **192.168.1.120**.
- **192.168.1.1** - IP-адрес Ideco NGFW Novum в локальной сети.

Блокировка 80 порта Ideco NGFW Novum

80 TCP порт используется для выпуска сертификатов Let`s Encrypt.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите правило:



Разрешение DNS-запросов через внешние DNS

ВАЖНО: Рекомендуем использовать в качестве DNS-сервер Ideco NGFW Novum. Но если необходимо использовать внешний DNS-сервер, то выполните действия:

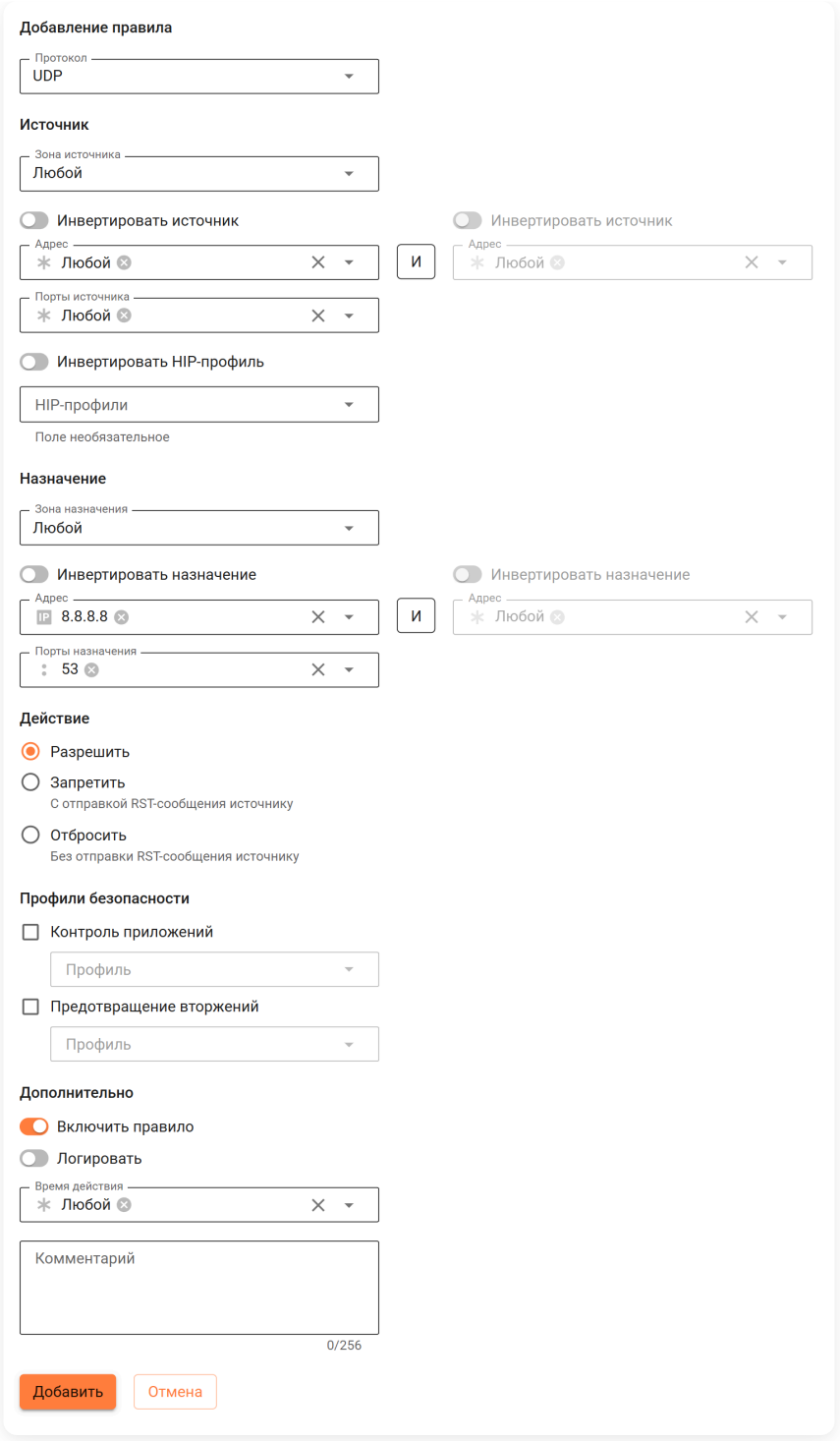
1. В **DNS** → **Внешние DNS** выключите **Перехват пользовательских DNS-запросов**.

2. Добавьте внешний DNS-сервер.

3. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

4. Создайте правило **Запретить все** и включите его.

5. Создайте правило, заполнив поля:



- **Протокол** - выберите UDP.
- **Назначение**:
  - **Адрес** - укажите IP-адрес внешнего DNS-сервера.
  - **Порт назначения** - укажите порт 53.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

Для работы протокола DNS может быть недостаточно правила с протоколом UDP, поскольку DNS использует в качестве транспорта UDP и TCP. Для решения задачи создайте аналогичное правило с протоколом TCP, используя кнопку **Клонировать** в таблице правил.

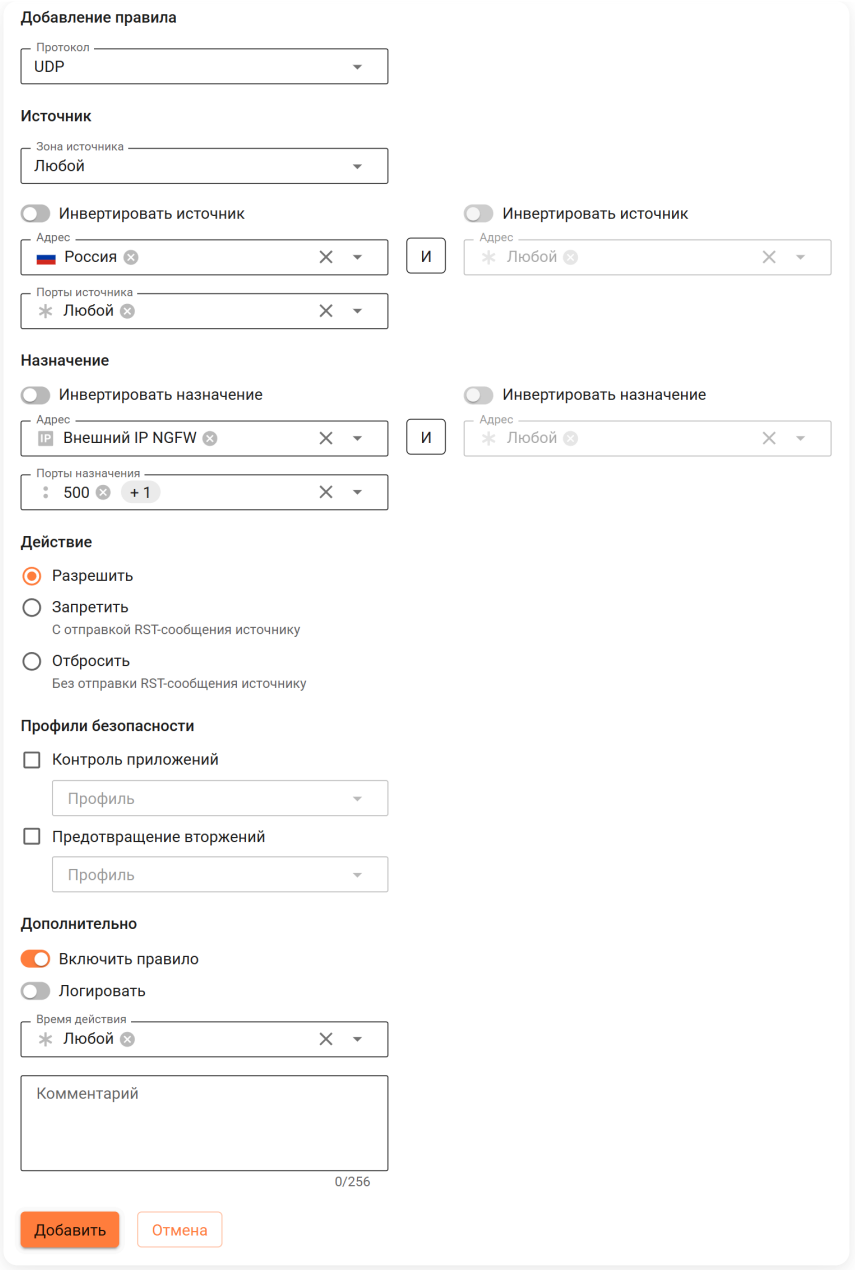
Доступ до Ideco NGFW Novum только из определенной внешней сети по IKEv2/IPsec

Пример: нужно разрешить доступ до Ideco NGFW Novum из России по VPN через IKEv2/IPsec.

ВАЖНО: Правило актуально, если на вкладке **INPUT** есть правило **Запретить все**.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:



- **Протокол** - выберите UDP.
- **Источник**:
  - **Адрес** - выберите страну Россия.
- **Назначение**:
  - **Адрес** - укажите внешний IP-адрес Ideco NGFW Novum.
  - **Порт назначения** - укажите порты 500 и 4500.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

Разрешение доступа к конкретным ресурсам при наличии запрещающего весь трафик правила

Примеры представлены в статье Как разрешить доступ к ресурсам в ограниченной сети.

Настройка одностороннего доступа из подсети к хосту другой подсети

На вкладке **Правила трафика** → **Файрвол** → **FORWARD** создайте два правила:

1. Правило, разрешающее доступ из подсети к хосту:

2. Правило, запрещающее доступ от хоста к подсети:

3. Расположите разрешающее правило выше запрещающего.

- **192.168.112.0/24** - подсеть, из которой требуется разрешить доступ до хоста.
- **192.168.19.119** - хост, который не должен иметь доступ до указанной подсети.

DNAT-правило для работы site-to-site IPsec с устройством в локальной сети

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **DNAT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:

- **5.120.1.25** - IP-адрес Ideco NGFW Novum во внешней сети.
- **192.168.1.50** - IP-адрес устройства в локальной сети.

Для полноценной работы IPsec создайте такое же правило с протоколом AH, нажав Клонировать. Помимо этого, нужно создать **DNAT**-правило с протоколом UDP и портами 500, 4500.

Полезные ссылки

- **Как разрешить доступ к ресурсам в ограниченной сети**

Логирование

Функциональность доступна в **Классическом** и **Системном контекстах**.

Принцип работы

Соединения, установленные до создания правил логирования, залогированы не будут. Если приходит пакет, атрибуты которого (протокол, порты и IP-адрес) соответствуют уже созданному соединению, к нему применяются те же действия, что и к другим пакетам этого соединения.

Первый пакет нового соединения (протокол, порты, IP-адреса не соответствуют атрибутам уже установленного соединения) проходит через правила вкладки **Логирование**. Если атрибуты пакета соответствуют правилу логирования, то на пакет ставится метка логирования. По умолчанию метки нет.

Срабатывают все правила логирования, настроенные на вкладке **Логирование**, по порядку. Если пакет соответствует нескольким правилам логирования, будет применено последнее из них.

Далее трафик проходит через правила в таблицах Межсетевого экрана. Если при срабатывании правила на пакете стояла метка логирования, то в логи попадают следующие данные:

- Атрибуты пакета, с которым произошло событие (протокол, порты и IP-адреса).
- Данные правил **Межсетевого экрана**: идентификатор правила, название таблицы и действие, которое произошло.
- Информация по DNAT: идентификатор правила, измененный IP-адрес и порт назначения.
- Информация по SNAT: идентификатор правила, измененный IP-адрес источника.
- Если в правиле указаны профили безопасности:
  - Данные профиля Контроля приложений: профиль, действие, протокол прикладного уровня, приложение.
  - Данные профиля Предотвращения вторжения: профиль, ID соединения, действие и ID сигнатуры.

Для просмотра логов перейдите в **Отчеты и журналы** → **Межсетевой экран**.

Модули **Контроль приложений** и **Предотвращение вторжений** могут задерживать решение о блокировке или разрешении соединения, поэтому информация в журнале появляется не сразу. После принятия решения запись в журнале **Межсетевой экран** обновляется.

Включите опцию **Логировать срабатывания правил** для начала логирования.

Не рекомендуем включать логирование всего трафика, так как при высоком потоке новых соединений логирование требует дополнительных ресурсов на сервере и возможна потеря части логов. Логирование необходимо, например, для определения модуля, блокирующего доступ в интернет.

Если для работы логирование не требуется, рекомендуем отключить опцию **Логировать срабатывания правил**.

Трафик для логирования

Правила **Логирования** позволяют гибко выбрать трафик для логирования. Создайте и включите в таблице правило логирования. Соединение залогируется и отразится в журнале **Межсетевой экран** при срабатывании правила **Межсетевого экрана**.

Действие **Не логировать** позволяет снять метку логирования.

Пример 1. Настройка логирования всего трафика на yandex.ru, кроме трафика от Иванова Ивана

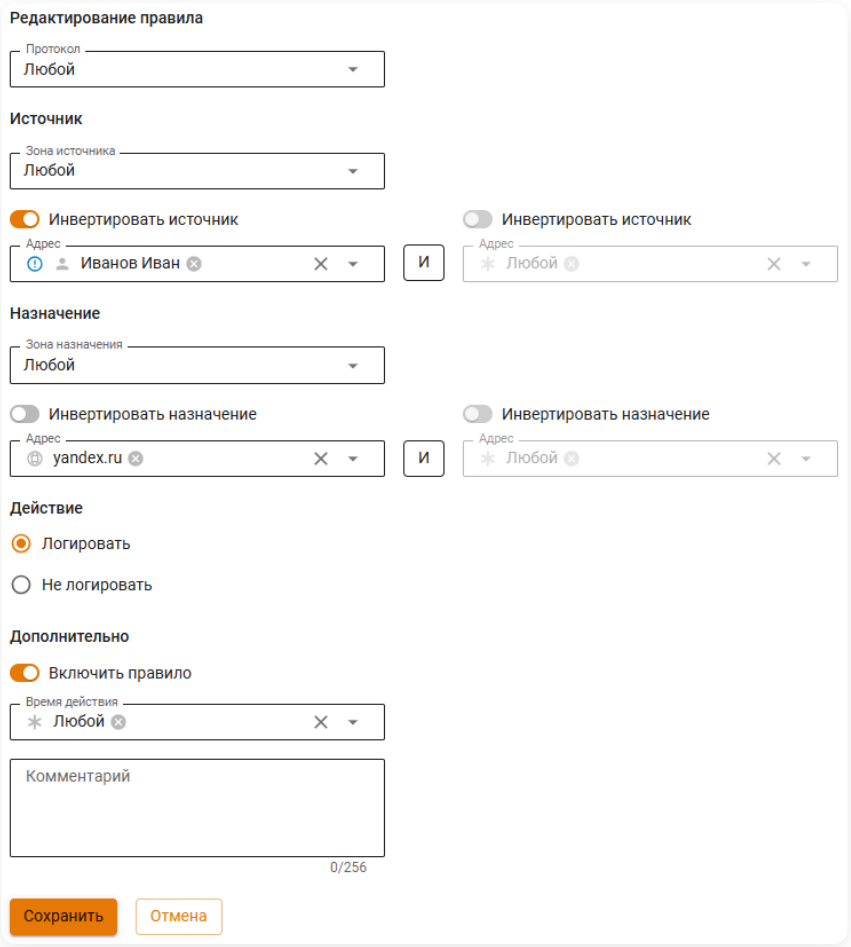
Настройте правило:

1. В поле **Источник** выберите ***Иванова Ивана*** и переведите опцию **Инвертировать источник** в положение **Включен**.

2. В поле **Назначение** выберите `yandex.ru`.

3. Выберите действие **Логировать**.

4. В поле **Дополнительно** включите правило:



Способ настройки через опцию **Инвертировать источник** желательно использовать при небольшом количестве правил логирования. При большом количестве правил логирования более удобен способ, описанный в примере 2.

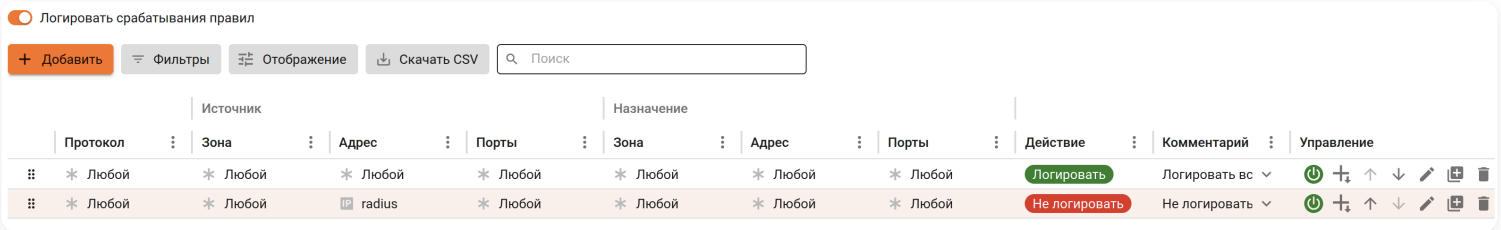
Пример 2. Настройка логирования всего трафика, кроме трафика от RADIUS сервера

Настройте два правила:

1. Правило с действием **Логировать** для всего трафика.

2. Правило с действием **Не логировать** для трафика от источника ***RADIUS***.

Расположите второе ниже:



Предварительная фильтрация

Классический контекст | Высокопроизводительный контекст

Вкладка **Предварительная фильтрация** позволяет заблокировать весь трафик, попадающий под условия таблицы, до просмотра таблиц **Межсетевого экрана** (например, **FORWARD** или **INPUT**). Используйте раздел, если требуется фильтрация пакетов на уровне TCP/IP.

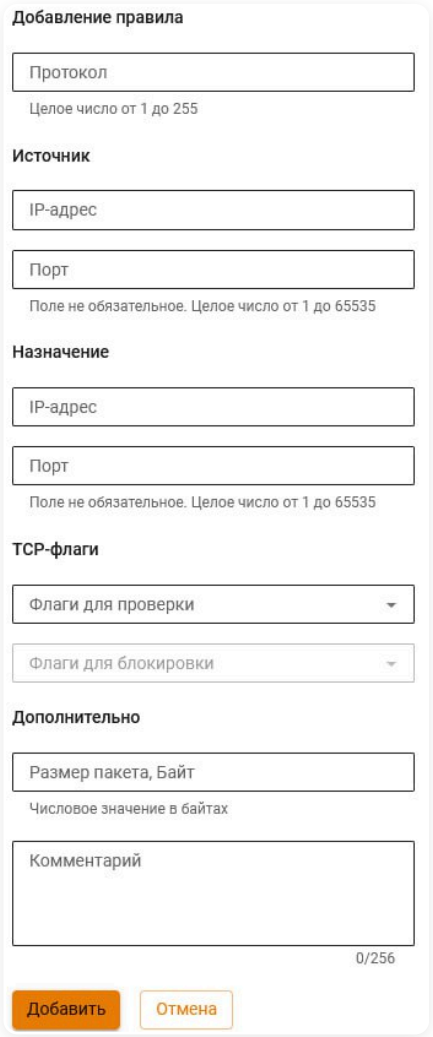
Включение хотя бы одного правила **Предварительной фильтрации** может привести к снижению сетевой производительности NGFW примерно на 20%.
При выключении правила производительность сразу восстановится.

При наличии большого количества правил воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Создание правил

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Предварительная фильтрация** и нажмите **Добавить**.

2. Заполните поля правила:



Расшифровка полей

- **Протокол** - укажите номер протокола из таблицы. Номер может быть в диапазоне от 0 до 255 включительно.

- **Источник**:
  - **IP-адрес** - укажите IP-адрес источника.
  - **Порт** - укажите порт источника.
- **Назначение**:
  - **IP-адрес** - укажите IP-адрес назначения.
  - **Порт** - укажите порт назначения.
- **TCP-флаги**:
  - **Флаги для проверки** - укажите флаги TCP, которые будут проверяться. В этом поле могут быть указаны флаги: **SYN**, **ACK**, **FIN**, **RST**, **URG**, **PSH**.
  - **Флаги для блокировки** - укажите флаги TCP, которые будут заблокированы. Флаг будет доступен для блокировки, только если флаг содержится в поле **Флаги для проверки**.
- **Дополнительно**:
  - **Размер пакета, Байт** - укажите размер пакета в байтах с учетом TCP- и IP-заголовков (40 + N, где N - размер полезных данных в пакете). Пакет указанного размера будет заблокирован.
  - **Комментарий**.

3. Нажмите **Добавить**.

Устранение проблем

При неправильно созданных правилах доступ к веб-интерфейсу может быть заблокирован (например, блокировка протокола TCP с проверкой и блокировкой флага **SYN**). Для возвращения доступа к веб-интерфейсу воспользуйтесь инструкцией или включите режим **Полный доступ**.

Тестирование правил

Классический контекст | Высокопроизводительный контекст

На вкладке создаются тесты для проверки работы правил таблицы **FORWARD** и **INPUT**.

Тест - это конкретный пример, в котором проверяется доступ к определенному IP-адресу с учетом правил таблицы **Межсетевого экрана**. Во время тестирования NGFW Novum генерирует тестовый пакет с заданным источником и назначением, после чего проверяет, как пакет проходит через **Межсетевой экран**.

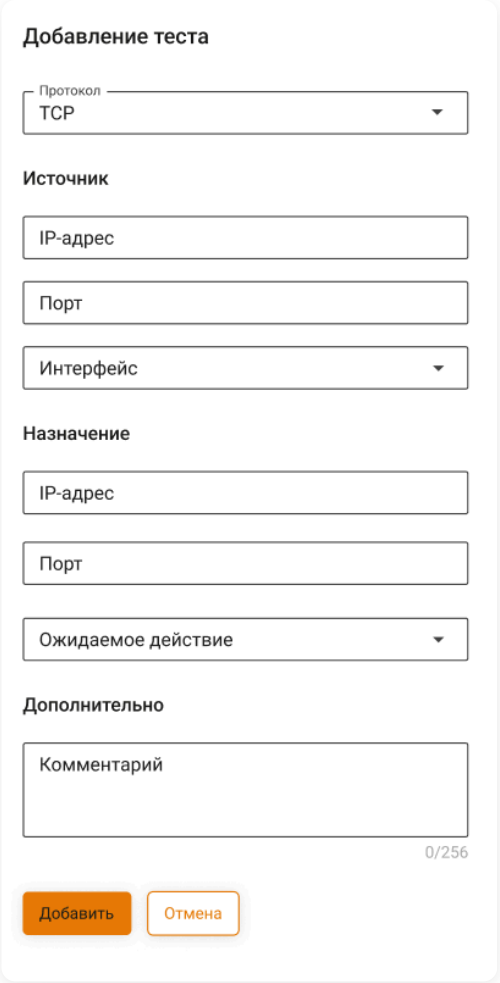
Рекомендуем использовать для источника порты из диапазона 49152 - 65535 (динамически выделяемые или частные порты, которые не регистрируются IANA).

Создание тестов

Для создания теста выполните действия:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Тестирование правил** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Протокол** (**TCP**/**UDP**).
- **IP-адрес** - адрес источника и назначения.

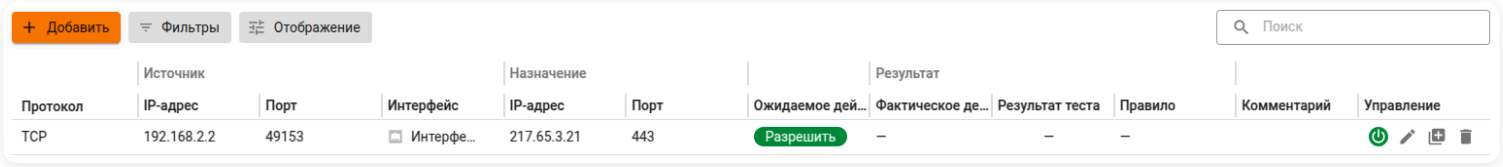
- **Порт** - порт источника и назначения.
- **Интерфейс** - сетевой интерфейс источника.

> Выбранный интерфейс должен быть настроен и подключен. Если интерфейс отключен, Ideco NGFW Novum не сможет выполнить тестирование.

- **Ожидаемое действие** - Разрешить или Запретить.
- **Комментарий** - необязательное поле.

3. Нажмите **Добавить**.

Созданные тесты добавляются в таблицу:



Запуск и результат тестирования

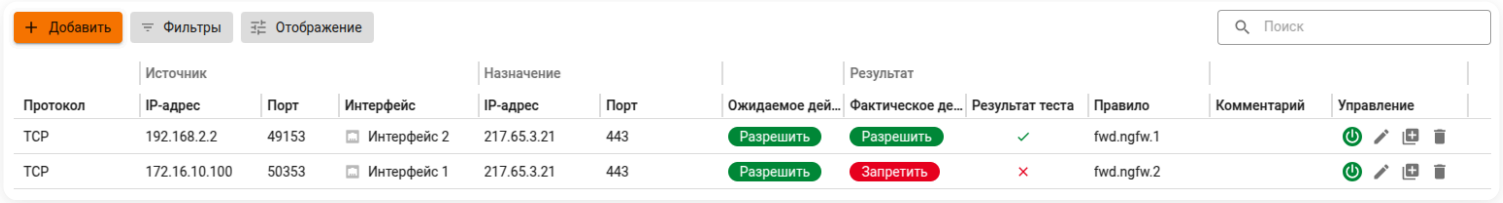
Запуск теста не происходит автоматически при добавлении. Для запуска:

1. Включите нужный тест .

2. Нажмите **Запустить тестирование** в левом нижнем углу вкладки.

> Если тест выключен, то тестирование запускаться не будет.

При совпадении ожидаемого и фактического действия тестирование считается успешным:



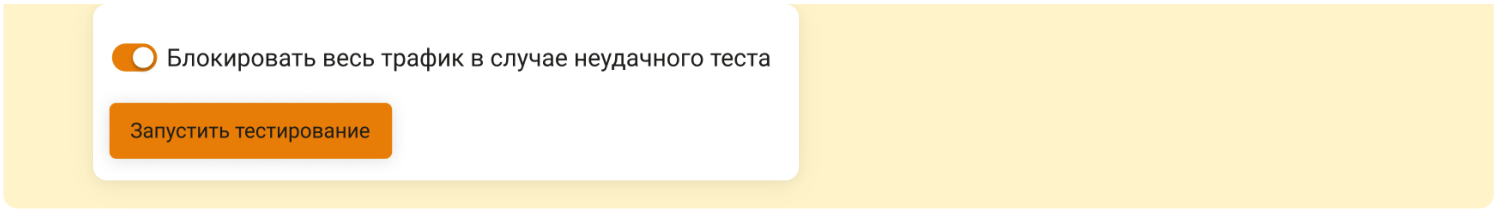
Залогированные правила вида `fwd.sys.xxx`, `inp.sys.xxx`, `out.sys.xxx` в столбце **Правило** - результат срабатывания системного правила, которое разрешило или запретило прохождение трафика в рамках проверки, если не сработало ни одно пользовательское правило. Это правила **Межсетевого экрана**, которыми нельзя управлять из веб-интерфейса Ideco NGFW Novum, правила **Межсетевого экрана** всегда включены.

> Расшифровка элементов системного правила `<name>.sys.xxx`:
>
> - `<name>.sys.` - название правила:
> - `fwd.sys` - Forward System: правило обработки трафика, проходящего между зонами сервера;
> - `inp.sys` - Input System: правило обработки входящего трафика;
> - `out.sys` - Output System: правило обработки исходящего трафика.
> - `xxx` - идентификатор правила. Например, `fwd.sys.22`

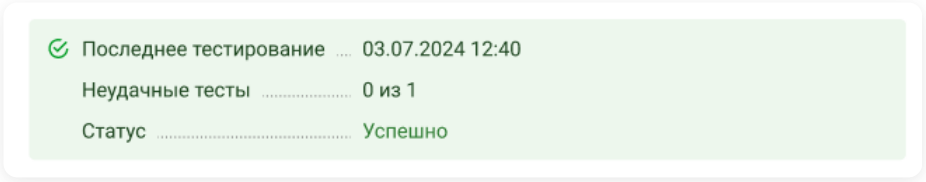
Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Межсетевого экрана**. Посмотреть системное правило, которое сработало, можно через Терминал, введя команду `iptables-save | grep 'sys.<ID правила>'` (смотрите примеры в статье)

Если у выбранного теста **Интерфейс** источника был удален (отображается **Удалено** в столбце **Интерфейс**), тестирование завершится с фактическим действием **Запретить**.

> Не рекомендуем включать опцию **Блокировать весь трафик в случае неудачного теста**, иначе при любом неуспешном результате теста (обозначен) весь трафик через NGFW Novum будет заблокирован. Единственный способ снятия блокировки - тестирование без ошибок. Отключение опции не сработает:



В правом нижнем углу вкладки представлены сведения о последнем тестировании: текущий статус (**Успешно**/**Ошибка**), время проведения и количество неуспешных тестов (из числа включенных в столбце **Управление**):



Повторный запуск сбрасывает результаты предыдущего тестирования.

Аппаратная фильтрация

Функциональность доступна в **Классическом** и **Системном контекстах**.

На вкладке можно настроить пакетную фильтрацию трафика на основе сетевых и физических адресов отправителей и (или) получателей. Пакеты будут блокироваться на аппаратном уровне без участия центрального процессора, с использованием вычислительных мощностей сетевой карты.

В Ideco NGFW Novum блокировка будет происходить в соответствии с выбранным режимом фильтрации. Одновременно может работать фильтрация по MAC-адресу источника или один из видов фильтрации по IP.

Созданные на вкладке правила применяются сразу ко всем поддерживаемым сетевым адаптерам, найденным в системе.

Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

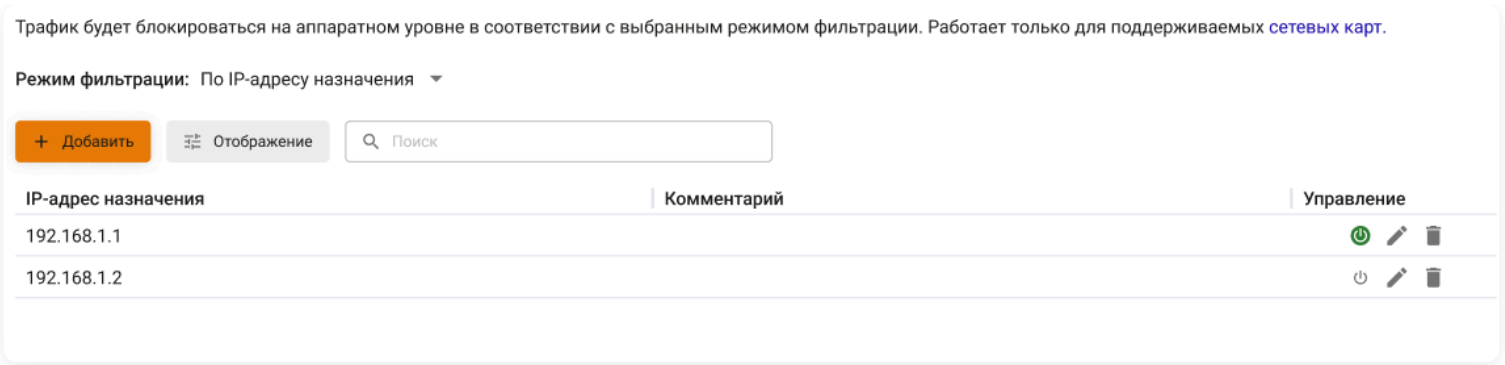
Список поддерживаемых сетевых карт

PCI-идентификатор	Модель адаптера
0x8086:0x0CF8	Ethernet Controller X710 Intel(R) FPGA Programmable Acceleration Card N3000 for Networking
0x8086:0x0D58	Ethernet Controller XXV710 Intel(R) FPGA Programmable Acceleration Card N3000 for Networking
0x8086:0x1572	Ethernet Controller X710 for 10GbE SFP+
0x8086:0x1574	Ethernet Controller XL710 Emulation
0x8086:0x1580	Ethernet Controller XL710 for 40GbE backplane
0x8086:0x1581	Ethernet Controller X710 for 10GbE backplane
0x8086:0x1583	Ethernet Controller XL710 for 40GbE QSFP+
0x8086:0x1584	Ethernet Controller XL710 for 40GbE QSFP+
0x8086:0x1585	Ethernet Controller X710 for 10GbE QSFP+
0x8086:0x1586	Ethernet Controller X710 for 10GBASE-T
0x8086:0x1587	Ethernet Controller XL710 for 20GbE backplane
0x8086:0x1588	Ethernet Controller XL710 for 20GbE backplane
0x8086:0x158A	Ethernet Controller XXV710 for 25GbE backplane
0x8086:0x158B	Ethernet Controller XXV710 for 25GbE SFP28
0x8086:0x15FF	Ethernet Controller X710 for 10GBASE-T
0x8086:0x104F	Ethernet Controller X710 for 10 Gigabit backplane
0x8086:0x104E	Ethernet Controller X710 for 10 Gigabit SFP+
0x8086:0x0DD2	Ethernet Network Adapter I710

Создание правил

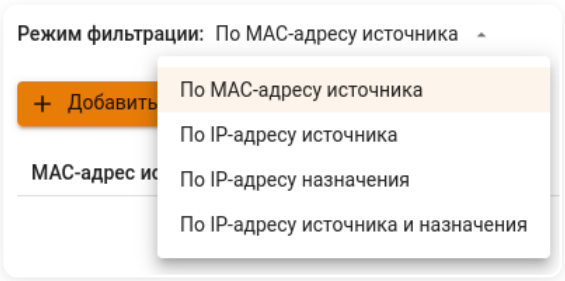
Администратор может создать не более 2500 правил каждого типа фильтрации.

Созданные правила отображаются в таблице в зависимости от выбранного режима фильтрации:



Чтобы создать правило определенного типа, выполните действия:

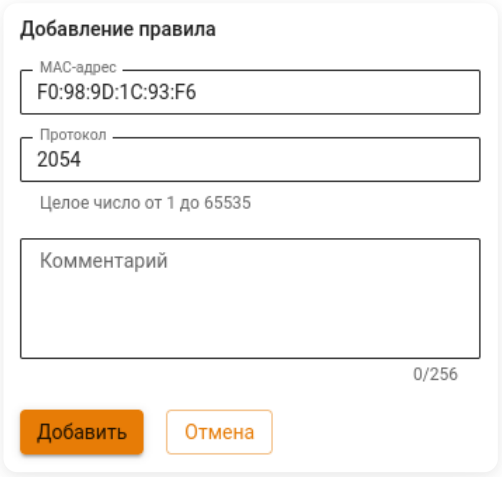
1. Выберите режим фильтрации, нажав на кнопку в левом верхнем углу:



- По MAC-адресу источника.
- По IP-адресу источника.
- По IP-адресу назначения.
- По IP-адресу источника и назначения.

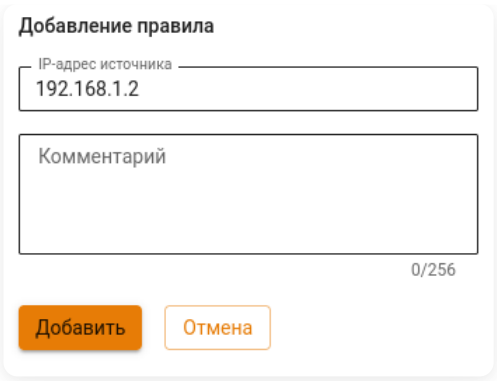
2. Нажмите **Добавить** и заполните поля:

Фильтрация по MAC-адресу источника



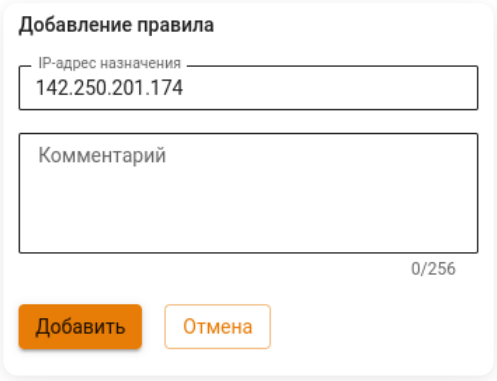
- **MAC-адрес** - введите физический адрес источника трафика.
- **Протокол** - введите номер протокола сетевого уровня. **Не указывайте протокол IPv4** (значение 2048), для фильтрации на сетевом уровне используйте правила ***По IP-адресу источника***, ***По IP-адресу назначения***, ***По IP-адресу источника и назначения***.
- **Комментарий** - поле необязательное.

Фильтрация по IP-адресу источника



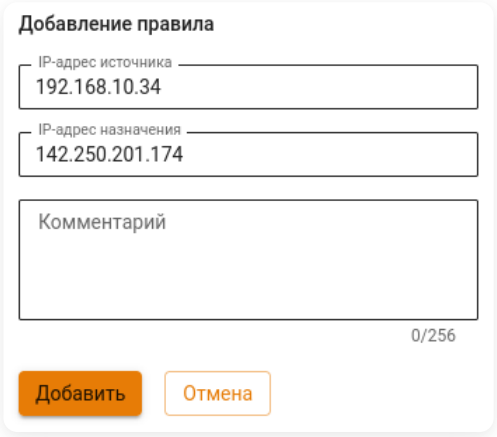
- **IP-адрес источника** - введите IP-адрес источника трафика.
- **Комментарий** - поле необязательное.

Фильтрация по IP-адресу назначения



- IP-адрес назначения - введите IP-адрес назначения трафика.
- Комментарий - поле необязательное.

Фильтрация по IP-адресу источника и назначения



- **IP-адрес источника** - введите IP-адрес источника трафика.
- **IP-адрес назначения** - введите IP-адрес назначения трафика.
- **Комментарий** - поле необязательное.

3. Нажмите **Добавить**.

4. Включите правило или оставьте выключенным.

Отключить аппаратную фильтрацию можно, выключив опцию **Межсетевой экран** в соответствующем разделе.

Настройка ALG

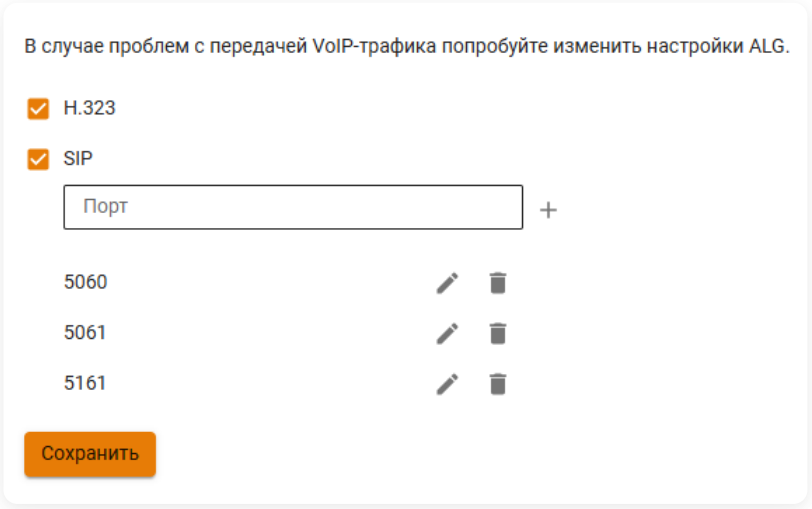
Функциональность доступна в **Классическом** и **Системном контекстах**.

Вкладка **Настройка ALG** позволяет управлять параметрами протоколов VoIP (H.323 и SIP), а также настраивать порты, используемые для передачи голосового трафика. Используйте раздел, если:

- Возникли проблемы с передачей VoIP-трафика, например, отсутствуют гудки или голос при повторных звонках между абонентами.
- Используются нестандартные порты для протокола SIP.

Изменение настроек ALG

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Настройка ALG** и заполните поля:



- **H.323** - активировано по умолчанию. Если протокол не используется, то отключите опцию.
- **SIP** - активировано по умолчанию. Если протокол не используется, то отключите опцию.
- **Порт** - укажите порт для протокола SIP, если используется нестандартный. Максимальное количество портов - 10.

2. Нажмите **Сохранить**.

Контент-фильтр

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Профили контент-фильтра**: `ideco-content-filter-backend`, `ideco-content-filter-backend-rules-file-syncer`, `ideco-content-filter-sky-db-updater`, `ideco-rocks-cf-tool`.

Список имен служб для других разделов доступен по ссылке.

Контент-фильтр проверяет запрашиваемые сайты в базе URL-адресов из пользовательских категорий Ideco NGFW Novum. Если адрес находится в списках, то применяются настроенные правила фильтрации.

Контент-фильтр работает на прикладном уровне (в частности, HTTPS), информация об IP-адресах может быть неточной. Для фильтрации на сетевом уровне по IP-адресам используйте Межсетевой экран.

Контент-фильтр включает пять вкладок:

- Правила - создание и управление правилами фильтрации.
- Пользовательские категории - управление собственных списков.
- Переопределение категорий - проверка и изменение категорий для сайтов из расширенной базы.
- Морфологические словари - фильтрация по ключевым словам.
- Настройки - параметры работы фильтра.

Особенности фильтрации

Контентная фильтрация применяется только к веб-запросам, направленным на внешние интернет-ресурсы через стандартные порты:

- HTTP - порт 80 TCP.
- HTTPS - порт 443 TCP.

Запросы к локальным веб-ресурсам, а также веб-трафик, передаваемый по нестандартным портам, не обрабатываются **Контент-фильтром**.

- **Фильтрация HTTPS**:
  - HTTPS-сайты без расшифровки трафика фильтруются только по домену (не по полному URL). Например, нельзя заблокировать только `http://example.com/page` и оставить доступ к `http://example.com/path` - будет заблокирован весь доступ к `example.com`. Также без расшифровки трафика невозможно применить правила категории **Файлы**: чтобы заблокировать или разрешить загрузку файлов определенных типов, система должна иметь возможность анализировать путь или имя файла в URL (например, `https://example.com/upload/test.pdf`).
  - Для полной фильтрации HTTPS создайте правила расшифровки HTTPS-трафика нужных категорий или всех веб-запросов (категория **Все запросы**).
- **Фильтрация по IP-адресам** работает для:
  - HTTP-запросов к IP-адресам напрямую.
  - Расшифрованных HTTPS-запросов к IP-адресам.
  - HTTPS-запросов к ресурсам, IP-адрес которых содержится в поле Common Name сертификата.

Для записи логов включите опцию **Включить логирование** в **Сервисы** → **Прокси** → **Основное**.

Полезные ссылки

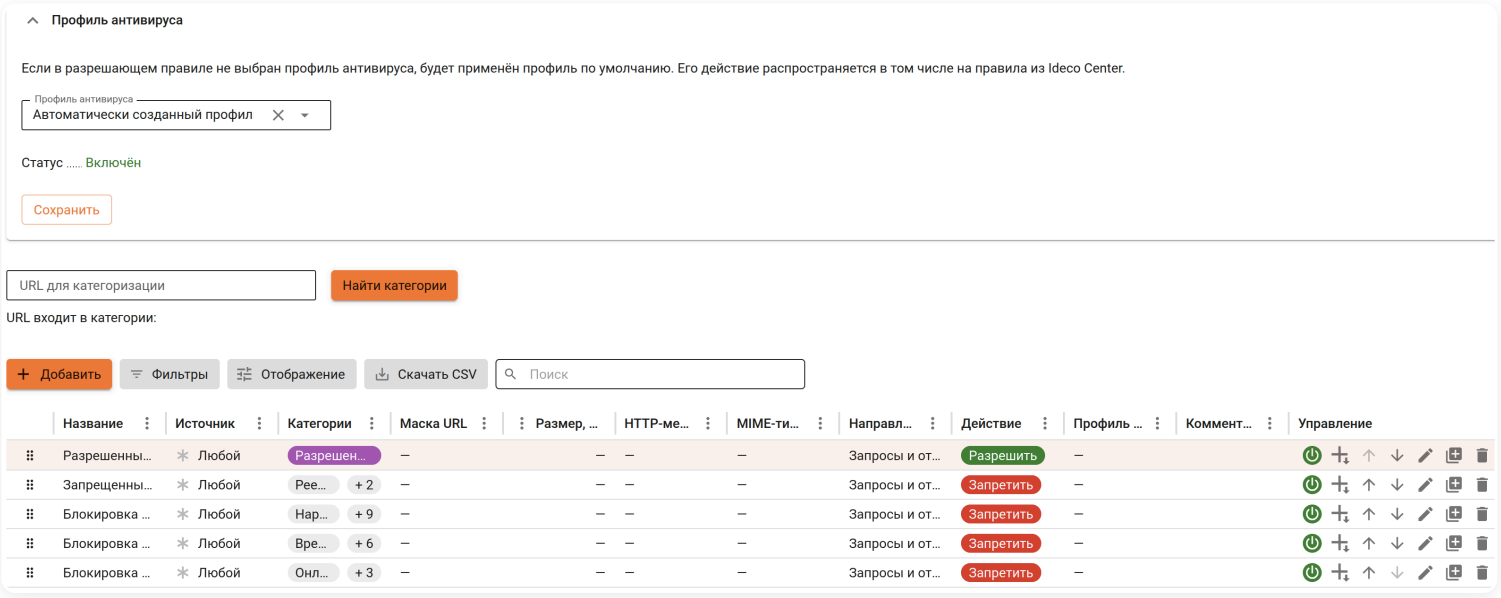
- **Блокировка загрузки файлов в файлообменники**
- **Блокировка популярных ресурсов**
- **Блокировка чат-ботов**

Правила

Функциональность доступна в **Классическом** и **Системном контекстах**.

Правила создаются в **Правила трафика** → **Контент-фильтр** → **Правила**.

Вкладка содержит:



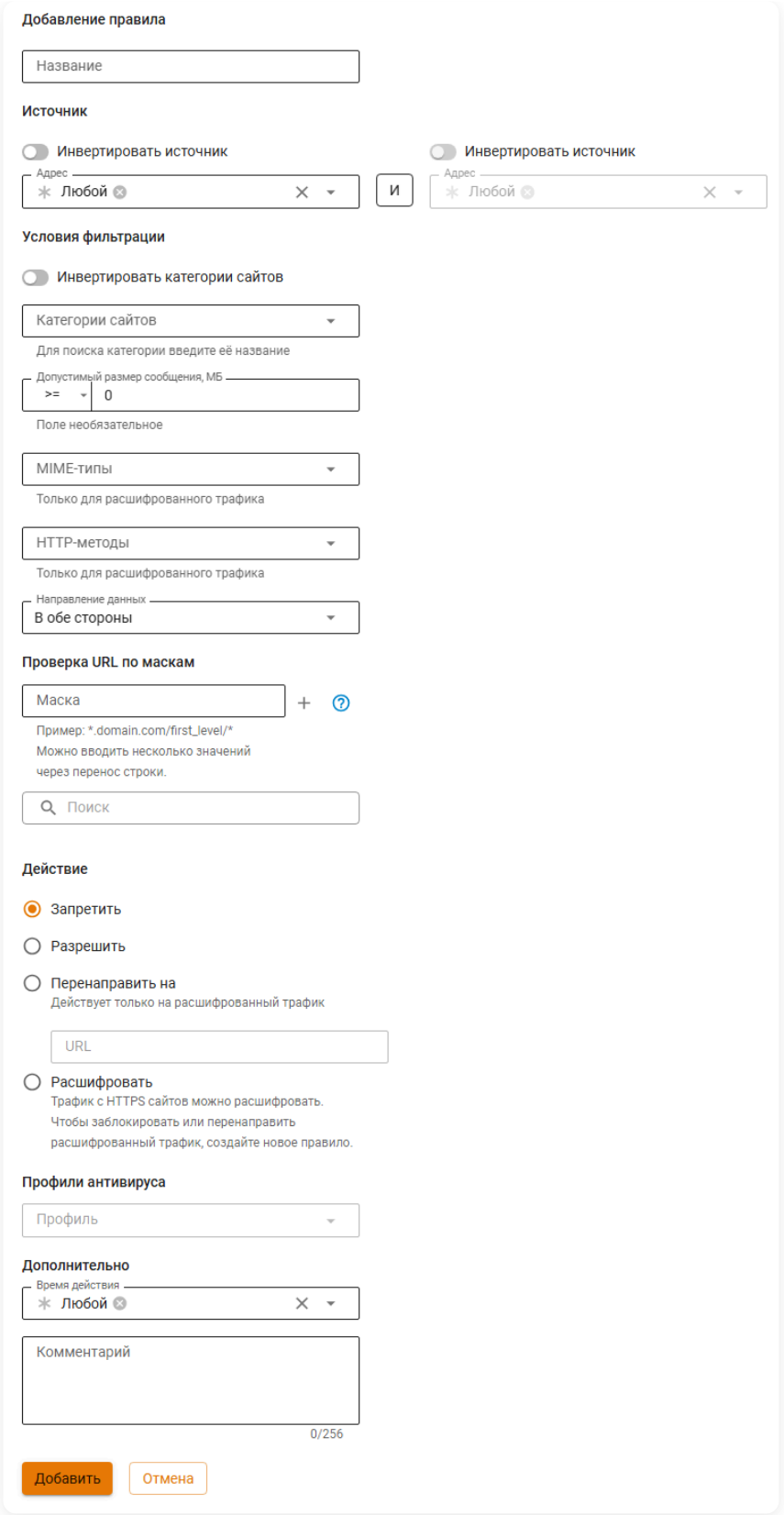
- **Профиль антивируса**. Настройка профиля **Антивируса** по умолчанию, который будет применяться:
  - К разрешающим правилам **Контент-фильтра** (включая правила из Ideco Center), где профиль не задан.
  - К трафику, который не попал ни под одно правило **Контент-фильтра**.
    Статус отображает состояние активности выбранного профиля **Антивируса**.

Чтобы задать профиль для конкретного правила, используйте поле **Профили антивируса** в форме создания или редактирования правила.

- **Строку поиска категории URL для категоризации**. Позволяет найти, к какой категории относится URL для создания правила.
- **Таблицу созданных правил**. Порядок применения правил описан в разделе ниже.

Создание правил

1. Нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Название** - название правила. Значение не должно быть длиннее 42 символов.
- **Источник**:
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика (src), для которых применяется правило. Доступные объекты: IP-адреса, диапазоны IP-адресов, сети, домены, страны или пользователи и группы.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
- **Условия фильтрации**:

- **Инвертировать категории сайтов** - позволяет использовать в правиле все категории, кроме выбранных в поле **Категории сайтов**.
- **Категории сайтов** - поле для выбора предустановленной или пользовательской категории, перечень ресурсов, на которые распространяется действие правила.

Если поле **Категории сайтов** пустое, правило работать не будет.

- **Допустимый размер сообщения** - объем HTTP/HTTPS-сообщений в МБ, только целое число:
  - `>=` - фильтрация сообщений, размер которых больше или равен указанному числу.
  - `<=` - фильтрация сообщений, размер которых меньше или равен указанному числу.
- **MIME-типы** - форматы содержимого, к которым будет применяться правило. Форматы объединены в группы в зависимости от типа контента. Например, Audio (mp4, wav, wave и др.), Video (jpeg, mpeg, jmp и др.), Image (bmp, gif, png и др.). Настройки можно применить как к группе форматов, так и каждому формату отдельно.
- **HTTP-методы** - методы запроса, которые будут применяться для всего HTTP- или HTTPS-трафика. Используются для более точной фильтрации трафика, например, для ограничения скачивания чего-либо на сайтах, заполнения форм и т.п. Доступные методы:
  - GET - извлечение данных ресурса, содержащих тело ответа.
  - HEAD - извлечение данных ресурса, не содержащих тело ответа.
  - POST - отправка данных на определенный ресурс.
  - PUT - замена текущих значений ресурса.
  - DELETE - удаление ресурса.
  - OPTIONS - описание параметров соединения с ресурсом.
  - PATCH - частичное изменение ресурса.
  - TRACE - вызов возвращаемого тестового сообщения с ресурса.
  - CONNECT - установка соединения с ресурсом.
- **Направление данных**:
  - В обе стороны - фильтрация как входящего, так и исходящего трафика.
  - Входящее направление - фильтрация трафика на Ideco NGFW Novum от внешних источников.
  - Исходящее направление - фильтрация трафика от Ideco NGFW Novum к внешним ресурсам.
- **Проверка URL по маскам**:
  - **Маска** - шаблон URL. Значение не должно быть длиннее 255 символов. Максимальное количество URL - 100. Позволяет указать, какие именно URL-адреса внутри выбранной категории должны попадать под действие правила. Правило будет применяться исключительно к тем URL, которые соответствуют хотя бы одной из указанных масок, даже если остальные страницы сайта принадлежат той же категории.

> Для фильтрации по конкретным путям требуется расшифровка трафика - MITM. Это позволит системе анализировать полный URL. Если достаточно проверить весь домен или всю категорию целиком, расшифровка трафика не обязательна.

  - **Поиск** - поиск по введенным значениям **Маски**.
- **Действие**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик и направляет трафик в модули **Морфологический анализ** и **Антивирус**.
  - **Перенаправить на** - перенаправляет расшифрованный трафик на указанный URL.
  - **Расшифровать** - расшифровывает трафик с HTTPS-сайтов.
- **Профили антивируса** - выбор профиля **Антивируса**, которым требуется фильтровать трафик.

> Если выбрать действие **Перенаправить на**, то нужно создать аналогичное правило с действием **Расшифровать** и поместить его выше перенаправляющего правила.
>
> Для расшифрованного трафика при создании и редактировании правила **Контент-фильтра** можно настроить доступ к ресурсам с помощью HTTP-методов запроса и MIME-типов. Проверка не осуществляется по пустым полям.

- **Дополнительно**:
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **Рабочее время**), которые определяются в Объектах. По умолчанию установлено значение **Любой**.
  - **Комментарий** - произвольный текст. Значение не должно быть длиннее 255 символов.

2. Для подтверждения создания правила нажмите **Добавить**.

Порядок применения правил

Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. Если стоящее выше правило разрешает ресурс для определенной группы пользователей, то правила ниже применяться не будут:

- Зашифрованный трафик обрабатывается правилами **Разрешить**, **Запретить** и **Расшифровать**. При срабатывании правила **Расшифровать** трафик расшифровывается и проходит по правилам с начала.
- Расшифрованный трафик обрабатывается правилами **Разрешить**, **Запретить** и **Перенаправить на**.

Можно создавать гибкие настройки фильтрации, исключая нужных пользователей из-под действия блокировок вышестоящими правилами.

Если правила не действуют, проведите диагностику проблем.

Управление правилами

В столбце **Управление** можно:

Включать или выключать правило.
Менять приоритет.
Редактировать правило.
Удалять правило.

Правила **Контентной фильтрации** применяются сразу после создания или включения.

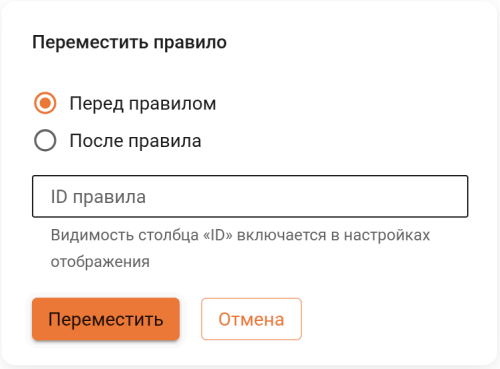
При наличии большого количества правил **Контент-фильтра** в таблице воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Для перемещения правил выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Особенности настройки правил

- При включении оператора `И` значения, выбранные в первом поле **Адрес**, нельзя указать во втором поле **Адрес**.
- Если хотя бы одно из условий **Источника** не выполняется, правило не применяется.
- Для расшифрованного трафика при создании и редактировании правила **Контент-фильтра** доступны более детальные настройки доступа к ресурсам с помощью HTTP-методов запроса, MIME-типов и проверки URL по маскам. Проверка не осуществляется по пустым полям.
- При создании шаблона **Маски** для проверки URL необходимо указывать протокол или использовать символ `*`. Важно учитывать правила:
  - Если `*` отсутствует в начале маски, поиск выполняется по точному совпадению с началом строки.
  - Если `*` отсутствует в конце маски, поиск осуществляется по точному совпадению с концом строки. Браузеры могут добавлять `/` в конце URL, поэтому рекомендуется всегда ставить `*` в конце маски. Например: `*example.com*` или `https://example.com*`.
  - Если в маске отсутствует `*`, поиск выполняется по точному совпадению всей строки.

Примеры использования масок

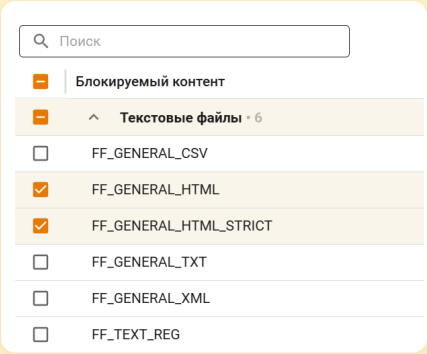
- `*example.com*` - сработает с `https://example.com`, `example.com/test` и `http://sub.example.com`.
- `*example.com` - сработает с `https://test.example.com` и `https://example.com`, не сработает с `https://example.com/path` и `https://example.com/`.

- `*//example.com*` - сработает с `https://example.com`, `http://example.com/path` и `https://sub.example.com/test`, не сработает с `https://sub.example.com`.
- `*//example.com` - сработает с `https://example.com` и `http://example.com`, не сработает с `http://example.com/path`, `https://example.com/` и `https://sub.example.com/`.
- `http*://example.com*` - сработает с `https://example.com`, `http://example.com/page`, не сработает с `ftp://example.com` и `https://sub.example.com/`.
- `https://example.com` - точное совпадение всей строки, которое сработает только с `https://example.com` и не сработает с `http://example.com` и `https://example.com/`.

Без расшифровки трафика (MITM):

- `*example.com*` - сработает с `https://example.com`, не сработает с `https://example.com/path`, `https://example.com/page`.

Антивирус блокирует веб-страницы, если в профиле Антивируса включена блокировка HTML-документов в **Текстовых файлах** и профиль выбран в правиле **Контент-фильтра**:



Полезные ссылки

- **Что делать, если не действуют правила Контент-фильтра**
- **Настройка HTTP-метода**
- **Настройка MIME-типов**
- **Блокировка загрузки файлов в файлообменники**
- **Блокировка популярных ресурсов**
- **Блокировка чат-ботов**

Описание категорий Контент-фильтра

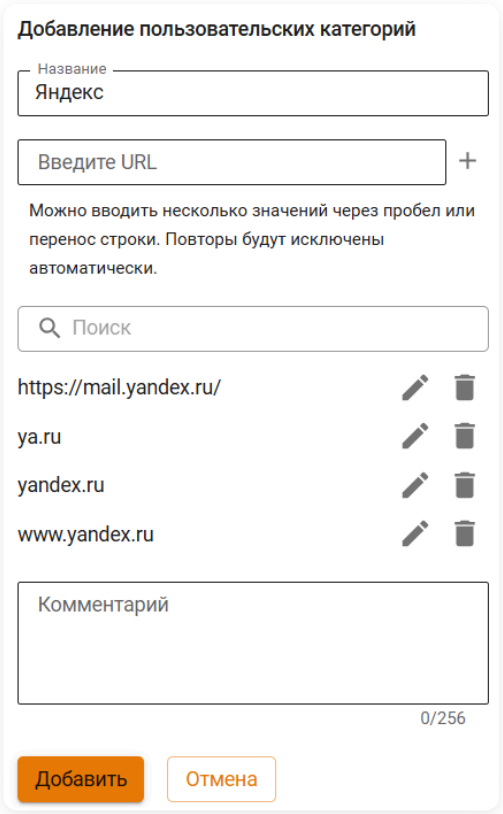
Классический контекст | Высокопроизводительный контекст

В Ideco NGFW Novum категории сайтов разделены на следующие виды:

- **Пользовательские** - категории, созданные на вкладке **Пользовательские категории**.
- **Расширенные** - автоматически пополняемые списки сайтов, отсортированные по темам.
- **Специальные** - системные категории для фильтрации запросов.
- **Файлы** - восемь сформированных категорий файлов, блокируемых по расширениям и MIME-типам. Предустановленные группы файлов (Исполняемые файлы, Архивы, Видеофайлы, Аудиофайлы, Flash-видео, Active-X, Torrent-файлы, Документы) нельзя редактировать. Для фильтрации HTTPS-трафика по категории файлов настройте расшифровку трафика.
- **Остальное** - системные категории для управления действиями пользователей в интернете. Для корректной работы по категории требуется расшифровка трафика.

Создание пользовательской категории

1. Нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Название** - название пользовательской категории, которое будет использоваться при настройке правила **Контент-фильтра**.
- **Введите URL** - адрес сайта/страницы или доменное имя (одно или несколько значений через пробел). Используйте следующие маски:
  - `1.1.1.1` - любой IP-адрес;
  - `test.ru`;
  - `www.test.ru`;
  - `http://www.test.ru/` или `https://www.test.ru/`;
  - `https://www.test.ru:8080`;
  - `https://xn--41a.xn-p1acf/` - punycode;
  - `*.test.ru` - для всех доменов третьего и выше уровней. **Важно:** такая маска не включает домен второго уровня `test.ru`. Чтобы добавить домен, достаточно указать `test.ru` (все поддомены также будут включены в правило).

Если URL или домен содержит специальные символы (。 или •), оставьте символы в исходном виде. Адрес будет автоматически закодирован в формат punycode.

- **Поиск** - поле поиска добавленных URL.
- **Комментарий** - необязательное поле. Не более 256 символов.

Вместо домена `.test` указывайте реальный домен.

Избегайте дублирования доменов в разных категориях. Например, если есть категория с `domain.ru`, добавление отдельной категории для `www.domain.ru` нарушит работу правил и `domain.ru` перестанет применяться к поддоменам, даже если новые категории не используются в правилах.

2. Для подтверждения создания категории нажмите **Добавить**.

Если в таблице большое количество пользовательских категорий, воспользуйтесь кнопкой **Фильтры**.

Специальные категории

- **Все запросы** - под эту категорию попадают все запросы к веб-ресурсам.
- **Все категоризированные запросы** - все запросы к веб-ресурсам, категоризированные по встроенным или пользовательским категориям.
- **Все не категоризированные запросы** - все запросы к веб-ресурсам, которые не были категоризированы по встроенным или пользовательским категориям.
- **Прямое обращение по IP** - запросы к веб-ресурсам по IP-адресу (http://84.201.128.105/).

Остальные категории

- **Активность в социальных сетях** – запрещает действия по публикации контента (написание постов, загрузка медиафайлов, комментирование) во ВКонтакте, сохраняя возможность просмотра материалов.
- **Загрузка файлов в файлообменники** – блокирует загрузку файлов в облачные хранилища (Google Диск, Яндекс.Диск, Облако Mail, Dropbox, OneDrive). Пример представлен в статье.

Расширенные категории

База URL-адресов, отсортированных по тематикам. Для обновления расширенных категорий включите опцию **Расширенная база категорий** на вкладке **Настройки**.

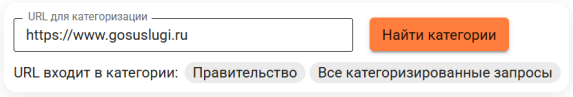
Расширенные категории

Категория	Описание
VPN, Прокси и анонимайзеры	Системы и сайты, предназначенные для обхода блокировок и получения доступа к нежелательным ресурсам в сети
Автомобили и транспорт	Сайты для автомобилистов. Сайты покупки и продажи автомобилей
Агрессия, расизм, терроризм	Сайты, посвященные пропаганде агрессии, расизма и терроризма
Алкоголь и табак	Сайты с информацией об алкоголе и табаке. Табачные и алкогольные интернет-магазины
Аниме	Видеоархивы с аниме-фильмами и сайты с рецензиями на аниме
Астрология	Сайты, посвященные оккультизму и астрологии, сайты астропрогнозов
Бизнес, экономика, маркетинг	Сайты с экономической информацией, новости бизнеса и деловой активности
Блоги и персональные сайты	Системы массового хостинга, блоги
Блокировка по предписанию	Сайты и материалы в сети, в отношении которых есть решение суда о запрете на публикацию
Веб-почта	Сайты веб-почты
Войска и вооружения	Сайты с информацией о вооружениях и армии
Вредоносное ПО	Сайты, распространяющие вирусы и преступное программное обеспечение
Генерация поддельных доменов	Алгоритмы, предназначенные для периодической генерации большого количества доменных имен
Грубость, матерщина, непристойность	Сайты, содержащие избыточное количество нецензурной лексики, а также немодерируемые форумы

Дом, семья, хобби	Сайты о домоводстве, семье, различных хобби
Доски объявлений	Сайты и порталы для размещения частных объявлений
Досуг и развлечения	Сайты кафе и ресторанов. Прочая информация о досуге и развлечениях
Закон о защите молодежи (Германия)	Сайты с материалами, которые могут навредить несовершеннолетним согласно немецкому законодательству
Здоровье и здравоохранение	Сайты больниц, поликлиник, прочих медицинских организаций, медицинские порталы
Знакомства	Сайты знакомств
ИИ Чат-боты	Сайты систем искусственного интеллекта
Интернет-библиотеки	Сайты, содержащие публикации книг и статей. Сайты с возможностью загрузки текстов художественных произведений
Интернет-магазины	Сайты интернет-магазинов и торговые площадки
Искусство	Сайты музеев. Сайты, посвященные искусству
Казино, лотереи, тотализаторы	Сайты казино, ставок и прочих азартных игр
Компьютерные игры	Сайты, посвященные компьютерным играм, и игровые серверы
Компьютеры и Интернет	Сайты, основной тематикой которых являются информационные технологии, программное обеспечение, интернет, компьютеры
Корпоративные сайты	Сайты организаций
Криптомайнинг	Майнинг злоумышленниками в браузере пользователя или на его устройстве
Наркотики	Сайты, рекламирующие или продающие наркотики, а также содержащие информацию о технологиях приготовления и употребления наркотических веществ
Наука и технологии	Сайты научных организаций. Информация и новости научного сообщества
Недавно зарегистрированные домены	Сайты, которые были созданы недавно
Недвижимость	Сайты с информацией о продаже и покупке недвижимости
Неиспользуемые домены	Неиспользуемые домены без контента, предназначенные для перепродажи любому покупателю
Некоммерческие организации	Сайты некоммерческих организаций
Новости и СМИ	Сайты новостных агентств и СМИ
Образование и учебные учреждения	Сайты образовательных учреждений, образовательные порталы
Онлайн-реклама и баннеры	Сервисы доставки рекламных объявлений и баннеров
Плагиат и рефераты	Архивы рефератов, ответов на вопросы ЕГЭ, готовые домашние задания и т.п.
Платные сайты сотовых операторов	Сайты сотовых операторов, за доступ к которым взимается отдельная плата с абонента
Поисковые системы	Сайты для поиска информации
Политика, общество, закон	Сайты политических новостей и политических партий. Справочники законов
Порнография и секс	Сайты, содержащие порнографию в любом виде
Порталы	Объединение из нескольких сайтов одной тематики
Правительство	Официальные сайты государственных органов
Программы-вымогатели	Сайты, связанные с программами-вымогателями
Работа и найм	Порталы поиска работы, сайты для размещения резюме и вакансий
Радио и музыка онлайн	Сайты онлайн-радиостанций и стриминговых сервисов
Реестр запрещенных сайтов	Реестр сайтов Роскомнадзора
Религия и атеизм	Сайты религиозных и антирелигиозных организаций, оккультных верований и учений
Сайты для взрослых	Сайты с возрастной маркировкой для взрослых
Сайты для детей	Сайты с детской возрастной маркировкой
Сексуальное насилие над детьми (Arachnid)	Сайты с детской эксплуатацией на основе базы Arachnid
Сексуальное насилие над детьми (IWF)	Сайты, связанные с эксплуатацией детей, на основе черного списка Internet Watch Foundation
Сети зараженных устройств и управляющие серверы	C&C-серверы, ботнеты, фишинговые и вредоносные хосты из черных списков
Социальные сети	Страницы социальных сетей
Спорт	Сайты, посвященные спорту или спортивным организациям
Торговля и покупки	Сайты о торговле и покупках, не относящиеся к категории интернет-магазинов
Торренты и P2P-сети	Сайты торрент-трекеров и P2P-систем

Трекеры и аналитика	Адреса систем учета посещений и веб-аналитики, в том числе системы слежения за пользователями
Туризм	Сайты, посвященные туризму и путешествиям
Файловые архивы	Файловые архивы программного обеспечения, файлообменники
Федеральный список Минюста	Материалы, внесенные в список экстремистских Министерством Юстиции РФ
Фильмы и видео онлайн	Сайты для онлайн-просмотра фильмов и видео
Финансы и финансовые учреждения	Сайты банков и прочих финансовых организаций
Фишинг и поддельные сайты	Фишинг и регистрация доменных имен, близких по написанию с адресами популярных сайтов.
Форумы	Сайты, предназначенные для дискуссий и обмена сообщениями между пользователями
Фотогалереи	Архивы фотографий, фотостоки
Чаты и мессенджеры	Сайты и серверы чатов и мессенджеров
Индикаторы компрометации ФинЦЕРТ	Адреса из ежедневных бюллетеней ФинЦЕРТ
Юмор	Юмористические и развлекательные сайты

Чтобы определить категорию сайта перейдите в раздел **Правила трафика** → **Контент-фильтр** и введите домен для проверки в поле **URL для категоризации**:



При нахождении несоответствия сайта и категории обратитесь в техническую поддержку или поменяйте категорию сайта на вкладке Переопределение категорий.

Полезные ссылки

- **Блокировка загрузки файлов в файлообменники**
- **Блокировка чат-ботов**

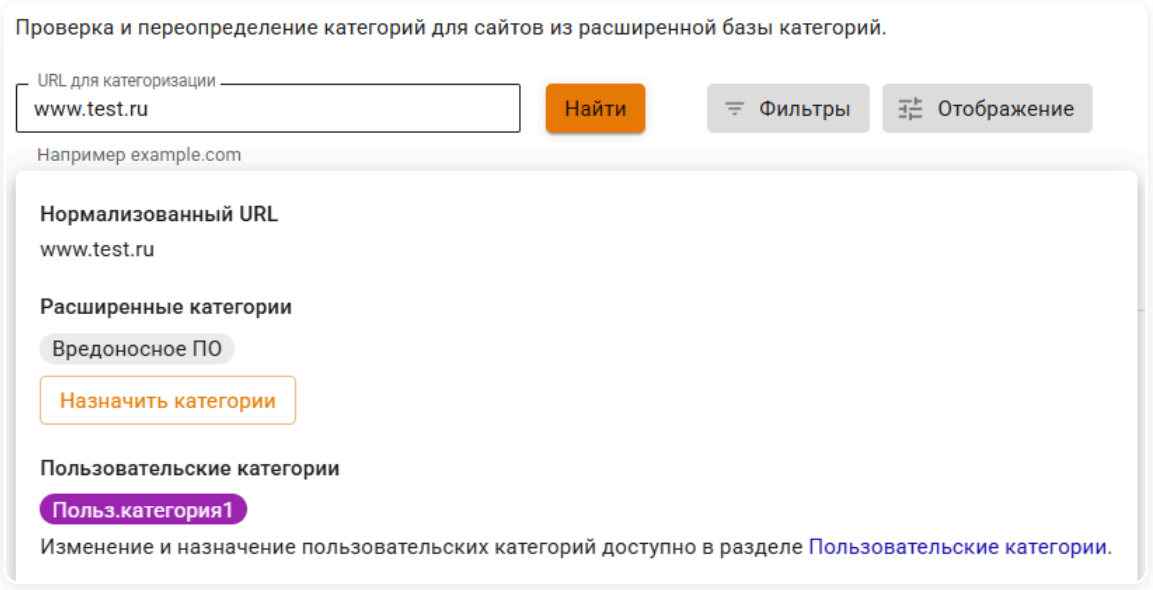
Переопределение категорий

Классический контекст | Высокопроизводительный контекст

На вкладке можно проверить, к каким категориям относится адрес сайта. При необходимости можно удалить некорректную категорию или назначить новую из расширенной базы категорий.

Проверка категорий

Для проверки категорий сайта введите URL в формате `example.com` в поле **URL для категоризации** и нажмите **Найти**. В результатах отобразятся расширенные и пользовательские категории, если URL содержится в них:



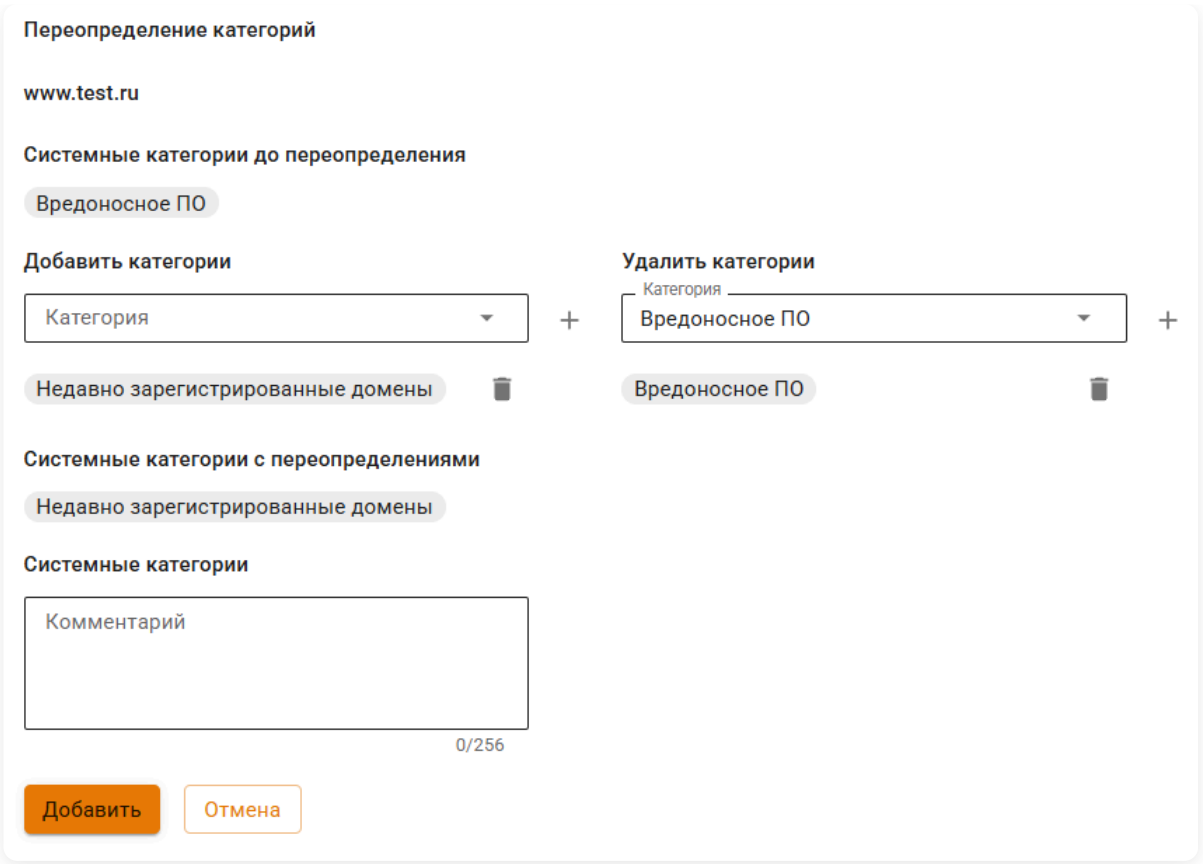
Для редактирования пользовательских категорий перейдите на вкладку **Пользовательские категории**.

Если URL отсутствует в базе расширенных категорий, то добавьте URL в подходящую пользовательскую категорию или создайте новую.

Создание правил переопределения

Для переопределения категорий выполните действия:

1. Нажмите **Переопределить** и заполните поля:

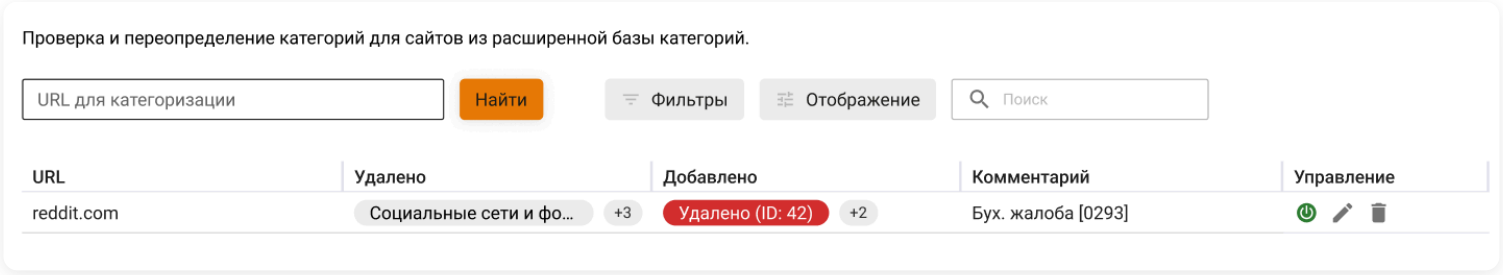


- **Добавить категории** - выберите из списка подходящую категорию и нажмите +. Не должна повторяться с уже назначенной категорией.
- **Удалить категории** - выберите из списка назначенную категорию и нажмите +. Не должна повторяться с добавляемой категорий.
- **Комментарий** - необязательное поле. Не более 256 символов.

2. Нажмите **Добавить**.

Управление правилами

В столбце **Управление** можно включать или выключать правило переопределения, редактировать и удалять. Правила применяются сразу после создания или включения:



При наличии большого количества правил в таблице воспользуйтесь кнопкой **Фильтры**.

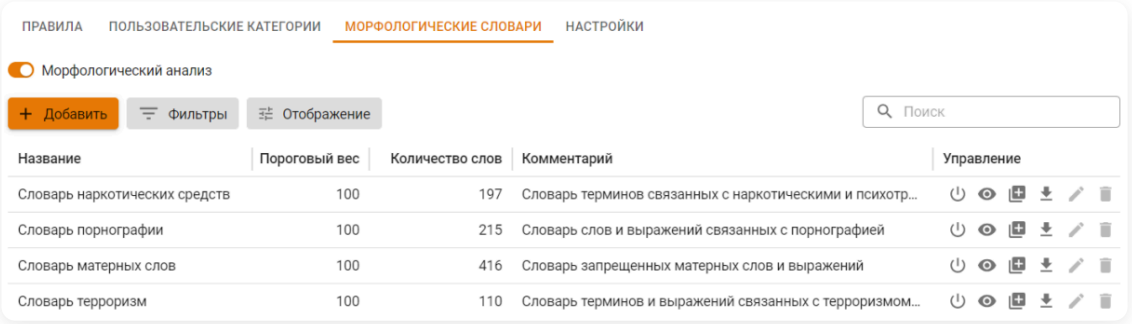
Если в таблице добавленные категории отмечены как удаленные:
1. Удалите неактуальную категорию.
2. При необходимости добавьте близкую по тематике.

Морфологические словари

Функциональность доступна в **Классическом** и **Системном контекстах**.

На вкладке **Морфологические словари** создаются и редактируются словари для проведения морфологического анализа сайтов. Если в тексте анализируемого сайта содержится достаточное для блокировки количество предварительно заданных слов и словосочетаний, доступ к ресурсу блокируется.

Для активации морфологического анализа включите опцию **Морфологический анализ**:



Для работы морфологического анализа требуется:

- Наличие хотя бы одного **включенного словаря**. Если ни один словарь не включен, морфологический анализ не проводится.
- Расшифровка трафика - создайте правило расшифровки в **Контент-фильтре**.

В Ideco NGFW Novum предустановлены четыре словаря (по умолчанию отключены):

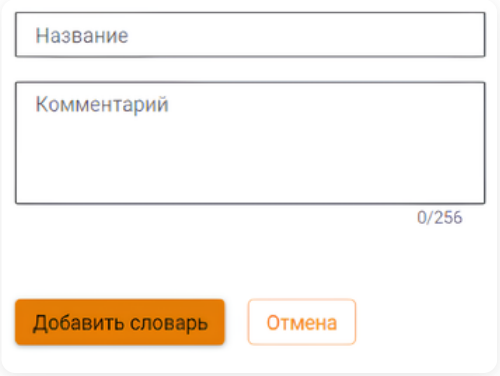
- Словарь наркотических средств
- Словарь порнографии
- Словарь матерных слов
- Словарь терроризм

Предустановленные словари можно включать или отключать, но нельзя редактировать и удалять.

Добавление морфологического словаря

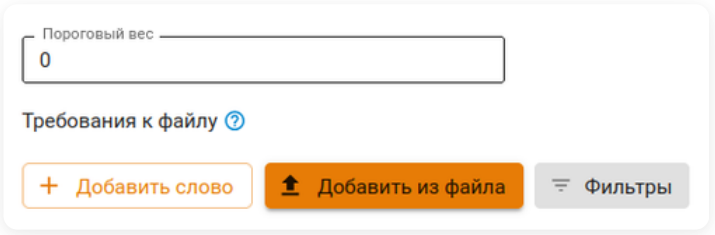
1. Нажмите **Добавить** и заполните поля:

Описание



- **Название** - название добавляемого словаря.
- **Комментарий** - произвольный текст. Значение не должно быть длиннее 255 символов.

Слова



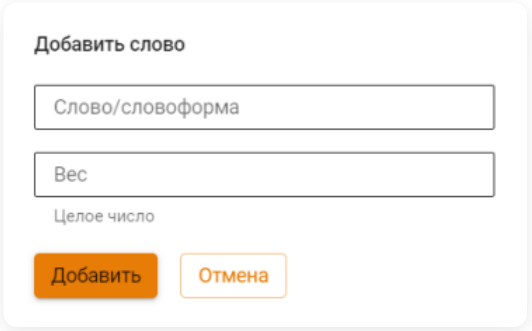
- **Пороговый вес** - общий вес указанных в настройках словаря слов (целое число от 0 до 2 147 483 648).

> Если при проверке сайта общий вес найденных на нем слов превысит пороговый, доступ к сайту будет заблокирован.

Добавьте слова для блокировки трафика вручную или загрузите из файла:

Вручную

Нажмите **Добавить слово** и заполните поля:



- **Слово/словоформа** - введите слово или словосочетание для блокировки трафика.
- **Вес** - укажите целое число.

Загрузка из файла

Нажмите **Добавить из файла** и выберите файл. В один словарь можно загружать несколько файлов. В этом случае дублирующиеся слова будут удалены, останется только одно вхождение с установленным весом.

Требования к загрузке из файла:

- Формат файла - CSV, кодировка - UTF-8.
- В одной строке должно быть одно слово или словосочетание и вес, разделенные точкой с запятой (`;`).
- Допустимо не указывать вес слова. В этом случае по умолчанию к каждому слову/словосочетанию без веса применится значение `20`, а файл будет представлять собой список без разделителей.

При неудачной загрузке файла появится окно с уведомлением **Файл не соответствует требованиям**.

Примеры файлов

- **Файл с указанием веса:**

```
слово;20
словосочетание;20
```

- **Файл без указания веса:**

```
слово
словосочетание
```

Пример работы:

При загрузке файлов и при **Пороговом значении** = `100` доступ к сайту будет заблокирован, если на сайте найдено 5 и более совпадений ("слово" и/или "словосочетание").

> Чтобы снизить вероятность блокировки сайта из-за морфологического анализа, уменьшите вес слов. Для повышения вероятности блокировки - увеличьте вес.

2. Для сохранения настроек нажмите **Добавить словарь**.

Если в таблице большое количество морфологических словарей, воспользуйтесь кнопкой **Фильтры**.

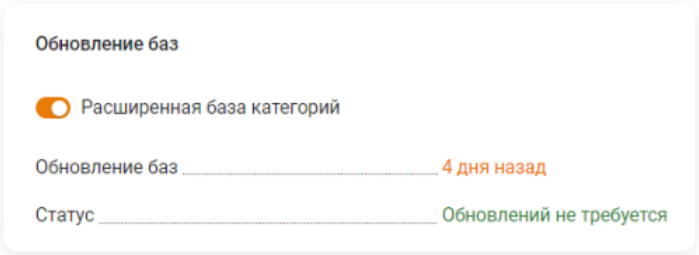
Результат морфологического анализа представлен в разделе **Отчеты и журналы** → **Веб-трафик**:

			Контент-фильтр					Антивирус		Источник				Наз...	
Д...	Резуль...	Причина	Резуль...	Расш...	Названи...	Категории сайта	Категория сработки	Резул...	Проф...	IP-адрес	Польз...	Группа	URL	IP-ад...	Общий, МБ
30.06....	✗	Словарь порнографии	✗	✗	–	Компьютерные и...	–	✓	defau...	192.16...	Mstisl...	Support	safeb...	8.8....	0,00
30.06....	✗	Словарь порнографии	✗	✗	–	Юмор	–	✓	defau...	192.16...	Pavel ...	Office	beac...	7.7....	0,01

Настройки

Обновление баз

Активация опции **Расширенная база категорий** включает автоматически обновляемые Расширенные категории, доступные при активной подписке в платных версиях продукта:



Если отключить опцию **Расширенная база категорий**, то все правила, включающие **Расширенные категории**, перестанут срабатывать.

Настройки безопасности

Блокировать протоколы QUIC и HTTP/3 - протоколы, используемые современными браузерами для доступа к ресурсам (например, Google и YouTube). Рекомендуется заблокировать QUIC и HTTP/3, иначе будет невозможно фильтровать ресурсы, работающие по данным протоколам. Заблокированный трафик нельзя исключить через списки исключений в **Прокси** → **Исключения**.

Безопасный поиск - принудительно включает безопасный поиск в поисковых системах (Google, Yandex, YouTube, Yahoo, Bing, Rambler).

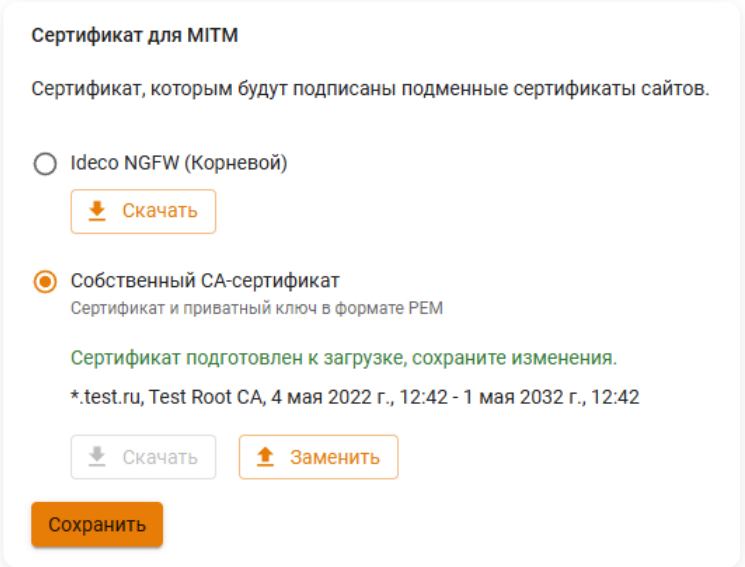
Для корректной работы необходимо включить HTTPS-фильтрацию с подменой сертификата для этих сервисов.

Сертификат для MITM

Если для повторного шифрования требуется использовать сторонний сертификат (не корневой сертификат Ideco NGFW Novum):

1. Нажмите **Загрузить** и выберите нужный сертификат.

2. Сохраните изменения:



Требования к стороннему сертификату:

- Должен быть выдан удостоверяющим центром **Certificate Authority**.
- Имеет расширение **.pem**.
- Содержит приватный ключ.

Настройка фильтрации HTTPS

В Ideco NGFW Novum фильтрация реализуется следующими методами:

- **Анализ заголовков Server Name Indication (SNI)** - благодаря этому методу возможен анализ домена, к которому подключается клиент, без подмены сертификата и вмешательства в HTTPS-трафик. Также анализируются домены, указанные в сертификате. Фильтрация HTTPS по SNI включена по умолчанию.
- **Метод SSL-bump** - фильтрация происходит путем динамической подмены сертификата сайта на **корневой сертификат Ideco NGFW Novum**. Таким образом, передающийся по защищенному HTTPS-соединению трафик становится доступным для обработки всем модулям Ideco NGFW Novum: антивирусу Касперского, внешним ICAP-сервисам и Контент-фильтру (можно категоризировать полный URL запроса и MIME-тип контента).

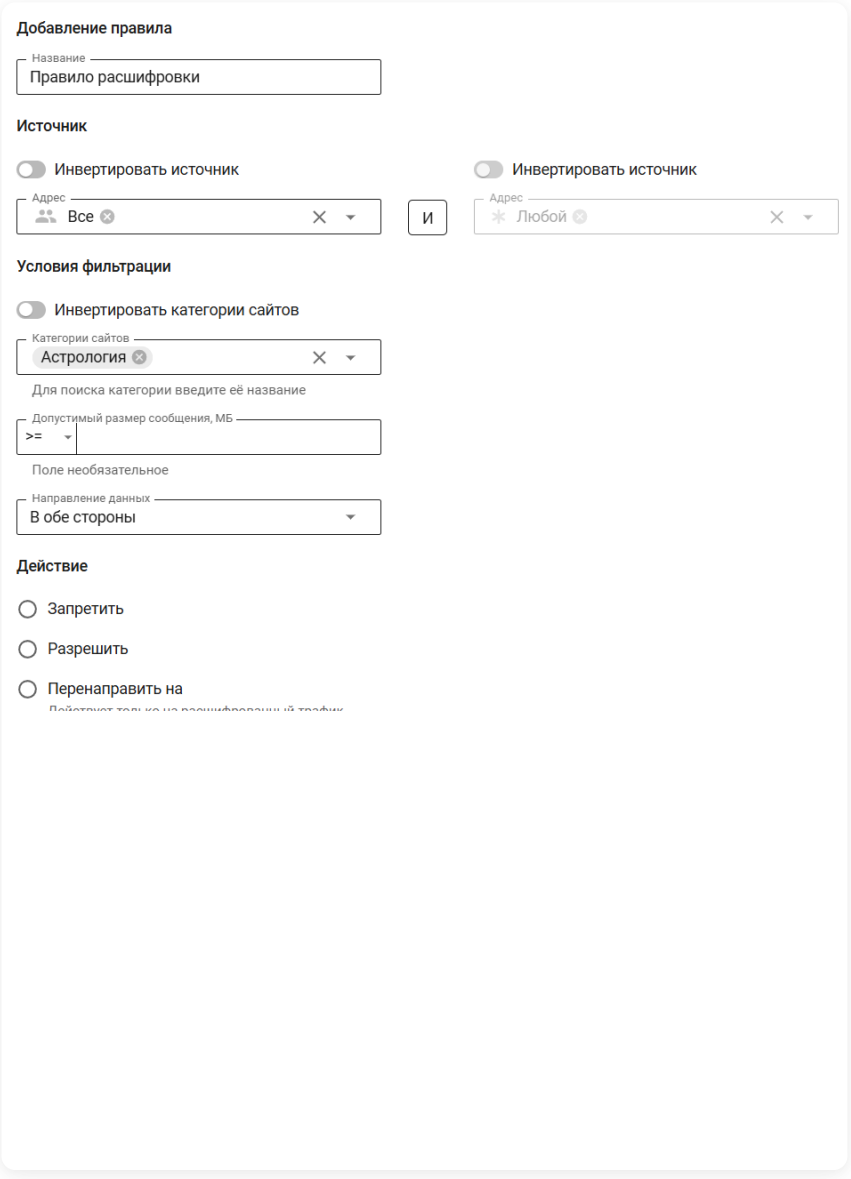
Настройка сервера и рабочих станций

Для работы SSL-bump требуется **настройка на обеих сторонах подключения**: сервера Ideco NGFW Novum и рабочей станции каждого пользователя в локальной сети.

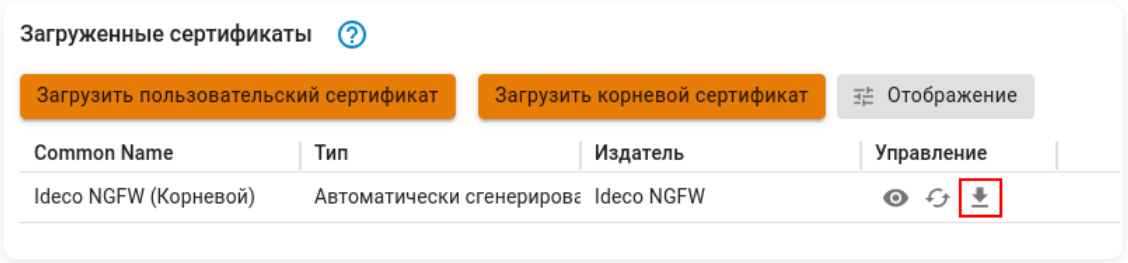
Настройка сервера Ideco NGFW Novum

1. Создайте правило расшифровки HTTPS-трафика в **Правила трафика** → **Контент-фильтр** → **Правила**. Создание правил подробно описано в статье.

Пример правила для расшифровки:



2. Скачайте корневой SSL-сертификат в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



Установка корневого сертификата на рабочей станции

При включенном правиле расшифровки HTTPS-трафика клиентские приложения (браузер, антивирусы, клиенты IM и другое сетевое ПО) потребуют подтверждения для подменного сертификата. Чтобы исключить появление предупреждений безопасности, установите корневой сертификат сервера Ideco NGFW Novum в операционной системе.

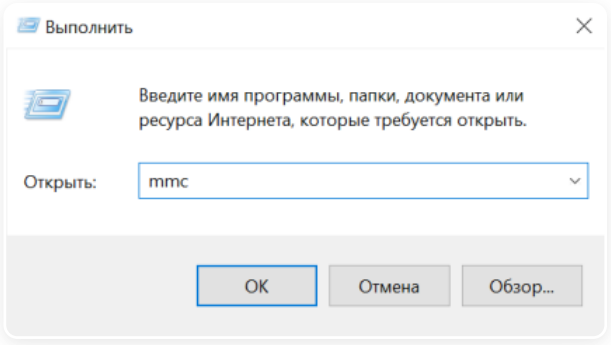
Установка сертификата на Linux

Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

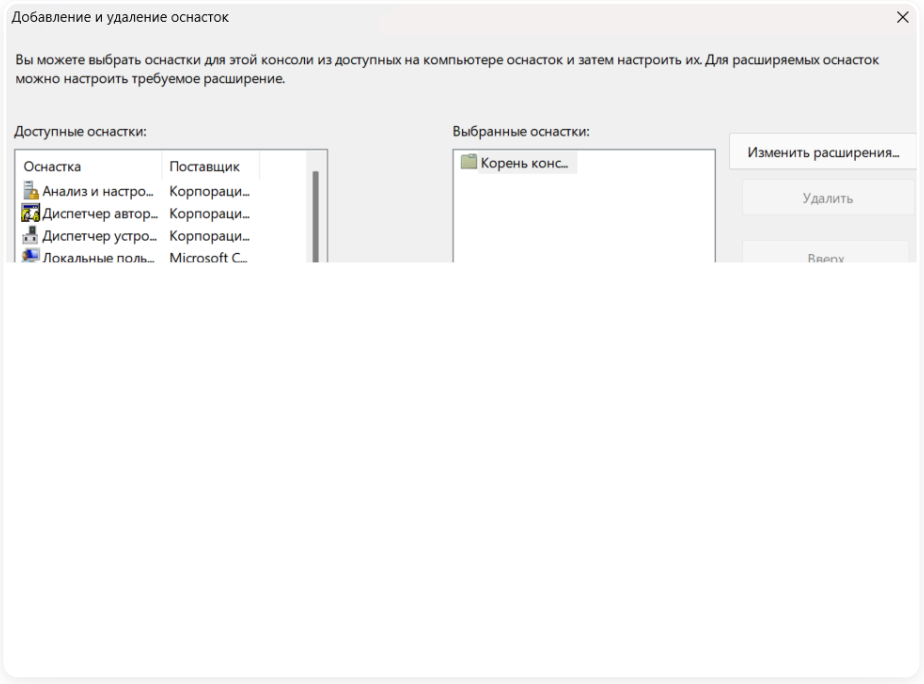
Установка сертификата на Windows

1. Откройте на рабочей станции центр управления сертификатами: **Пуск** → **Выполнить**, выполнив в диалоге команду **mmc**:



2. В меню **Файл** выберите **Добавить или удалить оснастку**:

3. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите кнопку **Добавить**:



4. В открывшемся окне выберите пункт **Учетной записи компьютера** и нажмите кнопку **Далее**:

5. В окне **Выбор компьютера** оставьте флаг **Локальный компьютер** и нажмите кнопку **Готово**.

6. В левой части окна нажмите на стрелку рядом с директорией **Сертификаты (локальный компьютер)** → **Доверенные корневые сертификаты** → **Сертификаты**:

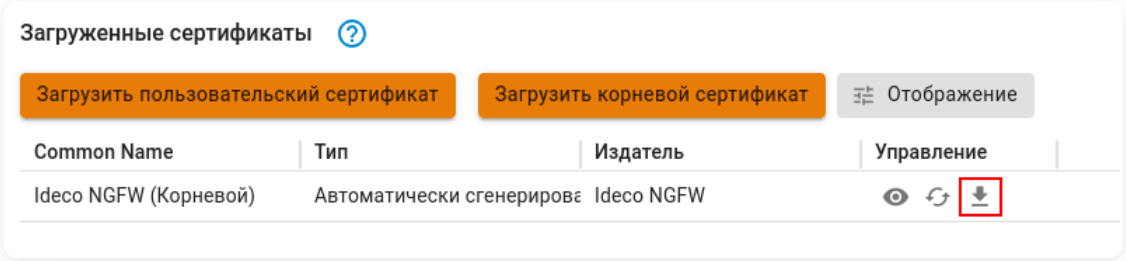
7. В меню **Действие** выберите **Все задачи** → **Импорт**:

8. Следуя инструкциям Мастера импорта сертификатов, импортируйте корневой сертификат сервера Ideco NGFW Novum. Импортированный сертификат появится в списке в правой части окна:

Автоматическая установка сертификата через Active Directory

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, можно установить сертификат Ideco NGFW Novum для всех пользователей автоматически с помощью Active Directory. Для этого необходимо выполнить действия:

1. Скачайте корневой SSL-сертификат в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



2. Зайдите на контроллер домена с правами администратора.

3. Запустите оснастку управления групповой политикой, выполнив команду **gpmc.msc**.

4. Найдите **политику домена**, использующуюся на компьютерах пользователей в **Объектах групповой политики** (Default Domain Policy). Нажмите на нее правой кнопкой мышки и выберите **Изменить**.

5. В открывшемся редакторе управления групповыми политиками выберите: **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Политики открытого ключа** → **Доверенные корневые центры сертификации**.

6. Нажмите правой кнопкой мыши по открывшемуся списку, выберите **Импорт** и импортируйте ключ Ideco NGFW Novum:

7. После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Настройка повторного шифрования трафика

1. В **Сервисы** → **Сертификаты** → **Загруженные сертификаты** загрузите сертификат, который будет использоваться для шифрования.

2. Перейдите в **Правила трафика** → **Контент-фильтр** → **Настройки**.

3. Выберите в пункте **Сертификат для MITM** сертификат, загруженный на шаге 1.

> Клиенты должны иметь загруженный сертификат в доверенных хранилищах. Рекомендации по настройке компьютера пользователя можно найти в разделе **Установка корневого сертификата на рабочей станции**.

Возможные проблемы и методы решения

Проблема	Решение
Включения расшифровки трафика может быть недостаточно для подмены сертификата некоторых сайтов (например, `ya.ru`, `google.com`).	Включить опцию **Блокировать протоколы QUIC и HTTP/3** в **Правила трафика** → **Контент-фильтр** → **Настройки**.

Проблема	Решение
Браузер не использует системное хранилище сертификатов.	1. Добавить сертификат Ideco NGFW Novum в доверенные сертификаты браузера. 2. В Mozilla Firefox присвоить параметру `security.enterprise_roots.enabled` (в **about:config**) значение `true` для доверия системным сертификатам.
На локальной машине используется антивирус, проверяющий HTTPS-трафик методом подмены сертификатов (сайты могут не открываться из-за двойной подмены сертификатов).	Отключить в настройках антивируса проверку HTTPS-трафика.
Обработка HTTPS-трафика по умолчанию (анализ SNI). NGFW Novum не пропускает по HTTPS-порту трафик, отличный от HTTPS.	Разрешить обход прокси-сервера к нужным ресурсам.
Блокировка HTTPS-ресурсов без отображения страницы блокировки.	Настроить доверие корневому SSL-сертификату NGFW Novum (даже при включенной только SNI-фильтрации), так как при блокировке HTTPS-ресурса будет применен SSL-bumping с подстановкой SSL-сертификата NGFW Novum для подмены контента ресурса страницей о блокировке сервером.

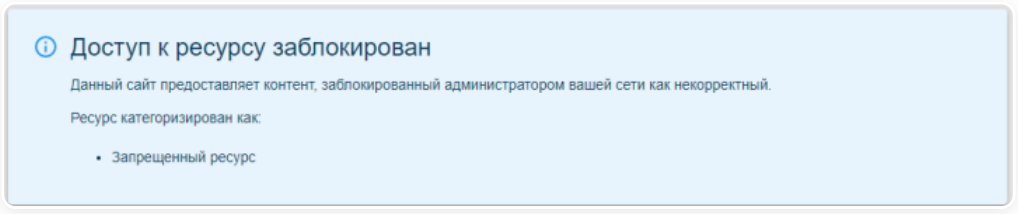
Полезные ссылки

- **Установка корневого сертификата на Astra Linux**
- **Установка корневого сертификата на Alt Linux**
- **Установка корневого сертификата на Red OS**
- **Установка корневого сертификата на Ubuntu/Debian**
- **Использование собственного CA-сертификата в Контент-фильтре**
- **Настройка HTTP-метода**
- **Настройка MIME-типов**

Изменение страницы блокировки Контент-фильтра

Классический контекст | Высокопроизводительный контекст

Страница блокировки Контент-фильтра по умолчанию содержит уведомление о блокировке доступа к ресурсу и категоризацию:



В процессе обновления Ideco NGFW Novum все ранее настроенные параметры шаблона блокировки могут быть сброшены.

Все внесенные изменения в шаблоны рекомендуется сохранить вне NGFW Novum, чтобы избежать их потери при обновлении. После обновления может потребоваться адаптация шаблонов под новую версию системы.

Для создания персонализированного шаблона страницы выполните действия:

1. Загрузите новый файл в директорию **/usr/share/ideco/vendor/**, чтобы изменить фавикон. Перейдите в **Управление сервером -> Администраторы** и убедитесь, что доступ по SSH разрешен. Затем откройте терминал на компьютере и введите команду:

```
scp C:\Users\Admin\Downloads\favicon.png admin@192.168.0.23:/usr/share/ideco/vendor
```

- `C:\Users\Admin\Downloads\favicon.png` - путь к файлу на вашем компьютере;
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW;
- Файл обязательно должен иметь имя **favicon.png**.

2. Загрузите новые файлы в директорию **/usr/share/ideco/proxy-backend/error_page_templates/images**, чтобы изменить иконки предупреждения. Введите команду:

```
scp C:\Users\Admin\Downloads\IDECO_ICON_INFO.svg admin@192.168.0.23:/usr/share/ideco/proxy-backend/error_page_templates/image
```

- `C:\Users\Admin\Downloads\IDECO_ICON_INFO.svg` - путь к файлу на вашем компьютере;
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW;
- Файлы обязательно должны иметь имя **IDECO_ICON_ERROR.svg, IDECO_ICON_INFO.svg, IDECO_ICON_SUCCESS.svg, IDECO_ICON_WARNING.svg**.

3. Чтобы изменить CSS-файл стилей для страниц ошибок, перейдите в директорию **/usr/share/ideco/proxy-backend/error_page_templates/** и откройте файл **style.css** в текстовом редакторе:

```
nano /usr/share/ideco/proxy-backend/error_page_templates/style.css
```

Пример изменения файла style.css

Чтобы изменить цвет текста и фона, отредактируйте блоки `error`, `warning`, `info`, `success`:

```
.error {
  background-color: #E6E2DD;
  color: #373A36;
}

.warning {
  background-color: #E6E2DD;
  color: #373A36;
}
```

```
.info {
  background-color: #E6E2DD;
  color: #373A36;
}

.success {
  background-color: #E6E2DD;
  color: #373A36;
}
```

Чтобы изменить цвет страницы, размер и отступы текста, отредактируйте блок `body`:

```
body {
  padding: 5% 12px;
  box-sizing: border-box;
  overflow: auto;
  background-color: #E6E2DD;
  font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
  font-size: 10px;
  line-height: 14px;
}
```

Чтобы изменить размер шрифта, отредактируйте блоки `h1` и `p`:

```
h1 {
  margin: 0;
  padding-bottom: 8px;
  font-weight: 500;
  font-size: 24px;
  line-height: 25px;
}

p {
  margin: 0;
  padding: 8px 0;
  font-style: normal;
  font-weight: normal;
  font-size: 14px;
  line-height: 16px;
}
```

Чтобы изменить цвет гиперссылок, отредактируйте блок `a`:

```
a {
  color: #D48166;
  text-decoration: none;
}
```

Чтобы изменить размер логотипа, отредактируйте блок `.icon`:

```
.icon {
  width: 150px;
  min-width: 150px;
  height: 150px;
  min-height: 150px;
  margin-right: 100px;
  background-position: center;
  background-size: cover;
}
```

Результат:

4. Отредактируйте HTML-файл, чтобы изменить общий шаблон для страниц ошибок. Перейдите в директорию **/usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU** и откройте файл **ERR_TEMPLATE.html** в текстовом редакторе:

```
nano /usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU/ERR_TEMPLATE.html
```

Пример изменения файла ERR_TEMPLATE.html

```
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width" />
  <link rel="icon" type="image/x-icon" href="IDECO_ICON_FAVICON">
  <link rel="apple-touch-icon" href="IDECO_ICON_FAVICON">
  <title>Доступ заблокирован</title>
  <style type="text/css">%l</style>
</head>

<body>
  <div class="widget info viewport_big">
    <span class="icon"></span>
    <div class="widget_content">
      <h1>Доступ заблокирован</h1>
      <p>Данный сайт предоставляет контент, заблокированный администратором. Причины блокировки описаны во <a href="https://t
      <p>Ресурс категоризирован как:</p>
      %O
      <p>Для предоставления доступа к ресурсу обратитесь к системному администратору одним из способов:</p>
      <p>Тел.: +7(000)000-00-00</p>
      <p>administrator@mail.ru</p>
      <p><a href="https://t.me/admin">Отправить заявку в Telegram</a></p>
    </div>
  </div>
  <div class="blocked_content">
    <h1>Контент заблокирован</h1>
  </div>
</body>
```

Пример страницы:

Полезные переменные, которые можно использовать в файле ERR_TEMPLATE.html

`%O` - категория в виде списка
`%o` - категория текстом
`%i` - IP-адрес клиента
`%U` - URL
`%L` - строка `Сервер: <имя-ngfw>`
`%E` - строка `[<текст-ошибки>]`, если ошибки не было, то `[No Error]`
`%e` - код ошибки, если ошибки не было, то `0`
`%t` - дата и время
5. Перейдите в **Управление сервером -> Терминал** и удалите директорию, в которой хранятся файлы кеша страниц ошибок:

```
rm -R /var/cache/ideco/proxy-backend/error_pages
```

6. Перезапустите сервис `ideco-proxy-backend`:

```
systemctl restart ideco-proxy-backend.service
```

7. Проверьте, корректно ли работают страницы ошибок, перейдя по запрещенным ссылкам.

Ограничение скорости

Классический контекст | Высокопроизводительный контекст

> Служба предназначена для ограничения скорости входящего интернет-трафика для пользователей сети.

Название службы раздела **Ограничение скорости**: `ideco-shaper-backend`.

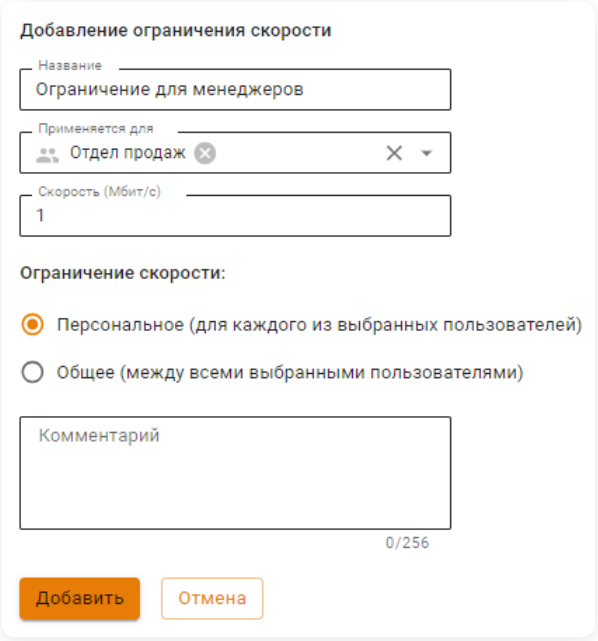
Список имен служб для других разделов доступен по ссылке.

В разделе **Ограничение скорости** создаются правила, позволяющие ограничить скорость входящего интернет-трафика для пользователей сети.

Модуль **Ограничение скорости** работает только при наличии хотя бы одного включенного правила. Если правила не созданы или все отключены, модуль будет находиться в статусе **Остановлен**.

Для исключения пользователя или групп пользователей из обработки правил **Ограничения скорости** добавьте соответствующее правило в разделе **Исключения**.

1. Для создания правила в **Правила трафика** → **Ограничение скорости** нажмите **Добавить** и заполните поля:

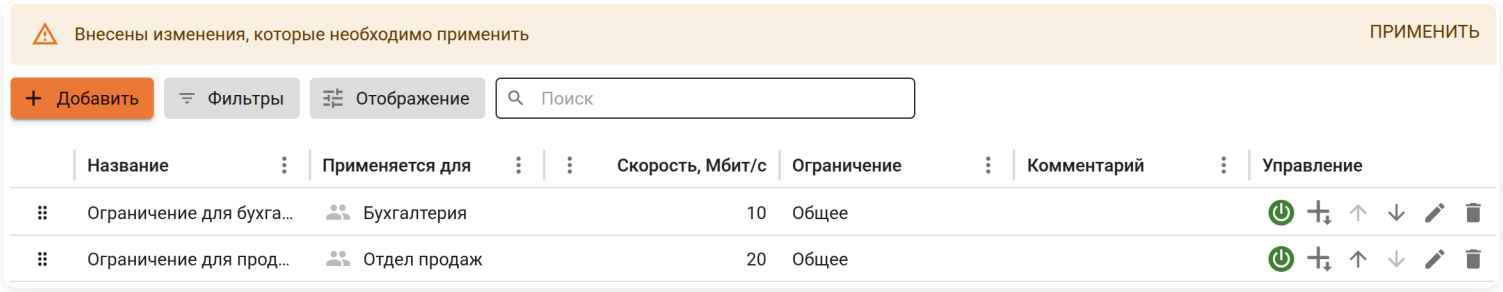


Расшифровка полей

- **Название** - введите название правила, например, Ограничение для менеджеров.
- **Применяется для** - выберите из выпадающего списка пользователя, группу и/или IP-адрес.
- **Скорость (Мбит/с)** - укажите лимит скорости.
- **Ограничение скорости** - выберите тип ограничения скорости:
  - **Персональное** - скорость будет ограничена для каждого из выбранных пользователей. Если под одной учетной записью авторизованы несколько устройств, каждое устройство получает отдельный полный лимит скорости.
  - **Общее** - скорость будет ограничена и разделится между всеми выбранными пользователями. Если под одной учетной записью авторизованы несколько устройств, суммарный лимит распределяется между всеми устройствами.

2. Нажмите **Добавить**.

3. Для применения созданного правила нажмите **Применить** над таблицей:



Если не применить правило и покинуть раздел **Ограничение скорости**, то созданное правило сохранится, но не будет действовать. Для применения правила вернитесь в раздел **Ограничение скорости** и нажмите **Применить**.
Не примененные правила будут удалены:

- При перезагрузке сервера.
- При переключении на другую ноду кластера.

В столбце **Управление** можно:

Включать или выключать правило.
Менять приоритет.
Редактировать правило.
Удалять правило.

При наличии большого количества правил в таблице воспользуйтесь кнопкой **Фильтры**.

Порядок применения правил

Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. То есть, если пользователь одновременно находится в нескольких группах, то к нему применяется правило, которое находится выше в списке правил.

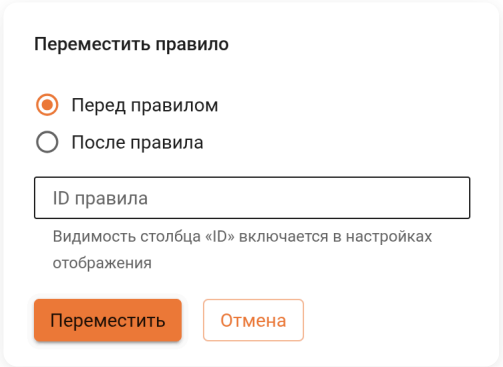
Правила **Ограничения скорости** не обрабатывают трафик между локальными сетями и сетями филиалов. Пользователи VPN приравниваются к пользователям локальных сетей.

Перемещение правил

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



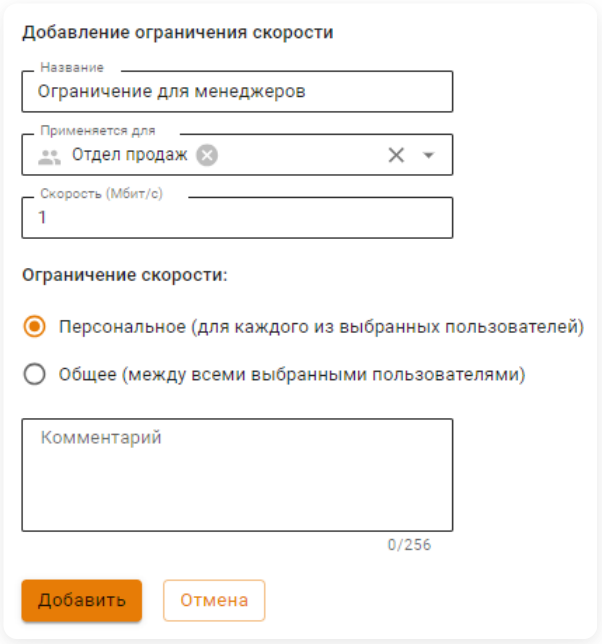
4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Примеры использования

Персональное ограничение

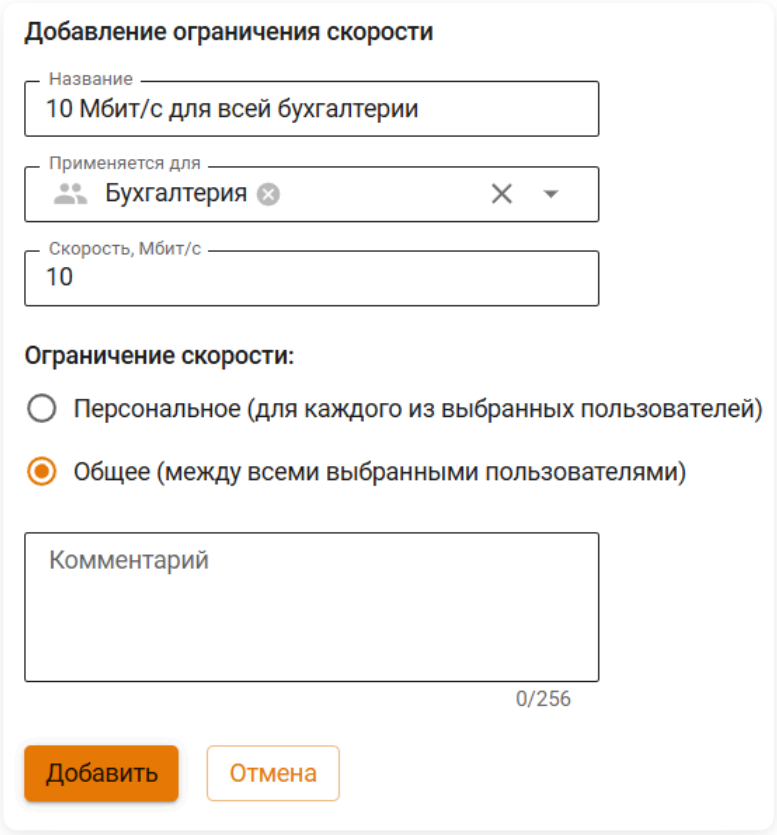
При выборе персонального ограничения скорости лимит скорости для каждого менеджера будет равен 1 Мбит/с:



Если под одной учетной записью авторизованы несколько устройств, каждое устройство получает полный лимит скорости: если задано ограничение 1 Мбит/с и авторизованы три устройства, каждое устройство получит 1 Мбит/с.

Общее ограничение

При выборе общего ограничения ширина канала для всей бухгалтерии будет равна 10 Мбит/с:



Если под одной учетной записью авторизованы несколько устройств, лимит скорости распределяется между всеми устройствами: если задано ограничение 10 Мбит/с и авторизованы три устройства, суммарная скорость для всех трех устройств составит 10 Мбит/с.

Полезные ссылки

- **Исключения**
- **Учетные записи**
- **Объекты**

Предотвращение вторжений

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Предотвращение вторжений**: `ideco-suricata`, `ideco-suricata-backend`, `ideco-suricata-event-syncer`, `ideco-suricata-profiles-syncer`, `ideco-suricata-profiles-syncer-backend`.

Список имен служб для других разделов доступен по ссылке.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE



Система **Предотвращения вторжений** (IDS/IPS, Intrusion detection system / Intrusion prevention system) предназначена для:

- [x] Обнаружения
- [x] Журналирования
- [x] Предотвращения атак злоумышленников на сервер, интегрированные службы и локальную сеть

Раздел состоит из трех вкладок:

- Группы сигнатур - список предустановленных групп сигнатур, распределенных по тактикам согласно матрице MITRE ATT&CK или в табличном виде.
- Пользовательские сигнатуры - позволяет добавить сигнатуры для обработки системой **Предотвращения вторжений**.
- Настройки - информация об обновлениях баз IPS и сетях, защищенных от вторжения.

Требования

Система **Предотвращения вторжений** доступна только в Enterprise-версии Ideco NGFW Novum с активной подпиской на обновления.

- Объем оперативной памяти - от 16 ГБ.
- Процессор - от 4 ядер.

После включения системы проверьте в разделе **Мониторинг** → **Графики загруженности**, что мощности процессора достаточно для анализа всего проходящего трафика.

Особенности настройки Межсетевого экрана и системы Предотвращение вторжений

- **Межсетевой экран** Ideco NGFW Novum анализирует трафик для поиска подходящего правила и применяет правило. Если в таблице есть несколько правил с одними и теми же условиями, применяется правило, стоящее выше по списку. Запрещающие правила **Межсетевого экрана** сразу блокируют соответствующий трафик, который не проходит дополнительную проверку в системе **Предотвращение вторжений**.
- Чтобы через модуль **Предотвращение вторжений** проходил трафик, для которого нет разрешающего правила в таблице **FORWARD** или **INPUT**, рекомендуем создать и включить в **Межсетевой экране** правило с источником **Любой** и назначением **Любой**, разместив правило в конец

таблицы. В этом случае трафик, который не был найден в правилах **Межсетевого экрана**, но соответствует профилям IPS, пройдет проверку системой **Предотвращения вторжений**.

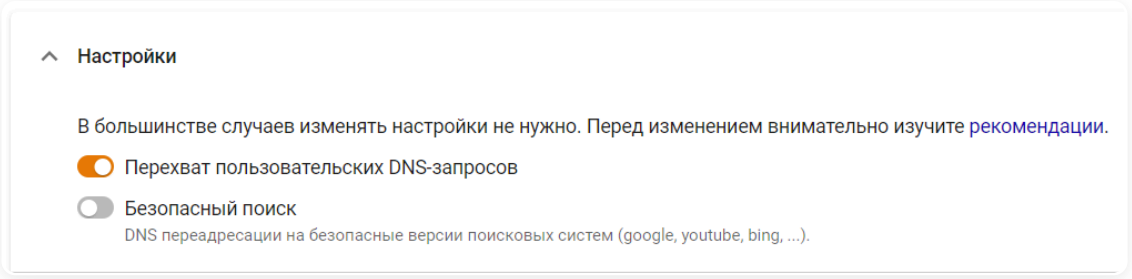
- Если в одном правиле **Межсетевого экрана** включены проверки и **Контролем приложений**, и системой **Предотвращения вторжений**, трафик сначала попадет в обработку DPI, затем - IPS.
- Чтобы трафик фильтровался системой **Предотвращение вторжений**, создайте для всех локальных интерфейсов правило **FORWARD**, содержащее нужный профиль безопасности.

С 18 версии Ideco NGFW Novum механизм работы системы **Предотвращения вторжений** изменился, появились возможности:

- [x] Работать с правилами IPS на уровне сигнатур, фильтровать и просматривать в удобном виде
- [x] Составлять независимые друг от друга наборы правил IPS и применять только к необходимому трафику с помощью профилей системы **Предотвращения вторжений**, которые назначаются в правилах **Межсетевого экрана**

Особенности обработки DNS-запросов

При включенной опции **Перехват пользовательских DNS-запросов** в **Сервисы** → **DNS** → **Внешние DNS-серверы** трафик обрабатывается не как **FORWARD**, а как **INPUT**:



Если опция **Перехват пользовательских DNS-запросов** включена (по умолчанию включена), создайте правила **INPUT** для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

Настройка обработки трафика

Чтобы система **Предотвращения вторжений** обрабатывала трафик:

1. Перейдите в **Правила трафика** → **Предотвращение вторжений** и включите работу системы:



2. Создайте необходимые профили IPS в **Профили безопасности** → **Предотвращение вторжений**.

3. Примените их в правилах Межсетевого экрана.

> В обработку трафика не попадают:
>
> - Сигнатуры, не включенные ни в один профиль.
> - Профили, не используемые в правилах **Межсетевого экрана**.

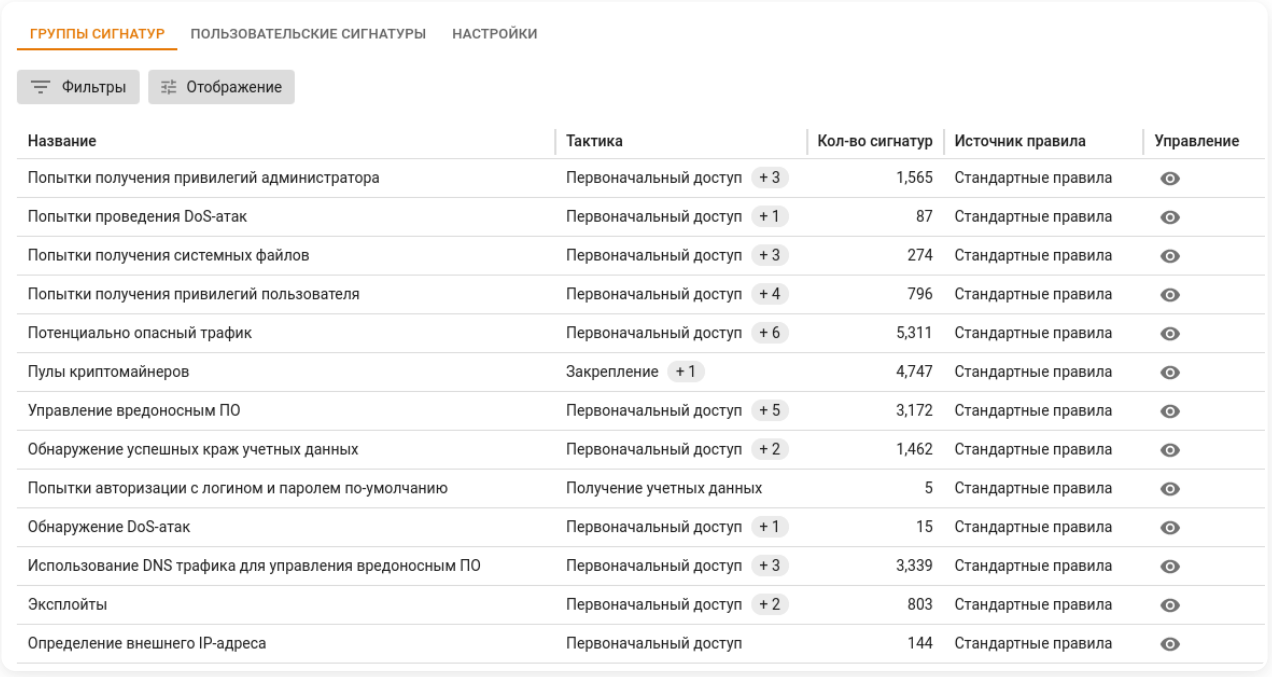
Полезные ссылки

- **Подробнее о Load Average**
- **Блокировка популярных ресурсов**

Группы сигнатур

Классический контекст | Высокопроизводительный контекст

На вкладке **Группы сигнатур** доступны для просмотра пользовательские и предустановленные сигнатуры:



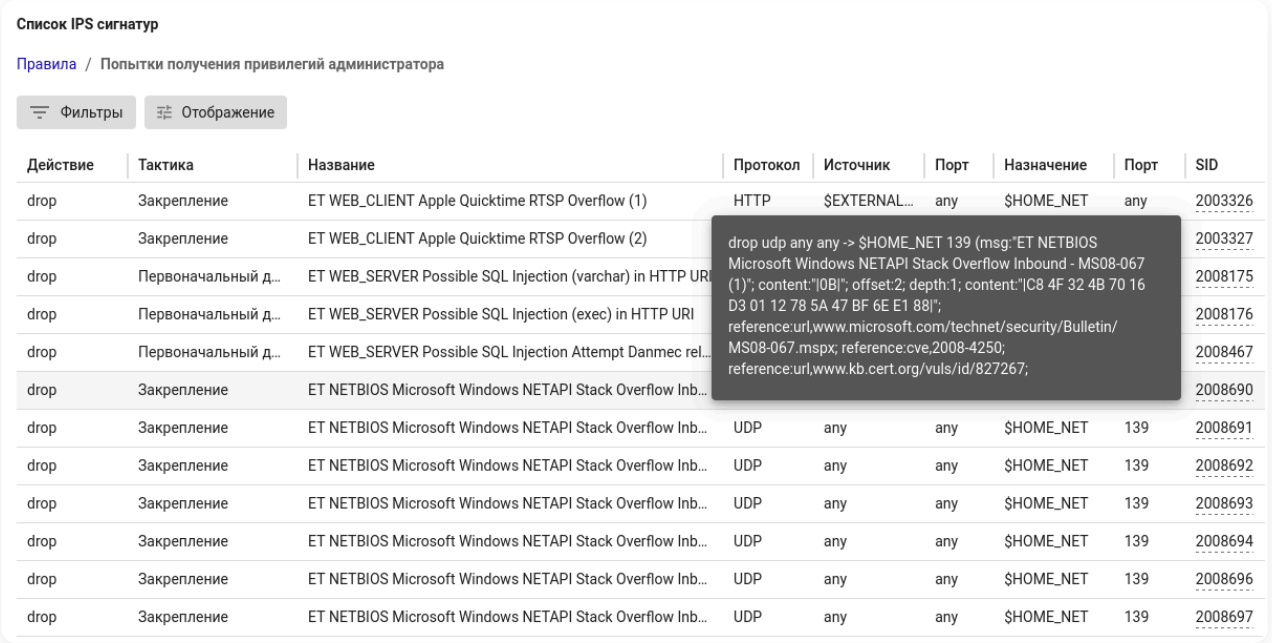
ГРУППЫ СИГНАТУР | ПОЛЬЗОВАТЕЛЬСКИЕ СИГНАТУРЫ | НАСТРОЙКИ

Фильтры | Отображение

Название	Тактика	Кол-во сигнатур	Источник правила	Управление
Попытки получения привилегий администратора	Первоначальный доступ +3	1,565	Стандартные правила	
Попытки проведения DoS-атак	Первоначальный доступ +1	87	Стандартные правила	
Попытки получения системных файлов	Первоначальный доступ +3	274	Стандартные правила	
Попытки получения привилегий пользователя	Первоначальный доступ +4	796	Стандартные правила	
Потенциально опасный трафик	Первоначальный доступ +6	5,311	Стандартные правила	
Пулы криптомайнеров	Закрепление +1	4,747	Стандартные правила	
Управление вредоносным ПО	Первоначальный доступ +5	3,172	Стандартные правила	
Обнаружение успешных краж учетных данных	Первоначальный доступ +2	1,462	Стандартные правила	
Попытки авторизации с логином и паролем по-умолчанию	Получение учетных данных	5	Стандартные правила	
Обнаружение DoS-атак	Первоначальный доступ +1	15	Стандартные правила	
Использование DNS трафика для управления вредоносным ПО	Первоначальный доступ +3	3,339	Стандартные правила	
Эксплойты	Первоначальный доступ +2	803	Стандартные правила	
Определение внешнего IP-адреса	Первоначальный доступ	144	Стандартные правила	

Чтобы увидеть сигнатуры, входящие в группу, нажмите на .

Чтобы увидеть содержание сигнатуры, наведите курсор мыши на SID:



Список IPS сигнатур

Правила / Попытки получения привилегий администратора

Фильтры | Отображение

Действие	Тактика	Название	Протокол	Источник	Порт	Назначение	Порт	SID
drop	Закрепление	ET WEB_CLIENT Apple Quicktime RTSP Overflow (1)	HTTP	$EXTERNAL...	any	$HOME_NET	any	2003326
drop	Закрепление	ET WEB_CLIENT Apple Quicktime RTSP Overflow (2)						2003327
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection (varchar) in HTTP URI						2008175
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection (exec) in HTTP URI						2008176
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection Attempt Danmec rel...						2008467
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...						2008690
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008691
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008692
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008693
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008694
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008696
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008697

drop udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (1)"; content:"|0B|"; offset:2; depth:1; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267;

Описание групп сигнатур

- **DNS поверх HTTPS** - обнаруживает и блокирует попытки скрыть DNS-запросы путем туннелирования через TLS/SSL (DNS поверх HTTPS). Правила анализируют трафик, чтобы выявить характерные для DoH-сессий доменные имена, используемые для обхода стандартных механизмов DNS-фильтрации. Такие методы злоумышленники могут применять для обхода сетевых политик, утечки данных или скрытого управления зараженными системами. Применение этих правил помогает предотвратить несанкционированное использование DoH.

- **SSL-сертификаты, используемые вредоносным ПО и ботнетами** - обнаруживает использование SSL-сертификатов, которые вредоносное ПО и ботнеты применяют для установления защищенных TLS-соединений с командными центрами злоумышленников (C2). Система анализирует отпечатки SSL-сертификатов, присутствующих в трафике, и выявляет попытки скрыть коммуникации посредством легитимно выглядящих шифрованных каналов. При обнаружении совпадений с известными вредоносными отпечатками такие соединения блокируются. Это предотвращает скрытое управление зараженными системами и снижает риск утечки данных и распространения кибератак.
- **Авторизация с подозрительным логином** - обнаруживает попытки авторизации с использованием подозрительных логинов, которые говорят о фишинговых атаках, переборе паролей или применении специализированных эксплойтов для несанкционированного доступа. Выявление таких аномалий позволяет своевременно блокировать соединения, предотвращая компрометацию систем и утечку данных.
- **Анонимайзеры** - обнаруживает использование анонимайзеров для сокрытия истинного источника трафика и возможного обхода систем контроля доступа. Определяются ключевые маркеры, связанные с различными сервисами анонимизации. Злоумышленники могут применять эти технологии для маскировки атак, утечек данных и обхода корпоративных политик безопасности, что делает их важными для своевременного обнаружения и блокировки.
- **Атаки на получение прав пользователя** - обнаруживает попытки получить несанкционированный доступ к учетным данным через эксплуатацию уязвимостей системы и применить специализированные инструменты. Анализируя сетевой трафик, фиксируются характерные маркеры атак, такие как выполнение команд для изменения настроек, обращения к реестру и т.д. Выявление подобной активности позволяет своевременно блокировать подозрительные соединения, предотвращая компрометацию систем и утечку конфиденциальной информации.
- **Атаки на получение привилегий администратора** - обнаруживает попытки получить административные привилегии с использованием уязвимостей и эксплойтов для эскалации прав. Анализируя сетевой трафик, определяет характерные маркеры активности. Такие действия могут указывать на внедрение вредоносного ПО или бэкдоров, что позволяет своевременно блокировать атаки и предотвращать компрометацию критически важных систем.
- **Блокирование активности троянских программ** - обнаруживает попытки эксплуатировать троянские программы, направленные на скрытую передачу данных, удаленно управлять зараженными системами, утечку конфиденциальной информации и др. Анализируя сетевой трафик, выявляет характерные маркеры активности вредоносных троянов - специфичные сигнатуры пакетов, аномальные HTTP-запросы, подозрительные команды и нестандартные DNS-запросы, связанные с ransomware. Блокировка таких соединений предотвращает дальнейшее распространение атак и защищает критически важные данные.
- **Блокирование атак** - обнаруживает попытки атак, направленные на эксплуатацию уязвимостей информационных систем, проведение сканирования портов, удаленное выполнение кода и другие методы вторжения. Анализирует входящий и исходящий сетевой трафик, фиксируя характерные сигнатуры эксплойтов, аномалии в пакетах, нестандартные команды и подозрительные запросы, указывающие на попытки получить несанкционированный доступ, провести DoS-атаки или обойти защитные механизмы. Оценивает репутацию IP-адресов и блокирует трафик, исходящий с адресов, имеющих негативную репутацию или принадлежащих к известным нодам Tor. Это позволяет предотвращать компрометацию инфраструктуры, утечку конфиденциальных данных и нарушение стабильности работы сетевых ресурсов.
- **Блокирование крупных утечек информации** - обнаруживает попытки несанкционированного экспорта данных из систем. Анализируя пакеты, фиксирует характерные маркеры экспорта и специфичные заголовки, свидетельствующие о массовой передаче конфиденциальной информации. Это позволяет оперативно блокировать такие соединения и предотвращать утечку критически важных данных.
- **Блокирование некорректных попыток получения привилегий пользователя** - обнаруживает попытки получить привилегии пользователя посредством некорректных или несанкционированных аутентификаций, которые могут указывать на попытки перебора или взлома учетных записей. Анализируя ответы серверов с сообщениями типа "Login failed", "Invalid login" и другие индикаторы неудачных входов, фиксирует подозрительные активности в протоколах FTP, SSH, RPC, SQL и других службах. Это позволяет оперативно блокировать подобные соединения, снижая риск компрометации учетных данных и предотвращая дальнейшие атаки.
- **Блокирование подозрительных RPC-запросов** - обнаруживает подозрительные RPC-запросы, предназначенные для вызова удаленных функций на сервере. Подозрительные RPC-запросы могут свидетельствовать о попытках эксплуатации уязвимостей или несанкционированного выполнения команд. Анализируя как UDP, так и TCP-трафик, фиксирует аномальные структуры пакетов, неверные параметры и нестандартные последовательности байтов, характерные для вредоносных активностей. Это позволяет оперативно блокировать подозрительные запросы, предотвращая потенциальное выполнение нежелательного кода и компрометацию систем.
- **Блокирование попыток запуска исполняемого кода** - обнаруживает попытки запуска исполняемого кода, направленные на удаленное выполнение команд и получение несанкционированного доступа к системам. Анализирует сетевой трафик на предмет характерных сигнатур RCE, включая специфичные байтовые последовательности, связанные с PHP object deserialization, веб-шеллами, Log4Shell и другими эксплойтами. Фиксирует аномалии в HTTP, TCP и UDP-запросах, что позволяет оперативно блокировать вредоносные попытки выполнения shellcode и предотвращать компрометацию целевых систем.
- **Блокирование утечек информации** - обнаруживает попытки несанкционированного извлечения конфиденциальных данных через сетевые протоколы. Анализируя входящий и исходящий трафик, фиксирует передачу содержимого критически важных файлов, а также различной системной информации. Выявление таких индикаторов утечки позволяет оперативно блокировать подозрительные соединения, предотвращая утечку секретных данных и снижая риск компрометации систем.
- **Запросы на скомпрометированные ресурсы** - обнаруживает нарушения корпоративных политик, связанные с обращениями к ресурсам, имеющим подозрительную репутацию. Правила фиксируют случаи, когда сетевой трафик указывает на несанкционированное использование различных протоколов, автоматизацию браузера или передачу данных в виде незащищенного контента. Такие сигнатуры служат индикаторами потенциального нарушения корпоративной безопасности, позволяя своевременно выявлять и блокировать подобные подключения.
- **Индикаторы компрометации ФинЦЕРТ** - обнаруживает и блокирует трафик с вредоносными файлами, а также попытки обращения к доменным именам, которые включены в бюллетени ФинЦЕРТ.
- **Использование DNS-трафика для управления вредоносным ПО** - обнаруживает попытки использовать DNS-трафик для управления вредоносным ПО, когда зараженные системы обращаются к серверам команд и контроля (C2) для получения инструкций. Анализируя DNS-запросы, TLS SNI и HTTP-заголовки, фиксирует обращения к известным вредоносным доменам и серверам, выявляя характерные паттерны связи с C2-инфраструктурой. Это позволяет оперативно блокировать такие соединения, предотвращая удаленное управление, утечку данных и дальнейшее распространение вредоносного кода.
- **Нежелательное программное обеспечение** - обнаруживает попытки использовать нежелательное программное обеспечение, включая adware и потенциально нежелательные утилиты, которые могут собирать и передавать конфиденциальные данные или связываться с вредоносными серверами. Анализируя HTTP, DNS и TLS-трафик, фиксирует характерные сигнатуры, специфичные запросы и уникальные идентификаторы,

связанные с подобной активностью. Это позволяет блокировать подозрительные соединения, предотвращать утечки информации и снижать риск компрометации конечных устройств.

- **Неизвестный тип трафика** - обнаруживает неопознанный трафик, который не соответствует стандартным протоколам или содержит аномальные, подозрительные шаблоны поведения. Анализирует HTTP-запросы, TLS-соединения и DNS-сообщения на предмет нестандартных User-Agent, специфических JA3-хешей, необычных кодировок, пустых или искаженных заголовков и прочих аномалий. Такие признаки могут указывать на попытки сканирования, обхода защитных механизмов или эксплуатацию уязвимостей. Выявление подобного трафика позволяет оперативно блокировать несанкционированное взаимодействие и снижать риск кибератак.
- **Нецелевое использование стандартных портов** - обнаруживает случаи нецелевого использования стандартных портов, когда сервисы, предназначенные для определенных протоколов, применяются для нелегитимных целей. Анализируя сетевой трафик, фиксирует аномальные подключения, при которых стандартный порт используется для обхода политик безопасности, скрытой передачи данных или запуска вредоносных операций. Это позволяет своевременно блокировать подозрительные соединения и предотвращать попытки эксплуатации инфраструктуры в обход установленных правил.
- **Обнаружение нарушений стандартов сетевых протоколов** - обнаруживает обращения по нестандартным или модифицированным протоколам, отклоняющимся от официальных спецификаций. Анализируя сетевой трафик, фиксирует аномальные баннеры, команды и последовательности данных, которые могут свидетельствовать о попытках обхода стандартных механизмов защиты или эксплуатации уязвимостей. Выявление таких нарушений позволяет оперативно блокировать трафик, не соответствующий протокольным стандартам, и предотвращать несанкционированный доступ и передачу вредоносного кода.
- **Обнаружение подозрительной сетевой активности** - обнаруживает аномалии в сетевом трафике, связанные с нестандартными или подозрительными действиями легитимных пользователей. Анализируя различные протоколы, включая HTTP, TCP, UDP, TLS и DNS, фиксирует отклонения от нормального поведения, такие как частые попытки подключения, необычные запросы или аномальные данные, которые могут свидетельствовать о сканировании сети, автоматизированных атаках или обходе защитных механизмов. Это позволяет своевременно выявлять и блокировать потенциально вредоносный трафик.
- **Обнаружение подозрительных команд** - обнаруживает команды, нехарактерные для стандартного поведения систем, которые злоумышленники могут использовать для обхода защитных мер. Анализируя сетевой трафик, фиксирует аномальные запросы и нестандартные вызовы, например, обращения к зарезервированным ресурсам (COM1, LPT1, LPT4, NULL), что свидетельствует о попытках эксплуатации и несанкционированного доступа. Блокировка таких команд помогает предотвратить возможные атаки и сохранить целостность информационных систем.
- **Обнаружение успешных краж учетных данных** - обнаруживает попытки несанкционированного извлечения учетных данных, направленные на получение логинов, паролей и другой конфиденциальной информации. Анализируя содержимое HTTP-запросов, POST-данные и серверные ответы, фиксирует характерные шаблоны фишинговых атак. Также учитываются сообщения об ошибках аутентификации, указывающие на успешное компрометирование учетных записей, что позволяет оперативно блокировать атаки и предотвращать утечку данных.
- **Определение внешнего IP-адреса** - обнаруживает попытки определения внешнего IP-адреса, когда внутренние системы обращаются к внешним сервисам для получения информации о своей публичной адресации. Анализирует HTTP-запросы, DNS-запросы и TLS SNI, указывающие на обращения к подобным ресурсам. Это позволяет блокировать несанкционированное взаимодействие с внешней инфраструктурой и предотвращать сбор данных для дальнейшей разведки или подготовки атак.
- **Ошибки в сетевых протоколах** - обнаруживает нарушения стандартов сетевых протоколов, фиксируя ошибки в форматировании сообщений, некорректные заголовки и структурные аномалии пакетов. Анализируя входящий и исходящий трафик, система выявляет сбои в реализации протокольных команд, которые могут быть следствием как технических недочетов, так и преднамеренных манипуляций злоумышленников. Это позволяет своевременно блокировать подозрительные соединения, предотвращая атаки, обход защитных механизмов и снижая риск компрометации информационных систем.
- **Подозрительное обращение к файлам** - обнаруживает обращения к файлам, которые не соответствуют обычным операциям системы и могут указывать на несанкционированный доступ или попытки извлечения/модификации критически важных данных. Анализируя сетевой трафик, фиксирует запросы на загрузку, копирование или просмотр файлов с нестандартными расширениями или путями, например, системных конфигураций, резервных копий или скрытых ресурсов. Это позволяет блокировать подозрительную активность, предотвращая утечку данных и возможную компрометацию системы.
- **Попытки авторизации с логином и паролем по-умолчанию** - обнаруживает попытки авторизации с использованием учетных данных по умолчанию, когда злоумышленники применяют стандартные логины и простые пароли для входа в систему. Анализируя трафик, система выявляет запросы, содержащие типичные параметры доступа к различным системам. Такие действия указывают на попытки несанкционированного доступа, что позволяет оперативно блокировать подобные соединения и предотвращать компрометацию сетевой инфраструктуры.
- **Попытки использования социальной инженерии** - обнаруживает попытки социальной инженерии, направленные на обман пользователей и получение конфиденциальной информации, такой как учетные данные/доступ к корпоративным ресурсам. Включает выявление фишинговых сайтов, мошеннических схем с техподдержкой, вредоносных редиректов и подозрительных доменов в DNS-запросах. Эти атаки часто имитируют известные сервисы или компании, побуждая жертву выполнить вредоносные действия, что может привести к утечке данных или компрометации системы.
- **Попытки получения привилегий администратора** - обнаруживает попытки повысить привилегии до уровня администратора и получить учетные данные с использованием различных техник. Включает детектирование эксплойтов, направленных на уязвимости в операционных системах и приложениях, SQL-инъекций, обхода аутентификации, эксплуатации слабых конфигураций сервисов, а также атак на учетные записи через протоколы Telnet, RDP, SMB и другие. Такие действия могут указывать на компрометацию системы или активность злоумышленников, пытающихся расширить контроль над сетью.
- **Попытки получения привилегий пользователя** - обнаруживает попытки повысить привилегии и компрометировать учетные данные пользователей, в том числе - использовать уязвимости в серверных приложениях, базах данных и сетевых сервисах. Включает правила для выявления SQL-инъекций, эксплуатации переполнения буфера, обхода аутентификации и атак на учетные записи пользователей. Используется для защиты от угроз, направленных на несанкционированный доступ и эскалацию привилегий в корпоративных и облачных средах.
- **Попытки получения системных файлов** - обнаруживает попытки получить конфигурационные и системные файлы, включая файлы паролей, журналы, резервные копии и другие критически важные данные. Включает правила для выявления сканирования уязвимостей, запроса конфигураций через веб-интерфейсы, злоупотребления FTP, SMB, SSH и др. Используется для предотвращения утечек данных и сбора информации, которые могут привести к дальнейшей компрометации инфраструктуры.

- **Попытки проведения DoS-атак** - обнаруживает попытки проведения атак типа отказа в обслуживании (DoS), включая флуд, амплификационные атаки и иные методы перегрузки сетевых ресурсов. Анализирует трафик на наличие аномальных запросов и последовательностей, характерных для DDoS-атак в протоколах VoIP, HTTP, NTP, SSDP и других. Фиксирует массовые запросы, некорректные ответы и превышение пороговых значений, что позволяет оперативно блокировать подобные соединения и предотвращать отказ в обслуживании легитимных пользователей.
- **Попытки сканирования сети** - обнаруживает попытки сканирования сети, свидетельствующие о разведке для последующих атак. Анализируя TCP, UDP, ICMP и HTTP-трафик, фиксирует массовые SYN-запросы, сканирование портов, аномальные User-Agent и повторяющиеся обращения к различным сервисам. Такие действия характерны для инструментов вроде Nmap и Zmap, которые злоумышленники используют для поиска уязвимостей. Выявление подобных активностей позволяет оперативно блокировать сканирование и предотвращать потенциальное проникновение в сеть.
- **Потенциально опасный трафик** - обнаруживает трафик с подозрительной шифровкой или запутанными, обфусцированными данными и нестандартными запросами, не характерными для легитимной сетевой активности. Анализируя HTTP, DNS, TLS и IP-заголовки, фиксирует аномальные User-Agent, обращения к подозрительным доменам и C2-серверам, а также другие индикаторы, свидетельствующие о попытках скрыть вредоносную коммуникацию. Это позволяет оперативно блокировать такие соединения, снижая риск проникновения и распространения атак.
- **Пулы криптомайнеров** - обнаруживает попытки взаимодействия с криптомайнинговой инфраструктурой через анализ DNS-запросов, TLS-сессий и TCP-трафика, фиксируя характерные доменные имена и сигнатуры, связанные с известными пулами. Выявляет обращения, используемые криптомайнерами для передачи нагрузки, и блокирует такие соединения, предотвращая несанкционированное использование сетевых ресурсов для майнинга и минимизируя риск утечки вычислительной мощности.
- **Расширенная база правил (от Лаборатории Касперского)** - обнаруживает трафик, который генерируют вредоносные инструменты, используемые злоумышленниками для разведки, атак и несанкционированного доступа. Анализируя HTTP, FTP, SIP, UDP и TCP-запросы, фиксирует аномалии, характерные для SQL-инъекций, эксплойтов, C&C-коммуникаций и других угроз. Правила от Лаборатории Касперского используют сигнатуры и поведенческий анализ для своевременного обнаружения и блокировки подозрительной активности, что помогает предотвратить утечку данных и повысить защиту сети от современных кибератак.
- **Телеметрия Windows** - обнаруживает попытки передать телеметрические данные Windows на серверы Microsoft и связанные сервисы. Анализирует сетевой трафик, включая TLS-сессии с SNI-запросами и DNS-запросы, выявляя характерные строки. Блокирует такие обращения, предотвращая автоматическую отправку телеметрии, что способствует защите конфиденциальности пользователей и снижению объема передаваемой информации.
- **Управление вредоносным ПО** - обнаруживает сетевой трафик инструментов, которые злоумышленники используют для разведки, атак и несанкционированного доступа, включая эксплойты, SQL-инъекции, обход аутентификации и C&C-коммуникации. Использует сигнатуры и поведенческий анализ для выявления характерных HTTP-, FTP-, SIP- и других запросов. Такие инструменты тесно связаны с вредоносным ПО и кибератаками, что позволяет оперативно блокировать их активность.
- **Целевое использование вредоносного ПО** - обнаруживает целевой трафик, связанный с вредоносным программным обеспечением, которое злоумышленники используют для компрометации систем, кражи данных и установления контроля над устройствами. Анализируя HTTP, DNS, TLS и другие протоколы, фиксирует обращения, характерные для APT-активностей и C&C-коммуникаций, а также сигнатуры известных вредоносных семейств. Блокировка таких запросов позволяет предотвратить целевые атаки и снизить риск утечки конфиденциальной информации.
- **Подключения к потенциально уязвимым web-приложениям** - обнаруживает попытки подключения к веб-приложениям с известными уязвимостями.
- **Эксплойты** - обнаруживает попытки эксплуатации системных уязвимостей с использованием эксплойт-китов, зачастую идентифицируемых по стандартным идентификаторам CVE-XXXX-XXXXX. Анализируя трафик в различных протоколах (HTTP, TLS, DNS и других), система фиксирует характерные сигнатуры и аномальные запросы, указывающие на запуск вредоносного кода или несанкционированный доступ. Блокировка таких соединений позволяет оперативно предотвратить компрометацию инфраструктуры и утечку конфиденциальной информации.

Пользовательские сигнатуры

Функциональность доступна в **Классическом** и **Системном контекстах**.

Пользовательская сигнатура - это кастомный шаблон, позволяющий идентифицировать определенные виды вредоносного трафика, аномалий в протоколах или известных атак. Такие сигнатуры можно добавлять на вкладке **Пользовательские сигнатуры**. При корректном добавлении появятся в таблице Группы сигнатур.

В обработке трафика не участвуют:

- Сигнатуры, которые не используются в профилях **Предотвращения вторжений**.
- Профили, которые не используются в правилах **Межсетевого экрана**.

Описание валидной сигнатуры

Валидная сигнатура включает три основные части:

- Действие при совпадении правила.
- Заголовок, определяющий протокол, IP-адреса или сети отправителя и получателя, порты и направление трафика.
- Опции, описывающие специфику сигнатуры.

Пример валидной сигнатуры

Генерирует предупреждение, если обнаружен HTTP GET-запрос, в URI которого встречается слово `rule`:

```
alert http $HOME_NET any → $EXTERNAL_NET any (msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http
```

где:

- `alert` - действие. Перечень валидных действий:
  - `alert` - пропустить пакет и сгенерировать предупреждение.
  - `pass` - пропустить пакет без предупреждения.
  - `drop` - отбросить пакет и сгенерировать предупреждение.
  - `reject` - отправить ошибку `RST/ICMP unreach` отправителю пакета.
  - `rejectdst` - отправить пакет с ошибкой `RST/ICMP error` получателю исходного пакета.
  - `rejectboth` - отправить пакеты с ошибкой `RST/ICMP error` отправителю и получателю исходного пакета.
- `http $HOME_NET any → $EXTERNAL_NET any` - заголовок, в том числе:
  - `http` - протокол. Валидные протоколы: сетевого уровня (`ip`, `icmp`), транспортного уровня (`tcp`, `udp`), уровня представления (`tls`, `ssl`), прикладного уровня (`http`, `dns`, `ssh`, `ftp` и другие).
  - `$HOME_NET` - сети отправителя, указанные в **Правила трафика → Предотвращение вторжений → Настройки → Сети, защищенные от вторжений**.
  - `any` - порты отправителя/получателя.
  - `->` - направление трафика. Два валидных значения: `->` - проверка трафика слева направо, `<>` - проверка трафика в обоих направлениях. Значение `<-` не является валидным. Например, при проверке пакетов, идущих из сети A в сеть B, валидное значение в сигнатуре - `сеть A → сеть B`, невалидное значение - `сеть B <- сеть A`.
  - `$EXTERNAL_NET` - сети получателя (значения, которые не попадают в `$HOME_NET`).
- `(msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1;)` - опции, заключенные в скобки и разделенные точкой с запятой.

Особенности опций валидной сигнатуры

Порядок опций важен, изменение влияет на порядок обработки. Например, указанная в примере опция `content:"GET"` относится к опции `http.method`, а опция `content:"rule"` - к опции `http.uri`.

Опции бывают двух основных видов:

- Влияющие на инспекцию трафика. При добавлении сигнатуры необходимо указать опции. Описание некоторых опций из примера:
  - `flow` - состояние соединения, направление следования пакета и др.;
  - `content` - содержимое пакета, по которому производится сопоставление.
- Метаопции - опции, не влияющие на инспекцию трафика, но влияющие на способ информирования о срабатывании сигнатуры. Список некоторых метаопций из примера:
  - `msg` - информация о сигнатуре и возможном алерте;
  - `classtype` - информация о классе правил и алертов (короткое и длинное название, приоритет);
  - `sid` - уникальный номер сигнатуры;
  - `rev` - версия сигнатуры;
  - `metadata` - дополнительная информация о сигнатуре. Формат `metadata`:

```
metadata: key value;
metadata: key value, key value;
```

Примеры указания тактики MITRE

1. Формат в правилах Касперского - `metadata: MITRE TA0001`:

```
alert http $HOME_NET any → $EXTERNAL_NET any (metadata: MITRE TA0001; msg:""; sid:1;)
```

- `TA0001` - MITRE_ID

2. Формат в Emerging Threats - `metadata: mitre_tactic_id TA0001`:

```
alert http $HOME_NET any → $EXTERNAL_NET any (metadata: mitre_tactic_id TA0001; msg:""; sid:1;)
```

- `TA0001` - MITRE_ID

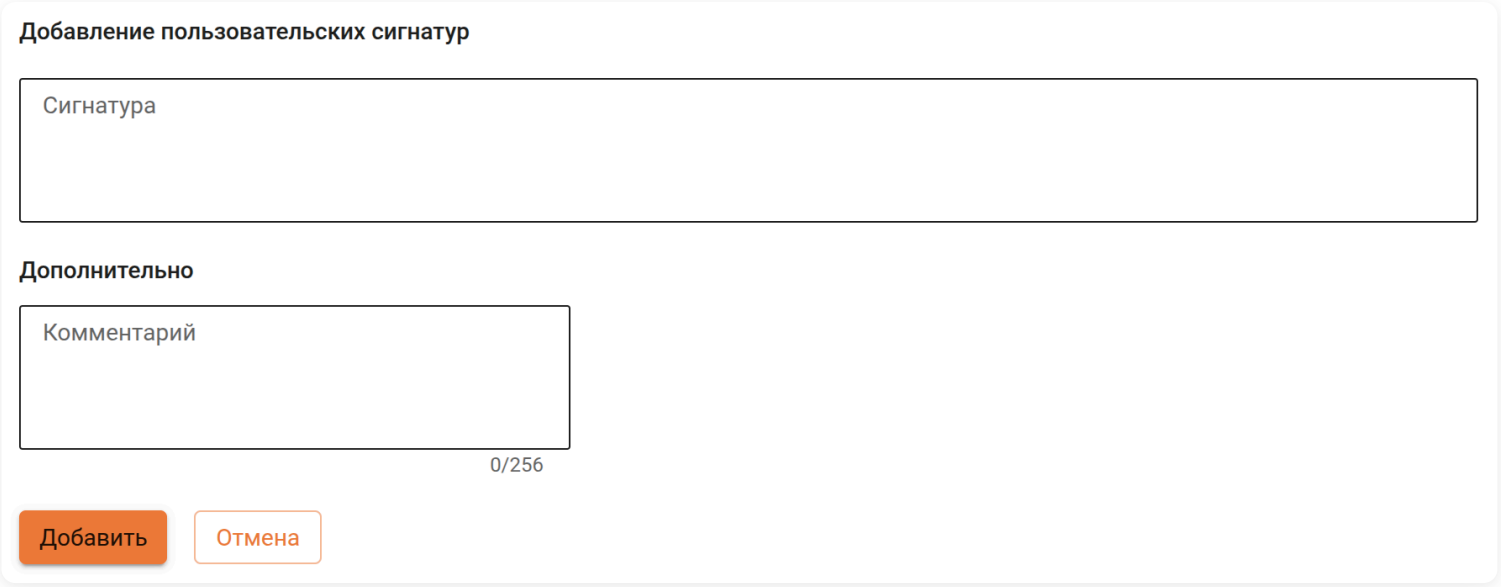
Символы `;` и `"` имеют специальное значение и должны быть экранированы с помощью символа `\` в случае использования в значениях опций.

Создание пользовательской сигнатуры

Нажмите **Добавить** и выберите способ добавления:

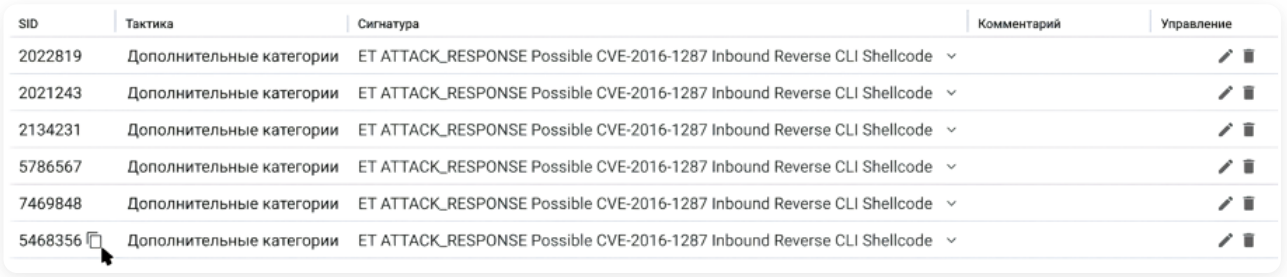
Вручную

В открывшейся форме введите сигнатуру, комментарий и нажмите **Добавить**:



Из файла

Загрузите текстовый файл с валидными сигнатурами (уникальные SID в диапазоне 1-999999). Если в структуре файла есть ошибки, система укажет номера строк с ошибками.



Проверка валидности сигнатур может занять некоторое время. Если одна из сигнатур не пройдет проверку, появится сообщение об ошибке у названия системы **Предотвращения вторжений**. Подробности можно будет увидеть в логах службы.

Пример создания исключения с конкретным адресом и сигнатурой

Пользователю необходимо добавить в исключения передачу трафика, который блокируется конкретной сигнатурой **Предотвращения вторжений** для конкретного отправителя (192.168.10.10) и получателя (1.1.1.1).

Если пользователь добавит в исключения конкретную сигнатуру, то разрешит этот трафик для всех адресов.
Если пользователь создаст исключение в разделе **Правила трафика** → **Исключения**, то исключается конкретный адрес для всех сигнатур.

Пользовательская сигнатура позволит создать исключение для конкретного адреса и конкретной сигнатуры одновременно. Для добавления такой сигнатуры:

1. Перейдите в **Отчеты и журналы** → **События безопасности** и найдите ID сигнатуры, которую необходимо добавить в исключения.

2. Скопируйте содержание сигнатуры (отображается при наведении на ID).

3. Перейдите в **Правила трафика** → **Предотвращение вторжений** → **Пользовательские сигнатуры** и нажмите **Добавить** → **Вручную**.

4. Вставьте скопированный лог в поле **Сигнатура** и измените в нем:

- Действие `drop` на `pass`.
- Значения `$HOME_NET` и/или `$EXTERNAL_NET` на нужный адрес отправителя/получателя.
- Значение `sid` на любое уникальное в диапазоне 1-999999.

Опции, не влияющие на инспекцию трафика, из сигнатуры можно удалить.
Если при добавлении сигнатуры оставить опцию `msg`, то в разделе **Отчеты и журналы** → **События безопасности** будут сохраняться логи по данной сигнатуре.

4. Нажмите **Добавить**.

Пример содержания сигнатуры в разделе **Отчеты и журналы** → **События безопасности**:

```
drop http $EXTERNAL_NET any → $HOME_NET any (msg:"ET HUNTING DDoS-Guard Hosted Content"; flow:established,to_client; http.sta
```

Пример пользовательской сигнатуры:

```
pass http 192.168.10.10 any → 1.1.1.1 any (flow:established,to_client; http.stat_code; content:"200"; http.server; content:"D
```

Полезные ссылки

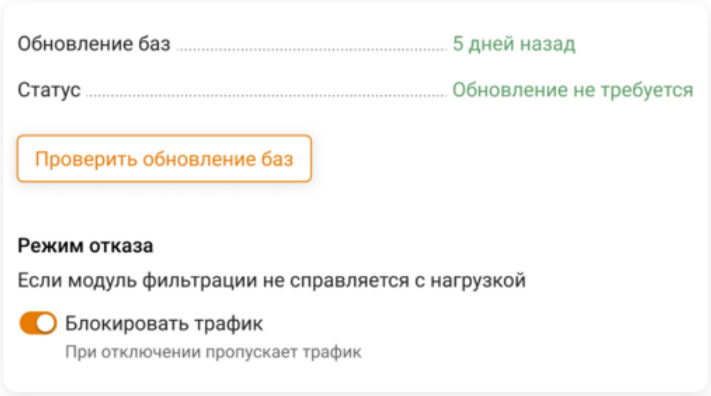
- **Полная документация по форматам сигнатур**.

Настройки

Классический контекст | Высокопроизводительный контекст

> Настройка дополнительных параметров фильтрации системы Предотвращение вторжений.

На вкладке можно проверить статус обновления баз системы **Предотвращение вторжений**, настроить **Режим отказа** и отредактировать список сетей, защищенных от вторжений:



Опция **Блокировать трафик** позволяет заблокировать весь трафик в случае перегрузки модуля **Предотвращение вторжений**.

Для добавления подсети в список защищенных нажмите **Добавить** и в поле **Подсеть** укажите локальные сети, обслуживаемые NGFW (сети локальных интерфейсов NGFW, маршрутизируемые на них сети удаленных сегментов локальной сети предприятия).

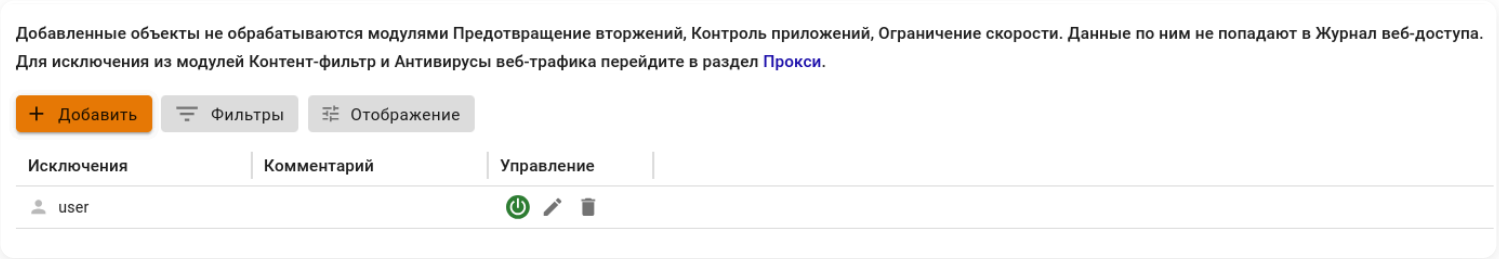
Для корректной работы системы **Предотвращение вторжений**:

- Не указывайте сети, принадлежащие внешним сетевым интерфейсам NGFW и внешним сетям. Указанные на вкладке сети участвуют в правилах системы **Предотвращения вторжений** как локальные.
- Не используйте сторонние DNS-серверы для компьютеров, т.к. служба определяет зараженные устройства по DNS-запросам, проходящим через нее.
- При использовании внутреннего домена AD рекомендуем:
  - В компьютерах указать DNS-сервер Ideco NGFW Novum в качестве единственного DNS-сервера.
  - В настройках DNS-сервера на NGFW указать Forward-зону для локального домена.

Исключения

Функциональность доступна в **Классическом** и **Системном контекстах**.

Правила в разделе **Исключения** отключают трафик из обработки системы Предотвращения вторжений, Контроля приложений, данные по ним не попадают в монитор трафика:



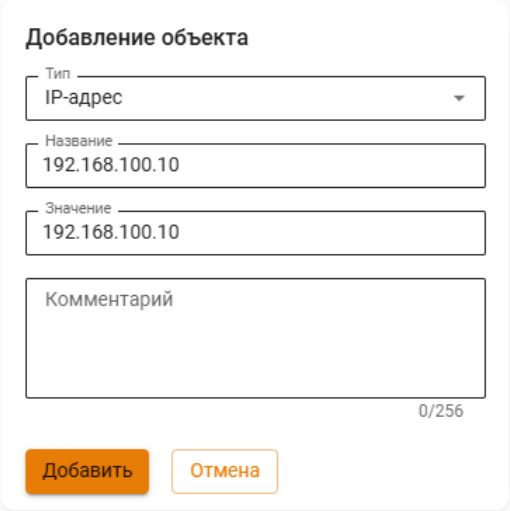
При наличии большого количества исключений в таблице воспользуйтесь кнопкой **Фильтры**.

Добавление исключения

Для предотвращения обработки трафика необходимо добавить объект в исключения:

1. Перейдите в **Правила трафика** → **Исключения** и нажмите **Добавить**.

2. Выберите существующий объект или создайте новый, заполнив поля:



- **Тип** - выберите тип объекта. Список доступных типов объектов приведен в статье.
- **Название** - укажите название объекта.
- **Значение** - укажите значение объекта в соответствии с выбранным типом.
- **Комментарий** - укажите произвольный комментарий. Необязательное поле.

3. Нажмите **Добавить**.

Если в качестве DNS-сервера у пользователя указан локальный адрес сервера Ideco NGFW Novum, то исключения работать не будут. Весь трафик, идущий на адреса локальных и VPN-интерфейсов Ideco NGFW Novum, всегда обрабатывается службой фильтрации трафика.

Объекты

Классический контекст | Высокопроизводительный контекст | API

В Ideco NGFW Novum можно создать объекты для использования в правилах межсетевого экрана, предотвращения вторжений и т.д.

Название службы раздела **Объекты**: `ideco-alias-backend`.

Список имен служб для других разделов доступен по ссылке.

Объектом называется сохраненный в NGFW Novum определенный тип данных, который можно использовать при создании правил.

Типы объектов

- **Зона** - логическое объединение сетевых интерфейсов. Используется для настройки правила межсетевого экрана на несколько интерфейсов.
- **IP-адрес** - IP-адрес IPv4. Пример: `10.0.0.1`.
- **Диапазон IP-адресов** - диапазон IP-адресов от первого до последнего, указанного в диапазоне. Пример: `10.0.0.1-10.0.0.25`.
- **Подсеть** - логический блок IP-адресации. Префикс маршрутизации выражается в нотации CIDR. Пример: `10.0.0.0/24`.
- **Домен** - символьное имя, служащее для идентификации объектов в интернете. Пример: `ideco.ru`.
- **Порт** - номер порта от 1 до 65535. Пример: `3389`.
- **Диапазон портов** - диапазон портов от первого до последнего, указанного в диапазоне. Пример: `1024-65535`.
- **Время** - диапазон времени. Пример: `ПН 9:00-18:00`.
- **Список IP-объектов** - группа объектов, состоящая из отдельных объектов, таких как IP-адрес, диапазон IP-адресов, подсеть, домен, пользователь, группа. При настроенной интеграции Active Directory доступны для выбора пользователи AD, группы безопасности AD, LDAP-фильтры. Пример: `10.0.0.1, 10.0.0.4, 10.0.0.126, test.com, user1`.
- **Список IP-адресов** - объект, состоящий из списка IP-адресов. Для создания объекта требуется загрузить любой текстовый файл (например: TXT/CSV). При этом в одной строке должен быть один адрес. Также допускается использование маски `/24` или `255.255.255.0`.
- **Порты** - группа портов. Пример: `25, 110, 143, 445, 465, 587, 993, 995`.
- **Расписание** - группа диапазонов времени. Пример: `ПН 9:00-12:00, ВТ 13:00-18:00`.
- **Список стран и континентов** - группа объектов, содержащая GeoIP.

При настроенной интеграции с Active Directory в правилах трафика доступны для выбора объекты, импортируемые из каталога.

Объекты, импортируемые из Active Directory

- **Пользователи AD** - учетные записи пользователей интегрированных доменов Active Directory. Становятся доступны для выбора в правилах после настройки интеграции с доменом.
- **Группы безопасности AD** - группы безопасности Active Directory, объединяющие учетные записи пользователей. Позволяют применить правило сразу ко всем пользователям группы.
- **LDAP-фильтры** - выборка учетных записей из каталога Active Directory с помощью фильтров. Подробнее - в статье **LDAP-фильтры**.

Объект **Зона** содержит набор предустановленных алиасов **Специальные**, которые объединяют определенные типы интерфейсов или трафик. Эти зоны нельзя удалить или изменить, но их можно использовать при создании правил фильтрации.

Специальные зоны

- **Внешние интерфейсы** - все интерфейсы с ролью **WAN**.
- **Внешние Ethernet-интерфейсы** - интерфейсы **Ethernet** с ролью **WAN**.
- **Внешние VPN-интерфейсы** - интерфейсы **L2TP**, **PPTP**, **PPPoE** с ролью **WAN**.
- **IPsec-интерфейсы** - соединения site-to-site IPsec.
- **Локальные интерфейсы** - интерфейсы с ролью **LAN**.
- **Туннельные интерфейсы** - интерфейсы **GRE**.
- **ГОСТ VPN-интерфейсы** - соединения, настроенные в **Сервисы** → **ГОСТ VPN**.
- **Исходящий трафик устройства** - исходящий трафик самого NGFW Novum.
- **Клиентский VPN-трафик** - трафик клиентских VPN-соединений.
- **WCCP GRE интерфейсы** - трафик туннелей до WCCP-сервера, созданных в **Сервисы** → **Прокси** → **WCCP**.

Объект **Зона** можно создавать и редактировать только в **Системном контексте**. В других контекстах объект будет доступен **только** для выбора.

Объект **IP-адрес** содержит набор предустановленных алиасов **Специальные**, которые объединяют определенные группы адресов.

Специальные IP-адреса

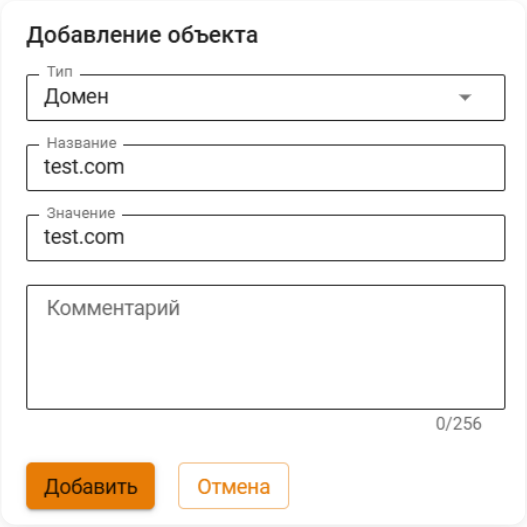
- **Черный список IP-адресов** - IP-адреса, внесенные в централизованные базы угроз (НКЦКИ, открытые источники).
- **Черный список ФинЦЕРТ** - IP-адреса из ежедневных бюллетеней ФинЦЕРТ.
- **Все пользователи AD** - IP-адреса пользователей из Active Directory.
- **Все доверенные пользователи AD** - IP-адреса пользователей из доверенных доменов Active Directory.

Создание объектов

Чтобы создать объект, необходимо выполнить следующие действия:

1. Перейдите в **Правила трафика** → **Объекты** и нажмите кнопку **Добавить** в левом верхнем углу экрана.

2. Выберите тип, название и значение объекта. По желанию можно указать произвольный комментарий не длиннее 128 символов:



3. Нажмите кнопку **Добавить**.

При наличии большого количества объектов в таблице воспользуйтесь кнопкой **Фильтры**.

Важно:

- Для создания групп объектов предварительно необходимо создать сами объекты. К группам объектов относятся: список IP-адресов, порты и расписание.
- Для создания объекта типа **Список IP-адресов** используйте любой текстовый файл (например: TXT/CSV), в котором будут перечислены нужные IP-адреса. Правила заполнения:
  - В строке должен быть один адрес.
  - Допускается использование маски /24 или 255.255.255.0.
- Для создания объекта типа **Зона** необходимо:
  - Создать соответствующий объект в разделе **Правила трафика** → **Объекты**.
  - Перейти в раздел **Сервисы** → **Сетевые интерфейсы** и при редактировании интерфейса добавить его в нужную зону.
- Для IPsec подключения зону можно добавить при создании подключения.
- Объекты типа **IP-адрес** и **Порт** можно создавать непосредственно при создании правил межсетевого экрана, введя нужный IP-адрес или порт в соответствующих полях.

В Ideco NGFW Novum также используется специальный алиас - **Любой**. Если при создании правила в каком-либо из полей выбран алиас **Любой**, правило будет распространяться на все объекты, доступные к выбору в том же поле.

Полезные ссылки

- **Ручная корректировка GeoIP**

Профили безопасности

Профили безопасности это наборы параметров для фильтрации трафика различными модулями и позволяет настраивать разные политики безопасности независимо друг от друга. Профили WAF будут использоваться только в публикациях сервисов в разделе Обратный прокси. Остальные профили - в правилах раздела Межсетевой экран.

Контроль приложений

Создание, настройка и примеры использования **Профилей контроля приложений**

Перейти >

Предотвращение вторжений

Создание, настройка и примеры использования **Профилей предотвращения вторжений**

Перейти >

Web Application Firewall

Создание WAF-профилей для защиты опубликованных веб-ресурсов от атак

Перейти >

Антивирус

Интеграция Kaspersky Anti-Virus Software Development Kit в Ideco NGFW

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Профили контроля приложений

Классический контекст | Высокопроизводительный контекст | API

Названия служб раздела **Профили контроля приложений**: `ideco-app-backend`, `ideco-app-control-nfq`.

Список имен служб для других разделов доступен по ссылке.

В **Профили безопасности** → **Контроль приложений** создаются профили, разрешающие или запрещающие доступ пользователя к заданному администратором набору приложений и протоколов. Созданные профили применяются при настройке правил в разделе **Межсетевой экран**. При наличии большого количества профилей в таблице воспользуйтесь кнопкой **Фильтры**.

Для выявления протоколов приложений осуществляется глубокий анализ трафика (Deep Packet Inspection - DPI). Собранные данные используются для мониторинга трафика. Определение протоколов выполняется системой в зависимости от состояния модуля **Профили контроля приложений**.

- Если включен, то весь трафик проходит через DPI, включая трафик, который обрабатывается правилами **Межсетевого экрана** без выбранного профиля **Контроля приложений**.
- Если выключен, то определение протоколов для трафика не производится.

Контроль приложений фильтрует трафик при условиях:

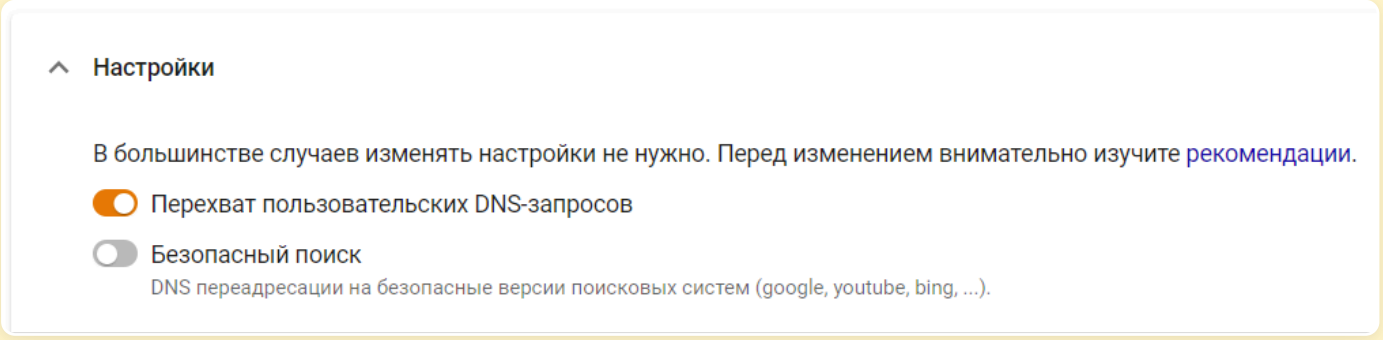
- В правиле **FORWARD** или **INPUT** раздела **Межсетевой экран** включена опция **Контроль приложений**.
- В этом правиле выбран профиль безопасности.

Трафик, не соответствующий условиям, фильтроваться не будет, даже если его протоколы определяются системой.

Принцип создания профилей **Контроля приложений**: все протоколы и приложения, которые не были запрещены, остаются разрешены.

Чтобы трафик фильтровался модулем **Контроль приложений**, создайте для всех локальных интерфейсов правило **FORWARD**, содержащее нужный профиль безопасности.

При включенной опции **Перехват пользовательских DNS-запросов** (по умолчанию включена) в разделе **Сервисы** → **DNS** → **Внешние DNS-серверы** трафик обрабатывается не как FORWARD, а как INPUT:



Создайте правила **INPUT** для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

Особенности обработки трафика с помощью профиля Контроля приложений

Контроль приложений проверяет только тот трафик, который соответствует разрешающему правилу **Межсетевого экрана** с включенной опцией **Профили контроля приложений** и выбранным профилем.

Порядок применения правил Межсетевого экрана

1. **Анализ трафика и поиск подходящего правила. Межсетевой экран** Ideco NGFW Novum проверяет трафик и последовательно (сверху вниз) сравнивает его с правилами из таблицы. Как только находится совпадение, соответствующее правило применяется.

2. **Приоритет правил.** Если **Межсетевой экран** находит несколько правил с одинаковыми условиями, то применяет правило, расположенное выше в списке.

3. **Взаимодействие с Контролем приложений.** Если трафик блокируется запрещающим правилом **Межсетевого экрана**, **Контроль приложений** не проверяет заблокированный трафик.

Доступные приложения и протоколы для создания профилей

Перечень групп приложений и протоколов, доступных для создания профилей

- Стриминговые сервисы
- Веб-ресурсы
- Компьютерные игры
- Видео-контент
- Реклама
- Контент для взрослых
- Передача данных
- Облачные сервисы
- Виртуальные ассистенты
- RPC
- IoT-Scada
- Удаленный доступ
- Обновления ПО
- Сети
- Социальные сети
- Криптовалюты
- Обмен файлами
- Системные
- Базы данных
- VoIP
- VPN
- Кибербезопасность
- Музыка
- Командная работа
- Магазины
- Чаты и мессенджеры
- Почта
- Медиа-контент
- Майнинг

Описание приложений и протоколов, доступных для создания профилей

Приложения и протоколы	**Описание**
1kxun	Китайский видеосервис. На нем представлены различные анимационные фильмы, телевидение, спорт и кино
AccuWeather	Частная американская медиа-компания, предоставляющая коммерческие услуги по прогнозированию погоды по всему миру
Activision	Американская компания по изданию и разработке компьютерных игр, разработчик Call of Duty
AdobeConnect	Платформа веб-конференций, которая позволяет пользователям проводить онлайн-встречи, вебинары
ADS_Analytic_Track	Отслеживание и аналитика рекламы (mobile marketing analytics and attribution platform)
AFP	Протокол представительского и прикладного уровней сетевой модели OSI, предоставляющий доступ к файлам в MacOS X
AJP	Протокол, который может проводить входящие запросы с веб-сервера до сервера приложений
Alibaba	Китайская публичная компания, работающая в сфере интернет-коммерции, владелец веб-порталов Taobao.com, Tmall, Alibaba.com и ряда других
AliCloud	Компания, предоставляющая ресурсы для облачных вычислений, дочерняя компания Alibaba Group
Amazon	Американская компания-разработчик платформ электронной коммерции и публично-облачных вычислений

AmazonAlexa	Облачная голосовая служба Amazon
AmazonAWS	Коммерческое публичное облако, поддерживаемое и развиваемое компанией Amazon
AmazonVideo	Стриминговый сервис компании Amazon
AmongUs	Многопользовательская компьютерная игра
AMQP	Открытый протокол прикладного уровня для передачи сообщений между компонентами системы
ANSI_C1222	Протокол прикладного уровня, предназначенный для использования в сетях электросчетчиков Smart Grid
AnyDesk	Приложение для удаленного рабочего стола, распространяемое AnyDesk Software GmbH
Apple	Компания-производитель смартфонов и компьютерной техники
AppleiCloud	Облачное хранилище от компании Apple, которое предоставляет пользователям доступ к их музыке, фотографиям, документам и другим файлам с любого устройства
AppleiTunes	Медиаплеер для организации и воспроизведения музыки и фильмов, разработанный компанией Apple и бесплатно распространявшийся для платформ MacOS и Windows
ApplePush	Сервис, созданный Apple для отправки уведомлений от сторонних приложений на устройства Apple
AppleSiri	Облачный персональный помощник и вопросно-ответная система компании Apple
AppleStore	Онлайн-магазин техники Apple и аксессуаров к ней
AppleTVPlus	Американский стриминговый сервис, принадлежащий и управляемый компанией Apple
Armagetron	Свободная компьютерная игра для операционных систем Linux, Windows, MacOS, FreeBSD и AmigaOS 4
AVAST	Семейство антивирусных программ, разработанных компанией Avast для операционных систем Windows, MacOS, Android и iOS
AVASTSecureDNS	Сервис защищенных DNS-серверов от компании Avast
Azure	Облачная платформа компании Microsoft. Предоставляет возможность разработки, выполнения приложений и хранения данных на серверах, расположенных в распределенных дата-центрах
BACnet	Сетевой протокол, применяемый в системах автоматизации зданий и сетях управления
Badoo	Приложение для онлайн-знакомств
BeckhoffADS	Открытый протокол обмена данными ADS на базе TCP/IP для общения с контроллером, разработанный BECKHOFF
BFCP	Протокол предназначен для обмена презентациями и демонстрации рабочего стола в рамках видеоконференции
BFD	Протокол обнаружения двунаправленной пересылки, который используется для обнаружения неисправностей между двумя маршрутизаторами или коммутаторами
BGP	Протокол динамической маршрутизации
BITCOIN	Криптовалюта, использующая децентрализованную систему для записи транзакций в блокчейне
BitTorrent	Пиринговый протокол для кооперативного обмена файлами через интернет
BJNP	Протокол обнаружения служб локальной сети, используемый принтерами и сканерами Canon. Компьютерные системы используют этот протокол для автоматического обнаружения устройств Canon в сети
Bloomberg	Американская компания, информационное агентство, один из двух ведущих американских поставщиков финансовой информации для профессиональных участников финансовых рынков
Bluesky	Bluesky Social представляет собой децентрализованную социальную платформу для микроблогов
Cachefly	Поставщик сети доставки контента
CAPWAP	Сетевой протокол с возможностью взаимодействия, который позволяет центральному контроллеру доступа к беспроводной локальной сети управлять набором беспроводных оконечных точек
Cassandra	Распределенная система управления базами данных, относящаяся к классу NoSQL-систем и рассчитанная на создание масштабируемых хранилищ данных, представленных в виде хеша
Ceph	Свободная программная объектная сеть хранения, обеспечивающая как файловый, так и блочный интерфейсы доступа
CHECKMK	Протокол используется для мониторинга серверных и контейнерных систем в ИТ-инфраструктуре
CIP	Информационно-управляющий протокол, который обеспечивает обмен сообщениями ввода/вывода в реальном времени и прямой обмен информационными сообщениями
CiscoSkinny	Корпоративный (проприетарный) VoIP-протокол для управления взаимодействием между оконечными телефонными устройствами и сервером телефонной системы (IP-АТС)
CiscoVPN	Протокол VPN, разработанный компанией Cisco Systems
Citrix	Программа, предоставляющая доступ к приложениям и рабочим столам с удаленного клиентского устройства с помощью ресурсов Citrix Virtual Apps and Desktops и Citrix DaaS
ClickHouse	Система управления базами данных с открытым исходным кодом, построенная на основе колонок
Cloudflare	Американская компания, предоставляющая услуги CDN, защиту от DDoS-атак, безопасный доступ к ресурсам и серверы DNS

CloudflareWarp	Бесплатный VPN от CloudFlare, который проксирует все сетевые запросы в системе (включая обновления Windows и др. ПО, трафик многопользовательских игр, торренты)
CNN	Американский круглосуточный кабельный телеканал новостей
COAP	Протокол для взаимодействия простых устройств, например, датчиков малой мощности, выключателей, клапанов, которые управляются или контролируются удаленно через интернет
CoD_Mobile	Бесплатный шутер для устройств iOS и Android
Collectd	Демон Unix, который собирает, передает и хранит данные о производительности компьютеров и сетевого оборудования
Controller_Area_Network	Стандарт протокола связи, используемый для обмена данными между устройствами в автомобильной промышленности и других промышленных приложениях
Corba	Технологический стандарт написания распределенных приложений, продвигаемый консорциумом OMG, и соответствующая ему информационная технология
CPHA	Алгоритм хеширования, который может использоваться для безопасного хранения паролей в PTC
Crashlytics	Инструмент отчетности о сбоях, который помогает выявлять ошибки
Crossfire	Южнокорейский тактический сетевой шутер от первого лица, разработанный компанией SmileGate
CryNetwork	Составной модуль для создания многопользовательских игр
Cybersec	Компании сферы кибербезопасности: checkpoint.com norton.com, kaspersky.com, fortinet.com
Dailymotion	Французский видеохостинг
DataSaver	Функция для Chrome, которая позволяет значительно сократить использование мобильных данных
Dazn	Спортивный стриминговый сервис
DCERPC	Система удаленного вызова процедур, разработанная для Distributed Computing Environment
Deezer	Французский интернет-сервис потоковой передачи музыки
DHCP	Протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети
DHCPV6	Протокол динамического конфигурирования хостов для межсетевого протокола версии 6
Diameter	Сеансовый протокол, созданный, отчасти, для преодоления некоторых ограничений протокола RADIUS
DirecTV	Компания прямого телерадиовещания в США, сигналы цифрового спутникового телевидения и радио передаются на территорию США и Латинской Америки
Discord	Кроссплатформенная проприетарная система мгновенного обмена сообщениями с поддержкой VoIP и видеоконференций, предназначенная для использования различными сообществами по интересам
DisneyPlus	Американский сервис потокового вещания типа OTT на основе подписки
DLEP	Протокол маршрутизации с учетом радиосвязи (RAR)
DNP3	Протокол передачи данных, используемый для связи между компонентами АСУ ТП
DNS	Протокол, используемый для получения IP адреса хоста по его доменному имени
DNScrypt	Протокол шифрования DNS-трафика
Dofus	Массовая многопользовательская ролевая онлайн-игра (MMORPG), использующая Flash-графику и фэнтезийный сеттинг
DoH_DoT	Протокол защиты DNS-трафика (запросов и ответов) от перехвата и подмены. В том числе включает обычные DNS-запросы адресов DoT/DoH-серверов
Dota2	Многопользовательская командная компьютерная игра в жанре MOBA, разработанная и изданная корпорацией Valve
DRDA	Набор протоколов, обеспечивающих возможность связи между программами и системами баз данных на разных платформах и позволяющих распределять реляционные данные по нескольким платформам
Dropbox	Файловый хостинг компании Dropbox Inc, включающий персональное облачное хранилище, синхронизацию файлов и программу-клиент
DTLS	Протокол передачи данных, обеспечивающий защищенность соединений для протоколов, использующих датаграммы
EAQ	Entitade Aferidora da Qualidade de Banda Larga - эксцентричный протокол VoIP/конференц-связи, который редко встречается в реальной жизни
eBay	Американская компания, предоставляющая услуги в областях интернет-аукционов и интернет-магазинов
Edgecast	Децентрализованное приложение для потоковой передачи видео, построенное на собственной технологии блокчейн THETA со смарт-контрактами
eDonkey	Файлообменная сеть, построенная по принципу P2P на основе сетевого протокола прикладного уровня MFTP
EGP	Устаревший протокол обмена информации между маршрутизаторами нескольких автономных систем
Elasticsearch	Тиражируемая программная поисковая система
ElectronicArts	Американская публичная транснациональная корпорация, занимающаяся распространением и изданием компьютерных игр (FIFA, Battlefield)

EpicGames	Американская компания, занимающаяся разработкой компьютерных игр и программного обеспечения, в частности - Fortnite
ETHEREUM	Криптовалюта и платформа для создания децентрализованных онлайн-сервисов на базе блокчейна
EthernetGlobalData	Протокол связи, разработанный GE Fanuc Automation для обмена данными в реальном времени между устройствами автоматизации и системами управления с использованием стандартной технологии Ethernet
EthernetIP	Промышленный сетевой стандарт, который поддерживает неявный обмен сообщениями (обмен сообщениями ввода/вывода в реальном времени), явный обмен (обмен сообщениями) или оба и использует широко распространенные коммерческие чипы связи Ethernet и физические носители
Ether-S-Bus	Промышленный протокол управления, используемый компанией SAIA Burgess
EtherSIO	Протокол используется для передачи данных между программируемыми логическими контроллерами и удаленными устройствами ввода/вывода производства компании Saia-Burgess Controls Ltd
Facebook	Крупнейшая социальная сеть в мире, которой владеет компания Meta Platforms
FacebookMessenger	Приложение для обмена мгновенными сообщениями и видео, созданное Meta
FacebookVoip	Голосовые и видеозвонки в FaceBook
FastCGI	Клиент-серверный протокол взаимодействия веб-сервера и приложения, дальнейшее развитие технологии CGI
FbookReelStory	Короткие видеоролики на Facebook
FINS	Открытый протокол связи поддерживаемый большинством контроллеров и сетей разработки компании Omron
FIX	Протокол передачи данных, являющийся международным стандартом для обмена данными между участниками биржевых торгов в режиме реального времени
FLUTE	Доставка файлов по однонаправленному транспорту
FortiClient	Комплексное решение безопасности, предназначенное для защиты компьютеров и ноутбуков. Также имеет версии для планшетов и мобильных устройств под управлением Android и Apple iOS
FTP_CONTROL	Протокол, предназначенный для передачи файлов в компьютерных сетях
FTP_DATA	Протокол доступа, предназначенный для удаленной передачи файлов в компьютерных сетях
FTPS	Расширение широко используемого протокола передачи файлов FTP, которое добавляет поддержку для криптографических протоколов уровней транспортной безопасности и защищенных сокетов
Fuze	Файловая система в пользовательском пространстве для Unix-подобных операционных систем, позволяющая непривилегированным пользователям создавать собственные файловые системы без редактирования кода ядра
GaijinEntertainment	Частная компания, разработчик и издатель компьютерных игр, в частности - War Thunder
Gearman	Платформа приложений с открытым исходным кодом, предназначенная для распределения соответствующих компьютерных задач на несколько компьютеров
GeForceNow	Облачный игровой сервис компании Nvidia
GenshinImpact	Компьютерная игра в жанре action-adventure с открытым миром и элементами RPG, разработанная китайской компанией miHoYo Limited
Git	Распределенная система управления версиями
GitHub	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки
GitLab	Веб-инструмент жизненного цикла DevOps с открытым исходным кодом, представляющий систему управления репозиториями кода для Git с собственной вики, системой отслеживания ошибок, CI/CD пайплайном и другими функциями
GMail	Бесплатная почтовая служба от компании Google. Предоставляет доступ к почтовым ящикам через веб-интерфейс и по протоколам POP3, SMTP и IMAP, а также в приложении Gmail на Android
Gnutella	Протокол для распределенного обмена файлами, в основном, музыкальными
Google	Американская технологическая компания, которая специализируется на поисковых технологиях, искусственном интеллекте, онлайн-рекламе, программным обеспечением, бытовой электроникой
GoogleCall	Аудио- и видеозвонки, совершаемые с помощью (любых) приложений Google (например, Google Meet)
GoogleChat	Коммуникационный сервис, разработанный компанией Google
GoogleClassroom	Облачная платформа для организации образовательного процесса
GoogleCloud	Предоставляемый компанией Google набор облачных служб. Выполняются на той же инфраструктуре, которую Google использует для своих продуктов, предназначенных для конечных потребителей
GoogleDocs	Текстовый онлайн-процессор, входящий в состав бесплатного веб-пакета редакторов GoogleDocs
GoogleDrive	Сервис хранения, редактирования и синхронизации файлов, разработанный компанией Google. Его функции включают хранение файлов в интернете, общий доступ к ним и совместное редактирование
GoogleMaps	Набор приложений, построенных на основе бесплатного картографического сервиса и технологии, предоставляемых компанией Google
GoogleMeet	Сервис видео-телефонной связи и видеоконференций, разработанный компанией Google

GoogleServices	Набор приложений и API, которые реализуют дополнительные возможности на устройствах Android. Сервисы Google для мобильных устройств включают основные приложения: Google Play, Gmail, Google Map, YouTube и Chrome
GoTo	Американская компания, предоставляющая услуги телефонных систем для бизнеса, контакт-центров и продукты для ИТ-поддержки
GRE	Протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems
GTP_C	Группа протоколов соединения на основе IP, используемая в сетях GSM, UMTS и LTE
GTP_PRIME	Группа протоколов связи на основе IP, используемых для передачи услуг пакетной радиосвязи общего пользования (GPRS) в сетях GSM, UMTS, LTE
GTP_U	Протокол используется для транспортировки пользовательских данных между пакетной сетью и радиосетью
GTP	Протокол туннелирования GPRS
Guildwars	Фэнтезийная массовая многопользовательская ролевая онлайн-игра, разработанная компанией ArenaNet и выпущенная компанией NCsoft в 2005 году
H323	Набор стандартов для передачи мультимедиа-данных по сетям с пакетной передачей
HalfLife2	Компьютерная игра, научно-фантастический шутер от первого лица
HAProxy	Программное обеспечение для балансировки нагрузки для TCP и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов
HART-IP	Адресуемый по магистрали удаленный преобразователь по IP. В основном используется для обмена данными в качестве стандартного глобального протокола между интеллектуальными устройствами и системой управления и некоторой интеллектуальной системой
HBO	Американский телеканал, принадлежащий компании WarnerMedia
Heroes_of_the_Storm	Онлайн-игра, разработанная Blizzard Entertainment для Microsoft Windows и MacOS
HiSLIP	Коммуникационный протокол для измерительного и тестового оборудования с использованием технологии VISA
HL7	Стандарт обмена, управления и интеграции электронной медицинской информации
HLS	Протокол для потоковой передачи медиа на основе HTTP, разработанный компанией Apple
HotspotShield	Программное обеспечение для организации виртуальной частной сети, обеспечивающей безопасную передачу данных по шифрованному соединению, защищенному от прослушивания
HP_VIRTGRP	Протокол HP Virtual Machine Group Management - часть пакета виртуализации, используемого в серверных средах HP
HSRP	Протокол маршрутизации семейства FHRP (англ. First-hop redundancy protocols), разработанный компанией Cisco и стандартизованный в RFC 2281
HTTP_Connect	Метод HTTP, который запускает двустороннюю связь с запрошенным ресурсом. Метод можно использовать для открытия туннеля
HTTP_Proxy	Тип прокси-сервера, который действует как сервер-посредник между клиентом и веб-сервером
HTTP	Протокол для получения с серверов гипертекстовых документов в формате HTML
HTTP2	Вторая крупная версия сетевого протокола HTTP, используемая для доступа к World Wide Web
Huawei	Трафик устройств Huawei
HuaweiCloud	Мобильное облако Huawei
Hulu	Стриминговый сервис по подписке, принадлежащий The Walt Disney Company
i3D	Протокол с низкой задержкой, используемый в основном игровыми серверами
IAX	Протокол обмена VoIP-данными между IP-АТС Asterisk и другим аналогичным софтсвичом или VoIP-телефоном
IceCast	Протокол для организации потокового цифрового аудиовещания и видеовещания
iCloudPrivateRelay	Сервис для маскировки IP-адреса пользователя с целью сохранения его конфиденциальности
ICMP	Протокол третьего уровня модели OSI, который используется для диагностики проблем со связностью в сети
ICMPV6	Протокол управляющих сообщений для межсетевого протокола версии 6
IEC60870	Набор протоколов для контроля и управления с использованием постоянного соединения
IEC62056	Набор стандартов Международной электротехнической комиссии для обмена данными учета электроэнергии
IEEE-C37118	Потоковый протокол для обмена и передачи данных синхрофазоров (или PMU), которые фиксируют устойчивое состояние или динамический отклик энергосистемы. Обеспечивает высокоскоростную передачу большого количества данных в режиме реального времени
IFLIX	Малайзийский бесплатный видеосервис
IGMP	Протокол управления групповой передачей данных в сетях, основанных на протоколе IP. Используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы
iHeartRadio	Американская платформа бесплатного вещания, подкастов и потокового радио, принадлежащая iHeartMedia
IMAP	Протокол для доступа к электронной почте

IMAPS	Протокол для осуществления доступа к электронной почте, включающий в себя обязательное шифрование
IMO	Веб-сервис и кроссплатформенное приложение для мгновенного обмена сообщениями и VoIP-звонков
Instagram	Американская социальная сеть для обмена фотографиями и видео
IP_in_IP	Протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет
IP_PIM	Семейство многоадресных протоколов маршрутизации для IP сетей, созданное для решения проблем групповой маршрутизации
IPP	Протокол, используемый для передачи документов на печать
IPSec	Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP
iQIYI	Китайская онлайн-видеоплатформа, предлагающая широкий спектр оригинального и лицензионного контента, включая фильмы, драмы, развлекательные шоу и аниме
IRC	Протокол прикладного уровня для обмена сообщениями в режиме реального времени
ISO9506-1-MMS	Протокол передачи данных реального времени и команд диспетчерского управления между сетевыми устройствами и/или программными приложениями
Jabber	Протокол основе на XML, открытый для использования. Предназначен для мгновенного обмена сообщениями и информацией о присутствии в режиме, приближенному к реального времени
JRMI	Протокол удаленного вызова методов Java
JSON-RPC	Протокол удаленного вызова процедур, использующий JSON для кодирования сообщений
Kafka	Распределенный программный брокер сообщений с открытым исходным кодом
KakaoTalk_Voice	Популярный в Южной Корее мессенджер, который поддерживает мгновенную передачу сообщений, позволяет отправлять файлы, а также совершать аудиозвонки и видеозвонки
KakaoTalk	Бесплатное мобильное приложение для мгновенного обмена сообщениями для смартфонов
KCP	Протокол связи, который максимально использует полосу пропускания для надежной связи с низкой задержкой
Kerberos	Протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними
Kismet	Сетевой детектор, анализатор пакетов и система обнаружения вторжений для беспроводных локальных сетей стандарта 802.11
KNXnet_IP	Протокол автоматизации зданий, который обеспечивает обмен данными и управляющей информацией через IP-сети, расширяя стандарт KNX для автоматизации дома и зданий
LastFM	Сервис для прослушивания музыки онлайн
LDAP	Протокол для доступа к службе каталогов X.500
LDP	Протокол маршрутизации, используемый для установления и поддержания путей с коммутацией меток в сети с многопротокольной коммутацией меток (MPLS)
Likee	Социальная сеть, пользователи которой могут создавать и распространять короткие музыкальные видео
Line	Приложение для смартфонов и ПК, средство моментального обмена сообщениями
LineCall	Система звонков/видеоконференций, используемая в популярном мобильном приложении для обмена сообщениями LINE
Linkedin	Американская социальная сеть для поиска и установления деловых контактов
LISP	Протокол маршрутизации, построенный на идее разделения топологического расположения точки присоединения к сети и идентификации узла
Livestream	Платная стриминговая платформа, которая позволяет клиентам загружать живое видео со своих мобильных устройств и компьютерных камер через интернет
LLMNR	Протокол, основанный на формате пакета данных DNS, который позволяет компьютерам выполнять разрешение имен хостов в локальной сети
LoLWildRift	League of Legends: Wild Rift - мобильная игра в жанре MOBA
LotusNotes	Программный продукт, платформа для автоматизации совместной деятельности рабочих групп, содержащий в себе средства электронной почты, персональных и групповых электронных календарей, службы мгновенных сообщений и среду исполнения приложений делового взаимодействия
MapleStory	Бесплатная многопользовательская ролевая онлайн-игра, разработанная южнокорейской компанией Wizet
Mastodon	Бесплатное программное обеспечение с открытым исходным кодом для запуска самостоятельных служб социальных сетей. Mastodon имеет функции микроблогов, аналогичные Twitter
MDNS	Многоадресный протокол DNS, используемый для преобразования имени хостов в IP-адреса в небольших сетях, не включающих локальный сервер имен
Megaco	Протокол для управления функциями шлюза на границе пакетной сети
Memcached	Протокол кеширования, используемый для ускорения динамических веб-приложений путем кеширования данных в памяти

MerakiCloud	Сервис компании Cisco, предоставляющий доступ к облачным технологиям
MGCP	Протокол управления медиашлюзами
Microsoft	Американская корпорация-разработчик в сфере проприетарного программного обеспечения для различного рода вычислительной техники: персональных компьютеров, игровых приставок, КПК, мобильных телефонов и прочего
Microsoft365	Набор веб-сервисов на основе платформы Microsoft Office, электронная почта, функции для общения и управления документами, которые распространяются на основе подписки по схеме программное обеспечение как услуга
Mining	Протоколы, использующиеся программами-майнерами
Modbus	Протокол, основанный на архитектуре ведущий - ведомый, применяется в промышленности для организации связи между электронными устройствами
Monero	Криптовалюта на основе протокола CryptoNote, ориентированная на повышенную конфиденциальность транзакций
MongoDB	Протокол, используемый для взаимодействия клиентов и серверов MongoDB
MPEG_TS	Протокол для передачи аудиоданных и видеоданных, описанных в MPEG2
MpegDash	Протокол потоковой передачи данных, предоставляющий возможность доставки потокового мультимедиа-контента через интернет по протоколу HTTP
MQTT	Упрощенный сетевой протокол, работающий поверх, ориентированный на обмен сообщениями между устройствами по принципу "издатель - подписчик"
MS_OneDrive	Облачное хранилище компании Microsoft. Является частью спектра онлайновых услуг Windows Live
MS-RPCH	Microsoft RPC-over-HTTP (RPC через HTTP) позволяет клиентам RPC подключаться через интернет к программам сервера RPC и выполнять удаленные вызовы процедур
MsSQL-TDS	Протокол прикладного уровня, используемый для передачи данных между сервером базы данных и клиентом
Mullvad	Сервис по поставке услуг виртуальной частной сети (VPN) с открытым исходным кодом, работает с использованием протоколов WireGuard и OpenVPN
Mumble	Свободное кроссплатформенное VoIP-приложение с открытым кодом, включающее особую технологию «позиционирования звука», как основную отличительную особенность
Munin	Бесплатное программное приложение для мониторинга компьютерных систем, сети и инфраструктуры с открытым исходным кодом
MySQL	Протокол, используемый для взаимодействия клиентов и серверов MySQL
Nano	Консольный текстовый редактор для UNIX и Unix-подобных операционных систем
NAT-PMP	Сетевой протокол для автоматической установки параметров преобразования сетевых адресов и конфигураций переадресации портов без участия пользователя
Nats	Система обмена сообщениями с открытым исходным кодом
NestLogSink	Система логирования для домашней системы пожарной безопасности от Google
NetBIOS	Протокол, используемый для обнаружения компьютеров в сети
NetEaseGames	Трафик различных игр NetEase
Netflix	Стриминговый сервис фильмов и сериалов
NetFlow	Протокол, предназначенный для учета сетевого трафика, разработанный компанией Cisco Systems
NFS	Протокол сетевого доступа к файловым системам
Nintendo	Японская компания, специализирующаяся на создании видеоигр и игровых систем
NOE	New Office Environment - протокол VoIP, используемый совместимыми телефонными системами Alcatel-Lucent
NoMachine	Проект итальянской компании Medialogic S.p.A. для дистанционной работы
Ntop	Программное обеспечение, которое исследует компьютерную сеть
NTP	Протокол для синхронизации внутренних часов компьютера
Nvidia	Американская технологическая компания, разработчик графических процессоров и систем на чипе (SoC)
OCS	Спецификация программных интерфейсов класса REST для интеграции социальных интернет-коммуникаций в среды рабочего стола
OCSP	Протокол, используемый для получения статуса отзыва цифрового сертификата X.509
OICQ	Распространенный в Китае сервис мгновенного обмена сообщениями
Ookla	Американская компания, которая владеет сервисом по измерению скорости интернета Speedtest
OPC-UA	Программный интерфейс для промышленного протокола связи и модели данных. Используется для связи между конечными устройствами различных производителей по принципу клиент/сервер
OpenDNS	Протокол, предоставляющий общедоступные DNS-серверы
OpenFlow	Протокол управления процессом обработки данных, передающихся по сети маршрутизаторами и коммутаторами
OpenVPN	Протокол VPN с открытым исходным кодом

OpenWire	Библиотека программирования потоков данных с открытым исходным кодом
OperaVPN	VPN-клиент, встроенный в браузер Opera
Oracle	Американская компания, специализируется на выпуске систем управления базами данных, связующего программного обеспечения, бизнес-приложений
OSPF	Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала
Outlook	Персональный информационный менеджер с функциями почтового клиента, входящий в пакет офисных программ Microsoft Office
Pandora	Тип цифровой криптовалюты
Pastebin	Веб-приложение, которое позволяет загружать отрывки текста, обычно фрагменты исходного кода, для возможности просмотра окружающими
PathofExile	Бесплатная онлайн-ролевая игра в жанре экшен
PFCP	Протокол, используемый для связи между функциями управления (CP) и пользователя (UP) в сетях 4G и 5G
PGM	Протокол надежной многоадресной передачи данных
Pinterest	Социальный интернет-сервис, фотохостинг, позволяющий пользователям добавлять в режиме онлайн-изображения
Playstation	Игровая приставка, разработанная компанией Sony Computer Entertainment
PlayStore	Онлайн-магазин приложений для Android
Pluralsight	Платформа для онлайн-обучения
POP3	Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP
POPS	Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP, включающий в себя обязательное шифрование
PostgreSQL	Протокол, используемый для взаимодействия клиентов и серверов PostgreSQL
PPTP	Туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищенное соединение с сервером за счет создания специального туннеля в стандартной, незащищенной сети
PrivateInternetAccess	Персональная служба VPN
PROFINET_IO	Протокол для связи реального времени (RT) и изохронного реального времени (IRT) с децентрализованной периферией
Protobuf	Протокол сериализации (передачи) структурированных данных, предложенный Google как эффективная бинарная альтернатива текстовому формату XML
ProtonVPN	Сервис по поставке услуг виртуальной частной сети (VPN), управляемый швейцарской компанией Proton AG
Psiphon	Бесплатный инструмент для обхода цензуры в интернете с открытым исходным кодом, в котором используется сочетание технологий защищенной связи и обфускации
PTPv2	Протокол синхронизации для промышленных сетей
QQ	Протокол мгновенного обмена сообщениями
QUIC	Экспериментальный интернет-протокол, позволяющий мультиплексировать несколько потоков данных между двумя компьютерами. Протокол работает поверх протокола UDP и содержит возможности шифрования, эквивалентные TLS и SSL
RADIUS	Протокол удаленной аутентификации пользователей, представляет собой ключевой элемент в обеспечении безопасности и управлении доступом в сетях
Radmin	Программа удаленного администрирования ПК для платформы Windows, которая позволяет полноценно работать на нескольких удаленных компьютерах с помощью графического интерфейса
Raft	Компьютерная игра в жанре симулятор выживания в открытом мире, разработанная шведской компанией Redbeet Interactive и изданная Axolot Games
RakNet	Кроссплатформенный сетевой сервис, разработанный Oculus VR для использования в игровой индустрии
RDP	Протокол удаленного рабочего стола
Reddit	Сайт, сочетающий черты социальной сети и форума, где зарегистрированные пользователи могут размещать ссылки на понравившуюся информацию в интернете и обсуждать ее
RESP	Двоичный протокол, в котором используются управляющие последовательности, закодированные в стандартном ASCII
RiotGames	Американская компания, разработчик видеоигр, издатель и организатор киберспортивных турниров (League of Legends)
RipeAtlas	Протокол зонда RIPE Atlas используется для крупнейшей в мире активной сети измерения интернета
RMCP	Протокол многоадресной передачи с ретрансляцией для предоставления услуг сквозной многоадресной передачи данных по сетям на базе IP-протокола
Roblox	Игровая онлайн-платформа и система создания игр, позволяющая любому пользователю создавать свои собственные и играть в созданные другими игры
Roughtime	Протокол с криптографической защитой на базе UDP, который используется для синхронизации времени серверов
RSH	Протокол, позволяющий подключаться удаленно к устройству и выполнять на нем команды

RSYNC	Утилита для удаленной синхронизации и копирования файлов
RTCP	Протокол управления передачей в реальном времени
RTMP	Проприетарный протокол потоковой передачи данных, в основном используемый для передачи потокового видео и аудиопотоков с веб-камер через интернет
RTP	Протокол, используемый при передаче трафика реального времени
RTPS	Real-Time Publish-Subscribe Protocol - это протокол реального времени для распределенных систем, обеспечивающий обмен структурированными данными
RTSP	Real Time Streaming Protocol - потоковый протокол реального времени - позволяет управлять вещанием: выполнять несколько команд, такие как "старт", "стоп", "переход на определенное время"
RX	Клиент-серверный RPC-протокол, расширенная и объединенная версия старых протоколов R и RFTP
S7Comm	Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400
S7CommPlus	Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400. Сложнее протокола S7Comm и использует двухбайтовое поле под названием ID сессии для защиты от атак воспроизведения
Salesforce	Американская компания, разработчик одноименной CRM-системы, предоставляемой по модели SaaS
SAP	Протокол позволяет сетевым устройствам постоянно корректировать данные о том, какие сервисные услуги имеются сейчас в сети
SCTP	Протокол управления потоком передачи с установлением соединения, как TCP, но передающий данные сообщениями, как UDP
SD-RTN	Software Defined Real-time Network - собственный протокол компании Agora, предназначен для потоковой передачи данных с низкой задержкой
Service_Location_Protocol	Протокол обнаружения сервисов, который позволяет компьютерам и иным устройствам находить сервисы в локальной сети без предварительной конфигурации
sFlow	Протокол, используемый для сбора, отправки и анализа информации о сетевом трафике в целях мониторинга
Showtime	Американский кабельный телевизионный канал
Signal	Криптографический протокол, созданный для обеспечения сквозного шифрования голосовых вызовов, видеозвонков и мгновенных сообщений
SignalVoip	Протокол голосовой связи в мессенджере Signal
Sina	Китайская интернет-компания, владеет аналогом Twitter - сервисом Sina Weibo
SinaWeibo	Китайский сервис микроблогов, запущенный компанией Sina Corp
SIP	Протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения, онлайн-игры)
SiriusXMRadio	Американская радиовещательная компания в сфере спутникового радио и онлайн-радио
Skype_Teams	Сервис Microsoft, предназначенный для командной работы и обмена информацией между участниками проекта или команды
Skype_TeamsCall	Бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее видеосвязь через интернет. Опционально использует технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны
Slack	Корпоративный мессенджер
SMBv1	Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети
SMBv23	Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети
SMPP	Протокол одноранговой передачи коротких сообщений
SMTP	Протокол, предназначенный для передачи электронной почты
SMTPS	Протокол для передачи электронной почты, включающий в себя обязательное шифрование
Snapchat	Мобильное приложение обмена сообщениями с прикрепленными фото и видео
SnapchatCall	Протокол голосовой передачи, основанный на VoIP, в мессенджере Snapchat
SNMP	Протокол для управления устройствами в IP-сетях
SOAP	Протокол обмена структурированными сообщениями в распределенной вычислительной среде
SOCKS	Протокол сеансового уровня модели OSI, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно для них) и таким образом использовать сервисы за межсетевыми экранами (файрволами)

Softether	Бесплатное кроссплатформенное многопротокольное программное обеспечение VPN-клиента и VPN-сервера с открытым исходным кодом
SOMEIP	Автомобильное программное обеспечение, которое может использоваться для передачи управляющих сообщений
SoundCloud	Онлайн-платформа для распространения оцифрованной звуковой информации (например, музыкальных произведений)
Source_Engine	Игровой сервис, разработанный Valve Corporation для собственного использования и лицензирования другим разработчикам
Spotify	Стриминговый сервис, позволяющий легально прослушивать музыкальные композиции, аудиокниги и подкасты, не скачивая их на устройство
SRTP	Протокол, определяющий профиль протокола RTP. Предназначен для шифрования, установления подлинности сообщения, целостности, защиты от подмены данных RTP в однонаправленных и multicast-передачах медиа и приложениях
SSDP	Протокол, служащий для объявления и обнаружения сетевых сервисов
SSH	Протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений
StarCraft	Серия компьютерных игр в жанре стратегии в реальном времени, разработанная компанией Blizzard Entertainment
Steam	Онлайн-сервис цифрового распространения компьютерных игр и программ
SteamDatagramRelay	Закрытая виртуальная игровая сеть Valve. Используя функции API, позволяет перенести игровой трафик на сетевые магистрали Valve
STOMP	Simple Text Oriented Messaging Protocol, протокол обмена сообщениями
STUN	Протокол, который позволяет клиенту, находящемуся за сервером трансляции адресов (или за несколькими такими серверами), определить свой внешний IP-адрес, способ трансляции адреса и порта во внешней сети, связанный с определенным внутренним номером порта
Syncthing	Приложение, позволяющее синхронизировать файлы между несколькими устройствами
Syslog	Протокол отправки и регистрации сообщений о происходящих в системе событиях
Tailscale	VPN-сервис, который работает поверх WireGuard и позволяет получить доступ к контроллеру даже если у вас нет своего VPN-сервера
TargusDataspeed	Проприетарный протокол, используемый для тестирования пропускной способности. Был разработан компанией TARGUSinfo
Teams	Корпоративная платформа, объединяющая в рабочем пространстве чат, встречи, заметки и вложения
TeamSpeak	Компьютерная программа, предназначенная для голосового общения в сети посредством технологии VoIP
TeamViewer	Программное обеспечение для удаленного доступа, удаленного управления и удаленного обслуживания компьютеров и других конечных устройств
Telegram	Кроссплатформенная система мгновенного обмена сообщениями с функциями обмена текстовыми, голосовыми и видеосообщениями, а также стикерами, фотографиями и файлами многих форматов
TelegramVoip	Голосовые и видеозвонки в мессенджере Telegram
Telnet	Протокол для реализации текстового терминального интерфейса по сети
Tencent	Китайский конгломерат, создавший китайский клон ICQ, собственную валюту, отдельную соцсеть, множество игр, торговую площадку и WeChat
TencentGames	Подразделение Tencent Interactive Entertainment, выпускающее видеоигры, разработчик PUPG MOBILE
TencentVideo	Китайская стриминговая платформа, принадлежащая Tencent
Teredo	Сетевой протокол, предназначенный для передачи IPv6-пакетов через сети IPv4, в частности, через устройства, работающие по технологии NAT, путем их инкапсуляции в UDP-дейтаграммы
TES_Online	The Elder Scrolls Online - это MMORPG, действие которой разворачивается в фэнтезийном мире Тамриэля
TeslaServices	Портал с сервисной и диагностической информацией для компаний и частных лиц, занимающихся профессиональным обслуживанием и ремонтом автомобилей Tesla
TFTP	Простой протокол передачи файлов, как правило, используется при загрузке бездисковых систем
Threads	Онлайн-сервис для микроблогинга, разработанный компанией Meta Platforms как дополнение к Instagram
Threema	Кроссплатформенное зашифрованное приложение для обмена мгновенными сообщениями
Thrift	Программный фреймворк Apache Thrift, предназначенный для масштабируемой разработки межъязыковых сервисов
Tidal	Интернет-сервис подписки на музыку, подкасты и потоковое видео, сочетающий в себе звук без потерь и музыкальные видеоролики высокой четкости с эксклюзивным контентом и специальными функциями для музыки
TikTok	Сервис для создания и просмотра коротких видео, принадлежащий пекинской компании ByteDance
TINC	Открытый, самомаршрутизирующийся сетевой протокол и программная реализация, используемая для сжатых и зашифрованных виртуальных частных сетей
TiVoConnect	Протокол TivoConnect обеспечивает автоматическое обнаружение оборудования для двух или более систем медиаплееров Tivo, работающих в одной сети

TLS	Протокол защиты транспортного уровня
TocaBoca	Интерактивная мобильная игра
Tor	Протокол анонимной сети виртуальных туннелей, предоставляющий передачу данных в зашифрованном виде
TPLINK_SHP	Протокол TP-Link Smart Home Protocol используется для подключения устройств "Умного дома" с помощью приложения-компаньона
TruPhone	Глобальная мобильная сеть, которая занимается разработкой технологии eSim, позволяющей подключаться к разным провайдерам без замены сим-карты
Tumblr	Протокол микроблогов, включающий в себя множество картинок, статей, видео и gif-изображений по разным тематикам и позволяющий пользователям публиковать посты в их тамблелог
TuneIn	Американский аудиопотоковый сервис, транслирующий новости, эфиры радиостанций, спортивные мероприятия, музыку и подкасты
TunnelBear	Кроссплатформенный VPN-клиент
TuyaLP	Протокол Tuya LAN используется для взаимодействия многих IoT-устройств, включая светодиодные лампы, лампочки, умные розетки и другое
Twitch	Видеостриминговый сервис, специализирующийся на тематике компьютерных игр, в том числе на трансляциях геймплея и киберспортивных турниров
Twitter	Американский сервис микроблогов и социальная сеть, в которой пользователи публикуют сообщения и взаимодействуют с ними
UBNTAC2	Утилита управления оборудованием Ubiquiti airControl, версия 2
UbuntuONE	Онлайн-хранилище для обмена файлами и синхронизации между компьютерами и мобильными устройствами
UFTP	Протокол передачи файлов на основе UDP
UltraSurf	Бесплатная утилита для обхода цензурных ограничений в интернете
UMAS	Unified Messaging Application Services - проприетарный протокол Schneider Electric, который используется для конфигурации, мониторинга сбора данных и управления промышленными контроллерами Schneider Electric
Unknown	Не распознанные модулем протоколы и приложения
Usenet	Протокол, используемый для общения и публикации файлов
VHUA	Протокол, который использовался для Skype-подобных сервисов в Китае
Viber	Приложение-мессенджер, которое позволяет отправлять сообщения, совершать видео- и голосовые VoIP-звонки через интернет
ViberVoip	Аудио/видеозвонки, совершаемые с помощью приложения Viber
Vimeo	Американский сервис для публикации и просмотра видео
VK	Приложение для взаимодействия с социальной сетью ВКонтакте
VMware	Американская компания-разработчик программного обеспечения для виртуализации
VNC	Протокол удаленного доступа к рабочему столу
VRRP	Протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
Vudu	Потоковый сервис цифрового видео
VXLAN	Протокол инкапсуляции, который обеспечивает подключение центров обработки данных с использованием туннелирования для расширения соединений канального уровня в используемой сети сетевого уровня
Warcraft3	Компьютерная игра в жанре стратегии в реальном времени с элементами RPG
Waze	Бесплатное социальное навигационное приложение для мобильных устройств, позволяющее отслеживать ситуацию на дорогах в режиме реального времени, прокладывать оптимальные маршруты, узнавать о расположении радаров скорости
WebDAV	Набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах
Webex	Американская компания, которая разрабатывает и продает приложения для веб-конференций, видео-конференц-связи и контакт-центра как сервиса
WebSocket	Протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером, используя постоянное соединение
WeChat	Мобильная коммуникационная система для передачи текстовых и голосовых сообщений, разработана китайской компанией Tencent
WhatsApp	Американский бесплатный сервис обмена мгновенными сообщениями и голосовой связи по IP, принадлежащий компании Meta
WhatsAppCall	Протокол голосовой передачи, основанный на VoIP
WhatsAppFiles	Протокол загрузки медиафайлов (изображений, видео, музыки, документов) мессенджера WhatsApp

Whois-DAS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP, применяется для получения регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем
Wikipedia	Самая крупная в мире онлайн-энциклопедия
WindowsUpdate	Сервис обновления операционной системы Windows
WireGuard	Высокоскоростной и безопасный VPN-протокол
WorldOfKungFu	3D MMORPG с боевыми искусствами, основанная на традиционной китайской культуре
WorldOfWarcraft	Массовая многопользовательская ролевая онлайн-игра
WSD	Протокол многоадресного обнаружения для поиска сервисов в локальной сети. Работает через TCP- и UDP-порт 3702 и использует IP-адрес многоадресной рассылки 239.255.255.250 или ff02::c
Xbox	Домашняя игровая консоль, разработанная и выпущенная американской корпорацией Microsoft
XDMCP	Протокол аутентификации между X-сервером и X-клиентом
Xiaomi	Китайская корпорация-производитель смартфонов, компьютерной и бытовой техники
Yahoo	Американская компания, специализирующаяся на проектах и услугах в интернете. Владеет поисковой системой с одноименным названием
Yandex	Российская транснациональная компания в отрасли информационных технологий, владеющая одноименной системой поиска в интернете, интернет-порталом и веб-службами
YandexCloud	Публичная облачная платформа, разработанная российской интернет-компанией Яндекс
YandexDirect	Сервис для размещения объявлений контекстной рекламы на Яндексе и на сайтах-партнерах его рекламной сети
YandexDisk	Сервис для хранения данных в облаке
YandexMail	Почтовый сервис от компании Яндекс
YandexMarket	Сервис заказа товаров онлайн
YandexMetrika	Бесплатный сервис веб-аналитики, предлагаемый Яндексом, который отслеживает и сообщает о трафике веб-сайта
YandexMusic	Стриминговый сервис компании Яндекс, позволяющий слушать музыкальные композиции, их подборки, альбомы
Yojimbo	Менеджер личной информации для MacOS от Bare Bones Software. Позволяет хранить заметки, изображения и медиафайлы, URL-адреса, веб-страницы и пароли
YouTube	Видеохостинг, предоставляющий пользователям услуги хранения, доставки и показа видео
YouTubeUpload	Загрузка файлов на видеохостинг YouTube
Z3950	Клиент-серверный протокол для поиска и получения информации с удаленных компьютерных баз данных
Zabbix	Свободная система мониторинга статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования
Zattoo	Телевизионная платформа, которая предлагает прямые телетрансляции и контент по запросу для компьютеров, мобильных телефонов, планшетов и других сетевых устройств
ZeroMQ	Высокопроизводительная асинхронная библиотека обмена сообщениями, ориентированная на использование в распределенных и параллельных вычислениях
Zoom	Проприетарная программа для организации видеоконференций, разработанная компанией Zoom Video Communications
ZUG	Протокол ZUG является частью консенсусной модели Casper 2.0

Если нужного приложения нет в таблице **Доступ к приложениям** профиля **Контроля приложений**, но необходимо разрешить или заблокировать это приложение, используйте правила **Межсетевого экрана**:

1. Выясните, какие адреса серверов, порты и протоколы использует приложение. Для этого:
   - Обратитесь к разработчикам приложения или найдите информацию в открытых источниках.
   - Используйте логирование трафика и журнал Межсетевой экран.
2. Создайте правило Межсетевого экрана, которое будет разрешать или блокировать трафик по этим параметрам.

Также можно направить в Техническую поддержку запрос на добавление нового протокола, чтобы в будущем приложение появилось в списке **Контроля приложений**.

Полезные ссылки

- **Особенности создания профилей**
- **Пример создания иерархической структуры**
- **Настройка фильтрации трафика**

- **Как разрешить доступ к ресурсам в ограниченной сети**
- **Блокировка популярных ресурсов**

Особенности создания профилей

Классический контекст | Высокопроизводительный контекст

Принцип создания профилей **Контроля приложений** - все протоколы и приложения, которые не были запрещены, остаются разрешены.

Для удобства настройки модуля фильтрации рекомендуем объединить пользователей в несколько групп/подгрупп (например, в соответствии с организационной структурой компании) и настроить профиль **Контроля приложений** отдельно для каждой группы.

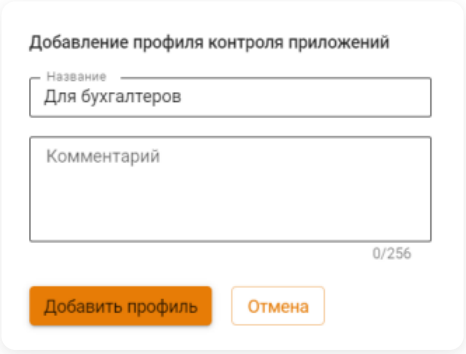
Создание профилей и добавление в правила Межсетевого экрана

Разберем создание профилей и добавление правил **Межсетевого экрана** на примере ограничения доступа к социальным сетям пользователям группы **Бухгалтерия**.

Создание профиля Контроля приложений

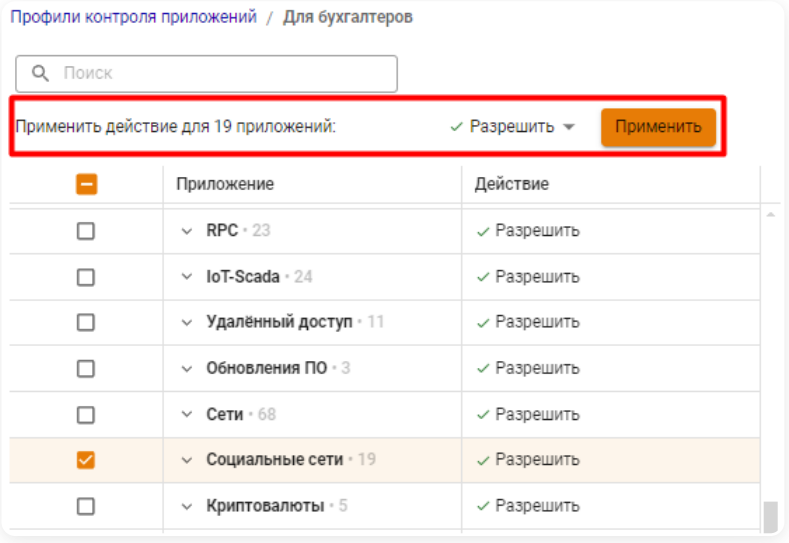
1. Перейдите в **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Заполните **Название**, **Комментарий** (необязательно) и добавьте профиль:

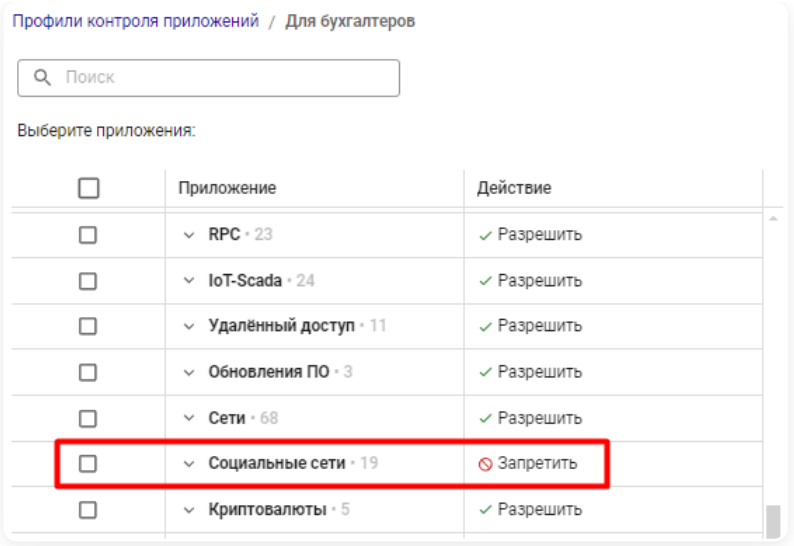


3. Нажмите в столбце **Управление** на  , затем **Доступ к приложениям**.

4. Выберите **Социальные сети** (при необходимости используйте поиск). Появится строка с выбором действия:



5. Примените действие **Запретить** рядом со строкой поиска и нажмите **Применить**. Действие применится к выбранным приложениям:



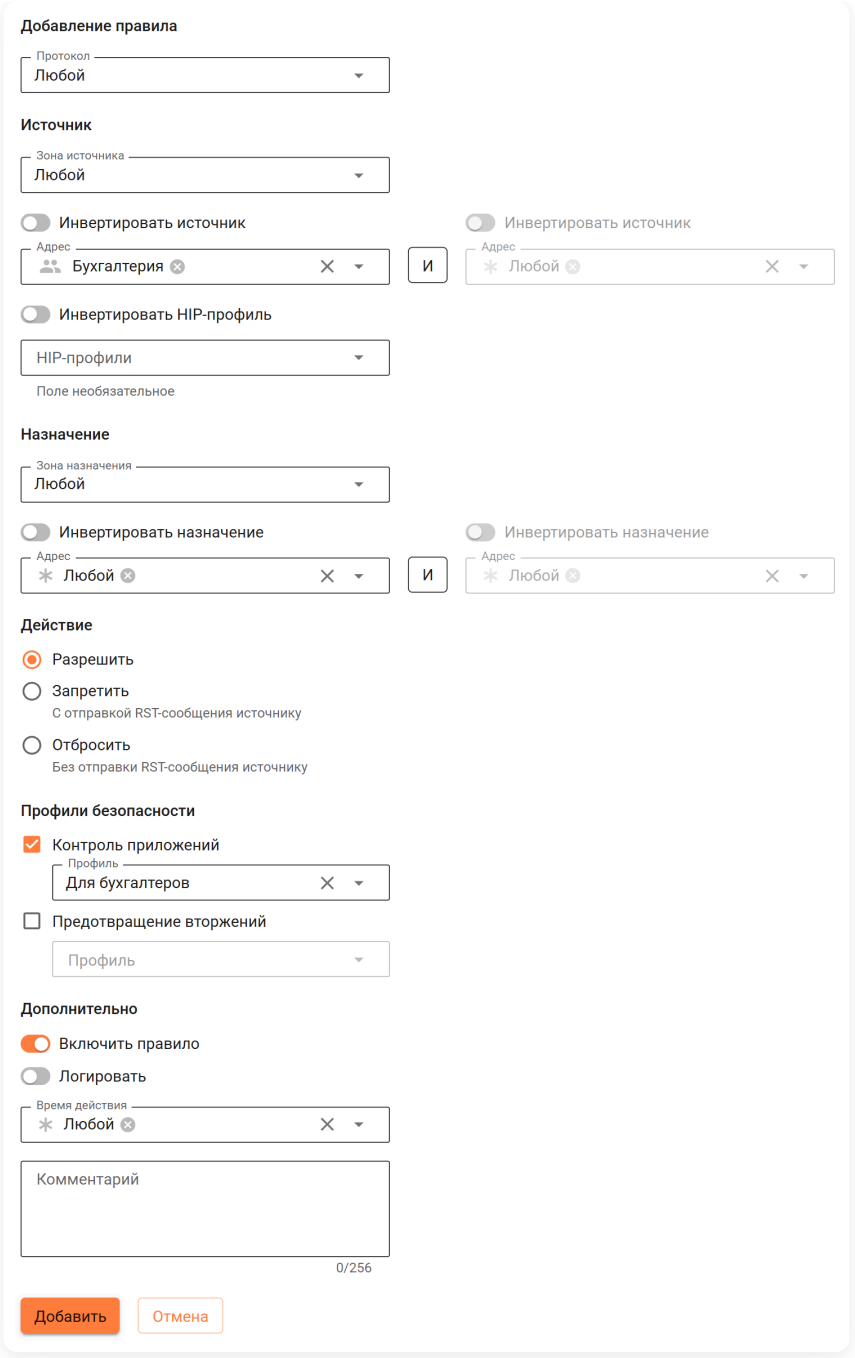
К неизвестным источникам по умолчанию применяется действие **Разрешить** (доступно для редактирования).

6. Нажмите **Сохранить**.

Добавление профиля в правила Межсетевого экрана

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать с помощью профиля **Контроля приложений**.
- **Источник** - выберите **Адрес**, **Зону**, созданную в **Системном контексте**, и **HIP-профиль** источника трафика.
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика, созданную в **Системном контексте**.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** в блоке **Профили безопасности** и из раскрывающегося списка выберите профиль, запрещающий социальные сети сотрудникам бухгалтерии.

4. Включите правило и нажмите **Добавить**.

5. Если в **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правило INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку DNS-трафик направляется в INPUT.

Иерархическая структура Профилей контроля приложений

Один из вариантов корректного применения политик безопасности к вложенной структуре пользователей - построение иерархической структуры профилей **Контроля приложений**:

- Профили для самой большой группы пользователей запрещают наибольшее количество протоколов и приложений.

- Профили для более мелких групп пользователей повторяют запрет для самой большой группы пользователей, но точечно разрешают определенные приложения и протоколы для конкретных подгрупп.
- Профили для конкретных пользователей разрешают определенные протоколы и приложения, необходимые этим конкретным пользователям. В этих профилях также остаются запреты, которые должны сохраниться для этих пользователей.

Полезные ссылки

- **Пример создания иерархической структуры**
- **Настройка фильтрации трафика, для которого в таблице FORWARD нет правил**

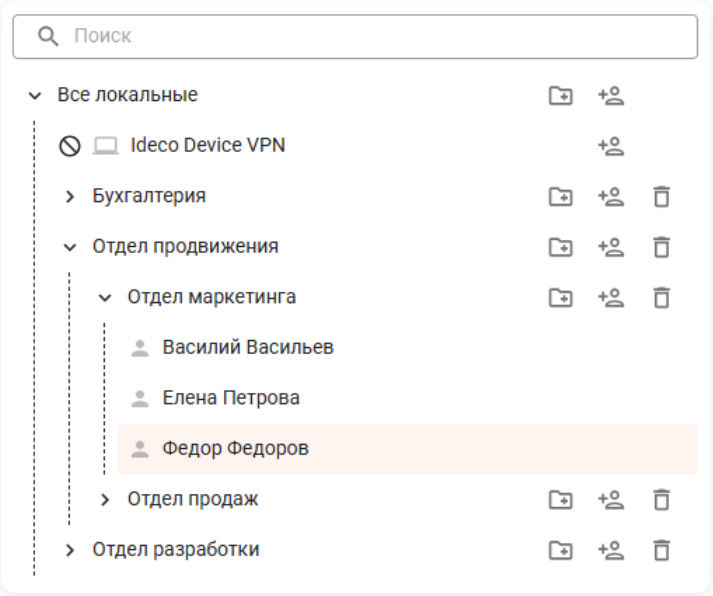
Пример создания иерархической структуры

Классический контекст | Высокопроизводительный контекст

Необходимо настроить профили **Контроля приложений** в соответствии с требованиями:

- Всем пользователям запрещены компьютерные игры, контент для взрослых, майнинг и криптовалюты.
- Доступ к социальным сетям разрешен только **Отделу продвижения**.
- Доступ к стриминговым сервисам разрешен только **Отделу маркетинга**.
- Доступ к музыкальным приложениям разрешен только **Федору Федорову** из **Отдела маркетинга**.

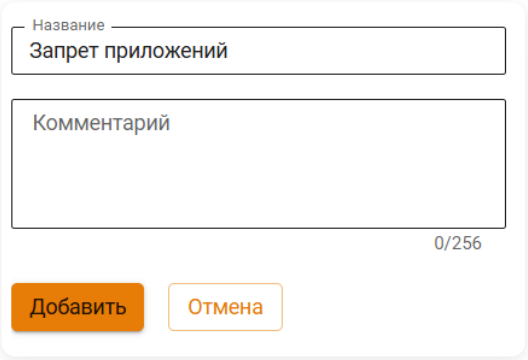
В описанном примере **Федор Федоров** - сотрудник **Отдела маркетинга**, а **Отдел маркетинга** - структурное подразделение **Отдела продвижения**:



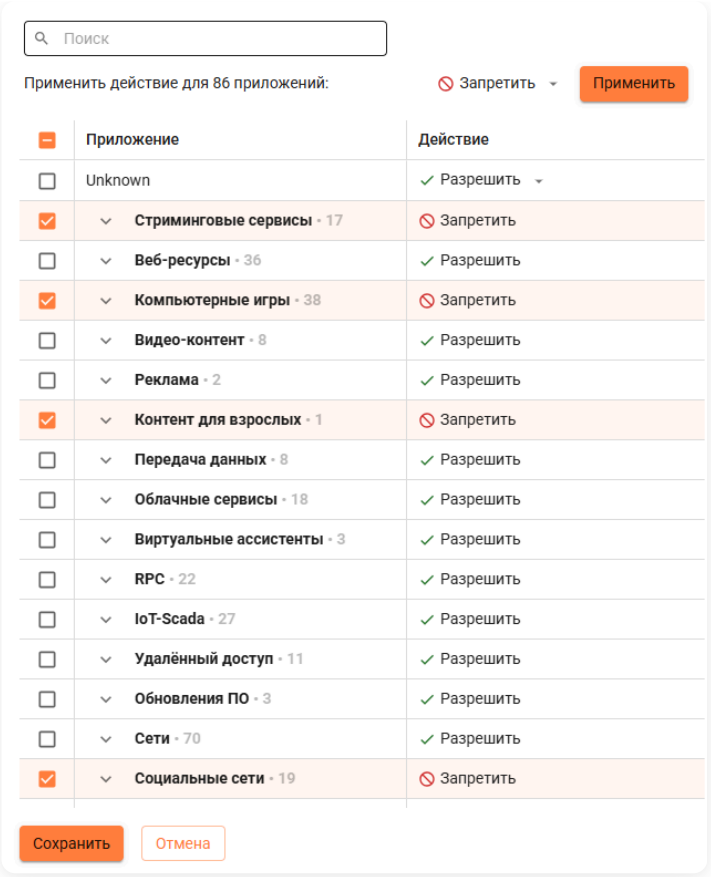
Создание профилей Контроля приложений

Создайте профили в соответствии с условиями примера:

1. Перейдите в **Профили безопасности** → **Контроль приложений**, чтобы создать профиль, запрещающий доступ к социальным сетям, стриминговым сервисам, музыкальным приложениям, компьютерным играм, контенту для взрослых, майнингу и криптовалютам. Нажмите **Добавить** и введите название профиля:



2. Настройте добавленный профиль:



- Перейдите в **Доступ к приложениям** и выберите группы приложений, которые необходимо запретить (перечислены в описании примера).
- Установите настройку **Запретить** и нажмите **Применить** в правом верхнем углу.
- После применения действия нажмите **Сохранить**.

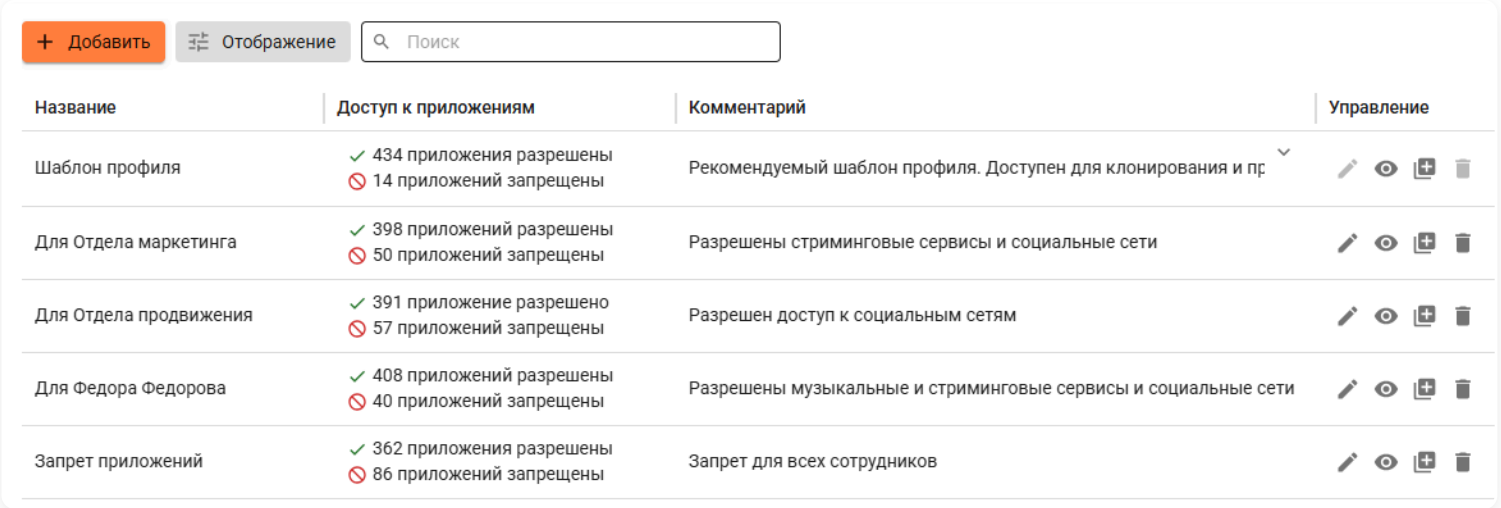
3. Создайте профиль для **Отдела продвижения**, разрешающий доступ к социальным сетям. Для этого:

- Клонируйте созданный профиль, нажав на  в столбце **Управление**.
- Отредактируйте клонированный профиль: поменяйте название (например, на **Для Отдела продвижения**) и настройки доступа к приложениям (разрешите доступ к социальным сетям).

4. Аналогично создайте профиль для Отдела маркетинга, разрешающий доступ к стриминговым сервисам. Для этого клонируйте профиль **Для Отдела продвижения**, введите название (например, **Для Отдела маркетинга**) и разрешите в нем доступ к стриминговым сервисам.

5. Создайте профиль для **Федора Федорова**, разрешающий доступ к музыкальным сервисам. Для этого клонируйте профиль **Для Отдела маркетинга** и установите необходимые настройки.

В итоге должен получиться набор профилей, учитывающий настройки, описанные в примере:

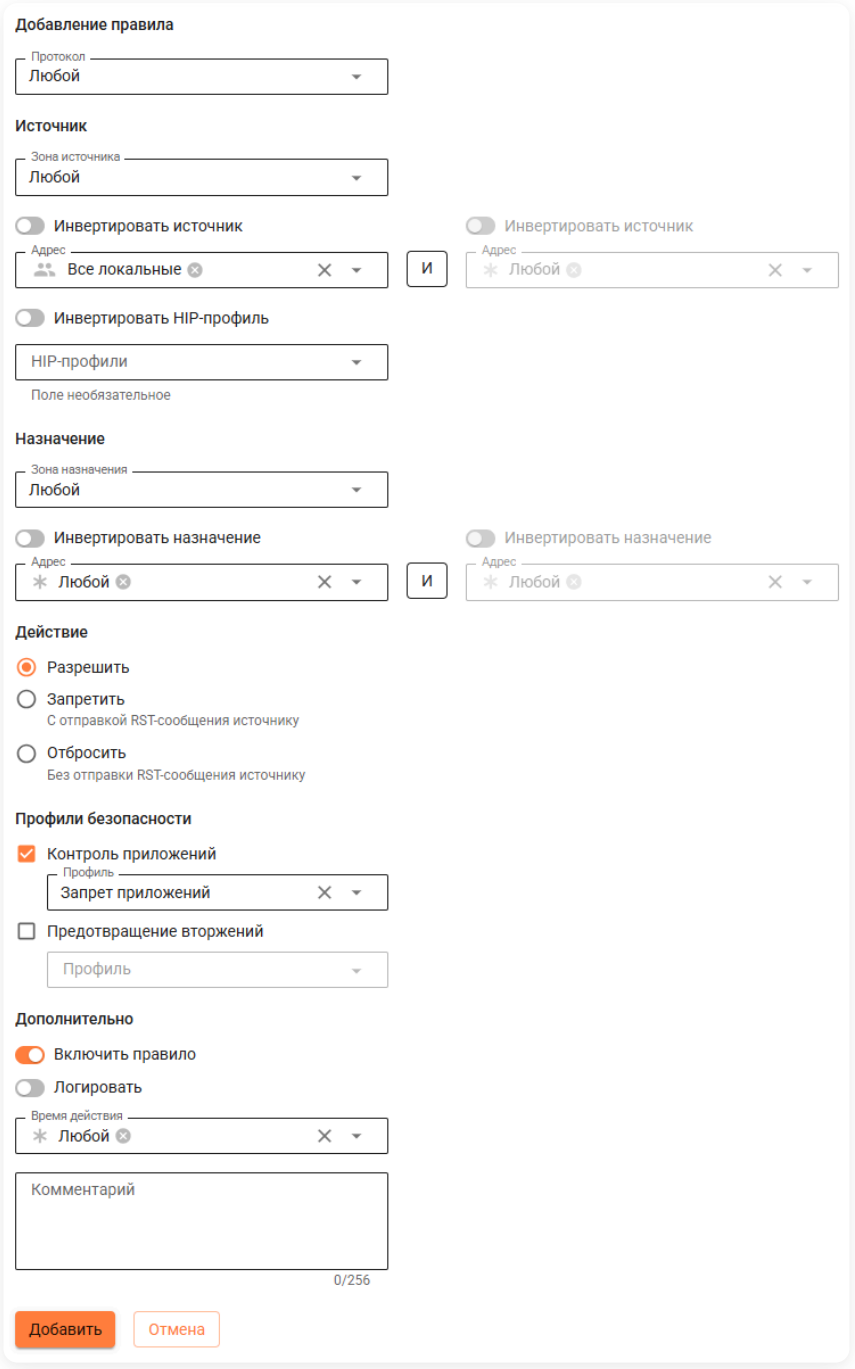


Создание правил Межсетевого экрана

Теперь необходимо создать и включить правила в **Межсетевом экране**, чтобы применить настройки для конкретных групп пользователей и установить приоритет прохождения трафика:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

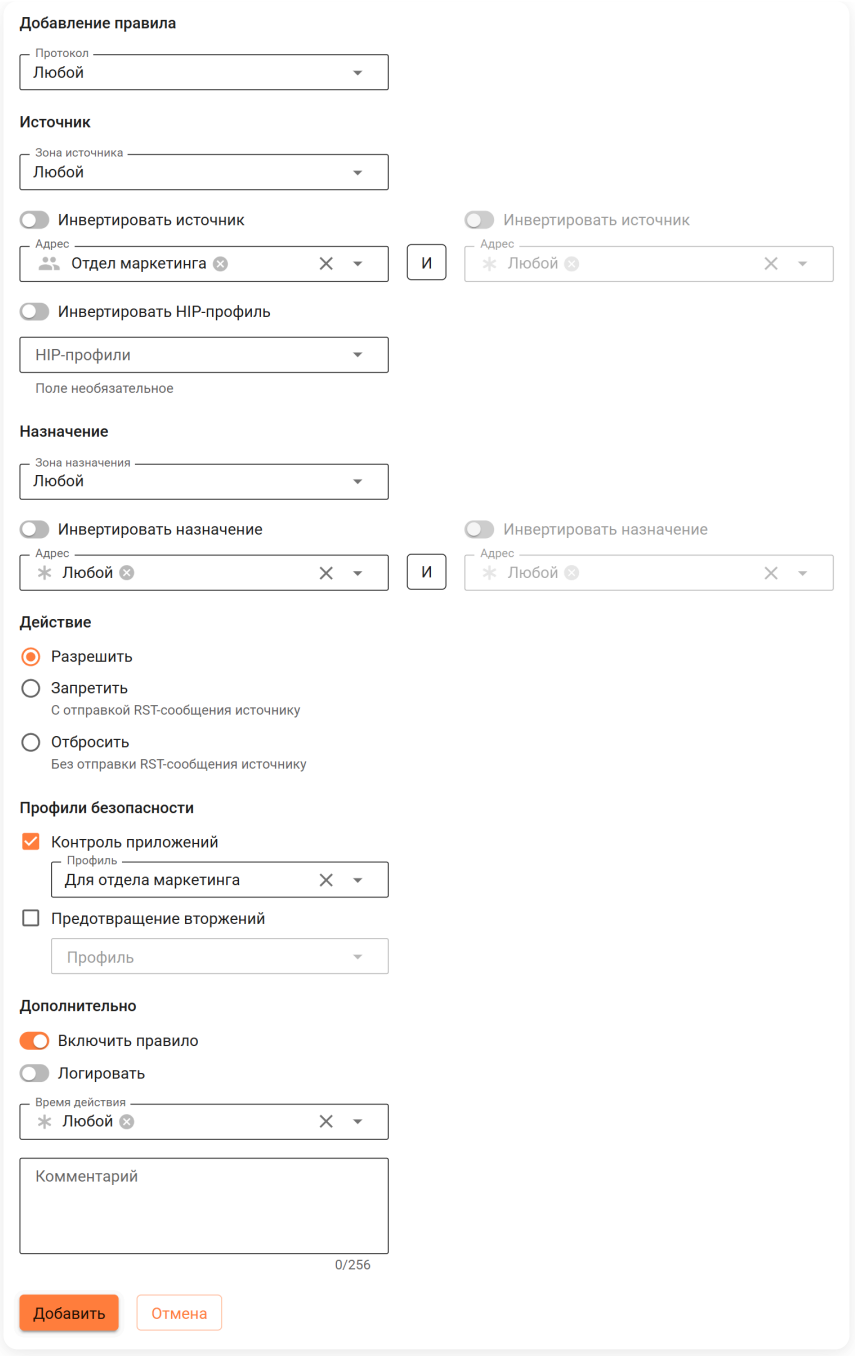
2. Заполните поля:



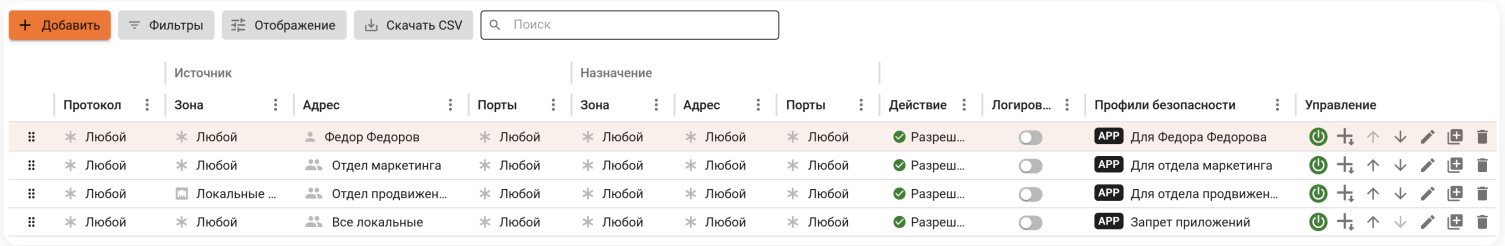
- **Адрес источника** - группа пользователей **Все локальные**.
- **Действие** - **Разрешить**.
- **Профили безопасности** - **Контроль приложений**, профиль **Запрет приложений**.

3. Включите правило и нажмите **Добавить**.

4. Аналогично создайте правила для каждого профиля. При создании правила **Межсетевого экрана** укажите соответствующий профилю адрес источника. Например, при создании правила с профилем фильтрации **Для Отдела маркетинга** выберите в поле **Адрес** блока **Источник** группу **Отдел маркетинга**:



5. Чтобы трафик проходил в соответствии с условиями примера, установите в **Межсетевом экране** следующую последовательность правил:



Чем выше в таблице стоит правило, тем выше его приоритет.

Разрешающее правило для сотрудника не сработает, если выше в таблице **Межсетевого экрана** находится правило, запрещающее трафик для отдела, в котором работает этот сотрудник.

6. Если в **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правила **INPUT** для протоколов **TCP** и **UDP** с теми же профилями безопасности, источником и портом `53` в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку DNS-трафик направляется в **INPUT**.

Настройка фильтрации трафика

Классический контекст | Высокопроизводительный контекст

Создайте профиль **Контроля приложений**, соответствующий нужным правилам:

1. Перейдите в **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Введите **Название** профиля, **Комментарий** и добавьте профиль.

3. Перейдите в **Доступ к приложениям**.

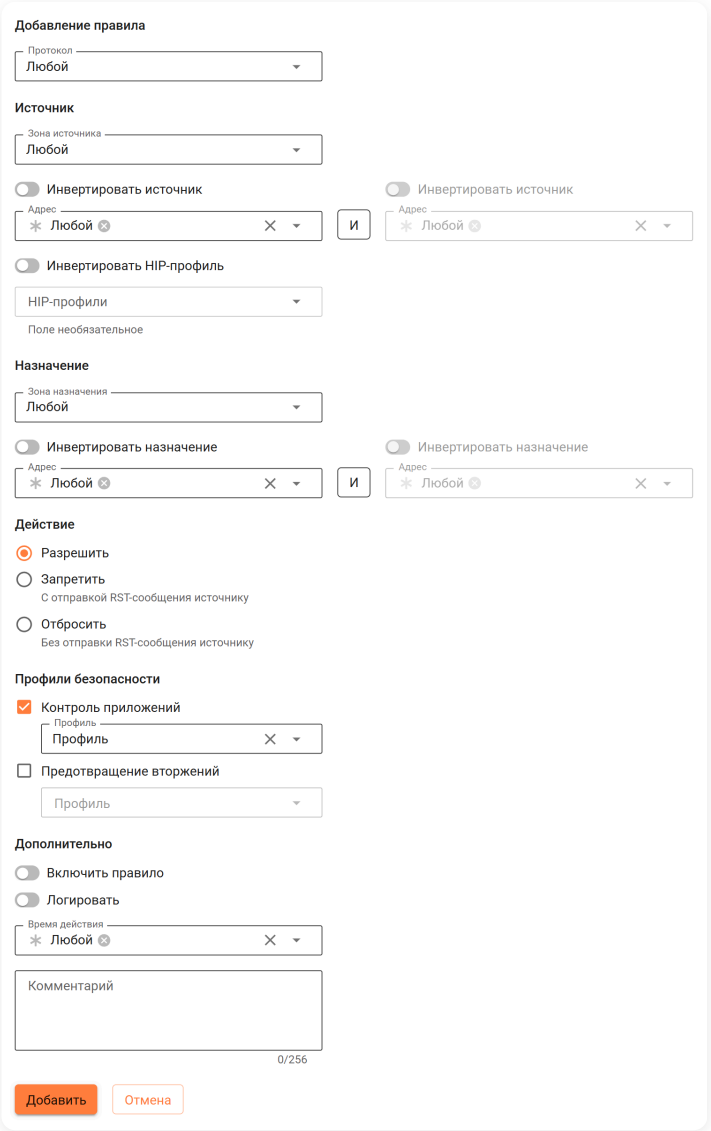
4. Выберите протоколы или группы протоколов и действия (**Запретить** или **Разрешить**), которые будут к ним применяться, затем нажмите **Применить**.

5. Нажмите **Сохранить**.

Далее создайте правило **Межсетевого экрана** с созданным профилем **Контроля приложений**:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите **Любой**.
- **Источник**:

    - **Зона источника** - выберите **Локальные интерфейсы**.
    - **Адрес** - укажите при необходимости адрес источника трафика.
    - **HIP-профиль** - укажите при необходимости профиль, соответствующий устройству, от которого исходит трафик.
- **Назначение**:
    - **Зона назначения** - выберите **Любой**.
    - **Адрес** - укажите при необходимости адрес источника трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** в блоке **Профили безопасности** и из раскрывающегося списка выберите созданный ранее профиль.

4. Включите правило и нажмите **Добавить**.

5. Поместите правило в конец таблицы **Межсетевого экрана**. Если в таблице есть правило, запрещающее все, поместите правило с профилем **Контроля приложений** над ним.

6. Если в **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, зоной источника **Локальные интерфейсы** и портом 53 в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку DNS-трафик направляется в INPUT.

Профили предотвращения вторжений

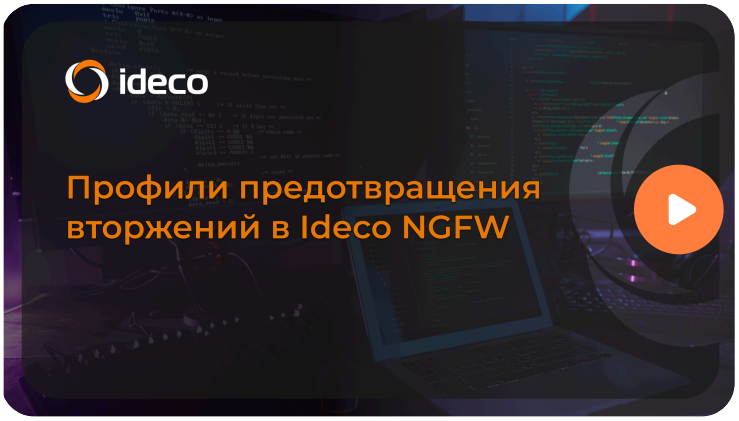
Классический контекст | Высокопроизводительный контекст | API

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



В разделе **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые NGFW Novum будет применять к трафику, соответствующему этим сигнатурам.

Профили предотвращения вторжений применяются при создании правил в разделе **Правила трафика** → **Межсетевой экран**.

Если профиль не добавлен в правила таблицы **FORWARD** или **INPUT** раздела **Правила трафика** → **Межсетевой экран**, трафик не будет фильтроваться модулем **Предотвращение вторжений**.

В обработке трафика не участвуют:

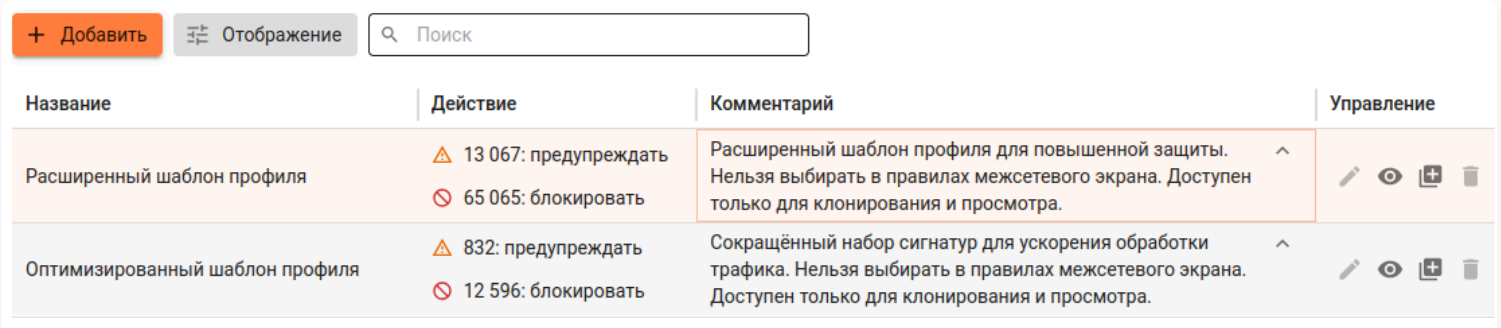
- Сигнатуры, не используемые в профилях.
- Профили, не используемые в правилах **Межсетевого экрана**.

Создание профилей

1. Перейдите в раздел **Профили безопасности** → **Предотвращение вторжений** и нажмите **Добавить**.

Создание профиля через шаблон

1. Для клонирования нажмите :



- **Расширенный шаблон профиля** - подходит для максимальной защиты от кибератак. Он включает динамически обновляемые черные списки хостов и эффективно очищает трафик из внешних сетей.
- **Оптимизированный шаблон профиля** - используется для достижения максимальной производительности. Он почти не содержит правил блокировки по черным спискам, поэтому не подходит для очистки внешнего трафика.

2. Чтобы просмотреть или изменить созданный профиль (описание и правила выбора сигнатур), нажмите на или .

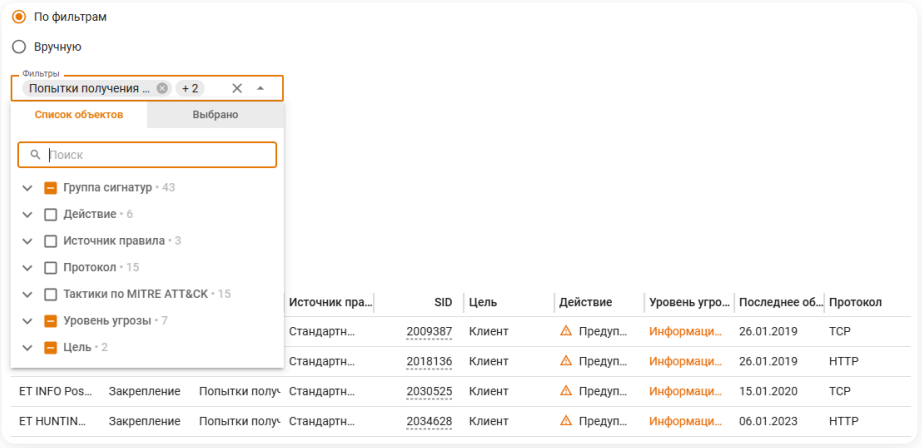
2. Введите название профиля, комментарий и нажмите **Добавить**.

3. Перейдите на вкладку **Сигнатуры** и нажмите **Добавить сигнатуры**.

4. Выберите способ добавления сигнатур в профиль:

По фильтрам

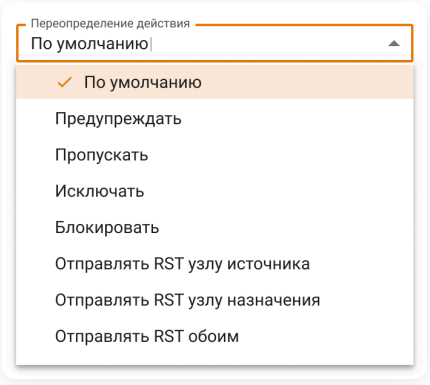
5. Выберите **Фильтры**. В таблице ниже отобразятся сигнатуры, соответствующие каждому из выбранных фильтров:



Доступные фильтры

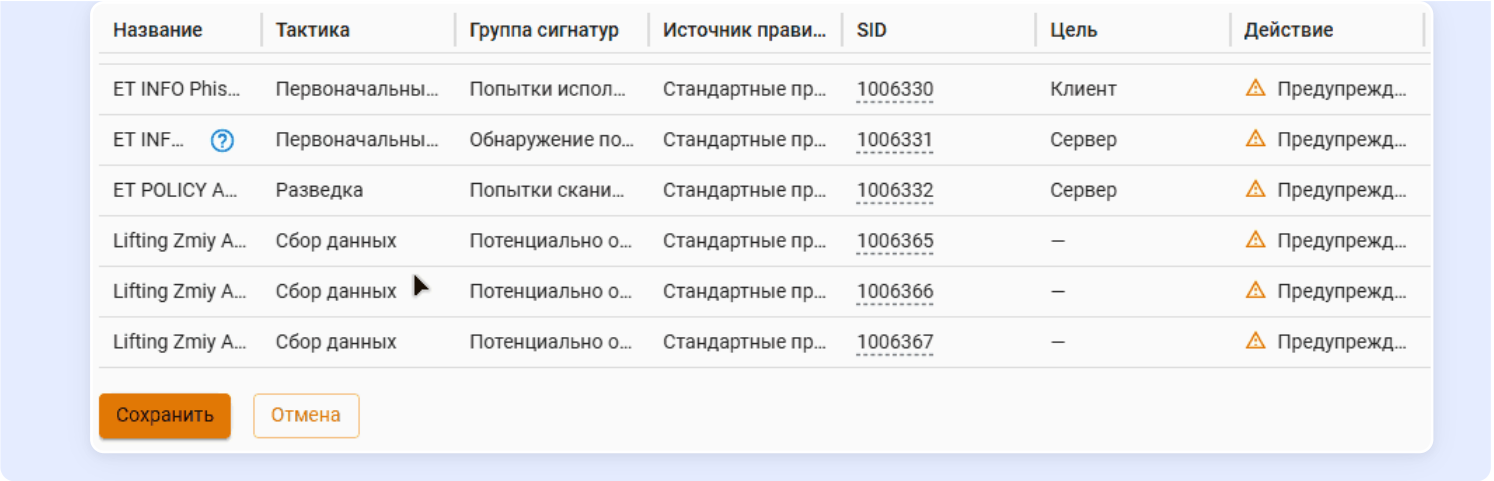
- **Группа сигнатур** - фильтр по готовым наборам сигнатур, сгруппированным по типу угроз.
- **Действие** - фильтр по действию, которое Ideco NGFW Novum применит к трафику, соответствующему сигнатуре.
- **Источник правила** - фильтр по источнику сигнатуры.
- **Протокол** - фильтр по сетевому протоколу, который анализирует сигнатура.
- **Тактики по MITRE ATT&CK** - фильтр по тактикам согласно матрице MITRE ATT&CK.
- **Уровень угрозы** - фильтр по степени опасности сигнатур в соответствии со стандартом CVSS (Common Vulnerability Scoring System).
- **Цель** - фильтр по цели атаки, которую обнаруживает сигнатура.

6. Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие **По умолчанию**:

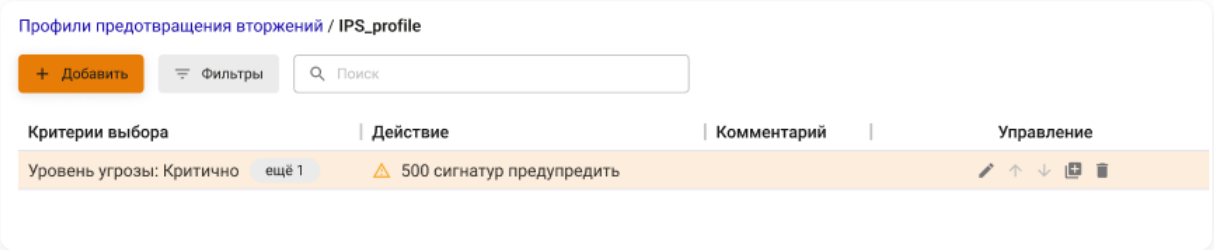


- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения. Система пропускает трафик, как если бы угроза отсутствовала.
- **Исключать** - исключить сигнатуру из профиля. Удаляет сигнатуру из анализа системы IPS, что снижает количество ложных срабатываний и предотвращает анализ по нежелательным правилам.
- **Блокировать** - отбросить пакет и сгенерировать предупреждение.
- **Отправлять RST узлу источника** - отправить ошибку `RST/ICMP unreach` отправителю пакета.
- **Отправлять RST узлу назначения** - отправить пакет с ошибкой `RST/ICMP error` получателю исходного пакета.
- **Отправлять RST обоим** - отправить пакеты с ошибкой `RST/ICMP error` отправителю и получателю исходного пакета.

Flowbit-сигнатуры предназначены для маркировки трафика. К Flowbit-сигнатуре могут быть применены только действия **Пропускать** и **Предупреждать**:

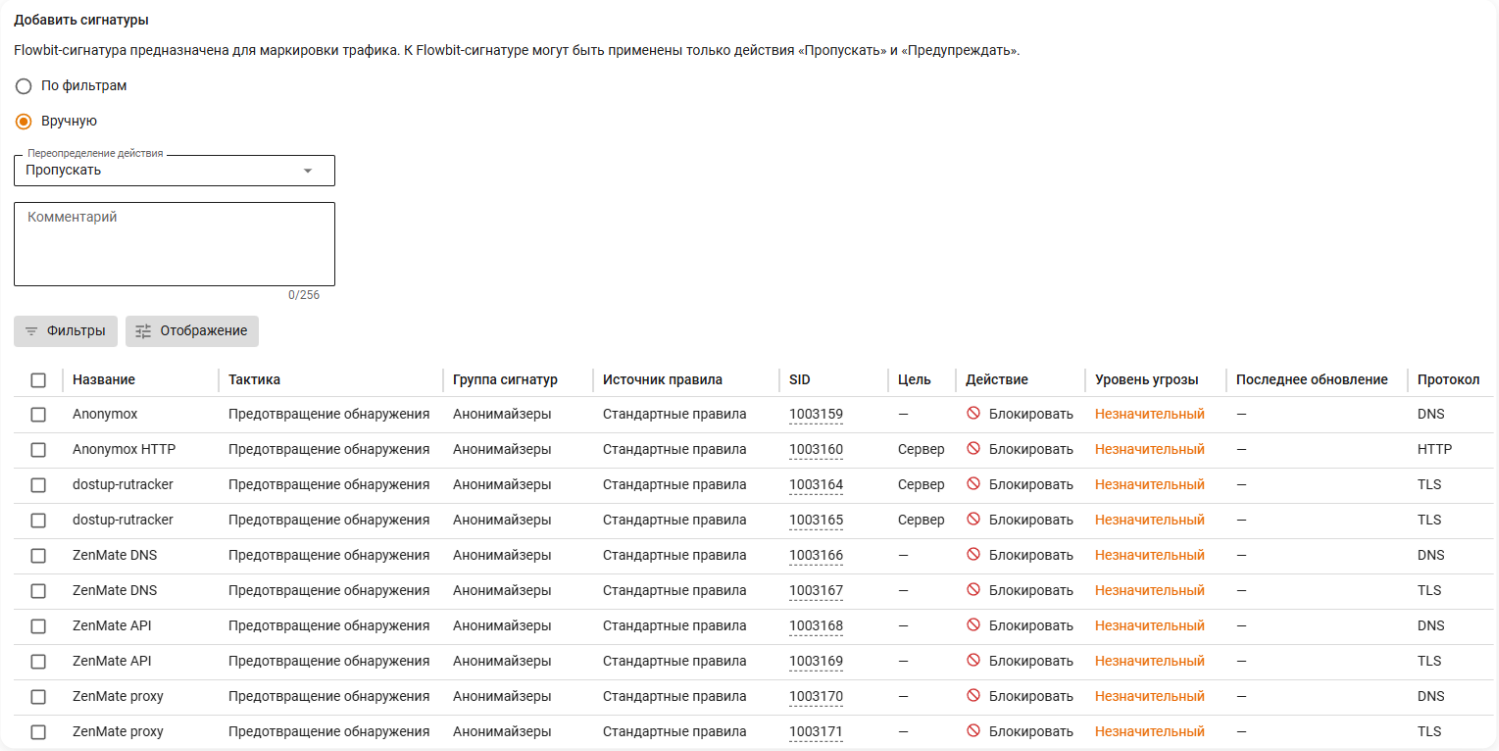


7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

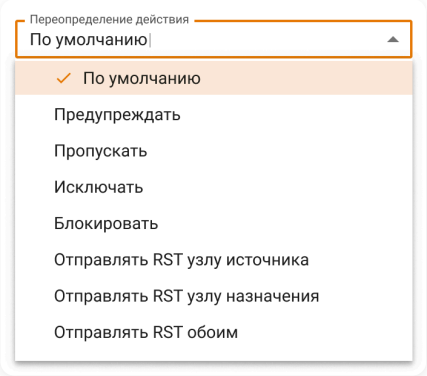


Вручную

5. В таблице отметьте сигнатуры, которые хотите добавить в профиль (при необходимости воспользуйтесь **Фильтром** отображения):

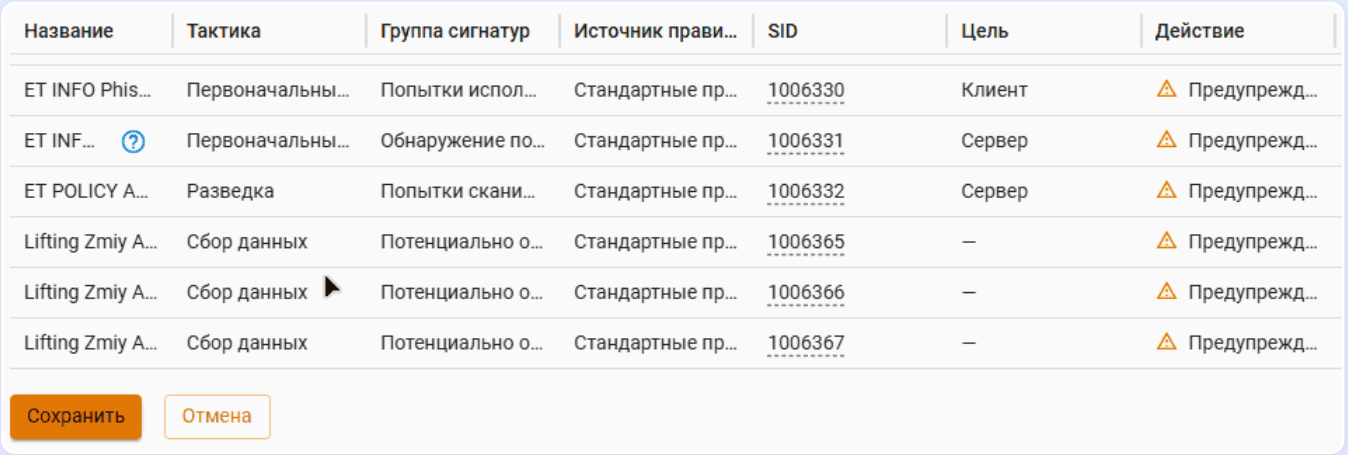


6. Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие **По умолчанию**:

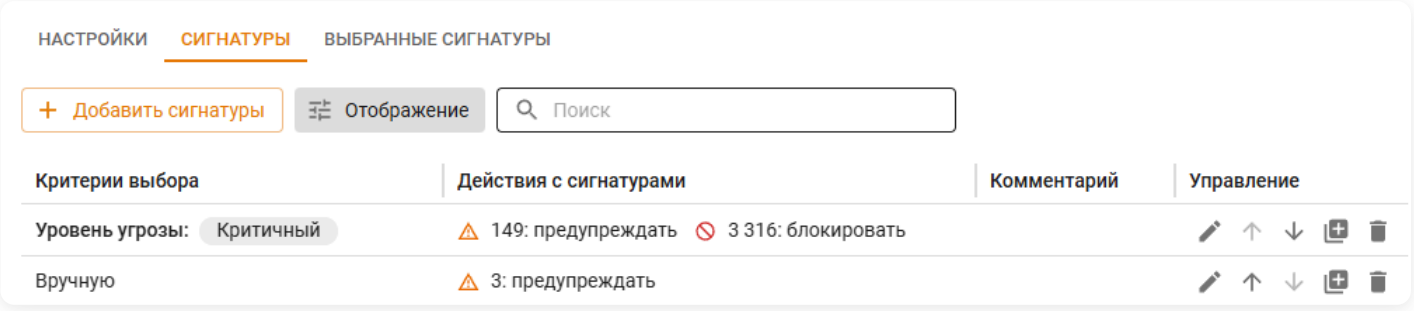


- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения. Система пропускает трафик, как если бы угроза отсутствовала.
- **Исключать** - исключить сигнатуру из профиля. Удаляет сигнатуру из анализа системы IPS, что снижает количество ложных срабатываний и предотвращает анализ по нежелательным правилам.
- **Блокировать** - отбросить пакет и сгенерировать предупреждение.
- **Отправлять RST узлу источника** - отправить ошибку `RST/ICMP unreach` отправителю пакета.
- **Отправлять RST узлу назначения** - отправить пакет с ошибкой `RST/ICMP error` получателю исходного пакета.
- **Отправлять RST обоим** - отправить пакеты с ошибкой `RST/ICMP error` отправителю и получателю исходного пакета.

Flowbit-сигнатуры предназначены для маркировки трафика. К Flowbit-сигнатуре могут быть применены только действия **Пропускать** и **Предупреждать**:



7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

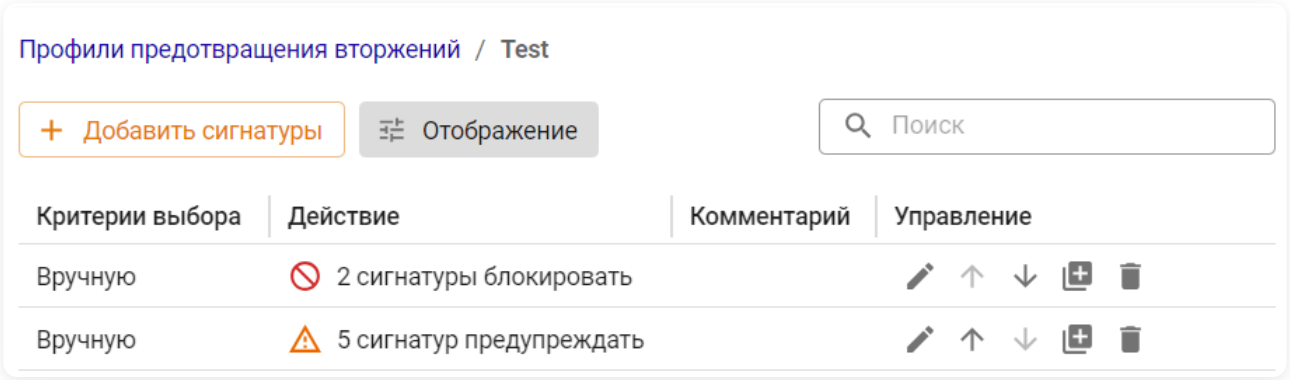


Количество сигнатур, отображаемых в таблице профилей, не всегда соответствует количеству сигнатур, добавленных при создании профиля. Это связано с тем, что для каждой сигнатуры может быть настроено несколько действий, но применяется только приоритетное. Приоритет определяется порядком правил внутри профиля.

В один профиль **Предотвращения вторжений** можно добавить несколько правил выбора сигнатур. Приоритет можно менять в таблице профиля кнопками ↑ и ↓.

Пример отображения профиля при выборе нескольких действий сигнатур

Настройки профиля Test:



- Действие **Блокировать** применяется для сигнатур Anonymox и Anonymox HTTP (2 сигнатуры).
- Действие **Предупреждать** применяется для сигнатур Anonymox, Anonymox HTTP, ZenMate DNS, ZenMate API и ZenMate proxy (5 сигнатур).
- Блокирующее правило приоритетнее предупреждающего.

При переходе в раздел **Профили безопасности** → **Предотвращение вторжений** в профиле Test отображаются 2 сигнатуры с действием **Блокировать** и 3 сигнатуры с действием **Предупреждать**, потому что фактически для дублирующихся сигнатур применяется более приоритетное правило:

Пример добавления сигнатур для исключения из анализа системы

1. Откройте редактирование профиля **Предотвращения вторжений**, нажав .

2. Перейдите на вкладку **Сигнатуры** и нажмите **Добавить сигнатуры**.

3. Выберите сигнатуры для исключения из фильтров или добавьте их вручную:

- Используйте ручной способ добавления и фильтрацию для точного поиска сигнатуры, например, по SID:

4. Выберите действие **Исключать** и нажмите **Добавить**.

5. В таблице измените приоритет сигнатур, переместив сигнатуры с действием **Исключить** выше:

6. Сохраните изменения в профиле.

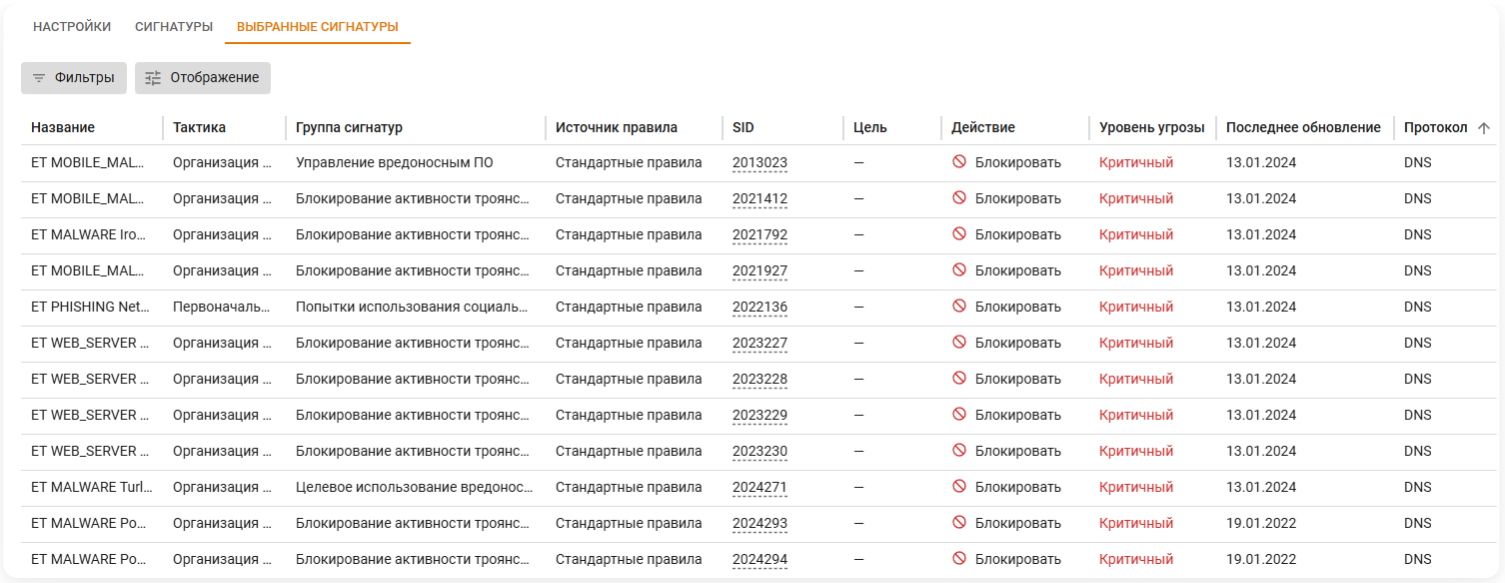
Использование оперативной памяти:

- Шаблоны профилей не потребляют оперативную память.
- Настроенный профиль потребляет оперативную память, даже если не задействован в правилах Межсетевого экрана.
- Объем оперативной памяти, потребляемый одним профилем, зависит от количества сигнатур. Потребление памяти профилями, настроенными по шаблонам:
  - Расширенный: ~450 МБ.
  - Оптимизированный: ~100 МБ.

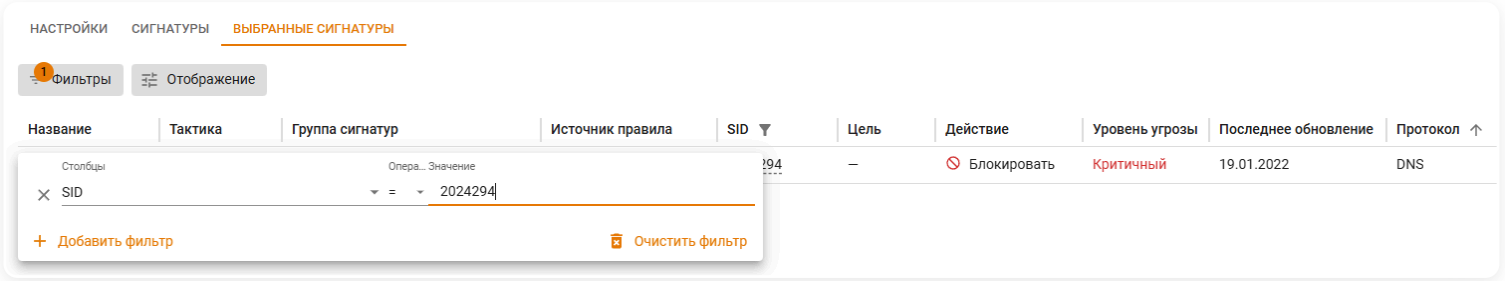
Указаны примерные значения, так как сигнатуры обновляются.

Управление профилями

Чтобы просмотреть или изменить созданный профиль (описание и правила выбора сигнатур), нажмите на или . На вкладке **Выбранные сигнатуры** представлены все сигнатуры, для которых настроено одно или несколько действий:



Для удобного поиска воспользуйтесь **Фильтром**. Например, чтобы найти нужную сигнатуру по идентификатору:

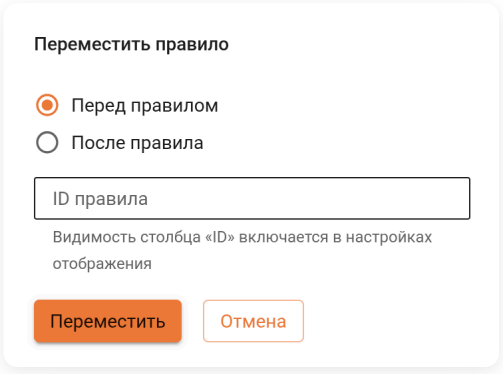


На вкладке **Сигнатуры** доступно перемещение правил. Выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



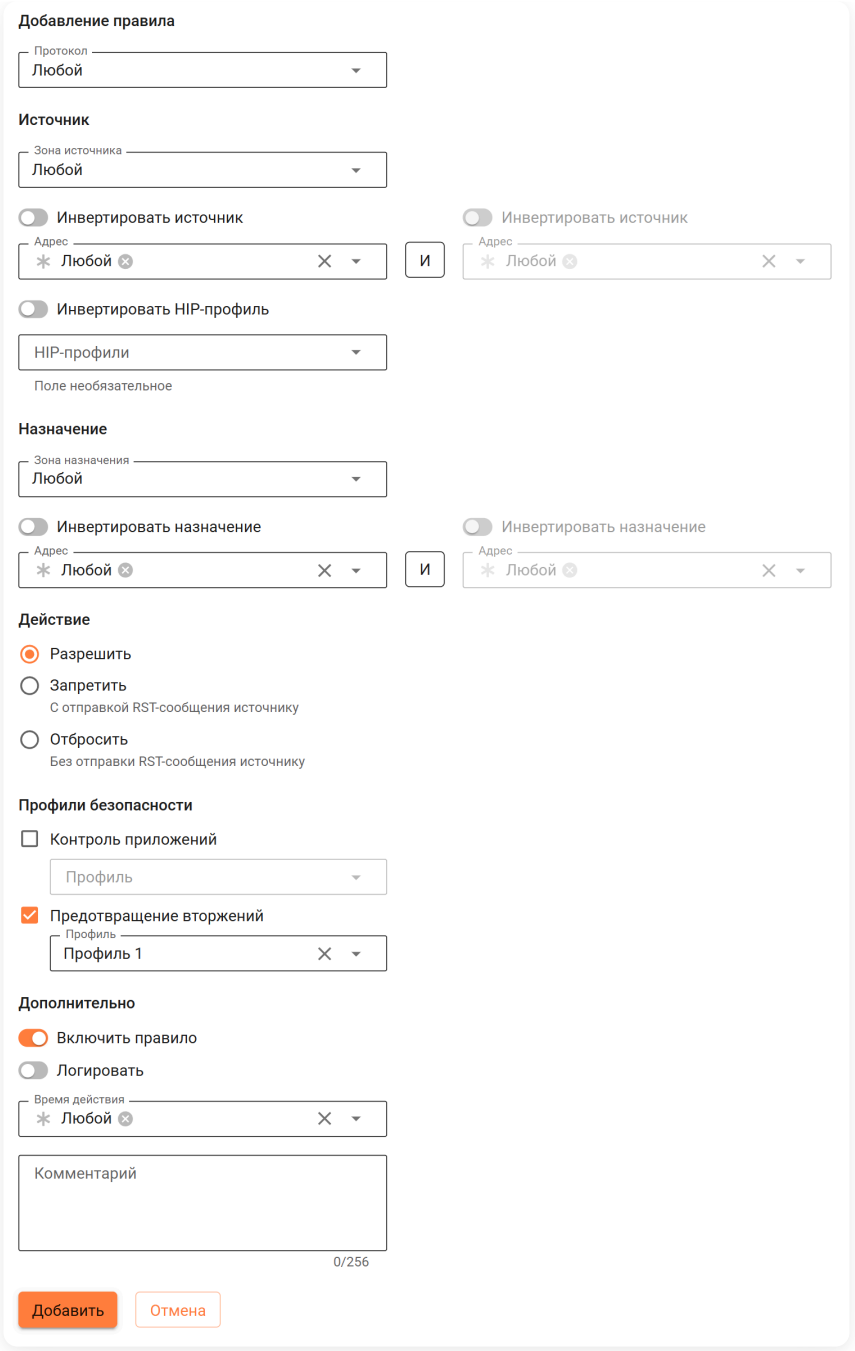
4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Добавление профилей в правила Межсетевого экрана

1. Перейдите в раздел **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать системой **Предотвращения вторжений**.
- **Источник** - выберите **Адрес**, **[Зону](*Зона)**, созданную в **Системном контексте**, и **HIP-профиль** источника трафика.
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика, созданную в **Системном контексте**.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Предотвращение вторжений** в блоке **Профили безопасности** и выберите необходимый профиль из раскрывающегося списка.

4. Включите правило и нажмите **Добавить**.

5. При включенной опции **Перехват пользовательских DNS-запросов** (по умолчанию опция включена) создайте правила **INPUT** с тем же профилем безопасности и портом 53 в разделе **Назначение** для протоколов TCP и UDP.

Полезные ссылки

- **Блокировка популярных ресурсов**

Профили Web Application Firewall

Классический VCE | Высокопроизводительный VCE | API

Название служб раздела **Профили Web Application Firewall**: `ideco-waf-backend`; `ideco-waf-event-syncer`.

Список служб для других разделов доступен по ссылке.

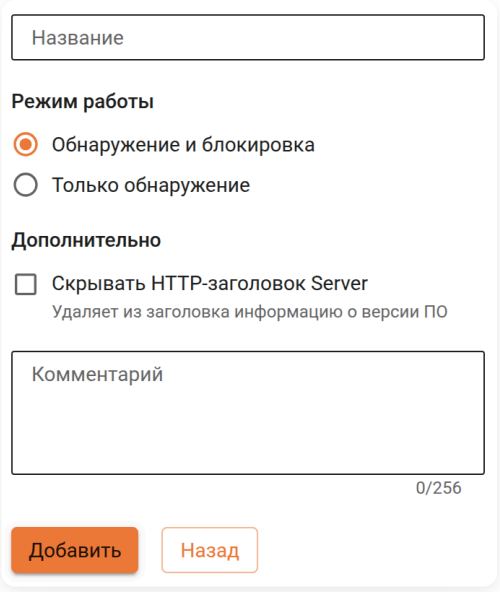
Использование WAF-профилей позволит настроить параметры защиты для опубликованного веб-ресурса. Профиль создается в **Профили безопасности → Web Application Firewall**.

Создание WAF-профилей не влияет на фильтрацию трафика. Чтобы включить фильтрацию, нужно использовать WAF-профили в разделе **Обратный прокси** при создании правила.

Создание профиля WAF

Для создания профиля WAF выполните действия:

1. Нажмите **Добавить** и заполните поля:

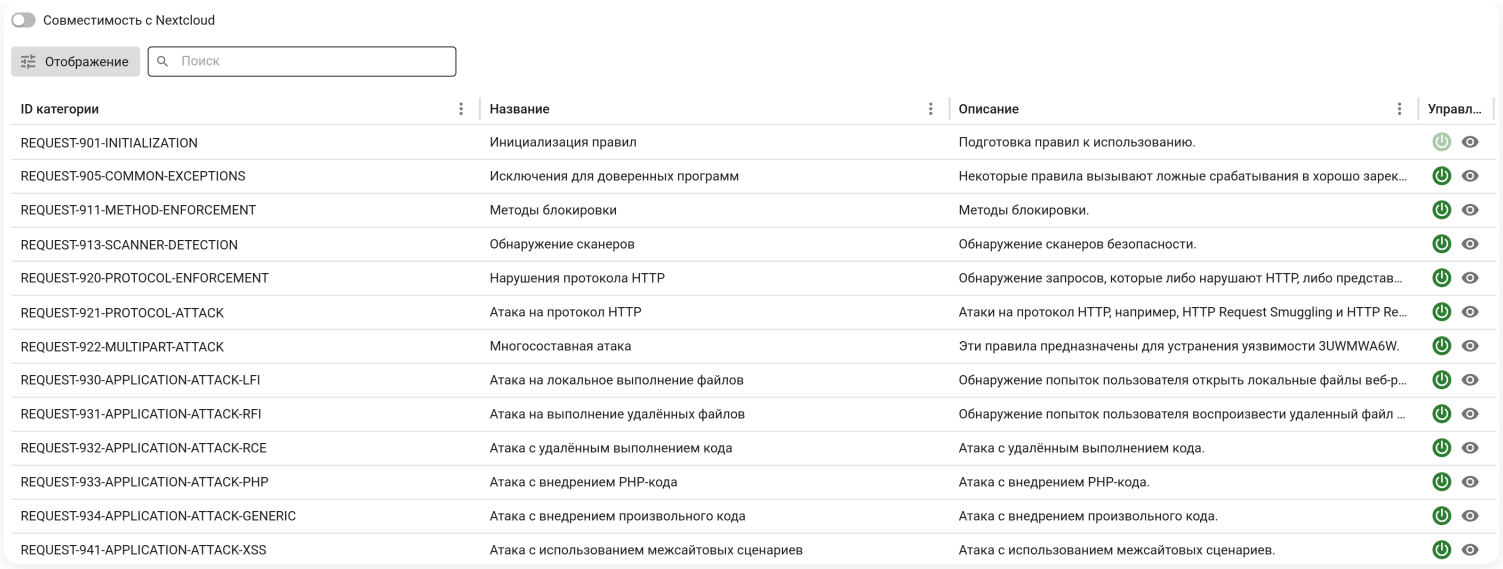


Расшифровка полей

- **Название** - введите название профиля.
- **Режим работы**:
  - **Обнаружение и блокировка** - подозрительные запросы будут блокироваться и логироваться WAF.
  - **Только обнаружение** - подозрительные запросы будут логироваться WAF, но не будут блокироваться.
- **Дополнительно**:
  - **Скрывать HTTP-заголовок Server** - позволяет скрыть данные, идентифицирующие сервер.
  - **Комментарий** - введите пояснение для профиля.

2. Нажмите **Добавить**.

3. На вкладке **Категории** включите или отключите правила:



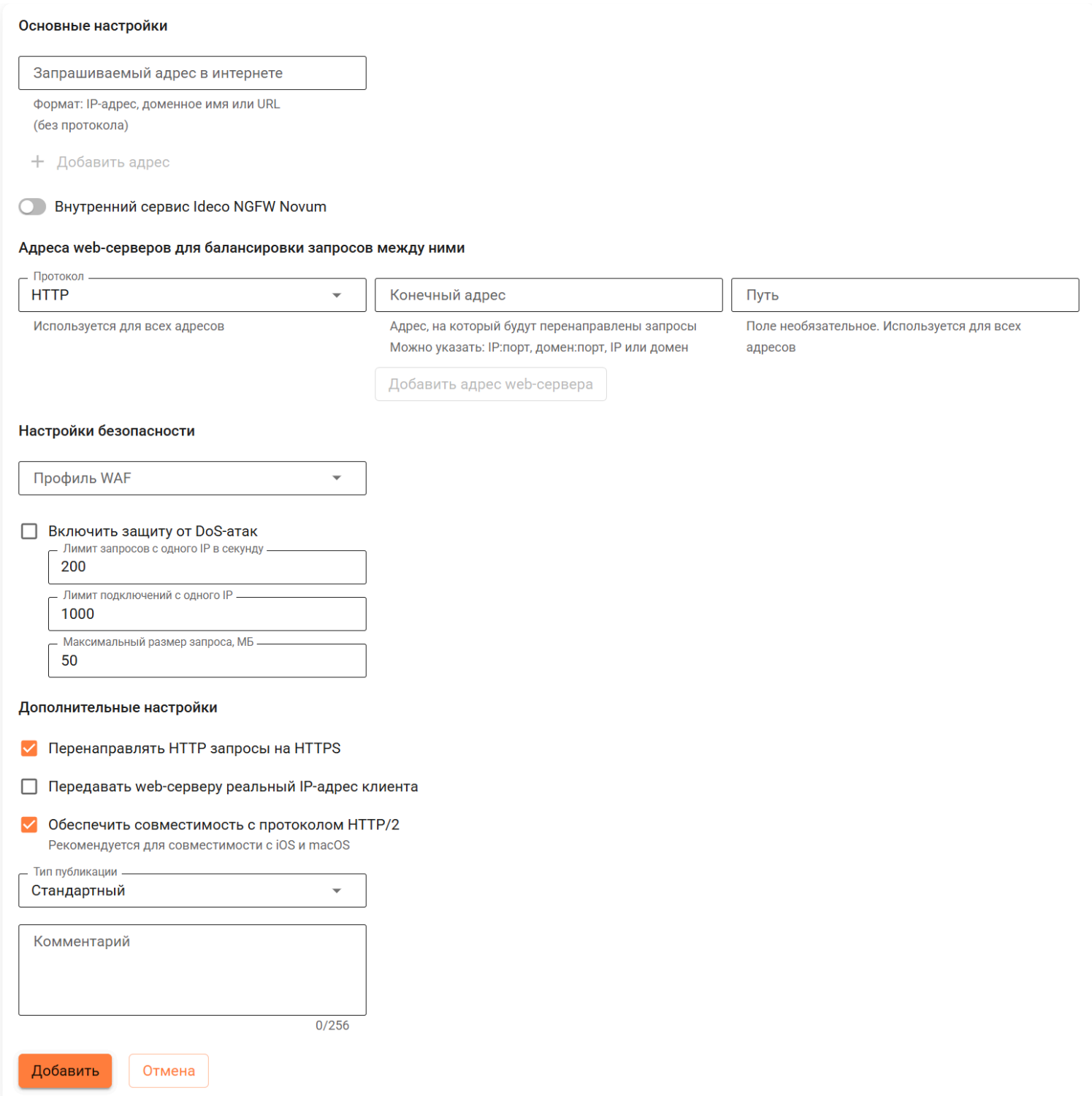
Если сервис Nextcloud работает за WAF, включите опцию **Совместимость с Nextcloud**:



Сигнатуры будут оптимизированы для определения атак на этот сервис. С выключенной опцией **Совместимость с Nextcloud** сервис может работать с ошибками.

Использование профиля WAF в правиле Обратного прокси

1. Перейдите в **Сервисы** → **Обратный прокси**, нажмите **Добавить** и заполните поля:



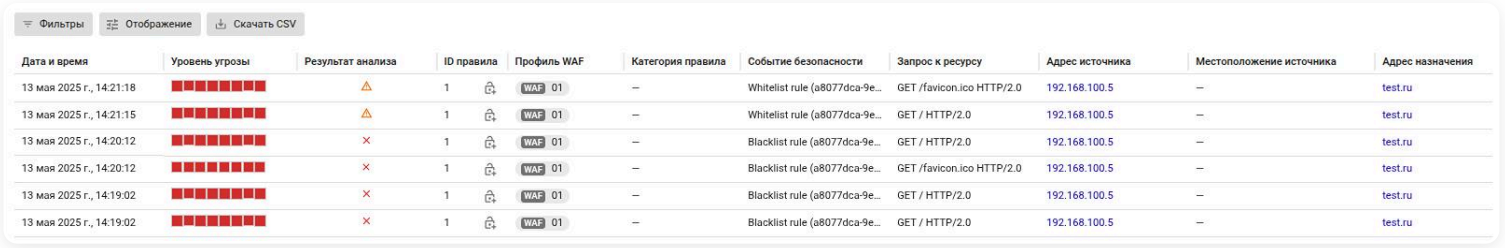
Расшифровка полей

- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных адресов нажмите кнопку **Добавить адрес**.
- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Конечный адрес** - адрес, на который будут перенаправлены запросы.
- **Путь** - поле необязательное и используется для всех адресов.
- **Профиль WAF** - выберите созданный ранее профиль WAF.
- **Перенаправлять HTTP-запросы на HTTPS** - включите настройку, если сайт работает по протоколу HTTPS. Позволяет автоматически переадресовывать пользователей с HTTP-версии.
- **Передавать web-серверу реальный IP-адрес клиента** - при необходимости включите настройку, чтобы публичный IP-адрес клиента при обратном проксировании не заменялся адресом NGFW Novum.

2. Нажмите **Добавить**.

Диагностика и добавление исключений

Срабатывание правил **Web Application Firewall** отображается в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**:



Добавить правило в исключение можно двумя способами:

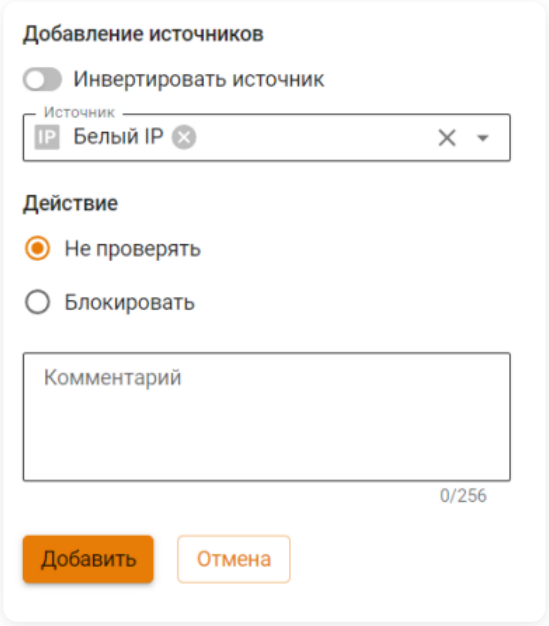
По IP-адресу

1. Перейдите в раздел **Профили Web Application Firewall** и у правила нажмите на .

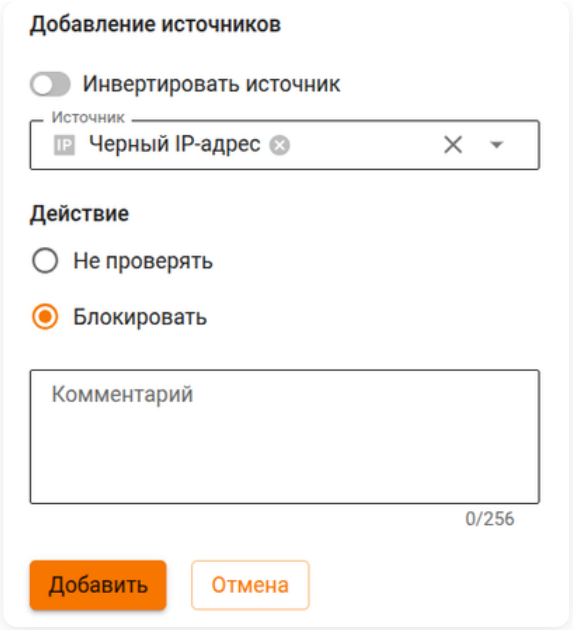
2. В **Белый и черный списки** нажмите **Добавить источник**:

> В каждый профиль WAF можно добавить не более двух тысяч источников в белых и черных списках.
> Если лимит будет превышен, появится сообщение в уведомлениях.

- Для добавления в белый список укажите необходимые IP-адреса и подсети, выберите действие **Не проверять**:



- Для добавления в черный список укажите необходимые IP-адреса и подсети, выберите действие **Блокировать**:



Исключения, добавленные в **Белый и черный списки**, логируются в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

По ID правила

Исключение добавляется двумя способами:

- На вкладке **Исключения**.
- На вкладке **Web Application Firewall**.

Не рекомендуем добавлять исключение по ID правила, так как из обработки исключатся все запросы, попадающие под исключенное правило.

На вкладке Исключения

1. Перейдите в раздел **Профили Web Application Firewall** и у правила нажмите на .

2. На вкладке **Исключения** нажмите **Добавить исключение** и укажите ID правила.

ID правила находится в журнале срабатывания правил в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

На вкладке Web Application Firewall

1. Перейдите в **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

2. Нажмите на в столбце ID правила.

Если описанные способы не помогли, обратитесь в Техническую поддержку.

Сохранение правил WAF при обновлении системы

Правила WAF, добавленные в основные файлы конфигурации, перезаписываются при обновлении Ideco NGFW Novum.

Чтобы пользовательские правила WAF сохранялись при обновлении, в Ideco NGFW Novum предусмотрены специальные файлы для пользовательских правил и исключений. Они позволяют встроиться в процесс обработки запроса до или после основных правил WAF:

- **Before-секция** - отключение определенных правил для конкретных IP-адресов или URL до того, как они сработают и заблокируют легитимный запрос (борьба с ложными срабатываниями).
- **After-секция** - добавление пользовательских проверок или изменение поведения системы после того, как стандартные правила отработали.

Пример внесения правил в after-секцию

Требуется, чтобы все срабатывания порогового правила `949110` приводили к ошибке `404`, а не к стандартному ответу CRS.

1. Создайте и откройте для редактирования файл `custom-waf.conf` в `/var/opt/ideco/reverse-backend/`:

```
nano /var/opt/ideco/reverse-backend/custom-waf.conf
```

2. Добавьте в файл необходимое правило. Например:

```
SecRuleUpdateActionById 949110 "t:none,deny,status:404"
```

- `t:none` - не применять трансформаций к данным;
- `deny` - при срабатывании правила заблокировать запрос;
- `status:404` - при блокировке передать клиенту HTTP-статус `404`.

3. Перезапустите службы `ideco-waf-backend`, `ideco-waf-event-syncer` и `ideco-reverse-backend`.

4. Убедитесь, что при срабатывании правила `949110` клиент получает статус ответа `404`.

Пример внесения правил в before-секцию

Требуется для трафика, у которого `Content-Type` начинается с `text/plain` при обращении к `url.path`, начинающемуся с `/api/v1/webhook`, исключить срабатывание правила `920420` и явно указать процессор обработки тела запроса.

1. Создайте и откройте для редактирования файл `custom-waf-before.conf` в `/var/opt/ideco/reverse-backend/`:

```
nano /var/opt/ideco/reverse-backend/custom-waf-before.conf
```

2. Добавьте в файл необходимое правило. Например:

```
SecRule REQUEST_HEADERS:Content-Type "@beginsWith text/plain" \
    "id:10001,\
    phase:1,\
    pass,\
    t:none,\
    nolog,\
    tag:'Custom_Exception',\
    ver:'Custom_Exceptions/1.0',\
    chain"
    SecRule REQUEST_URI "@rx ^/api/v1/webhook" \
        "t:none,\
        ctl:ruleRemoveById=920420,\
        ctl:requestBodyProcessor=JSON"
```

- `SecRule REQUEST_HEADERS:Content-Type "@beginsWith text/plain"` - условие срабатывания. Срабатывает, если `Content-Type` начинается с `text/plain` (например `text/plain; charset=utf-8`);
- `id:10001` - ID пользовательского правила;
- `phase:1` - проверка на фазе 1 (анализ заголовков запроса);
- `pass` - правило не блокирует, только выполняет свои действия (в том числе `ctl` из следующего звена `chain`);
- `t:none` - не применять трансформаций к данным;
- `nolog` - срабатывание этого правила не логируется;
- `tag:'Custom_Exception'`, `ver:'Custom_Exceptions/1.0'` - метки/версия для удобства в логах и управлении;
- `chain` - указывает, что это первое звено цепочки. Действия применяются, только если пройдет и следующее условие;
- `REQUEST_URI` - действие применяется к `url.path`, начинающемуся с `/api/v1/webhook`;
- `t:none` - не применять трансформаций к данным;
- `ctl:ruleRemoveById=920420` - для этого запроса отключается правило с ID `920420`;
- `ctl:requestBodyProcessor=JSON` - принудительно обрабатывает тело запроса как JSON.

3. Перезапустите службы: `ideco-waf-backend`, `ideco-waf-event-syncer` и `ideco-reverse-backend`.

4. Убедитесь в том, что запрос к `/api/v1/webhook` не блокируется правилами из основной базы.

Профили антивируса

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Профили антивируса**: `ideco-av-backend`.

Список имен служб для других разделов доступен по ссылке.

Антивирус в продукте использует технологию Kaspersky Anti-Virus Software Development Kit. Для включения модуля перейдите в **Профили безопасности → Антивирус**.

Опция **Профили антивируса** управляет только проверкой трафика в текущем контексте. Статус **Работает** отображает активность модуля **kav-scanner**, даже если **Антивирус** выключен во всех контекстах. В этом случае NGFW Novum не выполняет проверку трафика. Модуль **kav-scanner** работает всегда при наличии лицензии и ресурсов.

Антивирус приобретается отдельно от Ideco NGFW Novum, использование может быть ограничено условиями лицензии. Для покупки обратитесь в отдел продаж.

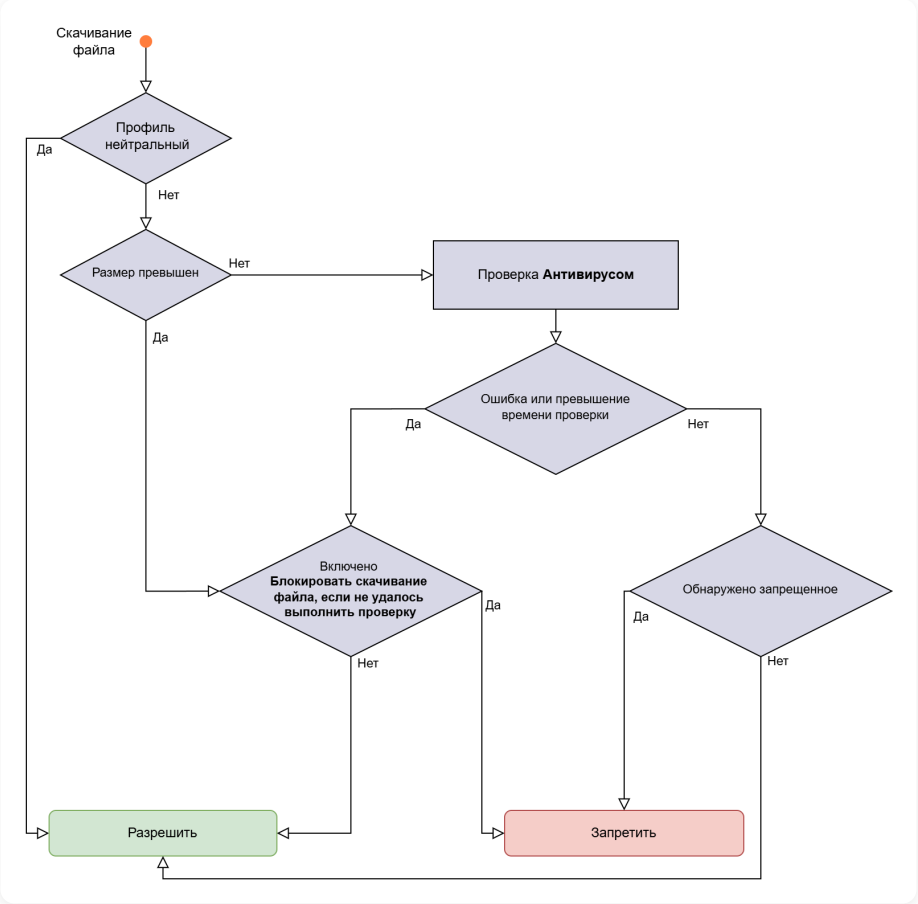
Корпоративные ключи, предназначенные для других продуктов Лаборатории Касперского, нельзя использовать для активации антивируса.

Антивирус связан с прокси-сервером и **Контент-фильтром** и фильтрует веб-трафик при выполнении следующих условий:

- В разделе **Контент-фильтр** настроена расшифровка веб-трафика. HTTPS-сайт проверяется только в случае расшифровки HTTPS-трафика **Контент-фильтром**. Рекомендации по настройке фильтрации HTTPS представлены в статье.
- Веб-ресурс не находится в списках исключений прокси-сервера по назначению.
- Пользователь, к которому поступает трафик, не добавлен в исключения прокси-сервера по источнику.

Для проверки трафика **Антивирусом** создайте правило в разделе **Контент-фильтр** и укажите нужный профиль антивируса. Если профиль не выбран, проверка будет выполняться с использованием профиля по умолчанию в блоке **Настройки**. Если профиль по умолчанию не выбран, проверка трафика не выполняется.

Схема работы профиля антивируса при проверке скачиваемого файла:

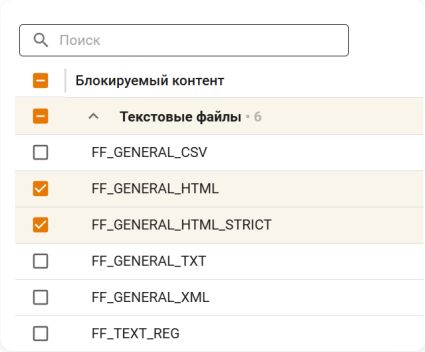


- **Профиль нейтральный** - профиль, в котором не включена блокировка ссылок, ПО и контента.

Результат проверки трафика **Антивирусом** представлен в разделе **Веб-трафик**.

Особенности работы Антивируса

- Ищет файлы заблокированных форматов в архивах. Если находит, то блокирует архив.
- Не блокирует некоторые типы файлов (например, CSV) без фиксированных байтов, используемых для определения типа файла (магических байтов). Все файлы, которые нельзя классифицировать по магическим байтам, Антивирус Касперского относит к TXT. Если необходимо блокировать подобные типы файлов, рекомендуем блокировку по расширению или по MIME-типу через Контент-фильтр.
- Блокирует веб-страницы, если в профиле Антивируса включена блокировка HTML-документов в **Текстовых файлах** и профиль выбран в правиле Контент-фильтра:



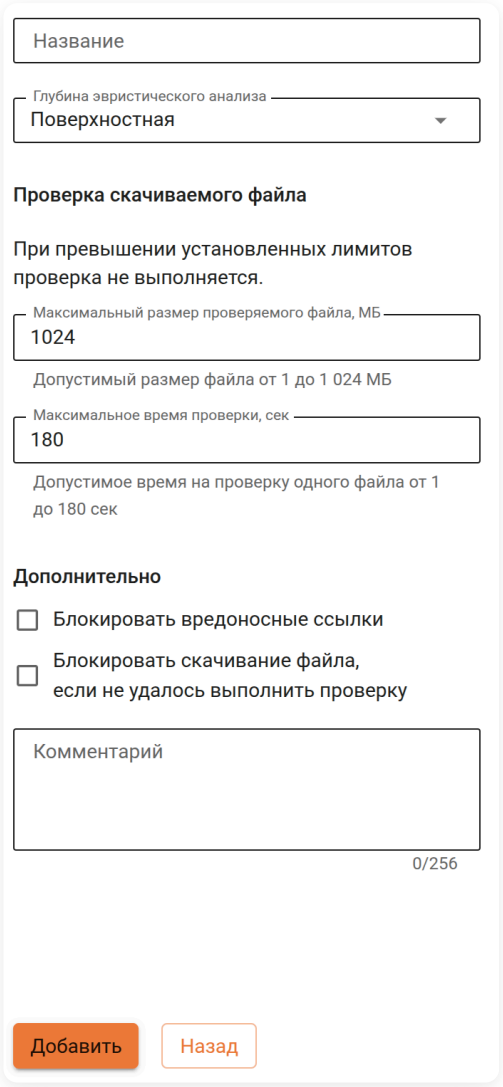
Если файл был загружен при выключенном **Антивирусе**, браузер (например, Google Chrome) может взять файл из кэша при повторной загрузке, минуя фильтрацию NGFW Novum.

Для восстановления антивирусной проверки необходимо очистить кэш браузера.

Профили

Для создания профиля выполните действия:

1. Нажмите **Добавить** и заполните поля на вкладке **Настройки**:



Расшифровка полей

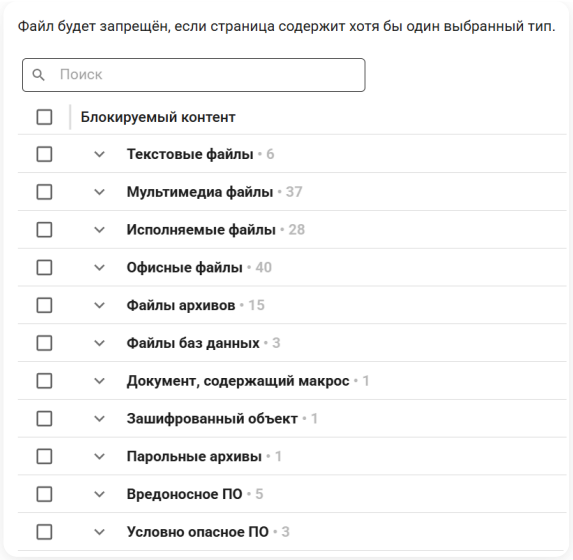
- **Название** - название профиля.
- **Глубина эвристического анализа** - степень обнаружения новых и неизвестных вредоносных программ:
  - **Не проводить проверку**.
  - **Поверхностная**.
  - **Средняя**.
  - **Глубокая**.
  - **Максимальная**.

Повышение уровня сканирования увеличивает глубину проверки, но потребует больше времени и системных ресурсов.

- **Проверка скачиваемого файла** - настройка проверки файлов. При превышении указанных лимитов проверка файлов не выполняется:
  - **Максимальный размер проверяемого файла, МБ** - максимальный объем проверяемого файла (от 1 до 1024 МБ).
  - **Максимальное время проверки, сек** - время на проверку одного файла (от 1 до 180 секунд).
- **Дополнительно:**
  - **Блокировать вредоносные ссылки** - проверка URL по базе вредоносных ссылок Web Malicious URL Filtering (WMUF).
  - **Блокировать скачивание файла, если не удалось выполнить проверку** - блокирование скачивания файла при превышении размера, времени проверки или обнаружении вредоносного контента. Если опция не включена, то файл будет пропущен без проверки.
  - **Комментарий** - произвольный текст. Не более 256 символов.

2. Нажмите **Добавить**.

3. Перейдите на вкладку **Блокировка по контенту** и укажите контент, который должен быть заблокирован:



Тип блокируемого контента

- **Документ, содержащий макрос** - объект, содержащий макросы Microsoft Office.
- **Зашифрованный объект** - объект, защищенный алгоритмом шифрования.
- **Парольные архивы** - запароленный архив.
- **Вредоносное ПО** - вредоносные инструменты, трояны, неопознанное вредоносное ПО высокой или средней опасности и другие категории, указанные в дереве классификации.
- **Условно опасное ПО** - рекламное ПО (Adware), порнографическое (Pornware) или потенциально опасное (Riskware), указанное в дереве классификации.

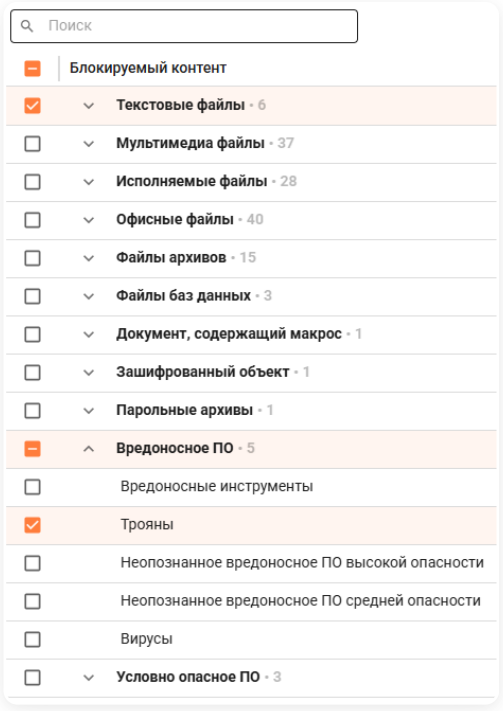
Тип блокируемого контента в файловом формате (**Файлы архивов**, **Исполняемые файлы**, **Мультимедиа файлы**, **Офисные файлы**, **Текстовые файлы**, **Файлы баз данных**, **Файлы веб-архивов**) и **Прочие форматы** указаны в статье.
При настройке блокировки применяется логика **ИЛИ**:

- Если выбрано одно значение, блокируется только трафик с указанным типом.
- Если выбрано несколько значений, блокируется трафик, содержащий любой из выбранных типов или сочетание типов.

Примеры блокировки контента

Пример 1. В профиле выбрана категория **Текстовые файлы**. Результат: будет заблокирован тип контента **Текстовые файлы**.

Пример 2. В профиле выбраны категории **Текстовые файлы** и **Трояны**:

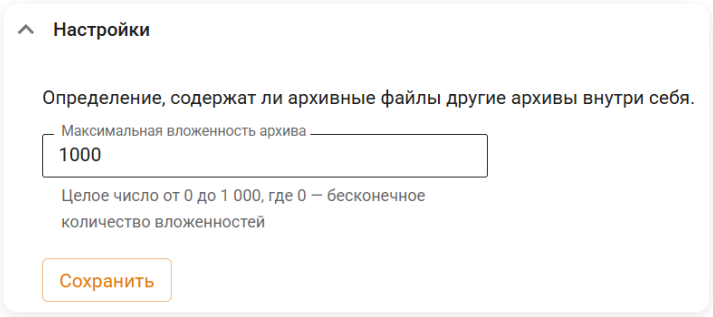


Будут блокироваться три типа контента:

- **Текстовые файлы**.
- **Трояны**.
- **Текстовые файлы**, содержащие **Трояны**.

4. Для подтверждения создания профиля нажмите **Сохранить**.

На вкладке **Основное** можно настроить **Максимальную вложенность архива**:



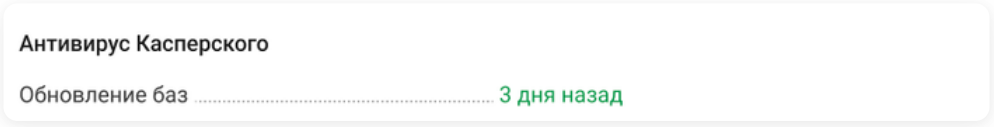
В поле укажите целое число от `0` до `1000`, где `0` - бесконечное количество вложенностей (`0` указано по умолчанию). Для запрета вложенных архивов укажите в поле значение `1`.

> Если включена опция **Блокировать скачивание файла**, попытка скачать архив с превышением указанной вложенности будет заблокирована.

Функция проверки вложенности не работает с запароленными архивами, которые можно заблокировать при создании профиля на вкладке **Блокировка по контенту**.

Обновление баз

На вкладке можно посмотреть информацию о последнем обновлении баз антивируса Касперского:



Проверка работы антивируса

Попробуйте скачать тестовые файлы с сайта: https://www.eicar.org/download-anti-malware-testfile.

В случае правильной настройки браузер выведет ошибку доступа:

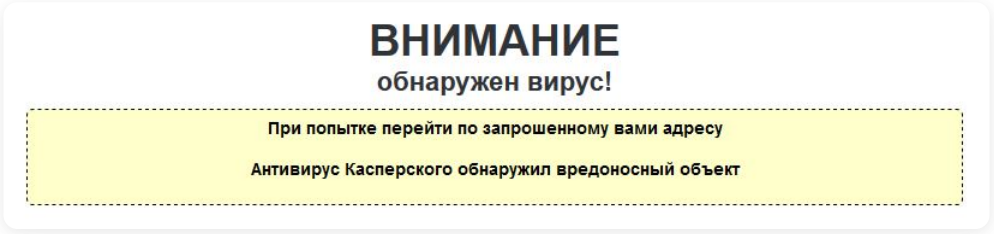


Таблица с описанием типов блокируемого контента модуля Антивирус

Таблица с описанием типов блокируемого контента, обрабатываемых модулем Антивирус:

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Текстовые файлы		FF_GENERAL_CSV	Comma-separated Values	csv	text/csv
Текстовые файлы		FF_GENERAL_HTML	HyperText Markup Language or fragments of HTML	htm; html	text/html
Текстовые файлы		FF_GENERAL_HTML_STRICT	HyperText Markup Language standalone document (generally with doctype or html tags)	htm; html	text/html
Текстовые файлы		FF_GENERAL_TXT	Plain Text	txt	text/plain
Текстовые файлы		FF_GENERAL_XML	Extensible Markup Language (XML)	xml	text/xml; a
Текстовые файлы		FF_TEXT_REG	Windows registry editor script	reg	
Мультимедиа файлы	Audio	FF_AUDIO_AAC	Advanced Audio Coding	aac; m4a	audio/aac
Мультимедиа файлы	Audio	FF_AUDIO_AC3	AC3 multichannel audio	ac3	audio/ac3
Мультимедиа файлы	Audio	FF_AUDIO_APE	Monkey' s Audio (APE)	ape	audio/x-m ape
Мультимедиа файлы	Audio	FF_AUDIO_CDA	CD digital Audio	cda	applicatio
Мультимедиа файлы	Audio	FF_AUDIO_FLAC	Free Lossless Audio Codec (FLAC)	flac	audio/x-fla
Мультимедиа файлы	Audio	FF_AUDIO_MIDI	MIDI	mid; midi	audio/mid
Мультимедиа файлы	Audio	FF_AUDIO_MKA	Matroska Audio	mka	audio/x-m
Мультимедиа файлы	Audio	FF_AUDIO_MP3	MPEG-1 Layer 3	mp3	audio/x-m audio/mpe audio/x-m
Мультимедиа файлы	Audio	FF_AUDIO_OGG	OGG Vorbis Audio	ogg	audio/x-og
Мультимедиа файлы	Audio	FF_AUDIO_RA	RealAudio	rm; ra; ravb	audio/vnd
Мультимедиа файлы	Audio	FF_AUDIO_WAV	Microsoft Wave	wav	audio/x-wa

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Мультимедиа файлы	Audio	FF_AUDIO_WEB_M	WebM Audio	webm; weba	audio/web
Мультимедиа файлы	Audio	FF_AUDIO_WMA	Windows Media Audio	wma	
Мультимедиа файлы	Image	FF_IMAGE_BMP	Windows Bitmap (DIB)	bmp	image/bm
Мультимедиа файлы	Image	FF_IMAGE_CDR	Corel Draw	cdr	
Мультимедиа файлы	Image	FF_IMAGE_EMF	Windows Meta-File	emf; wmf	
Мультимедиа файлы	Image	FF_IMAGE_EPS	Post-Script Format	eps	applicatio
Мультимедиа файлы	Image	FF_IMAGE_GIF	GIF	gif	image/gif
Мультимедиа файлы	Image	FF_IMAGE_JPEG	JPEG/JFIF	jpg; jpe; jpeg; jff	image/jpe
Мультимедиа файлы	Image	FF_IMAGE_PNG	Portable Graphics	png	image/png
Мультимедиа файлы	Image	FF_IMAGE_PSD	Adobe Photoshop	psd	
Мультимедиа файлы	Image	FF_IMAGE_TIFF	Targa Image File Format	tif; tiff	image/tif;
Мультимедиа файлы	Image	FF_IMAGE_WEBP	WebP	webp	image/we
Мультимедиа файлы		FF_MULTIMEDIA_SWF	ShockWave Flash	swf	applicatio
Мультимедиа файлы	Video	FF_VIDEO_3GPP	MPEG4 ISO format	3gp; 3g2; 3gp2; 3p2	
Мультимедиа файлы	Video	FF_VIDEO_ASF	Microsoft Container	asf; wmv	video/x-m
Мультимедиа файлы	Video	FF_VIDEO_AVI	Audio/Video Interleave	avi	video/avi;
Мультимедиа файлы	Video	FF_VIDEO_BIK	Bink Video	bik	
Мультимедиа файлы	Video	FF_VIDEO_DIVX	MPEG4	divx; mp4; m4v	video/mp4
Мультимедиа файлы	Video	FF_VIDEO_F4V	f4v	f4v	video/x-flv
Мультимедиа файлы	Video	FF_VIDEO_FLV	Adobe Flash Video	flv	video/x-flv
Мультимедиа файлы	Video	FF_VIDEO_MKV	Matroska Video	mkv	video/x-m
Мультимедиа файлы	Video	FF_VIDEO_MOV	Apple Quicktime	mov; qt	video/quic
Мультимедиа файлы	Video	FF_VIDEO_RM	RealMedia CB/VB	rm; rmvb	video/vnd
Мультимедиа файлы	Video	FF_VIDEO_RTMP	Real Time Messaging Protocol Message		applicatio
Мультимедиа файлы	Video	FF_VIDEO_VOB	MPEG1 (VCD) / MPEG2 (DVD) format	vob; dat; mpg; mpeg	video/mpe
Мультимедиа файлы	Video	FF_VIDEO_WEB_M	WebM Video	webm	video/web
Исполняемые файлы	Executable	FF_EXECUTABLE_APK	Android Application Package	apk	applicatio

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Исполняемые файлы	Executable	FF_EXECUTABLE_APPLE_SCRIPT	AppleScript Files	scpt; AppleScript	
Исполняемые файлы	Executable	FF_EXECUTABLE_BAT	Command Line Script	cmd; bat	applicatio
Исполняемые файлы	Executable	FF_EXECUTABLE_COM	COM - MS-DOS Application	com	
Исполняемые файлы	Executable	FF_EXECUTABLE_DEB	Debian Software Package	deb	applicatio
Исполняемые файлы	Executable	FF_EXECUTABLE_DEX	Dalvik Executable Format	dex; odex	
Исполняемые файлы	Executable	FF_EXECUTABLE_DOS	"DOS	Win-16	OS/2 - all
Исполняемые файлы	Executable	FF_EXECUTABLE_DOS_NE_RESOURCE	"DOS	Win-16	OS/2 - NE
Исполняемые файлы	Executable	FF_EXECUTABLE_ELF	Executable and Linkable Format	o; so; elf; prx	
Исполняемые файлы	Executable	FF_EXECUTABLE_JAVA	Java Class File	class	
Исполняемые файлы	Executable	FF_EXECUTABLE_JS	JavaScript	js	text/javas
Исполняемые файлы	Executable	FF_EXECUTABLE_MACHO	Mach object file format	; o; dylib	
Исполняемые файлы	Executable	FF_EXECUTABLE_MSI	Microsoft Installer Archive	msi	
Исполняемые файлы	Executable	FF_EXECUTABLE_PYC	Python Bytecode	pyc; pyo	
Исполняемые файлы	Executable	FF_EXECUTABLE_RPM	RPM Package	rpm	applicatio
Исполняемые файлы	Executable	FF_EXECUTABLE_SCRIPTS	Unix Scripts	sh; pl	
Исполняемые файлы	Executable	EFF_XECUTABLE_VBS	Visual Basic Script	vbs; vb	text/vbscri
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE	Win32 PE	exe; dll; ocx; scr	applicatio msdownlo vms/exe;
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_DLL	Win32 PE Dynamic Library	dll; ocx; scr	applicatio msdownlo
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_EXE	Win32 PE Executable File	exe	applicatio applicatio
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_EXEUI	Win32 PE Executable File for Windows GUI/CUI and POSIX Subsystems	exe	applicatio applicatio
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_ILLIBRARY	Win32 PE .Net IL Library	exe; dll; ocx; scr	applicatio msdownlo
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_ILONLY	Win32 PE .Net IL (Only)	exe; dll; ocx; scr	applicatio msdownlo
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_NET	Win32 PE .Net	exe; dll; scr	applicatio msdownlo

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Исполняемые файлы	.Net	FF_EXECUTABLE_WIN32PE_NET_RESOURCE_WITH_POSSIBLE_TRIVIAL_CODE	Win32 PE .Net Resource Only Library (May contain trival code)	dll	application msdownlo
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_RESOURCE	Win32 PE Resource Only Library	dll	application msdownlo
Исполняемые файлы	Windows	FF_EXECUTABLE_WIN32PE_SYS	Win32 PE File for Native Subsystem	sys	application
Исполняемые файлы	Windows	FF_EXECUTABLE_WINDOWS_SHELLLINK	MS Windows shell links	lnk	
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOC	Microsoft Word Document 97-2003	doc	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOCM	Microsoft Word Macro-Enabled Document	docm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOCX	Microsoft Word Document	docx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOT	Microsoft Word Template 97-2003	dot	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOTM	Microsoft Word Macro-Enabled Template	dotm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_DOTX	Microsoft Word Template	dotx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_POTM	Microsoft PowerPoint Macro-Enabled Template	potm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_POTX	Microsoft PowerPoint Template	potx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPSM	Microsoft PowerPoint Macro-Enabled Slide Show	ppsm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPSX	Microsoft PowerPoint Slide Show	ppsx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPT	Microsoft PowerPoint Presentation 97-2003	ppt; pot; pps	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPTM	Microsoft PowerPoint Macro-Enabled Presentation	pptm	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PPTX	Microsoft PowerPoint Presentation	pptx	application officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_PUB	Microsoft Publisher Document	pub	application
Офисные файлы	Microsoft Office	FF_MSOFFICE_SCRAP	Microsoft Shell Scrap Object	shs; shb	

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLAM	Microsoft Excel Macro-Enabled Add-in	xlam	applicatio
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLS	Microsoft Excel Document 97-2003	xsl	applicatio
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLSB	Microsoft Excel Binary Document	xlsb	applicatio
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLSM	Microsoft Excel Macro-Enabled Document	xlsm	applicatio officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLSX	Microsoft Excel Document	xlsx	applicatio officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLTM	Microsoft Excel Macro-Enabled Template	xltm	applicatio officedocu
Офисные файлы	Microsoft Office	FF_MSOFFICE_XLTX	Microsoft Excel Template	xltx	applicatio officedocu
Офисные файлы		FF_OFFICE_EML	Outlook Express Message	eml	message/
Офисные файлы		FF_OFFICE_MSG	Microsoft Outlook Message	msg	applicatio
Офисные файлы		FF_OFFICE_MSOFFICE	MS Office documents	doc; xls; ppt; dot; pot	applicatio applicatio applicatio
Офисные файлы		FF_OFFICE_MSOFFICE_MACRO	Office 2007 macro enabled docs	docm; xlsm; pptm; ppsm; dotm	applicatio
Офисные файлы		FF_OFFICE_ODP	OpenDocument Presentation	odp	applicatio
Офисные файлы		FF_OFFICE_ODS	OpenDocument Spreadsheet	ods	applicatio
Офисные файлы		FF_OFFICE_ODT	OpenDocument Text	odt	applicatio
Офисные файлы		FF_OFFICE_ONE	Microsoft OneNote Document	one	applicatio
Офисные файлы		FF_OFFICE_ONEPKG	Microsoft OneNote Package	onepkg	applicatio
Офисные файлы		FF_OFFICE_OPENXML	Open XML documents	docx; xlsx; pptx; dotx; potx	applicatio ***applicatio*** excel*; ap applicatio
Офисные файлы		FF_OFFICE_PDF	Adobe Acrobat	pdf	applicatio
Офисные файлы		FF_OFFICE_PST	MS Outlook Personal Folders	pst; ost	applicatio
Офисные файлы		FF_OFFICE_RTF	Rich Text Format	rtf	text/rtf; ap
Офисные файлы		FF_OFFICE_SXW	OpenOffice.org 1.0 Writer Document	sxw	applicatio
Офисные файлы		FF_OFFICE_VDX	Microsoft Visio Drawing XML	vdx; vsx; vtx	applicatio

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Офисные файлы		FF_OFFICE_VSD	Microsoft Visio Diagram	vsd; vss; vst	applicatio
Офисные файлы		FF_OFFICE_XPS	Open XML Paper Specification	xps; oxps	applicatio xpsdocum
Офисные файлы		FF_OFFICE_XSN	Microsoft InfoPath Template Form	xsn	applicatio
Файлы архивов		FF_ARCHIVE_ARJ	Arj archive	arj	applicatio
Файлы архивов		FF_ARCHIVE_7Z	7-zip archive	7z*; 7-z	
Файлы архивов		FF_ARCHIVE_ACE	ACE archive	ace	applicatio
Файлы архивов		FF_ARCHIVE_BZIP2	BZIP2 archive	bz; bz2; tbz; tbz2	applicatio
Файлы архивов		FF_ARCHIVE_CAB	Windows Cabinet	cab	
Файлы архивов		FF_ARCHIVE_DMG	Apple Disk Image	dmg; smi; img	applicatio
Файлы архивов		FF_ARCHIVE_GZIP	Gzip archive	gz; tgz	applicatio
Файлы архивов		FF_ARCHIVE_ISO	ISO-9660 CD Disk	iso	
Файлы архивов		FF_ARCHIVE_JAR	Java (ZIP) archive	jar	
Файлы архивов		FF_ARCHIVE_LZIP	Lzip archive	lz	applicatio
Файлы архивов		FF_ARCHIVE_RAR	RAR archive	rar	
Файлы архивов		FF_ARCHIVE_TAR	Tar archive	tar	applicatio
Файлы архивов		FF_ARCHIVE_XAR	Extensible archive format	xar	
Файлы архивов		FF_ARCHIVE_Z	Z (compress) archive	Z	applicatio
Файлы архивов		FF_ARCHIVE_ZIP	ZIP archive	zip	applicatio
Файлы баз данных		FF_DATABASE_ACCDB	Microsoft Access Database	accdb; accde; accdr	applicatio
Файлы баз данных		FF_DATABASE_ACCDC	Microsoft Access Signed Package	accdc	applicatio
Файлы баз данных		FF_DATABASE_MDB	Microsoft Access 2003 Database	mdb	applicatio
Документ, содержащий макрос		OFFICE_MSOFFICE_MACRO	Office 2007 macro enabled docs	docm; xlsm; pptm; ppsm; dotm	applicatio
Зашифрованный объект		ENCRYPTED	Файл с примененным шифрованием, содержимое недоступно без ключа/ пароля		applicatio
Парольные архивы		PASSWORD_PROTECTED_ARCHIVE	Архив, защищенный паролем	zip; rar; 7z; ace; arj; cab; dmg; gz; iso; jar; tar	applicatio applicatio compress
Вредоносное ПО		Вредоносные инструменты			
Вредоносное ПО		Трояны			

Категория	Подкатегория	Тип угрозы	Описание	Расширение	MIME-тип
Вредоносное ПО		Неопознанное вредоносное ПО высокой опасности			
Вредоносное ПО		Неопознанное вредоносное ПО средней опасности			
Вредоносное ПО		Вирусы			
Условно опасное ПО		Рекламное (Adware)			
Условно опасное ПО		Порнографическое (Pornware)			
Условно опасное ПО		Потенциально опасное (Riskware)			

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Сервисы

В разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

Сетевые интерфейсы

Настройка сетевых интерфейсов, поддерживаемых Ideco NGFW

Перейти >

IGMP Proxy

IGMP Proxy позволяет принимать мультикаст-трафик от провайдера

Перейти >

Прокси

Настройка прозрачного проксирования веб-трафика в локальной сети

Перейти >

Обратный прокси

Настройка публикация веб-ресурсов локальной сети таким образом, чтобы веб-ресурсы стали доступны потребителям из сети интернет

Перейти >

ЛК/Портал SSL VPN

Настройка личного кабинета пользователя в Ideco NGFW (публикация и управление доступом пользователей)

Перейти >

DNS

Сервер DNS преобразует человекочитаемые имена серверов в IP-адреса. В состав Ideco NGFW входит DNS-сервер, не требующий дополнительной настройки в большинстве случаев.

Перейти >

DHCP-сервер

Настройка DHCP-сервера для автоматического назначения IP-адресов сетевым устройствам в локальной сети

Перейти >

NTP-сервер

Настройка NTP-сервера для синхронизации времени

Перейти >

IPsec

Настройка подключений с помощью защищенного протокола IPsec

Перейти >

ГОСТ VPN

Настройка ГОСТ VPN для соединения двух устройств NGFW

Перейти >

Сертификаты

Создание, загрузка и управление SSL-сертификатами

Перейти >

USB-токены

Настройка USB-токенов для использования на Ideco NGFW

Перейти >

Netflow

В статье описана настройка экспорта статистики трафика на коллектор во внешней или локальной сети по протоколу Netflow.

Перейти >

Syslog

Настройка передачи системных сообщений (syslog) Ideco NGFW в сторонние коллекторы или в SIEM-системы

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

Сетевые интерфейсы

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Сетевые интерфейсы**: `ideco-l2-manager`, `ideco-local-menu`, `ideco-l2manager-rest`, `ideco-l2manager-l2migration`, `ideco-l2manager-dhclient`, `ideco-l2manager-backend`.

Список имен служб для других разделов доступен по ссылке.

Для создания сетевых интерфейсов воспользуйтесь статьями:

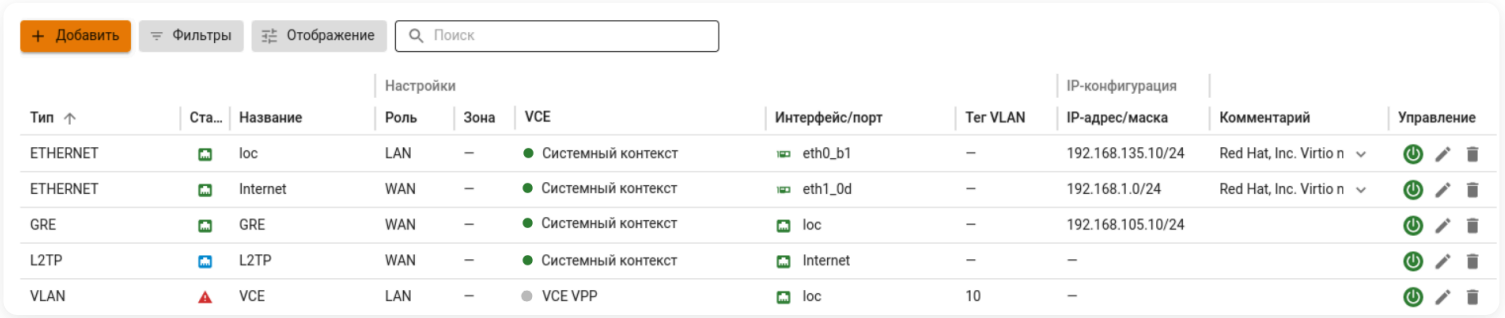
- **Интерфейсы**
- **Физические порты**

Интерфейсы можно создавать и редактировать только в **Системном контексте**. В других контекстах таблица интерфейсов доступна только для чтения.

Возможность передавать в VCE VPP отдельные порты сетевой карты зависит от модели сетевого адаптера:

- Если адаптер поддерживает разделение портов, порты можно передавать по отдельности.
- Если адаптер не поддерживает разделение портов, в VCE VPP необходимо передавать все порты сетевой карты. Иначе интерфейсы этой сетевой карты работать не будут.

Все созданные интерфейсы представлены в виде таблицы:



Статусы соединения

- Подключен

- Подключение

- Не подключен

- Статус неизвестен

Статусы VCE

- Работает

- Выключен

Редактирование сетевых интерфейсов

Интерфейсы можно редактировать, нажав , или удалить, нажав . Удалить интерфейс невозможно, пока на его основе созданы другие.

При создании, редактировании или удалении сетевого интерфейса перевыпускается **SSL-сертификат**, поэтому вероятно снижение скорости работы веб-интерфейса Ideco NGFW Novum. В этом случае рекомендуем нажать **F5**.

Ограничения сетевых интерфейсов

Максимальное количество сетевых интерфейсов, которое может обработать модуль **Ограничение скорости**:

- До 8 ГБ - **14 интерфейсов**.
- От 8 до 16 ГБ - **33 интерфейса**.
- 16 ГБ и более - **66 интерфейсов**.

Интерфейсы

Функциональность доступна в **Классическом** и **Системном контекстах**.

Интерфейсы соединяют устройство пользователя с различными сетевыми сегментами и определяют, как и для чего будут использоваться физические или виртуальные порты.

С версии 21 Ideco NGFW Novum у интерфейсов появились роли:

- **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.

Интерфейс **Control Plane** не обязателен - NGFW Novum можно администрировать и через LAN.

Однако для повышения безопасности рекомендуется ограничить доступ по **LAN** в правилах **Межсетевого экрана** (таблица INPUT, TCP 8443) и использовать для управления только интерфейс **Control Plane**.

- **LAN** – используется для создания локальных интерфейсов.

Для работы служб, зависящих от наличия локального интерфейса (например, **Прокси**), необходим хотя бы один сетевой интерфейс с ролью **LAN**.

- **WAN** – используется для подключения к провайдеру.

Памятка по частным IP-адресам IPv4

Согласно документу RFC 1918, для частных сетей зарезервированы следующие диапазоны адресов IPv4:

- **10.0.0.0/8** IP-адреса: `10.0.0.0 – 10.255.255.255`.
- **172.16.0.0/12** IP-адреса: `172.16.0.0 – 172.31.255.255`.
- **192.168.0.0/16** IP-адреса: `192.168.0.0 – 192.168.255.255`.

Сети, созданные в указанных диапазонах IP-адресов, для NGFW Novum считаются локальными и не подлежат публичной маршрутизации в интернете. Для настройки интерфейсов перейдите в **Сервисы** → **Сетевые интерфейсы**.

Основные интерфейсы

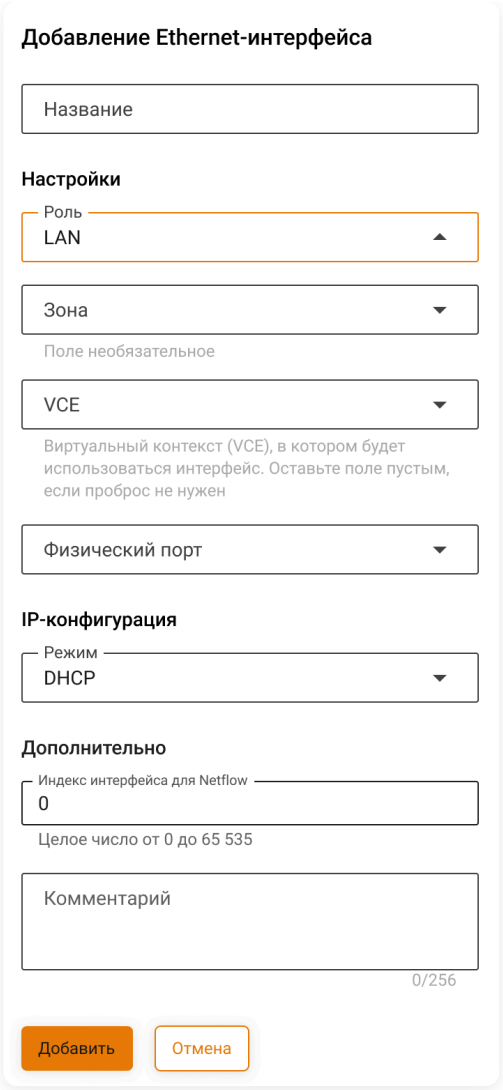
Ethernet

Ethernet - базовая технология проводных сетей, обеспечивающая передачу данных между устройствами. Технология поддерживает как прямое соединение устройств, так и работу через коммутаторы, обеспечивая гибкость и масштабируемость сетевой инфраструктуры.

Для настройки Ethernet-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Ethernet**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для подключения к провайдеру.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Физический порт** - порт на сетевом адаптере, который будет использоваться в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. Ethernet-интерфейс появится в таблице интерфейсов.

VLAN

VLAN (Virtual Local Area Network) - виртуальный сетевой интерфейс, позволяющий создавать и настраивать логические сегменты сети поверх существующей физической инфраструктуры. Данная технология дает возможность эффективно разделять сетевой трафик и организовывать изолированные сетевые сегменты в рамках единой сетевой структуры.

VLAN-интерфейс создается поверх родительского интерфейса и помечает все исходящие пакеты соответствующим тегом.

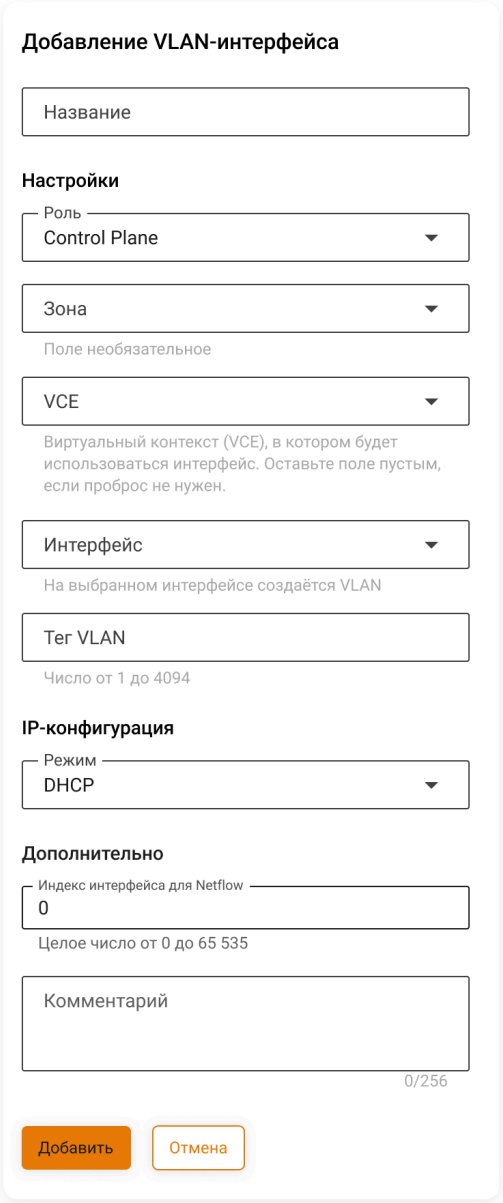
Различия в работе с VCE VPP и NGFW:

- В VCE NGFW можно передать VLAN-интерфейс, не передавая родительский интерфейс: VLAN-интерфейс конфигурируется, если родительский интерфейс отсутствует в контексте.
- В VCE VPP можно передать VLAN-интерфейс, только передав родительский интерфейс: VLAN-интерфейс не конфигурируется, если родительский интерфейс отсутствует в контексте.

Для настройки VLAN-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **VLAN**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для подключения к провайдеру.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.

- **Интерфейс** - родительский интерфейс, на базе которого создается VLAN-интерфейс: физический или агрегированный сетевой интерфейс, через который передается трафик данного VLAN. Доступные варианты: **Ethernet** и **LACP**.
- **Тег VLAN** - числовой идентификатор VLAN (от 1 до 4094), которым помечаются все пакеты VLAN-интерфейса.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. VLAN-интерфейс появится в таблице интерфейсов.

> **Как обрабатываются теги VLAN**
>
> Когда на сетевой интерфейс NGFW Novum приходит кадр с тегом соответствующего VLAN, тег снимается. NGFW Novum анализирует адрес назначения в IP-пакете и отправляет пакет в сетевой интерфейс согласно таблице маршрутизации. При отправке в кадр добавляется тег исходящего сетевого интерфейса (если он задан).
>
> Далее кадр передается на устройство на другом конце кабеля, например, на коммутатор. В зависимости от конфигурации VLAN на коммутаторе кадр либо передается без изменений, либо помещается в Native VLAN (его можно изменить).

LACP

LACP (Link Aggregation Control Protocol) - протокол агрегации каналов, предназначенный для объединения нескольких физических портов в единый логический интерфейс. Основное применение LACP заключается в увеличении общей пропускной способности канала и обеспечении его отказоустойчивости.

> Не рекомендуем использовать **LACP** на виртуальных сетевых адаптерах, так как системы виртуализации некорректно обрабатывают работу **LACP** на таких интерфейсах или вовсе не поддерживают этот режим.

Особенности работы LACP-интерфейсов:

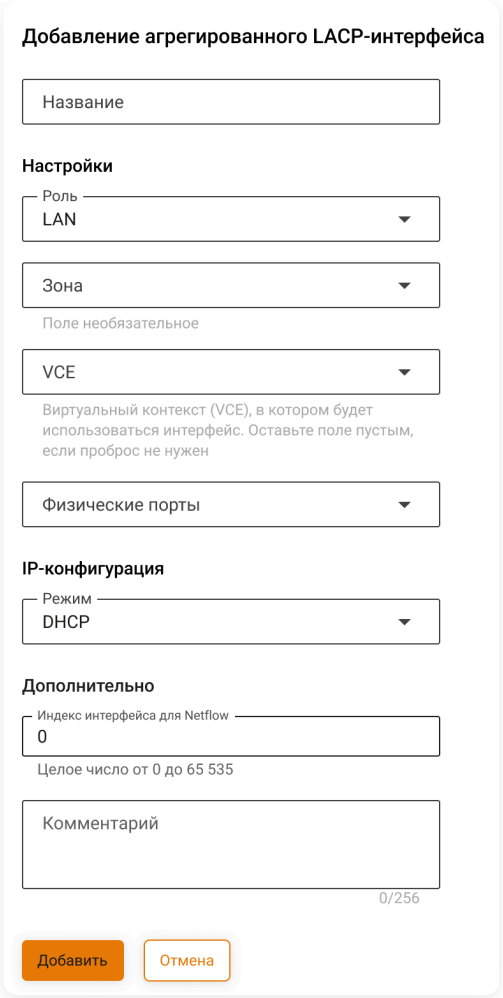
- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active**-режим - постоянная рассылка LACP пакетов.
- Используется режим вычисления хеша для распределения трафика **xmit_hash_policy layer2+3**.
- Проверка соседства осуществляется в режиме **fast** - каждую секунду.
- Количество физических портов, объединяемых в агрегированный интерфейс, не ограничено со стороны NGFW Novum, но также зависит от конфигурации аппаратных решений и организации сети.

> LACP-интерфейсы можно пробрасывать в виртуальные контексты (VCE VPP и VCE NGFW).
>
> Для создания LACP-интерфейса между нодами кластера достаточно указать один физический порт - система автоматически создаст канал между одноименными портами обеих нод. Например, если в кластере есть порт `client`, созданный LACP-интерфейс объединит `client` с первой ноды и `client` со второй ноды. Подробнее о настройке кластера - в статье.

Чтобы объединить несколько физических портов в один агрегированный LACP-интерфейс, выполните действия:

1. Нажмите **Добавить** и выберите **LACP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **Control Plane** - используется только для настройки и администрирования NGFW Novum. Интерфейс с этой ролью не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для подключения к провайдеру.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Физический порт** - порт на сетевом адаптере, который будет использоваться в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. LACP-интерфейс появится в таблице интерфейсов.

SPAN

SPAN (Switch Port Analyzer) - технология зеркалирования трафика, которая позволяет копировать пакеты данных с одного или нескольких портов коммутатора/маршрутизатора на специальный порт мониторинга. В Ideco NGFW Novum SPAN-интерфейс позволяет дублировать трафик локальных и внешних интерфейсов на отдельное внешнее устройство для анализа и выявления угроз.

SPAN-интерфейс должен использовать выделенный физический порт сетевой карты и не может делить его с другими интерфейсами.

Перед обновлением на 22 версию Ideco NGFW Novum убедитесь, что в качестве **Интерфейса назначения** выбран интерфейс, занимающий один физический порт сетевой карты. Если этот порт разделяется с другими интерфейсами, SPAN-интерфейс будет

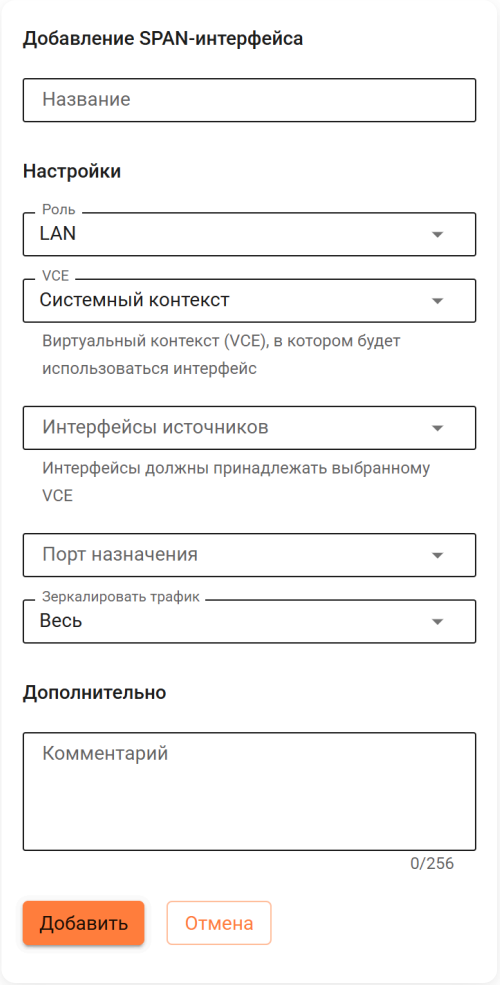
отключен после обновления.

SPAN-интерфейс может быть перегружен при большом количестве наблюдаемых интерфейсов.

Для настройки SPAN-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **SPAN**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - роль интерфейса в Ideco NGFW Novum:
  - **LAN** - используется для создания локальных интерфейсов.
  - **WAN** - используется для поддержки старых конфигураций Ideco NGFW, если в предыдущих версиях SPAN был настроен на подключении к провайдеру.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейсы источников** - выберите интерфейсы, трафик которых хотите дублировать. Доступные варианты: **Ethernet**, **VLAN** и **LACP**.
- **Порт назначения** - выберите порт, на который будет дублироваться трафик.
- **Зеркалировать трафик** - выберите тип трафика, который хотите дублировать. Доступные варианты: **Весь**, **Только входящий** или **Только исходящий**.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. SPAN-интерфейс появится в таблице интерфейсов.

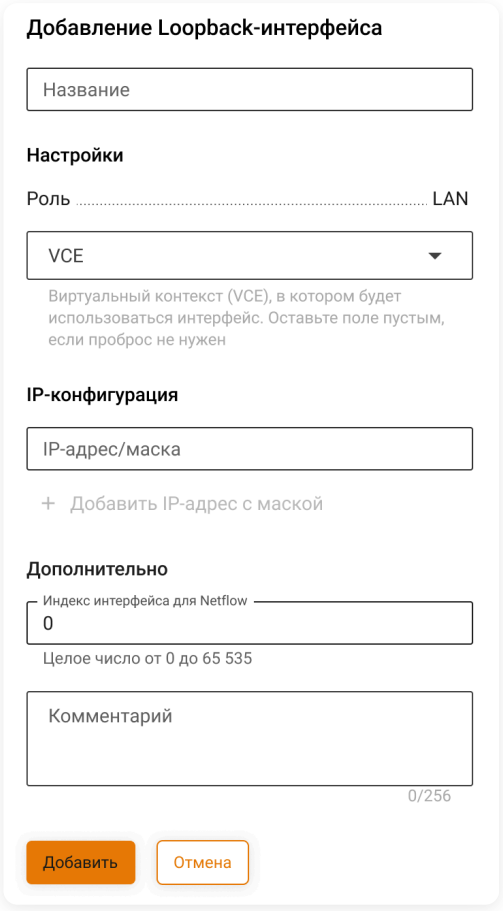
Loopback

Loopback - виртуальный интерфейс, не привязанный к физическому сетевому порту. Основная задача Loopback-интерфейса - обеспечение стабильного IP-адреса для устройства, который остается доступным даже при сбоях физических соединений.

Для настройки Loopback-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Loopback**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - только **LAN** для создания локальных интерфейсов.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **IP-адрес/маска** - IP-адрес, который требуется назначить на интерфейс, с маской в формате `x.x.x.x/x`.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

Чтобы избежать проблем с подключением пользователей к Loopback-интерфейсу по VPN, IP-адрес Loopback-интерфейса **не должен** входить в диапазоны адресов, используемые для SNAT. Если включен автоматический SNAT локальных сетей, IP-адрес Loopback-интерфейса не должен входить в диапазоны:

- `10.0.0.0/8`
- `192.168.0.0/16`
- `172.16.0.0/12`

3. Нажмите **Добавить**. Loopback-интерфейс появится в таблице интерфейсов.

Особенности настройки Loopback-интерфейса

При работе с Loopback-интерфейсом используйте правила:

- Для доступа к веб-интерфейсу Ideco NGFW Novum укажите в адресной строке браузера `<IP-адрес Loopback-интерфейса>:8443`.
- Для доступа к серверу по SSH:
  - Разрешите доступ по SSH.
  - Введите в терминале `ssh login@<IP-адрес Loopback-интерфейса>`.
- Для подключения пользователей по VPN на устройстве пользователя при создании VPN-подключения в качестве шлюза укажите домен или IP-адрес Loopback-интерфейса.
- В разделе **BGP** при добавлении **BGP-соседей** укажите в поле **Исходящий интерфейс** Loopback-интерфейс.

- При настройке **OSPF** укажите в поле **Интерфейс** Loopback-интерфейс.
- При создании маршрута Null route укажите Loopback-интерфейс в качестве шлюза для подсети/IP-адресов. В этом случае весь входящий на NGFW трафик, предназначенный для этих адресов, будет отбрасываться.
- При создании DNAT-правила **Межсетевого экрана** в поле **Адрес назначения** укажите IP-адрес, назначенный на Loopback-интерфейс. Опубликованные ресурсы будут доступны по IP-адресу Loopback-интерфейса.
- При создании SNAT-правила **Межсетевого экрана** в поле **Сменить IP-адрес источника** укажите IP-адрес, назначенный на Loopback-интерфейс. Исходный адрес, указанный в поле **Адрес источника**, будет заменен на адрес Loopback-интерфейса.

Для подключения к Loopback-интерфейсу настройте маршрутизацию до IP-адреса, назначенного на этот Loopback-интерфейс.

L2-мост

L2-мост не поддерживается в Классическом и Системном контекстах.

L2-мост используется для соединения двух сегментов сети на уровне канального доступа (L2). Он позволяет:

- Объединять две физические сети в один широковещательный домен для распространения broadcast-трафика (ARP, DHCP и так далее) по объединенной логической сети.
- Обеспечивать видимость всех устройств в обоих сегментах сети, объединенных мостом, как если бы эти устройства находились в одной коммутируемой сети.

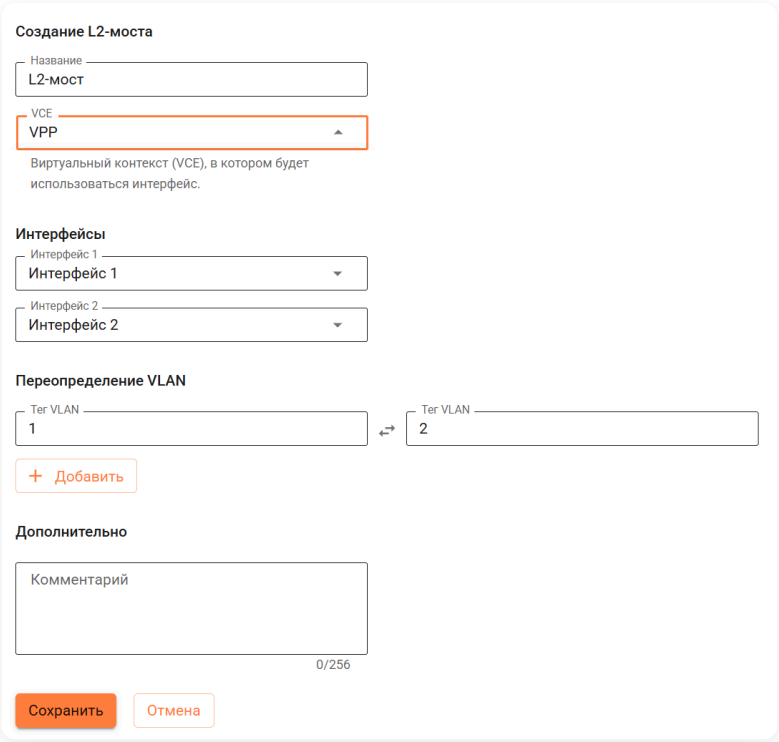
Для создания L2-моста:

1. Создайте два интерфейса. Допустимые интерфейсы:

- **Ethernet** (LAN, WAN).
- **LACP**.
- **VLAN**.

В поле **Физический порт** выберите свободные порты, которые будут объединены L2-мостом, а в поле **VCE** - высокопроизводительный контекст **VPP**.

2. Нажмите **Добавить**, выберите **L2-мост** и заполните поля:



Расшифровка полей

- **Название** - введите название L2-моста.
- **VCE** - выберите VCE VPP.

- **Интерфейсы** - выберите интерфейсы, между которыми будет настроен прозрачный L2-мост. Типы интерфейсов должны совпадать. Нельзя выбрать интерфейсы, имеющие дочерние. При выборе в этих полях VLAN-интерфейсов теги VLAN нельзя будет изменить в настройках моста.
- **Переопределение VLAN** - введите теги VLAN для маппинга или оставьте поля пустыми. Переопределение VLAN работает в обе стороны. При необходимости добавьте несколько пар тегов.
- **Комментарий** - введите описание L2-моста. Максимум 256 символов.

Трафик, проходящий через L2-мост, можно фильтровать политиками безопасности VCE VPP, за временным исключением средств прокси: Контент-фильтра, SSL/TLS-инспекций.

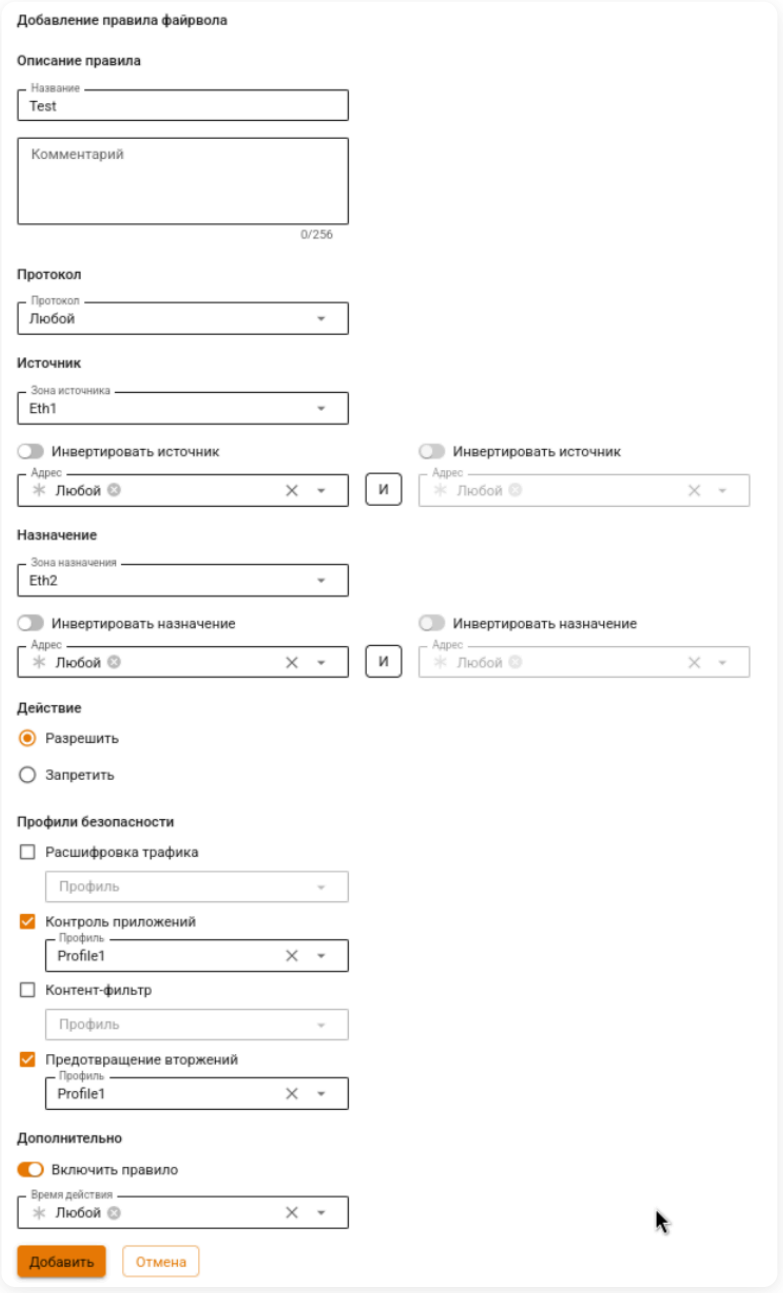
Пример настройки фильтрации

Создан L2-мост между Интерфейсом 1 (зона LAN) и Интерфейсом 2 (зона WAN).

Задача: включить фильтрацию DPI, IPS для трафика из зоны **WAN** в зону **LAN**.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Описание правила** - введите **Название** правила и **Комментарий**.
- **Протокол** - выберите протокол передачи данных: **AH**, **ESP**, **GRE**, **ICMP**, **TCP**, **UDP**, **TCP/UDP** (TCP или UDP) или **Любой**.
- **Источник**:
  - **Зона источника** - выберите Интерфейс 2 (зона WAN).

- **Адрес** - выберите **Любой**.
- **Назначение**:
  - **Зона назначения** - выберите Интерфейс 1 (зона LAN).
  - **Адрес** - выберите **Любой**.
- **Действия** - выберите **Разрешить**.
- **Профили безопасности**:
  - **Расшифровка трафика** - оставьте поле пустым.
  - **Контроль приложений** - выберите профиль Контроля приложений, которым требуется фильтровать трафик.
  - **Контент-фильтр** - оставьте поле пустым.
  - **Предотвращение вторжений** - выберите профиль системы Предотвращения вторжений, которым требуется фильтровать трафик.
- **Дополнительно** - включите правило и задайте время действия. По умолчанию правило выключено.

Подключение по 3G и 4G

В Ideco NGFW Novum поддерживаются модели USB-модемов с Network Communication **CDC-Ethernet**, список модемов представлен в таблице Список поддерживаемых USB-модемов.

Туннельные интерфейсы

GRE

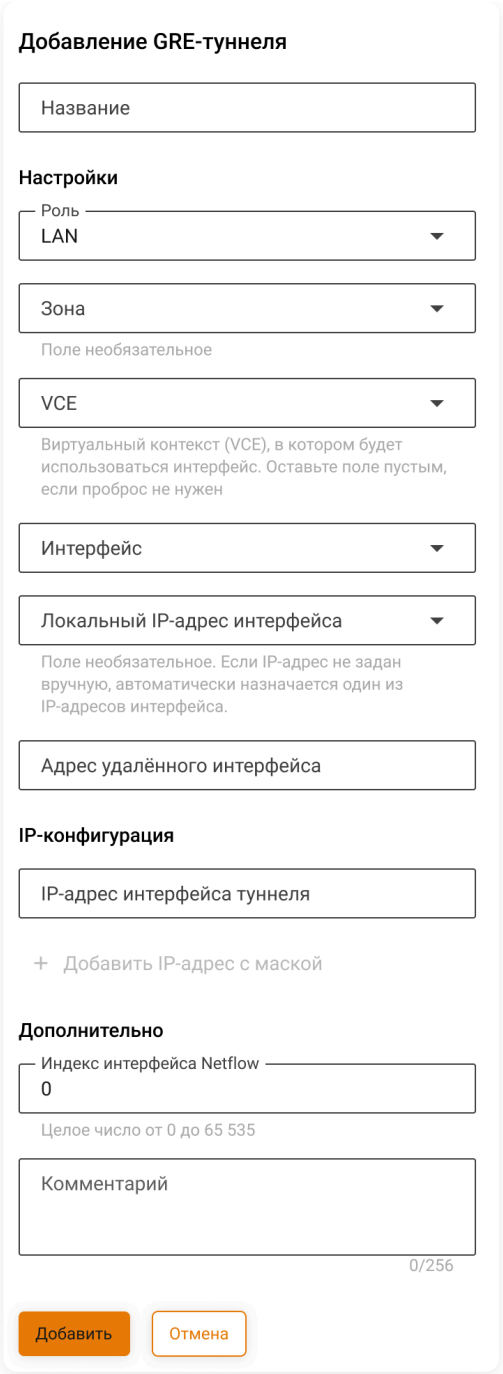
GRE-туннель - соединение, позволяющее передавать широковещательный трафик. Поддерживает работу протокола динамической маршрутизации OSPF. Пакеты, проходящие через GRE-туннель, не подвергаются шифрованию.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

Для настройки GRE-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **GRE**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - доступные роли **WAN** и **LAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN**, **LACP**, **PPTP**, **L2TP** и **PPPoE**.
- **Локальный IP-адрес интерфейса** - укажите IP-адрес родительского интерфейса, на котором запущен туннель.
- **Адрес удаленного интерфейса** - укажите IP-адрес интерфейса для подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес с маской создаваемого туннеля.
- **Шлюз** - укажите шлюз для направления трафика по умолчанию.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. GRE-туннель появится в таблице интерфейсов.

Если GRE-интерфейсу назначена роль **WAN**, для прохождения трафика может потребоваться:

- Авторизация пользователя. Например, по IP-адресу.
- Создание разрешающего правила **FORWARD** для трафика в GRE-туннеле в **Правила трафика** → **Межсетевой экран**.

L2TP

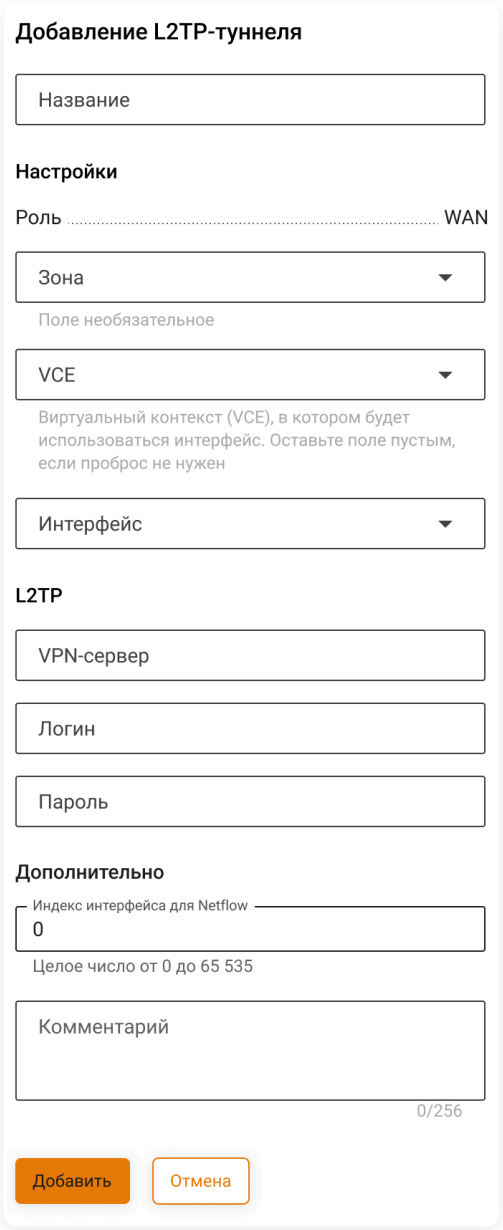
L2TP-туннель - технология подключения, использующая протокол L2TP, которая применяется интернет-провайдерами для повышения надежности процесса авторизации пользователей.

L2TP-туннель можно создать только на интерфейсах, настроенных на режим **Статический** или **DHCP** и роль **WAN**.

Для настройки L2TP-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **L2TP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.

- **Роль** - только **WAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN** и **LACP**.
- **VPN-сервер** - IP-адрес или доменное имя L2TP-сервера.
- **Логин** - имя пользователя для подключения по L2TP.
- **Пароль** - пароль пользователя для подключения по L2TP.
- **DNS-сервер** - укажите, если доменное имя VPN-сервера не резолвится через настроенные в Ideco NGFW Novum DNS-серверы.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. L2TP-туннель появится в таблице интерфейсов.

PPTP

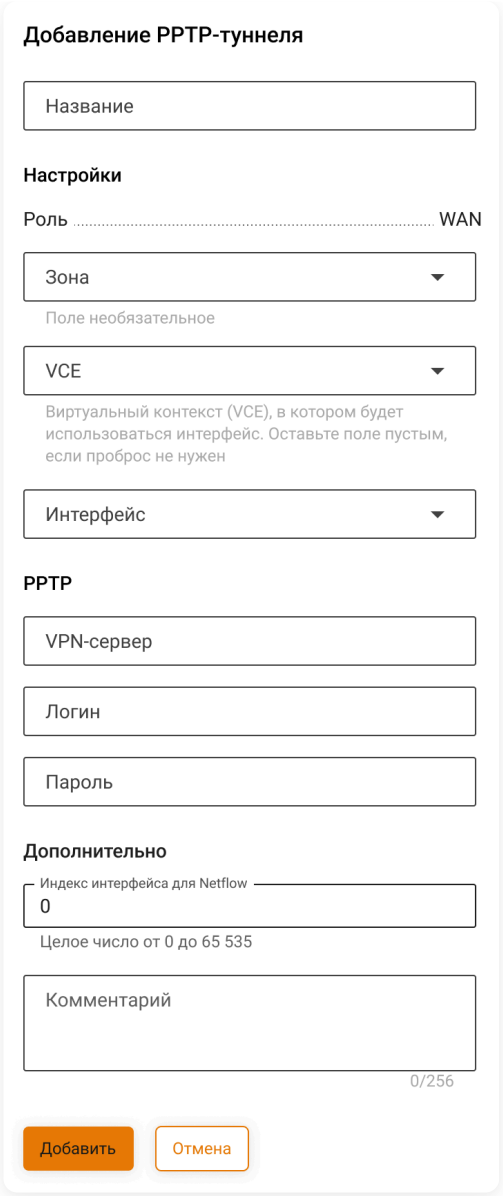
PPTP-туннель - один из первых VPN-протоколов, созданный для обеспечения защищенного доступа через интернет. Работает на базе протокола PPP (Point-to-Point Protocol), который обеспечивает аутентификацию и шифрование данных.

> PPTP-туннель можно создать только на интерфейсах, настроенных на режим **Статический** или **DHCP** и роль **WAN**.

Для настройки PPTP-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **PPTP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - только **WAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN** и **LACP**.
- **VPN-сервер** - IP-адрес или доменное имя PPTP-сервера.
- **Логин** - имя пользователя для подключения по PPTP.
- **Пароль** - пароль пользователя для подключения по PPTP.
- **DNS-сервер** - укажите, если доменное имя VPN-сервера не резолвится через настроенные в Ideco NGFW Novum DNS-серверы.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. PPTP-туннель появится в таблице интерфейсов.

PPPoE

PPPoE-туннель - технология подключения через протокол PPPoE, которая активно применяется интернет-провайдерами при организации доступа в сеть через xDSL-соединения.

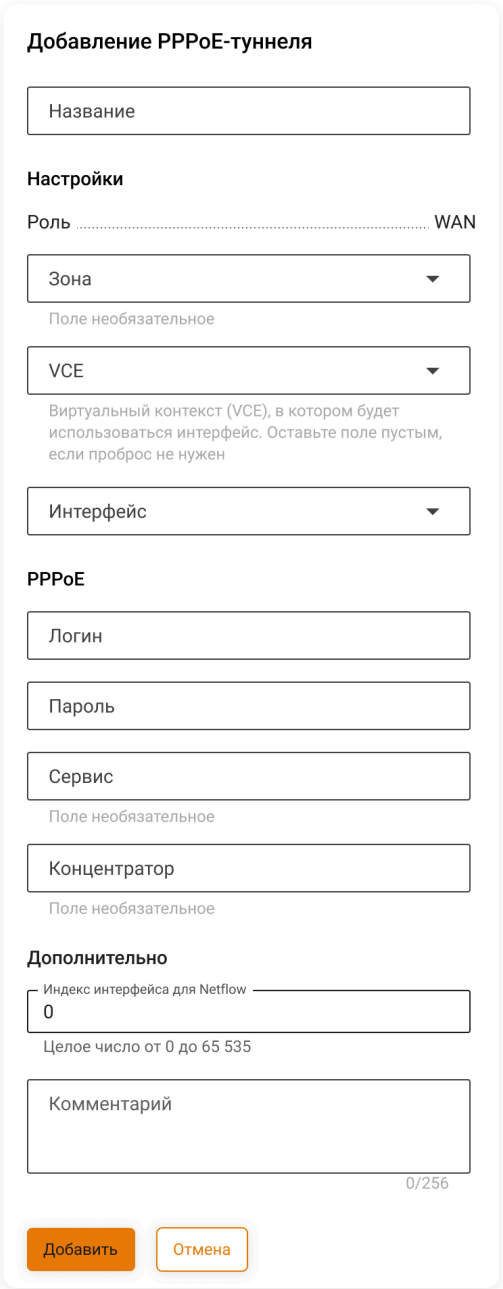
PPPoE-туннель можно создать только на интерфейсах, настроенных на режим **Без конфигурации** и роль **WAN**.

При подключении к провайдеру с использованием протокола PPPoE настройте DNS-сервер вручную, воспользовавшись статьей.

Для настройки PPPoE-туннеля выполните действия:

1. Нажмите **Добавить** и выберите **PPPoE**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для последующей идентификации интерфейса.
- **Роль** - только **WAN**.
- **Зона** - объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Оставьте поле пустым, если выбор зоны не требуется. Список предустановленных зон приведен в статье.
- **VCE** - виртуальный контекст (VCE), в котором будет использоваться интерфейс.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение. Для создания туннеля можно использовать интерфейсы: **Ethernet**, **VLAN** и **LACP**.
- **Логин** - имя пользователя для подключения по PPPoE.
- **Пароль** - пароль пользователя для подключения по PPPoE.
- **Сервис** - идентификатор сервиса. Необязательное поле.

- **Концентратор** - идентификатор концентратора. Необязательное поле.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

3. Нажмите **Добавить**. PPPoE-туннель появится в таблице интерфейсов.

Полезные ссылки

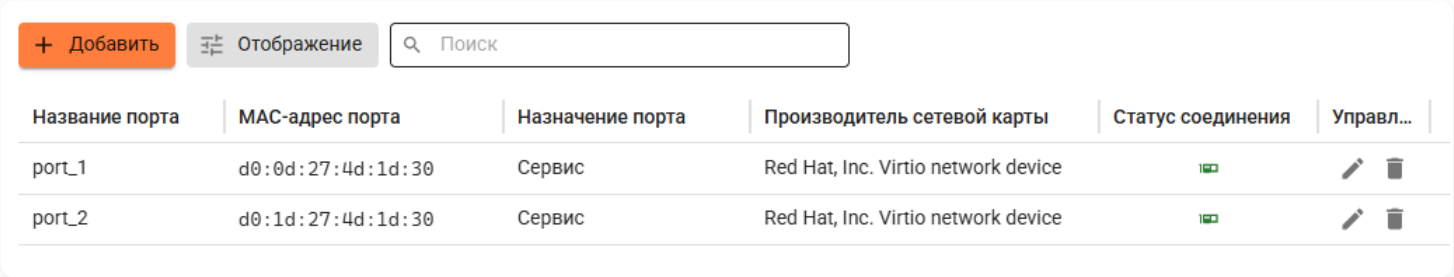
- **Межсетевой экран**
- **Администраторы**
- **BGP**
- **OSPF**
- **Внешние DNS-серверы**

Физические порты

Функциональность доступна в **Классическом** и **Системном контекстах**.

Физические порты связывают сетевую конфигурацию, что позволяет переносить настройки на другой порт без изменения политик безопасности даже при выходе из строя текущего порта.

Сетевые соединения в Ideco NGFW Novum настраиваются в **Сервисы** → **Сетевые интерфейсы** → **Интерфейсы** и ссылаются на **Физические порты**. При первичной установке Ideco NGFW Novum порты автоматически включаются в таблицу и получают название, например, `eth0_b1`. Записи в таблице отражают физические порты на корпусе устройства:



Если **Название порта** не соответствует физическому обозначению, переименуйте порт в соответствии с обозначением на корпусе устройства.

На сетевых картах может быть несколько сетевых портов, каждый из которых имеет свой MAC-адрес.

Возможность передавать в VCE VPP отдельные порты сетевой карты зависит от модели сетевого адаптера:

- Если адаптер поддерживает разделение портов, порты можно передавать по отдельности.
- Если адаптер не поддерживает разделение портов, в VCE VPP необходимо передавать все порты сетевой карты. Иначе интерфейсы этой сетевой карты работать не будут.

В кластеризации используется сетевая конфигурация, общая для обеих нод. Конфигурация ссылается на физические порты по их названию. Соответствие названий конкретным физическим картам хранится:

- Для аппаратных решений - в прошивке сервера (UEFI).
- Для виртуальных машин - внутри образа диска.

Подключение по 3G и 4G

В Ideco NGFW Novum поддерживаются модели USB-модемов с Network Communication **CDC-Ethernet**, список модемов представлен в таблице Список поддерживаемых USB-модемов. При подключении USB-модем будет отображаться в Ideco NGFW Novum как новый ethernet-интерфейс.

Статусы соединения

- Подключен
- Не подключен
- Статус порта неизвестен. Проверьте физический порт, его состояние и совместимость оборудования

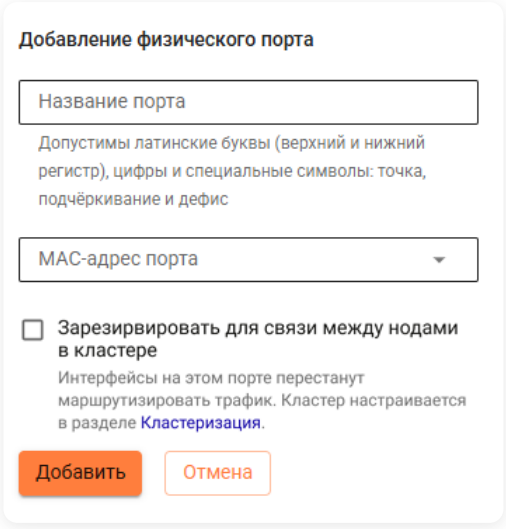
Управление портами

Порты можно редактировать, нажав , или удалить, нажав . При удалении порта созданные на его основе интерфейсы перестанут работать, пока не назначить на них новый порт. Для идентификации порта ориентируйтесь на наименование производителя или MAC-адрес.

Чтобы добавить новый порт, выполните действия:

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и нажмите **Добавить**.

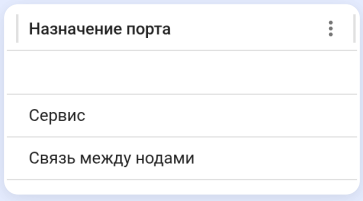
2. Заполните поля:



- **Название порта** - укажите обозначение порта на корпусе устройства.
- **MAC-адрес порта** - выберите свободный порт на сетевой карте.
- **Зарезервировать для связи между нодами в кластере** - включите опцию, если требуется использовать порт для настройки кластеризации. Подробнее в статье Кластеризация. В списке портов в колонке **Связь между нодами** порты со включенной опцией будут иметь значение **Связь между нодами**, а порты с выключенной опцией - значение **Сервис**.

Примеры настройки физических портов

Примеры актуальны для портов с назначением **Сервис**:

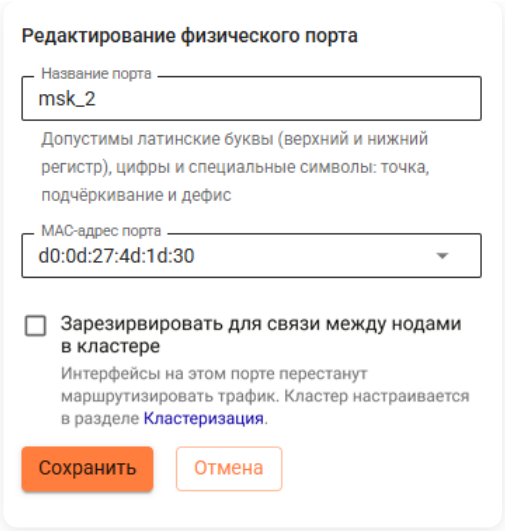


Переименование порта

Наименования всех используемых сетевых портов в кластере должны совпадать на обеих нодах. Подробнее в статье Настройка кластера.

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и нажмите .

2. Отредактируйте **Название порта** и нажмите **Сохранить**:



Перенос сетевого интерфейса на другой порт

Возможные причины переноса сетевого интерфейса на другой порт:

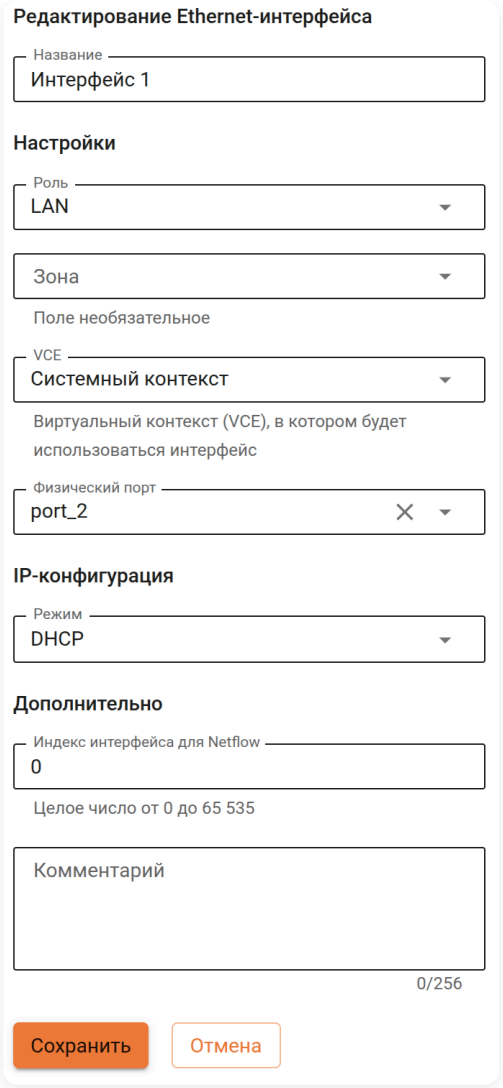
- Замена сетевой карты.
- Выход порта из строя.
- Изменение схемы подключения или порядка портов на устройстве.

> Перенос сетевого интерфейса на другой порт не влияет на настройки правил фильтрации.

Выполните действия:

1. Перейдите в **Сетевые интерфейсы** → **Интерфейсы** и отредактируйте необходимый интерфейс, нажав .

2. Выберите порт в поле **Физический порт** и нажмите **Сохранить**:



3. Если порт занят:

- Отключите интерфейс, порт которого необходимо переназначить на другой интерфейс, нажав .
- Выполните действия из пункта 1.

Перенос сетевых интерфейсов в кластере

Так как в кластеризации используется общая сетевая конфигурация, перенос сетевого интерфейса на другой порт выполняется только на активной ноде. При выходе из строя порта в кластере есть два варианта действий:

Использование другой пары портов

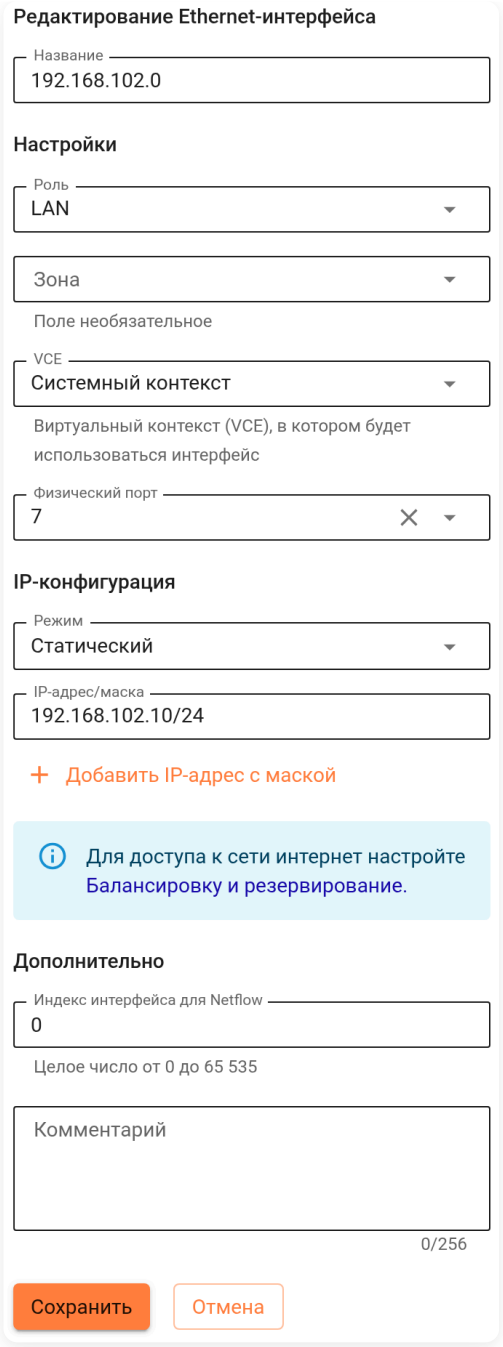
Рекомендуемый вариант, так как обеспечивает соответствие наименований портов физическим обозначениям на сервере.

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и найдите свободную пару портов в активной и пассивной нодах:

Название порта	MAC-адрес порта	Назначение порта	Производитель сетевой карты	Статус соединения	Управление
cluster (Активная) • 7					
1	bc:24:11:08:ee:d0	Сервис	Red Hat, Inc. Virtio network device		
2	bc:24:11:bb:cb:40	Связь между нодами	Red Hat, Inc. Virtio network device		
3	bc:24:11:85:6e:b9	Сервис	Red Hat, Inc. Virtio network device		
4	bc:24:11:df:1b:5a	Сервис	Red Hat, Inc. Virtio network device		
5	bc:24:11:14:6a:a9	Сервис	Red Hat, Inc. Virtio network device		
6	bc:24:11:97:d8:b9	Сервис	Red Hat, Inc. Virtio network device		
7	bc:24:11:19:ad:fb	Сервис	Red Hat, Inc. Virtio network device		
ngfw (Пассивная) • 7					
1	bc:24:11:3f:dd:98	Сервис	Red Hat, Inc. Virtio network device		
4	bc:24:11:14:fe:f3	Сервис	Red Hat, Inc. Virtio network device		
5	bc:24:11:10:67:e5	Сервис	Red Hat, Inc. Virtio network device		
3	bc:24:11:0f:c3:51	Сервис	Red Hat, Inc. Virtio network device		
2	bc:24:11:e4:e0:62	Связь между нодами	Red Hat, Inc. Virtio network device		
7	bc:24:11:10:49:7d	Сервис	Red Hat, Inc. Virtio network device		
6	bc:24:11:45:f2:50	Сервис	–		

2. Перейдите на вкладку **Интерфейсы** и отредактируйте интерфейс, порт которого вышел из строя, нажав .

3. Выберите порт в поле **Физический порт** и нажмите **Сохранить**:



Переименование свободного порта

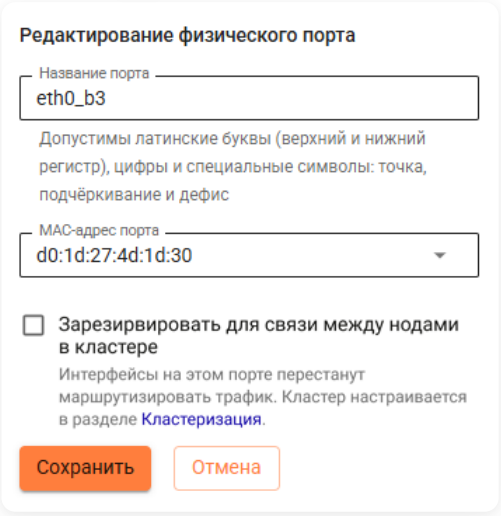
Может вызвать несоответствие между наименованием порта в веб-интерфейсе и физическим обозначением.

1. Перейдите в **Сетевые интерфейсы** → **Физические порты** и выберите свободный порт в ноде, порт которой вышел из строя:

Название порта	MAC-адрес порта	Назначение порта	Производитель сетевой карты	Статус соединения	Управление
cluster (Активная) • 7					
eth0_98	bc:24:11:08:ee:d0	Сервис	Red Hat, Inc. Virtio network device		
eth0_b3	bc:24:11:bb:cb:40	Связь между нодами	Red Hat, Inc. Virtio network device		
eth0_51	bc:24:11:85:6e:b9	Сервис	Red Hat, Inc. Virtio network device		
eth1_f3	bc:24:11:df:1b:5a	Сервис	Red Hat, Inc. Virtio network device		
eth0_e5	bc:24:11:14:6a:a9	Сервис	Red Hat, Inc. Virtio network device		
eth2_7d	bc:24:11:32:72:32	Сервис	–		
⚠ eth1_b9	bc:24:11:97:d8:b9	Сервис	Red Hat, Inc. Virtio network device		
ngfw (Пассивная) • 7					
eth0_98	bc:24:11:3f:dd:98	Сервис	Red Hat, Inc. Virtio network device		
eth1_f3	bc:24:11:14:fe:f3	Сервис	Red Hat, Inc. Virtio network device		
eth0_e5	bc:24:11:10:67:e5	Сервис	Red Hat, Inc. Virtio network device		
eth0_51	bc:24:11:0f:c3:51	Сервис	Red Hat, Inc. Virtio network device		
eth0_b3	bc:24:11:e4:e0:62	Связь между нодами	Red Hat, Inc. Virtio network device		
eth2_7d	bc:24:11:10:49:7d	Сервис	Red Hat, Inc. Virtio network device		
⚠ eth3_50	bc:24:11:45:f2:50	Сервис	Red Hat, Inc. Virtio network device		

2. Сохраните **Название порта**, вышедшего из строя, и нажмите для его удаления.

3. Нажмите для редактирования свободного порта и укажите название порта, сохраненное в пункте 2:



4. Нажмите **Сохранить**.

Рекомендуем на корпусе оборудования указать новое название порта, заданное в веб-интерфейсе, и переключить кабель в новый порт.

Перенос бэкапа на другой сервер

Пример настройки подробно описан в статье Бэкапы.

Полезные ссылки

- **Бэкапы**
- **Кластеризация**
- **Настройка кластера**
- **Список поддерживаемых USB-модемов**

IGMP Proxy

Классический контекст | Высокопроизводительный контекст

Название службы раздела **IGMP Proxy**: `ideco-igmpproxy-rest`, `ideco-igmpproxy-backend`, `ideco-igmpproxy`.

Список служб для других разделов доступен по ссылке.

IGMP Proxy - служба, которая позволяет передавать мультикастовый трафик через маршрутизатор. IGMP Proxy работает как посредник между мультикастовыми группами и сетью, оптимизируя передачу данных, что сокращает объем трафика, снижает нагрузку на сеть и повышает скорость работы сети.

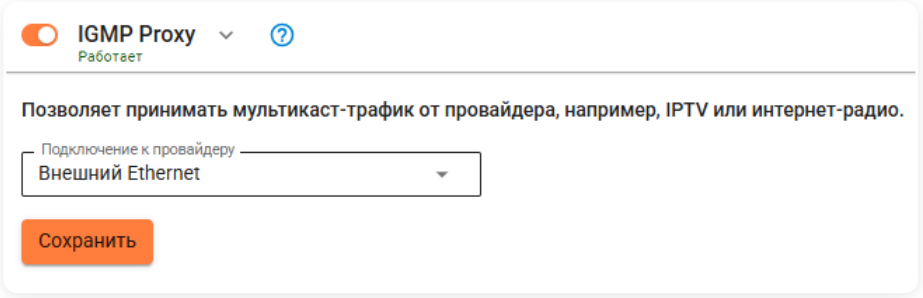
Со стороны клиентов **IGMP Proxy** поддерживает версии IGMPv1 и IGMPv2.

IGMP Proxy работает только с Ethernet-интерфейсами и не работает на интерфейсах VLAN, PPPoE или VPN (L2TP, PPTP).

Настройка в Ideco NGFW Novum

1. Прейдите в **Сервисы** → **IGMP Proxy** и включите опцию **IGMP Proxy**.

2. В поле **Подключение к провайдеру** выберите **Ethernet-подключение**:



Принцип работы

На примере подключения двух пользователей к мультикаст-потоку одного источника:

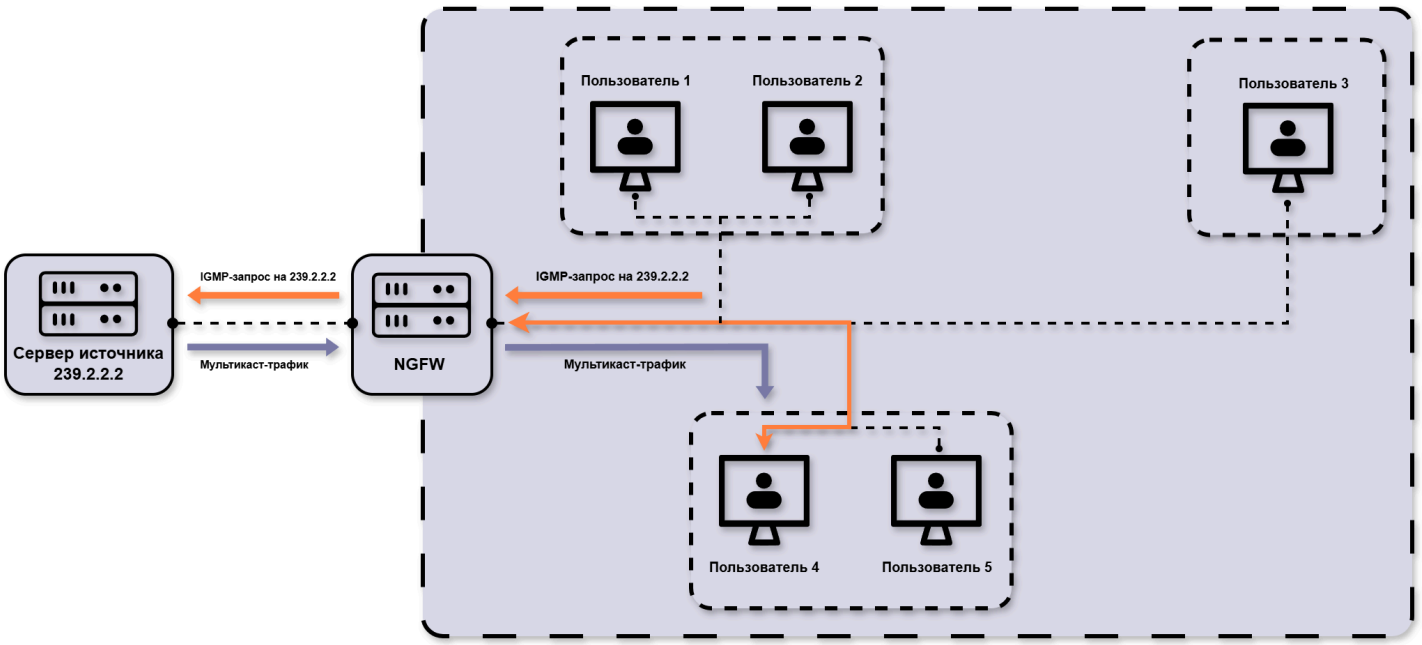
1. **Сервер источника** начинает трансляцию мультикаст-трафика с адреса из диапазона 224.0.0.0/4.

2. **Пользователь 4** хочет подключиться к трафику и генерирует IGMP-запрос (Join) на **Ideco NGFW Novum** для получения мультикаст-трафика от сервера источника.

3. **Ideco NGFW Novum** получает IGMP-запрос и отправляет аналогичный запрос к серверу источника.

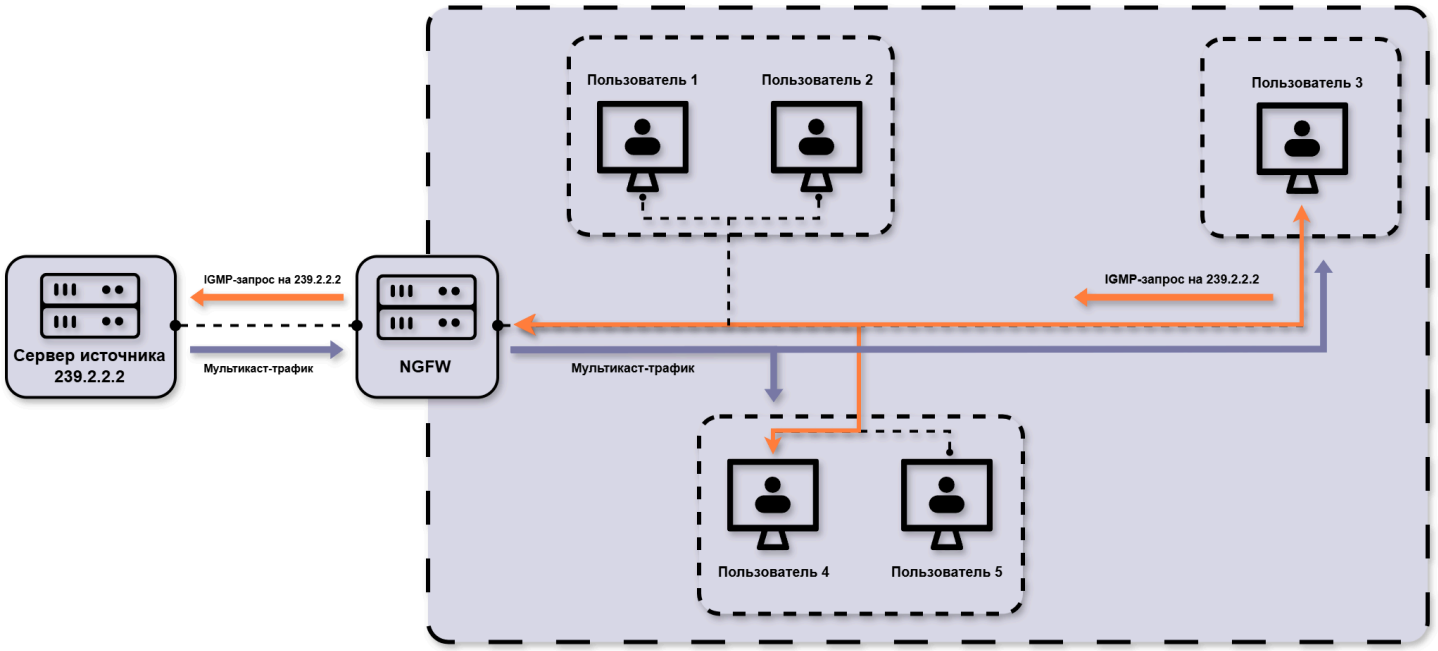
4. Сервер источника получает запрос и начинает транслировать мультикаст-трафик на **Ideco NGFW Novum**.

5. **Ideco NGFW Novum** пропускает трафик с адреса 239.2.2.2 в подсеть с **Пользователем 4**, и **Пользователь 4** становится получателем трафика:



6. **Пользователь 3**, находящийся в другой подсети, также решает подключиться к этой трансляции и генерирует IGMP-запрос (Join) на Ideco NGFW Novum.

7. **Ideco NGFW Novum** получает запрос и дублирует **Пользователю 3** трафик, поступающий **Пользователю 4**:



Ideco NGFW Novum периодически проверяет, есть ли получатели, отправляя пользователям IGMP-запрос (Query). Пользователи в ответ отправляют Join, как при подключении.

Если на Ideco NGFW Novum приходит хотя бы один Join, мультикаст-трафик продолжает транслироваться получателям.

Прокси

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Прокси**: `ideco-proxy-backend`, `squid`.

Список служб для других разделов доступен по ссылке.

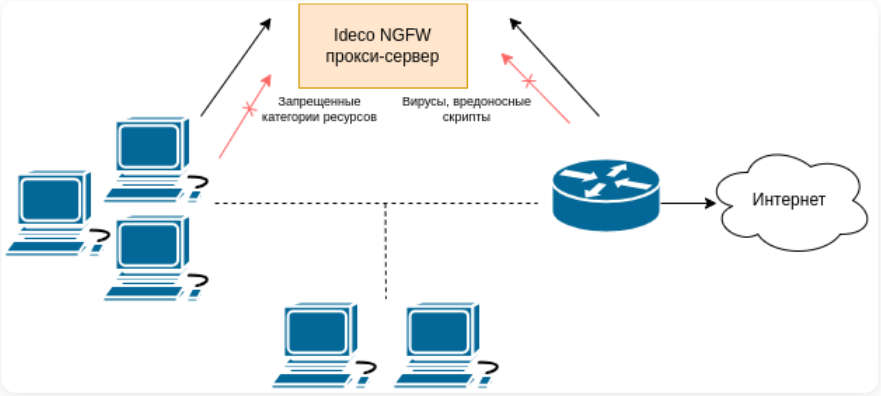
Прокси-сервер используется не только для проксирования веб-трафика, но и для передачи трафика сервисам:

- Антивирус для веб-трафика (Антивирус Касперского).
- Сервис отчетности по веб-трафику пользователей.
- Контент-фильтр.

Порядок обработки веб-трафика подробнее описан в статье.

Не указывайте на хостах локальной сети настройки прокси. Достаточно указания NGFW Novum в качестве шлюза по умолчанию для устройств в сети.

Для настройки фильтрации HTTPS-трафика нужно добавить корневой сертификат NGFW Novum на компьютеры пользователей. Подробнее в статье Настройка фильтрации HTTPS.



При использовании Ideco NGFW Novum в качестве прокси-сервера с прямыми подключениями к прокси большинство функций будет работать с некоторыми особенностями:

- В правилах **Файрвола** для пользователей необходимо указывать цепочки **INPUT** вместо **FORWARD**.
- Глубокий анализ трафика системой **Предотвращение вторжений** и модулем **Контроль приложений** будет осуществляться только для трафика, проходящего через прокси-сервер (часть правил работать не будет).
- Исключения из прокси-сервера необходимо делать средствами браузера или правилами маршрутизации на конечных устройствах. Настройки в разделе **Сервисы** → **Прокси** → **Исключения** применяются только для прозрачного режима работы прокси-сервера.

Для работы прокси-сервера необходим хотя бы один сетевой интерфейс с ролью **LAN**. Если настроен только интерфейс **Control Plane**, служба `squid` не запустится, при этом отобразится сообщение об отсутствии локальных интерфейсов. Для решения проблемы назначьте одному из интерфейсов роль **LAN** в **Сервисы** → **Сетевые интерфейсы**. Подробнее о настройке интерфейсов - в статье.

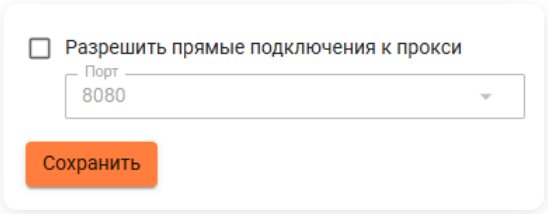
Основное

На вкладке **Основное** предоставлены возможности:

- **Разрешить прямые подключения к прокси** - применяется, когда Ideco NGFW Novum не является шлюзом по умолчанию для клиентов сети. Порт, указанный на стороне NGFW Novum, следует указать на сетевых устройствах локальной сети, веб-трафик которых нужно пропускать через

прокси.

- **Включить журналирование** - применяется для записи логов Антивируса и Контент-фильтра.

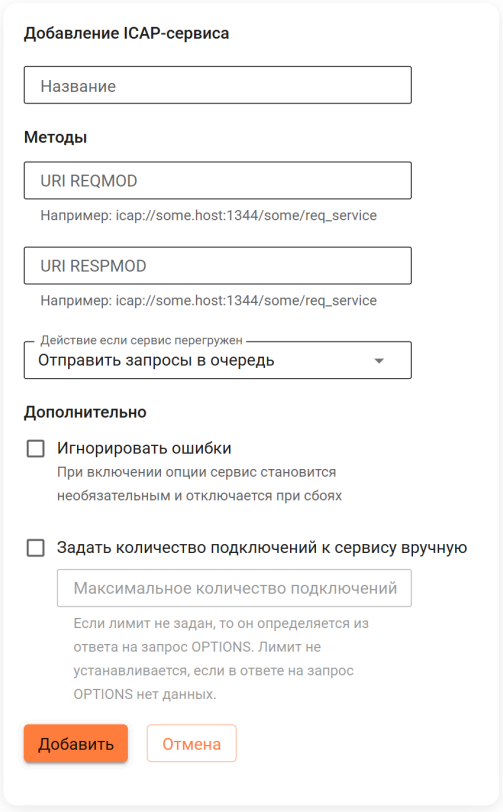


ICAP

ICAP-сервисы обрабатывают исходящий трафик (запросы) после работы Антивируса и Контент-фильтра Ideco NGFW Novum, а входящий (ответы) - перед Антивирусом.

> Для корректной работы ICAP-сервиса должна быть настроена расшифровка HTTPS-трафика в **Контент-фильтре**.

При добавлении ICAP-сервиса доступны настройки:



- **URI REQMOD** - URI для модификации HTTP-запросов перед их отправкой на сервер. Используется для обработки и изменения исходящего трафика.
- **URI RESPMOD** - URI для модификации HTTP-ответов перед их передачей клиенту. Применяется для обработки и изменения входящего трафика.
- **Если сервис перегружен** - опция позволяет выбрать сценарий действий при перегруженности ICAP-сервиса.
- **Игнорировать ошибки** - если включена опция, то сервис будет считаться необязательным. При недоступности или неправильной работе сервис не будет задействован.
- **Установить лимит подключений к сервису** - если значение не задано, максимальное количество подключений берется из ответа сервиса на запрос OPTIONS. Если максимальное количество подключений не указано в ответе на запрос OPTIONS, тогда - без ограничений.

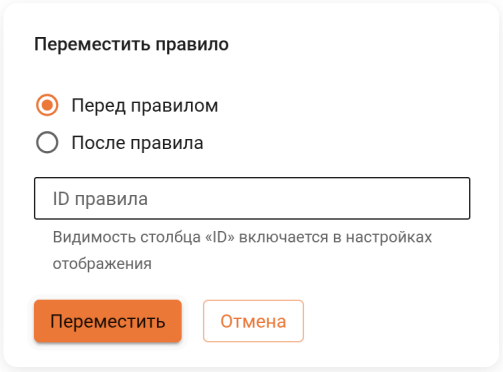
> Если указать в опции **Установить лимит подключений к сервису** значение меньше четырех, то клиентские подключения могут быть нестабильными.

Для перемещения сервисов в таблице выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

WCCP

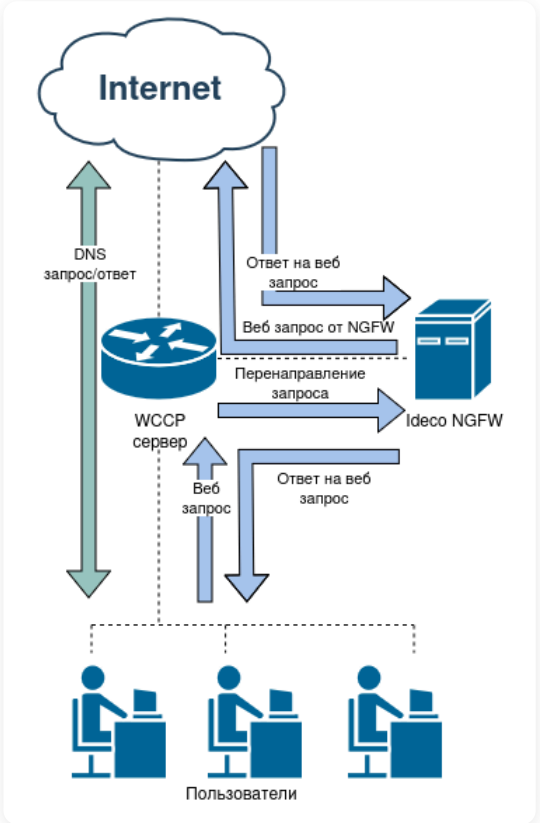
Протокол WCCP используется для перенаправления трафика на Ideco NGFW Novum. По умолчанию перенаправляется только HTTP/HTTPS-трафик.

Для активации WCCP включите опцию **Включить перенаправление трафика с WCCP-серверов на Ideco NGFW Novum**. Запустится процесс согласования параметров с WCCP-сервером.

В NGFW Novum предусмотрено два режима работы WCCP - L2 и GRE:

L2

Режим L2 используется, если WCCP-сервер и Ideco NGFW Novum находятся в одном сетевом сегменте:



Последовательность обработки веб-запросов на уровне L2:

1. Пользователь отправляет веб-запрос.

2. Запрос перенаправляется сервером на Ideco NGFW Novum.

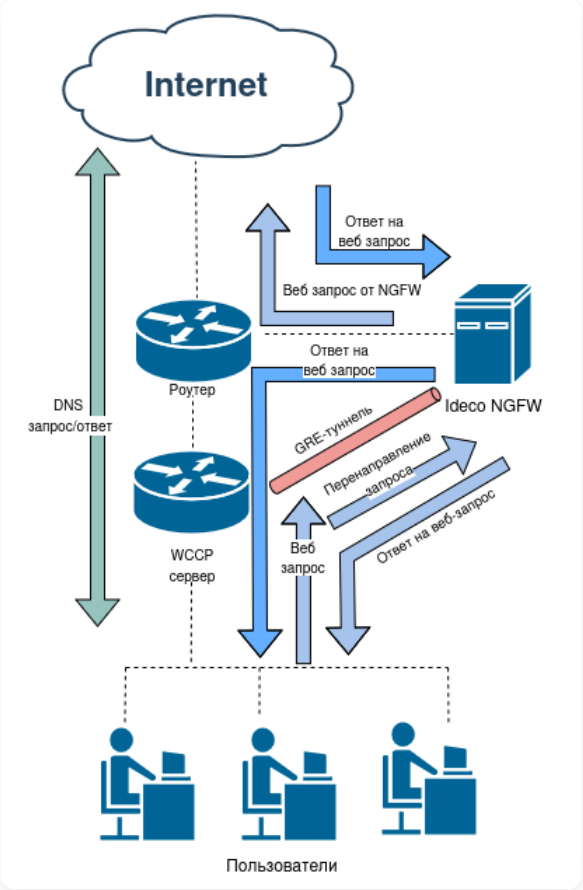
3. Ideco NGFW Novum обрабатывает запрос:

- Если запрос заблокирован, информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW Novum подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается обратно по тому же пути, по которому уходил на внешний сервер.
GRE

Для работы WCCP в GRE-режиме необходимо создать на Ideco NGFW Novum GRE-интерфейс, указав в поле **Адрес удаленного интерфейса** IP-адрес WCCP-сервера.

Режим GRE используется, если WCCP-сервер и Ideco NGFW Novum находятся в разных сетевых сегментах:



Последовательность обработки веб-запросов на уровне GRE:

1. Пользователь отправляет веб-запрос.

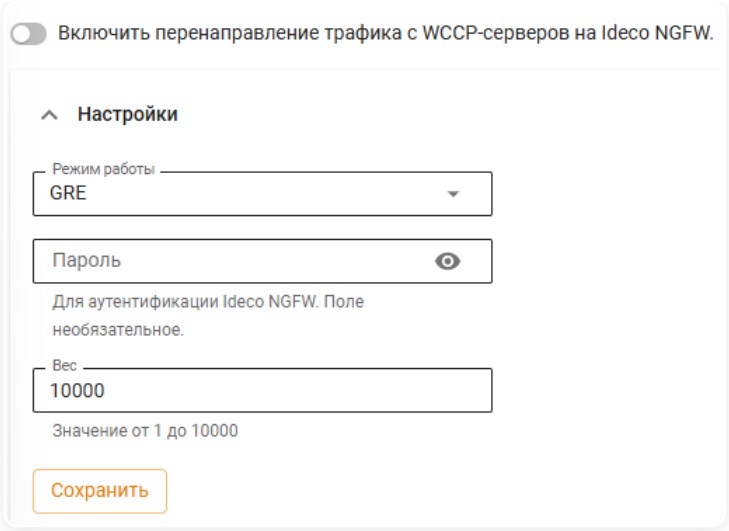
2. Запрос перенаправляется по GRE-туннелю на Ideco NGFW Novum.

3. Ideco NGFW Novum обрабатывает запрос:

- Если запрос заблокирован, то информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW Novum подменяет IP-адрес источника и направляет запрос на внешний сервер.

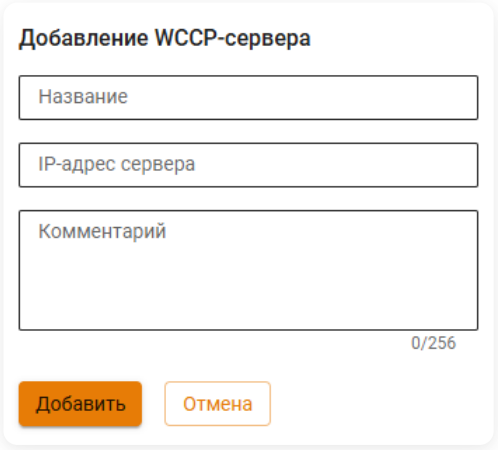
Ответ возвращается напрямую от Ideco NGFW Novum пользователю, минуя GRE-туннель.
Для выбора режима раскройте блок **Настройки**.

Если на WCCP-сервере задан пароль, сохраните пароль в соответствующем поле:



Если WCCP использует несколько Ideco NGFW Novum, настройте распределение трафика с помощью указания приоритета в поле **Вес**. Допустимые значения - от 1 до 10000.

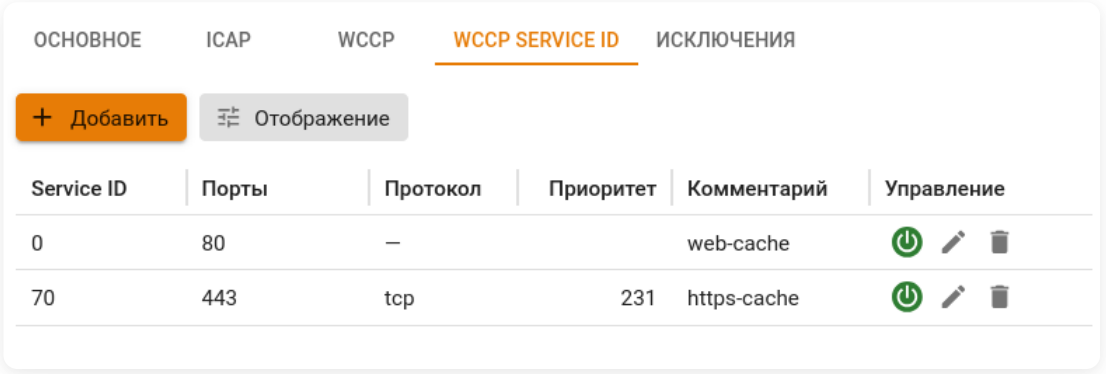
Для добавления WCCP-сервера нажмите кнопку **Добавить** и укажите IP-адрес сервера:



WCCP Service ID

Service ID - идентификаторы сервисной группы. Настройки на этой вкладке позволяют выбрать службы, трафик которых сервер WCCP будет перенаправлять на Ideco NGFW Novum.

По умолчанию настроены сервисы для HTTP/HTTPS-трафика:

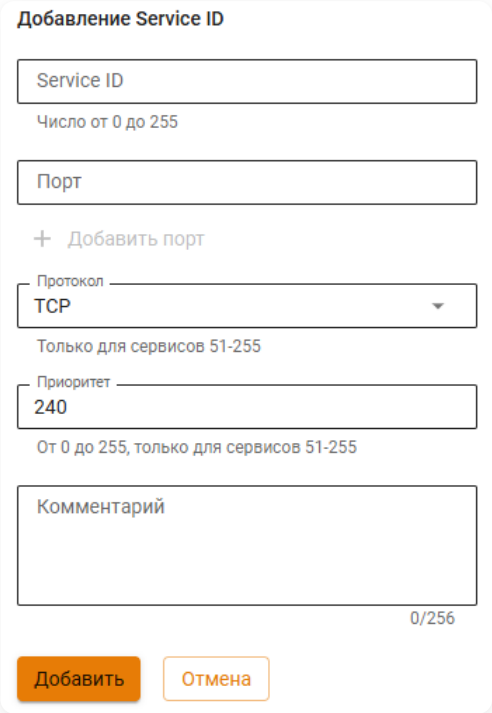


> Service ID с 0 по 50 зарезервированы под фиксированные сервисы. Для них выбирать порты и протоколы нельзя.
>
> Service ID 70 - общепринятое значение для HTTPS-трафика на 443 TCP-порт.

Чтобы настроить Service ID, выполните действия:

1. На вкладке **WCCP Service ID** нажмите кнопку **Добавить**.

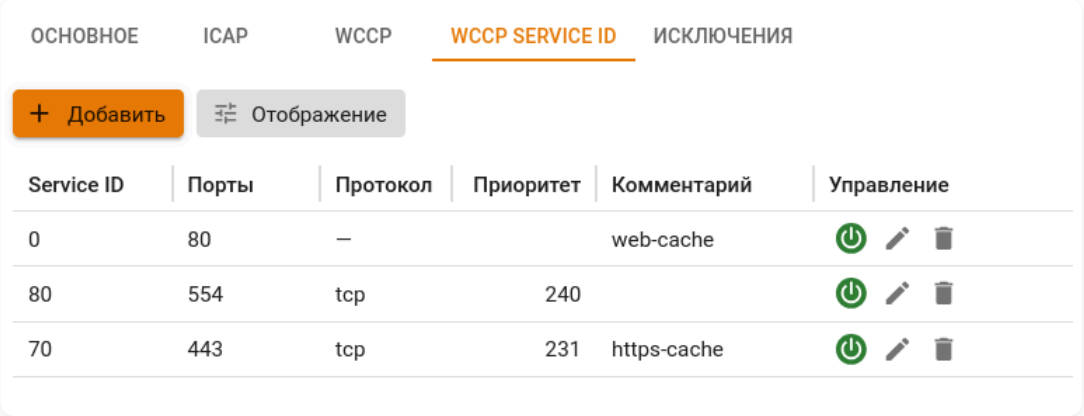
2. В открывшейся форме укажите следующие значения:



- **Service ID** - идентификатор сервисной группы, трафик которой планируется перенаправлять на прокси-сервер. Выбирайте значения от 51 до 255, чтобы избежать проблем со старыми серверами WCCP.
- **Порты** - укажите порты назначения. Максимум 8 значений.
- **Протокол** - укажите протокол для перенаправляемого трафика (TCP, UDP).
- **Приоритет** - укажите приоритет Service ID от 0 до 255. Чем больше число, тем выше приоритет.

Service ID должен соответствовать идентификатору группы, определенному на сервере WCCP.

3. Нажмите **Добавить**. Созданный Service ID появится в таблице:



Исключения

Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

Подробнее о типах исключений в статье Исключения.

Полезные ссылки

- **Настройка Ideco NGFW в качестве прокси с одним интерфейсом**
- **Настройка программы Proxifier для прямых подключений к прокси серверу**

Исключения

Функциональность доступна в **Классическом** и **Системном контекстах**.

Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

На вкладке **Исключения** можно исключить ресурсы из обработки прокси-сервером и всеми связанными службами (контент-фильтр, веб-отчетность, антивирусы):

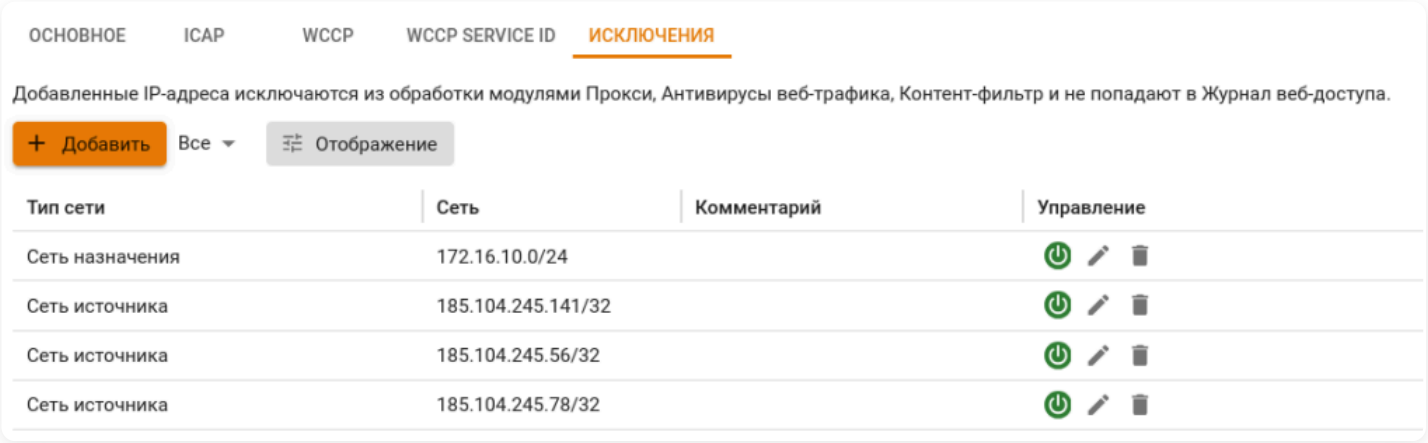
- **Сети источника** - указываются сети, трафик из которых исключается из обработки прокси-сервером.
- **Сети назначения** - указываются внешние сети или IP-адреса (как правило, адреса веб-сайтов или веб-сервисов), трафик до которых из всех локальных сетей NGFW исключается из обработки прокси-сервером.

Настоятельно не рекомендуем исключать из обработки прокси-сервером ВСЮ локальную сеть.

При прямом подключении к прокси-серверу нельзя исключить трафик из обработки прокси. Исключать трафик нужно в настройках прокси-сервера на устройстве (в веб-браузере или системных настройках прокси-сервера).

При создании исключений можно указывать только IP-адреса или IP-сети.

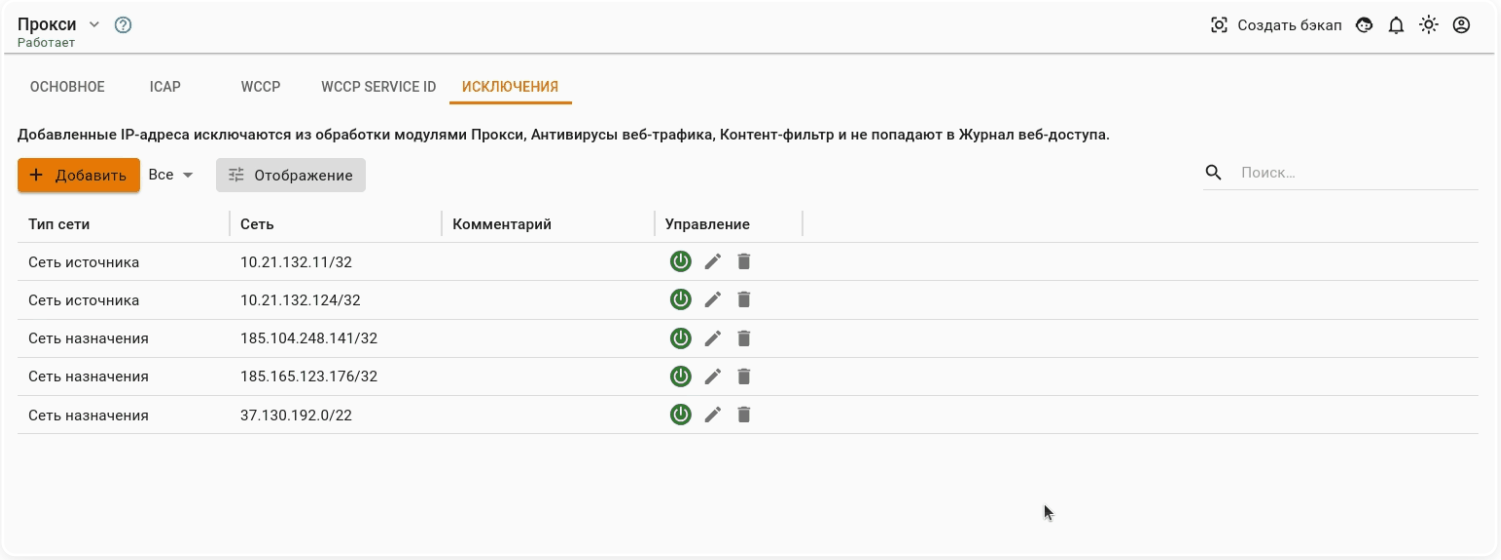
Трафик, исключенный из обработки прокси, не будет участвовать в **Отчетах**, проверяться на вирусы и обрабатываться модулем **Контент-фильтра**. В то же время трафик будет проверен **Межсетевым экраном**, модулями **Предотвращение вторжений** и **Контроль приложений**:



Если добавлено исключение в **Прокси**, соответствующий HTTP(S)-трафик перенаправляется в таблицу **FORWARD** для фильтрации и не попадает в зону **Исходящий трафик устройства**.

Поиск по таблице исключений

Над таблицей исключений расположена строка поиска позволяющая искать среди исключений определенные IP-адреса и сети. Для поиска начните вводить требуемый IP-адрес:



Программы, работающие по отличным от HTTP(S) протоколам через веб-прокси

Некоторые программы, отправляющие трафик на свои серверы по портам 80 и 443, но при этом работающие по протоколам, отличным от HTTP(S), не могут быть обработаны веб-прокси-сервером на NGFW с включенной фильтрацией HTTPS-трафика. Трафик таких программ следует исключать из обработки прокси в поле **Сети назначения**.

1С Коннект

- 185.104.248.141/32
- 185.151.243.218/32
- 185.99.140.108/32
- 185.99.140.101/32
- 185.99.140.102/32
- 185.99.140.103/32
- 185.99.140.104/32
- 185.99.140.105/32
- 185.99.140.106/32
- 185.99.140.107/32
- 185.99.140.108/32
- 185.99.140.114/32
- 185.99.140.115/32
- 193.107.238.195/32
- 77.223.98.83/32
- 77.244.213.204/32
- 78.155.206.40/32
- 78.155.218.78/32
- 80.249.148.135/32
- 88.198.27.15/32
- 88.198.27.27/32
- 88.221.132.128/32
- 92.242.35.35/32
- 46.4.207.211/32
- 2.16.154.81/32
- 185.188.183.87/32
- 185.24.93.122/32
- 185.244.173.25/32
- 185.143.172.61/32

ВЭД-Декларант

- 46.48.116.196/32
- 94.213.21.144/32

- 194.213.21.144/32
- 91.220.57.3/32
- 212.49.126.110/32

MAX

- 104.18.20.226/32
- 104.18.21.226/32
- 155.212.192.0/20
- 185.16.148.119/32
- 185.226.55.94/32
- 5.101.40.2/32

Webinar.ru

- 185.45.80.0/22
- 37.130.192.0/22

vks.samregion.ru

- 195.248.236.141/32

Магазин DNS

- 185.165.123.176/32
- 5.8.69.70/32

СДЭК

- 185.165.123.40/32

Сбербанк Бизнес Онлайн

- 194.54.14.137/32
- 194.54.15.90/32
- 194.186.207.124/32
- 194.186.207.182/32
- 195.8.62.178/32
- 92.38.2.37/32

Яндекс.Телемост

- 37.140.128.0/18
- 37.9.64.0/18
- 5.255.192.0/18
- 5.45.192.0/18
- 37.9.127.0/25
- 5.255.192.0/25
- 5.255.252.0/25
- 37.9.123.192/31
- 5.255.192.176/31
- 5.255.230.32/31

Более подробная информация по настройке Телемоста в корпоративной сети представлена по ссылке.

Обратный прокси

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Обратный прокси**: `ideco-reverse-backend`.

Список служб для других разделов доступен по ссылке.

Технология обратного прокси позволяет перенаправлять веб-трафик из интернета в локальную сеть. Отличия от DNAT:

- Работает на более высоком уровне (используются прикладные протоколы HTTP/HTTPS вместо сетевого протокола IP).
- Позволяет гибко реализовывать публикацию ресурсов.
- Предоставляет дополнительные функции безопасности.
- Позволяет эффективнее управлять трафиком.

Таким образом, имея одну ресурсную A-запись для внешнего сетевого интерфейса Ideco NGFW Novum, можно опубликовать несколько ресурсов в локальной сети, распределив их по нескольким входящим URL.

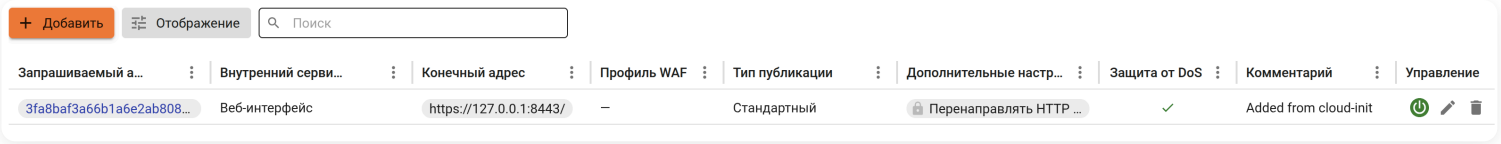
Для публикуемых ресурсов сертификаты не требуют ручной загрузки, Ideco NGFW Novum автоматически отправляет запрос на выпуск сертификата Let's Encrypt. Выпуск сертификата может занять до 20 минут. Сертификаты будут доступны в одноименном разделе.

Создание и настройка правила

Для добавления нового правила:

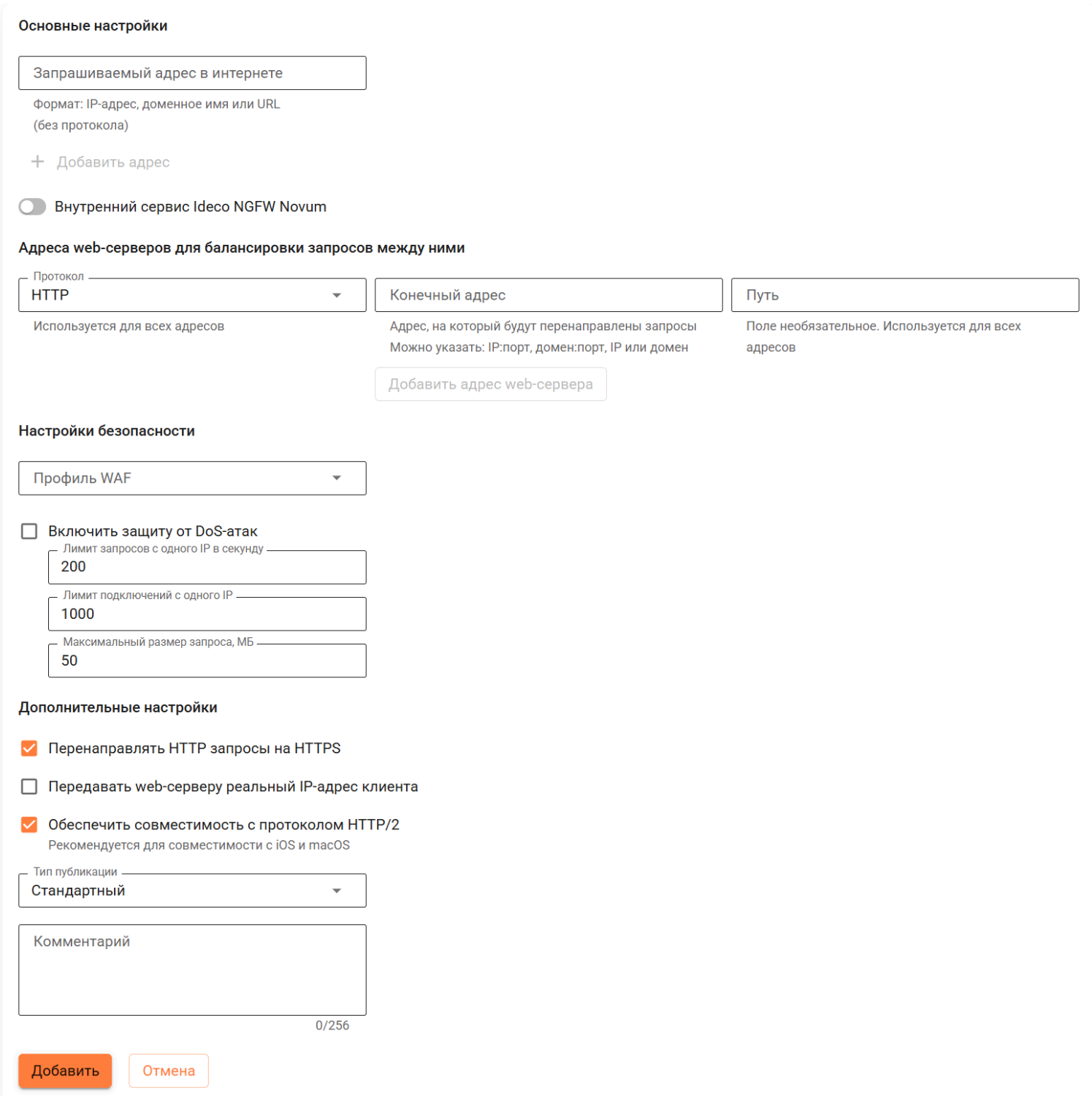
1. Перейдите в раздел **Сервисы → Обратный прокси**.

2. Нажмите **Добавить**:



Форма добавления правила разделена подразделы:

- **Основные настройки**.* **Адреса web-серверов для балансировки запросов между ними**.
- **Настройки безопасности**.
- **Дополнительные настройки**:



Основные настройки

- **Запрашиваемый адрес в интернете** - укажите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями из интернета. Для добавления дополнительных (альтернативных) адресов нажмите кнопку **Добавить адрес**.

При добавлении нескольких правил с одинаковыми значениями в поле **Запрашиваемый адрес в интернете** сработает только одно из созданных правил.

Если требуется опубликовать несколько ресурсов на одном и том же адресе, необходимо указать разные пути после основного IP-адреса/доменного имени/URL.

Пример. Чтобы опубликовать на IP-адресе `192.168.11.1` личный кабинет и почту, при создании правил в поле **Запрашиваемый адрес в интернете** укажите значения:

- Для личного кабинета - `192.168.11.1/cabinet`.

- Для почты - `192.168.11.1/mail`.

- **Внутренний сервис Ideco NGFW Novum** - включите опцию и выберите для публикации один из сервисов Ideco NGFW Novum: Личный кабинет/Портал SSL VPN, Веб-интерфейс или Почта.

Web-серверы для балансировки запросов

- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Конечный адрес** - адрес, на который будут перенаправлены запросы.
- **Путь** - необязательное поле, дописывает путь после **Конечный адрес**.

Если указать в поле **Запрашиваемый адрес в интернете** ***0.0.0.0***, перенаправление будет работать со всех внешних IP-адресов Ideco NGFW Novum на адрес из поля **Конечный адрес**.

Чтобы перенаправление работало с доменов Ideco NGFW Novum на адрес из поля **Конечный адрес**, необходимо явно указать домены в поле **Запрашиваемый адрес в интернете**.

Настройки безопасности

- **Профиль WAF** - позволяет задать параметры защиты веб-ресурса при указании WAF-профиля.
- **Включить защиту от DoS-атак** - опция ограничивает трафик на публикуемый ресурс. Параметры:
  - **Лимит запросов с одного IP в секунду** - от 0 до 4 294 967 295, по умолчанию 200. При превышении будет отправлена ошибка 503 `Service Temporarily Unavailable`. Если число ошибок равно 6 в течение 10 минут, то IP-адрес будет заблокирован на 40 минут. Значение 0 в поле означает, что ограничение по параметру не применяется.
  - **Лимит подключений с одного IP** - от 0 до 65 536, по умолчанию 1000. При превышении будет отправлена ошибка 503 `Service Temporarily Unavailable`. Если число ошибок равно 6 в течение 10 минут, то IP-адрес будет заблокирован на 40 минут. Значение 0 в поле означает, что ограничение по параметру не применяется.
  - **Максимальный размер запроса, МБ** - от 1 до 51 200, по умолчанию 50. Попытка отправить файл или другие данные большего объема приведет к ошибке 413 `Request Entity Too Large`.

При превышении лимита запросов с одного IP или подключений с одного IP после ошибки 503 может возникнуть ошибка `Connection Refused`. Такое поведение является нормальным и ожидаемым результатом совместной работы Nginx и `Fail2Ban`. Эти два механизма работают на разных уровнях сетевого стека и с разной скоростью реагирования.

Пример 1. Настройка строгой защиты от DoS-атак

Защита внутренних административных панелей или критичных API:

- **Лимит запросов с одного IP в секунду** - 50.
- **Лимит подключений с одного IP** - 100.
- **Максимальный размер запроса, МБ** - 10.

Низкие лимиты блокируют атаки, малый размер запроса ограничивает объем данных.

Пример 2. Настройка мягкой защиты от DoS-атак

Публичные API, CDN, сервисы с легитимной высокой нагрузкой:

- **Лимит запросов с одного IP в секунду**: 1000.
- **Лимит подключений с одного IP**: 5000.
- **Максимальный размер запроса, МБ**: 200.

Повышенные лимиты позволяют обрабатывать легитимный трафик, при этом сохраняется защита от явных атак. Увеличенный размер запроса поддерживает загрузку файлов.

Дополнительно

- **Перенаправлять HTTP-запросы на HTTPS** - опция используется, если сайт работает только по протоколу HTTPS. Если опция выключена, посетители, обратившиеся к сайту по HTTP, могут быть потеряны.

Если в поле **Запрашиваемый адрес в интернете** указан URL с путем (например: `example.com/path` или `192.168.111.13/cabinet`), то при включении опции **Перенаправлять HTTP запросы на HTTPS** добавляйте `/` в конец URL (например: `http://example.com/path/` или `192.168.111.13/cabinet/`). Без `/` будет ошибка 404. При использовании HTTPS `/` необязателен.

- **Передавать web-серверу реальный IP-адрес клиента** - при включенной опции для web-сервера передается публичный IP-адрес клиента. Если опция выключена, передается IP-адрес Ideco NGFW Novum. При этом IP-адрес клиента возможно узнать через специальные заголовки в запросах на проксируемые серверы (например, `proxy_set_header X-Forwarded-For $remote_addr`).

> **Web Application Firewall (WAF)** анализирует запросы к сайту и блокирует атаки на уязвимые компоненты веб-приложения (например типы атак OWASP TOP-10). При активации этого модуля также будут блокироваться злоумышленники, ведущие сканирование сайта на уязвимости, с помощью модуля защиты от брутфорс-атак.
>
> Не рекомендуем использовать проброс веб-интерфейса Ideco NGFW Novum через WAF, так как при попытке входа пользователь может быть заблокирован средствами WAF.

- **Обеспечить совместимость с протоколом HTTP/2** - при включении опции будут удалены заголовки `Upgrade`, `Proxy-Connection`, `Keep-Alive` и `Transfer-Encoding`, которые могут вызывать проблемы парсинга у клиентов, строго следующих спецификации `HTTP/2`. Например, встроенные сетевые библиотеки iOS/macOS.
- Поле **Тип публикации** позволяет выбрать один из типов: **Стандартный** или **Outlook Web Access**. Тип **Outlook Web Access** используется для публикации Microsoft Exchange.

В полях **Запрашиваемый адрес в интернете** и **Адрес в локальной сети** для типа **Outlook Web Access** укажите только домены `youdomain.ru` без остальной части URL (она не используется при публикации этим способом).

Если у вас имеется доверенный SSL-сертификат для домена, по которому будет идти обращение извне на публикуемый ресурс, то его можно загрузить в раздел **Сервисы** → **Сертификаты** с помощью кнопки **Добавить**.

Доменные имена, указываемые в поле **Запрашиваемый адрес в интернете**, должны переводиться во внешний IP-адрес сервера Ideco NGFW Novum. Доменные имена, указываемые в поле **Адрес в локальной сети**, должны переводиться в IP-адреса публикуемых ресурсов Ideco NGFW Novum.

> Чтобы исключить IP-адрес из обработки **Защитой от DoS-атак**, обратитесь в Техническую поддержку.

Публикация CMS

Нами протестирована и официально поддерживается публикация сайтов на двух популярных CMS: **Joomla** и **Wordpress**. Подробности публикации каждой CMS описаны ниже.

Joomla

Joomla в текущей реализации публикуется, если настроить перенаправление с внешнего домена на локальный домен без префикса:

- Ассоциировать с внешним адресом Ideco NGFW Novum дополнительное доменное имя специально для публикации Joomla: `joomla.mydomain.ru`.
- Настроить правило публикации `joomla.mydomain.ru` → `joomla.local:port` (порт не обязателен).

WordPress

WordPress в текущей реализации публикуется только в конфигурации, когда в WordPress и в обратном прокси настроен один и тот же домен:

- Для домена компании добавить A-запись `wordpress.mydomain.ru`, указывающую на внешний IP-адрес Ideco NGFW Novum.
- В админ-панели WordPress локального сервера должен быть настроен домен `wordpress.mydomain.ru` на стандартном порту HTTP.
- Добавить в обратный прокси правило публикации `wordpress.mydomain.ru` → `wordpress.mydomain.ru`.

Публикация Nextcloud

Для корректной работы Nextcloud с устройствами Apple добавьте в конфигурацию Nginx следующие строки:

```
location /.well-known/carddav {
    return 301 $scheme://$host/remote.php/dav;
}

location /.well-known/caldav {
    return 301 $scheme://$host/remote.php/dav;
}

location ^~ /.well-known {
    return 301 $scheme://$host/index.php$uri;
}
```

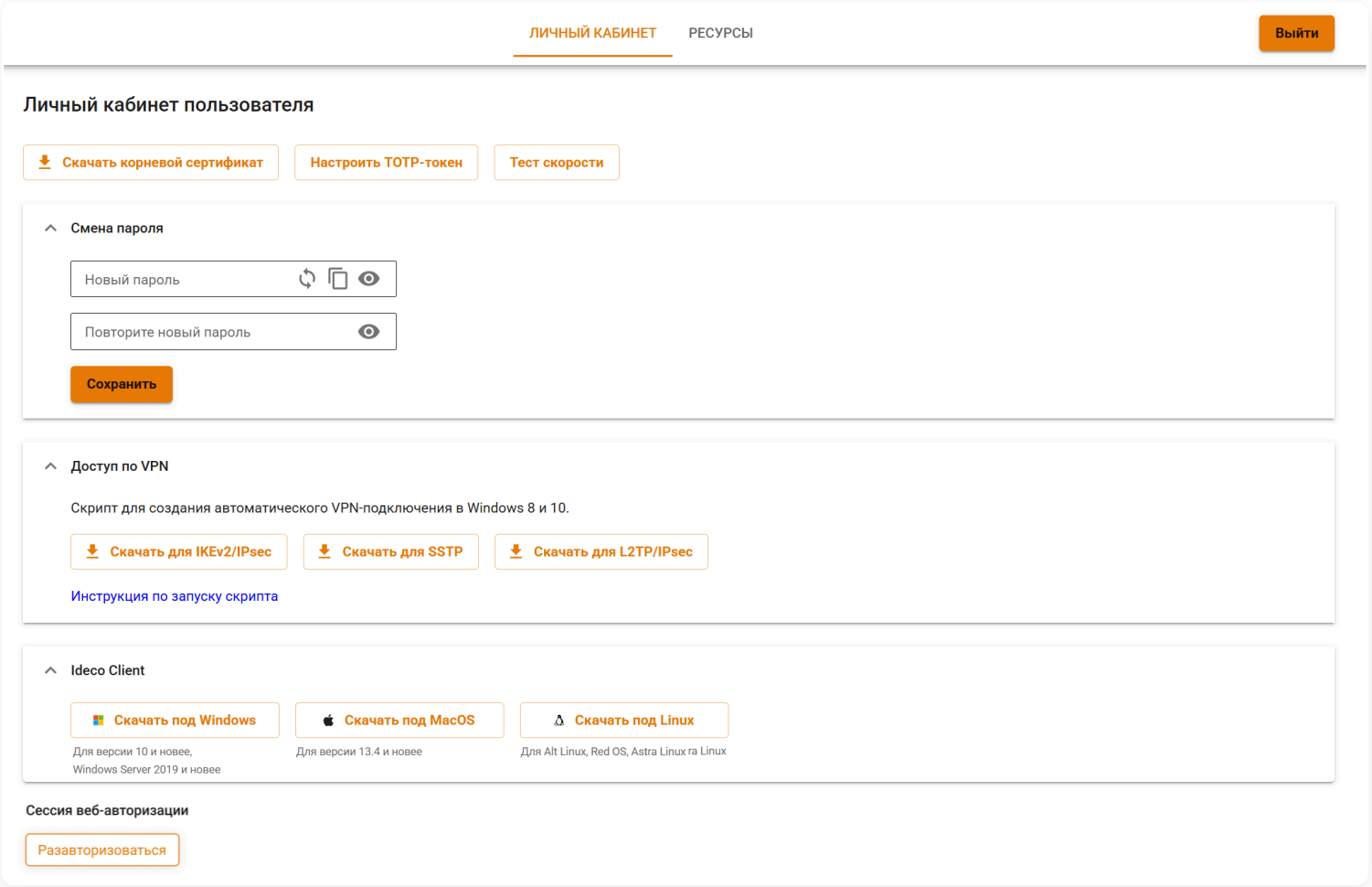
При использовании NGINX Proxy Manager добавьте в **Custom Nginx Configuration** → **Advanced Settings** запись `proxy_hide_header Upgrade;`, иначе мобильные устройства от Apple будут получать сообщение об ошибке **Connection Closed**.

ЛК/Портал SSL VPN

Классический контекст | Высокопроизводительный контекст | API

Портал SSL VPN предоставляет удаленным пользователям безопасный доступ к внутренним ресурсам, выступая в роли защищенной точки входа в корпоративную сеть.
Возможности личного кабинета Ideco NGFW Novum:

- **Скачивание корневого сертификата**.
- **Генерация TOTP-токена**. Для настройки двухфакторной аутентификации воспользуйтесь статьей.
- **Тестирование скорости**. При нажатии на Тест скорости откроется меню тестирования скорости между хостом и NGFW Novum.
- **Смена пароля**.
- **Скачивание скриптов для создания автоматического VPN-подключения в Windows 8 и 10**. Будут доступны скрипты настройки только тех типов подключения, которые указаны для пользователя в таблице **Доступ по VPN** в разделе **Пользователи → VPN-подключения**.
- **Скачивание Ideco Client**. Подробнее о работе в Ideco Client - в статье.
- **Деавторизация**. Деавторизация пользователя в сети NGFW Novum, если пользователь был авторизован через Web/SSO.



Поддерживаемые версии браузеров:

- Google Chrome версия 109 и выше
- Firefox версия 115 и выше
- Safari версия 15.4 и выше

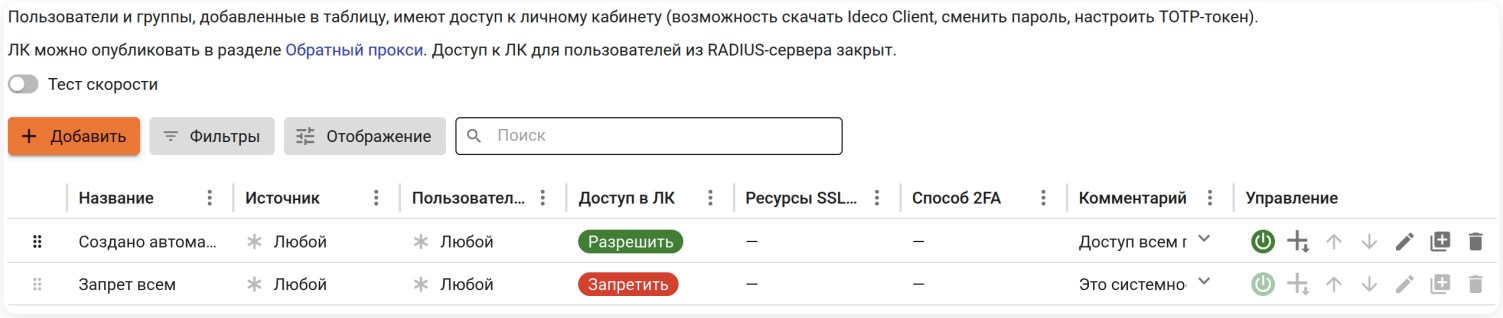
Настроить доступ пользователей в личный кабинет можно в **Сервисы** → **ЛК/Портал SSL VPN** → **Правила доступа**. Для этого необходимо создать **Правило доступа**, а затем опубликовать личный кабинет через **Обратный прокси**, чтобы пользователи получили к нему доступ. VPN-подключение не требуется, пользователь авторизуется через логин и пароль.

Настройка доступа в личный кабинет Ideco NGFW Novum

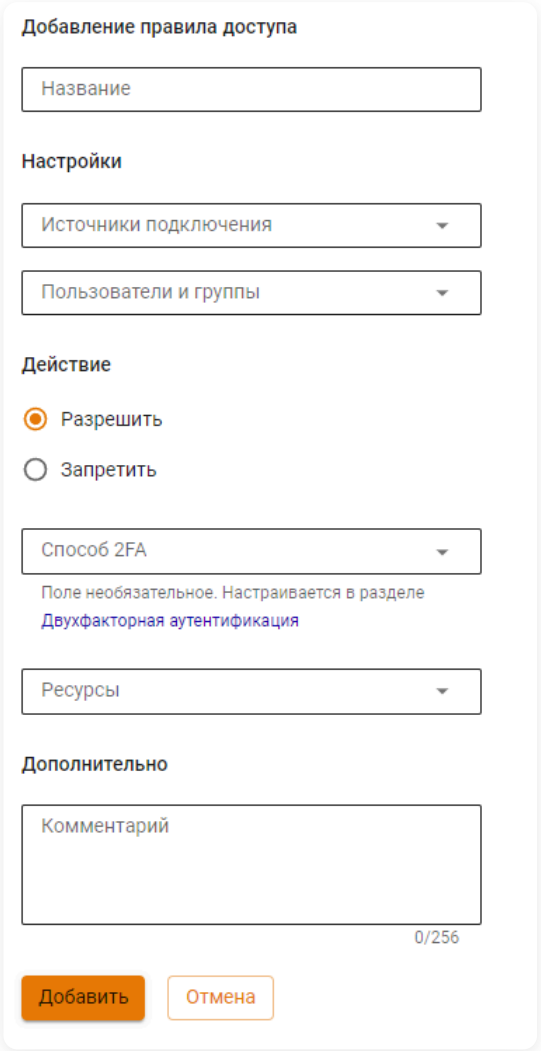
В разделе **Сервисы** → **ЛК/Портал SSL VPN** можно настроить доступ в личный кабинет.

Правила доступа

По умолчанию в таблице настроено правило доступа к личному кабинету для всех пользователей:



Для создания правила нажмите **Добавить** и заполните необходимые поля:



Расшифровка полей

- **Название** - укажите название правила доступа.
- **Источники подключения** - укажите IP-адреса, подсети, страны или домены.
- **Пользователи и группы** - выберите пользователей, группы пользователей, группы безопасности из AD, которым хотите предоставить доступ в личный кабинет.

- **Способ 2FA** - выберите метод двухфакторной аутентификации. Поле может быть пустым.
- **Ресурсы** - укажите необходимые ресурсы, созданные в **ЛК/Портал SSL VPN** → **Ресурсы**. Поле может быть пустым.
- **Комментарий** - произвольный текст, не более 256 символов.

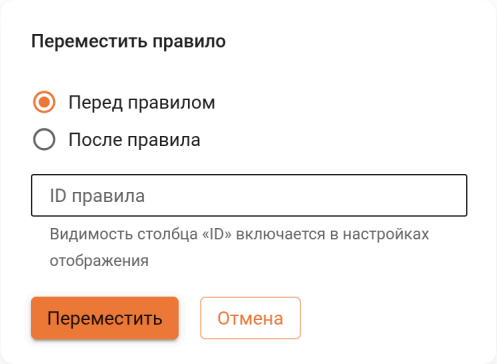
Если у пользователей приватные (серые) IP-адреса, не указывайте в качестве источника страну. Это связано с тем, что такие адреса не относятся к диапазонам IP-адресов ни одной страны и доступ к ним будет запрещен. Рекомендуется использовать диапазон IP-адресов.

Для перемещения правил выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

При наличии большого количества правил доступа в таблице воспользуйтесь кнопкой **Фильтры**.

Как обрабатываются правила:

1. При входе пользователя в ЛК правила проверяются сверху вниз до первого совпадения по полям **Источник** и **Пользователи и группы**.

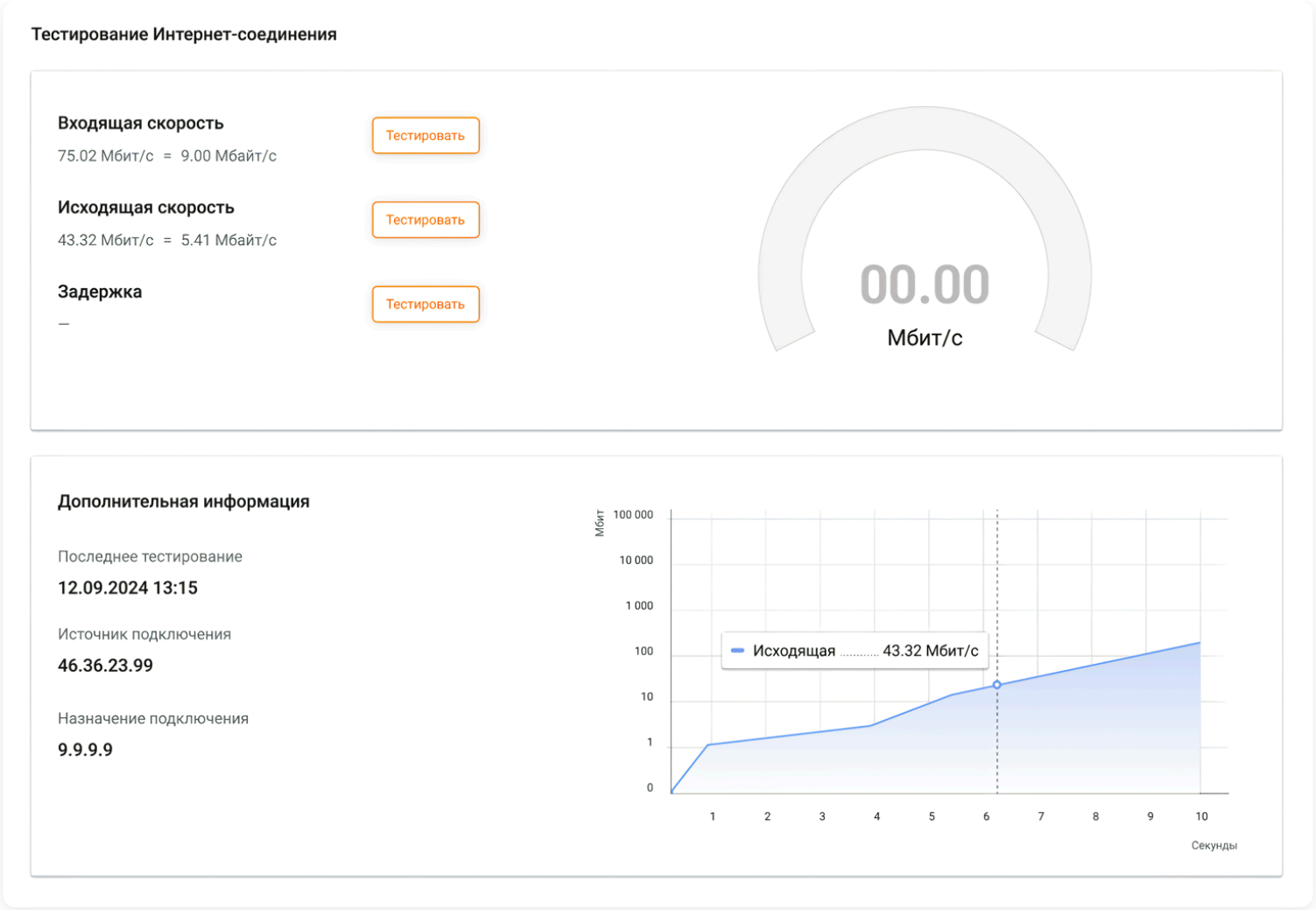
2. Если правило разрешающее, то доступные пользователю в ЛК ресурсы определяются этим правилом. Последующие правила с такими же полями учитываться не будут.

3. Доступ пользователя или группы пользователей к ресурсу определяется заново при изменении таблицы, пользователей и состава групп.

Тест скорости

Опция **Тест скорости** позволяет добавить в личный кабинет функцию проверки скорости интернет-соединения.

В **Тестирование интернет-соединения** пользователь может проверить входящую и исходящую скорость интернет-соединения, а также задержку (ping):



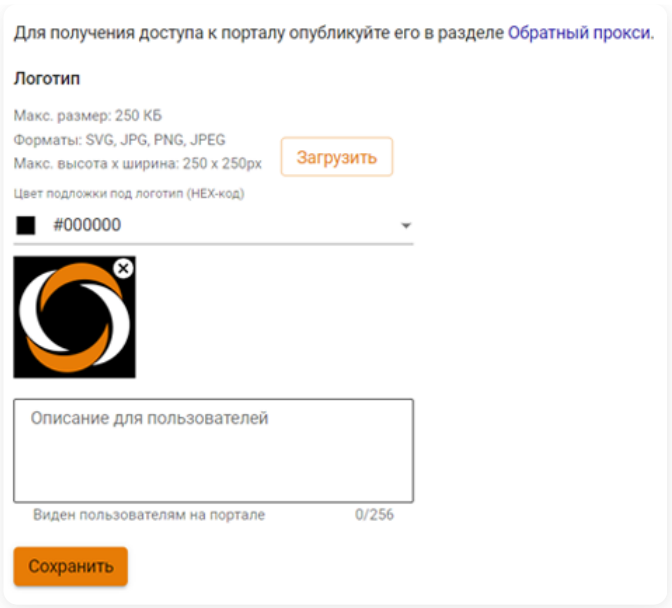
- **Последнее тестирование** - дата и время любого последнего теста.
- **Источник подключения** - IP-адрес пользователя.
- **Назначение подключения** - IP-адрес NGFW Novum.

Особенности работы:

- Продолжительность каждого теста составляет 10 секунд.
- Тесты запускаются последовательно, в каждый момент времени может быть активен только один тест.
- График обнуляется в момент запуска нового теста.

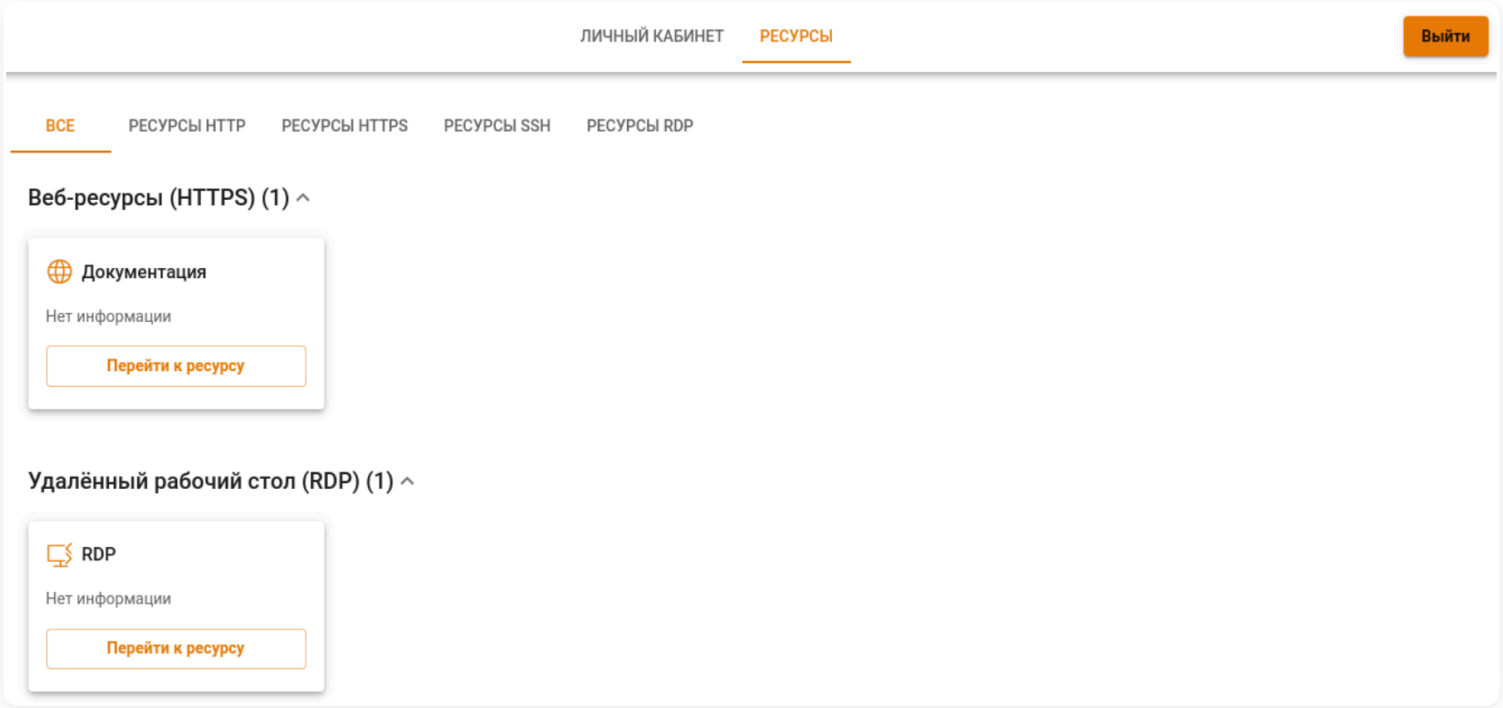
Внешний вид

На вкладке можно настроить внешний вид портала: изменить логотип и добавить описание, которое отображается рядом с логотипом:



Ресурсы

В личном кабинете Ideco NGFW Novum размещаются только внутренние ресурсы, доступные из локальной сети NGFW Novum. Ресурсы становятся доступны пользователям только после успешной авторизации и при наличии соответствующего разрешения в правилах доступа:

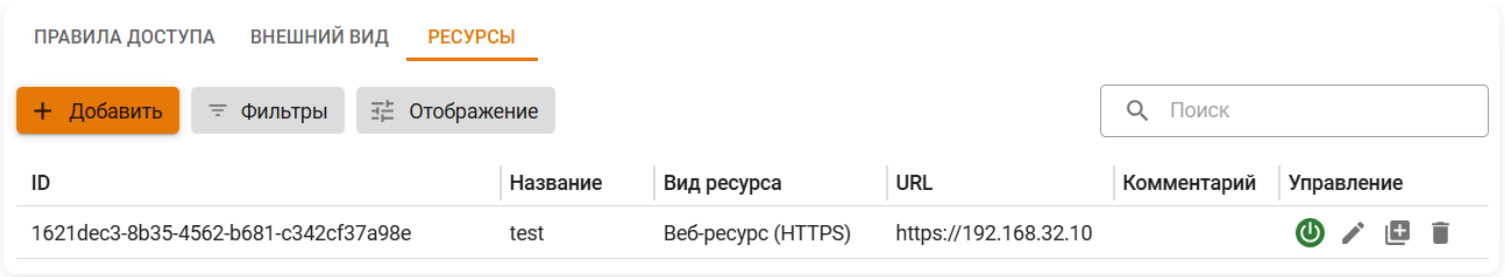


Веб-ресурсы HTTP(S) в SSL VPN работают по принципу **Обратного прокси** ЛК/SSL VPN.

Требования к URL в HTML-коде страниц веб-ресурсов HTTP(S) в ЛК/SSL VPN

URL, которые содержатся в HTML-коде веб-страниц публикуемого внутреннего ресурса (ссылки, картинки, скрипты, стили и т.д.), должны соответствовать одному из требований:

- URL относительные, не зависят от домена и пути. В этом случае браузер дополнит ссылки до полных с учетом домена и пути публикации ЛК.
- URL изначально доступны через интернет. Например, CDN для скриптов и картинок, которые используются ресурсом. Если URL ведут на внешние сайты, то трафик пойдет не через NGFW Novum.
- URL учитывают, что сайт публикуется через ЛК по определенному пути - `https://<домен_порт_публикации_ЛК>/<путь_публикации_ЛК>/resources/<resource_id>/..`. Идентификатор ресурса (`resource_id`) используется для публикации ресурса в ЛК, доступен для просмотра в столбце ID на вкладке **Ресурсы**. По умолчанию столбец в таблице не указан, можно настроить с помощью кнопки **Отображение**:

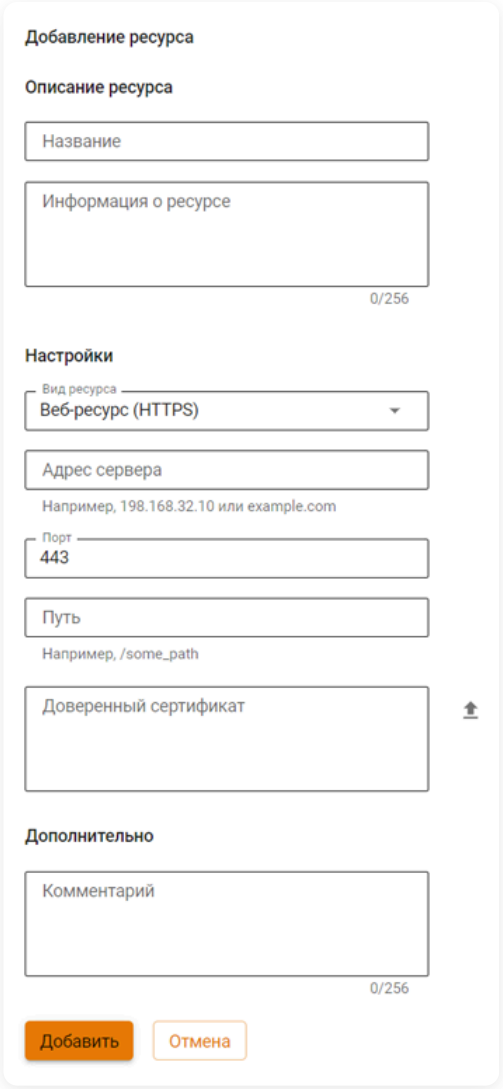


В случае несоответствия URL перечисленным требованиям публикуемый ресурс будет отображаться некорректно, т.к. браузер пользователя не сможет получить некоторые данные с этих URL (например, файлы CSS и JS).

Пример. Личный кабинет опубликован по адресу `example.com/site`, доступен ресурс HTTPS с ID `123`. Адрес, по которому пользователь переходит к ресурсу в личном кабинете - `https://example.com/site/resources/123/`. URL, которые соответствуют требованиям:

- Относительный URL `mysite/main/index.html`. Браузер дополняет ссылку до `https://example.com/site/resources/123/mysite/main/index.html`.
- Абсолютный URL `https://example.com/site/resources/123/mysite/pictures/image.png`. Публикуемый ресурс распознает опубликованные домен и путь, сразу формирует полную ссылку.

Чтобы добавить ресурс, перейдите в **Сервисы** → **ЛК/Портал SSL VPN** → **Ресурсы**, нажмите **Добавить** и заполните поля:



Расшифровка полей

Описание ресурса:

- **Название** - имя ресурса, может содержать до 42 символов.
- **Информация о ресурсе** - укажите текстовое описание, которое будет отображаться в личном кабинете, или оставьте поле пустым.

Настройки:

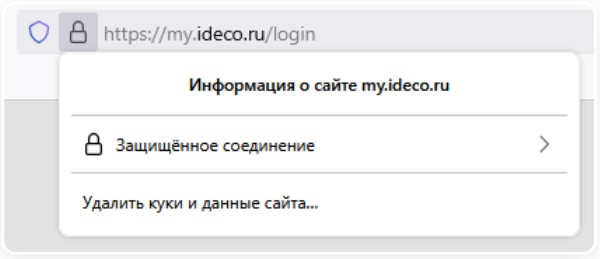
- **Вид ресурса** - **Веб-ресурс (HTTPS)**:

    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `443`.
    - **Путь** - укажите путь. Поле не является обязательным.
    - **Доверенный сертификат** - загрузите доверенный сертификат. Поле не является обязательным.
- **Вид ресурса** - **Веб-ресурс (HTTP)**:
    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `80`.
    - **Путь** - укажите путь. Поле не является обязательным.
- **Вид ресурса** - **Удаленный доступ (SSH)**:
    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `22`.
    - **Отпечаток ключа** - загрузите отпечаток ключа.
- **Вид ресурса** - **Удаленный рабочий стол (RDP)**:
    - **Адрес сервера** - укажите доменное имя или IP-адрес сервера.
    - **Порт** - по умолчанию значение `3389`.
- **Дополнительно:**
    - **Комментарий** - поле может быть пустым.

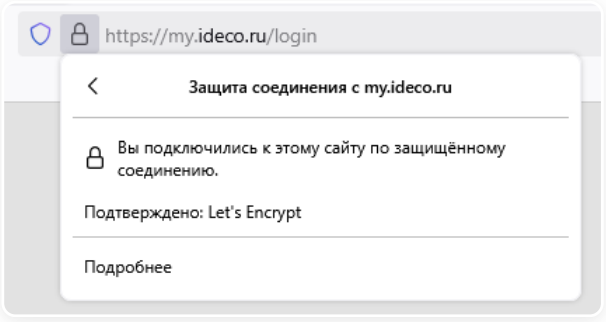
Где скачать доверенный сертификат

Пример скачивания сертификата в браузере Firefox:

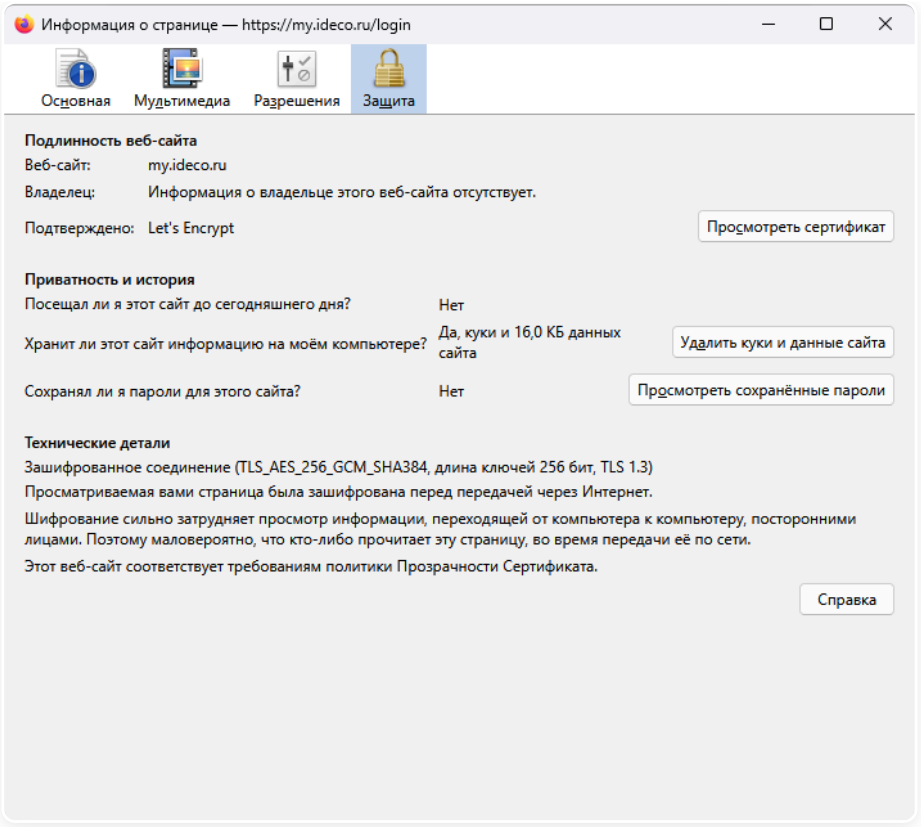
1. Нажмите в адресной строке браузера на значок с замком и выберите **Защищенное соединение**:



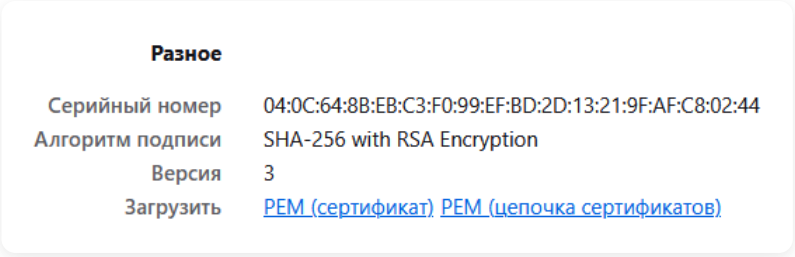
2. Нажмите **Подробнее**:



3. На вкладке **Защита** нажмите **Просмотреть сертификат**:



4. В разделе **Разное** скачайте сертификат из строки **Загрузить**:



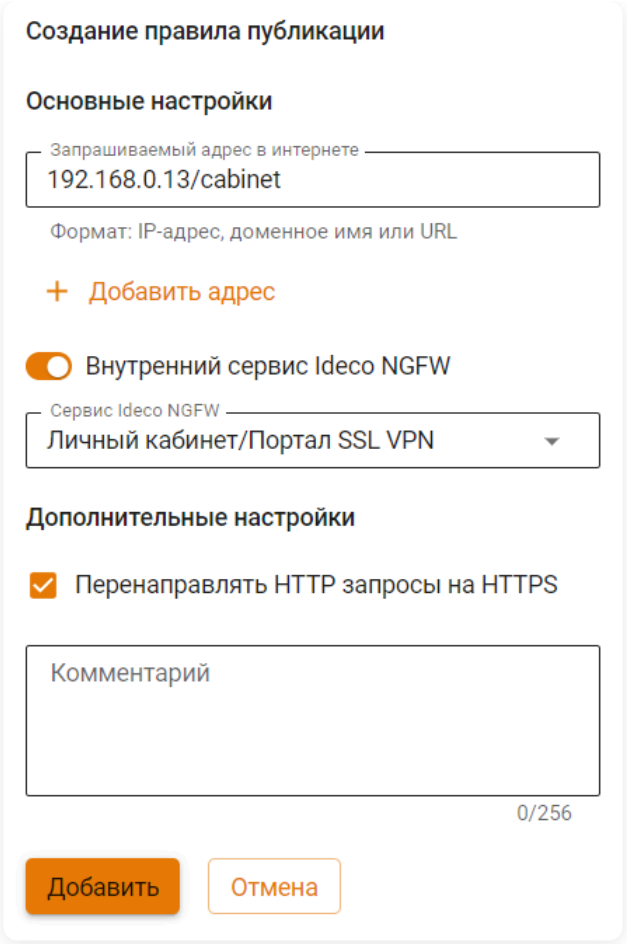
Адреса, на которые ссылается HTTP/HTTPS-ресурс, должны быть относительными во избежание нарушения CORS. Подробнее про CORS.

Публикация личного кабинета

Чтобы пользователи получили доступ в личный кабинет, он должен быть опубликован. Для публикации ЛК перейдите в **Сервисы** → **Обратный прокси** и выполните действия:

1. Нажмите **Добавить** и включите опцию **Внутренний сервис Ideco NGFW Novum**.

2. В поле **Запрашиваемый адрес в интернете** введите адрес, по которому хотите опубликовать личный кабинет:



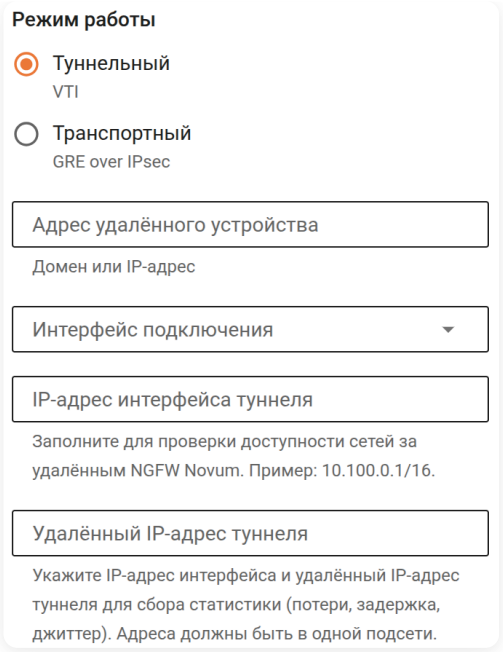
Чтобы система могла отличать личный кабинет от других ресурсов, опубликованных на данном адресе, следует указывать путь после основного IP-адреса/доменного имени/URL - например, `/cabinet`. Это обеспечивает корректную маршрутизацию. Подробнее - в статье.

3. Включите опцию **Перенаправлять HTTP-запросы на HTTPS**. Личный кабинет доступен только по HTTPS. При обращении по HTTP без перенаправления отобразится ошибка подключения.

Если в поле **Запрашиваемый адрес в интернете** указан URL с путем (например: `example.com/path` или `192.168.111.13/cabinet`), то при включении опции **Перенаправлять HTTP запросы на HTTPS** добавляйте `/` в конец URL (например: `http://example.com/path/` или `192.168.111.13/cabinet/`). Без `/` будет ошибка 404. При использовании HTTPS `/` необязателен.

4. Нажмите **Добавить**.

5. Для доступа пользователей к ресурсам в личном кабинете, которые расположены на удаленном хосте за IPsec-туннелем, необходимо заполнить поля в IPsec для входящего и исходящего подключения:



- **IP-адрес туннельного интерфейса** - укажите IP-адрес интерфейса туннеля на сервере, через который требуется получить доступ к ресурсам.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля на удаленном сервере, к ресурсам которого требуется получить доступ.

После этого пользователь сможет зайти в личный кабинет по логину и паролю либо через авторизацию в сети NGFW Novum.

Вход в личный кабинет Ideco NGFW Novum

Личный кабинет пользователя будет доступен по ссылке, указанной при публикации через **Обратный прокси**.

Чтобы зайти в личный кабинет, выполните действия:

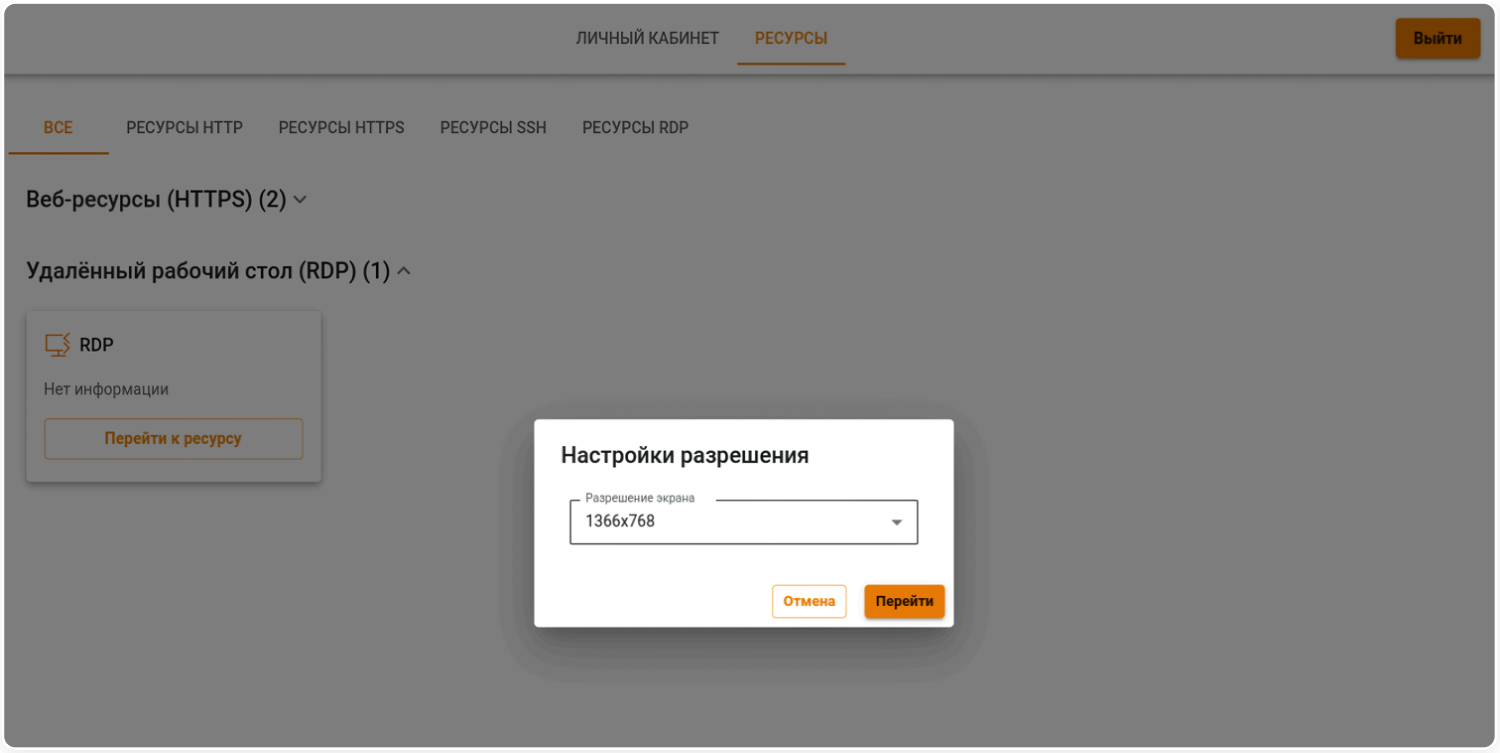
1. Перейдите по ссылке, указанной в правиле публикации личного кабинета.

2. В открывшейся форме авторизации введите логин и пароль пользователя.

Если пользователь уже авторизован в сети NGFW Novum, то логин и пароль вводить не потребуется, личный кабинет откроется сразу.

Настройка разрешения экрана

При подключении пользователя к ресурсу через удаленный рабочий стол (RDP) доступен выбор разрешения экрана:



Доступные настройки разрешения:

- 1920x1080
- 1366x768 (по умолчанию)
- 1024x768

DNS

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **DNS**: `ideco-dns-backend`, `unbound`, `nsd`, `unbound-anchor`, `unbound-keygen`, `ideco-dns-dnstap-reader`.

Список служб для других разделов доступен по ссылке.

Настройка выполняется в **Сервисы** → **DNS** на вкладках:

- **Внешние DNS-серверы** - позволяют указать DNS-серверы во внешних сетях, через которые будут разрешаться доменные имена, запрашиваемые из локальных сетей.
- **Forward-зоны** - позволяют указать сторонние DNS-серверы (в локальных или внешних сетях относительно NGFW) с указанием конкретных DNS-зон, которые эти серверы обслуживают. Перечисленные возможности DNS-сервера могут использоваться одновременно.
- **Master-зоны** - позволяют настроить полнофункциональный DNS-сервер, разрешающий имена в IP-адреса сетевых устройств в локальной сети.
- **DDNS** - обеспечивает доступ по доменному имени к устройствам с изменяющимся IP-адресом. В Ideco NGFW реализован через интеграцию с хостингом RU-CENTER.

При наличии большого количества Forward- и Master-зон в таблицах воспользуйтесь кнопкой **Фильтры**.

Полезные ссылки

- **Интеграция NGFW и SkyDNS**
- **Подключение через Ideco Client к внутреннему DNS**
- **Пример настройки Forward-зоны**

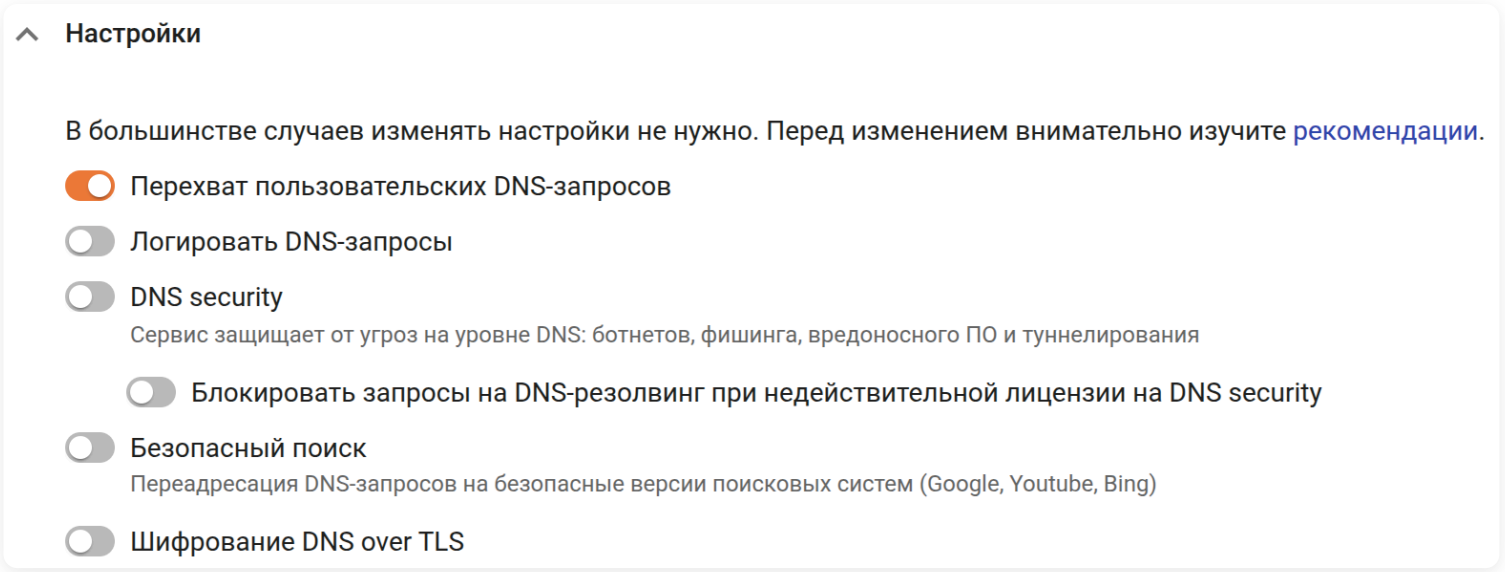
Внешние DNS-серверы

Классический контекст | Высокопроизводительный контекст

По умолчанию внешние DNS-серверы не указаны, и сервер разрешает имена в интернете, используя корневые DNS-серверы. В большинстве случаев изменять настройки не требуется.

Настройки

При необходимости измените настройки работы с внешними DNS-серверами:



Перехват пользовательских DNS-запросов

Включите опцию, чтобы все DNS-запросы пользователей принудительно направлялись на NGFW Novum, даже если на рабочей станции настроен другой DNS-сервер. **Перехват пользовательских DNS-запросов** позволяет контролировать защиту и функциональность DNS централизованно и независимо от потенциально вредоносных настроек.

Для VPN-пользователей опция **Перехват пользовательских DNS-запросов** будет работать только если в настройках VPN включена опция **Отправлять весь трафик на Ideco NGFW Novum**.

Включение перехвата пользовательских DNS-запросов блокирует использование DNS-over-TLS (DoT), DNS-over-QUIC (DoQ) и DNS-over-HTTPS (DoH) для трафика между пользователями и NGFW Novum.

При включенной опции **Перехват пользовательских DNS-запросов** трафик обрабатывается не как FORWARD, а как INPUT. Поэтому для корректной фильтрации трафика модулями **Контроль приложений** создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

Безопасный поиск

При резолвинге NGFW Novum будет возвращать адреса поисковых систем (Google, Youtube, Bing) с включенной фильтрацией нежелательного контента.

Шифрование DNS over TLS (DoT)

Опция включает шифрование DNS-запросов и ответов между NGFW Novum и DNS-сервером с помощью протокола TLS (порт 853). Опция работает только для DNS-серверов, указанных в разделе **Внешние DNS**, и не работает для серверов в FORWARD-зонах, а также корневых серверов. При этом:

- Никто не сможет перехватить и прочитать, какие сайты посещает клиент.
- Никто не сможет изменить DNS-ответ и перенаправить клиента на мошеннический сайт.

Необходимо учитывать, что шифрование добавляет дополнительный слой обработки, что может влиять на скорость резолвинга доменов.

Логировать DNS-запросы

Опция фиксирует обращения к DNS-серверам, которые проходили через Ideco NGFW Novum. Работает при указании адреса NGFW Novum как DNS-сервера либо при включенной опции **Перехват пользовательских DNS-запросов**. События отображаются в журнале DNS-запросы. Настройка полезна для отслеживания и анализа обращений к DNS-серверам, диагностики проблем с доступом к веб-ресурсам или мониторинга использования конкретных доменных имен.

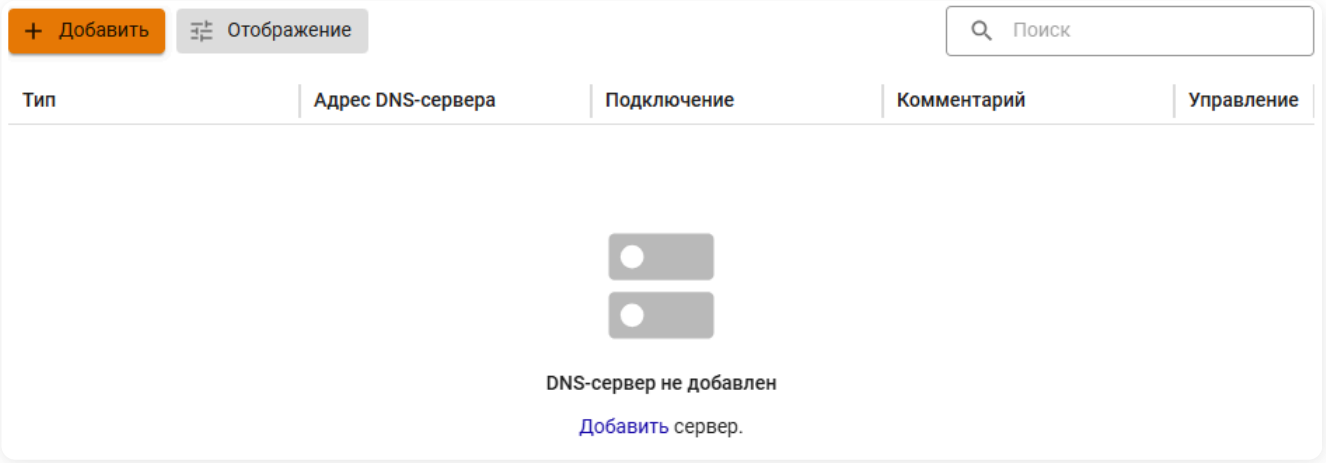
DNS security

Подробная информация в статье DNS security.

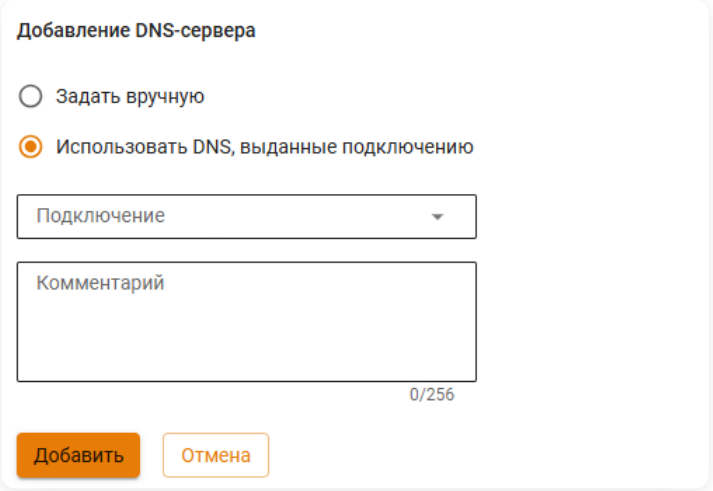
Рекомендации

- В Ideco NGFW Novum встроен кеширующий DNS-сервер. Рекомендуется использовать кеширующий DNS-сервер в качестве DNS-сервера для локальной сети, указав IP-адрес Ideco NGFW Novum в качестве DNS-сервера пользователям.
- Если интернет-провайдер или вышестоящее устройство блокирует DNS-запросы, то использование стандартной конфигурации с корневыми серверами невозможно. Рекомендуем задать серверы вручную или использовать DNS-серверы, выданные провайдером:

1. Нажмите **Добавить**:



2. Выберите **Задать вручную** или **Использовать DNS, выданные подключению**, указав нужное подключение:



- Не указывайте `8.8.8.8`, `1.1.1.1` или подобные известные DNS-серверы без необходимости. Ideco NGFW Novum справится с резолвингом самостоятельно.
- По возможности не используйте DNS, выданные интернет-провайдером, так как DNS, выданные интернет-провайдером, превышают TTL и долго отвечают. Ideco NGFW Novum настроит автоматически все необходимое для подключения к PPTP/L2TP через доменное имя. Если нужна особая внутренняя доменная зона провайдера, то создайте Forward-зону.
- Укажите фильтрующие DNS-серверы, если необходимо (SkyDNS или Яндекс-DNS).
- Не используйте DNS-серверы контроллера домена, даже если домен может самостоятельно разрешать доменные имена в интернете. Это необходимо для эффективного разрешения внутренних имен домена при интеграции с AD. Для резолвинга особых зон, не связанных с AD, создайте Forward-зону вручную.

Сторонние DNS-серверы для дополнительной фильтрации трафика

- SkyDNS при выключенном DNS-over-TLS `193.58.251.251`.
- SkyDNS при включенном DNS-over-TLS `193.58.251.10`.
- Yandex DNS `77.88.8.88`, `77.88.8.2`.
- Google DNS `8.8.8.8`, `8.8.4.4`.
- OpenDNS `208.67.222.222`, `208.67.220.220`, `208.67.222.220`, `208.67.220.222`.
- Cloudflare DNS `1.1.1.1`, `1.0.0.1`.

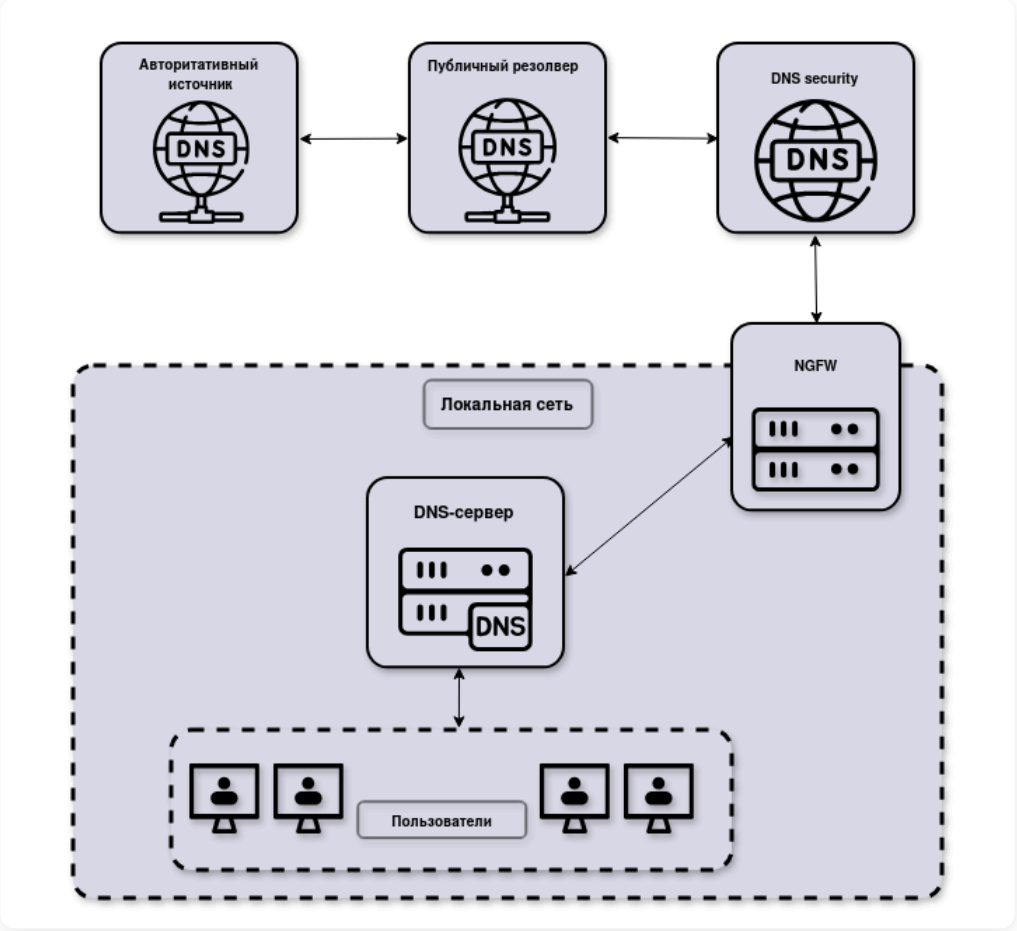
DNS security

Классический контекст | Высокопроизводительный контекст

Модуль должен быть включен в лицензию.

DNS Security - сервис, который защищает от угроз на уровне DNS: ботнетов, фишинга, вредоносного ПО, туннелирования и воровства данных.

Разрешение внешних DNS-доменов всегда работает через сторонние DNS-серверы в интернете. При включении опции **DNS security** облачный сервис выступает посредником между NGFW Novum и этими серверами. Схема DNS-трафика:



Использование функции защиты не делает функциональность NGFW Novum зависимой от интернета, но создает зависимость от облачной инфраструктуры. Отказоустойчивость и высокая доступность обеспечиваются за счет динамической маршрутизации BGP Anycast, которая автоматически направляет трафик к ближайшему доступному облачному узлу. Облачная инфраструктура распределена между узлами, расположенными на территории Российской Федерации.

Доступ к облаку предоставляется исключительно через зашифрованные соединения (DoT), что дополнительно усиливает безопасность.

Сервис **DNS security**:

- Позволяет предиктивно блокировать до 34% угроз на уровне DNS.
- Обеспечивает отказоустойчивость.
- Автоматически блокирует новые и подозрительные домены по мере их появления.
- Постоянно адаптируется к новым угрозам с помощью AI/ML-алгоритмов.
- Сокращает слепые зоны, защищая устройства без антивирусных агентов: промышленные контроллеры, датчики, камеры и офисную периферию.
- Автоматически обнаруживает и блокирует DNS-туннели за 5-10 минут, предотвращая эксфильтрацию данных.
- Блокирует переходы на зараженные сайты по фишинговым ссылкам еще до соединения.

- Автоматически реагирует на компрометацию сети, блокируя подозрительные соединения с C&C-серверами и домены, созданные алгоритмом (DGA).
- Шифрует DNS-запросы через DoH/DoT и использует DNSSEC, исключая перехват, подмену запросов и скрытые перенаправления.
- Обеспечивает глубокую аналитику DNS-трафика, ускоряет расследование инцидентов и снижает риск повторных атак.
- Не имеет доступа к приватной информации и не сохраняет ее.
- Не несет дополнительных рисков безопасности.
- Не вызывает значимой задержки или ухудшения работы.

Защита на уровне DNS выявляет и блокирует следующие угрозы:

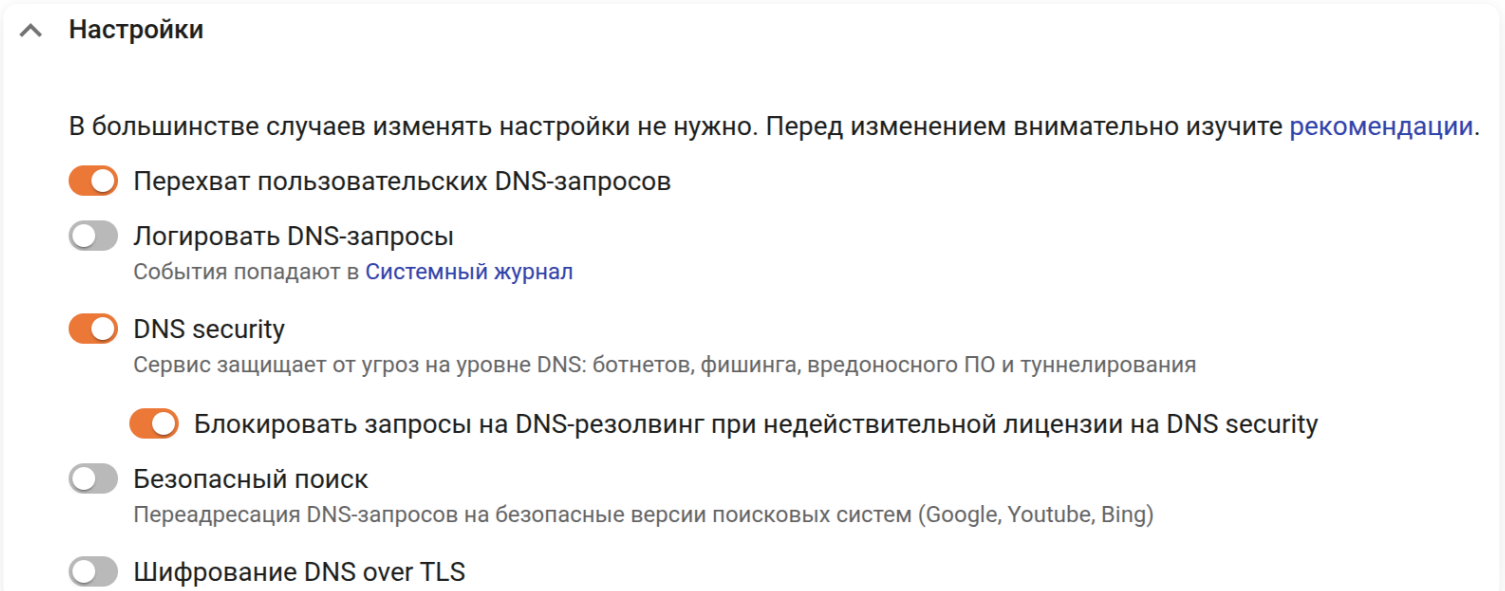
Типы угроз

Тип	Описание
DNS-туннелирование	Скрытая передача данных через DNS-запросы, используемая для кражи информации и управления зараженными системами
Недавно зарегистрированные домены	Домены, созданные менее 90 дней назад вручную или с помощью алгоритмов (DGA), которые не успевают попасть в базы угроз и воспринимаются как легитимные. Активно используются злоумышленниками для фишинга, построения C2-инфраструктуры и распространения вредоносного ПО
Botnets & C2	Распределенная сеть зараженных устройств, управляемых через командные и управляющие серверы (C2) для выполнения вредоносных действий
Cryptojacking	Скрытая атака, при которой ресурсы чужих устройств используются для майнинга криптовалюты без ведома владельца, что замедляет работу устройств и увеличивает энергопотребление
DGA	Алгоритм автоматической генерации доменных имен, используемых злоумышленниками для управления ботнетами, координации атак и распространения вредоносного ПО
Malware (Malicious Software)	Общее название для вредоносных программ, включая вирусы, трояны, шпионское ПО и ransomware, используемых для кражи данных, разрушения систем или получения удаленного доступа к устройствам
Phishing	Мошенничество через поддельные сайты, письма или сообщения с целью кражи логинов, паролей, данных карт или установки вредоносного ПО
Typosquatting	Регистрация доменов, похожих на легитимные, чтобы воспользоваться ошибками пользователей и похищать данные или показывать нежелательную рекламу
Ransomware	Вредоносное ПО, которое шифрует файлы жертвы и требует выкуп за их восстановление. Часто распространяется через фишинг или уязвимости, при этом оплата выкупа не гарантирует возврат данных
Запаркованные домены	Приобретенные, но неиспользуемые домены, которые могут применяться для фишинга, размещения вредоносного ПО или командных серверов злоумышленников

Настройка

1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы**.

2. Включите опцию **DNS Security**:



3. Включите опцию **Перехват пользовательских DNS-запросов** или укажите IP-адрес NGFW Novum как DNS-сервер на клиентских устройствах для фильтрации запросов.

4. Включите опцию **Блокировать запросы на DNS-резолвинг при недействительной лицензии на DNS security** для блокировки DNS-запросов в случае недействительной лицензии.

Важно

Если опция включена и лицензия недействительна:

- Доступ в интернет по доменным именам прекращается.
- Прямые подключения по IP-адресам продолжают работать.

При выключенной опции выполняется откат на обычный DNS-резолвинг без фильтрации **DNS Security**.

Результаты блокировки отображаются в столбце **Результат DNS Security** журнала **DNS-запросы**.

Отключите опцию **DNS Security**, если разрешение внешних доменов через интернет не требуется.

Особенности

При включении **DNS security**:

- Не будут использоваться заданные в таблице **Внешние DNS-серверы** или выданные провайдером DNS-серверы.
- Опция **Шифрование DNS over TLS** не имеет смысла, так как к соответствующим серверам подключений не будет.
- В браузере появится сообщение о недоступности ресурса при его блокировке.
- Если нужная запись есть в DNS-кеше NGFW Novum, резолвинг выполняется из кеша без обращения к облаку.

Если **DNS security** блокирует ресурс, который не должен быть заблокирован, обратитесь в Техническую поддержку.

При включении **DNS security** NGFW Novum обращается к адресу `193.58.251.10` на 853 TCP-порт. Убедитесь, что доступ не блокируется политиками безопасности.

Master-зоны

Классический контекст | Высокопроизводительный контекст

Master-зоны позволяют использовать Ideco NGFW Novum как сервер имен и переводить IP-адреса в доменные имена внутри сети.

DNS-сервер в Ideco NGFW Novum недоступен извне в целях безопасности. Для поддержки внешних DNS-зон рекомендуем использовать сторонние DNS-хостинги.

Формат записей

Формат записей для настройки Master-зоны соответствует формату записей DNS-сервера BIND.

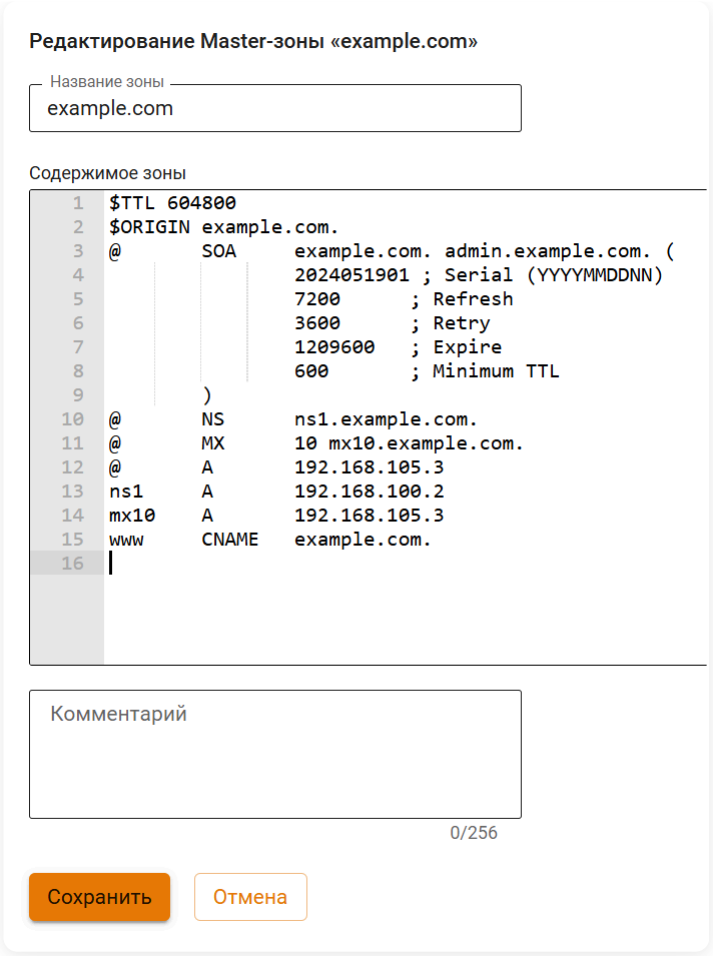
Описание параметров записи

- **TTL** - определяет время кеширования положительных ответов (например, найденного IP-адреса). Задается в секундах или с помощью сокращений: `m` (минуты), `h` (часы), `d` (дни), `w` (недели).
- **ORIGIN** - определяет текущее доменное имя. Значение `ORIGIN` заменяет символ `@` в записях, а также автоматически добавляется к любому имени, не заканчивающемуся точкой (`.`).
- **SOA** - описывает начальные параметры зоны и определяет зону ответственности сервера. Для каждой зоны допустима только одна запись SOA. Включает primary NS-сервер домена и email администратора (с заменой `@` на `.`, например: `admin.example.com`). Включает:
  - **Serial** - серийный номер зоны. Должен увеличиваться при любых изменениях, чтобы вторичные серверы обновили данные. Рекомендуемый формат: `YYYYMMDDnn` (год, месяц, день + двузначный номер изменения, начиная с `00`). Например, первое изменение 15 мая 2025 года будет `2025051500`, следующее в тот же день - `2025051501`.
  - **Refresh** - как часто вторичные серверы должны проверять первичный на наличие обновлений.
  - **Retry** - интервал между повторными попытками при неудачном обновлении.
  - **Expiry** - срок, после которого вторичный сервер прекратит использовать данные зоны, если не сможет обновиться.
  - **TTL** - минимальное время кеширования для вторичных серверов.
- **SRV** - указывает серверы, ответственные за определенные службы в домене (например, Jabber, Active Directory, SIP). Формат: `_служба._протокол.домен`.
- **NS** - указывает авторитетные DNS-серверы для домена. Для каждой `NS`-записи обязательно должны существовать сопоставимые `A` или `AAAA`-записи.
- **PTR** - преобразует IP-адрес в доменное имя (reverse DNS). Используется, например, для проверки почтовых серверов.
- **MX** - указывает почтовые серверы для домена. Формат: `Приоритет Сервер` (например, `10 mx.example.com`). Для каждого `MX` обязательна `A` или `AAAA`-запись.
- **A** - сопоставляет доменное имя с IPv4-адресом (например, `192.0.2.1`). Для каждого интерфейса требуется отдельная запись.
- **AAAA** - аналогична `A`, но для IPv6 (например, `2001:db8::1`).
- **CNAME** - задает алиас (псевдоним) для другого доменного имени. Для алиаса не должно быть других записей (например, `MX` или `TXT`).

Со всеми ресурсными записями можно ознакомиться по ссылке.
Пример записей:

Поле **Название зоны** должно соответствовать записи **$ORIGIN**, но без точки в конце. Например:

- **Имя зоны** - `168.192.in-addr.arpa`
- Запись **$ORIGIN** - `168.192.in-addr.arpa.`



Примеры записей в мастер-зону:

1. Имя зоны: ms:

```
$ORIGIN ms.
$TTL 600
@ SOA ns1.ms. administrator.ms. ( 4 7200 3600 1209600 600 )
@ NS ns1.ms.
@ MX 10 mx10.ms.
@ A 192.168.0.250
ns1 A 192.168.0.250
mx10 A 192.168.0.250
www CNAME @
```

2. Имя зоны: example.com:

```
$TTL 86400
@ SOA localhost. root.localhost. ( 2024120713 28800 14400 3600000 86400 )
@ NS my-dns-server.example.com.
my-dns-server A 1.2.3.4
```

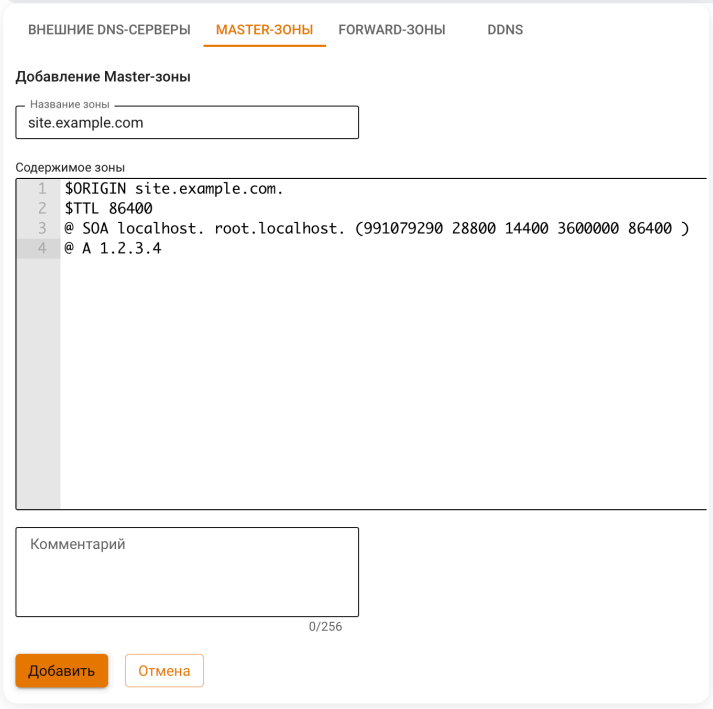
3. Имя зоны: site.example.com:

Если требуется скорректировать Master-зону для конкретного ресурса из зоны example.com, достаточно создать для ресурса отдельную Master-зону. В этом случае NGFW Novum будет управлять только им, а остальной зоной - текущий DNS-хостинг.

Пример описания для ресурса site.example.com из зоны example.com:

```
$ORIGIN site.example.com.
$TTL 86400
```

```
@ SOA localhost. root.localhost. (991079290 28800 14400 3600000 86400 )
@ A 1.2.3.4
```



Работа с IDN-доменами

IDN-домен - домен, составленный из национальных символов алфавита. Например, **дневник.ру**. Для корректной работы Master-зон с IDN-доменами выполните действия:

1. Преобразуйте IDN-домены в формат **Punycode**. Подробнее в RFC.

2. При создании содержимого Master-зоны используйте преобразованное в формат **Punycode** доменное имя.

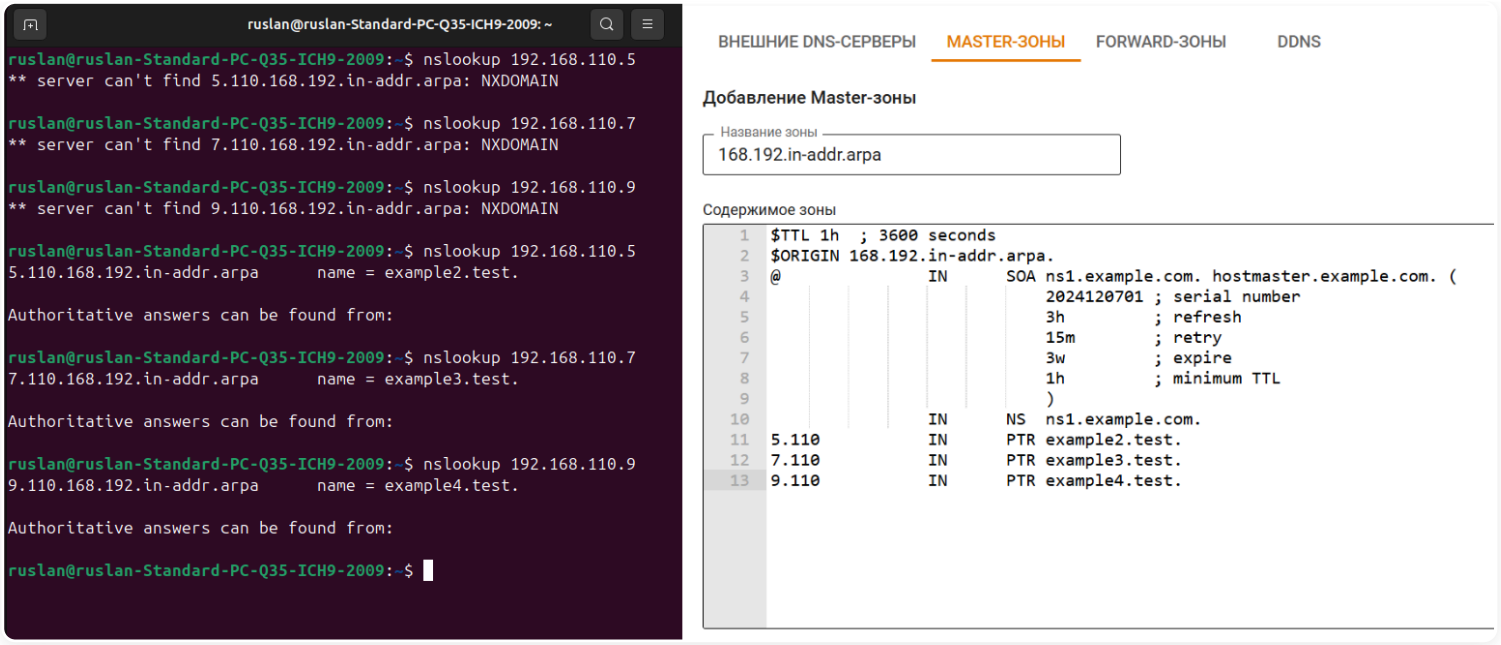
Не используйте Master-зоны для блокировки доступа к сайтам, для этого есть другие средства.

Блокировка таким способом работает неэффективно и не позволяет выборочно запрещать доступ по пользователям или подсетям. Также приводит к проблемам с излишним кешированием.

Обратная Master-зона

Обратная Master-зона используется для распознавания домена по IP-адресу.

Статические Master-зоны требуют ручного создания PTR-записей, динамические - генерируют PTR-записи автоматически. Пример обратной Master-зоны:



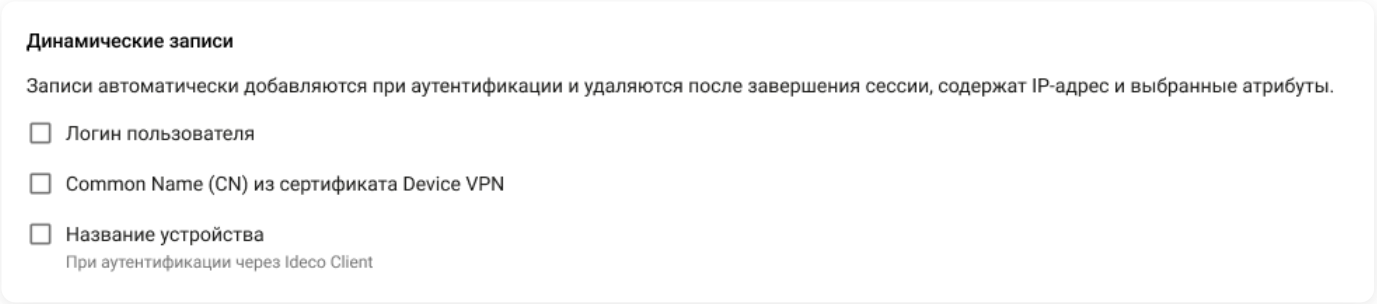
Имя зоны: 168.192.in-addr.arpa

Доменная зона соответствует IP-адресу 192.168.0.0/16. В содержимом зоны указаны три PTR-записи:

```
$TTL 1h  ; 3600 seconds
$ORIGIN 168.192.in-addr.arpa.
@               IN      SOA ns1.example.com. hostmaster.example.com. (
                            2024120701 ; serial number
                            3h         ; refresh
                            15m        ; retry
                            3w         ; expire
                            1h         ; minimum TTL
                            )
                IN      NS  ns1.example.com.
5.110           IN      PTR example2.test.
7.110           IN      PTR example3.test.
9.110           IN      PTR example4.test.
```

Динамические записи

Автоматически обновляемые DNS-записи создаются при аутентификации пользователей в Ideco NGFW, дополняя статические записи зоны. Выберите типы записей для добавления:



- **Логин пользователя** - идентификатор пользователя.
- **Common Name (CN) из сертификата Device VPN** - имя устройства из SSL-сертификата Device VPN.
- **Название устройства** - имя устройства из данных ZTNA (Zero Trust Network Access).

Логика добавления PTR-записей:

- Добавляются только при включении соответствующей опции (логин, CN, название устройства).
- Создаются только в паре с прямыми A-записями.
- Не создаются, если для прямой записи нет зоны.

Примеры динамических DNS-записей, где сессия имеет IP-адрес 192.0.2.2:

Доменное имя сессии	Абсолютное доменное имя сессии	Прямая зона	Прямая запись	Обратная зона	Обратная запись
ivanov.example.com.	ivanov.example.com.	example.com.	ivanov IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.com.
ivanov.example.com	ivanov.example.com.	example.com.	ivanov IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.com.
ivanov.example	ivanov.example.example.com.	example.com.	ivanov.example IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.example.com.
ivanov	ivanov.example.com.	example.com.	ivanov IN A 192.0.2.2	2.0.192.in-addr.arpa.	2 IN PTR ivanov.example.com.

Forward-зоны

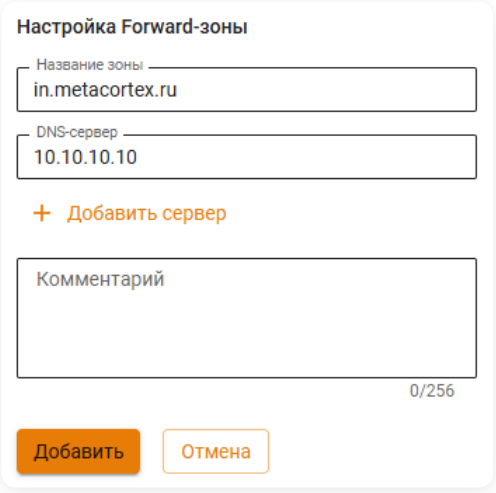
Классический контекст | Высокопроизводительный контекст

Позволяет задать DNS-сервер для разрешения имен конкретной DNS-зоны. Указав доступный в сети DNS-сервер и обслуживаемую зону, клиенты сети Ideco NGFW Novum получают возможность обращаться к ресурсам этой зоны по именам домена.

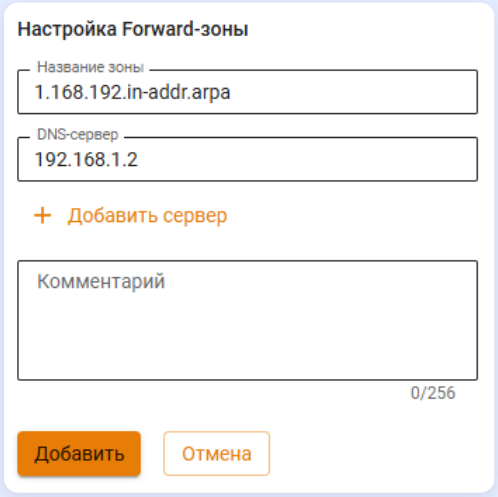
Пользовательские Forward-зоны DNS всегда имеют приоритет над автоматически созданной Forward-зоной для Active Directory.

Например, IT-отдел предприятия предоставляет ресурсы для сотрудников в зоне `in.metacortex.ru` под именами `realm1.in.metacortex.ru`, `sandbox.in.metacortex.ru` и использует для этого DNS-сервер `10.10.10.10`.

Для возможности доступа к этим ресурсам по доменным именам укажите Forward-зону провайдера как isp и далее задайте DNS-сервер `10.10.10.10`:



Для резолвинга PTR при интеграции с Active Directory пропишите обратную Forward-зону. Например, для подсети `192.168.1.0/24` в названии зоны нужно прописать `1.168.192.in-addr.arpa`:



Полезные ссылки

- **Пример настройки Forward-зоны**

- **Подключение через Ideco Client к внутреннему DNS**

DDNS

Функциональность доступна в **Классическом** и **Системном контекстах**.

Название службы раздела **DDNS**: `ideco-dns-backend`.

Список служб для других разделов доступен по ссылке.

DDNS в Ideco NGFW Novum реализован через интеграцию с хостингом RU-CENTER. Перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.

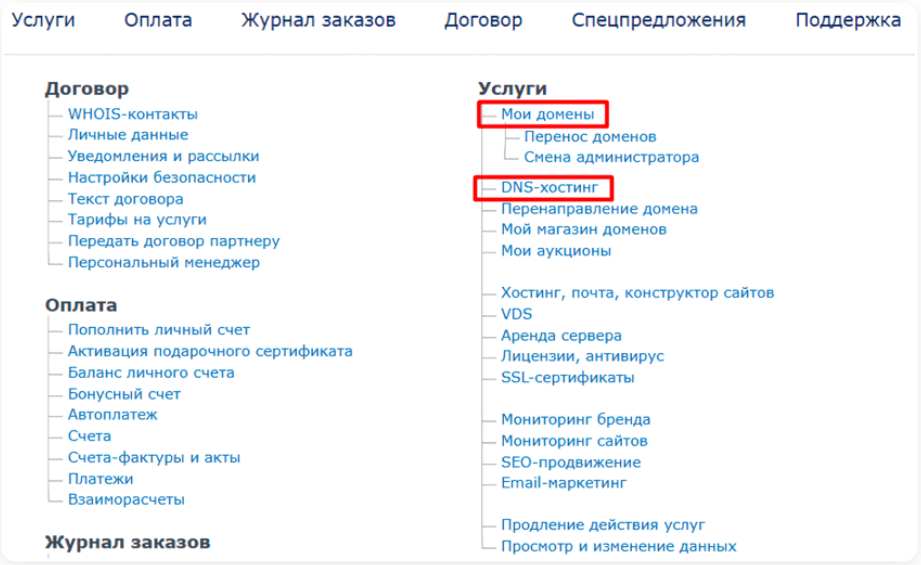
Для решения вопросов по работе с хостингом воспользуйтесь страницей помощи.

Настройка DDNS

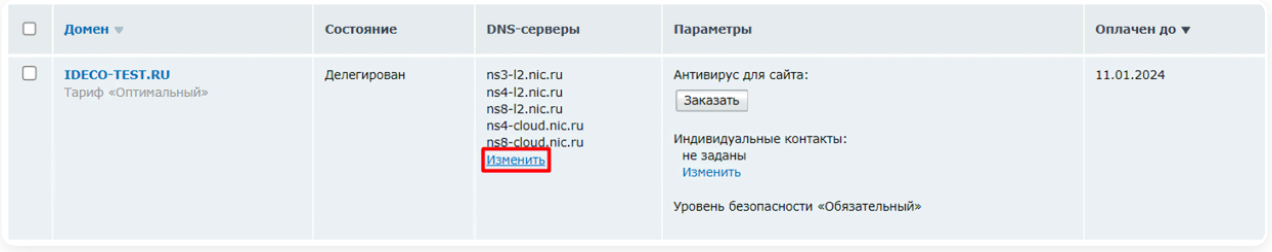
DDNS не будет работать:

- если NGFW находится за NAT.
- если включена балансировка трафика.

1. После входа в личный кабинет RU-CENTER откроется страница Для клиентов. Для дальнейшей работы откройте два раздела - **Мои домены** и **DNS-хостинг**:



2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:

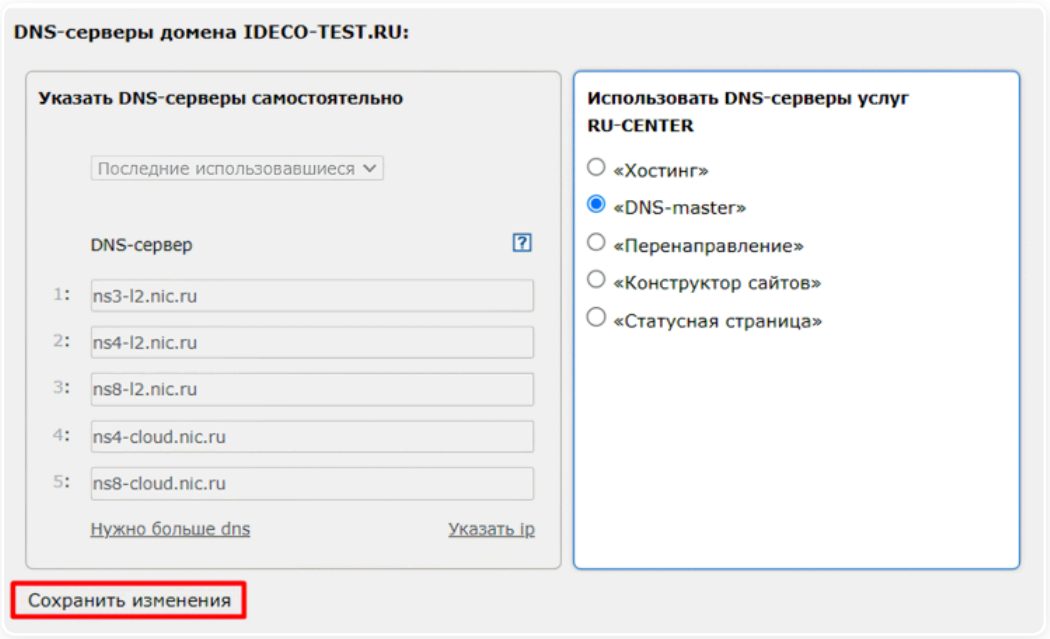


3. Делегируйте домен, отредактировав настройки DNS-серверов:

- **Указать DNS-серверы самостоятельно** - укажите DNS-серверы. Если домен был приобретен на хостинге RU-CENTER, поля заполнятся автоматически.

- **Использовать DNS-серверы услуг RU-CENTER** - выберите **DNS-master**.

Сохраните изменения:



Домен будет делегирован с заданным списком DNS-серверов. Это может занять несколько часов.

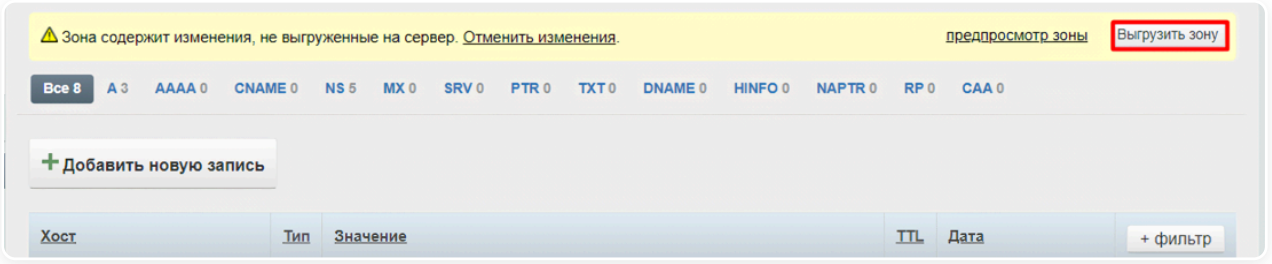
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

5. Выберите нужный домен или добавьте (если домен был приобретен на стороннем ресурсе), нажав соответствующую кнопку.

6. Добавьте две записи по кнопке **Добавить новую запись**:

- Первая запись:
  - Name - укажите знак `@`.
  - Type - выберите тип `A`.
  - IP address - текущий IP-адрес Ideco NGFW Novum (указывается в **Техническая поддержка** → **Информация для технической поддержки**).
  - TTL - оставьте не заполненным.
- Вторая запись:
  - Name - укажите `www`.
  - Type - выберите тип `A`.
  - IP address - текущий IP-адрес Ideco NGFW Novum.
  - TTL - оставьте не заполненным.

7. Нажмите кнопку **Выгрузить зону**:



8. Перейдите в раздел **DDNS** в Ideco NGFW Novum и заполните поля:

- **Домен на DNS-хостинге nic.ru** - укажите приобретенный домен.
- **Логин от API** и **Пароль от API** - для получения логина и пароля перейдите по ссылке Динамический DNS и нажмите **Получить**:



9. Сохраните настройки в Ideco NGFW Novum, нажав соответствующую кнопку.

DHCP-сервер

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **DHCP**: `ideco-dhcp-server-backend`.

Список служб для других разделов доступен по ссылке.

DHCP-сервер автоматически назначает IP-адреса и другие параметры сетевой конфигурации устройствам в сети по протоколу DHCP (Dynamic Host Configuration Protocol).

В Ideco NGFW Novum DHCP-сервер используется для упрощения управления сетевыми настройками:

- Исключает необходимость ручной конфигурации каждого устройства.
- Обеспечивает корректное распределение адресов.
- Предотвращает конфликты IP-адресов.

Это особенно актуально в динамических сетях с большим количеством подключаемых устройств.

Интерфейс Ideco NGFW Novum

- **Настройки** - позволяет настроить диапазон IP-адресов для автоматического назначения.
- **Привязка IP к MAC** - позволяет сформировать статические привязки IP-адресов к MAC-адресам.
- **Мониторинг аренды** - позволяет получить сведения об аренде IP-адреса для устройства.

Сетевые устройства в локальной сети должны быть настроены на автоматическое получение сетевых реквизитов от DHCP-сервера. Таким образом, клиенты отправляют широковещательный запрос в сегмент локальной сети, а сервер перехватывает и отправляет на эти запросы ответы, содержащие необходимые настройки для клиента.

Для сортировки строк таблицы по определенному столбцу нажмите на этот столбец в заголовке таблицы.

Для настройки DHCP-сервера перейдите в **Сервисы** → **DHCP-сервер**. Включите опцию **DHCP-сервер**:



На локальном интерфейсе Ideco NGFW Novum, участвующем в раздаче адресов, должен быть настроен статический IP-адрес.

Настройки

Если Ideco NGFW Novum является шлюзом и DNS-сервером для всех сетевых устройств локальной сети, то настройка службы ограничивается определением диапазона IP-адресов.

Если на Ideco NGFW Novum настроен перехват DNS, то резолвинг имен будет производиться при помощи сервера, указанного в настройках перехвата DNS.

Опция **Выдавать IP-адреса, указанные в авторизациях по IP без MAC** позволяет назначать IP-адреса из правил авторизации (без MAC-адреса) любому устройству в сети, если адрес свободен. Трафик устройства, получившего такой IP-адрес, будет обрабатываться как трафик пользователя из соответствующего правила авторизации.

При отключении опции IP-адреса из правил авторизации (без MAC-адреса) резервируются и не выдаются DHCP-сервером.

Для правил авторизации по IP+MAC резервирование работает всегда, независимо от состояния опции.

Если опция **Выдавать IP-адреса, указанные в авторизациях по IP без MAC** включена, нет гарантий, что устройство получит свой прежний IP-адрес. Если в правиле авторизации не указан MAC-адрес и нет привязки в DHCP, то IP-адрес будет выдан, если свободен на момент запроса. Если адрес занят другим устройством, сервер предложит новый.

Настройка DHCP-сервера делится на три блока:

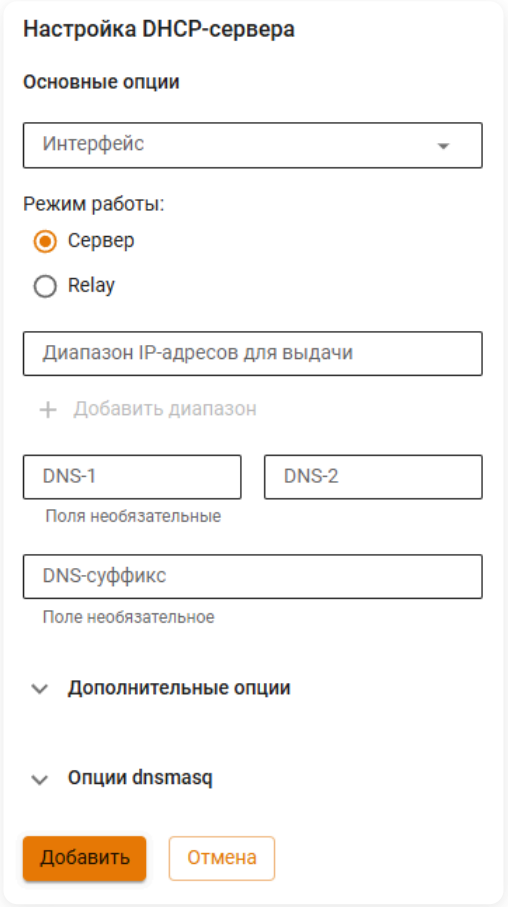
- **Основные опции** - задаются диапазоны IP-адресов и DNS-серверы.
- **Дополнительные опции** - статические маршруты, адреса WINS-серверов, время аренды, PXE Boot и WPAD.
- **Опции dnsmasq** - предназначены для ручного задания опций DHCP, передаваемых сервером клиенту при получении сетевых реквизитов от DHCP-сервера.

Основные опции

Если в разделе **Межсетевой экран** создано правило, которое запрещает весь трафик, то добавьте в таблицу **INPUT** разрешающее правило для UDP-портов 67 и 68, иначе DHCP не сможет раздавать IP-адреса и устройства не получат доступ к сети.

Режим работы Сервер

Выберите режим работы **Сервер**, чтобы настроить выдачу IP-адресов на Ideco NGFW Novum. Заполните поля:



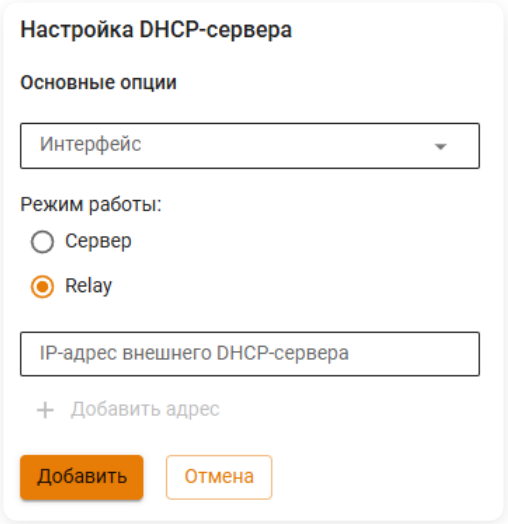
- **Интерфейс** - выберите интерфейс, который будет участвовать в раздаче адресов.

В **Системном контексте** невозможно выбрать интерфейсы, которые используются в VCE.

- **Диапазон IP-адресов для выдачи** - укажите диапазон IP-адресов, которые будут выданы устройствам в локальной сети, должен входить в одну из подсетей выбранного интерфейса. Размер диапазона не должен превышать 256 адресов.
- **DNS-1** и **DNS-2** - укажите IP-адреса DNS-серверов для устройств локальной сети. Если ни одно из полей не заполнено, то DNS-сервером для всех сетевых устройств локальной сети будет Ideco NGFW Novum.
- **DNS-суффикс** - введите домен, прибавляющийся к запрашиваемому имени устройства в локальной сети. Поле не обязательное. Нужен, для того, чтобы в локальной сети вводить не полное имя компьютера вместе с доменом, а только само имя.

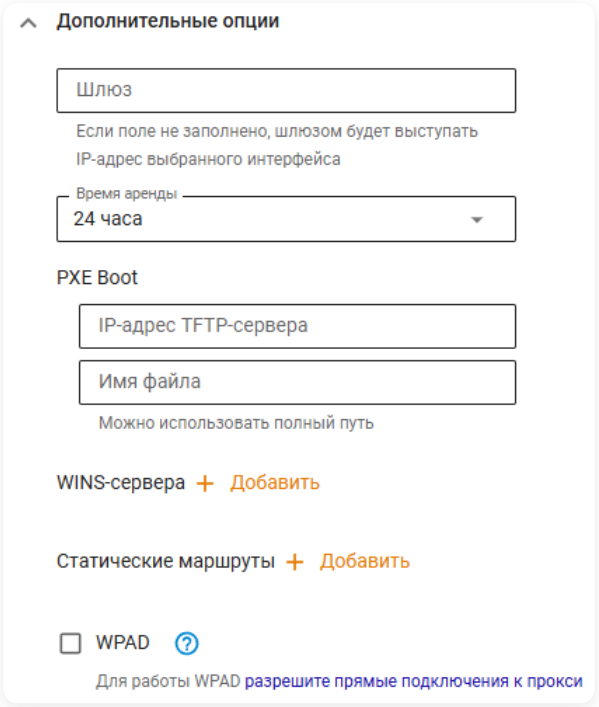
Режим работы Relay

Выберите режим работы **Relay**, если IP-адреса будет выдавать внешний DHCP-сервер. Выберите интерфейс, который будет участвовать в раздаче IP-адресов, и введите IP-адрес внешнего DHCP-сервера:



Включить/выключить, редактировать или удалить правила для выдачи IP-адресов можно кнопками управления в колонке **Управление**.

Дополнительные опции

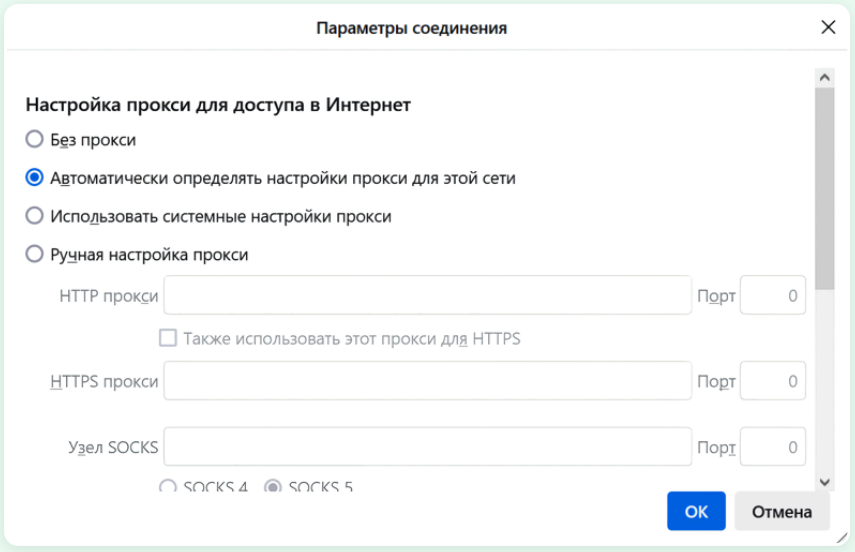


- **Шлюз** - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса.
- **Время аренды** - время, на которое выдается IP-адрес.
- **PXE Boot** - IP-адрес TFTP-сервера для настройки загрузки образа по сети.
- **WINS-сервера** - IP-адрес WINS-сервера.
- **Статические маршруты** - подсеть и шлюз для указания статического маршрута.
- **WPAD** - протокол автоматической настройки прокси.

При включении опции WPAD Ideco NGFW Novum будет автоматически генерировать файл с настройками подключения к прокси и передавать сгенерированный файл хостам в локальной сети, на которых настроено получение IP по DHCP. Локальные сети в файле конфигураций будут добавлены в исключения из прокси.

Для работы WPAD необходимо разрешить прямые подключения к прокси в разделе **Сервисы** → **Прокси**.

Браузеры Google Chrome и Microsoft Edge автоматически примут настройки прокси, переданные хостам по DHCP. В Mozilla Firefox необходимо будет дополнительно зайти в **Настройки браузера** → **Настройки прокси** и выбрать пункт **Автоматически определять настройки прокси для этой сети**:



Опции dnsmasq

Опция **dnsmasq** имеет больший приоритет чем опция, внесенная в блок **Основные опции** или **Дополнительные опции**.

Поле **Значение** может содержать только одну опцию.

Формат записи опции соответствует части записи опции в конфигурации dnsmasq - `[vendor:[<vendor-class>],][<opt>|option:<opt-name>],[<value>[,<value>]]`, где:

- `[vendor:[<vendor-class>],]` - вендор, необязательно.
- `[<opt>|option:<opt-name>]` - числовое или строковое (напр. option:nis-server) обозначение опции.
- `[<value>[,<value>]]` - одно или несколько значений опции через запятую.

Установите флаг **Force** если требуется отправлять опцию DHCP-клиенту, даже если клиент не запрашивал опцию.

Важно: некорректно заданные dnsmasq-опции могут привести к остановке работы раздела **DHCP-сервер**. Статус раздела сменится на **Модуль** `dnsmasq` **не смог запуститься** и **Служба** `ideco-dnsmasq` **остановлена**.

Для поиска некорректно заданной опции выполните действия:

- Перейдите в **Отчеты и журналы** → **Система**.
- В столбце **Сообщение** найдите запись формата `bad option at line 15 of /run/ideco-dhcp-server-backend/dnsmasq.conf`. В записи указано, на какую строку в конфиге нужно обратить внимание.
- Перейдите в **Управление сервером** → **Терминал**.
- Откройте конфиг `/run/ideco-dhcp-server-backend/dnsmasq.conf` и найдите нужную строку.

Расширение базовых опций, отсылаемых DHCP-сервером для конфигурирования IP-телефонов Avaya

Для IP-телефонов Avaya может потребоваться передать оборудованию опции 176 и 242. Для ознакомления со списком опций для конкретной модели обратитесь к документации нужной модели Avaya.

1. Перейдите к созданию настройки DHCP-сервера (**Сервисы** → **DHCP-сервер** → **Настройки** → **Добавить**).

2. Заполните **Основные** и **Дополнительные** опции.

3. Нажмите **Добавить опцию** и заполните 176 опцию. Опция используется для указания голосового сервера:

```
176,"MCIPADD=1.2.3.4,MCPORT=1719"
```

4. После добавления 176 опции добавьте 242, которая используется для серверов передачи данных:

```
242,"MCIPADD=1.1.1.2,MCPORT=1719"
```

После сохранения настроек IP-телефония Avaya будет получать от DHCP-сервера расширенный список опций.

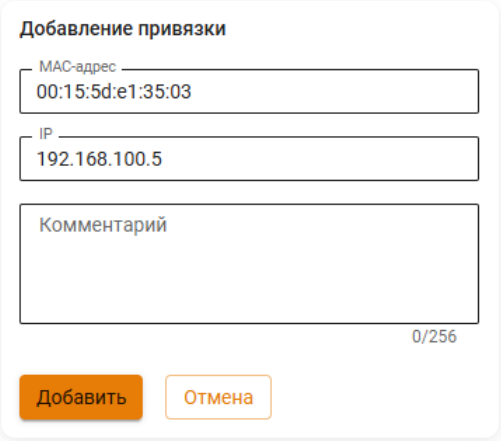
Привязка IP к MAC

IP-адрес, указанный в правиле привязки к MAC, может не входить в диапазон IP-адресов, заданный на вкладке **Настройки**. DHCP-сервер выдаст хосту этот IP-адрес.

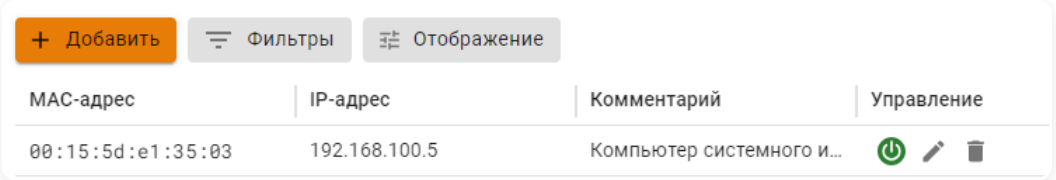
Для настройки в DHCP-сервере привязки IP-адреса к MAC-адресу необходимо:

1. В **Сервисы** → **DHCP** выберите вкладку **Привязка IP к MAC**.

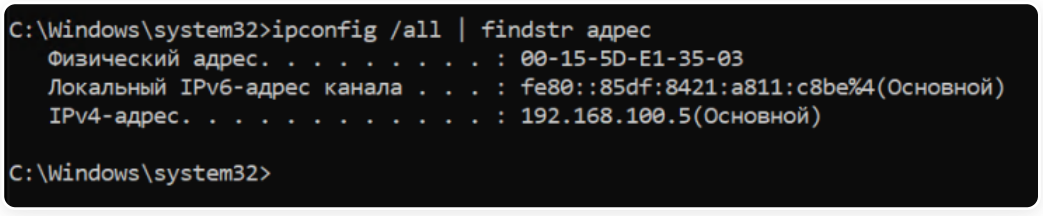
2. Создайте правило привязки **IP к MAC**:



Пример созданного правила привязки показан ниже на скриншоте:



Для проверки созданного правила на компьютере с указанным в правиле MAC-адресом получите IP-адрес по DHCP и проверьте результат с помощью команды `ipconfig /all` (для операционной системы Windows):



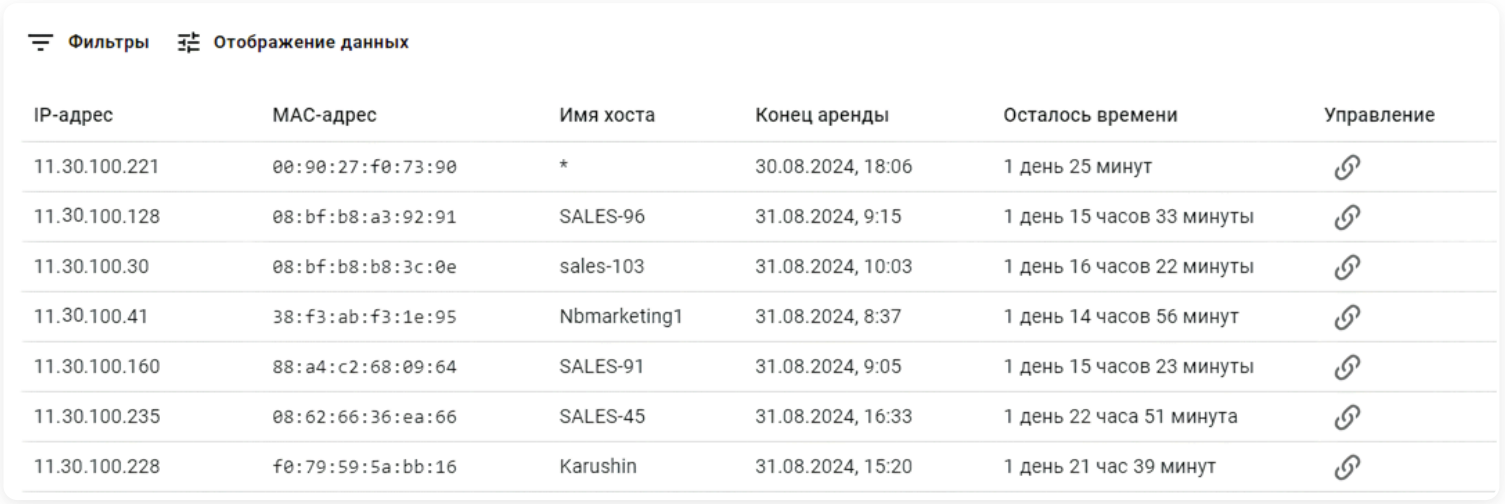
При наличии большого количества привязок в таблице воспользуйтесь кнопкой **Фильтры**.

Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW Novum.

Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (`01-02-03-04-05-06`). В настройках Ideco NGFW Novum октеты MAC-адреса разделяются только двоеточиями (`01:02:03:04:05:06`).

Мониторинг аренды

Содержит информацию об аренде IP-адресов для устройств. Для поиска воспользуйтесь кнопкой **Фильтры**:



IP-адрес	MAC-адрес	Имя хоста	Конец аренды	Осталось времени	Управление
11.30.100.221	00:90:27:f0:73:90	*	30.08.2024, 18:06	1 день 25 минут	
11.30.100.128	08:bf:b8:a3:92:91	SALES-96	31.08.2024, 9:15	1 день 15 часов 33 минуты	
11.30.100.30	08:bf:b8:b8:3c:0e	sales-103	31.08.2024, 10:03	1 день 16 часов 22 минуты	
11.30.100.41	38:f3:ab:f3:1e:95	Nbmarketing1	31.08.2024, 8:37	1 день 14 часов 56 минут	
11.30.100.160	88:a4:c2:68:09:64	SALES-91	31.08.2024, 9:05	1 день 15 часов 23 минуты	
11.30.100.235	08:62:66:36:ea:66	SALES-45	31.08.2024, 16:33	1 день 22 часа 51 минута	
11.30.100.228	f0:79:59:5a:bb:16	Karushin	31.08.2024, 15:20	1 день 21 час 39 минут	

При использовании фильтра по столбцу **Конец аренды** с оператором **[0...9]** правая граница интервала не включается в результат. Для выборки данных за конкретный день указывайте диапазон с 00:00 этого дня до 00:00 следующего дня.
Пример. Чтобы получить данные по адресам со сроком окончания аренды 13 января 2026 года, укажите:

- От: 13.01.2026 00:00.
- До: 14.01.2026 00:00.

Для привязки IP к MAC нажмите на в столбце **Управление**.

После завершения срока аренды IP-адреса и повторного подключения устройство запросит у DHCP-сервера свой предыдущий адрес:

- Если предыдущий IP-адрес свободен, сервер выдаст его устройству.
- Если запрошенный IP-адрес занят или зарезервирован, сервер выдаст новый.

Не рекомендуем полностью полагаться на возврат прежнего IP-адреса после истечения срока аренды, так как IP-адрес может быть отдан другому устройству.

Удаление аренды

Чтобы удалить аренду IP-адреса:

1. Перейдите в **Управление сервером** → **Терминал** и введите команду:

```
nano /var/cache/ideco/dhcp-server-backend/dnsmasq.leases
```

2. Удалите строку с нужной арендой IP-адреса и сохраните файл.

Полезные ссылки

- **Настройка Wi-Fi-сети**

NTP-сервер

Классический контекст | Высокопроизводительный контекст

Название службы раздела **NTP**: `chronyd`.

Список служб для других разделов доступен по ссылке.

NTP - протокол для синхронизации времени. Он позволяет установить точное время на компьютере, используя информацию от специальных серверов времени. По умолчанию работает на 123/UDP порте.

Принцип работы

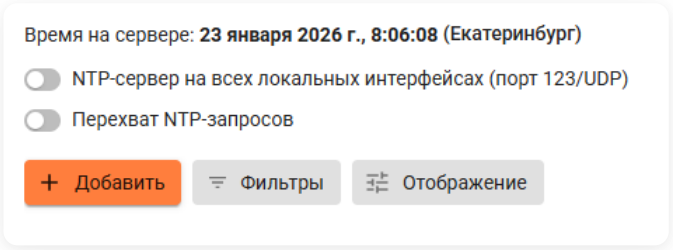
Серверы времени, используемые в NTP, имеют свою иерархию:

- Верхний уровень иерархии занимают официальные источники времени.
- На следующем уровне находятся сервера времени, которые синхронизируют свои часы с официальными источниками времени.
- На последнем уровне находятся клиенты NTP, которые получают информацию от серверов времени.

Ideco NGFW Novum по умолчанию работает как NTP-клиент, получая точное время от эталонных серверов верхнего уровня. При этом Ideco NGFW Novum также может быть настроен как локальный NTP-сервер для устройств во внутренней сети.

Настройка Ideco NGFW Novum

В **Сервисы** → **NTP-сервер** доступны настройки:



- **NTP-сервер на всех локальных интерфейсах (порт 123/UDP)** - при включении опции NGFW Novum будет доступен в качестве NTP-сервера для локальных клиентов. В этом случае NGFW Novum предоставляет время, синхронизированное с внешними эталонными серверами, устройствам в локальной сети, если они настроены на синхронизацию.
- **Перехват NTP-запросов** - при включении опции все запросы локальных клиентов будут обрабатываться NGFW Novum, даже если были отправлены на другой NTP-сервер. В результате все устройства в сети будут получать время только от NGFW Novum, независимо от их собственных настроек.
- Таблица внешних NTP-серверов - в таблице можно вручную указать NTP-серверы, с которыми необходимо синхронизировать время NGFW Novum:
  - Если таблица пуста, NGFW Novum автоматически использует встроенный список доверенных первичных серверов для синхронизации своего времени.
  - Если в таблице есть записи, NGFW Novum будет синхронизироваться только с указанными серверами.

Чтобы создать запись в таблице, нажмите **Добавить** и введите IP-адрес или доменное имя в поле **NTP-сервер**:

Добавление NTP-сервера

NTP-сервер

IP-адрес или доменное имя

Комментарий

0/256

Добавить Отмена

IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Название службы раздела **IPsec**: `ideco-ipsec-backend`.

Список служб для других разделов доступен по ссылке.

IPsec (Internet Protocol Security) - набор протоколов, обеспечивающих безопасную передачу данных в IP-сетях. Обеспечивает аутентификацию, целостность и шифрование данных между узлами.

Воспользуйтесь конфигураторами подключений для MikroTik или Cisco. Конфигураторы позволяют сгенерировать конфиг, запуск которого на удаленном устройстве установит заранее подготовленные настройки IPsec.

Особенности подключений IPsec

В туннельном режиме

- Поддерживается неограниченное число туннелируемых IP-адресов.
- **Туннельный** режим не пропускает широковещательные рассылки, поэтому в таком режиме настроить OSPF не получится.

Необходимо заполнять поле **IP-адрес интерфейса туннеля** для доступа Ideco NGFW Novum к удаленным сетям за другим устройством (например, для доступа к Ideco Center или Active Directory). В будущих версиях без указания IP-адреса доступность удаленных ресурсов для NGFW через IPsec не будет гарантирована.

Следует учесть, что при обновлении на версию 22:

- Существующие конфигурации с несколькими адресами удаленного устройства продолжат работать после миграции. В новой версии допускается только один **Адрес удаленного устройства**.
- **Группа балансировки и резервирования**, выбранная в поле **Интерфейс подключения**, будет перенесена в **Профиль next hop**. В новой версии в поле **Интерфейс подключения** допускается только один интерфейс.

Рекомендуем после обновления указать конкретный **Интерфейс подключения** и конкретный **Адрес удаленного устройства**, так как варианты с множественным выбором или объектом **Любой** будут удалены в следующих версиях.

В транспортном режиме

- Трафик не ограничивается IPSec-политиками, необходимо настраивать маршрутизацию вручную. Для подключения используется выбранный в настройках сетевой интерфейс.
- Пропускаются широковещательные рассылки. Рекомендуем в данном режиме использовать маршрутизацию на основе OSPF.
- Для резервирования канала можно создать несколько IPSec-подключений через разные внешние интерфейсы и определить приоритет направления трафика настройками **OSPF**.

Исходящие и входящие подключения

Настройте исходящее подключение, если Ideco NGFW Novum является инициатором подключения, а удаленное устройство - принимающей стороной. Если удаленное устройство - инициатор подключения, настройте входящее подключение.

Исходящее подключение

Для настройки исходящего подключения подготовьте:

Тип аутентификации	**Требуемые параметры**

Сертификат	• Подписанный удаленным устройством **Запрос на подпись сертификата**. Файл запроса скачивается из веб-интерфейса NGFW Novum при создании подключения, отправляется удаленному устройству и подписанный возвращается для настройки NGFW Novum. • Корневой сертификат удаленного устройства. • Список домашних локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	• PSK-ключ. Генерируется на NGFW Novum при создании подключения. • Идентификатор ключа, который потребуется удаленному устройству для идентификации подключения. • Список локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

Входящее подключение

Для настройки входящего подключения подготовьте:

Тип аутентификации	Требуемые параметры
Сертификат	• Запрос на подпись сертификата (.csr), полученный от удаленного устройства. • Список домашних локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	• PSK-ключ, сгенерированный на удаленном устройстве. • Идентификатор удаленной стороны, заданный в исходящем подключении удаленного устройства. Используется для сопоставления входящего подключения с PSK-ключом. • Список локальных сетей NGFW Novum, которые будут видны противоположной стороне. • Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

Примеры настройки IPsec

В туннельном режиме:

- **Подключение между двумя Ideco NGFW Novum в туннельном режиме работы**
- **Подключение Ideco NGFW Novum и MikroTik по IPsec в туннельном режиме**
- **Подключение Cisco IOS и Ideco NGFW Novum по IPsec в туннельном режиме**

В транспортном режиме:

- **Подключение между двумя Ideco NGFW Novum в транспортном режиме работы**
- **Подключение Ideco NGFW Novum и MikroTik по IPsec в транспортном режиме**
- **Подключение Cisco IOS и Ideco NGFW Novum по IPsec в транспортном режиме**

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключений. После сохранения изменений произойдет перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

После создания IPsec-подключения в **SD-WAN** → **Next hop** автоматически появляется новый next hop. Для настройки балансировки или резервирования:

1. Создайте несколько IPsec-подключений - для каждого появится свой next hop.

2. В разделе **SD-WAN** → **Профили IP SLA** настройте профиль для проверки доступности и качества канала.

3. В разделе **SD-WAN** → **Профили next hop** создайте профиль и выберите режим работы, добавив:

- **Next hop**, полученные при создании IPsec.
- **Профиль IP SLA**, настроенный на шаге 2.

IPsec использует протокол UDP, порты 500 и 4500. По умолчанию порты открыты, но если настроено запрещающее правило во вкладке **INPUT** раздела **Межсетевой экран**, не забудьте добавить разрешение для IPsec.

Выбор алгоритмов шифрования на удаленных устройствах

При настройке сторонних устройств необходимо явно указать алгоритмы шифрования, используемые для подключения.

Ideco NGFW Novum не поддерживает устаревшие и небезопасные алгоритмы (MD5, SHA1, AES128, DES, 3DES, blowfish и др.) при подключении site-to-site. Все site-to-site используют только IKEv2.

При конфигурировании сторонних устройств можно указать несколько поддерживаемых алгоритмов одновременно, так как не все устройства поддерживают современные алгоритмы.

Список алгоритмов

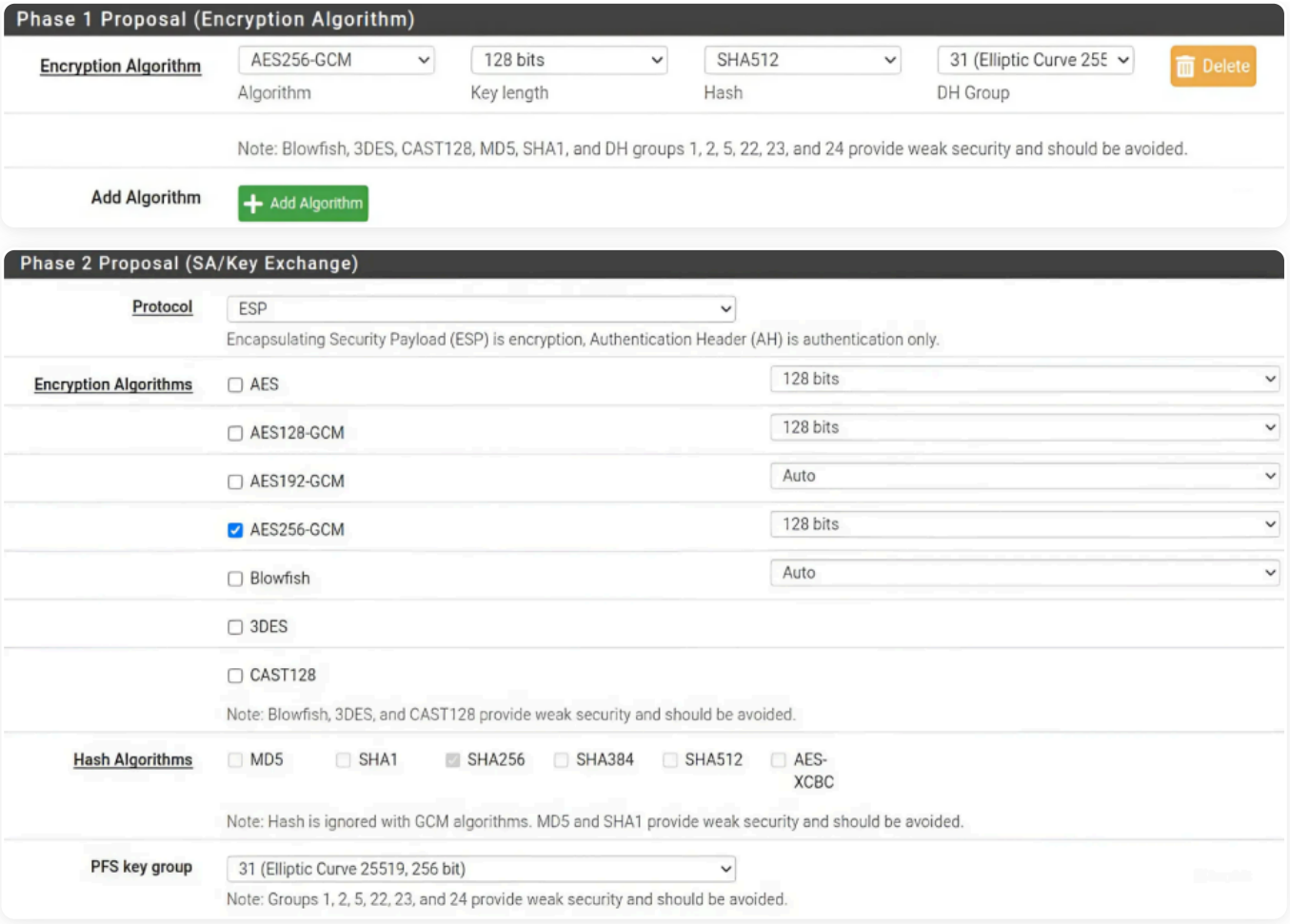
- **Phase 1 (IKE):**
  - encryption (шифрование):
    - **AES256-GCM**.
    - **AES256 (AES256-CBC)**.
  - integrity (hash, целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
    - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
  - prf (функция генерации случайных значений):
    - как правило, настраивается автоматически в зависимости от выбора алгоритмов integrity (пример ниже).
    - для AES-GCM может потребоваться указать явно. В этом случае по приоритету: **AESXCBC, SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman):
    - **Curve25519 (group 31)**.
    - **ECP256 (group 19)**.
    - **modp4096 (group 16)**.
    - **modp2048 (group 14)**.
  - Таймауты:
    - **Lifetime**: 14400 сек.
    - **DPD Timeout** (для L2TP/IPsec): 40 сек.
    - **DPD Delay**: 30 сек.
- **Phase 2 (ESP):**
  - encryption (шифрование):
    - **AES256-GCM**.
    - **AES256 (AES256-CBC)**.
  - integrity (целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
    - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman, PFS). **ВНИМАНИЕ! Если не указать группу, то подключение будет установлено, но через некоторое время не сработает параметр rekey**:
    - **Curve25519 (group 31)**.
    - **ECP256 (group 19)**.
    - **modp4096 (group 16)**.
    - **modp2048 (group 14)**.
  - Таймаут:
    - **Lifetime**: 3600 сек.

Пример использования алгоритмов

Пример:

- **Phase 1 (IKE)** (нужна одна из строк)**:**
  - AES256-GCM\PRF-HMAC-SHA512\Curve25519.
  - AES256(AES256-CBC)\SHA512\PRF-HMAC-SHA512\ECP384.
  - AES256(AES256-CBC)\SHA256\PRF-HMAC-SHA256\MODP2048.
- **Phase 2 (ESP)** (нужна одна из строк)**:**
  - AES256-GCM\ECP384.
  - AES256(AES256-CBC)\SHA256\MODP2048.

Пример настройки подключения pfSense к Ideco NGFW Novum по IPsec:



Мониторинг производительности сети

В Ideco NGFW Novum реализован мониторинг IPsec-соединений, аналогичный IP SLA (Internet Protocol Service Level Agreement). Система позволяет в реальном времени отслеживать ключевые метрики качества сетевого соединения.

В интерфейсе Ideco NGFW Novum для каждого активного соединения отображаются метрики:

- **Вх. скорость, Мбит/с** - скорость приема данных через туннель.
- **Исх. скорость, Мбит/с** - скорость передачи данных через туннель.
- **Средняя задержка, мс** - время, за которое пакет доходит до удаленной стороны туннеля и возвращается обратно.
- **Потеря пакетов, шт.** - количество отправленных, но не дошедших пакетов.
- **Джиттер, мс** - изменение задержки между пакетами.

Для сбора статистики в настройках IPsec-подключения на обеих сторонах заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Указанные IP-адреса должны принадлежать одной подсети.

ГОСТ VPN

Функциональность доступна только в **Системном контексте**.

ГОСТ VPN - это сервис для организации защищенных каналов связи между несколькими Ideco NGFW Novum с использованием технологии виртуальной частной сети. Соединение шифруется согласно требованиям ФСБ по ГОСТ-алгоритмам с применением российского сертифицированного решения от компании Рутокен.

Компания "Айдеко" пока не получила заключение от регулятора и только завершает работы по сертификации интеграции, поэтому использование ГОСТ VPN не закрывает требования регулятора по организации доверенного канала связи для передачи конфиденциальной информации через интернет.

Используются алгоритмы шифрования:

- **ГОСТ Р 34.10-2012** - для создания ключевой пары.
- **ГОСТ Р 34.12-2015** (**Кузнечик** и **Магма**) - для симметричного шифрования.
- **VKO ГОСТ Р 34.10-2012** - для выработки сессионных ключей.

Туннельное соединение можно использовать в **Маршрутизации**.

В разделе **Графики загруженности → ГОСТ VPN** представлена информация о входящих и исходящих соединениях ГОСТ VPN, а также данные мониторинга трафика.

Настройка ГОСТ VPN

Для настройки ГОСТ VPN необходимо подготовить два USB-токена в соответствии с инструкцией, представленной в статье, и подключить токены к USB-портам серверов.

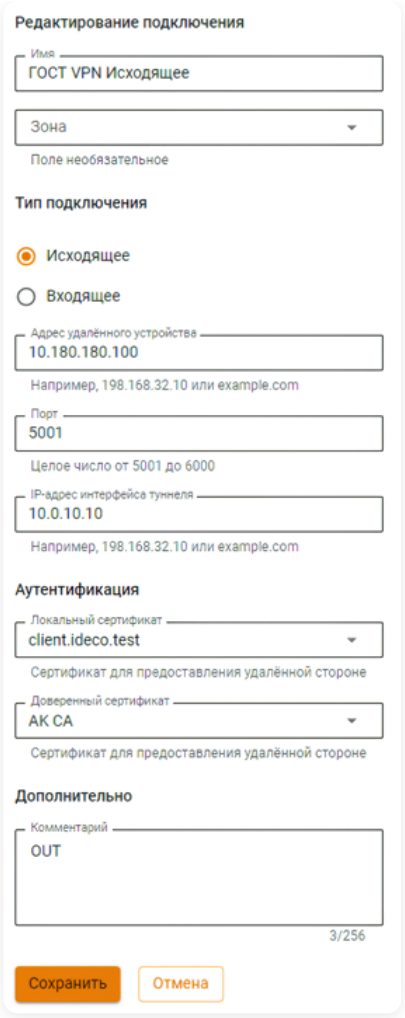
В случае извлечения USB-токена или истечения срока действия сертификатов, хранящихся на USB-токене, VPN-соединение будет разорвано.

Для создания соединения между двумя Ideco NGFW Novum необходимо настроить входящее соединение на одном NGFW и исходящее соединение на другом NGFW.

Настройка исходящего подключения

1. Перейдите в **Сервисы → ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



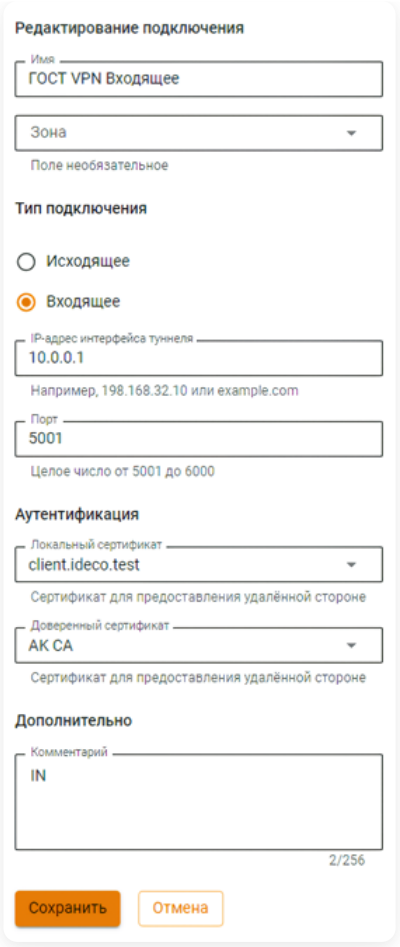
Расшифровка полей

- **Имя** - введите имя подключения, максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Тип подключения** - выберите **Исходящее**.
- **Адрес удаленного устройства** - введите доменное имя или белый IP-адрес удаленного Ideco NGFW Novum.
- **Порт** - введите порт в диапазоне от 5001 до 6000.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля, который будет использоваться для маршрутизации данных на сетевом уровне.
- **Локальный сертификат** - выберите локальный сертификат настраиваемого устройства, который содержит приватный ключ и хранится на USB-токене.
- **Доверенный сертификат** - выберите доверенный сертификат, который хранится на том же USB-токене, где находится локальный сертификат.

Настройка входящего подключения

1. Перейдите в **Сервисы** → **ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Имя** - введите имя подключения, максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Тип подключения** - выберите **Входящее**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля, который будет использоваться для маршрутизации данных на сетевом уровне.
- **Порт** - введите порт в диапазоне от 5001 до 6000.
- **Локальный сертификат** - выберите локальный сертификат настраиваемого устройства, который содержит приватный ключ и хранится на USB-токене.
- **Доверенный сертификат** - выберите доверенный сертификат, который хранится на том же USB-токене, где находится локальный сертификат.

Настройка ГОСТ VPN в кластере

Для корректной работы ГОСТ VPN в кластере необходимо:

1. Подготовить токены:

- Должно быть **два разных USB-токена** - по одному для каждой ноды кластера.
- **Не вставляйте оба токена в одну ноду** - это может привести к ошибкам в работе.

2. Подготовить сертификаты с учетом требований:

- На **каждом токене** необходимо сгенерировать свой сертификат.
- У полученных сертификатов должно быть **одинаковое значение CN (Common Name)**.
- Оба сертификата должны быть подписаны **одним и тем же удостоверяющим центром (Certificate Authority, CA)**.

3. Настроить привязки токенов:

- Для обоих токенов в конфигурации криптопровайдера необходимо прописать привязку **PIN-код - токен**.

Особенности работы в кластере:

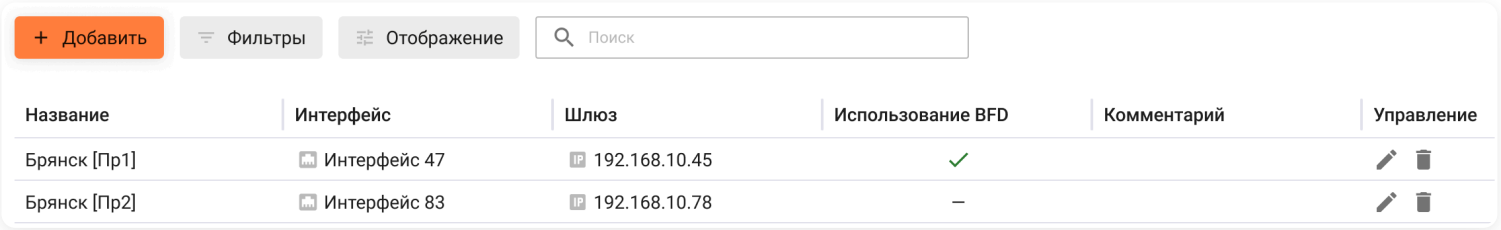
- VPN-соединение работает на **активной** в данный момент ноде.

- При отказе активной ноды кластер переключится на резервную, и использоваться будет сертификат токена, находящийся в резервной ноде. Соединение восстанавливается за счет идентичности сертификатов (CN, подпись CA) на обоих токенах.

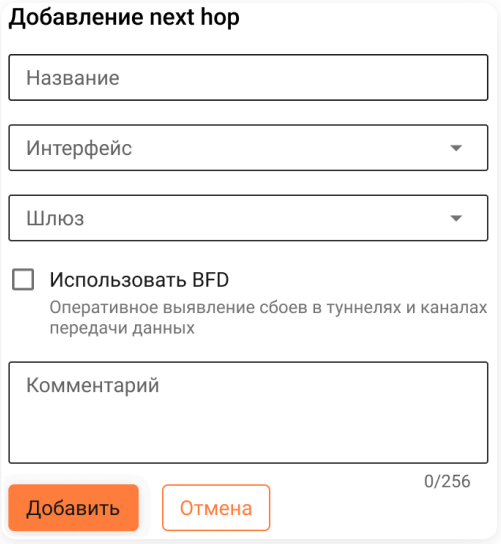
Настройка Next hop

Чтобы использовать туннель в маршрутизации, создайте **Next hop**:

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**:



2. Заполните поля:



- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс **ГОСТ VPN**.
- **Шлюз** - оставьте поле пустым. **ГОСТ VPN** является point-to-point соединением - трафик отправляется напрямую в туннельный интерфейс, минуя шлюз.

Для настройки мониторинга состояния **Next hop** воспользуйтесь статьей.

Статусы подключения

После настройки в таблице **ГОСТ VPN** появится site-to-site соединение, в котором можно отслеживать статус подключения.

Статус подключения ГОСТ VPN	Описание
Подключено	ГОСТ VPN подключен и работает
Соединяется	Происходит установление соединения или ожидание ответа от другого устройства
Отключение	Происходит разъединение подключенных устройств
Не подключено	Отсутствует подключение
Ошибка	Возникла ошибка

Полезные ссылки

- **Поддержка устаревших алгоритмов шифрования**
- **Пример генерации ключей и сертификатов ГОСТ VPN**

Сертификаты

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Сертификаты**: `ideco-cert-backend`.

Список служб для других разделов доступен по ссылке.

В разделе **Сертификаты** отображаются SSL-сертификаты или цепочки сертификатов, список которых формируется модулями:

- [x] Модуль обратного проксирования
- [x] VPN-серверы IKEv2 и SSTP
- [x] Веб-интерфейс
- [x] Веб-аутентификация
- [x] Почта
- [x] Ideco Client

Логика работы

Ideco NGFW Novum позволяет выпустить или загрузить корневые и некорневые (пользовательские) сертификаты:

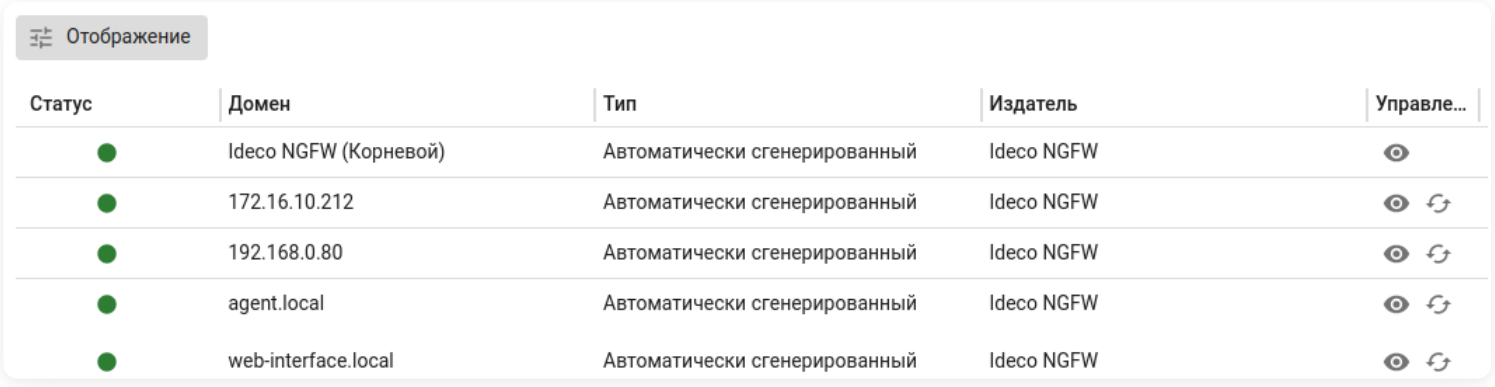
- **Корневые сертификаты** обязательно должны содержать атрибут **X509v3 Basic Constraints: CA: TRUE** для выпуска дочерних сертификатов. При первоначальной установке и запуске Ideco NGFW Novum корневой (самоподписанный) сертификат генерируется автоматически. Сертификат можно скачать, перейдя в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** и нажав .
- **Пользовательские сертификаты** - любые сертификаты на домен. Источником подписи для таких сертификатов могут выступать:
  - Корпоративный корневой сертификат.
  - Центры сертификации (Certificate Authority, CA).

Ideco NGFW Novum автоматически генерирует и подписывает сертификаты на домены, указанные в настройках модулей.

Действующие сертификаты

В таблице **Действующие сертификаты** отображаются:

- Автоматически сгенерированные цепочки сертификатов.
- Загруженные цепочки сертификатов, используемые модулями Ideco NGFW Novum:

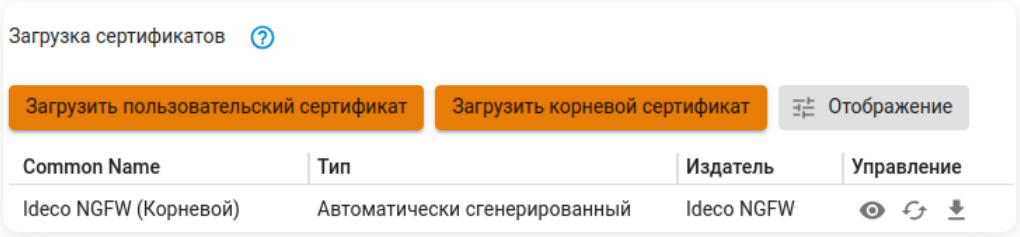


Если в таблице **Действующие сертификаты** одна и та же цепочка сертификатов указана в нескольких строках, значит, она используется несколькими модулями.

Загруженные сертификаты

В таблице **Загруженные сертификаты** отображаются:

- Все загруженные цепочки сертификатов.
- Корневой сертификат Ideco NGFW Novum:



Требования к SSL-сертификатам и инструкция по загрузке в статье.

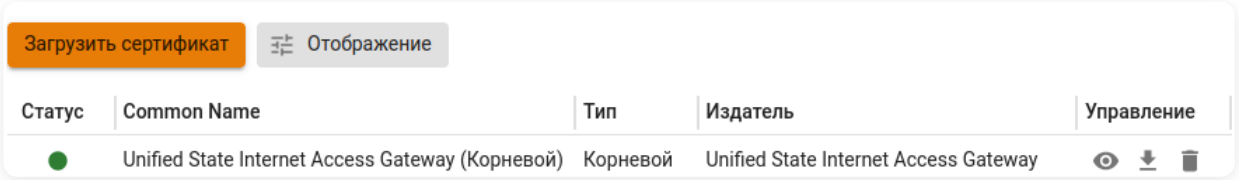
Системные сертификаты

Раздел позволяет загружать свои сертификаты в хранилище доверенных сертификатов ОС Fedora на Ideco NGFW Novum. Подробнее о системных сертификатах - по ссылке.

Загрузка в **Системные сертификаты** необходима, если Ideco NGFW Novum взаимодействует с сервисами, защищенными сертификатом от корпоративного или самоподписанного центра сертификации (CA). Чтобы Ideco NGFW Novum доверял такому сервису, корневой сертификат этого CA необходимо добавить в хранилище.

Если внешний сервис использует сертификат, выпущенный публичным доверенным CA (например, Let's Encrypt), загружать ничего не нужно - такие CA уже включены в стандартное хранилище доверенных сертификатов ОС Fedora.

После добавления сертификата в таблицу **Системные сертификаты** перезагрузите Ideco NGFW Novum. После перезагрузки Ideco NGFW Novum будет доверять загруженному сертификату и всем сертификатам, подписанным загруженным сертификатом:



Ideco Client

Раздел предназначен для управления сертификатами, используемыми для настройки авторизации пользователей и VPN-доступа через Ideco Client. Сертификаты позволяют реализовать привязку устройств к пользователям и третий фактор аутентификации.

Логика работы сертификатов Ideco Client

При подключении через Ideco Client система использует сертификаты устройства для:

- [x] Идентификации и привязки устройства к пользователю
- [x] Проверки подлинности устройства
- [x] Ограничения доступа к VPN только с доверенных устройств

Ideco NGFW Novum поддерживает два источника доверия:

- **Встроенный удостоверяющий центр (CA)**. Создается автоматически при первом запуске системы. Выпускает и подписывает сертификаты для устройств.
- **Сторонние удостоверяющие центры**. Можно загрузить CA-сертификаты сторонних УЦ для проверки сертификатов, выпущенных вне Ideco NGFW Novum.

В Ideco NGFW Novum серверные и клиентские сертификаты подписывают два независимых удостоверяющих центра. Корневой сертификат для выпуска серверных сертификатов Ideco NGFW Novum можно заменить собственным в разделе **Загруженные сертификаты**. **Локальный УЦ** Ideco Client - это отдельный удостоверяющий центр, который подписывает исключительно листовые клиентские сертификаты для устройств Ideco Client.

Замена корневого сертификата в разделе **Загруженные сертификаты** не влияет на **Локальный УЦ** Ideco Client и не заменяет его: он остается прежним и продолжает выпускать клиентские сертификаты для устройств.

Требования к сертификату устройства

Сертификат, выпускаемый на основании CSR-запроса, должен соответствовать следующим требованиям:

- **Тип ключа:** только EC (эллиптическая кривая).
- **Кривая:** только SECP256R1 (P-256).
- **Basic Constraints:** `CA: FALSE`.
- **Key Usage:** `digitalSignature` (critical).
- **Extended Key Usage:** `clientAuth` (critical).
- **Subject DN:** содержит непустой Common Name (CN).
- **Ограничения флагов:** сертификат не должен содержать других флагов, кроме `digitalSignature` и `clientAuth`.

Раздел представлен в виде вкладок:

- **Реестр** - таблица содержит действующие доверенные сертификаты:
  - **Сторонние УЦ** - загруженные администратором CA-сертификаты сторонних удостоверяющих центров в формате `.pem`.
  - **Локальный УЦ** - сертификаты, автоматически сгенерированные локальным удостоверяющим центром Ideco NGFW Novum:
    - **CA-сертификат локального УЦ** - локальный сертификат. Используется для выпуска и подписи сертификатов устройств пользователей.
    - **Выпущенные** - сертификаты устройств, сгенерированные и подписанные локальным УЦ после первой успешной авторизации пользователя через Ideco Client. Такие сертификаты автоматически устанавливаются через Ideco Client на устройство пользователя и обеспечивают идентификацию устройства при последующих подключениях.
- **Отозванные** - сертификаты, которые были отозваны из **Реестра**. Доступны только для редактирования поля **Комментарий**.

Управление сертификатами

В колонке Управление:

- просмотр основной информации о сертификате.
- перевыпуск сертификата.
- скачать сертификат.
- удалить загруженный сертификат.
- отозвать сертификат.

Добавление сертификатов:

- **Загрузить пользовательский сертификат** - позволяет загрузить собственный или приобретенный сертификат как пользовательский, например, на конкретный домен, список доменов (Wildcard) или сервис.
- **Загрузить корневой сертификат** - позволяет загрузить собственный или приобретенный сертификат как корневой, который будет использоваться Ideco NGFW Novum для выпуска и подписания серверных сертификатов. Загруженный корневой сертификат не влияет на **Локальный УЦ** Ideco Client и не заменяет его.
- **Загрузить сертификат** - позволяет загрузить CA-сертификат стороннего удостоверяющего центра в формате `.pem`. Загруженные сертификаты используются как доверенные при проверке сертификатов устройств и могут быть выбраны в настройках авторизации и VPN-доступа.

Процесс выпуска сертификата

Описанный процесс относится к сертификатам, сгенерированным Ideco NGFW Novum (веб-интерфейс, VPN, почта и др.), и не применяется к сертификатам Ideco Client. Сертификаты Ideco Client выпускаются отдельным локальным удостоверяющим центром NGFW Novum. Но для авторизации через Ideco Client используется системный сертификат NGFW Novum на домен, указанный в **Пользователи → Ideco Client → Основное**. О выпуске сертификатов Ideco Client смотрите в статье.

Ideco NGFW Novum выполняет следующие действия:

1. Создает локальную цепочку сертификатов, подписанную корневым (самоподписанным) сертификатом.

2. Параллельно с созданием локальной цепочки сертификатов отправляет запрос на выпуск цепочки в Let's Encrypt.

Условия автоматического выпуска сертификатов Let's Encrypt:

- Наличие доменного имени, зарегистрированного на статический белый IP-адрес, который назначен на внешний интерфейс Ideco NGFW Novum.
- Открытый 80 TCP-порт на внешнем интерфейсе. После установки Ideco NGFW Novum 80 TCP-порт по умолчанию открыт во внешнюю сеть.

Если при соблюдении перечисленных выше условий сертификат Let's Encrypt не выпускается автоматически, перейдите в **Управление сервером** → **Терминал** веб-интерфейса Ideco NGFW Novum и воспользуйтесь командой:

```
systemctl restart ideco-cert-backend.service
```

Команда для просмотра логов:

```
journalctl -u ideco-cert-backend.service -f
```

3. При успешном выпуске цепочки сертификатов Let's Encrypt заменяет локальную цепочку.

4. Если выпуск цепочки сертификатов Let's Encrypt завершился неудачей, NGFW Novum продолжает использовать локальную цепочку сертификатов.

Если требуется повторить попытку получения сертификата Let's Encrypt вместо самоподписанного, то нужно нажать **Перевыпустить** в столбце **Управление**.

Сертификат Let's Encrypt **выпускается на 3 месяца** и будет **автоматически перевыпущен** по окончании срока действия.

С 17 версии Ideco NGFW Novum автоматически сгенерированные NGFW Novum пользовательские сертификаты выпускаются на **825 дней** и будут автоматически перевыпущены по окончании срока действия. В предыдущих версиях срок действия таких сертификатов составлял **10 лет**.

Процесс перевыпуска сертификата

Описанный процесс относится к сертификатам, сгенерированным Ideco NGFW Novum (веб-интерфейс, VPN, почта и др.), и не применяется к сертификатам Ideco Client. Сертификаты Ideco Client выпускаются отдельным локальным удостоверяющим центром NGFW Novum. Но для авторизации через Ideco Client используется сертификат NGFW Novum на домен, указанный в **Пользователи** → **Ideco Client** → **Основное**.

Некорневая цепочка сертификатов

Чтобы перевыпустить некорневую цепочку сертификатов, нажмите в столбце **Управление** таблицы **Действующие сертификаты**. Ideco NGFW Novum будет актуализировать цепочку следующим образом:

- Проверит загруженные сертификаты. Если сертификат найден, заменит действующую цепочку сертификатов на домен новой.
- Если для данного домена новые сертификаты не загружались, Ideco NGFW Novum обратится к Let's Encrypt для выпуска новой цепочки.
- Если цепочка от Let's Encrypt получена, она отобразится в таблице.
- Если получить цепочку сертификатов от Let's Encrypt не удалось, продолжит использовать локальную цепочку сертификатов.

Корневой сертификат

Для перевыпуска корневого сертификата нажмите напротив соответствующей цепочки в таблице **Загруженные сертификаты**. Ideco NGFW Novum заменит цепочку на автоматически сгенерированный корневой сертификат.

Для работы Ideco Client под macOS необходимо, чтобы срок действия сертификата на домен или IP-адрес Ideco NGFW Novum, введенный в разделе **Пользователи** → **Ideco Client**, не превышал 825 дней.

Проверить, что срок действия загруженного пользовательского или сгенерированного Ideco NGFW Novum сертификата не превышает **825 дней**, можно в **Сервисы** → **Сертификаты** → **Действующие сертификаты**, нажав .

Локальная цепочка сертификатов

Чтобы перевыпустить локальную цепочку сертификатов, выполните действия:

1. Перейдите в **Управление сервером** → **Терминал**.

2. Перейдите в директорию `/var/cache/ideco/cert-backend`, выполнив команду:

```
cd /var/cache/ideco/cert-backend
```

3. Выведите содержимое директории, выполнив команду `ls`.

4. Скопируйте название файла сертификата, который требуется перевыпустить. Названия файлов будут иметь вид:

`test.ideco.ru-self-sign_chain_833bcda78229059d2c2886548c75e9e3.pem`, где `test.ideco.ru` - доменное имя или IP-адрес, на который выпущен сертификат.

5. Удалите файл, выполнив команду:

```
rm test.ideco.ru-self-sign_chain_d1f73bf1fcc4d55ca31004ecb13d19b3.pem
```

6. Перейдите в **Сервисы** → **Сертификаты** → **Действующие сертификаты** и перевыпустите сертификат на домен или IP-адрес Ideco NGFW Novum, нажав  .

Чтобы проверить, перевыпустился ли сертификат на новый срок, нажмите  .

Полезные ссылки

- **Использование собственного CA-сертификата в Контент-фильтре**
- **Как установить сертификат Ideco NGFW на Android**
- **Настройка корневого и подчиненного центра сертификации с помощью AD CS**
- **Настройки в Ideco NGFW Novum**

Загрузка SSL-сертификата на сервер

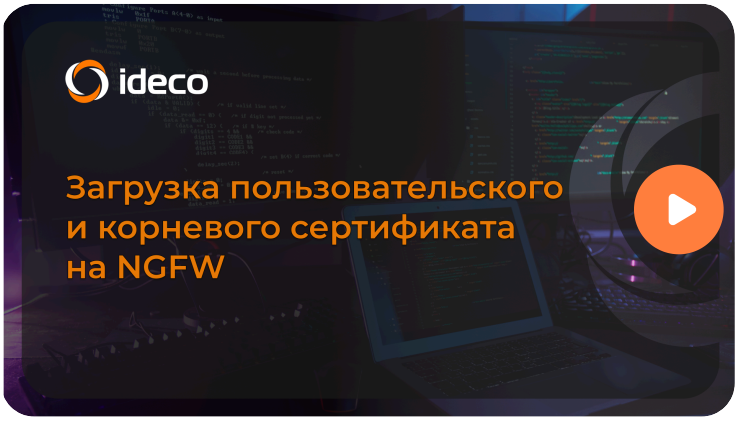
Классический контекст | Высокопроизводительный контекст

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE



Требования к сертификату

Перед загрузкой корневого или пользовательского сертификата на Ideco NGFW Novum убедитесь, что они отвечают следующим требованиям:

- **Формат файла.** Сертификаты должны иметь расширения **.pem**. Если у вашего сертификата другое расширение, конвертируйте сертификат. Как это сделать, описано ниже в разделе **Конвертация сертификата из формата pkcs12 в формат pem с помощью OpenSSL**.
- **Поле Common Name (CN).** В составе сертификата **Издатель** и **Субъект** должны содержать поле **Common Name** (общее имя). При загрузке собственной цепочки сертификатов **CN** последнего сертификата в цепочке должно соответствовать домену, для которого сертификат загружается.
- **Структура цепочки доверия.** Цепочка сертификата должна быть валидной и соответствовать структуре:

```
Приватный ключ
Сертификат на домен (Common Name)
Сертификат из состава бандла vendor-сертификатов (промежуточный сертификат, если есть)
...
Основной (корневой) сертификат
```

- **Уровень безопасности.** Сертификаты должны соответствовать минимально 3 или 4 уровню безопасности (Security Level 3-4) в соответствии со стандартами OpenSSL:
  - **Уровень 3** (128 бит):
    - Длина ключа: RSA - не менее 3072 бит. ECC - не менее 256 бит.
    - Версия TLS: Не ниже TLS 1.1.
    - Алгоритмы хеширования: Запрещено использование MD5 хеша.
    - Дополнительно: Отключены билеты сессии (Session Tickets).
  - **Уровень 4** (192 бита):
    - Длина ключа: RSA - не менее 7680 бит. ECC - не менее 384 бит.
    - Версия TLS: Не ниже TLS 1.2.
    - Алгоритмы хеширования: Запрещено использование SHA-1 для кода аутентификации сообщений (Message Authentication Code, MAC).

Если сертификат самоподписанный, его структура может содержать всего два блока - **Приватный ключ** и **Сертификат на домен (Common Name)**. Если структура сертификата невалидна, переходите к разделу ниже **Подготовка SSL-сертификата для загрузки на Ideco NGFW Novum**.

Если хотите загрузить сертификат как корневой, удостоверьтесь, что сертификат может выдавать дочерние сертификаты: **X509v3 Basic Constraints: CA: TRUE** (это можно проверить в открытом ключе сертификата).

Загрузка SSL-сертификата на Ideco NGFW Novum

Если сертификат удовлетворяет всем перечисленным выше условиям, загрузите его на Ideco NGFW Novum. Для этого:

1. Перейдите в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

2. Нажмите **Загрузить корневой сертификат** или **Загрузить пользовательский сертификат**.

3. Выберите нужный сертификат.

Загруженный корневой сертификат автоматически переподпишет все пользовательские сертификаты на домены, которые ранее автоматически сгенерировал Ideco NGFW Novum. Сертификаты Let's Encrypt и сертификаты, купленные у CA и Центров сертификации, переподписаны не будут.

Если в инфраструктуре компании есть свой корневой центр сертификации, выпустите сертификат с шаблоном **Subordinate Certification Authority** и загрузите его на Ideco NGFW Novum в качестве корневого. Это позволит выстроить цепочку доверия для автоматически выданных сертификатов до корневого центра сертификации. Пользовательские компьютеры будут доверять сертификатам, выданным на стороне Ideco NGFW Novum.

Подготовка SSL-сертификата для загрузки на Ideco NGFW Novum

При покупке доверенного SSL-сертификата на домен у Certificate Authority или Центра сертификации данные для его установки, как правило, высылаются электронным письмом в разрозненном виде. Для корректной загрузки сертификаты на домен промежуточные и корневые сертификаты нужно собрать в один файл в правильном порядке.

Некоторые данные (CSR-запрос и приватный ключ) генерируются только во время покупки SSL-сертификата и не высылаются в письме. Сразу сохраняйте такие данные на своем компьютере.

Корневые (самоподписанные) сертификаты также требуют построения цепочек. Структура таких сертификатов может содержать 2 блока - **Приватный ключ** и **Сертификат на домен (Common Name)** - или более в зависимости от того, есть ли у вас промежуточные сертификаты (из состава бандла vendor-сертификатов).

Для создания корректной цепочки сертификатов выполните действия:

1. Создайте текстовый файл вида:

```
-----BEGIN PRIVATE KEY-----
.....
.....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
```

2. Добавьте в блок (**BEGIN PRIVATE KEY**) ***расшифрованный*** приватный ключ.

Если Центр сертификации выдал приватный ключ в зашифрованном виде, расшифруйте его с помощью passphrase (фразы-пароля).

3. В каждый из блоков (**BEGIN CERTIFICATE**) добавьте сертификат. В начало - сертификат на домен, следом - сертификаты из бандла vendor-сертификатов (если они есть), в самый конец - корневой сертификат. Файл должен получить такую структуру:

```
Приватный ключ
Сертификат на домен
Сертификат из состава бандла vendor-сертификатов (при наличии)
...
Основной (корневой) сертификат
```

4. Сохраните файл с расширением **.pem** и загрузите его на Ideco NGFW Novum.

Конвертация сертификата из формата pkcs12 в формат pem с помощью openssl

> Для конвертации сертификата с помощью openssl на Windows воспользуйтесь ссылкой для загрузки OpenSSL на компьютер.

Для конвертации сертификата из формата **pkcs12** в формат **pem** выполните действия:

1. Откройте командную строку.

2. Введите команду `openssl pkcs12 -in certificate.pkcs12 -out certificate.pem` (сконвертирует сертификат в нужный формат), где:

- **certificate.pkcs12** - исходный сертификат который был получен у центра сертификации.
- **certificate.pem** - результат конвертации.

3. Откройте полученный файл и убедитесь, что файл имеет структуру:

```
-----BEGIN CERTIFICATE-----
..............
..............
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
..............
..............
-----END PRIVATE KEY-----
```

Если в сертификате написано `--BEGIN ENCRYPTED PRIVATE KEY--`, расшифруйте его, введя в OpenSSL команду

`openssl rsa -in certificate.pem -out certificate_decoded.pem`, где:

- **certificate.pem** - файл который был получен после конвертации.
- **certificate_decode.pem** - результат расшифровки.

Слабый ключ RSA в корневом сертификате

При загрузке сертификата с RSA-ключом 1024 бит или меньше возникает ошибка:



Сертификат считается криптографически слабым и небезопасным. Рекомендуется минимум 2048 бит для RSA.

Для изменения RSA-ключа выполните действия:

1. Откройте командную строку.

2. Проверьте размер ключа сертификата:

```
openssl x509 -in client_cert.pem -text -noout | grep "Public-Key"
```

- `client_cert.pem` - имя файла сертификата.

Пример результата:

```
Public-Key: (1024 bit)
```

3. Сгенерируйте новый RSA-ключ:

```
openssl genpkey -algorithm RSA -out client_new.key -pkeyopt rsa_keygen_bits:2048
```

- `client_new.key` - имя файла, в который будет сохранен новый приватный ключ.
- `rsa_keygen_bits` - 2048 или 4096 бит.

4. Создайте запрос на выпуск сертификата - CSR (Certificate Signing Request):

```
openssl req -new -key client_new.key -out client_new.csr -subj "/C=RU/ST=Moscow/L=Moscow/O=Company/OU=IT/CN=client.example.co
```

- `client_new.key` - имя файла с новым приватным ключом.
- `client_new.csr` - имя файла, куда сохранится запрос на сертификат.
- `"/C=RU/ST=Moscow/L=Moscow/O=Company/OU=IT/CN=client.example.com"` - данные субъекта сертификата:
  - `C` - страна.
  - `ST` - регион/штат.
  - `L` - город.
  - `O` - организация.
  - `OU` - подразделение.
  - `CN` - Common Name, имя сертификата.

5. Отправьте CSR в CA (сертификационный центр). В результате будет получен новый сертификат `client_new.crt` с указанным в пункте 3 размером RSA-ключа.

6. Загрузите новый сертификат в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**, нажав кнопку **Загрузить корневой сертификат**.

Создание самоподписанного сертификата с помощью PowerShell

Классический контекст | Высокопроизводительный контекст

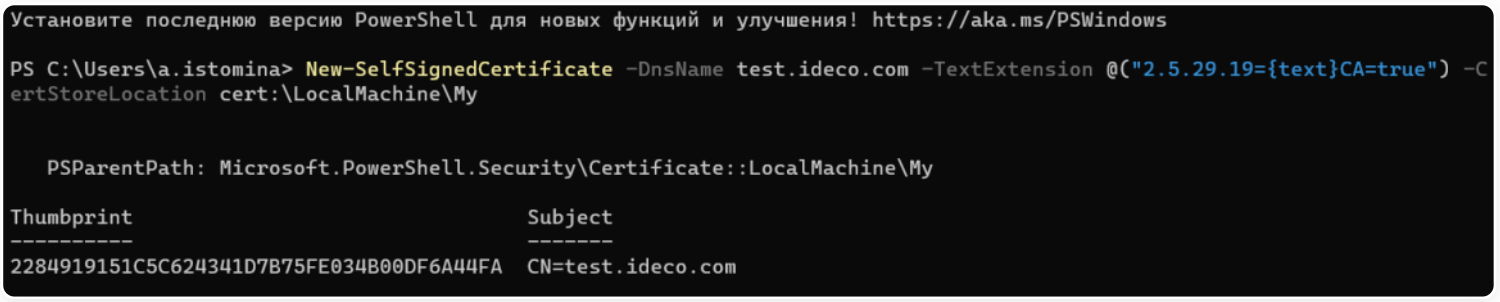
Чтобы создать корневой (самоподписанный) сертификат с помощью PowerShell, выполните следующие действия:

1. Запустите PowerShell от имени администратора.

2. Сгенерируйте сертификат, выполнив команду:

```
New-SelfSignedCertificate -DnsName test.ideco.com -TextExtension @("2.5.29.19={text}CA=true") -CertStoreLocation cert:\LocalM
```

Где `test.ideco.com` - домен.



Для просмотра сгенерированного сертификата выполните команду `certlm.msc`.

3. Сформируйте пароль для сертификата:

```
$CertPassword = ConvertTo-SecureString -String “12345” -Force -AsPlainText
```

Где `12345` - пароль.

4. Экспортируйте сертификат выполнив команду:

```
Export-PfxCertificate -Cert cert:\LocalMachine\My\2284919151C5C624341D7B75FE034B00DF6A44FA -FilePath C:\Users\pende\ssl\test.
```

- `2284919151C5C624341D7B75FE034B00DF6A44FA` - идентификатор сертификата полученный на шаге 2;
- `C:\Users\pende\ssl\test.ideco.pfx` - путь до папки, в которую требуется сохранить сертификат (проверьте корректность сертификата во избежание ошибок).

5. Конвертируйте сертификат в расширение .pem (пример конвертора).

Для загрузки сертификата на сервер воспользуйтесь статьей Загрузка SSL-сертификата на сервер

Создание самоподписанного корневого сертификата с помощью OpenSSL

Классический контекст | Высокопроизводительный контекст

Для генерации самоподписанного корневого сертификата с применением эллиптической кривой (ECC) выполните действия:

1. Сгенерируйте ECDSA-ключ:

```
openssl ecparam -name prime256v1 -genkey -out ecc-key.pem
```

- `ecparam` - работа с параметрами эллиптических кривых.
- `-name prime256v1` - выбор эллиптической кривой **NIST P-256**.
- `-genkey` - генерация нового приватного ключа.
- `-out ecc-key.pem` - сохранение ключа в файле **ecc-key.pem**.

2. Создайте самоподписанный сертификат:

```
openssl req \
-x509 \
-new \
-key ecc-key.pem \
-out cert.pem \
-days 3650 \
-sha256 \
-subj "/CN=MyRootCA/C=RU/ST=SomeState/L=SomeCity/O=MyOrganization/OU=RootCA" \
-nodes \
-addext "authorityKeyIdentifier=keyid,issuer" \
-addext "basicConstraints=CA:TRUE" \
-addext "keyUsage = keyCertSign, cRLSign, digitalSignature"
```

- `req -x509` - создание самоподписанного сертификата.
- `-new` - генерация нового запроса.
- `-key ecc-key.pem` - использование ранее сгенерированного ECC-ключа.
- `-out cert.pem` - сохранение сертификата в файле cert.pem.
- `-days 3650` - установка срока действия сертификата на 10 лет (3650 дней).
- `-sha256` - использование хеш-алгоритма SHA-256 для подписи.
- `-subj` - указание subject. Поле Common Name (CN) требует обязательного заполнения. При необходимости можно указать и другие поля:
  - `/CN=MyRootCA` - наименование сертификата.
  - `C=RU` - код страны в формате ISO 3166-1 alpha-2 (например, RU).
  - `ST=SomeState` - название региона или области (например, Moscow).
  - `L=SomeCity` - название города (например, Saint Petersburg).
  - `O=MyOrganization` - название организации.
  - `OU=RootCA` - название подразделения организации.
- `-nodes` - отсутствие шифрования приватного ключа паролем.
- `-addext "authorityKeyIdentifier=keyid,issuer"` - указание метода идентификации центра сертификации (CA) для цепочки сертификатов.
- `-addext basicConstraints=CA:TRUE"` - присвоение статусу сертификата CA, что позволяет подписывать другие сертификаты.
- `-addext "keyUsage = keyCertSign, cRLSign, digitalSignature"` - разрешение на выполнение цифровых подписей, подписей сертификатов и подписей списков отозванных сертификатов (CRL):
  - `keyCertSign` - может использоваться для подписи других сертификатов.
  - `cRLSign` - может использоваться для подписи CRL (Certificate Revocation List).
  - `digitalSignature` - может использоваться для цифровой подписи данных (параметр необязателен).

Результат: создание самоподписанный сертификата `cert.pem`, который:

- Включает приватный ECDSA-ключ `ecc-key.pem`.

- Действует как центр сертификации (CA) и может подписывать другие сертификаты.
- Включает Common Name: MyRootCA.
- Подписан алгоритмом SHA-256.
- Действителен в течение 10 лет.

Для загрузки сертификата на сервер воспользуйтесь статьей Загрузка SSL-сертификата на сервер

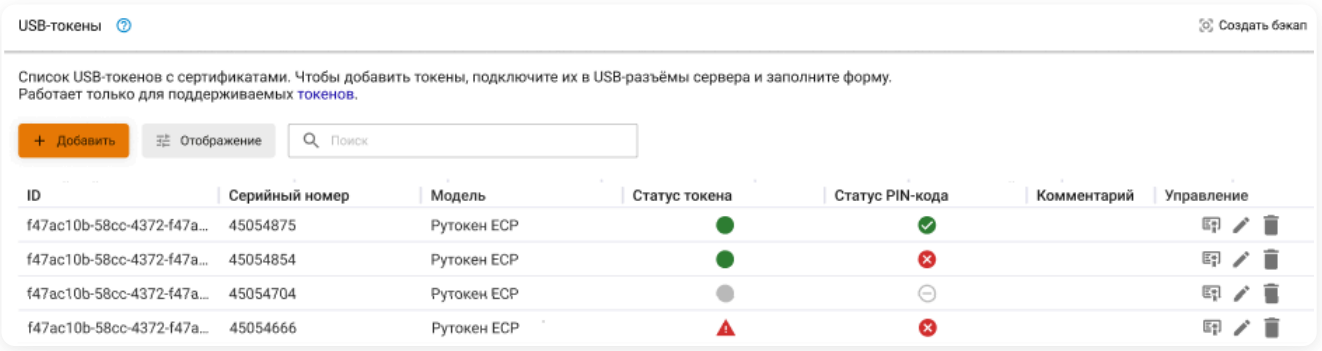
USB-токены

Функциональность доступна только в **Системном контексте**.

USB-токен - это аппаратное устройство для безопасного хранения цифровых сертификатов и работы с приватными ключами.

Ideco NGFW Novum поддерживает только USB-токен модели **Рутокен ЭЦП 3.0**. USB-токены других моделей могут не отображаться в веб-интерфейсе **Ideco NGFW Novum**.

В таблице USB-токенов представлена информация о серийном номере, модели, метке ключа и корректности настройки USB-токена:



Статусы токена

- токен подключен в USB-разъем сервера.

- токен не подключен в USB-разъем сервера.

- возникла ошибка или токен заблокирован.

Статусы PIN-кода

- верный PIN-код.

- неизвестный статус PIN-кода:

- PIN-код был введен, но USB-токен не был установлен в USB-разъем сервера.
- USB-токен с верным PIN-кодом был извлечен из USB-разъема сервера.

- неверный PIN-код.

Чтобы проверить содержимое USB-токенов и убедиться, что на токены загружены все необходимые сертификаты, нажмите на у соответствующего USB-токена.

Подготовка USB-токена

На USB-токен необходимо загрузить два сертификата: доверенный сертификат и сертификат с приватным ключом, который будет использоваться в качестве локального сертификата NGFW. При подготовке USB-токена запишите серийный номер и PIN-код. Это потребуется для дальнейшей настройки.

Пример генерации сертификатов приведен в статье.

Процесс подготовки USB-токена ЭЦП версии 3.0 от компании **Рутокен** подробно описан в документации производителя. В помощь предлагаются статьи, которые помогут разобраться как узнать серийный номер, сменить PIN-код и загрузить сертификаты на USB-токен:

- Панель управления Рутокен для ОС Windows
- Центр Управления Рутокен для ОС GNU/Linux
- Рутокен и OpenSSL
- Рутокен для КриптоПро

Если требуется сгенерировать сертификаты для тестирования ГОСТ VPN, рекомендуем воспользоваться статьей от производителя.

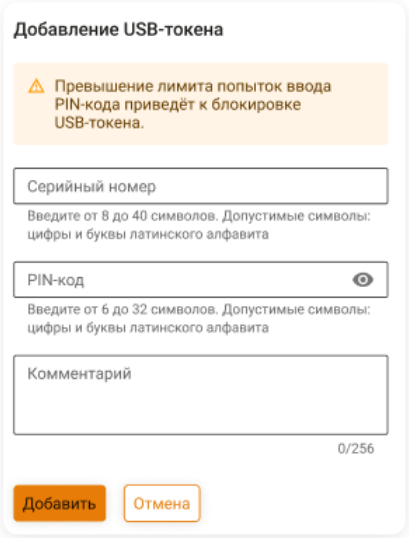
Настройка USB-токена на Ideco NGFW Novum

Перед добавлением USB-токена на Ideco NGFW Novum смените PIN-код пользователя, поскольку изначально на токенах от компании Рутокен установлен PIN-код по умолчанию: `12345678`. Инструкция по смене PIN-кода - по ссылке.

Для работы Ideco NGFW Novum с USB-токеном введите корректный PIN-код. NGFW Novum использует PIN-код для получения доступа к токену сразу после ввода и сохранения параметров токена. Если PIN-код не верный, NGFW Novum остановит попытки получить доступ до ввода и сохранения нового PIN-кода.

При превышении лимита попыток неправильного ввода PIN-кода устройство будет заблокировано. Лимит устанавливается производителем и считается до правильного ввода PIN-кода.

Чтобы добавить новый USB-токен, подключите USB-токен к USB-разъему вашего сервера. Нажмите **Добавить** и заполните поля:



- **Серийный номер** - формат для **Рутокен ЭЦП 3.0** представлен в виде десятизначного числа. Например, `1157977130`. Его можно найти на корпусе USB-токена или:
  - Для Linux - в Центре управления Рутокеном в разделе Об устройстве.
  - Для Windows - в Панели управления Рутокеном
- **PIN-код** - введите установленный ранее PIN-код пользователя.
- **Комментарий** - необязательное поле.

Netflow

Классический контекст | Высокопроизводительный контекст | API

Netflow - проприетарный открытый протокол, разработанный Cisco для мониторинга статистики трафика в сети. Ideco NGFW Novum выступает в качестве сенсора-экспортера, который собирает статистику при прохождении через него трафика.

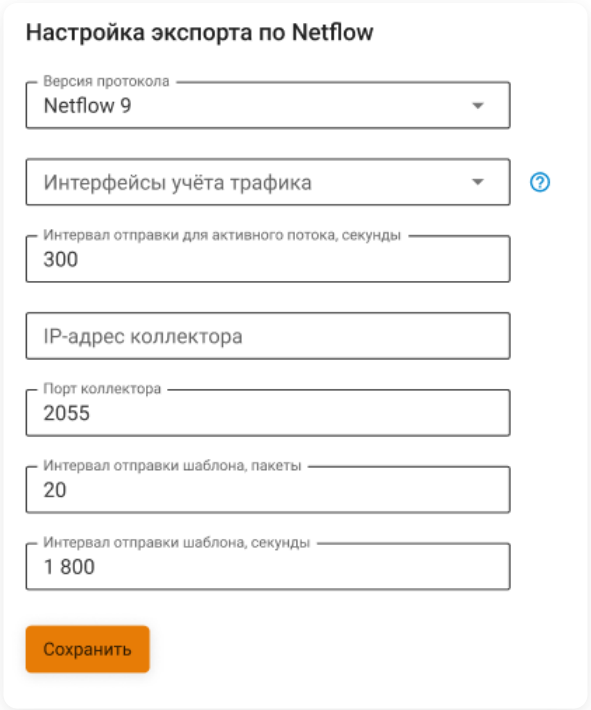
Netflow обеспечивает сбор информации об IP-трафике, обрабатываемом сетевыми устройствами (L3-коммутаторы, маршрутизаторы, сенсоры). Каждый поток является однонаправленным, т.е. каждое двунаправленное соединение **src <–> dst** интерпретируется как два потока: **src → dst** и **dst → src**.

Настройка экспорта по Netflow

При включении Netflow рекомендуем настроить индексы Netflow для интерфейсов, статистику по которым планируется передавать. Это можно сделать в настройках сетевых интерфейсов, значение по умолчанию - 0. Индексы Netflow не меняются при включении/выключении или изменении интерфейса.

Идентификаторами потоков служат индексы Netflow. Потоки с одинаковыми индексами для сбора статистики проходят через один интерфейс учета трафика.

Для настройки Netflow перейдите в **Сервисы → Netflow**:



- **Версия протокола** - выберите версию протокола Netflow. Доступны Netflow 5, Netflow 9 (по умолчанию) и Netflow 10 (IPFIX).
- **Интерфейсы учета трафика** - выберите интерфейсы, трафик которых хотите отслеживать. Если не заполнены, статистика не будет экспортироваться.
- **Интервал отправки для активного потока, секунды** - введите временной интервал, через который Ideco NGFW Novum будет отправлять на коллектор отчеты по потокам, которые не успели завершиться (информация о завершенных потоках отправляется по завершении). Допустимые значения: от 60 до 3600, по умолчанию - 300.
- **IP-адрес коллектора** - введите IP-адрес коллектора данных. Если не заполнен, статистика не будет экспортироваться.
- **Порт коллектора** - введите номер UDP-порта коллектора данных, используемого для приема пакетов Netflow.
- **Интервал отправки шаблона, пакеты** - количество пакетов, через которое на коллектор будет послан шаблон. Допустимые значения: от 10 до 600, по умолчанию - 20. Доступно только при выборе Netflow 9 или Netflow 10 (IPFIX) в поле **Версия протокола**.
- **Интервал отправки шаблона, секунды** - количество секунд, через которое на коллектор будет послан шаблон. Допустимые значения: от 60 до 86400, по умолчанию - 1800. Доступно только при выборе Netflow 9 или Netflow 10 (IPFIX) в поле **Версия протокола**.

При сборе статистики с интерфейсов Ethernet + PPTP/L2TP/PPPoE будет учитываться трафик не на родительском Veth, а на PPP-интерфейсе (Eppp), трафик с которого инкапсулируется в родительский.

Данные в Netflow передаются по протоколу UDP. Поэтому пока коллектор не получит шаблон передаваемых данных, отчеты будут игнорироваться. Правильная настройка полей **Интервал отправки шаблона** позволяет минимизировать потери при перезагрузке или потере связи с коллектором.

Структура передаваемых на коллектор данных

Структура заголовка и записей для Netflow 5 доступна по ссылке.

Структура шаблона для Netflow 9 и Netflow 10 (IPFIX) представлена в таблице:

Поле	Код поля	Длина поля, байт	Описание
IPV4_SRC_ADDR	8	4	IP-адрес источника
IPV4_DST_ADDR	12	4	IP-адрес назначения
INPUT_SNMP	10	2	Индекс входящего интерфейса
OUTPUT_SNMP	14	2	Индекс исходящего интерфейса
IN_BYTES	1	8	Количество байт, переданных в потоке
IN_PKTS	2	8	Количество пакетов, переданных в потоке
FIRST_SWITCHED	22	4	Время начала потока (sys uptime ms)
LAST_SWITCHED	21	4	Время последнего прохождения трафика в потоке (sys uptime ms)
L4_SRC_PORT	7	2	Порт источника
L4_DST_PORT	11	2	Порт назначения
TCP_FLAGS	6	1	Флаги TCP (суммарно зафиксированные за время наблюдения потока)
PROTOCOL	4	1	Код протокола
SRC_MASK	9	1	Маска IP-адреса источника
DST_MASK	13	1	Маска IP-адреса назначения

Syslog

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Syslog**: `ideco-logs-backend`, `ideco-monitor-backend`.

Список служб для других разделов доступен по ссылке.

Syslog - стандартный протокол для сбора, передачи и хранения системных сообщений от устройств и сервисов. Обеспечивает централизованный сбор информации о событиях в сети.

В Ideco NGFW Novum **Syslog** используется для отправки логов на удаленный сервер. Это позволяет администраторам осуществлять мониторинг безопасности, анализировать инциденты, выполнять диагностику проблем.

Пересылка системных сообщений

Чтобы настроить пересылку системных сообщений, перейдите в раздел **Сервисы** → **Syslog** и выполните действия:

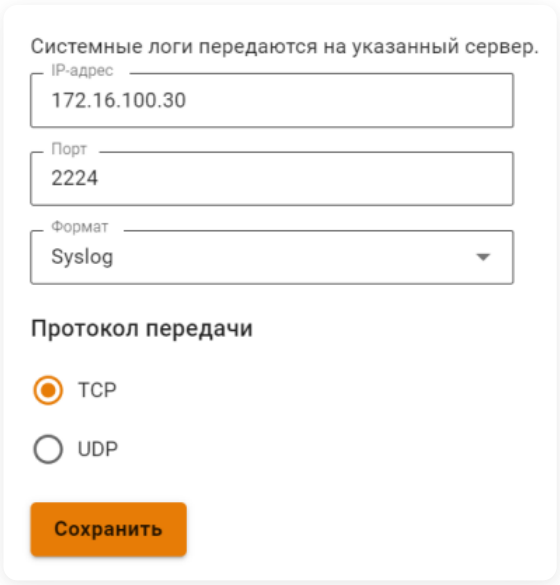
1. Укажите IP-адрес сервера-коллектора (любой локальный или публичный IP-адрес).

2. В поле **Порт** укажите порт, настроенный на сервере-коллекторе (в диапазоне от 1 до 65535).

3. Выберите формат передаваемых системных сообщений (Syslog или CEF).

4. Выберите протокол передачи системных логов - TCP или UDP.

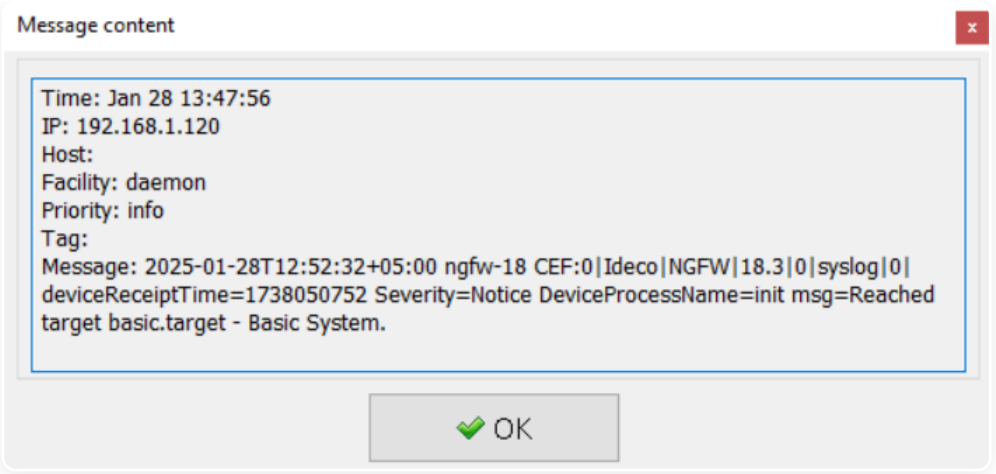
5. Нажмите **Сохранить** и включите опцию Syslog:



Рекомендуется передавать логи по протоколу TCP, так как он гарантирует доставку и соблюдает последовательность сообщений.

Расшифровка передаваемых логов

В статье представлены примеры сообщений (message) в форматах CEF и Syslog (скриншот из Visual Syslog server):



Message начинается со строки вида:

CEF

```
2024-11-18T15:38:54+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1759402874 Severity=Informational
```

где:

- `2024-11-18T15:38:54+05:00` - время события в Ideco NGFW Novum;
- `ideco-ngfw` - hostname сервера NGFW Novum, заданный в левом верхнем углу веб-интерфейса;
- `CEF:0` - версия формата CEF;
- `Ideco` - вендор;
- `NGFW` - название продукта;
- `21.0` - версия продукта;
- `0|syslog|0` - идентификатор лога, постоянный для NGFW Novum. Состоит из трех полей: идентификатор типа события, описание события, важность события.
- `deviceReceiptTime` - время события в системе NGFW Novum, может не совпадать с временем получения события по Syslog;
- `Severity` - уровень значимости события. Возможные значения:
  - `Emergency` - чрезвычайная ситуация;
  - `Alert` - тревога;
  - `Critical` - критическая ошибка;
  - `Error` - ошибка;
  - `Warning` - предупреждение;
  - `Notice` - уведомление;
  - `Informational` - информация;
  - `Debug` - отладка.

Syslog

```
2025-08-27T11:38:13+05:00 ideco-ngfw traffic-journal
```

где:

- `2025-08-27T11:38:13+05:00` - время события в Ideco NGFW Novum;
- `ideco-ngfw` - hostname сервера NGFW Novum, заданный в левом верхнем углу веб-интерфейса.

Уровень значимости события, передаваемый в столбец **Priority**:

- `emerg` - чрезвычайная ситуация;
- `alert` - тревога;
- `crit` - критическая ошибка;
- `err` - ошибка;
- `warning` - предупреждение;
- `notice` - уведомление;
- `info` - информация;

- `debug` - отладка.

Журнал Система

CEF:

```
2026-02-20T14:44:24+05:00 bez-nazvaniya-8fbd0bda-5d9d-4354-8bda-3c49bbcdf23b CEF:0|Ideco|NGFW|21.11|0|syslog|0|deviceReceiptT
```

Syslog:

```
2026-02-20T14:31:30+05:00 bez-nazvaniya-8fbd0bda-5d9d-4354-8bda-3c49bbcdf23b kav-scanner - - - Update in progress, 6 complete
```

Ключ	Описание	
DeviceProcessName	<название_службы>	Название источника журнала. Список всех служб доступен по ссылке

SIEM не сможет извлечь ключевые поля из сообщений журнала для последующего анализа. Такие сообщения доступны только для просмотра в исходном виде. С другими примерами можно ознакомиться по ссылке.

Журнал Трафик

CEF:

```
2025-08-27T11:38:13+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.1|0|syslog|0|deviceReceiptTime=1759385517 Severity=Informational dev
```

Syslog:

```
2025-08-27T11:38:13+05:00 ideco-ngfw traffic-journal - - - result:accept, rule_id:2, table:inp, action:l7_inspection, ips_pro
```

Ключ CEF	Ключ Syslog	Описание
deviceProcessName	traffic-journal	Название источника журнала
outcome	result	Общий результат проверки. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет
deviceEventClassId	rule_id	Идентификатор правила **Межсетевого экрана**. Пустая строка означает отсутствие значения.
name	table	Название таблицы, в которой сработало правило. Возможные значения: • `absent` - отсутствие значения; • `fwd` - таблица **FORWARD** раздела **Межсетевой экран** Ideco NGFW Novum; • `fwd_a` - постправило FORWARD Ideco Center; • `fwd_b` - предправило FORWARD Ideco Center; • `fwd_s` - системное правило FORWARD; • `inp` - таблица **INPUT** раздела **Межсетевой экран** Ideco NGFW Novum; • `inp_a` - постправило INPUT Ideco Center; • `inp_b` - предправило INPUT Ideco Center; • `inp_s` - системное правило INPUT.
act	action	Действие правила **Межсетевого экрана**. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет • `l7_inspection` - перенаправление в профиль безопасности
cs1	ips_profile	Название IPS профиля

cn1	ips_action	Действие IPS профиля. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет
cn2	ips_signature_id	Идентификатор сигнатуры, сработавшей в профиле
cs2	dpi_profile	Название DPI профиля
cn3	dpi_action	Действие DPI профиля. Возможные значения: • `absent` - отсутствие значения • `accept` - разрешение • `drop` - запрет
destinationServiceName	dpi_app	Название приложения
app	dpi_protocol	Название протокола прикладного уровня
proto	protocol	Название протокола
sourceAddress	src_ip	IP-адрес источника
sourcePort	src_port	Порт источника. Значение `0` - отсутствие данных
sourceZoneExternalID	src_zone	Название зоны источника
suser	src_user_name	Имя пользователя источника
suid	src_user_login	Логин пользователя источника
spriv	src_group	Название группы источника
cs3	src_location_name	Название локации источника
-	src_location_code	Код локации источника
destinationAddress	dst_ip	IP-адрес назначения
destinationPort	dst_port	Порт назначения. Значение `0` - отсутствие данных
destinationZoneExternalID	dst_zone	Название зоны назначения
duser	dst_user_name	Имя пользователя назначения
duid	dst_user_login	Логин пользователя назначения
dpriv	dst_group	Название группы назначения
cs4	dst_location_name	Название локации назначения
-	dst_location_code	Код локации назначения
cs5	dnat_rule_id	Идентификатор DNAT-правила. Пустая строка - отсутствие значения
destinationTranslatedAddress	dnat_ip	IP-адрес, на который был изменен адрес назначения
destinationTranslatedPort	dnat_port	Порт, на который был изменен порт назначения
cs6	snat_rule_id	Идентификатор SNAT-правила. Пустая строка - отсутствие значения
sourceTranslatedAddress	snat_ip	IP-адрес, на который был изменен адрес источника
deviceExternalId	cluster_id	Идентификатор кластера
-	cluster_name	Название кластера
externalId	vce_id	Идентификатор VCE
-	vce_name	Название VCE
eventId	flow_id	Идентификатор соединения. Уникален для каждой записи
start	nflog_timestamp	Служебная информация

Журнал Веб-трафик

CEF:

```
2025-10-02T16:01:14+05:00 ngfw CEF:0|Ideco|NGFW|21.1|0|syslog|0|deviceReceiptTime=1759402874 Severity=Informational DevicePro
```

Syslog:

```
2025-08-27T11:43:05+05:00 ideco-ngfw web-proxy - - - domain:st3-24.vk.com, uri:, categories:['РЎРѕС†РёР°Р»СЊРЅС‹Рµ СЃРµС‚Рё']
```

Ключ CEF	**Ключ Syslog**	**Описание**

DeviceProcessName	web-proxy	Название источника журнала
DestinationHostName	domain	Домен сайта
RequestUrl	uri	URI сайта, включающий все, кроме доменного имени и якорей
cat	categories	Список категорий, по которым был классифицирован сайт
in	incoming_traffic	Входящий трафик, байт
out	outgoing_traffic	Исходящий трафик, байт
FlexNumber1	traffic_amount	Общий трафик, байт
deviceAction	action	Результат проверки Контент-фильтра. Возможные значения: • `bump` - расшифровать • `allow` - разрешить • `deny` - запретить • `redirect` - перенаправить на другой сайт. Действует только на расшифрованный трафик
reason	blocked_reason	Причины блокировки: имя категории, имя словаря, HTTP-метод или MIME-тип, по которым был запрещен доступ к сайту
cs1	redirected_to	Если запрос попал под правило перенаправления, отображает url куда перенаправило, если нет - пустая строка
cs2	rule_name	Название правила Контент-фильтра
SourceAddress	source_ip	IP-адрес источника
SourcePort	source_port	Порт источника, число
DestinationAddress	destination_ip	IP-адрес назначения. Значение `0.0.0.0` означает отсутствие адреса назначения
DestinationPort	destination_port	Порт назначения, число. Значение `0` - отсутствие данных
ApplicationProtocol	proto_info	Версия HTTP-протокола. Отсутствие данных отображается пустой строкой
requestMethod	method	Метод, с которым был произведен запрос. Отсутствие данных отображается пустой строкой. При отображении в таблице GET-запрос - скачивание, остальные запросы - загрузка
Code	status_code	Код HTTP-ответа. Значение `0` - отсутствие данных
cs3	mime	Content-Type HTTP-запроса. Отсутствие данных отображается пустой строкой
requestClientApplication	useragent	User-Agent HTTP-запроса. Отсутствие данных отображается пустой строкой
cs4	user_name	Имя пользователя, который авторизован с IP источника
-	login	Логин пользователя
cs5	group_name	Имя группы, в которую входит пользователь
cs6	referer	Referer HTTP-запроса. Отсутствие данных отображается пустой строкой
cs7	vce_id	Идентификатор VCE
cs8	vce_name	Название VCE

Предотвращение вторжений

CEF:

```
2025-10-03T14:06:02+05:00 ngfw CEF:0|Ideco|NGFW|21.1|0|syslog|0|deviceReceiptTime=1759482362 Severity=Warning DeviceCustomStr
```

Syslog:

```
2025-10-03T14:01:38+05:00 ngfw suricata - - - flow_id:2113278673659098, in_iface:, sensor_name:ideco-ips, event_type:alert, s
```

Ключ CEF	**Ключ Syslog**	**Описание**
-	suricata	Название источника журнала
DeviceCustomString1	flow_id	Внутренний идентификатор системы **Предотвращения вторжений** flow (сессии)
DeviceInboundInterface	in_iface	Идентификатор входящего интерфейса
DeviceProcessName	sensor_name	Имя экземпляра системы **Предотвращения вторжений**
DeviceCustomString5	event_type	Тип события
SourceAddress	src_ip	IP-адрес источника

DeviceCustomString1	src_ip_type	Принадлежность адреса источника. Возможные значения: • `local` - локальный • `external` - внешний • `unknown` - принадлежность не определена
SourcePort	src_port	Порт источника
SourceCountry	src_country	Название местоположения источника
DeviceCustomString2	src_country_code	ISO-код страны источника
DeviceCustomString3	src_session_uuid	Внутренний идентификатор сессии Ideco NGFW Novum источника
SourceUserID	src_user_id	Идентификатор пользователя источника
SourceUserName	src_user_name	Имя пользователя источника
DestinationAddress	dest_ip	IP-адрес назначения
DeviceCustomString4	dest_ip_type	Принадлежность адреса назначения. Возможные значения: • `local` - локальный • `external` - внешний • `unknown` - принадлежность не определена
DestinationPort	dest_port	Порт назначения
DestinationCountry	dest_country	Название местоположения назначения
DeviceCustomString5	dest_country_code	ISO-код страны назначения
DeviceCustomString6	dest_session_uuid	Внутренний идентификатор сессии Ideco NGFW Novum назначения
DestinationUserID	dest_user_object_id	Идентификатор пользователя назначения
DestinationUserName	dest_user_name	Имя пользователя назначения
TransportProtocol	proto	Протокол
DeviceEventClassID	alert.signature_id	Идентификатор правила системы предотвращения вторжений
Message	alert.signature	Сообщение из сработавшего правила
DeviceEventCategory	alert.category	Описание колонки в веб-интерфейсе **События безопасности**. Соответствие `alert.category` → `alert.signature` описаны в файле.
Severity	alert.severity	Уровень угрозы, может принимать значения `1`, `2`, `3` и `256`, где `1` - самый высокий уровень угрозы
DeviceCustomString8	alert.gid	GID угрозы
DeviceCustomString9	alert.action	Действие по отношению к угрозе. Возможные значения: • `blocked` - блокировать • `allowed` - разрешить

Служебные поля результата анализа HTTP-трафика. Заполняются, если в процессе анализа трафика был определен HTTP-протокол:

DestinationHostName	http.hostname	Идентификатор хоста
RequestUrl	http.url	URL, на который был запрос
RequestClientApplication	http.http_user_agent	Информация, идентифицирующая HTTP-клиента

Служебные поля flow (сессии):

FlexNumber1	flow.pkts_toserver	Количество пакетов, переданное от клиента к серверу
FlexNumber2	flow.pkts_toclient	Количество пакетов, переданное от сервера к клиенту
BytesIn	flow.bytes_toserver	Количество байт, переданное от клиента к серверу
BytesOut	flow.bytes_toclient	Количество байт, переданное от сервера к клиенту
StartTime	flow.start	Начало сессии
EndTime	flow.end	Окончание сессии
FlexNumber3	flow.age	Возраст сессии
DeviceCustomString11	flow.state	Текущее состояние
DeviceCustomString12	flow.reason	Запущен ли IPsec в режиме отладки
FlexNumber4	flow.alerted	Сгенерировался ли поток `alert`

Состояние флага TCP flow(сессии):

DeviceCustomString14	tcp.tcp_flags	Значение поля flags в заголовке TCP
DeviceCustomString15	tcp.tcp_flags_ts	Timestamp флаги.
DeviceCustomString16	tcp.tcp_flags_tc	Флаг Truncated response
FlexNumber5	tcp.cwr	Флаг TCP-пакета, информирующий отправителя, что получен пакет с установленным флагом ECE (Подробнее в RFC 3186)
FlexNumber6	tcp.ecn	Флаг TCP-пакета, информирующий получателя, что узел способен на явное уведомление о перегрузке сети
FlexNumber7	tcp.urg	Флаг TCP-пакета, указывающий важность пакета
FlexNumber8	tcp.ack	Флаг получения TCP-пакета
FlexNumber9	tcp.psh	Флаг TCP-пакета, информирующий получателя, что все данные переданы и можно передать их приложению
FlexNumber10	tcp.rst	Флаг TCP-пакета, указывающий, что соединение завершено в аварийном режиме
FlexNumber11	tcp.syn	Флаг TCP-пакета, отвечающий за установку соединения
FlexNumber12	tcp.fin	Флаг TCP-пакета, указывающий на завершение соединения в штатном порядке
DeviceCustomString17	tcp.state	Состояние сеанса TCP

Ключ	**Описание**	
DeviceCustomString18	vce_id	Идентификатор VCE
DeviceCustomString19	vce_name	Название VCE

Журнал Web Application Firewall

CEF:

```
2026-04-03T15:36:50+05:00 ideco-ngfw CEF:0|Ideco|NGFW|22.0|0|syslog|0|rt=1775212610 deviceProcessName=modsecurity act=allowed
```

Syslog:

```
2026-04-03T15:32:10+05:00 ideco-ngfw waf - - - id:01KN9ED1B23GT115YHSM406MKJ, blocked:true, rule_file:/run/ideco-reverse-back
```

Ключ CEF	**Ключ Syslog**	**Описание**
deviceProcessName	waf	Название источника журнала
rt	-	Время события в формате Unix Timestamp
act	blocked	Действие, выполненное WAF. Возможные значения: • `allowed` - запрос пропущен • `blocked` - запрос заблокирован
msg	message	Текстовое сообщение из сработавшего правила
reason	nginx_message	Описание причины срабатывания правила
cat	category_name	Название категории правила
externalId	unique_id	Уникальный идентификатор HTTP-запроса
deviceExternalId	vce_id	Идентификатор VCE
requestMethod	-	HTTP-метод запроса: `GET`, `POST`
request	uri	URI запроса с параметрами строки запроса
src	nginx_client	IP-адрес источника
dst	nginx_server	IP-адрес назначения
dhost	nginx_host	Имя хоста защищаемого ресурса
filePath	rule_file	Путь к файлу с правилом, по которому сработал WAF
cs1	profile_id	Идентификатор профиля WAF
cs2	profile_name	Название профиля WAF
cs3	category_id	Идентификатор категории правила
cs4	ruleset_ver	Версия набора правил
cs5	ref	Координаты совпадения в запросе
cs6	data	Данные, которые послужили причиной срабатывания правила
cn1	rule_id	Идентификатор правила

cn2	rule_line	Номер строки в файле правил
cn3	severity	Уровень критичности правила. Возможные значения: • `0` - EMERGENCY • `1` - ALERT • `2` - CRITICAL • `3` - ERROR • `4` - WARNING • `5` - NOTICE • `6` - INFO • `7` - DEBUG
flexString1	nginx_client_country	Название местоположения источника
flexString2	tags	Теги правила, разделенные пробелом
sproc	vce_name	Название VCE
-	id	Идентификатор события в журнале WAF
-	hostname	Имя защищаемого ресурса
-	nginx_client_country_code	ISO-код страны источника
-	nginx_request	Стартовая строка HTTP-запроса (метод, URI, версия протокола)

Журнал Действия администраторов

CEF:

```
2026-01-21T12:52:57+05:00 bez-nazvaniya-2a6874b3-8156-4591-af99-4edc1e9f24d9 CEF:0|Ideco|NGFW|21.11|0|syslog|0|deviceProcessN
```

Syslog:

```
2026-01-21T12:48:59+05:00 bez-nazvaniya-2a6874b3-8156-4591-af99-4edc1e9f24d9 admin-audit - - - admin_id:6b17b3ce-2727-4318-95
```

Ключ CEF	**Ключ Syslog**	**Описание**
deviceProcessName	admin-audit	Название источника журнала
rt	-	Время события в формате Unix Timestamp
suid	admin_id	Идентификатор администратора
cs1	admin_login	Логин администратора
suser	admin_name	Имя администратора
dproc	backend	Название службы
src	ip	IP-адрес администратора
requestMethod	request_method	HTTP-метод запроса (GET, POST и т.д.)
cs2	request_body	Тело входящего запроса
request	request_url	URL, на который отправлен запрос
outcome	response_code	Код HTTP-ответа
cs3	response_body	Тело ответа
msg	message	Текстовое сообщение или описание события
cs4	target_id	Идентификатор целевого объекта (ресурса, сущности, операции)
deviceExternalId	vce_id	Идентификатор VCE
cs5	vce_name	Название VCE

Журнал DNS-запросы

CEF:

```
2026-02-04T11:00:15+05:00 bez-nazvaniya-23000007-c6d3-f255-a811-03c1a64d3b0e CEF: 0|Ideco|NGFW|21.12|0|syslog|0|deviceReceipt
```

Syslog:

```
2026-02-04T10:28:41+05:00 bez-nazvaniya-23000007-c6d3-f255-a811-03c1a64d3b0e dns-journal action:reply, protocol:UDP, src_ip:1
```

Ключ CEF	Ключ Syslog	Описание
deviceProcessName	dns-journal	Название источника журнала
act	action	Результат обработки DNS-запроса: • `query` - перехват запроса к серверу • `reply` - успешно • `cache` - из кэша • `fail` - ошибка
proto	protocol	Название протокола
src	src_ip	IP-адрес источника
request	qname	Доменное имя, указанное в DNS-запросе
cs1	qtype	Тип DNS-запроса (например, A, AAAA, MX, TXT)
cs2	qclass	Класс DNS-запроса (обычно IN - Internet)
cs3	opcode	Код операции DNS (например, стандартный запрос, обновление)
outcome	rcode	Код ответа DNS (результат обработки запроса)
cs4	id_wire	Идентификатор DNS-транзакции
cs5	flags	Флаги DNS-пакета (например, RD, RA, AA, TC)
cs6	answer	Раздел ответов DNS (ресурсные записи ответа)
flexString1	authority	Ресурсные записи секции Authority, указывающие на полномочный источник
flexString2	additional	Ресурсные записи секции Additional с дополнительной информацией
suid	src_user_login	Логин пользователя
suser	src_user_name	Имя пользователя
spriv	src_group	Группа пользователя
externalId	cluster_id	Идентификатор кластера
-	cluster_name	Название кластера
deviceExternalId	vce_id	Идентификатор VCE
sproc	vce_name	Название VCE

Примеры сообщений журнала Система

Авторизация через журнал безопасности AD

CEF:

```
2024-07-18T17:20:22+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1721305222 Severity=Notice DeviceProc
```

Syslog:

```
2024-07-18T16:19:39+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.205.254/32 is authorized as user 'Sanek'. Connec
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.205.254/32 is authorized as user 'Sanek'. Connection made from None, type 'log'.` - сообщение об авторизации пользователя `'Sanek'` через журнал безопасности AD (`type 'log'`).

Веб-авторизация

CEF:

```
2024-11-18T14:54:21+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731923661 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T14:47:11+05:00 ideco-ngfw ideco-web-authd - - - Subnet 192.168.101.25/32 is authorized as user 'user'. Connection
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-web-authd	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.25/32 is authorized as user 'user'. Connection made from None, type 'web'.` - сообщение об авторизации пользователя `'user'` через веб-авторизацию (`type 'web'`).

Авторизация по IP

CEF:

```
2024-11-18T18:51:43+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731937903 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T18:42:45+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.101.25/32 is authorized as user 'user'. Connecti
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.25/32 is authorized as user 'user'. Connection made from None, type 'ip'.` - сообщение об авторизации пользователя `'user'` по IP-адресу (`type 'ip'`).

Авторизация по MAC

CEF:

```
2024-11-18T18:54:21+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731938061 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:01:14+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.101.25/32 is authorized as user 'user'. Connecti
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.25/32 is authorized as user 'user'. Connection made from None, type 'mac'.` - сообщение об авторизации пользователя `'user'` по MAC-адресу (`type 'mac'`).

Авторизация по подсетям

CEF:

```
2024-11-18T19:07:54+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731938874 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:06:08+05:00 ideco-ngfw ideco-auth-backend - - - Subnet 192.168.101.0/24 is authorized as user 'user'. Connectio
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-auth-backend	Название источника журнала

Информация в сообщении:

- `Subnet 192.168.101.0/24 is authorized as user 'user'. Connection made from None, type 'net'.` - сообщение об авторизации пользователя `'user'` по подсети (`type 'net'`).

Авторизация по VPN

CEF:

```
2024-11-18T19:16:18+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731939378 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:17:56+05:00 ideco-ngfw ideco-vpn-authd - - - Subnet 10.128.0.5/32 is authorized as user 'user'. Connection made
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	ideco-vpn-authd	Название источника журнала

Информация в сообщении:

- `Subnet 10.128.0.5/32 is authorized as user 'user'. Connection made from '192.168.1.25', type 'pptp'` - сообщение об авторизации пользователя `'user'` по VPN (`type 'pptp'`).

Авторизация администратора

CEF:

```
2026-02-06T11:58:25+05:00 ngfw-21-server CEF:0|Ideco|NGFW|21.11|0|syslog|0|deviceReceiptTime=1770361105 Severity=Notice Devic
```

Syslog:

```
2026-02-05T16:14:47+05:00 ngfw-21-server ideco-web-backend - - - Admin 'admin' (session: AuthSessionInfo(auth_type='local', a
```

Ключ CEF	Ключ Syslog	Описание
deviceProcessName	ideco-web-backend	Название источника журнала

Информация в сообщении:

- `Admin 'admin' (session: AuthSessionInfo) has been successfully authorized for REST from IP '192.168.101.102'` - сообщение об авторизации администратора `'admin'` через веб-интерфейс с IP-адреса `'192.168.101.102'`.

Описание полей `AuthSessionInfo`:

- `auth_type` - тип авторизации;
- `auth_rule_id` - идентификатор правила, по которому авторизовался администратор;
- `auth_group_alias_id` - идентификатор группы безопасности или группы пользователей, по которой авторизовался администратор AD/ALD/FreeIPA;
- `admin_id` - идентификатор администратора;
- `competence` - список прав доступа администратора;
- `role_id` - идентификатор роли администратора;
- `role_name` - название роли администратора;
- `login` - логин администратора;
- `name` - имя администратора;
- `system_session` - признак системной сессии;
- `domain_name` - название домена при авторизации администратора AD/ALD/FreeIPA;
- `login_timestamp` - время события в формате Unix Timestamp;
- `ip` - IP-адрес, с которого выполнена авторизация;
- `access_method` - способ доступа;
- `remote_cc_session` - подключение к NGFW Novum из Ideco Center;
- `country_code` - ISO-код страны;
- `pid` - идентификатор процесса.

Служба fail2ban

CEF:

```
2024-11-18T19:26:57+05:00 ideco-ngfw CEF:0|Ideco|NGFW|21.0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Notice DeviceProc
```

Syslog:

```
2024-11-18T19:21:54+05:00 ideco-ngfw fail2ban - - - INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-18 19:21:54
```

Ключ	**Описание**	
DeviceProcessName	fail2ban	Название источника журнала

Информация в сообщении:

- `INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-18 19:21:54` - факт обнаружения правил безопасности с указанием группы правил (`[utm-vpn-authd]`), IP-адреса и даты/времени.
- `NOTICE [utm-vpn-authd] Ban 192.168.1.25` - факт блокировки или разблокировки IP-адреса с указанием группы правил (`[utm-vpn-authd]`).
- Список групп правил:
  - `utm-dovecot` - авторизация на почтовом сервере через почтовые клиенты;
  - `utm-postfix-connrate` - превышение лимита подключения к почтовому серверу;
  - `utm-postscreen-prgrt` - отслеживание нежелательных подключений (PREGREET) к почтовому серверу;
  - `utm-reverse-proxy-conn` - защита от DoS (лимит подключений);
  - `utm-reverse-proxy-req` - защита от DoS (лимит запросов в секунду);
  - `utm-reverse-proxy` - Web Application Firewall (WAF);
  - `utm-roundcube` - авторизация в веб-интерфейсе почтового сервера;
  - `utm-smtp` - авторизация по smtp;
  - `utm-smtp-rcpt` - защита от перебора почтовых ящиков;
  - `utm-ssh` - авторизация по ssh;
  - `utm-two-factor-codes` - прохождение двухфакторной аутентификации;
  - `utm-vpn-authd` - авторизация по VPN;
  - `utm-web-interface` - авторизация в административном веб-интерфейсе;
  - `utm-user-cabinet` - авторизация в пользовательском веб-интерфейсе.

SD-WAN

Классический контекст | Высокопроизводительный контекст | API

SD-WAN (Software-Defined Wide Area Network) - технология программно-определяемых распределенных сетей, которая управляет WAN-каналами на основе политик и обеспечивает интеллектуальную маршрутизацию трафика между филиалами, центрами обработки данных и облачными сервисами.

В разделе **SD-WAN** доступны настройки:

- **Next hop** - следующий узел маршрутизации, задающий интерфейс и шлюз, через которые будет отправляться трафик.
- **Профили next hop** - объединение нескольких next hop в одну логическую группу. В профиле задаются режим работы (резервирование или балансировка), приоритет и способ проверки доступности.
- **Профили IP SLA** - набор параметров для мониторинга качества канала: допустимые пороги задержки, джиттера и потери пакетов. Используется в **Профилях next hop** для оценки доступности канала.

Миграция при обновлении

Балансировка и резервирование

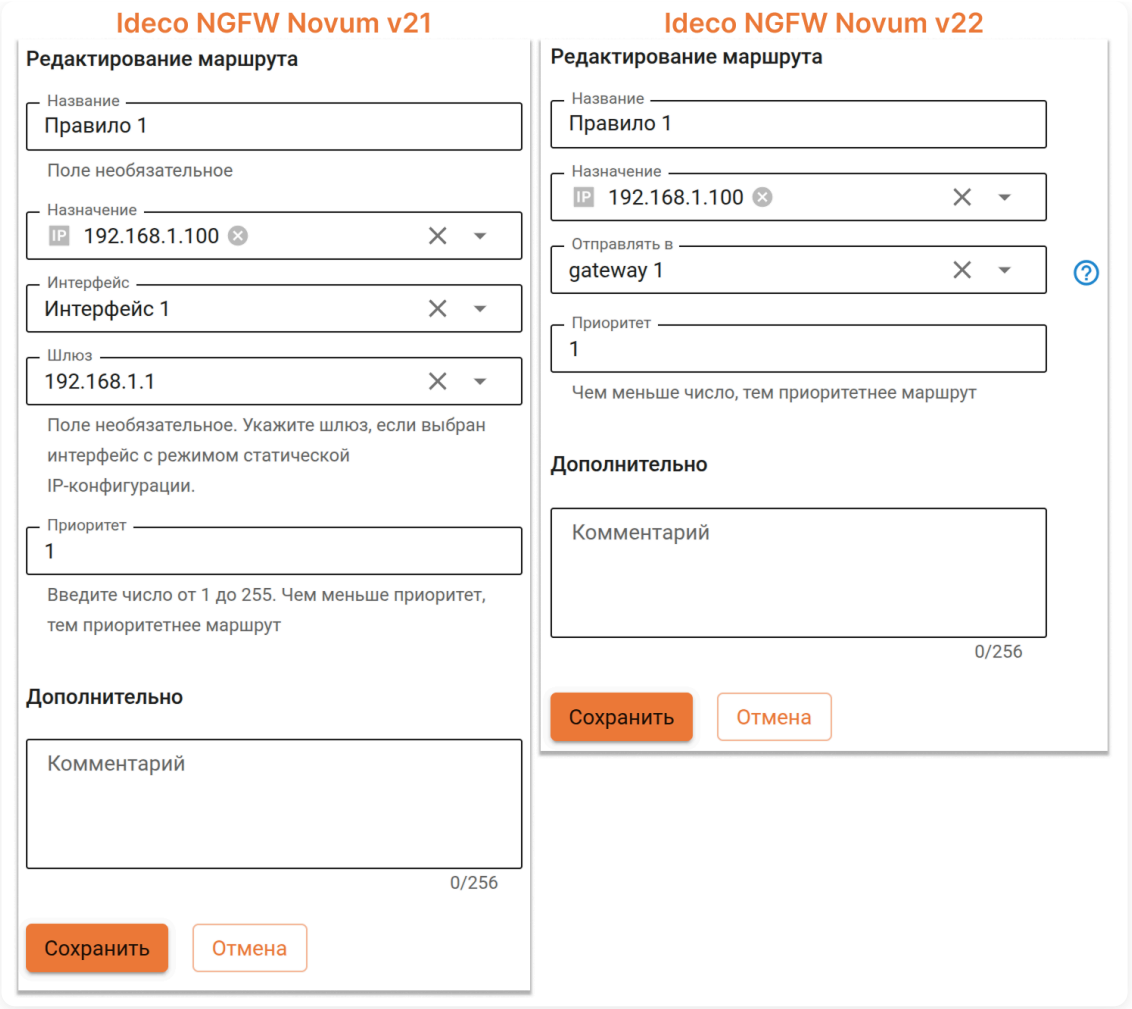
С версии 22 Ideco NGFW Novum раздел **Балансировка и резервирование** вошел в состав **SD-WAN**. При обновлении настройки будут перенесены автоматически. Миграция настроек:

- Все шлюзы, добавленные ранее на вкладке **Основное**, будут перенесены в **Next hop**.
- Выбранный ранее режим **Балансировки** или **Резервирования** будет преобразован в системный **Профиль next hop**. Помимо системного профиля, теперь можно создавать несколько пользовательских профилей.
- **Адреса для проверки связи** будут перенесены в системный **Профиль IP SLA**. Этот профиль будет выбран в системном профиле next hop при миграции.

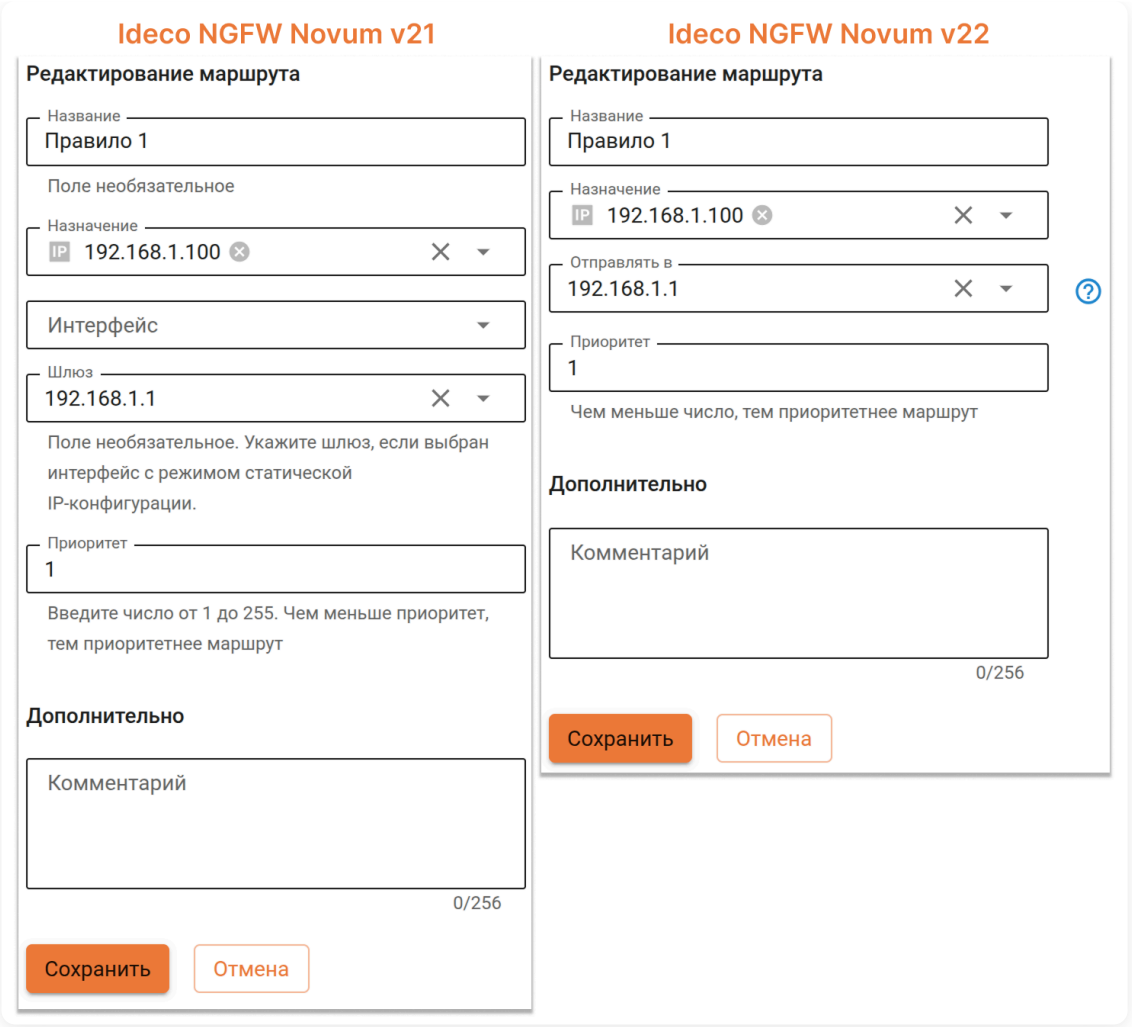
Маршрутизация (PBR, Статическая, Внешних сетей)

Логика создания **Next hop** при миграции маршрутов зависит от исходной конфигурации:

- Если в маршруте был указан **Интерфейс** - автоматически создается **Next hop**. Пример правила статической маршрутизации:



- Если в маршруте не был указан **Интерфейс** - **Next hop** не создается, маршрут сохраняется в прежнем виде. Пример правила статической маршрутизации:



Если в правиле маршрутизации **Внешних сетей** была включена опция **Использовать маршрут только при доступности шлюза (адаптивность)** - при миграции автоматически создается **Профиль next hop** с настроенной проверкой доступности шлюза. Это необходимо для корректной работы адаптивности после обновления.

С версии 22 Ideco NGFW Novum не поддерживает указание пользователя в поле **Шлюз** правил **Статической** маршрутизации. Если в правиле был указан пользователь, перед обновлением замените его на IP-адрес вручную.

IPsec

Следует учесть, что при обновлении на версию 22:

- Существующие конфигурации с несколькими адресами удаленного устройства продолжат работать после миграции. В новой версии допускается только один **Адрес удаленного устройства**.
- **Группа балансировки и резервирования**, выбранная в поле **Интерфейс подключения**, будет перенесена в **Профиль next hop**. В новой версии в поле **Интерфейс подключения** допускается только один интерфейс.

Рекомендуем после обновления указать конкретный **Интерфейс подключения** и конкретный **Адрес удаленного устройства**, так как варианты с множественным выбором или объектом **Любой** будут удалены в следующих версиях.

Next hop

Классический контекст | Высокопроизводительный контекст | API

Next hop - это следующий узел маршрутизации, на который передается сетевой трафик для дальнейшей доставки к целевой сети. В рамках **SD-WAN** next hop определяется после выбора маршрута до точки назначения и задает, через какой интерфейс и шлюз будет отправляться трафик.

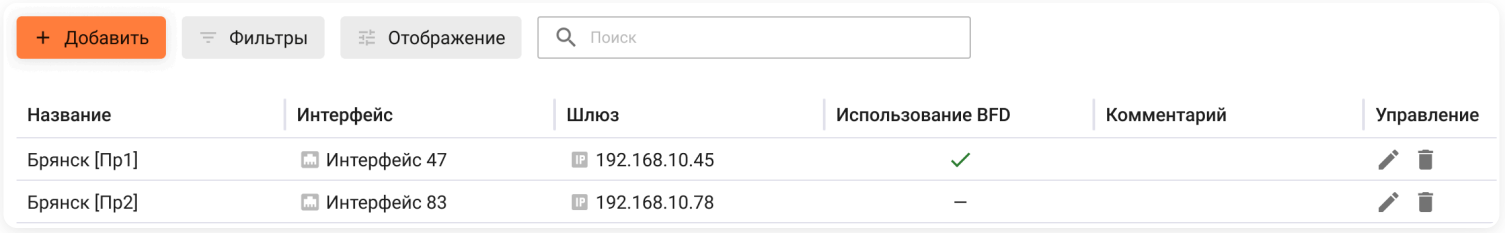
Next hop используется при настройке маршрутизации: **Статическая**, **PBR** и **Внешних сетей**.

Если нет необходимости в проверке доступности шлюза или резервировании, в поле **Отправить в** достаточно указать IP-адрес как **Объект** или **Значение**. Создайте **Next hop**, если:

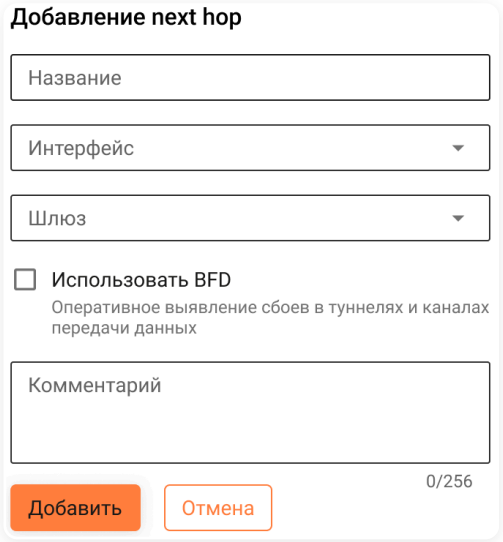
- Нужна проверка доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection).
- Планируется объединить несколько шлюзов в **Профиль next hop** для резервирования или балансировки трафика.
- При настройке **Статического** маршрута, правила **PBR** или **Внешних сетей** необходимо указать интерфейс.

Для добавления **Next hop** выполните действия:

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**:



2. Заполните поля:



- **Название** - укажите название.
- **Интерфейс** - выберите сетевой интерфейс, через который будет отправляться трафик к следующему узлу.
- **Шлюз** - укажите IP-адрес следующего узла маршрутизации (next hop), на который будет направляться трафик. Адрес шлюза должен находиться в сети выбранного интерфейса.

При выборе интерфейса, который получает IP-адрес по DHCP:

- Если оставить поле **Шлюз** пустым, то будет использован шлюз, полученный от DHCP-сервера.
- Если в поле **Шлюз** указать IP-адрес, то в качестве шлюза будет использоваться указанный IP-адрес, а полученный от DHCP-сервера проигнорируется.

- **Использовать BFD** - включите опцию для проверки доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection). Поддержка BFD должна быть включена и на стороне указанного шлюза.
- **Комментарий** - необязательное поле для описания **Next hop**.

> Интерфейс с ролью **Control Plane** используется только для настройки и администрирования NGFW Novum. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.

Добавленные **Next hop** можно редактировать, удалять и объединять в **Профили next hop**. Подробности в статье.

Мониторинг состояния Next hop

Для настройки проверки работоспособности **Next hop** выполните действия:

1. Создайте **Профиль IP SLA**, указав требования к качеству сетевого соединения и IP-адрес для проверки связи.

2. Создайте **Профиль next hop**:

- На вкладке **Настройки** выберите **Профиль IP SLA**, созданный на шаге 1.
- На вкладке **Next hop** выберите **Next hop**, для которого нужна проверка работоспособности.

> Уведомления о недоступности будут отображаться в **Отчеты и журналы** → **Система**.

Полезные ссылки

- **Статическая маршрутизация**
- **PBR**
- **Внешних сетей**
- **Профили next hop**

Профили next hop

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Профили next hop**: `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

Профили next hop - объединение нескольких шлюзов (next hop) в одну логическую группу. В профиле задаются режим работы шлюзов (резервирование или балансировка), их приоритет и способ проверки доступности.

Профили next hop используются при настройке маршрутизации: **Статическая**, **PBR** и **Внешних сетей**.

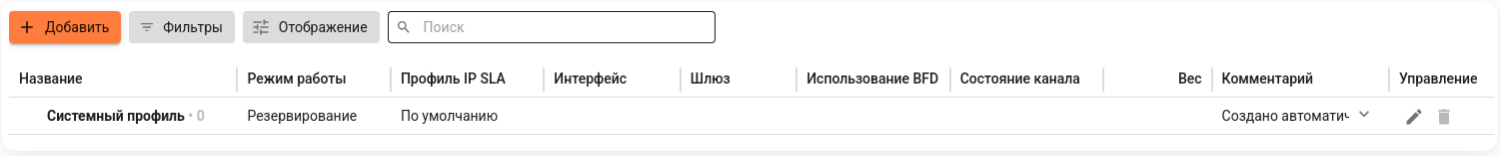
Режимы работы профилей:

- **Резервирование** - NGFW Novum использует шлюзы по приоритету. При недоступности основного шлюза трафик переходит через резервные.
- **Балансировка** - трафик распределяется между несколькими шлюзами по мере установления новых сетевых сессий, что позволяет равномерно распределять нагрузку. Режим использует механизм **ECMP** (Equal-Cost Multi-Path). Сессии одного пользователя могут проходить через разные шлюзы:
  - **Балансировка со стабильной привязкой** - сетевые сессии закрепляются за определенным шлюзом и всегда проходят через него. Рекомендуется, если на внешних интерфейсах не используется NAT.

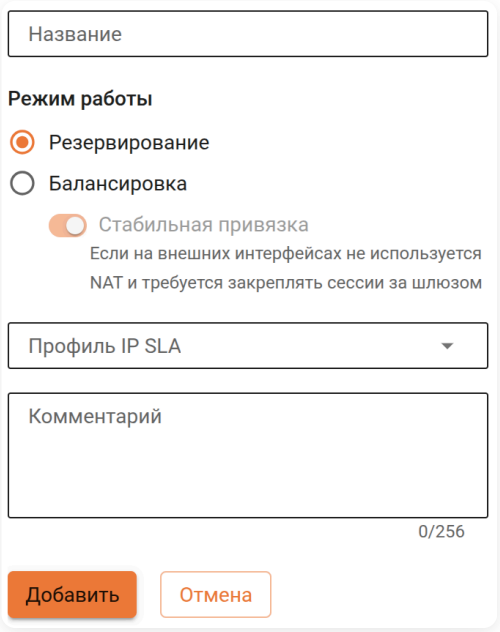
Добавление профиля

Для добавления **Профиля next hop** выполните действия:

1. Перейдите в **SD-WAN** → **Профили next hop** и нажмите **Добавить**:



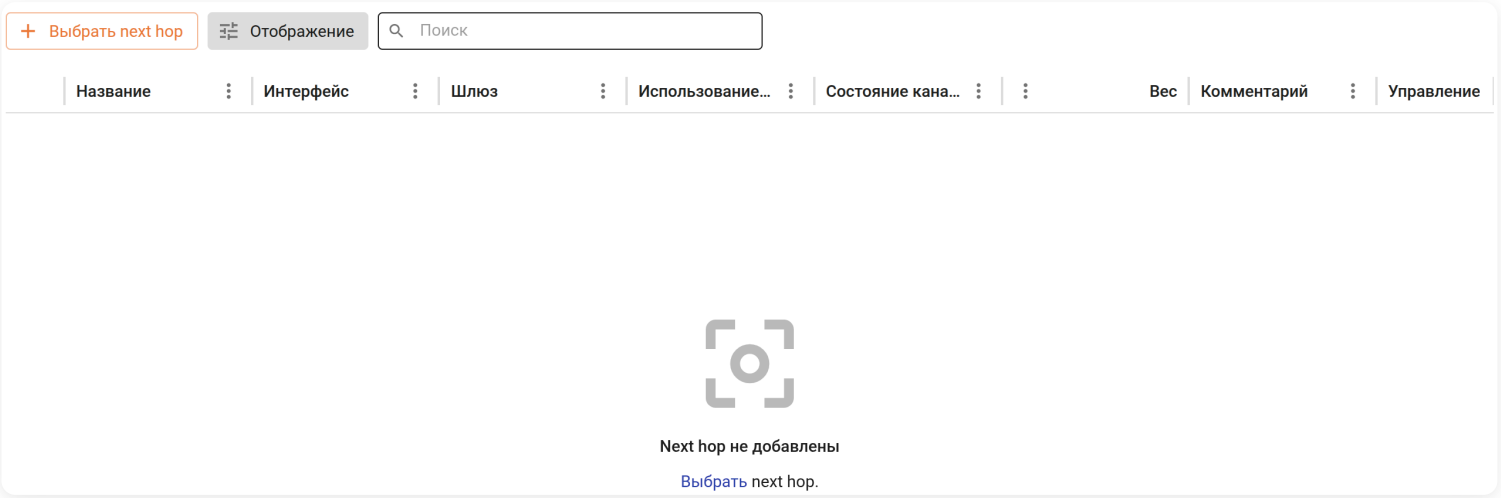
2. Заполните поля и нажмите **Добавить**:



Расшифровка полей

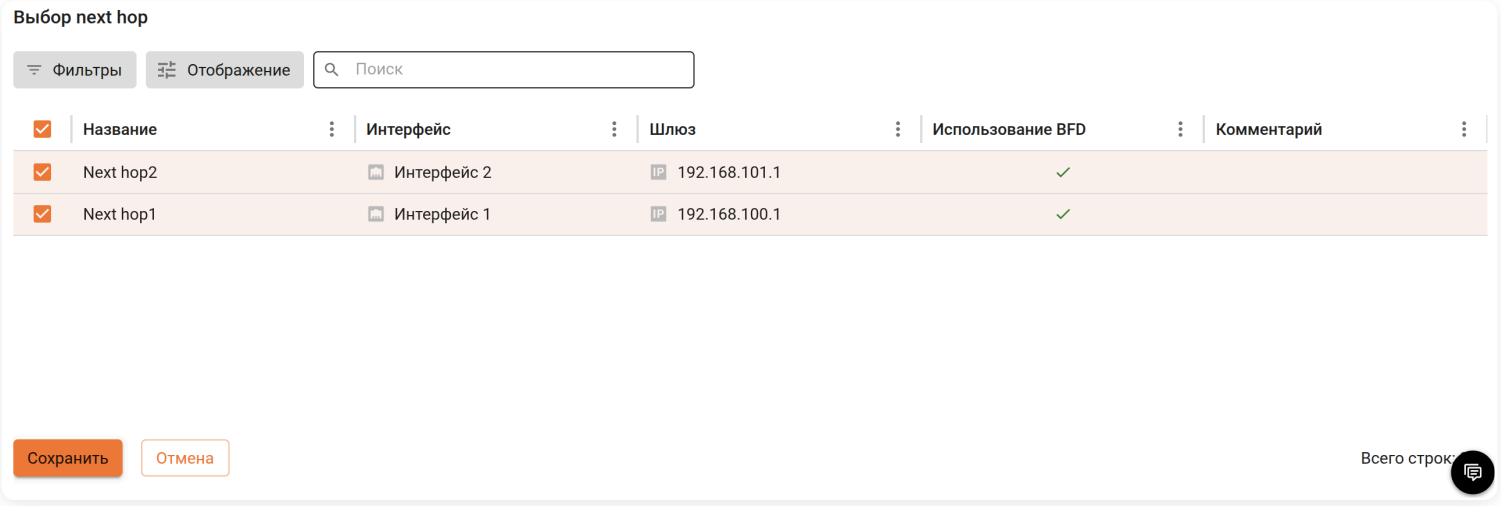
- **Название** - укажите название профиля.
- **Режим работы** - выберите способ использования шлюзов в профиле:
  - **Резервирование** - используется один основной шлюз, а остальные применяются как резервные при его недоступности.
  - **Балансировка** - трафик распределяется между несколькими шлюзами:
    - **Стабильная привязка** - включите опцию для закрепления сетевых сессий за определенным шлюзом. Рекомендуем включать, если на внешних интерфейсах не используется NAT и важно, чтобы трафик одной сессии всегда проходил через один шлюз.
- **Профиль IP SLA** - выберите профиль, который будет использоваться для проверки доступности шлюзов и качества канала.
- **Комментарий** - необязательное поле для описания профиля.

3. Перейдите на вкладку **Next hop**, нажмите **Выбрать next hop** и выполните действия в зависимости от выбранного режима работы:



Балансировка

4. Выберите нужные next hop и нажмите **Сохранить**:

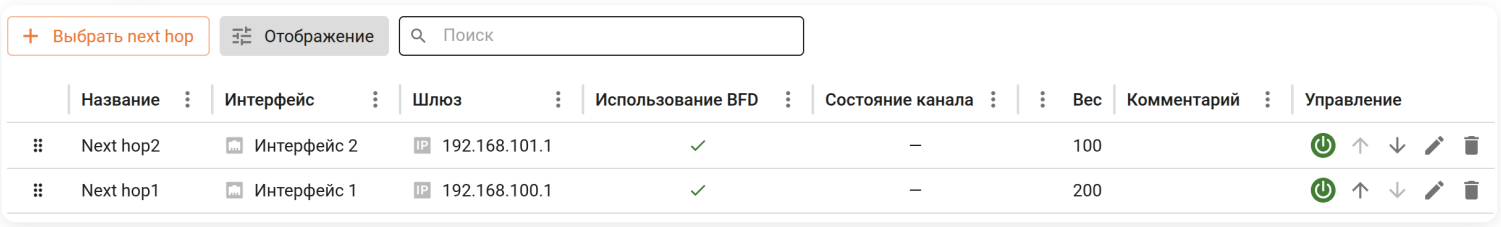


Изменение веса у next hop в профиле

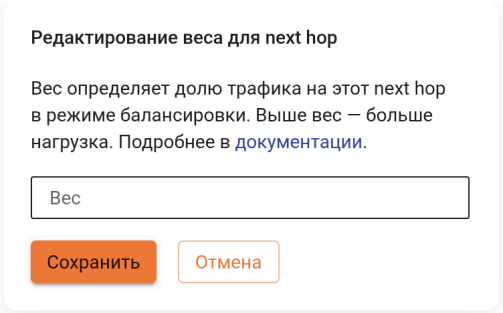
Вес - числовой коэффициент, определяющий долю трафика, направляемую на конкретный next hop при балансировке нагрузки. Чем выше вес относительно других узлов, тем больше запросов получит этот шлюз.

В поле **Вес** у выбранного next hop рекомендуем указывать пропускную способность интернет-провайдера. Балансировщик распределит трафик пропорционально весам всех активных узлов.

5. Нажмите напротив нужного next hop:



6. Введите вес и нажмите **Сохранить**:

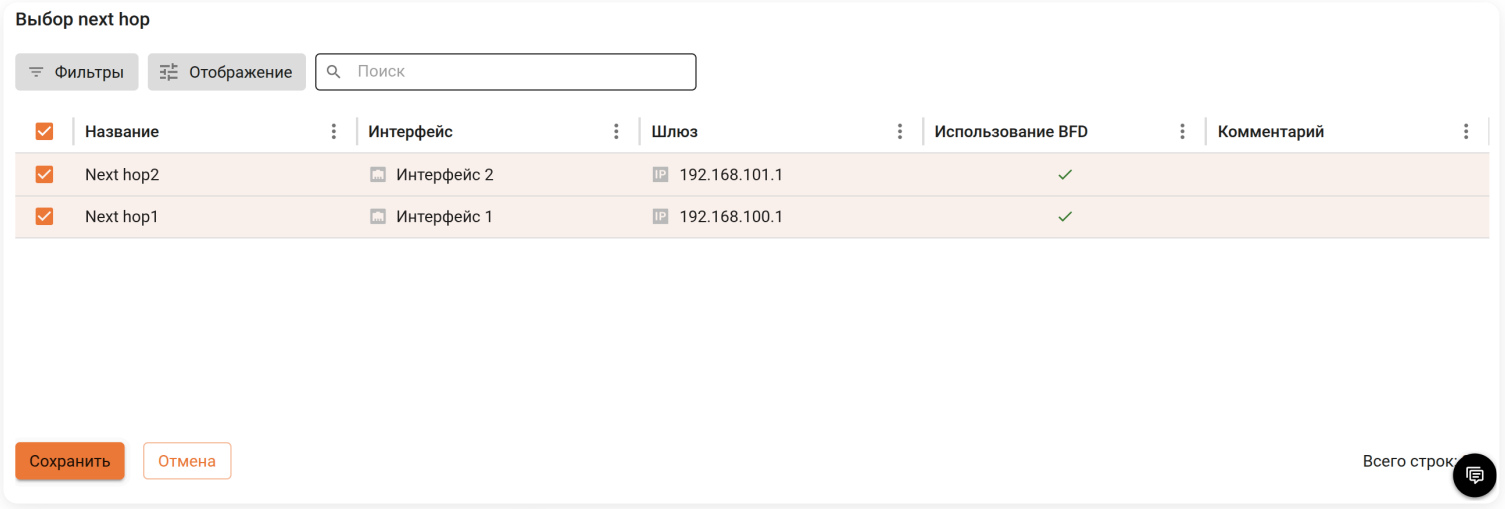


Next hop без указанного веса в балансировке не участвует.

Резервирование

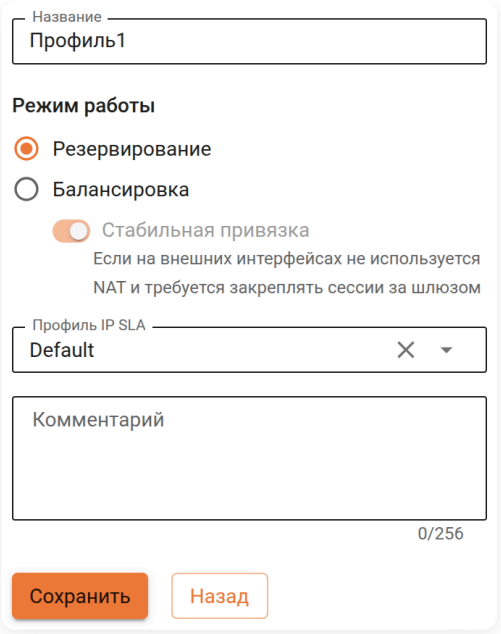
При **Резервировании** Ideco NGFW Novum использует шлюзы в соответствии с приоритетом. Приоритет задается порядком next hop в таблице, сверху вниз. Если интернет стал недоступен через используемый шлюз, то NGFW Novum будет перебирать подключения сверху вниз (до первого доступного шлюза).

4. Выберите нужные next hop и нажмите **Сохранить**:



5. Смените приоритет при необходимости, нажав ↑ ↓.

Вернитесь на вкладку **Настройки** и нажмите **Сохранить**:

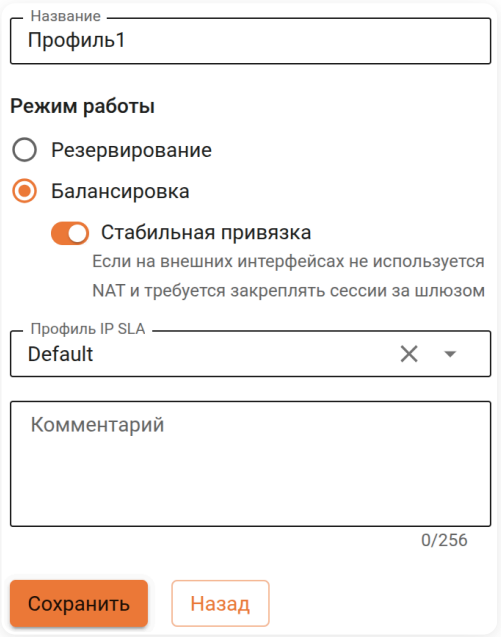


Изменение профиля

Для изменения режима профиля выполните действия:

1. Нажмите  напротив нужного профиля.

2. Выберите новый режим и нажмите **Сохранить**:



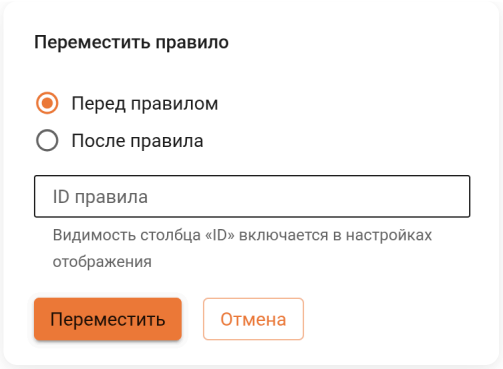
Если переключаете режим с **Резервирование** на **Балансировка**, настройте значение веса у next hop в профиле.

При изменении профиля на вкладке **Next hop** доступно перемещение добавленных next hop. Выполните действия:

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:



4. Нажмите **Переместить**.

Доступно перемещение правила мышью - удерживайте и перенесите правило в нужное место.

Полезные ссылки

- **Статическая маршрутизация**
- **PBR**
- **Внешних сетей**
- **Next hop**
- **Профили IP SLA**

Профили IP SLA

Классический контекст | Высокопроизводительный контекст | API

Профили IP SLA - набор параметров, определяющих требования к качеству сетевого соединения и правила мониторинга доступности канала. Профиль используется при создании **Профилей next hop** для оценки состояния канала и принятия решений о его доступности на основе измеряемых сетевых показателей.

В рамках **Профиля IP SLA** настраиваются параметры качества обслуживания:

- **Задержка** - максимально допустимое время передачи данных по сети.
- **Джиттер** - максимально допустимое колебание времени задержки пакетов, характеризующее стабильность соединения.
- **Потеря пакетов** - максимально допустимый процент потерянных пакетов в канале связи.

Если в одном из параметров значение превышает заданный порог, соединение не соответствует требованиям SLA.

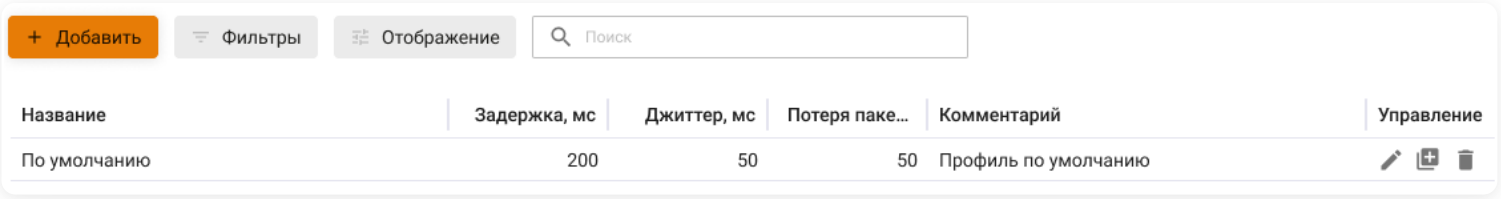
Для определения доступности канала в профиле используется протокол ICMP. Система отправляет ICMP-запросы на указанные IP-адреса. По результатам ответов оцениваются:

- Наличие или отсутствие соединения.
- Количество последовательных неудачных проверок.
- Количество последовательных успешных проверок.
- Минимальное время стабильной работы канала, необходимое для признания его активным.

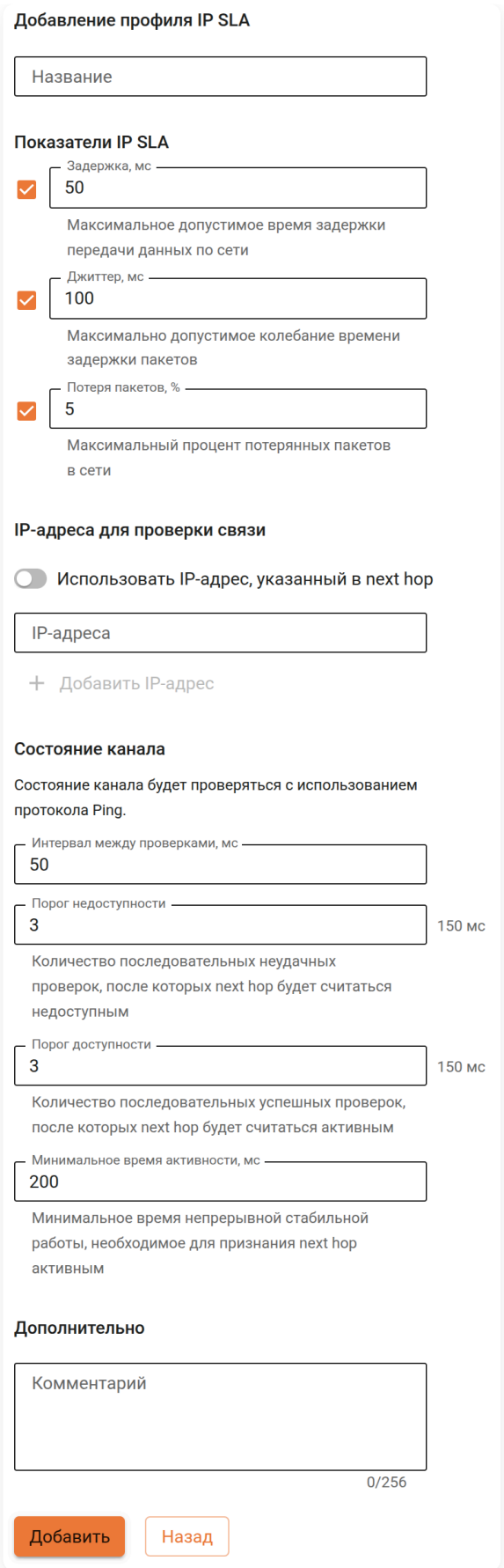
Если число неуспешных проверок превышает заданный порог, канал помечается как недоступный. Канал считается восстановленным после достижения порога успешных проверок и выдержки минимального времени активности.

Для добавления профиля выполните действия:

1. Перейдите в **SD-WAN** → **Профили IP SLA** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - укажите название профиля.
- **Показатели SLA** - включите опции:
  - **Задержка, мс** - задайте максимально допустимое время задержки передачи данных по сети.
  - **Джиттер, мс** - укажите максимально допустимое колебание времени задержки пакетов.

    - **Потеря пакетов, %** - укажите максимально допустимый процент потерянных пакетов в сети.
- **IP-адреса для проверки связи**:
    - **Использовать IP-адрес, указанный в next hop** - включите опцию для проверки доступности следующего узла (next hop), указанного в маршруте.
    - **IP-адрес** - укажите IP-адрес узла, до которого выполняется проверка доступности канала. Можно указать несколько адресов для проверки.
- **Состояние канала**:
    - **Интервал между проверками, мс** - определите периодичность выполнения проверок доступности канала.
    - **Порог недоступности** - укажите количество последовательных неудачных проверок, после которых next hop считается недоступным.
    - **Порог доступности** - укажите количество последовательных успешных проверок, после которых next hop считается активным (но не раньше, чем **Минимальное время активности, мс**).
    - **Минимальное время активности, мс** - укажите минимальное время непрерывной стабильной работы канала, необходимое для признания next hop активным.
- **Дополнительно**:
    - **Комментарий** - необязательное поле для описания профиля.

Маршрутизация

Классический контекст | Высокопроизводительный контекст

Маршрутизация - механизм определения пути сетевого пакета от источника к назначению. Модуль позволяет:

- Обеспечить сетевую связность между подсетями, филиалами и внешними сетями.
- Управлять направлением трафика в зависимости от адресов источника, назначения и других условий.
- Организовать отказоустойчивость и балансировку нагрузки между несколькими каналами связи.
- Обеспечить корректную доставку как исходящего, так и ответного трафика.

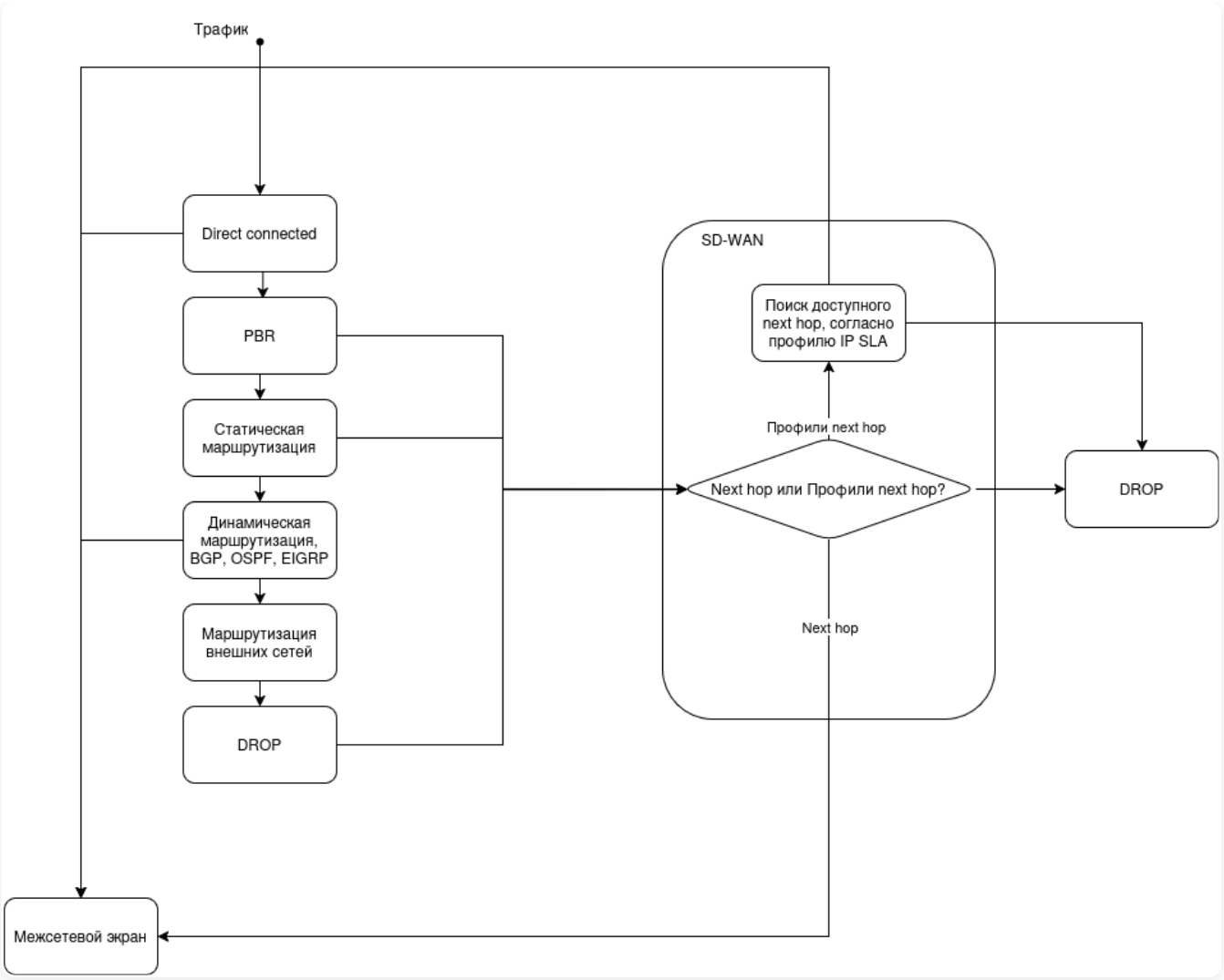
В разделе доступны настройки:

- **PBR** - маршрутизация на основе политик, которые устанавливаются администратором.
- **Статическая** - маршрутизация на основе заданных вручную маршрутов с фиксированными шлюзами и интерфейсами.
- **BGP** - динамическая маршрутизация на основе протокола прикладного уровня, обеспечивающая обмен маршрутами между сетями и автономными системами.
- **OSPF** - динамическая маршрутизация на основе протокола состояния каналов, определяющая оптимальные пути передачи данных внутри сети.
- **EIGRP** - динамическая маршрутизация на основе гибридного протокола. Он сочетает особенности дистанционно-векторного подхода и протоколов состояния каналов, что обеспечивает быструю сходимость и актуальность таблиц маршрутизации.
- **Внешних сетей** - маршрутизация, позволяющая направлять трафик от разных пользователей или групп пользователей по заданным маршрутам.

Обработка трафика

Трафик последовательно проходит этапы поиска маршрута. Путь пакета после его определения зависит от того, в какой таблице найден маршрут:

- Для маршрутов из таблиц **PBR**, **Статической** маршрутизации и маршрутизации **Внешних сетей** требуется дополнительный выбор next hop через **SD-WAN**.
- Маршруты из Direct connected и динамической маршрутизации направляются напрямую в **Межсетевой экран**:



После определения маршрута результат маршрутизации сохраняется. Путь пакета фиксируется, но может измениться при недоступности ранее выбранного next hop.

Этап 1. Поиск маршрута

Трафик проверяется на пяти уровнях в строгой последовательности. В зависимости от действия происходит переход:

Уровень	**Если маршрут найден**	**Если не найден**
Direct connected	Межсетевой экран	PBR
PBR	SD-WAN	Статическая маршрутизация
Статическая маршрутизация	SD-WAN	Динамическая маршрутизация
Динамическая маршрутизация (BGP, OSPF, EIGRP)	Межсетевой экран	Маршрутизация внешних сетей
Маршрутизация внешних сетей	SD-WAN	DROP

Этап 2. Выбор next hop

Когда маршрут найден в таблицах **PBR**, **Статической маршрутизации** или **Маршрутизации внешних сетей**, пакет направляется в **SD-WAN** для выбора next hop:

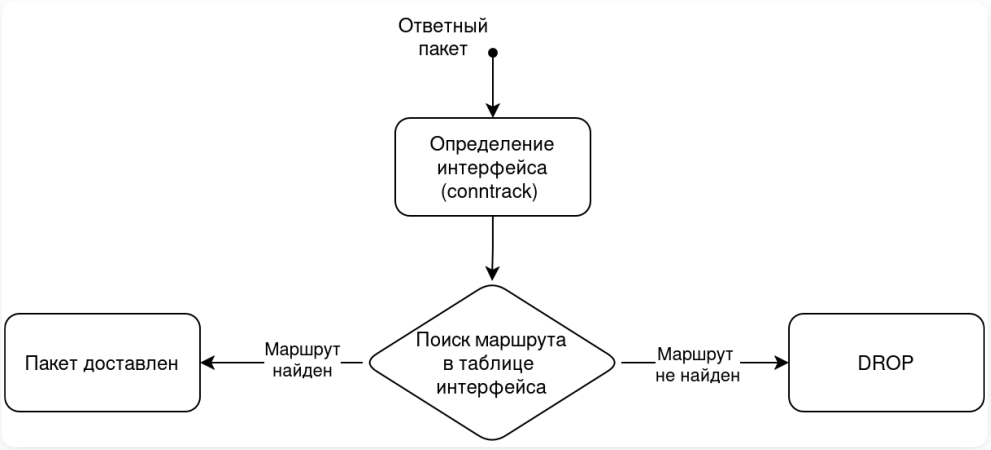
- Если используется конкретный **Next hop**, то проверяется его доступность:
  - Если доступен - пакет направляется в **Межсетевой экран**.
  - Если недоступен - пакет отбрасывается.
- Если используются **Профили next hop**:
  - Пакет направляется на этап **Поиск доступного next hop, согласно профилю IP SLA**. Выбранный next hop фиксируется и пакет направляется в **Межсетевой экран**.
  - Если в **Профиле next hop** следующие узлы недоступны - пакет отбрасывается.

Маршруты в таблицах **PBR** и **Внешних сетей** имеют приоритет сверху вниз, то есть **верхний маршрут приоритетнее нижнего**.

Для трафика не будут применяться нижестоящие правила, если хотя бы одно условие совпадает с вышестоящим правилом.

Обработка ответного трафика

Для пакетов, относящихся к уже установленному соединению, NGFW использует механизм Connection tracking (conntrack): ответный пакет отправляется через тот же интерфейс, с которого поступил исходный запрос, если для этого интерфейса существует подходящий маршрут:



Если маршрут в сторону интерфейса-источника отсутствует, ответный пакет не будет отправлен. Рекомендуем добавить явный маршрут (например, статический) в сеть источника через соответствующий интерфейс.

Полезные ссылки

- **Как избавиться от асимметричной маршрутизации трафика**

PBR

Классический контекст | Высокопроизводительный контекст | API

PBR (Policy-based Routing) - маршрутизация на основе политик, которые устанавливаются администратором. Позволяет направлять трафик по различным условиям, например, от конкретных пользователей или по протоколу. Применяется первой до всех остальных видов маршрутизации.

Способы применения:

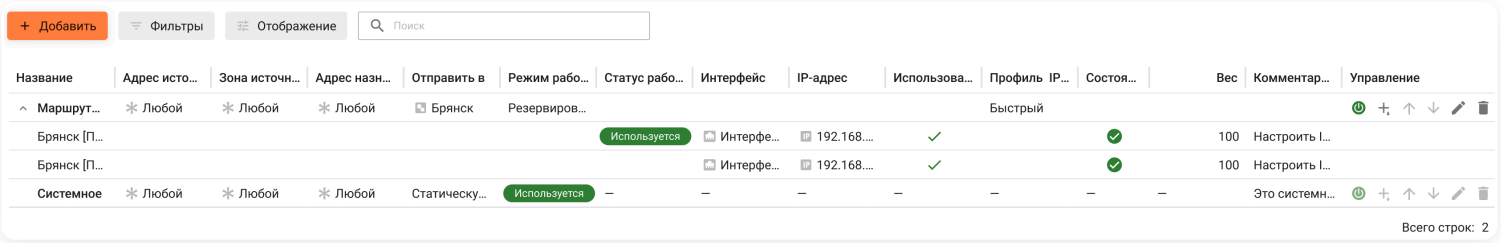
- Направление части трафика через интернет-провайдера с наименьшей стоимостью этого трафика.
- Предоставление доступа в интернет через одного из провайдеров для определенных пользователей/групп пользователей.

> Маршруты в таблице имеют приоритет сверху вниз, то есть **верхний маршрут приоритетнее нижнего**.

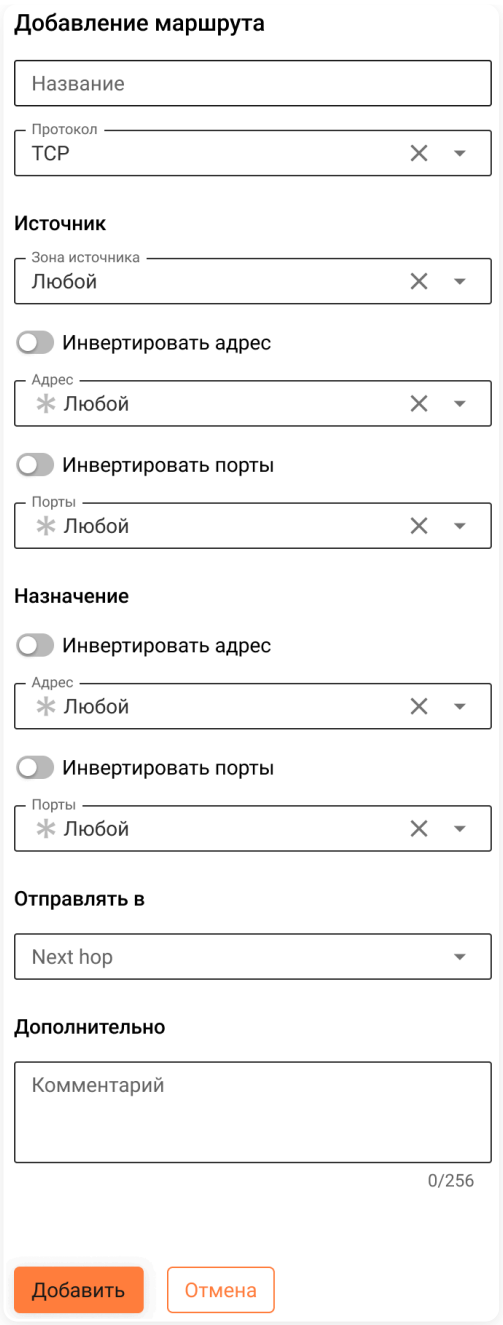
Перед обновлением на Ideco NGFW Novum версии 22 ознакомьтесь с информацией по ссылке.

Действия для настройки:

1. Перейдите в **Маршрутизация** → **PBR** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - введите название маршрута.
- **Протокол** - выберите протокол передачи данных: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP).
- **Источник**:
  - **Зона*** - выберите интерфейс или группу интерфейсов Ideco NGFW Novum, на которые приходит трафик от источника. Объект типа **Зона** можно создавать и редактировать только в **Системном контексте**.
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - выберите объект, трафик от которого нужно маршрутизировать. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
  - **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.
  - **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

Не рекомендуем указывать порт источника, так как он обычно выбирается случайным образом. Исключение - протоколы с фиксированными портами источника и назначения (например, DNS).

- **Назначение**:
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.

- **Адрес** - выберите объекты, при обращении к которым будет применяться этот маршрут. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
- **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.
- **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

- **Отправлять в** - выберите вариант, через который будет направляться трафик. В поле могут быть выбраны: Next hop, Профили next hop, IP-адреса или Статическая маршрутизация. IP-адрес можно указать как **Объект** или **Значение**. При выборе Статической маршрутизации NGFW Novum трафик перенаправляется в таблицу **Статической маршрутизации**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

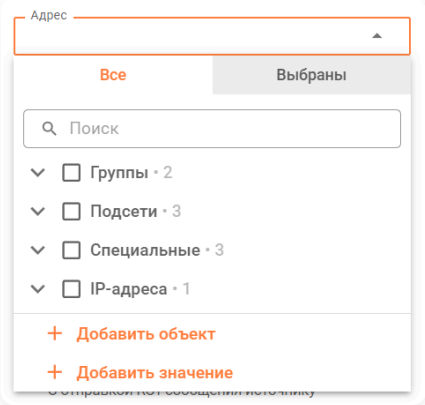
Отличие значений от объектов:

- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

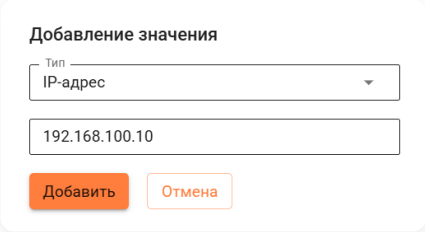
Управление значениями

Добавление

1. В поле нажмите **Добавить значение**:



2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:

Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:

2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

- **Дополнительно**:
  - **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

В столбце **Управление** можно:

 Включать или выключать правило.

 Менять приоритет.

 Редактировать правило.

 Удалять правило.

Полезные ссылки

- **Объекты**
- **Статическая маршрутизация**
- **Next hop**
- **Профили next hop**

Статическая маршрутизация

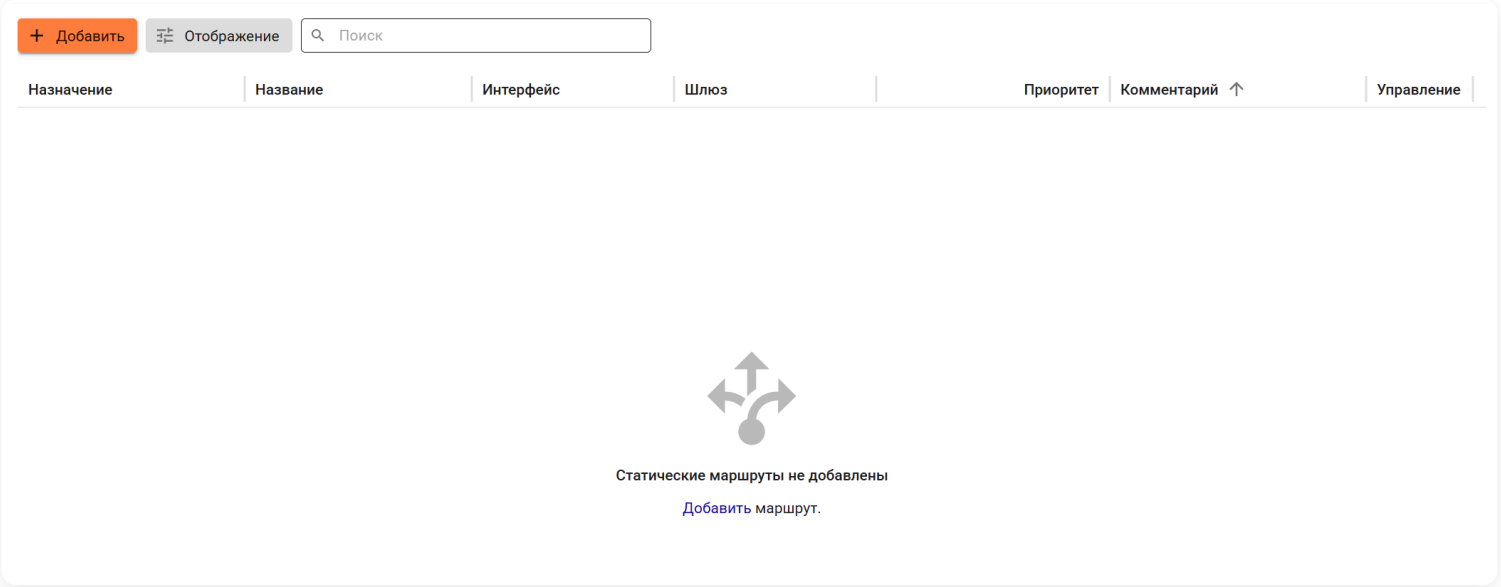
Классический контекст | Высокопроизводительный контекст | API

Статическая маршрутизация применяется в сценариях, где нет необходимости в сложной логике маршрутизации. Обработка статических маршрутов происходит после PBR, но до динамической маршрутизации и маршрутизации внешних сетей.

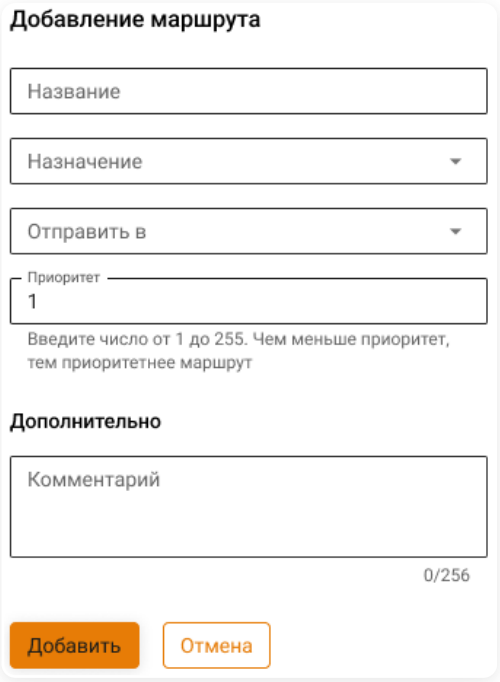
Перед обновлением на Ideco NGFW Novum версии 22 ознакомьтесь с информацией по ссылке.

Для добавления статического маршрута выполните действия:

1. Перейдите в раздел **Маршрутизация** → **Статическая** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - укажите название правила.

- **Назначение** - выберите объекты, при обращении к которым будет применяться это правило. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
- **Отправить в** - выберите IP-адрес, Next hop или профиль Next hop, через который будет отправлен трафик. IP-адрес можно указать как **Объект** или **Значение**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

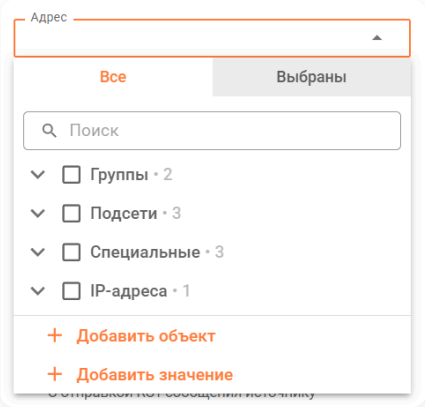
Отличие значений от объектов:

- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

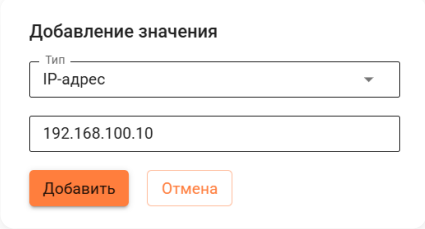
Управление значениями

Добавление

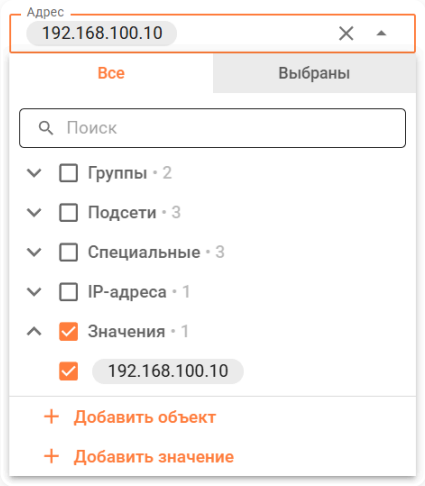
1. В поле нажмите **Добавить значение**:



2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:

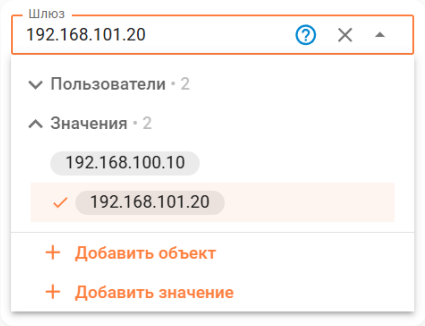


Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:



2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

Интерфейс с ролью **Control Plane** используется только для настройки и администрирования NGFW Novum. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям NGFW Novum.

- **Приоритет** - укажите приоритет маршрута. Чем меньше число, тем выше приоритет. При значении 255 трафик по этому маршруту будет заблокирован.
- **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

С версии 22 Ideco NGFW Novum не поддерживает указание пользователя в поле **Шлюз**. Если в правиле был указан пользователь, перед обновлением замените его на IP-адрес вручную.

Особенности

- **Порядок обработки маршрутов:**
  Статические маршруты обрабатываются после PBR, но до динамической маршрутизации (BGP, OSPF и EIGRP). Если в статической маршрутизации задан шлюз по умолчанию, трафик будет отправлен через него и не дойдет до динамической маршрутизации и правил маршрутизации внешних сетей.
- **Резервные маршруты через приоритет:**
  Если установить приоритет статического маршрута в диапазоне от 200 до 254, он станет менее приоритетным, чем маршруты, полученные через протоколы динамической маршрутизации. Это позволяет использовать статические маршруты как резервные:
  - Если динамическая маршрутизация предоставляет путь к сети, будет использован динамический маршрут.
  - Если динамический маршрут отсутствует, трафик пойдет по статическому маршруту.
- **Балансировка нагрузки (ECMP):**
  Если создать два маршрута к одному назначению с одинаковым приоритетом, трафик будет распределен между ними по принципу ECMP (Equal-Cost Multi-Path).
- **Блокировка трафика:**
  При значении приоритета 255 трафик по маршруту блокируется.

Полезные ссылки

- **Доступ из внешних сетей без NAT**
- **Как избавиться от асимметричной маршрутизации трафика**

BGP

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **BGP**: `frr`; `ideco-routing-backend`, `ideco-routing-rest`.

Список служб для других разделов доступен по ссылке.

Border Gateway Protocol (BGP) - это основной динамический протокол прикладного уровня, используемый для маршрутизации пакетов между автономными системами (сеть или группа сетей, работающих по единой политике маршрутизации).

Для запуска модуля необходимо предварительно настроить BGP:

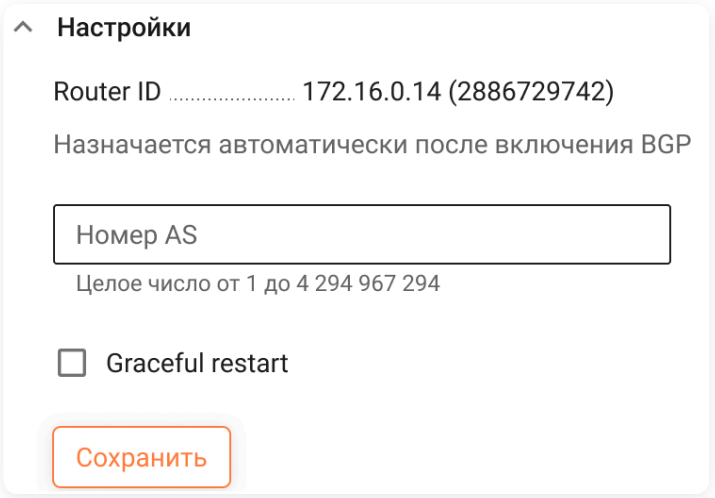
- Указать номер автономной системы.
- Создать и включить как минимум одного BGP-соседа.

На Ideco NGFW Novum по умолчанию включен **BGP Multipath** - механизм, позволяющий устанавливать несколько путей BGP к одному месту назначения в таблице IP-маршрутизации. **BGP Multipath** не влияет на процесс выбора лучшего пути.

Ideco NGFW Novum автоматически заполняет поле **Router ID** значением наибольшего IP-адреса локальной сети, указанного в разделе **Сетевые интерфейсы**. При необходимости измените IP-адрес в разделе **Сетевые интерфейсы**.

Настройка автономной системы

1. Перейдите в **Маршрутизация** → **BGP** и введите номер автономной системы в поле **Номер AS** в блоке **Настройки**:



2. Нажмите **Сохранить** и включите модуль **BGP**.

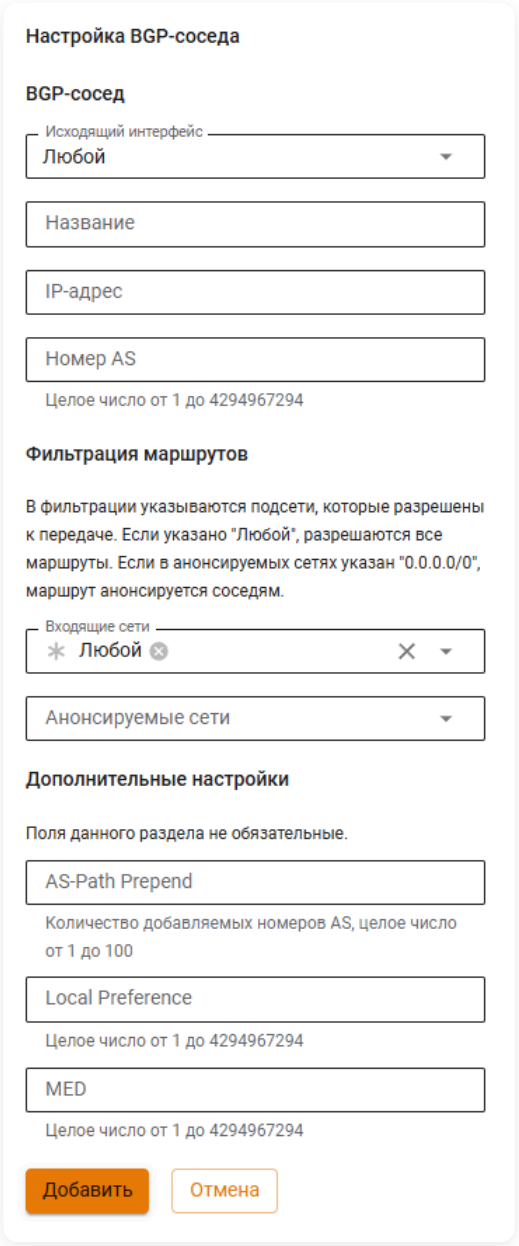
Graceful Restart - механизм обеспечения непрерывности маршрутизации, позволяющий сетевому устройству временно перезапустить управляющую плоскость (например, при обновлении ПО или восстановлении после сбоя) без немедленного перерасчета маршрутов у соседних устройств.

При включении **Graceful Restart** соседние маршрутизаторы не рассматривают кратковременный разрыв управления как отказ и продолжают использовать ранее полученные маршруты в течение ограниченного периода ожидания (120 секунд). Это позволяет избежать частых изменений состояния маршрутов и снижает влияние плановых или аварийных перезапусков на работу сети.

Graceful Restart работает только при поддержке со стороны соседних маршрутизаторов.

Настройка BGP-соседей

Для добавления BGP-соседа нажмите **Добавить** и заполните поля:

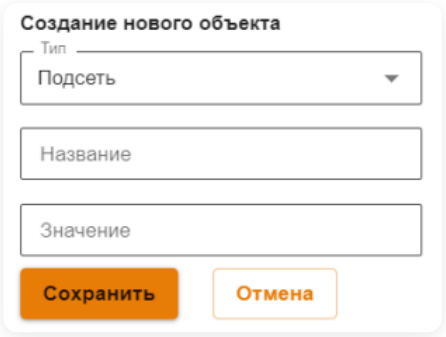


Расшифровка полей

- **Исходящий интерфейс** - интерфейс Ideco NGFW Novum, IP-адрес которого будет использован для обмена маршрутами. Для надежности и стабильности работы службы рекомендуем выбрать Loopback-интерфейс. Если выбран **Любой**, будет использоваться ближайший к соседу интерфейс. Для динамической маршрутизации поверх VPN-туннеля можно выбрать туннельный интерфейс **IPsec** или **IPsec GRE**.
- **Название** - любое значение.
- **IP-адрес** - IP-адрес BGP-соседа. Рекомендуем указать адрес Loopback-интерфейса соседа.
- **Номер AS** - номер автономной системы BGP-соседа.
- **Входящие сети** - сети, информацию от которых хотите получать. Если нужного объекта для фильтрации нет, то нажмите **Создать новый объект**. Если выбран объект **Любой**, то фильтрация будет отключена и будут приниматься все сети от BGP-соседа. Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру **0.0.0.0/0**.
- **Анонсируемые сети** - сети, информацию о которых хотите отправлять. Если нужного объекта для фильтрации нет, то нажмите **Создать новый объект**. Если выбран объект **Любой**, то фильтрация будет отключена и будет передаваться информация обо всех маршрутах, известных NGFW Novum (redistribute static, connected, ospf). Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру **0.0.0.0/0**.
- **AS-Path Prepend** - чем больше значение, тем менее приоритетным становится канал.
- **Local Preference** - определяет приоритет пути для выхода трафика. Чем больше значение, тем более приоритетным становится канал.
- **MED** - определяет приоритет пути для входа трафика. Чем меньше значение, тем приоритетнее путь.

Создание нового объекта

В поле **Входящие сети** или **Анонсируемые сети** нажмите **Создать новый объект** и заполните поля:



- **Тип** - значение **Подсеть**.
- **Название** - любое значение.
- **Значение** - значение подсети в формате: `подсеть/маска подсети`, например, `192.168.100.0/24`.

После настройки можно проверить состояние BGP-сессий с помощью утилиты `vtysh`. Примеры использования утилиты смотрите в статье.

Для динамической маршрутизации сетей двух NGFW Novum, соединенных по IPsec в туннельном режиме, воспользуйтесь BGP. Подробнее про настройку подключения двух NGFW Novum по IPsec - в статье.

Для **Входящих сетей** и **Анонсируемых сетей** объект **Любой** не может быть установлен одновременно с другими фильтрами.

OSPF

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **OSPF**: `frr`; `ideco-routing-backend`, `ideco-routing-rest`.

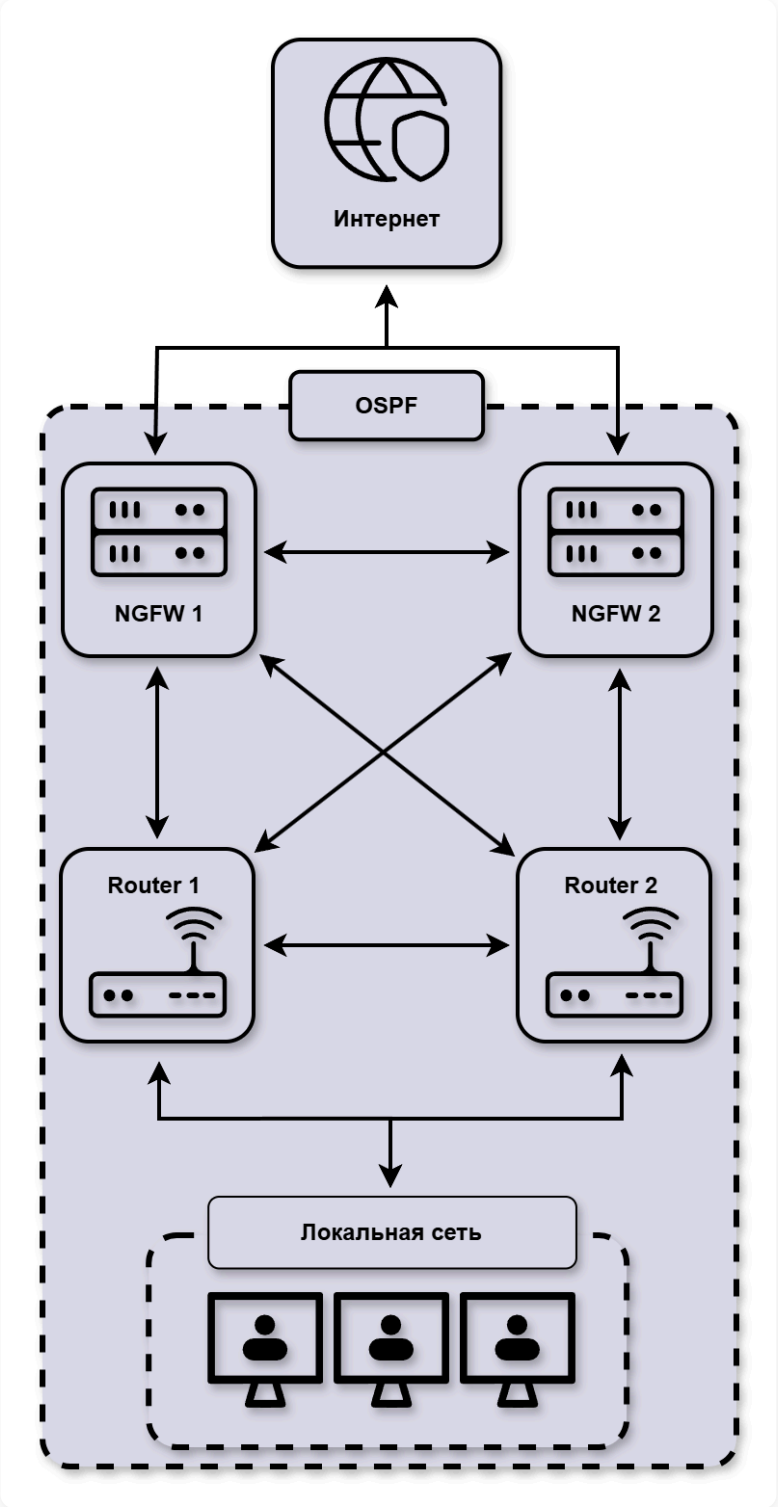
Список служб для других разделов доступен по ссылке.

Ideco NGFW Novum поддерживает OSPFv2 (Open Shortest Path First) - протокол динамической маршрутизации, который определяет оптимальные пути передачи данных на основе состояния каналов (интерфейсов маршрутизаторов или сетевых сегментов).

Рекомендуем использовать модуль в сетях, где применяется балансировка нагрузки на сеть и резервирование каналов.

При одинаковой стоимости нескольких путей до одного назначения используется ECMP (Equal-Cost Multi-Path) для балансировки нагрузки.

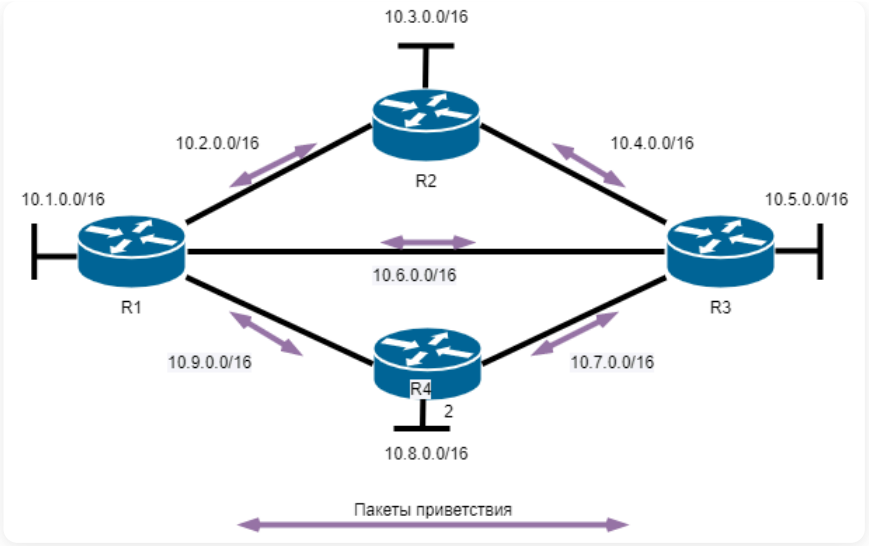
Пример топологии с использованием OSPF представлен на схеме



Принцип работы маршрутизации по состоянию канала

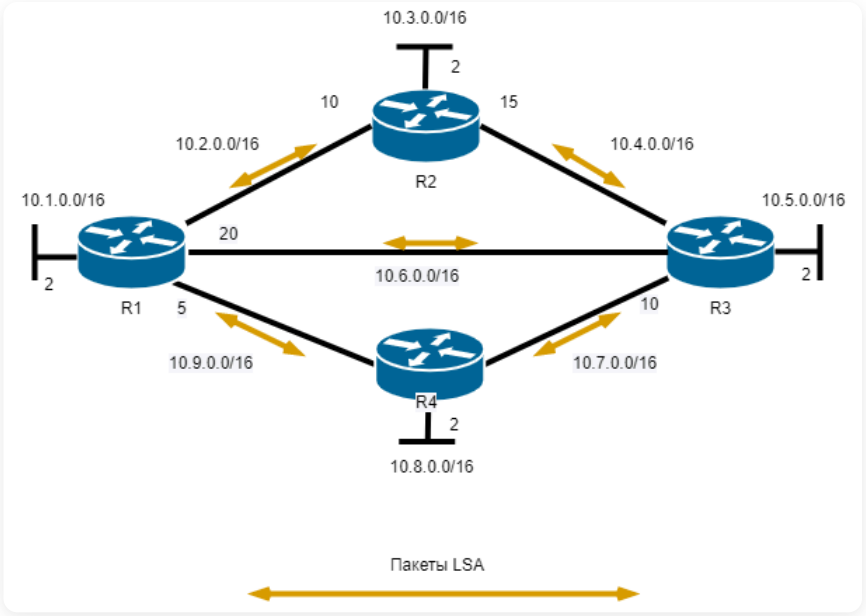
1. Установление отношений смежности с соседними устройствами

Маршрутизатор, использующий OSPF, отправляет hello-пакеты на мультикастовый адрес 224.0.0.5 со всех интерфейсов, где запущен OSPF. При наличии соседнего устройства маршрутизатор пытается установить с ним отношения смежности.



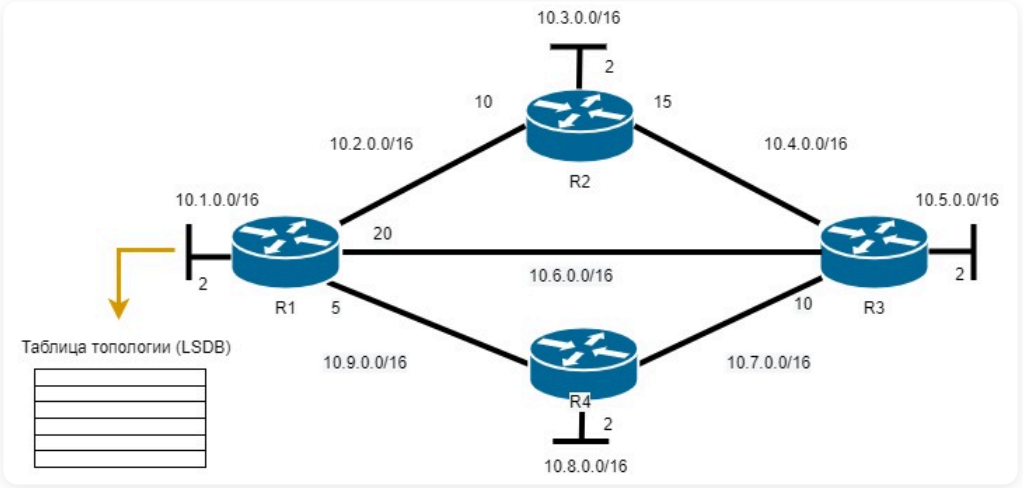
2. Обмен объявлениями о состоянии каналов

После установления смежности устройства выполняют обмен LSA. Пакеты LSA содержат информацию о состоянии и стоимости каждого канала с прямым подключением.



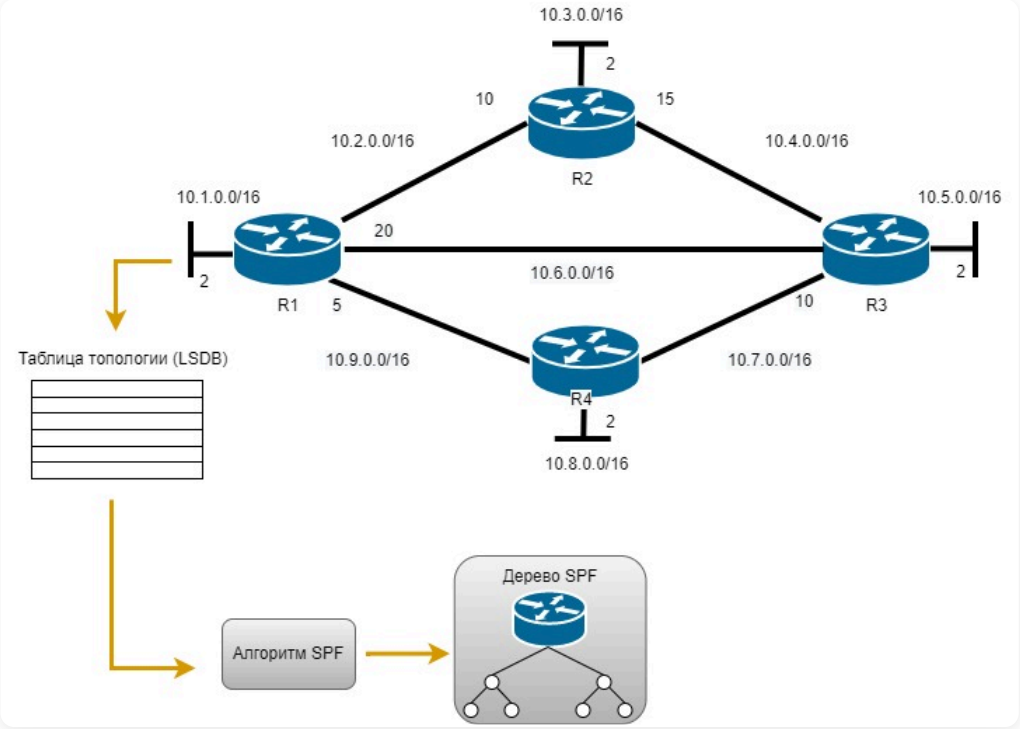
3. Создание базы данных состояния связи

На основе объявления LSA маршрутизаторы собирают базу данных, в которой содержатся данные о топологии сети в области.



4. Исполнение алгоритма SPF

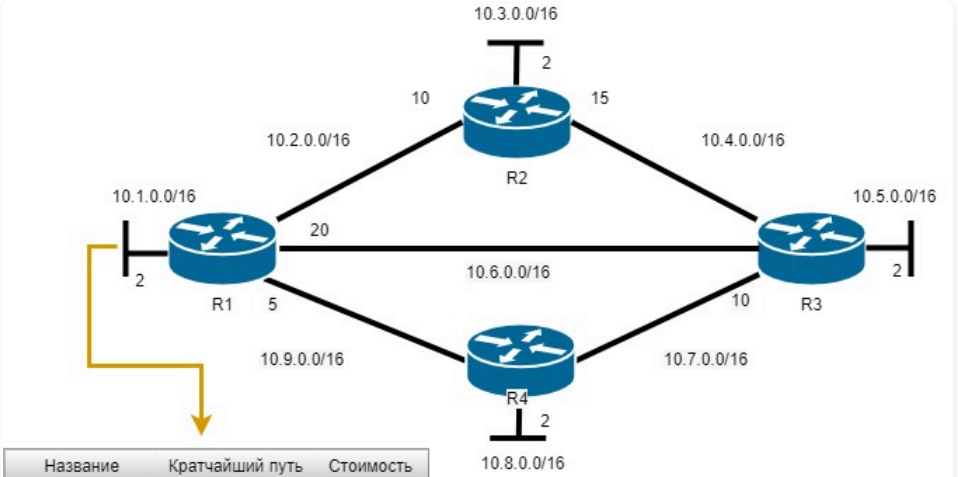
На устройствах выполняется алгоритм SPF, результатом которого является создание дерева кратчайших путей.



5. Выбор лучшего маршрута

На основании данных дерева SPF обновляются данные в таблице IP-маршрутизации.
Маршрут добавляется в таблицу маршрутизации, если отсутствует источник маршрута к той же сети с меньшим административным расстоянием, например, статический маршрут.

Решения по маршрутизации пакетов принимаются на основе записей в таблице маршрутизации.



Название	Кратчайший путь	Стоимость
10.3.0.0/16	R1 -> R2	12
10.4.0.0/16	R1 -> R2	25
10.5.0.0/16	R1 -> R3	22
10.7.0.0/16	R1 -> R4	17
10.8.0.0/16	R1 -> R4	7

Для настройки OSPF в Ideco NGFW Novum перейдите в **Маршрутизация** → **OSPF** и выполните действия на вкладках:

Основные

Ideco NGFW Novum автоматически заполняет поле **Router ID** значением наибольшего IP-адреса локальной сети, указанного в разделе **Сетевые интерфейсы**. При необходимости измените IP-адрес в разделе **Сетевые интерфейсы**.

Аутентификация соседей применяется для всех настроенных OSPF-интерфейсов. Важна для защиты маршрутной информации от несанкционированного вмешательства:

- Предотвращение подмены соседей (Spoofing) - злоумышленник не сможет подключиться к OSPF-домену, представившись легальным маршрутизатором, и передавать фальшивые LSA (Link-State Advertisements).
- Перехват и изменение OSPF-пакетов (например, подмена метрик или топологии).

Если пакет изменен, то хеш не будет совпадать и пакет будет отброшен. Хеш вычисляется на основе:

- Содержимого пакета (заголовок и данные).
- Секретного ключа, известного только доверенным маршрутизаторам.

Принцип работы MD5-аутентификации

На всех маршрутизаторах в одной зоне OSPF задается:

- Идентификатор ключа (Key ID).
- Секретный ключ (пароль).

При отправке OSPF-пакета маршрутизатор добавляет к нему:

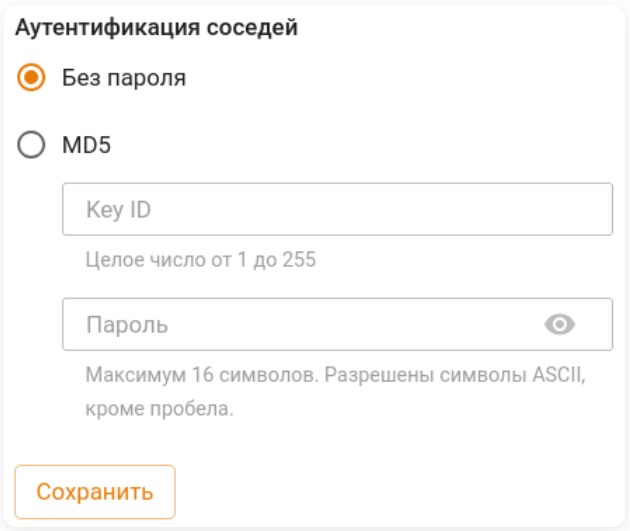
- Key ID.
- MD5-хеш, вычисленный по формуле: `MD5(OSPF_пакет + Секретный_ключ + Key_ID)`.

Принимающая сторона (получатель):
1. Берет Key ID из пакета.
2. Находит у себя секретный ключ, соответствующий переданному Key ID.
3. Вычисляет MD5-хеш по той же формуле и сравнивает с полученным:

- Если хеши совпали, пакет принимается.
- Если хеши не совпали, пакет отбрасывается с ошибкой.

> Все маршрутизаторы в зоне OSPF должны использовать MD5-аутентификацию, а также одинаковые Key ID и секретный ключ.

Настройка аутентификации



- **Без пароля** - вариант, если не нужно использовать аутентификацию. Выбран по умолчанию после миграции с Ideco NGFW Novum 19 версии.
- **MD5**:
  - **Key ID** - идентификатор ключа. Число в диапазоне от 1 до 255.
  - **Пароль** - секретный ключ.

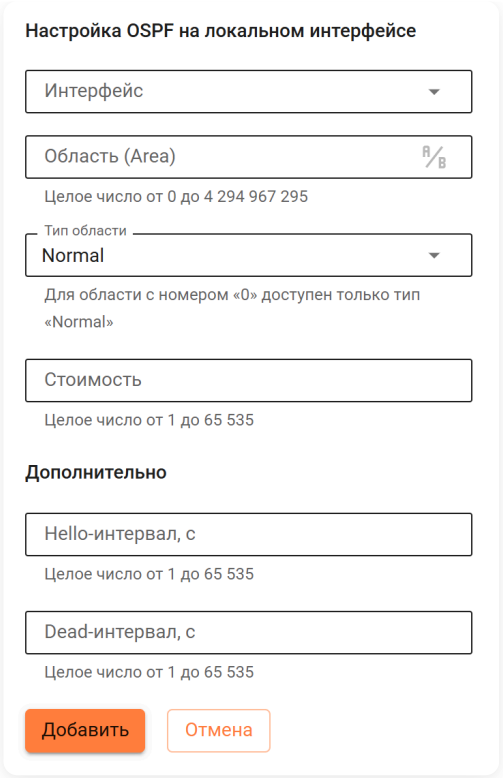
Требования к паролю

- **Максимальная длина пароля** - 16 символов.
- **Символы** - любые ASCII-символы, за исключением пробелов.

Настройка OSPF

1. Перейдите в **Маршрутизация** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



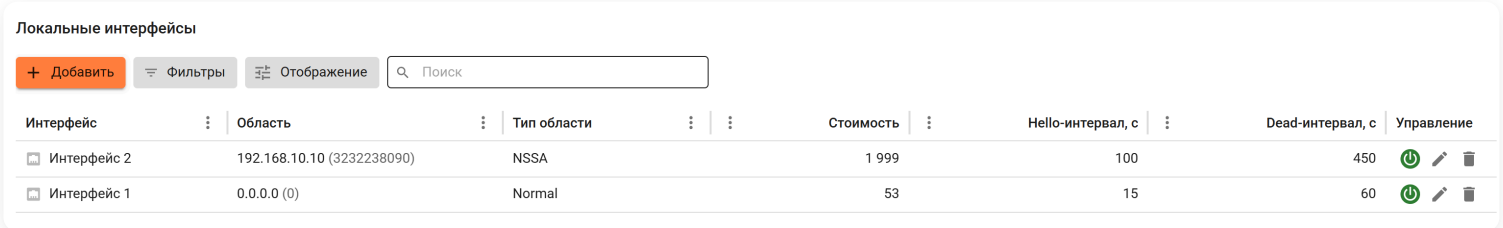
- **Интерфейс** - локальный или Loopback-интерфейс Ideco NGFW Novum, IP-адрес которого будет использован для обмена маршрутами.
- **Область (Area)** - номер области (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Тип области** - для области с указанным номером `area` должен быть выбран одинаковый тип при настройке всех OSPF-соседей. Для области с номером 0 (`0.0.0.0`) допустимо указывать только один тип - **Normal**. Допустимые значения: **Normal**, **Stub**, **NSSA**:
  - **Normal Area** (обычная зона) - стандартная зона OSPF, которая получает полную информацию о маршрутах как внутри автономной системы, так и за ее пределами. В такой зоне могут находиться как маршрутизаторы, так и конечные устройства.
  - **Stub Area** (усеченная зона) - зона, в которой не принимаются внешние маршруты (Type 5 LSA), но принимаются маршруты других зон. Вместо полной информации о внешних маршрутах используется маршрут по умолчанию.
  - **NSSA** (Not-So-Stubby Area) - разновидность Stub-зоны, которая может получать маршруты по умолчанию и отправлять свои маршруты в другие зоны через **ABR** (Area Border Router). В **NSSA** зоне используется специальный тип LSA (Type 7), который преобразуется в Type 5 на ABR.
- **Стоимость** - стоимость маршрута.
- **Hello-интервал** - время между отправкой Hello-пакетов, которое варьируется от 1 до 65535 секунд. Если поле не заполнено, по умолчанию используется значение 10 секунд. Для установления соседства между устройствами интервал должен быть одинаковым для всех участников сети.
- **Dead-интервал** - время, через которое сосед считается недоступным, если не получает Hello-пакеты. Диапазон значений - от 1 до 65535 секунд. Если поле не заполнено, по умолчанию в 4 раза больше, чем Hello-интервал. Для успешного соседства значение должно быть одинаковым у всех устройств в сегменте сети.

3. Нажмите **Добавить**.

4. Включите модуль **OSPF**.

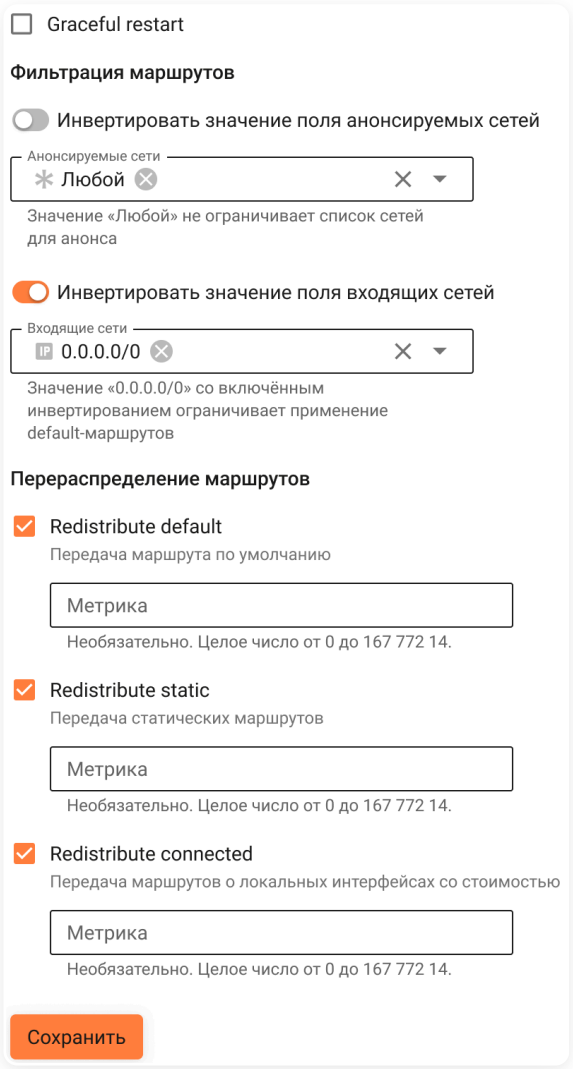
> Добавьте в таблицу OSPF **Loopback-интерфейс**, если на вкладке **Дополнительно** отключена опция **Redistribute connected** (по умолчанию включена), чтобы сети **Loopback-интерфейсов** анонсировались.

Пример готовой таблицы:



При наличии большого количества настроек OSPF в таблице воспользуйтесь кнопкой **Фильтры**.

Дополнительные



Graceful Restart - механизм обеспечения непрерывности маршрутизации, позволяющий сетевому устройству временно перезапустить управляющую плоскость (например, при обновлении ПО или восстановлении после сбоя) без немедленного перерасчета маршрутов у соседних устройств.

При включении **Graceful Restart** соседние маршрутизаторы не рассматривают кратковременный разрыв управления как отказ и продолжают использовать ранее полученные маршруты в течение ограниченного периода ожидания (120 секунд). Это позволяет избежать частых изменений состояния маршрутов и снижает влияние плановых или аварийных перезапусков на работу сети.

> **Graceful Restart** работает только при поддержке со стороны соседних маршрутизаторов.

Фильтрация маршрутов - фильтр для маршрутов, передаваемых и принимаемых от OSPF-соседей:

- **Анонсируемые сети** - маршруты, которые отправляются OSPF-соседям. По умолчанию используется значение **Любой**. Поле также фильтрует сети из блока **Перераспределение маршрутов**:
  - **Инвертировать значение поля анонсируемых сетей** - если опция включена, то OSPF-соседям будут отправлены маршруты ко всем сетям, кроме тех, что указаны в поле **Анонсируемые сети**.
- **Входящие сети** - маршруты, которые принимаются от OSPF-соседей. По умолчанию используется значение **Любой**, кроме `0.0.0.0/0`:
  - **Инвертировать значение поля входящих сетей** - если опция включена, то от OSPF-соседей будут приняты маршруты ко всем сетям, кроме указанных в поле **Входящие сети**.

Перераспределение маршрутов:

- **Redistribute default** - при включении опции для других устройств NGFW Novum будет являться шлюзом по умолчанию.
- **Redistribute static** - при включении опции будут анонсироваться статические маршруты, указанные в разделе **Маршрутизация** → **Статическая**, а также маршруты до VPN-сетей.

- **Redistribute connected** - при включении опции будут анонсироваться маршруты подсетей, подключенных напрямую, в том числе и Loopback-интерфейсов.

> Если **Redistribute connected** отключить, сети Loopback-интерфейсов будут анонсироваться при добавлении в таблицу OSPF **Loopback-интерфейса**.

Подробнее о значении поля **Метрика** - в статье.

Примеры работы фильтрации маршрутов

При включении опции:

- **Redistribute default** - чтобы NGFW Novum анонсировал себя как шлюз по умолчанию, в поле **Анонсируемые сети** укажите **Любой** или `0.0.0.0/0`.
- **Redistribute static** - если в **Маршрутизация** → **Статическая** задано шесть маршрутов, но в поле **Анонсируемые сети** указаны только три из них, то **OSPF** будет анонсировать только указанные **Анонсированные сети** OSPF-соседям.
- **Redistribute connected** - для исключения части подключенных напрямую сетей в поле **Анонсируемые сети** пропишите список сетей, которые необходимо анонсировать. Остальные подключенные сети анонсироваться не будут.

Настройка MikroTik

1. Авторизуйтесь на MikroTik и выполните команду:

```
routing ospf area add area-id=x.x.x.x default-cost=1 disabled=no inject-summary-lsa=no name=area1 type=default
```

- `x.x.x.x` - название зоны, которое указали при настройке Ideco NGFW Novum. ID должен быть уникален для каждого роутера.

2. Для передачи любых других сетей соседним устройствам по динамической маршрутизации введите команду:

```
routing ospf network add network=(другая подсеть)/24 area=area1
```

3. Повторите команду из пункта 1 для добавления каждой подсети.

4. Для вывода таблицы маршрутизации введите команду: `ip route print`.

Настройка Cisco

1. Запустите на Cisco процесс OSPF:

```
enable
conf t
router ospf 1
```

2. По умолчанию отключите отправку hello-пакетов на всех интерфейсах и включите на нужных интерфейсах:

```
passive-interface default
no passive-interface GigabitEthernet0/0
```

- `GigabitEthernet0/0` - название интерфейса.

3. Укажите сети, маршруты до которых хотите анонсировать:

```
network <IP-адрес подсети> <wildcart-маска подсети> area <номер зоны, указанный при настройке Ideco NGFW Novum>
```

Пример команды:

```
network 192.168.100.0 0.0.255.255 area 0
```

4. Если Cisco получил уведомление вида `*Dec 18 10:02:03.628: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.122.73 on GigabitEthernet0/0 from LOADING to FULL, Loading Done`, соседские отношения установлены.

5. Для просмотра списка соседей воспользуйтесь командой `show ip ospf neighbor`:

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.122.73    1   FULL/DR         00:00:38    192.168.102.11  GigabitEthernet0/0
Router#
```

6. Для вывода таблицы маршрутизации введите команду `show ip route` (в таблице должны появиться маршруты до сетей NGFW Novum):

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.102.11 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      10.0.0.0/16 is subnetted, 1 subnets
O E2     10.128.0.0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.100.0/32 is subnetted, 1 subnets
O E2     192.168.100.100
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.102.0/24 is directly connected, GigabitEthernet0/0
L        192.168.102.79/32 is directly connected, GigabitEthernet0/0
      192.168.103.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.103.0/24 is directly connected, GigabitEthernet0/1
L        192.168.103.130/32 is directly connected, GigabitEthernet0/1
O E2  192.168.122.0/24
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
```

Особенности работы OSPF в Ideco NGFW Novum

- В предустановленной конфигурации Ideco NGFW Novum - шлюз по умолчанию для других устройств.
- OSPF работает на локальных Ethernet-интерфейсах и на ГОСТ, GRE, GRE over IPsec интерфейсах.
- Значение **Типа сети** (**Network Type**) в Ideco NGFW Novum устанавливается автоматически в зависимости от типа интерфейса, используемого для OSPF:
  - GRE-интерфейсы - значение `p2p`.
  - Ethernet-интерфейсы - значение `broadcast`.

Примеры использования

Объединение филиальной сети с резервированием и/или балансировкой

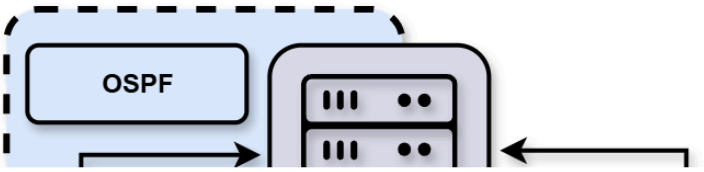


- Между **NGFW Novum-1** в Филиале 1 и **NGFW Novum-2** в Филиале 2 настраивается GRE-over-IPsec и OSPF.
- Каждый NGFW Novum подключен к двум провайдерам (**Провайдер-1** и **Провайдер-2**).

Преимущества настройки:

- Трафик будет автоматически балансироваться между **Провайдером-1** и **Провайдером-2**.
- При неисправности одного из провайдеров трафик автоматически смаршрутизируется через другое соединение.
- Отсутствует необходимость вручную настраивать маршруты до локальных сетей филиалов.

Схема с балансировкой доступа из локальной сети в интернет или другую сеть



- И **NGFW Novum-1**, и **NGFW Novum-2** используются в качестве шлюза по умолчанию.
- Между балансировщиком и каждым из NGFW Novum настроена OSPF.

Преимущества настройки:

- Трафик балансируется между **NGFW Novum-1** и **NGFW Novum-2**: часть пользователей из Локальной сети выходят в интернет через **NGFW Novum-1**, часть - через **NGFW Novum-2**.
- При неисправности одного из NGFW Novum трафик автоматически смаршрутизируется через другое соединение.
- Отсутствует необходимость вручную настраивать маршруты для хостов в Локальной сети.

Анонс конкретного хоста (/32)

Необходимо анонсировать конкретный хост `192.168.0.100/32` и обеспечить его распространение через OSPF на **NGFW Novum-2**, не передавая при этом всю сеть `192.168.0.0/24`.

Схема сети:

- **NGFW Novum-1** подключен к локальной сети `192.168.0.0/24`.
- **NGFW Novum-2** подключен к локальной сети `192.168.2.0/24`.
- Между ними настроен GRE-over-IPsec, в котором работает OSPF.

Выполните действия:

1. Перейдите в **Маршрутизация** → **Статическая** и добавьте маршрут:

- **Название** - укажите название маршрута.
- **Назначение** - выберите `192.168.0.100`.
- **Отправлять в** - выберите `192.168.0.1`.
- **Приоритет** - укажите необходимый приоритет маршруту.

2. Перейдите в **Маршрутизация** → **OSPF** → **Дополнительно** и настройте **Фильтрацию маршрутов**:

- **Анонсируемые сети** - выберите подсеть `192.168.0.100/32`.
- **Redistribute static** - включите опцию.

3. Нажмите **Сохранить**.

EIGRP

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **EIGRP**: `frr`; `ideco-routing-backend`, `ideco-routing-rest`.

Список служб для других разделов доступен по ссылке.

EIGRP (Enhanced Interior Gateway Routing Protocol) - продвинутый дистанционно-векторный протокол маршрутизации, разработанный компанией Cisco. EIGRP поддерживает высокую скорость обмена информацией о маршрутах для обеспечения актуальности таблиц маршрутизации.

Настройка модуля EIGRP на Ideco NGFW Novum состоит из шагов:

Шаг 1. Настройка аутентификации (MD5)

Для маршрутизаторов с EIGRP MD5-аутентификацию можно не настраивать только в доверенной и контролируемой среде, где уже есть защита или нет рисков.

Маршрутизаторы с разными или неверными ключами не будут устанавливать соседство - снижается риск подмены и несанкционированного участия в EIGRP.

Принцип работы MD5-аутентификации

На всех маршрутизаторах в одной зоне EIGRP задается:

- Идентификатор ключа (Key ID).
- Секретный ключ (пароль).

При отправке EIGRP-пакета маршрутизатор добавляет к нему:

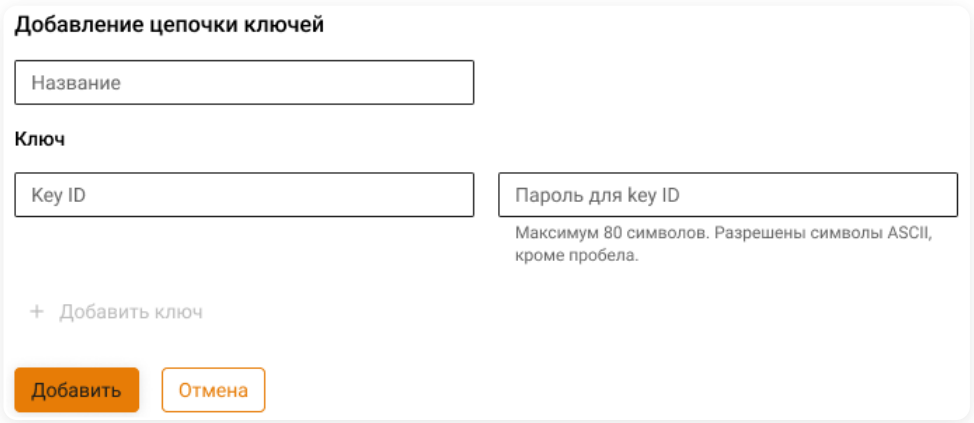
- Key ID.
- MD5-хеш, вычисленный по формуле: `MD5(EIGRP_пакет + Секретный_ключ + Key_ID)`.

Принимающая сторона (получатель):

1. Берет Key ID из пакета.
2. Находит у себя секретный ключ, соответствующий переданному Key ID.
3. Вычисляет MD5-хеш по той же формуле и сравнивает с полученным:

- Если хеши совпали, пакет принимается.
- Если хеши не совпали, пакет отбрасывается с ошибкой.

1. Перейдите в **Маршрутизация** → **EIGRP** → **Ключи** и нажмите **Добавить**:



- **Название** - введите название цепочки ключей. Название может быть неуникальным.
- **Key ID** - введите идентификатор ключа. Число в диапазоне от 1 до 255.
- **Пароль для key ID** - введите пароль для ключа.

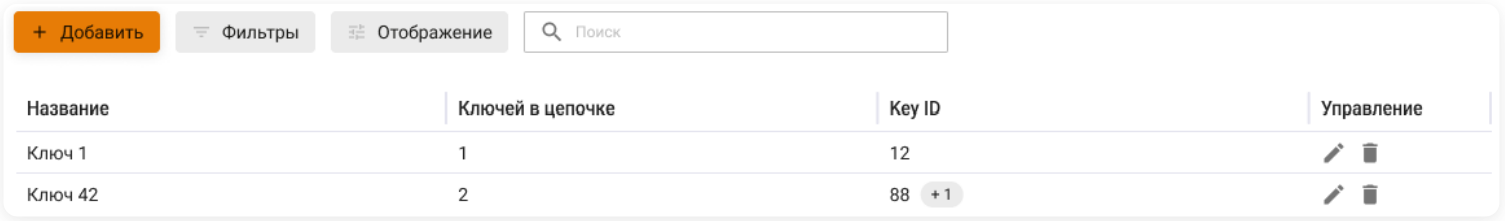
Требования к паролю

- **Максимальная длина пароля** - 80 символов.
- **Символы** - любые ASCII-символы, за исключением пробелов.

2. При необходимости добавьте в цепочку дополнительные ключи, нажав **Добавить ключ**.

3. Нажмите **Добавить**.

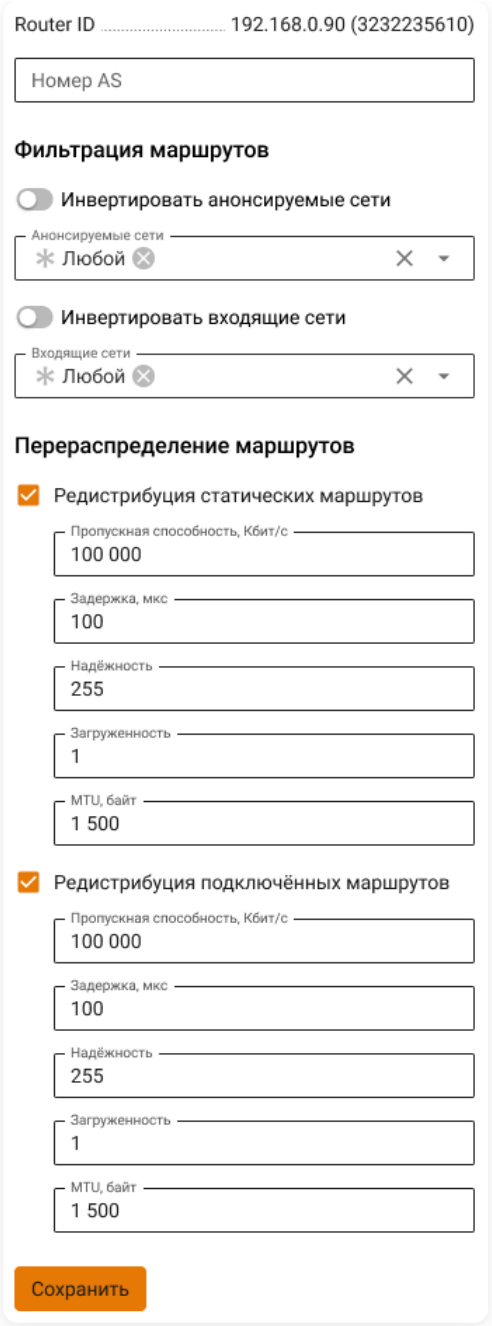
Созданные цепочки ключей отображаются в таблице:



Шаг 2. Настройка автономной системы EIGRP

Перед настройкой соседей необходимо на Ideco NGFW Novum указать номер автономной системы (AS) и активировать модуль.

1. Перейдите в **Маршрутизация** → **EIGRP** → **Настройки**:



2. Введите **Номер AS**. Маршрутизаторы с одной автономной системой обмениваются маршрутами и устанавливают соседство. Маршрутизаторы с разными AS друг с другом по EIGRP не взаимодействуют.

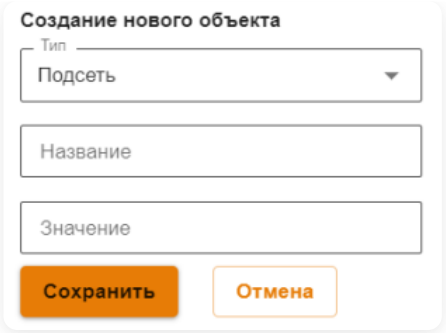
3. Настройте **Фильтрацию маршрутов**:

- **Анонсируемые сети** - список сетей, которые разрешено отправлять в EIGRP другим соседям.
- **Входящие сети** - список сетей, которые разрешено принимать от соседей по EIGRP и добавлять в таблицу маршрутизации.

Опции инвертирования позволяют использовать списки анонсируемых и входящих сетей наоборот, когда разрешено все, кроме указанных сетей.

Создание нового объекта

В поле **Анонсируемые сети** или **Входящие сети** нажмите **Создать новый объект** и заполните поля:



- **Тип** - значение **Подсеть**.
- **Название** - любое значение.
- **Значение** - значение подсети в формате: `подсеть/маска подсети`, например, `192.168.100.0/24`.

4. При необходимости настройте **Перераспределение маршрутов**:

- **Редистрибуция статических маршрутов** - при включении опции будут анонсироваться статические маршруты, указанные в разделе **Маршрутизация** → **Статическая**, а также маршруты до VPN-сетей.
- **Редистрибуция подключенных маршрутов** - при включении опции будут анонсироваться маршруты подсетей, подключенных напрямую, в том числе и Loopback-интерфейсов.

> Если **Редистрибуция подключенных маршрутов** отключена, сети Loopback-интерфейсов будут анонсироваться при добавлении **Loopback-интерфейса** в таблицу **Интерфейсы**.

При необходимости для каждого типа перераспределения задайте метрики:

- **Пропускная способность** - минимальная пропускная способность на всем пути к сети (Кбит/с). Чем выше пропускная способность, тем предпочтительнее маршрут. По умолчанию 100 000 Кбит/с.
- **Задержка** - сумма задержек интерфейсов на пути, в десятках микросекунд. По умолчанию 100.
- **Надежность** - оценка надежности канала (0–255), обычно от статистики потерь пакетов. По умолчанию 255.
- **Загруженность** - загрузка канала (0–255). По умолчанию 1.
- **MTU** - максимальный размер пакета на пути, в байтах. По умолчанию 1500.

> Обычно значений метрик по умолчанию достаточно для большинства сценариев. EIGRP использует композитную метрику (одно число), которая рассчитывается из указанных параметров. Задавайте их явно только при необходимости тонко управлять выбором пути.

5. Нажмите **Сохранить**.

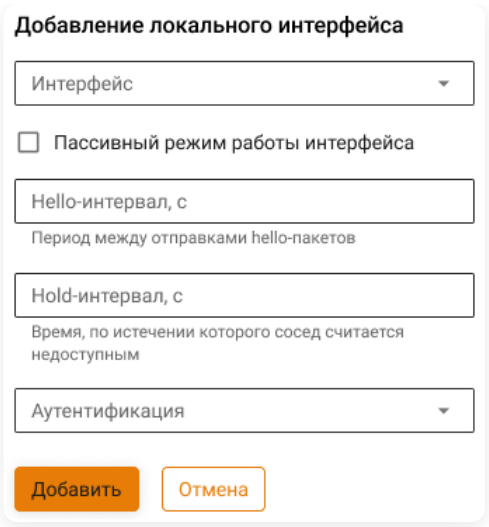
6. Включите модуль **EIGRP**.

Шаг 3. Настройка интерфейсов, участвующих в процессе EIGRP

> Если интерфейс не добавлен в таблицу или не активен, EIGRP на нем работать не будет.

Для каждого из сетевых интерфейсов, участвующих в EIGRP, на Ideco NGFW Novum выполните шаги:

1. Перейдите в **Маршрутизация** → **EIGRP** → **Интерфейсы** и нажмите **Добавить**:



2. Выберите интерфейс, на котором запускается протокол EIGRP в поле **Интерфейс**.

3. Включите опцию **Пассивный режим работы интерфейса**, если нужно, чтобы выбранный интерфейс участвовал в EIGRP, но не отправлял и не принимал EIGRP-пакеты. Интерфейс будет анонсировать свою сеть, но соседство с другими маршрутизаторами через него не устанавливается. При выборе пассивного режима остальные параметры интерфейса станут недоступны.

Пассивный режим работы интерфейса полезен, когда требуется подключить сеть в EIGRP, не создавая лишнего трафика и соседства (например, stub-сети).

4. Установите параметры интерфейса, если требуется:

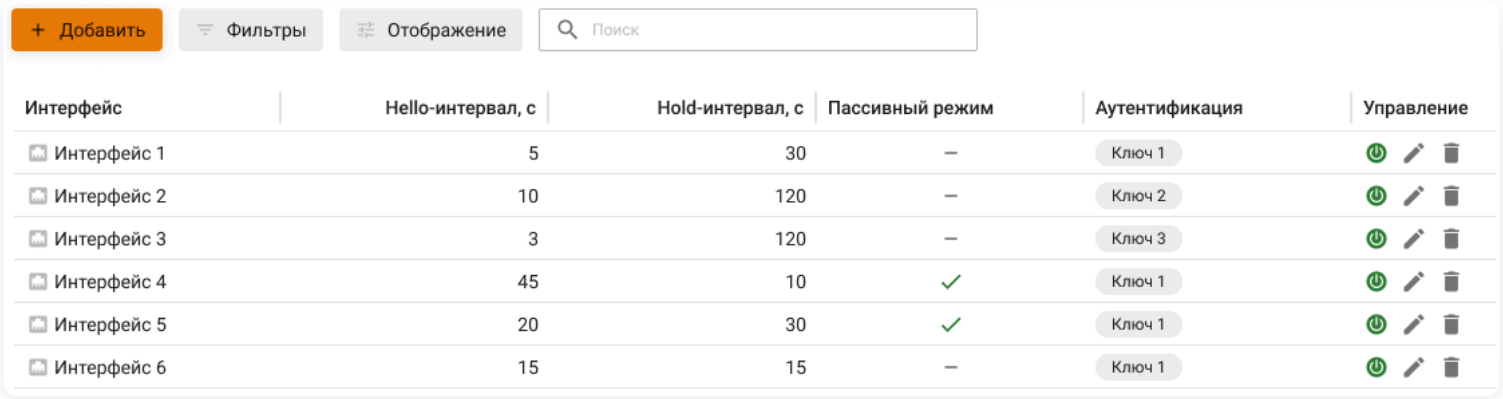
- **Hello-интервал** - интервал в секундах, с которым маршрутизатор отправляет пакеты Hello на multicast-адрес.
- **Hold-интервал** - максимальное время (в секундах) без пакетов Hello, после которого сосед считается потерянным и соседство сбрасывается.
- **Аутентификация** - выберите цепочку ключей, если используете MD5-аутентификацию.

5. Нажмите **Сохранить**.

Если соседство не устанавливается при включенной MD5, проверьте, что:

- Имя цепочки ключей привязано к интерфейсу.
- На соседнем устройстве настроен тот же ключ (ID и пароль).
- В логах системы нет ошибки `authentication mismatch`.

Интерфейсы, участвующие в маршрутизации EIGRP, отображаются в таблице:



При перенастройке EIGRP на Ideco NGFW Novum возможна кратковременная потеря связи с соседями.

Если после изменения настроек EIGRP перестал работать (например, соседи долго не появляются), выключите и включите модуль **EIGRP** вручную.

Маршрутизация внешних сетей

Классический контекст | Высокопроизводительный контекст | API

Позволяет направлять трафик от разных пользователей или групп пользователей по заданным маршрутам. Маршрутизация внешних сетей применяется после PBR, статической и динамической маршрутизации.

Способы применения:

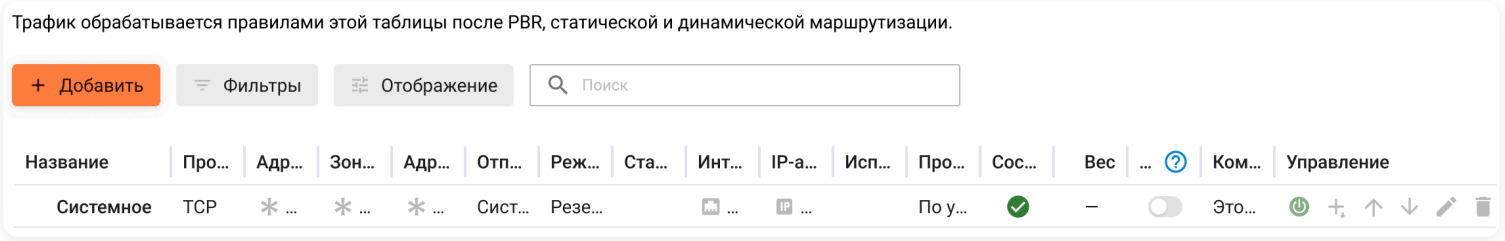
- Направление части трафика через интернет-провайдера с наименьшей стоимостью этого трафика.
- Предоставление доступа в интернет через одного из провайдеров для определенных пользователей/групп пользователей.

Маршруты в таблице имеют приоритет сверху вниз, то есть **верхний маршрут приоритетнее нижнего**.

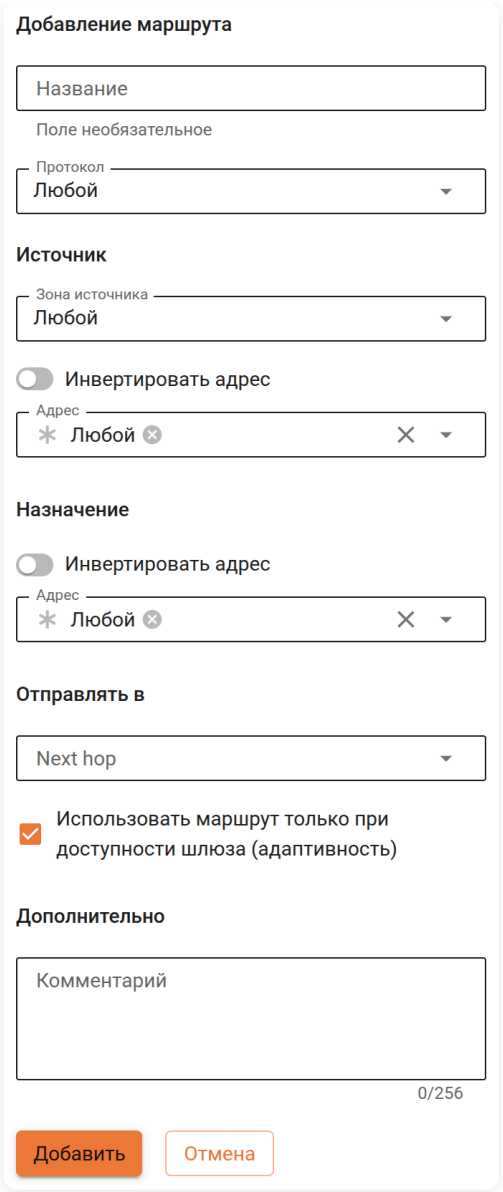
Перед обновлением на Ideco NGFW Novum версии 22 ознакомьтесь с информацией по ссылке.

Действия для настройки:

1. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**:



2. Заполните поля:



Расшифровка полей

- **Название** - введите название маршрута.
- **Протокол** - выберите протокол передачи данных: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP).
- **Источник**:
  - **Зона** - выберите интерфейс или группу интерфейсов Ideco NGFW Novum, на которые приходит трафик от источника. Объект типа **Зона** можно создавать и редактировать только в **Системном контексте**.
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - выберите объект, трафик от которого нужно маршрутизировать. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
  - **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.
  - **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

Не рекомендуем указывать порт источника, так как он обычно выбирается случайным образом. Исключение - протоколы с фиксированными портами источника и назначения (например, DNS).

- **Назначение**:
  - **Инвертировать адрес** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - выберите объекты, при обращении к которым будет применяться этот маршрут. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
  - **Инвертировать порты** - включите опцию, чтобы исключить в маршруте все объекты, кроме выбранных в поле **Порты**.

- **Порты** - укажите порт, список портов или диапазон портов, определенных в **Объектах**, при создании маршрута с протоколами TCP/UDP. Максимальное количество объектов в поле - 200.

- **Отправлять в** - выберите вариант, через который будет направляться трафик. В поле могут быть выбраны: Next hop, Профили next hop, IP-адреса или Статическая маршрутизация. IP-адрес можно указать как **Объект** или **Значение**. При выборе Статической маршрутизации NGFW Novum трафик перенаправляется в таблицу **Статической маршрутизации**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

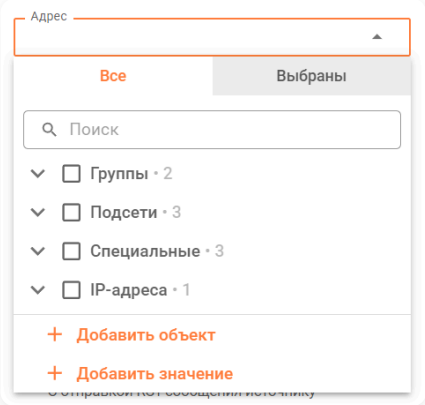
Отличие значений от объектов:

- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

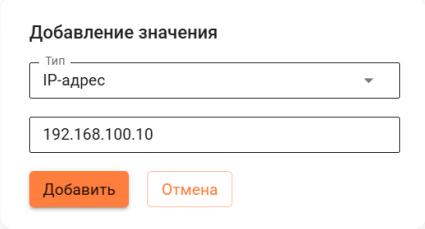
Управление значениями

Добавление

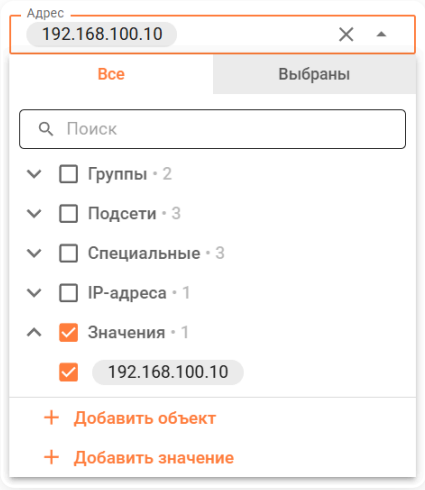
1. В поле нажмите **Добавить значение**:



2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:

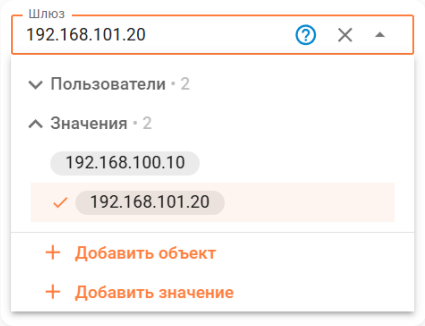


Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:



2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

- **Использовать маршрут только при доступности шлюза (адаптивность)** - включите опцию, чтобы маршрутизатор при недоступности **Next hop** продолжал поиск маршрута по нижестоящим правилам. Если опция отключена, трафик отбрасывается, а отправителю возвращается ошибка `destination unreachable`.
- **Дополнительно**:
  - **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

Адаптивность

Опция **Использовать маршрут только при доступности шлюза (адаптивность)** требует настроенной проверки доступности шлюза. Без проверки доступности NGFW Novum не сможет определить, что шлюз недоступен, и адаптивность не сработает.

Настроить проверку доступности можно одним из способов:

Next hop

Используйте этот способ, если в поле **Отправлять в** указан **Next hop**.

1. Перейдите в **SD-WAN** → **Next hop**.

2. Нажмите напротив нужного next hop.

3. Включите опцию **Использовать BFD**.

4. Нажмите **Сохранить**.

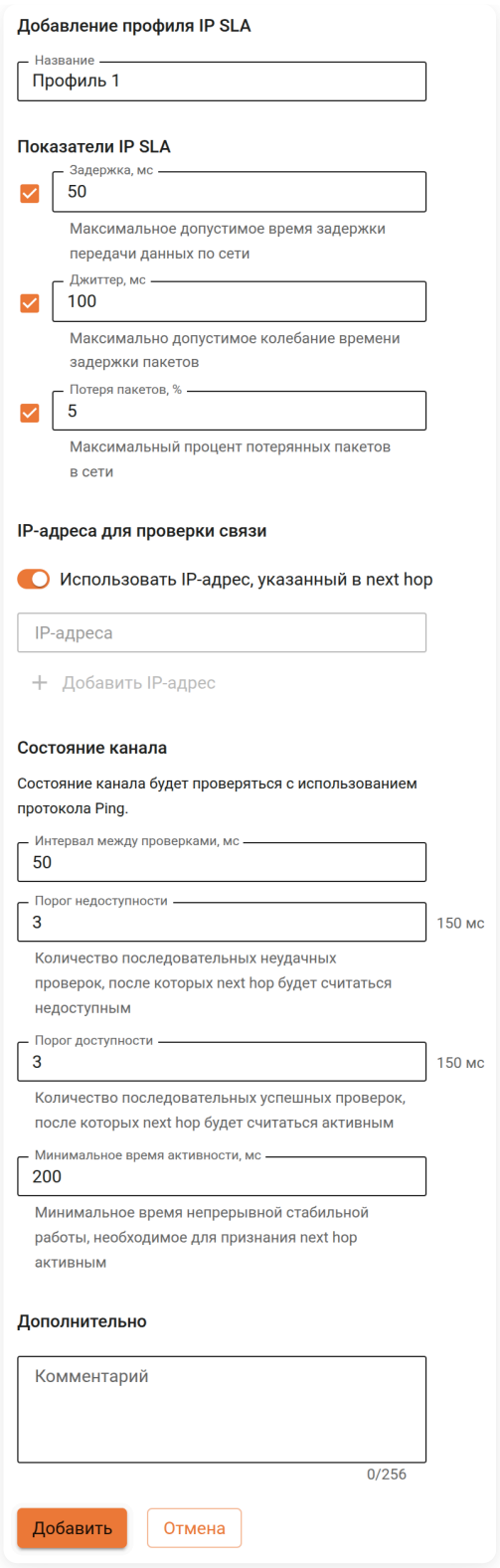
Поддержка BFD должна быть настроена и на стороне указанного шлюза. Без этого проверка доступности работать не будет.

Профили next hop

Используйте этот способ, если в поле **Отправлять в** указан **Профиль next hop**.

1. Перейдите в **SD-WAN** → **Профили IP SLA** и нажмите **Добавить**.

2. Заполните параметры профиля. В блоке **IP-адреса для проверки связи** включите опцию **Использовать IP-адрес, указанный в next hop**:



3. Нажмите **Сохранить**.

4. Перейдите в **SD-WAN** → **Профили next hop** и нажмите напротив нужного профиля.

5. В поле **Профиль IP SLA** выберите созданный профиль.

6. Нажмите **Сохранить**.

Автоматическое перенаправление трафика при недоступности шлюза можно реализовать без опции **Использовать маршрут только при доступности шлюза (адаптивность)**. Для этого в поле **Отправлять в** выберите **Профиль next hop** с режимом **Резервирование**. В этом случае трафик будет направляться через доступный next hop с учетом приоритета.

В столбце **Управление** можно:

 Включать или выключать правило.

 Менять приоритет.

 Редактировать правило.

 Удалять правило.

Полезные ссылки

- **Объекты**
- **Статическая маршрутизация**
- **Next hop**
- **Профили next hop**

Отчеты и журналы

Настройте получение данных об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени

Трафик

Статистика из **Контроля приложений** и **Контент-фильтра**

Перейти >

Система

Таблица логов работы служб

Перейти >

Веб-трафик

Статистика из проверки трафика антивирусом и модулем **Контент-фильтр**

Перейти >

Межсетевой экран

Таблица срабатываний правил **Межсетевого экрана**

Перейти >

События безопасности

Статистика событий модулей WAF и IPS, а также графики событий IPS

Перейти >

Действия администраторов

Таблица действий администраторов в Ideco NGFW

Перейти >

Аутентификация администраторов

Таблица аутентифицированных на Ideco NGFW администраторов

Перейти >

Аутентификация пользователей

Таблица аутентифицированных на Ideco NGFW пользователей

Перейти >

Аутентификация пользователей ЛК

Таблица сессий пользователей, авторизованных в личном кабинете Ideco NGFW

Перейти >

Конструктор отчетов

Создание шаблонов отчетов и настройка рассылки на электронную почту

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Трафик

Классический контекст | Высокопроизводительный контекст

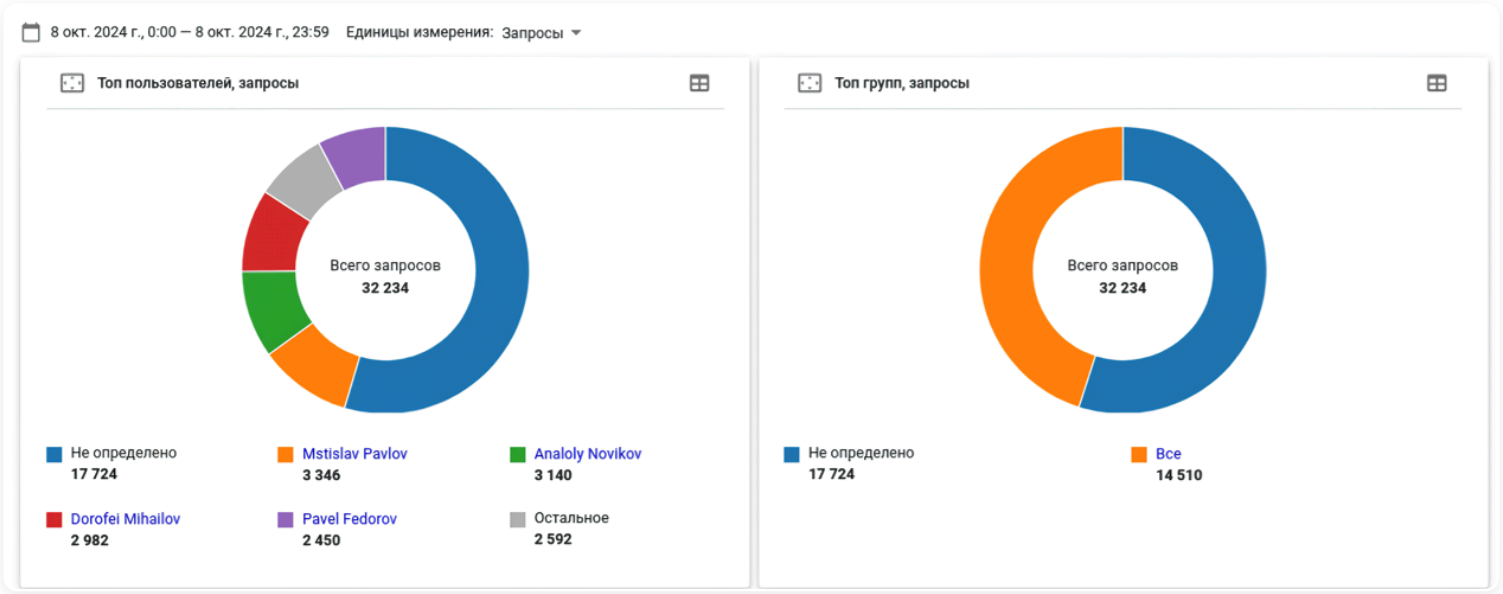
При включении опции **Трафик** в левом верхнем углу раздел начинает собирать статистику из Контент-фильтра и отображается в виде виджетов.

Способы отображения информации:

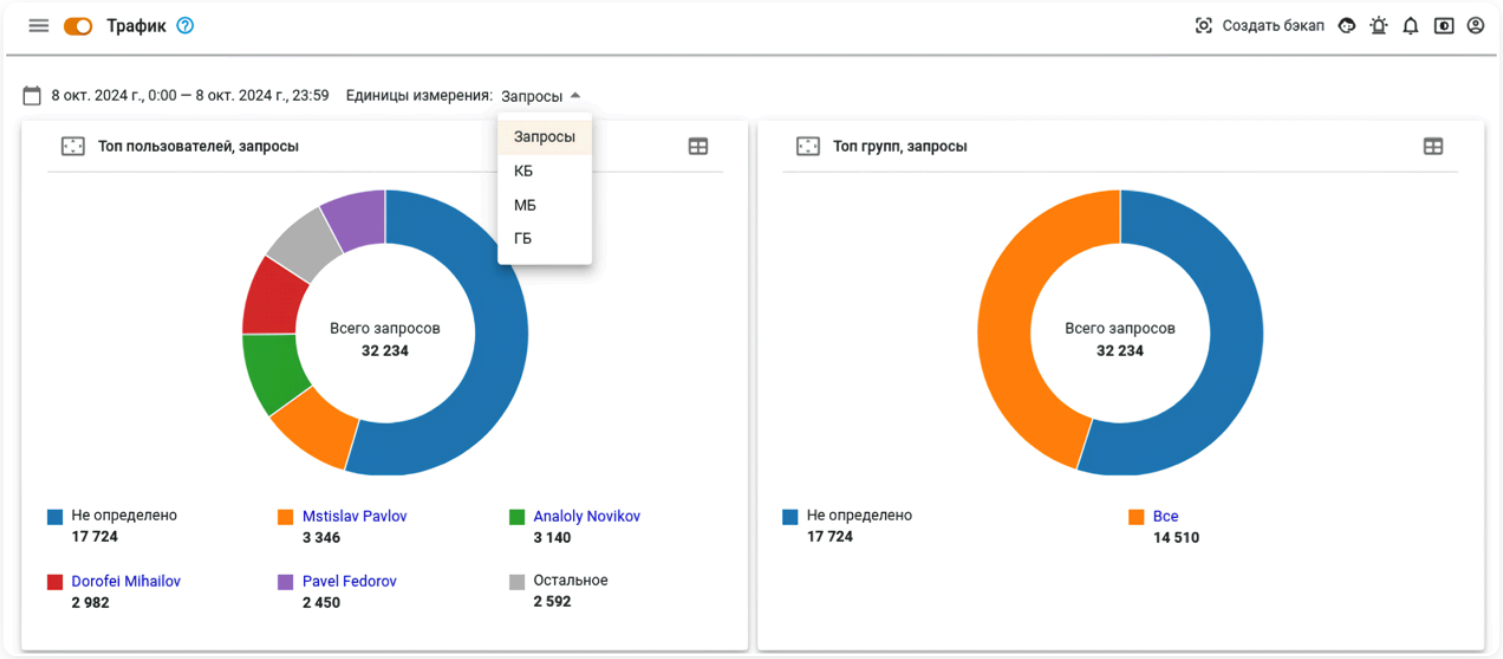
- Круговая диаграмма ( ) и таблица ( ).
- Развернутый режим ( ).

Диаграмма и таблица

Содержат топ-6 объектов. Каждый объект кликабелен и ведет на страницу с виджетами, в которых статистика фильтруется по этому объекту:



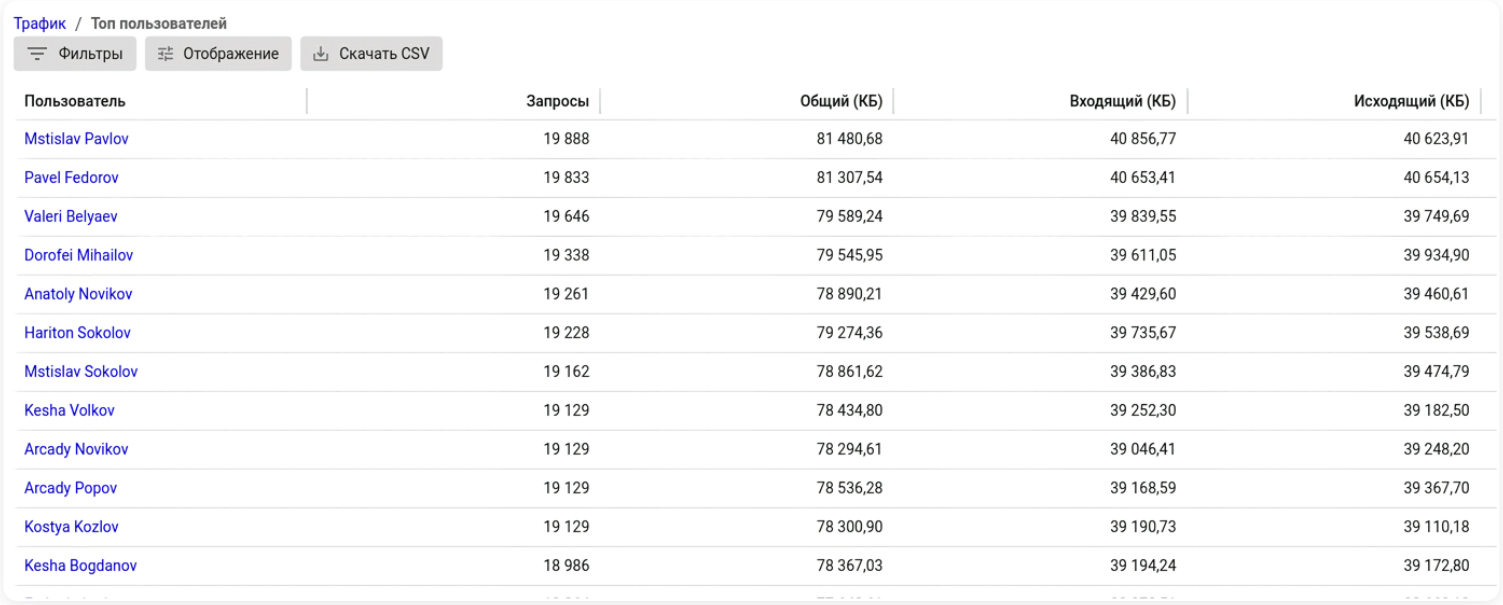
Единицу измерения можно изменить по кнопке над виджетами:



Не определено (трафик с неизвестным адресом и пользователем) - это любой трафик от самого Ideco NGFW Novum. Например, скачивание баз Контент-фильтра, GeoIP, сигнатур и т.д.

Развернутый режим

Содержит данные по всем объектам из топа. Для поиска по объектам воспользуйтесь кнопкой **Фильтры**.



Пользователь	Запросы	Общий (КБ)	Входящий (КБ)	Исходящий (КБ)
Mstislav Pavlov	19 888	81 480,68	40 856,77	40 623,91
Pavel Fedorov	19 833	81 307,54	40 653,41	40 654,13
Valeri Belyaev	19 646	79 589,24	39 839,55	39 749,69
Dorofei Mihailov	19 338	79 545,95	39 611,05	39 934,90
Anatoly Novikov	19 261	78 890,21	39 429,60	39 460,61
Hariton Sokolov	19 228	79 274,36	39 735,67	39 538,69
Mstislav Sokolov	19 162	78 861,62	39 386,83	39 474,79
Kesha Volkov	19 129	78 434,80	39 252,30	39 182,50
Arcady Novikov	19 129	78 294,61	39 046,41	39 248,20
Arcady Popov	19 129	78 536,28	39 168,59	39 367,70
Kostya Kozlov	19 129	78 300,90	39 190,73	39 110,18
Kesha Bogdanov	18 986	78 367,03	39 194,24	39 172,80

Если в левом верхнем углу установлен флаг в строке **Запросы**, то объекты отфильтруются по убыванию по колонке **Запросы**. Если **Трафик** - по убыванию в колонке **Входящий**.

Время и дата в виджете отображается в часовом поясе сервера.

Примеры использования:

На какие запрещенные сайты переходил определенный пользователь

- Откройте раздел **Отчеты и журналы** → **Трафик**.
- В виджете **Топ пользователей** найдите нужного пользователя и нажмите по нему. Если пользователя нет в списке, то нажмите **Развернуть** ( ) в левом верхнем углу виджета (откроется список всех пользователей).
- В виджете **Топ заблокированных сайтов** Ideco NGFW Novum покажет топ-5 блокировок. Для просмотра полного списка блокировок нажмите **Развернуть** ( ).

Каким пользователям заблокировали определенное приложение

- Откройте раздел **Отчеты и журналы** → **Трафик**.
- В виджете **Топ заблокированных протоколов** найдите требуемый протокол и нажмите по нему. Если протокола нет в списке, то нажмите **Развернуть** ( ).
- Чтобы увидеть список всех пользователей, у которых был заблокирован протокол, на открывшейся странице найдите виджет **Топ пользователей** и нажмите **Развернуть** ( ).

Подробнее о создании собственных шаблонов со статистикой - в статье Конструктор отчетов.

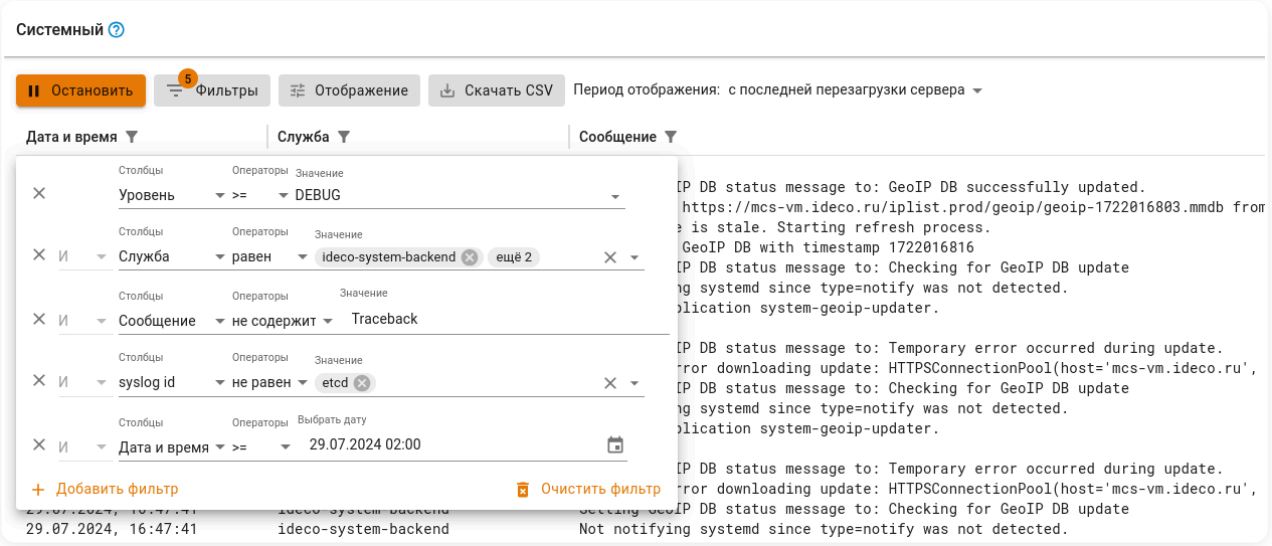
Система

Классический контекст | Высокопроизводительный контекст

Время хранения логов в разделе **Система** - 90 дней.

Для просмотра логов определенной службы воспользуйтесь строкой поиска или фильтром.

Для фильтрации логов по нескольким параметрам нажмите **Добавить фильтр** и выберите соответствующий критерий, значение и оператор в форме. Фильтрация по нескольким критериям:



По кнопке **Скачать CSV** сохраняются те строки логов, которые заданы фильтрацией.

Полный список служб смотрите в статье.

Удаление заблокированных соединений

Служба `ideco-conndrop` принудительно завершает сетевые соединения, запрещенные правилами **Межсетевого экрана**.

Алгоритм работы службы:

1. Присваивает соединению метку `ideco-irreversible-drop` при срабатывании запрещающего правила **Межсетевого экрана**.
2. Каждую минуту выполняет фильтрацию записей с меткой `ideco-irreversible-drop` и удаляет их.

Защита от брутфорс-атак (fail2ban)

Для просмотра логов службы `fail2ban` задайте фильтр `fail2ban` в строке поиска.

Как посмотреть заблокированные адреса и управлять белым списком, описано в статье **Защита от брутфорс-атак (fail2ban)**

Полезные ссылки

- **Ручная корректировка GeoIP**

Список служб

Классический контекст | Высокопроизводительный контекст

Логи представленных служб доступны в разделе Сервис:

Модуль	Имя службы
ALD Pro	ideco-ald-rest, ideco-ald-backend
Active Directory	ideco-ad-log-collector, ideco-ad-backend
BGP, OSPF	ideco-routing-rest, ideco-routing-backend, frr
Control Plane	nginx-control-plane
DNS	unbound-keygen, unbound-anchor, unbound, nsd, ideco-dns-backend, ideco-dns-dnstap-reader
DDNS	ideco-dns-backend
DHCP	ideco-dnsmasq, ideco-dhcp-server-backend
Data Plane	nginx-data-plane
IGMP Proxy	ideco-igmpproxy-rest, ideco-igmpproxy-backend, ideco-igmpproxy
IPsec	ideco-ipsec-backend
Ideco Center	ideco-central-console-backend
Ideco Client	ideco-websocket-vpn-server, ideco-agent-websocket, ideco-agent-backend
NTP	chronyd
Syslog	ideco-monitor-backend, ideco-logs-backend
VCE	ideco-vce-rest, ideco-vce-backend, ideco-vce-vpp
VPN-подключения	pcscd, ideco-vpn-sessions-sync, ideco-vpn-servers-backend, ideco-vpn-netns, ideco-vpn-dhcp-backend, ideco-vpn-authd, ideco-gost-vpn-rest, ideco-gost-vpn-backend, ideco-accel-sstp, ideco-accel-l2tp, strongswan, ideco-vpn-authd-dhcp-auth-server
Web Application Firewall	ideco-waf-event-syncer, ideco-waf-backend
Авторизация	ideco-auth-backend
Антивирус	klmsinit, kav-scanner, ideco-av-backend
Антиспам и антивирус	klms_postgres
Профили next hop, Маршрутизация	ideco-routing-backend
Бэкапы	ideco-backup-rotate, ideco-backup-restore, ideco-backup-create, ideco-backup-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-backend, ideco-web-authd
Дополнительно	ideco-system-swap, ideco-system-backend
Кластеризация	ideco-cluster-backup-pusher, ideco-cluster-backend
Контент-фильтр	ideco-content-filter-backend, ideco-content-filter-sky-db-updater, ideco-content-filter-backend-rules-file-syncer, ideco-rocks-cf-tool
Лицензия	ideco-license-backend
Межсетевой экран	ideco-fw-stats, ideco-firewall-rest, ideco-firewall-backend, ideco-apply-manual-blocklist, ideco-acl-rest, ideco-acl-backend, ideco-nflog
Обновления	ideco-sysupdate-backend
Обнаружение устройств	ideco-netscan-backend
Объекты	ideco-alias-backend
Обратный прокси	ideco-reverse-backend
Ограничение скорости	ideco-shaper-backend
Отчеты и журналы	ideco-reports-backend, ideco-logs-syncer, ideco-logs-backend, ideco-audit-backend

Модуль	Имя службы
Предотвращение вторжений	ideco-suricata-profiles-syncer, ideco-suricata-profiles-syncer-backend, ideco-suricata-event-syncer, ideco-suricata-backend, ideco-suricata
Прокси	squid, ideco-proxy-backend
Профили контроля приложений	ideco-app-stats, ideco-app-control-nfq, ideco-app-backend
Сертификаты	ideco-cert-backend
Сетевые интерфейсы	ideco-local-menu, ideco-l2manager-rest, ideco-l2manager-l2migration, ideco-l2manager-dhclient, ideco-l2manager-backend, ideco-l2-manager

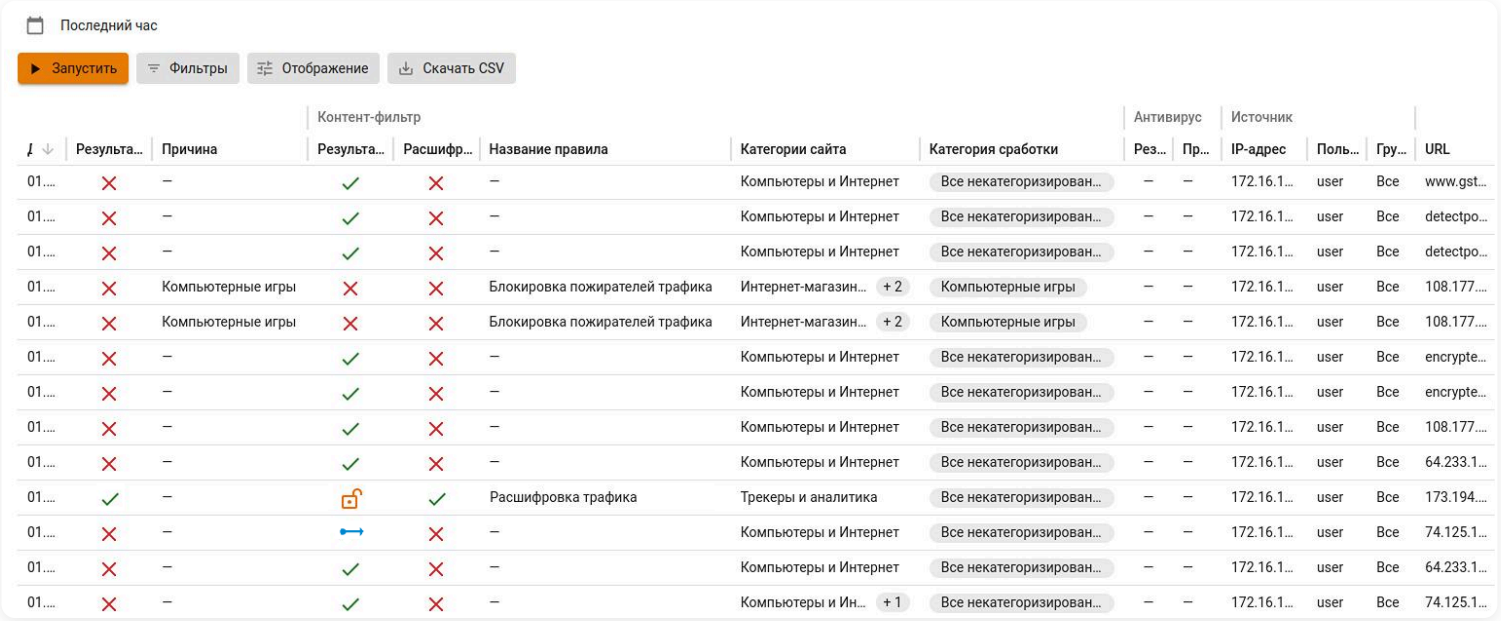
Служебные:

Модуль	Имя службы
API	ideco-rest-api-backend
MY.IDECO	ideco-mir-alerts
Авторизация и межсетевой экран	ideco-auth-backend-vpn-ipset-syncer
Базовая система и менеджер сессий (systemd)	user, var-log-journal, systemd-udevd, systemd-tmpfiles-setup, systemd-sysctl, systemd-oomd, systemd-nsresourced, systemd-modules-load, systemd-machined, systemd-logind, systemd-journald, systemd-hostnamed, systemd-homed, systemd-coredump, systemd-boot-random-seed, init, login, su
Демон для работы RDP в SSL VPN	guacd
Инженерная панель	ideco-engineering-panel-backend
Контроль целостности системы	ideco-check-sums
Локальная база данных	ideco-etcd-runtime-defrag, ideco-etcd-runtime, ideco-etcd-permanent-defrag, ideco-etcd-permanent
Настройка системы в облачных развертываниях	ideco-vk-cloud-license, ideco-cloud-init-backend
Ограничение скорости	ideco-netmap-loader, ideco-netmap-backend
Отчеты и журналы	ideco-clickhouse-enrichment
Проверка прав пользователей на перезапуск служб systemd	ideco-policy-backend
Ранняя инициализация системы	dracut-initqueue, dracut-cmdline
Сбор метрик и статистики	prometheus-node-exporter, prometheus, ideco-gatherstat-backend
Сервер базы данных	clickhouse-server
Системная шина	dbus-broker
Создание дампов ядра в случае падения	kdump
Управление томами	lvm2-monitor, lvm-activate-utm_421259

Веб-трафик

Классический контекст | Высокопроизводительный контекст

В разделе представлен результат проверки трафика антивирусом и модулем **Контент-фильтр**. Для просмотра отчета перейдите в **Отчеты и Журналы → Веб-трафик**:



Для настройки столбцов журнала нажмите **Отображение**.

Столбец	Описание
Общие	
Дата и время	Дата и время записи в формате `ДД.ММ.ГГГГ, ЧЧ:ММ:СС`
Результат проверки	Разрешено/расшифровано/запрещено/перенаправлено
Причина	Причины блокировки: название категории, имя словаря, HTTP-метод или MIME-тип, по которым был запрещен доступ к сайту
URL	Адрес запроса
Домен	Домен запроса
Путь	URL без домена
Перенаправлено на	Адрес, на который перенаправлен запрос
Referer	Заголовок Referer HTTP-запроса
Общий, МБ	Общий трафик
Входящий, МБ	Входящий трафик для запроса
Исходящий, МБ	Исходящий трафик для запроса
Тип/версия протокола	HTTP/HTTPS и версия протокола
Код ответа	Код ответа на запрос
Метод	Метод запроса
Тип контента	Заголовок Content-Type HTTP-запроса
Агент пользователя	Браузер или другой агент пользователя и его версия с указанием ОС
Контент-фильтр	

Результат	Результат работы Контент-фильтра:  - **Разрешено**  - **Расшифровано**  - **Запрещено** - **Перенаправлено на**
Расшифровка	 - **Трафик расшифрован**  - **Трафик не расшифрован**
Правило из Ideco Center	При наличии Ideco Center - постправило/предправило/локальное правило или прочерк
ID правила	Идентификатор правила контент-фильтра
Название правила	Название правила, под которое попадает запрос
Категории сайта	Категории из классификации сайтов, к которым относится запрос
Категория сработки	Категория из классификации сайтов контент-фильтром, по которой сайт был заблокирован
Антивирус	
Результат	Результат работы Антивируса: разрешено/расшифровано/запрещено/перенаправлено
ID	Идентификатор профиля антивируса
Профиль	Название профиля антивируса
Серьезность угрозы	Указанная антивирусом серьезность угрозы: информационный, низкий, средний, высокий
Тип обнаруженной угрозы	Указанный антивирусом тип угрозы: Рекламное (Adware), Вредоносные инструменты, Порнографическое (Pornware), Потенциально опасное (Riskware), Трояны, Неопознанное вредоносное ПО высокой опасности, Неопознанное вредоносное ПО средней опасности, Вирусы
Название объекта	Путь к файлу. Для простых файлов имеет неинформативное техническое значение, типа `Memory region 123`. Для архивов и других контейнеров содержит также путь к проверенному объекту внутри контейнера, типа `Memory region 123//virus.exe`
Тип объекта	Файл/URL (для вредоносных ссылок)
Формат объекта	Формат файла для функции блокировки по формату
Источник	
IP-адрес	Адрес источника
Порт	Порт источника запроса
Пользователь	Пользователь, от имени которого идет запрос
Группа	Группа, к которой относится пользователь
Назначение	
IP-адрес	Адрес назначения
Порт	Порт назначения
Кластер	
ID	Идентификатор кластера
Название	Название кластера
VCE	
ID	Идентификатор контекста
Название	Название контекста

Если с устройства пользователя недоступен какой-либо интернет-ресурс, в **Отчеты и журналы** → **Веб-трафик** можно найти правило, блокирующее ресурс.

Для просмотра блокировок по конкретному правилу воспользуйтесь кнопкой **Фильтры**, указав в форме наименование правила и оператор.

Межсетевой экран

Классический контекст | Высокопроизводительный контекст | API

В журнале отображается информация о срабатывании правил **Межсетевого экрана** (таблицы FORWARD и INPUT), а также о профилях **Предотвращения вторжений** и **Контроля приложений**.

Раздел позволяет быстро выявить модуль фильтрации, который блокирует трафик, и выявить DDoS-атаки.

В таблицу попадают соединения, которые подошли под правила в таблице Логирования. Фильтрация наиболее быстро работает с полями **Пользователь источника**.

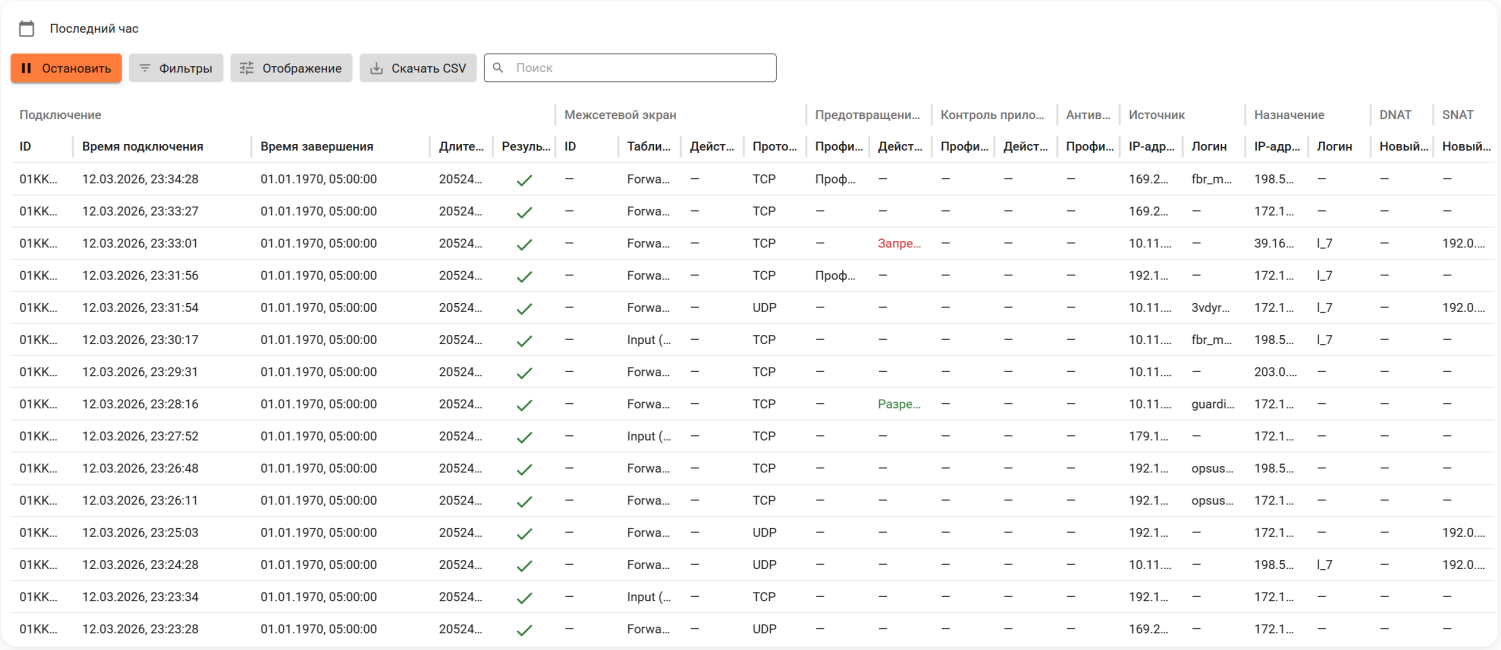
Соединения, которые были установлены до включения правил в таблице Логирование или не попали ранее под эти правила, не будут отображены в журнале.

Будьте внимательны: объем данных в журнале **Межсетевой экран** может кратно превысить объем данных любого другого журнала. Журнал хранит данные за три месяца, но при превышении размера журнала 15 ГБ старые записи будут удалены.

Чтобы отрегулировать столбцы, отображаемые в таблице, воспользуйтесь кнопкой **Отображение**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**.

При фильтрации по **Таблице правил (Межсетевой экран)** можно вывести срабатывания системных правил (Forward System и Input System). Это правила **Межсетевого экрана**, которыми нельзя управлять из веб-интерфейса Ideco NGFW Novum, они всегда включены. Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Межсетевого экрана**. По вопросам срабатывания системных правил обращайтесь в Техническую поддержку.



Столбец	Описание
Подключение	
ID	Идентификатор сессии
Время подключения	Дата начала сессии
Время завершения	Дата завершения сессии
Длительность	Длительность сессии

Результат	Результат проверки трафика тремя модулями фильтрации: Межсетевой экран, Предотвращение вторжений, Контроль приложений. Результат проверки:  - **Разрешено**  - **Расшифровано**  - **Запрещено** - **Перенаправлено на**
Межсетевой экран	
ID	Идентификатор правила Межсетевого экрана
Таблица правил	Правила, которые сработали: • FORWARD - таблица FORWARD раздела Межсетевой экран Ideco NGFW Novum • DNAT - таблица DNAT раздела Межсетевой экран Ideco NGFW Novum • INPUT - таблица INPUT раздела Межсетевой экран Ideco NGFW Novum • SNAT - таблица SNAT раздела Межсетевой экран Ideco NGFW Novum • FORWARD BEFORE - предправило FORWARD Ideco Center • FORWARD AFTER - постправило FORWARD Ideco Center • INPUT BEFORE - предправило INPUT Ideco Center • INPUT AFTER - постправило INPUT Ideco Center • FORWARD SYSTEM - системное правило FORWARD • INPUT SYSTEM - системное правило INPUT Информацию по системному правилу можно просмотреть через Терминал, введя команду `iptables-save / grep 'sys.<ID правила>'`. Смотрите примеры в статье
Действие	Действие, определенное для трафика, подпадающего под сработавшее правило. Возможные действия: Разрешить, Запретить, Перенаправить в профиль
Протокол	Протокол соединения
Предотвращение вторжений	
ID	Идентификатор профиля Предотвращения вторжений
Профиль	Название профиля Предотвращения вторжений, использованного в правиле Межсетевого экрана
ID сигнатуры	Идентификатор сигнатуры, которой соответствует трафик
Действие	Действие для трафика, определенное профилем
Контроль приложений	
ID	Идентификатор профиля Контроля приложений
Профиль	Название профиля Контроля приложений, использованного в правиле Межсетевого экрана
Действие	Действие для трафика, определенное профилем
Приложение	Приложение, действие для которого определено профилем
Протокол прикладного уровня	Протокол, к которому применяется действие, определенное профилем
Антивирус	
ID	Идентификатор профиля Антивируса
Профиль	Название профиля Антивируса
Источник	
IP-адрес	IP-адрес источника трафика
Порт	Порт источника трафика
Зона	Интерфейс или группа интерфейсов, из которых пришел трафик
Логин	Логин пользователя источника
Пользователь	Имя пользователя источника
Группа	Группа, в которую входит пользователь
Местоположение	Страна источника трафика (GeoIP)
Внешний IP-адрес	Внешний IP-адрес источника трафика
Назначение	

IP-адрес	IP-адрес назначения трафика
Порт	Порт назначения трафика
Зона	Интерфейс или группа интерфейсов, в которые вошел трафик
Логин	Логин пользователя назначения
Пользователь	Имя пользователя назначения
Группа	Группа, в которую входит пользователь
Местоположение	Страна назначения трафика (GeoIP)
DNAT	
ID	Идентификатор сработавшего правила таблицы DNAT
Новый IP назначения	IP-адрес, на который межсетевой экран поменял IP-адрес назначения
Новый порт назначения	Порт, на который межсетевой экран поменял Порт назначения
SNAT	
ID	Идентификатор сработавшего правила таблицы SNAT
Новый IP источника	IP-адрес, на который межсетевой экран поменял IP-адрес источника
Кластер	
ID	Идентификатор кластера, если кластер настроен на NGFW Novum
Название	Название кластера, если кластер настроен на NGFW Novum
VCE	
ID	Идентификатор VCE
Название	Название VCE

События безопасности

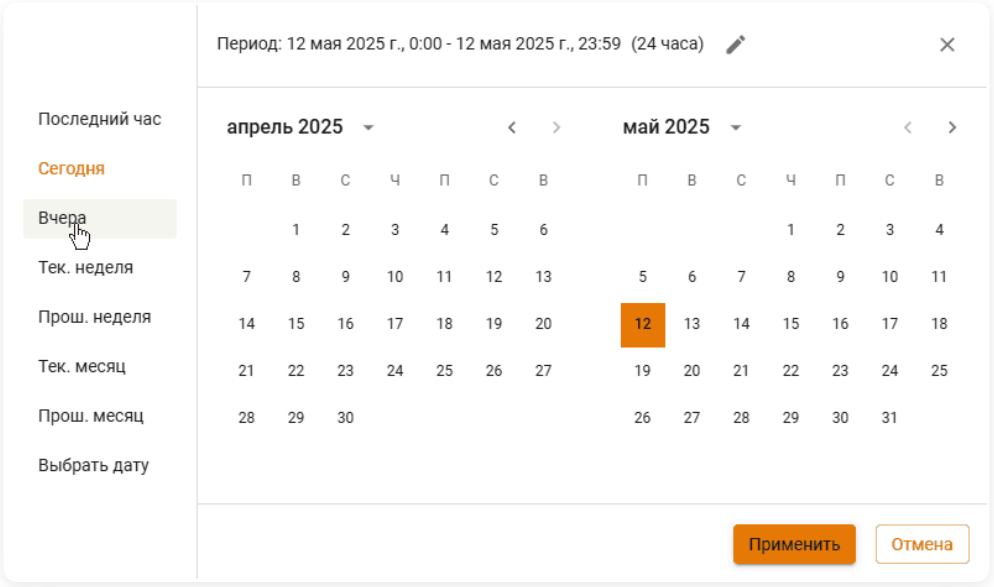
Классический контекст | Высокопроизводительный контекст | API

Все графики формируются в часовом поясе сервера.

В разделе **События безопасности** представлены события модулей WAF и IPS, а также графики событий IPS.

Выбор периода

Все отображаемые данные фильтруются по дате и времени. Например, выберите определенный временной период (по кнопке) или воспользуйтесь одним из предустановленных фильтров:



Если не выбран ни один фильтр по дате и времени, то по умолчанию устанавливается интервал **Сегодня** (Графики IPS) или **Последний час** (Журнал IPS, Web Application Firewall) в часовом поясе сервера.

Графики IPS

В этом разделе представлены графики, содержащие краткую информацию раздела **Предотвращение вторжений**. Подробные сведения обо всех срабатываниях правил **Предотвращение вторжений** можно найти на вкладке **Журнал IPS** в виде таблицы.

График Количество атак по уровню угрозы

Информация представлена в виде графика со значениями угрозы безопасности:

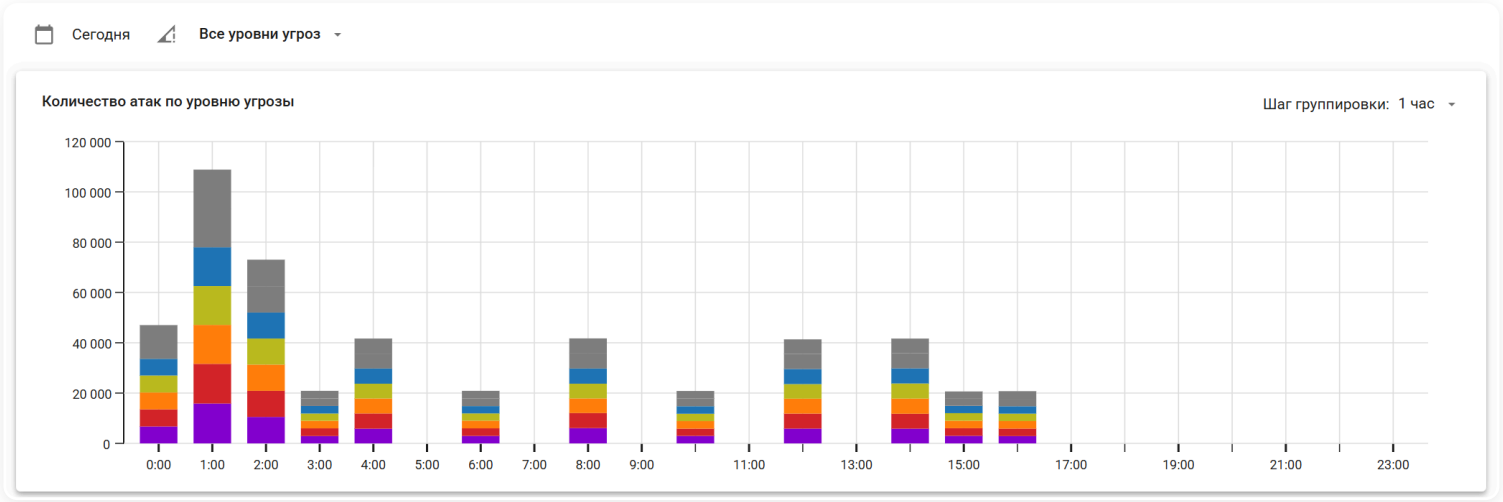
- **Не обнаружен** - уровень угрозы 0. Не удалось обнаружить уровень угрозы для сигнатуры
- **Критичный** - уровень угрозы 1
- **Опасный** - уровень угрозы 2
- **Незначительный** - уровень угрозы 3
- **Информационный** - уровень угрозы 4
- **Неопределенный** - уровень угрозы 255. Сигнатуры, явно не отнесенные ни к одной из категорий

Уровни угроз определяются в соответствии с характеристиками сигнатур в порядке убывания приоритета:

- Severity metadata - метаданные серьезности угрозы, явно заданные в сигнатуре. Если это поле присутствует, оно имеет наивысший приоритет при определении уровня угрозы.
- Priority - приоритет сигнатуры, указанный в ее описании. Используется, если поле Severity metadata отсутствует.
- Classtype - тип класса атаки (например, `trojan-activity` или `attempted-admin`). Используется для определения уровня угрозы, если ни Severity metadata, ни Priority не заданы.

Если нажать на уровень угрозы в правом списке, все графики будут отфильтрованы в соответствии с этим уровнем. Чтобы отменить фильтрацию, нажмите еще раз на выбранный уровень.

Пример графика **Количество атак по уровню угрозы**:



Описание дополнительных графиков

Топ атакованных адресов

В топ атакованных попадают как внешние, так и внутренние адреса. Один из примеров, когда атакованный адрес является внешним, - работа трояна изнутри защищаемой сети.

Топ заблокированных типов атак

График подсчитывает статистику типов атак (например, типы атак **Черный список IP-адресов** или **Попытки получения привилегий администратора**) по количеству срабатываний с этим типом атаки.

Топ внешних узлов по количеству блокировок

График содержит информацию о внешних адресах и количестве блокировок по ним.

Топ атакующих стран

Топ атакующих стран строится по IP-адресам, полученным при срабатывании правил в разделе **Предотвращение вторжений**. Если IP-адрес не геокодируется в наименование страны, адрес не будет отображается в виджете.

По этой причине локальные IP-адреса не отображаются в виджете.

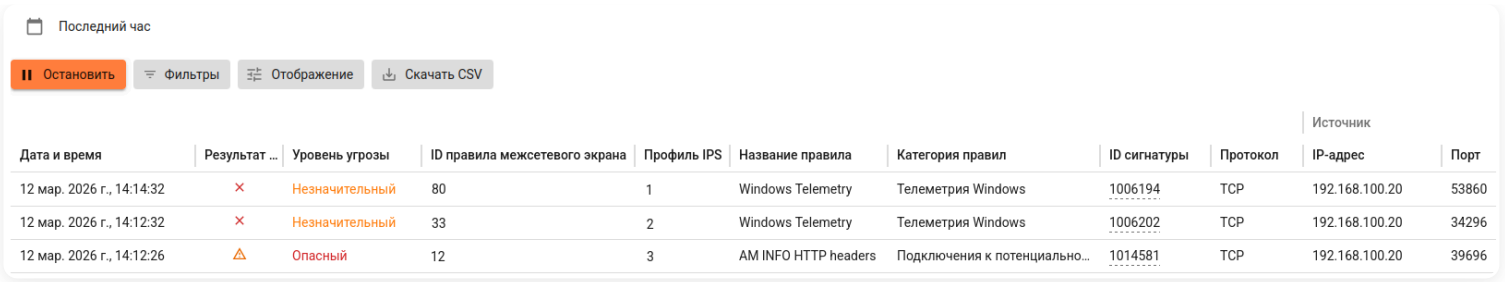
Топ подозрительных локальных узлов

Виджет отображает локальные IP-адреса, являющиеся источниками срабатываний правил системы **Предотвращение вторжений**. В топ попадают как авторизованные, так и неавторизованные пользователи, запросы которых блокировались. Если для IP-адреса не найдено соответствие с учетной записью пользователя, то имя пользователя отображаться не будет.

> Топ строится только по данным источника (src), данные назначения (dest) не учитываются. Источник локальный, если присутствует условие `src_ip_type == 'local'`.

Журнал IPS

В **Отчеты и журналы** → **События безопасности** → **Журнал IPS** можно просмотреть логи системы **Предотвращения вторжений**:



- Поле **Результат анализа** отображает действие системы:
  - `Blocked` - пакет блокирован.
  - Любая другая информация в этом поле - `Allowed`, информирование.
- В поле **Уровень угрозы** могут отображаться следующие значения:
  - **Критичный**
  - **Опасный**
  - **Незначительный**
  - **Информационный**
  - **Неопределенный**
  - **Не обнаружен**

Для проверки IP-адресов в столбцах **Источник** и **Назначение** скопируйте адрес и выполните его поиск в сервисе Whois.

Для корректного отображения информации из CSV-файла

1. Скачайте CSV-файл с логами системы **Предотвращения вторжений** за определенный период по соответствующей кнопке.

2. Откройте CSV-файл в MS Excel и выделите весь первый столбец.

3. Перейдите на вкладку **Данные** и нажмите кнопку **Текст по столбцам**.

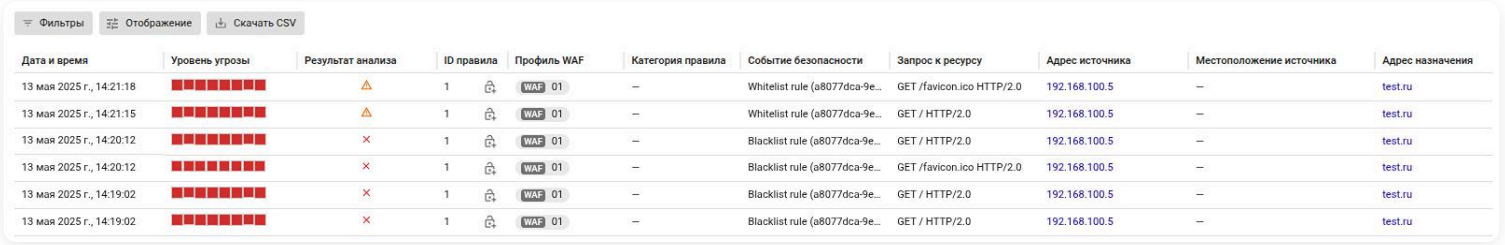
4. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:

5. В блоке **Символом-разделителем является:** выберите **запятая** и нажмите **Далее**:

6. В блоке **Формат данных столбца** выберите **Текстовый** и нажмите **Готово**:

Web Application Firewall

Вкладка **Отчеты и журналы** → **События безопасности** → **Web Application Firewall** содержит информацию о срабатывании правил Web Application Firewall в виде таблицы:



Для проверки IP-адресов в столбцах **Адрес источника** и **Адрес назначения** скопируйте адрес и выполните его поиск в сервисе Whois.

На вкладке **Web Application Firewall** отображается профиль WAF, параметры которого вызвали блокировку доступа к ресурсу.

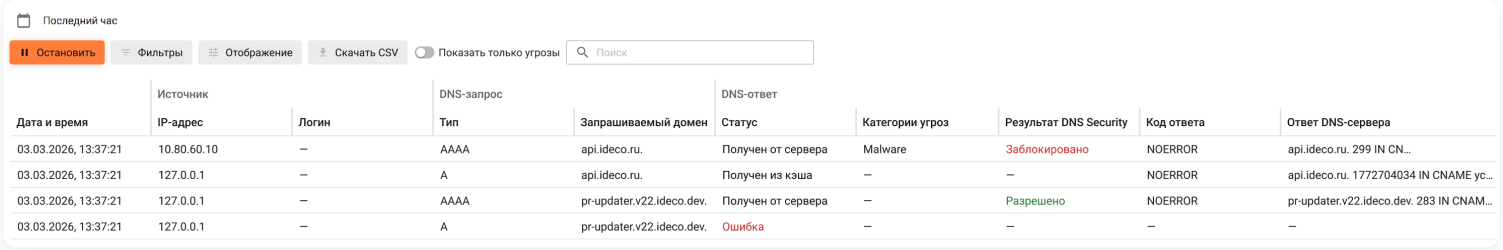
DNS-запросы

Классический контекст | Высокопроизводительный контекст | API

Время хранения данных в журнале **DNS-запросы** - 3 месяца.

В разделе отображается информация об обмене DNS-сообщениями, обработанными Ideco NGFW Novum при включенной опции **Логировать DNS-запросы** в **Сервисы → DNS → Внешние DNS-серверы**.

Журнал предназначен для анализа DNS-активности, выявления обращений к опасным и нежелательным доменам, а также просмотра DNS-запросов и результатов их обработки с привязкой к источнику:



Чтобы отрегулировать столбцы, отображаемые в таблице, воспользуйтесь кнопкой **Отображение**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**.

При включении опции **Показать только угрозы** в таблице остаются только те записи, у которых в столбце **Результат DNS Security** указано **Заблокировано**. Опция позволяет отфильтровать DNS-запросы, заблокированные сервисом DNS Security.

Описание столбцов

Столбец	Описание
	Общие
Дата и время	Дата и время записи в формате `ДД.ММ.ГГГГ, ЧЧ:ММ:СС`
	Источник
IP-адрес	IP-адрес источника DNS-запроса
Логин	Логин пользователя
Пользователь	Имя пользователя
Группа	Группа, в которую входит пользователь
	DNS-запрос
Код операции	Возможные значения: • QUERY - стандартный запрос • IQUERY - обратный запрос • STATUS - запрос состояния сервера • NOTIFY - уведомление вторичных серверов • UPDATE - динамическое обновление зоны
Класс	Класс запроса, определяющий тип сети: • IN (Internet) - основной класс • CH (Chaos) - для служебных или экспериментальных запросов • HS (Hesiod) - специальный класс для систем Hesiod

Тип	Тип DNS-запроса: • A (Address Record) - сопоставляет доменное имя с IPv4-адресом (например, example.com → 93.184.216.34) • AAAA (Quad-A Record) - сопоставляет доменное имя с IPv6-адресом (например, example.com → 2606:2800:220:1:248:1893:25c8:1946) • CNAME (Canonical Name Record) - перенаправляет одно доменное имя на другое (например, www.example.com → example.com) • MX (Mail Exchange Record) - указывает серверы, обрабатывающие почту для домена (например, example.com → mail.example.com) • TXT (Text Record) - содержит произвольный текст, часто используется для проверок (SPF, DKIM, DMARC) • NS (Name Server Record) - указывает DNS-серверы, отвечающие за домен (например, example.com → ns1.example.com) • SOA (Start of Authority) - содержит служебную информацию о зоне (первичный DNS-сервер, email администратора, TTL и другое) • PTR (Pointer Record) - используется для обратного DNS-запроса (например, 93.184.216.3 → example.com) • SRV (Service Record) - указывает серверы для определенных сервисов (например, SIP, XMPP) • CAA (Certification Authority Authorization) - определяет, какие центры сертификации могут выпускать SSL-сертификаты для домена
Протокол	Протокол соединения
Запрашиваемый домен	Доменное имя, указанное в DNS-запросе
Флаги	Свойства, отражающие особенности формирования и обработки запроса: • QR - запись является запросом • AA - авторитетный ответ, подтверждает, что сервер является авторитетным для зоны • TC - усеченный ответ, превышен размер пакета DNS • RD - рекурсия запрошена клиентом • RA - рекурсия доступна на сервере • Z - зарезервировано • AD - данные проверены DNSSEC, достоверность подтверждена • CD - проверка DNSSEC отключена
DNS-ответ	
Статус	Результат обработки DNS-запроса: • Получен от сервера - ответ на запрос получен от сервера • Получен из кэша - ответ на запрос сформирован из кэша • Ошибка - ошибка обработки
Результат DNS Security	Статус блокировки запроса сервисом DNS Security: • Заблокировано - домен заблокирован • Разрешено - категория угроз не найдена • Прочерк - сервис DNS Security был отключен при обработке запроса • Неизвестно - состояние сервиса DNS Security при обработке запроса неизвестно (значение для записей до версии NGFW Novum 21.1)
Категории угроз	Названия категорий из группы **Security**. Перечень категорий приведен в статье DNS security
Код ответа	Возможные значения: • NXDOMAIN - домен не существует • SERVFAIL - ошибка при обработке запроса сервером • REFUSED - сервер отклонил запрос • NOANSWER - нет данных для ответа • NOERROR - запрос обработан успешно • FORMERR - ошибка формата DNS-запроса • NOTIMPL - операция не поддерживается сервером • YXDOMAIN - домен уже существует (ошибка при создании или обновлении зоны) • YXRRSET - запись уже существует • NXRRSET - запись не существует • NOTAUTH - сервер не является авторитетным для зоны • NOTZONE - домен не относится к указанной зоне
Ответ DNS-сервера	Данные, возвращенные DNS-сервером в ответ на запрос (IP-адрес, имя сервера или иная информация)
Кластер	

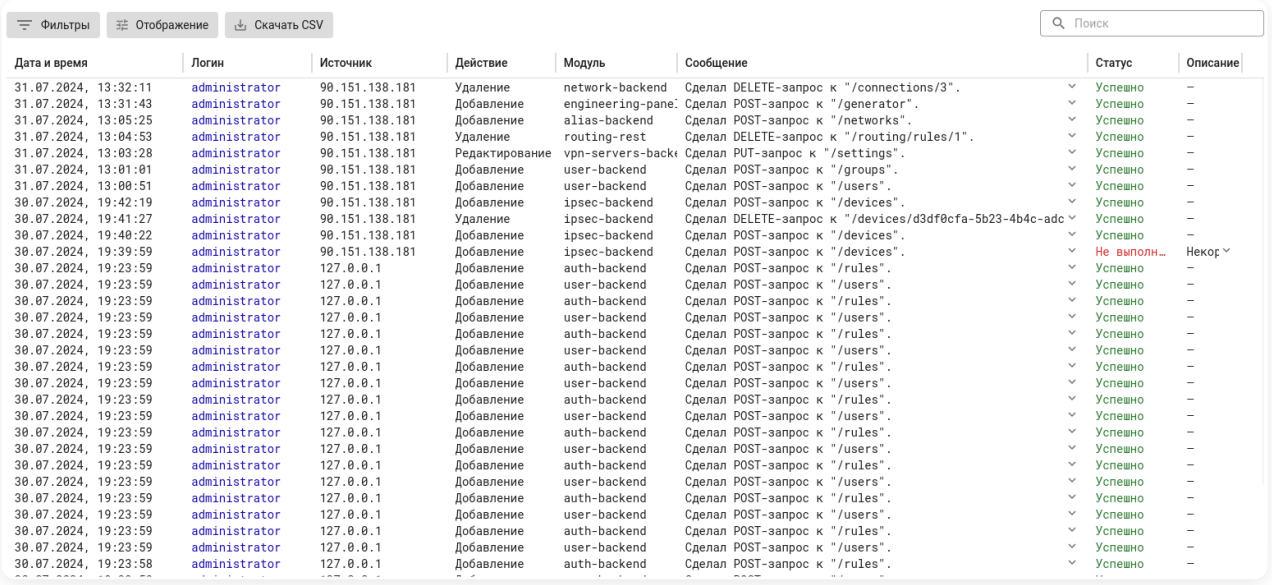
ID	Идентификатор кластера
Название	Название кластера
VCE	
ID	Идентификатор контекста
Название	Название контекста

Названия категорий в столбце **Категории угроз** отображаются при наличии лицензии сервиса **DNS-Security** и включенной опции в **Сервисы → DNS → Внешние DNS-серверы**.

Действия администраторов

Классический контекст | Высокопроизводительный контекст

Ideco NGFW Novum логирует действия администраторов, которые вносят изменения в конфигурацию NGFW Novum из веб-интерфейса, локального интерфейса и терминала. Действия, осуществляемые через локальное меню Ideco NGFW Novum, отображаются в журнале действий администраторов с источником `127.0.0.1`:



Дата и время	Логин	Источник	Действие	Модуль	Сообщение	Статус	Описание
31.07.2024, 13:32:11	administrator	90.151.138.181	Удаление	network-backend	Сделал DELETE-запрос к "/connections/3".	Успешно	–
31.07.2024, 13:31:43	administrator	90.151.138.181	Добавление	engineering-panel	Сделал POST-запрос к "/generator".	Успешно	–
31.07.2024, 13:05:25	administrator	90.151.138.181	Добавление	alias-backend	Сделал POST-запрос к "/networks".	Успешно	–
31.07.2024, 13:04:53	administrator	90.151.138.181	Удаление	routing-rest	Сделал DELETE-запрос к "/routing/rules/1".	Успешно	–
31.07.2024, 13:03:28	administrator	90.151.138.181	Редактирование	vpn-servers-backe	Сделал PUT-запрос к "/settings".	Успешно	–
31.07.2024, 13:01:01	administrator	90.151.138.181	Добавление	user-backend	Сделал POST-запрос к "/groups".	Успешно	–
31.07.2024, 13:00:51	administrator	90.151.138.181	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:42:19	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Успешно	–
30.07.2024, 19:41:27	administrator	90.151.138.181	Удаление	ipsec-backend	Сделал DELETE-запрос к "/devices/d3df0cfa-5b23-4b4c-adc	Успешно	–
30.07.2024, 19:40:22	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Успешно	–
30.07.2024, 19:39:59	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Не выполн…	Некор
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:58	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–

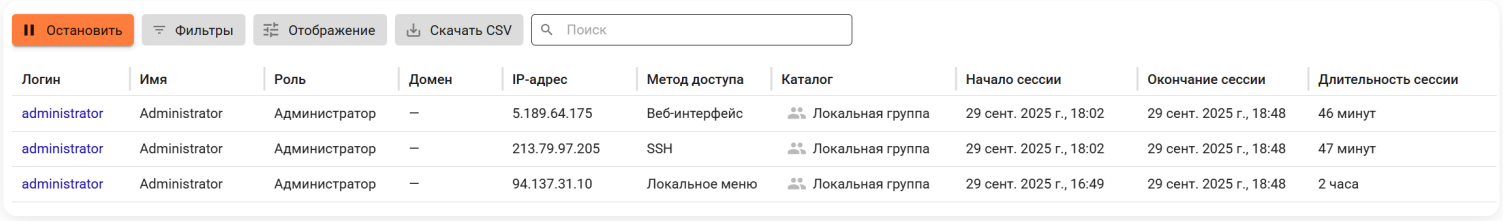
Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

При работе Ideco NGFW в режиме кластера логи действия администраторов не передаются резервной ноде.

Аутентификация администраторов

Классический контекст | Высокопроизводительный контекст

Время хранения данных в журнале **Аутентификация администраторов** составляет 1 год.



Логин	Имя	Роль	Домен	IP-адрес	Метод доступа	Каталог	Начало сессии	Окончание сессии	Длительность сессии
administrator	Administrator	Администратор	–	5.189.64.175	Веб-интерфейс	Локальная группа	29 сент. 2025 г., 18:02	29 сент. 2025 г., 18:48	46 минут
administrator	Administrator	Администратор	–	213.79.97.205	SSH	Локальная группа	29 сент. 2025 г., 18:02	29 сент. 2025 г., 18:48	47 минут
administrator	Administrator	Администратор	–	94.137.31.10	Локальное меню	Локальная группа	29 сент. 2025 г., 16:49	29 сент. 2025 г., 18:48	2 часа

Для поиска авторизованных администраторов нажмите **Фильтры** и укажите:

- В поле **Столбец** - требуемый параметр поиска.
- В последнем поле - значение.

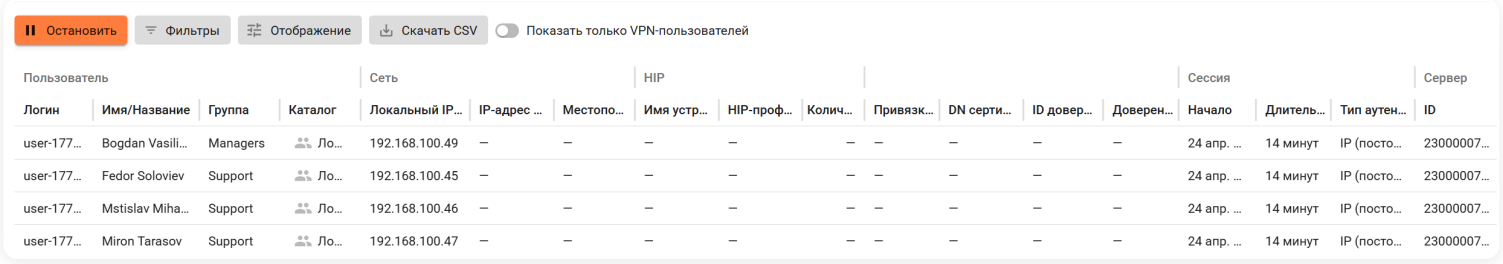
Особенности работы Журнала аутентификации администраторов

- Время жизни сессии администратора обновляется каждые 5 минут, поскольку происходит запись текущего времени в поле **Окончание сессии**. Если запрос на поиск будет отправлен до момента синхронизации буфера, то время окончания будет одно, в ином случае - другое.
- При завершении сессии администратора информация о разрыве сессии в журнале появляется сразу. Время окончания завершенной сесси больше не меняется.

Аутентификация пользователей

Классический контекст | Высокопроизводительный контекст | API

Время хранения данных в журнале **Аутентификации пользователей** составляет 180 дней.

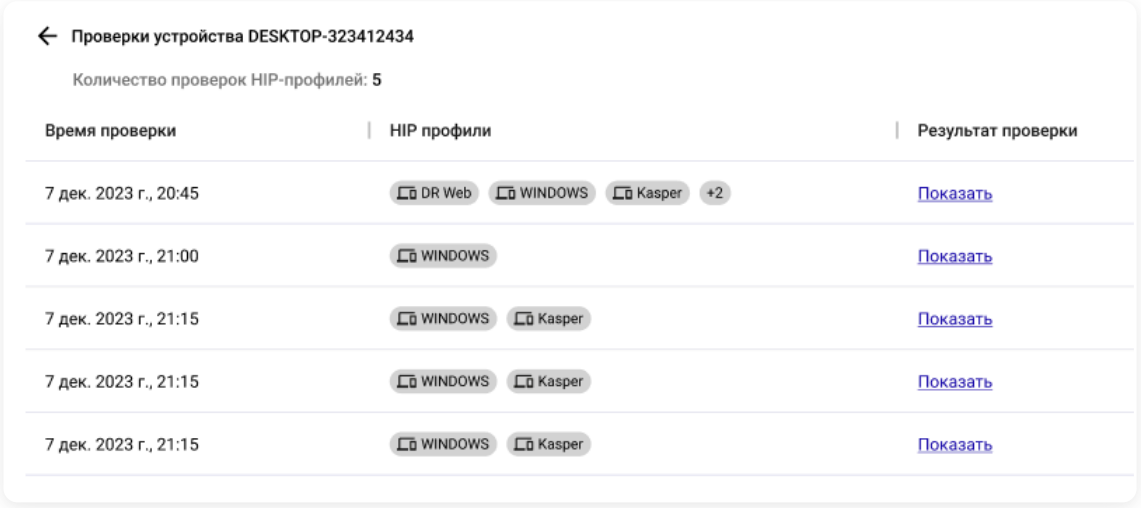


Для поиска авторизованных пользователей нажмите на **Фильтры**, укажите в поле **Столбец** требуемый параметр поиска и в последнем поле - значение.

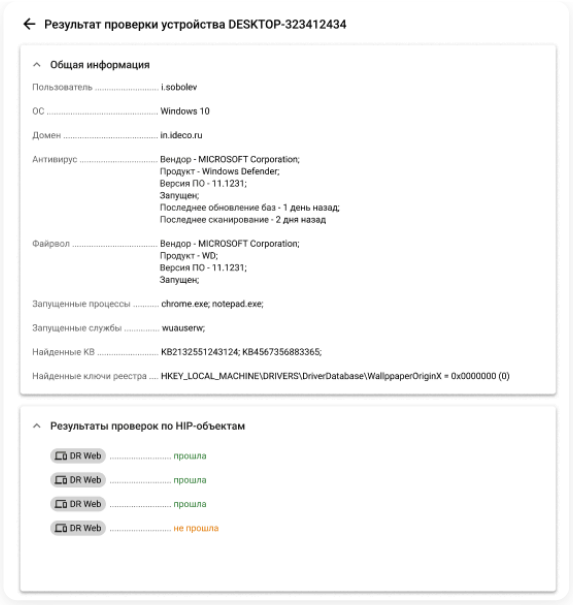
В столбце **Кол-во изменений профилей** указано количество изменений HIP-профилей, зафиксированных в результате проверок устройств, подключенных через Ideco Client. Изменения фиксируются при редактировании HIP-профиля в веб-интерфейсе или при смене профиля у устройств.

Для просмотра результатов проверок устройств, подключенных через Ideco Client, выполните действия:

1. Нажмите на число в столбце **Кол-во изменений профилей**. Откроется список проверок:



2. Нажмите **Показать** в столбце **Результат**, чтобы увидеть общую информацию и результат проверки по **HIP-объектам**:



Особенности работы Журнала аутентификации пользователей:

- Время окончания открытой сессии пользователя меняется каждые 5 минут, поскольку происходит запись текущего времени в поле **Окончание сессии**. Если запрос на поиск будет отправлен до момента синхронизации буфера, то время окончания будет одно, в ином случае - другое.
- Для завершенной сессии информация о времени закрытия не меняется.

Включение опции **Показать VPN-пользователей** отфильтрует в таблице журнала информацию обо всех VPN-сессиях по всем протоколам.

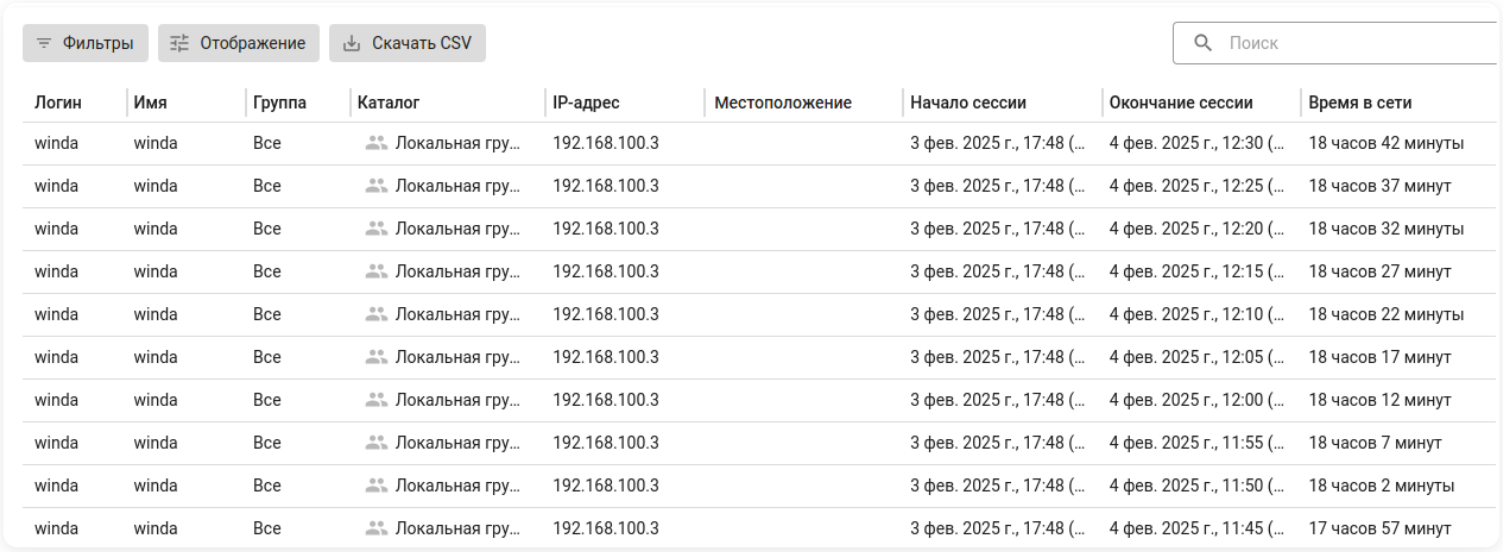
Аутентификация пользователей ЛК

Классический контекст | Высокопроизводительный контекст | API

Раздел представляет собой историю сессий пользователей, авторизованных в личном кабинете пользователя Ideco NGFW Novum.

Записи в журнале отображаются после настройки **Обратного прокси**. Технология SSL VPN используется пользователями для получения доступа к ресурсам в локальной сети через веб-браузер по HTTPS. При этом не устанавливается отдельное туннельное соединение.

Таблицу сессий можно скачать в формате CSV, воспользовавшись соответствующей кнопкой:



Логин	Имя	Группа	Каталог	IP-адрес	Местоположение	Начало сессии	Окончание сессии	Время в сети
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:30 (...	18 часов 42 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:25 (...	18 часов 37 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:20 (...	18 часов 32 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:15 (...	18 часов 27 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:10 (...	18 часов 22 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:05 (...	18 часов 17 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 12:00 (...	18 часов 12 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 11:55 (...	18 часов 7 минут
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 11:50 (...	18 часов 2 минуты
winda	winda	Все	Локальная гру...	192.168.100.3		3 фев. 2025 г., 17:48 (...	4 фев. 2025 г., 11:45 (...	17 часов 57 минут

Помимо общих сведений об учетной записи пользователя (логин, имя, группа и каталог), список сессий включает столбцы:

- **IP-адрес** - IP-адрес, с которого произведена аутентификация.
- **Местоположение** - страна IP-адреса, с которого произведена аутентификация. Значение пустое, если:
  - Отсутствует лицензия.
  - Невозможно получить базу GeoIP.
  - IP-адрес локальный.
- **Начало сессии** - момент запуска сессии с указанием даты в формате день/месяц/год и времени в формате час/минута.
- **Окончание сессии** - момент завершения сессии с указанием даты в формате день/месяц/год и времени в формате час/минута. Пустое значение, если сессия активна.
- **Время в сети** - продолжительность сессии с момента запуска.

Наличие столбцов в таблице регулируется кнопкой **Отображение**. По каждому столбцу доступна фильтрация и сортировка.

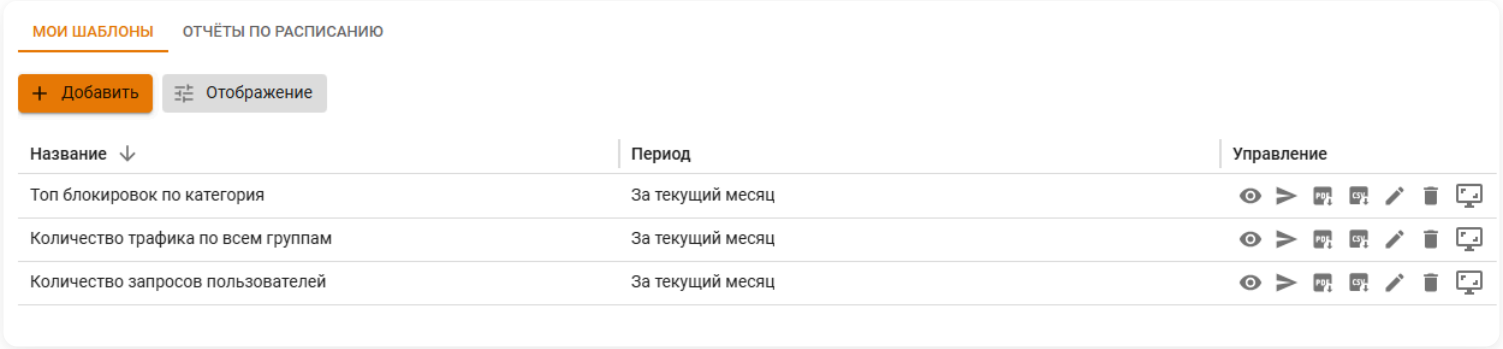
Для поиска нужной сессии воспользуйтесь одним из способов:

- Нажмите кнопку **Фильтры**, установите параметр поиска (все наименования доступных столбцов) и значение.
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Конструктор отчетов

Классический контекст | Высокопроизводительный контекст | API

В разделе **Отчеты и журналы** → **Конструктор отчетов** доступно создание шаблонов отчетов со статистическими данными и настройка автоматической отправки по email в форматах PDF и/или CSV по расписанию:



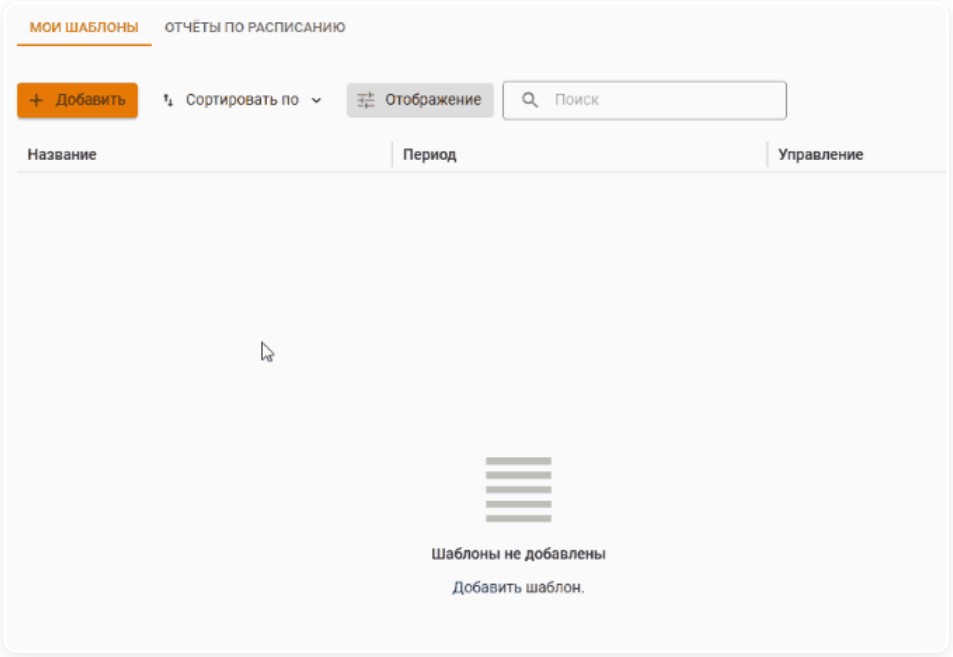
Ideco NGFW Novum хранит данные в течение определенного времени, по прошествии которого данные безвозвратно удаляются.

Сроки хранения данных по разделам:

- Система - 90 дней.
- Логи служб - 14 дней.
- Данные веб-трафика (Веб-трафик, а также посещенные сайты) - 1 месяц.
- События безопасности (Журнал IPS и Web application firewall) - 3 месяца.
- Действия администраторов и Аутентификация администраторов - 1 год.
- Аутентификация пользователей - 180 дней.

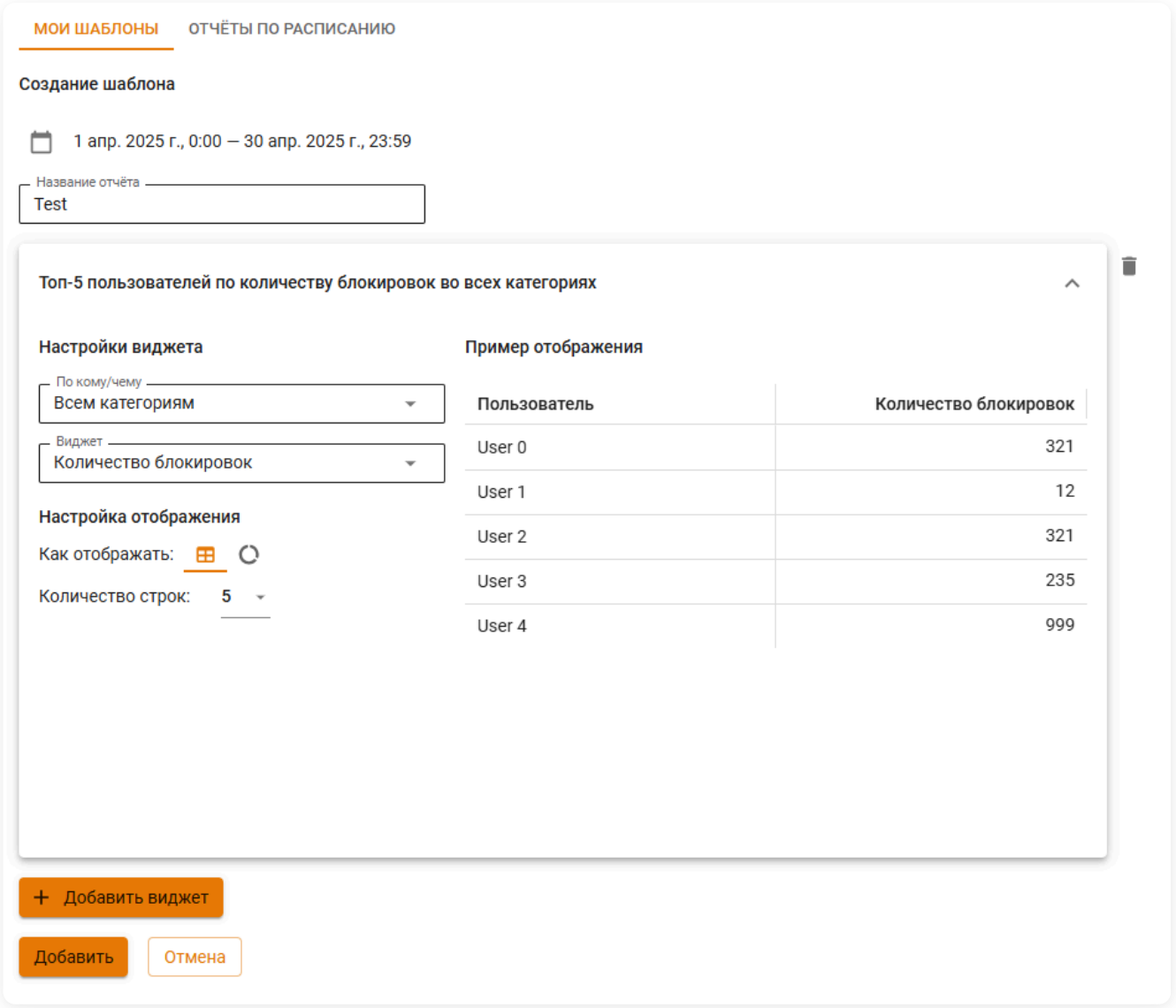
Создание шаблона

1. На вкладке **Мои шаблоны** нажмите **Добавить** и заполните поля:



- **Период** - укажите временной промежуток, за который следует сформировать отчет, из предложенных фильтров или укажите даты, нажав **Выбрать дату**.
- **Название отчета** - укажите название отчета.

2. Нажмите **Добавить виджет** и заполните поля:



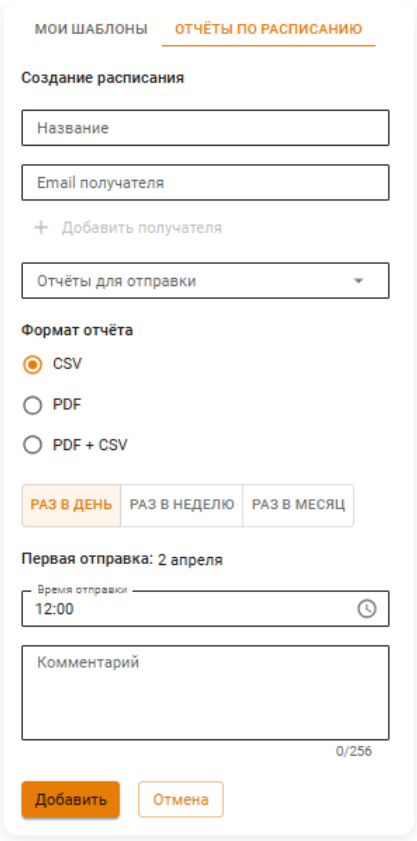
- **По кому/чему** - выберите объект, по которому будет собираться статистика. Если выбираете **Определенный** объект (например, ***Определенный пользователь*** или ***Определенная группа***), то появится дополнительное поле **Объекты**, где можно выбрать несколько объектов.
- **Виджет** - выберите, какую информацию хотите видеть по выбранному объекту. Один шаблон может содержать несколько виджетов. Некоторые виджеты позволяют настроить отображение данных в шаблоне отчета:
  - **Настройки отображения** - настройте, как должны отображаться данные в отчете.

3. Для сохранения шаблона нажмите **Добавить**.

Созданный шаблон можно редактировать, просмотреть в браузере, отправить на почту или скачать в формате PDF или CSV, нажав соответствующую кнопку в столбце **Управление**.

Настройка расписания

1. На вкладке **Отчеты по расписанию** нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Название** - укажите название расписания.
- **Email получателя** - укажите адрес электронной почты. Можно указать несколько почтовых адресов через кнопку **Добавить получателя**.
- **Отчеты для отправки** - выберите шаблон отчета для отправки.
- **Формат отчета** - выберите вариант формата для отправки отчета.
- **Периодичность рассылки отчетов**:
  - **Раз в день** - укажите время. Если при создании настройки время отправки меньше текущего на сервере, то отправка отчетов произойдет на следующий день.
  - **Раз в неделю** - укажите день и время отправки.
  - **Раз в месяц** - укажите необходимый день месяца. Если выбрано 31 число, но в месяце меньше дней, то выбирается последнее число месяца.
- **Комментарий** - произвольный текст, поясняющий назначение расписания отправки отчетов.
  Текст отображается только в Ideco NGFW Novum и не будет отправляться в отчетах.

2. Сохраните расписание, нажав **Добавить**.

3. Включите расписание, нажав на (по умолчанию выключено).

NGFW Novum сохранит все пользовательские настройки времени отправки во всех фильтрах (раз в день, раз в неделю и раз в месяц), но шаблон отчета будет отправляться автоматически после включения расписания и только в период, выбранный пользователем.

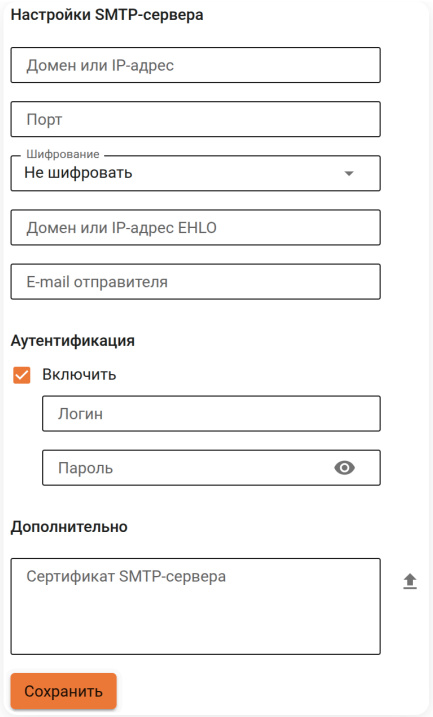
Если в таблице большое количество правил, воспользуйтесь кнопкой **Фильтры**:

Настройка отправки

1. На вкладке **Настройки отправки** выберите **Метод доставки**:

- **my.ideco.ru** - доставка писем с помощью MY.IDECO.
- **SMTP-сервер** - доставка писем с помощью SMTP-сервера.

При выборе метода **SMTP-сервер** заполните поля:



Расшифровка полей

Настройки SMTP-сервера:

- **Домен или IP-адрес** - домен или адрес SMTP-сервера, с помощью которого будут отправляться письма.
- **Порт** - порт SMTP-сервера.
- **Шифрование** - тип шифрования, используемый при соединении с SMTP-сервером. Доступные варианты: Не шифровать, TLS, STARTTLS.
- **Домен или IP-адрес EHLO** - домен или адрес, которые устройство указывает SMTP-серверу в команде EHLO.
- **E-mail отправителя** - адрес, от имени которого будут отправляться письма.

Аутентификация:

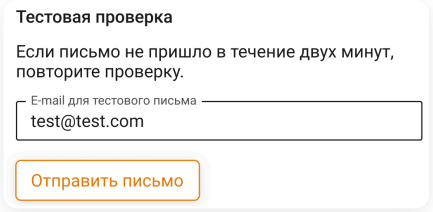
- **Включить** - при включении опции заполняются поля **Логин** и **Пароль** пользователя для аутентификации на SMTP-сервере.

Дополнительно:

- **Сертификат SMTP-сервера** - загрузка сертификата сервера. Используется, если SMTP-сервер применяет собственный сертификат и необходимо доверие со стороны Ideco NGFW Novum.

2. Нажмите **Сохранить**.

3. Для выполнения **Тестовой проверки** укажите e-mail получателя и нажмите **Отправить письмо**:



Пример настройки ежемесячного отчета

Необходимо настроить отправку отчета с информацией о заблокированных сайтах по всем пользователям. Периодичность - ежемесячно, каждое первое число месяца.

Создайте шаблон отчета, на основании которого будет собрана статистика для отправки:

1. Нажмите **Добавить** на вкладке **Мои шаблоны**.

2. Выберите временной период, за который следует сформировать отчет.

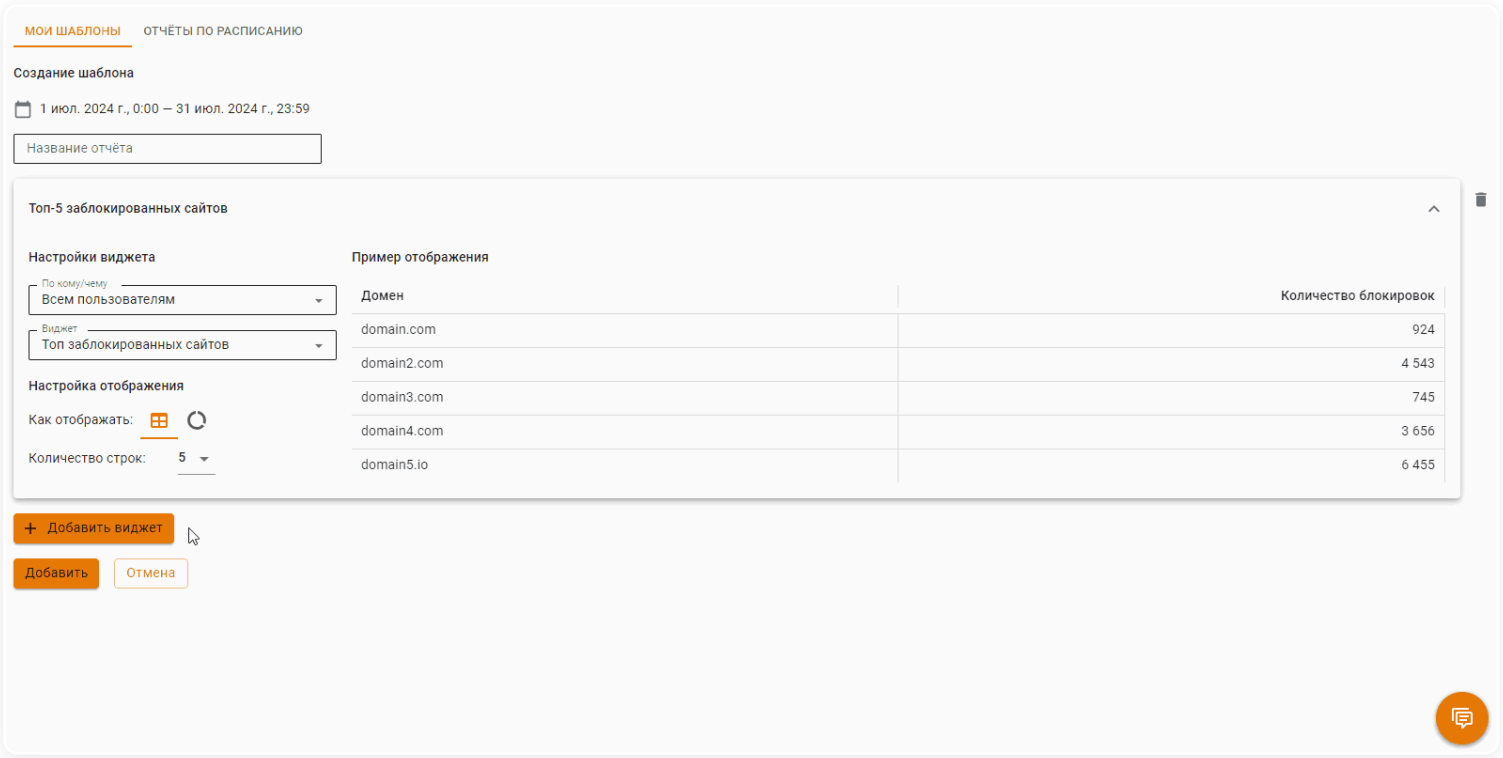
3. Укажите название в поле **Название отчета**.

4. Нажмите **Добавить виджет**.

5. Заполните поля:

- **По кому/чему** - выберите **Всем пользователям**.
- **Виджет** - выберите **Топ заблокированных сайтов**.

6. Укажите **Настройки отображения** в виде таблицы или круговой диаграммы:



7. Сохраните шаблон, нажав **Добавить**.

Создайте расписание, по которому шаблон отчета будет отправляться на электронную почту:

1. Нажмите **Добавить** на вкладке **Отчеты по расписанию**.

2. Заполните поля:

- **Название** - любое название, которое поможет идентифицировать правило расписания.
- **Email получателя** - электронная почта получателя отчета. Если нужно укажите дополнительные адреса, нажав **Добавить получателя**.

3. Выберите нужный шаблон в поле **Отчеты для отправки**.

4. Выберите формат, в котором хотите получать отчет.

5. Укажите настройки даты/дня и времени отправки отчета получателю (раз в месяц, каждый 1-й день месяца).

6. Сохраните расписание, нажав **Добавить**.

7. Включите расписание.

8. Перейдите на вкладку **Настройки отправки** и выберите **Метод доставки** отчета.

Управление сервером

Администраторы

Создание локальных администраторов, интеграция администраторов из сервисов Active Directory, ALD PRO, RADIUS

Перейти >

Ideco Center

Настройка интеграции Ideco NGFW к Ideco Center

Перейти >

VCE

Настройка VCE в Ideco NGFW, чтобы разделить одну локальную сеть на несколько независимых подсетей

Перейти >

Кластеризация

Настройка кластера, состоящего из двух серверов Ideco NGFW

Перейти >

Обновления

Настройка параметров автоматического обновления в Ideco NGFW

Перейти >

Бэкапы

Процесс создания и восстановления бэкапа Ideco NGFW

Перейти >

Терминал

Терминал для диагностики проблем на Ideco NGFW

Перейти >

Лицензия

Онлайн- Офлайн-привязка лицензии к серверу Ideco NGFW

Перейти >

Дополнительно

Настройка часового пояса и сбор анонимной статистики

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Администраторы

Классический контекст | Высокопроизводительный контекст | API

В Ideco NGFW Novum можно создать локальных администраторов или интегрировать администраторов из сервисов Active Directory, ALD PRO, FreeIPA, RADIUS.

При обновлении на версию 21 убедитесь, что логины локальных администраторов соответствуют требованиям:

- Не начинаются с цифры.
- Не содержат специальных и пробельных символов, кроме дефиса `-`.
- **Длина логина** - от 1 до 31 символа включительно.

Учетные записи администраторов, чьи логины не соответствуют требованиям, будут отключены.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока администратор будет автоматически деавторизован.

Сведения об авторизованных администраторах представлены в **Отчеты и журналы** → **Аутентификация администраторов** и **Сессии администраторов**.

Роли администраторов

Роль	Возможности
Администратор	• Полный доступ ко всем настройкам NGFW Novum, возможность создания новых настроек, правил, учетных записей других пользователей NGFW Novum, а также редактирования, управления и удаления их • Создание пользователей с правами администратора
Только просмотр	• Полный доступ к просмотру всех настроек NGFW Novum без возможности создания новых настроек, правил, учетных записей других пользователей NGFW Novum, а также редактирования, управления и удаления их

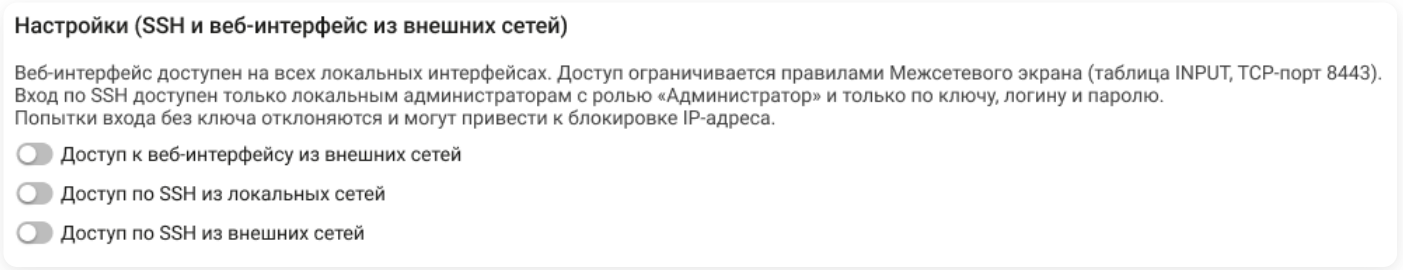
Администратор ИБ	• Выбор событий безопасности, подлежащих регистрации в журнале **События безопасности**
	• Чтение журнала **События безопасности**
	• Настройка параметров выгрузки информации о событиях безопасности, зарегистрированных в NGFW Novum
	• Формирование отчетов в формате `.csv` с учетом заданных критериев отбора и выгрузка их из журнала событий безопасности NGFW Novum
	• Настройка и получение оповещений в веб-интерфейсе NGFW Novum в случае:
	  ◦ выявления признаков вредоносного программного обеспечения в передаваемых файлах
	  ◦ выявления сетевого трафика, в котором обнаружен признак компьютерной атаки
	• Получение уведомлений о непройденной проверке контрольных сумм

Администратор межсетевого экрана	• Создание учетных записей других пользователей NGFW Novum.
	• Управление учетными записями пользователей NGFW Novum, в том числе возможность создания, изменения или удаления идентификаторов, а именно: логин пользователя, имя пользователя, IP-адрес пользователя, MAC-адрес пользователя, телефон пользователя
	• Назначение полномочий пользователям NGFW Novum, определяемых их ролями
	• Определение периода неактивности пользователя, по истечении которого сессия пользователя будет завершена (10 минут, 15 минут, 30 минут, 1 час, 2 часа, 8 часов, 12 часов, 1 день)
	• Установка правил фильтрации, позволяющих настроить разрешение или запрет (блокирование) прохождения сетевого трафика с использованием атрибутов фильтрации сетевого трафика, а также результатов обнаружения компьютерных атак и вредоносного программного обеспечения
	• Изменение и удаление правил фильтрации NGFW Novum
	• Применение правил фильтрации к:
	  ◦ сетевым интерфейсам NGFW Novum
	  ◦ идентифицированным пользователям NGFW Novum
	  ◦ идентифицированным приложениям, используемым при сетевом взаимодействии
	• Управление приоритетами применения правил фильтрации
	• Включение и отключение отдельных правил фильтрации при настройке анализа сетевого трафика на наличие признаков компьютерных атак
	• Установка собственных правил фильтрации при настройке анализа сетевого трафика на наличие признаков компьютерных атак
	• Управление режимами работы NGFW Novum
	• Изменение конфигурации NGFW Novum
	• Тестирование NGFW Novum

Администратор настройки доступов	• Создание учетных записей других пользователей NGFW Novum • Управление учетными записями пользователей NGFW Novum, в том числе возможность создания, изменения или удаления идентификаторов, а именно: логин пользователя, имя пользователя, IP-адрес пользователя, MAC-адрес пользователя, телефон пользователя • Назначение полномочий пользователям NGFW Novum, определяемых их ролями • Определение периода неактивности пользователя, по истечении которого сессия пользователя будет завершена (10 минут, 15 минут, 30 минут, 1 час, 2 часа, 8 часов, 12 часов, 1 день) • Создание, управление и удаление правил в разделах **Обратный прокси**, **Сертификаты**, **Почтовый релей** и **Ограничение скорости**
Просмотр отчетов	• Просмотр отчетов для следующих журналов: **Трафик**, **Система**, **Веб-трафик**, **Межсетевой экран**, **События безопасности**, **Аутентификация пользователей** и **Аутентификация пользователей ЛК**
Создание отчетов	• Просмотр, настройка и выгрузка отчетов в формате `.csv` для следующих журналов: **Трафик**, **Система**, **Веб-трафик**, **Межсетевой экран**, **События безопасности**, **Аутентификация пользователей**, **Аутентификация пользователей ЛК** и **Конструктор отчетов**

Доступ к веб-интерфейсу из внешней сети и удаленный доступ по SSH

Для настройки перейдите в **Управление сервером** → **Администраторы** → **Настройки**:



- **Доступ к веб-интерфейсу из внешней сети** - включите опцию для получения доступа к Ideco NGFW Novum из внешней сети. Это позволяет администрировать Ideco NGFW Novum удаленно. Попытки подбора паролей блокируются автоматически.
- **Доступ по SSH из локальных сетей** - включите для получения доступа к Ideco NGFW Novum по SSH из локальной сети (порт 22 TCP). Попытки подбора паролей блокируются автоматически.
- **Доступ по SSH из внешних сетей** - включите для получения доступа к Ideco NGFW Novum по SSH из внешних сетей (порт 22 TCP). Попытки подбора паролей блокируются автоматически.

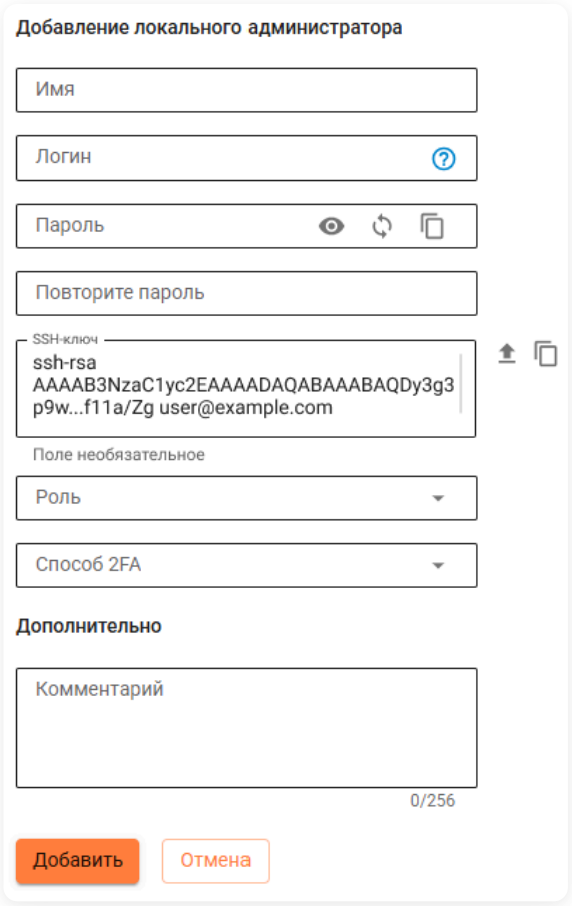
Подробнее о настройке подключения к веб-интерфейсу при удаленном доступе смотрите в статье Удаленный доступ для управления сервером.

Управление локальными администраторами

Чтобы добавить нового локального администратора выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **Администраторы** → **Локальные** и нажмите **Добавить**.

2. Заполните поля:



- **Имя** - введите имя нового администратора. Значение не должно быть длиннее 42 символов.
- **Логин** - введите логин нового администратора. Значение не должно начинаться с цифры, содержать специальные и пробельные символы, кроме дефиса `-`. Длина логина - от 1 до 31 символа.
- **Пароль/повторите пароль** - введите пароль нового администратора. Требования к паролю:
  - Минимальная длина пароля - 12 символов.
  - Содержит строчные и заглавные латинские буквы.
  - Содержит цифры.
  - Содержит специальные символы (! # $ % & ' * + и другие).
- **SSH-ключ** - вставьте SSH-ключ. Должна быть включена хотя бы одна из опций доступа по SSH.
- **Роль** - выберите роль.
- **Способ 2FA** - выберите второй фактор для авторизации администратора. Доступны TOTP-токен и RADIUS 2FA, настраиваемые на вкладке **Двухфакторная аутентификация**.

3. Нажмите **Добавить**.

Чтобы изменить имя и пароль администратора, нажмите  в столбце **Управление**.

Подробнее о восстановлении пароля администратора смотрите в статье по ссылке.

Если в таблице большое количество администраторов, воспользуйтесь кнопкой **Фильтры**.

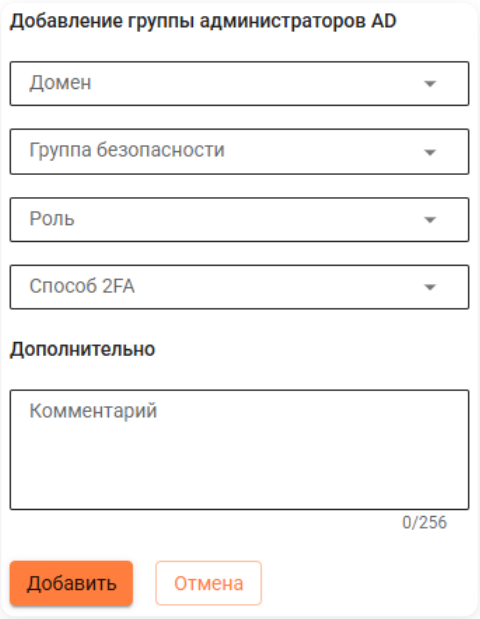
Управление AD/ALD/FreeIPA администраторами

Чтобы добавить администраторов, необходимо ввести NGFW Novum в домен Active Directory. При удалении домена AD/ALD/FreeIPA из Ideco NGFW Novum будут удалены сессии администраторов.

Чтобы интегрировать администраторов Active Directory, ALD Pro или FreeIPA с Ideco NGFW Novum, выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **Администраторы**, выберите нужную вкладку и нажмите **Добавить**.

2. Заполните поля:



- **Домен** - выберите доменное имя.
- **Группа безопасности** - выберите созданную группу безопасности.
- **Роль** - выберите роль. Роли AD/ALD/FreeIPA администраторов идентичны ролям локальных администраторов.
- **Способ 2FA** - выберите второй фактор для авторизации администратора. Доступны TOTP-токен и RADIUS 2FA, настраиваемые на вкладке **Двухфакторная аутентификация**.

3. Нажмите **Добавить**.

Особенности работы:

- Если администратор был авторизован по правилу или группе безопасности, которые были удалены, то сессия администратора будет удалена. Это произойдет только после синхронизации групп безопасности на Ideco NGFW Novum, которая выполняется каждые 5 минут.
- Если администратора исключить из группы безопасности, то администратор не будет удален сразу. Сессия завершится через некоторое время, и при следующей попытке авторизации администратор не сможет войти в систему.
- Если администратор соответствует нескольким правилам при авторизации, например, входит в несколько выбранных групп безопасности, ему будет отказано в доступе. Это необходимо, чтобы избежать проблем в определении прав доступа для администратора.

Управление RADIUS-администраторами

Особенности настройки RADIUS-сервера

В Ideco NGFW Novum используется **Vendor Code** 39410. Для авторизации через RADIUS укажите атрибуты:

```
ATTRIBUTE   Ideco-Administrator-Role           30  string
ATTRIBUTE   Ideco-Administrator-Name           31  string
```

`Ideco-Administrator-Role` обязателен для авторизации, а `Ideco-Administrator-Name` опционален. Атрибуты передают ID роли и ФИО администратора соответственно. Роли RADIUS-администраторов идентичны ролям локальных администраторов.

ID роли администраторов

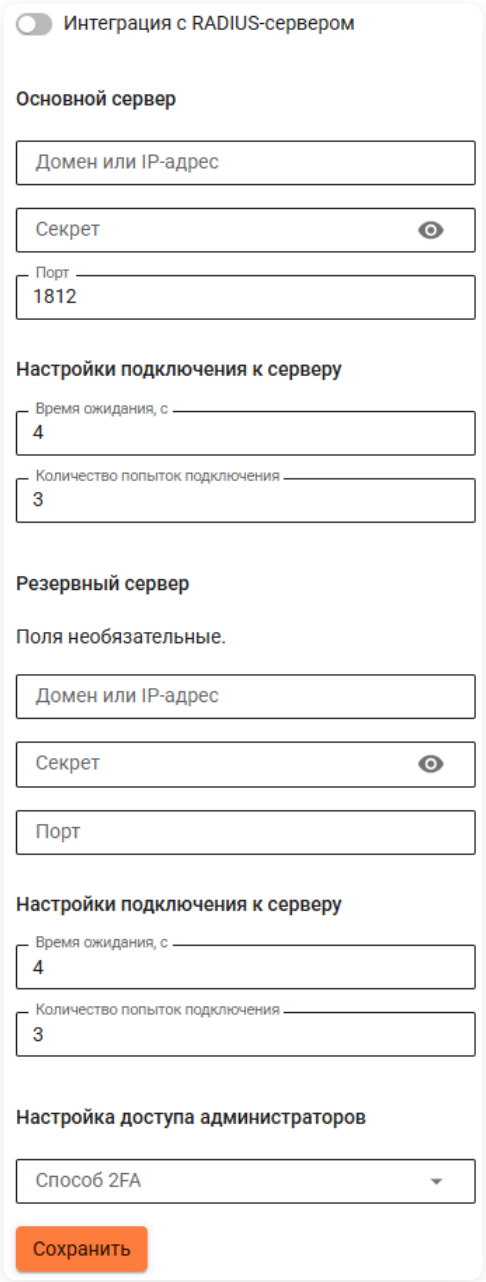
- `predefined_admin_write` - Администратор.
- `predefined_admin_readonly` - Только просмотр.
- `predefined_security_admin` - Администратор информационной безопасности.
- `predefined_firewall_admin` - Администратор межсетевого экрана.

- `predefined_access_settings_admin` - Администратор настройки доступов.
- `predefined_reports_view` - Просмотр отчетов.
- `predefined_reports_change` - Создание отчетов.

Интеграция администраторов RADIUS с Ideco NGFW Novum

Выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **Администраторы** → **RADIUS** и включите опцию **Интеграция с RADIUS-сервером**:



2. Укажите параметры соединения для основного RADIUS-сервера:

- **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
- **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
- **Порт** - порт, по которому будет происходить подключение к серверу. Поменяйте при необходимости.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию 4.
  - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию 3.
- **Способ 2FA** - выберите второй фактор для авторизации администратора. Доступны TOTP-токен и RADIUS 2FA, настраиваемые на вкладке **Двухфакторная аутентификация**.

3. При наличии в сети двух RADIUS-серверов настройте резервный с указанием порта подключения. При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.

4. Нажмите **Сохранить**.

Особенности удаления администраторов

- Если администратора удалить из раздела **Администраторы**, то сессия будет автоматически завершена, и администратор потеряет доступ к веб-интерфейсу.
- Если администратора удалить из группы безопасности, то сессия будет автоматически завершена через 24 часа после авторизации.

Чтобы удалить администратора, нажмите напротив нужной учетной записи. Можно удалить и собственный аккаунт.

Не рекомендуем удалять или отключать всех администраторов с ролью **Администратор**, это приведет к тому, что доступ к настройке Ideco NGFW Novum будет потерян. Если это произошло, обратитесь в Техническую поддержку.

Аутентификация администраторов

Ideco NGFW Novum не только блокирует попытки авторизации с неправильными логином или паролем, но и обнаруживает случаи, когда не удается получить информацию об администраторе из контроллера домена.
Если администратор не соответствует ни одному из правил авторизации, Ideco NGFW Novum считает попытку авторизации неудачной.
Доступ блокируется, если количество неудачных попыток превышает шесть, а для версии ФСТЭК - четыре.

Чтобы получить доступ к веб-интерфейсу Ideco NGFW Novum, администратору нужно выполнить процедуру аутентификации, указав логин и пароль.

Для разных групп администраторов предусмотрены разные логины:

- **Локальный администратор** - логин в формате `User`.
- **AD/ALD администратор** - логин в формате `User@test.com`, где `test.com` домен.
- **RADIUS администратор** - логин в формате `User@radius`, где `@radius` обязательная часть логина.

Двухфакторная аутентификация администраторов

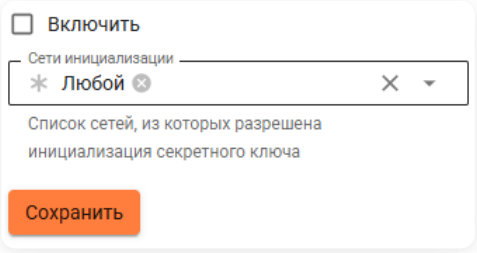
Для настройки двухфакторной аутентификации для администраторов перейдите в **Управление сервером → Администраторы → Двухфакторная аутентификация**. Для администраторов доступны два способа двухфакторной аутентификации:

- **TOTP-токен** - сканирование QR-кода или ручной ввод ключа (доступен только один токен).
- **RADIUS-серверы** - через RADIUS-серверы (может быть несколько).

Выберите необходимую вкладку:

TOTP-токен

Настройте использование TOTP-токена:



- **Включить** - опция активирует этот способ аутентификации.
- **Сети инициализации** - список сетей, из которых разрешена инициализация секретного ключа.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW Novum с использованием TOTP-токена смотрите по ссылкам:

- Rutube
- Youtube

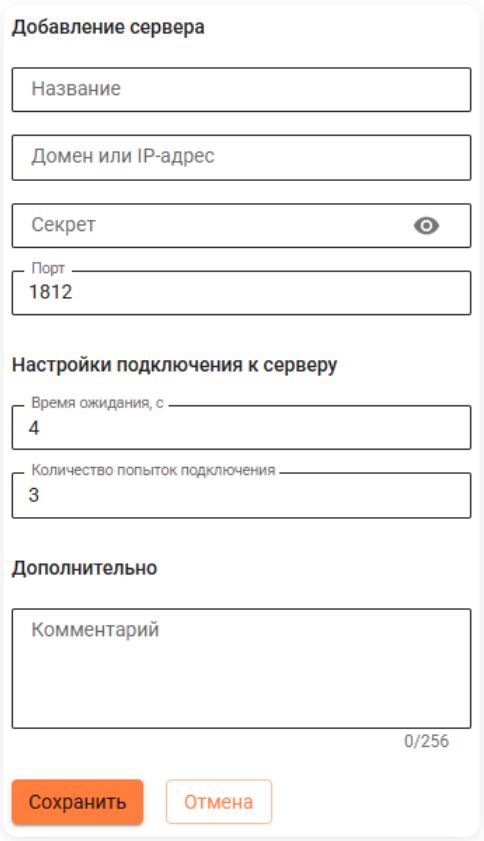
- docs.ideco.ru

RADIUS-сервер

При необходимости можно настроить несколько RADIUS-серверов для двухфакторной аутентификации. Для каждого сервера выполните шаги:

1. Нажмите **Добавить**.

2. Заполните поля:



- **Название** - уникальное название способа 2FA, которое будет использоваться в настройке доступа. Запрещены названия `TOTP-токен`, `Мультифактор` и `SMS Aero`.
- **Домен или IP-адрес** - домен или адрес внутреннего RADIUS-сервера.
- **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера.
- **Порт** - порт, по которому будет происходить подключение к серверу.
- **Настройки подключения к серверу**:
  - **Время ожидания, с** - время ожидания ответа от RADIUS в секундах. В диапазоне от 3 до 120. По умолчанию `4`.
  - **Количество попыток подключения** - число переподключений для RADIUS-сервера. В диапазоне от 1 до 5. По умолчанию `3`.
- **Комментарий** - необязательное поле.

3. Нажмите **Сохранить**.

Реестр 2FA

На вкладке отображаются все администраторы (локальные, AD, ALD, RADIUS) с инициализированным TOTP-токеном.

Если требуется сбросить TOTP-токен администратора (например, при потере телефона), нажмите напротив соответствующей записи:

Фильтры | Отображение | Поиск

ID	Логин	Имя	Домен	Каталог	Управление
43e4ed4c-832b-40c9-b8bd-ec9e4f…	z3vs101	Алексей	AD in.ideco	AD Active Directory	
78b43d57-5d0a-4681-8d6c-775bb…	i.petr0v14	Иван	AD in.ideco	ALD ALD Pro	
c078e196-1218-4cac-a0bf-b1a6d9…	-	-	AD in.ideco	RAD RAD	
c5dc4ef5-8067-4ec7-850d-03c143…	jup1ter	Константин	AD in.ideco	Локальные	

Удаленный доступ к серверу

Доступ по SSH к локальному меню сервера

Для подключения по SSH из внешних или локальных сетей выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы**.

2. Активируйте необходимую настройку:

- **Доступ по SSH из внешних сетей**.
- **Доступ по SSH из локальных сетей**.

3. Подключитесь к серверу с помощью любого SSH-клиента (для Windows, например, PuTTY), используя 22 порт. Необходимо указать логин и пароль **Администратора**.

4. Используйте `ideco-local-menu --debug` для доступа к локальному меню или `ls` для вывода каталогов текущей директории.

Пример подключения при помощи OpenSSH через консоль:

```
[test@My-PC home]$ ssh admin@192.168.100.183
admin@192.168.100.183's password:
Last login: Wed Sep  6 11:51:38 2023 from 192.168.100.1
[admin@localhost ~]#
```

Доступ к веб-интерфейсу сервера из интернета

Доступ из внешней сети:

- Включите функцию **Доступ к веб-интерфейсу из внешней сети** в **Управление сервером** → **Администраторы**. Для доступа введите внешний IP-адрес Ideco NGFW Novum и порт 8443.

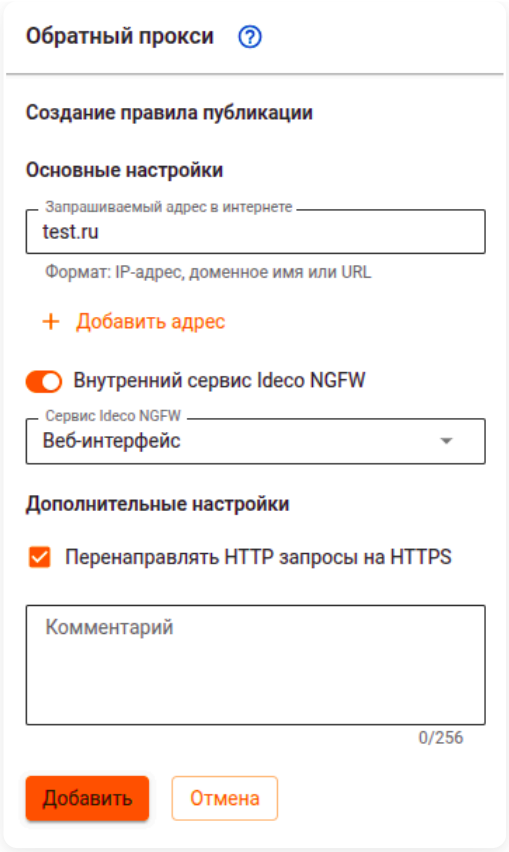
Доступ по VPN:

- Создайте VPN-подключение к серверу, например, по IKEv2 или SSTP. После подключения перейдите в веб-интерфейс по IP-адресу любого локального интерфейса с указанием порта 8443 (в том числе по IP-адресу из диапазона для VPN-подключений. Адрес по умолчанию - 10.128.0.1).

Публикация через обратный прокси:

1. Перейдите в **Сервисы** → **Обратный прокси**.

2. Добавьте новое правило, заполнив поля:



3. Укажите в качестве запрашиваемого адреса IP-адрес, доменное имя или URL, который будет запрашиваться пользователями.

4. Нажмите **Добавить** и перейдите по одному из адресов, которые были указаны в поле **Запрашиваемый адрес в интернете**.

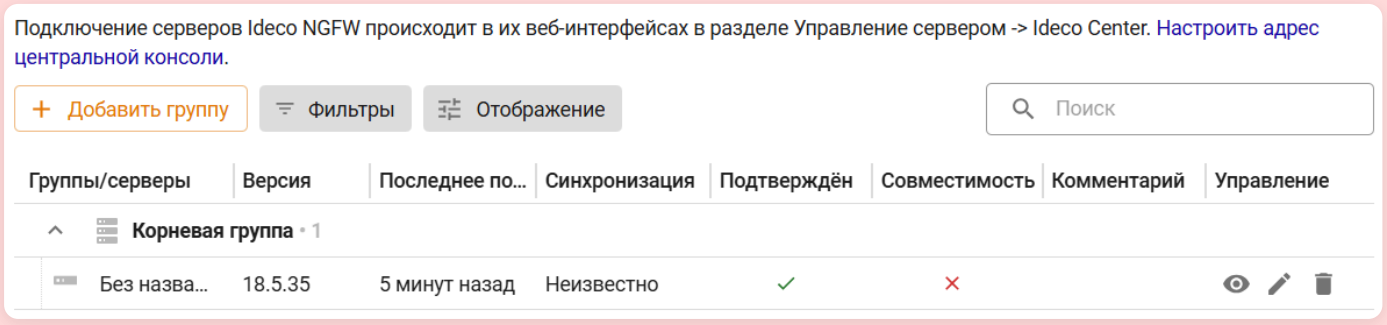
Ideco Center

Классический контекст | Высокопроизводительный контекст | API

Ideco Center - центральная консоль, помогающая в администрировании нескольких серверов Ideco NGFW Novum. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW Novum.

Подключение Ideco NGFW Novum к Ideco Center

При синхронизации Ideco Center и Ideco NGFW Novum с разными мажорными версиями передача правил с Ideco Center происходить не будет. При этом в разделе **Серверы** будет информация о том, что Ideco Center и Ideco NGFW Novum несовместимы:

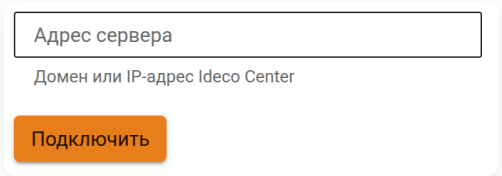


Особенности работы:

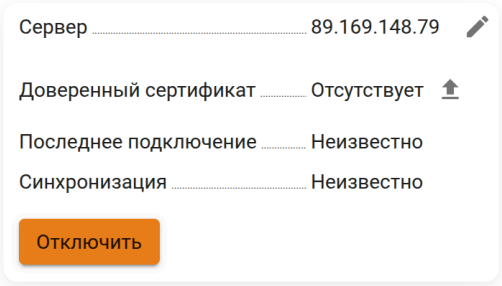
- Сетевое подключение производится в направлении от Ideco NGFW Novum к Ideco Center, т. е. возможна связь и когда Ideco NGFW Novum за NAT.
- Если сервер Ideco Center находится за NAT, в Ideco Center укажите IP-адрес NAT-устройства или доменное имя в **Управление сервером → Дополнительно → Адрес Ideco Center**.
- Для синхронизации базы данных отчетов и журналов между серверами используется WireGuard.
- Для остальных коммуникаций между серверами используется WebSocket.
- Соединение между серверами шифруется по протоколу TLS 1.3. Старые версии протокола (TLS 1.0, TLS 1.1, TLS 1.2) отключены.

1. Перейдите в **Управление сервером → Ideco Center**.

2. Введите IP-адрес или доменное имя в поле **Адрес сервера** и нажмите **Подключить**:

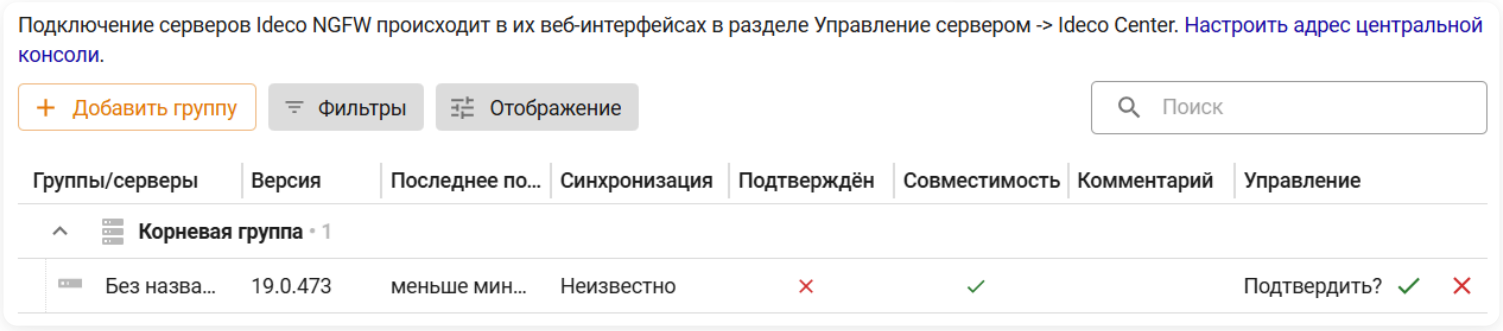


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW Novum или VCE:

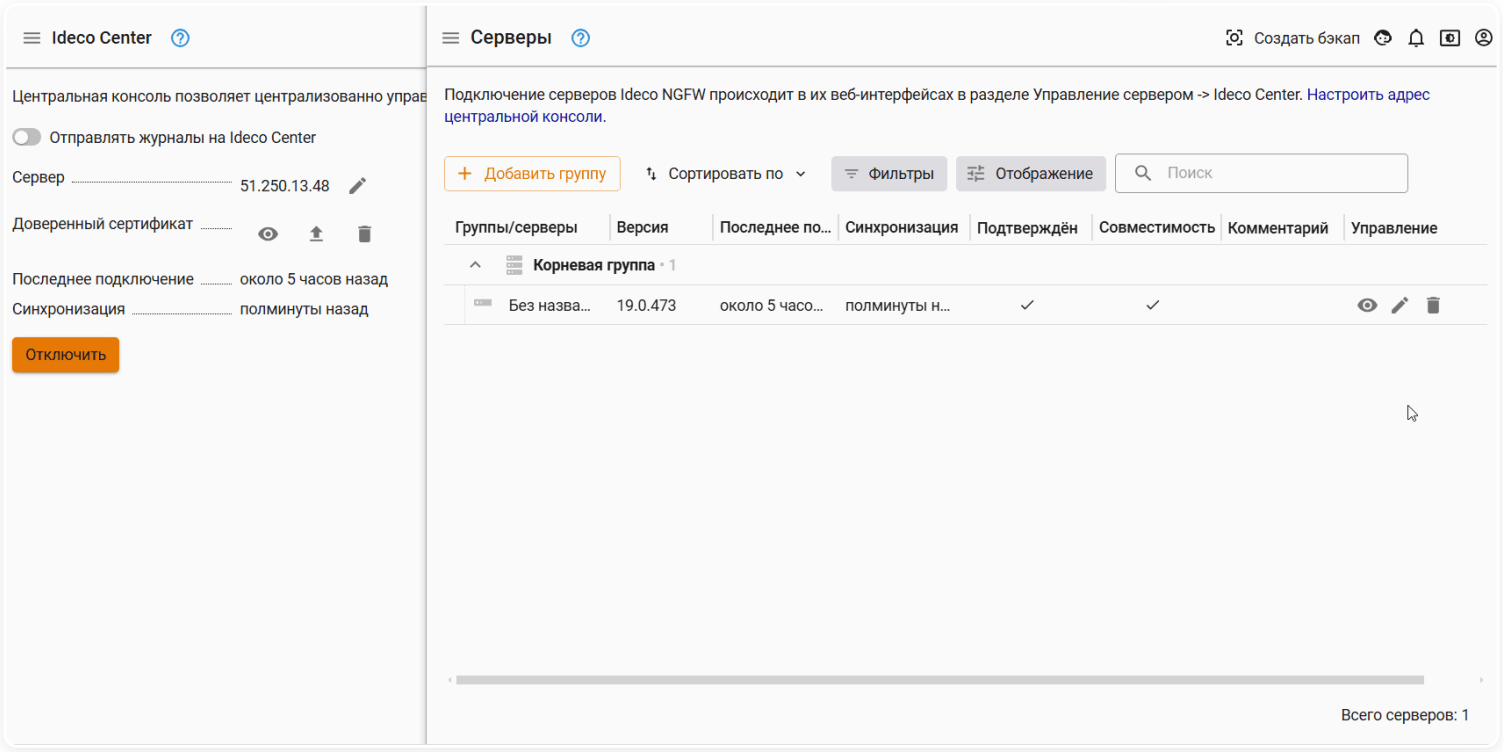


Скачать корневой сертификат можно в Ideco Center в разделе **Сервисы** → **Сертификаты**.

3. В интерфейсе Ideco Center перейдите в раздел **Серверы** и подтвердите подключение, нажав ✓:



Для удаления сервера Ideco NGFW Novum из Ideco Center разорвите привязку в интерфейсе Ideco Center, нажав 🗑:



VCE

API

Функциональность доступна в **Системном контексте**.

Название службы раздела **VCE**: `ideco-vce-backend`, `ideco-vce-rest`, `ideco-vce-vpp`.

Список служб для других разделов доступен по ссылке.

VCE (virtual context engine) - функциональность Ideco NGFW Novum, реализованная с помощью контейнеров Linux на базе systemd-nspawn, которая позволяет создавать виртуальные серверы (контексты) на одном системном NGFW Novum. Это дает возможность:

- Разбить одну локальную сеть на несколько независимых сетей с полной изоляцией трафика между ними. Коммуникация корневого сервера с виртуальными контекстами осуществляется через внешние сетевые мосты.
- Индивидуально создавать для каждой сети политики безопасности и объекты.
- Разграничивать доступ и независимо управлять дочерними VCE.

При этом нет необходимости устанавливать и настраивать для этого отдельные физические серверы.

Архитектура виртуальных контекстов не является Multitenancy.

Виртуальные контексты изолированы по ресурсам процессора и памяти, независимо обрабатывают трафик и имеют собственные конфигурации. Но интерфейсы и сетевые зоны контекстов конфигурируются из системного контекста, и администраторы системного контекста имеют доступ к конфиграции внутри VCE.

В 21 версии появилась возможность создавать два типа виртуальных контекстов:

- **Классический (VCE NGFW)** - контекст на основе решения NGFW. Настройки разделов в VCE NGFW идентичны настройкам в продукте Ideco NGFW Novum.
- **Высокопроизводительный (VCE VPP)** - контекст с обработкой трафика в VPP. Документация по настройке разделов VCE VPP доступна по ссылке.

Таблица с различиями между VCE NGFW и VCE VPP в статье.

Не предоставляйте доступ к VCE сторонним организациям, поскольку полная изоляция VCE не реализована и не предусмотрена. Предоставление доступа сторонним организациям может привести к угрозе безопасности сервера.

Платформы Ideco SX+ и Ideco SMX в текущих версиях не поддерживают запуск VCE. Поддержка планируется в следующих версиях.

Возможности VCE:

- Создание виртуальных контекстов и настройка независимых сетевых интерфейсов.
- Независимая настройка политик безопасности и прав доступа различным виртуальным контекстам.
- Связь с Ideco Center.
- Запуск и остановка виртуальных контекстов с одного **Системного контекста**.

Лицензия между **Системным контекстом** и всеми виртуальными контекстами общая. Это значит, что на Ideco NGFW Novum с лицензией на 100 пользователей можно создать неограниченное количество VCE, каждый из которых будет поддерживать 100 пользователей. В будущих версиях количество пользователей, ограниченное числом в лицензии, будет распределяться между **Системным контекстом** и всеми VCE.

В интерфейсе VCE недоступно:

- Создание кластера.
- Обновление.
- Переход в **Профиль** через иконку в шапке веб-интерфейса (настраивается в системном контексте).
- Возможность выключения и перезагрузки (настраивается в системном контексте).
- Энергосберегающий режим (настраивается в системном контексте).
- Изменение настроек часового пояса и языка (настраивается в системном контексте).
- Создание и редактирование Сетевых интерфейсов. В дочерних контекстах доступ ограничен интерфейсами текущего VCE в режиме только для чтения.
- Создание зон. Чтобы просмотреть доступные зоны в дочерних контекстах, перейдите в раздел **Правила трафика** → **Объекты**.

Важные моменты работы VCE:

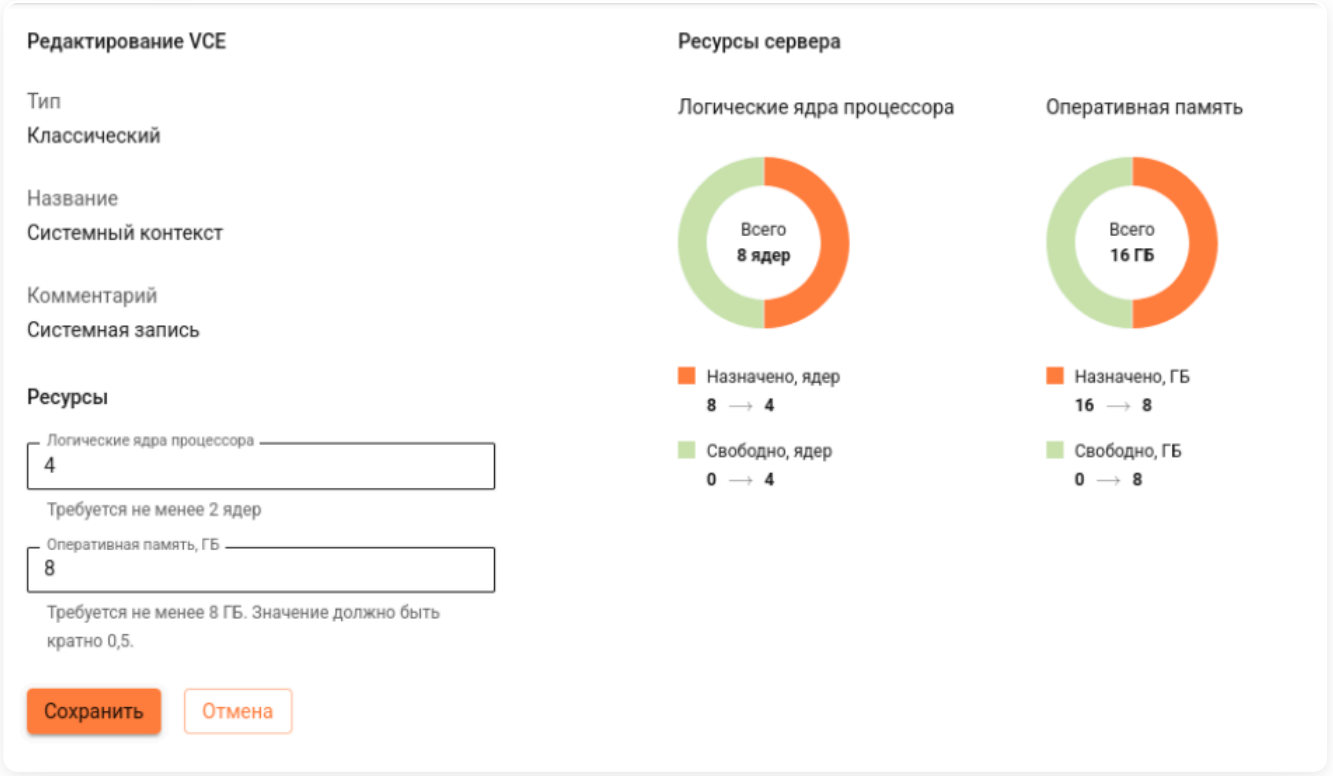
- В бэкап системного VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте бэкапы корневого NGFW и каждого из дочерних VCE.
- При восстановлении системы все настроенные VCE и их данные также откатятся к исходному состоянию.
- Если VCE исчерпает выделенные ресурсы:
  - При нехватке оперативной памяти система начнет выгружать данные на диск, что может привести к завершению процессов и нестабильной работе контекста.
  - При недостатке мощности выделенных ядер CPU возможны задержки и потеря пакетов.
- Каждый контекст использует собственные ресурсы и не влияет на другие.
- **Не рекомендуем использовать двухпроцессорные системы**, так как оптимизация для такого оборудования отсутствует. Поддержка планируется в следующих версиях.
- Рекомендуем отключить технологии при использовании **Высокопроизводительного** контекста, так как они могут существенно снижать производительность:
  - Hyper-Threading (Intel).
  - SMT (AMD).

Создание VCE

С 21 версии поддержка VCE без выделенных ресурсов прекращена.

Чтобы создать виртуальный контекст в рамках VCE, перейдите в **Управление сервером** → **VCE** и выполните действия:

1. Освободите ресурсы, назначенные в **Системном контексте**, и перенесите в список **Свободных ресурсов**. Для этого откройте редактирование VCE, нажав на , и перераспределите ресурсы:

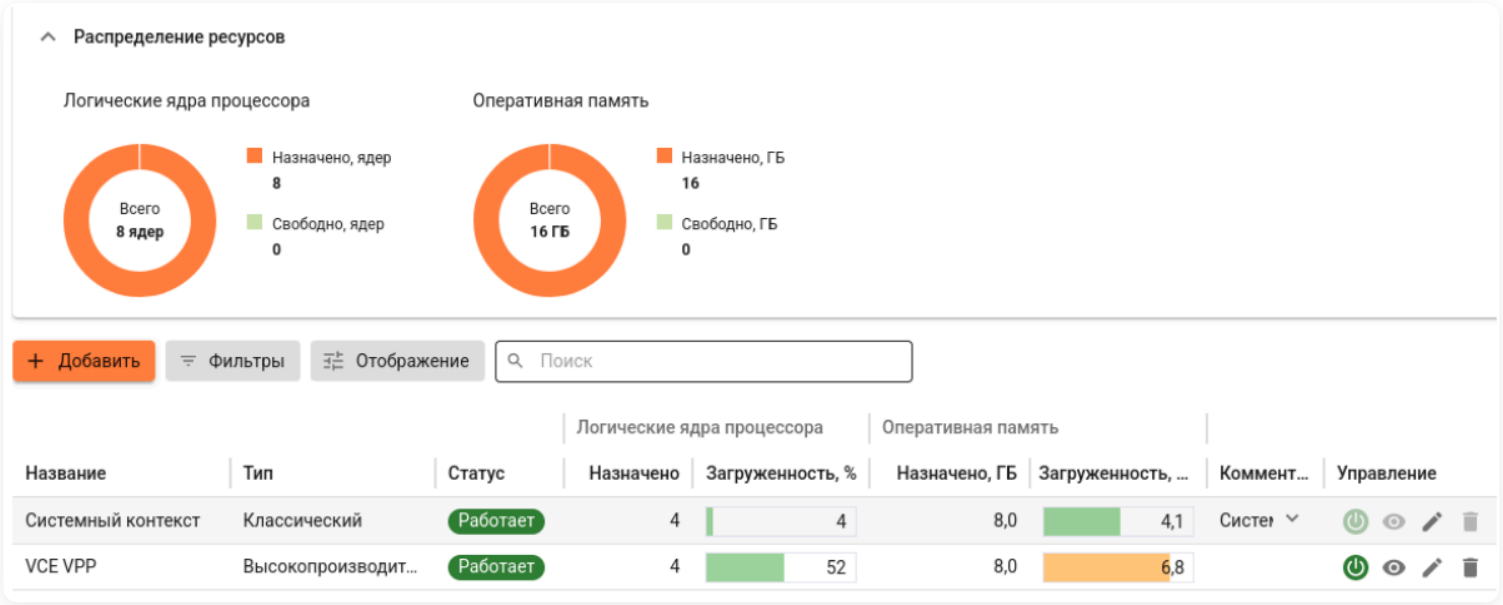


2. Нажмите **Добавить**.

3. Выберите тип создаваемого контекста: **Классический** или **Высокопроизводительный**. Укажите название контекста и назначьте ресурсы:

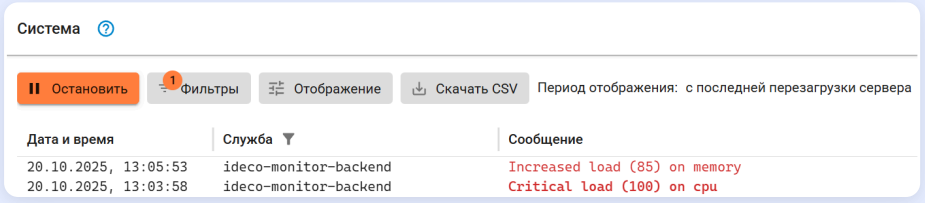
- Для работы классического контекста (VCE NGFW) потребуются минимум 8 ГБ оперативной памяти и 2 логических ядра.
- Для высокопроизводительного контекста (VCE VPP) потребуются минимум 8 ГБ оперативной памяти и 4 логических ядра.

4. Нажмите **Добавить** - виртуальный конктест появится в таблице:



5. Перейдите в **Сервисы → Сетевые интерфейсы** и на вкладке **Интерфейсы** создайте интерфейс для виртуального контекста. Для работы VCE нужен минимум один сетевой интерфейс. Пример настройки.

В 21 версии доступен **Мониторинг здоровья сервера**. Данные о состоянии сервера отображаются в разделе **Панель мониторинга**. При превышении пороговых значений Ideco NGFW Novum отправит уведомление и запишет событие в логи. Для просмотра этих записей перейдите в раздел **Система** и примените фильтр по службе `ideco-monitor-backend`:



Если для VCE выделены минимально возможные ресурсы, то они будут использоваться полностью, а пороговые значения будут всегда превышены. Это штатная работа Ideco NGFW Novum в таких условиях и не считается ошибкой.

Редактирование VCE

Чтобы отредактировать VCE, нажмите на . При редактировании можно менять:

- Название виртуального контекста.
- Выделенные ресурсы.

Изменение VCE приведет к перезапуску контекста и следующих служб:

- **Прокси** - в `ideco-proxy-backend` будет перезапущена служба `squid`.
- **Предотвращение вторжений** - в `ideco-suricata-backend` будет перезапущена служба `ideco-suricata`.
- **Антивирус** - в `ideco-av-backend` будут перезапущены службы `av4web` и `kav-scanner`.

Если в таблице большое количество VCE, воспользуйтесь кнопкой **Фильтры**.

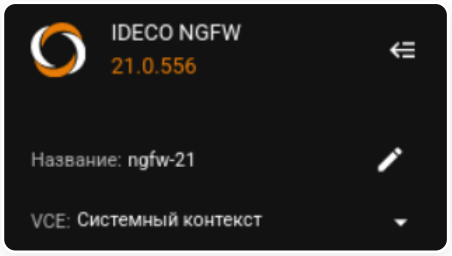
Удаление VCE

Удалить VCE можно, нажав на в системном VCE.

После удаления VCE все его настройки, журналы и внутренние данные будут безвозвратно утеряны. Восстановить их будет невозможно.

Переход в веб-интерфейс VCE

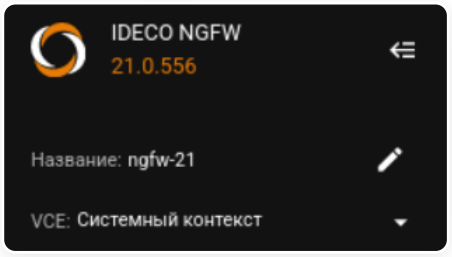
После создания VCE текущий сервер, в котором VCE был создан, будет обозначен как **Системный контекст**:



Перейти в веб-интерфейс созданного VCE из веб-интерфейса NGFW Novum можно двумя способами:

1. Перейдите в **Управление сервером** → **VCE** и нажмите на . В новой вкладке откроется веб-интерфейс VCE.

2. Нажмите на в левом верхнем углу и выберите нужный VCE:



Дополнительно

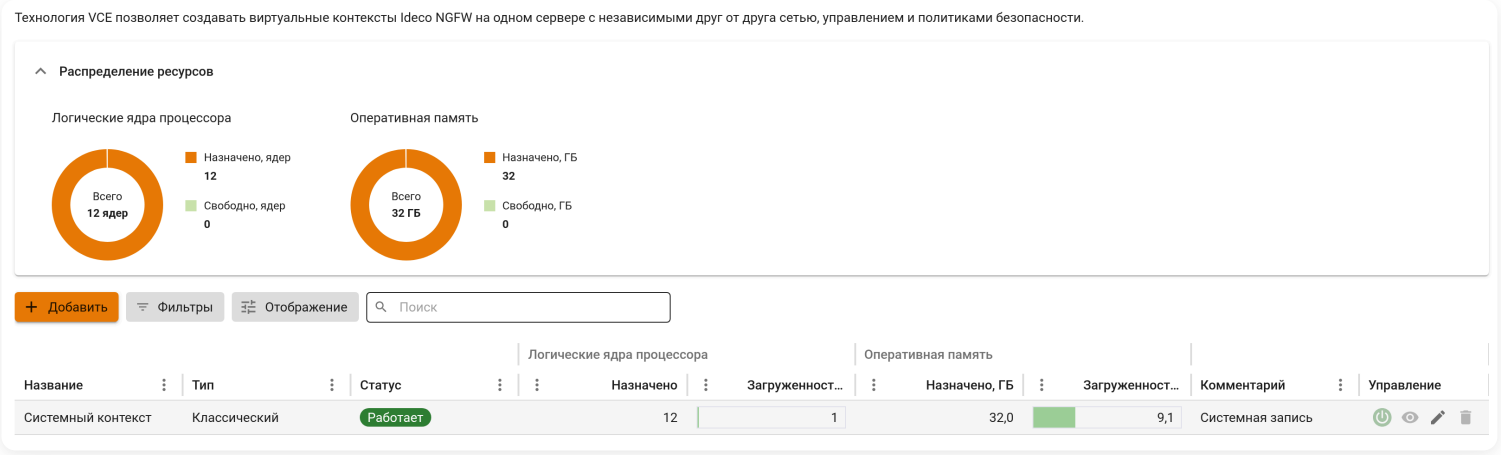
Пример распределения ресурсов для создания виртуального контекста

Настройка виртуального контекста для разделения основного и дочернего офисов, чтобы создавать и настраивать индивидуальные политики безопасности и объекты для каждого офиса.

Создание контекста состоит из двух этапов:

1. Распределение назначенных ресурсов в пул свободных.
2. Выделение свободных ресурсов новому виртуальному контексту.

Рассмотрим процесс на примере системы с конфигурацией: 12 логических ядер процессора и 32 ГБ оперативной памяти:



1. Перейдите в раздел редактирования **Системного контекста**, нажав на .

2. Распределите **Назначенные ресурсы** в пул **Свободных ресурсов** и нажмите **Сохранить**. Если физический сервер оснащен 12 ядрами и 32 ГБ оперативной памяти, а для **Системного контекста** выделено 8 ядер и 16 ГБ, то оставшиеся ресурсы будут перераспределены в свободные ресурсы:

- Для работы классического контекста (VCE NGFW) потребуются минимум 8 ГБ оперативной памяти и 2 логических ядра.
- Для высокопроизводительного контекста (VCE VPP) потребуются минимум 8 ГБ оперативной памяти и 4 логических ядра.

3. Нажмите **Добавить** и выберите тип создаваемого контекста: **Классический** или **Высокопроизводительный**. Укажите название контекста и назначьте свободные ресурсы:

4. Нажмите **Добавить** - виртуальный контекст появится в таблице:

Пример создания интерфейсов

1. Перейдите в **Сервисы** → **Сетевые интерфейсы Системного контекста** и создайте два интерфейса с ролью WAN и LAN, которые будут использоваться в виртуальном контексте:

2. В виртуальном контексте перейдите в **SD-WAN** → **Next hop** и добавьте шлюз для интерфейса с ролью WAN:

3. В виртуальном контексте в **Управление сервером** → **Лицензия** появится информация о лицензии:

Для высокопроизводительного контекста в **Правила трафика** → **Межсетевой экран** по умолчанию установлено запрещающее FORWARD-правило. Если не создать разрешающие правила, все порты и протоколы для пользователей будут запрещены.

Полезные ссылки

- **Настройка высокопроизводительного контекста**
- **Отличия VCE NGFW и VCE VPP**

Отличия VCE NGFW и VCE VPP

Функции, не описанные в таблице, присутствуют и в VCE NGFW, и в VCE VPP.

ГОСТ VPN, **USB-токены**, **Кластеризация** и **VCE** доступны только в **Системном контексте**.
Почтовый релей доступен в **Классическом** и **Системном** контекстах.

В таблице представлены отличия VCE NGFW и VCE VPP:

Функциональность	**NGFW**	**VPP**
Пользователи		
VPN-подключения через IKEv2/IPsec, L2TP/IPsec	✅	❌
Авторизация по MAC-адресу	✅	❌
Использование Профилей TLS в настройках авторизации	❌	✅
Обнаружение устройств	✅	❌
Мониторинг		
Сессии администраторов	✅	❌
Графики загруженности IPsec	✅	❌
Графики загруженности WCCP GRE	✅	❌
Графики загруженности ГОСТ VPN	✅	❌
Графики загруженности VCE	✅	❌
Правила трафика		
Межсетевой экран, функционал: • Аппаратная фильтрация • Настройка ALG • Логирование • Строгая проверка состояний в FORWARD	✅	❌
Персональное ограничение скорости	✅	❌
Исключения	✅	❌
Пользовательские сигнатуры в **Предотвращение вторжений**	✅	❌
Профили безопасности		
Контент-фильтр	Модуль в разделе **Правила трафика**. Функциональность: • Создание правил для запрета, разрешения и фильтрации веб-трафика • Фильтрация трафика только на 80 и 443 TCP-портах • Морфологические словари • Настройки безопасности и выбор сертификатов для MITM	Профили в разделе **Профили безопасности**. Функциональность: • Использование профилей в правилах Межсетевого экрана • Фильтрация трафика на любых TCP-портах

Профили TLS/SSL-инспекции	Модуля в **Профилях безопасности** нет. Доступно: • Расшифровка трафика правилами **Контент-фильтра** • Расшифровка трафика только на 80 и 443 TCP-портах	Профили в разделе **Профили безопасности**. Функциональность: • Использование профилей в правилах Межсетевого экрана • Расшифровка трафика на любых TCP-портах
Сетевые интерфейсы (все интерфейсы создаются, редактируются и удаляются только в системном контексте)		
Loopback	✅	❌
L2TP	✅	❌
PPPoE	✅	❌
PPTP	✅	❌
L2-мост	❌	✅
Сервисы		
Прокси, функции: • WCCP • Прямые подключения	✅	❌
Обратный прокси, функции: • Настройка web-серверов для балансировки запросов • Передача web-серверу реального IP-адреса клиента • Выбор типа публикации	✅	❌
ЛК/Портал SSL VPN, функции: • Публикация ресурсов SSL VPN	✅	❌
Перехват пользовательских DNS-запросов	Встроенная опция	Можно настроить вручную с помощью правил DNAT
DDNS	✅	❌
Перехват пользовательских NTP-запросов	✅	❌
IPsec	✅	❌
Маршрутизация		
Опция адаптивности при настройке маршрутизации Внешних сетей	✅	❌
Отчеты и журналы		
Трафик, виджеты: • Топ категорий • Топ сайтов • Топ заблокированных сайтов • Топ заблокированных категорий	✅	❌
Управление сервером		
Опция отправки журналов на Ideco Center	✅	❌
Обновления: • Вкладка **Система** • Выбор источника баз GeoIP	✅	❌
Перезагрузка сервера	✅	❌
Энергосберегающий режим	✅	❌

Полезные ссылки

- **Настройка высокопроизводительного контекста**
- **VCE**

Кластеризация

Функциональность доступна в **Системном контексте**.

Название службы раздела **Кластеризация**: `ideco-cluster-backend`, `ideco-cluster-backup-pusher`.

Список служб для других разделов доступен по ссылке.

Для настройки требуется активная лицензия с режимом кластеризации. Подробную информацию о лицензировании кластера можно найти в статье.

Каждое из двух устройств Ideco NGFW Novum, объединенных в кластер, называется нодой.

Кластер работает в режиме active-passive:

- **Активной** является нода, обрабатывающая трафик в данный момент.
- **Резервная** нода находится в предзагруженном состоянии и непрерывно отслеживает состояние активной ноды, а при отсутствии связи с ней переводит текущие задачи обработки трафика на себя.

При переключении нод резервная нода становится активной.

В любой момент обрабатывать трафик может только одна из нод.

Административно переключить ноды нельзя.

Если IP-адреса кластера настроены вручную, то кластер имеет один общий IP на внутреннем интерфейсе и другой общий IP на внешнем интерфейсе. В случае автоматической конфигурации по DHCP адреса будут отличаться в зависимости от ноды.

Межкластерное соединение

Сетевое взаимодействие между нодами осуществляется по одному или нескольким физическим каналам, для которых на каждой ноде резервируется один или несколько физических портов.

Для корректной работы кластера необходимо постоянное наличие связи между нодами посредством прямого сетевого соединения, без использования моста или коммутатора.

При настройке кластера доступен выбор типа соединения:

- **Ethernet** - для связи между нодами может быть настроен только один физический порт. При наличии нескольких портов для связи между нодами настроить этот тип соединения нельзя. Настроить второй порт для связи между нодами в созданном кластере с типом соединения **Ethernet** нельзя.
- **LACP** - для связи между нодами должно быть настроено несколько физических портов. При выходе из строя одного физического порта связь между нодами будет работать через другой. При этом кластер продолжит работать штатно. В кластере с типом **LACP** можно добавить порт для связи между нодами без потери связности.

VCE в кластере

При создании VCE на активной ноде:

- На резервной ноде создается VCE, который синхронизирует конфигурацию с VCE на активной ноде.
- Пользовательские сессии синхронизируются только в кластере **С синхронизацией сессий**.

При переключении нод VCE запускается с последней имеющейся конфигурацией.

При обновлении Ideco NGFW Novum с 20 версии кластеры получат тип соединения **Ethernet**.

Чтобы изменить тип кластерного соединения, нужно разрушить кластер.

Процесс синхронизации нод в кластере

- При синхронизации двух NGFW данные активной ноды копируются в резервную ноду.
- Синхронизация данных происходит автоматически в фоновом режиме.
- Автоматические бэкапы отключены на резервной ноде. Все бэкапы с активной ноды передаются на резервную в момент обмена данными и заменяют те бэкапы, которые там присутствовали ранее.

Обмен данными между нодами кластера происходит раз в минуту. Все несинхронизированные пользовательские изменения настроек и бэкапы **могут быть потеряны, если с момента внесения изменений на активной ноде до переключения нод не было обмена данными**.

Диагностика нод кластера

Проверить статус текущей ноды

Если подключение к серверу выполнено через веб-интерфейс или SSH - это активная нода.

Имя сервера можно посмотреть:

- В веб-интерфейсе - в левом верхнем углу, под именем кластера.
- В локальном меню - на стартовом экране в строке **Название сервера**.

Для проверки статуса текущей ноды используйте один из способов:

Локальное меню

На стартовом экране локального меню отображается статус ноды в строке **Состояние кластера**:

```
Название кластера:                      Без названия b42c0cae-9d59-4efa-a1ca-e635f3d45d67
Название сервера:                       Без названия b42c0cae-9d59-4efa-a1ca-e635f3d45d67
Тип кластера:                           С синхронизацией сессий
Тип соединения:                         LACP
Состояние кластера:                     Активная нода
Состояние локальных интерфейсов:        Настроены
Доступ Удаленного Помощника:            Отключено
Режим `Разрешить Интернет всем`:        Отключено
Доступ в веб-интерфейс:                 Доступен
Доступ к веб-интерфейсу из внешней сети:  Отключено

Адреса веб-интерфейса:
    https://192.168.1.10:8443
    https://192.168.101.10:8443

В случае возникновения ошибок на сервере, пожалуйста,
обратитесь в техподдержку:

Email: help@ideco.ru
Портал тех. поддержки: help.ideco.ru
Время работы тех. поддержки: ideco.ru/support


Нажмите любую клавишу для перехода к локальному меню.
Press Ctrl+R if you don't see the symbols above.
```

Команда в терминале

1. Откройте терминал одним из способов:

- В веб-интерфейсе перейдите в **Управление сервером** → **Терминал**.
- В локальном меню выберите **Консоль**.

2. Введите команду:

```
etcdctl_rt get /cluster/status/v1/record
```

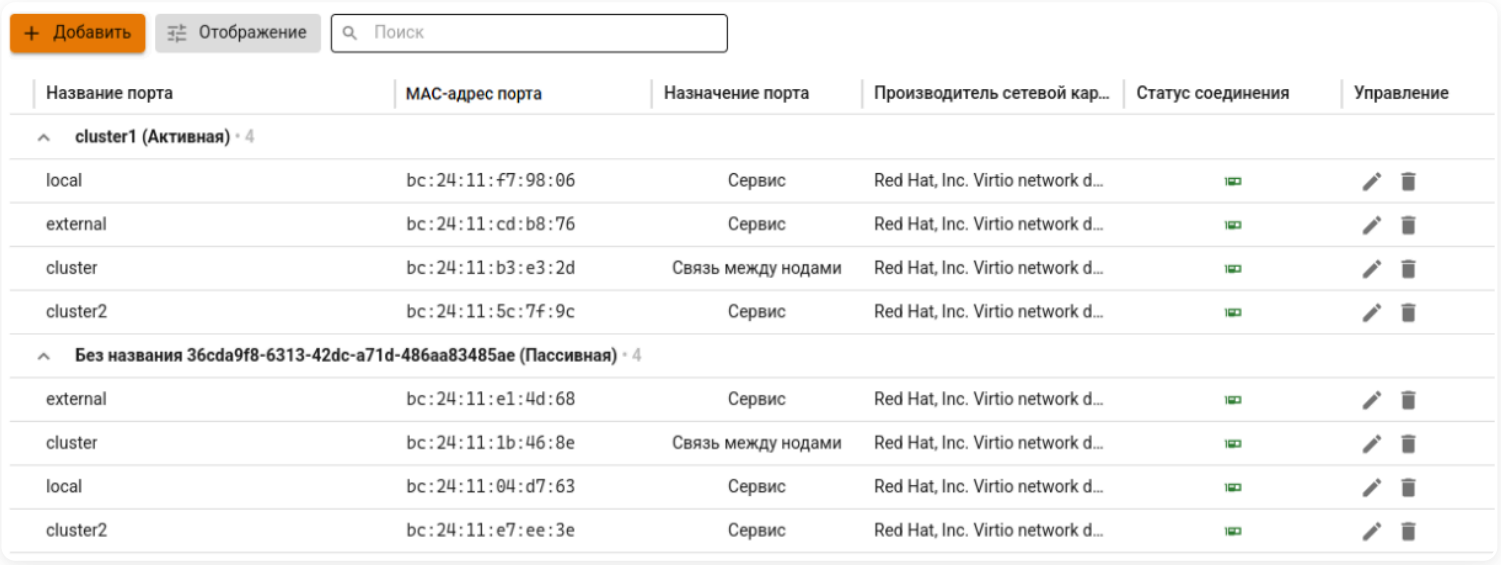
Возможные значения вывода:

- `{"state": "ACTIVE"}` - текущая нода - активная;
- `{"state": "RESERVE"}` - текущая нода - резервная. Статус не отобразится в выводе команды, так как проверка выполняется на активной ноде;
- `{"state": "NOT_CONFIGURED"}` - кластер не настроен.

Проверить состояние резервной ноды

Резервная нода доступна, если в разделе **Управление сервером** → **Кластеризация** присутствует сообщение о том, что связь с сервером установлена.

Проверить статусы физических портов резервной ноды можно в веб-интерфейсе активной ноды в таблице **Сервисы** → **Сетевые интерфейсы** → **Физические порты** в столбце **Статусы соединения**:



Проверить статусы сетевых интерфейсов и модулей резервной ноды можно, подключившись к ней по ssh (это возможно только в кластере **С синхронизацией сессий**). Для этого:

1. На активной ноде перейдите в **Управление сервером** → **Терминал**.

2. Введите команду `ideco-ssh-another-node` для подключения по ssh к резервной ноде.

3. Воспользуйтесь командами:

- `ip a` - для проверки статуса сетевых интерфесов резервной ноды.
- `systemctl status <название службы Ideco NGFW Novum>` - для проверки статуса служб Ideco NGFW Novum.

Особенности работы кластера

Особенности работы кластера с синхронизацией сессий

- При переключении на резервную ноду изменения с активной ноды применяются к бэкапам и базам данных на резервной ноде. Изменения не применяются к логам journald и мониторинга, а также аппаратным данным.
- Если активная нода теряет соединение (carrier down), переключение происходит моментально. Если нода перестает отвечать на запросы, переключение произойдет через 8 секунд.

- При переключении происходит синхронизация данных приложений с активной ноды на резервную.
- Нода, на которой есть внесенные администратором изменения, будет оставаться активной до синхронизации данных с резервной нодой.
- При отключении интерфейса локальной/внешней сети активная нода становится резервной, а резервная - активной.
- При отключении интерфейса локальной/внешней сети активной становится нода, у которой больше активных интерфейсов. Резервной - нода, у которой меньше активных интерфейсов.
- При одинаковом количестве отключенных интерфейсов на обеих нодах активной становится нода, у которой было меньше всего деградации сети (разрывов). Резервной - нода, у которой было больше всего разрывов.
- При одинаковом количестве отключенных/включенных интерфейсов на обеих нодах и одинаковом количестве разрывов сети активной становится нода, у которой больше uptime (запущена раньше). Резервной - нода, у которой uptime меньше (запущена позднее).
- При офлайн-обновлении кластера с синхронизацией сессий обновления баз **Предотвращения вторжений**, **Контент-фильтра** и **Антивирусов веб-трафика** не синхронизируются, каждая нода обновляется отдельно. Вторая нода обновится после того, как станет активной.

Особенности работы кластера без синхронизации сессий

- При переключении на резервную ноду синхронизируются все данные с диска активной ноды (синхронизация осуществляется за счет копирования файлов в файловой системе).
- При отключении интерфейса локальной/внешней сети механизм переключения нод в этом режиме кластера не предусмотрен.
- Время переключения нод - 15 секунд + загрузка резервной ноды.
- При переключении нод не синхронизируются логи мониторинга и journald, а также аппаратные данные.

Особенности работы с бэкапами при кластеризации

- Невозможно полное восстановление из бэкапов. При этом можно создать резервную копию и после разрушения кластера восстановить копию на ноде, которая была активной.
- На активной ноде доступно **Мгновенное восстановление из бэкапа**. Восстанавливаются все настройки, кроме статистики в отчетах. Данные на второй ноде также придут в соответствие с восстановленными настройками после синхронизации нод.

Особенности работы кластера в облачных сервисах

- Кластер в облаке можно поднять, только если облако поддерживает L2-связность.
- Если облако не поддерживает L2-связность, то отказоустойчивости можно достичь средствами самого облака.

Особенности работы кластера в гипервизорах

Для корректной работы кластерной сети в гипервизоре требуется дополнительная настройка сетевых адаптеров:

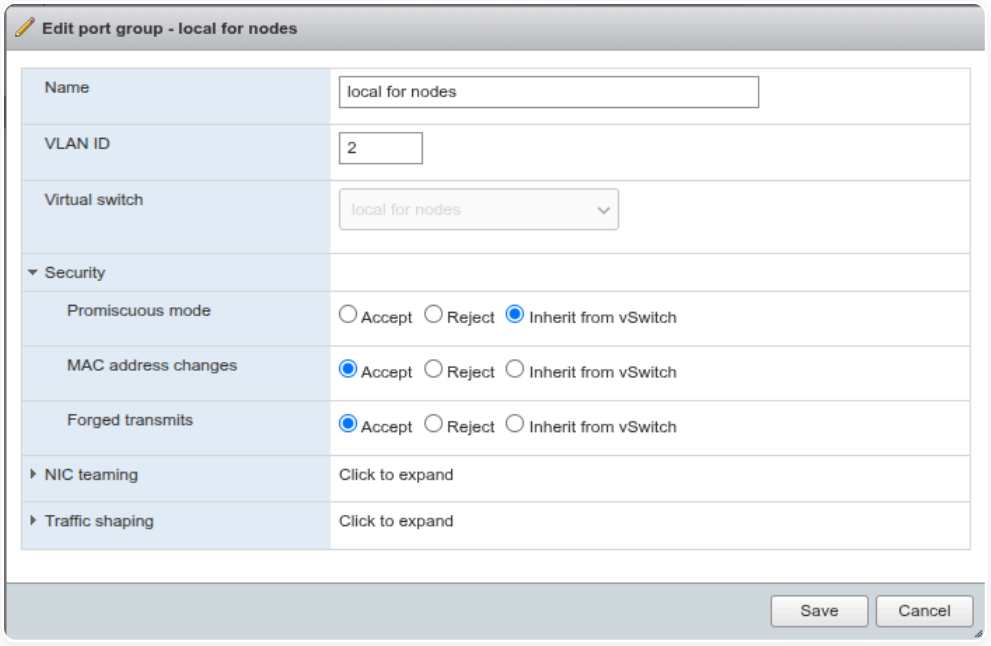
VMware ESXi:

1. В интерфейсе VMware ESXi перейдите в **Navigator** → **Networking** → **Port groups**.

2. Выберите группу портов, используемую для сети синхронизации нод, и нажмите **Edit settings**.

3. Раскройте раздел **Security**.

4. Установите значение **Accept** для двух параметров:



- **MAC address changes** - разрешает прием трафика на MAC, отличающийся от заданного в настройках ВМ.
- **Forged transmits** - разрешает отправку кадров с MAC-адресом источника, отличающимся от заданного в настройках ВМ.

5. Нажмите **Save**.

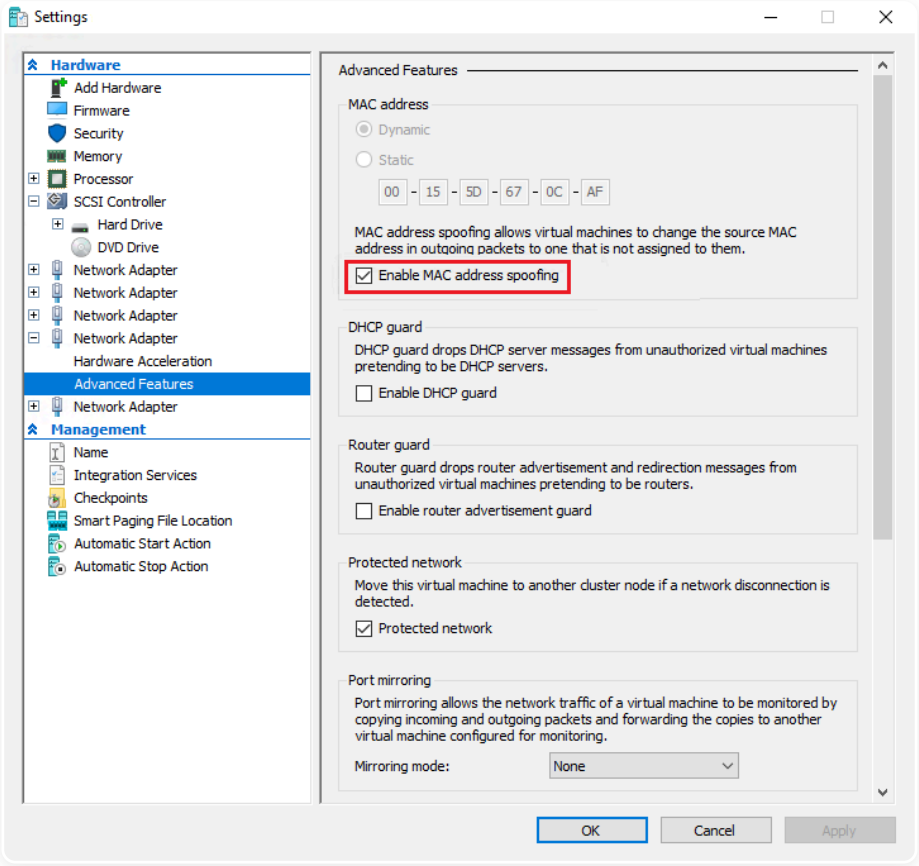
6. Перезапустите NGFW Novum.

> Для синхронизации нод кластера NGFW Novum в виртуальных средах не рекомендуется использовать LACP. Если требуется отказоустойчивость канала между ESXi-хостами, настройте LACP на стороне самих хостов и физических коммутаторов - агрегация будет работать прозрачно для NGFW Novum.

Microsoft Hyper-V:

1. Перейдите в **Hardware** → **Network Adapter** → **Advanced Features** → **MAC address**.

2. Включите опцию **Enable MAC address spoofing**:



Без этих настроек связь между нодами не будет установлена. Подробнее в статье Настройка гипервизора.

Возможные проблемы при работе двух Ideco NGFW Novum в кластере

- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.
- Два NGFW с разными версиями не синхронизируются.
- При обновлении Ideco NGFW Novum в кластере сначала обновится активная нода, затем резервная нода с младшей версией принудительно станет активной для обновления до версии активной ноды. Подробнее смотрите статью Обновление кластера.
- При различных размерах жестких дисков могут возникнуть проблемы синхронизации из-за нехватки места.
- Если у провайдера имеется привязка по MAC-адресу, то при переключении нод будет отсутствовать доступ в интернет.
- Если с момента создания бэкапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения этот бэкап будет потерян.
- Если с момента мгновенного восстановления из бэкапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения вторая нода окажется в состоянии до восстановления.

> **Кластерный режим совместим с агрегацией интерфейсов (LACP)**.

Полезные ссылки

- **Настройка кластера**
- **Обновление кластера**
- **Основные интерфейсы**
- **VCE**
- **Терминал**
- **Физические порты**
- **Предотвращение вторжений**
- **Контент-фильтр**
- **Настройка гипервизора**
- **Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG**

Настройка кластера

Функциональность доступна в **Классическом** и **Системном контекстах**.

Если на момент создания кластера у вас уже есть настроенный Ideco NGFW Novum, рекомендуем выбрать настроенный Ideco NGFW Novum в качестве активной ноды. Все настройки резервной ноды в процессе создания кластера будут удалены.

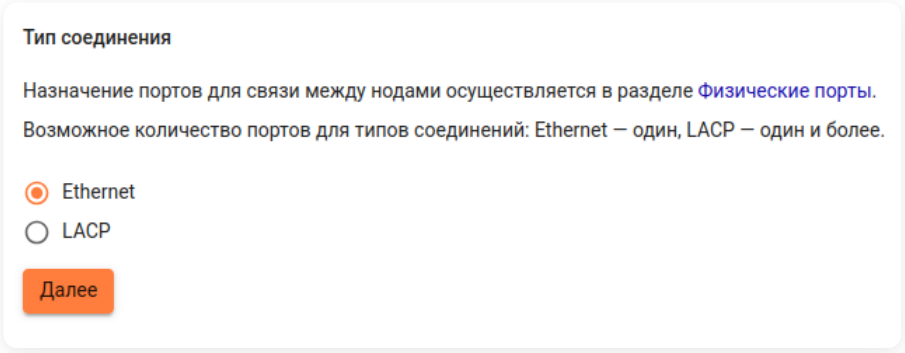
Требования

Для создания кластера необходимо соблюдение следующих требований:

- В кластере может быть только две ноды Ideco NGFW Novum.
- Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки, и один тип кластерного соединения.
- Сетевые порты для использования в кластере желательно соединять напрямую, т.к. на основе интерфейса происходит ускоренное переключение нод, поэтому не рекомендуется использовать коммутаторы для кластерной сети. Как минимум сеть должна быть изолирована.
- Для типа соединения **LACP** промежуточное оборудование (свитч между нодами) должно поддерживать LACP.
- В NGFW Novum нет возможности использовать геораспределенные ноды.
- При работе NGFW Novum в гипервизорах используйте средства отказоустойчивости гипервизора. Перед созданием кластера выполните дополнительную настройку сетевых адаптеров. Без нее связь между нодами не будет установлена. Подробнее - в разделе Особенности работы кластера в гипервизорах.

- Физические порты для связи между нодами на каждом Ideco NGFW Novum должны быть в одном сегменте локальной сети, в котором нет других устройств. Не используйте в качестве кластерной сети общедоступную сеть, используемую для передачи стороннего трафика. Обмен данными между нодами не защищен от подмены и прослушивания.
- При настройке кластеризации с использованием гипервизора убедитесь, что сетевые порты, предназначенные для связи между нодами, подключены к изолированной IPv6-сети.
- Не рекомендуем добавлять или удалять физические порты. При несовпадении количества портов на разных нодах кластер будет работать некорректно. Удаление физического порта, используемого для связи между нодами, разрушит кластер.
- Можно менять сетевые карты при редактировании физических портов в кластере, но не рекомендуется переименовывать их. При несовпадении названий портов на разных нодах кластер будет работать некорректно.

В кластере можно удалять, редактировать и создавать новые сетевые интерфейсы. Выполните действия в зависимости от **Типа соединения**:



Убедитесь, что все требования для создания кластера соблюдены:

- Если на сервере нет физических портов для связи между нодами, перейдите в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** и настройте один или несколько портов.
- Если названия и/или количество физических портов на нодах отличаются, отредактируйте порты в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** или в локальном меню сервера.

Ethernet

Ethernet - для связи между нодами может быть настроен только один физический порт. При наличии нескольких портов для связи между нодами настроить этот тип соединения нельзя.

Шаг 1 - Конфигурация резервной ноды

Конфигурация из локального меню Ideco NGFW Novum

1. В локальном меню резервной ноды выберите пункт **Физические порты** → **Показать список и отредактировать порт**:

```
Выберите порт:

-------------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------------
  1    |  eth0_d8  |  bc:24:11:48:49:d8  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  2    |  eth1_73  |  bc:24:11:84:eb:73  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  3    |  eth2_63  |  bc:24:11:de:13:63  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
```

2. Выберите физический порт, который планируете использовать для связи между нодами.

3. Введите название физического порта.

4. Оставьте прежние настройки сетевой карты.

5. Укажите режим работы порта **Для связи между нодами кластера**:

```
Текущий режим работы порта: Сервис
Выберите режим работы порта:

1. Для связи между нодами кластера
2. Сервисный порт (для построение интерфейсов на базе этого порта)

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1
Физический порт успешно обновлен.
```

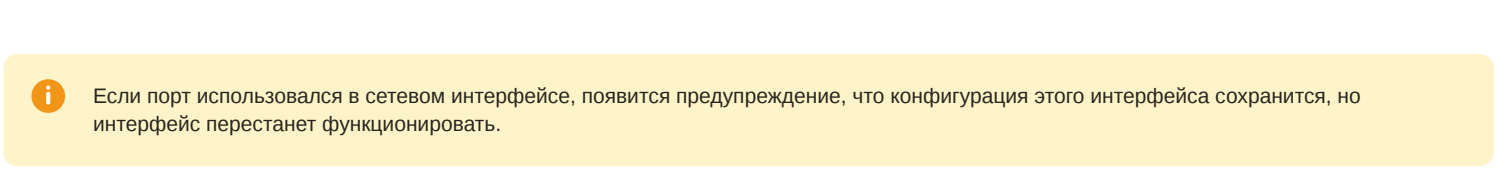
6. Перейдите в веб-интерфейс активной ноды и выполните настройки раздела **Шаг 2 - Конфигурация активной ноды**.

Конфигурация из веб-интерфейса Ideco NGFW Novum

1. Перейдите в **Сервисы** → **Сетевые интерфейсы** → **Физические порты**.

2. Выберите физический порт, который планируете использовать для связи между нодами, и нажмите  .

3. Включите опцию **Зарезервировать для связи между нодами в кластере** и нажмите **Сохранить**:



Если порт использовался в сетевом интерфейсе, появится предупреждение, что конфигурация этого интерфейса сохранится, но интерфейс перестанет функционировать.

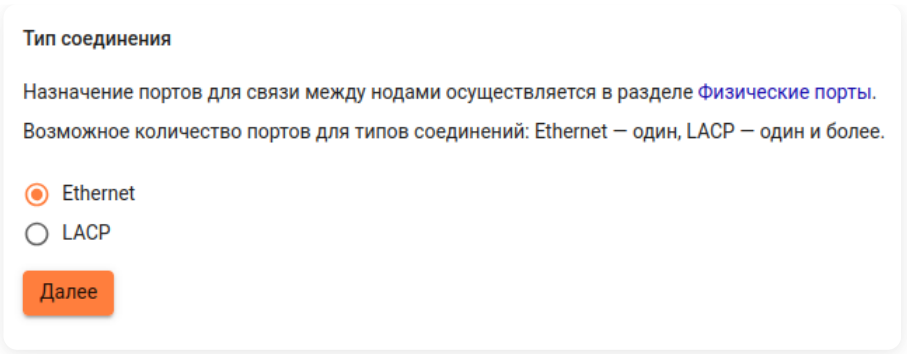
4. Перейдите в веб-интерфейс активной ноды и выполните настройки раздела **Шаг 2 - Конфигурация активной ноды**.

Шаг 2 - Конфигурация активной ноды

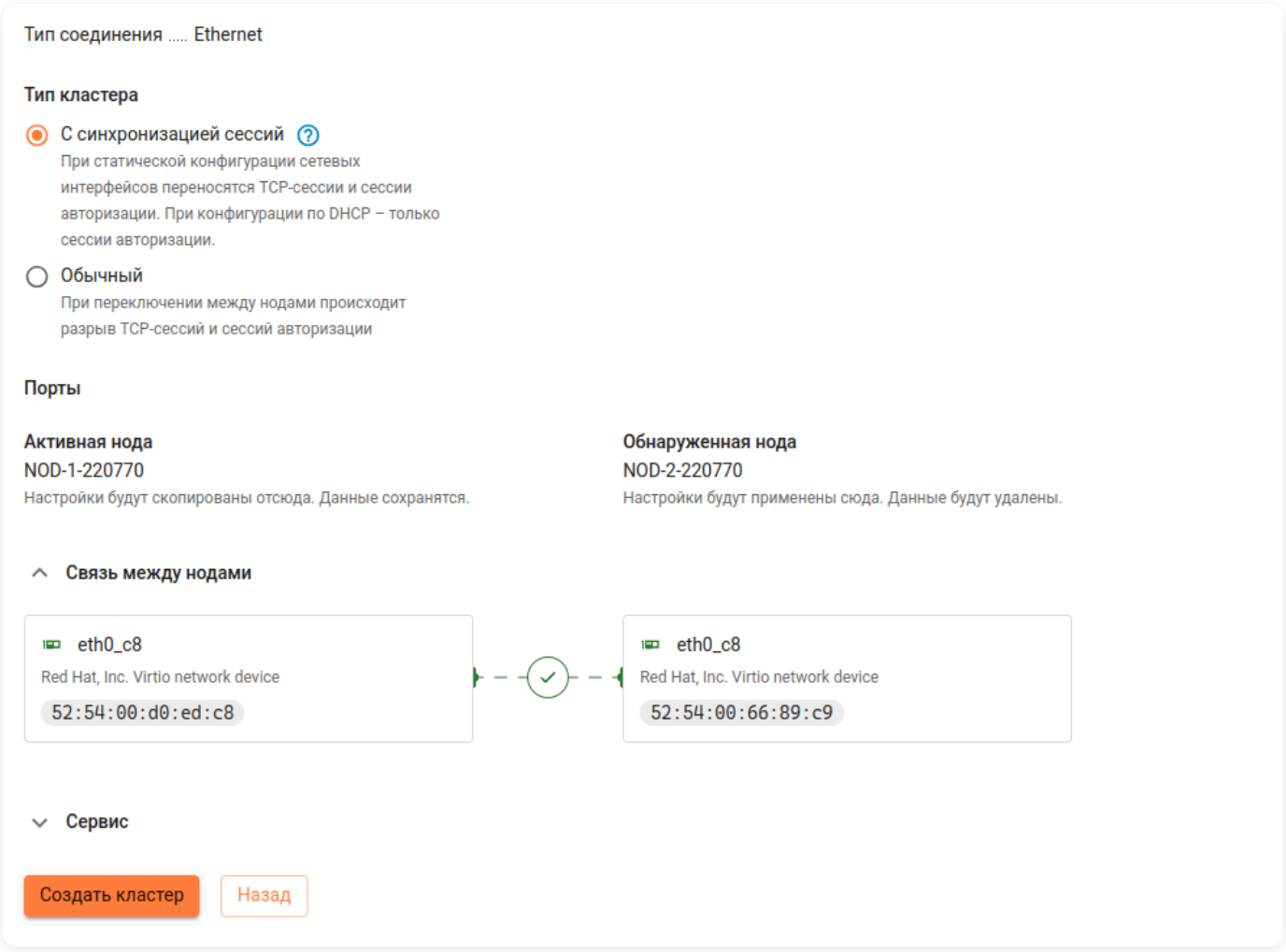
Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW Novum выполните действия:

1. Перейдите в **Управление сервером** → **Кластеризация**.

2. Выберите тип кластерного соединения **Ethernet** и нажмите **Далее**:



3. Выберите тип кластера и нажмите **Создать кластер**. Сетевые порты нод будут сопоставлены автоматически:



LACP

LACP - для связи между нодами должно быть настроено несколько физических портов. При выходе из строя одного физического порта связь между нодами будет работать через другой. При этом кластер продолжит работать штатно.

При создании LACP-интерфейса между нодами кластера достаточно указать один физический порт - система автоматически создаст канал между одноименными портами обеих нод. Например, если в кластере есть порт `client`, созданный LACP-интерфейс объединит `client` с первой ноды и `client` со второй ноды. Подробнее о создании LACP-интерфейса - в статье.

Шаг 1 - Конфигурация резервной ноды

Конфигурация из локального меню Ideco NGFW Novum

1. Выберите пункт **Физические порты** → **Показать список и отредактировать порт**:

```
Выберите порт:

-------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------
  1    |  eth0_d8  |  bc:24:11:48:49:d8  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------
  2    |  eth1_73  |  bc:24:11:84:eb:73  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------
  3    |  eth2_63  |  bc:24:11:de:13:63  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------
```

2. Выберите физический порт, который планируете использовать для связи между нодами.

3. Введите имя физического порта.

4. Оставьте прежние настройки сетевой карты.

5. Укажите режим работы порта **Для связи между нодами кластера**:

```
Текущий режим работы порта: Сервис
Выберите режим работы порта:

1. Для связи между нодами кластера
2. Сервисный порт (для построение интерфейсов на базе этого порта)

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1
Физический порт успешно обновлен.
```

6. В локальном меню резервной ноды выберите пункт **Выбор типа кластерной сети** и режим **LACP**:

```
Управление сервером

1. Консоль
2. Физические порты
3. Ethernet-интерфейсы
4. LACP-интерфейсы
5. VLAN-интерфейсы
6. Отключить все статические маршруты и добавить новый
7. Выбор типа кластерной сети
8. Включить доступ к веб-интерфейсу из внешней сети
9. Включить доступ к серверу по SSH из Интернет
10. Включить доступ к серверу по SSH из локальных сетей
11. Включить режим `Разрешить Интернет всем`
12. Сбросить блокировки по IP
13. Отключить пользовательский межсетевой экран
14. Создать новый бэкап
15. Восстановить из бэкапа
16. Мгновенно восстановить из бэкапа
17. Включить доступ Удаленного Помощника
18. Контакты технической поддержки
19. 2FA администраторов
20. Восстановиться на предыдущую версию
21. Перезагрузка сервера
22. Отключить сервер
23. Сменить пароль
24. Выход

Введите номер пункта и нажмите Enter.
# 7

1. Ethernet
2. LACP

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 2
```

7. Повторите пункты 1-5 для другого порта.

8. Перейдите в веб-интерфейс активной ноды и выполните настройки раздела **Шаг 2 - Конфигурация активной ноды**.

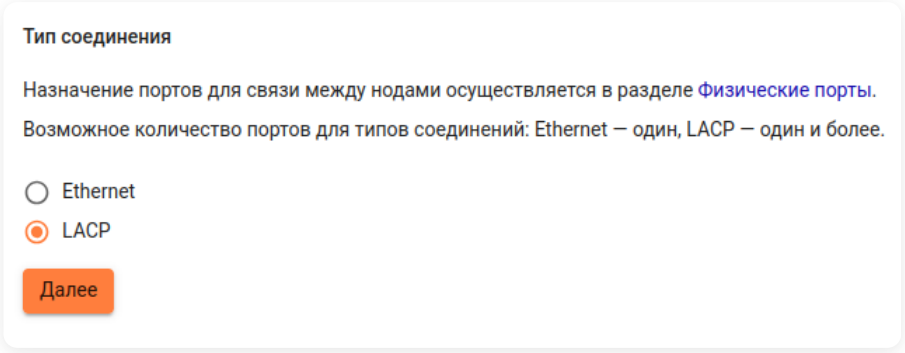
Конфигурация из веб-интерфейса Ideco NGFW Novum

1. Перейдите в **Сервисы → Сетевые интерфейсы → Физические порты**.

2. Выберите физический порт, который планируете использовать для связи между нодами, и нажмите  .

3. Включите опцию **Зарезервировать для связи между нодами в кластере** и нажмите **Сохранить**:

4. Перейдите в **Управление сервером** → **Кластеризация** и выберите тип кластерного соединения - **LACP**:



5. Нажмите **Далее** - тип кластерного соединения будет сохранен.

6. Вернитесь в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** и повторите действия из пункта 2-3 для другого порта.

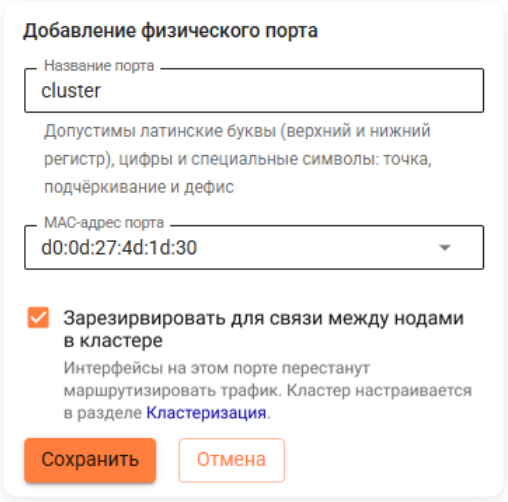
Шаг 2 - Конфигурация активной ноды

Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW Novum выполните действия:

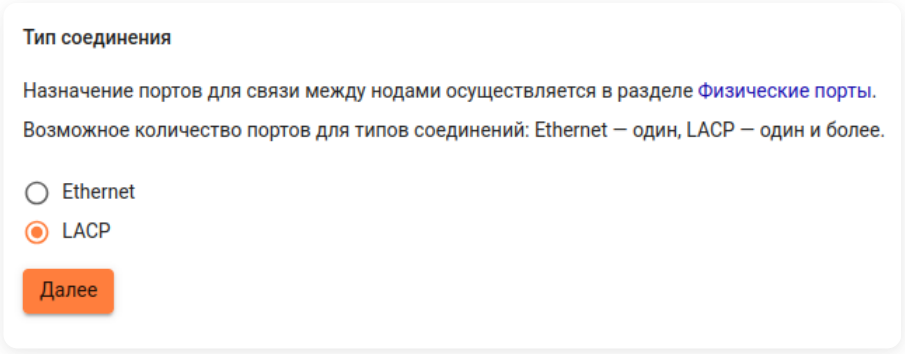
1. Перейдите в **Сервисы** → **Сетевые интерфейсы** → **Физические порты**.

2. Выберите физический порт, который планируете использовать для связи между нодами, и нажмите .

3. Включите опцию **Зарезервировать для связи между нодами в кластере** и нажмите **Сохранить**:



4. Перейдите в **Управление сервером** → **Кластеризация** и выберите тип кластерного соединения - **LACP**:

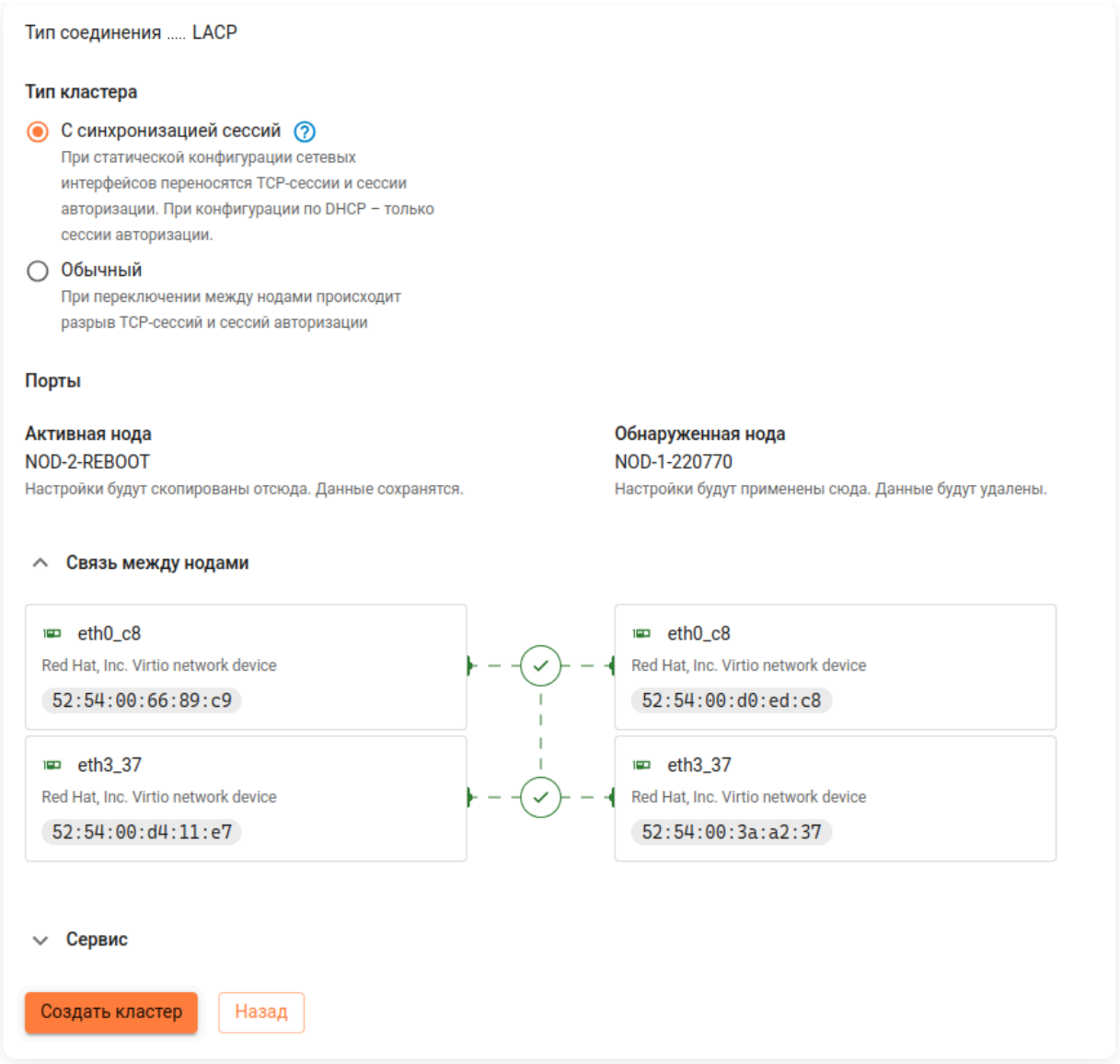


5. Нажмите **Далее** - тип кластерного соединения будет сохранен.

6. Вернитесь в **Сервисы** → **Сетевые интерфейсы** → **Физические порты** и повторите действия из пункта 2-3 для другого порта.

7. Перейдите в **Управление сервером** → **Кластеризация** и нажмите **Далее**.

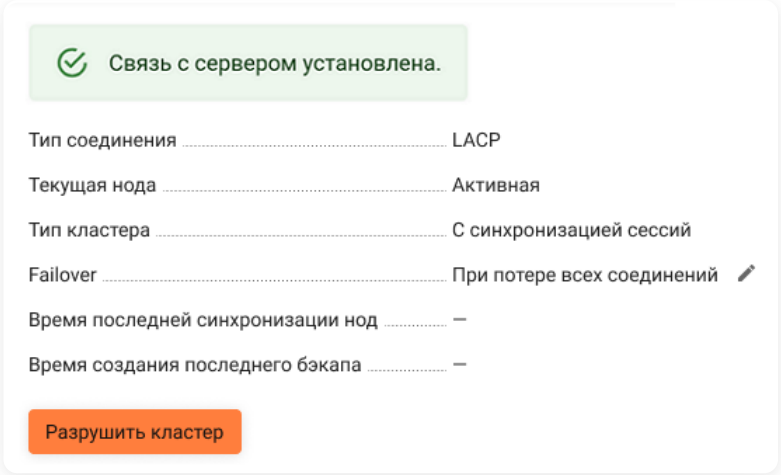
8. Выберите тип кластера и нажмите **Создать кластер**. Сетевые порты нод будут сопоставлены автоматически:



Если был настроен **Обычный** тип кластера, то при переключении между нодами происходит разрыв TCP-сессий пользователей и сессий авторизации.

Если был настроен тип кластера **С синхронизацией сессий**, то при статической конфигурации сетевых интерфейсов все TCP-сессии пользователей и сессии авторизации перенесутся на резервную ноду. При конфигурации по DHCP - перенесутся только сессии авторизации.

После применения настроек резервная нода перезагрузится, и в веб-интерфейсе активной ноды отобразится информация, что кластер создан:



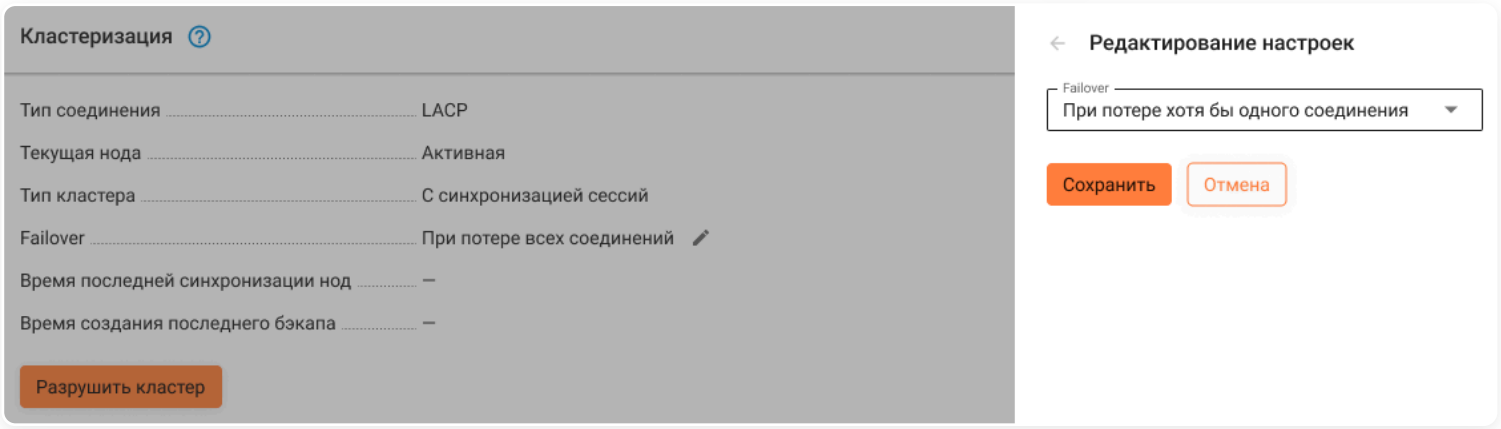
Во время перезагрузки резервной ноды в веб-интерфейсе активной ноды может временно отображаться статус о потере связи. Соединение восстановится автоматически после завершения загрузки резервной ноды.

Локальное меню резервной ноды доступно только в кластере **С синхронизацией сессий**.

В кластере **С синхронизацией сессий** доступна настройка **Failover**, которая определяет условие переключения на резервную ноду:

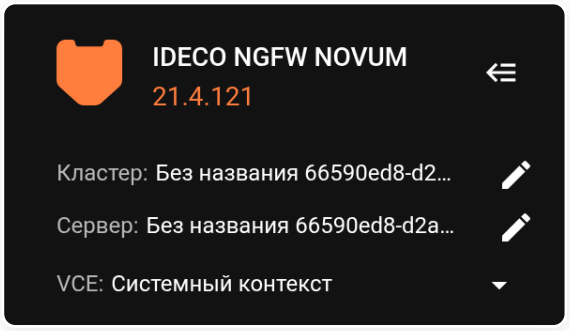
- При потере хотя бы одного соединения.
- При потере всех соединений.

По умолчанию установлено значение **При потере всех соединений**. Чтобы изменить значение, нажмите и отредактируйте настройку:



Изменение названия кластера и сервера

Название кластера или сервера можно изменить через веб-интерфейс активной ноды. Для этого нажмите на рядом с названием кластера или сервера в левом верхнем углу экрана:



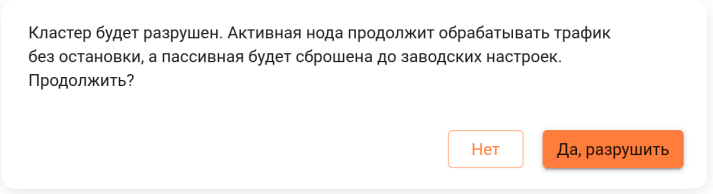
Разрушение кластера

Разрушить кластер можно только из активной ноды. При этом нода продолжит работать, а вторая нода (резервная) сбросит настройки до состояния только что установленного Ideco NGFW Novum. Для разрушения кластера:

В Веб-интерфейсе

1. Перейдите в **Управление сервером** → **Кластеризация** и нажмите кнопку **Разрушить кластер**.

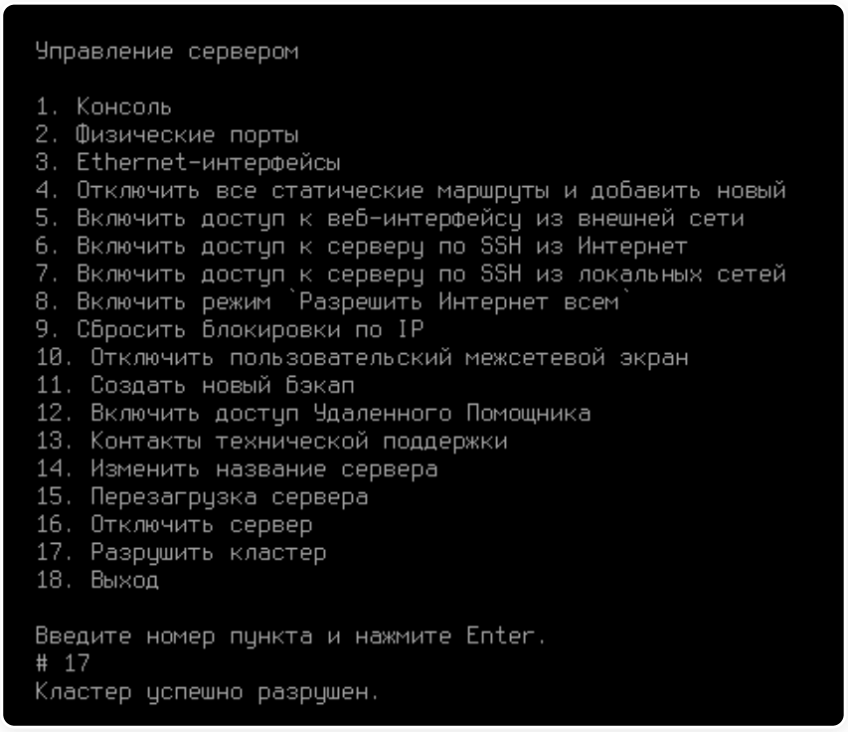
2. Появится окно с предупреждением:



3. Нажмите **Да, разрушить**.

В Локальном меню

В локальном меню резервной ноды выберите пункт **Разрушить кластер**:



Обновление кластера

Функциональность доступна в **Классическом** и **Системном контекстах**.

Процесс обновления Ideco NGFW Novum описан в статье **Обновления**.

Убедитесь в наличии лицензии на кластер.

Чтобы обновить NGFW до последней версии в режиме кластера, выполните действия:

1. Запустите обновление активной (первой) ноды в **Управление сервером** → **Обновление**. Сработает алгоритм обновления кластера Ideco NGFW Novum:

- Активная нода проверит время последней синхронизации и наличие лицензии на кластер.
- Если условия выполнены, активная нода установит обновление, перезагрузится и станет резервной.
- Вторая нода станет активной принудительно, скачает и установит обновления в автоматическом режиме.

Обновление активной ноды кластера будет заблокировано, если нода не синхронизирована с резервной нодой или с момента последней синхронизации прошло более 30 минут. Нода с младшей версией сможет обновиться без синхронизации. Это позволяет минимизировать потерю данных.

Для синхронизации оба устройства должны иметь одну версию системы, идентичную вплоть до номера сборки.

2. Дождитесь, пока вторая нода скачает и установит обновление. После завершения обновления кластер вновь будет работоспособен.

Обновления

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Обновления**: `ideco-sysupdate-backend`.

Список служб для других разделов доступен по ссылке.

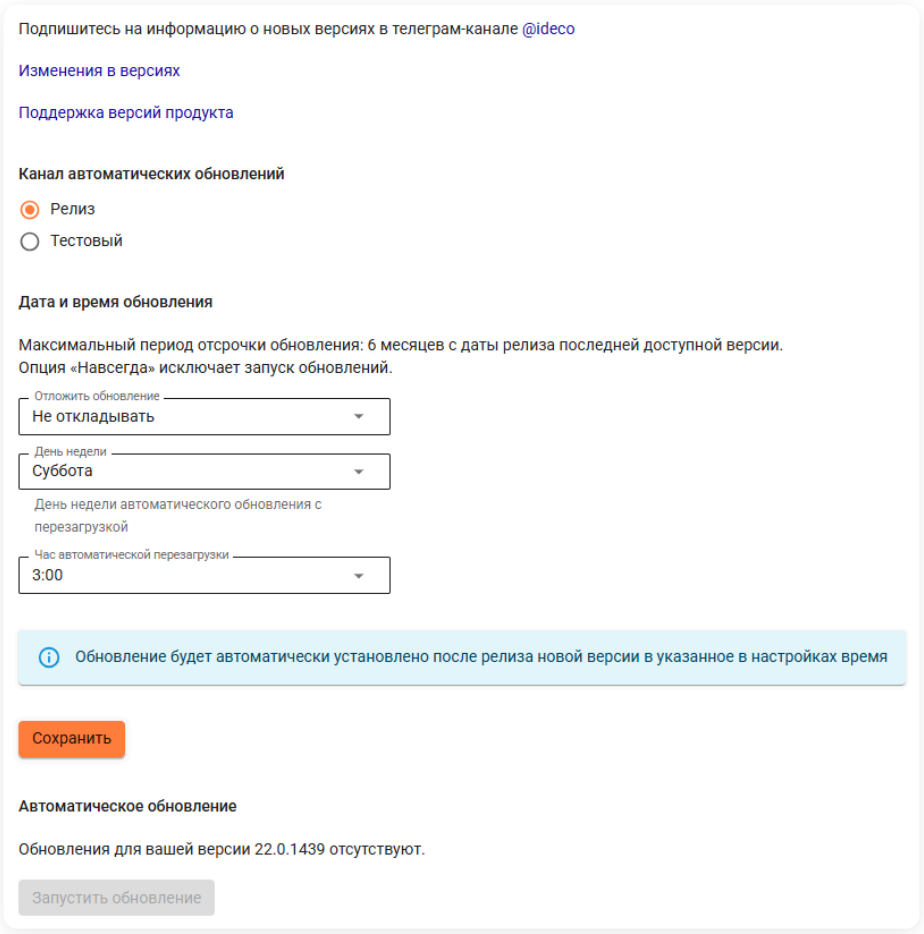
Система

Механизм обновления с версий Ideco UTM 7.9.9 - 14 описан в инструкции.

Обновить систему Ideco NGFW Novum можно как в офлайн-режиме, так и через интернет. Выбрать режим обновления можно в разделе **Управление сервером → Лицензия**.

Автоматическое обновление

Доступны настройки:



Расшифровка полей

- **Канал обновлений**:
  - **Релиз** - позволяет обновляться на стабильно работающие версии. Выбран по умолчанию.

    - **Тестовый** - позволяет быстрее обновляться как на релизные версии, так и на последние бета-версии продукта во время коротких периодов бета-тестирования новых мажорных версий.
- **Отложить обновления** - время, на которое будет отложено обновление. Максимальный срок - шесть месяцев с даты релиза последней версии, до которой доступно обновление.
- **День недели** - день недели запуска автоматического обновления.
- **Час автоматической перезагрузки** - час запуска автоматического обновления.
- **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

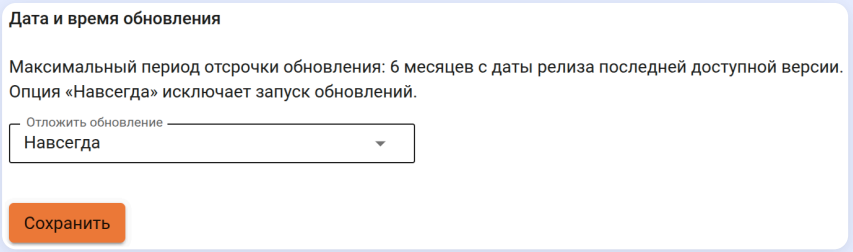
Кнопка **Запустить обновление** активна и только применяет обновление, когда оно уже скачано. Инициировать скачивание нельзя.

После принудительного обновления потребуется полная перезагрузка сервера.

По умолчанию сервер обновляется по субботам в 3:00 по часовому поясу, выбранному в настройках.

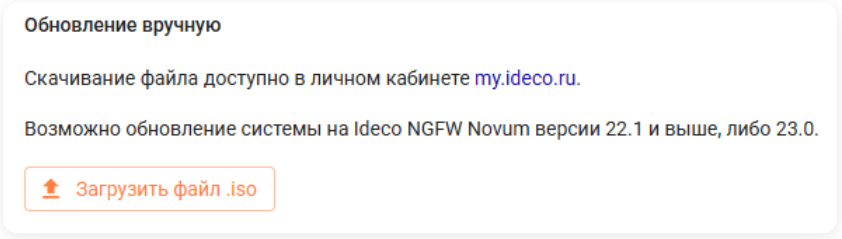
Обновление вручную

Чтобы обновлять Ideco NGFW Novum только вручную, в поле **Отложить обновление** выберите **Навсегда**:



Не рекомендуем отключать обновления, так как это приведет к пропуску важных улучшений и критических исправлений безопасности. Если автоматическое обновление отключено, регулярно проверяйте наличие новых версий.

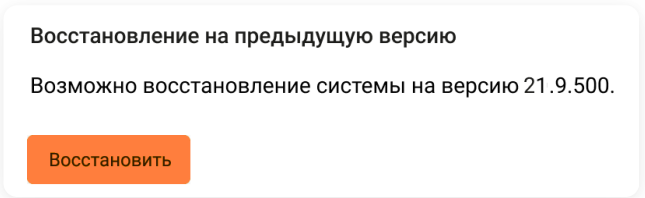
Для обновления необходимо скачать ISO-образ новой версии Ideco NGFW Novum в MY.IDECO и загрузить образ с внешнего носителя:



После проведения процедуры обновления новая версия будет отображаться в верхнем левом углу веб-интерфейса NGFW Novum.

Для обновления серверов Ideco NGFW Novum, подключенных к Ideco Center, перейдите в интерфейс NGFW Novum одним из способов, указанных в разделе Ideco Center.

Восстановление на предыдущую версию



Кнопка **Восстановить** позволяет вернуться к предыдущей версии NGFW Novum. Система будет перезагружена, при этом текущие настройки будут потеряны. После восстановления отложите автоматическое обновление.

При восстановлении системы все настроенные VCE с данными также откатятся к исходному состоянию.

Если в **Ideco NGFW Novum** настроен кластер, то в веб-интерфейсе будет отсутствовать пункт **Восстановление на предыдущую версию**.

При восстановлении на предыдущую версию данные перенесены не будут. NGFW Novum вернется в состояние, в котором был на момент обновления. Все изменения, внесенные после обновления, будут утеряны. Сохраните информацию на внешнем носителе, NGFW предоставляет возможность выгружать бэкапы на:

- Сетевое файловое хранилище по протоколу FTP.
- Сетевое файловое хранилище по протоколу NetBIOS (CIFS).
- ПК через кнопку **Скачать** в таблице бэкапов ( ) для переноса с сервера на иной внешний носитель вручную.

Бэкап можно восстановить только на версию NGFW Novum не ниже той, на которой был создан.

Процесс выхода релизов в каналы обновлений

Тестовый канал обновлений позволяет быстрее обновляться до новых версий (релизных или бета-версий во время активного тестирования). После выхода бета-версии NGFW Novum в **Тестовый** канал ожидается обратная связь от пользователей по использованию новой версии продукта. Обратная связь позволяет выявить недочеты и уязвимости в продукте. После исправления происходит выкладка в канал **Релиз**.

Если в версии NGFW Novum, вышедшей в канал **Релиз**, в ходе использования выявляются недочеты, то исправляются ближайшими обновлениями версии. Обновление в канале **Релиз** появляется постепенно.

Особенности обновления

NGFW Novum

- Обновление будет автоматически установлено в указанное в настройках время после релиза новой версии.
- Обновления можно отложить на срок до шести месяцев или навсегда. Если отложить обновление на определенный срок, то период будет отсчитываться от **даты релиза** последнего доступного обновления и корректироваться в соответствии с указанным для обновления днем недели.
- Даты релизов можно посмотреть на сайте или в документации в разделе Release notes.
- Номер мажорной версии NGFW Novum - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7).
- Автоматическое обновление Ideco NGFW Novum до следующей мажорной версии возможно только после установки последней минорной версии, выпущенной в релиз. Например, можно обновить NGFW Novum 17.2 до версии 17.9, а затем до версии 18.6.
- Ручное обновление Ideco NGFW Novum до следующей мажорной версии можно выполнить с любой версии. Например, можно обновить NGFW Novum 17.2 до версии 18.5.

Если обновление было отложено на шесть месяцев, но за это время вышел новый минорный релиз, дата обновления сдвигается. Шесть месяцев отсчитываются с даты выхода последнего доступного минорного релиза.

VCE

- При обновлении корневого NGFW Novum все включенные VCE автоматически обновляются вместе с корневым NGFW Novum.
- Если в системе есть выключенные VCE, которые созданы в младшей версии корневого NGFW Novum и не запускались после обновления, то обновление корневого NGFW Novum на следующую мажорную версию будет заблокировано.

Пример. Если в NGFW Novum версии 18.3 создали VCE, затем выключили его и обновили корневой NGFW Novum до 19.0, но сам VCE на 19.0 не включали, то переход с 19.0 на 20.0 будет заблокирован.

Включите все VCE для автоматического обновления до версии корневого NGFW Novum.

- Если VCE не включался после обновления корневого NGFW Novum, то:
  - VCE останется на предыдущей версии.
  - Корневой NGFW Novum можно обновить в рамках текущей мажорной версии.

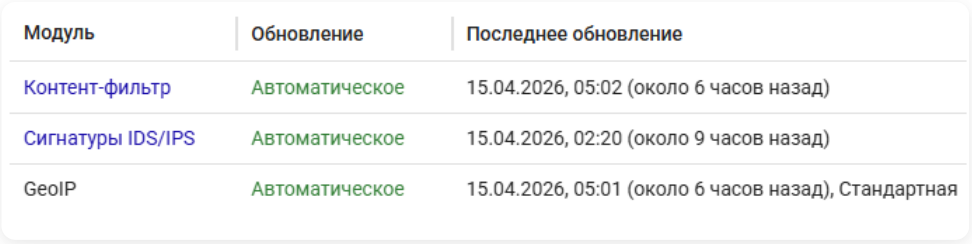
Пример. Корневой NGFW Novum можно обновить с 18.3 до 18.6, но выключенный VCE останется на 18.3.

Кластер

- Если активная нода кластера не синхронизирована с резервной или с момента последней синхронизации прошло более 30 минут, ее обновления будут заблокированы. Произойдет переключение нод кластера. Нода с младшей версией сможет обновиться без синхронизации.
- При офлайн-обновлении кластера с синхронизацией сессий обновления баз **Предотвращения вторжений**, **Контент-фильтра** и **Антивирусов веб-трафика** не синхронизируются, каждая нода обновляется отдельно. Вторая нода обновится после того, как станет активной.

Базы фильтрации

На вкладке **Базы фильтрации** отображается информация о последнем обновлении баз модулей фильтрации Ideco NGFW Novum: **Контент-фильтра**, **Предотвращения вторжений**, а также GeoIP (соответствия подсетей и стран):



Модуль	Обновление	Последнее обновление
Контент-фильтр	Автоматическое	15.04.2026, 05:02 (около 6 часов назад)
Сигнатуры IDS/IPS	Автоматическое	15.04.2026, 02:20 (около 9 часов назад)
GeoIP	Автоматическое	15.04.2026, 05:01 (около 6 часов назад), Стандартная

Обновить базы фильтрации Ideco NGFW Novum можно как в офлайн-режиме, так и по сети. Выбрать режим обновления можно в разделе **Управление сервером** → **Лицензия**.

Изменение источника баз GeoIP доступно только в **Системном контексте**.

Автоматическое обновление

1. В режиме **Автоматического обновления** выберите источник обновления баз GeoIP:

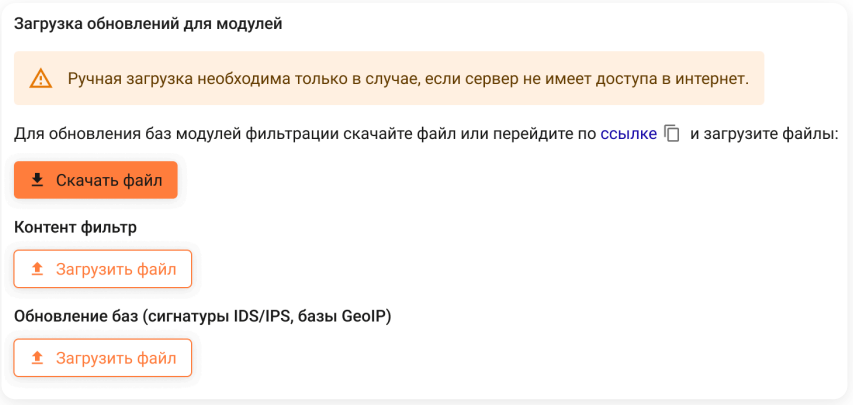


- **Стандартная** - международная база данных для определения геолокации по IP-адресам. Используется по умолчанию.
- **Минцифры** - база данных для определения стран, разработанная Министерством цифрового развития РФ.

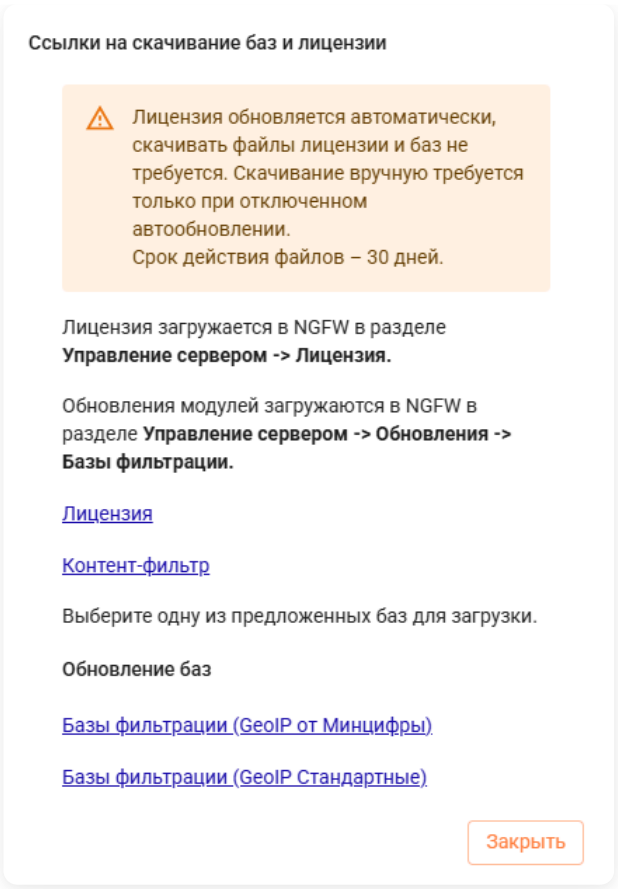
2. Нажмите **Сохранить**.

Изменения источника вступят в силу после подгрузки выбранной базы, источник отобразится в сведениях об обновлении в строке **GeoIP**.

В автоматическом режиме также доступно скачивание файлов для ручного обновления:



При переходе к скачиванию отобразится уведомление:



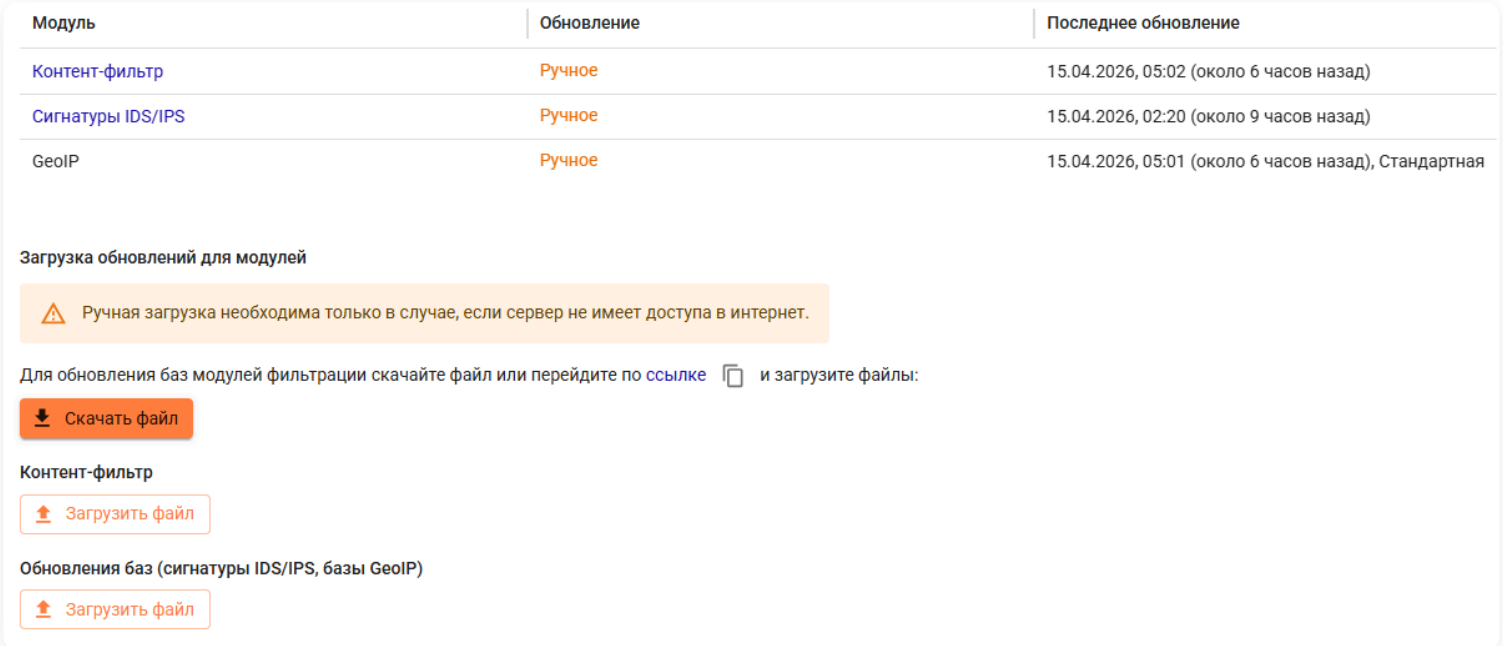
Ручное обновление

Базы фильтрации Ideco NGFW Novum могут меняться ежедневно, поэтому при ручной загрузке обновляйте базы как можно чаще.

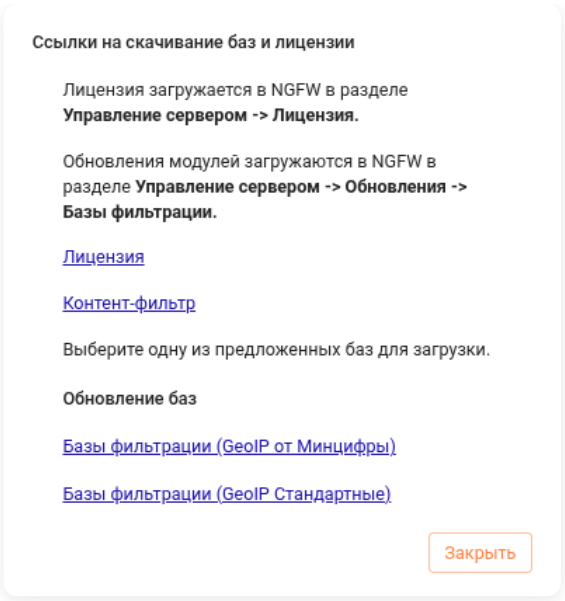
Ручная загрузка необходима только в случае, если сервер не имеет доступа в интернет, а в разделе **Управление сервером** → **Лицензия** выбран способ обновления **Ручная загрузка**.

Для загрузки файлов обновления баз на Ideco NGFW Novum выполните действия:

1. В интерфейсе Ideco NGFW Novum на вкладке **Управление сервером** → **Обновления** → **Базы фильтрации** скачайте файл или перейдите по ссылке:



2. Скачайте и загрузите файлы:



Если при скачивании Обновления баз (Предотвращение вторжений, базы GeoIP) через **Google Chrome** возникают проблемы, в настройках браузера разрешите **Небезопасный контент** для MY.IDECO.

Полезные ссылки

- **Источники данных**

Как восстановиться на прошлую версию после обновления Ideco NGFW Novum

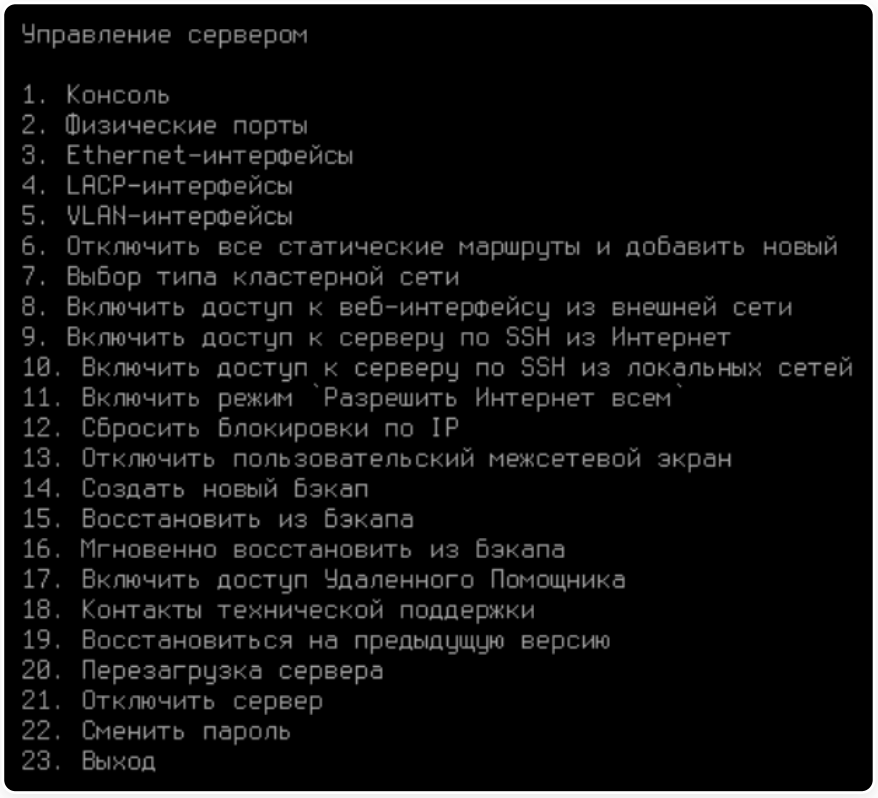
При восстановлении на предыдущую версию данные перенесены не будут. Сохраните бэкап на внешнем носителе. Информация о работе с API бэкапа описана в статье Бэкап.

Для восстановления на предыдущую версию выполните действия:

1. Перейдите в локальное меню Ideco NGFW Novum.

2. Введите логин и пароль администратора.

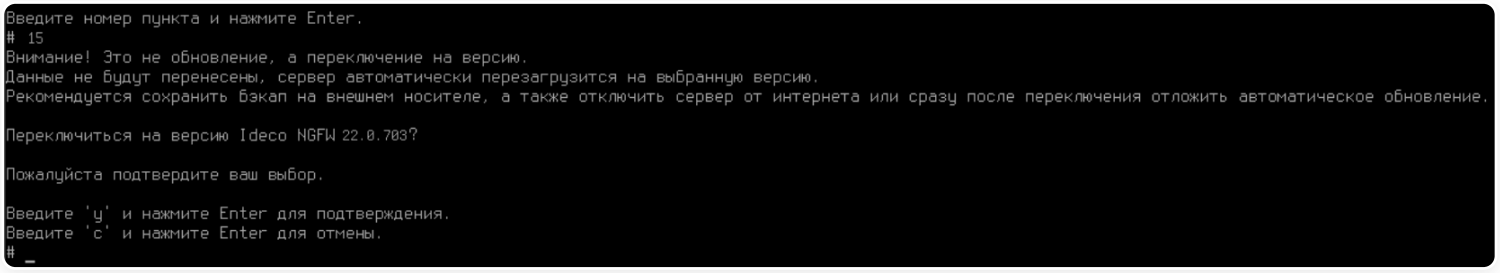
3. Укажите номер пункта **Восстановиться на предыдущую версию** и нажмите Enter:



Появится окно с предупреждением и описанием версии, на которую произойдет переключение.

> Если в Ideco NGFW Novum настроен кластер, то в локальном меню будет отсутствовать пункт **Восстановиться на предыдущую версию**.

3. Подтвердите выбор, введя y и нажав Enter:



4. После перезагрузки Ideco NGFW Novum переключится на предыдущую версию.

Бэкапы

Классический контекст | Высокопроизводительный контекст | API

Название служб раздела **Бэкапы**: `ideco-backup-backend`, `ideco-backup-create`, `ideco-backup-restore`, `ideco-backup-rotate`.

Список служб для других разделов доступен по ссылке.

Бэкап - это предварительно созданная резервная копия данных, позволяющая восстановить большинство настроек и сохраненной информации.

В NGFW Novum создается только полный бэкап, который включает все настройки, созданные администратором в веб-интерфейсе.

Бэкапы не включают:

- Системный журнал.
- Почту.
- Статистику web-трафика и другие отчеты.
- Любые кешируемые данные, базы антивирусов, правила IPS и т. п.
- Настройки созданных VCE.
- Любые данные, генерируемые в процессе работы системы автоматически.

В бэкап системного VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте отдельный бэкап системного VCE и каждого из дочерних VCE.

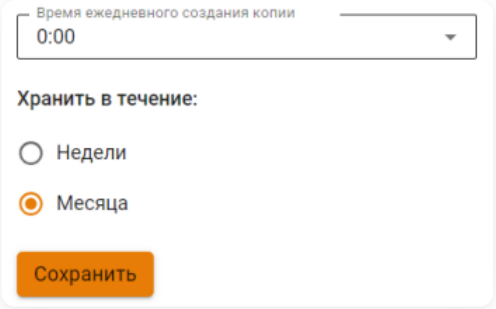
В NGFW Novum бэкап создается как автоматически, так и вручную.

Не рекомендуем использовать один и тот же бэкап для клонирования серверов. Это приведет к конфликту идентификаторов серверов и проблемам с подключением к Ideco Center, интеграцией с внешними системами (например, Active Directory, ALD), корректностью отчетности и т.д.

Интеграция с AD, ALD может перестать работать, если вы производите откат на предыдущую версию или разворачиваете старый бэкап, в котором присутствует устаревшая информация для аутентификации NGFW Novum на контроллере домена. При каждом изменении настроек интеграции информация для аутентификации NGFW Novum обновляется. Для решения проблемы интеграции NGFW Novum с AD, ALD сделайте переинтеграцию NGFW Novum с соответствующим сервисом.

Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в **Управление сервером** → **Бэкапы** → **Настройки**:



Установите время ежедневного создания и продолжительность хранения бэкапа на локальном жестком диске. При настройке выгрузки на сетевое файловое хранилище автоматический бэкап будет также дублироваться туда.

- **Время ежедневного создания копии** - укажите в настройках час. Рекомендуется выбирать ночное время для создания бэкапа.
- **Хранить в течение** - выберите срок хранения. Хранить бэкапы на локальном жестком диске можно в течение недели или месяца.

> Каждый автоматически созданный бэкап сохраняется в таблице бэкапов с комментарием **Автоматическая резервная копия**.

Рекомендуется хранить бэкапы не только на локальном жестком диске, но и на внешних носителях. NGFW Novum предоставляет возможность выгружать бэкапы на:

- Сетевое файловое хранилище по протоколу FTP.
- Сетевое файловое хранилище по протоколу NetBIOS (CIFS).
- ПК через кнопку **Скачать** в таблице бэкапов для переноса с сервера на иной внешний носитель вручную.

Для проверки корректности настройки сохранения бэкапов на FTP-сервере или в общей папке CIFS введите команду `ideco-backup-create` в терминале Ideco NGFW Novum. Команда создает автоматический бэкап в соответствии с заданными настройками сохранения.

> При настройке бэкапов указывайте путь к каталогу в UNIX-формате. Например, если в ОС Windows каталог открывается по пути `\\192.168.1.1\dir_1\dir_2\backup`, то в поле **Путь к каталогу** пропишите `dir_1/dir_2/backup`.

Бэкапы на удаленное файловое хранилище по протоколу FTP

Ключевые параметры, необходимые для настройки бэкапа на FTP-сервер, описаны в таблице:

Параметр	Описание
Адрес сервера	IP-адрес удаленного FTP-сервера, на котором будут размещаться бэкапы
Логин	Имя пользователя для авторизации на FTP-сервере
Пароль	Пароль для авторизации на FTP-сервере
Путь к каталогу	Каталог, в который будут записываться бэкапы

Бэкапы на сетевое файловое хранилище по протоколу NetBIOS (CIFS)

Ключевые параметры, необходимые для настройки бэкапа на NetBIOS-сервер, описаны в таблице:

Параметр	Описание
Адрес сервера	IP-адрес удаленного NetBIOS-сервера, на котором будут размещаться бэкапы
Логин	Имя пользователя для авторизации на сетевом ресурсе Windows
Пароль	Пароль для авторизации на сетевом ресурсе Windows
Путь к каталогу	Каталог, в который будут записываться бэкапы

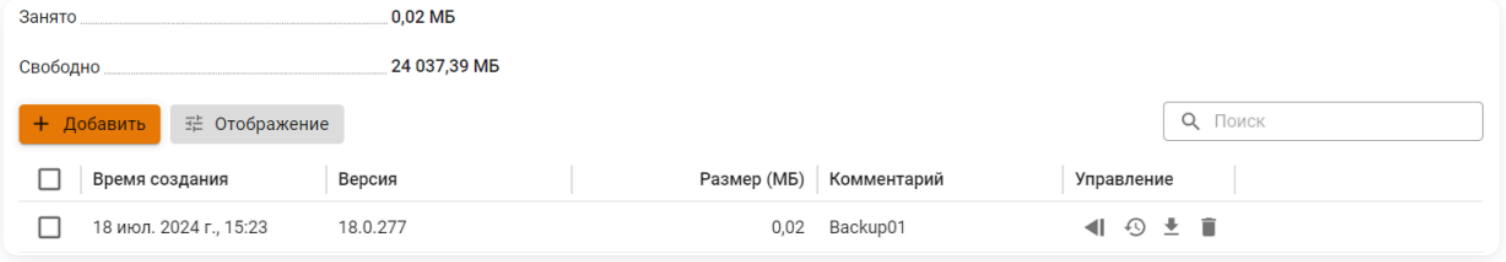
Ручное создание бэкапа

Через веб-интерфейс

Для создания бэкапа через интерфейс Ideco NGFW Novum выполните одно из действий:

- Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и нажмите **Добавить** → **Создать**.
- Нажмите **Создать бэкап** в правом верхнем углу веб-интерфейса.

Введите комментарий или оставьте поле пустым, нажмите **Создать**. Новый бэкап появится в таблице:



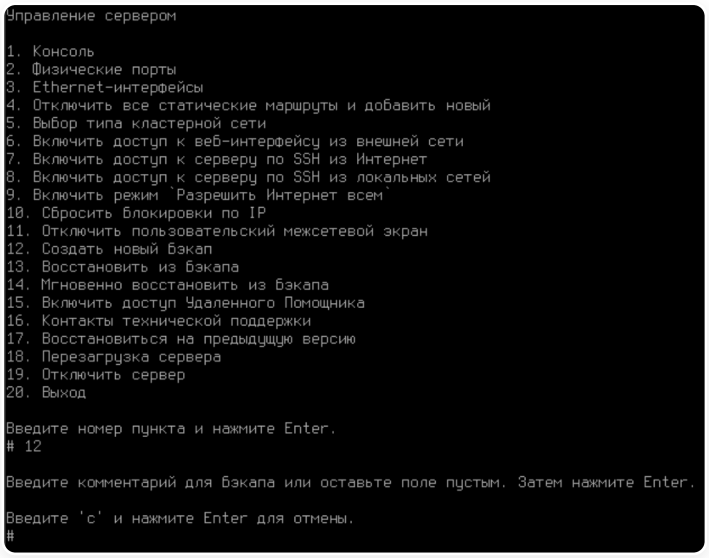
Через локальное меню

Чтобы создать новый бэкап через локальное меню Ideco NGFW Novum, выполните действия:

1. Выберите пункт **Создать новый бэкап** и нажмите **Enter**.

2. Введите комментарий для бэкапа и нажмите **Enter**.

Пример создания бэкапа через локальное меню приведен на скриншоте ниже:



Настройка сохранения бэкапа в сетевом файловом хранилище возможна только через веб-интерфейс Ideco NGFW Novum. Выгрузка на внешние сетевые хранилища производится только при автоматическом создании бэкапа.

Полезные ссылки

- **Восстановление конфигурации из бэкапа**

Терминал

Классический контекст | Высокопроизводительный контекст

Используйте терминал только для диагностики. Воздержитесь от команд, изменяющих файлы. Система рассчитана на настройку только через веб-интерфейс. Компания "Айдеко" не несет ответственности за негативные последствия работы с Ideco NGFW из терминала. Техническая поддержка вправе отказать в обслуживании, если окажется, что работа системы была нарушена из-за действий пользователя в терминале.

Основные команды

- **Утилиты сетевой диагностики:** `ping`, `host`, `nslookup`, `tracepath`, `tcpdump`, `arping`, `ss` (аналог `netstat`).
- **Файловый редактор:** `nano`.
- **Просмотр логов:** `journalctl -u <название службы>` (например, `journalctl -u ideco-routing-backend`).
- **Разблокировка в случае срабатывания защиты от брутфорс-атак:**
  - `fail2ban-client unban --all` - команда используется для снятия всех блокировок.
  - `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса. Укажите нужный IP-адрес в качестве аргумента.
- **Просмотр конфигурации FRR:** `vtysh`.
- **Просмотр системных правил Межсетевого экрана:**
  - `iptables -L |grep fwd.sys.<id правила>` - для просмотра системных правил FORWARD.
  - `iptables -L |grep inp.sys.<id правила>` - для просмотра системных правил INPUT.
  - `iptables -L -v` - для полного вывода всех цепочек системных правил со статистикой по каждому правилу.

Перечень цепочек системных правил

- `Chain forward_sys_rules` - системные FORWARD-правила, находятся перед пользовательскими.
- `Chain forward_user_rules_before` - пользовательские FORWARD-предправила от Ideco Center, находятся перед локальными пользовательскими.
- `Chain forward_user_rules` - пользовательские FORWARD-правила.
- `Chain forward_user_acl_rules` - правила списков ACL (через API).
- `Chain forward_user_rules_after` - пользовательские FORWARD-постправила от Ideco Center, находятся после локальных пользовательских.
- `Chain input_sys_rules` - системные INPUT-правила.
- `Chain input_sys_rules_E` - системные правила фильтрации для WAN-интерфейсов.
- `Chain input_user_rules_before` - пользовательские INPUT-предправила от Ideco Center, находятся перед локальными пользовательскими.
- `Chain input_user_rules` - пользовательские INPUT-правила.
- `Chain input_user_rules_after` - пользовательские INPUT-постправила от Ideco Center, находятся после локальных пользовательских.
- `Chain input_reject` - цепочка для отправки RST- или ICMP-ответа при блокировке.
- `Chain input_drop` - цепочка для дропа пакета при блокировке.
- `Chain preinput_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК перед INPUT.
- `Chain preinput_fstek_rules_log_bf` - опциональные правила по нормативам ФСТЭК для логирования BADFLAGS.
- `Chain input_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК на INPUT.
- `Chain forward_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК на FORWARD.
- `Chain output_fstek_rules` - опциональные правила защиты по нормативам ФСТЭК на OUTPUT.
- `Chain ips_nfq_rules` - цепочка для работы профилей IPS.
- `Chain l7_inspection` - цепочка, в которую перенаправляется трафик при срабатывании правила с действием **Разрешить**, если к нему применены профили DPI/IPS для проверки.
- `Chain fail2ban` - блокировки fail2ban по IP-адресу.
- `Chain filter_dns` - функциональность перехвата DNS-запросов.
- `Chain filter_log_user_rules` - пользовательские правила логирования соединения.
- `Chain set_log_mark_chain` - настройка логирования соединения.
- `Chain clear_log_mark_chain` - очистка логирования соединения.

- `Chain log_accept` - цепочка для разрешающего правила или разрешающей политики.
- `Chain smart_drop` - цепочка, в которую перенаправляется трафик при срабатывании правила с действием **Отбросить** (без отправки RST).
- `Chain smart_reject` - цепочка, в которую перенаправляется трафик при срабатывании правила с действием **Запретить** (с отправкой RST).
- **Вызов локального меню:** `ideco-local-menu --debug` - команда используется для доступа к локальному меню Ideco NGFW Novum.

Для просмотра подсказки по всем командам введите : `ideco-vppctl ?`

- **Просмотр списка всех физических интерфейсов, соответствующих сетевой карте:** `ideco-vppctl show hardware-interface brief`.
- **Просмотр списка всех сетевых интерфейсов, через которые проходит трафик:** `ideco-vppctl show interface`.
- **Просмотр списка всех IP-адресов интерфейсов:** `ideco-vppctl show interface addr`.
- **Просмотр таблицы маршрутизации:** `ideco-vppctl show ip fib`.
- **Запись последних 100 сетевых пакетов, прошедших через шлюз:** `ideco-vppctl pcap trace rx tx intfc any file capture.pcap`.
- **Просмотр ARP-таблицы:** `ip neigh show`.

Таблица служб

Модуль	Имя службы
ALD Pro	ideco-ald-rest, ideco-ald-backend
Active Directory	ideco-ad-log-collector, ideco-ad-backend
BGP, OSPF	ideco-routing-rest, ideco-routing-backend, frr
Веб-интерфейс администратора	nginx-control-plane (порты 8443 и 82)
DNS	unbound-keygen, unbound-anchor, unbound, nsd, ideco-dns-backend
DDNS	ideco-dns-backend
DHCP	ideco-dhcp-server-backend
Обратный прокси	nginx-data-plane (порты 443 и 80)
IGMP Proxy	ideco-igmpproxy-rest, ideco-igmpproxy-backend
IPsec	ideco-ipsec-backend
Ideco Center	ideco-central-console-backend
Ideco Client	ideco-websocket-vpn-server, ideco-agent-websocket, ideco-agent-backend
NTP	chronyd
Syslog	ideco-monitor-backend, ideco-logs-backend
VCE	ideco-vce-rest, ideco-vce-backend
VPN-подключения	pcscd, ideco-vpn-sessions-sync, ideco-vpn-servers-backend, ideco-vpn-netns, ideco-vpn-dhcp-backend, ideco-vpn-authd, ideco-gost-vpn-rest, ideco-gost-vpn-backend, ideco-accel-sstp, ideco-accel-l2tp, strongswan
Web Application Firewall	ideco-waf-event-syncer, ideco-waf-backend
Авторизация	ideco-auth-backend
Антивирус	klmsinit, kav-scanner, ideco-av-backend
Профили next hop, Маршрутизация	ideco-routing-backend
Бэкапы	ideco-backup-rotate, ideco-backup-restore, ideco-backup-create, ideco-backup-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-backend, ideco-web-authd
Дополнительно	ideco-system-swap, ideco-system-backend
Кластеризация	ideco-cluster-backup-pusher, ideco-cluster-backend
Контент-фильтр	ideco-content-filter-backend
Лицензия	ideco-license-backend
Межсетевой экран	ideco-fw-stats, ideco-firewall-rest, ideco-firewall-backend, ideco-apply-manual-blocklist, ideco-acl-rest, ideco-acl-backend, ideco-nflog
Обновления	ideco-sysupdate-backend
Обнаружение устройств	ideco-netscan-backend
Объекты	ideco-alias-backend
Обратный прокси	ideco-reverse-backend

Модуль	Имя службы
Ограничение скорости	ideco-shaper-backend
Отчеты и журналы	ideco-reports-backend, ideco-logs-syncer, ideco-logs-backend, ideco-audit-backend
Предотвращение вторжений	ideco-suricata-profiles-syncer, ideco-suricata-event-syncer, ideco-suricata-backend, ideco-suricata
Прокси	squid, ideco-proxy-backend
Профили контроля приложений	ideco-app-stats, ideco-app-control-nfq, ideco-app-backend
Сертификаты	ideco-cert-backend
Сетевые интерфейсы	ideco-l2manager-rest, ideco-l2manager-l2migration, ideco-l2manager-dhclient, ideco-l2manager-backend, ideco-l2-manager

Служебные:

Модуль	Имя службы
API	ideco-rest-api-backend
MY.IDECO	ideco-mir-alerts
Базовая система и менеджер сессий (systemd)	user, var-log-journal, systemd-udevd, systemd-tmpfiles-setup, systemd-sysctl, systemd-oomd, systemd-nsresourced, systemd-modules-load, systemd-machined, systemd-logind, systemd-journald, systemd-hostnamed, systemd-homed, systemd-coredump, systemd-boot-random-seed, init
Демон для работы RDP в SSL VPN	guacd
Инженерная панель	ideco-engineering-panel-backend
Контроль целостности системы	ideco-check-sums
Локальная база данных	ideco-etcd-runtime-defrag, ideco-etcd-runtime, ideco-etcd-permanent-defrag, ideco-etcd-permanent
Локальное меню	ideco-local-menu
Настройка системы в облачных развертываниях	ideco-vk-cloud-license, ideco-cloud-init-backend
Проверка прав пользователей на перезапуск служб systemd	ideco-policy-backend
Ранняя инициализация системы	dracut-initqueue, dracut-cmdline
Сбор метрик и статистики	prometheus-node-exporter, prometheus, ideco-gatherstat-backend
Сервер базы данных	clickhouse-server
Системная шина	dbus-broker
Создание дампов ядра в случае падения	kdump
Управление томами	lvm2-monitor, lvm-activate-utm_421259

Примеры использования утилит

Классический контекст | Высокопроизводительный контекст

Примеры использования утилиты vtysh

Просмотр таблицы маршрутизации

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра таблицы маршрутизации введите:

```
show ip route
```

Пример вывода утилиты:

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 1.1.1.1/32 [1/0] via 10.10.10.1, Leth1, weight 1, 00:02:32
O   10.10.10.0/24 [110/1] is directly connected, Leth1, weight 1, 00:02:28
C>* 10.10.10.0/24 is directly connected, Leth1, 00:02:33
C>* 10.11.12.0/25 is directly connected, Eeth2, 00:02:33
O>* 10.20.40.0/24 [110/21] via 10.10.10.201, Leth1, weight 1, 00:02:18
S>* 10.128.0.0/16 [1/0] is directly connected, Lvpn0, weight 1, 00:02:32
C>* 169.254.1.0/29 is directly connected, lb_local_in, 00:02:33
C>* 169.254.1.0/29 is directly connected, lb_local_out, 00:02:33
C>* 169.254.1.4/32 is directly connected, Lvpn0, 00:02:33
C>* 169.254.254.254/32 is directly connected, lo, 00:02:33
```

Полезная информация:

- Не все маршруты могут быть выгружены в ядро, поэтому при просмотре таблицы маршрутизации без утилиты `vtsyh` некоторые маршруты могут не отображаться.
- Для просмотра примененных маршрутов введите:

```
ip route show table 230
```

Просмотр конфигурации FRR

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра конфигурации введите:

```
show running-config
```

Пример вывода утилиты:

```
Building configuration...

Current configuration:
!
frr version 8.5.3
frr defaults traditional
hostname bez-nazvaniya-23000007-c6d8-01c2-a572-d68497c66441
no ipv6 forwarding
service integrated-vtysh-config
!
ip route 10.128.0.0/16 Lvpn0
!
interface Leth1
 ip ospf cost 125
exit
!
interface lo
 ip ospf passive
exit
!
router ospf
 ospf router-id 192.168.0.200
 redistribute connected
 redistribute static
 network 172.16.10.0/24 area 0.0.0.200
 default-information originate always
exit
!
ip prefix-list DEFAULT seq 5 deny 0.0.0.0/0
ip prefix-list DEFAULT seq 10 permit 0.0.0.0/0 le 32
!
route-map DEFMAP permit 10
 match ip address prefix-list DEFAULT
exit
!
ip protocol ospf route-map DEFMAP
!
end
```

Просмотр OSPF соседства

Убедитесь, что включен модуль OSPF.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей OSPF введите:

```
show ip ospf neighbor
```

Пример вывода утилиты:

```
Neighbor ID     Pri State           Up Time         Dead Time Address         Interface                         RXmtL RqstL DB
10.10.10.201      1 Full/DR         6m35s             34.709s 10.10.10.201    Leth1:10.10.10.126                    0     0
```

Просмотр BGP соседства

> Убедитесь, что включен модуль BGP.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей BGP введите:

```
show ip bgp neighbors
```

Пример вывода утилиты:

```
BGP neighbor is 10.10.10.2, remote AS 123, local AS 123, internal link
  Local Role: undefined
  Remote Role: undefined
 Member of peer-group V4_AS123_10_10_10_2 for session parameters
  BGP version 4, remote router ID 10.11.12.2, local router ID 10.11.12.71
  BGP state = Established, up for 00:00:10
  Last read 00:00:10, Last write 00:00:09
  Hold time is 180 seconds, keepalive interval is 60 seconds
  Configured hold time is 180 seconds, keepalive interval is 60 seconds
  Configured conditional advertisements interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Extended Message: advertised
    AddPath:
      IPv4 Unicast: RX advertised
    Long-lived Graceful Restart: advertised
    Route refresh: advertised and received(new)
    Enhanced Route Refresh: advertised
    Address Family IPv4 Unicast: advertised and received
    Hostname Capability: advertised (name: bez-nazvaniya-5f3323c3-6462-4981-b8a0-2b4397e3448a,domain name: n/a) not received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 0 seconds
      Address families by peer:
        none
  Graceful restart information:
    End-of-RIB send: IPv4 Unicast
    End-of-RIB received:
    Local GR Mode: Helper*

    Remote GR Mode: Helper

    R bit: False
    N bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
    IPv4 Unicast:
      F bit: False
      End-of-RIB sent: Yes
      End-of-RIB sent after update: Yes
      End-of-RIB received: No
      Timers:
        Configured Stale Path Time(sec): 360
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
```

```
    Opens:                  1         1
    Notifications:          0         0
    Updates:                1         3
    Keepalives:             1         2
    Route Refresh:          0         0
    Capability:             0         0
    Total:                  3         6
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  V4_AS123_10_10_10_2 peer-group member
  Update group 1, subgroup 1
  Packet Queue length 0
  NEXT_HOP is always this router
  Community attribute sent to this neighbor(all)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *IMPORT_V4_AS123_10_10_10_2
  Route map for outgoing advertisements is *EXPORT_V4_AS123_10_10_10_2
  12 accepted prefixes

  Connections established 1; dropped 0
  Last reset 00:05:26,  No AFI/SAFI activated for peer
  Internal BGP neighbor may be up to 255 hops away.
Local host: 10.10.10.126, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 38445
Nexthop: 10.10.10.126
Nexthop global: ::
Nexthop local: ::
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Estimated round trip time: 1 ms
Read thread: on  Write thread: on  FD used: 25
```

Примеры использования утилиты iptables

Просмотр системного правила INPUT

Пример просмотра правила с `id=59` для опции **Полный доступ**.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
iptables -L |grep inp.sys.59
```

3. Пример ответа на запрос:

```
-A INPUT -m condition --condition emergency_internet_access -m logger --mask 268435456 --value 268435456 --prefix inp.sys.59,
```

- `-A INPUT` - цепочка правил INPUT (для соединений с самим NGFW);
- `-m condition --condition emergency_internet_access` - условие для активации правила. Специфичное для Ideco NGFW Novum;
- `-m logger --mask 268435456 --value 268435456 --prefix inp.sys.59,accept` - уникальная метка правила, отличающая его от других в модуле **Тестирование правил**. Специфичное для Ideco NGFW Novum;
- `-j` - действие, специфичное для Ideco NGFW Novum. Возможные варианты:
  - `log_accept` - если включено логирование, залогировать и разрешить;
  - `smart_reject` - отбросить.

Правила могут быть более сложными. При необходимости дополнительную информацию можно найти в документации к iptables.

Просмотр системного правила FORWARD

Пример просмотра правила с `id=15` для опции **Блокировать протоколы QUIC и HTTP/3**.

1. Перейдите в **Управление сервером** → **Терминал**.

2. Введите в терминале:

```
iptables -L |grep fwd.sys.15
```

3. Пример ответа на запрос:

```
-A forward_sys_rules -p udp -m multiport --dports 80,443 -m condition --condition "quic_reject"  -m logger --mask 268435456 -
```

- `-A forward_sys_rules` - системное правило FORWARD;
- `-p udp` - протокол UDP;
  - `--dports 80,443` - порт назначения `80` или `443`;
- `-m condition --condition "quic_reject"` - условие для активации правила. Специфичное для Ideco NGFW Novum;
- `-m logger --mask 268435456 --value 268435456 --prefix fwd.sys.15,drop` - уникальная метка правила, отличающая его от других в модуле **Тестирование правил**. Специфичное для Ideco NGFW Novum;
- `-j` - действие, специфичное для Ideco NGFW Novum. Возможные варианты:
  - `log_accept` - если включено логирование, залогировать и разрешить;
  - `smart_reject` - отбросить.

Правила могут быть более сложными. При необходимости дополнительную информацию можно найти в документации к iptables.

Анализ трафика

Используйте утилиту `tcpdump` для анализа трафика на NGFW в разделе **Управление сервером → Терминал**.

Утилита `tcpdump` предустановлена в продукт Ideco NGFW Novum.

При запуске утилиты без каких-либо ключей/параметров произойдет перехват всех пакетов через первый доступный сетевой интерфейс (петлевые интерфейсы игнорируются). Отобразить список интерфейсов можно командой `tcpdump -D`. Для просмотра всех ключей утилиты введите `tcpdump -h`.

Для более гибкого использования утилиты используйте комбинацию ключей. **Например**, чтобы вывести пять пакетов с интерфейса `eth1`, введите:

```
tcpdump -i eth1 -c 5
```

Ключи и примеры команд для утилиты tcpdump

Использование tcpdump с применением ключей

Просмотр списка сетевых интерфейсов

Введите в терминале:

```
tcpdump -D
```

Пример вывода утилиты:

```
1.eth0
2.nflog (Linux netfilter log (NFLOG) interface)
3.nfqueue (Linux netfilter queue (NFQUEUE) interface)
4.eth1
5.any (Pseudo-device that captures on all interfaces)
6.lo [Loopback]
```

Захват пакетов, проходящих через определенный интерфейс

Введите в терминале для просмотра пакетов с интерфейса `eth1`:

```
tcpdump -i eth1
```

Пример вывода утилиты:

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
01:06:09.278817 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761, seq 1, length 64
01:06:09.279374 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 4761, seq 1, length 64
01:06:10.281142 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761, seq 2, length 6
```

Полезная информация:

- Ключ `-v` увеличивает количество отображаемой информации о пакетах (добавляется протокол, флаги пакета).
- Ключ `-vv` дает еще более подробную информацию (полный разбора пакета и вывод в терминал).

Пример использования с ключами:

```
tcpdump -i eth1 -v
```

```
tcpdump -i eth1 -vv
```

Вывод и захват только определенного числа пакетов

Введите в терминале для разбора пяти пакетов с интерфейса по-умолчанию:

```
tcpdump -c 5
```

Пример вывода утилиты:

```
04:19:07.675216 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 2186733178:2186733278, ack 204106815, win 37232, length 100
04:19:07.675497 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 100, win 65535, length 0
04:19:07.675747 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 100:136, ack 1, win 37232, length 36
04:19:07.675902 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 136, win 65535, length 0
04:19:07.676142 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 136:236, ack 1, win 37232, length 100
5 packets captured
```

Использование tcpdump с применением фильтров

Список часто используемых фильтров `tcpdump`:

- `port` - фильтрация пакетов по номеру порта.
- `host` - фильтрация исходящих и входящих пакетов по IP-адресу.
- `src` - фильтрация пакетов по IP-адресу источника.
- `dst` - фильтрация пакетов по IP-адресу назначения.

Для фильтрации по определенному протоколу укажите протокол в качестве фильтра:

- `tcp` - фильтрация пакетов `TCP`.
- `udp` - фильтрация пакетов `UDP`.
- `icmp` - фильтрация пакетов `ICMP`.
- `arp` - фильтрация пакетов `ARP`.

Для комбинирования фильтров используйте логические операторы:

- `and` - пакет выведется при совпадении условий у всех указанных фильтров.
- `or` - пакет выведется при совпадении условий у одного указанного фильтра.
- `not` - инвертирует условие фильтра.

Фильтрация пакетов по 80 порту

Введите в терминале:

```
tcpdump port 80
```

Пример вывода утилиты:

```
23:54:24.978612 IP 10.0.0.1.53971 > 10.0.0.50.80: Flags [SEW], seq 53967733, win 65535, options [mss 1460,nop,wscale 5,nop,no
23:54:24.978650 IP 10.0.0.50.80 > 10.0.0.1.53971: Flags [S.E], seq 996967790, ack 53967734, win 28960, options [mss 1460,sack
23:54:24.978699 IP 10.0.0.1.53972 > 10.0.0.50.80: Flags [SEW], seq 226341105, win 65535, options [mss 1460,nop,wscale 5,nop,n
23:54:24.978711 IP 10.0.0.50.80 > 10.0.0.1.53972: Flags [S.E], seq 1363851389, ack 226341106, win 28960, options [mss 1460,sa
```

Фильтрация пакетов по хосту с IP-адресом 10.0.2.15

Введите в терминале:

```
tcpdump host 10.0.2.15
```

Пример вывода утилиты:

```
03:48:06.087509 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 3862934963:3862934999, ack 65355639, win 37232, length 36
03:48:06.087806 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 36, win 65535, length 0
03:48:06.088087 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 36:72, ack 1, win 37232, length 36
```

```
03:48:06.088274 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 72, win 65535, length 0
03:48:06.088440 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 72:108, ack 1, win 37232, length 36
```

Фильтрация пакетов по IP-адресу назначения 8.8.8.8

Введите в терминале:

```
tcpdump dst 8.8.8.8
```

Пример вывода утилиты:

```
17:32:19.642154 IP desktop > dns.google: ICMP echo request, id 1, seq 1, length 64
17:32:20.644231 IP desktop > dns.google: ICMP echo request, id 1, seq 2, length 64
17:32:21.645715 IP desktop > dns.google: ICMP echo request, id 1, seq 3, length 64
17:32:22.647387 IP desktop > dns.google: ICMP echo request, id 1, seq 4, length 64
17:32:23.648814 IP desktop > dns.google: ICMP echo request, id 1, seq 5, length 64
```

Фильтрация пакетов по протоколу ICMP

Введите в терминале:

```
tcpdump icmp
```

Пример вывода утилиты:

```
04:03:47.408545 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812, seq 75, length 64
04:03:47.408999 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812, seq 75, length 64
04:03:48.408697 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812, seq 76, length 64
04:03:48.409208 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812, seq 76, length 64
04:03:49.411287 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812, seq 77, length 64
```

Фильтрация пакетов с интерфеса eth1 с IP-адресом источника 10.0.0.1 и 80 портом назначения

Введите в терминале:

```
tcpdump -i eth1 src 10.0.0.1 and dst port 80
```

Пример вывода утилиты:

```
00:18:17.155066 IP 10.0.0.1.54222 > 10.0.0.50.80: Flags [F.], seq 500773341, ack 2116767648, win 4117, options [nop,nop,TS va
00:18:17.155104 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [S], seq 904045691, win 65535, options [mss 1460,nop,wscale 5,nop,nop
00:18:17.157337 IP 10.0.0.1.54221 > 10.0.0.50.80: Flags [P.], seq 4282813257:4282813756, ack 1348066220, win 4111, options [n
00:18:17.157366 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [.], ack 1306947508, win 4117, options [nop,nop,TS val 257786174 ecr
```

Фильтрация пакетов по всем доступным протоколам, кроме ICMP

Введите в терминале:

```
tcpdump not icmp
```

Пример вывода утилиты:

```
17:45:34.847882 IP desktop.48552 > 149.154.167.41.https: Flags [P.], seq 3991504547:3991504748, ack 499514727, win 248, optio
17:45:34.918383 IP 149.154.167.41.https > desktop.48552: Flags [.], ack 201, win 7509, options [nop,nop,TS val 4205203056 ecr
17:45:34.919444 IP 149.154.167.41.https > desktop.48552: Flags [.], seq 1:1229, ack 201, win 7509, options [nop,nop,TS val 42
17:45:34.919475 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 1229, win 239, options [nop,nop,TS val 1585771377 ecr
17:45:34.919778 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 1229:2457, ack 201, win 7509, options [nop,nop,TS va
17:45:34.919804 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2457, win 239, options [nop,nop,TS val 1585771377 ecr
17:45:34.923322 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 2457:2845, ack 201, win 7509, options [nop,nop,TS va
17:45:34.923351 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2845, win 239, options [nop,nop,TS val 1585771381 ecr
17:45:35.644804 IP desktop.49669 > _gateway.domain: 65295+ PTR? 41.167.154.149.in-addr.arpa. (45)
```

Сохранение дампа захваченных пакетов в файл в формате .pcap

Введите в терминале:

```
tcpdump -w out.pcap
```

Для анализа захваченных пакетов в формате `.pcap` используйте Wireshark.

Использование в Ideco NGFW Novum

Проверка работы IPsec-туннелей

Команды помогут понять причину неработоспособности IPsec-туннеля:

1. Для проверки прохождения трафика на всех интерфейсах головного офиса по порту 4500 введите:

```
tcpdump -i any port 4500
```

2. Для проверки прохождения трафика на всех интерфейсах филиала по порту 500 введите:

```
tcpdump -i any port 500
```

Защита от брутфорс-атак (fail2ban)

Классический контекст | Высокопроизводительный контекст

Служба `fail2ban` отслеживает повторяющиеся неудачные попытки аутентификации с одного IP-адреса.

После шести неудачных попыток ввода пароля в течение 15 минут IP-адрес отправителя запросов блокируется на 45 минут.

Список служб, защищаемых от брутфорс-атак:

Модуль	Имя службы
VPN	ideco-vpn-authd
SSH	ideco-ssh, sshd
Веб-интерфейс	ideco-web-interface
Двухфакторная аутентификация	ideco-two-factor-codes
Обратный прокси	ideco-reverse-proxy, ideco-reverse-proxy-conn, ideco-reverse-proxy-req
Личный кабинет пользователя	ideco-user-cabinet, ideco-user-cabinet-backend, ideco-user-cabinet-proxy, ideco-user-cabinet-reports
Почтовые службы	ideco-dovecot, ideco-postfix-connrate, ideco-postscreen-prgrt, ideco-roundcube, ideco-smtp, ideco-smtp-rcpt

Просмотр логов

Логи службы `fail2ban` можно просмотреть двумя способами:

- В веб-интерфейсе в **Отчеты и журналы** → **Система**, задав фильтр `fail2ban`.
- В **Управление сервером** → **Терминал**, введя команду `journalctl -u fail2ban`.

Просмотр заблокированных адресов

Для получения списка IP-адресов, заблокированных `fail2ban`, используйте команды:

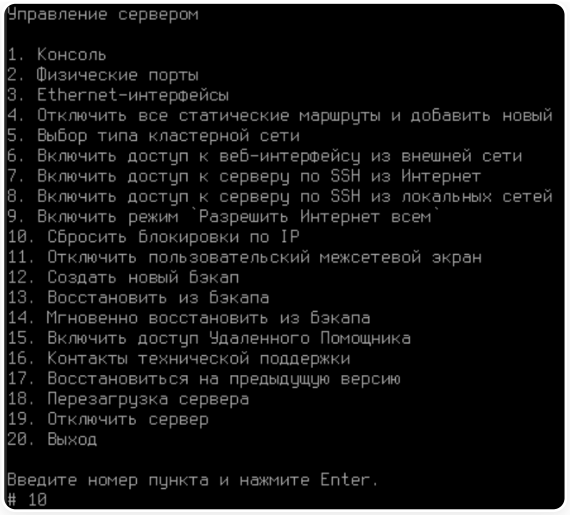
- `fail2ban-client status` - просмотр списка доступных Jail.
- `fail2ban-client get [Jail] banned` - просмотр списка адресов в указанном Jail. Например: `fail2ban-client get utm-ssh banned`.
- `fail2ban-client banned` - просмотр заблокированных адресов сразу по всем Jail (формат `python dict/json`).

Разблокировка IP-адресов

Для разблокировки через терминал используйте команды:

- `fail2ban-client unban --all` - снятие всех блокировок.
- `fail2ban-client unban <IP-адрес>` - разблокировка конкретного IP-адреса.

Блокировки можно сбросить из локального меню шлюза, выбрав опцию **Сбросить блокировки по IP**:



Добавление IP-адреса в белый список

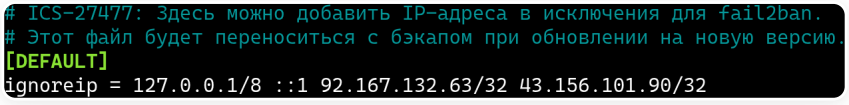
Если доверенный IP-адрес был заблокирован, добавьте его в белый список, чтобы предотвратить повторную блокировку. Для этого:

1. Перейдите в **Управление сервером** → **Терминал** и выполните команду:

```
nano /var/opt/ideco/fail2ban/excluded_ip_addresses.local
```

2. Найдите в файле параметр `ignoreip` и раскомментируйте строку, убрав символ `#` в начале.

3. Добавьте IP-адрес с маской `/32` или подсеть с нужной маской в конец строки через пробел. Для нескольких адресов укажите их последовательно через пробел:



4. Сохраните файл, нажав **Ctrl+O**, затем **Enter**.

5. Выйдите из редактора, нажав **Ctrl+X**.

6. Выполните команду `systemctl restart fail2ban` для перезагрузки службы и применения изменений.

Лицензия

Классический контекст | Высокопроизводительный контекст | API

Название службы раздела **Лицензия**: `ideco-license-backend`.

Список служб для других разделов доступен по ссылке.

В разделе **NGFW** MY.IDECO находится информация о зарегистрированных серверах и имеющихся лицензиях. Подробнее о видах лицензий в статье Лицензирование.

Доступные действия для управления лицензиями:

- Регистрация сервера.
- Добавление коммерческой или бесплатной лицензии.
- Привязка лицензии к серверу.
- Просмотр информации об имеющихся лицензиях.
- Офлайн-обновление лицензии и баз модулей фильтрации.

Лицензия между **Системным контекстом** и всеми виртуальными контекстами общая. Это значит, что на Ideco NGFW Novum с лицензией на 100 пользователей можно создать неограниченное количество VCE, каждый из которых будет поддерживать 100 пользователей. В будущих версиях количество пользователей, ограниченное числом в лицензии, будет распределяться между **Системным контекстом** и всеми VCE.

Добавление коммерческой (Enterprise) лицензии

1. Скопируйте токен лицензии из письма, отправленного после покупки лицензии. Формат токена: `owhYLGvT6Xmt819JyinSxREkJfvjVO63`.

2. В MY.IDECO перейдите в раздел **NGFW → Лицензирование**, нажмите **Добавить лицензию** и выберите **Коммерческую**.

3. Введите токен в поле **Токен лицензии** и нажмите **Добавить**.

Токен станет недействительным, а в таблице **Непривязанные лицензии** отобразится купленная лицензия.

Если требуется перепривязать купленную лицензию к серверу с уже установленной тестовой лицензией, воспользуйтесь статьей.

Добавление FREE (бесплатной) лицензии

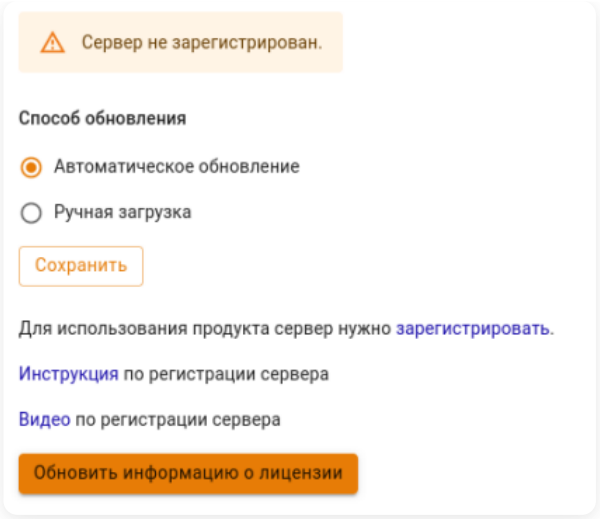
Для добавления FREE-лицензии в MY.IDECO перейдите в раздел **NGFW → Лицензирование**, нажмите **Добавить лицензию** и выберите **Бесплатную**. Добавленная лицензия отобразится в таблице **Непривязанные лицензии**.

Подробнее о бесплатной лицензии в статье Лицензирование.

Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн. Онлайн проводится только в MY.IDECO. Офлайн потребует доступ к веб-интерфейсу сервера.

Для онлайн-привязки лицензии в разделе **Управление сервером → Лицензия** веб-интерфейса Ideco NGFW Novum выберите способ обновления **Автоматическое обновление**. Для офлайн-привязки выберите **Ручную загрузку**:



Назначьте имеющиеся коммерческие лицензии на любой зарегистрированный сервер Ideco NGFW Novum с учетом следующих ограничений:

- Одна лицензия может быть привязана только к одному серверу.
- Демо-лицензию нельзя привязать к другому серверу.
- Демо-лицензию нельзя отвязать от сервера. Доступна только замена на другую лицензию.
- Демо-лицензию нельзя повторно получить на одну и ту же инсталляцию сервера.
- При удалении сервера с демо-лицензией также удаляется и лицензия.

После активации лицензия привязывается к оборудованию, на котором установлено программное обеспечение Ideco NGFW Novum. При замене оборудования или частей оборудования лицензия отвязывается и требует повторной привязки. Демо-лицензия при этом теряется.

Онлайн-привязка лицензии

Выберите удобный вариант привязки:

- В MY.IDECO на вкладке **Лицензирование** нажмите **Привязать лицензию**. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения.
- В MY.IDECO на вкладке **Лицензирование** выберите **Непривязанные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

Особенности работы онлайн-лицензии:

- При наличии доступа в интернет обновление данных о лицензии происходит один раз в сутки.
- Если связь с серверами лицензирования отсутствует, Ideco NGFW Novum предпринимает попытки соединения каждые 60 секунд до восстановления доступа.
- Если у Ideco NGFW Novum отсутствует связь с серверами лицензирования более 30 дней, то Ideco NGFW Novum перейдет в нелицензионный режим.
- Для использования Ideco NGFW Novum в закрытом контуре (без доступа к интернету) необходимо использовать офлайн-лицензию.

Офлайн-привязка лицензии

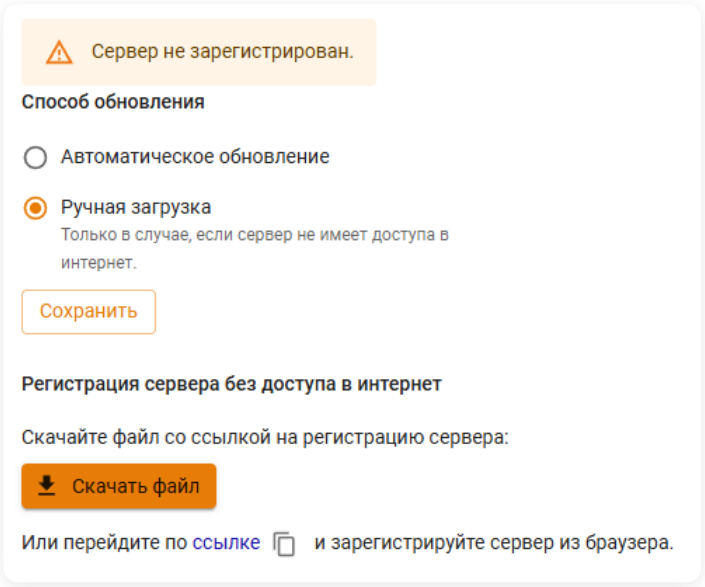
Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

1. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum. Выберите **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Для этого нажмите **Скачать файл** или скопируйте ссылку из веб-интерфейса:

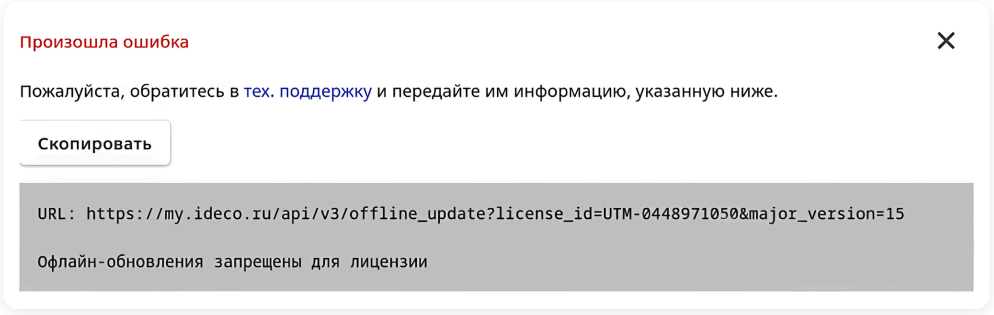


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

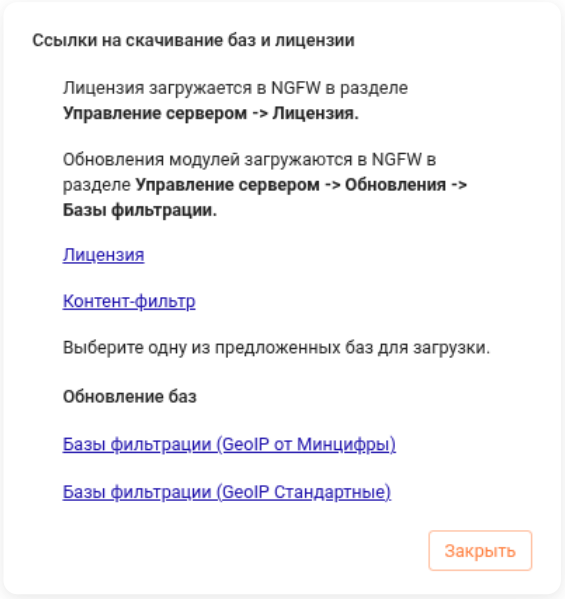
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

5. Перейдите в **NGFW** → **Лицензирование** в MY.IDECO. Нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `UTM (UTM Unknown)`.

Если была выбрана лицензия, не подходящая для офлайн-регистрации сервера, то появится ошибка:

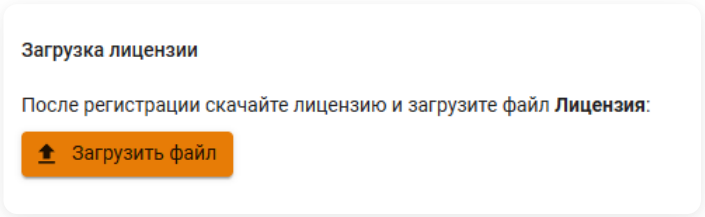


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



Если при скачивании Обновления баз (Предотвращение вторжений, базы GeoIP) через **Google Chrome** возникают проблемы, в настройках браузера разрешите **Небезопасный контент** для MY.IDECO.

7. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum и загрузите файл с лицензией, скачанный в пункте 6:



Повторная регистрация сервера после удаления

1. Откройте терминал и введите команду:

```
rm /var/cache/ideco/license-backend/license.json
systemctl restart ideco-license-backend.service
```

2. Следуйте пунктам по офлайн-регистрации, которые приведены выше.

Просмотр информации о лицензиях

Посмотреть информацию о модулях и лицензии можно:

- В MY.IDECO напротив нужного сервера.
- В разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco NGFW Novum.

Информация о лицензии содержит сведения о количестве пользователей, сроках действия лицензии, окончания обновлений и технической поддержки и других параметрах.

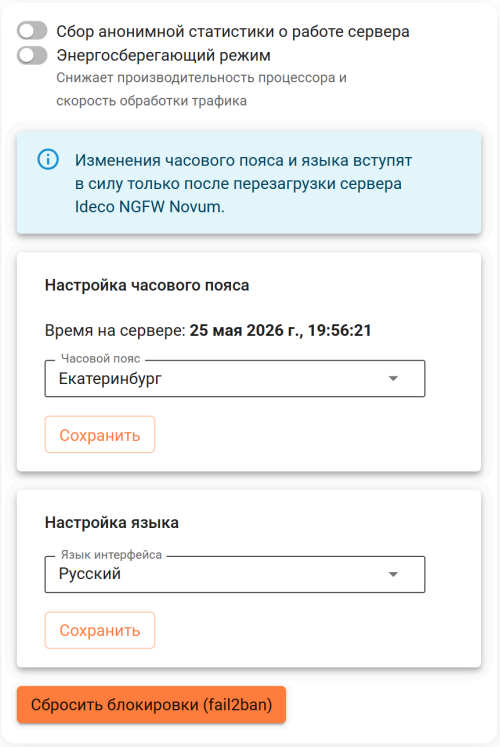
Дополнительно

Классический контекст | Высокопроизводительный контекст

Название службы раздела **Дополнительно**: `ideco-system-backend`, `ideco-system-swap`.

Список служб для других разделов доступен по ссылке.

Настройка часового пояса и сбор анонимной статистики через веб-интерфейс в разделе **Управление сервером** → **Дополнительно**:



- **Сбор анонимной статистики о работе сервера** - включите опцию, чтобы сервер мог отправлять информацию об используемых модулях. При этом исключается передача следующих данных:
  - Пользователи.
  - Проходящий через сервер трафик.
  - Сетевые интерфейсы.
  - Идентификаторы сервера и лицензии.
- **Энергосберегающий режим** - включите опцию для снижения производительности процессора и скорости обработки трафика.
- **Настройка часового пояса** - установите часовой пояс для корректного сбора логов и статистики.
- **Настройка языка** - укажите язык, удобный для работы в веб-интерфейсе.
- **Сбросить блокировки (fail2ban)** - используйте для сброса всех IP-адресов, заблокированных службой `fail2ban`. Если требуется разблокировать какой-то конкретный IP-адрес, воспользуйтесь командой `fail2ban-client unban <IP-адрес>` в терминале.

Служба `fail2ban` отслеживает повторяющиеся неудачные попытки аутентификации с одного IP-адреса.

После шести неудачных попыток ввода пароля в течение 15 минут IP-адрес отправителя запросов блокируется на 45 минут.

Почтовый релей

API

Функциональность доступна только в **Системном контексте**.

Все возможности по фильтрации почтового трафика можно также применить к внутреннему почтовому серверу, опубликовав сервер через почтовый релей.

Для фильтрации почтового трафика от вирусов, спама и фишинга рекомендуется покупка лицензии на антиспам Касперского.

Для настройки почтового сервера перейдите в раздел **Почтовый релей**. Настройка ключевых параметров выполняется в следующих разделах:

- **Основные настройки** - базовые параметры, необходимые для настройки почтового сервера, почтового релея и веб-почты.
- **Расширенные настройки** - параметры маршрутизации и ограничения почты, механизмы безопасности, а также DKIM-подпись исходящей почты для подтверждения легитимности отправителя.
- **Антиспам и антивирус** - управление работой службы антиспама и антивируса почтового сервера, а также настройка фильтрации.
- **Правила** - управление пересылкой писем, а также списками доверенных и заблокированных отправителей.
- **Почтовая очередь** - управление очередью отложенной входящей и исходящей почты.

Если используется почтовый сервер Ideco NGFW Novum, обязательно подключите дополнительный SSD. В настройках почтового сервера можно указать максимальный размер почтового ящика и максимальный размер письма. Подробнее в статье.

Параметры подключения и примеры настройки почтового клиента описаны в статье Настройка почтового клиента.

При настройке кластера почта доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.

Схема фильтрации почтового трафика

Полная схема и последовательность фильтрации:



Модуль **Антиспама и антивируса** Касперского использует собственный набор методик для фильтрации и обеспечивает высокий уровень детектирования спама при низких значениях ложных срабатываний (0,003-0,005% от общего количества сообщений).

Для защиты пользователей применяется набор технологий распознавания спама с использованием внешних облачных сервисов (DNSBL, SPF и SURBL) и собственных алгоритмов:

- Сигнатурный анализ текста и графики.
- Лингвистическая эвристика.
- Использование UDS-запросов в режиме реального времени.

Также для защиты проверяются все ссылки в почтовых сообщениях и письма со ссылками на фишинговые ресурсы блокируются.

Разрешенные адреса в настройках почты обеспечивают прохождение писем без фильтрации, начиная с уровня **Фильтрации по серым спискам**. **Предварительный спам-фильтр** срабатывает для любых адресатов.

Полезные ссылки

- **Основные настройки**
- **Расширенные настройки**
- **Антиспам и антивирус**
- **Правила**
- **Почтовая очередь**
- **Настройка почтового клиента**

Основные настройки

В разделе представлены базовые параметры, необходимые для настройки почтового сервера, почтового релея и веб-почты.

Настройка почтового сервера

Перейти >

Настройка почтового релея

Перейти >

Web-почта

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка почтового сервера

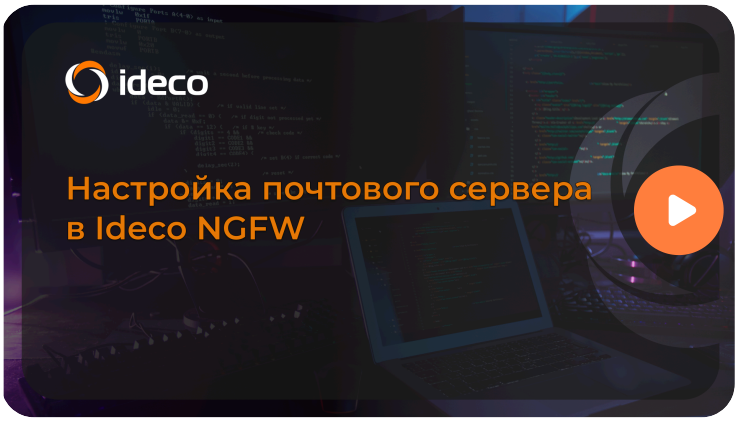
Функциональность доступна только в **Системном контексте**.

Видеоинструкция

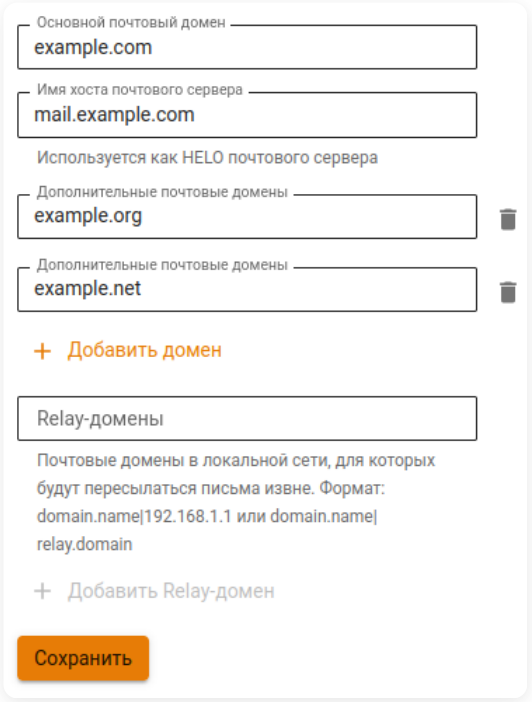
Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE



1. Перейдите в **Почтовый релей** → **Основные настройки** и заполните поля:



Расшифровка полей

- **Основной почтовый домен** - указывает серверу, для какого домена сервер принимает и обрабатывает электронную почту. Все пользовательские почтовые ящики закреплены за этим доменом. Переписка с внешними получателями осуществляется от имени указанного домена.
- **Имя хоста почтового сервера** - должно разрешаться из интернета во внешний IP-адрес NGFW. Указанное имя используется в качестве идентификатора при передаче почты между почтовыми серверами. Необходимо для корректной работы почтового сервера в интернете.
- **Дополнительные почтовые домены** - домены, которые почтовый сервер будет считать своими. Электронная почта, отправляемая с ящиков в этих почтовых доменах, будет обрабатываться сервером при условии правильной установки MX-записей.

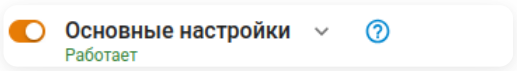
Имя хоста почтового сервера, как правило, совпадает с MX-записью для вашего домена.

При настройке авторизации в почте проверьте, чтобы основной или дополнительный почтовый домен совпадал с доменами **Каталога авторизации** в **Пользователи** → **Аутентификация**. В противном случае аутентификация будет выполняться через **Каталог по**

умолчанию: если пользователь есть в каталоге, аутентификация пройдет успешно по логину, указанному до `@`.

Настройку **Доменный суффикс для локальных пользователей** можно использовать совместно с настройкой почтового домена, чтобы для данного почтового домена использовался каталог **Локальные пользователи**.

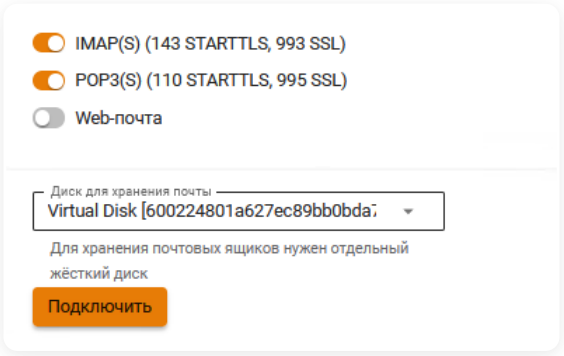
2. Включите почтовый сервер Ideco NGFW Novum:



3. Выберите протокол получения электронной почты:

- **IMAP(S) (143 STARTTLS, 993 SSL)** - подключение к почтовым ящикам с сохранением писем на сервере. Изменения (прочтение, перемещение, удаление) синхронизируются между устройствами. Удобен для использования с нескольких устройств.
- **POP3(S) (110 STARTTLS, 995 SSL)** - загрузка писем с сервера на клиент с последующим удалением с сервера. Настроить сохранение копий можно на почтовом клиенте. Подходит для проверки почты с одного устройства.

4. Подключите к серверу дополнительный жесткий диск:



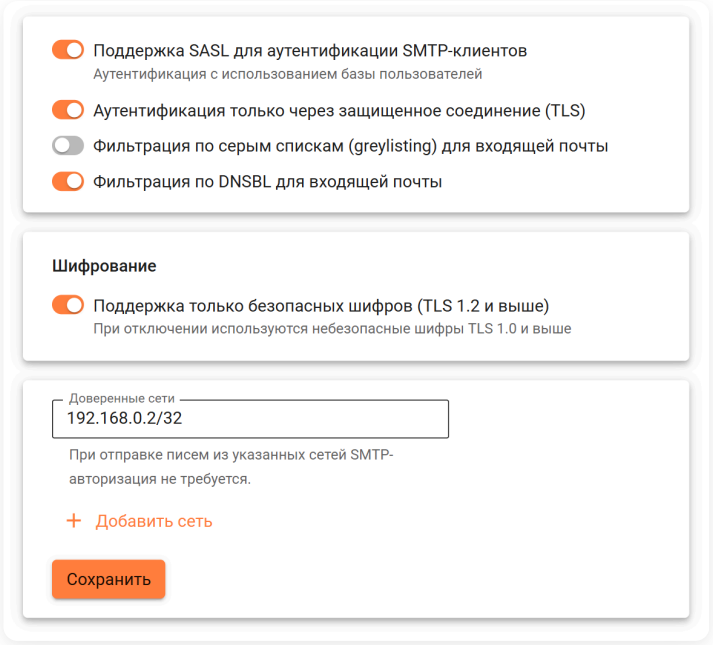
Если диск после подключения не отображается:

- Проверьте, стерты ли с диска все данные, в том числе таблица разделов.
- Обратитесь в техническую поддержку, если проблему не удалось решить самостоятельно.

Хранение почты на дополнительном HDD/SSD-диске обязательно. Рекомендуем использовать SSD-диск.

Поддерживаются SATA/SAS- и NVMe-накопители. Дополнительное устройство используется только для работы почтового сервера, другие данные на нем храниться не будут.

5. Чтобы разрешить прием входящей почты на порт 25 от сторонних доменов с серых IP-подсетей, внесите подсети в список доверенных. Для этого перейдите в **Почтовый релей** → **Расширенные настройки** → **Безопасность** и укажите в поле **Доверенные сети** адрес почтового сервера для подключения к NGFW Novum:



Подробнее о расширенных настройках - в статье.

SSL-сертификат для почтового домена

После сохранения настроек почтового сервера Ideco NGFW Novum создает локальный сертификат, подписанный корневым (самоподписанным) сертификатом. Параллельно с созданием локального сертификата отправляется запрос на выпуск сертификата Let's Encrypt:

- Если сертификат Let's Encrypt успешно выпущен, то Let's Encrypt заменит собой локальный сертификат.
- Если выпуск сертификата Let's Encrypt завершился неудачей, то будет использоваться локальный сертификат.

Для замены автоматически выпущенного сертификата перейдите в **Сервисы → Сертификаты → Загруженные сертификаты** и загрузите собственную цепочку сертификатов. **CN (Общее имя)** последнего сертификата в цепочке должно соответствовать домену, для которого загружается сертификат. Подробнее в инструкции.

Проверка настроек почтового сервера

Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса check.smtp.bz.

При правильной настройке почтовый сервер на Ideco NGFW Novum должен получить результат **Отлично**.

Создание копии диска с почтой

1. Подключите второй физический диск, на который будете клонировать почту.

2. В терминале выполните команду `lsblk` и посмотрите название дисков:

```
NAME                   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sr0                     11:0     1   1,8G  0 rom
nvme01                  259:0    0   150G  0 disk
├─nvme01p1              259:1    0   512M  0 part
├─nvme01p2              259:2    0     2M  0 part
└─nvme01p3              259:3    0 149,5G  0 part
  ├─utm_72874-root_one 253:0    0     4G  0 lvm  /run/ideco-erofs
  ├─utm_72874-data     253:1    0  63,7G  0 lvm  /run/ideco-overlay-dir
  ├─utm_72874-logs     253:2    0     2G  0 lvm  /var/log/journal
  ├─utm_72874-root_two 253:3    0     4G  0 lvm
  └─utm_72874-swap     253:4    0  15,3G  0 lvm  [SWAP]
nvme02                  259:4    0    50G  0 disk /var/spool/mail
nvme03                  259:5    0    55G  0 disk
```

- В примере используются диски:
  - `nvme01` - для работы NGFW.
  - `nvme02` - для хранения почты.
  - `nvme03` - новый диск.

3. Выполните поблочное копирование с помощью утилиты dd, введя команду:

```
dd if=/dev/nvme02 of=/dev/nvme03 bs=4M status=progress
```

- `if=/dev/nvme02` - источник данных для копирования.
- `of=/dev/nvme03` - место назначения для скопированных данных.

После выполнения команды все данные на диске `nvme03` будут перезаписаны. Если размер диска `nvme02` превышает размер диска `nvme03`, то копирование завершится неудачно.

Web-почта

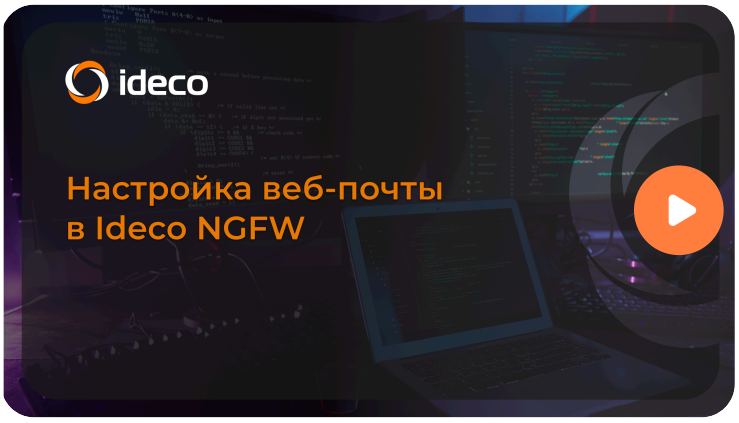
Функциональность доступна только в **Системном контексте**.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

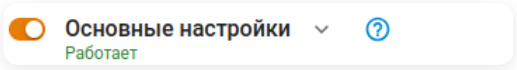
YouTube | RUTUBE | VK Видео



Веб-интерфейс встроенного почтового клиента работает с почтовым сервером по протоколу IMAP и обладает возможностями:

- Создание и отправка писем с поддержкой загрузки нескольких вложений.
- Просмотр, удаление, перемещение письма, а также управление IMAP-папками почтового ящика.
- Персональная (для конкретного ящика) адресная книга, работающая только в рамках веб-приложения.
- Поддержка формата VCARD в адресной книге с возможностью экспорта или сохранения контактов на компьютер.
- Календарь для создания событий и отправки уведомлений сотрудникам по электронной почте.
- Цветные метки писем, аналогично клиенту Thunderbird. Проставляются клавишами от 1 до 5, при этом метки сохраняются на сервере и отображаются в других почтовых клиентах.

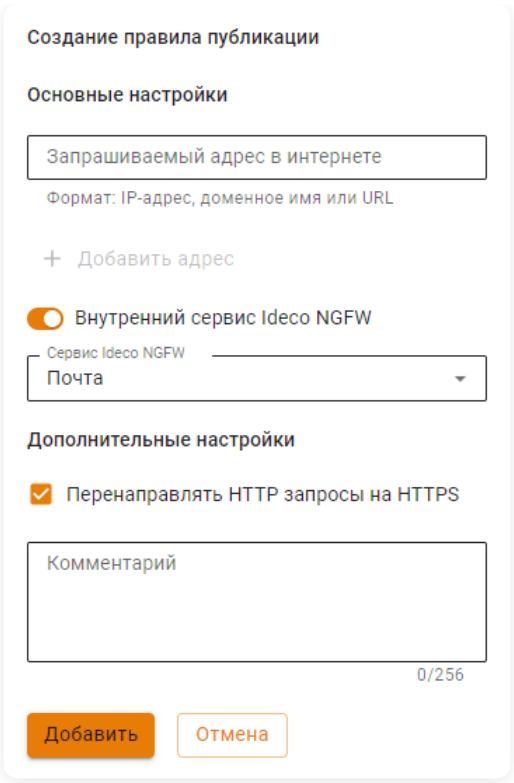
Перед настройкой веб-почты убедитесь, что на Ideco NGFW Novum включен почтовый сервер:



Для работы веб-почты необходимо:

1. Активировать опцию **Web-почта** в **Почтовый релей** → **Основные настройки**.

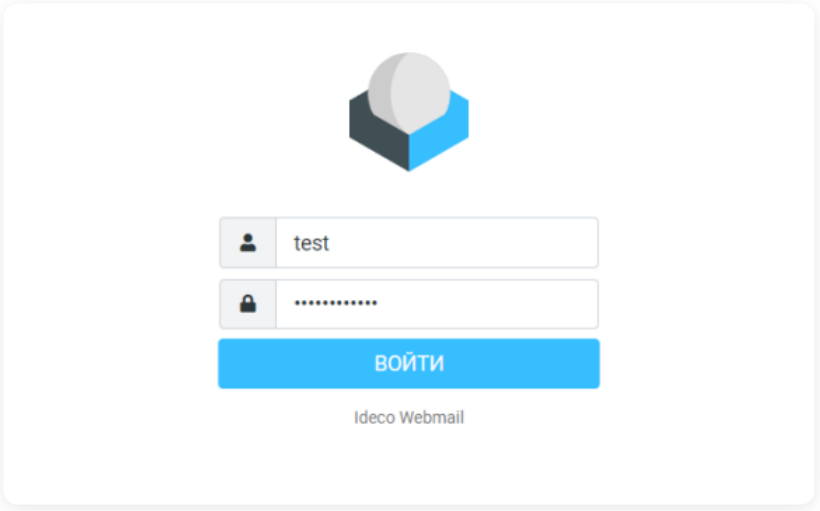
2. Создать и добавить правило публикации в **Сервисы** → **Обратный прокси**:



- В поле **Запрашиваемый адрес в интернете** введите домен, IP-адрес или URL, по которому должна быть доступна веб-почта (например, `webmail.example.com`, `192.168.100.40` или `192.168.100.20/webmail`).
- Включите опцию **Внутренний сервис Ideco NGFW Novum**.
- В качестве сервиса выберите **Почта**.
- В блоке **Дополнительные настройки** включите опцию **Перенаправлять HTTP запросы на HTTPS**.

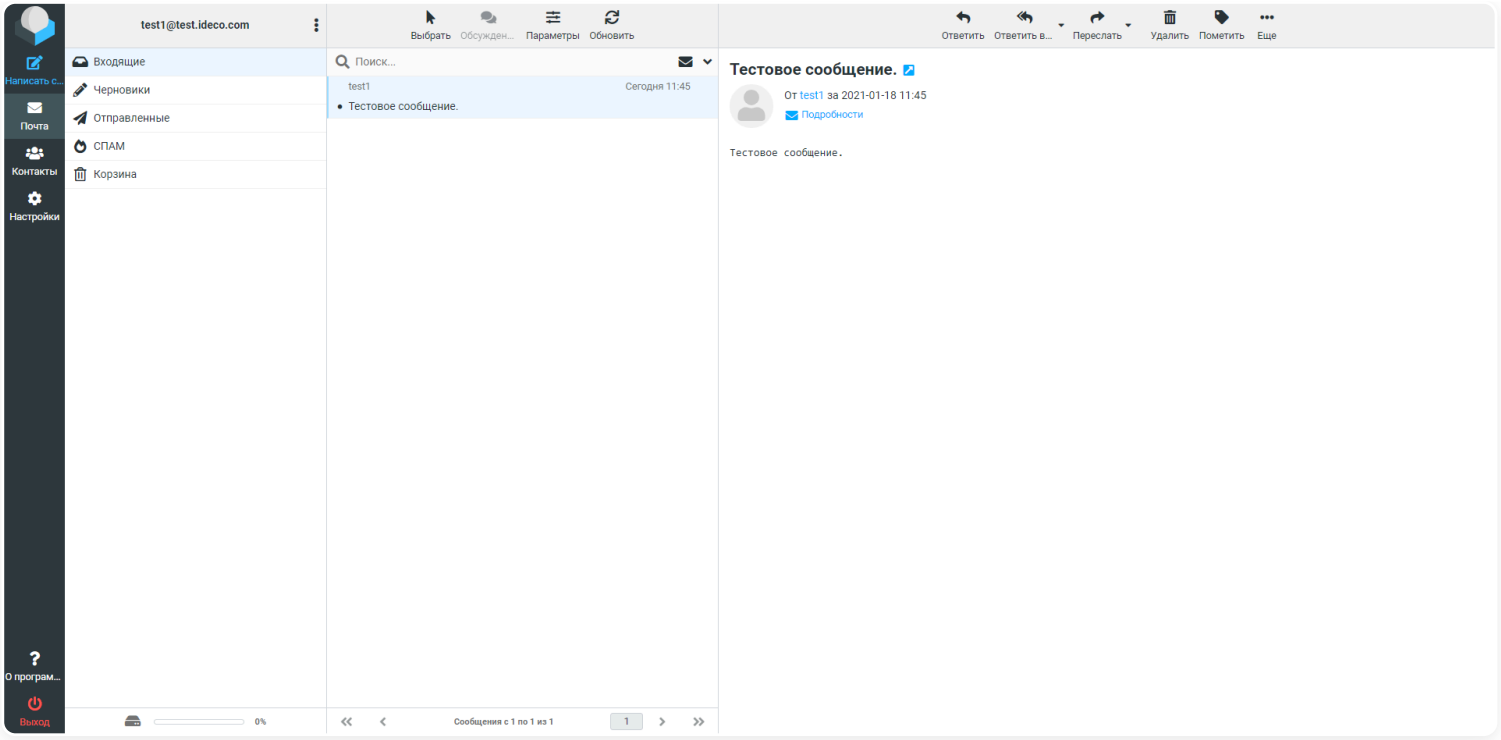
- Чтобы пользователи имели доступ к веб-почте из внешней сети, в правиле публикации в поле **Запрашиваемый адрес в интернете** укажите **белый IP-адрес или зарегистрированный домен**.
- Для подключения обязательно используйте HTTPS.
- С версии 17 Ideco NGFW Novum веб-почта не доступна через `IP-адрес_или_домен_веб-интерфейса:8443/webmail`, так как не связана с административным веб-интерфейсом NGFW.

После создания правила из локальной или внешней сети в браузере наберите: `https://<IP-адрес>`, `https://<домен>` или `https://<URL>`:



- В качестве логина укажите логин от учетной записи пользователя.
- В качестве пароля пропишите пароль от учетной записи пользователя. **Установить отдельный пароль на почту нельзя.**

При успешном входе в браузере откроется веб-интерфейс почтового ящика пользователя:



В правом верхнем углу в разделе **Еще...** находится расширенный поиск по всем письмам ящика.

Настройка почтового релея

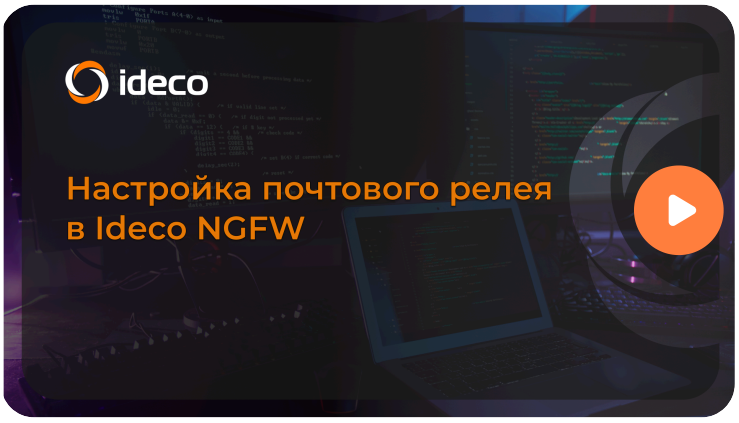
Функциональность доступна только в **Системном контексте**.

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео



Работа в режиме открытого почтового релея невозможна, поэтому Ideco NGFW Novum в режиме Relay может принимать почту только в следующих случаях:

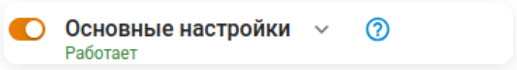
- Когда почта адресована исключительно указанному Relay-домену.
- Из сетей, которые входят в список доверенных в **Почтовый релей** → **Расширенные настройки** → **Безопасность**.

Остальная почта будет отвергнута сервером.

Все почтовые домены должны быть ассоциированы с внешним адресом сервера Ideco NGFW Novum (A- и MX-записи в DNS-зоне).

NGFW Novum не поддерживает кириллические почтовые домены.

Перед настройкой почтового релея убедитесь, что на Ideco NGFW Novum включен почтовый сервер:



Настройка пересылки почты

Для пересылки почты с почтового сервера в локальной сети через Ideco NGFW Novum выполните действия:

Входящая

1. Перейдите в **Почтовый релей** → **Основные настройки** и заполните поля **Основной почтовый домен** и **Имя хоста почтового сервера**:

Основной почтовый домен Ideco NGFW Novum и имя хоста почтового сервера должны отличаться от Relay-доменов. Если Ideco NGFW Novum используется только в режиме Relay:

- В поле **Основной почтовый домен** укажите любой валидный несуществующий домен.
- В поле **Имя хоста почтового сервера** укажите реальное доменное имя с соответствующими DNS-записями.

2. Заполните поле **Relay-домены** в формате `corp-domain.ru|10.20.30.40`:

- `corp-domain.ru` - почтовый домен, зарегистрированный в интернете на публичный адрес Ideco NGFW Novum.
- `10.20.30.40` - адрес почтового сервера в локальной сети.

3. Если требуется проверка почты на спам и вирусы, перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

Исходящая

Для пересылки исходящей почты дополнительных настроек на стороне NGFW Novum не требуется, но почта не будет проверяться на спам и вирусы. Если нужна такая проверка, выполните действия:

1. Перейдите в **Почтовый релей** → **Основные настройки** и заполните поля **Основной почтовый домен** и **Имя хоста почтового сервера**:

2. Перейдите в **Почтовый релей** → **Расширенные настройки** → **Безопасность** и укажите в поле **Доверенные сети** адрес почтового сервера для подключения к NGFW Novum:

3. Перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

4. На почтовом сервере клиента в настройках отправки исходящей почты по протоколу SMTP укажите внешний IP-адрес Ideco NGFW Novum.

Настройка доступа почтовых клиентов

Доступ из внешней сети

Для подключения почтовых клиентов из внешней сети, перейдите в **Правила трафика** → **Межсетевой экран** → **DNAT**, создайте и включите правило проброса портов, используемых вашим почтовым сервером для клиентских подключений: POP3(S), IMAP(S), SMTPS (465), SUBMISSION (587):

Расшифровка полей

- **Протокол** - укажите TCP.
- **Назначение**:
  - **Адрес** - внешний IP-адрес Ideco NGFW Novum.
  - **Порты назначения** - порты, которые использует ваш почтовый клиент: POP3, IMAP, SMTPS (465), SUBMISSION (587), POP3S или IMAPS.
  - **Сменить IP-адрес назначения** - IP-адрес почтового сервера в локальной сети.
- **Действие** - DNAT.
- **Дополнительно** - включите правило.

SMTP, в отличие от SMTPS, нельзя пробрасывать через DNAT, так как трафик не попадет на почтовый релей и поэтому:

- Не пройдет проверку Антиспамом.
- Не будет направляться на нужный почтовый сервер в сети, если серверов несколько.

Доступ по VPN

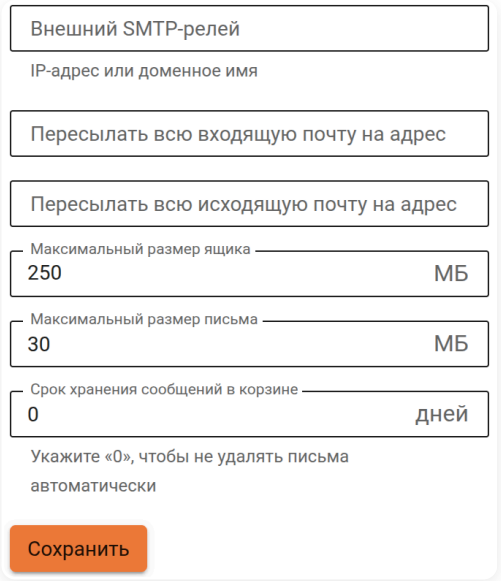
Пользователи смогут подключаться к почтовому серверу по IP-адресу почтового сервера в локальной сети.
Убедитесь, что VPN-подключение корректно настроено и есть разрешающее правило доступа.

Расширенные настройки

Функциональность доступна только в **Системном контексте**.

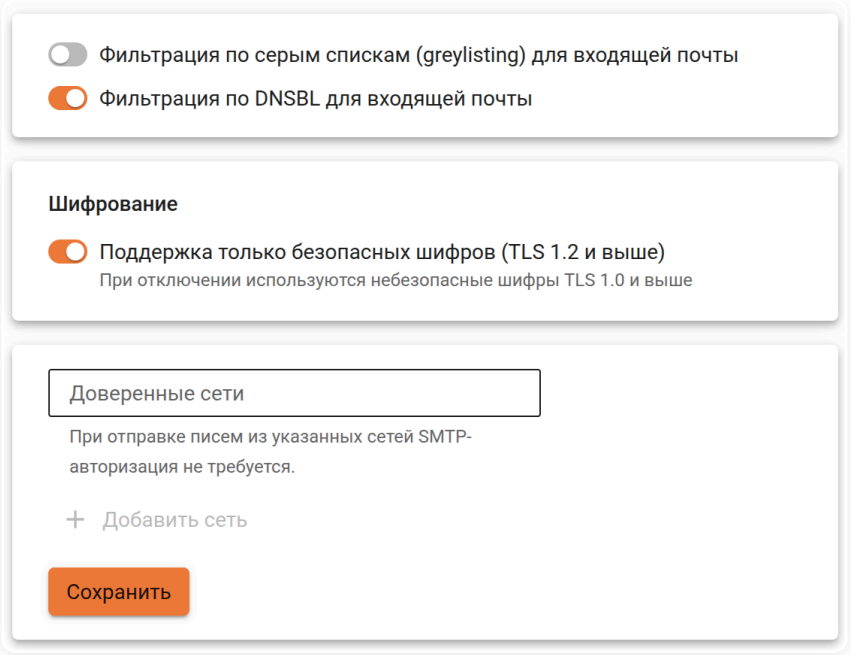
Раздел **Расширенные настройки** состоит из трех подразделов: **Основное, Безопасность, DKIM-подпись**.

Основное



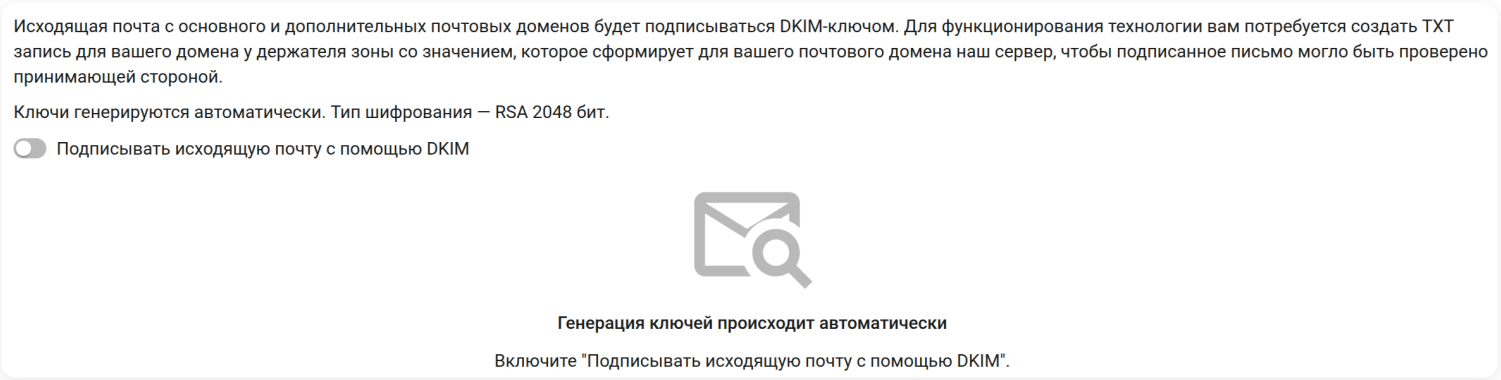
- **Внешний SMTP-релей.** Вся исходящая почта будет отправляться на указанный адрес. Используется, например, если почта должна проходить через вышестоящий сервер провайдера перед отправкой в интернет.
- **Пересылать всю исходящую почту на адрес.** Вся исходящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости.
- **Пересылать всю входящую почту на адрес.** Вся входящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости.
- **Максимальный размер ящика.** Ограничение на максимальный размер почтового ящика в Мбайтах (**100 ГБ - максимальное значение**).
- **Максимальный размер письма.** Ограничение на максимальный размер формируемого сервером письма в Мбайтах (**150 МБ - максимальное значение**).
- **Срок хранения сообщений в корзине.** Количество дней, в течение которых почта хранится в корзине перед удалением. Максимальный срок хранения - 60 дней.

Безопасность



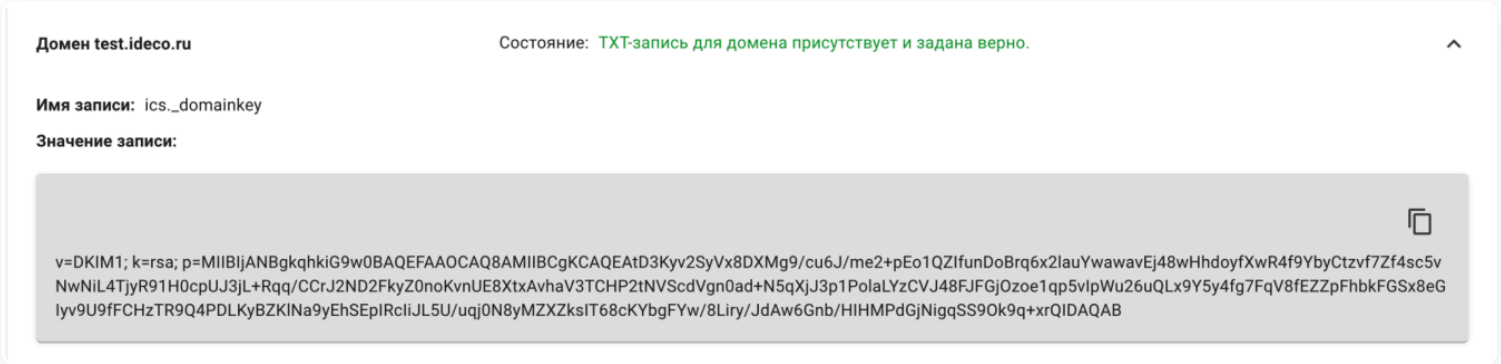
- **Фильтрация по серым спискам (greylisting) для входящей почты.** Включает фильтрацию по серым спискам (greylisting) для входящей почты. При этом почта от неизвестных доменов отправителей может приходить с небольшой задержкой.
- **Фильтрация по DNSBL для входящей почты.** Включает фильтрацию по DNSBL для входящей почты.
- **Поддержка только безопасных шифров (TLS 1.2 и выше)**. При отключении используются небезопасные шифры TLS 1.0 и выше.
- **Доверенные сети.** Авторизация на сервере для доступа к почтовому ящику не требуется при попытке доступа из этих сетей. Указываются IP-сети и хосты в нотации CIDR или с префиксом сети, например, `10.0.0.5/255.255.255.255` или `192.168.0.0/16`.

DKIM-подпись



Настраивается в **Почтовый релей → Расширенные настройки → DKIM-подпись.** Подписывает исходящую с сервера корреспонденцию уникальной для почтового домена подписью так, что другие почтовые серверы в сети интернет могут убедиться, что почта легитимна и заслуживает доверия.

Для функционирования технологии потребуется создать TXT-запись для домена у держателя зоны со значением, которое сформирует для этого почтового домена наш сервер. TXT-записи будут сформированы для основного почтового домена, настроенного на Ideco NGFW Novum, и дополнительных почтовых доменов (если указаны). Сервер также проверит, правильно ли была указана запись и резолвится ли запись в интернет:



Объем TXT-записи достаточно велик и многие регистраторы/держатели зон испытывают сложности с предоставлением интерфейса клиентам для указания TXT-записей длиннее 255 символов. Зачастую регистраторы/держатели зон предоставляют возможность указания TXT-записей длиной до 256 символов, согласно стандарту RFC1035. Но другой стандарт, RFC4408, предполагает объединение строк в случаях, когда нужно использовать длинные TXT-записи при настройке SPF и DKIM. Оперируйте этой информацией в диалоге с держателем доменной зоны. Как правило, держатели зон находят способ создания длинных TXT-записей.

Подпись содержит сочетание кавычек (кавычка-пробел-кавычка: **" "**).

Если хостинг не воспринимает такой формат записи, удалите эти символы.

Настройка домена у регистратора/держателя зоны

Для создания почтового сервера потребуется доменное имя. Зарегистрируйте доменное имя у интернет-провайдера или напрямую у регистратора, например, в RUcenter.

После того как было зарегистрировано доменное имя, потребуется внести изменения в описание зоны на DNS-сервере (у держателя доменной зоны, которой зачастую является регистратор).

1. Создайте ресурсную запись типа A с именем для почтового сервера в домене, указывающую на внешний IP-адрес Ideco NGFW Novum. **Убедитесь, что на внешнем интерфейсе NGFW назначен публичный адрес, доступный из сети интернет.**

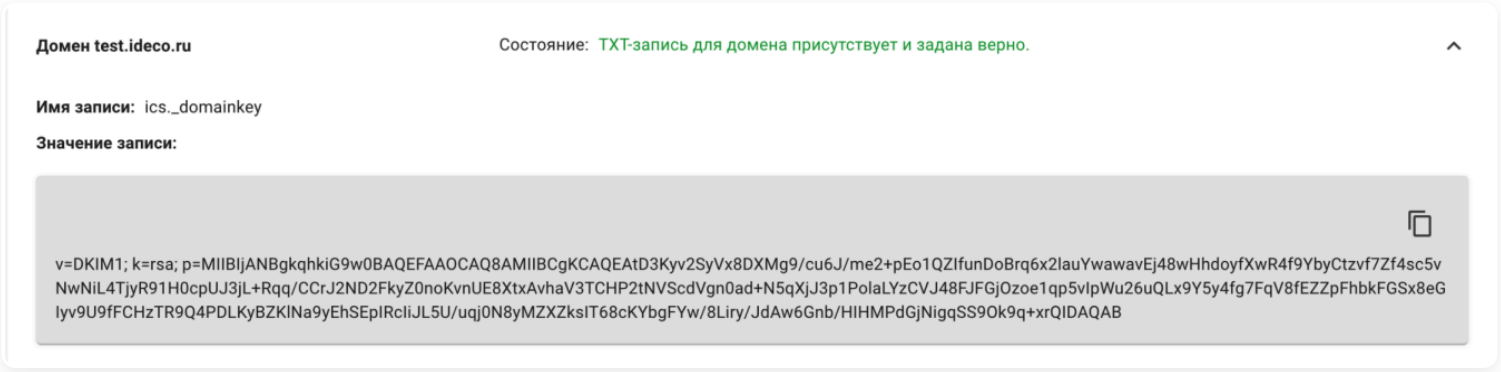
2. Добавьте ресурсную запись типа MX, указывающую на A-запись, которая была создана на предыдущем шаге. MX-запись указывает на сетевой узел, который занимается обработкой почтовых сообщений для домена, и должна ссылаться на доменное имя почтового сервера, а не на IP-адрес.

Рекомендуем:

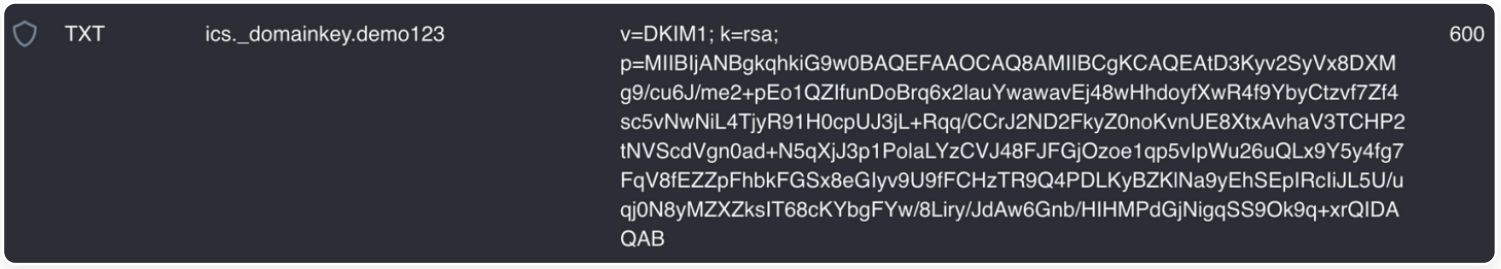
3. Добавить обратную ресурсную запись типа PTR. Эта запись должна быть прописана в файле обратной зоны. Эти изменения должны быть сделаны на стороне интернет-провайдера. Обратитесь к нему с просьбой прописать обратную ресурсную запись для IP-адреса, которая должна ссылаться на запись типа MX.

4. Настроить SPF-запись для почтового сервера.

5. После настройки почтового сервера настроить также DKIM-подпись почтовых сообщений. Для этого перейдите в **Почтовый релей** → **Расширенные настройки** → **DKIM-подпись** и активируйте пункт **Подписывать исходящую почту с помощью DKIM**:



Также создайте TXT-запись для домена у держателя зоны с именем из строки ***Имя записи*** и с содержимым, которое было сформировано Ideco NGFW Novum в **Значение записи**:



Рассмотрим набор необходимых записей на примере вымышленного домена `example.net`:

- A-запись вида: `mail.example.net. IN A 23.45.67.89`, где 23.45.67.89 - это внешний IP-адрес Ideco NGFW Novum.
- MX-запись вида: `example.net. MX 10 mail.example.net`.
- Обратитесь на хостинг для регистрации PTR-записи для нужного IP-адреса вида: `89.67.45.23.in-addr.arpa IN PTR mail.example.net`.
- SPF-запись, объявляющая другим почтовым серверам в интернет, что отправка писем с домена разрешена только с хоста почтового сервера, указанного в MX-записи: `example.net. IN TXT "v=spf1 a mx -all"`.

Синтаксис SPF:

- "v=spf1" - версия SPF, обязательный параметр, всегда spf1, никакие другие версии не работают;
- "+" - принимать письма (по умолчанию);
- "-" - отклонить;
- "~" - "мягкое" отклонение (письмо будет принято, но будет помечено как спам);

- "?" - нейтральное отношение;
- "mx" - включает все адреса серверов, указанные в MX-записях домена;

При использовании почтового сервера на NGFW в качестве почтового релея ресурсные записи будут выглядеть так же, так как в интернете почтовый сервер в локальной сети будет представлен SMTP-релеем на NGFW.

Антиспам и антивирус

Функциональность доступна только в **Системном контексте**.

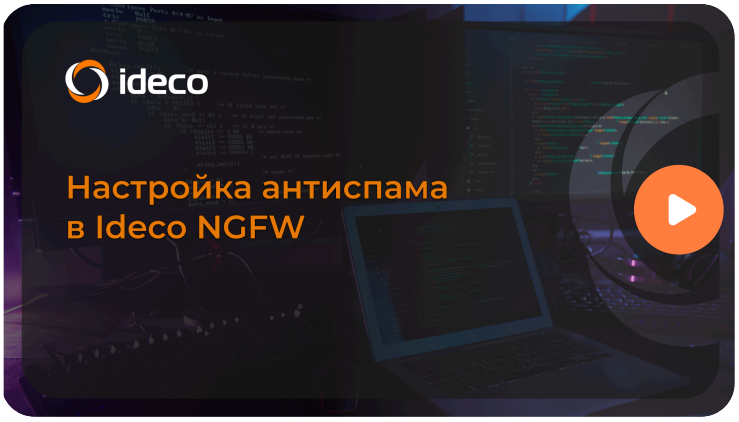
API

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube RUTUBE VK Видео



Раздел **Антиспам и антивирус** состоит из вкладок: **Основное** и **Настройки фильтрации**.

Основное



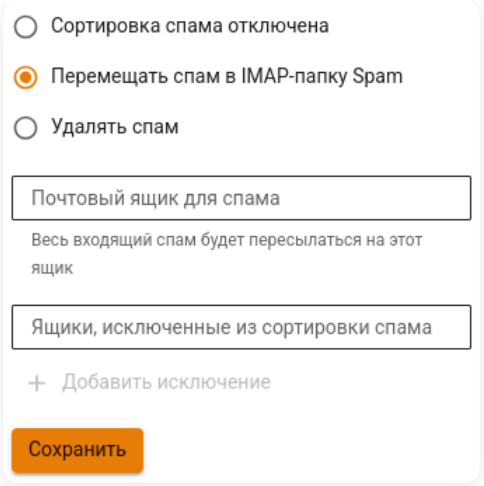
Позволяет управлять работой службы антиспама и антивируса почтового сервера на базе Kaspersky Security for Linux Mail Server с функцией машинного обучения и искусственного интеллекта. Также на вкладке предоставлена возможность добавления лицензионного ключа антиспама. Ключ поставляется в файле, имеющем расширение `.key`.

Если приобретена лицензия на антиспам, но нет в распоряжении лицензионного ключа, проверьте переписку с отделом продаж нашей компании (`sales@ideco.ru`) на наличие вложений. В случае отсутствия вложений запросите ключ заново, выслав письмо на `sales@ideco.ru` с указанием наименования организации или номера лицензии.

Для работы антиспама и антивируса Касперского необходимо включить почтовый сервер. Перед загрузкой ключа обязательно включите модуль **Антиспам и антивирус**.

Настройки фильтрации

Позволяет задать правила обработки и сортировки нежелательных сообщений:



- **Сортировка спама отключена** - отключение сортировки.
- **Перемещать спам в IMAP-папку Spam** - перемещение нежелательных писем в папку Spam, созданную почтовым сервером/релеем. По умолчанию опция включена.
- **Удалять спам** - удаление нежелательных писем с сервера.
- **Почтовый ящик для спама** - пересылка всего входящего спама на указанный ящик. Не указывайте ящик Spam.
- **Ящики, исключенные из сортировки спама** - указание почтовых адресов, которые не будут проверяться на спам.

Правила для разрешенных адресов в Антиспаме формируются автоматически на основе правил, добавленных на NGFW Novum в **Правила** → **Разрешенные адреса**. Адреса, добавленные на вкладке **Запрещенные адреса**, обрабатываются только NGFW Novum.

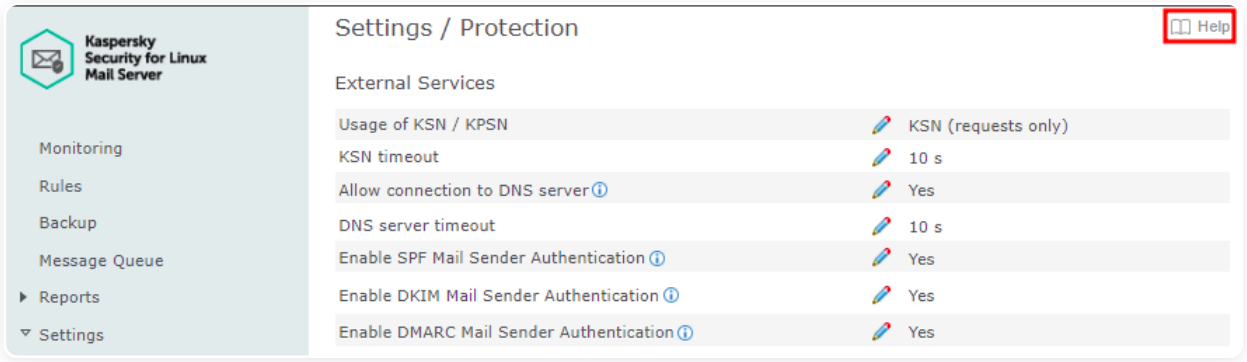
Веб-интерфейс для Антиспама

> Для включения веб-интерфейса Антиспама требуется, чтобы модуль **Антиспам и антивирус** был включен.

Веб-интерфейс имеет следующие преимущества:

- Отображает детальную статистику по категориям Антиспама Касперского.
- Генерирует отчеты по работе за определенный период.
- Отображает очередь обрабатываемых сообщений.
- Ведет аудит всех действий, производимых с Антиспамом.

Документацию по продукту Kaspersky Security for Linux Mail Server можно посмотреть по ссылке. Также перейти в документацию можно через веб-интерфейс, нажав на кнопку **Help**:



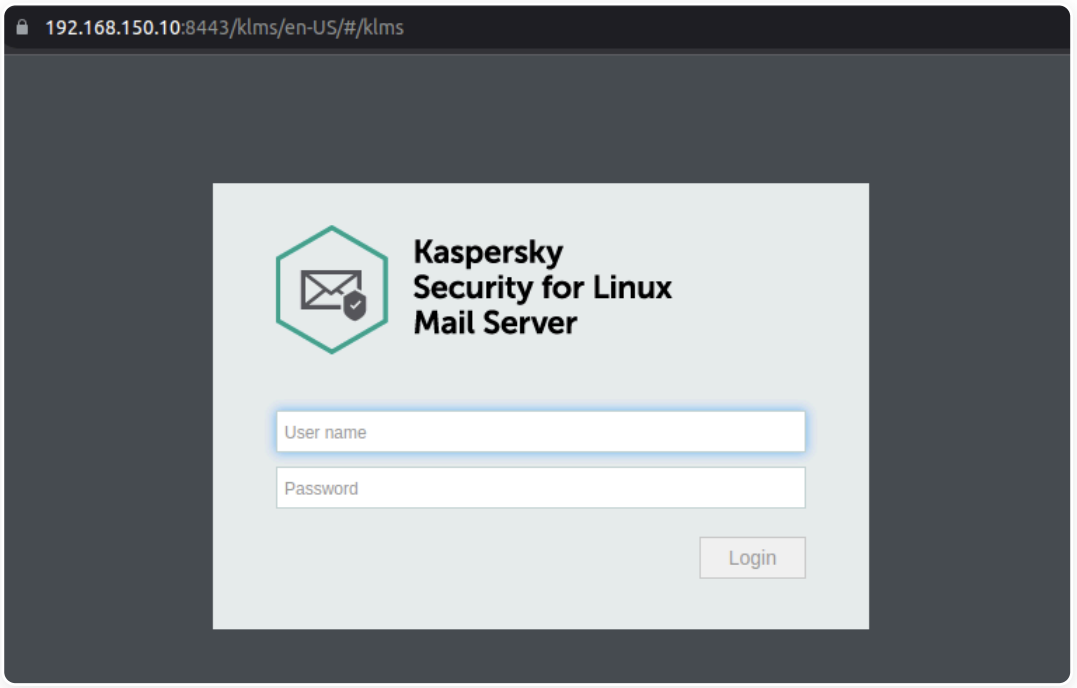
Чтобы включить веб-интерфейс для Антиспама:

1. Перейдите в **Управление сервером** → **Терминал** и выполните команду `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`

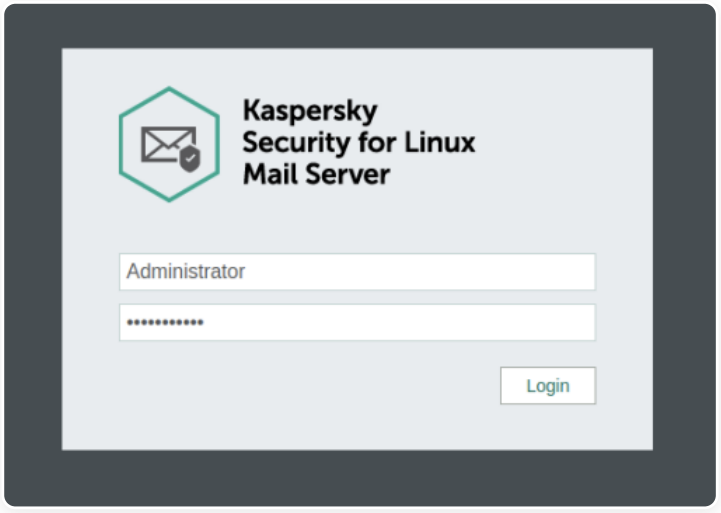
2. Задайте пароль для стандартного аккаунта **Administrator**, состоящий минимум из 8 символов: строчных букв, заглавных букв, специальных символов, чисел:

```
[admin@localhost ~]# /opt/kaspersky/klms/bin/klms-control --set-web-admin-password
Password must satisfy three of four requirements:
       (1) Contains an uppercase letter;
       (2) Contains a lowercase letter;
       (3) Contains a special symbol;
       (4) Contains a number.
       And it must at least contain 8 characters

Enter new WEB console password for Administrator:
Retype new WEB console password for Administrator:
[admin@localhost ~]#
```

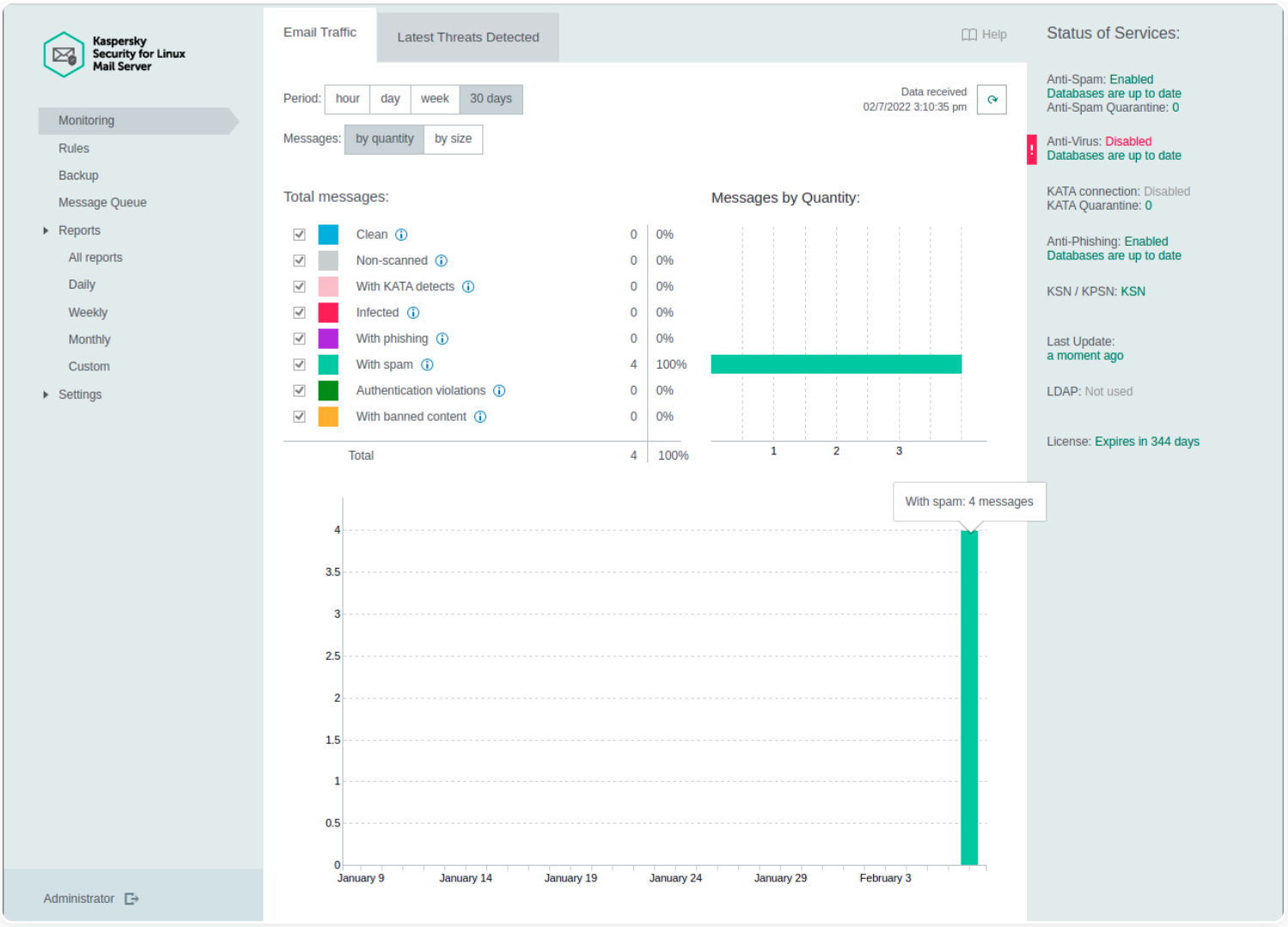
3. Перейдите в адресной строке по пути `ngfw_ip_address:8443/klms/` чтобы получить доступ к веб-интерфейсу:



4. Войдите в веб-интерфейс с учетной записью **Administrator** и ранее заданным в терминале паролем:



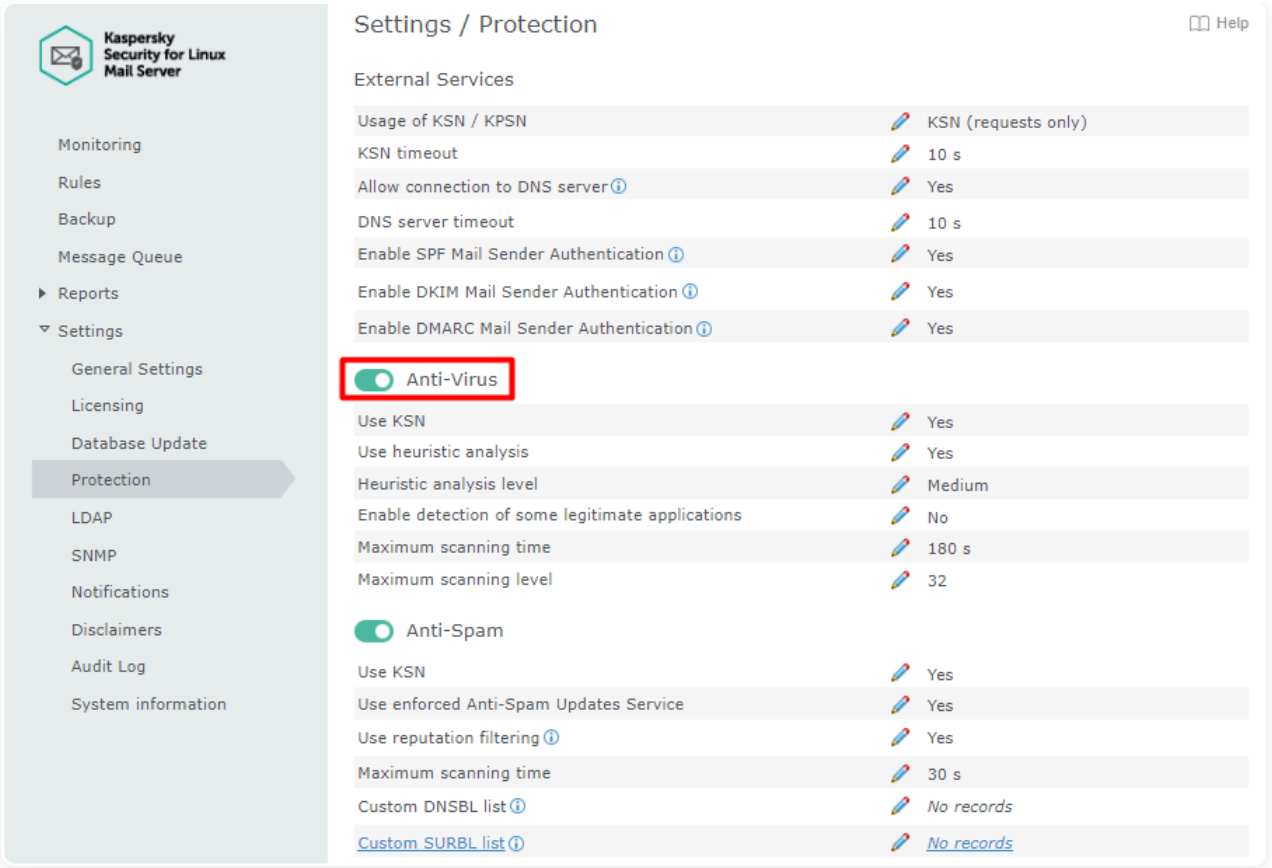
После успешного входа будет отображен дашборд со статистикой работы Антиспама:



Включение Антивируса почтового сервера

1. Перейдите в веб-интерфейс Антиспама.

2. Включите антивирус почтового сервера, перейдите в **Settings** → **Protection** и активируйте опцию **Anti-Virus**:



Службы антиспама и антивируса почтового сервера преднастроены для оптимальной работы в составе Ideco NGFW Novum. Не рекомендуем вносить какие-либо изменения в раздел **Settings**. Веб-интерфейс решения Kaspersky Security for Linux Mail Server предусмотрен только для работы с отчетностью и для внесения изменений, описанных в этой статье.

Правила

API

Функциональность доступна только в **Системном контексте**.

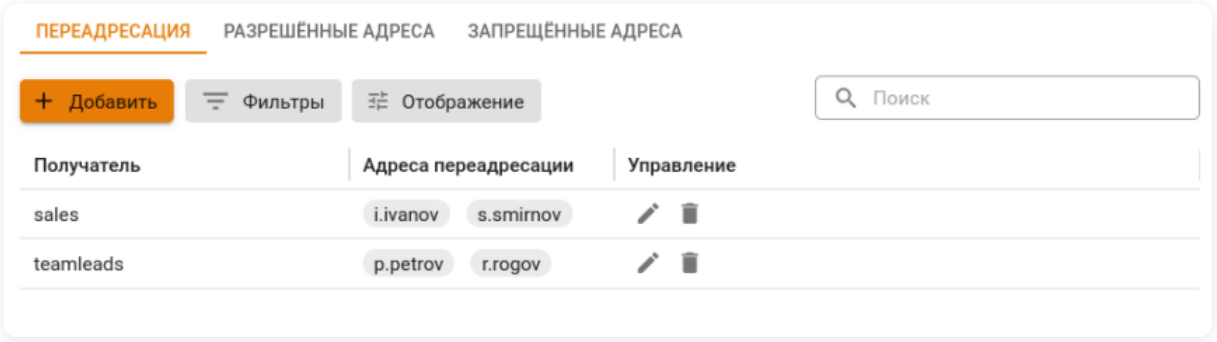
Раздел **Правила** состоит из трех вкладок: **Переадресация, Разрешенные адреса, Запрещенные адреса**. На каждой вкладке доступна фильтрация по кнопке **Фильтры**.

Переадресация

Позволяет настроить переадресацию почты на сервере с помощью почтовых алиасов.

Алиасы, в отличие от почтовых ящиков, не требуют логинов и паролей, алиасы закрепляются за ящиком и служат копией ящика с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, может служить группой рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в графе **Получатель**, должен реально существовать.

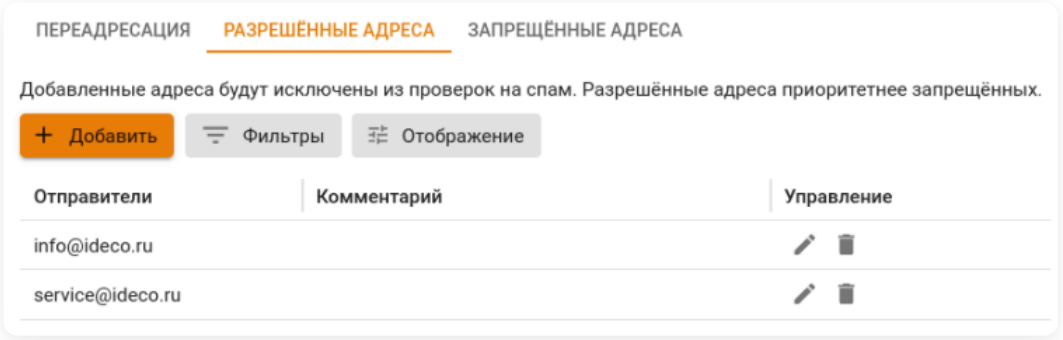
Подробнее с документацией по настройке почтовых алиасов на Ideco NGFW Novum ознакомьтесь в статье Переадресация почты:



Разрешенные адреса

Позволяет указывать почтовые домены, IP-адреса почтовых серверов и почтовые ящики, отправления с которых не будут проверяться на спам.

Если ящик одновременно указан в **Запрещенном адресе** и в **Разрешенном адресе**, то наивысший приоритет имеет **Разрешенный адрес**.



При занесении пересекающихся источников в оба списка корреляции между источниками не происходит. Приоритет будет отдан сначала IP-адресам, затем ящикам и затем доменам. То есть, если запрещен IP-адрес почтового сервера и разрешен домен, который IP-адрес

обслуживает, то письма от него будут блокироваться (блокировка по IP-адресу имеет приоритет). Обратный пример: разрешен IP-адрес, но запрещен домен. Письма блокируются, просто на более поздней стадии, при проверке почтового домена.

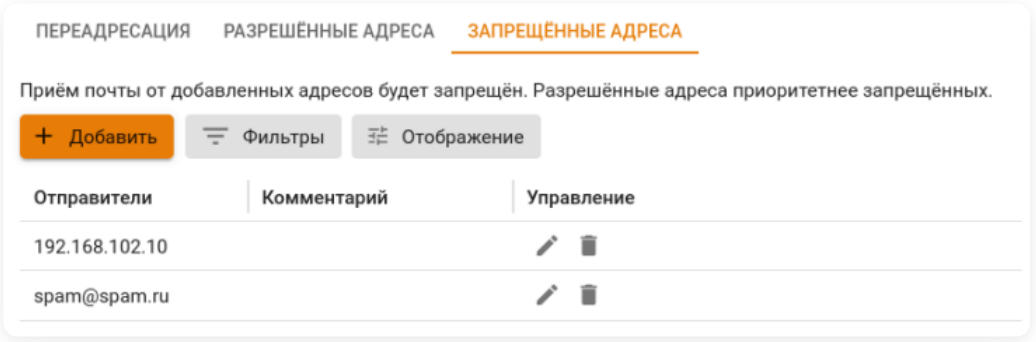
Еще один пример: в **Разрешенные адреса** внесен домен, в **Запрещенные адреса** - ящик из этого домена. Тогда письма с ящика будут заблокированы.

Обратный пример: письма от ящика, занесенного в **Разрешенные адреса**, будут разрешены, даже если домен, которому принадлежит ящик, занесен в **Запрещенные адреса**.

Схема обработки писем в почтовом сервере представлена в статье Схема фильтрации почтового трафика. Обратите внимание, что Разрешенные и Запрещенные адреса срабатывают после нескольких предварительных этапов фильтрации.

Запрещенные адреса

Позволяет указывать почтовые домены и ящики, отправления с которых не будут приниматься сервером:



Переадресация почты

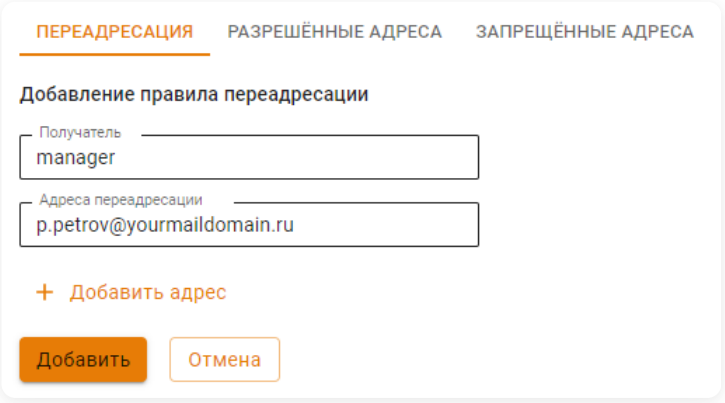
Функциональность доступна только в **Системном контексте**.

Чтобы создавать и редактировать почтовые правила переадресации (алиасы), перейдите в **Почтовый релей → Правила → Переадресация**.

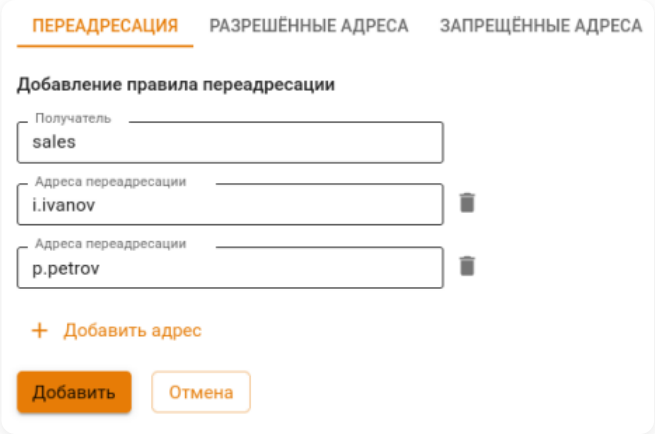
Почтовые алиасы отличаются от почтовых ящиков тем, что не требуют логинов и паролей. Алиасы закрепляются за ящиком и служат копией ящика с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, можно сказать что алиас - это группа почтовых ящиков или группа рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Часть адреса `@yourdomain.com` можно не указывать при создании правил, если ящик расположен на почтовом сервере Ideco NGFW Novum. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в поле **Получатель**, должен реально существовать.

Примеры

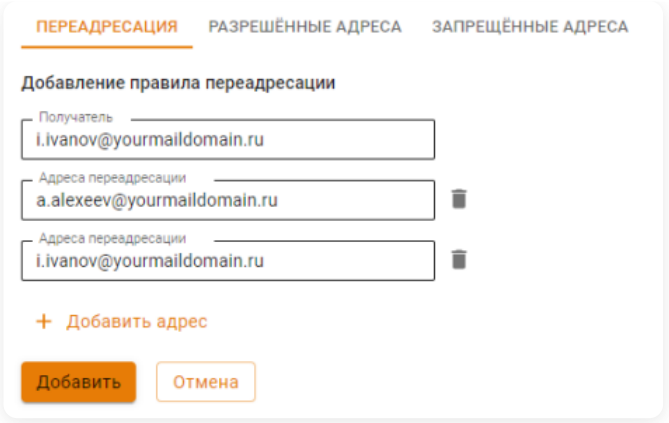
- Создать алиас `manager@yourdomain.ru` для ящика менеджера компании для связи с клиентами и партнерами, у которого реальный почтовый ящик имеет имя `p.petrov@yourmaildomain.ru`:



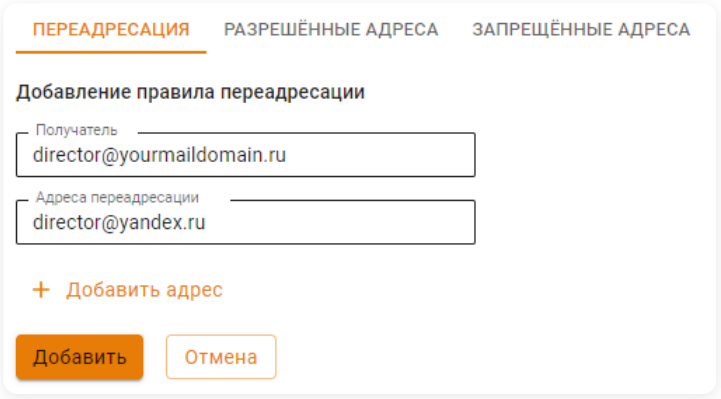
- Создать корпоративный алиас для отдела продаж `sales@yourmaildomail.ru`, чтобы почта пересылалась на всех сотрудников этого отдела:



- Создать временный алиас для переадресации почты сотрудника, который находится в отпуске `i.ivanov@yourmaildomail.ru`, на ящик коллеги `a.alexeev@yourmaildomain.ru` с сохранением почты на ящике `i.ivanov@yourmaildomail.ru`:



- Создать алиас `director@yourmaildomain.ru`, который будет перенаправлять почту на реальный ящик `director@yandex.ru`:



Работа почты при настроенных правилах переадресации

Письма, приходящие на несуществующий ящик (алиас) `manager@yourdomain.ru`, будут попадать на реальный `p.petrov@yourmaildomain.ru`. Также есть алиас для отдела продаж `sales@yourmaildomail.ru`, который, по сути, служит алиасом для рассылки почты и сам писем не хранит. Это удобно, если есть информация для отдела продаж, которую надо распространить на каждого сотрудника. Все то же самое можно сделать, если просто указать в письме всех получателей, но использовать алиас намного удобнее. Также сотрудник с почтой `i.ivanov@yourmaildomail.ru` сейчас находится в отпуске, вся приходящая к нему почта попадает на его ящик и дублируется на `a.alexeev@yourmaildomain.ru`. Последнее правило позволяет директору получать почту не на корпоративный ящик, а на его личную почту на Яндексе.

Алиас не является действительным почтовым ящиком. К нему нельзя подключиться почтовым клиентом, используя логин и пароль, как в обычном почтовом аккаунте. Таким образом, создание алиасов не увеличивает максимально возможное количество реальных почтовых аккаунтов на Ideco NGFW Novum.

Почтовая очередь

API

Функциональность доступна только в **Системном контексте**.

Модуль позволяет управлять входящей и исходящей отложенной корреспонденцией. Для анализа возможных причин задержки корреспонденции в очереди можно использовать информацию из соответствующего столбца таблицы для каждого письма. По кнопке **Фильтры** доступна фильтрация по каждому столбцу.

Почтовая очередь позволяет выполнять следующие выборочные и групповые действия с отправлениями:

- Очистка очереди
- Повторная отправка отдельного письма
- Удаление отдельных писем из очереди
- Повторная отправка всей корреспонденции из очереди

Значение в столбце **Время доставки** соответствует времени поступления письма в очередь. Если письмо не будет отправлено в течение 7 дней, то письмо будет удалено из почтовой очереди и не будет доставлено получателю.

При обновлении Ideco NGFW Novum почтовая очередь очищается.

Проверка настроек почтового сервера

Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса check.smtp.bz.

При правильной настройке почтовый сервер на Ideco NGFW Novum должен получить результат **Отлично**.

Настройка почтовых клиентов

Функциональность доступна в **Системном контексте**.

Примечание

В Ideco NGFW Novum нет ограничений по количеству почтовых клиентов для одного почтового адреса по протоколу IMAP.

Настройка почтового клиента при работе из локальной сети

1. Сервер входящей почты работает на 995 TCP-порту (POP3) и на 143 TCP-порту (IMAP) с шифрованием STARTTLS/SSL:

- В качестве логина прописывается логин от учетной записи пользователя.
- В качестве пароля всегда прописывается пароль от учетной записи пользователя (в том числе для пользователей, импортированных из Active Directory). Задать отдельный пароль на почтовый ящик нельзя.

2. Сервер исходящей почты работает на 587 порту TCP с шифрованием STARTTLS/SSL. Без авторизации возможна отправка почты только из доверенных сетей (настройте доверенные сети в **Почтовый релей** → **Расширенные настройки** → **Безопасность**).

Настройка почтового клиента при работе из внешней сети

Важно

Начиная с версии UTM 7.0.0, подключиться из внешней сети клиентом Microsoft Outlook (любой версии) по протоколу POP3 можно только с типом шифрования SSL. Подключение к почтовому серверу извне без шифрования запрещено.

Остается возможность подключаться по протоколу IMAP с использованием STARTTLS или SSL. Для этого выберите соответствующий тип шифрования в Outlook.

1. Сервер входящей почты работает на 995 TCP-порту (POP3S) и на 143 TCP-порту (IMAP-STARTTLS/SSL), шифрование обязательно:

- В качестве логина прописывается логин от учетной записи пользователя.
- В качестве пароля всегда прописывается пароль от учетной записи пользователя. Задать отдельный пароль на почтовый ящик нельзя.

2. Сервер исходящей почты работает только с авторизацией и шифрованием. Необходимо использовать 587 порт для подключения (а не 25). Тип шифрования, логин и пароль указываются аналогично серверу входящей почты.

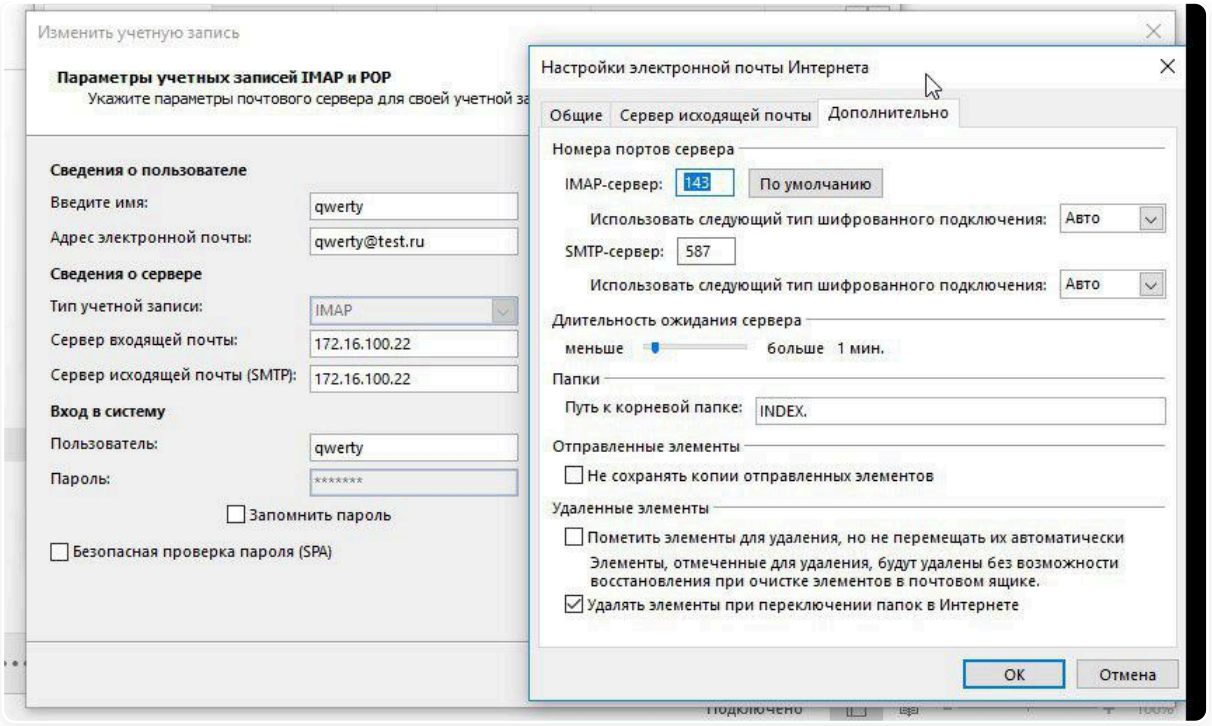
Для любого почтового клиента, кроме веб-почты в составе NGFW, установите корневой сертификат сервера NGFW. Сертификат можно скачать в **Сервисы** → **Сертификаты**.

Примеры настроек популярных почтовых клиентов

Outlook 2013 и 2016

Пример настроек клиента Microsoft Outlook 2013 по протоколу IMAP:

Пример настроек клиента Microsoft Outlook 2016 по протоколу IMAP:



Для отображения IMAP-папок отключите опцию **При просмотре дерева в Outlook показывать только подписанные папки** в свойствах IMAP-папок:

---

iPhone

Установка корневого SSL-сертификат NGFW

1. Скачайте сертификат в **Сервисы** → **Сертификаты** и перенесите на настраиваемое устройство (например, отправив по почте).

2. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством**.

3. Выберите сертификат и нажмите кнопку **Установить**:

4. Зайдите в **Настройки** → **Основные** → **Об этом устройстве** и выберите **Доверие сертификатов**.

5. Включите опцию **Доверять корневым сертификатам полностью**:

Настройка почтового ящика

1. Перейдите в Учетную запись почты и нажмите **Дополнительно**:

2. Скорректируйте настройки:

Thunderbird

1. Перейдите в **Настройки** → **Параметры ученой записи**.

2. Заполните обязательные поля:

- **Имя сервера**.
- **Порт**.
- **Имя пользователя**.
- **Защита соединения**.
- **Метод аутентификации** (рекомендуем указать **Обычный пароль**).

При необходимости заполните **Параметры сервера** и **Хранилище сообщений**.

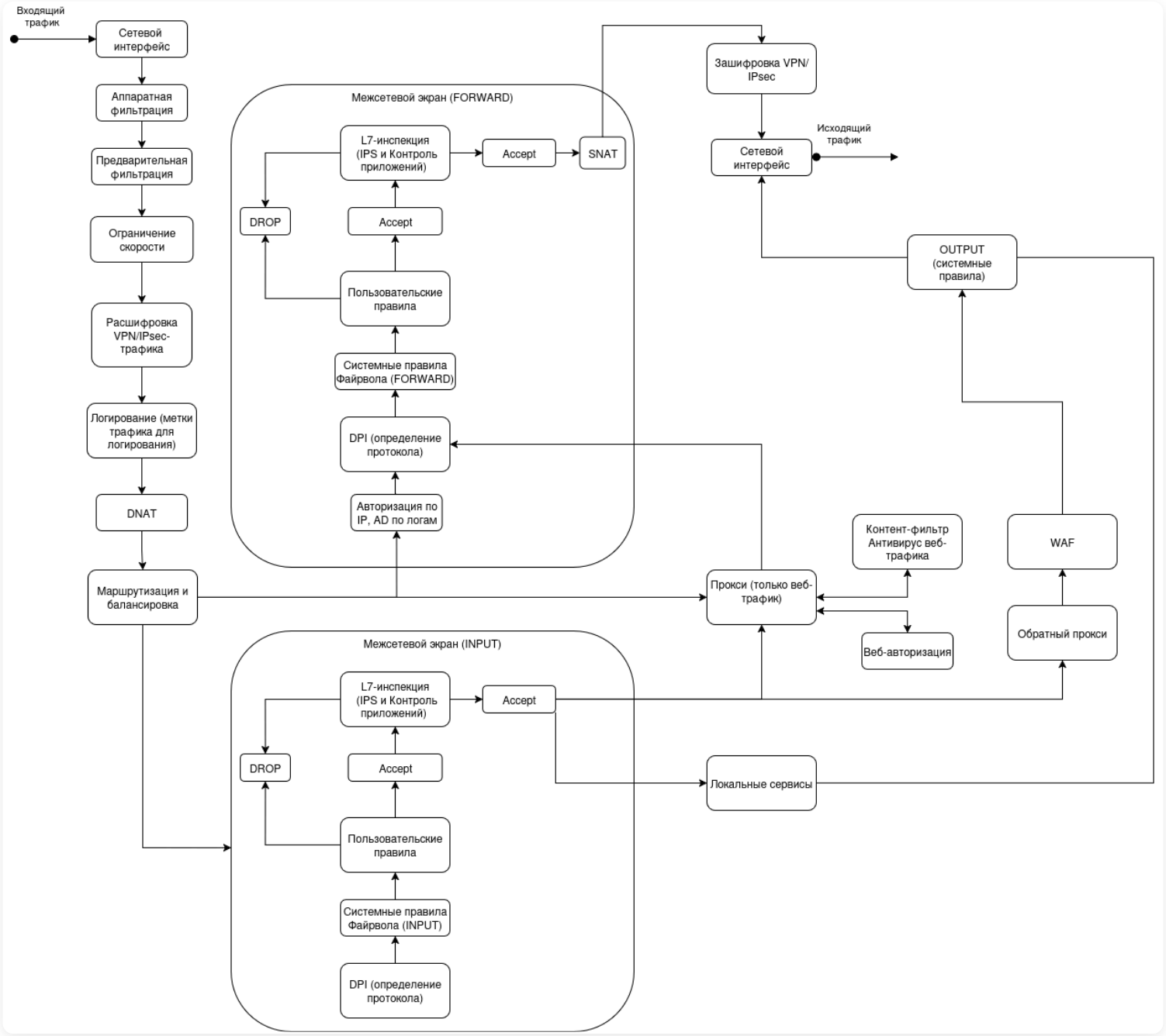
Полный цикл обработки трафика в Ideco NGFW Novum

Классический контекст | Высокопроизводительный контекст

Статья описывает цикл, который проходят пакеты трафика в Ideco NGFW Novum, в зависимости от сценария.

Обработку трафика условно можно разделить на три стадии:

- Предварительная.
- Межсетевой экран.
- Завершающая.



К **Предварительной стадии** можно отнести **Аппаратную** и **Предварительную фильтрацию**.

На второй стадии трафик проходит либо таблицу **INPUT**, либо таблицу **FORWARD** **Межсетевого экрана**:

- В первом случае - одно из двух:
  - Трафик проходит таблицу **INPUT** (пользовательские правила и L7-фильтрацию) и направляется в локальные сервисы NGFW (например, DNS, NTP).
  - Трафик направляется в **Прокси** или **Обратный прокси**, обрабатывается соответствующими модулями и направляется в таблицу **FORWARD** (от **Прокси**) или в **OUTPUT** (от **Обратного прокси**).
- Во втором случае трафик проходит таблицу **FORWARD** (пользовательские правила, L7-фильтрацию, **Прокси** с **Расшифровкой TLS**, **Контент-фильтром** и **Антивирусом**).

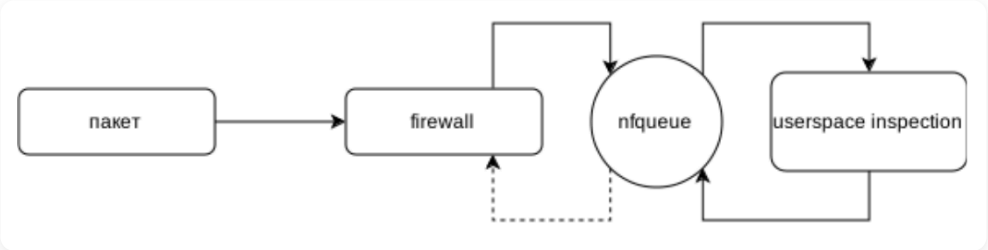
На **Завершающей стадии** трафик после обработки зашифровывается (при необходимости) и направляется получателю.

Принцип работы L7-инспекций

Межсетевой экран работает по принципу stateful-фильтрации - решение о пропуске или блокировке принимается один раз при установлении соединения. L7-инспекции анализируют каждый пакет в рамках этого соединения и могут инициировать блокировку на любом этапе.

Трафик на обработку **Предотвращением вторжений** из **Межсетевого экрана** передается через NFQUEUE.

NFQUEUE - это технология интеграции межсетевого экрана linux с userspace-процессами, выполняющими инспекцию, которая позволяет выполнять L7-инспекции после L3-правил **Межсетевого экрана**:



Примеры прохождения трафика

Транзит трафика с фильтрацией и прозрачным прокси

1. Трафик пользователя попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию**, **Ограничение скорости** (если трафик подпадает под правила, то может быть заблокирован и дальше не пойдет).

2. Если пользователь подключился через VPN, трафик будет расшифрован.

3. Будет проверена DNAT-таблица **Межсетевого экрана**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

4. Веб-трафик направляется в **Прокси** для веб-авторизации, проверки **Контент-фильтром** и **Антивирусом веб-трафика**.

5. Трафик направляется в **FORWARD**-таблицу **Межсетевого экрана**:

- Если трафик подпадает под запрещающее правило, он блокируется.
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию при включенных модулях **Предотвращение вторжений** и/или **Контроль приложений**.

6. Трафик проверяется на соответствие правилам таблицы **SNAT**. При необходимости подменяется IP-адрес источника.

7. Если пользователь подключился через VPN, трафик будет зашифрован.

Прямое подключение к прокси

1. Трафик пользователя попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию**, **Ограничение скорости** (если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет).

2. Будет проверена **DNAT**-таблица **Межсетевого экрана**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT**, веб-трафик оттуда захватывается **Прокси**, где обрабатывается **Контент-фильтром** и **Антивирусом веб-трафика**. Пользователь проходит веб-авторизацию (если веб-авторизация настроена).

4. Трафик направляется в **FORWARD**-таблицу **Межсетевого экрана**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию при включенных модулях **Предотвращение вторжений** и/или **Контроль приложений**.

5. Запрос направляется ресурсу, на который обратился пользователь, ответ направляется пользователю (трафик вновь проходит пункт 1 - пункт 4).

Публикация ресурсов через обратный прокси

1. Трафик из внешней сети попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию** (если трафик подпадает под их правила, то он может быть заблокирован и дальше не пойдет).

2. Будет проверена **DNAT**-таблица **Межсетевого экрана**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT Межсетевого экрана**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию при включенных модулях **Предотвращение вторжений** и/или **Контроль приложений**.

3. Трафик попадает в **Обратный прокси**, где проходит через **Web Application Firewall**. Если трафик подпадает под правила WAF, он может быть отброшен.

4. Трафик направляется ресурсу в локальной сети, который был опубликован через **Обратный прокси**, и возвращает ответ.

Полный доступ

1. Трафик пользователя попадает на Ideco NGFW Novum, проходит **Аппаратную** и **Предварительную фильтрацию**, **Ограничение скорости**. Если трафик подпадает под правила - он будет заблокирован и дальше не пойдет.

2. Пользователи могут подключаться через VPN, включая шифрованные подключения.

3. **DNAT**-таблица **Межсетевого экрана** не проверяется: даже если трафик подпадет под правила - IP-адрес или порт назначения не изменится.

4. Трафик, минуя стадию авторизации, пройдет таблицу **FORWARD** и не будет отброшен вне зависимости от созданных там правил фильтрации.

Порядок обработки веб-трафика в Ideco NGFW Novum

Порядок обработки веб-трафика:

1. Ограничение скорости.

2. DNS.

3. Захват трафика для фильтрации (прокси-сервер):

- Контент-фильтр.
- Антивирус веб-трафика.

4. Межсетевой экран.

5. Контроль приложений.

6. Система Предотвращения вторжений.

INPUT-правила Межсетевого экрана обрабатывают трафик раньше DNS (если включен перехват DNS-запросов) и прокси-сервера.

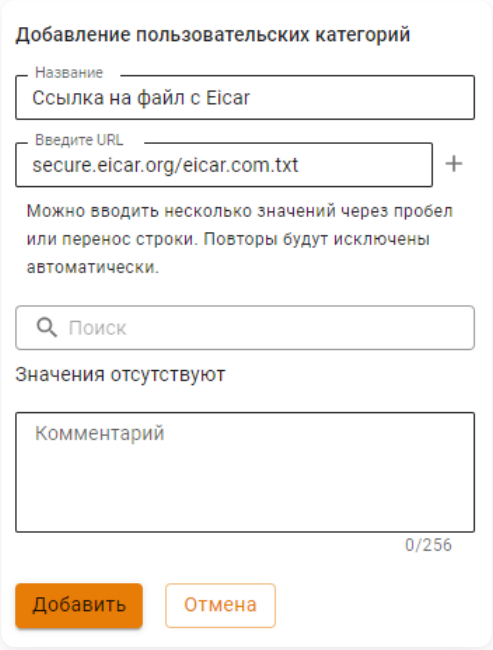
В модули **Контроль приложений** и **Предотвращение вторжений** отправится только трафик, который попадает под разрешающее правило **Межсетевого экрана** с включенной проверкой через профиль контроля приложений и профиль предотвращения вторжений соответственно.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика?

Для примера использовался тестовый файл с Eicar, доступный для скачивания по ссылке.

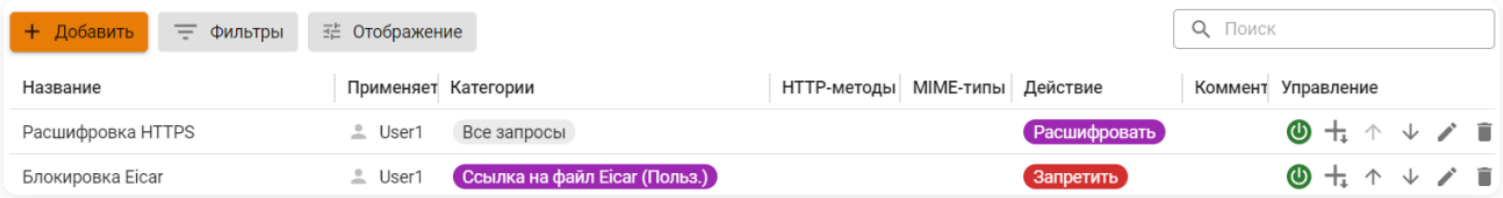
1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Пользовательские категории**. Нажмите **Добавить**.

2. Введите ссылку на ресурс и нажмите + :



3. Перейдите на вкладку **Правила** и создайте два правила для **User1**:

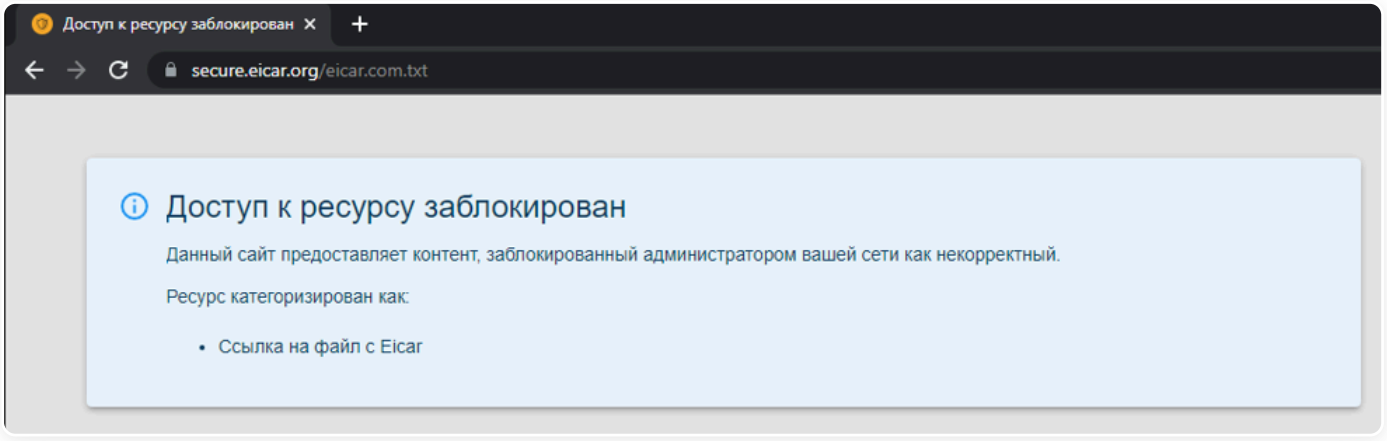
- Правило расшифровки всех HTTPS-запросов, чтобы антивирус мог работать с HTTPS-трафиком.
- Правило блокировки созданной пользовательской категории:



4. Убедитесь, что опция **Антивирус** переведена в положение **Включен**.

5. Авторизуйте пользователя и перейдите по ссылке на скачивание Eicar.

Откроется страница блокировки **Контент-фильтра**:



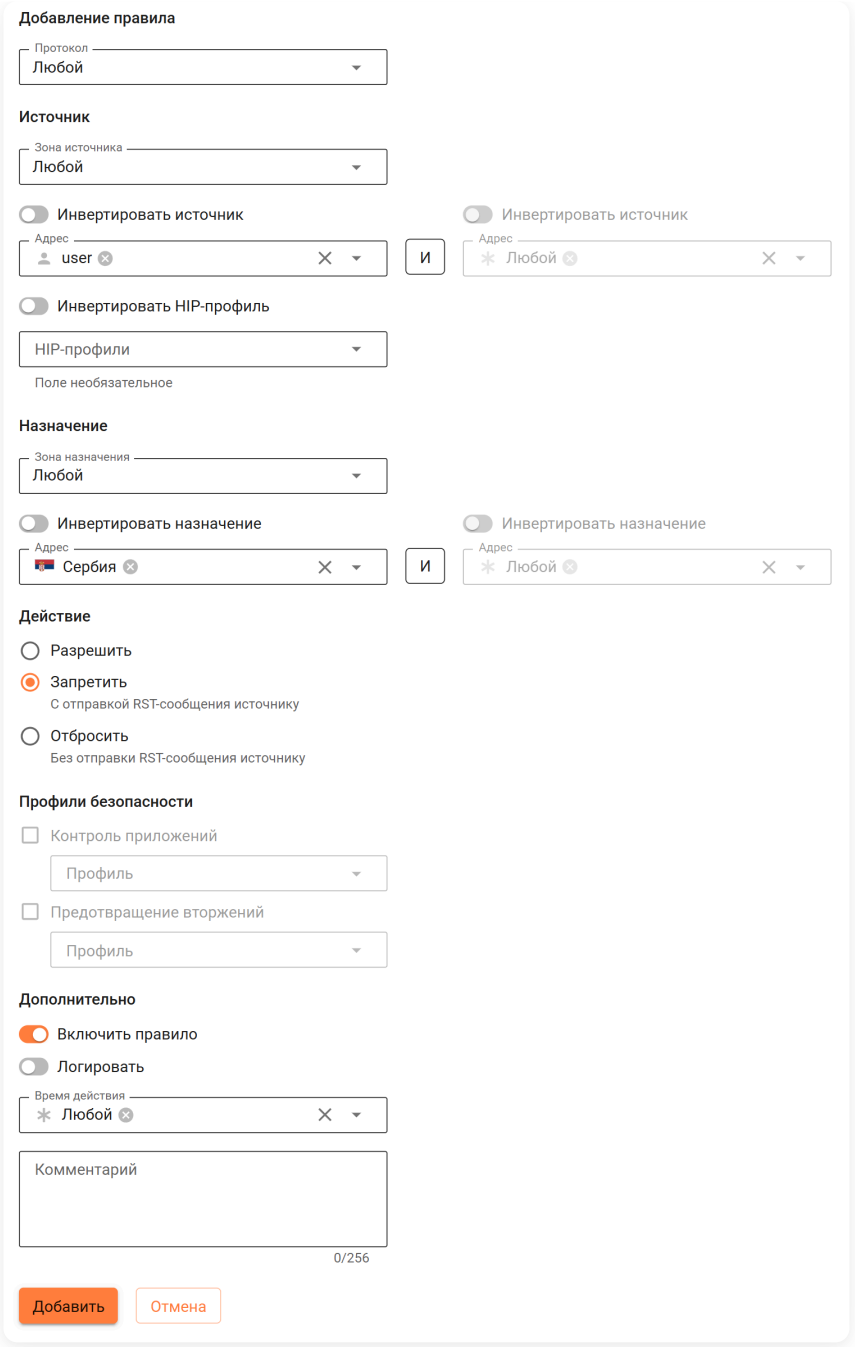
Контент-фильтр обрабатывает трафик приоритетнее, чем антивирусы. Просмотреть информацию о срабатывании правил **Контент-фильтра** можно в **Отчеты** → **Трафик** → **Топ сайтов**.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Межсетевой экран?

Для примера заблокируем пользователю `user` сайт `rts.rs`.

1. Перейдите в **Правила трафика** → **Межсетевой экран**, на вкладку **FORWARD** и нажмите **Добавить**.

2. Заполните поля:

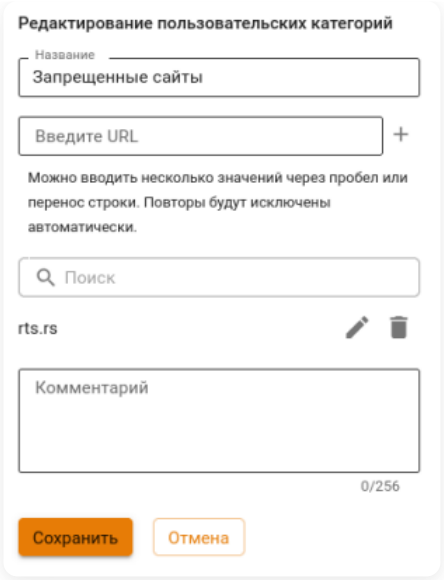


- **Протокол** - выберите **Любой**.
- **Адрес** источника - выберите пользователя `user`.
- **Адрес** назначения - выберите страну **Сербия**.
- **Действие** - выберите **Запретить**.

3. Нажмите **Добавить**.

4. Перейдите в **Правила трафика** → **Контент-фильтр** → **Пользовательские категории** и нажмите на  напротив категории **Запрещенные сайты**.

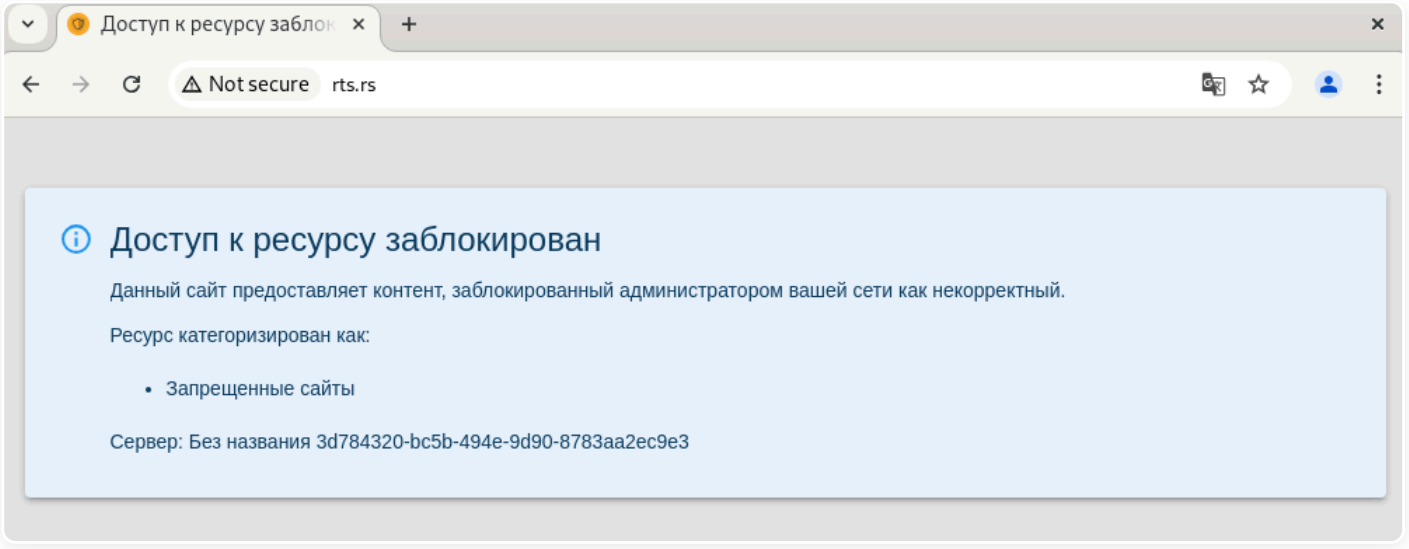
5. Добавьте ссылку на сайт `rts.rs` и нажмите **Сохранить**:



6. Убедитесь, что в таблице правил **Контент-фильтра** включено правило запрета для категории **Запрещенные сайты**.

7. Авторизуйте пользователя и перейдите на сайт `rts.rs`.

Откроется страница блокировки **Контент-фильтра**:



Контент-фильтр обрабатывает трафик приоритетнее, чем **Межсетевой экран**.

В статье представлен полный перечень видеоинструкций по продуктам Ideco

Ссылки на другие ресурсы

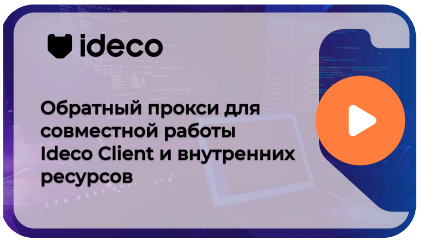
YouTube | RUTUBE | VK Видео



Последние видео







Видеоинструкции NGFW

Список видеоинструкции разбитые по разделам

Пользователи | Правила трафика | Профили безопасности | Сервисы | Маршрутизация | Управление сервером | Почтовый релей

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Вопросы и ответы

Как заблокировать чат-боты?

Заблокировать чат-боты можно, создав правило в Контент-фильтре. О том, как это сделать, написано в статье Блокировка чат-ботов.

Как настроить совместную работу ViPNet-Координатора с Ideco NGFW Novum ?

Процесс настройки подробно описан в статье.

Как настроить автоматическую аутентификацию на Linux через веб-интерфейс ?

Процесс настройки подробно описан в статье Настройка автоматической аутентификации на NGFW на Linux. Скрипт подходит для всех Linux-систем с Python 3.5 и выше.

Есть ли возможность добавлять сигнатуры IPS?

Да, добавьте сигнатуру вручную в файл `/var/opt/ideco/suricata-backend/custom.rules`. Важно: sid правила не должен совпадать с существующими.

Подробнее о добавлении в статье Как исключить узел из обработки системой IDS/IPS через терминал.

Как настроить кластеризацию Active/Active?

Для настройки кластеризации Active/Active воспользуйтесь решением наших партнеров АО "НПП "Цифровые решения". Инструкция по интеграции Ideco NGFW Novum и брокера сетевых пакетов DS Integrity NG - по ссылке.

Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW Novum?

Порядок обработки веб-трафика и примеры проверки работоспособности модулей описаны в статье.

Хочу работать из дома, подключившись по RDP к своем компьютеру в офисе. Можно ли опубликовать RDP, чтобы RDP был доступен из интернета?

Не рекомендуем так делать. В такой ситуации существуют риски успешного взлома с помощью RDP. Даже сложный пароль и актуальные обновления не гарантируют того, что злоумышленники не смогут проникнуть внутрь сети через опубликованный RDP. Не рекомендуем публиковать RDP и подобные сервисы "наружу" (SSH, FTP и т.д.), так как это увеличивает количество потенциальных точек входа для злоумышленников. Рекомендуем использовать подключение по VPN к своей сети.

Как создать VPN-подключение?

В зависимости от операционной системы выберите подходящую инструкцию из Инструкций по созданию VPN-подключений.

Что делать, если ваш IP попал в черные списки DNSBL?

Если используете белый статический IP-адрес, то попадание IP-адреса в черные списки может означать, что в сети зафиксирована бот-активность, участие в DDoS-атаках, либо рассылка спама.

Наличие в черных списках динамического IP-адреса из "домашних" диапазонов IP-адресов провайдеров в целом нормальное явление, т. к. вредоносная активность в таком случае может исходить не из вашей сети.

Порядок действий при попадании в черный список описан в статье.

Утрачен пароль администратора, как восстановить?

При утере пароля администратора можно восстановить, имея физический доступ к серверу. Подробнее о процессе восстановления в статье Как восстановить доступ к Ideco NGFW Novum.

После обновления потребовалось вернуть предыдущую версию со всеми настройками. Как это сделать?

Возможность восстановиться на предыдущую версию после обновления Ideco NGFW Novum доступна с 12.X версий. Подробнее о процессе восстановления в статье Как восстановиться на прошлую версию после обновления Ideco NGFW Novum.

Как подобрать аппаратную платформу для Ideco NGFW Novum?

Ideco NGFW Novum представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW Novum основан на Fedora 42 и содержит ядро Linux с набором драйверов от этой ОС с небольшими изменениями с нашей стороны. Таким образом, Ideco NGFW Novum можно установить на большую часть оборудования, поддерживающего Fedora 42. Подробнее в статье Выбор аппаратной платформы для Ideco NGFW Novum.

Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW Novum?

Для настройки Ideco NGFW Novum воспользуйтесь рекомендациями из статьи Поддержка устаревших алгоритмов шифрования.

Как настроить прямое подключение к прокси-серверу, если ПО его не поддерживает?

При использовании прямых подключений к прокси-серверу выход в интернет будет поддерживаться всеми программами, имеющими настройки прокси-сервера, либо программами, применяющими системные настройки прокси.

Некоторое ПО не имеет настроек прокси-сервера, поэтому необходимо использовать специализированное ПО на конечных рабочих станциях для вывода в интернет таких программ. Одно из таких ПО - Proxifier.

Инструкция по настройке программы Proxifier для прямых подключений к прокси-серверу доступна по ссылке.

Как эффективно заблокировать Ammyy Admin, Анонимайзеры, BitTorrent и т. д.?

Примеры блокировки программ удаленного доступа, анонимайзеров, торрентов и др. описаны в статье Блокировка популярных ресурсов.

Как настроить SSO-авторизацию для Astra Linux в домене AD?

Описание процесса настройки можно найти в статье Настройка прозрачной авторизации на Astra linux. Это решение подходит для браузеров Chromium и Firefox.

Как восстановить Ideco NGFW Novum до первоначальных настроек?

Для возврата к первоначальным настройкам используйте бэкап, созданный после установки Ideco NGFW Novum. Если бэкапа нет - переустановите Ideco NGFW Novum.

Пример настройки Forward-зоны

Как настроить сеть, чтобы пользователи локальной сети могли обращаться к ресурсам, опубликованным на Ideco NGFW Novum. Ресурсы находятся в защищенной сети, и доступ к ним должен осуществляться напрямую, без выхода через внешний интерфейс. Подробнее в статье.

Как публиковать веб-приложения



Функциональность доступна в **Классическом** и **Системном контекстах**.

Публикация веб-серверов возможна через обратный прокси-сервер.

Как настроить публичный IP-адрес на компьютере в локальной сети

Для версии Ideco UTM 7.9.0 и старше настройка публичного IP-адреса для компьютеров, находящихся в локальной сети, невозможна.

Используйте портмаппинг, чтобы пробросить весь диапазон портов от 0 до 65535 для получения эффекта присутствия локального сервера на внешнем IP-адресе.

Практические руководства

Пошаговые инструкции по настройке и использованию возможностей Ideco NGFW

VPN-подключения

Создание VPN-подключений в различных операционных системах и устройствах

Перейти >

Аутентификация

Настройка сертификатов и аутентификации пользователей в Ideco NGFW

Перейти >

Сервисы

Практические руководства по настройке сервисов Ideco NGFW

Перейти >

Правила трафика

Настройка блокировок, межсетевого экрана и фильтрации трафика в Ideco NGFW

Перейти >

SD-WAN

Практические руководства по настройке SD-WAN в Ideco NGFW Novum

Перейти >

Маршрутизация

Практические руководства по настройке маршрутизации в Ideco NGFW Novum

Перейти >

Управление сервером

Практические руководства по управлению сервером Ideco NGFW

Перейти >

Интеграции

Практические руководства по интеграции Ideco NGFW со сторонними решениями

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Пользователи

Практические руководства по настройке VPN-подключений и аутентификации пользователей

VPN-подключения

Инструкции по созданию VPN-подключений на различных операционных системах и устройствах

Перейти >

Аутентификация

Настройка сертификатов, прозрачной авторизации и веб-аутентификации

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Инструкции по созданию VPN-подключений

Создание VPN-подключения в Ubuntu

Перейти >

Инструкция по созданию подключения в Fedora

Перейти >

Инструкция по созданию подключения в Astra Linux

Перейти >

Инструкция по созданию подключения в Windows

Перейти >

Инструкция по созданию VPN-подключения на мобильных устройствах

Перейти >

Инструкция по созданию подключения в Mac OS

Перейти >

Подключение по SSTP Wi-Fi-роутеров Keenetic

Перейти >

Создание VPN-подключения в Alt Linux

Перейти >

Как избежать проблем с подключением VPN-клиентов при нескольких серверах

Перейти >

Подключение Keenetic по SSTP или IPsec

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Создание VPN-подключения в Alt Linux

Функциональность доступна в **Классическом** и **Системном контекстах**.

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее правило для VPN-подключения.

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

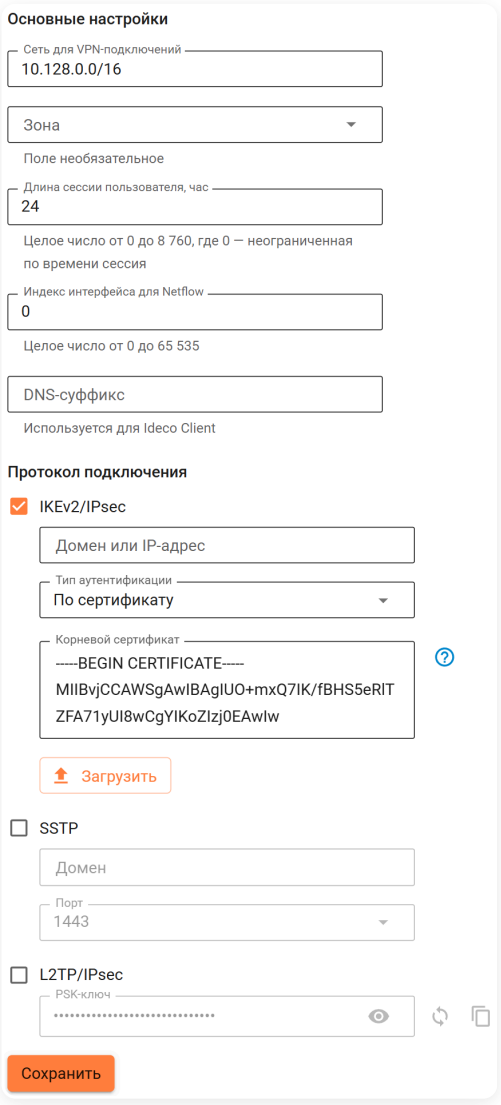
Не рекомендуем использовать для VPN-подключений кириллические логины.

Настройка подключения по протоколу IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Выберите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы → Сертификаты → Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя, нажав **Скачать корневой сертификат**.

Применение сертификатов для VPN-подключений:

- Если сертификат издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority):
  - Убедитесь, что домен указан в поле Subject Alternative Name (SAN).
  - Загрузите сертификат в **Сервисы → Сертификаты → Загруженные сертификаты**, нажав **Загрузить пользовательский сертификат**.

Создание подключения в Alt Linux:

1. Откройте терминал сочетанием клавиш **Ctrl+Alt+T** или из **Меню** и установите необходимые пакеты:

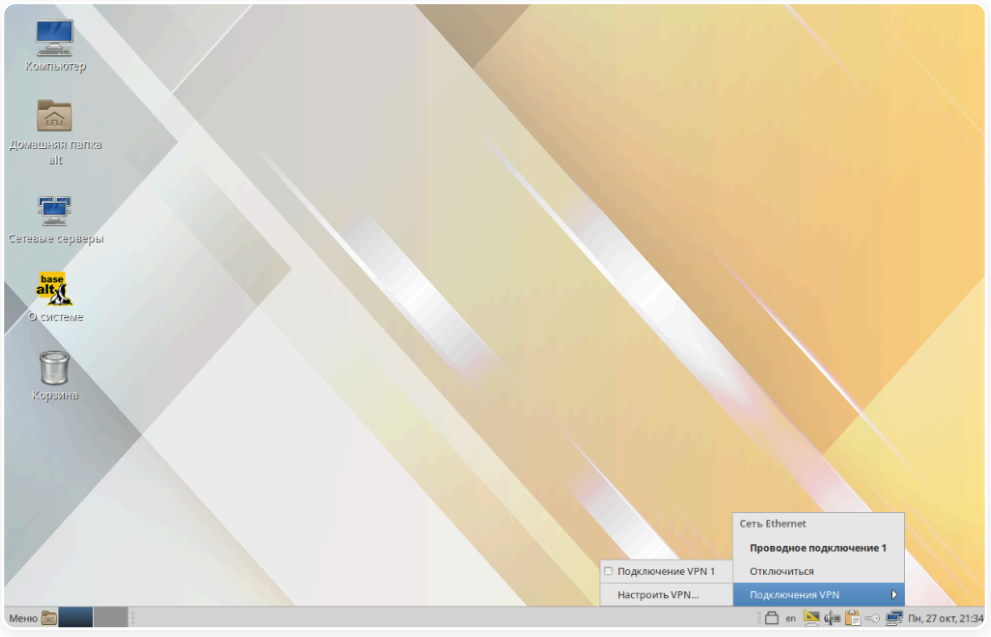
```
apt-get update && apt-get dist-upgrade && apt-get install NetworkManager-strongswan NetworkManager-strongswan-gnome strongswa
```

2. Установите корневой сертификат на рабочую станцию:

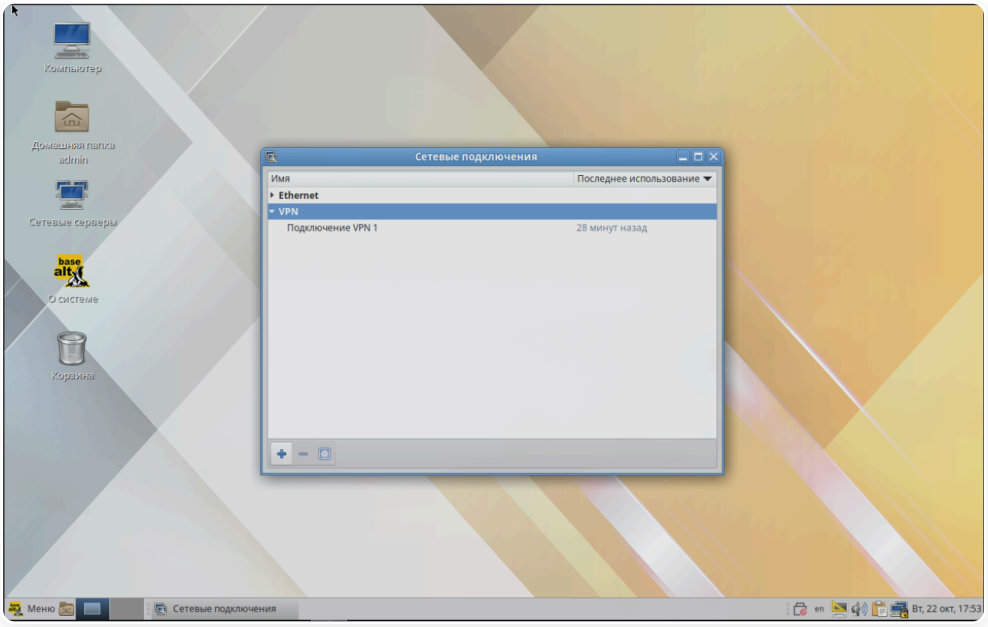
```
cp root-ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

- `root-ca.crt` - расположение сертификата/имя файла сертификата.

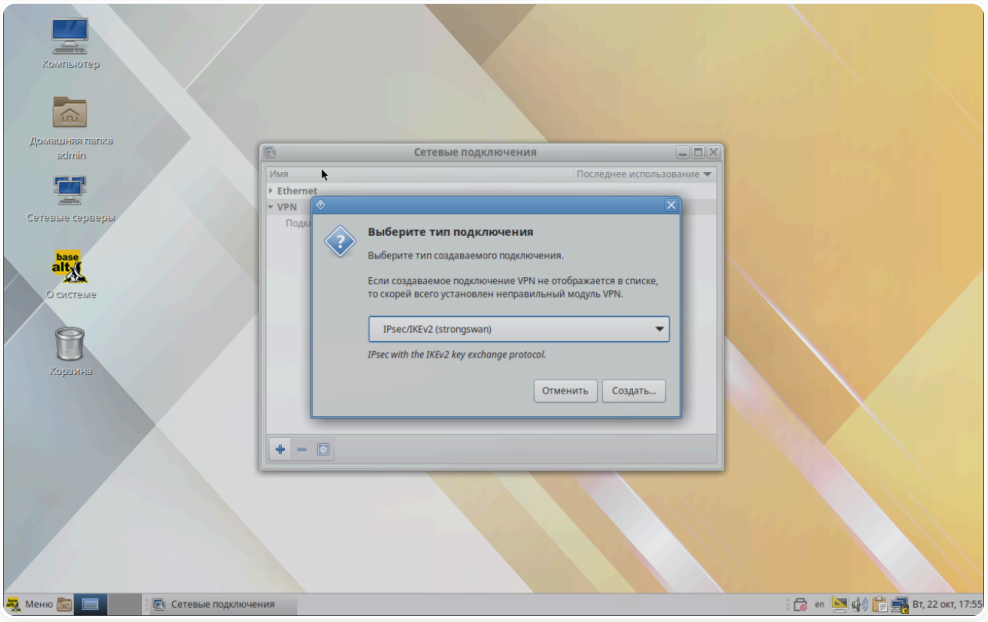
3. Перейдите в **Подключения VPN** и нажмите **Настроить VPN**:



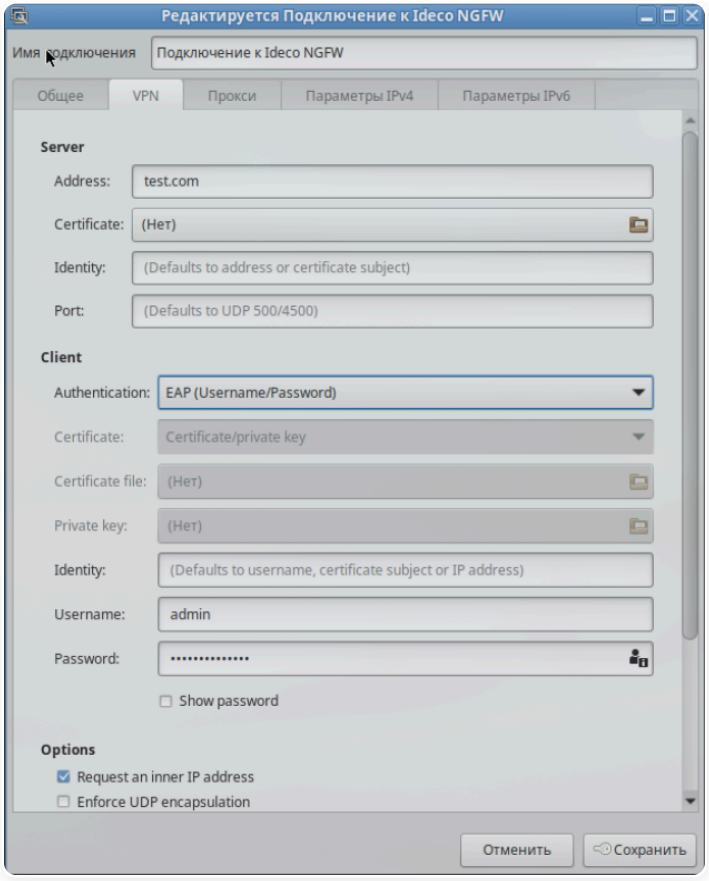
4. Добавьте новое VPN-подключение, нажав :



5. Выберите тип VPN-подключения `IPsec/IKEv2 (strongswan)` и нажмите **Создать**:

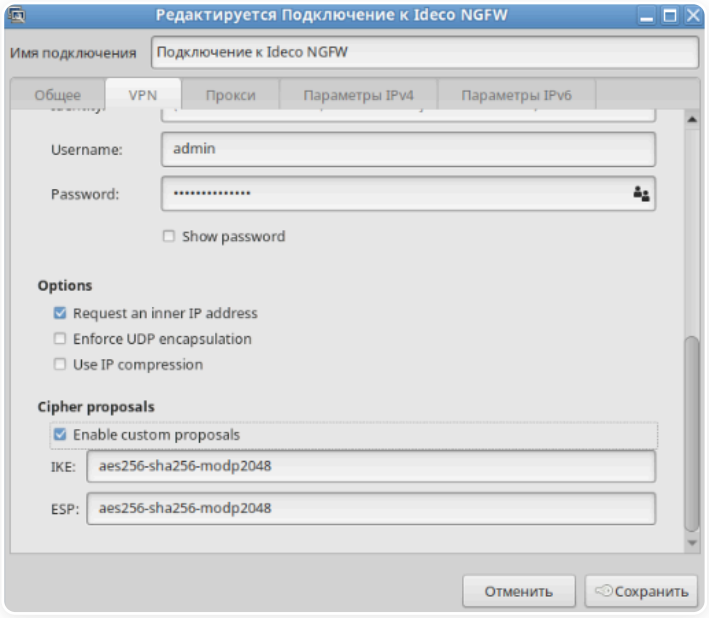


6. Заполните необходимые поля для создания VPN-подключения, как на скриншоте:



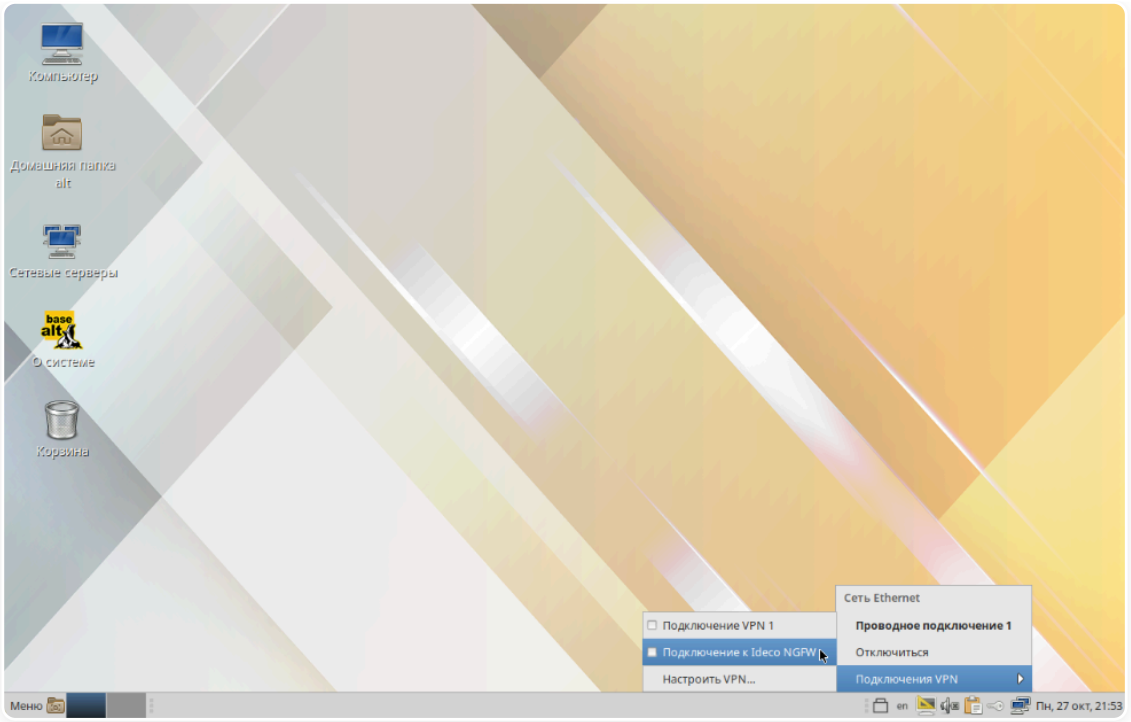
- **Address** - адрес шлюза.
- **Authentication** - тип аутентификации.
- **Username** - логин пользователя в Ideco NGFW Novum.
- **Password** - пароль пользователя в Ideco NGFW Novum.

7. Заполните параметры шифрования, как на скриншоте, и нажмите **Сохранить**:



- В блоке **Options** включите опцию **Request an inner IP address**.
- В блоке **Cipher proposals** включите опцию **Enable custom proposals** и заполните поля:
  - **IKE** - aes256-sha256-modp2048.
  - **ESP** - aes256-sha256-modp2048.

8. Запустите созданное VPN-подключение:



Полезные ссылки

- VPN-подключения

Создание VPN-подключения в Ubuntu

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

Не рекомендуем использовать для VPN-подключений кириллические логины.

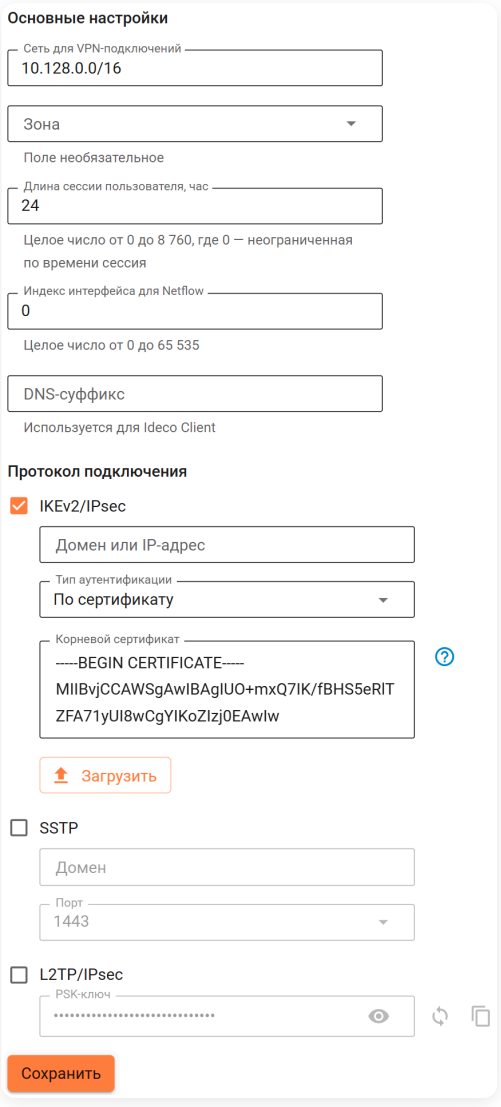
Инструкция актуальна для версии Ubuntu 24.04 LTS.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:

- **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
- **По сертификату** - вход по сертификату пользователя.

- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Ubuntu:

1. Откройте терминал и выполните команду:

```
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-extra-plugins
```

2. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

3. Перейдите в терминале в директорию с загруженным корневым сертификатом (если на доменное имя NGFW выпущен Let`s Encrypt сертификат, сразу перейдите к пункту 6).

4. Установите корневой сертификат NGFW Novum в хранилище доверенных сертификатов Ubuntu:

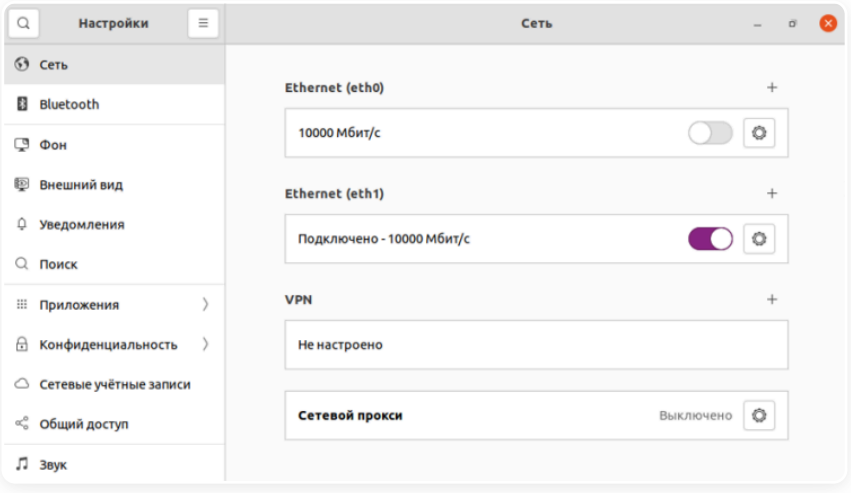
```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

- `ca.crt` - имя скачанного сертификата.

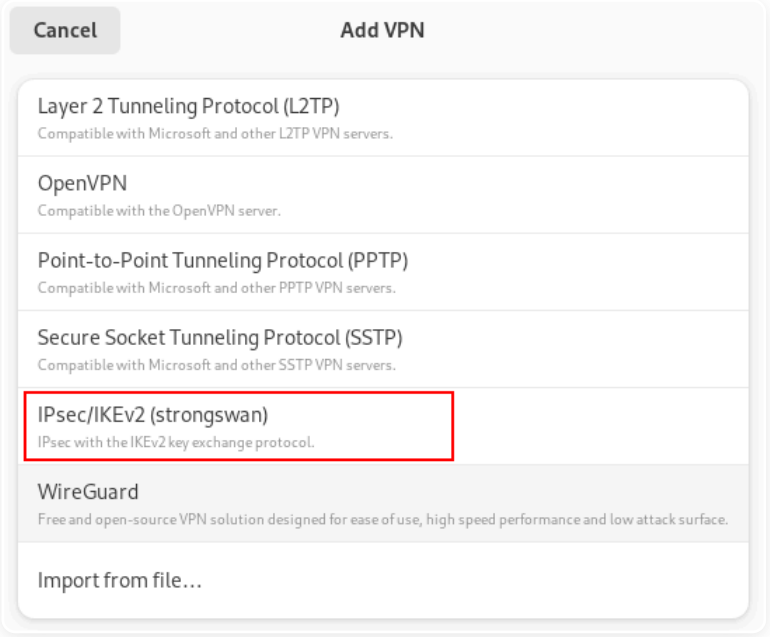
5. Для обновления сертификатов устройства выполните команду:

```
sudo update-ca-certificates
```

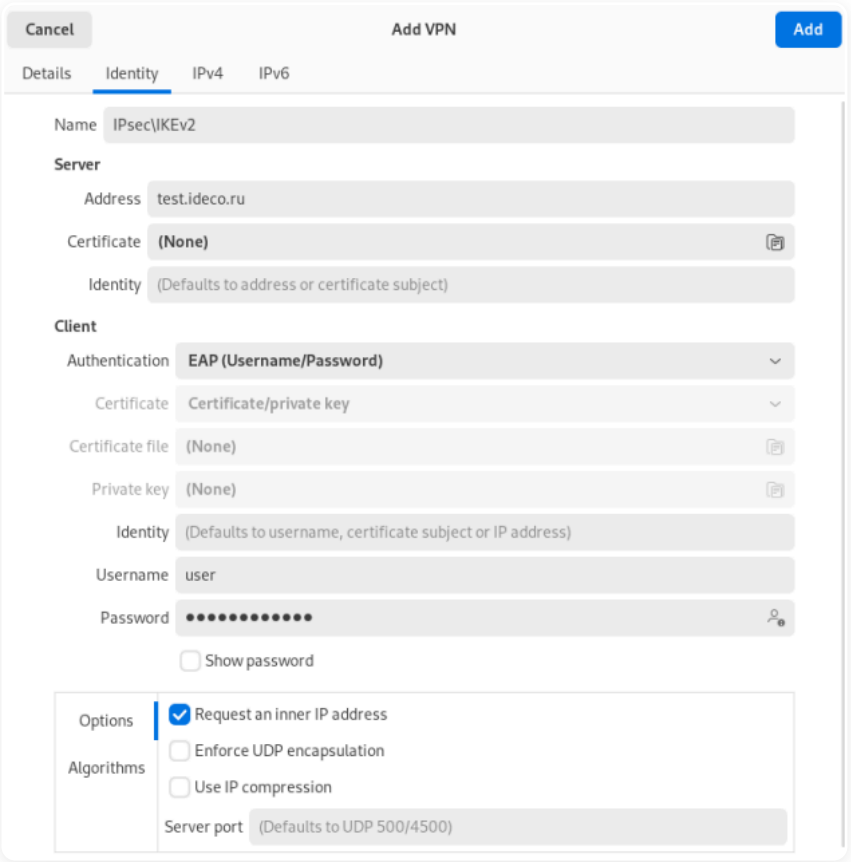
6. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите +:



7. В появившемся окне выберите **IPsec\IKEv2 (strongswan)**:



8. На вкладке **Identity (Идентификация)** заполните поля:



- **Название** - имя подключения.
- **Address** - домен, который указан в настройках **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Authentication** - рекомендуем выбрать EAP.
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.

Установите флаг **Request an inner IP address** и нажмите **Добавить**.

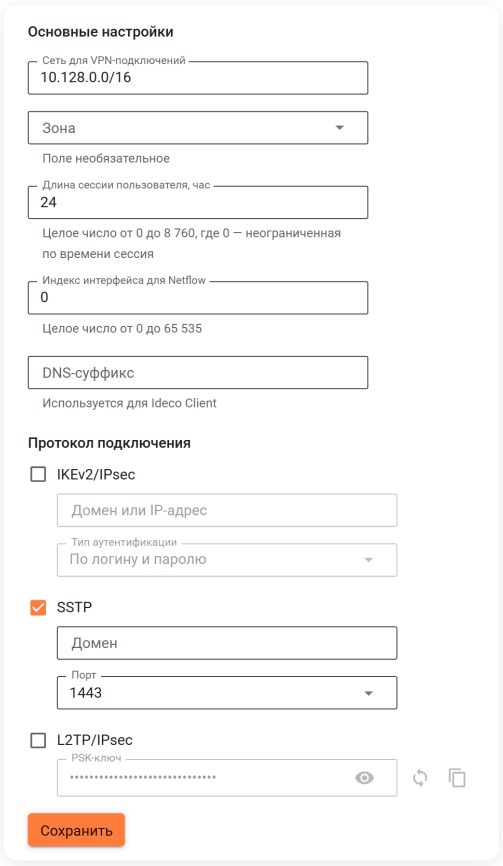
9. Включите созданное VPN-подключение.

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Ubuntu:

1. Откройте терминал и выполните команды:

```
sudo apt-add-repository ppa:eivnaes/network-manager-sstp
sudo apt install -y network-manager-sstp sstp-client
```

2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. Перейдите в терминале в директорию с загруженным корневым сертификатом (если на доменное имя NGFW выпущен Let`s Encrypt сертификат, сразу перейдите к пункту 6).

4. Установите корневой сертификат NGFW в хранилище доверенных сертификатов Ubuntu:

```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

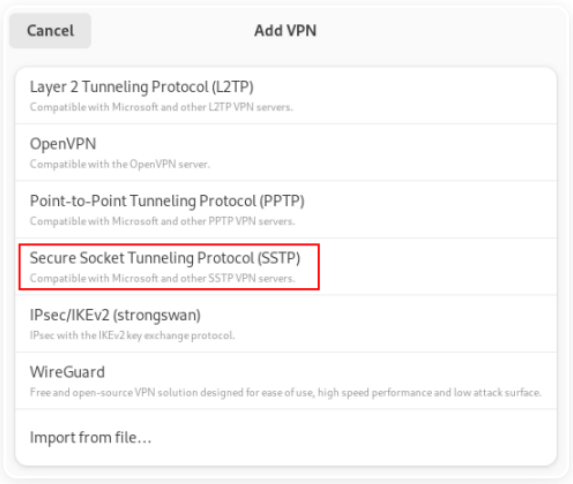
- `ca.crt` - имя скачанного сертификата.

5. Для обновления сертификатов устройства выполните команду:

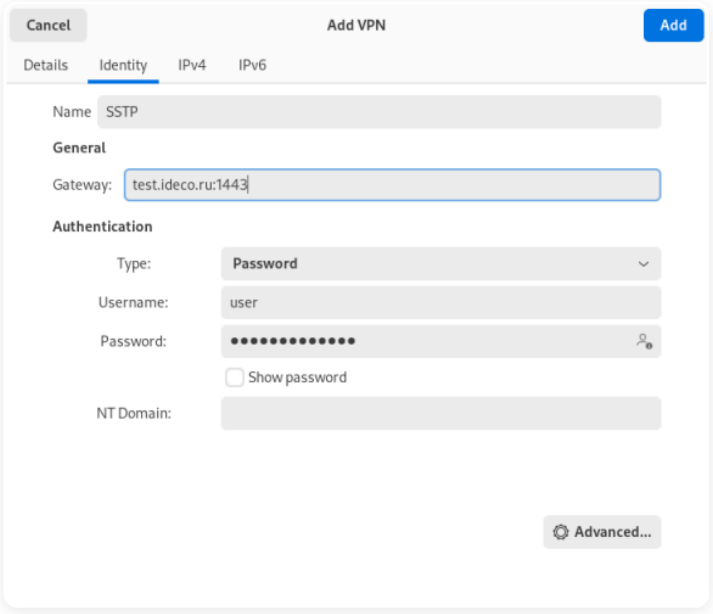
```
sudo update-ca-certificates
```

6. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋.

7. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)** (**Туннельный протокол типа точка-точка (SSTP)**):



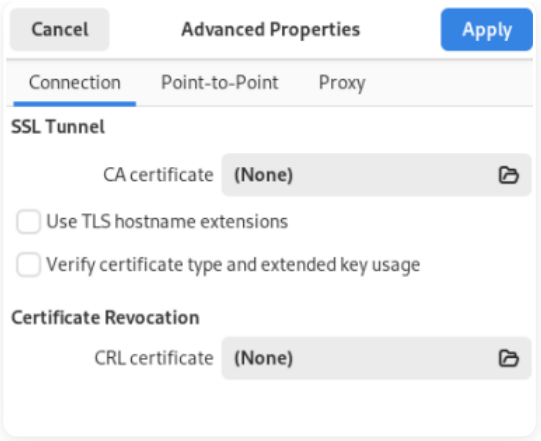
8. На вкладке **Identity (Идентификация)** заполните поля:



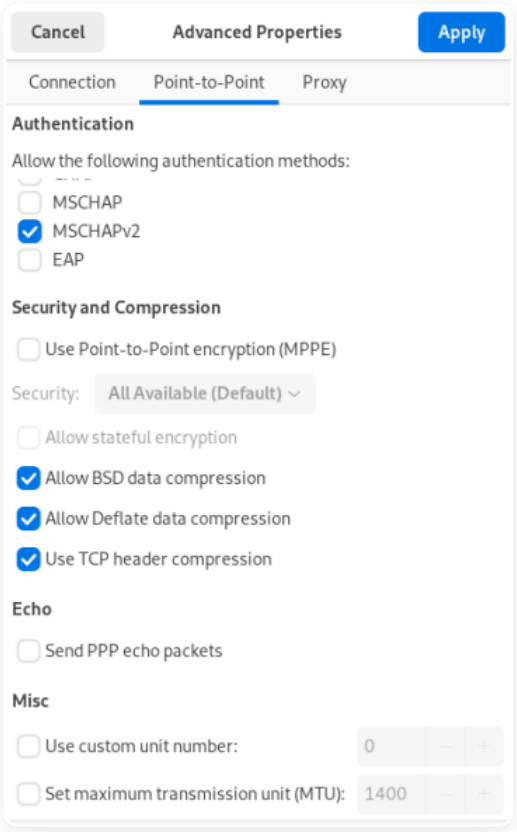
- **Название** - имя подключения.
- **Шлюз** - укажите в формате `домен:<порт, выбранный на NGFW>`.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.
- **NT-домен** - оставьте поле пустым.

9. Нажмите **Advanced**:

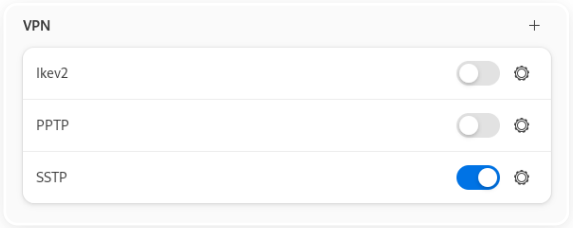
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**.
  - **Verify certificate type and extended key usage**:



- На вкладке **Point-to-Point** установите флаги на пунктах:
  - **Разрешить следующие методы аутентификации** - установите флаг только на ***MSCHAPv2***.
  - **Использовать для данных сжатие BSD**.
  - **Использовать для данных сжатие Deflate**.
  - **Использовать сжатие заголовков TCP**:



10. Нажмите **Добавить** и включите созданное VPN-подключение:



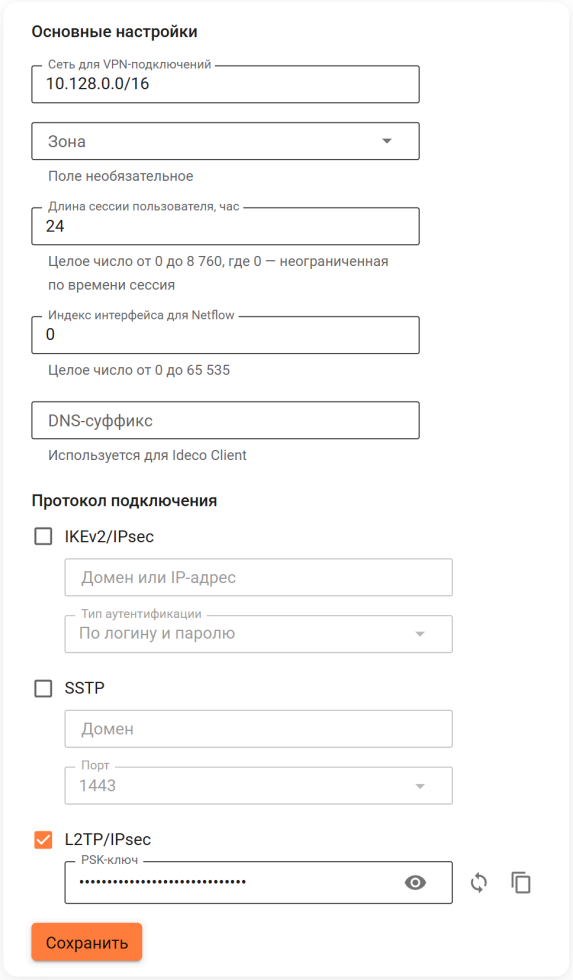
L2TP/IPsec

Важно: L2TP/IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если клиентов более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Ubuntu:

1. Подключите репозиторий, в котором находятся необходимые пакеты для создания L2TP VPN-соединения, а затем обновите информацию о репозиториях. Для этого выполните команды:

```
sudo add-apt-repository ppa:nm-l2tp/network-manager-l2tp
sudo apt update
```

2. Установите дополнение к стандартному NetworkManager с помощью двух пакетов:

```
sudo apt install -y network-manager-l2tp network-manager-l2tp-gnome
```

3. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

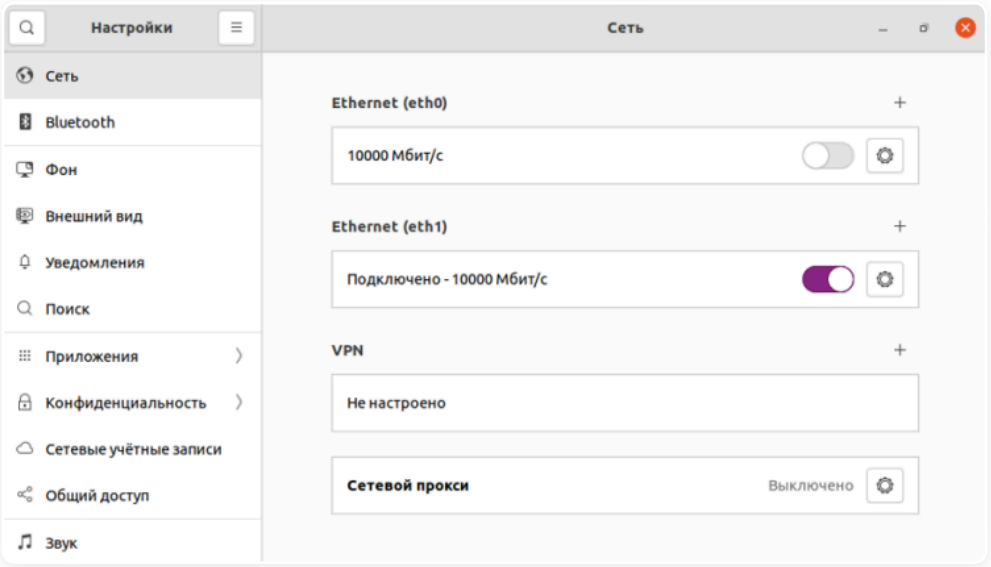
4. Проверьте установленные пакеты:

```
dpkg --get-selections | grep l2tp
```

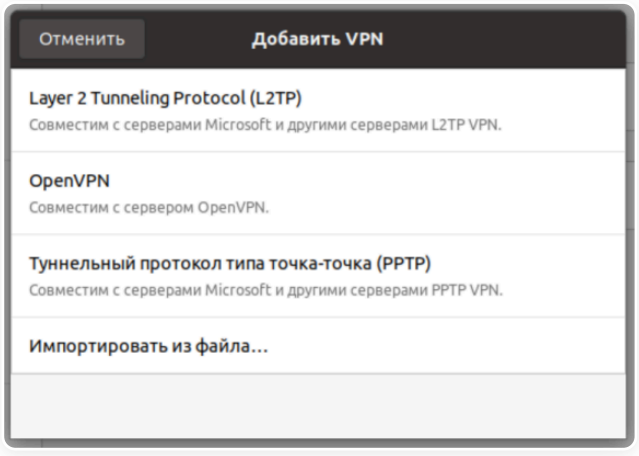
Важно: если в списке пакетов находится `go-l2tp`, удалите пакет и установите `xl2tpd`:

```
sudo apt purge go-l2tp
sudo apt install xl2tpd
```

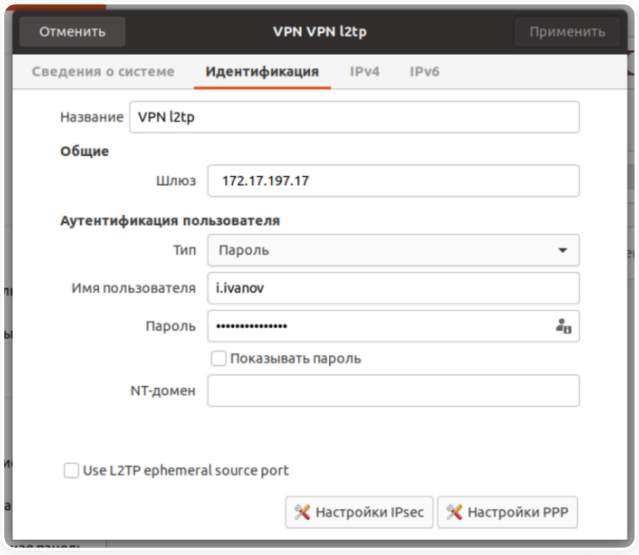
5. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋:



6. В появившемся окне выберите пункт **Layer 2 Tunneling Protocol (L2TP)**:

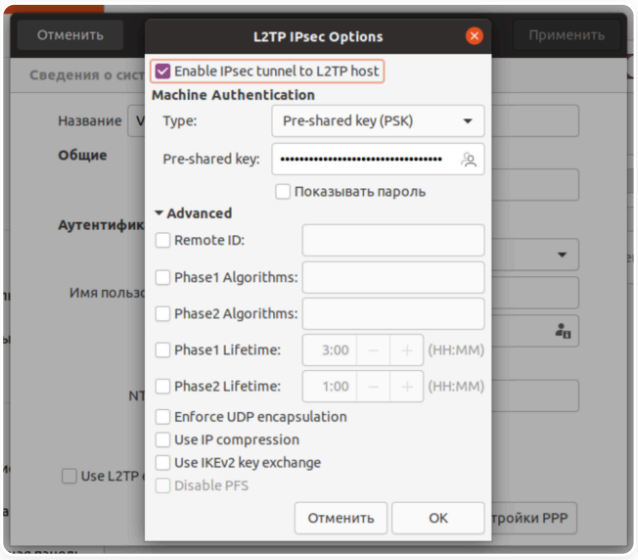


7. На вкладке **Идентификация** заполните поля:



- **Название** - имя подключения.
- **Шлюз** - домен или IP-адрес Ideco NGFW Novum.
- **Тип** - Password (аутентификация по имени пользователя и паролю).
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.
- **NT-домен** - оставьте поле пустым.

8. Перейдите в **Настройки IPsec** и включите настройку **Enable IPsec tunnel to L2TP host**, чтобы активировалась возможность настраивать остальные параметры:

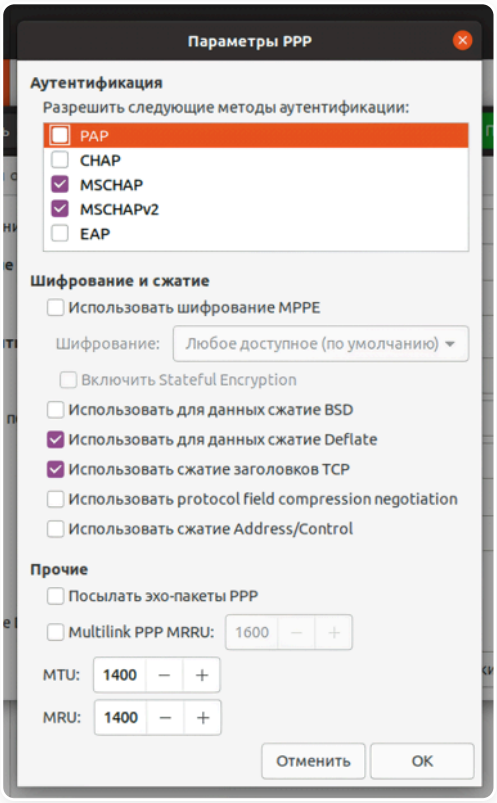


- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу.
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи** → **VPN-подключения** → **Основное** из поля **PSK**.

Раздел **Advanced** необязателен для заполнения.

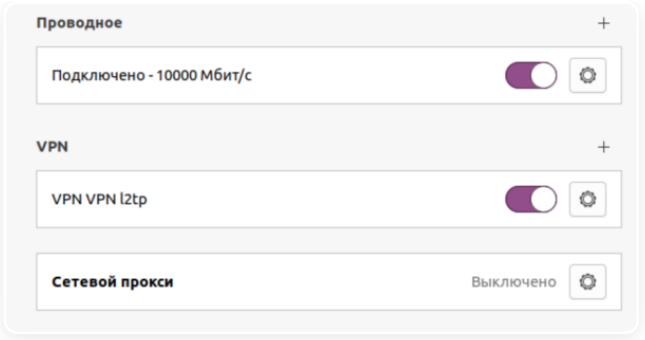
После окончания настройки **L2TP IPsec Options** нажмите **OK**.

9. При необходимости перейдите в **Настройки PPP** и настройте раздел **Аутентификация**, **Шифрование и сжатие** и **Прочие**:



После настройки **Параметры PPP** нажмите **OK** и **Применить**.

10. Включите созданное VPN-подключение:



Полезные ссылки

- VPN-подключения

Инструкция по созданию подключения в Fedora

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

Инструкция актуальна для Fedora 41. Рекомендуемый протокол подключения - IKEv2/IPsec.

Перед настройкой

1. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте правило разрешающее VPN-подключение.

2. Загрузите на устройство корневой сертификат Ideco NGFW Novum. Файл сертификата должен находиться в общедоступном каталоге.

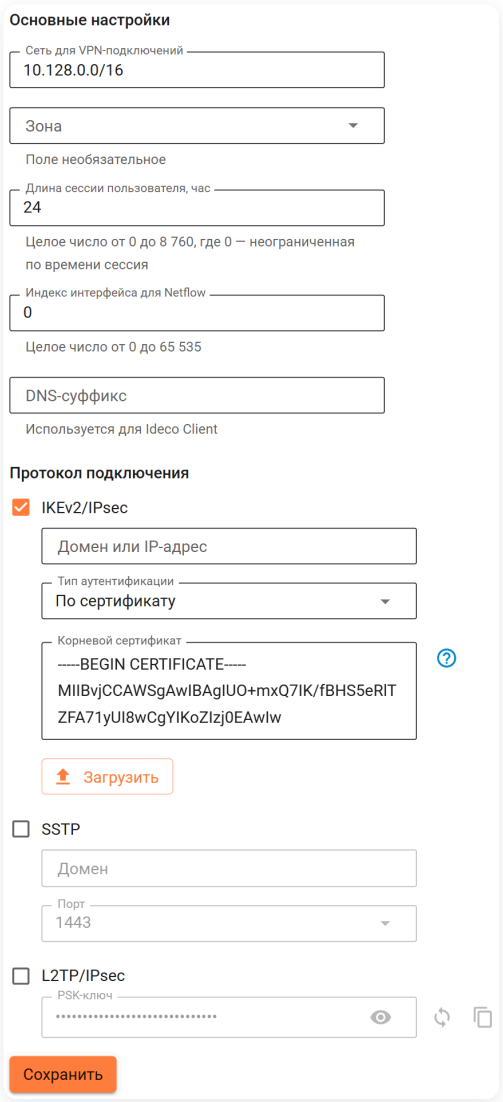
Загружать сертификат **ISRG_ROOT_X1** не требуется, так как сертификат уже есть в Fedora 41 и находится в каталоге `/etc/ssl/certs`.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.

- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Создание подключения в Fedora:

1. Для поддержки подключения по IPsec для NetworkManager установите пакет **NetworkManager-strongswan**:

```
sudo dnf -y install NetworkManager-strongswan
```

2. Установите пакет для настройки IPsec-подключения через графический интерфейс:

- Окружение рабочего стола GNOME:

```
sudo dnf -y install NetworkManager-strongswan-gnome
```

- Окружение рабочего стола KDE:

```
sudo dnf -y install plasma-nm-strongswan
```

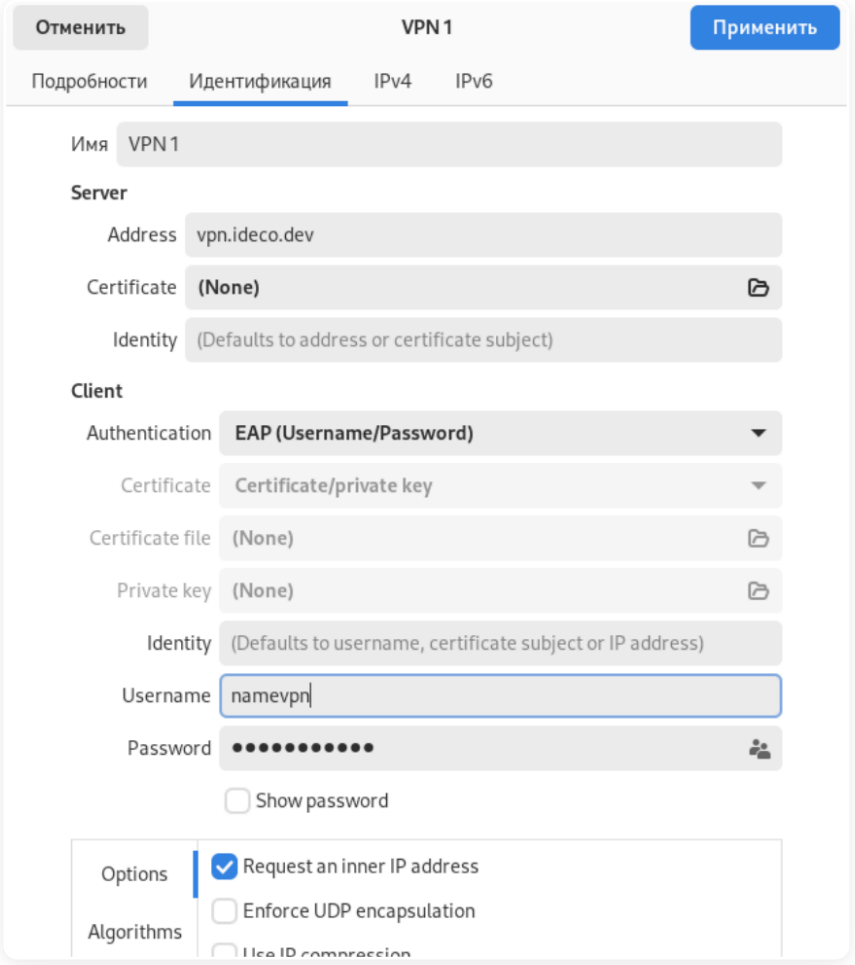
Создание подключения в Fedora:

1. Загрузите корневой сертификат NGFW Novum, включая всю цепочку доверия, в каталог `/etc/strongswan/ipsec.d/cacerts`.

2. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите  .

3. В появившемся окне выберите **IPsec\IKEv2 (strongswan)**.

4. В **Идентификация** заполните поля:



- **Имя** - название VPN-подключения.
- **Address** - доменное имя шлюза для VPN-подключения.
- **Authentication** - EAP (Username/Password).
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

5. Установите флаг **Request an inner IP address**.

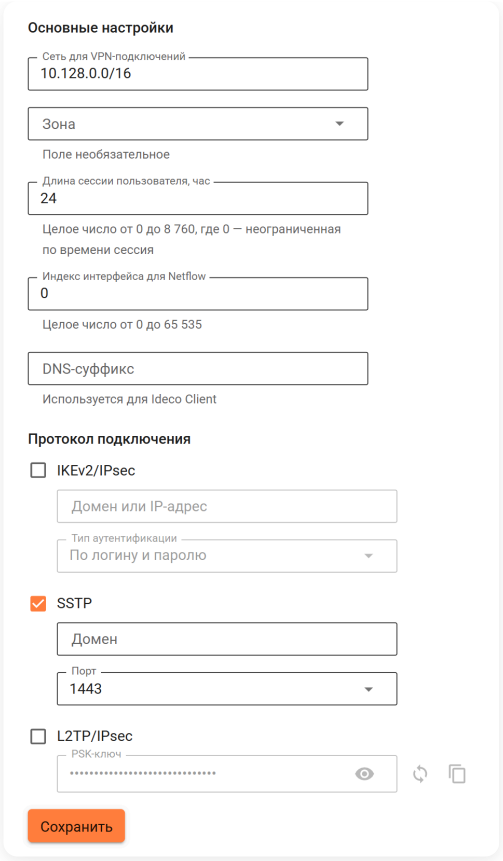
6. Нажмите **Применить** и включите созданное VPN-подключение.

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Создание подключения в Fedora:

1. Откройте терминал и установите необходимые пакеты, выполнив команду:

- Окружение рабочего стола GNOME:

```
sudo dnf install NetworkManager-sstp.x86_64 NetworkManager-sstp-gnome.x86_64 sstp-client.x86_64
```

- Окружение рабочего стола KDE:

```
sudo dnf install NetworkManager-sstp.x86_64 plasma-nm-sstp.x86_64 sstp-client.x86_64
```

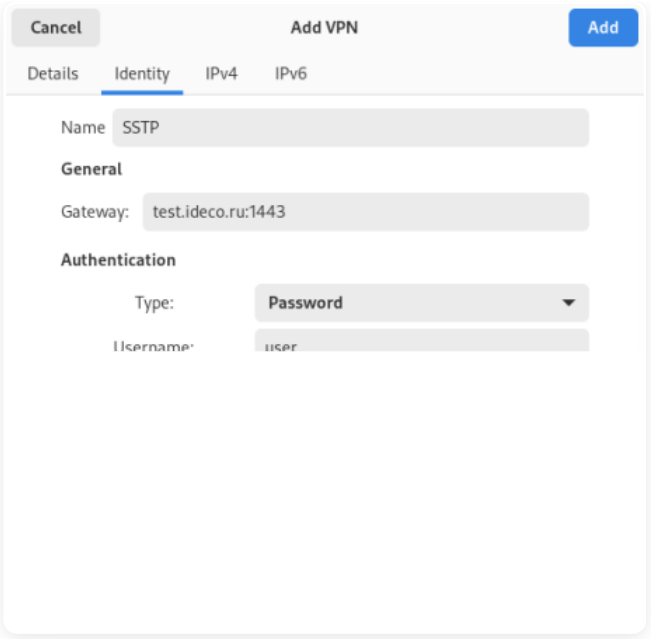
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите +.

4. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)**.

5. В разделе **Идентификация** заполните поля:

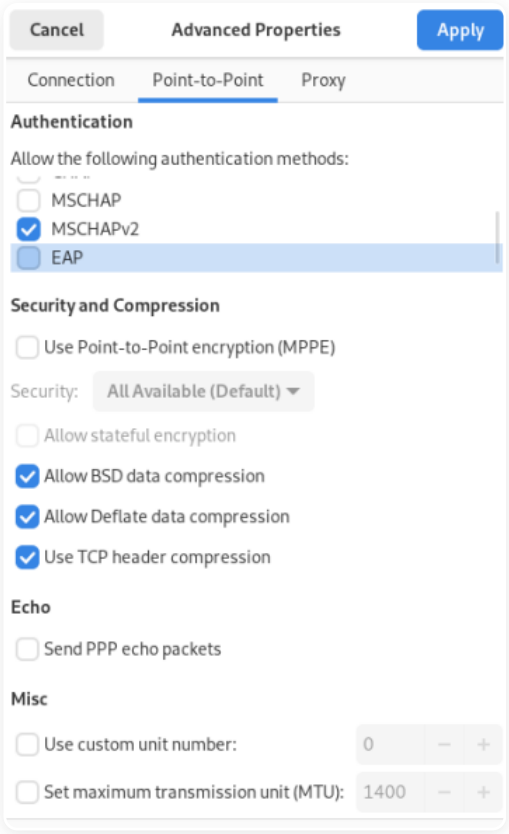


- **Name** - название VPN-подключения.
- **Gateway** - укажите в формате `домен:<порт, выбранный на NGFW>`.
- **Username** - имя пользователя на Ideco NGFW Novum.
- **Password** - пароль пользователя на Ideco NGFW Novum.

6. Нажмите **Advanced**:

- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**.
  - **Verify certificate type and extended key usage**:

- На вкладке **Point-to-Point** рекомендуем установить флаги на пунктах:



- **Allow the following authentication methods** - установите флаг на ***MSCHAPv2***.
- **Allow BSD data compression**.

- **Allow Deflate data compression**.
- **Allow TCP header compression**.

7. Нажмите **Добавить** и включите созданное VPN-подключение.

> Если подключение по SSTP не устанавливается:
>
> 1. Выполните команду `sestatus`, чтобы узнать текущий режим SELinux. Если режим **Enforcing**, SELinux может блокировать работу SSTP.
>
> 2. Переведите SELinux в режим **Permissive**. Для этого выполните команду `sudo setenforce 0`. Это до перезагрузки отключит принудительный контроль доступа SELinux.
>
> 3. Попробуйте подключиться к VPN через SSTP. Если проблема была в SELinux, подключение должно заработать.
>
> 4. Если заработало, то измените файл `sudo nano /etc/selinux/config` и установите `SELINUX=permissive` или `SELINUX=disabled`. После этого перезагрузите систему.
>
> Рекомендуем режим **Permissive** (setenforce 0) использовать только для диагностики и не оставлять SELinux в этом режиме на постоянной основе, так как это снижает уровень безопасности системы.

L2TP/IPsec

L2TP/IPsec клиенты, находящиеся за одним NAT, могут испытывать проблемы подключения, если клиентов более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

Создание подключения в Fedora:

1. Установите необходимые пакеты для создания L2TP VPN-соединения, выполнив команду:

- Окружение рабочего стола GNOME:

```
sudo dnf install NetworkManager-l2tp.x86_64 NetworkManager-l2tp-gnome.x86_64 xl2tpd.x86_64
```

- Окружение рабочего стола KDE:

```
sudo dnf install NetworkManager-l2tp.x86_64 plasma-nm-l2tp.x86_64 xl2tpd.x86_64
```

2. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

4. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите +.

5. В окне создания подключений по VPN выберите пункт **Layer 2 Tunneling Protocol (L2TP)**.

6. На вкладке **Идентификация** заполните поля:

- **Name** - название VPN-подключения.
- **Gateway** - доменное имя или IP-адрес NGFW.
- **Type** - Password.
- **User Name** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

7. Перейдите в **Настройки IPsec** и включите настройку **Enable IPsec tunnel to L2TP host**, чтобы активировалась возможность настраивать остальные параметры:

- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу.
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи** → **VPN-подключения** → **Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения.

После окончания настройки **L2TP IPsec Options** нажмите **OK**.

8. При необходимости перейдите в **Настройки PPP** и настройте раздел **Аутентификация**, **Шифрование и сжатие** и **Прочие**:

После настройки **Параметров PPP** нажмите **OK** и **Применить**.

9. Включите созданное VPN-подключение.

Полезные ссылки

- **VPN-подключения**
- **Подключение по IKEv2/IPsec**

Инструкция по созданию подключения в Astra Linux

Функциональность доступна в **Классическом** и **Системном контекстах**.

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

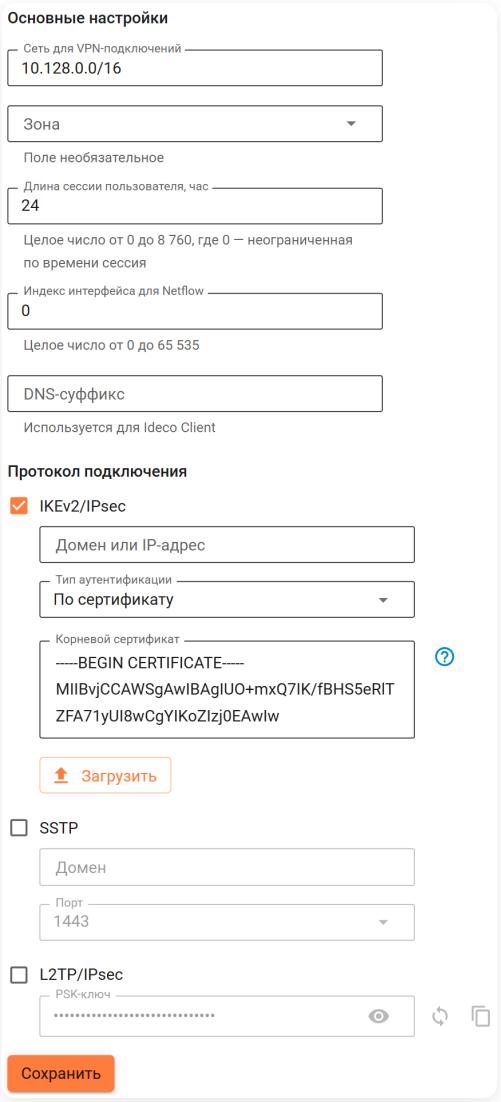
Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.
- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.

- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Astra Linux:

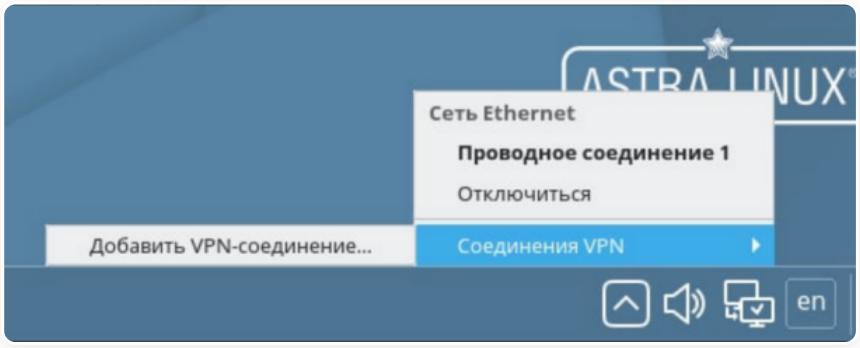
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt install libcharon-extra-plugins
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-extra-plugins
```

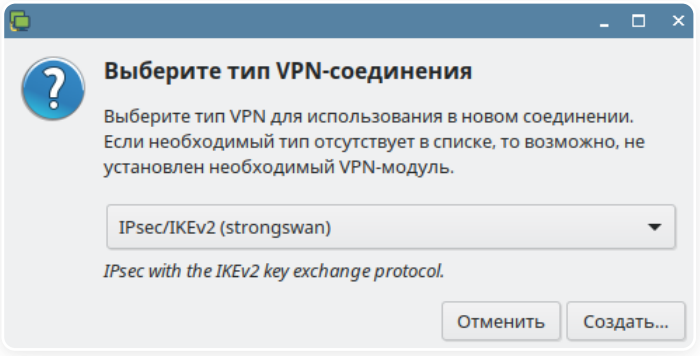
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

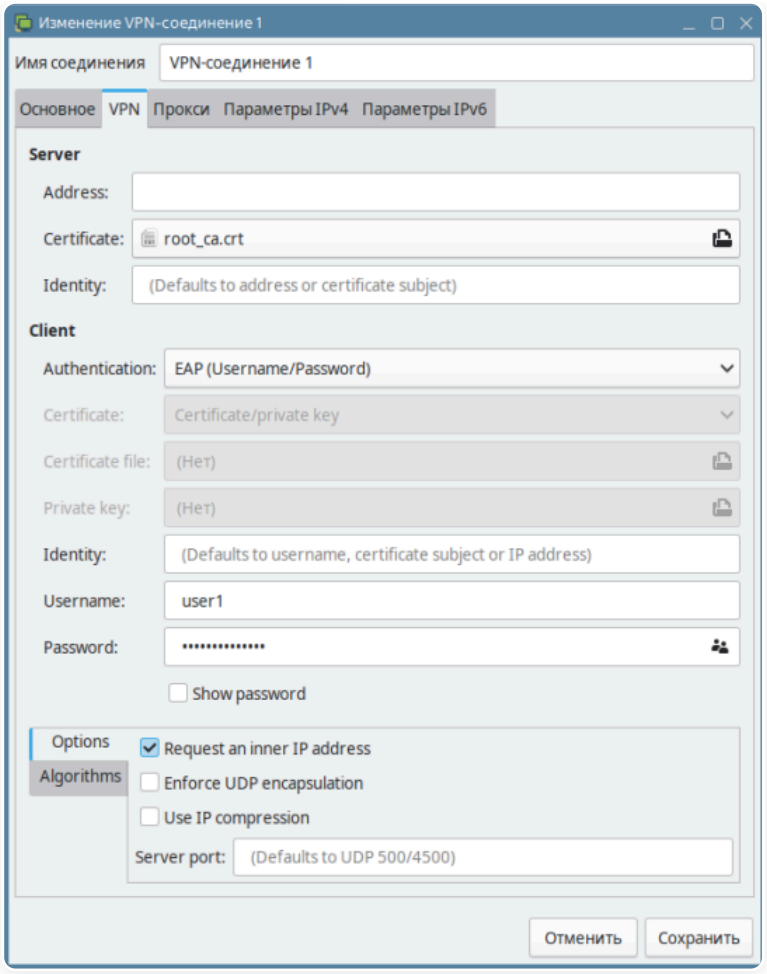
3. В настройках сети выберите **Соединения VPN** → **Добавить VPN-соединение**:



4. Выберите тип соединения **IPsec/IKEv2 (strongswan)** и нажмите **Создать**:



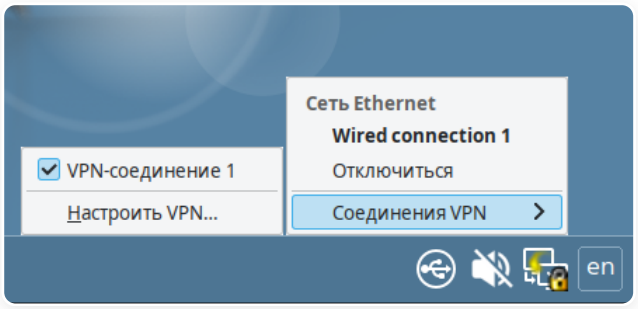
5. На вкладке **VPN** заполните поля:



- **Имя соединения** - имя подключения.
- **Address** - введите домен или IP-адрес, который указан в настройках **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Certificate** - выберите корневой сертификат NGFW или оставьте поле пустым, если используется сертификат Let's Encrypt.
- **Authentication** - рекомендуем выбрать EAP (Username/Password).
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.

Установите флаг **Request an inner IP address** и нажмите **Добавить**.

6. В настройках сети выберите **Соединения VPN** и установите флаг в строке с созданным соединением:



Проверить способы шифрования можно в конфигурации NGFW. Для этого откройте терминал NGFW и введите команду:

```
cat /run/ideco-ipsec-backend/strongswan/swanctl/conf.d/rw_ikev2.conf
```

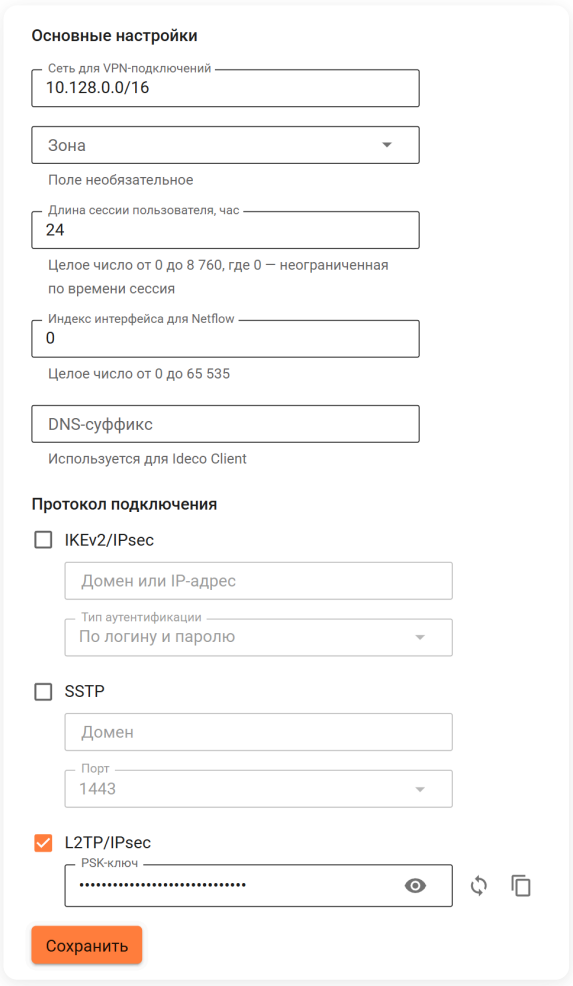
- для Phase1 Algorithm ищите значения **proposals=**;
- для Phase2 Algorithms ищите значения **esp_proposals=**.

L2TP/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи → VPN-подключения → Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Astra Linux:

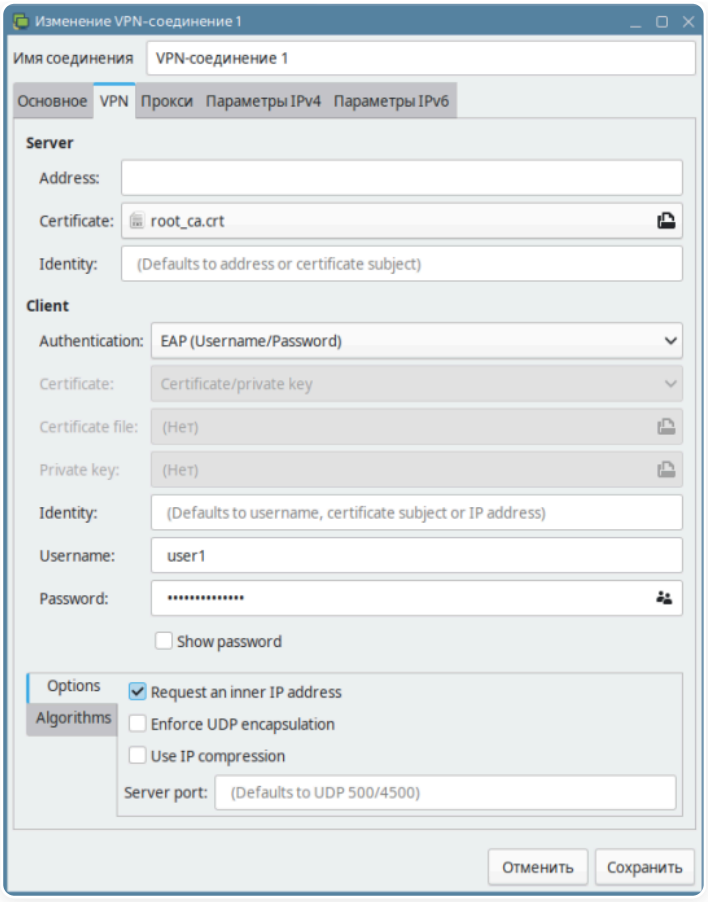
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt update
sudo apt install network-manager-l2tp-gnome
```

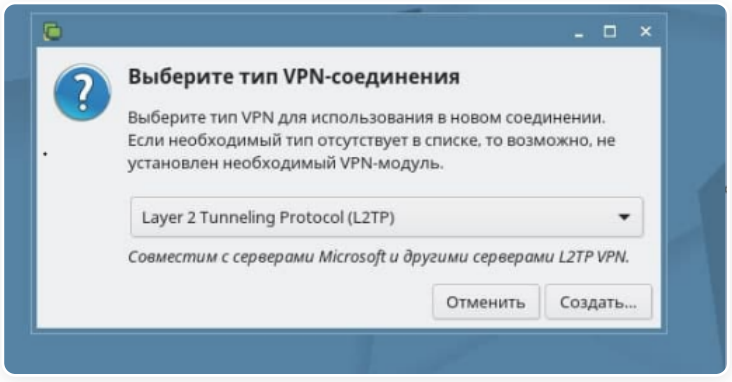
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

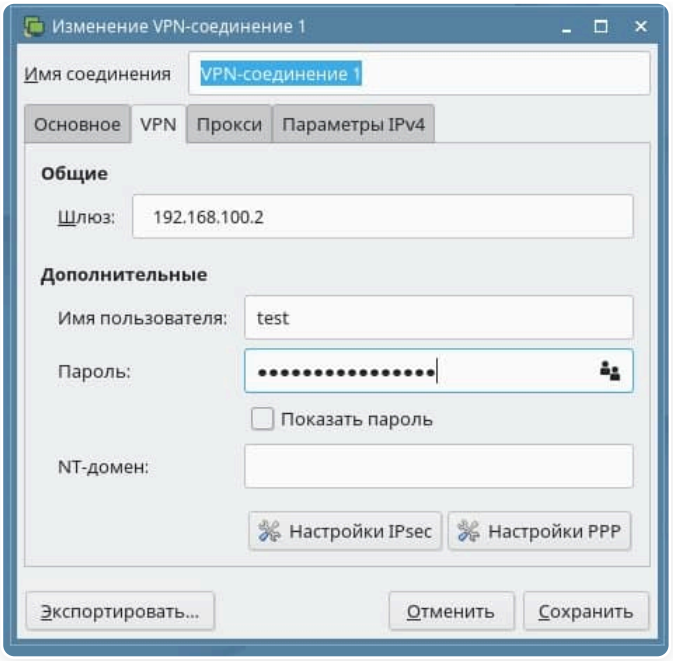
3. В настройках сети выберите **Соединения VPN → Добавить VPN-соединение**:



4. Выберите тип соединения **Layer 2 Tunneling Protocol (L2TP)** и нажмите **Создать**:



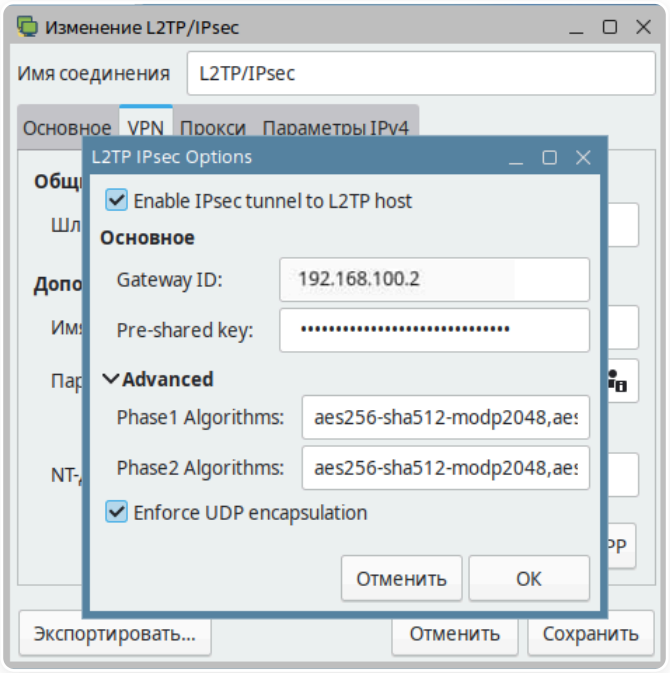
5. На вкладке **VPN** заполните поля:



- **Шлюз** - IP-адрес или домен внешнего интерфейса Ideco NGFW Novum.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя. В правой части поля выберите вариант хранения для пароля от VPN-соединения.

6. Нажмите **Настройки IPsec**.

7. Заполните поля:

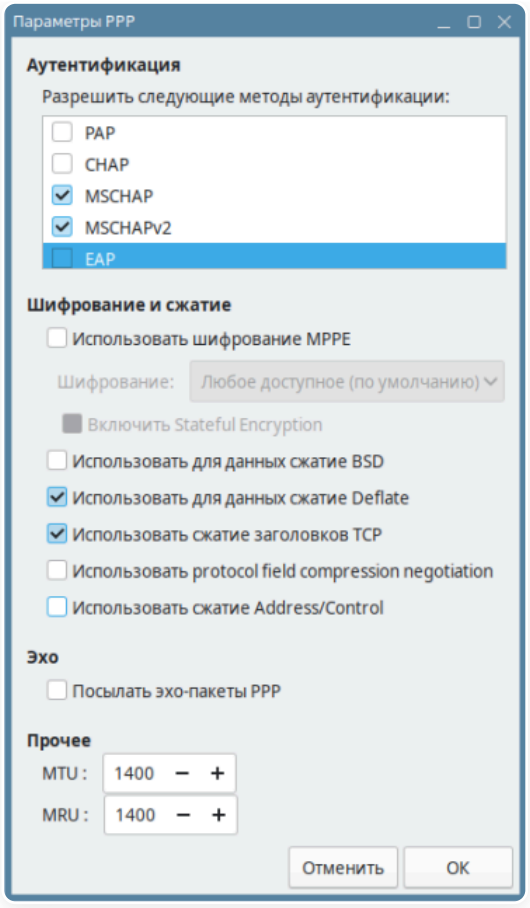


- **Gateway ID** - IP-адрес интерфейса, к которому осуществляется подключение.
- **Pre-shared key** - PSK-ключ из настроек Ideco NGFW Novum (**Пользователи** → **VPN-подключения** → **Основное**).
- **Phase1 Algorithm** - `aes256-sha512-modp2048,aes256-sha512-modp1024,aes256-sha1-ecp256,aes256-sha1-modp2048,aes256-sha1-modp1024!`. *
- **Phase2 Algorithms** - `aes256-sha512-modp2048,aes256-sha256-modp2048,aes256-sha1-modp2048,aes128-sha1-modp2048,aes256-sha512-modp1024,aes256-sha256-modp1024,aes256-sha1-modp1024,aes128-sha1-modp1024,aes256-sha512,aes256-sha256,aes256-sha1,aes128-sha1!`.*

* Обязательно поставьте восклицательный знак в конце строки.

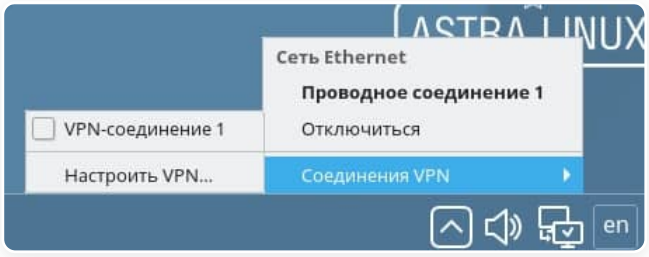
Так как Astra Linux по умолчанию запрашивает не самые защищенные алгоритмы, рекомендуем заполнить поля **Phase1 Algorithm** и **Phase2 Algorithms** самостоятельно.

8. При необходимости перейдите в **Настройки PPP** и настройте разделы **Аутентификация**, **Шифрование и сжатие**, **Прочее**:



9. Нажмите **ОК**, затем **Сохранить**.

Далее в настройках сети **Соединения VPN** появится VPN-подключение. Для активации включите опцию **VPN-соединение**:



Полезные ссылки

- **VPN-подключения**

Инструкция по созданию подключения в Windows

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Не рекомендуем использовать для VPN-подключений кириллические логины.

Создание VPN-подключения в Windows

Для корректной передачи маршрутов клиенту убедитесь, что опция **Использовать основной шлюз удаленной сети** выключена. Для отключения опции перейдите в **Панель управления** → **Сеть и интернет** → **Центр управления сетями и общим доступом** → **Изменение параметров адаптера** → **Свойства**. После этого перейдите в **Сеть** → **IP версии 4 (TCP/IPv4)** → **Дополнительно**.

IKEv2/IPsec

Выберите тип аутентификации пользователей и выполните действия:

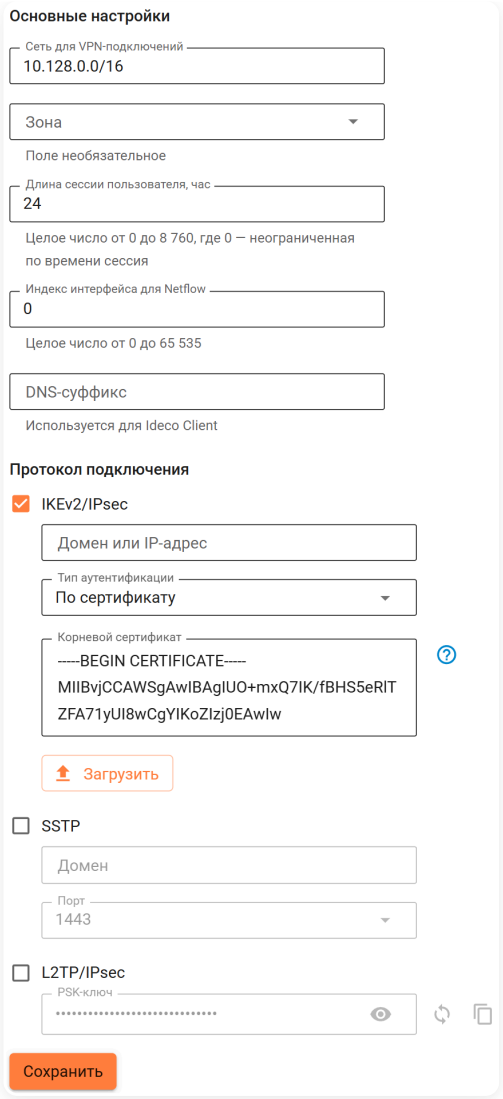
По логину и паролю **По сертификату**

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Домен и IP-адрес** - укажите доменное имя или IP-адрес, по которому будут подключаться пользователи.
- **Тип аутентификации** - выберите тип **По логину и паролю**.

3. Нажмите **Сохранить**.

4. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

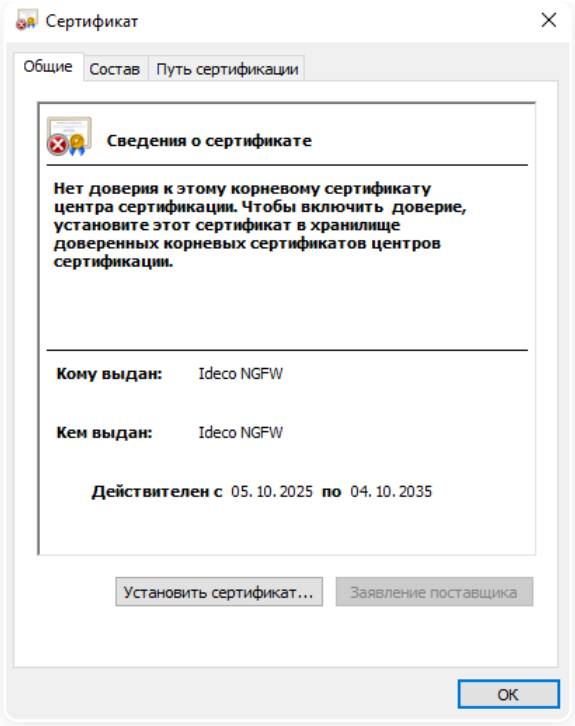
- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Windows:

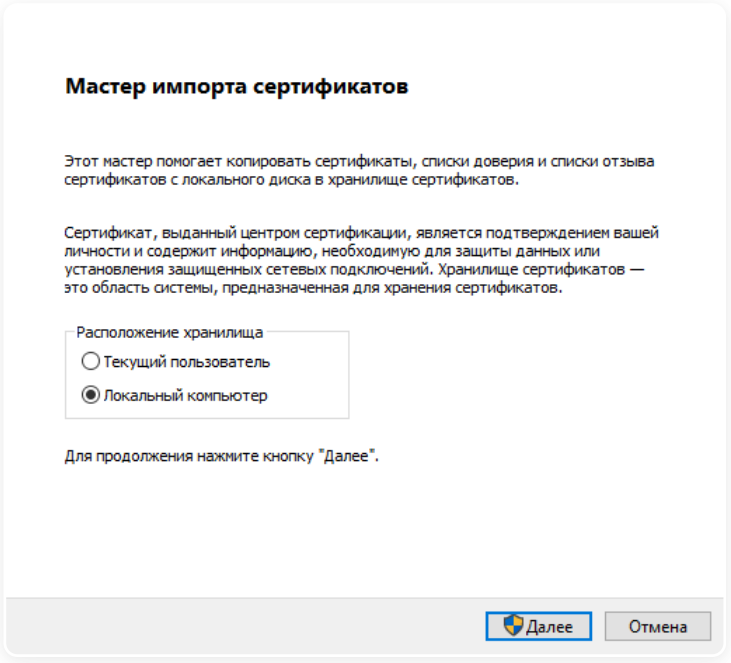
1. Импортируйте сертификат Ideco NGFW Novum:

Пример для Windows

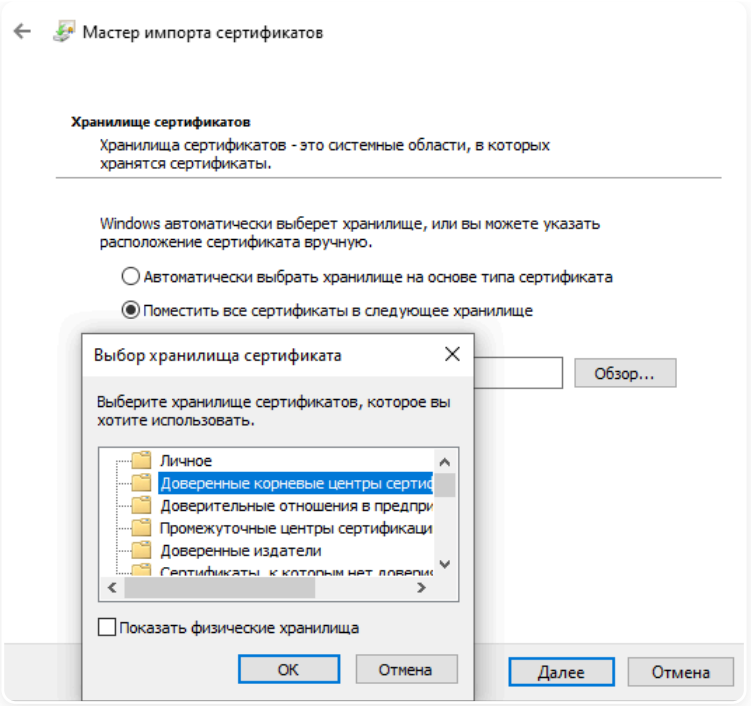
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



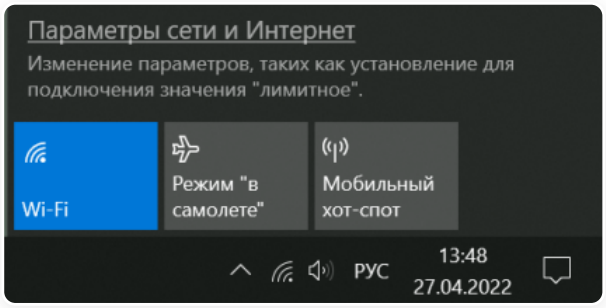
2. Выберите расположение хранилища **Локальный компьютер**:



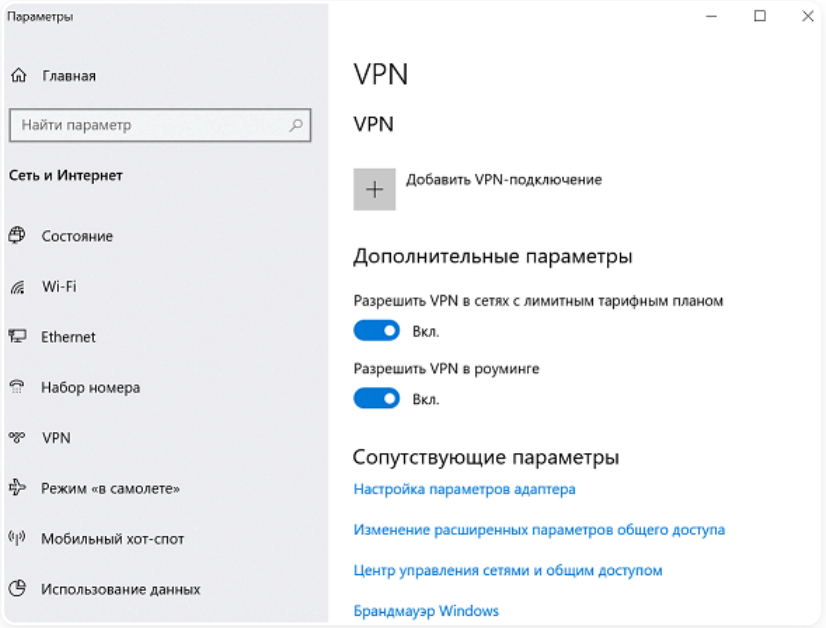
3. Установите сертификат в **Доверенные корневые центры сертификации**:



2. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



3. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



4. Заполните соответствующие поля и нажмите **Сохранить**:



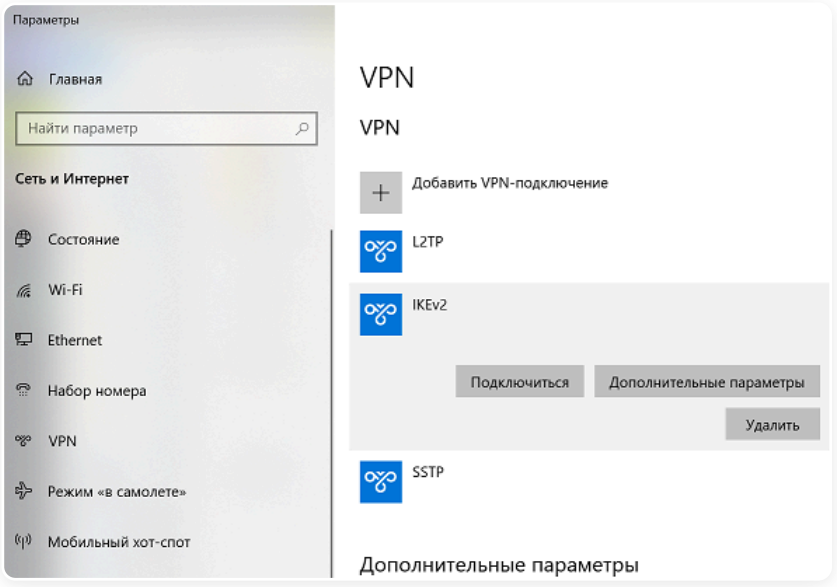
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера.
- **Тип VPN** - протокол IKEv2.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

5. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

6. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).
- **Протокол расширенной проверки подлинности (EAP)** - Microsoft защищенный пароль (EAP MSCHAPV2).

7. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



8. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры** → **Изменить**.

L2TP/IPsec

Подготовка:

Для аутентификации пользователей по сертификату необходимо экспортировать:

- **Корневой сертификат** Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя.
- **Полную цепочку промежуточных сертификатов**, если сертификат пользователя выпущен промежуточным УЦ.
- **Пользовательский сертификат**.

Требования к сертификатам

Алгоритмы хеширования:

- Для подписи сертификатов рекомендуется использовать алгоритм SHA-256 или более стойкий (например, SHA-384, SHA-512).
- Алгоритм SHA-1 не поддерживается.

Ключевые расширения:

- **Для промежуточного сертификата:**
- `basicConstraints=critical,CA:TRUE` - используется для указания, что сертификат может подписывать другие сертификаты.
- **Для пользовательского сертификата:**
- `subjectAltName=DNS:...` - используется для указания альтернативных имен (например, DNS или IP-адреса).

Примеры генерации сертификатов УЦ:

Создание корневого и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **CN** - укажите логин учетной записи пользователя для авторизации.

3. Подписание пользовательского сертификата корневым:

```
openssl x509 -req -in client.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

4. Создание PFX-архива для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile rootCA.crt -passout pass:1234
```

Создание корневого, промежуточного и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание промежуточного сертификата:

```
openssl genrsa -out interCA.key 4096
openssl req -new -key interCA.key -out interCA.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"

openssl x509 -req -in interCA.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out interCA.crt -days 1825 -sha256 \
-extfile <(printf "basicConstraints=critical,CA:TRUE")
```

3. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **Common Name (CN)** - укажите логин учетной записи пользователя для авторизации.

4. Подписание пользовательского сертификата промежуточным:

```
openssl x509 -req -in client.csr -CA interCA.crt -CAkey interCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

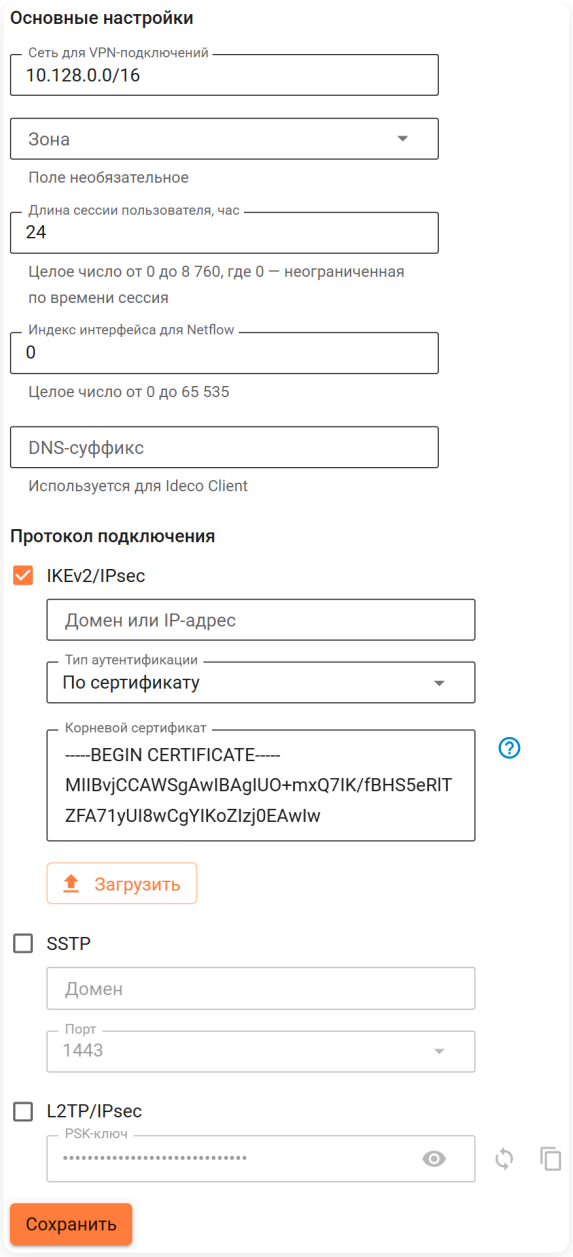
5. Создание PFX-архива с полной цепочкой доверия для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile <(cat interCA.crt rootCA.crt) -passout pass:1234
```

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Домен и IP-адрес** - укажите доменное имя или IP-адрес, по которому будут подключаться пользователи.
- **Тип аутентификации** - выберите тип **По сертификату**.
- **Корневой сертификат** - загрузите корневой сертификат УЦ или объединенный в один файл корневой и все промежуточные сертификаты.

3. Нажмите **Сохранить**.

4. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

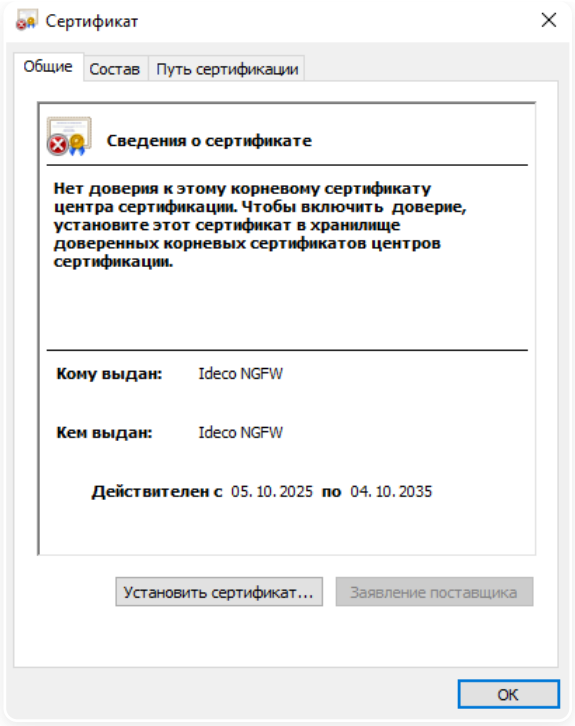
- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в Windows:

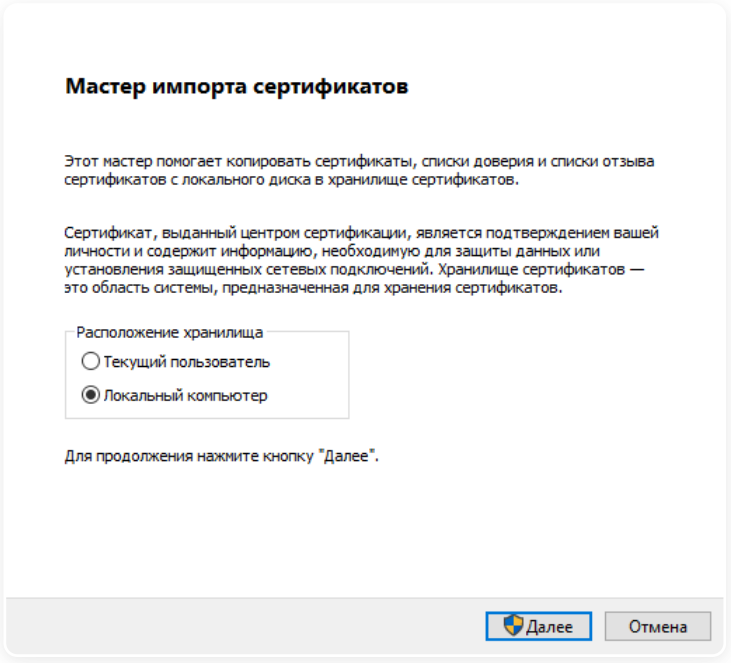
1. Импортируйте корневой сертификат Ideco NGFW Novum:

Пример для Windows

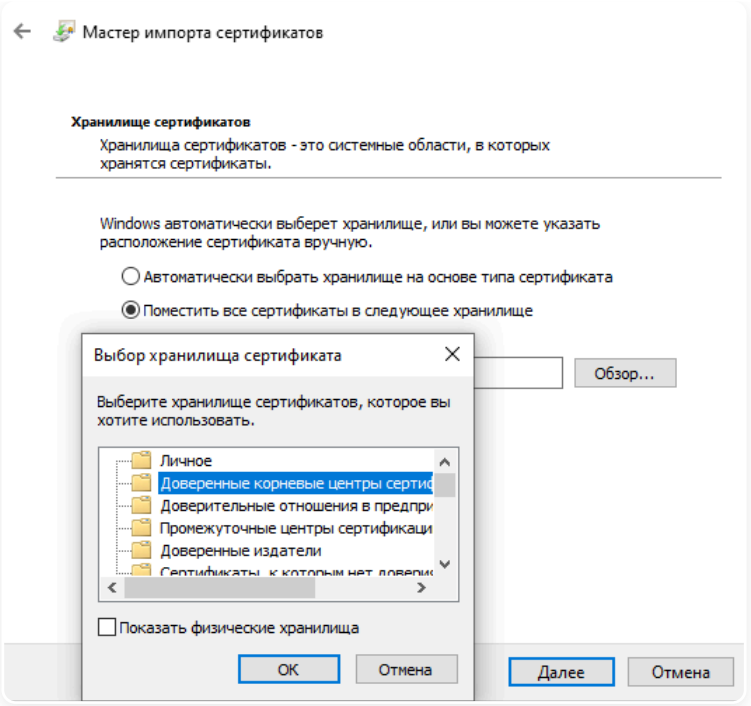
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



2. Выберите расположение хранилища **Локальный компьютер**:



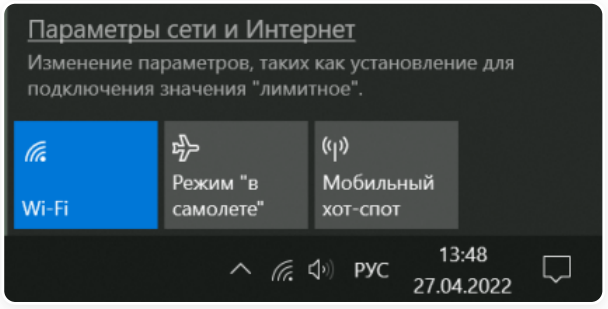
3. Установите сертификат в **Доверенные корневые центры сертификации**:



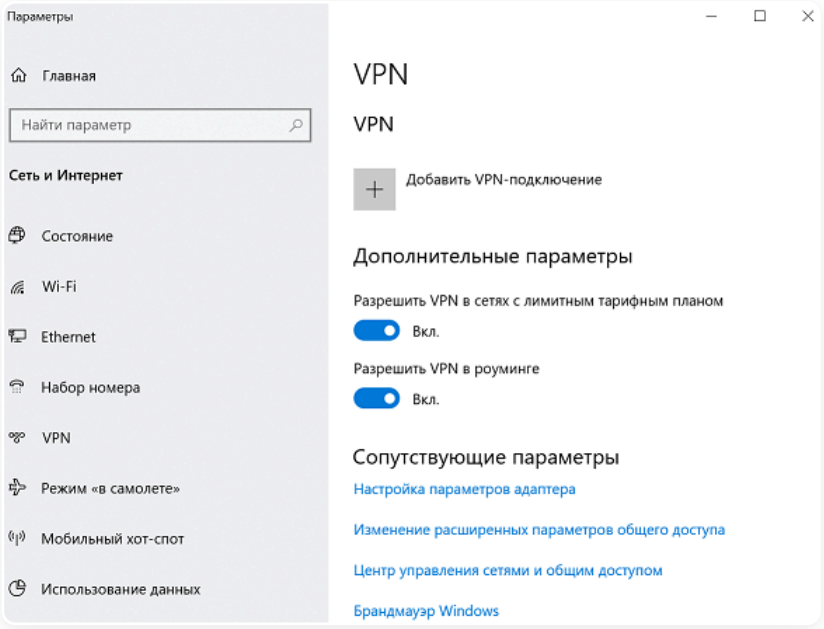
2. Импортируйте пользовательский сертификат:

- Расположение хранилище - **Текущий пользователь**.
- Выбор хранилища - **Личное**.

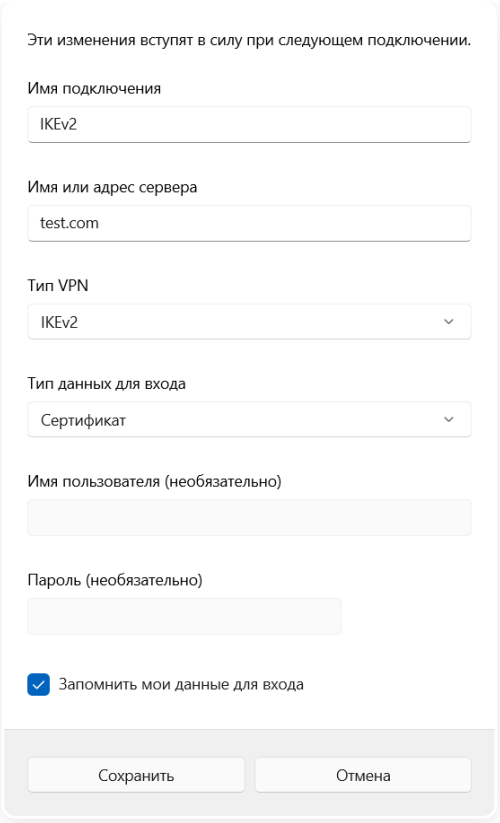
3. Кликните на иконку сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



4. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



5. Заполните соответствующие поля и нажмите **Сохранить**:



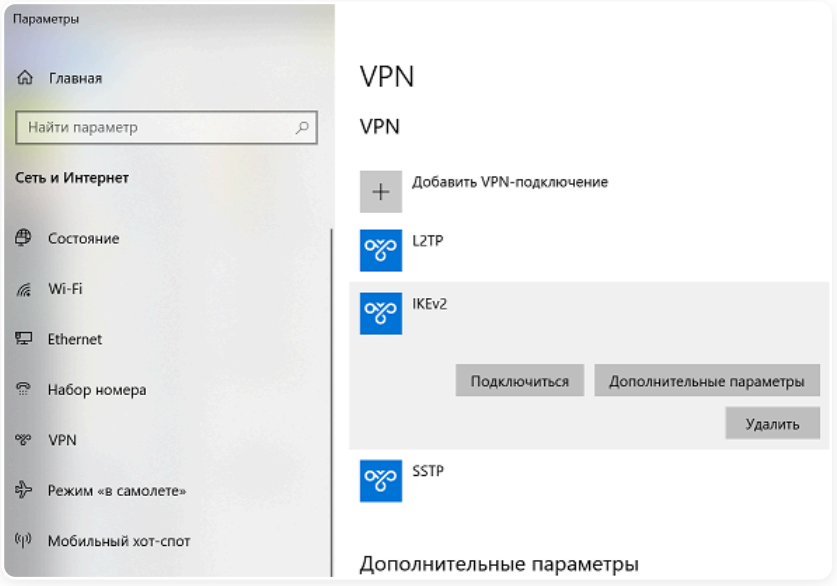
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера.
- **Тип VPN** - протокол IKEv2.
- **Тип данных для входа** - сертификат.

6. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

7. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).
- **Протокол расширенной проверки подлинности (EAP)** - Microsoft: Смарт-карта или другой сертификат (EAP-TLS).

8. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



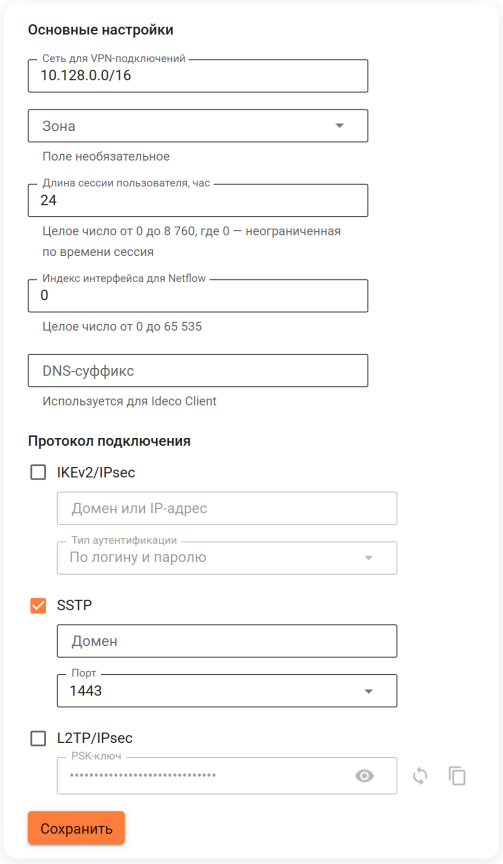
9. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры → Изменить**.

Вкладка 4

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи → VPN-подключения → Основное**.

2. Включите опцию **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы → Сертификаты → Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

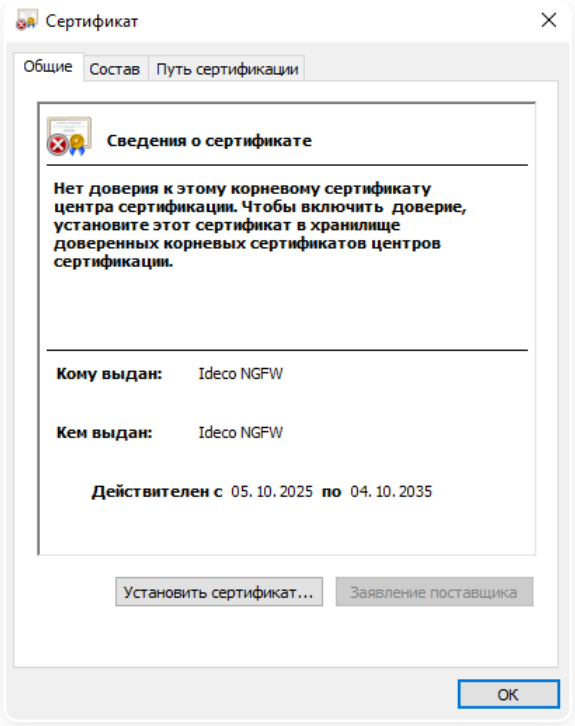
Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы → Сертификаты → Загруженные сертификаты**.

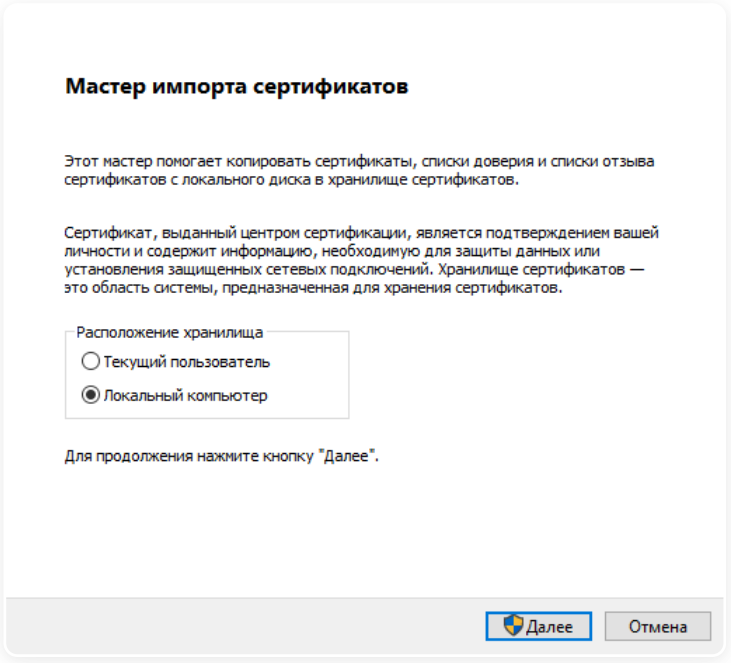
4. Импортируйте сертификат Ideco NGFW Novum:

Пример для Windows

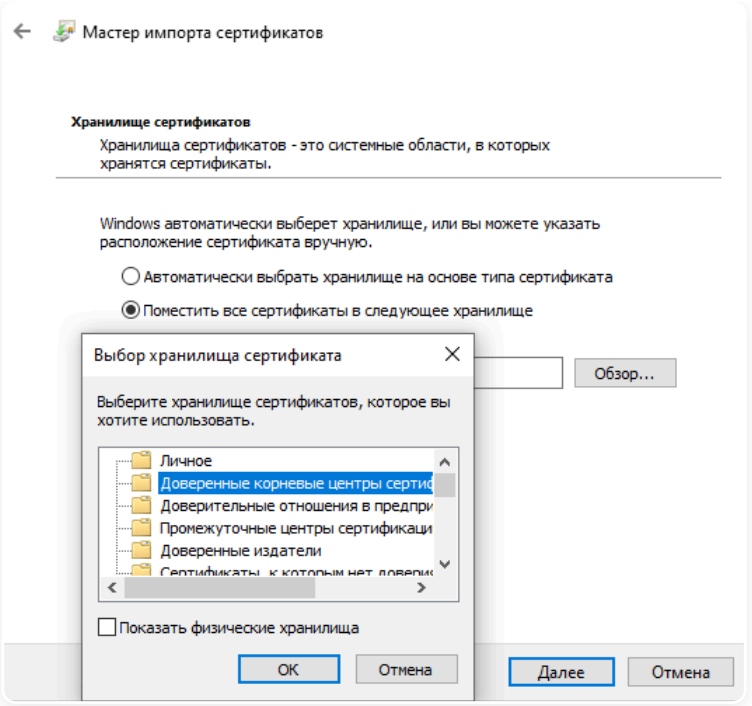
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



2. Выберите расположение хранилища **Локальный компьютер**:

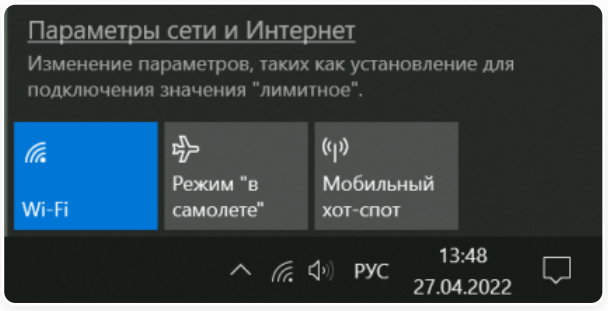


3. Установите сертификат в **Доверенные корневые центры сертификации**:

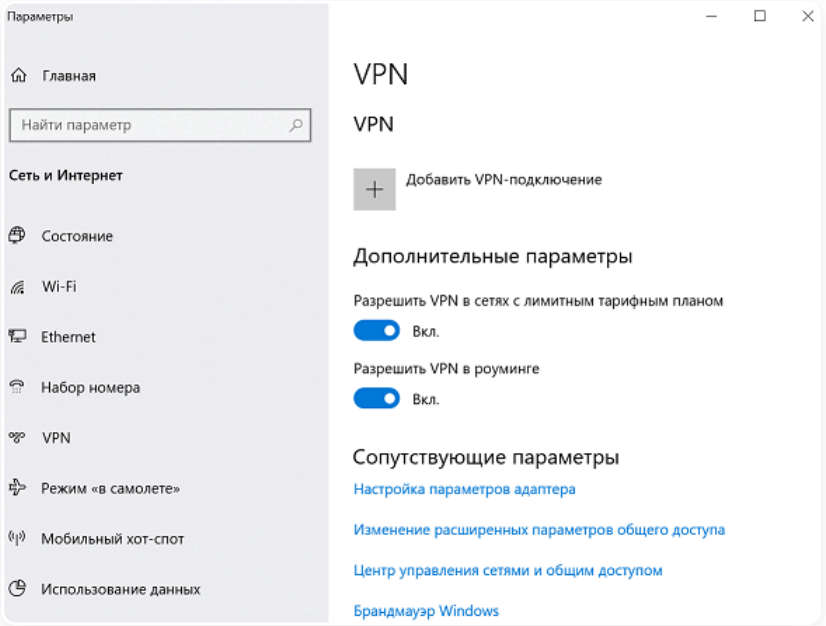


Создание подключения в Windows:

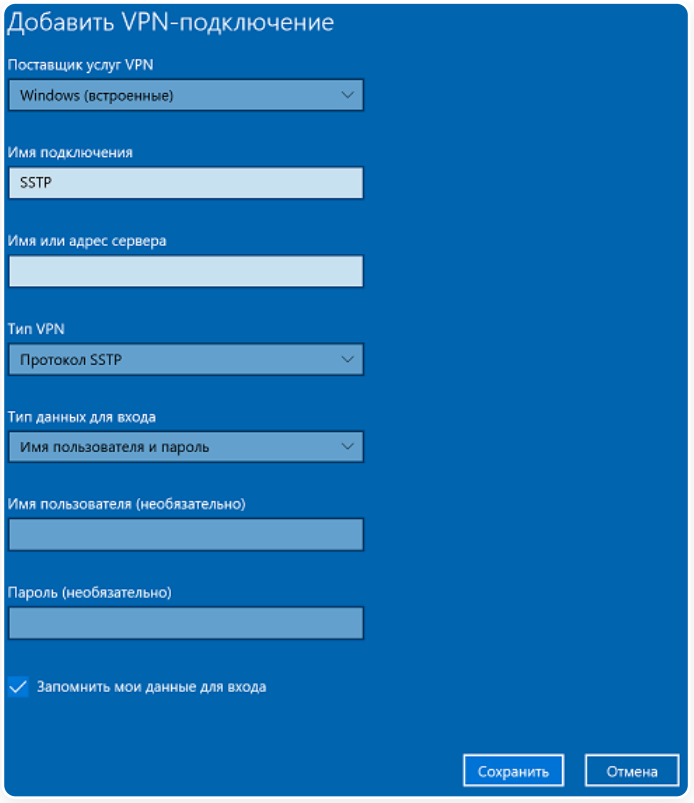
1. Кликните на иконку сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



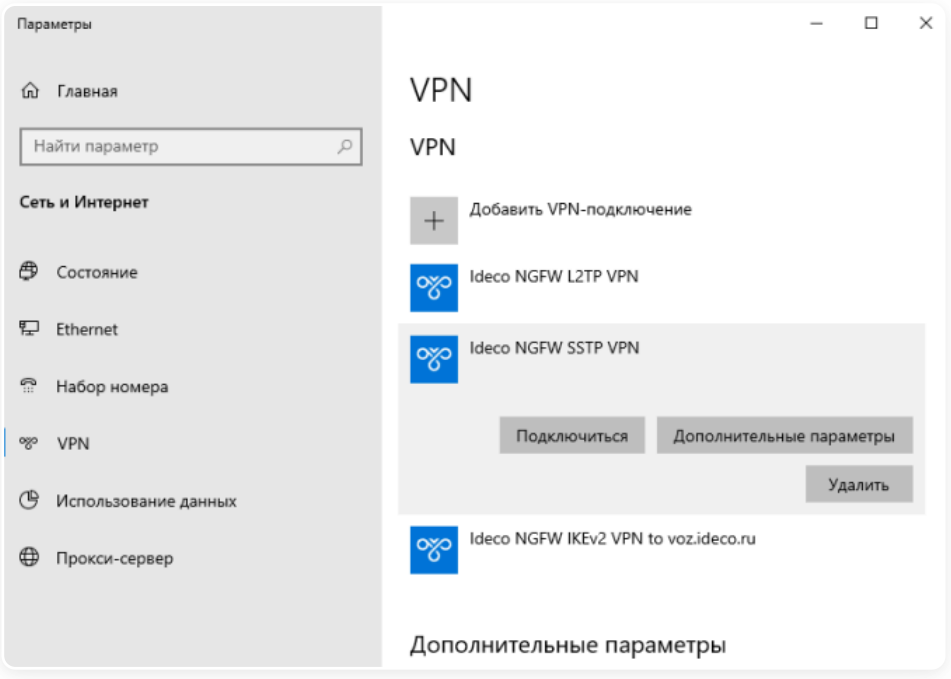
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера в формате ***адрес_VPN_сервера:порт***.
- **Тип VPN** - протокол SSTP.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).
- **Разрешить следующие протоколы** - протокол Microsoft CHAP версии 2 (MS-CHAP v2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры → Изменить**.

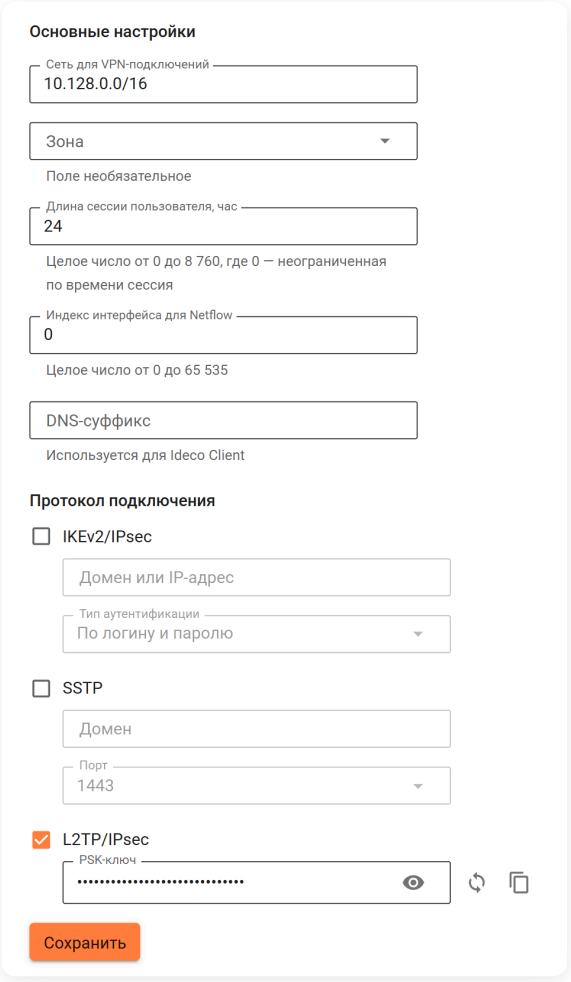
Вкладка 5

> **Важно:** L2TP/IPsec клиенты, находящиеся за одним NAT, могут испытывать проблемы подключения, если клиентов более одного. В решении проблемы поможет инструкция. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

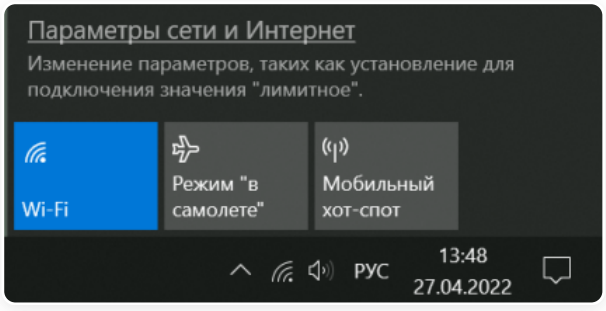
1. Перейдите в **Пользователи → VPN-подключения → Основное**.

2. Включите опцию **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

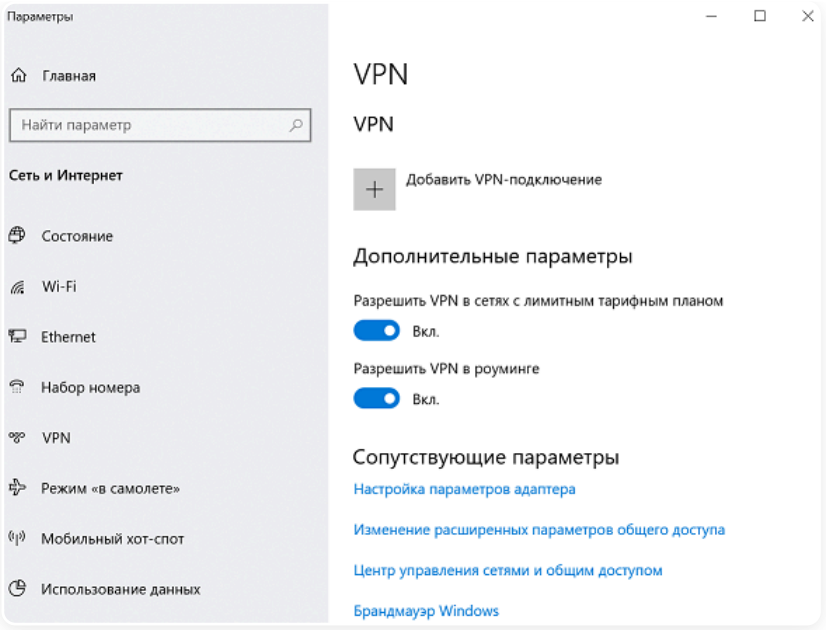


Создание подключения в Windows:

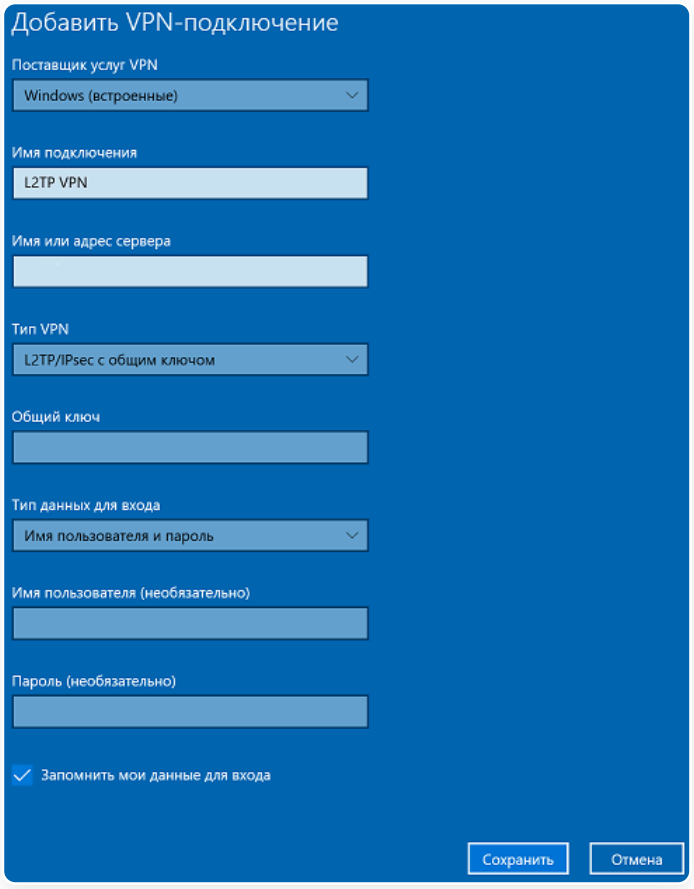
1. Кликните на иконку сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера.
- **Тип VPN** - протокол L2TP/IPsec с общим ключом.
- **Общий ключ** - значение поля **PSK** в разделе **Пользователи → VPN-подключения → Основное → Подключение по L2TP/IPsec**.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

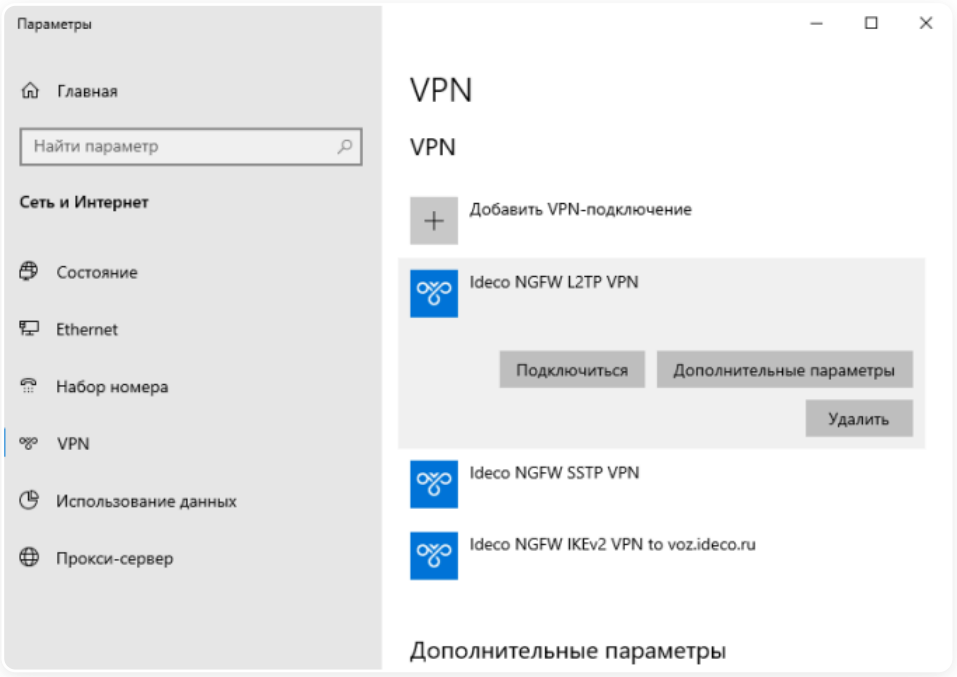
4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования).

- **Разрешить следующие протоколы** - протокол Microsoft CHAP версии 2 (MS-CHAP v2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры** → **Изменить**.

Если создается VPN-подключение к NGFW через проброс портов:

1. Откройте **Редактор реестра**.

2. Перейдите в `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent` и создайте DWORD-параметр с именем AssumeUDPEncapsulationContextOnSendRule и значением `2`.

3. Перезагрузите Windows.

Возможные неполадки:

1. Неправильно указан логин или пароль пользователя. Часто при повторном соединении предлагается указать домен. Старайтесь создавать для учетных записей цифро-буквенные пароли, желательно на латинице. Если есть сомнения в этом пункте, то временно установите логин и пароль пользователю `user` и `123456`.

2. Чтобы пакеты пошли через VPN-туннель, надо убедиться, что в настройках этого подключения стоит чекбокс **Использовать основной шлюз в удаленной сети** в **Настройка параметров адаптера** → **Правой кнопкой мыши по подключению** → **Свойства** → **Сеть** → **Свойства опции "Протокол интернета версии 4 (TCP/IPv4)"** → **Дополнительно**. Если же маршрутизировать все пакеты в этот интерфейс не обязательно, то маршрут надо прописать вручную.

3. Подключение происходит через DNAT, т.е. внешний интерфейс Ideco NGFW Novum не имеет "белого" IP-адреса, а необходимые для работы порты (500 и 4500) "проброшены" на внешний интерфейс устройства, расположенного перед Ideco NGFW Novum и имеющего "белый" IP-адрес. В данном случае VPN-подключение либо вообще не будет устанавливаться, либо будут периодические обрывы. Решение - исключить устройство перед Ideco NGFW Novum и указать на внешнем интерфейсе Ideco NGFW Novum "белый" IP-адрес, к которому в итоге и будут осуществляться L2TP/IPsec-подключения. Либо используйте протокол SSTP, который проще опубликовать с помощью проброса портов.

4. Если в ОС Windows 10 повторно подключиться по L2TP, но при этом использовать **невалидный** ключ PSK (введя его в дополнительных параметрах), подключение все равно будет установлено успешно. Это связано с особенностями работы ОС.

Убедитесь, что локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. Если пересекается, то доступа к сети организации не будет (трафик по таблице маршрутизации пойдет в физический интерфейс, а не в VPN). Адресацию необходимо менять.

Ошибки работы VPN-подключений

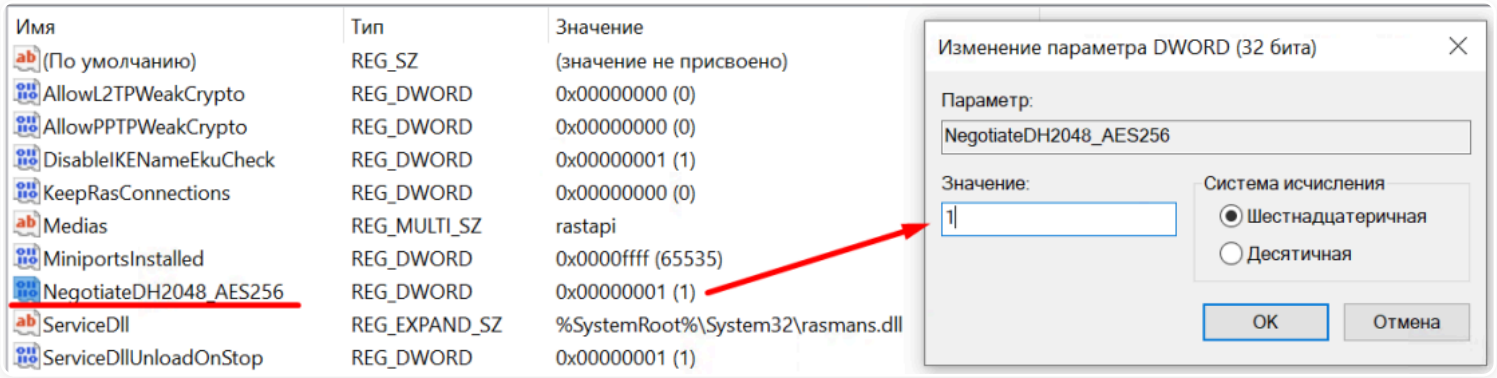
Если при подключении по IKEv2 возникает "Ошибка сопоставления групповой политики" или ошибка с кодом "13868"

Если VPN-подключение по протоколам IPSec в Windows автоматически разрывается через 7 часов 45 минут, для восстановления связи подойдут следующие действия:

1. Переподключите соединение. Соединение восстановится, но через 7 часов 45 минут вновь будет автоматически разорвано. Если требуется, чтобы подключение не разрывалось автоматически, то выполните действия из следующего пункта.

2. Внесите изменения в реестр:

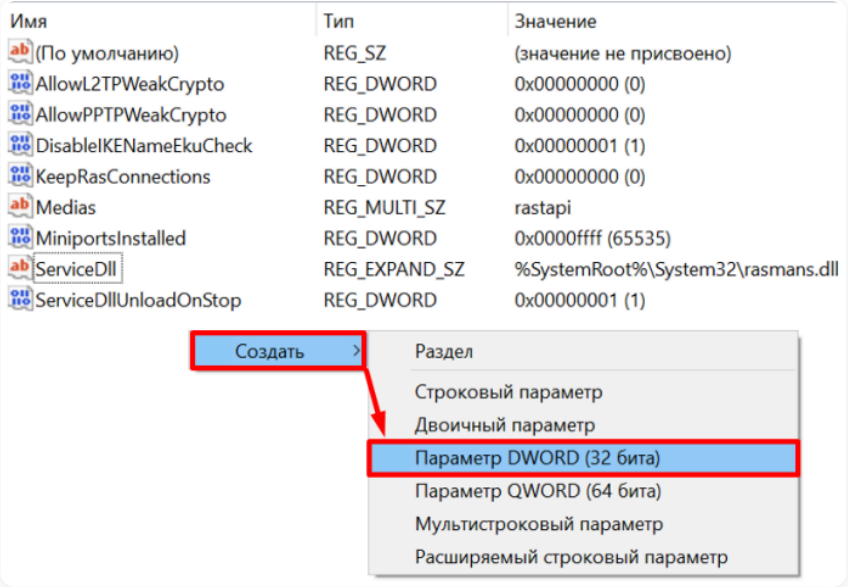
- Откройте **Редактор реестра**.
- Перейдите по пути `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters`.
- Нажмите правой кнопкой мыши по параметру с именем **NegotiateDH2048_AES256** и нажмите **Изменить**.
- В строке **Значение** укажите значение `1`:



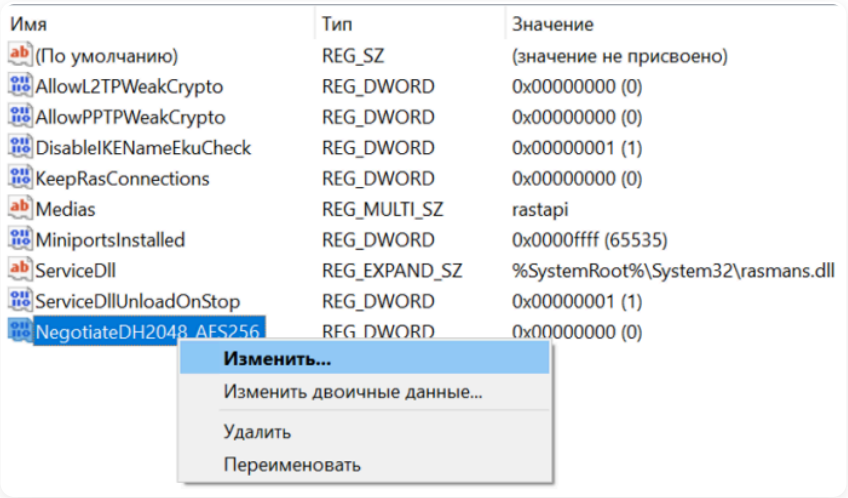
- Нажмите **OK**.
- Перезагрузите Windows.

Если параметра с именем **NegotiateDH2048_AES256** нет, то создайте его. Для этого:

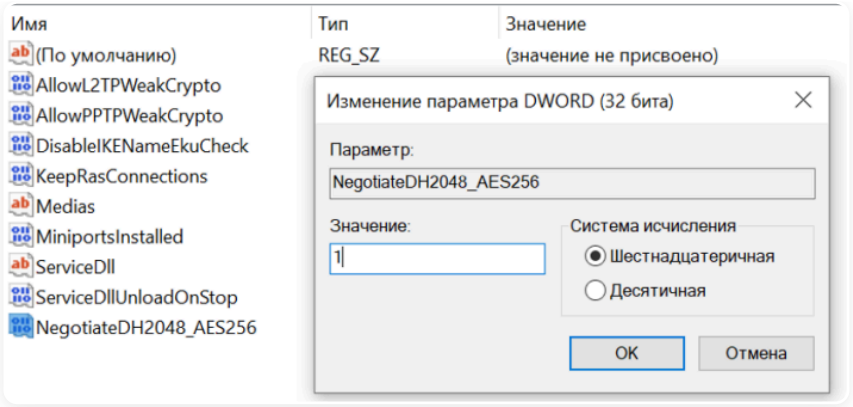
- Нажмите правой кнопкой мыши по свободному месту реестра в **Parameters** и выберите **Создать** → **DWORD**:



- Задайте имя **NegotiateDH2048_AES256**.
- Нажмите правой кнопкой мыши по созданному файлу и выберите **Изменить**:



- В строке **Значение** укажите значение `1`:



- Нажмите **OK**.

3. Перезагрузите Windows.

В Ideco NGFW Novum также есть возможность загрузить с сервера готовые скрипты для создания VPN-подключения в ОС Windows версий 8.1 и 10. Для загрузки и запуска скриптов воспользуйтесь инструкцией.

Создание VPN-подключения на мобильных устройствах

> В статье описана настройка VPN-подключения к Ideco NGFW Novum на мобильных устройствах по протоколам IKEv2/IPsec, L2TP/IPsec, SSTP.

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** в Ideco NGFW Novum и создайте разрешающее правило для VPN-подключения.

Применение сертификатов в протоколе IKEv2/IPsec и SSTP:

- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Скачать сертификат можно в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя, нажав **Скачать корневой сертификат**.

Не рекомендуем использовать для VPN-подключений кириллические логины.

Android

Android

Если в вашей версии Android возникают проблемы при подключении VPN описанными ниже способами, рекомендуем использовать сторонние приложения (например, StrongSwan).

1. Перейдите в **Настройки** → **Подключения** → **Другие настройки** → **VPN** и добавьте подключение. При необходимости воспользуйтесь строкой поиска по настройкам.

2. Выберите тип подключения и заполните поля:

IKEv2/IPsec MSCHAPv2

- **Название сети** - имя подключения.
- **Адрес сервера** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Идентификатор IPsec** - логин пользователя, которому разрешено подключение по VPN.
- **Сертификат ЦС IPsec** - не проверять сервер.
- **Сертификат сервера** - принято от сервера.
- **Имя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

L2TP/IPsec PSK

Начиная с версии Android 12 прекращена поддержка протокола L2TP. Не рекомендуем использовать L2TP, так как подключение крайне небезопасно.

- **Имя** - имя подключения.
- **Адрес сервера** - домен или IP-адрес Ideco NGFW Novum.

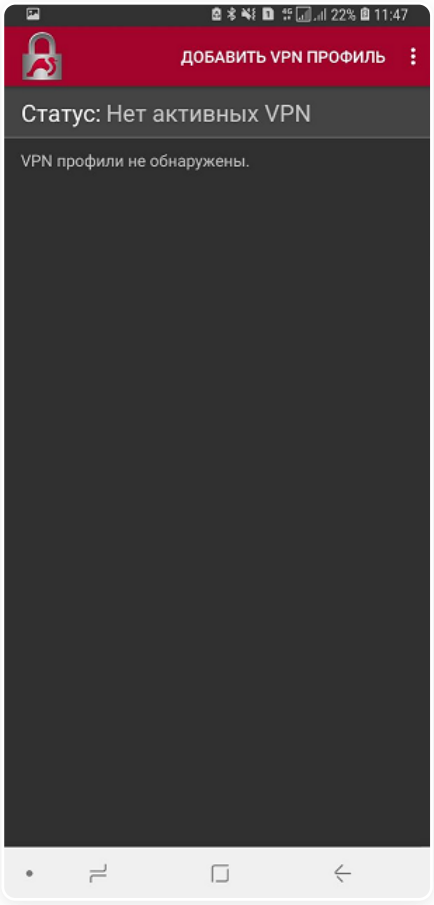
- **Общий ключ IPsec** - значение поля **PSK** в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по L2TP/IPsec** в Ideco NGFW Novum.

3. Нажмите **Сохранить** и активируйте подключение.

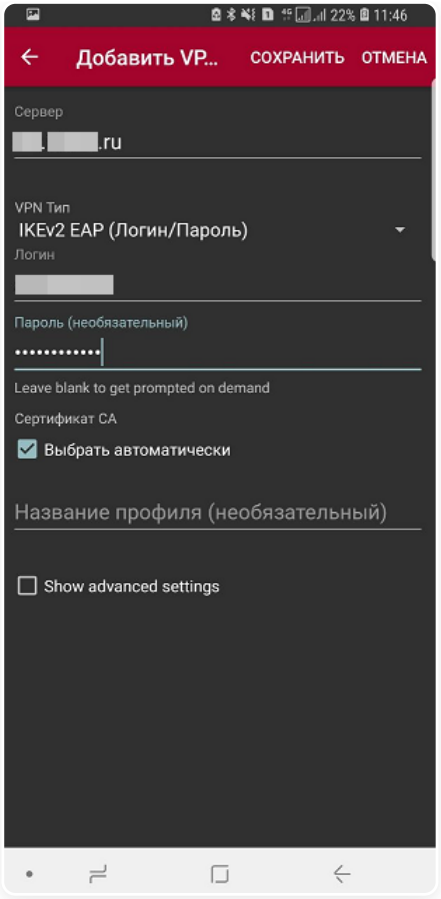
StrongSwan

> Приложение StrongSwan позволяет создавать VPN-подключение только через протокол IKEv2.

1. Нажмите **Добавить VPN профиль**:



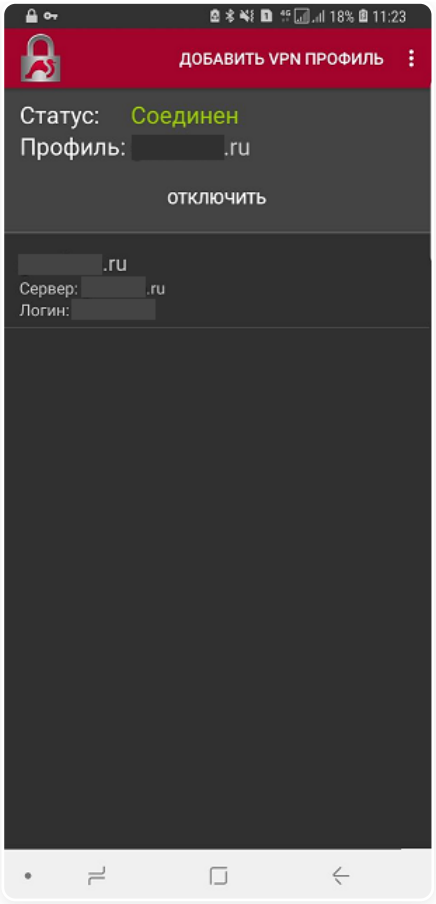
2. Заполните поля:



Расшифровка полей

- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **VPN тип** - IKEv2 EAP (Логин/Пароль).
- **Логин** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

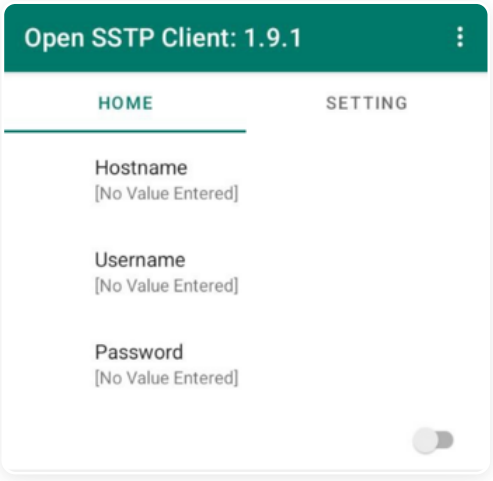
3. Нажмите **Сохранить** и перейдите по созданному подключению:



Open SSTP Client

Приложение Open SSTP Client позволяет создавать VPN-подключение через протокол SSTP.

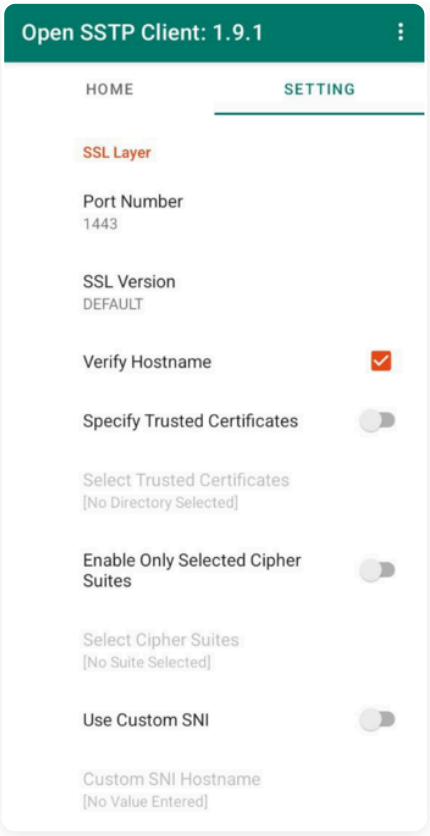
1. Откройте приложение и заполните поля:



Расшифровка полей

- **Hostname** - домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по SSTP**.
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

2. На вкладке **SETTING** укажите в поле **Port Number** порт подключения, указанный в NGFW. По умолчанию порт 1443.



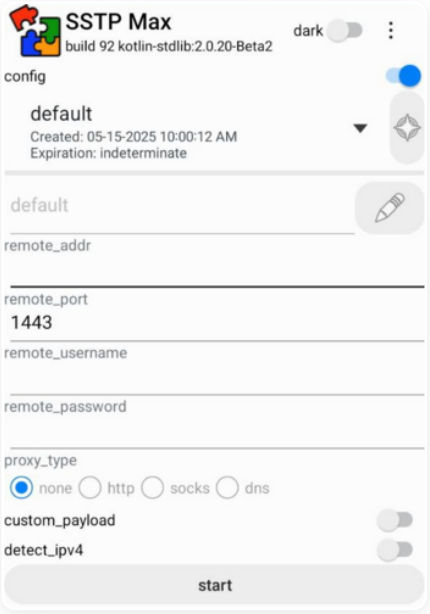
Для автоматического подключения включите опцию **Enable Reconnection** на вкладке **SETTING**.

3. На вкладке **HOME** переключите опцию в правом нижнем углу в положение включено.

SSTP Max

Приложение SSTP Max позволяет создавать VPN-подключение через протокол SSTP. Но рекомендуем к использованию приложение Open SSTP Client.

1. Откройте приложение и заполните поля:



Расшифровка полей

- **remote_addr** - домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по SSTP**.

- **remote_port** - порт подключения, указанный в NGFW. По умолчанию порт 1443.
- **remote_username** - логин пользователя, которому разрешено подключение по VPN.
- **remote_password** - пароль пользователя.

2. Нажмите start.

---

iOS

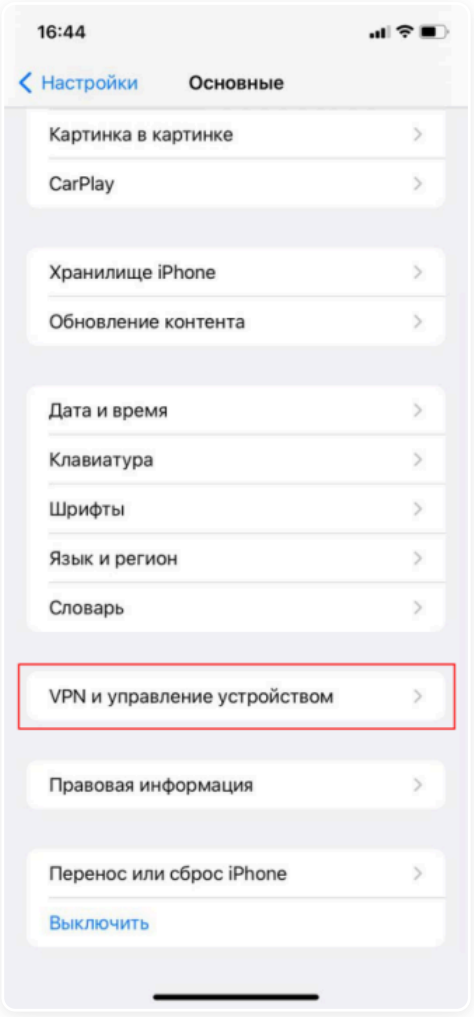
iOS

Выберите тип аутентификации пользователей и выполните действия:

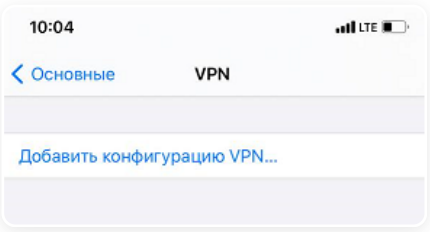
По логину и паролю **По сертификату**

Brooog IKEv2

1. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством** → **VPN**:

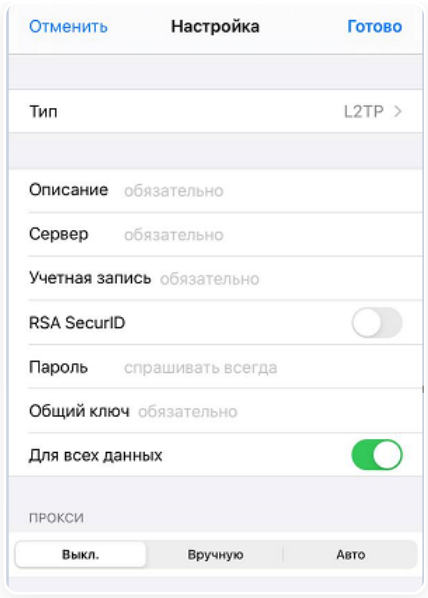


2. Нажмите **Добавить конфигурацию VPN**:



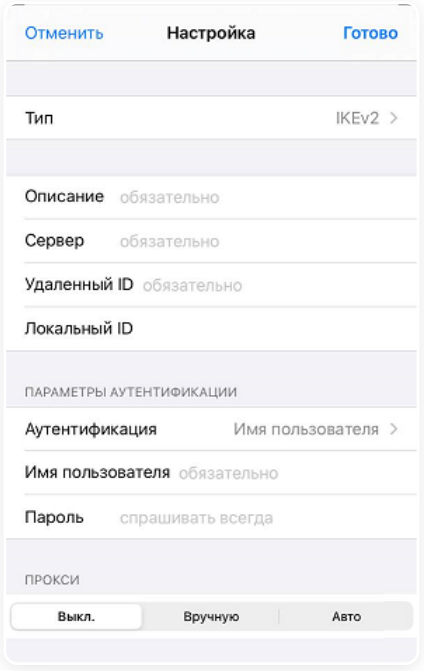
3. Выберите **Тип** подключения и заполните поля:

L2TP



- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес Ideco NGFW Novum.
- **Учетная запись** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.
- **Общий ключ** - значение поля **PSK** в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по L2TP/IPsec** в Ideco NGFW Novum.

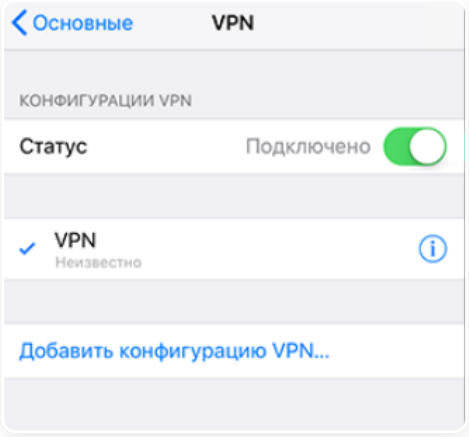
IKEv2



- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Удаленный ID** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

4. Нажмите **Готово**.

5. Включите опцию **Статус**:



Вкладка 3

Подготовка:

Для аутентификации пользователей по сертификату необходимо экспортировать:

- **Корневой сертификат** Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя.
- **Полную цепочку промежуточных сертификатов**, если сертификат пользователя выпущен промежуточным УЦ.
- **Пользовательский сертификат**.

Требования к сертификатам

Алгоритмы хеширования:

- Для подписи сертификатов рекомендуется использовать алгоритм SHA-256 или более стойкий (например, SHA-384, SHA-512).
- Алгоритм SHA-1 не поддерживается.

Ключевые расширения:

- **Для промежуточного сертификата:**
- `basicConstraints=critical,CA:TRUE` - используется для указания, что сертификат может подписывать другие сертификаты.
- **Для пользовательского сертификата:**
- `subjectAltName=DNS:...` - используется для указания альтернативных имен (например, DNS или IP-адреса).

Примеры генерации сертификатов УЦ:

Создание корневого и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **CN** - укажите логин учетной записи пользователя для авторизации.

3. Подписание пользовательского сертификата корневым:

```
openssl x509 -req -in client.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

4. Создание PFX-архива для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile rootCA.crt -passout pass:1234
```

Создание корневого, промежуточного и пользовательского сертификатов

1. Создание корневого сертификата:

```
openssl genrsa -out rootCA.key 4096
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя" \
-out rootCA.crt
```

2. Создание промежуточного сертификата:

```
openssl genrsa -out interCA.key 4096
openssl req -new -key interCA.key -out interCA.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"

openssl x509 -req -in interCA.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial \
-out interCA.crt -days 1825 -sha256 \
-extfile <(printf "basicConstraints=critical,CA:TRUE")
```

3. Создание пользовательского ключа и запроса на сертификат (CSR):

```
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr \
-subj "/C=<страна>/ST=<область>/L=<город>/O=<организация>/CN=общее_имя"
```

- **Common Name (CN)** - укажите логин учетной записи пользователя для авторизации.

4. Подписание пользовательского сертификата промежуточным:

```
openssl x509 -req -in client.csr -CA interCA.crt -CAkey interCA.key -CAcreateserial \
-out client.crt -days 825 -sha256 \
-extfile <(printf "subjectAltName=DNS:<логин_пользователя>")
```

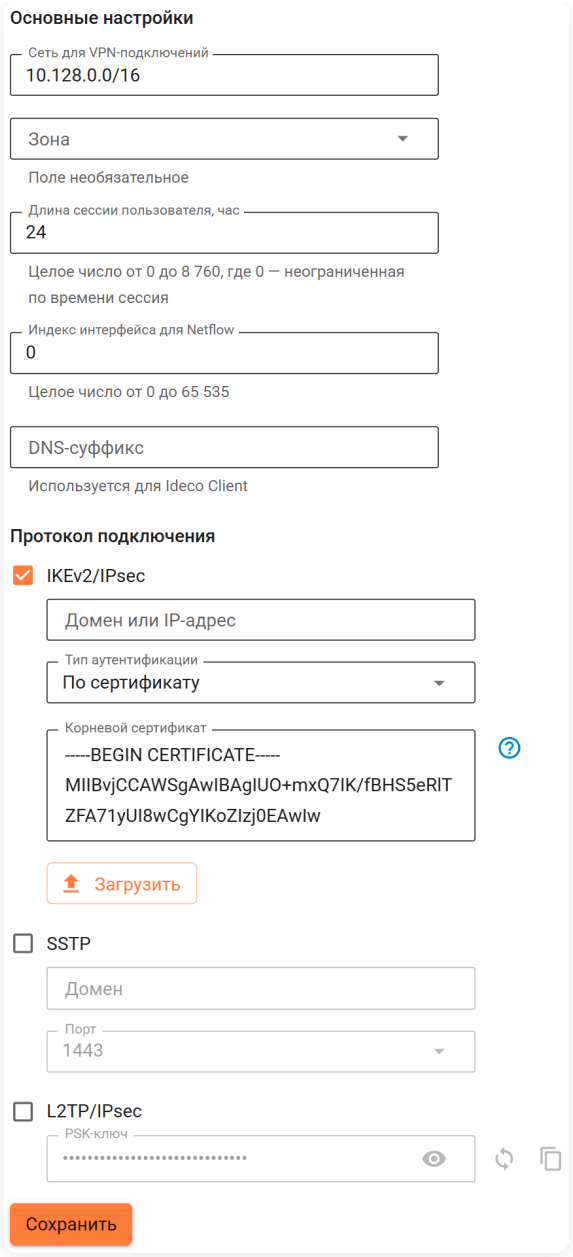
5. Создание PFX-архива с полной цепочкой доверия для экспорта:

```
openssl pkcs12 -export -out client.pfx -inkey client.key -in client.crt \
-certfile <(cat interCA.crt rootCA.crt) -passout pass:1234
```

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Домен и IP-адрес** - укажите доменное имя или IP-адрес, по которому будут подключаться пользователи.
- **Тип аутентификации** - выберите тип **По сертификату**.
- **Корневой сертификат** - загрузите корневой сертификат УЦ или объединенный в один файл корневой и все промежуточные сертификаты.

3. Нажмите **Сохранить**.

4. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

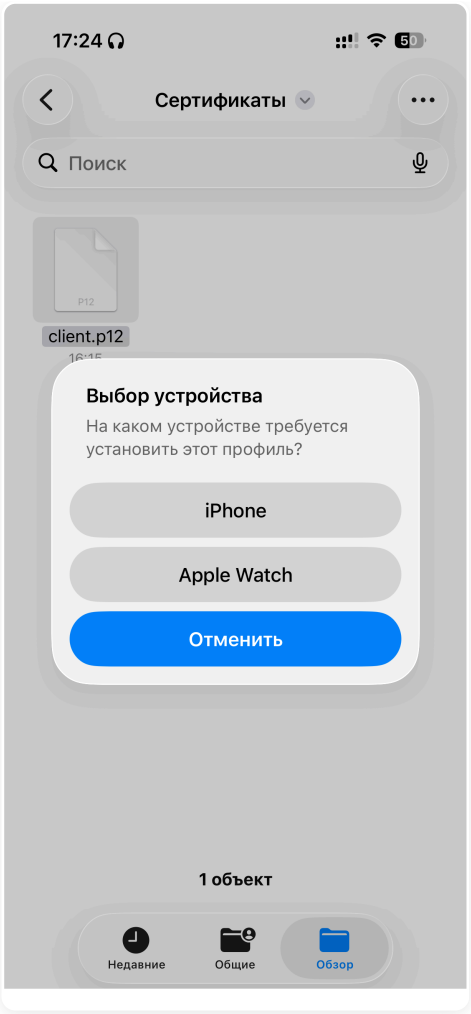
Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let's Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в IOS:

1. Загрузите пользовательский сертификат на устройство пользователя.

2. Нажмите на сертификат и выберите устройство, на которое требуется установить профиль:

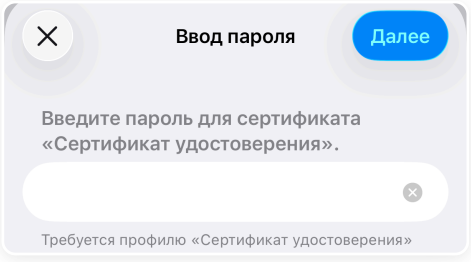


3. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством**.

4. В блоке **Загруженный профиль** выберите **Сертификат удостоверения** и нажмите **Установить**:

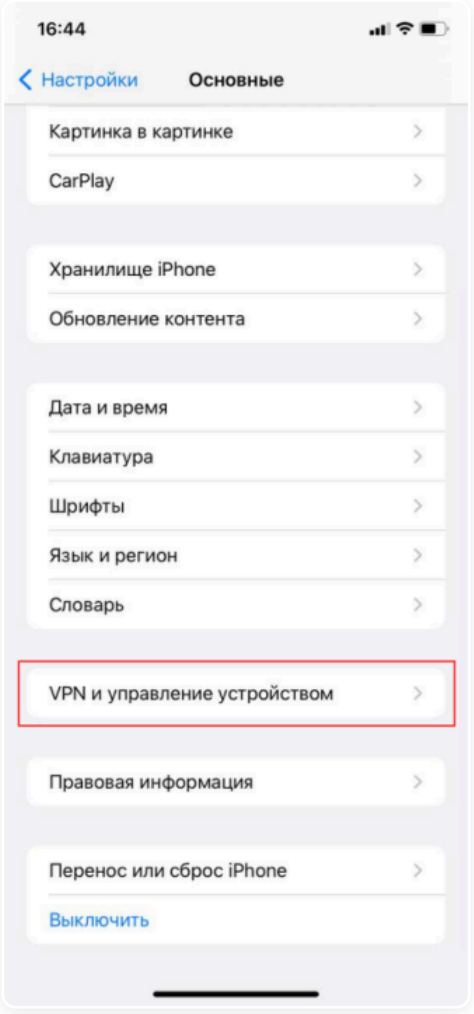
5. Введите код-пароль, используемый для разблокировки устройства, и нажмите **Установить**.

6. Введите пароль для сертификата и нажмите **Далее**:

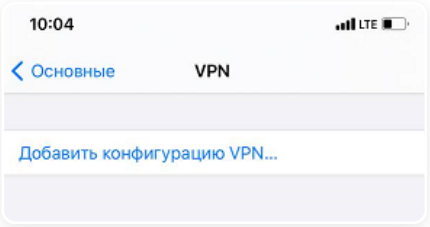


7. Нажмите .

8. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством** → **VPN**:



9. Нажмите **Добавить конфигурацию VPN**:

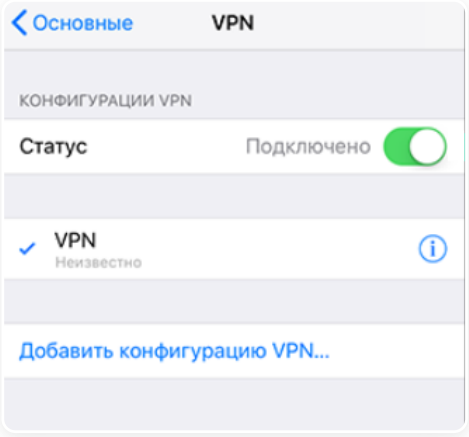


10. Заполните поля:

- **Тип** - выберите IKEv2.
- **Описание** - введите название соединения.
- **Сервер** - укажите домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Удаленный ID** - укажите домен, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Локальный ID** - введите логин пользователя.
- **Аутентификация** - выберите **Сертификат**.
- **Сертификат** - выберите сертификат.

11. Нажмите .

12. Включите опцию **Статус**:



Вкладка 4

1. Нажмите **Add VPN Connection**:

2. Заполните поля и включите опцию **Connect on Demand**:

Расшифровка полей

- **Server** - домен или IP-адрес, указанный в Ideco NGFW Novum в разделе **Пользователи** → **VPN-подключения** → **Основное** → **IKEv2/IPsec**.
- **Username** - логин пользователя, которому разрешено подключение по VPN.
- **Password** - пароль пользователя.

3. Нажмите **Save** и переведите опцию в режим **CONNECTED**:

Полезные ссылки

- **VPN-подключения**
- **Подключение по IKEv2/IPsec**

Инструкция по созданию подключения в macOS

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Не рекомендуем использовать для VPN-подключений кириллические логины.

При проблемах с подключением на IOS требуется:

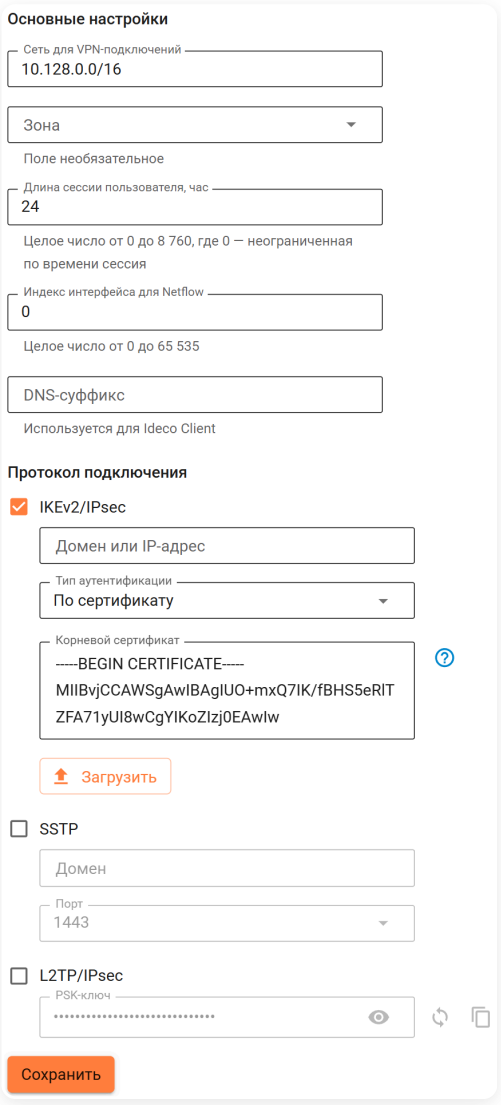
1. Проверить, что в качестве VPN-сервера указано доменное имя VPN-сервера в разделе **Пользователи** → **VPN-подключения**.
2. Проверить, что на доменное имя VPN-сервера выдан сертификат Let's Encrypt.

IKEv2/IPsec

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **IKEv2/IPsec** и заполните поля:



- **Индекс интерфейса для Netflow** - если используете Netflow, введите целое число от 0 до 65535 для идентификации интерфейса.
- **Домен или IP-адрес** - укажите внешний IP-адрес или доменное имя NGFW Novum, к которому будет подключаться клиент.

- **Тип аутентификации** - выберите тип аутентификации пользователя:
  - **По логину и паролю** - вход по логину и паролю учетной записи пользователя.
  - **По сертификату** - вход по сертификату пользователя.
- **Корневой сертификат** - загрузите корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то загрузите полную цепочку доверия: все промежуточные и корневой сертификаты.

> Методы аутентификации для протокола IKEv2/IPsec работают по принципу **или-или** в рамках одного контекста. Если выбран вход по сертификату, то аутентификация по логину и паролю для этого контекста доступна не будет, и наоборот. Для предоставления пользователям обоих методов необходимо настроить отдельный VCE.

3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

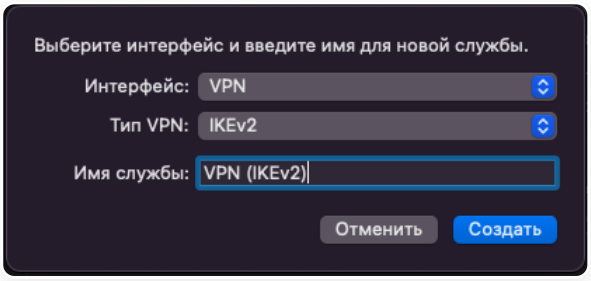
- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в macOS:

1. Перейдите в **Системные настройки** → **Сеть**.

2. Нажмите **Добавить** в левом нижнем углу (иконка +).

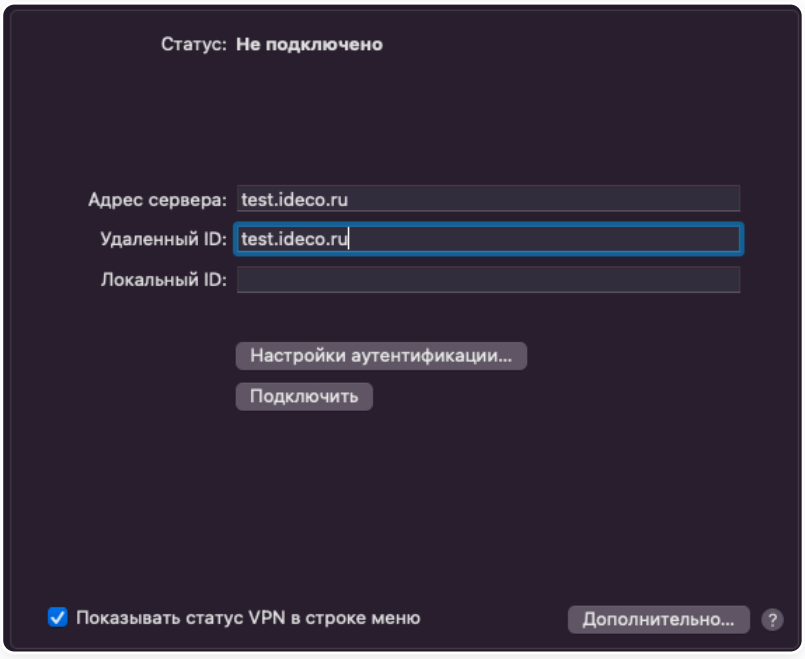
3. Заполните поля:



- **Интерфейс** - VPN.
- **Тип VPN** - IKEv2.
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

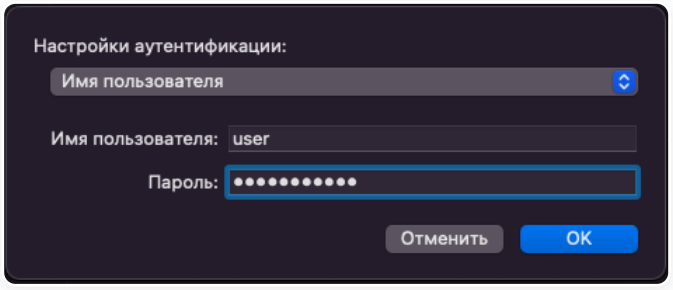
5. Установите параметры подключения:



- **Адрес сервера** - адрес VPN-сервера.
- **Удаленный ID** - продублируйте адрес VPN-сервера.

6. Выберите **Настройки аутентификации**.

7. Укажите идентификационные данные и нажмите **OK**:



- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

8. Нажмите **OK**.

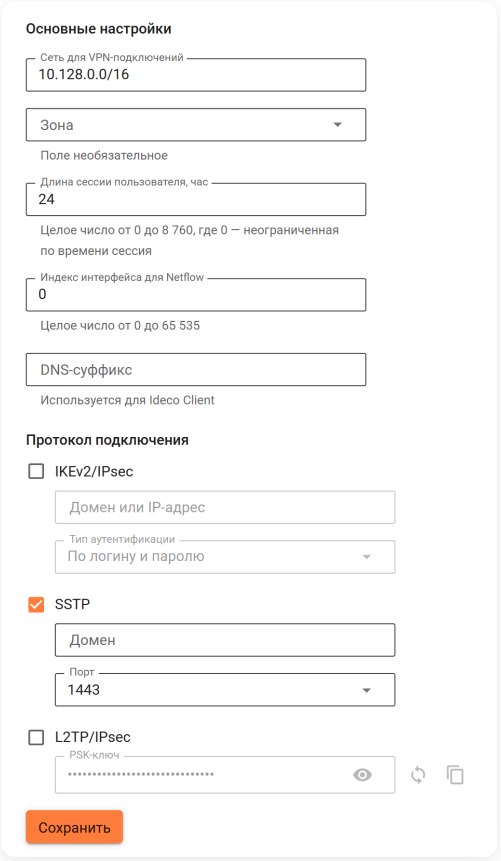
9. Включите опцию **Показывать статус VPN в строке меню**, нажмите **Применить** и включите соединение.

SSTP

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

2. Включите опцию **SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW Novum в **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW Novum или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

- Если сертификат для VPN-подключений издан NGFW Novum, установите корневой сертификат NGFW Novum на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**.

Создание подключения в macOS:

1. Откройте терминал и установите `sstp-client`, выполнив команды:

```
brew update
brew install sstp-client
```

2. Создайте и включите SSTP-подключение. Путь к утилите `sstpc` зависит от процессора Mac:

> Узнать архитектуру процессора можно командой `uname -m`:
>
> - `arm64` - Apple Silicon.
> - `x86_64` - Intel.
>
> Также путь установки Homebrew покажет команда `brew --prefix`.

- **Для Mac с процессорами Apple Silicon (M1/M2/M3/M4)** - каталог `/opt/homebrew`:

```
sudo /opt/homebrew/sbin/sstpc --cert-warn --tls-ext --user <логин пользователя Ideco NGFW Novum> --password <пароль польз
```

- **Для Mac с процессорами Intel** - каталог `/usr/local`:

```
sudo /usr/local/sbin/sstpc --cert-warn --tls-ext --user <логин пользователя Ideco NGFW Novum> --password <пароль пользова
```

Если указан параметр `defaultroute`, в VPN-туннель будет заворачиваться весь трафик.

Чтобы через VPN-туннель проходил только трафик до определенных сетей, используйте параметр `nodefaultroute` и добавьте маршруты в таблицу маршрутизации вручную, например: `sudo route add -net "172.16.0.0/12" -interface ppp0`.

3. Для проверки подключения откройте новую вкладку или окно терминала и введите команду `ifconfig -a`. Если в выводе присутствует строка вида `ppp0: flags=8051 mtu 1500 inet 10.128.0.0 → 10.128.0.1 netmask 0xff000000`, подключение установлено.

4. Чтобы отключить соединение, перейдите в терминал, из которого соединение было установлено, и нажмите **Ctrl+C**.

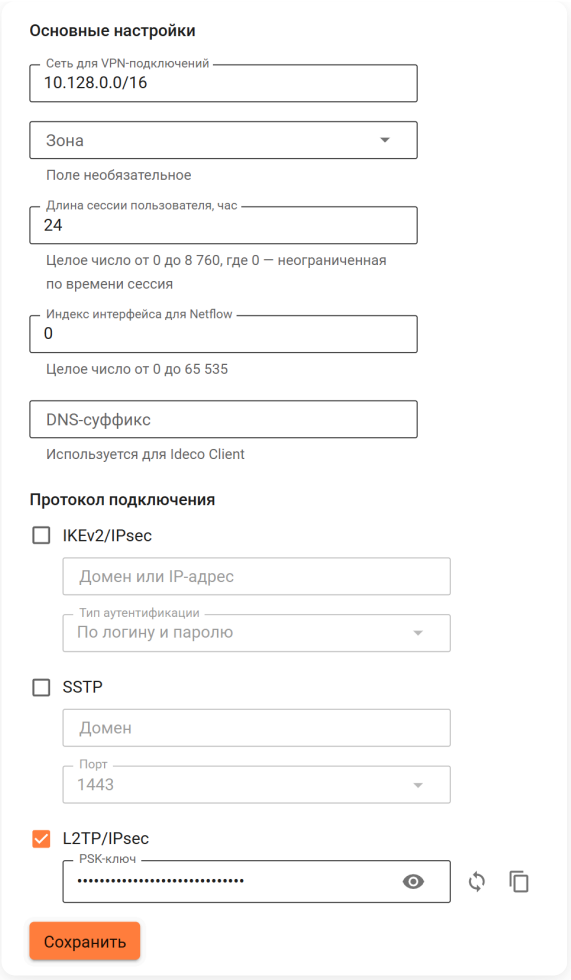
L2TP/IPsec

Важно: L2TP/IPsec-клиенты, находящиеся за одним NAT, могут испытывать проблемы с подключением, если клиентов более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW Novum:

1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**.

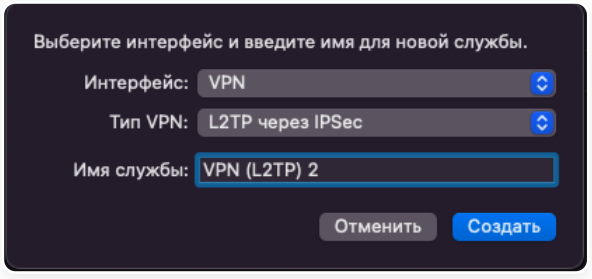
2. Включите опцию **L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в macOS:

1. Перейдите в **Системные настройки** → **Сеть** и нажмите **Добавить** в левом нижнем углу (иконка (+)).

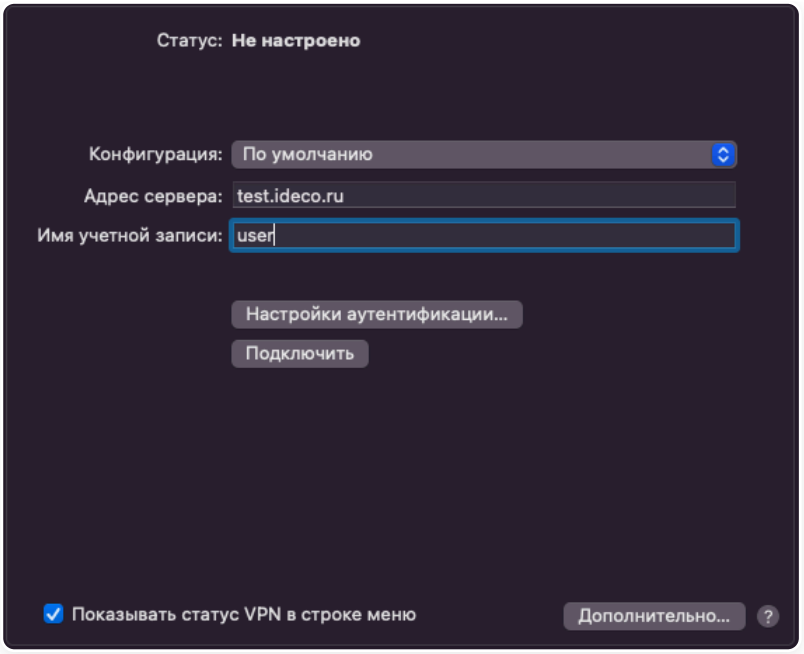
3. Заполните поля:



- **Интерфейс** - VPN.
- **Тип VPN** - L2TP через IPsec.
- **Имя службы** - имя подключения.

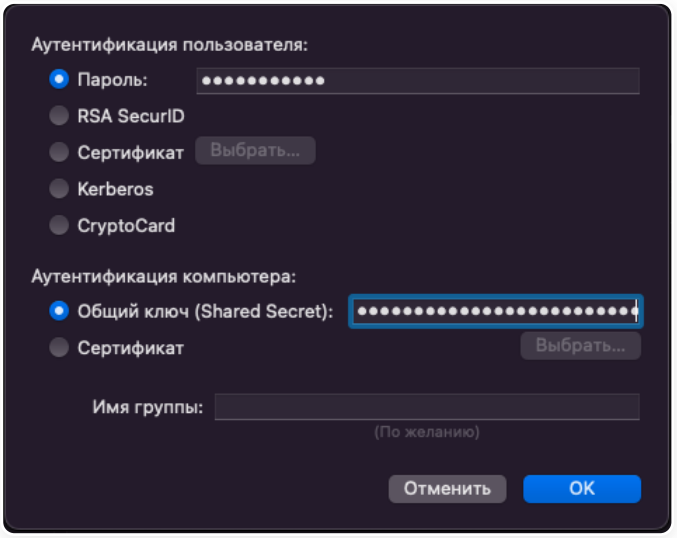
4. Нажмите **Создать**.

5. Заполните **Адрес сервера** и **Имя учетной записи**:



6. Включите опцию **Показывать статус VPN в строке меню** и выберите **Настройки аутентификации**.

7. В **Аутентификации пользователя** заполните **Пароль**, в **Аутентификации компьютера** - **Общий ключ (Shared Secret)**:



8. Нажмите **ОК** → **Применить** и включите соединение.

Полезные ссылки

- **VPN-подключения**

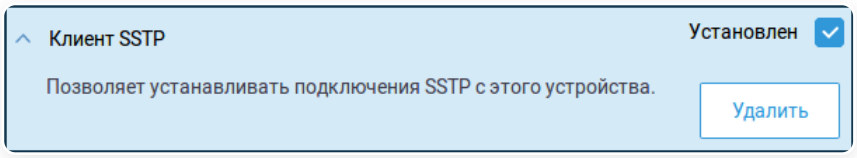
Подключение по SSTP Wi-Fi-роутеров Keenetic

Поддерживаются все роутеры на базе KeeneticOS 3.x.x.

1. Выполните настройку пользователей в Ideco NGFW Novum и включите SSTP в **Пользователи** → **VPN-подключения** → **Основное**.

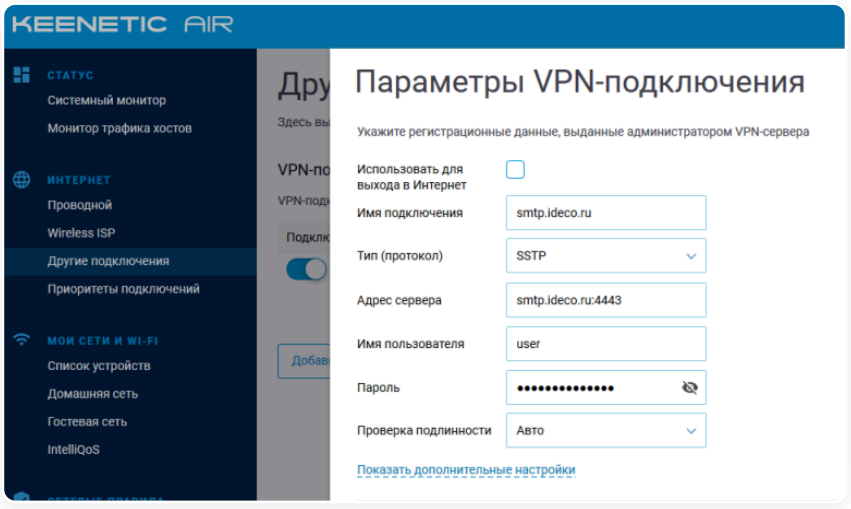
2. Зайдите в веб-интерфейс управления Keenetic: `http://my.keenetic.net`.

3. Установите компонент системы **Клиент SSTP** на странице **Общие настройки** в разделе **Обновления и компоненты**, нажмите **Изменить набор компонентов**:



Подробнее о настройках в документации Keenetic.

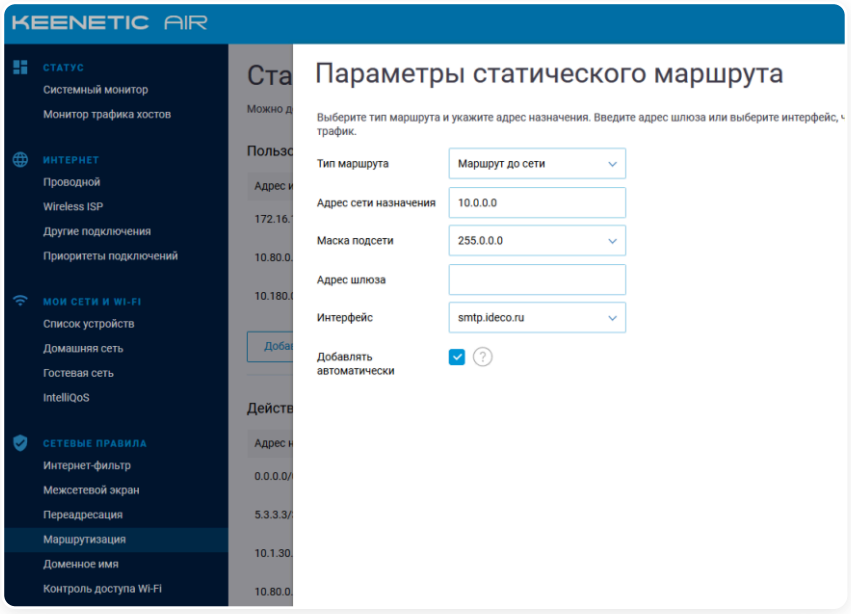
4. Создайте подключение в **Интернет** → **Другие подключения** нажмите кнопку **Добавить подключение**



Не устанавливайте флаг **Использовать для выхода в интернет**.

Введите имя подключения, протокол SSTP, адрес сервера (**обязательно укажите в адресе порт через двоеточие**), имя пользователя и пароль.

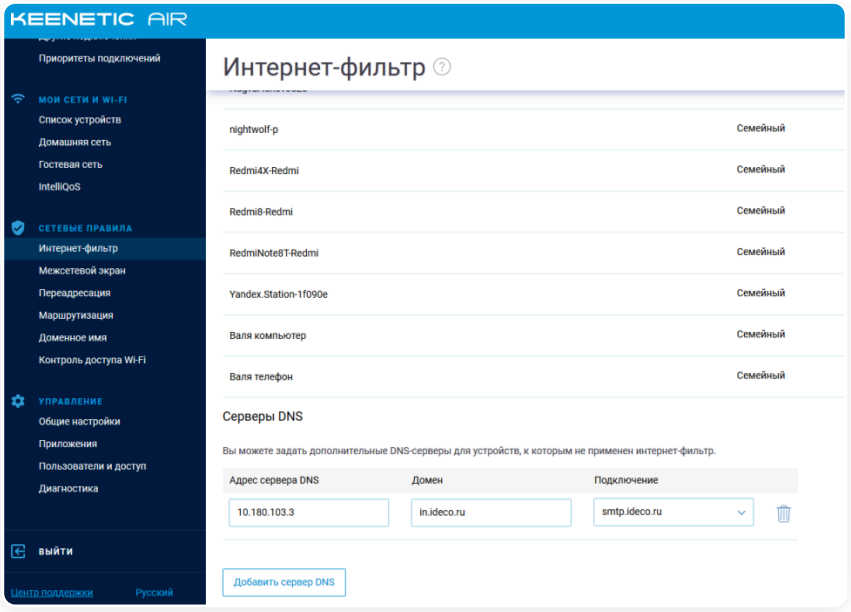
5. В **Сетевые правила** → **Маршруты** добавьте маршруты в рабочую сеть. Например, если сеть офиса `10.0.0.0/8`, добавьте маршрут:



Выберите в качестве **Интерфейса** созданное VPN-подключение и установите флаг **Добавлять автоматически**, чтобы маршрут действовал только при активном VPN-подключении.

6. Настройте DNS для локального домена (например, Active Directory), чтобы обращаться к ресурсам (файловым и иным серверам) по DNS-именам.

В **Сетевые правила** → **Интернет-фильтр** → **Серверы DNS** укажите DNS-сервер контроллера домена и имя домена:



Настройка закончена.

7. Используйте утилиту **ping** в командной строке для проверки связи и маршрутизации.

`nslookup` - для проверки резолвинга локальных имен рабочей сети.

Если VPN работает, но с некоторыми ресурсами (например, файловыми или RDP) нет связи, воспользуйтесь инструкцией для диагностики проблем.

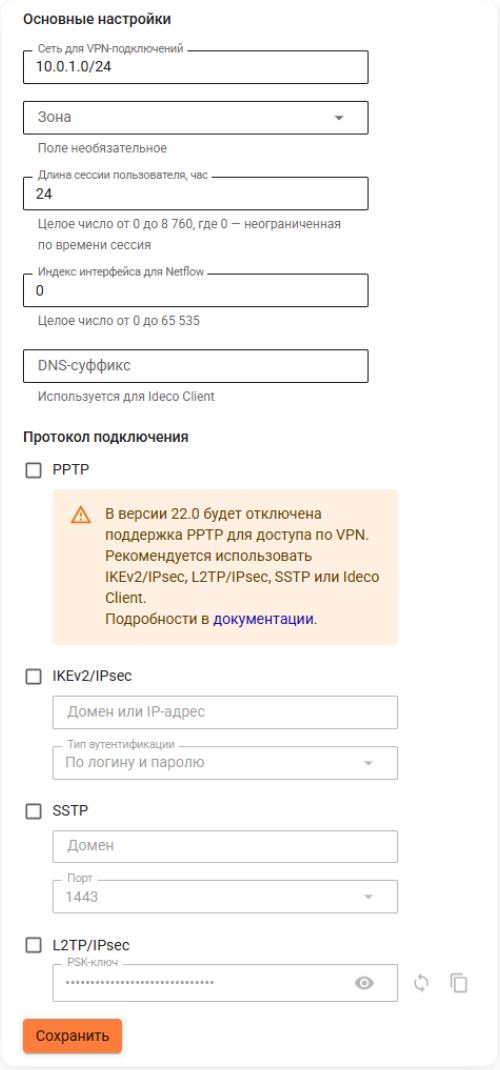
Полезные ссылки

- **Подключение по SSTP**

Как избежать проблем с подключением VPN-клиентов при использовании нескольких серверов Ideco NGFW Novum

При использовании нескольких серверов Ideco NGFW Novum могут возникнуть проблемы с подключением VPN-клиентов. Частая причина - пересечение подсетей, используемых для выдачи IP-адресов удаленным пользователям.

Для решения проблемы настройте изолированные подсети для каждого сервера в **Пользователи** → **VPN-подключения** → **Основное**:



В поле **Сеть для VPN-подключений** укажите уникальные значения, например:

- Для ideco1 - `10.0.1.0/24`.
- Для ideco2 - `10.0.2.0/24`.

Подробнее о настройке VPN-подключений - в статье.

Избегайте пересечений подсетей с другими сервисами внутри одного сервера. Убедитесь, что подсеть для VPN не пересекается с:

- Диапазонами IP-адресов для выдачи в **Сервисы** → **DHCP**.
- Правилами авторизации **По подсетям**. Подробнее - в статье.
- Статическими привязками в **Пользователи** → **VPN-подключения** → **Выдача IP-адресов**.

Если проблема сохраняется, обратитесь в Техническую поддержку.

Полезные ссылки

- **VPN-подключения**
- **Особенности маршрутизации и организации доступа**

Подключение Keenetic по SSTP или IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Для создания подключения используются протоколы:

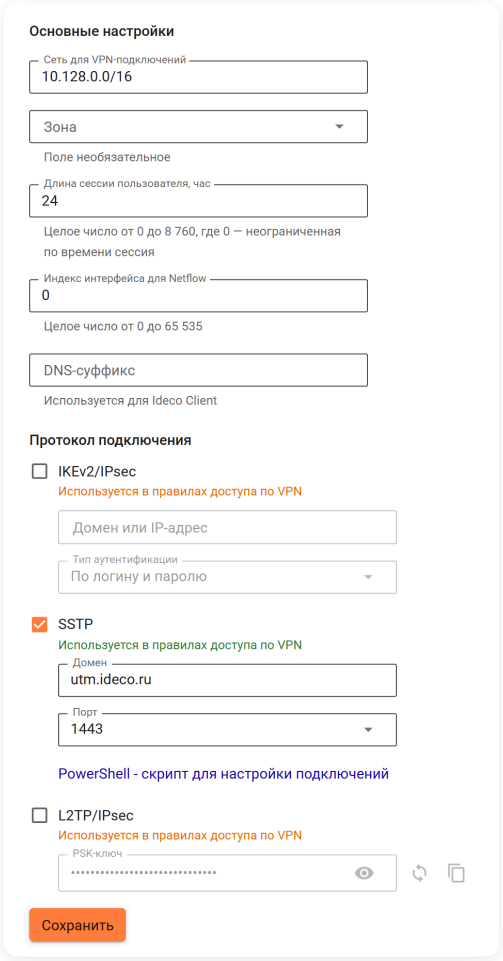
- **SSTP** - для безопасного соединения между клиентом и сервером.
- **IPsec** - для безопасной передачи данных в IP-сетях.

Подключение по SSTP

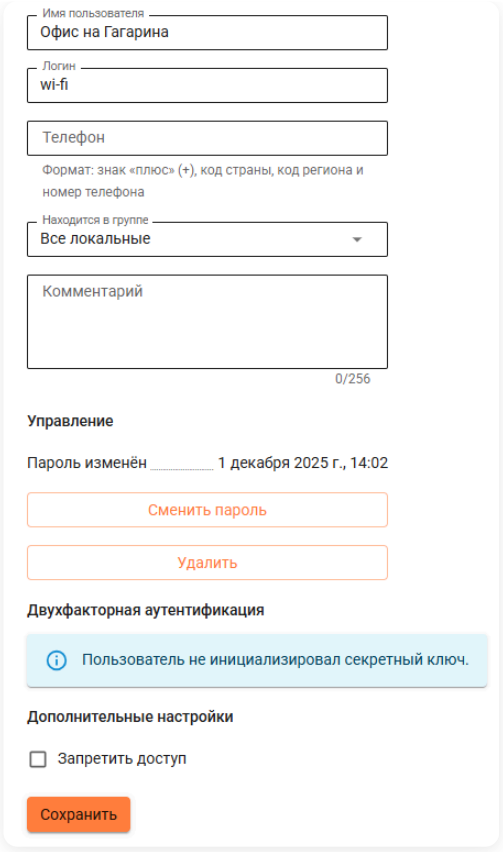
Если доступ из центрального офиса в сеть за Keenetic не нужен, воспользуйтесь инструкцией по подключению в режиме client-to-site.

Настройка Ideco NGFW Novum

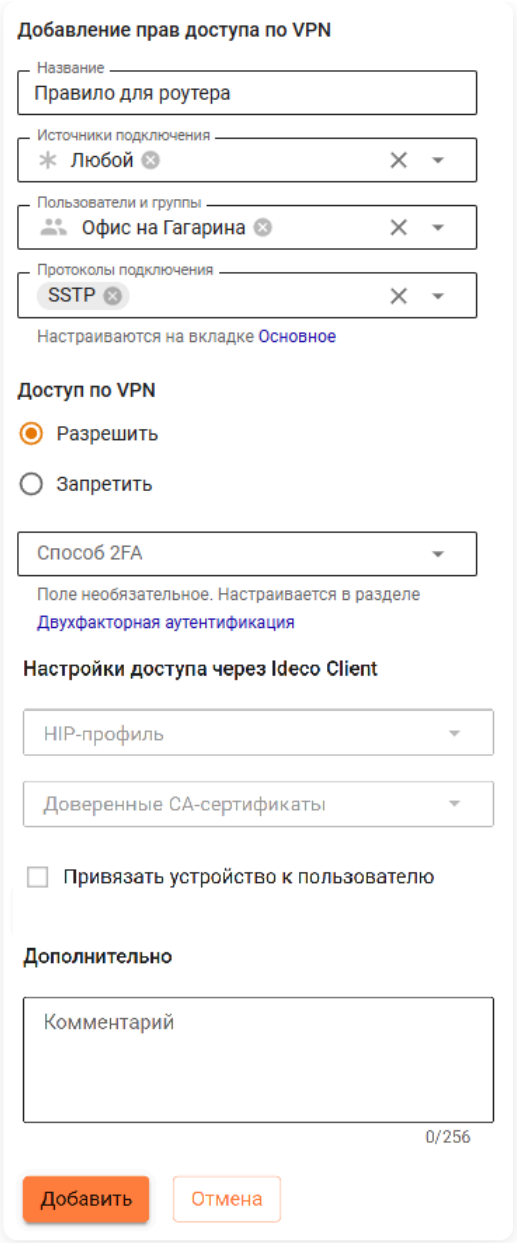
1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**, включите настройку SSTP, укажите домен и порт для подключения:



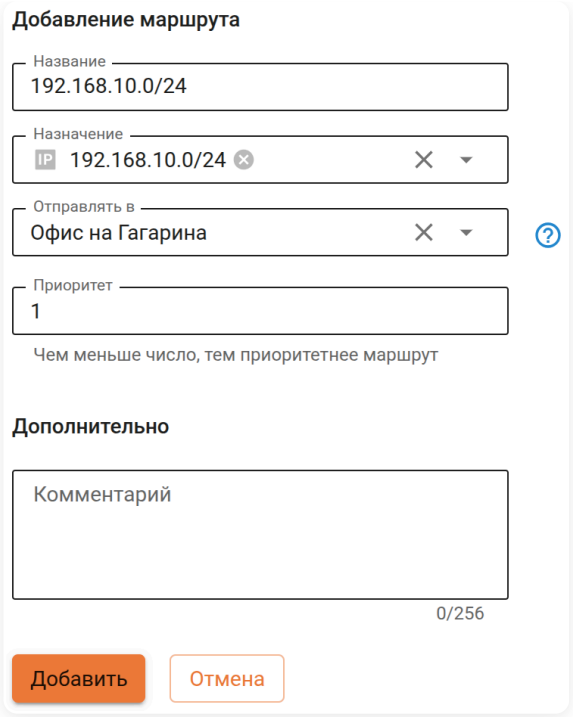
2. Перейдите в **Пользователи** → **Учетные записи** и создайте специального пользователя для удаленного роутера. Логин и пароль пользователя будут использоваться на роутере:



3. Перейдите в **VPN-подключения** → **Доступ по VPN** и создайте правило доступа по VPN для этого пользователя:



4. Пропишите маршруты в удаленную сеть. Например, если сеть за роутером `192.168.10.0/24`, необходимо добавить маршрут в **Маршрутизация** → **Статическая**:



Настройка роутера Keenetic

Настройте VPN-подключение роутера Keenetic по инструкции для client-to-site подключений.

Необходимо выполнить все три пункта:

1. Настроить VPN-подключение.

2. Настроить маршруты.

3. Настроить DNS для резолвинга локального домена (если используете Active Directory).

Для проверки связи используйте утилиты ping и traceroute.

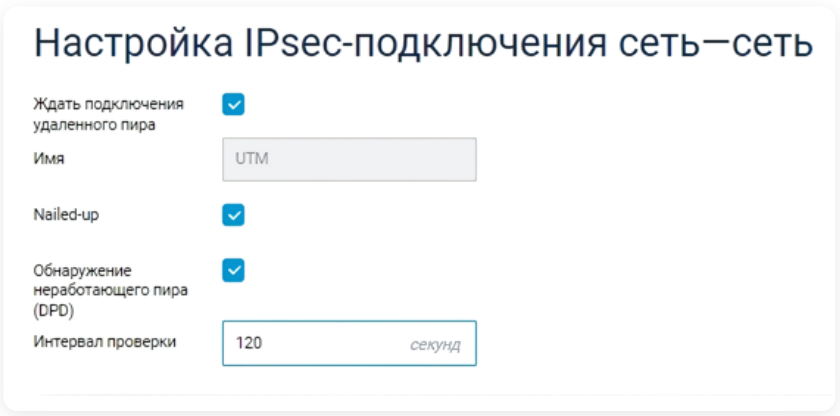
Доступ часто блокируется в Windows из-за настроек сетевых профилей.

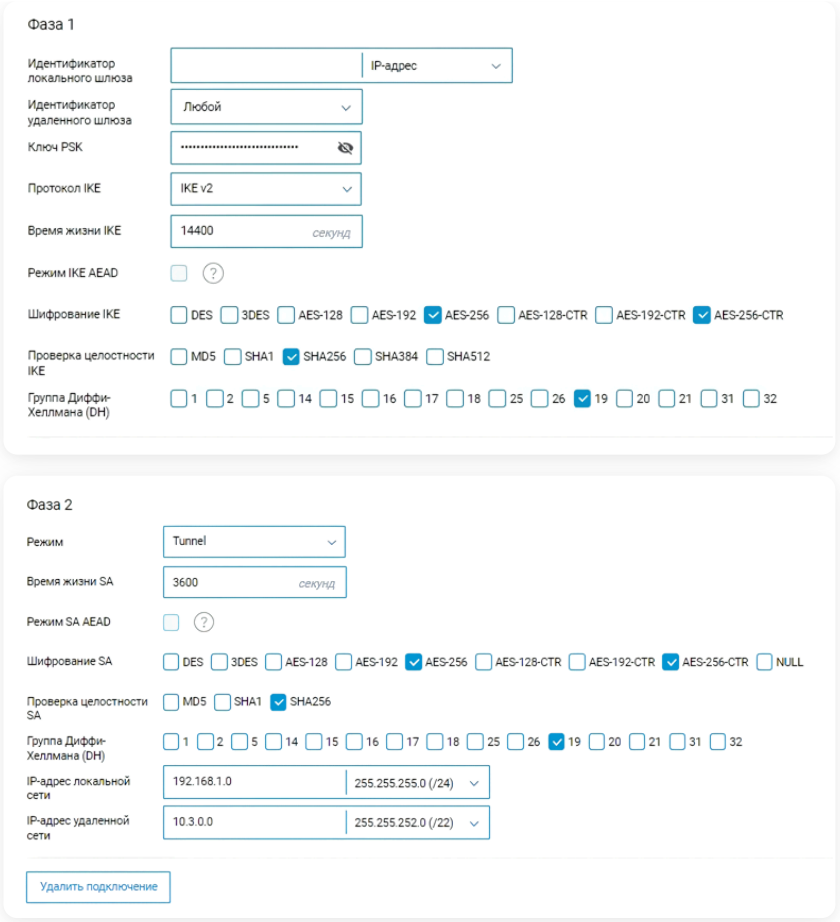
Разрешите доступ до внешних сетей во всех профилях, выполнив команду в PowerShell (запущенного с правами администратора):
`Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`

Подключение по IPsec

На стороне Ideco NGFW Novum настройте подключения в **Сервисы** → **IPsec** → **Исходящие подключения** или в **Сервисы** → **IPsec** → **Входящие подключения**.

На стороне устройства Keenetic при создании подключения в **Интернет** → **Другие подключения** используйте следующие настройки протоколов шифрования:





В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **Подключение по SSTP Wi-Fi-роутеров Keenetic**
- **IPsec**

Аутентификация

Настройка сертификатов и аутентификации пользователей в Ideco NGFW

Настройка корневого и подчиненного центра сертификации с помощью AD CS

Перейти >

Использование собственного CA-сертификата в Контент-фильтре

Перейти >

Как установить сертификат Ideco NGFW на Android

Перейти >

Настройка прозрачной авторизации на Astra Linux

Перейти >

Настройка автоматической веб-аутентификации на Ideco NGFW на Linux

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка корневого и подчиненного центра сертификации с помощью AD CS

Как подготовить и настроить корневой центр сертификации (Root CA), а затем на его основе создать подчиненный центр сертификации (Subordinate CA) через Active Directory Certificate Services (AD CS) для работы с NGFW Novum.

Предварительные требования:

- Необходимо развернуть две виртуальные машины в одной сети с правами администратора:
  - Корневой центр сертификации (Root CA) - Windows Server 2022 без роли контроллера домена (рекомендуется).
  - Подчиненный центр сертификации (Subordinate CA) - Windows Server 2022 с ролью контроллера домена (DC).

Настройка корневого центра сертификации (Root CA)

Шаг 1. Подготовка конфигурационного файла

На сервере, претендующем на роль корневого центра сертификации, необходимо создать INF-файл с именем `CAPolicy.inf` по пути `C:\Windows\CAPolicy.inf`. В файле укажите:

```
[Version]
Signature="$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
CRLPeriod=Years
CRLPeriodUnits=1
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=30
CRLOverlapPeriod=Weeks
CRLOverlapUnits=1
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=0

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=True
```

Расшифровка полей

Version

- `Signature="$Windows NT$"` - файл предназначен для операционной системы Windows NT и совместимых версий. Этот маркер обязателен для правильного распознавания системы.

Certsrv Server

- `RenewalKeyLength=2048` - длина нового ключа шифрования для сертификата самого Центра сертификации (CA) при его обновлении;
- `RenewalValidityPeriod=Years` - единица измерения срока действия для нового сертификата CA;
- `RenewalValidityPeriodUnits=20` - значение срока действия нового сертификата CA;
- `CRLPeriod=Years` - единица измерения интервала публикации основного списка отозванных сертификатов (CRL);
- `CRLPeriodUnits=1` - значение интервала публикации основного CRL;
- `CRLDeltaPeriod=Days` - единица измерения интервала публикации дельта-CRL (разностного списка отзыва);
- `CRLDeltaPeriodUnits=30` - значение интервала публикации дельта-CRL;
- `CRLOverlapPeriod=Weeks` - единица измерения интервала перекрытия (времени жизни) старого CRL;
- `CRLOverlapUnits=1` - значение интервала перекрытия CRL;
- `LoadDefaultTemplates=0` - значение определяет, будут ли шаблоны сертификатов загружаться по умолчанию при установке корпоративного центра сертификации:

- Если значение `0`, шаблоны не загружаются;
- Если значение `1`, шаблоны загружаются.

- `AlternateSignatureAlgorithm=0` - значение управляет алгоритмом подписи сертификатов от центра сертификации:
  - Если значение `0`, будет использоваться стандартный алгоритм (обычно SHA256RSA, где сначала создается хэш SHA256, а затем применяется подпись RSA);
  - Если значение `1`, будет применяться альтернативный алгоритм для совместимости с устаревшими системами, например, SHA1RSA. Рекомендуется выбрать значение `0`, так как оно более безопасное.

CRLDistributionPoint

- `Empty=True` - исключает URL-адреса точек распространения CRL из сертификатов, выпущенных центром сертификации.

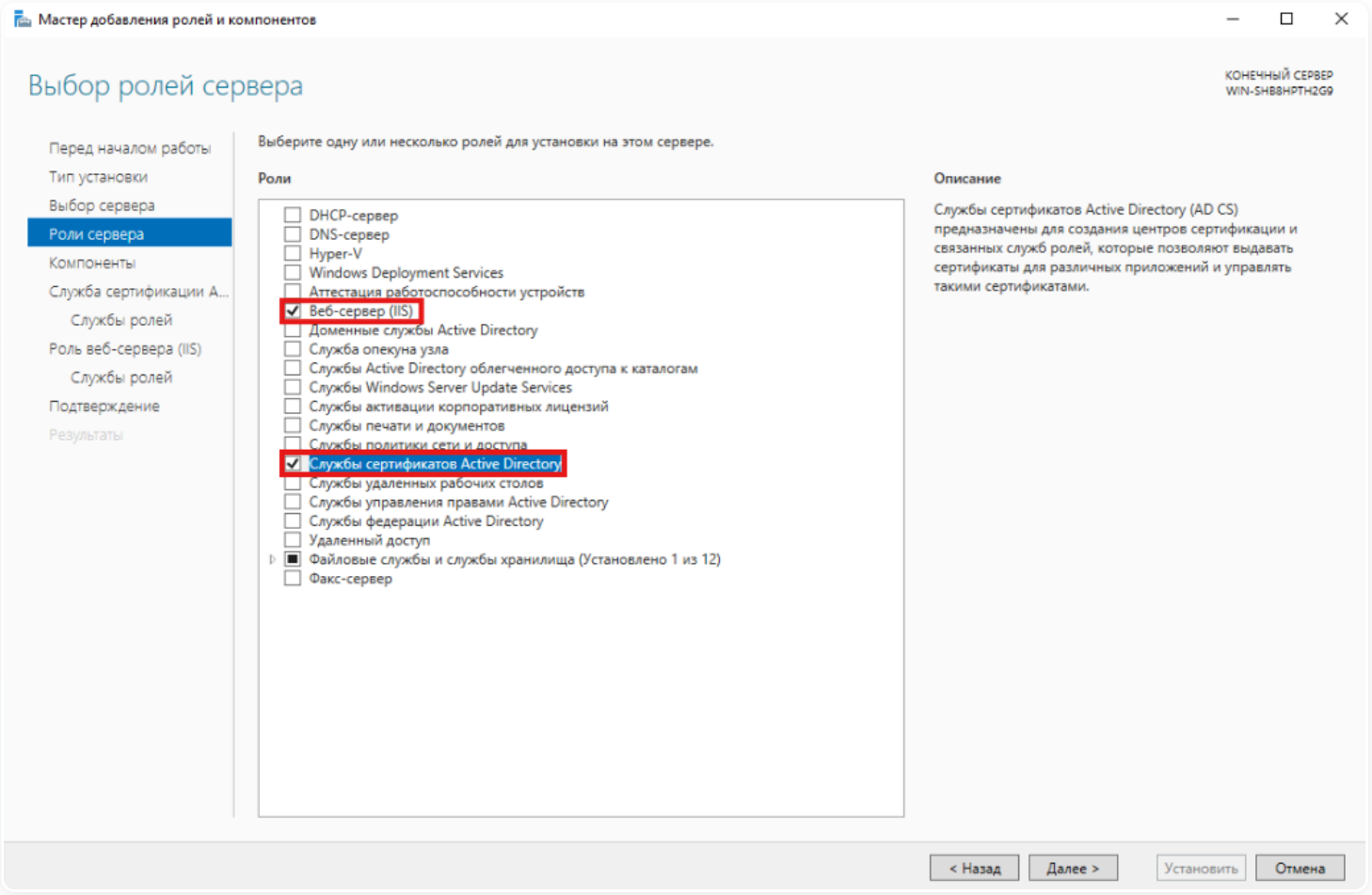
AuthorityInformationAccess

- `Empty=True` - не добавляет URL-адрес AIA в сертификаты, выданные центром сертификации.

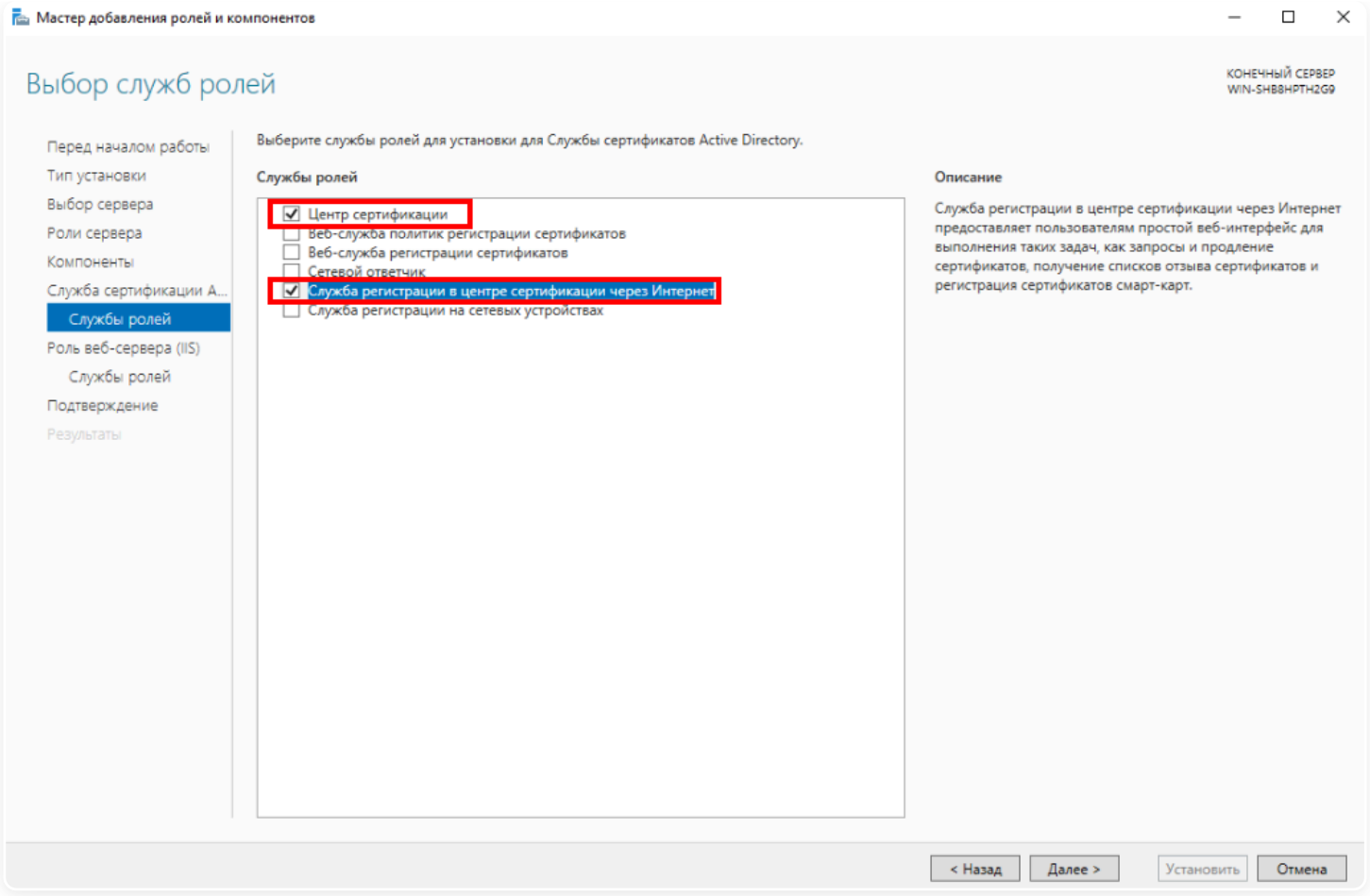
Шаг 2. Установка ролей служб сертификации

1. Откройте **Диспетчер серверов** и перейдите в **Управление** → **Добавление ролей и компонентов**.

2. На этапе **Роли сервера** выберите роль **Службы сертификатов Active Directory** и **Веб-сервер (IIS)**:



3. В окне **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:

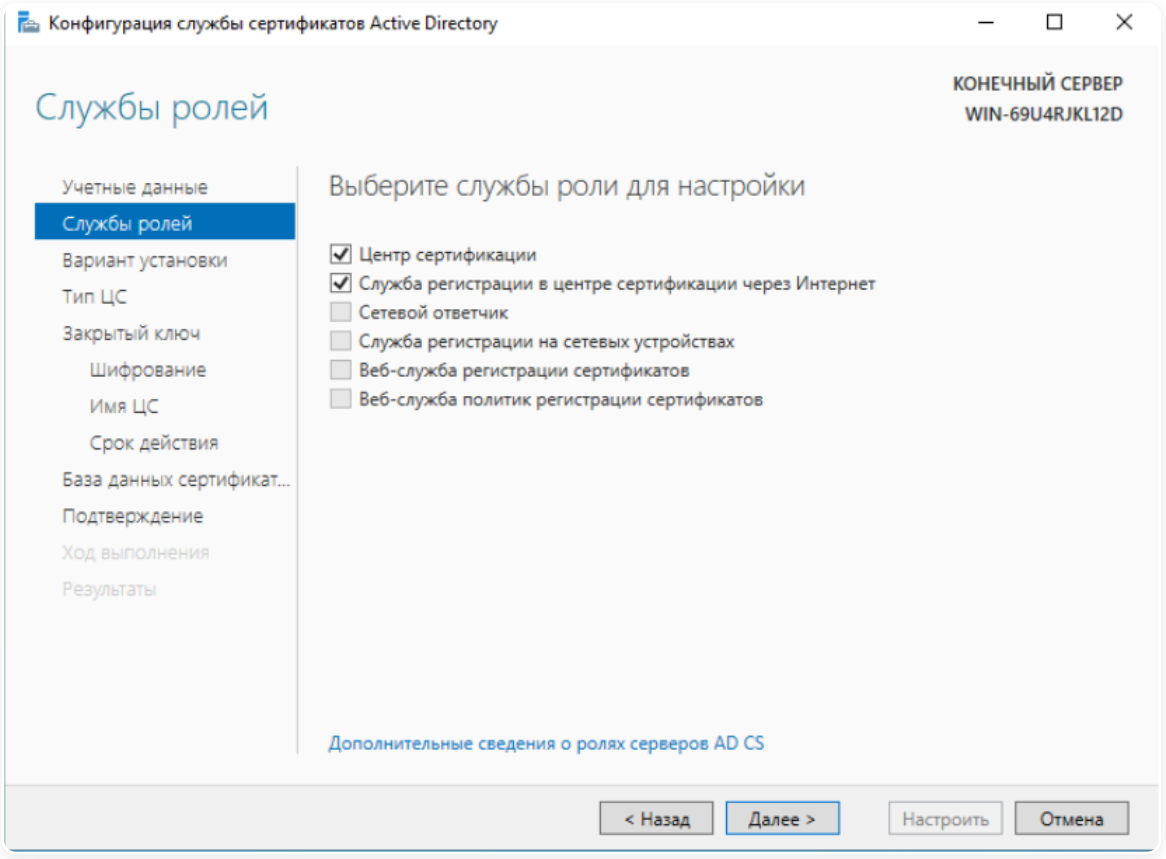


4. Завершите установку.

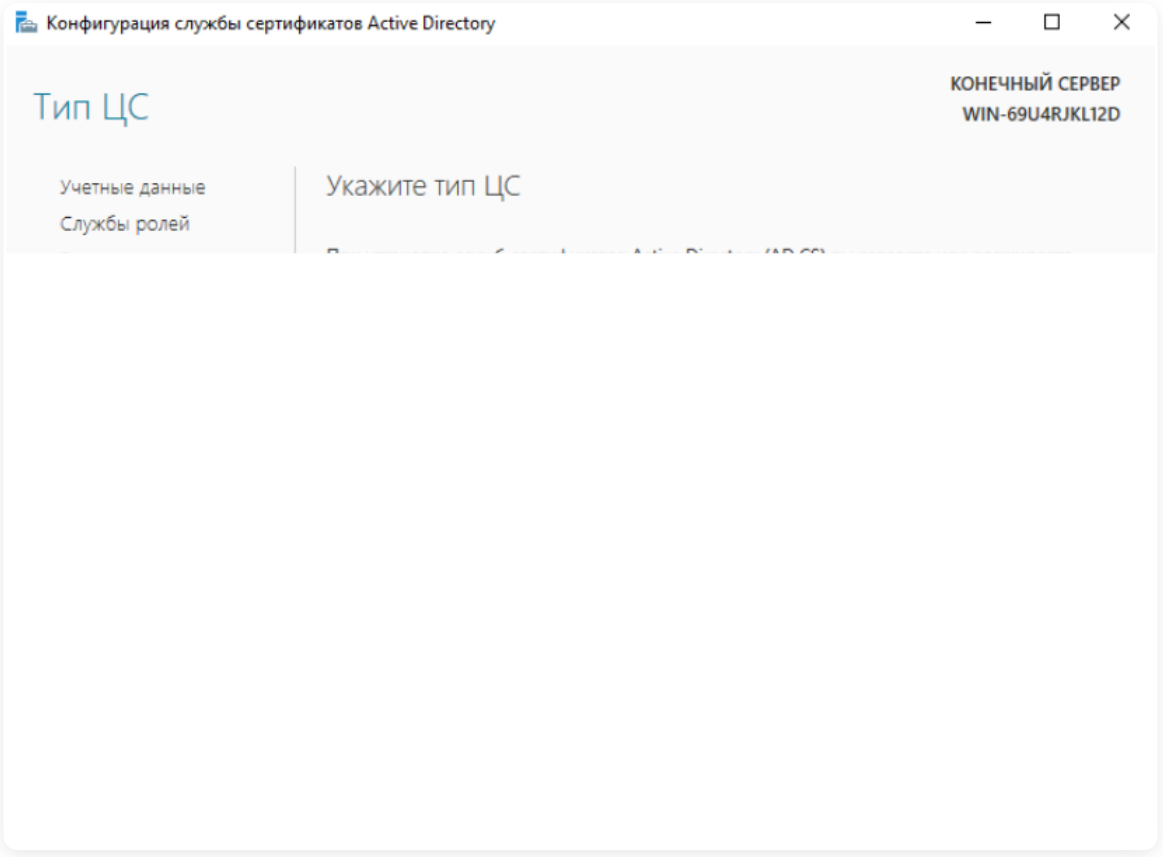
Шаг 3. Настройка служб сертификации

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

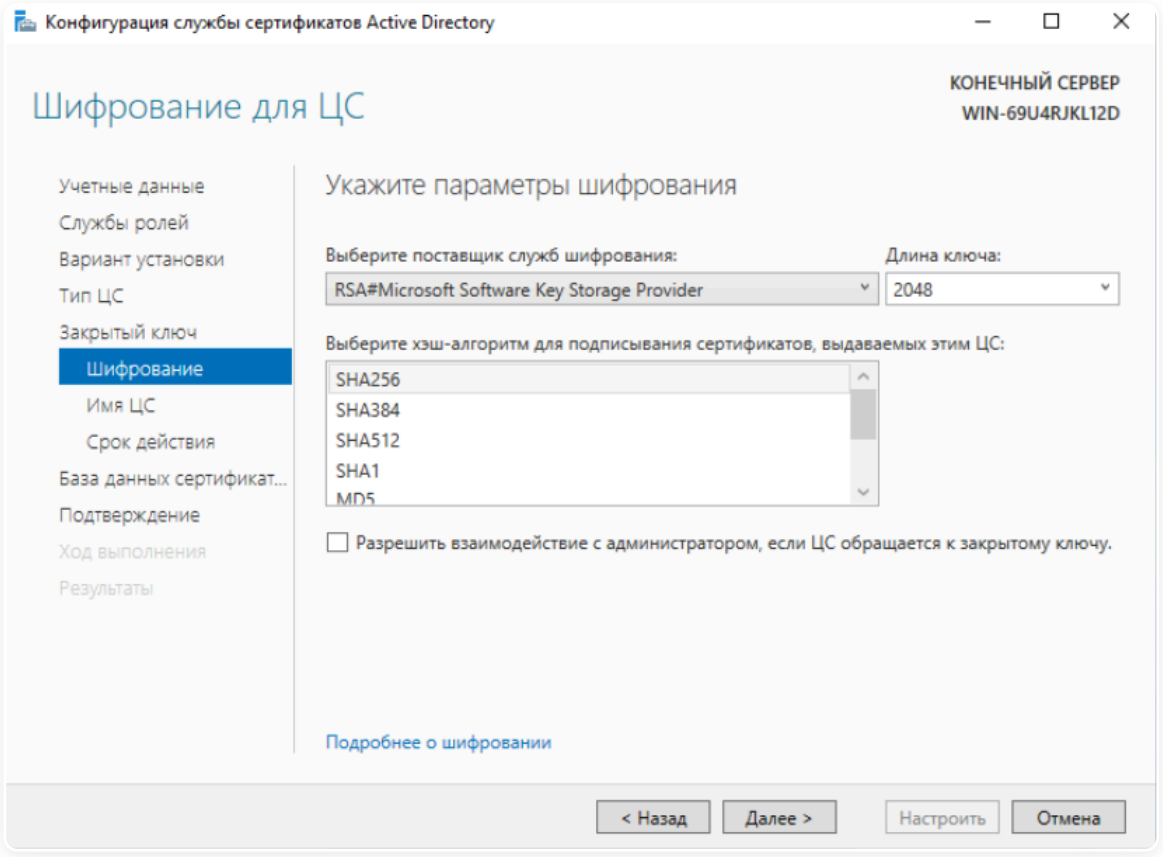
2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



3. На этапе **Тип ЦС** выберите **Корневой ЦС**:



4. На этапе **Шифрование** убедитесь, что выбран алгоритм **SHA256**:



5. На этапе **Имя ЦС** задайте имя (например, `TestRootCA`):

6. Завершите настройку:

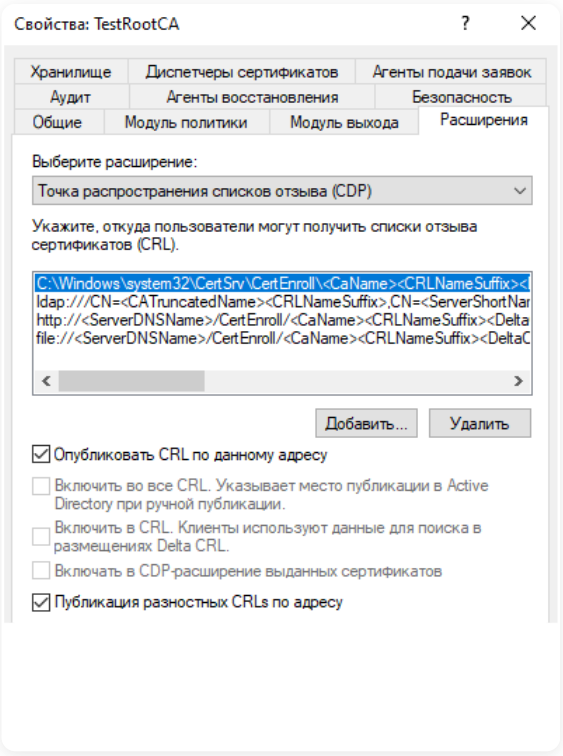
Шаг 4. Настройка точек распространения (CDP/AIA)

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**.

2. Нажмите правой кнопкой мыши по имени созданного центра сертификации `TestRootCA` и перейдите в **Свойства**.

3. На вкладке **Расширения** выберите расширение **Точка распространения списков отзыва (CDP)**.

4. Удалите пути, начинающиеся с `ldap://`, `file://` и `http://`:



5. Нажмите **Добавить** и введите URL `http://<домен-сервера>/Certs/`. Затем добавьте переменные `<CaName>`, `<CRLNameSuffix>` и `<DeltaCRLAllowed>` после `Certs/`. Конечный путь будет выглядеть так: `http://test.com/Certs/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.

6. Выберите добавленный URL и активируйте опции **Включить в CRL** и **Включать в CDP-расширение выданных сертификатов**:

7. На вкладке **Расширения** выберите расширение **Доступ к сведениям о центрах сертификации (AIA)**.

8. Удалите пути, начинающиеся с `ldap://`, `file://` и `http://`:

9. Нажмите **Добавить** и введите URL `http://<домен-сервера>/CertsAIA/`. Затем добавьте переменные `<ServerDNSName>`, `<CaName>` и `<CertificateName>` после `Certs/`. Конечный путь будет выглядеть так: `http://test.com/CertsAIA/<ServerDNSName>_<CaName><CertificateName>.crt`.

10. Выберите добавленный URL и активируйте опции **Включать в AIA-расширение выданных сертификатов**.

11. Примените изменения и перезапустите службу.

Шаг 5. Экспорт корневого сертификата

1. Откройте консоль управления. Для этого нажмите **Win + R**, введите команду `mmc` и нажмите **Enter**.

2. Перейдите в **Файл** → **Добавить или удалить оснастку**.

3. Выберите **Сертификаты** и нажмите **Добавить**.

4. Выберите опцию **учетной записи компьютера** и нажмите **Далее** → **Готово** → **ОК**.

5. Перейдите в **Сертификаты (локальный компьютер)** → **Личное** → **Сертификаты**. Нажмите правой кнопкой мыши по корневому сертификату `TestRootCA` и выберите **Все задачи** → **Экспорт**.

6. Выберите **Нет, не экспортировать закрытый ключ** и нажмите **Далее**.

7. Выберите формат **Файлы X.509 (.CER) в кодировке DER** и нажмите **Далее**.

8. Сохраните файл (например, `Root_CA.cer`) и перенесите этот файл на сервер подчиненного центра сертификации.

Настройка подчиненного центра сертификации (Subordinate CA)

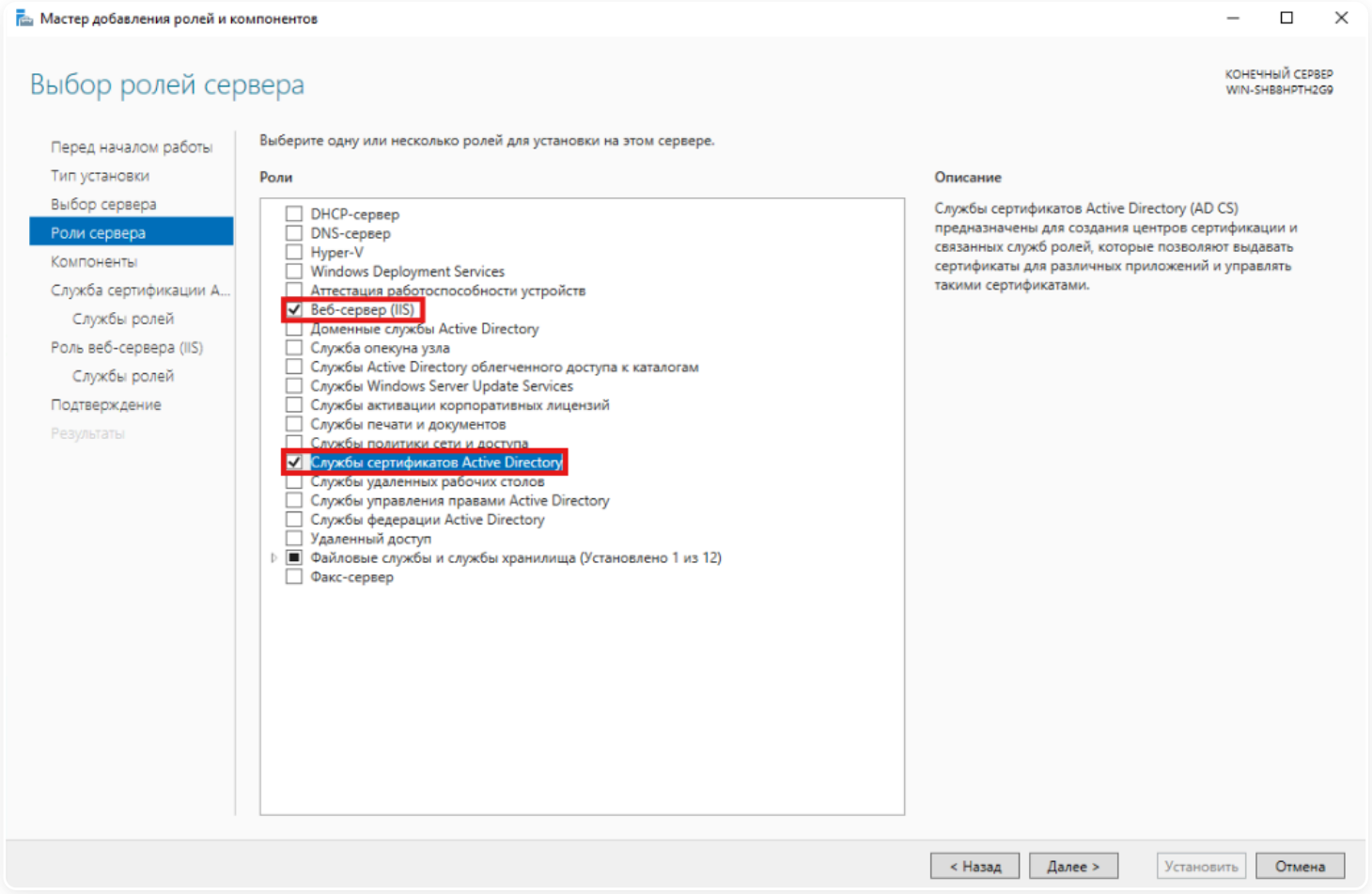
Шаг 1. Установка доверия к корню и установка ролей

На подчиненном центре сертификации (контроллере домена):

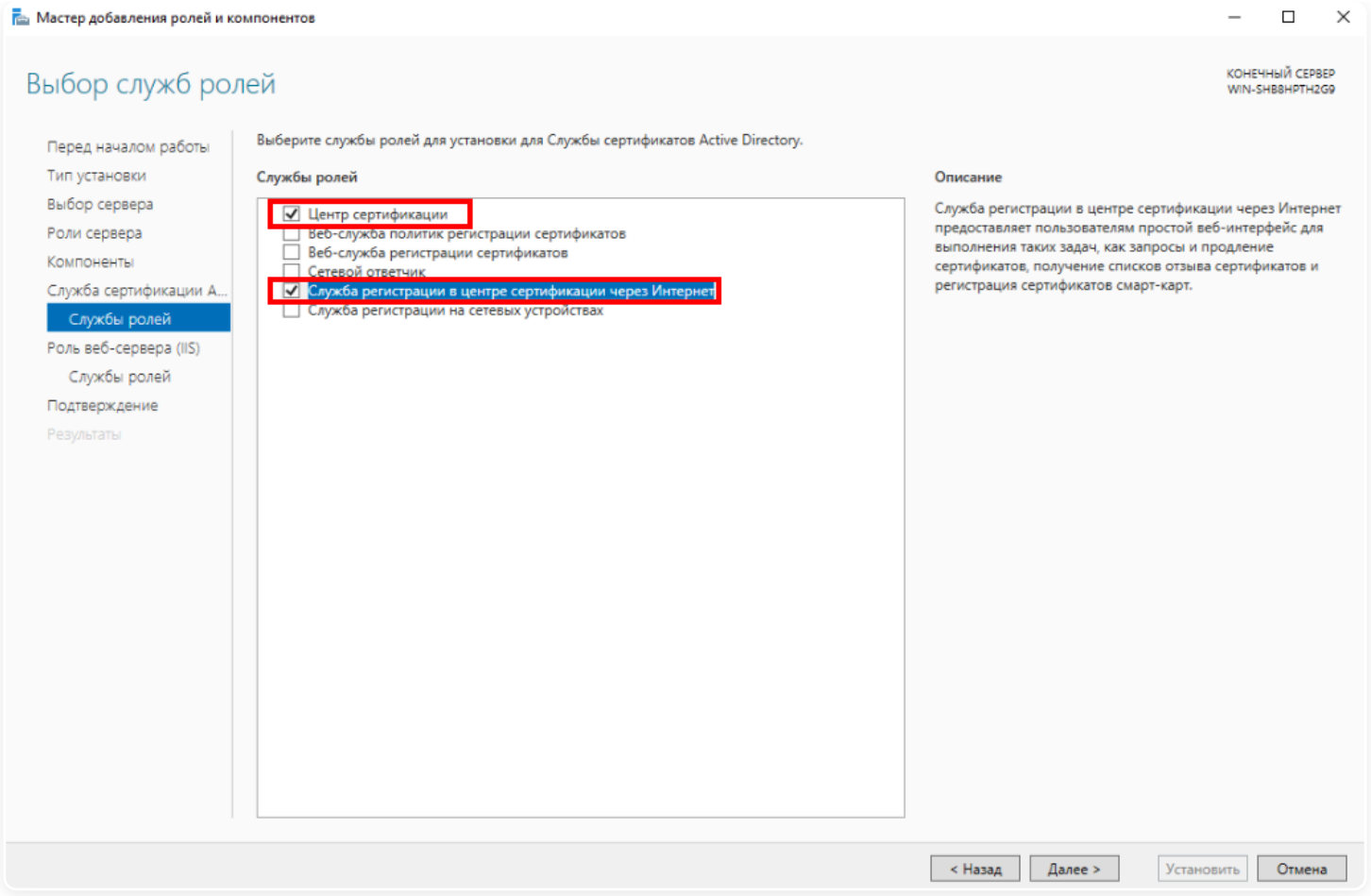
1. Установите сертификат `Root_CA.cer` в хранилище **Доверенные корневые центры сертификации** для локального компьютера.

2. Откройте **Диспетчер серверов** и перейдите в **Управление → Добавление ролей и компонентов**.

3. На этапе **Роли сервера** выберите роль **Службы сертификатов Active Directory** и **Веб-сервер (IIS)**:



4. В окне **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



5. Завершите установку.

Шаг 2. Настройка подчиненного центра сертификации и создание запроса (CSR)

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:

3. На этапе **Тип ЦС** выберите **Подчиненный ЦС**:

4. На этапе **Имя ЦС** задайте имя (например, `SubCAcert`):

5. На этапе **Запрос сертификата** сохраните запрос в файл `.req`. Скопируйте путь к файлу:

6. Завершите настройку. По завершении настройки система выдаст информационное предупреждение, которое является стандартным.

Шаг 3. Завершение настройки подчиненного центра сертификации

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. На подчиненном центре сертификации нажмите правой кнопкой мыши **Установить сертификат ЦС** и выберите скачанный файл. Установите файл в папку **Доверенные корневые центры сертификации**.

2. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на центр сертификации и выберите **Все задачи** → **Запуск службы**.

Шаг 4. Настройка IIS для публикации CRL и сертификатов

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Диспетчер служб IIS**.

2. Нажмите правой кнопкой мыши по узлу сервера, выберите **Добавить веб-сайт** и заполните поля:

- **Имя сайта** - введите `CertAU`.

- **Физический путь** - создайте новую папку `CA_site` по пути `C:\CA_site`.
- **Имя узла** - укажите доменное имя, по которому будет доступен сайт, например, `marketing.contoso.com`.

3. После добавления веб-сайта перейдите в раздел **Просмотр каталогов** и нажмите **Включить**:

4. Нажмите правой кнопкой мыши по созданному в пункте 3 веб-сайту, выберите **Добавить виртуальный каталог** и заполните поля:

- **Псевдоним** - укажите `Certs`.
- **Физический путь** - создайте новую папку `CDP` по пути `C:\CA_site\CDP`.

5. Повторите пункт 4. Создайте новый виртуальный каталог с псевдонимом `certsAIA` и укажите путь `C:\CA_site\AIA`.

6. Для каждого созданного каталога перейдите в раздел **Просмотр каталогов** и нажмите **Включить**.

7. Скопируйте файлы `.crl` и `.crt` с корневого центра сертификации в соответствующие папки на подчиненном.

8. Для сайта `CertAU` откройте раздел **Фильтрация запросов**. Выберите действие **Изменить параметры** и включите опцию **Разрешить двойное преобразование**.

Шаг 5. Настройка CDP и AIA на подчиненном центре сертификации

1. Откройте **Диспетчер серверов** и перейдите в **Средства → Центр сертификации**.

2. Нажмите правой кнопкой мыши по центру сертификации и перейдите в **Свойства**.

3. На вкладке **Расширения** удалите пути, начинающиеся с `ldap://`, `file://` и `http://`.

4. Добавьте новые пути:

- Для CDP конечный путь будет выглядеть так: `http://<домен-сервера>/Certs/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.
- Для AIA конечный путь будет выглядеть так: `http://<домен-сервера>/CertsAIA/<ServerDNSName>_<CaName><CertificateName>.crt`.

5. Выберите добавленный URL и активируйте опции:

- Для CDP: **Включить в CRL** и **Включать в CDP-расширение выданных сертификатов**.
- Для AIA: **Включать в AIA-расширение выданных сертификатов**.

Шаг 6. Получение сертификата от корневого центра сертификации

1. Откройте файл `.req` в блокноте и скопируйте текст.

2. Откройте в браузере `http://<IP-адрес-корневого-центра-сертификации>/certsrv`.

3. Перейдите в **Запросить сертификат → Расширенный запрос сертификата**:

4. Вставьте текст запроса в поле и нажмите **Выдать**:

5. В корневом центре сертификации откройте **Диспетчер серверов** и перейдите в **Средства → Центр сертификации**.

6. Перейдите в папку **Запросы в ожидании**, найдите запрос, нажмите правой кнопкой мыши **Все задачи → Выдать**.

7. С подчиненного центра сертификации вернитесь на страницу браузера `http://<IP-адрес-корневого-центра-сертификации>/certsrv`, выберите **Просмотр состояния ожидаемого запроса сертификата** и скачайте выданный сертификат.

Шаг 7. Настройка путей для публикации подчиненного центра сертификации (CRLDelta)

1. Откройте **Диспетчер серверов** и перейдите в **Средства → Диспетчер служб IIS**.

2. Создайте виртуальный каталог `subCA/CDP`. Для этого нажмите правой кнопкой мыши по веб-сайту `CertAU`, выберите **Добавить виртуальный каталог** и заполните поля:

- **Псевдоним** - укажите `subCA/CDP`.
- **Физический путь** - создайте новую папку `CDP` по пути `C:\CA_site\subCA\CDP`.

3. Повторите шаги из пункта 2 для создания виртуального каталога `subCA/AIA`:

- **Псевдоним** - укажите `subCA/AIA`.
- **Физический путь** - создайте новую папку `CDP` по пути `C:\CA_site\subCA\AIA`.

4. Откройте **Свойства** центра сертификации и на вкладке **Расширения** добавьте физические пути для публикации:

- Для CDP конечный путь будет выглядеть так: `C:\CA_site\subCA\CDP\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.
- Для AIA конечный путь будет выглядеть так: `C:\CA_site\subCA\AIA\<ServerDNSName>_<CaName><CertificateName>.crt`.

5. Выберите добавленный путь для CDP и активируйте опции **Опубликовать CRL по данному адресу** и **Публикация разностных CRL по адресу**.

6. Скопируйте сертификат подчиненного центра сертификации из папки `C:\Windows\System32\certsrv\CertEnroll` в папку `C:\CA_site\subCA\AIA`.

7. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на центр сертификации и выберите **Все задачи** → **Публикация**, чтобы обновить CRL.

Создание шаблона сертификата и тестовая выдача

Шаг 1. Создание шаблона сертификата

1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на папку **Шаблоны сертификатов** и выберите **Управление**.

2. Найдите шаблон **Пользователь**, нажмите правой кнопкой мыши и выберите **Скопировать шаблон**.

3. Настройте шаблон в соответствии с вашими требованиями (имя, срок действия, криптопровайдеры и так далее):

4. На вкладке **Безопасность** добавьте группу **Компьютеры домена** и/или **Пользователи домена** с разрешениями **Чтение** и **Заявка**:

5. Вернитесь в раздел **Центр сертификации** → **Шаблоны сертификатов**. Нажмите правой кнопкой мыши в пустой области **Создать** → **Выдаваемый шаблон сертификата** и выберите созданный шаблон.

Шаг 2. Тестовая выдача сертификата на клиентском устройстве

1. На клиентском устройстве установите корневой сертификат `Root_CA.cer` и сертификаты от подчиненного центра в хранилище **Доверенные корневые центры сертификации**.

2. Откройте консоль управления. Для этого нажмите **Win + R**, введите команду `mmc` и нажмите **Enter**.

3. Перейдите в **Файл** → **Добавить или удалить оснастку**.

4. Выберите **Сертификаты** и нажмите **Добавить**.

5. Выберите опцию **моей учетной записи компьютера** и нажмите **Готово** → **ОК**.

6. Перейдите в **Сертификаты - текущий пользователь**. Нажмите правой кнопкой мыши по папке **Личное** и выберите **Все задачи** → **Запросить новый сертификат**.

7. Выберите созданный шаблон и нажмите **Заявка**.

8. Убедитесь, что сертификат появился в личном хранилище:

Полезные ссылки

- **Active Directory/Samba DC**
- **Сертификаты**

Использование собственного CA-сертификата в Контент-фильтре

В **Контент-фильтре** возможно использование не корневого сертификата Ideco NGFW Novum, а собственного CA-сертификата. Процедура настройки такого сертификата включает этапы:

1. Генерация приватного ключа и CA-сертификата.

2. Подготовка CA-сертификата для загрузки на сервер NGFW Novum.

3. Загрузка CA-сертификата на сервер NGFW Novum.

4. Установка CA-сертификата на устройство пользователя.

Шаг 1. Генерация приватного ключа и CA-сертификата

1. Сгенерируйте приватный ключ корневого сертификата без применения **passphrase**, фразы-пароля:

```
openssl genrsa -aes256 -out ideco-cf_root-ca.key 4096
```

- `-aes256` - приватный ключ зашифрован алгоритмом AES-256;
- `ideco-cf_root-ca.key` - название файла, содержащего приватный ключ.

2. Сгенерируйте корневой сертификат, используя приватный ключ корневого сертификата:

```
openssl req -x509 -new -sha256 -days 1825 -key ideco-cf_root-ca.key -out ideco-cf_root-ca.pem
```

- `-sha256` - использование алгоритма SHA256 при создании сертификата;
- `-days 1825` - срок действия сертификата в днях;
- `ideco-cf_root-ca.key` - название файла, содержащего приватный ключ сертификата;
- `ideco-cf_root-ca.pem` - название файла, содержащего сам сертификат.

3. Заполните параметры сертификата:

```
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Moscow
Locality Name (eg, city) [Default City]:Moscow
Organization Name (eg, company) [Default Company Ltd]:Test
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:MyName
Email Address []:test@ideco.ru
```

Расшифровка строк

- `Country Name (2 letter code) [XX]` - код страны в формате ISO 3166-1 alpha-2 (например, `RU`).
- `State or Province Name (full name) [Some-State]` - название региона или области (например, `Moscow`).
- `Locality Name (eg, city) [Default City]` - название города (например, `Saint Petersburg`).
- `Organization Name (eg, company) [Internet Widgits Pty Ltd]` - название организации.
- `Organizational Unit Name (eg, section) []` - название подразделения организации.
- `Common Name (e.g. server FQDN or YOUR name) []` - наименование сертификата, например `Ideco`.
- `Email Address []` - контактный email.

Дополнительные атрибуты:

- **A challenge password []** - пароль для дополнительной аутентификации. Поле должно быть пустым.
- **An optional company name []:** - полное юридическое название организации.

4. Проверьте, что сертификат был успешно создан:

```
openssl x509 -text -noout -in ideco-cf_root-ca.pem
```

Требования к CA-сертификату:

- Должен иметь атрибут `CA:TRUE`.
- Для RSA длина ключа должна быть не менее 1024 бит. Рекомендуем использовать длину ключа не менее 2048 бит.

После генерации вы должны получить ключ и сертификат в файлах:

- `ideco-cf_root-ca.key` - файл, содержащий приватный ключ сертификата;
- `ideco-cf_root-ca.pem` - файл, содержащий CA-сертификат.

Шаг 2. Подготовка сертификата для загрузки на сервер

Для корректной загрузки на сервер Ideco NGFW Novum CA-сертификат нужно собрать в один файл, называемый бандлом, в правильном порядке. Структура файла должна содержать два блока - **Приватный ключ** и **CA-сертификат**.

Для создания бандла выполните действия:

1. Создайте текстовый файл вида:

```
-----BEGIN PRIVATE KEY-----
.....
.....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
```

2. Добавьте в блок `BEGIN PRIVATE KEY` приватный ключ.

3. В блок `BEGIN CERTIFICATE` добавьте сгенерированный CA-сертификат. Файл бандла должен получить такую структуру:

```
-----BEGIN PRIVATE KEY-----
Приватный ключ
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
CA-сертификат
-----END CERTIFICATE-----
```

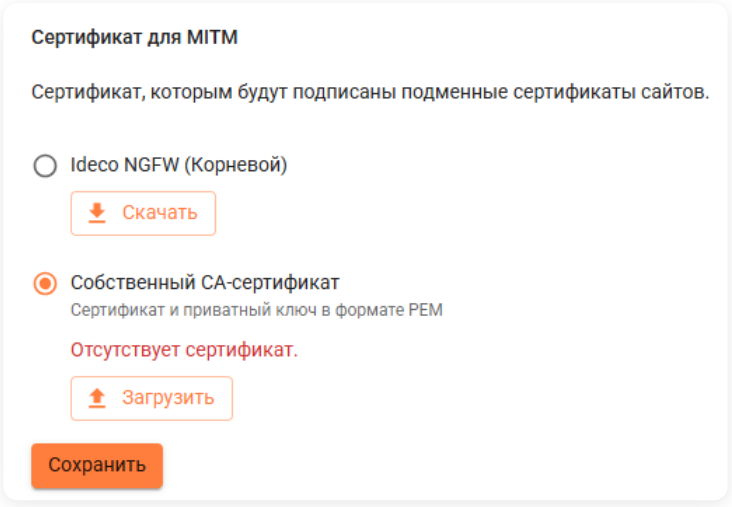
4. Сохраните файл бандла с именем, отличным от PEM-файла CA-сертификата, и расширением **.pem**, например, `ideco-cf_root-ca-key.pem`.

Шаг 3. Загрузка сертификата на сервер

Загрузите файл бандла на Ideco NGFW Novum. Для этого:

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Настройки**.

2. В поле **Сертификат для MITM** выберите опцию **Собственный CA-сертификат**:



3. Нажмите **Загрузить** и выберите созданный файл бандла `ideco-cf_root-ca-key.pem`.

Шаг 4. Установка CA-сертификата на устройство пользователя

На устройства пользователей необходимо установить только CA-сертификат, без приватного ключа.

Установите на устройства пользователей файл CA-сертификата (без приватного ключа), в нашем примере `ideco-cf_root-ca.pem`. Варианты установки:

Установка CA-сертификата вручную

Установка сертификата на Linux

Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

Установка сертификата на Windows

1. Откройте на рабочей станции центр управления сертификатами: **Пуск** → **Выполнить**, введите **mmc** и нажмите **Enter**:

2. В меню **Файл** выберите **Добавить или удалить оснастку**:

3. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите **Добавить**:

4. В открывшемся окне выберите пункт **Учетной записи компьютера** и нажмите **Далее**:

5. В окне **Выбор компьютера** оставьте флаг **Локальный компьютер** и нажмите **Готово**.

6. В левой части окна нажмите на стрелку рядом с директорией **Сертификаты (локальный компьютер)** → **Доверенные корневые сертификаты** → **Сертификаты**:

7. В меню **Действие** выберите **Все задачи** → **Импорт**:

8. Следуя инструкциям **Мастера импорта сертификатов**, импортируйте CA-сертификат. Импортированный сертификат появится в списке в правой части окна:

Автоматическая установка CA-сертификата через Active Directory

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, можно установить сертификат Ideco NGFW Novum для всех пользователей автоматически:

1. Зайдите на контроллер домена с правами администратора.

2. Запустите оснастку **Управление групповой политикой**, выполнив команду **gpmc.msc**.

3. Найдите **политику домена**, использующуюся на компьютерах пользователей в **Объектах групповой политики** (Default Domain Policy). Нажмите на нее правой кнопкой мыши и выберите **Изменить**:

4. В открывшемся редакторе управления групповыми политиками выберите: **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Политики открытого ключа** → **Доверенные корневые центры сертификации**.

5. Нажмите правой кнопкой мыши по открывшемуся списку, выберите **Импорт** и импортируйте ключ Ideco NGFW Novum:

6. После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Полезные ссылки

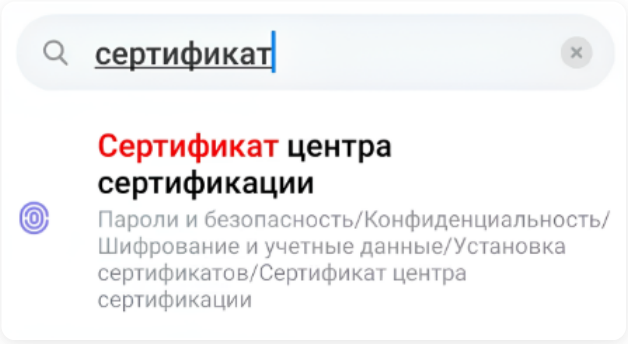
- **Настройка фильтрации HTTPS**
- **Сертификаты**

Как установить сертификат Ideco NGFW Novum на Android

1. Скачайте сертификат Ideco NGFW Novum на Android-устройство.

2. Перейдите в **Настройки**.

3. В поиске введите `Сертификат`:

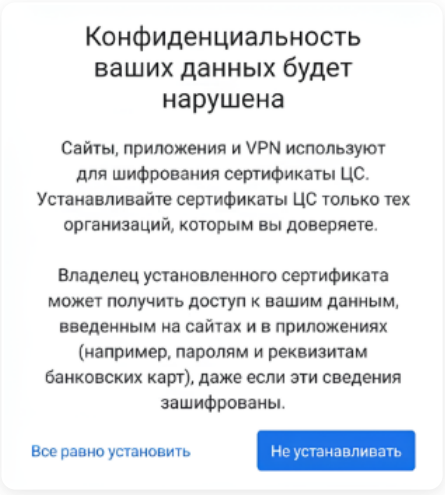


4. Выберите **Сертификат центра сертификации**.

> В зависимости от версии Android и версии оболочки путь может отличаться. Ориентируйтесь на расположение **Пароли и безопасность/ Конфиденциальность/Шифрование и учетные данные**.

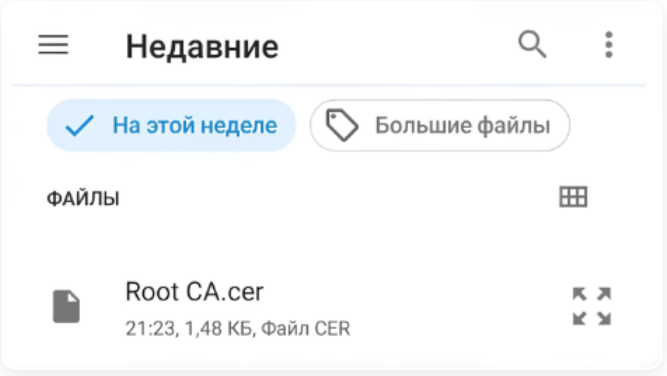
5. Если появится окно **Укажите название сертификата**, введите удобное вам название.

6. Выберите **Сертификат центра сертификации** и нажмите **ОК**. Если откроется предупреждение, нажмите **Все равно установить** или **Установить в любом случае**:



7. Введите пароль или PIN-код от устройства. Нажмите **Подтвердить**.

8. В загрузках выберите скачанный сертификат `Root CA.cer`:



После установки в нижней части экрана появится уведомление **Сертификат установлен**.

Полезные ссылки

- **Сертификаты**

Настройка прозрачной авторизации на Astra Linux

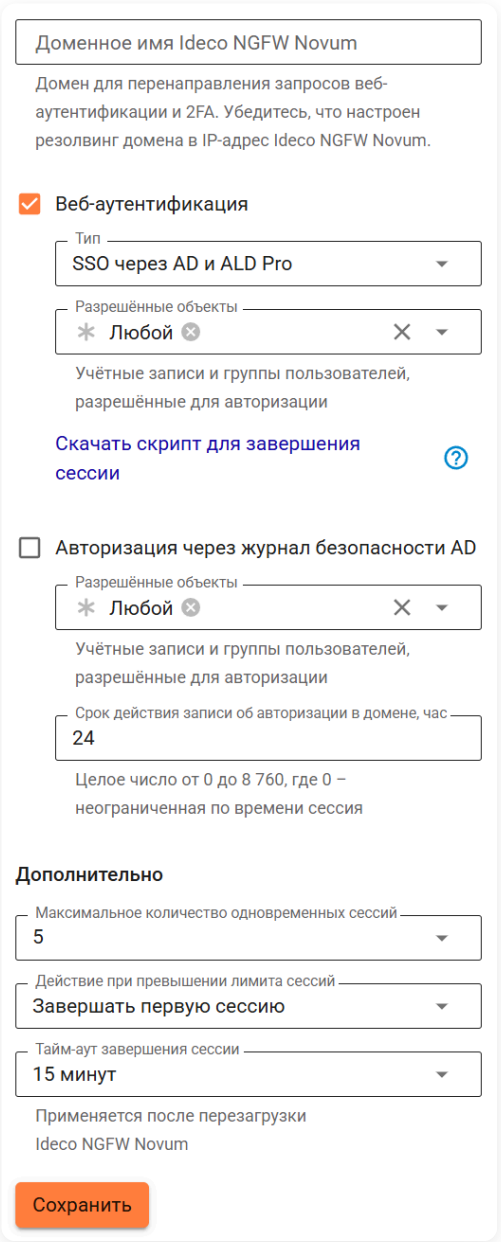
Решение подходит для браузеров **Yandex**, **Chromium** и **Firefox.**

1. Установите и настройте NGFW на устройстве администратора, получите лицензию.

2. Введите Astra Linux в домен (например, через Active Directory).

3. Введите NGFW в домен, что и Astra Linux, и импортируйте пользователей (в том числе Astra Linux) в группу.

4. Выберите **SSO через AD и ALD Pro** на вкладке **Пользователи** → **Авторизация** → **Настройки** в Ideco NGFW Novum:



5. Зайдите под доменной учетной записью на Astra Linux.

6. В зависимости от выбранного браузера, выполните действия:

Для браузера Yandex

1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и впишите в него строку:

```
{
  "AuthServerAllowlist": "имя_NGFW.имя_домена",
  "AuthNegotiateDelegateAllowlist": "имя_NGFW.имя_домена"
}
```

2. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.

Для браузера Chromium

1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и впишите в него строку:

```
{
    "AuthServerAllowlist": "имя_NGFW.имя_домена" ,
    "AuthNegotiateDelegateAllowlist": "имя_NGFW.имя_домена"
}
```

2. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.

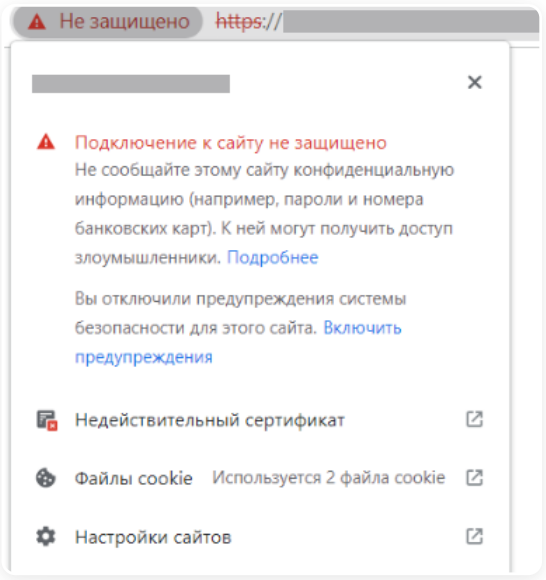
Для браузера Firefox

1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

2. Введите параметр `security.enterprise_roots.enabled` и дважды кликните по блоку, чтобы значение изменилось на **True**, что позволит Firefox доверять системным сертификатам и авторизовывать пользователей при переходе на HTTPS-сайты.

3. В параметрах `network.automatic-ntlm-auth.trusted-uris` и `network.negotiate-auth.trusted-uris` укажите `имя_NGFW.имя_домена`.

4. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.
7. При возникновении проблемы с доверенным сертификатом установите корневой сертификат NGFW. Пример проблемы:

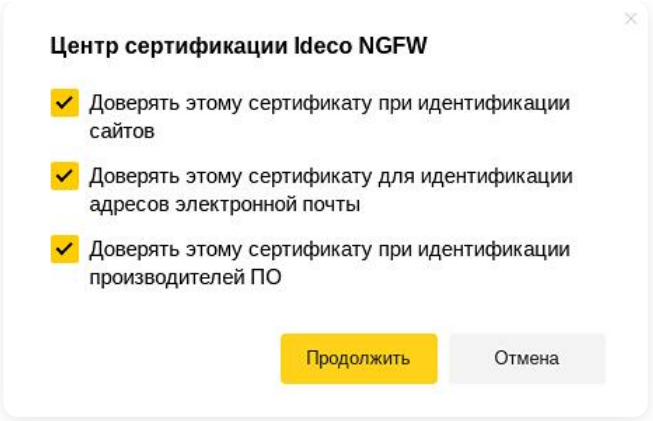


Для браузера Yandex

1. Скачайте корневой сертификат.

2. В браузере Yandex перейдите в **Настройки** → **Системные** → **Управление сертификатами** → **Центры сертификации** → **Импорт** и добавьте сертификат в список доверенных.

3. Включите опции доверия для сертификата:

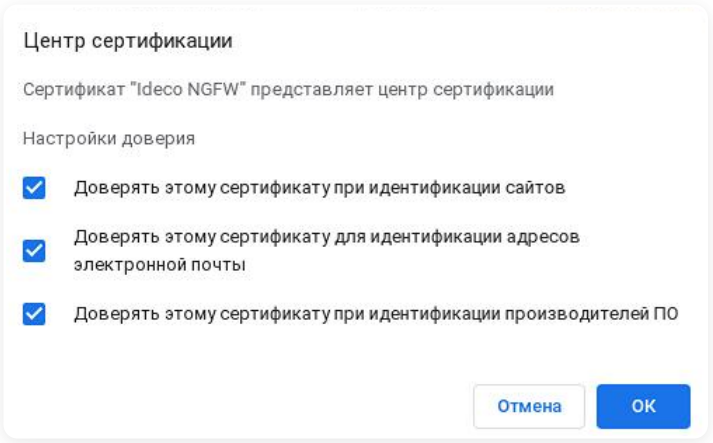


Для браузера Chromium

1. Скачайте корневой сертификат.

2. В браузере Chromium перейдите в **Настройки** → **Конфиденциальность и безопасность** → **Безопасность** → **Настроить сертификаты** → **Центры сертификации** → **Импортировать** и добавьте сертификат в список доверенных.

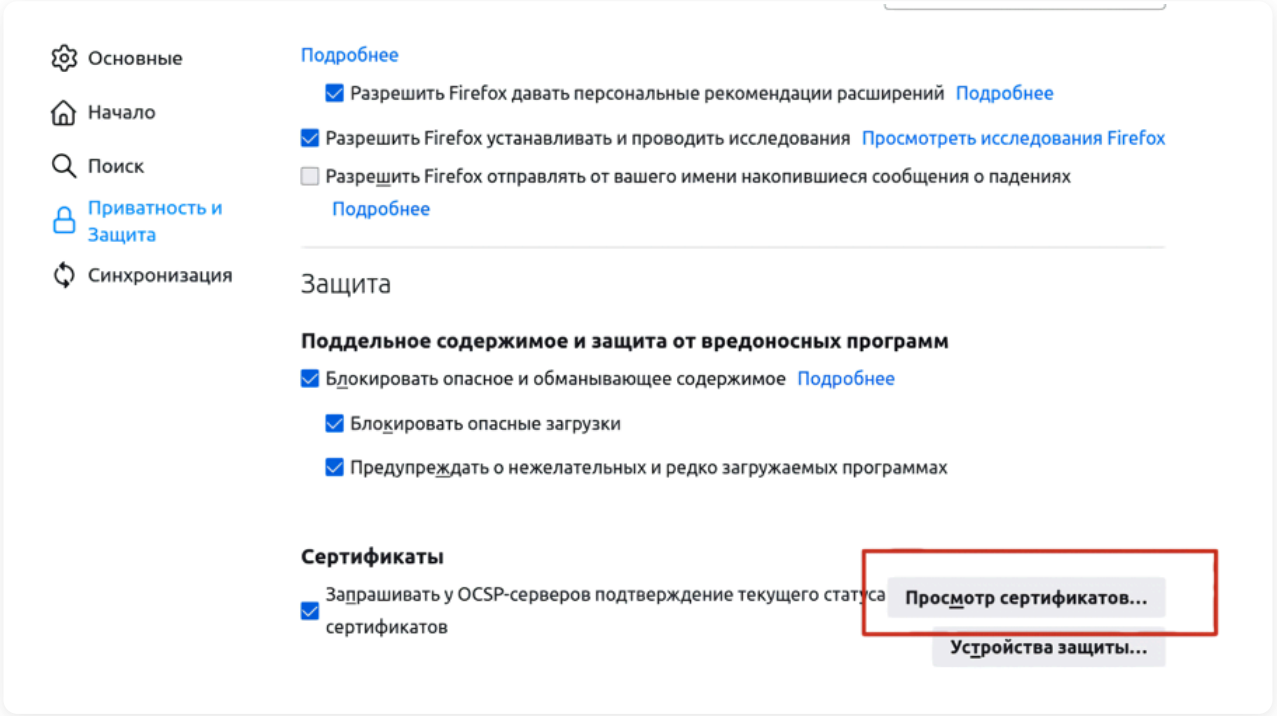
3. Включите опции доверия для сертификата:



Для браузера Firefox

1. Скачайте корневой сертификат.

2. В настройках браузера Mozilla Firefox в пункте **Приватность и Защита** в разделе **Защита** выберите **Просмотр сертификатов**:



3. На вкладке **Центры сертификации** нажмите **Импортировать** и выберите скачанный с NGFW сертификат.

4. Отметьте пункт **Доверять при идентификации веб-сайтов** и подтвердите.

Полезные ссылки

- **Авторизация**
- **Веб-аутентификация**

Настройка автоматической веб-аутентификации на Ideco NGFW Novum на Linux

Для настройки автоматической аутентификации выполните действия:

1. Перейдите в домашнюю директорию пользователя (Home) и включите отображение скрытых файлов.

2. Перейдите в папку `.config` и создайте там каталог `ideco-utm`.

3. Скачайте корневой сертификат NGFW. Подробнее в статье и поместите сертификат в каталог, созданный на предыдущем шаге.

4. Создайте в папке `ideco-utm` файл `auth.conf`. Откройте его, введите логин и пароль пользователя по образцу:

```
login=логин_пользователя
password=пароль_пользователя
```

5. Скачайте скрипт на компьютер пользователя, перейдя по ссылке, и настройте автозагрузку в соответствии с описанным ниже алгоритмом. Чтобы сохранить файл, кликните правой кнопкой мыши в любом месте страницы и выберите пункт **Сохранить как**.

Для корректной работы скрипта имя корневого сертификата должно быть `root_ca.crt`.

Настройка автозагрузки скрипта

Для настройки выясните возможность добавления приложений в автозагрузку через графический интерфейс. При отсутствии такой возможности настройте автозагрузку через терминал.

Для настройки через терминал потребуются права администратора.

Настройка через терминал

Если сделать скрипт исполняемым файлом с помощью команды `chmod +x <путь до скрипта>`, можно не указывать путь до python.

1. Откройте терминал и введите команду:

```
sudo nano /etc/systemd/system/auto-authorization.service
```

2. Заполните файл следующим образом:

```
[Unit]
Description=Auto-Authorization

[Service]
Type=simple
User=имя_пользователя_в_системе
ExecStart=полный_путь_до_python полный_путь_до_скрипта --check-timeout=60

[Install]
WantedBy=multi-user.target
```

Введите имя пользователя Linux и полный путь до скрипта.

3. Сохраните файл и выйдите из редактора.

4. Добавьте службу в автозагрузку командой `systemctl enable auto-authorization`.

Скрипт поддерживает множество ключей, с помощью которых можно менять путь к файлам и другие параметры. Для вывода справки утилиты используйте ключ `-h`.

Для проверки статуса ранее настроенной службы введите `systemctl status auto-authorization.service`

Проверить работу настройки можно с помощью интерфейса Ideco NGFW Novum. Зайдите в раздел **Мониторинг** → **Сессии пользователей** и завершите сессию пользователя, для которого настраивалась автоматическая аутентификация. Чтобы удалить авторизованную сессию, нажмите на соответствующую пиктограмму и подтвердите выбор.

Если выйти из сессии на устройстве пользователя и повторно открыть браузер, то запрос на авторизацию не должен появиться.

Полезные ссылки

- **Веб-аутентификация**

Как безопасно подключить удаленного подрядчика

> Статья описывает полный цикл настройки Ideco NGFW Novum для безопасного подключения внешнего подрядчика к внутренним ресурсам компании. Конфигурация строится по принципу минимально необходимого доступа и охватывает сетевую изоляцию, аутентификацию, проверку устройства и аудит сессий.

Пример. Финансовый отдел компании привлекает внешнего подрядчика для работы в системе 1С. Подрядчик должен подключаться удаленно к RDP-серверу финансового отдела, на котором развернута 1С, до завершения контракта. Задача администратора - предоставить строго ограниченный доступ и обеспечить контроль подключения на каждом уровне.

Требования к безопасности:

- Доступ только к RDP-серверу финансового отдела с системой 1С.
- Доступ исключительно по протоколу RDP (порт 3389). Весь остальной трафик запрещен через **Межсетевой экран** и модуль **Контроль приложений**.
- Аутентификация через Ideco Client: логин/пароль и обязательная двухфакторная аутентификация (MFA).
- Подключение разрешено только с территории России и только в рабочее время (с 09:00 до 18:00 по будням).
- Устройство подрядчика должно соответствовать требованиям: Windows 11, активный антивирус Касперского.
- Постоянный контроль защищенности точки подключения: проверка IPS на RDP-уязвимости.
- Подрядчик не должен иметь доступа к смежным сегментам сети (другие отделы, внутренняя инфраструктура) для исключения горизонтального перемещения в случае компрометации доступа.
- Полная запись всех сессий подрядчика для последующего аудита.
- Автоматическое отключение сессии по истечении рабочего времени или времени бездействия.
- Запрет split-tunneling: трафик подрядчика в интернет не должен проходить через корпоративные ресурсы.
- Доступ предоставляется на ограниченный срок с ручным отключением учетной записи по его истечении.

Модель угроз

Таблица описывает потенциальные угрозы при подключении удаленного подрядчика и механизмы защиты от каждой из них.

Вектор угрозы	Описание	Механизм защиты
Несанкционированный доступ к смежным сегментам сети	Подрядчик получает доступ к ресурсам за пределами RDP-сервера финансового отдела	Правила FORWARD в **Межсетевом экране**: разрешен только трафик к IP-адресу RDP-сервера по порту 3389. Запрещающее правило блокирует весь остальной трафик
Использование протоколов, отличных от RDP	Попытка передачи данных через HTTP, SSH, SMB и другие протоколы	Профиль **Контроля приложений** запрещает все протоколы, кроме RDP
Эксплуатация RDP-уязвимостей	Атака на RDP-сервер через известные уязвимости (BlueKeep, DejaBlue и другие)	Профиль **Предотвращения вторжений** с включенными группами сигнатур для RDP-уязвимостей и атак на получение привилегий
Компрометация учетных данных	Перехват или подбор логина и пароля	Двухфакторная аутентификация (TOTP-токен) при подключении через Ideco Client
Подключение с зараженного устройства	Устройство без антивируса или с устаревшими базами используется как точка входа в сеть	HIP-профиль в правиле доступа по VPN проверяет наличие Windows 11 и активного антивируса Касперского. Устройства, не прошедшие проверку, блокируются при подключении
Подключение из-за пределов России	Попытка подключения из нетипичной геолокации, указывающая на компрометацию учетной записи	GeoIP-фильтрация в правиле **Межсетевого экрана**: разрешены подключения только с территории России
Подключение в нерабочее время	Несанкционированная активность вне контролируемого периода	Поле **Время действия** в правиле **Межсетевого экрана** ограничивает доступ рабочими часами (09:00-18:00, будни) на основе объекта временного интервала
Утечка данных через интернет	Подрядчик пытается передать корпоративные данные через интернет-ресурсы, используя VPN-туннель	Запрет split-tunneling: в правиле передачи маршрутов указана только подсеть RDP-сервера, интернет-трафик подрядчика не маршрутизируется через NGFW Novum
Сохранение доступа после завершения контракта	Учетная запись остается активной после окончания срока работ	Ручное включение опции **Запретить доступ** в карточке пользователя по завершении контракта. Чек-лист завершения работ

Настройка в Ideco NGFW Novum

Подрядчик подключается к NGFW Novum из внешней сети через Ideco Client. NGFW Novum выполняет аутентификацию, проверяет устройство по **HIP-профилю** и применяет правила **Межсетевого экрана**. Трафик подрядчика проходит через профили **Контроля приложений** и **Предотвращения вторжений**, после чего маршрутизируется к RDP-серверу финансового отдела.

Пример адресации:

- Внешний IP-адрес Ideco NGFW Novum - `203.0.113.1`.
- Пул VPN-адресов Ideco Client - `10.128.0.0/16` (по умолчанию).
- RDP-сервер финансового отдела (1С) - `192.168.10.50`.
- Порт RDP - `3389/TCP`.

Задействованные модули NGFW Novum

Настройка безопасного доступа для подрядчика выполняется с помощью модулей:

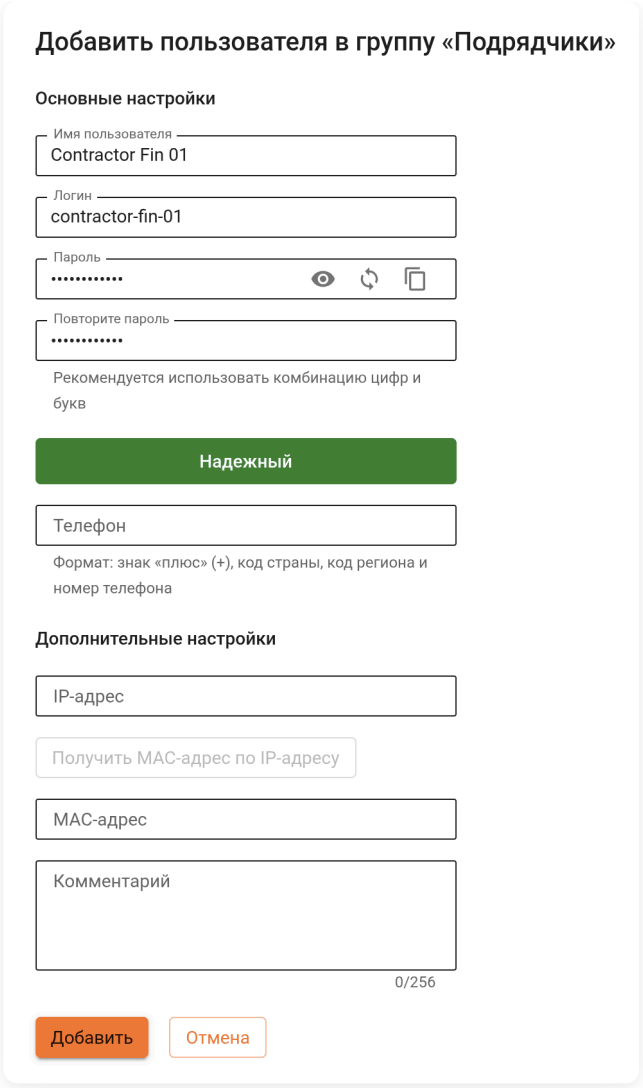
- **Ideco Client** - VPN-клиент для подключения подрядчика к NGFW Novum. Обеспечивает шифрованный туннель и передает информацию о состоянии устройства для проверки HIP-профилем.
- **Двухфакторная аутентификация (TOTP-токен)** - второй фактор при подключении через Ideco Client. Подрядчик вводит одноразовый код из приложения-аутентификатора.
- **Межсетевой экран (FORWARD)** - правила, ограничивающие доступ подрядчика одним IP-адресом и одним портом. GeoIP-фильтрация и ограничение по времени действия применяются в этих же правилах.
- **Профиль контроля приложений** - разрешает только протокол RDP.
- **Профиль предотвращения вторжений** - анализирует трафик подрядчика на предмет эксплойтов и RDP-уязвимостей.
- **HIP-профиль (профиль устройства)** - проверяет соответствие устройства подрядчика требованиям: операционная система Windows 11 и активный антивирус Касперского. Назначается в правиле доступа по VPN и блокирует подключение при несоответствии.
- **Логирование** - запись сессий подрядчика в журналы NGFW Novum для аудита.
- **Syslog** - передача журналов в SIEM-систему для долгосрочного хранения и анализа.

Создание учетной записи подрядчика

1. Перейдите в **Пользователи** → **Учетные записи**.

2. Выберите группу **Все локальные** в дереве пользователей. Нажмите на  для создания группы, введите название **Подрядчики** и нажмите **Добавить**.

3. Выберите созданную группу **Подрядчики** в дереве пользователей. На вкладке **Основное** нажмите **Создать пользователя** и заполните поля:



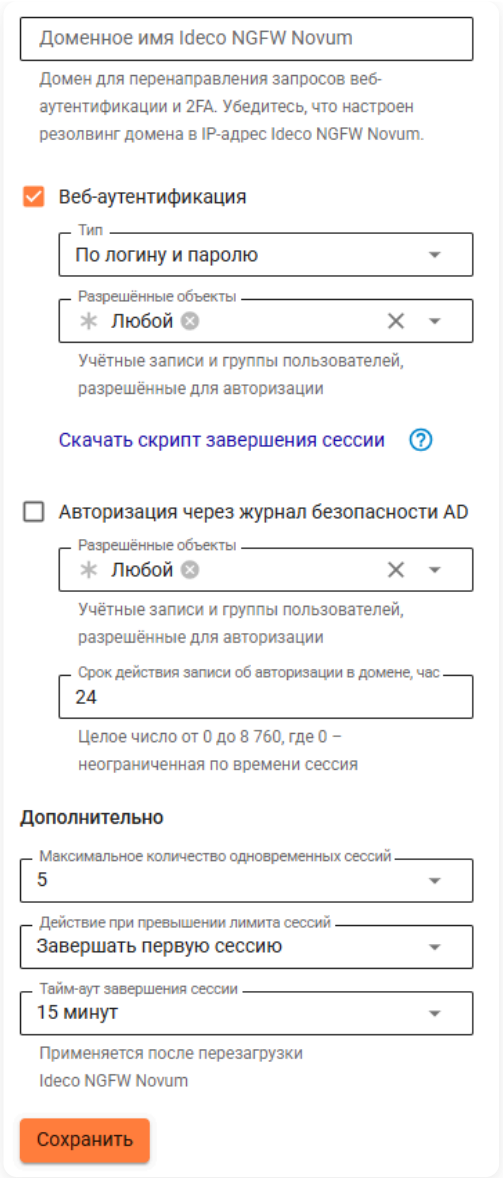
- **Имя пользователя** - введите отображаемое имя. Например, `Contractor Fin 01`.
- **Логин** - укажите логин. Например, `contractor-fin-01`.
- **Пароль** и **Повторите пароль** - задайте сложный пароль длиной не менее 12 символов.

4. Нажмите **Добавить**.

> По завершении контракта включите опцию **Запретить доступ** в карточке пользователя - это заблокирует учетную запись немедленно.

Настройка двухфакторной аутентификации

1. Перейдите в **Пользователи** → **Авторизация** и убедитесь, что опция **Веб-аутентификация** включена:



2. Укажите доменное имя Ideco NGFW Novum в поле **Доменное имя Ideco NGFW Novum**, чтобы на сервер перенаправлялись запросы двухфакторной аутентификации.

3. Перейдите в **Пользователи** → **Аутентификация** → **Двухфакторная аутентификация**.

4. Включите опцию **TOTP-токен**.

5. Включите опцию **Разрешить инициализацию секретного ключа из внешних сетей**, если подрядчик будет генерировать QR-код из внешней сети.

6. Нажмите **Сохранить**.

Создание HIP-профиля для проверки устройства подрядчика

HIP-профили позволяют задать критерии проверки устройств, подключающихся через Ideco Client. Для подрядчика настройте проверку операционной системы и антивируса.

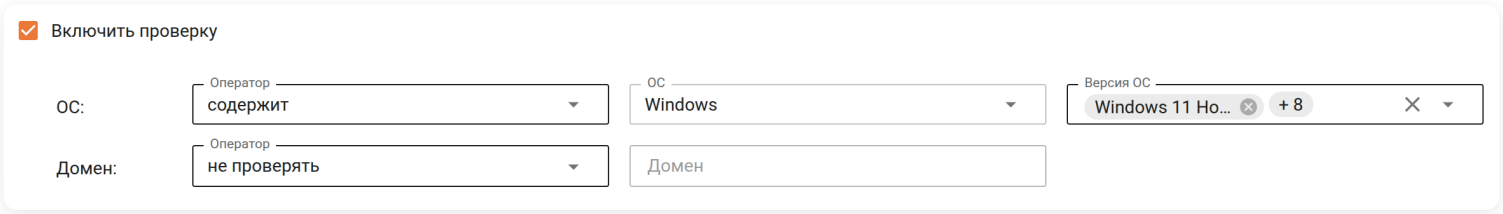
Создание HIP-объекта

1. Перейдите в **Пользователи** → **Профили устройств** → **HIP-объекты** и нажмите **Добавить**.

2. Введите название. Например, `Contractor-Device-Requirements`.

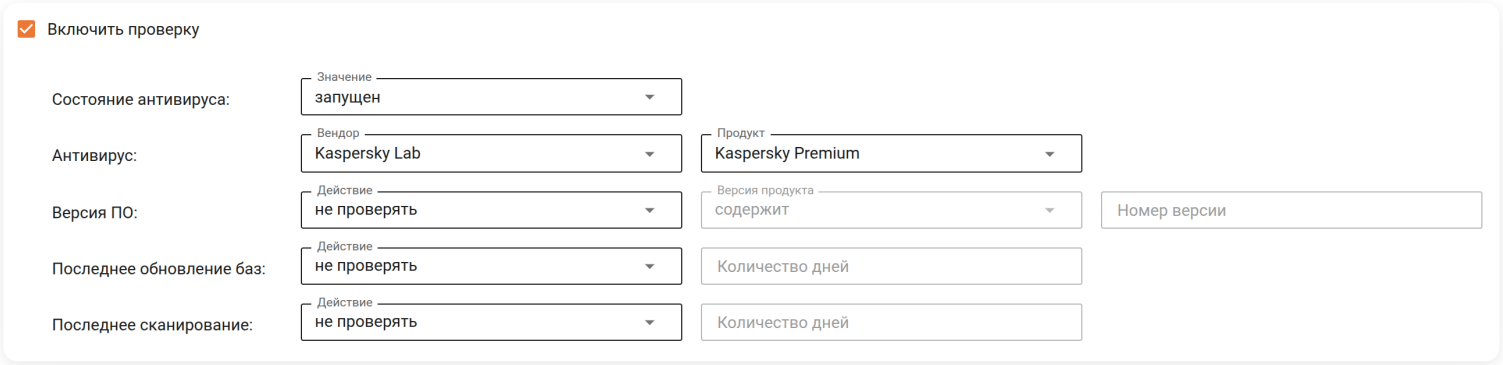
3. Включите проверки, нажав **Включить проверку** для каждого критерия:

ОС и домен



- Оператор - **содержит**.
- ОС - **Windows**.
- Версия ОС - **11**.

Антивирус



- Состояние антивируса - **Запущен**.
- Вендор - `Kaspersky Lab`.

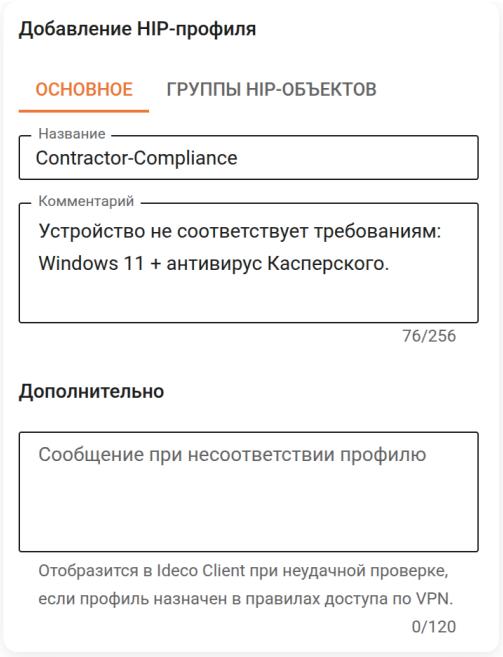
> Для большей детализации можно добавить версию установленного пакета обновлений.

4. Нажмите **Добавить**.

Создание HIP-профиля

1. Перейдите на вкладку **HIP-профили** и нажмите **Добавить**.

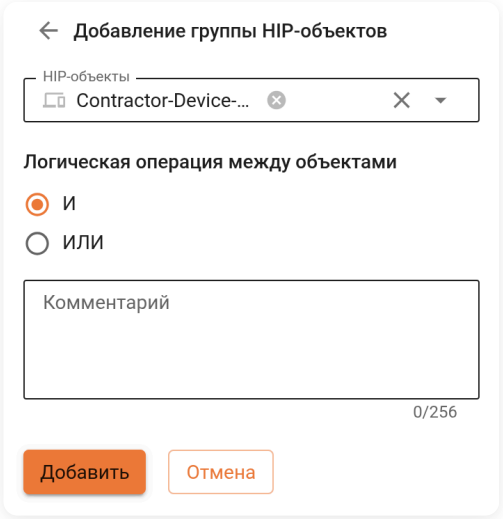
2. Заполните поля на вкладке **Основное**:



- **Название HIP-профиля** - `Contractor-Compliance`.
- **Сообщение при несоответствии профилю** - `Устройство не соответствует требованиям: Windows 11 + антивирус Касперского`.

3. Перейдите на вкладку **Группы HIP-объектов**.

4. Нажмите **Добавить группу**, заполните поля и нажмите **Добавить**:



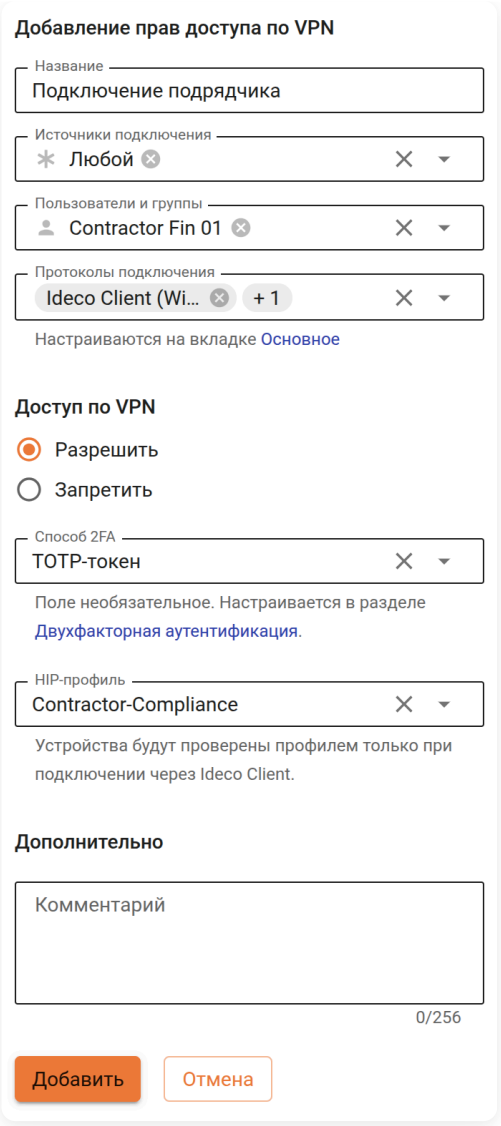
- **HIP-объекты** - выберите созданный объект `Contractor-Device-Requirements`.
- **Логическая операция между объектами** - укажите логическую операцию **И**.

4. Нажмите **Добавить**.

Настройка VPN-подключения через Ideco Client

1. Перейдите в **Пользователи** → **Ideco Client** и убедитесь, что служба включена.

2. Перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и нажмите **Добавить**. Заполните поля:

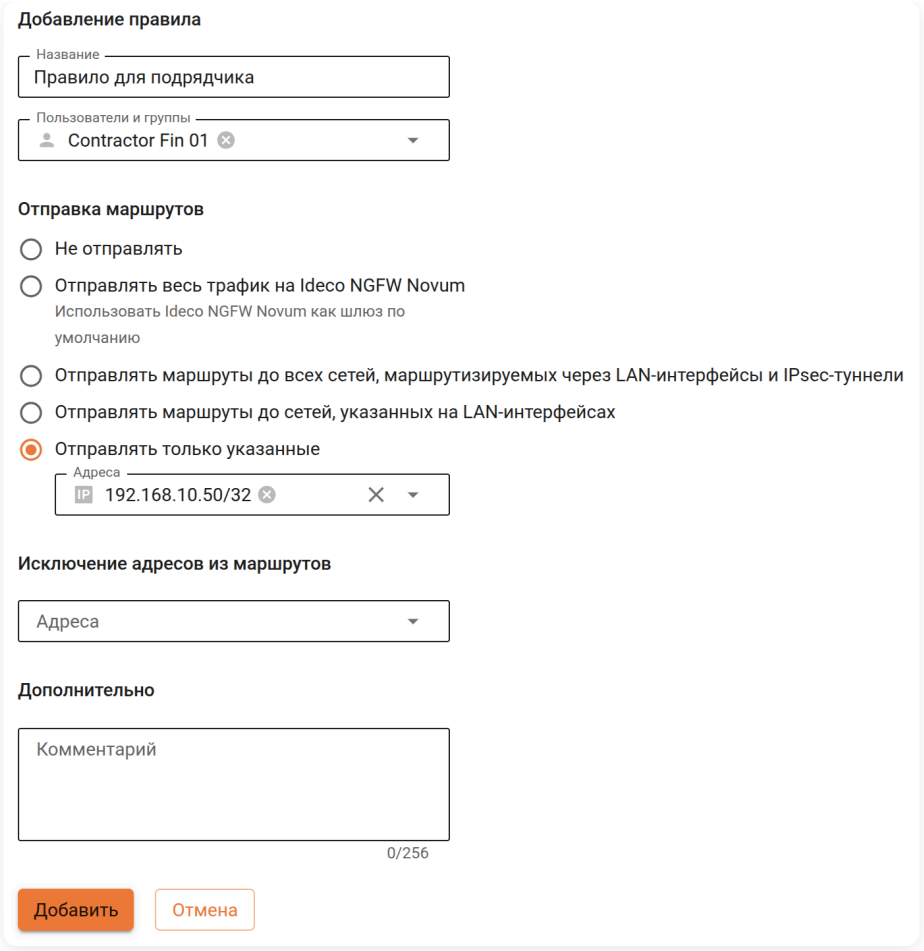


- **Пользователи и группы** - выберите пользователя `contractor-fin-01`.
- **Способ 2FA** - выберите **TOTP-токен**.
- **HIP-профиль** - выберите `Contractor-Compliance`.

> Именно здесь HIP-профиль блокирует само VPN-подключение при несоответствии устройства требованиям - с сообщением, заданным в профиле.

3. Нажмите **Добавить**.

4. Перейдите на вкладку **Передача маршрутов** и нажмите **Добавить**. Заполните поля:



- **Пользователи и группы** - выберите пользователя `contractor-fin-01`.
- **Тип передачи** - выберите **Отправлять только указанные**.
- **Сети** - укажите `192.168.10.50/32`.

5. Нажмите **Добавить**.

Эта настройка ограничит маршрутизацию на стороне VPN-клиента: на устройство подрядчика будет передан только маршрут до RDP-сервера. Интернет-трафик подрядчика не будет проходить через NGFW Novum (запрет split-tunneling).

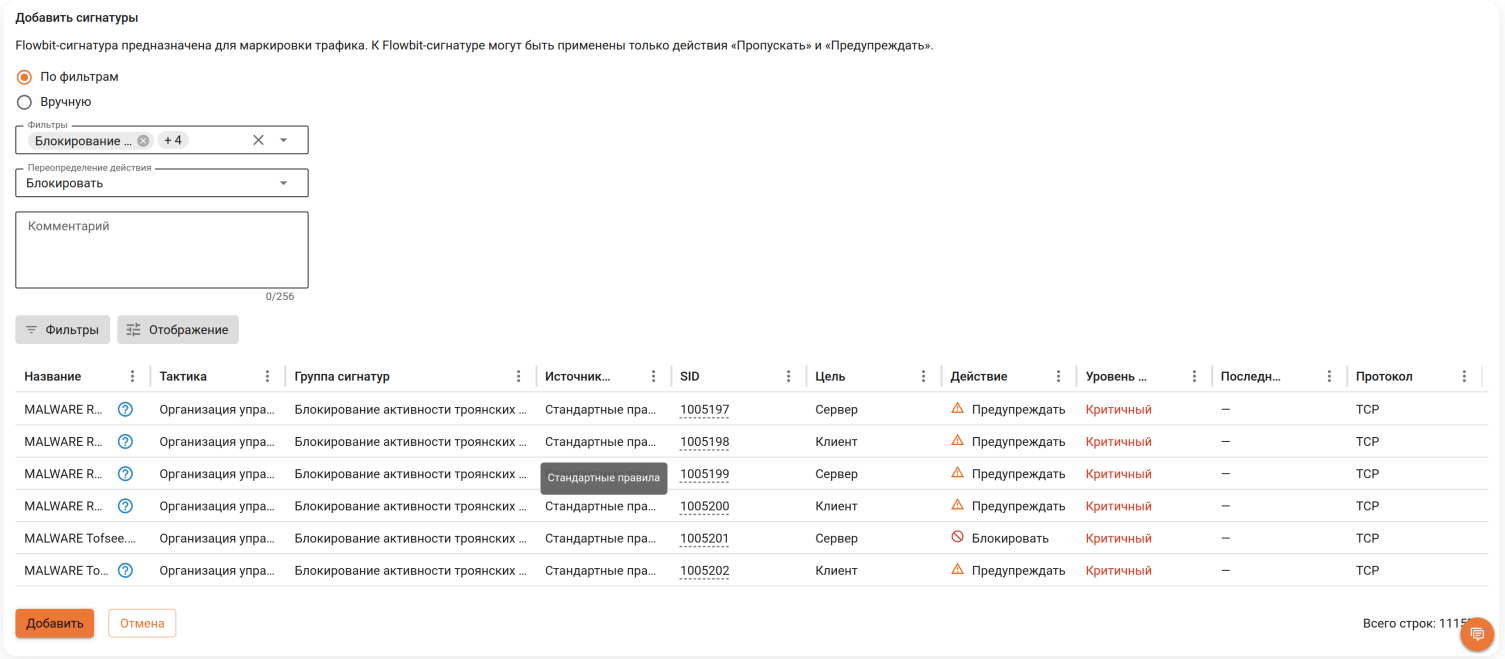
Создание профиля Предотвращения вторжений

1. Перейдите в **Профили безопасности** → **Предотвращение вторжений** и нажмите **Добавить**.

2. Введите название профиля, например, `IPS-Contractor-RDP`, и нажмите **Добавить**.

3. Перейдите на вкладку **Сигнатуры** созданного профиля и нажмите **Добавить сигнатуры**.

4. Выберите способ **По фильтрам**. Последовательно добавьте каждую из групп сигнатур, связанных с защитой RDP-соединений. Для каждой группы выберите действие **Блокировать** и нажмите **Добавить**:



- **Блокирование атак** - обнаружение эксплойтов, сканирования портов и попыток удаленного выполнения кода.
- **Атаки на получение прав пользователя** - выявление попыток получить несанкционированный доступ к учетным данным.
- **Атаки на получение привилегий администратора** - защита от эскалации привилегий.
- **Блокирование активности троянских программ** - обнаружение вредоносной активности в канале подключения.
- **Блокирование крупных утечек информации** - предотвращение несанкционированного экспорта данных.

5. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

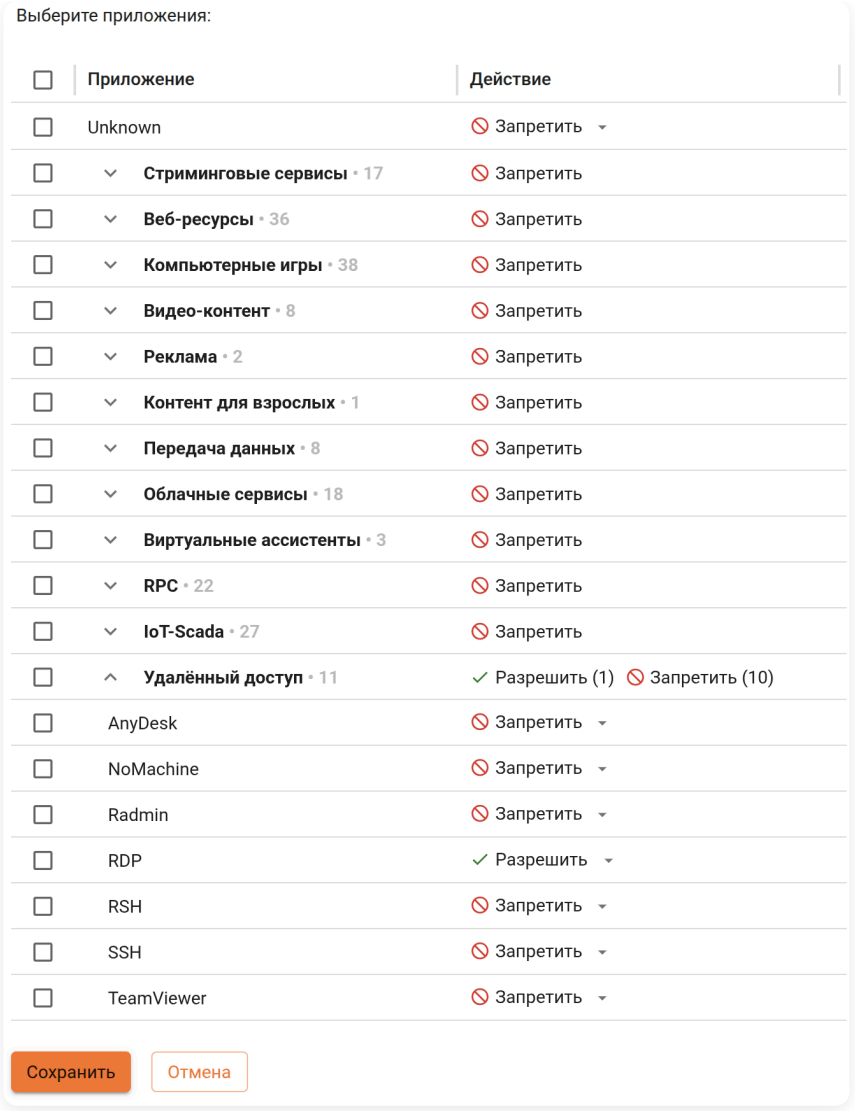
Создание профиля Контроля приложений

1. Перейдите в **Профили безопасности → Контроль приложений** и нажмите **Добавить**.

2. Введите название профиля, например `AppControl-RDP-Only`, и нажмите **Добавить**.

3. Перейдите на вкладку **Доступ к приложениям**.

4. Выберите все протоколы и приложения, которые необходимо заблокировать (например, HTTP, HTTPS, SMB, SSH, FTP и другие). Примените к ним действие **Запретить**:



5. Нажмите **Сохранить**.

Принцип работы по умолчанию: все протоколы и приложения, которые явно не запрещены, остаются разрешены. Создавать отдельное разрешающее правило для RDP не нужно - он разрешен автоматически, пока не попадет под запрет.

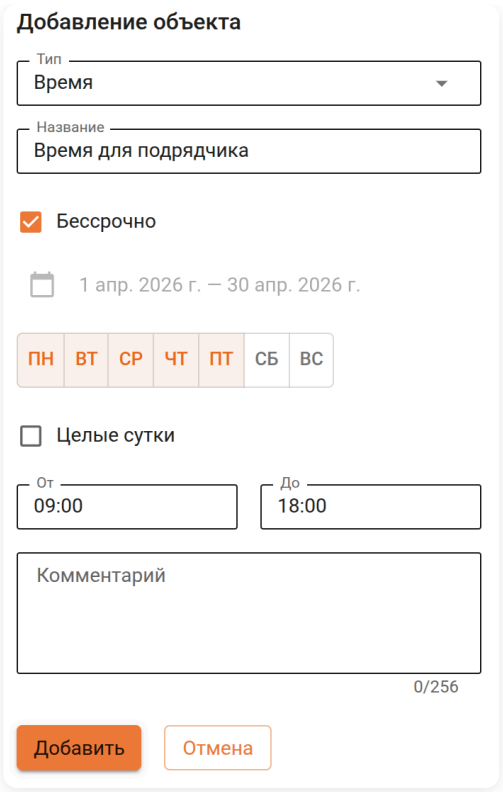
Настройка правил Межсетевого экрана

Правила **Межсетевого экрана** обеспечивают сетевую изоляцию подрядчика. Создайте правила в порядке, указанном ниже, и убедитесь, что разрешающее правило расположено выше запрещающего в таблице.

Создание объекта Время

Перед настройкой правила необходимо создать объект временного интервала, который будет использован в поле **Время действия** правила **Межсетевого экрана**.

1. Перейдите в **Правила трафика** → **Объекты**, нажмите **Добавить** и заполните поля:



- **Тип** - выберите тип объекта **Время**.
- **Название** - укажите название. Например, `Время для подрядчика`.

Укажите временные промежутки: **понедельник–пятница**, с **09:00** до **18:00**.

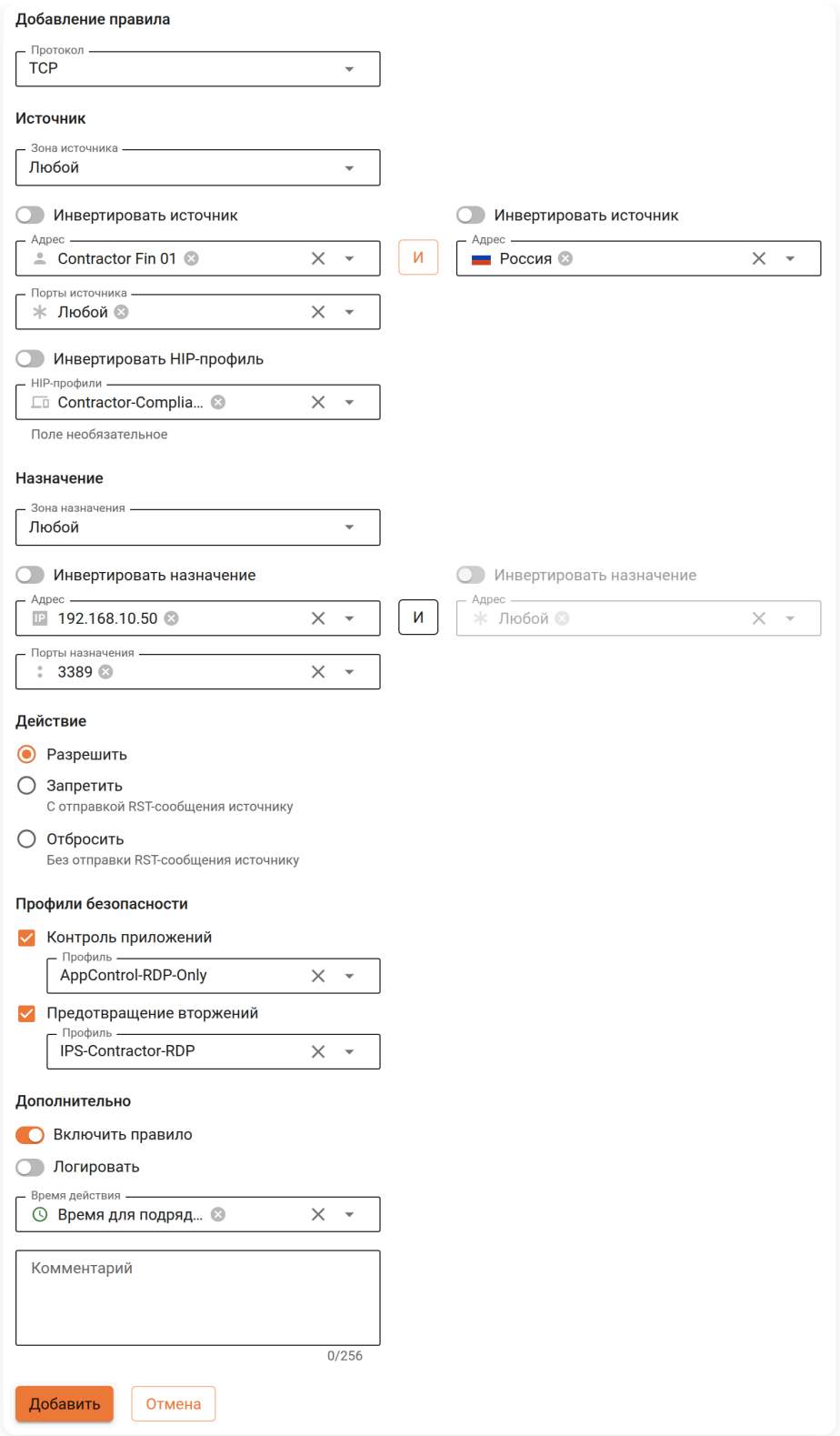
2. Нажмите **Добавить**.

Время задается по часовому поясу сервера, так как сервер не знает локального времени клиента.

Разрешающее правило для доступа к RDP-серверу

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - TCP.
- **Источник**:
  - **Адрес** - пользователь `contractor-fin-01`.
  - С помощью оператора **И** добавьте второе условие: **Страна** - Россия (GeoIP-фильтрация).
  - **HIP-профили** - `Contractor-Compliance` для дополнительной проверки соответствия устройства на уровне трафика.
- **Назначение**:
  - **Адрес** - IP-адрес RDP-сервера `192.168.10.50`.
  - **Порты назначения** - `3389`.
- **Действие** - Разрешить.
- **Профили безопасности**:
  - **Контроль приложений** - `AppControl-RDP-Only`.
  - **Предотвращение вторжений** - `IPS-Contractor-RDP`.

- **Дополнительно**:
  - **Время действия** - объект `Время для подрядчика`.
  - **Включить правило** - включите опцию.

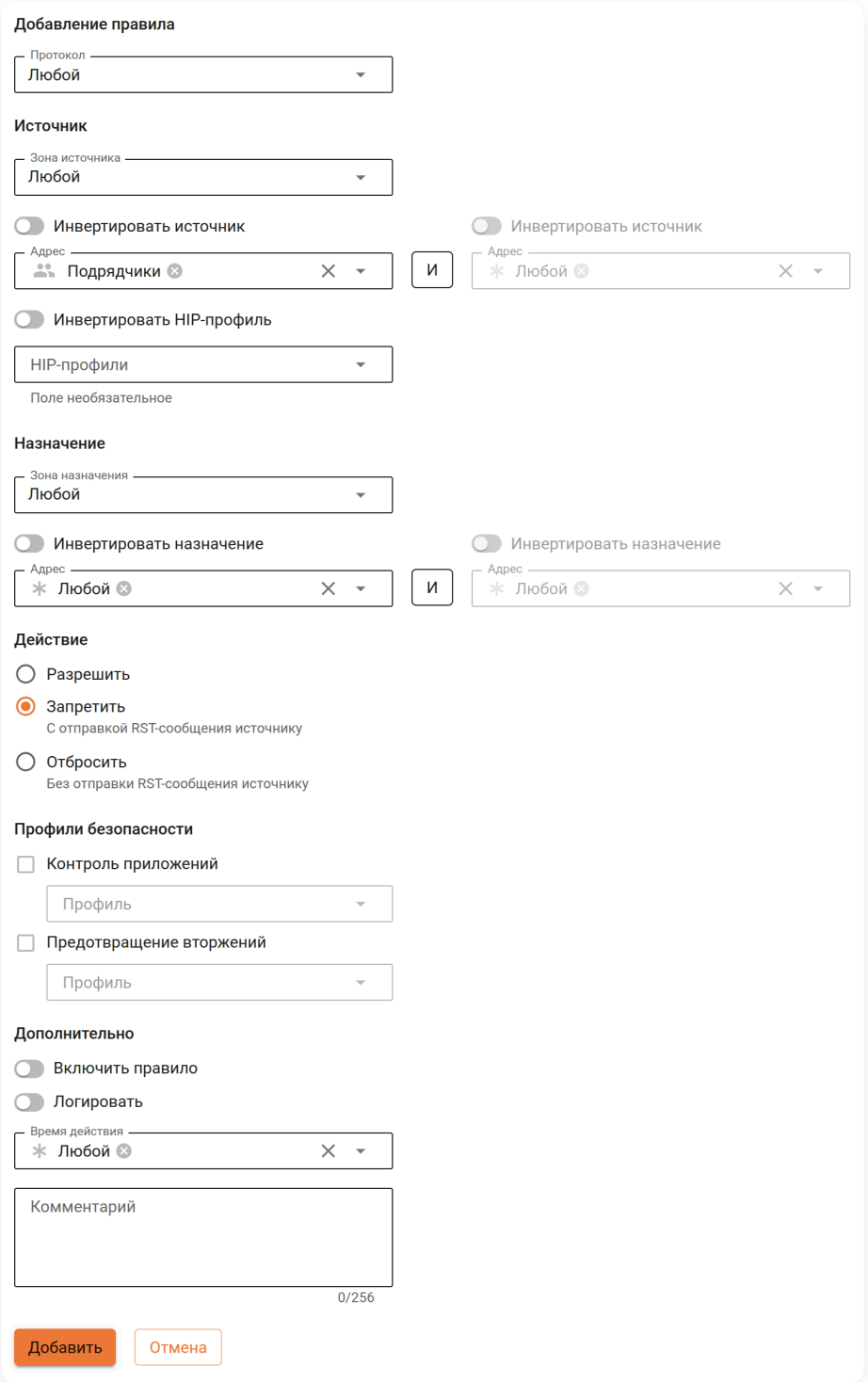
3. Нажмите **Добавить**.

> В зависимости от используемой версии протокола RDP также может потребоваться правило с UDP. Создайте аналогичное правило с протоколом UDP, используя кнопку **Клонировать** в таблице правил.

Запрещающее правило для блокировки остального трафика

1. На вкладке **FORWARD** нажмите **Добавить**.

2. Заполните поля:



- **Источник**:

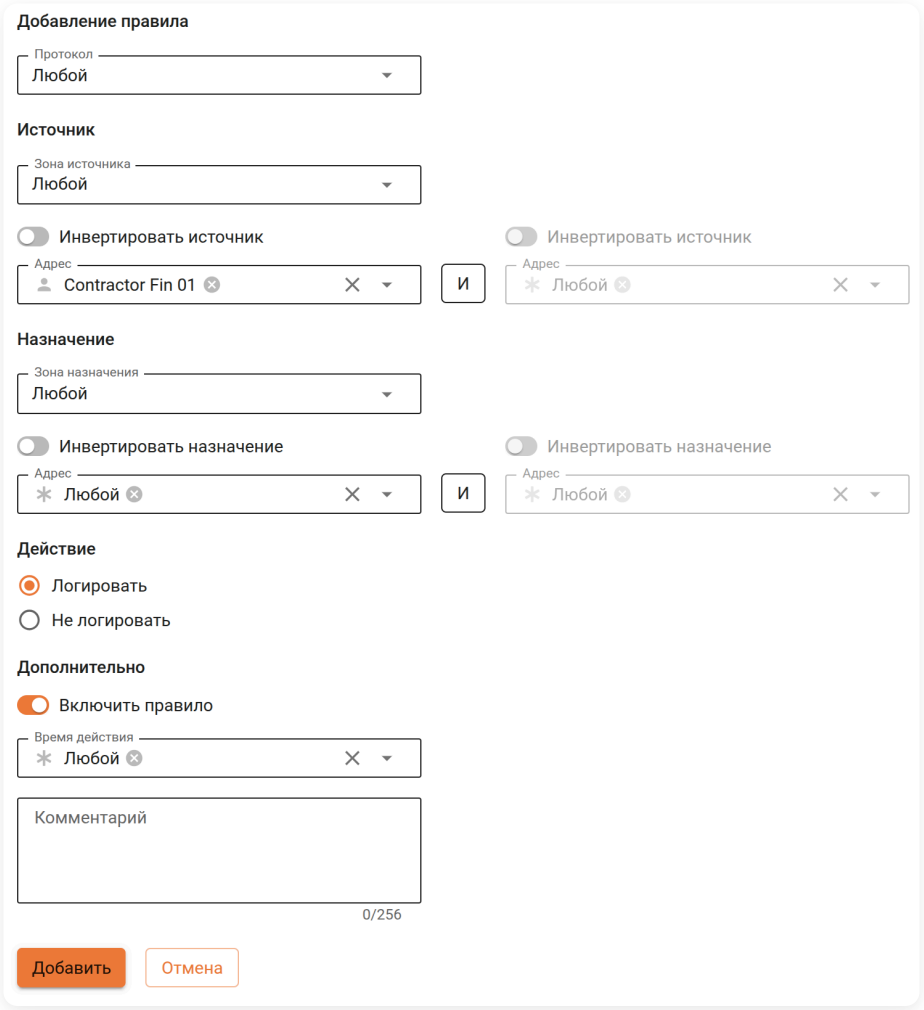
- **Адрес** - пользователь `contractor-fin-01` или группа **Подрядчики**.
- **Дополнительно**:
  - **Действие** - Запретить.
  - **Включить правило** - включите опцию.

3. Нажмите **Добавить**.

Настройка логирования

Для записи всех сессий подрядчика настройте логирование трафика.

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **Логирование**, нажмите **Добавить** и заполните поля:



- **Источник** - выберите пользователя `contractor-fin-01` или группу **Подрядчики**.
- **Действие** - Логировать.
- **Включить правило** - включите опцию.

2. Нажмите **Добавить**.

3. Включите опцию **Логировать срабатывания правил**.

> Записи доступны в **Отчеты и журналы** → **Межсетевой экран**. Информация о срабатывании профилей **Контроля приложений** и **Предотвращения вторжений** также фиксируется в журнале.

Передача журналов в SIEM-систему

Для долгосрочного хранения и анализа настройте передачу логов через Syslog:

1. Перейдите в **Сервисы** → **Syslog** и включите модуль.

2. Укажите адрес и порт SIEM-системы или Syslog-коллектора.

3. Выберите **Протокол передачи**.

4. Нажмите **Сохранить**.

Все события, включая сессии подрядчика, срабатывания системы **Предотвращения вторжений** и действия **Межсетевого экрана**, будут передаваться в указанную систему.

Установка Ideco Client на устройство подрядчика

1. Передайте подрядчику ссылку для скачивания Ideco Client. Скачать клиент можно в веб-интерфейсе Ideco NGFW Novum или в личном кабинете пользователя.

2. Подрядчик устанавливает Ideco Client на устройство с Windows 11.

3. При первом подключении подрядчик указывает:

- **Адрес сервера** - внешний IP-адрес или доменное имя Ideco NGFW Novum.
- **Логин** - `contractor-fin-01`.
- **Пароль** - пароль, заданный при создании учетной записи.

4. После ввода логина и пароля подрядчик перенаправляется на страницу двухфакторной аутентификации. При первом подключении необходимо войти в личный кабинет NGFW Novum, нажать **Настроить двухфакторную аутентификацию** и отсканировать QR-код в приложении-аутентификаторе (Яндекс ID, Google Authenticator или Microsoft Authenticator).

5. При последующих подключениях подрядчик вводит одноразовый код из приложения для прохождения двухфакторной аутентификации.

После успешной аутентификации Ideco Client устанавливает VPN-туннель. NGFW Novum проверяет устройство по HIP-профилю `Contractor-Compliance`. Если устройство не соответствует требованиям (отсутствует Windows 11 или антивирус Касперского не активен), подключение блокируется с сообщением **Устройство не соответствует требованиям: Windows 11 + антивирус Касперского**.

Чек-лист: проверка настройки

После завершения настройки выполните проверку:

- ☑ Убедитесь, что подрядчик подключается через Ideco Client и проходит двухфакторную аутентификацию
- ☑ Проверьте, что в **Мониторинг** → **Сессии пользователей** отображается сессия подрядчика с назначенным HIP-профилем `Contractor-Compliance`
- ☑ Убедитесь, что подрядчик имеет доступ только к RDP-серверу по адресу `192.168.10.50:3389`, весь остальной трафик должен быть заблокирован
- ☑ Проверьте **Отчеты и журналы** → **События безопасности** → **Журнал IPS** на наличие записей по трафику подрядчика
- ☑ Проверьте записи в **Отчеты и журналы** → **Межсетевой экран** для аудита сессий
- ☑ Попробуйте подключиться за пределами рабочего времени (после 18:00 или в выходной) и убедитесь, что доступ запрещен

Чек-лист: действия при завершении работы с подрядчиком

По окончании контрактного периода выполните действия:

- ☑ Завершите активную сессию подрядчика в **Мониторинг** → **Сессии пользователей**, если она активна
- ☑ Откройте карточку пользователя `contractor-fin-01` в **Пользователи** → **Учетные записи** и на вкладке **Основное** включите опцию **Запретить доступ**
- ☑ Отключите правило `Contractor-Allow-RDP` в **Правила трафика** → **Межсетевой экран** → **FORWARD**
- ☑ Отключите правило `Contractor-Deny-All` в **Правила трафика** → **Межсетевой экран** → **FORWARD**
- ☑ Удалите запись пользователя `contractor-fin-01` из таблицы **Доступ по VPN** в **Пользователи** → **VPN-подключения**
- ☑ Сбросьте секретный ключ двухфакторной аутентификации в карточке пользователя `contractor-fin-01` в **Пользователи** → **Учетные записи**
- ☑ Сохраните журналы сессий подрядчика из **Отчеты и журналы** → **Межсетевой экран** и **Отчеты и журналы** → **Аутентификация пользователей** для архива либо убедитесь, что они уже имеются в SIEM-системе
- ☑ При необходимости удалите учетную запись, группу, HIP-профиль и профили безопасности, если они больше не используются

Полезные ссылки

- **Двухфакторная аутентификация**
- **Пользователи**
- **Профили устройств**
- **Управление учетными записями и группами**

Сервисы

Практические руководства по настройке сервисов Ideco NGFW

DNS

Настройка DNS-сервера и Forward-зон

Перейти >

Сетевые интерфейсы

Настройка Wi-Fi-сети и LACP

Перейти >

IPsec

Подключение различных устройств к Ideco NGFW по IPsec

Перейти >

ГОСТ VPN

Генерация ключей и сертификатов ГОСТ VPN

Перейти >

Прокси

Настройка прямых подключений к прокси-серверу

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

DNS

Практические руководства по настройке DNS в Ideco NGFW

Подключение через Ideco Client к внутреннему DNS

Перейти >

Пример настройки Forward-зоны

Перейти >

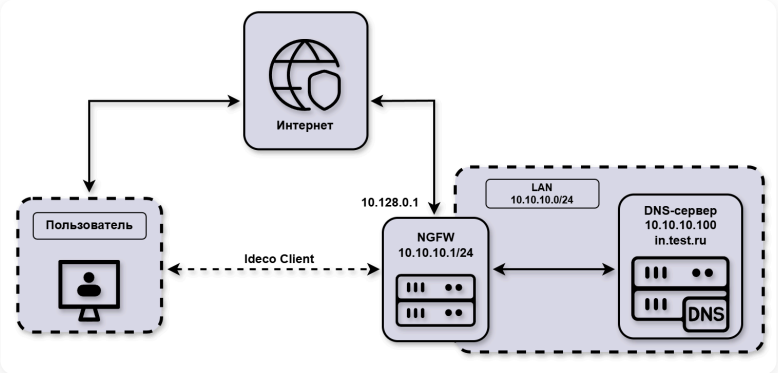
Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Подключение через Ideco Client к внутреннему DNS

Клиенты, подключающиеся к NGFW Novum из внешней сети через Ideco Client, изначально не видят внутренний DNS-сервер.

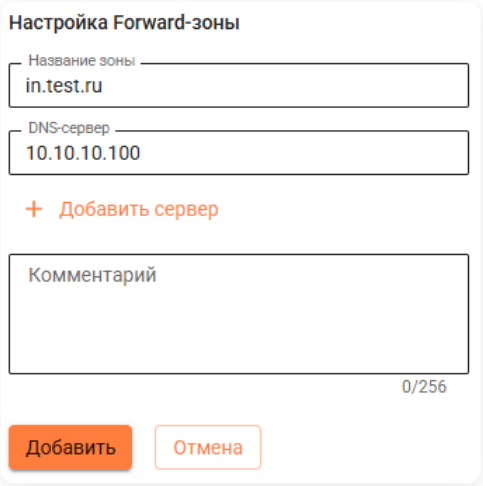
Схема сети:



Для настройки подключения к внутреннему DNS-серверу выполните действия:

1. Перейдите в **Сервисы** → **DNS** → **FORWARD-ЗОНЫ** и нажмите **Добавить**.

2. Заполните форму и нажмите **Добавить**:



После настройки NGFW Novum клиенты, подключающиеся к NGFW Novum с помощью Ideco Client из интернета, смогут использовать внутренний DNS-сервер.

Полезные ссылки

- **DNS**
- **Forward-зоны**
- **Ideco Client**

Пример настройки Forward-зоны

Как настроить сеть, чтобы пользователи локальной сети могли обращаться к ресурсам, опубликованным на Ideco NGFW Novum. Ресурсы находятся в защищенной сети, и доступ к ним должен осуществляться напрямую, без выхода через внешний интерфейс.

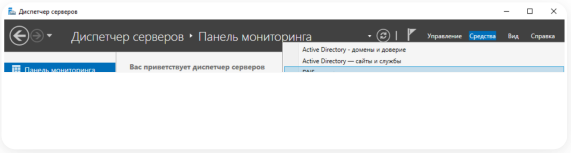
Если в сети уже есть DNS-сервер

1. На DNS-сервере, например, в AD, создайте новую зону прямого просмотра, на которую будут перенаправляться запросы пользователей. В зоне прямого просмотра создайте необходимые DNS-записи с приватными IP-адресами.

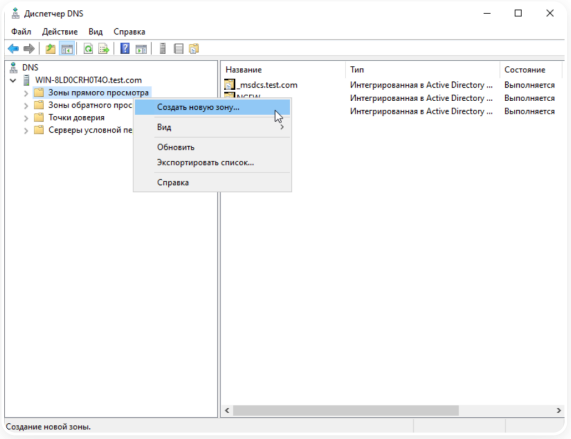
2. На Ideco NGFW Novum настройте Forwad-зону для перенаправления пользователей на зону прямого просмотра в AD.

Пример с настройкой DNS-сервера в AD

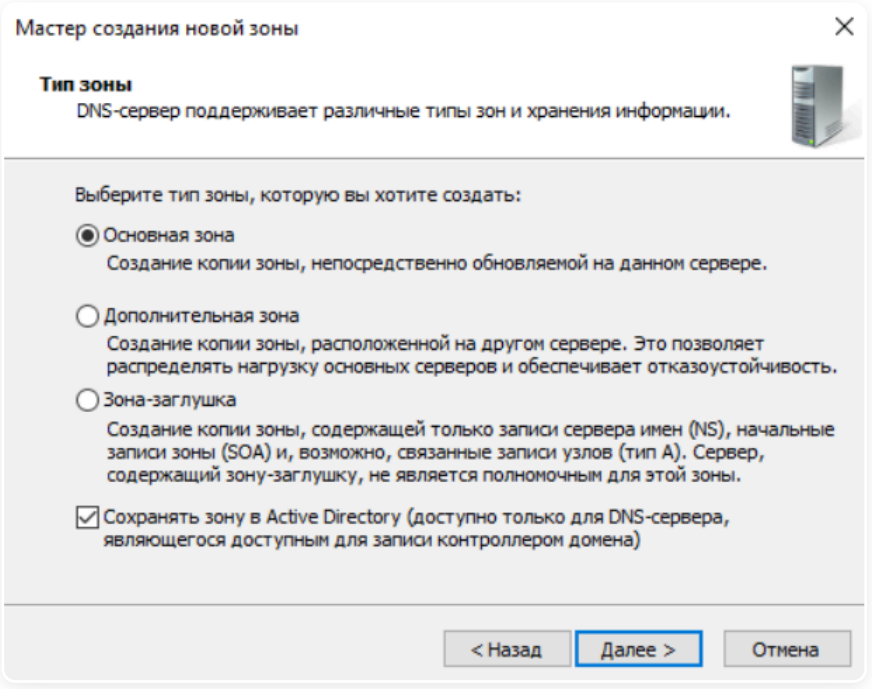
1. На контроллере домена откройте **Диспетчер сервера** → **Средства** → **DNS**:



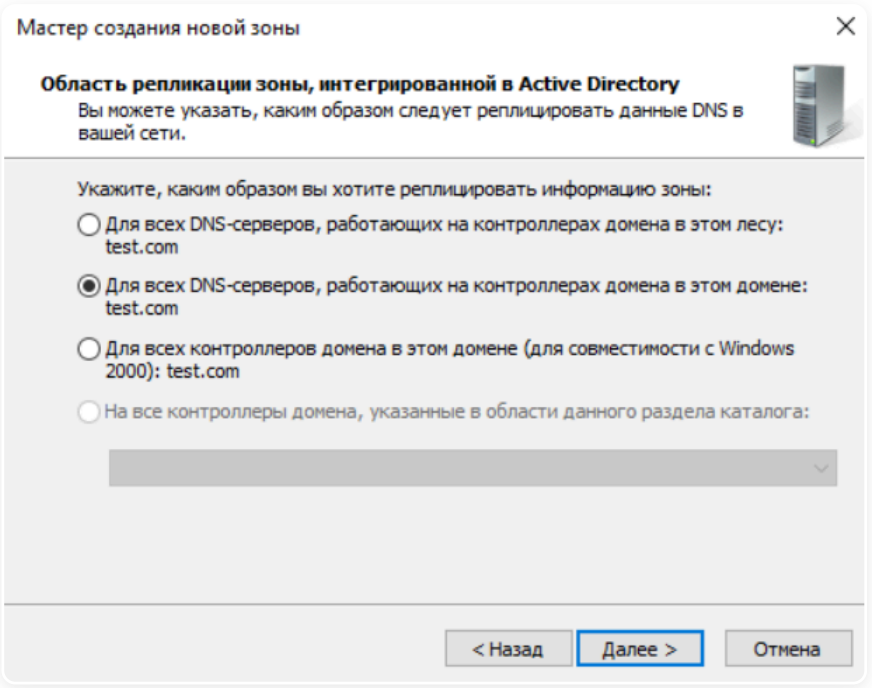
2. В новом окне разверните узел сервера, нажмите правой кнопкой мыши на **Зоны прямого просмотра** и выберите **Создать новую зону**:



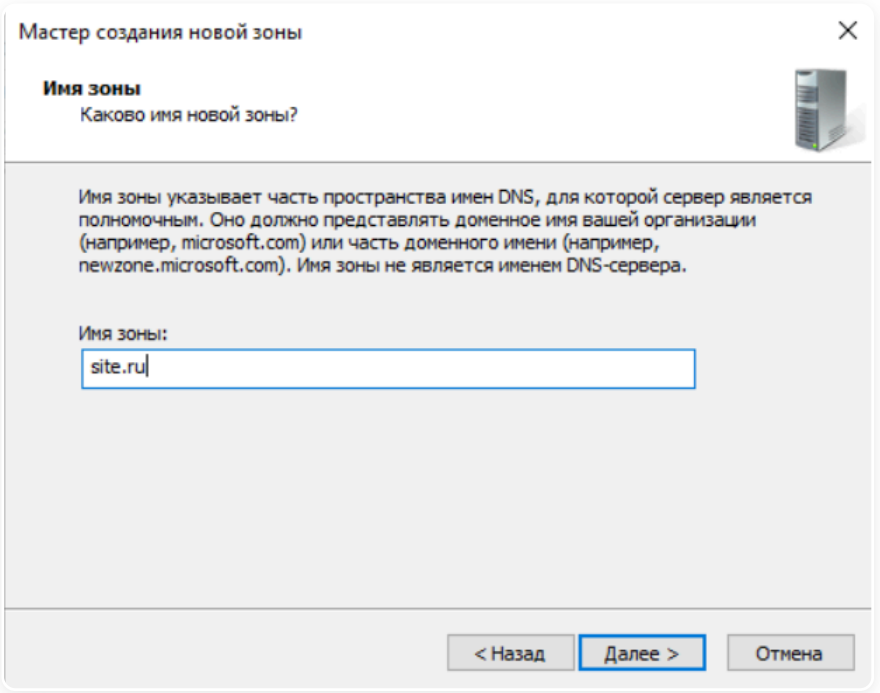
3. Нажмите **Далее** и выберите тип **Основная зона**. Для интеграции с AD убедитесь, что включена опция **Хранить зону в Active Directory**:



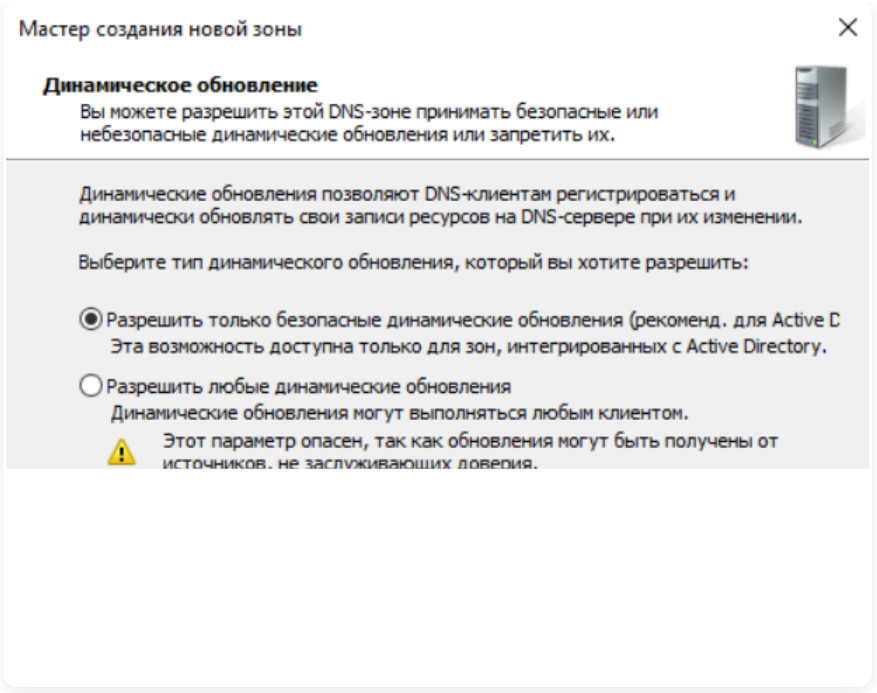
4. Выберите область репликации для зоны (например, **На все DNS-серверы, работающие на контроллерах домена в этом домене**), чтобы зона автоматически реплицировалась:



5. Укажите имя зоны:



6. Настройте динамические обновления. Для безопасности в доменной среде рекомендуется выбрать **Разрешать только безопасные динамические обновления**:



7. Нажмите **Готово**.

8. Создайте новую A-запись. В DNS-менеджере нажмите правой кнопкой мыши по созданной зоне и выберите **Создать узел (A или AAAA)**:

9. Заполните поля:

- **Имя** - введите имя хоста (например, `in` для полного доменного имени `in.site.ru`).
- **IP-адрес** - введите внутренний IP-адрес сервера.
- **Создать связанную запись (PTR)** - по желанию можно включить опцию для автоматического создания соответствующей PTR-записи в зоне обратного просмотра.

10. Сохраните запись, нажав **Добавить узел**.

11. Перейдите в Ideco NGFW Novum в раздел **Сервисы** → **DNS** → **FORWARD-зоны** и нажмите **Добавить**.

12. Заполните поля:

- **Название зоны** - укажите имя зоны из пункта 5.
- **DNS-сервер** - укажите IP-адрес из пункта 9.

13. Нажмите **Добавить**.

Полезные ссылки

- **DNS**
- **Forward-зоны**

Сетевые интерфейсы

Практические руководства по настройке сетевых интерфейсов в Ideco NGFW

Настройка Wi-Fi-сети

Перейти >

Настройка LACP на Hyper-V

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка Wi-Fi-сети

В текущей версии Ideco NGFW Novum не поддерживает Wi-Fi-адаптеры. Для работы беспроводных клиентов необходимо использовать беспроводные точки доступа или Wi-Fi-маршрутизаторы.

Для выхода в интернет пользователей, подключающихся по Wi-Fi, необходима авторизация пользователей или Wi-Fi-роутера в Ideco NGFW Novum. Способ авторизации зависит от режима работы маршрутизатора.

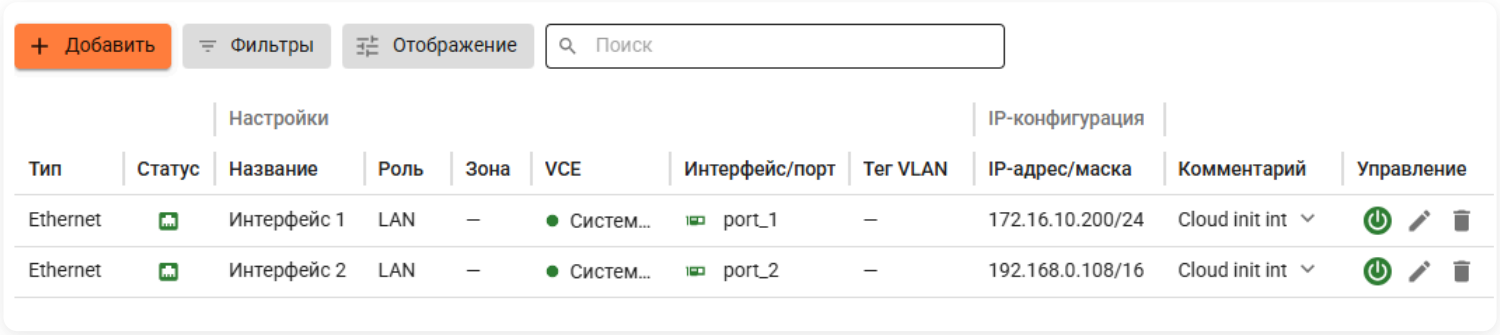
Режим точки доступа или bridge

В режиме точки доступа или bridge устройство Wi-Fi позволяет беспроводным клиентам подключаться к локальной сети.

Для этого индивидуально авторизуйте всех беспроводных клиентов на Ideco NGFW Novum с помощью IP-авторизации. Воспользуйтесь рекомендациями по настройке:

- Используйте отдельную логическую сеть для клиентов Wi-Fi с настроенным DHCP-сервером.
- Создайте в **Сервисы** → **Сетевые интерфейсы** новый интерфейс, в IP-конфигурации выберите режим **Статический**, добавьте IP-адрес, служащий шлюзом для этой сети.
- Создайте группу пользователей, подключающихся по Wi-Fi.
- С помощью Контент-фильтра настройте необходимые ограничения для пользователей Wi-Fi.
- Если Wi-Fi-роутер подключен к отдельному физическому интерфейсу Ideco NGFW Novum, то в **Межсетевом экране** запретите доступ из беспроводной сети в локальную сеть.

Пример настройки интерфейса для клиентов, подключающихся по Wi-Fi:



- `172.16.10.200/24` - интерфейс для беспроводной Wi-Fi-сети.
- `192.168.0.108/16` - интерфейс для локальной Ethernet-сети.

Настройка DHCP

1. Создайте в **Сервисы** → **Сетевые интерфейсы** новый интерфейс, в IP-конфигурации выберите режим **DHCP**.

2. Перейдите в **Сервисы** → **DHCP-сервер** и выберите сетевой интерфейс, настроенный на прошлом шаге.

3. Назначьте диапазон IP-адресов для DHCP-сервера и нажмите **Сохранить**.

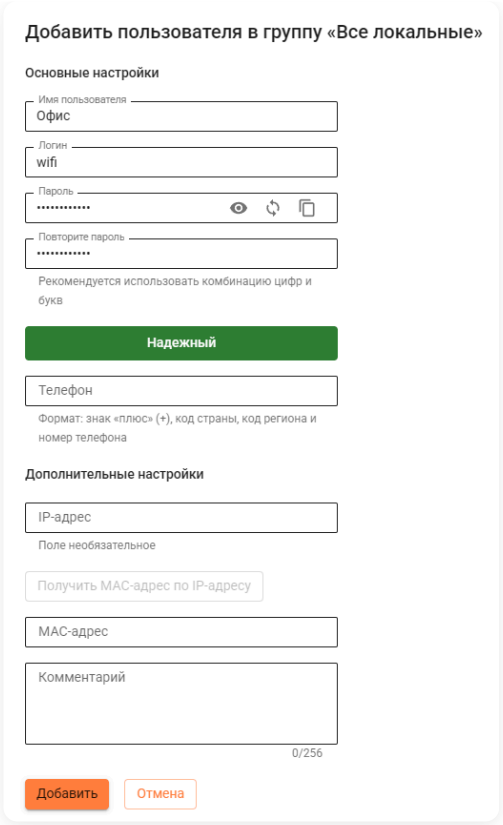
Для индивидуальной авторизации Wi-Fi-пользователей и учета их трафика и статистики воспользуйтесь Веб-аутентификацией. При таком способе авторизации Ideco NGFW Novum будет учитывать каждого пользователя, подключившегося по Wi-Fi. Это следует принять во внимание при планировании лицензирования Ideco NGFW Novum.

Режим роутера

В режиме роутера устройство Wi-Fi скрывает за NAT устройства беспроводной сети. Таким образом, для Ideco NGFW Novum достаточно будет авторизовать только точку доступа как одного из пользователей.

Пример настройки пользователя в режиме роутера:

1. В **Пользователи** → **Учетные записи** создайте пользователя для Wi-Fi-роутера:



2. Перейдите к настройкам пользователя, выберите **IP и MAC авторизация**, добавьте правило и укажите IP-адрес. Правило также можно добавить в **Пользователи** → **Авторизация** → **IP и MAC**.

К пользователю необходимо применить общие ограничения **Контент-фильтра** для Wi-Fi-сети.

Настройка DHCP

При работе маршрутизатора в режиме роутера не требуется дополнительной настройки DHCP-сервера Ideco NGFW Novum, так как работает встроенный DHCP-сервер маршрутизатора. Если у вас не получилось подключиться к Wi-Fi-сети, нужно проверить работу DHCP-сервера маршрутизатора.

При этом способе авторизации в Ideco NGFW Novum будет использоваться одна лицензия на точку доступа Wi-Fi. Отдельно настроить фильтрацию трафика и считать статистику по трафику в отчетах для отдельных клиентов Wi-Fi будет невозможно.

Полезные ссылки

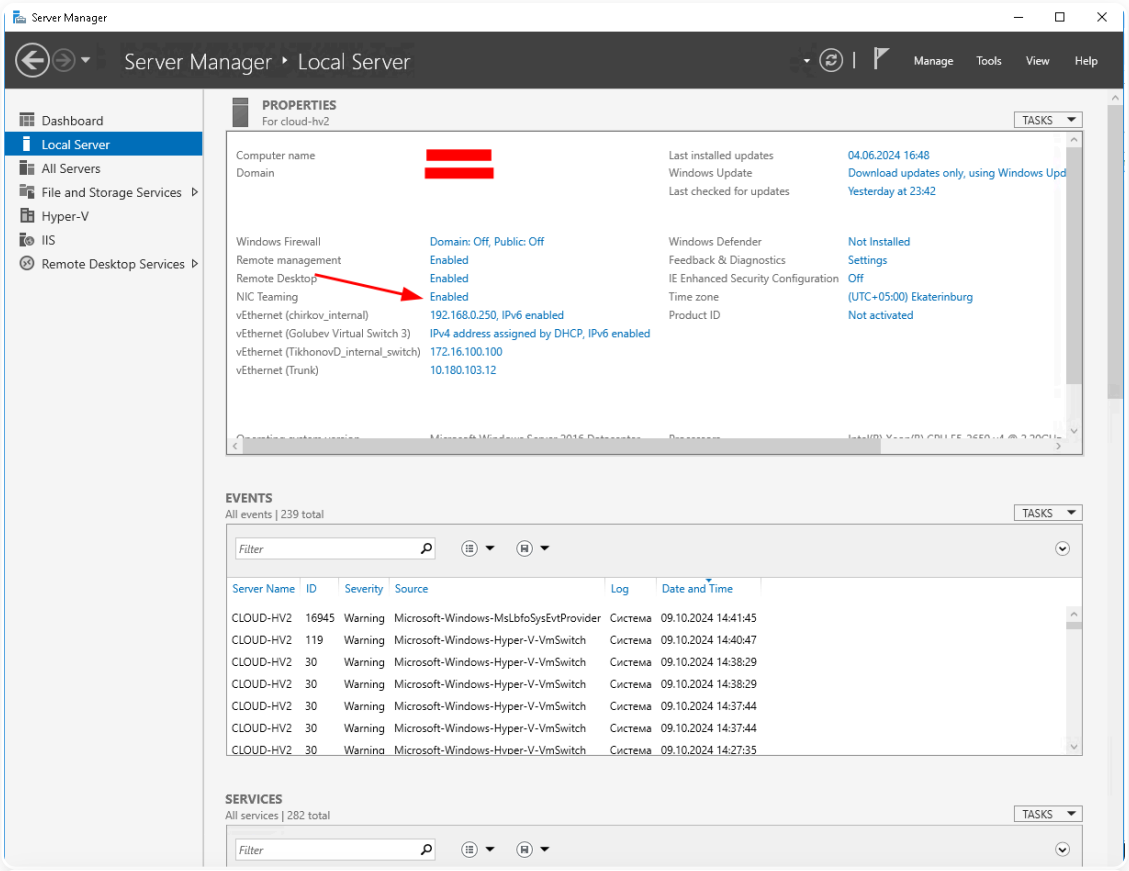
- **DHCP-сервер**
- **Авторизация**
- **Интерфейсы**

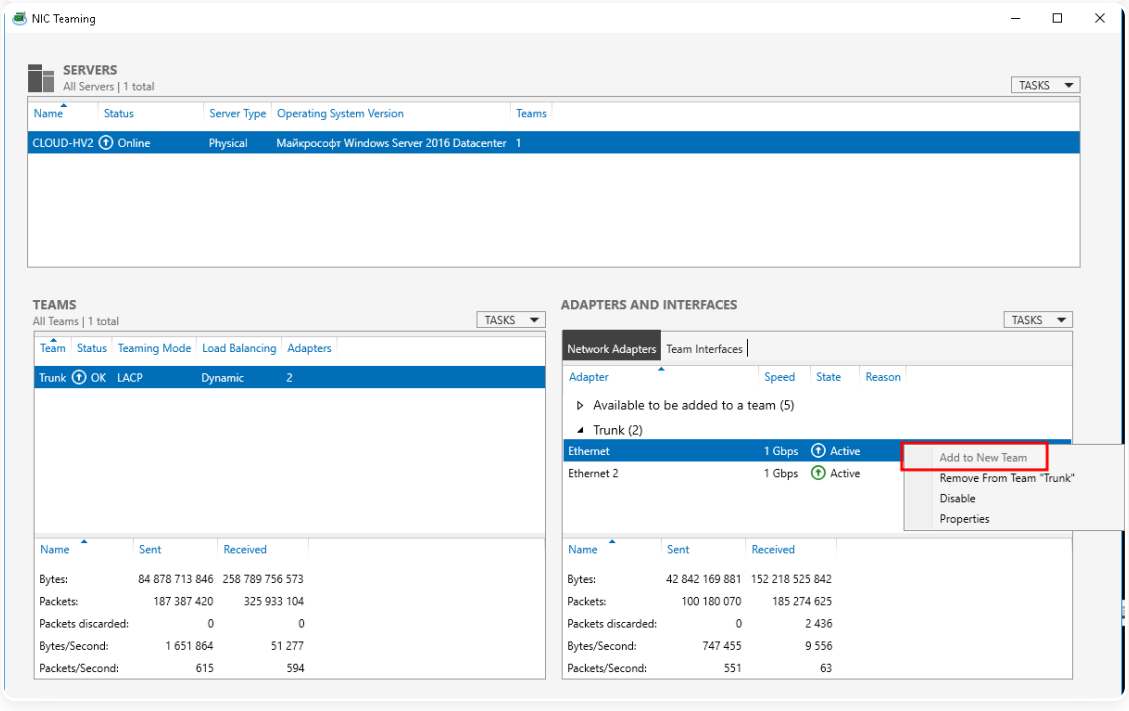
Настройка LACP в Hyper-V

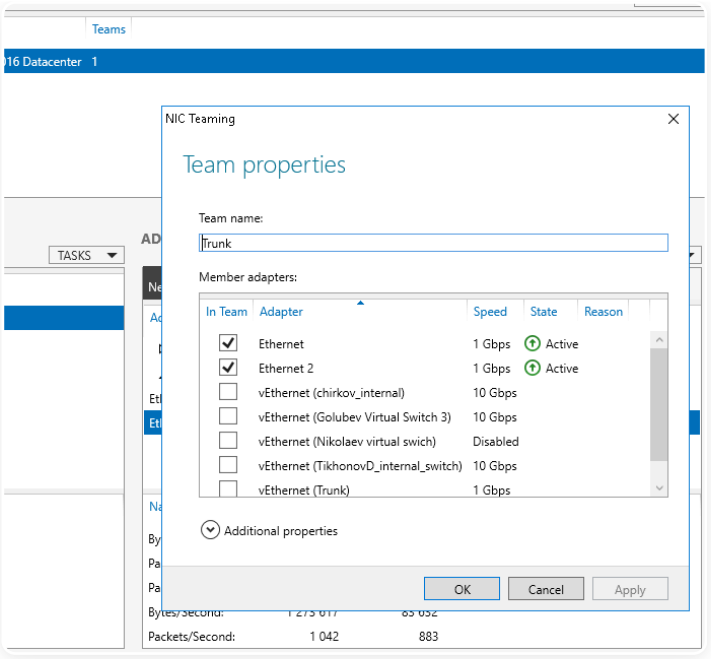
Для настройки LACP в гипервизоре Hyper-V существуют два способа:

Настройка на хост системе

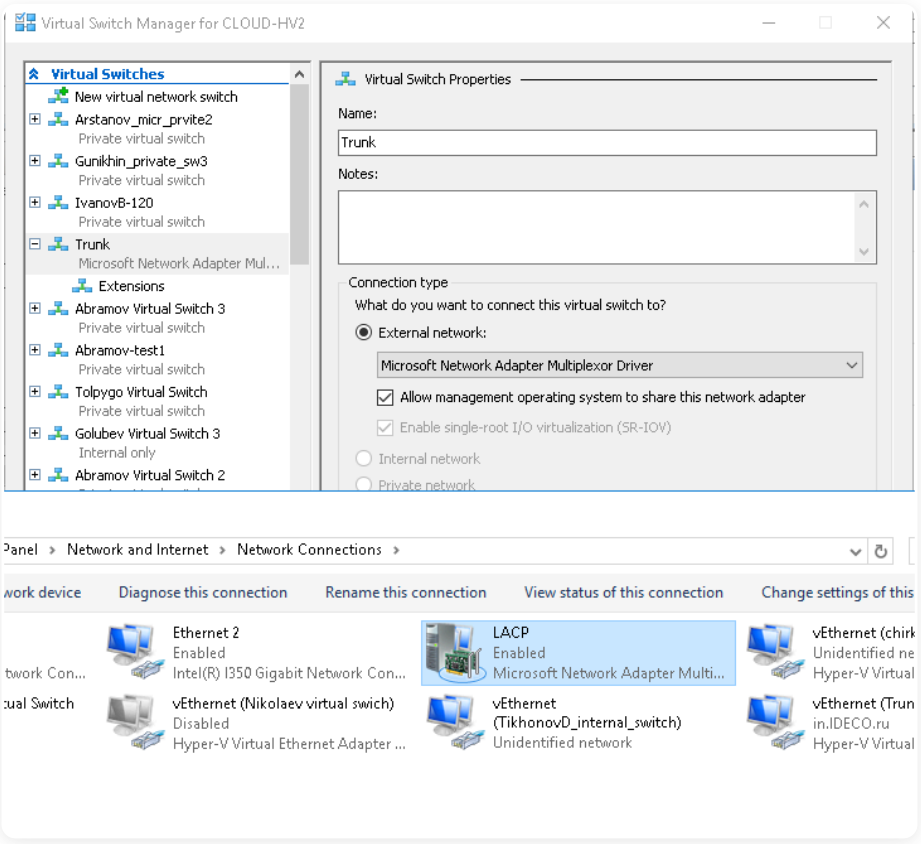
1. Объедините физические интерфейсы:







2. Выберите созданный интерфейс при настройке виртуального свитча:



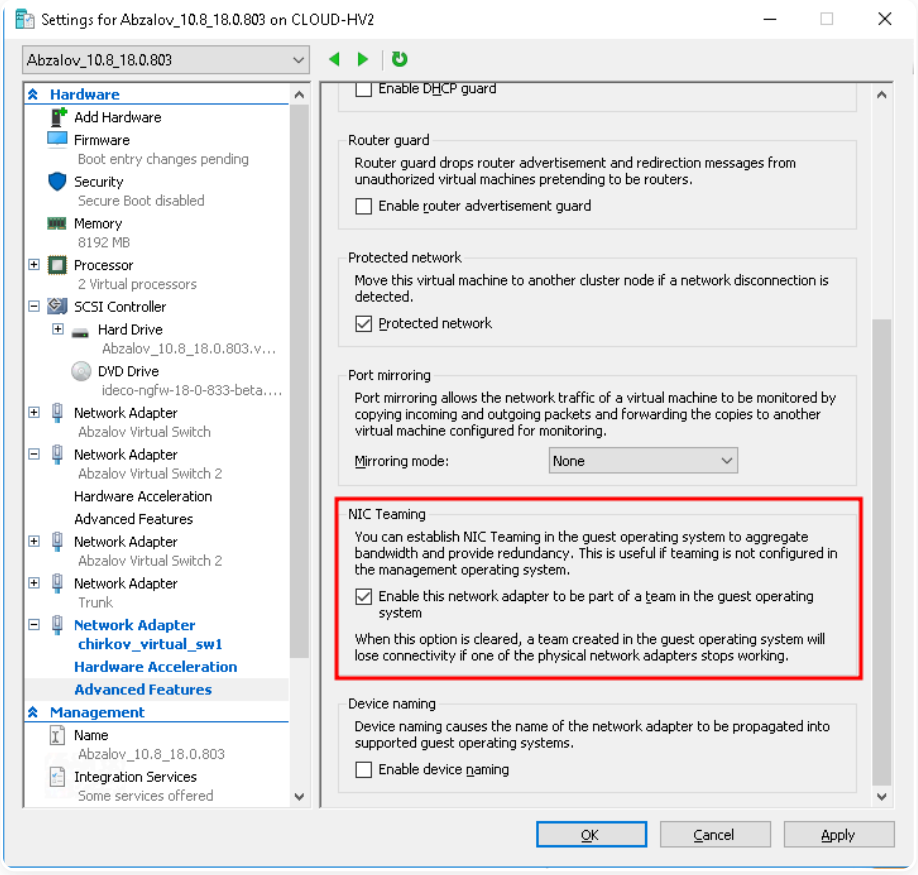
Получившийся виртуальный свитч можно использовать для добавления новых интерфейсов в LACP на гостевую систему.

3. Настройте подключение в **Сетевые интерфейсы → Внешние и локальные** для вновь созданного LACP-интерфейса, как для обычного сетевого интерфейса NGFW.

Настройка на гостевой системе

1. Добавьте необходимое количество интерфейсов на гостевую систему, на основе виртуального свитча, например, с названием **Virtual Switch 1**.

2. На каждом добавляемом интерфейсе включите опцию NIC Teaming:



3. Добавьте вновь созданные интерфейсы в LACP-интерфейсы NGFW в **Сетевые интерфейсы → Агрегированные(LACP)**.

4. Настройте подключения в **Сетевые интерфейсы → Внешние и локальные**.

Полезные ссылки

- **Настройка гипервизора**
- **Интерфейсы**

IPsec

Практические руководства по подключению устройств к Ideco NGFW по IPsec

Подключение между двумя Ideco NGFW в туннельном режиме работы

Перейти >

Подключение между двумя Ideco NGFW в транспортном режиме работы

Перейти >

Подключение Ideco NGFW и Mikrotik по IPsec в туннельном режиме

Перейти >

Подключение Ideco NGFW и Mikrotik по IPsec в транспортном режиме

Перейти >

Подключение MikroTik и Ideco NGFW по L2TP/IPsec

Перейти >

Подключение Cisco IOS и Ideco NGFW по IPsec в туннельном режиме

Перейти >

Подключение Cisco IOS и Ideco NGFW по IPsec в транспортном режиме

Перейти >

Подключение Cisco IOS и Ideco NGFW по route-based IPsec

Перейти >

Подключение pfSense к Ideco NGFW по IPsec

Перейти >

Подключение Kerio Control и Ideco NGFW по IPsec

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Подключение между двумя Ideco NGFW Novum в туннельном режиме работы

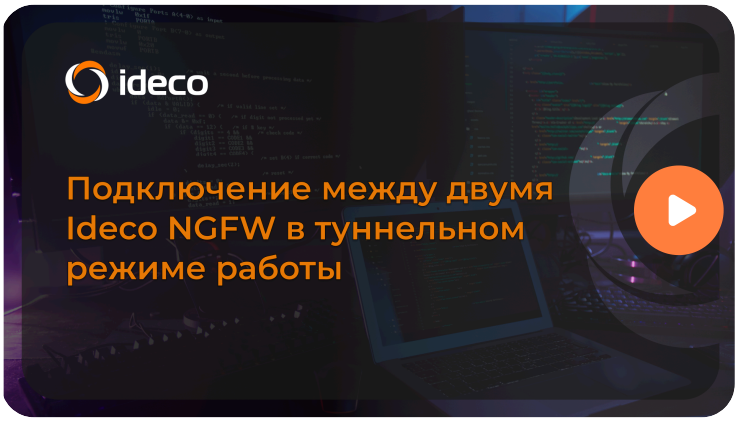
Функциональность доступна в **Классическом** и **Системном контекстах**.

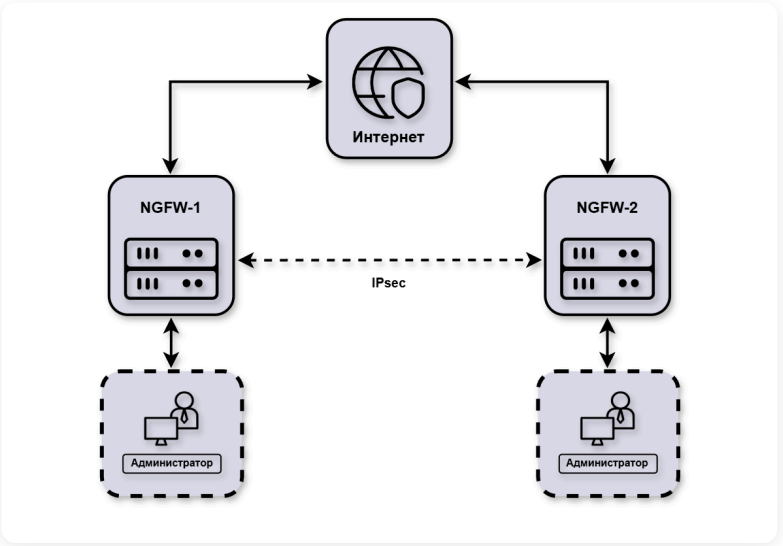
Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео





Для создания IPsec-подключения между Ideco NGFW Novum нужно настроить на одном NGFW Novum входящее подключение, а на другом NGFW Novum - исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключение, а на **NGFW-2** - входящее подключение.

Шаг 1. Проверка условий подключения

Перед созданием подключения убедитесь, что:

- На **NGFW-1** и **NGFW-2 правильно настроены временные зоны**. Без этого подключение не установится.
- Для работы IPsec все подсети, участвующие в соединениях, не пересекаются.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. **Входящее подключение должно настраиваться на сервере с белым IP-адресом**.
- Пользовательские правила из раздела **Правила трафика** → **Межсетевой экран** → **INPUT** не блокируют входящий трафик для протоколов ESP и UDP (порты 500 и 4500), поступающий на внешние интерфейсы **NGFW-2**.
- Сети для VPN-подключений у **NGFW-1** и **NGFW-2** не пересекаются.

Шаг 2. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в **Сервисы → IPsec → Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:

Добавление подключения

Название подключения

Зона

Режим работы

- Туннельный
  VTI
- Транспортный
  GRE over IPsec

Адрес удалённого устройства

Домен или IP-адрес

Интерфейс подключения

IP-адрес интерфейса туннеля

Заполните для проверки доступности сетей за удалённым NGFW Novum. Пример: 10.100.0.1/16.

Удалённый IP-адрес туннеля

Укажите IP-адрес интерфейса и удалённый IP-адрес туннеля для сбора статистики (потери, задержка, джиттер). Адреса должны быть в одной подсети.

IPsec-политики

- [x] Автоматическое создание маршрутов
  При выборе подсети 0.0.0.0/0 маршрут создаваться не будет

Домашние локальные сети

Удалённые локальные сети

Тип аутентификации

- Сертификат
  Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
- PSK
  Обеспечивает низкий уровень безопасности, поддерживается большинством устройств

Запрос на подпись сертификата

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBuAIBADBWMQ4wDAYDVQQKDAVJZG
VjbzEMMAoGA1UECwwDVVRNMTYwNAYD
```

Подписанный сертификат NGFW Novum

Загрузить

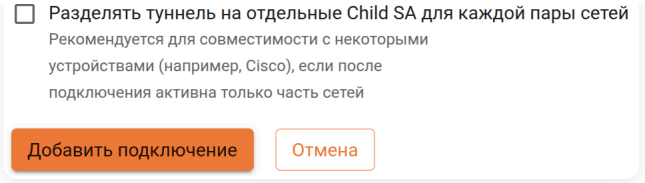
Корневой сертификат удалённого устройства

Загрузить

Дополнительно

Индекс интерфейса для Netflow

0



Расшифровка полей

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW Novum или белый IP-адрес другого Ideco NGFW Novum. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля:
  - При настройке BGP-соседства для динамической маршрутизации и сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**:
  - Для сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW Novum.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW Novum или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW Novum.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW Novum.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните сертификат для настройки входящего подключения.
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните ключ для настройки входящего подключения. Заполните поле **Идентификатор UTM**.

> Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.
>
> Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно настроить статические маршруты до удаленных локальных сетей NGFW в **Сервисы → Маршрутизация** или динамическую маршрутизацию через BGP в **Сервисы → BGP**.

3. Выполните действие для нужного типа аутентификации:

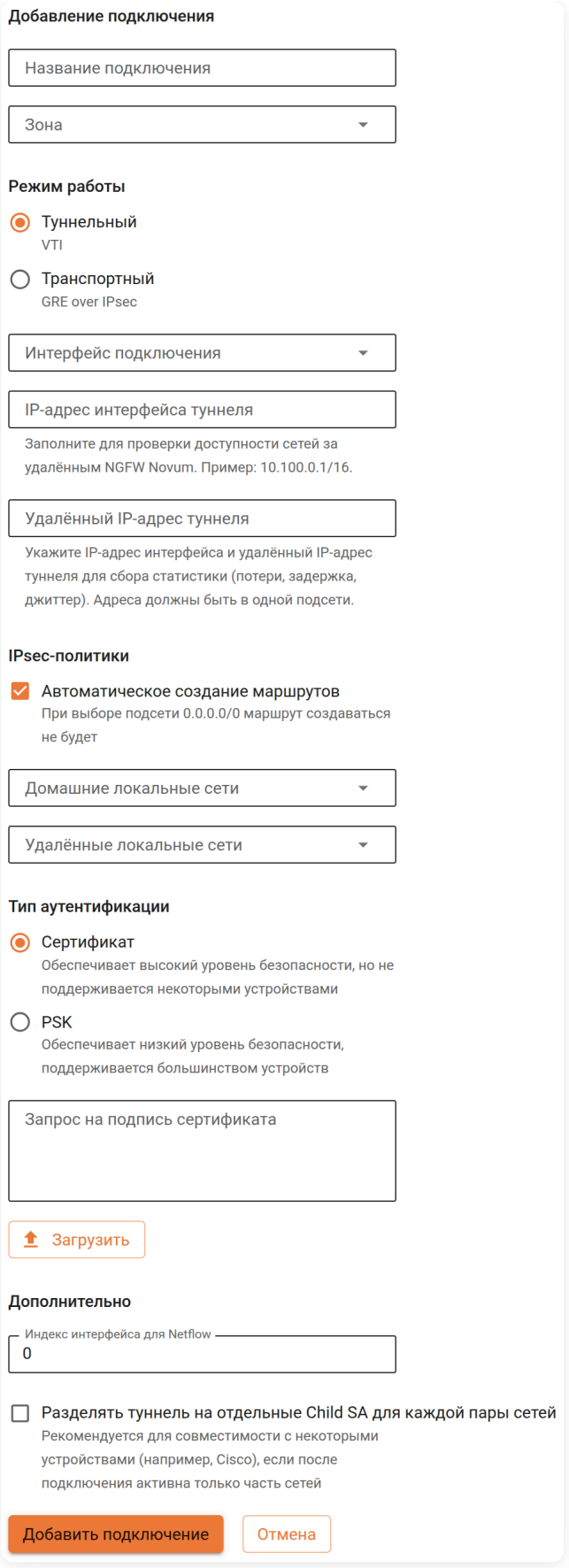
- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 3**.
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 3** для настройки входящего подключения на **NGFW-2**.

Шаг 3. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в **Сервисы → IPsec → Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля:
  - При настройке BGP-соседства для динамической маршрутизации и сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**:
  - Для сбора статистики обмена пакетами.
  - Для обеспечения доступа Ideco NGFW Novum к удаленным сетям за IPsec туннелем. Например, для доступа пользователей к ресурсам в личном кабинете.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW Novum.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW Novum или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW Novum.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW Novum.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - **Сертификат** - заполните поле **Запрос на подпись сертификата**, вставив значение сохраненное при первоначальной настройке исходящего подключения.
  - **PSK** - заполните поле **PSK ключ**, вставив значение сохраненное при первоначальной настройке исходящего подключения. Заполните поле **Идентификатор удаленной стороны**.

> Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно настроить статические маршруты до удаленных локальных сетей NGFW Novum в **Сервисы** → **Маршрутизация** или динамическую маршрутизацию через BGP в **Сервисы** → **BGP**.

3. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

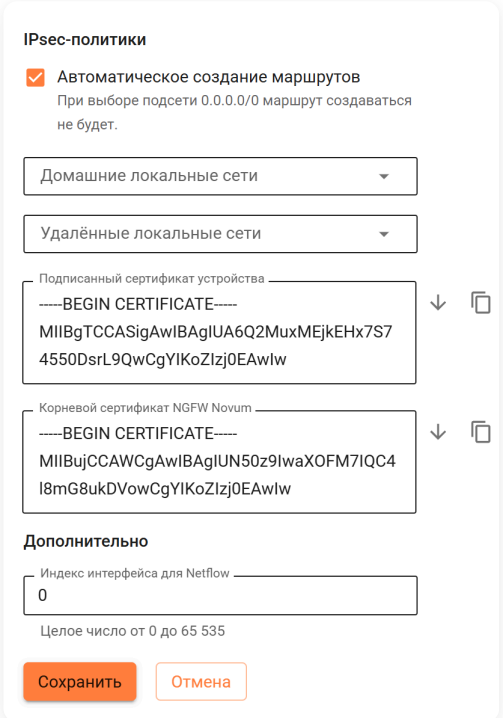
Если был выбран тип аутентификации **PSK**, то настройка завершена.

Если был выбран тип аутентификации **Сертификат**, то выполните **Шаг 4**.

Шаг 4. Донастройка исходящего подключения с типом аутентификации Сертификат

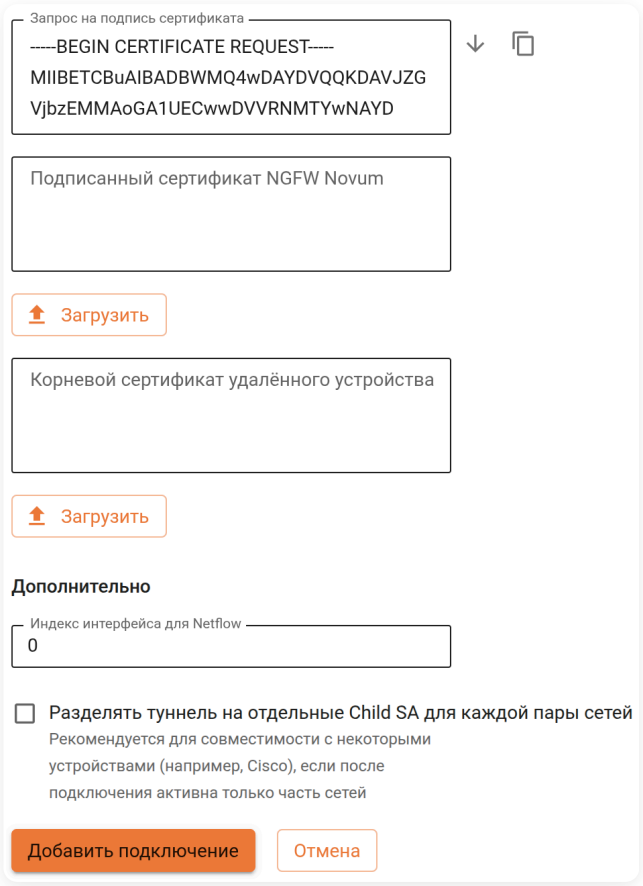
1. В **NGFW-2** перейдите в **Сервисы** → **IPsec** → **Входящие подключения** и нажмите  по ранее созданному входящему подключению.

2. Скопируйте поля **Подписанный сертификат устройства** и **Корневой сертификат NGFW**:



3. В **NGFW-1** перейдите в **Сервисы** → **IPsec** → **Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** значениями, ранее скопированными из **NGFW-2**:



5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

> Если соединение по IPsec не устанавливается, воспользуйтесь статьей.

Настройка доступа к локальным сетям по VPN из NGFW-1 к NGFW-2

Для доступа к локальным сетям по VPN из **NGFW-1** к **NGFW-2** выполните действия:

1. Перейдите к редактированию настроенного IPsec-подключения на **NGFW-2**.

2. Укажите в поле **Домашние локальные сети** сеть, используемую для VPN в **NGFW-2**.

> В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение между двумя Ideco NGFW Novum в транспортном режиме работы

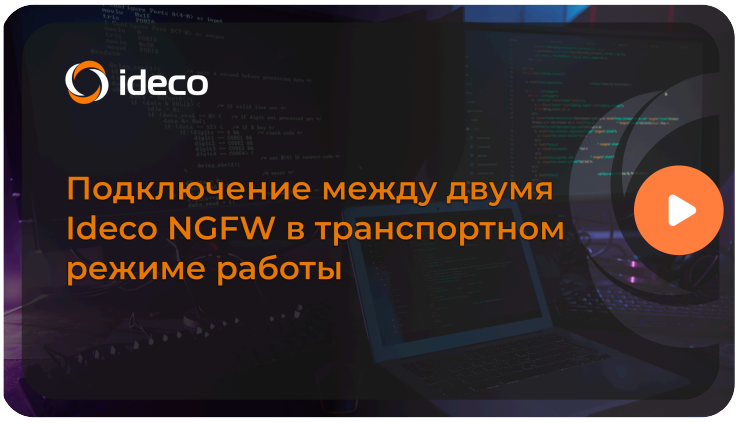
Функциональность доступна в **Классическом** и **Системном контекстах**.

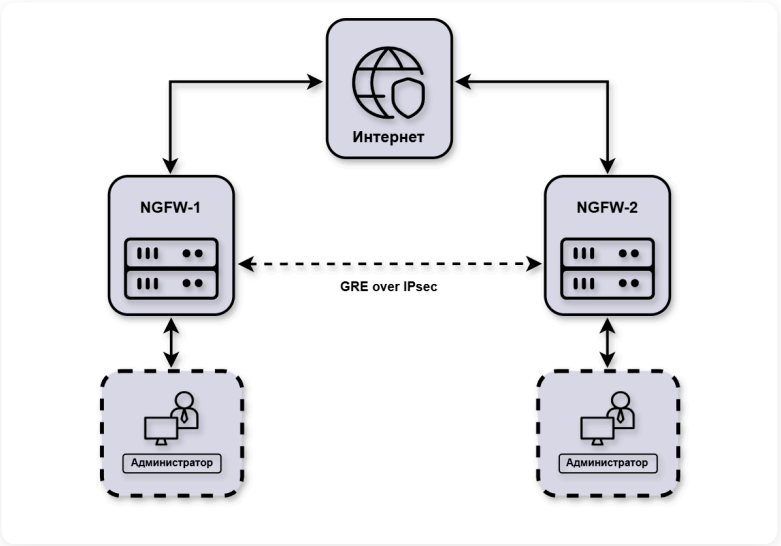
Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube | RUTUBE | VK Видео





GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

При замене/перевыпуске корневого сертификата в разделе Сертификаты, IPsec-подключения перестанут работать и необходимо будет пересоздать.

Перед настройкой убедитесь, что:

- В каждой из подключаемых сторон **правильно настроена временная зона**. Без этого установить подключение невозможно.
- Пользовательские правила из раздела **Правила трафика** → **Межсетевой экран** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW Novum для протоколов ESP и UDP (порты 500 и 4500).
- Пользовательские правила из раздела **Правила трафика** → **Межсетевой экран** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW Novum для протокола GRE.
- Ни один Ideco NGFW Novum не находится за NAT, так как в таком случае подключение двух Ideco NGFW Novum в транспортном режиме недоступно.
- Все IP-подсети, участвующие в соединениях не должны пересекаться и, тем более, не должны совпадать.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. Входящее подключение должно настраиваться на сервере с белым IP-адресом.

- Сети для VPN-подключений у двух NGFW не пересекаются.

Для создания IPsec подключения между Ideco NGFW Novum нужно настроить на одном NGFW входящее подключение, а на другом NGFW исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключение, а на **NGFW-2** входящее подключение.

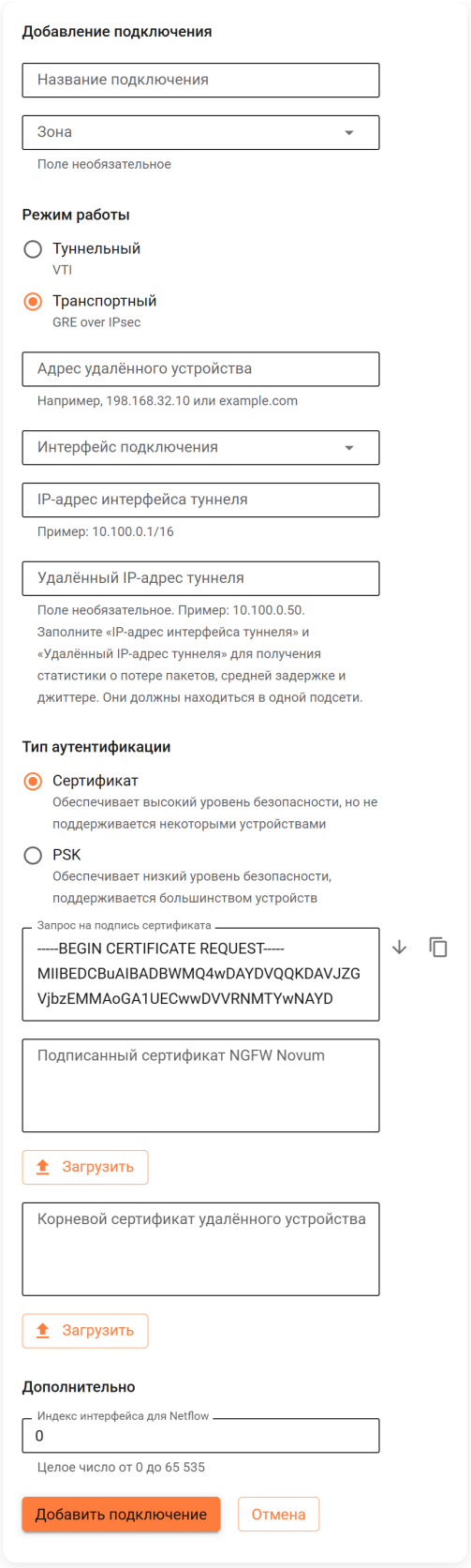
Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

Шаг 1. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в **Сервисы** → **IPsec** → **Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Название подключения** - максимальное количество символов 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW Novum или белый IP-адрес другого Ideco NGFW Novum. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните его для настройки входящего подключения.
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните его для настройки входящего подключения. Заполните поле **Идентификатор NGFW**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Если тип аутентификации:

- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 2**.
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 2** для настройки входящего подключения на другом NGFW.



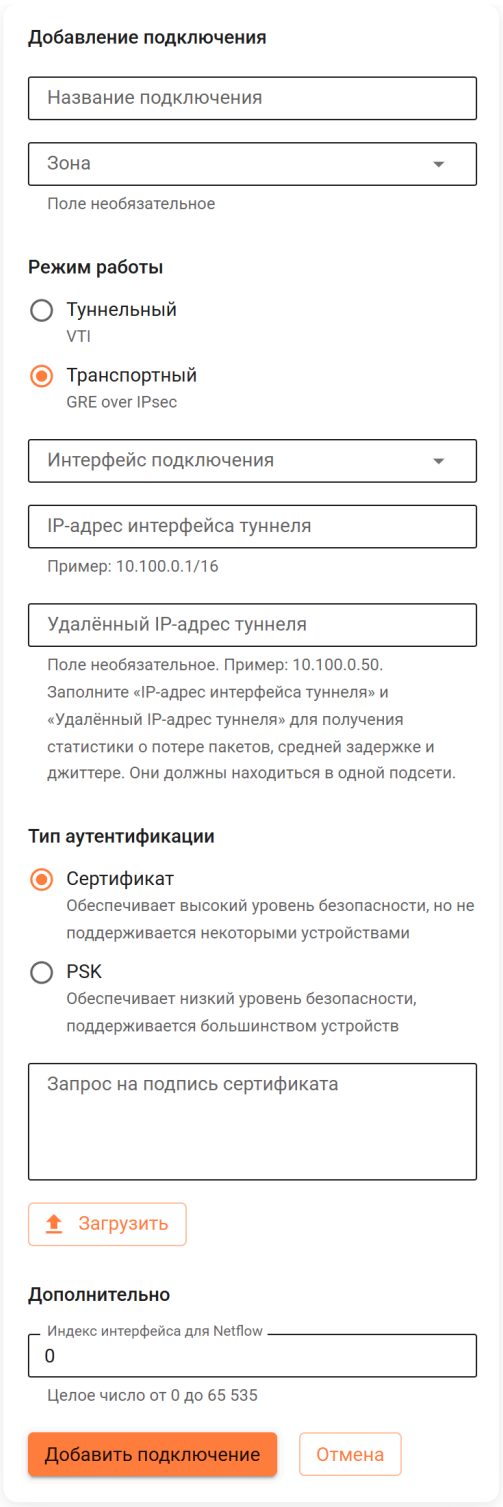
В поле **Интерфейс подключения** при выборе Loopback-интерфейса обеспечьте сетевой доступ к IP-адресу этого интерфейса настройками маршрутизации.

Шаг 2. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в **Сервисы** → **IPsec** → **Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - **Сертификат** - заполните поле **Запрос на подпись сертификата**, вставив значение сохраненное при первоначальной настройке исходящего подключения.
  - **PSK** - заполните поле **PSK ключ**, вставив значение сохраненное при первоначальной настройке исходящего подключения.Заполните поле **Идентификатор удаленной стороны**.

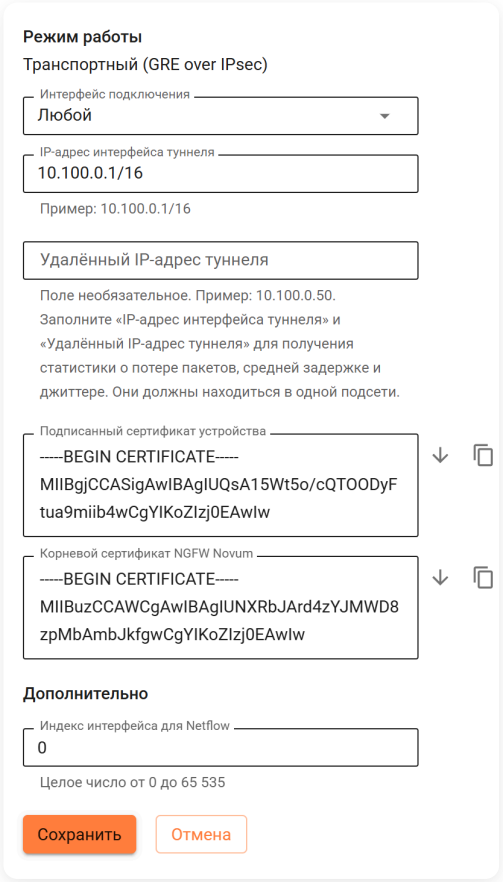
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Шаг 3. Донастройка исходящего подключения с типом аутентификации Сертификат

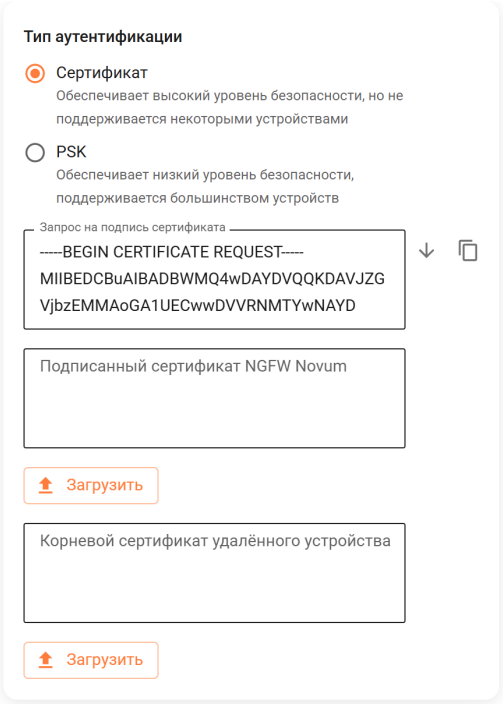
1. В **NGFW-2** перейдите в **Сервисы** → **IPsec** → **Входящие подключения** и нажмите по ранее созданному входящему подключению.

2. Скопируйте поля **Подписанный сертификат устройства** и **Корневой сертификат NGFW**:



3. В **NGFW-1** перейдите в **Сервисы** → **IPsec** → **Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** ранее скопированным значением при редактировании входящего подключения:



5. Нажмите **Сохранить**.

Шаг 4. Настройка маршрутизации

Маршрутизацию можно настроить тремя способами:

- Статические маршруты до локальных сетей удаленного NGFW в разделе **Сервисы** → **Маршрутизация**.
- Динамическая маршрутизация через BGP в разделе **Сервисы** → **BGP**.
- Динамическая маршрутизация через OSPF в разделе **Сервисы** → **OSPF**.

Рекомендуем для настройки маршрутизации использовать OSPF, в этом случае нет необходимости вручную настраивать маршруты до локальных сетей филиалов.

Также настройками OSPF можно определить приоритет направления трафика для резервирования каналов при создании нескольких IPSec-подключений.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Ideco NGFW Novum и MikroTik по IPsec в туннельном режиме

Функциональность доступна в **Классическом** и **Системном контекстах**.

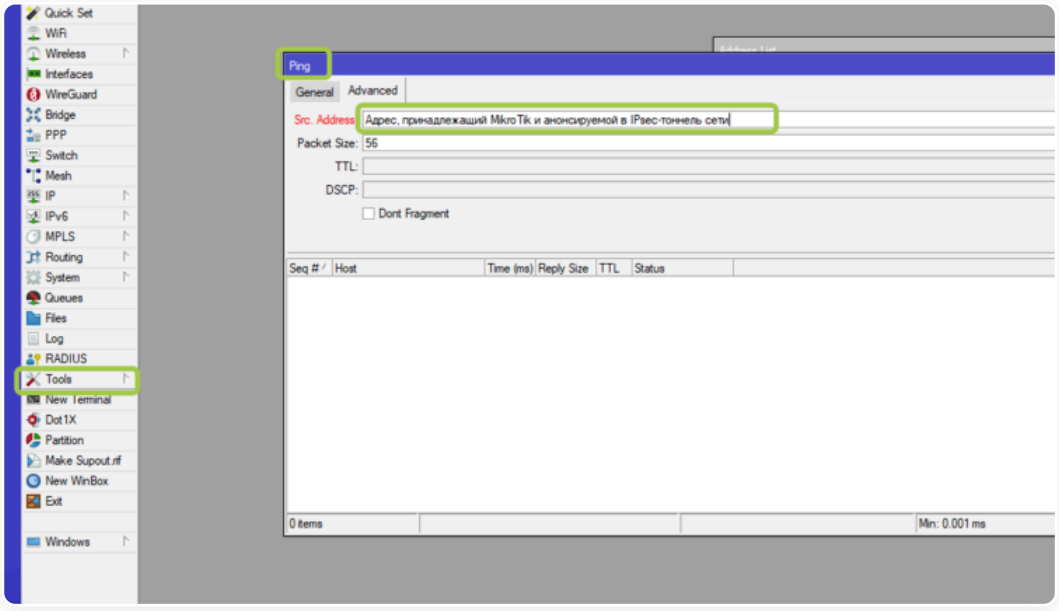
В статье описана настройка IPsec-подключения между Ideco NGFW Novum и MikroTik с аутентификацией по сертификатам или PSK. Локальные сети в разных офисах не должны пересекаться.

Требования и подготовка

Основные требования:

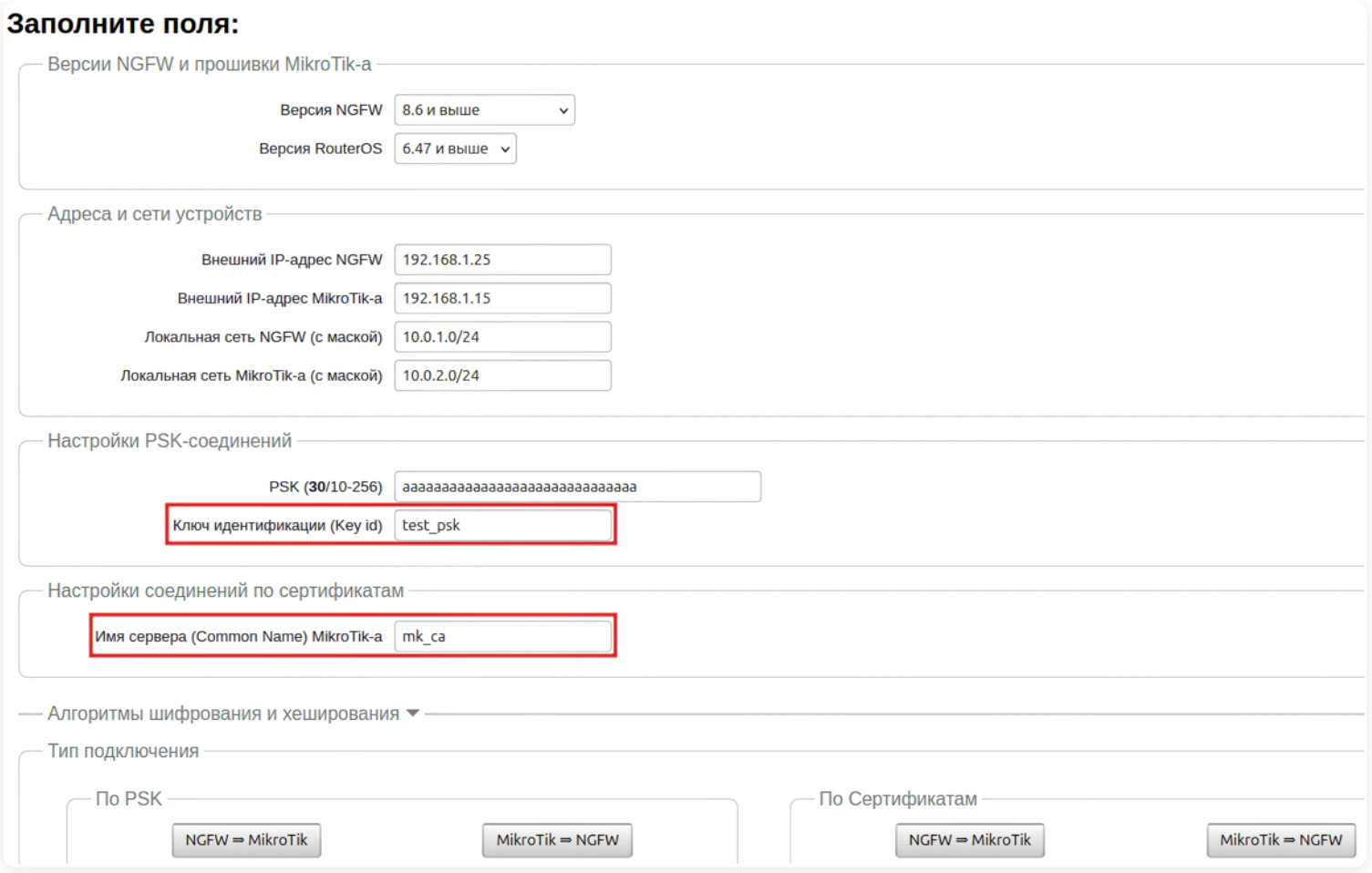
- Локальные сети в разных офисах не должны пересекаться.
- Для корректной работы подключений по сертификатам убедитесь, что время на Ideco NGFW Novum и MikroTik совпадает. Расхождение времени между устройствами приведет к ошибкам аутентификации. Рекомендуется настроить NTP-клиент на каждом из устройств.
- IPsec-подключения от Ideco NGFW Novum к MikroTik версии 6.45 и ниже по сертификатам не работают, так как нельзя использовать современные криптоалгоритмы.

Для проверки доступности анонсируемых сетей Ideco NGFW Novum с MikroTik указывайте IP-адрес источника:



При подключении нескольких устройств MikroTik к одному Ideco NGFW Novum **в туннельном режиме** через конфигуратор скриптов для MikroTik рекомендуем:

- Для PSK - укажите разные **Идентификаторы ключа (key-id)** для каждого устройства.
- Для сертификатов - укажите разные **Имена сервера (Common Name)** для каждого устройства:



Подключение от Ideco NGFW Novum к MikroTik

Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

Шаг 1. Настройка Ideco NGFW Novum (исходящее подключение)

Сгенерируйте запрос на подпись сертификата:

1. В Ideco NGFW Novum откройте **Сервисы** → **IPsec** → **Исходящие подключения**, нажмите **Добавить** и заполните поля:

Добавление подключения

Название подключения

Зона

Режим работы

- Туннельный
  VTI
- Транспортный
  GRE over IPsec

Адрес удалённого устройства

Домен или IP-адрес

Интерфейс подключения

IP-адрес интерфейса туннеля

Заполните для проверки доступности сетей за удалённым NGFW Novum. Пример: 10.100.0.1/16.

Удалённый IP-адрес туннеля

Укажите IP-адрес интерфейса и удалённый IP-адрес туннеля для сбора статистики (потери, задержка, джиттер). Адреса должны быть в одной подсети.

IPsec-политики

- [x] Автоматическое создание маршрутов
  При выборе подсети 0.0.0.0/0 маршрут создаваться не будет

Домашние локальные сети

Удалённые локальные сети

Тип аутентификации

- Сертификат
  Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
- PSK
  Обеспечивает низкий уровень безопасности, поддерживается большинством устройств

Запрос на подпись сертификата

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBuAIBADBWMQ4wDAYDVQQKDAVJZG
VjbzEMMAoGA1UECwwDVVRNMTYwNAYD
```

Подписанный сертификат NGFW Novum

Загрузить

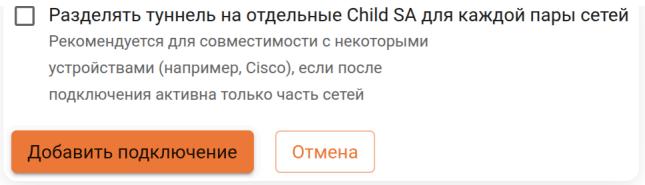
Корневой сертификат удалённого устройства

Загрузить

Дополнительно

Индекс интерфейса для Netflow

0



Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - укажите внешний IP-адрес MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **Сертификат**.
- **Запрос на подпись сертификата** - будет сгенерирован **запрос, который необходимо отправить для подписи на MikroTik**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. После подписания запроса необходимо продолжить настройку подключения в Ideco NGFW Novum.

> **Не закрывайте вкладку с настройками.** При закрытии вкладки **Запрос на подпись сертификата** изменит значение и процесс подписания файла **NGFW.csr** потребуется повторить.

Шаг 2. Настройка MikroTik (входящее подключение)

Файл **NGFW.csr**, полученный из Ideco NGFW Novum, необходимо загрузить в файловое хранилище MikroTik:

1. Откройте раздел **File**.

2. Нажмите кнопку **Browse**.

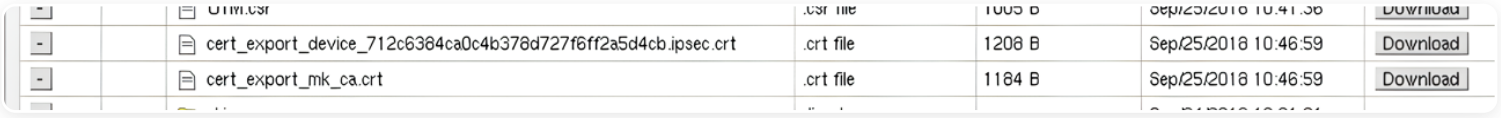
3. Выберите и загрузите файл.

Настроить MikroTik можно через:

- GUI.
- Консоль устройства.
- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт. Вставьте в скрипт код, сгенерированный конфигуратором, затем запустите.

В файловой системе MikroTik появятся два файла, которые необходимо скачать, чтобы впоследствии загрузить на NGFW:



Файл `cert_export_device_<случайный набор символов>.ipsec.crt` - подписанный сертификат NGFW.

Файл `cert_export_mk_ca.crt` - корневой сертификат MikroTik.

Шаг 3. Завершение настройки Ideco NGFW Novum

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW Novum.

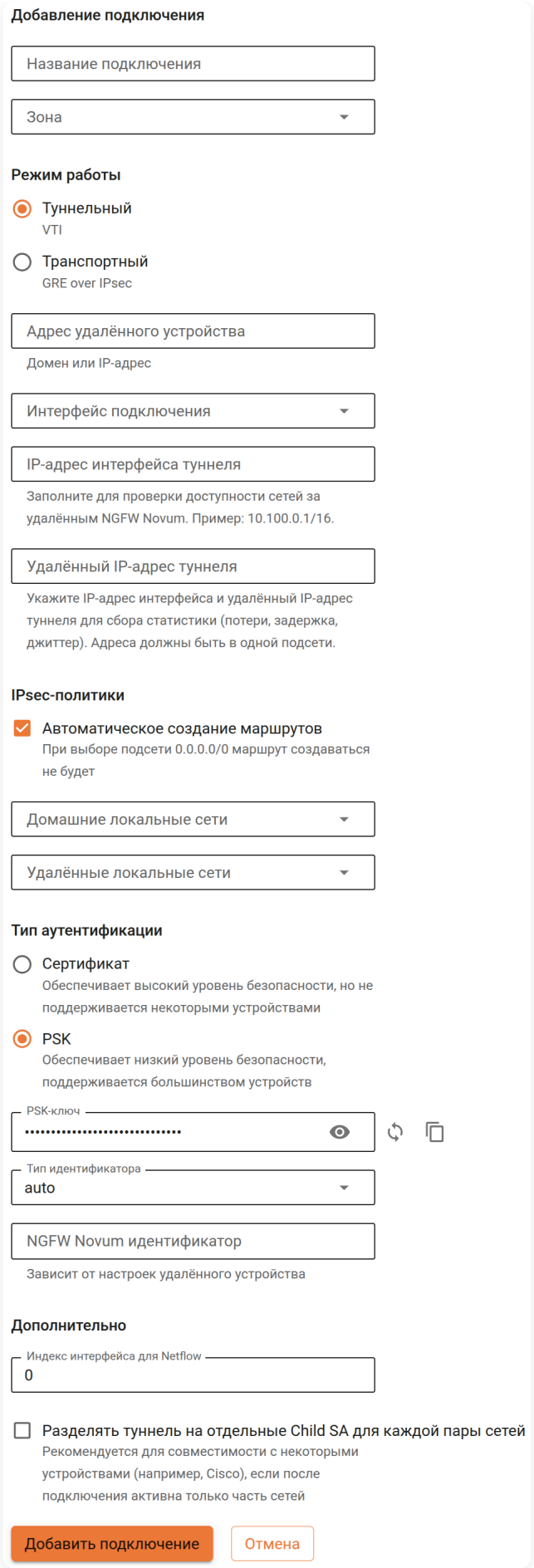
1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

PSK

Шаг 1. Настройка Ideco NGFW Novum (исходящее подключение)

1. Откройте **Сервисы** → **IPsec** → **Исходящие подключения**, нажмите **Добавить** и заполните поля:

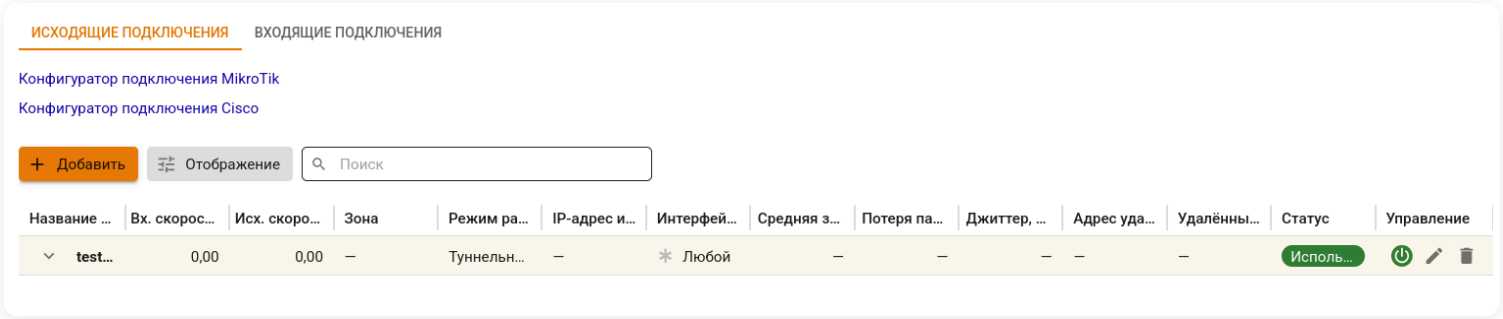


Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.

- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - укажите внешний IP-адрес MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **PSK**. В поле **PSK-ключ** будет сгенерирован случайный PSK-ключ для настройки подключения в MikroTik.
- **Тип идентификатора** - выберите **auto**.
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего IPsec-подключения в MikroTik.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. После заполнения всех полей нажмите **Добавить подключение**. В списке подключений появится созданное подключение:



Шаг 2. Настройка MikroTik (входящее подключение)

Настроить MikroTik можно через:

- GUI.
- Консоль устройства.
- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт. Вставьте в скрипт код, сгенерированный конфигуратором, и запустите.

Подключение от MikroTik к Ideco NGFW Novum

Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

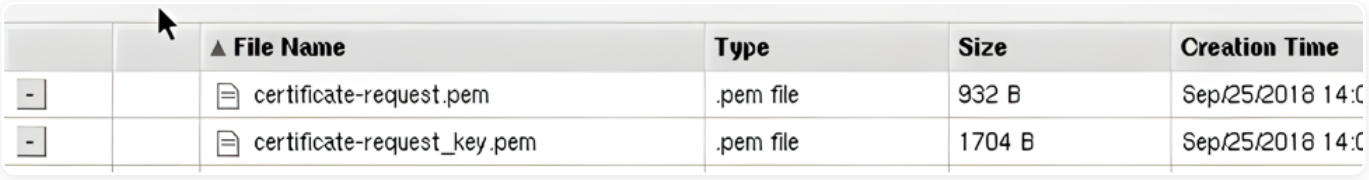
Шаг 1. Предварительная настройка MikroTik

Настроить MikroTik можно через:

- GUI.
- Консоль устройства.
- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт для генерации запроса на подпись сертификата. Вставьте в скрипт код, сгенерированный конфигуратором, и запустите. Конфигуратором генерируется два скрипта, поэтому в MikroTik также создайте два скрипта.

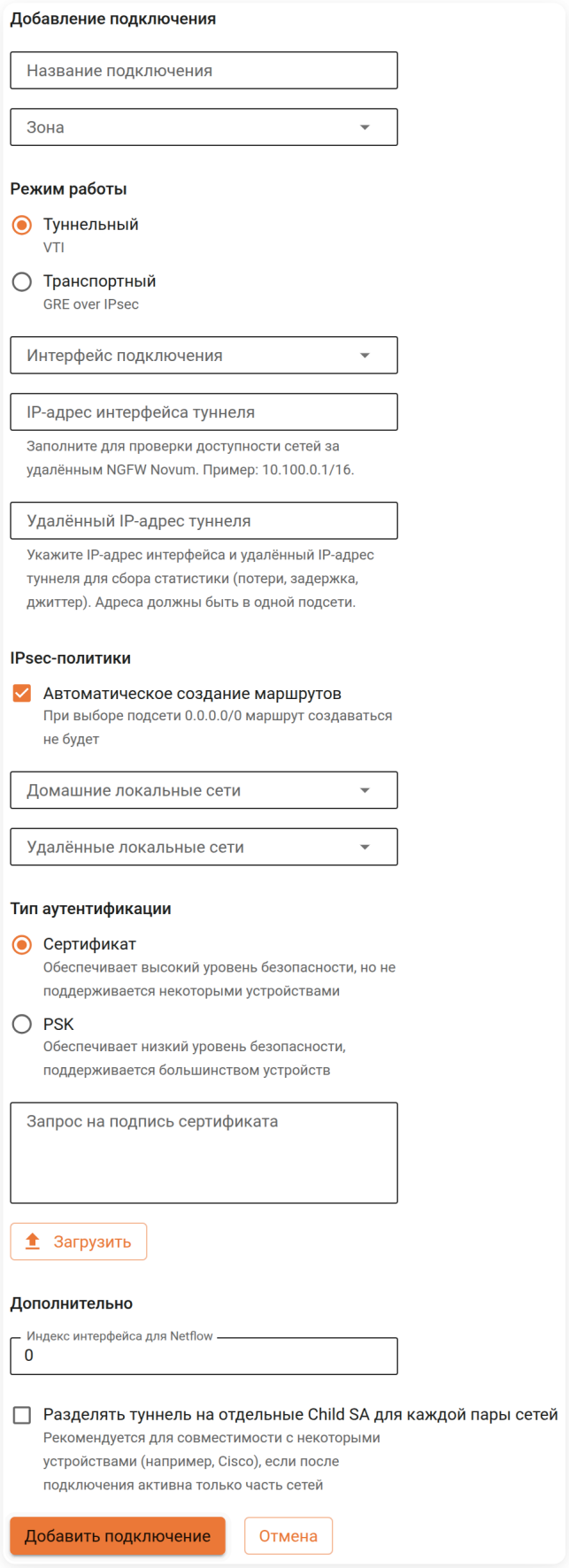
Перед настройкой необходимо запустить первый скрипт для запроса на подпись сертификата. После чего в файловом хранилище MikroTik появятся два файла, которые необходимо скачать. Файлы потребуются для дальнейшей настройки:



- Файл `certificate-request.pem` - запрос на подпись сертификата.
- Файл `certificate-request_key.pem` - приватный ключ.

Шаг 2. Настройка Ideco NGFW Novum (входящее подключение)

1. В Ideco NGFW Novum откройте **Сервисы** → **IPsec** → **Входящие подключения**, нажмите **Добавить** и заполните поля:

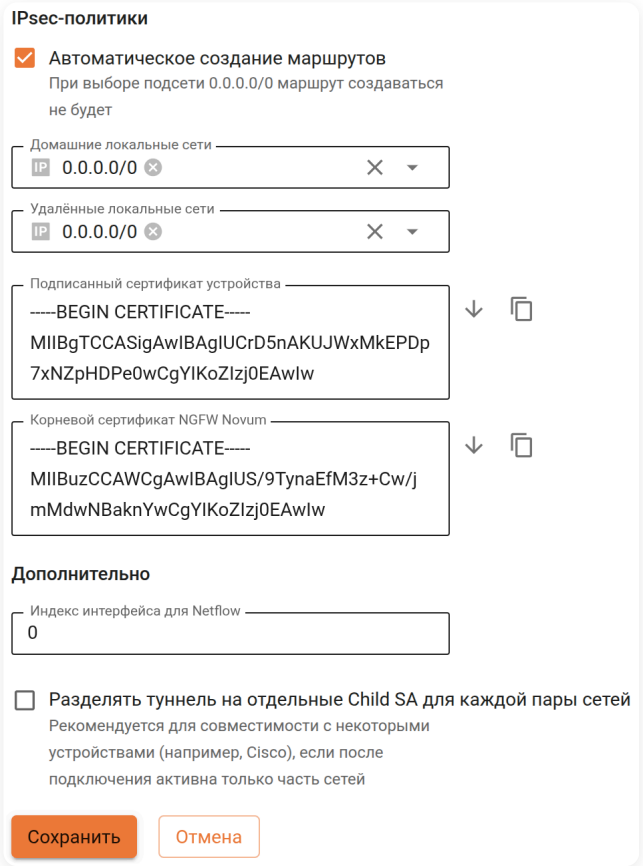


Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону, в которую требуется добавить IPsec-подключение. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **Сертификат**.
- **Запрос на подпись сертификата** - загрузите запрос на подпись, **полученный от MikroTik**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Нажмите кнопку **Добавить подключение**. Нажмите на кнопку редактирования соединения ( ), чтобы продолжить настройку.

3. Откройте созданное IPsec-соединение, нажав на , и скачайте файлы **Подписанного сертификата устройства** (`device.crt`) и **Корневого сертификата NGFW** (`NGFW.crt`):



Шаг 3. Настройка MikroTik (исходящее подключение)

1. Загрузите на MikroTik скачанные ранее файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`) через WinBox или по SSH.

2. Запустите второй сгенерированный конфигуратором скрипт.

PSK

Шаг 1. Настройка MikroTik (исходящее подключение)

Настроить устройство MikroTik можно через:

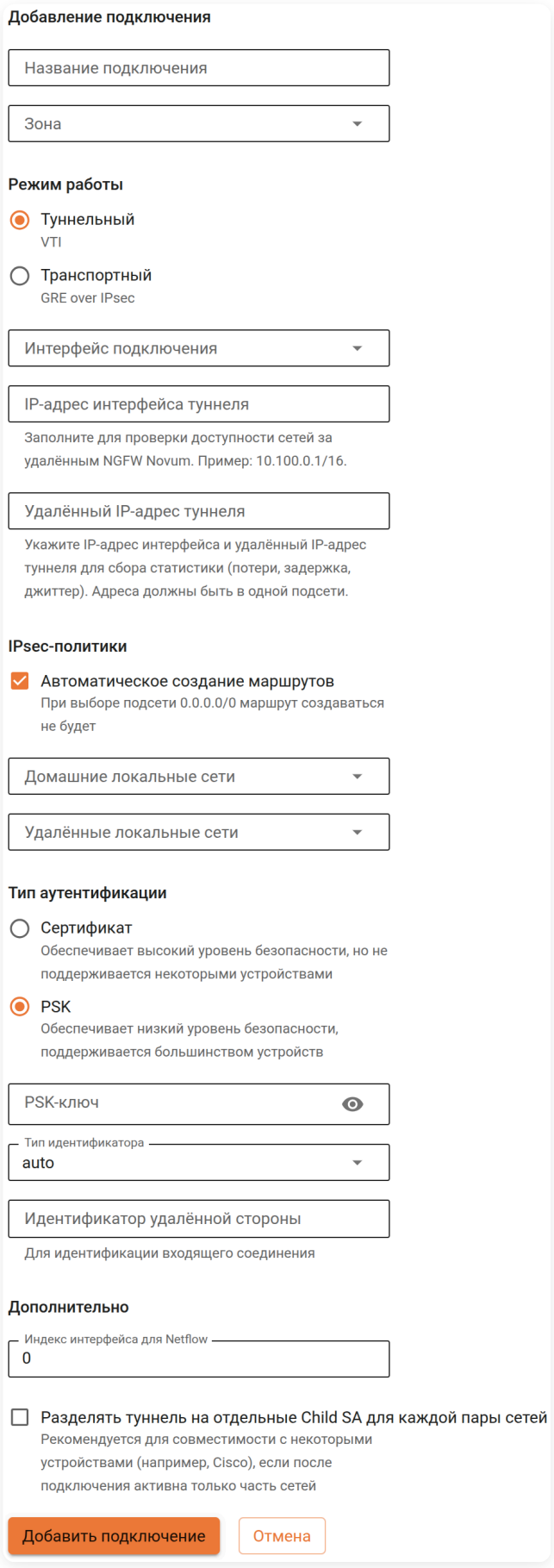
- GUI.
- Консоль устройства.

- Конфигурационные скрипты (https://mikrotik.ideco.ru/).

После генерации скрипта откройте **System** → **Scripts** и создайте скрипт. Вставьте в скрипт код, сгенерированный конфигуратором, и запустите.

Шаг 2. Настройка Ideco NGFW Novum (входящее подключение)

1. В Ideco NGFW Novum откройте **Сервисы** → **IPsec** → **Входящие подключения**, нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - вставьте PSK-ключ, полученный от MikroTik.
- **Тип идентификатора** - выберите **keyid**.
- **Идентификатор удаленной стороны** - вставьте идентификатор MikroTik (параметр key-id в `/ip ipsec peers`).
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Нажмите кнопку **Добавить подключение**.

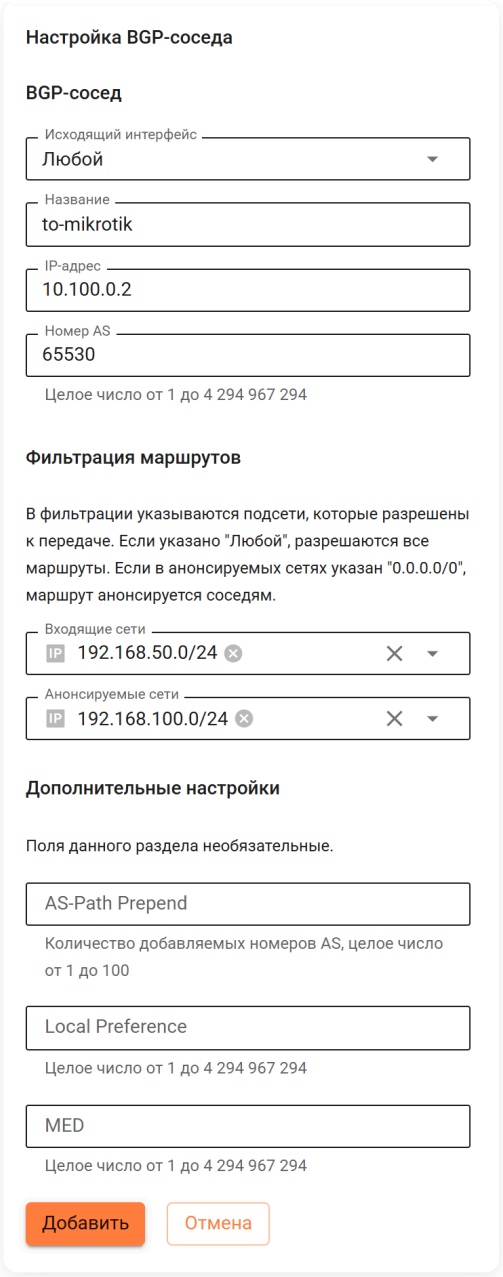
Настройка динамической маршрутизации (BGP)

Настройка Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в поле **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:



Расшифровка полей

- **Исходящий интерфейс** - выберите **Любой**.
- **Название** - любое значение.
- **IP-адрес** - укажите IP-адрес интерфейса туннеля MikroTik.
- **Номер AS** - номер автономной системы MikroTik.
- **Входящие сети** - укажите локальные сети MikroTik.
- **Анонсируемые сети** - укажите локальные сети Ideco NGFW Novum.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

5. Включите модуль **BGP**.

Настройка MikroTik

1. Настройте общий шаблон BGP:

```
/routing bgp template set default address-families=ip disabled=no output.default-originate=always router-id=<Router-ID MikroT
```

2. Добавьте BGP-сессию с Ideco NGFW Novum:

```
/routing bgp connection add address-families=ip as=<AS MikroTik> disabled=no local.role=ebgp-peer name=<Имя подключения> outp
```

Возможные проблемы

Соединение не устанавливается при повторной активации

Если после отключения VPN-подключение не восстанавливается, удаленное устройство заблокировано fail2ban. Сбросьте блокировки по IP на Ideco NGFW Novum. Подробнее в статье Защита от брутфорс-атак.

Fail2ban отслеживает в log-файлах попытки обратиться к сервисам и, если находит повторяющиеся неудачные попытки авторизации с одного и того же IP-адреса или хоста, блокирует IP-адрес.

Соединение периодически разрывается

При работе туннеля между Ideco NGFW Novum и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW Novum.

Для автоматизации процесса поддержания соединения создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW Novum:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в **System** → **Scripts**.

3. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



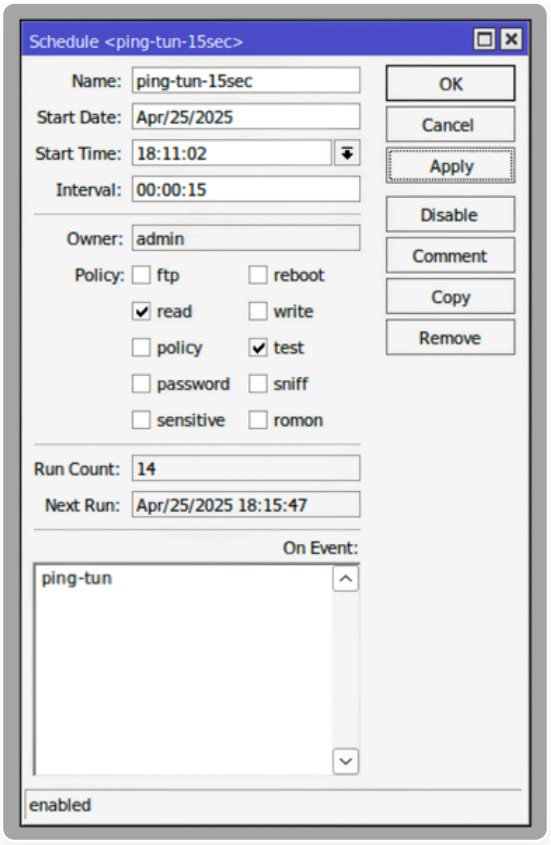
- **Name** - название скрипта (не поддерживаются пробелы и нижние подчеркивания).
- **Policy** - включите опции **read** и **test**.
- **Source** - введите команду `ping <IP-адрес Ideco NGFW Novum> count=3`.

4. Нажмите **Apply**, затем **Ok**.

Далее настройте запуск скрипта по расписанию в планировщике заданий:

1. Перейдите в **System** → **Scheduler**.

2. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



- **Name** - название задания (не поддерживаются пробелы и нижние подчеркивания).
- **Interval** - интервал 00:00:15 (каждые 15 секунд).
- **Policy** - включите опции **read** и **test**.
- **On Event** - введите название созданного ранее скрипта.

3. Нажмите **Apply**, затем **Ok**.

По завершению настройки MikroTik каждые 15 секунд будет отправлять три ICMP-запроса на адрес Ideco NGFW Novum. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Ideco NGFW Novum и MikroTik по IPsec в транспортном режиме

Функциональность доступна в **Классическом** и **Системном контекстах**.

При объединении сетей с помощью VPN локальные сети в разных офисах не должны пересекаться.

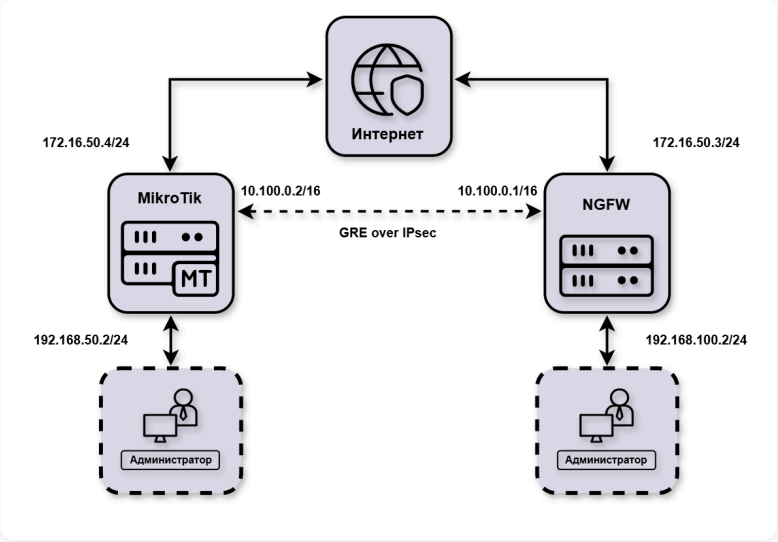
Для корректной работы подключений по сертификатам убедитесь, что время на Ideco NGFW Novum и MikroTik совпадает. Расхождение времени между устройствами приведет к ошибкам аутентификации. Рекомендуется настроить NTP-клиент на каждом из устройств.

IPsec-подключения от Ideco NGFW Novum к MikroTik по сертификатам к MikroTik версии 6.45 и ниже не работают, так как нельзя использовать современные криптоалгоритмы.

GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

Рассмотрим настройку подключения по схеме:



- `172.16.50.3/24` - внешний IP-адрес NGFW.
- `192.168.100.2/24` - локальный IP-адрес NGFW.
- `10.100.0.1/30` - IP-адрес GRE-туннеля NGFW.
- `172.16.50.4/24` - внешний IP-адрес MikroTik.
- `192.168.50.2/24` - локальный IP-адрес MikroTik.
- `10.100.0.2/30` - IP-адрес GRE-туннеля MikroTik.

Для настройки подключения MikroTik и Ideco NGFW Novum следуйте инструкции в каждом из пунктов.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

PSK-ключ

Для PSK-ключа допустимы все печатные ASCII-символы (коды от 0x20 до 0x7E), включая:

- **Латинские буквы в верхнем и нижнем регистре** (A–Z, a–z).
- **Цифры** (0–9).
- **Пробел и специальные символы** (! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ { | } ~).

Подключение от Ideco NGFW Novum к MikroTik

Предварительная настройка MikroTik

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

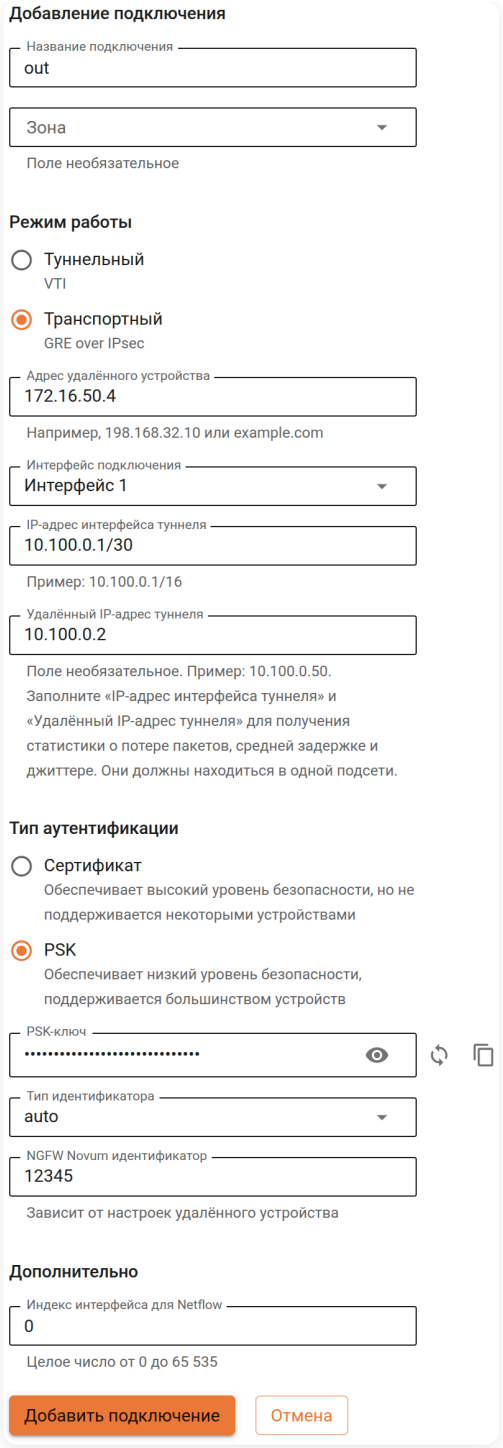
2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1 remote-address=172.16.50.3
/ip address add address=10.100.0.2/30 interface=gre-tunnel1 network=10.100.0.0
```

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на Ideco NGFW Novum

1. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - будет сгенерирован случайный PSK-ключ для настройки подключения в MikroTik.
- **Тип идентификатора** - выберите **keyid**.
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего подключения в MikroTik.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Настройка входящего IPsec-подключения на MikroTik

1. Настройте IPsec-подключение со стороны MikroTik:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256 name=from_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=from_192.168.100.0/24 enc-algorithms=aes-256-cbc name=172.16.50.3 pfs-g

/ip ipsec peer add address=172.16.50.3/32 comment=from_192.168.100.0/24 exchange-mode=ike2 name=from_192.168.100.0/24 passive

/ip ipsec identity add comment=from_192.168.100.0/24 peer=from_192.168.100.0/24 secret="<Сгенерированный NGFW PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.
```

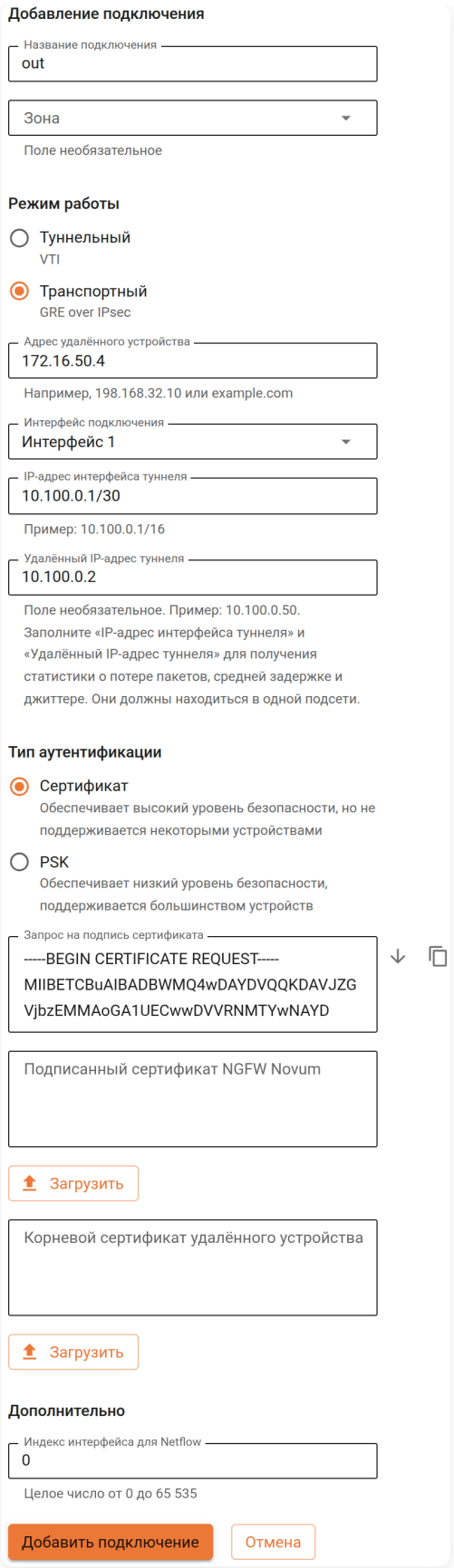
2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Тип аутентификации Сертификат

Настройка исходящего IPsec-подключения на Ideco NGFW Novum

1. Перейдите в **IPsec** → **Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.

- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Скачайте **Запрос на подпись сертификата**.

4. Не закрывая форму создания исходящего подключения NGFW, перейдите к настройке Mikrotik.

Настройка входящего IPsec-подключения на MikroTik

1. Загрузите скачанный ранее файл с **Запросом на подпись сертификата** (`NGFW.crt`) на MikroTik через WinBox или по SSH.

2. Создайте корневой сертификат MikroTik:

```
/certificate add common-name=mk_ca name=mk_ca_template key-usage=key-cert-sign,crl-sign,digital-signature,content-commitment
/certificate sign mk_ca_template ca-crl-host=172.16.50.4 name=mk_ca
```

3. Подпишите сертификат Ideco NGFW Novum и сделайте сертификат доверенным:

```
/certificate sign-certificate-request file-name=NGFW.csr ca=mk_ca
/certificate set [find name~"^device_.+\\.ipsec\$"] trusted=yes
```

4. Экспортируйте корневой сертификат MikroTik и подписанный сертификат NGFW в формат `.pem`:

```
/certificate export-certificate mk_ca type=pem
/certificate export-certificate [find name~"^device_.+\\.ipsec\$"] type=pem
```

5. Загрузите с MikroTik корневой сертификат MikroTik и подписанный сертификат NGFW через WinBox или по SSH. Названия файлов содержат `cert_export`.

6. Настройте входящее IPsec-соединение на MikroTik:

```
/ip ipsec profile add name=from_192.168.100.0/24 hash-algorithm=sha256 enc-algorithm=aes-256 dh-group=modp4096 dpd-interval=1

/ip ipsec peer add name=from_192.168.100.0/24 address=172.16.50.3/32 profile=from_192.168.100.0/24 exchange-mode=ike2 passive

/ip ipsec identity add peer=from_192.168.100.0/24 auth-method=digital-signature certificate=mk_ca remote-certificate=[: put [

/ip ipsec proposal add name=172.16.50.3 enc-algorithms=aes-256-cbc auth-algorithms=sha256 pfs-group=modp4096 comment=from_192

/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.
```

7. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Донастройка исходящего IPsec-подключение на Ideco NGFW Novum

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW Novum.

1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

3. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Подключение от MikroTik к Ideco NGFW Novum

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на MikroTik

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1 remote-address=172.16.50.3
/ip address add address=10.100.0.2/30 interface=gre-tunnel1 network=10.100.0.0
```

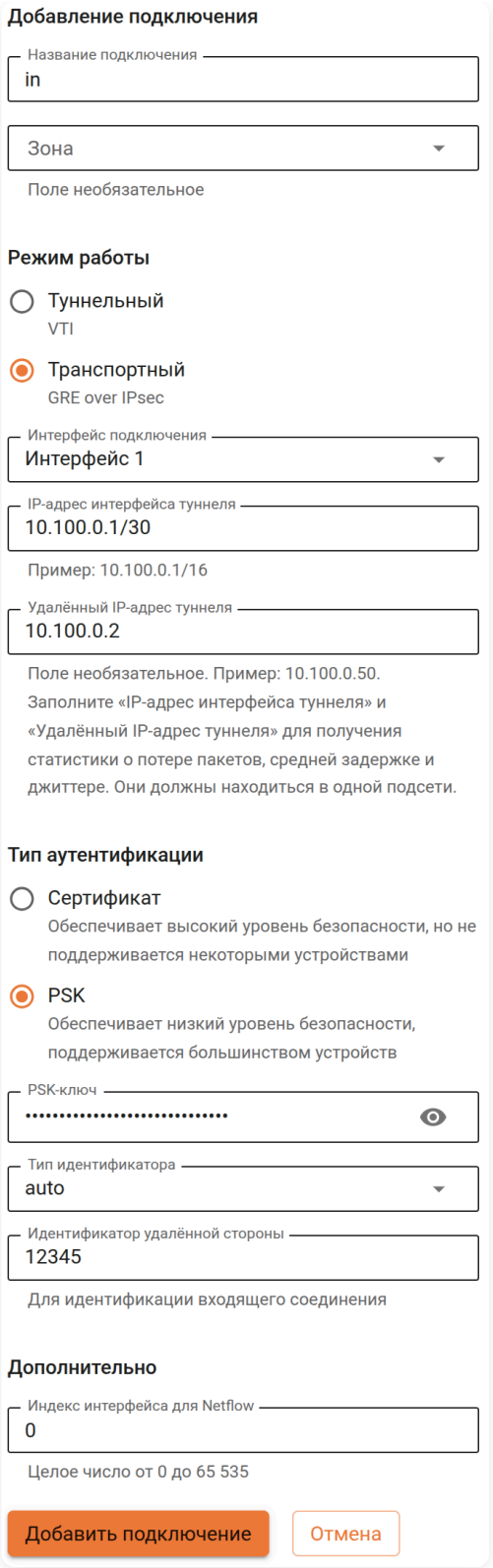
3. Настройте IPsec-подключение со стороны MikroTik:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256 name=to_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-algorithms=aes-256-cbc name=172.16.50.3 pfs-gro

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-mode=ike2 name=to_192.168.100.0/24 profile=to_

/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 my-id=key-id:"test_psk" secret="<PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.16
```

4. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Настройка входящего IPsec-подключения на Ideco NGFW Novum

1. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - введите PSK-ключ, указанный при настройке исходящего IPsec-подключения в MikroTik.
- **Тип идентификатора** - выберите **keyid**.

- **NGFW идентификатор** - введите **key-id**, использованный при настройке исходящего IPsec-подключения в MikroTik.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Тип аутентификации Сертификат

Предварительная настройка MikroTik

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1 remote-address=172.16.50.3
/ip address add address=10.100.0.2/30 interface=gre-tunnel1 network=10.100.0.0
```

3. Сгенерируйте запрос на подпись сертификата:

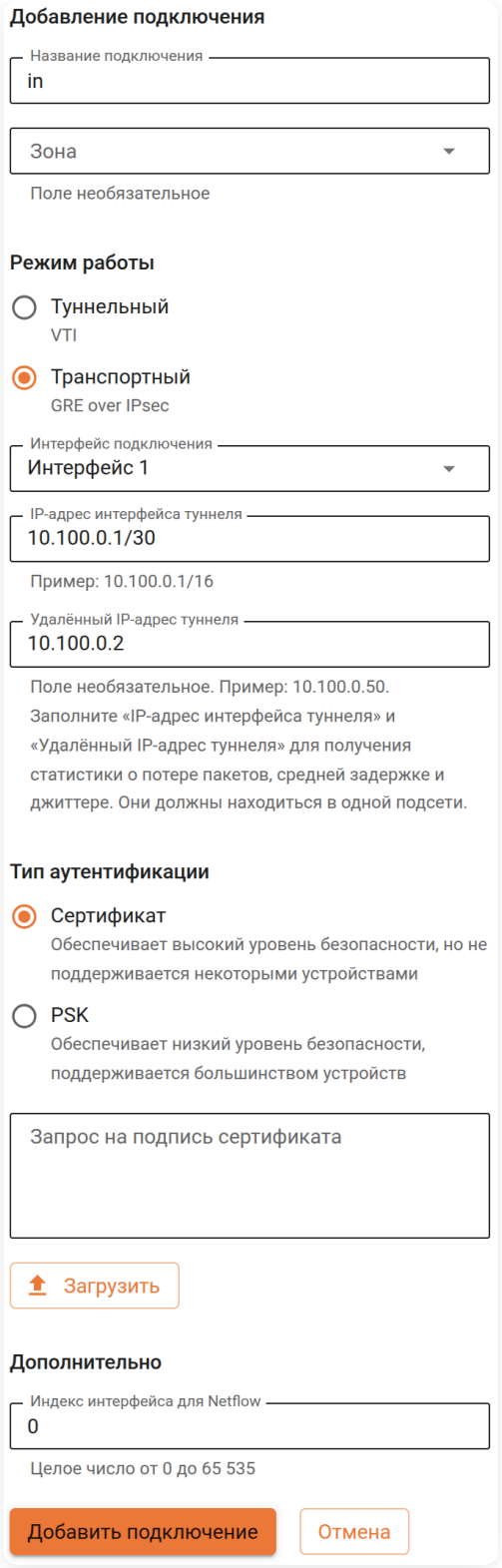
```
/certificate add name=mk_ca common-name=mk_ca key-usage=digital-signature,content-commitment
/certificate create-certificate-request key-passphrase="" template=mk_ca
```

4. Загрузите файл `certificate-request.pem` с MikroTik через WinBox или по SHH.

Настройка входящего IPsec-подключения на Ideco NGFW Novum

1. Перейдите в **IPsec** → **Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения. Подробнее об объекте **Зона** в статье.
- **Режим работы** - выберите **Транспортный** режим.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Загрузите скачанный ранее с MikroTik файл `certificate-request.pem` в поле **Запрос на подпись сертификата**.

4. Нажмите **Добавить подключение**.

5. Откройте созданное IPsec-соединение, нажав на , и загрузите файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`).

6. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Настройка исходящего IPsec-подключение на MikroTik

1. Загрузите на MikroTik скачанные ранее файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`) через WinBox или по SSH.

2. Импортируйте сертификаты:

```
/certificate import file-name=NGFW.crt passphrase=""
/certificate import file-name=device.crt passphrase=""
/certificate import file-name=certificate-request_key.pem passphrase=""
```

3. Настройте IPsec-соединение:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256 name=to_192.168.100.0/24 dpd-interval=120

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-mode=ike2 name=to_192.168.100.0/24 profile=to_

/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 auth-method=digital-signature certificate=device.

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-algorithms=aes-256-cbc name=172.16.50.3 pfs-gro

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.16.50.3 protocol=gre src-address=172.16
```

4. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

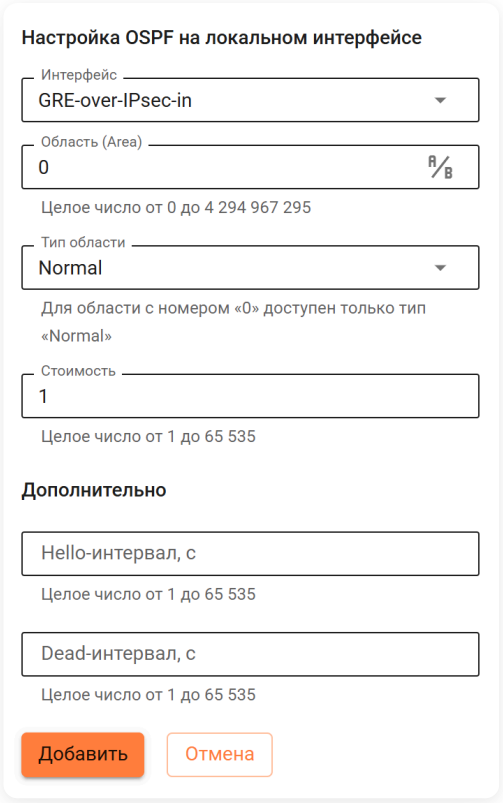
Настройка динамической маршрутизации

OSPF

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW Novum, настроенный ранее.
- **Область (Area)** - введите номер области (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Тип области** - для области с указанным номером `area` должен быть выбран одинаковый тип на всех OSPF-соседях. Для области с номером 0 (`0.0.0.0`) допустимо указывать только один тип - **Normal**. Допустимые значения: **Normal**, **Stub**, **NSSA**:
  - **Normal Area** (обычная зона) - стандартная зона OSPF, которая получает полную информацию о маршрутах как внутри автономной системы, так и за ее пределами. В такой зоне могут находиться как маршрутизаторы, так и конечные устройства.
  - **Stub Area** (усеченная зона) - зона, в которой не принимаются внешние маршруты (Type 5 LSA), но принимаются маршруты других зон. Вместо полной информации о внешних маршрутах используется маршрут по умолчанию.
  - **NSSA** (Not-So-Stubby Area) - разновидность stub-зоны, которая может получать маршруты по умолчанию и отправлять свои маршруты в другие зоны через **ABR** (Area Border Router). В **NSSA** зоне используется специальный тип LSA (Type 7), который преобразуется в Type 5 на ABR.
- **Стоимость** - введите стоимость маршрута.
- **Hello-интервал** - укажите время между отправкой Hello-пакетов, которое варьируется от 1 до 65535 секунд. Если поле не заполнено, по умолчанию используется значение 10 секунд. Для установления соседства между устройствами интервал должен быть одинаковым для всех участников сети.
- **Dead-интервал** - укажите время, через которое сосед считается недоступным, если не получает Hello-пакеты. Диапазон значений - от 1 до 65535 секунд. Если поле не заполнено, по умолчанию в 4 раза больше, чем Hello-интервал. Для успешного соседства значение должно быть одинаковым у всех устройств в сегменте сети.

3. Нажмите **Сохранить**.

4. Включите модуль **OSPF**.

Настройка на MikroTik (RouterOS 6.48.6)

1. Настройте область (значение `area`, должно совпадать на NGFW и Mikrotik):

```
/routing ospf area
add name=backbone area-id=0.0.0.0 type=default default-cost=1 inject-summary-lsa=no
```

3. Объявите сети, участвующие в OSPF:

```
/routing ospf network
add network=192.168.50.0/24 area=backbone
add network=10.100.0.0/16 area=backbone
```

Настройка на MikroTik (RouterOS 7.18.2)

1. Настройте OSPF Instance (процесс OSPF, управляющий определенной группой маршрутов и интерфейсов):

```
/routing ospf instance
add name=<Название Instance> router-id=<Router-ID Mikrotik> redistribute=connected in-filter-chain=ospf-in out-filter-chain=o
```

2. Настройте магистральную зону (значение `area`, должно совпадать на NGFW и Mikrotik):

```
/routing ospf area
add name=backbone area-id=0.0.0.0 instance=<Название Instance>
```

3. Настройте интерфейсы:

```
/routing ospf interface-template
add interfaces=<Название GRE-интерфейса> area=backbone type=ptp network=10.100.0.0/16 cost=10
add interfaces=<Название интерфейса локальной сети> area=backbone type=broadcast network=192.168.50.0/24 cost=1
```

4. Настройте фильтрацию:

```
/routing filter rule
add chain=ospf-in rule="accept" disabled=no comment="Разрешаем все входящие маршруты"
add chain=ospf-out rule="accept" disabled=no comment="Разрешаем все исходящие маршруты"
```

Разрешение всех маршрутов без фильтрации допустимо в тестовых средах, простых или полностью контролируемых топологиях. В

распределенных сетях рекомендуем применять фильтрацию OSPF-маршрутов.

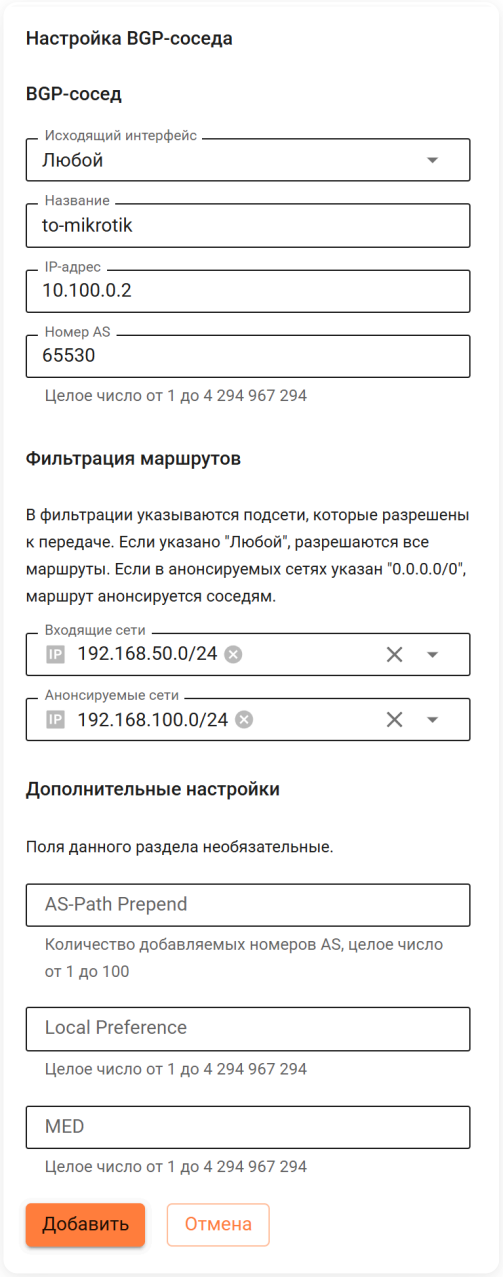
BGP

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. Введите номер автономной системы в поле **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:



- **Исходящий интерфейс** - выберите **Любой**.
- **Название** - любое значение.
- **IP-адрес** - IP-адрес GRE-интерфейса MikroTik.
- **Номер AS** - введите номер автономной системы MikroTik.
- **Входящие сети** - введите сети MikroTik, информацию от которых хотите получать. Если нужного объекта для фильтрации нет, нажмите **Создать новый объект**. Если выбран объект **Любой**, фильтрация будет отключена. Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру `0.0.0.0/0`.
- **Анонсируемые сети** - введите сети Ideco NGFW Novum, информацию о которых хотите отправлять. Если нужного объекта для фильтрации нет, нажмите **Создать новый объект**. Если выбран объект **Любой**, будет передаваться информация обо всех маршрутах, известных NGFW Novum. Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру `0.0.0.0/0`.
- **AS-Path Prepend** - введите число. Чем больше значение, тем менее приоритетным становится канал.

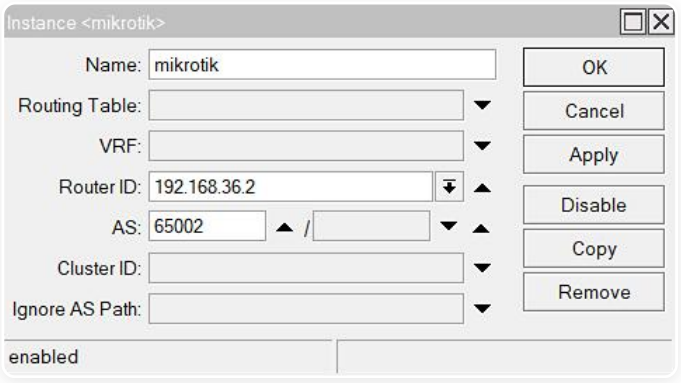
- **Local Preference** - введите число. Определяет приоритет пути для выхода трафика. Чем больше значение, тем более приоритетным становится канал.
- **MED** - введите число. Определяет приоритет пути для входа трафика. Чем меньше значение, тем приоритетнее путь.

3. Нажмите **Сохранить**.

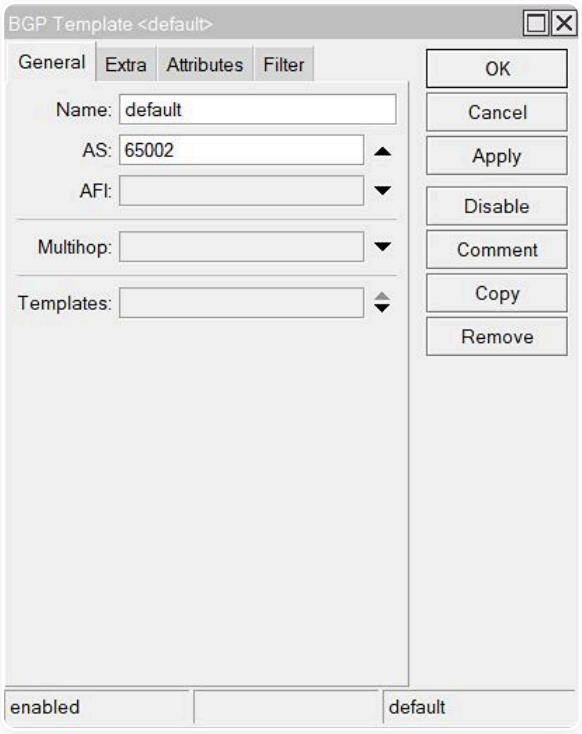
Настройка на MikroTik (RouterOS 7.20.6) через Winbox

Откройте Winbox и подключитесь к MikroTik. Все дальнейшие настройки BGP выполняются в разделе **Routing** → **BGP**.

1. На вкладке **Templates** откройте предустановленный шаблон **default** и задайте номер автономной системы в поле **AS**:



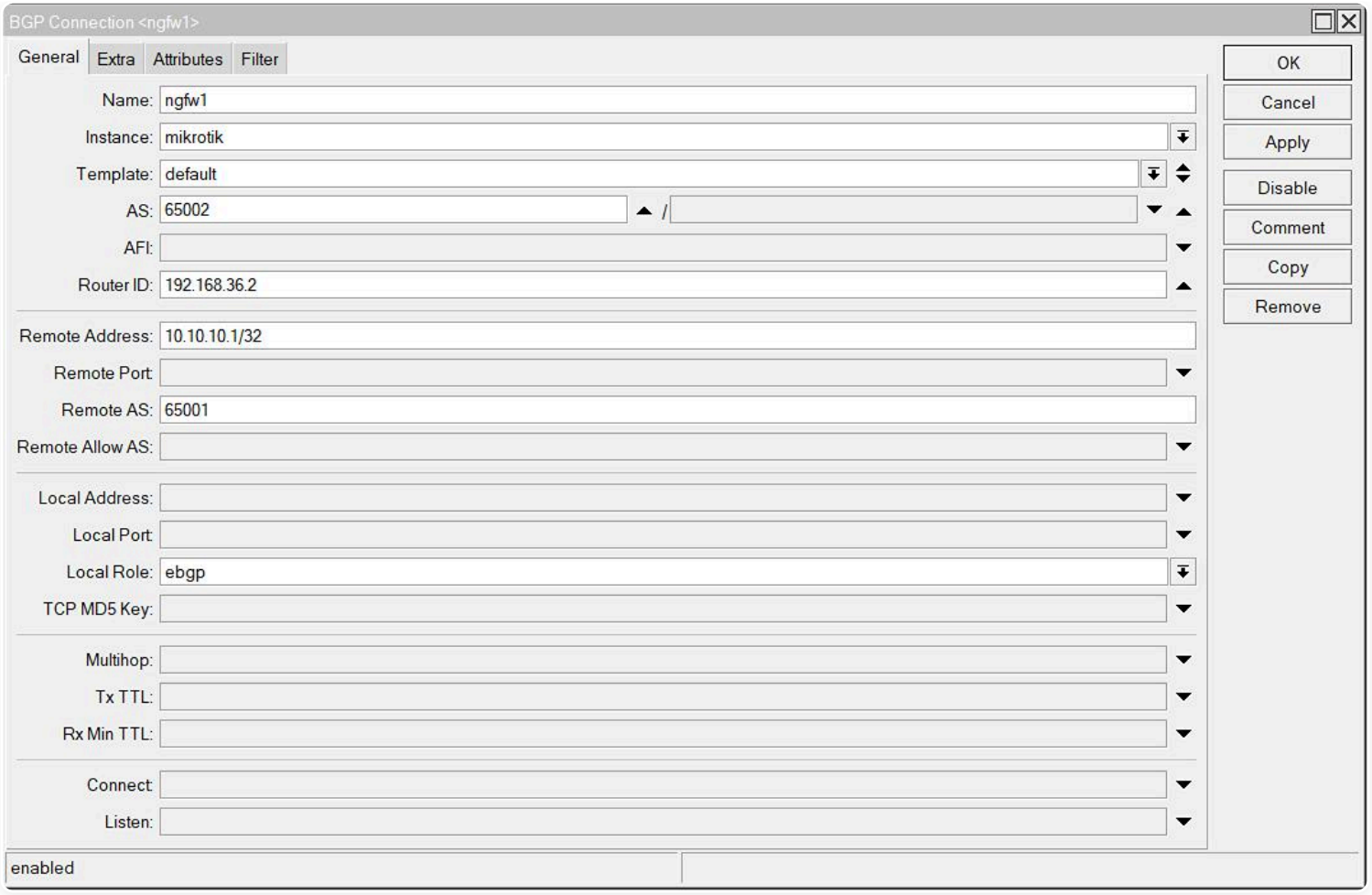
2. На вкладке **Instances** создайте экземпляр BGP с параметрами:



- **Name** - введите произвольное имя.
- **Router ID** - введите IP-адрес одного из локальных интерфейсов MikroTik, например, LAN-интерфейса.
- **AS** - введите номер автономной системы MikroTik.

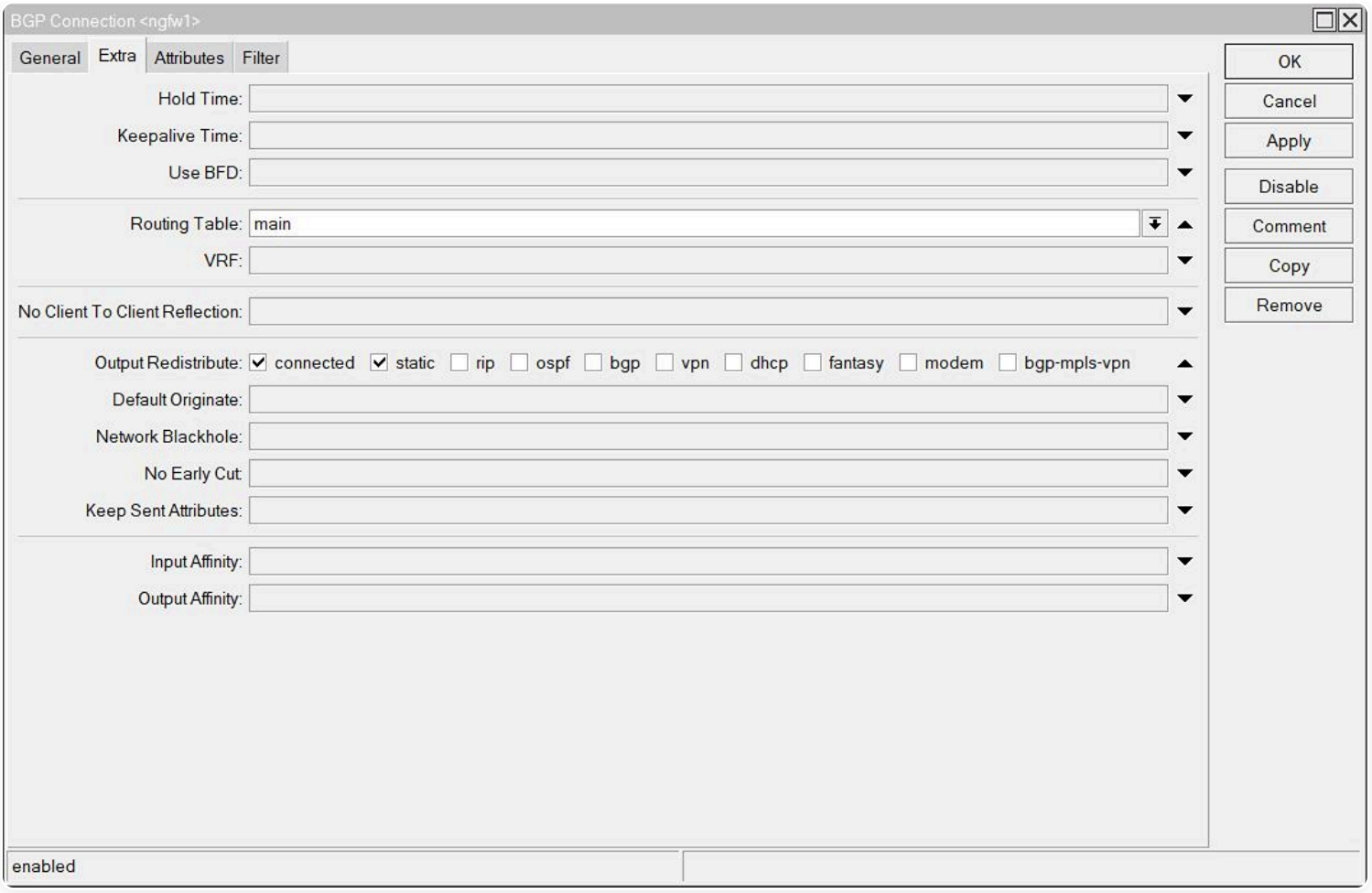
3. Нажмите **OK**.

4. Перейдите на вкладку **Connections**, создайте новое BGP-соединение и заполните поля на вкладке **General**:



- **Name** - введите произвольное имя.
- **Instance** - выберите экземпляр BGP, созданный на шаге 2.
- **Template** - выберите шаблон **default**, отредактированный на шаге 1.
- **AS** - введите номер автономной системы MikroTik.
- **Router ID** - введите IP-адрес одного из локальных интерфейсов MikroTik. Значение должно совпадать с указанным в экземпляре BGP на шаге 2 - здесь оно переопределяется для конкретного соединения.
- **Remote Address** - введите IP-адрес GRE-интерфейса NGFW Novum с маской `/32`.
- **Remote AS** - введите номер автономной системы NGFW Novum.
- **Local Role** - определяет роль данного узла в BGP-сессии. Укажите `ebgp`, так как соединение устанавливается между разными автономными системами (внешний BGP).

5. Перейдите на вкладку **Extra** и заполните поля:



- **Routing Table** - таблица маршрутизации, в которую будут помещаться маршруты, полученные от BGP-соседа. Укажите `main` для использования основной таблицы.
- **Output Redistribute** - отметьте `connected` и `static`, чтобы передавать BGP-соседу подключенные и статические маршруты MikroTik.

6. Нажмите **OK**.

Настройка на MikroTik через CLI

1. Настройте общий шаблон BGP, укажите номер автономной системы и основную таблицу маршрутизации:

```
/routing bgp template set default as=<номер AS MikroTik> disabled=no router-id=<IP-адрес локального интерфейса MikroTik> rout
```

2. Добавьте BGP-соединение с NGFW Novum:

```
/routing bgp connection add name=ngfw remote.address=<IP-адрес GRE-интерфейса NGFW Novum>/32 remote.as=<номер AS NGFW Novum>
```

Проверка результата

Проверка маршрутов на MikroTik

Перейдите в **IP** → **Routes**. В таблице маршрутизации должна появиться подсеть NGFW Novum со статусом `b` (получена по BGP) и шлюзом - IP-адрес GRE-интерфейса NGFW Novum.

Проверка через CLI:

```
/ip route print where bgp
```

Проверка статуса BGP-сессии на MikroTik

Через CLI проверьте, что BGP-сессия установлена:

```
/routing bgp session print
```

В выводе статус соединения должен быть `established`.

Проверка статуса IPsec на MikroTik

Перейдите в **IP** → **IPsec** → **Active Peers**. Должна отображаться запись с внешним IP-адресом NGFW Novum - это подтвердит, что IPsec-сессия установлена.

Перейдите в **IP** → **IPsec** → **Installed SAs**. Должны присутствовать активные записи SA - это подтвердит, что шифрование работает.

Проверка через CLI:

```
/ip ipsec active-peers print
/ip ipsec installed-sa print
```

Проверка на стороне Ideco NGFW Novum

Перейдите в **Управление сервером** → **Терминал** и выполните команды:

1. Проверьте статус IPsec-подключения:

```
ipsec status
```

Подключение должно быть в статусе **Established**.

2. Проверьте таблицы маршрутизации:

```
ip route show proto bgp
```

В выводе должна присутствовать подсеть MikroTik.

Проверка связи между хостами

С хоста в подсети NGFW Novum выполните:

```
ping <хост в подсети MikroTik>
```

С хоста в подсети MikroTik выполните:

```
/ping <хост в подсети NGFW Novum>
```

Обе проверки должны пройти успешно. Убедитесь, что NAT не применяется - в ответах должны фигурировать реальные IP-адреса хостов, а не транслированные.

Возможные проблемы

Соединение не устанавливается при повторной активации

Если подключение было отключено и при попытке включения соединение не установилось, удаленное устройство попало в fail2ban. Для установки соединения сбросьте блокировки по IP на Ideco NGFW Novum. О сбросе блокировки читайте в статье Защита от брутфорс-атак.

Fail2ban отслеживает в log-файлах попытки обратиться к сервисам, и, если находит повторяющиеся неудачные попытки авторизации с одного и того же IP-адреса или хоста, блокирует IP-адрес.

Соединение периодически разрывается

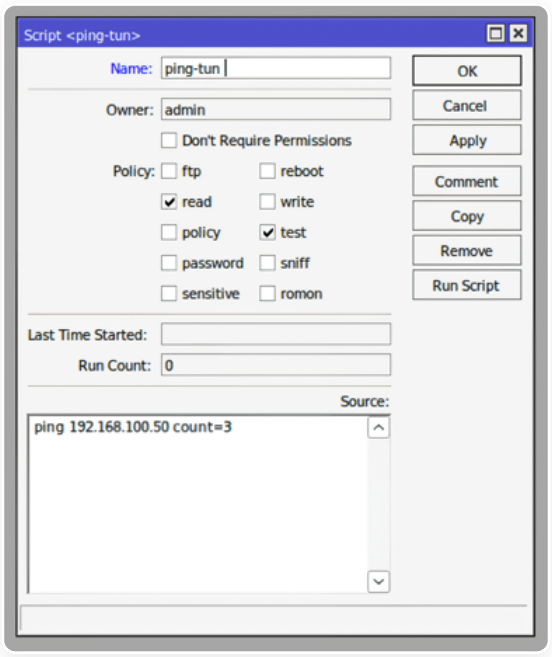
При работе туннеля между Ideco NGFW Novum и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW Novum.

Для автоматизации процесса поддержания соединения, создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW Novum:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в **System** → **Scripts**.

3. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



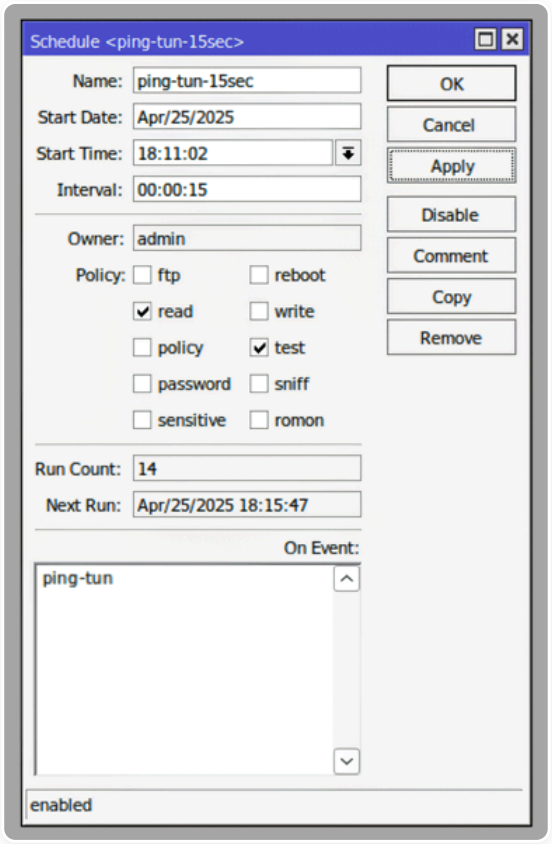
- **Name** - название скрипта (не поддерживаются пробелы и нижние подчеркивания).
- **Policy** - оставьте флаги на **read** и **test**.
- **Source** - введите команду `ping <ID-адрес Ideco NGFW Novum> count=3`.

4. Нажмите **Apply**, затем **Ok**.

Далее настройте запуск скрипта по расписанию в планировщике заданий:

1. Перейдите в **System** → **Scheduler**.

2. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



- **Name** - название задания (не поддерживаются пробелы и нижние подчеркивания).

- **Interval** - интервал 00:00:15 (каждые 15 секунд).
- **Policy** - оставьте флаги на **read** и **test**.
- **On Event** - введите название созданного ранее скрипта.

3. Нажмите **Apply**, затем **Ok**.

По завершению настройки MikroTik каждые 15 секунд будет отправлять три ICMP-запроса на адрес Ideco NGFW Novum. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.



В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение MikroTik и Ideco NGFW Novum по L2TP/IPsec

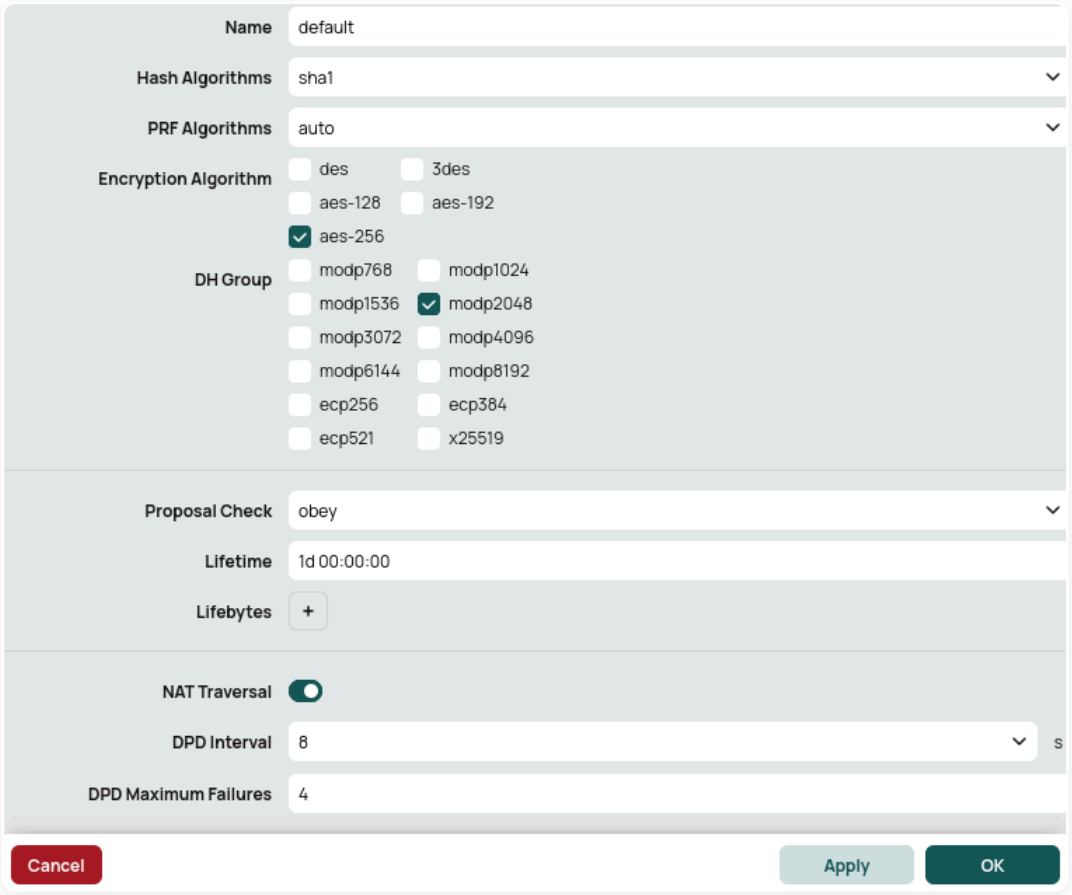
Функциональность доступна в **Классическом** и **Системном контекстах**.

Подключение MikroTik к Ideco NGFW Novum по L2TP/IPsec

- Настройте VPN-сервер на Ideco NGFW Novum в **Пользователи** → **VPN-подключения**. Подробная инструкция по настройке - в статье Подключение по L2TP/IPsec.
- Настройте подключение на MikroTik:

Веб-интерфейс

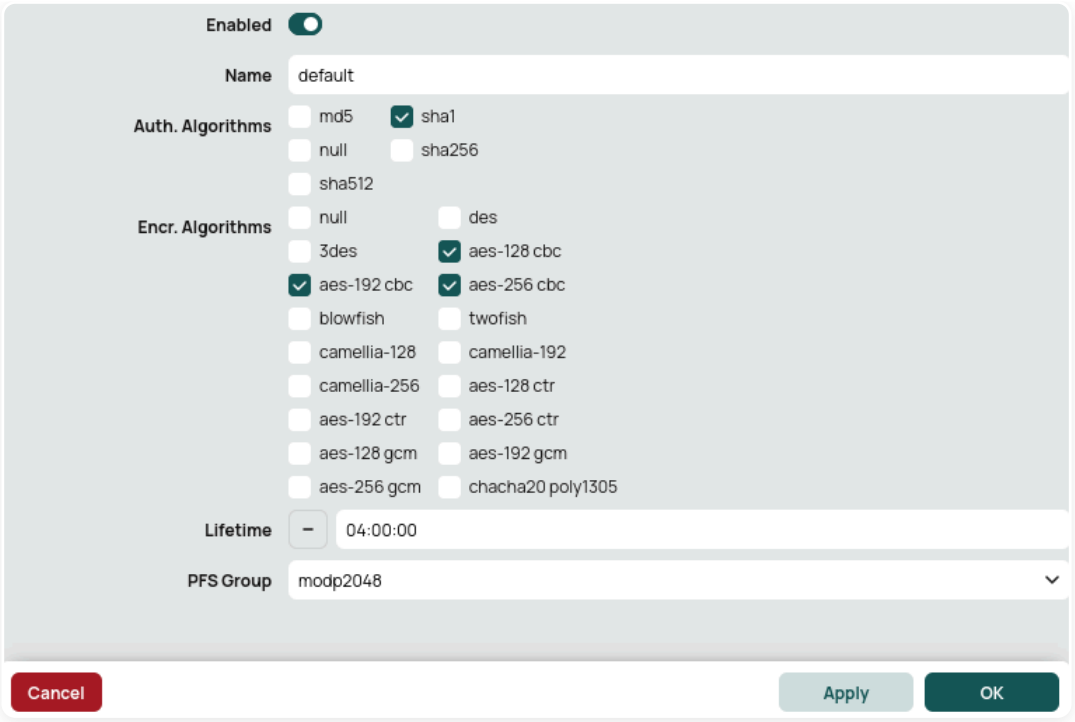
1. Перейдите в **IP** → **IPsec** → **Profiles**, выберите профиль **default** и заполните поля:



- **Hash Algorithms** - `sha1`.
- **Encryption Algorithm** - `aes-256`.
- **DH Group** - `modp2048`.

2. Нажмите **OK**.

3. Перейдите в **IP** → **IPsec** → **Proposals**, выберите профиль **default** и заполните поля:

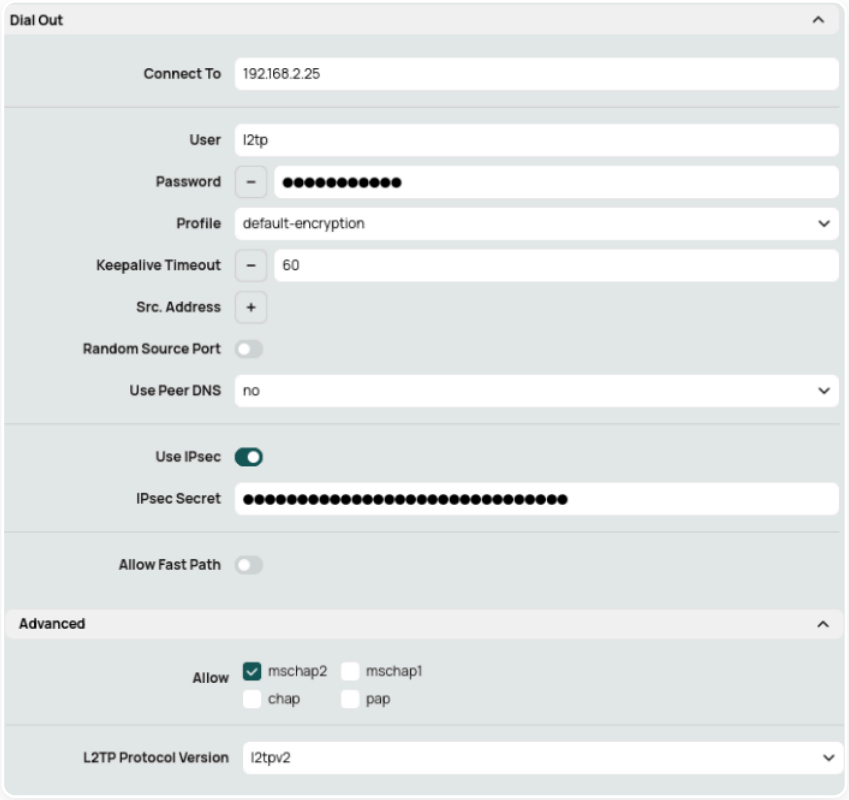


- **Auth. Algorithms** - `sha1`.
- **Encr. Algorithms** - `aes-256-cbc`, `aes-192-cbc`, `aes-128-cbc`.
- **PFS Group** - `modp2048`.

4. Нажмите **OK**.

5. Перейдите в **Interfaces**, нажмите **New** и выберите **L2TP Client**.

6. Заполните поля:



Расшифровка полей

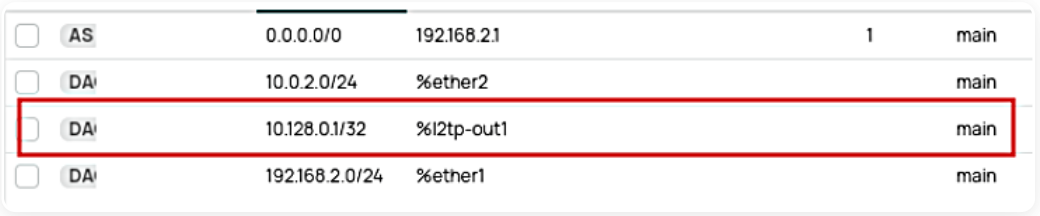
- **Dial Out**:
  - **Connect To** - IP-адрес Ideco NGFW Novum.
  - **User** - логин пользователя, которому разрешено подключение по VPN.

- **Password** - пароль пользователя.
- **Use IPsec** - включите опцию.
- **IPsec Secret** - ключ, скопированный по пути **Пользователи** → **VPN-подключения** → **Основное** из поля **PSK**.

- **Advanced**:
  - **Allow** - `mschap2`.

7. Нажмите **OK**.

8. Перейдите в **IP** → **Routes** и проверьте, что маршрут создан:



Терминал

1. Отредактируйте IPsec profile:

```
ip ipsec profile set default hash-algorithm=sha1 enc-algorithm=aes-256 dh-group=modp2048
```

2. Отредактируйте IPsec proposals:

```
ip ipsec proposal set default auth-algorithms=sha1 enc-algorithms=aes-256-cbc,aes-192-cbc,aes-128-cbc pfs-group=modp2048
```

3. Создайте подключение к Ideco NGFW Novum:

```
interface l2tp-client add connect-to=<server> profile=default disabled=no name=<interface_name> password="<password>" user="<
```

4. Добавьте маршрут до первого адреса VPN-сети NGFW (remote VPN subnet):

```
ip route add dst-address=<remote VPN subnet> gateway=l2tp-out1
```

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

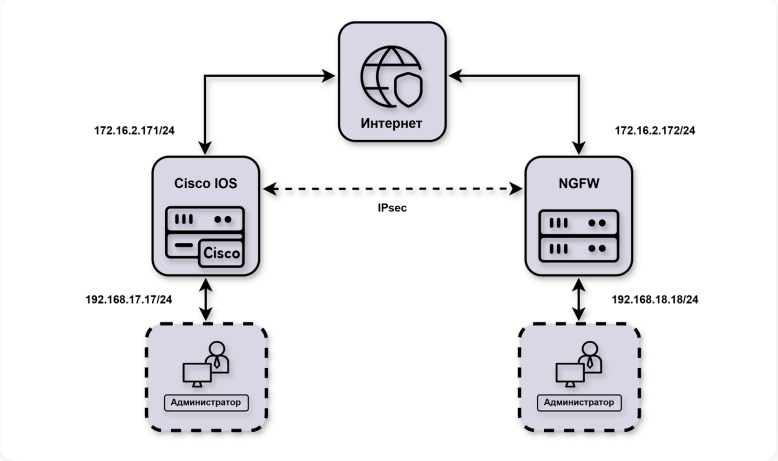
Полезные ссылки

- **IPsec**

Подключение Cisco IOS и Ideco NGFW Novum по IPsec в туннельном режиме

Функциональность доступна в **Классическом** и **Системном контекстах**.

Рассмотрим настройку подключения по схеме ниже:



Адресация:

- `172.16.2.172/24` - внешний IP-адрес NGFW.
- `192.168.18.18/24` - локальный IP-адрес NGFW.
- `172.16.2.171/24` - внешний IP-адрес Cisco.
- `192.168.17.17/24` - локальный IP-адрес Cisco.

Для настройки подключения Cisco IOS к Ideco NGFW Novum следуйте инструкции ниже.

Первоначальная настройка Ideco NGFW Novum и Cisco IOS

Настройка Ideco NGFW Novum

Настройте на Ideco NGFW Novum локальный и внешний интерфейсы. Инструкция по настройке - в статье.

Настройка Cisco IOS XE

Настроить Cisco можно, воспользовавшись нашими конфигурационными скриптами, сгенерированными по адресу https://cisco.ideco.ru/.

Для настройки Cisco через консоль выполните действия:

1. Настройте локальный интерфейс:

```
enable
conf t
interface GigabitEthernet2
ip address <локальный IP Cisco> <маска подсети>
no shutdown
ip nat inside
exit
```

2. Настройте внешний интерфейс:

```
interface GigabitEthernet1
ip address <внешний IP Cisco> <маска подсети>
no shutdown
```

```
ip nat outside
exit
```

3. Проверьте наличие связи между внешними интерфейсами Ideco NGFW Novum и Cisco. Для этого в консоли Cisco используйте команду `ping <внешний IP NGFW>`. Результат вывода команды - наличие ICMP-ответов.

4. Создайте access-list с адресацией локальной сети:

```
ip access-list extended NAT
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit
```

5. Настройте NAT:

```
ip nat inside source list NAT interface GigabitEthernet1 overload
exit
```

6. Сохраните настройки конфигурации:

```
write memory
```

7. **После сохранения настроек проверьте, что из локальной сети Cisco присутствует доступ в интернет.**

Для этого перейдите на какой-нибудь сайт (например: https://www.cisco.com/) с устройства в локальной сети Cisco.

Особенности работы Cisco в некоторых версиях:

- Cisco передает внешний IP-адрес вместо **KeyID** (проверьте, включив расширенный лог IPsec на Cisco). При настройке подключения от таких роутеров к Ideco NGFW Novum в качестве **Идентификатора удаленной стороны** укажите внешний IP-адрес Cisco, в качестве **Типа идентификатора** - auto.
- Если в подключении site2site активную сторону представляет Cisco и Child_SA закрывается, то пассивная сторона не сможет отправить пакет в сторону Cisco, пока Cisco не создаст новый Child_SA.

Инструкция проверена на **Cisco IOS XE версии 17.3.5**. При использовании других версий Cisco IOS синтаксис отдельных команд может отличаться.

Подключение от Ideco NGFW Novum к Cisco

Настройка IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
exit
```

3. Создайте peer:

```
crypto ikev2 keyring key
peer strongswan
```

```
address <внешний IP NGFW>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile:

```
crypto ikev2 profile ikev2profile
match identity remote key-id <key-id>
authentication remote pre-share
authentication local pre-share
keyring local key
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode tunnel
exit
```

6. Создайте ipsec-isakmp:

```
crypto map cmap 10 ipsec-isakmp
set peer <внешний IP NGFW>
set transform-set TS
set ikev2-profile ikev2profile
match address cryptoacl
reverse-route
exit
```

7. Настройте crypto map на внешнем интерфейсе:

```
interface GigabitEthernet1
crypto map cmap
exit
```

8. Создайте access-list для трафика между локальными сетями Cisco и NGFW:

```
ip access-list extended cryptoacl
permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
exit
```

9. Добавьте в access-list NAT исключения трафика между локальными сетями Cisco и NGFW (правило `deny` должно оказаться выше, чем `permit`):

```
ip access-list extended NAT
no permit ip <локальная подсеть Cisco> <обратная маска подсети> any
deny ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit

end
```

10. Сохраните настройки конфигурации:

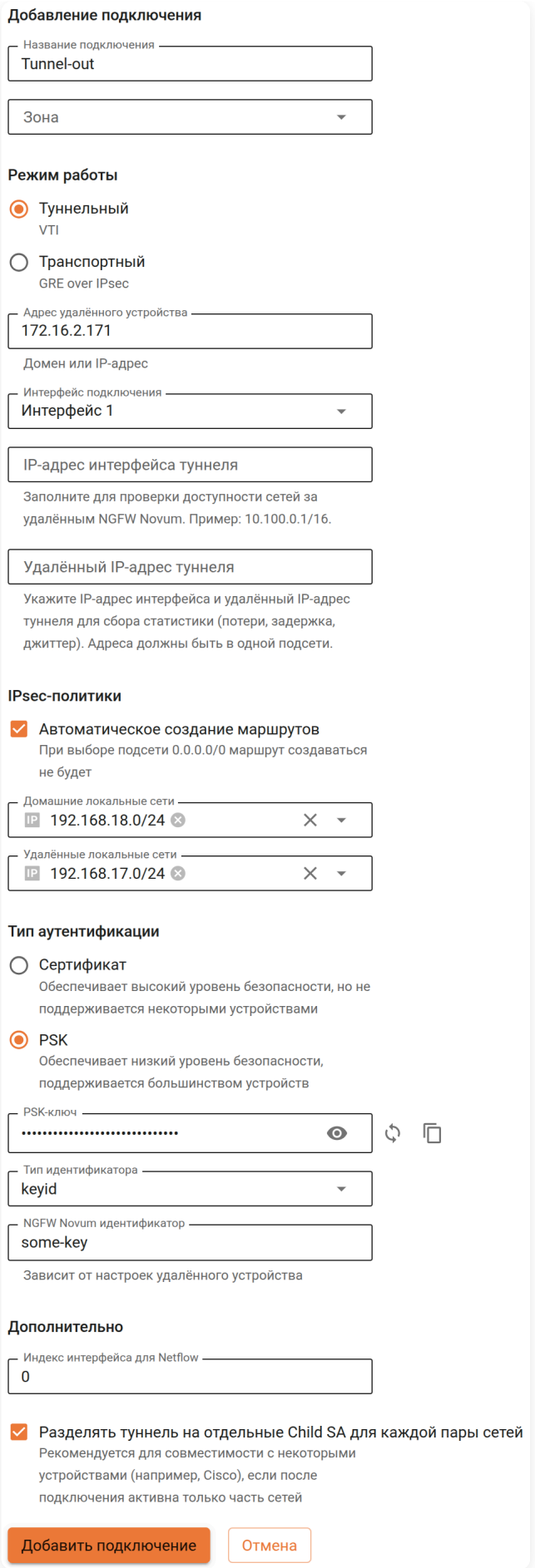
```
write memory
```

Настройка исходящего подключения на Ideco NGFW Novum

Для настройки исходящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPsec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.

- **Адрес удаленного устройства** - введите IP-адрес Cisco. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное. Заполняется при настройке BGP-соседства для динамической маршрутизации, получения статистики обмена пакетами или для обеспечения доступа Ideco NGFW Novum к удаленным сетям за другим устройством.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Поле необязательное. Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.
- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - будет сгенерирован случайный PSK-ключ для подключения в Cisco.
- **Идентификатор NGFW** - введенный ключ будет использоваться для идентификации исходящего подключения. Введите также этот идентификатор в Cisco.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Разделять туннель на отдельные Child SA для каждой пары сетей** - включите опцию для создания отдельного Child SA на каждую пару локальной и удаленной подсети, обеспечивая доступность всех сетей сразу после установления VPN. Актуально для совместимости с некоторыми типами устройств (например, Cisco), которые не поддерживают несколько селекторов трафика в одном Child SA.

3. Сохраните созданное подключение, затем нажмите на кнопку **Включить**.

4. Проверьте, что подключение установлено и используется (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Используется**).

5. Проверьте наличие трафика между локальными сетями.
Итоговая конфигурация IKEv2 IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Ideco NGFW Novum к Cisco

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy ikev2policy
 match fvrf any
 proposal ikev2proposal

crypto ikev2 keyring key
  peer strongswan
   address <внешний IP NGFW>
   pre-shared-key local <psk>
   pre-shared-key remote <psk>

crypto ikev2 profile ikev2profile
  match identity remote key-id <key-id>
  authentication remote pre-share
  authentication local pre-share
  keyring local key

crypto ipsec transform-set TS esp-gcm 256
 mode tunnel

crypto map cmap 10 ipsec-isakmp
 set peer <внешний IP NGFW>
 set transform-set TS
 set ikev2-profile ikev2profile
 match address cryptoacl
 reverse-route

interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
 crypto map cmap
```

```
interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid

ip nat inside source list NAT interface GigabitEthernet1 overload

ip access-list extended NAT
 deny   ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
ip access-list extended cryptoacl
 permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
```

Подключение от Cisco к Ideco NGFW Novum

Настройка IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
exit
```

3. Создайте peer:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP NGFW>
identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile:

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP NGFW> 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local key
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode tunnel
exit
```

6. Создайте ipsec-isakmp:

```
crypto map cmap 10 ipsec-isakmp
set peer <внешний IP NGFW>
set transform-set TS
set ikev2-profile ikev2profile
match address cryptoacl
reverse-route
exit
```

7. Настройте crypto map на внешнем интерфейсе:

```
interface GigabitEthernet1
crypto map cmap
exit
```

8. Создайте access-list для трафика между локальными сетями Cisco и NGFW:

```
ip access-list extended cryptoacl
permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
exit
```

9. Добавьте в access-list NAT исключения трафика между локальными сетями Cisco и NGFW (правило `deny` должно оказаться выше чем `permit`):

```
ip access-list extended NAT
no permit ip <локальная подсеть Cisco> <обратная маска подсети> any
deny ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit

end
```

10. Сохраните настройки конфигурации:

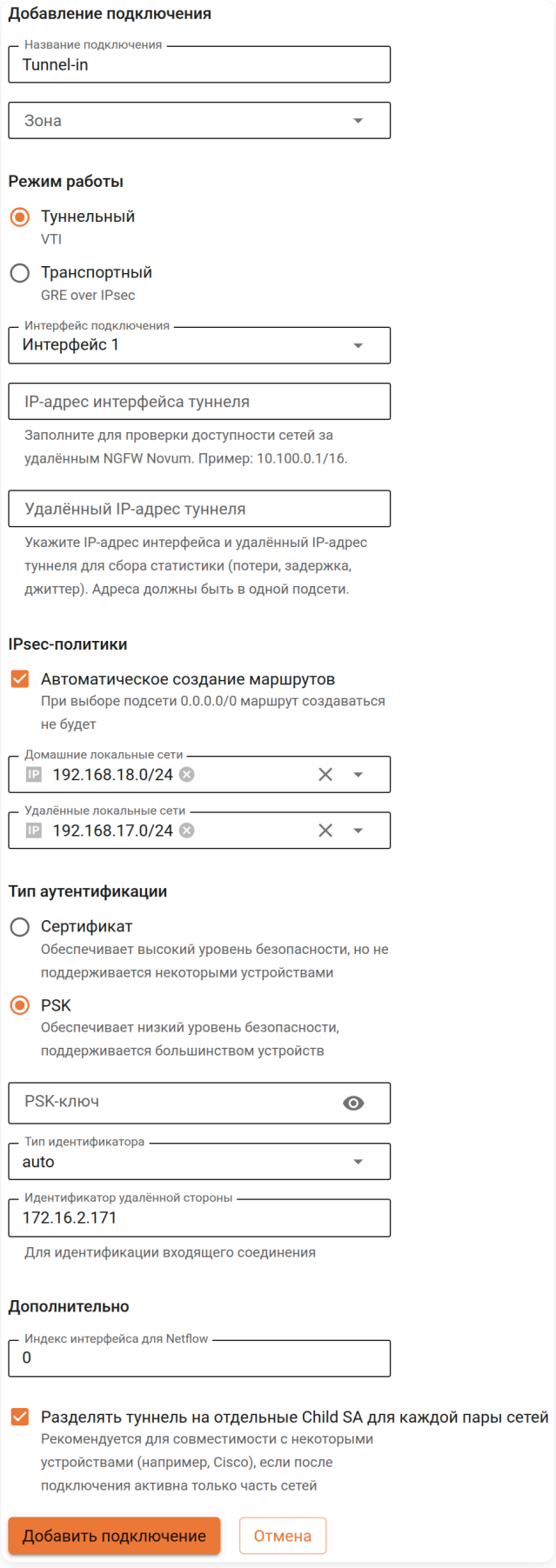
```
write memory
```

Настройка входящего подключения на Ideco NGFW Novum

Для настройки входящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы → IPsec → Устройства (входящие подключения)**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPSec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное. Заполняется при настройке BGP-соседства для динамической маршрутизации, получения статистики обмена пакетами или для обеспечения доступа Ideco NGFW Novum к удаленным сетям за другим устройством.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Поле необязательное. Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. IP-адреса должны находиться в одной подсети. Заполняется для получения статистики обмена пакетами.
- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ.
- **Тип идентификатора** - keyid или auto, если Cisco передает IP-адрес вместо key-id.
- **Идентификатор удаленной стороны** - вставьте идентификатор Cisco (параметр Key ID) или IP-адрес Cisco, если Cisco передает IP-адрес вместо key-id.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Разделять туннель на отдельные Child SA для каждой пары сетей** - включите опцию для создания отдельного Child SA на каждую пару локальной и удаленной подсети, обеспечивая доступность всех сетей сразу после установления VPN. Актуально для совместимости с некоторыми типами устройств (например, Cisco), которые не поддерживают несколько селекторов трафика в одном Child SA.

3. Сохраните созданное подключение, затем нажмите на кнопку **Включить**.

4. Проверьте, что подключение установлено и используется (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Используется**).

5. Проверьте наличие трафика между локальными сетями.
Итоговая конфигурация IKEv2 IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW Novum

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy ikev2policy
 match fvrf any
 proposal ikev2proposal

crypto ikev2 keyring key
  peer strongswan
   address <внешний IP NGFW>
   identity key-i <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
   pre-shared-key local <psk>
   pre-shared-key remote <psk>

crypto ikev2 profile ikev2profile
  match identity remote address <внешний IP NGFW> 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local key

crypto ipsec transform-set TS esp-gcm 256
 mode tunnel

crypto map cmap 10 ipsec-isakmp
 set peer <внешний IP NGFW>
 set transform-set TS
 set ikev2-profile ikev2profile
 match address cryptoacl
 reverse-route

interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
 crypto map cmap
```

```
interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid

ip nat inside source list NAT interface GigabitEthernet1 overload

ip access-list extended NAT
 deny   ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
ip access-list extended cryptoacl
 permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW> <обратная маска подсети>
```

Настройка динамической маршрутизации (BGP)

Настройка на Cisco

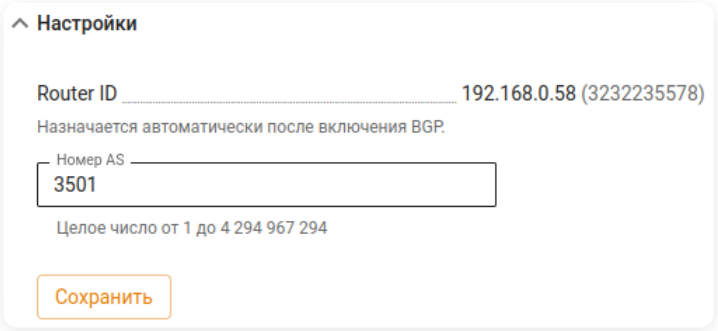
Настройте BGP на роутере:

```
conf t
router bgp 3500
 neighbor <внешний IP NGFW> remote-as 3501
 neighbor <внешний IP NGFW> ebgp-multihop 2
 !
 address-family ipv4
 network <локальная подсеть Cisco> mask <маска подсети>
 neighbor <внешний IP NGFW> activate
 exit-address-family
```

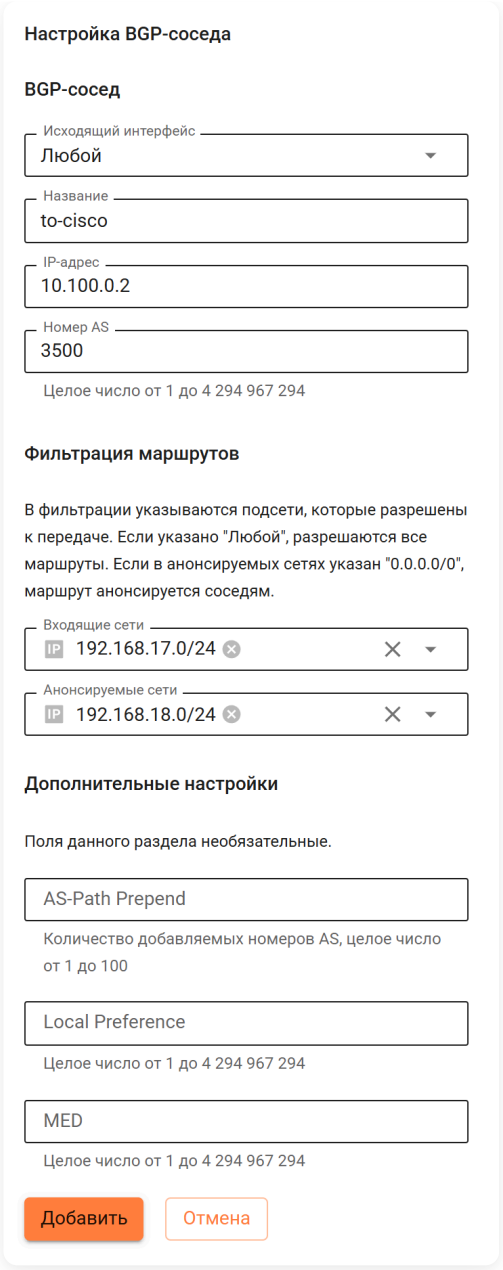
Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. Введите в блоке **Настройки** номер автономной системы в поле **Номер AS** и нажмите **Сохранить**:



3. Заполните поля:



Расшифровка полей

- **Исходящий интерфейс** - выберите **Любой**.
- **IP-адрес** - укажите внешний IP-адрес Cisco.
- **Номер AS** - номер AS Cisco (указанный в команде `router bgp 3500`).
- **Входящие сети** - укажите локальные сети Cisco.
- **Анонсируемые сети** - укажите локальные сети Ideco NGFW Novum.
- **Дополнительные настройки** при необходимости:
  - **AS-Path Prepend** - укажите приоритетность канала.
  - **Local Preference** - определите приоритет пути для выхода трафика. Чем больше значение, тем более приоритетным становится канал.
  - **MED** - определите приоритет пути для входа трафика. Чем меньше значение, тем приоритетнее путь.

4. Включите модуль **BGP**.



В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Cisco IOS и Ideco NGFW Novum по IPsec в транспортном режиме

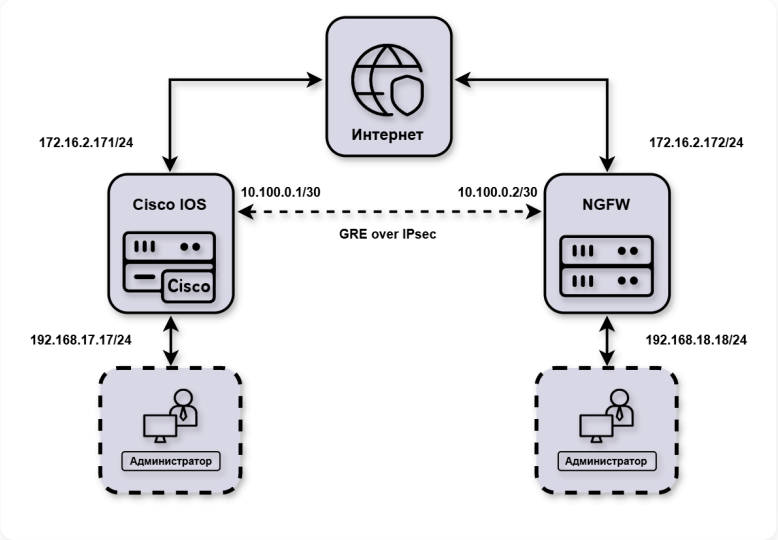
Функциональность доступна в **Классическом** и **Системном контекстах**.

GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

В GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

Для доступности локальных сетей NGFW и Cisco с удаленного устройства при подключении по GRE over IPsec настройте на обоих устройствах статические маршруты или динамическую маршрутизацию через **BGP**.

Рассмотрим настройку подключения по схеме ниже:



Адресация:

- `172.16.2.172/24` - внешний IP-адрес NGFW.
- `192.168.18.18/24` - локальный IP-адрес NGFW.
- `172.16.2.171/24` - внешний IP-адрес Cisco.
- `192.168.17.17/24` - локальный IP-адрес Cisco.
- `10.100.0.1/30` - IP-адрес интерфейса туннеля NGFW.
- `10.100.0.2/30` - IP-адрес интерфейса туннеля Cisco.

Для настройки подключения Cisco IOS к Ideco NGFW Novum следуйте инструкции ниже.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе **Интерфейсы**. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec либо использовать разные адреса для настроек GRE и GRE over IPSec.

Первоначальная настройка Ideco NGFW Novum и Cisco IOS

Настройка Ideco NGFW Novum

Настройте на Ideco NGFW Novum локальный и внешний интерфейсы. Инструкция по настройке - в статье.

Настройка Cisco IOS через консоль

1. Настройте локальный интерфейс:

```
enable
conf t
interface GigabitEthernet2
ip address <локальный IP Cisco> <маска подсети>
no shutdown
ip nat inside
exit
```

2. Настройте внешний интерфейс:

```
interface GigabitEthernet1
ip address <внешний IP Cisco> <маска подсети>
no shutdown
ip nat outside
exit
```

3. Проверьте наличие связи между внешними интерфейсами Ideco NGFW Novum и Cisco. Для этого в консоли Cisco используйте команду `ping <внешний IP NGFW>`. Результат вывода команды - наличие ICMP-ответов.

4. Создайте access-list и NAT для доступа из локальной сети в интернет:

```
ip access-list extended NAT
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit
ip nat inside source list NAT interface gigabitEthernet 1 overload
```

5. Сохраните настройки конфигурации:

```
write memory
```

5. **После сохранения настроек проверьте, что из локальной сети Cisco присутствует доступ в интернет.**

Для этого перейдите на какой-нибудь сайт (например: https://www.cisco.com/) с устройства в локальной сети Cisco.

Особенности работы Cisco в некоторых версиях:

- Cisco передает внешний IP-адрес вместо **KeyID** (проверьте, включив расширенный лог IPsec на Cisco). При настройке подключения от таких роутеров к Ideco NGFW Novum в качестве **Идентификатора удаленной стороны** укажите внешний IP-адрес Cisco, в качестве **Типа идентификатора** - auto.
- Если в подключении site2site активную сторону представляет Cisco и Child_SA закрывается, то пассивная сторона не сможет отправить пакет в сторону Cisco, пока Cisco не создаст новый Child_SA.

Подключение от Ideco NGFW Novum к Cisco

Настройка IKEv2+GRE-over-IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
```

```
proposal ikev2proposal
exit
```

3. Создайте peer (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

- Для подключения от Ideco NGFW Novum к Cisco:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP-адрес NGFW>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

- Для подключения от Cisco к Ideco NGFW Novum:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP NGFW>
identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

- Для подключения от Ideco NGFW Novum к Cisco:

```
crypto ikev2 profile ikev2profile
match identity remote key-id <key-id>
authentication remote pre-share
authentication local pre-share
keyring local key
dpd 10 3 periodic
exit
```

- Для подключения от Cisco к Ideco NGFW Novum:

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP NGFW> 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local key
dpd 10 3 periodic
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode transport
exit
```

6. Настройте профиль IPsec:

```
crypto ipsec profile ikev2TSprofile
set transform-set TS
set pfs group19
set ikev2-profile ikev2profile
exit
```

7. Создайте туннельный интерфейс:

```
interface Tunnel0
ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
ip mtu 1400
tunnel source GigabitEthernet 1
tunnel destination <внешний IP-адрес NGFW>
tunnel protection ipsec profile ikev2TSprofile
exit
```

8. Настройте динамическую маршрутизацию (BGP или OSPF) или статический маршрут до локальных сетей Ideco NGFW Novum:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

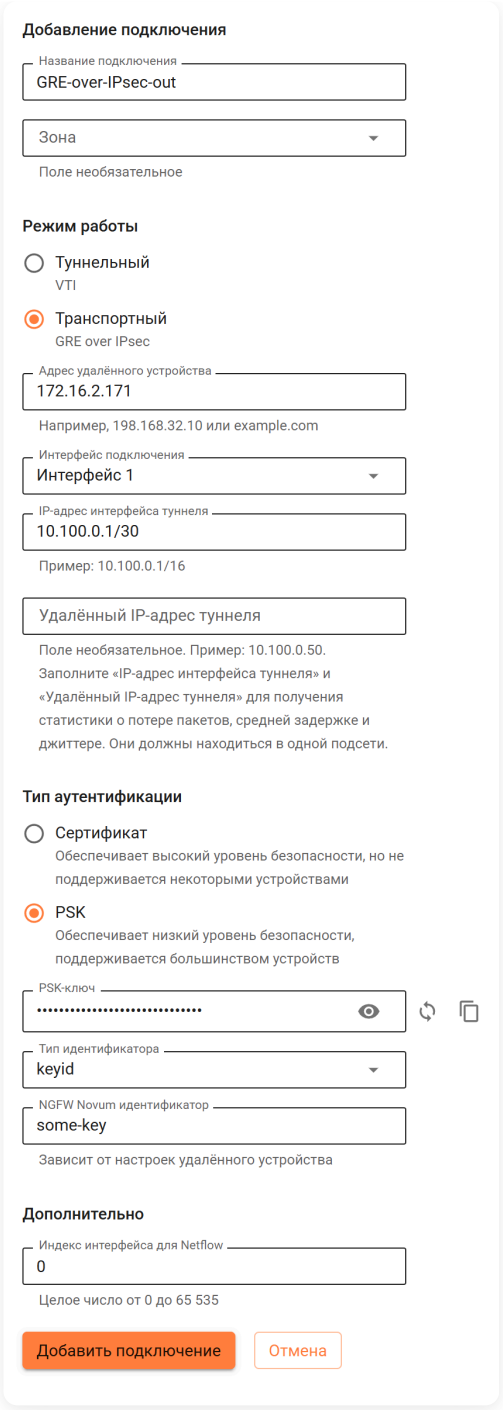
```
write memory
```

Настройка исходящего подключения на Ideco NGFW Novum

Для настройки исходящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPSec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **Адрес удаленного устройства** - введите IP-адрес Cisco. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля Cisco. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере.
- **Тип аутентификации** - PSK.
- **PSK** - будет сгенерирован случайный PSK-ключ для подключения в Cisco.
- **NGFW идентификатор** - введенный ключ будет использоваться для идентификации исходящего подключения. Введите также идентификатор в Cisco.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Проверьте, что подключение установилось (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

4. Проверьте наличие трафика между туннельными интерфейсами NGFW и Cisco. Для этого в консоли Cisco или терминале NGFW используйте утилиту `ping`.
Итоговая конфигурация IKEv2 GRE over IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Ideco NGFW Novum к Cisco

```
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 2

!
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
!
!
crypto ikev2 keyring key
 peer strongswan
  address <внешний IP-адрес NGFW>
  pre-shared-key local <psk>
  pre-shared-key remote <psk>
!
!
crypto ikev2 profile ikev2profile
 match identity remote key-id <key-id>
 authentication remote pre-share
 authentication local pre-share
 keyring local key
 dpd 10 3 periodic
!
!
crypto ipsec transform-set TS esp-gcm 256
 mode transport
!
!
crypto ipsec profile ikev2TSprofile
 set transform-set TS
 set pfs group2
 set ikev2-profile ikev2profile
!
!
interface Tunnel0
 ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
 ip mtu 1400
 tunnel source GigabitEthernet 1
 tunnel destination <внешний IP-адрес NGFW>
 tunnel protection ipsec profile ikev2TSprofile
!
interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid

interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid
!
ip nat inside source list NAT interface GigabitEthernet1 overload
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
!
ip access-list extended NAT
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
```

Подключение от Cisco к Ideco NGFW Novum

Настройка IKEv2+GRE-over-IPsec на Cisco

1. Создайте proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создайте policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
exit
```

3. Создайте peer (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP NGFW>
identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создайте IKEv2 profile (key-id - идентификатор удаленной стороны, т. е. Ideco NGFW Novum):

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP NGFW> 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local key
dpd 10 3 periodic
exit
```

5. Настройте шифрование в ESP:

```
crypto ipsec transform-set TS esp-gcm 256
mode transport
exit
```

6. Настройте профиль IPsec:

```
crypto ipsec profile ikev2TSprofile
set transform-set TS
set pfs group19
set ikev2-profile ikev2profile
exit
```

7. Создайте туннельный интерфейс:

```
interface Tunnel0
ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
ip mtu 1400
tunnel source GigabitEthernet 1
```

```
tunnel destination <внешний IP-адрес NGFW>
tunnel protection ipsec profile ikev2TSprofile
exit
```

8. Настройте динамическую маршрутизацию (BGP или OSPF) или статический маршрут до локальных сетей Ideco NGFW Novum:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

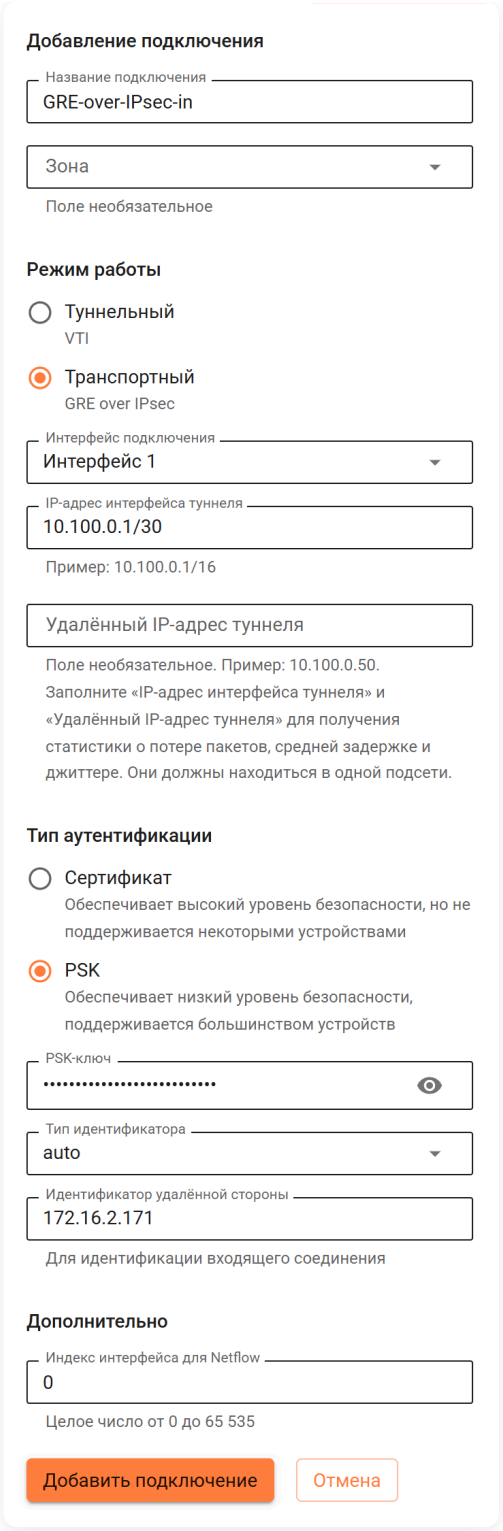
```
write memory
```

Настройка входящего подключения на Ideco NGFW Novum

Для настройки входящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Устройства(входящие подключения)**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPsec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **Интерфейс подключения** - выберите внешний интерфейс NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля Cisco. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ.
- **Тип идентификатора** - keyid или auto, если Cisco передает IP-адрес вместо key-id.
- **Идентификатор удаленной стороны** - вставьте идентификатор Cisco (параметр Key ID) или IP-адрес Cisco, если Cisco передает IP-адрес вместо key-id.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Сохраните созданное подключение, затем нажмите на кнопку **Включить**.

4. Проверьте, что подключение установлено (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

5. Проверьте наличие трафика между туннельными интерфейсами NGFW и Cisco. Для этого в консоли Cisco или терминале NGFW используйте утилиту `ping`.
Итоговая конфигурация IKEv2 GRE over IPsec на Cisco IOS должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW Novum

```
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 2

!
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
!
!
crypto ikev2 keyring key
 peer strongswan
  address <внешний IP NGFW>
  identity key-id <key-id> # Если Cisco передает IP вместо key-id, то identity address <внешний IP-адрес Cisco>
  pre-shared-key local <psk>
  pre-shared-key remote <psk>
!
!
crypto ikev2 profile ikev2profile
 match identity remote address <внешний IP NGFW> 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local key
!
!
crypto ipsec transform-set TS esp-gcm 256
 mode transport
!
!
crypto ipsec profile ikev2TSprofile
 set transform-set TS
 set pfs group2
 set ikev2-profile ikev2profile
!
!
interface Tunnel0
 ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
 ip mtu 1400
 tunnel source GigabitEthernet 1
 tunnel destination <внешний IP-адрес NGFW>
 tunnel protection ipsec profile ikev2TSprofile
!
interface GigabitEthernet1
! внешний интерфейс
 ip address <внешний IP Cisco> <маска подсети>
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid

interface GigabitEthernet2
! локальный интерфейс
 ip address <локальный IP Cisco> <маска подсети>
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid
!
ip nat inside source list NAT interface GigabitEthernet1 overload
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

```
!
ip access-list extended NAT
 permit ip <локальная подсеть Cisco> <обратная маска подсети> any
```

Настройка динамической маршрутизации

OSPF

Настройка на Cisco

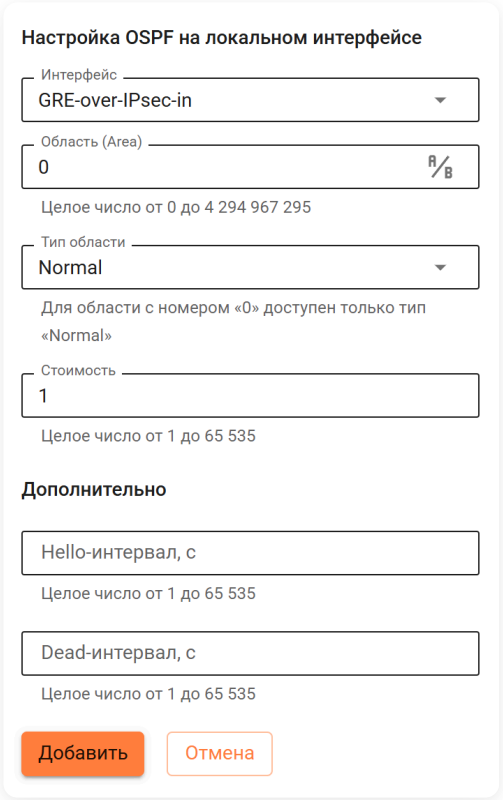
Настройте процесс OSPF на роутере (значение `area` должно совпадать на Cisco и NGFW):

```
conf t
router ospf 1
passive-interface default
 no passive-interface Tunnel0
 network <подсеть туннельного интерфейса Cisco> <обратная маска> area 0
 network <локальная подсеть Cisco> <обратная маска> area 0
exit
```

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW Novum, настроенный ранее.
- **Область (Area)** - введите номер области (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Тип области** - для области с указанным номером `area` должен быть выбран одинаковый тип на всех OSPF-соседях. Для области с номером 0 (`0.0.0.0`) допустимо указывать только один тип - **Normal**. Допустимые значения: **Normal**, **Stub**, **NSSA**:
  - **Normal Area** (обычная зона) - стандартная зона OSPF, которая получает полную информацию о маршрутах как внутри автономной системы, так и за ее пределами. В такой зоне могут находиться как маршрутизаторы, так и конечные устройства.
  - **Stub Area** (усеченная зона) - зона, в которой не принимаются внешние маршруты (Type 5 LSA), но принимаются маршруты других зон. Вместо полной информации о внешних маршрутах используется маршрут по умолчанию.
  - **NSSA** (Not-So-Stubby Area) - разновидность stub-зоны, которая может получать маршруты по умолчанию и отправлять свои маршруты в другие зоны через **ABR** (Area Border Router). В **NSSA** зоне используется специальный тип LSA (Type 7), который преобразуется в Type 5 на ABR.

- **Стоимость** - введите стоимость маршрута.
- **Hello-интервал** - укажите время между отправкой Hello-пакетов, которое варьируется от 1 до 65535 секунд. Если поле не заполнено, по умолчанию используется значение 10 секунд. Для установления соседства между устройствами интервал должен быть одинаковым для всех участников сети.
- **Dead-интервал** - укажите время, через которое сосед считается недоступным, если не получает Hello-пакеты. Диапазон значений - от 1 до 65535 секунд. Если поле не заполнено, по умолчанию в 4 раза больше, чем Hello-интервал. Для успешного соседства значение должно быть одинаковым у всех устройств в сегменте сети.

3. Нажмите **Сохранить**.

4. Включите модуль **OSPF**.

Для подключения нескольких устройств Cisco к одному Ideco NGFW Novum и передачи маршрутов между всеми устройствами:

1. Создайте для каждого Cisco Gre-over-IPsec подключение к Ideco NGFW Novum.

2. Подключите каждое устройство Cisco по OSPF.

При такой конфигурации локальные сети каждого Cisco будут доступны с Ideco NGFW Novum и других устройств Cisco.

BGP

Настройка на Cisco

Настройте процесс BGP на роутере:

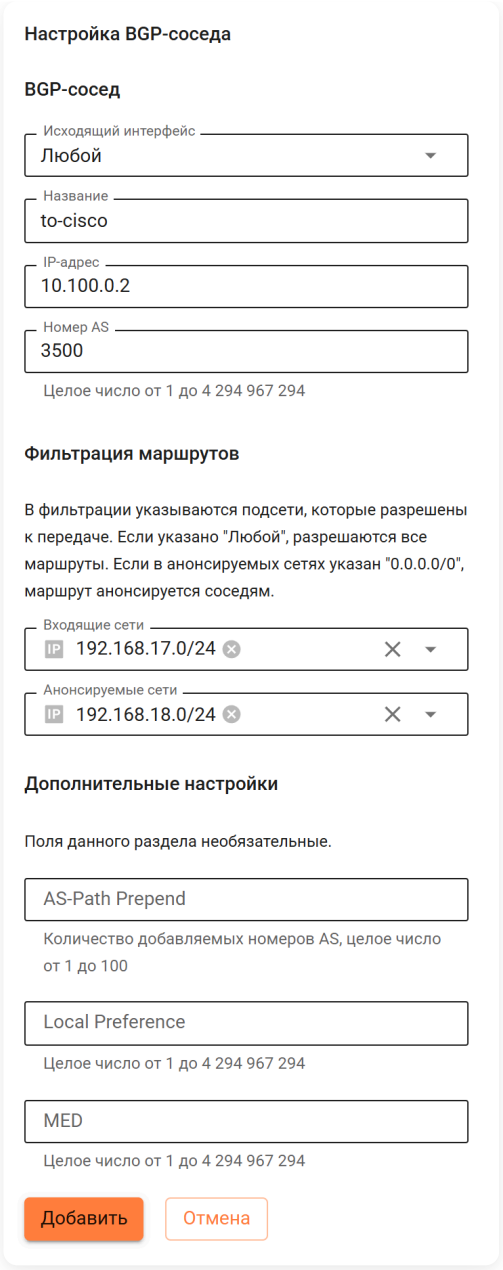
```
conf t
router bgp 3500
 neighbor <IP интерфейса туннеля NGFW> remote-as 3501
 neighbor <IP интерфейса туннеля NGFW> ebgp-multihop 2
 neighbor <IP интерфейса туннеля NGFW> update-source Tunnel0
 !
 address-family ipv4
  network <локальная подсеть Cisco> mask <маска подсети>
  neighbor <IP интерфейса туннеля NGFW> activate
 exit-address-family
```

Настройка на Ideco NGFW Novum

1. Перейдите в **Маршрутизация** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в поле **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:



- **Исходящий интерфейс** - выберите **Любой**.
- **IP-адрес** - укажите IP-адрес интерфейса туннеля Cisco.
- **Номер AS** - номер AS Cisco (указанный в команде `router bgp 3500`).
- **Входящие сети** - укажите локальные сети Cisco.
- **Анонсируемые сети** - укажите локальные сети Ideco NGFW Novum.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

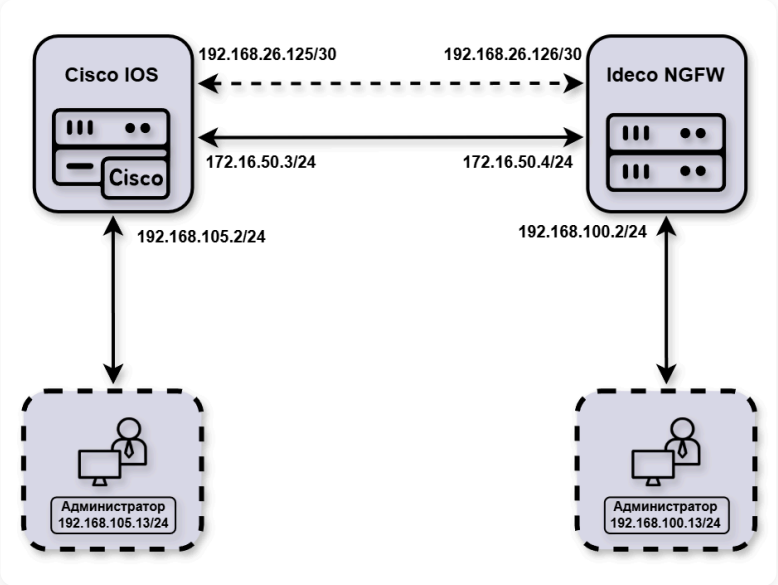
5. Включите модуль **BGP**.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Подключение Cisco IOS и Ideco NGFW Novum по route-based IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Рассмотрим процесс настройки подключения в туннельном режиме по следующей схеме:



Адресация:

- `192.168.26.125/30` - IP-адрес интерфейса туннеля NGFW.
- `192.168.26.126/30` - IP-адрес интерфейса туннеля Cisco.
- `172.16.50.3/24` - внешний IP-адрес NGFW.
- `192.168.100.2/24` - локальный IP-адрес NGFW.
- `172.16.50.4/24` - внешний IP-адрес Cisco.
- `192.168.105.2/24` - локальный IP-адрес Cisco.

Инструкция проверена на **Cisco IOS XE версии 17.3.5**. При использовании других версий Cisco IOS синтаксис отдельных команд может отличаться.

Первоначальная настройка Ideco NGFW Novum и Cisco IOS

Настройка Ideco NGFW Novum

Настройте на Ideco NGFW Novum локальный и внешний интерфейсы. Подробная информация находится в статье Первоначальная настройка.

Настройка Cisco

Для настройки Cisco через консоль выполните действия:

1. Настройка локального и внешнего интерфейса:

```
enable
configure terminal
interface gigabitEthernet 1
ip address <внешний IP-адрес Cisco> <маска подсети>
no shutdown
ip nat outside
exit
```

```
interface gigabitEthernet 2
ip address <локальный IP-адрес Cisco> <маска подсети>
no shutdown
ip nat inside
exit
```

2. Настройка DNS и добавление маршрута по умолчанию для доступа в интернет:

```
configure terminal
ip name-server <IP-адрес DNS-сервера>
ip route 0.0.0.0 0.0.0.0 <IP-адрес провайдера>
```

3. Создание access-list и NAT для доступа из локальной сети в интернет:

```
ip access-list extended NAT
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit
ip nat inside source list NAT interface gigabitEthernet 1 overload
```

4. Добавление локального администратора и настройка доступа по SSH:

```
configure terminal
username admin privilege 15 secret <пароль>
hostname <имя роутера>
ip domain name <имя домена>
crypto key generate rsa
ip ssh version 2
aaa new-model
line vty 0 4
transport input ssh
privilege level 15
exit
```

5. Сохранение настроек конфигурации:

```
write
```

Настройка route-based IPsec на Cisco

1. Создание proposal:

```
configure terminal
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создание policy:

```
crypto ikev2 policy ikev2policy
proposal ikev2proposal
exit
```

3. Создание peer:

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP-адрес NGFW>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создание IKEv2 profile:

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP-адрес NGFW> <маска подсети>
identity local address <внешний IP-адрес Cisco>
authentication remote pre-share
authentication local pre-share
keyring local key
no config-exchange set send
no config-exchange set accept
no config-exchange request
exit
```

5. Настройка шифрования в esp:

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
exit
```

6. Создание ipsec profile:

```
crypto ipsec profile ikev2TSprofile
set transform-set TS
set pfs group19
set ikev2-profile ikev2profile
exit
```

7. Создание туннельного интерфейса:

```
interface Tunnel3000
ip address <IP-адрес интерфейса туннеля Cisco> <маска подсети>
tunnel source gigabitEthernet 1
tunnel mode ipsec ipv4
tunnel destination <внешний IP-адрес NGFW>
tunnel protection ipsec profile ikev2TSprofile
exit
```

8. Сохранение настроек конфигурации:

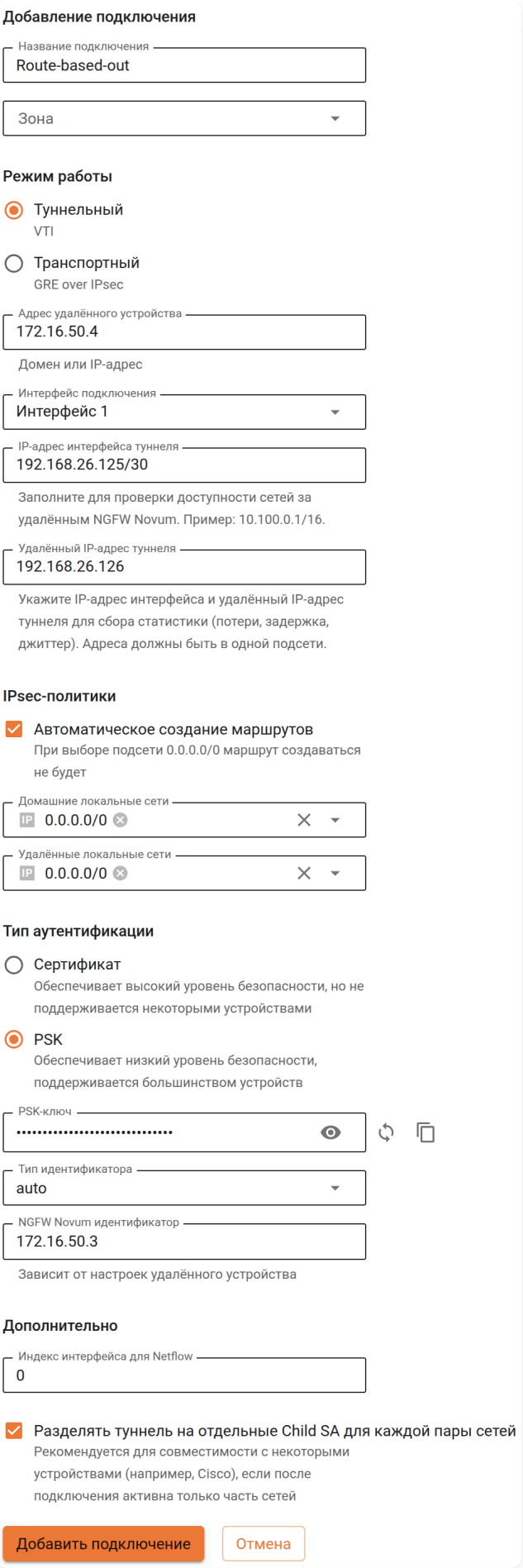
```
write
```

Настройка исходящего подключения на Ideco NGFW Novum

Для настройки исходящего IPsec-подключения на Ideco NGFW Novum выполните действия:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы → IPsec → Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPsec подключения. Список предустановленных зон приведен в статье.

- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - введите IP-адрес Cisco. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля NGFW Novum.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Адреса должны находиться в одной подсети.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ созданный на третьем этапе в разделе **Настройка route-based IPsec на Cisco**.
- **NGFW идентификатор** - укажите внешний IP-адрес NGFW Novum.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Разделять туннель на отдельные Child SA для каждой пары сетей** - включите опцию для создания отдельного Child SA на каждую пару локальной и удаленной подсети, обеспечивая доступность всех сетей сразу после установления VPN. Актуально для совместимости с некоторыми типами устройств (например, Cisco), которые не поддерживают несколько селекторов трафика в одном Child SA.

3. Проверьте, что подключение установилось (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

4. Проверьте наличие трафика между локальными сетями (TCP и web).
Итоговая конфигурация route-based IPsec на Cisco должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW Novum

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy ikev2policy
 proposal ikev2proposal

crypto ikev2 keyring key
 peer strongswan
  address <внешний IP-адрес NGFW>
  pre-shared-key local <psk>
  pre-shared-key remote <psk>

crypto ikev2 profile ikev2profile
 match identity remote address <внешний IP-адрес NGFW> <маска подсети>
 identity local address <внешний IP-адрес Cisco>
 authentication remote pre-share
 authentication local pre-share
 keyring local key
 no config-exchange set send
 no config-exchange set accept
 no config-exchange request

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile ikev2TSprofile
 set transform-set TS
 set pfs group19
 set ikev2-profile ikev2profile
```



В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **IPsec**

Подключение pfSense к Ideco NGFW Novum по IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

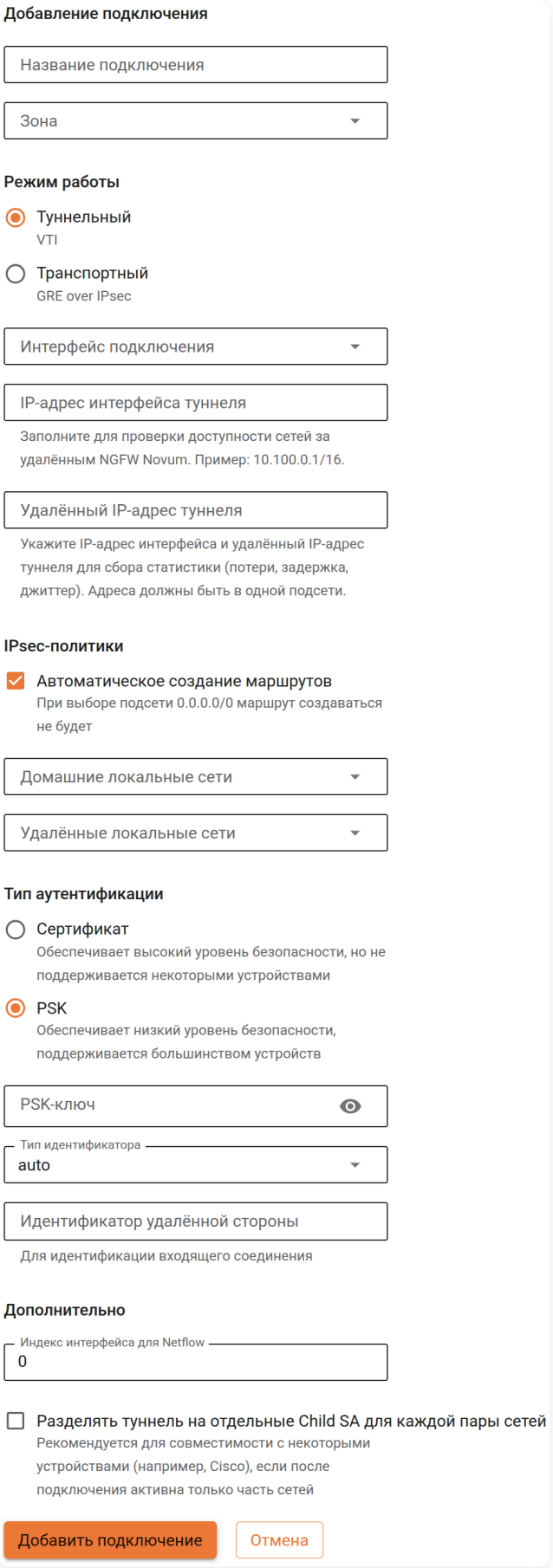
Объединяемые локальные сети не должны пересекаться!

Настройка входящего подключения

Для настройки Ideco NGFW Novum следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Входящие подключения**.

2. Добавьте новое подключение:



- **Название подключения** - любое.
- **Зона** - укажите зону для добавления IPSec-подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Тип аутентификации** - выберите PSK.
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения.
- **Идентификатор удаленной стороны** - введите значение, которое будет использоваться для идентификации pfSense.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW Novum, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW Novum.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

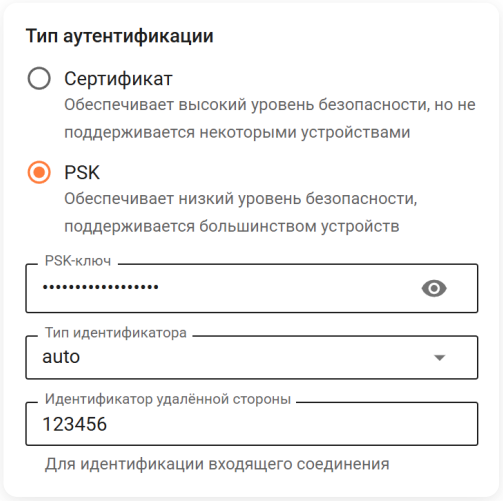
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.

3. Сохраните созданное подключение, нажмите на кнопку **Включить**.

4. Скопируйте значение идентификатора удаленной стороны одним из способов:

В интерфейсе NGFW

В **Сервисы** → **IPsec** → **Входящие подключения** в поле **Идентификатор удаленной стороны**:



Через терминал

На Ideco NGFW Novum в папке `/run/ideco-ipsec-backend/strongswan/swanctl/conf.d/` будет сгенерирован конфигурационный файл. Необходимо перейти в консоль и открыть на редактирование файл вида `device_<номер>.conf`. Из этого файла необходимо скопировать значение строки `id` (идентификатор удаленной стороны):

```
        children {
            device2utm_1_fqdn-0 {

                policies = no

                start_action = none
                esp_proposals = aes256gcm16-curve25519-ecp256-modp4096-modp2048-modp1024,aes256-sha512-sha384-sha256-curve25519-ecp256-modp4096-modp2048-modp1024

                local_ts = 192.168.101.0/24
                remote_ts = 192.168.201.0/24

                dpd_action = clear
                close_action = clear

                # ICS-24156 Вместо дефолтных 10% от 1ч, увеличиваем rand_time до 20%,
                # чтобы уменьшить вероятность одновременного рекеинга и появления дубликатов CHILD_SA
                rand_time = 720s

                updown = /usr/bin/ideco-ipsec-updown
            }
        }
        local {
            auth = psk
        }
        remote {
            # Во входящих подключениях нам не известен заранее IP удаленного устройства,
            # поэтому в качестве идентификатора подключения используем указанный идентификатор.
            # В исходящих подключениях мы таким образом даем себя идентифицировать.
            # ( https://wiki.strongswan.org/projects/strongswan/wiki/IdentityParsing )
            id = 123456
            auth = psk
        }
    }
}
secrets {
    ike-device2utm_1_fqdn-0 {
        # Hex encoded PSK aaaaaaaaa:',
        id = 123456
        secret = 0x61616161616161616161
    }
}
```

5. Перейдите к настройке pfSense, предварительно записав значение строки `id` (идентификатор удаленной стороны).

Настройка pfSense

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите в **VPN** → **IPsec** → **Tunnels**.

2. Добавьте новое подключение:

- **Description** - любое.
- **Key Exchange version** - IKEv2.
- **Internet Protocol** - IPv4.
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW Novum.
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW Novum.
- **Authentication Method** - Mutual PSK.
- **My identifier и Peer identifier** - сюда вставьте значение строки `id` на Ideco NGFW Novum (см. шаг 4 в настройке Ideco NGFW Novum).
- **Pre-Shared Key** - вставьте PSK-ключ, который ранее прописывали на Ideco NGFW Novum.
- **Encryption Algorithm** - используйте следующие параметры:
  - **Algorithm** - AES256-GCM.
  - **Key length** - 128 bit.
  - **Hash** - SHA256.
  - **DH Group** - Elliptic Curve 25519-256.

Все остальные значения можно оставить по умолчанию.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2. Здесь укажите:

- **Encryption Algorithm** - используйте следующие параметры:
  - **Algorithm** - AES256-GCM.
  - **Key length** - 128 bit.
  - **Hash** - SHA256.
  - **DH Group** - Elliptic Curve 25519-256.
- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW Novum.
- **Remote Network** - локальную сеть Ideco NGFW Novum, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. Разрешите хождение трафика между локальными сетями pfSense и Ideco NGFW Novum в настройках файрвола pfSense (перейдите в **Firewall** → **Rules** → **IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW Novum и pfSense).

Обращаем внимание на раздел файрвола WAN - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

7. Теперь перейдите в **Status** → **IPsec** (там должно появиться созданное подключение), нажмите **Connect VPN**.

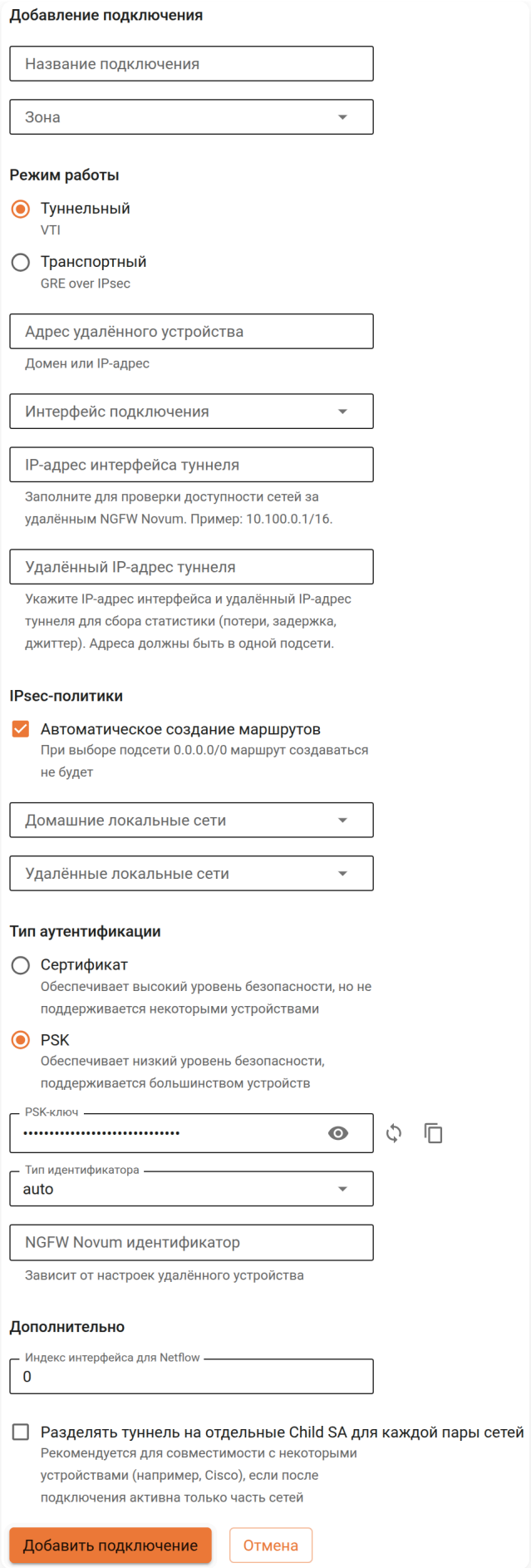
Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое указано в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

Настройка исходящего подключения

Для настройки Ideco NGFW Novum следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение:



- **Название** - любое.
- **Зона** - укажите зону для добавления IPSec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.

- **Адрес удаленного устройства** - укажите внешний IP-адрес pfSense. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW Novum, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW Novum.
- **Тип аутентификации** - выберите тип PSK.
- **PSK-ключ** - укажите PSK-ключ, который будет использоваться для подключения.
- **Тип идентификатора** - выберите auto.
- **Идентификатор NGFW** - введите значение, которое будет использоваться для идентификации Ideco NGFW Novum на pfSense.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Настройка pfSense

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите в **VPN > IPsec > Advanced Options** и в поле **Child SA Start Action** выберите параметр **None (Responder Only)**.

2. Добавьте новое подключение:

- **Key Exchange version** - IKEv2.
- **Internet Protocol** - IPv4.
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW Novum.
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW Novum.
- **Description** - любое.
- **Authentication Method** - Mutual PSK.
- **My identifier** - My ip address.
- **Peer identifier** - KeyID tag. Введите идентификатор удаленной стороны, т. е. Ideco NGFW Novum.
- **Pre-Shared Key** - введите PSK-ключ.
- **Encryption Algorithm**:
  - Для **Ideco UTM версии 10.0 и Ideco NGFW Novum версии 16.0 и новее** используйте следующие параметры:
    - **Algorithm** - AES256-GCM.
    - **Key length** - 128 bit.
    - **Hash** - SHA256.
    - **DH Group** - Elliptic Curve 25519-256.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2 и укажите следующие значения:

- **Encryption Algorithm**:
  - **Для Ideco UTM версии 10.0 и Ideco NGFW Novum версии 16.0 и новее** используйте следующие параметры:
    - **Algorithm** - AES256-GCM.
    - **Key length** - 128 bit.
    - **Hash** - SHA256.
    - **DH Group** - Elliptic Curve 25519-256.
- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW Novum.
- **Remote Network** - локальную сеть Ideco NGFW Novum, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. В настройках файрвола pfSense перейдите в **Firewall → Rules → IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW Novum и pfSense.

7. Обратите внимание на раздел файрвола **WAN** - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

8. Перейдите в **Status → IPsec** (там должно появиться созданное подключение), нажмите на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое указали в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **IPsec**

Подключение Kerio Control и Ideco NGFW Novum по IPsec

Функциональность доступна в **Классическом** и **Системном контекстах**.

Объединяемые локальные сети не должны пересекаться!

Предварительная настройка Kerio Control

1. По умолчанию Kerio Control использует IKEv1 для создания подключений к сторонним устройствам. Включить IKEv2 можно через консоль, выполнив действия:

- Подключиться к Kerio Control по SSH.
- Перейти в папку `/var/winroute`.
- Открыть на редактирование файл `winroute.cfg`.
- В нем найти раздел, начинающийся с текста `<table name="Firewall">`.
- В этом разделе найти строку `<variable name="IKEVersion">ikev1</variable>` и изменить в ней `ikev1` на `ikev2`.
- После этого требуется перезагрузить сервер и убедиться, что изменения в настройках сохранились.

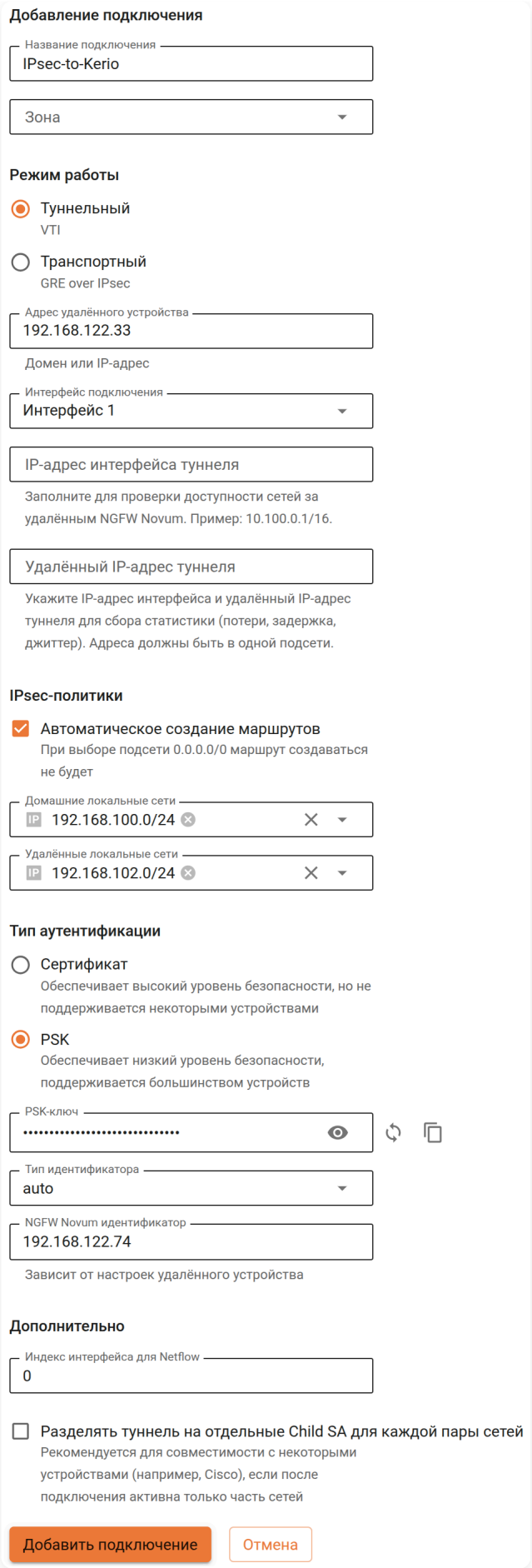
2. В разделе **Правила трафика** разрешите трафик VPN-служб.

Подключение от Ideco NGFW Novum к Kerio Control

Настройка исходящего подключения на Ideco NGFW Novum

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Исходящие подключения**.

2. Добавьте новое подключение и заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPsec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.

- **Адрес удаленного устройства** - укажите внешний IP-адрес Kerio Control. Если необходимы балансировка или резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение и создайте **Профиль next hop**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW Novum, которая будет видна из подсети Kerio Control.
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW Novum.
- **Тип аутентификации** - выберите тип PSK.
- **PSK-ключ** - укажите PSK-ключ, который будет использоваться для подключения.
- **Тип идентификатора** - выберите auto.
- **Идентификатор NGFW** - укажите IP-адрес внешнего интерфейса Ideco NGFW Novum, который будет использоваться для подключения.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Адреса должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

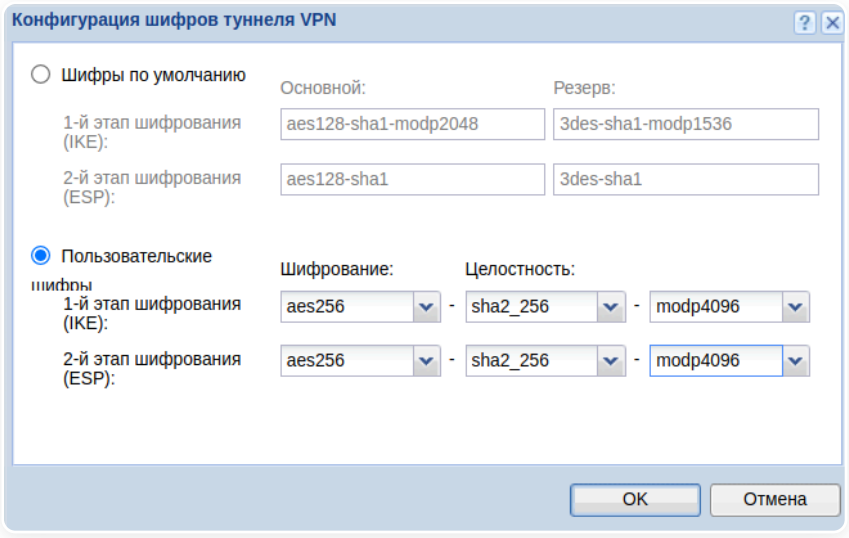
Настройка завершена, теперь переходим к настройке Kerio Control.

Настройка входящего подключения на Kerio Control

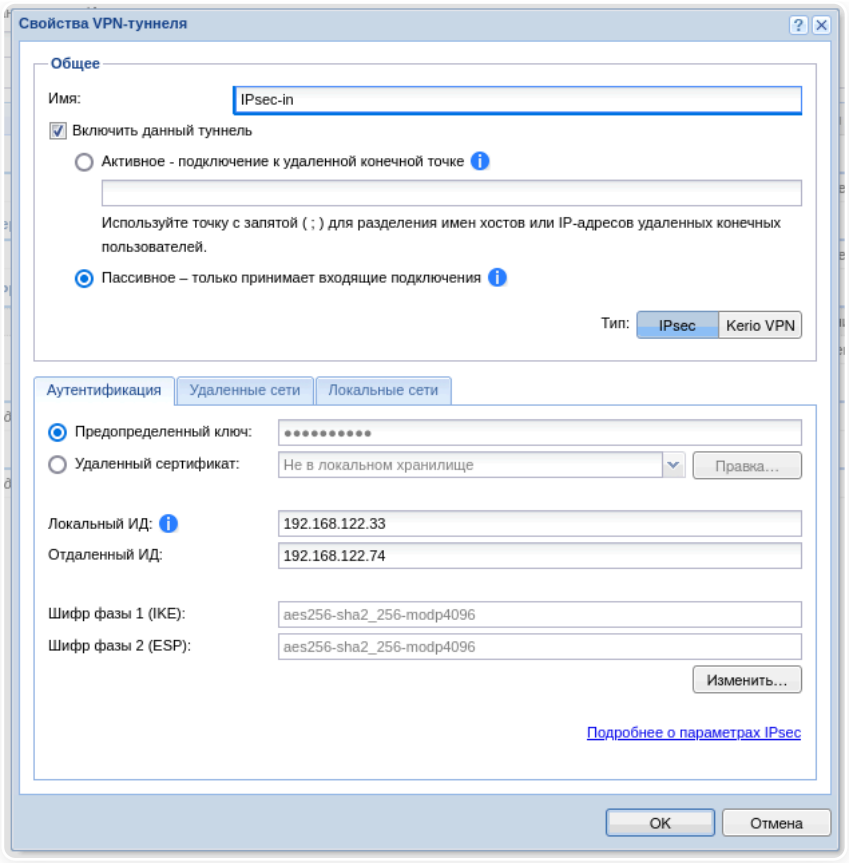
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель...**.

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec.
- **Имя** - произвольное.
- **Включить данный туннель**.
- Тип **Пассивное**.
- **Предопределенный ключ** - введите PSK-ключ, который был указан при создании подключения на Ideco NGFW Novum.
- **Локальный ИД** - укажите IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения.
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW Novum.
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



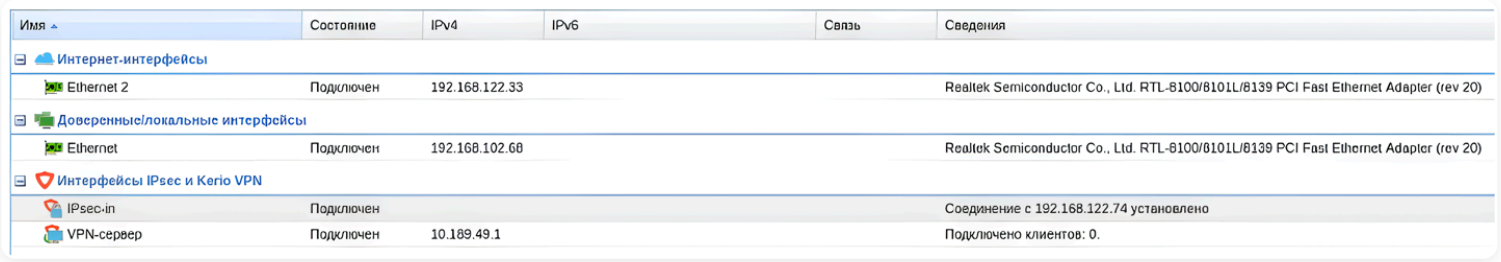
Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW Novum, которая будет видна из подсети Kerio Control.

4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW Novum, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице:



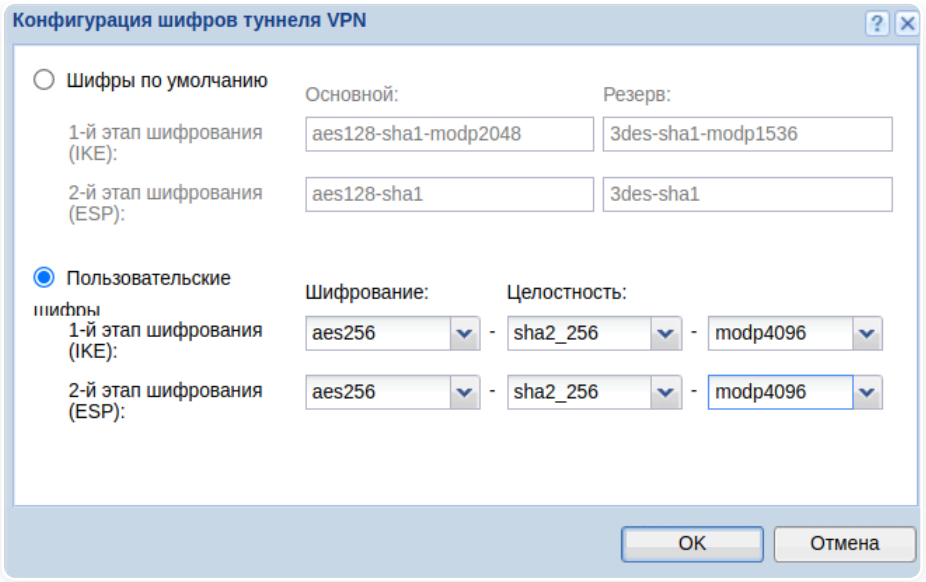
Подключение от Kerio Control к Ideco NGFW Novum

Настройка исходящего подключения на Kerio Control

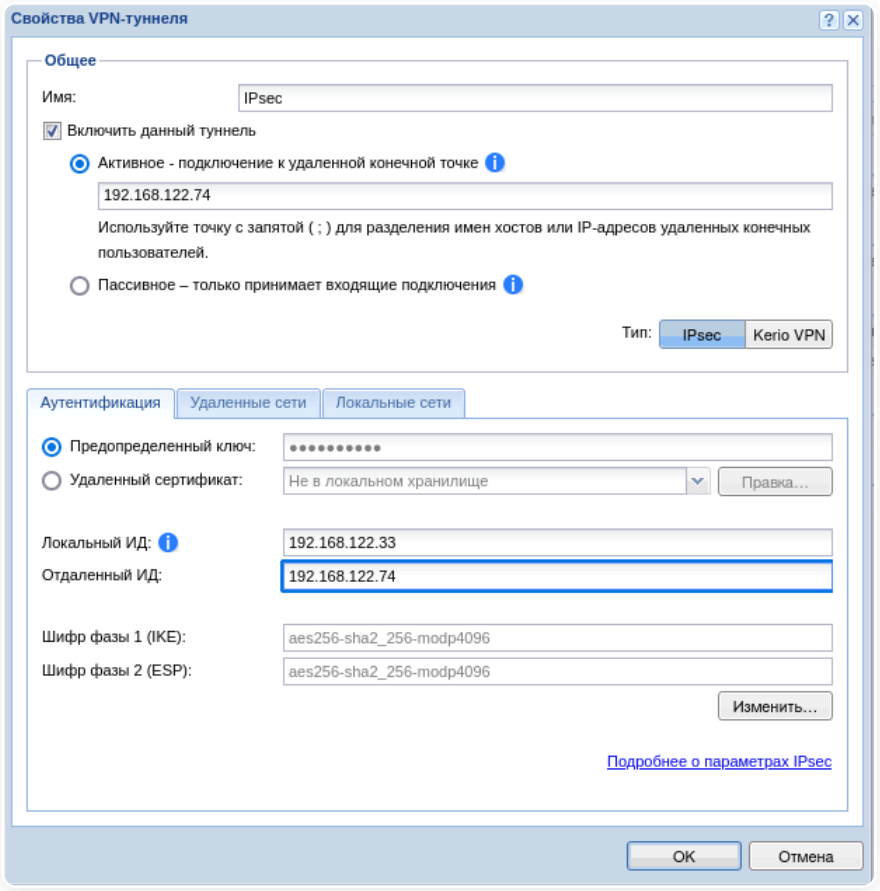
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель...**.

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec.
- **Имя** - произвольное.
- **Включить данный туннель**.
- Выберите тип **Активное** и в поле под ним пропишите IP-адрес внешнего интерфейса Ideco NGFW Novum, который будет использоваться для подключения.
- **Предопределенный ключ** - введите PSK-ключ, который будет использоваться для подключения.
- **Локальный ИД** - укажите ключ, который будет задан в поле **Идентификатор NGFW** при настройке входящего подключения на Ideco NGFW Novum, или IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения. **Предпочтительное значение - имя хоста Kerio**.
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW Novum, который будет использоваться для подключения.
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW Novum, которая будет видна из подсети Kerio Control.

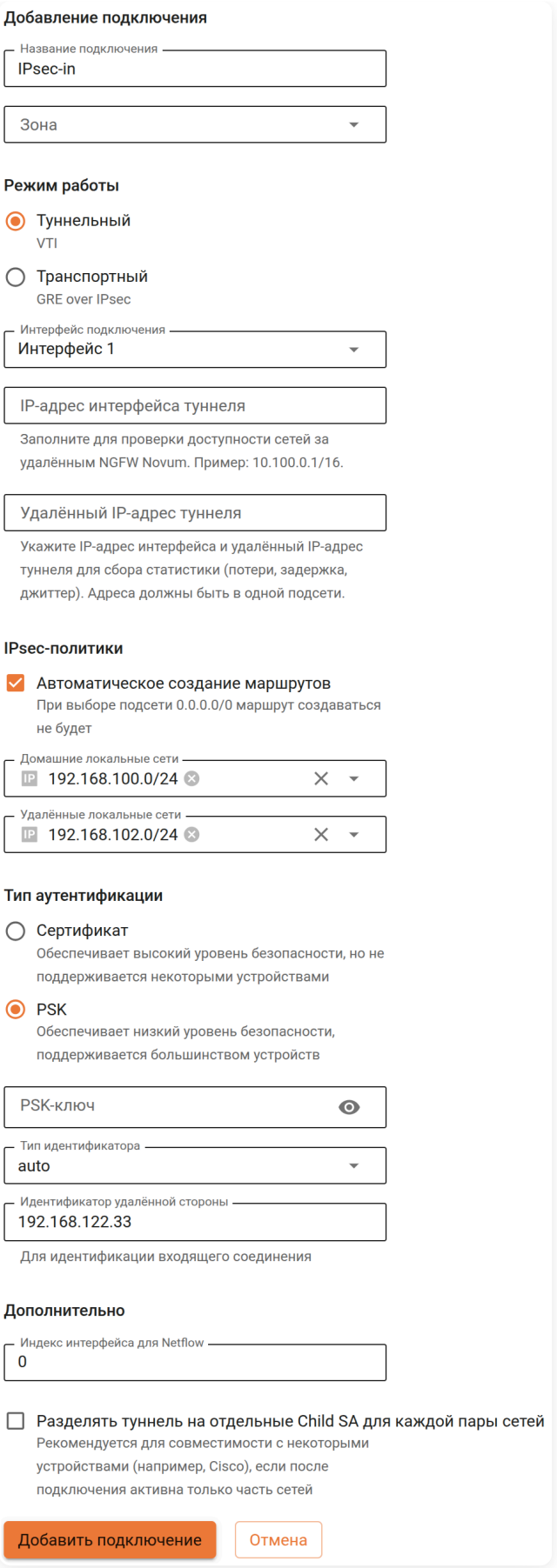
4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW Novum, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице.

Настройка входящего подключения на Ideco NGFW Novum

1. В веб-интерфейсе Ideco NGFW Novum откройте вкладку **Сервисы** → **IPsec** → **Входящие подключения**.

2. Добавьте новое подключение и заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec подключения. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Туннельный**.
- **Интерфейс подключения** - выберите интерфейс, который будет использоваться для создания подключения.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW Novum, которая будет видна из подсети Kerio Control.
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW Novum.
- **Тип аутентификации** - выберите тип PSK.
- **PSK-ключ** - введите PSK-ключ, который был указан при создании подключения в Kerio.
- **Тип идентификатора** - выберите auto.
- **Идентификатор удаленной стороны** - укажите **Локальный ИД**, указанный при настройке исходящего подключения на Kerio.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. IP-адреса должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

Настройка завершена.

При возникновении проблем обратите внимание на настройки файрвола Kerio Control.

В Ideco NGFW Novum имеется возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключения. При этом происходит перезапуск всех IPsec-соединений, в которых использовались измененные подсети.

Полезные ссылки

- **IPsec**

ГОСТ VPN

Практические руководства по работе с ГОСТ VPN в Ideco NGFW

Пример генерации ключей и сертификатов ГОСТ VPN

Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Пример генерации ключей и сертификатов ГОСТ VPN

Выполните команды:

1. Установите OpenSC (pkcs11-tool):

```
dnf install opensc
```

2. Создайте в текущей директории файл `openssl.conf`:

```
openssl_conf = openssl_init

[ openssl_init ]
engines = engine_section

[ engine_section ]
gost = gost_section

[ gost_section ]
dynamic_path = /usr/lib64/librtengine.so
pkcs11_path = /usr/lib64/librtpkcs11ecp.so
default_algorithms = CIPHERS, DIGEST, PKEY

[ crypto_policy ]
MinProtocol = TLSv1.2
MaxProtocol = TLSv1.3
Ciphersuites =  TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_SHA256:TLS_GOSTR34
CipherString = @SECLEVEL=1:kEECDH:kRSA:kEDH:kPSK:kDHEPSK:kECDHEPSK:kRSAPSK:-aDSS:-3DES:!DES:!RC4:!RC2:!IDEA:-SEED:!eNULL:!aNU
```

3. Включите поддержку ГОСТ в openssl:

```
export OPENSSL_CONF=openssl.conf
```

Далее введите команды для работы с сертификатами (в примере пин-код токена `12345678`).

4. Создайте закрытый ключ и CA сертификат:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out ca.key
openssl req -addext basicConstraints=CA:TRUE,pathlen:0 -x509 -new -nodes -days 3650 -key ca.key -out ca.crt -subj "/C=RU/ST=M
```

Здесь и далее в примере используются:

- `id = 3231 (hex) = 21 (dec)` - для локальных сертификатов;
- `id = 3230 (hex) = 20 (dec)` - для CA сертификатов.

5. Установите сертификат на токен:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l --pin 12345678 -y cert -w ca.crt --id 3230 --label GOST_CA_Cert
```

6. Сгенерируйте ключевую пару на токене:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen --key-type GOSTR3410-2012-256:A -l --pin 12345678 --id 3231 --
```

Важные параметры:

- `usage-derive`;
- `usage-decrypt`;
- `key-type GOSTR3410-2012-256:A`.

7. Сделайте запрос на сертификат (система запросит пин-код):

```
openssl req -addext basicConstraints=CA:FALSE,pathlen:0 -new -keyform engine -key "pkcs11:id=21" -engine rtengine -out server
```

Вместо домена `.test` указывайте реальный домен.

8. Подпишите сертификат:

```
openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -md_gost12_256
```

9. Установите сертификат на токен:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l --pin 12345678 -y cert -w server.crt --id 3231 --label GOST_Server_Cert
```

10. Если требуется протестировать, выгрузите сертификат из токена:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -p 12345678 -r --type cert --id 3231 | openssl x509 -inform der > server
```

Полезные ссылки

- **ГОСТ VPN**

Прокси

Практические руководства по настройке прокси-сервера в Ideco NGFW

Настройка Ideco NGFW в качестве прокси с одним интерфейсом

Перейти ›

Настройка программы Proxifier для прямых подключений к прокси-серверу

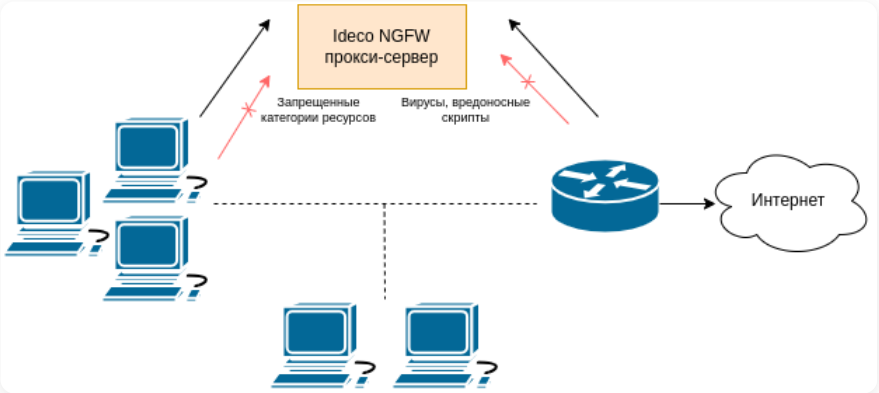
Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка Ideco NGFW Novum в качестве прокси с одним интерфейсом

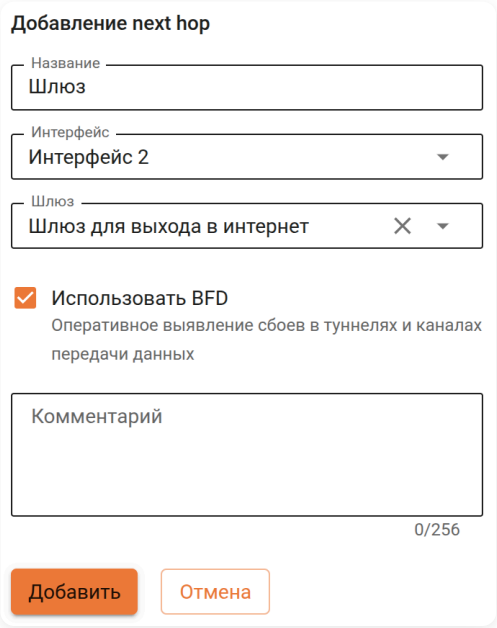
Функциональность доступна в **Классическом** и **Системном контекстах**.



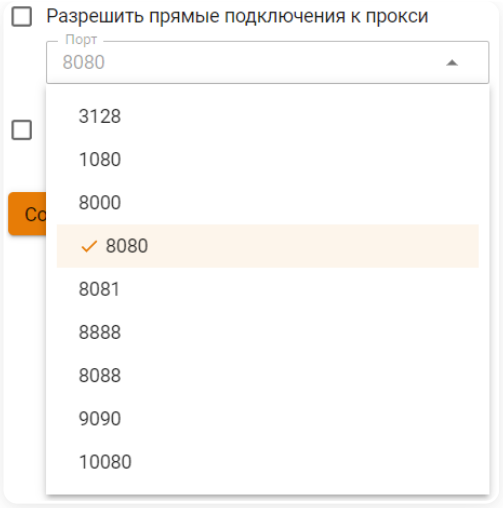
При необходимости можно использовать Ideco NGFW Novum в качестве прокси-сервера с прямыми подключениями клиентов к прокси. Для этого выполните действия:

1. Создайте интерфейс с ролью LAN через локальное меню сервера. Подробнее в статье.

2. Перейдите в **SD-WAN** → **Next hop** и добавьте шлюз для настроенного интерфейса:



3. Разрешите прямые подключения к прокси-серверу в разделе **Сервисы** → **Прокси**, выбрав нужный порт из списка:



Если прямое подключение к прокси требуется только части клиентских устройств или части локальных интерфейсов, то создайте INPUT-правило **Межсетевого экрана**. Пример приведен ниже.

При использовании запрещающих все правил:

- Убедитесь, что разрешающие правила для прокси расположены выше в таблице.
- Проверьте, что трафик служебной подсети `169.254.1.0/30` не ограничен FORWARD-правилами **Межсетевого экрана**.

Для учета, контроля и проверки веб-трафика на вирусы, требуется соблюдение следующих условий:

- Локальная подсеть не пересекается с внешним интерфейсом NGFW Novum.
- У сервера Ideco NGFW Novum есть доступ в интернет.
- На клиентских устройствах указан адрес веб-прокси (в настройках прокси-сервера в браузерах).

Пример настройки INPUT-правила

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **INPUT**, создайте **разрешающее** правило и включите:

- **Протокол** - TCP.
- **Источник**:
  - **Зона источника** - локальный интерфейс или конкретные интерфейсы.
  - **Адрес** - IP-адреса или подсети разрешенных пользовательских устройств.
- **Назначение**:
  - **Адрес** - IP-адрес локального интерфейса NGFW.
  - **Порт назначения** - порт, указанный в настройках **Прокси**.
- **Действия** - **Разрешить**.

2. Если необходимо ограничить доступ к прокси, создайте **запрещающее** INPUT-правило и поместите под разрешающим:

- **Протокол** - TCP.
- **Источник**:
  - **Зона источника** - локальный интерфейс или конкретные интерфейсы.
  - **Адрес** - **Любой**. Доступ будет запрещен всем, кроме адресов в разрешающем правиле.
- **Назначение**:
  - **Адрес** - IP-адрес локального интерфейса NGFW.
  - **Порт назначения** - порт, указанный в настройках **Прокси**.
- **Действия** - **Запретить**.

Настройка прямого подключения к прокси на клиентских устройствах

Для настройки выполните действия:

1. Укажите IP-адрес локального интерфейса Ideco NGFW Novum в качестве веб-прокси в локальной сети на клиентских устройствах.

2. В настройках прокси на клиентской машине укажите порт для прямых подключений к прокси (возможен выбор портов из списка: 3128, 1080, 8000, 8080, 8888, 8081, 8088, 10080).

Если в настройках программы под ОС Windows или macOS X нет возможности указать прокси-сервер, воспользуйтесь сторонним ПО для маршрутизации всего трафика рабочей станции на прокси-сервер. Такую возможность предоставляет программа **Proxifier**, которую можно настроить для прямых подключений к прокси. Для настройки воспользуйтесь статьей.

Полезные ссылки

- **Прокси**

Настройка программы Proxifier для прямых подключений к прокси серверу

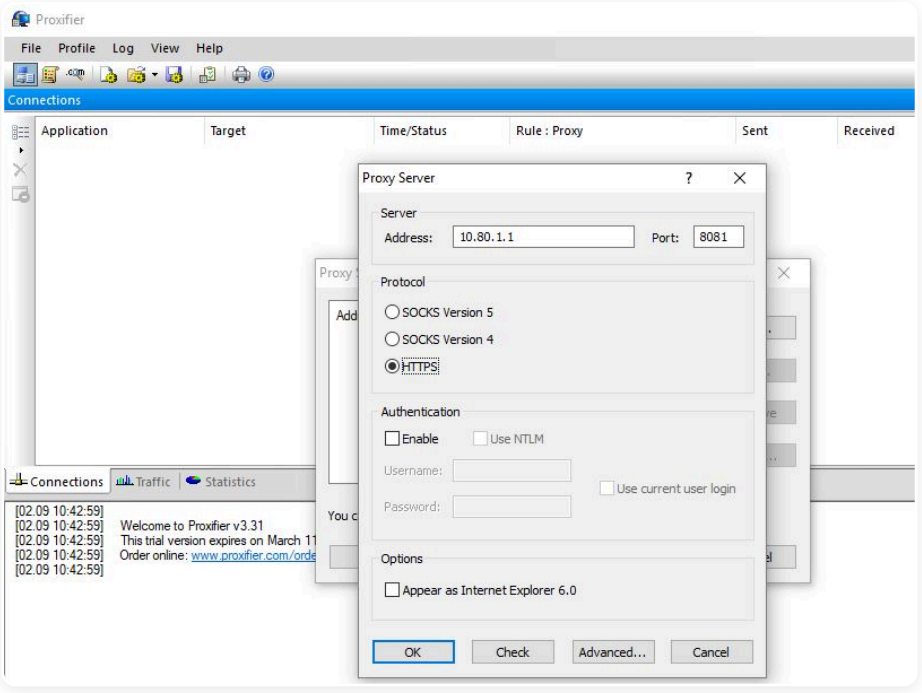
Функциональность доступна в **Классическом** и **Системном контекстах**.

Скачать Proxifier можно с сайта разработчика.

Настройка

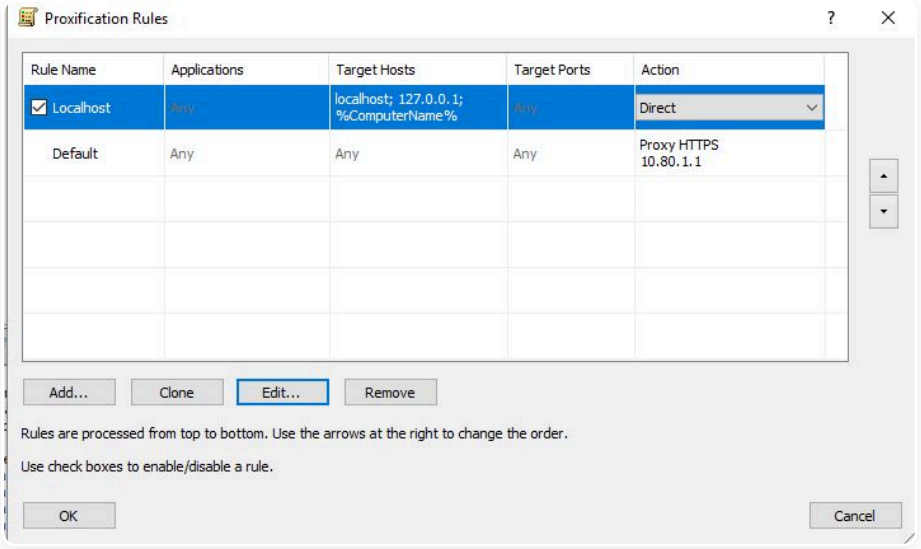
Выполните стандартные настройки браузера для прямых подключений к прокси-серверу, а затем настройте программу для перенаправления остального трафика на прокси-сервер.

Пропишите в настройках прокси-сервера в Proxyfier IP-адрес локального интерфейса Ideco NGFW Novum и порт, указанный в настройке прокси для прямых подключений (см. документацию по прокси-серверу). Тип протокола: HTTPS. Настройки авторизации указывать необязательно:



После добавления прокси-сервера ответьте утвердительно на вопросы о создании правил перенаправления трафика на него.

Либо эти настройки можно отредактировать позже:



Настройка закончена, программы будут выходить в интернет через заданный прокси-сервер.

Полезные ссылки

- **Прокси**

Правила трафика

Практические руководства по настройке правил трафика в Ideco NGFW

Блокировка популярных ресурсов

Настройка блокировки популярных интернет-ресурсов

Перейти >

Контент-фильтр

Настройка блокировки через Контент-фильтр

Перейти >

Межсетевой экран

Настройка правил Межсетевого экрана

Перейти >

Ручная корректировка GeoIP

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Контент-фильтр

Практические руководства по настройке Контент-фильтра в Ideco NGFW

Блокировка чат-ботов

Настройка блокировки чат-ботов в Контент-фильтре

Перейти >

Настройка HTTP-метода

Пример настройки HTTP-метода в Контент-фильтре

Перейти >

Настройка MIME-типов

Пример настройки MIME-типов в Контент-фильтре

Перейти >

Блокировка загрузки файлов в файлообменники

Настройка блокировки загрузки файлов в файлообменники в Контент-фильтре

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

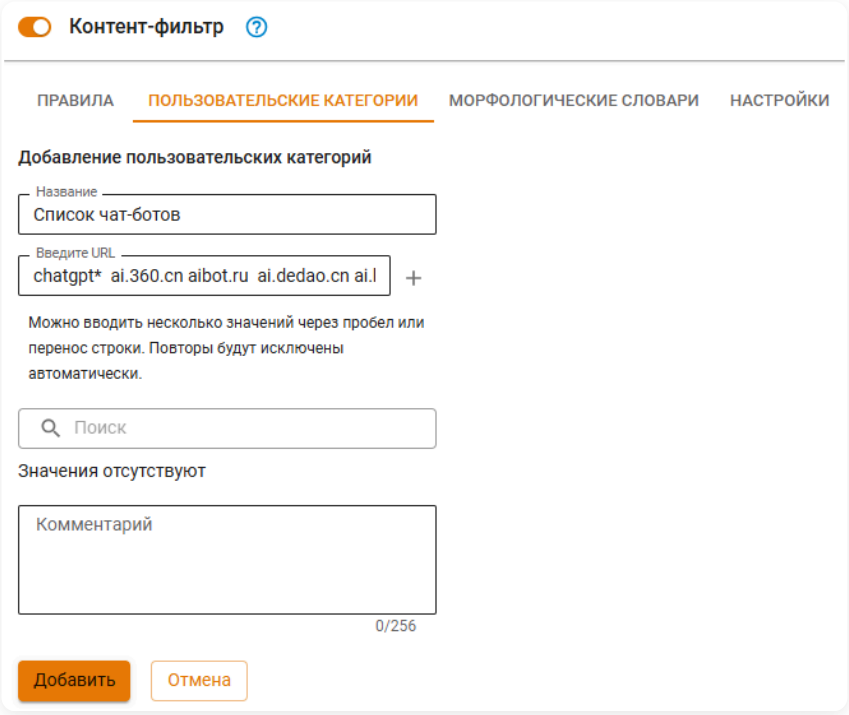
OK

Блокировка чат-ботов

Для блокировки ресурсов, которые взаимодействуют с чат-ботами, необходимо создать правило в **Контент-фильтре**:

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Пользовательские категории**.

2. Добавьте новую категорию и заполните поля:



- **Название** - введите любое название.
- **URL** - скопируйте и вставьте список URL из блока ниже.
- **Комментарий** - заполнение не обязательно.

Список URL

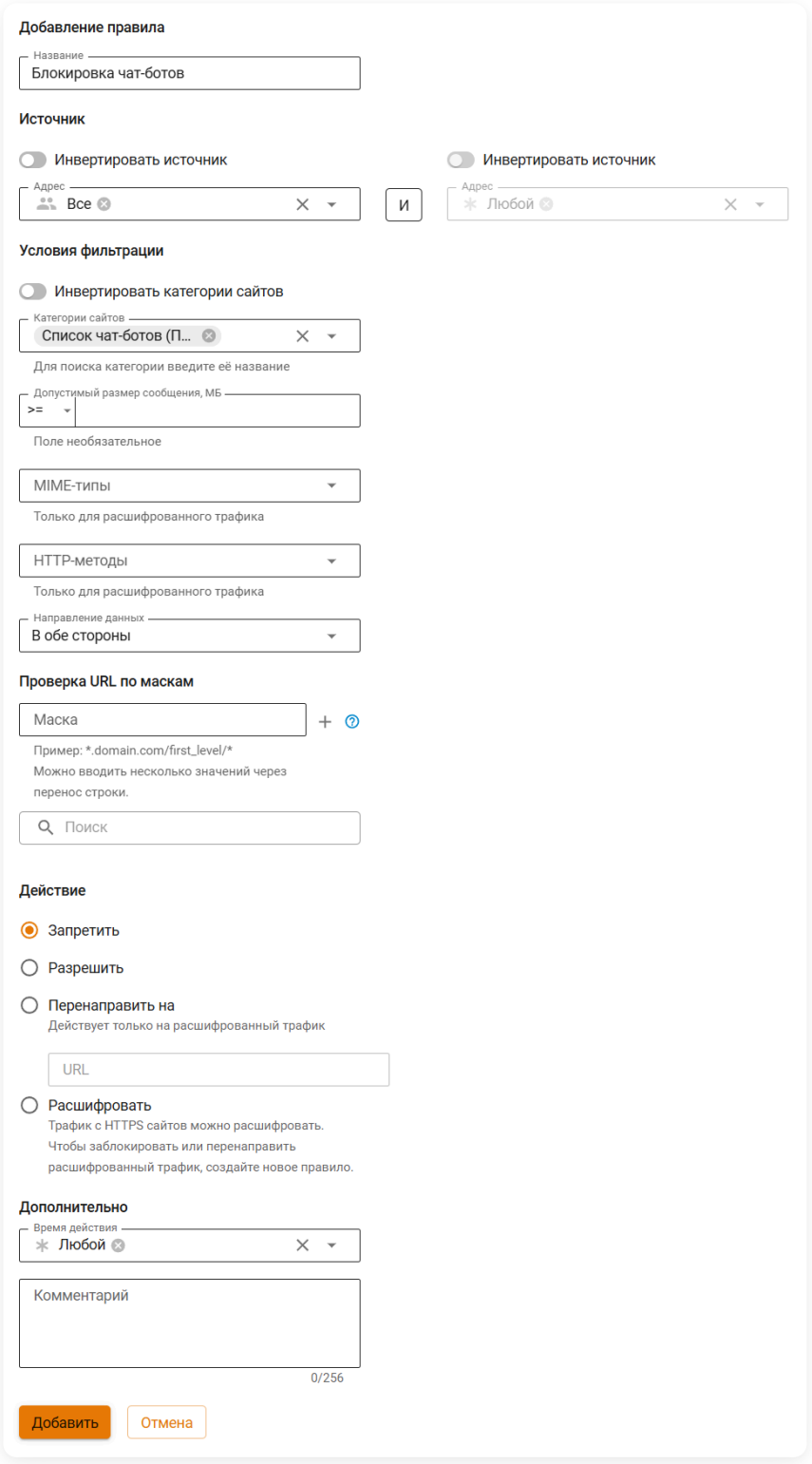
```
chatgpt*
ai.360.cn
aibot.ru
ai.dedao.cn
ai.ls
aiservice.vercel.app
aitianhu.com
anse.app
anthropic.com
b.ai-huan.xyz
bard.google.com
bettergpt.chat
bing.com
chadgpt.ru
character.ai
chat4gpt.ru
chat9.yqcloud.top
chat.acytoo.com
chataigpt.org
chat.ai-open.ru
chatboxai.app
chat.dfehub.com
chat.getgpt.world
chatglm.cn
chatgp.ru
chat.gpt4free.io
```

```
chatgpt4rus.ru
chatgpt.ai
chatgptbot.ru
chat-gpt.com
chatgptfree.ai
chat-gpt-free.ru
chatgptlogin.ac
chatgpt-me.ru
chat-gpt-na.ru
chatgptnarusskom.ru
chat-gpt.org
chatgpt.org
chatgpt.pro
chat-gpt.ru
chatgpt-telegram.com
chatgptweb.ru
chathub.gg
chatinfo.ru
chat.lmsys.org
chat.openai.com
chat.ramxn.dev
chat.su
claude.ai
crfm.stanford.edu
deepai.org
easychat-ai.app
itbabushka.com
forefront.com
freechatgpt.chat
free-chatgpt.ru
free.easychat.work
gpt2.ru
gpt4all.io
gpt-chatbot.ru
gptchatbot.ru
gptchatly.com
gpt-gm.h2o.ai
gptgo.ai
gpt-open.ru
gptschat.ru
gradio.app
h2o.ai
huggingface.co
iask.ai
liaobots.com
liftweb.ru
lmsys.org
macgpt.com
mashagpt.ru
moss.fastnlp.top
neice.tiangong.cn
openai.ru
openai-gpt.ru
openai-chat-gpt.ru
open-assistant.io
opencat.app
petals.ml
play.vercel.ai
poe.com
ru-chatgpt.ru
rugpt.chat
sdk.vercel.ai
supertest.lockchat.app
tenchat.ru
theb.ai
timeai.ru
tongyi.aliyun.com
tools.zmo.ai
trychatgpt.ru
wewordle.org
xinghuo.xfyun.cn
```

```
yandex-gpt.com
yandex-gpt.ru
yiyan.baidu.com
you.com
zhpt.tech
```

4. Сохраните категорию.

3. Перейдите в **Правила** и добавьте новое правило с действием **Запретить**:



Полезные ссылки

- **Правила**
- **Описание категорий Контент-фильтра**

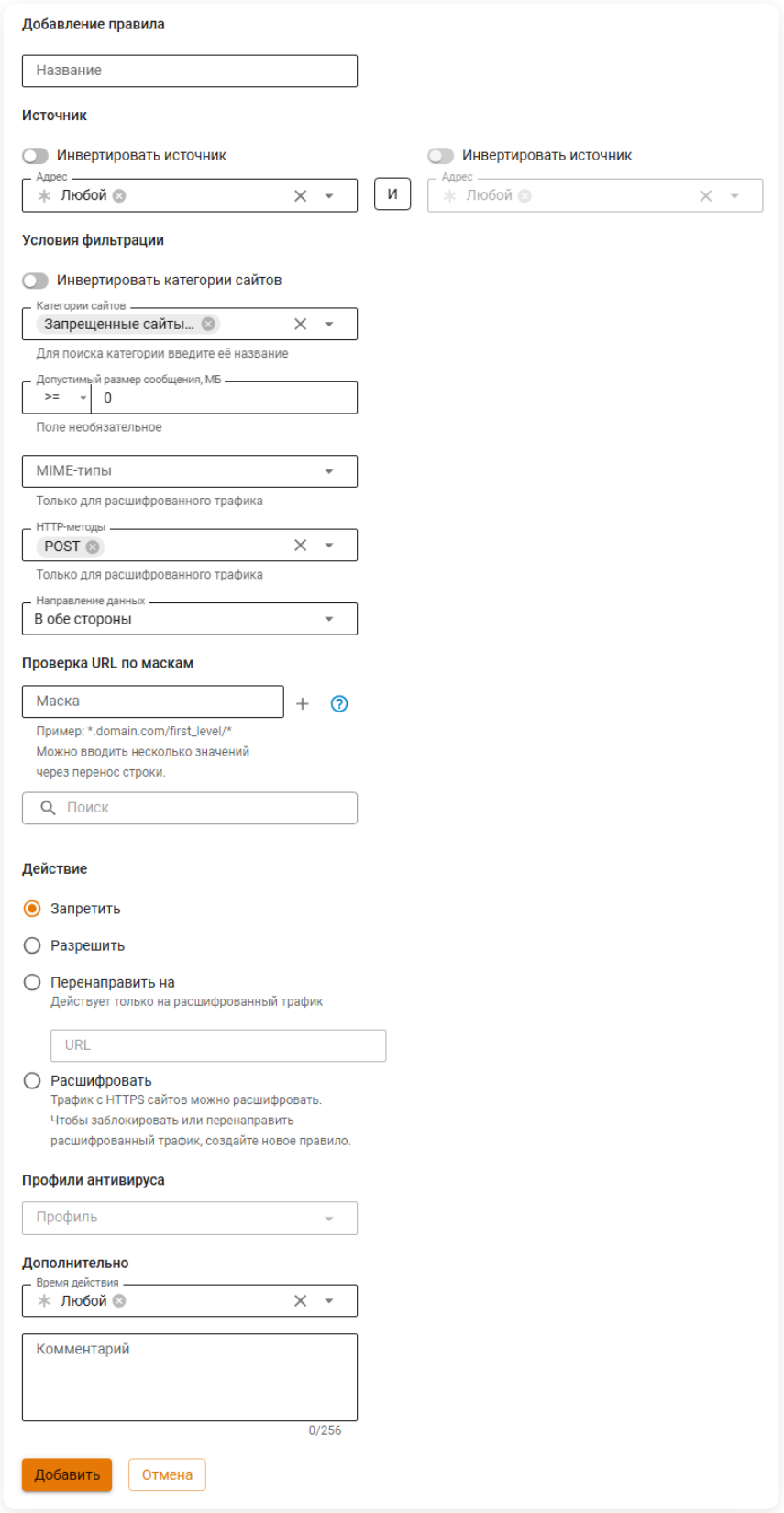
- **Контент-фильтр**

Настройка HTTP-метода

Пример. Необходимо запретить пользователям вводить данные на запрещенных сайтах.

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**.

2. Заполните поля:



- **Адрес** - выберите пользователей, для которых будет работать правило.
- **Категории сайтов** - выберите категорию сайтов, для которых должно работать правило, например, **Запрещенные сайты**.
- **HTTP-методы** - выберите метод `POST`, чтобы запретить отправку данных на определенный ресурс.
- Выберите **Запретить**, чтобы правило работало как запрещающее.

При сохранении правила сайты будут открываться, но пользователь не сможет отправить данные (например, заполнить форму обратной связи или ввести логин и пароль).

Полезные ссылки

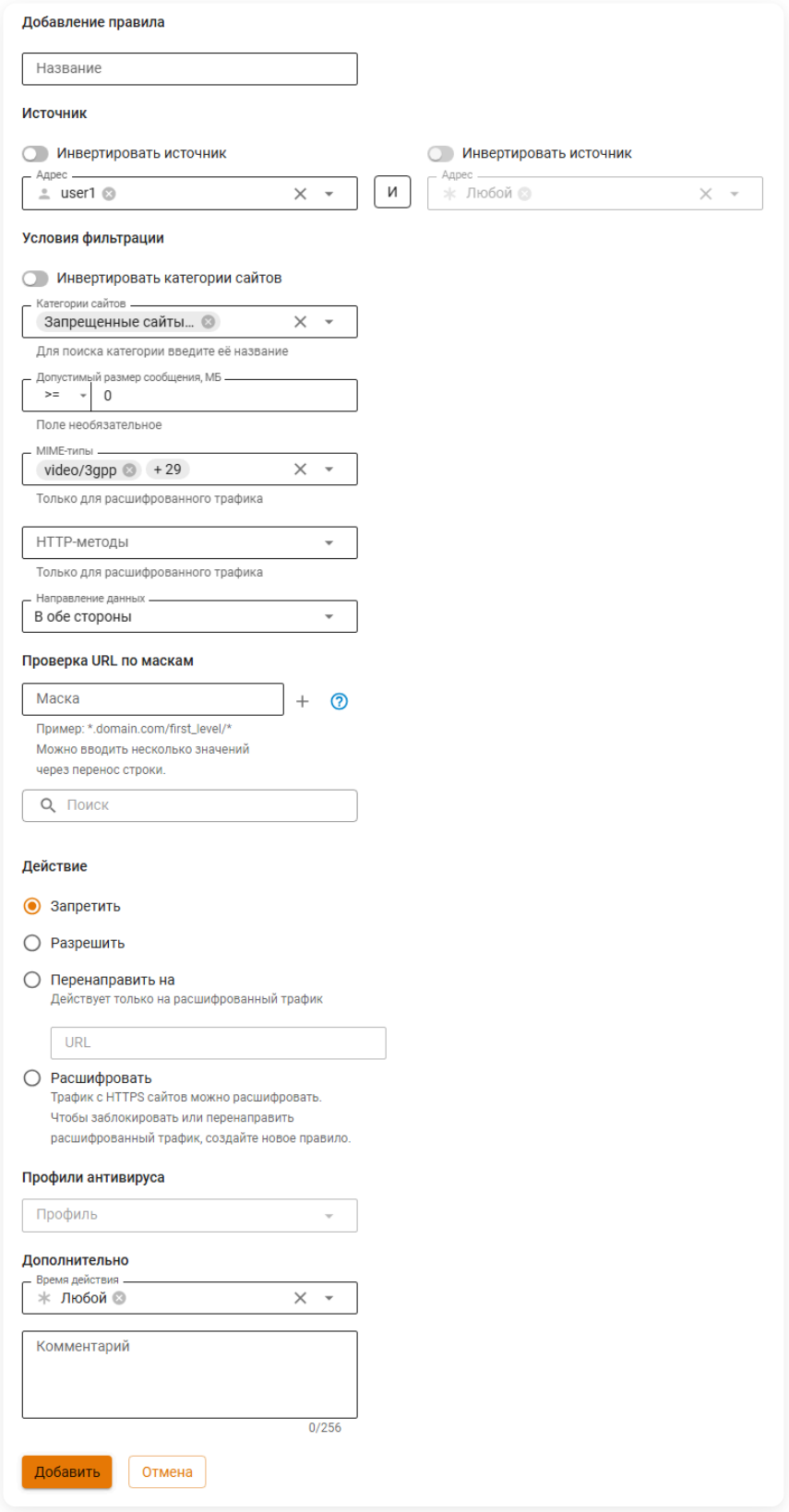
- **Настройка фильтрации HTTPS**

Настройка MIME-типов

Пример. Необходимо запретить конкретному пользователю (например, user1) воспроизводить видеоконтент на запрещенных сайтах.

1. Перейдите в **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**.

2. Заполните поля, как на скриншоте:



- В поле **Категории сайтов** укажите предварительно созданную пользовательскую категорию **Запрещенные сайты**.
- В поле **MIME-типы** выберите все форматы группы **Video**.
- Примените действие правила **Запретить**.

При сохранении правила сайт откроется, если трафик не заблокирован другим правилом, но видеоконтент не воспроизведется.

Полезные ссылки

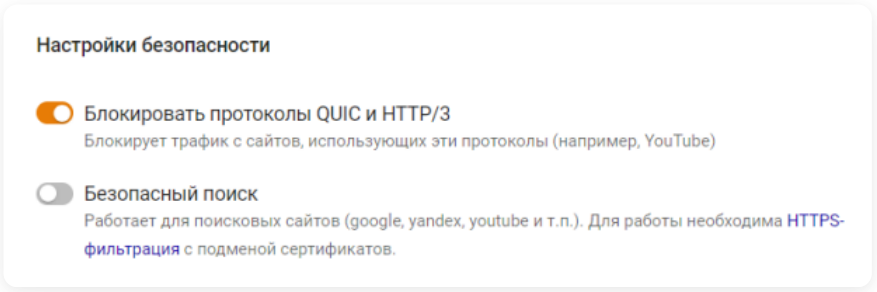
- **Настройка фильтрации HTTPS**

Блокировка загрузки файлов в файлообменники

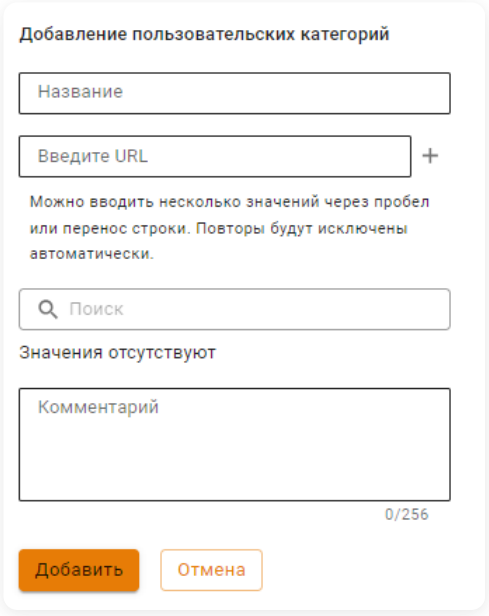
Блокирование этой категории требует особой настройки правил **Контент-фильтра**. В случае с файлообменниками расшифровки трафика может быть недостаточно у категорий: **Файлообменники, Файловые хранилища, Файловые архивы** и **Загрузка файлов в файлообменники**.

Чтобы заблокировать загрузку файлов в облака через браузер, выполните действия:

1. Включите **Блокировку протоколов Quic/HTTP3** в **Контент-фильтр** → **Настройки**:



2. Создайте пользовательскую категорию для расшифровки трафика и укажите домены нужных файлообменников, используя маску `example.com`:



3. Создайте правило, расшифровывающее трафик созданной в пункте 2 категории:



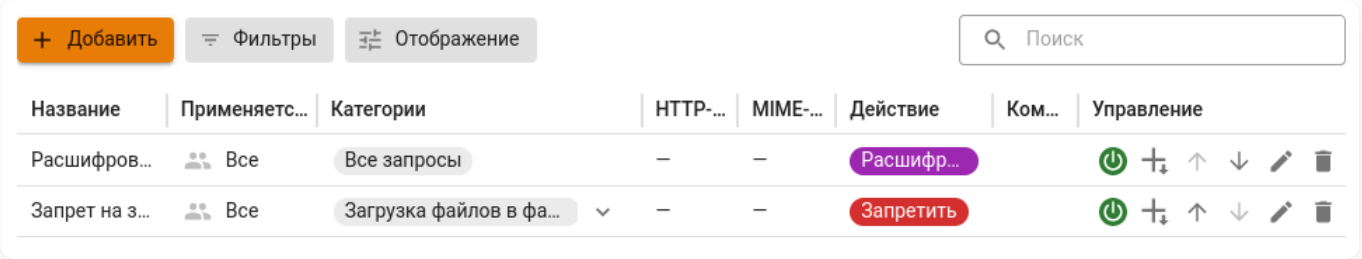
4. Ниже создайте запрещающее правило для категории **Загрузка файлов в файлообменник**:



5. Проверьте, работает ли блокировка: с устройства пользователя, для которого настроена, зайдите на сайты нужных файлообменников и попробуйте загрузить файлы.

Если загрузка проходит, то:

- Добавьте в пользовательскую категорию домены файлообменников, используя любые варианты масок: `subdomain.example.com`, `*.subdomain.example.com`, `subdomain.example.com/home`, `*.example.com`.
- Создайте в **Контент-фильтре** правило, расшифровывающее весь трафик пользователя, а ниже - правило, запрещающее загрузку файлов в файлообменники:



Если не удалось выполнить настройку, то обратитесь в Техническую поддержку.

Полезные ссылки

- **Контент-фильтр**
- **Описание категорий Контент-фильтра**

Межсетевой экран

Практические руководства по настройке правил Межсетевого экрана в Ideco NGFW

Как разрешить доступ к ресурсам в ограниченной сети

Примеры настройки правил для разрешения доступа к конкретным ресурсам при ограниченном интернете

Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

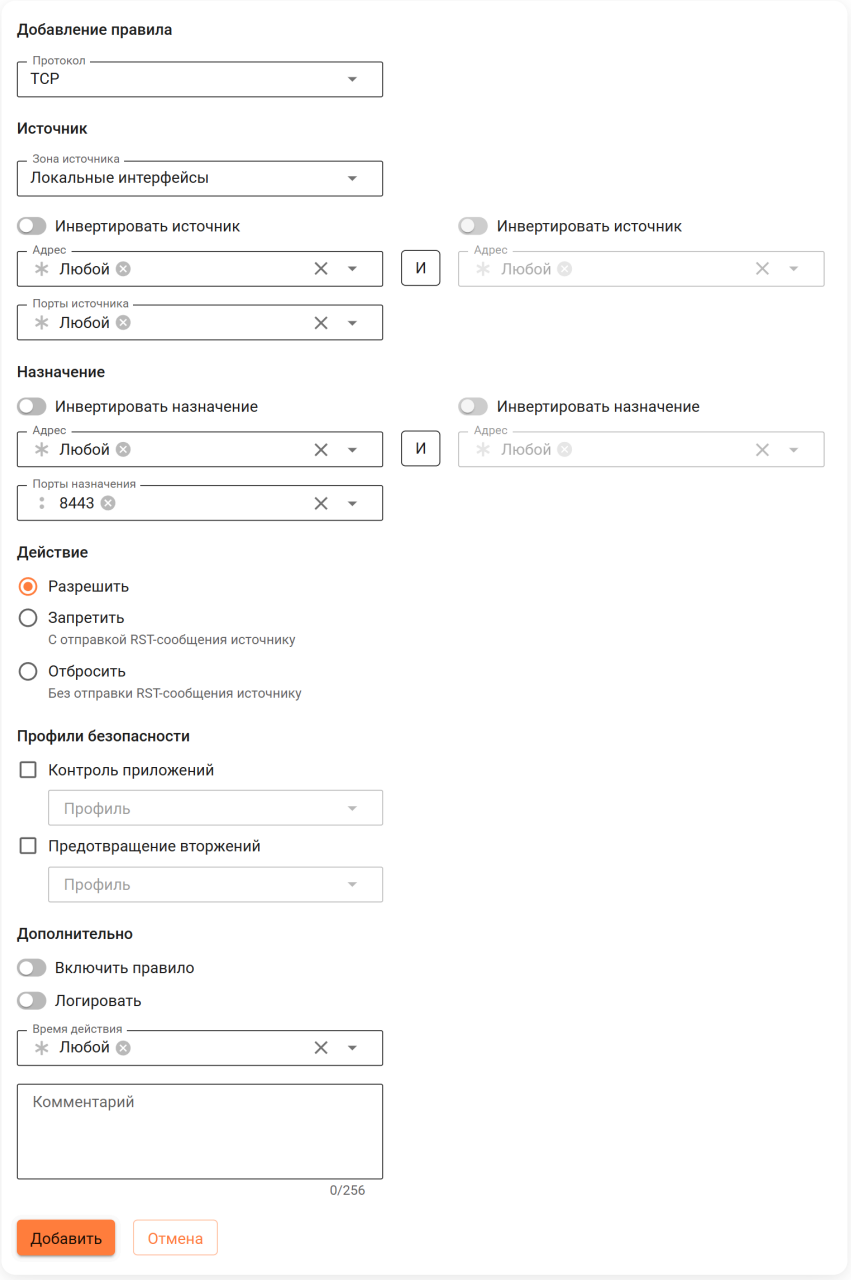
OK

Как разрешить доступ к ресурсам в ограниченной сети

Разрешить доступ к веб-интерфейсу Ideco NGFW Novum из локальной сети

Пример. Необходимо ограничить доступ ко всем внутренним ресурсам Ideco NGFW Novum, кроме веб-интерфейса администратора Ideco NGFW Novum.

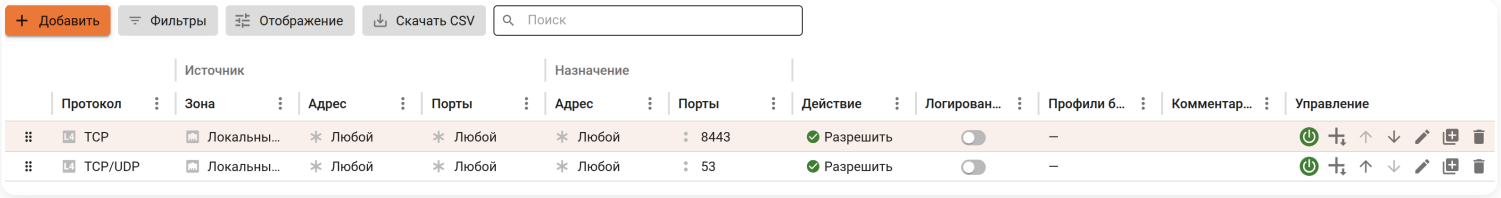
1. В **Правила трафика** → **Межсетевой экран** → **INPUT** создайте разрешающее правило, заполнив поля:



- **Протокол** - протокол транспортного уровня TCP.
- **Зона источника** - можно выбрать только один источник, для каждого источника создается отдельное правило. Выберите значение **Локальные интерфейсы**, чтобы разрешить доступ из локальной сети.
- **Адрес источника** - при необходимости укажите учетную запись пользователя или IP-адрес, которому необходимо разрешить доступ к веб-интерфейсу Ideco NGFW Novum.
- **Порт** - 8443.

Включите правило и нажмите **Добавить**.

2. Если Ideco NGFW Novum используется как DNS-сервер или включен перехват пользовательских DNS-запросов, необходимо в таблице INPUT создать правила для протоколов TCP и UDP, разрешающие подключение из локальной сети на порт 53:



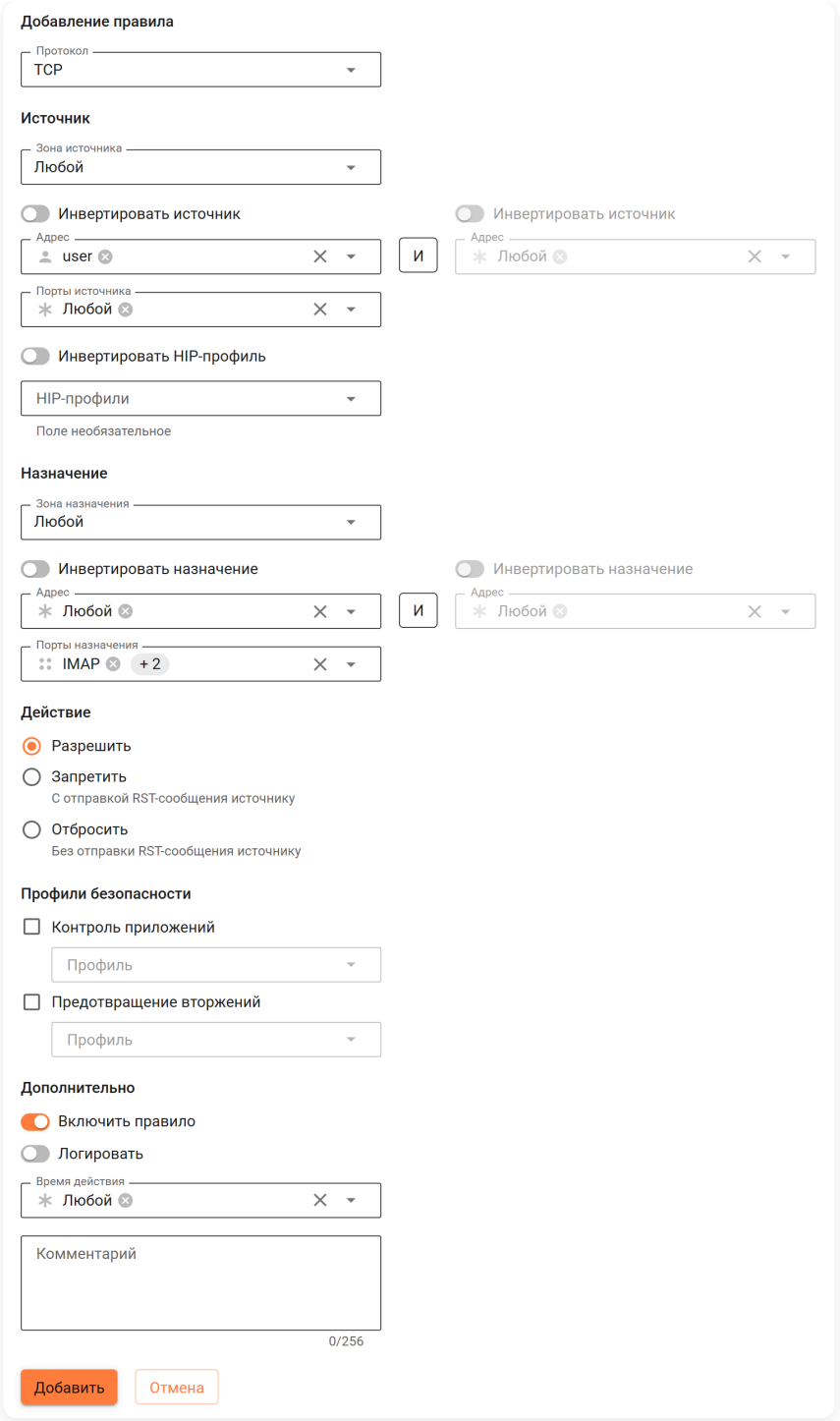
3. Создайте запрещающее весь трафик правило INPUT. При создании правила доступна опция **Включить правило** в разделе **Дополнительно**. Не включайте правило, пока не убедитесь, что в таблице разрешающее правило находится выше запрещающего.

При потере доступа к веб-интерфейсу Ideco NGFW Novum воспользуйтесь опцией **Полный доступ**.

Разрешить доступ к почтовым сервисам конкретному пользователю

Пример. Необходимо ограничить весь транзитный трафик всем пользователям, но разрешить доступ к внешним почтовым сервисам пользователю user.

1. В **Правила трафика** → **Межсетевой экран** → **FORWARD** создайте разрешающее правило, заполнив поля:



- **Протокол** - протокол транспортного уровня TCP.
- **Адрес источника** - user.
- **Порты назначения** - IMAP, POP3, MAIL (порты, используемые для передачи почты по протоколам POP3, IMAP, SMTP в т.ч. защищенных версий).

Включите правило и нажмите **Добавить**.

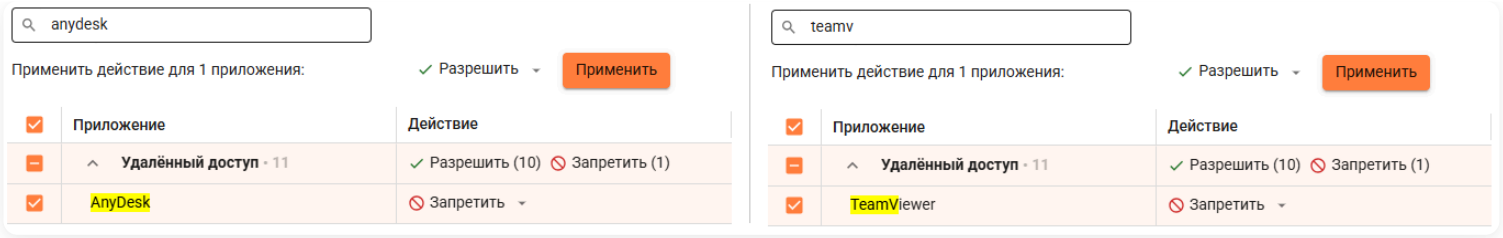
2. Создайте запрещающее весь трафик правило FORWARD. В таблице поместите разрешающее правило выше запрещающего.

Разрешить трафик из локальной во внешнюю сеть, но запретить конкретные приложения

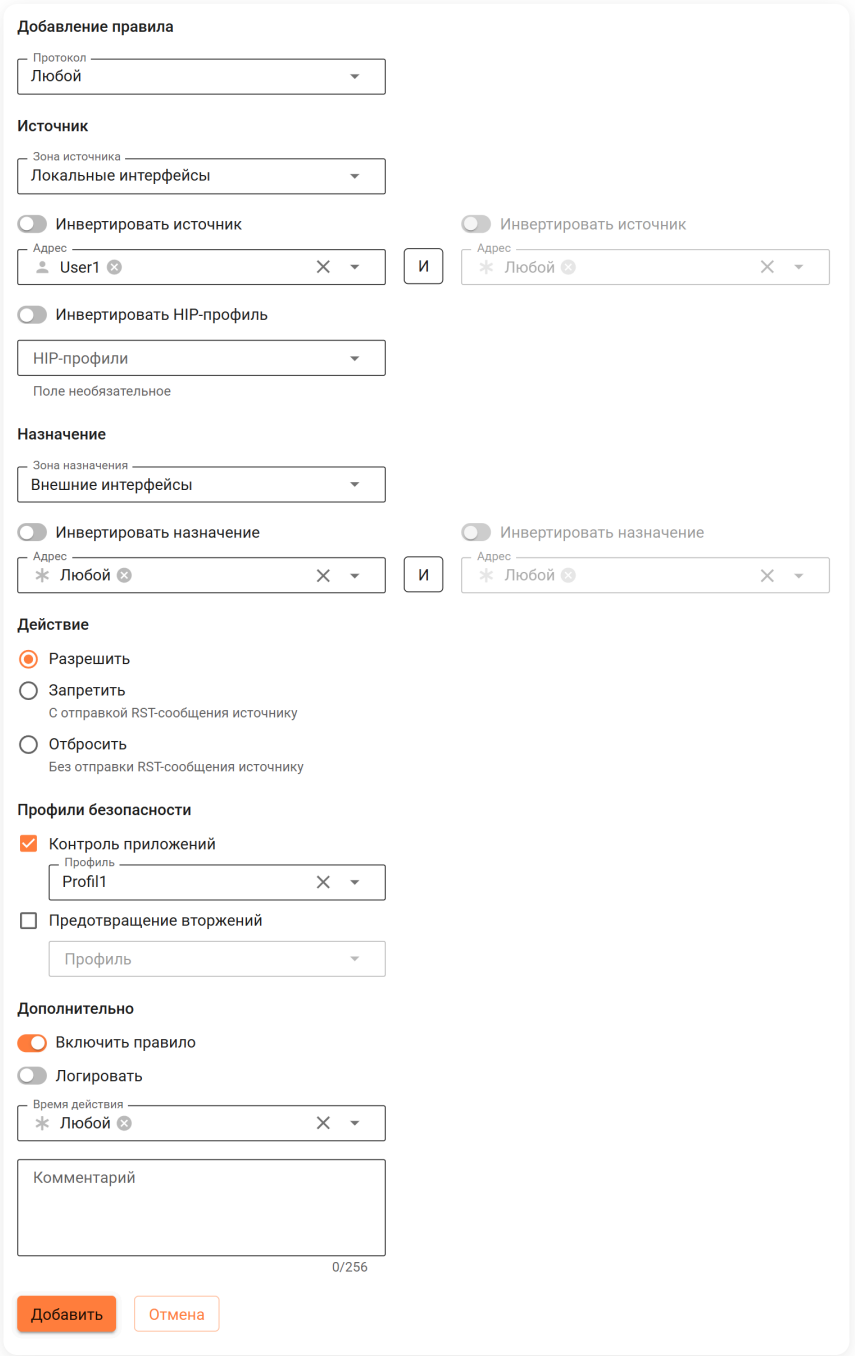
Пример. Необходимо ограничить весь транзитный трафик, но разрешить трафик из локальной во внешнюю сеть. При этом нужно запретить доступ пользователю `User1` к приложению удаленного доступа AnyDesk, а пользователю `User2` - к TeamViewer.

Выполните действия:

1. В разделе **Профили безопасности** → **Контроль приложений** создайте профили (например, `Profil1` и `Profil2`), запрещающие доступ к AnyDesk и TeamViewer:



2. В разделе **Правила трафика** → **Межсетевой экран** → **FORWARD** добавьте разрешающее правило для `User1`, заполнив поля:

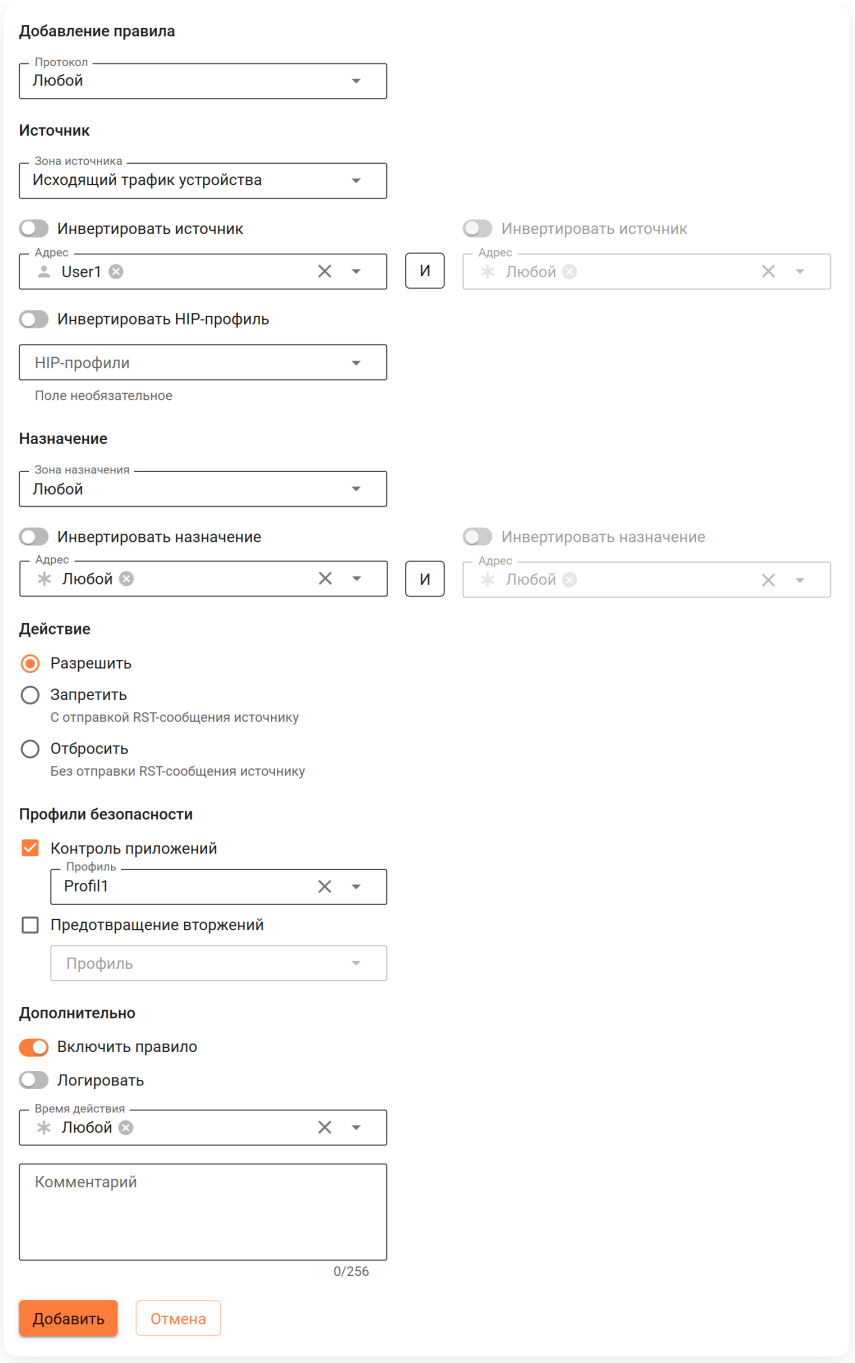


- **Протокол** - выберите **Любой**.
- **Зона источника** - выберите **Локальные интерфейсы**, чтобы разрешить доступ из локальной сети.
- **Адрес** - выберите пользователя `User1`.
- **Зона назначения** - выберите **Внешние интерфейсы**, чтобы разрешить доступ во внешнюю сеть.
- **Профили безопасности** - укажите профиль **Контроля приложений** `Profil1`, созданный в шаге 1.

Включите правило и нажмите **Добавить**.

3. По аналогии с шагом 2 добавьте разрешающее правило для `User2` с профилем **Контроля приложений** `Profil2`.

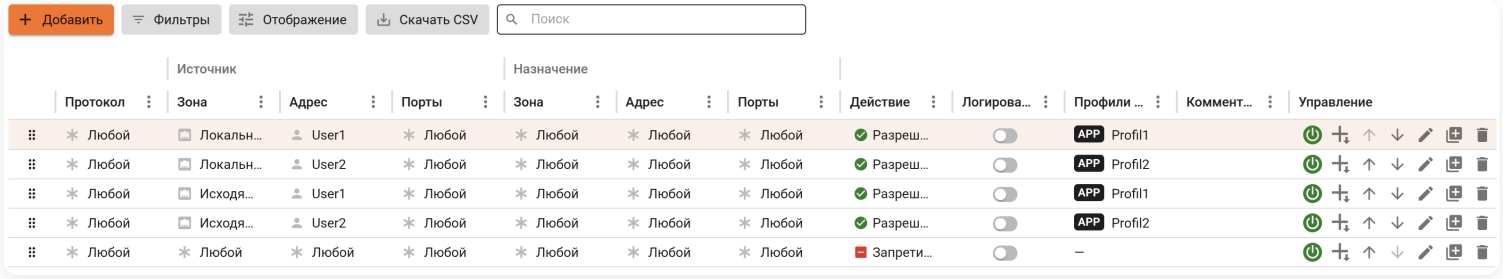
4. Добавьте правило, разрешающее трафик для специальной зоны источника **Исходящий трафик устройства** для `User1`:



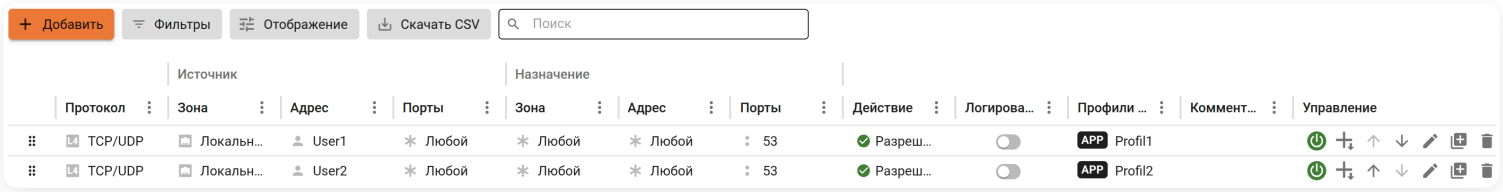
- **Протокол** - выберите **Любой**.
- **Зона источника** - выберите **Исходящий трафик устройства**, необходимо для работы прямого и прозрачного прокси, веб-трафика.
- **Адрес** - выберите пользователя `User1`.
- **Зона назначения** - выберите **Любой**.
- **Профили безопасности** - укажите профиль **Контроля приложений** `Profil1`.

5. По аналогии с шагом 4 добавьте разрешающее правило для `User2` с профилем **Контроля приложений** `Profil2`.

6. Создайте запрещающее весь трафик правило FORWARD. В таблице поместите разрешающие правила выше запрещающего:



7. Если в разделе **Сервисы** → **DNS** включена опция **Перехват пользовательских DNS-запросов**, создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**. Это необходимо для инспекции перехваченного DNS-трафика, поскольку он направляется в INPUT:



Полезные ссылки

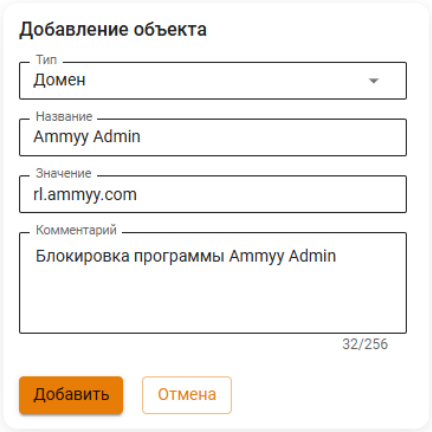
- **Межсетевой экран**
- **Примеры создания правил межсетевого экрана**

Блокировка популярных ресурсов

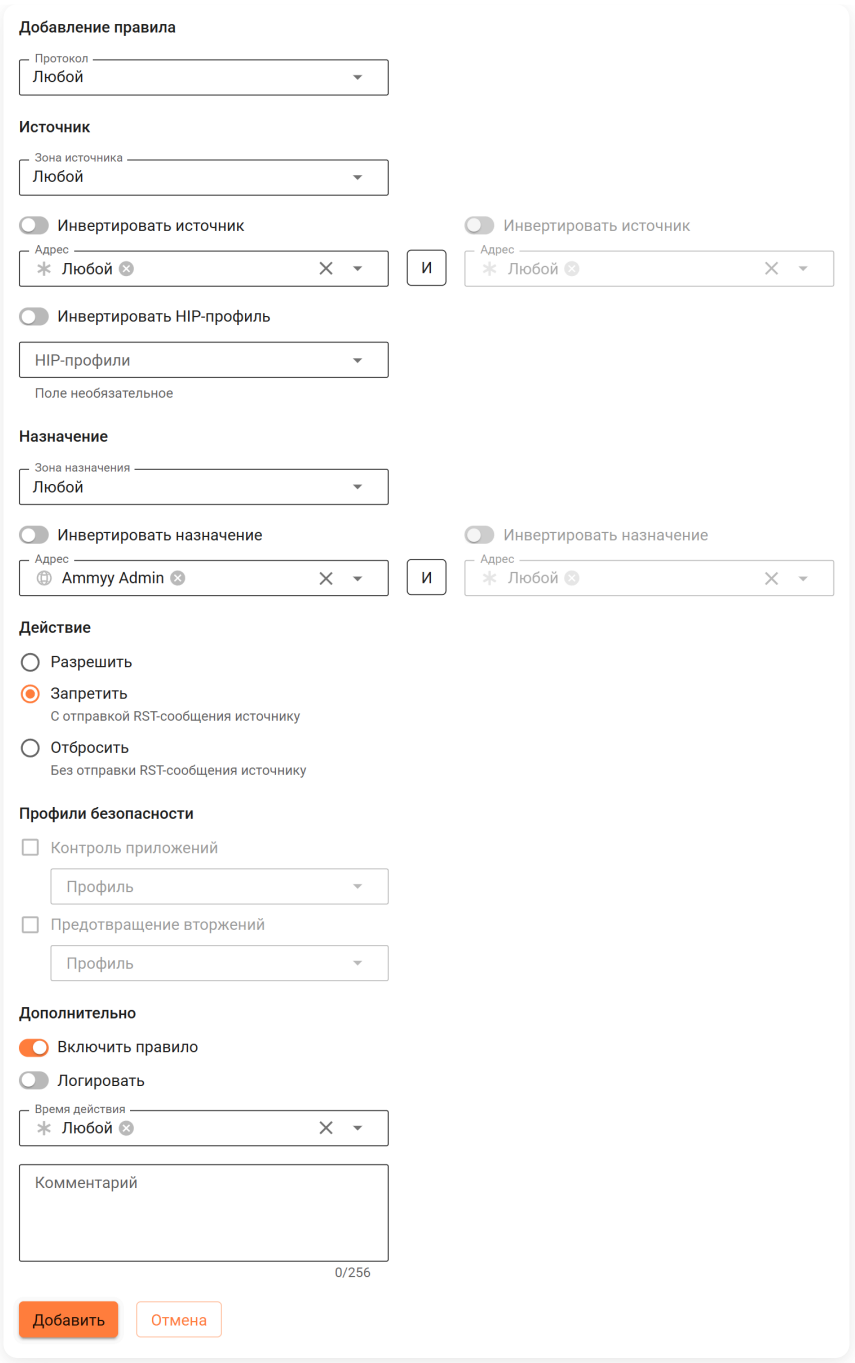
Блокировка Ammyy Admin

Ammyy Admin - это система удаленного доступа и администрирования. Чтобы заблокировать систему, выполните следующие настройки:

1. Откройте раздел **Правила трафика** → **Объекты** и создайте объект типа **Домен** с доменным именем rl.ammyy.com:



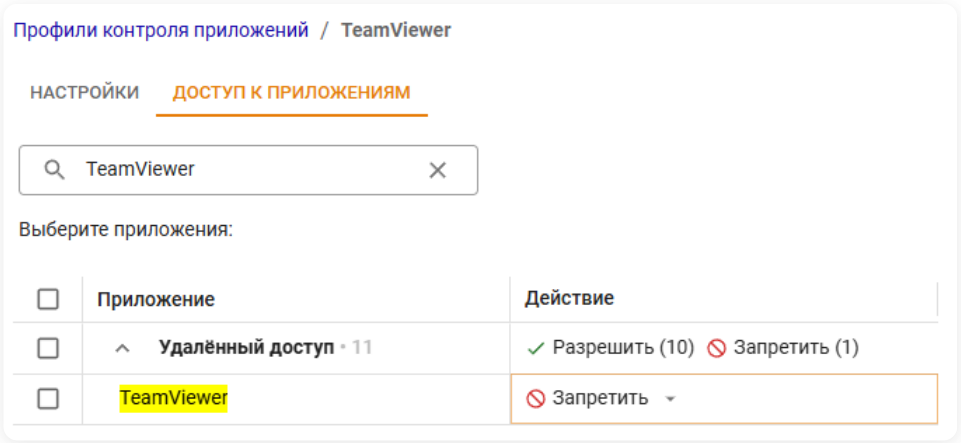
2. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**, создайте и включите правило запрета для нужных пользователей или групп. В поле **Назначение** выберите объект, созданный в пункте 1:



Блокировка TeamViewer

TeamViewer - это программное обеспечение для удаленного доступа и управления компьютерами. TeamViewer можно заблокировать с помощью Контроля приложений.

1. Перейдите в **Профили безопасности** → **Контроль приложений**. Создайте новый профиль для TeamViewer с действием **Запретить**:

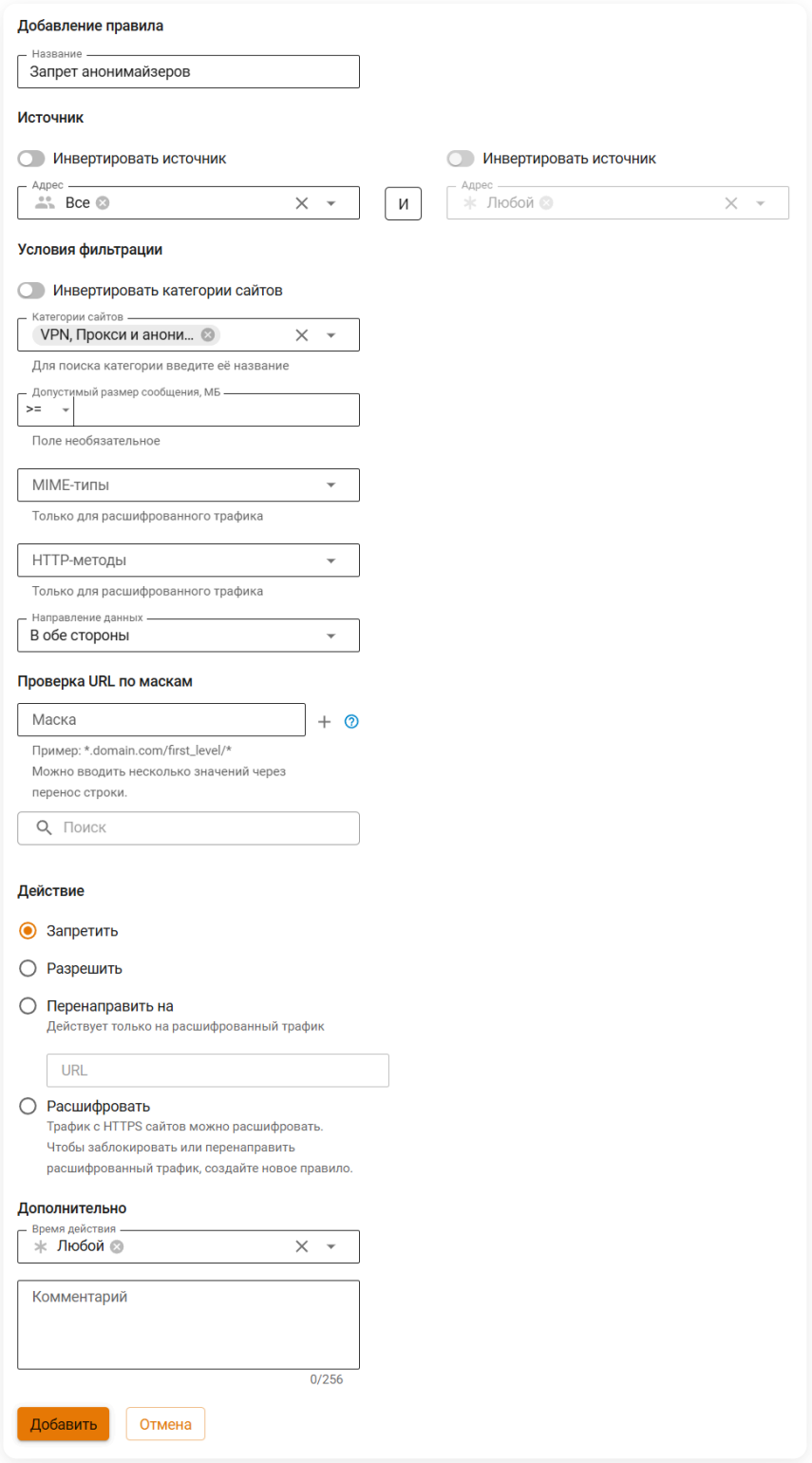


2. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

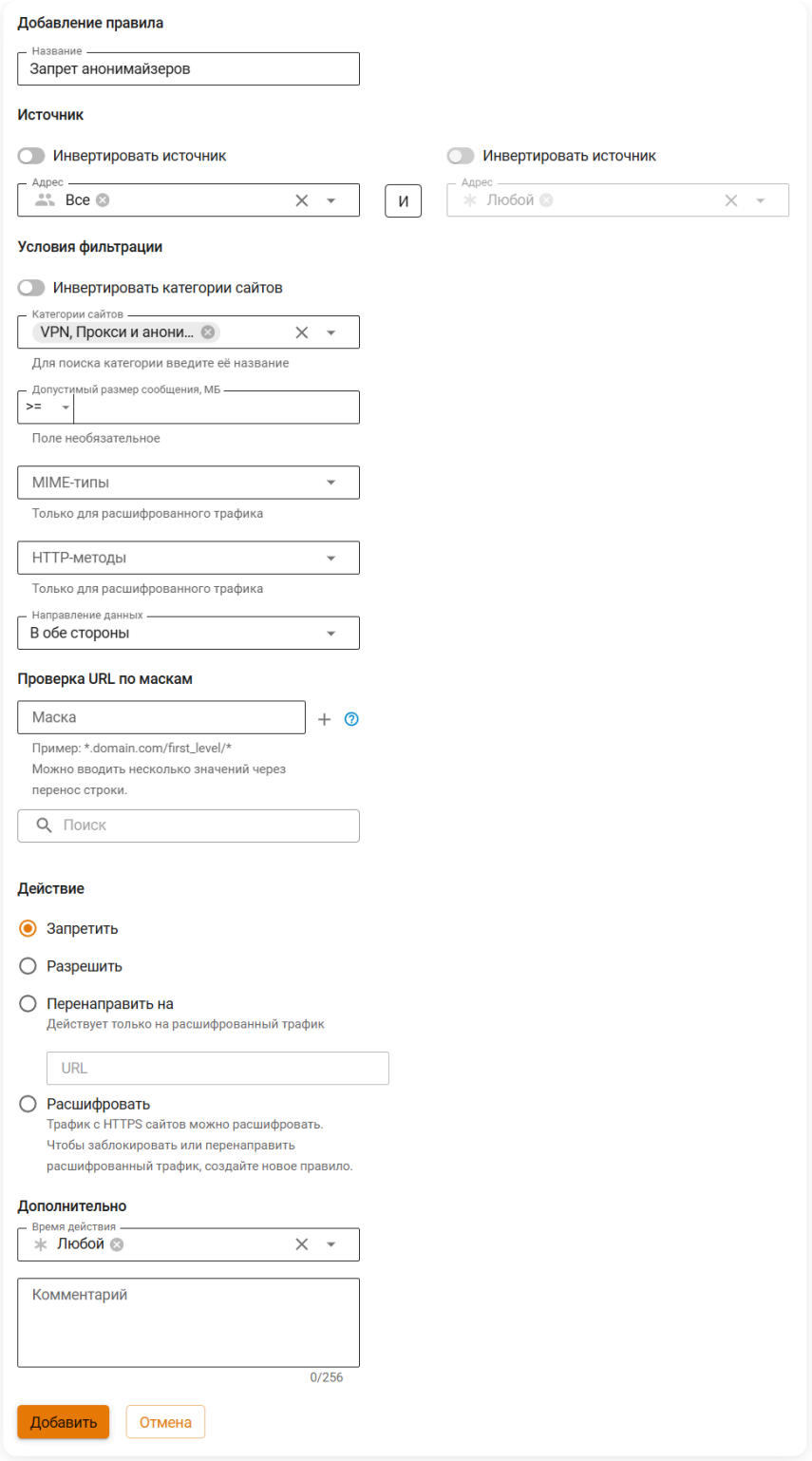
Блокировка анонимайзеров

Заблокировать анонимайзеры можно в разделе **Правила трафика** тремя способами:

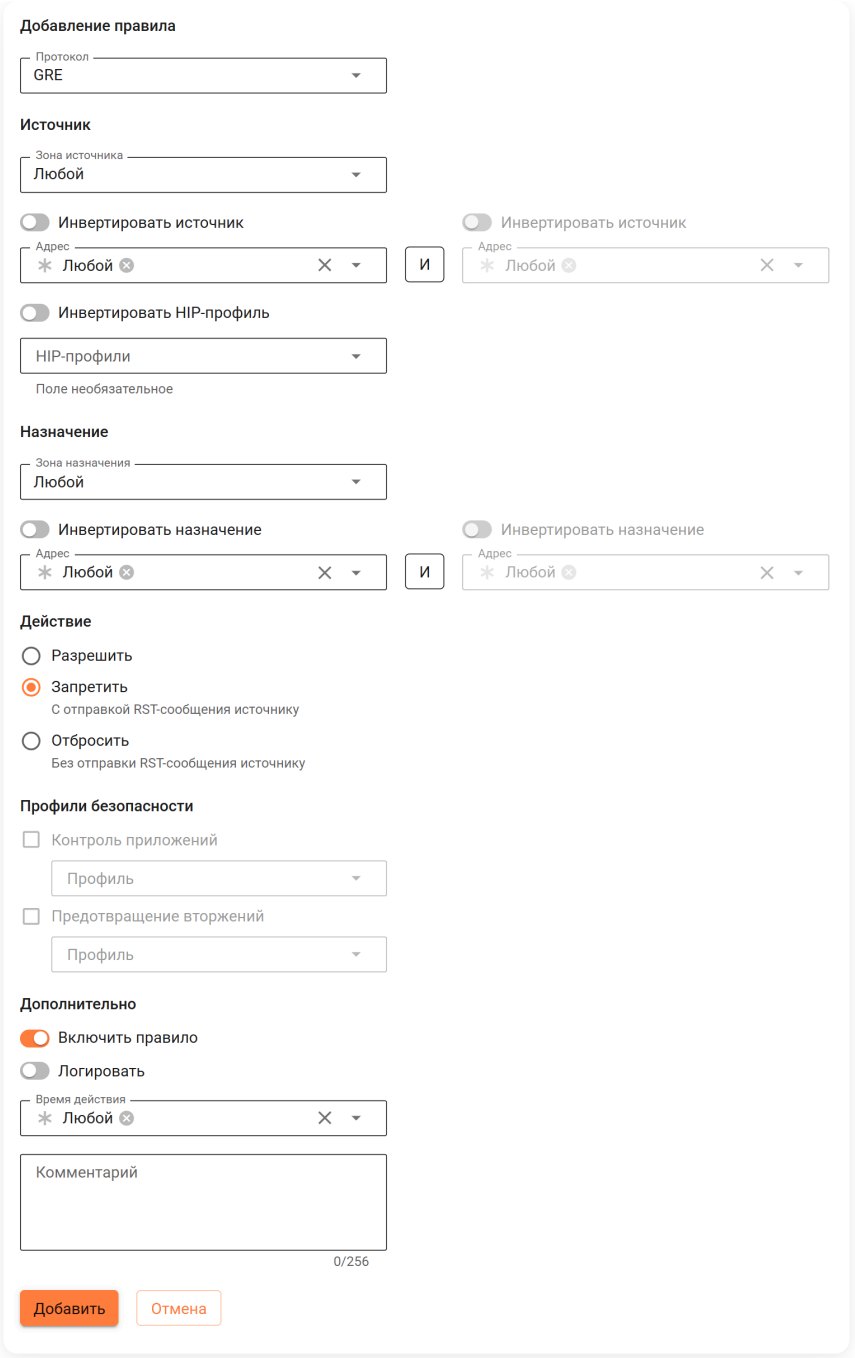
1. Анонимайзеры, работающие по протоколам HTTP(S), блокируются в **Правила трафика** → **Контент-фильтр**. Для этого создайте правило, в котором запретите категорию сайтов **Анонимайзеры**:



2. Чтобы предотвратить обход **Контент-фильтра**, создайте правило, которое будет блокировать прямые обращения по IP-адресам в Контент-фильтре:



3. Для блокировки VPN-анонимайзеров, использующих протокол PPTP, достаточно заблокировать протокол GRE в правилах **Межсетевого экрана**:

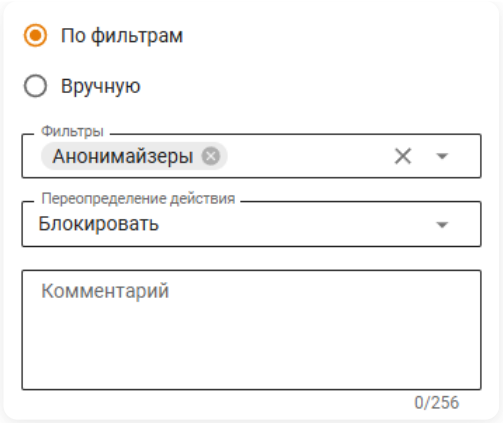


Блокировка Opera.Turbo, Opera VPN, Yandex.Turbo, friGate, Anonymox

Чтобы заблокировать функции браузеров, которые используются для обхода контентной фильтрации, воспользуйтесь модулем Предотвращение вторжений.

1. Перейдите в **Профили безопасности** → **Предотвращение вторжений**. Создайте новый профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило, блокирующее группу сигнатур **Анонимайзеры**:



3. Нажмите **Добавить**.

4. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилем, созданным ранее.

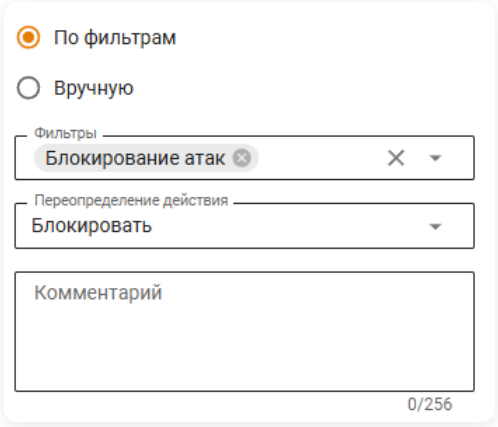
Блокировка Tor

Tor - специально разработанное программное обеспечение и среда прокси-серверов, предназначенная для обхода различного рода блокировок, поэтому полностью заблокировать Tor сейчас невозможно.

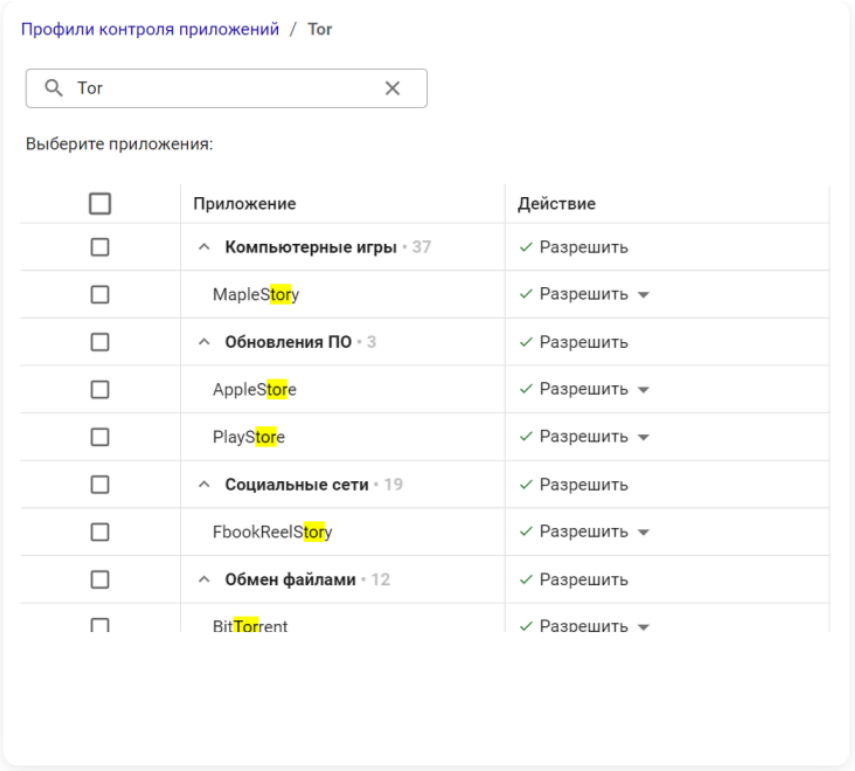
Для противодействия использованию сети Tor, а также для журналирования попыток подключения и использования сети Tor, выполните следующие настройки:

1. В **Профили безопасности** → **Предотвращение вторжений** создайте профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило для группы сигнатур **Блокирование атак**:



3. В **Профили безопасности** → **Контроль приложений** добавьте профиль, запрещающий приложение Tor:



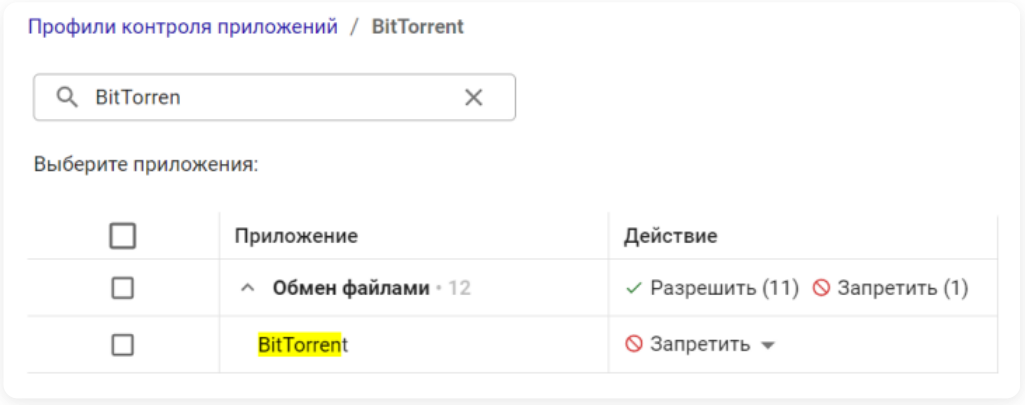
4. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилями **Предотвращения вторжений** и **Контроля приложений**, созданными ранее.

Блокировка торрентов

BitTorrent - P2P-протокол, предназначенный для обмена файлами через интернет.

Для ограничения возможности использования торрентов выполните следующие настройки:

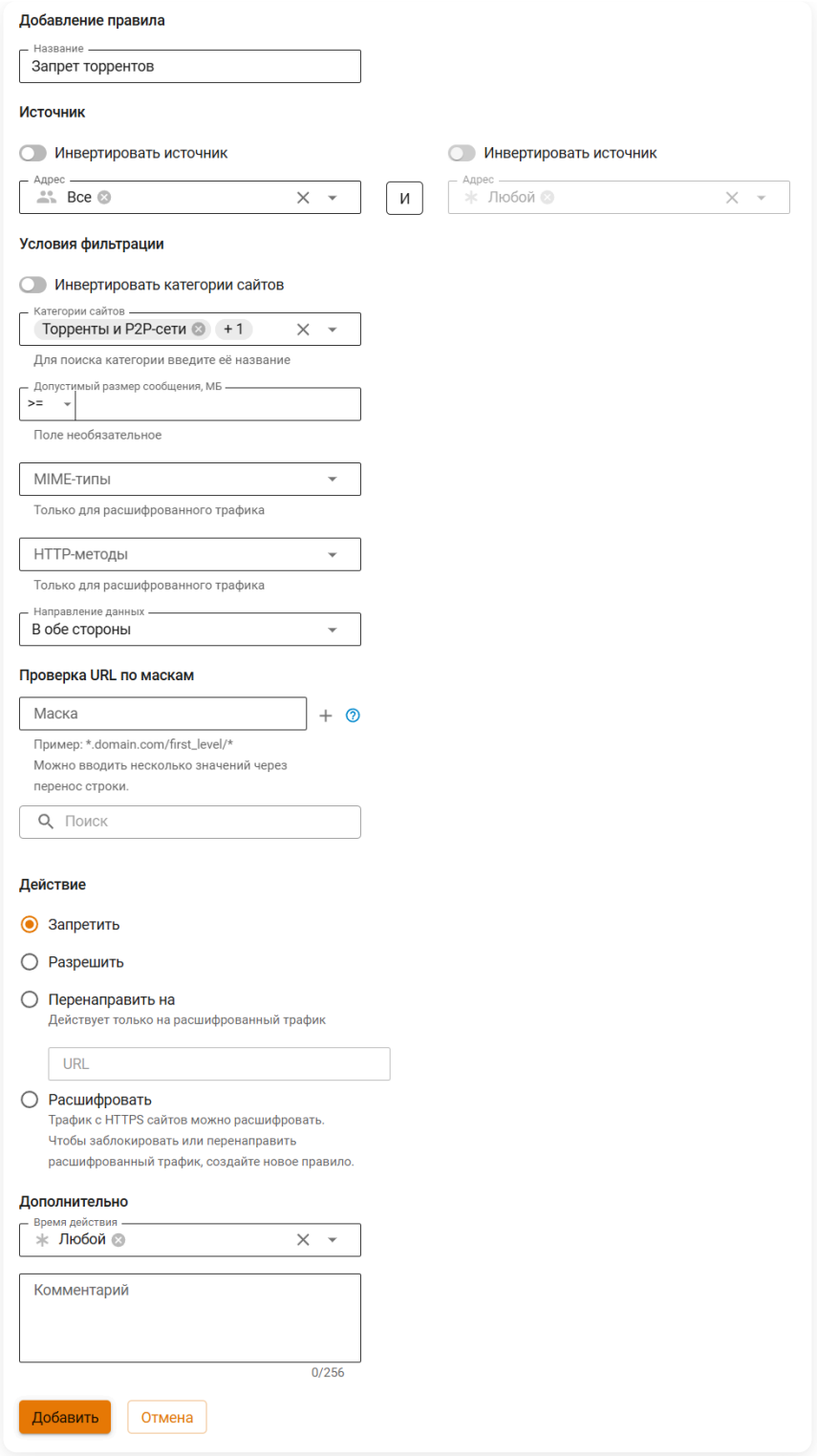
1. Запретите протокол BitTorrent с помощью правила в **Профили безопасности** → **Контроль приложений**:



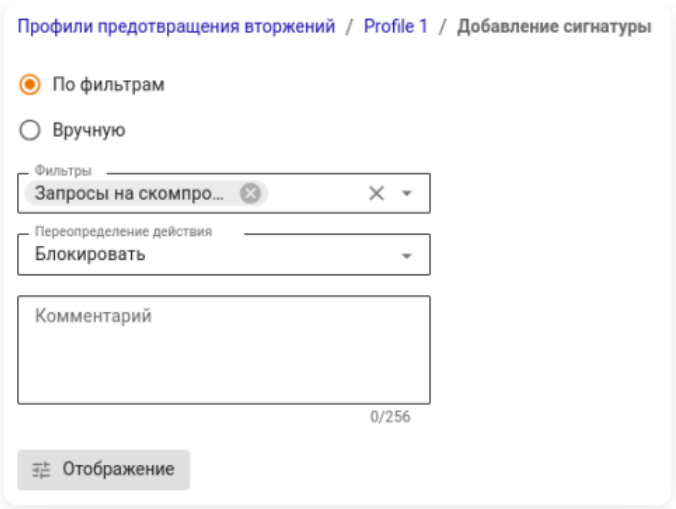
2. В **Правила трафика** → **Межсетевой экран** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

3. Разрешите нужные TCP и UDP порты пользователям. Затем создайте и включите в **Правила трафика** → **Межсетевой экран** → **FORWARD** правило, которое запрещает все протоколы (правила действуют сверху вниз).

4. В **Контент-фильтр** заблокируйте доступ к сайтам-каталогам и торрент-файлам. Для этого запретите категории **Торрент-трекеры** и **Torrent-файлы**:



5. В **Профили безопасности** → **Предотвращение вторжений** создайте профиль, блокирующий группу сигнатур **Запросы на скомпрометированные ресурсы**, которая позволяет блокировать активность P2P-программ:



Блокировка Telegram

Telegram - облачный мессенджер для мобильных устройств и компьютеров (приложение и веб-версия).

Telegram не блокируется **Контролем приложений**, если в приложении настроить опцию **Использовать собственный прокси** в **Настройки** → **Продвинутые настройки** → **Тип соединения**:

При необходимости рекомендуем блокировать доступ к приложению Telegram на рабочих станциях: запрещать установку и запуск приложения политиками безопасности или антивирусом.

Веб-версию Telegram можно заблокировать с помощью **Контент-фильтра**. Для этого выполните следующие действия:

1. Создайте пользовательскую категорию, включающую значение `web.telegram.org`, или отредактируйте уже существующую:

2. Укажите созданную или отредактированную пользовательскую категорию при добавлении правила **Контент-фильтра** с действием **Запретить**:

Полезные ссылки

- **Контент-фильтр**
- **Контроль приложений**
- **Межсетевой экран**
- **Правила**
- **Предотвращение вторжений**
- **Предотвращение вторжений**

Ручная корректировка GeoIP

Чтобы изменить привязку IP-адреса или сети к стране, добавьте необходимую запись в файл `/var/opt/ideco/system-backend/geoip.override`. Можно добавлять IP-адреса и сети в формате CIDR для привязки к указанной стране.

Информация о корректировке GeoIP отображается в журнале Система.

Формат записи файла

```
<network> <country>
```

- `network` - сеть в CIDR-нотации (например, 109.70.184.0/21).

> Индивидуальные IP-адреса должны быть оформлены как сеть с маской подсети `/32`.

- `country` - ISO-код (Alpha-2) страны, в которую будет помещен IP-адрес или сеть.

```
1.2.9.10/32 us
1.2.10.0/24 ru
104.28.130.178/32 ru
```

- `1.2.9.10/32 us` - перемещение IP-адреса `1.2.9.10/32` в список **Соединенные Штаты**, остальные IP-адреса подсети `1.2.9.0/24` останутся в списке **Российская Федерация**.
- `1.2.10.0/24 ru` - подсеть `1.2.10.0/24` добавится к списку **Российская Федерация**.
- `104.28.130.178/32 ru` - IP-адрес `104.28.130.178/32` исключится из списка **Соединенные Штаты** и добавится в список **Российская Федерация**.

Порядок действий

Для изменения привязки IP-адреса или сети к стране:

1. Перейдите в **Управление сервером** → **Терминал**.

2. Отредактируйте файл: `/var/opt/ideco/system-backend/geoip.override`:

```
nano /var/opt/ideco/system-backend/geoip.override
```

Изменение GeoIP базы произойдет в течение минуты.

> Некорректные записи в файле игнорируются и сведения об ошибках фиксируются в журнале Система в формате `Invalid IpList Patch line "<СТРОКА>": <ОШИБКА>`.

Список зон IpList

> **Важно**: ручное добавление IP-адреса в список определенной страны не добавляет IP-адрес автоматически в список группы стран или континента. Для добавления IP-адреса во все необходимые списки пропишите эти группы в файле:
>
> ```
> 123.123.123.123/32 at
> 123.123.123.123/32 eu_group
> 123.123.123.123/32 eu_union_group
> ```
>
> В этом примере IP-адрес будет одновременно добавлен в списки: **Австрия**, **Европа** и **Европейский союз**.

Зона (country)	Местоположение
ad	Андорра
ae	Объединенные Арабские Эмираты
af	Афганистан
af_group	Африка
ag	Антигуа и Барбуда
ai	Ангилья
al	Албания
am	Армения
an_group	Антарктика
ao	Ангола
aq	Антарктида
ar	Аргентина
as	Американское Самоа
as_group	Азия
at	Австрия
au	Австралия
aw	Аруба
ax	Аланды
az	Азербайджан
ba	Босния
bb	Барбадос
bd	Бангладеш
be	Бельгия
bf	Буркина Фасо
bg	Болгария
bh	Бахрейн
bi	Бурунди
bj	Бенин
bl	Сен-Бартельми
bm	Бермудские острова
bn	Бруней Даруссалам
bo	Боливия
bq	Бонайре, Синт-Эстатиус и Саба
br	Бразилия
bs	Багамские острова
bt	Бутан
bv	Остров Буве
bw	Ботсвана
by	Беларусь
bz	Белиз
ca	Канада
cc	Кокосовые острова
cd	Конго, Демократическая Республика
cf	Центрально-Африканская Республика
cg	Республика Конго
ch	Швейцария
ci	Кот-д'Ивуар
ck	Острова Кука

Зона (country)	Местоположение
cl	Чили
cm	Камерун
cn	Китай
co	Колумбия
cr	Коста-Рика
cu	Куба
cv	Кабо-Верде
cw	Кюрасао
cx	Остров Рождества
cy	Кипр
cz	Чешская Республика
de	Германия
dj	Джибути
dk	Дания
dm	Остров Доминика
do	Доминиканская Республика
dz	Алжир
ec	Эквадор
ee	Эстония
eg	Египет
eh	Западная Сахара
er	Эритрея
es	Испания
et	Эфиопия
eu_group	Европа
eu_union_group	Европейский Союз
fi	Финляндия
fj	Фиджи
fk	Фолклендские острова
fm	Федеративные Штаты Микронезии
fo	Фарерские острова
fr	Франция
ga	Габон
gb	Великобритания
gd	Гренада
ge	Грузия
gf	Французская Гвиана
gg	Гернси
gh	Гана
gi	Гибралтар
gl	Гренландия
gm	Гамбия
gn	Гвинея
gp	Гваделупа
gq	Экваториальная Гвинея
gr	Греция
gs	Южная Георгия и Южные Сандвичевы острова
gt	Гватемала

Зона (country)	Местоположение
gu	Гуам
gw	Гвинея-Биссау
gy	Гайана
hk	Гонконг
hm	Острова Херд и Макдональд
hn	Гондурас
hr	Хорватия
ht	Гаити
hu	Венгрия
id	Индонезия
ie	Ирландия
il	Израиль
im	Остров Мэн
in	Индия
io	Британская территория в Индийском океане
iq	Ирак
ir	Иран
is	Исландия
it	Италия
je	Джерси
jm	Ямайка
jo	Иордания
jp	Япония
ke	Кения
kg	Кыргызстан
kh	Камбоджа
ki	Кирибати
km	Коморские острова
kn	Сент-Киттс и Невис
kp	КНДР
kr	Южная Корея
kw	Кувейт
ky	Каймановы Острова
kz	Казахстан
la	Лаос
lb	Ливан
lc	Сент-Люсия
li	Лихтенштейн
lk	Шри-Ланка
lr	Либерия
ls	Лесото
lt	Литва
lu	Люксембург
lv	Латвия
ly	Ливия
ma	Марокко
mc	Монако
md	Молдова

Зона (country)	Местоположение
me	Черногория
mf	Сен-Мартен
mg	Мадагаскар
mh	Маршалловы Острова
mk	Македония
ml	Мали
mm	Мьянма (Бирма)
mn	Монголия
mo	Макао
mp	Северные Марианские острова
mq	Мартиника
mr	Мавритания
ms	Монтсеррат
mt	Мальта
mu	Маврикий
mv	Мальдивы
mw	Малави
mx	Мексика
my	Малайзия
mz	Мозамбик
na	Намибия
na_group	Северная Америка
nc	Новая Каледония
ne	Нигер
nf	Остров Норфолк
ng	Нигерия
ni	Никарагуа
nl	Нидерланды
no	Норвегия
np	Непал
nr	Науру
nu	Ниуэ
nz	Новая Зеландия
oc_group	Океания
om	Оман
pa	Панама
pe	Перу
pf	Французская Полинезия
pg	Папуа - Новая Гвинея
ph	Филиппины
pk	Пакистан
pl	Польша
pm	Сен-Пьер и Микелон
pn	Острова Питкэрн
pr	Пуэрто-Рико
ps	Палестина
pt	Португалия
pw	Палау

Зона (country)	Местоположение
py	Парагвай
qa	Катар
re	Реюньон
ro	Румыния
rs	Сербия
ru	Российская Федерация
rw	Руанда
sa	Саудовская Аравия
sa_group	Южная Америка
sb	Соломоновы Острова
sc	Сейшельские острова
sd	Судан
se	Швеция
sg	Сингапур
sh	Остров Св. Елены
si	Словения
sj	Шпицберген и Ян-Майен
sk	Словакия
sl	Сьерра-Леоне
sm	Сан-Марино
sn	Сенегал
so	Сомали
sr	Суринам
ss	Южный Судан
st	Сан-Томе и Принсипи
sv	Сальвадор
sx	Синт-Мартен
sy	Сирийская Арабская Республика
sz	Эсватини
tc	Острова Теркс и Кайкос
td	Чад
tf	Французские Южные территории
tg	Того
th	Таиланд
tj	Таджикистан
tk	Токелау
tl	Тимор-Лесте
tm	Туркменистан
tn	Тунис
to	Тонга
tr	Турция
tt	Тринидад и Тобаго
tv	Тувалу
tw	Тайвань
tz	Танзания
ua	Украина
ug	Уганда
um	Внешние малые острова (США)

Зона (country)	Местоположение
us	Соединенные Штаты
uy	Уругвай
uz	Узбекистан
va	Государство-город Ватикан
vc	Сент-Винсент и Гренадины
ve	Венесуэла
vg	Виргинские острова (Великобритания)
vi	Виргинские острова (США)
vn	Вьетнам
vu	Вануату
wf	Острова Уоллис и Футуна
ws	Самоа
xk	Косово
ye	Йемен
yt	Майотта
za	ЮАР
zm	Замбия
zw	Зимбабве

Полезные ссылки

- **Объекты**
- **Система**

SD-WAN

Практические руководства по настройке SD-WAN в Ideco NGFW Novum

Резервирование трех WAN-каналов через SD-WAN

Перейти ›

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Резервирование трех WAN-каналов через SD-WAN

Классический контекст | Высокопроизводительный контекст

Руководство описывает настройку каскадного резервирования WAN на удаленной площадке с тремя каналами доступа в интернет:

- **Интерфейс 1** - проводной провайдер, шлюз 192.0.2.1 (основной канал).
- **Интерфейс 2** - LTE-модем в Ethernet-режиме, шлюз 10.0.0.1 (первый резервный канал).
- **Интерфейс 3** - спутниковый терминал, шлюз 10.0.1.1 (второй резервный канал).
- **Локальная сеть** - 172.16.0.0/24.

После настройки при обрыве проводного канала трафик автоматически перейдет на LTE, при обрыве LTE - на спутник. После восстановления канала с более высоким приоритетом трафик вернется на него автоматически.

Что нужно учесть перед настройкой

Каналы имеют принципиально разные характеристики:

Тип канала	Ориентировочная задержка	Джиттер	Особенности
Проводной провайдер	5-30 мс	низкий	Стабильный, предсказуемый
LTE-модем	30-80 мс	средний	Зависит от загруженности сети и уровня сигнала
Спутниковый терминал (GEO)	500-700 мс	высокий	Большая задержка из-за расстояния до спутника. Непригоден для VoIP и видеозвонков. Трафик значительно дороже проводного и LTE

Значения задержки и джиттера ориентировочные. Реальные показатели зависят от оборудования и условий работы канала.

Настройка

Шаг 1. Настройте интерфейсы

Убедитесь, что все три внешних интерфейса настроены и получают адреса от своих провайдеров. Подробнее о настройке интерфейсов в статье.

Шаг 2. Создайте Next hop для каждого канала

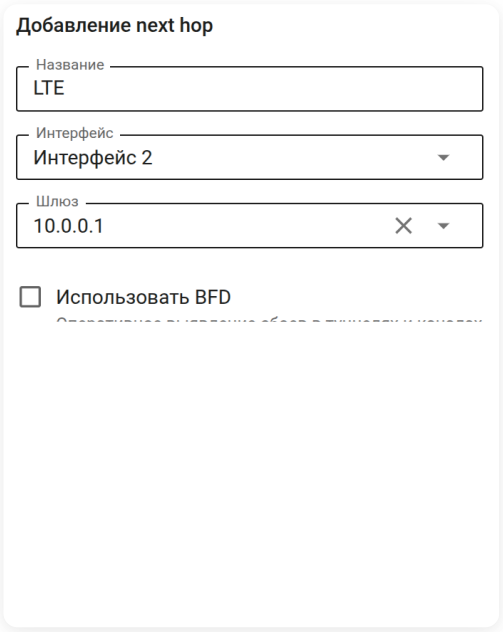
1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля:

Проводной провайдер

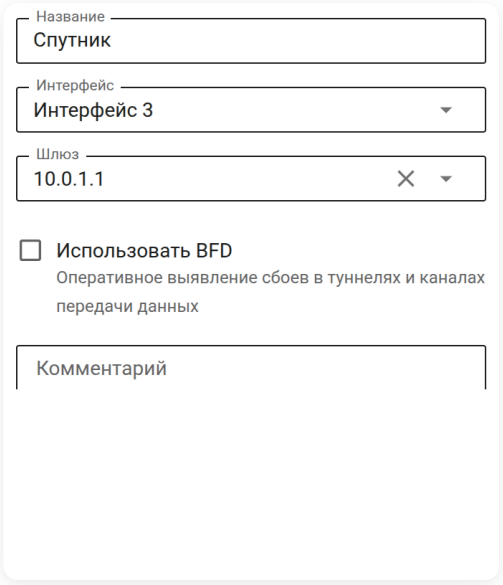
- **Название** - укажите `Проводной`.
- **Интерфейс** - выберите `Интерфейс 1`.
- **Шлюз** - укажите `192.0.2.1`.
- **Использовать BFD** - оставьте опцию выключенной.

LTE



- **Название** - укажите `LTE`.
- **Интерфейс** - выберите `Интерфейс 2`.
- **Шлюз** - укажите `10.0.0.1`.
- **Использовать BFD** - оставьте опцию выключенной.

Спутник



- **Название** - укажите `Спутник`.
- **Интерфейс** - выберите `Интерфейс 3`.
- **Шлюз** - укажите `10.0.1.1`.
- **Использовать BFD** - оставьте опцию выключенной.

---

3. Нажмите **Добавить**.

BFD требует поддержки на стороне шлюза провайдера. Операторы LTE и спутниковые операторы, как правило, BFD не поддерживают, поэтому для проверки доступности каналов используйте профили IP SLA на следующем шаге.

Шаг 3. Создайте профиль IP SLA

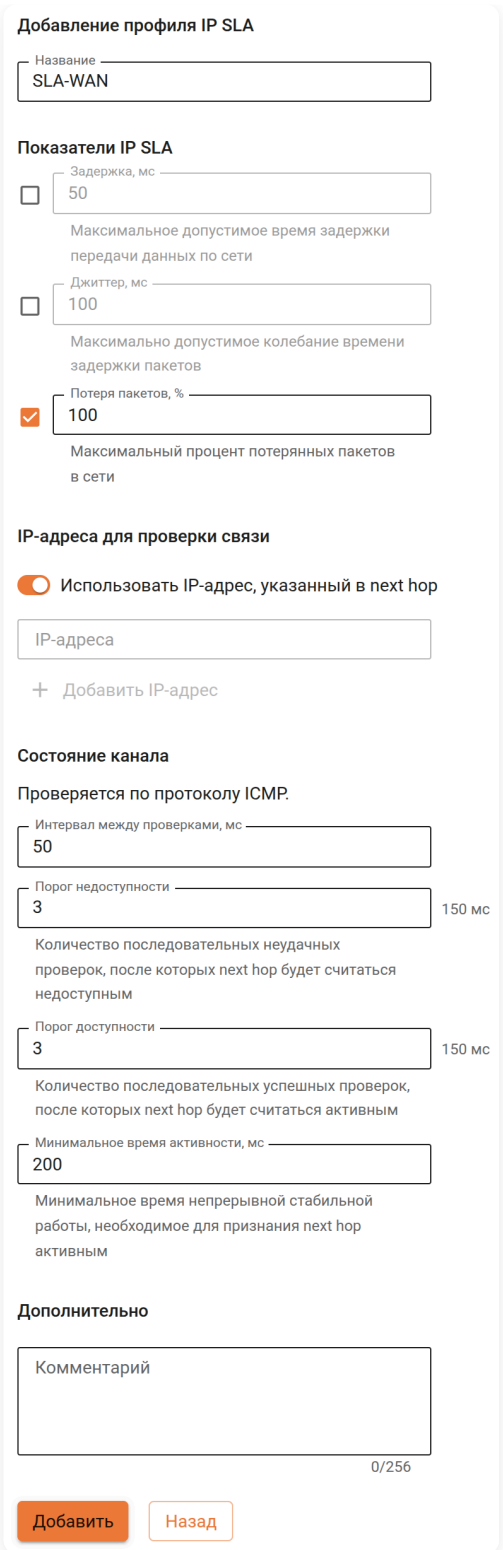
Профиль IP SLA применяется ко всем узлам в **Профиле next hop**.

Поскольку каналы различаются по задержке, в особенности спутниковый (с базовой задержкой ~500-700 мс), использовать пороги задержки и джиттера в общем профиле нецелесообразно: канал с высокой задержкой будет постоянно считаться недоступным. Для резервирования достаточно проверять только доступность шлюза по ICMP.

Выполните действия:

1. Перейдите в **SD-WAN** → **Профили IP SLA** и нажмите **Добавить**.

2. Заполните поля:



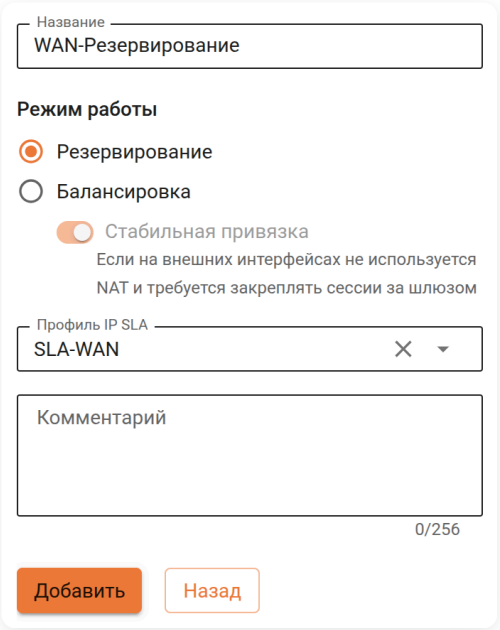
- **Название** - укажите `SLA-WAN`.
- **Показатели SLA**:
  - **Задержка, мс** - оставьте опцию выключенной. Базовая задержка спутникового канала (~500-700 мс) превысит любой разумный порог.
  - **Джиттер, мс** - оставьте опцию выключенной по той же причине.
  - **Потеря пакетов, %** - включите опцию и укажите `100`.
- **Использовать IP-адрес, указанный в next hop** - включите опцию. Система будет проверять шлюз каждого next hop по его собственному IP-адресу.
- **Интервал между проверками, мс** - задайте частоту проверок, например, `50`.
- **Порог недоступности** - задайте количество последовательных неудачных проверок для признания канала недоступным, например, `3`.
- **Порог доступности** - задайте количество последовательных успешных проверок для признания канала восстановленным, например, `3`.
- **Минимальное время активности, мс** - задайте минимальное время стабильной работы перед тем, как канал будет признан активным, например, `200`.

3. Нажмите **Добавить**.

Шаг 4. Создайте профиль next hop в режиме Резервирование

1. Перейдите в **SD-WAN** → **Профили next hop** и нажмите **Добавить**.

2. На вкладке **Настройки** заполните поля:

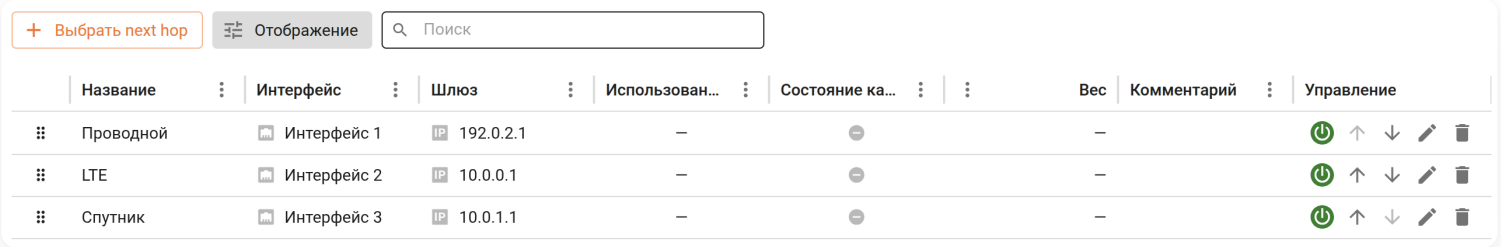


- **Название** - укажите `WAN-Резервирование`.
- **Режим работы** - выберите **Резервирование**.
- **Профиль IP SLA** - выберите `SLA-WAN`.

3. Нажмите **Добавить** и перейдите на вкладку **Next hop**.

4. Нажмите **Выбрать next hop**, отметьте `Проводной`, `LTE` и `Спутник`, нажмите **Выбрать**.

5. Расставьте приоритет с помощью ↑ ↓ - порядок должен быть сверху вниз:

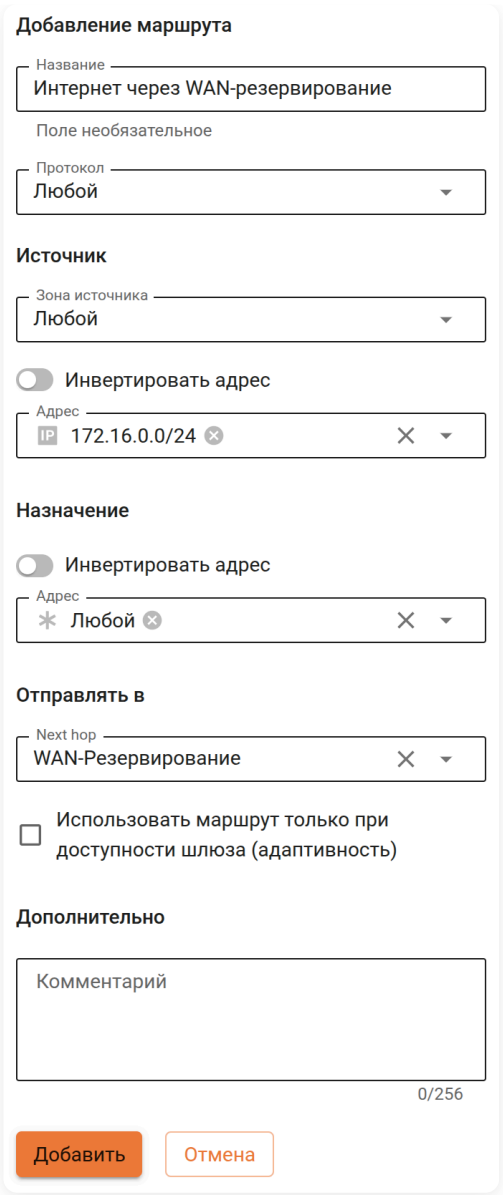


6. Вернитесь на вкладку **Настройки** и нажмите **Сохранить**.

Шаг 5. Примените профиль в правиле маршрутизации

1. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**.

2. Заполните поля:



- **Название** - укажите `Интернет через WAN-резервирование`.
- **Источник**:
  - **Адрес** - выберите подсеть `172.16.0.0/24`.
- **Отправлять в** - выберите профиль `WAN-Резервирование`.

3. Нажмите **Добавить**.

Проверка каскадного переключения

1. Убедитесь, что трафик идет через проводной канал: проверьте доступность интернета с устройства в сети `172.16.0.0/24`.

2. Отключите проводной канал (физически или на стороне провайдера). Дождитесь срабатывания порога недоступности в профиле `SLA-WAN`.

3. Убедитесь, что трафик переключился на LTE: проверьте доступность интернета. События переключения отображаются в **Отчеты и журналы** → **Система**.

4. Не восстанавливая проводной канал, отключите LTE. Дождитесь срабатывания порога недоступности в профиле `SLA-WAN`.

5. Убедитесь, что трафик переключился на спутник.

6. Восстановите LTE. После достижения порога доступности и минимального времени активности в профиле `SLA-WAN` трафик должен вернуться на LTE.

7. Восстановите проводной канал. После достижения порога доступности в профиле `SLA-WAN` трафик должен вернуться на проводной канал.

Если переключение не произошло, проверьте события в **Отчеты и журналы** → **Система** и убедитесь, что пороги IP SLA выставлены корректно для вашего оборудования.

Если все три канала признаны недоступными, маршрут до внешних сетей исчезнет и трафик будет отброшен. При восстановлении любого из каналов трафик автоматически направится через него после достижения порога доступности и минимального времени активности в профиле `SLA-WAN`.

Полезные ссылки

- **Next hop**
- **Профили next hop**
- **Профили IP SLA**
- **Маршрутизация внешних сетей**
- **Интерфейсы**

Маршрутизация

Практические руководства по настройке маршрутизации в Ideco NGFW

Как избавиться от асимметричной маршрутизации трафика

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Как избавиться от асимметричной маршрутизации трафика

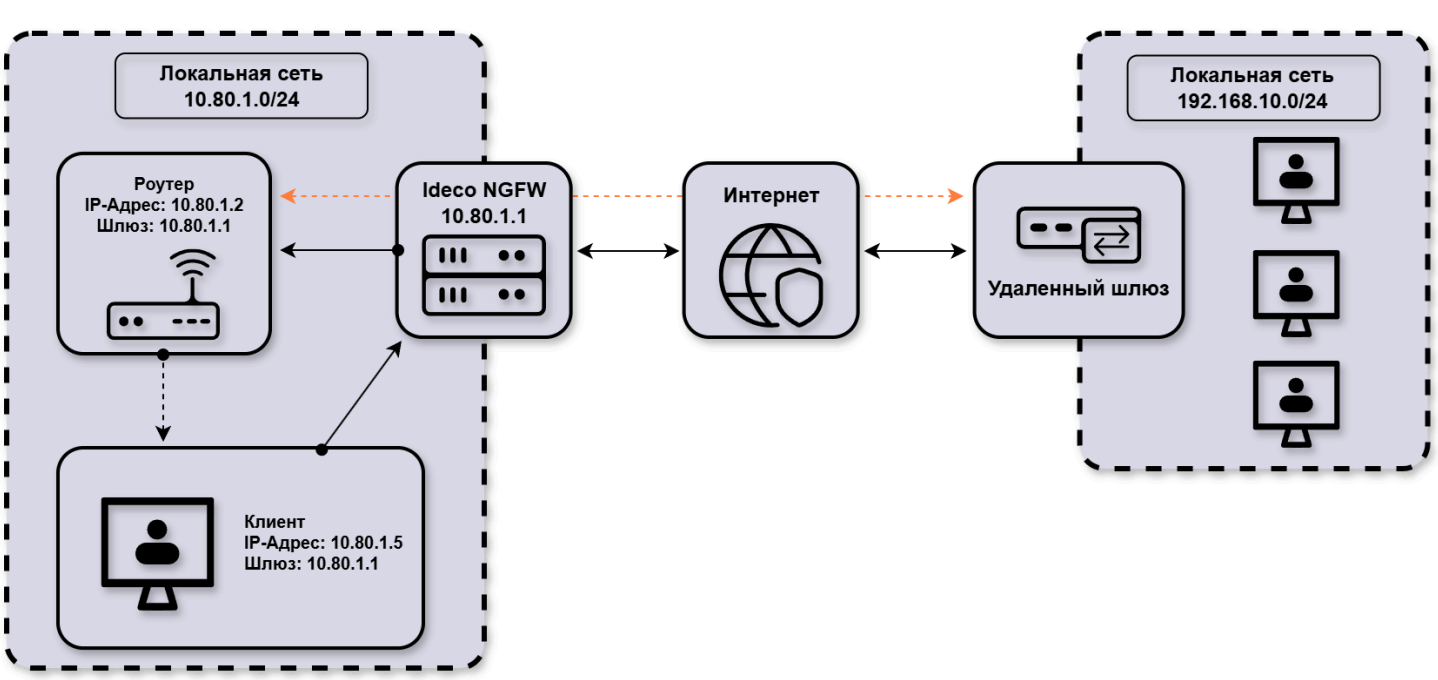
Классический контекст | Высокопроизводительный контекст

При настройке доступа в удаленные сети через маршрутизатор в локальной сети может возникнуть асимметричная маршрутизация, препятствующая прохождению пакетов между двумя локальными сетями. В этой статье описаны случаи возникновения асимметричной маршрутизации и способы предотвращения.

Пример. В локальной сети NGFW Novum используется маршрутизатор, устанавливающий связь с другими сетями. NGFW Novum - шлюз по умолчанию для клиентов сети. Требуется настроить маршрутизацию на NGFW Novum так, чтобы клиенты сети `10.80.1.0/24` получали доступ к удаленной сети `192.168.10.0/24` и обратно через маршрутизатор.

Асимметричная маршрутизация при наличии маршрутизатора в локальной сети

Неправильная топология сети, способствующая асимметричной маршрутизации:

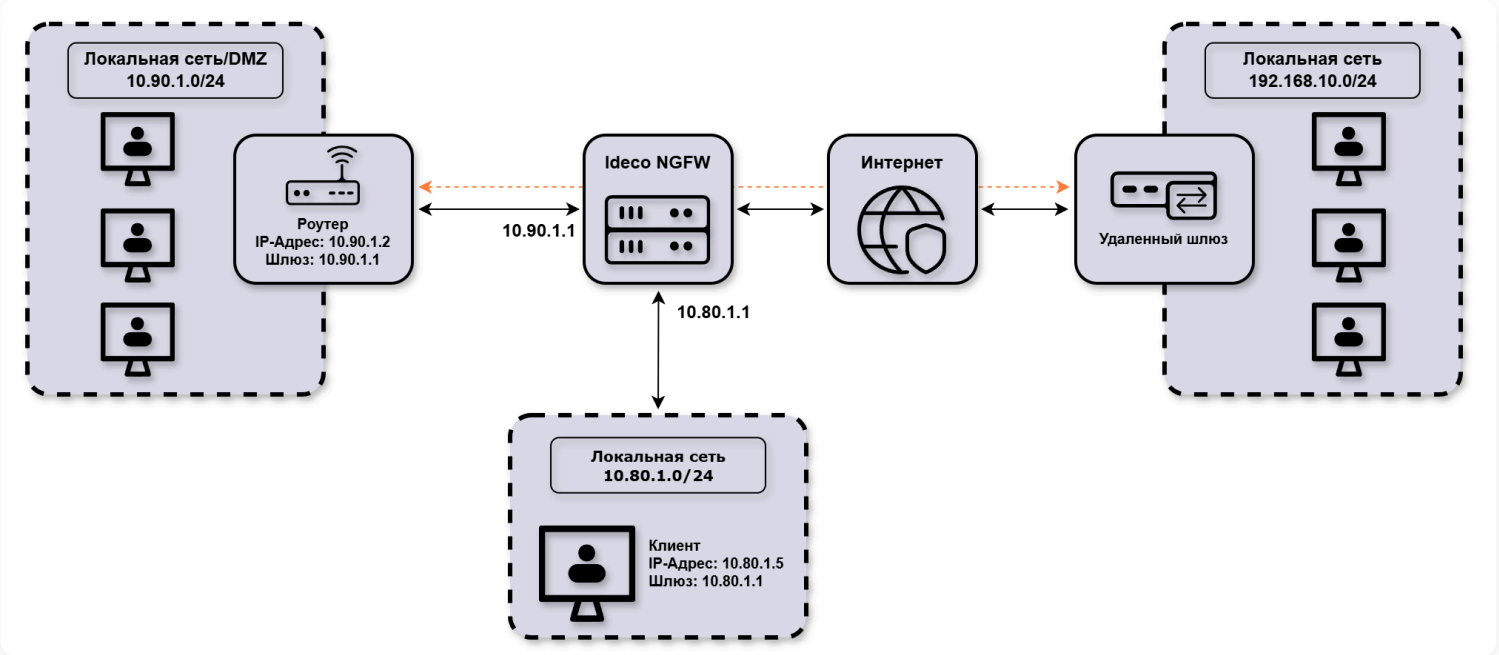


- `10.80.1.1` - шлюз для локальной сети `10.80.1.0/24`.
- `10.80.1.2` - маршрутизатор, имеющий доступ к удаленной сети `192.168.10.0/24`.
- `10.80.1.5` - адрес хоста в локальной сети.
- **Оранжевая стрелка** - двусторонняя связь маршрутизатора с удаленным шлюзом или маршрутизатором, обеспечивающая доступ к удаленной сети `192.168.10.0/24` (туннель к шлюзу, маршрут до маршрутизатора в соседнюю сеть предприятия).
- **Черные стрелки** - трафик от хостов локальной сети `10.80.1.0/24` до удаленной сети `192.168.10.0/24` через шлюз NGFW Novum (`10.80.1.1`) и маршрутизатор (`10.80.1.2`).
- **Пунктирная стрелка** - трафик, который маршрутизатор возвращает хостам локальной сети в обход NGFW Novum, поэтому хосты этот трафик обратно не принимают.

Часть трафика от клиентов до маршрутизатора идет через шлюз, а часть - непосредственно от маршрутизатора до абонентов сети. Разная маршрутизация на разных участках делает прохождение пакетов между двумя локальными сетями невозможным.

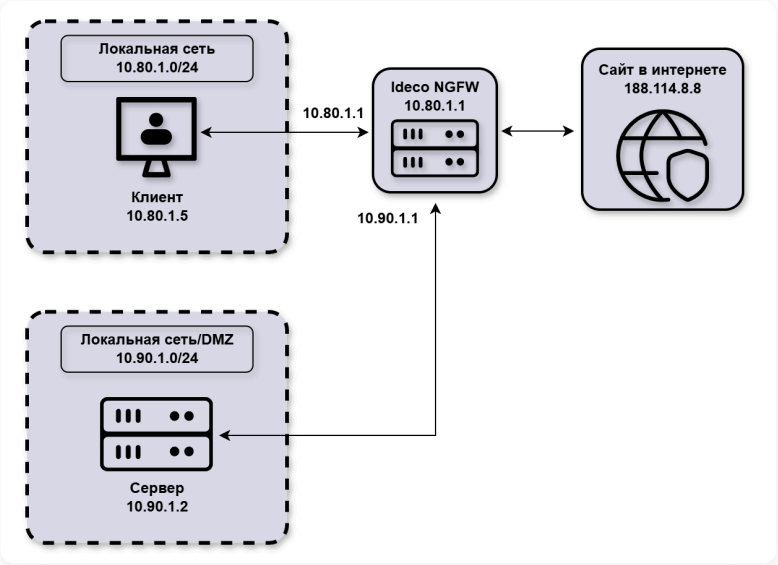
Решение: Изоляция маршрутизатора в отдельную сеть (DMZ)

Правильная топология сети:



Для правильной работы схемы потребуется:

1. Вынести маршрутизатор в отдельную локальную сеть (DMZ `10.90.1.0/24`), чтобы избежать асимметричной маршрутизации между маршрутизатором и клиентами локальной сети:



2. Настроить DMZ на NGFW Novum, добавив на локальный интерфейс NGFW Novum еще один IP-адрес (`10.90.1.0/24`), к локальной сети которого подключен маршрутизатор.

3. Настроить IP-адрес на маршрутизаторе из адресного пространства новой сети `10.90.1.2`. Шлюзом указать дополнительный IP-адрес, настроенный на локальном интерфейсе NGFW Novum из этой сети `10.90.1.1`.

Физически маршрутизатор и клиенты локальной сети будут находиться в одном сегменте сети, имея при этом разную IP-адресацию и шлюзы. Как правило, схемы с виртуальной изоляцией сетей на основе одного физического интерфейса достаточно.

Для физической изоляции локальной сети клиентов NGFW Novum и маршрутизатора:

- Подключите к NGFW Novum дополнительную сетевую карту.
- Настройте на подключенной сетевой карте дополнительный локальный интерфейс и отдельную IP-адресацию в этой сети.
- Укажите в качестве шлюза для маршрутизатора адрес, настроенный на дополнительном локальном интерфейсе.

Физически маршрутизатор будет находиться в сегменте дополнительной сетевой карты.

Шаг 1. Настройка сетевого интерфейса

Для настройки нескольких IP-подсетей на одном локальном интерфейсе NGFW Novum перейдите в **Сервисы** → **Сетевые интерфейсы** и выполните действия:

1. Откройте Ethernet-интерфейс с ролью **LAN** для локальной сети `10.80.1.1/24`, нажав на .

2. В поле **Режим** выберите **Статический** и введите IP-адрес вручную.

3. Нажмите **Добавить IP-адрес с маской** и введите IP-адрес `10.90.1.1/24` для изоляции маршрутизатора:

4. Нажмите **Сохранить**.

Шаг 2. Настройка маршрутизации

После изоляции маршрутизатора в DMZ нужно указать маршрут на NGFW Novum до удаленной сети. Для этого выполните действия:

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс для локальной сети.
- **Шлюз** - введите адрес маршрутизатора в DMZ `10.90.1.2`.

3. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:

- **Название** - укажите название.
- **Источник** - введите адрес локальной сети `10.80.1.0/24`.
- **Назначение** - введите адрес внешней сети `192.168.10.0/24`.
- **Отправлять в** - выберите созданный на шаге 2 **Next hop**.

В результате трафик между сетями `10.80.1.0/24` и `192.168.10.0/24` во всех направлениях будет направляться через NGFW Novum и маршрутизатор.

Шаг 3. Настройка клиентских машин

Хосты сетей, которые теперь обслуживает NGFW Novum (`10.80.1.0/24` и `10.90.1.0/24`), физически включены в один Ethernet-сегмент. Чтобы шлюзом и DNS-сервером для хостов этих сетей был соответствующий адрес на локальном интерфейсе NGFW Novum, укажите:

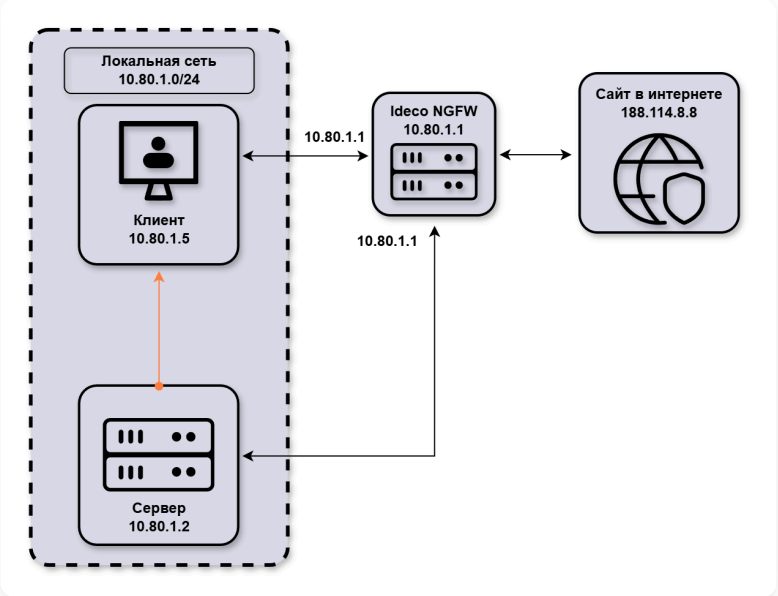
1. Для хостов из подсети `10.80.1.0/24` значение шлюза и DNS-сервера - `10.80.1.1`.

2. Для хостов из подсети `10.90.1.0/24` значение шлюза и DNS-сервера - `10.90.1.1`.

Если по какой-то причине изолировать сервер в DMZ невозможно, создайте на NGFW Novum специальное **SNAT**-правило.

Асимметричная маршрутизация при публикации ресурсов через DNAT

Асимметричная маршрутизация также возникает, когда в одной локальной сети находятся хост и сервер, на котором расположен опубликованный при помощи **DNAT**-правила ресурс:

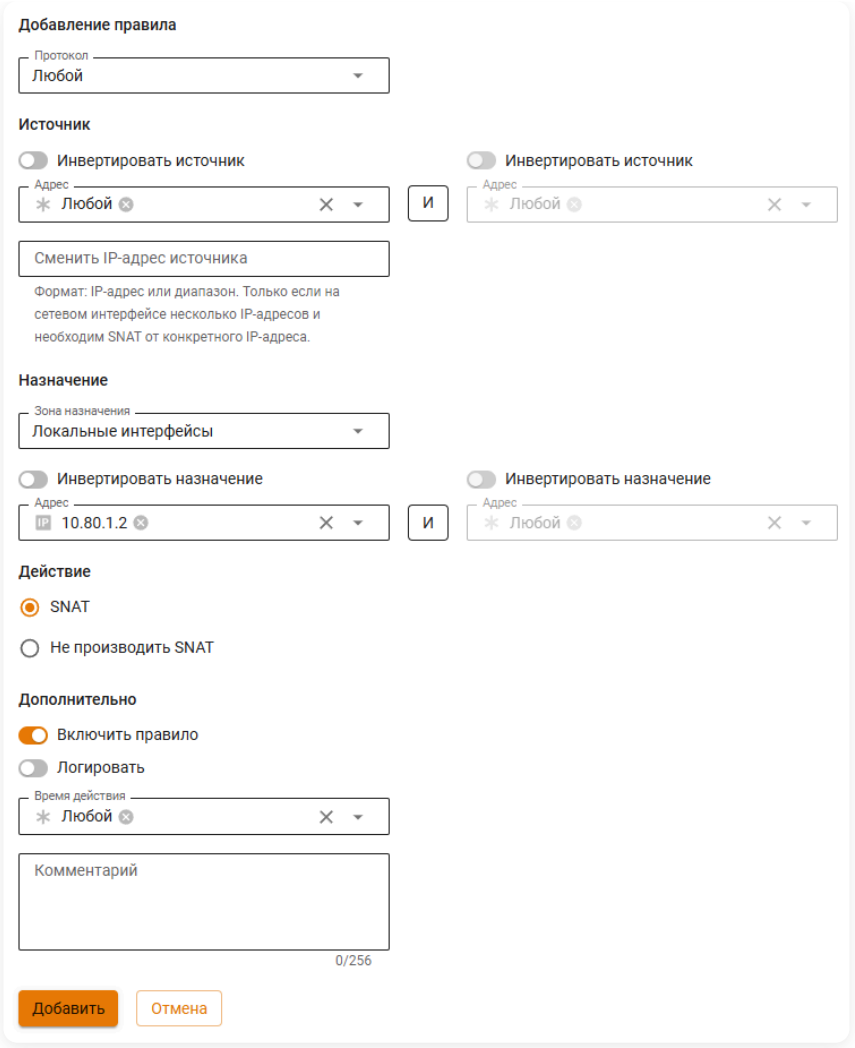


- `10.80.1.1` - адрес Ideco NGFW Novum в локальной сети.
- `10.80.1.2` - адрес сервера в локальной сети.
- `10.80.1.5` - адрес хоста в локальной сети.
- `188.114.8.8` - адрес ресурса в интернете.
- **Оранжевая стрелка** - ответ напрямую от сервера хосту в локальной сети.

Когда хост `10.80.1.5` обращается к ресурс по внешнему адресу `188.114.8.8` (например, в случае обращения по доменному имени, которое разрешено во внешнем IP), трафик проходит через NGFW Novum. На NGFW Novum срабатывает правило **DNAT** и перенаправляет трафик на сервер `10.80.1.2`, а сервер отвечает хосту, минуя NGFW Novum.

Решение: Принудительное направление ответного трафика через NGFW Novum с помощью SNAT-правила

Чтобы сервер `10.80.1.2` не отвечал напрямую на `10.80.1.5`, а отправлял ответ на NGFW Novum `10.80.1.1`, нужно в **Правила трафика** → **Межсетевой экран** → **SNAT** создать и включить правило:



- **Назначение:**
  - **Зона назначения** - укажите **Локальные интерфейсы**.
  - **Адрес** - укажите IP-адрес `10.80.1.2`.

Трафик хоста `10.80.1.5` на внешний адрес ресурса `188.114.8.8` будет перенаправлен на адрес сервера `10.80.1.2` правилом **DNAT**. При этом созданное правило **SNAT** заменит адрес источника `10.80.1.5` на адрес NGFW Novum - пакет приобретет вид: `src 10.80.1.1 dst 10.80.1.2`. Ответ от сервера также пройдет через NGFW Novum - пакет `src 10.80.1.2 dst 10.80.1.1`.

Полезные ссылки

- **Маршрутизация**
- **Статическая маршрутизация**

Управление сервером

Практические руководства по управлению сервером Ideco NGFW

Тестирование оперативной памяти сервера

Перейти >

Как настроить автоматическое включение после сбоя питания

Перейти >

Сброс пароля IPMI на сервере NGFW Novum

Перейти >

Поддержка устаревших алгоритмов шифрования

Перейти >

Восстановление конфигурации из бэкапа

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Как подключить Ideco NGFW Novum к Zabbix Server по SNMP

Классический контекст | Высокопроизводительный контекст

Протокол SNMP используется для сбора данных с сетевых устройств. Подключение Ideco NGFW Novum к Zabbix по SNMP позволяет централизованно мониторить его состояние и получать оповещения о проблемах.

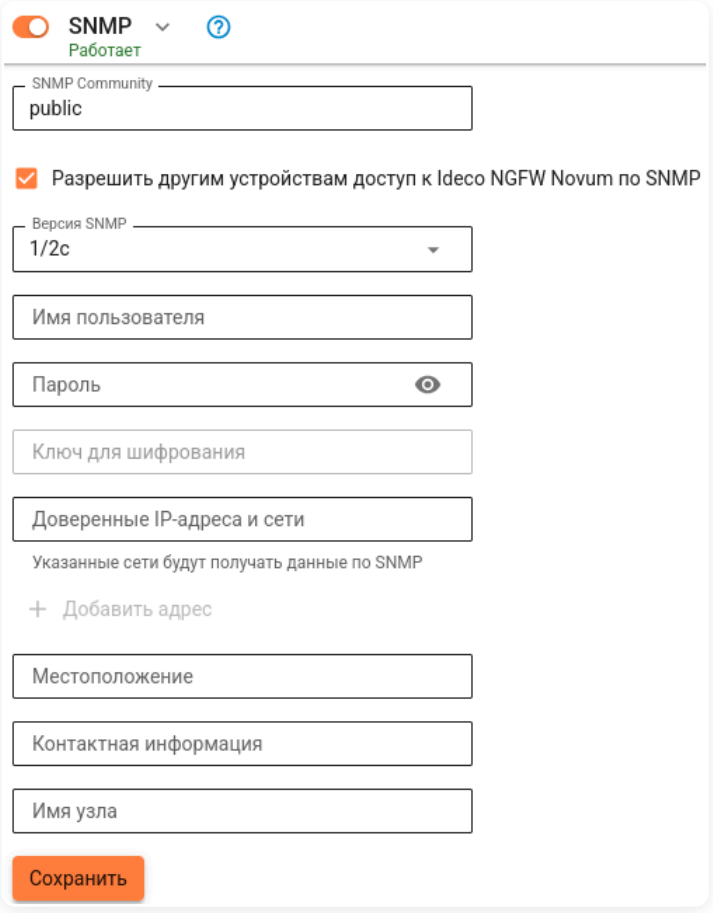
В статье - пошаговая инструкция по настройке SNMP на Ideco NGFW Novum и добавлению устройства в Zabbix Server.

Предусловия:

- Zabbix Server установлен и работает.
- Наличие сетевой доступности между Zabbix Server и Ideco NGFW Novum по UDP 161.

Настройка Ideco NGFW Novum

1. Перейдите в **Мониторинг** → **SNMP**, включите опцию **Разрешить другим устройствам доступ к Ideco NGFW Novum по SNMP** и заполните поля:



- **SNMP community** - введите название.
- **Версия SNMP** - выберите **1/2c**.
- **Доверенные IP-адреса и сети** - введите адрес Zabbix-сервера.

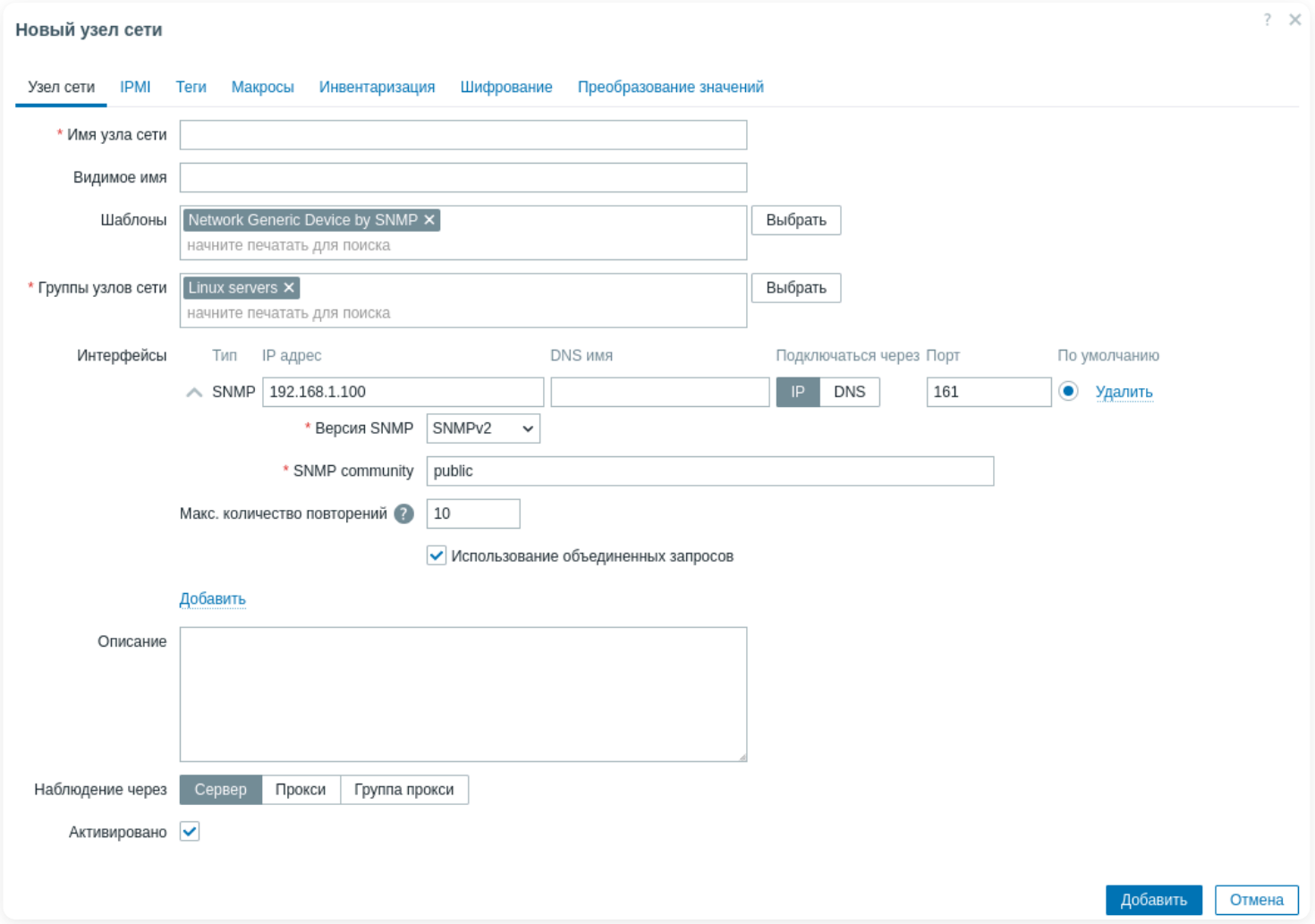
2. Нажмите **Сохранить**.

Настройка Zabbix-сервера

Инструкция актуальна для Zabbix версии 7.0.

1. Перейдите в **Сбор данных** → **Узлы сети** и в правом верхнем углу нажмите **Создать узел сети**.

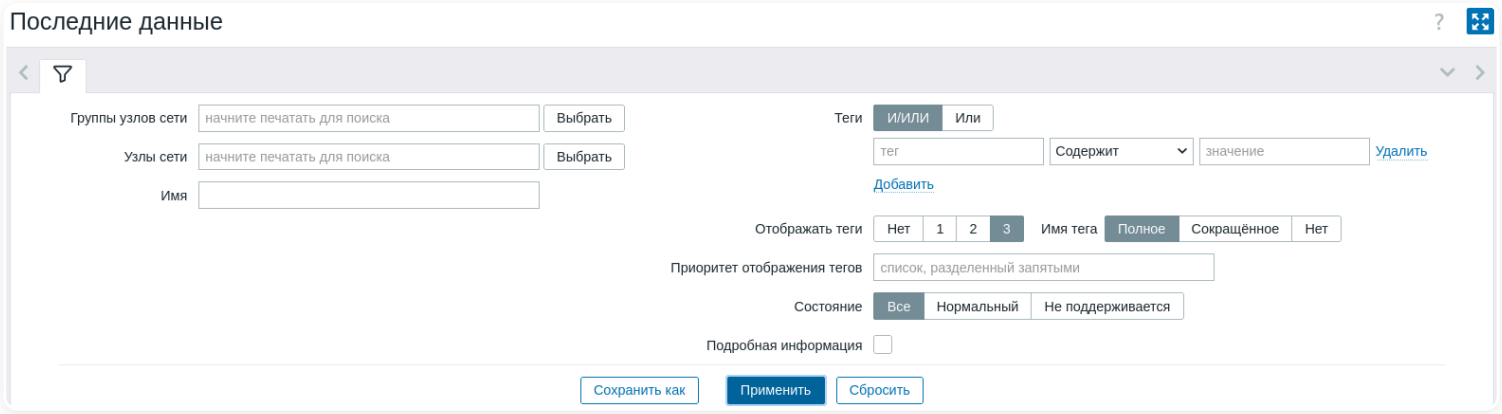
2. Заполните поля:



- **Имя узла сети** - введите название узла.
- **Шаблоны** - выберите в группе шаблонов **Templates/Network devices** → **Network Generic Device by SNMP**.
- **Группы узлов сети** - выберите **Linux servers**.
- **Интерфейсы** - нажмите **Добавить** и выберите **SNMP**:
  - **IP адрес** - введите IP-адрес NGFW Novum.
  - **Версия SNMP** - выберите **SNMPv2**.
  - **SNMP community** - введите название, указанное в настройках NGFW Novum.

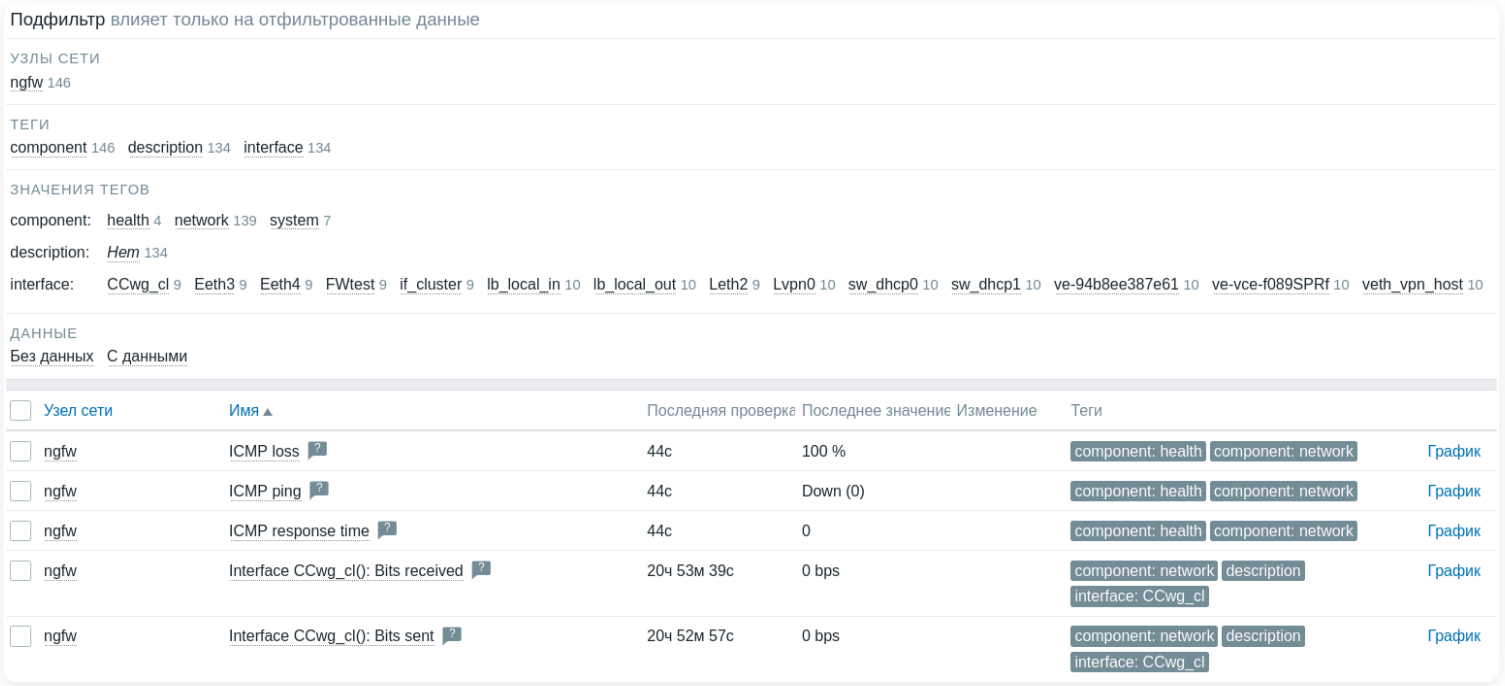
3. Нажмите **Добавить**.

4. Перейдите в **Мониторинг** → **Последние данные** и заполните поля:



- **Группы узлов сети** - выберите **Linux servers**.
- **Узлы сети** - выберите узел, созданный ранее.

5. Нажмите **Применить**. В таблице отобразятся данные NGFW Novum:



Подробнее об отображаемых данных шаблона **Network Generic Device by SNMP** можно посмотреть в статье.

Полезные ссылки

- **SNMP**
- **Zabbix-агент**

Тестирование оперативной памяти сервера

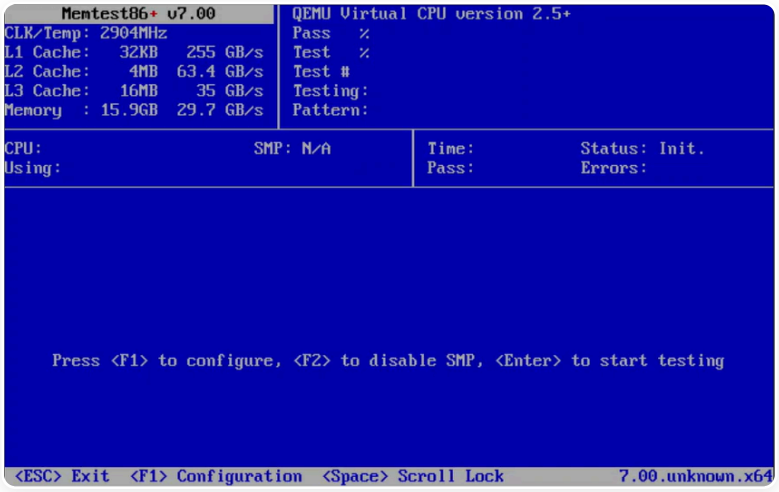
Для нормальной работы сервера все аппаратные компоненты сервера должны функционировать исправно.
Тестирование памяти помогает выявить и исключить проблемы с оперативной памятью сервера при поиске неисправностей.

При загрузке GRUB используйте Memtest86+ для тестирования оперативной памяти.
Для запуска тестирования выполните действия:

1. При загрузке сервера выберите **Memory test**:

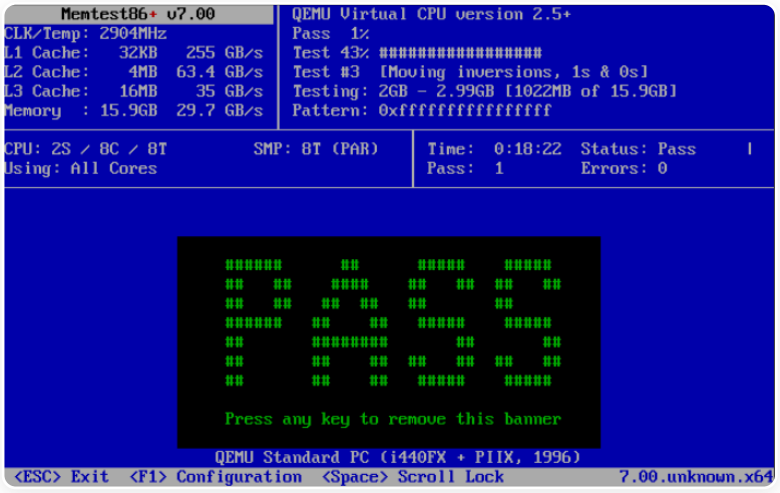


2. Нажмите **Enter** или подождите 5 секунд для автоматического запуска тестирования:

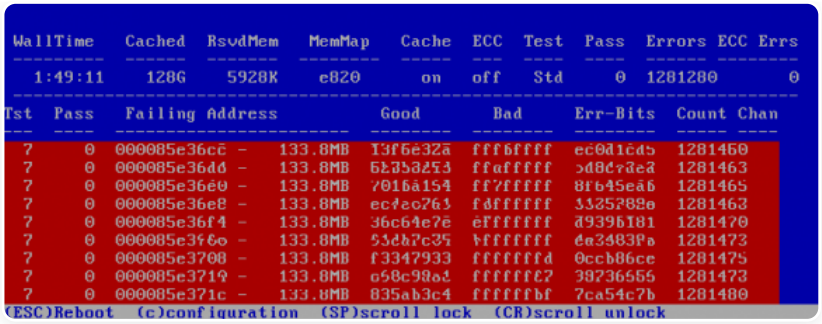


> Для выбора режима диагностики **Fail-Safe Mode** нажмите **F1**.
>
> Для выбора режима диагностики **Multi-Threading(SMP)** нажмите **F2**.

- Если появится запись **PASS**, тесты памяти пройдены успешно:



- При ошибке памяти появится запись вида:



Полезные ссылки

- Выбор аппаратной платформы

Как настроить автоматическое включение аппаратного комплекса Ideco NGFW Novum после сбоя питания

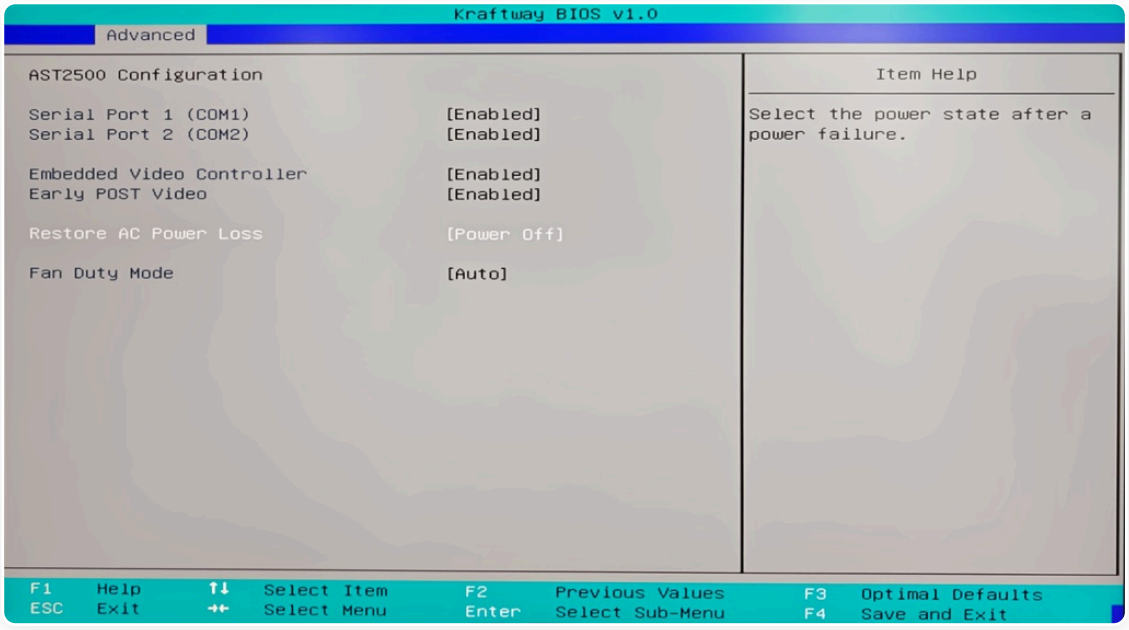
Решение подходит для всех моделей аппаратных комплексов Ideco NGFW Novum.

Для автоматического восстановления работы аппаратного комплекса Ideco NGFW Novum после сбоя электропитания необходимо активировать опцию **Restore AC Power Loss (Восстановления питания после сбоя)** в BIOS. Для включения опции:

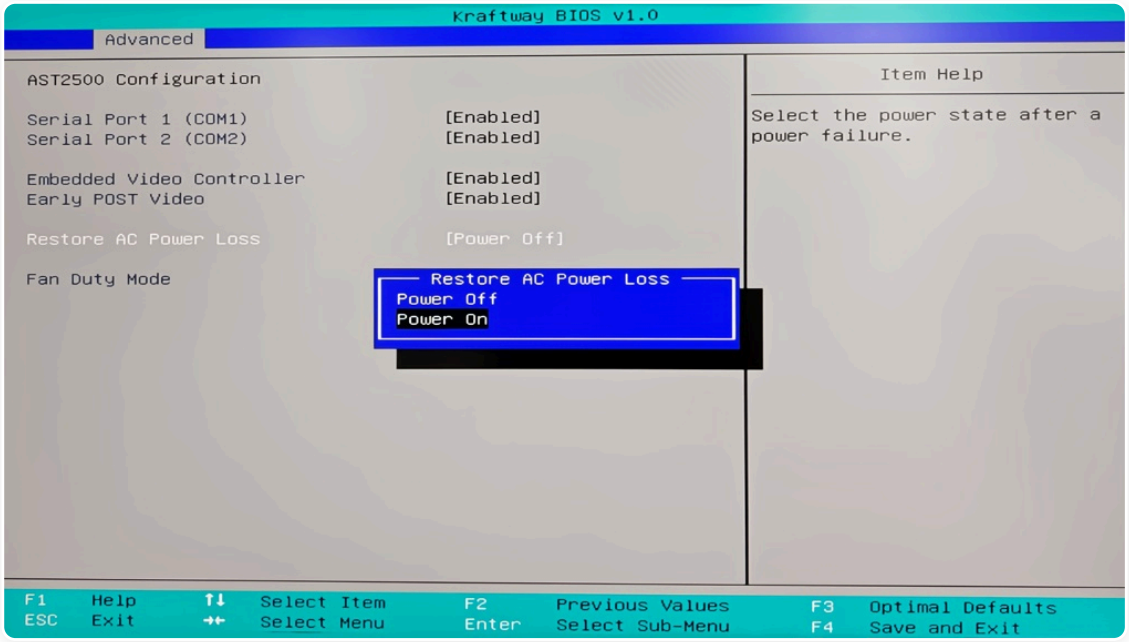
1. Запустите перезагрузку сервера.

2. Во время начальной загрузки нажмите `Delete`, чтобы зайти в BIOS.

3. В BIOS перейдите на вкладку **Advanced (Настройки)** и выберите **AST2500 Configuration (Настройка контроллера AST2500)**.



4. В меню найдите параметр **Restore AC Power Loss (Восстановления питания после сбоя)** и установите для него значение **Power ON (Включать питание)**.



5. Для сохранения настроек и выхода из BIOS нажмите `F4` и подтвердите действие.

После активации опции сервер будет автоматически запускаться при восстановлении электропитания.

Сброс пароля IPMI на сервере NGFW Novum

При первом входе в IPMI с логином `ADMIN` система требует смены пароля по умолчанию. Если новый пароль будет утерян, его можно сбросить с помощью утилиты `ipmitool`. Утилита уже предустановлена в NGFW Novum, поэтому устанавливать отдельно не требуется. Данный метод позволяет изменить пароль для существующей учетной записи.

Для сброса пароля выполните действия:

Шаг 1. Смена пароля

1. Для смены пароля потребуется узнать ID пользователя. В терминале NGFW Novum выполните команду:

```
ipmitool user list
```

2. Введите команду для смены пароля:

```
ipmitool -I open user set password <user_id> <new_password>
```

- `user_id` - идентификатор пользователя из списка (например, `2` для учетной записи `ADMIN`).
- `new_password` - новый пароль. Должен соответствовать требованиям:
  - Не менее 8 символов.
  - Должен содержать заглавные и строчные буквы, цифры и специальные символы.

Шаг 2. Проверка пароля в веб-интерфейсе

1. Откройте браузер и перейдите по IP-адресу IPMI-интерфейса.

2. Введите учетные данные, указанные на шаге 2. Вход выполнен.

Полезные ссылки

- **Выбор аппаратной платформы**

Поддержка устаревших алгоритмов шифрования

Ideco NGFW Novum основан на операционной системе Fedora. В Ideco NGFW Novum используется Fedora 42. Подробнее об изменениях политики алгоритмов можно прочитать в статье.

Устаревшие алгоритмы, как (криптографическое) хеширование и шифрование, обычно имеют время жизни, по истечении которого считаются либо слишком рискованными для использования, либо просто небезопасными.

Могут возникнуть неполадки, связанные с работой HTTPS, например, при пробросе OWA (веб-интерфейс для доступа к Microsoft Exchange). Столкнувшись с этим, выполните следующие действия для перехода в режим совместимости уровней политики шифрования:

1. Зайдите в консоль Ideco NGFW Novum. Это можно сделать из локального меню, по ssh или через веб-интерфейс Ideco NGFW Novum.

2. Введите в терминале команду `update-crypto-policies --set DEFAULT:FEDORA32`.

3. Перезагрузите Ideco NGFW Novum.



Настоятельно не рекомендуем использовать данную настройку, так как при следующем обновлении Ideco NGFW Novum настройки режима совместимости будут сброшены. В более новых версиях данная возможность будет отключена.

Полезные ссылки

- **ГОСТ VPN**

Восстановление конфигурации из бэкапа

Восстановление в рамках одного сервера

В NGFW Novum возможно полное и мгновенное восстановление из бэкапа.

При выполнении полного восстановления система будет перезагружена для применения настроек сервера.

При мгновенном восстановлении бэкап применяется без перезагрузки. При этом логи журнала **Система** не входят в бэкап, поэтому содержимое журнала не изменяется при восстановлении.

При восстановлении системы из резервной копии информация о лицензии не будет восстановлена, поскольку это может привести к использованию устаревшей лицензии.

После завершения процесса восстановления Ideco NGFW Novum автоматически отправит запрос в личный кабинет для обновления лицензии. Офлайн-лицензию необходимо загрузить самостоятельно.

Если резервное копирование используется для переноса настроек с одного сервера на другой, выполните "перепривязку" лицензии.

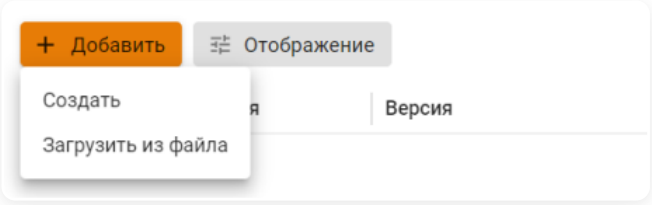
Полное восстановление конфигурации возможно только из бэкапов, версия которых не превышает версию текущей установленной системы.
Например, для Ideco NGFW Novum версии 20 подойдут бэкапы с 19 или 20 версии. При этом важно учитывать минорные версии: например, в версии 19.13 невозможно восстановление из бэкапа, созданного в 19.14.

Мгновенное восстановление возможно только из бэкапа, созданного в той же версии, что и текущая версия на сервере.

Через веб-интерфейс

Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и нажмите кнопку **Полное восстановление** или **Мгновенное восстановление** в столбце **Управление**.

Также можно загрузить бэкап из файла. Например, в случае переноса с другого сервера. Для восстановления конфигураций бэкапа, который находится на внешнем носителе, перейдите на **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

- **Восстановить из бэкапа** - восстановятся все настройки и перезагрузится сервер.
- **Мгновенно восстановить из бэкапа** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

Нажмите **Enter**.

2. Выберите из списка бэкап, введя пункт нужной копии, и нажмите **Enter**.

3. Перезагрузите сервер при запуске полного восстановления, введя **y**, а затем **Enter**. При мгновенном восстановлении перезагрузка не нужна.

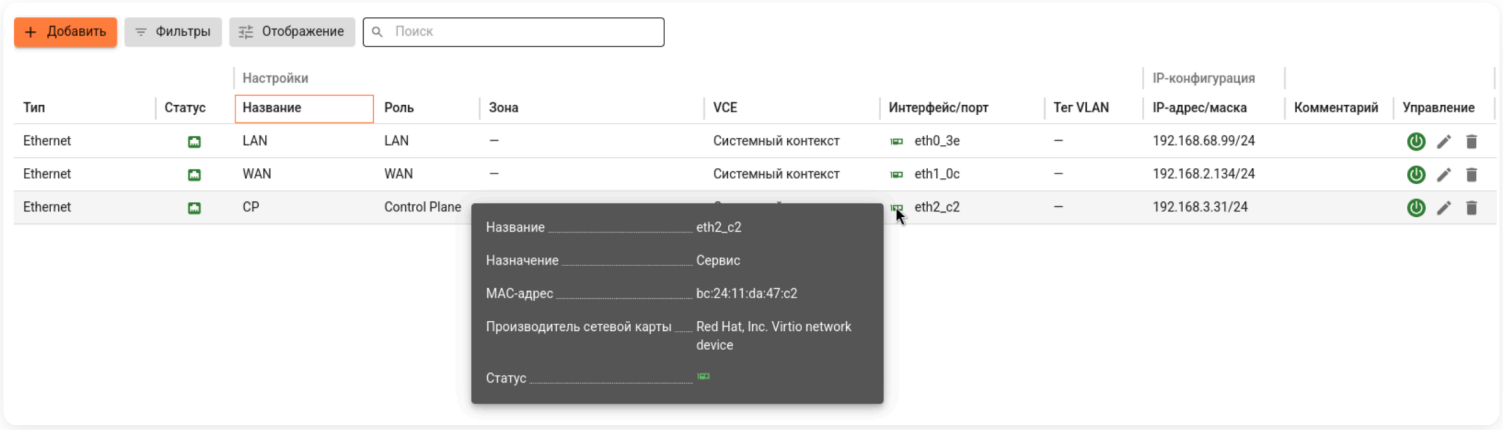
Пример восстановления из бэкапа через локальное меню:

```
Введите номер пункта и нажмите Enter.
# 13

Выберите бэкап для восстановления:

1.
Время:          12.01.2026 14:29:26
Версия:         Ideco NGFW 22.9.297
Комментарий:    backup01
2.
Время:          12.01.2026 14:26:01
Версия:         Ideco NGFW 22.9.297
Комментарий:

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1

Выбран бэкап

Время:          12.01.2026 14:29:26
Версия:         Ideco NGFW 22.9.297
Комментарий:    backup01

Для восстановления из бэкапа необходима перезагрузка.
Перезагрузить сервер и восстановить настройки сейчас?

Пожалуйста подтвердите ваш выбор.

Введите 'y' и нажмите Enter для подтверждения.
Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# y
```

Восстановление на другом сервере

Если необходимо восстановить конфигурацию из бэкапа на другом сервере, установите Ideco NGFW Novum на новый сервер и выполните шаги по восстановлению данных:

1. На новом сервере перейдите в **Сервисы** → **Сетевые интерфейсы**, наведите курсор на значение в столбце **Интерфейс/Порт** и запишите MAC-адрес Control Plane интерфейса:



2. Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите **Добавить** → **Загрузить из файла** и выберите бэкап, скачанный со старого сервера.

3. Нажмите в столбце **Управление** для перезагрузки сервера и применения настроек.

> После перезагрузки веб-интерфейс будет недоступен, так как настройки сетевых интерфейсов были заменены настройками из бэкапа.

4. Зайдите в локальное меню Ideco NGFW Novum, введите логин и пароль.

5. Перейдите в **Ethernet-интерфейсы** → **Изменить интерфейс**:

```
Управление сервером

1. Консоль
2. Физические порты
3. Ethernet-интерфейсы
4. Отключить все статические маршруты и добавить новый
5. Выбор типа кластерной сети
6. Отключить доступ к веб-интерфейсу из внешней сети
7. Включить доступ к серверу по SSH из Интернет
8. Включить доступ к серверу по SSH из локальных сетей
9. Включить режим `Разрешить Интернет всем`
10. Сбросить блокировки по IP
11. Отключить пользовательский межсетевой экран
12. Создать новый бэкап
13. Восстановить из бэкапа
14. Мгновенно восстановить из бэкапа
15. Включить доступ Удаленного Помощника
16. Контакты технической поддержки
17. Восстановиться на предыдущую версию
18. Перезагрузка сервера
19. Отключить сервер
20. Выход

Введите номер пункта и нажмите Enter.
# 3

1. Показать список интерфейсов
2. Создать интерфейс
3. Изменить интерфейс
4. Удалить интерфейс

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 3
```

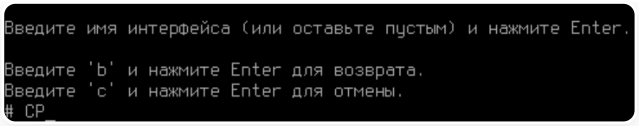
6. Выберите Control Plane интерфейс:

```
Выберите порт

-------------------------------------------------------------------------------------------------
  N    |  Название    |  Роль    |  VCE                |  Порт    |  IP                 |  Статус
-------------------------------------------------------------------------------------------------
  1    |  LAN         |  LAN     |  Корневой контекст  |          |  192.168.155.55/24  |  unknown
-------------------------------------------------------------------------------------------------
  2    |  WAN         |  WAN     |  Корневой контекст  |          |  192.168.1.81/24    |  unknown
-------------------------------------------------------------------------------------------------
  3    |  CP          |  CP      |  Корневой контекст  |          |  192.168.2.83/24    |  unknown
-------------------------------------------------------------------------------------------------

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 3_
```

7. Выберите порт, MAC-адрес которого был записан на шаге 1:

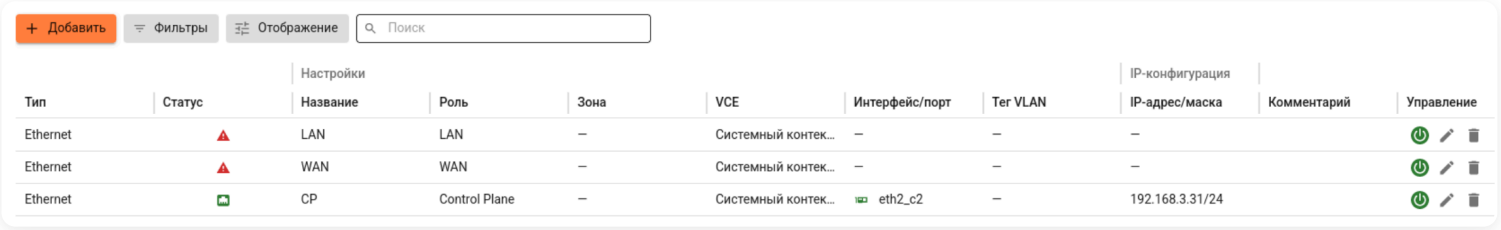
```
Выберите порт

-------------------------------------------------------------------------------------------------
  N    |  Порт                       |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------------
  1    |  Оставить прежние настройки |                     |                |
-------------------------------------------------------------------------------------------------
  2    |  eth0_3e                    |  bc:24:11:1a:f6:3e  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  3    |  eth1_0c                    |  bc:24:11:b2:48:0c  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  4    |  eth2_c2                    |  bc:24:11:da:47:c2  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 4_
```

8. Введите имя интерфейса или оставьте пустым:



9. Настройте Control Plane интерфейс, следуя инструкции с шага 3 в статье Установка в разделе **Настройка интерфейса управления**.

10. Перейдите в веб-интерфейс в **Сервисы** → **Сетевые интерфейсы** и настройте интерфейсы, привязав к ним физические порты:



11. Проверьте корректность настроек в разделах:

- **Сервисы** → **DNS** - внешние DNS-серверы.
- **Сервисы** → **DHCP-сервер** - опции DHCP-сервера.
- **Правила трафика** → **Файрвол** - зоны источника и зоны назначения в правилах.
- **Маршрутизация** → **OSPF** - настройку интерфейсов.
- **Маршрутизация** → **Внешних сетей** - правила маршрутизации.
- **Маршрутизация** → **Балансировка и резервирование** - настройку балансировки и адрес шлюза.

Перенос лицензии

Если сервер переносится из-за неисправности старого, необходимо перепривязать лицензию. Для этого:

1. Перейдите в MY.IDECO.

2. Отвяжите лицензию от старого сервера, нажав на .

3. Отвяжите demo-лицензию от нового сервера, нажав на .

4. Привяжите enterprise-лицензию к новому серверу, нажав **Свободные лицензии** → **Привязать к серверу**.

> В случае возникновения проблем при привязке лицензий обратитесь в Техническую поддержку.

Перенос данных почтового сервера

1. Скопируйте всю почту из папки `/var/mail/` на внешнее хранилище. Это можно сделать с помощью различных программ для копирования файлов между локальным компьютером и удаленным сервером (например: rsync, WinSCP, scp от ssh и др.).

2. Установите с загрузочного образа последнюю версию Ideco NGFW Novum на физический диск.

3. Подключите второй физический диск, который будет использоваться для хранения почты.

4. В веб-интерфейсе Ideco NGFW Novum перейдите в **Почтовый релей** → **Основные настройки**, выберите диск для хранения почты и отформатируйте диск.

5. Разрешите доступ по SSH из локальных сетей в **Управление сервером** → **Администраторы**.

6. Подключитесь к NGFW Novum, например, с помощью программы WinSCP и выгрузите всю скопированную почту по пути `/var/spool/mail/`.

7. По окончании выгрузки файлов почты выполните команду:

```
chown -R ideco-mail-backend:ideco-mail-backend /var/spool/mail/
```

> Команда выше меняет владельца и группу для файлов почты, чтобы почтовый демон `dovecot` мог иметь доступ к этим файлам.

> Если на Ideco NGFW Novum настроен кластер, то перед работой с бэкапами нужно ознакомиться с особенностями работы бэкапов:

- Невозможно полное восстановление из бэкапов. При этом можно создать резервную копию и после разрушения кластера восстановить копию на ноде, которая была активной.
- На активной ноде доступно **Мгновенное восстановление из бэкапа**. Восстанавливаются все настройки, кроме статистики в отчетах. Данные на второй ноде также придут в соответствие с восстановленными настройками после синхронизации нод.

Полезные ссылки

- **Бэкапы**

Публикация ресурсов

Доступ из внешних сетей без NAT

Перейти >

Портмаппинг (проброс портов, DNAT)

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

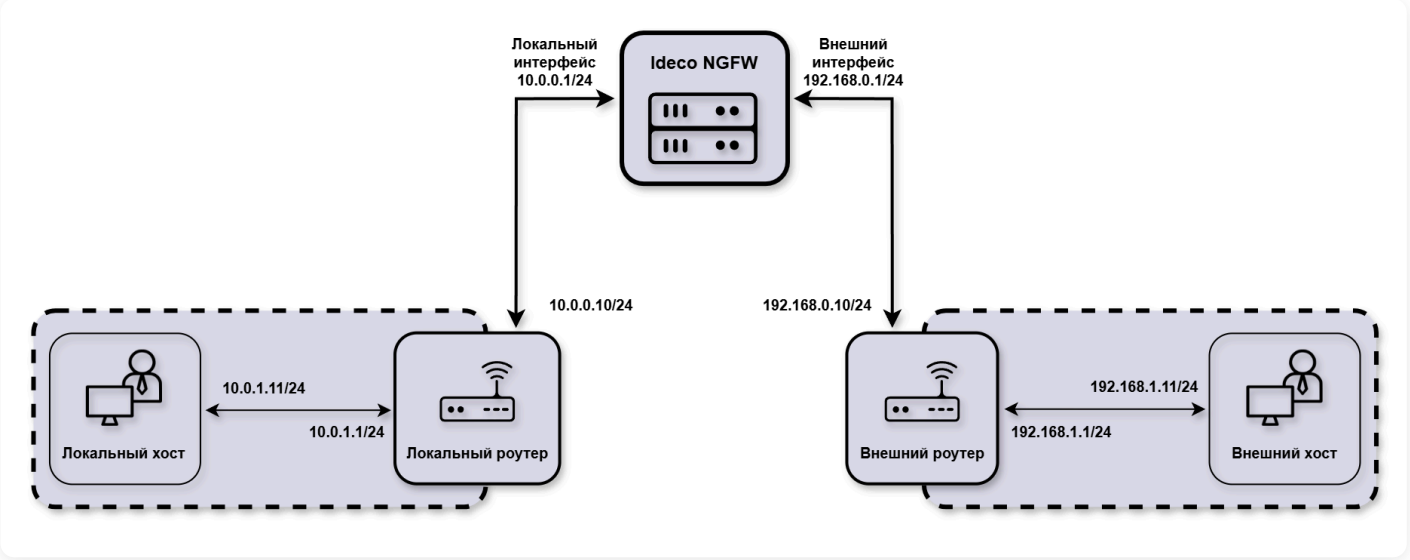
Доступ из внешних сетей без NAT

Классический контекст | Высокопроизводительный контекст

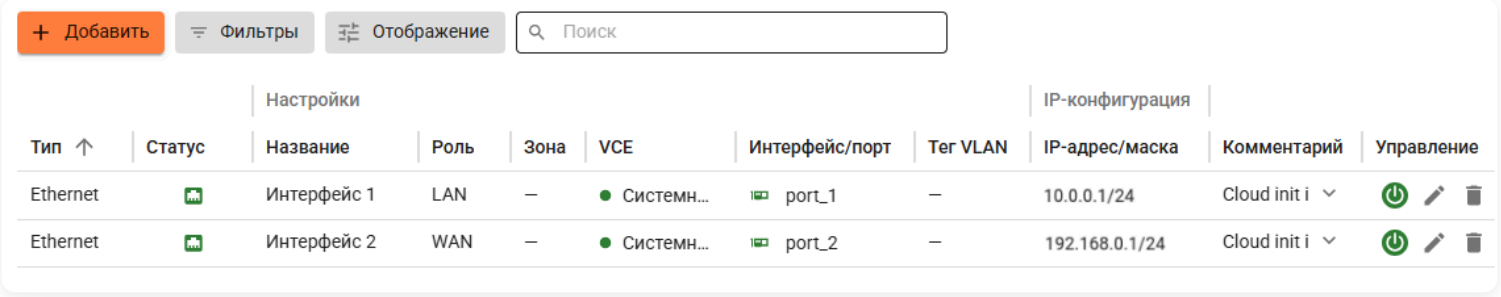
Если Ideco NGFW Novum расположен не на границе с интернетом, а внутри локальной сети, и при этом одна из подключенных сетей считается внешней, доступны действия:

- Организовать прямой доступ к ресурсам внешних по отношению к Ideco NGFW Novum сетей без использования NAT.
- Разрешить доступ из внешних относительно Ideco NGFW Novum сетей в локальную сеть с прямым обращением к локальным IP-адресам.

Пример. Настройка Ideco NGFW Novum для доступа без NAT в следующей конфигурации сети:



1. Настройте сетевые интерфейсы в **Сервисы** → **Сетевые интерфейсы** → **Интерфейсы** на Ideco NGFW Novum:



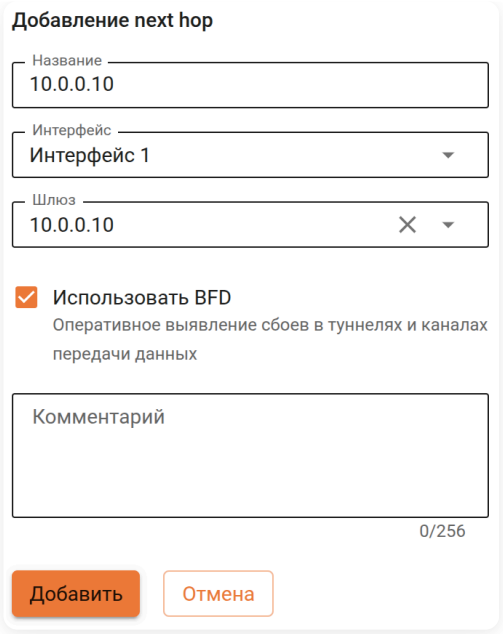
- С ролью **LAN** - интерфейс для доступа в пользовательскую локальную сеть.
- С ролью **WAN** - интерфейс для доступа в пользовательскую внешнюю сеть.

2. В разделе **Маршрутизация** создайте правила для доступа к IP-адресам пользователей, которые находятся за маршрутизаторами:

Для Локальных сетей

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

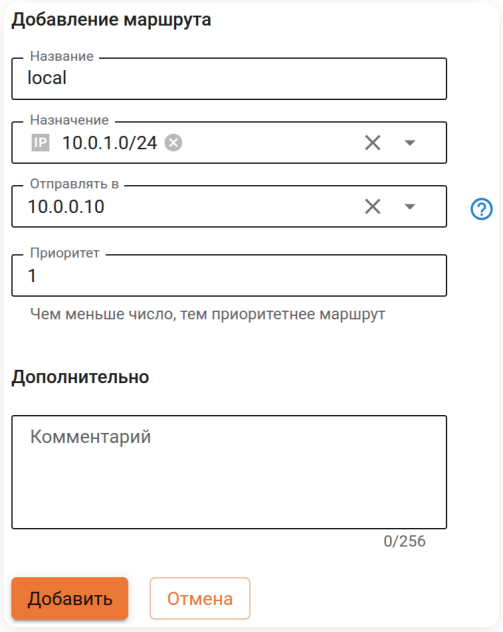
2. Заполните поля и нажмите **Добавить**:



- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс для доступа в пользовательскую локальную сеть.
- **Шлюз** - укажите адрес маршрутизатора (`10.0.0.10`).

3. Перейдите в **Маршрутизация** → **Статическая** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:



- **Название** - укажите название.
- **Назначение** - выберите адрес локальной сети за маршрутизатором (`10.0.1.0/24`).
- **Отправлять в** - выберите созданный на шаге 2 **Next hop**.

Для Внешних сетей

1. Перейдите в **SD-WAN** → **Next hop** и нажмите **Добавить**.

2. Заполните поля и нажмите **Добавить**:

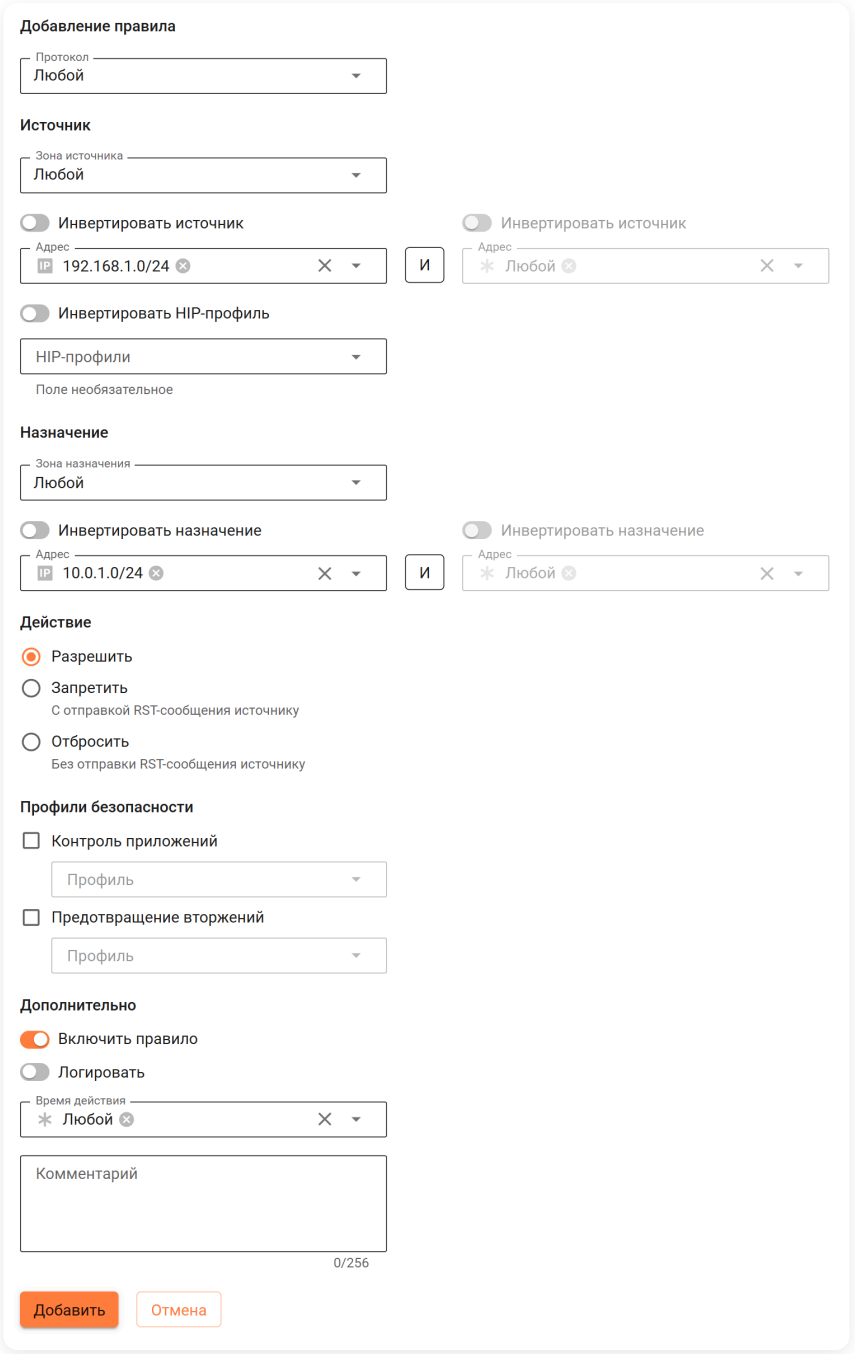
- **Название** - укажите название.
- **Интерфейс** - выберите интерфейс для доступа в пользовательскую внешнюю сеть.
- **Шлюз** - укажите адрес маршрутизатора (`192.168.0.10`).

3. Перейдите в **Маршрутизация** → **Внешних сетей** и нажмите **Добавить**.

4. Заполните поля и нажмите **Добавить**:

- **Название** - укажите название.
- **Назначение** - выберите адрес внешней сети за маршрутизатором (`192.168.1.0/24`).
- **Отправлять в** - выберите созданный на шаге 2 **Next hop**.

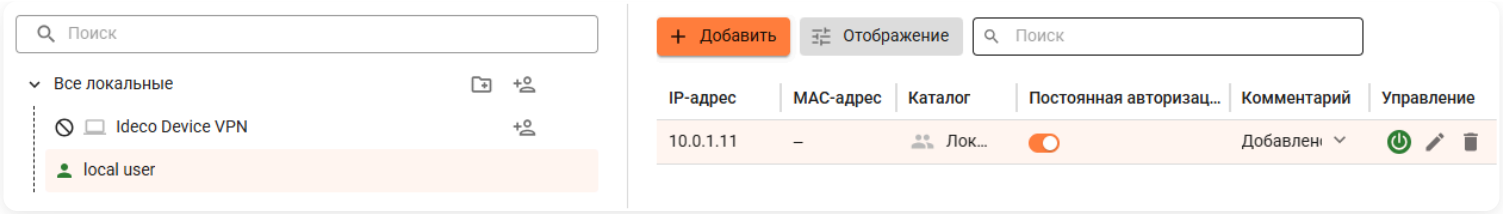
3. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**, создайте и включите правило для доступа хостов из внешней сети `192.168.1.0/24` до IP-адресов пользователей локальной сети `10.0.1.0/24`:



Правило необходимо, чтобы разрешить трафик в пользовательской цепочке **FORWARD**. Трафик из внешних сетей в локальные, не указанный в таблице **FORWARD**, будет заблокирован системным правилом.

4. Перейдите в **Правила трафика** → **Межсетевой экран** → **SNAT** и отключите опцию **Автоматический SNAT локальных сетей**.

5. Перейдите в **Пользователи** → **Учетные записи** и включите опцию **Постоянная авторизация** для пользователей локальной сети `10.0.1.0/24` на вкладке **IP и MAC авторизация**. Устройства локальной сети должны быть авторизованы на NGFW:



Учитывайте риски подобного доступа с точки зрения информационной безопасности. Не предоставляйте доступ для внешних сетей и хостов, в безопасности которых не уверены.

Полезные ссылки

- **Межсетевой экран**
- **Статическая маршрутизация**

Портмаппинг (проброс портов, DNAT)

Сервер предоставляет доступ к опубликованному в интернете веб-ресурсу (сервису, сетевой службе) на устройстве в локальной сети с серым IP-адресом. Ресурс публикуется путем трансляции (проброса) любого неиспользуемого сетевого порта на публичном IP-адресе сервера Ideco NGFW Novum на порт ресурса, работающего на устройстве в локальной сети. При этом все обращения из внешних сетей на публичный адрес сервера Ideco по транслируемому порту перенаправляются на публикуемый порт данного ресурса. Эта технология называется DNAT, portmapper или port forwarding.

Для настройки портмаппинга в Ideco NGFW Novum добавьте правило в **Правила трафика** → **Межсетевой экран** → **DNAT**. При создании правила укажите адреса сервера, публикуемой машины и сетевого порта, с которого и на который осуществляется трансляция сетевых запросов извне.

Создайте разрешающее FORWARD-правило, если:

- В таблице FORWARD есть запрещающее прохождение трафика правило. В этом случае поместите созданное правило выше запрещающего.
- Нужна проверка трафика профилями безопасности. В этом случае укажите в правиле нужные профили **Контроля приложений** или **Предотвращения вторжений**.
  Укажите при создании правила назначение (адрес устройства в локальной сети) и порт назначения.

> **Не рекомендуется использовать проброс портов для публикации веб- и почтовых серверов (80, 443 порты).** Для публикации портов воспользуйтесь обратным прокси-сервером.

Особенности создания правил DNAT с версии 18

- В предыдущих версиях профили безопасности настраивались в отдельных разделах. С версии 18 **Контроль приложений** настраиваются в правилах **Межсетевого экрана**.
- Для проверки трафика модулем **Контроль приложений** и системой **Предотвращения вторжений** необходимо создать FORWARD-правило с включенными настройками профилей безопасности.
- В случае проблем с доступом до публикуемой службы проверьте **Отчеты и журналы** → **События безопасности** → **Журнал IPS** и при необходимости отредактируйте правила нужного профиля **Предотвращения вторжений**.

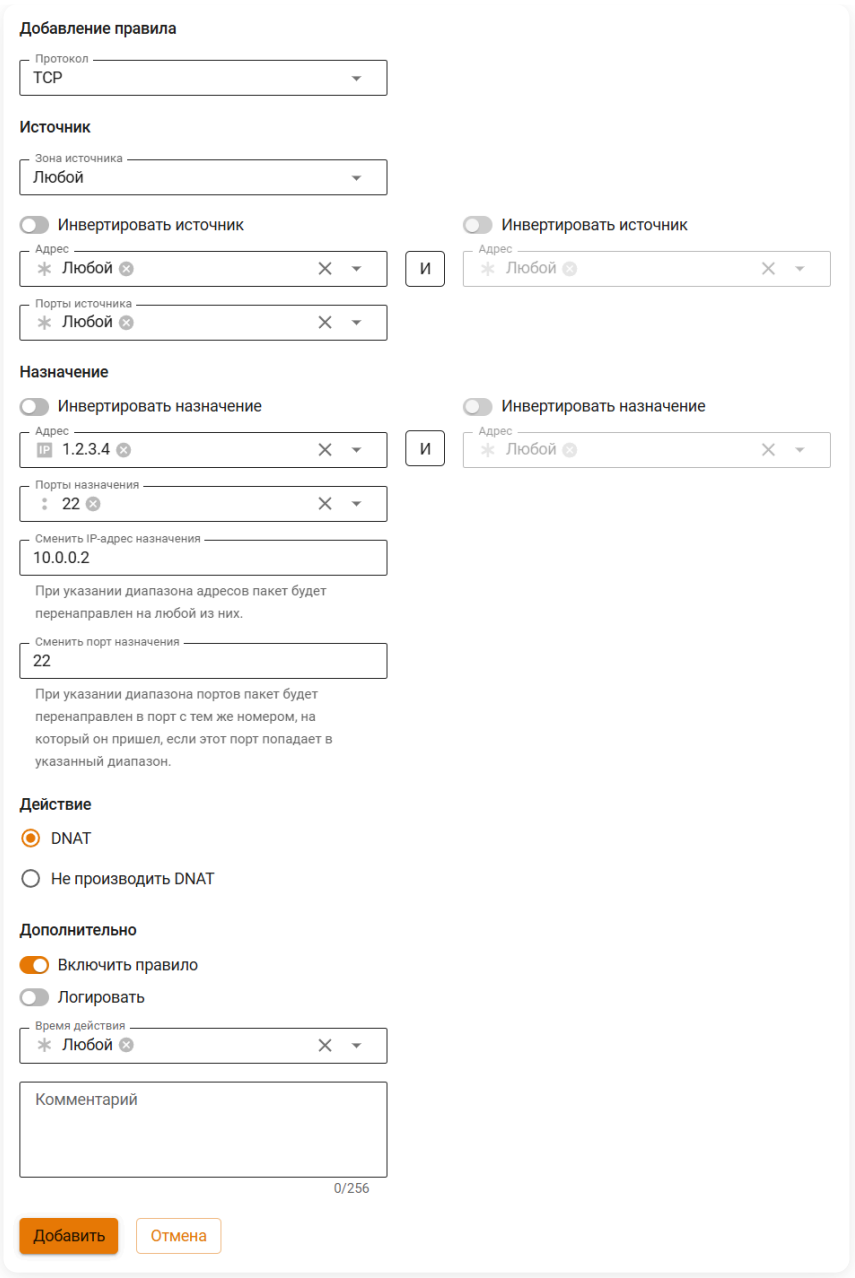
Создание правил DNAT и FORWARD в Межсетевом экране Ideco NGFW Novum

Пример:

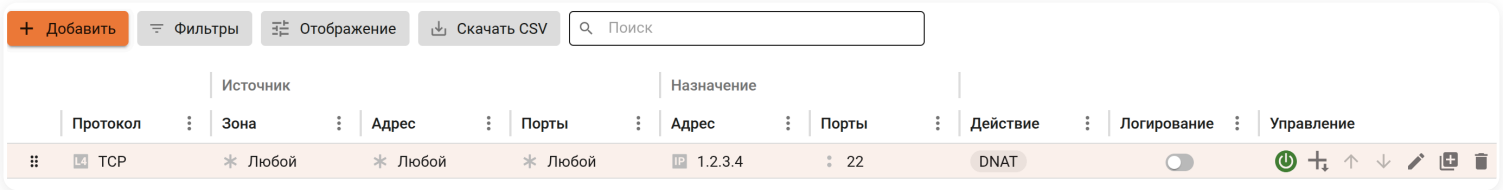
- Публичный адрес сервера Ideco - `1.2.3.4`.
- Публикуемая служба - SSH, работающая на 22 TCP-порте.
- Адрес компьютера в локальной сети, где запущена служба, к которой нужен доступ извне - `10.0.0.2`.

Для настройки трансляции запросов к службе извне через сервер Ideco NGFW Novum на устройство в локальной сети перейдите в **Правила трафика** → **Межсетевой экран** → **DNAT** и нажмите **Добавить**.

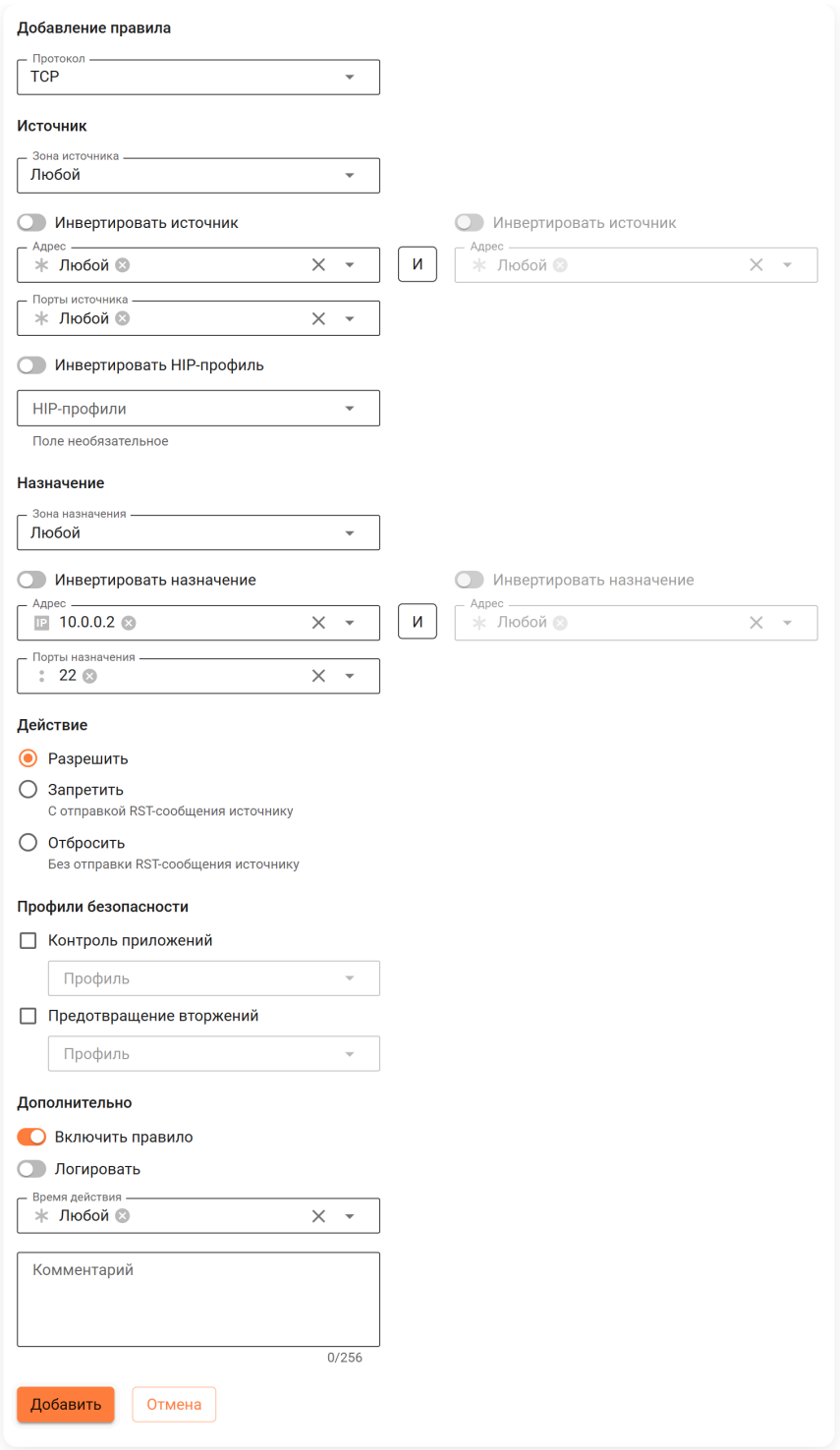
Заполните поля в соответствии с характеристиками, указанными в примере:



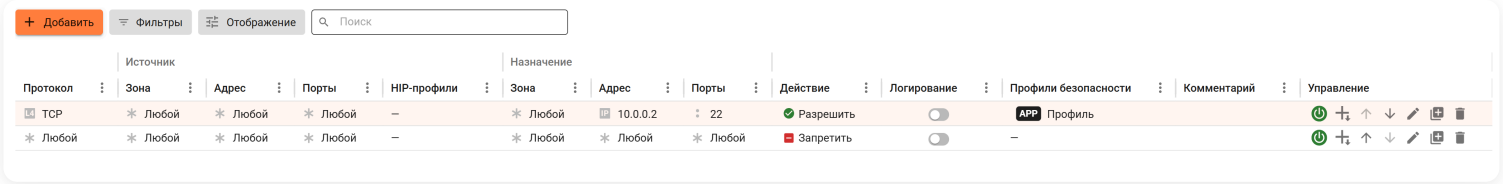
Вид правила в таблице после сохранения:



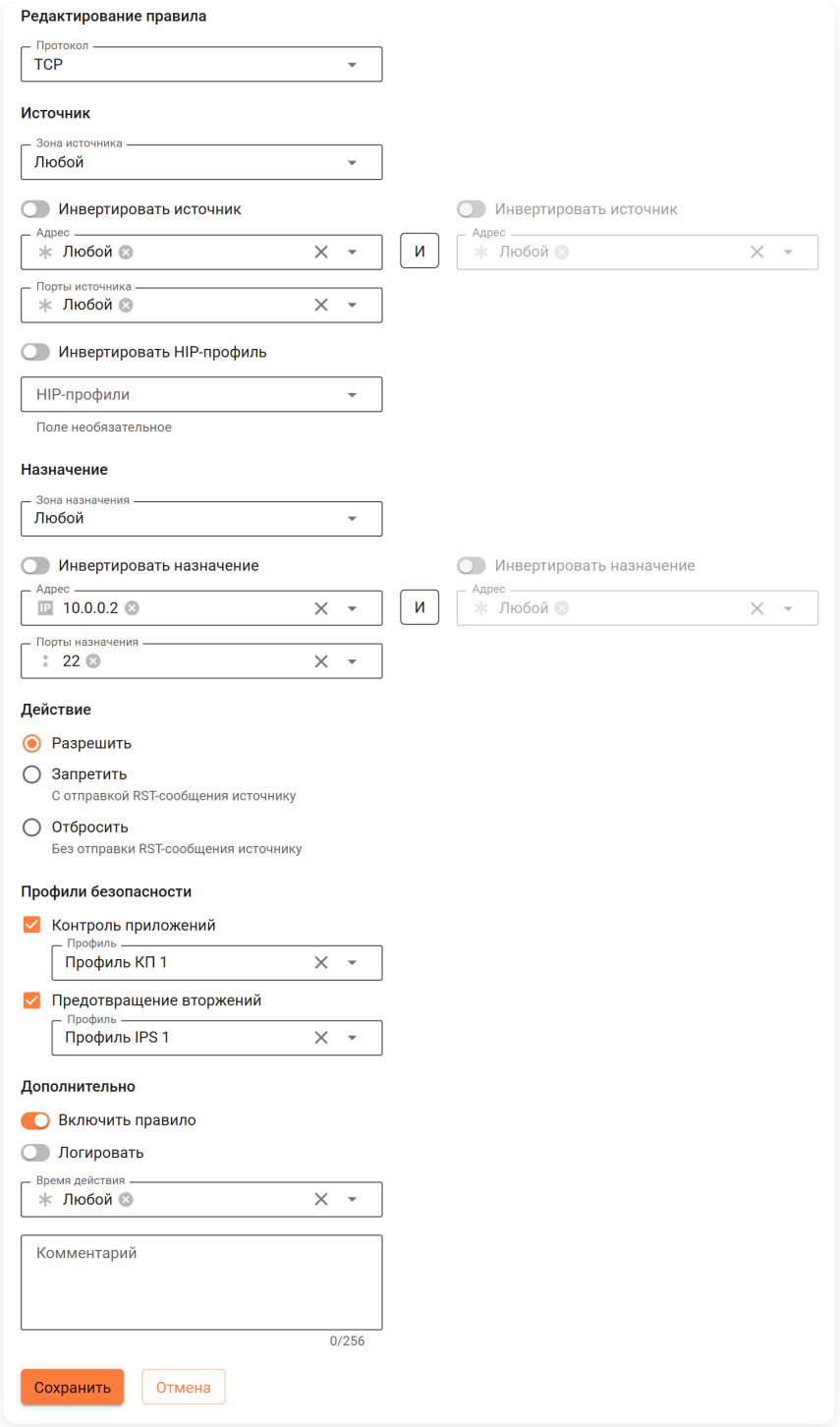
Проверьте наличие запрещающих правил в таблице **FORWARD**. При необходимости создайте правило, разрешающее трафик:



Поместите созданное правило выше запрещающего трафик:



Если хотите, чтобы трафик проверялся профилями безопасности, включите в созданном правиле соответствующие настройки:



Настройки **Межсетевого экрана** применяются сразу при создании правил.

Частые ошибки

- Если включен режим **Полный доступ**, правила **Межсетевого экрана**, включая таблицу **DNAT**, не работают. При этом трафик пользователя проходит Аппаратную и Предварительную фильтрацию. Если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет.

Рекомендации

- Проверять работу правила **DNAT** следует из внешней сети. Если необходим доступ из локальной сети, используйте обратный прокси-сервер для публикации веб-ресурсов.
- Порт на внешнем интерфейсе сервера, с которого транслируются запросы, не всегда совпадает с публикуемым портом самой службы. Например, для предотвращения автоматических попыток подключения вредоносного ПО на популярный сервис внешние запросы транслируются на порт 4489, а в локальную сеть - на порт 3389.
- Для защиты от нежелательных подключений к публикуемой службе при создании правила укажите в поле **Источник** IP-адрес или подсеть, с которой разрешено подключаться к этой службе.
- Если осуществляется трансляция на один и тот же номер порта локального сервера, заполнять поле **Сменить порт назначения** не обязательно. Система автоматически переадресует запрос на соответствующий порт устройства в локальной сети.

Устранение неполадок

- Убедитесь, что клиент, на которого осуществляется проброс портов, отвечает на эхо-запросы ping к внешним ресурсам. Основным шлюзом на данном устройстве следует указать локальный IP-адрес Ideco NGFW Novum, либо прописать маршрут.
- При правильной настройке публикуемая служба отвечает клиенту во внешней сети через тот же внешний интерфейс сервера, с которого изначально пришел запрос. Настройте правильный адрес SNAT для опубликованного сервиса с помощью создания правил в таблице SNAT, если в созданном правиле в поле **Назначение** указан публичный IP-адрес сервера для приема подключений извне, а также в случае переопределения автоматических правил NAT.
- Правило трансляции запросов на сервере не работает, если брандмауэр Windows или другие программы защиты блокируют соединения с внешних адресов в интернете. Для диагностики убедитесь, что настройки встроенного брандмауэра Windows или сторонних файрволов и антивирусов разрешают целевое соединение. Например, для проверки настроек брандмауэра на устройстве Windows перейдите в **Панель управления → Брандмауэр Защитника Windows → Дополнительные параметры → Правила для входящих подключений / Правила для исходящих подключений**.
- Правило портмаппинга пробрасывает трафик из внешней сети на хост в локальной сети. Трафик запроса ресурса из этой же локальной сети при обращении на внешний адрес не будет проброшен правильно. Во избежание асимметричной маршрутизации при диагностике сетевыми утилитами подключайтесь из внешних для NGFW сетей, а внутри локальной сети обращайтесь к сервису по IP-адресу сервиса в локальной сети. Альтернативный вариант - вынесите ресурс в отдельную локальную сеть, DMZ и обращайтесь к ресурсу из локальной сети клиентов по внешнему IP-адресу.

Полезные ссылки

- **Межсетевой экран**

Интеграции

Практические руководства по интеграции Ideco NGFW со сторонними решениями

Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG

Перейти >

Настройка совместной работы ViPNet Координатор с Ideco NGFW

Перейти >

Интеграция NGFW и SkyDNS

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка кластера Active/Active с брокером сетевых пакетов DS Integrity NG

В Ideco NGFW Novum реализована кластеризация Active/Passive. Повысить отказоустойчивость можно, создав кластер Active/Active. Для этого воспользуйтесь решением наших партнеров АО "НПП "Цифровые решения" - брокером сетевых пакетов DS Integrity NG.

Расположите брокер сетевых пакетов перед Ideco NGFW Novum. Брокер будет самостоятельно балансировать трафик устройств в локальной сети между нодами созданного кластера.

При падении одной ноды трафик перебалансируется между остальными Ideco NGFW Novum без перерыва в связи. Это реализует схему кластера Active/Active.

Объединять в кластер устройства Ideco NGFW Novum между собой не нужно.

Для корректной работы нод установите одинаковые настройки.

Для централизованного управления нодами Ideco NGFW Novum воспользуйтесь Ideco Center.

Особенности использования схемы:

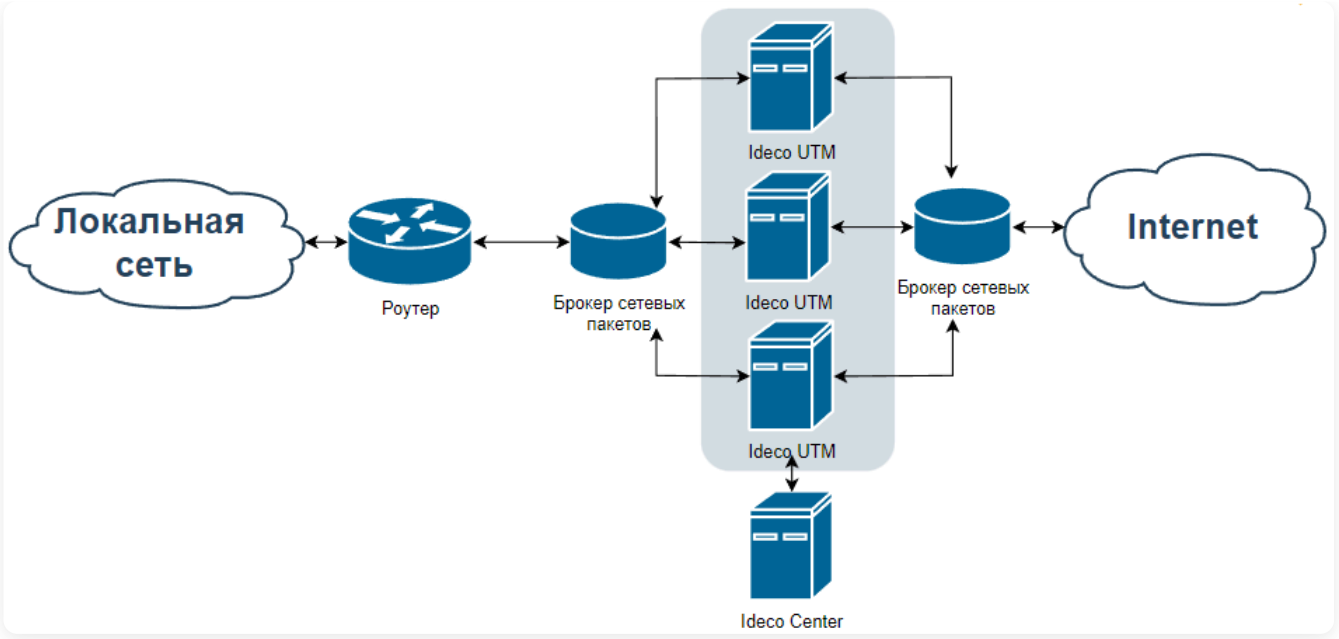
- Настройки, которые нельзя распространить через Ideco Center, придется вручную изменять на каждом Ideco NGFW Novum.
- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.
- Данные отчетности, логов и мониторинга не синхронизируются между нодами. В каждой ноде хранятся свои данные.
- Восстановление из бэкапа и обновление системы будет затрагивать только одну ноду. Каждую ноду потребуется обновлять отдельно.
- Между локальной сетью и брокером сетевых пакетов потребуется расположить роутер с настроенной динамической маршрутизацией (OSPF) для обмена маршрутами.
- На каждую ноду Ideco NGFW Novum потребуется отдельная лицензия. По вопросам условий лицензирования при использовании такой конфигурации обратитесь к менеджерам.

Примеры трех типовых схем совместного использования брокера сетевых пакетов DS Integrity NG и Ideco NGFW Novum ниже. На этой основе встройте оба решения в свою сеть.

На каждом Ideco NGFW Novum для обмена маршрутами необходимо настроить OSPF для всех локальных интерфейсов. Название зоны и вес должны быть идентичными настроенным ранее на роутере. Информация о настройке OSPF описана в статье OSPF. Там же находятся инструкции для настройки OSPF для MikroTik, который можно использовать в качестве роутера.

По вопросам настройки брокера обращайтесь в техническую поддержку АО "НПП "Цифровые решения".

Пример 1 - Два брокера, по одному со стороны локальной и внешней сетей



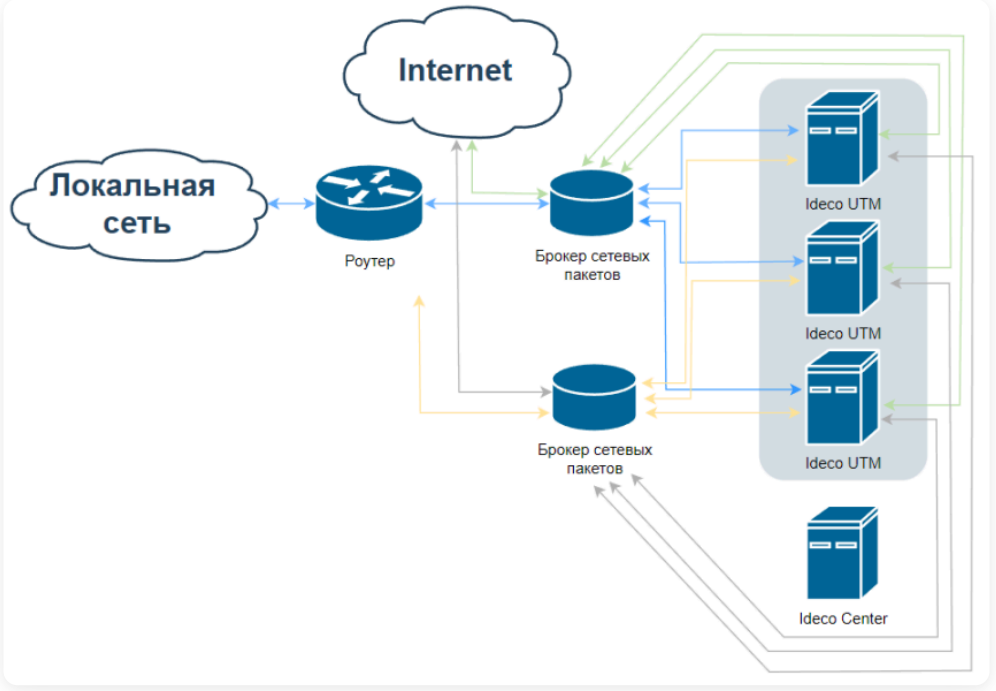
Настройка Ideco NGFW Novum:

На каждом устройстве Ideco NGFW Novum необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW Novum.

На каждом Ideco NGFW Novum в качестве шлюза внешнего интерфейса нужно использовать IP-адрес, полученный от провайдера.

Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW Novum



Настройка Ideco NGFW Novum

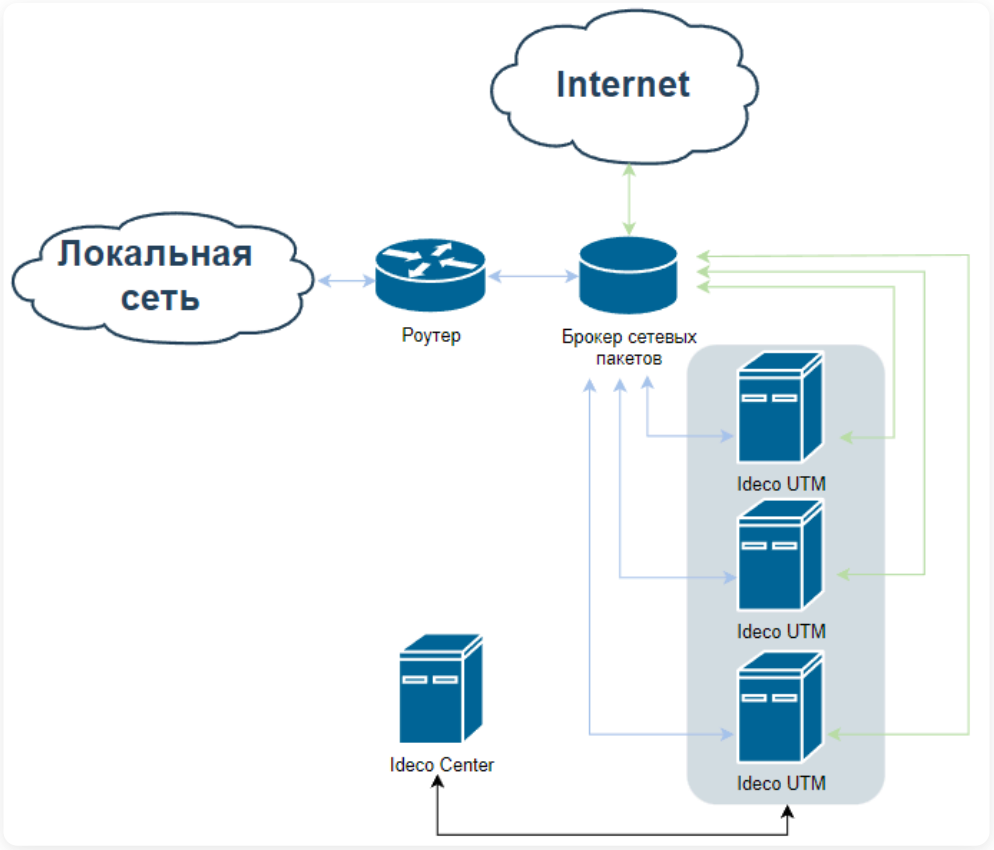
На каждом устройстве Ideco NGFW Novum необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW Novum.
- На каждом NGFW будет два локальных и два внешних интерфейса. Шлюзом внешних интерфейсов нужно указать IP-адрес, полученный от провайдера.

На Ideco NGFW Novum в этой конфигурации в разделе **SD-WAN** → **Профили next hop** должен быть активирован режим резервирования. Приоритетным внешним интерфейсом должен быть выбран интерфейс, который идет к основному брокеру сетевых пакетов.

Пример 3 - Один брокер, расположенный перед Ideco NGFW Novum



Настройка Ideco NGFW Novum

На каждом устройстве Ideco NGFW Novum необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW Novum.
- Шлюзом внешнего интерфейса нужно указать IP-адрес, полученный от провайдера.

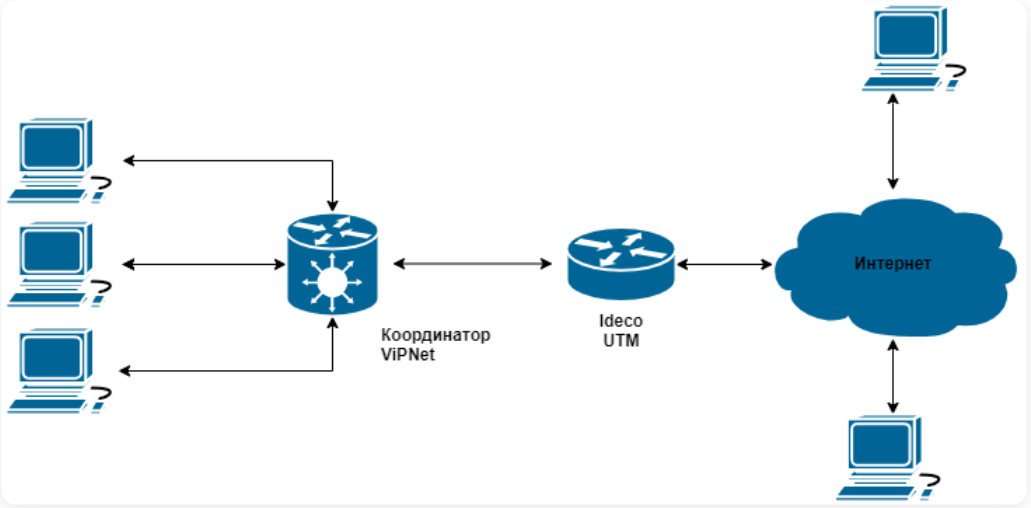
Полезные ссылки

- **Кластеризация**

Рекомендации по настройке NGFW для работы совместно с ViPNet-координатором

ViPNet-координатор используется для шифрования трафика подсети, в которой является шлюзом. Шифрование позволяет обеспечить конфиденциальность информации, передаваемой по незащищенному каналу.

Схема совместной работы Ideco NGFW Novum с ViPNet-координатором:



Настройка Ideco NGFW Novum и ViPNet-координатора

Для корректной работы Координатора совместно с NGFW выполните действия:

1. Настройте проброс порта udp 55777 на IP адрес координатора в **Межсетевой экран → DNAT (перенаправление портов)**.

2. Переведите Координатор в режим **Со статической трансляцией адресов**.

Работа Координатора в режиме динамической трансляции адресов совместно с Ideco NGFW Novum не гарантируется.

Более подробно о настройке ViPNet можно узнать в статье.

Полезные ссылки

- **Межсетевой экран**

Интеграция NGFW и SkyDNS

Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

Чем может быть полезна интеграция

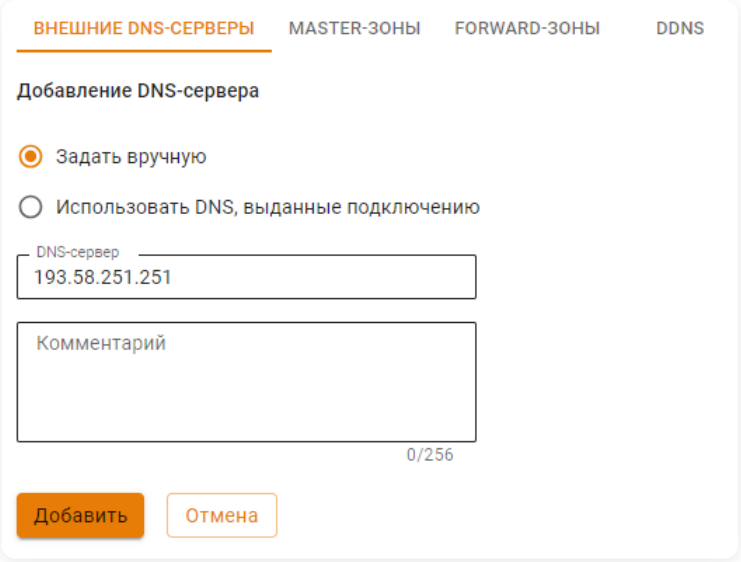
- **Защита от зараженных сайтов**. Вредоносные скрипты могут содержать сайты, как взломанные злоумышленниками, так и созданные специально для распространения вредоносного ПО.
- **Защита от бот-сетей**. Созданные из зараженных вредоносными программами компьютеров сети используются в DDoS-атаках на серверы, рассылках спама, похищениях паролей от интернет-банков и сервисов и в других целях. DNS-фильтрация ограничивает доступ к выявленным серверам для управления бот-сетями. В результате злоумышленники не смогут управлять компьютером, даже если компьютер заражен вредоносной программой.
- **Защита от нежелательных сайтов**. SkyDNS фильтрует интернет-ресурсы по более чем 50 категориям, что повышает качество фильтрации нежелательного контента.
- **Соблюдение 436-ФЗ О защите детей от информации, причиняющей вред их здоровью и развитию**. Сервис SkyDNS полностью соответствует требованиям Правил подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети интернет Минобрнауки РФ.

Настройка интеграции Ideco NGFW Novum и SkyDNS

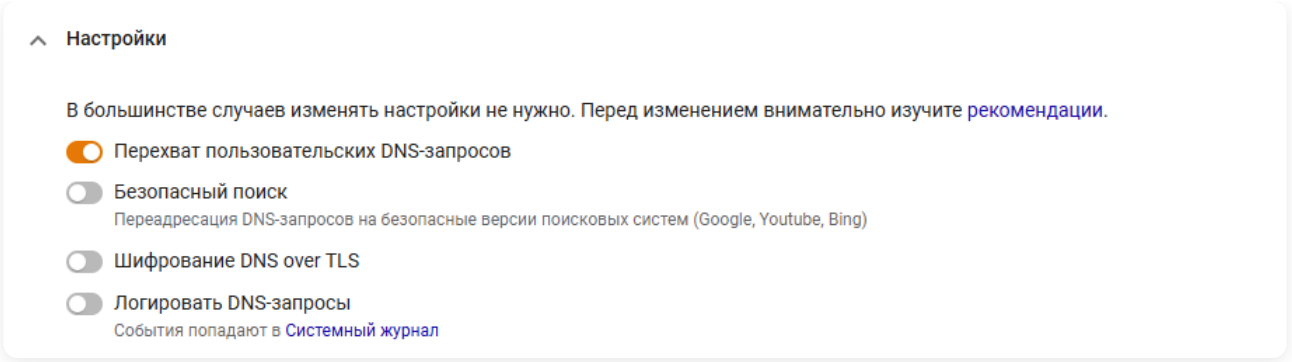
Чтобы настроить интеграцию со SkyDNS, выполните действия:

1. Перейдите в **Сервисы** → **DNS** → **Внешние DNS-серверы** и нажмите **Добавить**.

2. Выберите пункт **Задать вручную** и в поле **DNS-сервер** введите IP-адрес DNS-сервера SkyDNS (`193.58.251.251`) и нажмите **Добавить**:

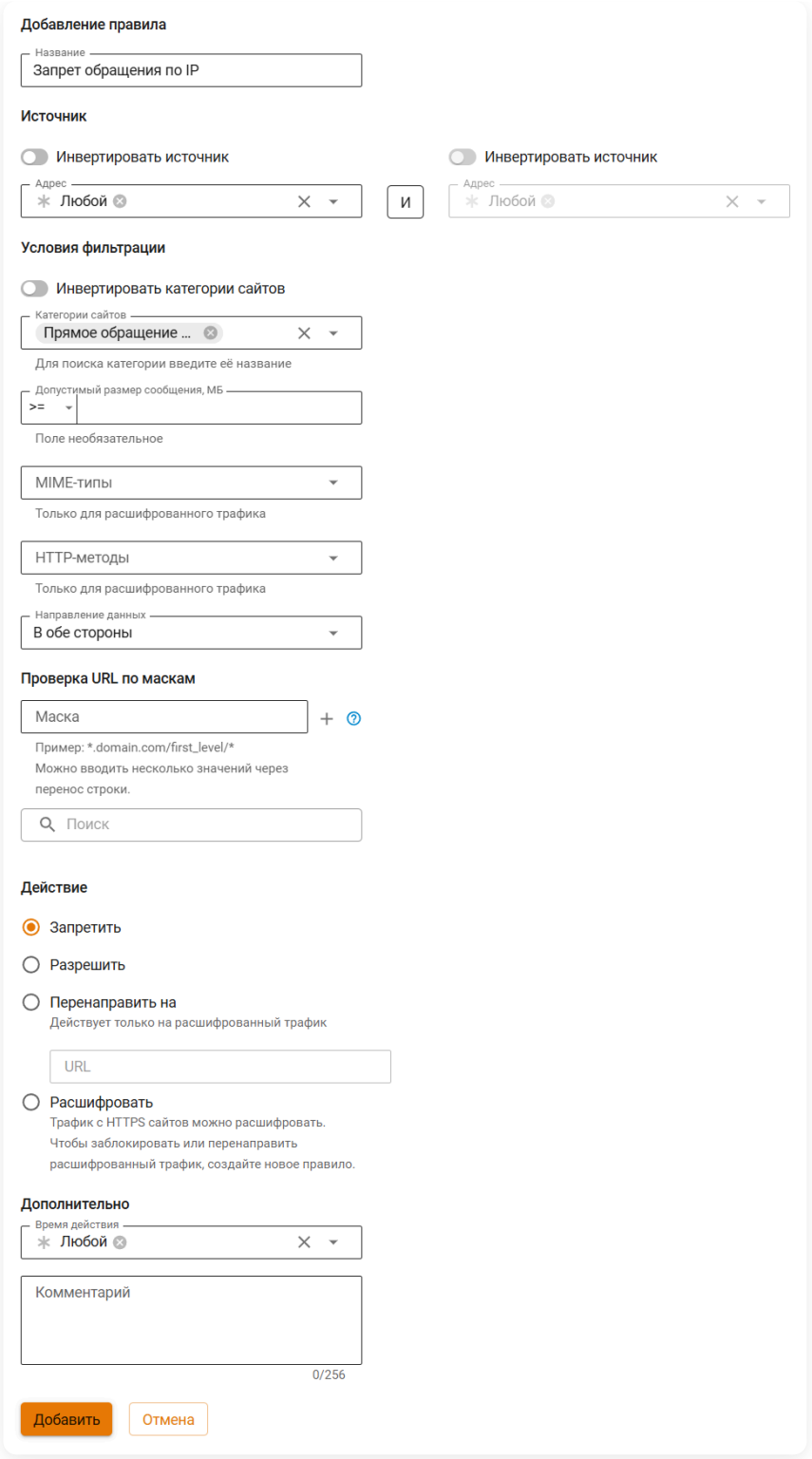


3. В настройках DNS включите опцию **Перехват пользовательских DNS-запросов** для запрета обращения к другим DNS-серверам (если фильтрация через SkyDNS обязательна для всей сети):



4. Если внутри локальной сети или внутри сети провайдера есть внутренняя DNS-зона, не обслуживаемая внешними DNS-серверами (например, домен Active Directory), укажите внутреннюю DNS-зону в разделе **DNS** → **FORWARD-ЗОНЫ**.

5. Перейдите в **Правила трафика** → **Контент-фильтр** и создайте правило запрета прямого обращения к сайтам по IP-адресу:



6. Пропишите IP-адрес локального интерфейса Ideco NGFW Novum в качестве единственного DNS-сервера в сетевых настройках на всех устройствах, которые требуется защитить.

Пользователи, получающие адреса автоматически через DHCP-сервер Ideco NGFW Novum или подключающиеся по VPN, получают нужные настройки автоматически.

Чтобы исключить некоторые компьютеры из фильтрации, пропишите на них другой внешний DNS-сервер (например, 8.8.8.8) и не включайте **Перехват пользовательских DNS-запросов**.

7. При наличии у Ideco NGFW Novum статического белого IP-адреса привяжите адрес к аккаунту SkyDNS в личном кабинете на сайте SkyDNS (в разделе **Настройки → Сети**).

8. Настройте запрет доступа к сайтам по категориям безопасного поиска и другие сервисы в личном кабинете на сайте SkyDNS.

Документация по настройке и активации сервиса SkyDNS

Документация доступна на сайте сервиса.

По вопросам настройки сервиса обращайтесь в техническую поддержку SkyDNS.

Схема фильтрации веб-трафика при использовании SkyDNS



Полезные ссылки

- **DNS**

Решение проблем

Диагностика и устранение типичных проблем при работе с Ideco NGFW

Доступ в интернет

Решение проблем с доступом в интернет через Ideco NGFW

Перейти >

VPN

Решение проблем с VPN-подключениями в Ideco NGFW

Перейти >

Ошибки при авторизации

Устранение ошибок при авторизации пользователей в Ideco NGFW

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Доступ в интернет

Решение проблем с доступом в интернет через Ideco NGFW

Что делать, если IP попал в черные списки DNSBL

Перейти >

Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Перейти >

Что делать, если не работает интернет

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Что делать, если IP попал в черные списки DNSBL

Если используется белый статический IP-адрес, то попадание IP-адреса в черные списки может означать, что в сети зафиксирована бот-активность, участие в DDoS-атаках либо рассылка спама.

Наличие в черных списках динамического IP-адреса из "домашних" диапазонов IP-адресов провайдеров в целом нормальное явление, т. к. вредоносная активность в таком случае может исходить не из вашей сети.

Порядок действий при попадании в черный список

1. Узнайте причину попадания в DNSBL-список. Часто сервис называет конкретный вирус или сетевой червь и особенности - используемые порты, протоколы. Выполните рекомендации сервиса.

2. Активируйте систему предотвращения вторжений на шлюзе. Проанализируйте логи, наличие обращений к командным центрам ботнетов.

3. Проверьте все компьютеры сети антивирусом. Убедитесь, что антивирусная защита активирована, базы обновлены (как правило, вирусы мешают обновлению баз или работе антивирусного ПО).

4. После лечения зараженных компьютеров отправьте в DNSBL-сервис сообщение с просьбой исключить IP из черного списка.

Ideco NGFW Novum

Наше решение обладает всей функциональностью, обеспечивающей максимальную защиту от спам-ботов, ботнет-клиентов и предотвращение вирусной активности в сети.

До 22 пользователей - решение предоставляется бесплатно. Для 10000 пользователей доступна 40-дневная пробная версия.

Скачать Ideco NGFW Novum

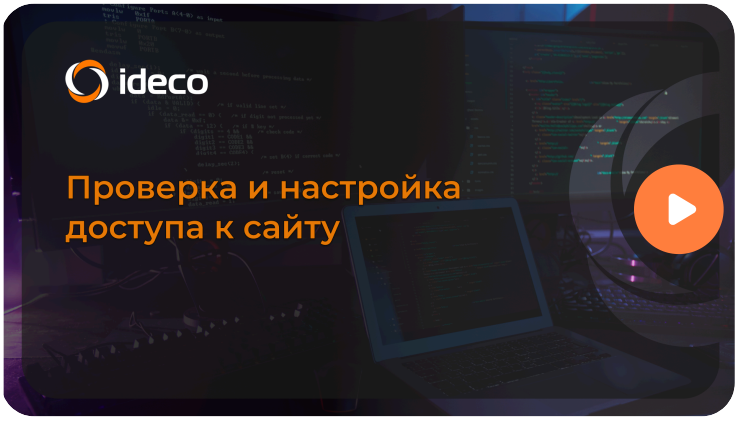
Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Видеоинструкция

Другие видеоинструкции доступны по ссылке.

Смотрите видео на наших страницах в соцсетях.

YouTube



Перед проверкой модулей фильтрации NGFW убедитесь, что на работу сайта не влияют:

- Технические проблемы на самом ресурсе.
- Блокировка со стороны провайдера.
- Некорректная работа устройства пользователя и т.д.

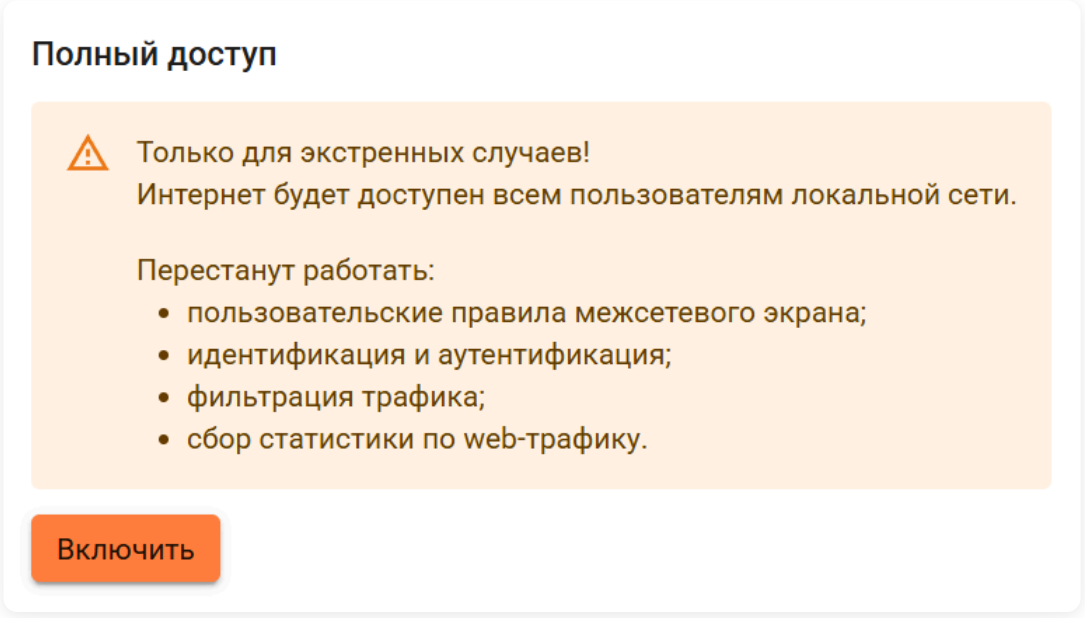
Откройте сайт с устройства вне локальной сети NGFW. Например, со смартфона через мобильный интернет. Если сайт доступен, перейдите в веб-интерфейс NGFW.

Для определения модуля фильтрации, блокирующего сайт, можно проверить логи в разделах Системный журнал. Это может помочь определить причину возникшей проблемы и более точно диагностировать.

Шаг 1. Проверьте, открывается ли сайт в режиме **Полный доступ**

1. Нажмите на в верхней правой части веб-интерфейса NGFW.

2. Нажмите **Включить** в блоке **Полный доступ**:



3. Откройте сайт.

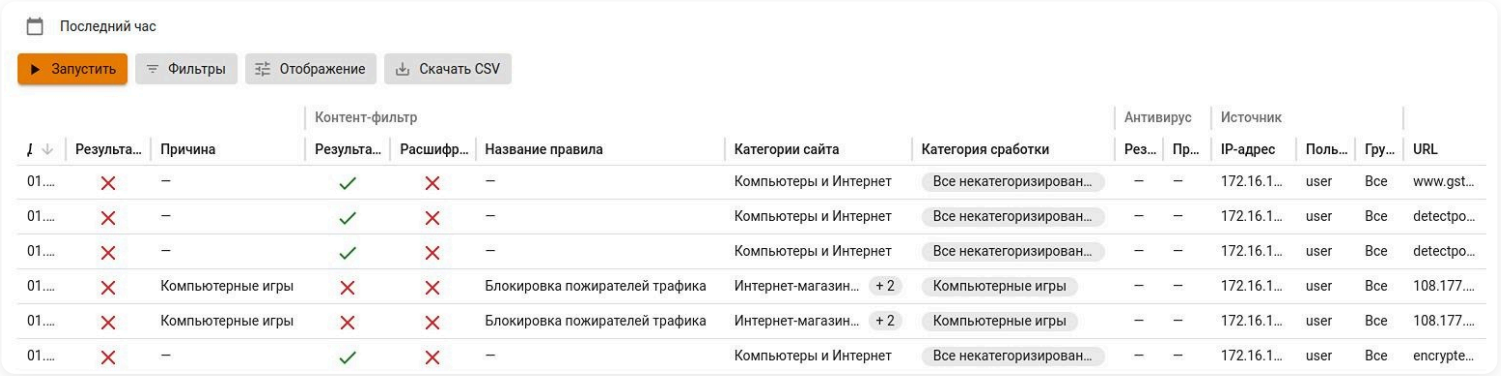
Если сайт не открывается, проверьте, откроется ли сайт на другом устройстве с того же IP-адреса:

- Если не открывается, рекомендуем обратиться к провайдеру. Скорее всего, провайдер блокирует IP-адрес или адрес сайта.
- Если сайт открывается, проверьте настройки устройства пользователя.

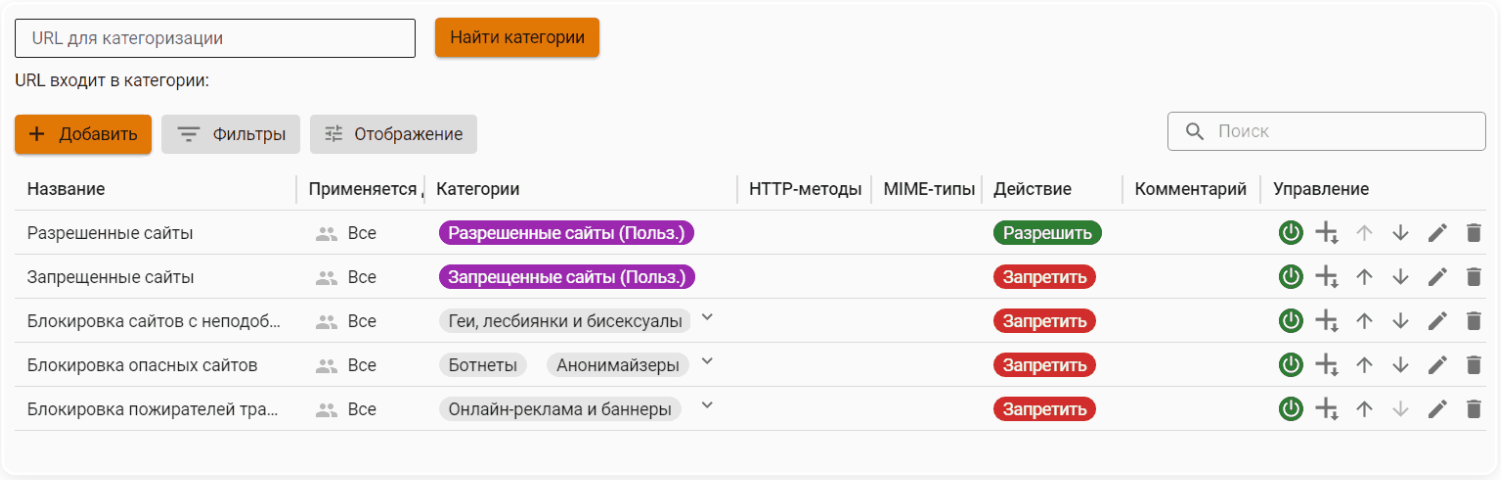
Шаг 2. Проверьте, не блокируется ли сайт правилом Контент-фильтра

1. Откройте сайт с устройства пользователя.

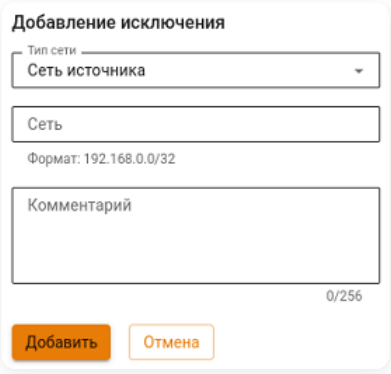
2. В NGFW перейдите в **Отчеты и журналы** → **Веб-трафик** и посмотрите, какое правило блокирует сайт:



3. Для поиска блокирующего правила также можно ввести URL сайта в строку поиска категорий **Контент-фильтра** в **Правила трафика** → **Контент-фильтр** → **Правила**:



4. Если сайт блокируется правилом **Контент-фильтра**, измените настройки **Контент-фильтра** или добавьте сайт в исключения в разделе **Сервисы** → **Прокси** на вкладке **Исключения**:



В **Сервисы** → **Прокси** → **Исключения** рекомендуем добавлять заведомо надежные сервисы.

Добавлять в исключения адреса клиентов вашей сети не рекомендуется, так как в этом случае веб-трафик клиентов не будет фильтроваться правилами **Контент-фильтра** и не будет попадать в отчеты.

Шаг 3. Проверьте, не блокирует ли сайт правило **Межсетевого экрана**

Найдите блокирующее правило одним из способов:

Первый способ. Счетчик срабатываний

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

2. Нажмите на **Отображение** и включите **Счетчик срабатываний**:

3. Откройте сайт с устройства пользователя.

4. Найдите в таблице FORWARD правило с заметным увеличением количества срабатываний.

Второй способ. Тестовое правило

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **FORWARD**.

2. Создайте тестовое правило, разрешающее любой трафик:

3. Правило добавится в конец таблицы. Поместите созданное правило на одну позицию вверх, нажав на кнопку .

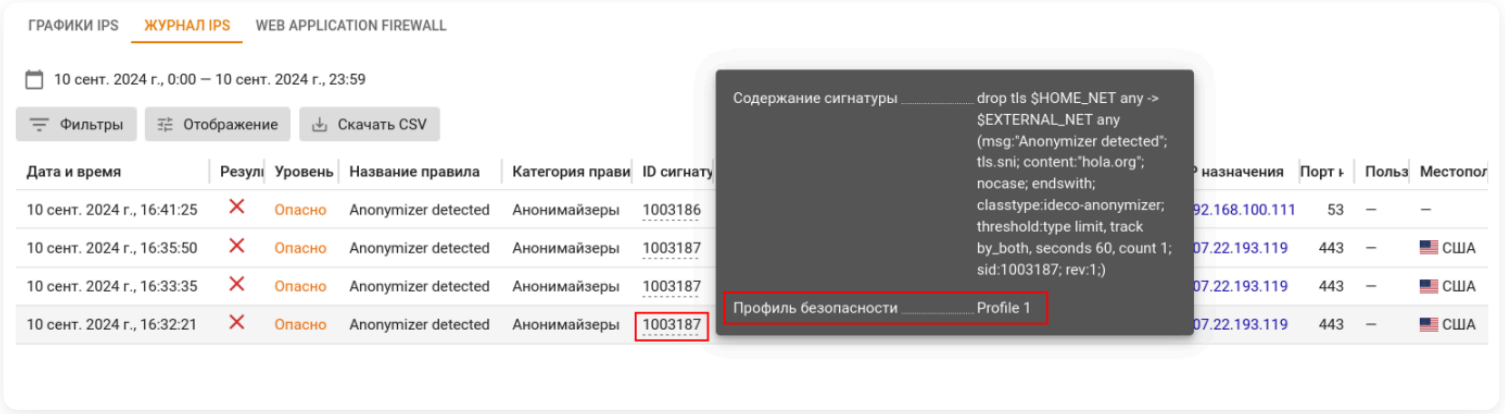
4. Откройте сайт с устройства пользователя.

5. Если сайт не открывается, поднимите тестовое правило на позицию выше и повторно откройте сайт с устройства пользователя. Повторяйте эти действия до тех пор, пока сайт не откроется.

6. Если сайт открывается, блокирующее правило расположено ниже тестового.

Если блокирующее правило направляет трафик через систему Предотвращения вторжений

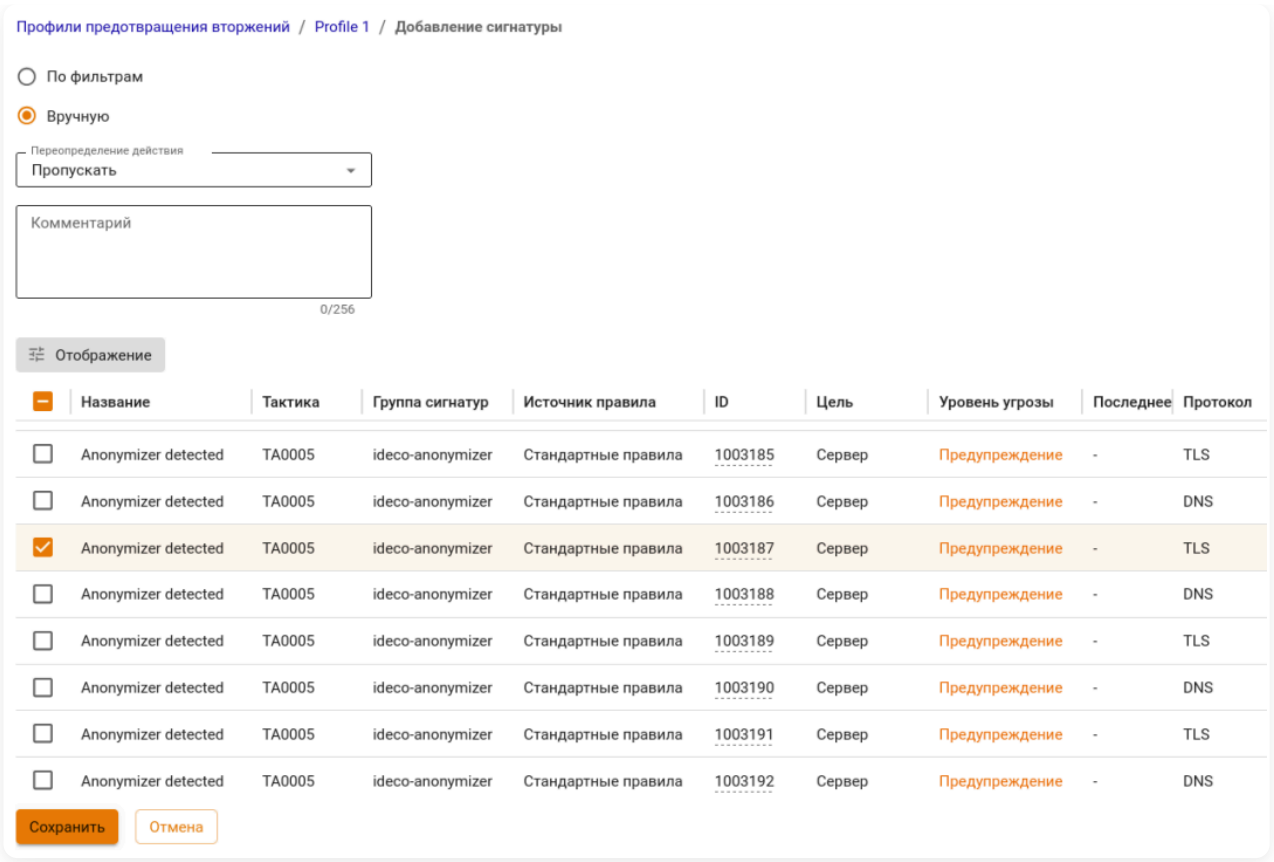
1. Перейдите в раздел **Отчеты и журналы** → **События безопасности** на вкладку **Журнал IPS** и найдите в таблице ID сигнатуры, заблокировавшей сайт, и название профиля, к которому относится сигнатура:



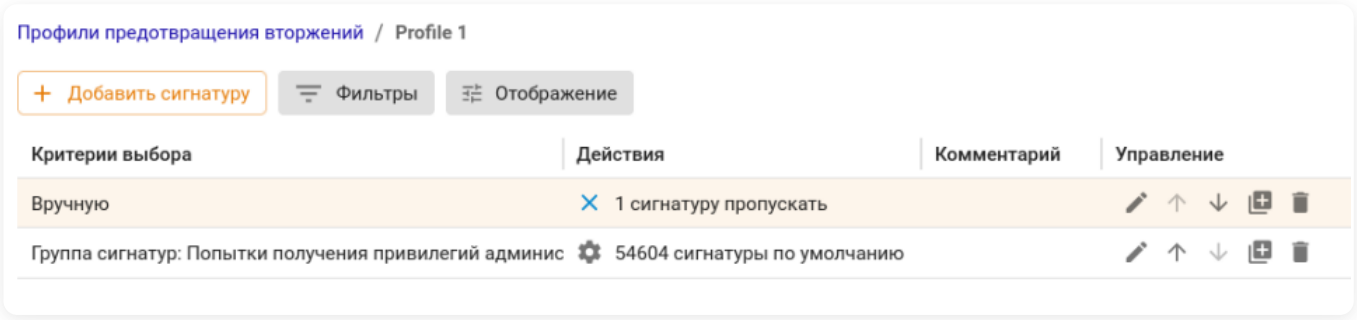
2. Перейдите в **Профили безопасности** → **Предотвращение вторжений**, нажмите на напротив профиля, заблокировавшего сайт, и выберите **Сигнатуры**.

3. Нажмите **Добавить сигнатуру** и выберите способ **Вручную**.

4. В таблице сигнатур по ID найдите сигнатуру (или сигнатуры), заблокировавшую сайт, и переопределите действие для нее:



5. Нажмите **Добавить** и переместите только что созданное правило на самый верх таблицы правил профиля:



Если блокирующее правило направляет трафик через Контроль приложений

1. Перейдите в **Отчеты и журналы** → **Трафик**.

2. В виджете **Топ заблокированных протоколов** найдите протоколы, которые блокируются **Контролем приложений**.

3. Перейдите в **Профили безопасности** → **Контроль приложений** и отредактируйте профиль, разрешив заблокированные протоколы.

Шаг 4. Определите блокируемый домен или IP-адрес (рассмотрим на примере FireFox)

1. Откройте в браузере нужный сайт.

2. Откройте инструменты веб-разработчика одним из способов:

- Нажмите Ctrl+Shift+I.
- Нажмите на ☰ в правом верхнем углу браузера, перейдите в **Другие инструменты** → **Инструменты веб-разработчика**.

3. Выберите вкладку **Сеть**.

4. Обновите страницу.

5. Отсортируйте столбец **Статус** левой кнопкой мыши. Обратите внимание на коды состояния 4xx и 5xx. Часто именно эти запросы блокируются NGFW.

Если решить проблему не удалось

Отправьте в техподдержку:

1. Скриншот ошибки в браузере.

2. Скриншот отсортированных ошибок из браузера, чтобы было видно проблемные домены или IP-адреса.

Что делать, если не работает интернет

Если при первоначальной настройке Ideco NGFW Novum у пользователей отсутствует интернет, выполните шаги для диагностики и решения проблемы.

Шаг 1. Проверьте лицензию

Перейдите в **Управление сервером** → **Лицензия** и проверьте, привязана ли лицензия к серверу.

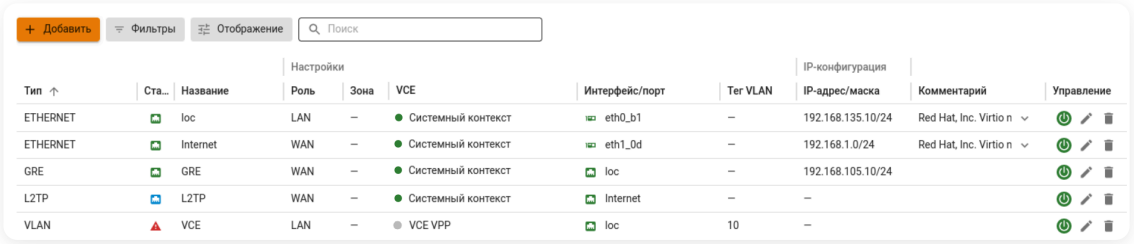
Шаг 2. Проверьте настройки межсетевого экрана

Перейдите в **Правила трафика** → **Межсетевой экран** и отключите в разделах **FORWARD** и **INPUT** правила, запрещающие все.

Шаг 3. Проверьте настройки интерфейсов

Проверьте, правильно ли настроен интерфейс

Перейдите в **Сервисы** → **Сетевые интерфейсы**. Если Ideco NGFW Novum использует выделенный интерфейс для подключения к провайдеру и работает не только как прокси, то проверьте тип подключения и роль:



- Тип подключения должен соответствовать требованиям провайдера.
- Роль должна быть **WAN**.

Проверьте подключение

1. Если провайдер требует VLAN, проверьте настройку VLAN-интерфейса. Убедитесь, что тег указан корректно.

2. Проверьте ICMP-запросы. Выполните команду `ping` до шлюза провайдера. Если отвечает, добавьте шлюз в список адресов для проверки связи.

Проверьте IP-адреса локального интерфейса

Внутренняя сеть должна относиться к приватным диапазонам. Если используются публичные IP-адреса:

- Рекомендуем перейти на приватную адресацию.
- В качестве временного решения создайте правило **SNAT**, где источник - ваша локальная сеть, назначение - внешний интерфейс.

Шаг 4. Включите режим Полный доступ

> Используйте опцию только для диагностики.

В правой верхней части окна Ideco NGFW Novum нажмите на иконку технической поддержки, а затем нажмите **Включить** в блоке **Полный доступ**. После включения:

- Сбор веб-статистики будет отключен.
- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включен автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Межсетевого экрана**.

Цикл обработки трафика в Ideco NGFW Novum описан в статье.

Если интернет появился, то проблема в неверно настроенной авторизации, правилах Межсетевого экрана или маршрутизации.

Шаг 5. Проверьте настройки пользователей

Проверьте авторизацию пользователей

- В Ideco NGFW Novum для авторизации пользователей обязательно требуется сопоставление IP-адреса с пользователем.
- На этапе первоначальной настройки не рекомендуем использовать настройку **Постоянная авторизация пользователя** и **Обнаружение устройств**.
- Пользователи ALD должны быть выгружены в Ideco NGFW Novum.
- Проверьте, что связь установлена с внешними каталогами ALD Pro, Active Directory и RADIUS.

Проверьте тип авторизации

- Если используется **MAC и IP+MAC авторизация**, то на компьютере клиента шлюзом по умолчанию должен быть указан Ideco NGFW Novum. В случае некорректной настройки шлюза, авторизация не будет работать.
- Если используется **Веб-аутентификация**, в поле **Разрешенные объекты** должны быть указаны учетные записи или группы пользователей, которым разрешена авторизация. Пользователю необходимо открыть браузер и попытаться перейти на любой внешний сайт (например, google.com).
- Если используется **Авторизация через журнал безопасности AD**, то:
  - В поле **Разрешенные объекты** должны быть указаны учетные записи или группы пользователей, которым разрешена авторизация.
  - Настройки на стороне контроллера домена.

Не рекомендуем использовать авторизацию через журнал безопасности AD.

Шаг 6. Проверьте работу DNS

Перейдите в **Управление сервером** → **Терминал** и выполните команду `nslookup ya.ru`.

Если разрешение имен работает, то укажите IP-адрес Ideco NGFW Novum в качестве DNS-сервера на рабочих станциях (в одноранговой сети) или в настройках внутреннего DNS-сервера, в разделе серверов перенаправления (в доменной сети).

Если не указать серверы DNS, Ideco NGFW Novum использует корневые серверы DNS, которые может блокировать провайдер. В таких случаях попробуйте указать в качестве DNS `8.8.8.8`, `1.1.1.1` и `77.88.8.8`. Если провайдер блокирует доступ и к ним тоже, используйте серверы провайдера в качестве серверов DNS.



Если не удалось решить проблему, обратитесь в Техническую поддержку

VPN

Решение проблем с VPN-подключениями в Ideco NGFW

Что делать, если не работает VPN-подключение на Windows

Перейти >

Если соединение по IPsec не устанавливается

Перейти >

Особенности маршрутизации и организации доступа (VPN)

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Что делать, если не работает VPN-подключение на Windows

В статье собраны основные методы диагностики для проверки работы VPN-подключения.

Шаг 1. Проверьте параметры VPN-подключения

1. Откройте **Параметры Windows (Win + I)** → **Сеть и Интернет** → **VPN**.

2. Выберите **VPN-подключение** и нажмите **Дополнительные параметры** → **Изменить**.

3. В открывшемся окне проверьте соответствие данным в Ideco NGFW Novum:

IKEv2/IPsec

- **Имя или адрес сервера** - должны соответствовать полю **Домен или IP-адрес** настроек IKEv2/IPsec.
- **Тип VPN** - IKEv2.
- **Тип данных для входа** - должен соответствовать полю **Тип аутентификации**. Если соответствует, проверьте настройки:
  - **Имя пользователя и пароль** - должны соответствовать данным пользователя.
  - **Сертификат** - проверьте, что в Ideco NGFW Novum загружен корневой сертификат Удостоверяющего Центра (УЦ), который выпустил сертификат пользователя. Если сертификат пользователя выпущен промежуточным УЦ, то должна быть загружена полная цепочка доверия: все промежуточные и корневой сертификаты.

SSTP

- **Имя или адрес сервера** - должны соответствовать полям **Домен** и **Порт** настроек SSTP. Проверьте, что в поле указаны данные в формате `example.ru:1443`, а домен не содержит кириллицу и `.local`.
- **Тип VPN** - SSTP.
- **Имя пользователя** и **Пароль** - должны соответствовать данным пользователя.

L2TP/IPsec

- **Имя или адрес сервера** - должны соответствовать домену или IP-адресу настроек L2TP/IPsec.
- **Тип VPN** - L2TP/IPsec с общим ключом.
- **Общий ключ** - должен соответствовать ключу из настроек L2TP/IPsec.
- **Имя пользователя** и **Пароль** - должны соответствовать данным пользователя.



Не используйте кириллические логины, а также не указывайте в качестве логина IP-адрес.

4. Проверьте, что на компьютер пользователя корректно установлен корневой сертификат.

5. Проверьте настройки VPN-подключения на стороне Ideco NGFW Novum:

- В разделе **Пользователи** → **VPN-подключения** модуль VPN-подключения активен.
- На вкладке **Пользователи** → **VPN-подключения** → **Основное** настроено и активно необходимое VPN-подключение.
- На вкладке **Пользователи** → **VPN-подключения** → **Доступ по VPN** добавлено правило, разрешающее подключение пользователю.

Шаг 2. Проверьте доступность VPN-сервера

1. Нажмите **Win + R**, введите `cmd` и нажмите **Enter**.

2. В командной строке выполните команду `ping <адрес_сервера>`. Например, `ping vpn.example.com`.

3. Проверьте ответ:

- Если есть ответы со временем отклика - сервер доступен. Переходите к следующему шагу.
- Если отображается сообщение `Превышен интервал ожидания` - есть проблема с сетевым путем или адресом.

4. Если ping не проходит, но вы уверены в правильности адреса, выполните альтернативную проверку с помощью команды `tracert <адрес_сервера>`. Она покажет, на каком участке сети обрывается связь.

Шаг 3. Проверьте информацию из журнала событий

1. Нажмите **Win + R**, введите `eventvwr.msc` и нажмите **Enter**, чтобы открыть журнал событий.

2. В левой колонке перейдите к **Журналы Windows** → **Система**.

3. В правой части окна нажмите **Фильтр текущего журнала**.

4. В поле **Источник** выберите **RasClient**.

5. Изучите события с уровнем **Ошибка** и **Предупреждение**. Информация из вкладок **Общие** и **Подробности** поможет определить причину и найти способ устранения.

Шаг 4. Сбросьте и перезагрузите сетевые компоненты Windows

Запустите командную строку от имени администратора и выполните команды по порядку, дожидаясь завершения каждой команды:

1. `netsh winsock reset` - сбрасывает каталог сетевых сокетов.

2. `netsh int ip reset` - сбрасывает настройки TCP/IP.

3. `ipconfig /flushdns` - очищает кэш DNS-клиента.

> Дальнейшие команды предназначены для сетей, где IP-адрес назначается автоматически (DHCP). Если на компьютере настроен статический IP-адрес, выполнение этих команд приведет к потере сетевого подключения, и интернет не восстановится автоматически.

4. `ipconfig /release` - освобождает текущий IP-адрес.

5. `ipconfig /renew` - запрашивает новый IP-адрес.

После выполнения команд перезагрузите компьютер.

Шаг 5. Проверьте состояние необходимых служб Windows

1. Нажмите **Win + R**, введите `services.msc` и нажмите **Enter**.

2. Найдите следующие службы и убедитесь, что тип запуска этих служб - **Автоматически**, а состояние - **Выполняется**:

- `Диспетчер подключений удаленного доступа` (Remote Access Connection Manager) - отвечает за управление подключениями удаленного доступа, включая VPN-подключения. Без этой службы Windows не сможет установить туннель.
- `Служба сетевых подключений` (Network Connections) - управляет объектами в папке **Сетевые подключения**, отвечает за отображение сетевых адаптеров (включая VPN-адаптеры) в интерфейсе Windows. Если служба остановлена, VPN-профиль не будет отображаться и его не получится создать.
- `Служба списка сетей` (Network List Service) - определяет характеристики сетевого подключения, собирает и хранит информацию о сетях.

3. Если служба остановлена, нажмите на ее название правой кнопкой мыши и выберите **Запустить**. Если тип запуска не **Автоматически**, дважды кликните по службе и в выпадающем списке **Тип запуска** выберите **Автоматически**. Нажмите **Применить**, затем **Запустить**.

4. Если ключевые службы отсутствуют или не запускаются, то системные компоненты Windows повреждены. Для восстановления выполните проверку целостности системных файлов (сначала `sfc /scannow`, затем `DISM /Online /Cleanup-Image /RestoreHealth` в командной строке от имени администратора) и перезагрузите компьютер.

5. Если это не помогает, используйте точку восстановления системы или другие средства восстановления Windows, так как без этих служб создание и работа VPN-подключения невозможны.

Шаг 6. Проверьте настройки брандмауэра и антивируса

Брандмауэр Windows

1. Временно отключите брандмауэр Windows. Для этого откройте **Параметры Windows (Win + I)** → **Конфиденциальность и защита** → **Безопасность Windows** → **Брандмауэр и защита сети**.

2. Отключите брандмауэр для частных и публичных сетей.

3. Установите VPN-соединение.

Антивирус

1. Найдите иконку антивируса в системном трее.

2. Перейдите в настройки, временно отключите антивирус и его функции сетевого экрана.

3. Установите VPN-соединение.

Шаг 7. Пересоздайте VPN-подключение

1. Откройте раздел **Параметры Windows (Win + I)** → **Сеть и Интернет** → **VPN**.

2. Выберите подключение и нажмите **Удалить**.

3. Нажмите **Добавить VPN-подключение** и создайте новое подключение.

4. Заполните все поля. Рекомендуем заполнять поля вручную и проверить раскладку клавиатуры.

5. Установите VPN-соединение.

Шаг 8. Проверьте драйверы сетевого адаптера

1. Нажмите **Win + X** и выберите **Диспетчер устройств**.

2. Раскройте **Сетевые адаптеры**.

3. Найдите основной адаптер и выберите **Обновить драйвер** → **Автоматический поиск обновленных драйверов**.

4. Если система найдет новый драйвер - установите его и перезагрузите компьютер.

Шаг 9. Если ничего не помогло

Если ни один из вариантов решения не помог, обратитесь в Техническую поддержку.

Если соединение по IPsec не устанавливается

1. Перезагрузите сервисы двух NGFW, выполнив команду `systemctl restart ideco-ipsec-backend.service && systemctl restart strongswan.service`.

2. Проверьте работоспособность перезагруженных сервисов:

- выполните команду `systemctl status strongswan.service`;
- перейдите в **Сервисы** → **IPsec**.

Если при переходе в раздел **IPsec** и выполнении команды возникли ошибки, то перейдите к пункту 3.

3. Пересоздайте соединение из веб-интерфейса по инструкции Настройка подключения между Филиалом и Главным офисом.

Если пересоздание соединения не помогло, перейдите к пункту 4.

4. Проверьте, ходит ли трафик по портам 500 и 4500, выполнив команды `tcpdump -i any port 4500 -ttttnnn` и `tcpdump -i any port 500 -ttttnnn` в головном офисе и филиале.

Если трафик уходит с одного NGFW и приходит на второй NGFW, то обратитесь в техническую поддержку.

Если трафик уходит с одного NGFW и не приходит на второй NGFW, обратитесь к провайдеру.

Особенности маршрутизации и организации доступа

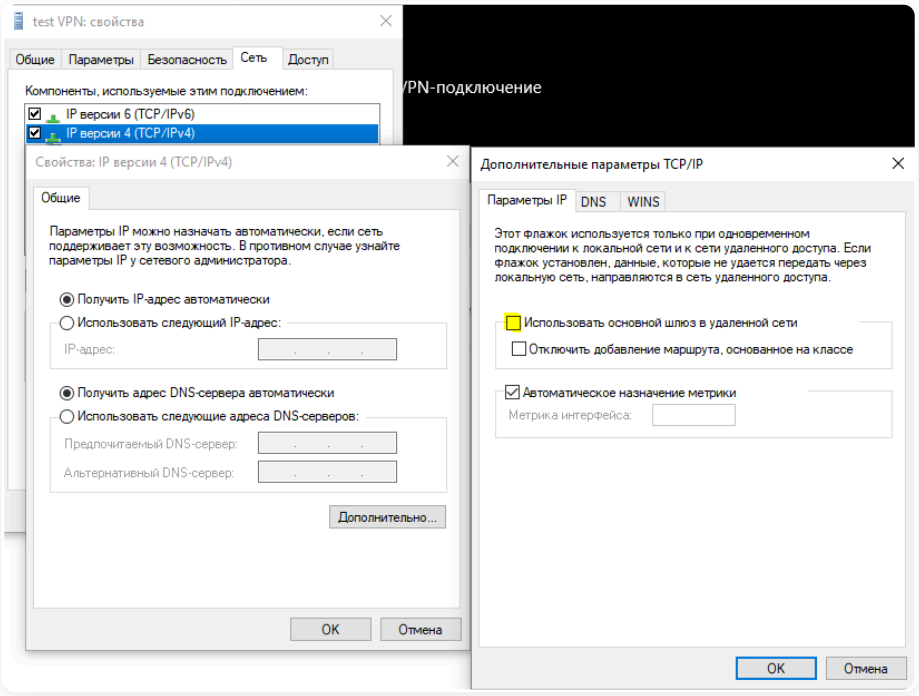
Классический контекст | Высокопроизводительный контекст

В статье рассматриваются потенциальные проблемы, связанные с доступом к ресурсам локальной сети через VPN, и предлагаются решения, такие как настройка маршрутов, исключение определенных сетей в антивирусном ПО и создание правил SNAT на NGFW Novum.

Организация доступа по VPN только к ресурсам локальной сети

Для организации доступа выполните действия:

1. В **Сеть** → **IP версии 4** → **Дополнительно** → **Параметры IP** уберите флаг **Использовать основной шлюз в удаленной сети**:



Особенности VPN-соединения с доступом только к ресурсам локальной сети

При выборе типа передачи маршрутов **Отправлять только указанные сети** маршрут до VPN-сервера и DNS-сервера построен не будет.

Если в NGFW Novum добавить передачу IP-адреса VPN-сервера NGFW Novum (DNS), то маршрут восстановится, а домен будет преобразовываться со следующими особенностями:

- Таблица с включенным шлюзом:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.5      5
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255          On-link         127.0.0.1    331
    192.168.100.2  255.255.255.255          On-link        10.200.0.5      5
  192.168.100.130  255.255.255.255          On-link        10.200.0.5      5
    192.168.122.0    255.255.255.0          On-link    192.168.122.10    281
   192.168.122.10  255.255.255.255          On-link    192.168.122.10    281
  192.168.122.255  255.255.255.255          On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0          On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0          On-link    192.168.122.10    281
  255.255.255.255  255.255.255.255          On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255          On-link    192.168.122.10    281
===========================================================================
```

- Таблица с отключенным шлюзом:

- Таблица с отключенным шлюзом и добавленной публикацией IP NGFW Novum:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255          On-link        10.200.0.4     26
       10.200.0.4  255.255.255.255          On-link        10.200.0.4    281
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    331
```

Маршрут до сервера (в примере - 10.200.0.1) добавляется, но имеет более низкий приоритет, чем маршрут по-умолчанию. Соответственно запросы обрабатываются с задержкой и не обрабатываются при перехвате маршрутом по-умолчанию.

Рекомендуем вручную указать маршрут до DNS NGFW Novum, либо добавить маршрут в список публикуемых маршрутов на стороне NGFW Novum. Также можно использовать сторонний DNS-сервер.
2. Пропишите маршрут до корпоративной сети. В Windows 8, 8.1, 10 автоматически создается маршрут на основе класса, в зависимости от адреса, полученного по VPN. Для IPsec-IKEv2 можно настроить автоматическое получение маршрута.

Пример маршрута: если корпоративная сеть имеет адрес `172.16.0.0/16`, а сеть для VPN-подключений, настроенная на Ideco NGFW Novum, имеет адрес `10.128.0.0/16`:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1
```

Маршрут может не работать, когда есть пинг до интерфейса `10.128.0.1`, но нет пинга до хостов в локальной сети. В этом случае при создании маршрута нужно указать номер интерфейса VPN-подключения:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn
```

- `nn` - номер интерфейса VPN-подключения, посмотреть который можно при активном VPN-подключении в выводе в консоли команды `route print` раздел "Список интерфейсов".

Не удается получить доступ к компьютерам в локальной сети Ideco NGFW Novum

Для получения доступа к компьютерам в локальной сети Ideco NGFW Novum убедитесь, что:

1. Локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. В противном случае доступ к сети организации будет невозможен (трафик будет идти через физический интерфейс, а не через VPN).

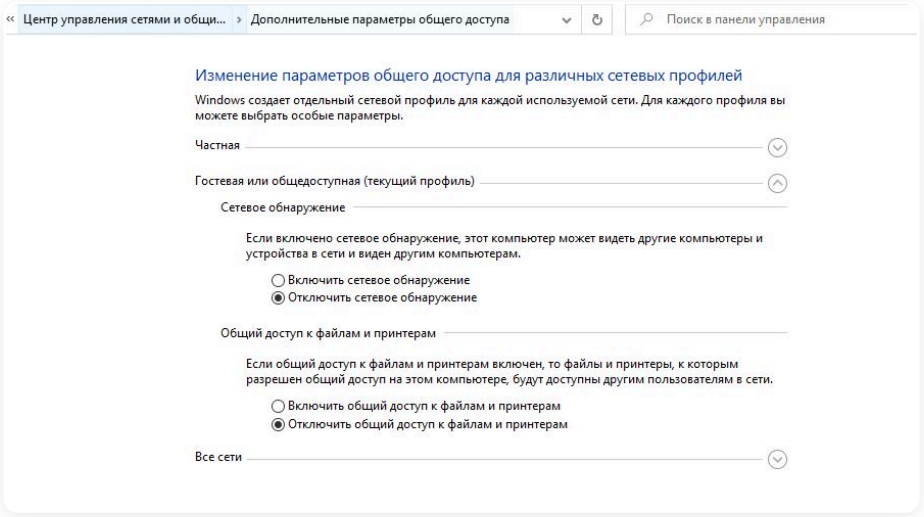
2. На компьютерах локальной сети основным шлюзом должен быть Ideco NGFW Novum. Если это не так, то вручную необходимо прописать соответствующий маршрут, чтобы сетевые пакеты шли на Ideco NGFW Novum для VPN-сети. **Например**:

```
route -p add 10.128.0.0 mask 255.255.0.0 10.1.1.1
```

- `10.128.0.0/16` - адрес VPN-сети Ideco NGFW Novum (настраивается в разделе **Пользователи** → **VPN-подключения**).
- `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW Novum.

3. На Ideco NGFW Novum в разделе **Межсетевой экран** → **FORWARD** нет запрещающих правил.

4. Компьютеры и серверы на Windows не ограничивают доступ к сетевым папкам с помощью правил настроек профилей сети (как на стороне подключающегося по VPN компьютера, так и на стороне компьютеров и серверов локальной сети):



Получение доступа к файлам и принтерам для профиля "Все сети" и "Частные сети"

Для получения доступа выполните действия:

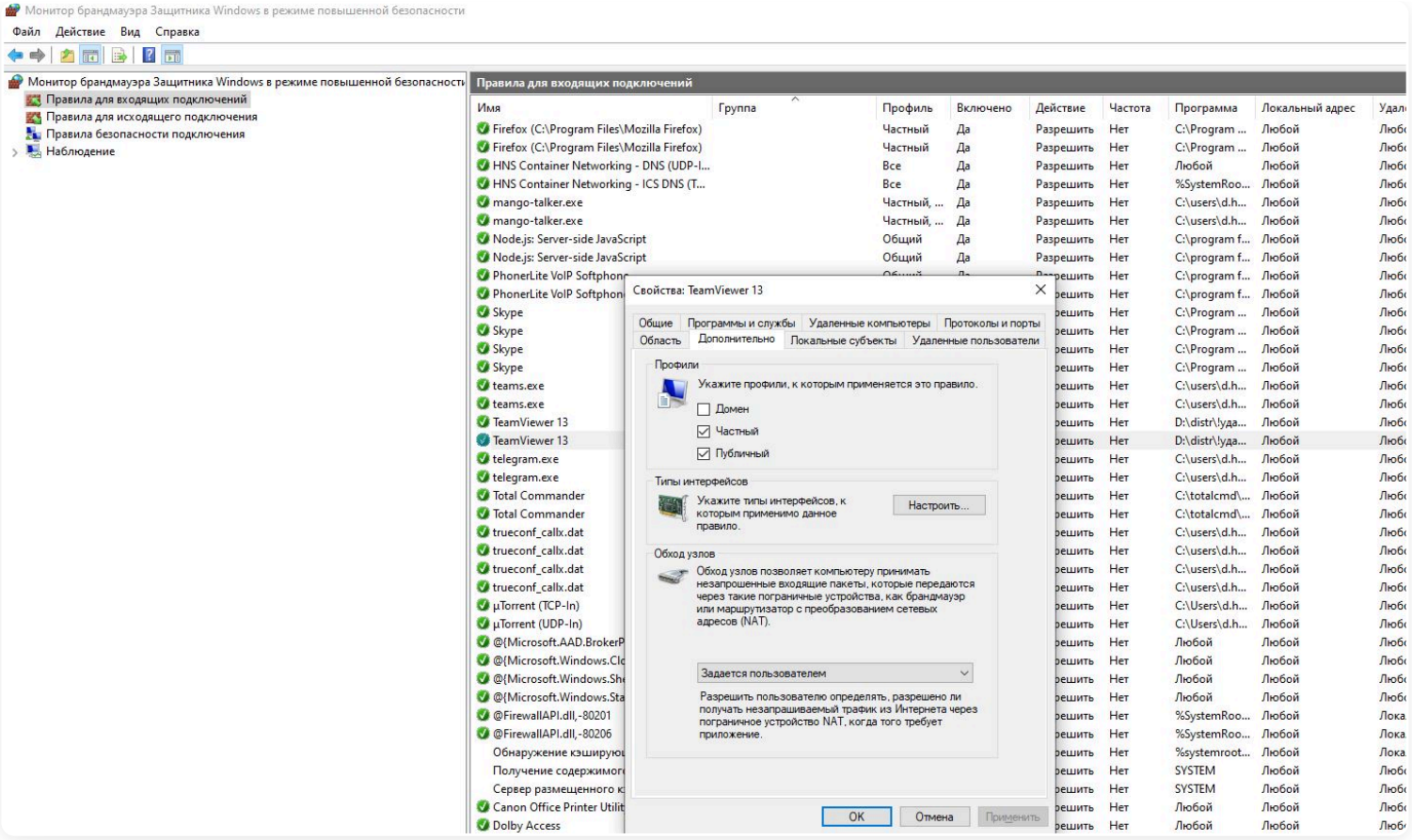
1. Перейдите в PowerShell (запустите PowerShell с повышением прав до администратора).

2. Выполните команду: `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`.

Возможные проблемы:

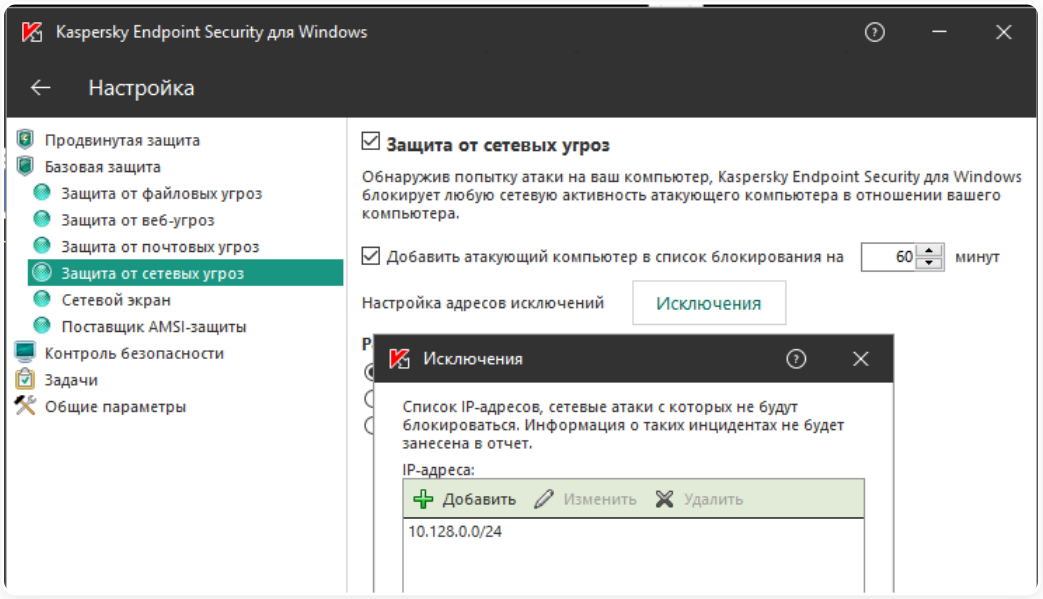
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей.

  Проверьте это в настройках входящих и исходящих подключений (необходимо разрешить доступ из частных и локальных сетей):



- Антивирусное ПО на компьютере может блокировать доступ из нелокальных сетей. Либо блокировать доступ конкретных программ.

  Например, для **Kaspersky Endpoint Security** нужно добавить сеть для VPN-подключений (по умолчанию `10.128.0.0/16`) в исключения:



Получение доступа к локальной сети Филиала

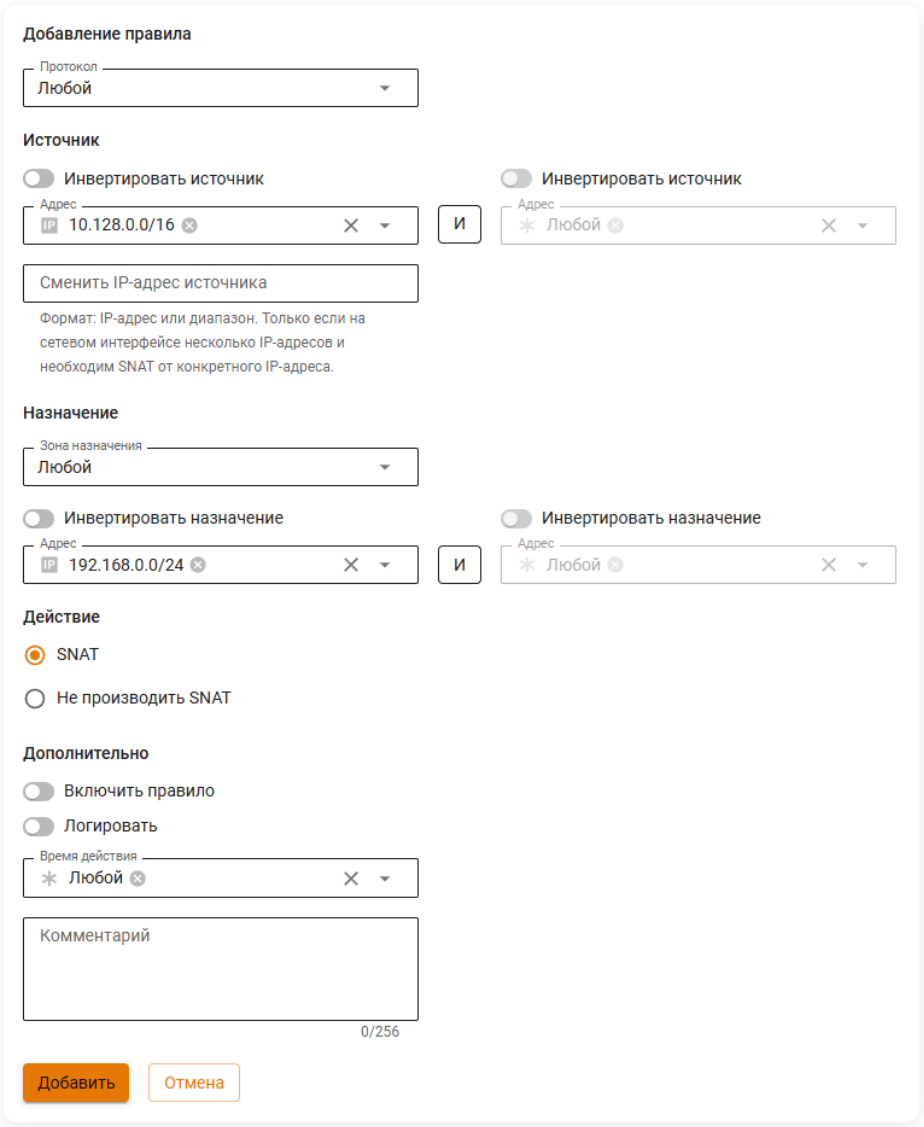
Чтобы обеспечить доступ, убедитесь, что VPN-сети обоих NGFW Novum не пересекаются. Затем проверьте настройки основного NGFW Novum, следуя инструкциям, описанным в статье.

Получение доступа к хостам локальной сети, если за NGFW Novum есть маршрутизатор, выступающий в качестве ядра локальной сети

Чтобы обеспечить доступ, нужно настроить на роутере маршрут от нужной локальной сети до VPN-сети. Для настройки маршрута на роутере укажите в качестве назначения VPN-сеть (`10.128.0.0/16`), в качестве шлюза - NGFW Novum (`172.16.0.1`).

Если настроить на роутере маршрут невозможно, можно создать на NGFW Novum SNAT-правило:

1. Перейдите в **Правила трафика** → **Межсетевой экран** → **SNAT**, нажмите **Добавить** и укажите параметры:



- **Источник** - VPN-сеть (`10.128.0.0/16`).
- **Назначение** - сеть за роутером, к которой требуется получить доступ из VPN-сети (`192.168.0.0/24`).

3. Нажмите **Добавить**.

В этом случае при отправке пакетов на роутер NGFW Novum подменит IP-адрес источника своим. За счет этого роутер направит ответ от хоста в локальной сети на NGFW Novum, который затем перенаправит его в VPN-сеть.

У хостов из локальной сети `192.168.0.0/24` не будет доступа к VPN-сети `10.128.0.0/16`.

Полезные ссылки

- **Как избежать проблем с подключением VPN-клиентов при нескольких серверах**

Ошибки при авторизации

Решение проблем с авторизацией в Ideco NGFW

Ошибка при авторизации "The browser is outdated"

Перейти >

Ошибка 400 Bad Request Request Header Or Cookie Too Large при авторизации в браузерах

Перейти >

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Ошибка при авторизации "The browser is outdated"

Если используется браузер, который не поддерживает NGFW, при авторизации появится ошибка **Your browser is outdated. This version of browser is unsecure and unsupported by modern web-technologies. Please, install the latest version of one of the listed browsers**.

Поддерживаемые версии браузеров:

- Google Chrome версия >= 109;
- Firefox версия >= 115;
- Safari версия >= 15.4.

Рекомендуем обновить браузер до минимально поддерживаемой версии.

Для продолжения авторизации несмотря на риски потребуется нажать **I understand the risks and wish to continue**.

Ошибка 400 Bad Request Request Header Or Cookie Too Large при авторизации в браузерах

Ошибка возникает на Windows 7, 8, 11, Windows Server 2008 R2, 2012, 2022 из-за большого количества групп безопасности и неспособности токена Kerberos вместить все данные.

По умолчанию размер токена Kerberos:

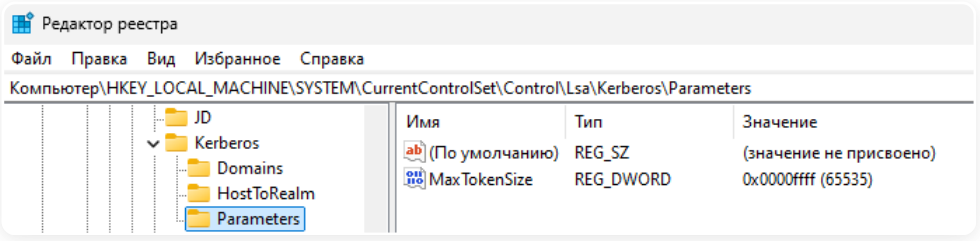
- **Windows 7 и Windows Server 2008R2** - 12000 байт.
- **Windows 8 и Windows Server 2012 (включая Windows Server 2022 и Windows 11)** - 48000 байт.

Для решения проблемы нужно увеличить размер токена на пользовательской ОС. Для этого:

1. Откройте редактор реестра и перейдите в раздел **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters**.

2. Создайте новый параметр типа **DWORD (32-bit)** с именем **MaxTokenSize**.

3. Задайте максимальное значение размера буфера - 65535 байт в десятичной системе счисления:



4. Перезагрузите компьютер.

Чтобы узнать текущее значение параметра **MaxTokenSize**, выполните следующую команду в **PowerShell**:

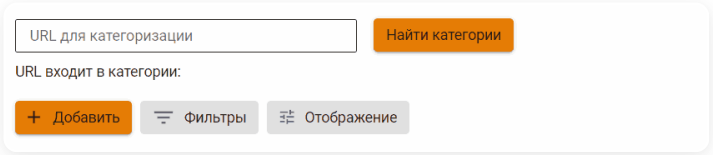
```
Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters|select MaxTokenSize
```

Что делать, если не действуют правила Контент-фильтра

Если правила контентной фильтрации не действуют, проверьте следующие параметры в настройках:

- IP-адрес пользователя должен соответствовать его адресу в авторизации (раздел **Мониторинг** → **Сессии пользователей**), пользователь должен находиться в группе, на которую назначено правило.
- IP-адрес пользователя и ресурса, к которому обращается, не должен входить в исключения прокси-сервера.
- В браузере и на компьютере пользователя не должны использоваться функции или плагины VPN, не прописаны сторонние прокси-серверы.

Дополнительно проверьте настройки категоризации ресурса, к которому обращаетесь, в поле **URL для категоризации** на вкладке **Правила**:



Если сайт неправильно категоризирован, поменяйте категорию на вкладке Переопределение категорий или воспользуйтесь формой обратной связи SkyDNS.

Как восстановить доступ к Ideco NGFW Novum

Для этого нужно выполнить следующие действия:

1. Перезагрузите сервер. При появлении меню загрузчика GRUB с выбором ядра Linux для загрузки системы нажмите англоязычную клавишу **E** на клавиатуре:

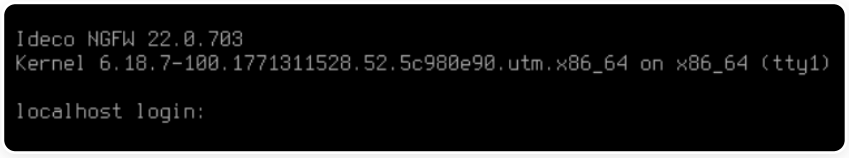


2. Откроется окно параметров ядра с возможностью редактирования. Переместите указатель стрелками на клавиатуре вправо до слова `quiet` и допишите текст `p=1`:



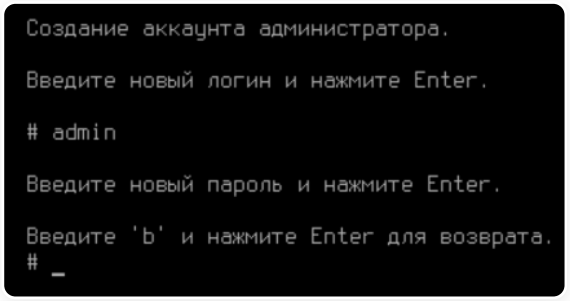
3. Нажмите `Enter`.

4. Не нажимайте никаких клавиш при появлении окна:



Дождитесь появления локальной консоли.

5. После повторной загрузки системы появится окно создания аккаунта администратора. Задайте новый логин и пароль администратора:



Требования к логину и паролю

Логин:

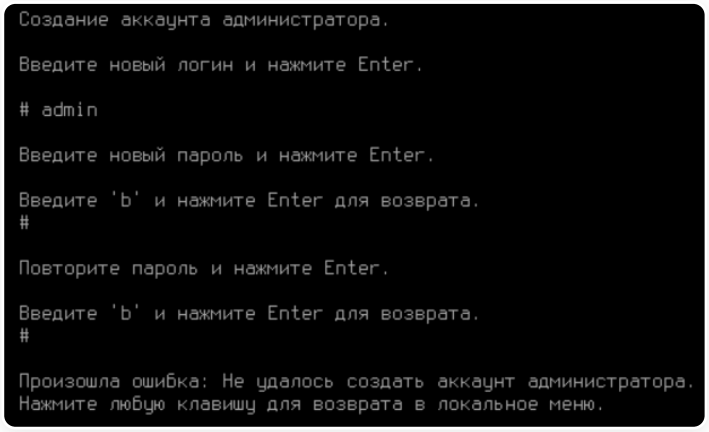
- Не должен начинаться с цифры.
- Не должен содержать специальных и пробельных символов, кроме дефиса `-`.
- **Длина логина** - от 1 до 31 символа включительно.

Пароль:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.
- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

Если при создании нового логина администратора логин будет совпадать с предыдущим логином, то будет выведена ошибка. Создайте имя администратора, отличное от предыдущего.

Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;`, `^[[4~;` и т.д.



Как изменить дату и время в Ideco NGFW Novum

Если дата и время в Ideco NGFW Novum установлены неверно, сервер не сможет получить лицензию. Для установки корректных значений:

1. Перейдите в раздел **Управление сервером** → **Терминал**.

2. Остановите службу `chronyd`, которая автоматически синхронизирует системные часы с NTP-серверами:

```
systemctl stop chronyd
```



Без отключения службы изменить дату и время не получится.

3. Убедитесь, что служба остановлена:

```
systemctl status chronyd
```

В строке `Active` должно отображаться значение `inactive (dead)`.

4. Установите корректную дату и время в формате `ГГГГ-ММ-ДД ЧЧ:ММ:СС`:

```
timedatectl set-time "2026-04-22 12:33:14"
```

5. Проверьте, что изменения применились:

```
timedatectl
```

6. Выполните регистрацию сервера и привяжите лицензию. Подробнее в статье.

7. После регистрации сервера вернитесь в **Управление сервером** → **Терминал** и запустите службу `chronyd`, чтобы восстановить автоматическую синхронизацию времени:

```
systemctl start chronyd
```

8. Убедитесь, что служба успешно запустилась:

```
systemctl status chronyd
```

В строке `Active` должно отображаться значение `active (running)`.

При необходимости добавьте адрес NTP-сервера. Подробнее в статье.

Новое в документации

Май 2026

Практические руководства

Резервирование трех WAN-каналов через SD-WAN

Настройка Ideco NGFW Novum

Настройка высокопроизводительного контекста

Аутентификация по сертификату

Диагностика работы Ideco Client с помощью логирования

Управление Ideco Client через CLI

DNS-запросы

EIGRP

Next hop

Профили next hop

Профили IP SLA

Объекты

05.06.26

Межсетевой экран

05.06.26

Настройка фильтрации трафика

05.06.26

Особенности создания профилей

05.06.26

Пример создания иерархической структуры

05.06.26

Профили предотвращения вторжений

05.06.26

Терминал

05.06.26

Прокси

05.06.26

Полный цикл обработки трафика в Ideco NGFW Novum

05.06.26

Syslog

05.06.26

Установка и настройка Ideco Client на Windows

05.06.26

Кластеризация

05.06.26

Настройка высокопроизводительного контекста

05.06.26

Сетевые интерфейсы

05.06.26

Интерфейсы

05.06.26

Аутентификация

05.06.26

Настройка SSO-аутентификации

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

05.06.26

Сертификаты

04.06.26

Настройка Device VPN

04.06.26

Инструкция по созданию подключения в macOS

03.06.26

VPN-подключения

29.05.26

Миграция настроек Device VPN

29.05.26

Резервирование трех WAN-каналов через SD-WAN

29.05.26

Ideco NGFW Novum 22.3.52

29.05.26

Доступ из внешних сетей без NAT

28.05.26

Управление Ideco Client через CLI

28.05.26

Ограничение скорости

28.05.26

События безопасности

21.05.26

Active Directory/Samba DC

21.05.26

EIGRP

20.05.26

DNS-запросы

18.05.26

Ideco Client

16.05.26

Блокировки WAF

16.05.26

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

Ideco NGFW Novum 22.1.108

15.05.26

Аутентификация по сертификату

13.05.26

Продолжая использовать сайт, вы соглашаетесь на предоставление cookie и сбор данных через сервис Яндекс.Метрика. Мы используем данные в обобщенном виде для повышения удобства использования сайта, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.