Об Ideco NGFW

> Межсетевой экран Ideco NGFW - современное программное решение для защиты сетевого периметра, которое позволяет сделать доступ в интернет абсолютно управляемым, безопасным и надежным.

Возможности Ideco NGFW:

- Межсетевой экран
- Система предотвращения вторжений
- Контент-фильтр
- Контроль приложений
- Антивирусная и антиспам-проверка трафика
- Защита от ботнетов, фишинга и шпионского ПО
- VPN site-to-site (GRE, IPSec, ГОСТ VPN) и client-to-site (IKEv2/IPSec, L2TP/IPSec, SSTP, Wireguard) с 2FA
- Логирование действий администратора
- Управление через Центральную консоль
- 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, которые позволяют создать надежный барьер для защиты локальной сети от современных угроз безопасности.

Техническое описание Ideco NGFW доступно по ссылке.

Online-документация актуальна для версий Ideco UTM начиная с 7.9 и Ideco NGFW с 16.0 (выбрать нужную версию можно в верхней части меню).

Скачать Ideco NGFW можно в личном кабинете.

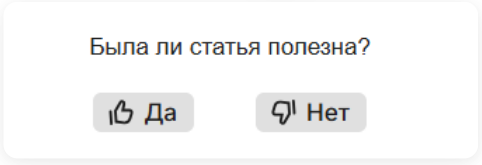
Видеодокументация доступна на YouTube и Rutube.

Обратная связь

Мы постоянно совершенствуем нашу документацию и всегда рады вашим отзывам.

Как оставить отзыв:

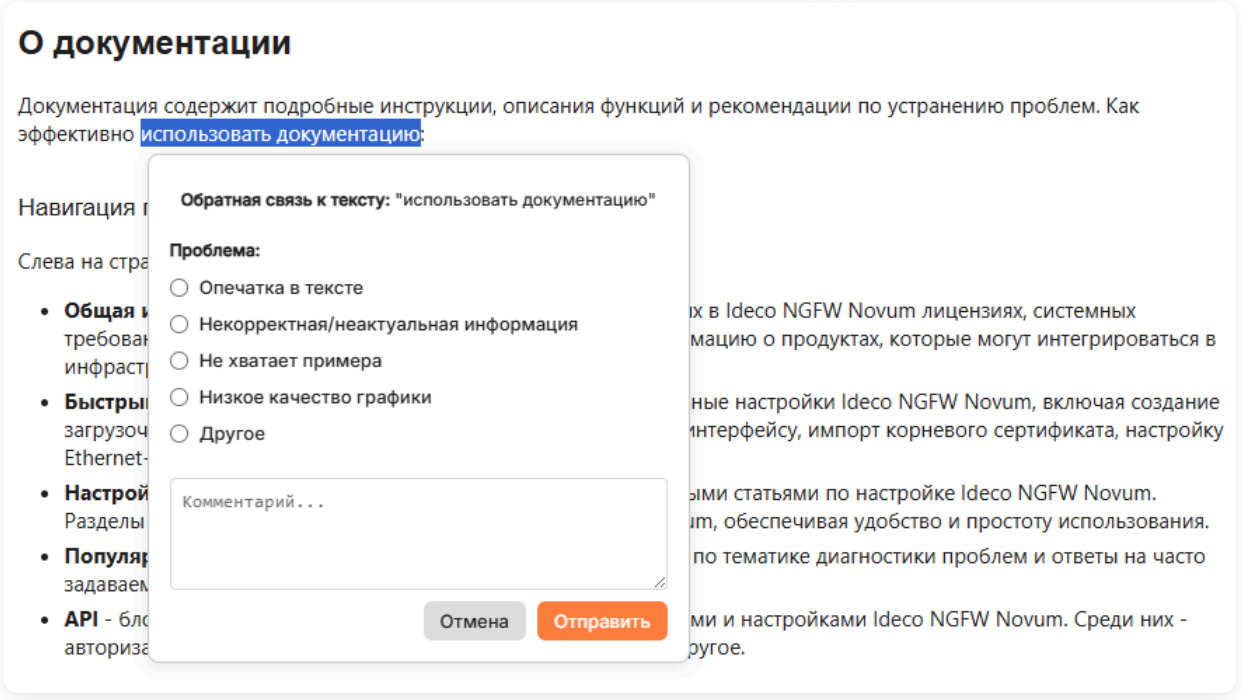
- Поставить реакцию в правом верхнем углу или в конце любой статьи:



- Написать комментарий к фрагменту текста внутри статьи.

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 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 есть три основные характеристики:

- **Количество пользователей Ideco NGFW** - авторизованные пользователи локальной сети или подключенные по VPN пользователи, трафик которых проверяется и контролируется шлюзом.
- **Редакция Ideco NGFW (вид лицензии)** - набор доступных к использованию модулей в системе и особенности их работы.
- **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 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**.

Виды лицензий

В Ideco NGFW доступны лицензии:

Enterprise

Enterprise - коммерческая лицензия.

- ☑ Бессрочное право на использование Ideco NGFW
- ☑ Включает в себя годовую подписку **Security Update**
- ☑ Лицензирование по числу активных пользователей или по количеству ядер виртуальной машины
- ☑ 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.
- 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:

- **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.

> ℹ Для использования кластера Ideco NGFW потребуется дополнительная лицензия на кластеризацию.

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:

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокированы FORWARD- и INPUT-трафик. Кроме доступа до 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 **Свободные лицензии**.

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

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокированы FORWARD- и INPUT-трафик. Кроме доступа до 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.

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:

- В личном кабинете MY.IDECO. 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.

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

Системные требования

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

- 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 четвертого класса защиты используется только ПАК.

Производительность платформы

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

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

- Задействованные компоненты NGFW (**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 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 на аппаратной платформе.

Программно-аппаратный комплекс

Работа Ideco NGFW 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 MX2/LX/LX+ - номер записи 10465633, ссылка.
- Для Ideco NGFW 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).

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	- 16 ГБ (16-64 ГБ в зависимости от количества пользователей).
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 (Compatability Support Module).
Дополнительно	- Монитор и клавиатура (не требуется, если используется IPMI).

На каждый VCE требуется минимум:

- Процессор: 2 ядра.
- Оперативная память: 8 ГБ.

- 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. Встроенные в материнские платы программные и полуаппаратные RAID-контроллеры 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 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 4K 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 (Compatability Support Module).
Дополнительно	- Внутренние часы виртуальной машины должны быть настроены на хранение времени во временной зоне UTC.

На каждый VCE требуется минимум:

- Процессор: 2 ядра.
- Оперативная память: 8 ГБ.
- 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

> Условия и график работы технической поддержки компании "Айдеко", доступной по подписке, а также способы обращения и необходимые данные для помощи.

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 почитать на сайте компании "Айдеко".

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
Интерактивный онлайн-чат со специалистом технической поддержки	https://my.ideco.ru/, https://ideco.ru/, веб-интерфейс Ideco NGFW

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.

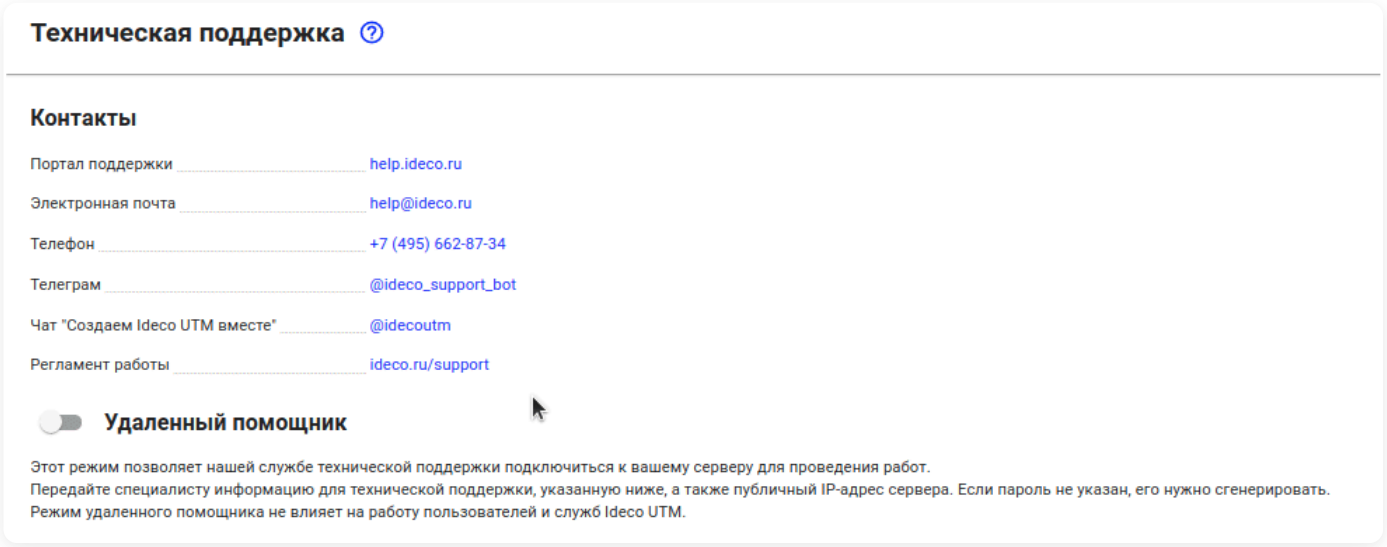
При обращении необходимо предоставить следующую информацию: название организации, ваши контактные данные, номер лицензии.

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 файрвола. При этом становится доступно подключение по SSH из локальных и внешних сетей.



Включение режима удаленного помощника из веб-интерфейса

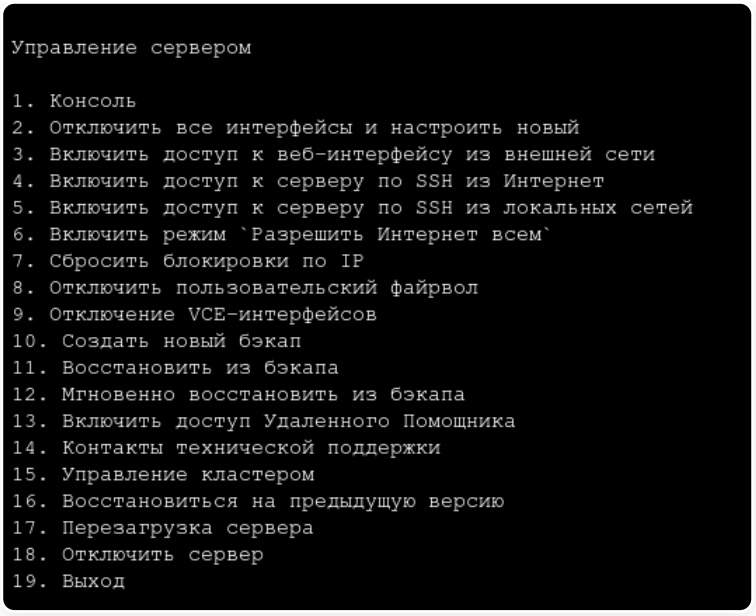
Для подключения специалиста технической поддержки сообщите ему **Информацию для технической поддержки**, нажав кнопку **Скопировать**. Также нужно отдельно передать публичный IP-адрес сервера. Если сервер подключен не напрямую к Ideco NGFW, выполните проброс с внешнего маршрутизатора до 22-го порта на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

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

Включение режима удаленного помощника из локального меню сервера

Чтобы включить режим удаленного помощника, в локальном меню Ideco NGFW выберите пункт **Включить доступ Удаленного помощника**, введя пункт **13**, 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, и скачать ее 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.

Разрешить интернет всем: диагностика неполадок

Используйте режим только для диагностики.

Режим **Разрешить интернет всем** не отключается автоматически и продолжает работать, пока его не отключить вручную.

При включении:

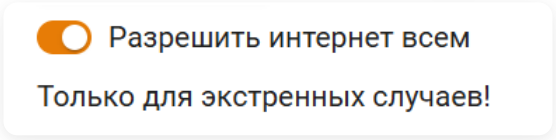
- Сбор веб-статистики будет отключен.
- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включён автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Файрвола** и DNAT.

Цикл обработки трафика в Ideco NGFW описан в статье.

Включить режим можно через:

Веб-интерфейс

Нажмите на иконку технической поддержки в верхней правой части окна и включите **Разрешить интернет всем**:



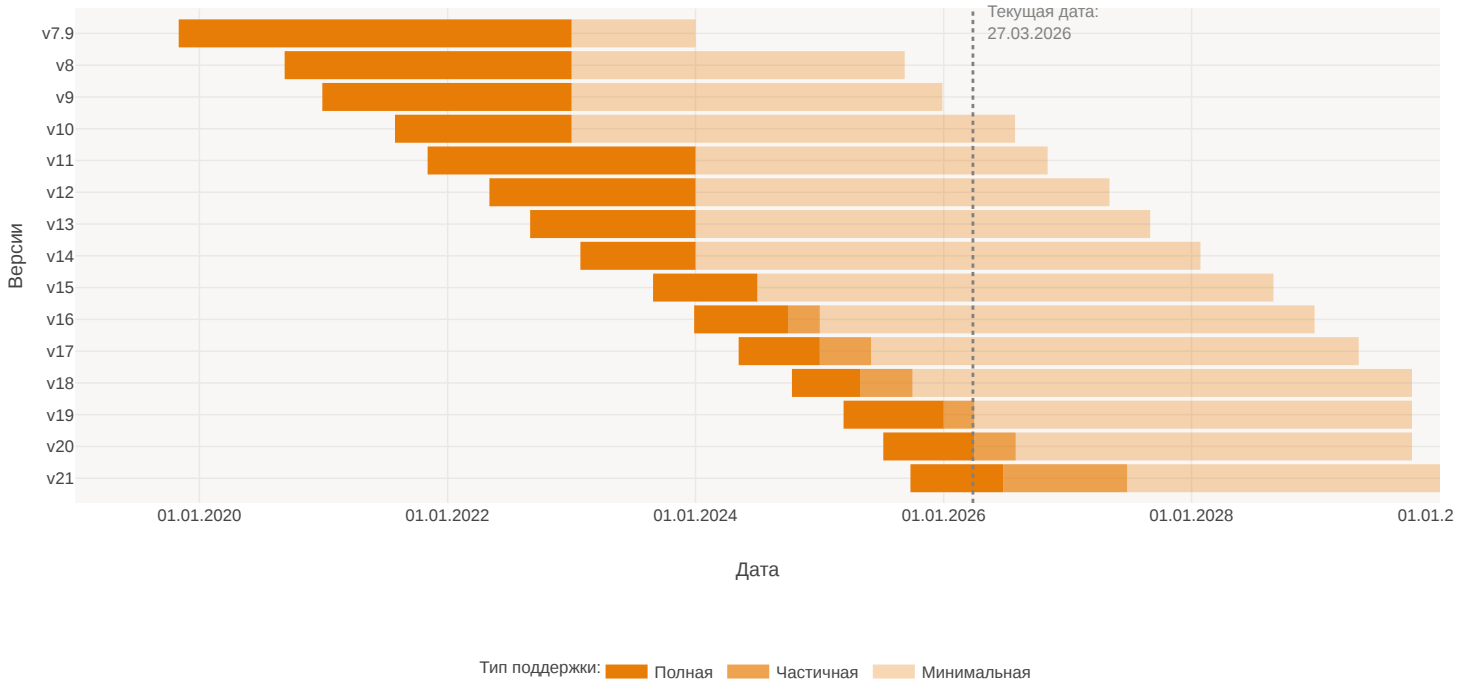
Локальное меню

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

Информация о поддержке версий Ideco NGFW

В статье описываются типы поддержки Ideco NGFW 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

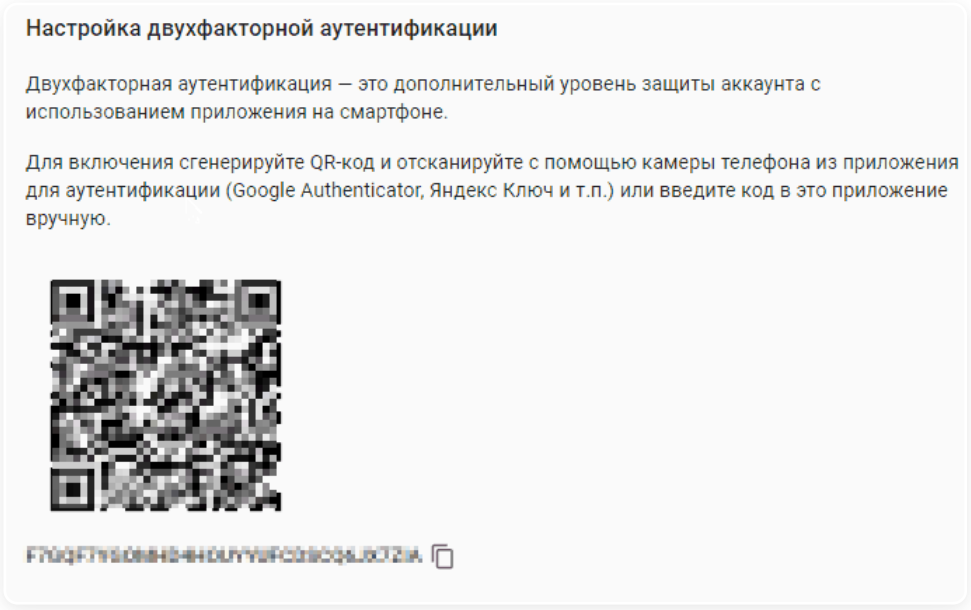
TOTP (Time-based One-Time Password) - это временные одноразовые пароли, которые меняются каждые 30 секунд. Метод аутентификации с использованием TOTP-токенов обеспечивает дополнительный уровень безопасности для ваших аккаунтов.

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. Подробнее - в статье. Система отобразит QR-код и секретный ключ (строка букв и цифр):

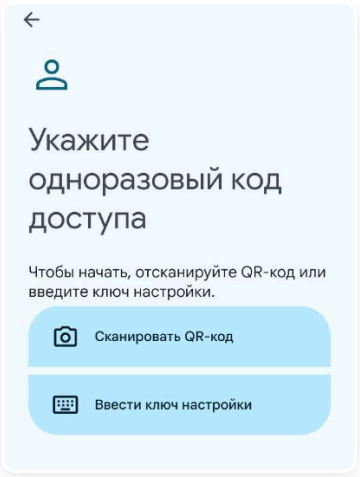


3. Добавьте аккаунт в приложение.

Google Authenticator

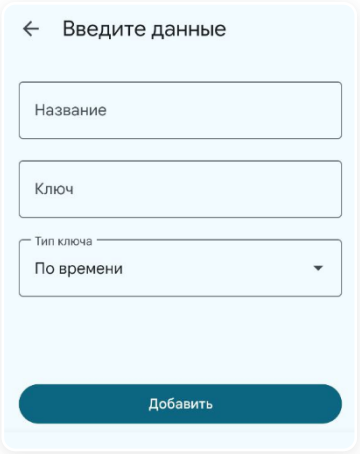
1. Запустите приложение и нажмите **Начать**.

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**.

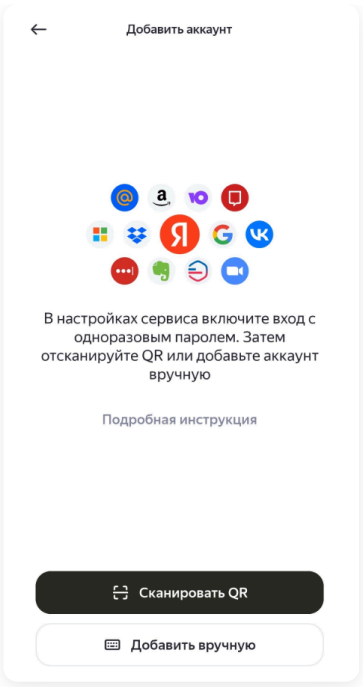
4. Нажмите **Добавить**.

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

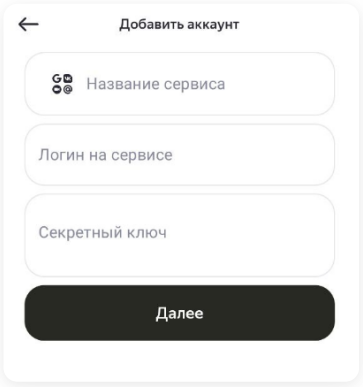
Яндекс ID

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.

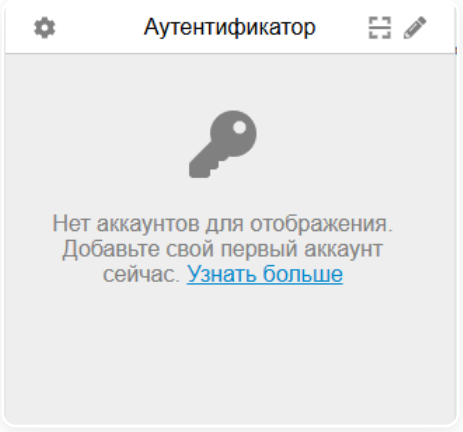
3. Нажмите **Далее**.

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

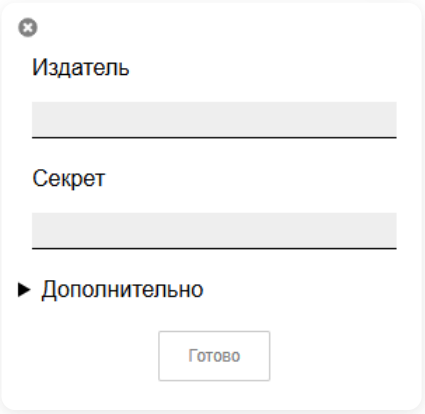
Расширение Аутентификатор

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 таблице представлена информация о продуктах других вендоров, протестированных на совместимость и возможность интеграции с продуктами Ideco.

Продукт	Компания	Класс продукта
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
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
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
Multifactor	ООО "Мультифактор"	Система двухфакторной аутентификации и контроля доступа
SKY DNS	"СкайДНС"	Решение DNS Security и фильтрация контента
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
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
Антивирус Касперского	ЗАО "Лаборатория Касперского"	Антивирус
Контур Staffcop Enterprise	ООО "АТОМ Безопасность"	Система расследования инцидентов внутренней информационной безопасности
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

Источники данных

Ideco NGFW 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.v19.ideco.dev	443 TCP-порт
Отправка анонимной статистики	gatherstat.v19.ideco.dev	443 TCP-порт
Обновления баз GeoIP	ip-list.v19.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.v19.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

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 необходимо, чтобы доступ к вышеуказанным ресурсам был разрешен настройками фильтрации.

Учитывайте при обновлении, что `v19` в домене соответствует версии Ideco NGFW. Эту часть можно заменить символом `*` при настройке фильтрации (пример: `license.*.ideco.dev`).

Рекомендации при первоначальной настройке

Рекомендуемая последовательность шагов для минимальной настройки Ideco NGFW:

1. Зарегистрируйтесь на 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, и выполните предварительные действия. Ideco NGFW можно устанавливать как на виртуальную машину.

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

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

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

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

Подготовка платформы к установке

Установка на гипервизор

Перейти >

Создание загрузочного USB-накопителя

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

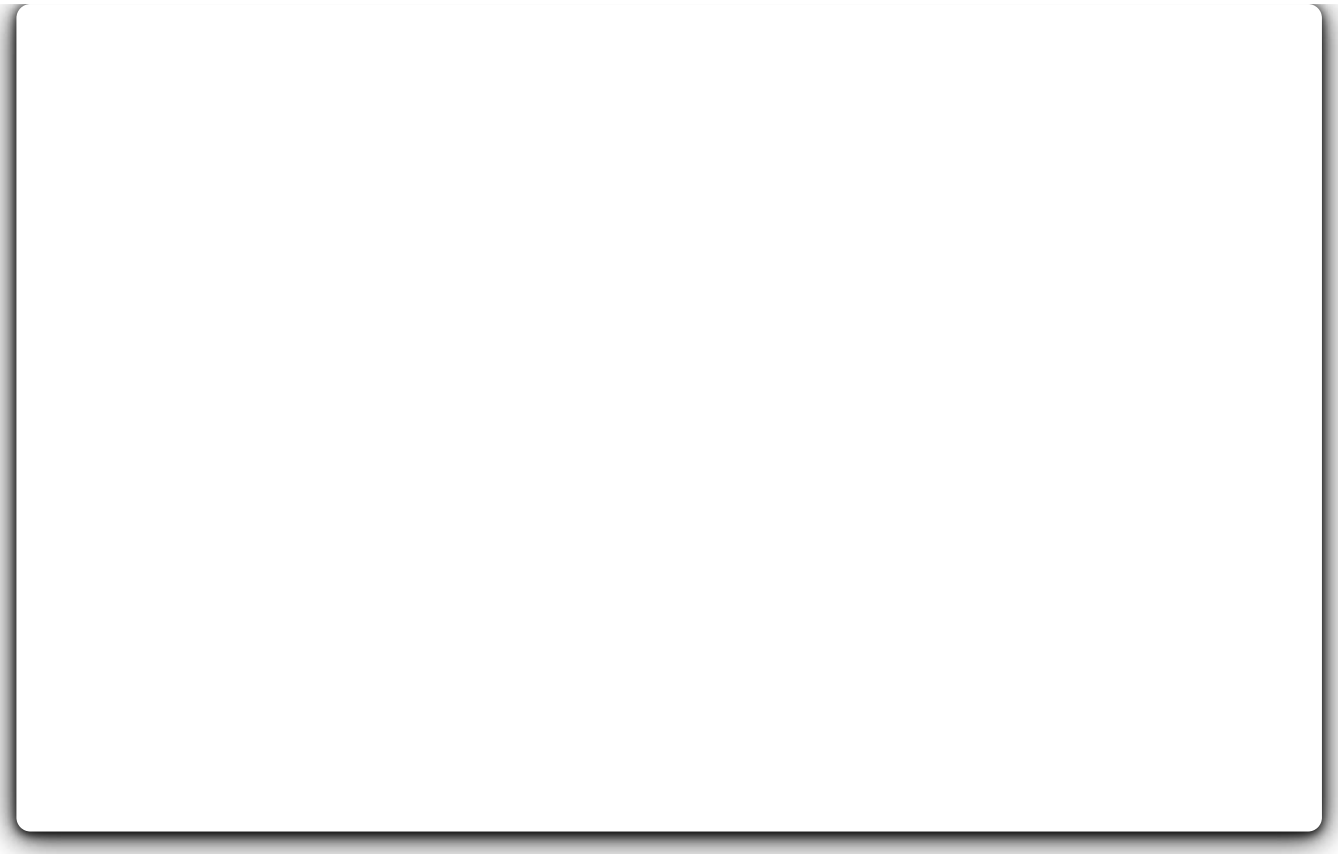
2. Укажите виртуальной машине и установите остальные настройки как на скриншоте:



3. ыб ерите хранилище для виртуальной машины:



4. Установите размер оперативной памяти 1 и размер диска 1 . После выберите в поле rive Datastore ISO file и ук ажите путь к загрузочному образу:

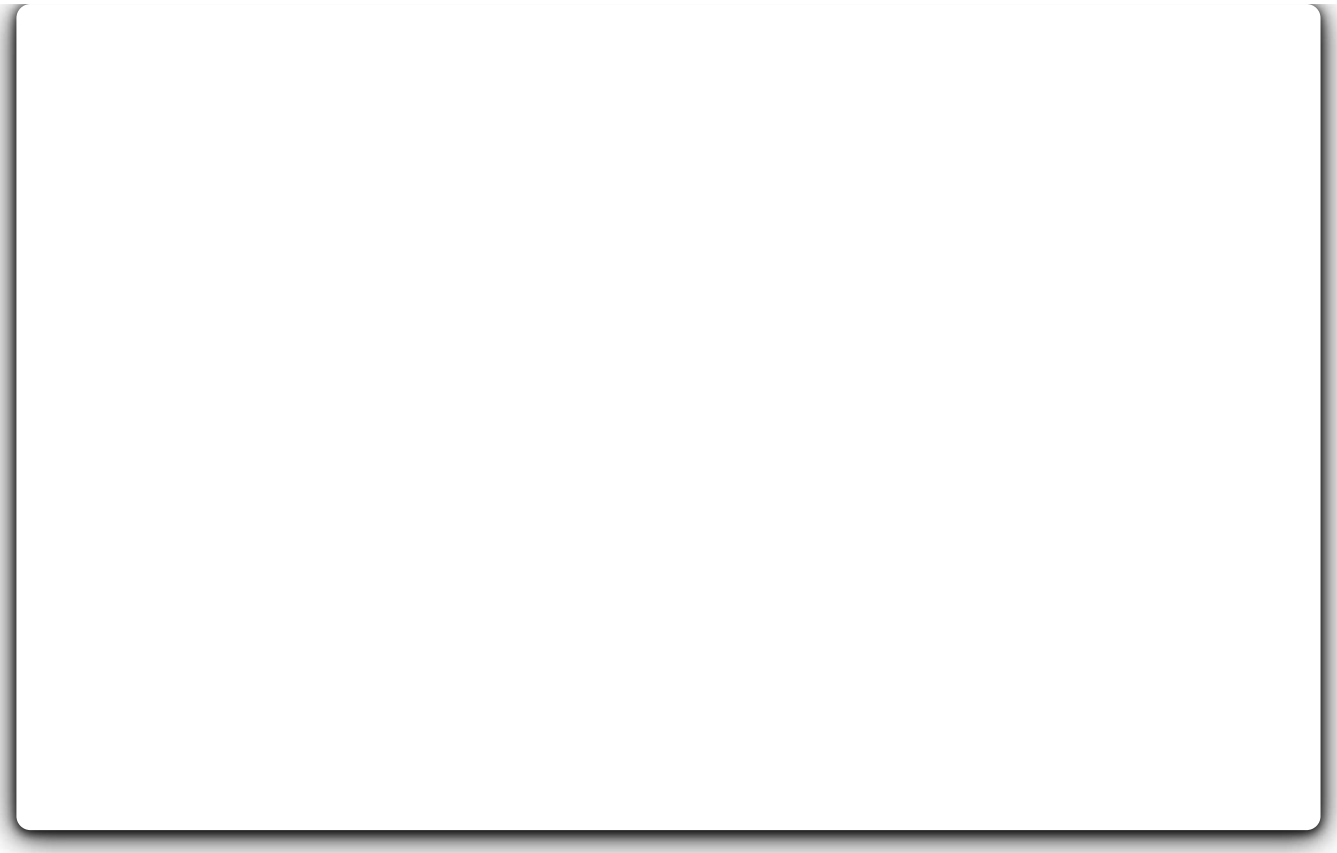


. азверните раздел emory и вкл чите опци eserve all guest memory ll ioc ed



- eserve all guest memory ll ocked опция выкл чена, гипервизор динамически распределяет доступну опера тивну память ме жду всеми виртуальными машинами.

.к л чите на вкладке ptions$ выбрав в поле irm are EFI:



. ажмит е inis:



are or station 1 .

астройк а

Перед установкой Ideco NGFW:

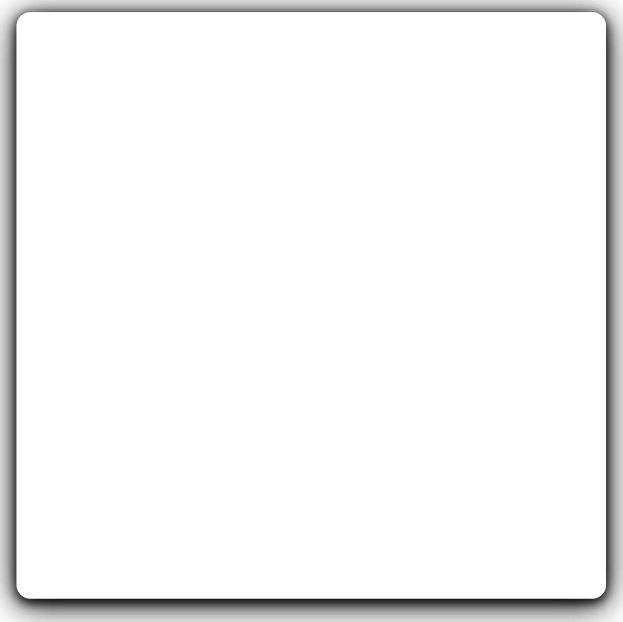
- Увеличьте размер видеопамяти для виртуальной машины до 1 .
- Используйте виртуальные сетевые адаптеры vmxnet .

1. Создайте виртуальну машину , нажав reate a e irtual ac ine

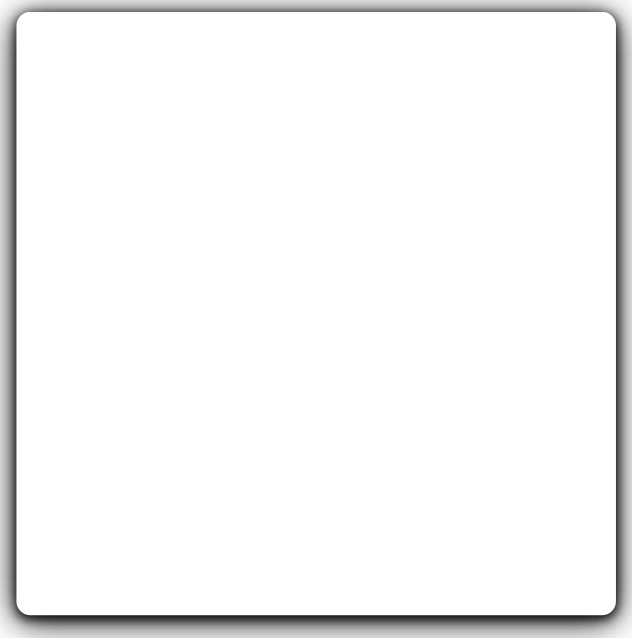
2. Укажите загрузочный ISOобра з:

3. ыб ерите гостеву операционну сист ему inuxи в раскрыващ емся списке укажите тип edora -:it

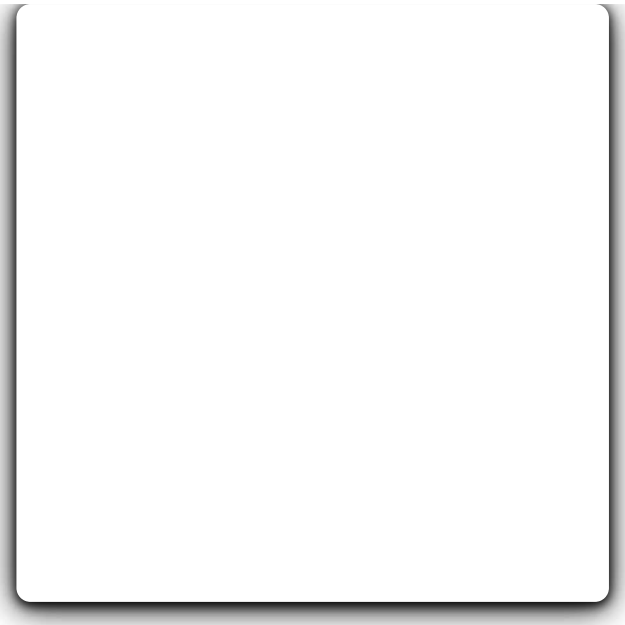
4. Укажите имя виртуальной машины и директори для с оздания виртуального диска:



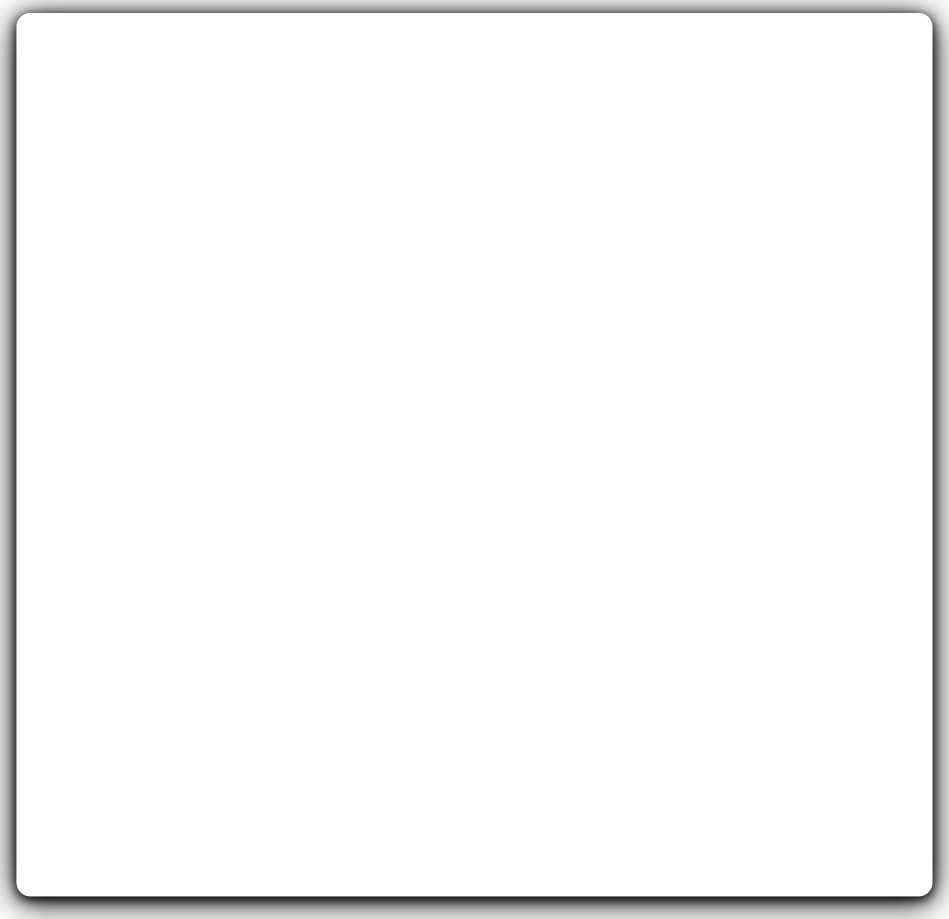
. Укажите размер вирутального жесткого диска 1 :



. ыб ерите ustomie ard aredля изменения настроек виртуальной машины:

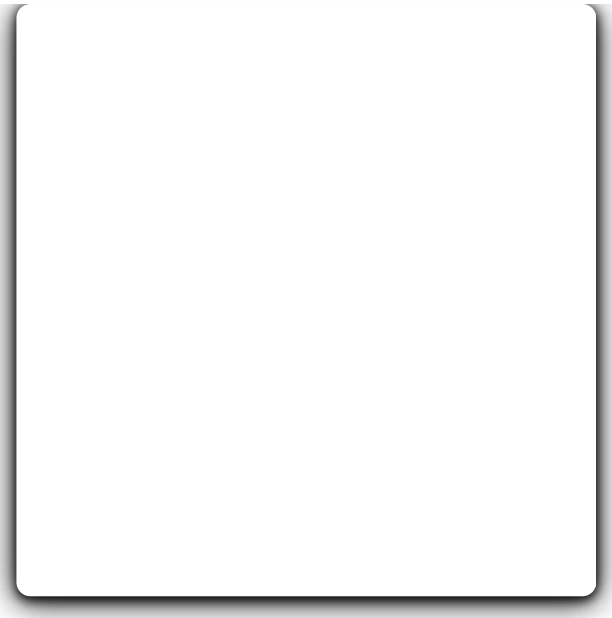


. Укажите размер виртуальной оперативной памяти 1 :

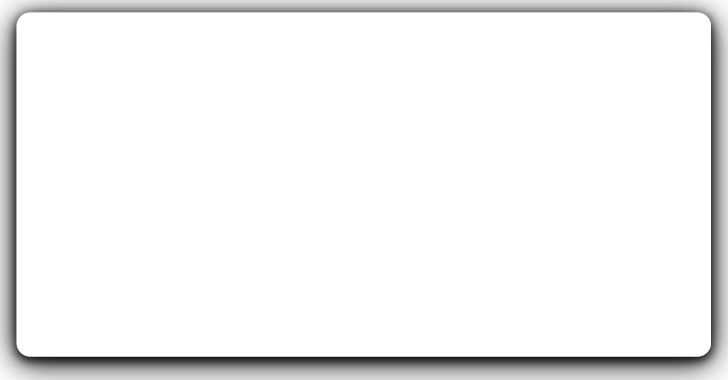


8. Укажите количество ядер процесса равное 4:

9. ыйдит е из мен и нажмит е inis для окончания настройки:



10. Откройте окно виртуальной машины и нажмите dit virtual mac ine settings



11. Перейдите в ptions dvanced и активируйте опци isa le memory page trimming. Установите для параметра irm are ype значение :

- isa le memory page trimming — если опция выкл чена, гипервизор динамически распределяет доступну опера тивну память ме жду всеми виртуальными машинами.

12. ажмит е для завершения настройки виртуальной машины.

irtual ox . .1

астройк а

По умолчани при с оздании виртуальной машины создается одна сетевая карта с типом подкл чения .

1. Укажите виртуальной машины (), выб ерите директори для и у становите путь до загрузочного образа NGFW. Остальные параметры установите как на скриншоте:



2. Установите размер оперативной памяти (1) и нажмите :

3. Создайте виртуальный жесткий диск под (Об ем не меньше 1):

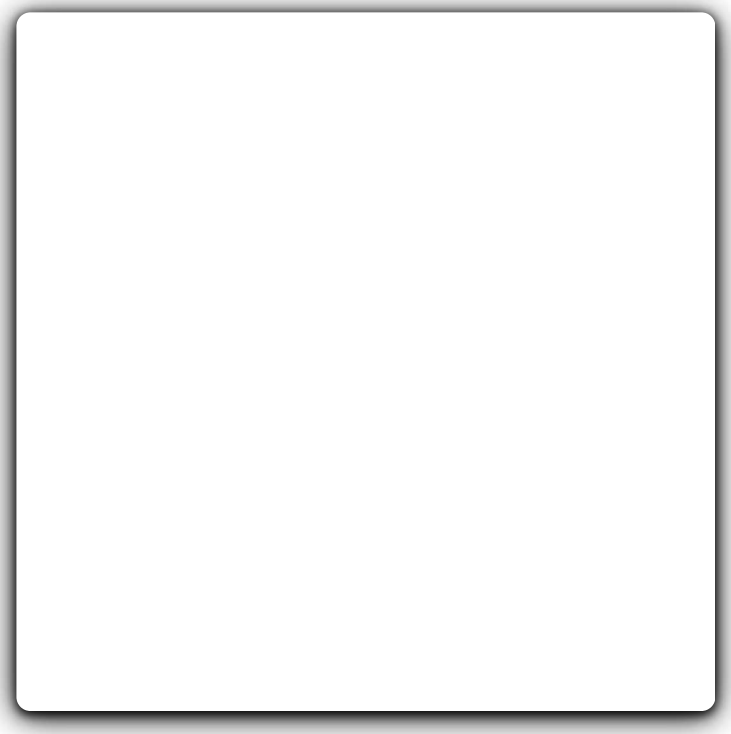


4. ажмит е

астройк а

1. При установке Ideco NGFW выберите тип операционной системы - edora

2. к л чите опци и нажмите кнопку на пятом шаге (virtm-manager) установки:



3. Измените интерфейс на virtio для дисков и сетевых карт.

4. ыб ерите режим кеширования. сли диски име т формат co 2 или ra , используйте rite ac. сли используется другой формат дисков, проконсультируйтесь с системным администратором или с ехнической поддержкой.

. появившемся окне на вк ладке в поле irm are выберите пункт x usr s are . ыбор того пункта вкл чит и выкл чит опци ecure oot.

сли пункта x usr s are нет в списке, доустановите пакет ovmf. U untu тот пакет устанавливается командой sudo apt install ovmf.

. Перейдите в раздел emory и измените тег <memballoon model='virtio'/> на <memballoon model='none'/>, чтобы откл чить emory allooning повысить производительность. При вкл ченной опции гипервизор динамически распределяет доступну опера тивну память между виртуальными машинами, из-за чего гостевая ОС может видеть больший обем памяти, чем фак тически выделено.

roxmox

астройк а

1. ажмит е , вкл чите опци и введите имя машины:



2. ра зделе выберите хранилище и заполните поля:



- - образ с нужной версией NGFW.
- :
  - - Linux.
  - - .x - 2.0 ernel.

3. ра зделе заполните поля:



- - 3 .
- - Ð .
- - хранилище для UEFI-диска.
- - вкл чите опци, чт обы операционная система могла передавать гипервизору информаци о св оих внутренних состояниях.
- - откл чите опци.

4. ра зделе укажите нужный размер диска (не меньше 1 0) и выб ерите хранилище для NGFW:



- - irtIOloc.
- - вкл чите опци, если ну жно ск ономить дисковое пространство. Она позволяет автоматически очищать освобожденные блоки на диске.

Проверьте свободное место на диске.

. ра зделе укажите количество сокетов и ядер (от четырех ядер) и выберите тип, который поддерживает SSE 4.2:



. ра зделе укажите обем опера тивной памяти (не менее 1):



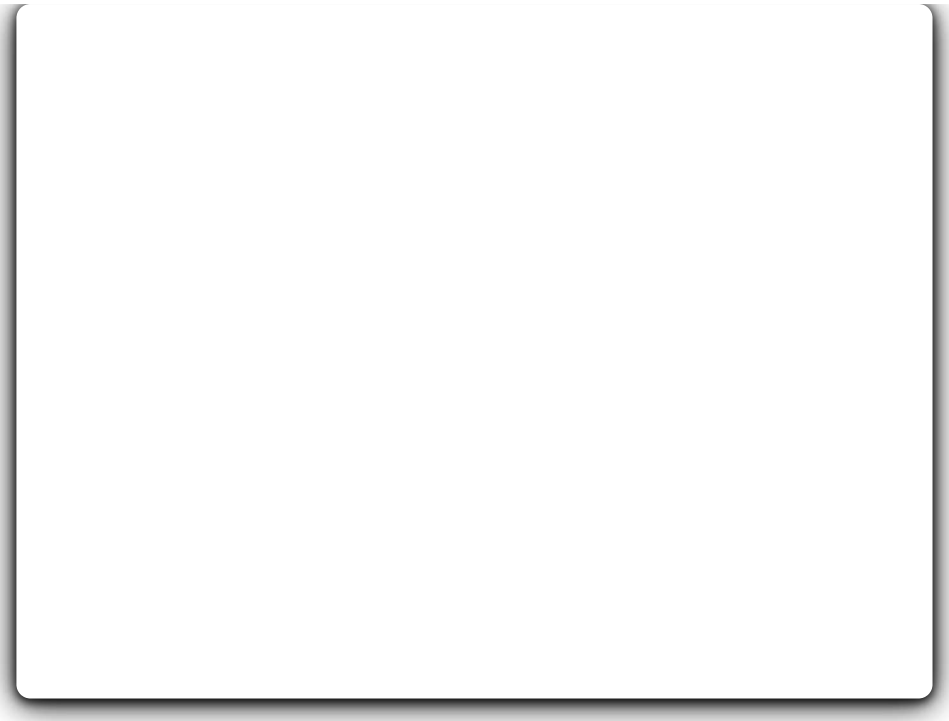
- - откл чите опци для об еспечения максимальной производительности. При вкл ченной опции гипервизор динамически распределяет доступну опера тивну память ме жду виртуальными машинами, из-за чего гостевая ОС может видеть больший обем памяти, чем фактически выделено.

. ра зделе в поле выберите сетевой мост для локального интерфейса:



екомендуем откл чить опци , чтобы облегчить настройку и отладку файрвола в Ideco NGFW и избежать конфликтов обработки трафика.

8. ра зделе проверьте заданные настройки и нажмите :



екомендуем откл чить опци , так как потребуется добавить еще одно сетевое устройство.

9. Для работы NGFW также понадобится мост на сетевой интерфейс, чтобы получить доступ в интернет. ажмит е на созданну вир туальну машину , выберите и добавьте мост, соответствущий выбранном у ранее коммутатору:

icroso t yper-

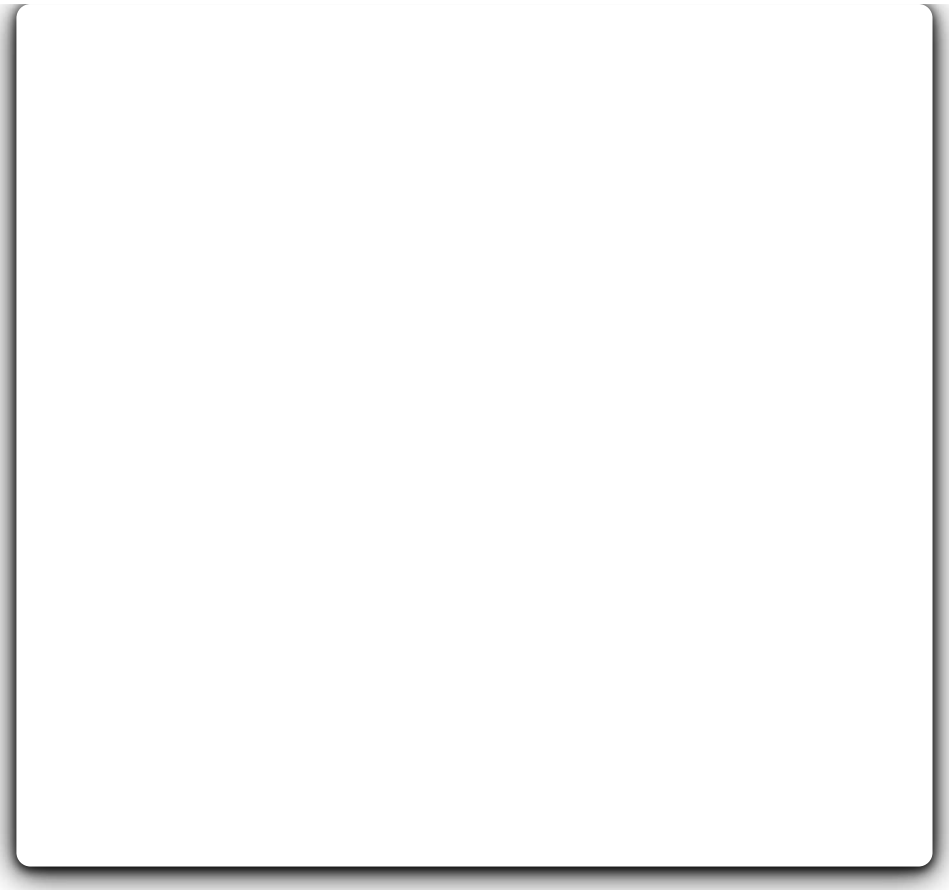
- Поддерживается только второе поколение виртуальных машин под Windo s Server 2012 2 или выше.
- Откл чите опци ecure oot .
- Откл чите опци ynamic memory .
- Используйте et or dapter .

аги по у становке Ideco NGFW после создания загрузочного US -нак опителя можно прочитать в статье Установка.

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

1. Перейдите в ardvare et or dapter dvanced eatures address

2. к л чите опци na le address spoo ing



При первом запуске в проверьте, что urrent ecure oot tate в состоянии isa led



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.

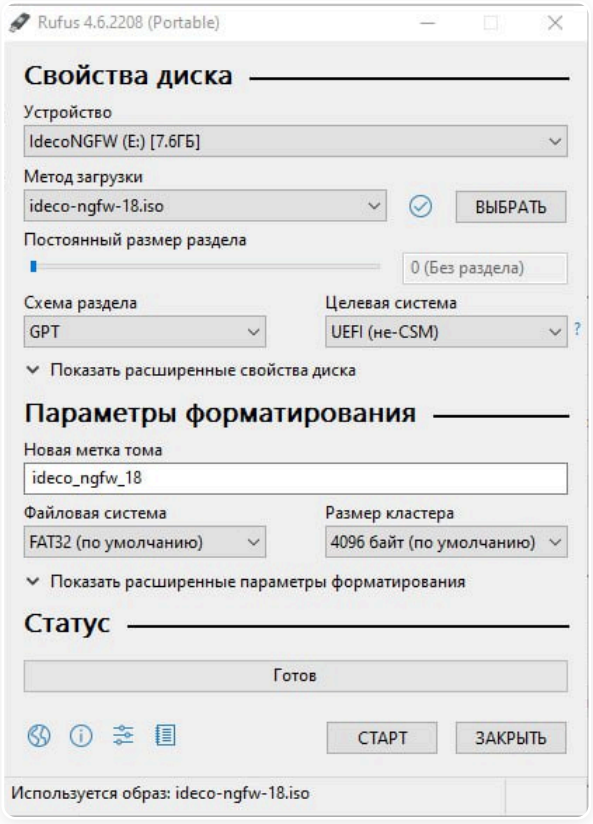
3. Выберите нужный USB-накопитель в пункте **Устройство**.

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

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

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>"
```

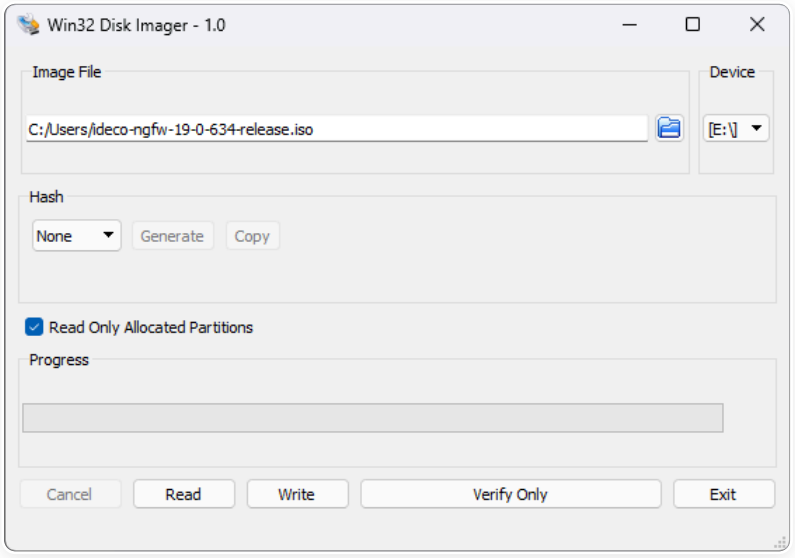
2. Установите программу Win32diskimager и запустите.

3. Нажмите на значок синей папки и выберите ISO-файл, который вы 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-19-11-29-release.iso" | sha256sum -c
```

2. Найдите USB-носитель в системе:

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

Ответ:

```
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-19-11-29-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 после создания загрузочного USB-накопителя можно прочитать в статье Установка.

Установка

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube

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

Процесс установки

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

Для установки Ideco NGFW выполните действия:

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

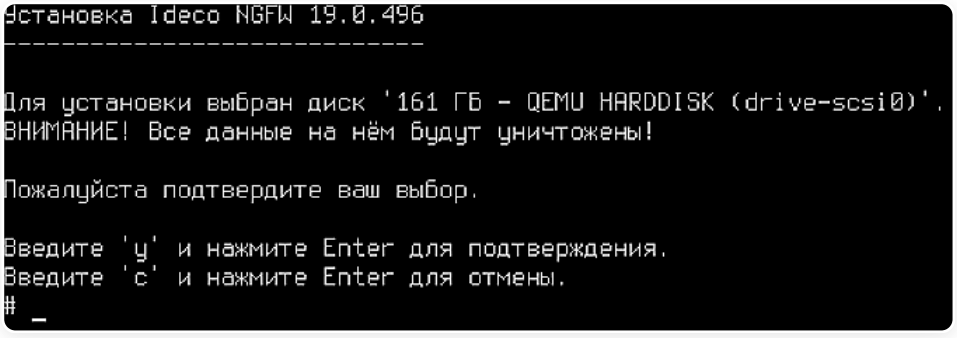


При установке или загрузке сервера Ideco NGFW не рекомендуем нажимать на клавиатуре:

- `-` - 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**.

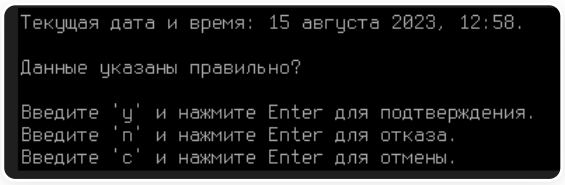
2. Выберите диск и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой находится сервер:



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



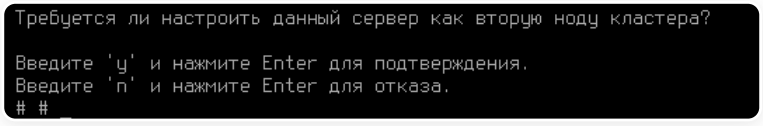
Извлеките USB-диск после установки Ideco NGFW, чтобы загрузка с него не началась заново.

5. Не нажимайте никаких клавиш при появлении окна:

После загрузки система автоматически перейдет к локальному интерфейсу Ideco NGFW.

Настройка второй ноды кластера

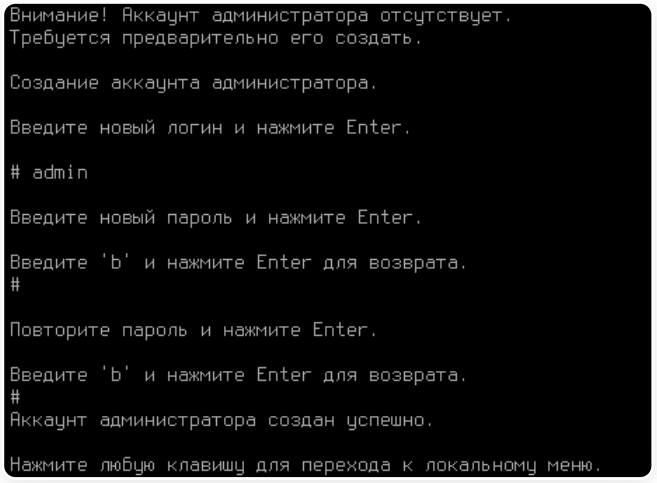
1. Введите **y** для начала настройки NGFW как второй ноды кластера:



2. Для продолжения настройки воспользуйтесь статьей Кластеризация.

Создание учетной записи администратора

Для входа в веб-интерфейс (после уведомления "*Создание аккаунта администратора*") создайте учетную запись администратора, соблюдая требования к паролю:



Требования к паролю

- 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.

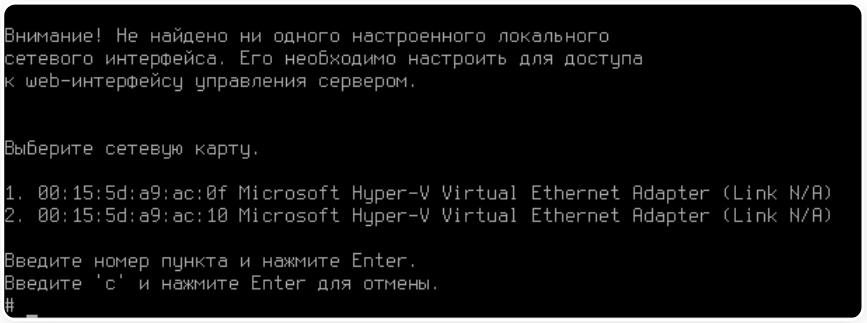
Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;`, `^[[4~;` и т.д.

Настройка локального интерфейса

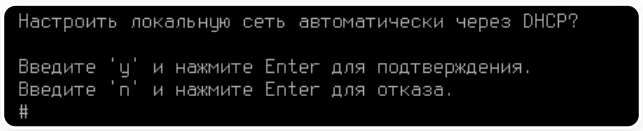
При использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса.
Для корректной идентификации сетевой карты используйте ее MAC-адрес.

Для настройки Ideco NGFW через веб-интерфейс настройте локальный интерфейс в локальном меню шлюза:

1. Введите номер сетевого адаптера под локальный интерфейс:



2. Настройте локальную сеть автоматически через DHCP, введя **y**, или вручную, введя **n**:



3. Введите локальный IP-адрес и маску подсети в формате `ip/маска` и нажмите **Enter**:

```
Введите IP/префикс и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# 10.10.0.185/24
```

4. Введите адрес шлюза или оставьте поле пустым:

- При настройке **Ideco NGFW в качестве шлюза** оставьте поле шлюз пустым:

```
Введите адрес шлюза (или оставьте пустым) и нажмите Enter.

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

- При настройке **Ideco NGFW в качестве прокси** введите шлюз с доступом в интернет:

```
Введите адрес шлюза (или оставьте пустым) и нажмите Enter.

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

5. Задайте тег VLAN (стандарт VLAN 802.3q) или оставьте поле пустым:

```
Введите VLAN тэг (или оставьте пустым) и нажмите Enter.

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

После создания локального интерфейса откроется локальное меню управления сервером:

```
Управление сервером

1. Консоль
2. Отключить все интерфейсы и настроить новый
3. Включить доступ к веб-интерфейсу из внешней сети
4. Включить доступ к серверу по SSH из Интернет
5. Включить доступ к серверу по SSH из локальных сетей
6. Включить режим `Разрешить Интернет всем`
7. Сбросить блокировки по IP
8. Отключить пользовательский файрвол
9. Отключение VCE-интерфейсов
10. Создать новый бэкап
11. Восстановить из бэкапа
12. Мгновенно восстановить из бэкапа
13. Включить доступ Удаленного Помощника
14. Контакты технической поддержки
15. Управление кластером
16. Восстановиться на предыдущую версию
17. Перезагрузка сервера
18. Отключить сервер
19. Выход
```

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

Полезные ссылки

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

Первоначальная настройка

Для получения доступа в интернет и настроить авторизацию. В противном случае доступ в интернет для устройства с установленным Ideco NGFW будет заблокирован.

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

Подключение к веб-интерфейсу Ideco NGFW

1. Запустите на любом компьютере в локальной сети поддерживаемый интернет-браузер (современные версии браузеров Firefox, Chrome и браузеров, основанных на Chromium).

2. Введите в адресной строке IP-адрес, указанный при настройке локального 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 NGFW.

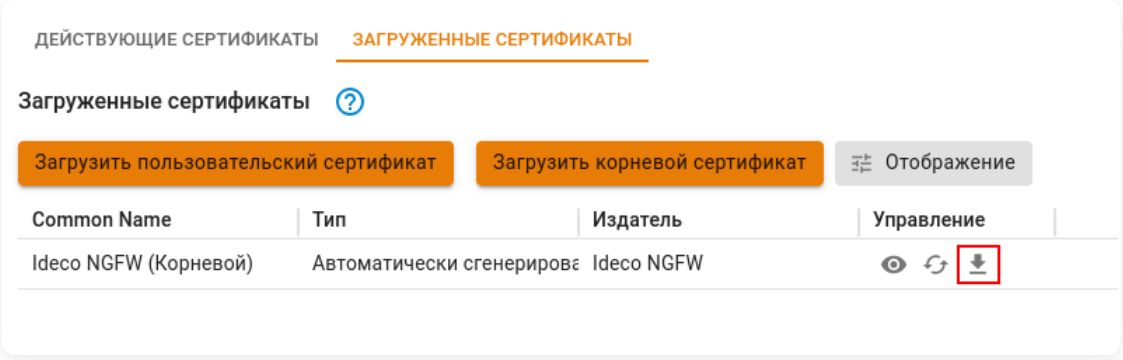
Импорт корневого сертификата NGFW

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

1. Скачайте сертификат одним из способов:

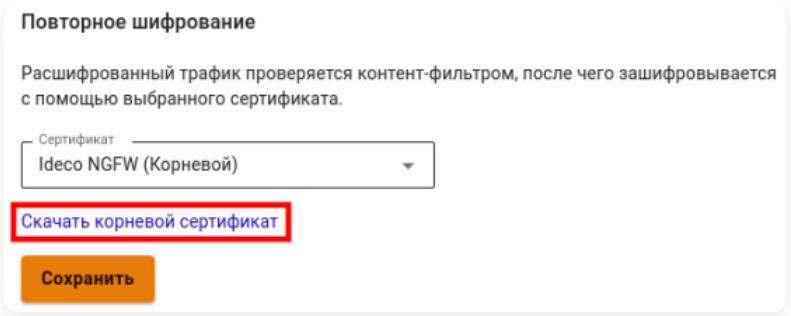
Из раздела Сервисы

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



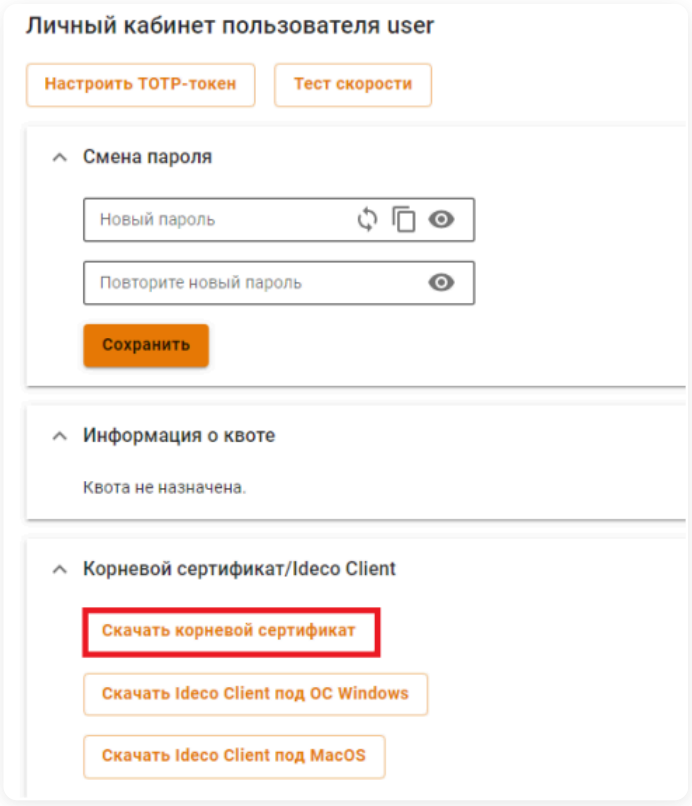
Из раздела Правила трафика

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



Из личного кабинета пользователя

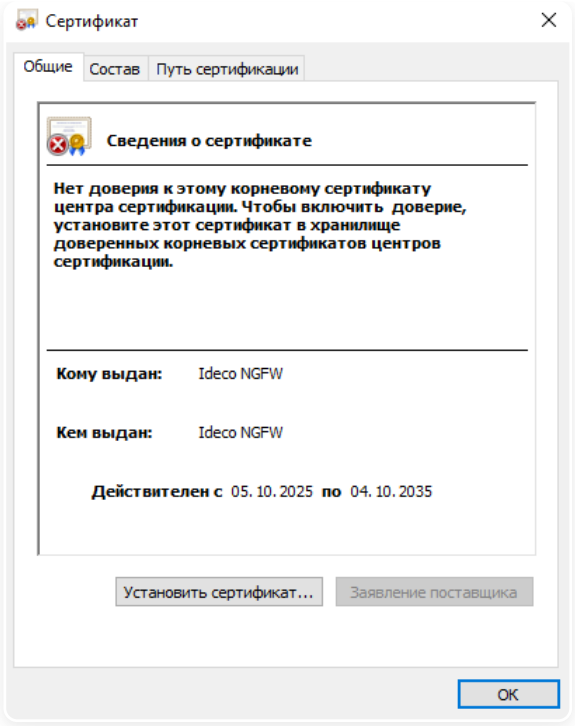
В личном кабинете Ideco NGFW под учетной записью одного из пользователей перейдите на вкладку **Корневой сертификат/Ideco Client** и нажмите **Скачать корневой сертификат**:



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

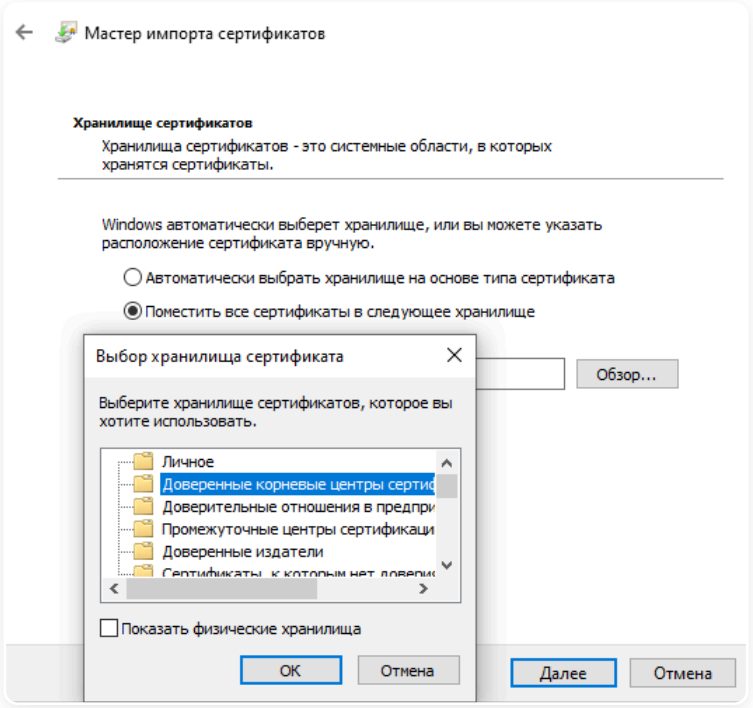
Пример для Windows

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

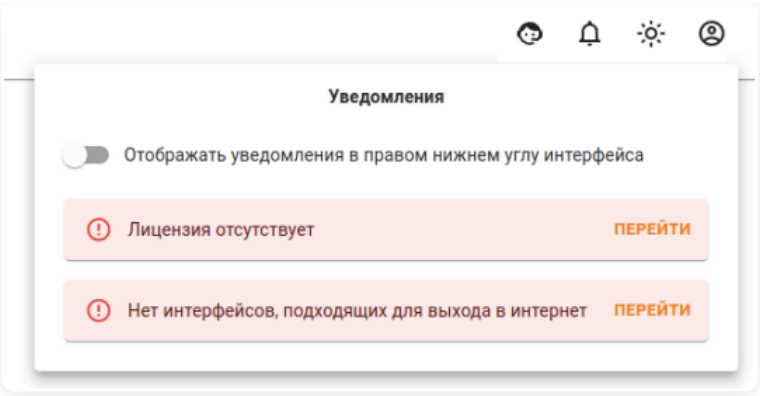


2. Выберите расположение хранилища **Локальный компьютер**:

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:



Настройка Ethernet-подключения для доступа в интернет

При создании, редактировании или удалении сетевого интерфейса перевыпускается SSL-сертификат, поэтому вероятно снижение скорости работы веб-интерфейса Ideco NGFW. В этом случае рекомендуем нажать F5.

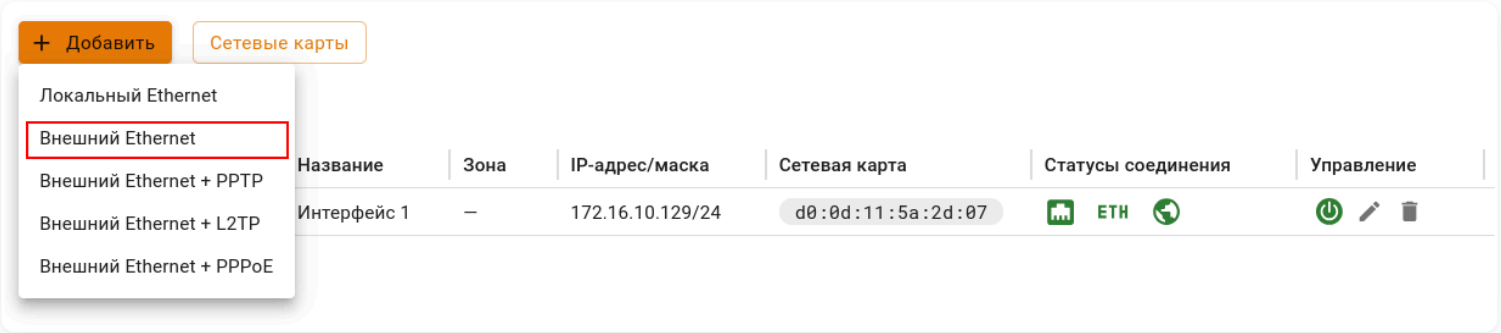
Этот тип подключения требует настройки параметров, описанных ниже в таблице.

Параметр	Примечание
Сетевая карта	Укажите сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру. Для идентификации адаптера ориентируйтесь на наименование производителя или MAC-адрес
IP-адрес и маска	Укажите сетевые реквизиты, которые были назначены провайдером. Укажите IP-адрес и сетевую маску в формате CIDR или четырех октетов
Шлюз по умолчанию	Укажите IP-адрес шлюза интернет-провайдера, через который будет осуществляться подключение к сети интернет

Для настройки Ethernet-подключения выполните:

1. Перейдите в раздел **Сервисы** → **Сетевые интерфейсы**.

2. Нажмите **Добавить** и выберите пункт **Внешний Ethernet**:



Будьте внимательны!

При выборе пункта **Локальный Ethernet** и заполнении поля **Шлюз** доступ в интернет будет отсутствовать. Шлюз указывается только если NGFW работает в режиме прямого прокси с одним интерфейсом.

3. Выберите подходящую сетевую карту.

4. Заполните необходимые поля и нажмите **Добавить**.

Включите опцию **Автоматическая конфигурация через DHCP** если провайдер поддерживает автоматическое конфигурирование внешнего сетевого интерфейса с помощью протокола DHCP.

Настройка других типов подключений

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

- Внешние и локальные интерфейсы;
- Одновременное подключение к нескольким провайдерам.

Регистрация сервера

Для активации лицензии необходима обязательная регистрация сервера в личном кабинете.

Выберите удобный способ получения лицензии:

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

Онлайн-регистрация

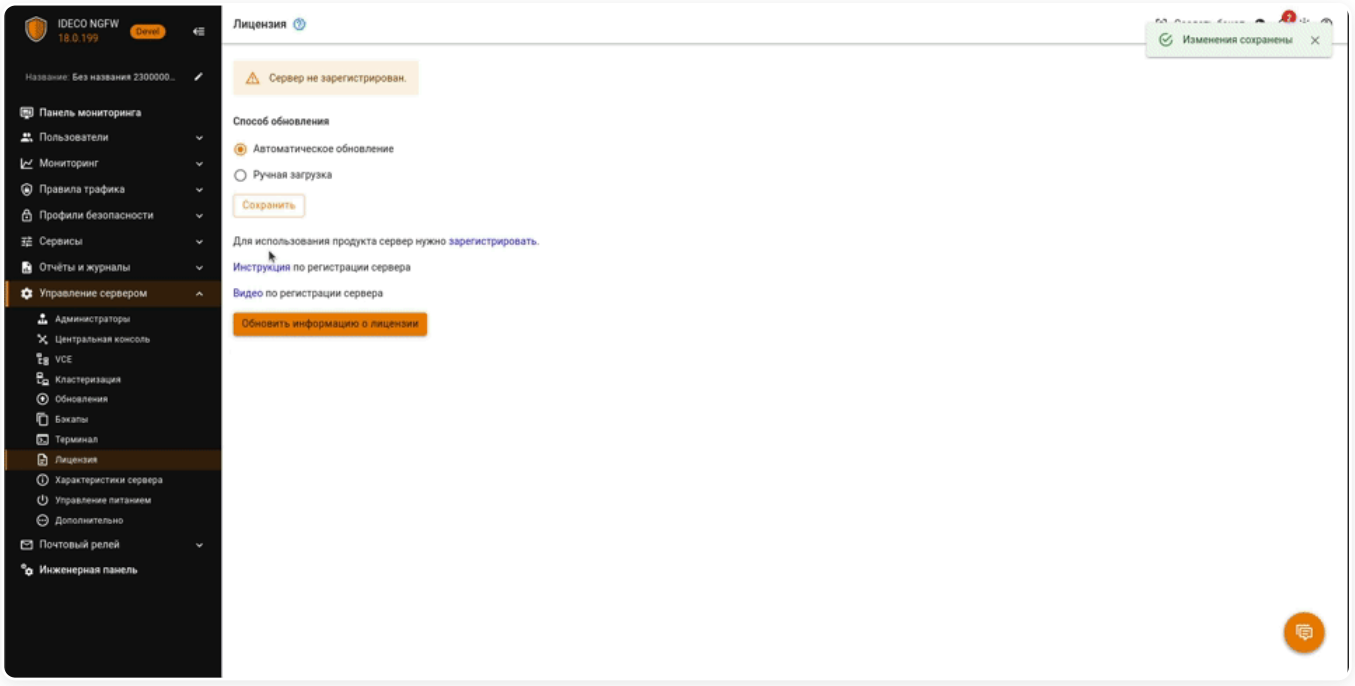
Перед онлайн-регистрацией создайте **Внешний Ethernet-интерфейс** для выхода в интернет. Затем активируйте опцию **Разрешить интернет всем**. Не забудьте отключить опцию после получения лицензии.

Шаги онлайн-регистрации сервера и привязки лицензии:

1. Перейдите в веб-интерфейс Ideco NGFW в раздел **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:

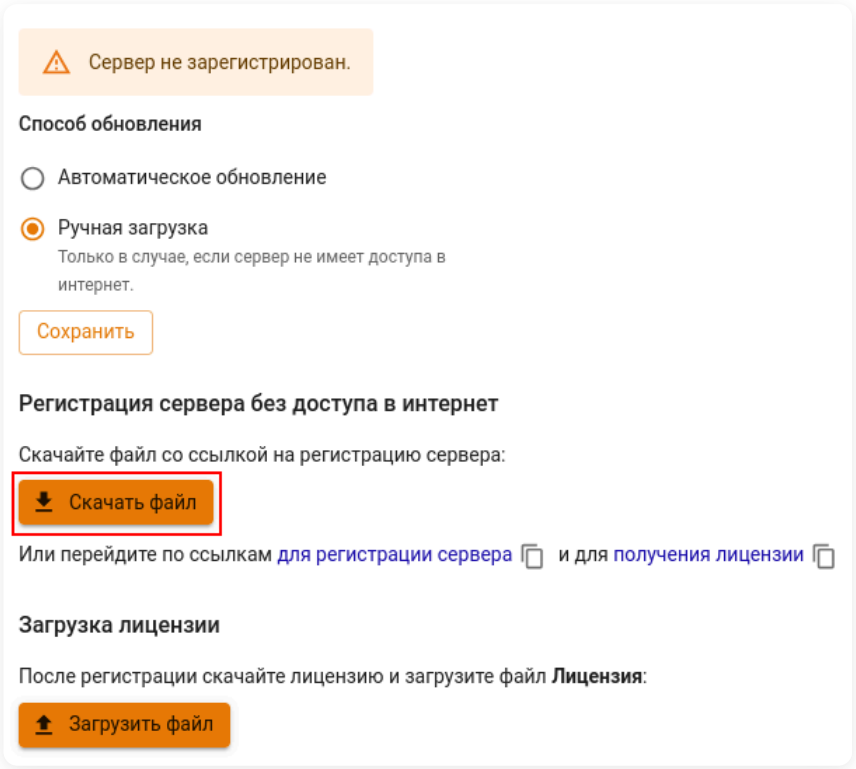
- Rutube

- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

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

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Это можно сделать, нажав на кнопку, или скопировать ссылку из веб-интерфейса:

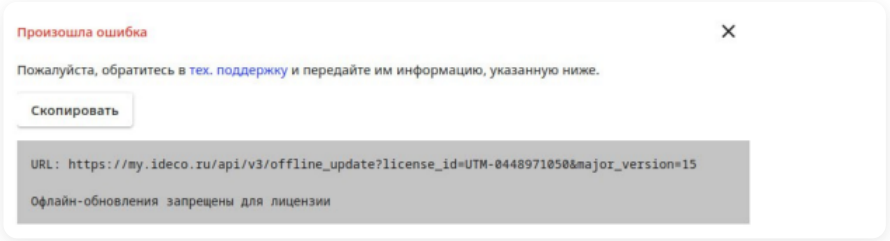


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

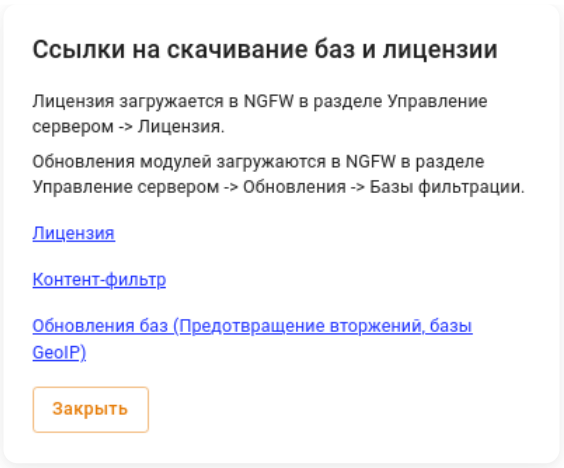
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

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:

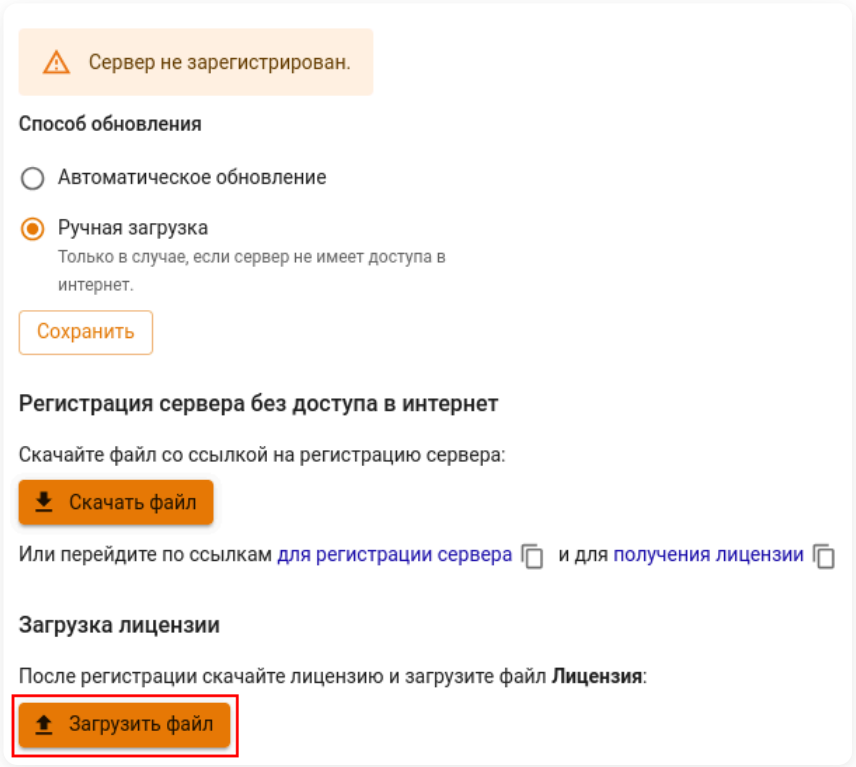


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



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** в веб-интерфейсе Ideco NGFW и загрузите файл с лицензией, скачанный в пункте 6:



Повторная регистрация сервера после удаления

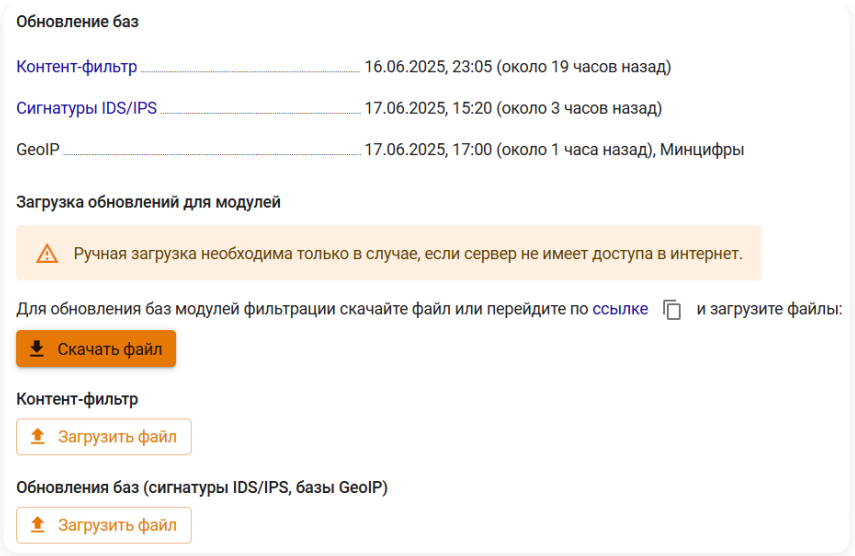
1. Откройте терминал и введите команду:

```
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 в раздел **Управление сервером** → **Обновления** → **Базы фильтрации** и загрузите скачанные в шестом пункте Офлайн-регистрации файлы, нажав на соответствующие кнопки:



Базы фильтрации Ideco NGFW могут меняться ежедневно, поэтому при ручной загрузке обновляйте их 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.

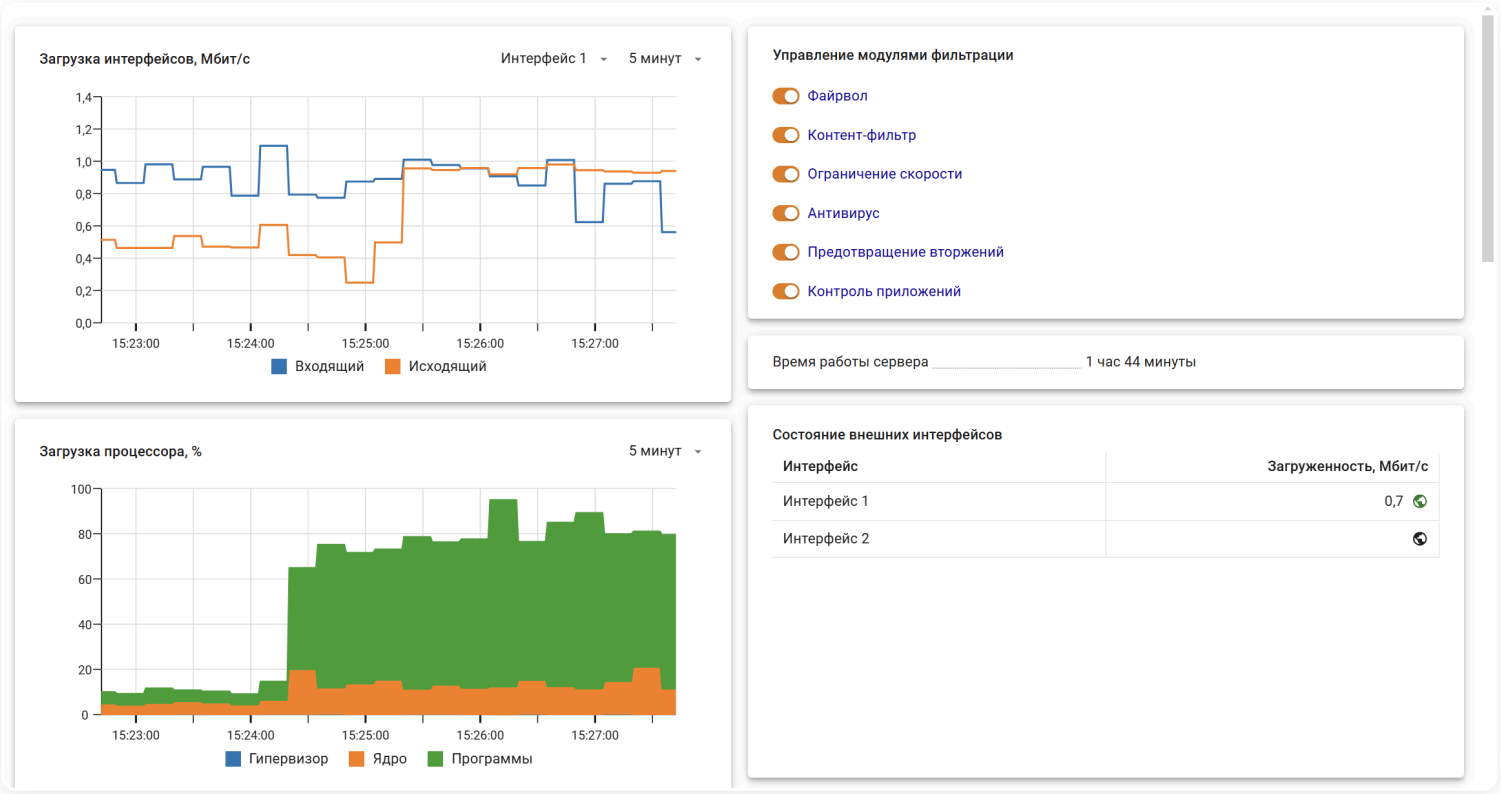
- **IP и MAC авторизация** - способ авторизации, при котором пользователь получает доступ в интернет без ввода логина и пароля:
  - **Авторизация по IP-адресу**. Проверьте, чтобы IP-адрес устройства пользователя совпадал с IP-адресом, указанным администратором в настройках учетной записи пользователя 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.

Панель мониторинга

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



Отображение оперативной информации

- Загрузка сетевых 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.

Управление модулями фильтрации

Блок позволяет включить или выключить соответствующие модули фильтрации:

- Файрвол.
- 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 **Контроля приложений**. При этом учитывается служебный трафик NGFW (`169.254.1.1`):
  - DNS-запросы для резолвинга доменных имен из **Правила трафика** → **Объекты**.
  - ICMP-проверки доступности адресов из **Сервисы** → **Балансировка и резервирование** → **Адреса для проверки связи**.
  - Служебные запросы:
    - Выпуск Let's Encrypt сертификатов.
    - Проверка лицензии MY.IDECO.
    - Загрузка баз **Контент-фильтра** и IPS.
    - Скачивание ISO-образов обновлений.
  - Любые запросы, выполняемые через терминал NGFW.

Пользователи

Учетные записи
Создание и управление учетными записями пользователей

Перейти >

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

Перейти >

Двухфакторная аутентификация
Типы двухфакторной аутентификации и особенности их настройки

Перейти >

VPN-подключение
Настройка VPN-подключения с использованием протоколов: PPTP, 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 >

Active Directory/Samba DC
Настройка односторонней синхронизации с контроллером домена на базе Microsoft Active Directory и Samba DC

Перейти >

ALD Pro
Настройка односторонней синхронизации с системой управления каталогами ALD Pro

Перейти >

RADIUS
Настройка RADIUS-сервера, двухфакторная аутентификация пользователей и управление учетными записями

Перейти >

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

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Учетные записи

В веб-интерфейсе Ideco NGFW пользователи отображаются в виде дерева и могут быть организованы в группы с неограниченной вложенностью. Дерево учетных записей доступно в разделе **Пользователи → Учетные записи**.

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

В Ideco NGFW реализован принцип наследования, которое позволяет задавать и изменять общие параметры для всех пользователей группы через родительскую группу. Это упрощает управление и настройки для всей группы одновременно.

> Все пользователи Ideco NGFW по умолчанию входят в группу **Все**. Если при создании какого-либо правила в параметрах будет выбрана группа **Все**, правило будет распространяться на всех пользователей NGFW.

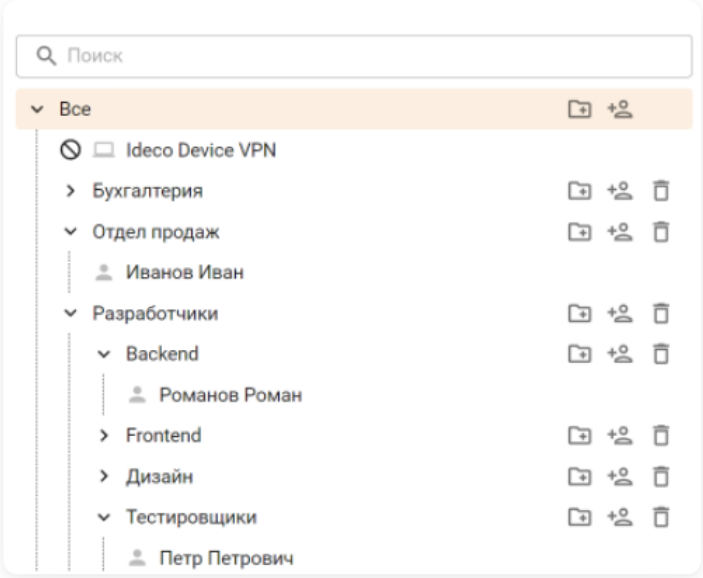
Цвет пиктограммы пользователя зависит от состояния учетной записи пользователя:

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

Пример дерева пользователей:



Управление учетными записями и группами

Создание учетной записи пользователя

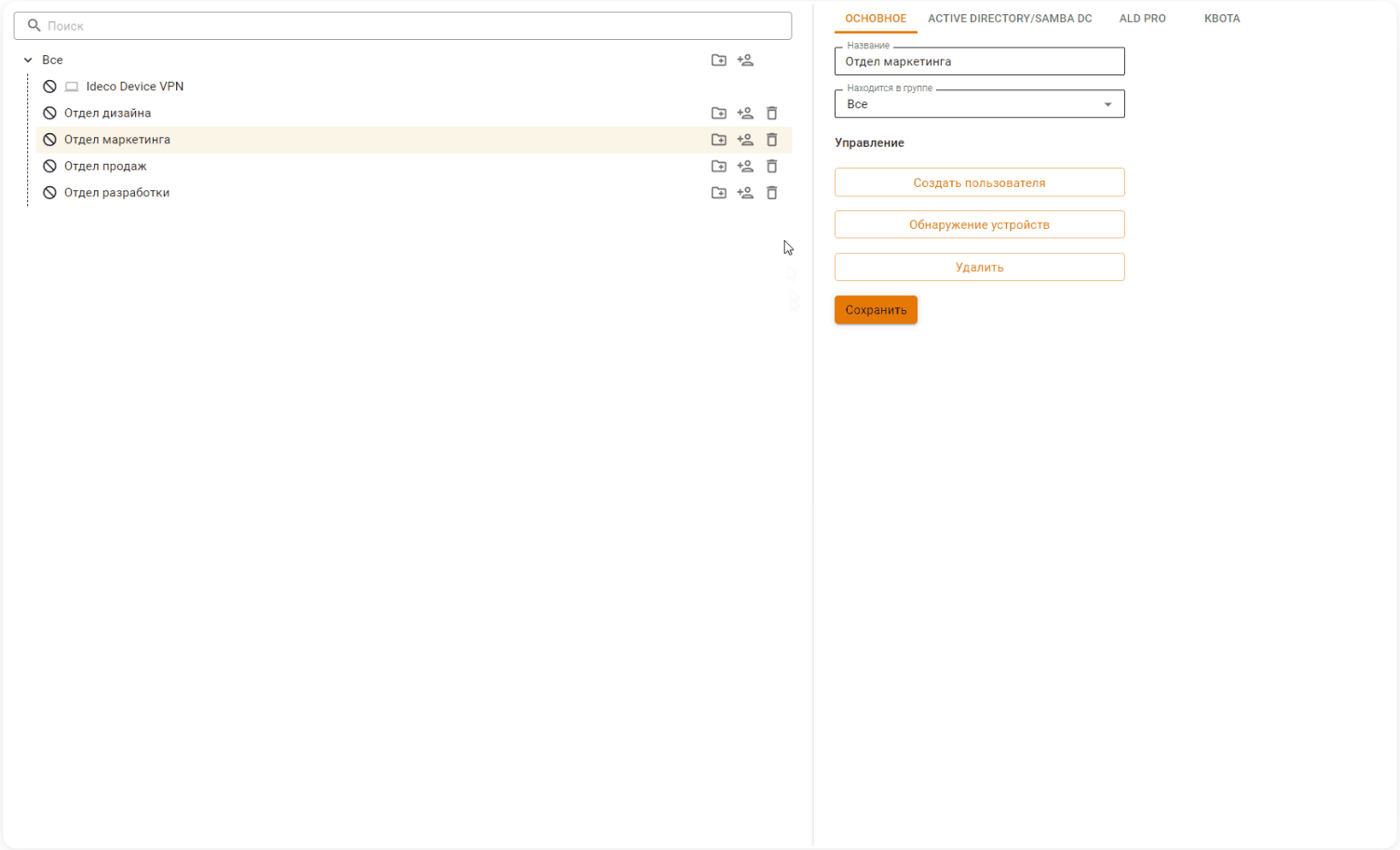
Не используйте в качестве логина пользователя IP-адрес, так как возникнет ошибка при подключении по IKEv2.

Способы создания учетной записи пользователя и группы:

Пользователь в определенной группе

1. Выберите группу, в которую добавится пользователь.

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



3. Заполните поля:

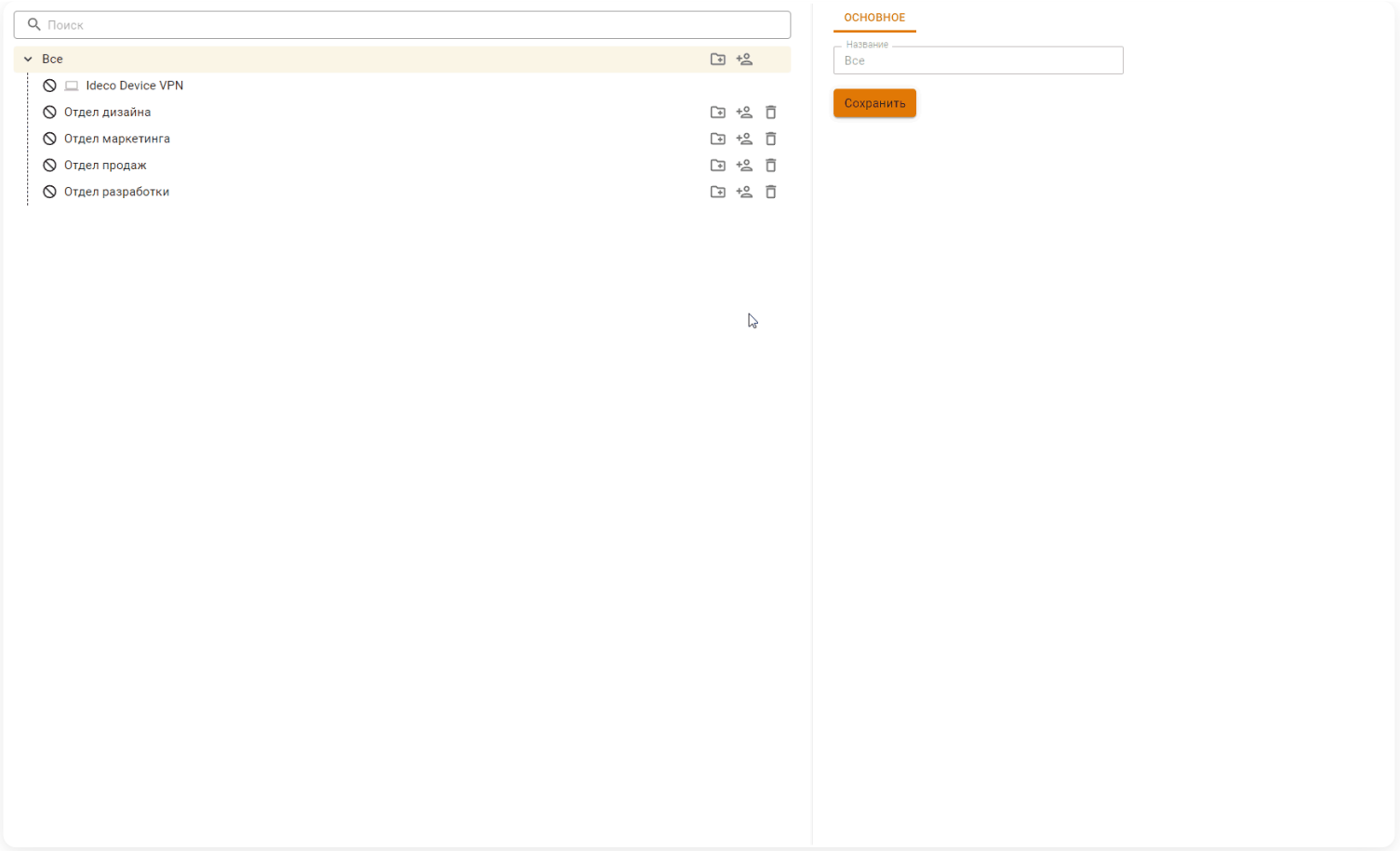
- **Имя пользователя** - имя пользователя. Например, Иванов Иван. Максимальное количество символов - 128.
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - пароль, который содержит комбинацию цифр и букв.
- **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 разделе **Пользователи → Авторизации → IP и MAC авторизация Ideco NGFW.

4. Нажмите **Добавить**.

Пользователь вне групп

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

2. Нажмите :



3. Заполните поля:

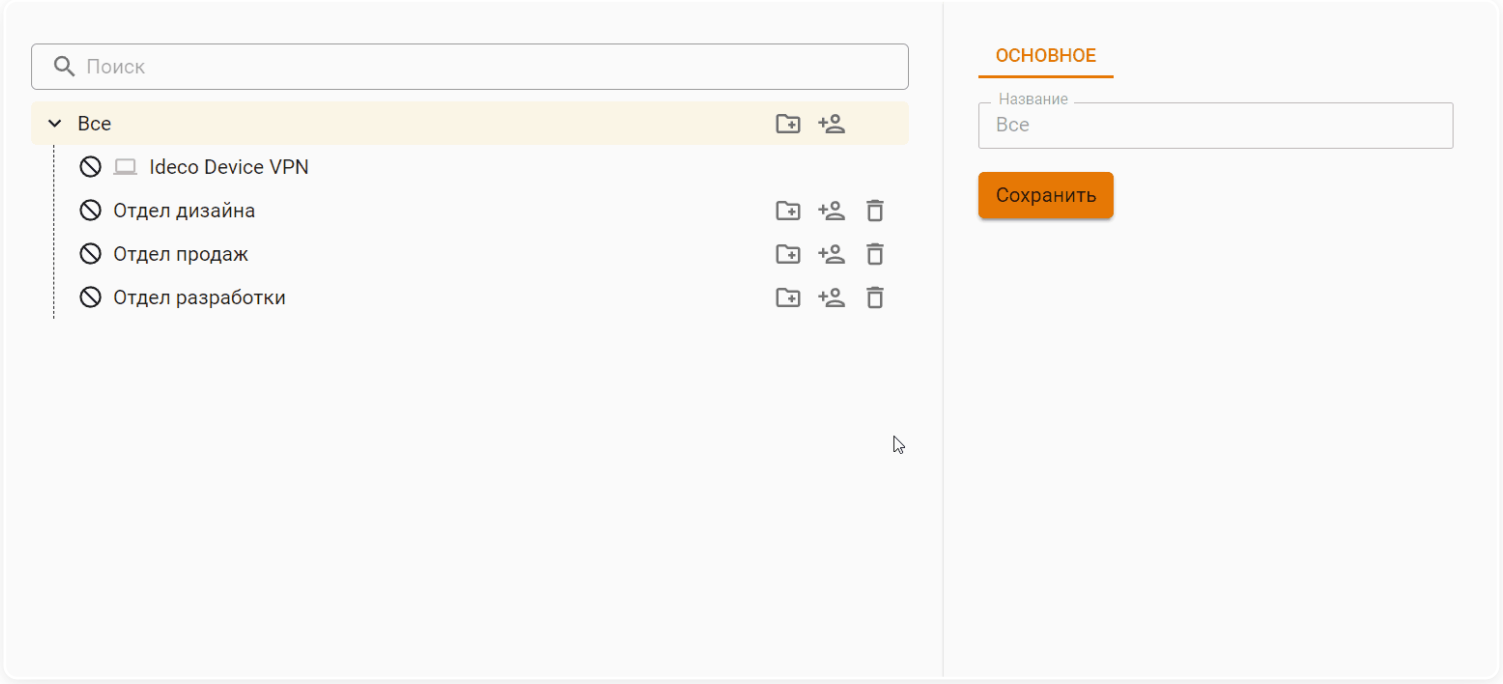
- **Имя пользователя** - имя пользователя. Например, Иванов Иван. Максимальное количество символов - 128.
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - пароль, который содержит комбинацию цифр и букв.
- **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 разделе **Пользователи → Авторизации → IP и MAC авторизация Ideco NGFW.

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, импортированных из Active Directory, проверка пароля осуществляется средствами Active Directory.

Рекомендации к созданию сложности паролей

Доступна автоматическая генерация пароля!

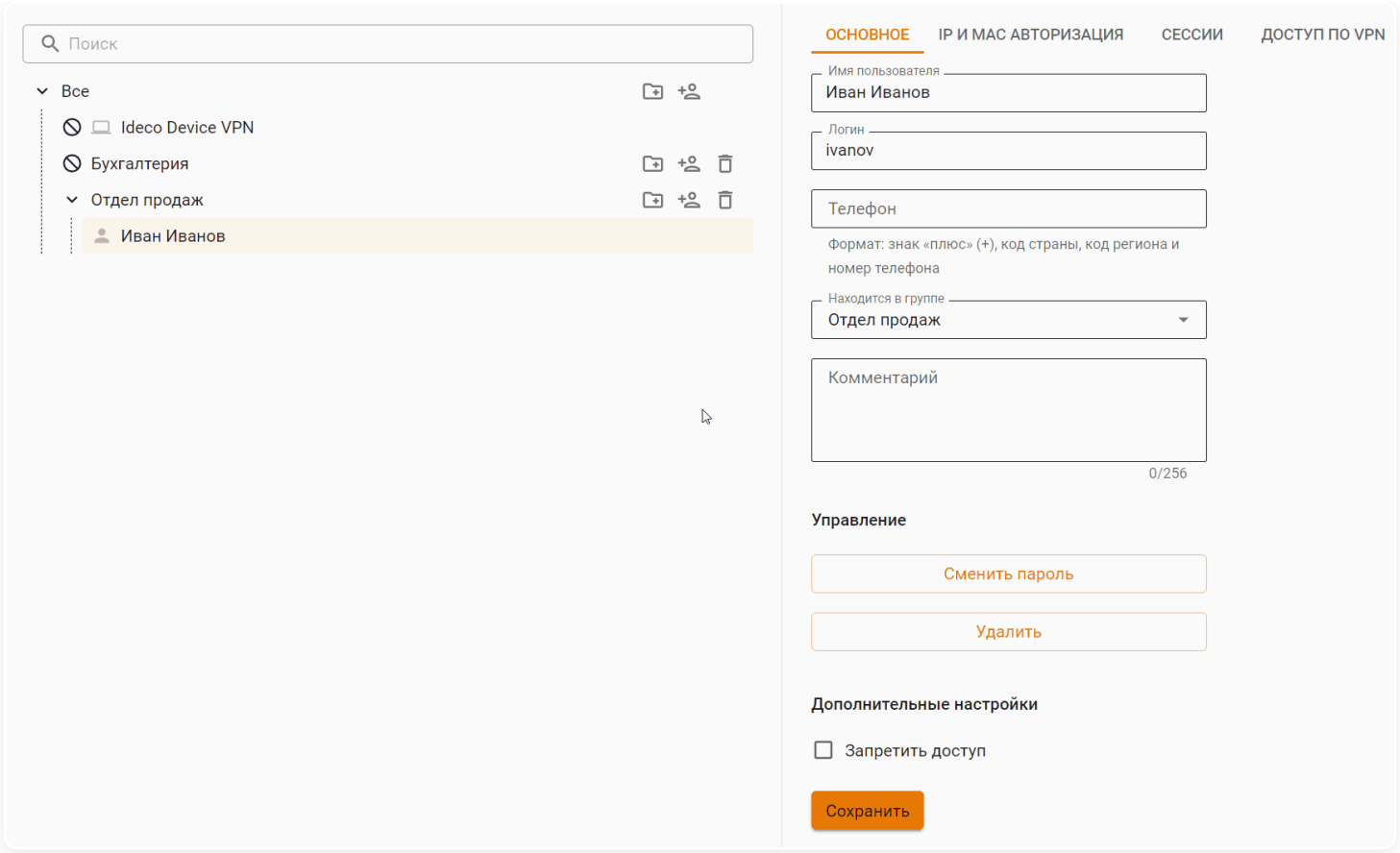
- Минимальная длина - 12 символов.
- Использование строчных и заглавных латинских символов.
- Использование цифр и специальных символов.

Создать пользователя Ideco NGFW в группу Active Directory нельзя. Если требуется добавить дополнительного пользователя в группу Active Directory, это необходимо делать в дереве пользователей на контроллере домена.

Удаление учетной записи пользователя или группы

Реализовано два варианта удаления:

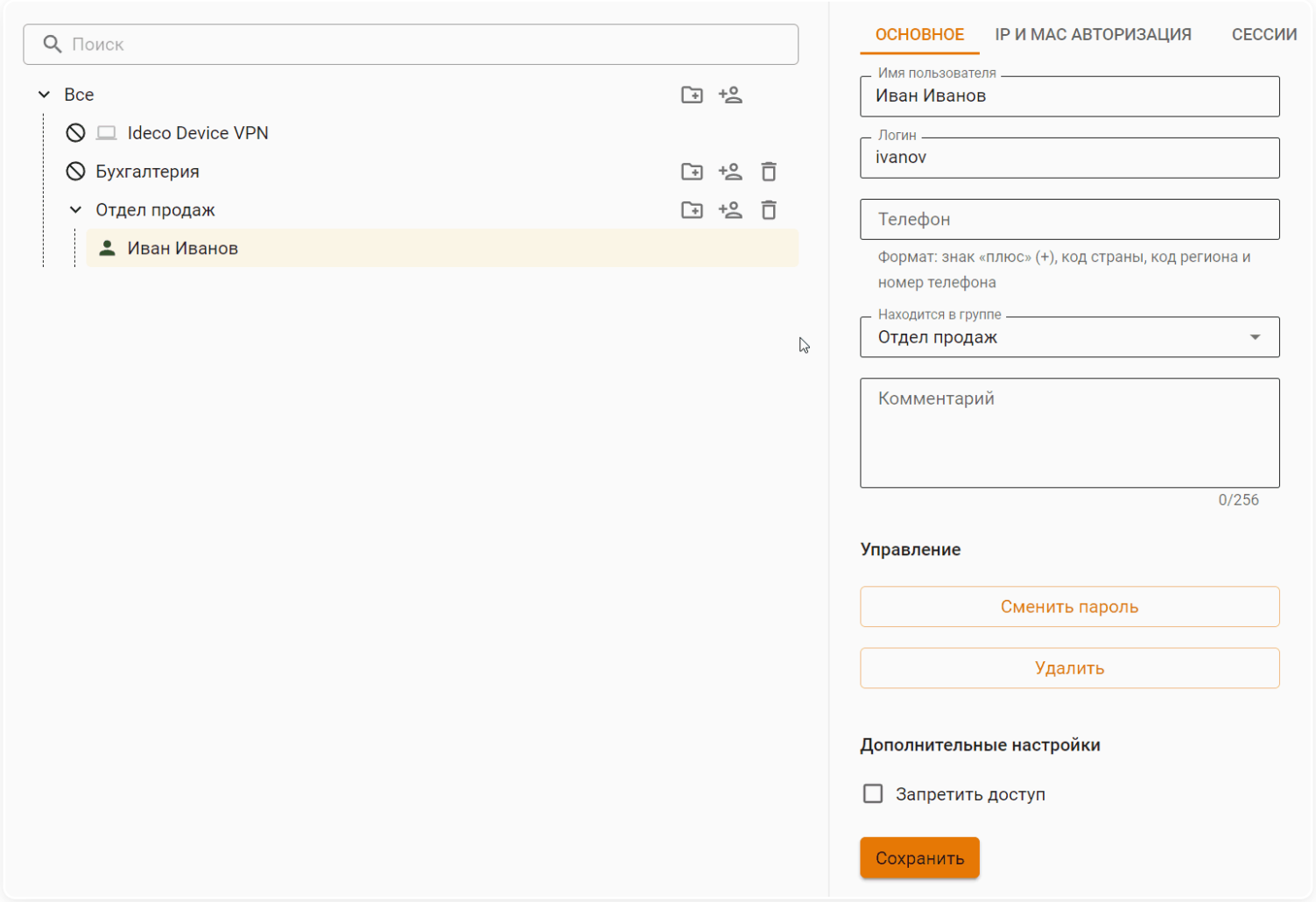
- Наведите курсор на пользователя и нажмите на .
- Нажмите на **Удалить** на вкладке **Основное**:



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.

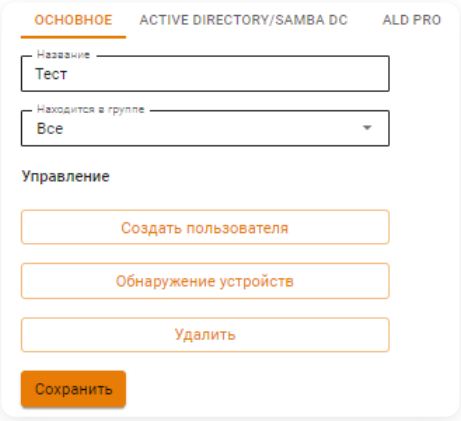
Настройка пользователей

Чтобы изменить параметры учетной записи 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. Настройки, заданные для группы, автоматически применяются ко всем ее участникам.

Основное



- **Изменить название и вложенность группы**. Для этого в соответствующем поле введите новое название и укажите группу, в которую требуется переместить эту группу;
- **Создать пользователя**. При нажатии на одноименную кнопку появится форма создания пользователя;
- **Обнаружение устройств**. При нажатии на одноименную кнопку откроется раздел Обнаружение устройств;
- **Удаление группы**. Вместе с группой удаляются учетные записи пользователей группы и привязки по IP- и MAC-адресам.

Active Directory/Samba DC

Категория содержит информацию об имени домена и типе группы. Процесс настройки синхронизации с Active Directory/Samba DC и импорт пользователей описан в статье Интеграция с Active Directory/Samba DC.

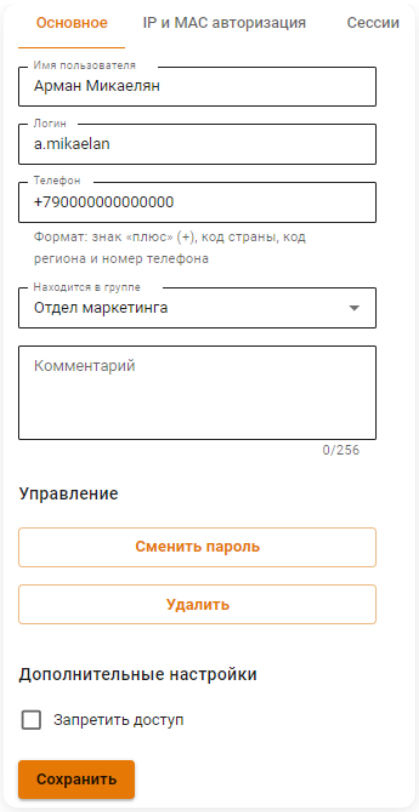
ALD Pro

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 пользователей

Основное

Основные настройки включают параметры, определяющие статус учетных записей пользователя. Базовые параметры:



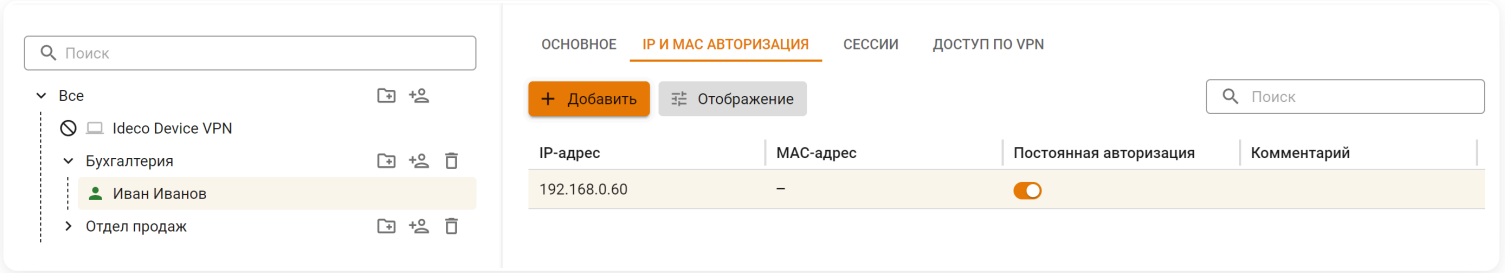
- **Имя пользователя** - имя пользователя, например, Иванов Иван. Максимальное количество символов - 128;
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32;
- **Телефон** - телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона;
- **Находится в группе** - используйте это поле для перемещения пользователя в другую группу;
- **Запретить доступ** - при установке этого флага пользователь не сможет авторизоваться, соответственно - пользоваться ресурсами интернета, почтой и личным кабинетом.

Для пользователей из Active Directory на вкладке **Основное** нельзя редактировать имя, логин, телефон, менять группу или пароль.

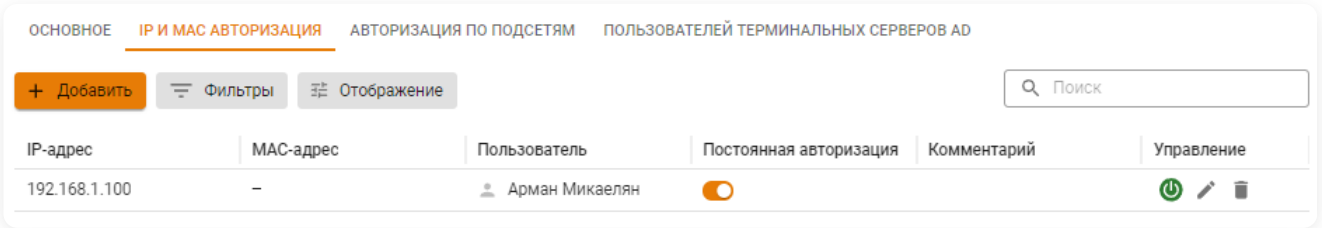
IP и MAC авторизация

Категория содержит правила авторизации по IP и MAC, созданные для определенного пользователя в двух разделах:

- **Пользователи → Учетные записи → IP и MAC авторизация**:



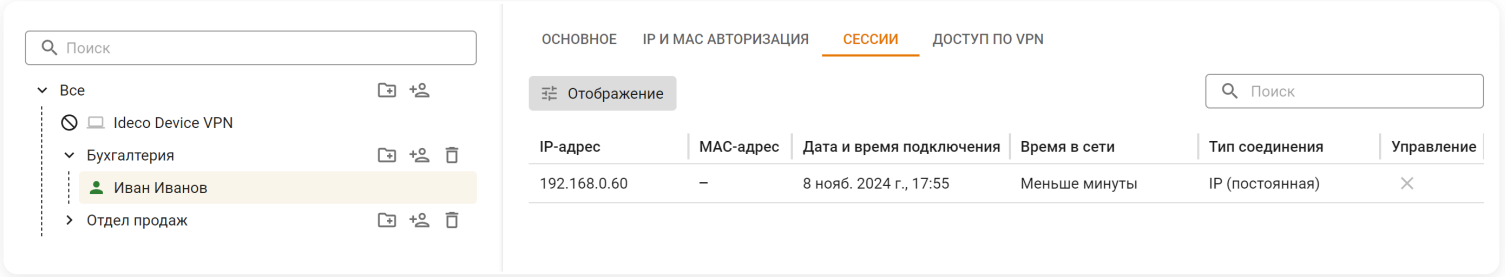
- **Пользователи → Авторизации**:



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

Сессии

Содержит таблицу с информацией обо всех активных сессиях пользователях:



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 разделе **VPN-подключения** → **Доступ по VPN**.

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

Авторизация пользователей

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 с возможностью контроля его трафика оно должно быть авторизовано на NGFW под учетной записью пользователя.

Особенности авторизации пользователей в Ideco NGFW:

- Количество приобретенных по лицензии учетных записей ограничивает число авторизованных пользователей.
- Сессия авторизации учетной записи привязана к IP-адресам хостов на протяжении действия сессии.
- Неавторизованный на NGFW хост не имеет доступа во внешние сети.
- Сессии авторизации пользователя, не проявляющего активность, завершаются по тайм-ауту и могут быть заняты новыми сессиями пользователей.

Для настройки автоматической авторизации пользователей при входе в систему воспользуйтесь статьей.

Общая информация

Все виды авторизации на Ideco NGFW являются IP-based (работают на основе IP-адреса хоста), и любая сессия авторизации привязана к IP-адресу хоста, с которого она установлена.

Под одной пользовательской учетной записью возможна одновременная авторизация **до пяти устройств**. При авторизации шестого устройства будет автоматически разорвана первая сессия. Например:

При авторизации по VPN

Если при авторизации первой сессии использовался VPN, включая Ideco Client, то при попытке входа в шестую сессию пользователь будет авторизован, а первая сессия будет автоматически разорвана.

При авторизации по IP, MAC, IP+MAC, WEB, NTLM, Ideco Agent, Log, Kerberos

Если в первой сессии использовались методы авторизации IP, MAC, IP+MAC, WEB, NTLM, Ideco Agent, Log, Kerberos, то в шестой сессии пользователь проходит авторизацию. При этом статус первой сессии в разделе **Сессии пользователей**. Это означает, что сессия вышла за пределы лицензии и будет автоматически разорвана.

Если разорвать шестую сессию, то первая сессия снова станет активной, а иконка исчезнет.
Сессия пользователя автоматически завершается при неактивности (отсутствии соединений с интернетом) в течение указанного в настройках времени (кроме подключений по VPN).

Трафик может генерировать и сама операционная система без участия пользователя (например, телеметрия Windows). Из-за этого тайм-аут для пользователя будет постоянно сбрасываться.

Время автоматического завершения сессии пользователя можно изменить с помощью настройки **Тайм-аут отключения** в разделе **Пользователи → Авторизация**:



Для применения нового тайм-аута отключения требуется перезагрузка Ideco NGFW.

Также можно авторизовать пользователей, которые подключаются по VPN с помощью протоколов IPsec IKEv2, SSTP, L2TP IPsec, PPTP. Инструкция по запуску PowerShell скриптов представлена в статье.

Полезные ссылки

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

Веб-аутентификация

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

Список служб для других разделов доступен по ссылке.

Веб-аутентификация в Ideco NGFW - тип авторизации, который предполагает, что отправленный через веб-браузер запрос неавторизованного пользователя будет переадресован на страницу авторизации Ideco NGFW. 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;
- 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.

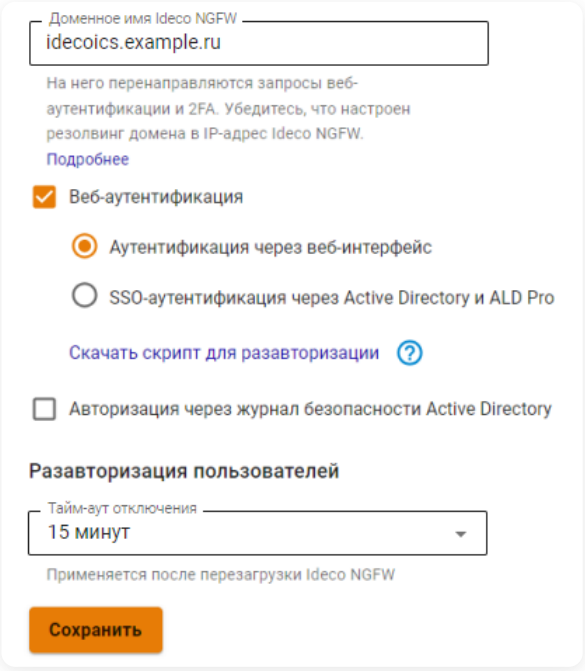
Рекомендуемые настройки для корректной работы веб-аутентификации:

- При входе на HTTPS-сайт пользователь должен подтвердить доверие к сертификату Ideco NGFW, либо сертификат должен быть добавлен в доверенные корневые центры сертификации на устройстве (например, через политики домена);
- Рекомендуется указывать в качестве DNS-сервера на компьютерах и устройствах локальной сети IP-адрес локального интерфейса Ideco NGFW.

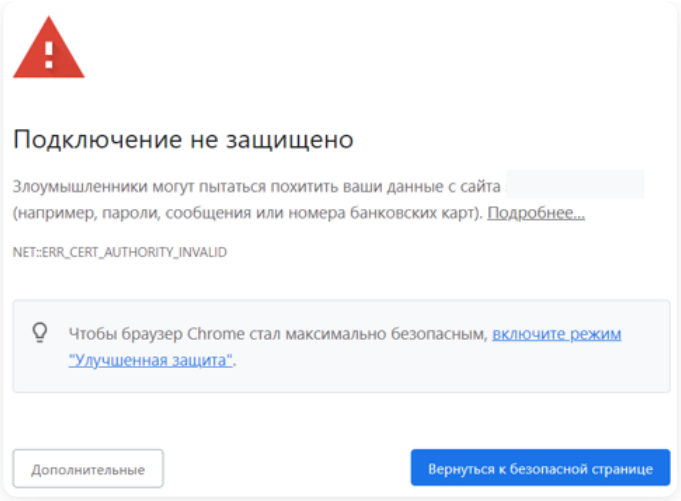
Аутентификация через веб-интерфейс

Чтобы настроить авторизацию через веб-интерфейс, выполните действия:

1. В разделе **Пользователи** → **Авторизация** выберите пункты **Веб-аутентификация** → **Аутентификация через веб-интерфейс**:



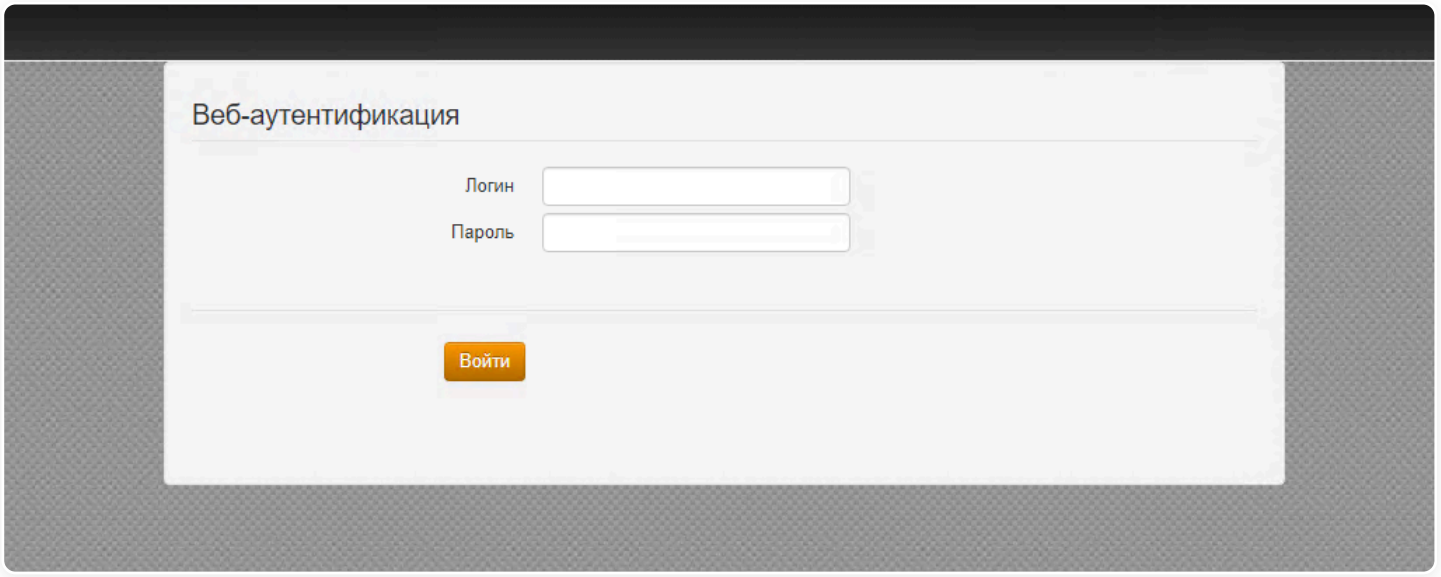
После заполнения поля **Имя домена** и сохранения настроек будет выдан Let's Encrypt сертификат. Пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



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

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

2. Откройте веб-браузер с устройства пользователя. Должно появиться окно авторизации, где необходимо ввести логин и пароль от созданной на Ideco NGFW 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**

IP и MAC авторизация

В Ideco NGFW можно создать правила авторизации по IP, MAC и IP+MAC.

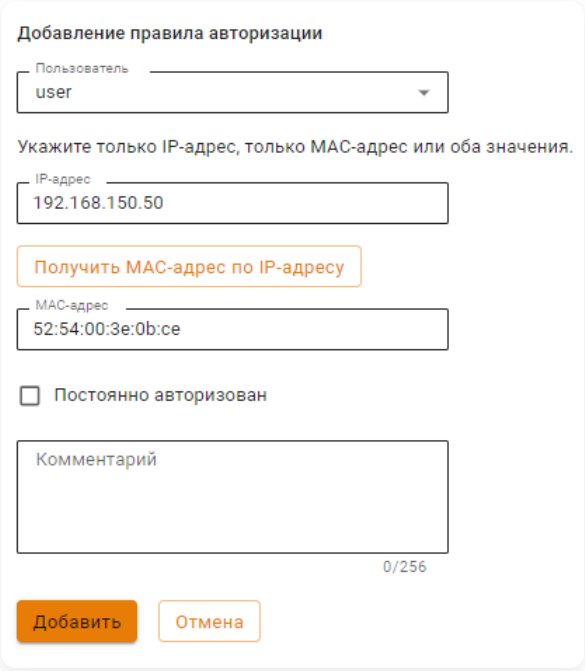
Правила **IP и MAC авторизации** создают аналогичную привязку в DHCP-сервере Ideco NGFW. Но если одни и те же IP- и MAC-адреса будут использоваться во включенных правилах DHCP-сервера, то правила DHCP-сервера будут выполняться в первую очередь.

Созданные в разделе **Авторизация → IP и MAC авторизация** правила отражаются в карточке пользователя.

Для настройки IP и MAC авторизации выполните действия:

1. В разделе **Авторизация → IP и MAC авторизация** нажмите **Добавить**.

2. Создать правило привязки **IP и MAC авторизации**:



При наличии большого количества правил привязки в таблице воспользуйтесь кнопкой **Фильтры**.

3. Если требуется обеспечить непрерывный доступ в интернет, установите флаг **Постоянно авторизован**. 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.

Статьи об авторизации пользователей только по IP- или MAC-адресу:

Авторизация по IP-адресу

Авторизация по MAC-адресу

Авторизация по IP-адресу

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 широковещательных доменах и требуют доступ в интернет.

Если устройством является маршрутизатор, в котором включен SNAT, при авторизации его внешнего IP на NGFW все пользователи за этим маршрутизатором получат доступ в интернет.

Пользователи, которые находятся за маршрутизатором в локальной сети NGFW, не могут авторизоваться по IP+MAC, так как маршрутизатор не обрабатывает трафик уровня L2.

Если настроена авторизация по IP-адресу, то этот IP не будет выдаваться DHCP.

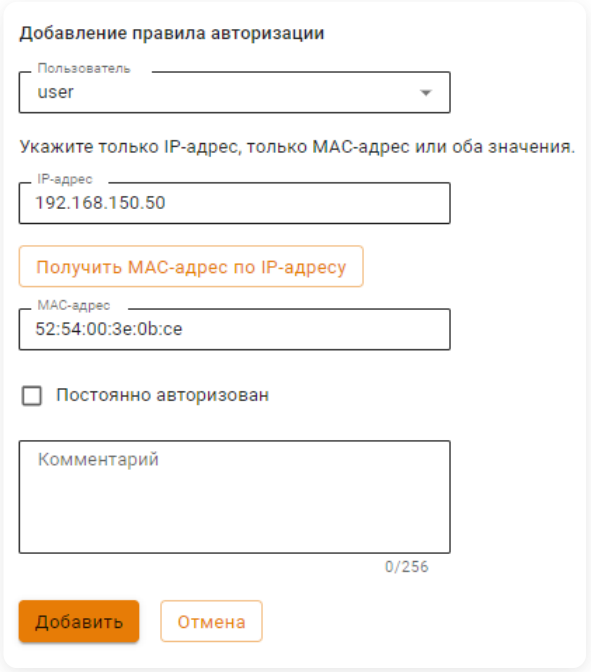
Настройка авторизации по IP

Для авторизации пользователя по IP-адресу выполните действия:

1. Создайте пользователя.

2. Перейдите в раздел **Пользователи** → **Учетные записи** → **Карточка пользователя** → **IP и MAC авторизация** или **Пользователи** → **Авторизация** → **IP и MAC авторизация**.

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 пользователя и IP Ideco NGFW в одной подсети.

Рекомендации по использованию авторизации по IP-адресу:

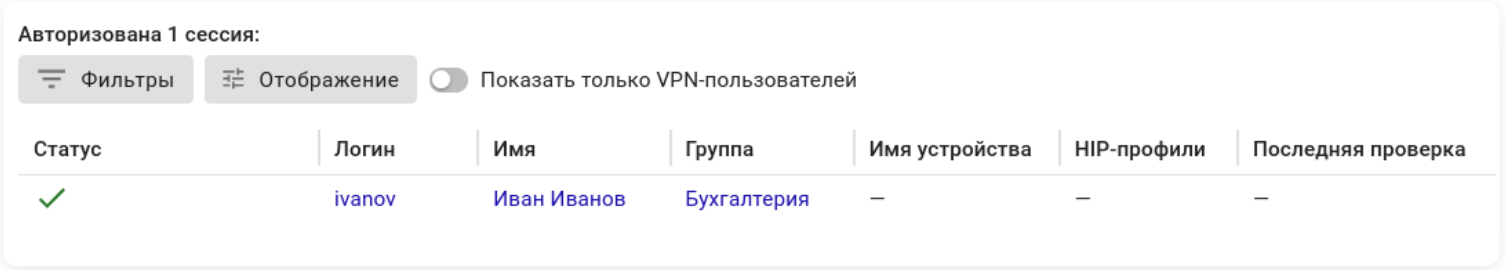
- Настройте для пользователя, которым является сетевое оборудование, **Постоянную авторизацию**. Это позволит NGFW создать сессию, а сетевому оборудованию не потребуется делать запрос в интернет;
- Настройте статический IP-адрес или DHCP с привязкой по IP-адресу. Это требуется, например, для ресурсов, опубликованных через DNAT;
- Воспользуйтесь поиском устройств для автоматического создания пользователей при попытке выхода в интернет. Подробнее о настройке читайте 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 NGFW 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 AC-адресу

Этот тип авторизации подойдет для тех устройств, у которых время от времени меняется местоположение между локальными сетями внутри организации (например, рабочие ноутбуки сотрудников) или сетевых устройств, на которых не настроена привязка IP+MAC и выдается IP-адрес через HCP .

Для авторизации пользователя на NGFW по MAC-адресу оба устройства должны находиться в одном широковещательном домене, а NGFW должен выступать шлюзом для устройств.

> Пользователи, находящиеся за роутером в локальной сети NGFW, 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 и пользователь находились в одном L2-сегменте сети.

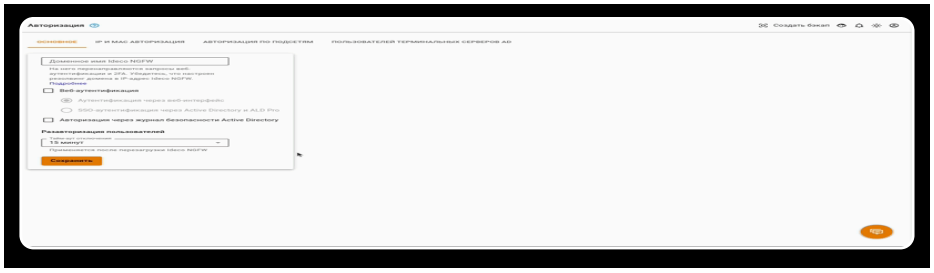
Настройка авторизации по AC

Для авторизации пользователя по MAC-адресу выполните действия:

. знайте MAC-адрес устройства. Для этого в командной строке Windows введите `i con i a ind t dd e` или `i con i a`



м домене. Для этого в разделе **правление сервером** → **Терминал** веб-интерфейса NGFW введите команду `i nei h`:



Эта команда выводит AP-т аблицу NGFW. Наличие записи с MAC-адресом устройства и статусом EACHABLE - марк ер L2-доступности между NGFW и устройством пользователя.

. Создайте правило-связку **Пользователь -- AC-адре** в разделе **Пользователи** → **Авторизация** → и **AC авторизация**.



> Для MAC-адресов невозможно настроить постоянную авторизацию, т. к. для создания авторизованной сессии необходим IP-адрес.

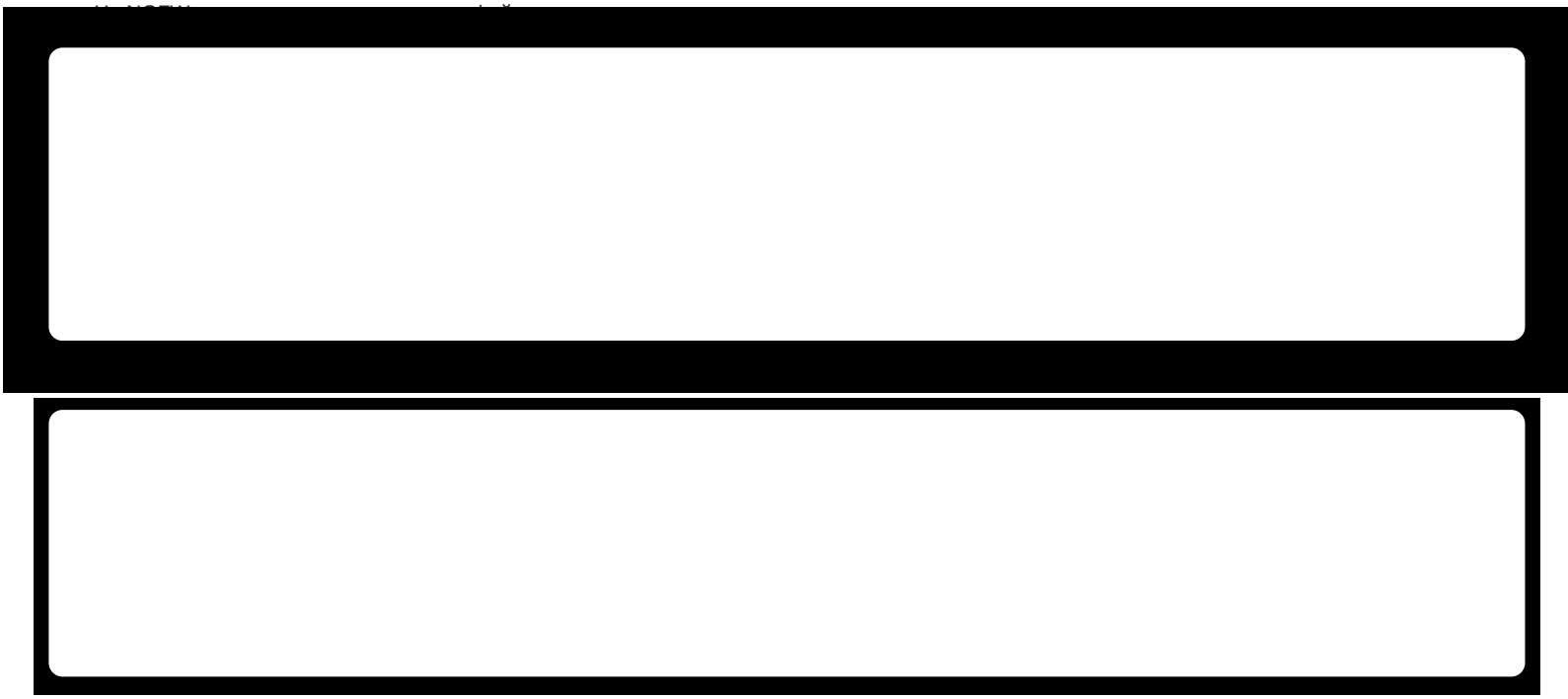
екомендуем использовать MAC-авторизацию в комбинации с ВР-серв ером.

Поведение AC-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 рекомендуем использовать авторизацию по MAC-адресу.

Для авторизации по MAC настройте ВР-серв ер (собственный или на NGFW). В раздаваемых реквизитах шлюзом должен выступать локальный интерфейс NGFW.

Пример Пользователю `u e` понадобилось переместиться с ноутбуком между локальными сетями:



- по льзователя одна активная сессия в разделе **Сессии пользователей**:



При переходе пользователя из одной локальной сети в другую ему выдаются другие сетевые реквизиты от ВР-серв ера, в которых шлюзом указан NGFW. 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 реквизиты от ВР-серв ера и получите новые с помощью команд:

- Windows - `i con i e ea e i con i ene`
- Lin x - `udo dhc ient -`.

Настройка авторизации по AC-адресу для сетево о принтера и друи сетевы устройств

Сетевые устройства, которым необходим доступ в интернет, должны быть авторизованы на NGFW. Такие устройства можно назвать статическими, для них подойдет авторизация по MAC-адресу.

т обы авторизовать сетевой принтер, необходимо создать пользователя на NGFW вручную или через Обнаружение устройств:



В разделе **Пользователи** → **Авторизация** → и **AC авторизация** для сетевого принтера необходимо создать правило **Пользователь -- AC-адрес**:



При обнаружении активности от сетевого принтера или другого устройства сессия пользователя появится в **ониторин** → **Се ссии пользователей**:



Опция **андомизация AC-адреса** будет мешать при авторизации мобильного устройства по MAC-адресу. екомендуется эту опцию отключать либо использовать другие типы авторизации (например, Веб-аутентификацию

Авторизация по подсетям

Чтобы не регистрировать каждое устройство как отдельного пользователя NGFW и не задавать для него факторы авторизации, создайте правило на вкладке **Пользователи** → **Авторизация** → **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.

Будьте внимательны при создании правил Авторизации по подсетям! Любое **пересечение сетей** при авторизации может привести к проблемам. Например:

- на вкладке **Авторизация по подсетям** для разных пользователей созданы правила с пересекающимися сетями;
- в разделе **Пользователи** → **Учетные записи** создан пользователь с IP-адресом из подсети в правилах **Авторизации по подсетям**;
- на вкладке **VPN-подключения** → **Правила выдачи IP-адресов** добавлена привязка к IP-адресам из подсети в правилах **Авторизации по подсетям**;
- на вкладке **Авторизация по подсетям** создано правило с подсетью, частично пересекающейся с диапазоном IP-адресов для выдачи в разделе **Сервисы** → **DHCP**.

Работа DHCP возможна в случае, если диапазон выдачи IP-адресов не превышает количество адресов в подсети, указанной в правиле **Авторизация по подсетям**.

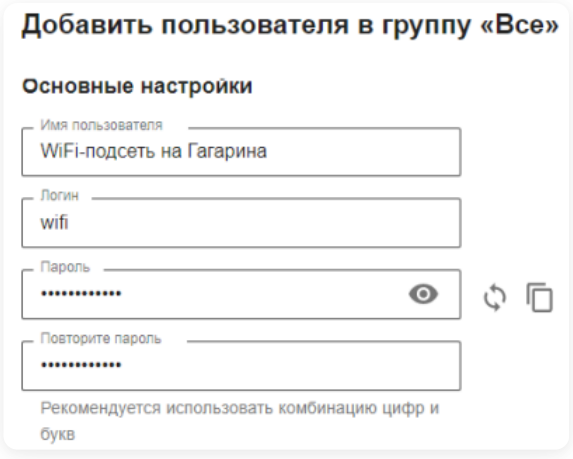
Пример использования

Есть Wi-Fi-подсеть 192.168.10.0/24, для устройств которой требуется авторизация.

Для создания правила авторизации выполните действия:

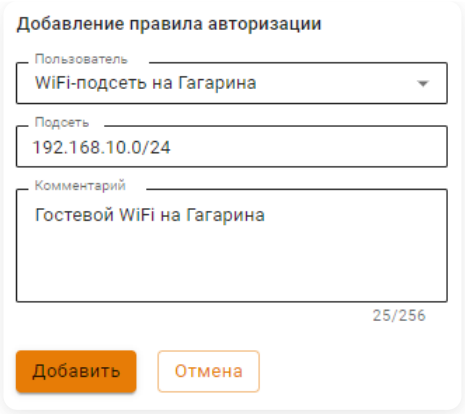
1. Перейдите в раздел **Пользователи** → **Учетные записи** и нажмите .

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



3. Перейдите на вкладку **Пользователи** → **Авторизация** → **Авторизация по подсетям** и нажмите **Добавить**.

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



- **Пользователь** - выберите созданного в п. 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.

Авторизация пользователей терминальных серверов

Особенности работы для пользователей терминальных серверов AD:

- Пользователи имеют один IP-адрес, поэтому правила **Файрвола** и **Контроля приложений**, примененные для одного пользователя, будут действовать на всех;
- **Контент-фильтр** распознает этих пользователей, поэтому его правила применяются для отдельных пользователей и групп;
- Сессии авторизации не создаются, так как пользователи терминальных серверов обращаются с одним IP-адресом;
- Работает только при прямых подключениях к прокси;
- В **Журнале веб-доступа** не отображаются события по терминальным пользователям.

Для авторизации пользователей терминальных серверов установите флаг **Авторизовать пользователей терминальных серверов** и укажите IP-адрес терминального сервера в одноименной строке. Отправляющие запросы с этих IP-адресов пользователи считаются пользователями терминальных серверов и авторизуются через SSO.

Обратите внимание, что при большом количестве пользователей на сервере терминалов может потребоваться увеличить количество одновременных сессий с одного адреса в дополнительных параметрах безопасности.

Возможна **раздельная авторизация пользователей** терминального сервера, работающего под управлением ОС Windows Server, с помощью авторизации через SSO. При этом сам сервер по IP авторизовывать не нужно.

Для раздельной авторизации пользователей терминального сервера:

- На сервере терминалов настройте **Remote Desktop IP Virtualization**.
- На сервере Ideco NGFW настройте авторизацию пользователей через SSO.

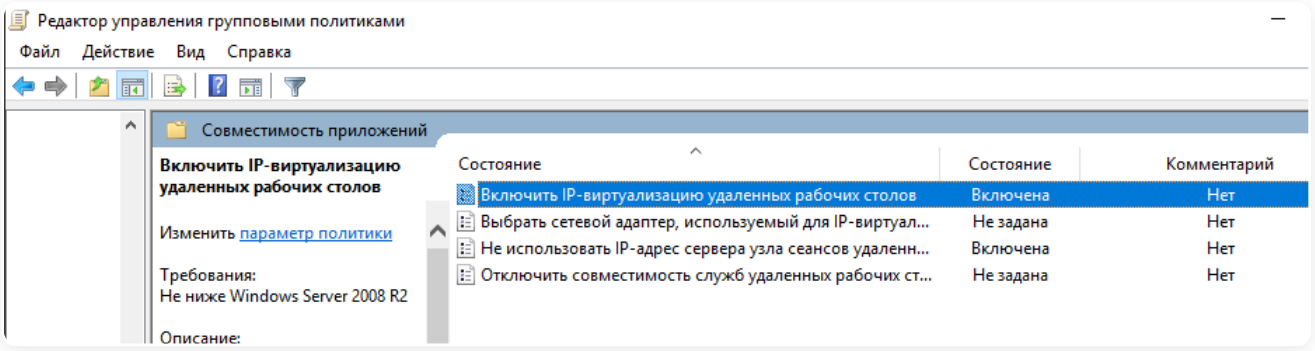
> Авторизация пользователей терминального сервера по логам контроллера домена AD пока не реализована.

Настройка Remote Desktop IP Virtualization на Windows Server 2012

Для работы функции Remote Desktop IP Virtualization на одном из Windows-серверов должна быть добавлена роль DHCP-сервера (с другими DHCP-серверами эта функция может работать некорректно) и выделена область IP-адресов для пользователей терминального сервера.

В **Редакторе управления групповыми политиками** перейдите по пути: **Computer Configation → Policies → Administrative Templates → Windows Components → Remote Desktop Service → Remote Desktop Session Host → Application Compatibility**.

Путь для русскоязычной версии: **Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Служба удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Совместимость приложений**. Включите опцию **Turn on Remote Desktop IP Virtualization (Включить IP-виртуализацию удаленных рабочих столов)** в групповой политике с параметром **Per Session (Для сеансов)**:



Рекомендуется включить опцию **Do not use Remote Desktop Session Host server IP address when virtual IP address is not available (Не использовать IP-адрес сервера узла сеансов удаленных рабочих столов, если виртуальный IP-адрес недоступен)**.

Командой `gpupdate /force` выполнить обновление всех политик.

Проверьте изменение настроек командой в PowerShell:

```
Get-WmiObject -Namespace root\cimv2\TerminalServices -query "select * from Win32_TSVirtualIP"
```

Значения:

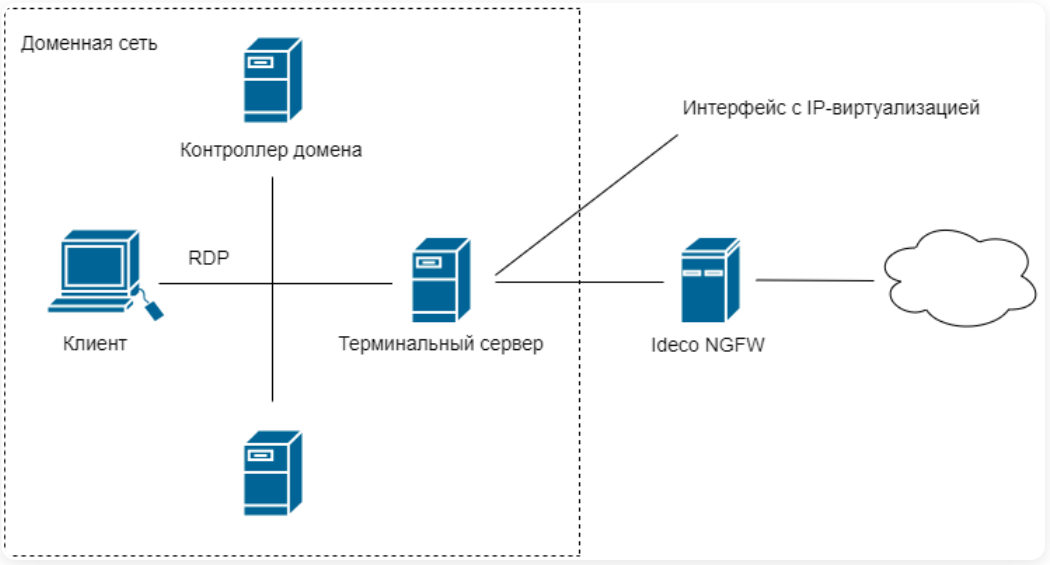
- `VirtualIPActive = 1` - вкл. виртуализация;

- `VirtualIPMode=0` - для сессии.

Настройка Remote Desktop IP Virtualization на Windows Server 2022

> Не подтверждено, что Remote Desktop IP Virtualization работает на Windows Server 2019. Рекомендуем обновить терминальный сервер до Windows Server 2022.

Условия



1. Windows Server 2022 с ролью контроллера домена;

2. Windows Server 2022 с ролью терминального сервера. Отдельный сервер опционален, можно добавить эту роль серверу с ролью контроллера домена;

3. Ideco NGFW, введен в домен опционально;

4. Клиентские Windows-машины, введенные в домен;

5. (опционально) Windows Server 2022 с ролью DHCP-сервера для динамической раздачи виртуальных IP-адресов. Конфликтует в ролью терминального сервера, поэтому DHCP-сервер и терминальный сервер должны быть разными машинами. DHCP-сервер используется на базе Windows Server. DHCP-сервер на Ideco NGFW, например, не подойдет.

Настройка

> Все настройки выполняются от имени администратора.

Установите все последние обновления Windows Server и перезагрузите серверы.

На сервере с ролью терминального сервера выполните следующие действия:

1. Отключите WinSock2. Переместите (рекомендуется) или удалите раздел реестра по указанному пути с помощью **Редактора реестра** (regedit):

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\AppId_Catalog\2C69D9F1

2. Включите компонент IPFilterBitmaps:

Добавление параметра через глобальную политику реестра с помощью Редактора реестра (regedit) (рекомендуется)

Путь: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

Ключ: IPFilterBitmaps

Тип: REG_DWORD

Значение: 1

Добавление параметра через групповую политику реестра с помощью Редактора реестра (regedit)

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAppSrv\VirtualIP

Ключ: IPFilterBitmaps

Тип: REG_DWORD

Значение: 1
3. Перезагрузите сервер.

4. Настройте IP-виртуализацию удаленных рабочих столов на сервере с ролью терминального сервера.

Далее описана настройка для режима **Для сеансов**, который выдает виртуальный IP-адрес каждой пользовательской сессии:

Через редактирование объекта WMI-инфраструктуры (глобальную политику реестра) в PowerShell (рекомендуется)

Значение для метода SelectNetworkAdapter - MAC-адрес сетевого интерфейса, который будет использоваться для IP-виртуализации. Выполните команду:

```
$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TSVirtualIP
$obj.SelectNetworkAdapter('52-54-00-00-90-01')
$obj.SetVirtualMode(0)
$obj.SetVirtualIPActive(1)
```

После выполнения команды убедитесь, что все параметры выставлены правильно, введя `$obj`.

Через групповую политику с помощью Редактора локальной групповой политики (gpedit.msc)

1. Перейдите в раздел **Политика Локальный компьютер → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Совместимость приложений**.

Путь для англоязычной версии: **Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Application Compatibility**.

2. Включите параметр политики **Включить IP-виртуализацию удаленных рабочих столов** с параметром **Для сеансов**.

Англоязычная версия: **Turn on Remote Desktop IP Virtualization** с параметром **Per Session**.

3. Включите параметр политики **Выбрать сетевой адаптер, используемый для IP-виртуализации удаленных рабочих столов** в параметр **IP-адрес с маской сетевого интерфейса, который будет использоваться для IP-виртуализации** (например, 192.168.100.200/24).

Англоязычная версия: **Select the network adapter to be used for Remote Desktop IP Virtualization** в параметр **IP adress and network mask corresponding to the network adapter to be used for Remote Desktop IP Virtualization**.

4. (опционально) Включите параметр политики **Не использовать IP-адрес сервера узла сеансов рабочих столов, если IP-адрес недоступен** (**Do not use Remote Desktop Session Host server IP address when virtual IP address is not available**).

5. Повторно перезагрузите сервер.

Настройте выдачу виртуальных IP-адресов:

{% cut "Для статической выдачи виртуальных IP-адресов на сервере с ролью терминального сервера" %}{# dlya-staticheskoj-vydachi-virtualnyh-ip-adresov-na-servere-s-rolyu-terminalnogo-servera}

Включите компонент IPPool. Через групповую политику реестра с помощью **Редактора реестра** (regedit) добавьте параметр:

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAPPSrv\VirtualIP

Ключ: IPPool

Тип: REG_SZ (строковый параметр)

Значение: `%SystemRoot%\system32\TSVIPool.dll`

Настройте статический диапазон IP-адресов:

1. Создайте новый раздел IPPool по пути HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAPPSrv\VirtualIP через групповую политику реестра с помощью **Редактора реестра** (regedit).

2. Добавьте в новый раздел параметры типа REG_SZ (строковый параметр):

- Ключ Start, значение - начало диапазона IP-адресов (например, 192.168.100.200);
- Ключ End, значение - конец диапазона IP-адресов (например, 192.168.100.210);
- Ключ SubnetMask, значение - маска подсети (например, 255.255.255.0).

3. Перезагрузите сервер с ролью терминального сервера.

Для динамической выдачи виртуальных IP-адресов на сервере с ролью DHCP-сервера

Выдайте DHCP-серверу необходимые привилегии через групповую политику реестра с помощью **Редактора реестра»** (regedit):

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp

Ключ: RequiredPrivileges

Тип: REG_MULTI_SZ (многострочный параметр)

Значение:

```
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
```

Перезагрузите сервер с ролью DHCP-сервера.
В случае успешной настройки на интерфейс, выбранный для IP-виртуализации, при подключении клиентов будут выдаваться виртуальные IP-адреса, которые исходящие запросы будут использовать в качестве источника.

```
Локальный IPv6-адрес канала . . . : fe80::ac9e:64f3:5cba:891b%14
IPv4-адрес. . . . . . . . . . . . : 192.168.100.90(Основной)
Маска подсети . . . . . . . . . . : 255.255.255.0
IPv4-адрес. . . . . . . . . . . . : 192.168.100.161(Устаревший)
Маска подсети . . . . . . . . . . : 255.255.255.0
```

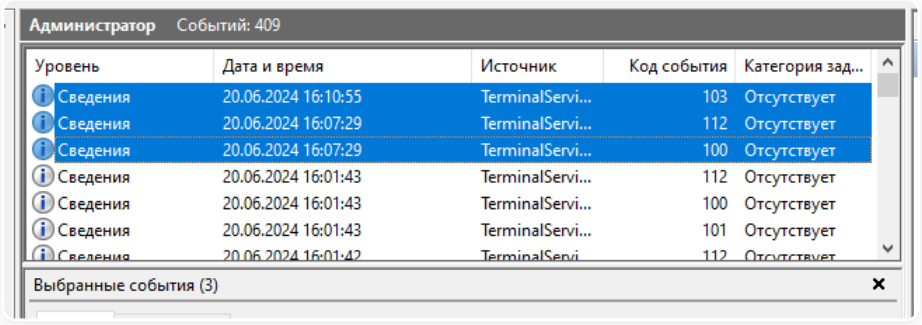
Диагностика

Виртуальные IP-адреса не выдаются

На сервере с ролью терминального сервера проверьте работоспособность службы IP-виртуализации. Для этого перейдите в раздел **Просмотр событий (локальный компьютер) → Журналы приложений и служб → Microsoft → Windows → Terminal Services-TSAppSrv-TSVIP → Администратор**.

Путь для англоязычной версии: **Event Viewer (Local) → Applications and Services Logs → Misrosoft → Windows → Terminal Services-TSAppSrv-TSVIP → Administrator**.

Успешно запущенная служба произведет события 100 и 112 после запуска и 103, 104 при подключении/отключении клиента:



В объекте WMI-инфраструктуры (независимо от вида настройки самой IP-виртуализации) в PowerShell выполните:

```
$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TSVirtualIP
$obj
```

Убедитесь, что параметр `IP.VirtualIPActive` = 1.

```
__PATH                          : \\WIN-RHQ28K71VT1\Root\CIMV2\TerminalServices:Win32_TSVirtual
                                  IP.VirtualIPActive=1
```

Если что-то отличается, убедитесь, что все инструкции по настройке выполнены правильно, а DHCP-сервер работает исправно. При необходимости выполните настройку заново рекомендуемыми способами.

Подключения используют основной IP-адрес терминального сервера

Использовать IP-виртуализацию будут только Windows-приложения, работающие на WinSock, то есть приложения, использующие протоколы TCP или UDP. ICMP-приложения вроде `ping` не будут использовать IP-виртуализацию.

Подключения будут использовать основной IP-адрес терминального сервера также в случае, когда запрашиваемый адрес недоступен (например, `Destination Unreachable`).

IP-виртуализация работает только для пользователей, подключенных к терминальному серверу через службу mstsc (**Подключение к удаленному рабочему столу**).

Двухфакторная аутентификация

Название службы раздела **Двухфакторная аутентификация**: `ideco-web-authd`.

Список служб для других разделов доступен по ссылке.

Двухфакторная аутентификация позволяет аутентифицировать пользователей только внешних сетей (VPN) с использованием второго фактора.

В Ideco NGFW реализовано три 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.

Для входа в личный кабинет Ideco NGFW с использованием **Мультифактора** необходим доступ в интернет.

Двухфакторная аутентификация для пользователей **RADIUS-сервера** работает только при авторизации через **Ideco Client**. Для этого нужно настроить двухфакторную аутентификацию на **RADIUS-сервере**, о настройке Ideco NGFW - в статье.

Настройки Ideco NGFW с разными типами аутентификации

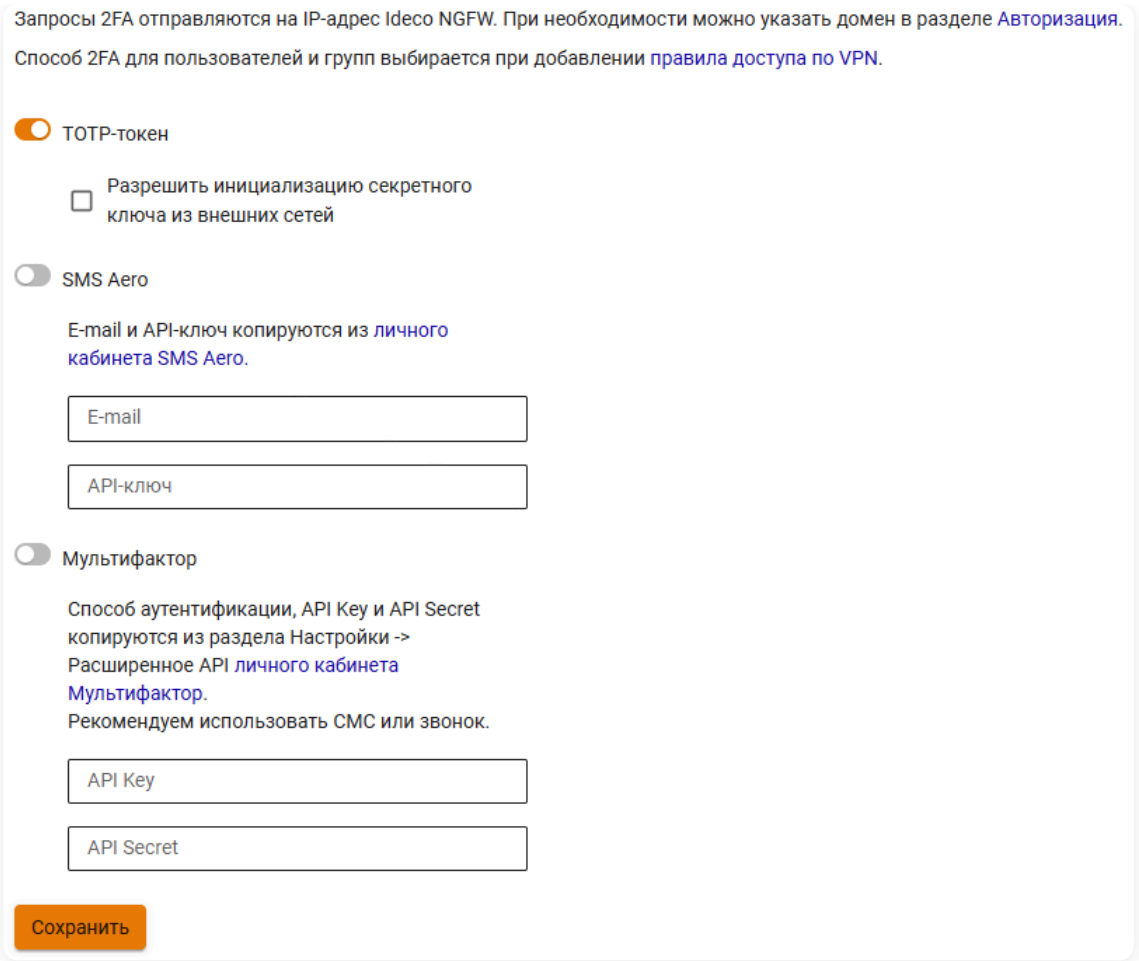
Для работы двухфакторной аутентификации выполните действия:

1. Укажите домен Ideco NGFW, чтобы на сервер перенаправлялись запросы двухфакторной аутентификации:

- Перейдите в раздел **Пользователи** → **Авторизация**.
- Включите веб-аутентификацию.
- Введите домен в поле **Доменное имя Ideco NGFW**.

2. Настройте VPN-подключение в разделе **Пользователи** → **VPN-подключения** → **Основное**, воспользовавшись инструкцией.

3. Перейдите в раздел **Пользователи** → **Двухфакторная аутентификация**. Включите необходимые типы аутентификации и заполните соответствующие поля:



TOTP-токен

Опция **Разрешить инициализацию секретного ключа из внешних сетей** разрешит генерацию QR-кода в личном кабинете пользователя из внешней сети.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW с использованием TOTP-токена смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

SMS Aero

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. Нажмите **Сохранить**.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW с использованием SMS Aero смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Мультифактор

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 его, отсканировав QR-код.

1. Заполните **API Key** и **API Secret**. Для этого скопируйте значение полей в личном кабинете пользователя Multifactor в разделе **Настройки** → **Расширенное API** → **Включить API**.

2. Нажмите **Сохранить**.

Для корректной работы двухфакторной аутентификации через Мультифактор необходимо обеспечить доступ к следующим подсетям:

- 37.220.160.0/21
- 46.235.184.0/21
- 93.93.88.0/21
- 78.41.104.0/21
- 185.17.168.0/22
- 212.193.144.0/20
- 195.208.30.60/30
- 195.209.64.0/21
- 195.209.80.0/20
- 195.208.64.0/20
- 195.209.75.0/25
- 195.209.74.0/24

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**.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW с использованием Мультифактора смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

4. Разрешите доступ по VPN нужным группам пользователей в разделе **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

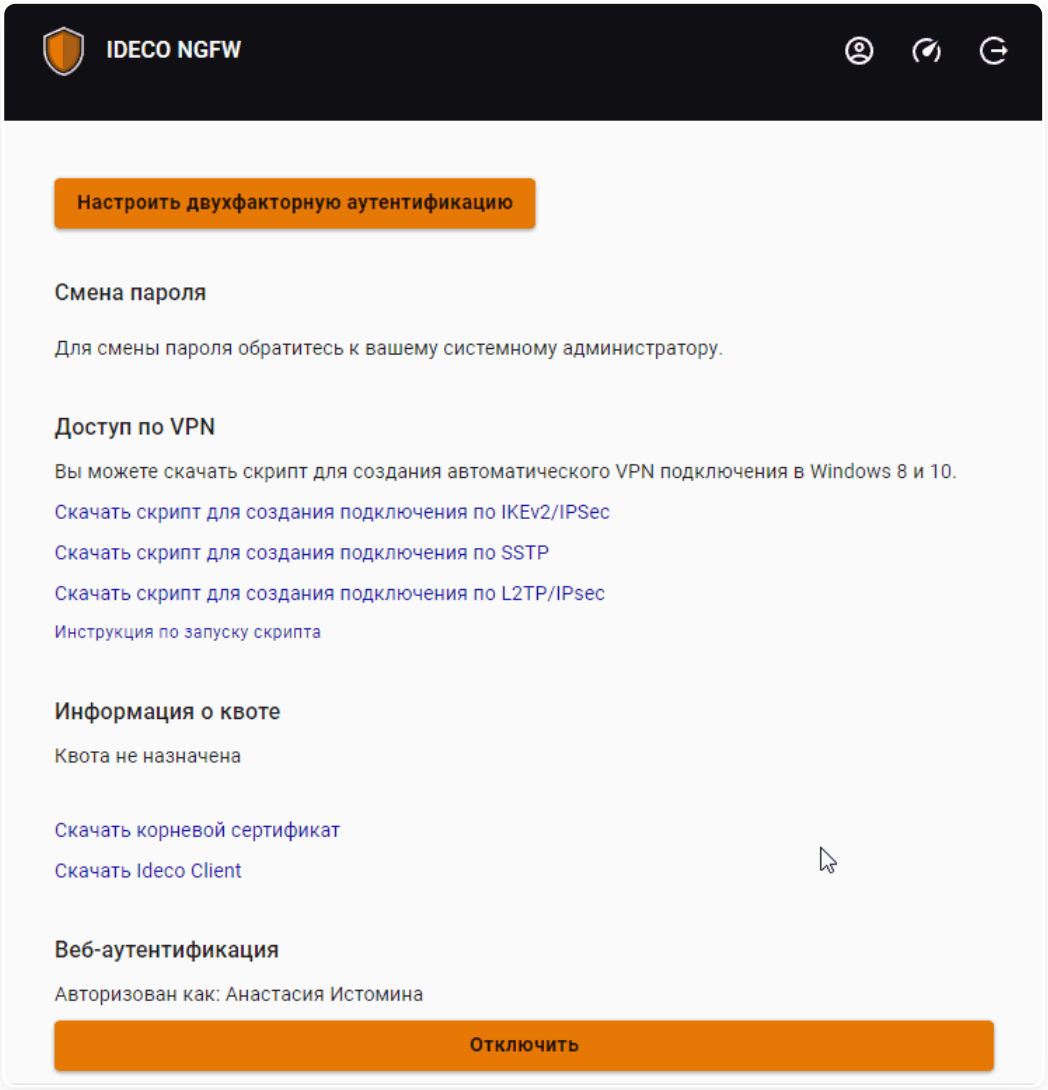
Для настройки двухфакторной аутентификации на устройстве пользователя воспользуйтесь инструкциями:

TOTP-токен

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Войдите в личный кабинет NGFW, указав логин и пароль пользователя.

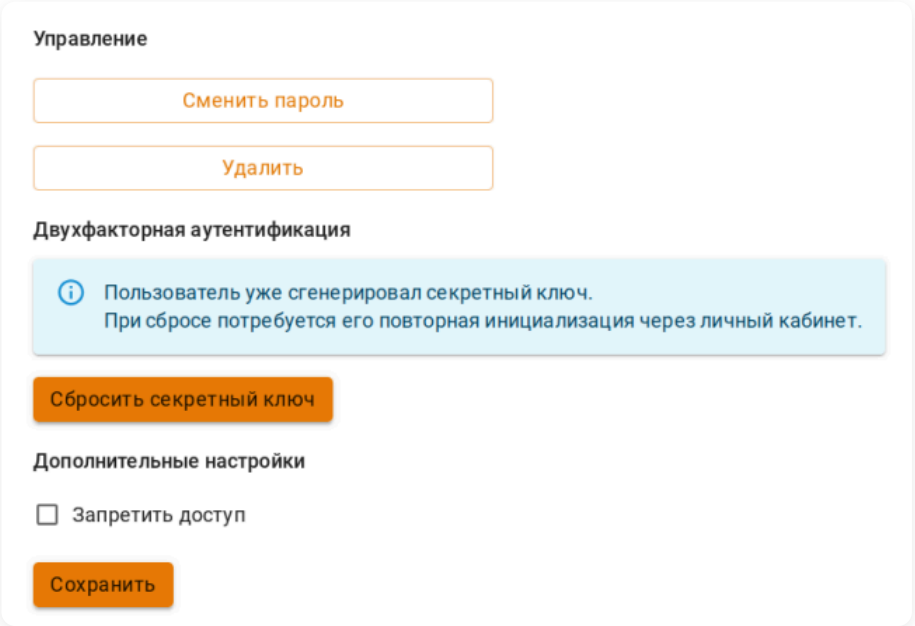
3. Нажмите кнопку **Настроить двухфакторную аутентификацию** и выберите **Сгенерировать QR-код**:



4. Войдите в приложение для аутентификации (Яндекс ID, Google Authenticator или Microsoft Authenticator и т.п.), отсканируйте 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.

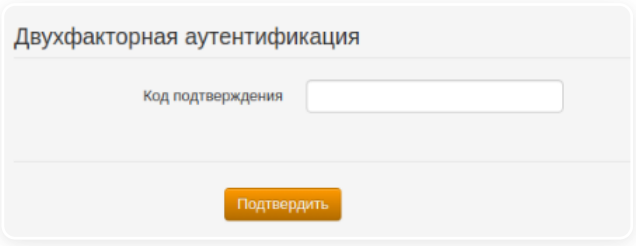
Если вернуться в личный кабинет, не отсканировав QR-код, то повторно он появится только после сброса секретного ключа в карточке пользователя.

Чтобы сбросить секретный ключ, перейдите в раздел **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 вы получили в приложении:



Особенности использования TOTP-токена:

- Для корректной работы необходимо, чтобы время на Ideco NGFW и устройстве пользователя было синхронизировано с точностью до минуты.
- Если секретный ключ был сброшен во время аутентификации пользователя и он не смог ее пройти, 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:

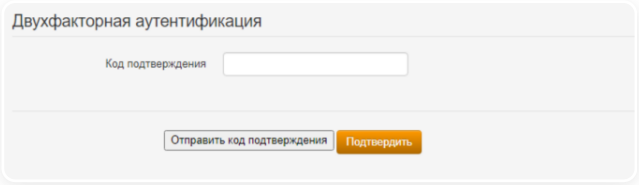
- Откройте параметры и перейдите в раздел **Сеть и Интернет** → **VPN** → **Настройка параметров адаптера**.
- Нажмите правой кнопкой мыши по созданному подключению и выберите **Свойства**.
- Перейдите на вкладку **Сеть**.
- Нажмите на **IP версии 4 (TCP/IPv4)** → **Свойства** → **Дополнительно**.
- Снимите флаг с пункта **Использовать основной шлюз в удаленной сети**.
- Нажмите **ОК**.

Для Ubuntu:

- Перейдите в раздел **Настройки** → **Сеть**.
- Откройте настройки VPN-подключения.
- Перейдите на вкладку **IPv4**.
- Установите флаг в пункте **Использовать это подключение для ресурсов этой сети**.

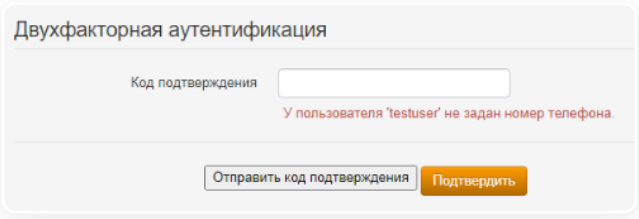
3. Включите созданное VPN-подключение.

4. Перейдете в браузер, откроется страница аутентификации:

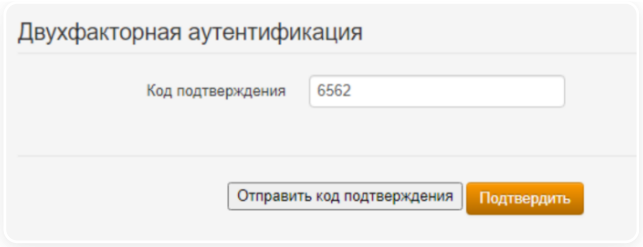


5. Нажмите **Отправить код подтверждения**. На номер телефона, указанный в учетной записи, придет SMS с кодом:

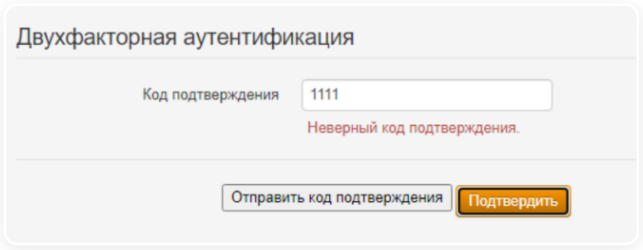
- Если номер телефона в карточке пользователя отсутствует, то на странице аутентификации появится предупреждение:



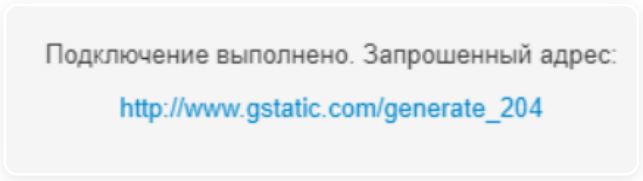
- Если номер телефона сохранен, то на указанный номер телефона поступит SMS. Введите код из SMS и нажмите **Подтвердить**:



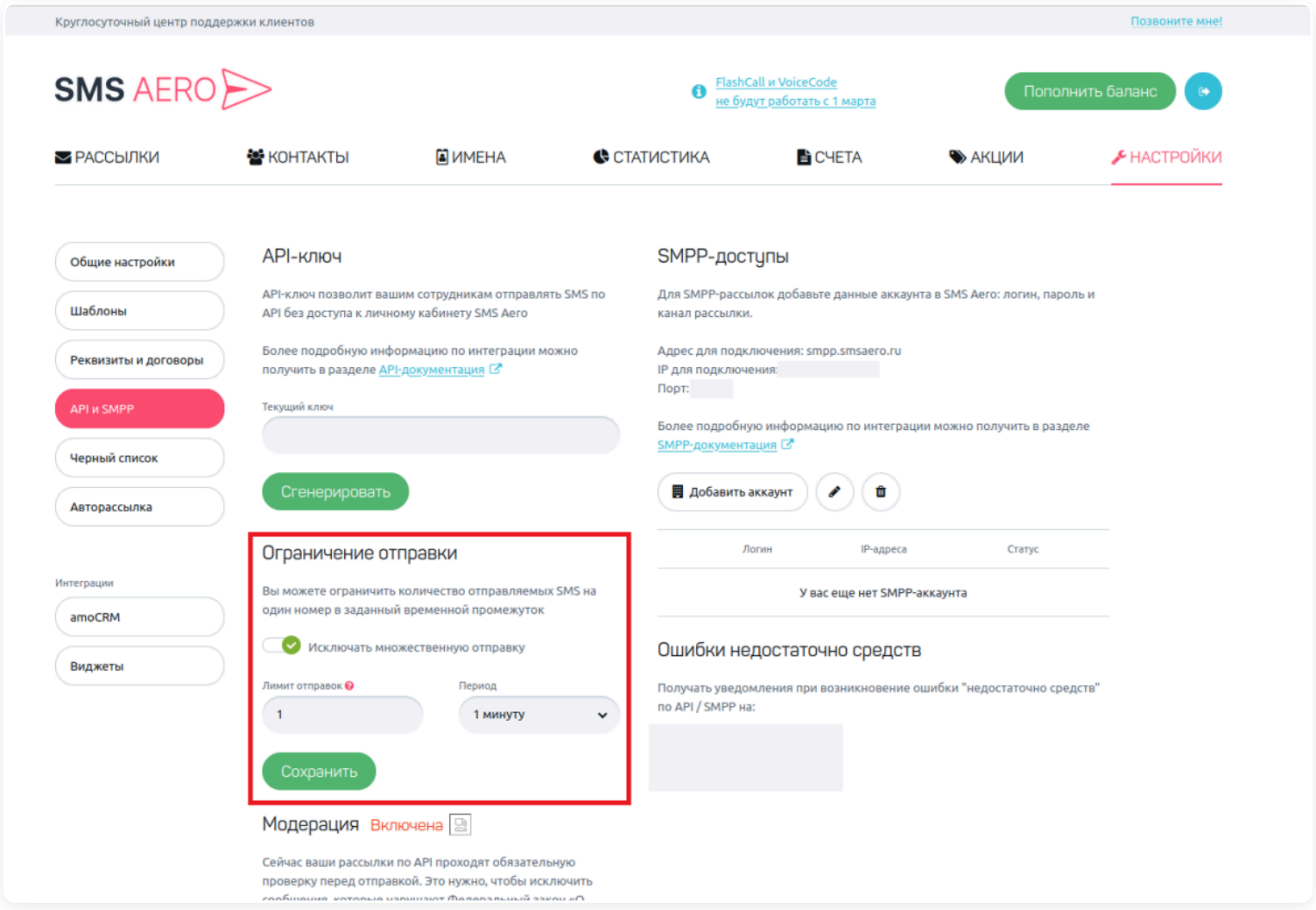
- Если код введен неверно, то появится соответствующее предупреждение:



- 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:

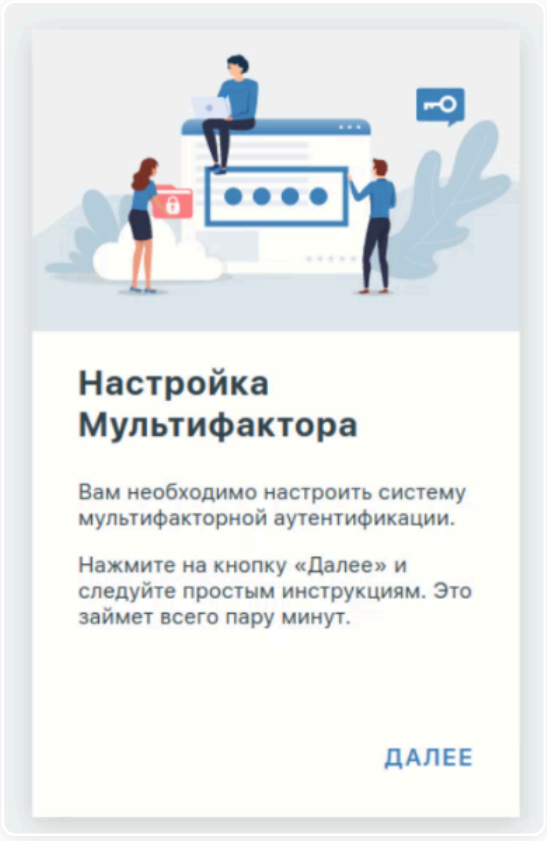


Мультифактор

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Включите созданное VPN-подключение.

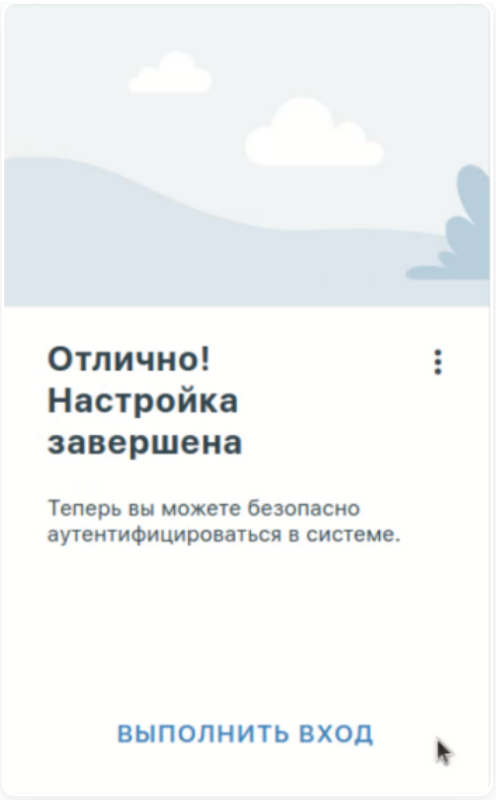
3. При переходе в браузер откроется страница аутентификации:



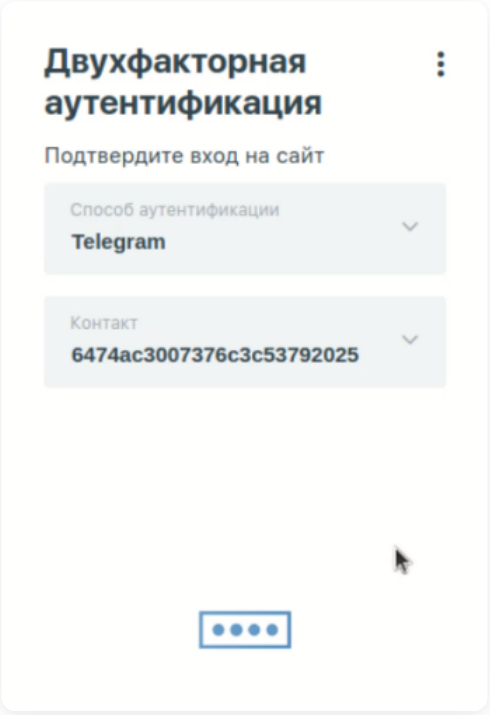
4. После нажатия **Далее** появится страница с предложением установить приложение на устройство пользователя. Если приложение установлено, нажмите **Далее**.

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.

VPN-подключения

Название службы раздела **VPN-подключения**: `ideco-accel-l2tp`; `ideco-accel-pptp`; `ideco-accel-sstp`; `ideco-vpn-servers-backend`; `ideco-vpn-authd`; `ideco-vpn-dhcp-backend`.

Список служб для других разделов доступен по ссылке.

Для получения доступа к локальной сети компании необходимо настроить VPN-сервер и подключиться через него. Можно использовать VPN-клиент, который уже есть в операционной системе, или установить отдельный.

В Ideco NGFW нет разделения локальных интерфейсов на VPN-интерфейсы и Ethernet, поскольку Ideco NGFW не имеет локальных VPN-интерфейсов.

Настройка VPN-сервера происходит в несколько этапов:

- Настройка протоколов, маршрутов и адресации.
- Настройка политик доступа из внешних сетей.
- Настройка двухфакторной аутентификации (опционально).

Поддерживаемые протоколы

Ideco NGFW поддерживает четыре протокола туннельных соединений:

- 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.
- PPTP - не рекомендуется. Этот способ подключения **крайне небезопасен** и оставлен исключительно для совместимости со старыми решениями.

Предварительные требования

Чтобы VPN-подключение работало на устройствах пользователей, необходимо загрузить корневой сертификат:

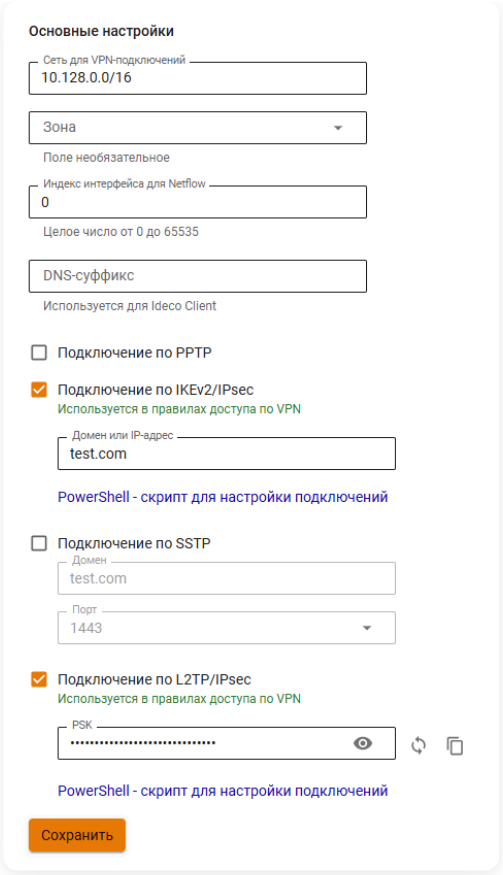
- Корневые сертификаты Ideco NGFW действительны в течение 10 лет.
- Если используется сертификат Let's Encrypt, обновление будет происходить автоматически.

Настройка VPN-подключения

Для настройки VPN-подключения перейдите в **Пользователи** → **VPN-подключения**.

Основное

На вкладке настраиваются протоколы, маршруты и адресация VPN-подключений. Для настройки заполните поля:



Расшифровка полей

- **Сеть для VPN-подключений** - укажите подсеть, в рамках которой будут динамически назначаться IP-адреса. 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. Подробнее об объекте **Зона** в статье.

Если требуется настроить VPN-подключение к Loopback-интерфейсу, оставьте поле **Зона** пустым.

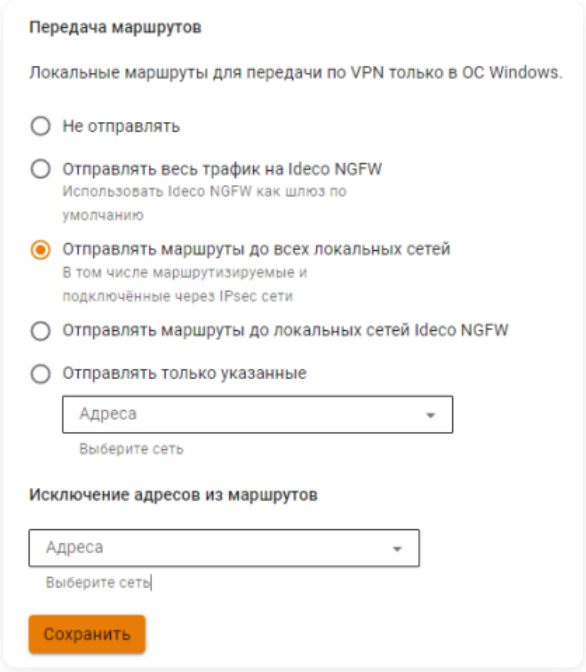
- **DNS-суффикс** - укажите DNS-суффикс, если для подключения по VPN используется Ideco Client.
- Выберите, какой протокол подключения будет использоваться.

Начиная с версии 16.0, 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.

В блоке **Передача маршрутов** укажите, как будут передаваться маршруты:



Маршруты, переданные Ideco NGFW для VPN-клиента, имеют меньшую метрику (т. е. высокий приоритет)

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.

Расшифровка полей

- **Не отправлять** - никакие маршруты не передаются клиенту, никакой трафик не будет проходить через NGFW.
- **Отправлять весь трафик на Ideco NGFW** - передается маршрут 0.0.0.0/0, весь трафик направляется через NGFW.
- **Отправлять маршруты до всех локальных сетей** - передаются маршруты до всех локальных сетей NGFW, в том числе подключенных через IPsec и маршрутизируемых, кроме маршрутов: **OSPF**, **BGP**, и **Маршрутизации внешних сетей**.
- **Отправлять маршруты до локальных сетей Ideco NGFW** - передаются только маршруты до локальных сетей NGFW, без учета IPsec и маршрутизируемых.
- **Отправлять только указанные** - выберите сети, до которых будут передаваться маршруты.

Если маршруты VPN-клиентов пересекаются с маршрутами, передаваемыми Ideco NGFW, то выберите **Не отправлять** или **Отправлять только указанные**.

Если при подключении по VPN (SSTP, IKEv2, PPTP, L2TP) не удается получить маршруты до сетей Ideco NGFW, то это связано с тем, что 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-server**.

Если пакет DHCP превышает 576 байт, то он может быть проигнорирован клиентом DHCP и применение маршрутов не произойдет (зависит от реализации клиента).

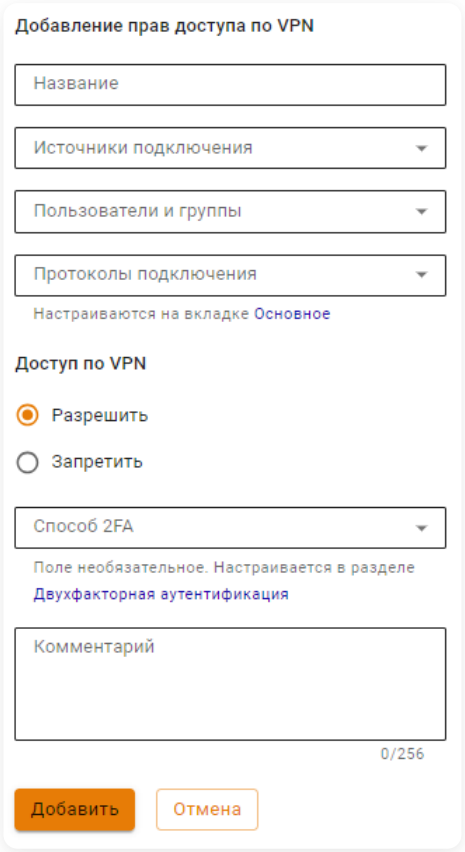
Доступ по VPN

На вкладке настраиваются правила доступа для пользователей и групп на внешние интерфейсы NGFW.

При совпадении условий (**Источник подключения**, **Пользователи и группы**, **Протокол подключения**) выполняется действие, выбранное при создании правил. Созданные правила применяются сверху вниз.

В правилах можно использовать как группы пользователей Ideco NGFW, так и группы безопасности AD. Для добавления группы безопасности AD для VPN не требуется импорт в дерево пользователей. Введите Ideco NGFW в домен и при создании правила **Доступ по VPN** в поле **Пользователи и группы** выберите необходимую группу безопасности.

Для настройки правил доступа, перейдите на вкладку **Пользователи** → **VPN-подключения** → **Доступ по VPN** и нажмите **Добавить**.



Расшифровка полей

- **Название** - укажите название правила.
- **Источники подключения** - выберите, откуда будет производиться подключение по VPN (IP-адреса, подсети, страны).
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Протоколы подключения** - выберите протокол (настраивается на вкладке **Основное**).
- **Доступ по VPN** - разрешите или запретите доступ по созданному правилу.
- **Способ 2FA** - выберите способ двухфакторной аутентификации.
- **Комментарий** - добавьте комментарий (опционально).

Для разных групп пользователей возможно указать разные типы двухфакторной аутентификации. Для настройки двухфакторной аутентификации воспользуйтесь статьей.

Правила выдачи IP-адресов

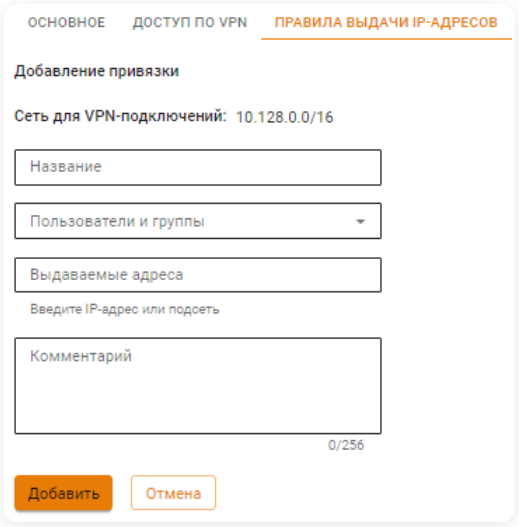
На вкладке можно создать правила для выдачи IP-адресов пользователям, подключающимся по VPN.

NGFW 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 и он уже используется в текущей сессии, то указанный в правиле пользователь не сможет установить второе VPN-подключение - оно 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 перейдите на вкладку **Пользователи → VPN-подключения → Правила выдачи IP-адресов** и нажмите **Добавить**.



Расшифровка полей

- **Название** - укажите название правила.
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Выдаваемые адреса** - укажите фиксированный IP-адрес или подсеть, которые будут выдаваться пользователям.
- **Комментарий** - укажите комментарий к правилу (опционально).

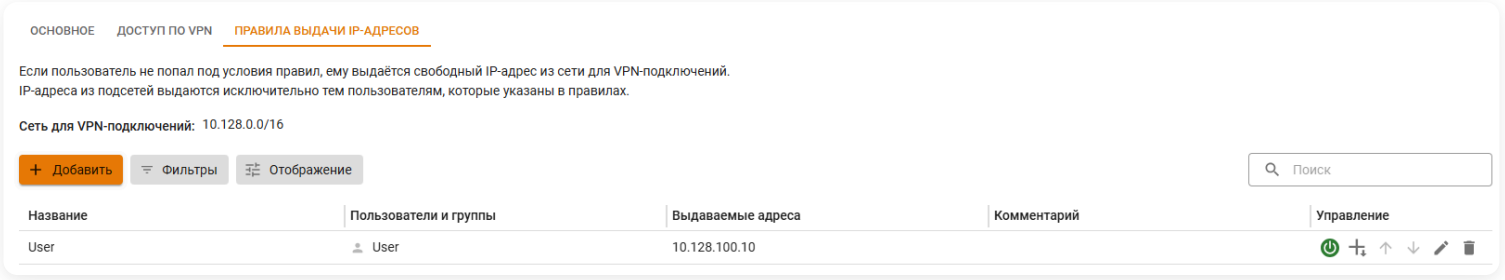
При наличии большого количества правил выдачи IP-адресов в таблице воспользуйтесь кнопкой **Фильтры**.

Чтобы отключить правило, нажмите на в столбце управления. Чтобы удалить правило, нажмите .

Статическая привязка IP-адресов

IP-адрес пользователю назначается автоматически из пула адресов для VPN, настраиваемого в разделе **Пользователи → VPN-подключения** (например 10.128.0.0/16).

Чтобы настроить **статическую** привязку адресов, выдаваемых по VPN определенным пользователям, нужно перейти в раздел **Пользователи → VPN-подключения → Правила выдачи IP-адресов**, нажать **Добавить** и указать нужного пользователя и IP-адрес. Пример настройки фиксированного IP-адреса VPN представлен ниже:



Полезные ссылки

- Инструкции по созданию VPN-подключений.

Подключение по PPTP

Не используйте этот тип подключения, он крайне небезопасен, оставлен исключительно для совместимости со старыми решениями. Используйте IKEv2/IPsec.

Подключение по протоколу PPTP предполагает авторизацию по защищенному сетевому туннелю между сетевым устройством пользователя и интернет-шлюзом Ideco NGFW.

Для аутентификации пользователя применяется связка логин/пароль пользователя Ideco NGFW или пользователя из Active Directory.

Для авторизации по протоколу PPTP необходимо назначить IP-адрес сетевому устройству, а также настроить на нем подключение по протоколу PPTP с указанием IP-адреса интернет-шлюза Ideco NGFW в качестве адреса PPTP-сервера.

При успешной аутентификации и установлении PPTP-туннеля сетевому устройству будет автоматически назначен дополнительный IP-адрес для получения доступа к ресурсам интернета. Использование авторизации по PPTP никак не отражается на возможности доступа сетевого устройства к ресурсам локальной сети.

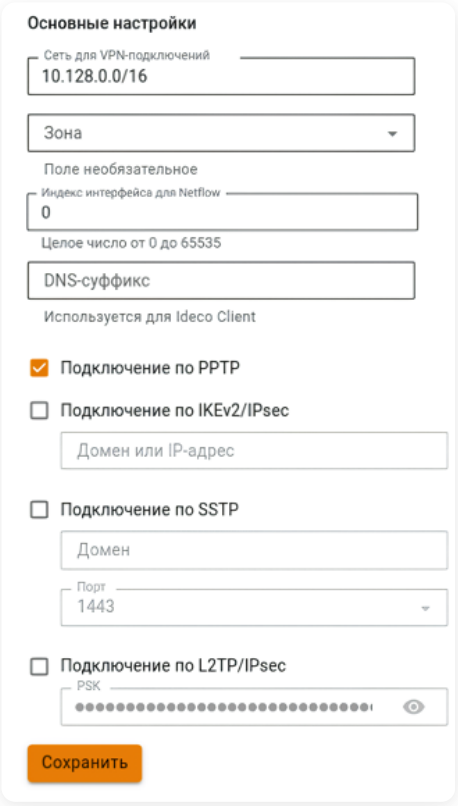
Не рекомендуем использовать для VPN-подключений кириллические логины.

Настройка Ideco NGFW

Основные настройки

Для настройки авторизации по протоколу PPTP выполните действия:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение по PPTP**.

3. В поле **Индекс интерфейса для Netflow** введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

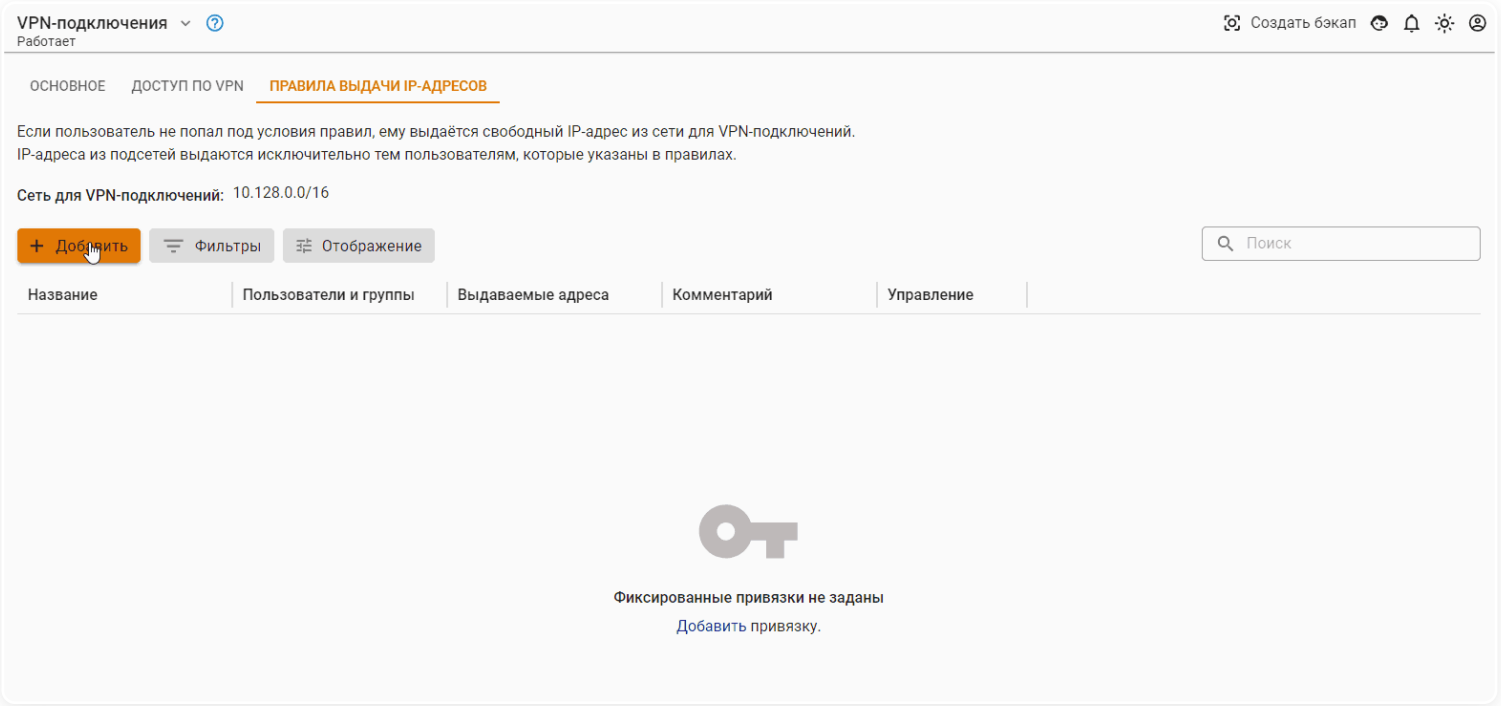
4. Нажмите **Сохранить**.

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).

Чтобы настроить **статическую** привязку адресов, выдаваемых по VPN определенным пользователям:

1. Перейдите в раздел **Пользователи → VPN-подключения → Правила выдачи IP-адресов**:



2. Нажмите **Добавить** и укажите название сети, нужного пользователя и IP-адрес.

3. Нажмите **Добавить**, чтобы сохранить изменения:

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи → VPN-подключения → Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключение.

Возможные неполадки

- Провайдер блокирует GRE-протокол, используемый в PPTP-соединении, что приводит к **ошибке 619** при подключении к внешнему адресу IdecoNGFW. Определить сторону проблемы можно, подключаясь с разных мест и от разных провайдеров. Если из некоторых мест подключение удается, значит, проблема на стороне клиента. Определив провайдера, нужно попытаться решить проблему с ним либо использовать IPsec-IKEv2 или SSTP;
- Заблокирован порт 1723 TCP. Проверить доступность можно с помощью стандартных утилит, таких как telnet. Если соединения нет, то туннель не может быть установлен;
- Неправильно указаны логин или пароль пользователя. Если это происходит, то часто при повторном соединении предлагается указать домен. Рекомендуется использовать для паролей латинские символы и цифры. При ошибке ввода пароля более 6 раз IP-адрес пользователя блокируется службой защиты от подбора паролей;
- При подключении через клиента ОС Windows убедитесь, что в настройках подключения включена опция **Использовать основной шлюз в удаленной сети** в разделе **Свойства подключения VPN → Вкладка Сеть → Свойства опции "Протокол интернета версии 4 (TCP/IPv4)" → Дополнительно**. Если маршрутизировать все пакеты в этот интерфейс не обязательно, то маршрут надо писать вручную;
- При возникновении ошибки **Подключение было закрыто удаленным компьютером** необходимо включить поддержку MPPE 128-bit (в Windows эта опция включена по умолчанию) и среди протоколов аутентификации отметить только MSCHAPV2.

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.

Подключение по IKEv2/IPsec

Видеоинструкцию смотрите по ссылкам:

- Youtube
- docs.ideco.ru

IKEv2/IPsec - протокол, который используется для создания защищенного соединения между двумя устройствами в сети.

Данный протокол VPN является предпочтительным и рекомендованным для всех сценариев использования.

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 или пользователя из Active Directory.

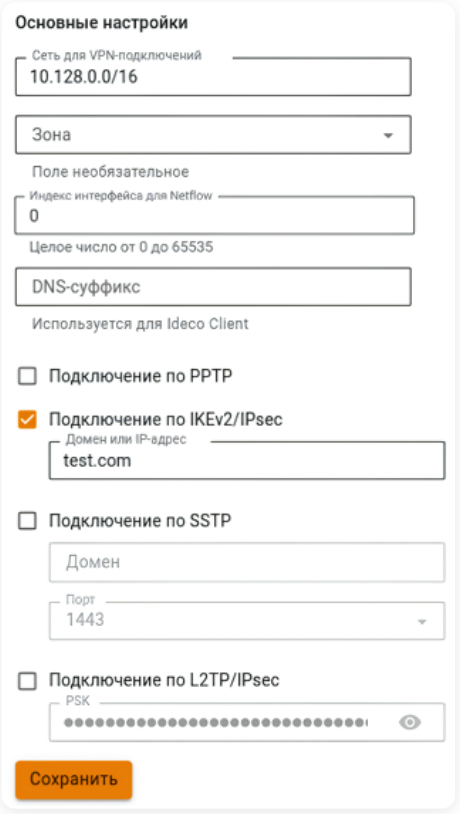
Не применяйте Wildcard-сертификаты для IKEv2/IPsec. Эти сертификаты не поддерживаются IPsec-клиентами из-за ограничений в проверке доменных имен.

Настройка Ideco NGFW

Не рекомендуем использовать для VPN-подключений кириллические логины и пароли, а так же указывать в качестве логина IP-адрес.

Основные настройки

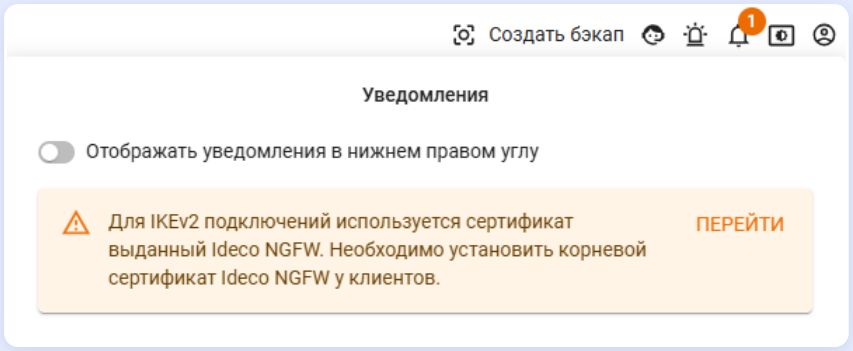
1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение по IKEv2/IPsec**.

3. В соответствующем поле укажите доменное имя или IP-адрес и 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 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 разделе **Сервисы → Сертификаты → Загруженные сертификаты**.

4. Если используете Netflow, то в поле **Индекс интерфейса для Netflow** введите целое число от 0 до 65535 для идентификации интерфейса.

5. Передача клиентам маршрутов до ваших локальных сетей происходит автоматически. Для управления доступом к сетям используйте Файрвол.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи → VPN-подключения → Доступ по VPN** разрешающее правило. Подробнее - в статье VPN-подключение.

Поддержка IKEv2/IPsec в клиентских 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.
- **KeeneticOS 3.5** и выше. Инструкция по настройке.
- MikroTik.
- Cisco routers.

Подключение по SSTP

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

По возможности не используйте этот тип подключения. Этот способ подключения 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 или пользователя из Active Directory.

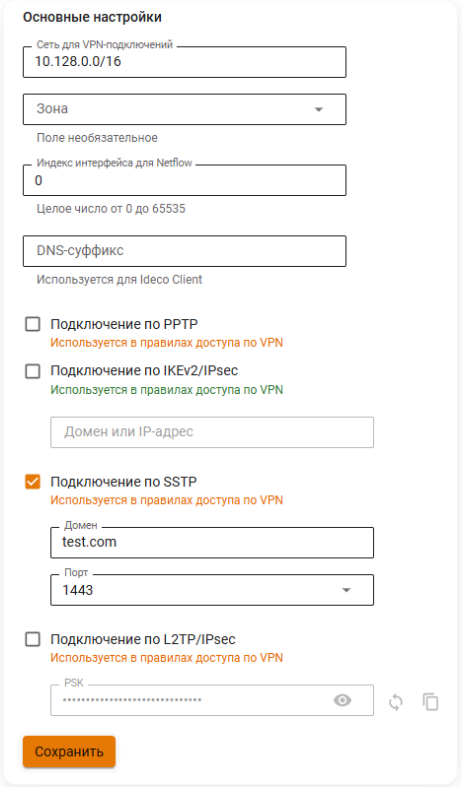
Особенности работы:

- 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 не поддерживает подключение MikroTik по SSTP, так как MikroTik использует устаревший и небезопасный алгоритм SHA-1.

Настройка Ideco NGFW

Основные настройки

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение SSTP**.

3. Подключение возможно только по DNS-имени, поэтому IP-адрес внешнего интерфейса Ideco NGFW должен резолвиться в одно из имен вашей внешней доменной зоны. В поле **Домен** укажите данное DNS-имя (используйте реальное имя с правильной A-записью, т. к. оно необходимо для выписки сертификата Let's Encrypt).

4. В поле **Индекс интерфейса для Netflow** введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. **Порт** - выберите предлагаемый порт (из вариантов: 1443, 2443, 3443, 4443).

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. 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.

Подключение по L2TP/IPsec

Видеоинструкцию смотрите по ссылкам:

- Youtube
- docs.ideco.ru

По возможности не используйте этот тип подключения. Он 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.

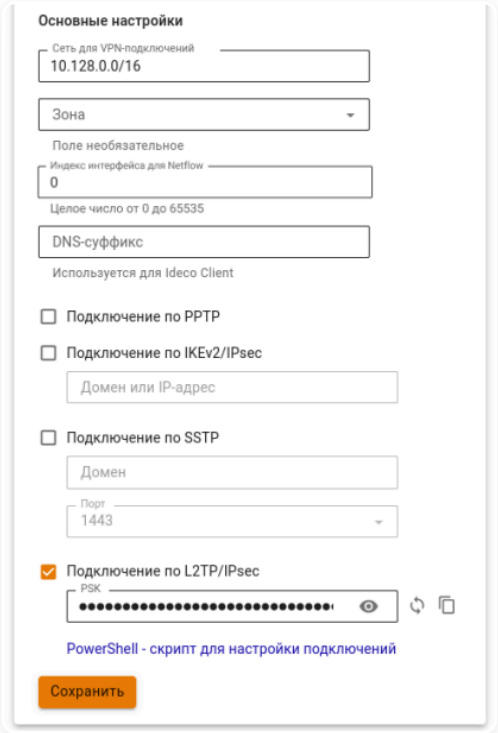
Для аутентификации используется связка логин/пароль пользователя Ideco NGFW или пользователя из Active Directory, а также PSK-ключ, который был указан при настройке соединения.

Не рекомендуем использовать для VPN-подключений кириллические логины. А так же указывать в качестве логина IP-адрес.

Настройка Ideco NGFW

Основные настройки

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение по L2TP/IPsec**.

3. Укажите секретную фразу (PSK-ключ).

4. В поле **Индекс интерфейса для Netflow** введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Нажмите **Сохранить**.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключение.

Полезные ссылки

- L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их 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.

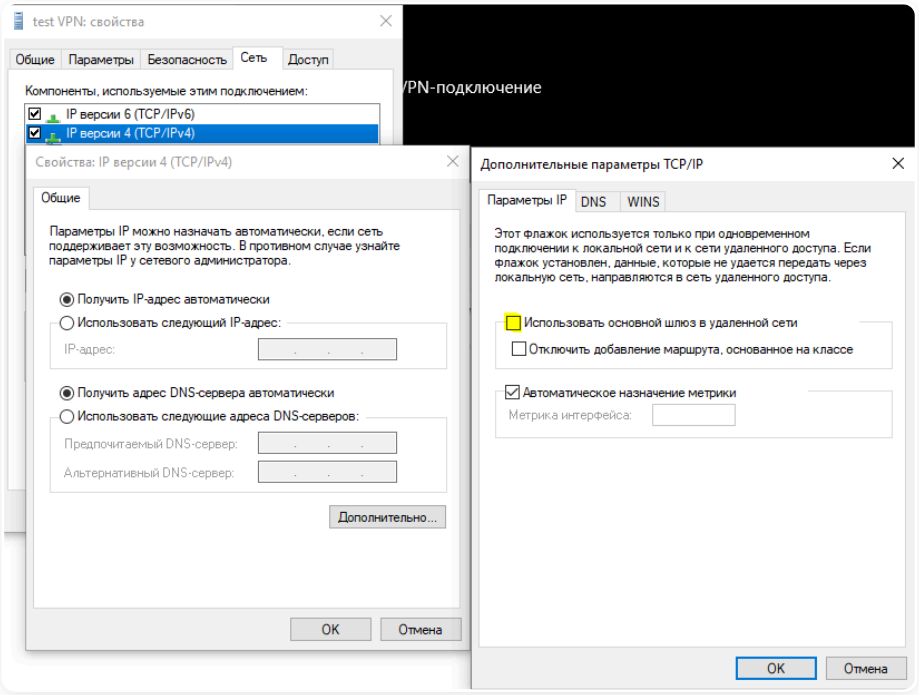
Особенности маршрутизации и организации доступа

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.

Организация доступа по VPN только к ресурсам локальной сети

Для организации доступа выполните действия:

1. На вкладке **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 добавить передачу IP-адреса VPN-сервера NGFW (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:

```
===========================================================================
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
        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 и добавленной публикацией IP NGFW:

```
===========================================================================
IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес          Маска сети      Адрес шлюза       Интерфейс  Метрика
```

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 либо добавить его в список публикуемых маршрутов на стороне NGFW. 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, 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

Для получения доступа к компьютерам в локальной сети Ideco NGFW 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);

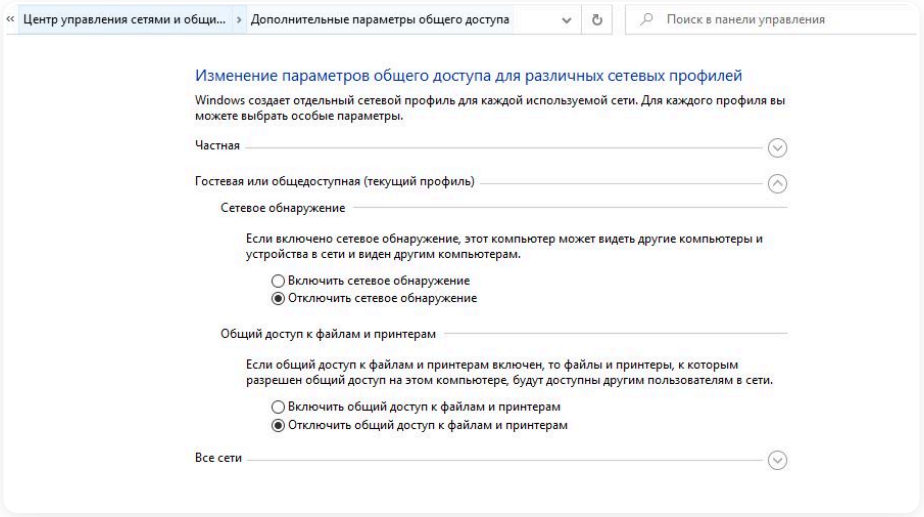
2. На компьютерах локальной сети основным шлюзом должен быть Ideco NGFW. Если это не так, то вручную необходимо прописать соответствующий маршрут, чтобы сетевые пакеты шли на Ideco NGFW для VPN-сети. **Например**:

```
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 (настраивается в разделе **Пользователи** → **VPN-подключения**);
- `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW.

3. На Ideco NGFW в разделе **Файрвол** → **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:

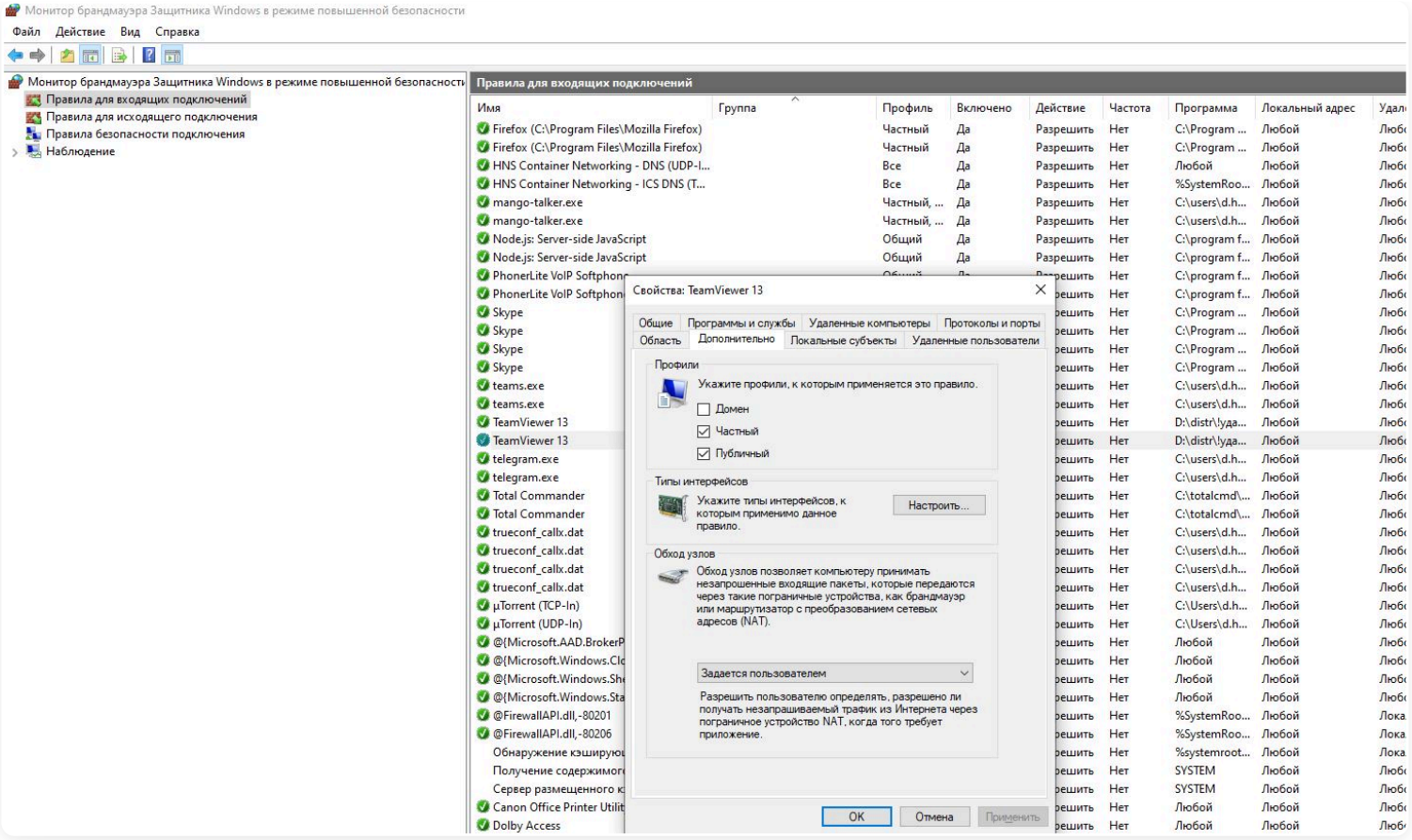
1. Перейдите в PowerShell (запустите его с повышением прав до администратора).

2. Выполните команду: `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`.

Возможные проблемы:

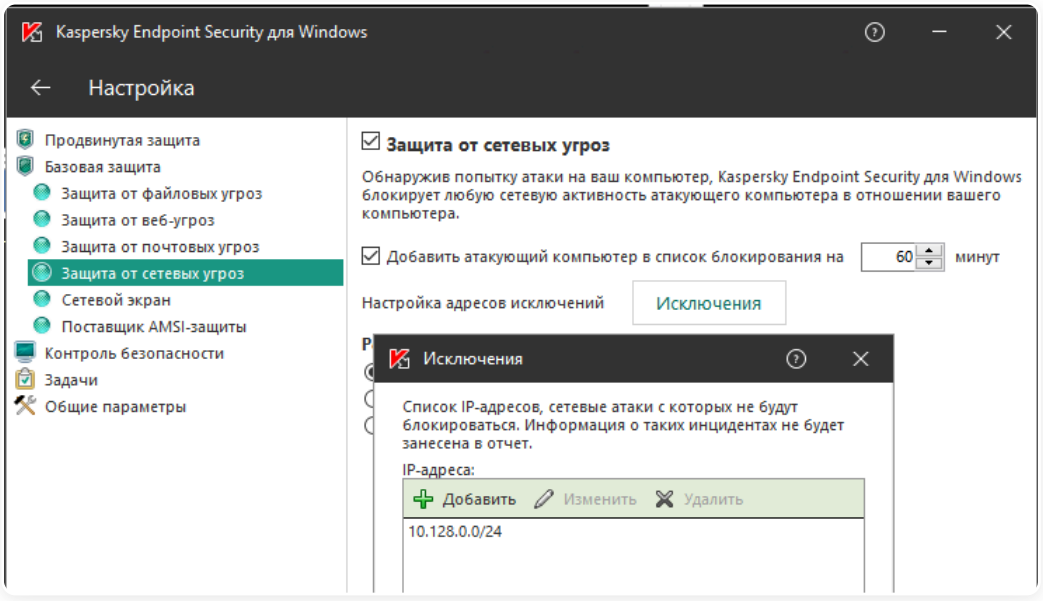
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей.

  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 не пересекаются. Затем проверьте настройки основного NGFW, следуя инструкциям, описанным в статье.

Получение доступа до хостов локальной сети, если за NGFW 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 (`172.16.0.1`).

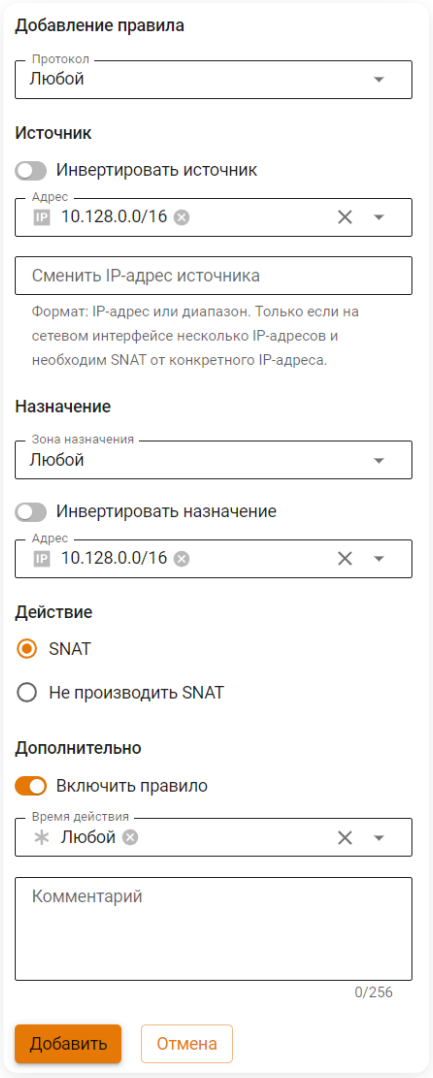
Если настроить на роутере маршрут невозможно, можно создать на NGFW SNAT-правило:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **SNAT** и нажмите **Добавить**.

2. Укажите следующие 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 подменит IP-адрес источника своим. За счет этого роутер направит ответ от хоста в локальной сети на NGFW, 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`.

Инструкция по запуску PowerShell скриптов

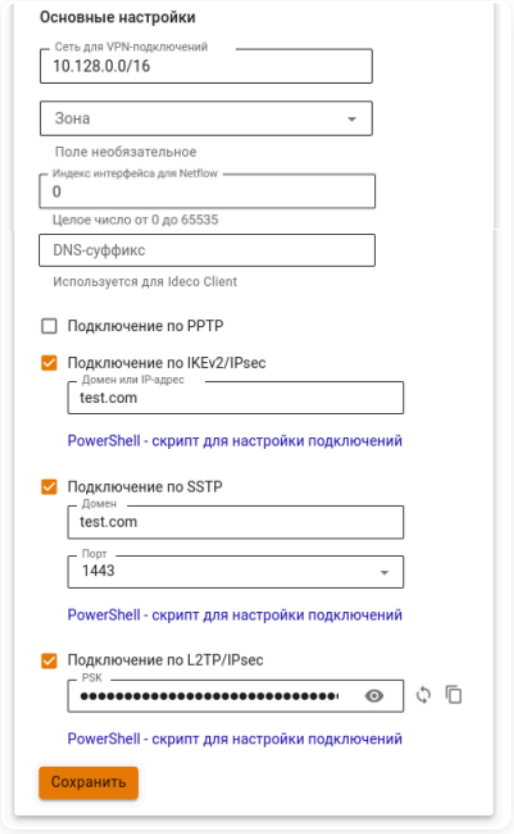
Для подключения по VPN к Ideco NGFW с белым IP адресом достаточно действий, указанных ниже. Если Ideco NGFW выходит в интернет через маршрутизатор, воспользуйтесь пунктом Подключение по VPN к Ideco NGFW с доступом в интернет через маршрутизатор.

Запуск PowerShell-скрипта

1. Скачайте скрипт одним из способов:

Из Ideco NGFW:

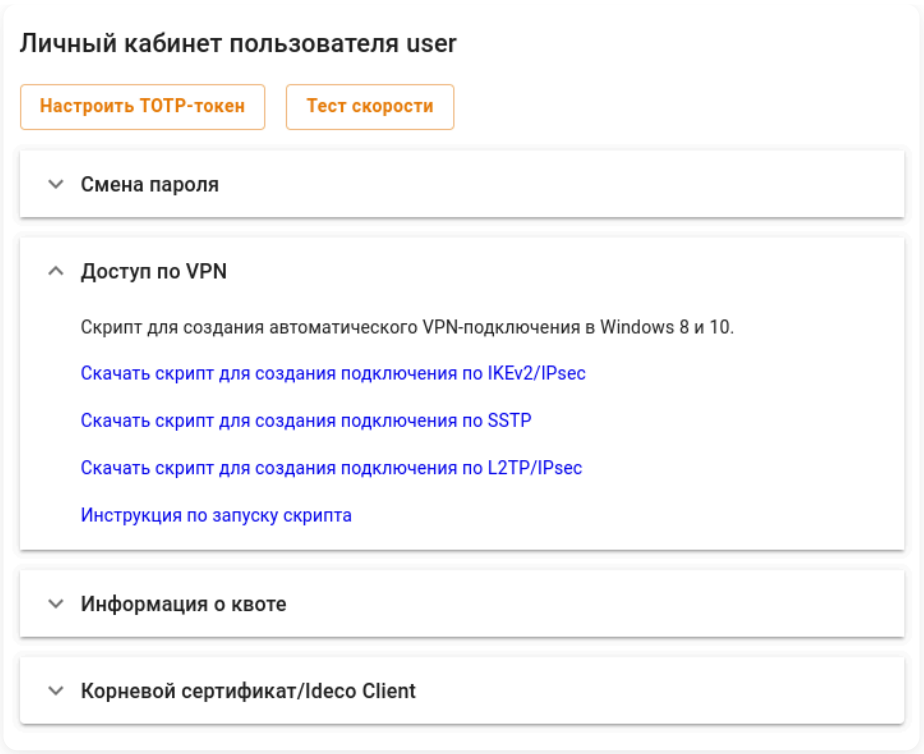
- Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



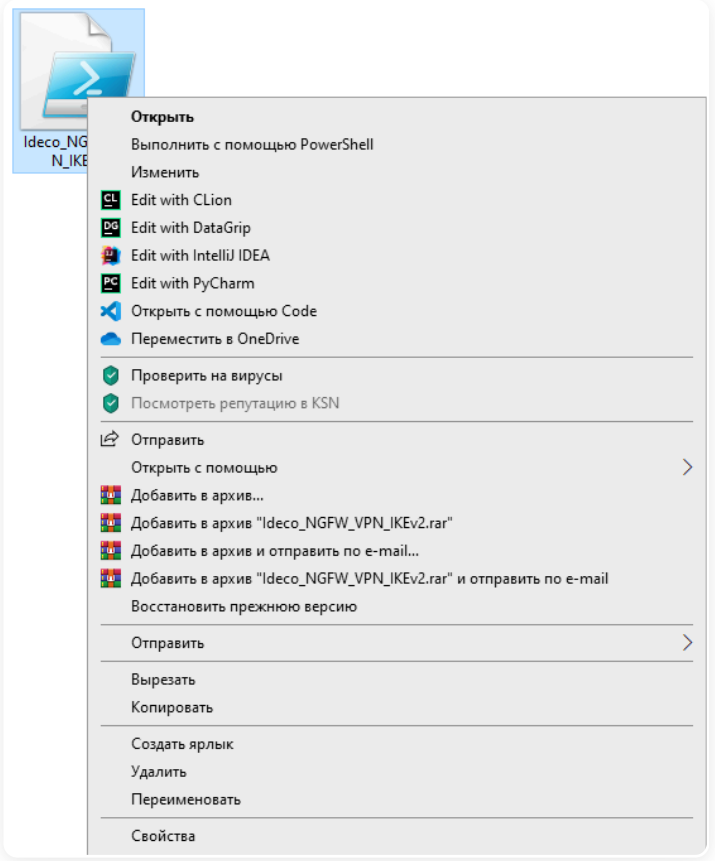
- Включите и настройте требуемый протокол подключения.
- Перейдите по ссылке **PowerShell - скрипт для настройки подключений**.
- Перенесите скачанный файл на устройство, на котором требуется создать VPN-подключение.

В личном кабинете пользователя:

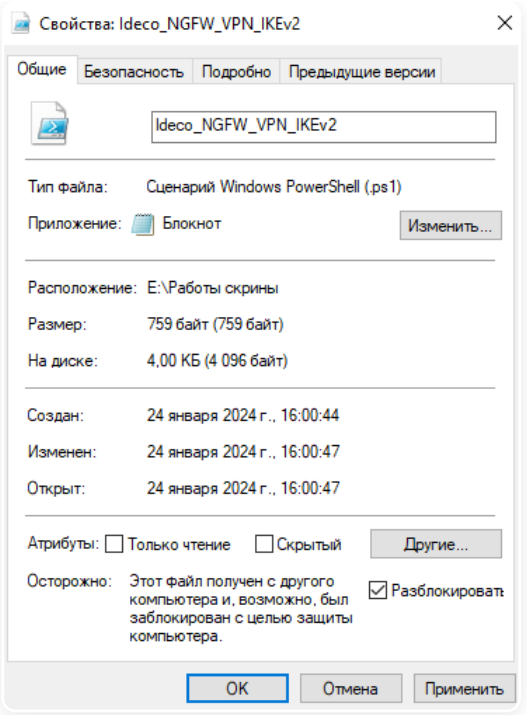
- Скачайте скрипт, перейдя по ссылке **Скачать скрипт для создания подключения**:



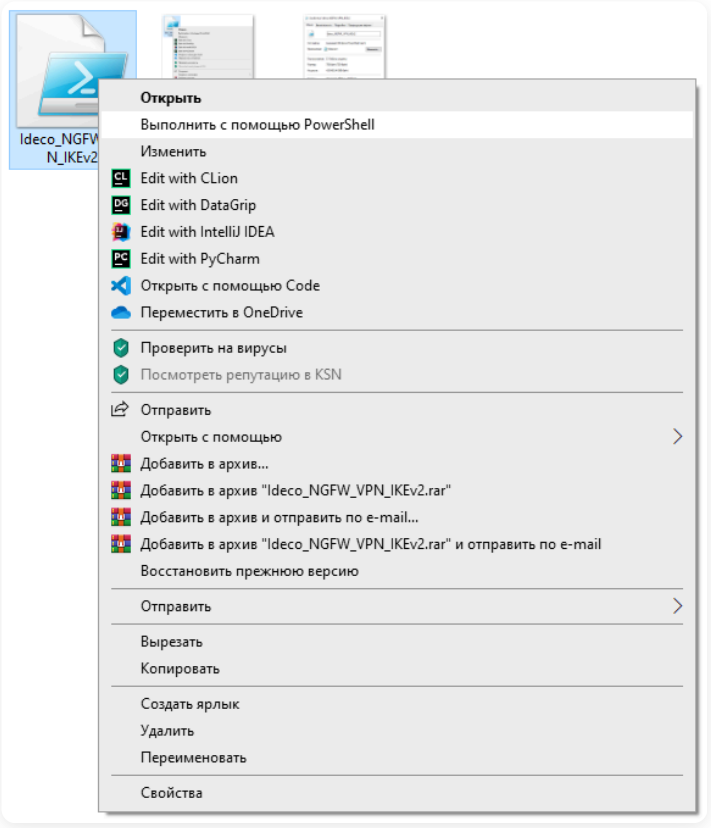
2. Нажмите правой кнопкой мыши по скачанному файлу и в контекстном меню выберите **Свойства**:



3. Включите опцию **Разблокировать** справа в нижнем углу свойств файла (по умолчанию ОС блокирует выполнение скачанных из интернета файлов):

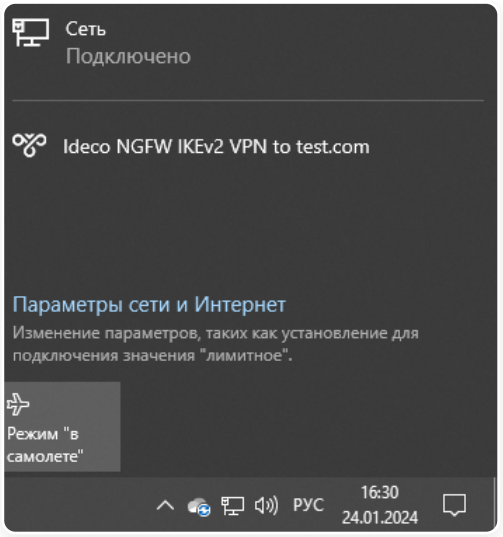


4. Нажмите правой кнопкой мыши на файл и выберите пункт **Выполнить в PowerShell**. Затем подтвердите действие, нажав **Да** на вопрос о внесении изменений в компьютер:



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 отключение создано, нажмите **Подключиться** в списке сетей.



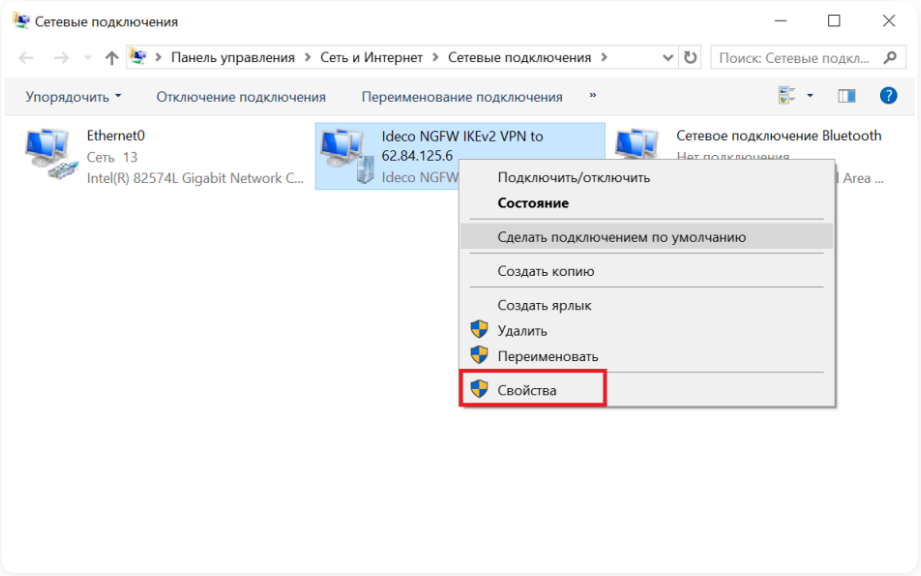
DNS-суффиксы для VPN-подключений

PowerShell-скрипты прописывают основной DNS-суффикс для создаваемого VPN-подключения. Он соответствует домену, в который введен Ideco NGFW. Это позволяет обращаться к устройствам за VPN по короткому имени.

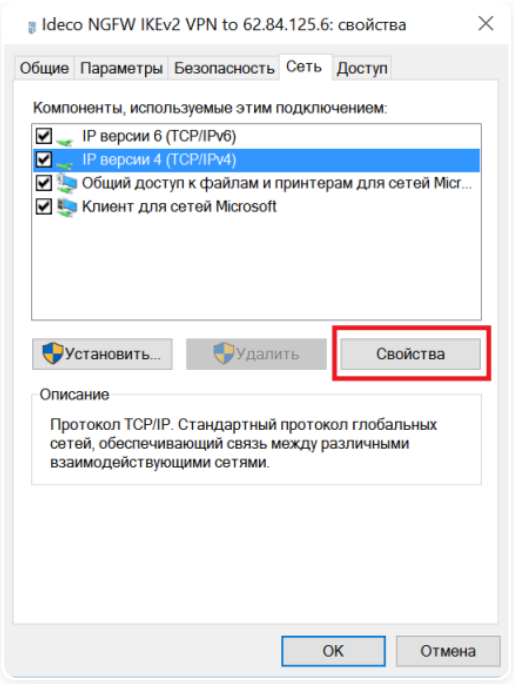
> Если Ideco NGFW введен в несколько доменов, то DNS-суффиксы в PowerShell-скриптах не прописываются, их необходимо настраивать вручную на подключенном по VPN устройстве.

Чтобы настроить DNS-суффиксы для созданного VPN-подключения в Windows, выполните действия:

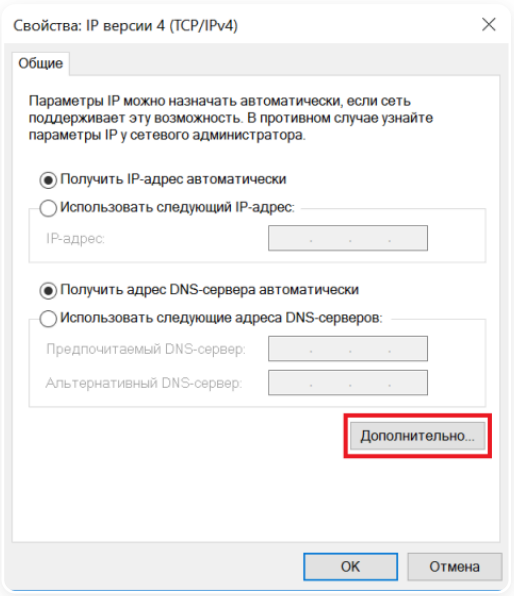
1. Перейдите в **Сетевые подключения**, нажмите правой кнопкой мыши по нужному VPN-подключению и выберите **Свойства**:



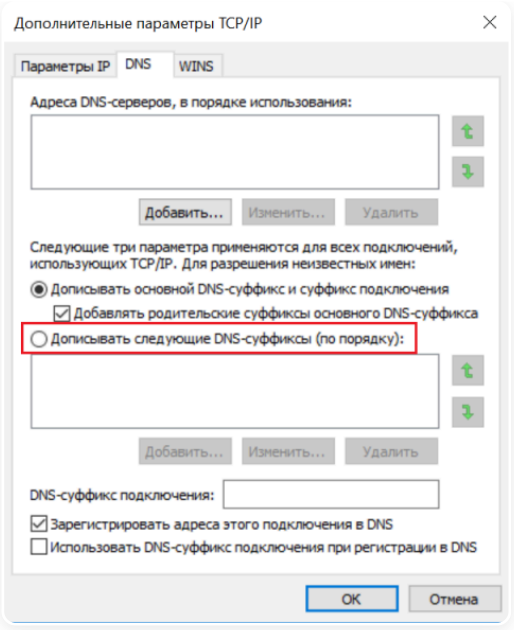
2. В открывшемся окне перейдите на вкладку **Сеть**, выберите компонент **IP версии 4 (TCP/IPv4)** и нажмите **Свойства**:



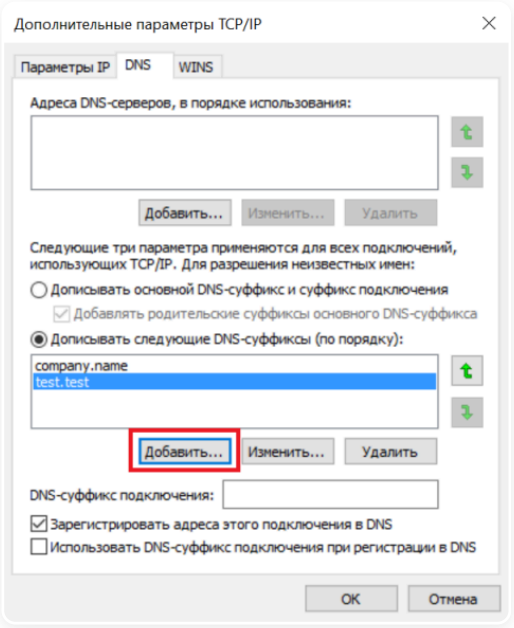
3. В открывшемся окне нажмите **Дополнительно**:



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. Этот порядок можно менять стрелками.

Подключение по VPN к Ideco NGFW 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 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 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 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

Название службы раздела **Ideco Client**: `ideco-agent-backend`; `ideco-agent-websocket`.

Список служб для других разделов доступен по ссылке.

Ideco Client - программа-клиент, которая управляет авторизацией пользователей при подключении к NGFW.

Ideco Client использует протокол WireGuard, но наша реализация WireGuard совместима только с Ideco NGFW: Ideco Client не является универсальным клиентом WireGuard, а поддержка WireGuard в Ideco NGFW ограничена.

Ideco Client недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

Возможности Ideco Client

- [x] Авторизация в локальной сети
- [x] VPN-подключение из внешних сетей
- [x] VPN-подключение из локальных сетей
- [x] Двухфакторная аутентификация
- [x] Режим работы Device VPN
- [x] Сбор данных о подключающихся устройствах

Сбор данных о подключающихся устройствах позволяет задавать критерии проверки - HIP-профили - и использовать их в правилах **Файрвола**.

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.

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	+	+	+
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	+	+	+

Ввод двухфакторной аутентификации	Показать окно ввода двухфакторной аутентификации при запросе от NGFW 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. Файрвол	Проверка Файрволом	+		
ZTNA. Антивирус	Проверка Антивирусами	+	+	
Версия	Проверка актуальной версии Ideco Client	+	+	+
Терминальный сервер	Поддержка работы терминальных серверов	+		
Балансировка Active-Active 302 Редирект	Подключение к Ideco NGFW по выданному балансировщиком адресу или другому серверу	+	+	+
Кастомная настройка	Кастомная настройка конфигурации Ideco Client: автосоздание профилей, запрет редактирования профилей и т.д.	+	+	+

Файрвол

Windows

Вендор	**Продукт**
Microsoft	Windows Firewall

Антивирус

Windows

Вендор	**Продукт**
Microsoft	Windows Defender
Kaspersky Lab	• Kaspersky Free • Kaspersky Small Office Security • Kaspersky Internet Security • Kaspersky Endpoint Security
Dr.Web	Dr.Web Security Space
Comodo	Comodo Internet Security

macOS

Вендор	**Продукт**
Kaspersky Lab	• Kaspersky Free • Kaspersky Endpoint Security Все остальные продукты Kaspersky Lab по умолчанию определяются как Kaspersky Free.
DrWeb	Dr.Web для macOS

Поддерживаемые версии ОС и порты подключения

Поддерживаемые версии ОС	• Windows 10 22H2 и выше **Важно:** Ideco Client не работает на ОС Windows 11 версии 24H2. Варианты решения описаны ниже • macOS версии 12.7 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 за NAT	• 80 TCP - для работы сертификатов Let's Encrypt • 14765 TCP и 3051 UDP - для работы Ideco Client

Настройки в Ideco NGFW

Перейдите в **Пользователи** → **Ideco Client** → **Основное**:

- В поле **Домен** укажите доменное имя или IP-адрес Ideco NGFW. Например: `example.ru`, `ideco.example.ru` или `52.251.83.117`
- Для подключения пользователей локальных сетей по VPN включите опцию **Создавать туннель при подключении из локальной сети**. Включение или выключении опции разрывает текущие сессии из локальных сетей.
- Для настройки Device VPN включите опцию **Принимать подключения в режиме Device VPN** Подробнее в статье.

Для корректного подключения из внешней сети создайте правило в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее пользователю VPN-подключение.

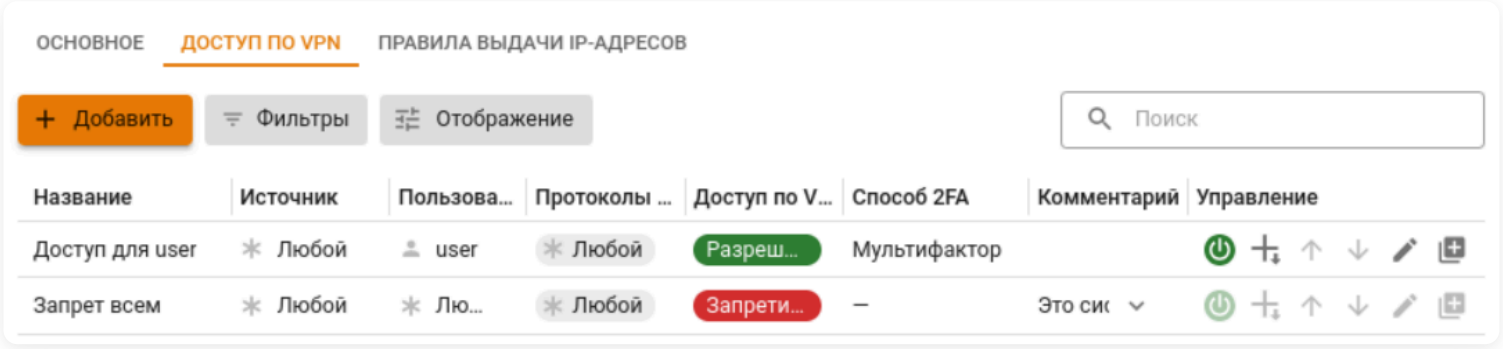
Настройка двухфакторной аутентификации в Ideco Client

В веб-интерфейсе Ideco NGFW:

1. Создайте учетную запись пользователя в разделе **Пользователи** → **Учетные записи**.

2. Перейдите в раздел **Пользователи** → **Двухфакторная аутентификация** и выберите подходящие типы. Настройте двухфакторную аутентификацию способами, указанными в статье.

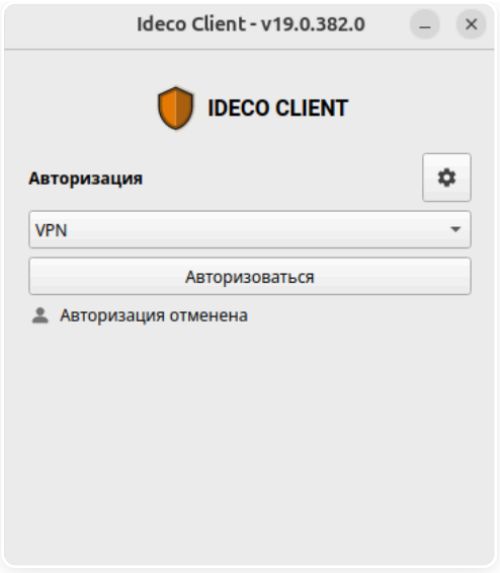
3. Добавьте правило в разделе **Пользователи** → **VPN-подключения** → **Доступ по VPN**. В настройках правила укажите созданную учетную запись пользователя и тип двухфакторной аутентификации, выбранный в шаге 2. В поле **Протоколы** укажите значение **Любой**:



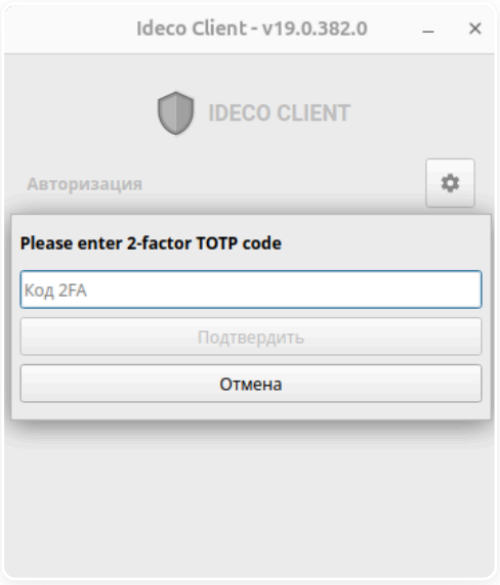
На устройстве пользователя:

1. Установите и запустите приложение Ideco Client. Инструкции по установке: Windows.

2. Авторизуйтесь через настроенную учетную запись пользователя:

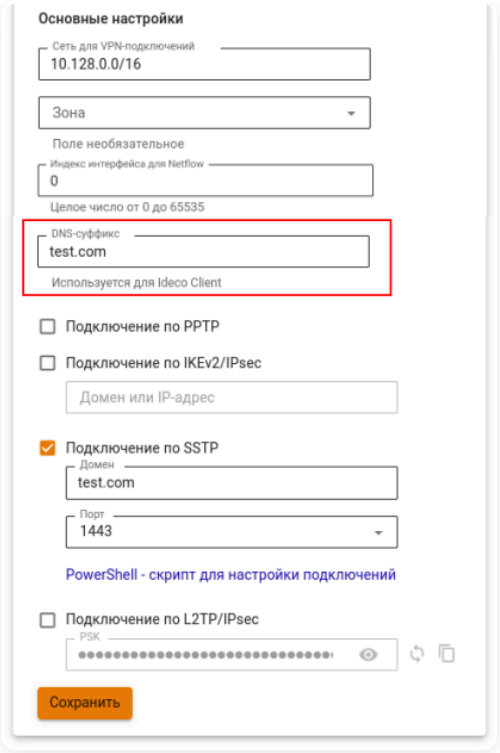


3. Введите код двухфакторной аутентификации:



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**:

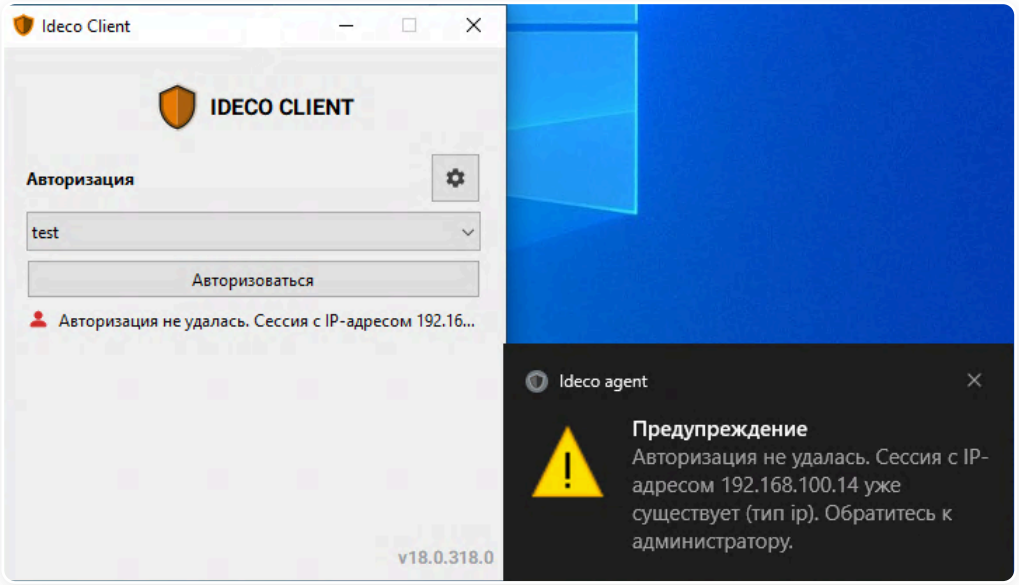


Суффикс будет передан устройствам через Ideco Client и позволит использовать короткие имена серверов (например, server-1c вместо server-1c.company.lan). Без суффикса разрешение таких имен работать не будет.

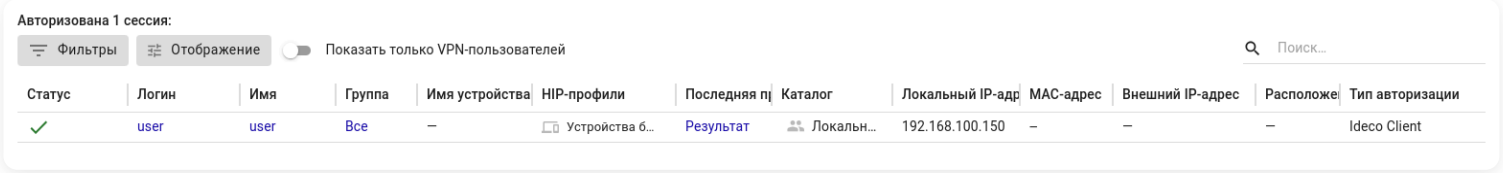
Ideco NGFW поддерживает только один DNS-суффикс. Не указывайте DNS-суффикс, если NGFW введен в несколько доменов.

Особенности работы Ideco Client

- Только один профиль может быть с опцией автоподключения. Если активировать автоподключение для другого профиля, у предыдущего эта опция отключится.
- SSO-аутентификация в IdecoClient не будет работать для доверенных доменов.* 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: `IdecoAgent.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:



DNS-запросы 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** сеть до NGFW 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).
- При VPN-подключении через Ideco Client DNS-запросы идут на адрес NGFW, но в передаваемом на Ideco Client списке нет маршрута до DNS NGFW.

Рекомендуем при выборе типа передачи маршрутов **Отправлять только указанные сети** добавить в список DNS NGFW, чтобы клиент VPN построил таблицу маршрутизации до этой сети.

Особенности маршрутизации и организации доступа по VPN к ресурсам локальной сети описаны в статье.

Балансировка и редиректы VPN-подключений

Device VPN

Device VPN - режим работы Ideco Client, в котором клиентское устройство авторизуется на Ideco NGFW 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

Для авторизации через Device VPN используется корневой сертификат с приватным ключом. На основе этого ключа администратор создает пользовательские сертификаты для конечных устройств.

Как работает перенос настроек с профилями при смене версии

При запуске Ideco Client выполняет последовательность действий:

1. Ideco Client проверяет наличие настроек в ключе реестра текущей версии.

2. Если настройки найдены, они применяются.

3. Если настройки текущей версии отсутствуют, ищет в ключах реестра прошлых версий (от новой к старой).

4. При нахождении настроек в предыдущих версиях они копируются в ключ реестра текущей версии Ideco Client.

5. Если настройки не найдены, то в ключе реестра текущей версии создаются настройки с параметрами по умолчанию.

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 ключ реестра текущей версии, то при следующем запуске Ideco Client инициирует поиск и копирование настроек. Если настройки не будут найдены в ключах реестра предыдущих версий, то будет создан ключ с настройками по умолчанию.

Примеры работы переноса настроек

Первая установка Ideco Client

Ideco Client не установлен и в реестре компьютера нет настроек Ideco Client:

1. При запуске Ideco Client создает в реестре ключ текущей версии Ideco Client с настройками по умолчанию. Например, `\HKEY_CURRENT_USER\Software\Ideco\Agent\19.1.3`.

2. Копирование не выполняется.

Обновление Ideco Client на следующую версию

Пользователь обновляет Ideco Client с 18.3.2 до 19.0.1:

1. Ideco Client проверяет наличие настроек в ключе реестра версии 19.0.1 - `\HKEY_CURRENT_USER\Software\Ideco\Agent\19.0.1`.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в ключах реестра предыдущих версий от более новой к более старой.

4. Если настройки найдены в ключе реестра одной из прошлых версий, то они копируются в ключ реестра версии 19.0.1.

5. Если настройки не найдены, то создается ключ реестра версии 19.0.1 с параметрами по умолчанию.

Возврат Ideco Client на предыдущую версию

Возврат Ideco Client с версии 19.0.2 на 19.0.1:

1. При запуске Ideco Client ищет настройки в ключе реестра версии, на которую происходит возврат - `\HKEY_CURRENT_USER\Software\Ideco\Agent\19.0.1`.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в ключах реестра предыдущих версий от более новой к более старой.

4. Если настройки найдены, они копируются в ключ реестра версии 19.0.1.

5. Если настройки не найдены, то создается ключ реестра версии 19.0.1 с параметрами по умолчанию.

> Копирование не происходит назад по версиям, поэтому копирование настроек из версии 19.0.2 на 19.0.1 невозможно.

Повторное обновление Ideco Client после возврата на предыдущую версию

1. Пользователь использовал версию 19.0.2.

2. Выполнен возврат на версию 19.0.1.

3. Пользователь создал новый профиль в версии 19.0.1

4. Выполнено обновление до версии 19.0.2.

5. При запуске Ideco Client настройки и профили из версии 19.0.1 не будут перенесены в версию 19.0.2, поскольку в ключе реестра уже существуют настройки, созданные при первом запуске версии 19.0.2.

Решение проблемы с подключением на ОС Windows 11 версии 24H2/25H2

Вариант 1. Включить компонент **Virtual Machine Platform**:

1. Установите последнюю версию MS Visual C++ Redistributable.

2. Нажмите комбинацию клавиш **Windows + R** и введите команду `appwiz.cpl`.

3. В левой части окна выберите **Включение или отключение компонентов Windows**.

4. Включите функцию **Virtual Machine Platform** (**Платформа виртуальной машины**).

5. Нажмите **ОК** и перезагрузите компьютер.

Вариант 2. Вернуть предыдущую версию операционной системы Windows 11 23H2.

Вариант 3. Использовать альтернативный способ VPN-подключения.

Ideco Client не работает, если внутренние ресурсы опубликованы через DNAT

> Видеоинструкцию смотрите по ссылкам:
>
> - Rutube

- Youtube
- docs.ideco.ru

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.

Полезные ссылки

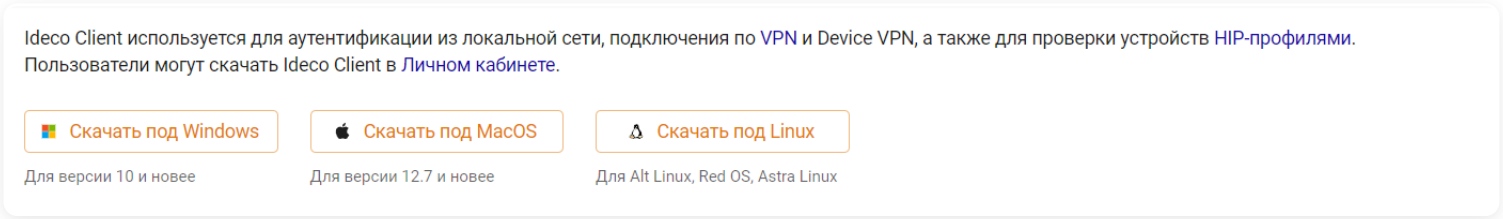
- **Балансировка VPN-подключений**
- **Настройка Device VPN**
- **Создание сертификатов для Device VPN**
- **Кастомная настройка Ideco Client**
- **Как включить режим отладки для Ideco Client**

Установка и настройка Ideco Client на Windows

Скачивание

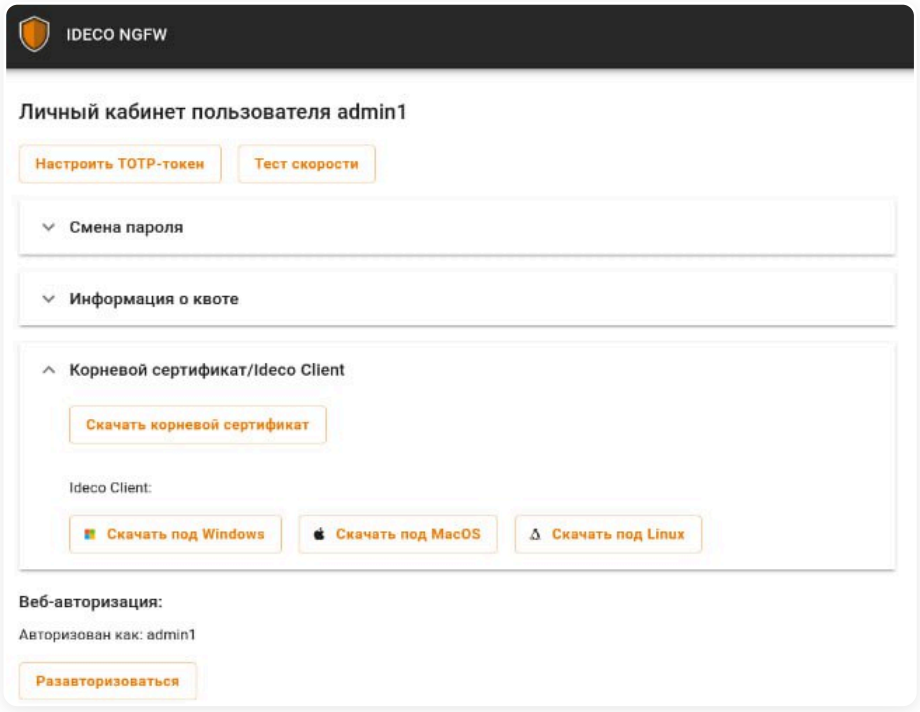
Для администратора

Перейдите в раздел **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Windows**:



Для пользователя

Нажмите на кнопку **Скачать под Windows** в личном кабинете пользователя:



Установка

Сохраните и запустите файл установки *IdecoAgent.msi*.

Если требуется заранее установить адрес подключения, в командной строке перейдите в директорию с файлом `cd [путь до файла]` и откройте файл `IdecoAgent.msi` с ключом `utm_address`, в котором нужно указать адрес Ideco NGFW (команда: `IdecoAgent.msi utm_address=адрес_ngfw`).

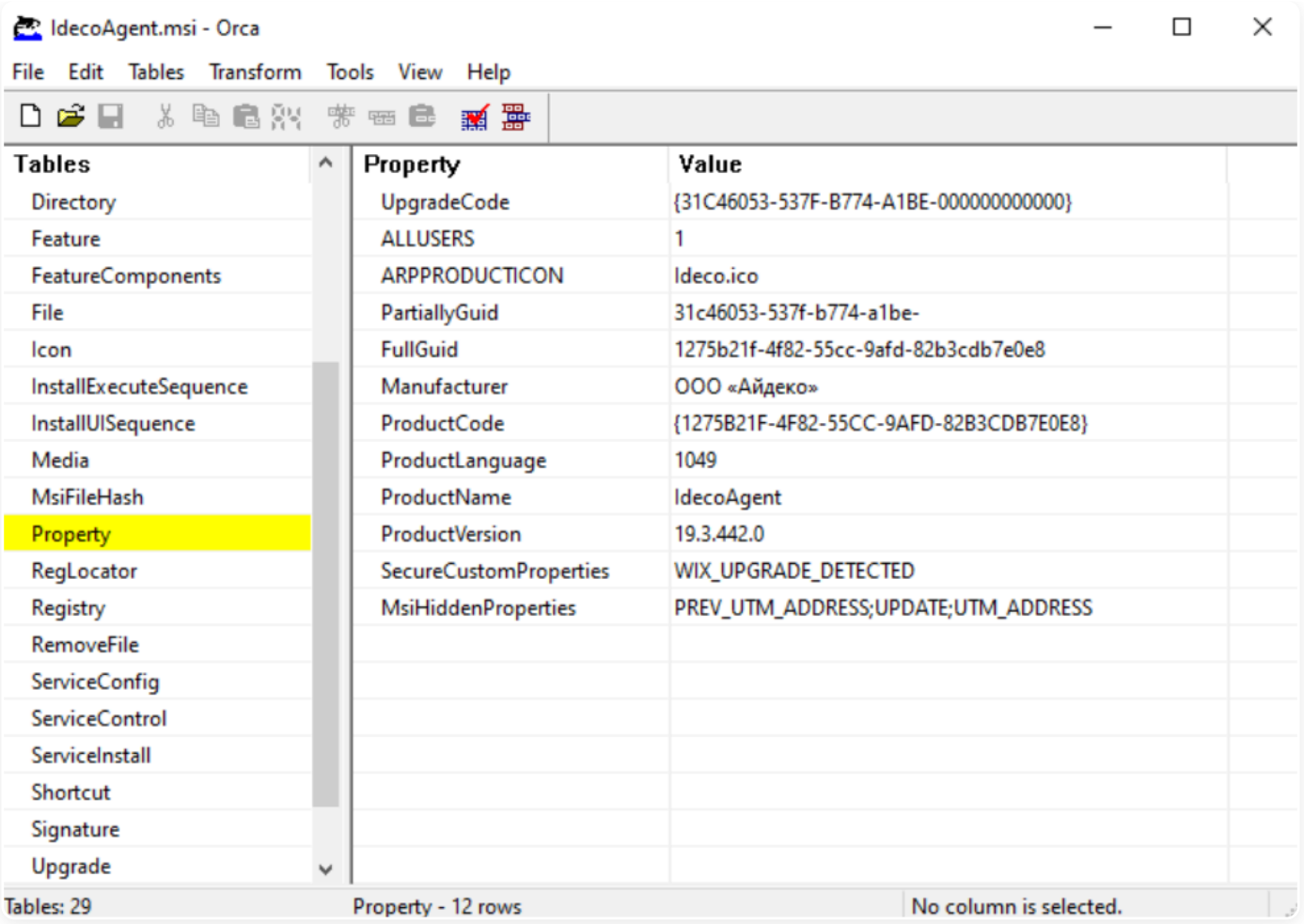
Чтобы оптимизировать процесс установки Ideco Client с помощью GPO, добавьте параметр адреса Ideco NGFW `IdecoAgent.msi UTM_ADDRESS=адрес_ngfw` в установочный файл `IdecoAgent.msi`. Для этого воспользуйтесь утилитой Orca.

Как добавить параметр в Orca

1. Запустите Orca.

2. Нажмите **File** → **Open** и откройте `IdecoAgent.msi`.

3. В дереве таблиц найдите **Property**:



4. Нажмите **Tables** → **Add Row**, чтобы добавить новую запись.

5. В поле **Property** введите `UTM_ADDRESS`, в поле **Value** - IP-адрес или доменное имя Ideco NGFW. Нажмите **Ок**.

6. Нажмите **File** → **Save**, чтобы сохранить изменения.

7. Закройте Orca.
В этом случае *msi-файл* будет установлен с уже заполненным полем **Хост**, а авторизация компьютера будет происходить через SSO-профиль по умолчанию в "тихом" режиме автоподключения.

Если Kaspersky Plus блокирует установку и обновление

1. Откройте **Настройки** → **Настройки безопасности** → **Исключения и действия с найденными объектами** → **Указать доверенные приложения**:

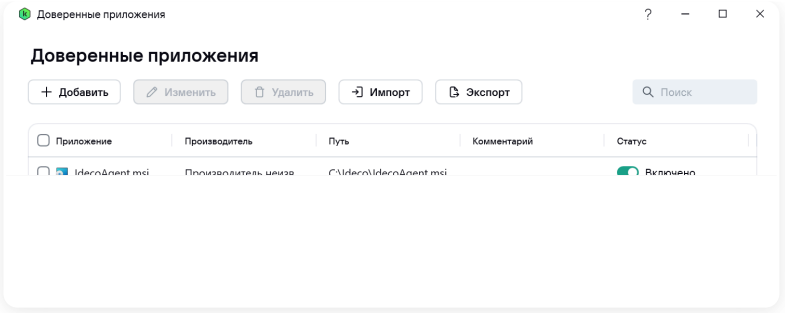
2. Нажмите **Добавить**, выберите скачанный msi-файл Ideco Client и нажмите **Выбрать**:

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:



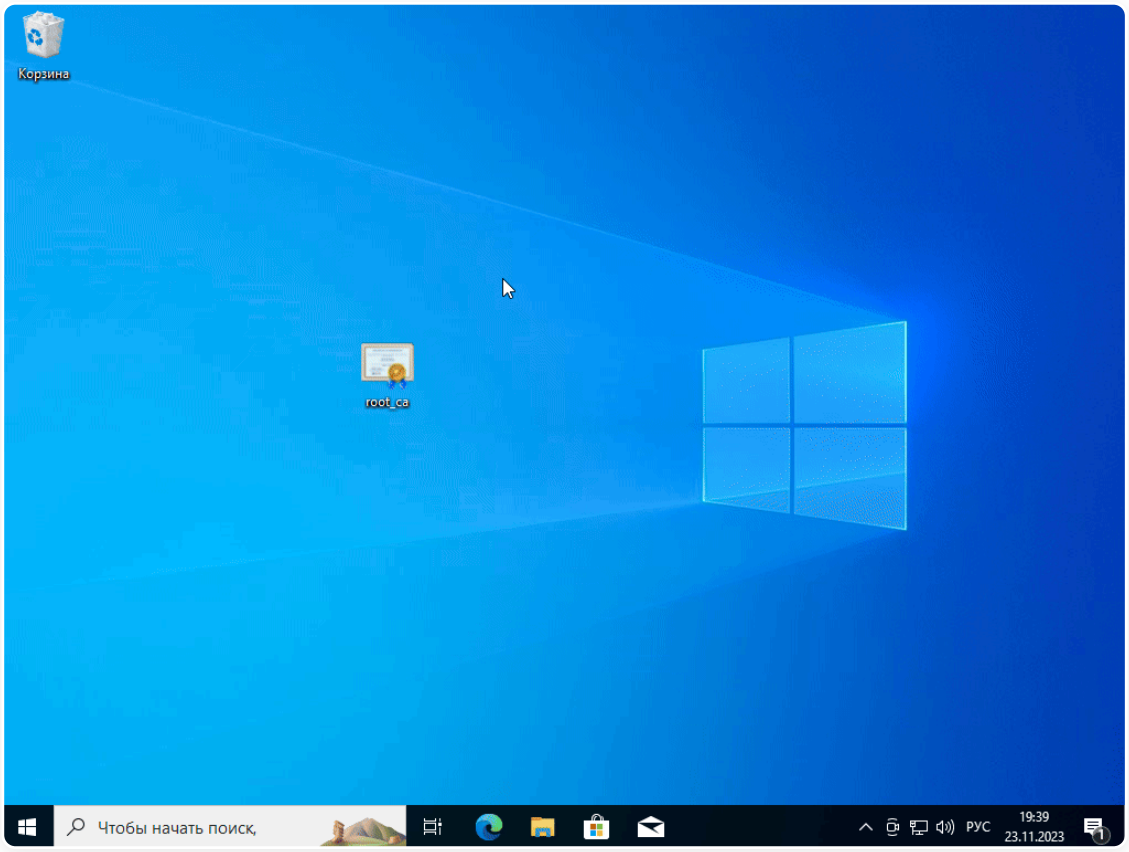
7. Откройте **Настройки** → **Настройки безопасности** → **Настройки сети** и настройте раздел:

8. Нажмите **Сохранить**.

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt, импортируйте корневой сертификат Ideco NGFW 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**.

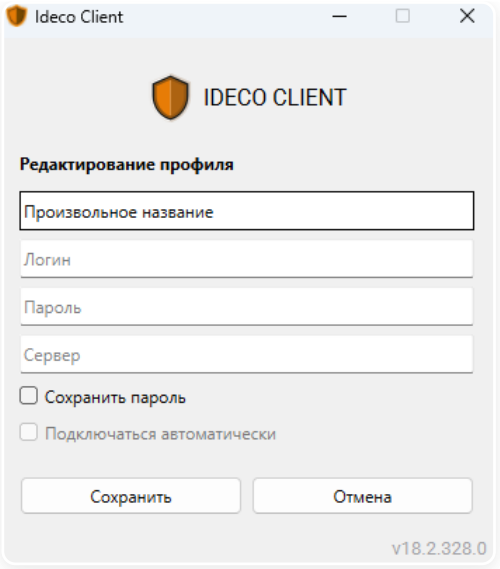
4. Выберите пункт **Поместить все сертификаты в следующее хранилище**, нажмите **Обзор** и выберите папку **Доверенные корневые центры сертификации**.

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 хост в зависимости от количества доменов, в которые введен NGFW:

NGFW введен в один домен

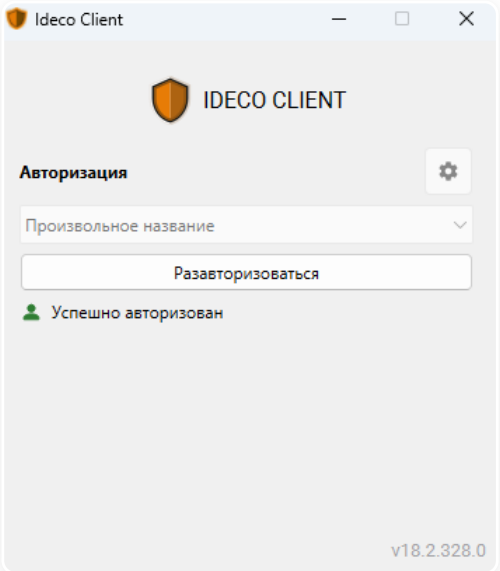
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:

NGFW введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW**:

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



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**.

Полезные ссылки

- **Кастомная настройка Ideco Client**
- **Как включить режим отладки для Ideco Client**

Установка и настройка Ideco Client на MacOS

Особенности работы Ideco Client на MacOS

- Ideco Client для MacOS требует версии системы 12.7 и выше;
- HIP-профили на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

- ОС;
- процесс;
- антивирус (Kaspersky).

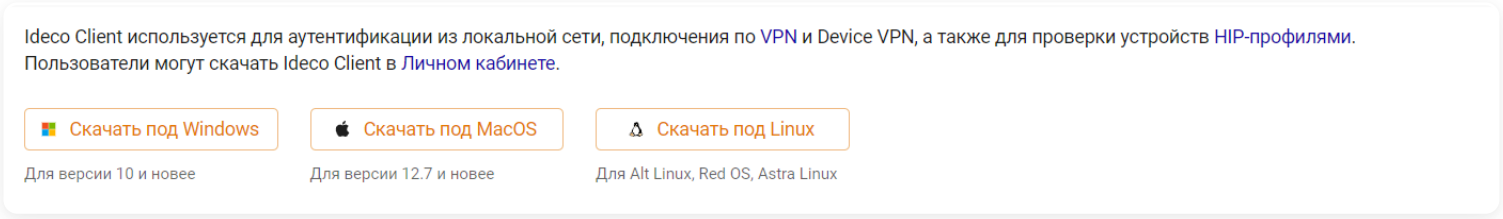
Недоступные HIP-профили

- домен;
- межсетевой экран;
- реестр (всегда только Windows);
- службы (всегда только Windows);
- пакет обновлений Knowledge Base (всегда только Windows).

Скачивание

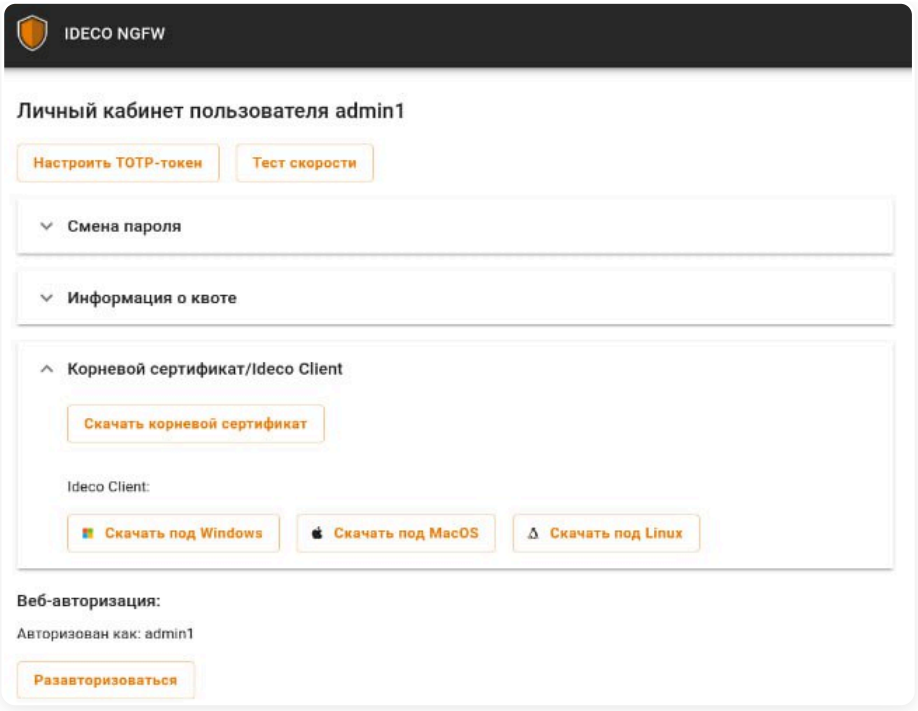
Для администратора

Перейдите в раздел **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под MacOS**:



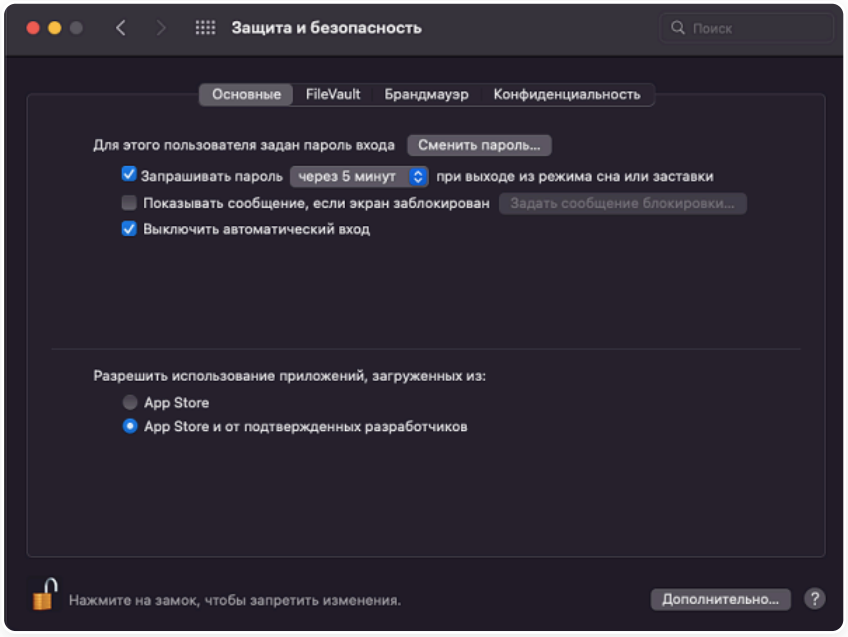
Для пользователя

Нажмите кнопку **Скачать под MacOS** в личном кабинете пользователя:



Установка

В некоторых версиях MacOS необходимо явно разрешить установку приложения не из App Store. Для этого перейдите в раздел **Защита и безопасность** → **Основные** и разрешите использование приложений, загруженных из **App Store и от подтвержденных разработчиков**:

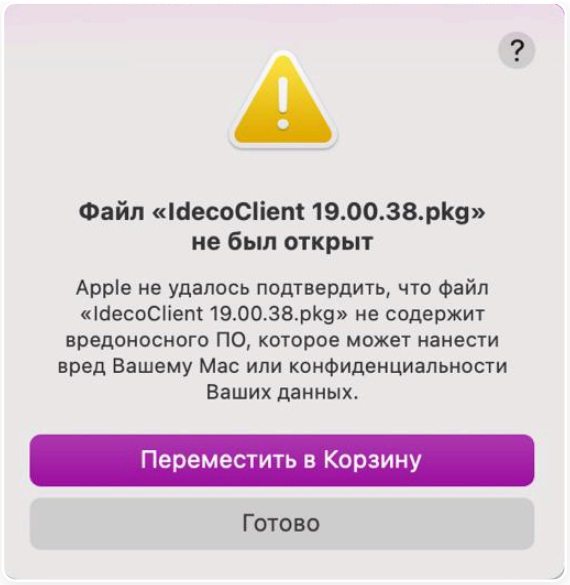


Чтобы установить **Ideco Client** на MacOS, выполните действия:

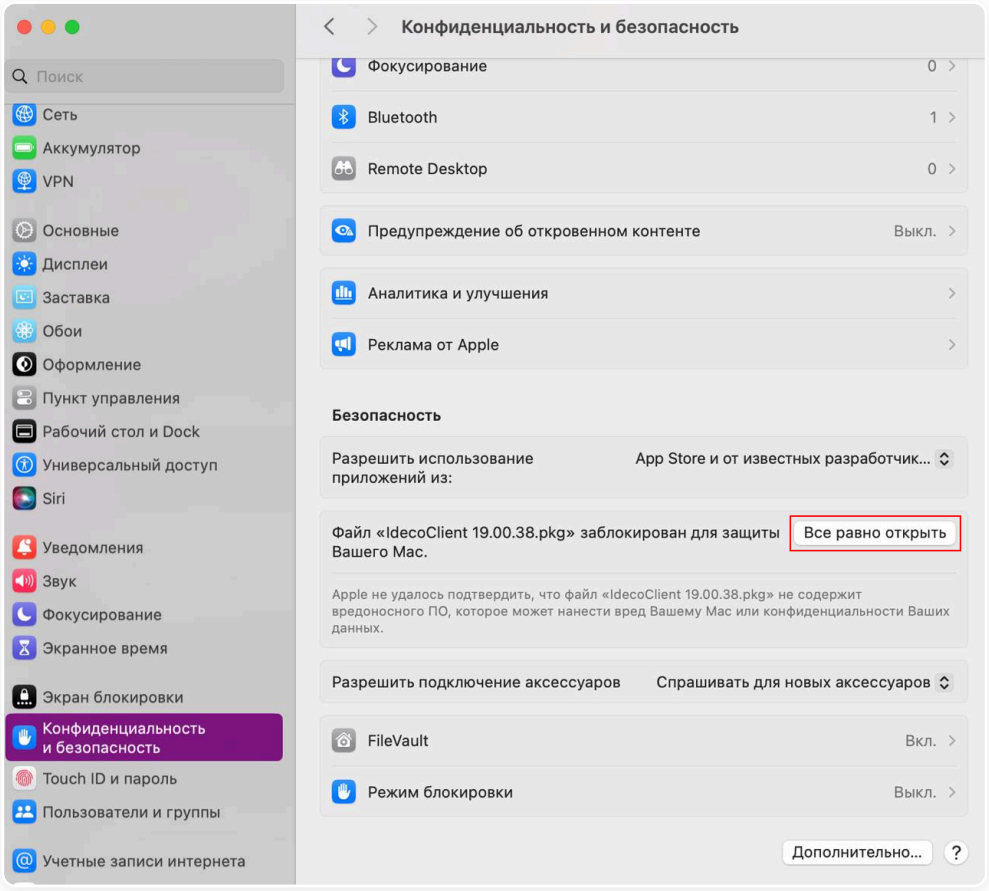
1. Кликните по файлу *IdecoClient.pkg* правой кнопкой мыши и выберите **Открыть**.

MacOS Sequoia

1. При открытии файла *IdecoClient.pkg* система сообщит о потенциальной опасности приложения. Нажмите **Готово**:



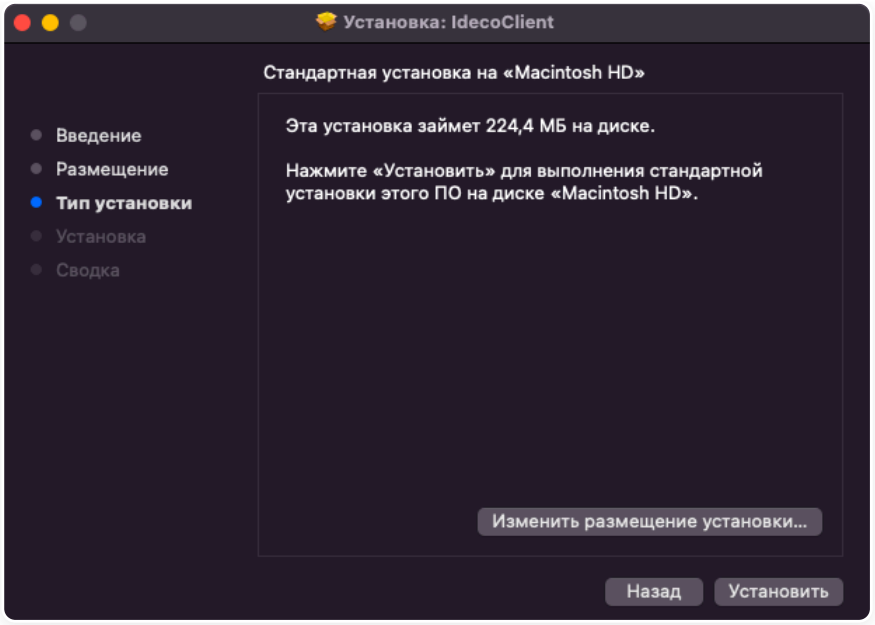
2. Перейдите в раздел **Конфиденциальность и безопасность** и нажмите **Все равно открыть** рядом с именем файла:



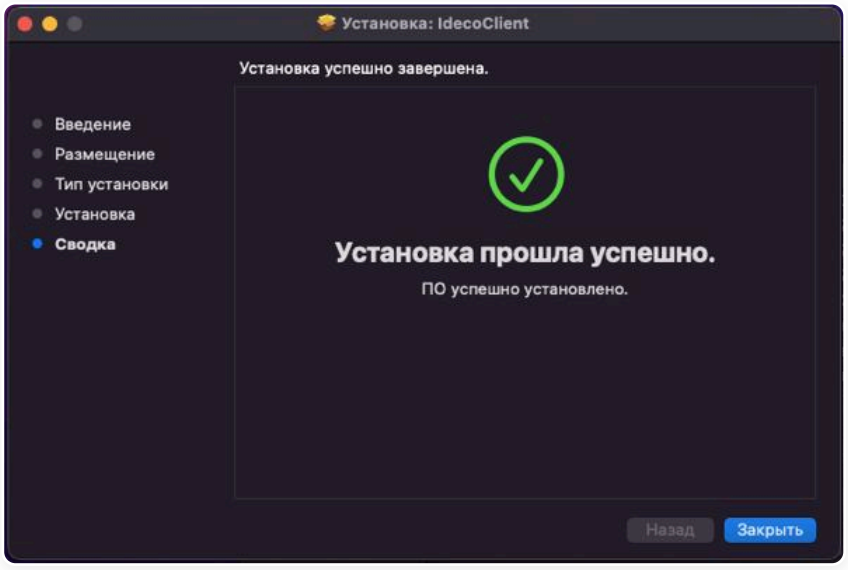
MacOS Monterey и MacOS Sonoma

При открытии файла *IdecoClient.pkg* система выдаст предупреждение. Подтвердите действие:

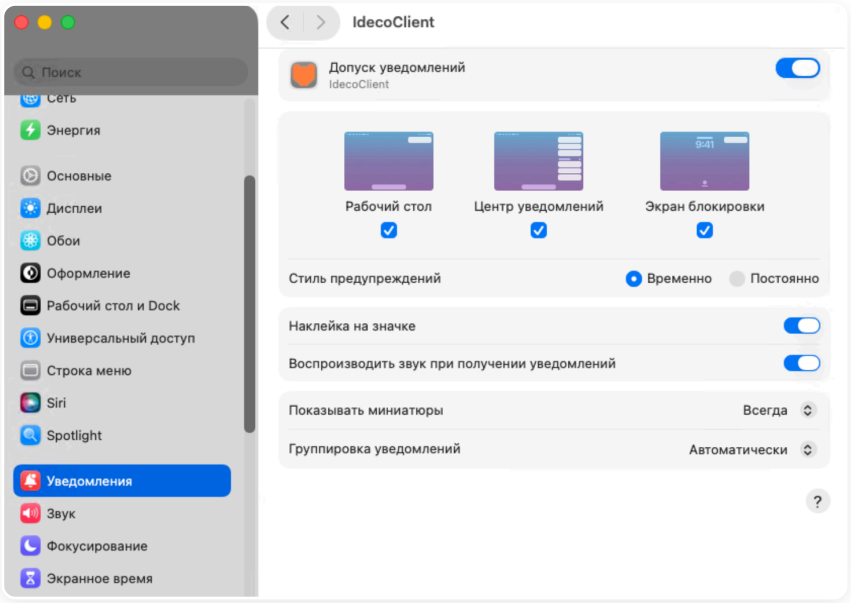
2. Нажмите **Продолжить**. В открывшемся окне нажмите **Установить**:



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 по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt убедитесь, что срок действия оконечного сертификата на этот домен или IP-адрес составляет не более 825 дней. Если это так, то импортируйте **корневой** сертификат Ideco NGFW на компьютер. Если срок действия оконечного сертификата на этот домен или IP-адрес превышает 825 дней, загрузите на NGFW свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

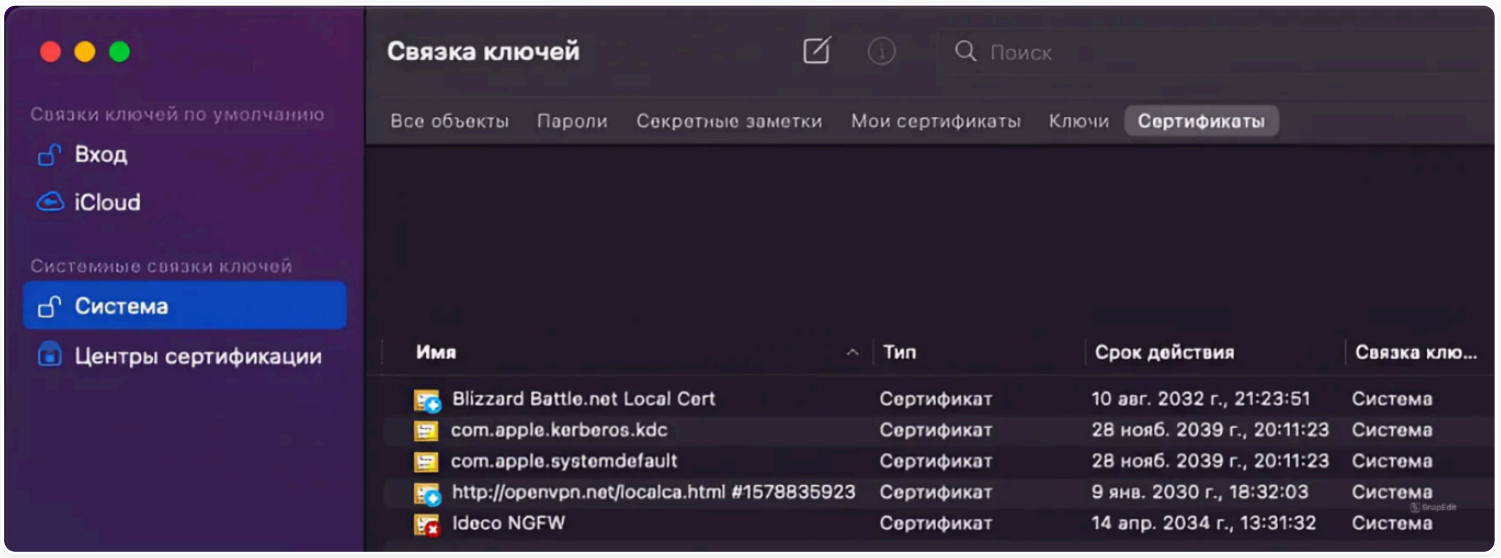
Установка корневого сертификата Ideco NGFW на MacOS

Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW 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 получить доступ к этим файлам и прочитать их. Рекомендуем сохранить файлы в другую директорию, например, в корневую директорию домашней папки пользователя.

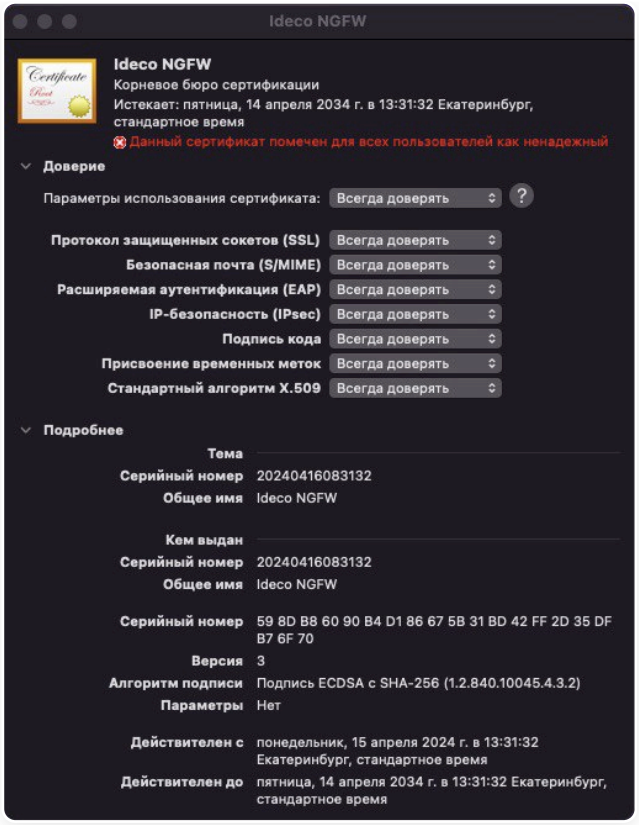
Установка через Связку ключей

1. Откройте скачанный файл *root_ca.crt* в приложении **Связка ключей**, сертификат Ideco NGFW появится в папке **Система**:

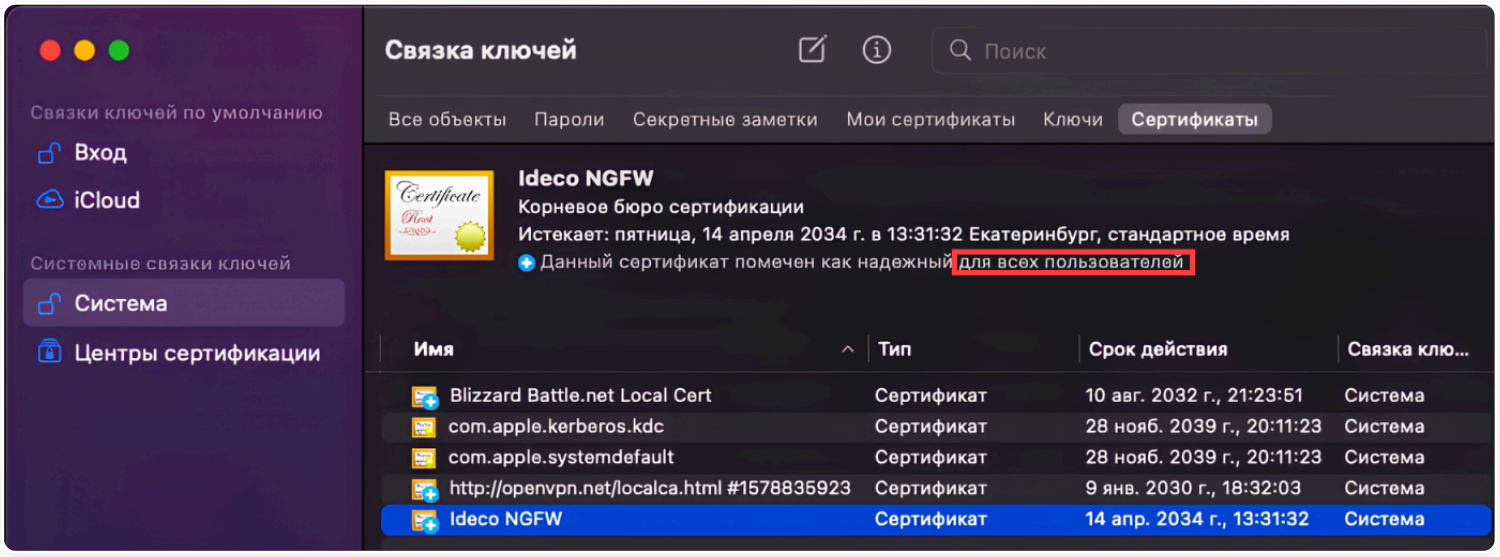


2. Нажмите по сертификату правой кнопкой мыши и выберите **Свойства**.

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:

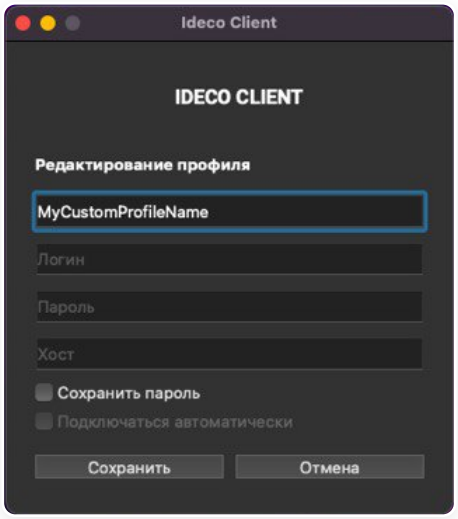
```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <путь к сертификату>/root_ca.crt
```

2. Перезагрузите компьютер.

Первый запуск

1. Запустите Ideco Client.

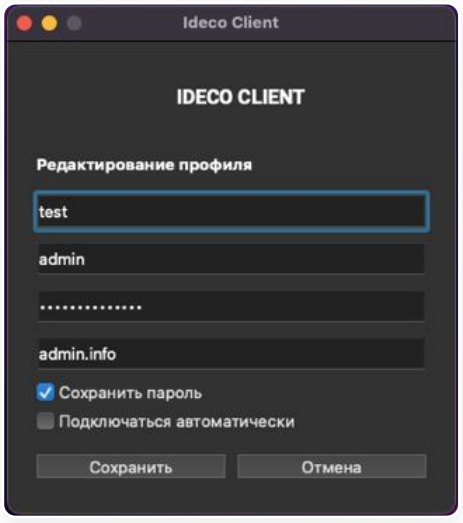
2. Введите данные:



- **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 в зависимости от количества доменов, в которые введен NGFW:

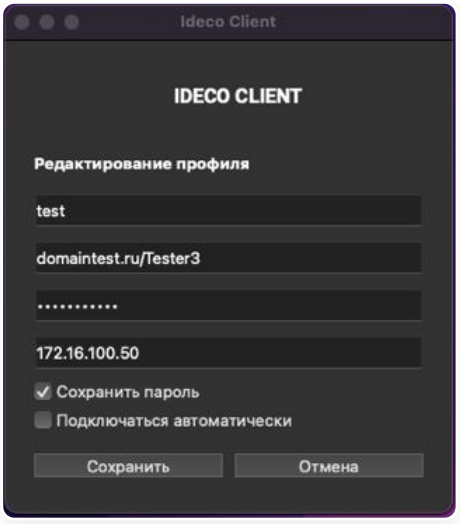
NGFW введен в один домен

Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:



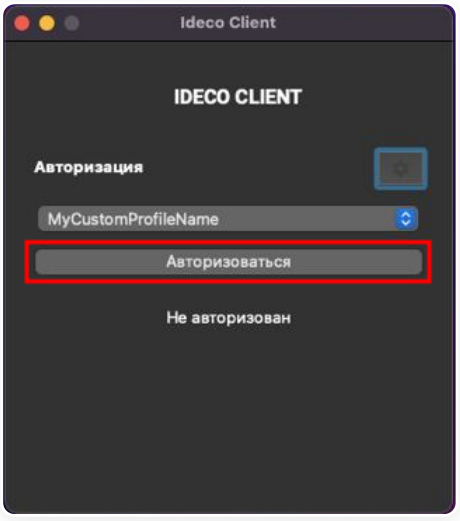
NGFW введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW**:



3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



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**.

Установка и настройка Ideco Client на Linux

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:

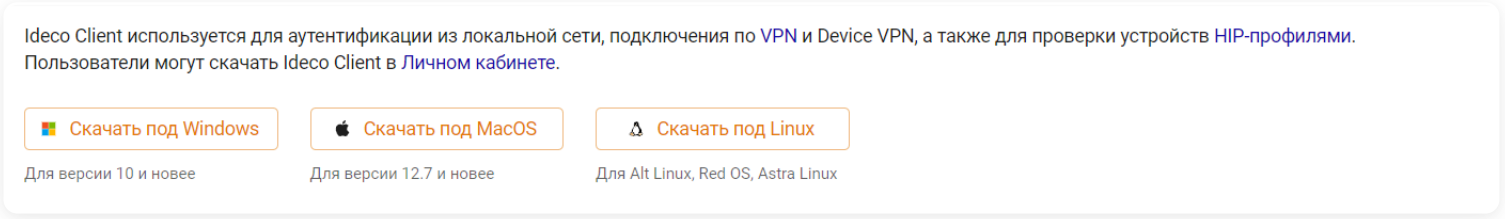
```
bool os_specific::isProcessExist(const std::string &processName)
```

Длина строки `processName` составляет не более 15 символов. Если название процесса длиннее, оно будет обрезано до максимально доступного числа символов. В этом случае проверка не будет выполнена корректно.

Скачивание

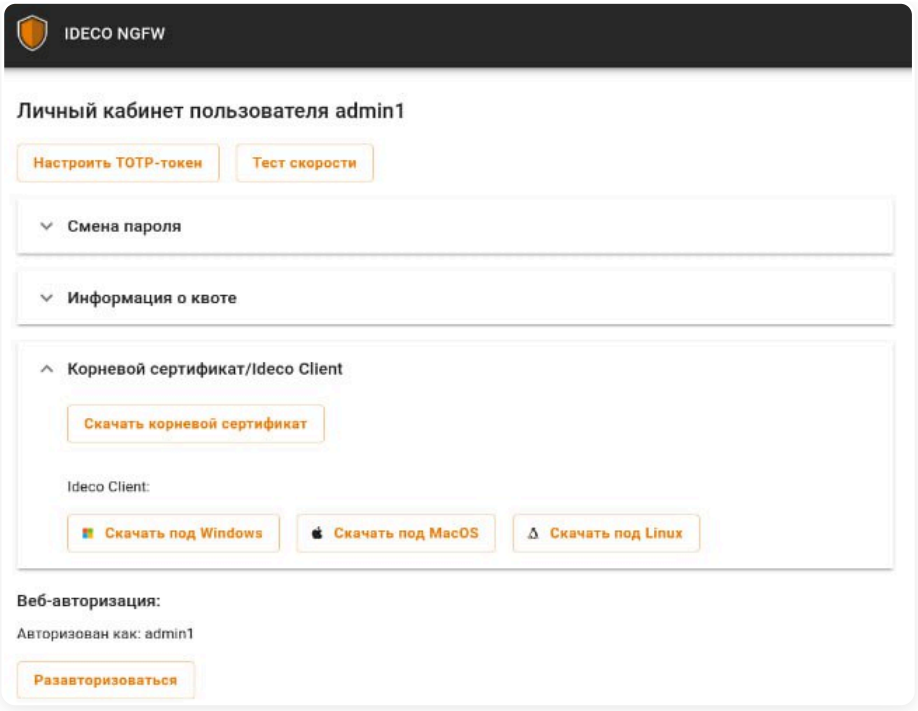
Для администратора

Перейдите в раздел **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Linux**:



Для пользователя

Перейдите в личный кабинет пользователя и нажмите **Скачать под Linux**:



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 IdecoAgent.sh
```

3. Запустите файл установки Ideco Client:

```
./IdecoAgent.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 на Astra Linux удалите настройку службы IdecoService:

```
sudo rm /etc/systemd/system/IdecoService.service
```

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW 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 на компьютер. Если срок действия сертификата на этот домен или IP-адрес превышает 825 дней, загрузите на NGFW свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

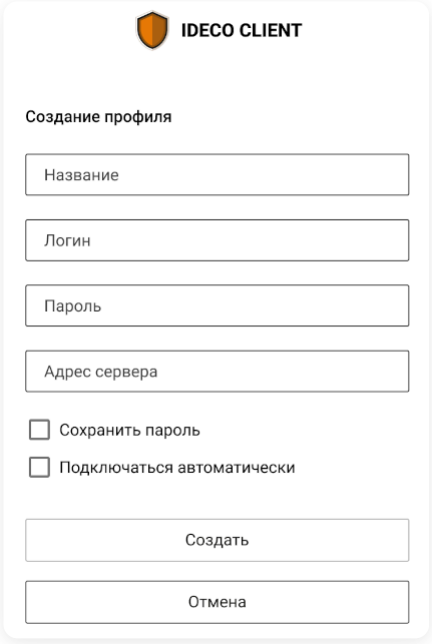
Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- 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.

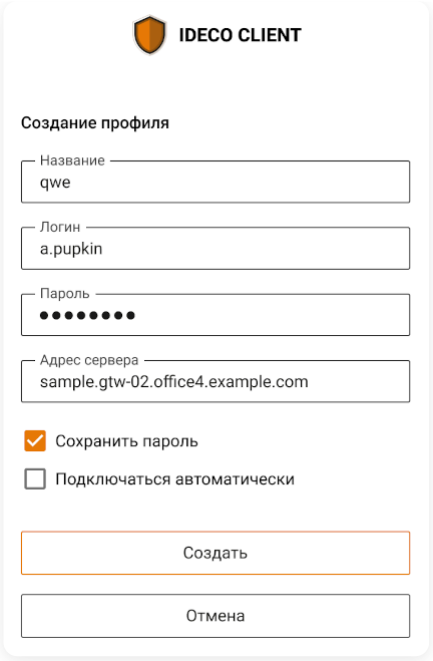
2. Введите данные:



- **Имя профиля** - может не совпадать с логином и будет использоваться при выборе профиля для авторизации.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Хост** - укажите логин и хост в зависимости от количества доменов, в которые введен NGFW:

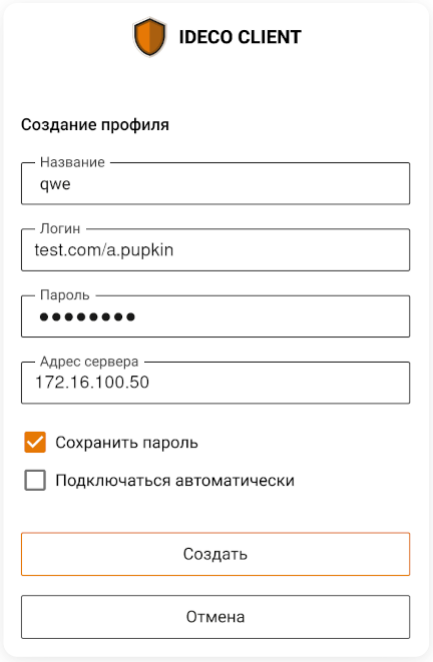
NGFW введен в один домен

Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес.



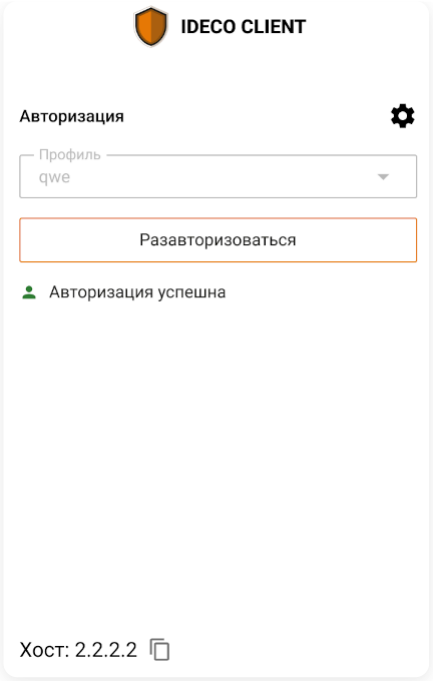
NGFW введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW**.



3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



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>
```

2. Запустите файл удаления Ideco Client:

```
./uninstall.sh
```

Настройка Device VPN

Device VPN позволяет получить доступ к устройству даже когда пользователь не использует Ideco Client, и устройство имеет доступ в интернет или до Ideco NGFW. Это позволяет осуществлять удаленное администрирование, обновление ПО и антивирусов, мониторинг.

В качестве **Сертификата устройства** Device VPN можно использовать:

- Самоподписанные сертификаты.
- Сертификаты, выданные Центрами сертификации (Certificate Authority, CA).

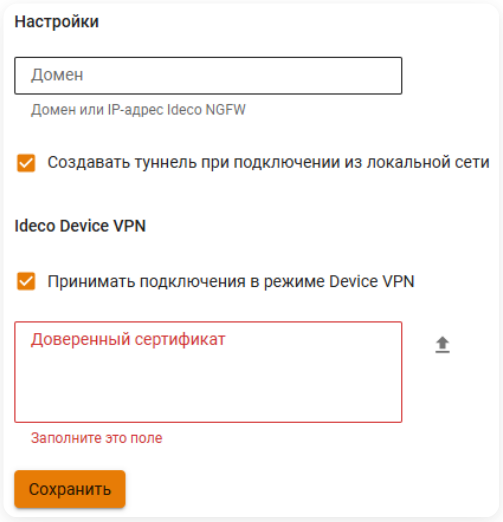
Чтобы подключить устройство к Ideco NGFW в режиме Device VPN, выполните действия:

1. Перейдите в раздел **Пользователи → Ideco Client**.

2. Введите домен или IP-адрес Ideco NGFW и включите настройку **Создавать туннель при подключении из локальной сети**, если устройства пользователей находятся в локальной сети.

3. Включите настройку **Принимать подключения в режиме Device VPN**.

4. Загрузите доверенный сертификат в формате `.pem` и нажмите **Сохранить**. Процесс создания сертификата описан в статье Создание сертификатов для Device VPN:



5. Установите Ideco Client на устройство пользователя.

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.

> 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:

Для Windows

Откройте командную строку от имени администратора и введите:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --set-devicevpn-cert-path=<абсолютный путь до файла сертификата> --set-devic
```

Для вывода заданных параметров в командную строку воспользуйтесь командой:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --print-devicevpn-config=True
```

Для Linux

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient.sh --set-devicevpn-cert-path=<абсолютный путь до файла сертификата> --set-d
```

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-devicevpn-cert-path=<абсолютный путь до файла сертификата> --set-devi
```

Для вывода заданных параметров в консоль воспользуйтесь командой:

```
(sudo) <абсолютный путь до IdecoClient>/IdecoClient --print-devicevpn-config=True
```

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 в дальнейшем. Ideco NGFW извлекает имя пользователя из поля **Common Name** сертификата.

При неудачной конфигурации Device VPN служба Ideco Client будет постоянно пытаться подключиться к Ideco NGFW. 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 убедиться, что подключение Device VPN выполнено.

Создание сертификатов для Device VPN

> В статье описан процесс создания сертификатов с использованием OpenSSL для подключения по Device VPN между Ideco NGFW 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*:

```
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.

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:

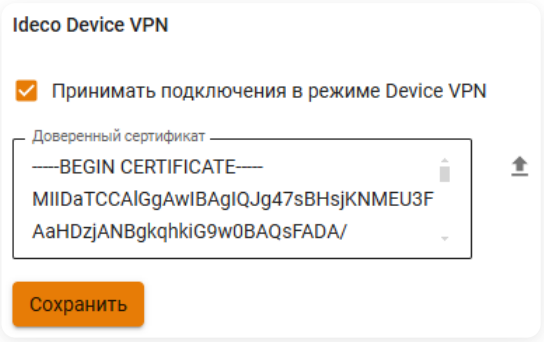
- **A challenge password []** - пароль для дополнительной аутентификации. Рекомендуем оставить поле пустым.
- **An optional company name []:** - полное юридическое название организации.

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.

5. В разделе **Пользователи** → **Ideco Client** в поле **Доверенный сертификат** загрузите созданый сертификат `ideco-dvpn_root-ca.pem` без приватного ключа:



После этого корневой сертификат будет необходим для создания пользовательских сертификатов.

Создание пользовательского сертификата для конечного устройства

1. Сгенерируйте приватный ключ без применения шифрования (в дальнейшем незашифрованный ключ размещается 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.

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)** - название региона или области (например, Moscow).
- **Locality Name (eg, city) [Default City]** - название города (например, Saint Petersburg).
- **Organization Name (eg, company) [Default Company Ltd]** - название организации.
- **Organizational Unit Name (eg, section) []** - название подразделения организации.
- **Common Name (eg, your name or your server's hostname) []** - 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. Создайте файл **client1-dvpn.ext** для генерации сертификата. Включите в него параметры:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
```

5. 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.

6. Проверьте, что сертификат был успешно создан командой:

```
openssl x509 -text -noout -in client1-dvpn.crt
```

- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат;
- Сертификат должен иметь атрибут `CA:FALSE` и `Subject Key Identifier`.

7. Объедините приватный ключ и сертификат пользовательского устройства:

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

```
Get-Content client1-dvpn.key, client1-dvpn.crt | Set-Content 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.

8. Сертификат `client1-dvpn.pem` с приватным ключом внутри, полученный на этом этапе, устанавливается на пользовательском устройстве и используется в параметрах Ideco Client.

Балансировка и редиректы VPN-подключений

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.

При указании в параметре `target` SRV-записи `.` подключение происходить не будет, и 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 кнопки **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. Затем происходит сортировка сначала по параметру SRV-записи `priority`, затем при равенстве параметров `priority` у двух и более записей происходит сортировка 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.

Алгоритм работы Ideco Client при редиректах

После формирования списка для подключения Ideco Client пытается подключиться к серверам из списка. Если при попытке подключения отправлен редирект с кодом ответа 302, то Ideco Client будет пытаться подключиться по указанному в редиректе адресу до первой успешной установки соединения.

Если при подключении к серверу в ответе приходит редирект с кодом ответа 302, то для полученного в редиректе адреса поиск SRV-записей производиться не будет. 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.

Подробнее о работе Ideco Client при редиректе в статье. Обработка запросов с редиректом позволяет использовать VPN-балансировщик для распределения нагрузки между несколькими NGFW.

Кастомная настройка Ideco Client

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

- Запрет на создание новых профилей;
- Запрет на сохранение пароля;
- Запрет на редактирование профиля;
- Установка профиля по умолчанию;
- 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:

```
{
    "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.
- `"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 его значение 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.

Ideco NGFW использует имя входа пользователей AD с атрибутом `sAMAccountName` (SAM). Если на AD используется атрибут `userPrincipalName` (UPN), необходимо, чтобы атрибуты SAM и UPN были идентичны. Различия в SAM и UPN приведут к проблемам с аутентификацией пользователей на NGFW.

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.

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 True
```

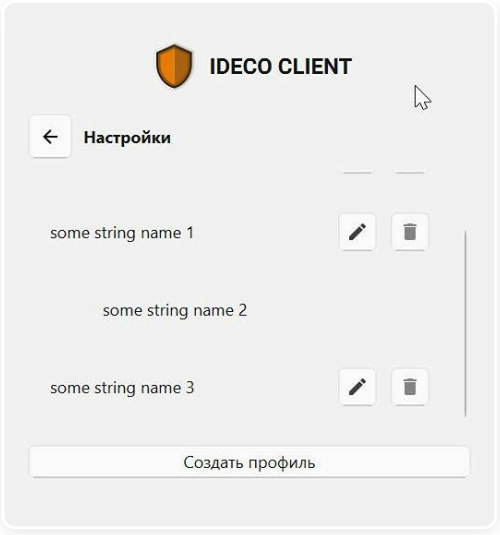
Linux или MacOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --reset-json-config True
```

Примеры настроек файла конфигурации

Запретить пользователю редактировать преднастроенный профиль



Профиль **some string name 2** создан в файле конфигурации и его 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 и их можно редактировать или удалять.

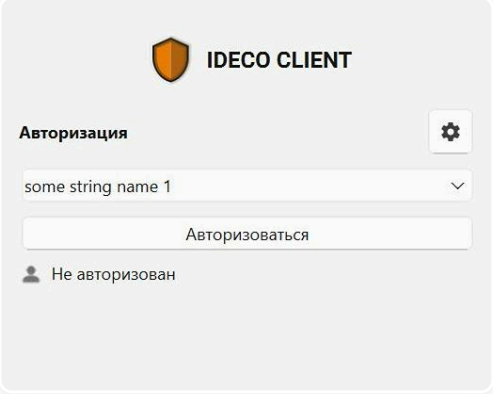
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "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.
- `"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.
- `"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.
- `"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:

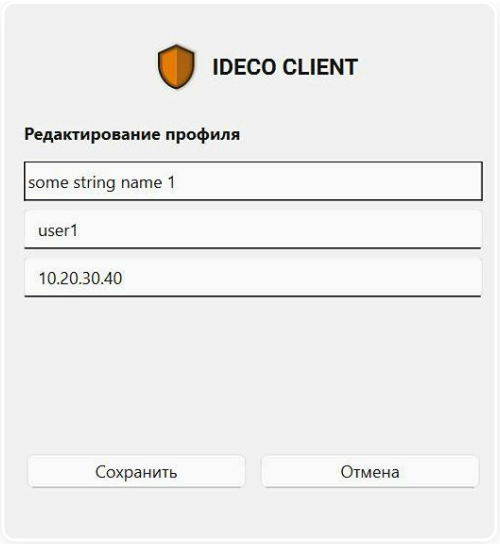
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "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.
- `"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.
- `"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.
- `"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.
- `"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.

Профили устройств

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

- 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

- Операционная система
- Пакет обновлений Windows
- Антивирус
- Межсетевой экран
- Процесс, запущенный на устройстве
- Запущенная служба Windows
- Ключ реестра Windows

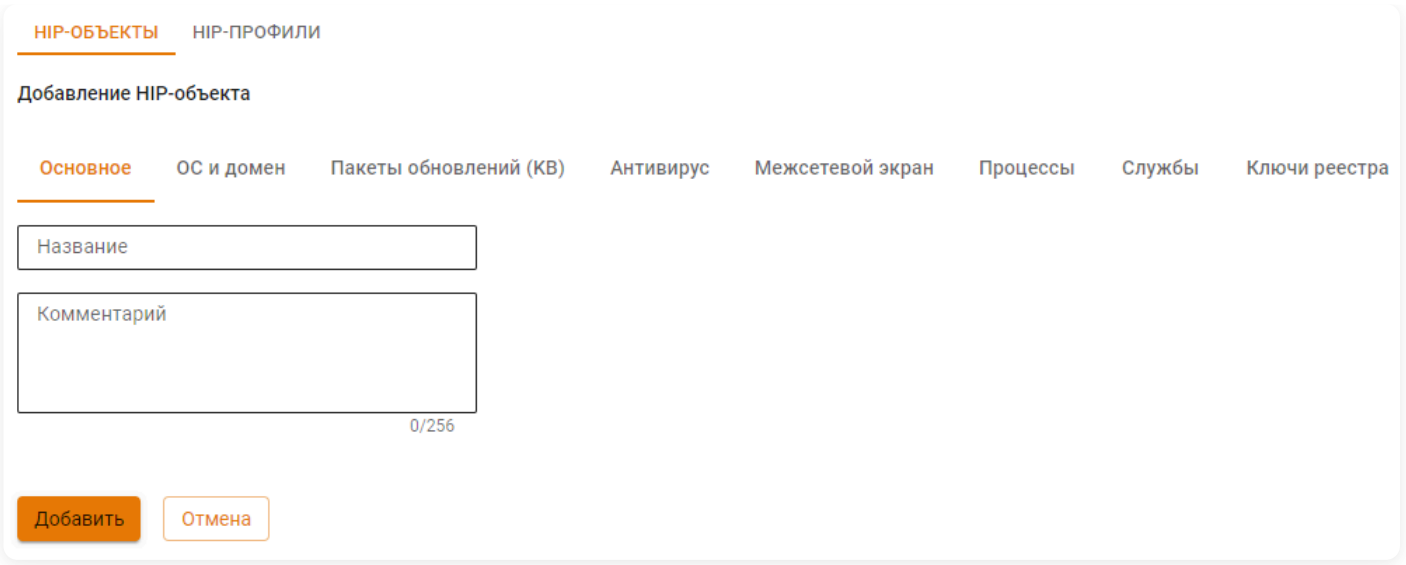
HIP-объекты

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.

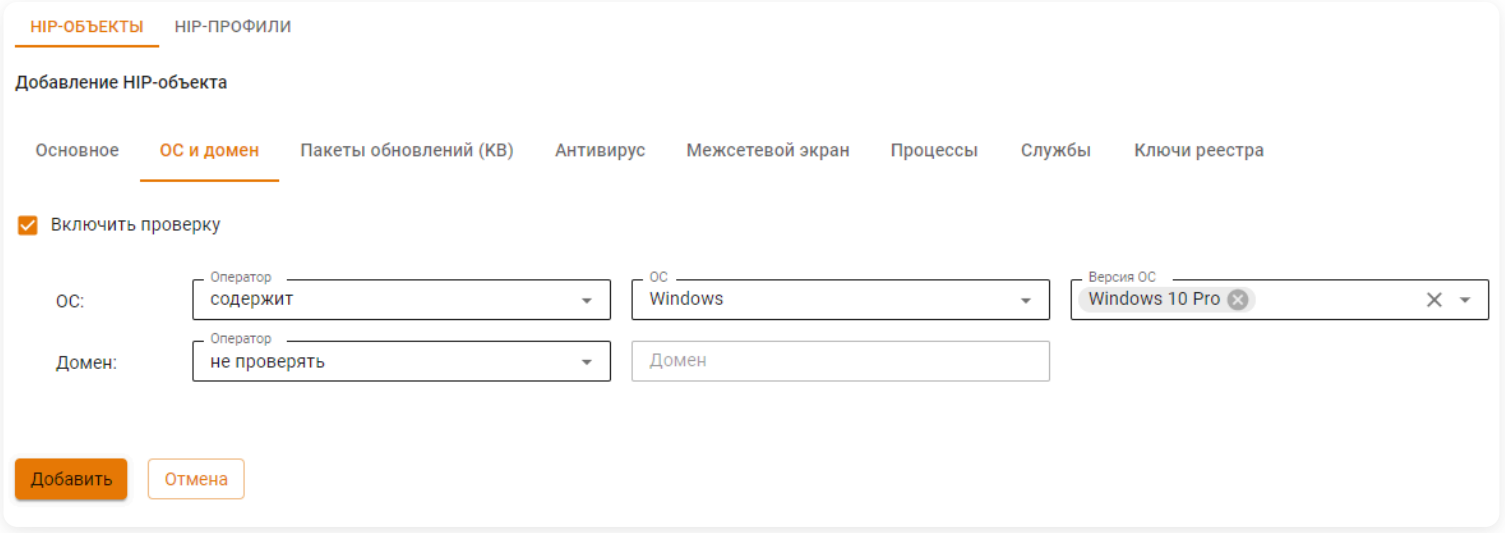
Для создания HIP-объекта выполните действия:

1. Перейдите в **Профили устройств** → **HIP-объекты** и нажмите **Добавить**.

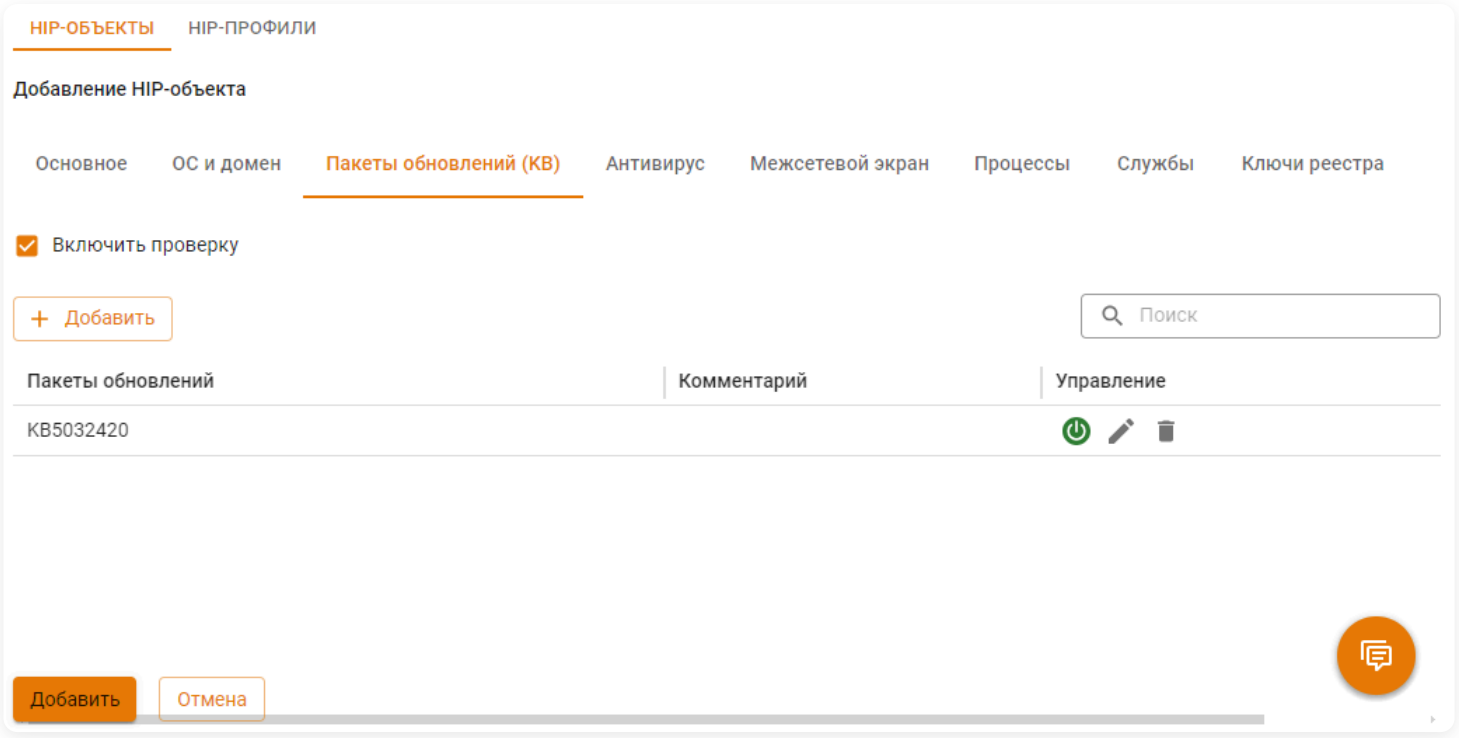
2. Введите **Название HIP-объекта** и выберите критерии для проверки:



3. Нажмите **Включить проверку** для проверки выбранного критерия и заполните поля, указав оператор (**Содержит**, **Не содержит**, **Не проверять**):



Критерий может не содержать оператор:



4. После этого 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

HIP-профили

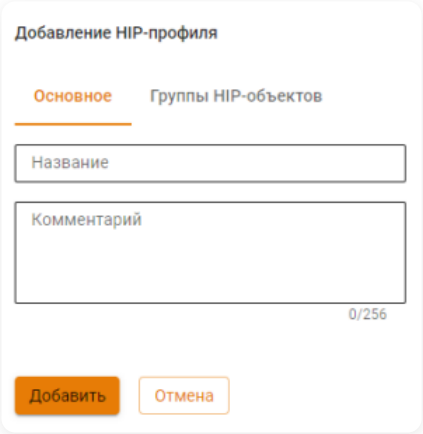
На вкладке создаются HIP-профили, состоящие из сгруппированных с помощью логических операций HIP-объектов И/ИЛИ.

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.

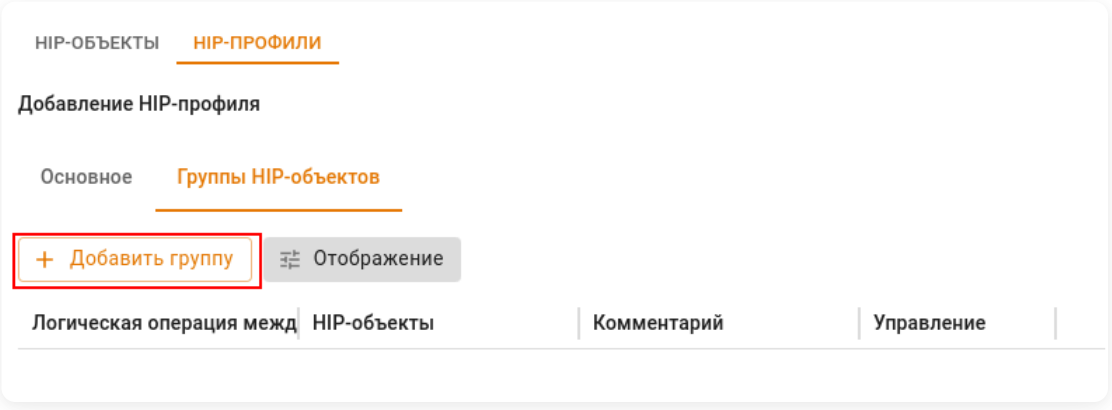
Для создания HIP-профиля выполните действия:

1. Перейдите в раздел **Профили устройств** → **HIP-профили** и нажмите **Добавить**.

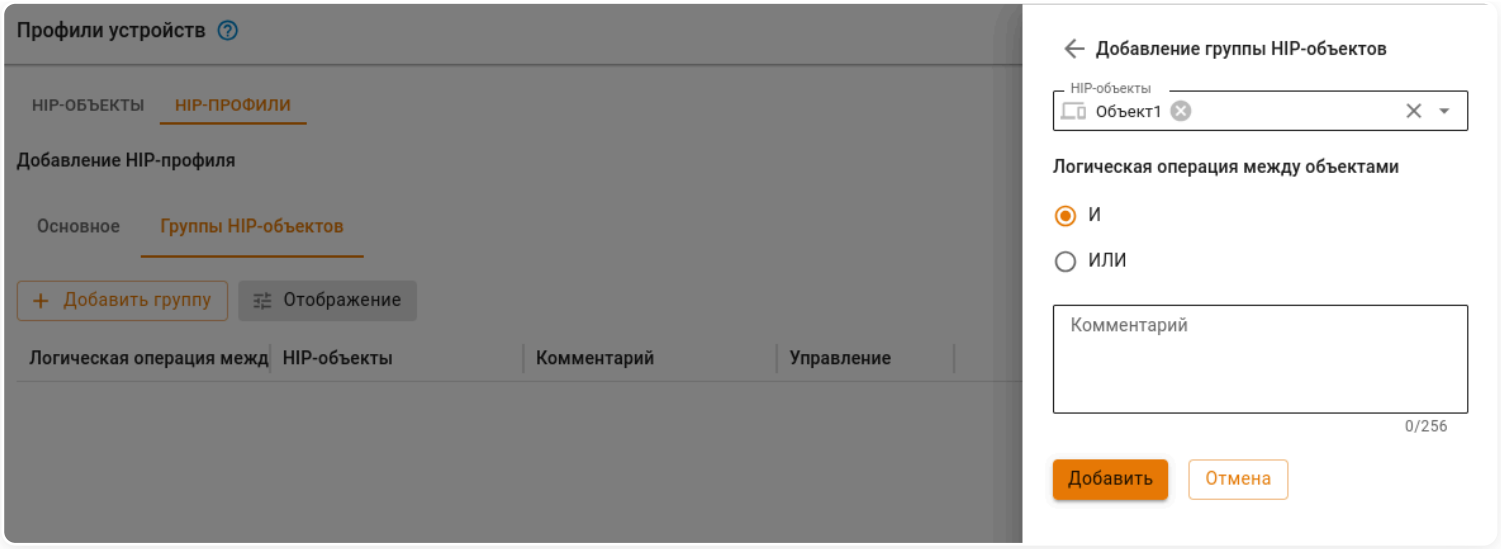
2. Введите **Название HIP-профиля**:



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 правиле FORWARD **Файрвола**. 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 **Файрвола**. Чтобы с помощью профилей ограничить или разрешить доступ к ресурсами сети, необходимо:

1. Создать HIP-объекты.

2. Сгруппировать созданные HIP-объекты в HIP-профилей.

3. В разделе **Правила трафика** → **Файрвол** → **FORWARD** создать и включить правило с использованием одного или нескольких профилей, созданных в пункте 2.

Проверка профилей происходит каждые 15 минут.

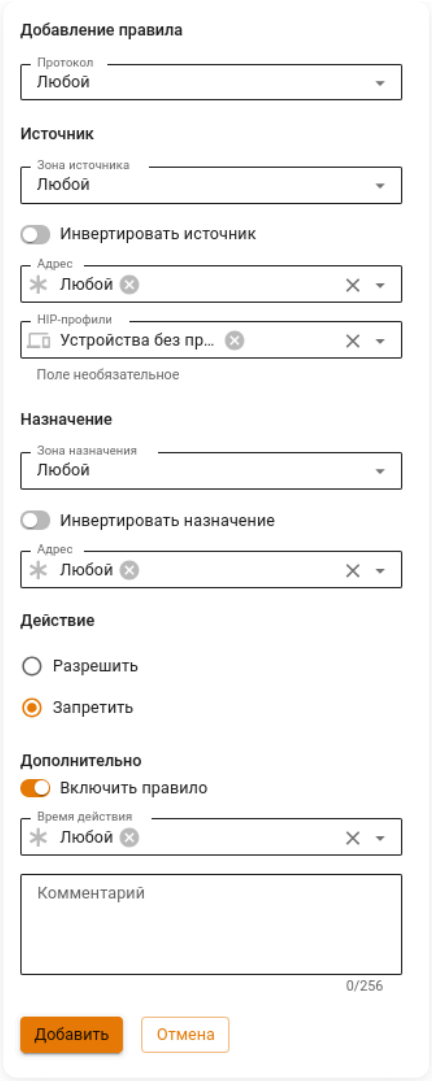
Примеры использования

Запрет доступа к сети устройствам без профиля

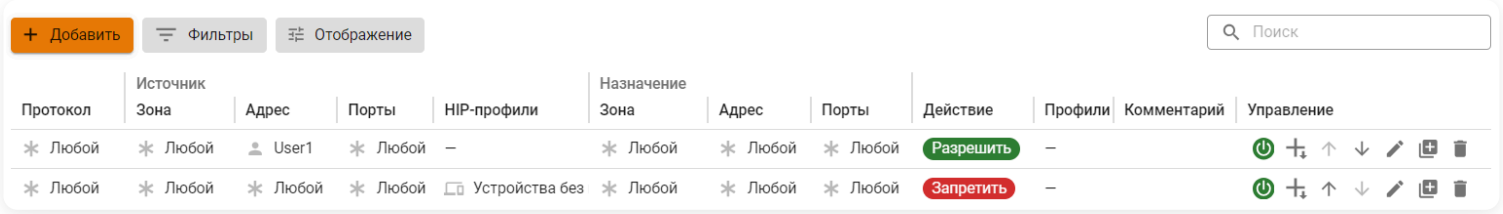
Устройствам, которые не прошли проверку на соответствие ни одному из созданных HIP-профилей, назначается специальный HIP-профиль **Устройство без профиля**. Доступ таких устройств к сети можно ограничить правилом **Файрвола**. Для этого:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD**.

2. Создайте и включите правило вида:



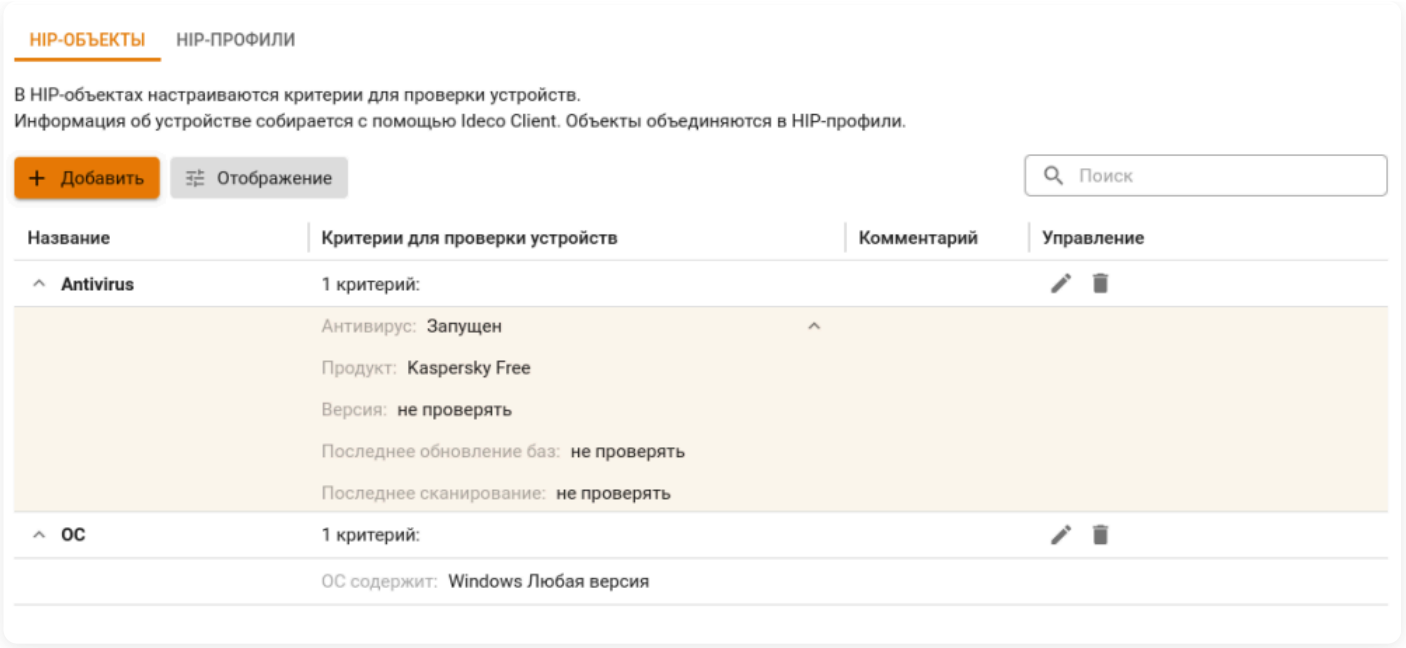
Важно!
Если в таблице правил **Файрвола** выше запрещающего правило находится другое правило, которому соответствует трафик одного или нескольких устройств без профиля (например, правило для пользователя или группы пользователей без указания HIP-профиля), то к трафику будет применено правило, расположенное выше в таблице. Например:



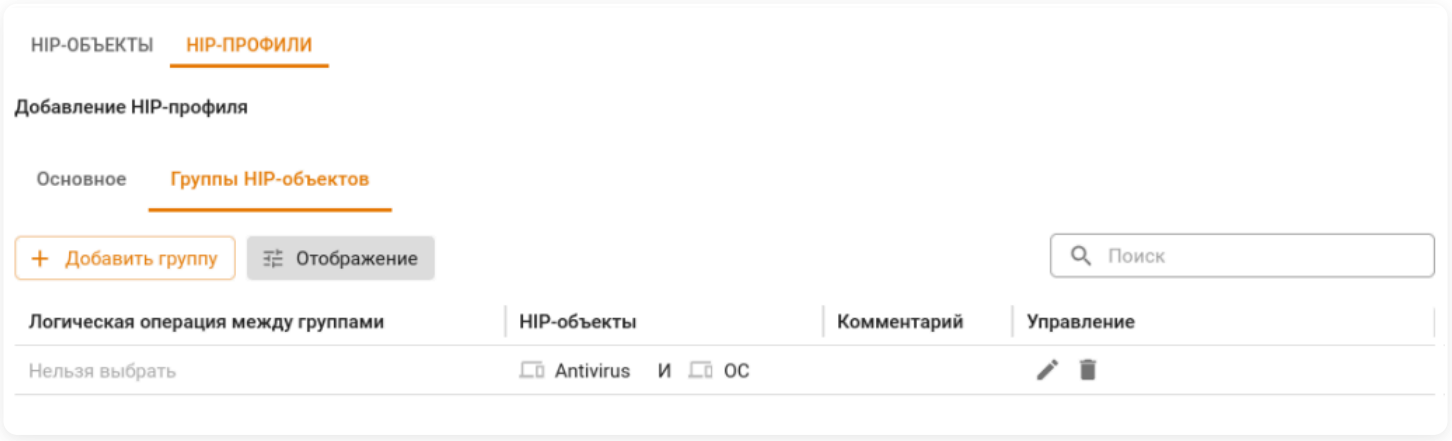
Ограничение доступа устройств к сети

В качестве примера настроим **Файрвол** так, чтобы пользователи имели доступ к сети, только если их устройства соответствуют HIP-профилю `Profile1`. Для этого:

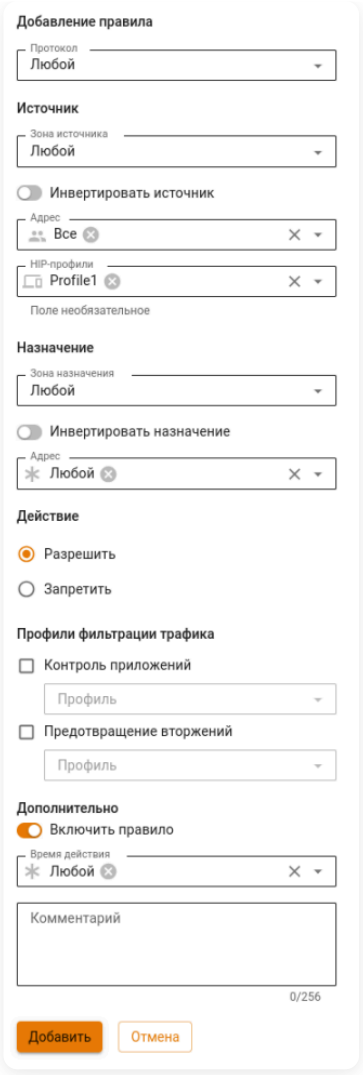
1. Перейдите в раздел **Пользователи** → **Профили устройств** → **HIP-объекты** и создайте требуемые HIP-объекты:



2. Перейдите на вкладку **HIP-профили** и создайте профиль с созданными ранее HIP-объектами:



3. Перейдите в раздел **Правила трафика** → **Файрвол** → **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.

Active Directory/Samba DC

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Название службы раздела **Active Directory/Samba DC**: `ideco-ad-backend`, `ideco-ad-log-collector@<имя домена>`.

Список служб для других разделов доступен по ссылке.

При интеграции импортируются учетные записи и номера телефонов пользователей, исключая пароли. При аутентификации пользователей проверка осуществляется средствами Active Directory или Samba DC соответственно.

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, перейдите в раздел Управление сервером → Терминал и выполните команду:

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

Особенности интеграции с несколькими доменами

- Из дерева контроллеров домена в Ideco NGFW импортируются данные только того контроллера, для которого был запущен импорт пользователей.
- При импорте пользователей из разных доменов необходимо убедиться, что учетные записи не имеют одинаковых логинов. В противном случае система выдаст сообщение об ошибке.
- 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 Ideco NGFW).

Ввод сервера в домен

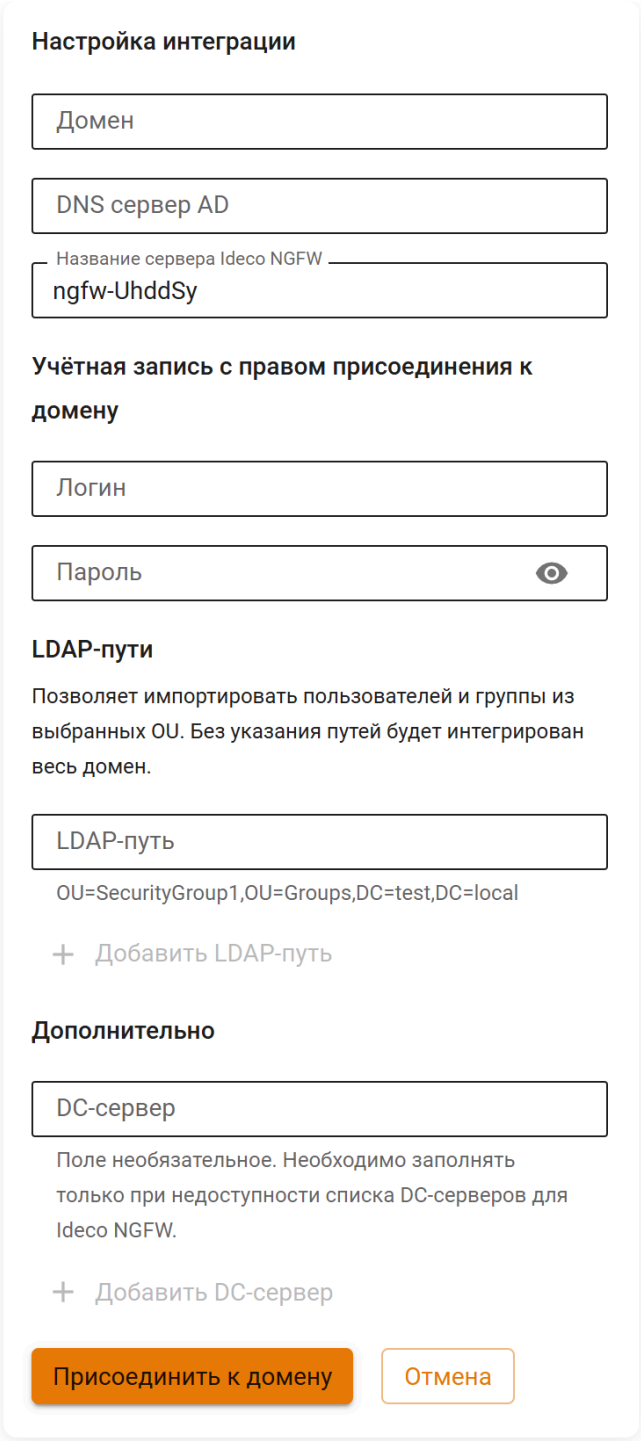
Перед вводом в домен:

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

Выполните действия:

1. Перейдите на вкладку **Пользователи** → **Active Directory/Samba DC**.

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



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

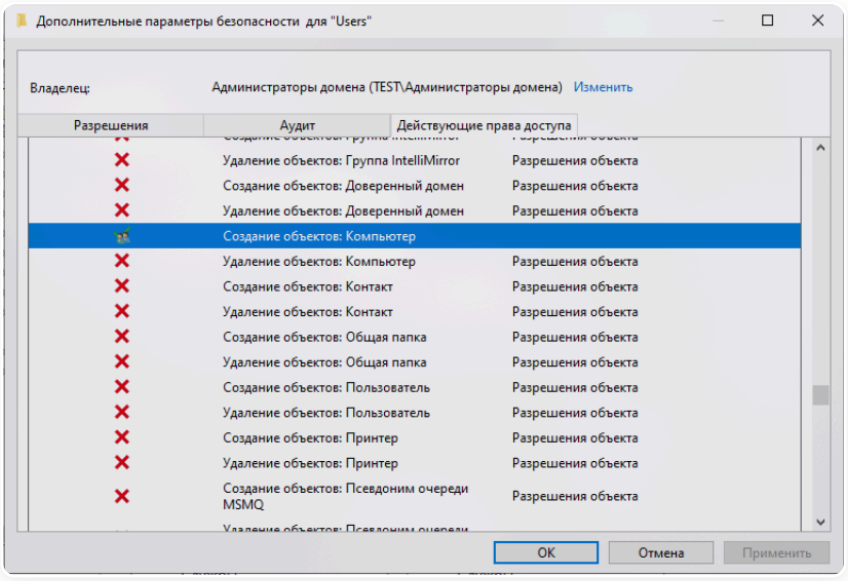
- **SSO через AD и ALD Pro** с токенами NTLM.
- VPN (IKEv2, SSTP, L2TP/IPsec, PPTP).
- Ideco Client с аутентификаций по логину и паролю.

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, длина которого не должна превышать 64 символа. Например: `mydomain.example`.
- **DNS-сервер AD** - адрес сервера, обладающий ролью DNS-сервера в контроллере домена, доступный с локального интерфейса Ideco NGFW.
- **Название сервера Ideco NGFW** - имя компьютера, под которым Ideco NGFW 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. 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**.

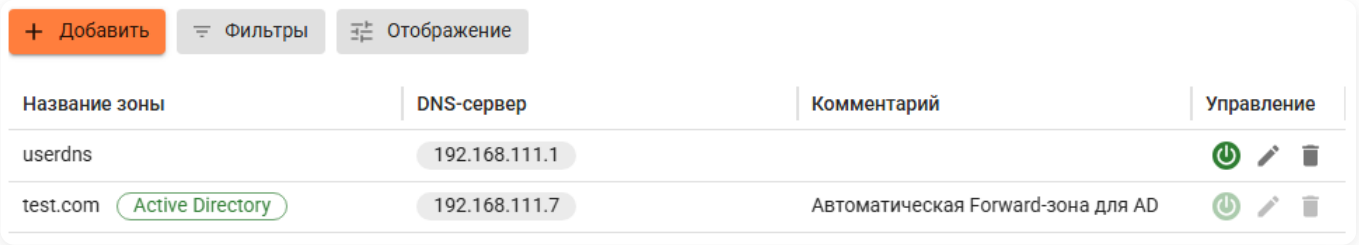
- **LDAP-пути** - LDAP-пути для импорта пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет импортировать только нужные группы пользователей, чтобы избежать импорта всего дерева пользователей AD.
- **DC-сервер** - контроллер домена. Заполняется только при недоступности контроллера домена для Ideco NGFW.

3. Нажмите **Присоединить к домену**. Процесс присоединения к домену может занять до одной минуты.

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

Настройка DNS для разрешения имен локального домена

В Ideco NGFW Forward-зона DNS создается в **Сервисы** → **Защита и управление DNS** → **Forward-зоны** автоматически при вводе сервера в домен:



При такой настройке компьютеры могут использовать Ideco NGFW 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 из домена перейдите в **Пользователи** → **Active Directory/Samba DC** и нажмите напротив интеграции. После подтверждения:

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

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

Полезные ссылки

Импорт пользователей

Аутентификация пользователей AD/Samba DC

Импорт пользователей

Ideco NGFW также поддерживает интеграцию с AD-администраторами. Подробные инструкции по настройке описаны в статье Администраторы.

Импортировать группы пользователей контроллера домена можно в специально созданные группы пользователей в Ideco NGFW. Их название может быть произвольным.

Особенности импорта пользователей в Ideco NGFW

- После импорта пользователи будут автоматически синхронизироваться с контроллером домена каждые 15 минут.
- Можно импортировать разные группы пользователей контроллера домена в различные группы Ideco NGFW. Это позволит удобно назначать правила фильтрации для каждого модуля фильтрации.
- Пользователи контроллера домена могут быть импортированы только в одну группу Ideco NGFW. При этом пользователь будет добавлен в группу, в которую был импортирован последним.
- В процессе импорта пользователей также импортируются номера телефонов, которые можно использовать для двухфакторной аутентификации.

Перед импортом пользователей убедитесь, что:

- Учетные записи AD не имеют одинаковых логинов с локальными учетными записями. В противном случае система выдаст сообщение об ошибке.
- Права устройств пользователей не ограничены на чтение.

Импорт учетных записей из LDAP-каталога

В Ideco NGFW можно импортировать учетные записи из LDAP-каталога. Для этого используются протоколы LDAP и LDAPS. При этом последний не требует дополнительных настроек на стороне NGFW и используется автоматически в случае использования его на контроллере домена.

Для импорта пользователей выполните действия:

1. Создайте группу в дереве пользователей Ideco NGFW. Подробнее о создании групп - в статье **Управление пользователями**.

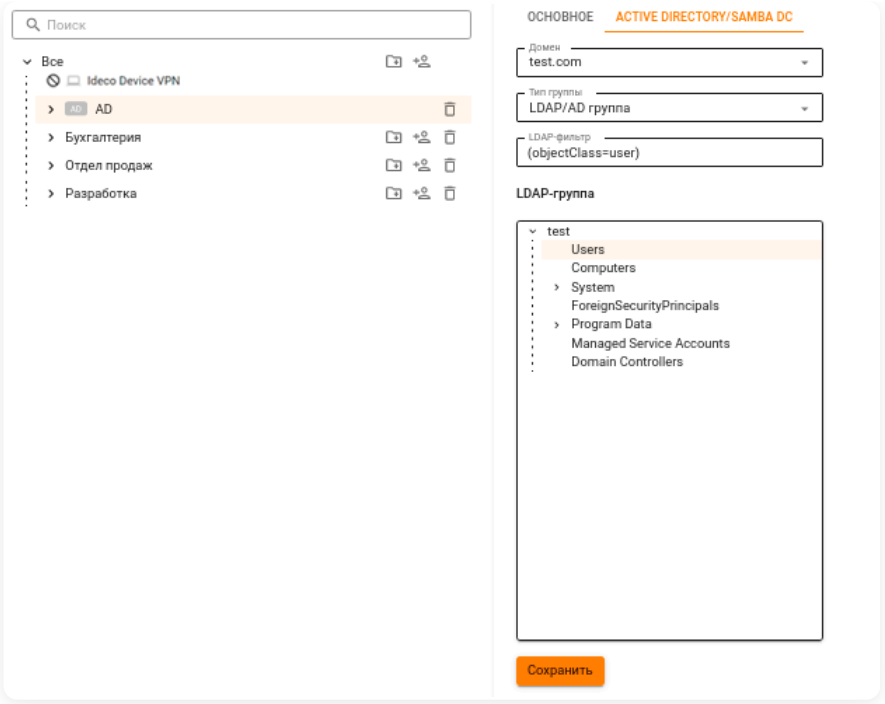
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC** в правой части экрана.

3. Выберите домен, из которого требуется импортировать пользователей.

4. В поле **Тип группы** выберите LDAP/AD группа.

5. При нажатии на поле **LDAP группа** будет отображен либо весь домен, либо группы, которые были указаны при вводе NGFW в домен. Выберите из него необходимую группу для импорта (можно выбрать корневую группу для импорта всего дерева).

6. Нажмите **Сохранить** (будет произведен импорт пользователей):



При необходимости воспользуйтесь фильтром запросов. Например, если в одних и тех же контейнерах находятся пользователи и компьютеры, а импортировать нужно только пользователей, то в поле **LDAP-фильтр** напишите: `(&(objectCategory=person)(objectClass=user))`

> Не стоит импортировать подгруппы уже импортированной группы, потому что они автоматически будут импортированы вместе с основной группой.

Импорт учетных записей из групп безопасности

1. Создайте группу в дереве пользователей Ideco NGFW.

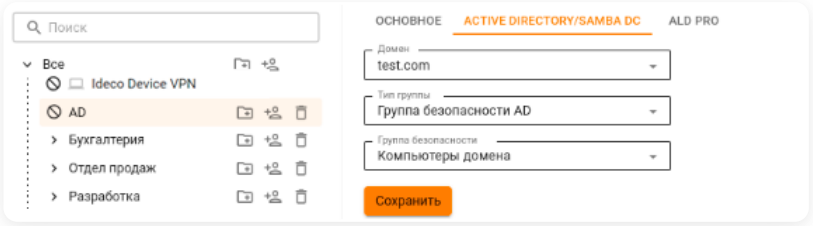
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC**.

3. В поле **Имя домена** выберите нужный домен.

4. В поле **Тип группы** выберите **Группа безопасности AD**.

5. В поле ниже из раскрывающегося списка выберите нужную группу безопасности.

6. Нажмите на кнопку **Сохранить**.



Если импортировались не все пользователи

Если импортировались не все пользователи, то включите режим совместимости. **Важно**: включенный режим совместимости импортирует пользователей медленнее.

Примеры включения через терминал и браузер:

Терминал

1. Авторизуйтесь командой:

```
curl -c /tmp/cookie -b /tmp/cookie -X POST https://адрес_сервера/web/auth/login -d '{"login": "логин", "password": "пароль",
```

2. Отправьте запрос на включение режима:

```
curl -c /tmp/cookie -b /tmp/cookie -X PATCH https://адрес_сервера/ad_backend/security_group_import_settings -d '{"compatibili
```

Браузер

1. Откройте веб-интерфейс Ideco NGFW и нажмите F12.

2. Перейдите на вкладку **Сеть** и нажмите на любой запрос.

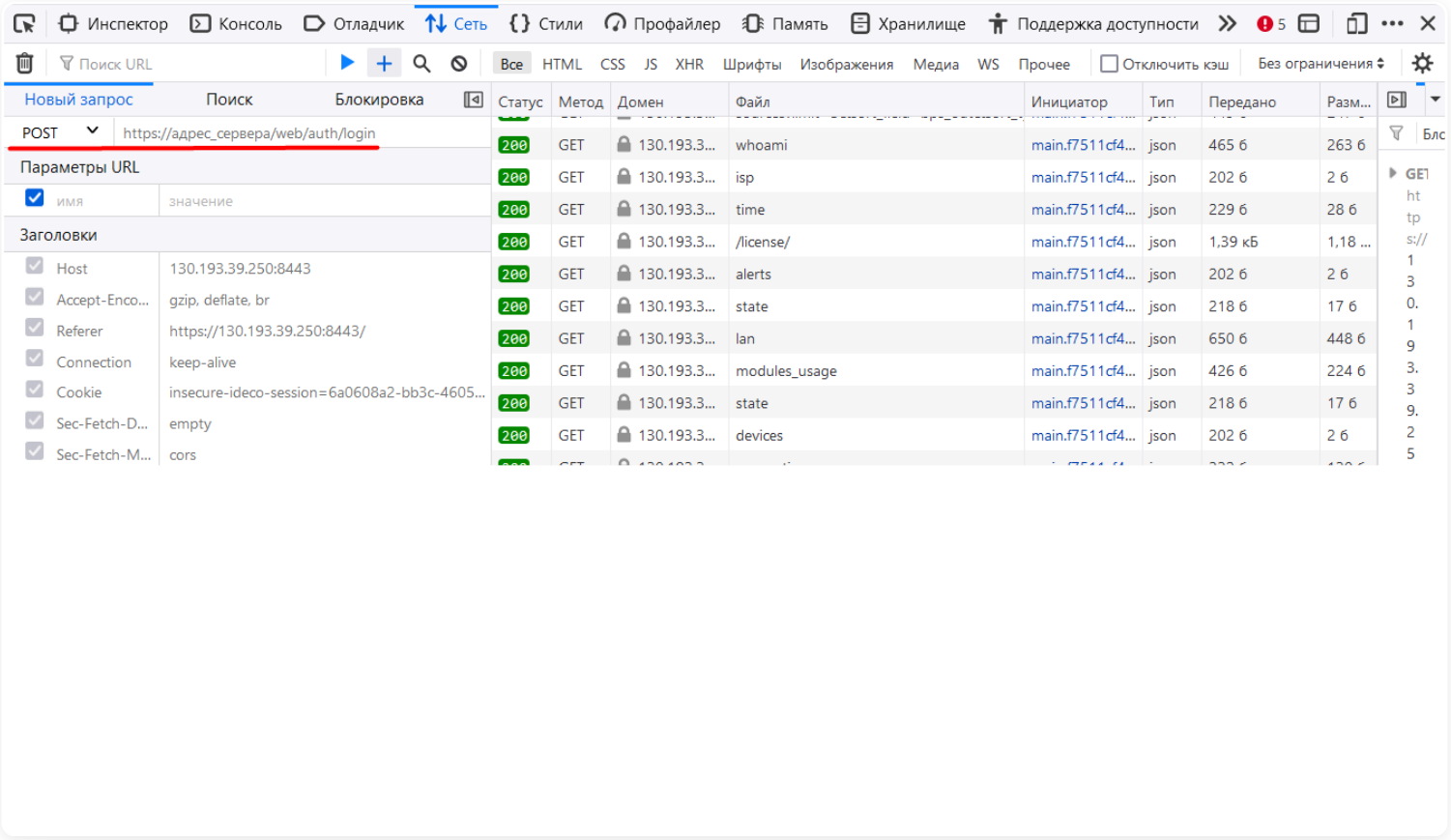
3. В появившемся окне перейдите на вкладку **Новый запрос**.

4. Отправьте запрос авторизации:

```
POST https://адрес_сервера/web/auth/login
```

Тело запроса:

```
{
    "login": "логин", "password": "пароль", "rest_path": "/"
}
```

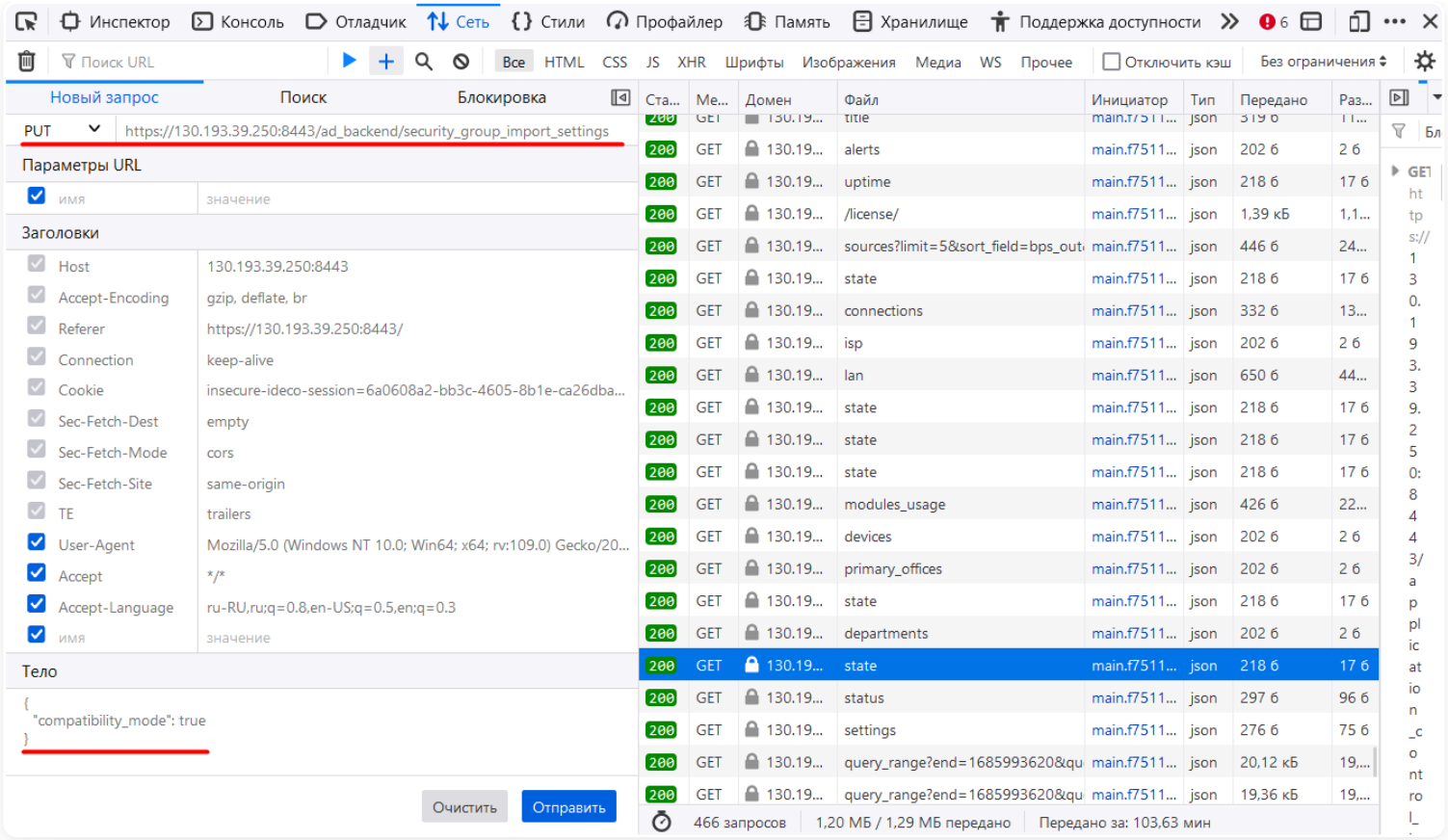


5. Отправьте запрос на включение режима:

```
PATCH /ad_backend/security_group_import_settings
```

Тело запроса:

```
{
  "compatibility_mode": true
}
```



Для выключения режима совместимости в теле запроса вместо `true` укажите `false`.

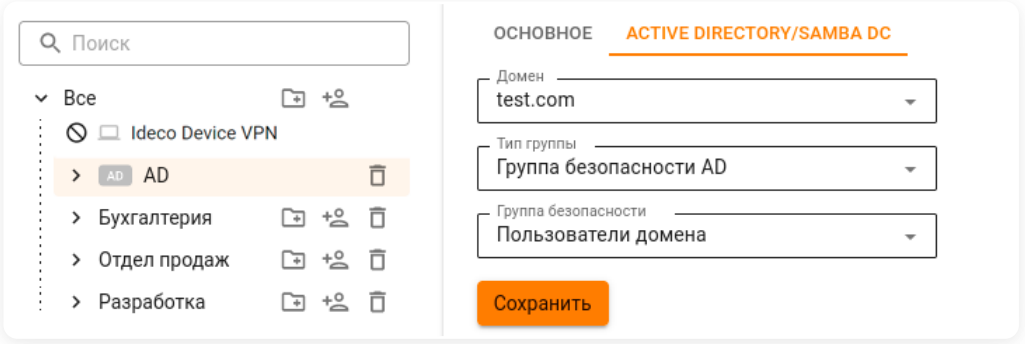
Настройка учетных записей и групп безопасности в качестве объектов фильтрации

Импортированные из AD/Samba группы безопасности и учетные записи можно использовать в качестве объектов фильтрации в разделах:

- Файрвол
- Контент-фильтр
- Ограничение скорости

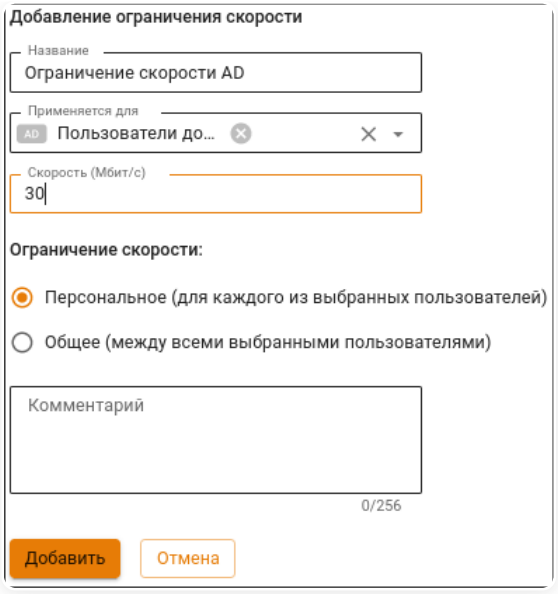
Пример использования учетной записи, импортированной из Active Directory, для ограничения скорости

1. Импортируйте из AD учетные записи или группы безопасности в разделе **Пользователи** → **Учетные записи** (подробнее в статье Импорт пользователей). В этом примере импортируется группа безопасности AD **Пользователи домена**:



2. Перейдите в раздел, в котором требуется использовать импортированную из AD группу или учетную запись. Например, в **Ограничение скорости**.

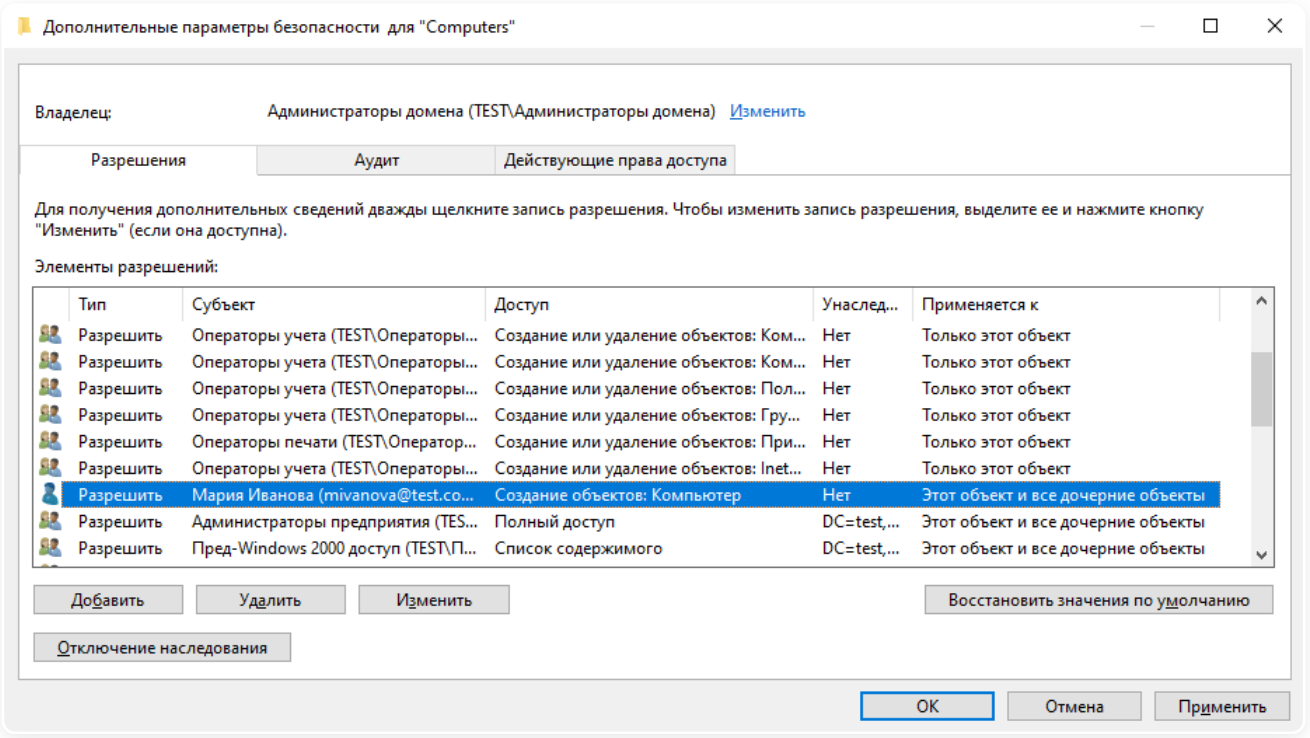
3. Заполните поля и нажмите **Добавить**:



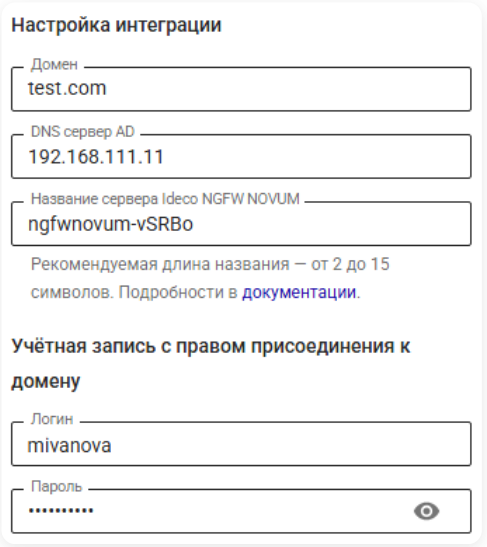
- **Название** - введите название правила, например, Ограничение для менеджеров.
- **Применяются для** - выберите из выпадающего списка отдельного пользователя и/или группу.
- **Скорость** (Мбит/с) - лимит скорости для выбранных пользователей.

Настройка прав для интеграции Active Directory

Для интеграции Ideco NGFW 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 в **Пользователи** → **Active Directory/Samba DC**:



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

Область применения	Необходимые права и атрибуты

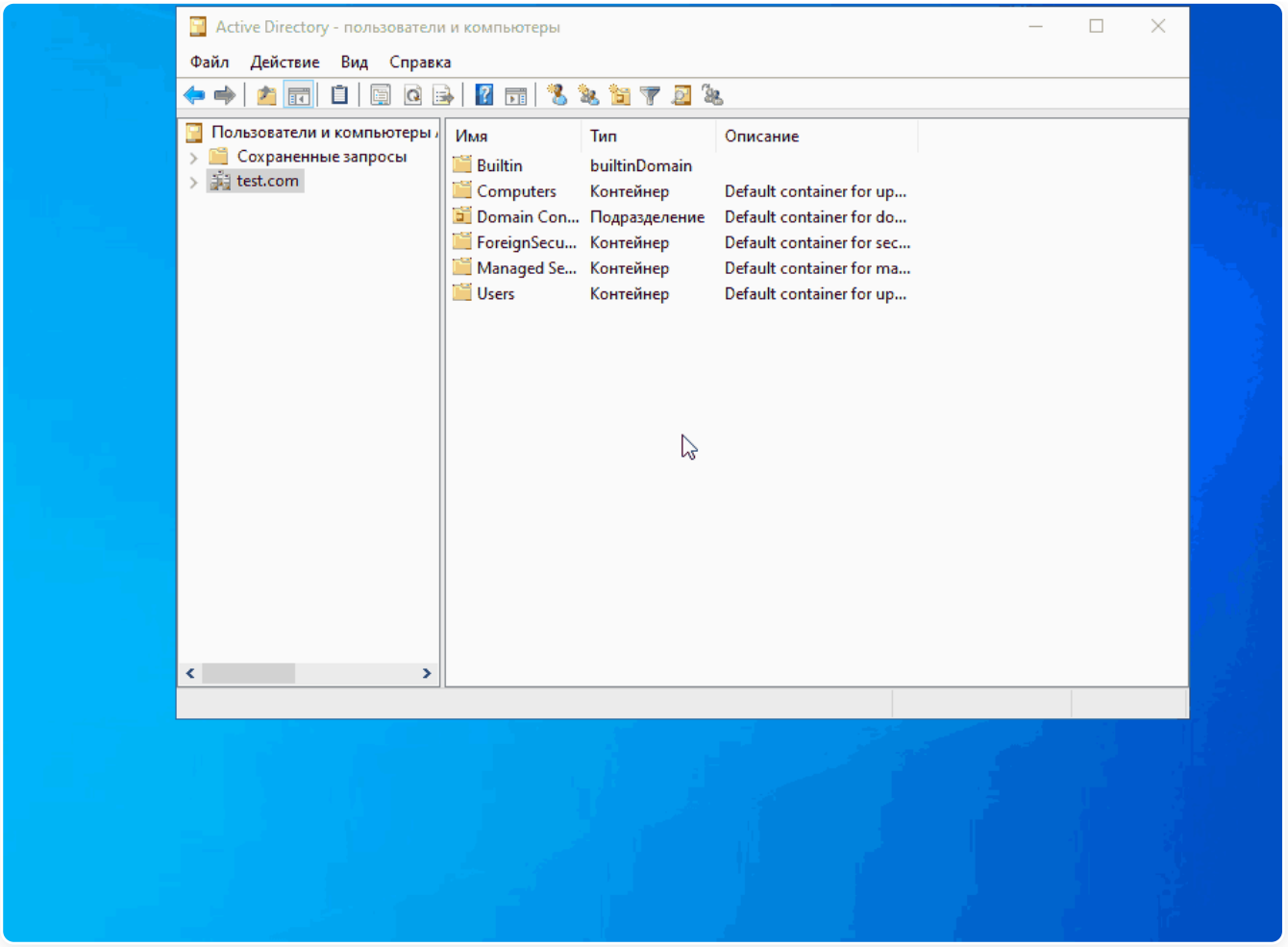
Поиск пользователей	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ name
	  ◦ modifyTimeStamp
	  ◦ objectGUID
	  ◦ objectSid
	  ◦ cn
	  ◦ displayName
	  ◦ login
	  ◦ mobile
	  ◦ objectClass
	  ◦ userAccountControl
	  ◦ sAMAccountName
	  ◦ userPrincipalName
	  ◦ accountExpires
	  ◦ msDS-UserPasswordExpiryTimeComputed
	  ◦ 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**).

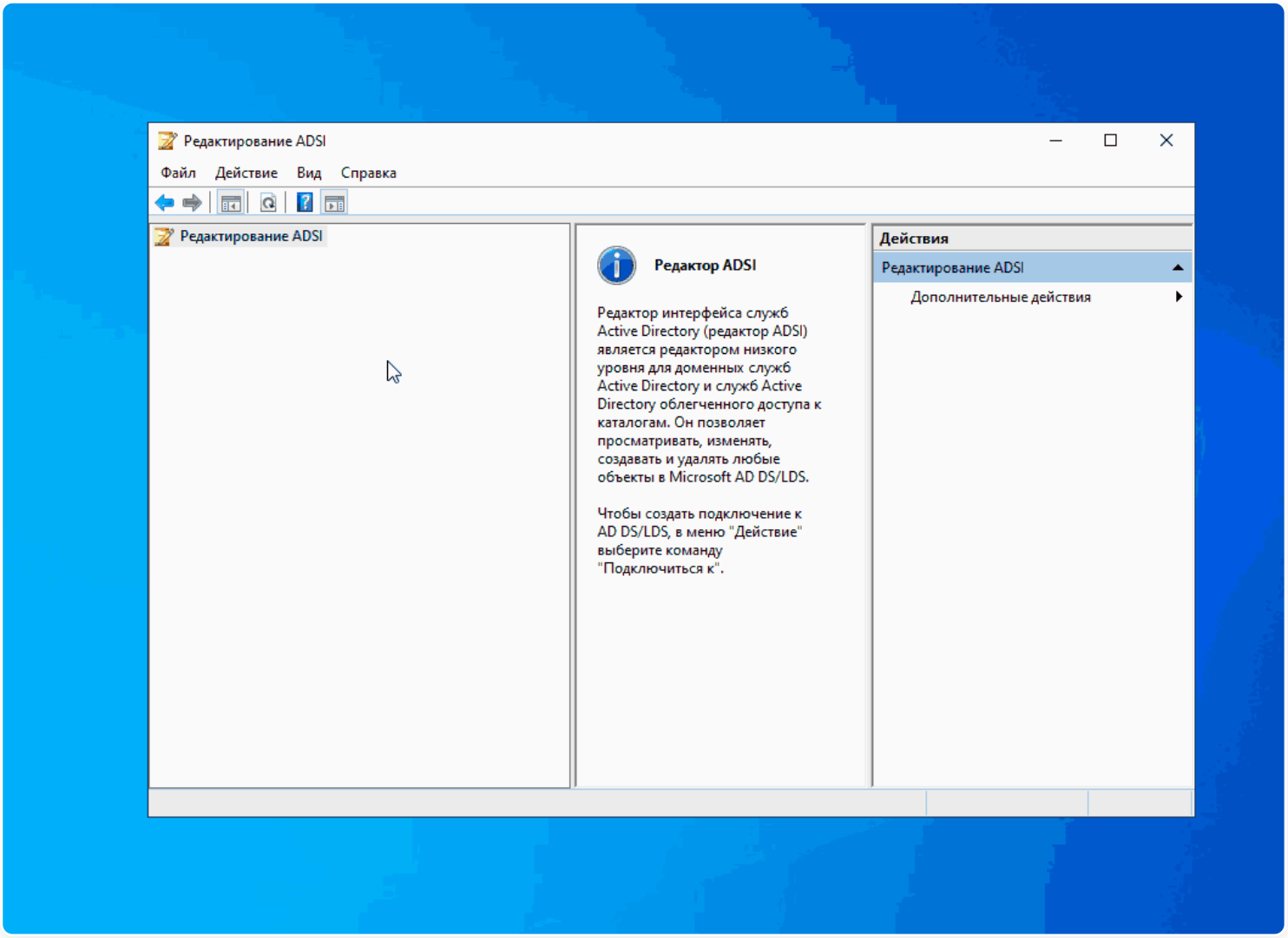
2. Нажмите правой кнопкой на объекте домена, выберите **Properties** → **Security** → **Advanced** (**Свойства** → **Безопасность** → **Дополнительно**).

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 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 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 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

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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

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

Ideco NGFW использует имя входа пользователей AD с атрибутом `sAMAccountName` (SAM). Если на AD используется атрибут `userPrincipalName` (UPN), необходимо, чтобы атрибуты SAM и UPN были идентичны. Различия в SAM и UPN приведут к проблемам с аутентификацией пользователей на NGFW.

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 пользователей терминальных серверов (с использованием Remote Desktop IP Virtualization на терминальном сервере).
- **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.

Особенности авторизации пользователей доверенных доменов

Если у домена, в который введен NGFW, настроено доверие с другим доменом, то пользователи доверенного домена смогут авторизоваться на NGFW 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

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

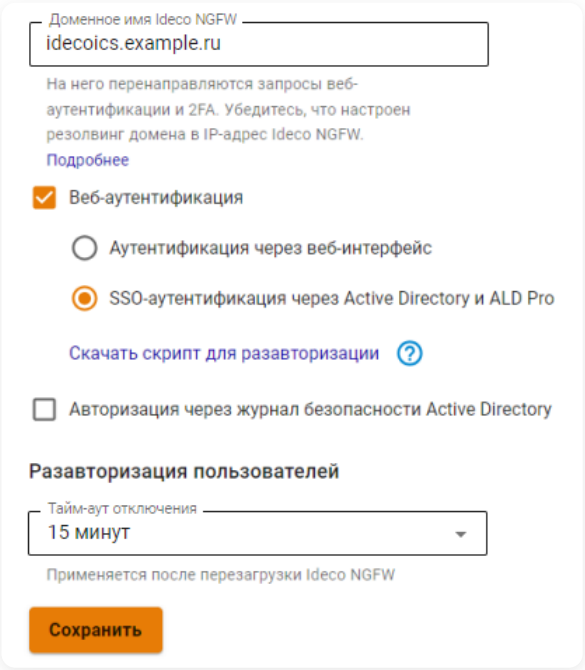
Настройка SSO-аутентификации

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

Список служб для других разделов доступен по ссылке.

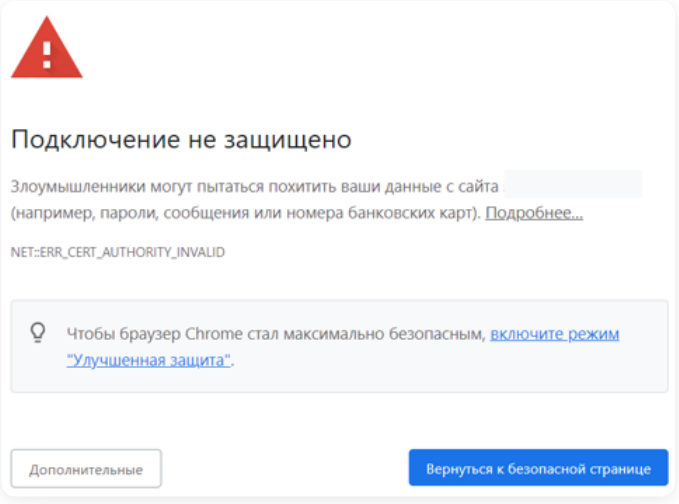
Настройка SSO-аутентификации на стороне NGFW

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



- **Доменное имя Ideco NGFW** - укажите доменное имя Ideco NGFW.
- **Веб-аутентификация** - включите настройку и выберите **SSO-аутентификация через Active Directory и ALD Pro** для авторизации с использованием токенов Kerberos или NTLM.
- **Авторизация через журнал безопасности Active Directory** - включите, если требуется, чтобы Ideco NGFW отслеживал события успешного входа в журнале безопасности AD и авторизовывал пользователя по ним, если трафик идет с того же IP-адреса.
- **Тайм-аут отключения** - установите тайм-аут разавторизации 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.

Для работы аутентификации через веб-браузер с использованием Kerberos или NTLM настройте Internet Explorer (остальные браузеры получат его настройки).

Настройка на стороне сервера Active Directory

Настройка аутентификации через веб-браузер

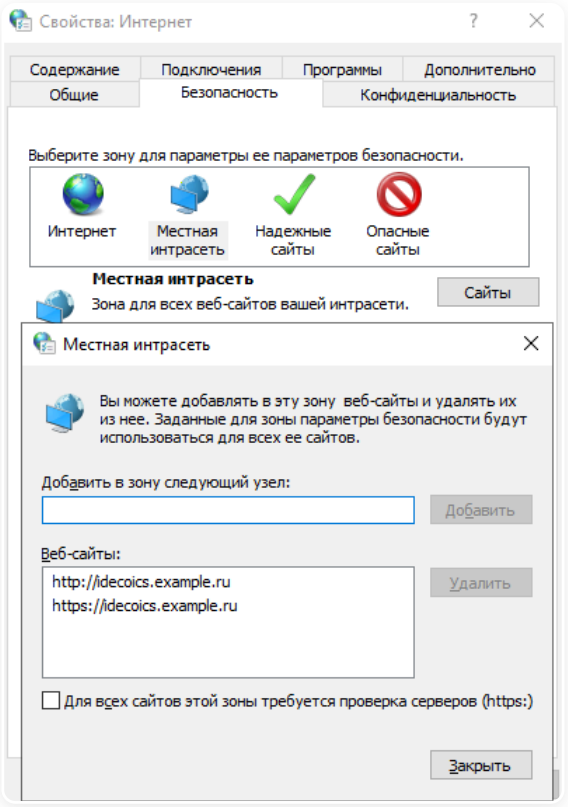
1. В поиск введите **Изменение параметров временных файлов Интернета**.

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

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

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

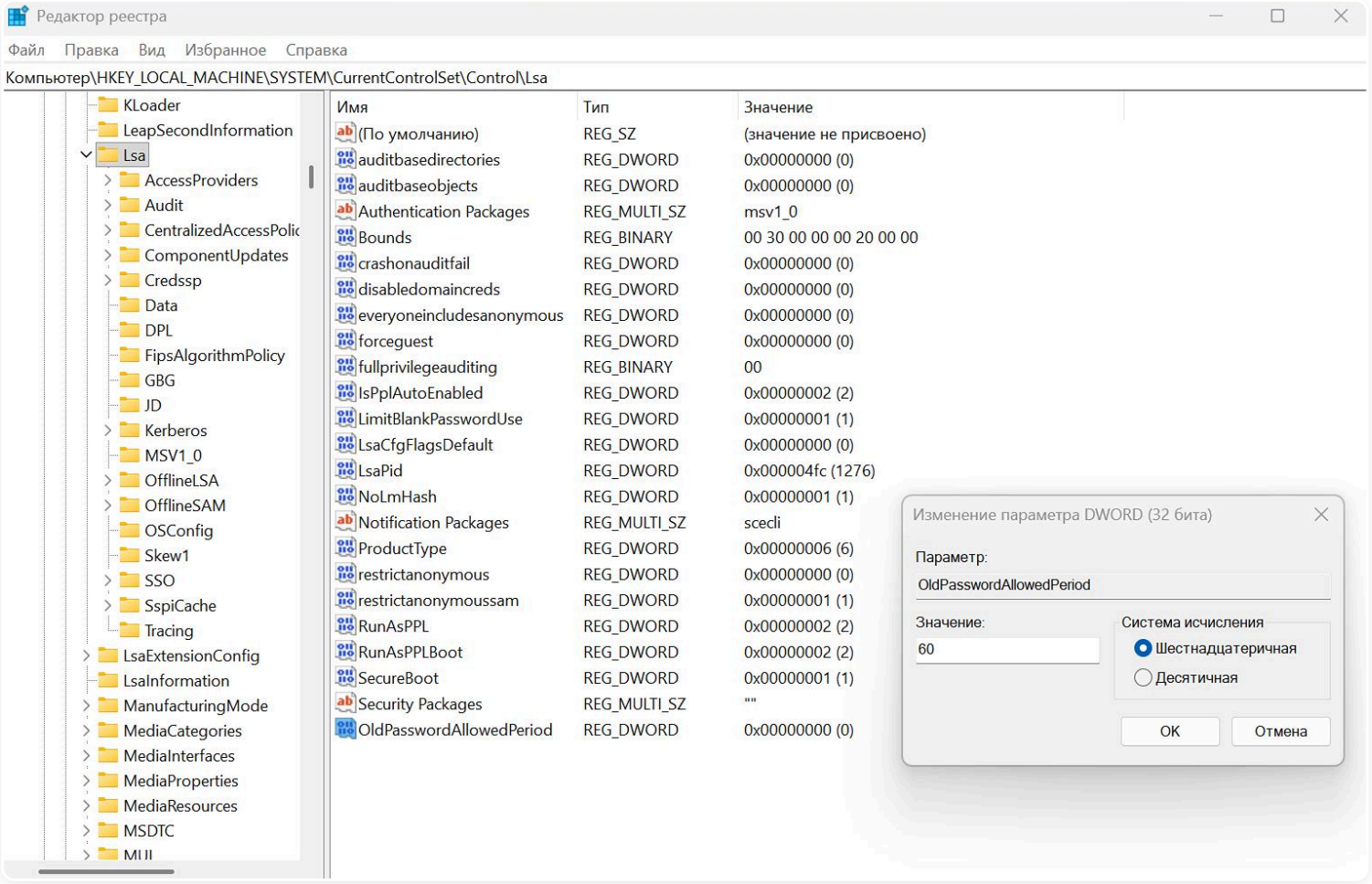
Пример ввода Ideco NGFW в домен `example.ru` под именем `idecoics`:



Особенности использования NTLM токенов

При использовании NTLM токенов для веб-аутентификации, а так же 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:



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.

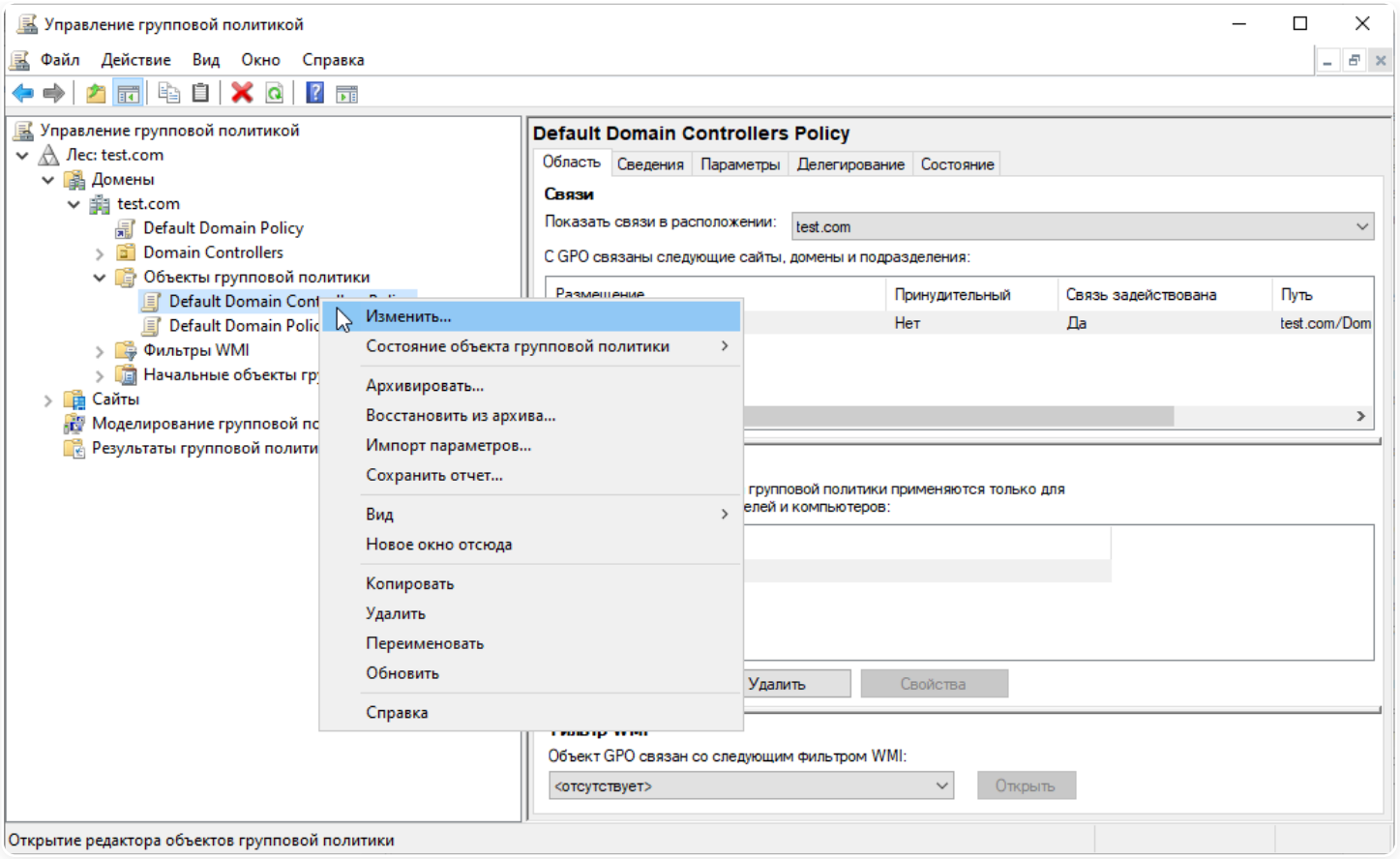
2. Перейдите по пути:

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:

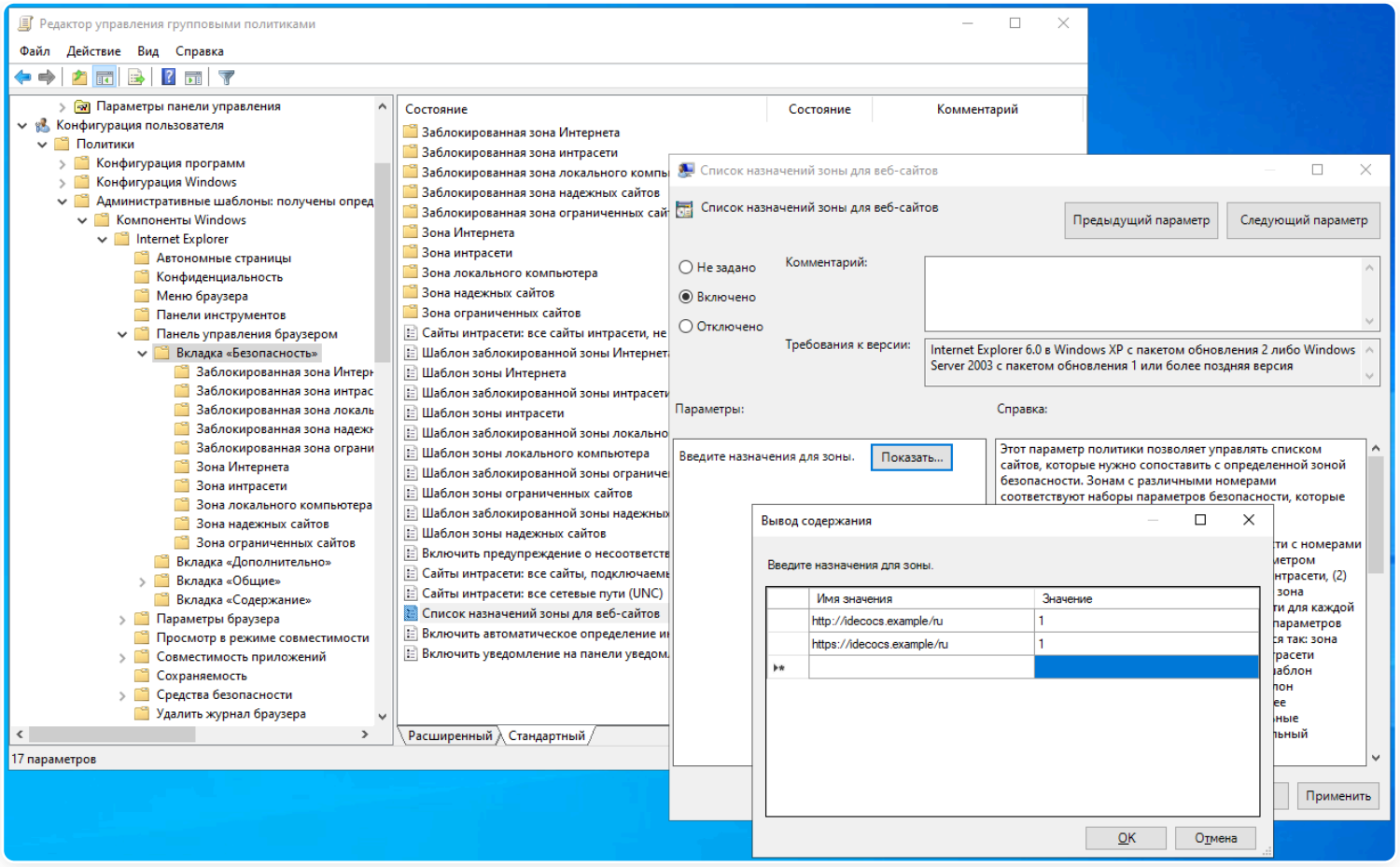
Англоязычная версия

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.

3. Введите назначение зоны для DNS-имени Ideco NGFW (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. Чтобы не делать это каждый раз, можно добавить корневой сертификат Ideco NGFW в доверенные корневые сертификаты устройства.

Настройка браузера Mozilla Firefox для веб-аутентификации по SSO или NTLM

Для использования браузера **Mozilla Firefox** на странице настроек (введите *about:config* в адресной строке) укажите следующие параметры:

- **network.automatic-ntlm-auth.trusted-uris** и **network.negotiate-auth.trusted-uris** добавьте адрес локального интерфейса Ideco NGFW (например, `idecoUTM.example.ru`).
- **security.enterprise_roots.enabled** в значении `true` позволит Firefox доверять системным сертификатам и авторизовать пользователей при переходе на HTTPS-сайты.

Настройка браузера Chromium для веб-аутентификации по SSO или NTLM

1. Откройте **Редактор реестра**.

2. Перейдите по пути `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Chromium` (для компьютера) или `HKEY_CURRENT_USER\SOFTWARE\Policies\Chromium` (для конкретного пользователя).

3. Создайте два новых ключа:

- Первый ключ должен иметь тип `REG_SZ`, имя `AuthServerAllowlist` и значение `*.имя_домена`.
- Второй ключ также должен иметь тип `REG_SZ`, имя `AuthNegotiateDelegateAllowlist` и значение `*.имя_домена`.

Настройка браузера Яндекс для веб-аутентификации по SSO или NTLM

1. Откройте **Редактор реестра**.

2. Перейдите по пути `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\YandexBrowser` (для компьютера) или `HKEY_CURRENT_USER\SOFTWARE\Policies\YandexBrowser` (для конкретного пользователя).

3. Создайте два новых ключа:

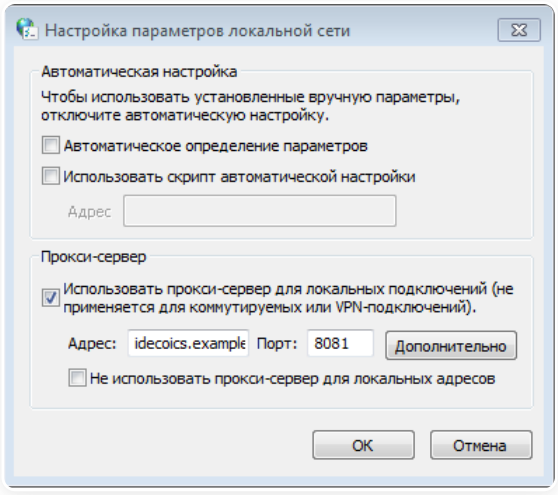
- Первый ключ должен иметь тип `REG_SZ`, имя `AuthServerAllowlist` и значение `*.имя_домена`.
- Второй ключ также должен иметь тип `REG_SZ`, имя `AuthNegotiateDelegateAllowlist` и значение `*.имя_домена`.

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**.

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



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:

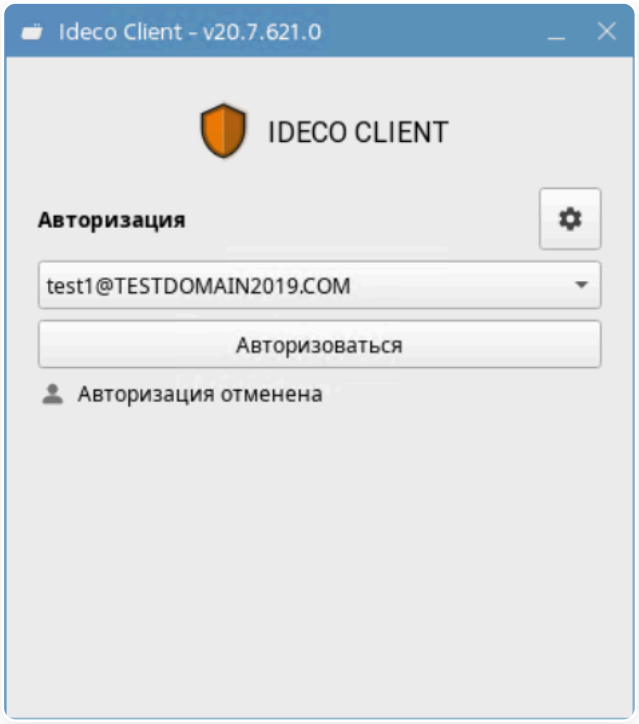
- **network.automatic-ntlm-auth.allow-proxies** = false.
- **network.negotiate-auth.allow-proxies** = false.

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 с Active Directory. Ideco Client пытается получить токен для авторизации на NGFW. Но NGFW 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 на контроллере домена не удалена и имеет необходимые права.

3. Проверьте, что настройки интеграции пользовательского компьютера с AD и NGFW 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` (подробнее в статье). Проверьте логи (например, с помощью `journalctl`, `KSystemLog` или `logcheck`) на ошибки получения SSO-токенов вида:

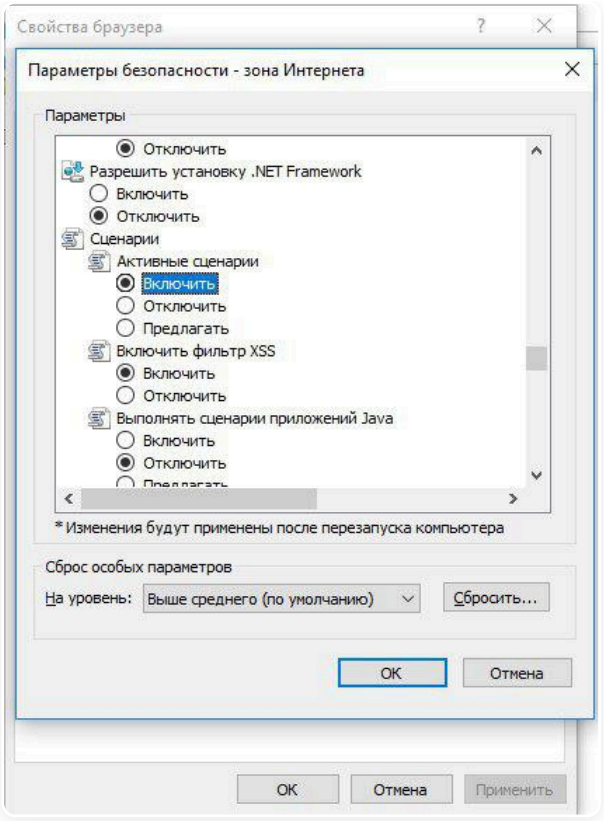
```
SSOGenToken завершился с ошибкой: 'genTokenInternal: <major error string> (<minor error string>)'
```

- `<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.

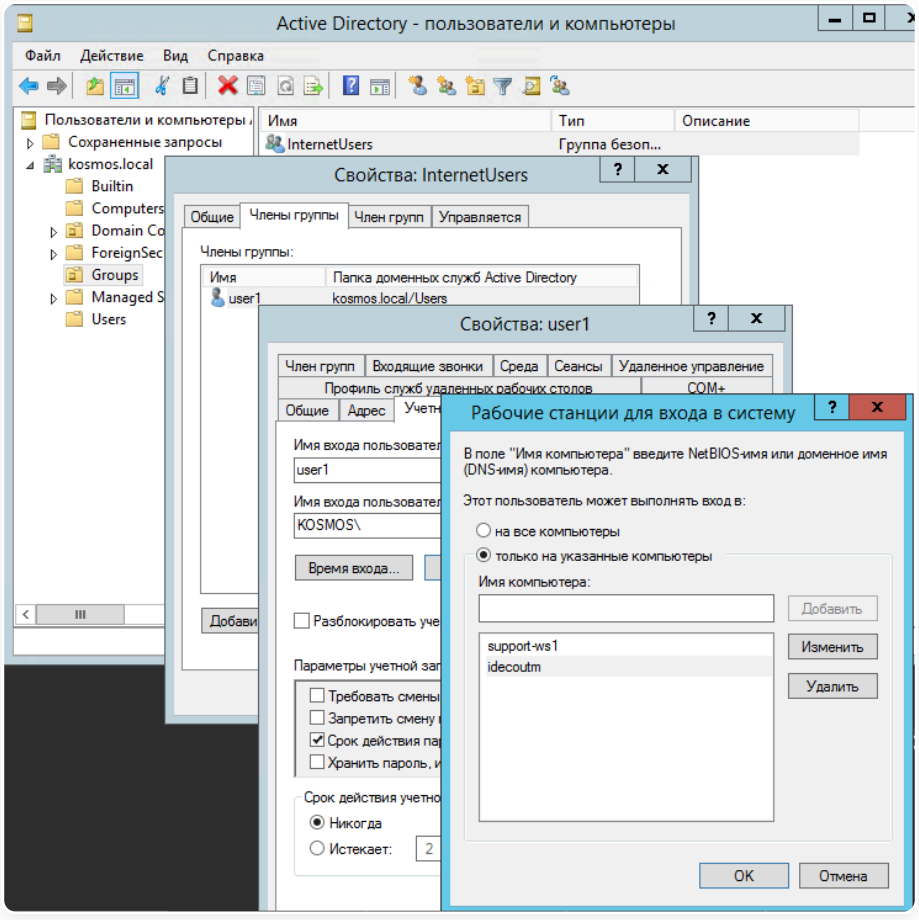
Для получения доступа требуется аутентификация

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. На контроллере домена зайдите в свойства выбранных пользователей на вкладку **Учетная запись → Вход на...**, выберите пункт **только на указанные компьютеры** и пропишите имя рабочей станции для входа в систему.

Пример такой настройки представлен на скриншоте ниже:



Полезные ссылки

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

Настройка авторизации через журнал безопасности

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

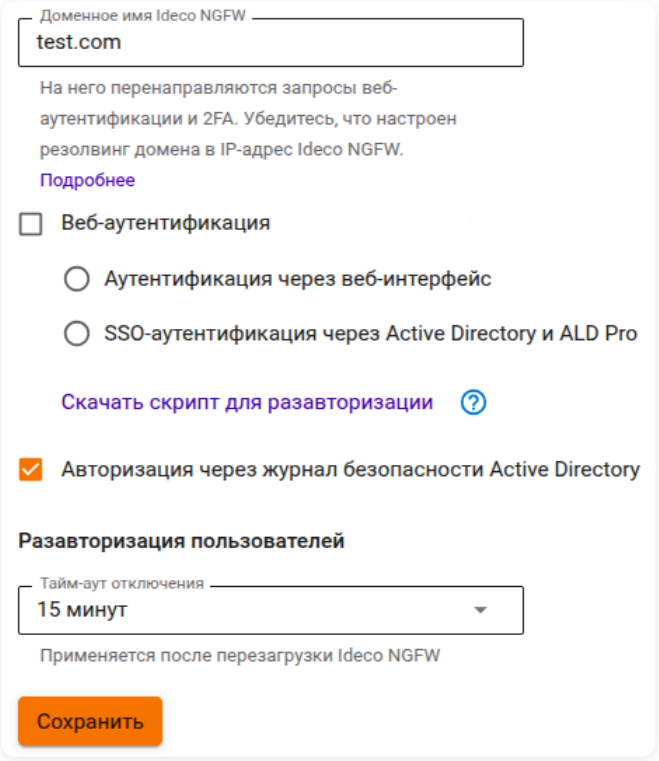
Авторизацию через журнал безопасности Active Directory рекомендуется использовать совместно с SSO-аутентификацией. Авторизация только через журнал безопасности может ограничить возможности управления и настройки прав доступа.

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

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

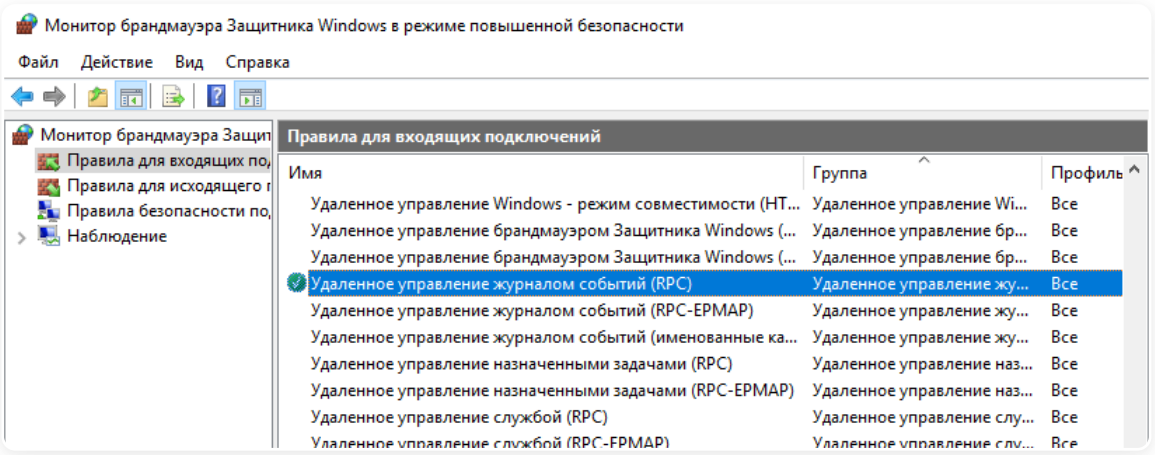


- **Доменное имя Ideco NGFW** - не требуется, если используется только авторизация через журнал безопасности AD.
- **Веб-аутентификация** - не требуется. Авторизация через журнал безопасности AD обеспечивает аутентификацию.
- **Авторизация через журнал безопасности Active Directory** - включите, чтобы Ideco NGFW 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.
- **Тайм-аут отключения** - установите тайм-аут разавторизации пользователей. Значение по умолчанию - 15 минут. Диапазон доступных значений - от 10 минут до 1 дня.

Настройка на стороне сервера Active Directory

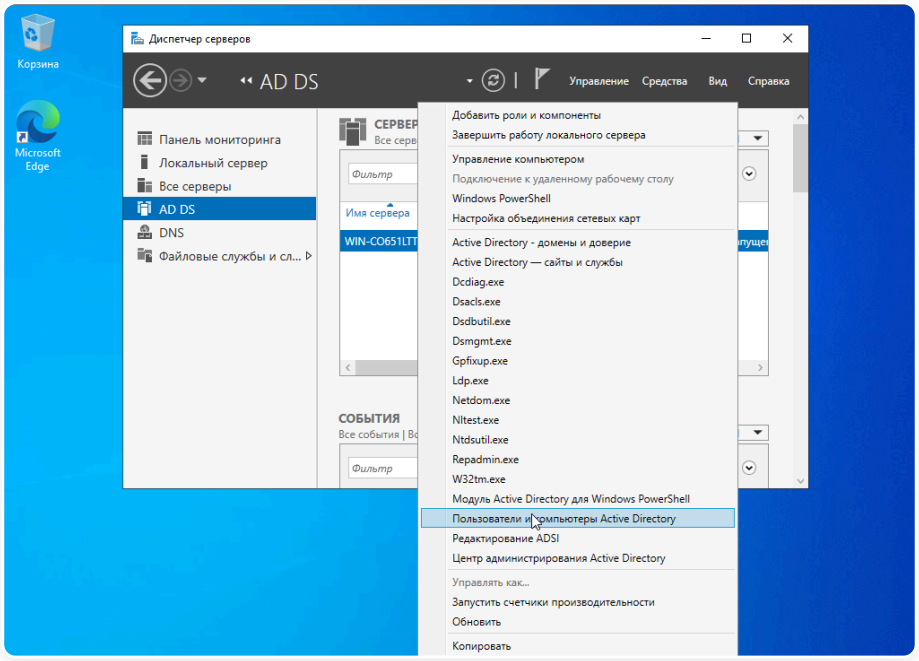
Перед настройкой убедитесь, что Ideco NGFW уже введен в домен.

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

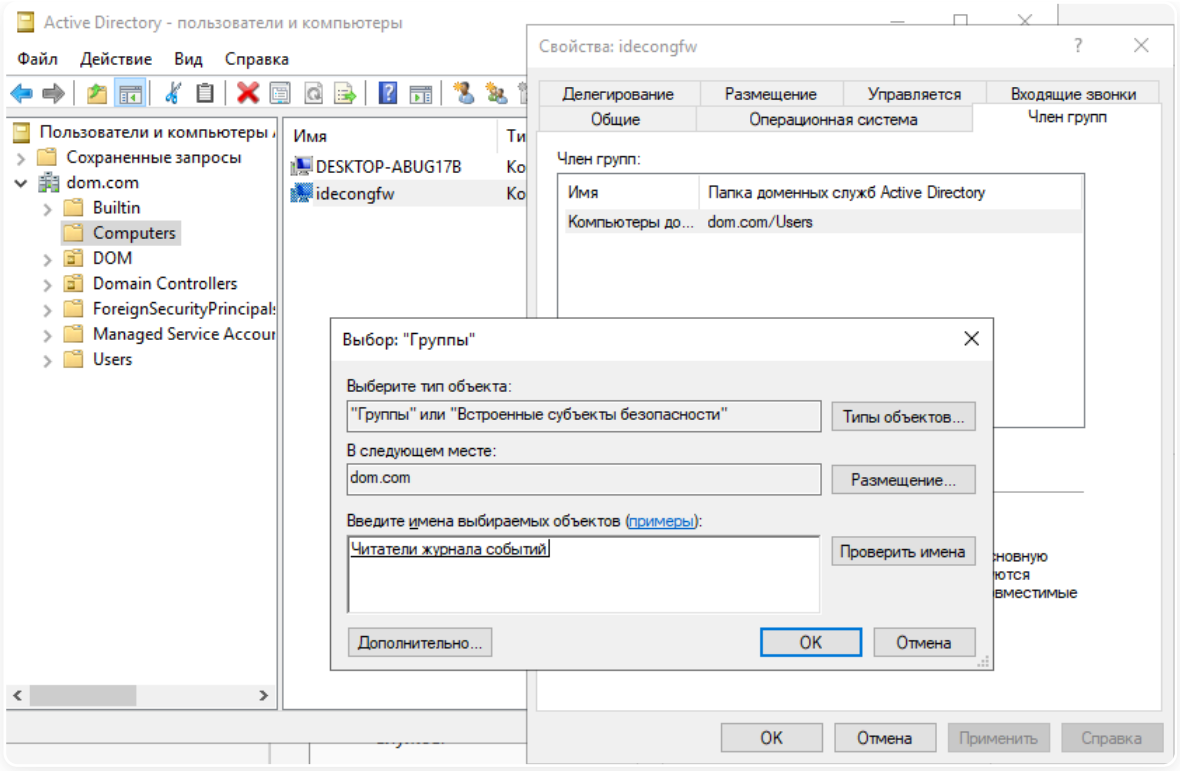


2. Добавьте Ideco NGFW в группу безопасности **Читатели журнала событий (Event Log Readers)**. Чтобы это сделать:

- 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 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. 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 **ОК**.

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 автоматической разавторизации

При переходе с более ранних версий на Ideco NGFW v17 изменился скрипт автоматической разавторизации. Чтобы избежать ошибок, скачайте и перенастройте скрипт в соответствии с инструкцией ниже.

Разавторизация пользователей возможна в полностью автоматическом режиме. Для этого настройте скрипт (logout), который будет запускаться при выходе пользователей из системы с помощью групповых политик домена (GPO).

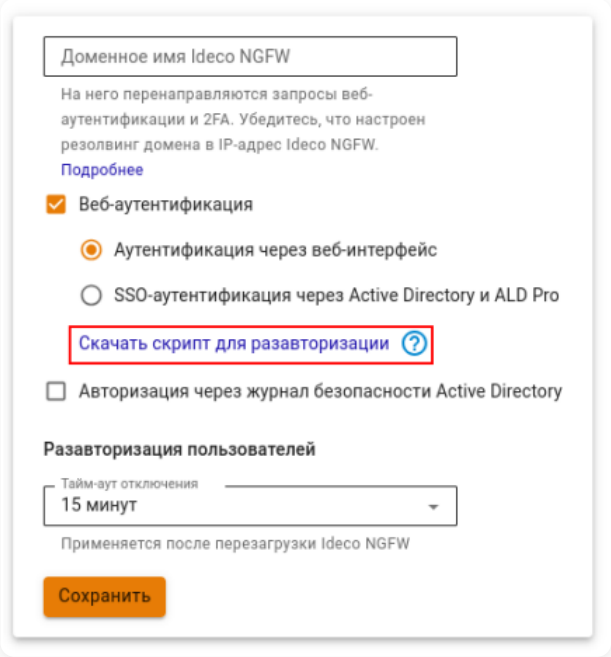
Для работы скрипта выполните все настройки политик безопасности домена и браузера, описанные в статье Авторизация пользователей.

Для авторизации по SSO используйте Ideco Client.

Разавторизация пользователя

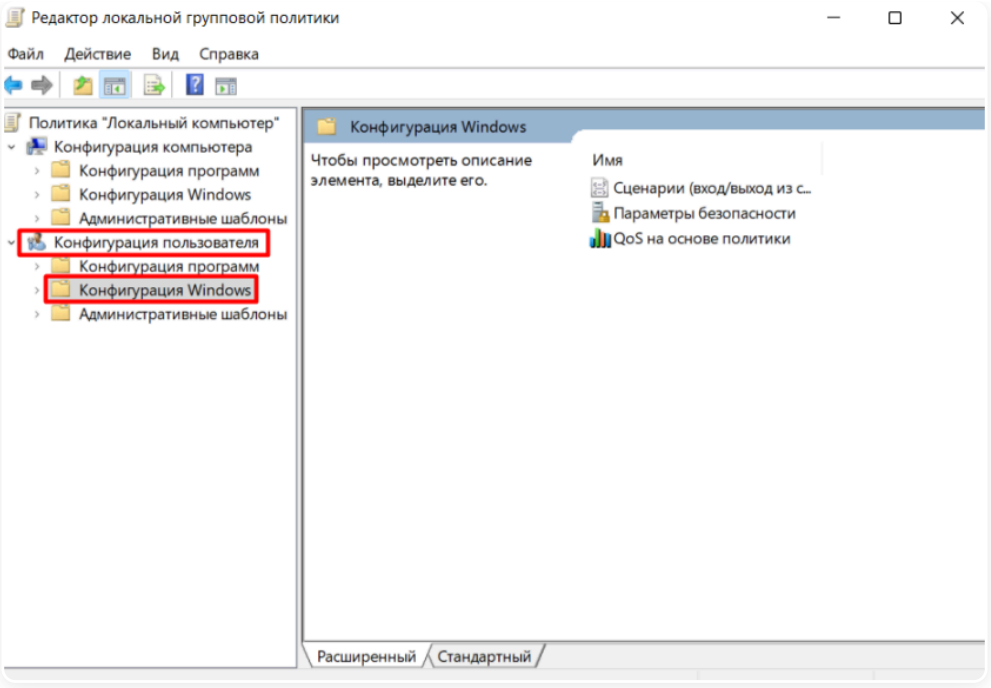
Чтобы скрипт разавторизации работал корректно, установите на компьютеры пользователей корневой сертификат сервера Ideco NGFW и сделайте его доверенным. Это можно сделать как локально, так и через групповые политики домена, следуя инструкции.

1. Чтобы скачать скрипт, перейдите в раздел **Пользователи** → **Авторизация** → **Основное**. Включите опцию **Веб-аутентификация**, после чего появится кнопка **Скачать скрипт для разавторизации**:



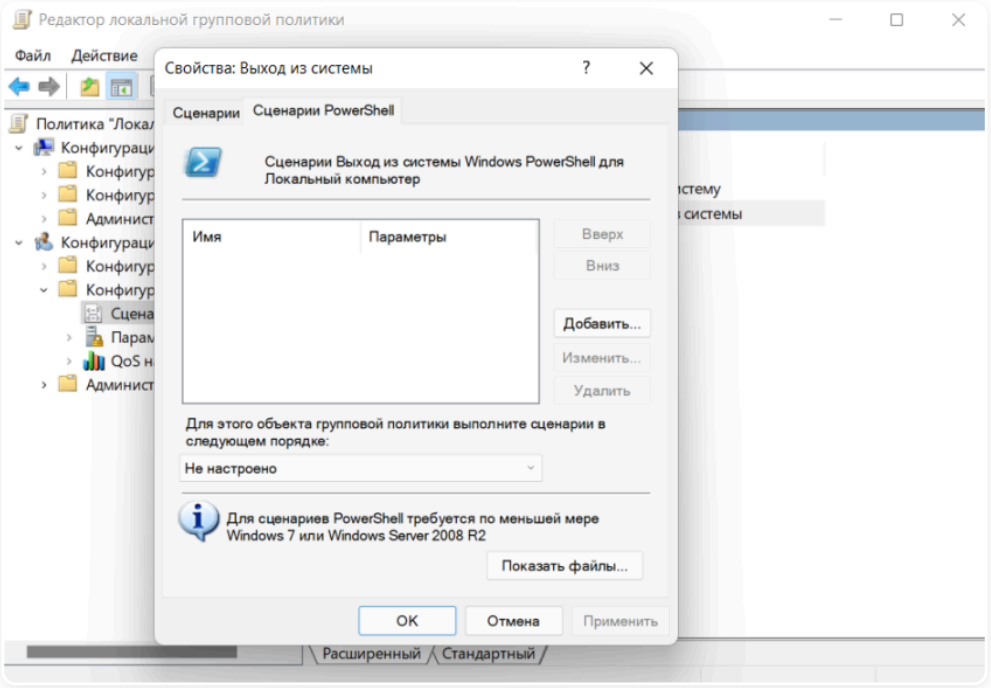
2. Откройте групповые политики (gpedit.msc) от имени администратора на устройстве пользователя.

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

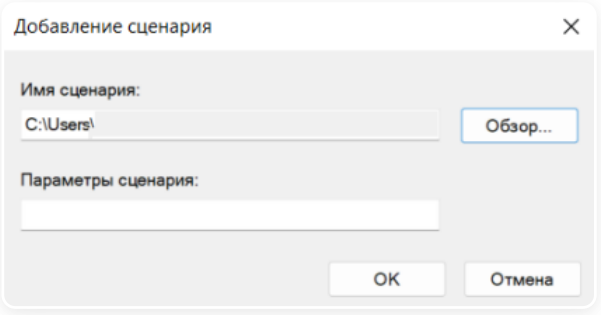


4. Нажмите **Сценарии (вход/выход из системы)**.

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



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

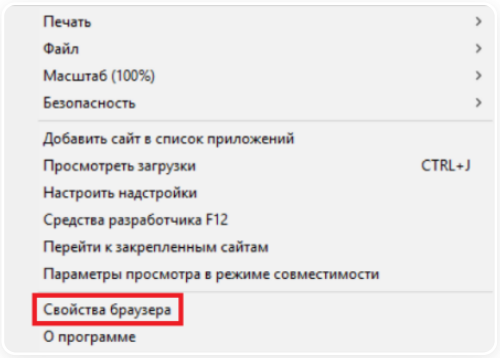


7. Откройте командную строку и обновите групповые политики, введя команду `gpupdate /force`.

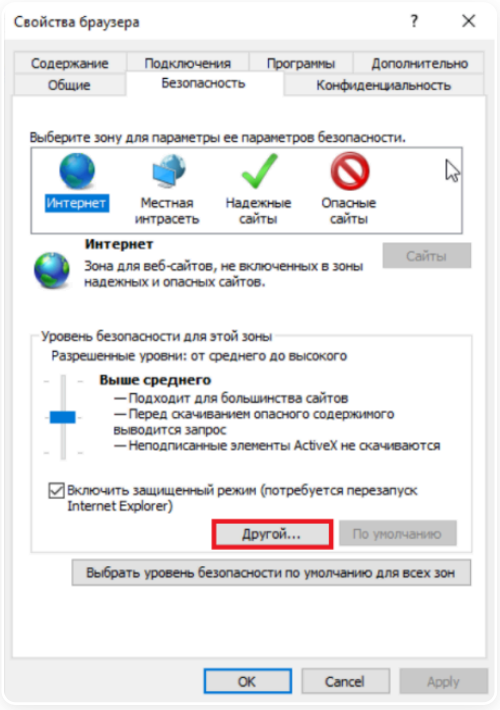
Если в вашем браузере появляется окно с текстом **Для получения доступа требуется аутентификация** и авторизация происходит только при ручном переходе по ссылке, включите JavaScript. Ниже представлены настройки для разных браузеров:

Internet Explorer

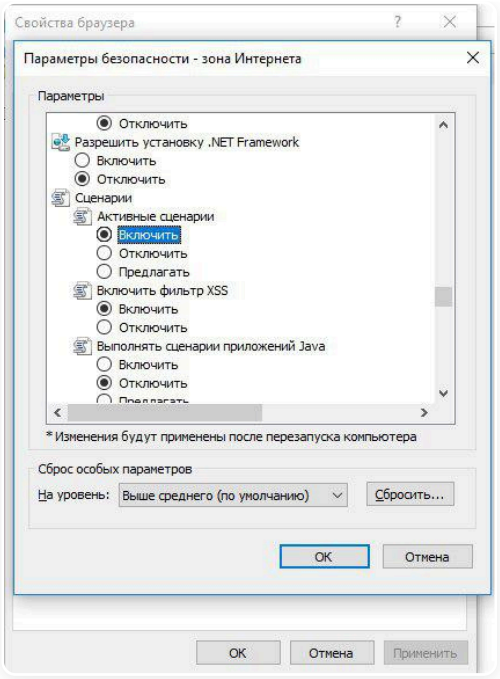
1. В правом верхнем углу браузера нажмите на кнопку **Сервис** в виде шестерни или комбинацию клавиш Alt+X. В выпадающем меню выберите **Свойства браузера**:



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

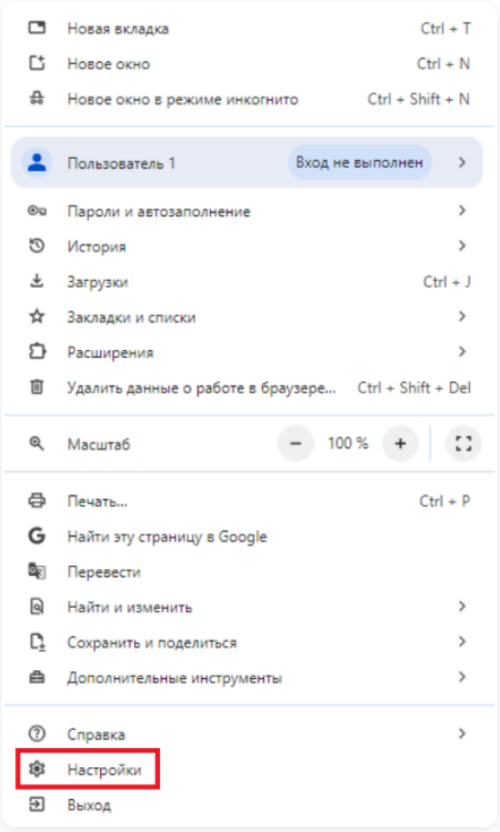


3. В окне **Параметры** переключите параметр **Активные сценарии** в значение **Включить**:

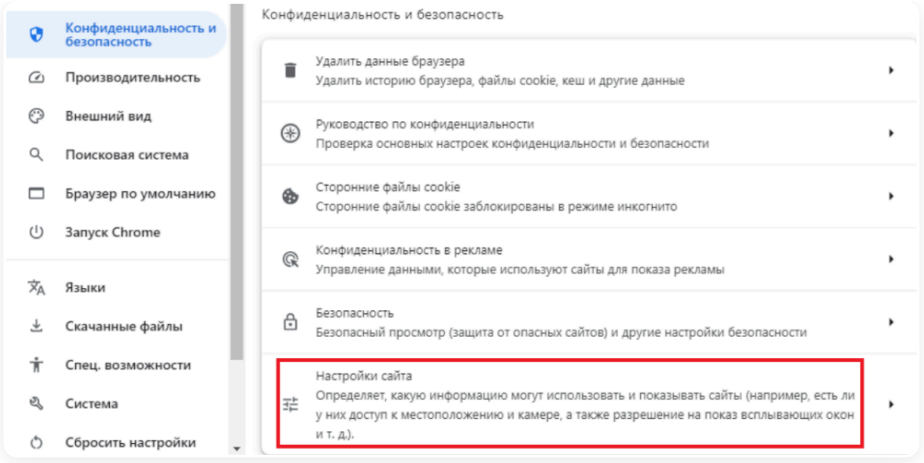


Google Chrome

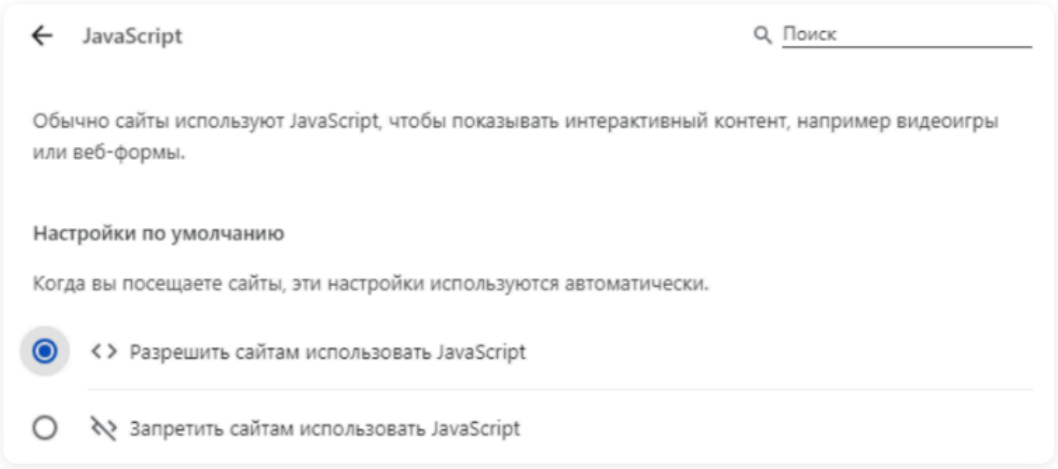
1. В правом верхнем углу браузера нажмите на кнопку с тремя точками и выберите **Настройки** в выпадающем меню:



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

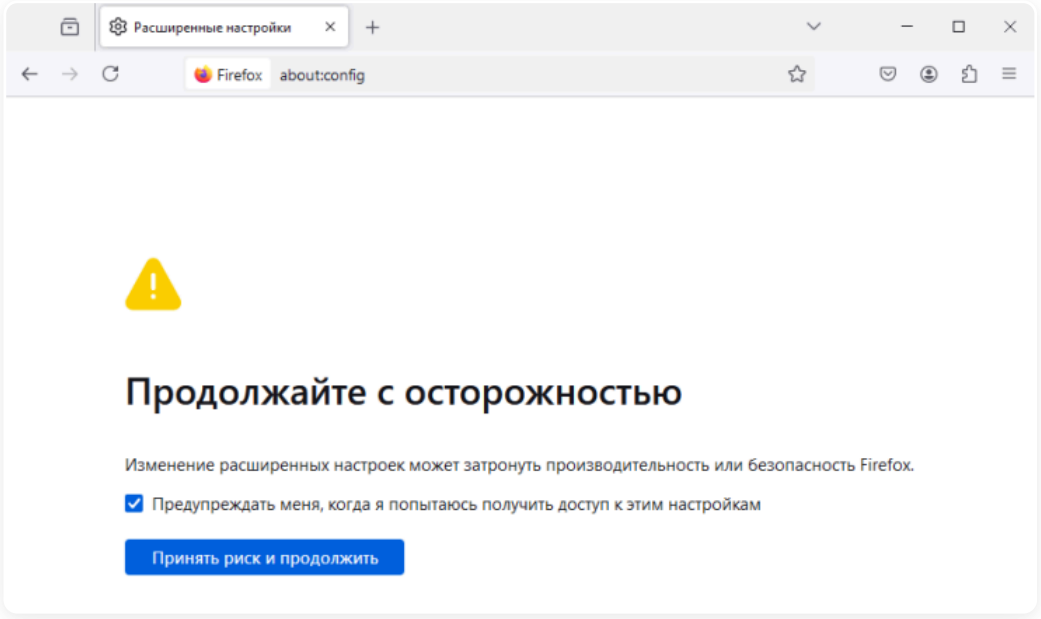


3. В настройках **JavaScript** разрешите сайтам использовать JavaScript:

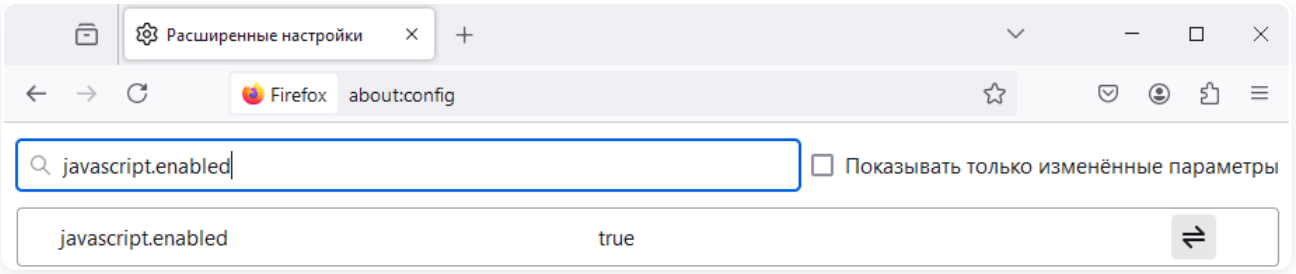


Firefox

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

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

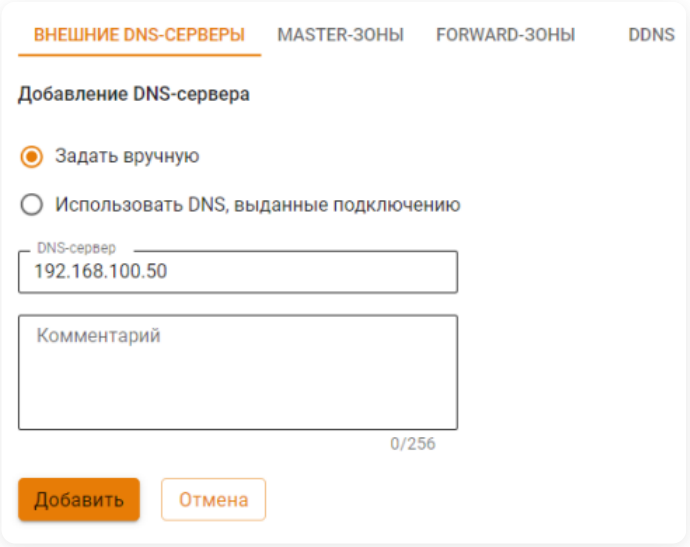
Список служб для других разделов доступен по ссылке.

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

Ideco NGFW поддерживает версии ALD Pro от 1.4.

Ввод сервера в домен

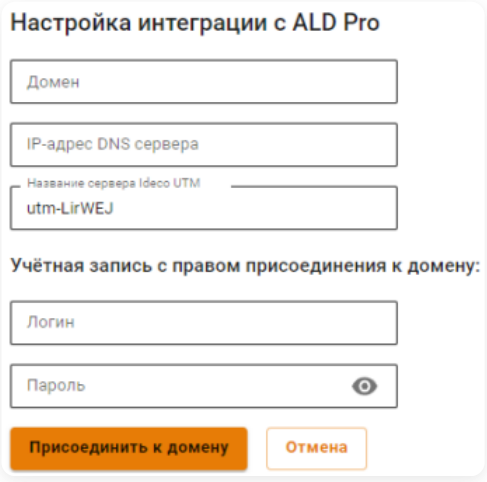
1. Перейдите в раздел **Сервисы** → **Защита и управление DNS** → **Внешние DNS-серверы** и добавьте IP-адрес устройства с установленной системой ALD Pro:



2. Перейдите в **Пользователи** → **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.

- **Имя сервера Ideco NGFW** - 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 без блокировки и считаются **активными**.

Для импорта пользователей выполните действия:

1. Перейдите в раздел **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 **Файрволе**).

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

Пользователь может быть импортирован только в одну группу Ideco NGFW. 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.

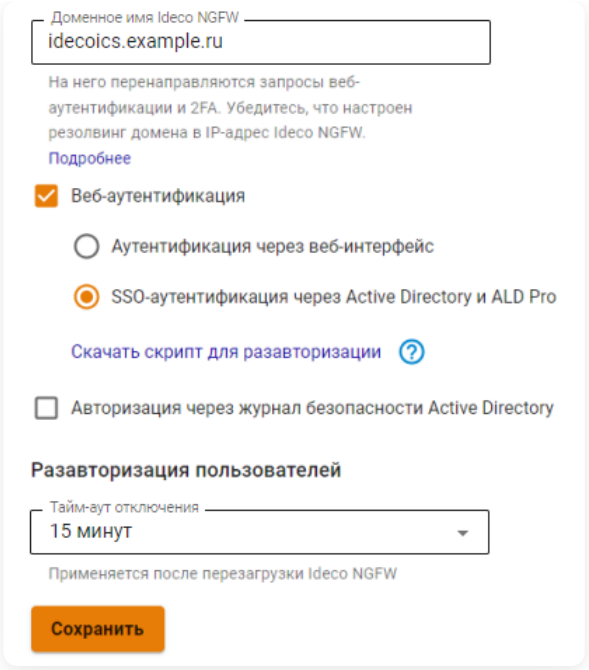
Настройка Ideco NGFW

Для настройки аутентификации выполните действия:

1. Перейдите в **Пользователи** → **Авторизация** → **Настройки**.

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

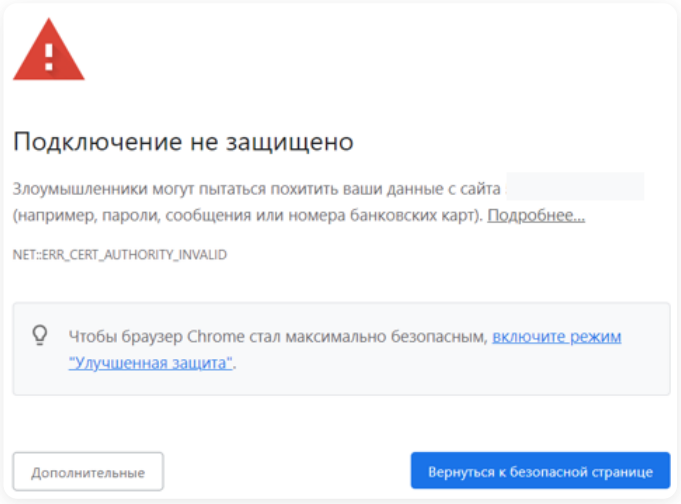
3. Выберите **Тип** входа в систему:



- **Аутентификация через веб-интерфейс** - вход по логину/паролю.
- **SSO-аутентификация через Active Directory и ALD Pro** - вход через SSO.

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

После заполнения поля **Доменное имя Ideco NGFW** 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 не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW, то страница авторизации будет подписана корневым сертификатом NGFW.

5. Настройте способы авторизации импортированных пользователей. Доступные способы:

- 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 в случаях, когда 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

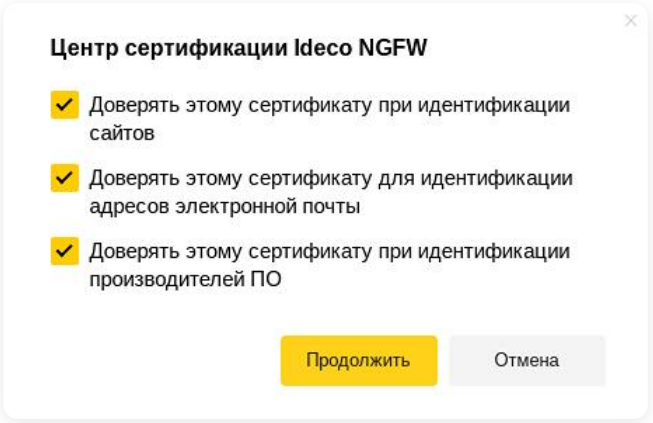
1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и добавьте строки:

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

2. Скачайте корневой сертификат.

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

4. Включите опции доверия для сертификата:



Настройка браузера Google Chrome

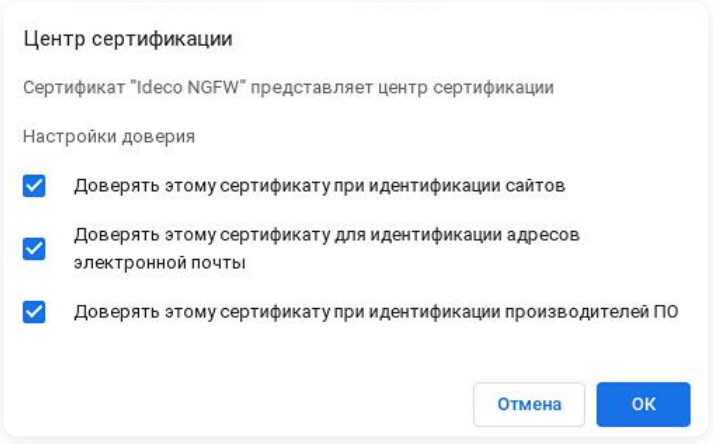
1. Создайте файл **mydomain.json** в директории `/etc/opt/chrome/policies/managed/` и добавьте строки:

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

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите на вкладку **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

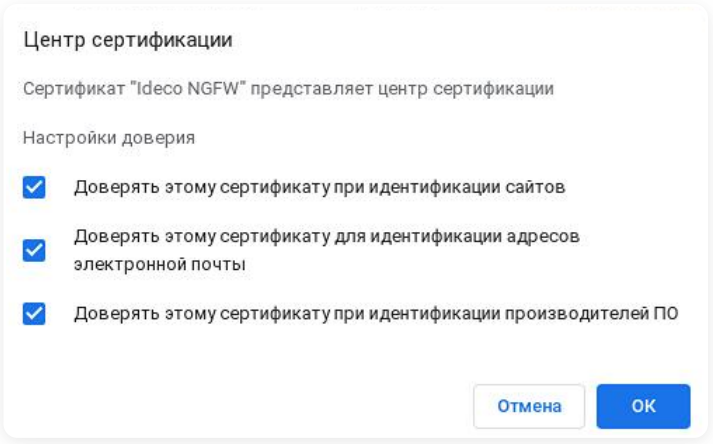
1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и добавьте строки:

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

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите на вкладку **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

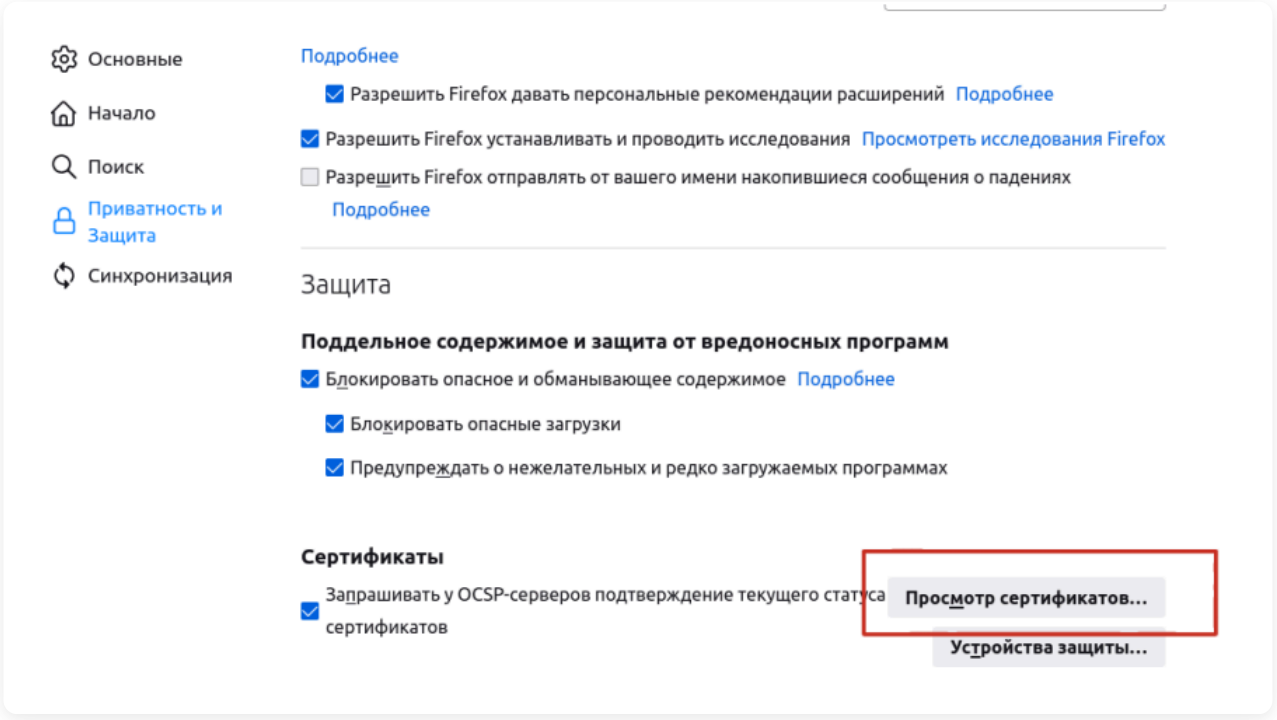
1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

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 локального интерфейса и доменное имя Ideco NGFW в директорию `/etc/hosts`.
Пример: `192.168.100.10 ngfw.domain.ald`.

Руководства по эксплуатации ALD Pro доступны на официальном сайте.

RADIUS

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.
- Пользователи RADIUS могут авторизоваться с помощью Ideco Client без установления VPN-туннеля.
- При отключенной интеграции с RADIUS-сервером пользователи RADIUS не смогут аутентифицироваться на Ideco NGFW.
- 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 поддерживает интеграцию с RADIUS-администраторами. Подробные инструкции по настройке описаны в статье Администраторы.

Настройка интеграции

Для настройки интеграции с RADIUS-сервером выполните действия:

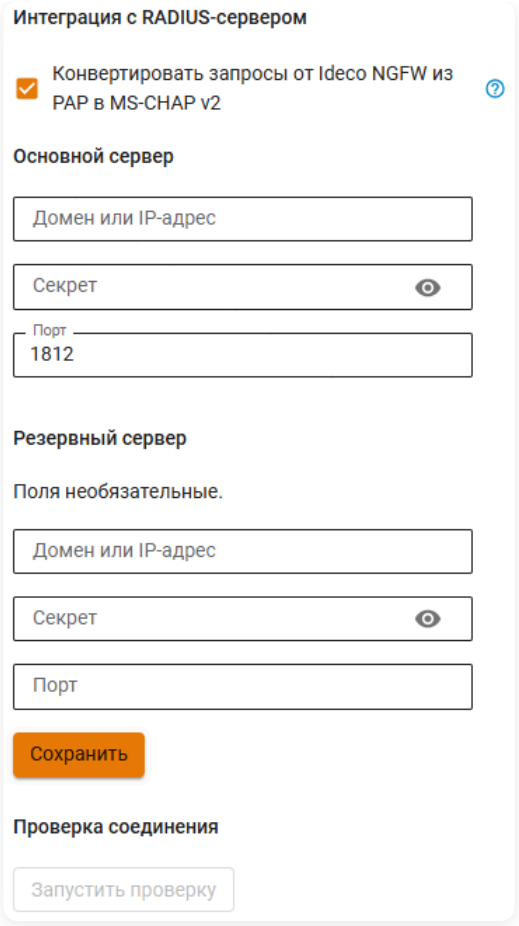
1. Перейдите в **Пользователи** → **RADIUS** и включите опцию **RADIUS**.

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

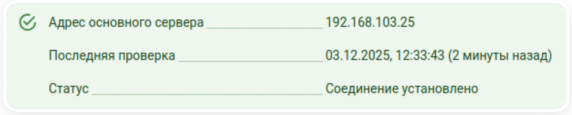
2. Включите опцию **Конвертировать запросы от Ideco NGFW из PAP в MS-CHAP v2**. Опция повышает безопасность и защиту от перехвата паролей между NGFW и RADIUS-сервером, или когда RADIUS-сервер поддерживает только MS-CHAP v2. Выключите опцию только если необходимо настроить двухфакторную аутентификацию для пользователей RADIUS-сервера.

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

2. Заполните поля:



- **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. По умолчанию используется порт 1812.
- **Резервный сервер** - при наличии в сети двух RADIUS-серверов настройте один как резервный с указанием порта подключения. При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.
- **Проверка соединения** - нажмите **Запустить проверку**, чтобы проверить соединение с RADIUS-сервером. При успешной проверке будет показано, что соединение установлено:



3. Нажмите **Сохранить**.

Добавление пользователей в дерево пользователей Ideco NGFW

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

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

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

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

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

Ограничения для группы и пользователей RADIUS:

- Запрещено менять параметры пользователя (в том числе поля **Имя** и **Комментарий**), за исключением опции **Запретить доступ**.
- Разрешено удалять и переименовывать группу **RADIUS**.
- Запрещено перемещать пользователей в другие группы.
- Запрещено перемещать других пользователей NGFW 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 только 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 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:

1. В веб-интерфейсе Ideco NGFW в **Пользователи** → **RADIUS** отключите опцию **Конвертировать запросы от Ideco NGFW 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.

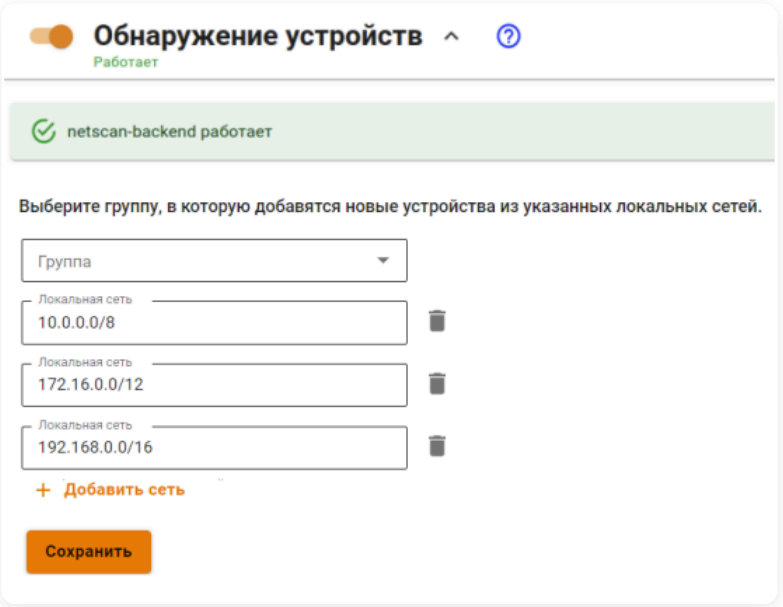
3. Настройте на RADIUS-сервере механизм двухфакторной аутентификации. Настраивать 2FA на Ideco NGFW не нужно.

Обнаружение устройств

Совет

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. 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 уже есть учетная запись с логином, равным NetBIOS-имени машины, то NGFW использует данные пользователя без обновления его параметров (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 этом 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 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 >

Telegram-бот

В статье описана настройка оповещений от Ideco Monitoring Bot

Перейти >

SNMP

В статье описана настройка доступа к Ideco NGFW по протоколу SNMP

Перейти >

Zabbix-агент

В статье описана интеграция Zabbix-агента в Ideco NGFW

Перейти >

Netflow

В статье описана настройка экспорта статистики трафика на коллектор во внешней или локальной сети по протоколу Netflow.

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

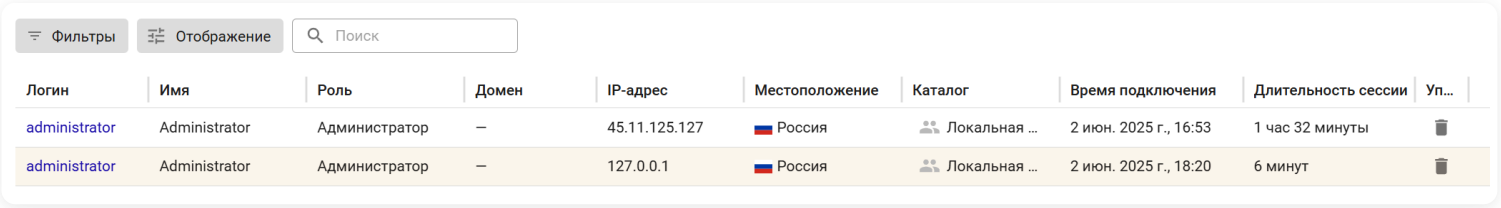
Раздел содержит список всех сессий администраторов в NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS.

Сессии администраторов, подключенных через Ideco Center, не отображаются в разделе.

Сессии администраторов

Сессия с IP-адресом 127.0.0.1 - сессия администратора, работающего в локальном меню сервера.

Таблица сессий авторизованных администраторов в NGFW:



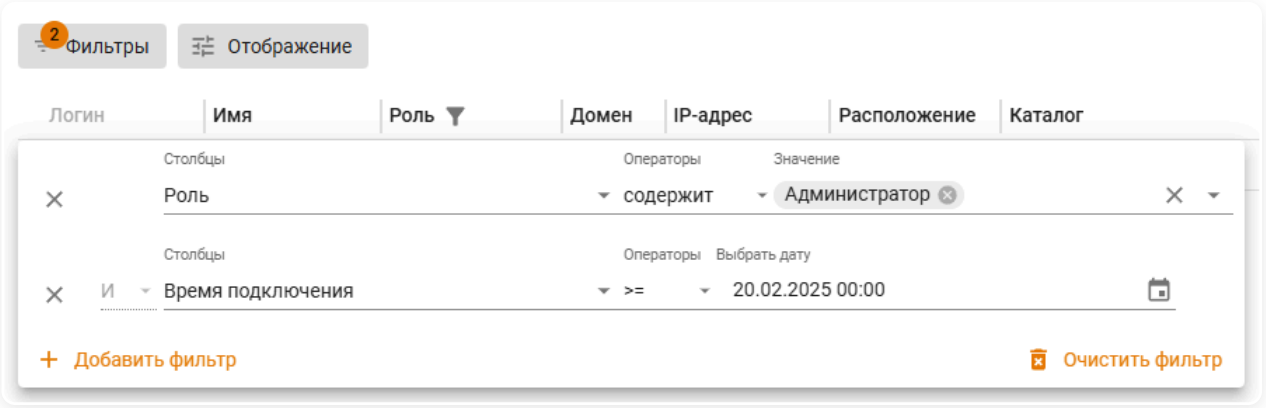
- **Роль** - возможные роли: Администратор, Только просмотр, Администратор ИБ, Администратор файрвола, Администратор настройки доступов, Просмотр отчетов, Создание отчетов.
- **Домен** - доменное имя, если администратор импортирован из Active Directory или ALD PRO. В ином случае в ячейке прочерк.
- **IP-адрес** - IP-адрес устройства, с которого авторизован администратор.
- **Расположение** - географическое расположение администратора.
- **Каталог** - тип администратора в зависимости от источника добавления: Локальная группа, AD, ALD, 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 завершить сессию любого администратора из интерфейса Ideco NGFW.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока сессия администратора будет автоматически завершена.

В столбце **Управление** администратор может завершить свою сессию.

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:



Полезные ссылки

Администраторы

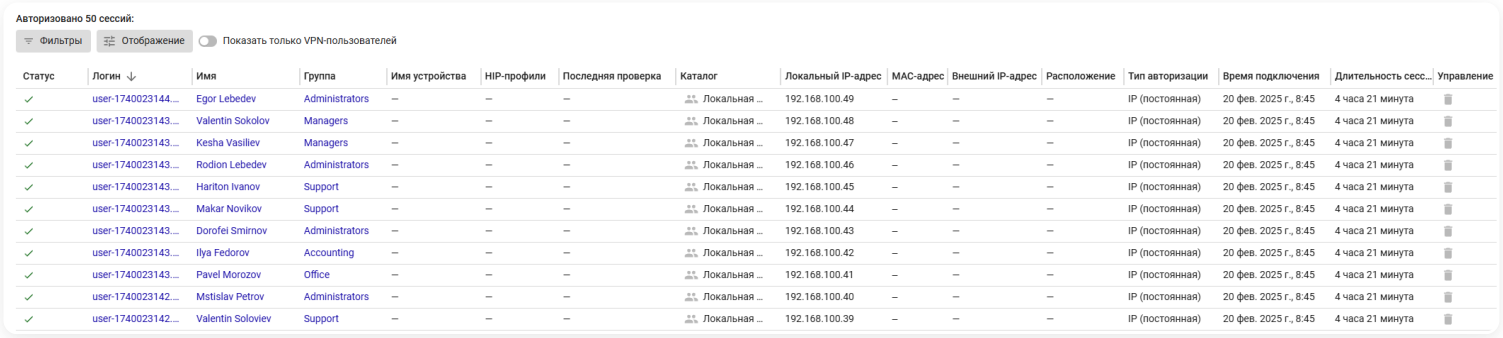
Действия администраторов

Сессии пользователей

Раздел содержит список всех сессий пользователей, которые авторизовались в NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS.

Количество сессий в мониторинге не является показателем занимаемых лицензий, так как под одной пользовательской учетной записью возможно одновременное авторизация до 5 устройств, что учитывается как одна лицензия.

Таблица сессий авторизованных пользователей в NGFW:



Статусы подключения пользователей

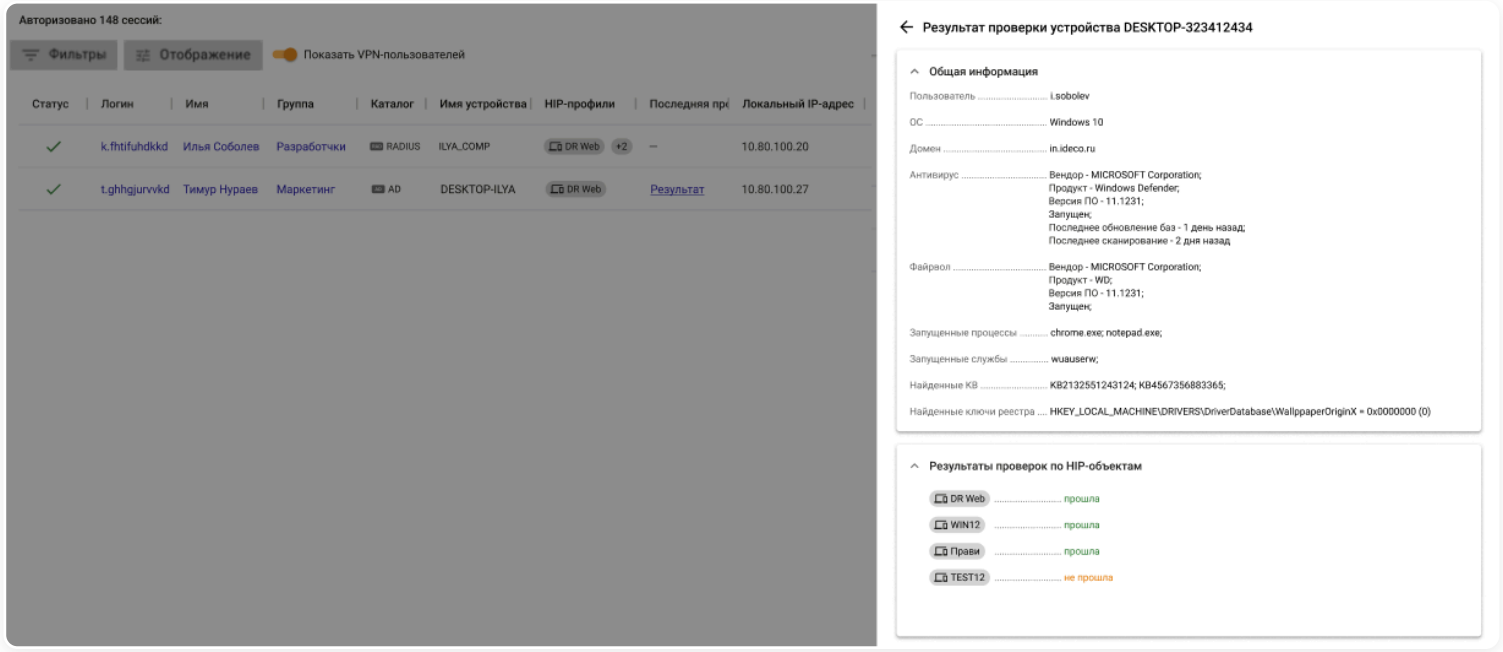
- **Подключено**. Пользователь авторизован;

- **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 активные 5 сессий;

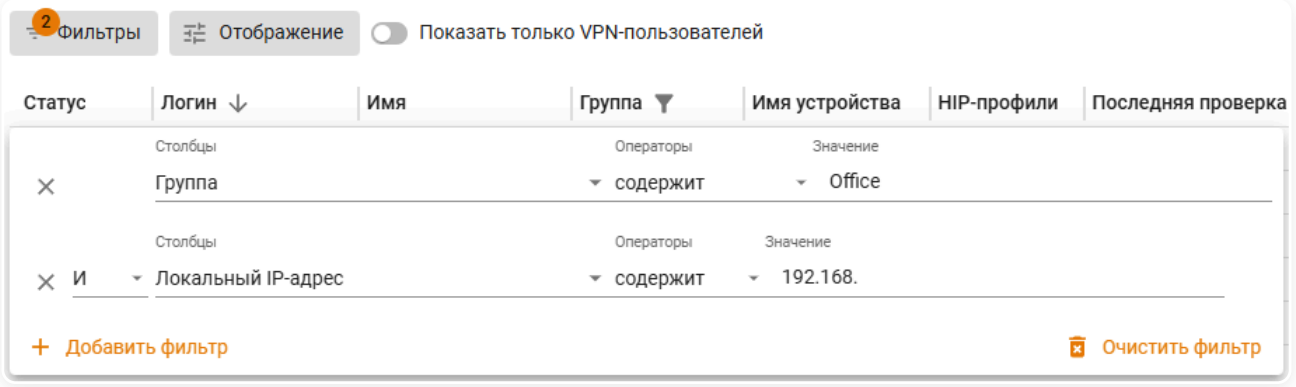
- **Сессия удаляется**. Появляется при разрыве сессии с динамическим IP-адресом. Сессия с таким статусом будет удалена через 30 секунд.

Для просмотра результата проверки устройства, подключенного через Ideco Client, кликните 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:



Опция **Показать только VPN-пользователей** позволяет отображать в таблице журнала только тех пользователей, которые подключены к NGFW через VPN.

Полезные ссылки

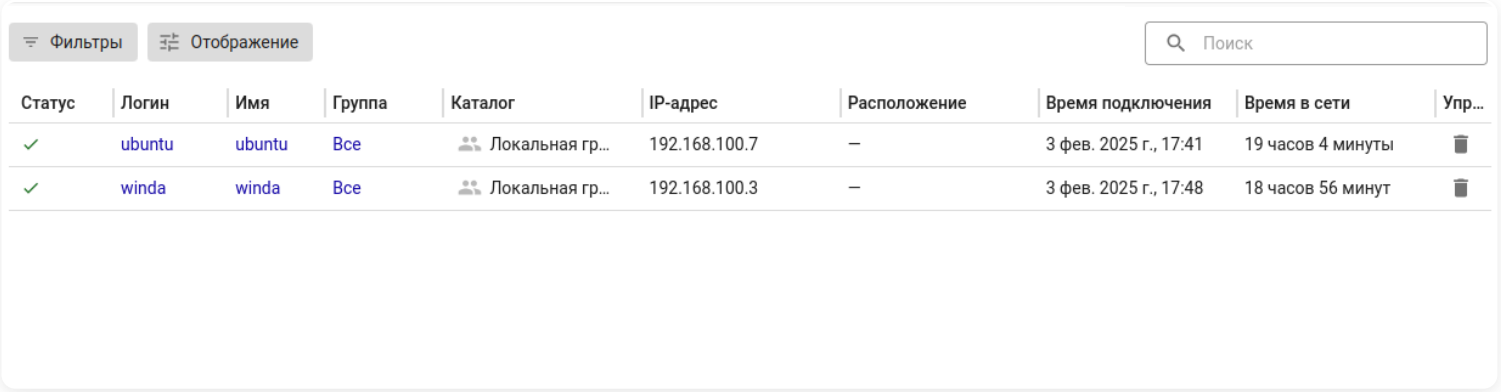
Авторизация пользователей

Сессии ЛК

Сессии ЛК - таблица активных сессий в личном кабинете Ideco NGFW. 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 разделе **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 и каталог), таблица активных сессий содержит столбцы:

- **Статус** - доступные значения: авторизован, 2FA (ожидает 2FA, генерация TOTP для прохождения 2FA);
- **IP-адрес** - IP-адрес, с которого произведена начальная аутентификация сессии в ЛК;
- **Расположение** - 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 **Расположение** 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 и его значение;
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Графики загруженности

Модуль **Графики загруженности** позволяет просматривать данные о состоянии Ideco NGFW 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, 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%);
- 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, статической и динамической балансировки.

Диски

Содержит статистику об объеме записанной и прочитанной информации в определенный промежуток времени (график **Диск**) и количестве обращений к диску за это же время (график **Операции ввода-вывода**). Дает оценку интенсивности использования диска. Информация о свободном и занятом объеме на диске доступна в разделе Бэкапы.

VPN

Содержит информацию о количестве подключений пользователей по протоколам L2TP/IPsec, PPTP и IKEv2.

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.

Полезные ссылки

- Сетевые интерфейсы
- Балансировка и резервирование
- Кластеризация
- Бэкапы
- ГОСТ VPN

- Инструкции по созданию VPN-подключений

Монитор трафика

В разделе **Мониторинг → Монитор трафика** можно просматривать данные о трафике (вх./исх. скорость, количество сессий), проходящем через Ideco NGFW в режиме реального времени.

Для работы **Монитора трафика** необходимо необходимо включить Контроль приложений.

Раздел **Монитор трафика** состоит из вкладок:

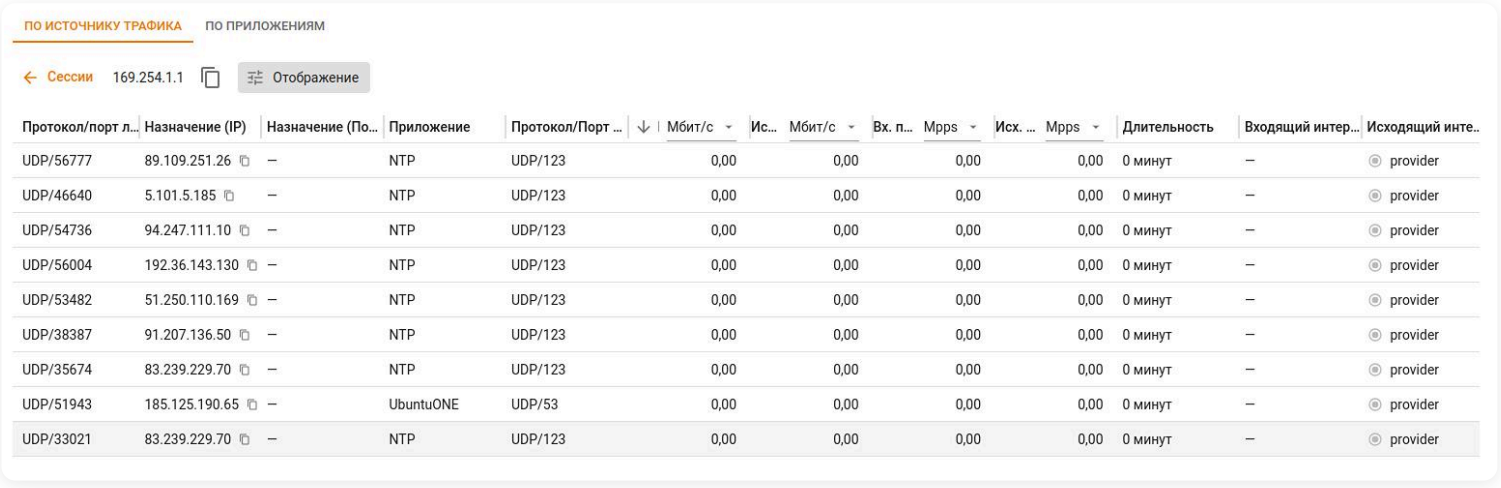
По источнику трафика

Вкладка **По источнику трафика** позволяет отслеживать активность пользователей сети и выявлять тех, кто нагружает канал трафиком:



Источник (IP)	Источник (Пользователь)	Источник (Объекты)	Сессии	Вх. скор... Мбит/с	Исх. скорость Мбит/с	Вх. пакеты Mpps	Исх. пакеты Mpps
169.254.1.1	–	–	70	0,01	0,01	0,00	0,00
172.16.50.3	–	–	6	0,00	0,00	0,00	0,00
172.16.50.255	–	–	1	0,00	0,00	0,00	0,00
192.168.100.1	–	–	10	0,00	0,00	0,00	0,00

Для просмотра информации об активности определенного узла локальной сети нажмите на **количество сессий** в таблице:



Протокол/порт л...	Назначение (IP)	Назначение (По...	Приложение	Протокол/Порт ...	Мбит/с	Ис... Мбит/с	Вх. п... Mpps	Исх. ... Mpps	Длительность	Входящий интер...	Исходящий инте..
UDP/56777	89.109.251.26	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/46640	5.101.5.185	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/54736	94.247.111.10	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/56004	192.36.143.130	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/53482	51.250.110.169	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/38387	91.207.136.50	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/35674	83.239.229.70	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/51943	185.125.190.65	–	UbuntuONE	UDP/53	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/33021	83.239.229.70	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider

По приложениям

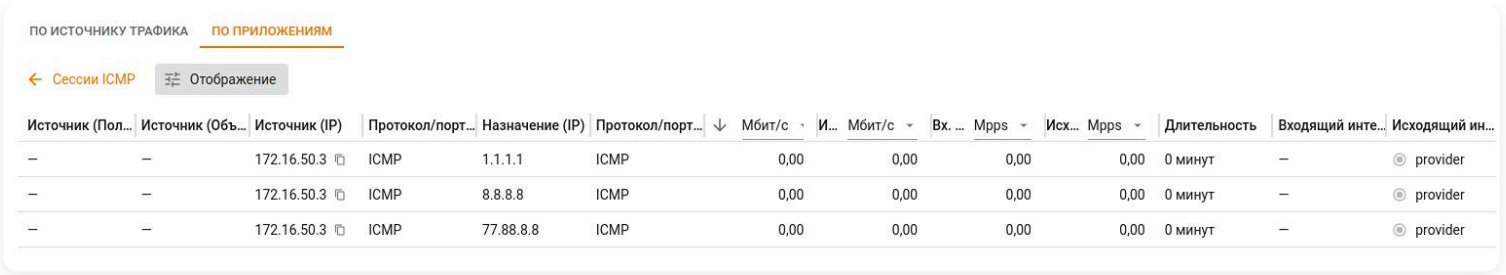
Вкладка **По приложениям** позволяет отслеживать активность приложений.

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:



Приложение	Сессии	Вх. скорость Мбит/с	Исх. скорость Мбит/с	Вх. пакеты Mpps	Исх. пакеты Mpps
ICMP	3	0,00	0,00	0,00	0,00
NTP	13	0,00	0,00	0,00	0,00
Unknown	2	0,00	0,00	0,00	0,00
TLS	1	0,00	0,00	0,00	0,00
Dropbox	2	0,00	0,00	0,00	0,00

Для просмотра подробной информации об активности определенного приложения нажмите на **количество сессий** в таблице:



Полезные ссылки

- Контроль приложений

Telegram-бот

Ideco Monitoring Bot - это Telegram-бот, который отправляет уведомления о событиях в Ideco NGFW (уведомления из колокольчика):

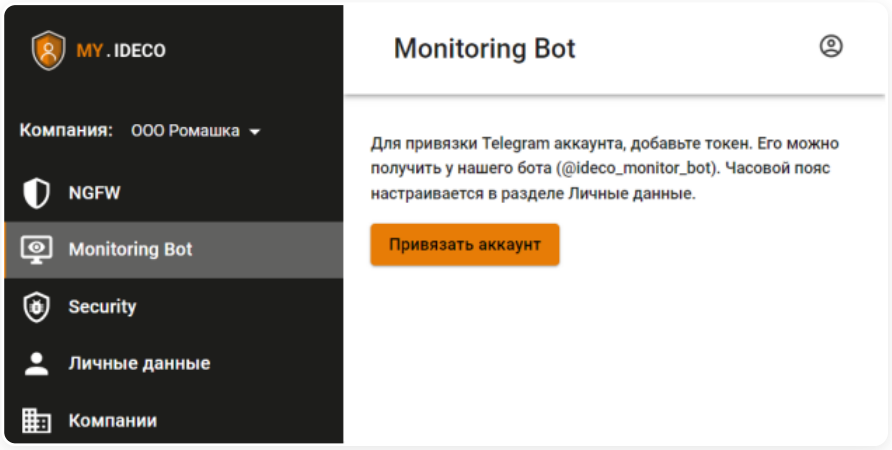
- В личные сообщения;
- В беседы, где 2 и более участников (groups).

Привязка бота и настройка оповещений Ideco Monitoring Bot осуществляется в личном кабинете.

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 личном кабинете.
5. Нажмите **Привязать аккаунт**.
6. Введите код в поле **Токен Telegram-аккаунта** и нажмите **Привязать**:

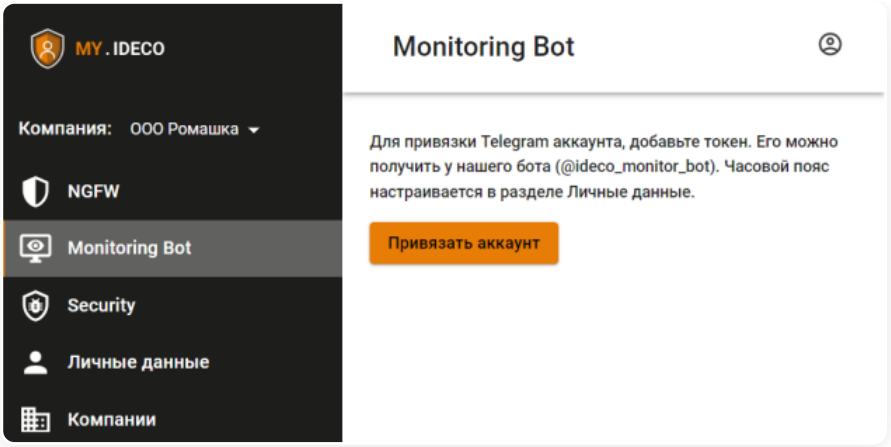


Уведомления начнут приходить в Telegram-аккаунт.

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 личном кабинете.
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 личном кабинете.
2. Выберите аккаунт или группу и нажмите .
3. Выберите уведомления, которые хотели бы получать.

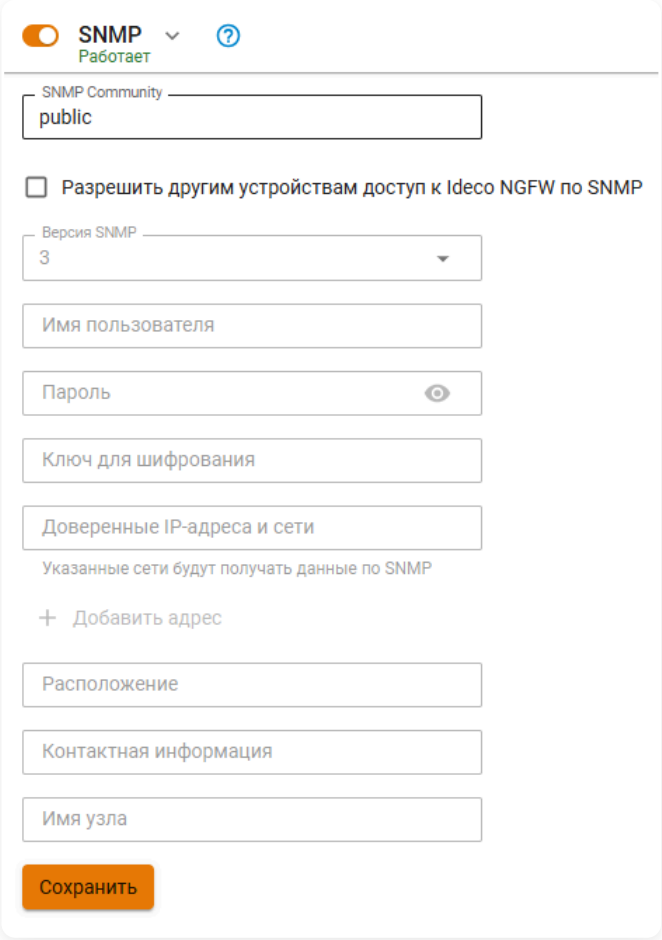
Если требуется временно отключить отправку уведомлений, нажмите на . Оповещения перестанут приходить, пока снова не нажмете на эту иконку.

SNMP

SNMP - это протокол для управления и мониторинга сетевых устройств, таких как маршрутизаторы, коммутаторы и фаерволы.
Модуль **SNMP** обеспечивает мониторинг работы Ideco NGFW по протоколу SNMP версий 1/2c и 3.

Настройка подключения

Для подключения по протоколу SNMP в разделе **Мониторинг** → **SNMP** включите опцию и заполните поля:



Версия 1/2c

- **Имя пользователя**;
- **Пароль** (минимальное количество символов - 8);
- **Доверенные IP-адреса и сети**.

Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и являются необязательными.

Версия 3

- **Имя пользователя**;
- **Пароль** (минимальное количество символов - 8);
- **Ключ шифрования**;
- **Доверенные IP-адреса и сети**.

Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.

Рекомендуем: На сервере, с которым будет установлено соединение по SNMPv3, укажите 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 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`).

Интеграция с Zabbix

Zabbix - система с открытым исходным кодом для мониторинга параметров сети, состояния и работоспособности серверов.

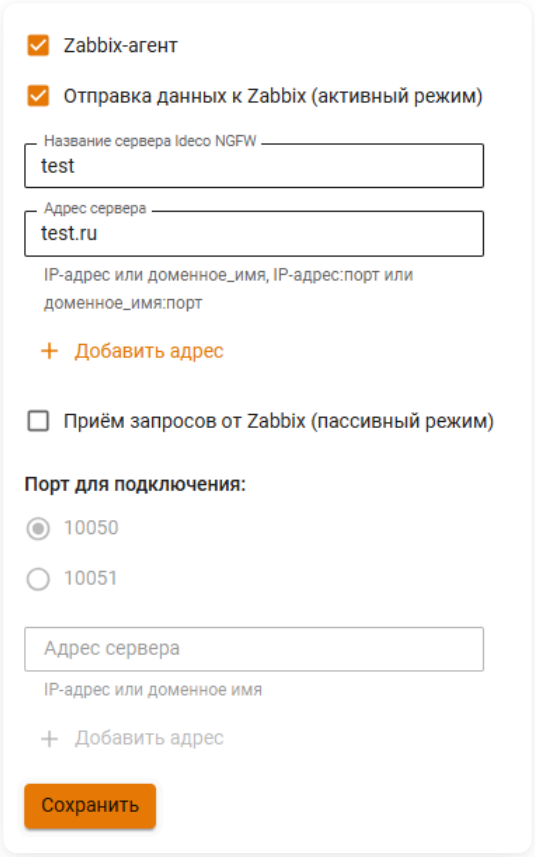
Настройка Zabbix-агента

Для работы системы мониторинга Zabbix в Ideco NGFW активируйте опцию **Zabbix-агент** после настройки интеграции с Zabbix.

Интеграция с системой мониторинга Zabbix возможна в двух режимах: **Активный** и **Пассивный**.

Активный

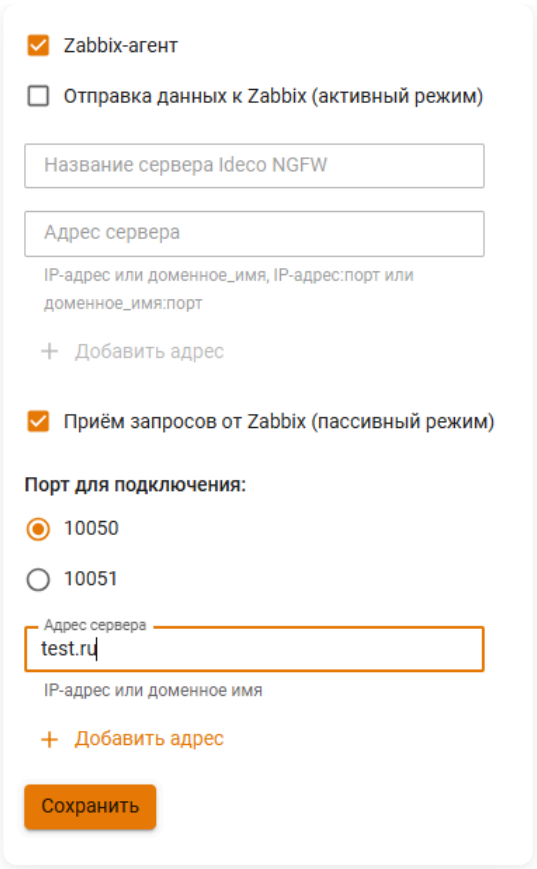
Соединение с Zabbix-сервером происходит со стороны Ideco NGFW. Для настройки заполните поля:



- **Имя сервера Ideco NGFW** - 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 может находиться как внутри локальной сети Ideco NGFW, так и за ее пределами. Подключение мониторинга возможно как к локальным, так и к внешним интерфейсам.

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

Netflow

Netflow - проприетарный открытый протокол, разработанный Cisco для мониторинга статистики трафика в сети. Ideco NGFW выступает в качестве сенсора-экспортера, который собирает статистику при прохождении через него трафика.

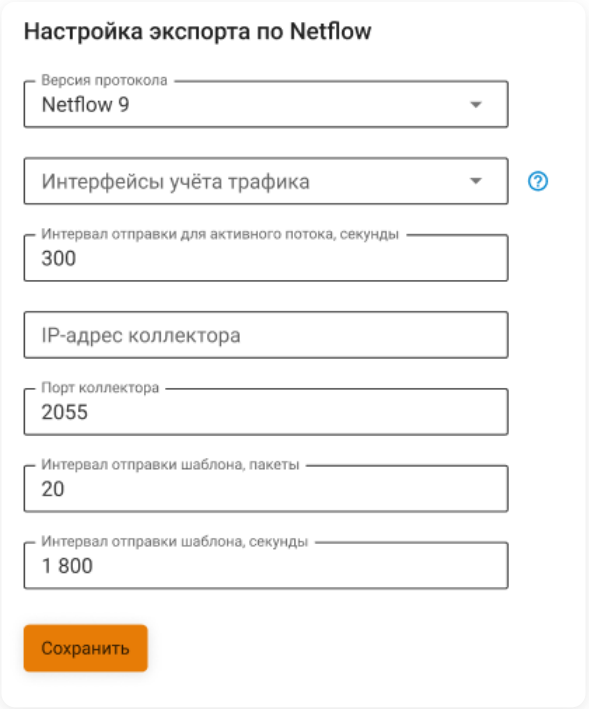
Netflow обеспечивает сбор информации об IP-трафике, обрабатываемом сетевыми устройствами (L3-коммутаторы, маршрутизаторы, сенсоры). Каждый поток является однонаправленным, т.е. каждое двунаправленное соединение **src <--> dst** интерпретируется как два потока: **src -> dst** и **dst -> src**.

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 на вкладку **Мониторинг** → **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 мониторить (доступны Ethernet-интерфейсы. Если не заполнены, статистика не будет экспортироваться;
- **Интервал отправки для активного потока, секунды** - введите временной интервал, через который NGFW будет отправлять на коллектор отчеты по потокам, которые не успели завершиться (информация о завершенных потоках отправляется по завершении). От 60 до 3600 секунд, 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. Минимум 10, максимум 6000, 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. Минимум 60, максимум 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 потере связи с коллектором или его перезагрузке.

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

Правила трафика

В этом разделе описывается настройка служб, определяющих основные правила фильтрации трафика в Ideco NGFW.

Файрвол

Создание правил Файрвола, 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 >

Антивирус

Интеграция Kaspersky Anti-Virus Software Development Kit в Ideco NGFW

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 **Файрвола**, **Контент-фильтра**, **Контроля приложений**, **Маршрутизации**

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Файрвол

Название службы раздела **Файрвол**: `ideco-firewall-backend`.

Список имен служб для других разделов доступен по ссылке.

Файрвол - средство управления трафиком на сервере (межсетевой экран). Поддерживает фильтрацию пакетов с контролем состояния соединений (Stateful Inspection) - решение о блокировке принимается на все соединение.

Файрвол 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 **Файрвола** можно создавать наборы правил, которые разграничивают трафик между различными сетями: локальными, VPN и публичными (интернет). В Ideco NGFW 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**).

Файрвол 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

Файрвол 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.

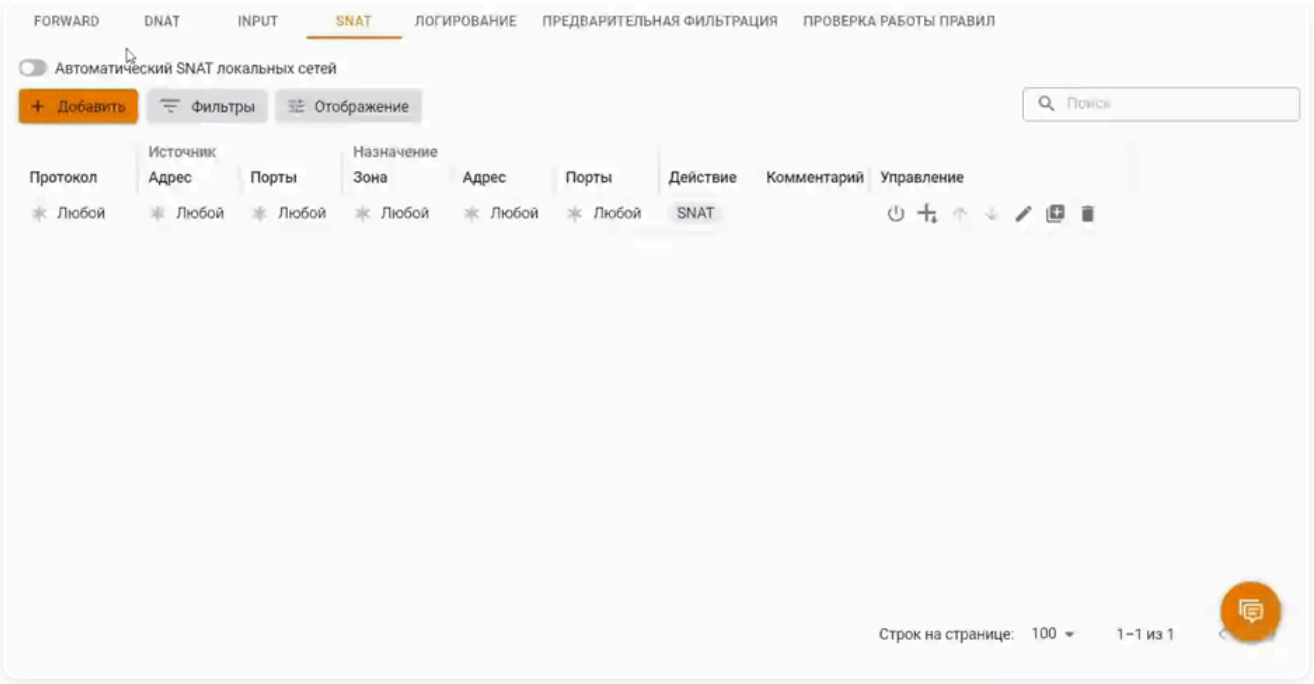
Для работы DPI/IPS в правилах **Файрвола** можно подключить **Профили безопасности**, создав разрешающее правило с включенной проверкой через **Контроль приложений** и/или систему **Предотвращения вторжений**. Профили настраиваются в разделе **Профили безопасности**.

Настройка и управление правилами

Настройка производится в разделе веб-интерфейса **Правила трафика** → **Файрвол**. На вкладках раздела добавляются правила управления трафиком, которые отображаются в таблицах **Файрвола**. При наличии большого количества правил используйте кнопку **Фильтры**.

Если необходимо использовать большое количество правил, можно использовать API. Эти правила не будут отображаться в веб-интерфейсе, но будут работать значительно быстрее.

Включите опцию **Счетчик срабатываний** для подсчета количества срабатываний правил **Файрвола**. После включения опции в таблице появится соответствующий столбец:



Особенности

- Включение режима удаленного помощника изменяет таблицу правил **Файрвола**, разрешая подключение по SSH из локальных и внешних сетей.
- В Ideco NGFW 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 **Файрволе** 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 файрвол** и нажмите Enter:

```
Управление сервером

1. Консоль
2. Отключить все интерфейсы и настроить новый
3. Включить доступ к веб-интерфейсу из внешней сети
4. Включить доступ к серверу по SSH из Интернет
5. Включить доступ к серверу по SSH из локальных сетей
6. Включить режим `Разрешить Интернет всем`
7. Сбросить блокировки по IP
8. Отключить пользовательский файрвол
9. Отключение VCE-интерфейсов
10. Создать новый бэкап
11. Восстановить из бэкапа
12. Мгновенно восстановить из бэкапа
13. Включить доступ Удаленного Помощника
14. Контакты технической поддержки
15. Управление кластером
16. Восстановиться на предыдущую версию
17. Перезагрузка сервера
18. Отключить сервер
19. Выход

Введите номер пункта и нажмите Enter.
# 8
```

При отключении пользовательского файрвола в веб-интерфейсе системные правила продолжают работу.

Полезные ссылки

Настройка Файрвола

- **Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT)**;
- **Примеры создания правил файрвола**;
- **Логирование**;
- **Тестирование правил**;
- **Предварительная фильтрация**;
- **Аппаратная фильтрация**.

Профили безопасности

- **Контроль приложений**;
- **Предотвращение вторжений**.

Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT)

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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 сервера (например, почтового сервера);
- **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 **Файрвола** воспользуйтесь кнопкой **Фильтры**.

Создание правил

Для создания правила в нужной таблице нажмите кнопку **Добавить**.

Укажите необходимые параметры, действия правила и нажмите кнопку **Добавить**. Правило будет добавлено в конец списка. Если необходимо, измените его приоритет кнопками ↑ ↓.

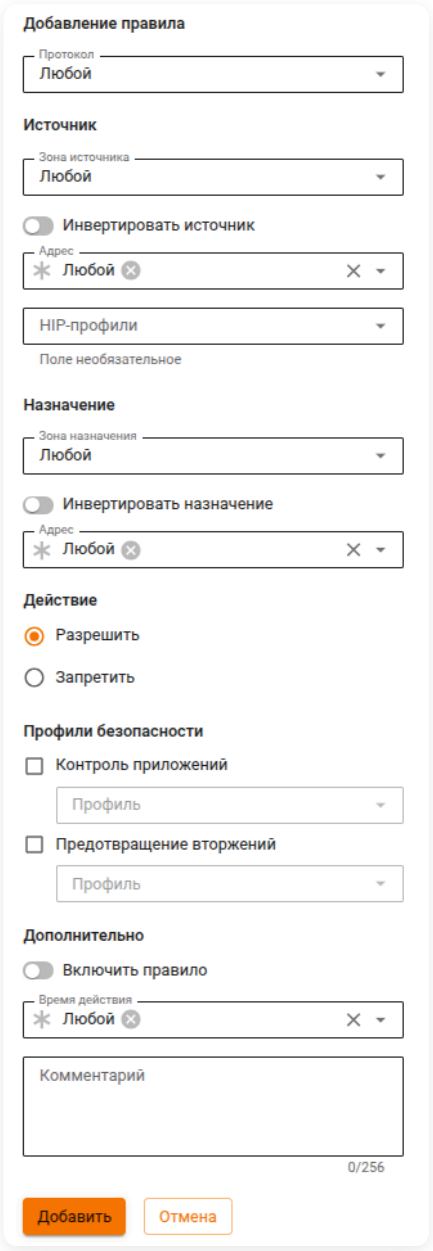
В качестве **Зоны источника** или **Зоны назначения** можно выбрать **Специальные** типы:

Специальные типы

- **Внешние интерфейсы** - все интерфейсы, используемые для подключения к интернету.
- **Внешние Ethernet-интерфейсы** - все Ethernet-интерфейсы, используемые для подключения к интернету.
- **Внешние VPN-интерфейсы** - все туннельные интерфейсы для подключения к интернету (Ethernet+PPPoE, Ethernet+PPTP, Ethernet+L2TP).
- **IPsec-интерфейсы** - все IPsec-интерфейсы, используемые для site-to-site-подключений к удаленным офисам.
- **Локальные интерфейсы** - все интерфейсы, используемые для подключения к клиентам в локальной сети.
- **Исходящий трафик устройства** - используется для фильтрации исходящего трафика самого устройства Ideco NGFW.
- **Клиентский VPN-трафик** - используется для фильтрации трафика, идущего от клиентов, подключившихся к NGFW по VPN.
- **Любой** - не фильтровать трафик по какому-либо типу интерфейса или зоны.

В Ideco NGFW нет подразделения локальных интерфейсов на VPN-интерфейсы и Ethernet, поскольку Ideco NGFW не имеет локальных VPN-интерфейсов.

FORWARD



Расшифровка полей

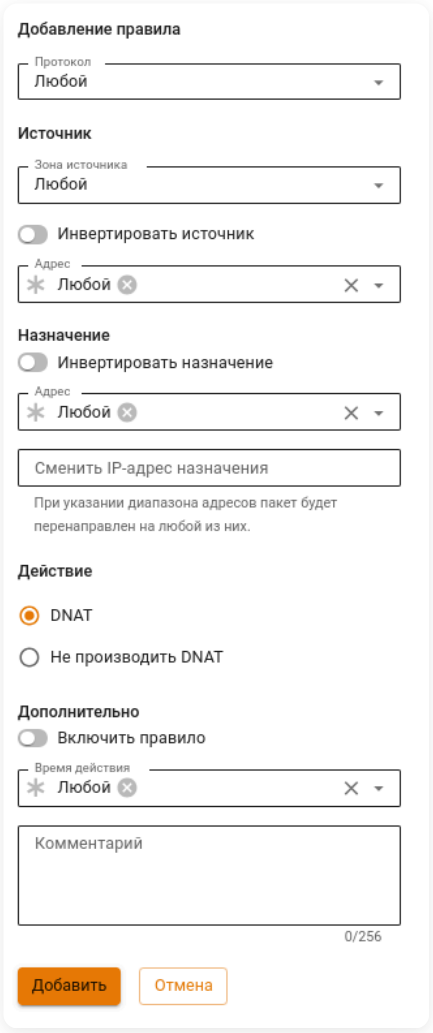
- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны или **Специальные типы**.
  - **Инвертировать 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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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.
  - **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 или **Специальные типы**.
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **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 их IP-адресов, файрвол автоматически это учтет).

Максимальное количество объектов в поле - 200.

- **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**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
- **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.
  - **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

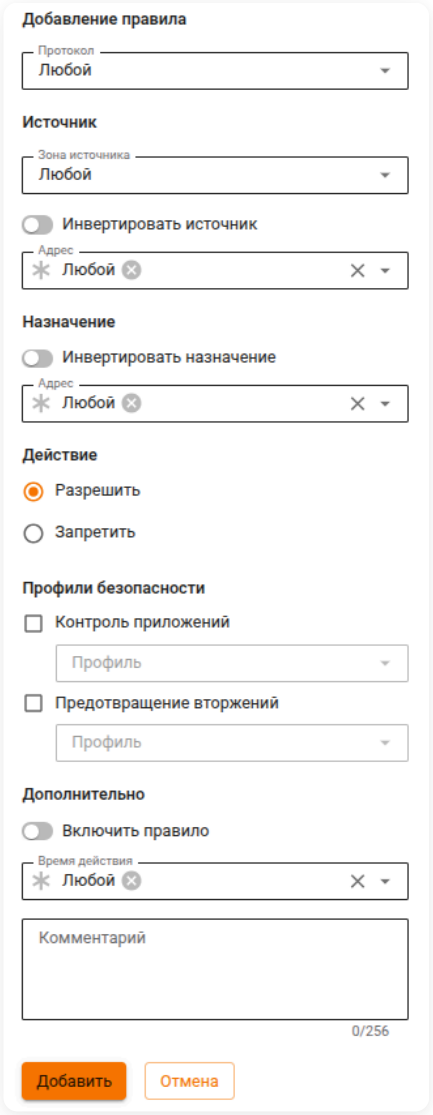


Расшифровка полей

- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны 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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 строке **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 их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 он пришел, если этот порт попадает в указанный диапазон.
- **Действия**:
  - **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.
  - **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 (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).

- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны 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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 строке **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 их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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.
- **Действия**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
- **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.
  - **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.

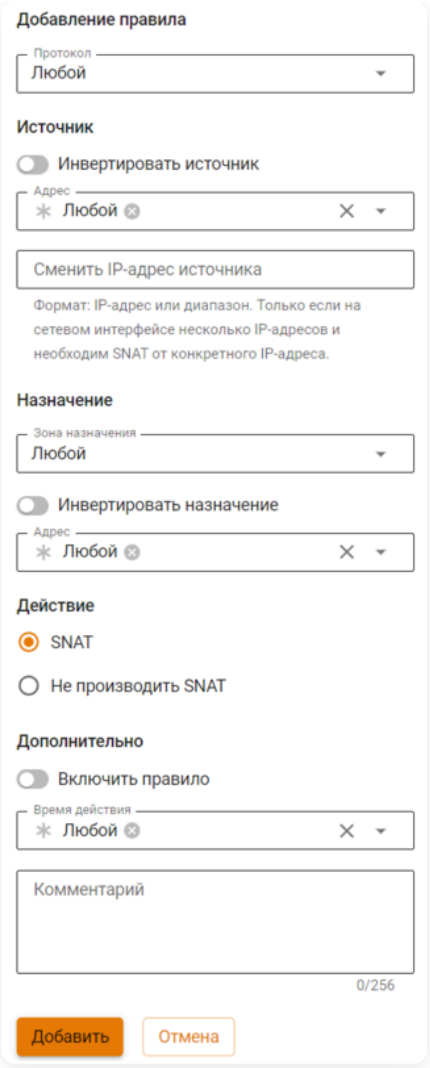
SNAT

> 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**.

> Пользовательские правила **SNAT** имеют приоритет над автоматическим **SNAT** для локальных сетей.



Расшифровка полей

- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).
- **Источник**:
  - **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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 или **Специальные типы**.
- **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **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 их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
- **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.
  - **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.

Использование профилей безопасности

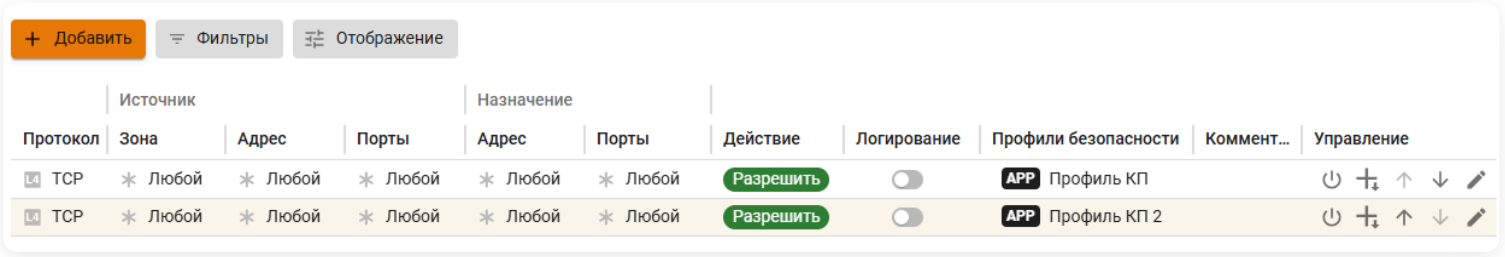
Файрвол Ideco NGFW обрабатывает правила последовательно, сверху вниз. Первое правило, условия которого совпадают с характеристиками проходящего трафика, определяет:

- 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".

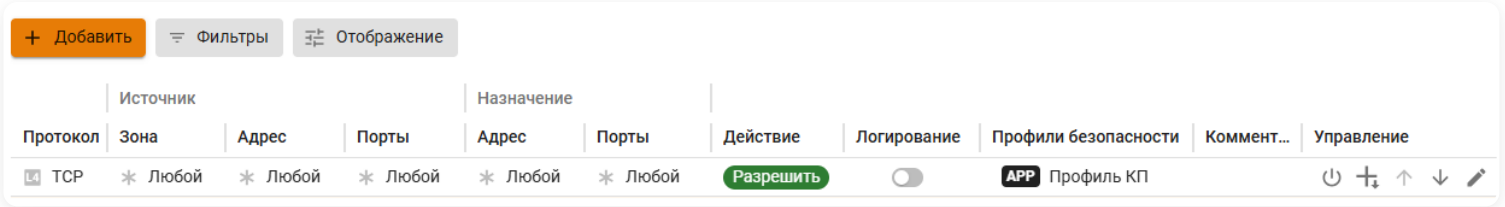


В этом случае при возникновении соответствующего трафика сотрудникам будет ограничен доступ только к социальным сетям - второе правило не будет применено, потому что трафик уже обработан вышестоящим правилом.

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 **Файрвол** → **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, т.к. **INPUT**-правила Файрвола 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, но **зона интерфейса источника сохраняется**.
- Не используйте зону, указанную в разделе **VPN-подключения** → **Основное**, для блокировки TCP. В противном случае HTTP- и HTTPS-трафик через эту зону не будет заблокирован.

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. Для предотвращения блокировки клиентского HTTP/HTTPS-трафика **рекомендуем**:
  - Создать правило, разрешающее трафик от пользователя.
  - Создать правило, разрешающее трафик для специальной зоны источника **Исходящий трафик устройства**.
- При создании правил **Файрвола** 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

- **Полный цикл обработки трафика в Ideco NGFW**
- **Порядок обработки веб-трафика в Ideco NGFW**
- **Объекты**
- **Профили устройств**
- **Логирование**
- **Контроль приложений**
- **Предотвращение вторжений**

Примеры создания правил файрвола

Настройка правил файрвола для IPsec-подключений

Чтобы настроить правило **Файрвола** 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 файрвола

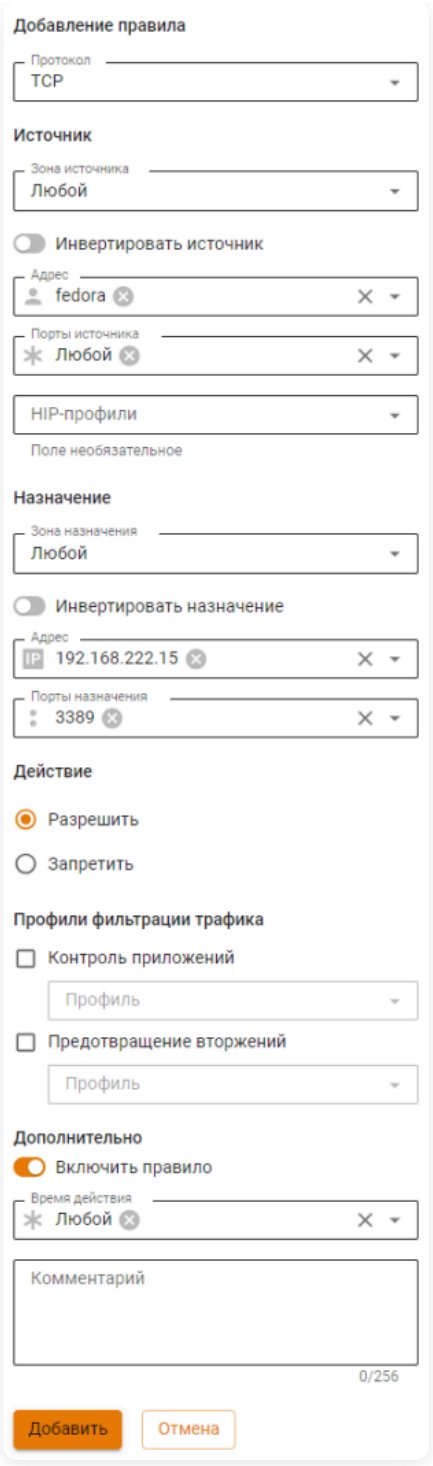
Вопросы блокировки программ удаленного управления (AmmyAdmin и TeamViewer), мессенджеров и другого ПО - описаны в статье Блокировка популярных ресурсов.

Доступ к терминальному серверу для определенного пользователя

1. На вкладке **Правила трафика** → **Файрвол** → **FORWARD** нажмите **Добавить**.

2. Заполните поля:

- **Протокол** - выберите TCP.
- **Адрес** - выберите пользователя или группу пользователей.
- **Назначения** - укажите адрес терминального сервера.
- **Порты назначения** - укажите порт 3389.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

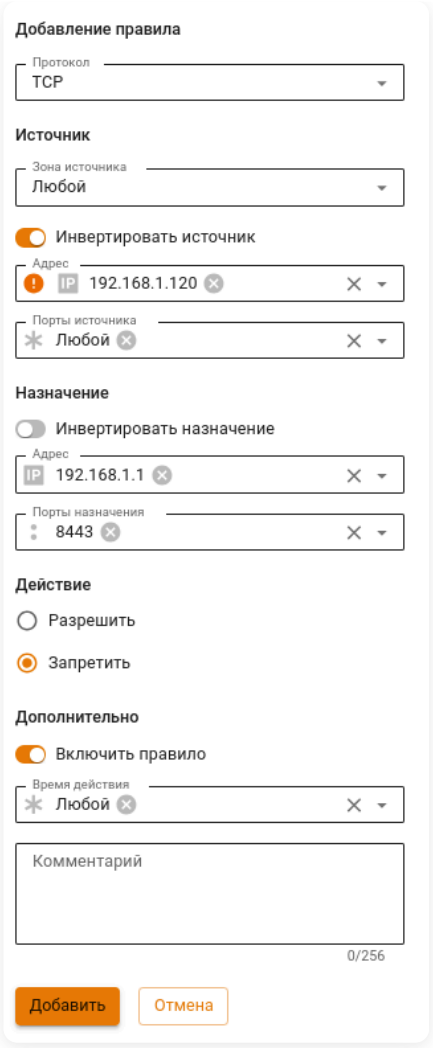


3. Нажмите **Добавить**.

Блокировка доступа к веб-интерфейсу (порт 8443) всем, кроме определенного адреса

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:



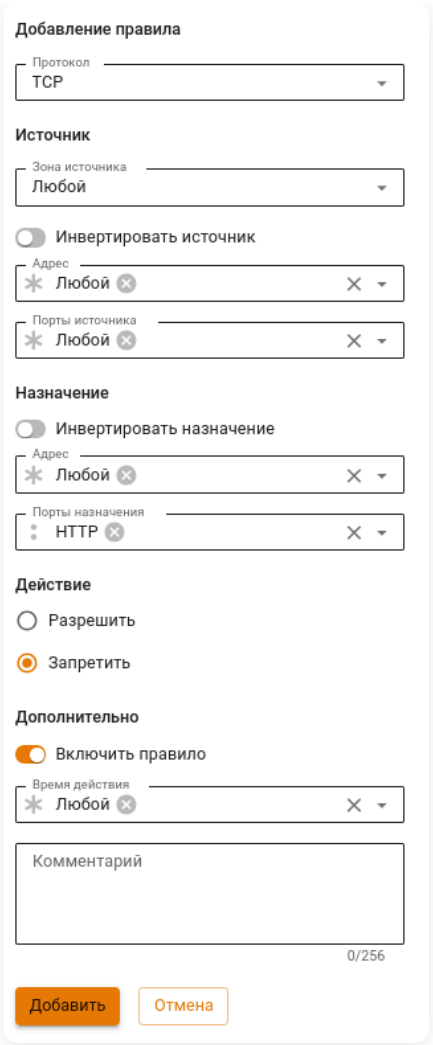
- Доступ к веб-интерфейсу будет разрешен только с IP-адреса **192.168.1.120**.
- **192.168.1.1** - IP-адрес Ideco NGFW в локальной сети.

Блокировка 80 порта Ideco NGFW

80 TCP порт используется для выпуска сертификатов Let`s Encrypt.

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:



Разрешение DNS-запросов через внешние DNS

ВАЖНО: Рекомендуем использовать в качестве DNS-сервер Ideco NGFW. Но если необходимо использовать внешний DNS-сервер, то выполните действия:

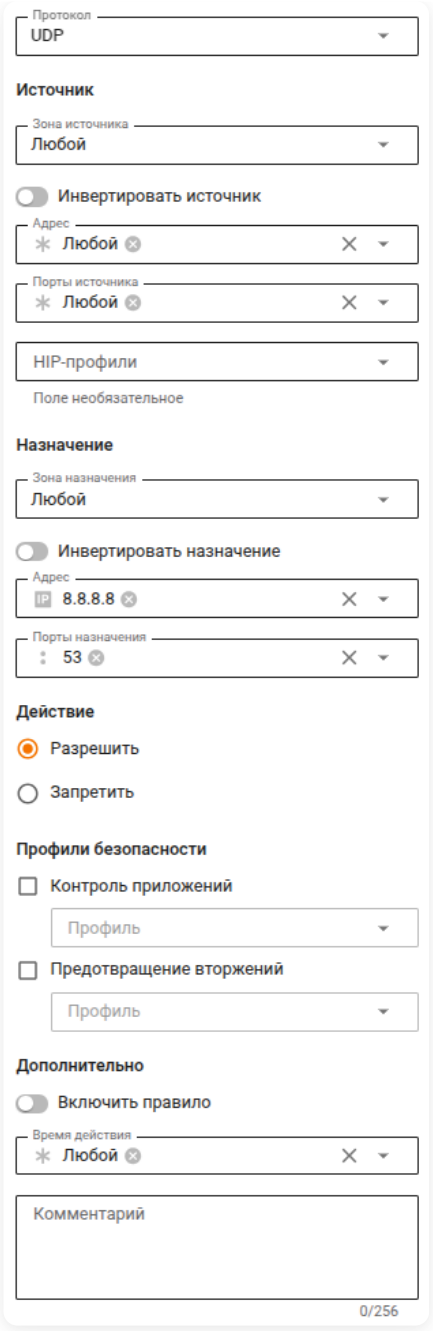
1. На вкладке **Защита и управление DNS** → **Внешние DNS** выключите **Перехват пользовательских DNS-запросов**.

2. Добавьте внешний DNS-сервер.

3. Перейдите на вкладку **Правила трафика** → **Файрвол** → **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.

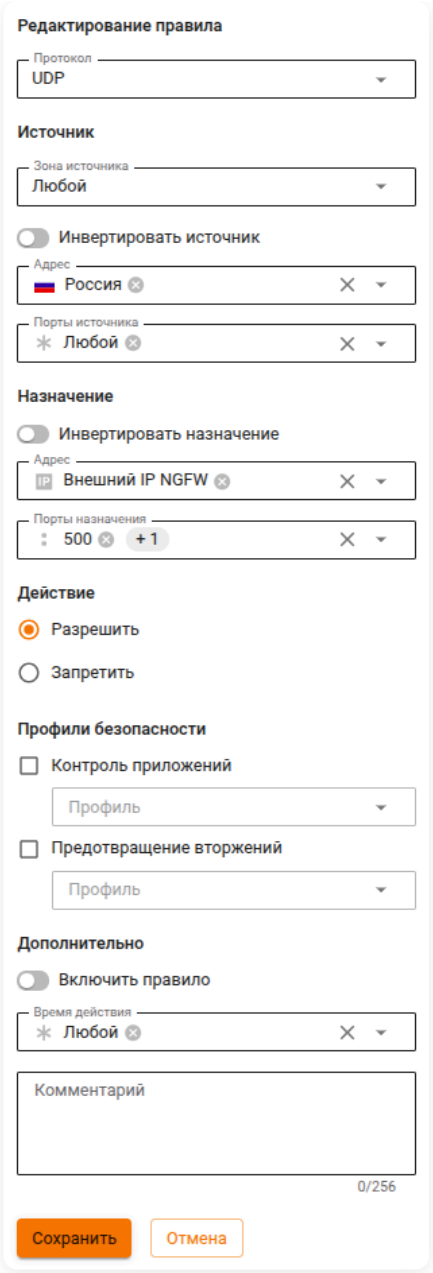
Доступ до Ideco NGFW только из определенной внешней сети по IKEv2/IPsec

Пример: нужно разрешить доступ до Ideco NGFW из России по VPN через IKEv2/IPsec.

ВАЖНО: Правило актуально, если на вкладке **INPUT** есть правило **Запретить все**.

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **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.
  - **Порт назначения** - укажите порты 500 и 4500.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

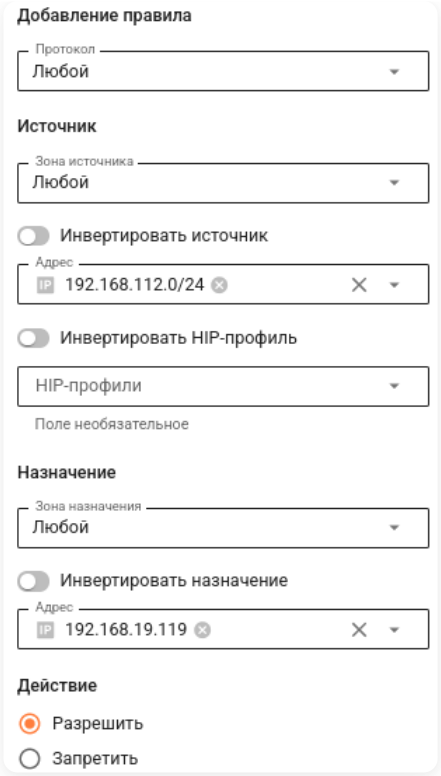
Разрешение доступа к конкретным ресурсам при наличии запрещающего весь трафик правила

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 на вкладку **Правила трафика → Файрвол → DNAT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:

- **5.120.1.25** - IP-адрес Ideco NGFW 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.

Логирование

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 Файрвола. 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 **Файрвола**: 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 раздел **Отчеты и журналы → Журнал трафика.

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 трафика** 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 трафика** при срабатывании правила **Файрвола**.

Действие **Не логировать** позволяет снять метку логирования.

Пример 1. Настройка логирования всего трафика на yandex.ru, кроме трафика от Иванова Ивана

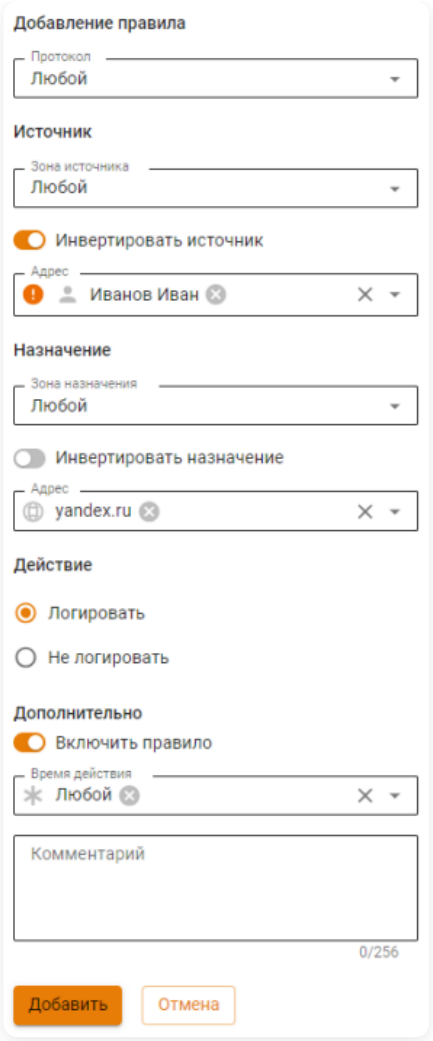
Настройте правило:

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:



Тестирование правил

На вкладке создаются тесты для проверки работы правил таблицы FORWARD и INPUT.

Тест - это конкретный пример, в котором проверяется доступ до определенного IP-адреса с учетом правил таблицы **Файрвола**. Во время тестирования NGFW генерирует тестовый пакет с заданным источником и назначением, после чего проверяет, как пакет проходит через **Файрвол**.

Рекомендуем использовать для источника порты из диапазона 49152 - 65535 (динамически выделяемые или частные порты, которые не регистрируются IANA).

Создание тестов

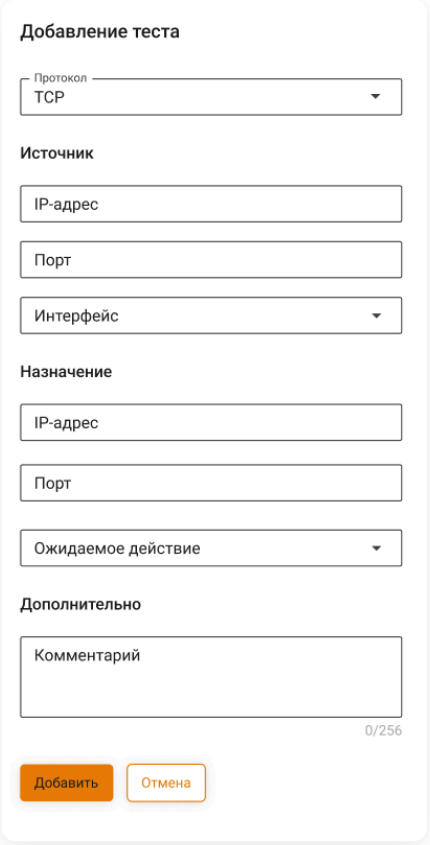
В качестве интерфейса источника можно выбрать:

- Туннельный (GRE).
- Локальный Ethernet.
- Внешний Ethernet.
- Внешний Ethernet + PPTP.
- Внешний Ethernet + L2TP.
- Внешний Ethernet + PPPoE.

Для создания теста выполните действия:

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **Тестирование правил** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Протокол** (**TCP**/**UDP**).
- **IP-адрес** - адрес источника и назначения.
- **Порт** - порт источника и назначения.

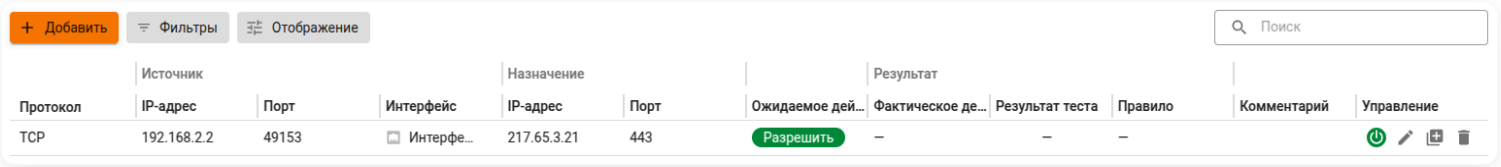
- **Интерфейс** - сетевой интерфейс источника.

> Выбранный интерфейс должен быть настроен и подключен. Если интерфейс отключен, Ideco NGFW не сможет выполнить тестирование.

- **Ожидаемое действие** - Разрешить или Запретить.
- **Комментарий** - необязательное поле.

3. Нажмите **Добавить**.

Созданные тесты добавляются в таблицу:



Запуск и результат тестирования

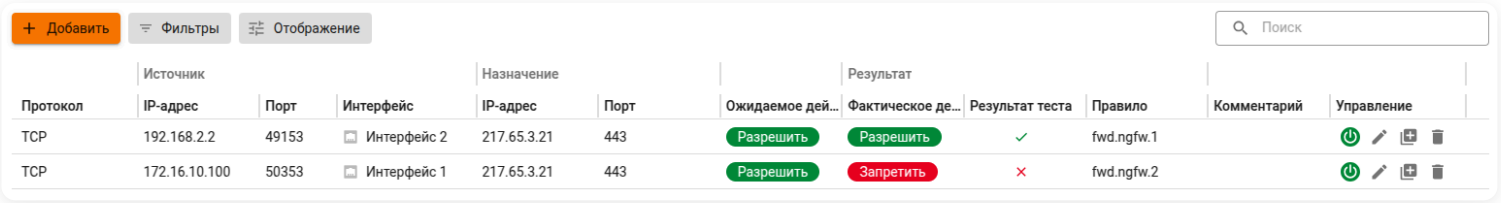
Запуск теста не происходит автоматически при его добавлении. Для запуска:

1. Включите нужный тест .

2. Нажмите **Запустить тестирование** в левом нижнем углу вкладки.

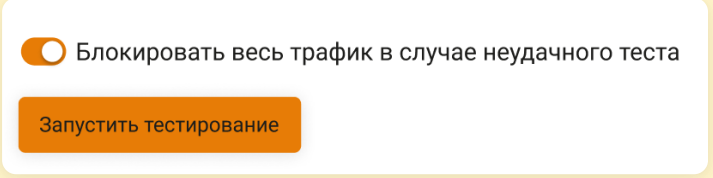
> Если тест выключен, то его тестирование запускаться не будет.

При совпадении ожидаемого и фактического действия тестирование считается успешным:

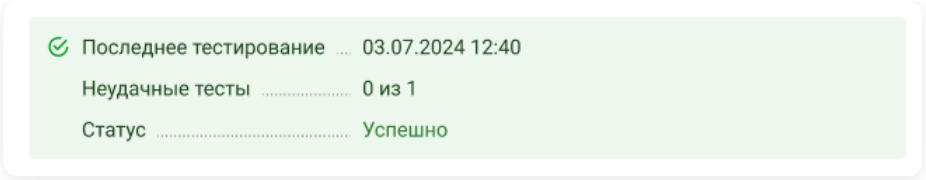


Залогированные правила вида `fwd.sys.xxx`, `inp.sys.xxx`, `out.sys.xxx` в столбце **Правило** - результат срабатывания системного правила, которое разрешило или запретило прохождение трафика в рамках проверки, если не сработало ни одно пользовательское правило. Это правила **Файрвола**, которыми нельзя управлять из веб-интерфейса Ideco NGFW, они всегда включены. Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Файрвола**. Посмотреть системное правило, которое сработало, можно через Терминал.

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 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.

Предварительная фильтрация

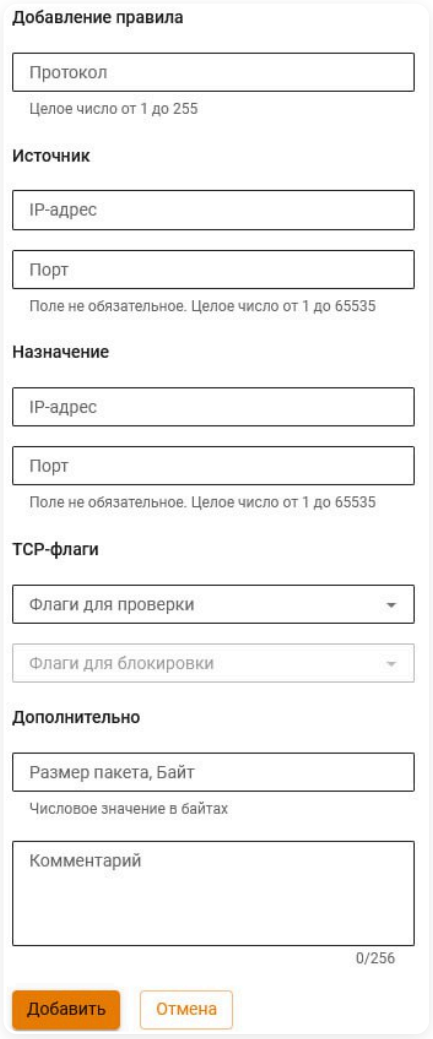
Вкладка **Предварительная фильтрация** позволяет заблокировать весь трафик, попадающий под условия таблицы, до просмотра таблиц **Файрвола** (например, **FORWARD** или **INPUT**). Используйте этот раздел, если требуется фильтрация пакетов на уровне TCP/IP.

Включение хотя бы одного правила **Предварительной фильтрации** может привести к снижению сетевой производительности NGFW примерно на 20%.
При выключении правила производительность сразу восстановится.

Создание правил

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **Предварительная фильтрация** и нажмите **Добавить**.

2. Заполните поля правила:



Расшифрока 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 он 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 **Разрешить интернет всем**.

Аппаратная фильтрация

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 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.

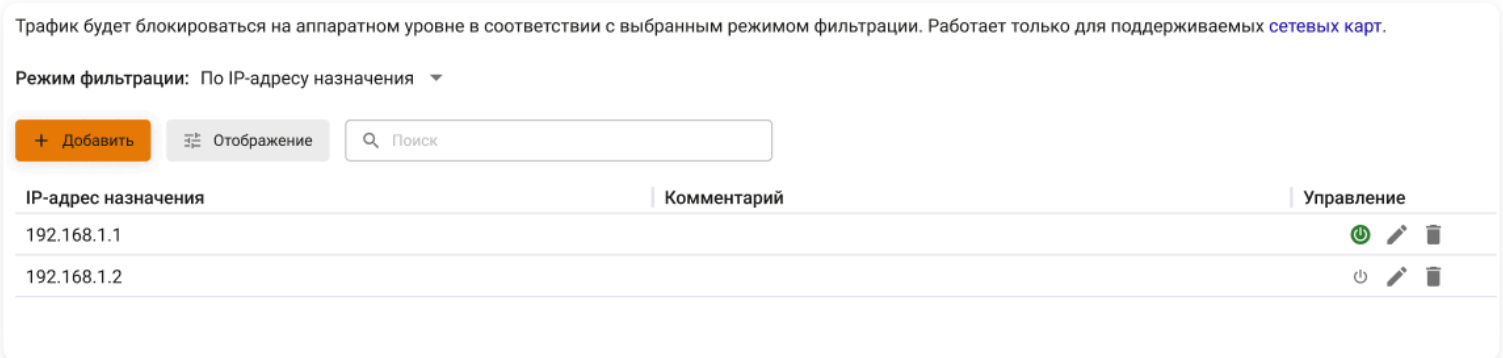
Список поддерживаемых сетевых карт

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

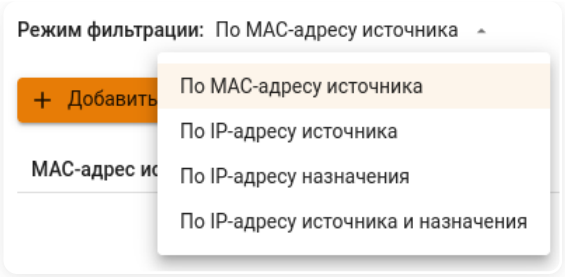
Администратор может создать не более 2500 правил каждого типа фильтрации.

Созданные правила отображаются в таблице в зависимости от выбранного режима фильтрации:



Чтобы создать правило определенного типа, выполните действия:

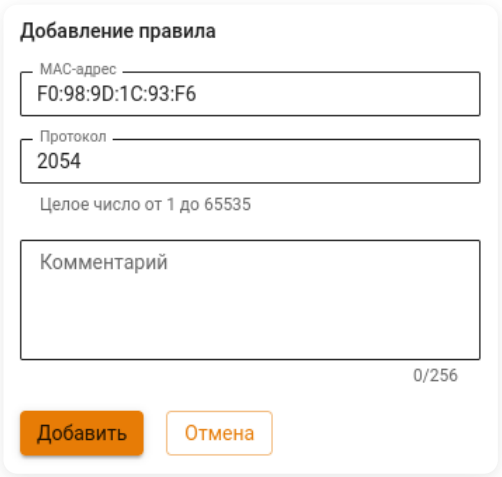
1. Выберите режим фильтрации, нажмав на кнопку в левом верхнем углу:



- По MAC-адресу источника;
- По IP-адресу источника;
- По IP-адресу назначения;
- По IP-адресу источника и назначения.

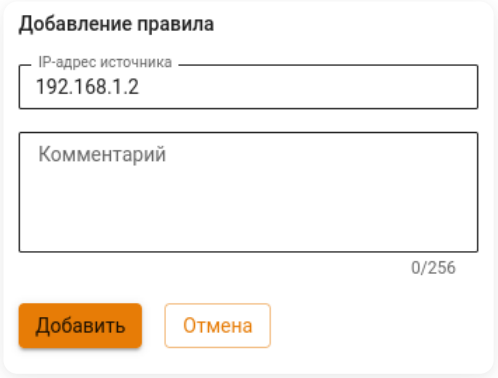
2. Нажмите **Добавить** и заполните поля:

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*;
- **Коментарий** - поле необязательное.

Фильтрация по IP-адресу источника

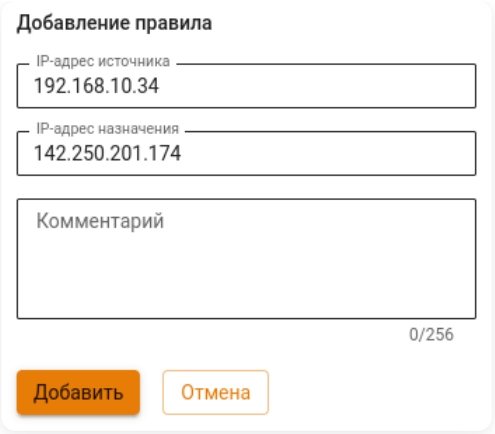


- **IP-адрес источника** - введите IP-адрес источника трафика;
- **Коментарий** - поле необязательное.

Фильтрация по IP-адресу назначения

- IP-адрес назначения - введите IP-адрес назначения трафика;
- Коментарий - 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;
- **Коментарий** - поле необязательное.

3. Нажмите **Добавить**.

4. Включите правило или оставьте его выключенным.

Отключить аппаратную фильтрацию можно, выключив опцию **Файрвол** в соответствующем разделе.

Контент-фильтр

Название службы раздела **Контент-фильтра**: `ideco-content-filter-backend`.

Список имен служб для других разделов доступен по ссылке.

Контент-фильтр проверяет запрашиваемые сайты в базе URL-адресов из пользовательских категорий Ideco NGFW. 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 Файрвол.

Контент-фильтр включает четыре вкладки:

- Правила - создание и управление правилами фильтрации.
- Пользовательские категории - управление собственных списков.
- 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 поставьте флаг **Включить логирование** на вкладке **Сервисы → Прокси → Основное**.

Для изменения страницы блокировки **Контент-фильтра** обратитесь в Техническую поддержку.

Полезные ссылки

- Файрвол
- Настройка фильтрации HTTPS
- Блокировка чат-ботов

- Техническая поддержка

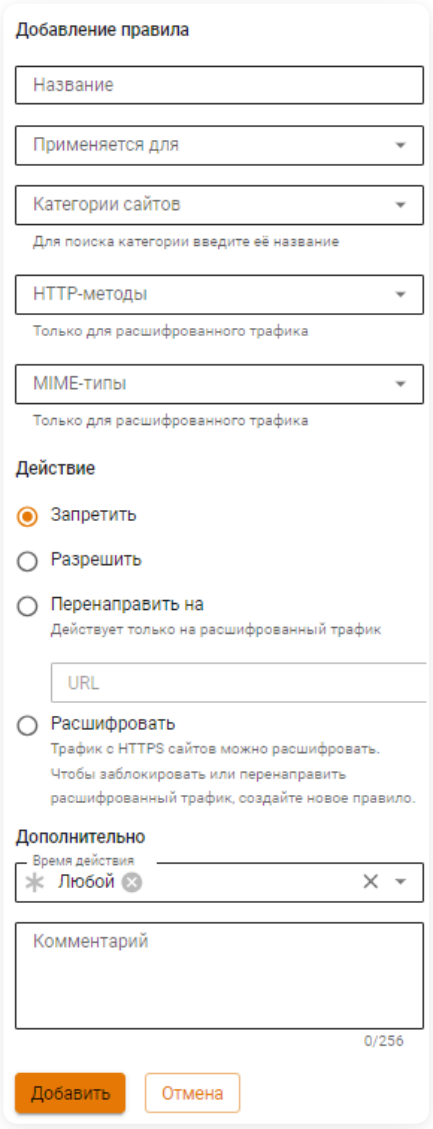
Правила

Правила создаются на вкладке **Правила трафика → Контент-фильтр → Правила**. Помимо возможности добавления правил **Контент-фильтра**, вкладка содержит:

- **Строку поиска категории URL для категоризации**. Позволяет найти, к какой категории относится URL для создания правила.
- **Таблицу созданных правил**. Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. Таким образом, если вышестоящим правилом будет разрешен какой-то ресурс для определенной группы пользователей, то правила ниже применяться не будут. Можно создавать гибкие настройки фильтрации, исключая нужных пользователей вышестоящими правилами из правил блокировки. Аналогичным образом действуют правила расшифровки HTTPS.

Создание правил

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



Расшифровка полей

- **Название** - название добавляемого правила.
- **Применяется для** - пользователь или группа пользователей, IP-адреса или список IP-объектов, для которых применяется правило.
- **Категории сайтов** - поле для выбора предустановленной или пользовательской категории, перечень ресурсов, на которые распространяется действие правила.

Для расшифрованного трафика при создании и редактировании правила **Контент-фильтра** доступны более детальные настройки доступа к ресурсам с помощью HTTP-методов запроса и MIME-типов. Если поля остаются пустыми, проверка по ним не осуществляется.

- **HTTP-методы** - методы запроса, которые будут применяться для всего HTTP- или HTTPS-трафика. Используются для более точной фильтрации трафика, например, для ограничения скачивание чего-либо на сайтах, заполнение 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.
- **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.
- **Действия**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
  - **Перенаправить на** - позволяет указать URL, на который будет перенаправлен расшифрованный трафик.
  - **Расшифровать** - расшифровывает трафик с HTTPS сайтов.

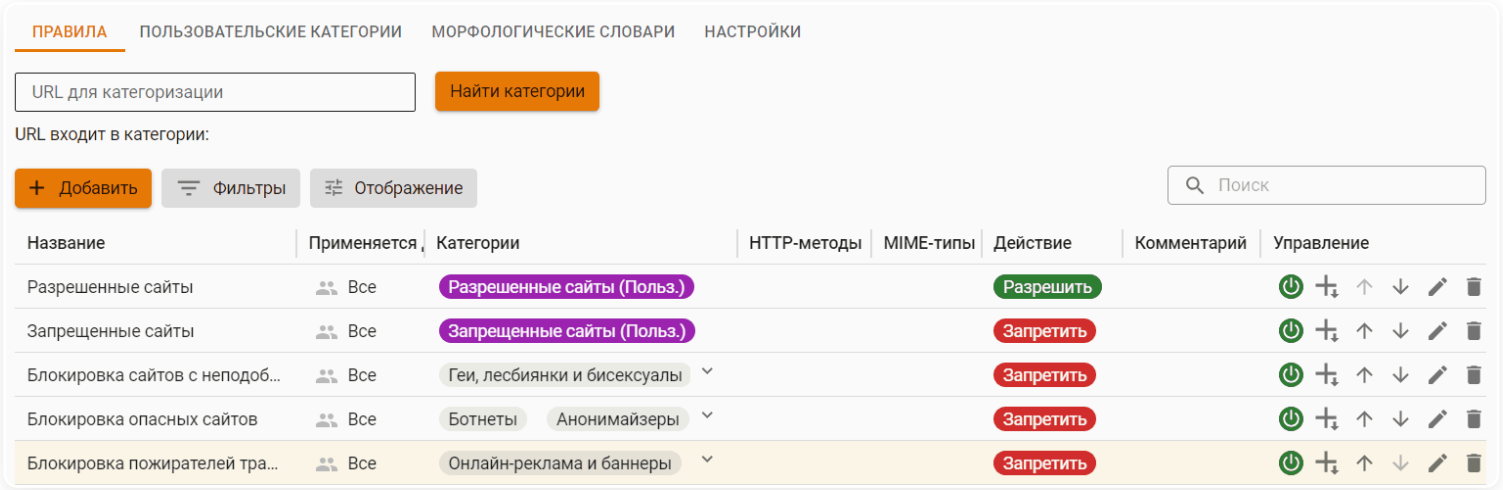
Если выбрать действие **Перенаправить на**, то нужно создать аналогичное правило с действием **Расшифровать** и поместить его выше перенаправляющего правила.

- **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**.

Управление правилами

В столбце **Управление** можно включать или выключать правило, менять его приоритет, редактировать и удалять. Правила контентной фильтрации применяются сразу после создания или включения:



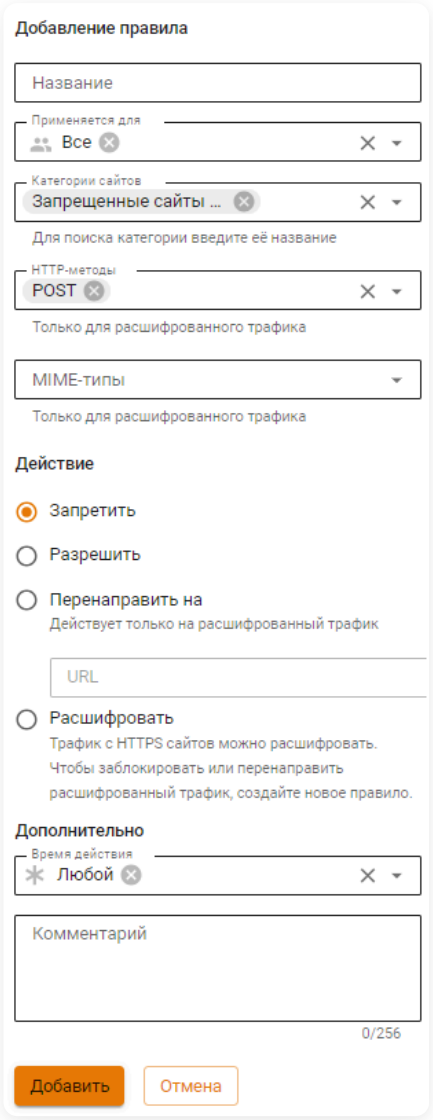
При наличии большого количества правил **Контент-фильтра** в таблице воспользуйтесь кнопкой **Фильтры**.

Дополнительно

Пример настройки HTTP-метода

Необходимо запретить пользователям вводить данные на запрещенных сайтах.

Перейдите в раздел **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**. Заполните поля:



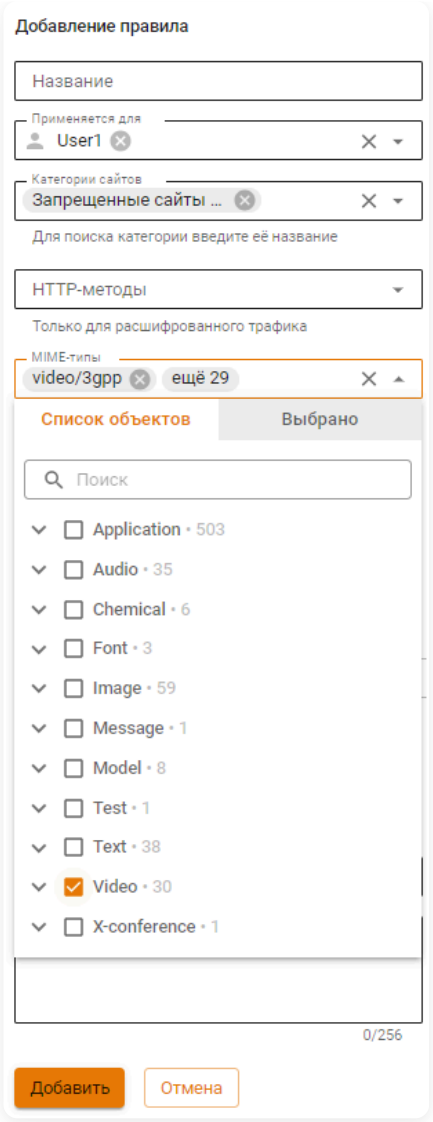
- **Применяется для** - выберите пользователей, для которых будет работать правило.
- **Категории сайтов** - выберите категорию сайтов, для которых должно работать правило, например, **Запрещенные сайты**.
- **HTTP-методы** - выберите метод `POST`, чтобы запретить отправку данных на определенный ресурс.
- 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).

Пример настройки MIME-типов

Необходимо запретить конкретному пользователю (например, User1) воспроизводить видеоконтент на запрещенных сайтах.

Перейдите в раздел **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**. Заполните поля:

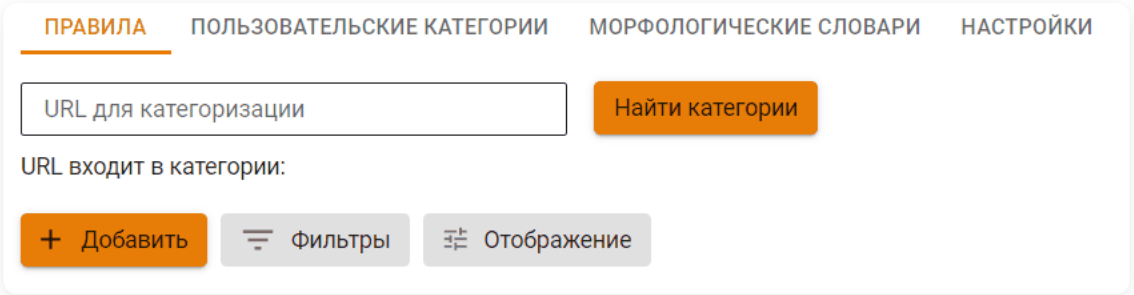


В поле **Категории сайтов** укажите предварительно созданную пользовательскую категорию **Запрещенные сайты**. В поле **MIME-типы** выберите все форматы группы **Video**. Примените действие правила **Запретить**. При сохранении правила сайт откроется, если трафик не заблокирован другим правилом, но видеоконтент не воспроизведется.

Диагностика

Если правила контентной фильтрации не действуют, проверьте следующие параметры в настройках:

- IP-адрес компьютера пользователя должен соответствовать его адресу в авторизации (раздел **Мониторинг - Сессии пользователей**), пользователь должен находиться в нужной группе, на которую назначено правило.
- IP-адрес пользователя и ресурса, к которому обращается, не должен входить в исключения прокси-сервера.
- Проверьте правильность категоризации ресурса, к которому обращаетесь, в поле **URL для категоризации** на вкладке **Правила**:



- В браузере и на компьютере пользователя не используются функции или плагины VPN, не прописаны сторонние прокси-серверы.

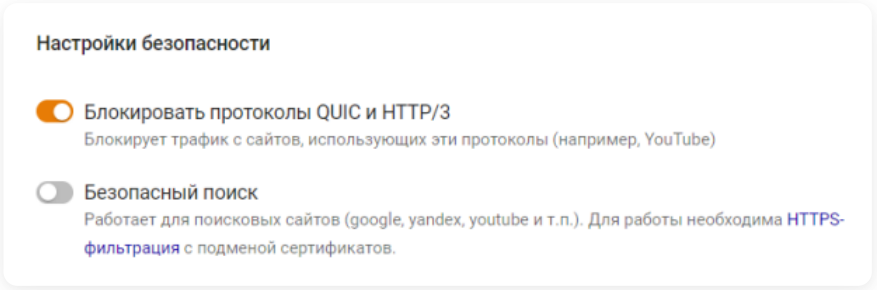
Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

Блокировка загрузки файлов в файлообменники

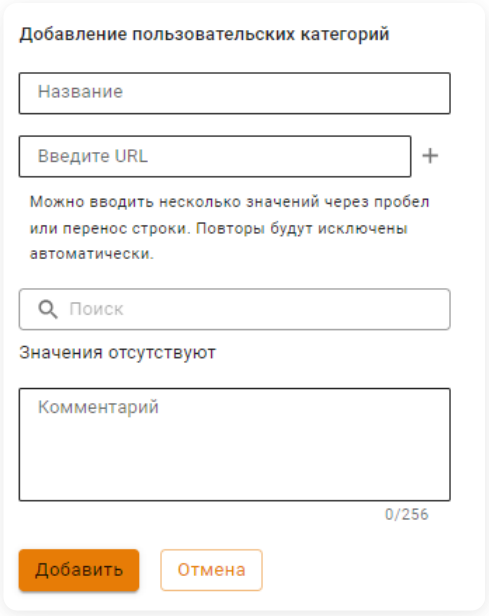
Блокирование этой категории требует особой настройки правил **Контент-фильтра**. В случае с файлообменниками расшифровки трафика может быть недостаточно у категорий: **Файлообменники, Файловые хранилища, Файловые архивы** и **Загрузка файлов в файлообменники**.

Чтобы заблокировать загрузку файлов в облака через браузер, выполните действия:

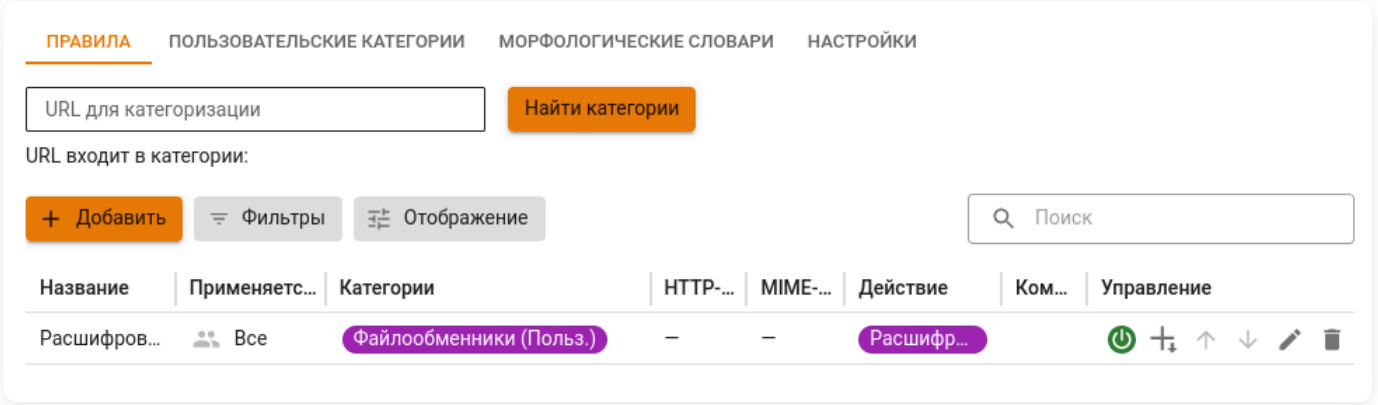
1. Включите **Блокировку протоколов Quic/HTTP3** на вкладке **Контент-фильтр** → **Настройки**:



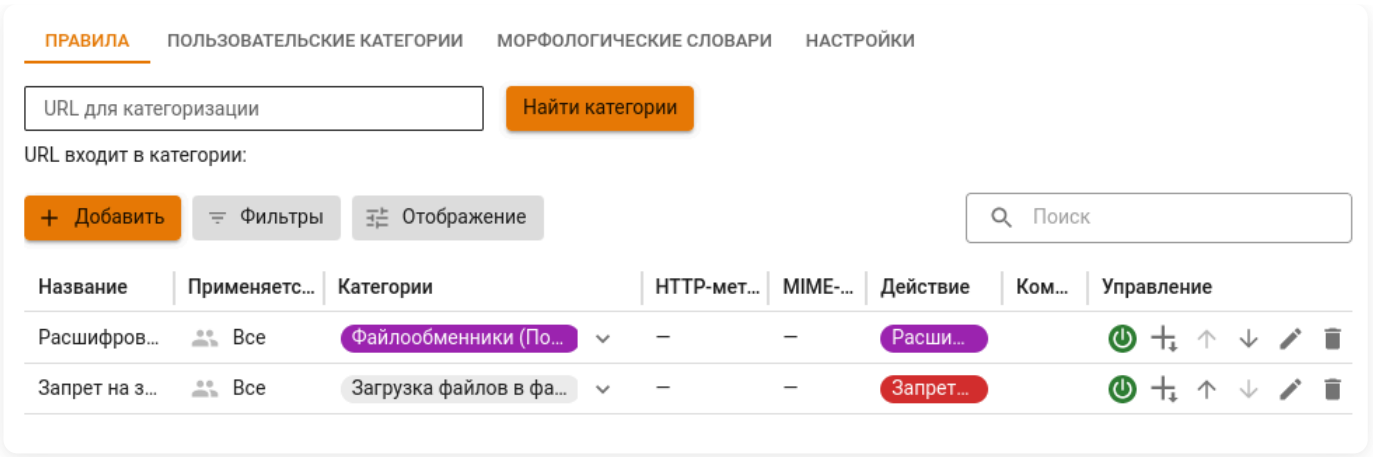
2. Создайте пользовательскую категорию для расшифровки трафика и укажите домены нужных файлообменников, используя маску `example.com`:



3. Создайте правило, расшифровывающее трафик созданной в п. 2 категории:



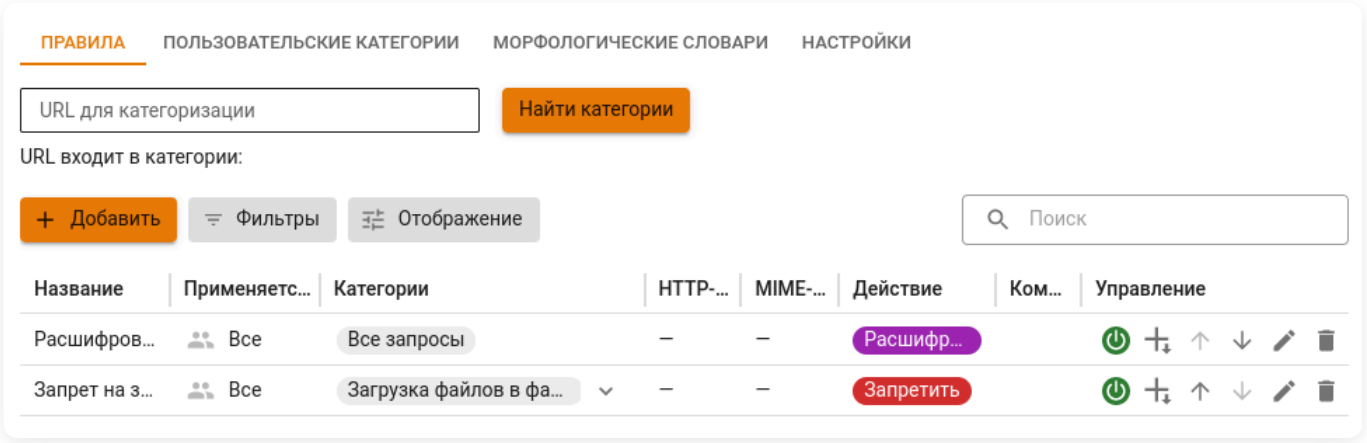
4. Ниже создайте запрещающее правило для категории **Загрузка файлов в файлообменник**:



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.

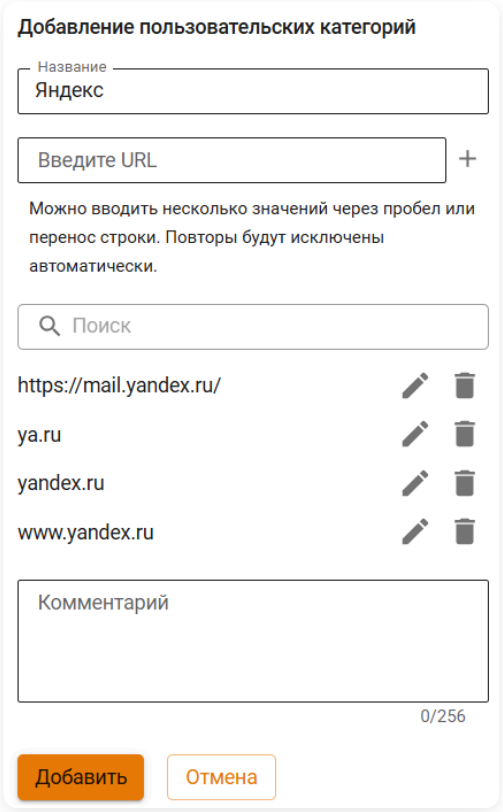
Описание категорий Контент-фильтра

В Ideco NGFW категории сайтов разделены на следующие виды:

- **Пользовательские** - категории, созданные на вкладке **Пользовательские категории**.
- **Специальные** - системные категории для фильтрации запросов.
- **Расширенные** - автоматически пополняемые списки сайтов, отсортированные по темам.
- **Файлы** - восемь сформированных категорий файлов, блокируемых по расширениям и MIME-типами. Предустановленные группы файлов (Исполняемые файлы, Архивы, Видеофайлы, Аудиофайлы, Flash-видео, Active-X, Torrent-файлы, Документы) нельзя редактировать. Для фильтрации HTTPS-трафика по категории файлов требуется настроить 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 его включить достаточно указать домен test.ru (все его поддомены также попадут под это правило).

Если URL или домен содержит специальные символы (。 или •), оставьте их в исходном виде. Адрес будут автоматически закодирован в

формат punycode.

- **Поиск** - поле поиска добавленных URL.
- **Комментарий** - можно заполнить или оставить пустым.

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) в 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

База URL-адресов, отсортированных по тематикам. Для обновления расширенных категорий включите опцию **Расширенная база категорий** на вкладке **Настройки**.

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
Юмор	Юмористические и развлекательные сайты

В версии 20 Ideco NGFW состав категорий контент-фильтра изменен. Часть категорий удалены, часть объединены в общие категории.

При переходе Ideco NGFW с версии 19 на 20 в правилах применятся новые категории в соответствии с таблицей **Изменение категорий**. Если в версии 20 нужная категория отсутствует, то поле **Категории сайтов** останется пустым, а правило перестанет работать.

Категории без изменений

- Войска и вооружения
- Знакомства
- ИИ Чат-боты
- Интернет-магазины
- Искусство
- Казино, лотереи, тотализаторы
- Компьютерные игры
- Наркотики
- Недвижимость
- Неизвестные сайты
- Некоммерческие организации
- Образование и учебные учреждения
- Онлайн-реклама и баннеры
- Платные сайты мобильных операторов
- Поисковые системы
- Правительство
- Сайты для детей
- Социальные сети
- Спорт
- Туризм
- Форумы
- Фотогалереи
- Юмор

Удаленные категории

- Взлом.
- Высокий уровень риска
- Криминальные навыки/хакинг
- Оплата за серфинг
- Пиратство и хищение авторских прав
- Природа и ее сохранение
- Системы централизованной аутентификации
- Страхование
- Частные IP-адреса

Изменение категорий

v19	v20
Web-почта	Веб-почта
Аборты	Здоровье и здравоохранение

v19	v20
Аборты - одобрение	Здоровье и здравоохранение
Аборты - осуждение	Здоровье и здравоохранение
Автомобили/Транспорт	Автомобили и транспорт
Алкоголь	Алкоголь и табак
Анонимайзеры	Прокси и анонимайзеры
Архитектура	Наука и технологии
Астрология и гороскопы	Астрология
Атеизм и агностицизм	Религия и атеизм
Аудио для прослушивания и скачивания	Радио и музыка онлайн
Аукционы и рынки	Торговля и покупки
Банки	Финансы и финансовые учреждения
Безопасность	Порталы
Бизнес и услуги (общая)	Бизнес, экономика, маркетинг
Бизнес/Сервисы	Бизнес, экономика, маркетинг
Биотехнологии	Наука и технологии
Благотворительные учреждения	Некоммерческие организации
Ботнеты	Сети зараженных устройств и управляющие серверы
Веб-хостинг, интернет-провайдеры и телекоммуникационные компании	Компьютеры и Интернет
Видео для прослушивания и скачивания	Фильмы и видео онлайн
Виртуальные открытки	Досуг и развлечения
Возможный риск	Неизвестные сайты
Вооруженные силы	Войска и вооружения
Геи, лесбиянки и бисексуалы	Сайты для взрослых
Готовые домашние задания	Плагиат и рефераты
Для взрослых	Сайты для взрослых
Дом, сад и семья	Дом, семья, хобби
Дом/Отдых	Дом, семья, хобби
Дома престарелых и уход за больными	Здоровье и здравоохранение
Домашние животные	Дом, семья, хобби
Доставка и логистика	Бизнес, экономика, маркетинг
Еда и рестораны	Досуг и развлечения
Законодательство и политика	Политика, общество, закон
Запаркованные	Неиспользуемые домены
Здоровье	Здоровье и здравоохранение
Здравоохранение и медицина	Здоровье и здравоохранение
Игрушки	Торговля и покупки
Изображения жестокого обращения с детьми	Сексуальное насилие над детьми (Arachnid)
Интернет и IP-телефония	Компьютеры и Интернет
Информационная безопасность	Компьютеры и Интернет
Каталоги	Порталы
Компьютеры и технологии	Компьютеры и Интернет
Конкурсы и опросы	Досуг и развлечения
Контент серверы	Content Delivery Networks
Криминальные навыки	Агрессия, расизм, терроризм
Купальные костюмы	Торговля и покупки
Купоны	Досуг и развлечения
Литература и книги	Интернет-библиотеки
Марихуана	Наркотики

v19	v20
Маркетинговые услуги	Торговля и покупки
Мгновенные сообщения	Чаты и мессенджеры
Мебель для дома и офиса	Торговля и покупки
Мобильные телефоны	Компьютеры и Интернет
Мода и красота	Досуг и развлечения
Музыка	Радио и музыка онлайн
Мультфильмы, аниме и комиксы	Аниме
Насилие	Агрессия, расизм, терроризм
Не для детского просмотра	Сайты для взрослых
Недоступные	Неизвестные сайты
Неизвестный уровень риска	Неизвестные сайты
Нераспознаваемый контент	Неизвестные сайты
Нетрадиционные религии и оккультные верования	Религия и атеизм
Новости	Новости и СМИ
Обзоры продукции и Сравнение цен	Порталы
Оборудование, ПО, электроника	Компьютеры и Интернет
Онлайн-офисы	Порталы
Онлайн-торговля акциями	Финансы и финансовые учреждения
Онлайн-управление информацией	Порталы
Откровенные изображения	Сайты для взрослых
Парки, зоны отдыха и спортивные залы	Досуг и развлечения
Переадресация	Запаркованные домены
Переводчики	Образование и учебные учреждения
Персональные страницы	Блоги и персональные сайты
Персональные страницы и блоги	Блоги и персональные сайты
Пиринговые сети	Торренты и P2P-сети
Питание и диеты	Здоровье и здравоохранение
Пищевые добавки и витамины	Здоровье и здравоохранение
Поиск работы	Работа и найм
Поисковики изображений	Поисковые системы
Политика и закон	Политика, общество, закон
Порнография	Порнография и секс
Порнография/секс	Порнография и секс
Порталы	Порталы
Производство	Наука и технологии
Профессиональные сообщества	Форумы
Развлекательные места и события	Туризм
Развлекательные новости и сайты про знаменитостей	Досуг и развлечения
Развлечения и видео	Категория разделена на две: Фильмы и видео онлайн; Досуг и развлечения
Разное	Неизвестные сайты
Религии	Религия и атеизм
Рестораны	Торговля и покупки
Сайты сообществ	Форумы
Самопомощь и зависимости	Здоровье и здравоохранение
Секс и Эротика	Порнография и секс
Сексуальное воспитание и образование	Сайты для взрослых
Сельское хозяйство	Бизнес, экономика, маркетинг
Сквернословие	Грубость, матершина, непристойность

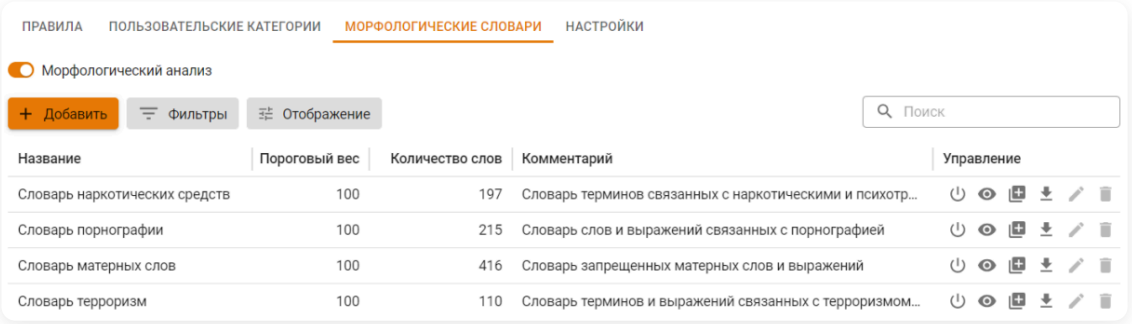
v19	v20
Скомпрометированные	Вредоносное ПО
Сообщества лоббистов и торговые ассоциации	Торговля и покупки
Социальные сообщества	Социальные сети
Спам	Онлайн-реклама и баннеры
Список Минюста	Федеральный список Минюста
Спонсируемые государством	Правительство
Спорт и отдых	Спорт
Спортивная охота	Спорт
Спортивные соревнования	Спорт
Справочные материалы и карты	Порталы
Средний уровень риска	Неизвестные сайты
Табак	Алкоголь и табак
Тайный сбор информации	Вредоносное ПО
Текстовые сообщения	Чаты и мессенджеры
Телевидение и фильмы	Фильмы и видео онлайн
Технологии (в целом)	Наука и технологии
Только для взрослых (18+)	Сайты для взрослых
Торговля и покупки	Интернет-магазины
Торрент-трекеры	Торренты и P2P-сети
Транспортные средства	Автомобили и транспорт
Удаленный доступ	Компьютеры и Интернет
Учебные заведения	Образование и учебные учреждения
Учебные материалы и исследования	Образование и учебные учреждения
Файловые архивы	Категория разделена на две: Фотогалереи; Компьютеры и Интернет
Файловые хранилища	Файловые архивы
Файлообменники	Торренты и P2P-сети
Фармацевтика	Здоровье и здравоохранение
Финансовые инструменты и котировки	Финансы и финансовые учреждения
Финансы	Финансы и финансовые учреждения
Финансы (в целом)	Финансы и финансовые учреждения
Фитнес и Отдых	Досуг и развлечения
Фишинг/мошенничество	Фишинг и поддельные сайты
Хобби и Досуг	Дом, семья, хобби
Центры распространения вредоносного ПО	Вредоносное ПО
Центры управления и контроля	Сети зараженных устройств и управляющие серверы
Чаты	Чаты и мессенджеры
Чаты/Мессенджеры	Чаты и мессенджеры
Шпионские и опасные сайты	Вредоносное ПО
Шпионское и сомнительное ПО	Вредоносное ПО
Экстремизм	Агрессия, расизм, терроризм
Эротика	Сайты для взрослых

При нахождении несоответствия сайта и категории обратитесь в техническую поддержку

Морфологические словари

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 предустановлены четыре словаря (по умолчанию отключены):

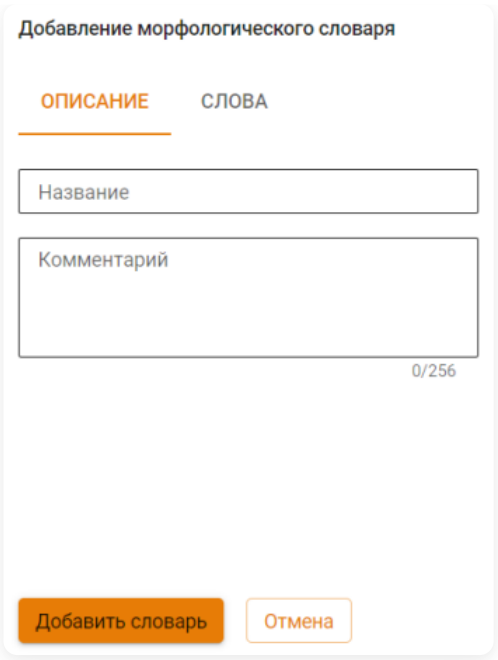
- Словарь наркотических средств
- Словарь порнографии
- Словарь матерных слов
- Словарь терроризм

Предустановленные словари можно включать или отключать, но нельзя редактировать и удалять.

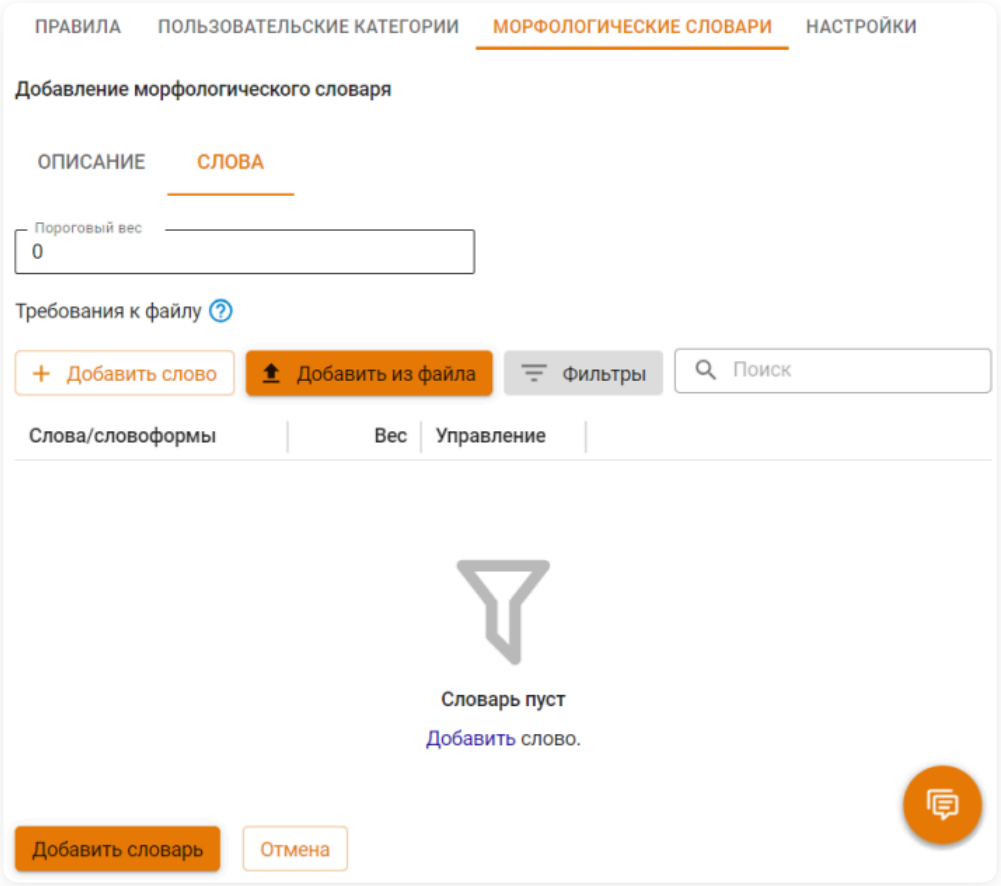
Добавление морфологического словаря

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

- На вкладке **Описание**:
  - **Название** - название добавляемого словаря.
  - **Комментарий** - произвольный текст. Значение не должно быть длиннее 255 символов:



- На вкладке **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:



2. 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.

Чтобы снизить вероятность блокировки сайта из-за морфологического анализа, уменьшите вес слов. Для повышения вероятности блокировки - увеличьте вес.

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/словосочению 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").

3. Для сохранения настроек нажмите **Добавить словарь**.

Если в таблице большое количество морфологических словарей, воспользуйтесь кнопкой **Фильтры**.

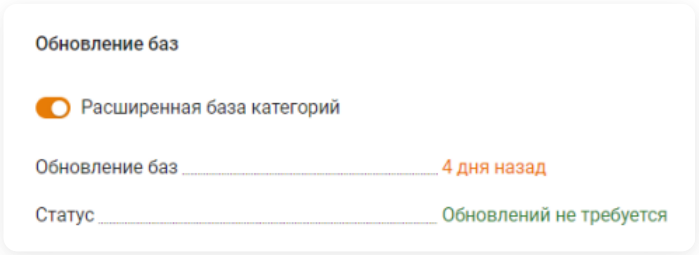
Результат морфологического анализа представлен в разделе **Отчеты и журналы** → **Журнал веб-трафика**:

		Антивирус		Контент-фильтр					
Дата и время	Резу...	Резу...	Анти...	Результат проверки	Расшифровка	Название правила	Причина запрета	Категории сайта	Категория сработки
02.06.2025, 17:12:04	✗	✓	–	✗	✗	–	Словарь порнографии	Все некатегоризирован...	Все некатегоризированные
02.06.2025, 17:12:04	✗	✓	–	✗	✗	–	Словарь порнографии	Все некатегоризирован...	Все некатегоризированные

Настройки

Обновление баз

Активация опции **Расширенная база категорий** включает более 140 автоматически обновляемых категорий, доступных только при активной подписке в платных версиях продукта:



Если отключить опцию **Расширенная база категорий**, то все правила, включающие в себя 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 на вкладке **Прокси** → **Исключения**.

Безопасный поиск - принудительно включает безопасный поиск в поисковых системах (Google, Yandex, YouTube, Yahoo, Bing, Rambler).

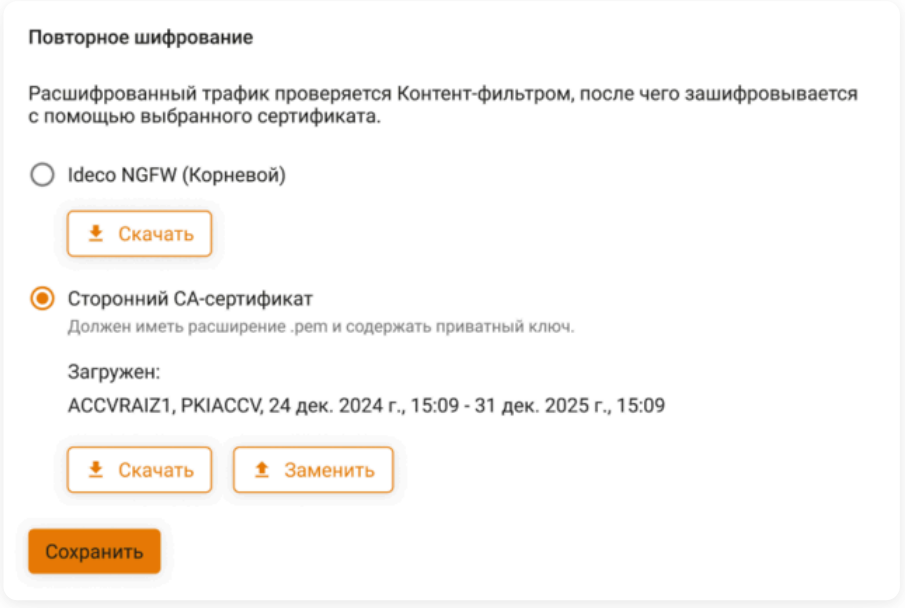
Для корректной работы необходимо включить HTTPS-фильтрацию с подменой сертификата для этих сервисов.

Повторное шифрование

Если для повторного шифрования требуется использовать сторонний сертификат (не корневой сертификат Ideco NGFW):

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 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**. Таким образом, передающийся по защищенному HTTPS-соединению трафик становится доступным для обработки всем модулям Ideco NGFW: антивирусу Касперского, внешним ICAP-сервисам и Контент-фильтру (можно категоризировать полный URL запроса и MIME-тип контента).

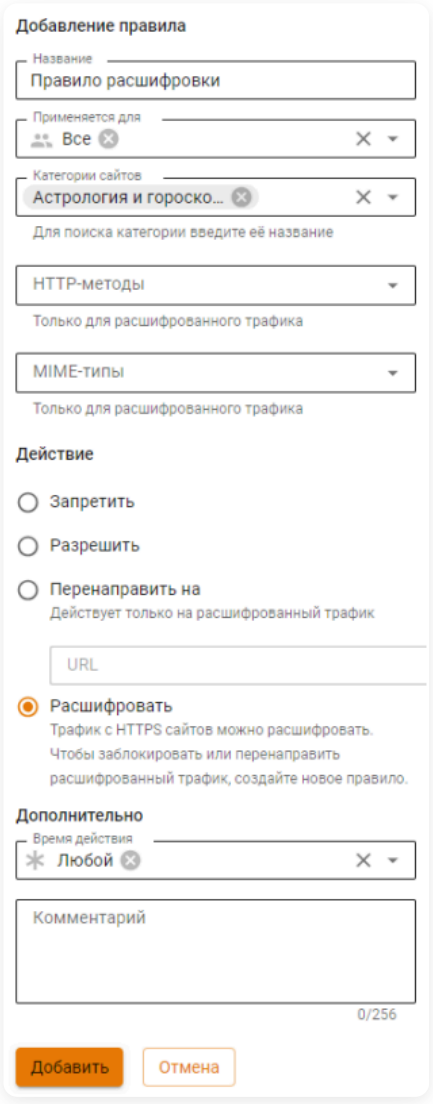
Настройка сервера и рабочих станций

Для работы SSL-bump требуется **настройка на обеих сторонах подключения**: сервера Ideco NGFW и рабочей станции каждого пользователя в локальной сети.

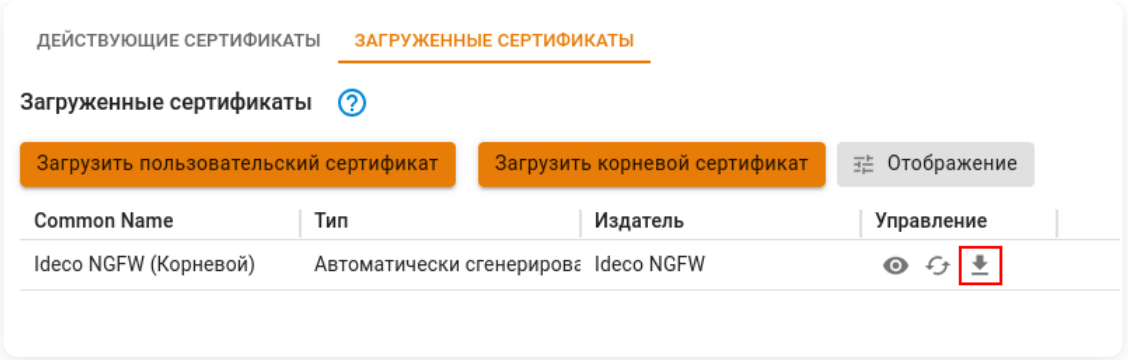
Настройка сервера Ideco NGFW

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 на вкладке **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 в операционной системе.

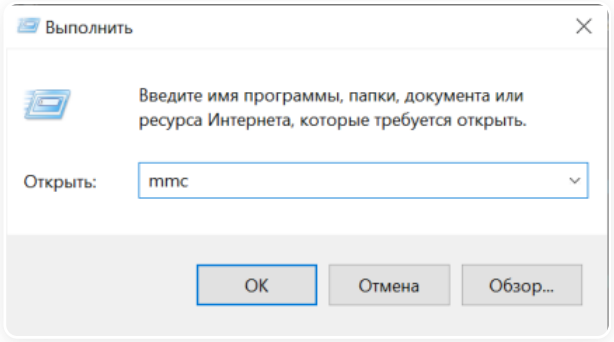
Установка сертификата на Linux

Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

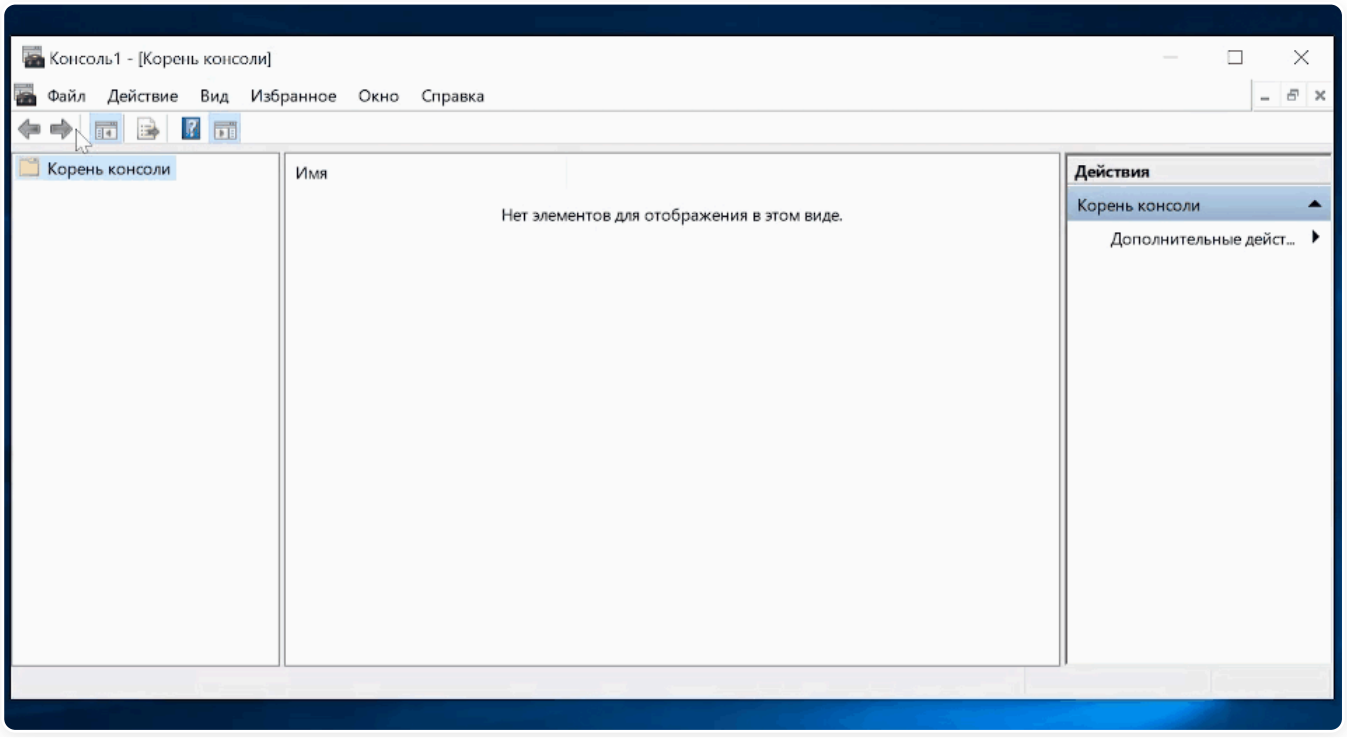
- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

Установка сертификата на Windows

1. Откройте на рабочей станции центр управления сертификатами: **Пуск** → **Выполнить**, выполнив в диалоге команду **mmc**:

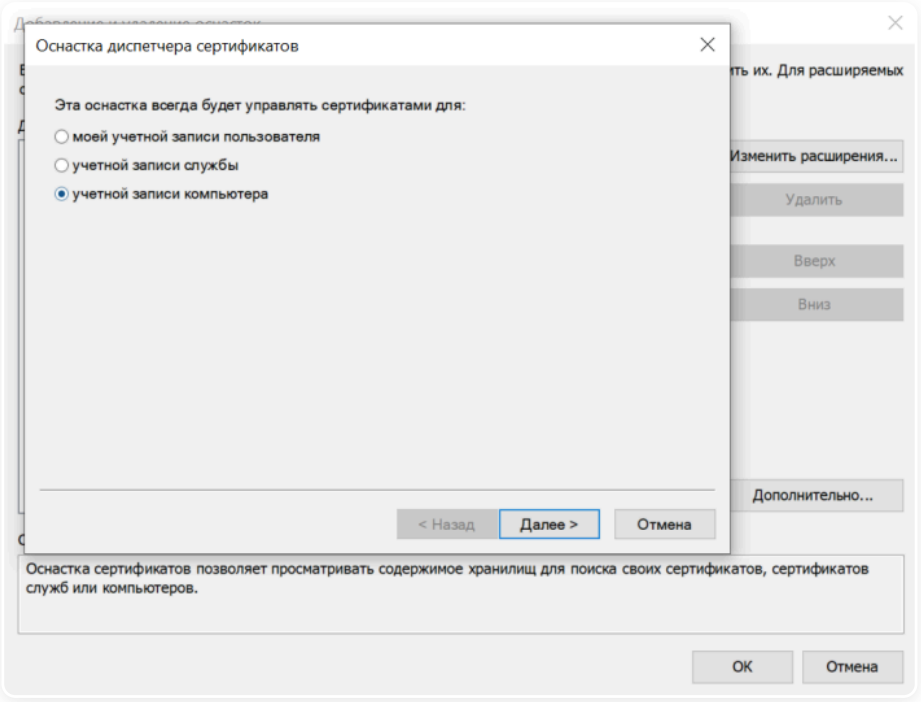


2. В меню **Файл** выберите **Добавить или удалить оснастку**:



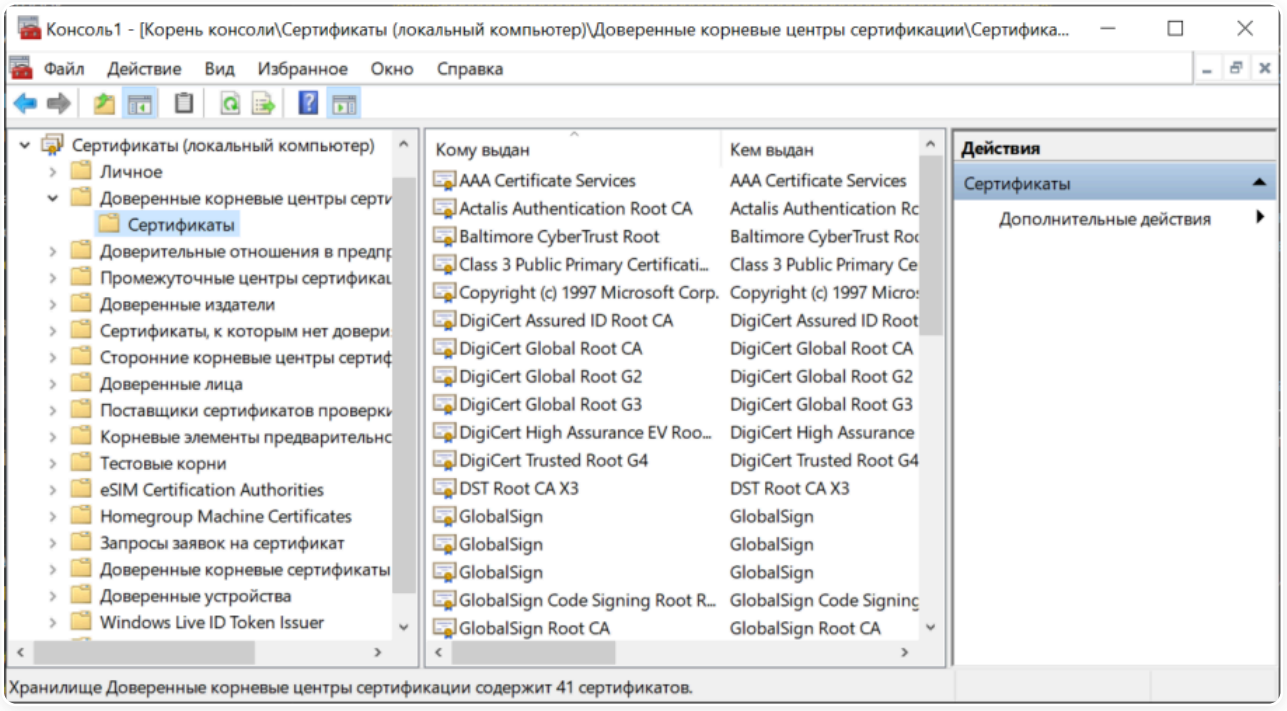
3. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите кнопку **Добавить**:

4. В открывшемся окне выберите пункт **Учетная запись 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. 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 для всех пользователей автоматически с помощью Active Directory. Для этого необходимо выполнить действия:

1. Скачайте корневой SSL-сертификат, открыв раздел веб-интерфейса Ideco NGFW **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



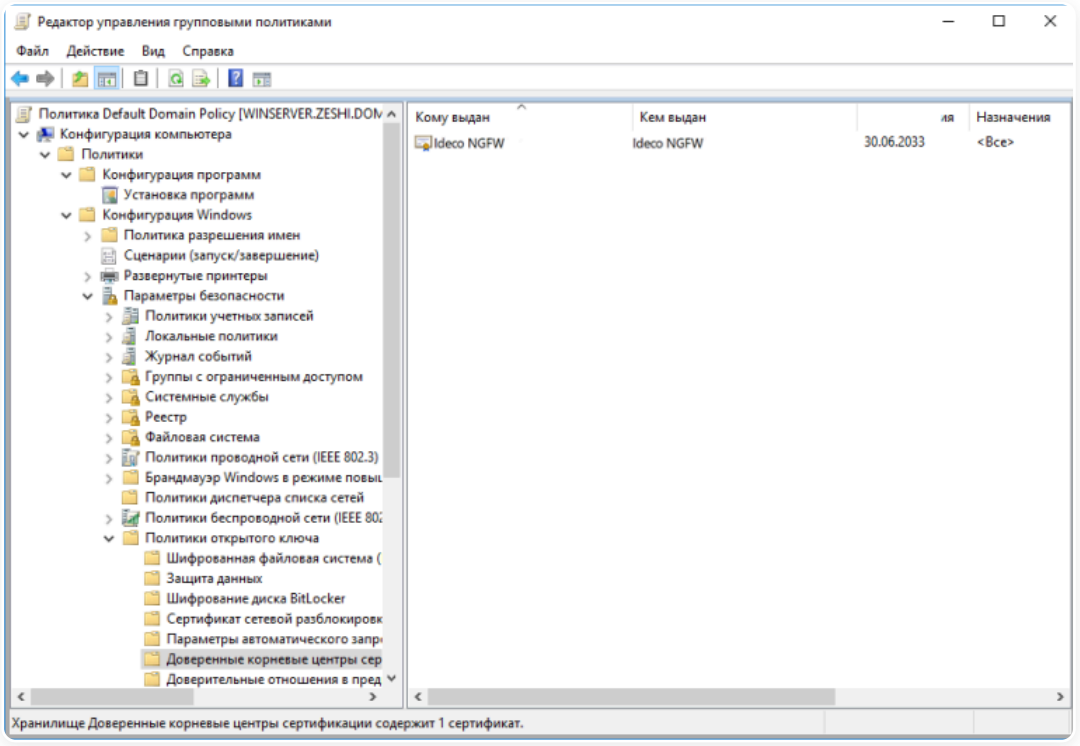
2. Зайдите на контроллер домена с правами администратора.

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.



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. На вкладке **Сервисы** → **Сертификаты** → **Загруженные сертификаты** загрузите сертификат, который будет использоваться для шифрования.

2. Перейдите на вкладку **Правила трафика** → **Контент-фильтр** → **Настройки**.

3. Выберите в пункте **Повторное шифрование** 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

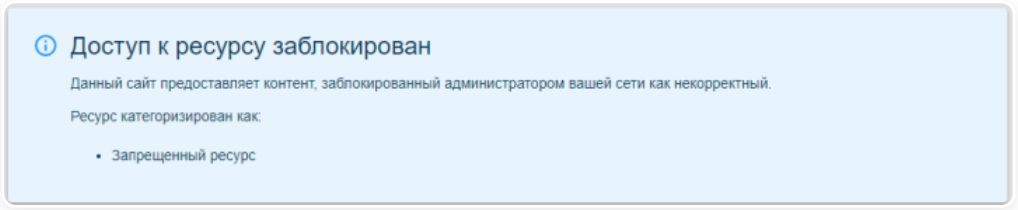
Проблема	Решение
Включения расшифровки трафика может быть недостаточно для подмены сертификата некоторых сайтов (например, `ya.ru`, `google.com`).	Включить опцию **Блокировать протоколы QUIC и HTTP/3** на вкладке **Правила трафика** → **Контент-фильтр** → **Настройки**.
Браузер не использует системное хранилище сертификатов.	1. Добавить сертификат Ideco NGFW 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 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 (даже при включенной только SNI-фильтрации), так как при блокировке HTTPS-ресурса будет применен SSL-bumping с подстановкой SSL-сертификата NGFW для подмены контента ресурса страницей о его 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**

Изменение страницы блокировки Контент-фильтра

Страница блокировки Контент-фильтра по умолчанию содержит уведомление о блокировке доступа к ресурсу и категоризацию:



В процессе обновления Ideco NGFW все ранее настроенные параметры шаблона блокировки могут быть сброшены.

Все внесенные изменения в шаблоны рекомендуется сохранить вне NGFW, чтобы избежать их потери при обновлении. После обновления может потребоваться адаптация шаблонов под новую версию системы.

Для создания персонализированного шаблона страницы выполните действия:

1. Чтобы изменить фавикон, загрузите новый файл в директорию **/usr/share/ideco/vendor/**. Для этого перейдите в раздел **Управление сервером → Администраторы** и убедитесь, что доступ по SSH разрешен. Затем откройте терминал на компьютере и введите следующую 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 компьютере.
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW.
- Файл обязательно должен называться **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 компьютере.
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW.
- Файлы обязательно должны называться **IDECO_ICON_ERROR.svg, IDECO_ICON_INFO.svg, IDECO_ICON_SUCCESS.svg, IDECO_ICON_WARNING.svg**.

3. Отредактируйте CSS-файл, чтобы изменить стили для страниц ошибок. Перейдите в **Управление сервером -> Терминал** и откройте файл **style.css** из директории **/usr/share/ideco/proxy-backend/error_page_templates/** 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 страницу блокировки. Перейдите в директорию **/usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU/error_content/** и откройте файл **ERR_CF_BLOCK_PAGE** в текстовом редакторе:

```
nano /usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU/error_content/ERR_CF_BLOCK_PAGE
```

Пример изменения файла ERR_CF_BLOCK_PAGE

```
<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://telegram.im/@admin">Отправить заявку в Telegram</a></p>
    </div>
  </div>
  <div class="blocked_content">
    <h1>Контент заблокирован</h1>
  </div>
</body>
```

Результат:

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

Название службы раздела *Ограничение скорости*: `ideco-shaper-backend`.

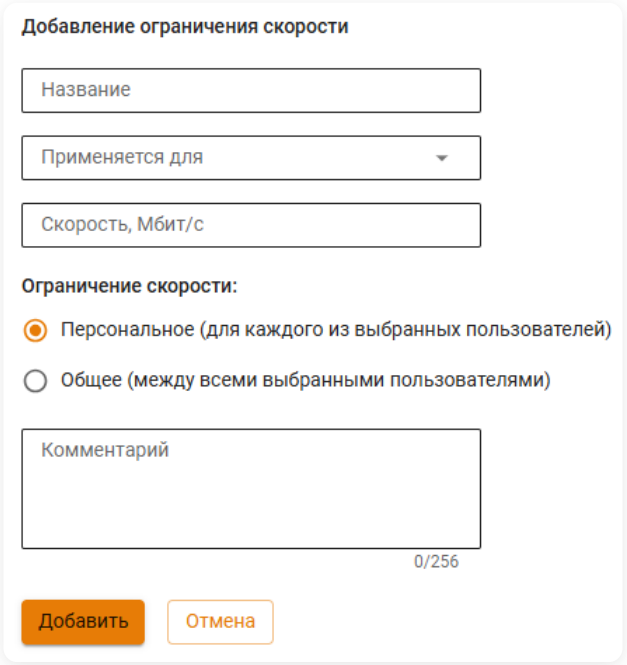
Список имен служб для других разделов, доступен по ссылке.

В разделе **Ограничение скорости** создаются правила, позволяющие ограничить скорость входящего интернет-трафика для пользователей сети.

Для исключения пользователя или групп пользователей из обработки правил **Ограничения скорости** добавьте соответствующее правило в разделе Исключения.

Настройка ограничения скорости

1. Для создания правила в разделе **Правила трафика** → **Ограничение скорости** нажмите **Добавить** и заполните поля:

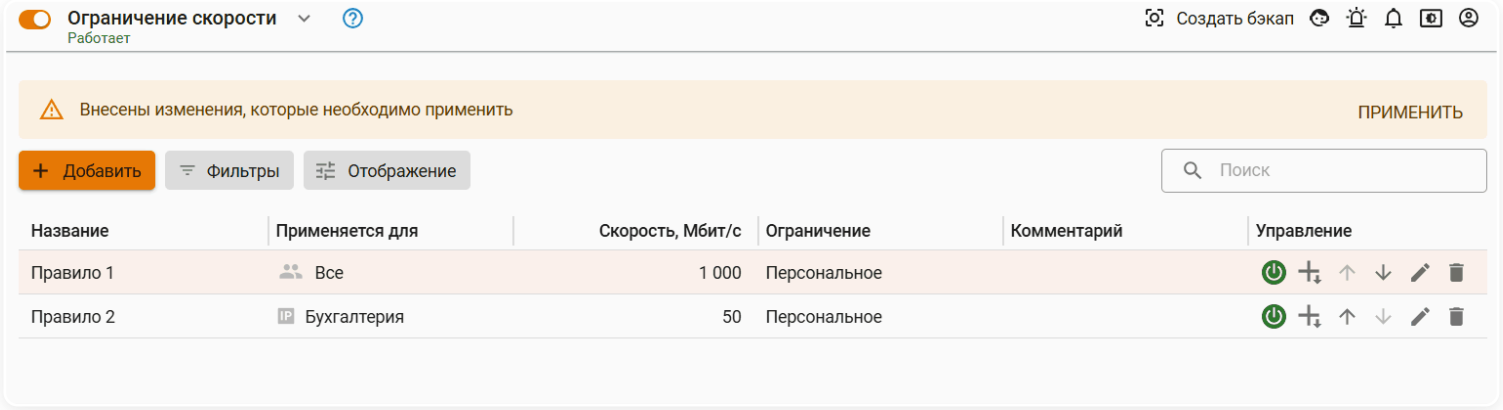


Расшифровка полей

- **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.
  - **Общее** - скорость будет ограничена и разделится между всеми выбранными пользователями.

2. Нажмите **Добавить**.

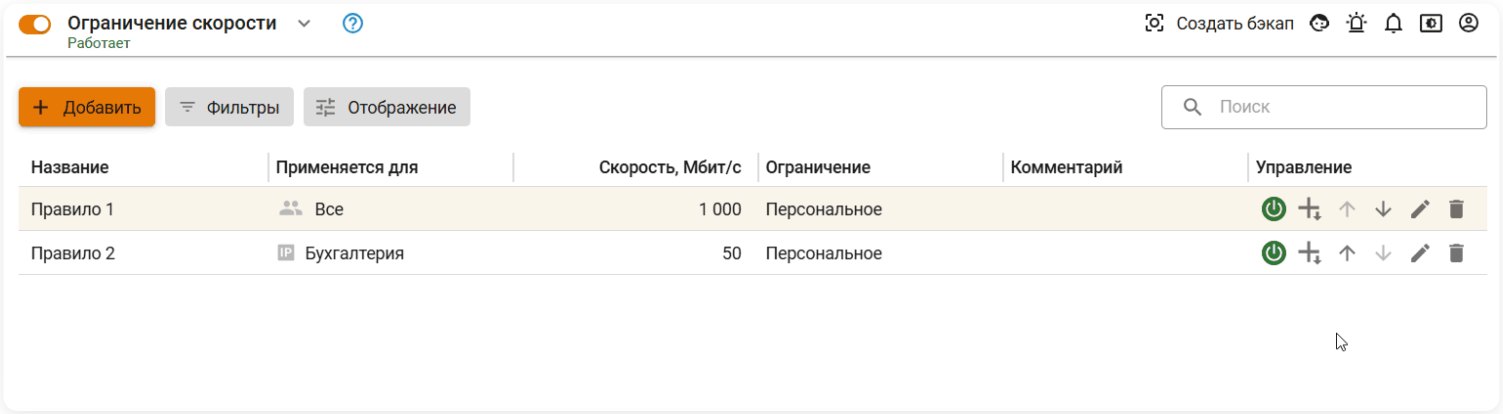
3. Для применения созданного правила нажмите **Применить** над таблицей:



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.

Включить или выключить правило, изменить его приоритет, редактировать или удалить можно кнопками управления в столбце **Управление**:



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.

Примеры использования

Персональное ограничение

При выборе персонального ограничения скорости лимит скорости для каждого менеджера будет равен 1 Мбит/с:

Общее ограничение

При выборе общего ограничения ширина канала для всей бухгалтерии будет равна 10 Мбит/с:

Полезные ссылки

- Исключения
- Объекты
- Учетные записи

Антивирус

Название службы раздела **Антивирус**: `ideco-av-backend`.

Список имен служб для других разделов доступен по ссылке.

Антивирус в продукте создан на базе Kaspersky Anti-Virus Software Development Kit. Антивирус приобретается отдельно от Ideco NGFW, использование может быть ограничено условиями лицензии. Для покупки обратитесь в отдел продаж.

Корпоративные ключи, предназначенные для других продуктов Лаборатории Касперского, не могут быть использованы для активации антивируса.

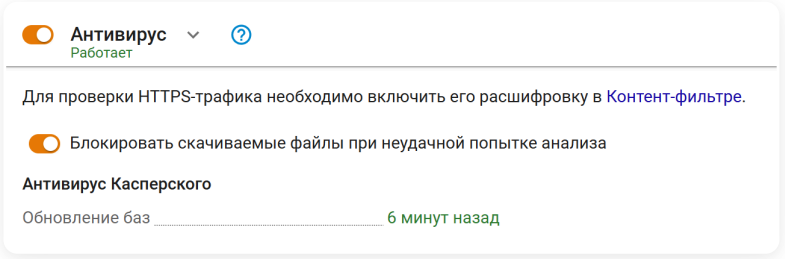
Модуль **Антивирус** связан с прокси-сервером и **Контент-фильтром**, поэтому фильтрует веб-трафик при выполнении следующих условий:

- **Включена расшифровка трафика.** В разделе **Контент-фильтр** настроена расшифровка веб-трафика. HTTPS-сайт проверяется только в случае расшифровки HTTPS-трафика **Контент-фильтром**.
- **Отсутствуют исключения в прокси-сервере.** Веб-ресурс не должен находиться в списках исключений прокси-сервера по назначению, а пользователь - в списках исключений по источнику. Трафик, попадающий в эти исключения, не направляется на антивирусную проверку.

Настройка

Для работы **Антивируса** выполните действия:

1. Перейдите в **Правила трафика** → **Антивирус** и включите модуль:

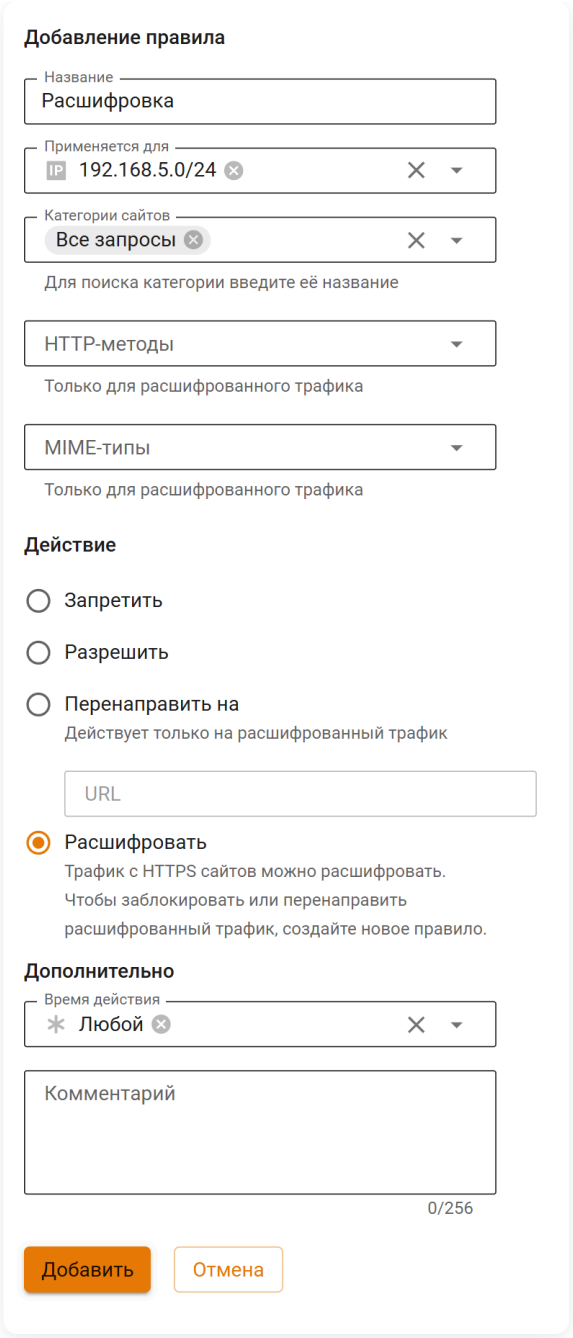


При необходимости включите опцию **Блокировать скачиваемые файлы при неудачной попытке анализа** для блокировки скачиваемых файлов, если не удается провести анализ файла.

2. Перейдите в **Правила трафика** → **Контент-фильтр** → **Правила** и создайте правило расшифровки HTTPS-трафика. Настройка расшифровки представлена в статье.

Пример правила расшифровки

Необходимо проверять антивирусом весь веб-трафик пользователей подсети `192.168.5.0/24`. Для этого создано правило **Контент-фильтра** с действием **Расшифровать**:



Правило применяется к сети `192.168.5.0/24` (поле **Применяется для**) и категории **Все запросы** (поле **Категории сайтов**) для проверки всех сайтов.

3. Если нужно отключить проверку для определенного HTTPS-трафика, перейдите в **Сервисы** → **Прокси** → **Исключения** и добавьте исключения:

- Сеть веб-ресурса - в списки по назначению.
- Сеть пользователя - в списки по источнику.

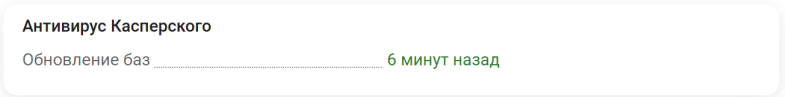
> Добавленные сети исключаются из обработки модулями **Прокси**, **Контент-фильтр** и не попадают в **Веб-трафик**.

Настройки антивирусной фильтрации не требуют ручного конфигурирования и при необходимости оптимизируются в обновлениях версий Ideco NGFW.

Результат проверки трафика антивирусом представлен в Журнале веб-трафика.

Обновление баз

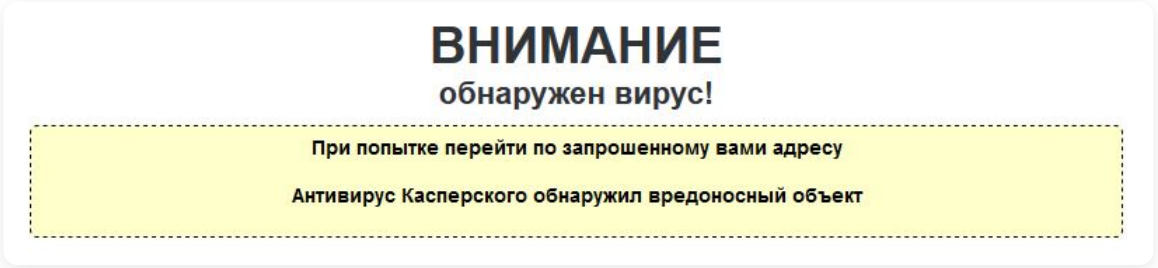
В разделе **Антивирус** можно посмотреть информацию о последнем обновлении баз антивируса Касперского:



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:



Предотвращение вторжений

Название службы раздела **Предотвращение вторжений**: `ideco-suricata-backend`; `ideco-suricata`; `ideco-suricata-event-syncer`; `ideco-suricata-profiles-syncer`.

Список имен служб для других разделов доступен по ссылке.

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Система **Предотвращения вторжений** (IDS/IPS, Intrusion detection system / Intrusion prevention system) предназначена для:

- ☑ Обнаружения
- ☑ Журналирования
- ☑ 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 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 Файрвола и системы Предотвращение вторжений

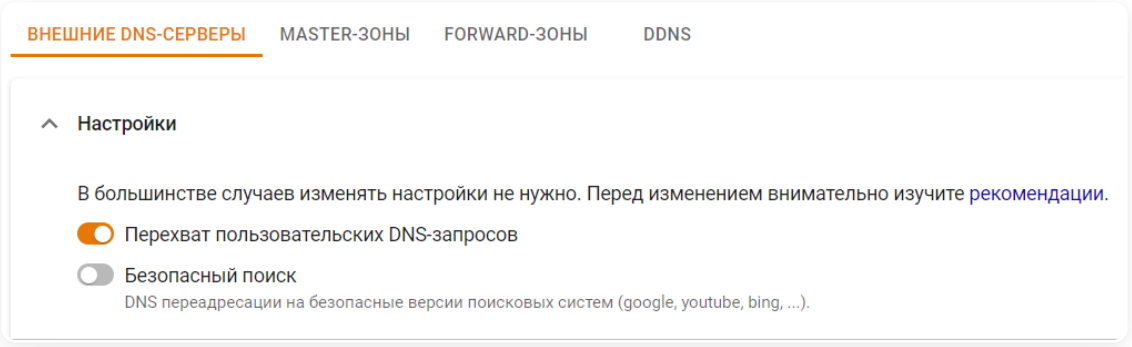
- **Файрвол** Ideco NGFW анализирует трафик для поиска подходящего правила и применяет его. Если в таблице есть несколько правил с одними и теми же условиями, применяется правило, стоящее выше по списку. Запрещающие правила **Файрвола** сразу блокируют соответствующий трафик, он не проходит дополнительную 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 **Файрволе** правило с источником **Любой** и назначением **Любой**, разместив его в конец таблицы. В этом случае трафик, который не был найден в правилах **Файрвола**, но соответствует профилям IPS, пройдет проверку системой **Предотвращения вторжений**.
- Если в одном правиле **Файрвола** 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 механизм работы системы **Предотвращения вторжений** изменился, появились возможности:

- ☑ Работать с правилами IPS на уровне сигнатур, фильтровать их и просматривать в удобном виде
- ☑ Составлять независимые друг от друга наборы правил IPS и применять их только к необходимому трафику с помощью профилей системы **Предотвращения вторжений**, которые назначаются в правилах **Файрвола**

Особенности обработки DNS-запросов

При включенной опции **Перехват пользовательских DNS-запросов** в разделе **Сервисы** → **Защита и управление DNS** → **Внешние DNS-серверы** трафик обрабатывается не как **FORWARD**, а как **INPUT**:

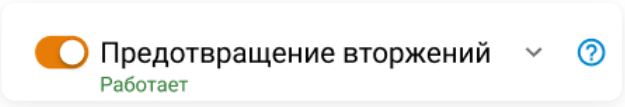


Если опция **Перехват пользовательских DNS-запросов** включена (по умолчанию включена), создайте правила **INPUT** для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

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 разделе **Профили безопасности** → **Предотвращение вторжений**.

3. Примените их в правилах Файрвола.

В обработку трафика не попадают:

- Сигнатуры, не включенные ни в один профиль.
- Профили, не используемые в правилах **Файрвола**.

Полезные ссылки

Подробнее о Load Average



¼ Í ÚÞ Ì Ý Ý Ñ ÜØ Û Ú ÛÚÜØ×ß 6 6 + Î ÒÜÔÑØ ÑÐ Ìß Ñ Ù ÙÚÜ ÏÛØÚ å Ù Ô Ö Ì

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

1. Подключитесь к серверу с помощью SSH-клиента 3 X 7 7 . Программа бесплатна, и скачать ее 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:

- Û Ú Ü 22;
- ×Ú Ï Ô-ùemsup;
- Û Ì Ü ×Úè ßÔÛÙ Ù ç Õ Û Ü ×Ôêâ Ñ Ù Ô Ñ Ì ×Ñ Ù ÙÚÜ ÏÛØÚ å Ù Ô Ö Ì

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

Пользовательские сигнатуры

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 **Файрвола**.

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; htt
```

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, его 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 их необходимо указать. 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 их использования в значениях опций.

Создание пользовательской сигнатуры

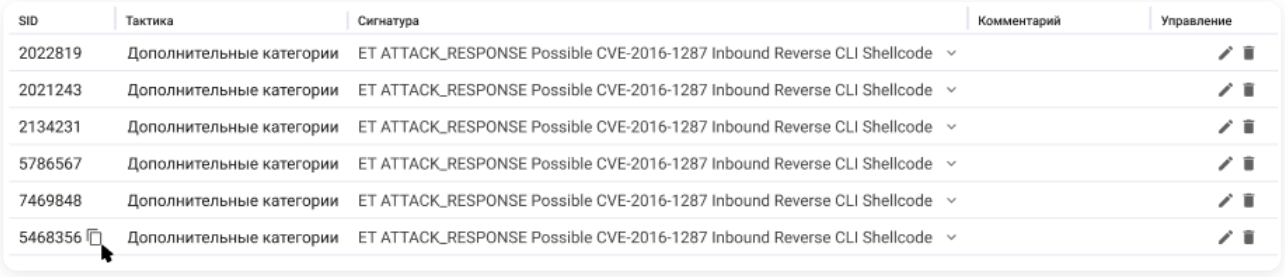
Нажмите **Добавить** и выберите способ добавления:

Вручную

В открывшейся форме введите комментарий, сигнатуру 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 раздел **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 раздел **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.st
```

Пример пользовательской сигнатуры:

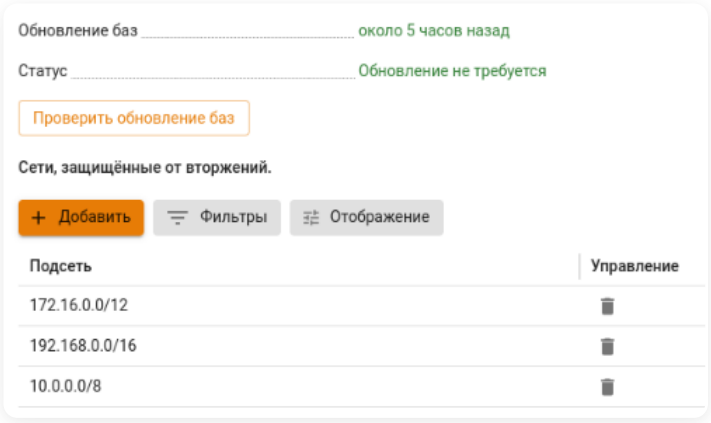
```
pass http 192.168.10.10 any -> 1.1.1.1 any (flow:established,to_client; http.stat_code; content:"200"; http.server; content:"
```

Полезные ссылки

Полная документация по форматам сигнатур.

Настройки

На вкладке можно проверить статус обновления баз системы **Предотвращение вторжений** и отредактировать список сетей, защищенных от вторжений:



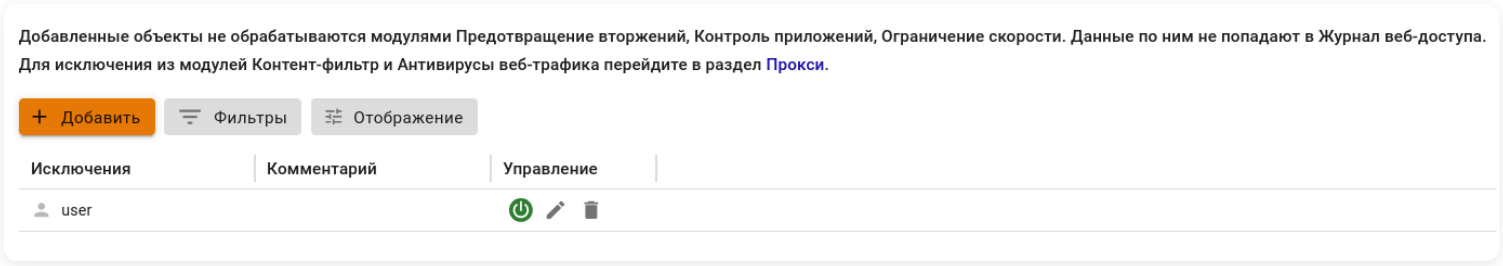
Для добавления подсети в список защищенных нажмите **Добавить** и в поле **Подсеть** укажите локальные сети, обслуживаемые NGFW (сети локальных интерфейсов NGFW, маршрутизируемые на них сети удаленных сегментов локальной сети предприятия).

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 в качестве единственного DNS-сервера.
  - В настройках DNS-сервера на NGFW указать Forward-зону для локального домена.

Исключения

Правила в разделе **Исключения** отключают трафик из обработки системы Предотвращения вторжений, Контроля приложений, данные по ним не попадают в монитор трафика:



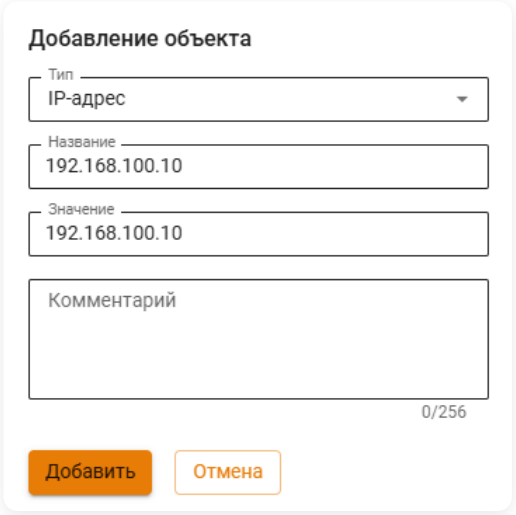
При наличии большого количества исключений в таблице воспользуйтесь кнопкой **Фильтры**.

Добавление исключения

Для предотвращения обработки трафика необходимо добавить объект в исключения:

1. Перейдите в раздел **Правила трафика** → **Исключения** и нажмите **Добавить**.

2. Выберите существующий объект или создайте новый, указав его тип, название и значение объекта. По желанию можно указать произвольный комментарий:



3. Нажмите **Добавить**.

Если в качестве DNS-сервера у пользователя указан локальный адрес сервера Ideco NGFW, то исключения работать не будут. Весь трафик, идущий на адреса локальных и VPN-интерфейсов Ideco NGFW, всегда обрабатывается службой фильтрации трафика.

Особенность работы исключений по домену

1. При добавлении исключения по домену NGFW выполняет DNS-резолв указанного домена.

2. Полученные в результате резолва IP-адреса добавляются в список IP-адресов, используемый правилами фильтрации.

3. Клиент при обращении к ресурсу выполняет собственный DNS-резолв домена.

4. В зависимости от региона, балансировки нагрузки или времени клиент может получить другие IP-адреса того же домена.

5. Если IP-адрес, полученный клиентом, отсутствует в списке IP-адресов NGFW, исключение не применяется и трафик блокируется.

Для корректной работы исключений рекомендуем включить **Перехват пользовательских DNS-запросов** в **Сервисы** → **DNS** → **Внешние DNS-серверы**. Но даже в этом случае возможны кратковременные блокировки из-за DNS-кэша и задержек обновления списка IP-адресов,

используемого правилами фильтрации (ipset).

Объекты

Название службы раздела *Объекты*: `ideco-alias-backend`.

Список имен служб для других разделов доступен по ссылке.

Типы объектов

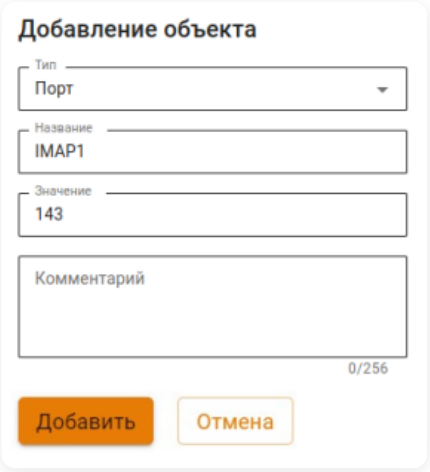
- **Зона** - логическое объединение сетевых интерфейсов. Используется для настройки правила файрвола на несколько интерфейсов.
- **IP-адрес** - IP-адрес IPv4. Пример: 10.0.0.1.
- **Диапазон IP-адресов** - диапазон IP-адресов от первого до последнего, указанного в диапазоне. Пример: 10.0.0.1-10.0.0.25.
- **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 и домен. Пример: 10.0.0.1, 10.0.0.4, 10.0.0.126.
- **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** - группа объектов, содержащая GeoIP.

Создание объектов

Чтобы создать объект, необходимо выполнить следующие действия:

1. Перейдите в раздел **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 файрвола, введя нужный IP-адрес или порт в соответствующих полях.



В Ideco NGFW также используется специальный алиас - **Любой**. Если при создании правила в каком-либо из полей выбран этот алиас, правило будет распространяться на все объекты, доступные к выбору в том же поле.

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 Файрвол.

Web Application Firewall

Создание WAF-профилей для защиты опубликованных веб-ресурсов от атак

Перейти >

Контроль приложений

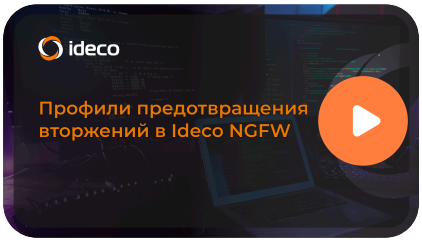
Создание, настройка и примеры использования профилей **Контроля приложений**

Перейти >

Предотвращение вторжений

Создание, настройка и примеры использования профилей **Предотвращение вторжений**

Перейти >



Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Web Application Firewall

Название служб раздела **Web Application Firewall**: `ideco-waf-backend`; `ideco-waf-event-syncer`.

Список служб для других разделов доступен по ссылке.

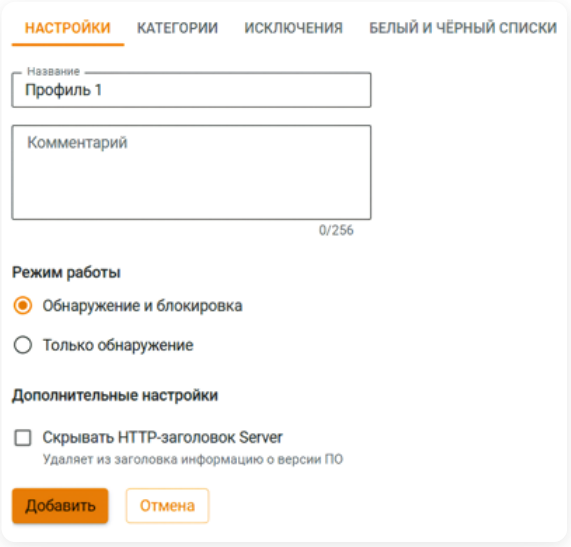
Использование WAF-профилей позволит настроить параметры защиты для опубликованного веб-ресурса. Профиль создается в разделе **Профили безопасности → Web Application Firewall**. Подробные описания сигнатур можно найти в документации ModSecurity.

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:

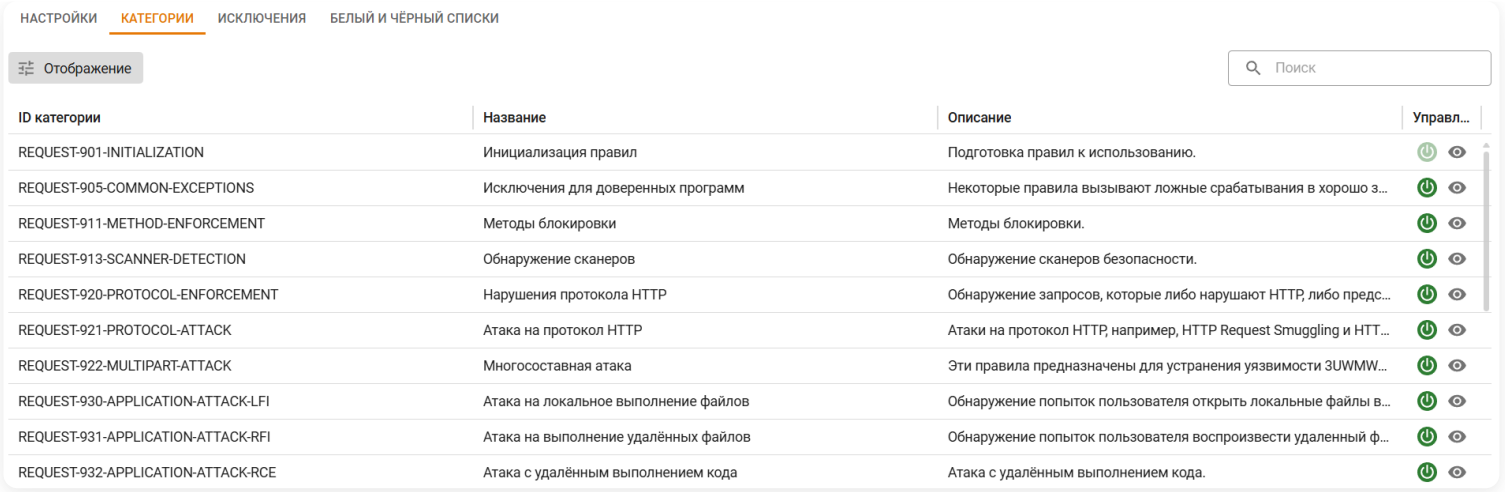


Расшифровка полей

- **Название** - введите название профиля.
- **Комментарий** - введите пояснение для профиля.
- **Режим работы**:
  - **Обнаружение и блокировка** - подозрительные запросы будут блокироваться и логироваться WAF.
  - **Только обнаружение** - подозрительные запросы будут логироваться WAF, но не будут блокироваться.
- **Дополнительные настройки**:
  - **Скрывать HTTP-заголовок Server** - позволяет скрыть данные, идентифицирующие сервер.

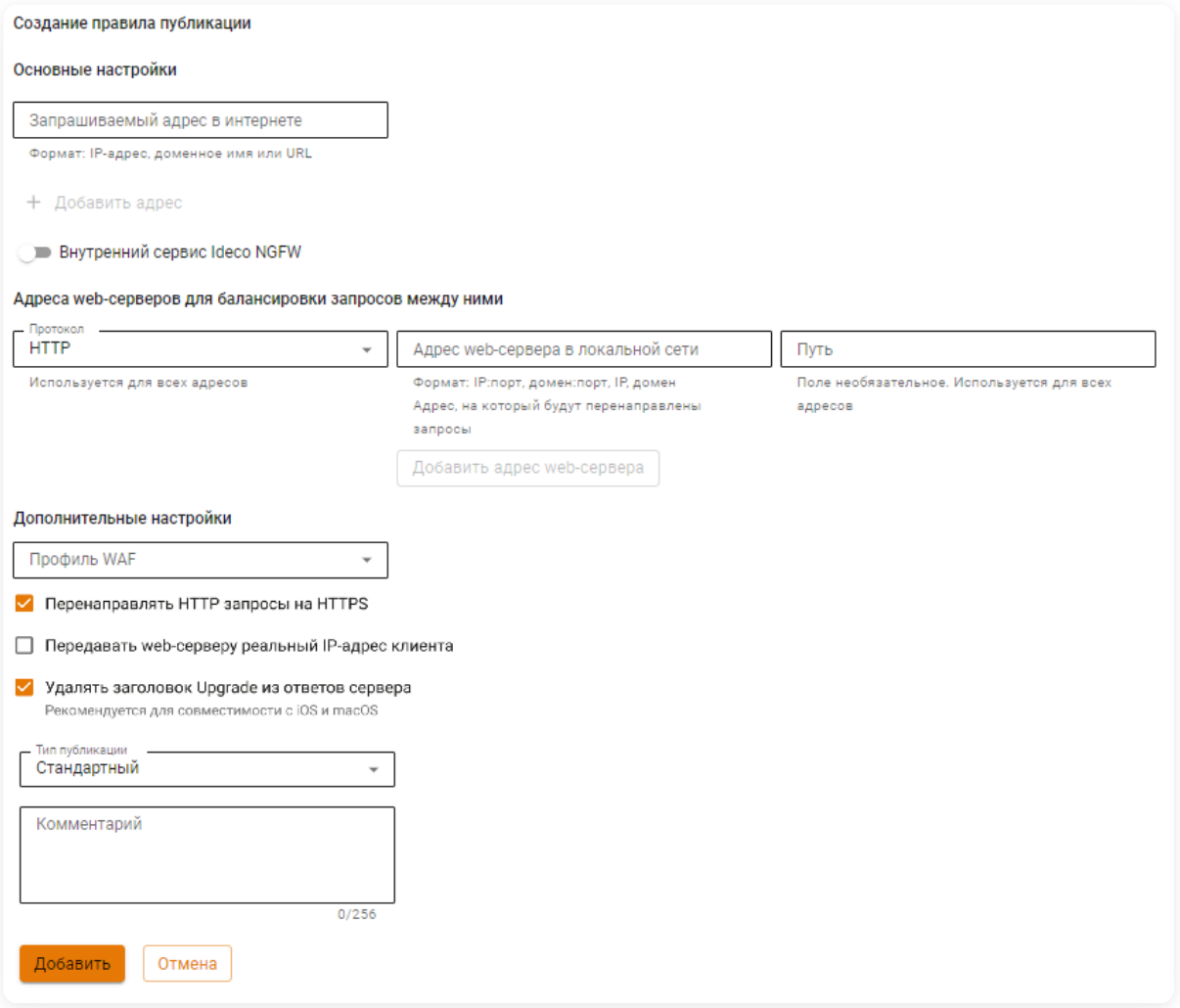
2. Нажмите **Добавить**.

3. На вкладке **Категории** включите или отключите правила:



Использование профиля WAF в правиле Обратного прокси

1. Перейдите в раздел **Сервисы** → **Обратный прокси**, нажмите **Добавить** и заполните поля:



Расшифровка полей

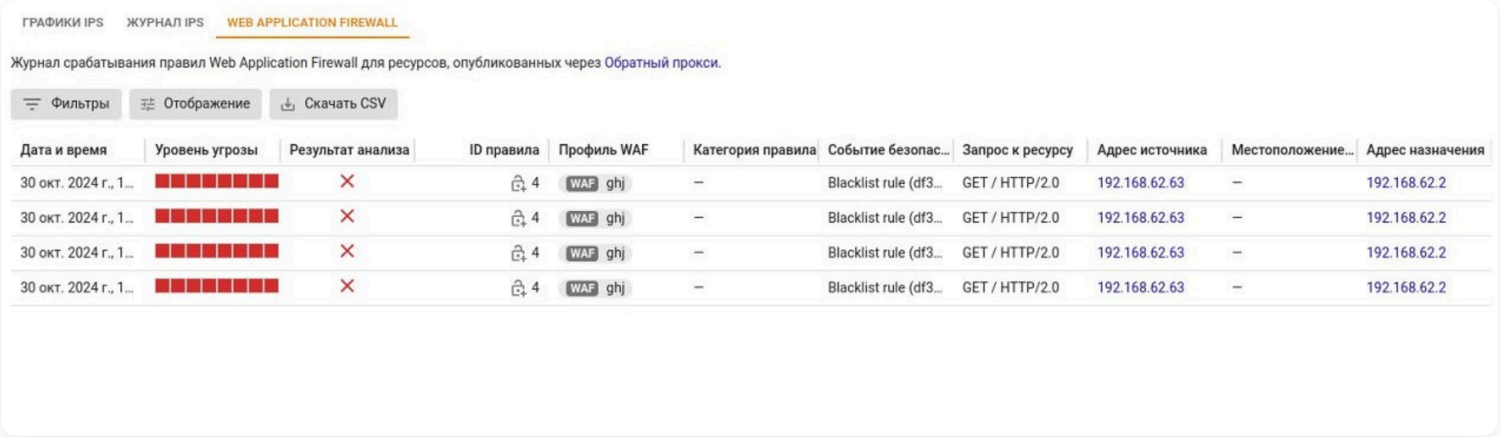
- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных адресов нажмите кнопку **Добавить адрес**.
- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Адрес web-сервера в локальной сети** - 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.

2. Нажмите **Добавить**.

Диагностика и добавление исключений

Срабатывание правил **Web Application Firewall** отображается на вкладке **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**:



Добавить правило в исключение можно двумя способами:

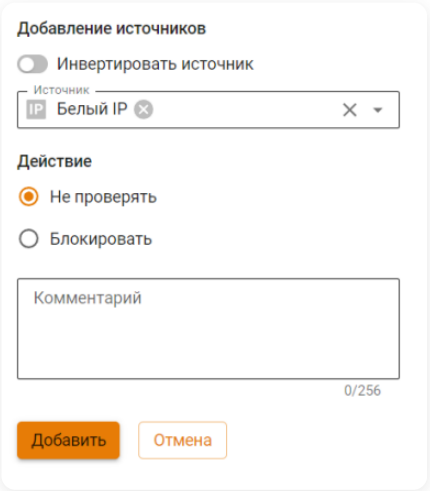
По IP-адресу

1. Перейдите в раздел **Web Application Firewall** и у правила нажмите на  .

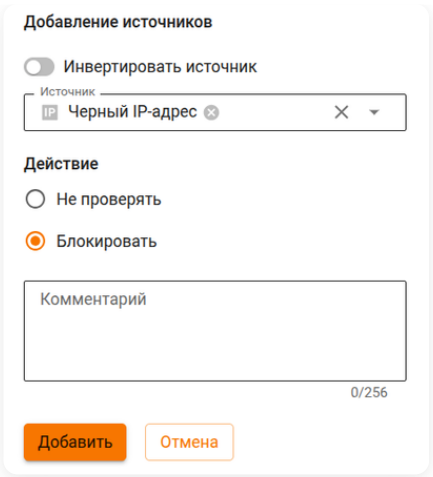
2. На вкладке **Белый и черный списки** нажмите **Добавить источник**:

> 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 на вкладке **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 **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 на вкладке **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

На вкладке Web Application Firewall

1. Перейдите на вкладку **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.

Чтобы пользовательские правила WAF сохранялись при обновлении, в Ideco NGFW предусмотрен специальный файл (after-секция) для пользовательских правил и исключений. Он позволяет встроиться в процесс обработки запроса для добавления пользовательских проверок или изменения поведения системы после отработки стандартных правил.

Для внесения правил в after-секцию:

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"
```

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`.

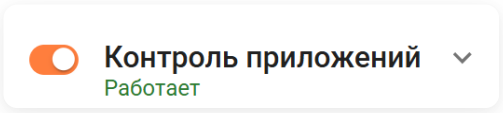
Контроль приложений

Названия служб раздела **Контроль приложений**: `ideco-app-backend` и `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 **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:

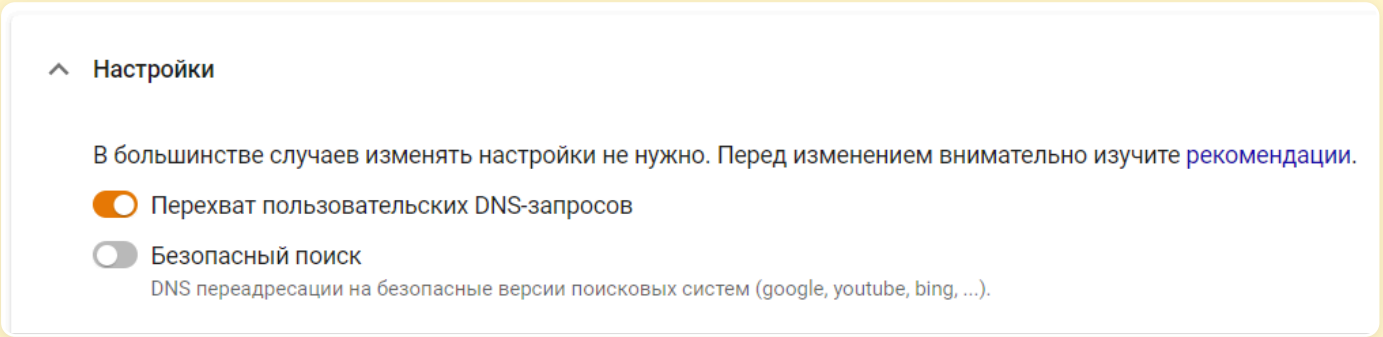
- В правиле **FORWARD** или **INPUT** раздела **Межсетевой экран** включена опция **Контроль приложений**.
- В этом правиле выбран профиль безопасности.

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 **Контролем 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** → **Защита и управление 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**.

При наличии большого количества профилей в таблице воспользуйтесь кнопкой **Фильтры**.

Особенности обработки трафика с помощью профиля Контроля приложений

Контроль приложений проверяет только тот трафик, который соответствует разрешающему правилу **Файрвола** с включенной опцией **Контроля приложений** и выбранным профилем.

Порядок применения правил Файрвола

- **Файрвол** Ideco NGFW анализирует трафик, ищет подходящее правило в таблице (сверху вниз) и применяет его.
- Если в списке несколько правил с одинаковыми условиями, применяется правило, которое выше в таблице.
- Трафик не проходит дополнительную проверку **Контролем приложений**, если заблокирован запрещающим правилом **Файрвола**.

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 Socialg 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 теле-радиовещания 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 **Файрвола**:

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 Файрвол.
2. Создайте правило Файрвола, 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

Особенности создания профилей

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.

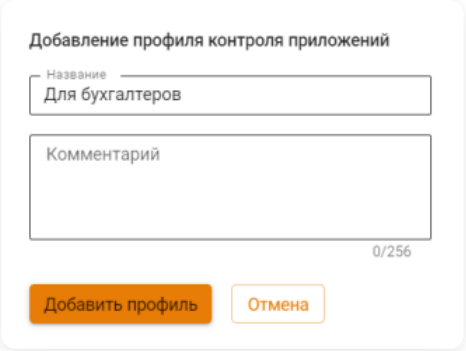
Создание профилей и добавление в правила Файрвола

Пример. Необходимо ограничить доступ к социальным сетям пользователям группы "Бухгалтерия".

Создание профиля Контроля приложений

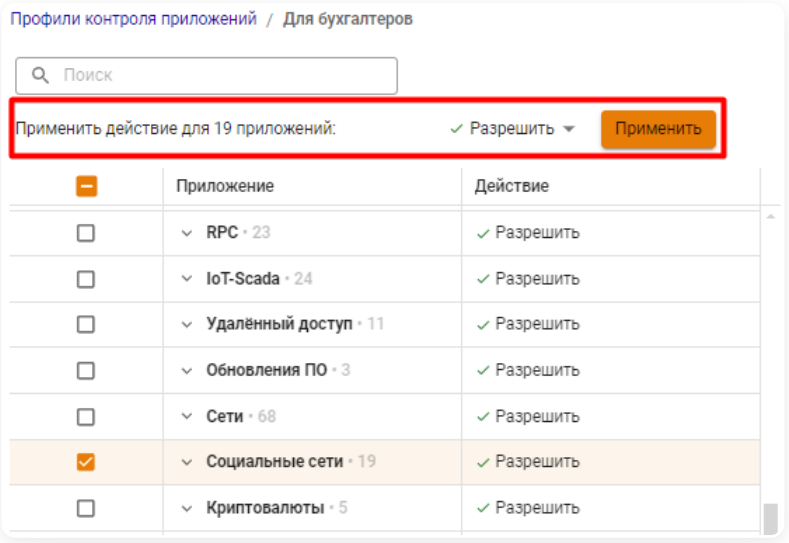
1. Перейдите в раздел **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Заполните **Название**, **Комментарий** (необязательно) и добавьте профиль:

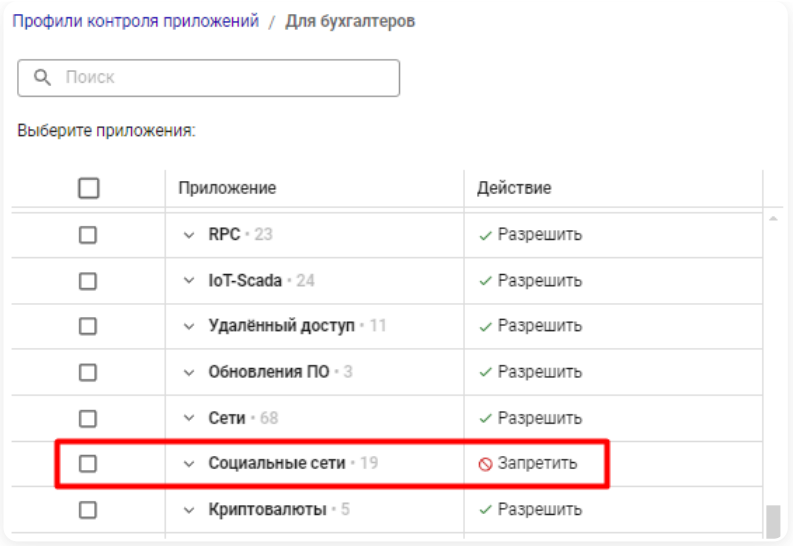


3. Нажмите в столбце **Управление** на  , затем **Доступ к приложениям**.

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:



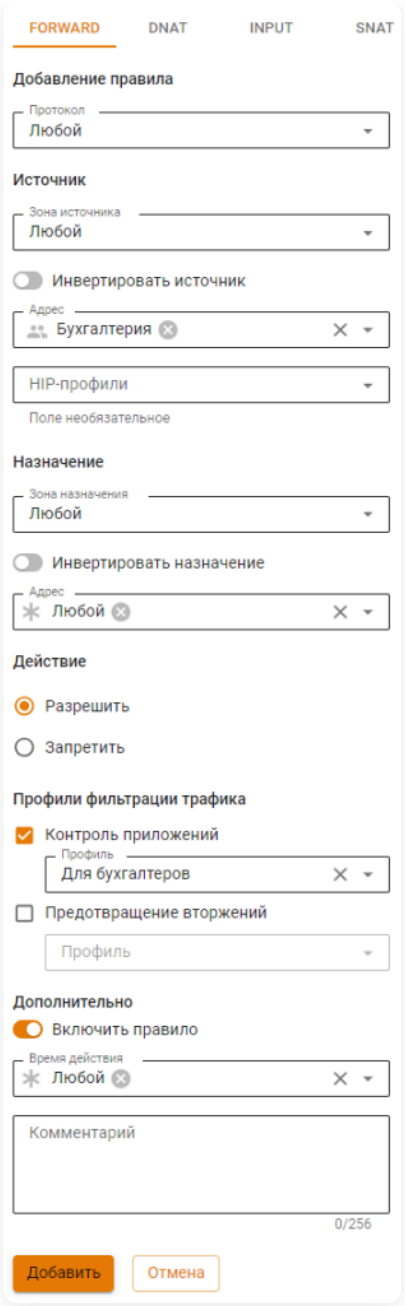
К неизвестным источникам по умолчанию применяется действие **Разрешить** (доступно для редактирования).

6. Нажмите **Сохранить**.

Добавление профиля в правила Файрвола

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать с помощью профиля **Контроля приложений**;
- **Источник** - выберите **Адрес**, **Зону** и **HIP-профиль** источника трафика;
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика;
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** и в разделе **Профили для фильтрации** из раскрывающегося списка выберите профиль, запрещающий социальные сети сотрудникам бухгалтерии.

4. Включите правило или оставьте его выключенным.

5. Нажмите **Добавить**.

6. Если в разделе **Сервисы → Защита и управление 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 он 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

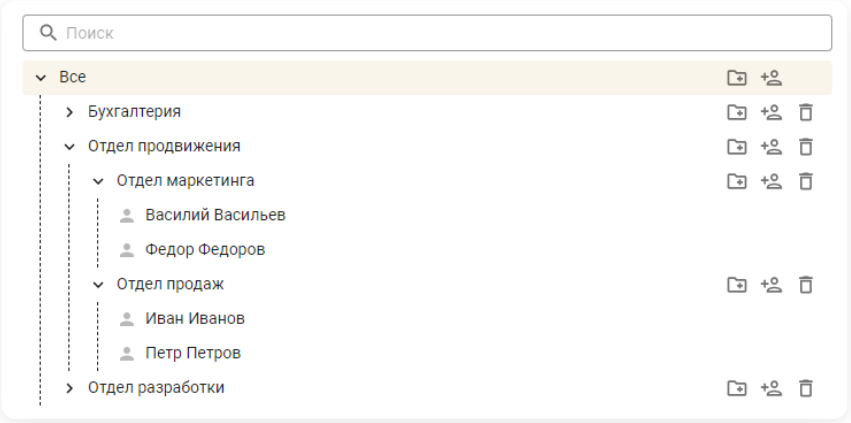
Настройка фильтрации трафика, для которого в таблице FORWARD нет правил

Пример создания иерархической структуры

Пример. 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.

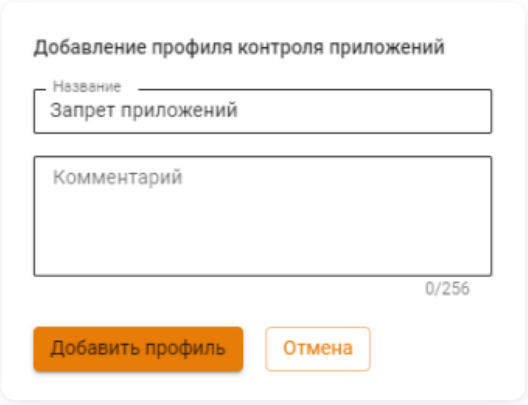
В описанном примере Федор Федоров - сотрудник Отдела маркетинга, а Отдел маркетинга - структурное подразделение Отдела продвижения:



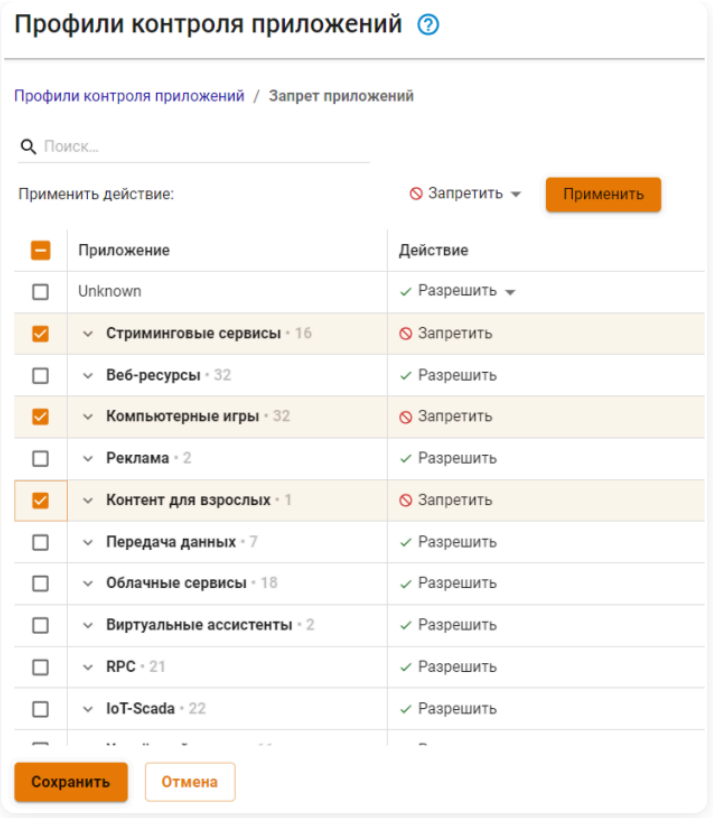
Создание профилей Контроля приложений

Создайте профили в соответствии с условиями примера:

1. Перейдите в раздел **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:



- Нажмите в столбце **Управление** на , а затем **Доступ к приложениям**;
- 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** в левом нижнем углу.

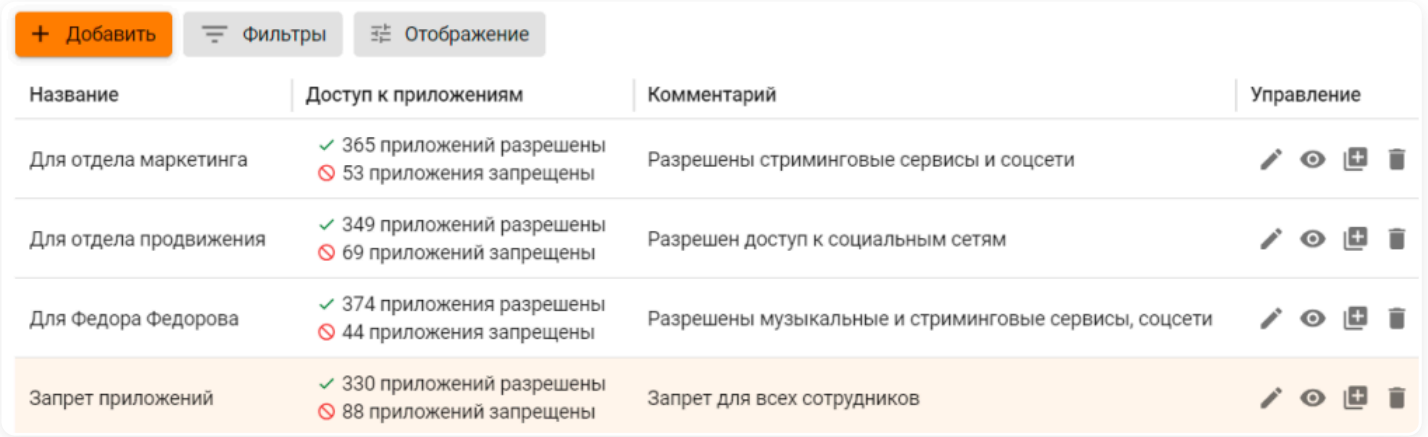
3. Создайте профиль для Отдела продвижения, разрешающий доступ к социальным сетям. Для этого:

- 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:

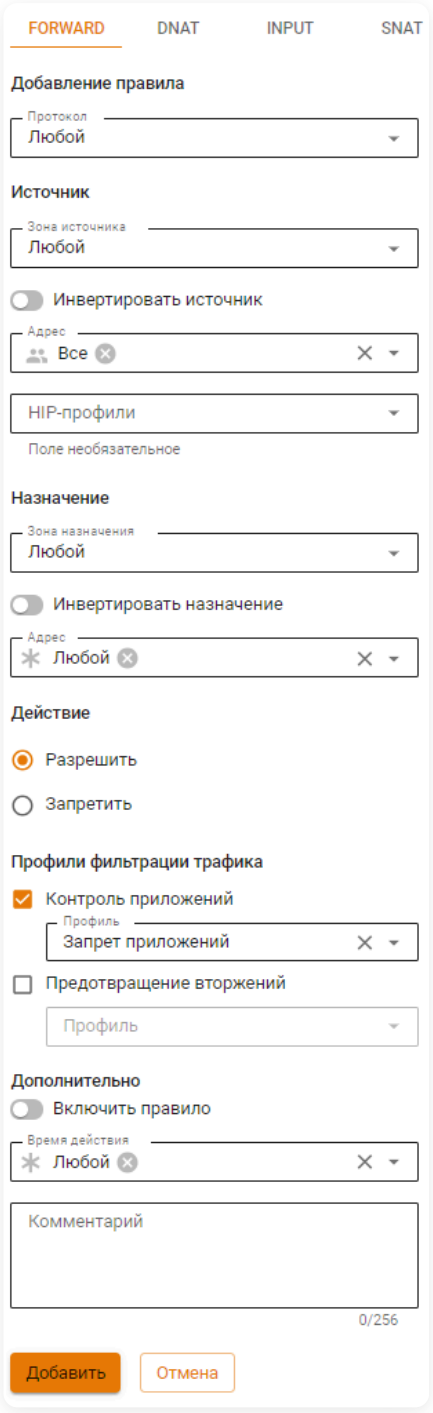


Создание правил Файрвола

Теперь необходимо создать и включить правила в **Файрволе**, чтобы применить настройки для конкретных групп пользователей и установить приоритет прохождения трафика:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

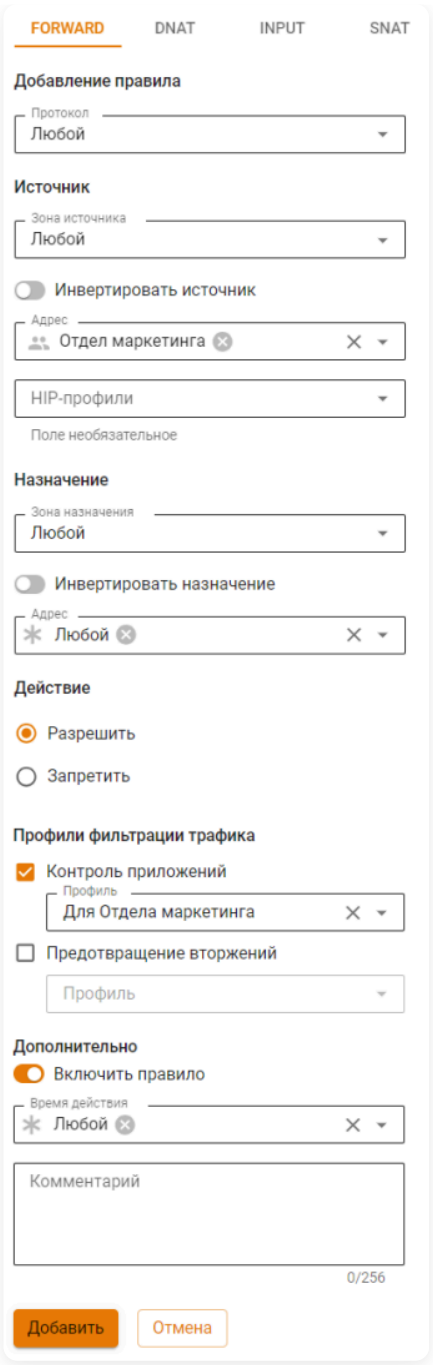
2. Заполните поля:



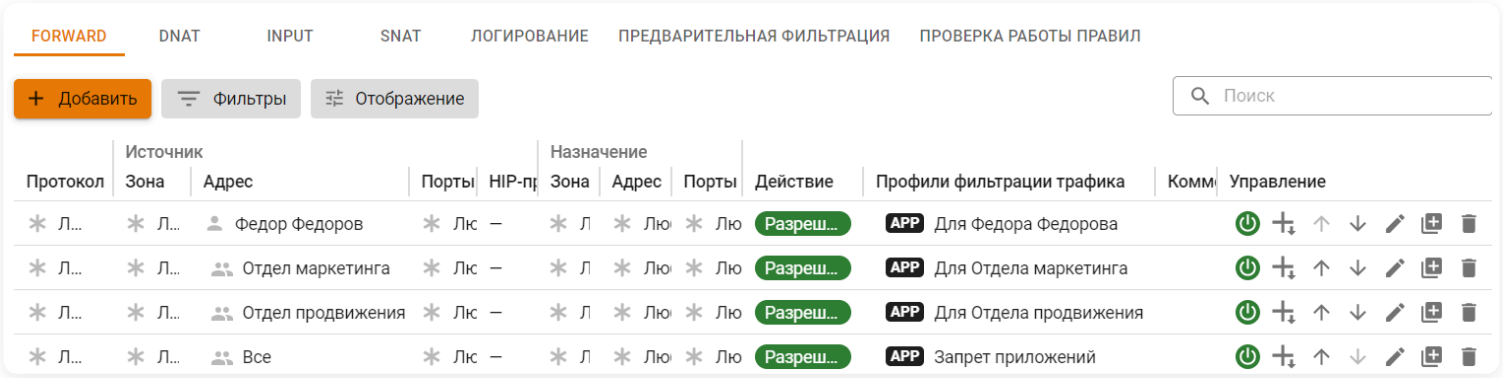
- **Адрес источника** - группа пользователей **Все**;
- **Действие** - **Разрешить**;
- **Профили безопасности** - **Контроль приложений**, профиль **Запрет приложений**;

3. Включите правило и нажмите **Добавить**.

4. Аналогично создайте правила для каждого профиля. При создании правила **Файрвола** укажите соответствующий профилю адрес источника. Например, при создании правила с профилем фильтрации **Для Отдела маркетинга** выберите в поле **Адрес** раздела **Источник** группу Отдел маркетинга:



5. Чтобы трафик проходил в соответствии с условиями примера, установите в **Файрволе** следующую последовательность правил:



Чем выше в таблице стоит правило, тем выше его приоритет.

Разрешающее правило для сотрудника не сработает, если выше в таблице **Файрвола** находится правило, запрещающее трафик для отдела, в котором работает этот сотрудник.

6. Если в разделе **Сервисы** → **Защита и управление 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 он направляется в INPUT.

Настройка фильтрации трафика

Создайте профиль **Контроля приложений**, соответствующий нужным правилам:

1. Перейдите в раздел **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Введите **Название** профиля, **Комментарий** и добавьте профиль.

3. Нажмите в столбце **Управление** на , затем **Доступ к приложениям**.

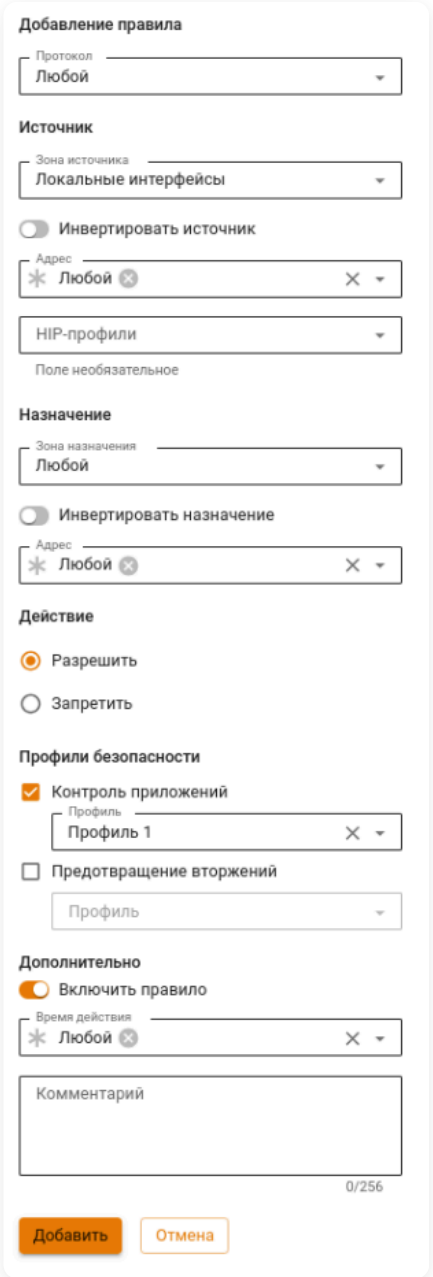
4. Выберите протоколы или группы протоколов и действия (**Запретить** или **Разрешить**), которые будут к ним применяться, затем нажмите **Применить**.

5. Нажмите **Сохранить** в левом нижнем углу.

Далее создайте правило **Файрвола** с созданным профилем **Контроля приложений**:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите **Любой**;

- **Источник**:
  - **Зона источника** - выберите **Локальные интерфейсы**;
  - При необходимости укажите **Адрес** и **HIP-профиль** источника трафика.
- **Назначение**:
  - **Зона назначения** - выберите **Любой**;
  - При необходимости укажите **Адрес** назначения трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** в профилях безопасности и из раскрывающегося списка выберите созданный ранее профиль.

4. Включите правило и нажмите **Добавить**.

5. Поместите правило в конец таблицы **Файрвола**. Если в таблице есть правило, запрещающее все, поместите правило с профилем **Контроля приложений** над ним.

6. Если в разделе **Сервисы → Защита и управление 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 он направляется в INPUT.

Предотвращение вторжений

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

В разделе **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые NGFW будет применять к трафику, соответствующему этим сигнатурам.

Профили **Предотвращения вторжений** применяются при создании правил в разделе **Правила трафика** → **Файрвол**.

Если профиль не добавлен в правила таблицы **FORWARD** или **INPUT** раздела **Правила трафика** → **Файрвол**, трафик не будет фильтроваться системой **Предотвращения вторжений**.

В отбработке трафика не участвуют:

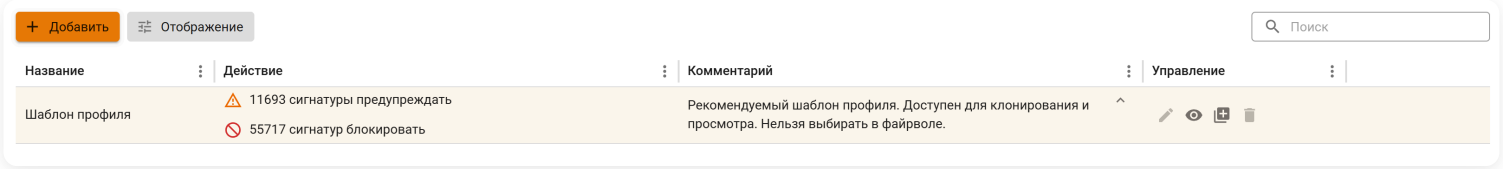
- Сигнатуры, не используемые в профилях.
- Профили, не используемые в правилах **Файрвола**.

Создание профилей

1. Перейдите в **Профили безопасности** → **Предотвращение вторжений** и нажмите **Добавить**.

Создание профиля через шаблон

1. Для клонирования нажмите :



- **Шаблон профиля** - подходит для максимальной защиты от кибератак. Включает динамически обновляемые черные списки хостов и эффективно очищает трафик из внешних сетей.

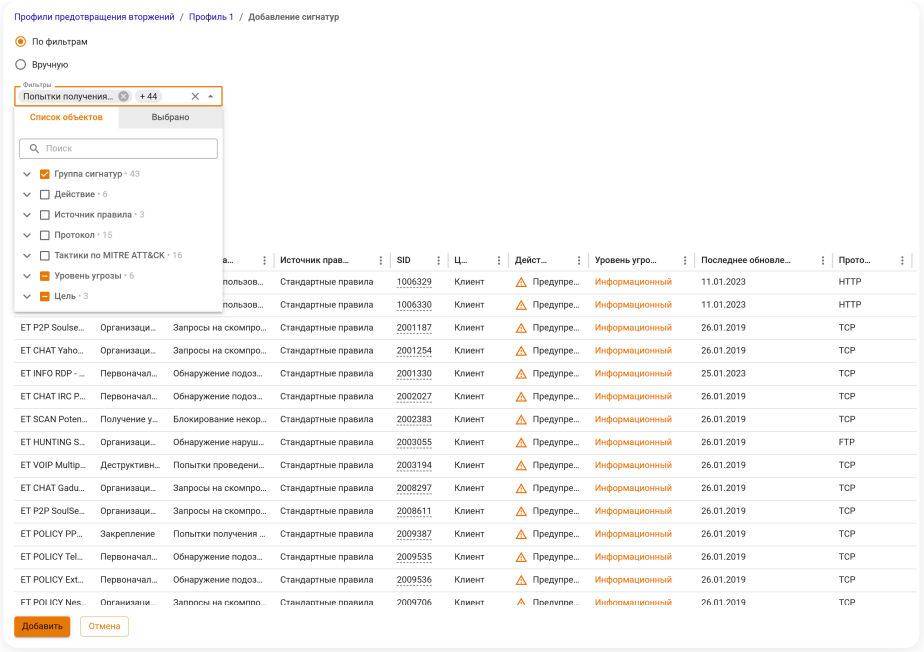
2. Чтобы просмотреть или изменить созданный профиль (описание и правила выбора сигнатур), нажмите или .
2. Введите название профиля, комментарий и нажмите **Добавить**.

3. Перейдите на вкладку **Сигнатуры** и нажмите **Добавить сигнатуры**.

4. Выберите способ добавления сигнатур в профиль:

По фильтрам

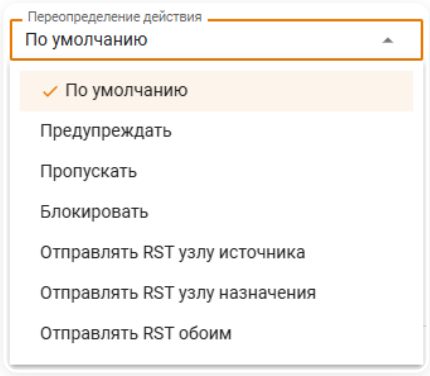
5. Выберите **Фильтры**. В таблице ниже отобразятся сигнатуры, соответствующие каждому из выбранных фильтров:



Доступные фильтры

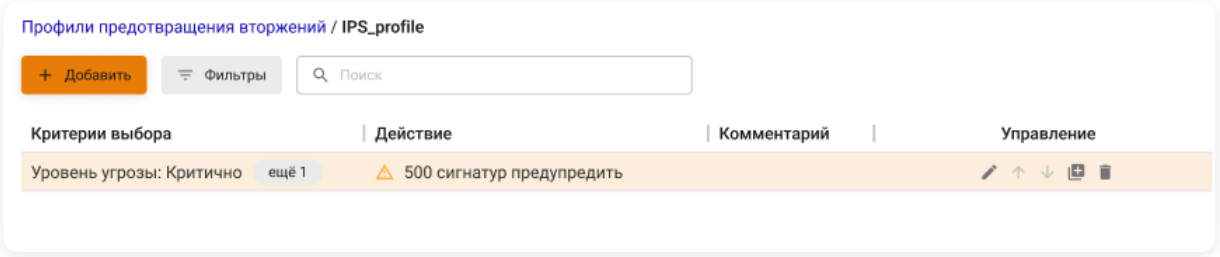
- **Группа сигнатур** - фильтр по готовым наборам сигнатур, сгруппированным по типу угроз.
- **Действие** - фильтр по действию, которое Ideco NGFW применит к трафику, соответствующему сигнатуре.
- **Источник правила** - фильтр по источнику сигнатуры.
- **Протокол** - фильтр по сетевому протоколу, который 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**:



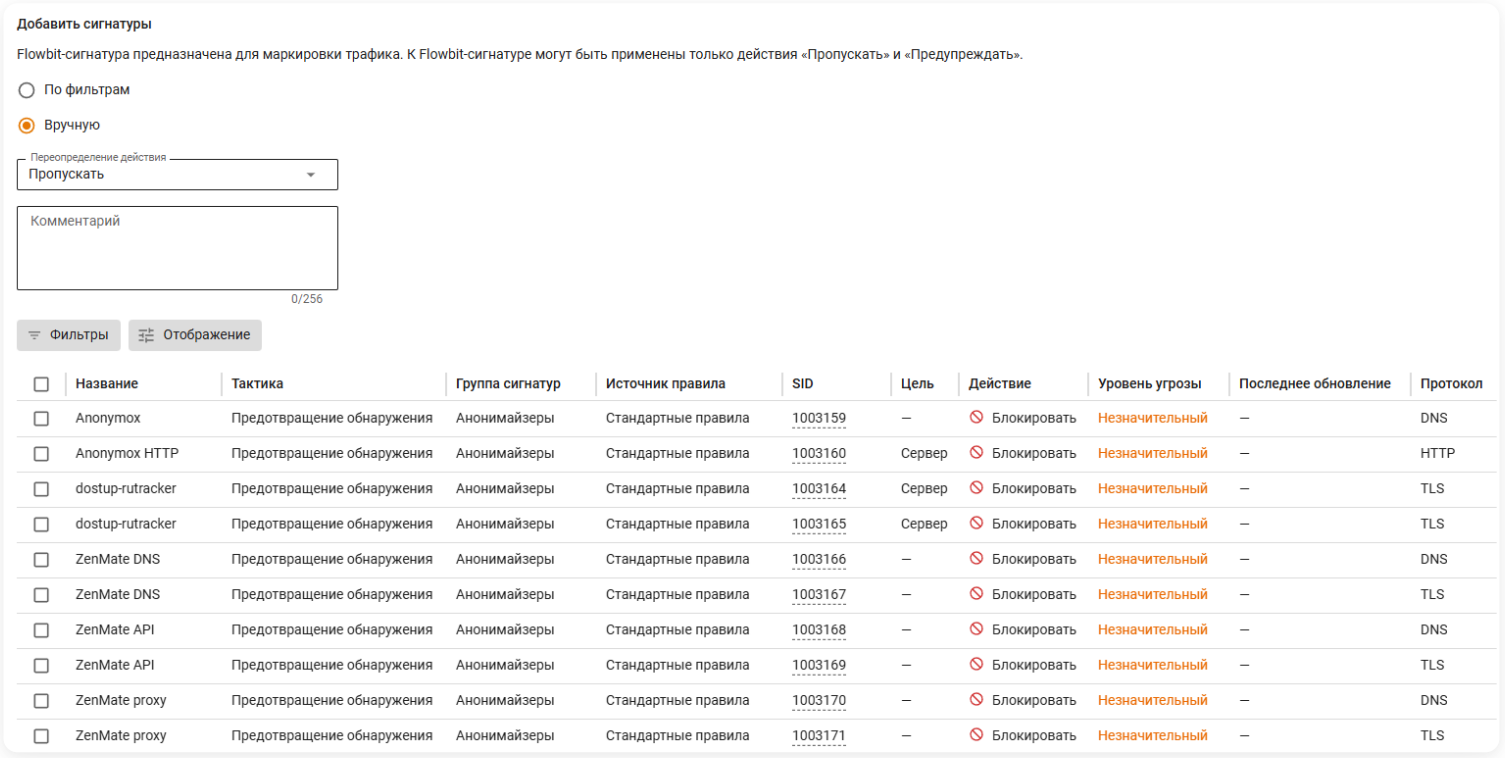
- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения.
- **Блокировать** - отбросить пакет и сгенерировать предупреждение.
- **Отправлять RST 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.

7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

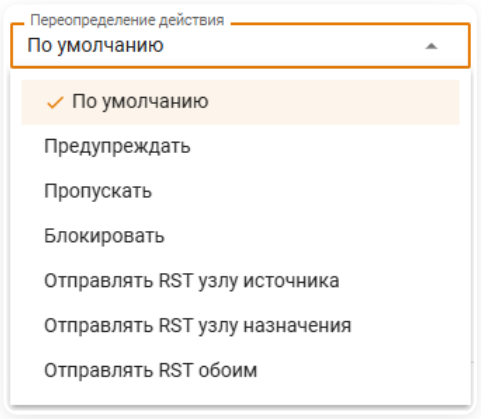


Вручную

5. В таблице отметьте сигнатуры, которые хотите добавить в профиль.При необходимости используйте **Фильтры**:

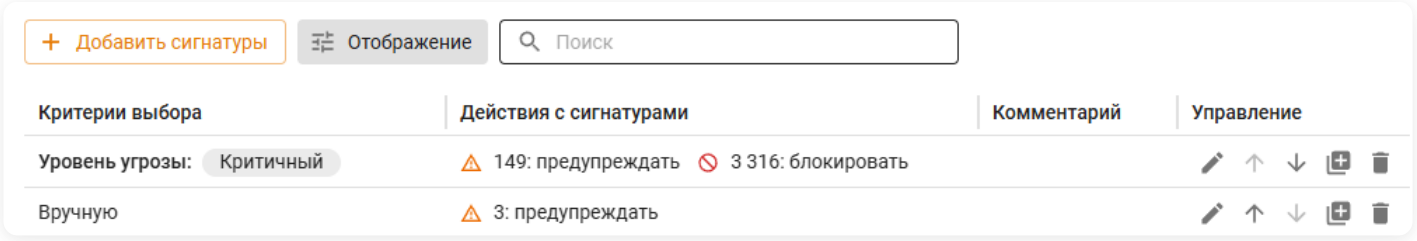


6. Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие **По умолчанию**:



- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения.
- **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.

7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

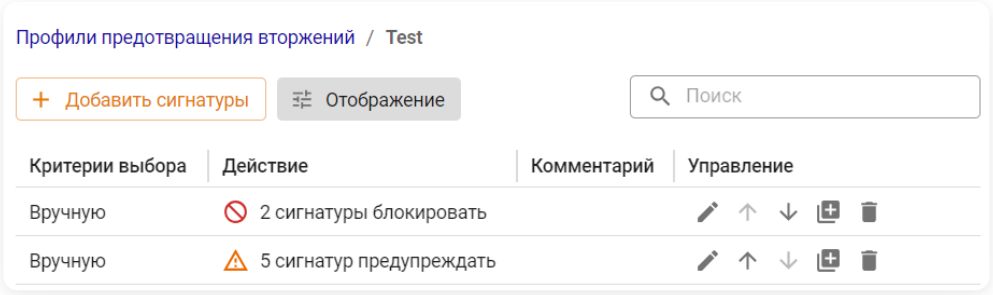


Количество сигнатур, отображаемых в таблице профилей, не всегда соответствует количеству сигнатур, добавленных при создании профиля. Это связано с тем, что для каждой сигнатуры может быть настроено несколько действий, но применяется только приоритетное. Приоритет определяется порядком правил внутри профиля.

В один профиль **Предотвращения вторжений** можно добавить несколько правил выбора сигнатур. Их приоритет можно менять в таблице профиля кнопками ↑ и ↓.

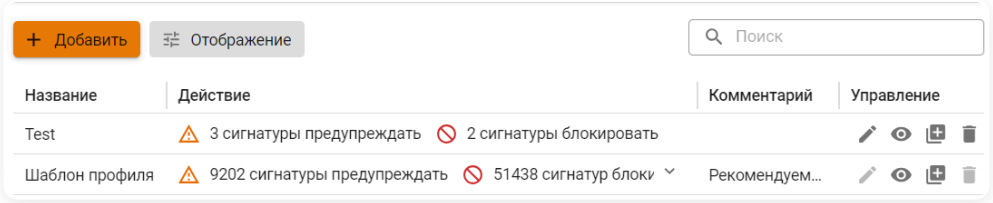
Пример отображения профиля при выборе нескольких действий сигнатур

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 **Профили безопасности** → **Предотвращение вторжений** в профиле Test отображаются две сигнатуры с действием **Блокировать** и три сигнатуры с действием **Предупреждать**, потому что фактически для дублирующихся сигнатур применяется более приоритетное правило:

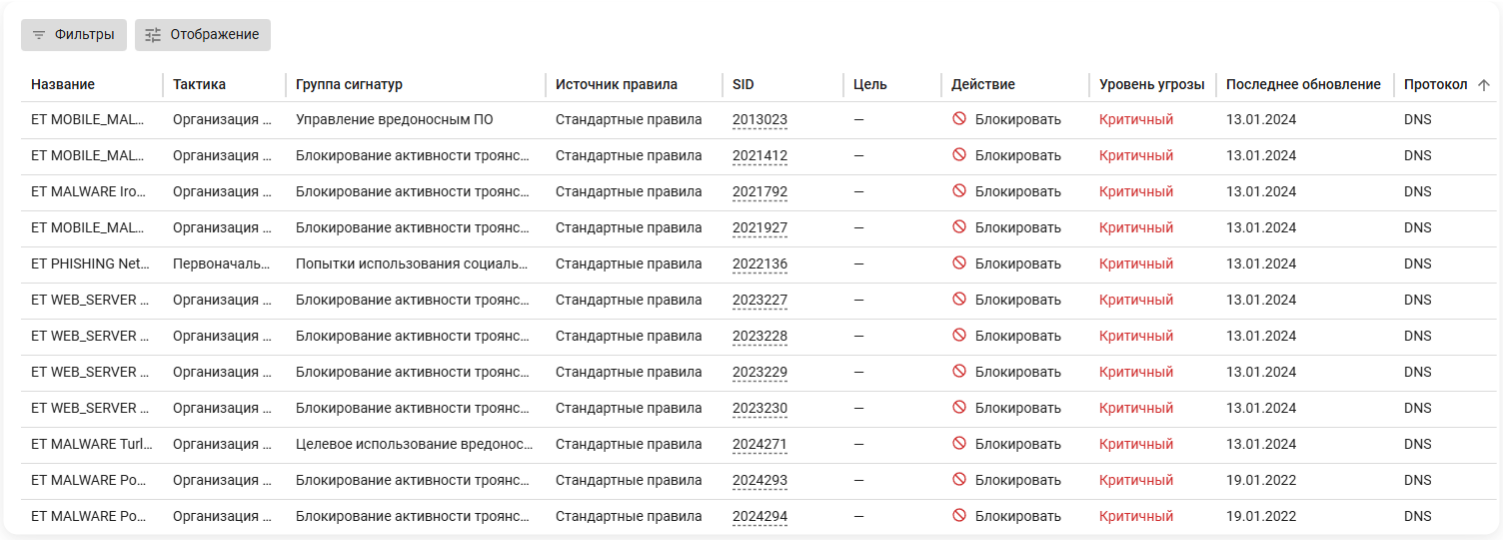


Использование оперативной памяти:

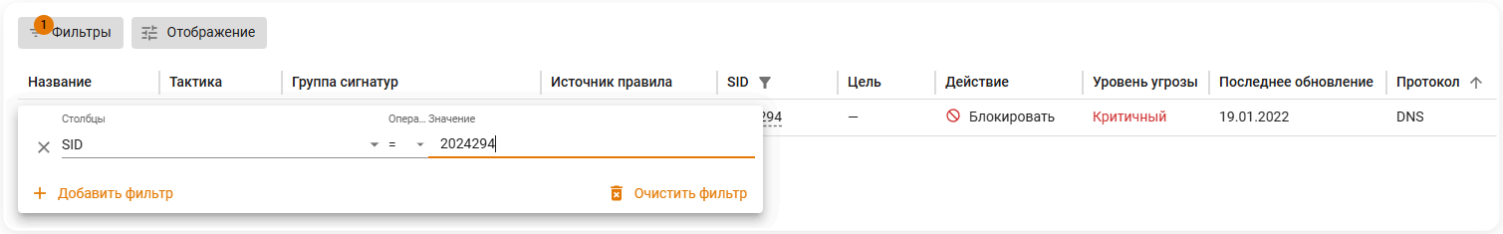
- Шаблон профиля не потребляет оперативную память.
- Настроенный профиль потребляет оперативную память, даже если не задействован в правилах Файрвола.
- Объем оперативной памяти, потребляемый одним профилем, зависит от количества сигнатур. Профиль, настроенный по рекомендуемому шаблону, использует ~450 МБ. Указано примерное значение, так как сигнатуры обновляются.

Изменение и просмотр профилей

Чтобы просмотреть созданный профиль (описание и правила выбора сигнатур), нажмите ✎. На вкладке **Выбранные сигнатуры** представлены все сигнатуры, для которых настроено одно или несколько действий:



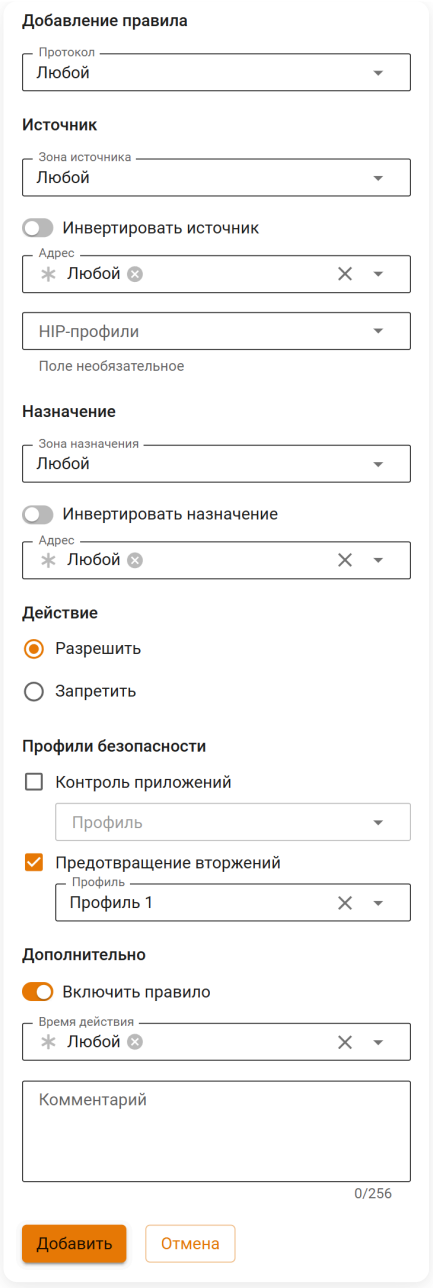
Для удобного поиска используйте **Фильтры**. Например, чтобы найти нужную сигнатуру по идентификатору:



Добавление профилей в правила Файрвола

1. Перейдите в **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, трафик которого требуется фильтровать системой **Предотвращения вторжений**.
- **Источник** - выберите **Адрес**, **Зону** и **HIP-профиль** источника трафика.
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Предотвращение вторжений** в разделе **Профили фильтрации трафика** и выберите необходимый профиль из раскрывающегося списка.

4. Включите правило или оставьте его выключенным.

5. Нажмите **Добавить**.

6. 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.

Сервисы

В этом 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 >

Балансировка и резервирование

Настройка резервирования каналов, статической и динамической балансировки

Перейти >

Маршрутизация

Настройка маршрутизации сетевого трафика, проходящего через Ideco NGFW.

Перейти >

BGP

Настройка BGP для обмена информацией о доступности сетей

Перейти >

OSPF

Настройка BGP для обмена информацией о доступности сетей

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 они стали доступны потребителям из сети интернет

Перейти >

ЛК/Портал SSL VPN

Настройка личного кабинета пользователя в Ideco NGFW (публикация и управление доступом пользователей)

Перейти >

Защита и управление 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 >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Сетевые интерфейсы

Название службы раздела *Сетевые интерфейсы*: `ideco-network-backend`; `ideco-network-nic`.

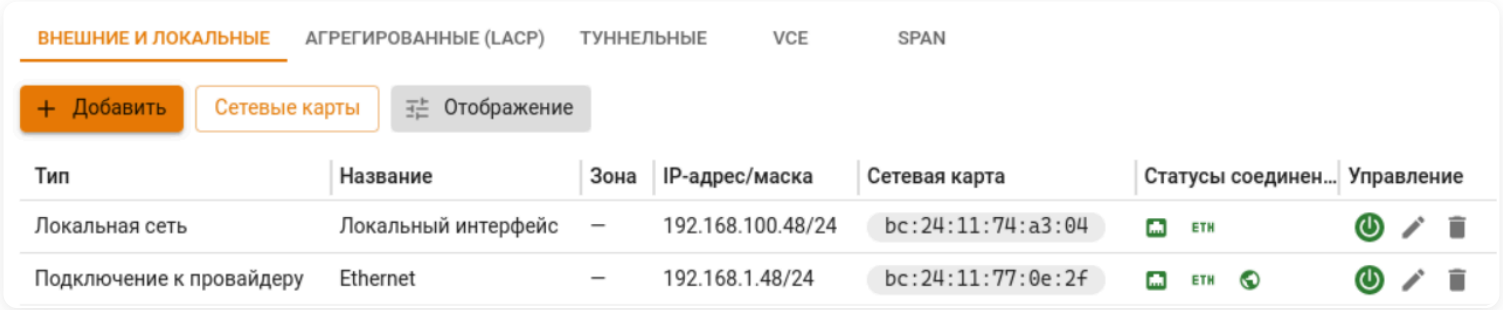
Список имен служб для других разделов доступен по ссылке.

Сетевой порт становится активным только после создания сетевого интерфейса (внешнего или локального). До этого момента индикаторы на подключенных сетевых портах не горят и Ethernet-кадры не передаются.

Для создания сетевых интерфейсов воспользуйтесь статьями:

- **Внешние и локальные интерфейсы**
- **Агрегированные интерфейсы (LACP)**
- **Туннельные интерфейфсы (GRE)**
- **VCE-интерфейсы**
- **SPAN-интерфейсы**

Все созданные интерфейсы представлены в виде таблиц на пяти вкладках:



Статусы соединения

- Сигнал есть

- Статус сигнала не определен

- Сигнала нет

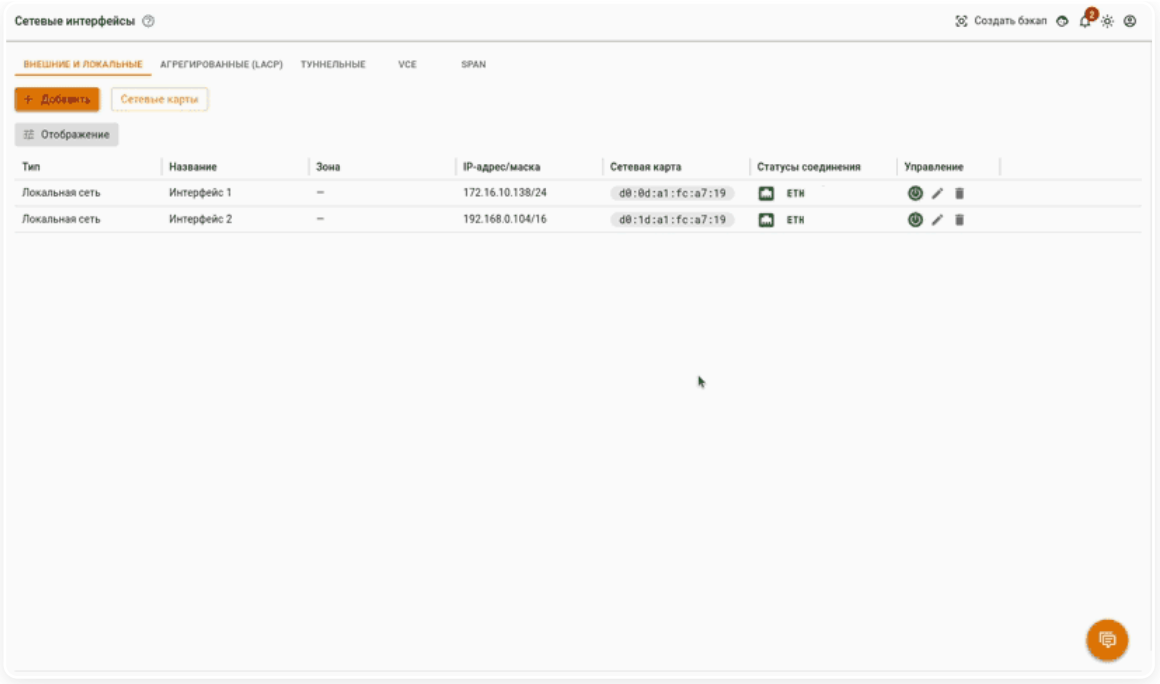
- IP-адрес назначен

- Соединение с интернетом установлено

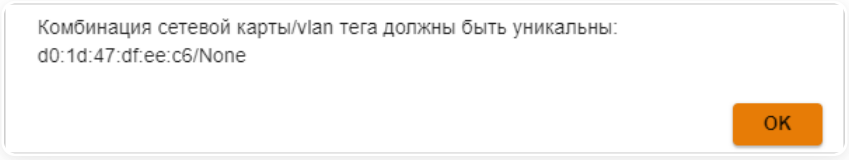
- Соединение с интернетом отсутствует

Редактирование сетевых интерфейсов

В режиме редактирования доступно изменение названия, сетевой карты (по кнопке), зоны, индекса интерфейса для Netflow и настроек конфигурации (вручную или автоматически):



Если сетевая карта уже используется каким-либо интерфейсом, то NGFW выведет окно с ошибкой:



При создании, редактировании или удалении сетевого интерфейса перевыпускается SSL-сертификат, поэтому вероятно снижение скорости работы веб-интерфейса Ideco NGFW. В этом случае рекомендуем нажать F5.

Миграция NGFW

При миграции NGFW с одной физической машины на другую (перенос диска или восстановление бэкапа на новом оборудовании), будут восстановлены настройки всех сетевых интерфейсов, указанные до миграции. Для удаления ненужных интерфейсов воспользуйтесь кнопкой .

Например: исходная версия NGFW 17.X → провели миграцию NGFW на новое оборудование → настроили новое оборудование → провели обновление → в разделе Сетевые интерфейсы будут отображаться старые (до миграции) и новые (после миграции и настройки) сетевые интерфейсы.

Ограничения сетевых интерфейсов

В зависимости от объема оперативной памяти на сервере в Ideco NGFW есть ограничения на количество сетевых интерфейсов:

- Количество сетевых интерфейсов (не VLAN):
  - до 16 ГБ - **40 сетевых интерфейсов**.
- Количество сетевых VLAN-интерфейсов:
  - до 8 ГБ - **14 VLAN-интерфейсов**;
  - от 8 до 16 ГБ - **33 VLAN-интерфейса**;
  - 16 ГБ и более - **66 VLAN-интерфейсов**.

При создании большего количества VLAN-интерфейсов могут возникнуть проблемы в работе Контроля приложений и Ограничения скорости.

В Ideco NGFW нет подразделения локальных интерфейсов на VPN-интерфейсы и Ethernet, поскольку Ideco NGFW не содержит локальных VPN-интерфейсов.

Внешние и локальные интерфейсы

На вкладке **Внешние и локальные** настраиваются Ethernet-интерфейсы:

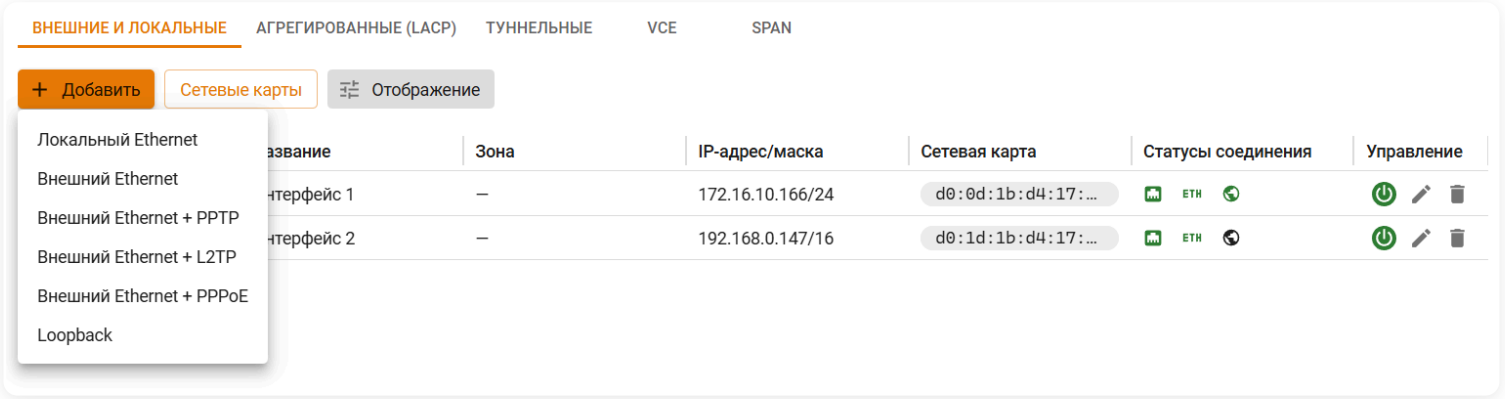
- **Локальный Ethernet** - настройка локальной сети.
- **Внешний Ethernet** - настройка подключения к интернету. Как правило, вся необходимая информация для настройки содержится в договоре с интернет-провайдером.
- **Подключение по PPTP** (Point-to-Point Tunneling Protocol) - один из старейших VPN-протоколов, разработанный для обеспечения защищенного доступа через интернет. Основан на использовании протокола PPP (Point-to-Point Protocol) для аутентификации и шифрования данных.
- **Подключение по L2TP** - подключение с применением протокола L2TP иногда используется интернет-провайдерами в целях обеспечения более надежной авторизации.
- **Подключение по PPPoE** - подключение с применением протокола PPPoE традиционно используется провайдерами, предлагающими подключение через xDSL.
- **Loopback-интерфейс** - виртуальный интерфейс, который может использоваться для динамической маршрутизации (BGP и OSPF), удаленного администрирования и подключения пользователей по VPN. Преимущество Loopback-интерфейса в том, что он никогда не перестанет работать, пока его не отключат административно.

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 считаются локальными и не подлежат публичной маршрутизации в интернете.
Для настройки внешних и локальных интерфейсов нажмите **Добавить**:



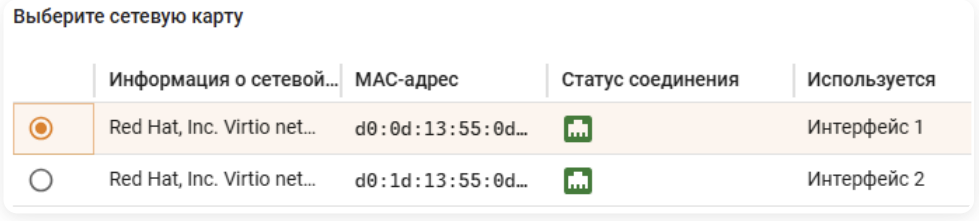
Выберите нужный интерфейс и следуйте инструкции:

Локальный Ethernet

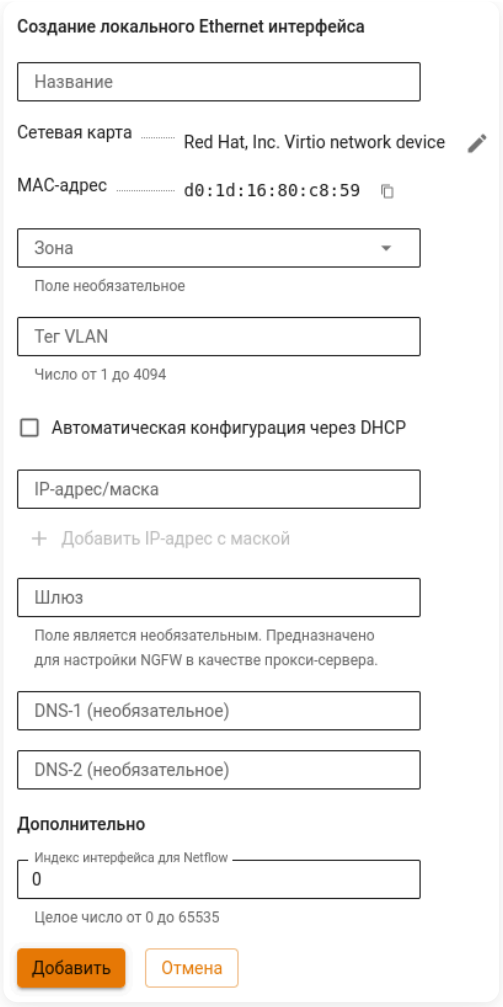
Ручная настройка

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название интерфейса** - имя для идентификации интерфейса.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Тег VLAN** - VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется в том случае, если сетевая карта уже используется.
- **Автоматическая настройка через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Как минимум, должен быть указан хотя бы один IP-адрес.
- **Шлюз** - IP-адрес шлюза.
- **DNS** - доступно два поля для указания DNS сервера (необязательно).
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

При выборе пункта **Локальный Ethernet** и заполнении поля **Шлюз** доступ в интернет будет отсутствовать.

Поле **Шлюз** в Локальном интерфейсе задается только если:

- Нет Внешнего интерфейса NGFW;
- NGFW используется как прокси-сервер.

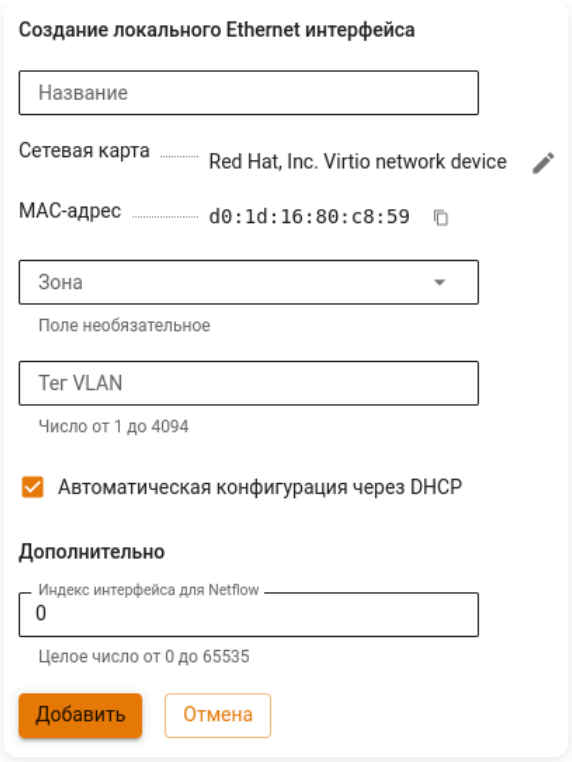
3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Автоматическая настройка

Используется, если ваш интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

1. Выберите сетевую карту.

2. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется:



3. При необходимости выберите объект типа **Зона** в одноименном поле.

4. Включите настройку **Автоматическая конфигурация через DHCP**.

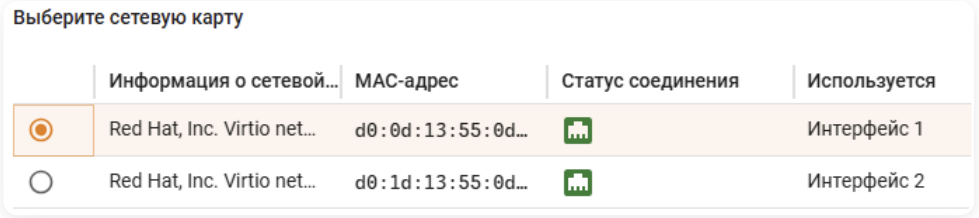
5. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Внешний Ethernet

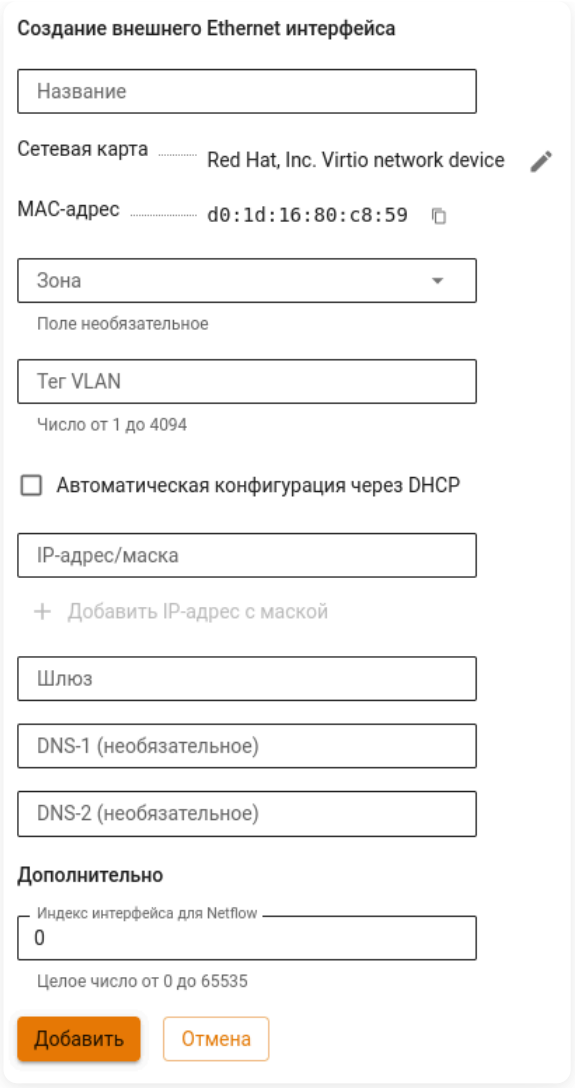
Ручная настройка

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название интерфейса** - имя, с помощью которого возможно в дальнейшем идентифицировать интерфейс.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется только в том случае, если сетевая карта уже используется.
- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес.
- **Шлюз** - укажите IP-адрес шлюза интернет-провайдера, через который будет осуществляться подключение к сети интернет.
- **DNS** - доступно два поля для указания DNS-сервера (необязательно).
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Автоматическая настройка

Используется, если интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

1. Выберите сетевую карту.

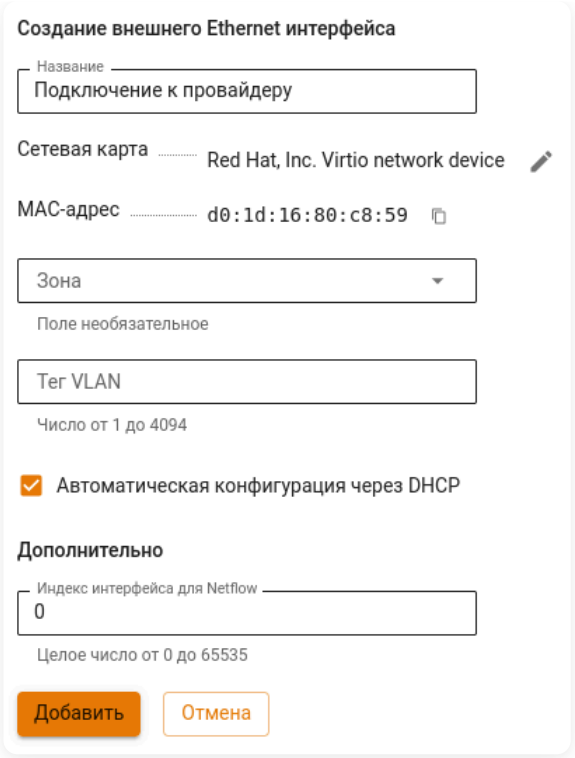
2. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется.

3. При необходимости выберите объект типа **Зона** в одноименном поле.

4. Включите настройку **Автоматическая конфигурация через DHCP**.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Пример настройки:



Подключение по 3G и 4G

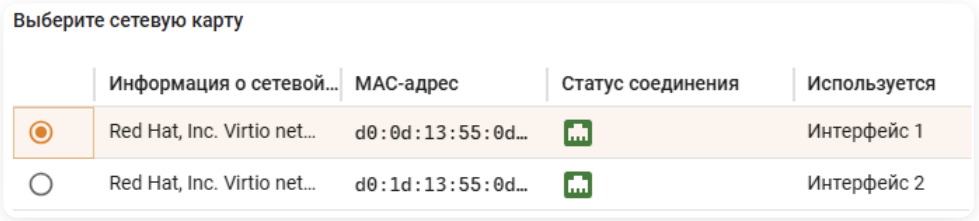
Сервер Ideco NGFW поддерживает некоторые модели USB-модемов, например, **Huawei E8372**. При подключении USB-модем будет отображаться в Ideco NGFW как новый ethernet-интерфейс.

Ideco NGFW поддерживает модели USB-модемов с Network Communication типа **CDC-Ethernet**. Список таких модемов представлен в таблице Список поддерживаемых USB-модемов.

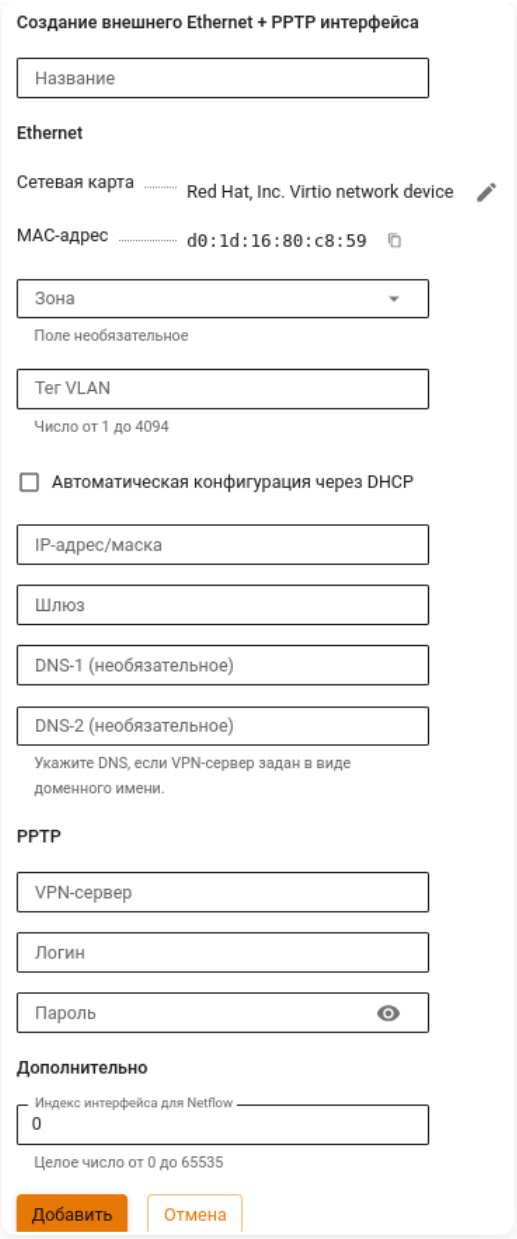
PPTP

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



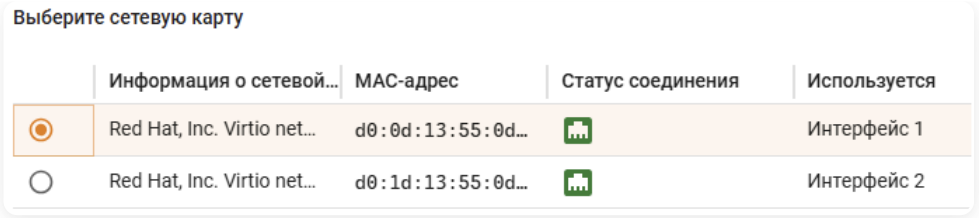
- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q.
- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес.
- **Шлюз** - IP-адрес шлюза.
- **DNS** - доступно два поля для указания DNS-сервера (необязательно).
- **VPN-сервер** - IP-адрес или доменное имя PPTP-сервера.
- **Логин** - имя пользователя для подключения по PPTP.
- **Пароль** - пароль для подключения по PPTP.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

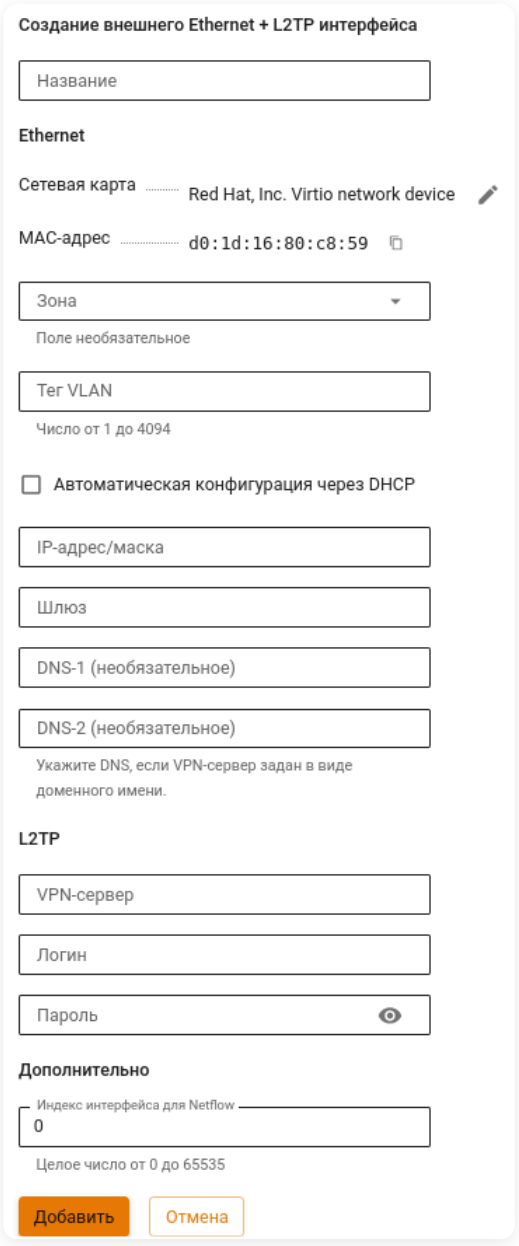
L2TP

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае если сетевая карта уже используется. Стандарт VLAN 802.3q.
- **Автоматическая конфигурация через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес.
- **Шлюз** - IP-адрес шлюза.
- **DNS** - доступно два поля для указания DNS-сервера (необязательно).
- **VPN-сервер** - IP-адрес или доменное имя L2TP-сервера.
- **Логин** - имя пользователя для подключения по L2TP.
- **Пароль** - пароль для подключения по L2TP.

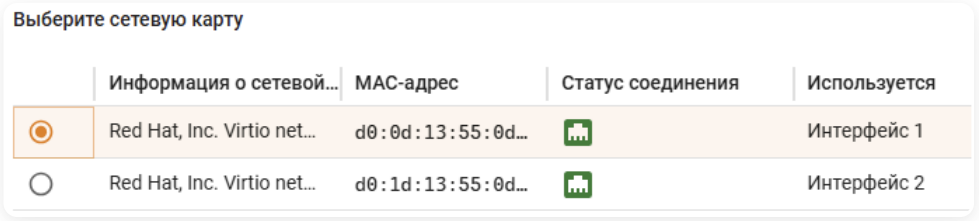
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

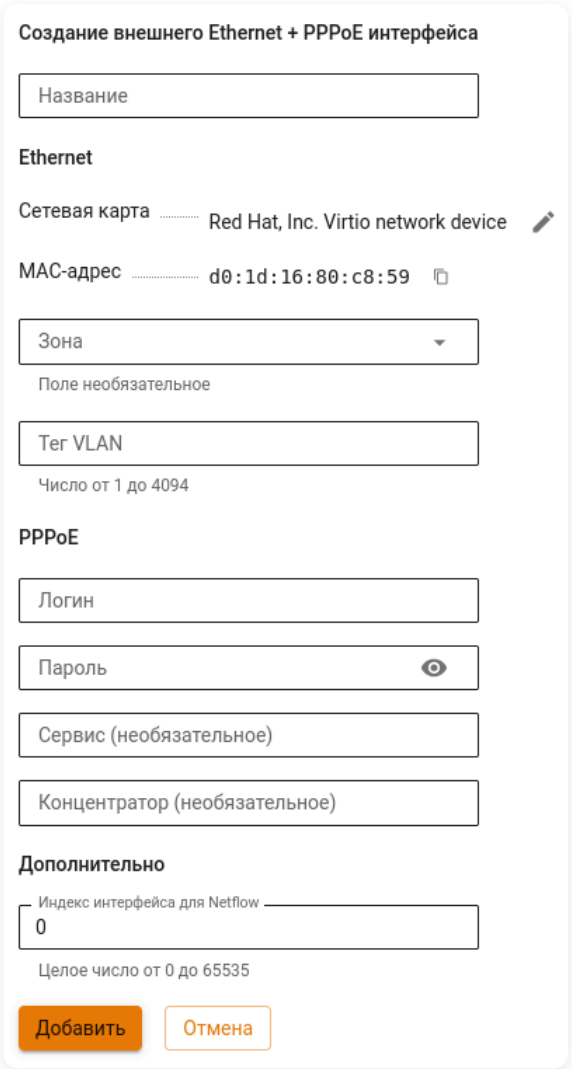
PPPoE

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q.
- **Логин** - имя пользователя для подключения по PPPoE.
- **Пароль** - пароль 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.

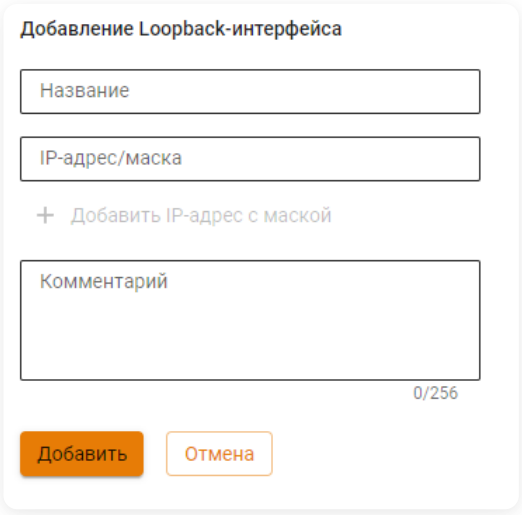
3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

При подключении к провайдеру с использованием протокола PPPoE настройте DNS-сервер вручную, воспользовавшись статьей.

Loopback

> Нельзя создавать Loopback-интерфейс в настроенном кластере. Если все же требуется использовать Loopback-интерфейс, настройте его до объединения в кластер.

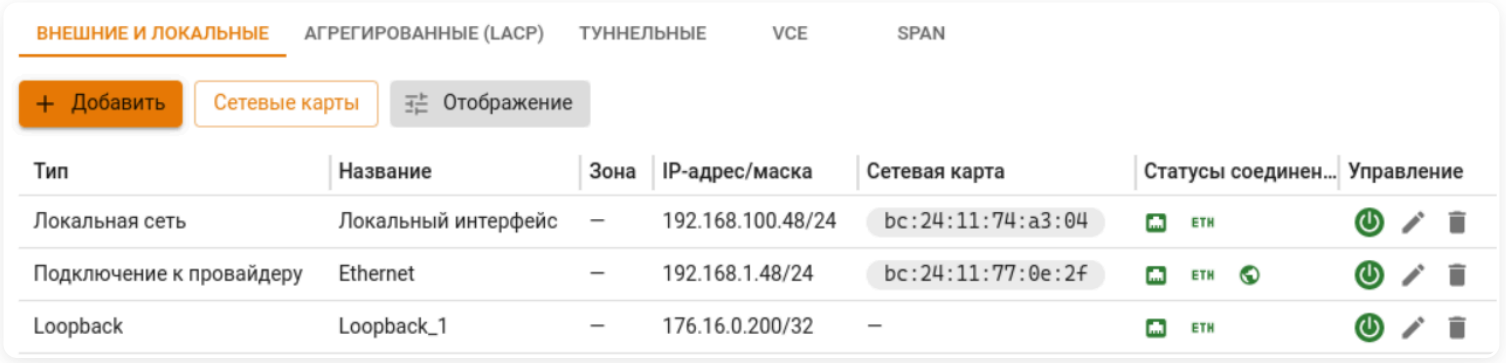
1. Заполните поля:



- **Название** - введите название интерфейса;
- **IP-адрес/маска** - введите IP-адрес, который требуется назначить на Loopback-интерфейс, с маской в формате `x.x.x.x/x`;
- **Комментарий** - поле не обязательное.

> 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`

2. Нажмите **Добавить**. Loopback-интерфейс появится в таблице внешних и локальных интерфейсов:



Особенности настройки Loopback-интерфейса

При работе с Loopback-интерфейсом используйте правила:

- Для доступа к веб-интерфейсу Ideco NGFW 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 **Файрвола** в поле **Адрес назначения** укажите IP-адрес, назначенный на Loopback-интерфейс. Опубликованные ресурсы будут доступны по IP-адресу Loopback-интерфейса.
- При создании SNAT-правила **Файрвола** 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.

Агрегированные интерфейсы

LACP-интерфейсы (Link Aggregation Control Protocol) - протокол, предназначенный для объединения нескольких физических каналов в один логический в сетях Ethernet.

Особенности работы агрегированных интерфейсов

Агрегированные каналы LACP используются как для повышения пропускной способности, так и для повышения отказоустойчивости.

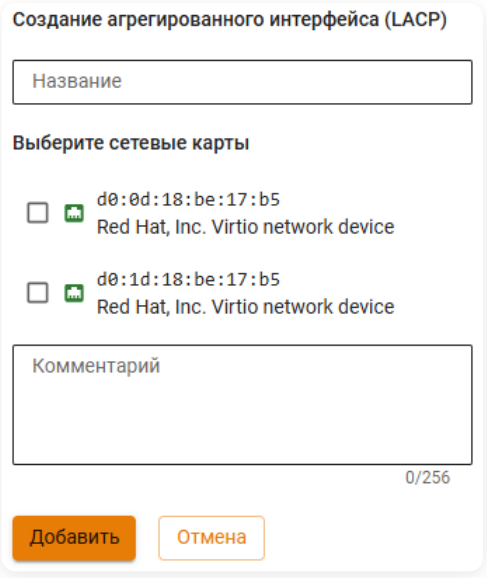
Не рекомендуем использовать **LACP** на виртуальных сетевых адаптерах, так как системы виртуализации некорректно обрабатывают работу **LACP** на таких интерфейсах или вовсе не поддерживают этот режим.

Особенности работы LACP-интерфейсов:

- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active** режим - постоянная рассылка LACP пакетов.
- Проверка соседства осуществляется в режиме **slow** - раз в 30 секунд.
- Количество сетевых карт, объединяемых в агрегированный интерфейс, не ограничено.
- Нельзя добавлять в VCE LACP-интерфейсы и логические VLAN-интерфейсы, созданные на агрегированном интерфейсе.
- Нельзя добавлять LACP-интерфейсы в кластерном режиме.

Настройка агрегированного интерфейса

Чтобы объединить несколько сетевых интерфейсов в один агрегированный, перейдите в **Сервисы** → **Сетевые интерфейсы** → **Агрегированные (LACP)**, нажмите **Добавить** и выполните действия:



1. Укажите название для последующей идентификации интерфейса.

2. Выберите сетевые карты.

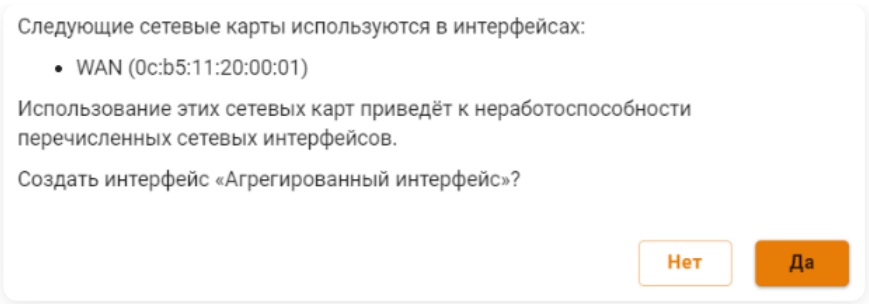
3. Нажмите **Добавить**.

Статусы сетевых карт

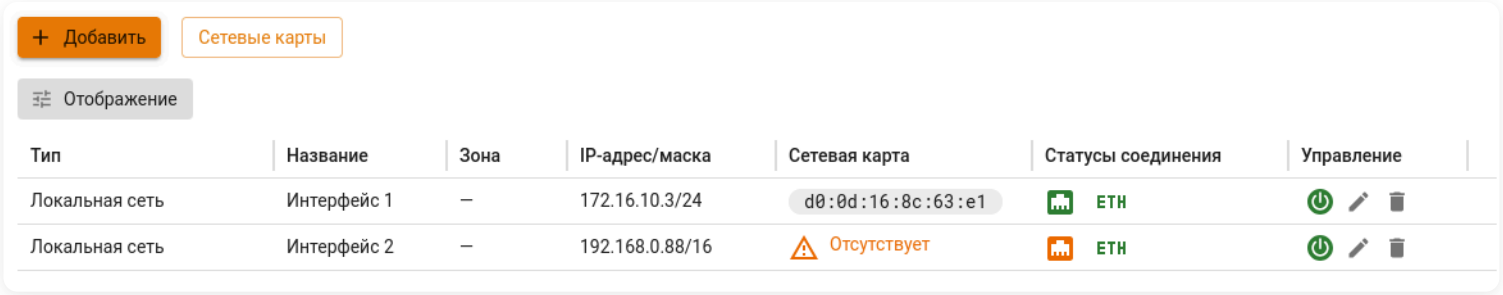
- Сетевая карта уже используется другим интерфейсом

- Сетевая карта не используется

Если были выбраны уже использующиеся сетевые карты, то при нажатии на кнопку **Добавить** появится сообщение:

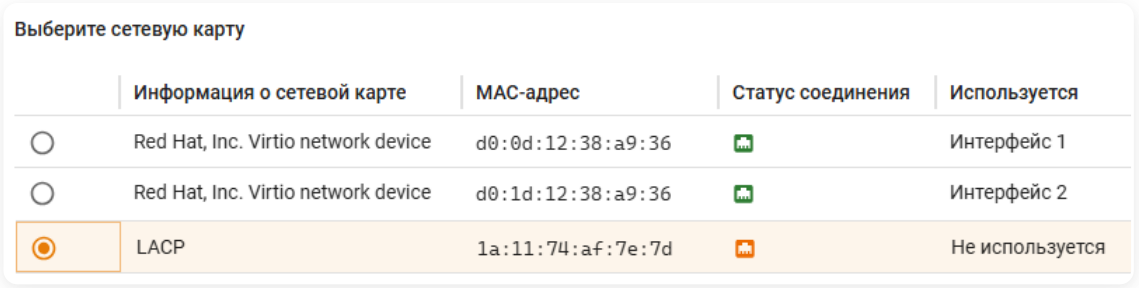


При выборе **Да** сетевая карта будет использоваться агрегированным интерфейсом и станет недоступна для ранее созданного сетевого интерфейса:



Создание логического интерфейса

На основе созданного агрегированного интерфейса можно добавить любой логический интерфейс, в том числе с указанием VLAN. Для этого перейдите в **Сервисы** → **Сетевые интерфейсы** → **Внешние и локальные** и создайте Ethernet-интерфейс, выбрав в качестве сетевой карты добавленный на предыдущем шаге LACP-интерфейс:

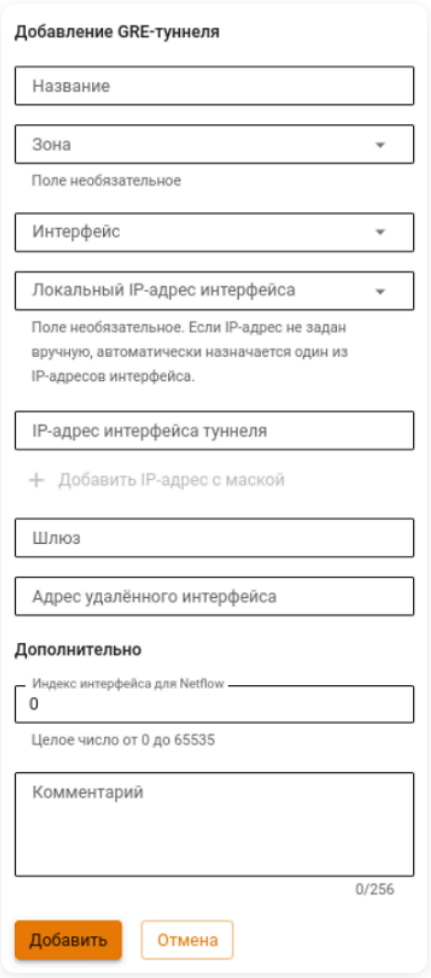


Туннельные интерфейсы

GRE-туннель - это соединение точка-точка с возможностью передавать широковещательный трафик. На таких интерфейсах может работать протокол динамической маршрутизации OSPF. Пакеты, проходящие внутри GRE, не шифруются.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе Туннельные. 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 добавления GRE-туннеля нажмите **Добавить**, заполните поля и нажмите **Добавить**:



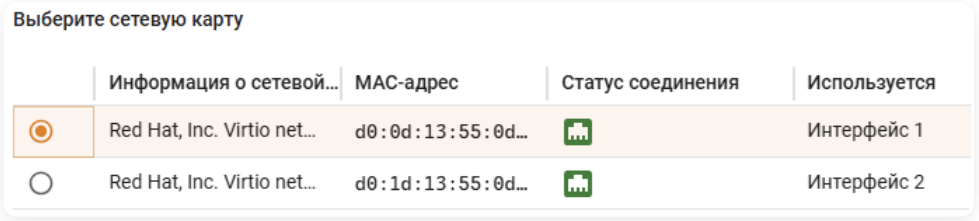
- **Название** - введите название туннельного интерфейса.
- **Зона** - выберите объект типа **Зона**, в состав которого будет входить создаваемый туннельный интерфейс. Список предустановленных зон приведен в статье.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение.
- **Локальный IP-адрес интерфейса** - укажите IP-адрес родительского интерфейса запущенного туннеля.
- **Адрес удаленного интерфейса** - укажите IP-адрес интерфейса для подключения.
- **IP-адрес/маска** - 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** - необязательное поле.

VCE-интерфейсы

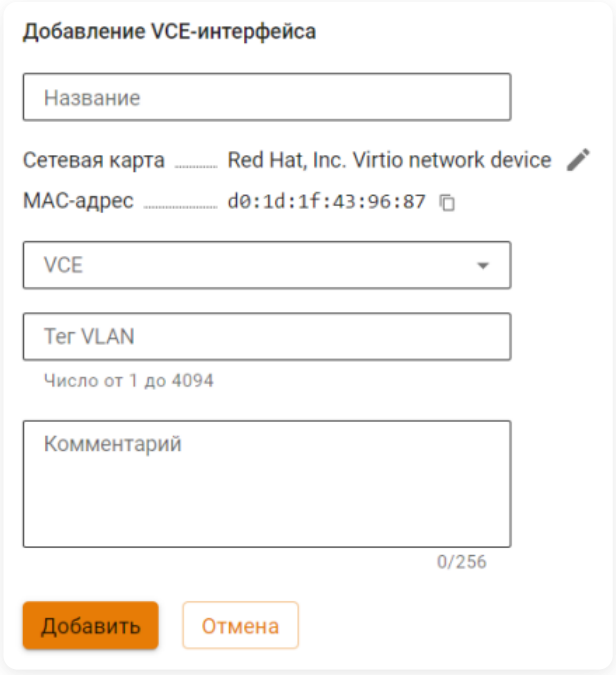
В Ideco NGFW есть возможность пробросить сетевые карты и VLAN-интерфейсы Ideco NGFW в виртуальные серверы, созданные в разделе **Управление сервером** → **VCE**.

Чтобы назначить сетевую карту или VLAN-интерфейс VCE, нажмите **Добавить** и выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название** - введите название VCE-интерфейса;
- **VCE** - выберите из списка VCE, созданный в разделе **Управление сервером** → **VCE**;
- **Тег VLAN** - если нужно пробросить в VCE порт сетевой карты, оставьте поле пустым. Если нужно пробросить только VLAN, укажите тег VLAN - число от 1 до 4094;
- **Комментарий** - поле может быть пустым.

Не присваивайте VCE сетевые карты, которые используются корневым NGFW, без указания тега VLAN. В противном случае доступ к веб-интерфейсу NGFW будет потерян.

3. Нажмите **Добавить**.

При наличии большого количества VCE-интерфейсов в таблице воспользуйтесь кнопкой **Фильтры**.

По кнопке **Сетевые карты** доступны все сетевые карты корневого VCE, еще не проброшенные в дочерние VCE.

Переданная VCE сетевая карта будет недоступна для использования корневым NGFW. Также невозможно будет назначить эту карту другому VCE без указания тега VLAN.

SPAN-интерфейсы

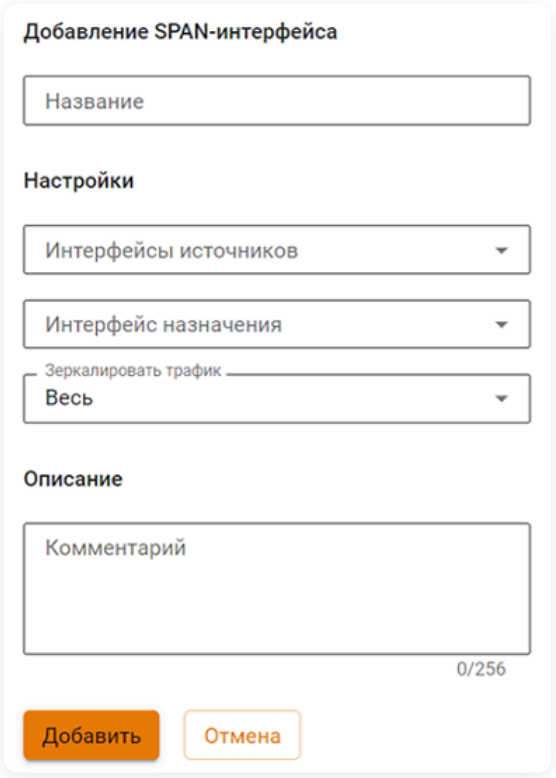
SPAN (Switch Port ANalyzer) - функция, позволяющая копировать пакеты с порта или группы портов коммутатора или маршрутизатора (порт зеркалирования) и отправлять на выбранный порт (порт мониторинга). В Ideco NGFW SPAN-интерфейс позволяет дублировать трафик локальных и внешних интерфейсов на отдельное внешнее устройство для его мониторинга, анализа и выявления угроз.

SPAN-интерфейс должен быть свободным Ethernet-интерфейсом, не используемым для других целей.

Чтобы создать SPAN-интерфейс, выполните действия:

1. Перейдите в раздел **Сервисы** → **Сетевые интерфейсы** → **SPAN** и нажмите **Добавить**.

2. Заполните поля:



- **Название** - введите название SPAN-интерфейса;
- **Интерфейсы источников** - выберите интерфейсы, трафик которых хотите дублировать. Доступные варианты: Ethernet (как внешние, так и локальные, за исключением PPPoE, L2TP и PPTP), VLAN, а также клиентский VPN-трафик;
- **Интерфейс назначения** - выберите интерфейс, на который будет дублироваться трафик;

Не указывайте в полях **Интерфейс источника** и **Интерфейс назначения** интерфейсы Ethernet + L2TP/PPTP/PPPoE. Этот тип интерфейсов не поддерживается в настройках SPAN.

- **Зеркалировать трафик** - выберите тип трафика, который хотите дублировать. Доступные варианты: Весь, Только входящий или Исходящий;
- **Комментарий** - поле может быть пустым.

3. Нажмите **Добавить**.

SPAN-интерфейс может быть перегружен при большом количестве наблюдаемых интерфейсов.

Балансировка и резервирование

Название службы раздела **Балансировка и резервирование**: `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

При наличии нескольких подключений к интернет-провайдерам балансировку и резервирование можно осуществлять следующими способами:

- **Резервирование** - при отключении основного интерфейса трафик будет направлен через все доступные.
- **Статическая балансировка** - трафик между несколькими подключениями будет разделен согласно правилам маршрутизации.
- **Динамическая балансировка** - подключения будут поочередно переключаться в зависимости от нагрузки, при этом сессии пользователей будут равномерно распределяться между доступными подключениями.

Перед настройкой резервирования каналов, динамической и статической балансировки, убедитесь, что на сервере созданы минимум два подключения к интернету. Если подключение одно, создайте дополнительное. Подробнее - в статье Внешние и локальные интерфейсы.

Если на внешний интерфейс назначено более одного IP-адреса, то при использовании режимов балансировки и резервирования будет использоваться IP-адрес, выбранный случайным образом при запуске Ideco NGFW.

Для балансировки и резервирования в Ideco NGFW важно учитывать настройки маршрутизации и NAT.

Практические последствия неправильной настройки:

- Нарушение балансировки трафика между каналами из-за некорректных маршрутов.
- Проблемы с возвратом пакетов при использовании NAT без учета маршрутов.
- Потеря резервирования каналов при неправильной настройке приоритетов.
- Снижение производительности сети из-за неоптимальных путей прохождения трафика.

Правильная настройка маршрутизации и NAT позволяет эффективно использовать возможности Ideco NGFW по балансировке и резервированию трафика, обеспечивая высокую доступность и производительность сетевой инфраструктуры.

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Основное

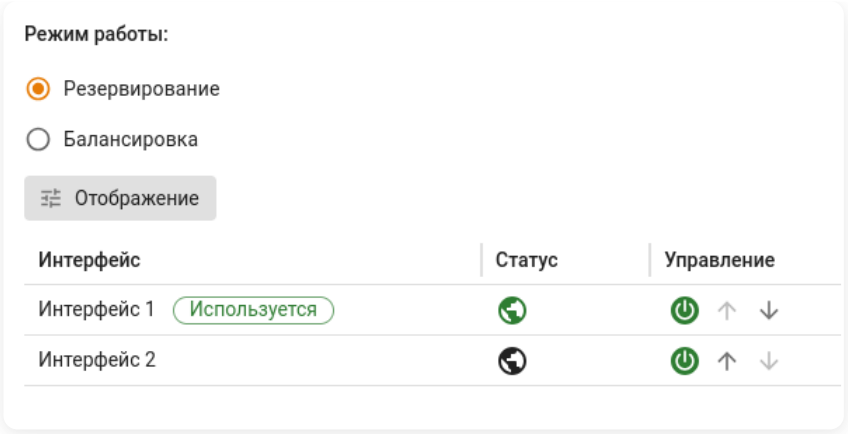
На вкладке доступен выбор режимов - **Балансировка** или **Резервирование**.

При **Резервировании** Ideco NGFW использует каналы в соответствии с их приоритетом. Приоритет задается порядком подключений в таблице, сверху вниз. Если интернет стал недоступен через используемое подключение, то Ideco NGFW будет перебирать подключения сверху вниз до первого активного.

При **Балансировке** Ideco NGFW балансирует трафик в зависимости от загрузки подключений.

Резервирование каналов

Перейдите в раздел **Сервисы** → **Балансировка и резервирование** и выберите режим **Резервирование**.



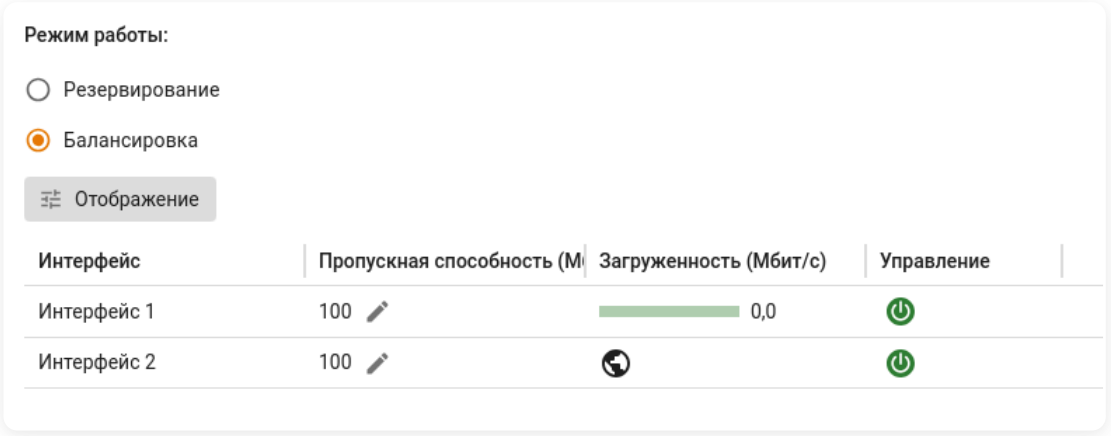
Подключение, которое используется в данный момент, отмечено тегом **Используется**. Для смены приоритета используйте соответствующие элементы управления ( ).

Динамическая балансировка. Распределение нагрузки по нескольким подключениям

Действия для настройки:

1. Перейдите в раздел **Сервисы** → **Балансировка и резервирование**.

2. Выберите режим работы **Балансировка**.



Для равномерного распределения сессий между подключениями необходимо указать значение **Пропускной способности** - максимальной скорости интернета по тарифам провайдеров. Ideco NGFW будет автоматически балансировать трафик в зависимости от загрузки подключений.

Трафик балансируется автоматически без дополнительных настроек, включая тарфик прокси-сервера.

Статическая балансировка. Доступ к сети интернет через определенное подключение к провайдеру

Способы применения:

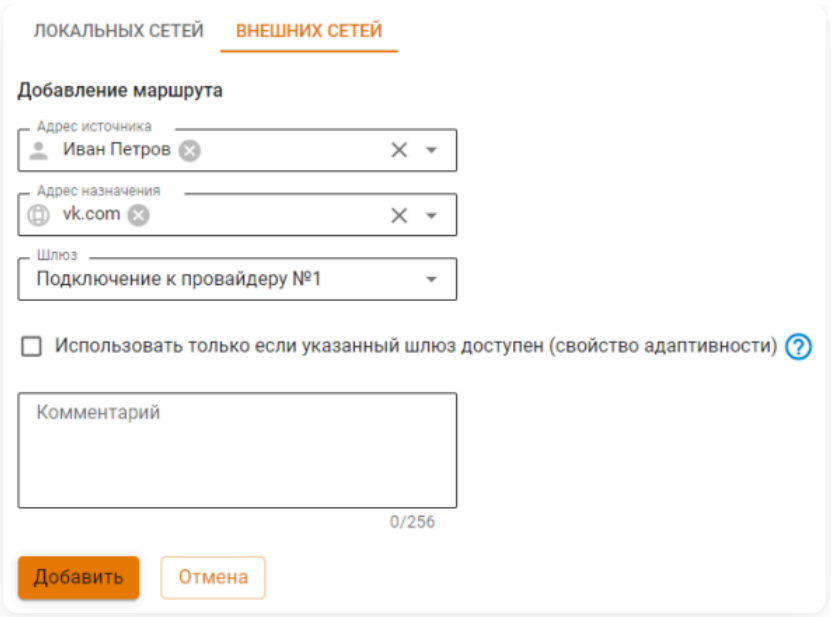
- Направление части трафика через интернет-провайдера, чья тарификация для этого трафика дешевле.
- Предоставление доступа к внутренним сетям одного из провайдеров для определенных пользователей/групп пользователей.

Действия для настройки:

1. Перейдите в раздел меню **Сервисы** → **Маршрутизация** → **Внешних сетей**.

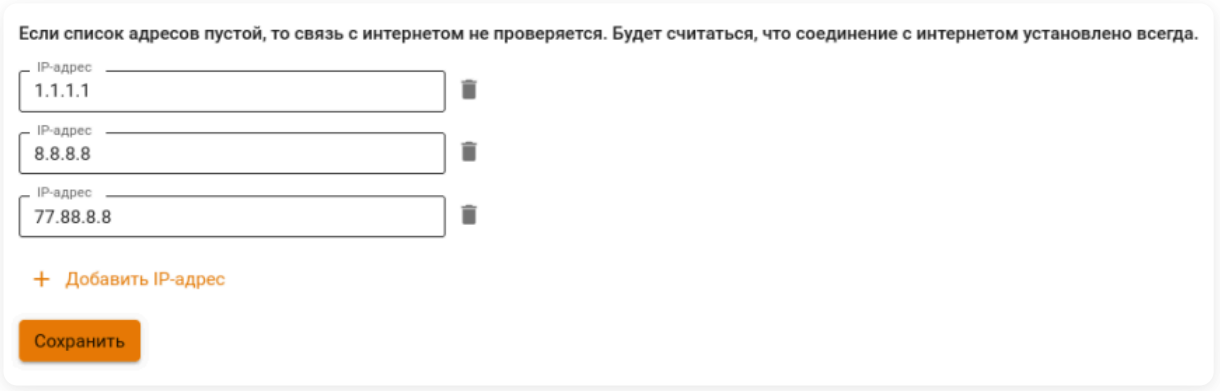
2. Добавьте правила маршрутизации для определенного списка ресурсов, трафик к которым необходимо направить через нужное подключение к провайдеру, нажав кнопку **Добавить**.

Пример направления трафика к ресурсу **vk.com** от пользователя **Иван Петров** через подключение к провайдеру **Подключение к провайдеру №1**:



Адреса для проверки связи

На вкладке задаются IP-адреса, которые Ideco NGFW будет использовать для проверки связи с интернетом. По умолчанию заданы три IP-адреса - DNS-серверы Cloudflare, Google и Яндекс:



Ideco NGFW посылает на эти адреса ping-запросы. Соединение с интернетом считается установленным, если проходит пинг хотя бы до одного адреса из списка. Если этого не происходит, Ideco NGFW считает, что соединение с интернетом у интерфейса отсутствует - статус интерфейса меняется с на . Полный цикл проверки, включая определение доступности нового шлюза после изменения настроек, занимает до 30 секунд.

Если список IP-адресов пуст, проверка интернет-соединения не выполняется. NGFW считает, что интернет всегда доступен. В этом случае:

- Режим **Резервирование** не будет работать.
- Режим **Балансировка** будет работать некорректно, если на одном из интерфейсов отсутствует интернет.

Маршрутизация

Название службы раздела **Маршрутизация**: `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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.
- Автоматически переключаться на альтернативный маршрут при недоступности шлюза или интерфейса (адаптивность).
- Обеспечить корректную доставку как исходящего, так и ответного трафика.

Доступность шлюза проверяется с помощью отправки ARP-запроса на получение MAC-адреса для IP, указанного в качестве шлюза.

В веб-интерфейсе Ideco NGFW есть возможность маршрутизировать локальные и внешние сети. Создавать и редактировать маршруты можно в разделе **Сервисы → Маршрутизация**.

Для организации доступа в удаленные сети через роутер в локальной сети читайте статью по ссылке.

При маршрутизации локальных и внешних сетей доступны GRE-интерфейсы в качестве шлюза.

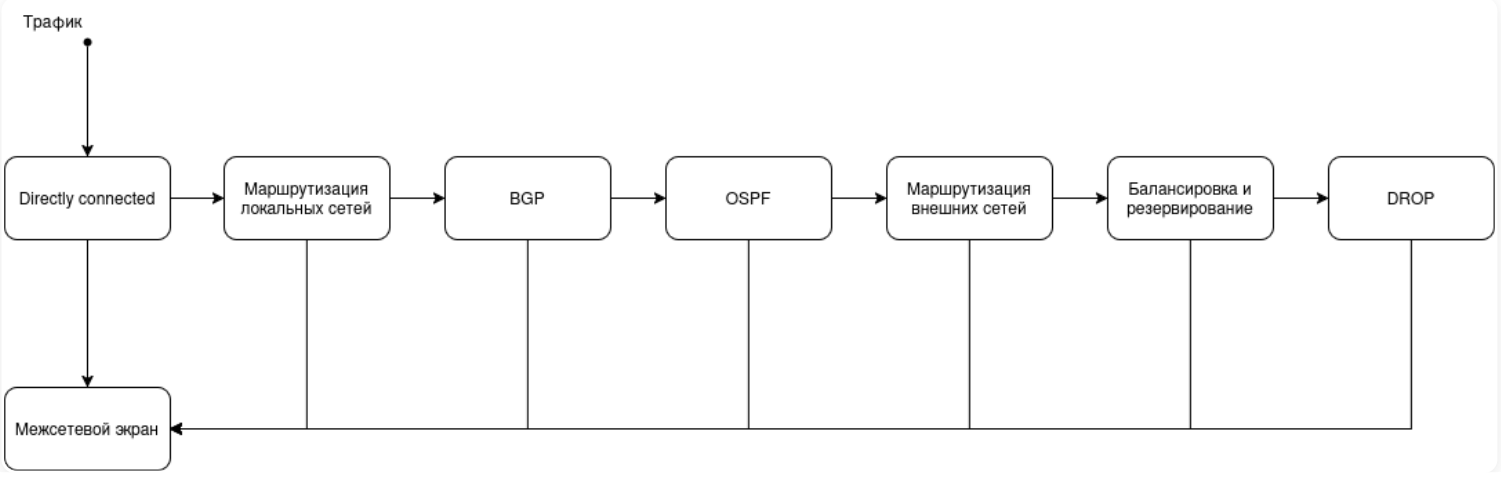
Обработка трафика

В процессе маршрутизации пакет проходит через несколько последовательных этапов:

- Если маршрут найден на каком-либо из этапов, пакет передается в модуль фильтрации **Межсетевой экран**.
- Если маршрут не найден, поиск продолжается в таблицах следующего блока.

После определения маршрута результат маршрутизации сохраняется. Путь пакета фиксируется и не изменяется при последующей обработке.

Этапы обработки пакета



1. **Directly connected** - проверяется, принадлежит ли адрес назначения одной из локально доступных подсетей.

2. **Маршрутизация локальных сетей** - выполняется поиск маршрута в таблицах маршрутизации локальных сетей.

3. **BGP** - выполняется поиск маршрута в таблице динамического протокола BGP.

4. **OSPF** - выполняется поиск маршрута в таблице динамического протокола OSPF.

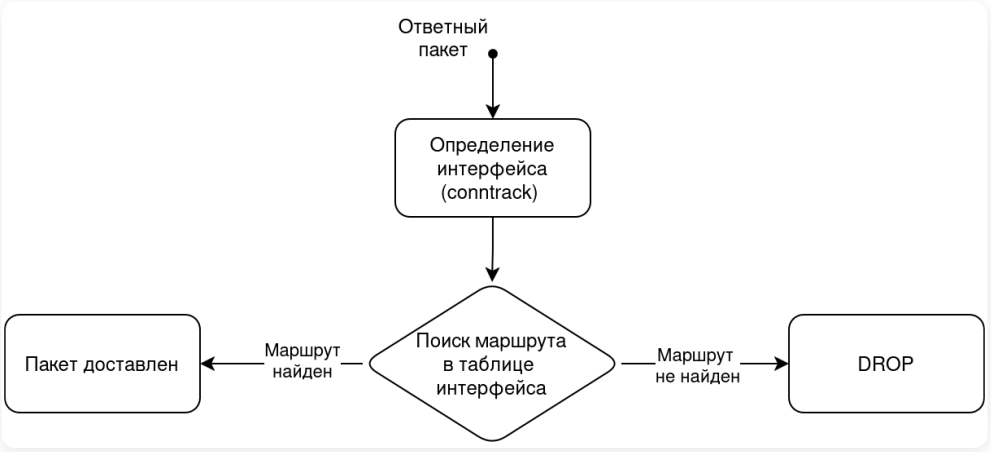
5. **Маршрутизация внешних сетей** - используются политики маршрутизации, определяющие, по каким условиям (например, по источнику или интерфейсу) будет направляться сетевой трафик. В соответствии с найденной политикой пакет перенаправляется на указанный маршрут. В качестве одного из вариантов действия правила может быть перенаправление в **Балансировку и резервирование**.

6. **Балансировка и резервирование** - выполняется распределение трафика между несколькими шлюзами или выбор резервного маршрута.

В маршрутизации **Внешних сетей** 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.

Настройка маршрутизации

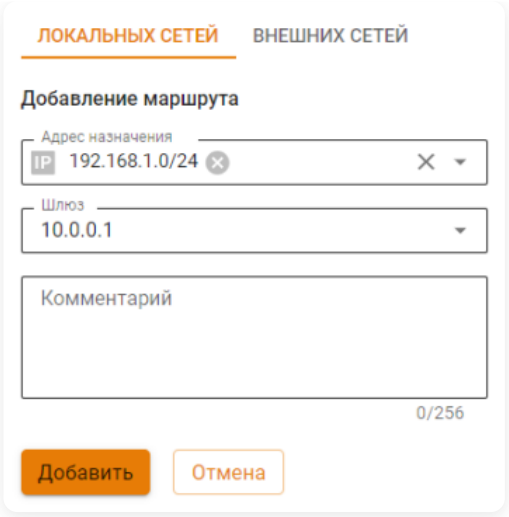
Маршрутизация локальных сетей

Для маршрутизации локальных сетей при добавлении маршрута отсутствует поле **Адрес источника**, так как сеть внутренняя.

Для добавления нового маршрута:

1. Перейдите в раздел **Сервисы** → **Маршрутизация** → **Локальных сетей** и нажмите **Добавить**.

2. Заполните поля:



- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться правило. Возможные типы объектов: IP-адрес, подсеть, домен, список IP-объектов, диапазон IP-адресов.
- **Шлюз** - выберите объект, через который направляется трафик. Возможные типы объектов: IP-адрес, пользователь.
- **Комментарий** - необязательное поле описания маршрута. Значение не должно быть длиннее 128 символов.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

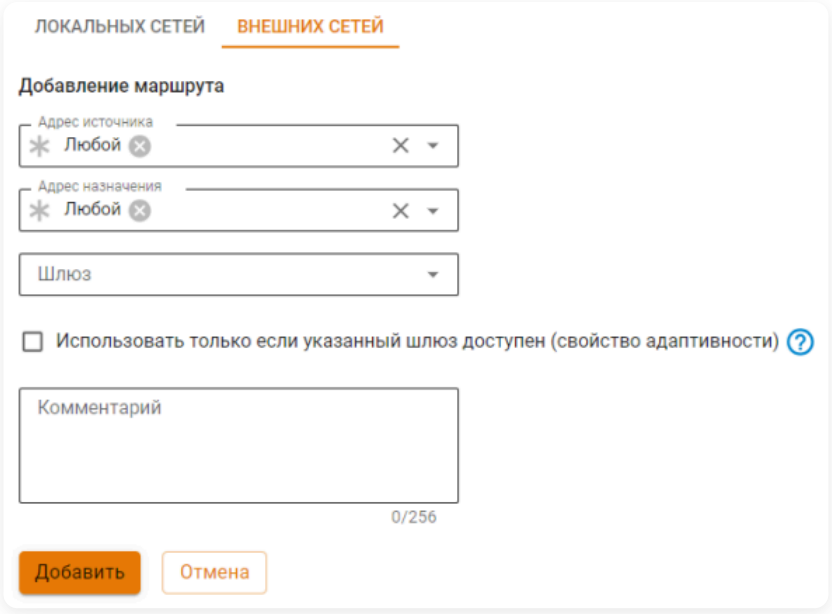
При создании IPsec-подключения в разделе **Сервисы** → **IPsec** с включенной опцией **Автоматическое создание маршрутов** будут добавляться маршруты до локальных сетей Ideco NGFW в таблицу **Маршрутизации локальных сетей**.

Маршрутизация внешних сетей

Для добавления нового маршрута:

1. Перейдите в раздел **Сервисы** → **Маршрутизация** → **Внешних сетей** и нажмите кнопку **Добавить**.

2. Заполните поля:

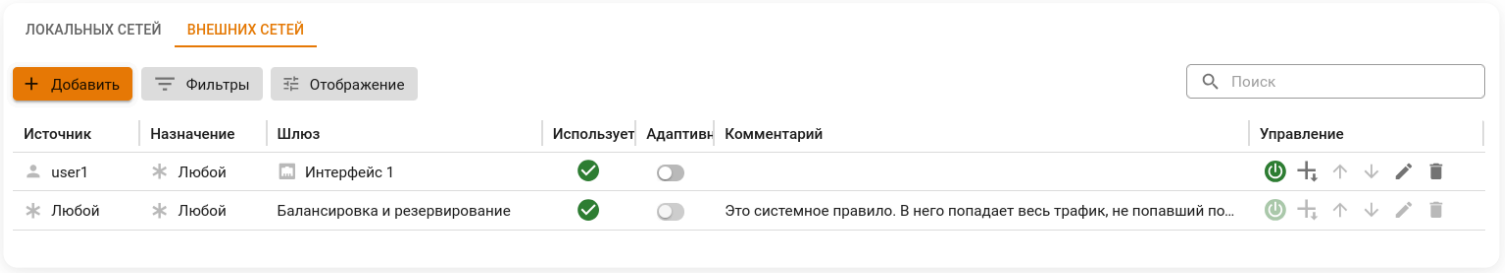


- **Адрес источника** - выберите объекты, для которых будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен.
- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен.
- **Шлюз** - выберите объект, через который будет направлен трафик. Возможные типы объектов: сетевой интерфейс, IP-адрес.
- **Использовать только если указанный шлюз доступен (свойство адаптивности)** - если свойство включено, то при недоступности шлюза или интерфейса поиск маршрута продолжится по следующим правилам маршрутизации. Если свойство отключено (по умолчанию), то трафик

отправляется в выбранный шлюз или интерфейс. Если шлюз недоступен или интерфейс не работает, то трафик будет отброшен (destination unreachable).

- **Комментарий** - необязательное поле описания маршрута. Значение не должно быть длиннее 128 символов.

После сохранения маршрута страница выглядит так:



Кнопки ↓ и ↑ повышают или понижают приоритет правила.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

Статусы в столбце **Используется**:

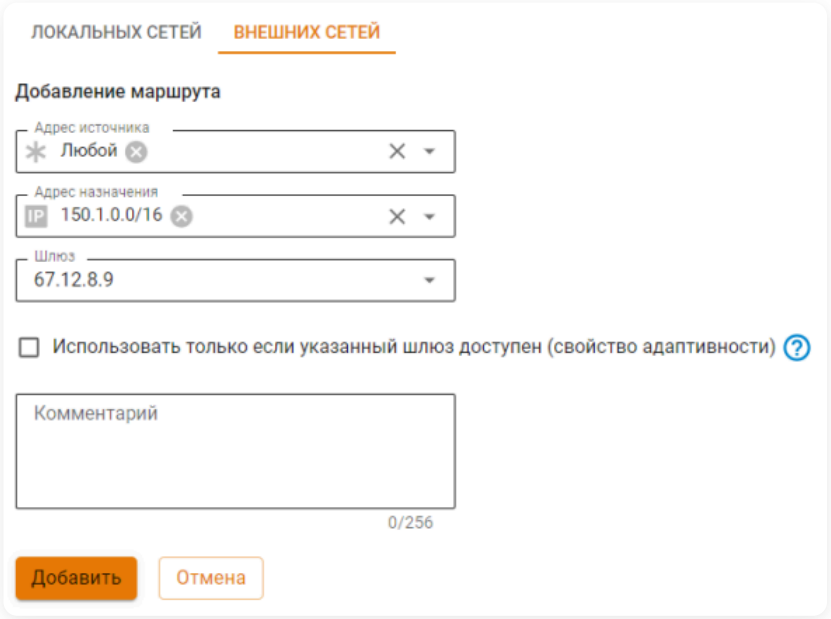
- маршрут активен и трафик, попадающий под условия маршрута, будет перенаправлен в указанный **Шлюз**;
- маршрут не активен и трафик, попадающий под условия маршрута, не будет обработан правилом.

Трафик, не попавший под условия правил маршрутизации, или с объектом **Любой** в качестве шлюза, будет отправлен в Балансировку и резервирование.

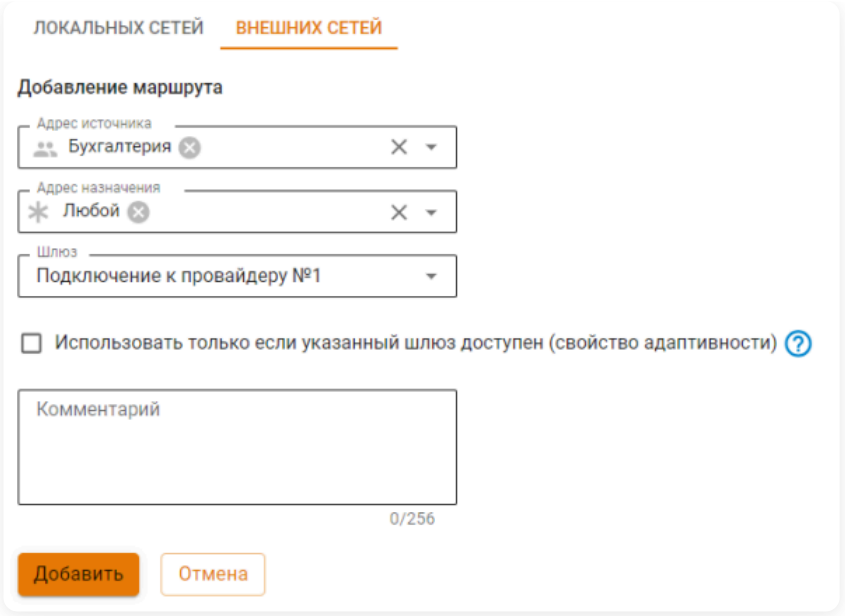
Примеры популярных маршрутов

При маршрутизации трафика через подключения к провайдеру важно понимать, что чаще всего одного маршрута недостаточно. Понадобится также переопределить адрес с помощью SNAT, иначе такой маршрут не будет работать. SNAT можно настроить с помощью Файрвола.

Задача: любой трафик в подсеть 150.1.0.0/16 направлять на шлюз 67.12.8.9



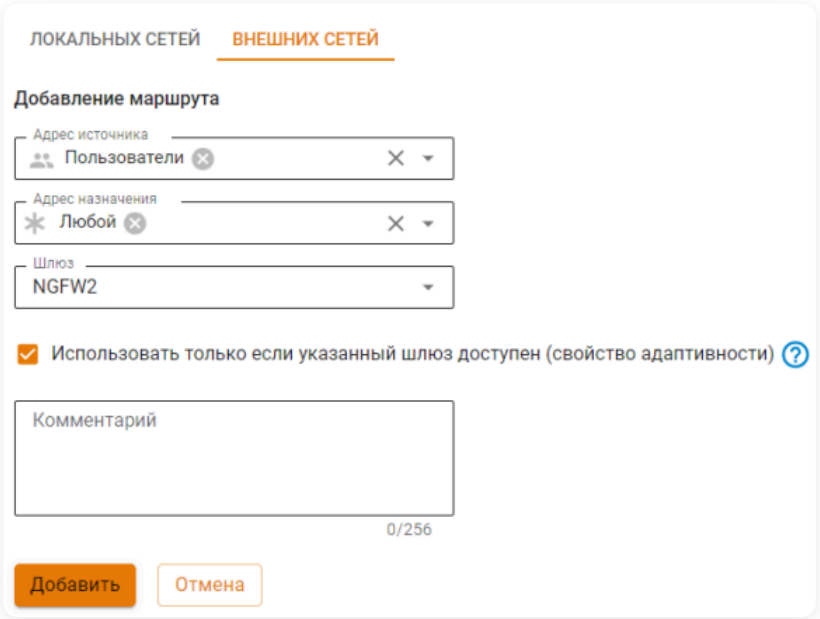
Задача: весь трафик пользователей из группы Бухгалтерия направить через шлюз выбранного сетевого интерфейса



Если настраивается маршрут в удаленную сеть через дополнительный роутер, расположенный в одной локальной сети с клиентами, то убедитесь, что нет "асимметричной маршрутизации" и роутер вынесен в DMZ. Подробнее в статье Как избавиться от асимметричной маршрутизации трафика.

Задача: предоставить доступ в интернет пользователям NGFW1, подключенного по IPsec к NGFW2, через внешний интерфейс NGFW2

Для доступа в интернет пользователям NGFW1 укажите в качестве шлюза IPsec-подключение к NGFW2:



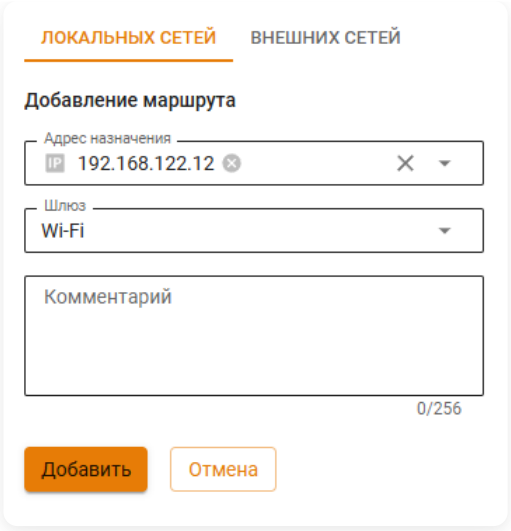
Задача: создать правило маршрутизации до сетей филиала через подключение client-to-site

Если установка подключения site-to-site до сетей филиала недоступна, в Ideco NGFW можно настроить подключение роутера client-to-site. В этом случае при добавлении маршрута локальных сетей в качестве шлюза используется роутер, который подключается по VPN.

Для настройки подключения выполните действия:

1. В разделе **Пользователи** → **Учетные записи** создайте учетную запись для роутера с разрешенным доступом к VPN.

2. При добавлении маршрута в разделе **Сервисы** → **Маршрутизация** → **Локальных сетей** выберите созданного пользователя в поле **Шлюз**:



Сети за роутером станут доступны после установки VPN-подключения через Ideco NGFW.

Информация об особенностях маршрутизации и организации доступа при настроенном VPN-подключении представлена в статье.

Полезные ссылки

- **OSPF**
- **BGP**
- **Балансировка и резервирование**
- **Особенности маршрутизации и организации доступа**
- **Как избавиться от асимметричной маршрутизации трафика**

BGP

Название службы раздела **BGP**: `frr`; `ideco-routing-backend`.

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:

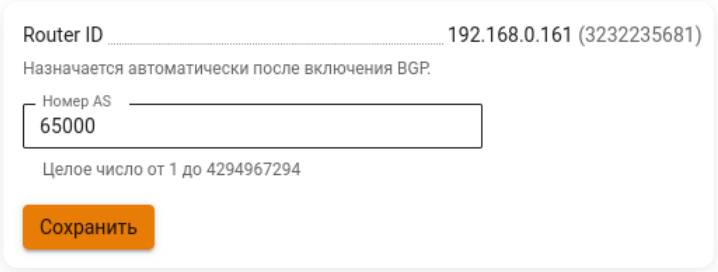
- Указать номер автономной системы.
- Создать и включить как минимум одного BGP-соседа.

На Ideco NGFW 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.

Настройка автономной системы

Перейдите в раздел **Сервисы** → **BGP** и заполните поля:

1. Введите номер автономной системы в строку **Номер AS** и нажмите **Сохранить**:

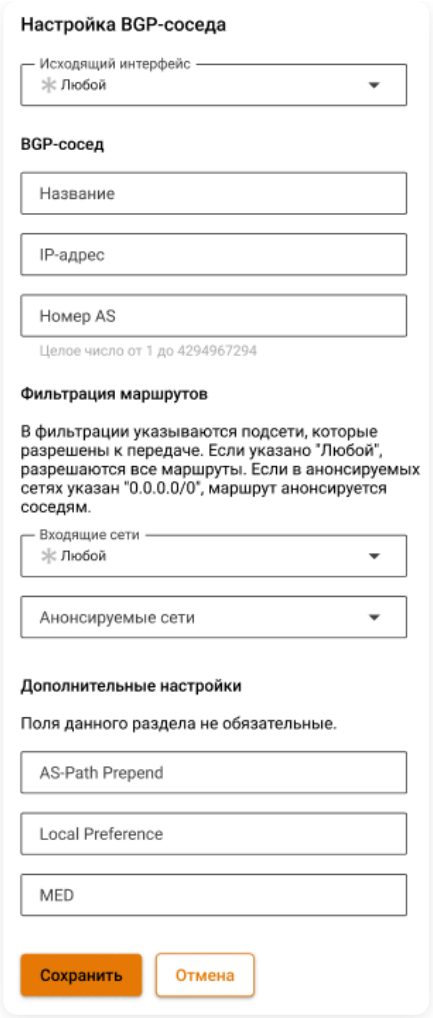


Ideco NGFW автоматически заполняет поле **Router ID** значением наибольшего IP-адреса локальной сети, указанного в разделе Сетевые интерфейсы.

2. Включите модуль **BGP**.

Настройка BGP-соседей

Для добавления BGP-соседа нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Исходящий интерфейс** - интерфейс Ideco NGFW, 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.
- **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 (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 объектов фильтрации

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, соединенных по IPSec в тунельном режиме, воспользуйтесь BGP. Подробнее про настройку подключения двух NGFW по IPSec - в статье.

Для **Входящих сетей** и **Анонсируемых сетей** объект **Любой** не может быть установлен одновременно с другими фильтрами.

Полезные ссылки

- Сетевые интерфейсы
- Внешние и локальные интерфейсы
- Подключение между двумя Ideco NGFW в транспортном режиме работы

OSPF

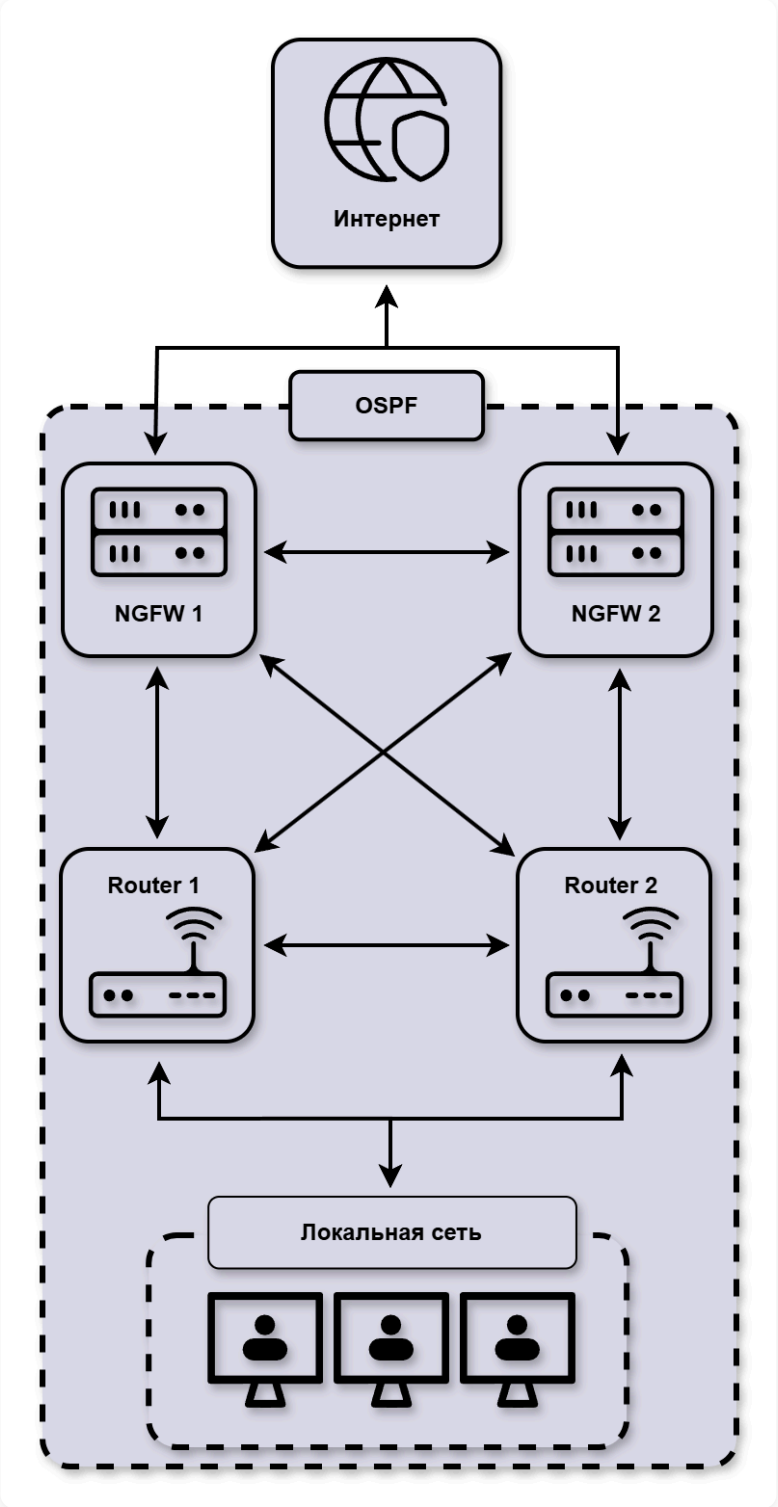
Название службы раздела **OSPF**: `frr`; `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

Ideco NGFW 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.

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.

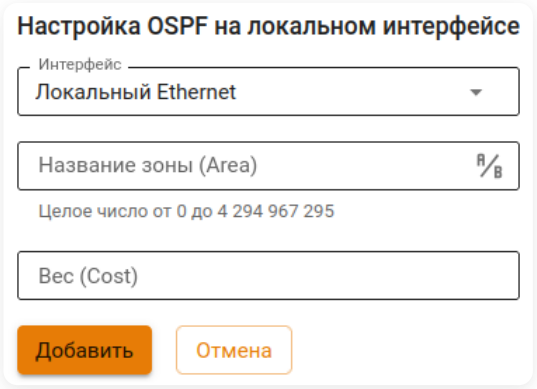
Настройка OSPF

Для настройки OSPF в Ideco NGFW перейдите в раздел **Сервисы** → **OSPF** и выполните действия на вкладках:

Основные

Router ID - IP-адрес маршрутизатора. Присваивается автоматически в виде наибольшего IP-адреса локальной сети, заданной в разделе Сетевые интерфейсы.

1. Нажмите кнопку **Добавить** и заполните поля:

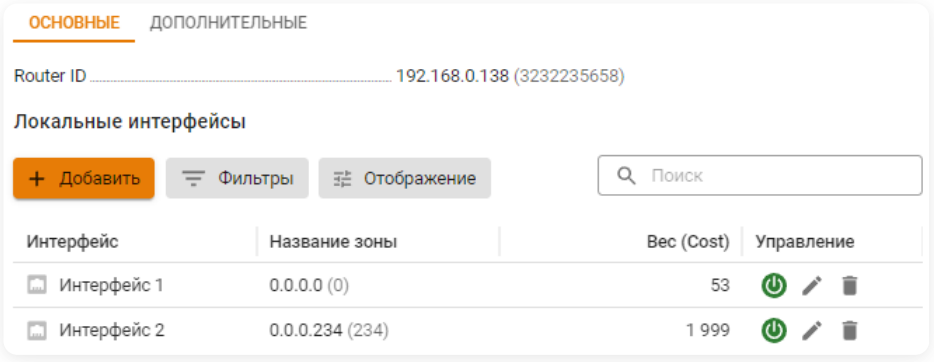


- **Интерфейс** - локальный или Loopback-интерфейс Ideco NGFW, IP-адрес которого будет использован для обмена маршрутами.
- **Название зоны** - номер зоны (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Вес** - стоимость маршрута.

2. Нажмите **Добавить**.

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

Включите настройки (по умолчанию включены):

- **Redistribute default** - маршруты по умолчанию. Устройство, принявшее эту информацию, будет отправлять на NGFW весь трафик.
- **Redistribute static** - статические маршруты, указанные на вкладке **Локальных сетей** в разделе **Сервисы** → **Маршрутизация**.
- **Redistribute connected** - 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.

> Для передачи маршрутов до VPN-сети через OSPF необходимо в разделе **OSPF** → **Дополнительные** включить опцию **Redistribute static (передача статических маршрутов)**.

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**. 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 п. 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>
```

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`:

6. Для вывода таблицы маршрутизации введите команду `show ip route` (в таблице должны появиться маршруты до сетей NGFW):

Особенности работы OSPF в Ideco NGFW

- Ideco NGFW всегда будет являться шлюзом по умолчанию для других устройств. Считать другие устройства шлюзом по умолчанию NGFW не сможет.
- OSPF работает только на локальных интерфейсах: Локальные Ethernet-интерфейсы.
- Значение *Tuna cemu* (*Network Type*) в Ideco NGFW 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-1** в Филиале 1 и **NGFW-2** в Филиале 2 настраивается GRE-over-IPsec и OSPF.
- Каждый NGFW 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-1**, и **NGFW-2** используются в качестве шлюза по умолчанию.
- Между балансировщиком и каждым из NGFW настроена OSPF.

Преимущества настройки:

- Трафик балансируется между **NGFW-1** и **NGFW-2**: часть пользователей из Локальной сети выходят в интернет через **NGFW-1**, часть - через **NGFW-2**.
- При неисправности одного из NGFW трафик автоматически смаршрутизируется через другое соединение.
- Отсутствует необходимость вручную настраивать маршруты для хостов в Локальной сети.

Полезные ссылки

- Сетевые интерфейсы
- Внешние и локальные интерфейсы
- Подключение между двумя Ideco NGFW в транспортном режиме работы

IGMP Proxy

Название службы раздела **IGMP Proxy**: `ideco-igmpproxy-backend`, `ideco-igmpproxy`.

Список служб для других разделов доступен по ссылке.

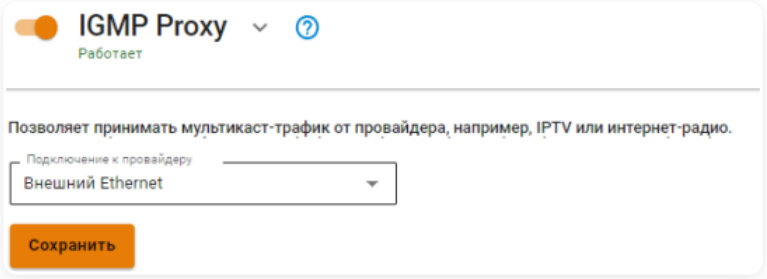
IGMP Proxy - служба, которая проксирует (передает) мультикаст-трафик сквозь роутер. Это сокращает объем трафика, что влияет на скорость работы и нагрузку сети.

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

Для настройки перейдите в раздел **Сервисы** → **IGMP Proxy**. Включите опцию **IGMP Proxy**. В строке **Подключение к провайдеру** выберите Ethernet-подключение.



Принцип работы

На примере подключения двух пользователей к мультикаст-потоку одного источника:

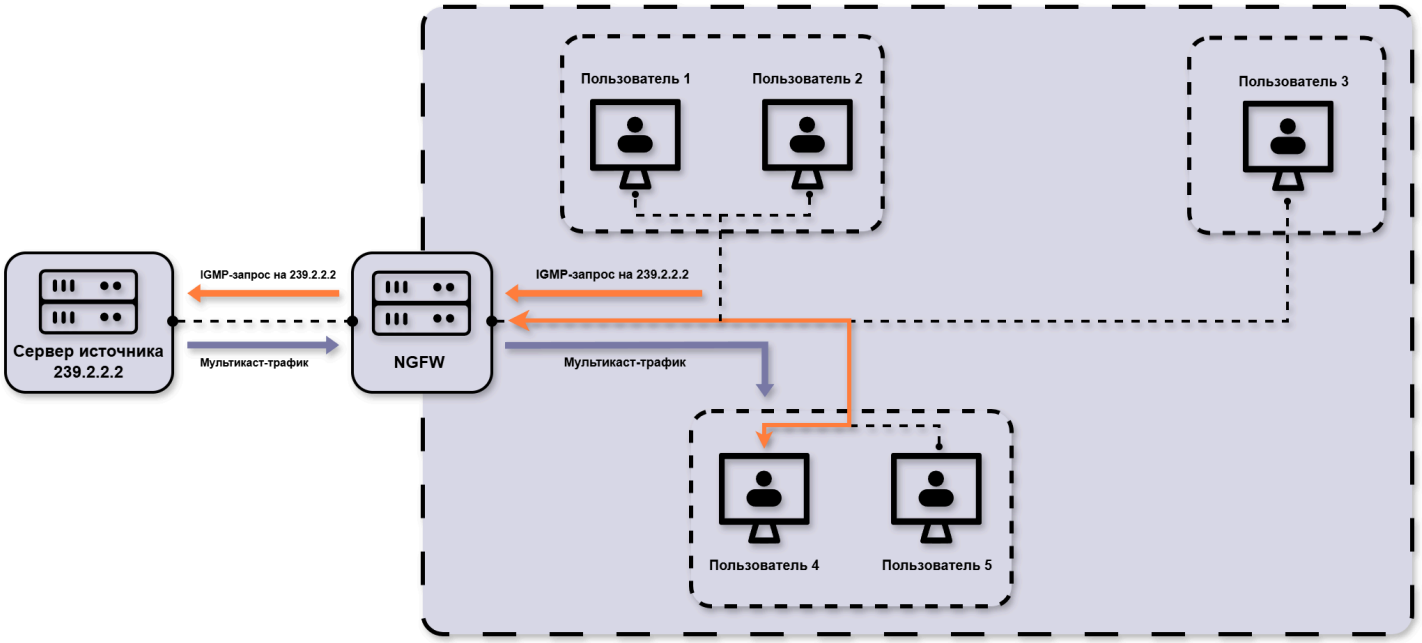
1. **Сервер источника** начинает трансляцию мультикаст-трафика с адреса из диапазона 224.0.0.0/4.

2. **Пользователь 4** хочет подключиться к трафику и генерирует IGMP-запрос (Join) на **Ideco NGFW** для получения мультикаст-трафика от сервера источника.

3. **Ideco NGFW** получает IGMP-запрос и отправляет аналогичный запрос к серверу источника.

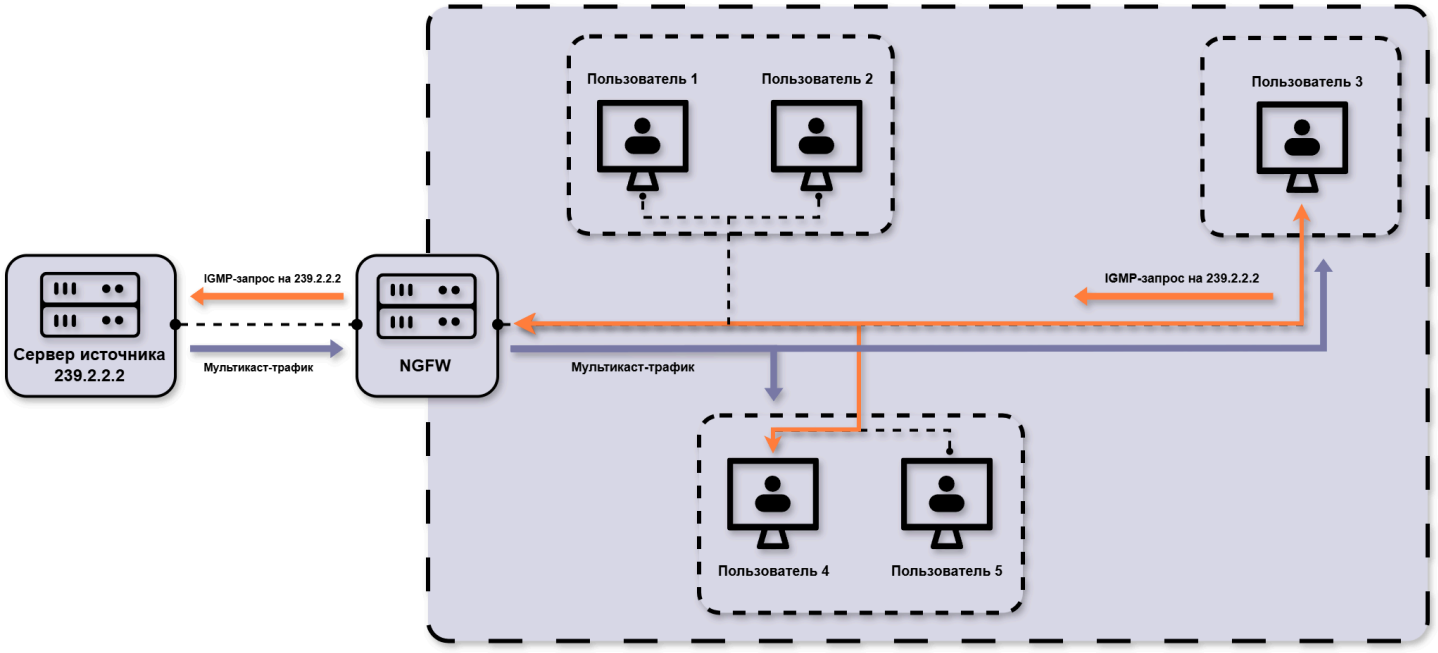
4. Сервер источника получает запрос и начинает транслировать мультикаст-трафик на **Ideco NGFW**.

5. **Ideco NGFW** пропускает трафик с адреса 239.2.2.2 в подсеть с **Пользователем 4**, и **Пользователь 4** становится его получателем:



6. **Пользователь 3**, находящийся в другой подсети, также решает подключиться к этой трансляции и генерирует IGMP-запрос (Join) на Ideco NGFW.

7. **Ideco NGFW** получает этот запрос и дублирует **Пользователю 3** трафик, поступающий **Пользователю 4**:



Ideco NGFW периодически проверяет, есть ли получатели, отправляя пользователям IGMP-запрос (Query). Пользователи в ответ отправляют Join, как при подключении.

Если на Ideco NGFW приходит хотя бы один Join, то мультикаст-трафик продолжает транслироваться получателям.

Прокси

Название службы раздела **Прокси**: `ideco-proxy-backend`, `squid`.

Список служб для других разделов доступен по ссылке.

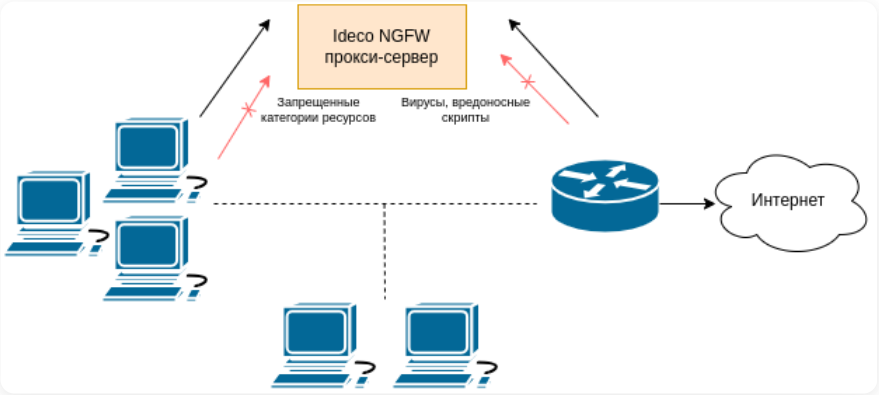
Прокси-сервер используется не только для проксирования веб-трафика, но и для передачи трафика сервисам:

- 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 в качестве шлюза по умолчанию для устройств в сети.

Для настройки фильтрации HTTPS-трафика нужно добавить корневой сертификат NGFW на компьютеры пользователей. Подробнее в статье Настройка фильтрации HTTPS.



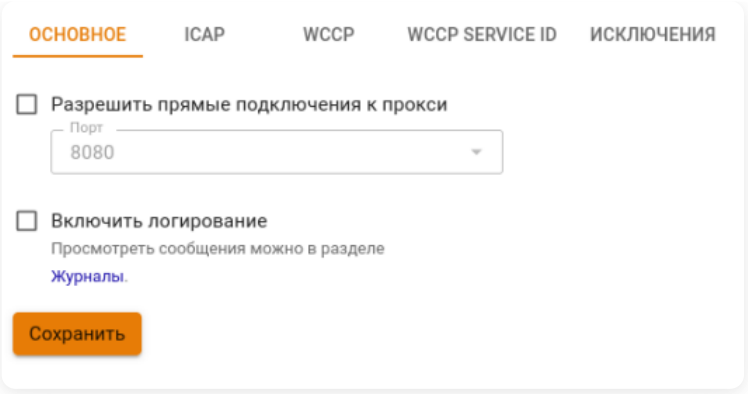
При использовании Ideco NGFW в качестве прокси-сервера с прямыми подключениями к прокси большинство функций будет работать с некоторыми особенностями:

- В правилах **Файрвола** для пользователей необходимо указывать цепочки INPUT вместо FORWARD.
- Глубокий анализ трафика системой предотвращения вторжений и модулем контроля 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.

Основное

На вкладке **Основное** предоставлены возможности:

- **Разрешить прямые подключения к прокси** - применяется, когда Ideco NGFW не является шлюзом по умолчанию для клиентов сети. Порт, указанный на стороне NGFW, следует указать на сетевых устройствах локальной сети, веб-трафик которых нужно пропускать через прокси.
- **Включить журналирование** - применяется для записи логов **Контент-фильтра** и **Антивируса**.



О настройке прямого подключения к прокси и прокси с одним интерфейсом читайте в статье.

ICAP

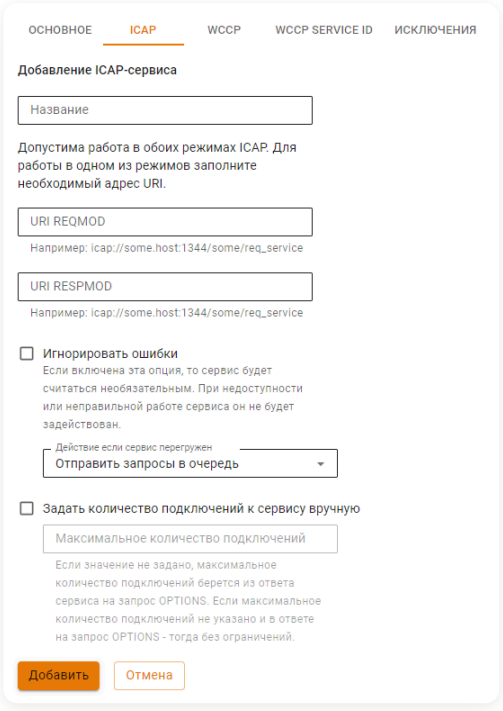
Протокол ICAP позволяет отправлять HTTP(S)-трафик в расшифрованном виде на сторонние серверы. ICAP-сервисы обрабатывают трафик после работы Антивируса и Контент-фильтра Ideco NGFW, блокируя запросы в соответствии с установленными политиками сервиса.

Если трафик попадает под любое запрещающее правило Ideco NGFW или ICAP-сервиса, трафик будет заблокирован.

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.
- **Игнорировать ошибки** - если включена эта опция, то сервис будет считаться необязательным. При недоступности или неправильной работе сервис не будет задействован.
- **Действие если сервис перегружен** - опция позволяет выбрать сценарий действий при перегруженности ICAP-сервиса.
- **Задать количество подключений к сервису вручную** - 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 **Задать количество подключений к сервису вручную** значение меньше четырех, то клиентские подключения могут быть нестабильными.



Для корректной работы ICAP-сервиса должна быть настроена расшифровка HTTPS-трафика в **Контент-фильтре**.

WCCP

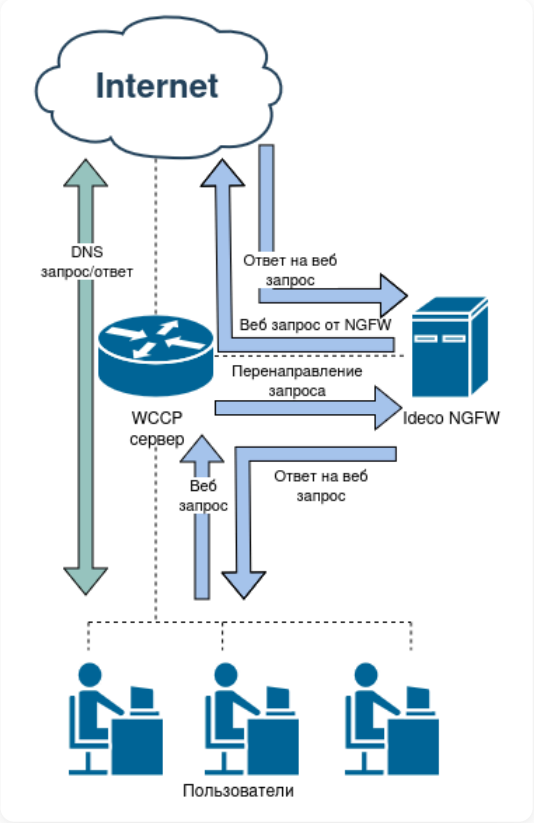
Протокол WCCP используется для перенаправления трафика на Ideco NGFW. По умолчанию перенаправляется только HTTP/HTTPS-трафик.

Для активации WCCP включите опцию **Включить перенаправление трафика с WCCP-серверов на Ideco NGFW**. Ideco NGFW запустит процесс согласования параметров с WCCP-сервером.

В NGFW предусмотрено два режима работы WCCP - L2 и GRE:

L2

Режим L2 используется, если WCCP-сервер и Ideco NGFW находятся в одном сетевом сегменте:



Последовательность обработки веб-запросов на уровне L2:

1. Пользователь отправляет веб-запрос.

2. Запрос перенаправляется сервером на Ideco NGFW.

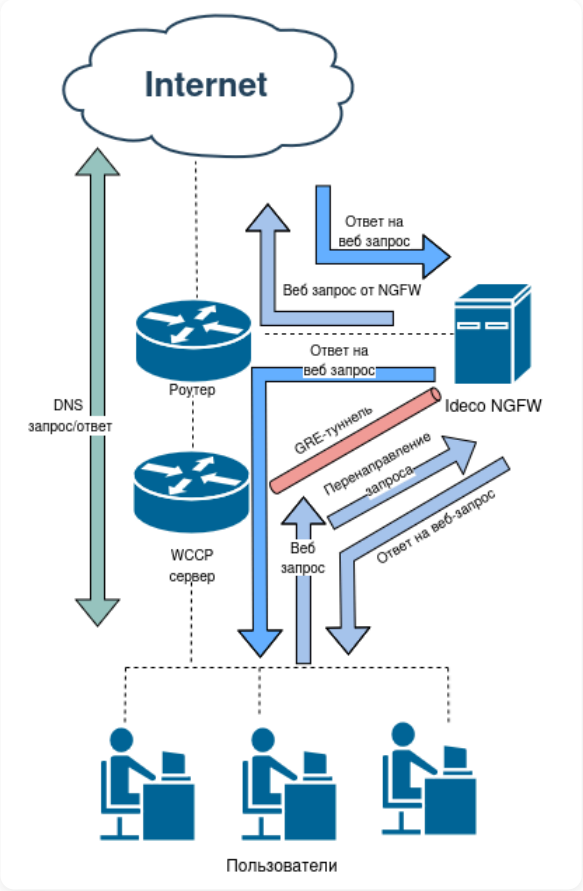
3. Ideco NGFW обрабатывает запрос:

- Если запрос заблокирован, информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается обратно по тому же пути, по которому уходил на внешний сервер.

GRE

Режим GRE используется, если WCCP-сервер и Ideco NGFW находятся в разных сетевых сегментах:



Последовательность обработки веб-запросов на уровне GRE:

1. Пользователь отправляет веб-запрос.

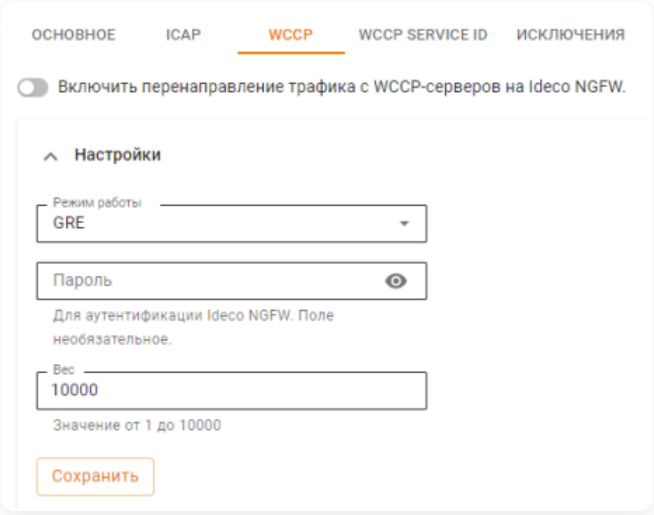
2. Запрос перенаправляется по GRE-туннелю на Ideco NGFW.

3. Ideco NGFW обрабатывает запрос:

- Если запрос заблокирован, то информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

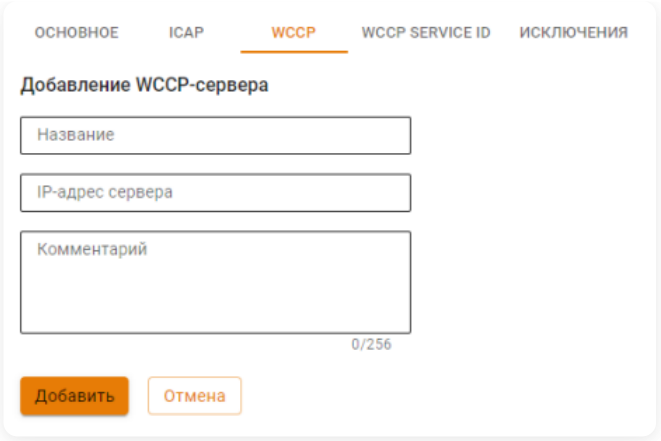
Ответ возвращается напрямую от Ideco NGFW пользователю, минуя GRE-туннель.
Для выбора режима раскройте блок **Настройки**.

Если на WCCP-сервере задан пароль, сохраните его в соответствующем поле:



Если WCCP использует несколько Ideco NGFW, настройте распределение трафика с помощью указания приоритета в поле **Вес**. Допустимые значения - от 1 до 10000.

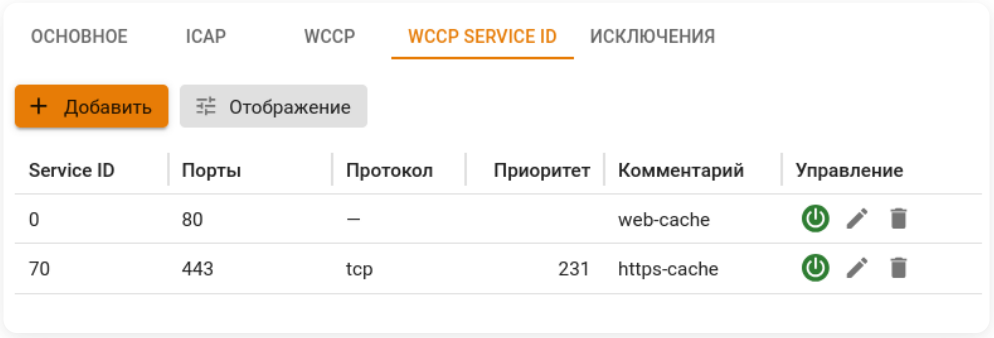
Для добавления WCCP-сервера нажмите кнопку **Добавить** и укажите IP-адрес сервера:



WCCP Service ID

Service ID - идентификаторы сервисной группы. Настройки на этой вкладке позволяют выбрать службы, трафик которых сервер WCCP будет перенаправлять на Ideco NGFW.

По умолчанию настроены сервисы для HTTP/HTTPS-трафика:

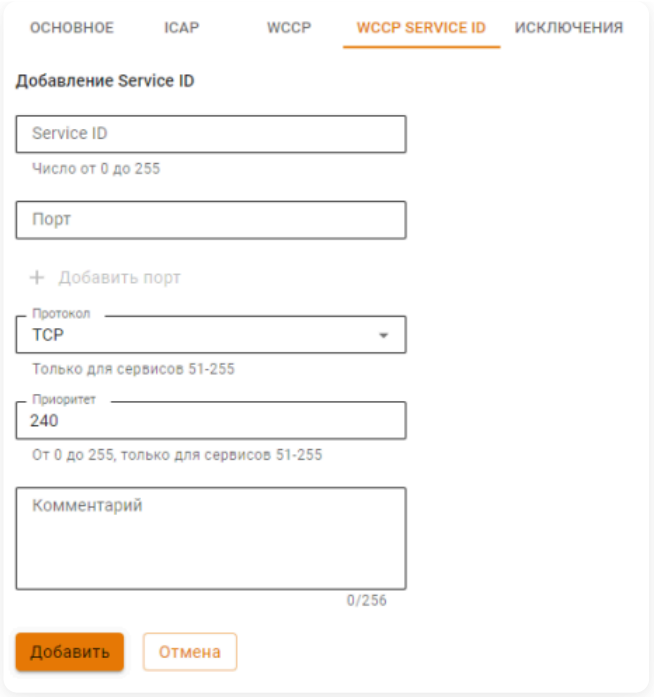


> Service ID с 0 по 50 зарезервированы под фиксированные сервисы. Для них выбирать порты и протоколы нельзя.
>
> Service ID 70 - общепринятое значение для HTTPS-трафика на 443 TCP-порт.

Чтобы настроить Service ID, выполните действия:

1. На вкладке **WCCP Service ID** нажмите кнопку **Добавить**.

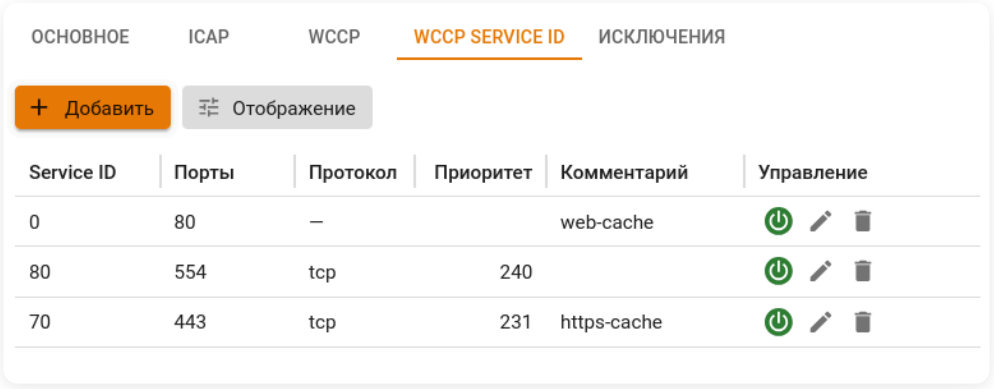
2. В открывшейся форме укажите следующие значения:



- **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 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.

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.

На вкладке **Исключения** можно исключить ресурсы из обработки прокси-сервером и всеми связанными службами (контент-фильтр, веб-отчетность, антивирусы):

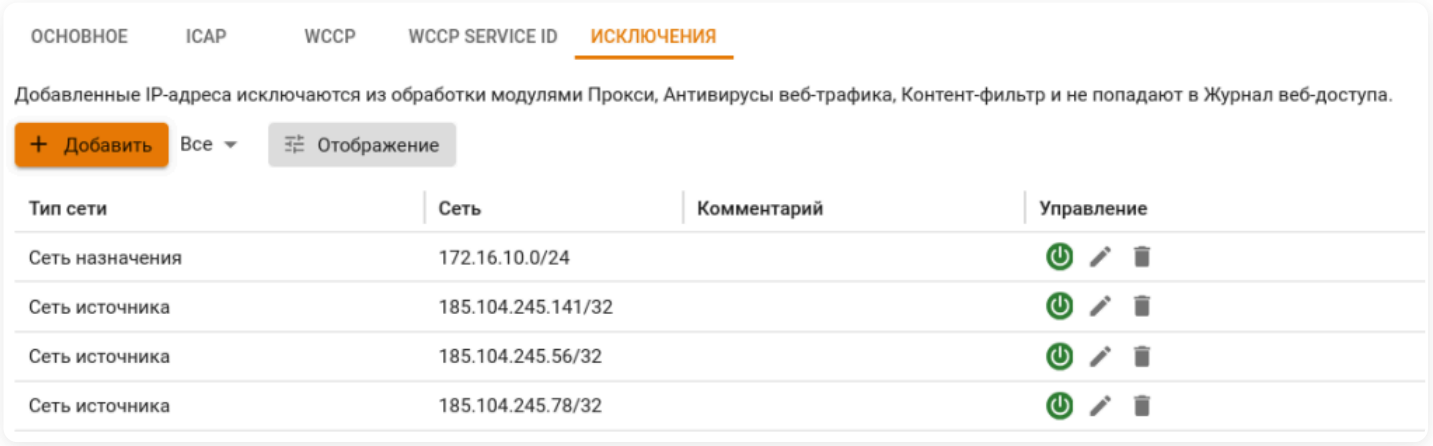
- **Сети источника** - указываются сети, трафик из которых исключается из обработки прокси-сервером;
- **Сети назначения** - указываются внешние сети или IP-адреса (как правило, адреса веб-сайтов или веб-сервисов), трафик до которых из всех локальных сетей NGFW исключается из обработки прокси-сервером.

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).

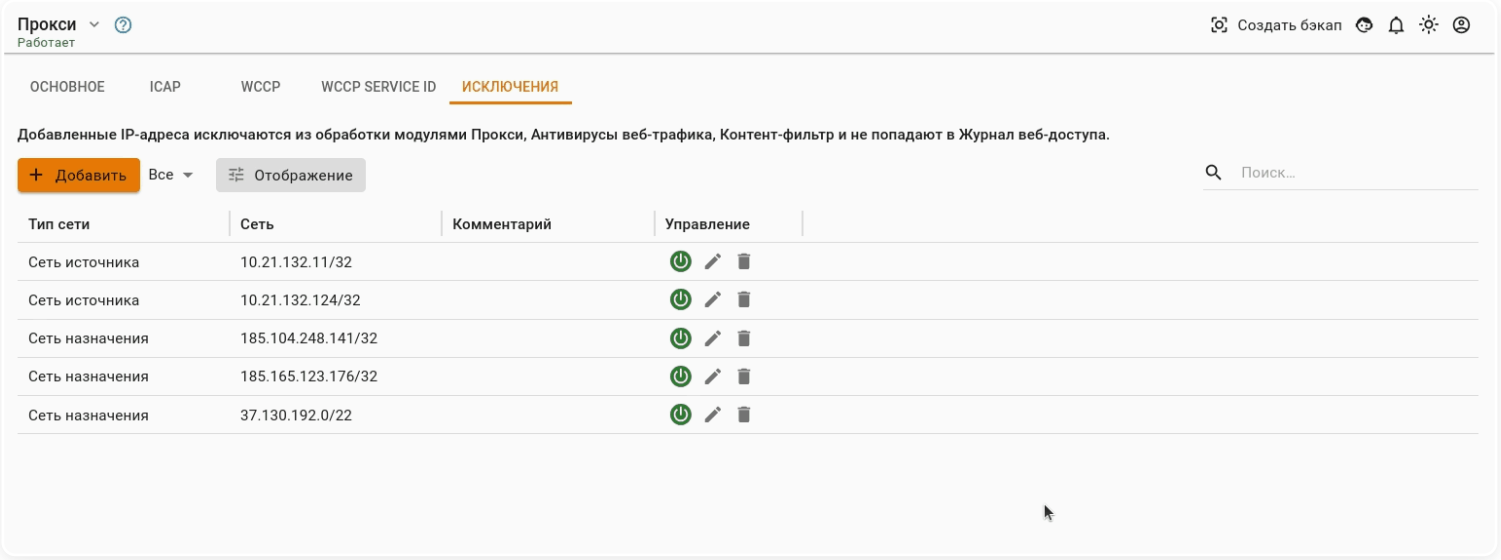
При создании исключений можно указывать только IP-адреса или IP-сети.

Трафик, исключенный из обработки прокси, не будет участвовать в **Отчетах**, проверяться на вирусы и обрабатываться модулем **Контент-фильтра**. В то же время такой трафик будет проверен **Файрволом**, модулями **Предотвращение вторжений** и **Контроль приложений**.



Поиск по таблице исключений

Над таблицей исключений расположена строка поиска. Она позволяет 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

- 194.54.15.90/32
- 194.186.207.124/32
- 194.186.207.182/32
- 195.8.62.178/32
- 194.54.15.90/32
- 10.21.132.124/32
- 92.38.2.37/24

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.

Настройка прямого подключения к прокси

Для настройки выполните действия:

1. Укажите IP-адрес локального интерфейса Ideco NGFW в качестве веб-прокси в локальной сети на клиентских устройствах.

2. В настройках прокси на Ideco NGFW укажите порт для прямых подключений к прокси (возможен выбор портов из списка: 3128, 1080, 8000, 8080, 8888, 8081, 8088, 10080).

В таком режиме NGFW сможет предоставлять клиентским устройствам веб-трафик по другим портам (по умолчанию - по всем, при необходимости можно закрыть порты Файрволом).

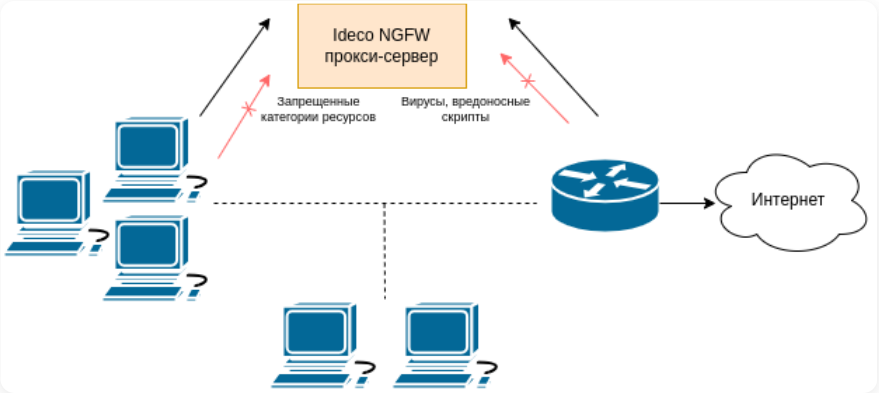
Если прямое подключение к прокси требуется только части клиентских устройств или части локальных интерфейсов, то создайте INPUT-правило **Файрвола**. Пример приведен ниже.

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 **Файрвола**.

Для учета, контроля и проверки веб-трафика на вирусы, требуется соблюдение следующих условий:

- Локальная подсеть не пересекается с внешним интерфейсом NGFW.
- У сервера Ideco NGFW есть доступ в интернет.
- На клиентских устройствах указан адрес веб-прокси (в настройках прокси-сервера в браузерах).



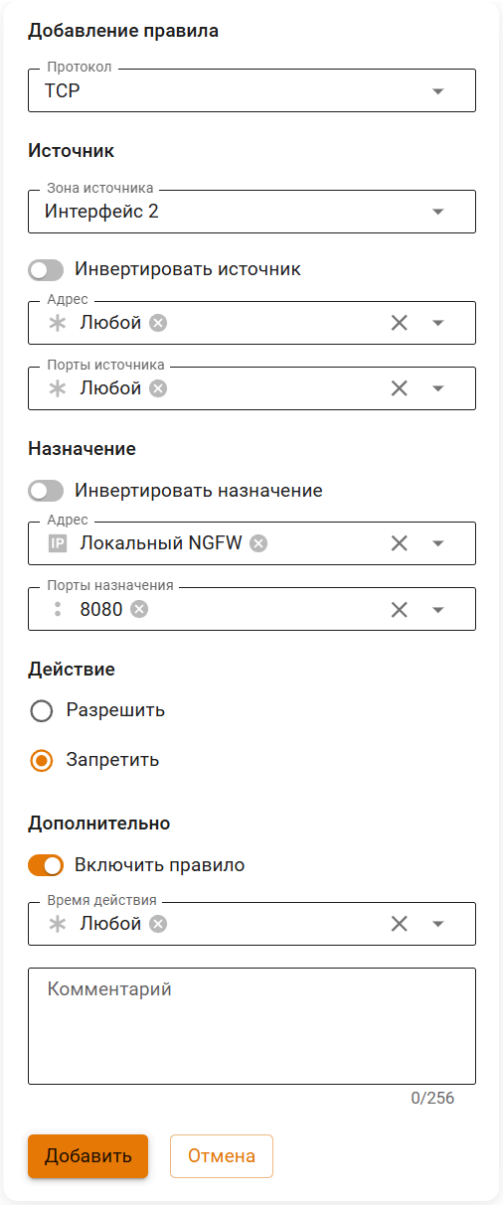
Если в настройках программы под ОС Windows или MacOS X нет возможности указать прокси-сервер, воспользуйтесь сторонним ПО для маршрутизации всего трафика рабочей станции на прокси-сервер. Такую возможность предоставляет программа **Proxifier**, которую можно настроить для прямых подключений к прокси, воспользовавшись статьей.

Пример настройки INPUT-правила

1. Перейдите в **Правила трафика** → **Файрвол** → **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:

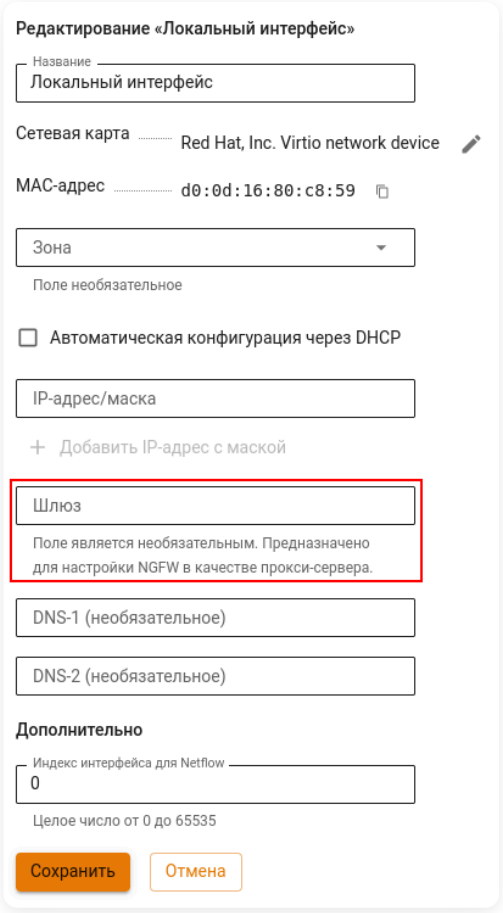


- **Протокол** - TCP.
- **Источник**:
  - **Зона источника** - локальный интерфейс или конкретные интерфейсы.
  - **Адрес** - **Любой**. Доступ будет запрещен всем, кроме адресов в разрешающем правиле.
- **Назначение**:
  - **Адрес** - IP-адрес локального интерфейса NGFW.
  - **Порт назначения** - порт, указанный в настройках **Прокси**.
- **Действия** - **Запретить**.

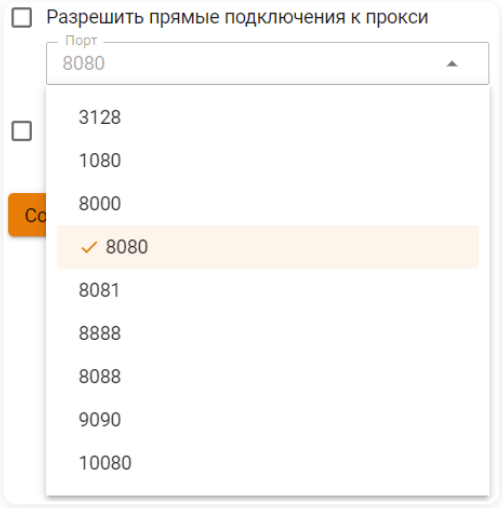
Настройка прокси с одним интерфейсом

При необходимости можно использовать Ideco NGFW в качестве прокси-сервера с прямыми подключениями клиентов к прокси, с одним интерфейсом. Для этого выполните действия:

1. При создании локального интерфейса в разделе **Сервисы** → **Сетевые интерфейсы** укажите **Шлюз**:



2. Разрешите прямые подключения к прокси-серверу в разделе **Сервисы** → **Прокси**, выбрав нужный порт из списка:



Обратный прокси

Название службы раздела **Обратный прокси**: `ideco-reverse-backend`.

Список служб для других разделов доступен по ссылке.

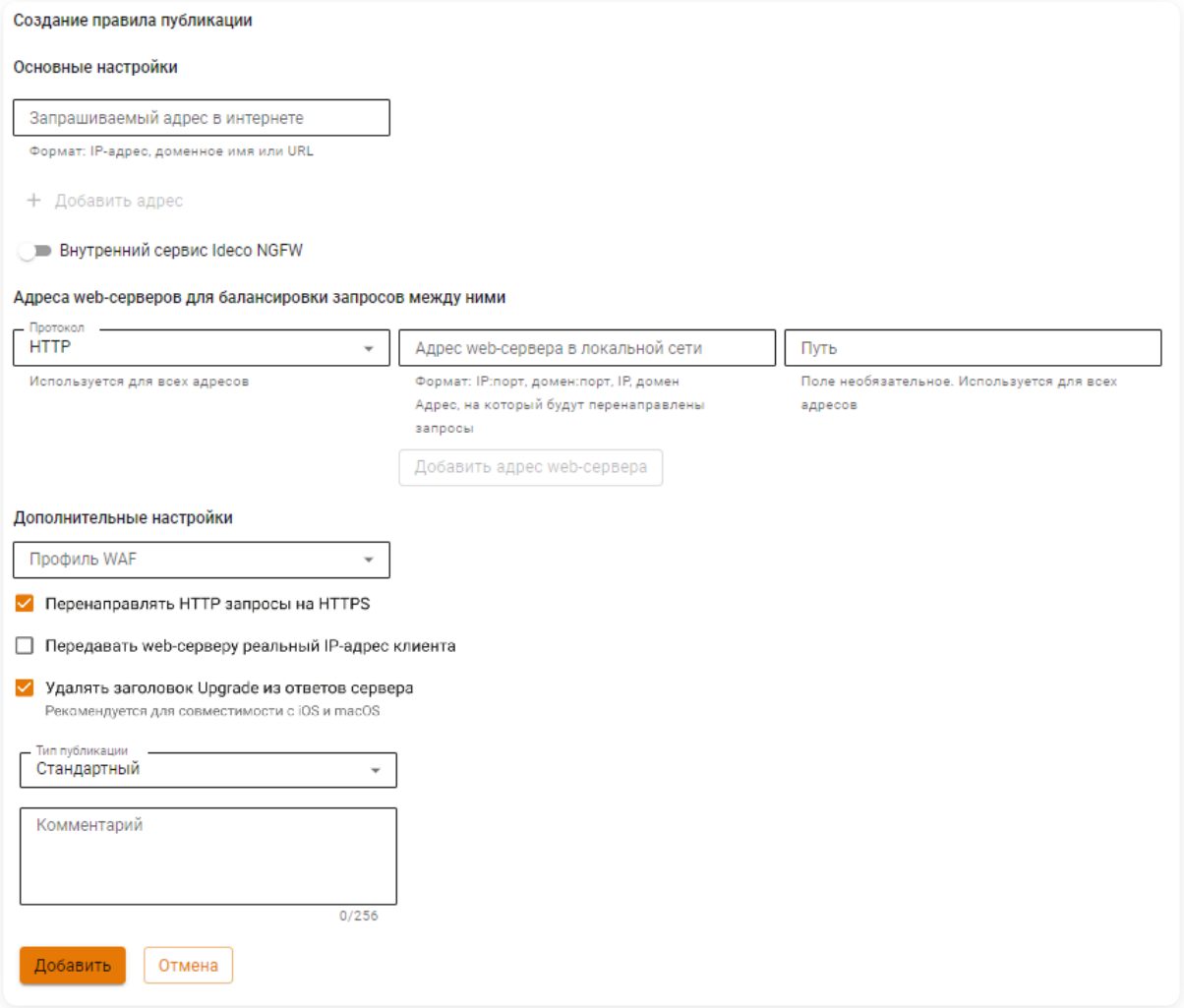
Технология обратного прокси позволяет проксировать веб-трафик из сети интернет в локальную сеть. Отличается от DNAT тем, что работает на более высоком уровне (прикладной протокол HTTP вместо сетевого протокола IP) и позволяет более гибко реализовать публикацию ресурсов.

Обратный прокси позволяет смаршрутизировать запрос на HTTP-сервер в локальной сети из внешней сети. Таким образом, имея одну ресурсную A-запись для внешнего сетевого интерфейса NGFW, можно опубликовать несколько ресурсов в локальной сети, распределив их по нескольким входящим URL.

Создание и настройка правила

Настройка сертификатов для публикуемых ресурсов не требует их ручной загрузки. Ideco NGFW сам отправляет запрос на выпуск сертификата Let's Encrypt. Выпуск сертификата может занять до 20 минут. Выпущенные сертификаты будут доступны в разделе Сертификаты.

Для создания правила перейдите в раздел **Сервисы** → **Обратный прокси** и нажмите на кнопку **Добавить**. Форма добавления правила разделена на три подраздела: **Основные настройки**, **Адреса web-серверов для балансировки запросов между ними** и **Дополнительные настройки**.



Основные настройки

- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных 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** - включите опцию и выберите для публикации один из сервисов Ideco NGFW: Личный кабинет/Портал SSL VPN.

Адреса web-серверов для балансировки запросов между ними

- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Адрес web-сервера в локальной сети** - адрес, на который будут перенаправлены запросы.
- **Путь** - поле необязательное и используется для всех адресов.

Если указать в поле **Запрашиваемый адрес в интернете** *0.0.0.0*, перенаправление будет работать со всех внешних IP-адресов Ideco NGFW на адрес из поля **Адрес web-сервера в локальной сети**.

Чтобы перенаправление работало с доменов Ideco NGFW на адрес из поля **Адрес web-сервера в локальной сети**, необходимо явно указать домены в поле **Запрашиваемый адрес в интернете**.

Дополнительные настройки

- **Профиль WAF** - позволяет задать параметры защиты веб-ресурса при указании WAF-профиля.
- **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. 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 (в частности, типы атак, входящие в OWASP TOP-10). При активации этого модуля также будут блокироваться злоумышленники, ведущие сканирование сайта на уязвимости, с помощью модуля защиты от brute force атак.

Не рекомендуем использовать проброс веб-интерфейса NGFW через WAF, так как при попытке входа пользователь может быть заблокирован средствами WAF.

- **Удалять заголовок Upgrade из ответов сервера** - включите опцию, если сайт недоступен на устройствах Apple. Опция уберет запрещенный стандартом `RFC 7540` заголовок `Upgrade` из ответов `HTTP/2`, предотвращая разрыв соединения.
- Поле **Тип публикации** позволяет выбрать один из типов: **Стандартный** и **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 резолвиться во внешний IP-адрес сервера NGFW. Доменные имена, указываемые в поле **Адрес в локальной сети**, должны резолвиться в IP-адреса публикуемых ресурсов самим сервером NGFW.

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 NGFW 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 NGFW.
- На локальном сервере, в админ-панели WordPress должен быть настроен домен `wordpress.mydomain.ru` на стандартном порту HTTP.
- Добавить в обратный прокси правило публикации `wordpress.mydomain.ru` -> `wordpress.mydomain.ru`.

Защита от DoS-атак

Включение опции **Защита от DoS-атак** ограничивает трафик, если:

- скорость - более 200 запросов в секунду с одного IP-адреса.
- количество подключений с одного IP-адреса - более 1000.
- размер запроса - более 50 Мб.
- время ожидания на чтение заголовка и тела запроса - более 5 секунд.



Чтобы исключить IP-адрес из обработки **Защитой от DoS-атак**, обратитесь в Техническую поддержку.

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;
}
```

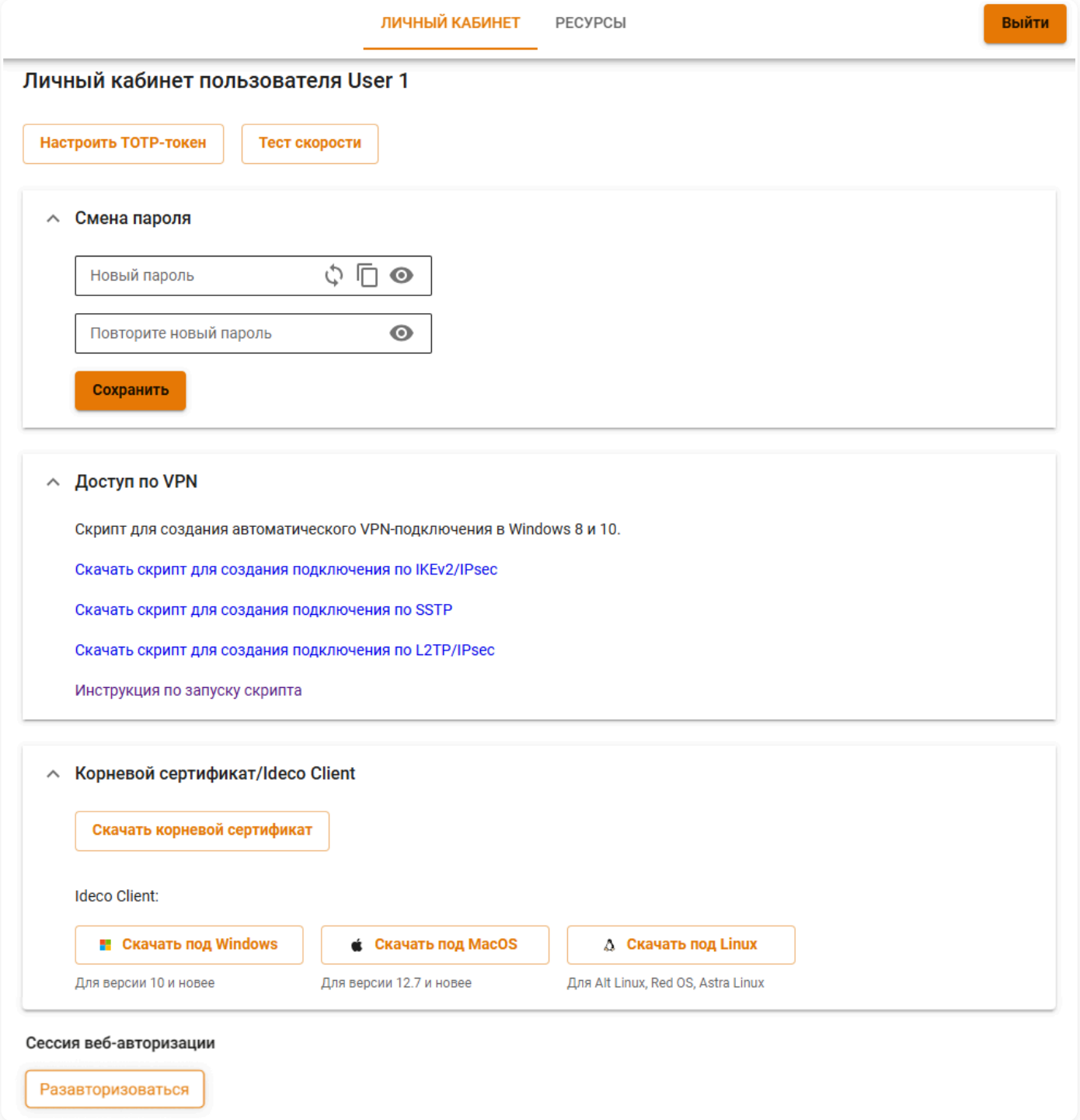
При использовании NGINX Proxy Manager добавьте в **Custom Nginx Configuration** → **Advanced Settings** запись `proxy_hide_header Upgrade;`, иначе мобильные устройства от Apple будут получать сообщение об ошибке **Connection Closed**.

ЛК/Портал SSL VPN

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:

- **Генерация TOTP-токена**. Для настройки двухфакторной аутентификации воспользуйтесь статьей.
- **Тестирование скорости**. При нажатии на Тест скорости в веб-интерфейсе личного кабинета откроется меню тестирования скорости между хостом и NGFW.
- **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 корневого сертификата**.
- **Скачивание Ideco Client**. Подробнее о работе в Ideco Client - в статье.
- **Разавторизация**. Завершение сессии пользователя в сети NGFW, если он был авторизован через Web/SSO.



Поддерживаемые версии браузеров:

- Google Chrome версия 76 и выше
- Firefox версия 71 и выше
- Safari версия 13 и выше

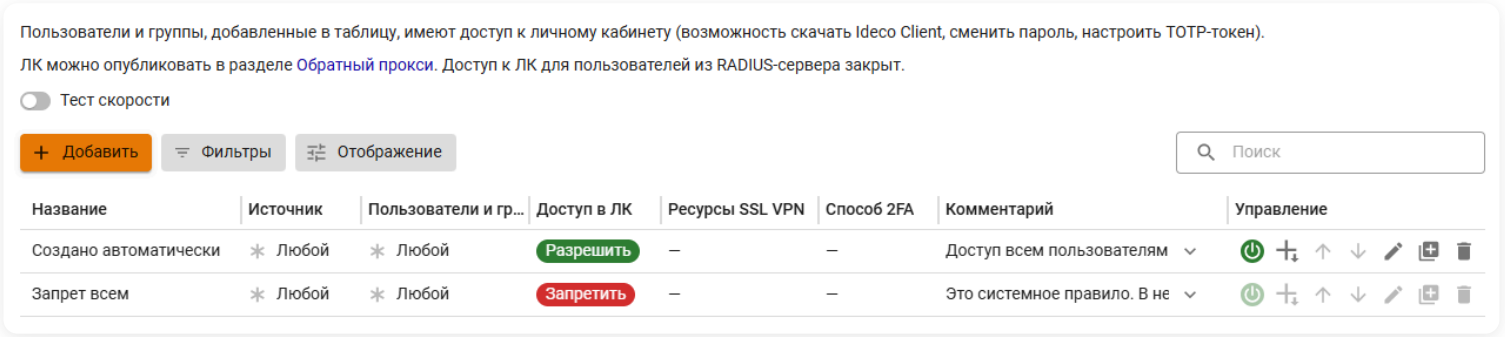
Настроить доступ пользователей в личный кабинет можно на вкладке **Сервисы** → **ЛК/Портал SSL VPN** → **Правила доступа**. Для этого необходимо создать **Правило доступа**, а затем опубликовать личный кабинет через **Обратный прокси**, чтобы пользователи получили к нему доступ. VPN-подключение не требуется, пользователь авторизуется через логин и пароль.

Настройка доступа в личный кабинет Ideco NGFW

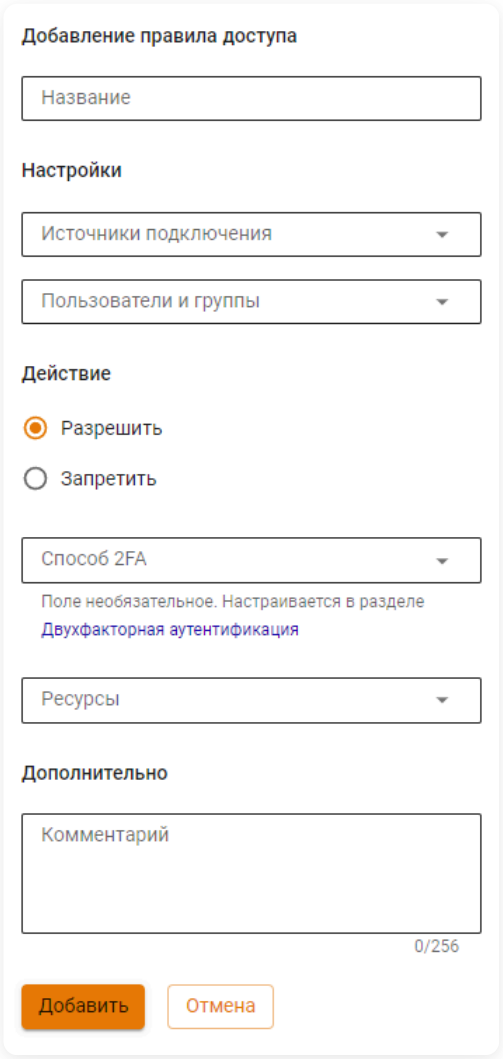
В разделе **Сервисы** → **ЛК/Портал SSL VPN** можно настроить доступ в личный кабинет.

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.

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**.

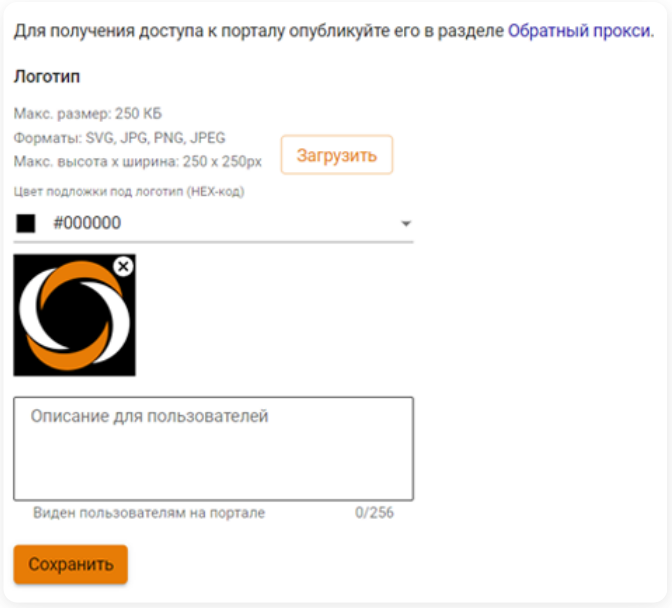
2. Если правило разрешающее, то доступные пользователю в ЛК ресурсы определяются этим правилом. Последующие правила с такими же полями учитываться не будут.

3. Доступ пользователя или группы пользователей к ресурсу определяется заново при изменении таблицы, пользователей и состава групп.

Опция **Тест скорости** позволяет добавить в личный кабинет функцию проверки скорости интернет-соединения.

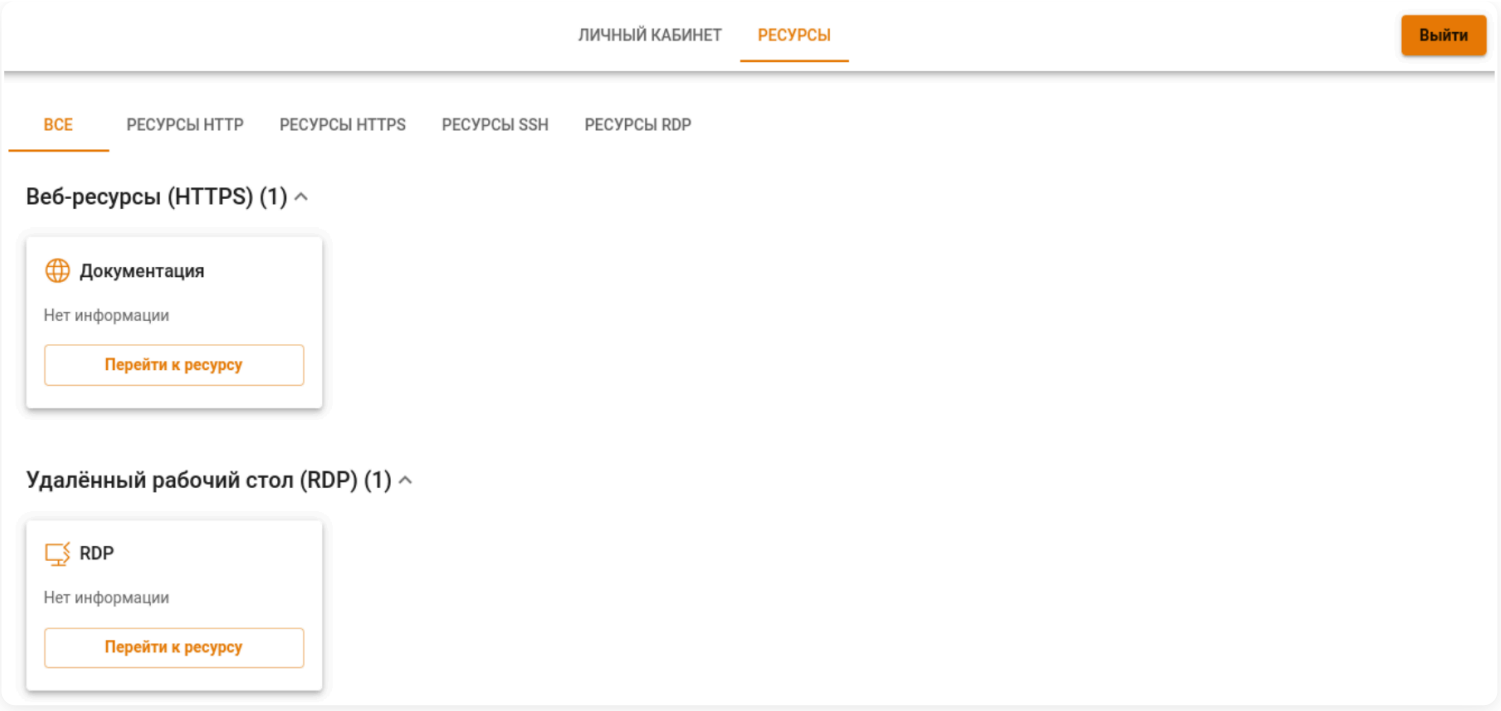
Внешний вид

На вкладке можно настроить внешний вид портала: изменить логотип и добавить описание, которое отображается рядом с логотипом:



Ресурсы

В личном кабинете Ideco NGFW размещаются только внутренние ресурсы, доступные из локальной сети NGFW. Ресурсы становятся доступны пользователям только после успешной авторизации и при наличии соответствующего разрешения в правилах доступа:

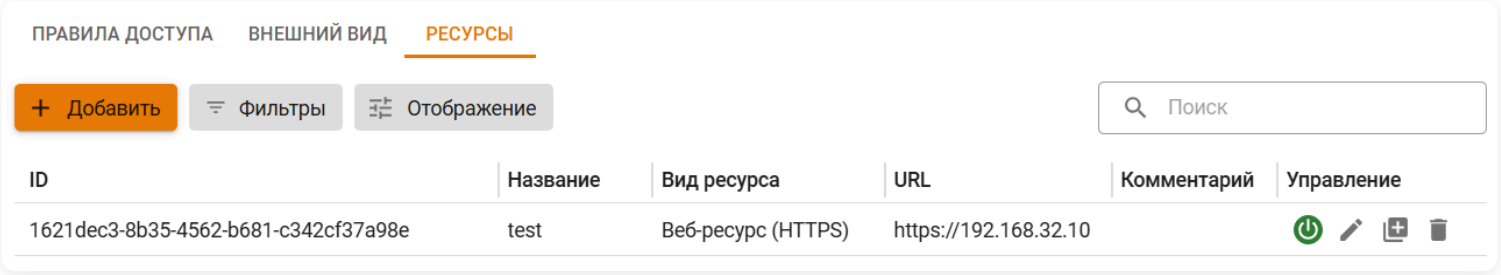


Веб-ресурсы HTTP(S) в SSL VPN работают по принципу **Обратного прокси** ЛК/SSL VPN.

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.
- 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**:

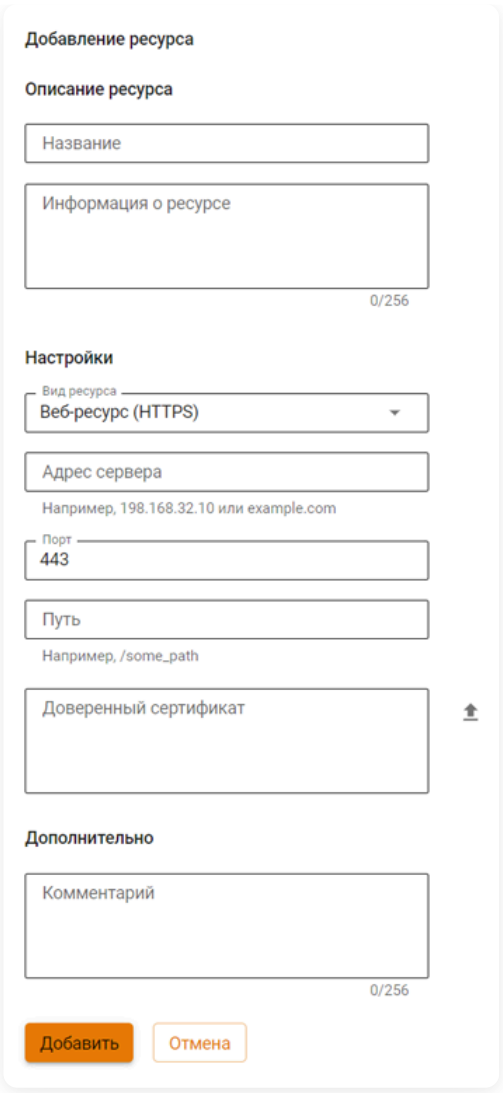


В случае несоответствия URL перечисленным требованиям публикуемый ресурс будет отображаться некорректно, т.к. браузер пользователя не сможет получить некоторые данные с этих URL (например, файлы CSS и JS).

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.

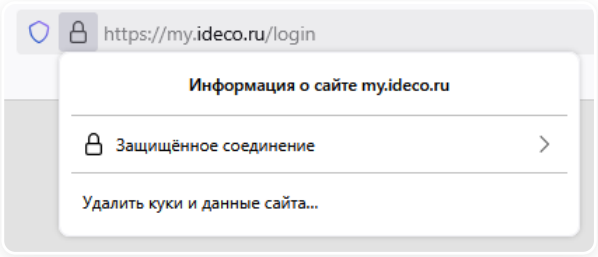
Настройки:

- **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.

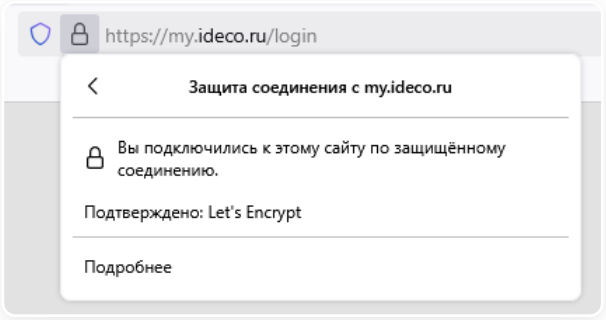
Где скачать доверенный сертификат

Пример скачивания сертификата в браузере Firefox:

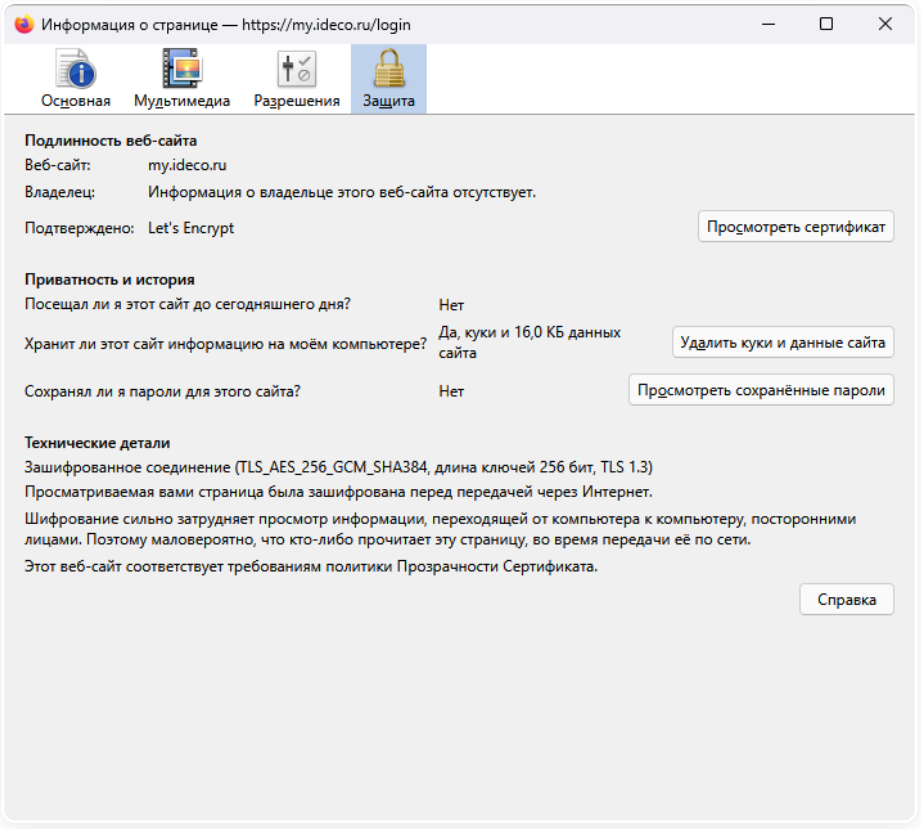
1. Нажмите в адресной строке браузера на значок с замком и выберите **Защищенное соединение**:



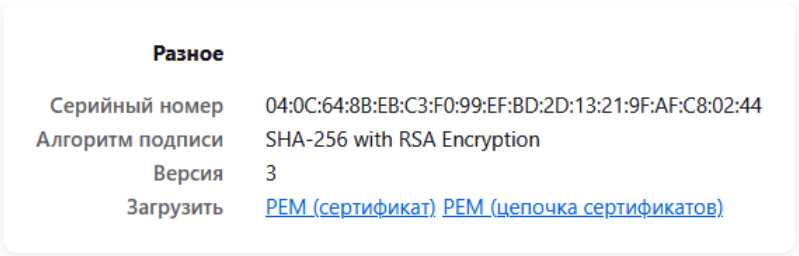
2. Нажмите **Подробнее**:



3. На вкладке **Защита** нажмите **Просмотреть сертификат**:



4. В разделе **Разное** скачайте сертификат из строки **Загрузить**:



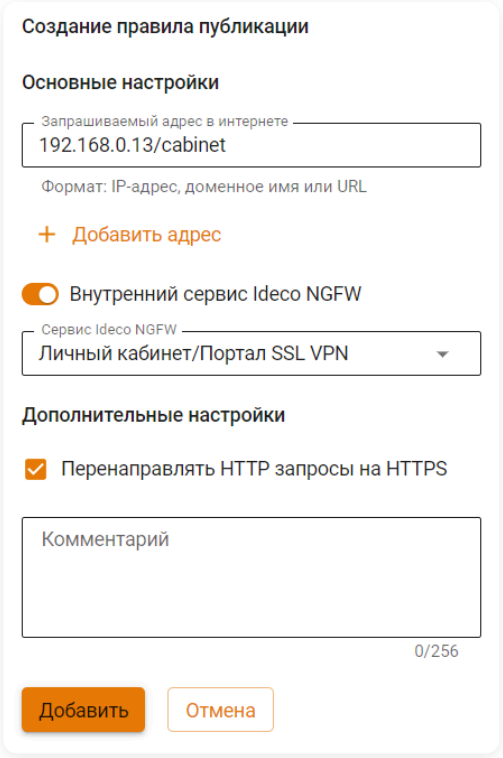
Адреса, на которые ссылается HTTP/HTTPS-ресурс, должны быть относительными во избежание нарушения CORS. Подробнее про CORS.

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**.

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**.

После этого пользователь сможет зайти в личный кабинет по логину и паролю либо через авторизацию в сети NGFW.

Вход в личный кабинет Ideco NGFW

Личный кабинет пользователя будет доступен по ссылке, указанной при публикации через **Обратный прокси**.

Чтобы зайти в личный кабинет, выполните действия:

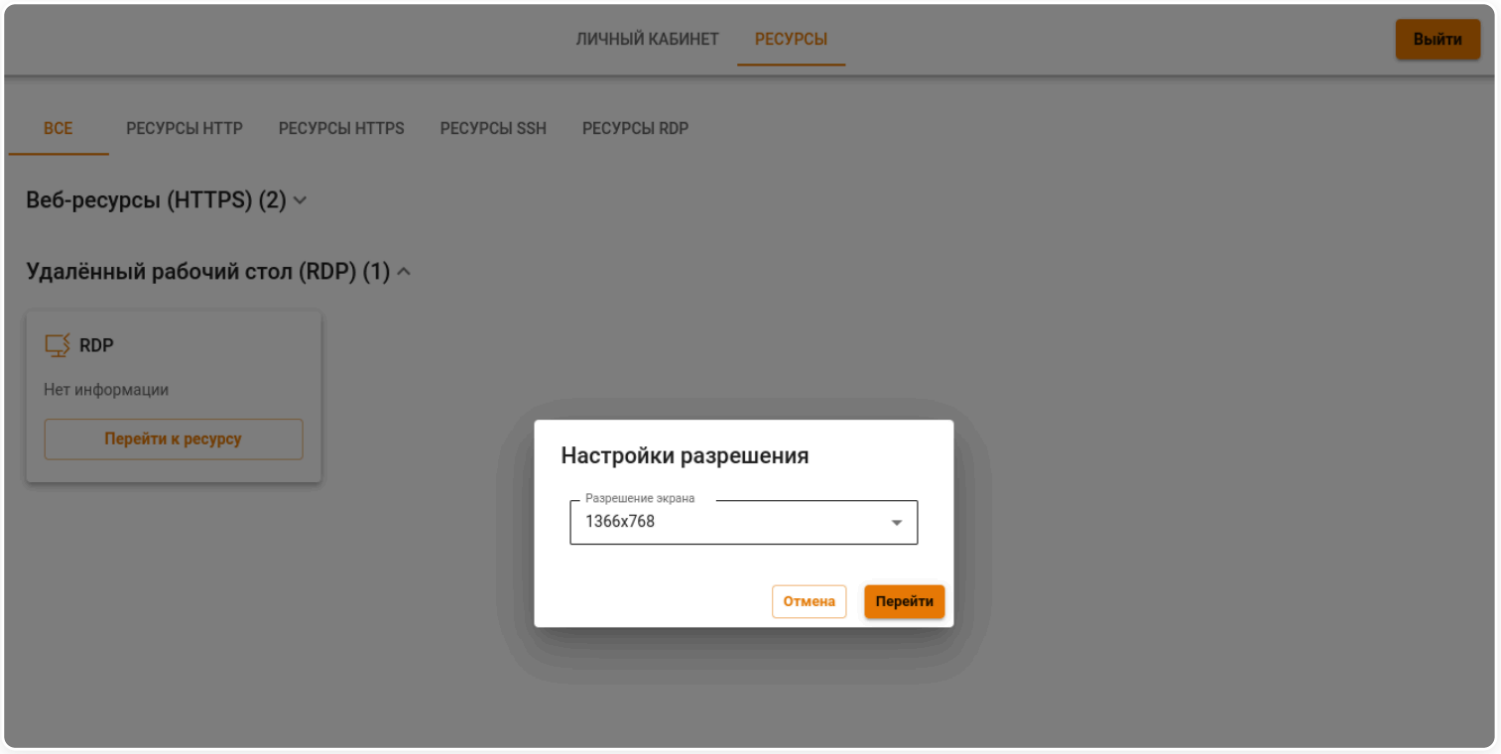
1. Перейдите по ссылке, указанной в правиле публикации личного кабинета.

2. В открывшейся форме авторизации введите логин и пароль пользователя.

Если пользователь уже авторизован в сети NGFW, 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

Защита и управление DNS

Название службы раздела **Защита и управление DNS**: `ideco-unbound`; `ideco-dns-backend; nsd`.

Список служб для других разделов доступен по ссылке.

Настройка производится в разделе **Сервер** → **Защита и управление DNS** на следующих 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.

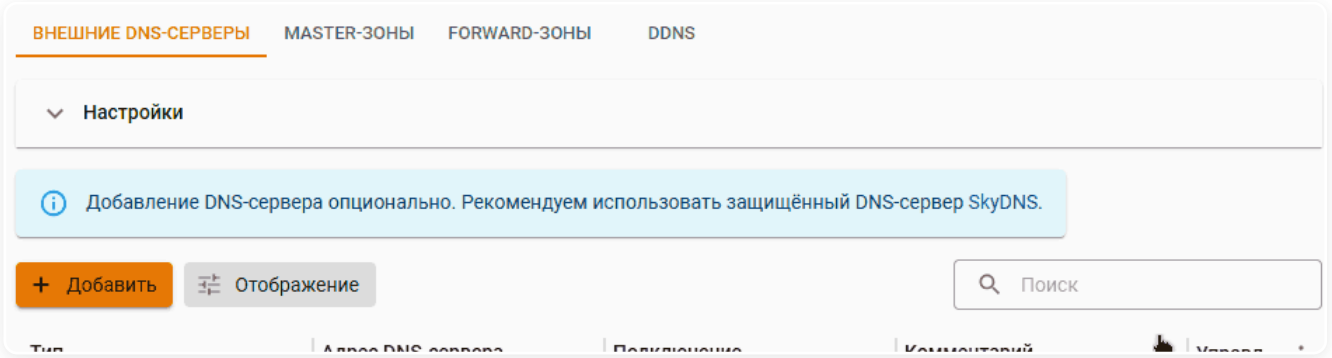
При наличии большого количества Forward- и Master-зон в таблицах воспользуйтесь кнопкой **Фильтры**.

Внешние DNS-серверы

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, если на рабочей станции пользователя указаны сторонние DNS-серверы (например, с целью обхода блокировок). Опция работает глобально для всех хостов в локальной сети и предупреждает возможную подмену адреса ресурса при резолвинге домена. Запрос перенаправляется на DNS-сервер NGFW, который формирует ответ вместо исходного DNS-сервера.

Для VPN-пользователей опция **Перехват пользовательских DNS-запросов** будет работать только если в настройках VPN включена опция **Отправлять весь трафик на Ideco NGFW**.

Включение перехвата пользовательских DNS-запросов блокирует использование DNS-over-TLS (DoT), DNS-over-QUIC (DoQ) и DNS-over-HTTPS (DoH).

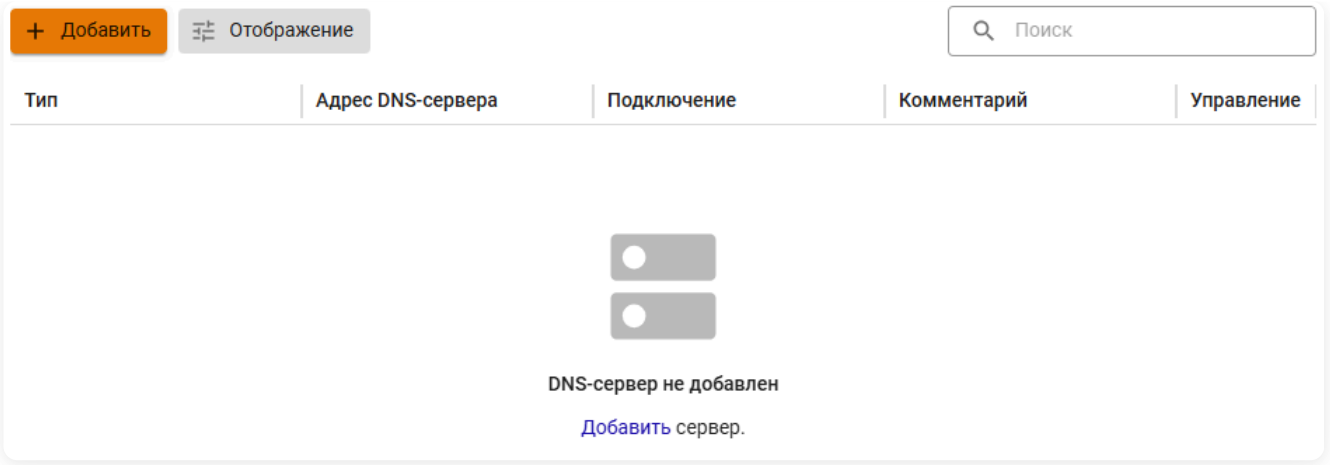
При включенной опции **Перехват пользовательских DNS-запросов** трафик обрабатывается не как FORWARD, а как INPUT. Поэтому для корректной фильтрации трафика модулями **Контроль приложений** создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

- **Безопасный поиск** - при резолвинге NGFW будет возвращать адреса поисковых систем (Google, Youtube, Bing) с включенной фильтрацией нежелательного контента.

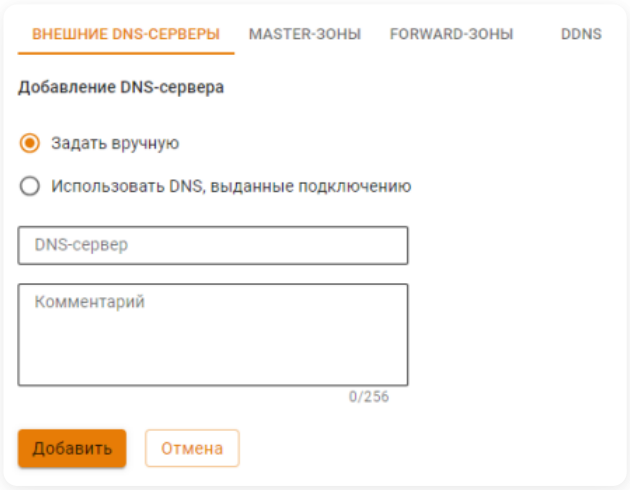
Рекомендации

- В Ideco NGFW встроен кеширующий DNS-сервер. Рекомендуется использовать его в качестве DNS-сервера для локальной сети. Достаточно прописать IP-адрес Ideco NGFW 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 справится с резолвингом самостоятельно.
- Не указывайте DNS-серверы контроллера домена, даже если он может самостоятельно резолвить доменные имена в интернете. При интеграции с AD для работы AD и резолвинга внутренних имен домена. Для резолвинга особых зон, не связанных с AD, создайте Forward-зону вручную.
- По возможности не используйте DNS, выданные интернет-провайдером, так как они превышают TTL и долго отвечают. Ideco NGFW 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).

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`.
- Open DNS `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`.

Master-зоны

Master-зоны позволяют использовать Ideco NGFW как сервер имен и переводить IP-адреса в доменные имена внутри сети.

DNS-сервер в Ideco NGFW 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.

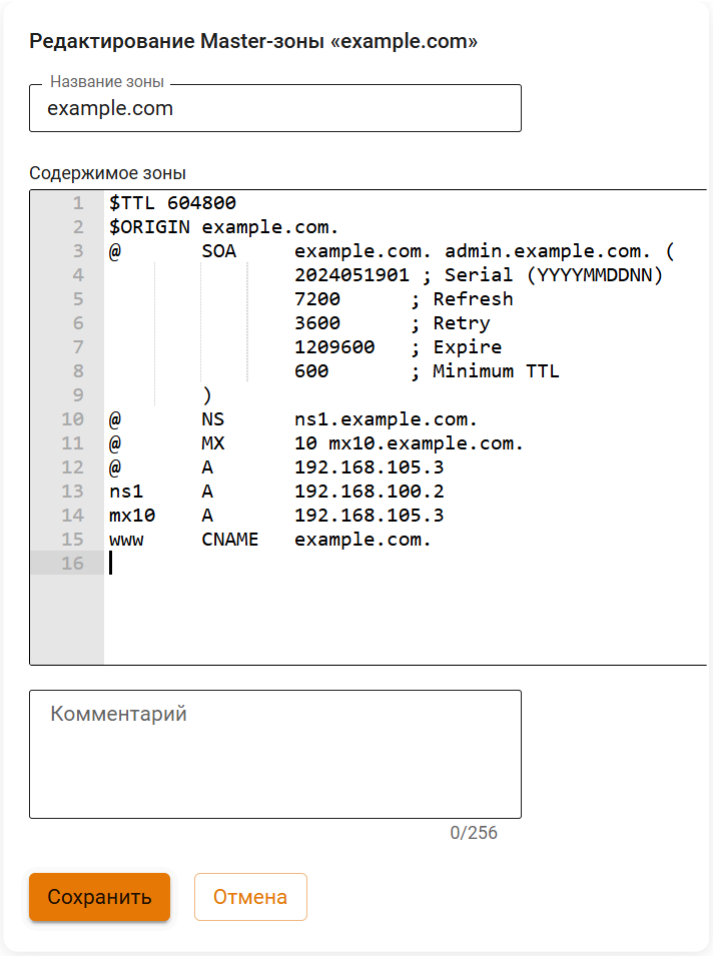
Описание параметров записи

- **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 @
```

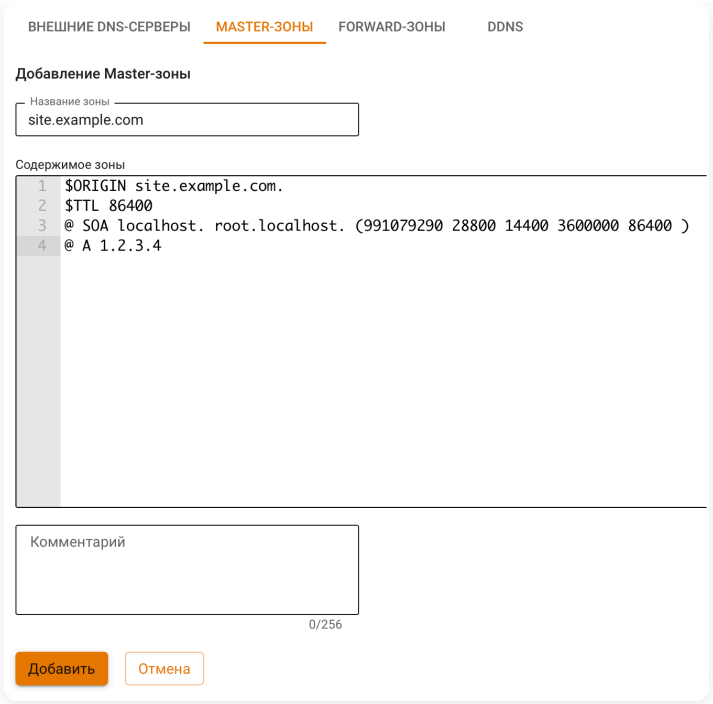
2. Имя зоны: example.com

```
$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 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.

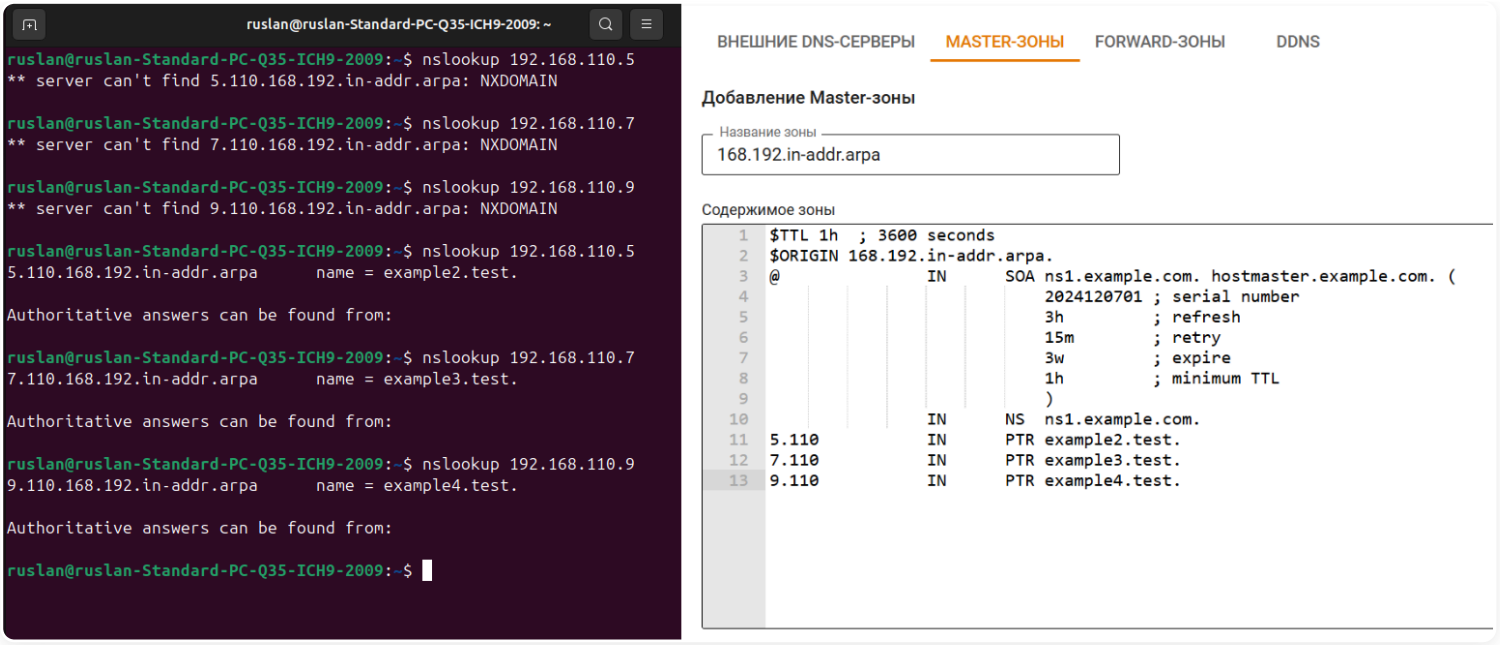
2. При создании содержимого Master-зоны используйте преобразованное в формат **Punycode** доменное имя.

> 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 их 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.
```

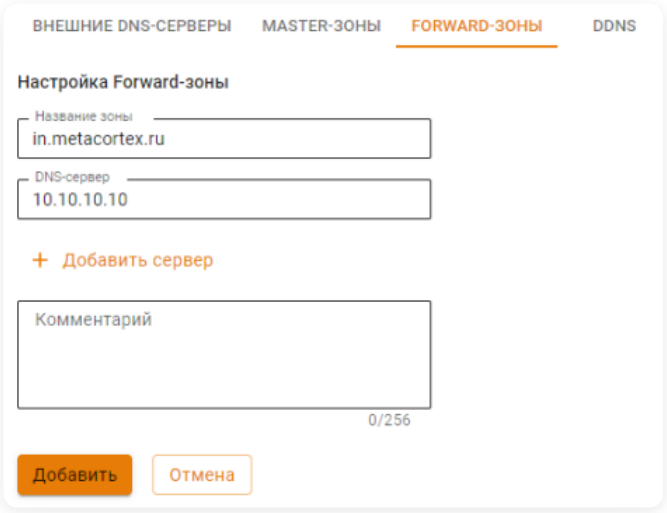
Forward-зоны

Позволяет задать DNS-сервер для разрешения имен конкретной DNS-зоны. Указав доступный в сети DNS-сервер и обслуживаемую зону, клиенты сети Ideco NGFW получают возможность обращаться к ресурсам этой зоны по именам домена.

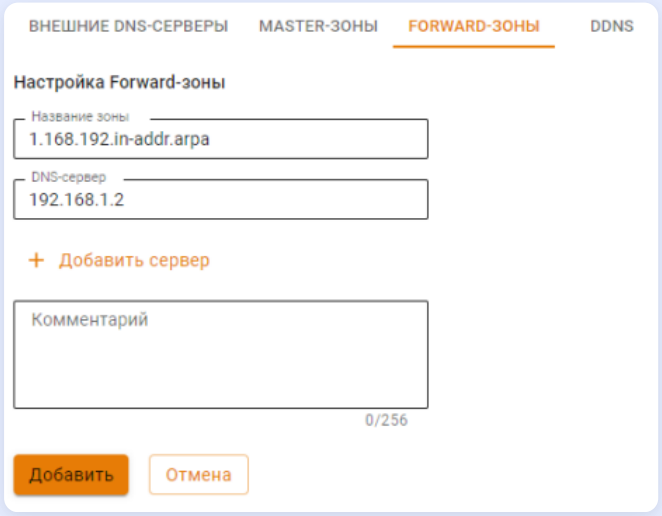
Пользовательские Forward-зоны DNS всегда имеют приоритет над автоматически созданной Forward-зоной для Active Directory.

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**:



DDNS

Название службы раздела **DDNS**: `ideco-dns-backend`.

Список служб для других разделов доступен по ссылке.

DDNS в Ideco NGFW реализован через интеграцию с хостингом RU-CENTER. Перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.

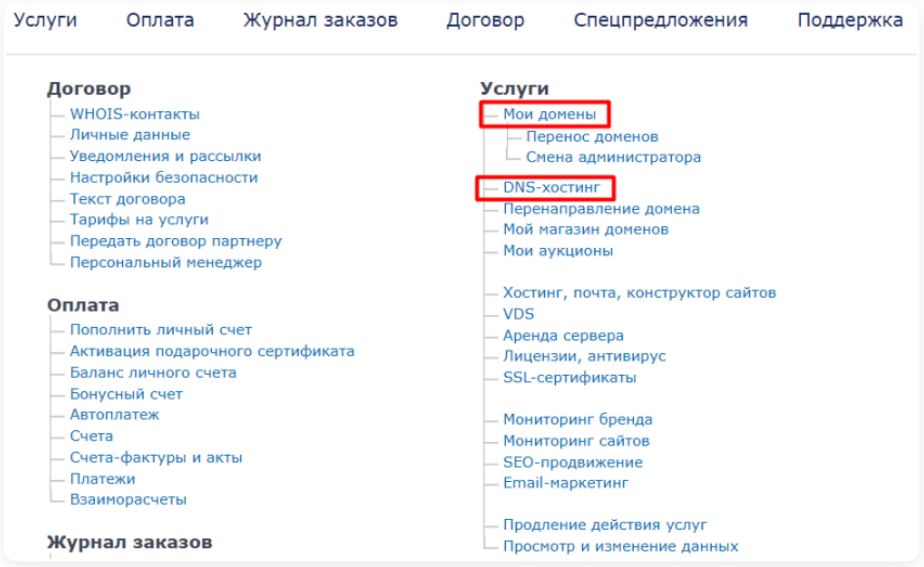
Для решения вопросов по работе с хостингом воспользуйтесь страницей помощи.

Настройка DDNS

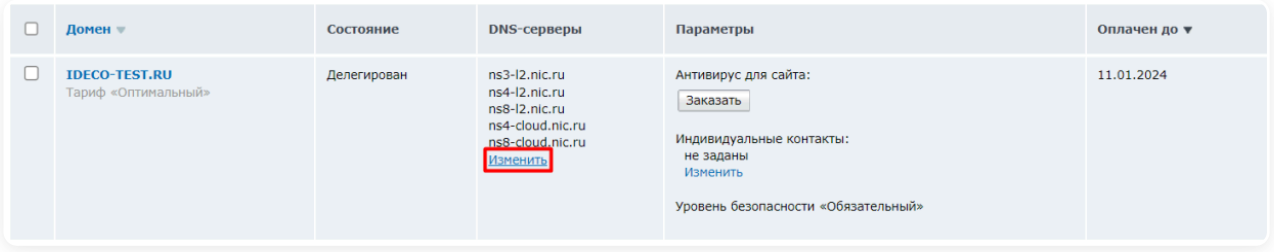
DDNS не будет работать:

- 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**:



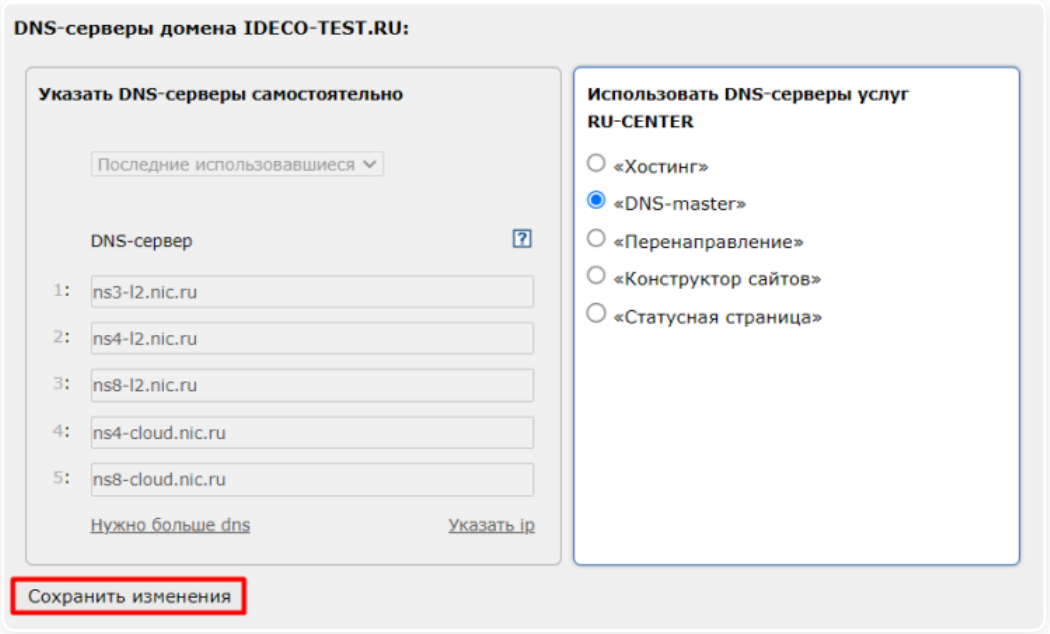
2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:



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.

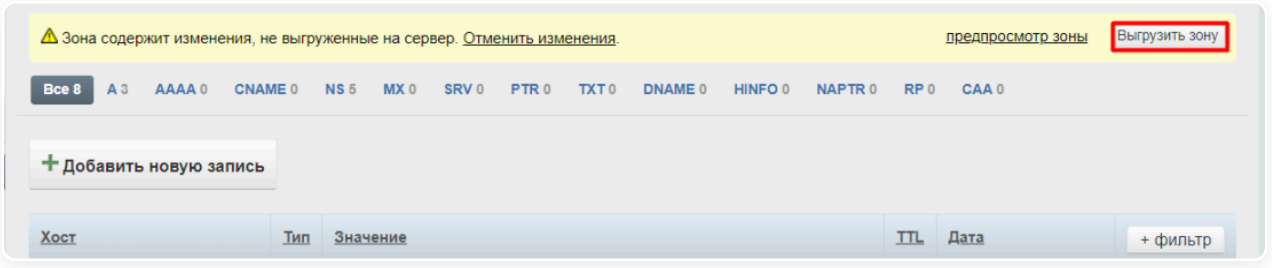
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

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**:

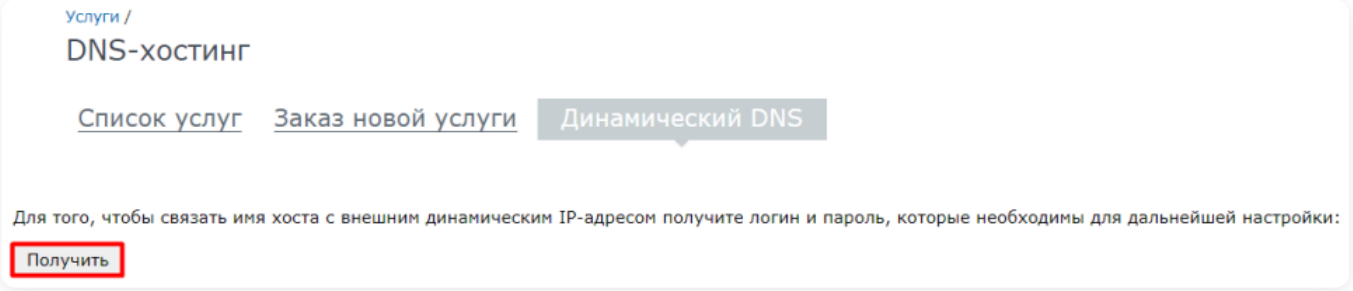
- Первая запись:
  - Name - укажите знак `@`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco NGFW (указывается в разделе *Техническая поддержка* → *Информация для технической поддержки*);
  - TTL - оставьте не заполненным.
- Вторая запись:
  - Name - укажите `www`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco NGFW;
  - TTL - оставьте не заполненным.

7. Нажмите кнопку **Выгрузить зону**:



8. Перейдите в раздел **DDNS** в Ideco NGFW 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, нажав соответствующую кнопку.

DHCP-сервер

Название службы раздела **DHCP**: `ideco-dnsmasq`.

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 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

- **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 управления настройками DHCP-сервера перейдите в раздел **Сервисы** → **DHCP-сервер**.

На локальном интерфейсе Ideco NGFW, участвующем в раздаче адресов, должен быть настроен статический IP-адрес.

При использовании DHCP-сервера включите опцию в левом верхнем углу:



Настройки

Если Ideco NGFW является шлюзом и DNS-сервером для всех сетевых устройств локальной сети, то настройка службы ограничивается определением диапазона IP-адресов.

Если на Ideco NGFW 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:

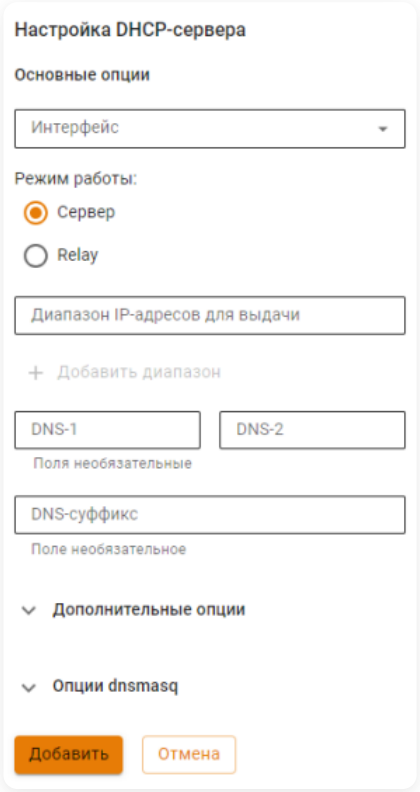
- **Основные опции** - задаются диапазоны IP-адресов и DNS-серверы.
- **Дополнительные опции** - статические маршруты, адреса WINS-серверов, время аренды, PXE Boot и WPAD.
- **Опции dnsmasq** - предназначены для ручного задания опций DHCP, передаваемых сервером клиенту при получении сетевых реквизитов от DHCP-сервера.

Основные опции

Если в разделе **Файрвол** 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

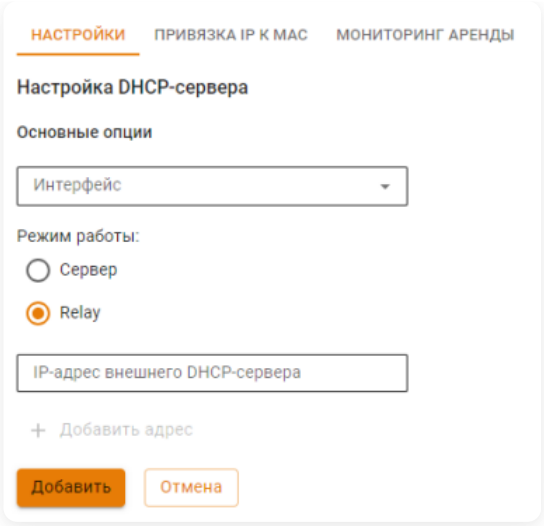
Выберите режим работы **Сервер**, чтобы настроить выдачу IP-адресов на Ideco NGFW. Заполните поля:



- **Интерфейс** - выберите интерфейс, который будет участвовать в раздаче адресов.
- **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.
- **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.

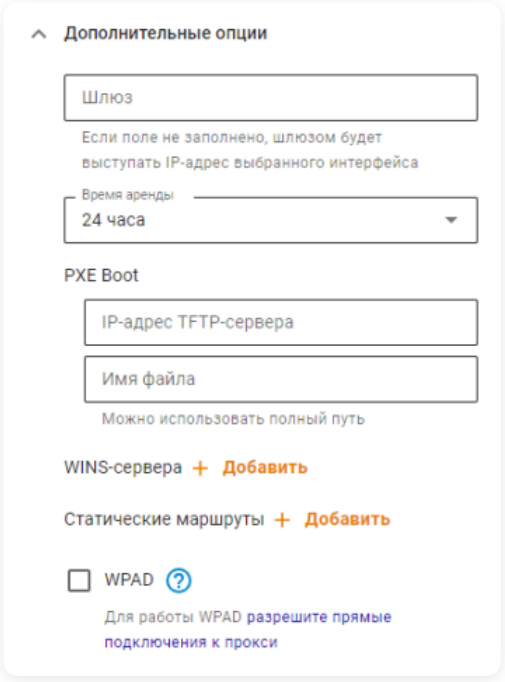
Режим работы Relay

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

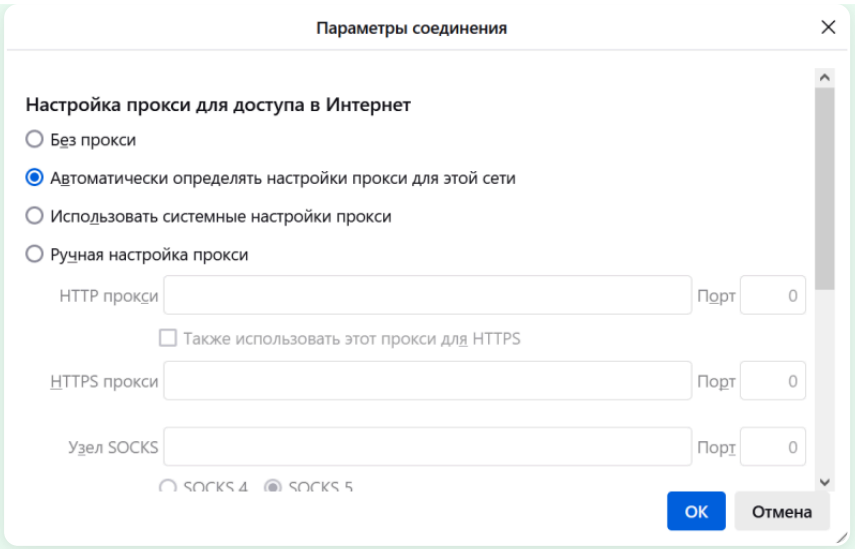


- **Шлюз** - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса.
- **Время аренды** - время, на которое выдается IP-адрес.
- **PXE Boot** - IP-адрес TFTP-сервера для настройки загрузки образа по сети.
- **WINS-сервера** - IP-адрес WINS-сервера.
- **Статические маршруты** - подсеть и шлюз для указания статического маршрута.
- **WPAD** - протокол автоматической настройки прокси.

При включении опции WPAD Ideco NGFW 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**.

Строка **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 он ее не запрашивал.

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 раздел **Отчеты и журналы** → **Системный журнал**.
- 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 раздел **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. Она используется для указания голосового сервера:

```
176,"MCIPADD=1.2.3.4,MCPORT=1719"
```

4. После добавления 176 опции добавьте 242. Она 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.

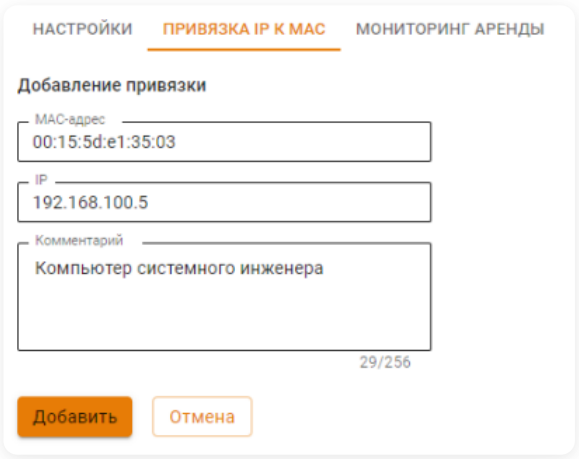
Привязка IP к MAC

> 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.

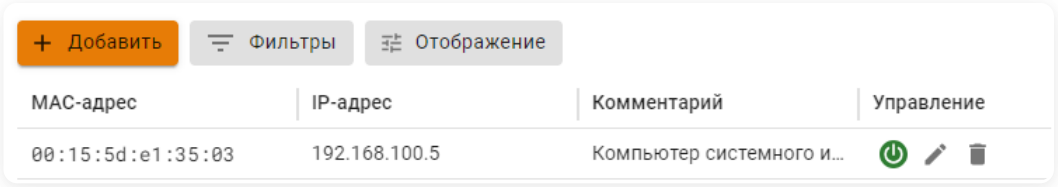
Для настройки в DHCP-сервере привязки IP-адреса к MAC-адресу необходимо:

1. В разделе **Сервисы** → **DHCP** выберите вкладку **Привязка IP к MAC**.

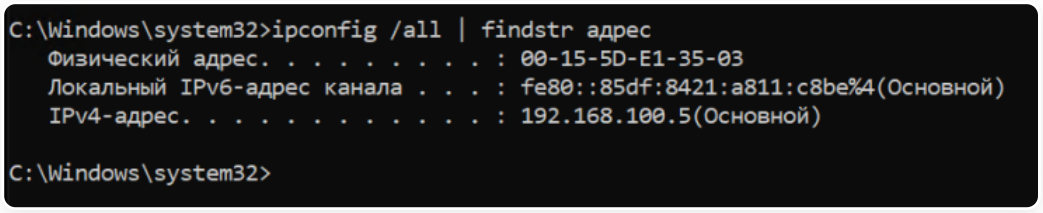
2. Создайте правило привязки **IP к MAC**:



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**.

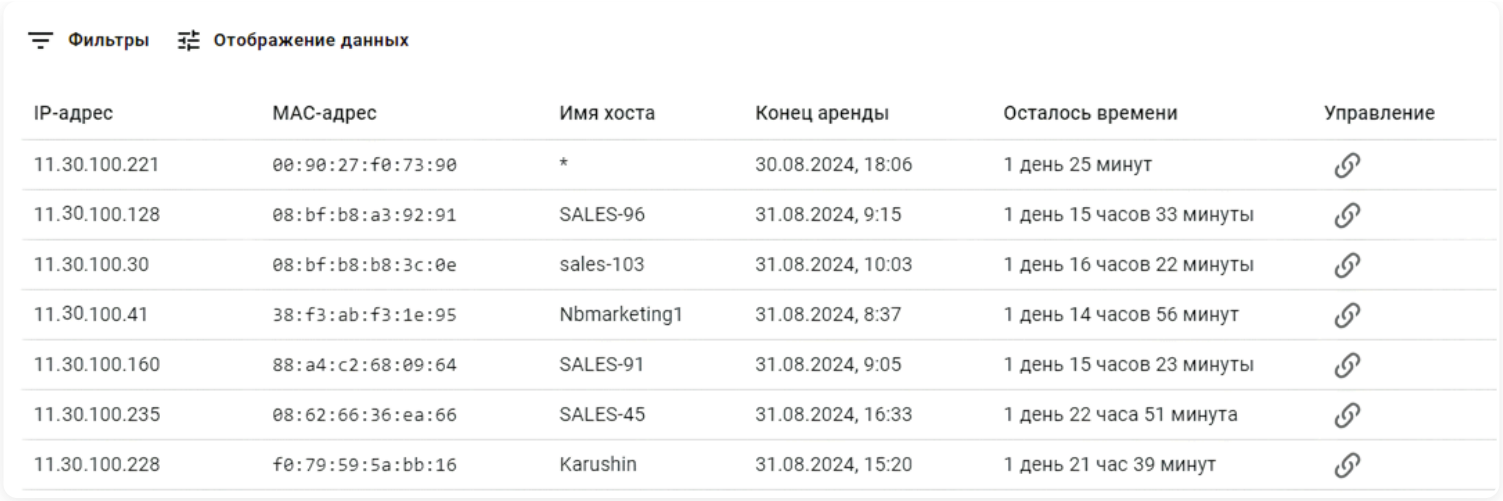
> Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW.
>
> Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (`01-02-03-04-05-06`). В настройках Ideco NGFW октеты MAC-адреса разделяются только двоеточиями (`01:02:03:04:05:06`).

Настройка DHCP-сервера для Wi-Fi сетей:

При настройке Wi-Fi сетей может понадобиться настройка DHCP-сервера. Для получения подробной информации перейдите в статью.

Мониторинг аренды

Содержит информацию об аренде IP-адресов для устройств. Для поиска воспользуйтесь кнопкой **Фильтры**:



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.

NTP-сервер

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-порту.

Принцип работы

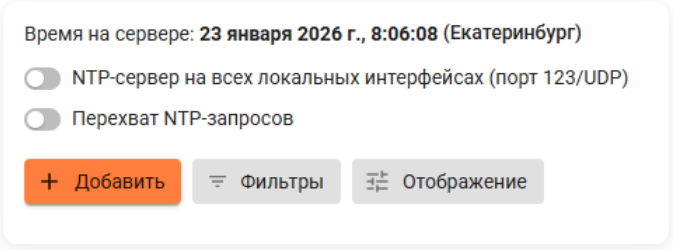
Серверы времени, используемые в NTP, имеют свою иерархию:

- 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 по умолчанию работает как NTP-клиент, получая точное время от эталонных серверов верхнего уровня. При этом Ideco NGFW также может быть настроен как локальный NTP-сервер для устройств во внутренней сети.

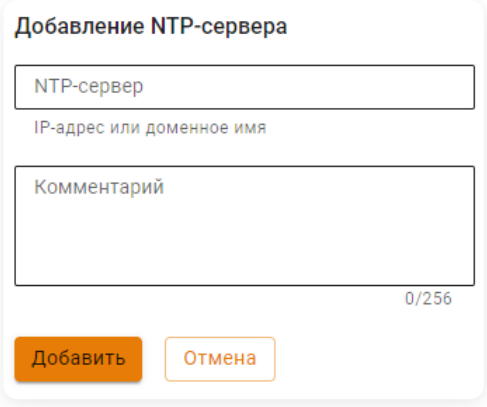
Настройка Ideco NGFW

В **Сервисы** → **NTP-сервер** доступны настройки:



- **NTP-сервер на всех локальных интерфейсах (порт 123/UDP)** - при включении опции NGFW будет доступен в качестве NTP-сервера для локальных клиентов. В этом случае NGFW 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, даже если были отправлены на другой NTP-сервер. В результате все устройства в сети будут получать время только от NGFW, независимо от их собственных настроек.
- Таблица внешних NTP-серверов - в таблице можно вручную указать NTP-серверы, с которыми необходимо синхронизировать время NGFW:
  - Если таблица пуста, NGFW синхронизирует время с сервером `ntp.ideco.ru`.
  - Если в таблице есть записи, NGFW будет синхронизироваться только с указанными серверами.

Чтобы создать запись в таблице, нажмите **Добавить** и введите IP-адрес или доменное имя в поле **NTP-сервер**:



При наличии большого количества NTP-серверов в таблице воспользуйтесь кнопкой **Фильтры**.

IPsec

Название службы раздела **IPsec**: `ideco-ipsec-backend`, `strongswan`.

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. Они позволяют сгенерировать конфиг, запуск которого на удаленном устройстве установит заранее подготовленные настройки IPsec.

Особенности подключений IPsec

В туннельном режиме:

- Интерфейсы без выхода в интернет имеют меньший приоритет по сравнению с интерфейсами с доступом в интернет.
- Поддерживается неограниченное число туннелируемых IP-адресов.
- Для создания туннелей используются все внешние интерфейсы со шлюзом по умолчанию и все **Адреса удаленного устройства**, указанные при создании IPsec-подключений.
- Для каждого **Адреса удаленного устройства** создается столько туннелей, сколько имеется внешних интерфейсов.
- Выбор конкретного туннеля для обмена трафиком зависит от приоритета внешнего интерфейса в таблице раздела **Балансировка и резервирование**. Приоритет интерфейса определяется местом в таблице: чем выше интерфейс, тем больше у него приоритет.

Необходимо заполнять поле **IP-адрес интерфейса туннеля** для обеспечения доступа Ideco NGFW к удаленным сетям за другим устройством (например, для доступа к Ideco Center или Active Directory). В будущих версиях Ideco NGFW без указания IP-адреса доступность удаленных ресурсов через IPsec не будет гарантирована.

Туннельный режим не пропускает широковещательные рассылки, поэтому в таком режиме настроить OSPF не получится.

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.

IPsec использует протокол UDP, порты 500 и 4500. По умолчанию они открыты, но если настроено запрещающее правило во вкладке **INPUT** раздела **Файрвол**, не забудьте добавить разрешение для IPsec.

Исходящие и входящие подключения

Настройте исходящее подключение, если Ideco NGFW 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 при создании подключения, отправляется удаленному устройству и подписанный возвращается для настройки NGFW. • Корневой сертификат удаленного устройства. • Список домашних локальных сетей NGFW, которые будут видны противоположной стороне. • Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	• PSK-ключ. Генерируется на NGFW при создании подключения. • Идентификатор ключа, который потребуется удаленному устройству для идентификации подключения. • Список локальных сетей NGFW, 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, 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 для идентификации входящего подключения. • Список локальных сетей NGFW, которые будут видны противоположной стороне. • Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

Выбор алгоритмов шифрования на удаленных устройствах

При настройке сторонних устройств необходимо явно указать алгоритмы шифрования, используемые для подключения.

Ideco NGFW 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, SHA256, SHA384**.
  - 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)**.
    - **modp1024 (group 2)**.
  - Таймауты:
    - **Lifetime**: 14400 сек.
    - **DPD Timeout** (для L2TP/IPsec): 40 сек.
    - **DPD Delay**: 30 сек.
- **Phase 2 (ESP):**
  - encryption (шифрование):

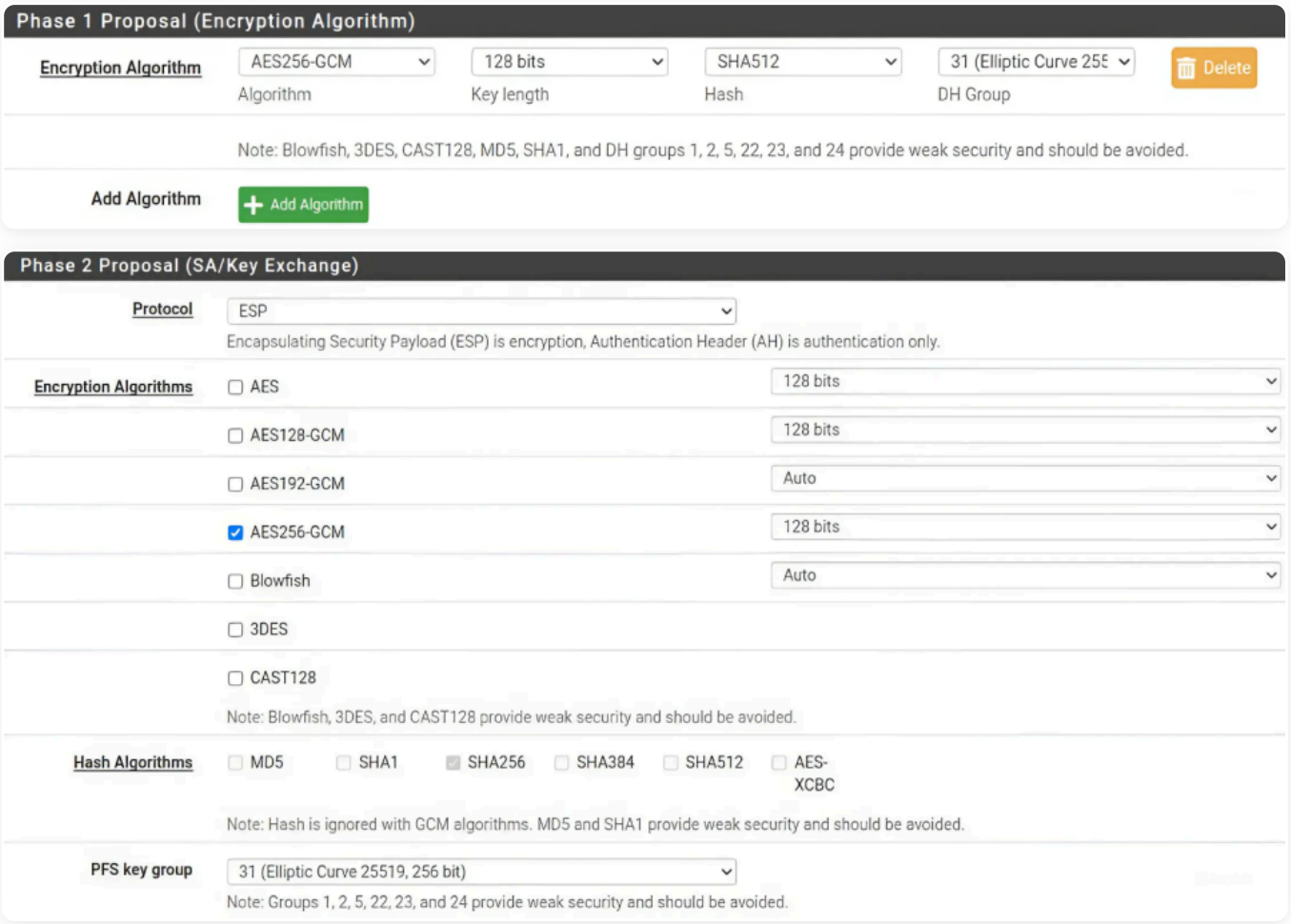
        - **AES256-GCM**.
        - **AES256 (AES256-CBC)**.
    - integrity (целостность):
        - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
        - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
    - DH (Группа Diffie-Hellman, 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)**.
        - **modp1024 (group 2)**.
    - 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 по IPsec:



В Ideco NGFW 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.

Мониторинг производительности сети

В Ideco NGFW 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 для каждого активного соединения отображаются метрики:

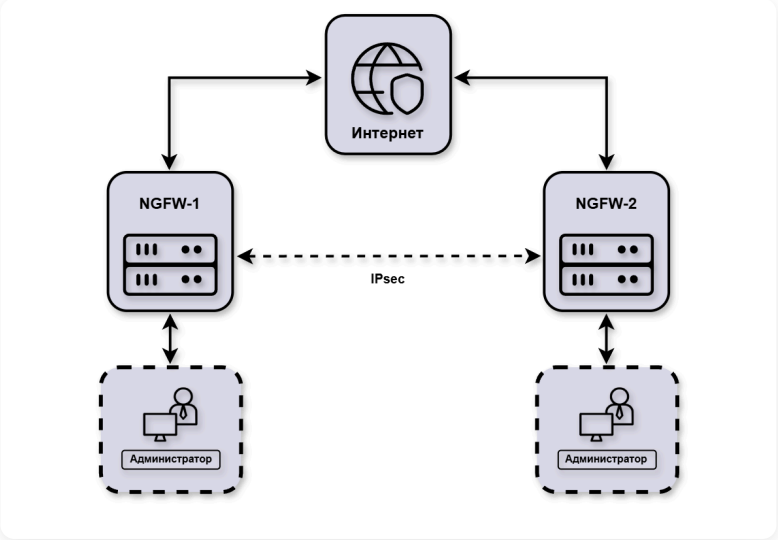
- **Вх. скорость, Мбит/с** - скорость приема данных через туннель.
- **Исх. скорость, Мбит/с** - скорость передачи данных через туннель.
- **Средняя задержка, мс** - время, за которое пакет доходит до удаленной стороны туннеля и возвращается обратно.
- **Потеря пакетов, шт.** - количество количество 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.

Подключение между двумя Ideco NGFW в туннельном режиме работы

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru



Для создания IPsec-подключения между Ideco NGFW 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.

Шаг 1. Проверка условий подключения

Перед созданием подключения убедитесь, что:

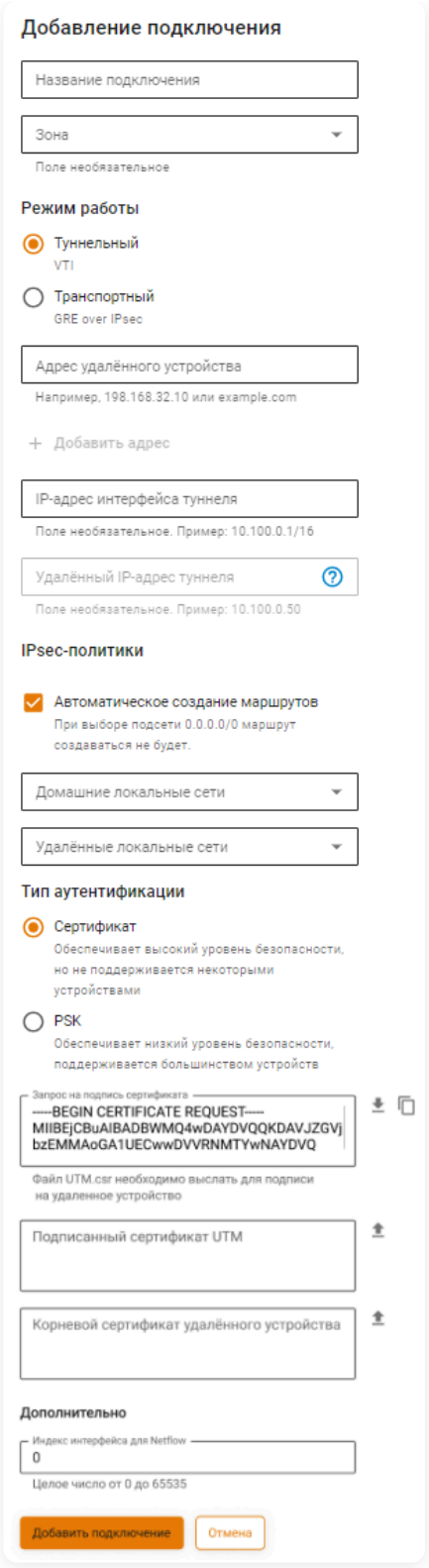
- На **NGFW-1** и **NGFW-2 правильно настроены временные зоны**. Без этого подключение не установится.
- Для работы IPsec все подсети, участвующие в соединениях, не пересекаются.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. **Входящее подключение должно настраиваться на сервере с белым IP-адресом**.
- Пользовательские правила из раздела **Правила трафика** → **Файрвол** → **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 раздел **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 **Туннельный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес. Адресов может быть несколько. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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 к удаленным сетям за другим устройством.

- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW.
- **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 UTM**.



Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они 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 разделе **Сервисы** → **Маршрутизация** или динамическую маршрутизацию через BGP в разделе **Сервисы** → **BGP**.

3. Выполните действие для нужного типа аутентификации:

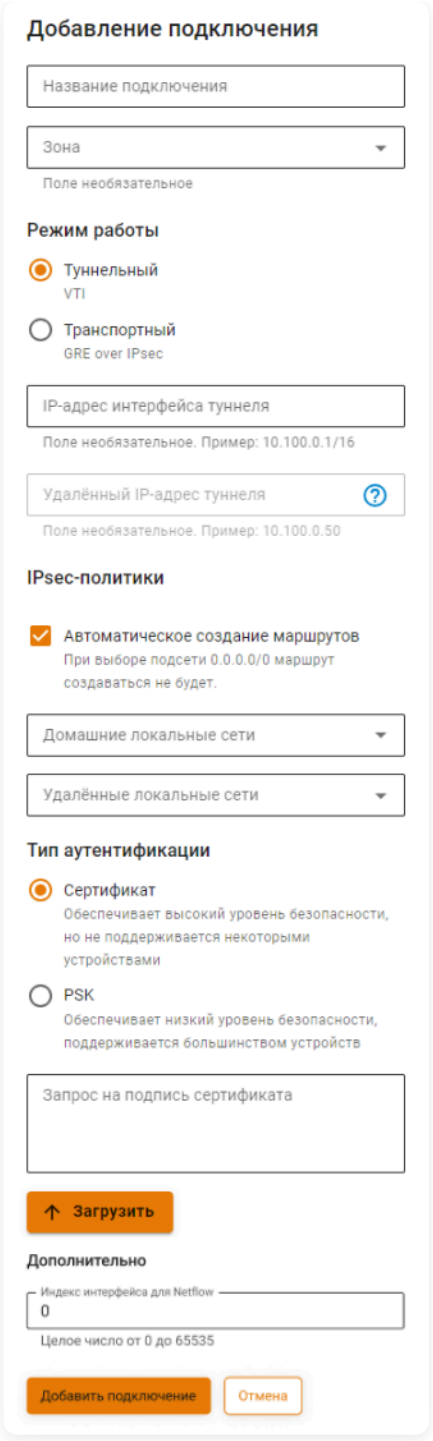
- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 3**.
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 3** для настройки входящего подключения на **NGFW-2**.

Шаг 3. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **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**.
- **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 к удаленным сетям за другим устройством.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-1**. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW.

- **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW.

- **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 в разделе **Сервисы** → **Маршрутизация** или динамическую маршрутизацию через BGP в разделе **Сервисы** → **BGP**.

3. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

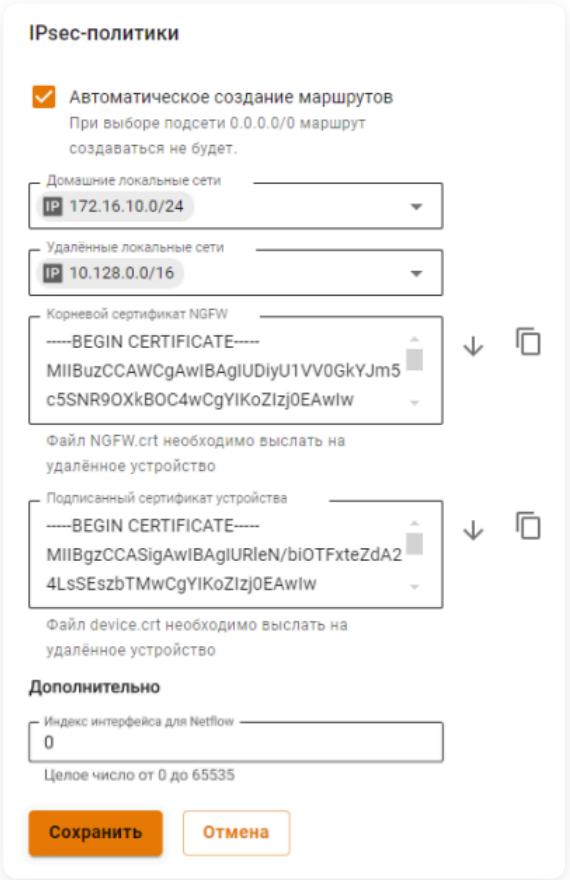
Если был выбран тип аутентификации **PSK**, то настройка завершена.

Если был выбран тип аутентификации **Сертификат**, то выполните **Шаг 4**.

Шаг 4. Донастройка исходящего подключения с типом аутентификации Сертификат

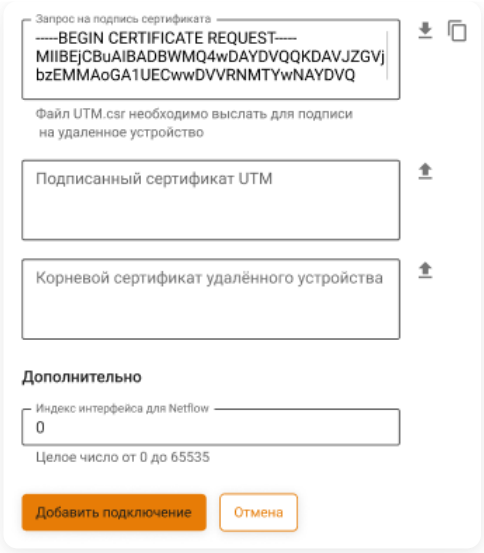
1. В **NGFW-2** перейдите в раздел **Сервисы** → **IPsec** → **Входящие подключения** и нажмите по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **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**.

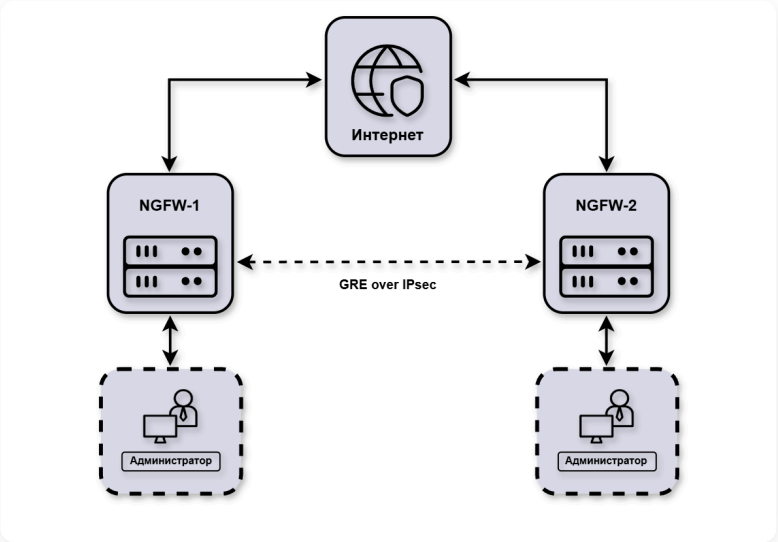
2. Укажите в поле **Домашние локальные сети** сеть, используемую для VPN в **NGFW-2**.

> В Ideco NGFW 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 в транспортном режиме работы

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru



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 их 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** → **Файрвол** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протоколов ESP и UDP (порты 500 и 4500).
- Пользовательские правила из раздела **Правила трафика** → **Файрвол** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протокола GRE.
- Ни один Ideco NGFW не находится за NAT, так как в таком случае подключение двух Ideco NGFW 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 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.

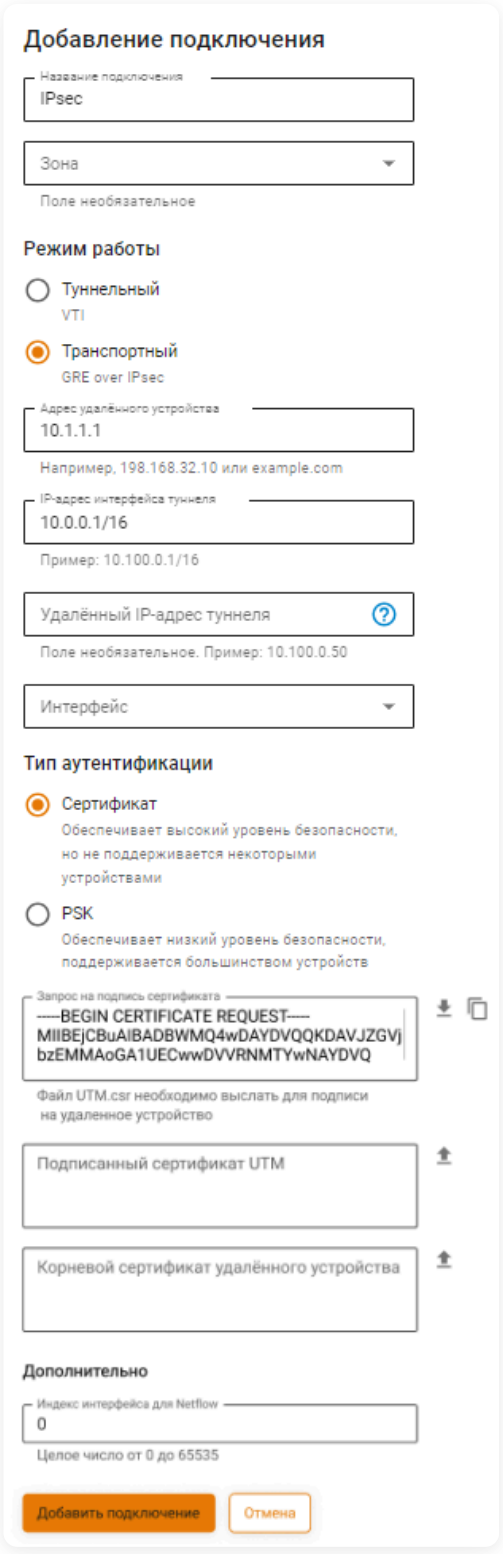
Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе Туннельные. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec, либо использовать разные адреса для 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 раздел **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 или его белый IP-адрес.
- **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.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его IP-адрес, доступный с сетевого интерфейса, указанного в поле выше.
- **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.

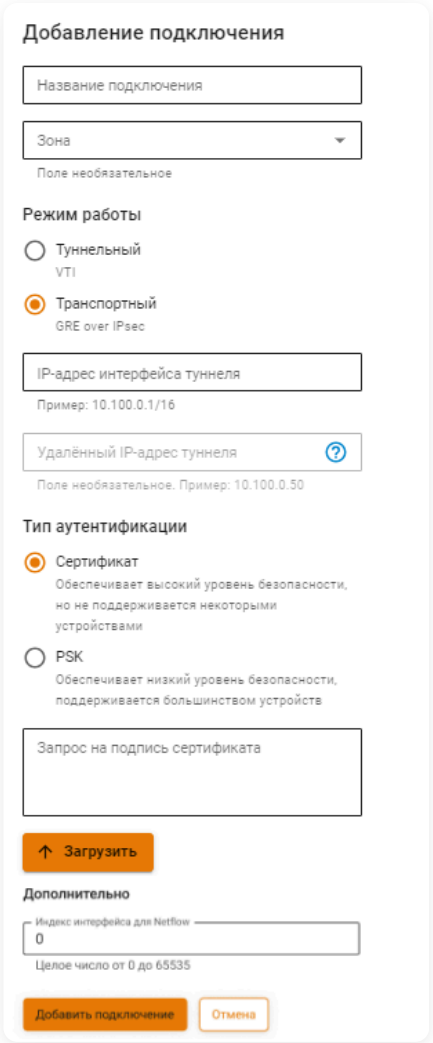
4. Если тип аутентификации - **PSK**, проверьте правильность заполнения полей и нажмите **Добавить подключение** и перейдите к **Шагу 2**. Если тип аутентификации - **Сертификат**, **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 2** для настройки входящего подключения на другом NGFW.

Шаг 2. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **Сервисы** → **IPsec** → **Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

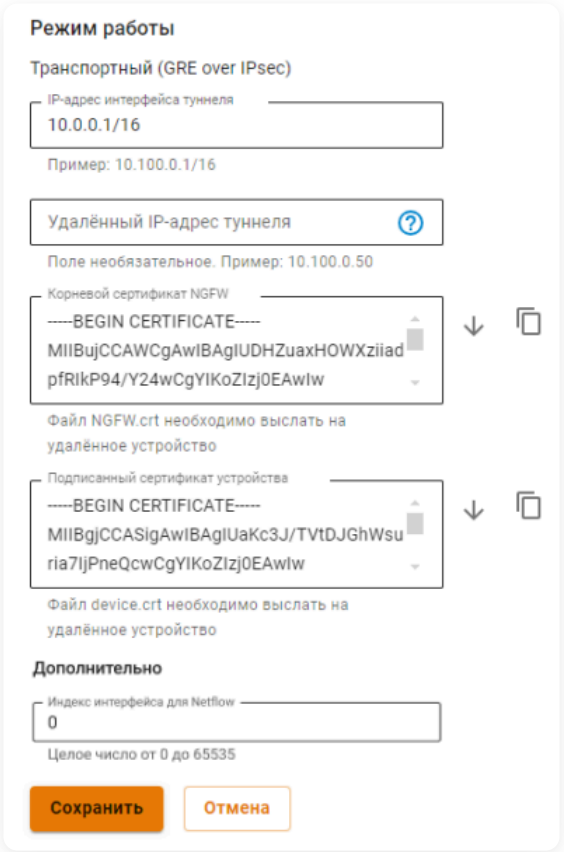
- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **IP-адрес интерфейса туннеля** - укажите 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 интрефейса 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

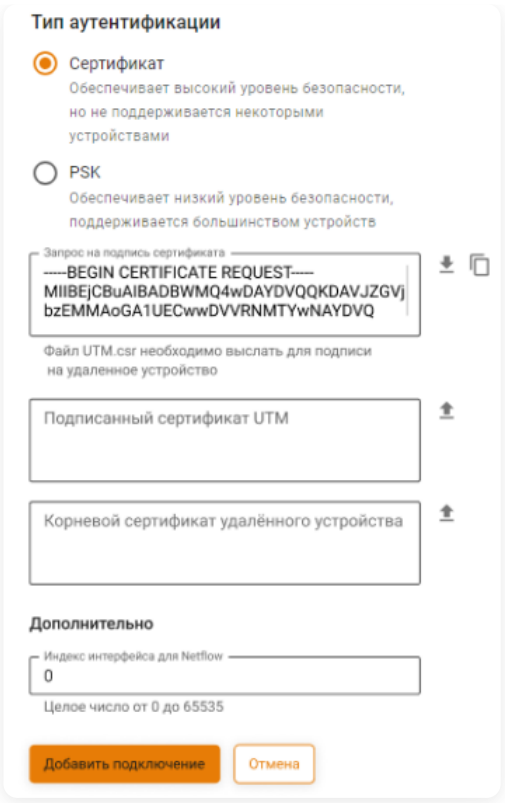
1. В **NGFW-2** перейдите в раздел **Сервисы** → **IPsec** → **Входящие подключения** и нажмите по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **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 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 и MikroTik по IPsec в туннельном режиме

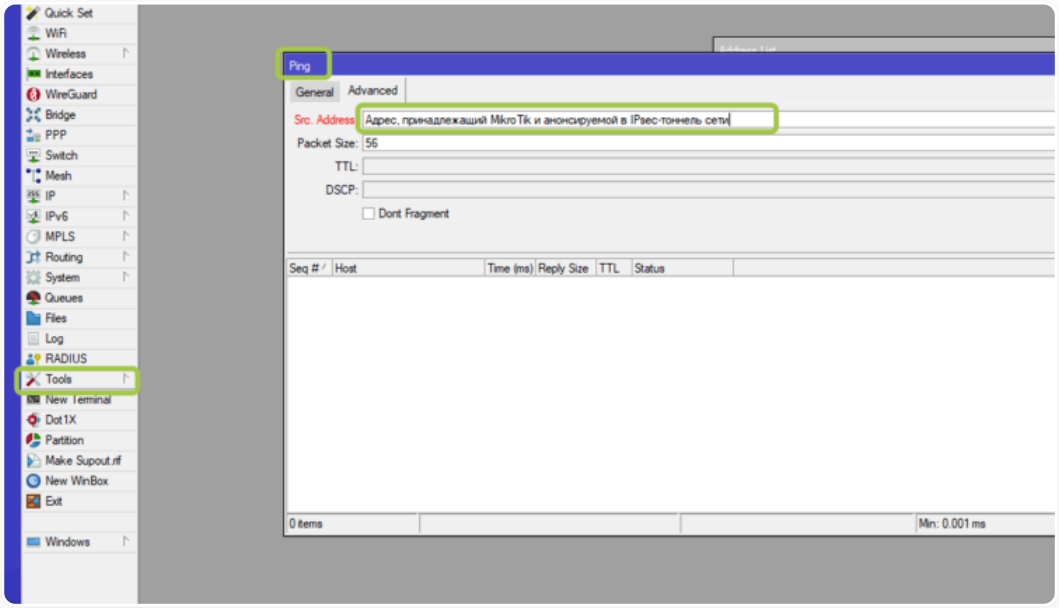
В статье описана настройка IPsec-подключения между Ideco NGFW и MikroTik с аутентификацией по сертификатам или PSK.

Требования и подготовка

Основные требования:

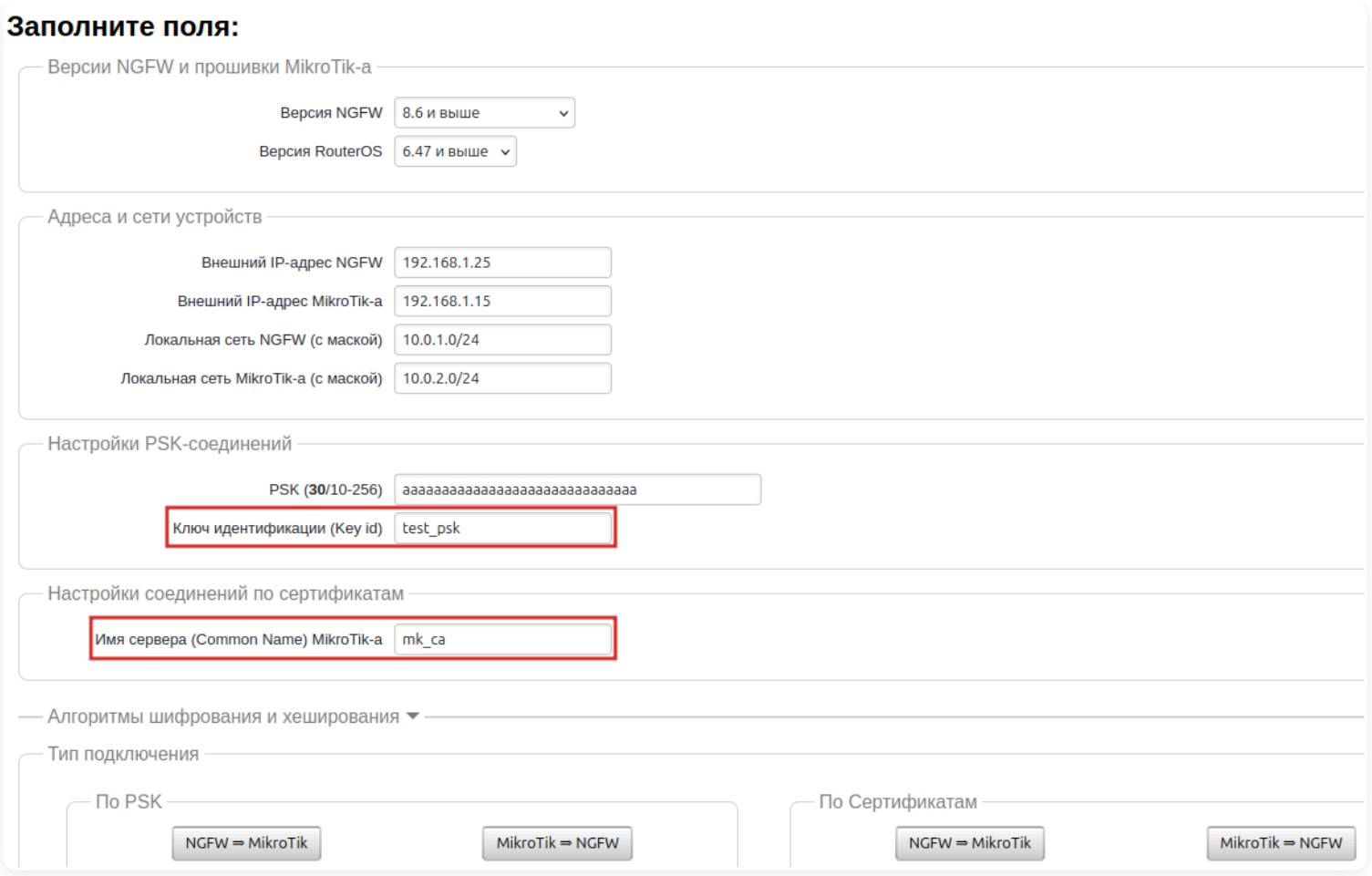
- Локальные сети в разных офисах не должны пересекаться.
- Для корректной работы подключений по сертификатам синхронизируйте время на MikroTik по NTP (например, предоставьте доступ в интернет).
- IPsec-подключения от Ideco NGFW к MikroTik версии 6.45 и ниже по сертификатам не работают, так как нельзя использовать современные криптоалгоритмы.

Для проверки доступности анонсируемых сетей Ideco NGFW с MikroTik указывайте IP-адрес источника:



При подключении нескольких устройств MikroTik к одному Ideco NGFW **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 к MikroTik

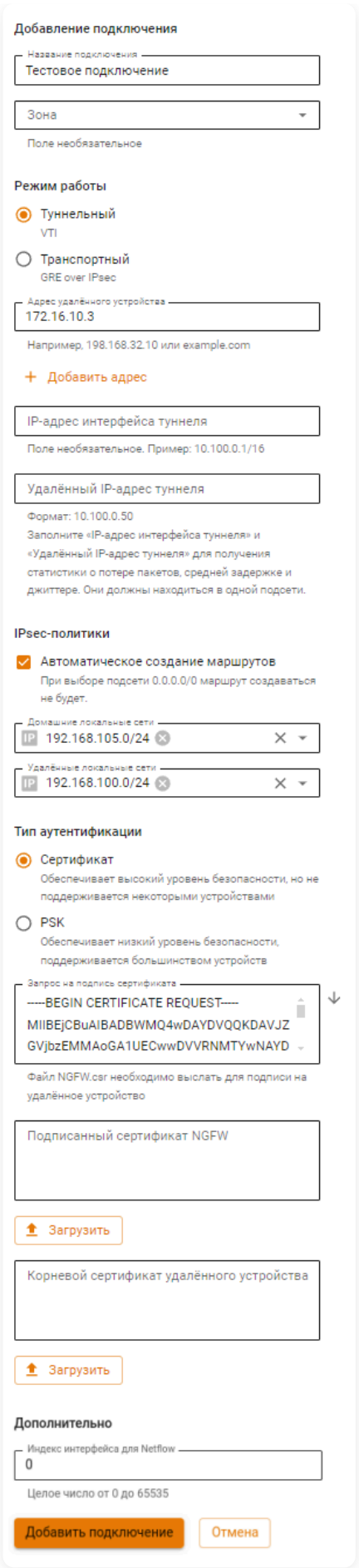
Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

Шаг 1. Настройка Ideco NGFW (исходящее подключение)

Сгенерируйте запрос на подпись сертификата:

1. В Ideco NGFW 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. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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.

> **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, необходимо загрузить в файловое хранилище MikroTik:

1. Откройте раздел **File**.

2. Нажмите кнопку **Browse**.

3. Выберите файл и загрузите его.

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

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW.

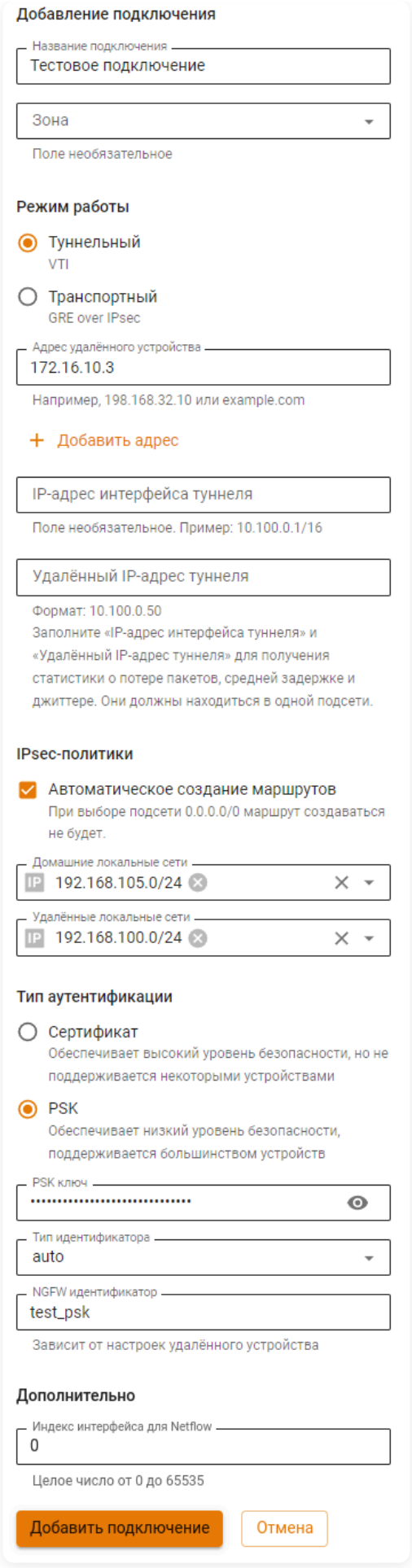
1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

PSK

Шаг 1. Настройка Ideco NGFW (исходящее подключение)

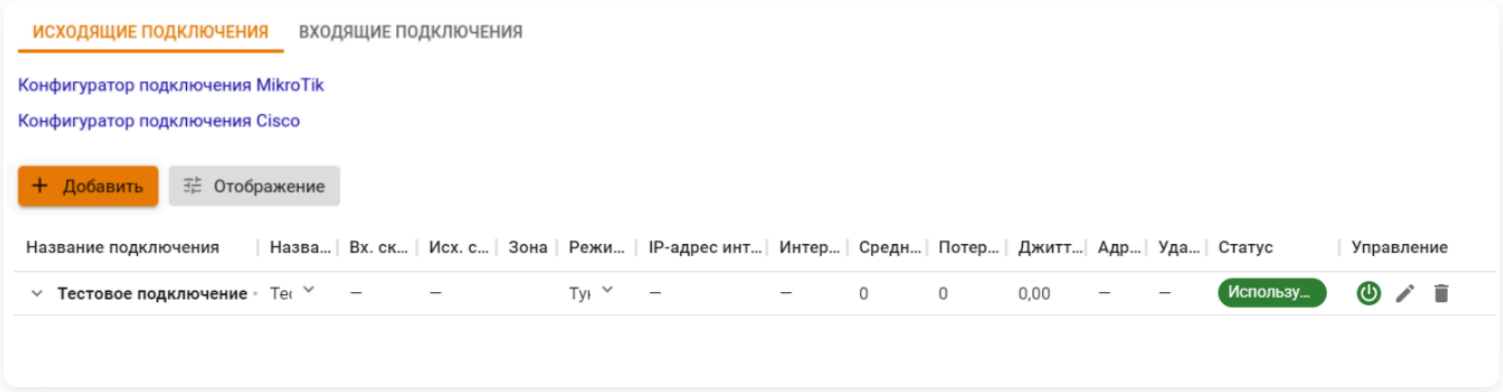
1. Откройте **Сервисы** → **IPsec** → **Исходящие подключения**, нажмите **Добавить** и заполните поля:



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 устройства MikroTik. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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. Он потребуется 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

Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

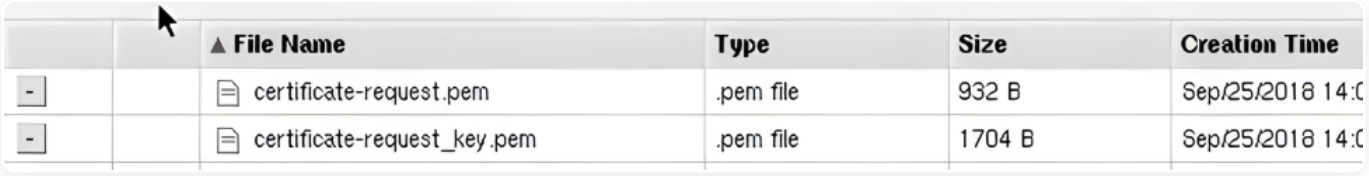
Шаг 1. Предварительная настройка MikroTik

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.

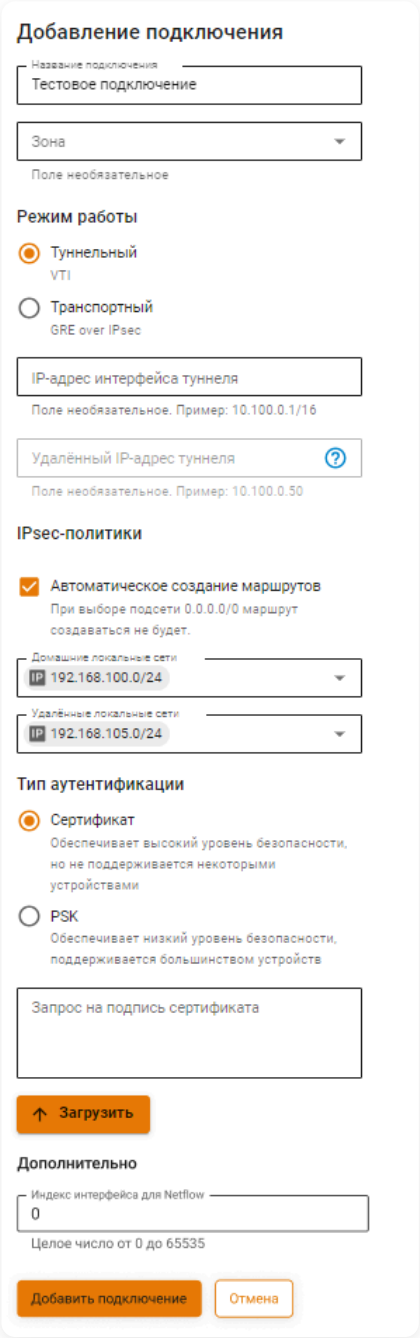
Перед настройкой необходимо запустить первый скрипт для запроса на подпись сертификата. После чего в файловом хранилище MikroTik появятся два файла, которые необходимо скачать. Файлы потребуются для дальнейшей настройки:



- Файл `certificate-request.pem` - запрос на подпись сертификата.
- Файл `certificate-request_key.pem` - приватный ключ.

Шаг 2. Настройка Ideco NGFW (входящее подключение)

1. В Ideco NGFW откройте **Сервисы** → **IPsec** → **Входящие подключения**, нажмите **Добавить** и заполните поля:



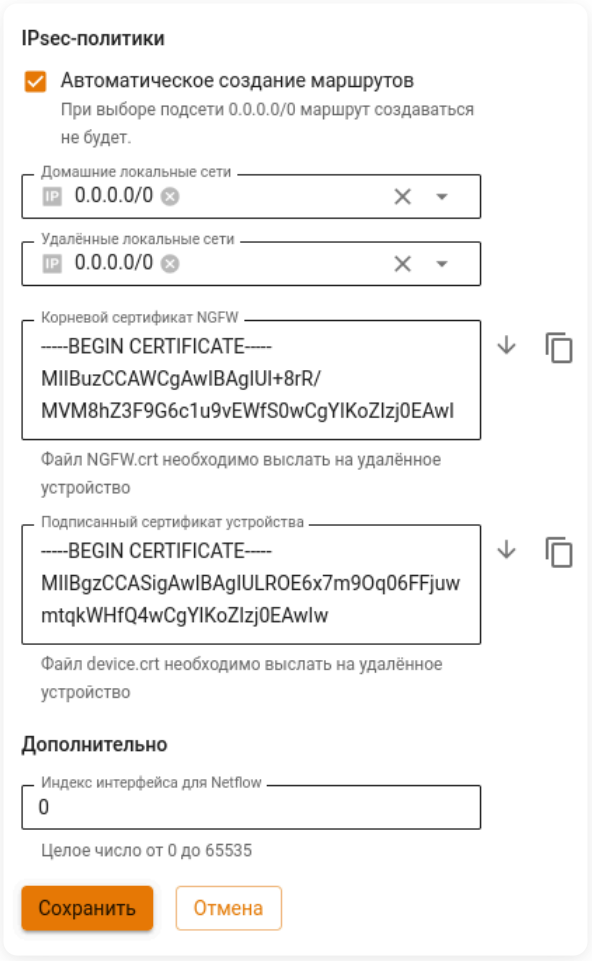
Расшифровка полей

- **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**.
- **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 **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.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)

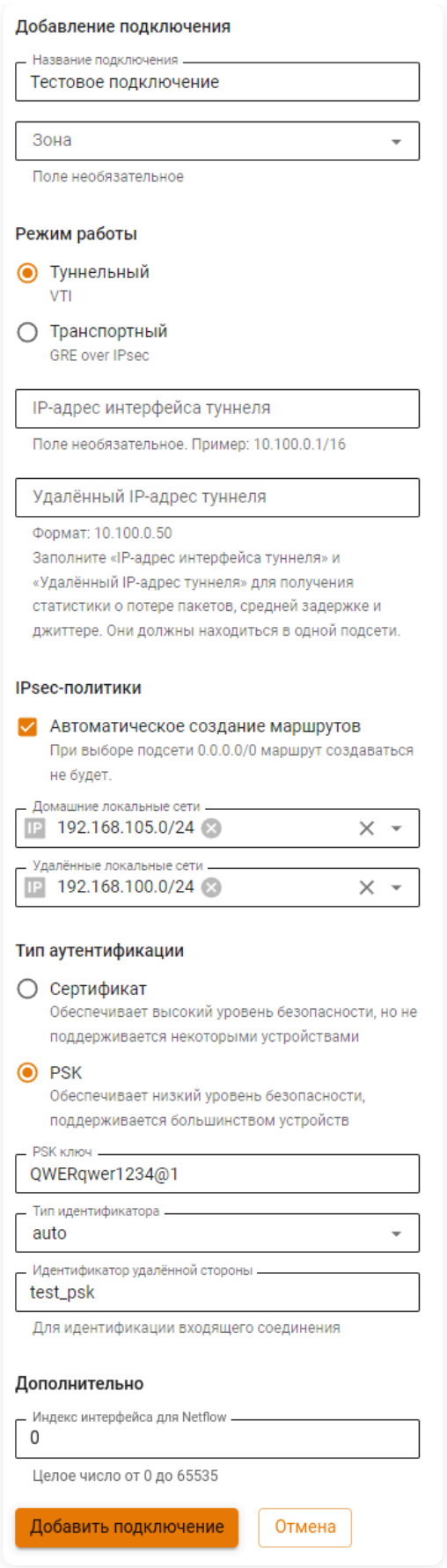
Настроить устройство MikroTik можно через:

- 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 (входящее подключение)

1. В Ideco NGFW 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**.

- **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 **auto**.
- **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**.

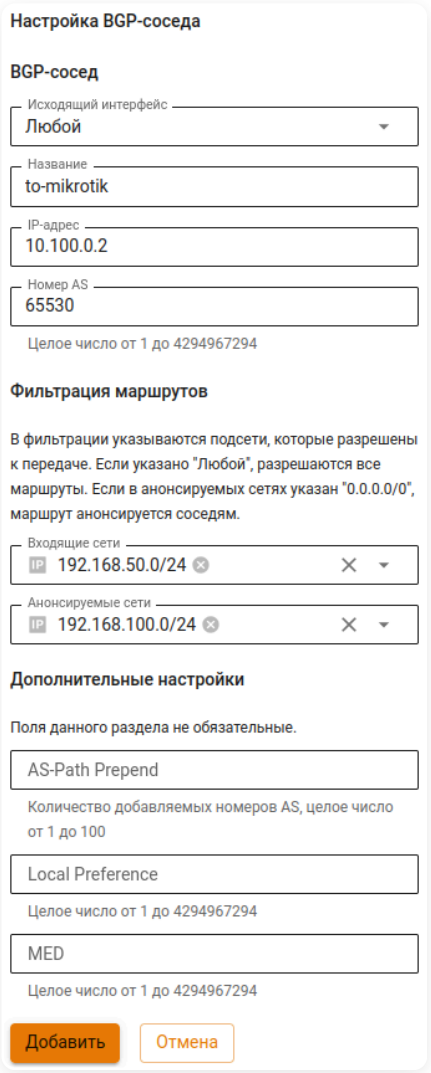
Настройка динамической маршрутизации (BGP)

Настройка Ideco NGFW

1. Перейдите в **Сервисы** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в строку **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.

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:

```
/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. 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

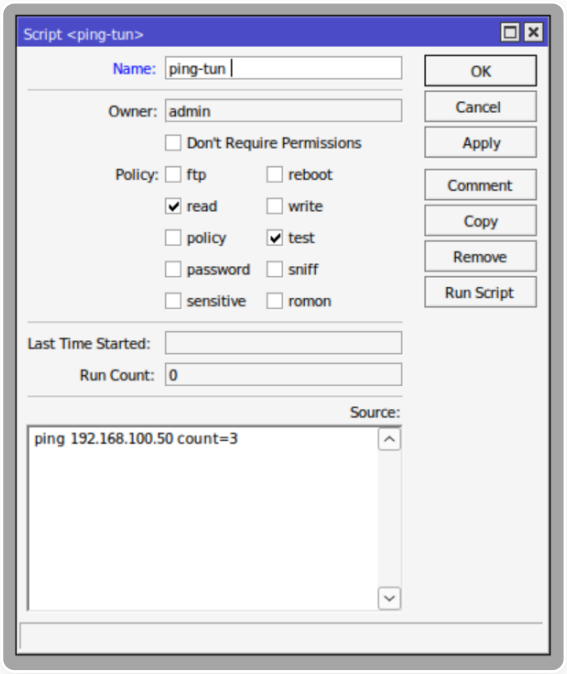
При работе туннеля между Ideco NGFW и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW.

Для автоматизации процесса поддержания соединения создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в **System** → **Scripts**.

3. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



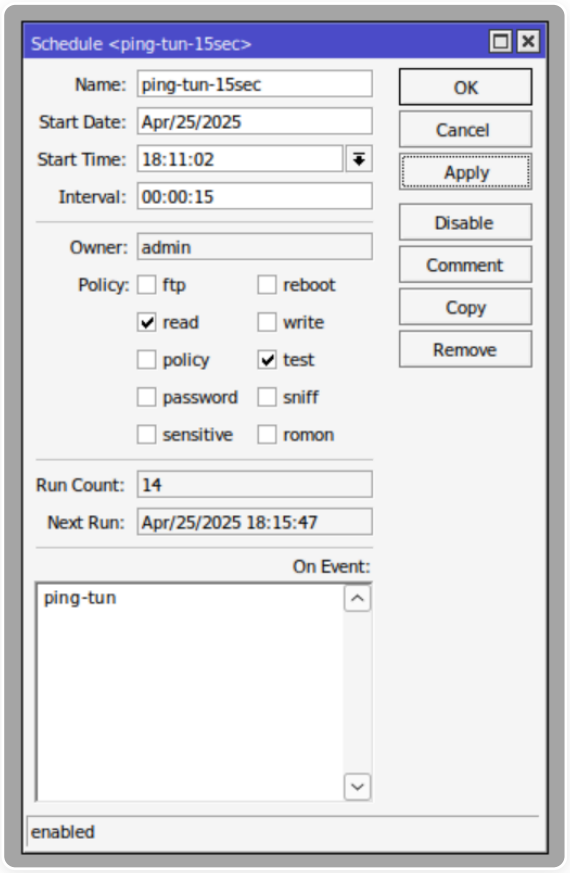
- **Name** - название скрипта (не поддерживаются пробелы и нижние подчеркивания).
- **Policy** - включите опции **read** и **test**.
- **Source** - введите команду `ping <IP-адрес Ideco NGFW> count=3`.

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. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.

> В Ideco NGFW 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 и MikroTik по IPsec в транспортном режиме

При объединении сетей с помощью VPN локальные сети в разных офисах не должны пересекаться.

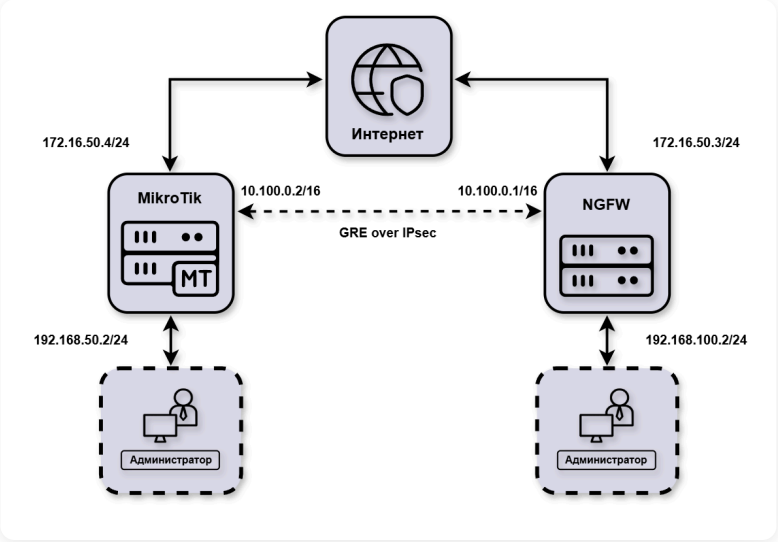
Для корректной работы подключений по сертификатам синхронизируйте время на MikroTik по NTP (например, предоставьте доступ в интернет).

IPsec-подключения от Ideco NGFW 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 следуйте инструкции в каждом из пунктов.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используются другим, уже действующим GRE-туннелем в разделе Туннельные. 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 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
```

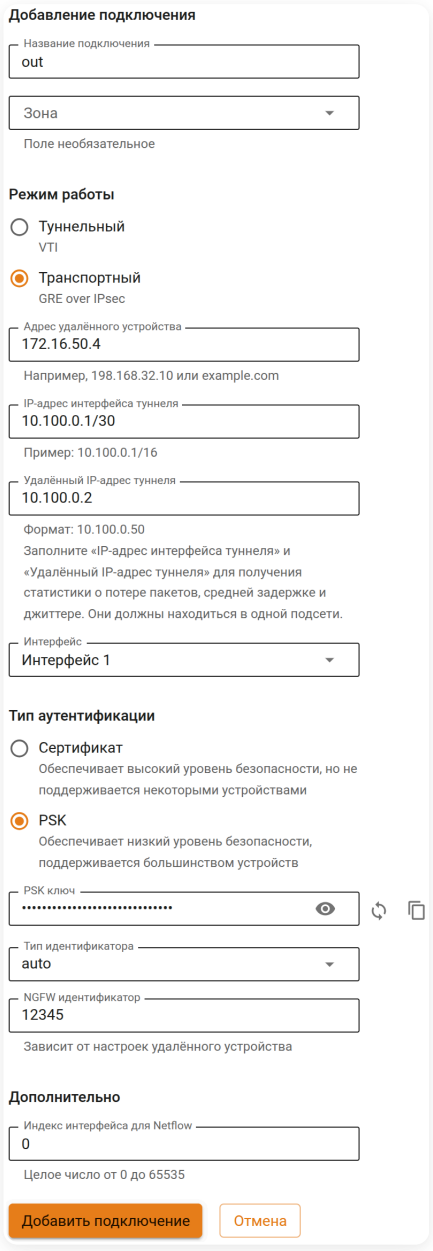
2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/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

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.
- **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.
- **Интерфейс** - выберите внешний интерфейс NGFW.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - будет сгенерирован случайный PSK-ключ. Он потребуется 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.
```

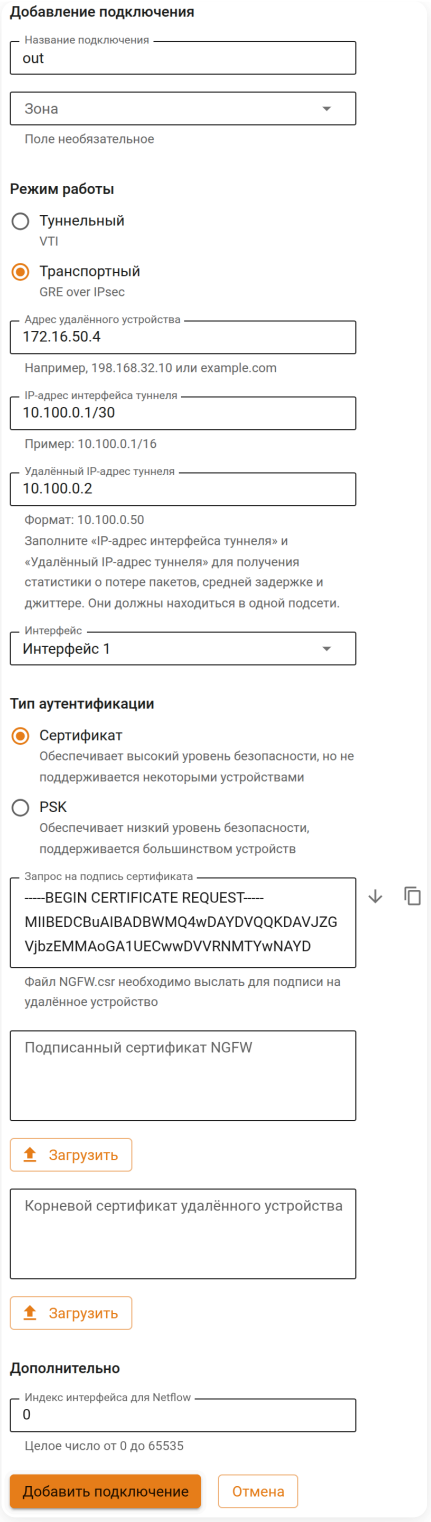
2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Тип аутентификации Сертификат

Настройка исходящего IPsec-подключения на Ideco NGFW

1. Перейдите в раздел **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.
- **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.
- **Интерфейс** - выберите интерфейс NGFW.
- **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 и сделайте его 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

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW.

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

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
```

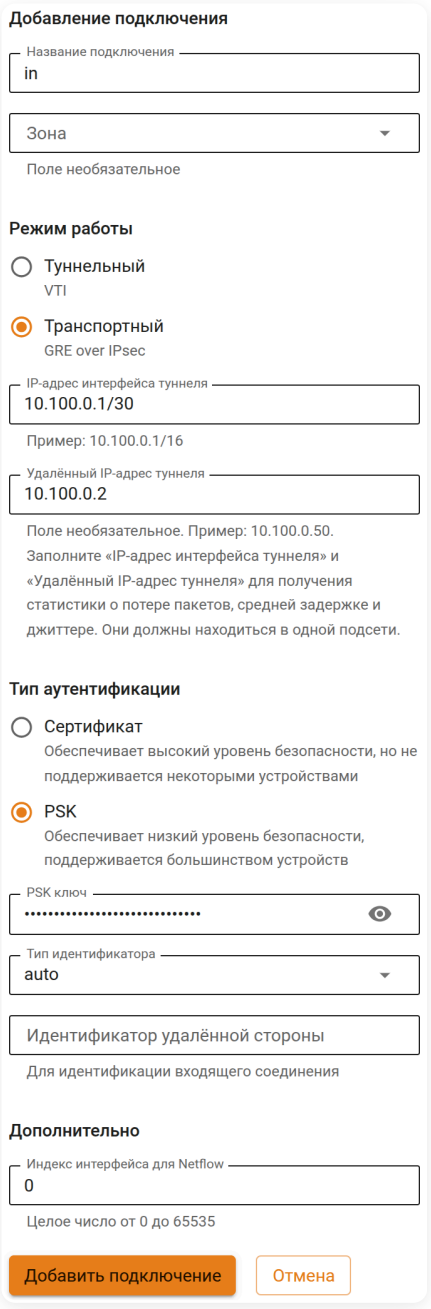
3. Настройте IPsec-подключение со стороны MikroTik:

```
/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

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.
- **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:

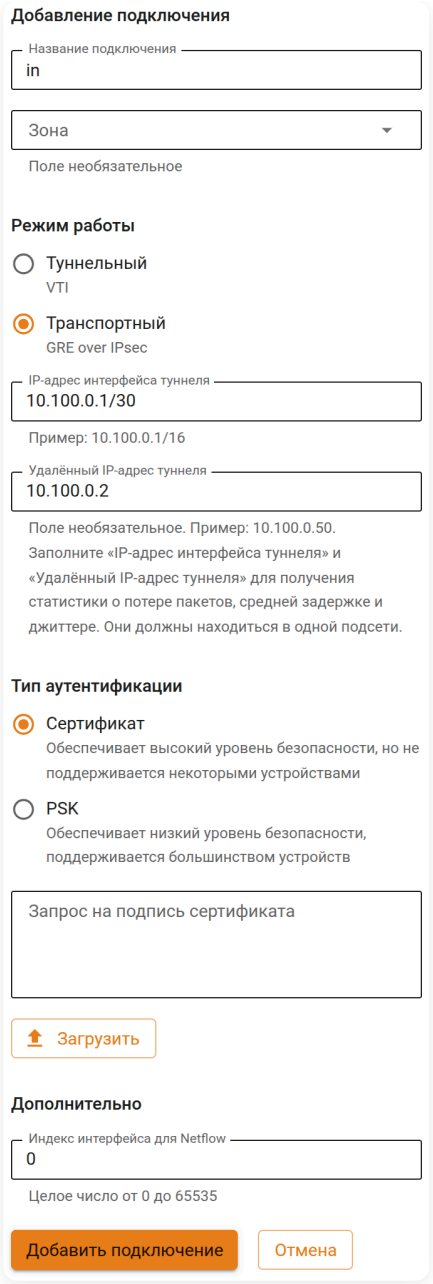
```
/certificate add name=mk_ca common-name=mk_ca key-usage=digital-signature,content-commitment
/certificate create-certificate-request key-passphrase="" template=mk_ca
```

4. Загрузите файл `certificate-request.pem` с MikroTik через WinBox или по SHH.

Настройка входящего IPsec-подключения на Ideco NGFW

1. Перейдите в раздел **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.
- **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.

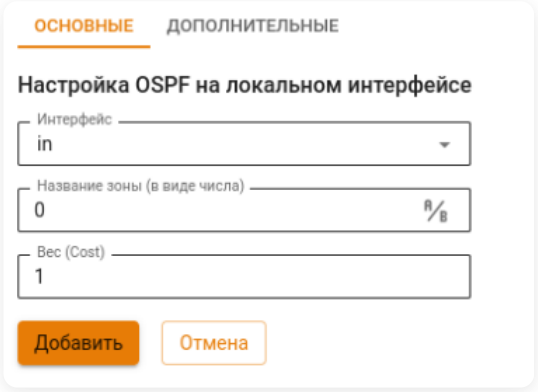
Настройка динамической маршрутизации

OSPF

Настройка на Ideco NGFW

1. Перейдите в раздел **Сервисы** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW, настроенный ранее.
- **Название зоны** - введите номер зоны (значение `area`, должно совпадать на NGFW и Mikrotik). Можно ввести в виде числа или IP-адреса, нажав иконку .
- **Вес** - введите стоимость маршрута.

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

1. Перейдите в раздел **Сервисы** → **BGP** и нажмите **Добавить**.

2. Введите номер автономной системы в строку **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:

- **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.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

5. Включите модуль **BGP**.

Настройка на 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:

```
/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 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. 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 и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW.

Для автоматизации процесса поддержания соединения, создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в раздел **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> count=3`.

4. Нажмите **Apply**, затем **Ok**.

Далее настройте запуск скрипта по расписанию в планировщике заданий:

1. Перейдите в раздел **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. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.



В Ideco NGFW 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.

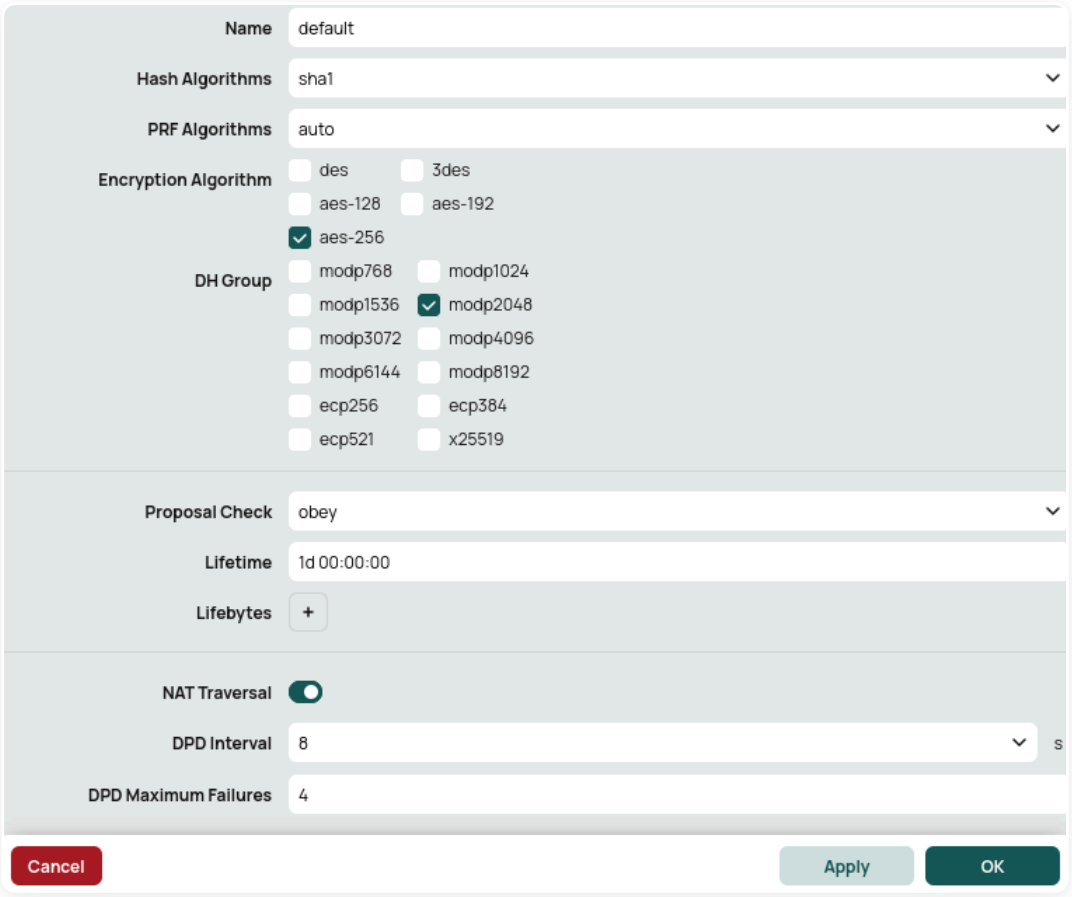
Подключение MikroTik и Ideco NGFW по L2TP/IPsec

Подключение MikroTik к Ideco NGFW по L2TP/IPsec

- Настройте VPN-сервер на Ideco NGFW в разделе **Пользователи** → **VPN-подключения**. Подробная инструкция по настройке - в статье Подключение по L2TP/IPsec;
- Настройте подключение на MikroTik:

Веб-интерфейс

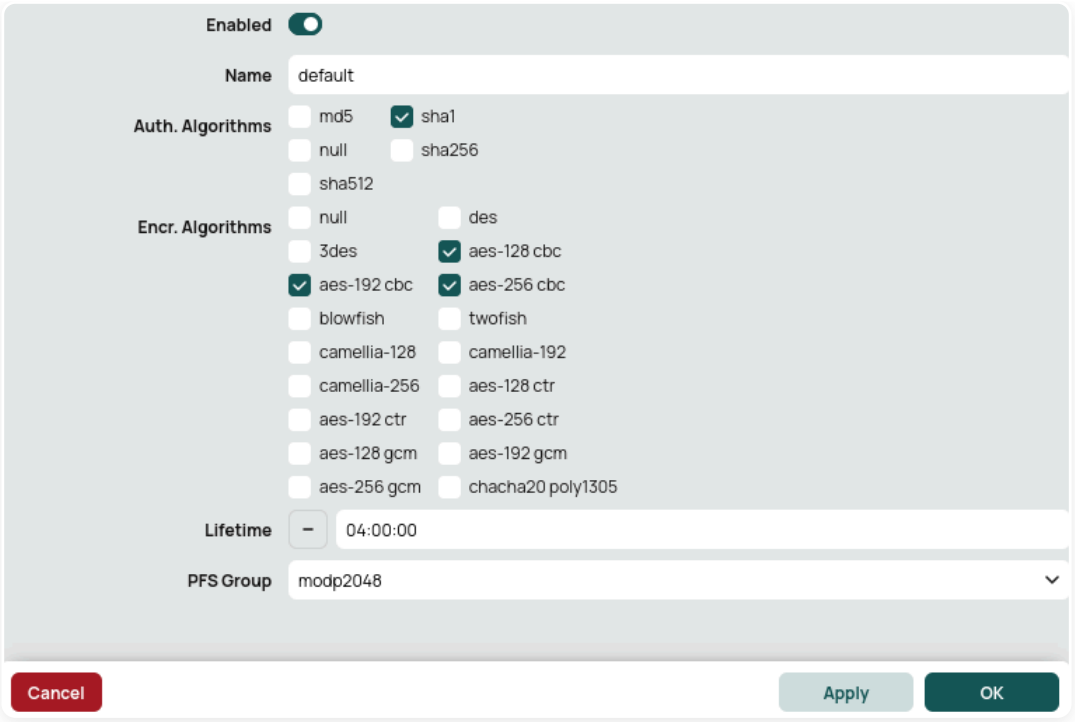
1. Перейдите в раздел **IP** → **IPsec** → **Profiles**, выберите профиль **default** и заполните поля:



- **Hash Algorithms** - `sha1`.
- **Encryption Algorithm** - `aes-256`.
- **DH Group** - `modp2048`.

2. Нажмите **OK**.

3. Перейдите в раздел **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 раздел **Interfaces**, нажмите **New** и выберите **L2TP Client**.

6. Заполните поля:

Расшифровка полей

- **Dial Out**:
  - **Connect To** - IP-адрес Ideco NGFW.
  - **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 раздел **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:

```
interface l2tp-client add connect-to=<server> profile=default disabled=no name=<interface_name> password="<password>" user="<
```

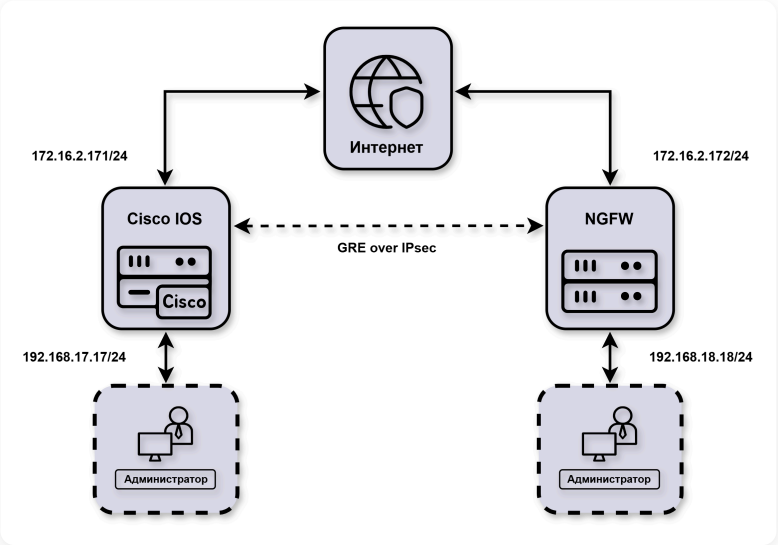
4. Добавьте маршрут до первого адреса VPN-сети NGFW (remote VPN subnet):

```
ip route add dst-address=<remote VPN subnet> gateway=l2tp-out1
```

В Ideco NGFW 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 по IPsec в туннельном режиме

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 следуйте инструкции ниже.

Первоначальная настройка Ideco NGFW и Cisco IOS

Настройка Ideco NGFW

Настройте на Ideco NGFW 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 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 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 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:

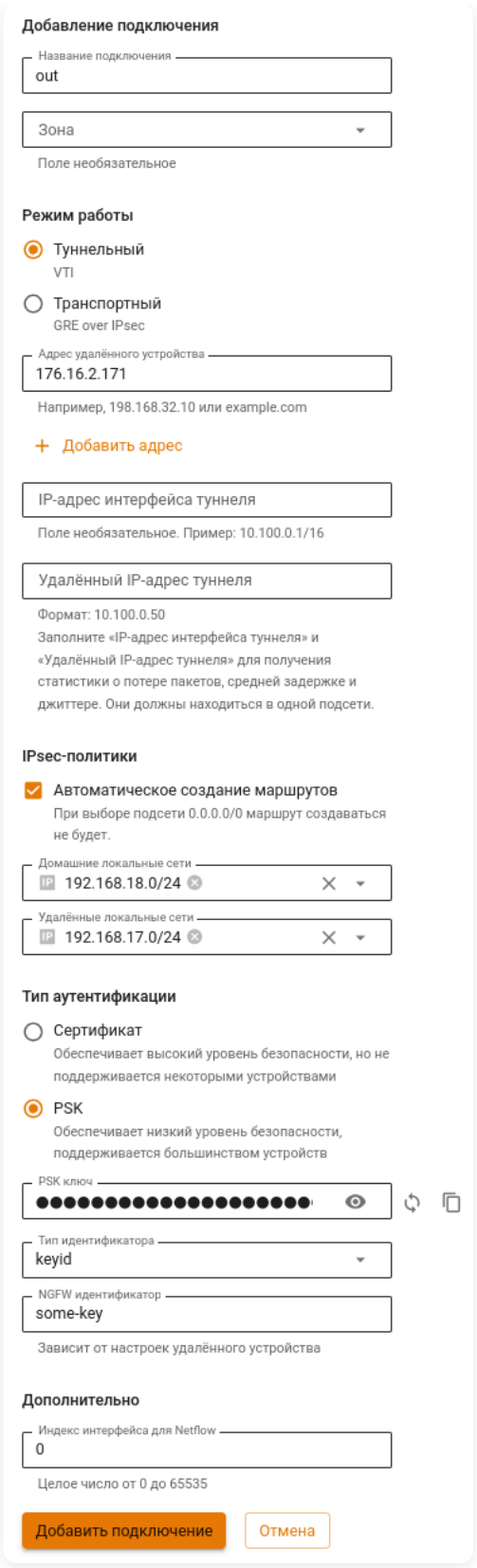
```
write memory
```

Настройка исходящего подключения на Ideco NGFW

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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 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 интрефейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной

подсети.

- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - будет сгенерирован случайный PSK-ключ. Он потребуется, чтобы настроить подключение 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.

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 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

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:

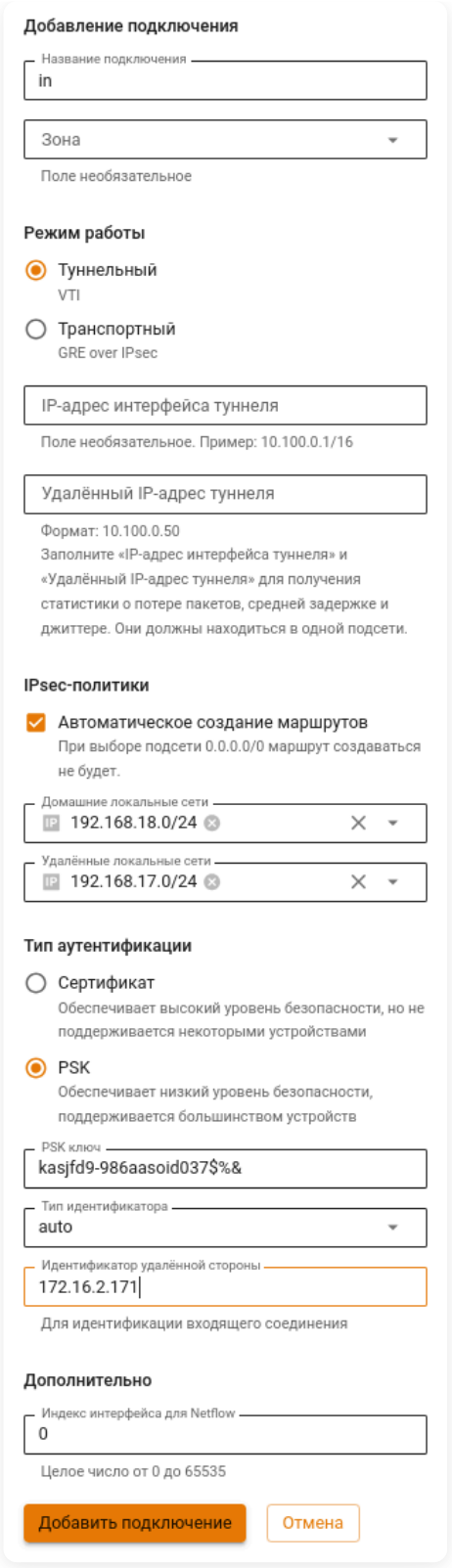
```
write memory
```

Настройка входящего подключения на Ideco NGFW

Для настройки входящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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**.
- **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 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 интрефейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети. заполняется для получения статистики обмена пакетами.
- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW.
- **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.

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

```
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

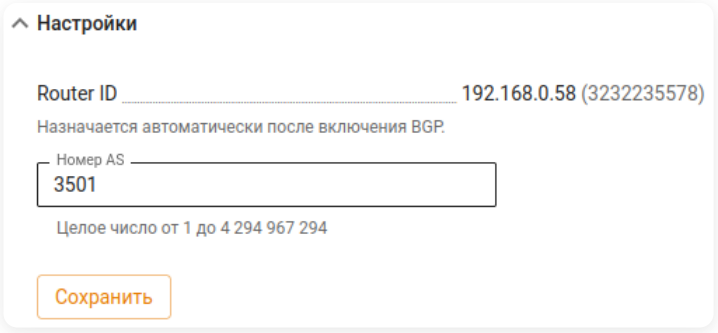
Настройте BGP на роутере:

```
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
```

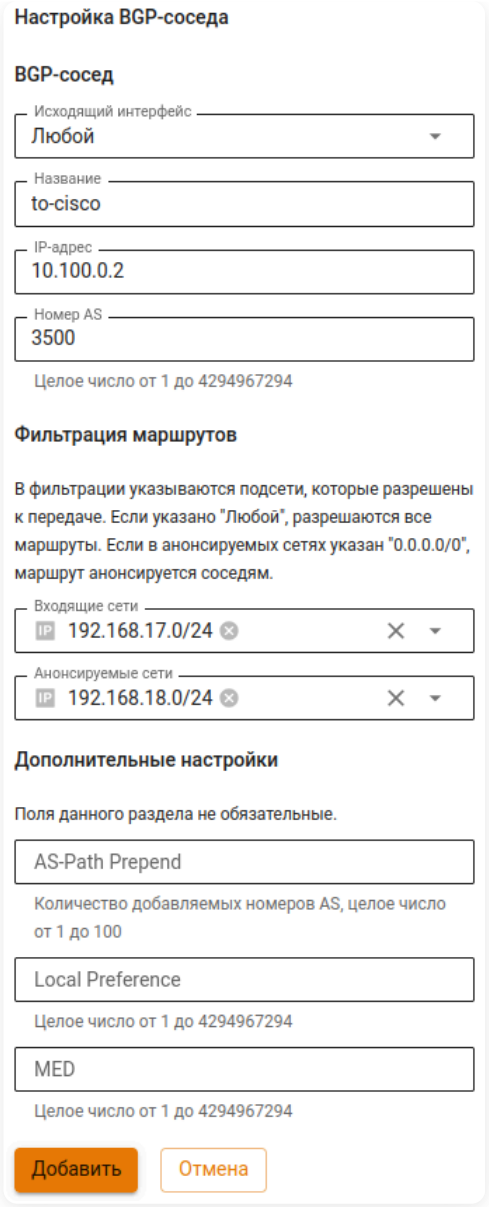
Настройка на Ideco NGFW

1. Перейдите в **Сервисы** → **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.
- **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 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.

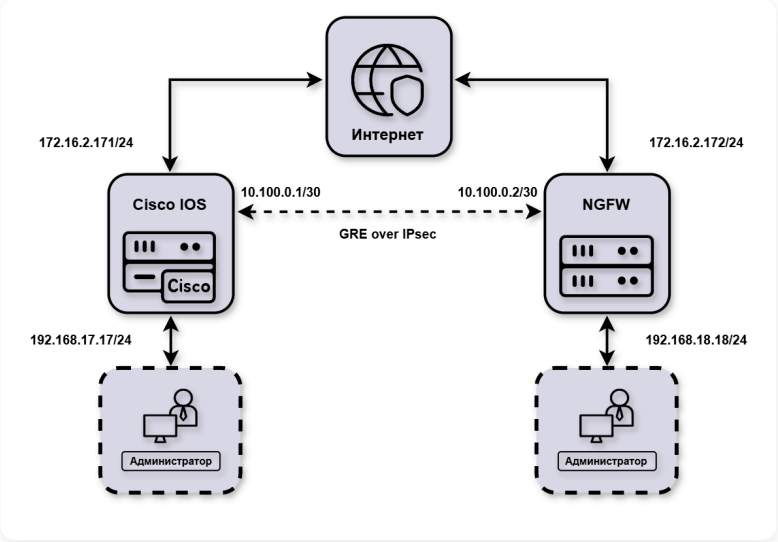
Подключение Cisco IOS и Ideco NGFW по IPsec в транспортном режиме

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 следуйте инструкции ниже.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе Туннельные. 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 и Cisco IOS

Настройка Ideco NGFW

Настройте на Ideco NGFW 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 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 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 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):

- Для подключения от Ideco NGFW 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:

```
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):

- Для подключения от Ideco NGFW 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:

```
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:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

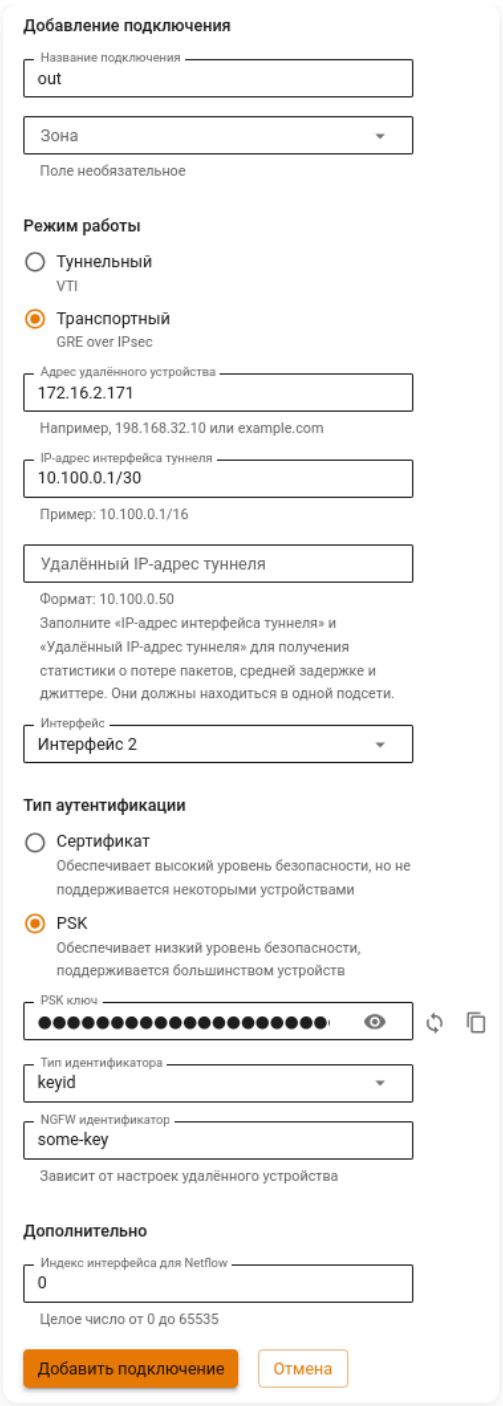
```
write memory
```

Настройка исходящего подключения на Ideco NGFW

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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.
- **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. Он потребуется, чтобы настроить подключение в Cisco.
- **NGFW идентификатор** - 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.

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 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

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):

```
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):

```
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:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

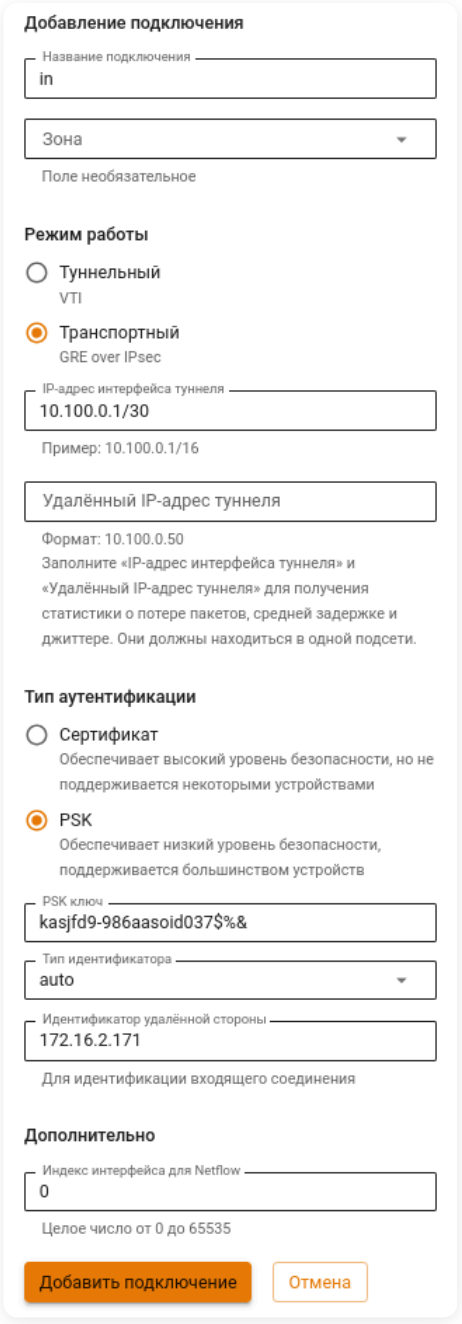
```
write memory
```

Настройка входящего подключения на Ideco NGFW

Для настройки входящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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**.

- **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

```
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

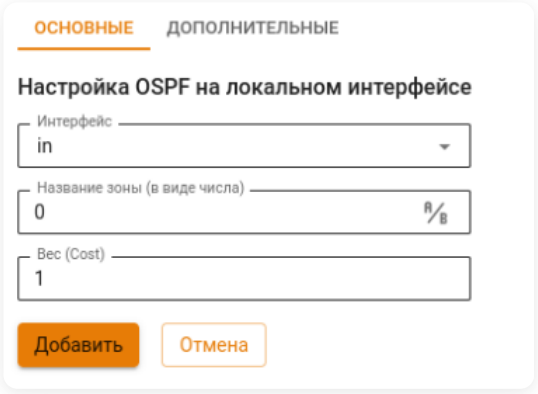
Настройте процесс OSPF на роутере (значение `area` должно совпадать на Cisco и NGFW):

```
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

1. Перейдите в раздел **Сервисы** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW, настроенный ранее.
- **Название зоны** - введите номер зоны (значение `area`, должно совпадать на NGFW и Cisco). Можно ввести в виде числа или IP-адреса, нажав иконку A/B.
- **Вес** - введите стоимость маршрута.

3. Нажмите **Сохранить**.

4. Включите модуль **OSPF**.

Для подключения нескольких устройств Cisco к одному Ideco NGFW и передачи маршрутов между всеми устройствами:

1. Создайте для каждого Cisco Gre-over-IPsec подключение к Ideco NGFW.

2. Подключите каждое устройство Cisco по OSPF.

При такой конфигурации локальные сети каждого Cisco будут доступны с Ideco NGFW и других устройств Cisco.

BGP

Настройка на Cisco

Настройте процесс BGP на роутере:

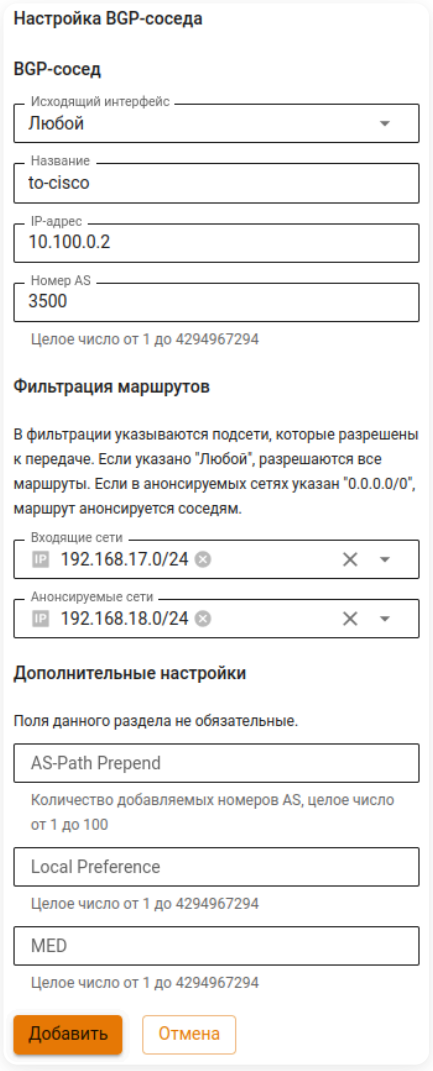
```
conf t
router bgp 3500
 neighbor <IP интерфейса туннеля NGFW> remote-as 3501
 neighbor <IP интерфейса туннеля NGFW> ebgp-multihop 2
 neighbor <IP интерфейса туннеля NGFW> update-source Tunnel0
 !
 address-family ipv4
  network <локальная подсеть Cisco> mask <маска подсети>
  neighbor <IP интерфейса туннеля NGFW> activate
 exit-address-family
```

Настройка на Ideco NGFW

1. Перейдите в раздел **Сервисы** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в строку **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.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

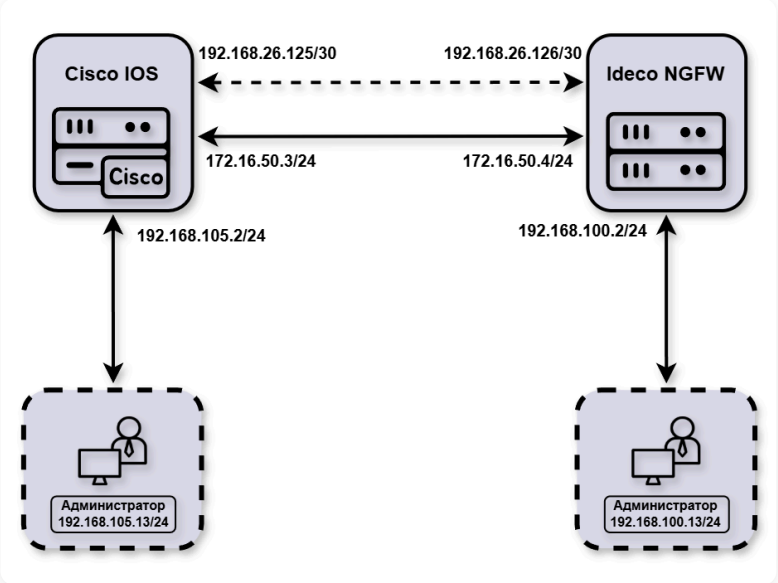
5. Включите модуль **BGP**.



В Ideco NGFW 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 по route-based IPsec

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.

Первоначальная настройка Ideco NGFW и Cisco IOS

Настройка Ideco NGFW

Настройте на Ideco NGFW 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:

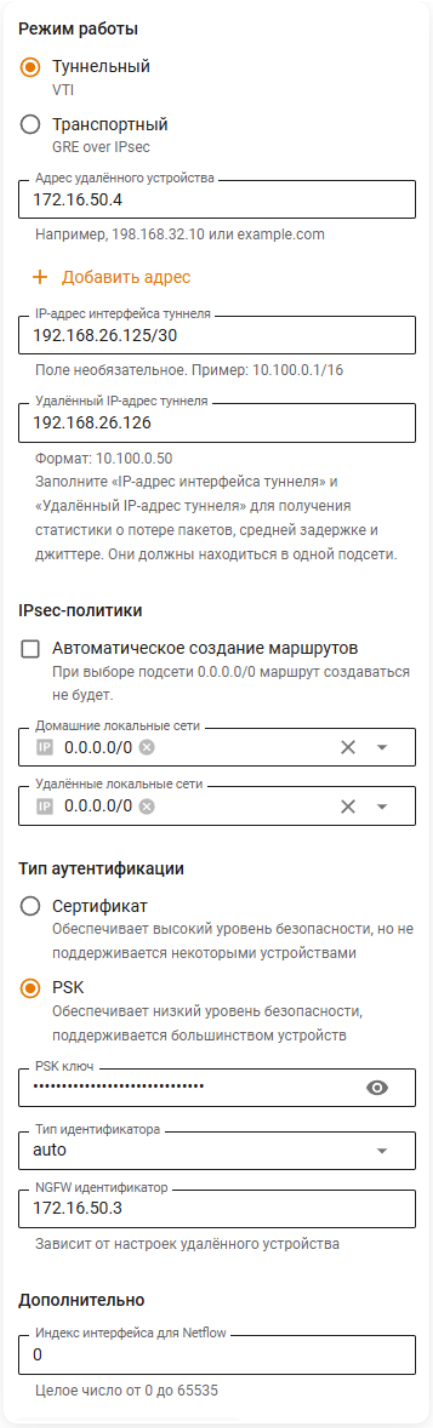
```
write
```

Настройка исходящего подключения на Ideco NGFW

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Они должны находиться в одной подсети. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW.
- **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.
- **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 локальными сетями (TCP и web).

Итоговая конфигурация route-based IPsec на Cisco должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW

```
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 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 pfSense к Ideco NGFW по IPsec

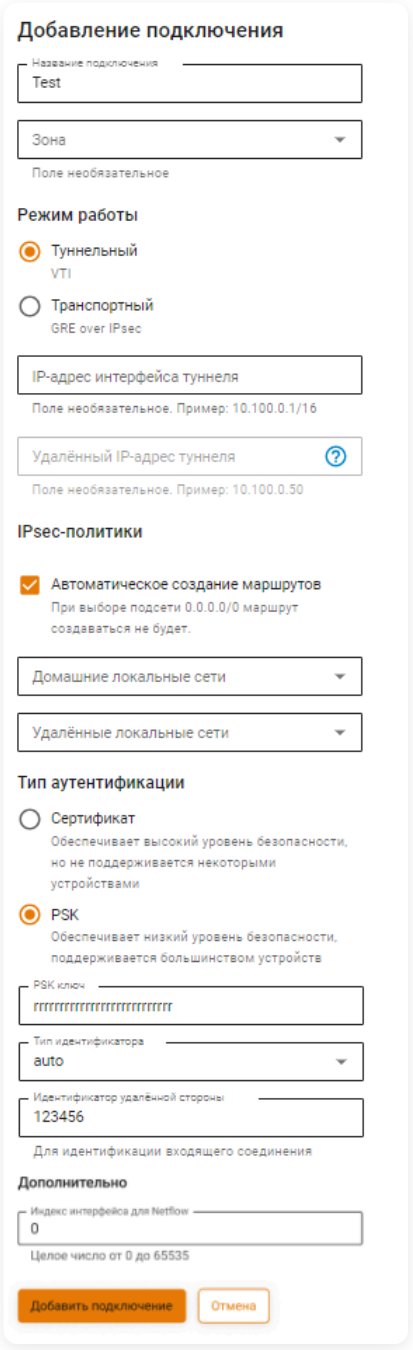
Объединяемые локальные сети не должны пересекаться!

Настройка входящего подключения

Для настройки Ideco NGFW следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW 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**.
- **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** - PSK.
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения.
- **Идентификатор удаленной стороны** - любой.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

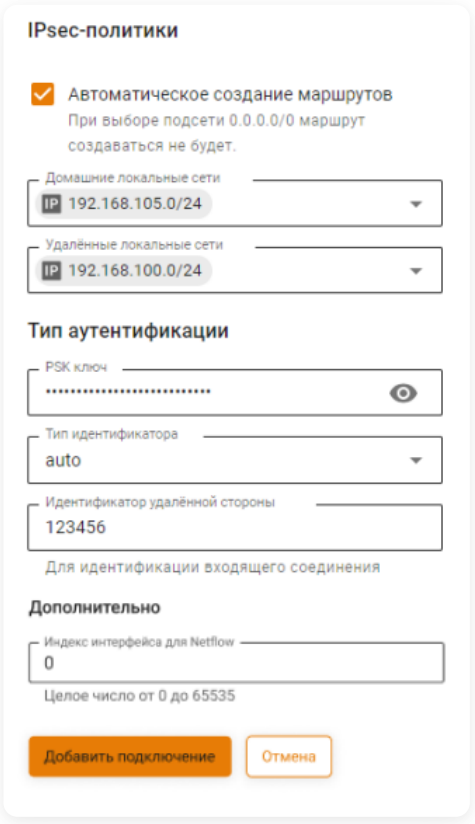
> Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

3. Сохраните созданное подключение, нажмите на кнопку **Включить**.

4. Скопируйте значение идентификатора удаленной стороны одним из способов:

В интерфейсе NGFW

На вкладке **Сервисы** → **IPsec** → **Входящие подключения** в строке **Идентификатор удаленной стороны**:



Через терминал

На Ideco NGFW 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):

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 на вкладку **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;
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;
- **Authentication Method** - Mutual PSK;
- **My identifier и Peer identifier** - сюда вставьте значение строки `id` на Ideco NGFW (см. шаг 4 в настройке Ideco NGFW);
- **Pre-Shared Key** - вставьте PSK-ключ, который ранее прописывали на Ideco NGFW;
- **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;
- **Remote Network** - локальную сеть Ideco NGFW, 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 в настройках файрвола pfSense (переходим на вкладку **Firewall → Rules → IPsec** и создаем два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense).

Обращаем внимание на раздел файрвола WAN - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

7. Теперь переходим на вкладку **Status → IPsec** (там должно появится созданное подключение), нажимаем на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы указали 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 следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW 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.
- **Адрес удаленного устройства** - укажите адрес удаленного устройства.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения.
- **NGFW идентификатор** - любой.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP.
- **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 на вкладку **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;
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;
- **Description** - любое;
- **Authentication Method** - Mutual PSK;
- **My identifier** - My ip address;
- **Peer identifier** - KeyID tag. Введите идентификатор удаленной стороны, т. е. Ideco NGFW;
- **Pre-Shared Key** - введите PSK-ключ;
- **Encryption Algorithm**:
  - Для **Ideco UTM версии 10.0 и Ideco NGFW 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 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;
- **Remote Network** - локальную сеть Ideco NGFW, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. В настройках файрвола pfSense перейдите на вкладку **Firewall** → **Rules** → **IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense.

7. Обратите внимание на раздел файрвола **WAN** - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

8. Перейдите на вкладку **Status** → **IPsec** (там должно появится созданное подключение), нажмите на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы 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 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 Keenetic по SSTP или IPsec

> В статье описана настройка VPN-соединения между маршрутизатором Keenetic и Ideco NGFW.

Для создания подключения используются протоколы:

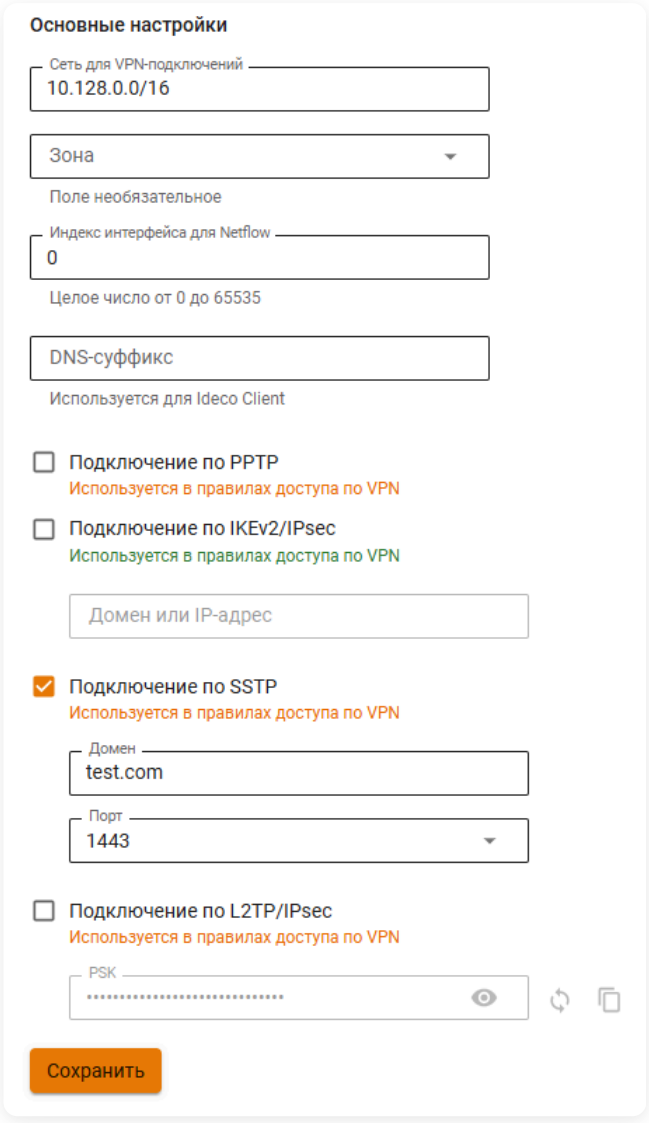
- **SSTP** - для безопасного соединения между клиентом и сервером.
- **IPsec** - для безопасной передачи данных в IP-сетях.

Подключение по SSTP

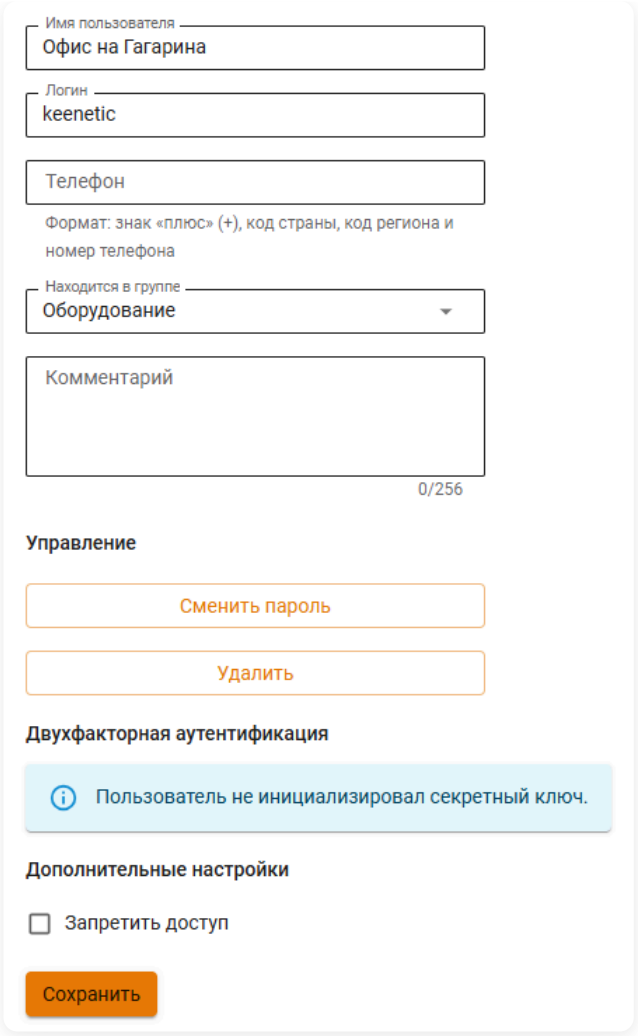
Если доступ из центрального офиса в сеть за Keenetic не нужен, воспользуйтесь инструкцией по подключению в режиме client-to-site.

Настройка Ideco NGFW

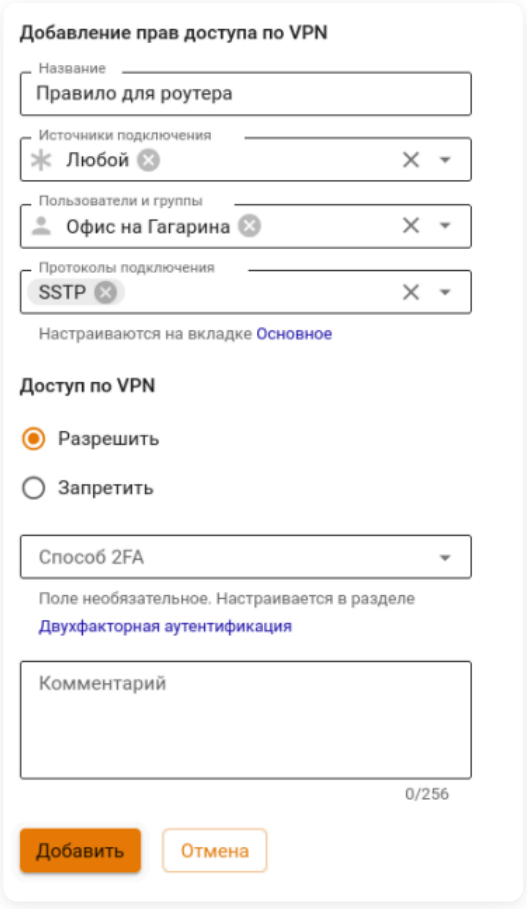
1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**, включите настройку SSTP, укажите домен и порт для подключения:



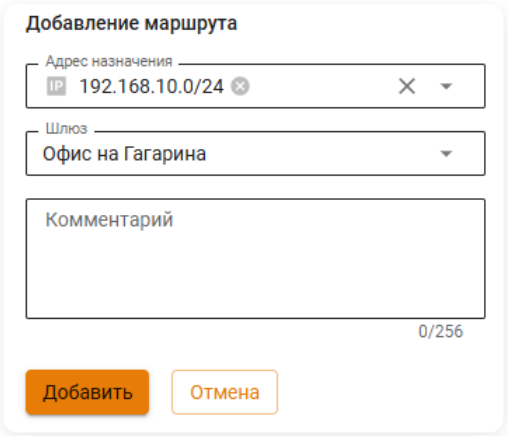
2. Перейдите в **Пользователи** → **Учетные записи** и создайте специального пользователя для удаленного роутера. Логин и пароль пользователя будут использоваться на роутере:



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 **Сервисы** → **Маршрутизация** → **Локальные сети**:



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.

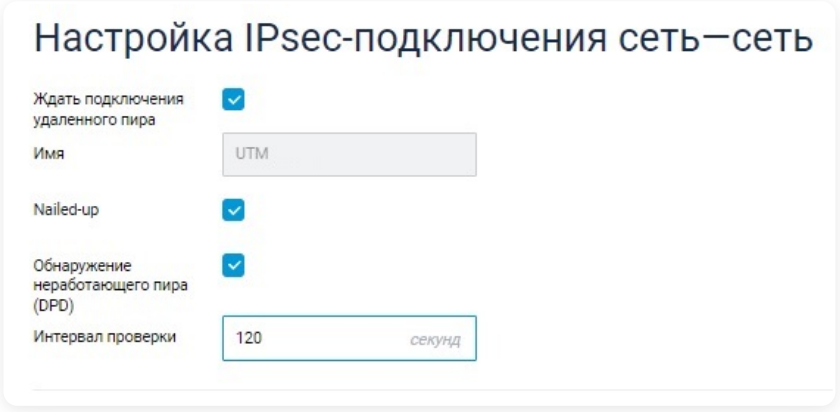
Доступ часто блокируется в Windows из-за настроек сетевых профилей.

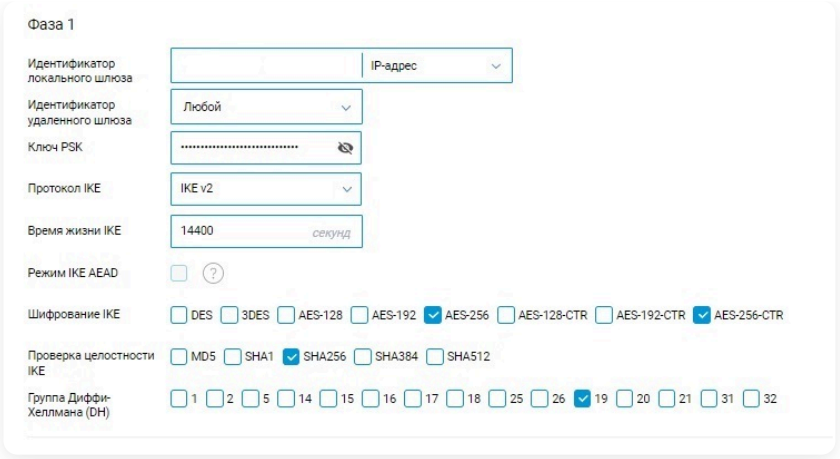
Разрешите доступ до внешних сетей во всех профилях, выполнив команду в PowerShell (запущенного с правами администратора):
`Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`

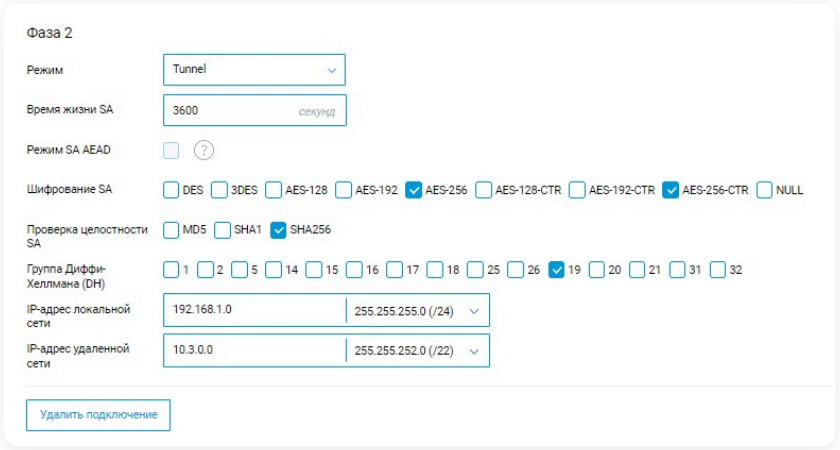
Подключение по IPsec

На стороне Ideco NGFW 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 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**

ГОСТ VPN

ГОСТ VPN - это сервис для организации защищенных каналов связи между несколькими Ideco NGFW с использованием технологии виртуальной частной сети. Соединение шифруется согласно требованиям ФСБ по ГОСТ-алгоритмам с применением российского сертифицированного решения от компании Рутокен.

Раздел **ГОСТ VPN** недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

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

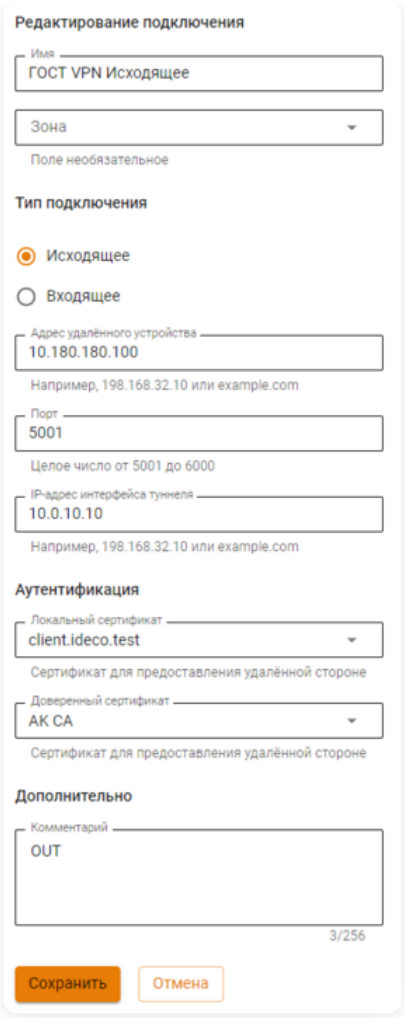
Для настройки ГОСТ VPN необходимо подготовить два USB-токена в соответствии с инструкцией, представленной в статье, и подключить токены к USB-портам серверов.

В случае извлечения USB-токена или истечения срока действия сертификатов, хранящихся на USB-токене, VPN-соединение будет разорвано.

Настройка исходящего подключения

1. Перейдите в раздел **Сервисы** → **ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



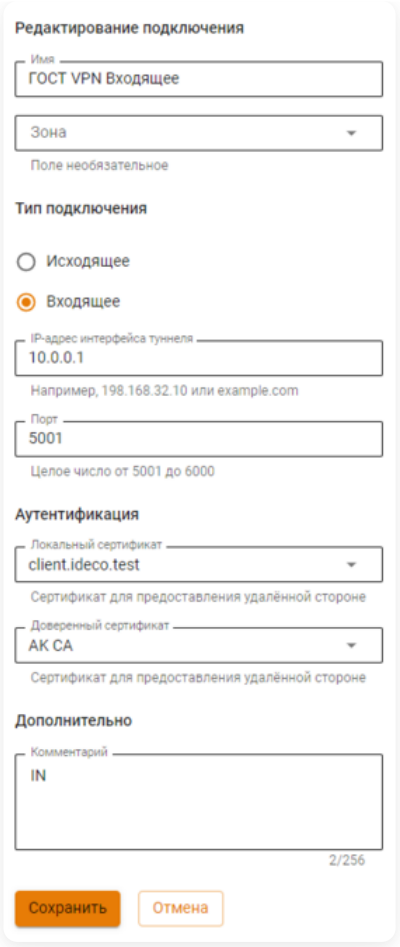
Расшифровка полей

- **Имя** - введите имя подключения, максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым.
- **Тип подключения** - выберите **Исходящее**.
- **Адрес удаленного устройства** - введите доменное имя или белый IP-адрес удаленного Ideco NGFW.
- **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 раздел **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.
- **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.

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

Сертификаты

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

Логика работы

NGFW позволяет выпустить или загрузить корневые и некорневые (пользовательские) сертификаты:

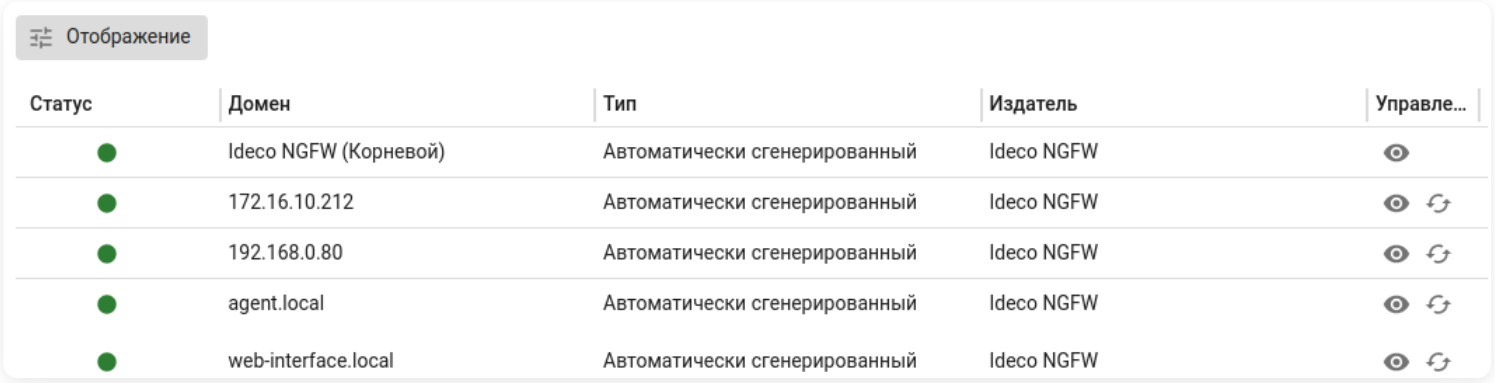
- **Корневые сертификаты** обязательно должны содержать атрибут **X509v3 Basic Constraints: CA: TRUE** для выпуска дочерних сертификатов. При первоначальной установке и запуске NGFW корневой (самоподписанный) сертификат генерируется автоматически. Сертификат можно скачать, перейдя в **Сервисы** → **Сертификаты** → **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).

NGFW 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:

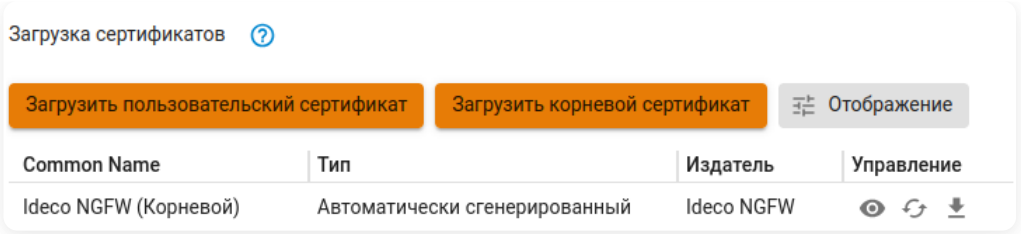


Если в таблице **Действующие сертификаты** одна и та же цепочка сертификатов указана в нескольких строках, значит, она используется несколькими модулями.

Загруженные сертификаты

В таблице **Загруженные сертификаты** отображаются:

- Все загруженные цепочки сертификатов.
- Корневой сертификат Ideco NGFW:

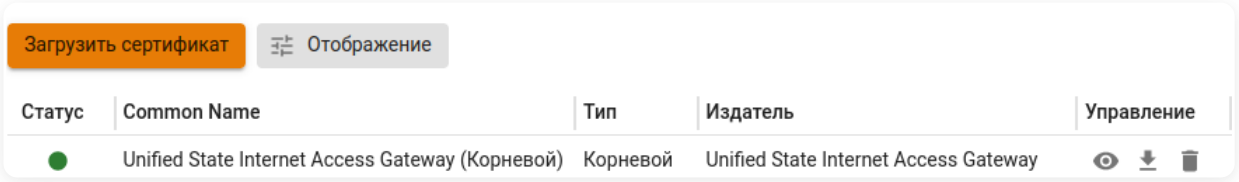


Требования к SSL-сертификатам и инструкция по загрузке в статье.

Системные сертификаты

Раздел позволяет загружать свои сертификаты в хранилище доверенных сертификатов ОС Fedora на NGFW. Подробнее о системных сертификатах - по ссылке.

После добавления сертификата в таблицу **Системные сертификаты** перезагрузите Ideco NGFW. После перезагрузки Ideco NGFW будет доверять загруженному сертификату и всем сертификатам, подписанным загруженным сертификатом:



Загрузка в **Системные сертификаты** необходима, если Ideco NGFW взаимодействует с сервисами, защищенными сертификатом от корпоративного или самоподписанного центра сертификации (CA). Чтобы Ideco NGFW 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.

Управление сертификатами

- просмотр основной информации о сертификате.
- перевыпуск сертификата.
- скачать сертификат.
- удалить загруженный сертификат.

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 NGFW для выпуска и подписания дочерних сертификатов.

Процесс выпуска сертификата

NGFW 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.
- Открытый 80 TCP-порт на внешнем интерфейсе. После установки Ideco NGFW 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** 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 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 автоматически сгенерированные NGFW 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

Некорневая цепочка сертификатов

Чтобы перевыпустить некорневую цепочку сертификатов, нажмите в столбце **Управление** таблицы **Действующие сертификаты**. NGFW 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 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**. NGFW заменит ее на автоматически сгенерированный корневой сертификат.

Для работы Ideco Client под MacOS необходимо, чтобы срок действия сертификата на домен или IP-адрес NGFW, введенный в разделе **Пользователи** → **Ideco Client**, не превышал 825 дней.

Проверить, что срок действия загруженного пользовательского или сгенерированного NGFW 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 NGFW, нажав .

Чтобы проверить, перевыпустился ли сертификат на новый срок, нажмите .

Загрузка SSL-сертификата на сервер

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Требования к сертификату

Перед загрузкой корневого или пользовательского сертификата на Ideco NGFW 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 NGFW**.

Если вы хотите загрузить сертификат как корневой, удостоверьтесь, что он может выдавать дочерние сертификаты: **X509v3 Basic Constraints: CA: TRUE** (это можно проверить в открытом ключе сертификата).

Загрузка SSL-сертификата на NGFW

Если сертификат удовлетворяет всем перечисленным выше условиям, загрузите его на NGFW. Для этого:

1. Перейдите в раздел **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 NGFW. 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 в качестве корневого. Это позволит выстроить цепочку доверия для автоматически выданных сертификатов до корневого центра сертификации. Пользовательские компьютеры будут доверять сертификатам, выданным на стороне NGFW.

Подготовка SSL-сертификата для загрузки на NGFW

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 NGFW.

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 он имеет структуру:

```
-----BEGIN CERTIFICATE-----
..............
..............
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
..............
..............
-----END PRIVATE KEY-----
```

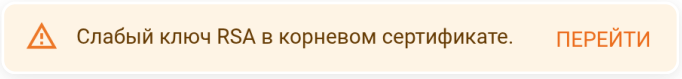
Если в сертификате написано `--BEGIN ENCRYPTED PRIVATE KEY--`, расшифруйте его, введя в OpenSSL команду

`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

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.

```
Установите последнюю версию PowerShell для новых функций и улучшения! https://aka.ms/PSWindows

PS C:\Users\a.istomina> New-SelfSignedCertificate -DnsName test.ideco.com -TextExtension @("2.5.29.19={text}CA=true") -C
ertStoreLocation cert:\LocalMachine\My


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
2284919151C5C624341D7B75FE034B00DF6A44FA  CN=test.ideco.com
```

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 его корректность 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

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

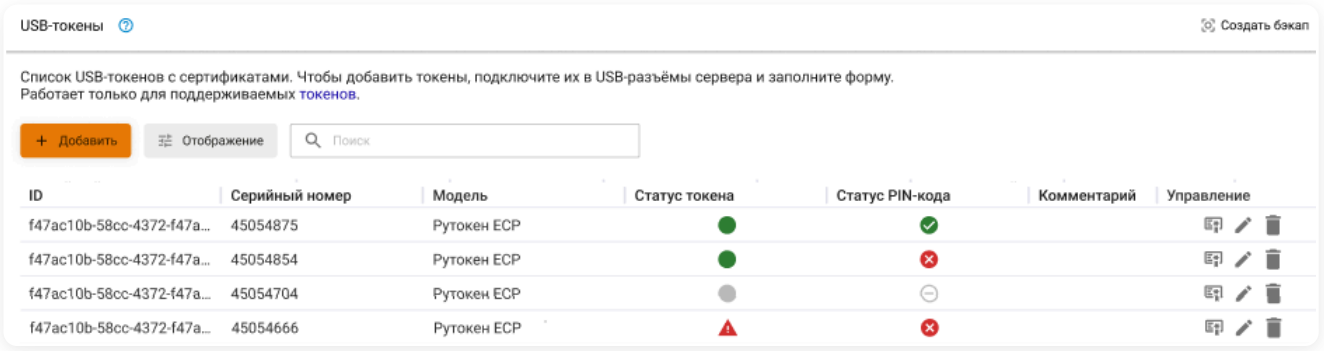
USB-токены

USB-токен - это аппаратное устройство для безопасного хранения цифровых сертификатов и работы с приватными ключами.

Раздел **USB-токены** недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

Ideco NGFW поддерживает только USB-токен модели **Рутокен ЭЦП 3.0**. USB-токены других моделей могут не отображаться в веб-интерфейсе **Ideco NGFW**.

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 его 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.

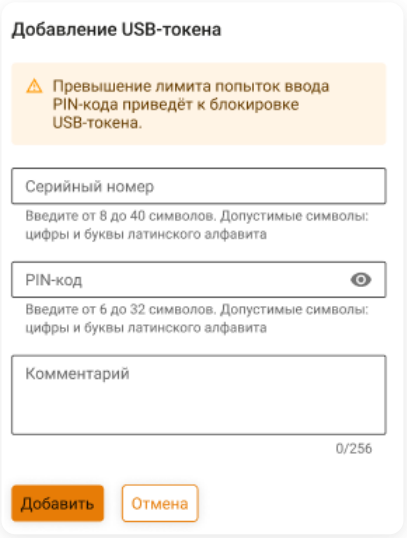
Если требуется сгенерировать сертификаты для тестирования ГОСТ VPN, рекомендуем воспользоваться статьей от производителя.

Настройка USB-токена на Ideco NGFW

Для работы Ideco NGFW с USB-токеном введите корректный PIN-код. После этого NGFW сможет использовать токен для настройки ГОСТ VPN.

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`.
- **PIN-код** - на токенах от компании Рутокен установлен PIN-код по умолчанию: `12345678`.
- **Комментарий** - необязательное поле.

Отчеты и журналы

В этом разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

Трафик

В разделе представлена статистика из **Контроля приложений** и **Контент-фильтра**

Перейти >

Системный журнал

Таблица логов работы служб

Перейти >

Журнал веб-трафика

В разделе представлен результат проверки трафика антивирусом и модулем **Контент-фильтр**

Перейти >

Журнал трафика

В разделе представлена таблица о срабатывании правил **Файрвола**

Перейти >

События безопасности

Статистика событий модулей WAF и IPS, а также графики событий IPS

Перейти >

Действия администраторов

В разделе представлена таблица о действиях администраторов в Ideco NGFW

Перейти >

Аутентификация администраторов

Таблица аутентифицированных на Ideco NGFW администраторов

Перейти >

Журнал аутентификации

В разделе представлена таблица аутентифицированных на Ideco NGFW пользователей

Перейти >

Журнал авторизации ЛК

В разделе представлена таблица сессий пользователей, авторизованных в личном кабинете Ideco NGFW

Перейти >

Конструктор отчетов

Создание шаблонов отчетов и настройка рассылки на электронную почту

Перейти >

Syslog

Настройка передачи системных сообщений (syslog) Ideco NGFW в сторонние коллекторы или в SIEM-системы

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Трафик

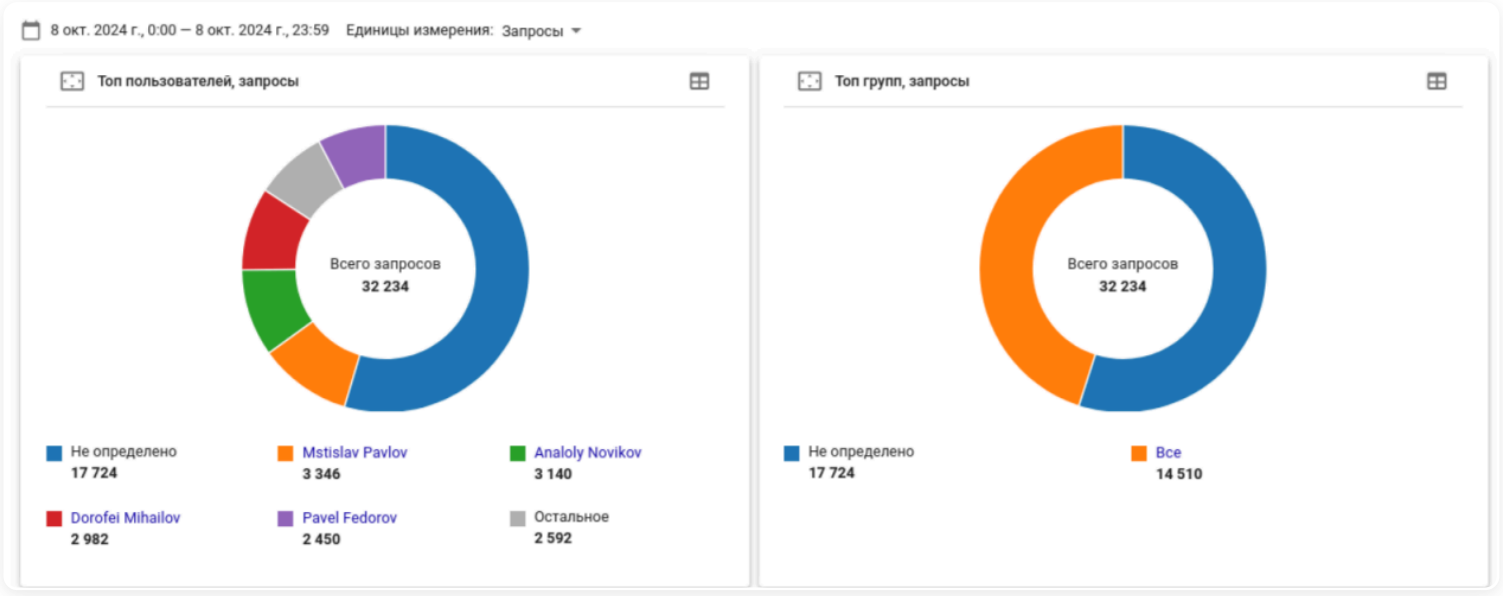
При переводе ползунка **Трафик** в левом верхнем углу в положение **Включен** раздел начинает собирать статистику из Контент-фильтра и отображается в виде виджетов.

Способы отображения информации:

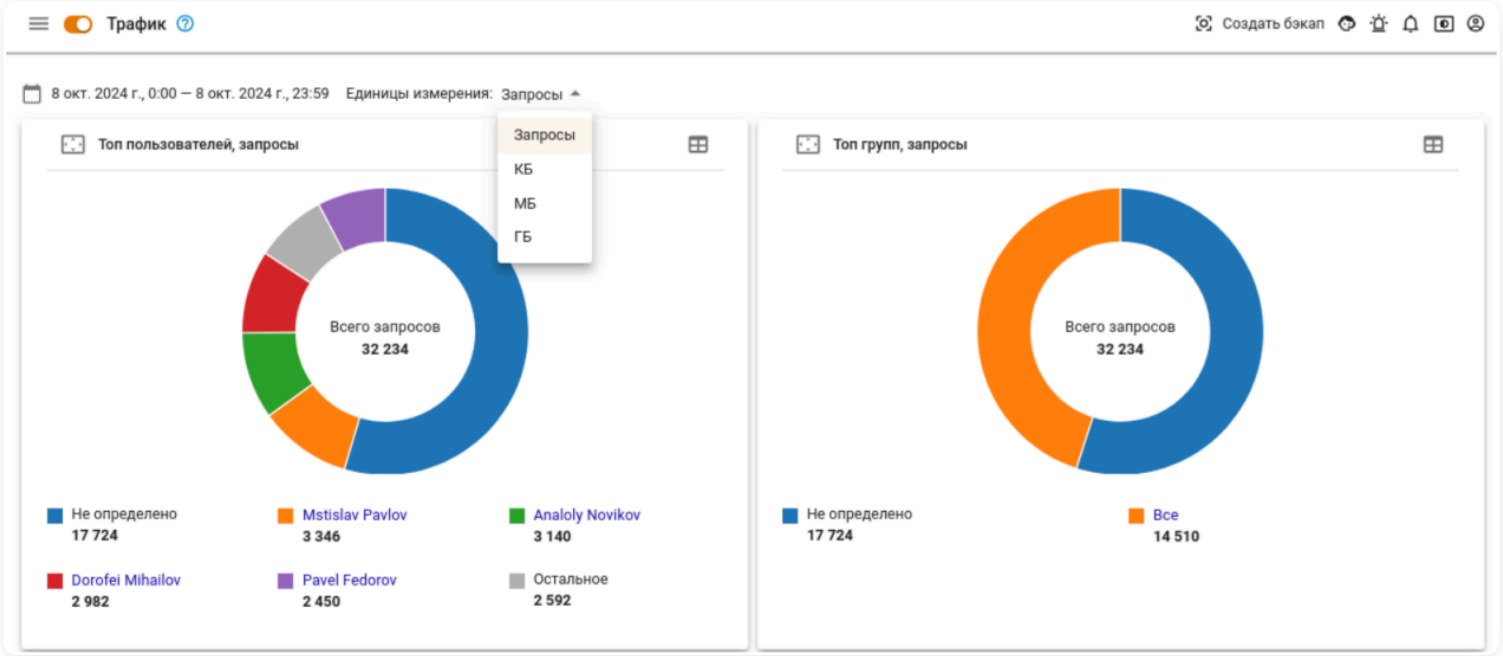
- Круговая диаграмма ( ) и таблица ( );
- Развернутый режим ( ).

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:

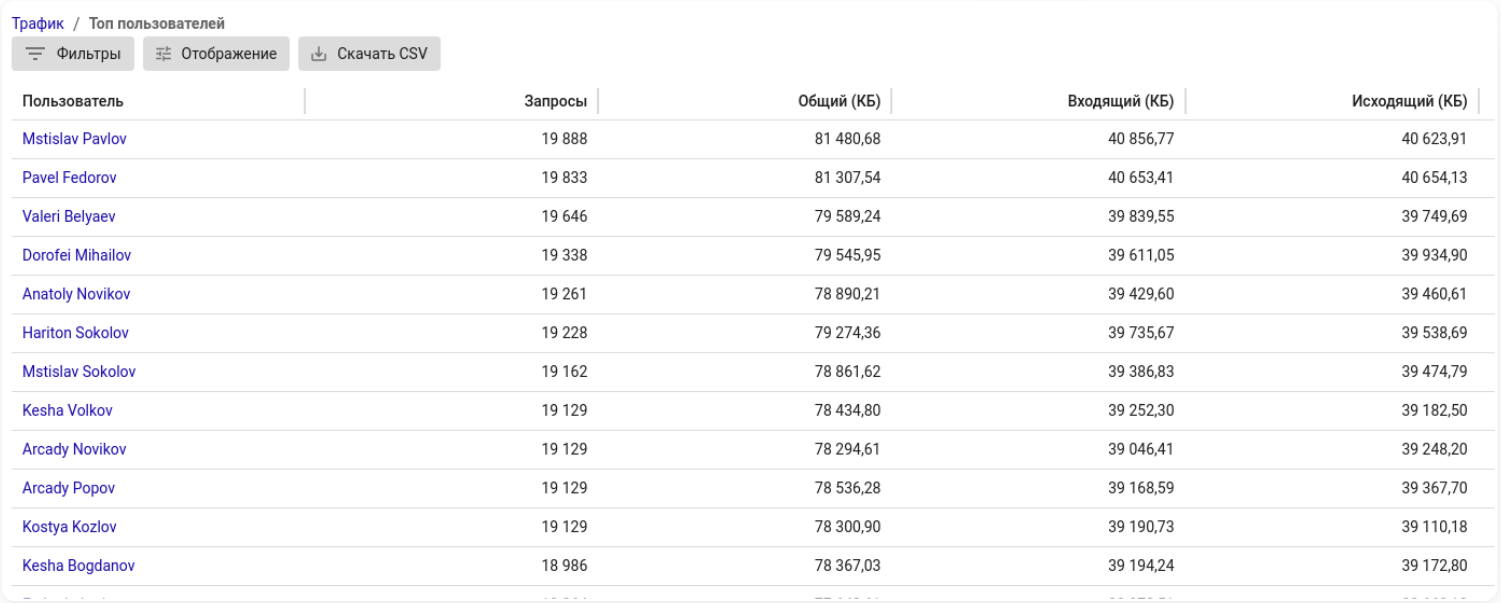


Не определено (трафик с неизвестным адресом и пользователем) - это любой трафик от самого Ideco NGFW. Например, скачивание баз

Контент-фильтра, GeoIP, сигнатур и т.д.

Развернутый режим

Содержит данные по всем объектам из топа. Для поиска по объектам воспользуйтесь **Фильтром** (Фильтры).


Трафик / Топ пользователей

Фильтры | Отображение | Скачать CSV

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 кликните по нему.

  Если пользователя нет в списке, то нажмите **Развернуть** ( ) в левом верхнем углу виджета (откроется список всех пользователей);
- В виджете **Топ заблокированных сайтов** NGFW 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 кликните по нему. Если его нет в списке, то нажмите **Развернуть** ( );
- Чтобы увидеть список всех пользователей, у которых был заблокирован этот протокол, на открывшейся странице найдите виджет **Топ пользователей**

  и нажмите **Развернуть** ( ).

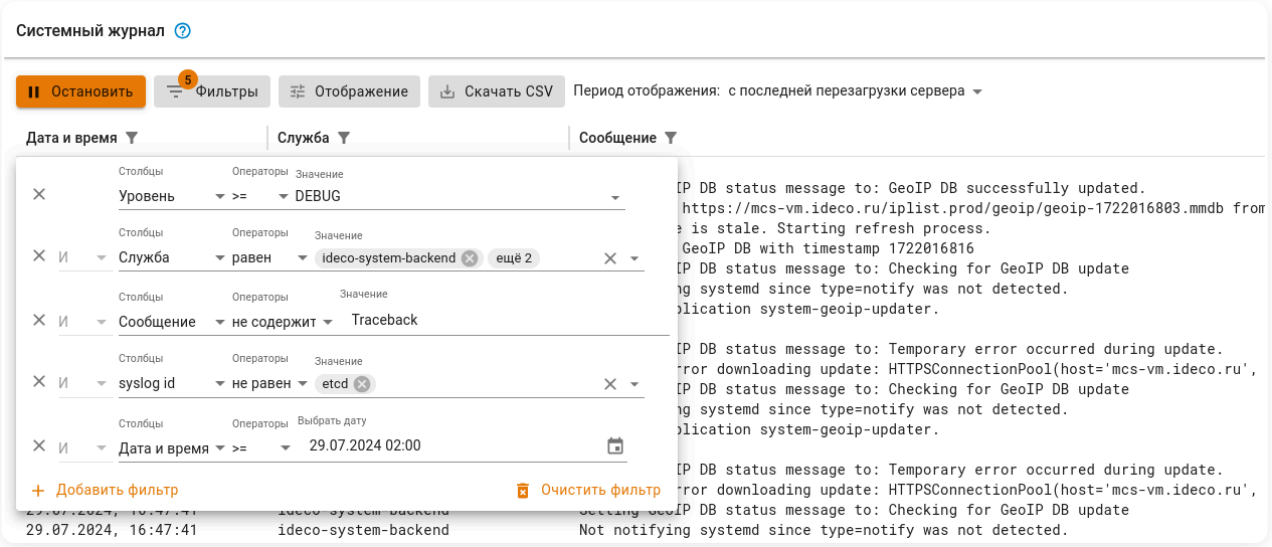
Подробнее о создании собственных шаблонов со статистикой - в статье Конструктор отчетов.

Системный журнал

Время хранения логов в разделе **Журналы** - 90 дней. Для событий служб **strongswan**, **squid**, **ideco-app-control**, **fail2ban** срок хранения - 14 дней, для **ideco-conndrop** - 2 дня.

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 **Файрвола**.

Алгоритм работы службы:

1. Присваивает соединению метку `ideco-irreversible-drop` при срабатывании запрещающего правила **Файрвола**.
2. Каждую минуту выполняет фильтрацию записей с меткой `ideco-irreversible-drop` и удаляет их.

Защита от брутфорс-атак

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
Веб-интерфейс	ideco-web-interface
Двухфакторная аутентификация	ideco-two-factor-codes

Модуль	Имя службы
Личный кабинет пользователя	ideco-user-cabinet
Обратный прокси	ideco-reverse-proxy, ideco-reverse-proxy-conn, ideco-reverse-proxy-req
Почтовые службы	ideco-dovecot, ideco-postfix-connrate, ideco-postscreen-prgrt, ideco-roundcube, ideco-smtp, ideco-smtp-rcpt

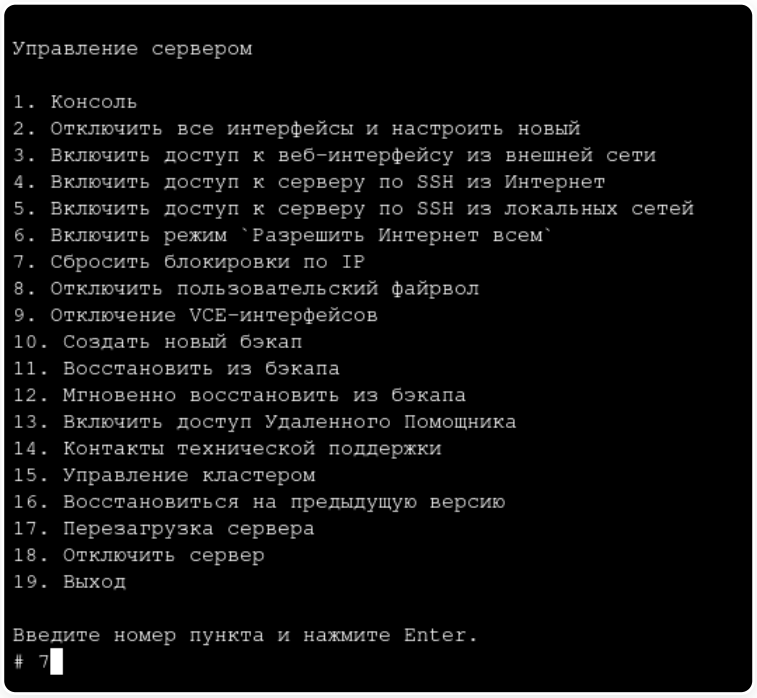
Логи службы `fail2ban` можно увидеть:

- В веб-интерфейсе в разделе **Отчеты и журналы** → **Системный журнал**, задав фильтр `fail2ban`.
- В разделе **Управление сервером** → **Терминал**, введя команду `journalctl -u fail2ban`.

Для разблокировки через терминал используйте команды:

- `fail2ban-client unban --all` - команда используется для снятия всех блокировок;
- `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса, указав нужный IP-адрес в качестве аргумента.

Блокировки можно сбросить из локального меню шлюза, выбрав опцию **Сбросить блокировки по IP**:



Список служб

Логи представленных служб доступны в разделе Система:

Модуль	Имя службы
Active Directory	ideco-ad-backend
ALD Pro	ideco-ald-rest, ideco-ald-backend
DHCP	ideco-dhclient, ideco-dhcp-server-backend
DNS	ideco-dns-backend, unbound, nsd, unbound-anchor, unbound-keygen, ideco-dns-dnstap-reader
DDNS	ideco-dns-backend
Ideco Center	ideco-central-console-backend
Ideco Client	ideco-agent-websocket, ideco-agent-backend, ideco-app-stats
IGMP Proxy	ideco-igmpproxy-backend, ideco-igmpproxy-rest
IPsec	ideco-ipsec-backend
NTP	chronyd
Syslog	ideco-logs-backend
VCE	ideco-vce-backend, ideco-vce-rest
VPN-подключения	ideco-vpn-authd, ideco-vpn-dhcp-backend, ideco-vpn-servers-backend, ideco-vpn-netns, ideco-vpn-sessions-sync
Web Application Firewall	ideco-waf-backend, ideco-waf-event-syncer
Авторизация	ideco-auth-backend
Антивирус	ideco-av-backend
Бэкапы	ideco-backup-backend, ideco-backup-create, ideco-backup-rotate
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-authd
Действия администраторов	ideco-audit-backend
Дополнительно (язык, часовой пояс, включение особых режимов работы)	ideco-system-backend
Доступ по SSH	sshd
Защита от повторяющихся вредоносных или подозрительных действиях, в т.ч. от брутфорс-атак (brute force - атака полным перебором)	fail2ban
Кластеризация	ideco-cluster-backend
Контент-фильтр	ideco-content-filter-backend
Контроль приложений	ideco-app-backend, ideco-app-control-nfq
Личный кабинет пользователя	ideco-user-cabinet-backend
Лицензия	ideco-license-backend
Локальное меню	ideco-local-menu
Маршрутизация	ideco-routing-backend, ideco-routing-rest
Обновления	ideco-sysupdate-backend
Обнаружение устройств	ideco-netscan-backend
Объекты	ideco-alias-backend
Ограничение скорости	ideco-shaper-backend
Обратный прокси	ideco-reverse-backend
Отправка оповещений через телеграм-бота	ideco-mir-alerts
Отчеты и журналы	ideco-logs-backend, ideco-reports-backend, ideco-logs-syncer
Почтовый релей	ideco-mail-backend
Предотвращение вторжений	ideco-suricata, ideco-suricata-backend, ideco-suricata-event-syncer, ideco-suricata-profiles-syncer-backend
Проверка скорости	ideco-speedtest

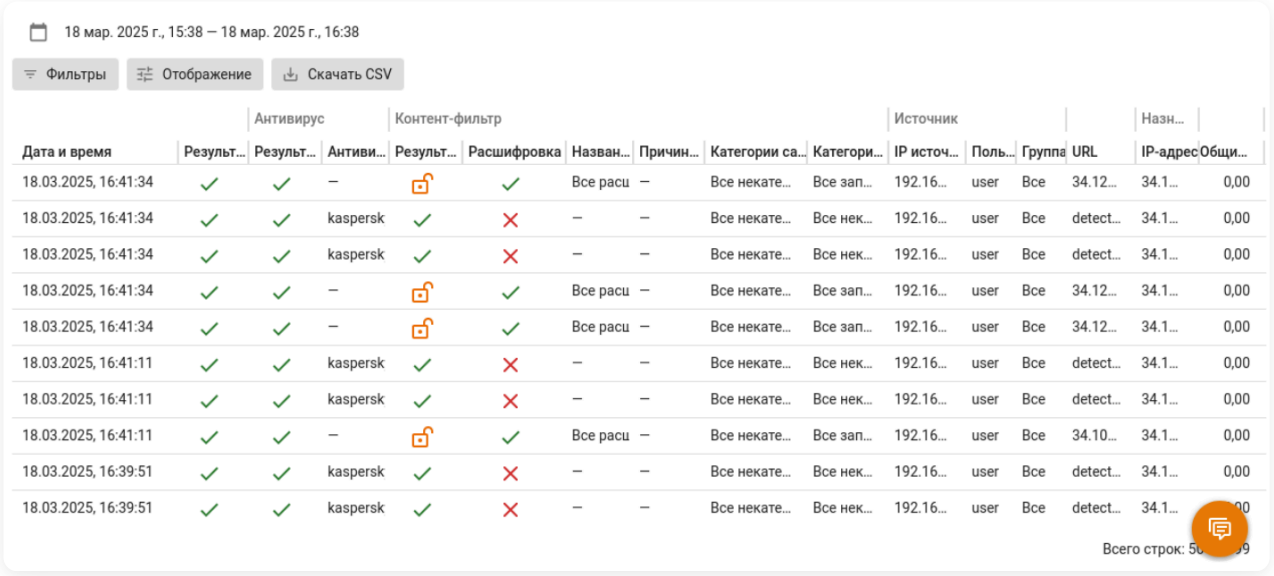
Модуль	Имя службы
Прокси	ideco-proxy-backend, squid
Сбор анонимной статистики о работе сервера	ideco-gatherstat-backend
Сертификаты	ideco-cert-backend
Сетевые интерфейсы	ideco-network-backend, ideco-network-nic
Учетные записи	ideco-user-backend
Файрвол	ideco-firewall-backend

Служебные:

Модуль	Имя службы
Локальная база данных	ideco-etcd-runtime, ideco-etcd-permanent
Сбор метрик и статистики	prometheus, prometheus-node-exporter
Сервер базы данных	clickhouse-server

Журнал веб-трафика

В разделе представлен результат проверки трафика антивирусом и модулем **Контент-фильтр**. Для просмотра отчета перейдите в раздел **Отчеты и Журналы → Журнал веб-трафика**:



Для настройки столбцов журнала нажмите **Отображение**.

Описание столбцов

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 проверки	Результат работы Контент-фильтра: разрешено/расшифровано/запрещено/перенаправлено
Расшифровка	Производилась или нет расшифровка запроса
ID	Идентификатор правила контент-фильтра
Правило из Ideco Center	При наличии Ideco Center - постправило/предправило/локальное правило или прочерк
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 проверки	Результат работы Антивируса: разрешено/расшифровано/запрещено/перенаправлено
ID	Идентификатор профиля антивируса
Профиль	Профиль антивируса
Серьезность угрозы	Указанная антивирусом серьезность угрозы: информационный, низкий, средний, высокий
Тип блокируемого контента	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

Результаты проверки

- **Разрешено**
- **Расшифровано**
- **Запрещено**
- **Перенаправлено на**

Расшифровка

- **Трафик расшифрован**
- **Трафик не расшифрован**

Если с устройства пользователя недоступен какой-либо интернет-ресурс, в разделе **Журнал веб-трафика** можно найти правило, блокирующее этот ресурс.

Для просмотра блокировок по конкретному правилу воспользуйтесь кнопкой **Фильтры**, указав в форме наименование правила и оператор.

Журнал трафика

На вкладке отображается информация о срабатывании правил **Файрвола** (таблицы FORWARD, DNAT, SNAT и INPUT), в том числе - о профилях **Предотвращения вторжений** и **Контроля приложений**.

Раздел позволяет быстро выявить модуль фильтрации, который блокирует трафик, а также 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 трафика** 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.

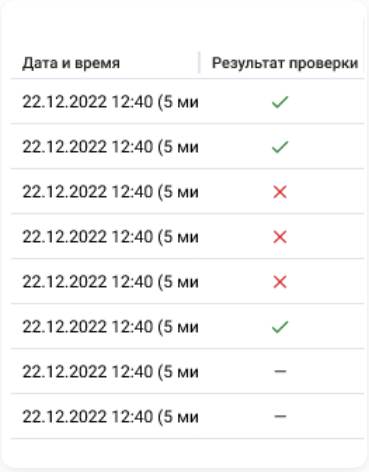
Чтобы отрегулировать столбцы, отображаемые в таблице, воспользуйтесь кнопкой **Отображение**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**.

При фильтрации по **Таблице правил (Файрвол)** можно вывести срабатывния системных правил (Forward System и Input System). Это правила **Файрвола**, которыми нельзя управлять из веб-интерфейса Ideco NGFW, они всегда включены. Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Файрвола**. По вопросам срабатывания системных правил обращайтесь в Техническую поддержку.

В таблице отображаются группы:

Общее



- **Дата и время** - дата и время срабатывания правила;
- **Результат проверки** - совокупный результат проверки трафика тремя модулями фильтрации: **Файрвол**, **Предотвращение вторжений**, **Контроль приложений**.

Файрвол

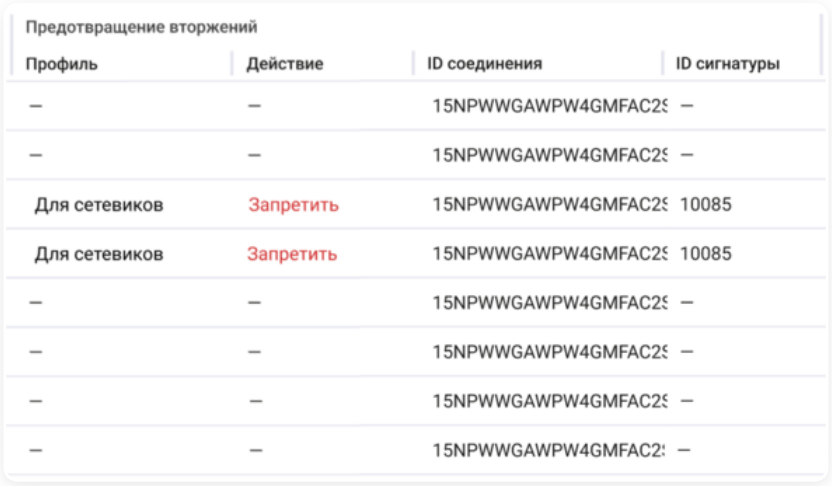
В группе **Файрвол** логируются **только** FORWARD и INPUT правила. Для просмотра правил DNAT и SNAT перейдите к соответствующей группе.

- **ID правила** - идентификатор сработавшего правила таблицы **FORWARD** и **INPUT**.
- **Таблица правил** - правила, которые сработали:
  - **FORWARD** - таблица **FORWARD** раздела **Файрвол** Ideco NGFW.

- **FORWARD BEFORE** - предправило FORWARD Ideco Center.
- **FORWARD AFTER** - постправило FORWARD Ideco Center.
- **FORWARD SYSTEM** - системное правило FORWARD.
- **INPUT** - таблица **INPUT** раздела **Файрвол** Ideco NGFW.
- **INPUT BEFORE** - предправило INPUT Ideco Center.
- **INPUT AFTER** - постправило INPUT Ideco Center.
- **INPUT SYSTEM** - системное правило INPUT.

- **Действие правила** - действие, определенное для трафика, подпадающего под сработавшее правило. Возможные действия: Разрешить, Запретить, Перенаправить в профиль.
- **Протокол** - протокол соединения.

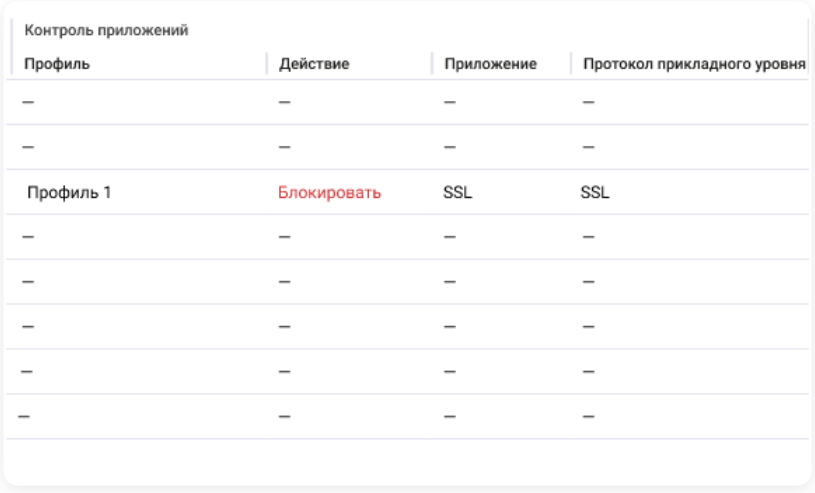
Предотвращение вторжений


Предотвращение вторжений

Профиль	Действие	ID соединения	ID сигнатуры
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
Для сетевиков	Запретить	15NPWWGAWPW4GMFAC2S	10085
Для сетевиков	Запретить	15NPWWGAWPW4GMFAC2S	10085
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–

- **Профиль** - название профиля **Предотвращения вторжений**, использованного в правиле **Файрвола**.
- **Действие** - действие для трафика, определенное профилем (*Разрешить*, *Запретить*, -).
- **ID соединения** - идентификатор соединения, трафик которого был обработан **Предотвращением вторжений**. Просмотреть логи системы Предотвращения вторжений можно в **Отчеты и журналы** → **События безопасности** → **Журнал IPS**.
- **ID сигнатуры** - идентификатор сигнатуры, которой соответствует трафик.

Контроль приложений


Контроль приложений

Профиль	Действие	Приложение	Протокол прикладного уровня
–	–	–	–
–	–	–	–
Профиль 1	Блокировать	SSL	SSL
–	–	–	–
–	–	–	–
–	–	–	–
–	–	–	–
–	–	–	–

- **Профиль** - название профиля **Контроля приложений**, использованного в правиле **Файрвола**;
- **Действие** - действие для трафика, определенное профилем;
- **Приложение** - приложение, действие для которого определено профилем;
- **Протокол прикладного уровня** - протокол, к которому применяется действие, определенное профилем.

Источник

Источник

IP-адрес	Порт	Зона	Логин	Пользователь	Группа	Местоположение
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	Англия
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.136	43612	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.136	43612	Любой	a.qwertyy	Имя Фамилия	Разработка	–

- **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).

Назначение

Назначение

IP-адрес	Порт	Зона	Логин	Пользователь	Группа	Местоположение
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	Англия
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.201	2222	–	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.201	2222	–	a.qwertyy	Имя Фамилия	Разработка	–

- **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/SNAT

DNAT			SNAT	
ID правила	Новый IP назначения	Новый порт назначения	ID правила	Новый IP источника
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
17	217.65.3.21	443	–	–
–	–	–	2	217.65.3.21

DNAT:

- **ID правила** - идентификатор сработавшего правила таблицы **DNAT**;
- **Новый IP назначения** - IP-адрес, на который файрвол поменял **IP-адрес назначения**;
- **Новый порт назначения** - порт, на который файрвол поменял **Порт назначения**.

SNAT:

- **ID правила** - идентификатор сработавшего правила таблицы **SNAT**;
- **Новый IP источника** - IP-адрес, на который файрвол поменял **IP-адрес источника**.

Кластер/VCE

Кластер		VCE	
ID	Название	ID	Название
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1

Кластер:

- **ID** - идентификатор кластера (если он настроен на NGFW);
- **Название** - название кластера (если он настроен на NGFW).

VCE:

- **ID** - идентификатор VCE;
- **Название** - название VCE.

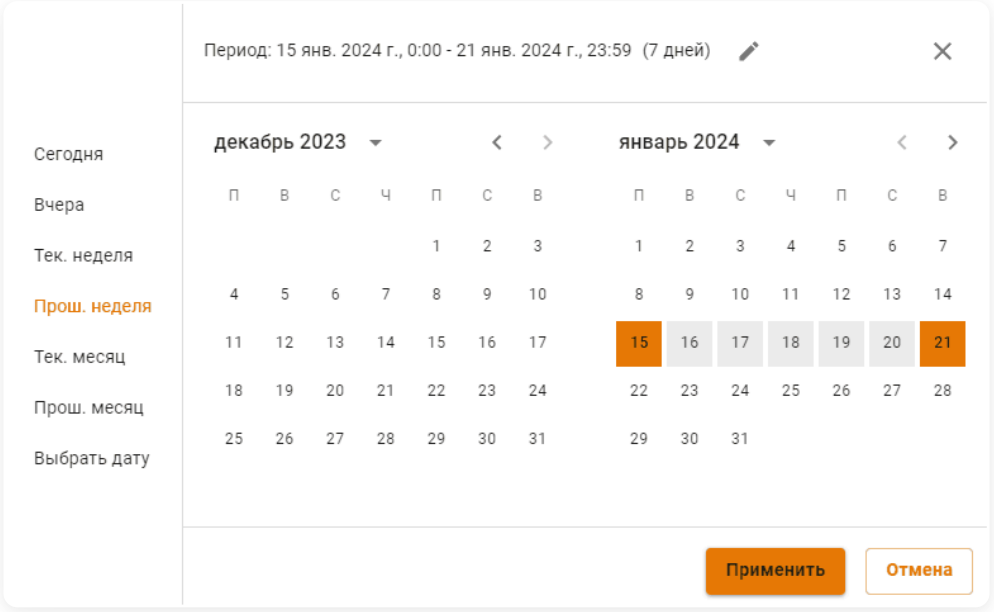
События безопасности

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** 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.

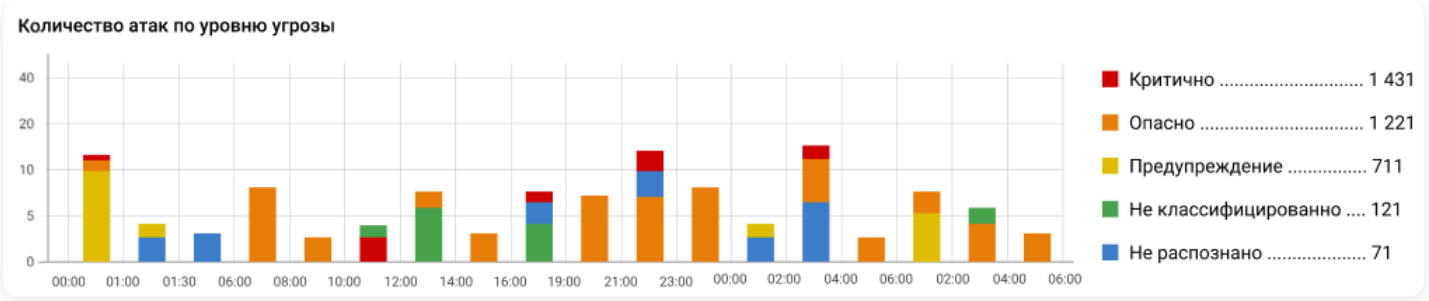
График Количество атак по уровню угрозы

Информация представлена в виде графика с пятью значениями угрозы безопасности:

- **Критично** - уровень угрозы 1;
- **Важно** - уровень угрозы 2;
- **Предупреждение** - уровень угрозы 3;
- **Не классифицировано** - уровень угрозы 4;
- **Не распознано** - уровень угрозы 255.

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, такой адрес не отображается в виджете.

По этой причине локальные IP-адреса не отображаются в виджете.

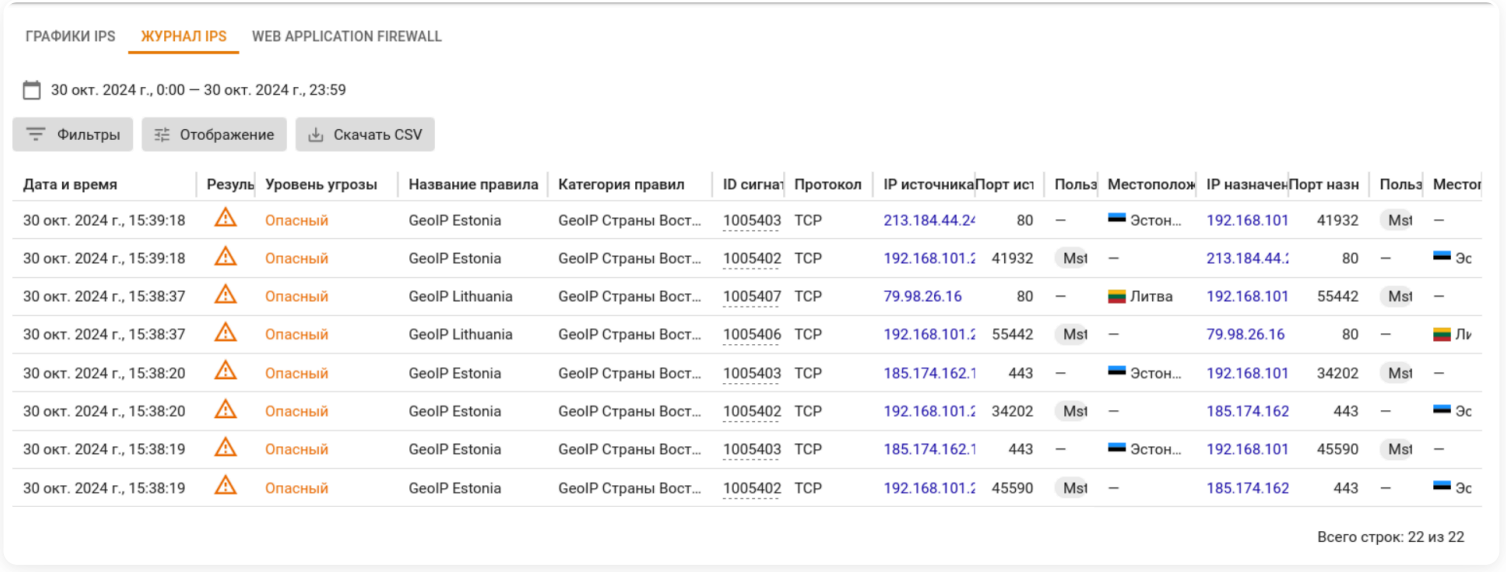
Топ подозрительных локальных узлов

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 разделе **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:
  - Критично;
  - Опасно;
  - Предупреждение;
  - Не распознано;
  - Не классифицировано

IP-адреса в столбцах **Источник** и **Назначение** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.

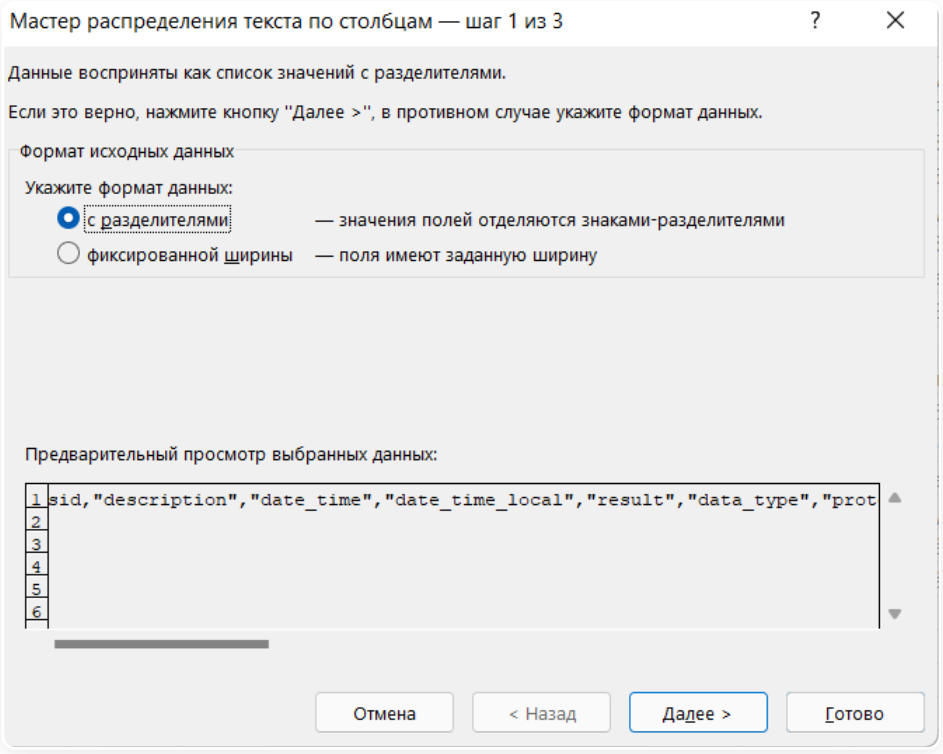
Для корректного отображения информации из CSV-файла выполните действия:

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.

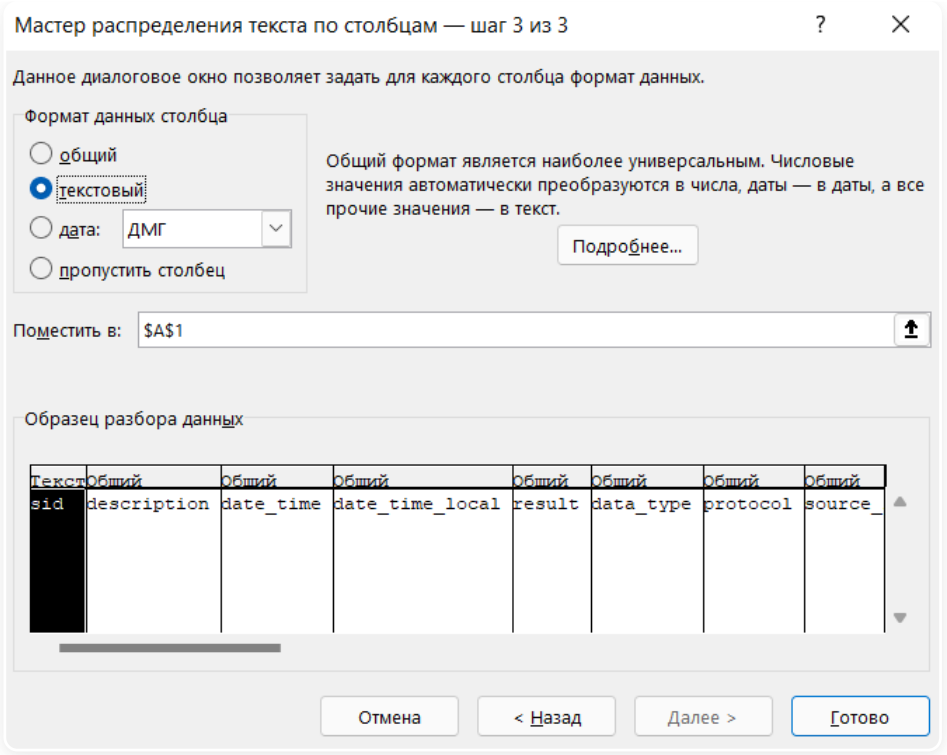
3. Перейдите на вкладку **Данные** и нажмите кнопку **Текст по столбцам**.

4. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:



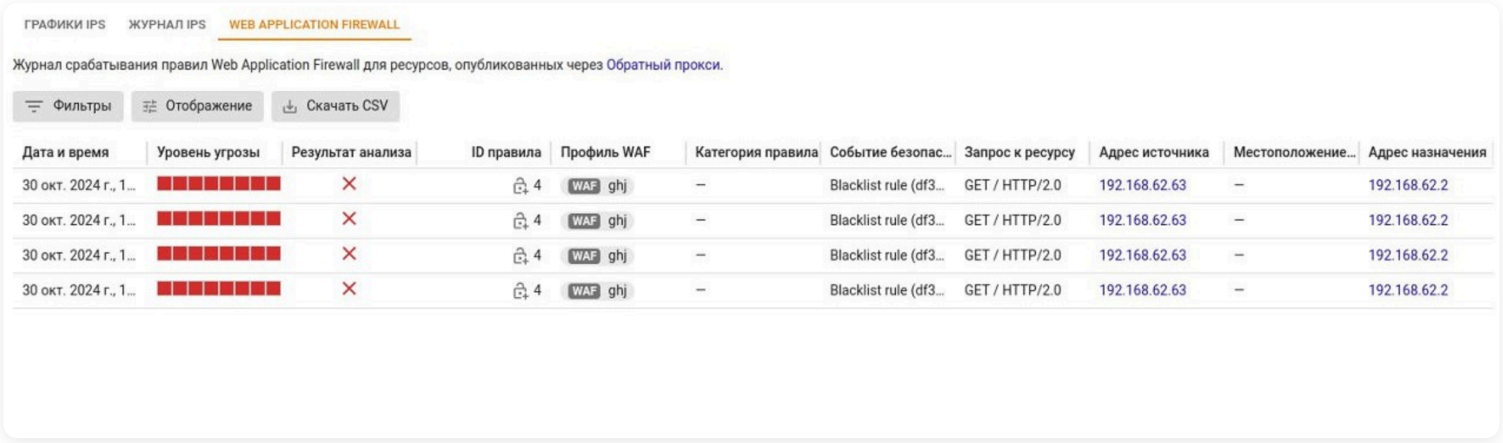
5. В блоке **Символом-разделителем является:** выберите **запятая** и нажмите **Далее**:

6. В блоке **Формат данных столбца** выберите **Текстовый** и нажмите **Готово**:



Web Application Firewall

Раздел **Отчеты и журналы** → **События безопасности** → **Web Application Firewall** содержит информацию о срабатывании правил Web Application Firewall в виде таблицы:

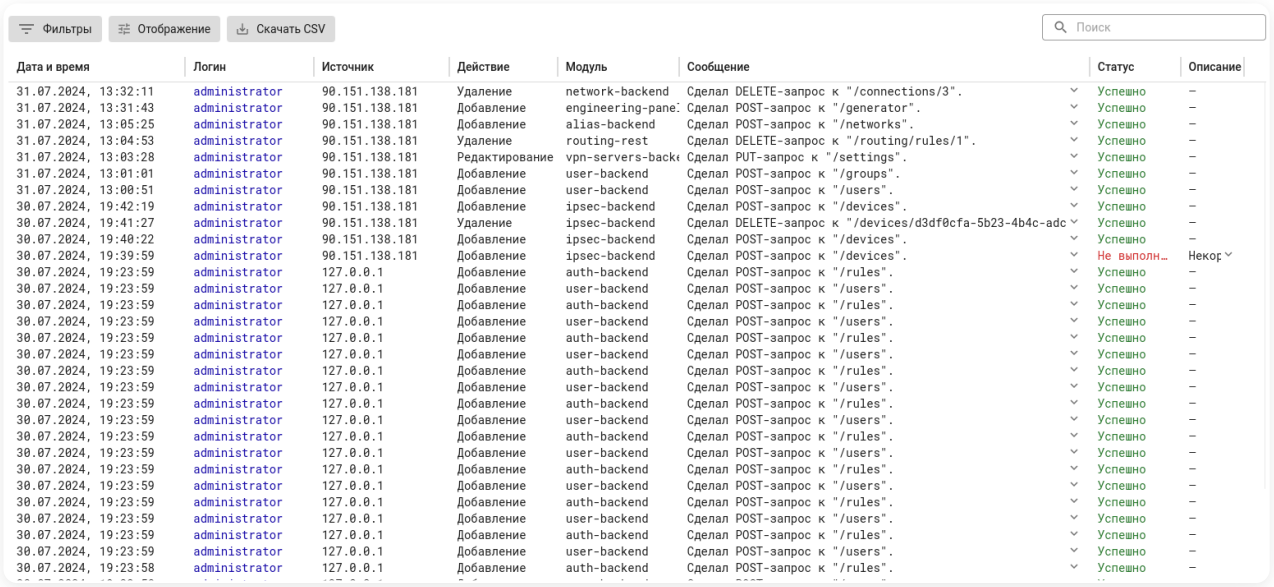


IP-адреса в столбцах **Адрес источника** и **Адрес назначения** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.

На вкладке **Web Application Firewall** отображается профиль WAF, параметры которого вызвали блокировку доступа к ресурсу.

Действия администраторов

Ideco NGFW логирует действия администраторов, которые вносят изменения в конфигурацию NGFW из веб-интерфейса, локального интерфейса и терминала. Действия, осуществляемые через локальное меню NGFW, отображаются в журнале действий администраторов с источником 127.0.0.1:



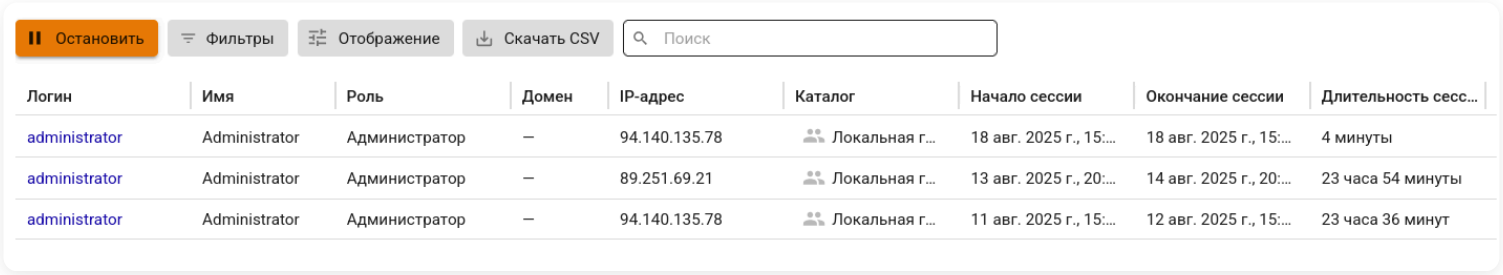
Дата и время	Логин	Источник	Действие	Модуль	Сообщение	Статус	Описание
31.07.2024, 13:32:11	administrator	90.151.138.181	Удаление	network-backend	Сделал DELETE-запрос к "/connections/3".	Успешно	–
31.07.2024, 13:31:43	administrator	90.151.138.181	Добавление	engineering-pane	Сделал POST-запрос к "/generator".	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-back	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, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	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

Время хранения данных в журнале **Аутентификация администраторов** составляет 1 год.



Для поиска авторизованных администраторов нажмите **Фильтры** и укажите:

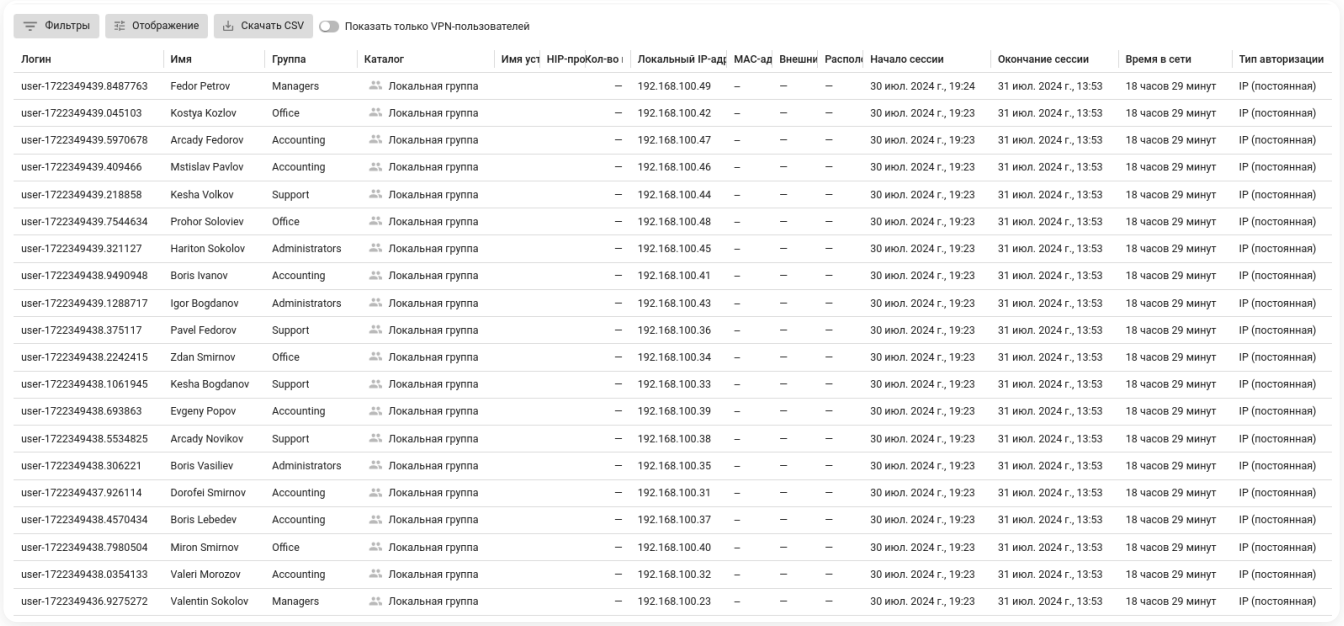
- В поле **Столбец** - требуемый параметр поиска.
- В последнем поле - значение.

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.

Журнал аутентификации

Время хранения данных в **Журнале аутентификации** составляет 180 дней.



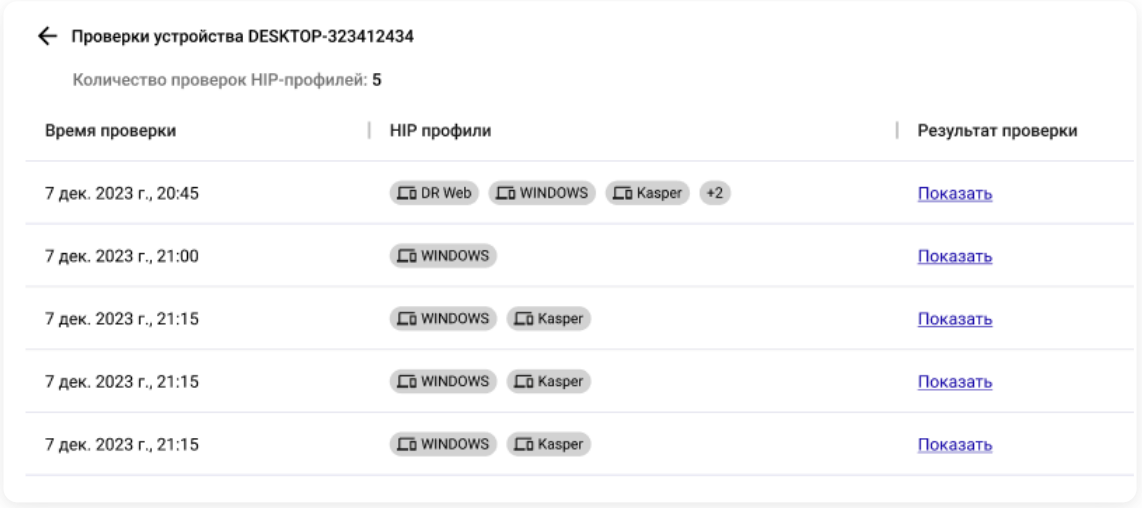
Логин	Имя	Группа	Каталог	Имя уст	HIP-про	Кол-во	Локальный IP-адр	MAC-ад	Внешни	Распол	Начало сессии	Окончание сессии	Время в сети	Тип авторизации
user-1722349439.8487763	Fedor Petrov	Managers	Локальная группа			–	192.168.100.49	–	–	–	30 июл. 2024 г., 19:24	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.045103	Kostya Kozlov	Office	Локальная группа			–	192.168.100.42	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.5970678	Arcady Fedorov	Accounting	Локальная группа			–	192.168.100.47	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.409466	Mstislav Pavlov	Accounting	Локальная группа			–	192.168.100.46	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.218858	Kesha Volkov	Support	Локальная группа			–	192.168.100.44	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.7544634	Prohor Soloviev	Office	Локальная группа			–	192.168.100.48	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.321127	Hariton Sokolov	Administrators	Локальная группа			–	192.168.100.45	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.9490948	Boris Ivanov	Accounting	Локальная группа			–	192.168.100.41	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.1288717	Igor Bogdanov	Administrators	Локальная группа			–	192.168.100.43	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.375117	Pavel Fedorov	Support	Локальная группа			–	192.168.100.36	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.2242415	Zdan Smirnov	Office	Локальная группа			–	192.168.100.34	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.1061945	Kesha Bogdanov	Support	Локальная группа			–	192.168.100.33	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.693863	Evgeny Popov	Accounting	Локальная группа			–	192.168.100.39	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.5534825	Arcady Novikov	Support	Локальная группа			–	192.168.100.38	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.306221	Boris Vasiliev	Administrators	Локальная группа			–	192.168.100.35	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349437.926114	Dorofei Smirnov	Accounting	Локальная группа			–	192.168.100.31	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.4570434	Boris Lebedev	Accounting	Локальная группа			–	192.168.100.37	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.7980504	Miron Smirnov	Office	Локальная группа			–	192.168.100.40	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.0354133	Valeri Morozov	Accounting	Локальная группа			–	192.168.100.32	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349436.9275272	Valentin Sokolov	Managers	Локальная группа			–	192.168.100.23	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)

Для поиска авторизованных пользователей нажмите на **Фильтры**, укажите в поле **Столбец** требуемый параметр поиска и в последнем поле - его значение.

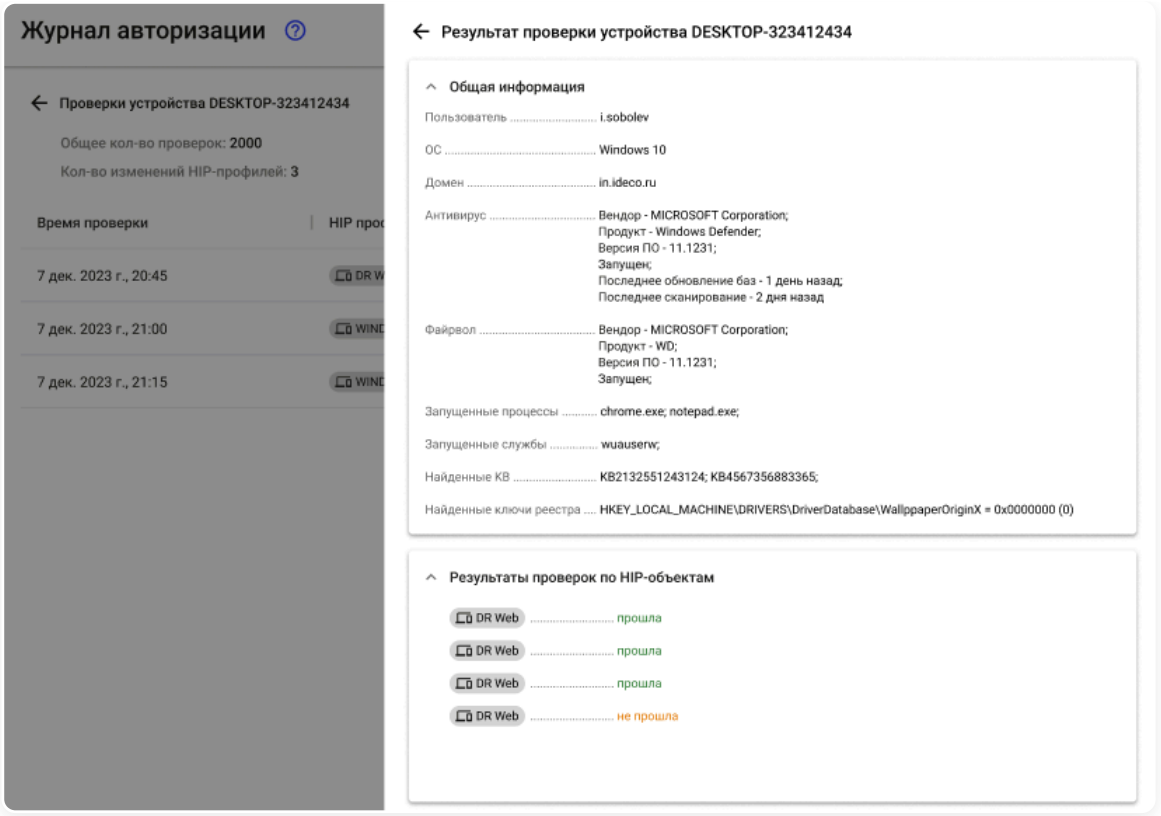
В столбце **Кол-во изменений профилей** указано количество изменений HIP-профилей, зафиксированных в результате проверок устройств, подключенных через Ideco Client. Изменения фиксируются при редактировании HIP-профиля в веб-интерфейсе или изменении соответствия устройств настроенным профилям.

Для просмотра результатов проверок устройств, подключенных через Ideco Client, выполните действия:

1. Кликните на число в столбце **Кол-во изменений профилей**. Откроется список проверок:



2. Кликните **Показать** в столбце **Результат**, чтобы увидеть общую информацию и результат проверки по HIP-объектам:



Особенности работы Журнала аутентификации:

- 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.

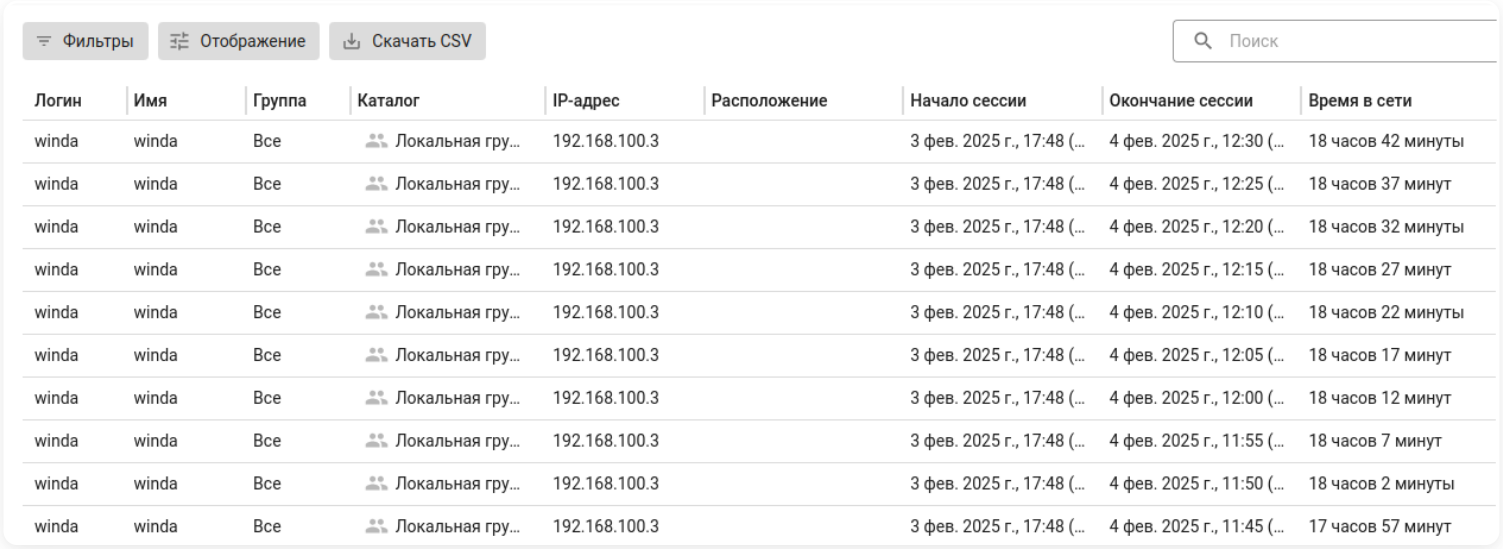
Включение опции **Показать VPN-пользователей** отфильтрует в таблице журнала информацию обо всех VPN-сессиях по всем протоколам.

Журнал аутентификации ЛК

Журнал аутентификации ЛК представляет собой историю сессий пользователей, авторизованных в личном кабинете пользователя Ideco NGFW.

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	Расположение	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;
- **Расположение** - 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:

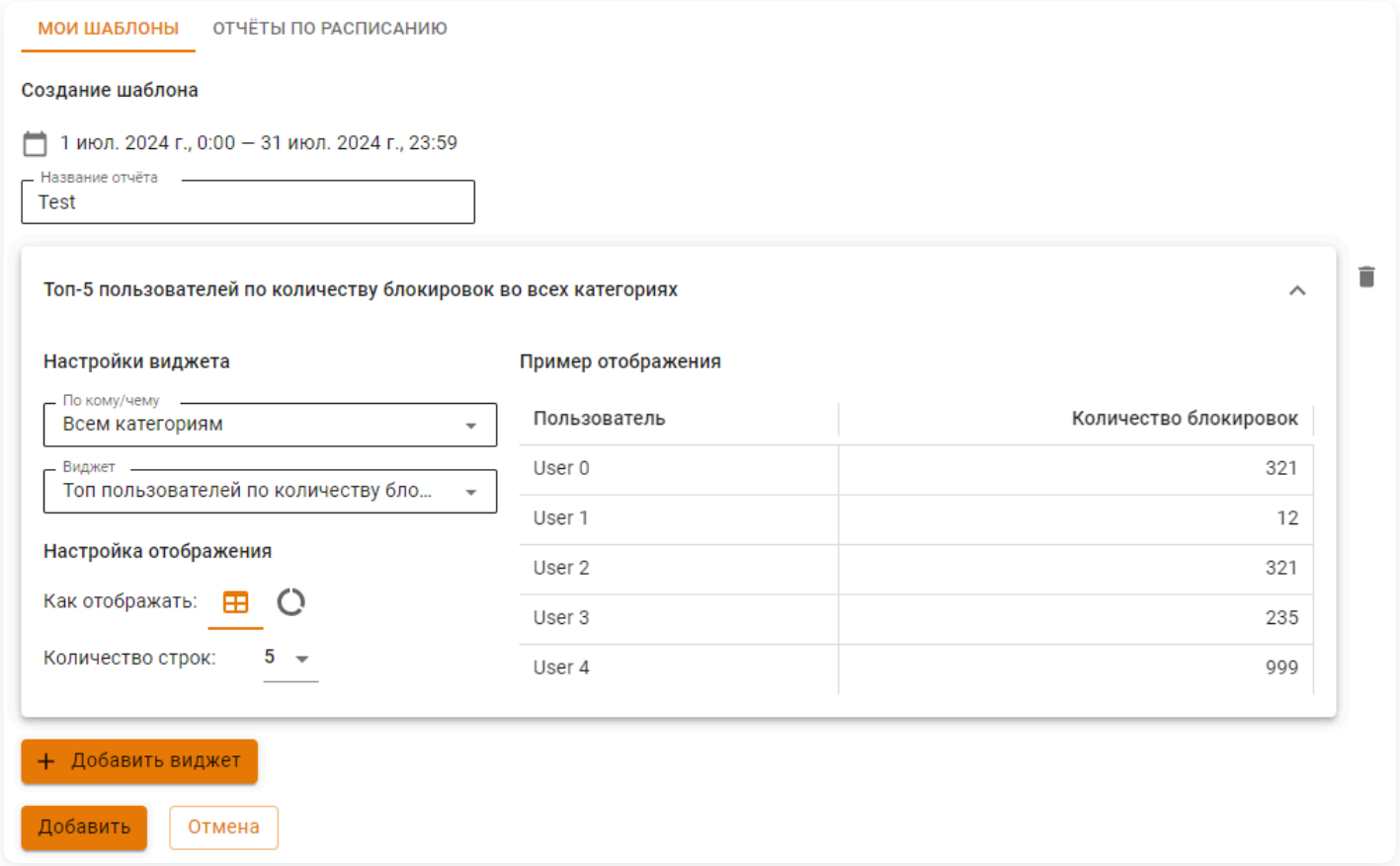
- Нажмите кнопку **Фильтры**, установите параметр поиска (все наименования доступных столбцов) и его значение;
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Конструктор отчетов

Мои шаблоны

На этой вкладке создаются шаблоны со статистикой, которые можно посмотреть в браузере, отправить на электронную почту и сохранить в формате PDF или CSV.

Для создания шаблона нажмите **Добавить** в левом верхнем углу. Откроется меню настройки шаблона. Задайте временной промежуток и название отчета, нажмите **Добавить виджет**:



- В строке **По кому/чему** выберите объект, по которому будет собираться статистика. Если выбираете **Определенный** объект (например, *Определенный пользователь* или *Определенная группа*), то появится дополнительная строка **Объекты**, где можно выбрать несколько объектов;
- В строке **Виджет** укажите, какую информацию хотите видеть по выбранному объекту. Один шаблон может содержать несколько виджетов;
- Задайте **Настройки отображения**.

После окончания настройки шаблона нажмите **Добавить**.

Ideco NGFW хранит данные в течение определенного времени, по прошествии которого они безвозвратно удаляются и не могут быть включены в отчеты.

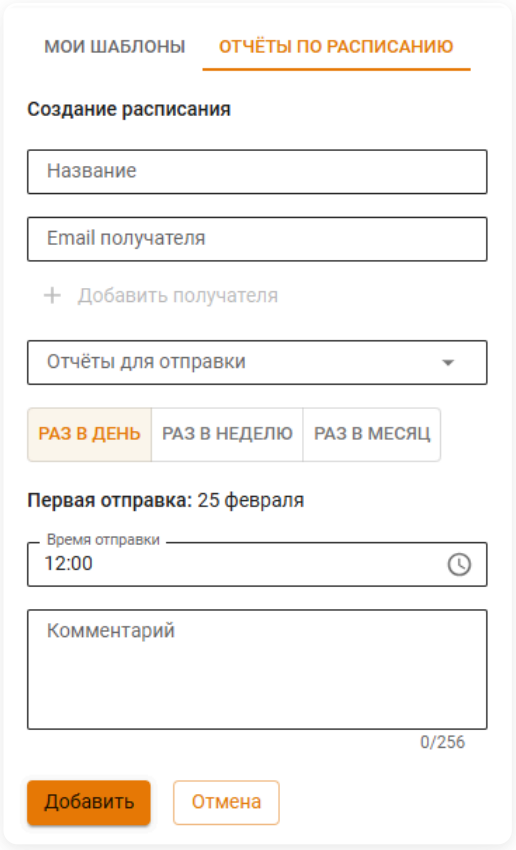
Сроки хранения данных по разделам:

- Системный журнал - 90 дней;
- Логи служб - 14 дней;
- Данные веб-трафика (Журнал веб-трафика, а также посещенные сайты) - 1 месяц;
- События безопасности (Журнал IPS и Web application firewall) - 3 месяца;
- Действия администраторов и Авторизация администраторов - 1 год;
- Журнал аутентификации - 180 дней.

Отчеты по расписанию

На этой вкладке создаются и редактируются настройки для отправки рассылки на электронную почту. Отчеты отправляются в формате PDF.

Для создания настройки нажмите **Отчеты по расписанию** → **Добавить** в левом верхнем углу. В одной настройке можно указать несколько почтовых адресов (кнопка **Добавить получателя**) и несколько отчетов (поле **Отчеты для отправки**):



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-е число, но в месяце меньше дней, то выбирается последнее число месяца.

Текст, добавленный в поле **Комментарий**, не будет отправляться в отчетах и отображается только в Ideco NGFW.

NGFW сохранит все пользовательские настройки времени отправки во всех фильтрах (раз в день, раз в неделю и раз в месяц) после нажатия на кнопку **Комментарий**, но отправляться шаблон будет только в период, выбранный пользователем.

Отчет создается выключенным. Чтобы его включить нажмите на . Если в таблице большое количество отчетов, воспользуйтесь кнопкой **Фильтры**.

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, из предложенных фильтров или укажите даты нажав **Выберите дату**.

3. Укажите название отчета (строка *Название отчета*).

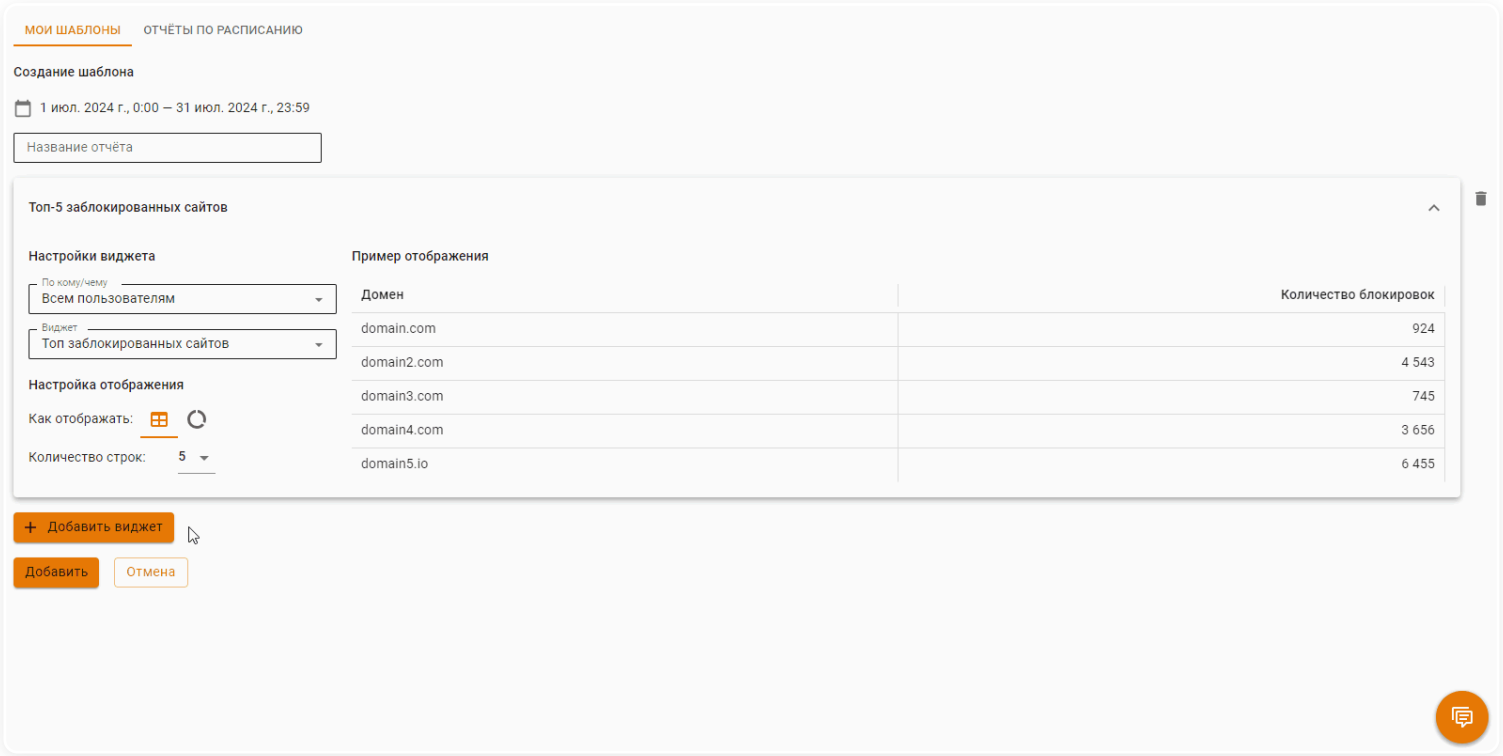
4. Кликните по кнопке **Добавить виджет**.

5. Заполните строки:

- **По кому/чему** - выберите **Всем пользователям**;

- **Виджет** - выберите **Топ заблокированных сайтов**;

6. Укажите **Настройки отображения** в виде таблицы или круговой диаграммы:



7. Сохраните шаблон по кнопке **Добавить**.

Создайте правило, по которому шаблон отчета будет отправляться на электронную почту:

1. Нажмите **Добавить** на вкладке **Отчеты по расписанию**.

2. Заполните строки:

- **Название** - любое название, которое поможет идентифицировать правило расписания;
- **Email получателя** - электронная почта получателя отчета. Если нужно отправлять отчет нескольким получателям, укажите дополнительные адреса по кнопке **Добавить получателя**.

3. Выберите нужный шаблон в поле **Отчеты для отправки**.

4. Укажите настройки даты/дня и времени отправки отчета получателю (раз в месяц, каждый 1-й день месяца).

Syslog

Название службы раздела **Syslog**: `ideco-logs-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 **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 **Отчеты и журналы** → **Syslog** и выполните действия:

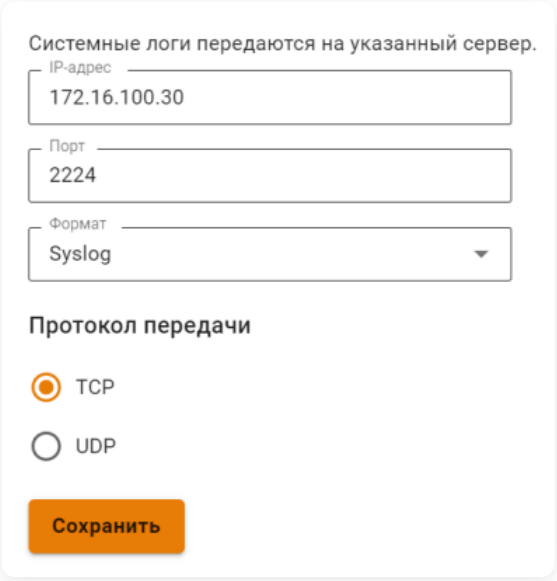
1. Укажите IP-адрес сервера-коллектора (любой локальный или публичный IP-адрес).

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.

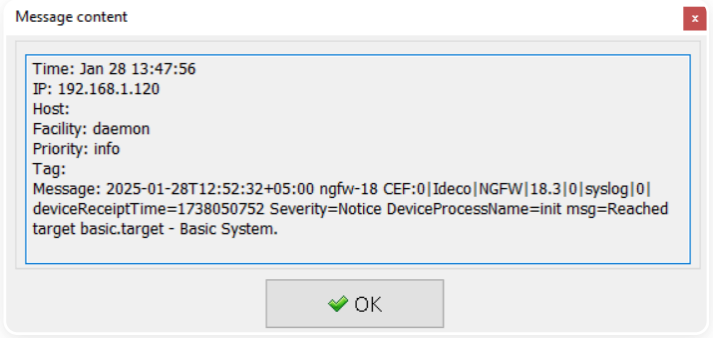
5. Нажмите **Сохранить** и включите опцию **Syslog**:



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

```
2025-10-15T15:38:54+05:00 ideco-ngfw CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=17605272289 Severity=Informational
```

где:

- `2025-10-15T15:38:54+05:00` - время события в Ideco NGFW;
- `ideco-ngfw` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `CEF:0` - версия формата CEF;
- `Ideco` - вендор;
- `NGFW` - название продукта;
- `19.0` - версия продукта;
- `0|syslog|0` - идентификатор лога, постоянный для NGFW. Состоит из трех полей: идентификатор типа события, описание события, важность события;
- `deviceReceiptTime` - время события в системе NGFW, 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;
- `ideco-ngfw` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса.

Журнал Трафик

CEF:

```
2025-10-16T16:32:06+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1760614326 Severity Informational device
```

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 службы.

outcome	result	Общий результат проверки. Возможные значения: • `absent` - отсутствие значения; • `accept` - разрешение; • `drop` - запрет.
deviceEventClassId	rule_id	Идентификатор правила **Файрвола**. Пустая строка означает отсутствие значения.
name	table	Название таблицы, в которой сработало правило. Возможные значения: • `absent` - отсутствие значения; • `fwd` - таблица **FORWARD** раздела **Файрвол** Ideco NGFW; • `fwd_a` - постправило FORWARD Ideco Center; • `fwd_b` - предправило FORWARD Ideco Center; • `fwd_s` - системное правило FORWARD; • `inp` - таблица **INPUT** раздела **Файрвол** Ideco NGFW; • `inp_a` - постправило INPUT Ideco Center; • `inp_b` - предправило INPUT Ideco Center; • `inp_s` - системное правило INPUT.
act	action	Действие правила **Файрвола**. 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 протокола прикладного уровня.
app	dpi_protocol	Название приложения.
proto	protocol	Название протокола.
sourceAddress	src_ip	IP-адрес источника.
sourcePort	src_port	Порт источника. Значение `0` означает 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.
cs4	dst_location_name	Название локации назначения.
-	dst_location_code	Код локации назначения.
destinationAddress	dst_ip	IP-адрес назначения.
destinationPort	dst_port	Порт назначения. Значение `0` означает 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.

cs5	dst_location_name	Название локации назначения.
cs6	dst_location_code	Код локации назначения.
flexNumber1	dnat_rule_id	Идентификатор DNAT правила. Пустая строка означает отсутствие значения.
destinationTranslatedAddress	dnat_ip	IP-адрес, на который был изменен адрес назначения.
destinationTranslatedPort	dnat_port	Порт, на который был изменен порт назначения.
flexNumber2	snat_rule_id	Идентификатор SNAT правила. Пустая строка означает 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:

```
2025-10-16T17:02:26+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.7|0|syslog|0|deviceReceiptTime=1760616146 Severity=Informational Device
```

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**	**Описание**
DeviceProcessName	web-proxy	Название службы.
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.
DeviceCustomString1	redirected_to	Если запрос попал под правило перенаправления, отображает url куда перенаправило, если нет - пустая строка.
DeviceCustomString2	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` означает 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` означает отсутствие данных.
DeviceCustomString3	mime	Content-Type HTTP запроса. Отсутствие данных отображается пустой строкой.
requestClientApplication	useragent	User-Agent HTTP запроса. Отсутствие данных отображается пустой строкой.
DeviceCustomString4	user_name	Имя пользователя, который авторизован с IP источника.
-	login	Логин пользователя.

DeviceCustomString5	group_name	Имя группы, в которую входит пользователь.
DeviceCustomString6	referer	Referer HTTP запроса. Отсутствие данных отображается пустой строкой.

Предотвращение вторжений

CEF:

```
2025-10-15T18:21:45+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.7|0|syslog|0|deviceReceiptTime=1760534505 Severity=Warning DeviceCustom
```

Syslog:

```
2025-08-25T16:38:36+05:00 ideco-ngfw suricata - - - flow_id:1344232018329395, in_iface:, sensor_name:ideco-ips, event_type:al
```

где:

Ключ CEF	**Ключ Syslog**	**Описание**
-	suricata	Название службы.
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 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 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.
EndTime	flow.end	Окончание.
FlexNumber3	flow.age	Возраст.
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 TCP-пакета, указывающий, что пакет получен.
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.

Из сообщений модулей, перечисленных ниже, SIEM не сможет извлечь ключевые поля для последующего анализа. Такие сообщения доступны только для просмотра в исходном виде.

Контент-фильтр

Логирование включается в разделе **Сервисы** → **Прокси** → **Основное**. Просмотр логов доступен в веб-интерфейсе в разделе **Отчеты и журналы** → **Системный журнал**. Название служб для фильтрации: `ideco-content-filter-backend` и `squid`.

CEF:

```
2025-08-25T17:31:18+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1760540338 Severity=Notice DeviceProcess
```

Syslog:

```
2025-08-25T17:31:18+05:00 ideco-ngfw squid - - - {192.168.100.11 - - [25/Aug/2025:17:31:18 +0500] "GET http://porno365.plus/c
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	web-proxy	Название службы.

Информация в сообщении:

- `192.168.100.11` - IP-адрес пользователя;

- `[25/Aug/2025:17:31:18 +0500]` - дата/время события блокировки;
- `GET` - метод;
- `http://porno365.plus/categories` - URL заблокированного ресурса;
- `HTTP/1.1` - протокол;
- `403` - код состояния HTTP;
- `7470` - передано байт (в ответ, включая HTTP-заголовок);
- `https://www.google.com/` - HTTP referer;
- `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0` - цифровой отпечаток браузера;
- `TCP_DENIED:HIER_NONE` - техническое сообщение от squid;
- `Custom deny 3 P‘P»PsPєPёCЂPsPIPєP° CЃP°P№C,PsPI CЃ PSPµPїPsPґPsP±P°CЂC‰PёPj PєPsPSC,PµPSC,PsPj cf_extended.id.16 group.id.1  0` - сообщение о запрете из-за пользовательской категории;
- `"av_name"` - название антивируса, если он включен, в примере антивирус отключен;
- `"av_object_infected"` - результат проверки антивирусом, пустое поле - вирус не обнаружен;
- `"av_object_size"` - размер проверяемого объекта;
- `"av_virus_name"` - название обнаруженного вируса;
- `"x_infection_found"` - подтверждение, что запрос был обработан ICAP-оберткой для антивируса (Касперский);
- `"x_virus_id"` - идентификатор вируса/вредоносной программы;
- `"x_av_verifed"` - результат проверки антивирусом;
- `"morph-action"` - результат проверки **Морфологическим анализом**;
- `"morph-dict-id"` - название морфологического словаря, указывается в случае запрета **Морфологическим анализом**.

Авторизация через журнал безопасности AD

CEF:

```
2025-10-15T18:21:45+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1721305222 Severity=Notice DeviceProcess
```

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 службы.

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-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731923661 Severity=Notice DeviceProces
```

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 службы.

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-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731937903 Severity=Notice DeviceProces
```

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 службы.

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|18.0|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 службы.

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-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731938874 Severity=Notice DeviceProces
```

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 службы.

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'`).

Подключение по VPN

CEF:

```
2024-11-18T19:16:18+05:00 ideco-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731939378 Severity=Notice DeviceProces
```

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 службы.

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'`).

Служба fail2ban

CEF:

```
2024-11-18T19:26:57+05:00 ideco-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Notice DeviceProces

2024-11-18T19:26:57+05:00 ideco-ngfw CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Warning DevicePro
```

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 службы.

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.

Управление сервером

В этом разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

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 даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Администраторы

В Ideco NGFW вы можете создать локальных администраторов или интегрировать администраторов из сервисов Active Directory, ALD PRO, RADIUS.

Сведения об авторизованных администраторах представлены в разделах **Аутентификация администраторов** и **Сессии администраторов**.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока сессия администратора будет автоматчиески завершена.

Роли администраторов

Роль	Возможности
Администратор	• Полный доступ ко всем настройкам NGFW, возможность создания новых настроек, правил, учетных записей других пользователей NGFW, а также редактирования, управления и удаления их • Создание пользователей с правами администратора
Только просмотр	• Полный доступ к просмотру всех настроек NGFW без возможности создания новых настроек, правил, учетных записей других пользователей NGFW, а также редактирования, управления и удаления их

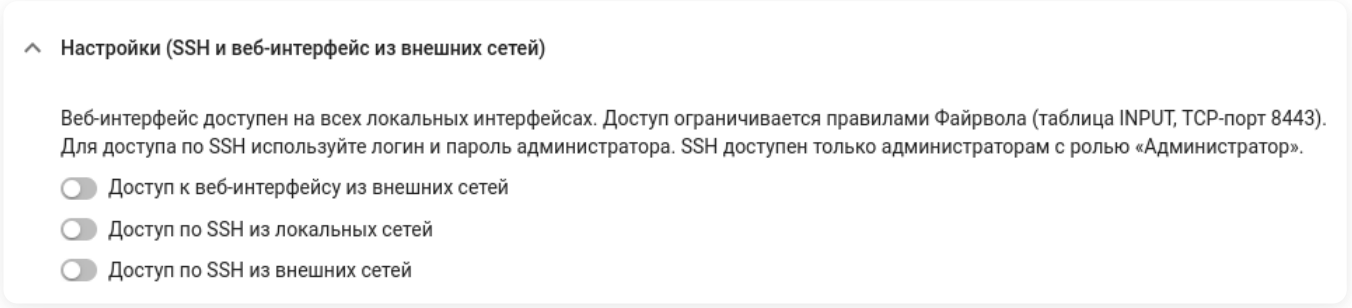
Администратор ИБ	• Выбор событий безопасности, подлежащих регистрации в журнале **События безопасности**
	• Чтение журнала **События безопасности**
	• Настройка параметров выгрузки информации о событиях безопасности, зарегистрированных в NGFW
	• Формирование отчетов в формате `.csv` с учетом заданных критериев отбора и выгрузка их из журнала событий безопасности NGFW
	• Настройка и получение оповещений в веб-интерфейсе NGFW 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 файрвола	• Создание учетных записей других пользователей NGFW.
	• Управление учетными записями пользователей NGFW, 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, 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
	• Применение правил фильтрации к:
	  ◦ сетевым интерфейсам NGFW
	  ◦ идентифицированным пользователям NGFW
	  ◦ 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
	• Изменение конфигурации NGFW
	• Тестирование NGFW

Администратор настройки доступов	• Создание учетных записей других пользователей NGFW • Управление учетными записями пользователей NGFW, 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, определяемых их ролями • Определение периода неактивности пользователя, по истечении которого сессия пользователя завершится (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**, **Журнал событий**, **Журнал веб-трафика**, **События безопасности** и **Журнал аутентификации**
Создание отчетов	• Просмотр, настройка и выгрузка отчетов в формате .csv для следующих журналов: **Трафик**, **Журнал событий**, **Журнал веб-трафика**, **События безопасности**, **Журнал аутентификации** и **Конструктор отчетов**

Доступ к веб-интерфейсу из внешней сети и удаленный доступ по SSH

- Для получения доступа к Ideco NGFW из внешней сети включите опцию **Доступ к веб-интерфейсу из внешней сети**. Эта функция помогает администрировать Ideco NGFW удаленно. Попытки подбора паролей блокируются автоматически.
- Для получения доступа к Ideco NGFW по SSH из локальной или внешних сетей включите соответствующие опции. Доступ осуществляется по 22 TCP-порту. Попытки подбора паролей также будут автоматически блокироваться:



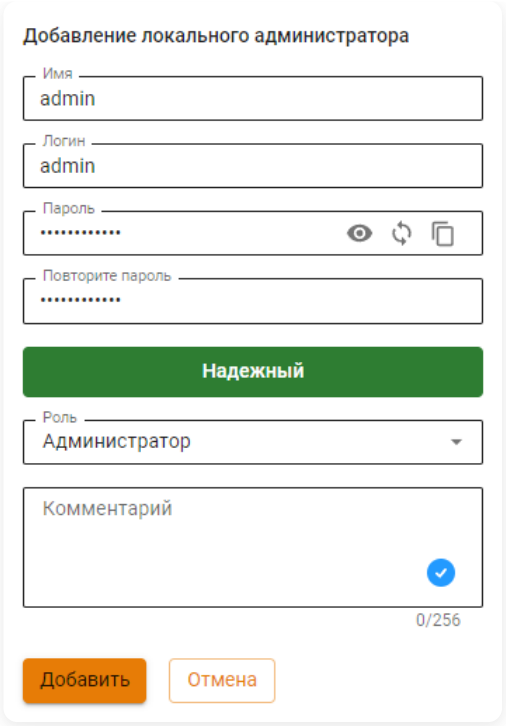
Подробнее о настройке подключения к веб-интерфейсу при удаленном доступе смотрите в статье Удаленный доступ для управления сервером.

Управление локальными администраторами

Чтобы добавить нового локального администратора выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **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 превышать 42 символа и не должно состоять только из цифр.
- **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).
- **Роль** - выберите роль.

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**.

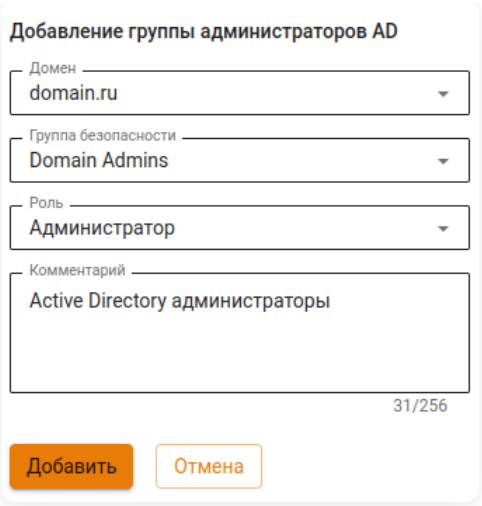
Управление AD/ALD администраторами

Чтобы добавить администраторов, необходимо ввести NGFW в домен Active Directory. При удалении домена AD/ALD из Ideco NGFW будут удалены сессии администраторов.

Чтобы интегрировать администраторов Active Directory или ALD Pro с Ideco NGFW, выполните действия:

1. Перейдите в **Управление сервером** → **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 администраторов идентичны ролям локальных администраторов.

3. Нажмите **Добавить**.

Особенности работы:

- Если администратор был авторизован по правилу или группе безопасности, которые были удалены, его сессия будет удалена. Это произойдет только после синхронизации групп безопасности на Ideco NGFW, которая выполняется каждые 5 минут.
- Если администратора исключить из группы безопасности, он не будет удален сразу. Его сессия завершится через некоторое время, и при следующей попытке авторизации он 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 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.

Чтобы узнать ID роли RADIUS-администратора:

1. Перейдите в **Управление сервером** → **Администраторы** → **Роли**.

2. Нажмите на **Отображение** и включите столбец ID. ID роли появится в левом столбце таблицы.

ID роли администраторов

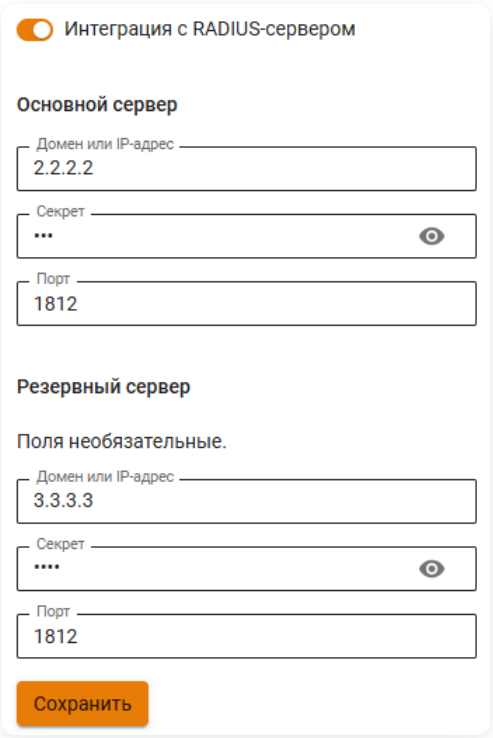
- `predefined_admin_write` - Администратор.
- `predefined_admin_readonly` - Только просмотр.
- `predefined_security_admin` - Администратор информационной безопасности.
- `predefined_firewall_admin` - Администратор файрвола.
- `predefined_access_settings_admin` - Администратор настройки доступов.
- `predefined_reports_view` - Просмотр отчетов.
- `predefined_reports_change` - Создание отчетов.

Интеграция администраторов RADIUS с Ideco NGFW

Выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **RADIUS** и включите опцию **Интеграция с RADIUS-сервером**.

2. Укажите доменное имя или IP-адрес внутреннего RADIUS-сервера и секрет (пароль доступа). Если требуется, поменяйте порт, по которому будет происходить подключение к серверу:



При наличии в сети двух RADIUS-серверов настройте один как резервный с указанием порта подключения.
При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.

3. Нажмите **Сохранить**.

Особенности удаления администраторов

- Если администратора удалить из раздела **Администраторы**, его сессия будет автоматически завершена, и он 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 на 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 будет потерян. Если это произошло, обратитесь в Техническую поддержку.

Аутентификация администраторов

Ideco NGFW 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 считает попытку авторизации неудачной и блокирует доступ, если количество неудачных попыток превышает шесть.

Чтобы получить доступ к веб-интерфейсу Ideco NGFW, администратору нужно выполнить процедуру аутентификации, указав логин и пароль.

Для разных групп администраторов предусмотрены разные логины:

- **Локальный администратор** - логин в формат `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.

Ideco Center

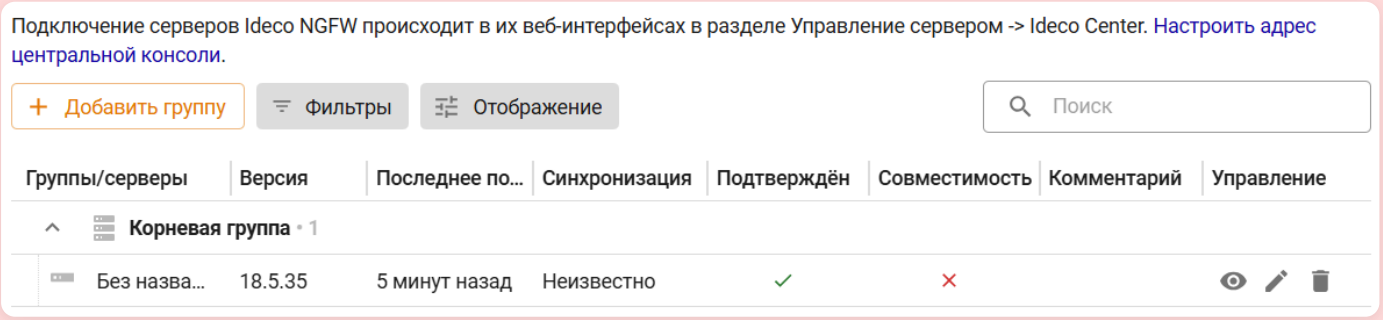
Название службы раздела **Ideco Center**: `ideco-central-console-backend`.

Список служб для других разделов доступен по ссылке.

Ideco Center - это центральная консоль, которая поможет в администрировании нескольких серверов Ideco NGFW. На данный момент не требует лицензирования и не имеет ограничений к использованию. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW, даже если они были подключены после того, как политики были настроены.

Подключение Ideco NGFW к Ideco Center

При синхронизации Ideco Center и Ideco NGFW 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 несовместимы:

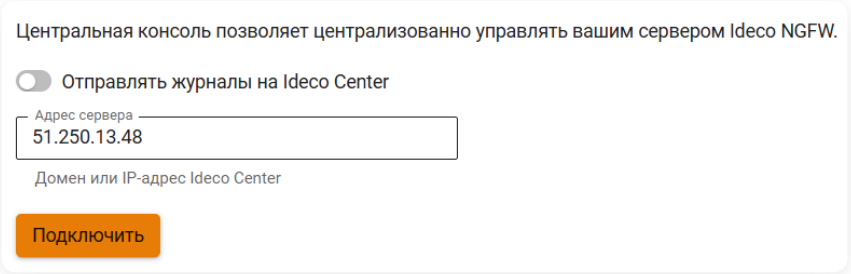


Особенности работы:

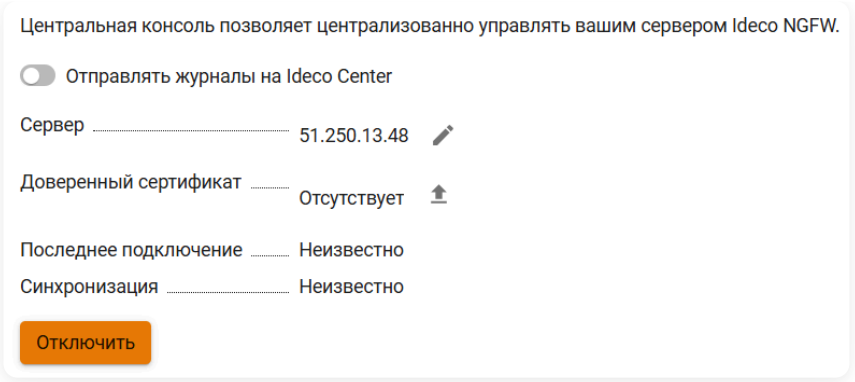
- Если в подключаемом Ideco NGFW используется кластер, достаточно подключить только активную ноду, пассивная автоматически примет эту настройку;
- Сетевое подключение производится в направлении от Ideco NGFW к Ideco Center, т. е. возможна связь и когда Ideco NGFW за NAT;
- Если сервер Ideco Center находится за NAT, укажите IP-адрес NAT-устройства или доменное имя, перейдя в Ideco Center в раздел **Управление сервером → Дополнительно → Адрес Ideco Center**.

1. Перейдите в раздел **Управление сервером → Ideco Center**.

2. Введите IP-адрес или доменное имя в строке **Адрес сервера** и нажмите **Подключить**:

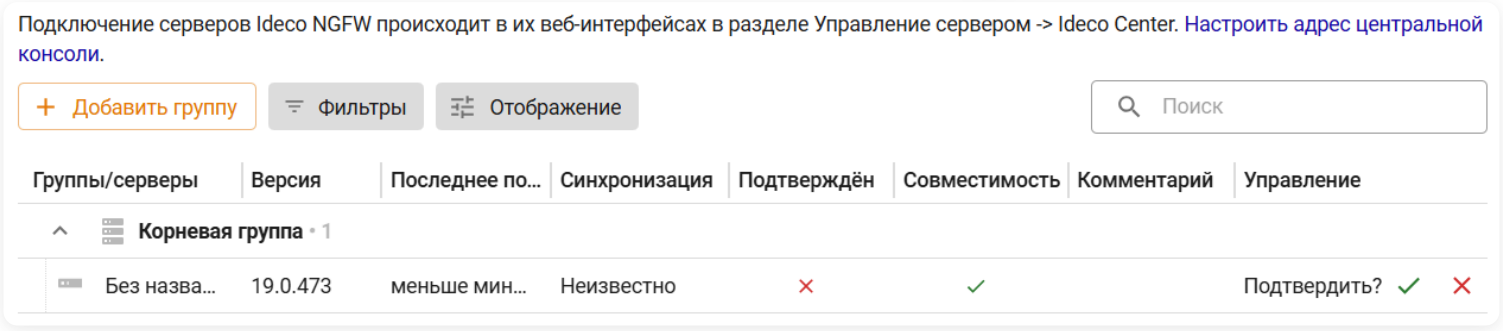


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW:

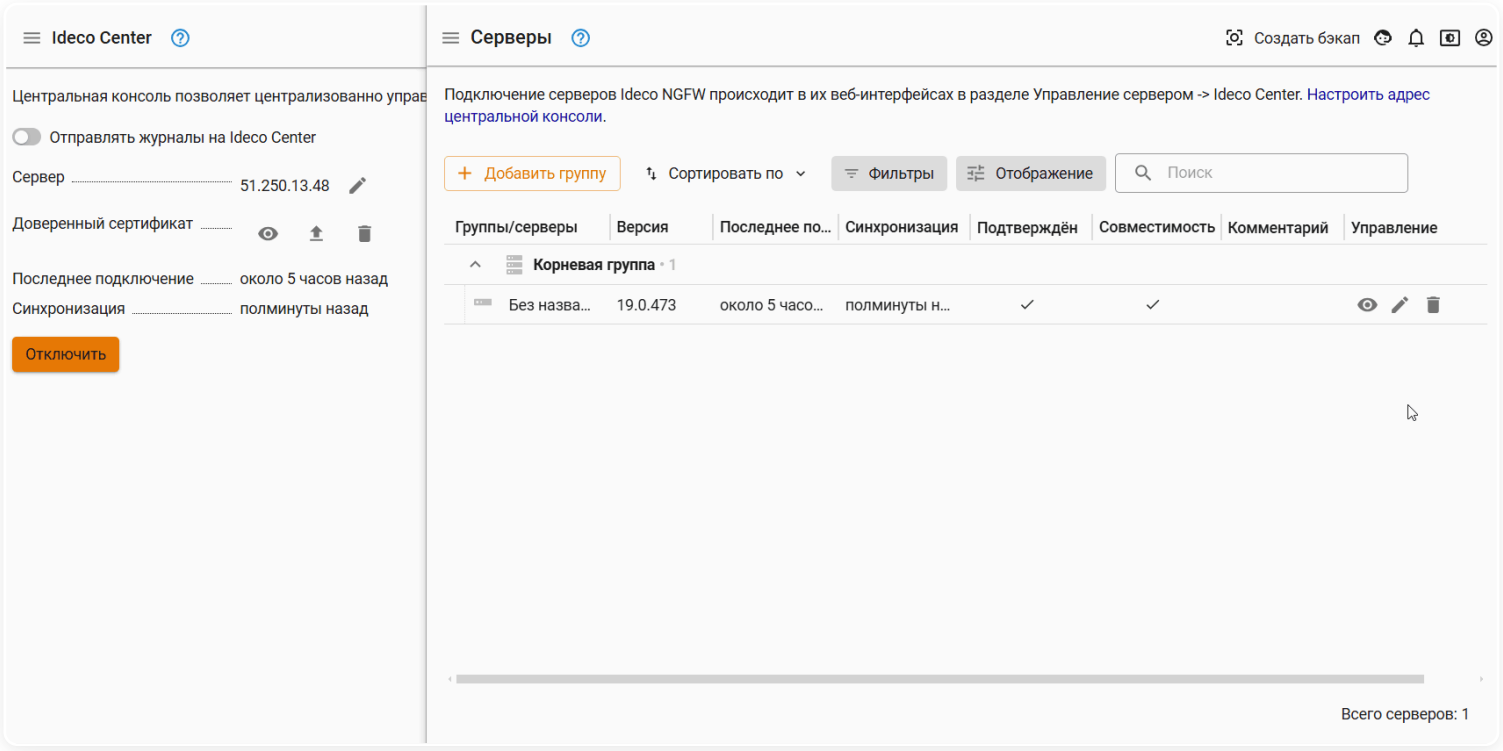


Скачать корневой сертификат можно в Ideco Center, раздел **Сервисы** → **Сертификаты**.

3. В интерфейсе Ideco Center перейдите в раздел **Серверы** и подтвердите подключение кнопкой :



Для удаления сервера Ideco NGFW из Ideco Center разорвите привязку в интерфейсе Ideco Center:



Настройка просмотра логов

Для отображения логов Ideco NGFW в разделе **Отчеты и журналы** Ideco Center необходимо включить опцию **Отправлять журналы на Ideco Center**:

Центральная консоль позволяет централизованно управлять вашим сервером Ideco NGFW.

Отправлять журналы на Ideco Center

Сервер 158.160.58.43

Доверенный сертификат .....

Последнее подключение ..... около 3 часов назад

Синхронизация ..... полминуты назад

Отключить

VCE

Название службы раздела **VCE**: `ideco-vce-backend`.

Список служб для других разделов доступен по ссылке.

VCE (virtual context engine) - это функциональность Ideco NGFW, реализованная с помощью контейнеров Linux на базе systemd-nspawn, которая позволяет создавать виртуальные серверы (контексты) на одном корневом NGFW. 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.

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.

Сейчас для каждого созданного VCE загружается файл лицензии корневой системы. Это значит, что на Ideco NGFW с лицензией на 100 пользователей можно создать неограниченное количество VCE, каждый из которых также будет поддерживать по 100 пользователей.

Функциональность созданных внутри NGFW виртуальных VCE почти не отличается от функциональности NGFW.

Возможности VCE:

- Создание виртуальных серверов Ideco NGFW и настройка независимых сетевых интерфейсов.
- Независимая настройка политик безопасности и прав доступа различным виртуальным NGFW.
- Связь с Ideco Center.
- Запуск и остановка виртуальных серверов с одного корневого NGFW.

В интерфейсе VCE недоступно:

- Создание кластера.
- Обновление.
- Переход в **Профиль** через иконку в шапке веб-интерфейса (настраивается в корневой системе).
- Возможность выключения и перезагрузки (настраивается в корневой системе).
- Энергосберегающий режим (настраивается в корневой системе).
- Изменение настроек часового пояса и языка (настраивается в корневой системе).

Важные моменты работы VCE:

- В бэкап корневого 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.
- Нельзя добавлять в VCE LACP-интерфейсы.
- **Не рекомендуем создавать VCE на нодах кластера.** Если на одной из нод кластера создан VCE, со второй нодой будут синхронизироваться только данные таблицы раздела **Управление сервером -> VCE**. После переключения на пассивной ноде будет создан VCE с тем же именем и комментарием, но внутренние настройки VCE (администраторы, сетевые интерфейсы, политики безопасности и т. д.) не перенесутся.

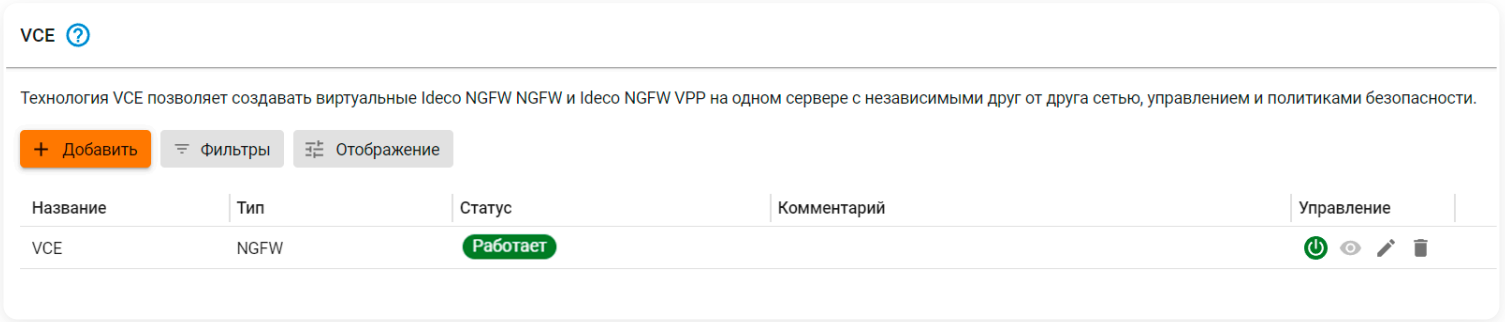
Создание VCE

Для работы VCE требуется минимум 8 ГБ оперативной памяти, а максимум можно выделить 16 ГБ.

Чтобы создать виртуальный сервер в рамках VCE, перейдите в раздел **Управление сервером** → **VCE** и выполните действия:

1. Нажмите кнопку **Добавить**.

2. Введите название сервера и нажмите **Добавить**. Виртуальный сервер появится в таблице:



3. Перейдите в раздел **Сервисы → Сетевые интерфейсы** и на вкладке **VCE** создайте интерфейс для виртуального сервера. Для работы VCE нужен минимум один сетевой интерфейс. Подробнее о создании VCE-интерфейсов в статье.

Сетевой интерфейс без тега VLAN, подключенный к VCE, будет недоступен для использования корневым NGFW.

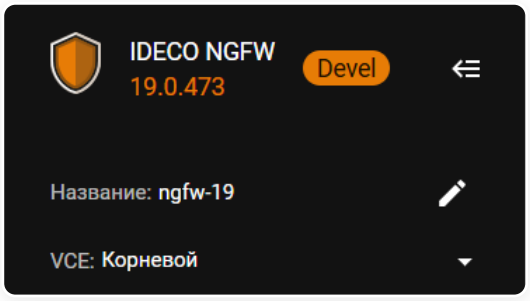
Если VCE выключен, переданные ему сетевые интерфейсы становятся вновь доступны корневому NGFW, их можно использовать для создания нового виртуального сервера. При этом VCE, которому они принадлежали ранее, станет недоступен после включения.

Чтобы отредактировать VCE, нажмите на . При редактировании можно менять название виртуального сервера. Редактирование доступно в том числе для работающего VCE.

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

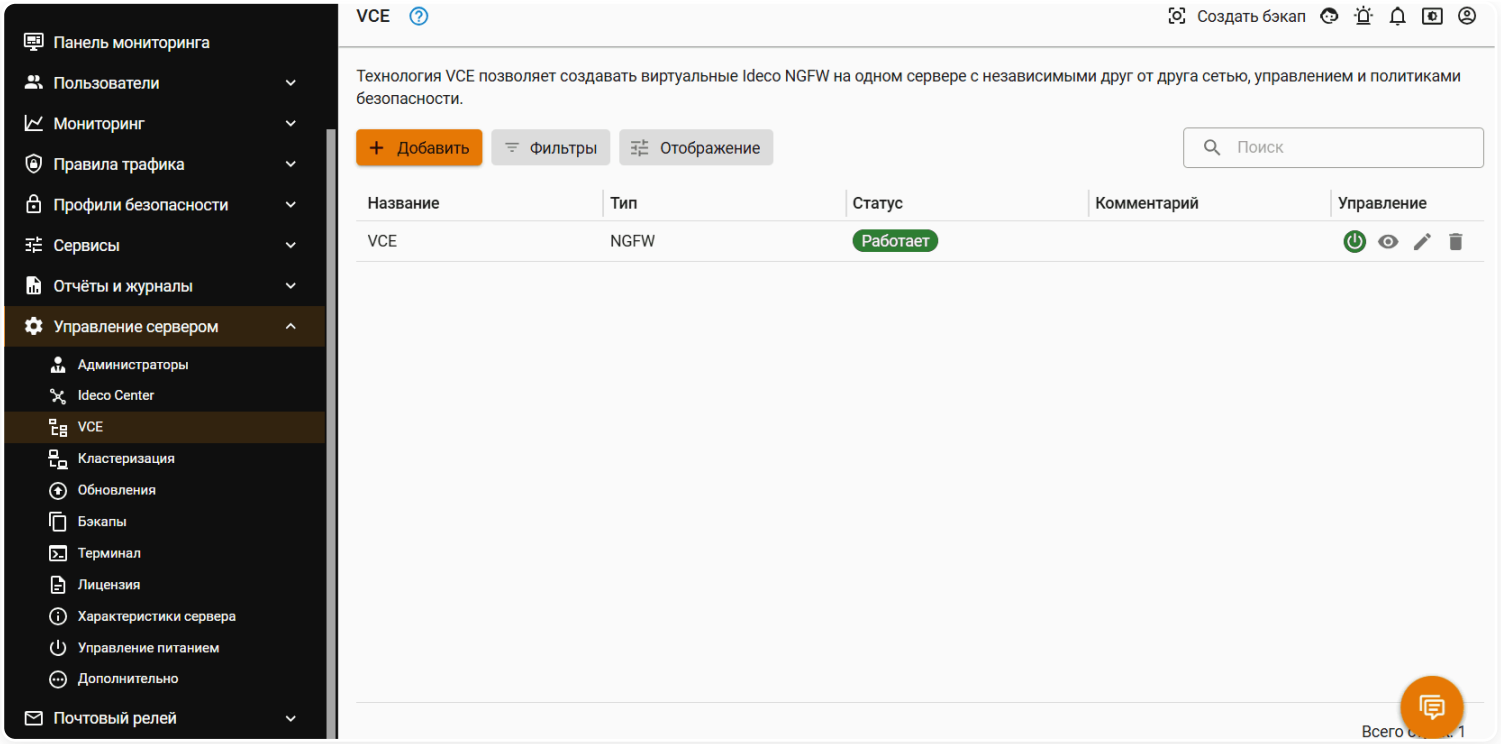
Переход в веб-интерфейс VCE

После создания VCE текущий сервер NGFW, в котором VCE был создан, будет обозначен как корневой:



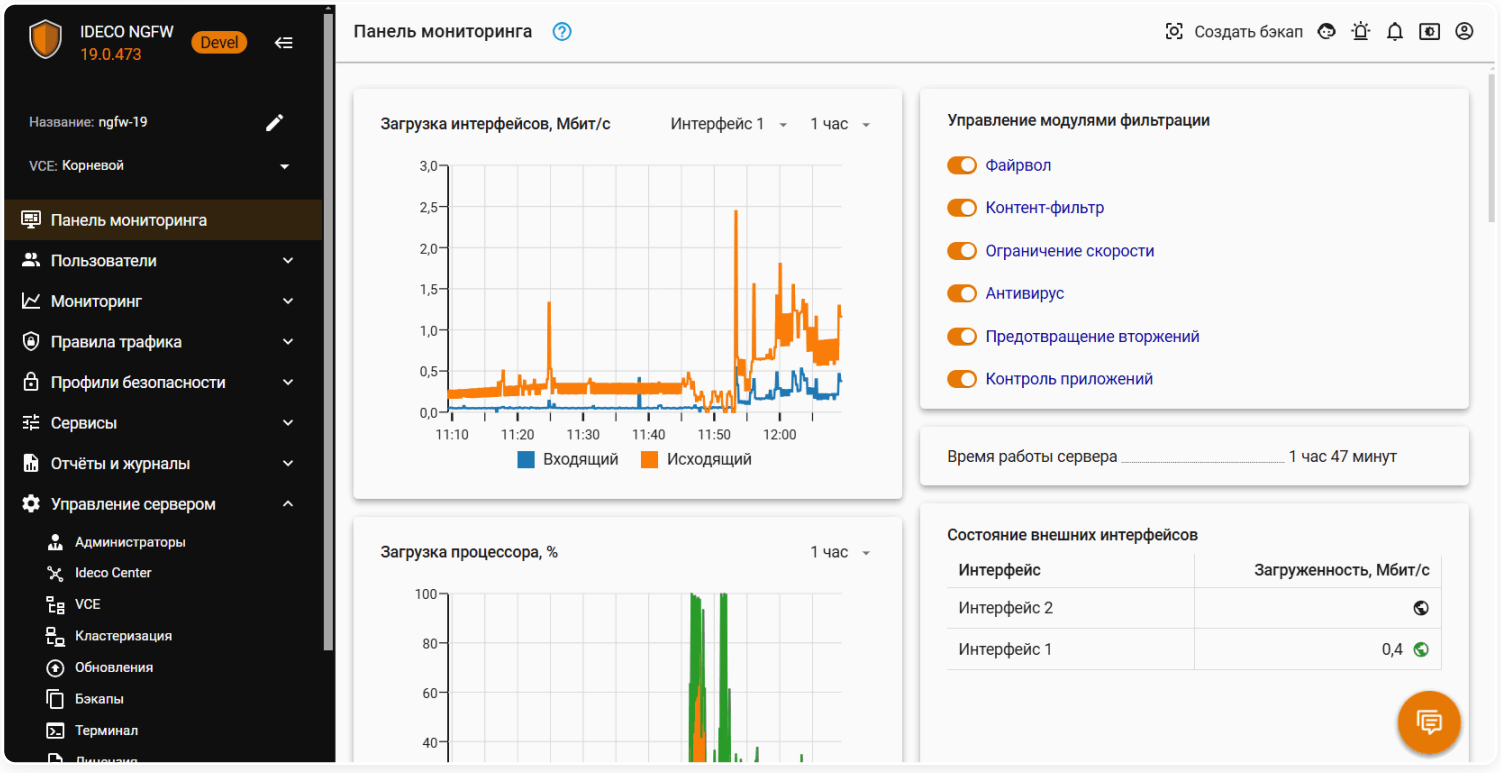
Перейти в веб-интерфейс созданного VCE из веб-интерфейса NGFW можно двумя способами:

1. Перейдите в **Управление сервером → VCE** и нажмите на :



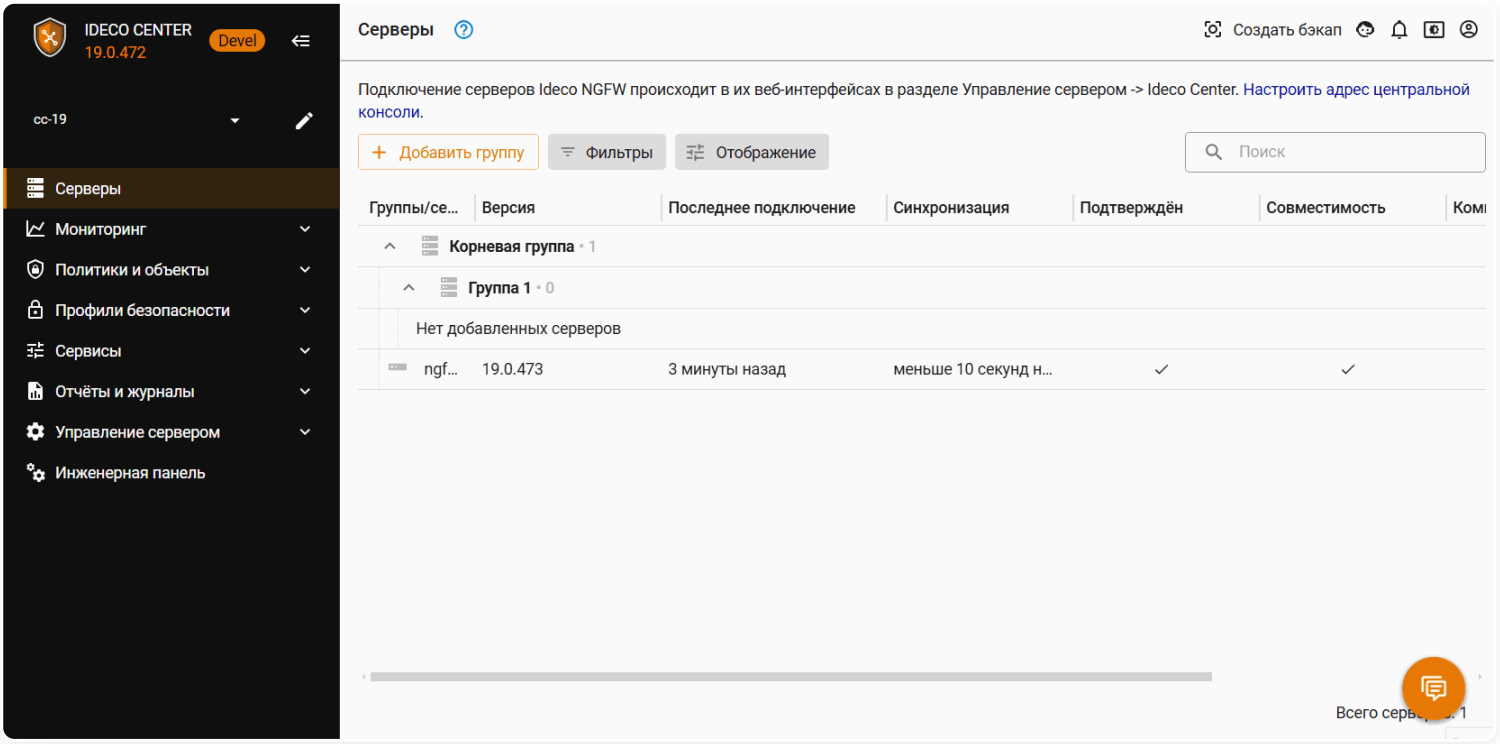
В новой вкладке откроется веб-интерфейс VCE.

2. Нажмите на  в левом верхнем углу и выберите нужный VCE:



Также перейти в веб-интерфейс VCE можно из веб-интерфейса Ideco Center. Для этого сначала перейдите из интерфейса Ideco Center в интерфейс корневого NGFW одним из способов, указанных в статье.

Пример перехода:



Удаление VCE

Удалить VCE можно, нажав на в корневом VCE.

После удаления VCE все его настройки, журналы и внутренние данные будут безвозвратно утеряны. Восстановить их будет невозможно.

Кластеризация

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, 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.

В любой момент обрабатывать трафик может только одна из нод.

Административно переключить ноды нельзя.

Критерии выбора активной ноды

- **Процент сетевых интерфейсов с линком** - отношение количества настроенных физических сетевых интерфейсов, находящихся в состоянии `up` и имеющих подключение (`carrier`), к общему числу настроенных физических интерфейсов. Значение `1.0` означает, что подключение присутствует на всех интерфейсах.
- **Количество деградаций сети** - число ухудшений значения показателя **Процент сетевых интерфейсов с линком**. Деградацией считается любое уменьшение значения относительно предыдущего максимума (например, `0.5` → `1.0` → `0.2` → `0.5` - одна деградация). Показатель используется для снижения вероятности переключений при нестабильных (мигающих) подключениях.
- **Uptime** - время непрерывной работы ноды с момента последней загрузки. Более высокий `uptime` означает более длительную и стабильную работу ноды без сбоев.

Сетевое взаимодействие между нодами осуществляется по *Кластерной сети*. Это физический канал, под который на каждой из нод резервируется по одному физическому порту. При переключении нод резервная нода становится активной.

Если IP-адреса кластера настроены вручную, то он 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.

Процесс синхронизации нод в кластере

- При синхронизации двух NGFW данные активной ноды копируются в резервную ноду. Вся информация на резервной ноде перезаписывается.
- 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.

Для корректной работы кластера необходимо постоянное наличие связи между нодами. Для моментального переключения ноды следует соединять прямым сетевым соединением, не используя мост или коммутатор.

Обмен данными между нодами кластера происходит раз в три минуты. 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

Имя сервера активной ноды отображается в левом верхнем углу веб-интерфейса, под именем кластера.

Для проверки статуса текущей ноды:

1. Перейдите в раздел **Управление сервером** → **Терминал** веб-интерфейса NGFW или в консоль в локальном меню.

2. Введите команду:

```
etcdctl_rt get /cluster/status/v1/record
```

Вывод команды:

- `{"state": "ACTIVE"}` - текущая нода - активная;
- `{"state": "RESERVE"}` - текущая нода - резервная;
- `{"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 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 раздел **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>` - для проверки статуса служб Ideco NGFW.

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.
- Время переключения нод - 15 секунд. При потери связи между нодами переключение происходит моментально.
- 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.

Возможные проблемы при работе двух Ideco NGFW 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 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 несовместим с агрегацией интерфейсов (LACP)**. При добавленном LACP-интерефейсе настройка кластера будет невозможна. В работающем кластере нельзя создать LACP-интерфейсы.

Для перехода между режимами требуется:

- Либо разрушить кластер (для создания LACP-интерфейса).
- Либо удалить агрегированные интерфейсы (для настройки кластера).

Не рекомендуем создавать VCE на нодах кластера. Если на одной из нод кластера создан VCE, со второй нодой будут синхронизироваться только данные таблицы раздела **Управление сервером -> VCE**. После переключения на пассивной ноде будет создан VCE с тем же именем и комментарием, но внутренние настройки VCE (администраторы, сетевые интерфейсы, политики безопасности и т. д.) не перенесутся.

Настройка кластера

Если на момент создания кластера у вас уже есть настроенный Ideco NGFW, рекомендуем выбрать его в качестве активной ноды. Все настройки резервной ноды в процессе создания кластера будут удалены.

Требования

Для создания кластера необходимо соблюдение следующих требований:

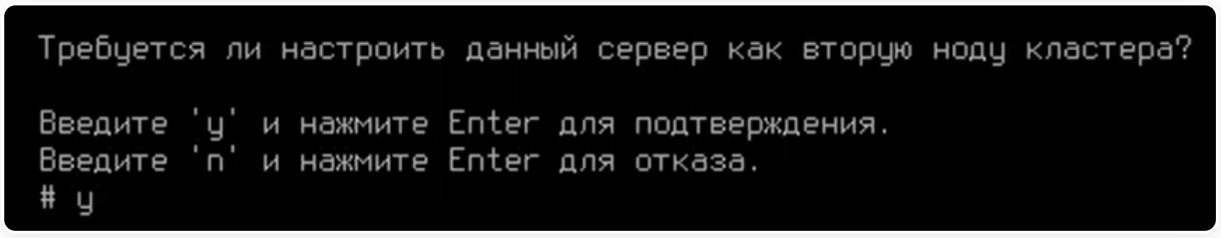
- В кластере может быть только две ноды Ideco NGFW;
- Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки;
- Количество **используемых** физических сетевых портов на обоих серверах должно совпадать. В ином случае создать кластер нельзя. При этом само наличие дополнительных физических сетевых портов на нодах на создание кластера никак не влияет;
- 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;
- Не рекомендуется объединять в кластер георазпределенные ноды;
- При работе NGFW на гипервизорах используйте средства отказоустойчивости гипервизора.

- Интерфейсы для создания кластерной сети на каждом Ideco NGFW 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 сетевой порт, предназначенный для связи между нодами, подключен к изолированной IPv6 сети.
- Запрещено добавлять сетевые интерфейсы, но РАЗРЕШЕНО отключать и редактировать. Удаление сетевого интерфейса, использующегося для связи между нодами, разрушит кластер.

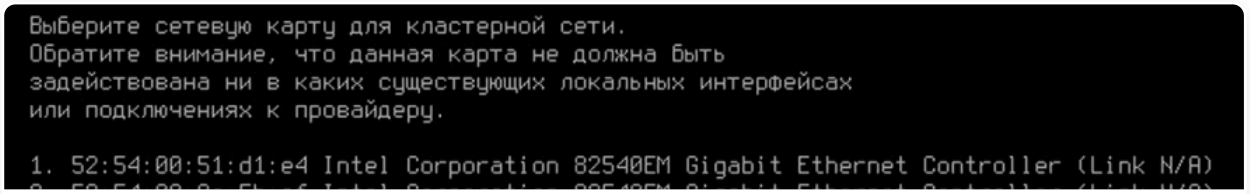
Шаг 1 - Конфигурация резервной ноды

Если только установили сервер Ideco NGFW

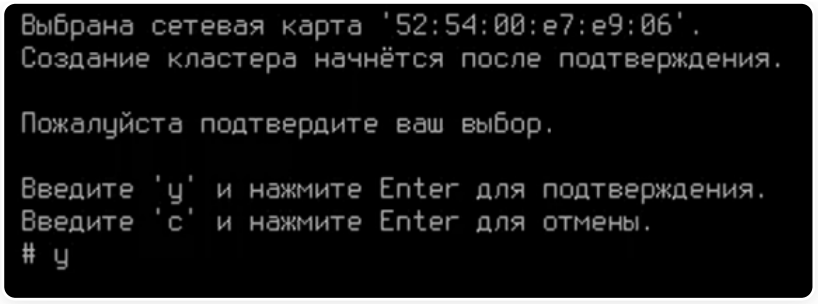
1. При входе в локальное меню резервной ноды, увидев следующее сообщение, введите **y** и нажмите **Enter**:



2. Выберите сетевой порт:

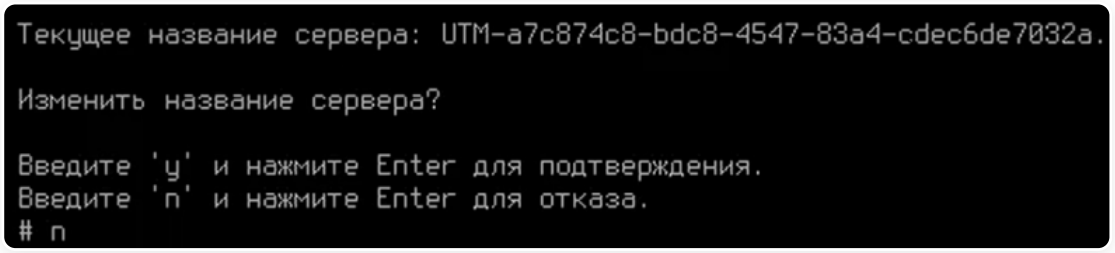


3. Подтвердите создание кластера, введя **y** и нажав **Enter**:



4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *Изменить название сервера?*, появится надпись с предложением ввести новое название.

Допустимое количество символов в названии - от 2 до 62:



После ввода нового названия нажмите **Enter** для продолжения.

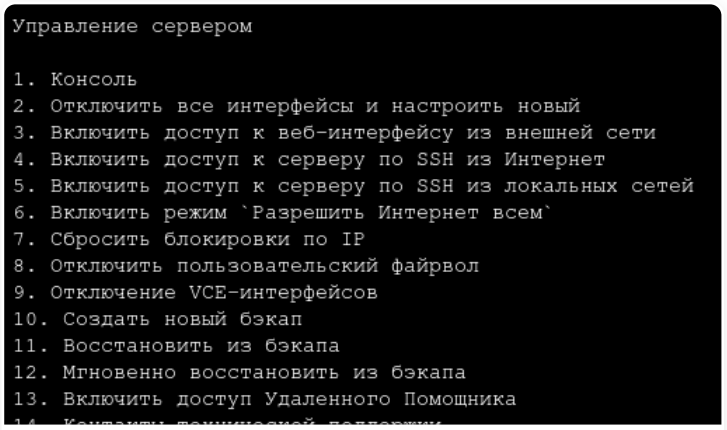
5. Появится сообщение, что процесс создания кластера запущен:

Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Если создаете резервную ноду из уже установленного сервера Ideco NGFW с лицензией и доступом в интернет

1. Перейдите в локальное меню;

2. Выберите пункт **Управление кластером**. Подтвердите создание кластера, введя **y** и нажав **Enter**:



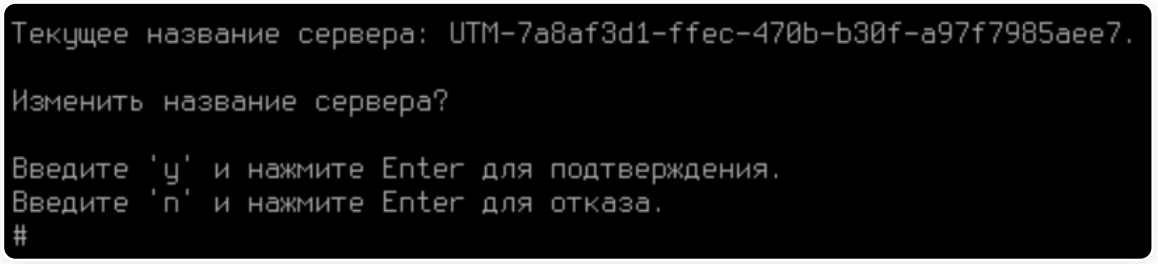
Если на ноде нет свободных сетевых портов, создание кластера будет недоступно.

Если кластер на ноде уже настроен, при выборе пункта *Управление кластером* будет доступно только его разрушение.

3. Выберите свободный физический сетевой порт для создания кластерной сети и подтвердите выбор:

4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *"Изменить название сервера?"* появится надпись с предложением ввести новое название.

Допустимое количество символов в названии - от 2 до 42:



После ввода нового названия нажмите **Enter** для продолжения.

5. Появится сообщение, что процесс создания кластера запущен:

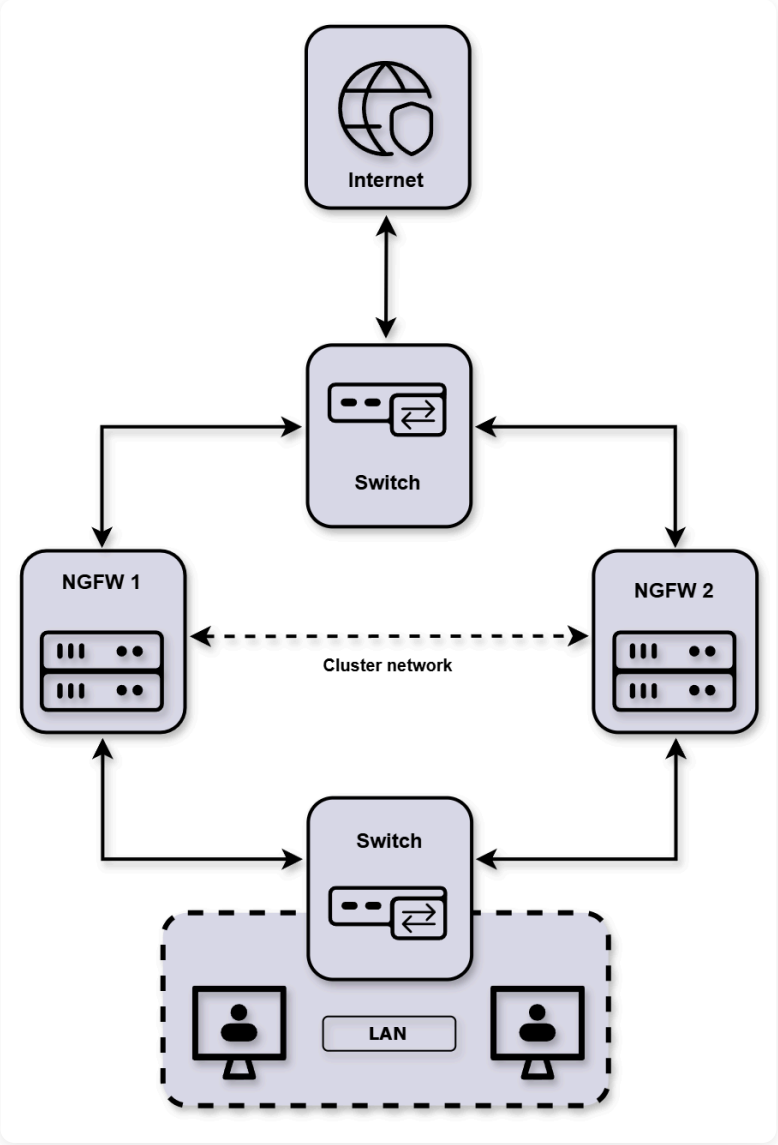
Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Шаг 2 - Конфигурация активной ноды

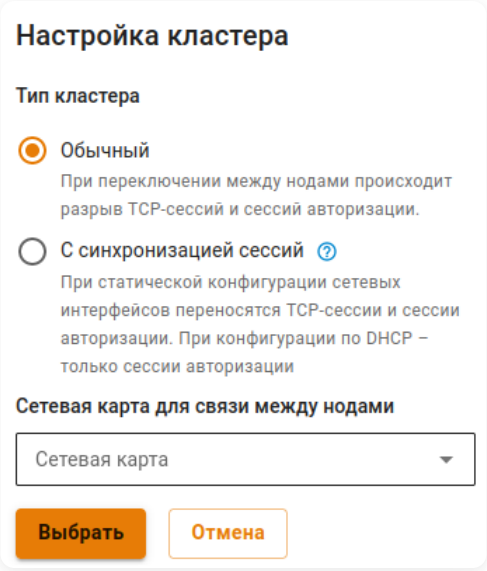
Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW выполните следующие действия:

1. Перейдите в раздел **Управление сервером** → **Кластеризация** и нажмите кнопку **Настроить кластер отказоустойчивости**.

2. Подтвердите, что топология сети соответствует схеме:



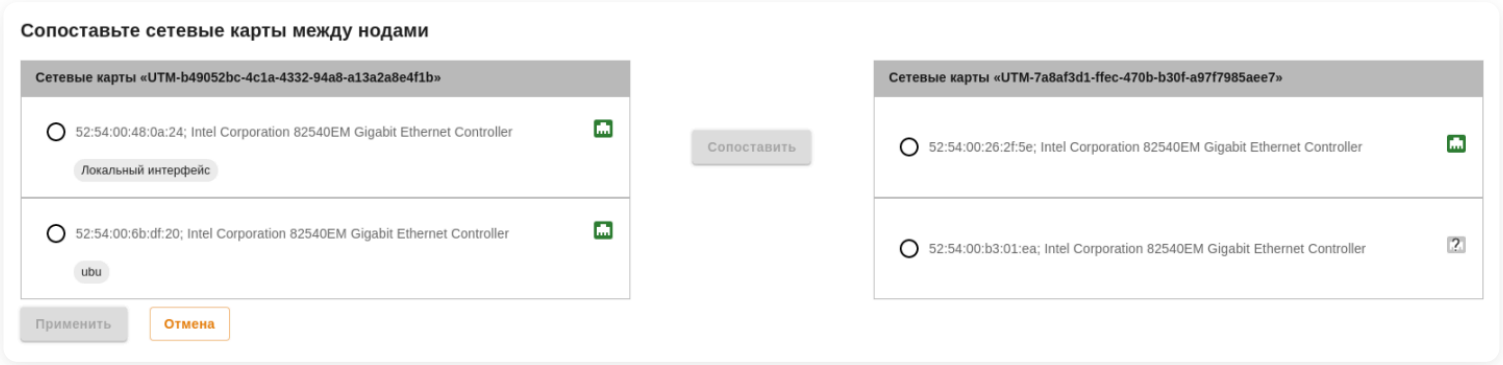
3. Выберите тип кластера и сетевой порт для соединения между нодами:



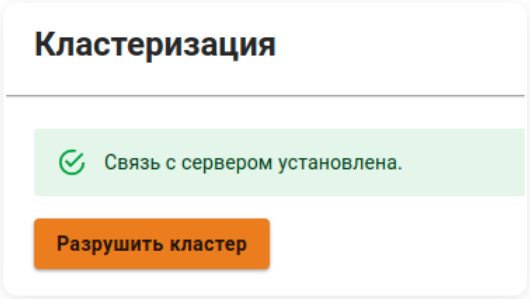
Если был настроен **Обычный** тип кластера, то при переключении между нодами происходит разрыв TCP-сессий пользователей и сессий авторизации.

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.

4. Сопоставьте сетевые порты. Для этого выберите в каждом столбце по одному сетевому порту и нажмите **Сопоставить**:



5. После применения настроек резервная нода перезагрузится, и в веб-интерфейсе активной ноды отобразится информация о том, что связь с сервером установлена.

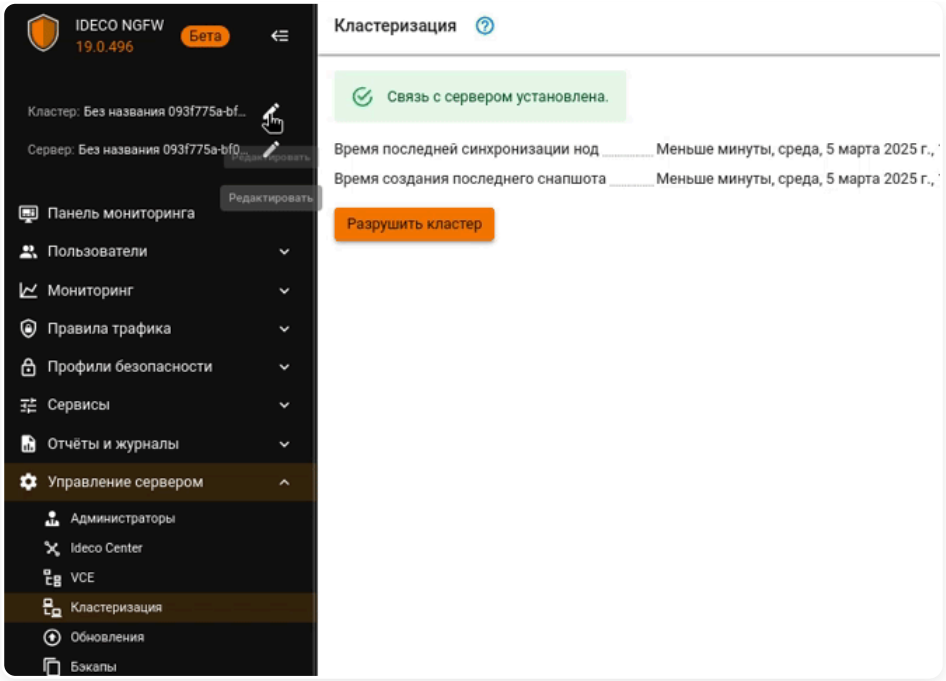


Во время перезагрузки резервной ноды в веб-интерфейсе активной ноды может временно отображаться статус о потере связи. Соединение восстановится автоматически после завершения загрузки резервной ноды.

Локальное меню резервной ноды недоступно в NGFW, начиная с версии 16.0.

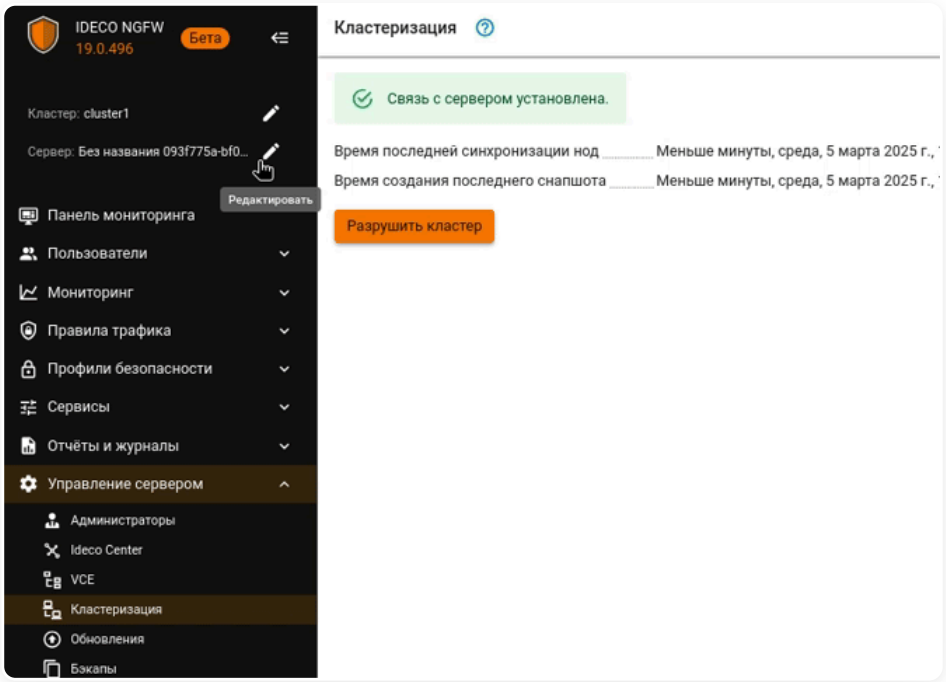
Изменение названия кластера

Изменить название кластера можно в веб-интерфейсе активной ноды, нажав на кнопку **Редактировать** рядом с названием кластера в левом верхнем углу экрана:



Изменение названия сервера

Изменить название сервера можно у активной ноды из веб-интерфейса, нажав кнопку **Редактировать** рядом с названием сервера в левом верхнем углу экрана:

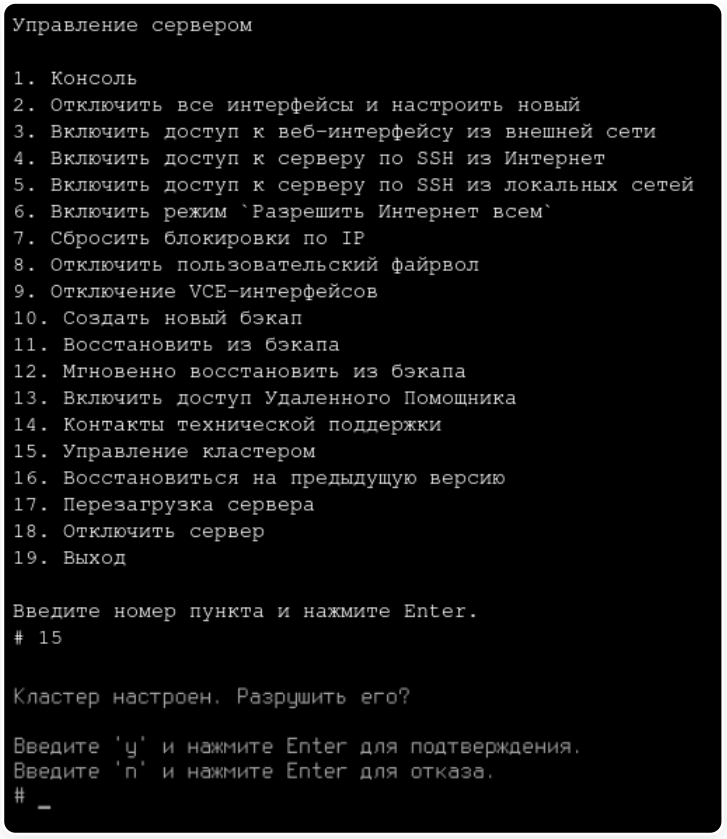


Разрушение кластера

Разрушить кластер можно только из локального меню или веб-интерфейса *активной* ноды. При этом она продолжит работать, а вторая нода (резервная) сбросит настройки до состояния только что установленного Ideco NGFW.

Разрушение кластера из локального меню:

1. Выберите пункт локального меню **Управление кластером**, введите **y** и нажмите **Enter**;

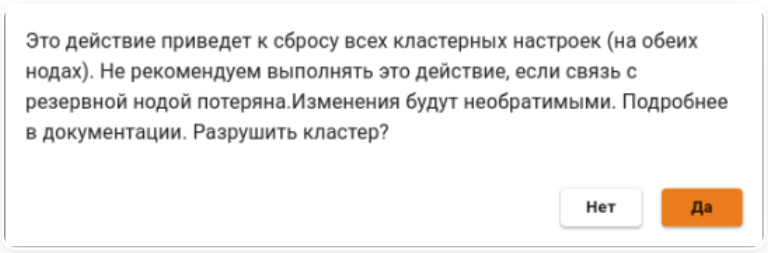


2. Подтвердите выбор.

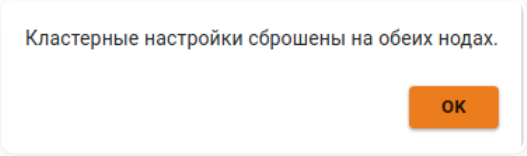
Разрушение кластера из веб-интерфейса:

1. Перейдите в раздел **Управление сервером** → **Кластеризация** и нажмите кнопку **Разрушить кластер**.

2. Появится окно с предупреждением:



3. Нажмите **ОК**:



Обновление кластера

Процесс обновления Ideco NGFW 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 разделе **Управление сервером** → **Обновление**. Сработает алгоритм обновления кластера Ideco NGFW:

- 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 она 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

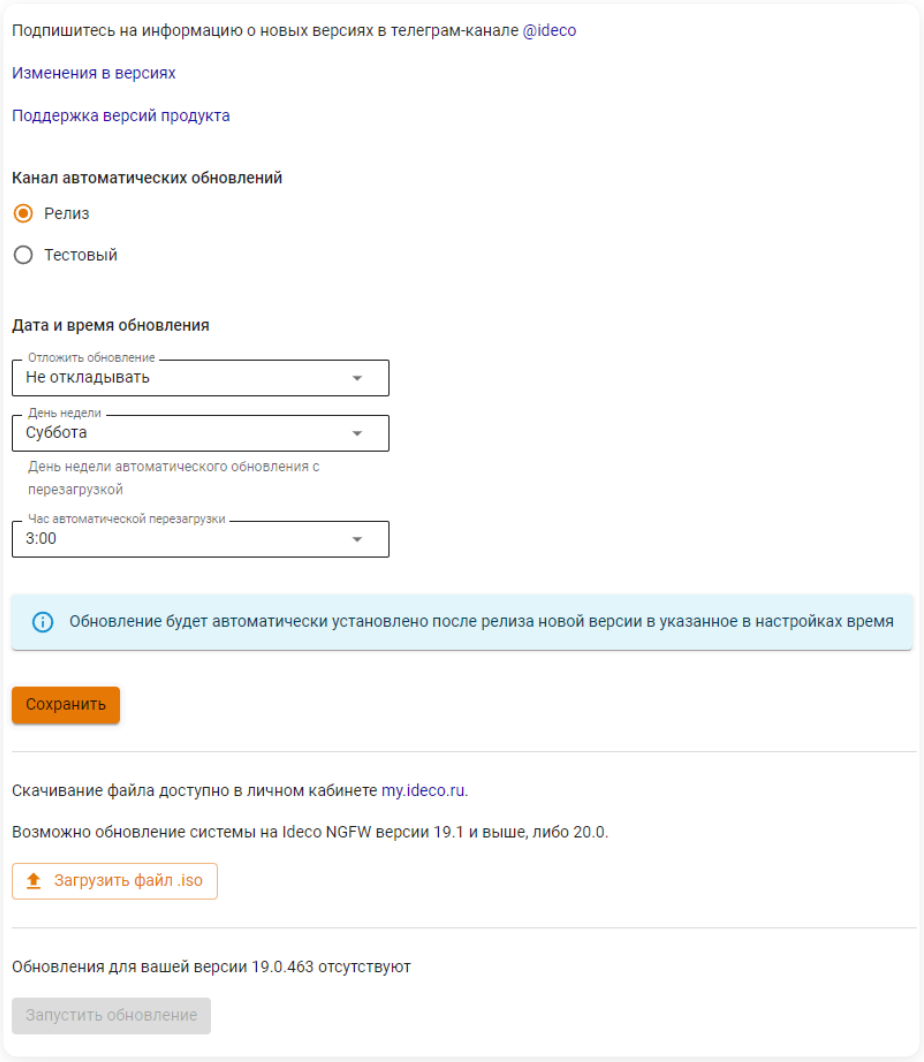
Название службы раздела **Обновления**: `ideco-sysupdate-backend`.

Список служб для других разделов доступен по ссылке.

Система

Обновить систему Ideco NGFW можно как в офлайн-режиме, так и через интернет. Отрегулировать режим обновления можно в разделе **Управление сервером → Лицензия**.

В режиме **Автоматического обновления** доступны следующие настройки:



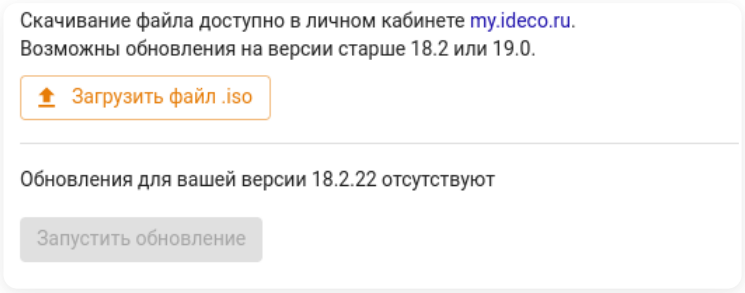
Расшифровка полей

- **Канал обновлений** - пункт **Релиз** позволяет обновляться на стабильно работающие версии. Пункт **Тестовый** позволяет быстрее обновляться как на релизные версии, так и на последние бета-версии продукта во время коротких периодов бета-тестирования новых мажорных версий. По умолчанию выбран пункт **Релиз**.
- **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.
- **Загрузить файл .iso** - позволяет обновить Ideco NGFW путем загрузки ISO-образа необходимой версии.
- **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

По умолчанию сервер обновляется по субботам в 3:00. Чтобы выполнять обновление Ideco NGFW 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.

В режиме **Ручной загрузки** обновлений необходимо скачать ISO-образ новой версии Ideco NGFW в личном кабинете MY.IDECO и загрузить его с внешнего носителя:



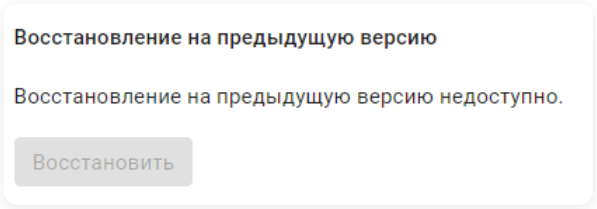
Кнопка принудительного обновления активна, когда обновление уже скачано, и только применяет его, инициировать скачивание нельзя.

После принудительного обновления потребуется полная перезагрузка сервера.

После проведения процедуры обновления новая версия будет отображаться в верхнем левом углу веб-интерфейса NGFW.

Обновить серверы Ideco NGFW, подключенные к центральной консоли, можно через Ideco Center. Для этого нужно перейти в интерфейс NGFW одним из способов, указанных в разделе Ideco Center.

Восстановление на предыдущую версию



Кнопка **Восстановить** позволяет вернуться к предыдущей версии NGFW. Система будет перезагружена, при этом текущие настройки будут потеряны. После восстановления отложите автоматическое обновление.

Если в **Ideco NGFW** настроен кластер, то в веб-интерфейсе будет отсутствовать пункт **Восстановление на предыдущую версию**.

При восстановлении на предыдущую версию данные перенесены не будут. NGFW 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 не ниже той, на которой он был создан.

Процесс выхода релизов в каналы обновлений

Тестовый канал обновлений позволяет быстрее обновляться до новых версий (релизных или бета-версий во время их активного тестирования). После выхода бета-версии NGFW в **Тестовый** канал ожидается обратная связь от пользователей по использованию новой версии продукта. Обратная связь позволяет выявить недочеты и уязвимости в продукте. После их исправления происходит выкладка в канал **Релиз**.

Если в версии NGFW, вышедшей в канал **Релиз**, в ходе использования выявляются недочеты, то они исправляются ближайшими обновлениями версии. Обновление в канале **Релиз** появляется постепенно.

Особенности обновления

NGFW

- 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 Changelog.
- Номер мажорной версии NGFW - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7).
- Автоматическое обновление Ideco NGFW до следующей мажорной версии возможно только после установки последней минорной версии, выпущенной в релиз. Например, можно обновить NGFW 17.2 до версии 17.9, а затем до версии 18.6.
- Ручное обновление Ideco NGFW до следующей мажорной версии можно выполнить с любой версии. Например, можно обновить NGFW 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 все включенные VCE автоматически обновляются вместе с корневым NGFW.
- Если в системе есть выключенные VCE, которые созданы в младшей версии корневого NGFW и не запускались после обновления, то обновление корневого NGFW на следующую мажорную версию будет заблокировано.

Пример: Если в NGFW версии 18.3 создали VCE, затем выключили его и обновили корневой NGFW 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.

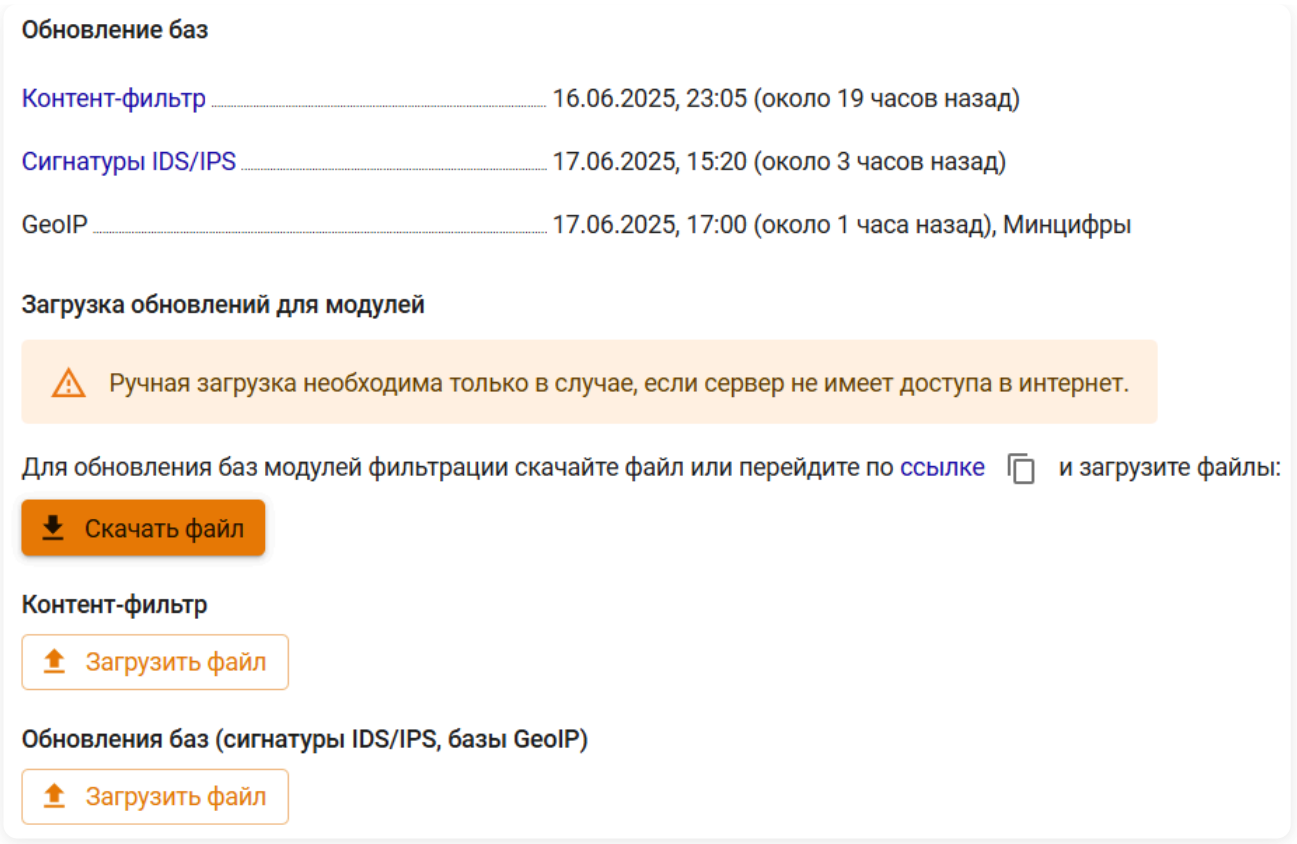
- Если VCE не включался после обновления корневого NGFW, то:
  - VCE останется на предыдущей версии.
  - Корневой NGFW можно обновить в рамках текущей мажорной версии.

  Пример: корневой NGFW 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.

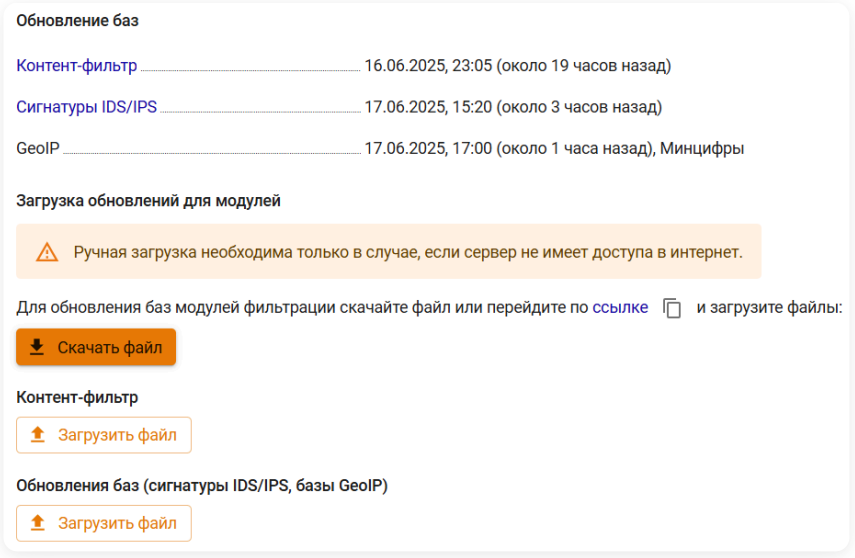
Базы фильтрации



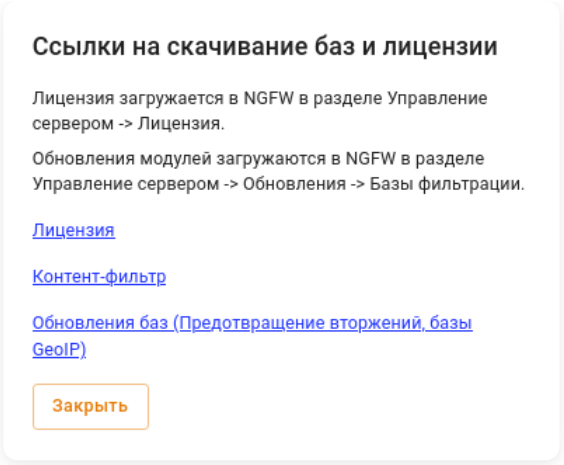
На вкладке доступны обновления баз модулей фильтрации Ideco NGFW - баз **Контент-фильтра** и модуля **Предотвращения вторжений**, а также баз соответствия подсетей и стран (GeoIP).

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 выполните действия:

1. В интерфейсе Ideco NGFW 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.

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

Полезные ссылки

- **Источники данных**

Бэкапы

Бэкап - это предварительно созданная резервная копия данных, позволяющая восстановить большинство настроек и сохраненной информации.

Название служб раздела **Бэкапы**: `ideco-backup-backend`; `ideco-backup-create`; `ideco-backup-restore`; `ideco-backup-rotate`.

Список служб для других разделов доступен по ссылке.

В NGFW создается только полный бэкап, который включают в себя 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 корневого VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте бэкап отдельно по корневому VCE и по каждому из дочерних VCE.

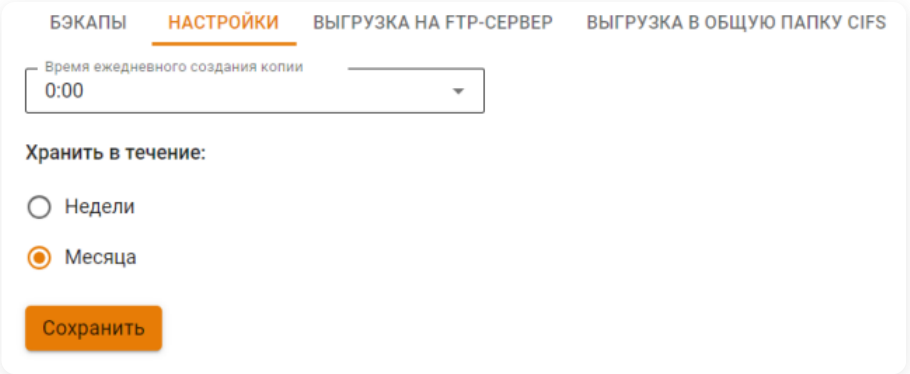
В NGFW бэкап создается как автоматически, так и вручную.

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 на контроллере домена. При каждом изменении настроек интеграции информация для аутентификации NGFW обновляется. Для решения проблемы интеграции NGFW с AD, ALD сделайте переинтеграцию NGFW с соответствующим сервисом.

Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в раздел **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** - 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 предоставляет возможность выгружать бэкапы:

- на сетевое файловое хранилище по протоколу FTP;
- на сетевое файловое хранилище по протоколу NetBIOS (CIFS);
- на 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. 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)

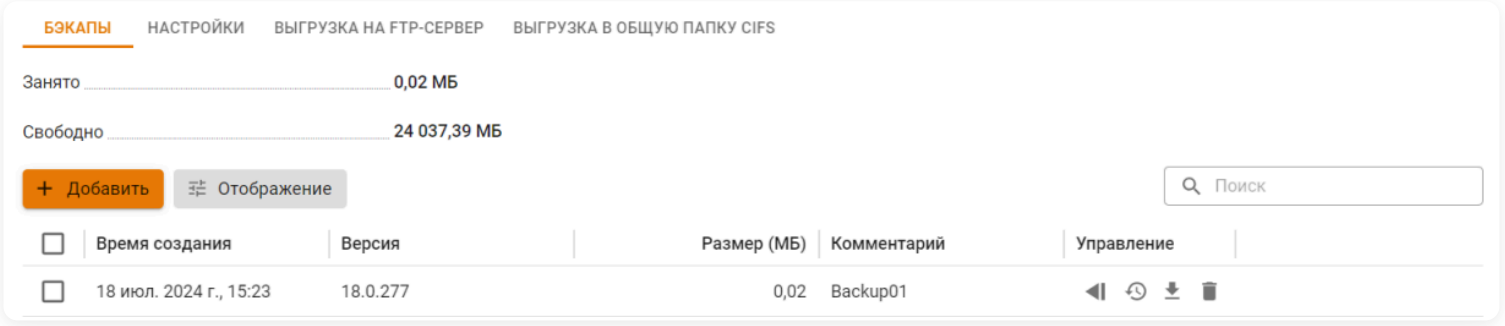
Ключевые параметры, необходимые для настройки бэкапа на NetBIOS-сервер, описаны в таблице:

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 перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и нажмите **Добавить** → **Создать**. Введите комментарий и нажмите **Добавить** или нажмите **Создать бэкап** в правом верхнем углу веб-интерфейса. Новый бэкап появится в таблице:



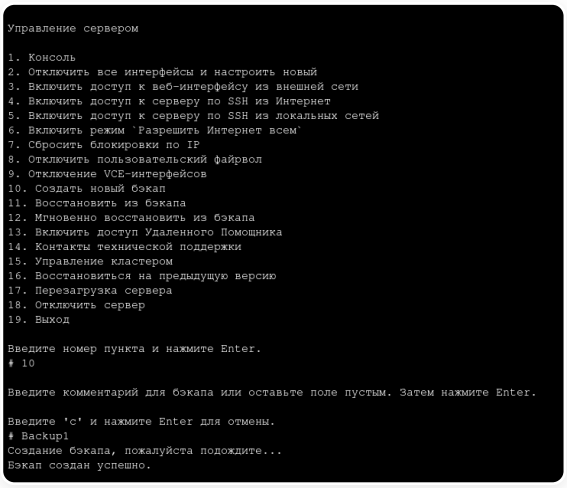
Через локальное меню

Чтобы создать новый бэкап через локальное меню Ideco NGFW, выполните действия:

1. Выберите пункт **10** 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. Выгрузка на внешние сетевые хранилища производится только при автоматическом создании бэкапа.

Восстановление конфигурации из бэкапа

В рамках одного сервера

В NGFW восстановление из бэкапа возможно полное и мгновенное.

При выполнении полного восстановления система будет перезагружена для применения настроек сервера. При мгновенном восстановлении бэкап применяется без перезагрузки.

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 автоматически отправит запрос в MY.IDECO для обновления лицензии. Если используется офлайн-лицензия, ее необходимо загрузить самостоятельно.

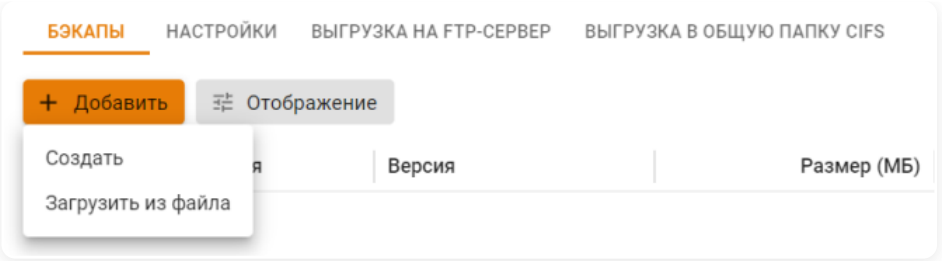
Полное восстановление конфигурации возможно только из бэкапов, версия которых не превышает версию текущей установленной системы.
Например, для Ideco NGFW версии 20 подойдут бэкапы с 19 или 20 версии. При этом важно учитывать минорные версии: например, в версии 19.13 невозможно восстановление из бэкапа, 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** → **вкладка Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

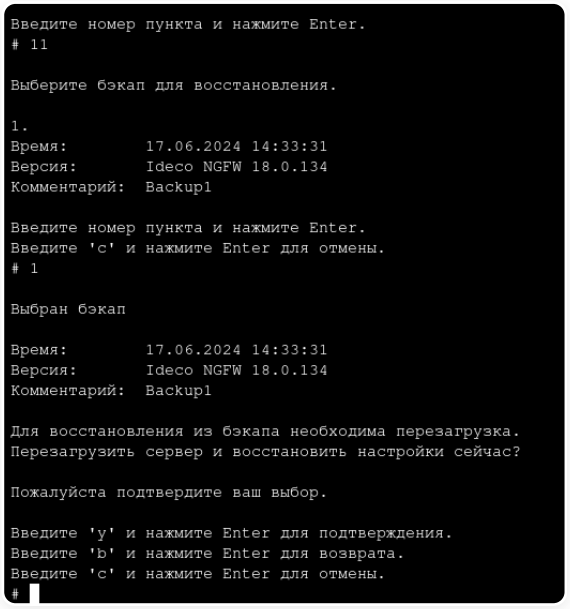
- **11** - восстановятся все настройки и перезагрузится сервер.
- **12** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

  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:



На другом сервере

Если необходимо восстановить конфигурацию из бэкапа на другом сервере, установите Ideco NGFW на новый сервер и выполните шаги по восстановлению данных:

1. На новом сервере перейдите в **Сервисы** → **Сетевые интерфейсы** и запишите MAC-адрес локальной сетевой карты, он потребуется для перенастройки локального интерфейса.

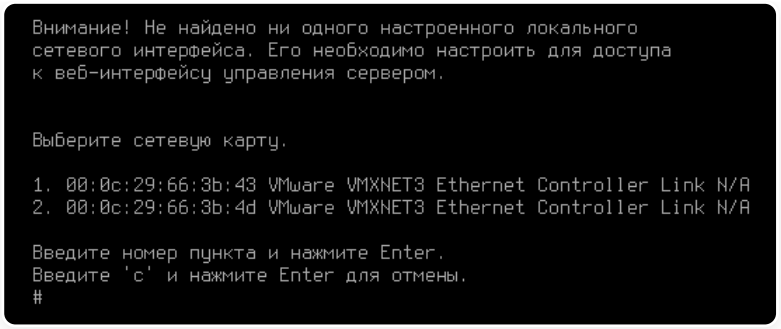
2. Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите **Добавить** → **Загрузить из файла** и выберите созданный на другом сервере бэкап.

3. Нажмите кнопку в столбце **Управление**. Система будет перезагружена для применения настроек сервера.

После перезагрузки веб-интерфейс будет недоступен, поскольку ни один локальный интерфейс не настроен.

4. Зайдите в локальное меню Ideco NGFW, введите логин и пароль.

5. Выберите сетевую карту с MAC-адресом, который записали ранее, и настройте локальный интерфейс следуя инструкции в статье Процесс установки:



После настройки локального интерфейса обязательно перезагрузите сервер, иначе восстановление пройдет некорректно.

6. Перейдите в веб-интерфейс в **Сервисы** → **Сетевые интерфейсы** и настройте интерфейсы, восстановленные из бэкапа, привязав к ним сетевые карты:

7. Проверьте корректность настроек в разделах:

- **Сервисы** → **Защита и управление DNS** - выданные подключению внешние DNS-серверы.
- **Сервисы** → **DHCP** - опции DHCP-сервера.
- **Сервисы** → **OSPF** - настройки интерфейсов.
- **Правила трафика** → **Файрвол** - зоны источника и зоны назначения в правилах.
- **Сервисы** → **Маршрутизация** → **Внешних сетей** - правила маршрутизации.

Привязка лицензии к новому серверу

Если сервер переносится из-за неисправности старого, необходимо перепривязать лицензию. Для этого:

1. Перейдите в MY.IDECO.

2. Отвяжите лицензию от неисправного сервера, нажав на .

3. Отвяжите demo-лицензию от нового сервера, нажав на .

4. Привяжите enterprise-лицензию к новому серверу, нажав **Привязать лицензию**.

При подключении к Ideco Center клон сервера, восстановленный из бэкапа, не появится в таблице серверов Ideco Center. Изменится только **Последнее подключение** в строке неисправного сервера. Это происходит из-за конфликта с донором бэкапа, если у них одинаковый cluster_id. Сервер-клон подменяет собой уже подключенный Ideco NGFW.

В случае возникновения такой проблемы 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 на физический диск.

3. Подключите второй физический диск, который будет использоваться для хранения почты.

4. В веб-интерфейсе Ideco NGFW перейдите в **Почтовый релей** → **Основные настройки**, выберите диск для хранения почты и отформатируйте его.

5. Разрешите доступ по SSH из локальных сетей в разделе **Управление сервером** → **Администраторы**.

6. Подключитесь к NGFW, 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 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.

Терминал

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`).
- **Проверка скорости интернета:** `speedtest-cli`.
- **Просмотр ARP-таблицы:** `ip neigh show`.
- **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 Файрвола:**
  - `iptables -L |grep fwd.sys.<id правила>` - для просмотра системных правил Forward.
  - `iptables -L |grep inp.sys.<id правила>` - для просмотра системных правил Input.
- **Вызов локального меню:** `ideco-local-menu --debug` - команда используется для доступа к локальному меню Ideco NGFW.

Таблица служб

Раздел	Имя службы
Файрвол	ideco-nflog;ideco-firewall-backend
Профили контроля приложений	ideco-app-backend; ideco-app-control-nfq
Контент-фильтр	ideco-content-filter-backend
Ограничение скорости	ideco-shaper-backend
Антивирус	ideco-av-backend
Предотвращение вторжений	ideco-suricata-backend; ideco-suricata; ideco-suricata-event-syncer; ideco-suricata-profiles-syncer
Объекты	ideco-alias-backend
Сетевые интерфейсы	ideco-network-backend; ideco-network-nic
Балансировка и резервирование, Маршрутизация	ideco-routing-backend
BGP, OSPF	frr; ideco-routing-backend
Прокси	ideco-proxy-backend; squid
Обратный прокси	ideco-reverse-backend
DNS	ideco-dns-backend; unbound; nsd
DDNS	ideco-dns-backend
DHCP	ideco-dnsmasq
NTP	chronyd
IPsec	ideco-ipsec-backend; strongswan
Ideco Center	ideco-central-console-backend
VCE	ideco-vce-backend
Кластеризация	ideco-cluster-backend; ideco-cluster-backup-pusher
Обновления	ideco-sysupdate-backend

Раздел	Имя службы
Бэкапы	ideco-backup-backend; ideco-backup-create; ideco-backup-restore; ideco-backup-rotate
Лицензия	ideco-license-backend
VPN-подключения	ideco-accel-l2tp; ideco-accel-pptp; ideco-accel-sstp; ideco-vpn-servers-backend; ideco-vpn-authd; ideco-vpn-dhcp-backend
Авторизация	ideco-auth-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-authd
Active Directory	ideco-ad-backend; ideco-ad-log-collector@<имя домена>
ALD Pro	ideco-ald-rest; ideco-ald-backend
Ideco Client	ideco-agent-backend; ideco-agent-websocket
Syslog	ideco-logs-backend
Обнаружение устройств	ideco-netscan-backend
Web Application Firewall	ideco-waf-backend; ideco-waf-event-syncer
IGMP Proxy	ideco-igmpproxy-backend; ideco-igmpproxy

Примеры использования утилит

Примеры использования утилиты vtysh

Просмотр таблицы маршрутизации

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в раздел **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.

Просмотр конфигурации FRR

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в раздел **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 раздел **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 раздел **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
```

Лицензия

Название службы раздела **Лицензия**: `ideco-license-backend`.

Список служб для других разделов доступен по ссылке.

В разделе **NGFW** личного кабинета 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.

Добавление коммерческой (Enterprise) лицензии

1. Скопируйте токен лицензии из письма, отправленного после покупки лицензии. Формат токена: `owhYLGvT6Xmt819JyinSxREkJfvjVO63`.

2. Перейдите в личный кабинет MY.IDECO в раздел **NGFW** → **Лицензирование** и нажмите **Добавить коммерческую лицензию**.

3. Введите токен в поле **Токен лицензии** и нажмите **Добавить**.

Токен станет недействительным, а в таблице **Свободные лицензии** отобразится купленная лицензия.

Если требуется перепривязать купленную лицензию к серверу с уже установленной тестовой лицензией, воспользуйтесь статьей.

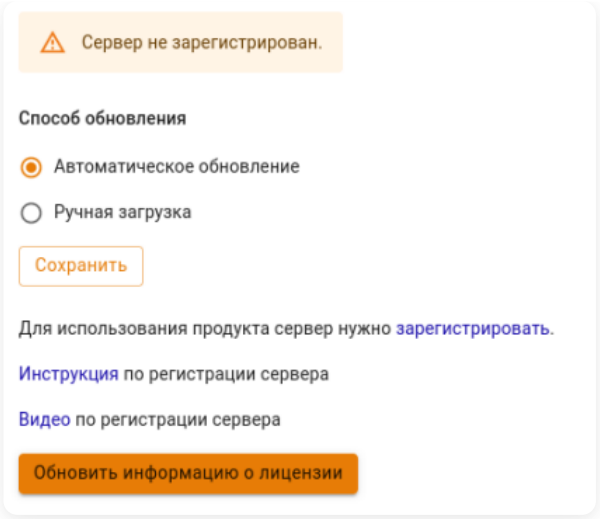
Добавление FREE (бесплатной) лицензии

Для добавления FREE-лицензии нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Свободные лицензии**.

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.

Чтобы выбрать онлайн-привязку, в веб-интерфейсе Ideco NGFW в разделе **Управление сервером** → **Лицензия** выберите способ обновления **Автоматическое обновление**, для офлайн-привязки выберите **Ручную загрузку**:



Назначьте имеющиеся коммерческие лицензии на любой зарегистрированный сервер Ideco NGFW с учетом следующих ограничений:

- Одна лицензия может быть привязана только к одному серверу.
- Демо-лицензию нельзя привязать к другому серверу.
- 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. При замене оборудования или его частей она отвязывается и требует повторной привязки. Демо-лицензия при этом теряется.

Онлайн-привязка лицензии

В MY.IDECO на вкладке **Лицензирование** нажмите **Привязать лицензию**. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения.

Офлайн-привязка лицензии

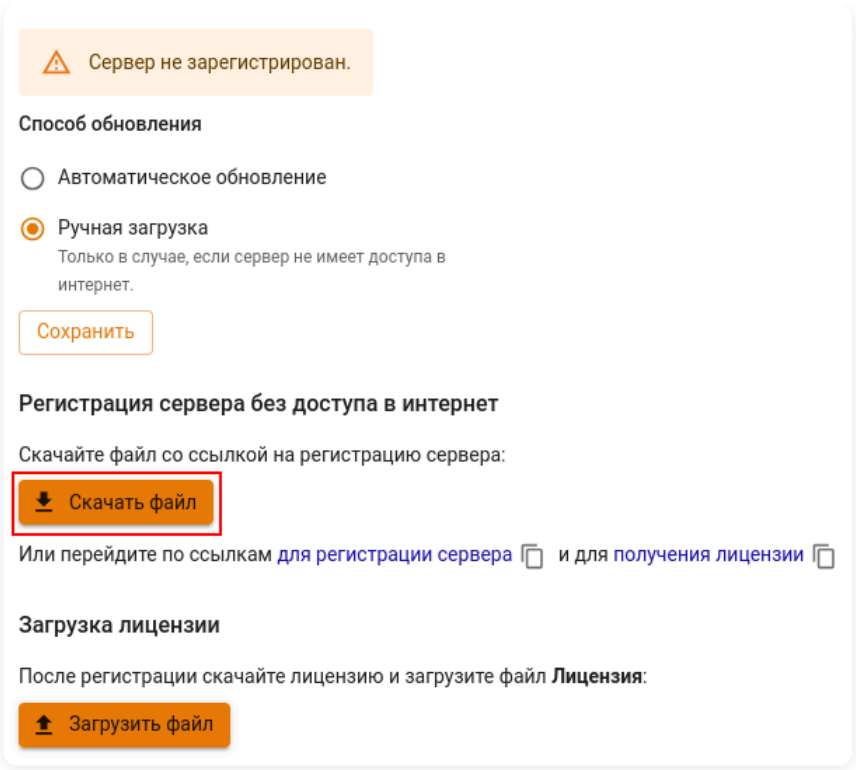
Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

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

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Это можно сделать, нажав на кнопку, или скопировать ссылку из веб-интерфейса:

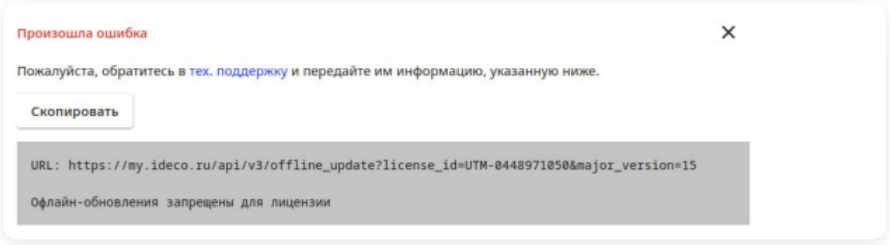


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

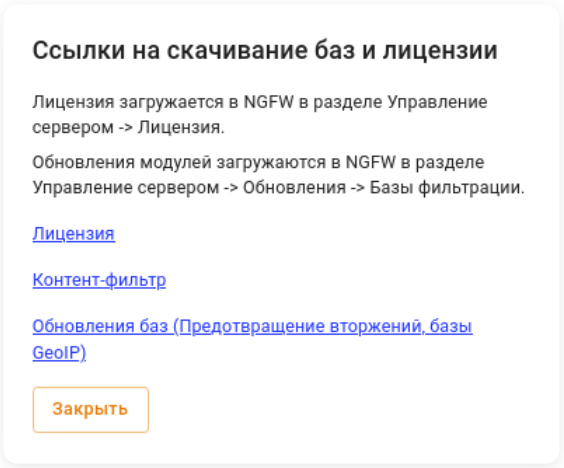
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

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:

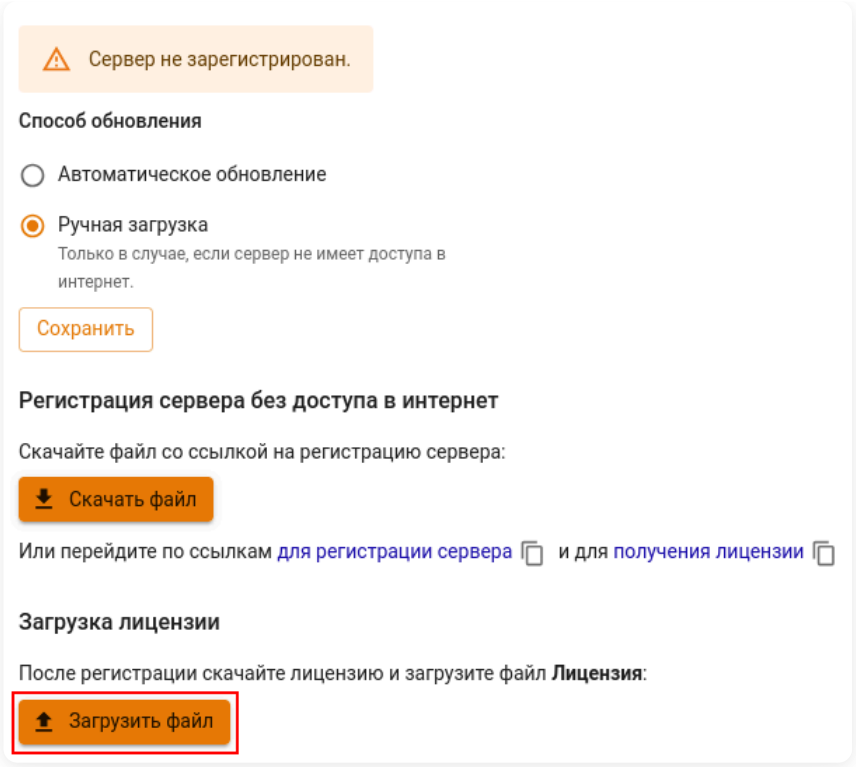


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



> 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** в веб-интерфейсе Ideco NGFW 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 личном кабинете MY.IDECO напротив нужного сервера;
- В веб-интерфейсе Ideco NGFW, в разделе **Управление сервером** → **Лицензия**.

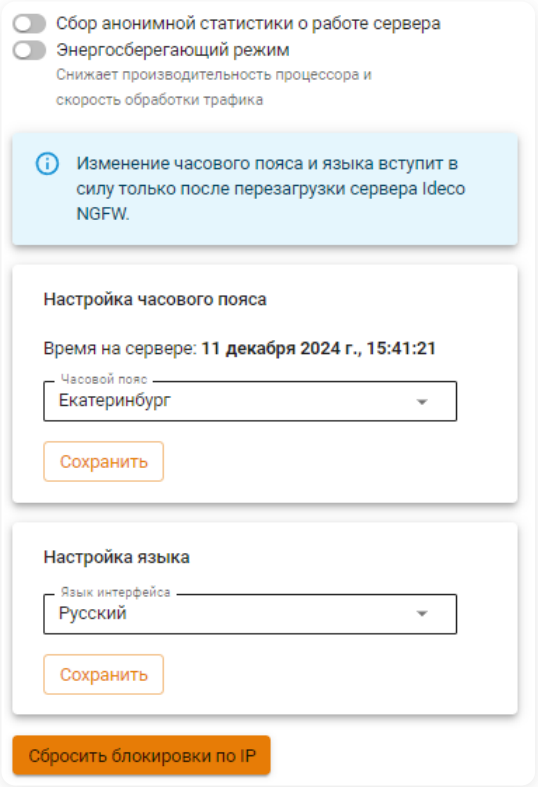
Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др.

Дополнительно

Изменение часового пояса вступит в силу только после перезагрузки сервера Ideco NGFW.

В интерфейсе VCE изменение настроек часового пояса и языка недоступно.

Настройка осуществляется через веб-интерфейс в разделе **Управление сервером** → **Дополнительно**.



- **Настройка часового пояса** - установите часовой пояс для корректного сбора логов и статистики.
- **Сбор анонимной статистики о работе сервера** - включение этого параметра разрешает серверу отправлять информацию об используемых модулях. При этом не отправляется информация о пользователях, проходящем через сервер трафике, сетевых интерфейсах и идентификаторах сервера и лицензии.
- **Энергосберегающий режим** - включение этого режима снижает производительность процессора и 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 по IP** - 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

Все возможности по фильтрации почтового трафика можно также применить к внутреннему почтовому серверу, опубликовав его 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, 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 даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

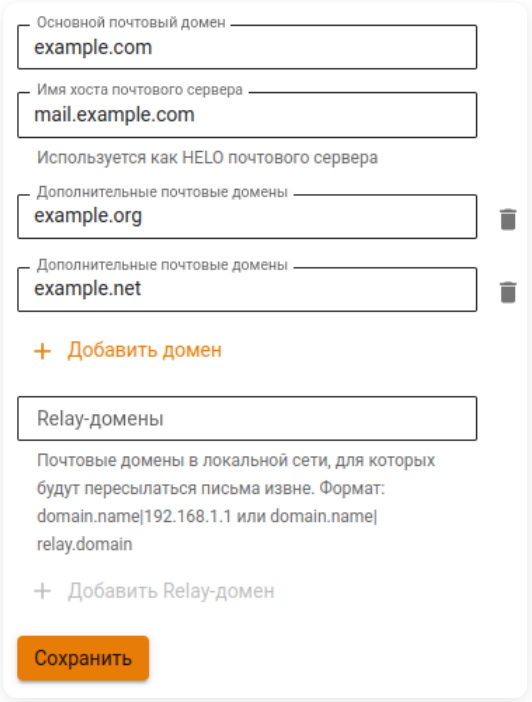
OK

Настройка почтового сервера

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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.

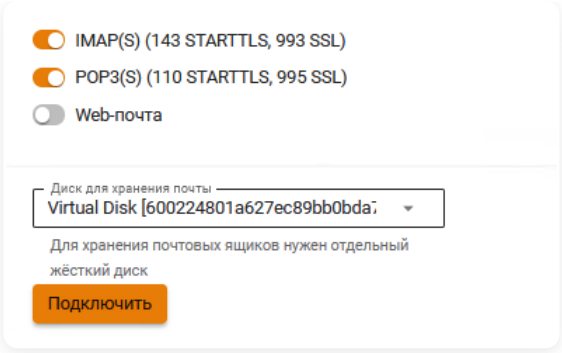
2. Включите почтовый сервер Ideco NGFW:



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, начиная с Ideco UTM версии 7.9.0. 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.

SSL-сертификат для почтового домена

После сохранения настроек почтового сервера Ideco NGFW 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 он 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 должен получить 10 баллов из 10.

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

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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.

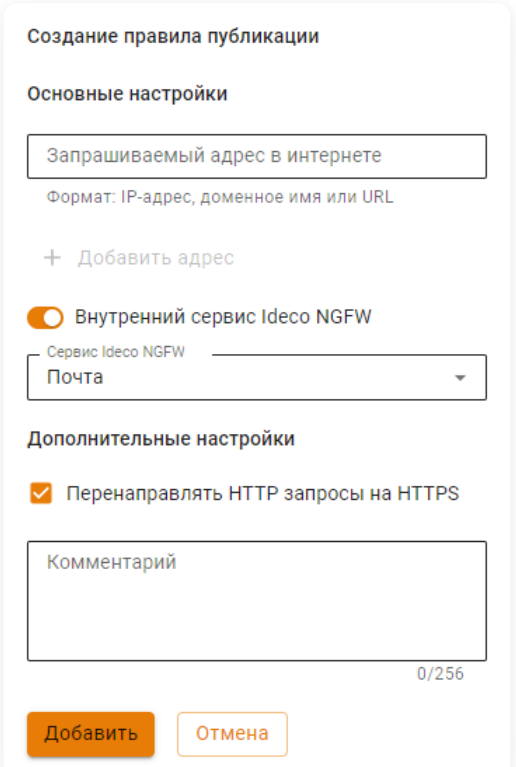
Перед настройкой веб-почты убедитесь, что на Ideco NGFW включен почтовый сервер:



Для работы веб-почты необходимо:

1. Активировать опцию **Web-почта** в **Почтовый релей** → **Основные настройки**.

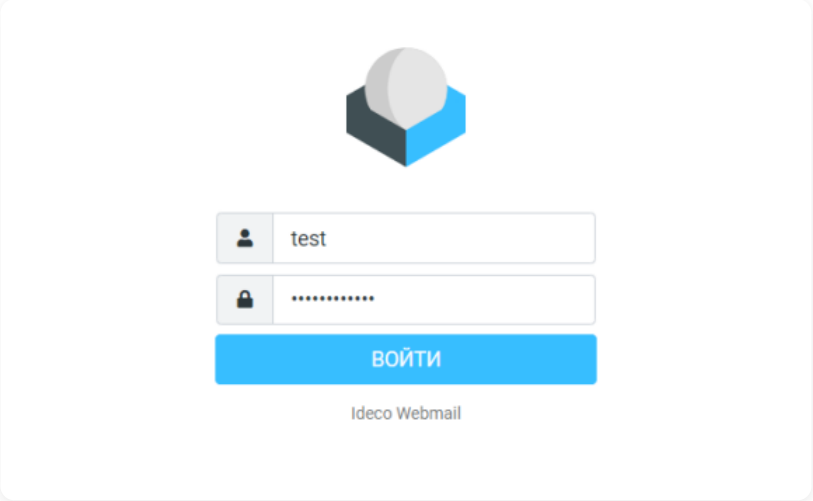
2. Создать и добавить правило публикации в **Сервисы** → **Обратный прокси**:



- 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**.
- В качестве сервиса выберите **Почта**.
- В блоке **Дополнительные настройки** включите опцию **Перенаправлять HTTP запросы на HTTPS**.

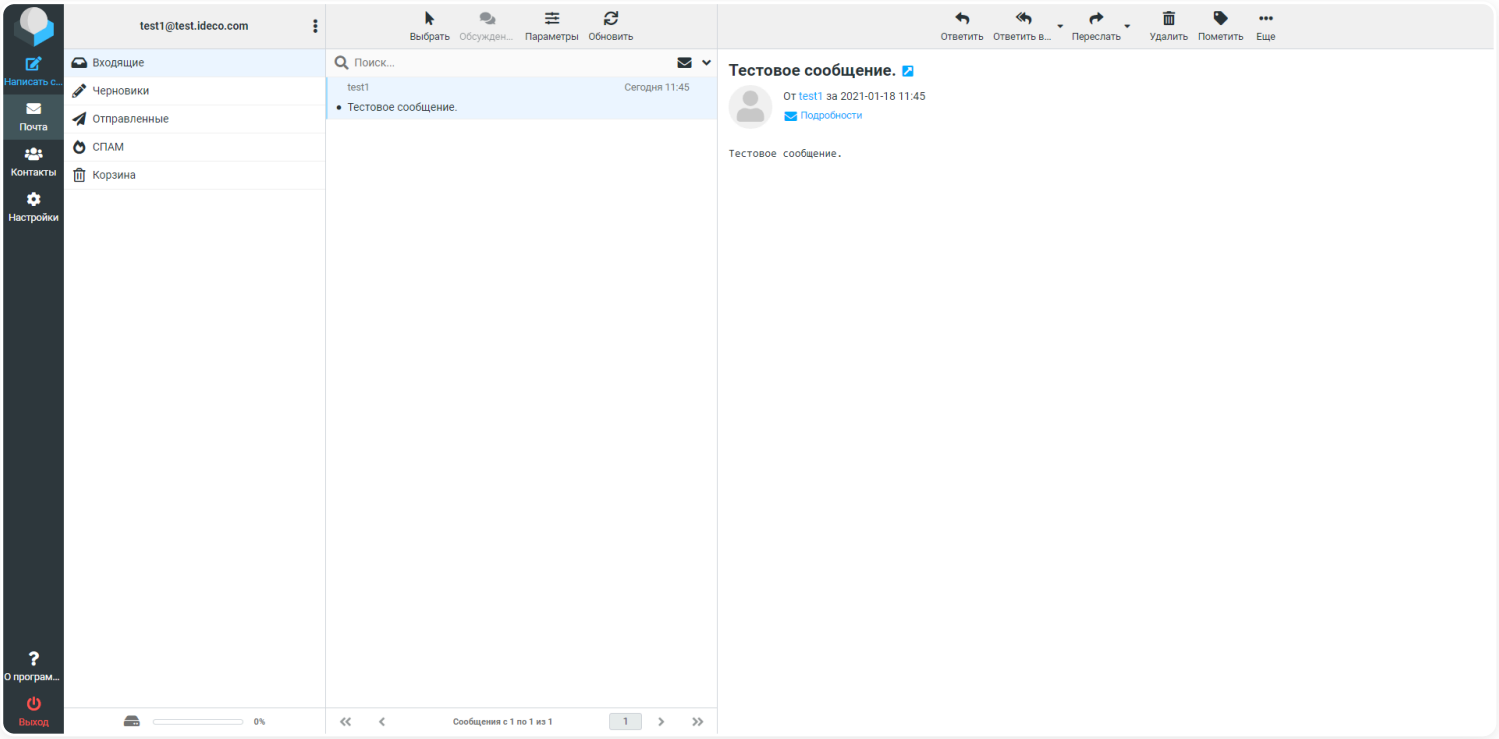
- Чтобы пользователи имели доступ к веб-почте из внешней сети, в правиле публикации в поле **Запрашиваемый адрес в интернете** укажите **белый IP-адрес или зарегистрированный домен**.
- Для подключения обязательно используйте HTTPS.
- С версии 17 Ideco NGFW веб-почта не доступна через `IP-адрес_или_домен_веб-интерфейса:8443/webmail`, 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

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Работа в режиме открытого почтового релея невозможна, поэтому Ideco NGFW 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 (A- и MX-записи в DNS-зоне).

NGFW не поддерживает кириллические почтовые домены.

Перед настройкой почтового релея убедитесь, что на Ideco NGFW включен почтовый сервер:

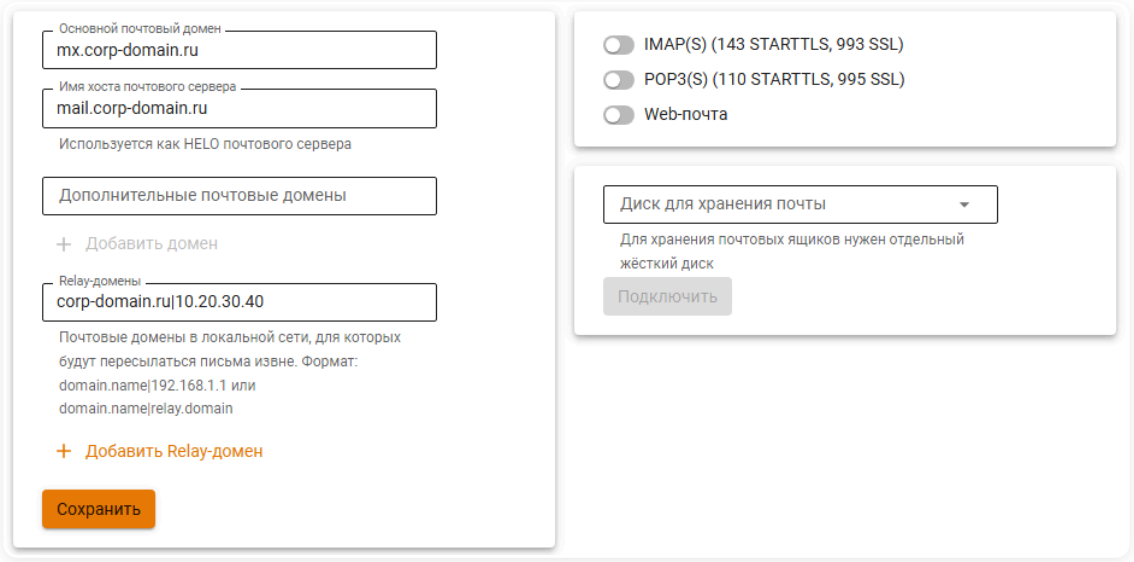


Настройка пересылки почты

Для пересылки почты с почтового сервера в локальной сети через Ideco NGFW 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 и имя хоста почтового сервера должны отличаться от Relay-доменов. Если Ideco NGFW 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`:

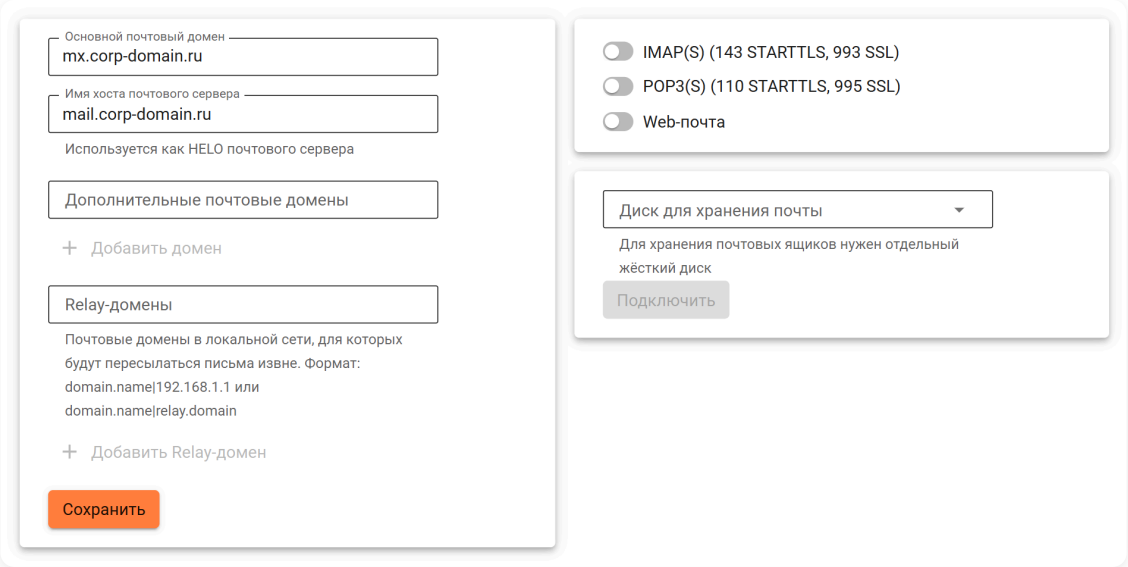
- `corp-domain.ru` - почтовый домен, зарегистрированный в интернете на публичный адрес Ideco NGFW.
- `10.20.30.40` - адрес почтового сервера в локальной сети.

3. Если требуется проверка почты на спам и вирусы, перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

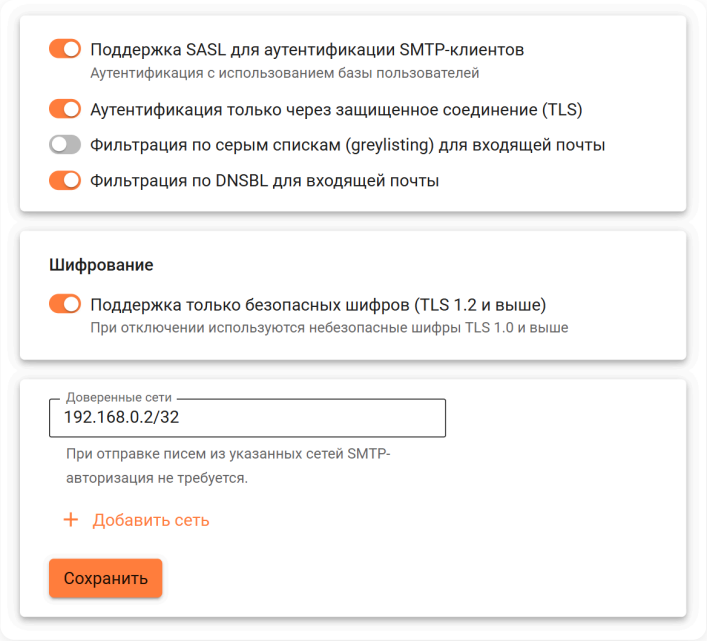
Исходящая

Для пересылки исходящей почты дополнительных настроек на стороне NGFW 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:



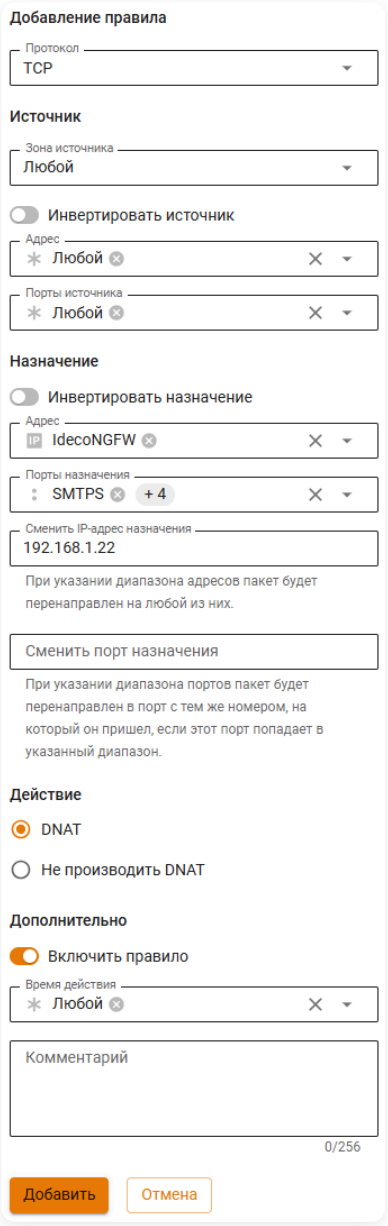
3. Перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

4. На почтовом сервере клиента в настройках отправки исходящей почты по протоколу SMTP укажите внешний IP-адрес Ideco NGFW.

Настройка доступа почтовых клиентов

Доступ из внешней сети

Для подключения почтовых клиентов из внешней сети, перейдите в **Правила трафика** → **Файрвол** → **DNAT**, создайте и включите правило проброса портов POP3(S), IMAP(S) и SMTPS:



Расшифровка полей

- **Протокол** - укажите TCP.
- **Назначение**:
  - **Адрес** - внешний IP-адрес Ideco NGFW.
  - **Порты назначения** - порты, которые использует ваш почтовый клиент (POP3, IMAP, SMTPS, 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.

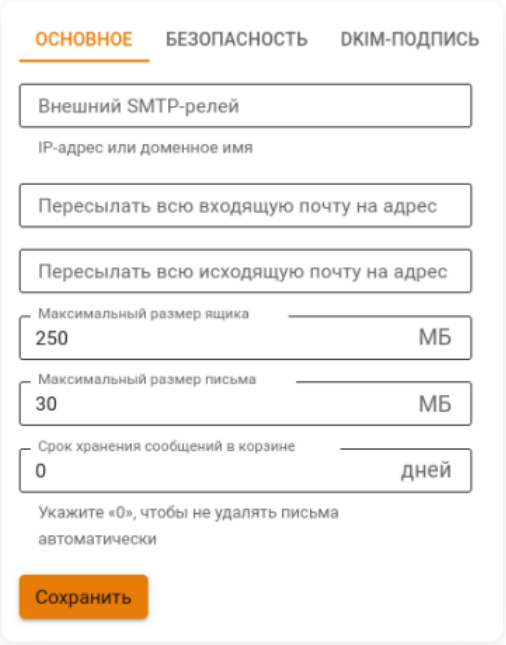
Доступ по VPN

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

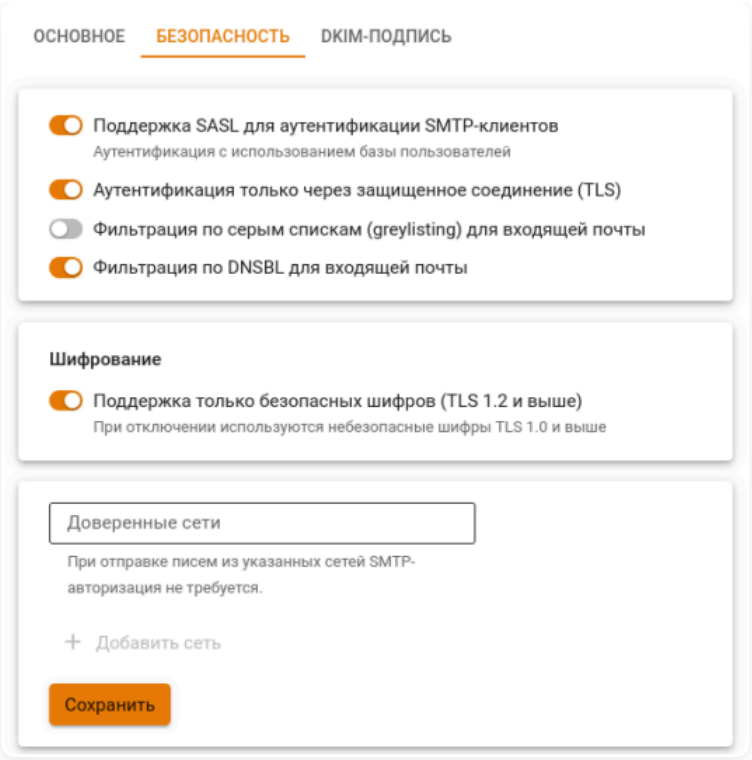
Раздел **Расширенные настройки** состоит из трех подразделов: **Основное, Безопасность, DKIM-подпись**.

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 мегабайтах (**100 ГБ - максимальное значение**).
- **Максимальный размер письма.** Ограничение на максимальный размер формируемого сервером письма в мегабайтах (**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

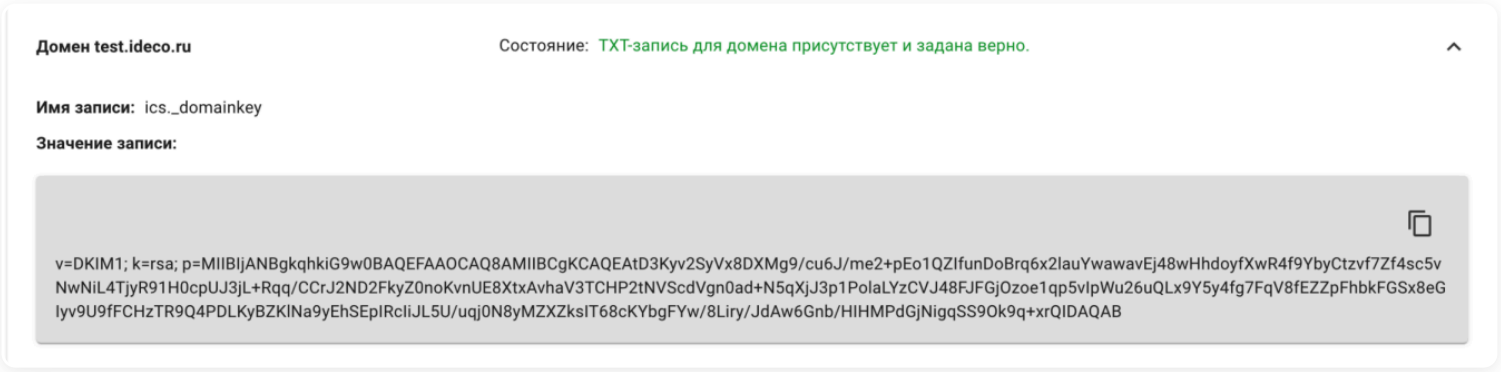


- **Поддержка SASL для аутентификации SMTP-клиентов.** Подключиться к почтовому ящику из интернета и отправить письмо, используя SMTP сервер Ideco, можно будет только, пройдя авторизацию по логину и паролю, заданному для этой учетной записи пользователя на сервере. **Не включайте этот параметр, если используете NGFW в качестве почтового релея**.
- **Разрешить аутентификацию только через защищенное соединение (TLS).** Запрещает незащищенную передачу учетных данных клиента при аутентификации на SMTP сервере.
- **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 разделе **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, и дополнительных почтовых доменов (если указаны). Сервер также проверит, правильно ли была указана запись и резолвится ли она 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 они 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 его 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. **Убедитесь, что на внешнем интерфейсе NGFW назначен публичный адрес, доступный из сети интернет.**

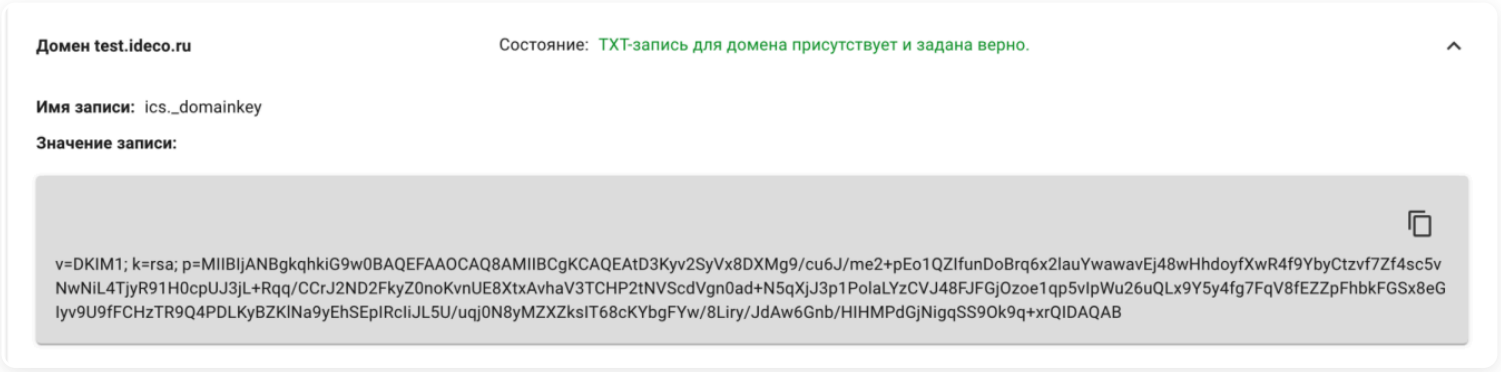
2. Добавьте ресурсную запись типа MX, указывающую на A-запись, которая была создана на предыдущем шаге. Запись типа MX указывает на сетевой узел, который занимается обработкой почтовых сообщений для домена. Она должна ссылаться на доменное имя почтового сервера, а не на IP-адрес.

Рекомендуем:

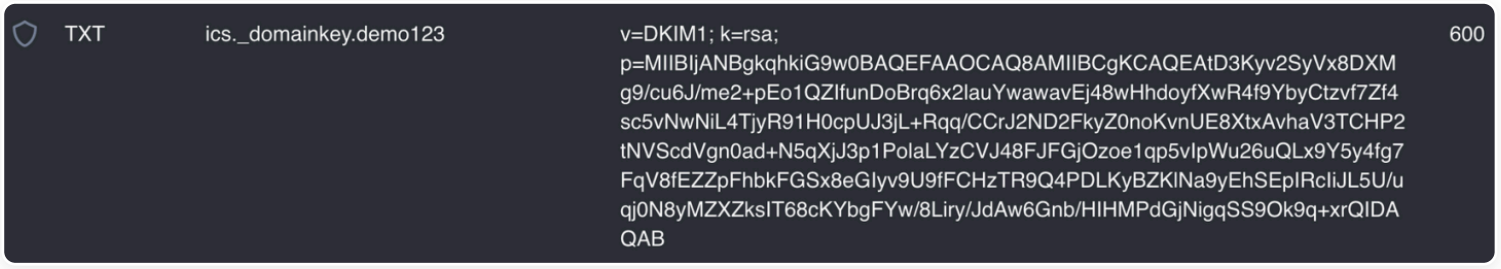
3. Добавить обратную ресурсную запись типа PTR. Эта запись должна быть прописана в файле обратной зоны. Эти изменения должны быть сделаны на стороне интернет-провайдера. Обратитесь к нему с просьбой прописать обратную ресурсную запись для IP-адреса, которая должна ссылаться на запись типа MX.

4. Настроить SPF-запись для почтового сервера.

5. После настройки почтового сервера настроить также DKIM-подпись почтовых сообщений. Для этого перейдите в раздел **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 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.
- MX-запись вида: `example.net. MX 10 mail.example.net`.
- Обратитесь на свой 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 в себя 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.

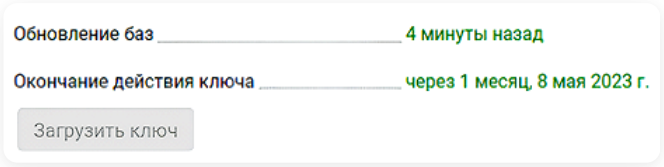
Антиспам и антивирус

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Раздел **Антиспам и антивирус** состоит из вкладок: **Основное** и **Настройки фильтрации**.

Основное



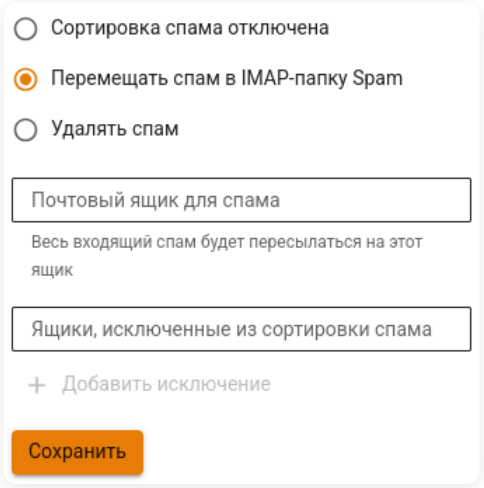
Позволяет управлять работой службы антиспама и антивируса почтового сервера на базе Kaspersky Security for Linux Mail Server с функцией машинного обучения и искусственного интеллекта. Также на вкладке предоставлена возможность добавления лицензионного ключа антиспама. Ключ поставляется в файле, имеющем 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 в **Правила** → **Разрешенные адреса**. Адреса, добавленные на вкладке **Запрещенные адреса**, обрабатываются только NGFW.

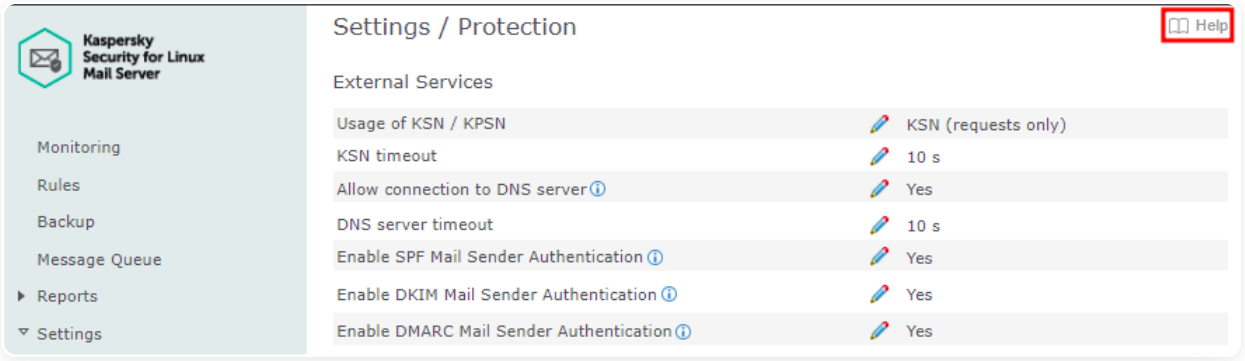
Веб-интерфейс для Антиспама

> 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**:



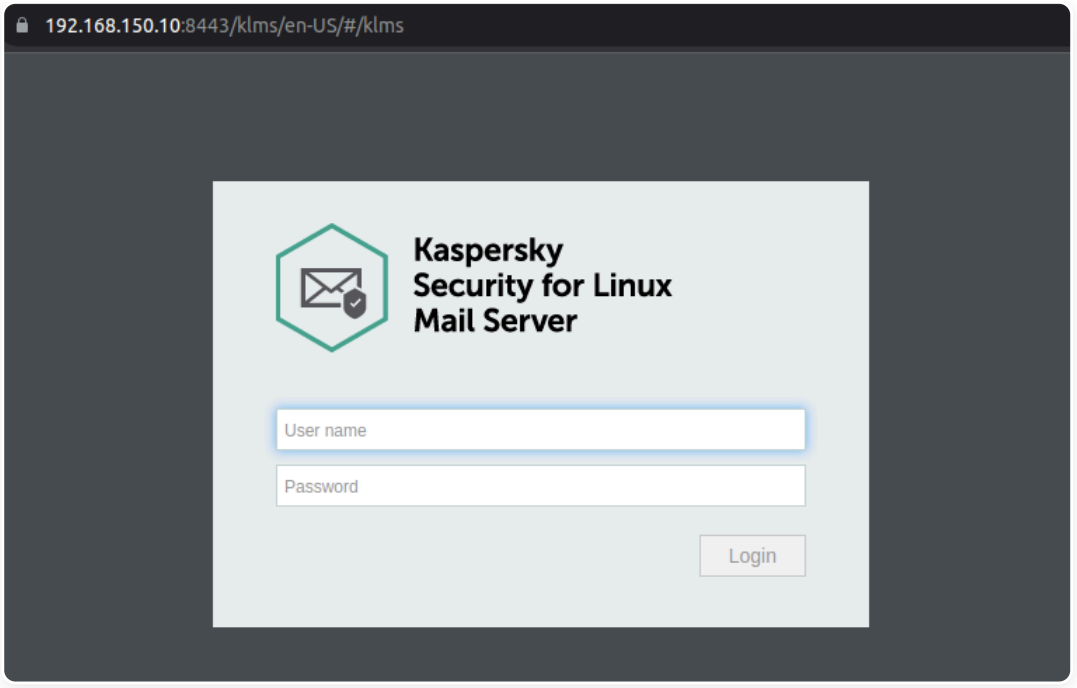
Чтобы включить веб-интерфейс для Антиспама:

1. Перейдите в раздел **Управление сервером** → **Терминал** и выполните команду `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`

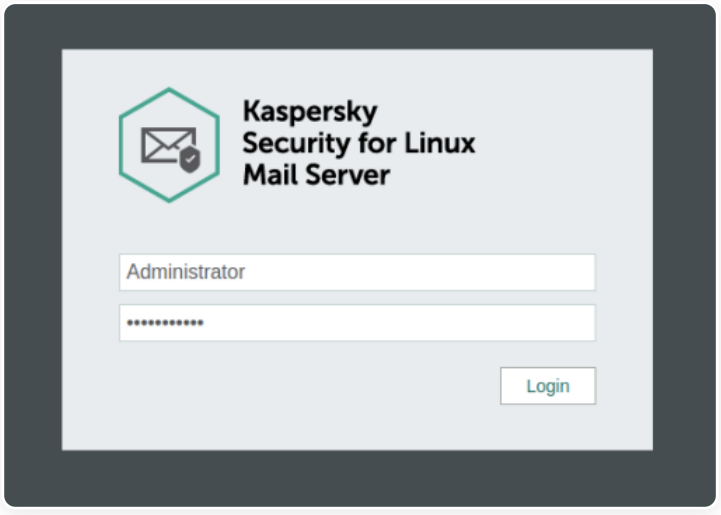
2. Задайте пароль для стандартного аккаунта **Administrator**, состоящий минимум из 8 символов: строчных букв, заглавных букв, специальных символов, чисел.

```
[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 ~]#
```

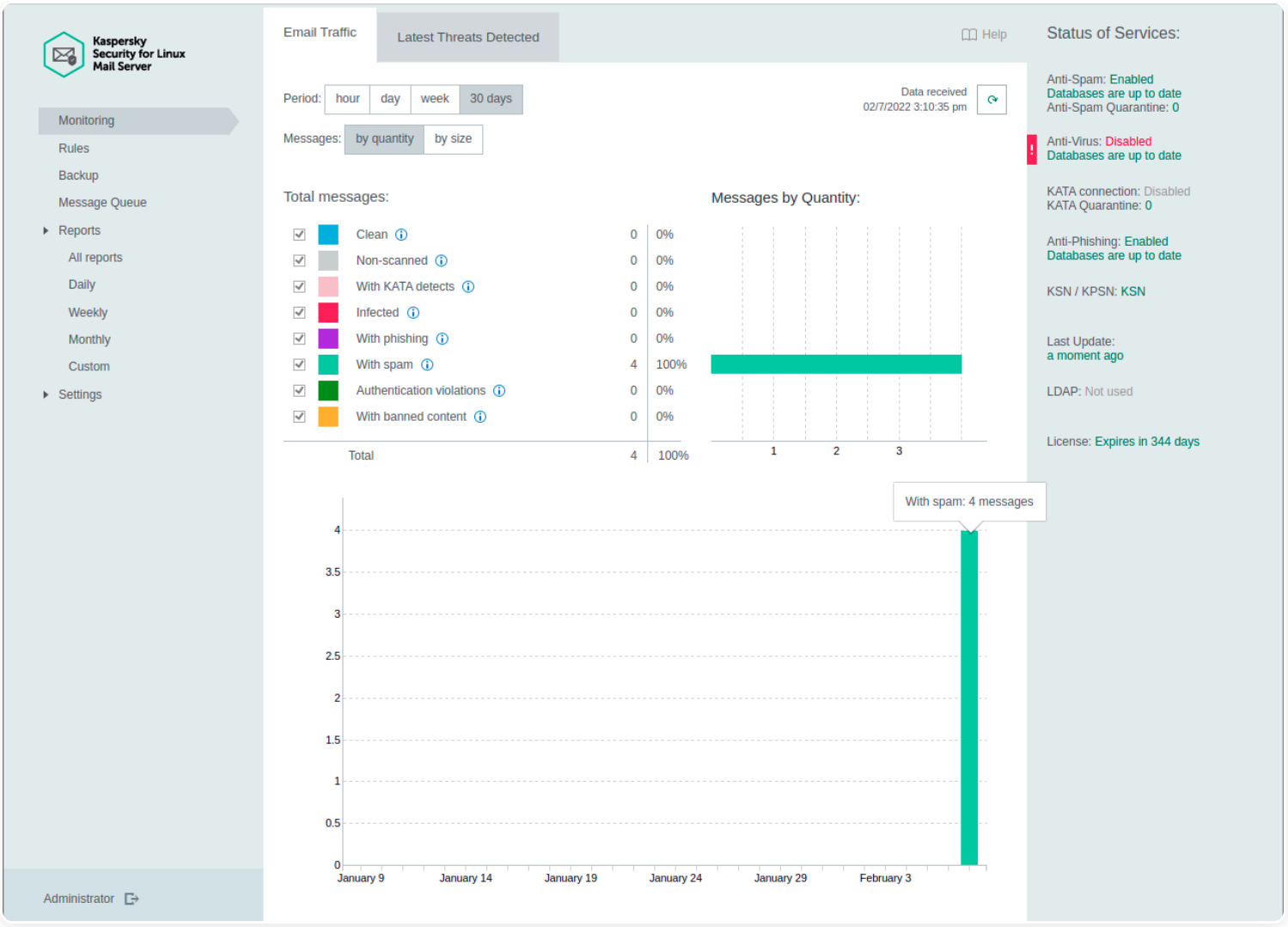
3. Перейдите в адресной строке по пути `ngfw_ip_address:8443/klms/` чтобы получить доступ к веб-интерфейсу:



4. Войдите в веб-интерфейс с учетной записью **Administrator** и ранее заданным в терминале паролем:



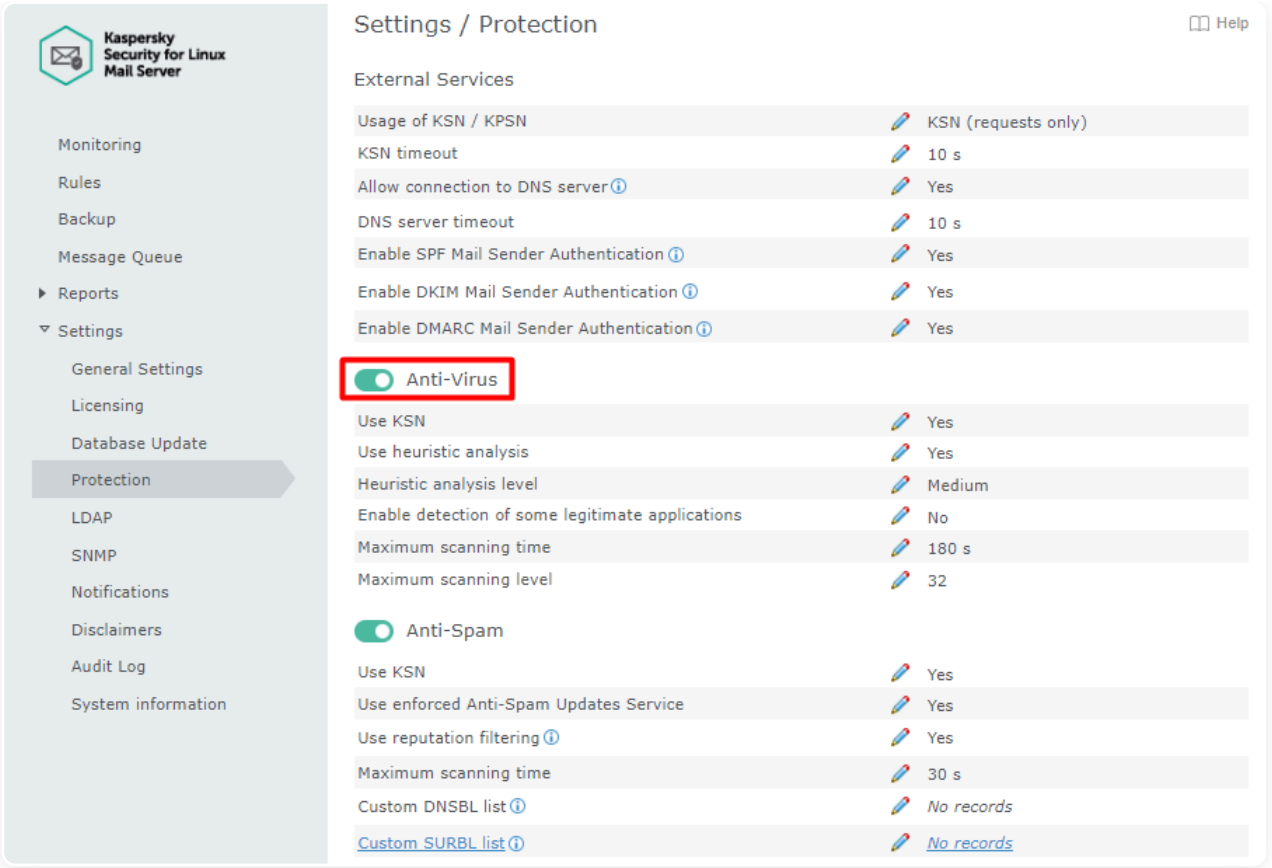
После успешного входа будет отображен дашборд со статистикой работы Антиспама:



Включение Антивируса почтового сервера

1. Перейдите в веб-интерфейс Антиспама.

2. Включите антивирус почтового сервера, перейдите в раздел **Settings** → **Protection** и активируйте опцию **Anti-Virus**:



Службы антиспама и антивируса почтового сервера преднастроены для оптимальной работы в составе Ideco NGFW. Не рекомендуем вносить какие-либо изменения в раздел **Settings**. Веб-интерфейс решения Kaspersky Security for Linux Mail Server предусмотрен только для работы с отчётностью и для внесения изменений, описанных в этой статье.

Правила

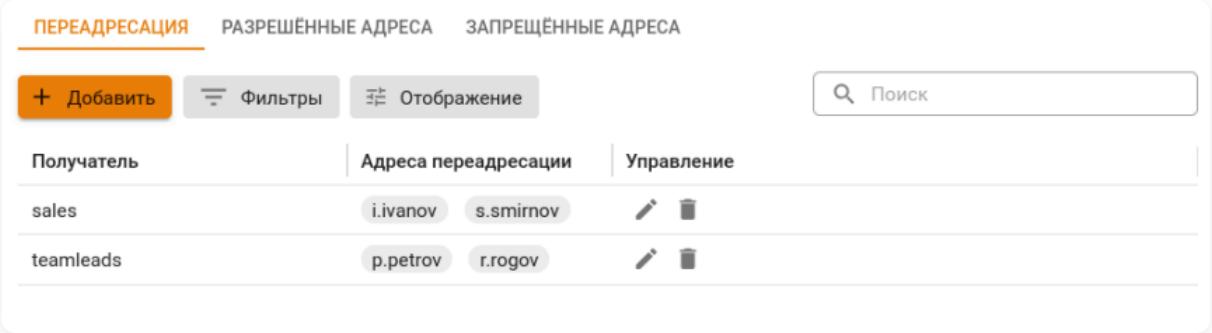
Раздел **Правила** состоит из трех вкладок: **Переадресация, Разрешенные адреса, Запрещенные адреса**. На каждой вкладке доступна фильтрация по кнопке **Фильтры**.

Переадресация

Позволяет настроить переадресацию почты на сервере с помощью почтовых алиасов.

Алиасы, в отличие от почтовых ящиков, не требуют логинов и паролей, они закрепляются за ящиком и служат его копией 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.

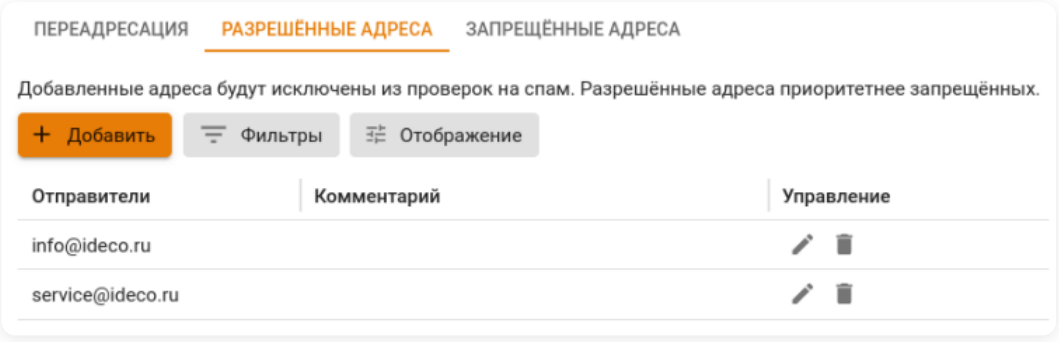
Подробнее с документацией по настройке почтовых алиасов на Ideco NGFW ознакомьтесь в статье Переадресация почты.



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 он 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.

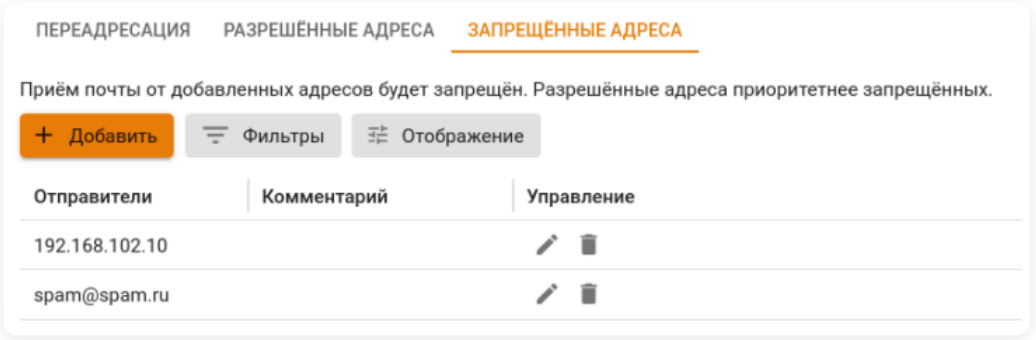
Еще один пример: в **Разрешенные адреса** внесен домен, в **Запрещенные адреса** - ящик из этого домена. Тогда письма с ящика будут заблокированы.

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.



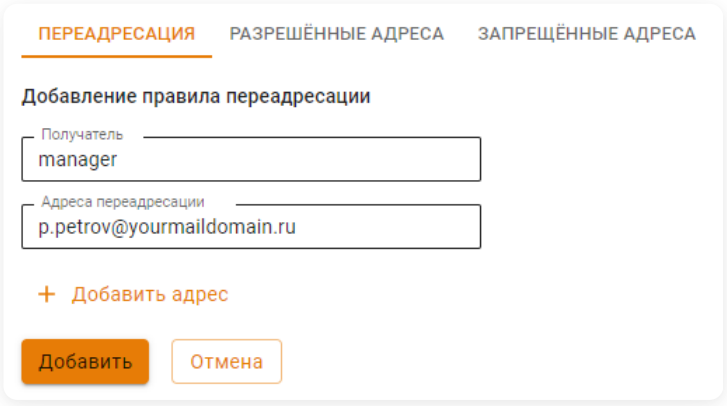
Переадресация почты

Чтобы создавать и редактировать почтовые правила переадресации (алиасы), перейдите в раздел **Почтовый релей** → **Правила** → **Переадресация**.

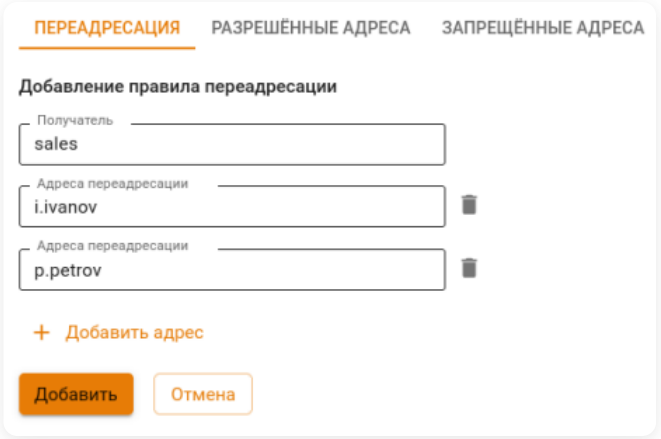
Почтовые алиасы отличаются от почтовых ящиков тем, что не требуют логинов и паролей. Они закрепляются за ящиком и служат его копией с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, можно сказать что алиас - это группа почтовых ящиков или группа рассылки. Поступающая на алиас 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. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в поле **Получатель**, должен реально существовать.

Примеры:

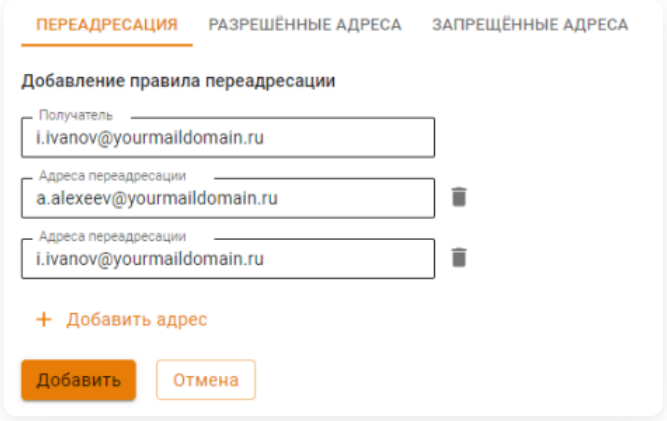
- Создать алиас `manager@yourdomain.ru` для ящика менеджера компании для связи с клиентами и партнерами, у которого реальный почтовый ящик имеет имя `p.petrov@yourmaildomain.ru`:



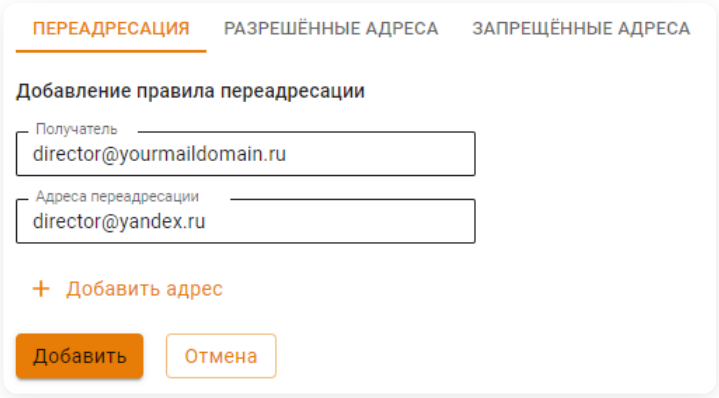
- Создать корпоративный алиас для отдела продаж `sales@yourmaildomail.ru`, чтобы почта пересылалась на всех сотрудников этого отдела:



- Создать временный алиас для переадресации почты сотрудника, который находится в отпуске `i.ivanov@yourmaildomail.ru`, на ящик его 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.

Почтовая очередь

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 оно будет удалено из почтовой очереди и не будет доставлено получателю.

При обновлении Ideco NGFW 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 должен получить 10 баллов из 10.

Публикация ресурсов

Доступ из внешних сетей без NAT

Перейти >

Настройка публичного IP-адреса на компьютере в локальной сети

Перейти >

Портмаппинг (проброс портов, DNAT)

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

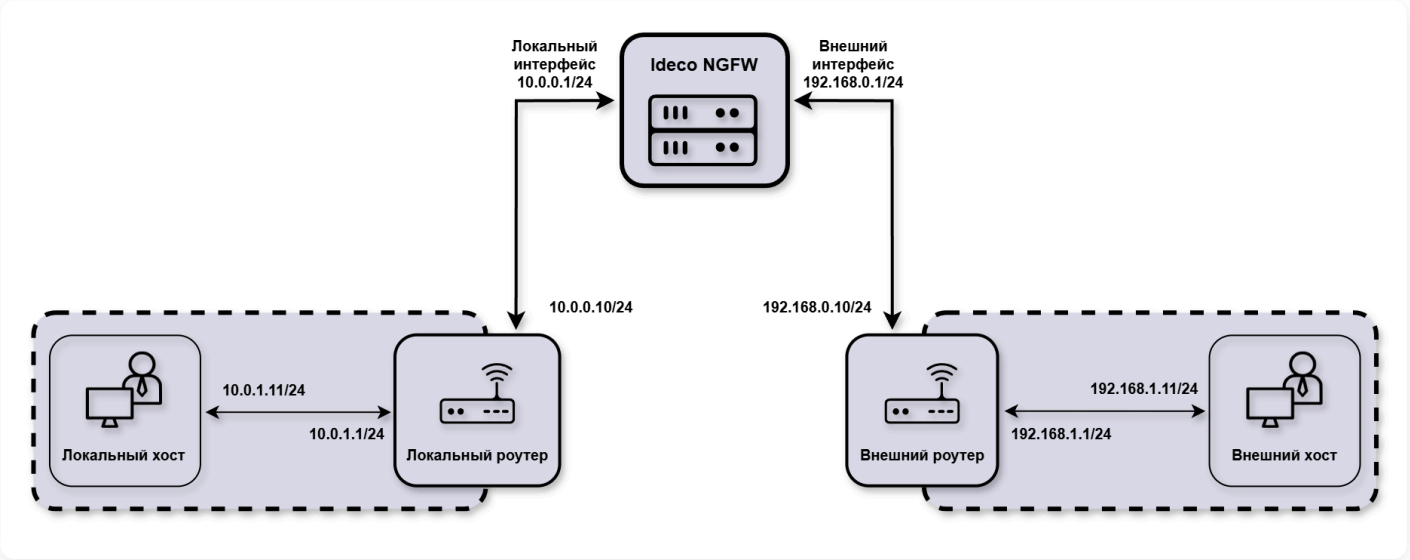
OK

Доступ из внешних сетей без NAT

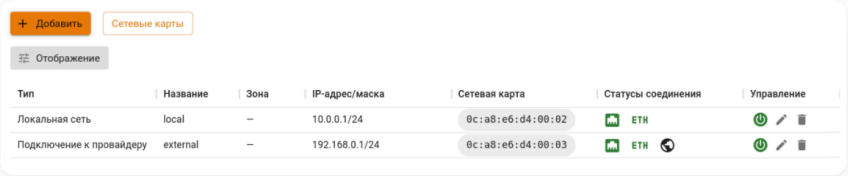
При необходимости (как правило, когда Ideco NGFW расположен внутри локальной сети, а не на границе с интернетом) возможно:

- Организовать прямой доступ к ресурсам внешних по отношению к Ideco NGFW сетей без использования NAT.
- Разрешить доступ из внешних относительно Ideco NGFW сетей в локальную сеть с прямым обращением к локальным IP-адресам.

Для примера разберем настройку Ideco NGFW для доступа без NAT в следующей конфигурации сети:



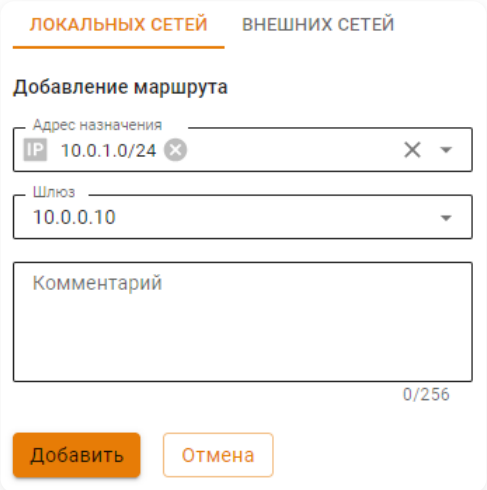
1. Настройте сетевые интерфейсы в разделе **Сервисы** → **Сетевые интерфейсы** на Ideco NGFW:



- **local** - интерфейс для доступа в пользовательскую локальную сеть.
- **external** - интерфейс для доступа в пользовательскую внешнюю сеть пользователей.

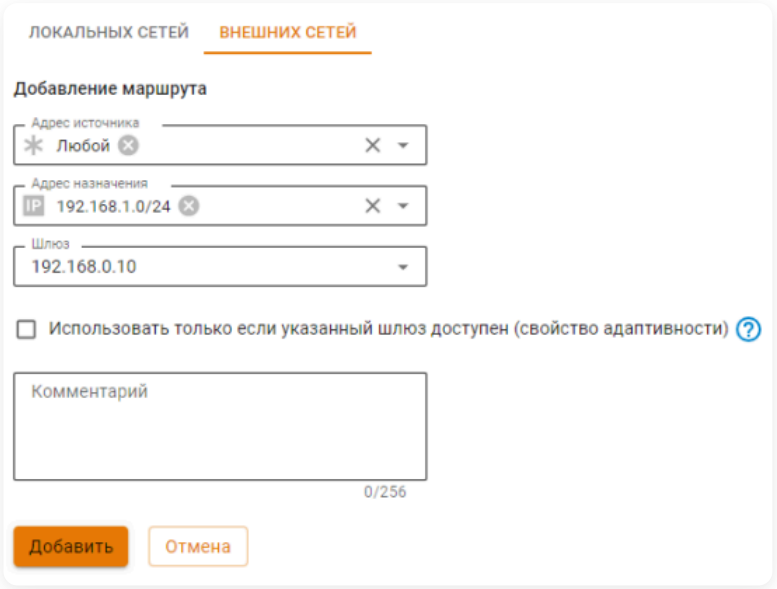
2. Перейдите в раздел **Сервисы** → **Маршрутизация** и создайте правила для доступа к IP-адресам пользователей, которые находятся за маршрутизаторами:

- Для **Локальных сетей**:



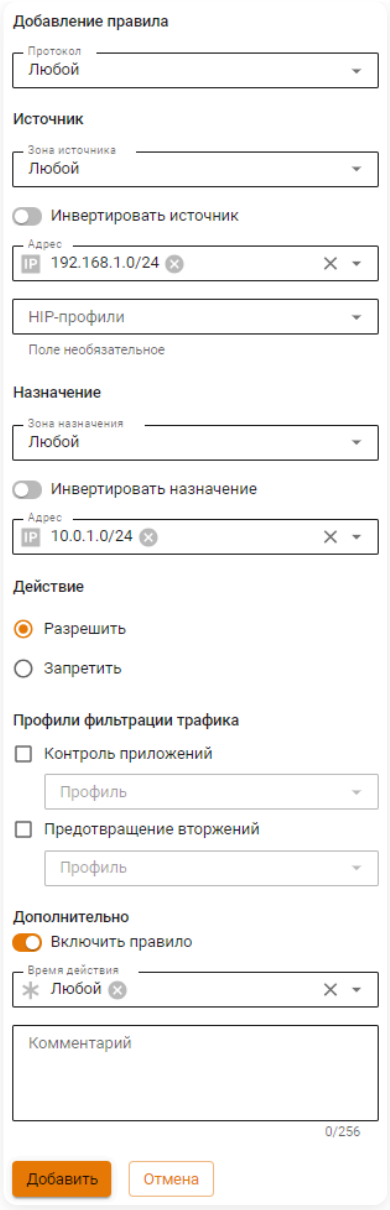
- **Адрес назначения** - адрес локальной сети за маршрутизатором (`10.0.1.0/24`).
- **Шлюз** - адрес машрутизатора (`10.0.0.10`).

- Для **Внешних сетей**:



- **Источник** - Любой.
- **Адрес назначения** - адрес внешней сети за маршрутизатором (`192.168.1.0/24`).
- **Шлюз** - адрес машрутизатора (`192.168.0.10`).

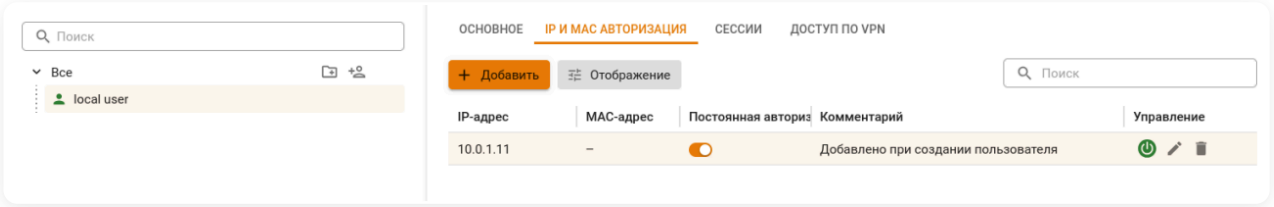
3. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD**, создайте и включите правило для доступа хостов из внешней сети `192.168.1.0/24` до IP-адресов пользователей локальной сети `10.0.1.0/24`:



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 раздел **Правила трафика** → **Файрвол** → **SNAT** и отключите опцию **Автоматический SNAT локальных сетей**.

5. Перейдите в раздел **Пользователи** → **Учетные записи** и включите опцию **Постоянная авторизация** для пользователей локальной сети `10.0.1.0/24`. 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.

Правила трафика Ideco NGFW будут работать только для трафика, приходящего из внешней сети в локальную сеть.

Настройка публичного IP-адреса 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 их диапазон от 0 до 65535 для получения эффекта присутствия локального сервера на внешнем IP-адресе.

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 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 добавьте правило в разделе **Правила трафика** → **Файрвол** → **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 их публикации воспользуйтесь обратным прокси-сервером.

Особенности создания правил DNAT в версии 18

- В предыдущих версиях профили безопасности настраивались в отдельных разделах. В версии 18 **Контроль приложений** настраиваются в правилах **Файрвола**.
- 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**.

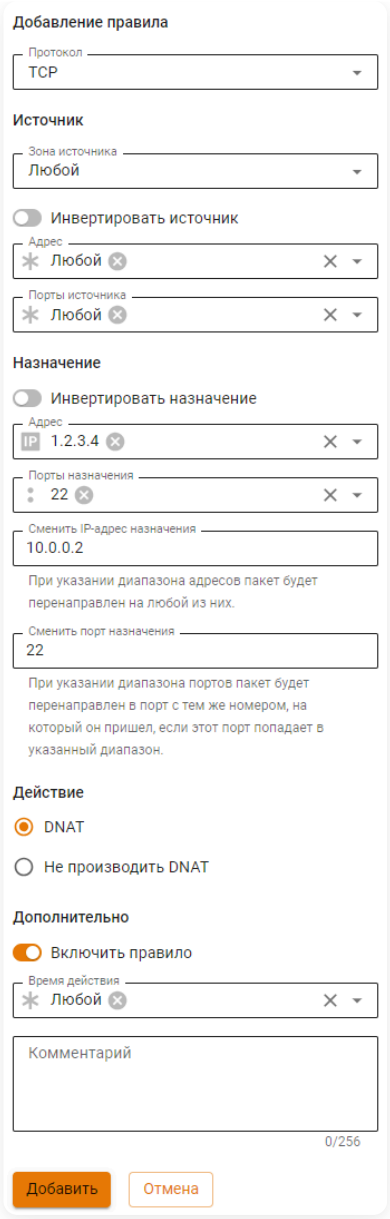
Создание правил DNAT и FORWARD в Файрволе Ideco NGFW

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 на устройство в локальной сети перейдите в раздел **Правила трафика** → **Файрвол** → **DNAT** и нажмите **Добавить**.

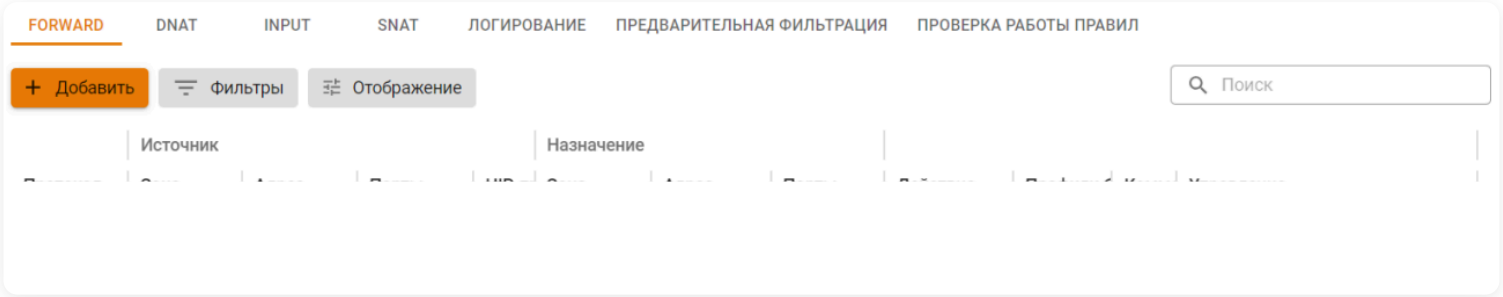
Заполните поля в соответствии с характеристиками, указанными в примере:



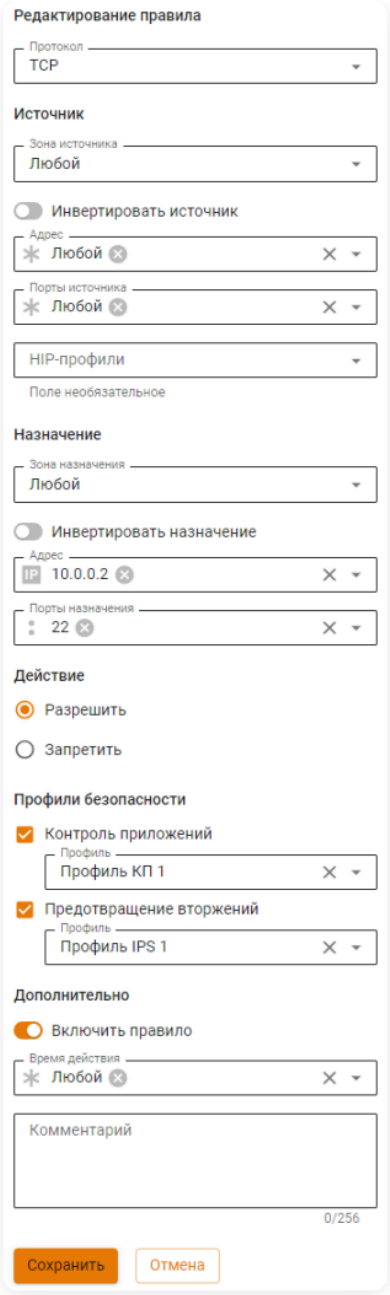
Вид правила в таблице после сохранения:

Проверьте наличие запрещающих правил в таблице FORWARD. При необходимости создайте правило, разрешающее трафик:

Поместите созданное правило выше запрещающего трафик:



Если вы хотите, чтобы трафик проверялся профилями безопасности, включите в созданном правиле соответствующие настройки:



Настройки **Файрвола** применяются сразу при создании правил.

Частые ошибки

- Если включен режим **Разрешить интернет всем**, правила **Файрвола**, 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.
- Если в одной локальной сети находятся пользователи и сервер с опубликованным при помощи DNAT-правила ресурсом, вероятна асимметричная маршрутизация. Информация о способах устранения асимметричной маршрутизации трафика представлена в статье.

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, 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 его IP-адресу в локальной сети. Альтернативный вариант - вынесите ресурс в отдельную локальную сеть, DMZ и обращайтесь к ресурсу из локальной сети клиентов по внешнему IP-адресу.

Интеграция NGFW и SkyDNS

Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

Чем может быть полезна интеграция:

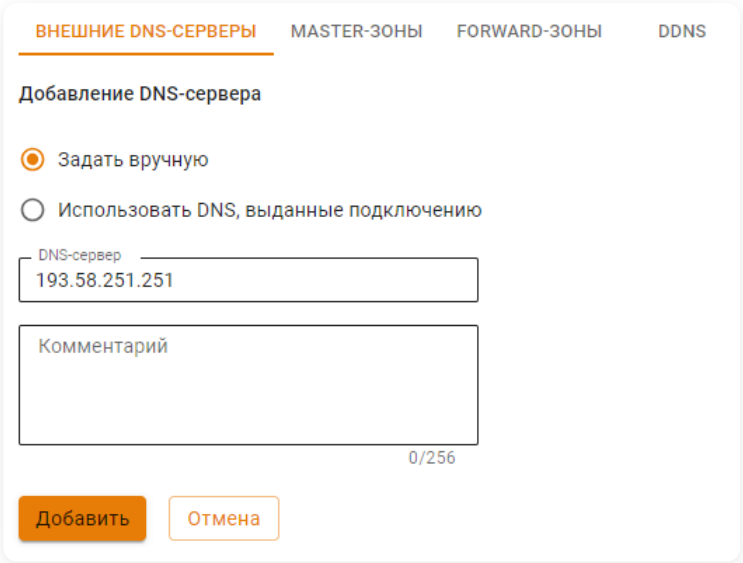
- **Защита от зараженных сайтов**. Вредоносные скрипты могут содержать сайты, как взломанные злоумышленниками, так и созданные специально для распространения вредоносного ПО.
- **Защита от бот-сетей**. Созданные из зараженных вредоносными программами компьютеров сети используются в DDoS-атаках на серверы, 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 он 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 и SkyDNS

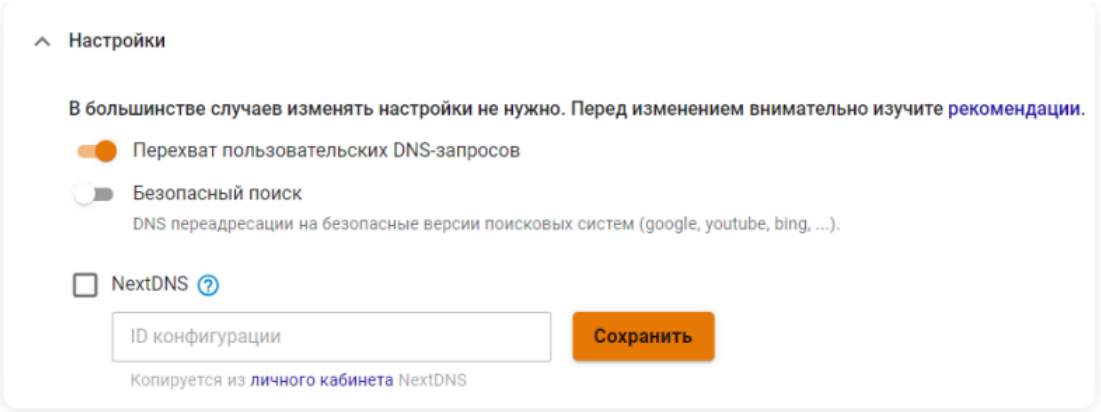
Чтобы настроить интеграцию со SkyDNS, выполните действия:

1. Перейдите в раздел **Сервисы** → **Защита и управление 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**:

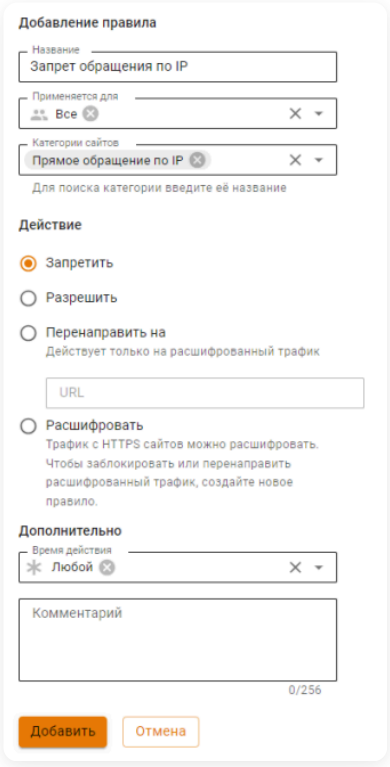


3. В настройках DNS включите опцию **Перехват пользовательских DNS-запросов** для запрета обращения к другим DNS-серверам (если фильтрация через SkyDNS обязательна для всей сети):



4. Если внутри локальной сети или внутри сети провайдера есть внутренняя DNS-зона, не обслуживаемая внешними DNS-серверами (например, домен Active Directory), укажите ее в разделе **Защита и управление DNS** → **FORWARD-ЗОНЫ**.

5. Перейдите в раздел **Правила трафика** → **Контент-фильтр** и создайте правило запрета прямого обращения к сайтам по IP-адресу:



6. Пропишите IP-адрес локального интерфейса Ideco NGFW в качестве единственного DNS-сервера в сетевых настройках на всех устройствах, которые требуется защитить.

Пользователи, получающие адреса автоматически через DHCP-сервер Ideco NGFW 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 статического белого IP-адреса привяжите этот 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

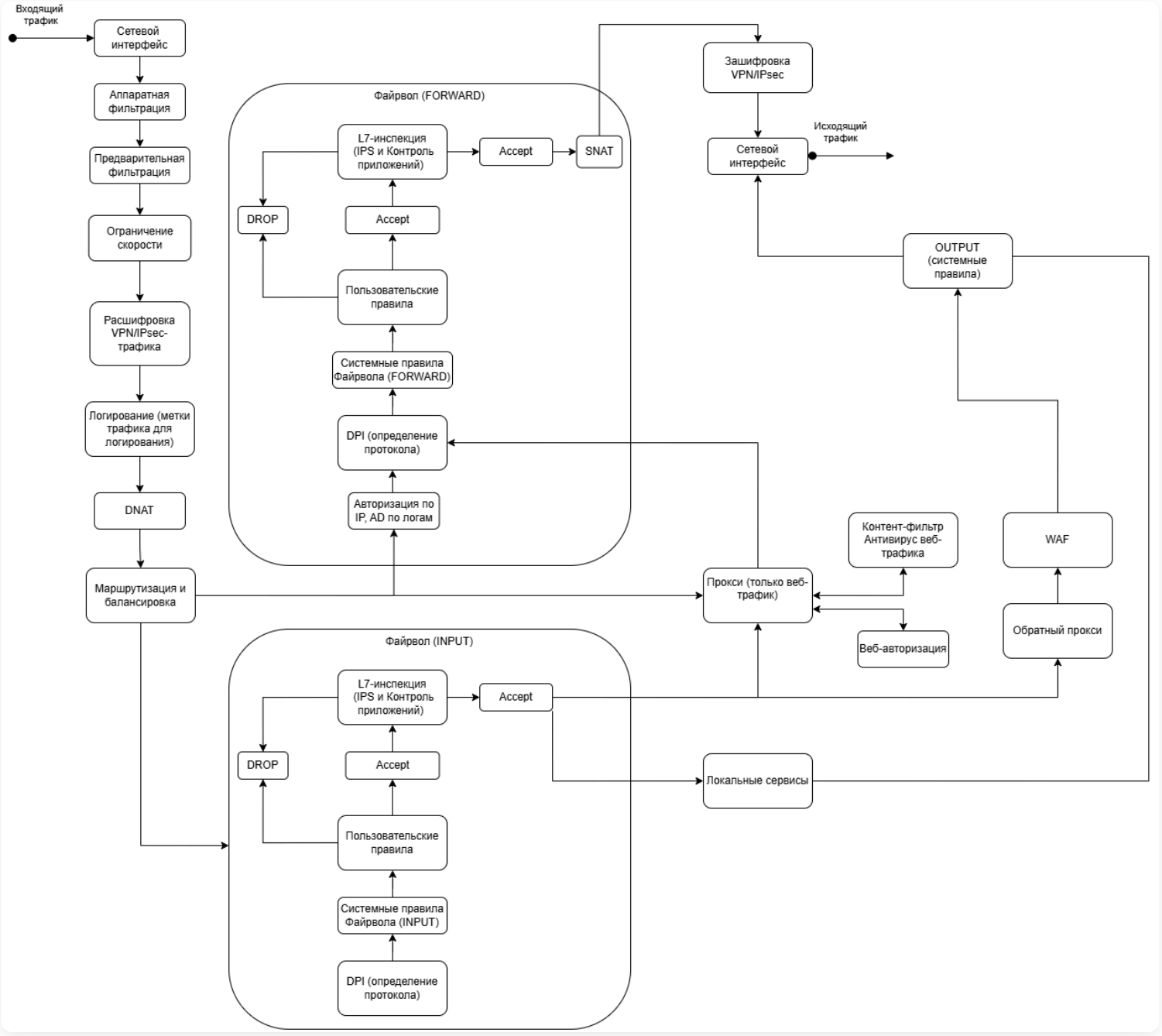


Полный цикл обработки трафика в Ideco NGFW

Статья описывает цикл, который проходят пакеты трафика в Ideco NGFW, в зависимости от сценария.

Обработку трафика условно можно разделить на три стадии:

- Предварительная;
- Файрвол;
- Завершающая.



К **Предварительной стадии** можно отнести Аппаратную, он проходит маршрутизацию и балансировку.

На второй стадии трафик проходит либо таблицу **INPUT**, либо таблицу **FORWARD** **Файрвола**:

- В первом случае - одно из двух:
  - Трафик проходит таблицу **INPUT** (системные и пользовательские правила, L7-фильтрацию) и направляется в локальные сервисы NGFW (например, DNS, NTP);

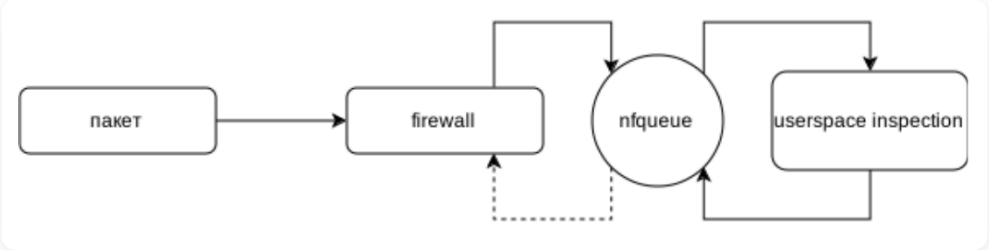
    - Трафик направляется в **Прокси** или **Обратный прокси**, обрабатывается соответствующими модулями и направляется в таблицу **FORWARD** (от **Прокси**) или в **OUTPUT** (от **Обратного прокси**).
- Во втором случае трафик проходит таблицу **FORWARD** (системные и пользовательские правила, L7-фильтрацию).

На **Завершающей стадии** трафик после обработки зашифровывается (при необходимости) и направляется получателю.

Принцип работы L7-инспекций

Трафик на обработку Предотвращением вторжений из Файрвола передается через NFQUEUE.

NFQUEUE - это технология интеграции файрвола linux с userspace-процессами, выполняющими инспекцию. Она позволяет выполнять L7-инспекции после L3-правил **Файрвола**:



Примеры прохождения трафика

Транзит трафика с фильтрацией и прозрачным прокси

1. Трафик пользователя попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию, Ограничение скорости (если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет).

2. Если пользователь подключился через VPN, трафик будет расшифрован.

3. Будет проверена DNAT-таблица **Файрвола**: 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 **Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, 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, 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 **Файрвола**: 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 она настроена).

4. Трафик направляется в **FORWARD**-таблицу **Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, Контроль приложений).

5. Запрос направляется ресурсу, на который обратился пользователь, ответ направляется пользователю (трафик вновь проходит п. 1 - п. 4).

Публикация ресурсов через обратный прокси

1. Трафик из внешней сети попадает на Ideco NGFW, 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 **Файрвола**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, 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.

Разрешить интернет всем

1. Трафик пользователя попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию, Ограничение скорости. Если трафик подпадает под правила - он может быть заблокирован и дальше не пойдет.

2. Пользователи могут подключаться через VPN, включая шифрованные подключения.

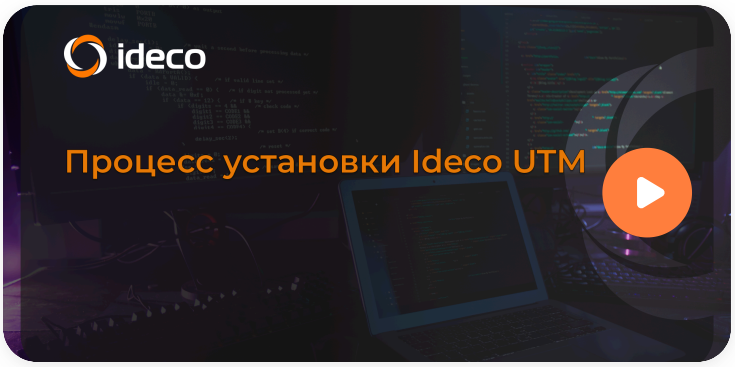
3. DNAT-таблица **Файрвола** не проверяется: даже если трафик подпадет под правила - IP-адрес или порт назначения не изменится.

4. Трафик, минуя стадию авторизации, пройдет таблицу **FORWARD** и не будет отброшен вне зависимости от созданных там правил фильтрации.

В статье представлен полный перечень видеоинструкций по продуктам Ideco

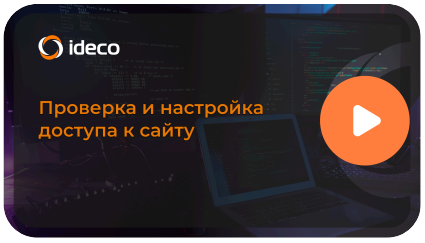
Ссылки на другие ресурсы

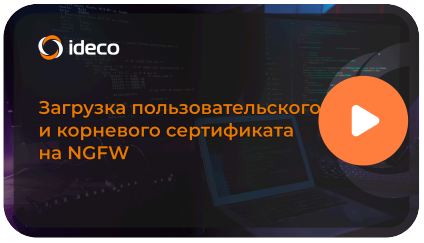
YouTube RUTUBE VK Видео



Последние видео







Видеоинструкции NGFW

Список видеоинструкции разбитые по разделам

Пользователи | Правила трафика | Профили безопасности | Сервисы | Управление сервером | Почтовый релей

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

FAQ

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 ?

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 и брокера сетевых пакетов DS Integrity NG - по ссылке.

Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW?

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 он 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 сети за роутером, находящимся после NGFW, не доступны по VPN?

Для решения вопроса воспользуйтесь статьей Доступ в удаленные сети через роутер в локальной сети.

Что делать, если ваш IP попал в черные списки DNSBL?

Если вы 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 его восстановить?

При утере пароля администратора можно его восстановить, имея физический доступ к серверу. Подробнее о процессе восстановления в статье Как восстановить доступ к Ideco NGFW.

После обновления потребовалось вернуть предыдущую версию со всеми настройками. Как это сделать?

Возможность восстановиться на предыдущую версию после обновления Ideco NGFW доступна с 12.X версий. Подробнее о процессе восстановления в статье Как восстановиться на прошлую версию после обновления Ideco NGFW.

Как подобрать аппаратную платформу для Ideco NGFW?

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 40 и содержит ядро Linux с набором драйверов от этой ОС с небольшими изменениями с нашей стороны. Таким образом, Ideco NGFW можно установить на большую часть оборудования, поддерживающего Fedora 40. Подробнее в статье Выбор аппаратной платформы для Ideco NGFW.

Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW?

Для настройки Ideco NGFW 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 до первоначальных настроек?

Для возврата к первоначальным настройкам используйте бэкап, созданный после установки Ideco NGFW. Если бэкапа нет - переустановите Ideco NGFW.

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 >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Инструкция по созданию VPN-подключения в Alt Linux

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 раздел **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

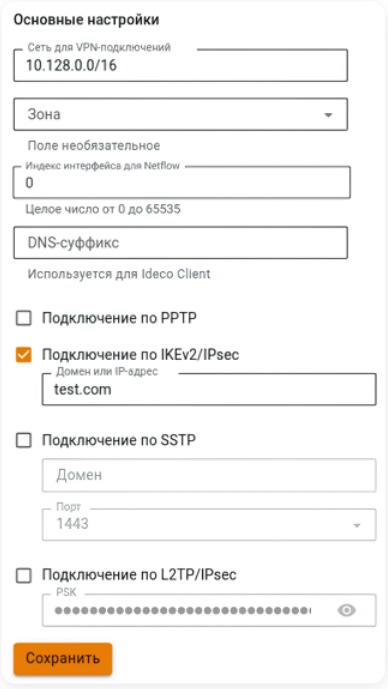
Не рекомендуем использовать для VPN-подключений кириллические логины.

Протокол IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите опцию **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

Создание подключения Alt Linux:

1. Откройте терминал сочетанием клавиш Ctrl+Alt+T и установите необходимые пакеты:

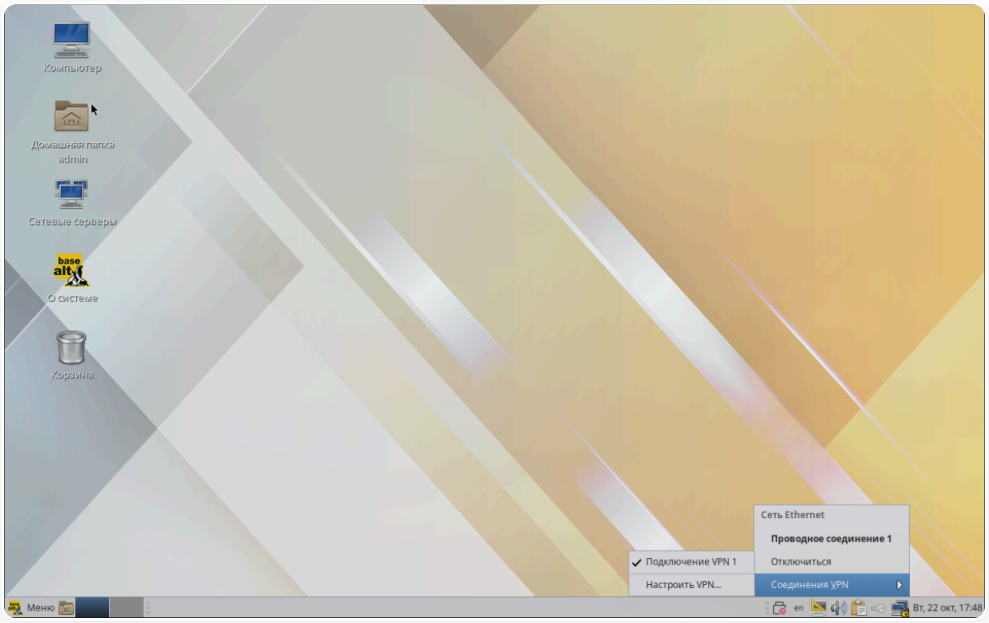
```
apt-get update && apt-get dist-upgrade && apt-get install NetworkManager-strongswan NetworkManager-strongswan-gnome strongswa
```

2. Установите корневой сертификат на рабочую станцию:

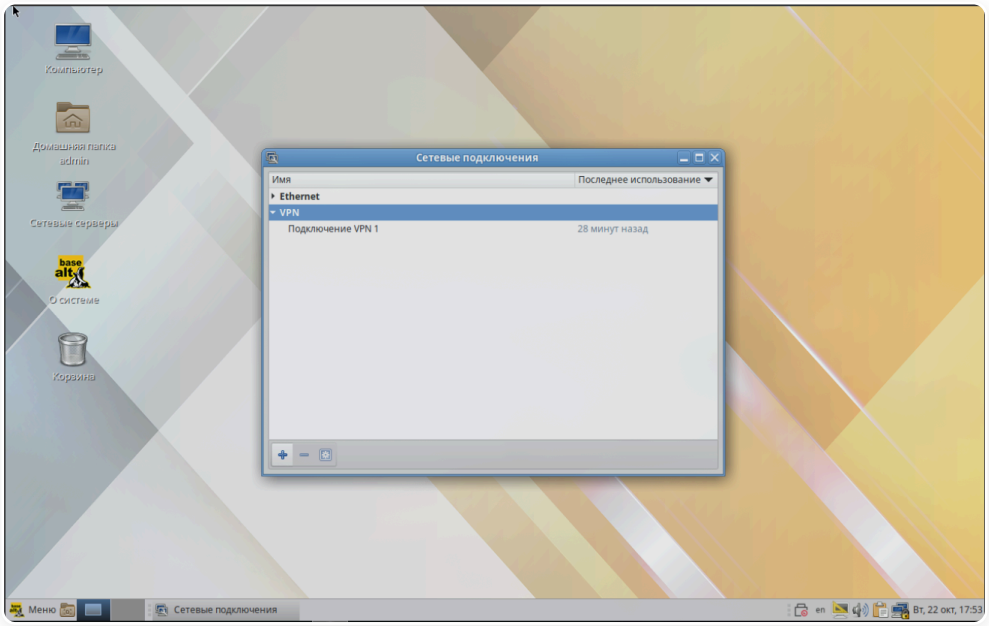
```
cp root-ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

- `root-ca.crt` - путь к сертификату.

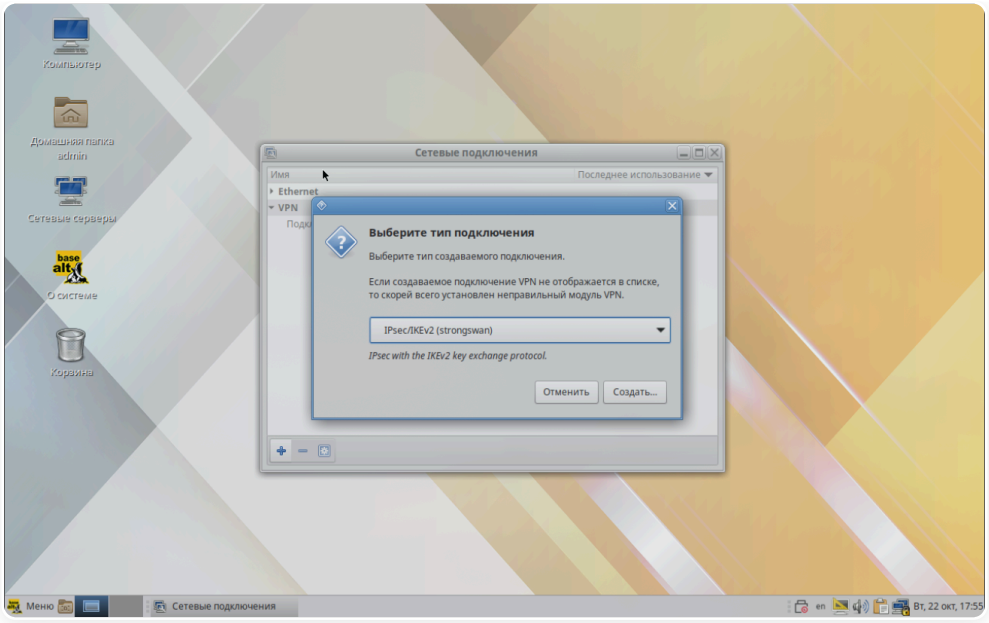
3. Перейдите в **Соединения VPN** и нажмите **Настроить VPN**:



4. Добавьте новое VPN-подключение:

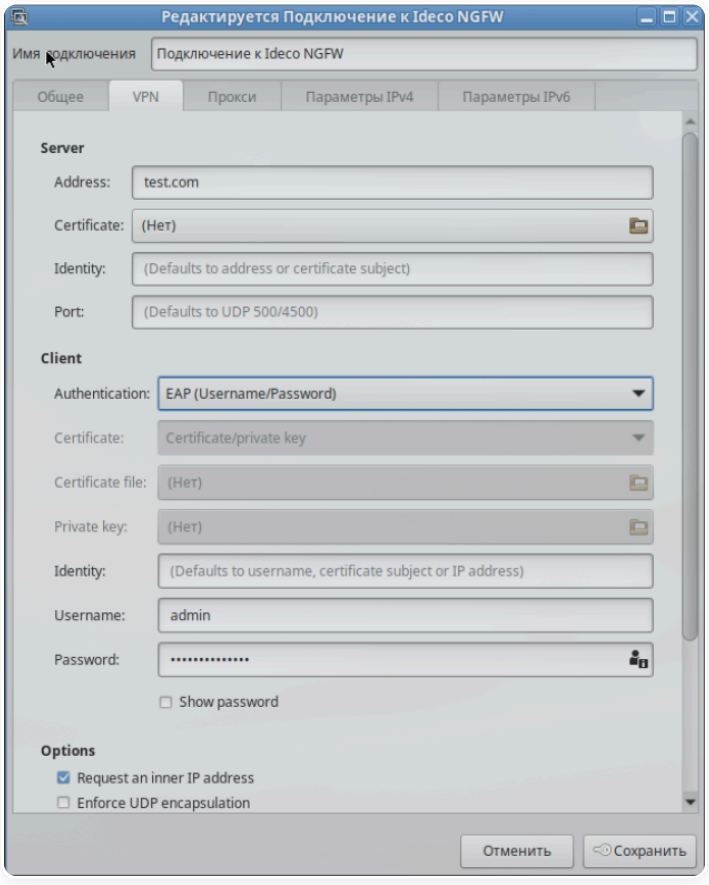


5. Выберите тип VPN-подключения `IPsec/IKEv2 (strongswan)` и нажмите **Создать**:

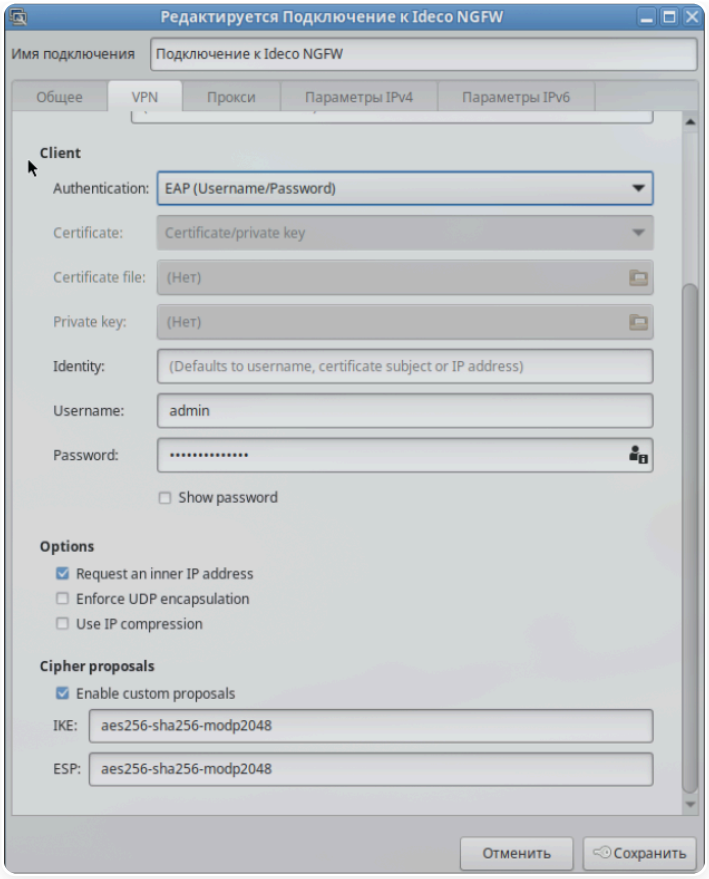


6. Заполните необходимые поля для создания VPN-подключения, как на скриншоте:

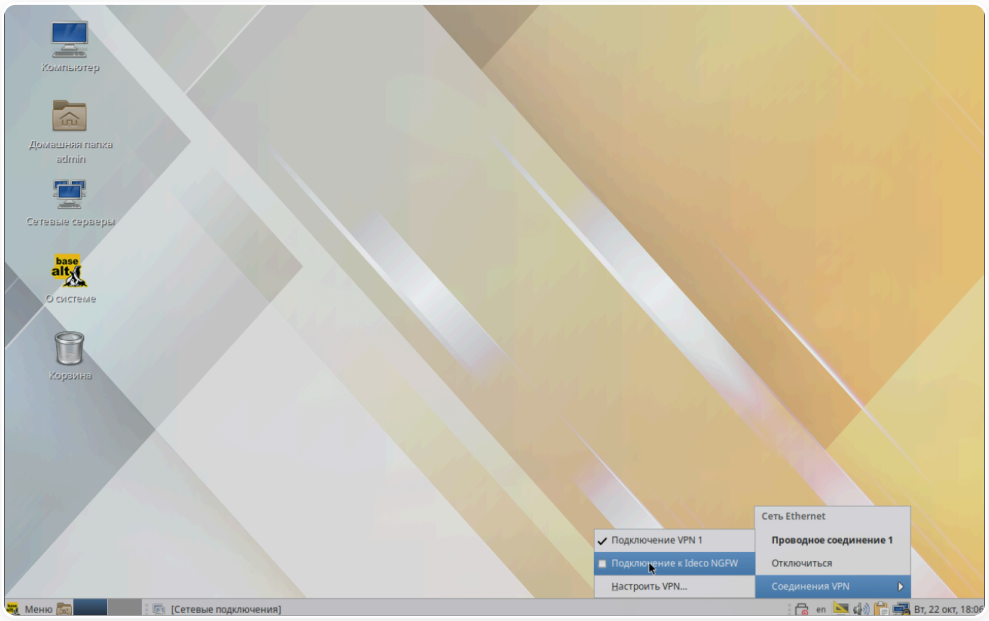
- Address - адрес шлюза;
- Authentication - тип аутентификации;
- Username - логин пользователя на Ideco NGFW;
- Password - пароль пользователя на Ideco NGFW.



7. Заполните параметры шифрования, как на скриншоте, и нажмите **Сохранить**:



8. Включите созданное VPN-подключение:



Создание VPN-подключения в Ubuntu

Перед настройкой VPN-подключения перейдите в раздел **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.

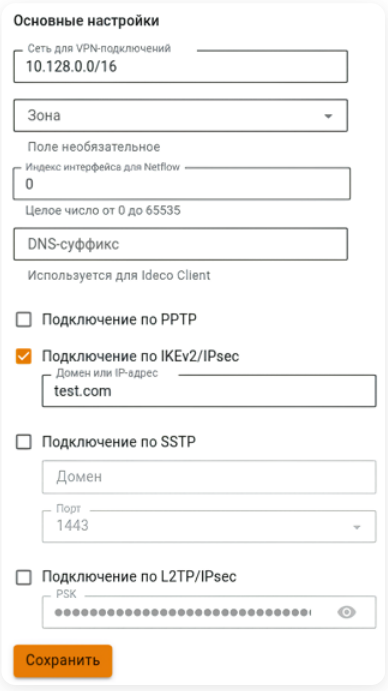
Инструкция актуальна для версии Ubuntu 24.04 LTS.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен или IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе 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 в хранилище доверенных сертификатов Ubuntu:

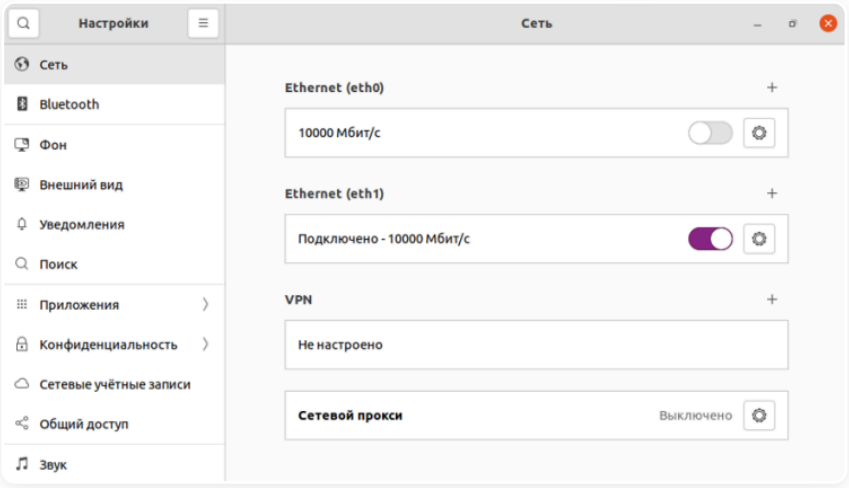
```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

- `ca.crt` - имя скачанного сертификата.

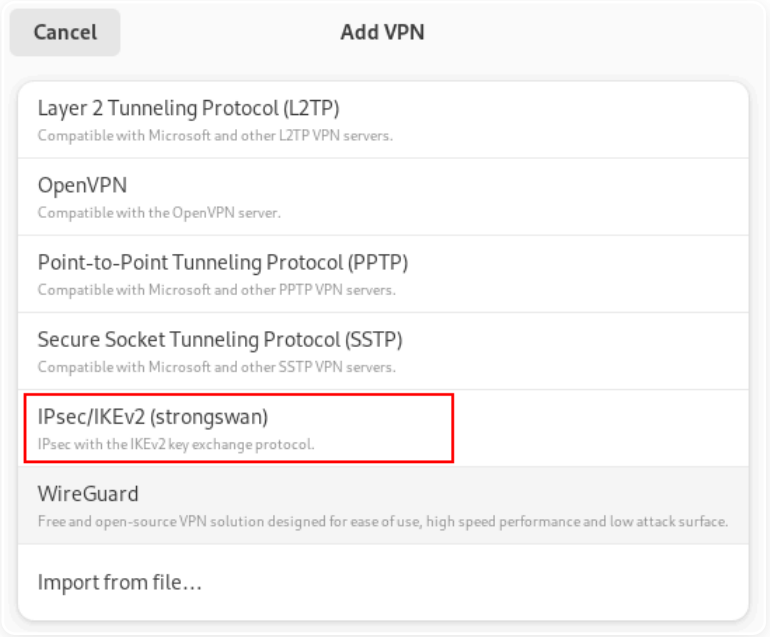
5. Для обновления сертификатов устройства выполните команду:

```
sudo update-ca-certificates
```

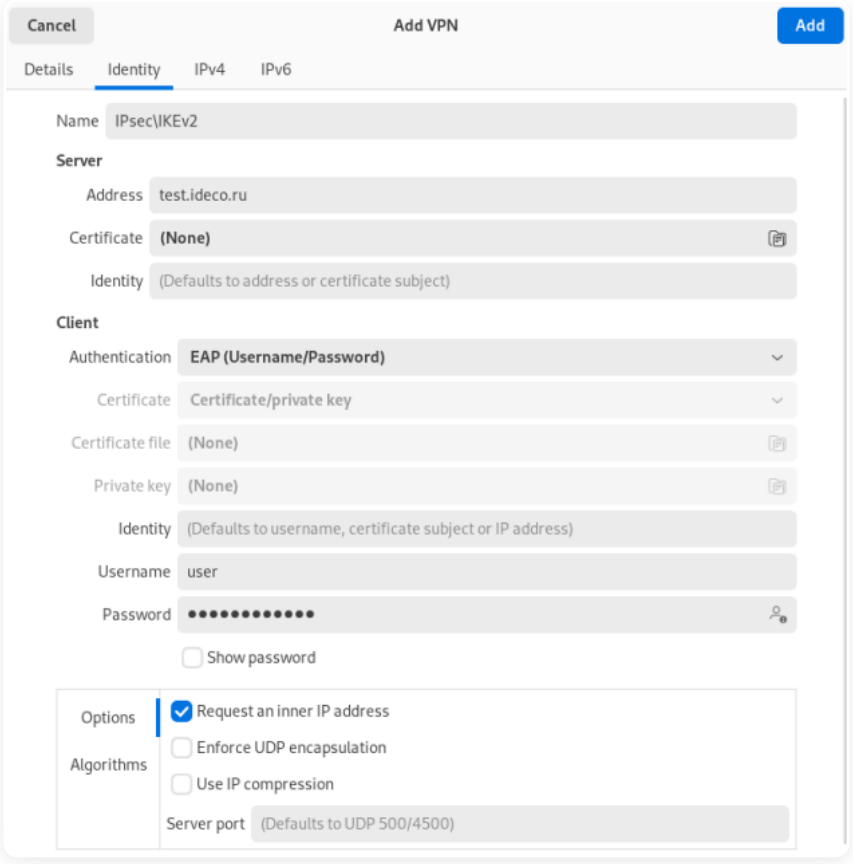
6. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋:



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** → **Подключение по 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.

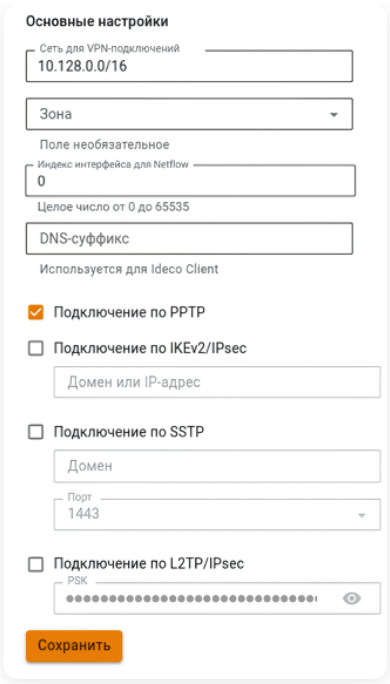
Установите флаг **Request an inner IP address** и нажмите **Добавить**.

9. Включите созданное VPN-подключение.

PPTP

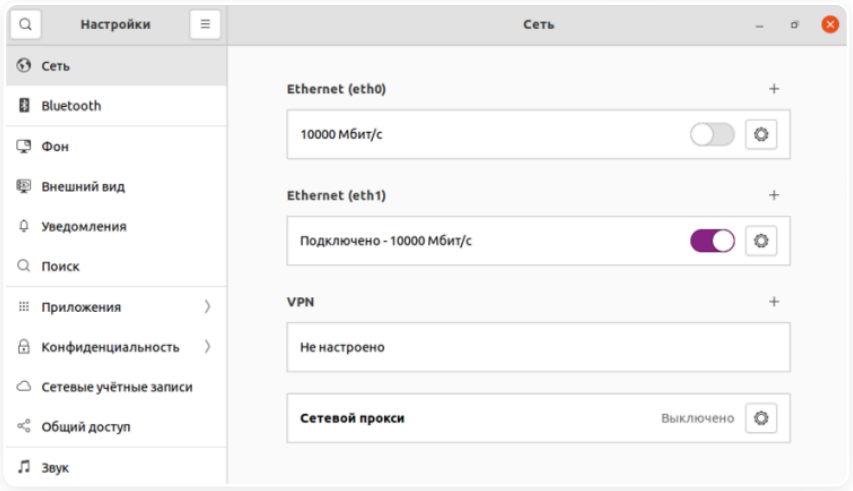
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное** и установите флаг **Подключение по PPTP**:



Создание подключения в Ubuntu:

1. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋:



2. В появившемся окне выберите **Туннельный протокол типа точка-точка (PPTP)**:

3. На вкладке **Идентификация** заполните поля:

- **Название** - имя подключения.
- **Шлюз** - домен или IP-адрес Ideco 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.

Рекомендуем нажать **Дополнительно** и установить флаги на пунктах:

- **Разрешить следующие методы аутентификации** - установите флаг на *MSCHAPv2*.
- **Использовать шифрование MPPE** - в строке *Шифрование* выберите 128-бит (наиболее защищенное).
- **Использовать для данных сжатие BSD**.
- **Использовать для данных сжатие Deflate**.
- **Использовать сжатие заголовков TCP**.

4. Нажмите **ОК** и **Добавить**.

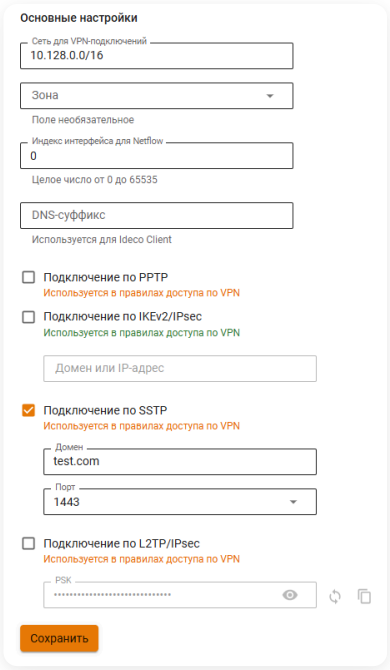
5. Включите созданное VPN-подключение:

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе 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 их более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **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
```

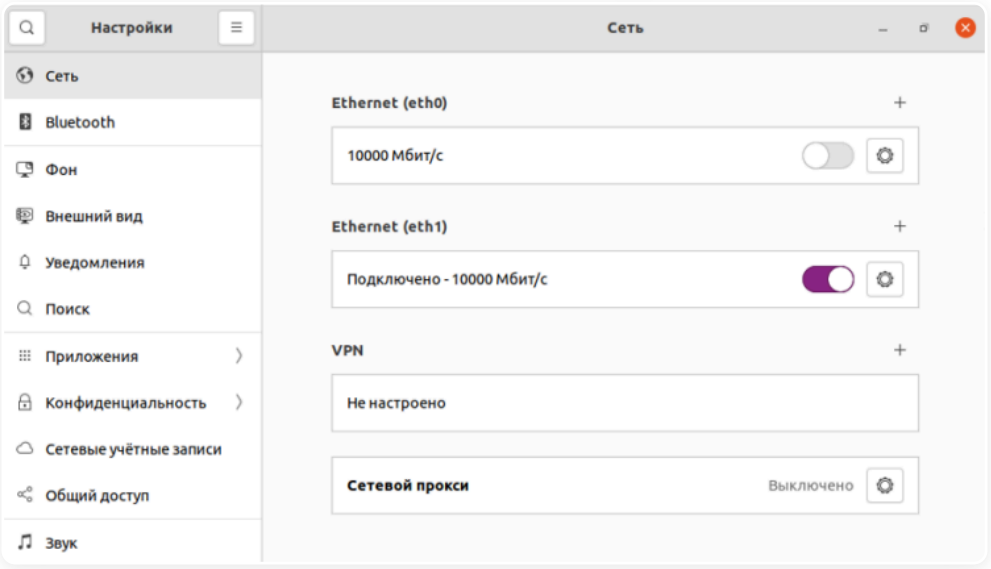
4. Проверьте установленные пакеты:

```
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.
- **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:

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 раздел **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте правило разрешающее VPN-подключение.

2. Загрузите на устройство корневой сертификат Ideco NGFW. Файл сертификата должен находиться в общедоступном каталоге.

Загружать сертификат **ISRG_ROOT_X1** не требуется, так как он уже есть в Fedora 40 и находится в каталоге `/etc/ssl/certs`.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен или IP-адрес**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW 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, 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 разделе **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.

PPTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное** и установите флаг **Подключение по PPTP**:

Создание подключения в Fedora:

1. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите +.

2. В окне создания подключений выберите пункт **Туннельный протокол типа точка-точка (PPTP)**.

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

- **Имя** - название VPN-подключения;
- **Gateway** - доменное имя или IP-адрес NGFW;
- **User name** - логин пользователя, которому разрешено подключение по VPN;
- **Password** - пароль пользователя.

Рекомендуем нажать **Advanced** и установить флаги на пунктах:

- **Разрешить следующие методы аутентификации** - на *MSCHAPv2*;
- **Использовать шифрование MPPE** - в строке *Шифрование* выберите 128-бит (наиболее защищенное);
- **Использовать для данных сжатие BSD**;
- **Использовать для данных сжатие Deflate**;
- **Использовать сжатие заголовков TCP**.

5. Нажмите **Apply**, затем **Применить**.

6. Включите созданное VPN-подключение.

Если подключение по PPTP не устанавливается:

1. Выполните команду `sestatus`, чтобы узнать текущий режим SELinux. Если режим **Enforcing**, SELinux может блокировать работу PPTP.

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 PPTP. 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.

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **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;
- **Password** - пароль пользователя на Ideco NGFW.

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 их более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **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.

Инструкция по созданию подключения в Astra Linux

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

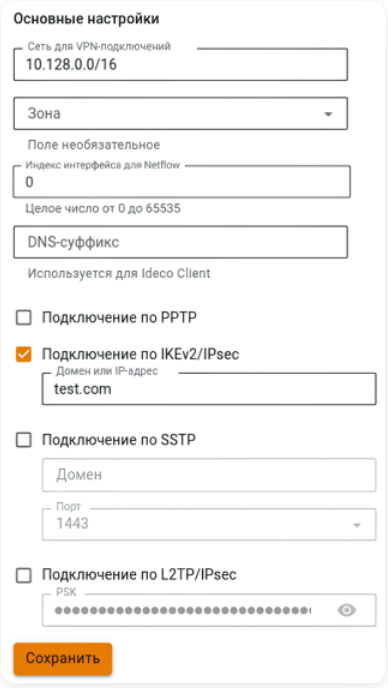
Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите на вкладку **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW на вкладке **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

Создание подключения в Astra Linux:

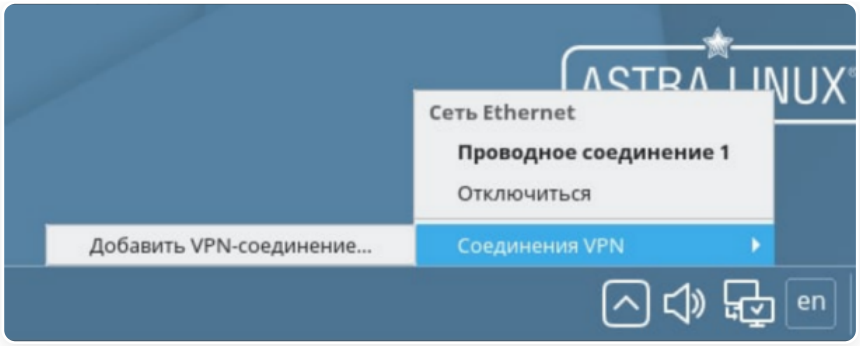
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt install libcharon-extra-plugins
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-extra-plugins
```

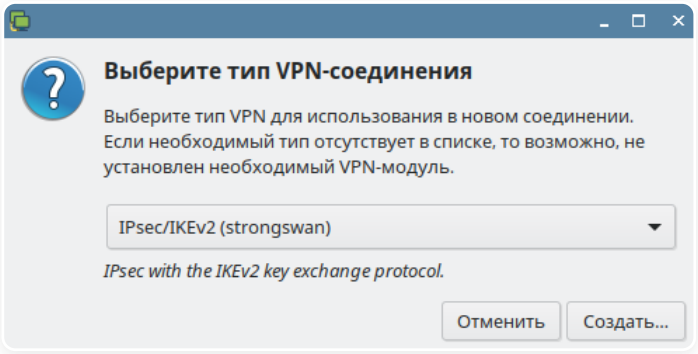
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. В настройках сети выберите **Соединения VPN** → **Добавить VPN-соединение**:



4. Выберите тип соединения **IPsec/IKEv2 (strongswan)** и нажмите **Создать**:

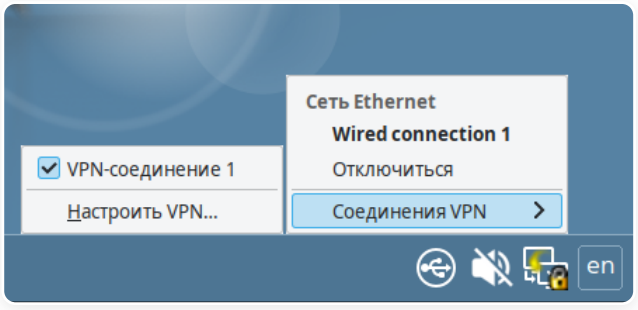


5. На вкладке **VPN** заполните поля:

- **Имя соединения** - имя подключения;
- **Address** - введите домен или IP-адрес, который указан в настройках **Пользователи → VPN-подключения → Основное → Подключение по 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
```

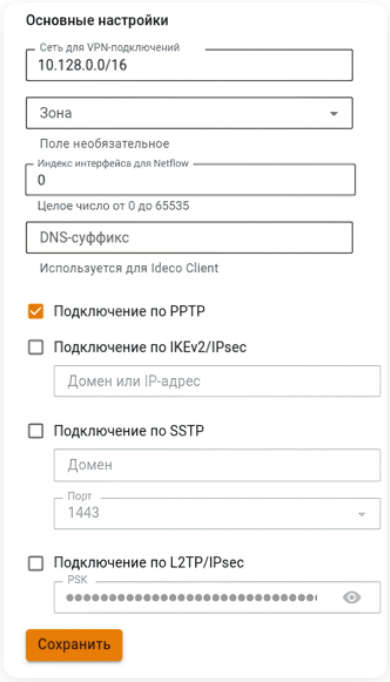
- для Phase1 Algorithm ищите значения **proposals=**;
- для Phase2 Algorithms ищите значения **esp_proposals=**.

PPTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по PPTP**:



Создание подключения в Astra Linux:

1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt update
sudo apt install network-manager-pptp network-manager-pptp-gnome pptp-linux
```

2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. В настройках сети выберите **Соединения VPN** → **Добавить VPN-соединение**:

4. Выберите тип соединения **Туннельный протокол типа точка-точка (PPTP)** и нажмите **Создать**:

5. На вкладке **VPN** заполните поля и нажмите **Сохранить**:

- **Имя соединения** - имя подключения;
- **Шлюз** - IP-адрес или домен внешнего интерфейса Ideco NGFW;
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля веберите вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

6. В настройках сети выберите **Соединения VPN** и установите флаг в строке с созданным соединением:

L2TP/IPsec

Настройка Ideco NGFW:

1. Перейдите на вкладку **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

Создание подключения в Astra Linux:

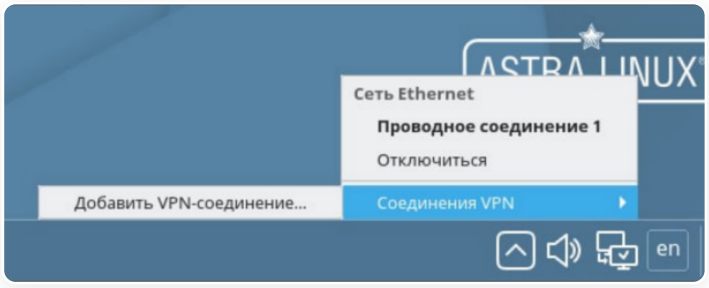
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
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;
- **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 (**Пользователи** → **VPN-подключение** → **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**:

Инструкция по созданию подключения в Windows

Перед настройкой VPN-подключения перейдите в раздел **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 на вкладку **Сеть** → **IP версии 4 (TCP/IPv4)** → **Дополнительно**.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

4. Импортируйте сертификат Ideco NGFW:

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 иконке 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 IKEv2.

- **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).
- **Протокол расширенной проверки подлинности (EAP)** - Microsoft защищенный пароль (EAP MSCHAPV2).

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**.

PPTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное** и установите флаг **Подключение по PPTP**:

Создание подключения в Windows:

1. Кликните на иконке 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 PPTP.
- **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**.

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

4. Импортируйте сертификат Ideco NGFW:

Пример для Windows

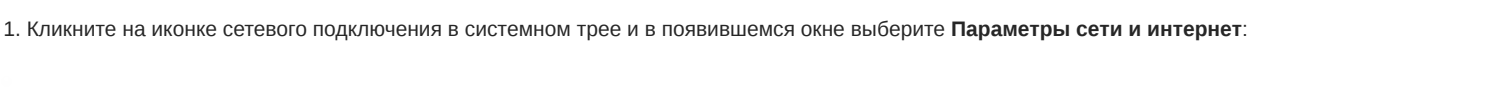
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



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



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

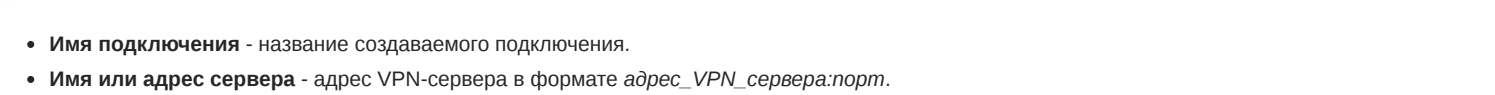


Создание подключения в Windows:

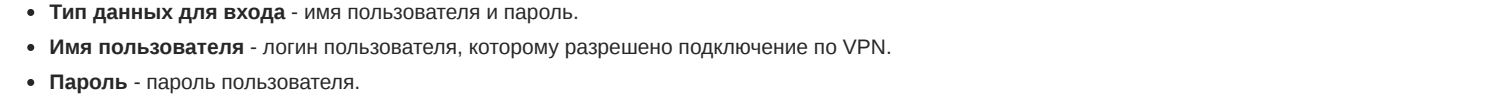
1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



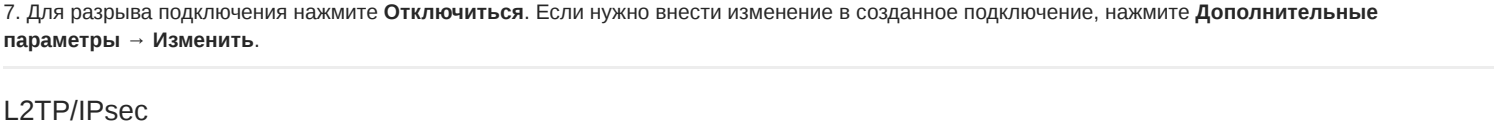
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера в формате *адрес_VPN_сервера:порт*.
- **Тип VPN** - протокол SSTP.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение 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**.

L2TP/IPsec

Важно: L2TP/IPsec клиенты, находящиеся за одним NAT, могут испытывать проблемы подключения, если их более одного. В решении проблемы поможет инструкция. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Windows:

1. Кликните на иконке 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 строки **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 разделе **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 не имеет "белого" IP-адреса, а необходимые для работы порты (500 и 4500) "проброшены" на внешний интерфейс устройства, расположенного перед Ideco NGFW 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 и указать на внешнем интерфейсе Ideco NGFW "белый" IP-адрес, к которому в итоге и будут осуществляться L2TP/IPsec-подключения. Либо используйте протокол SSTP - его 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. Оно 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 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 на мобильных устройствах по протоколам IKEv2/IPsec, L2TP/IPsec, SSTP и PPTP.

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** в Ideco NGFW 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

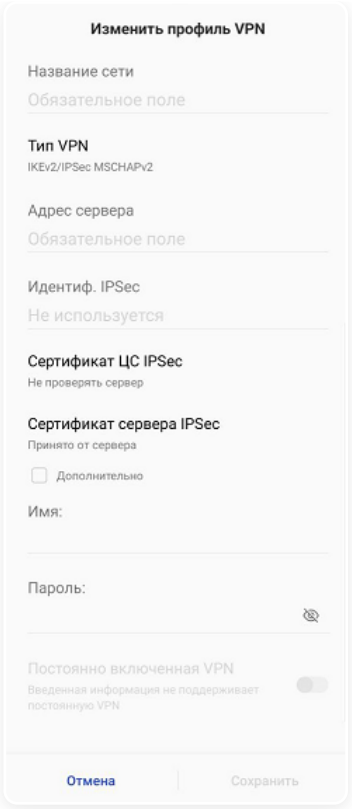
Android

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:

Для IKEv2/IPsec MSCHAPv2:

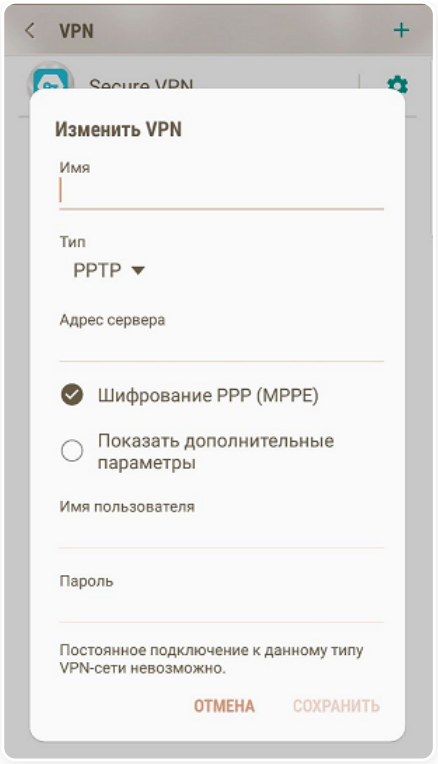


Расшифровка полей

- **Название сети** - имя подключения.
- **Адрес сервера** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по 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.

Для PPTP:

Начиная с версии Android 12 прекращена поддержка протокола PPTP. Не рекомендуем использовать PPTP, так как подключение крайне небезопасно.

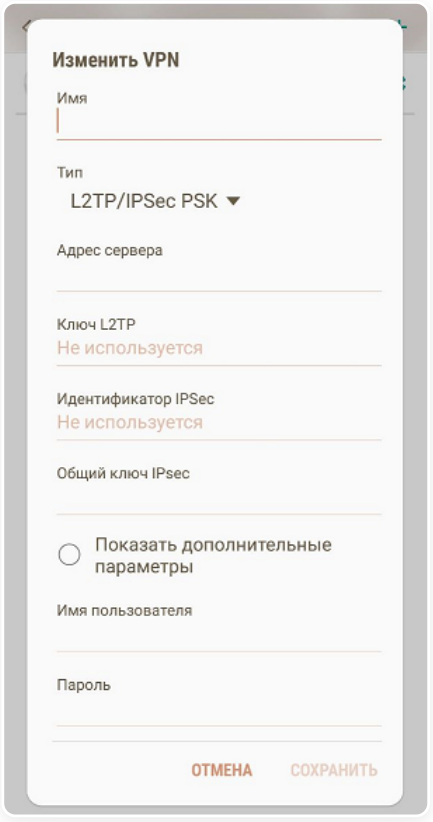


Расшифровка полей

- **Имя** - имя подключения.
- **Адрес сервера** - домен или IP-адрес Ideco NGFW.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

Для L2TP/IPsec PSK:

Начиная с версии Android 12 прекращена поддержка протокола L2TP. Не рекомендуем использовать L2TP, так как подключение крайне небезопасно.



Расшифровка полей

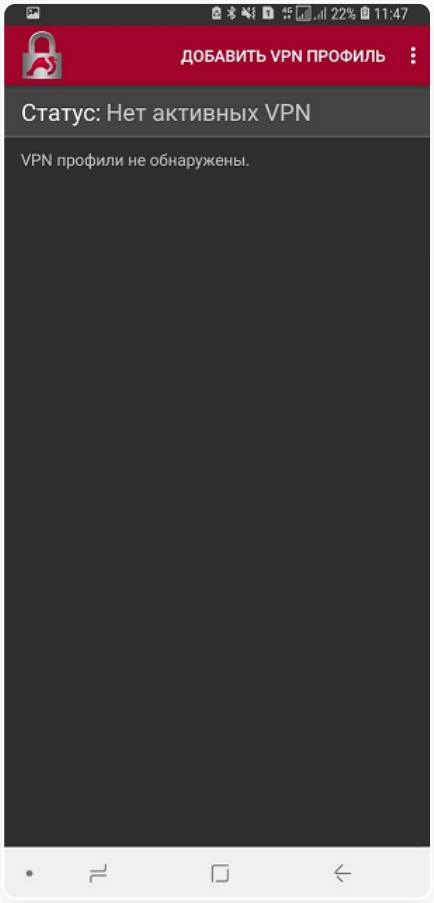
- **Имя** - имя подключения.
- **Адрес сервера** - домен или IP-адрес Ideco NGFW.
- **Общий ключ IPsec** - значение поля **PSK** в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по L2TP/IPsec** в Ideco NGFW.

3. Нажмите **Сохранить** и активируйте подключение.

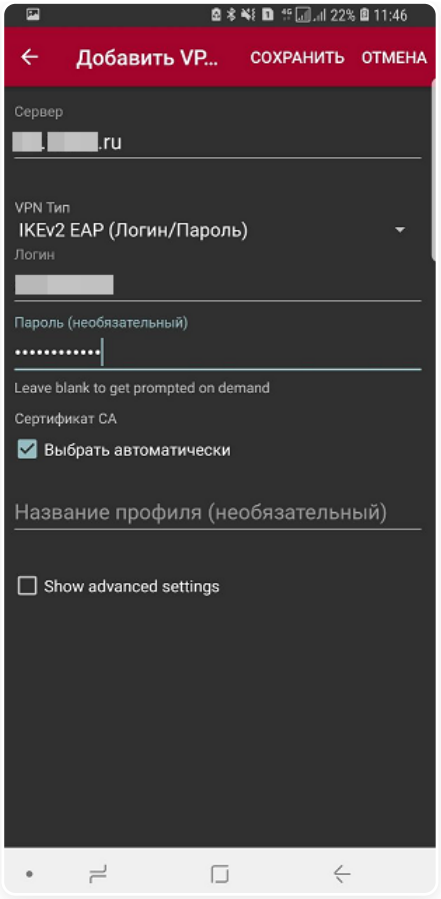
StrongSwan

Приложение StrongSwan позволяет создавать VPN-подключение только через протокол IKEv2.

1. Нажмите **Добавить VPN профиль**:



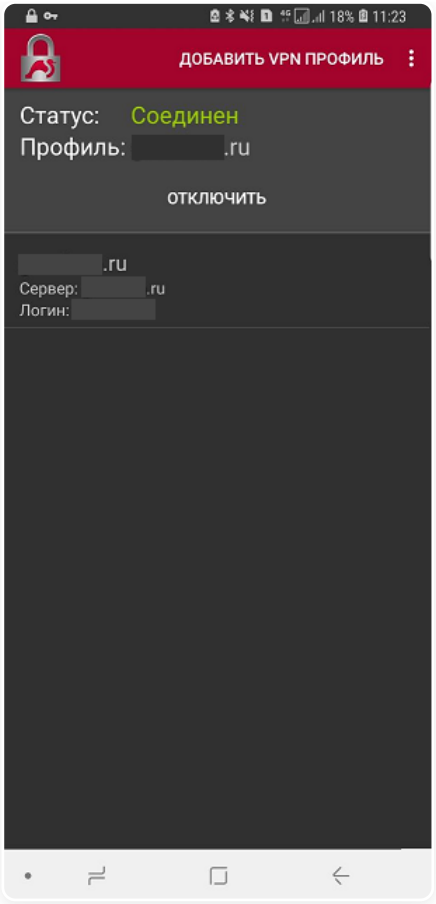
2. Заполните поля:



Расшифровка полей

- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по IKEv2/IPsec**.
- **VPN тип** - IKEv2 EAP (Логин/Пароль).
- **Логин** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

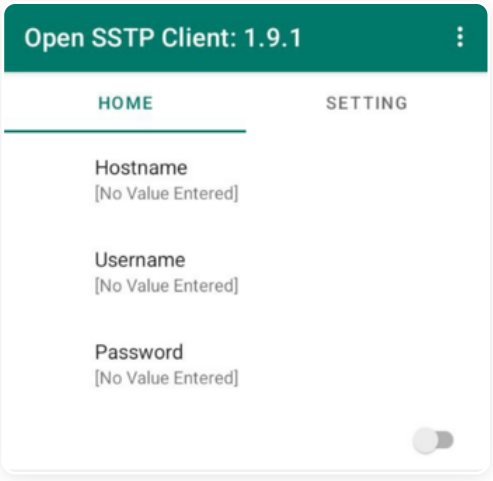
3. Нажмите **Сохранить** и перейдите по созданному подключению:



Open SSTP Client

Приложение Open SSTP Client позволяет создавать VPN-подключение через протокол SSTP.

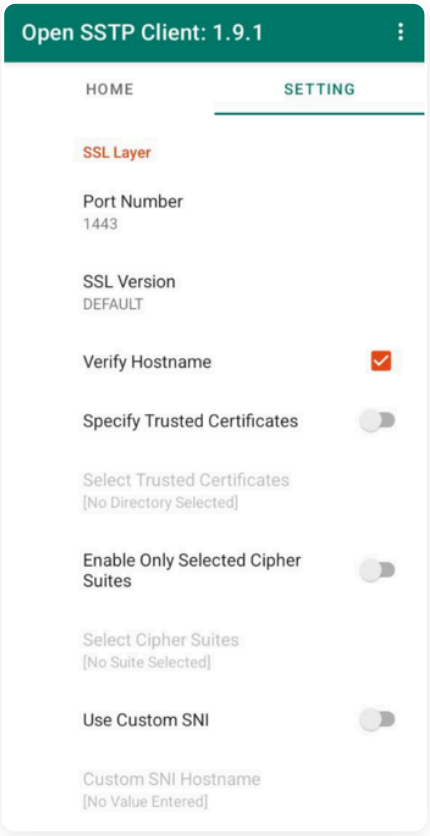
1. Откройте приложение и заполните поля:



Расшифровка полей

- **Hostname** - домен, указанный в Ideco NGFW 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.



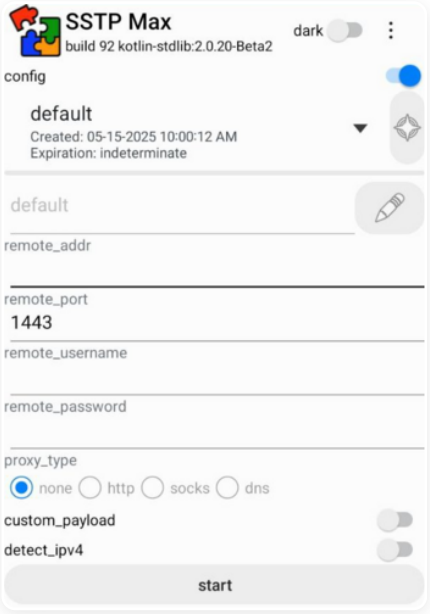
Для автоматического подключения включите опцию **Enable Reconnection** на вкладке **SETTING**.

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 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.

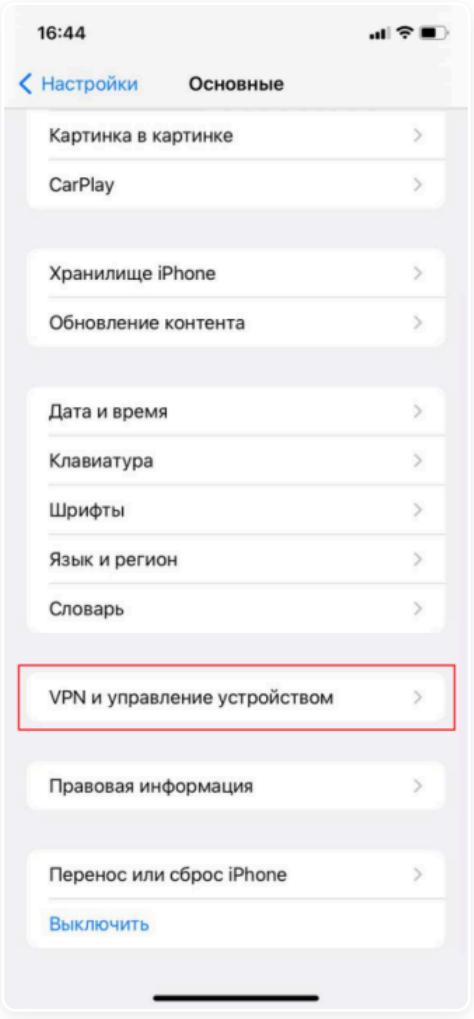
2. Нажмите start.

---

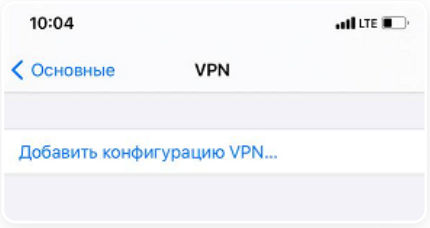
iOS

iOS

1. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством** → **VPN**:



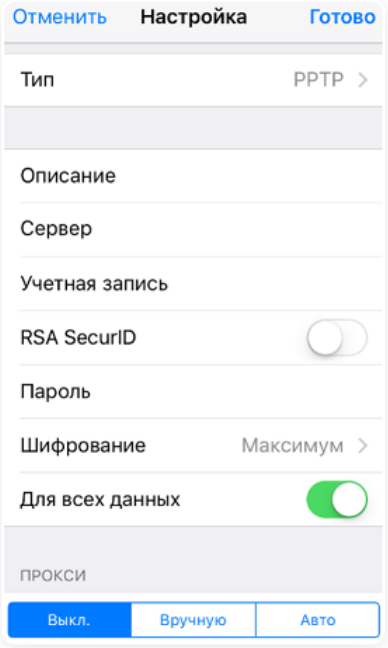
2. Нажмите **Добавить конфигурацию VPN**:



3. Выберите **Тип** подключения и заполните поля:

Для PPTP:

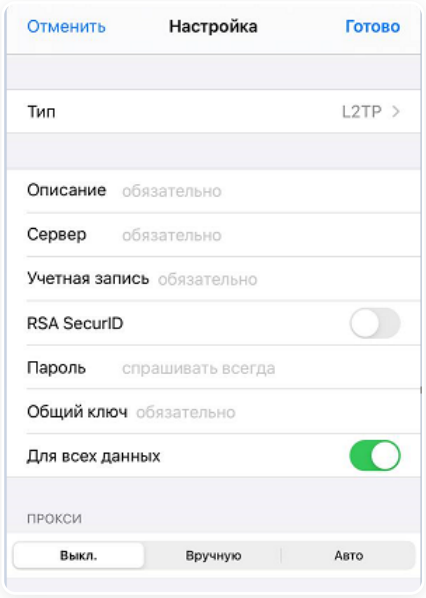
> Начиная с версии iOS 10 прекращена поддержка протокола PPTP. Не рекомендуем использовать PPTP, так как подключение крайне небезопасно.



Расшифровка полей

- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес Ideco NGFW.
- **Учетная запись** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

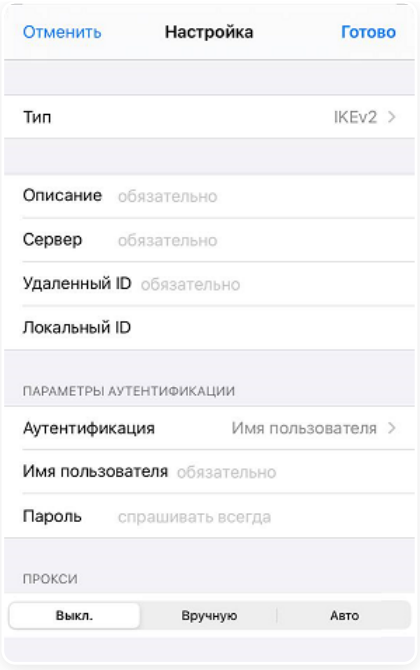
Для L2TP:



Расшифровка полей

- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес Ideco NGFW.
- **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.

Для IKEv2:

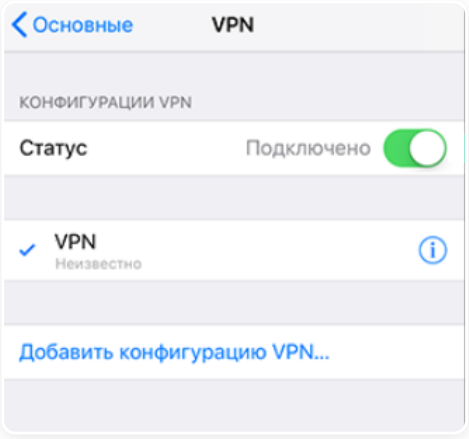


Расшифровка полей

- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи → VPN-подключения → Основное → Подключение по IKEv2/IPsec**.
- **Удаленный ID** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи → VPN-подключения → Основное → Подключение по IKEv2/IPsec**.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

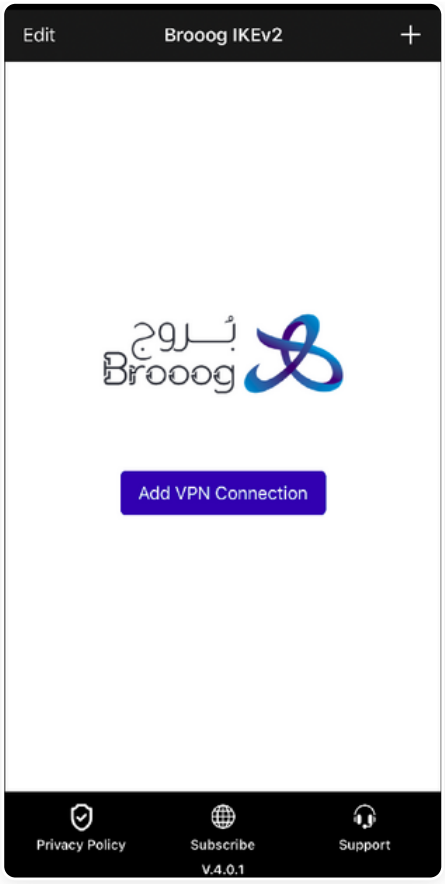
4. Нажмите **Готово**.

5. Включите опцию **Статус**:

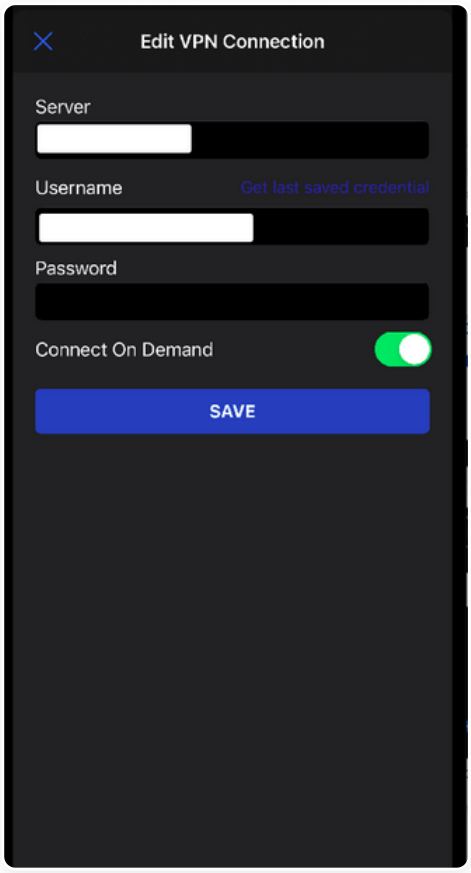


Brooog IKEv2

1. Нажмите **Add VPN Connection**:



2. Заполните поля и включите опцию **Connect on Demand**:

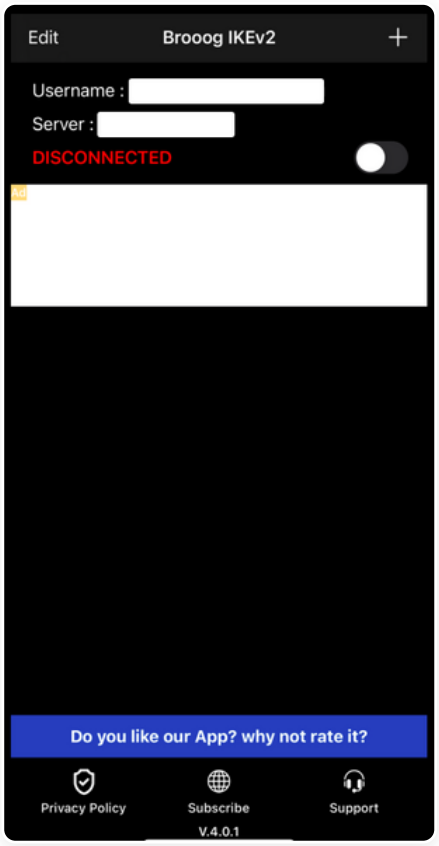


Расшифровка полей

- **Server** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи → VPN-подключения → Основное → Подключение по IKEv2/IPsec**.
- **Username** - логин пользователя, которому разрешено подключение по VPN.

- **Password** - пароль пользователя.

3. Нажмите **Save** и переведите опцию в режим **CONNECTED**:



Инструкция по созданию подключения в Mac OS

Перед настройкой VPN-подключения перейдите в раздел **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:

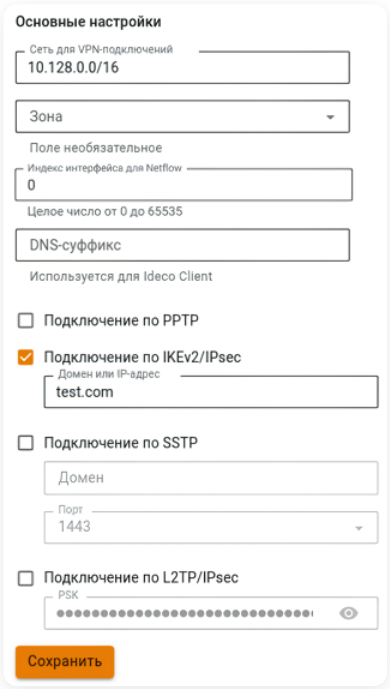
1. Проверить, что в качестве VPN-сервера указано его доменное имя в разделе **Пользователи** → **VPN-подключения**.
2. Проверить, что на доменное имя VPN-сервера выдан сертификат Let's Encrypt.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен или IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

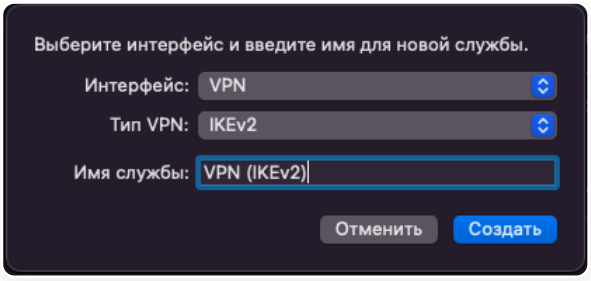
- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в разделе Сервисы → Сертификаты → Загруженные сертификаты.

Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки** → **Сеть**.

2. Нажмите **Добавить** в левом нижнем углу (иконка +).

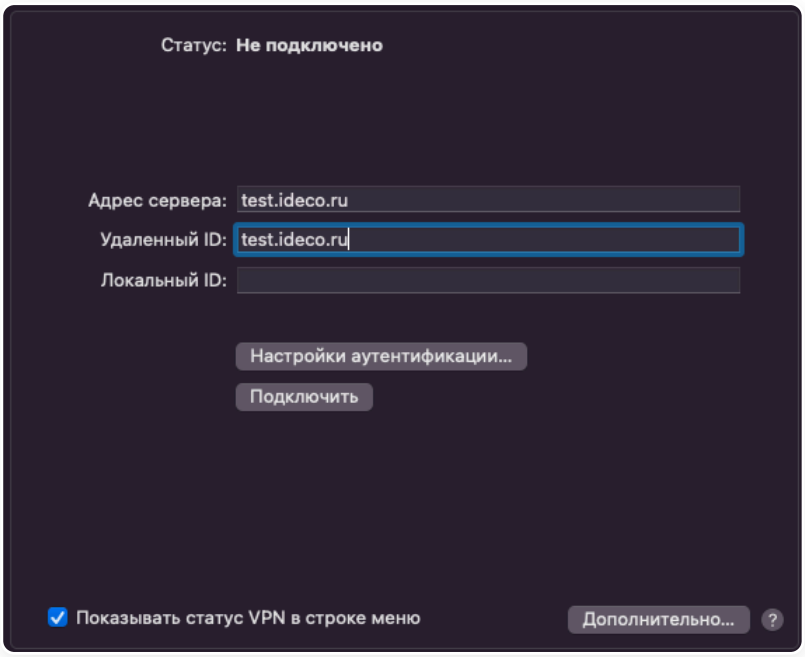
3. Заполните поля:



- **Интерфейс** - VPN;
- **Тип VPN** - IKEv2;
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

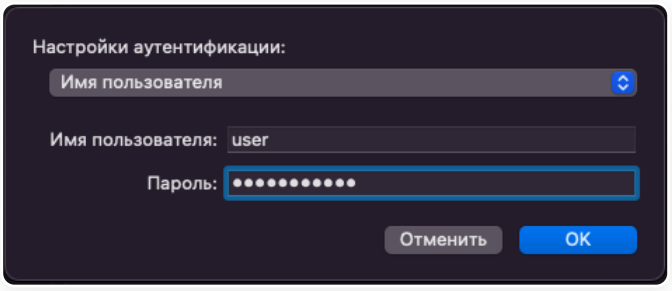
5. Установите параметры подключения:



- **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**.

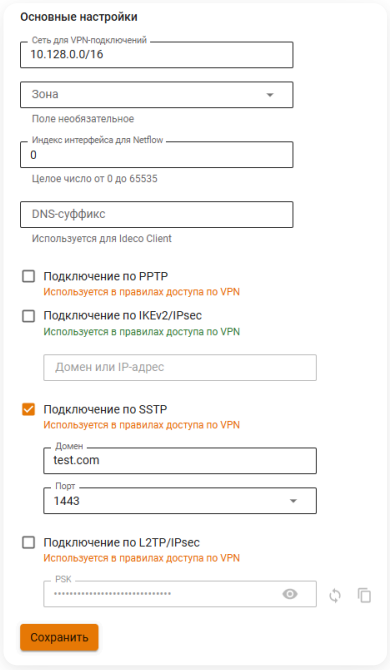
9. Поставьте флаг в пункте **Показывать статус VPN в строке меню**, нажмите **Применить** и включите соединение.

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе 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 командой:

```
sudo /usr/local/sbin/sstpc --cert-warn --tls-ext --user <логин пользователя Ideco NGFW> --password <Пароль пользователя Ideco
```

- 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 маршрутизация 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 оно было установлено, и нажмите **Ctrl+C**.

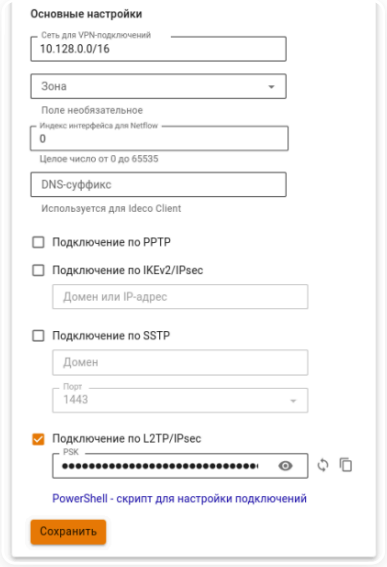
L2TP/IPsec

Важно: L2TP IPsec-клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их более одного. Рекомендуем вместо L2TP IPsec использовать IKEv2 IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

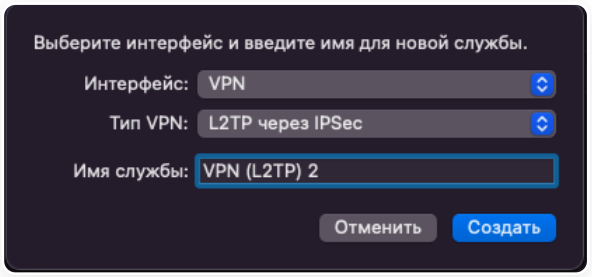
2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки** → **Сеть** и нажмите **Добавить** в левом нижнем углу (иконка (+)).

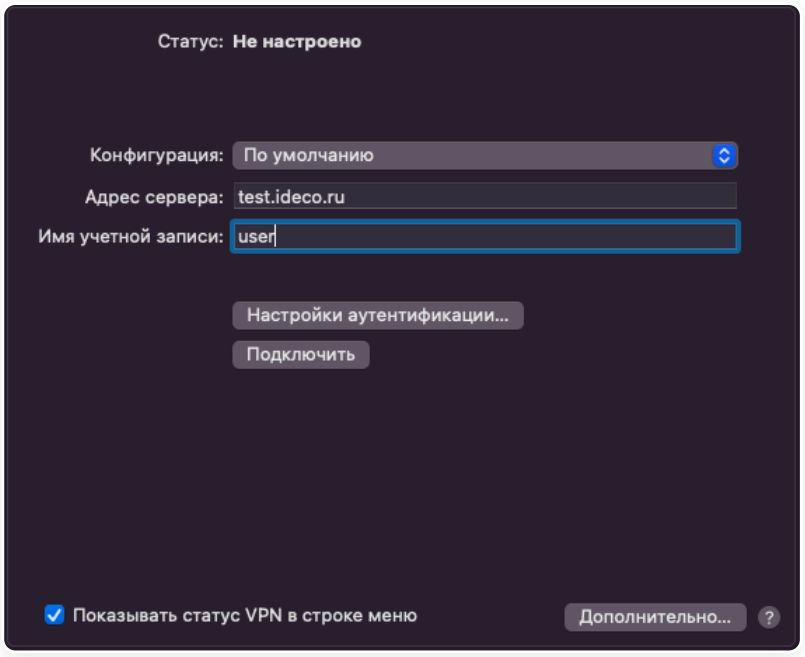
3. Заполните поля:



- **Интерфейс** - VPN;
- **Тип VPN** - L2TP через IPsec;
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

5. Заполните **Адрес сервера** и **Имя учетной записи**:



6. Поставьте флаг на пункте **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.

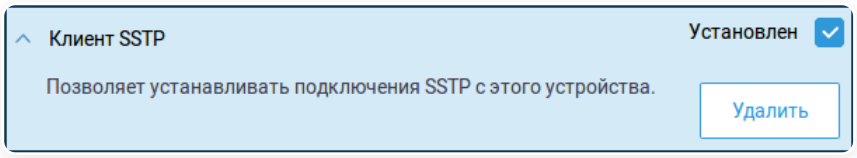
Подключение по SSTP Wi-Fi-роутеров Keenetic

Поддерживаются все роутеры на базе KeeneticOS 3.x.x.

1. Выполните настройку пользователей в Ideco NGFW и включите SSTP в разделе **Пользователи** → **VPN-подключения** → **Основное**.

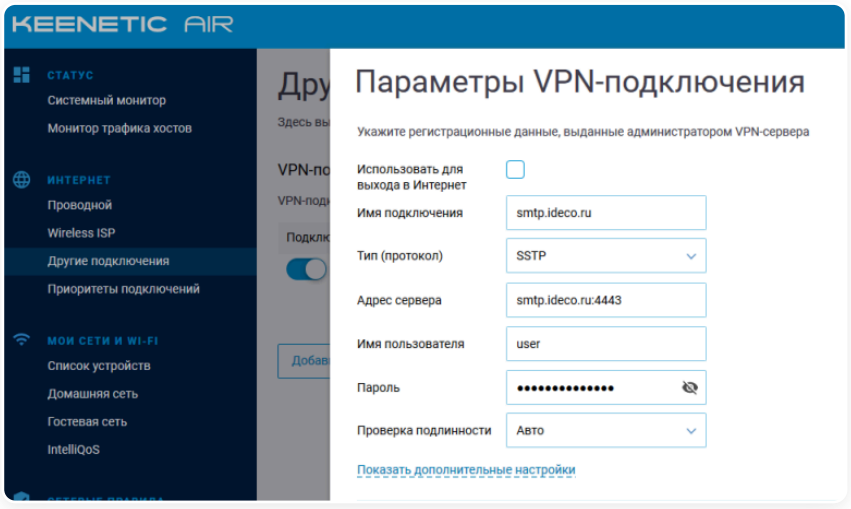
2. Зайдите в веб-интерфейс управления Keenetic: `http://my.keenetic.net`.

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.

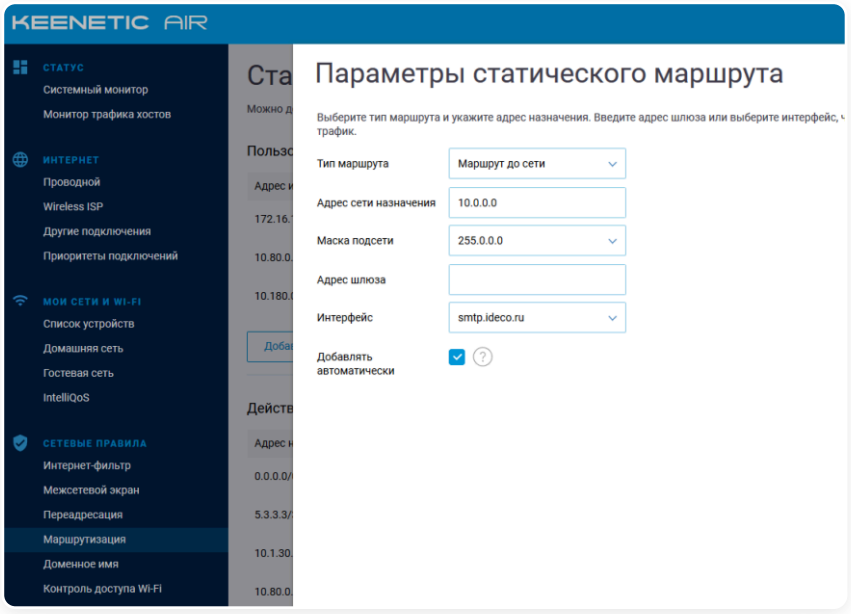
4. Создайте подключение в разделе **Интернет** → **Другие подключения** нажмите кнопку **Добавить подключение**



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.

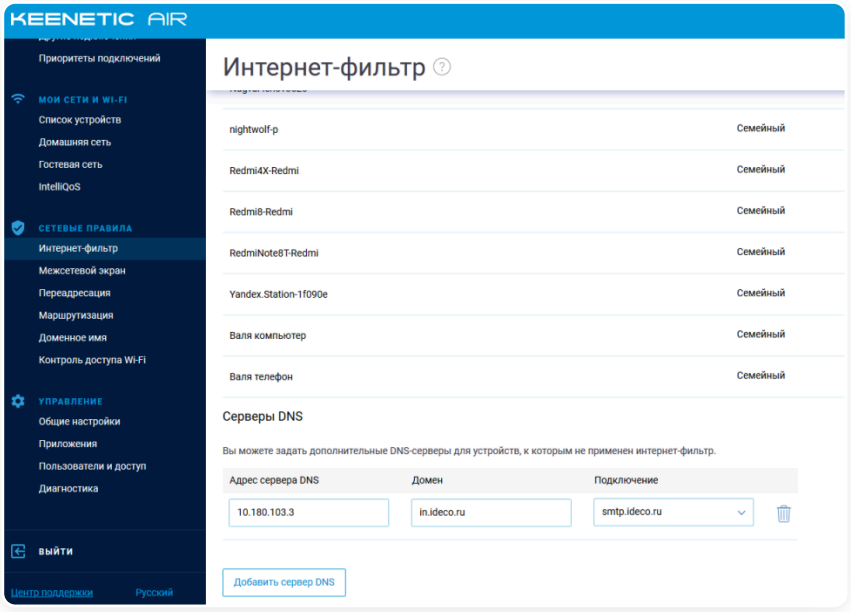
5. В разделе **Сетевые правила** → **Маршруты** добавьте маршруты в рабочую сеть. Например, если сеть офиса `10.0.0.0/8`, добавьте маршрут:



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 разделе **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.

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.

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.

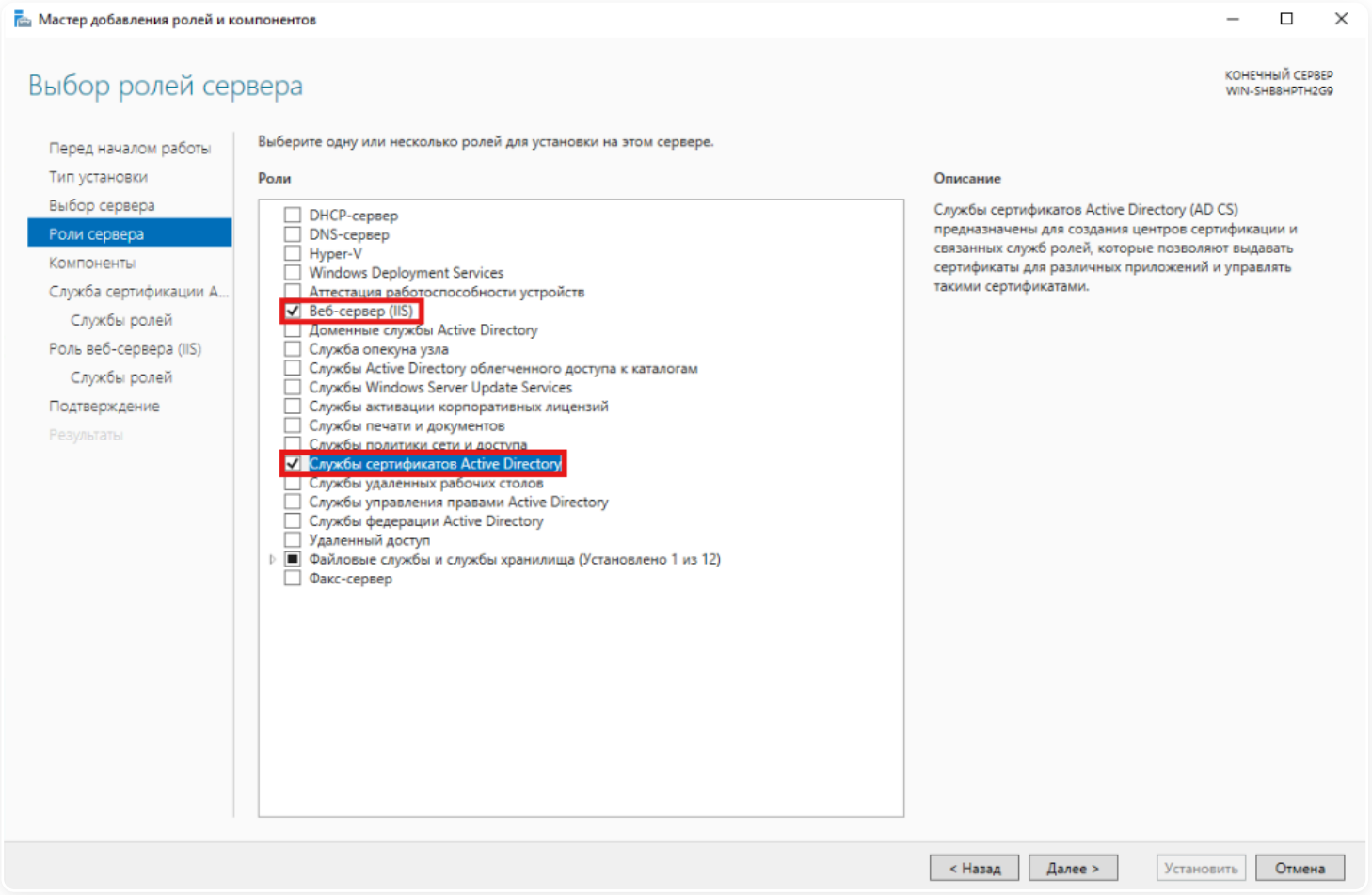
AuthorityInformationAccess

- `Empty=True` - не добавляет URL-адрес AIA в сертификаты, выданные центром сертификации.

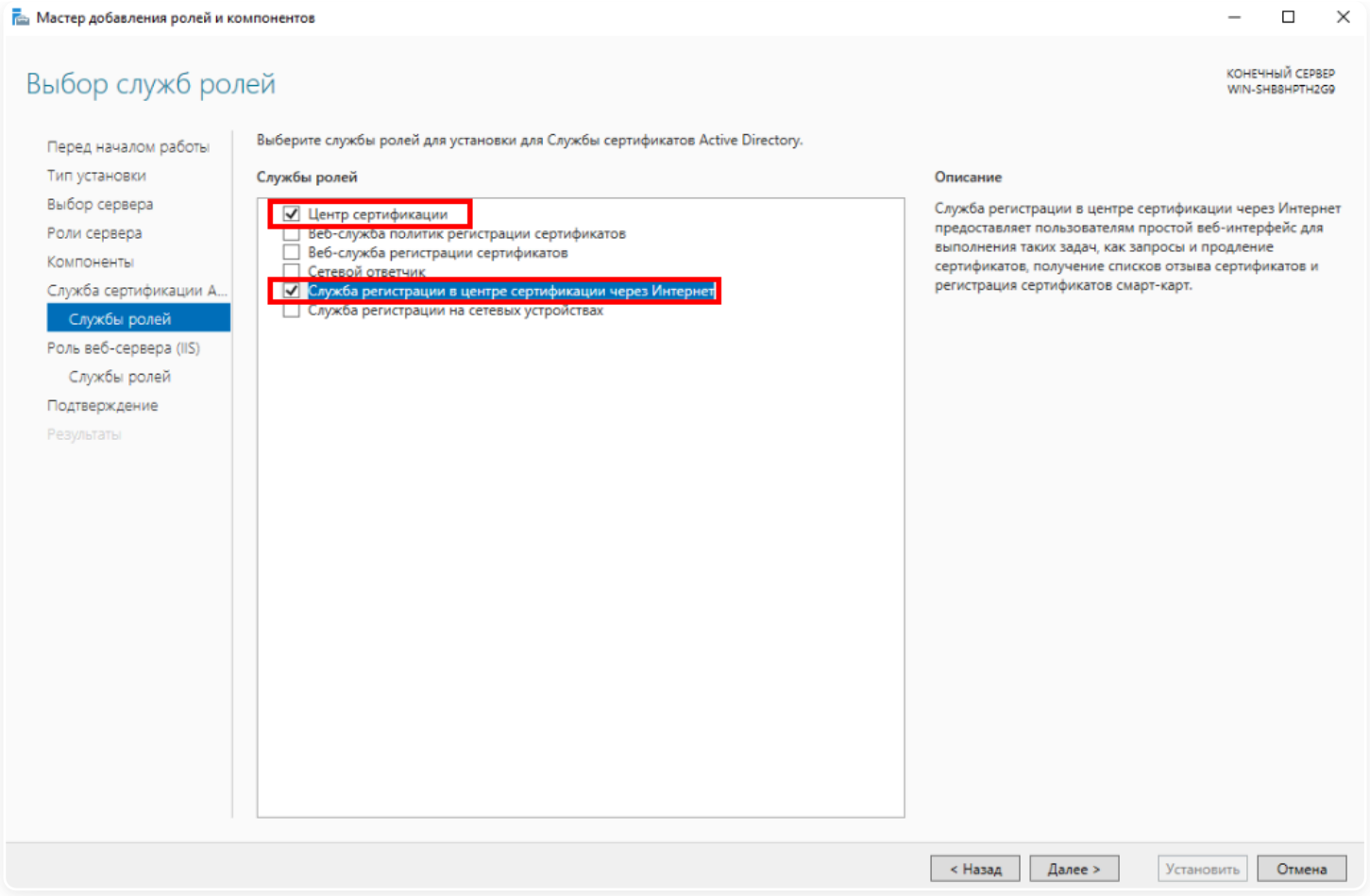
Шаг 2. Установка ролей служб сертификации

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**:

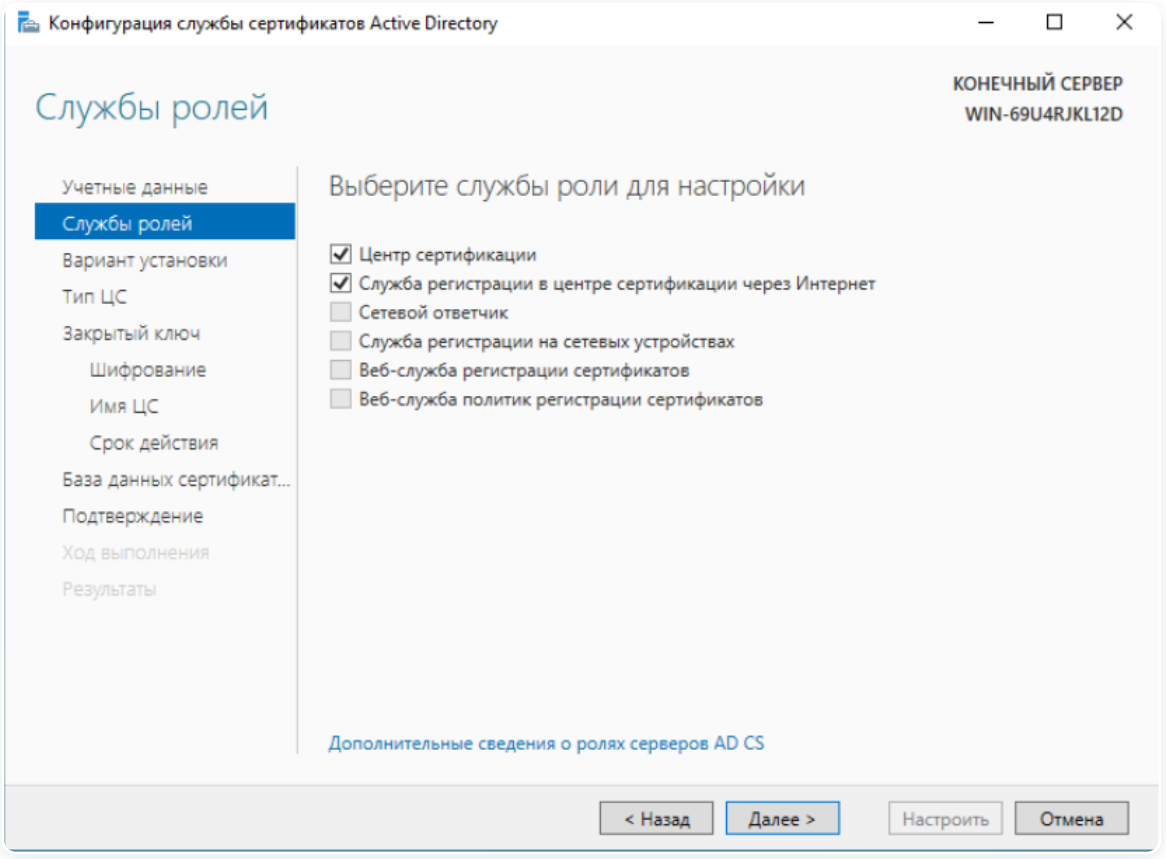


4. Завершите установку.

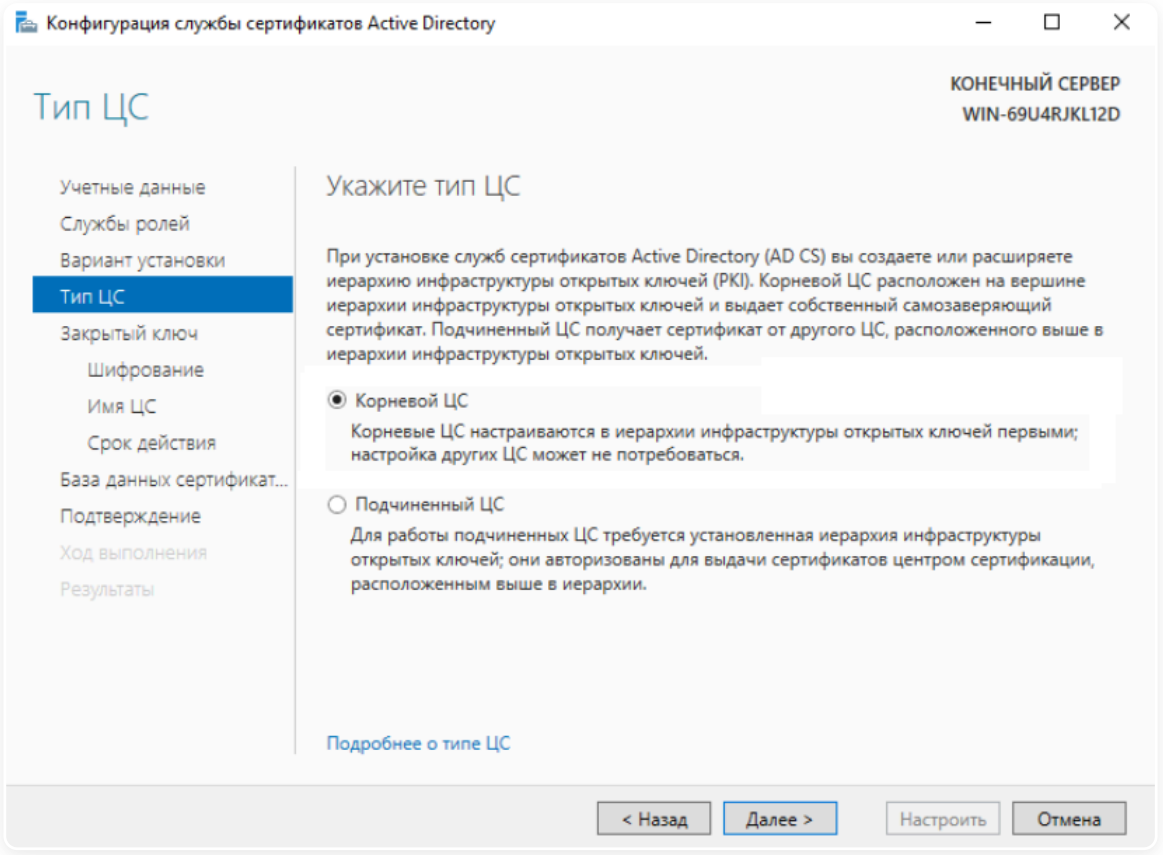
Шаг 3. Настройка служб сертификации

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

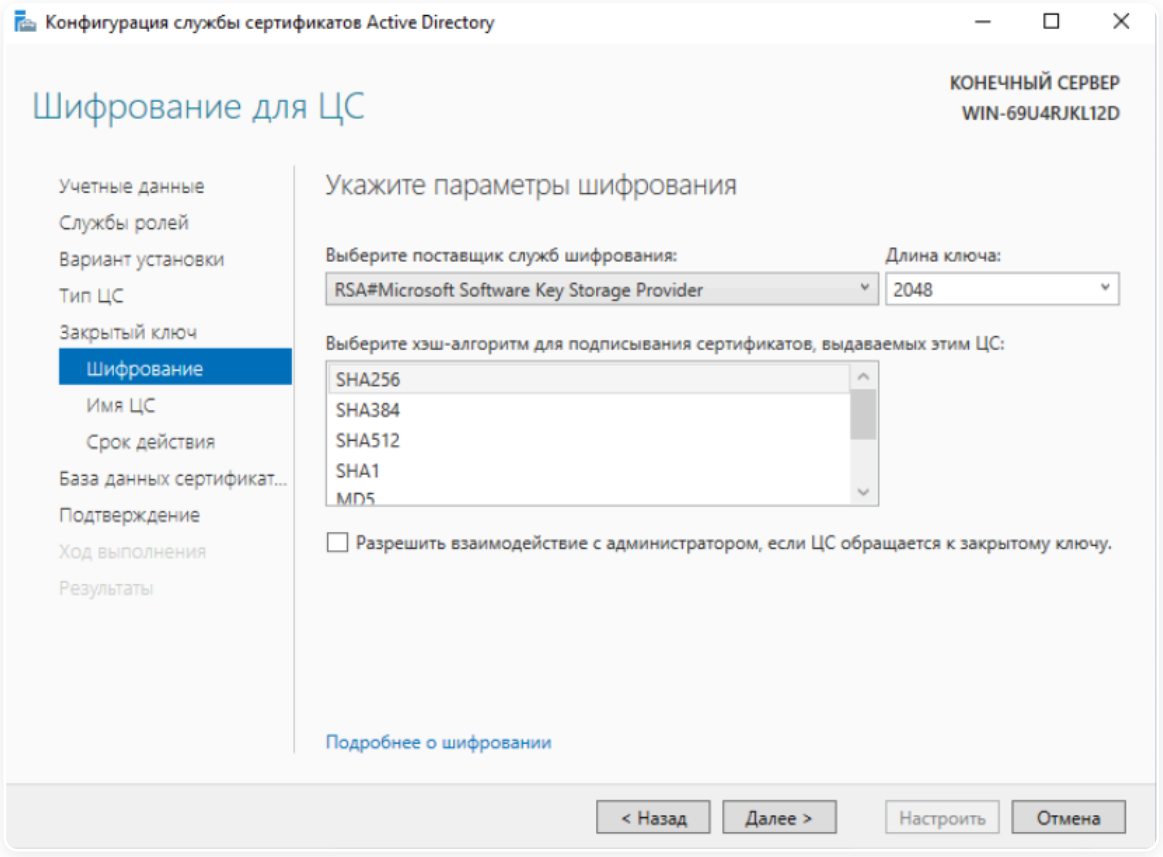
2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



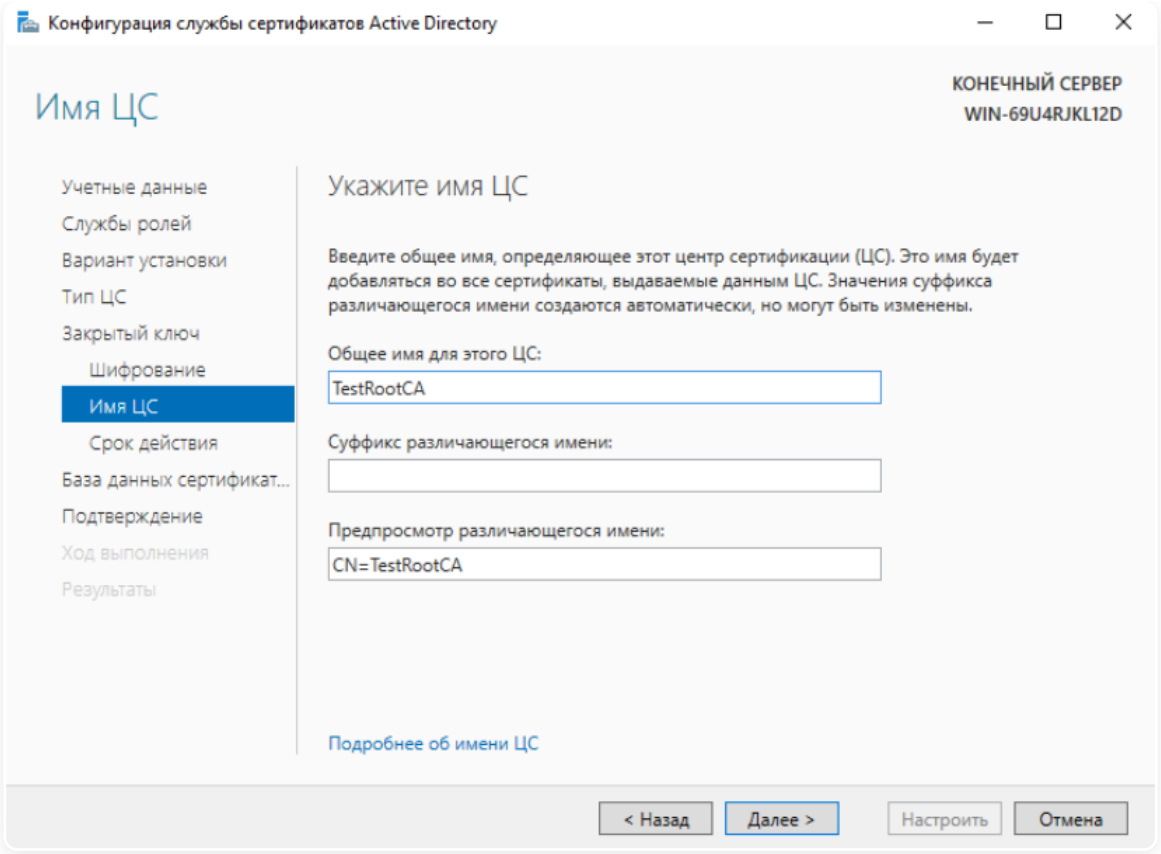
3. На этапе **Тип ЦС** выберите **Корневой ЦС**:



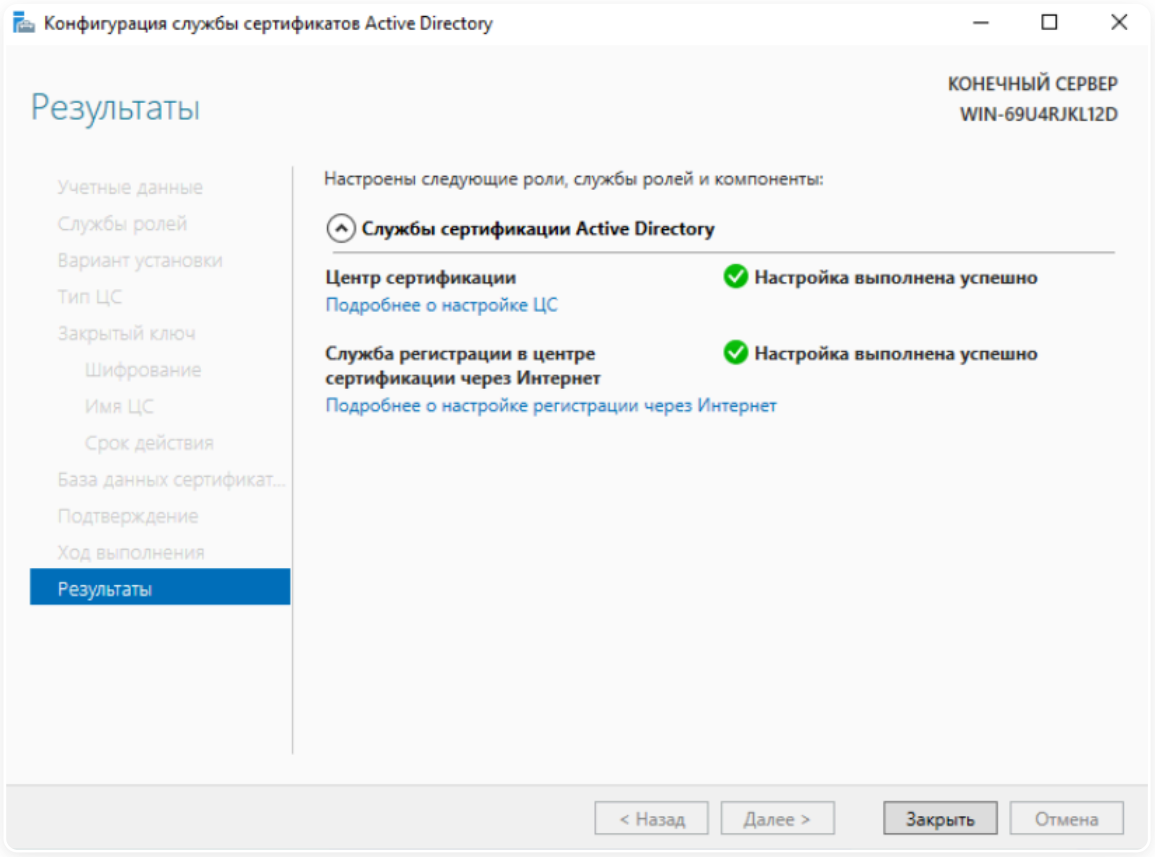
4. На этапе **Шифрование** убедитесь, что выбран алгоритм **SHA256**:



5. На этапе **Имя ЦС** задайте имя (например, `TestRootCA`):



6. Завершите настройку:



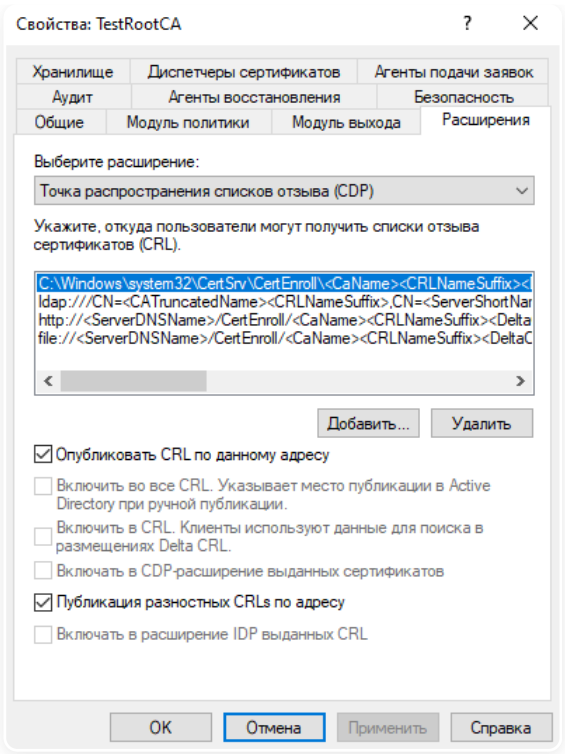
Шаг 4. Настройка точек распространения (CDP/AIA)

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**.

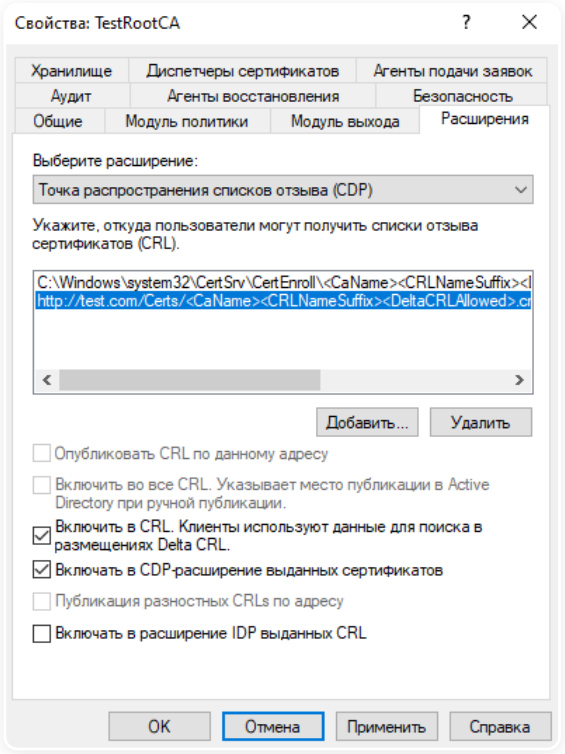
3. На вкладке **Расширения** выберите расширение **Точка распространения списков отзыва (CDP)**.

4. Удалите пути, начинающиеся с `ldap://`, `file://` и `http://`:



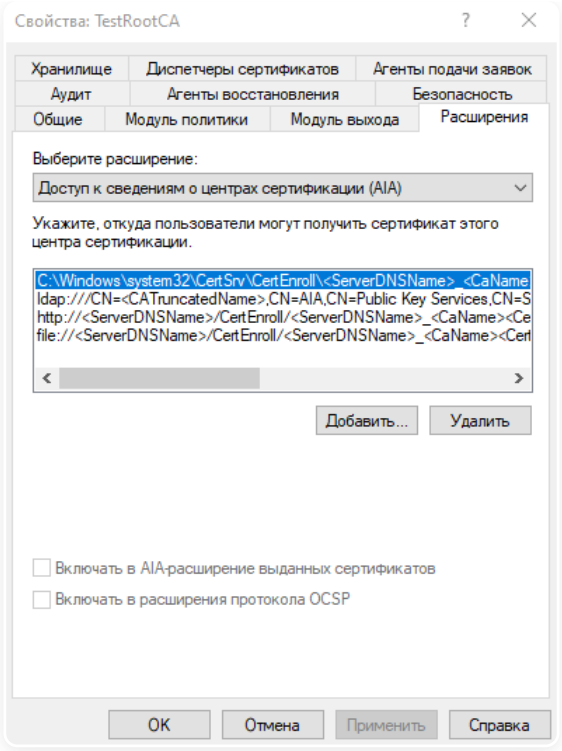
5. Нажмите **Добавить** и введите URL `http://<домен-сервера>/Certs/`. Затем добавьте переменные `<CaName>`, `<CRLNameSuffix>` и `<DeltaCRLAllowed>` после `Certs/`. Конечный путь будет выглядеть так: `http://test.com/Certs/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.

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 → OK**.

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)

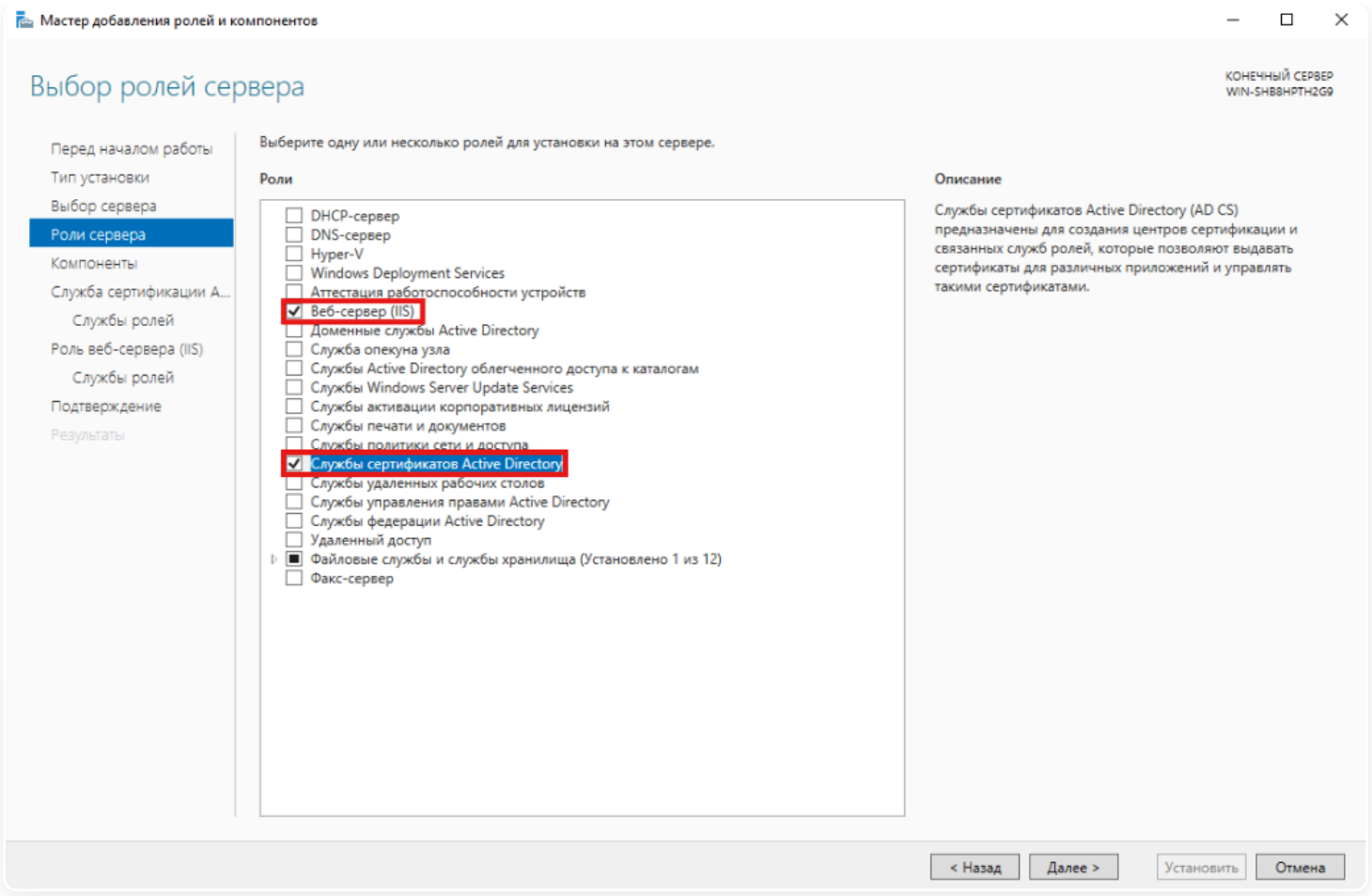
Шаг 1. Установка доверия к корню и установка ролей

На подчиненном центре сертификации (контроллере домена):

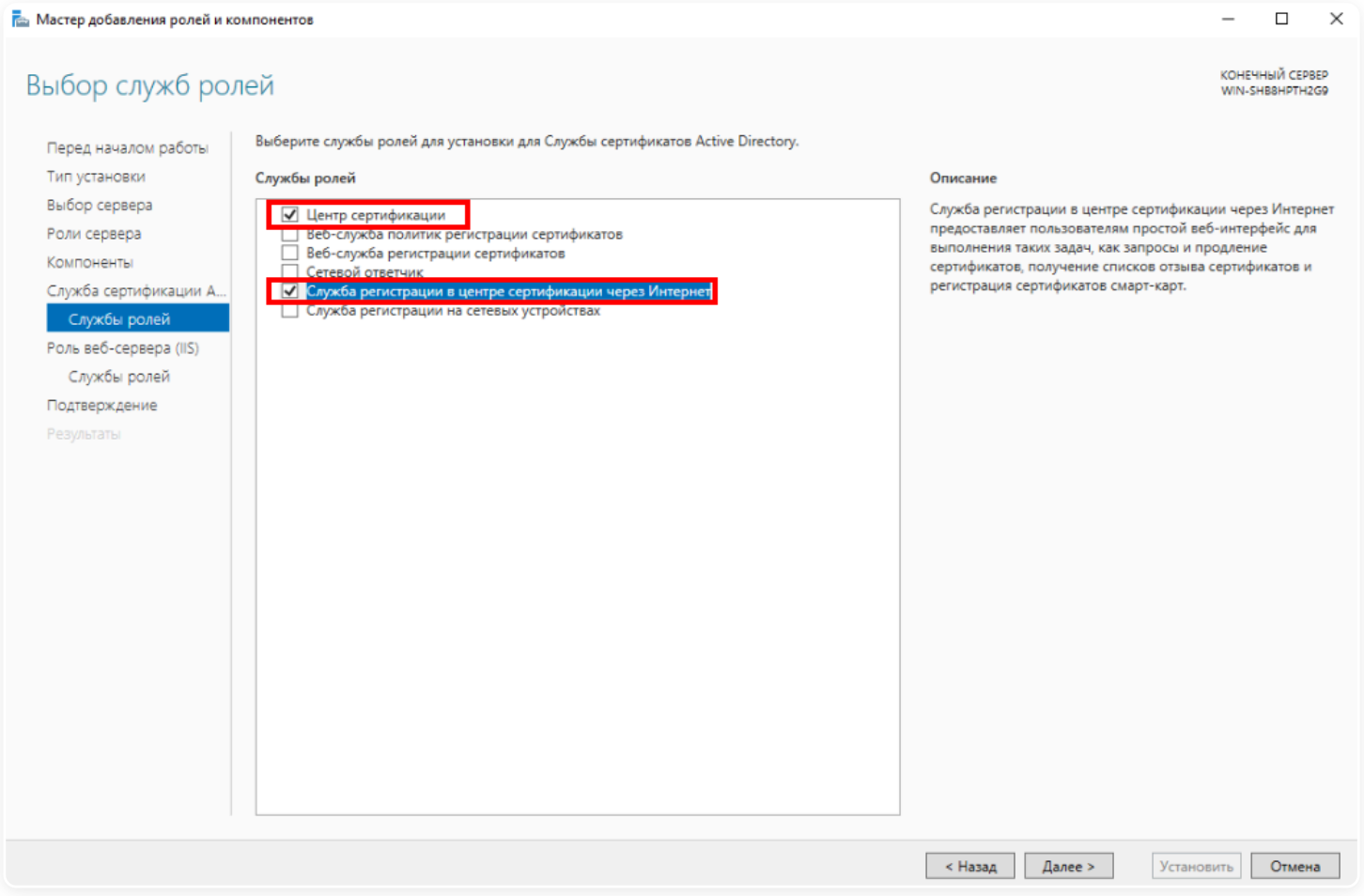
1. Установите сертификат `Root_CA.cer` в хранилище **Доверенные корневые центры сертификации** для локального компьютера.

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**:

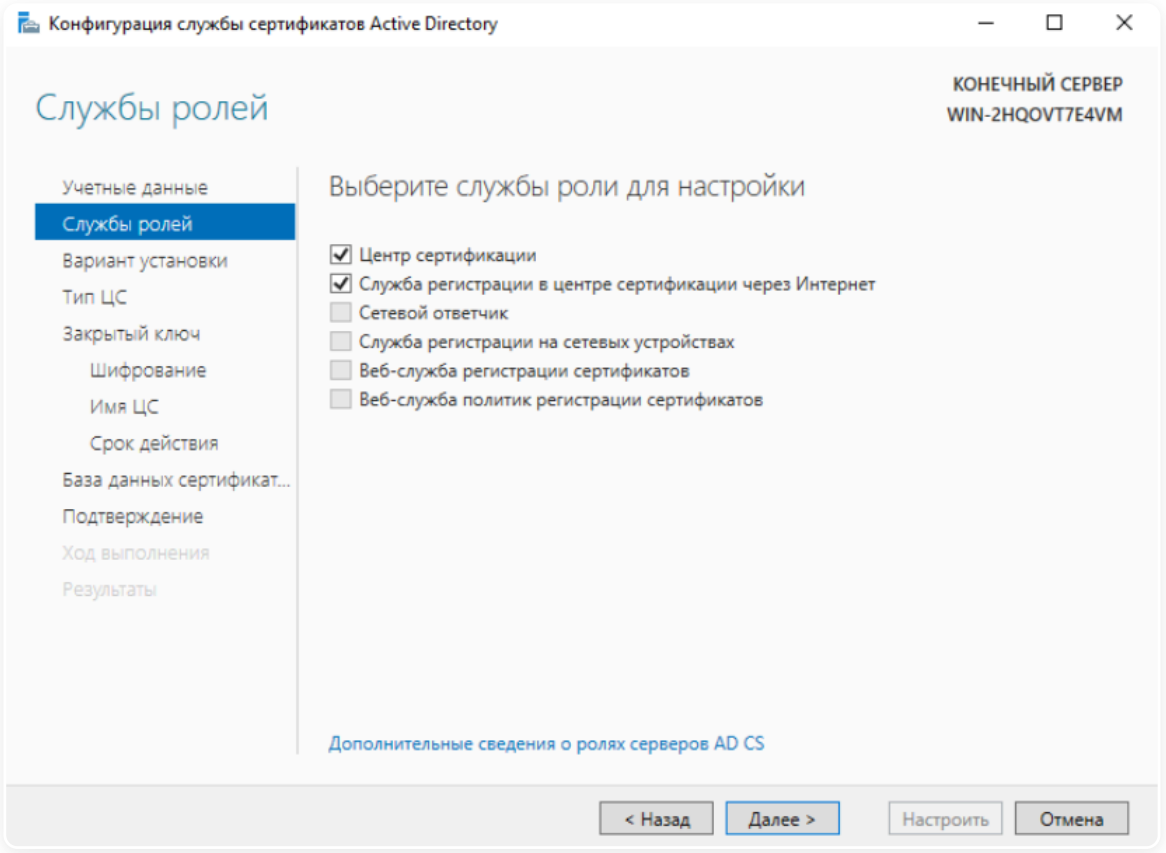


5. Завершите установку.

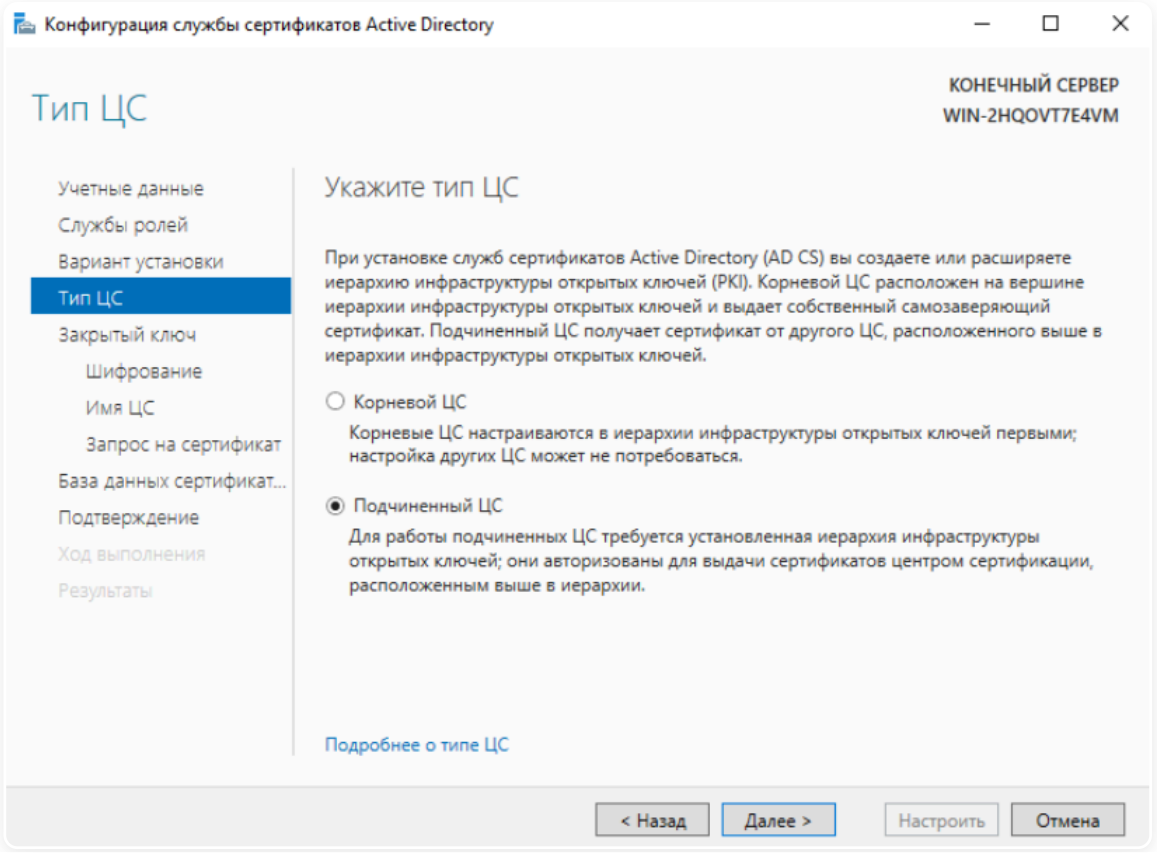
Шаг 2. Настройка подчиненного центра сертификации и создание запроса (CSR)

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

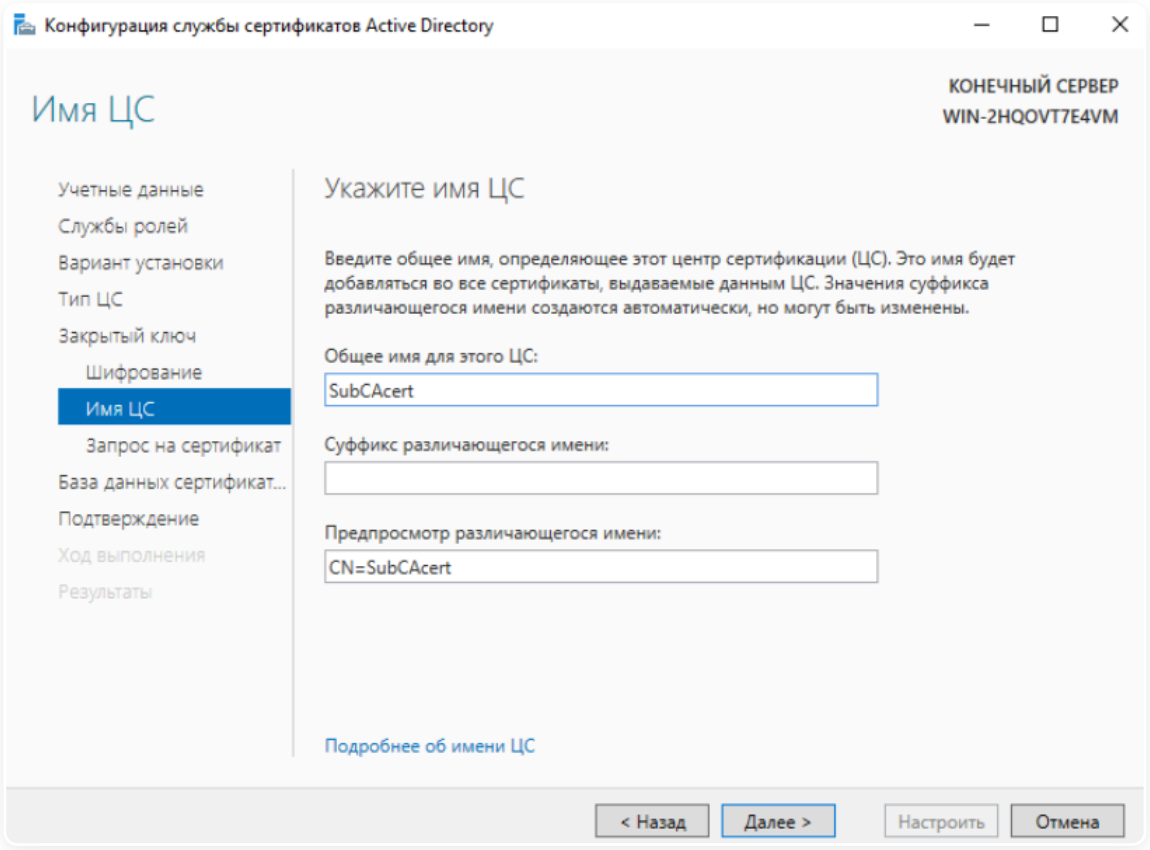
2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



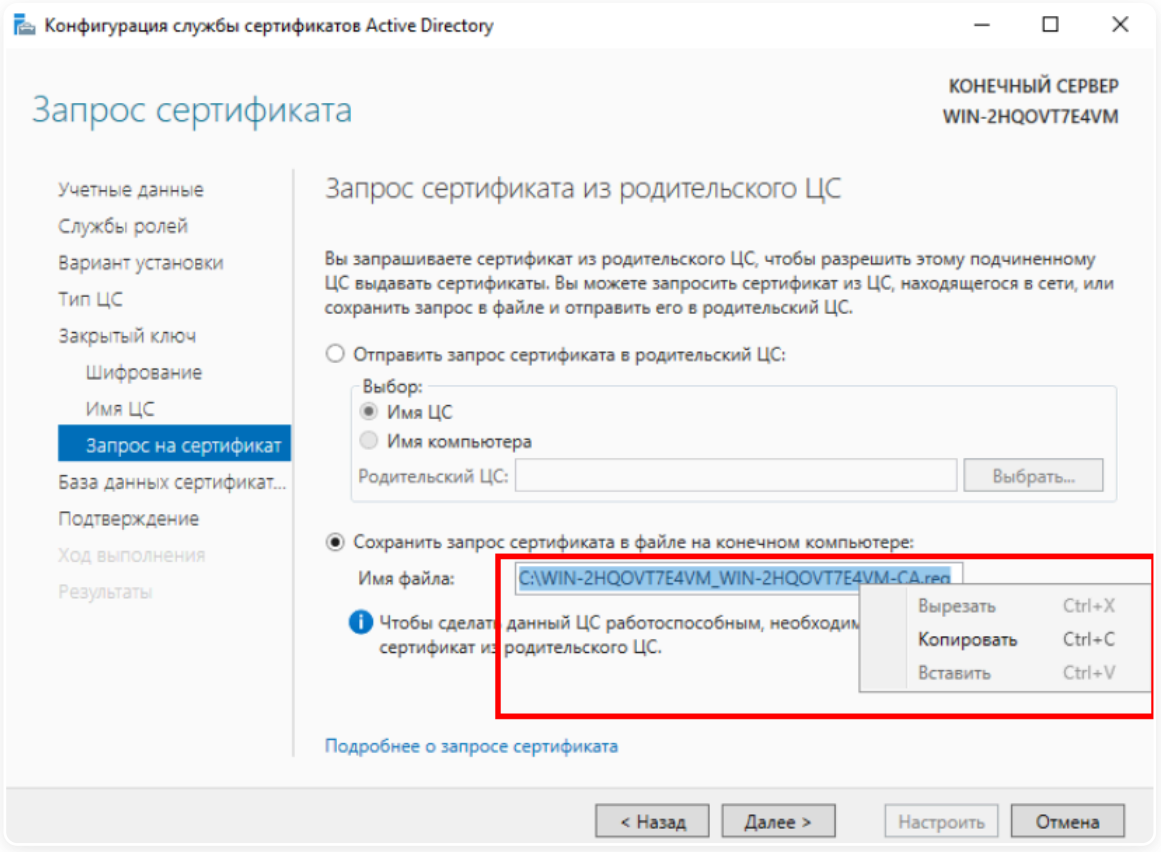
3. На этапе **Тип ЦС** выберите **Подчиненный ЦС**:



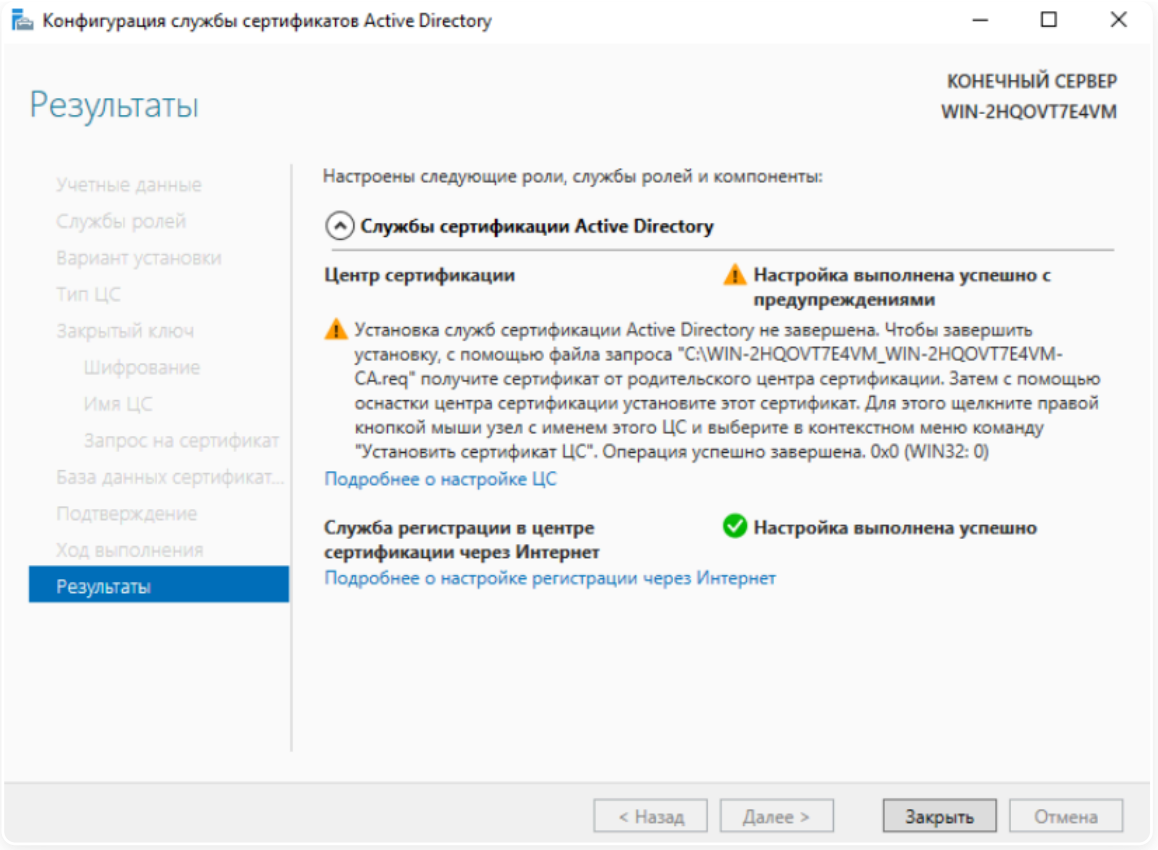
4. На этапе **Имя ЦС** задайте имя (например, `SubCAcert`):



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

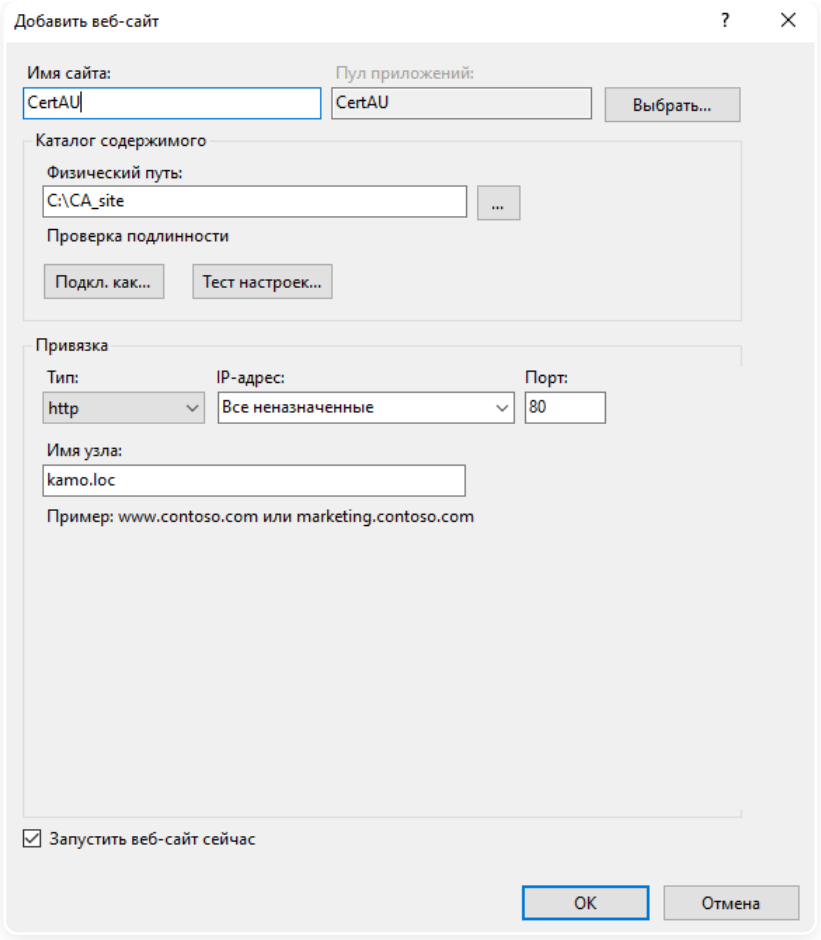
1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. На подчиненном центре сертификации нажмите правой кнопкой мыши **Установить сертификат ЦС** и выберите скачанный файл. Установите файл в папку **Доверенные корневые центры сертификации**.

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

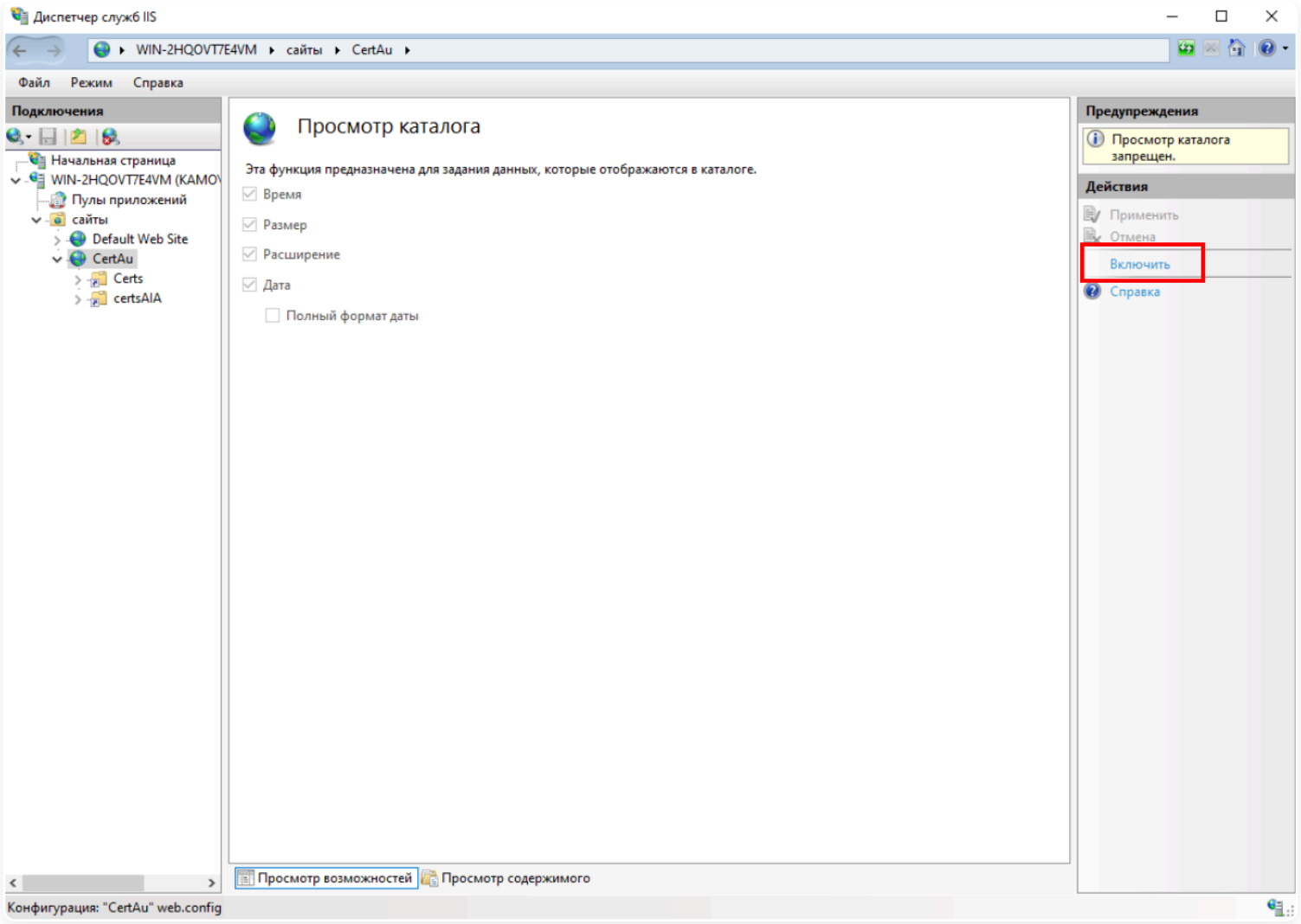
1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Диспетчер служб IIS**.

2. Нажмите правой кнопкой мыши по узлу сервера, выберите **Добавить веб-сайт** и заполните поля:

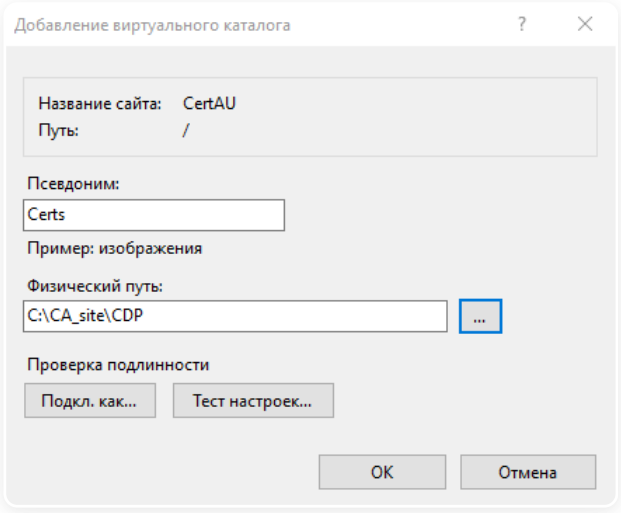


- **Имя сайта** - введите `CertAU`.
- **Физический путь** - создайте новую папку `CA_site` по пути `C:\CA_site`.
- **Имя узла** - укажите доменное имя, по которому будет доступен сайт, например, `marketing.contoso.com`.

3. После добавления веб-сайта перейдите в раздел **Просмотр каталогов** и нажимите **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:

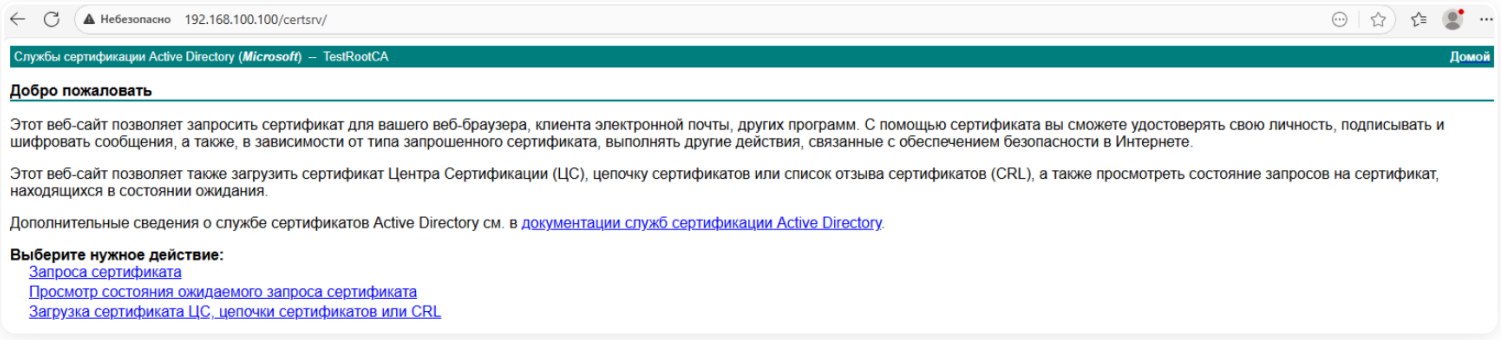
- Для CDP: **Включить в CRL** и **Включать в CDP-расширение выданных сертификатов**.
- Для AIA: **Включать в AIA-расширение выданных сертификатов**.

Шаг 6. Получение сертификата от корневого центра сертификации

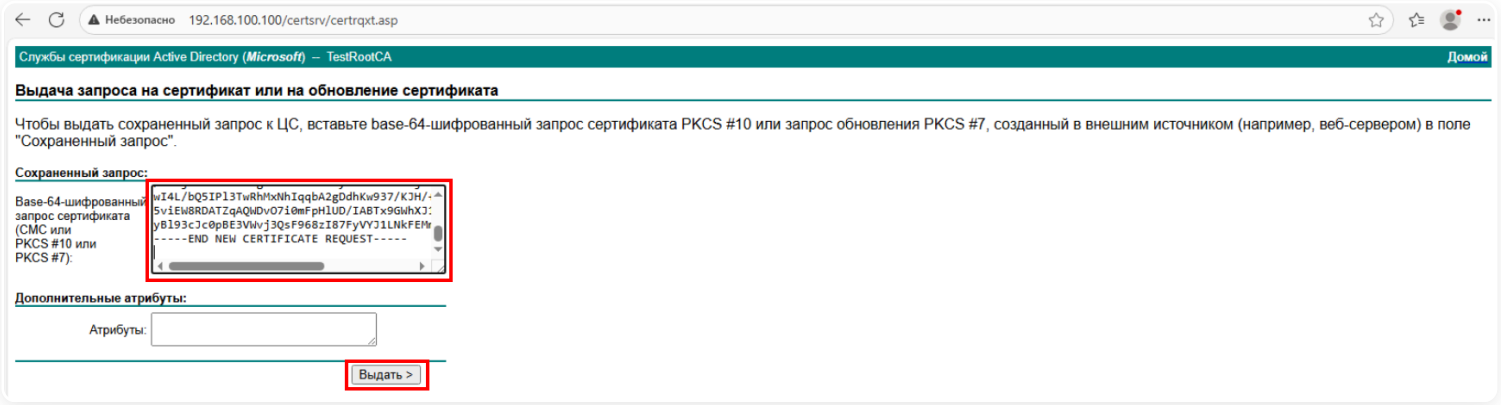
1. Откройте файл `.req` в блокноте и скопируйте текст.

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.

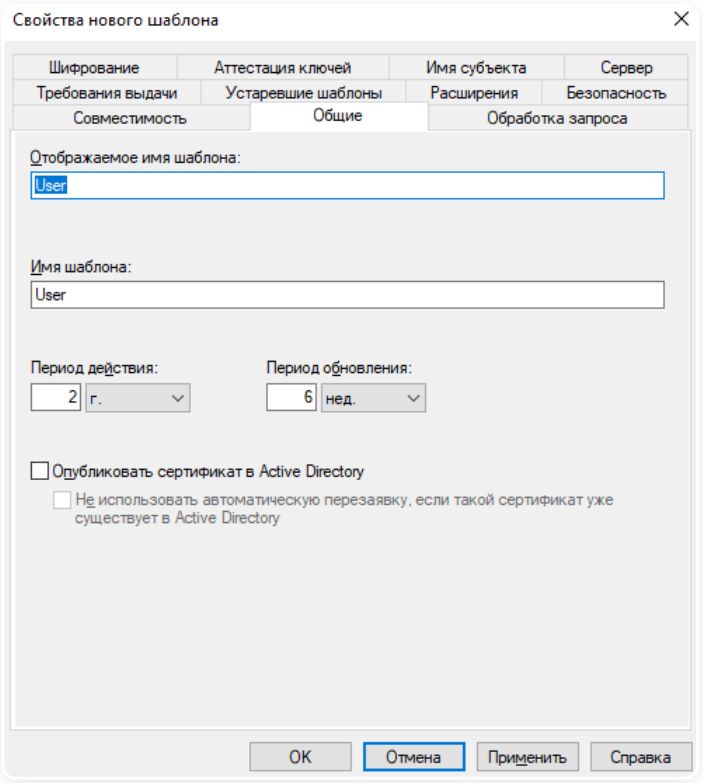
Создание шаблона сертификата и тестовая выдача

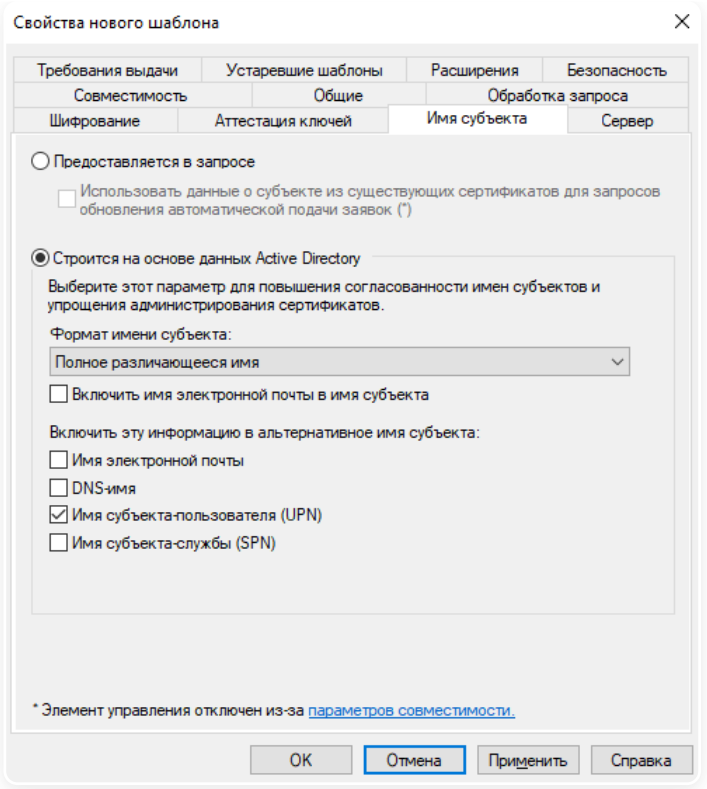
Шаг 1. Создание шаблона сертификата

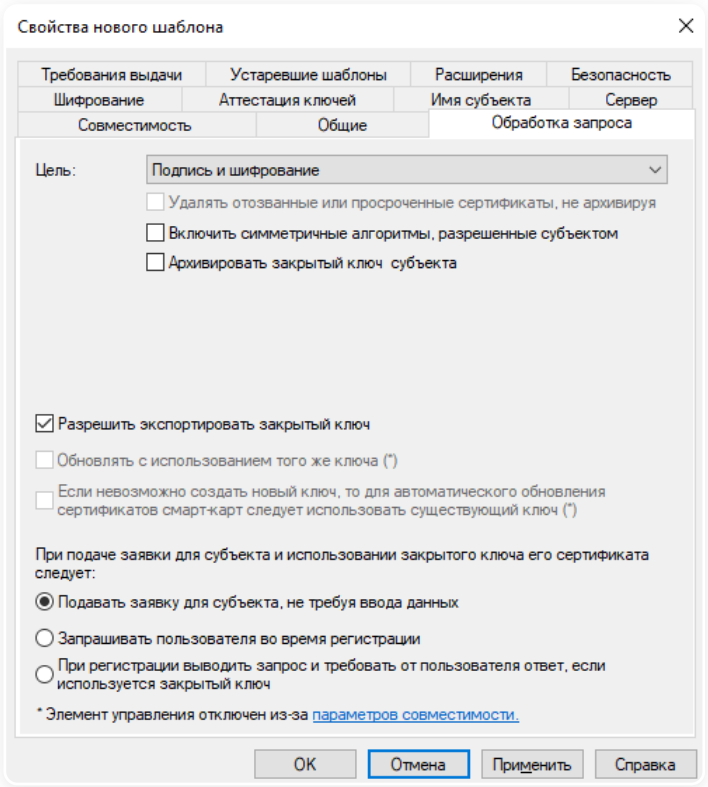
1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на папку **Шаблоны сертификатов** и выберите **Управление**.

2. Найдите шаблон **Пользователь**, нажмите правой кнопкой мыши и выберите **Скопировать шаблон**.

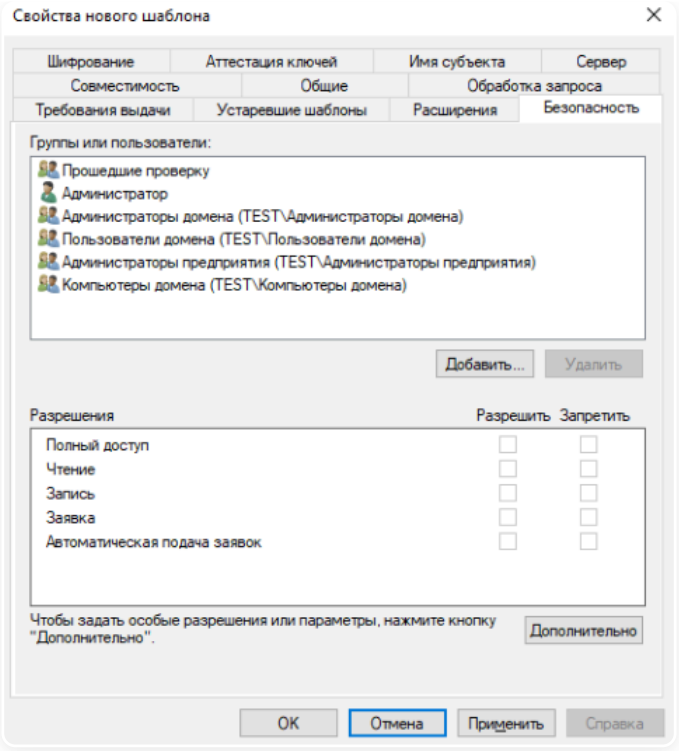
3. Настройте шаблон в соответствии с вашими требованиями (имя, срок действия, криптопровайдеры и так далее):







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**.

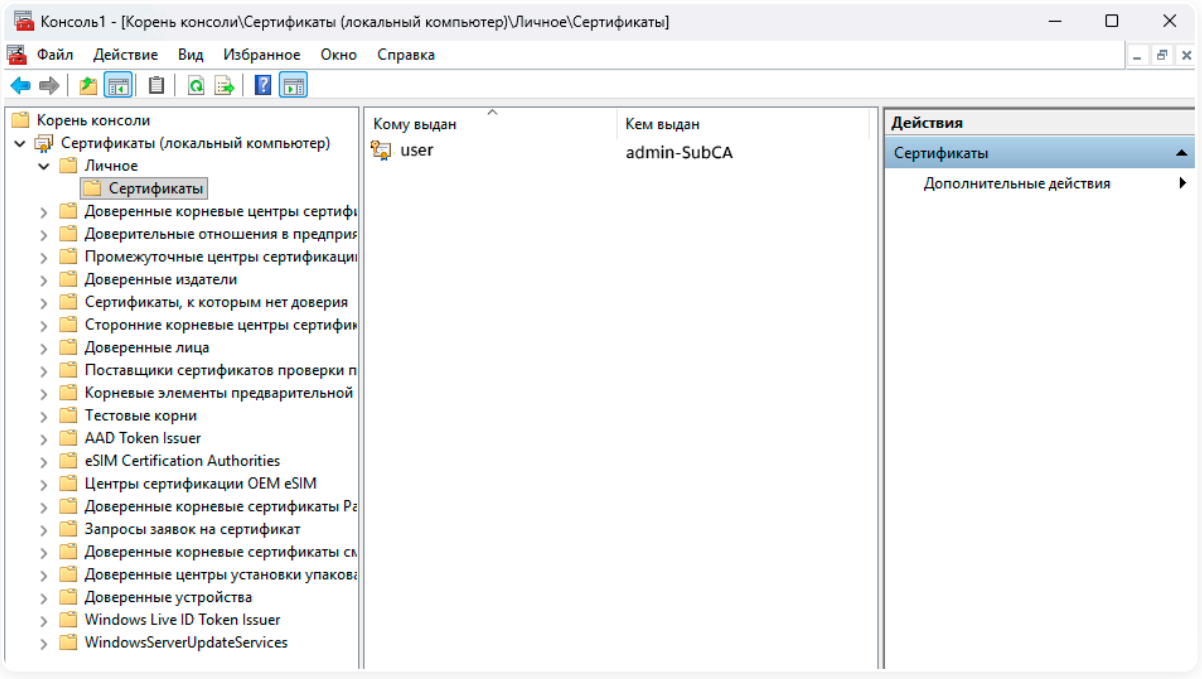
4. Выберите **Сертификаты** и нажмите **Добавить**.

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:



Настройка Wi-Fi-сети

В текущей версии Ideco NGFW 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. Способ авторизации зависит от режима работы маршрутизатора.

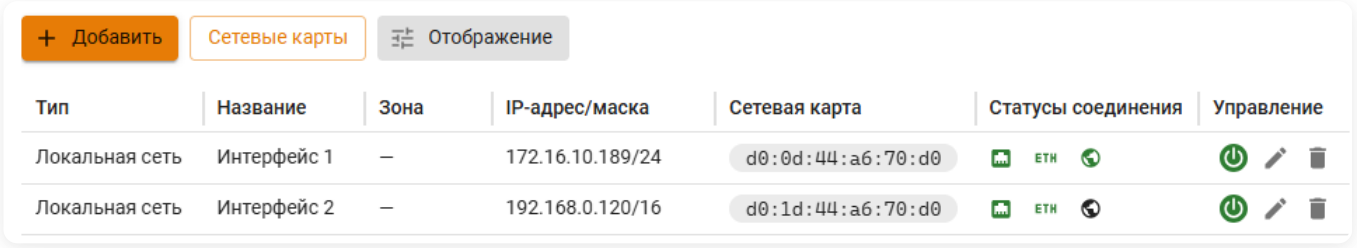
Режим точки доступа или bridge

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 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 и укажите 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, то в **Файрволе** запретите доступ из беспроводной сети в локальную сеть.

Пример настройки интерфейса для клиентов, подключающихся по Wi-Fi:



- **172.16.10.189/24** - шлюз для беспроводной Wi-Fi-сети.
- **192.168.0.120/16** - шлюз для локальной Ethernet-сети.

Настройка DHCP

1. В **Сервисы** → **Сетевые интерфейсы** создайте отдельный интерфейс для клиентов Wi-Fi с автоматической конфигурацией через 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**.

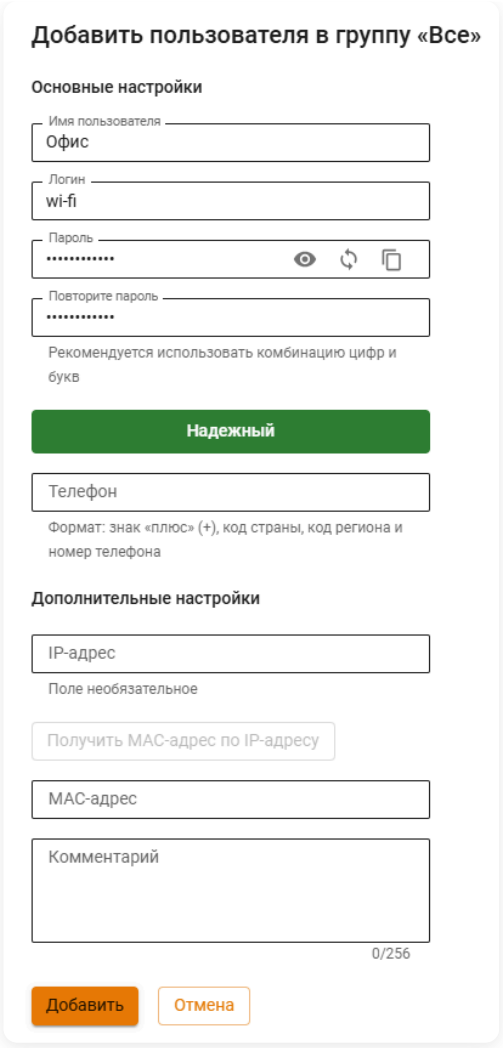
Для индивидуальной авторизации Wi-Fi-пользователей и учета их трафика и статистики воспользуйтесь авторизацией через веб-браузер. При таком способе авторизации Ideco NGFW будет учитывать каждого пользователя, подключившегося по Wi-Fi. Это следует принять во внимание при планировании лицензирования Ideco NGFW.

Режим роутера

В режиме роутера устройство Wi-Fi скрывает за NAT устройства беспроводной сети. Таким образом, для Ideco NGFW 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 авторизация**.

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, поскольку 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 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.

Подключение к Ideco NGFW по COM-порту

Установка Ideco NGFW по COM-порту

COM-порт по умолчанию включен.

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

Шаг 1. Создание загрузочного USB-накопителя

Создайте загрузочный USB-накопитель Ideco NGFW. 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, если опция **Console Redirection** отсутствует в BIOS или выключена.
> - Процесс загрузки сервера, начиная с BIOS и заканчивая установщиком Ideco NGFW, если опция **Console Redirection** включена.

2. Выполните установку Ideco NGFW.

Управление Ideco NGFW 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 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**

Анализ трафика

Используйте утилиту `tcpdump` для анализа трафика на NGFW в разделе **Управление сервером → Терминал**.

Утилита `tcpdump` предустановлена в продукт Ideco NGFW.

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 его 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

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:

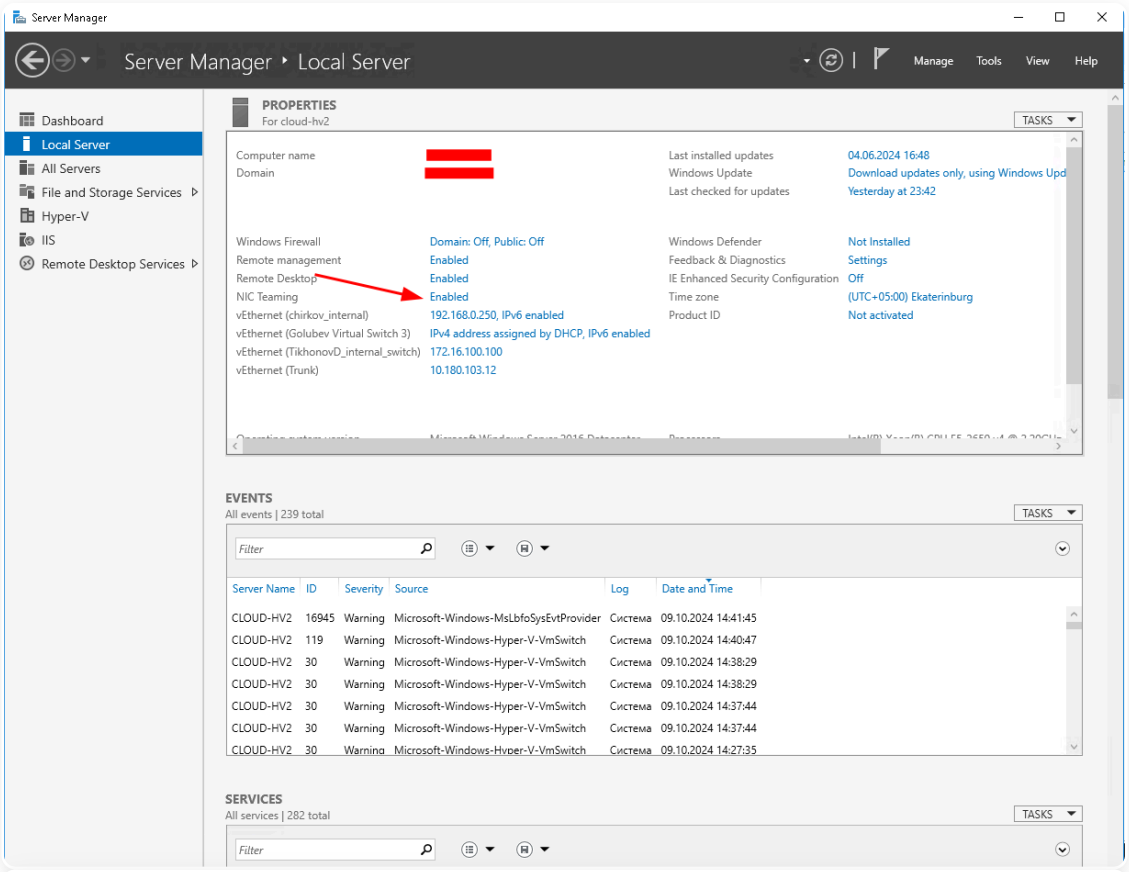
```
tcpdump -i any port 500
```

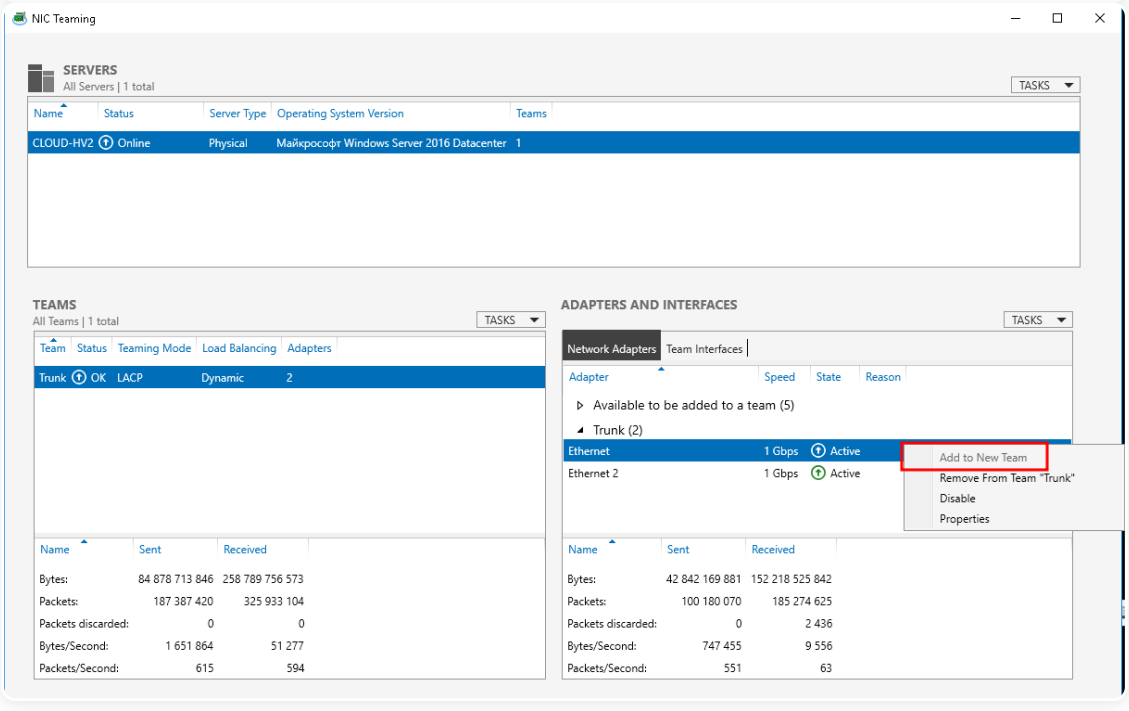
Настройка LACP на Hyper-V

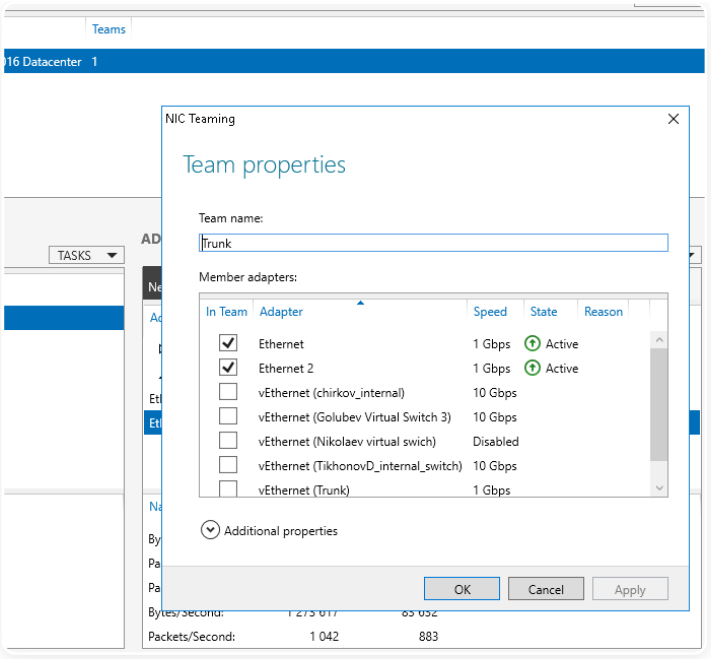
Для настройки LACP на гипервизоре Hyper-V существуют два способа:

Настройка на хост системе

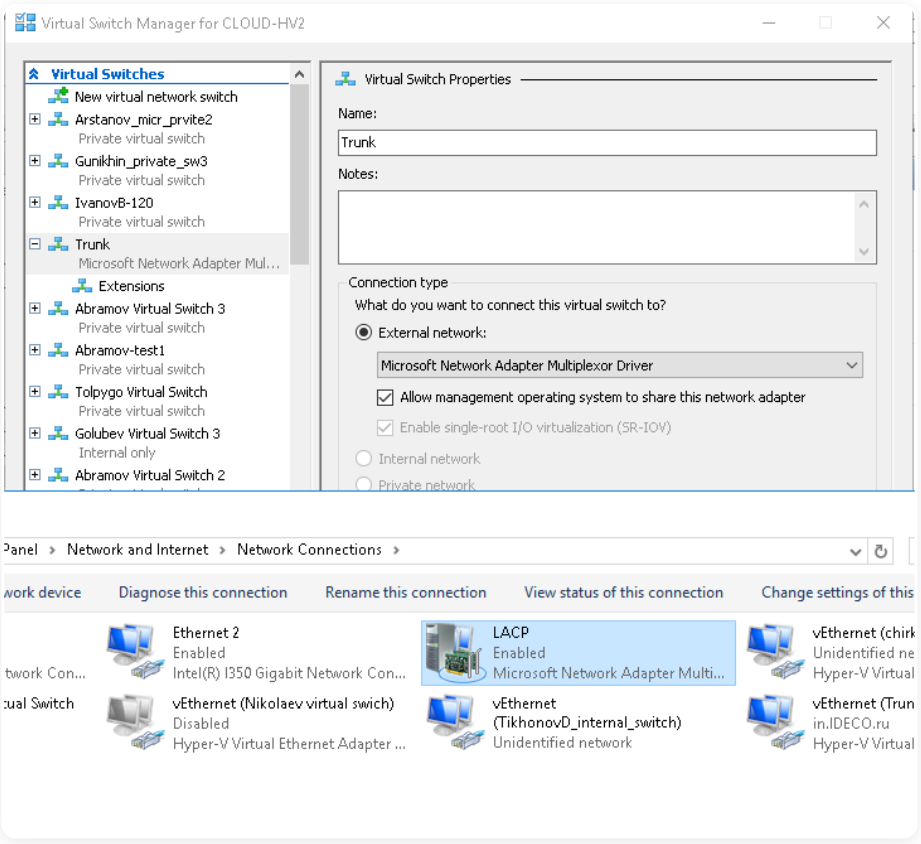
1. Объедините физические интерфейсы:







2. Выберите созданный интерфейс при настройке виртуального свитча:



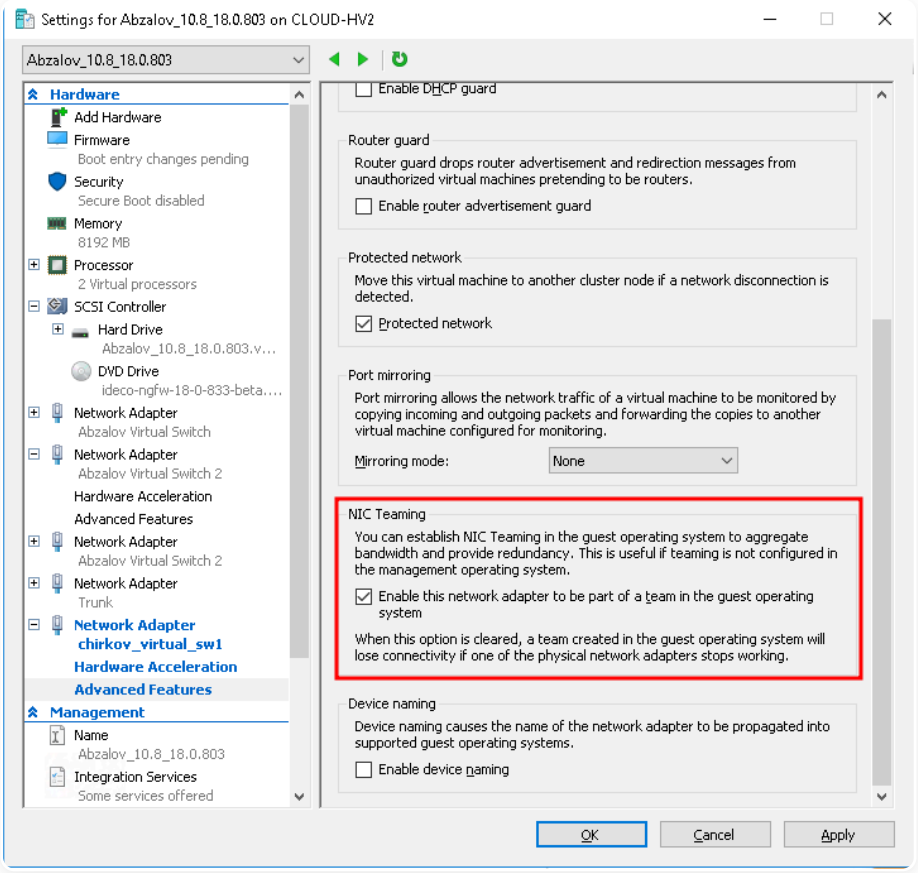
Получившийся виртуальный свитч можно использовать для добавления новых интерфейсов в LACP на гостевую систему.

3. Настройте подключение на вкладке **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 разделе **Сетевые интерфейсы → Агрегированные(LACP)**.

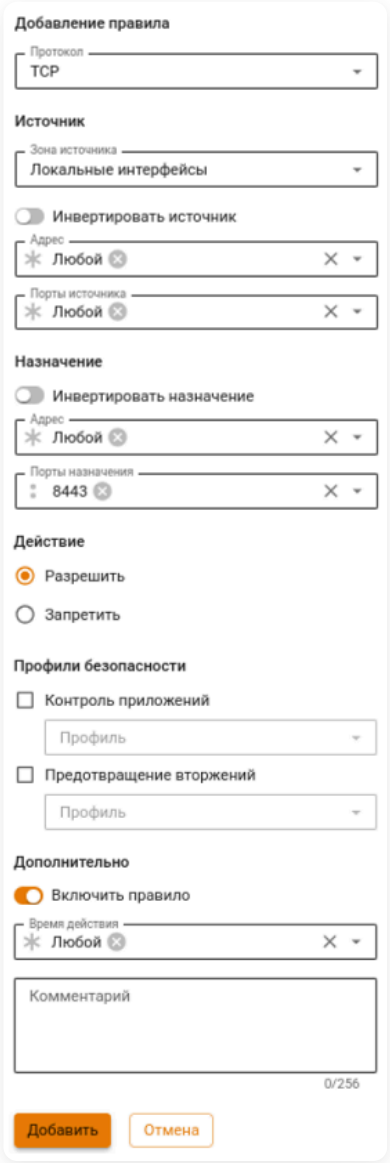
4. Настройте подключения на вкладке **Сетевые интерфейсы → Внешние и локальные**.

Как разрешить доступ к ресурсам в ограниченной сети

Разрешить доступ к веб-интерфейсу Ideco NGFW из локальной сети

Пример. Необходимо ограничить доступ ко всем внутренним ресурсам Ideco NGFW, кроме веб-интерфейса администратора Ideco NGFW.

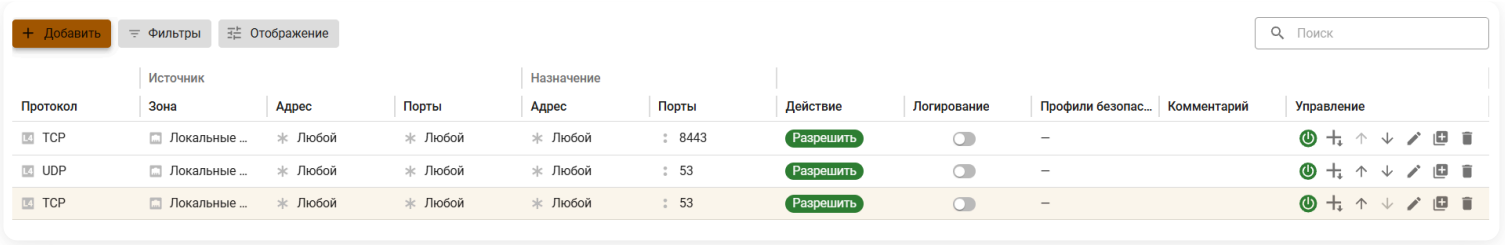
1. В разделе **Правила трафика** → **Файрвол** → **INPUT** создайте разрешающее правило, заполнив поля:



- **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.
- **Порт** - 8443.

Включите правило и нажмите **Добавить**.

2. Если Ideco NGFW 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:



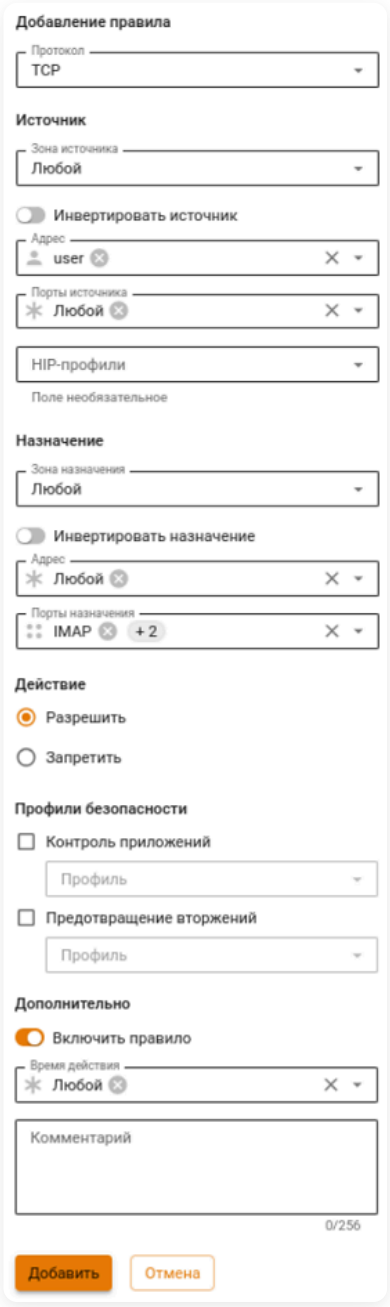
3. Создайте запрещающее весь трафик правило INPUT. При создании правила доступна опция **Включить правило** в разделе **Дополнительно**. Не включайте его, пока не убедитесь, что в таблице разрешающее правило находится выше запрещающего.

При потере доступа к веб-интерфейсу Ideco NGFW воспользуйтесь опцией **Включить режим 'Разрешить интернет всем'**.

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 разделе **Правила трафика** → **Файрвол** → **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 и их защищенных версий).

Включите правило и нажмите **Добавить**.

2. Создайте запрещающее весь трафик правило FORWARD. В таблице поместите разрешающее правило выше запрещающего.

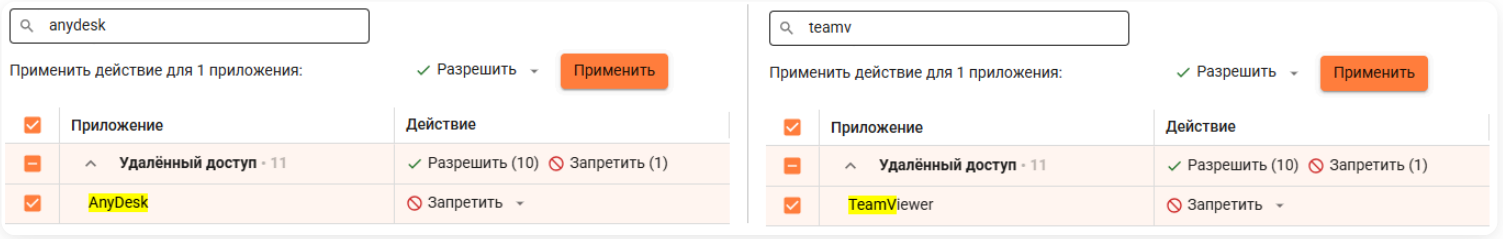
Разрешить трафик из локальной во внешнюю сеть, но запретить конкретные приложения

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.

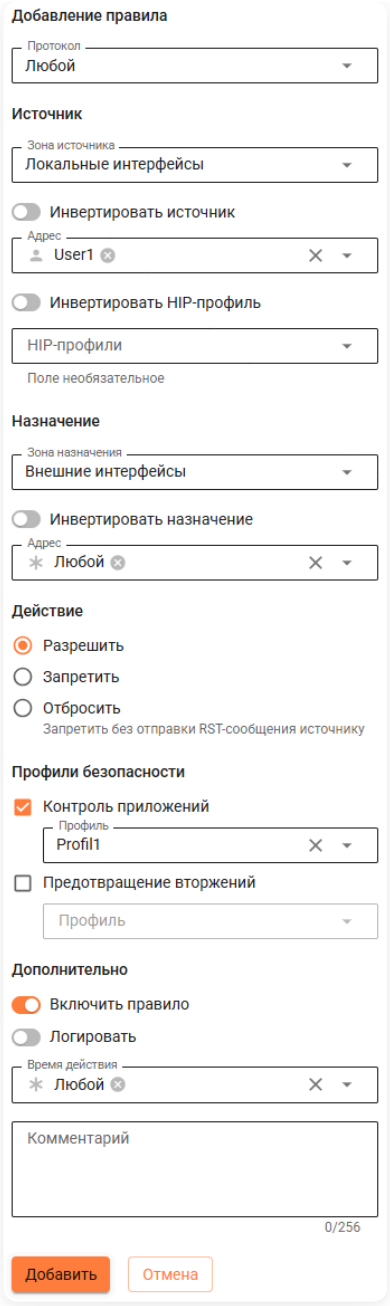
> Для успешного запрета доступа к приложениям удаленного доступа AnyDesk и TeamViewer до настройки на NGFW необходимо полностью удалить данные об этих приложениях в системе, если они запускались пользователями ранее.

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** → **Файрвол** → **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`:

Добавление правила

Протокол
Любой

Источник

Зона источника
Исходящий трафик устройства

Инвертировать источник

Адрес
Любой

Инвертировать HIP-профиль

HIP-профили

Поле необязательное

Назначение

Зона назначения
Любой

Инвертировать назначение

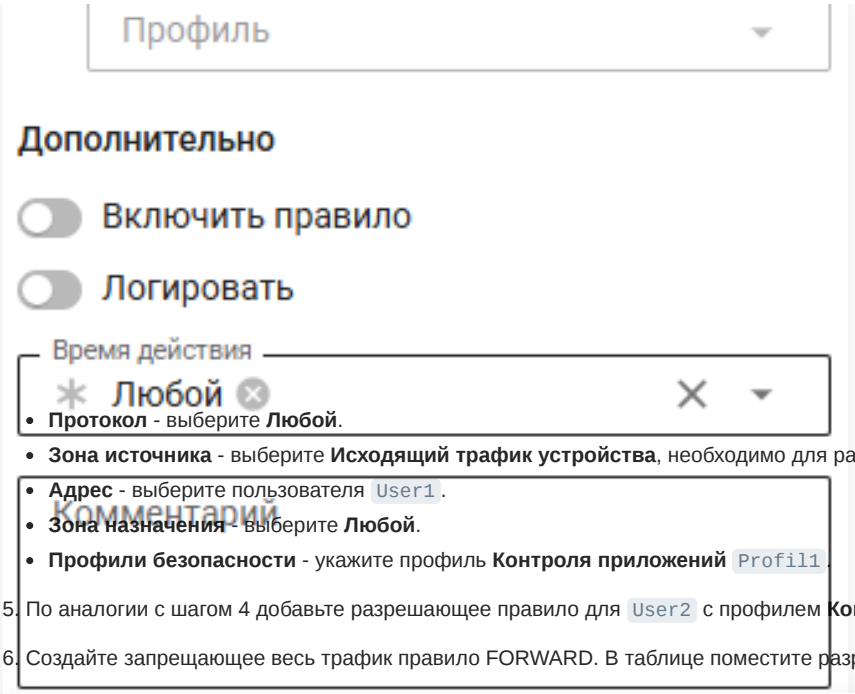
Адрес
User1

Действие

- (•) Разрешить
- ( ) Запретить
- ( ) Отбросить
  Запретить без отправки RST-сообщения источнику

Профили безопасности

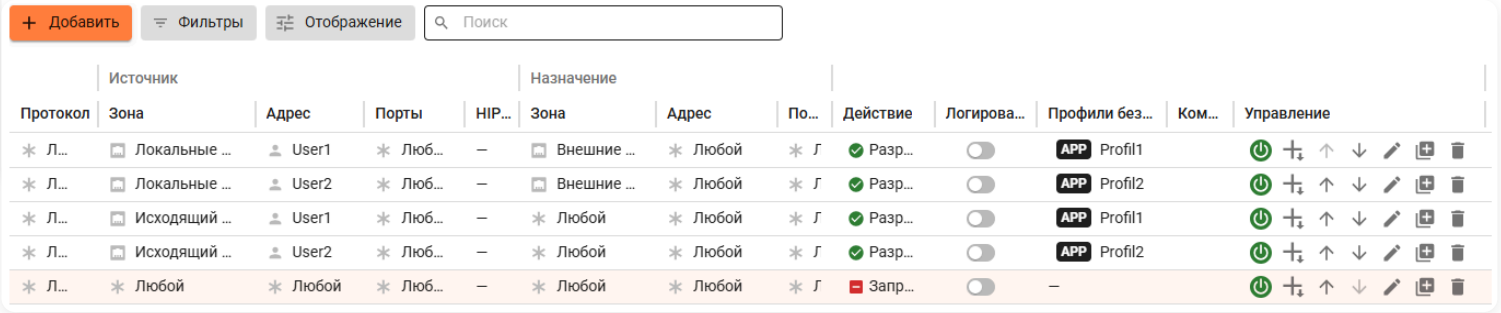
- [x] Контроль приложений
  Профиль
  Profil1
- [ ] Предотвращение вторжений



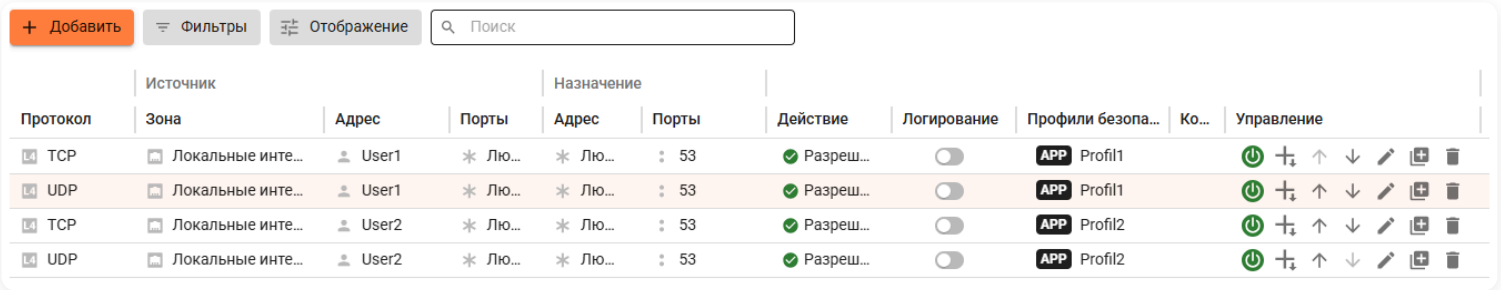
- **Протокол** - выберите **Любой**.
- **Зона источника** - выберите **Исходящий трафик устройства**, необходимо для работы прямого и прозрачного прокси, веб-трафика.
- **Адрес** - выберите пользователя `User1`.
- **Зона назначения** - выберите **Любой**.
- **Профили безопасности** - укажите профиль **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** → **Защита и управление 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:



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 раздел **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 **Администратора** и его пароль.

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 разделе **Управление сервером** → **Администраторы**. Для доступа введите внешний IP-адрес Ideco NGFW и порт 8443.

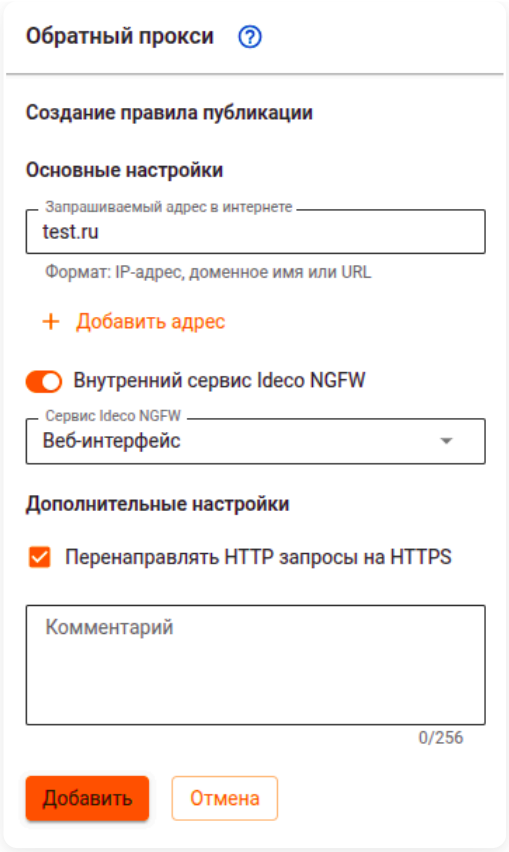
Доступ по VPN:

- 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 раздел **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**.

Тестирование оперативной памяти сервера

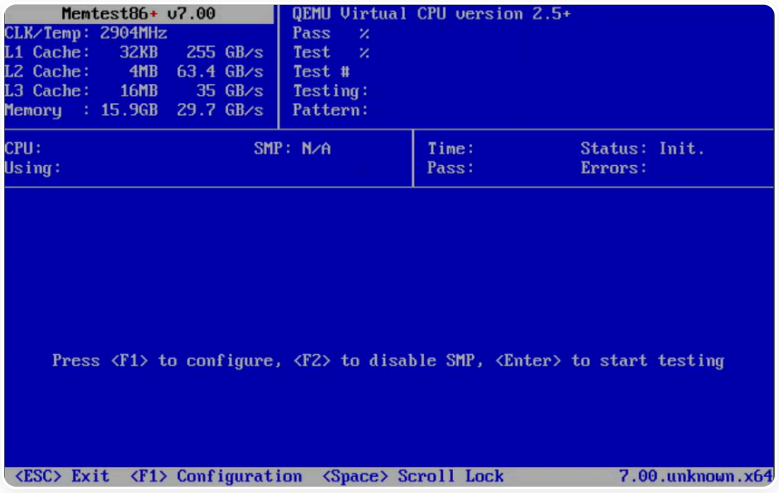
Для нормальной работы сервера все его аппаратные компоненты должны функционировать исправно.
Тестирование памяти помогает выявить и исключить проблемы с оперативной памятью сервера при поиске неисправностей.

При загрузке GRUB используйте Memtest86+ для тестирования оперативной памяти.
Для запуска тестирования выполните действия:

1. При загрузке сервера выберите **Memory test**:



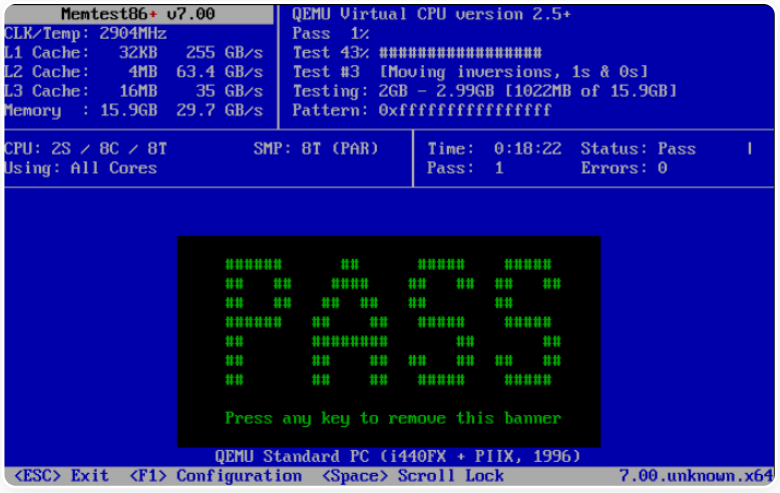
2. Нажмите **Enter** или подождите 5 секунд для автоматического запуска тестирования:



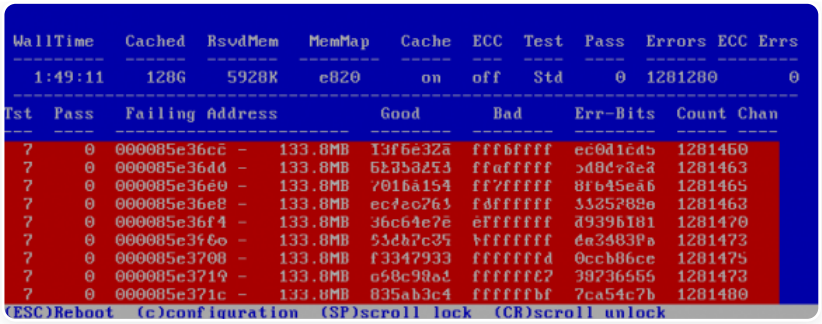
Для выбора режима диагностики **Fail-Safe Mode** нажмите **F1**.

Для выбора режима диагностики **Multi-Threading(SMP)** нажмите **F2**.

- Если появится запись **PASS**, тесты памяти пройдены успешно:



- При ошибке памяти появится запись вида:


WallTime Cached RsvdMem MemMap Cache ECC Test Pass Errors ECC Errs
1:49:11 128G 5928K e820 on off Std 0 1281280 0
Tst Pass Failing Address Good Bad Err-Bits Count Chan
7 0 000085e36cc - 133.8MB 13f6e32a fffbffff ec0d1cd5 1281460
7 0 000085e36dd - 133.8MB 6b3b3d53 ffaffffff 3d8c7ded 1281463
7 0 000085e36e0 - 133.8MB 7016a154 ff7fffff 8f645ea6 1281465
7 0 000085e36e8 - 133.8MB ec7ec763 fdffffff 3335788e 1281463
7 0 000085e36f4 - 133.8MB 36c64e7e efffffff d939b181 1281470
7 0 000085e3f6c - 133.8MB 53db7c35 bfffffff 6a3483fa 1281473
7 0 000085e3708 - 133.8MB f3347933 fffffffd 0ccb86ce 1281475
7 0 000085e3719 - 133.8MB a58c98a2 ffffffc7 38736555 1281473
7 0 000085e371c - 133.8MB 835ab3c4 ffffffbf 7ca54c7b 1281480
(ESC)Reboot (c)configuration (SP)scroll lock (CR)scroll unlock

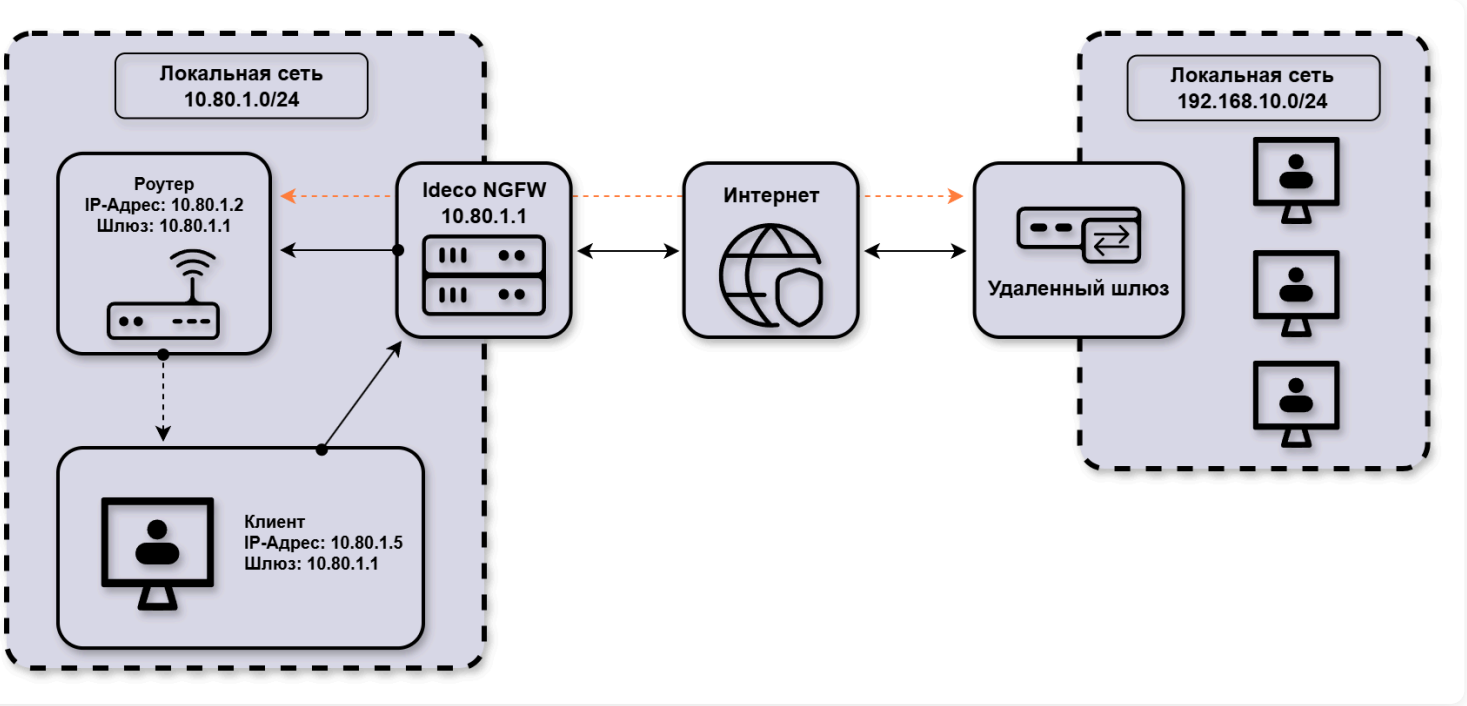
Как избавиться от асимметричной маршрутизации трафика

При попытке настроить доступ в удаленные сети через роутер 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 используется роутер, устанавливающий связь с другими сетями. NGFW - шлюз по умолчанию для клиентов сети. Требуется настроить маршрутизацию на NGFW так, чтобы клиенты сети `10.80.1.0/24` получали доступ в удаленную сеть `192.168.10.0/24` и обратно через роутер.

Асимметричная маршрутизация при наличии роутера в локальной сети

Неправильная топология сети, способствующая асимметричной маршрутизации:

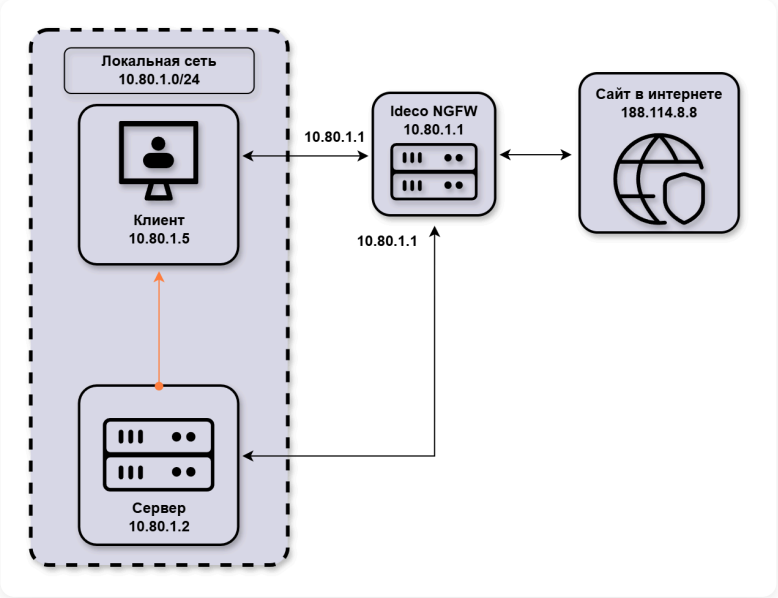


- `10.80.1.1` - шлюз для локальной сети `10.80.1.0/24`.
- `10.80.1.2` - роутер, имеющий доступ в удаленную сеть `192.168.10.0/24`.
- `10.80.1.5` - адрес хоста в локальной сети.
- **Оранжевая стрелка** - двусторонняя связь роутера с удаленным шлюзом или роутером, обеспечивающая доступ к удаленной сети `192.168.10.0/24` (туннель к шлюзу, маршрут до роутера 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 (`10.80.1.1`) и роутер (`10.80.1.2`).
- **Пунктирная стрелка** - трафик, который роутер возвращает хостам локальной сети в обход NGFW, поэтому хосты этот трафик обратно не принимают.

Часть трафика от клиентов до роутера идет через шлюз, а часть - непосредственно от роутера до абонентов сети. Разная маршрутизация на разных участках делает прохождение пакетов между двумя локальными сетями невозможной.

Асимметричная маршрутизация при публикации сайтов через DNAT

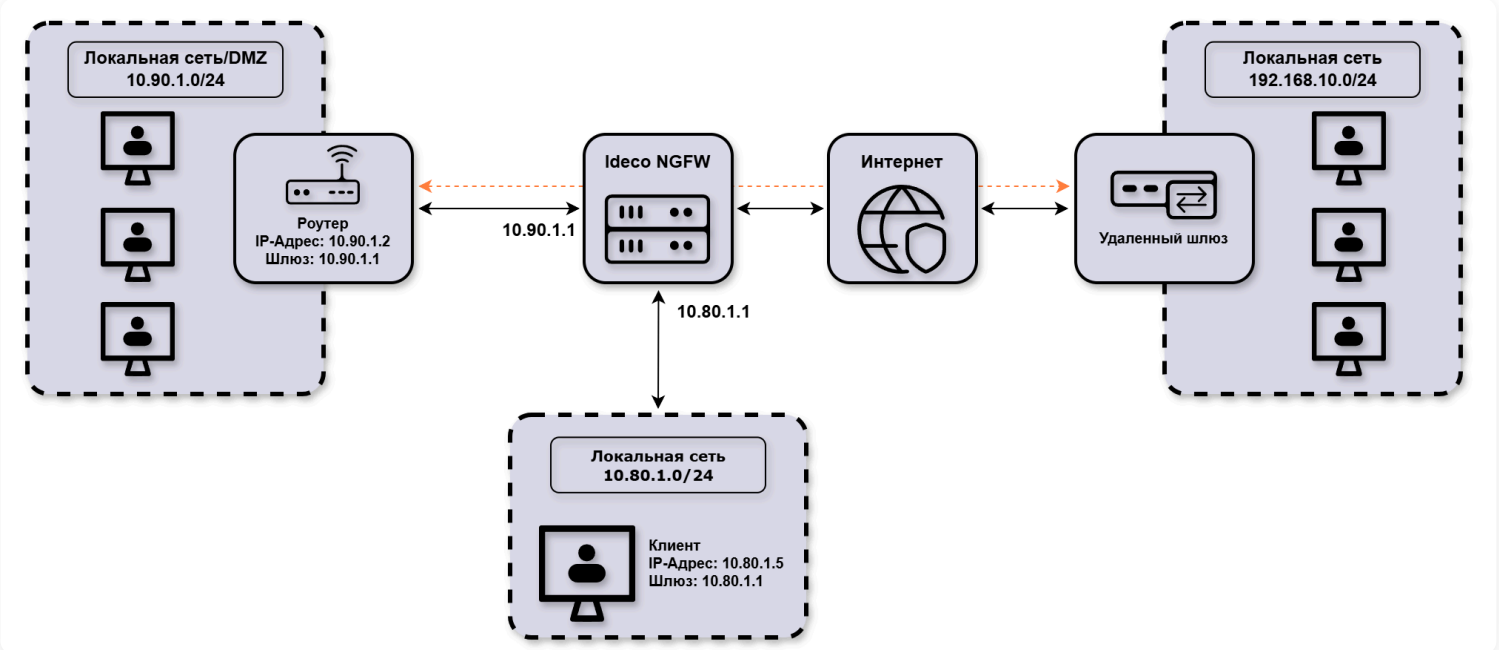
Асимметричная маршрутизация также возникает, когда в одной локальной сети находится хост и сервер, на котором расположен опубликованный при помощи DNAT-правила ресурс:



- `10.80.1.1` - адрес Ideco NGFW 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 сайта в интернете.
- **Оранжевая стрелка** - ответ напрямую от сервера хосту в локальной сети.

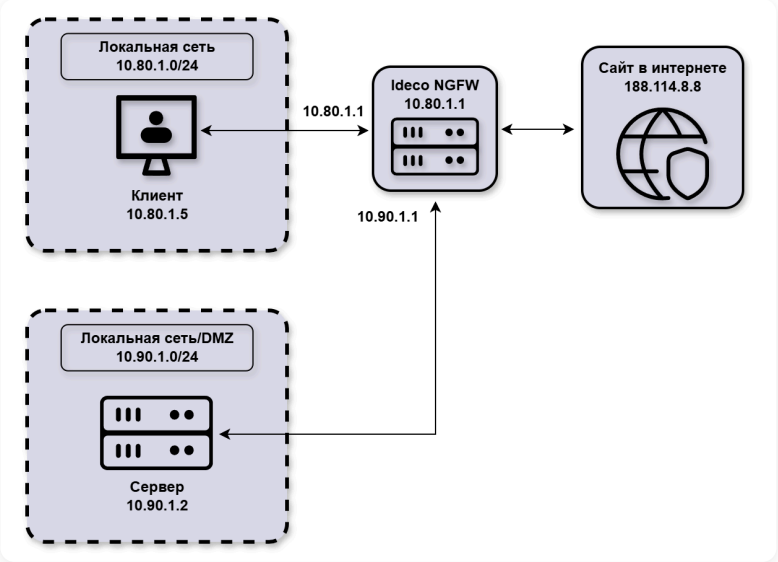
Когда хост `10.80.1.5` обращается на сайт по внешнему адресу `188.114.8.8` (например, в случае обращения по доменному имени, которое разрешено во внешнем IP), трафик проходит через NGFW. На NGFW срабатывает правило DNAT и перенаправляет трафик на сервер `10.80.1.2`, а сервер отвечает хосту, минуя NGFW.

Правильная топология сети:



Для правильной работы схемы потребуется:

1. Вынести роутер в отдельную локальную сеть (DMZ `10.90.1.0/24`), чтобы избежать асимметричной маршрутизации между роутером и клиентами локальной сети:



2. Настроить DMZ на NGFW, добавив на локальный интерфейс NGFW еще один IP-адрес (`10.90.1.0/24`), к локальной сети которого подключен роутер.

3. Настроить IP-адрес на роутере из адресного пространства новой сети `10.90.1.2`. Шлюзом указать дополнительный IP-адрес, настроенный на локальном интерфейсе NGFW из этой сети `10.90.1.1`.

Физически роутер 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 и роутера:

- Подключите к Ideco NGFW дополнительную сетевую карту;
- Настройте на сетевой карте дополнительный локальный интерфейс и отдельную IP-адресацию в этой сети;
- Укажите в качестве шлюза для роутера адрес, настроенный на дополнительном локальном интерфейсе.

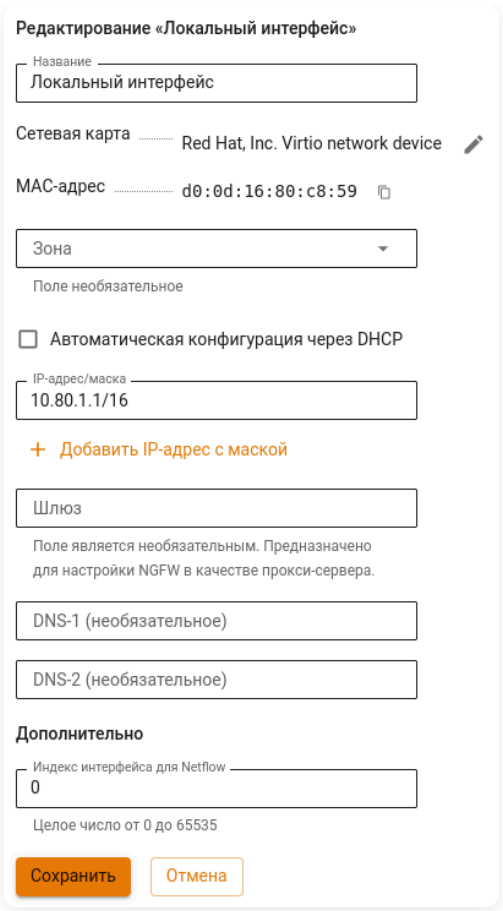
Физически роутер будет находиться в сегменте дополнительной сетевой карты.

Настройка NGFW

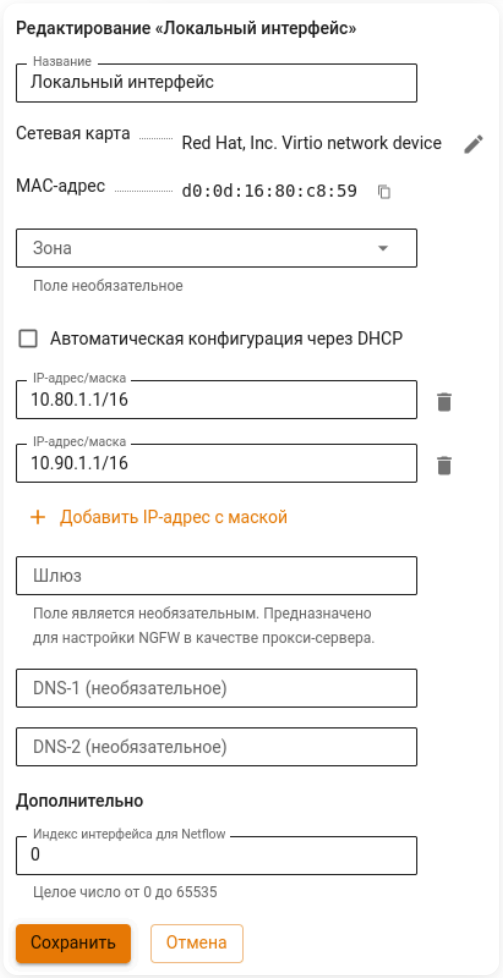
Для настройки нескольких виртуальных локальных сетей на одном физическом локальном интерфейсе NGFW перейдите в раздел **Сервисы** → **Сетевые интерфейсы** и выполните действия:

1. Откройте в режиме редактирования **Локальный интерфейс**, к которому подключены пользователи нужной вам локальной сети (`10.80.1.1/24`), нажав на напротив его названия.

2. Если IP-адрес вашей локальной сети был автоматически сконфигурирован через DHCP, отключите опцию и введите его вручную:



3. Нажмите на **+ Добавить IP-адрес с маской** и введите IP-адрес DMZ для изоляции роутера:

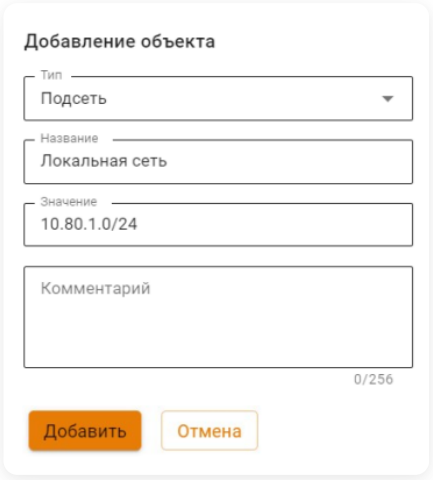


4. Нажмите **Сохранить**.

После изоляции роутера в DMZ нужно указать маршрут на NGFW до удаленной сети. Для этого перейдите в **Сервисы** → **Маршрутизация** и выполните действия:

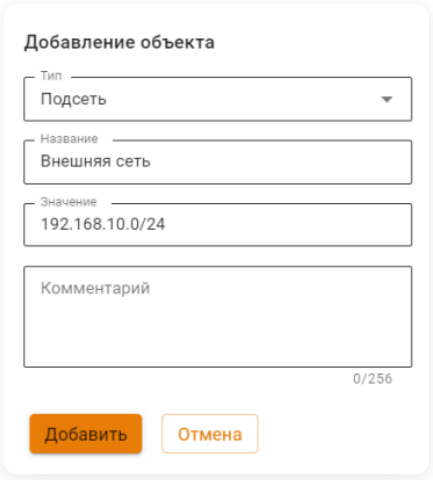
1. Перейдите на вкладку **Внешних сетей** нажмите кнопку **Добавить**.

2. В поле **Адрес источника** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес вашей локальной сети (`10.80.1.0/24`):



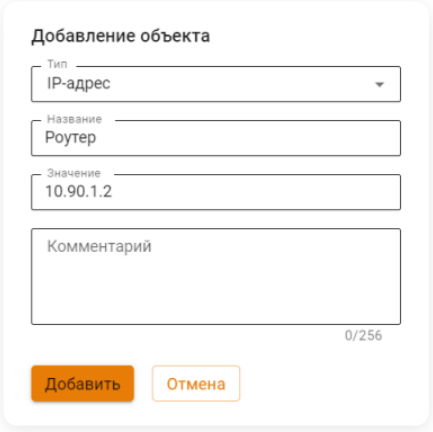
Выберите в качестве источника только что созданный объект.

3. В поле **Адрес назначения** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес внешней сети (`192.168.10.0/24`), в которую нужно настроить доступ:

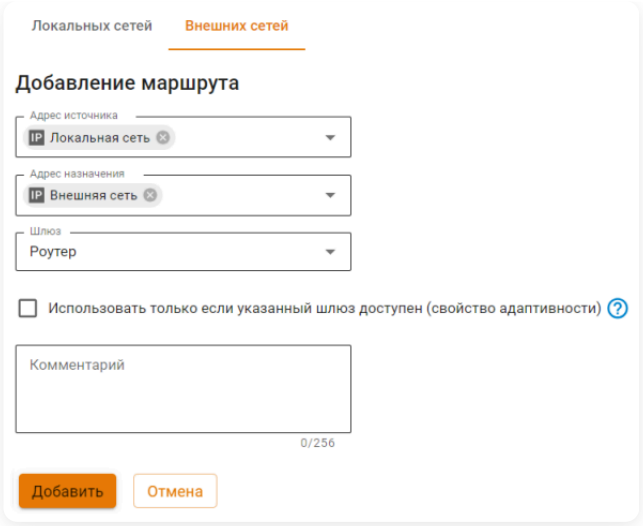


Выберите в качестве назначения только что созданный объект.

4. В поле **Шлюз** нажмите **Добавить объект**, выберите тип **IP-адрес** и введите адрес роутера в DMZ (`10.90.1.2`):



5. Сохраните маршрут вида:



Теперь трафик между сетями NGFW (`10.80.1.0/24` и `192.168.10.0/24`) во всех направлениях будет направляться через NGFW и роутер.

Настройка клиентских машин

Хосты сетей, которые теперь обслуживает NGFW (`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, укажите:

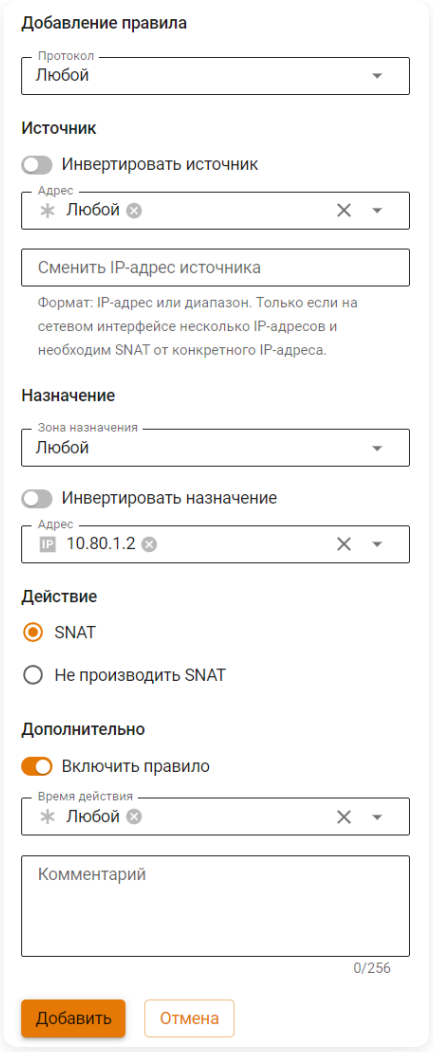
1. Для хостов из подсети `10.80.1.0/24` значение шлюза и DNS-сервера - `10.80.1.1`.

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 специальное SNAT-правило.

Создание на NGFW SNAT-правила для избежания асимметричной маршрутизации

Чтобы сервер `10.80.1.2` не отвечал напрямую на `10.80.1.5`, а посылал ответ на NGFW `10.80.1.1`, нужно в разделе **Правила трафика** → **Файрвол** → **SNAT** создать и включить правило вида:



Заполните поля:

- Назначение - `10.80.1.2`;
- Зона назначения - Локальные интерфейсы.

В этом случае трафик хоста `10.80.1.5` на внешний адрес сайта `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 - пакет приобретет вид: `scr 10.80.1.1 dst 10.80.1.2`. Ответ от сервера также пройдет через NGFW - пакет `scr 10.80.1.2 dst 10.80.1.1`.

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 его 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

Наше решение обладает всей функциональностью, обеспечивающей максимальную защиту от спам-ботов, ботнет-клиентов и предотвращение вирусной активности в сети.

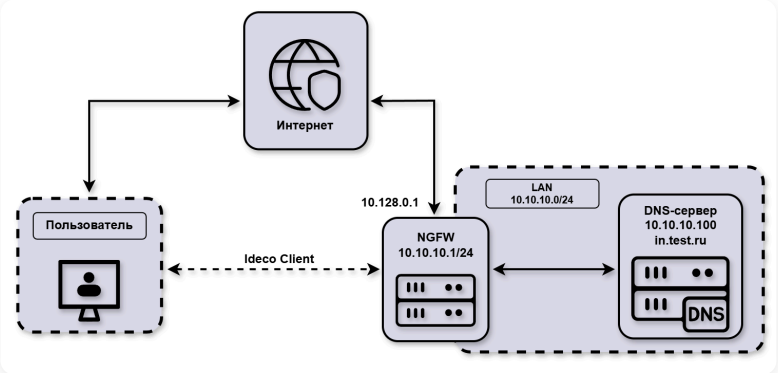
До 22 пользователей - решение предоставляется бесплатно. Для 10000 пользователей доступна 40-дневная пробная версия.

Скачать Ideco NGFW

Подключение через Ideco Client к внутреннему DNS

Клиенты, подключающиеся к NGFW из внешней сети через Ideco Client, изначально не видят внутренний DNS-сервер.

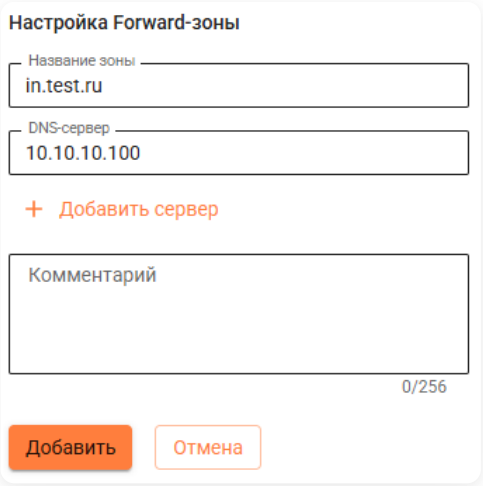
Схема сети:



Для настройки подключения к внутреннему DNS-серверу выполните действия:

1. Перейдите в **Сервисы** → **Защита и управление DNS** → **FORWARD-ЗОНЫ** и нажмите **Добавить**.

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

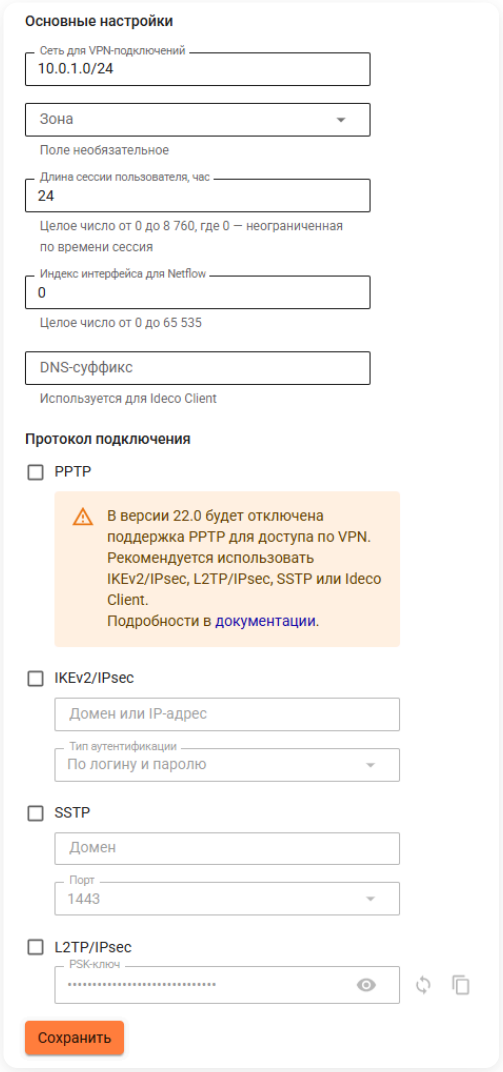


После настройки NGFW клиенты, подключающиеся к NGFW с помощью Ideco Client из интернета, смогут использовать внутренний DNS-сервер.

Как избежать проблем с подключением VPN-клиентов при использовании нескольких серверов Ideco NGFW

При использовании нескольких серверов Ideco NGFW 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.

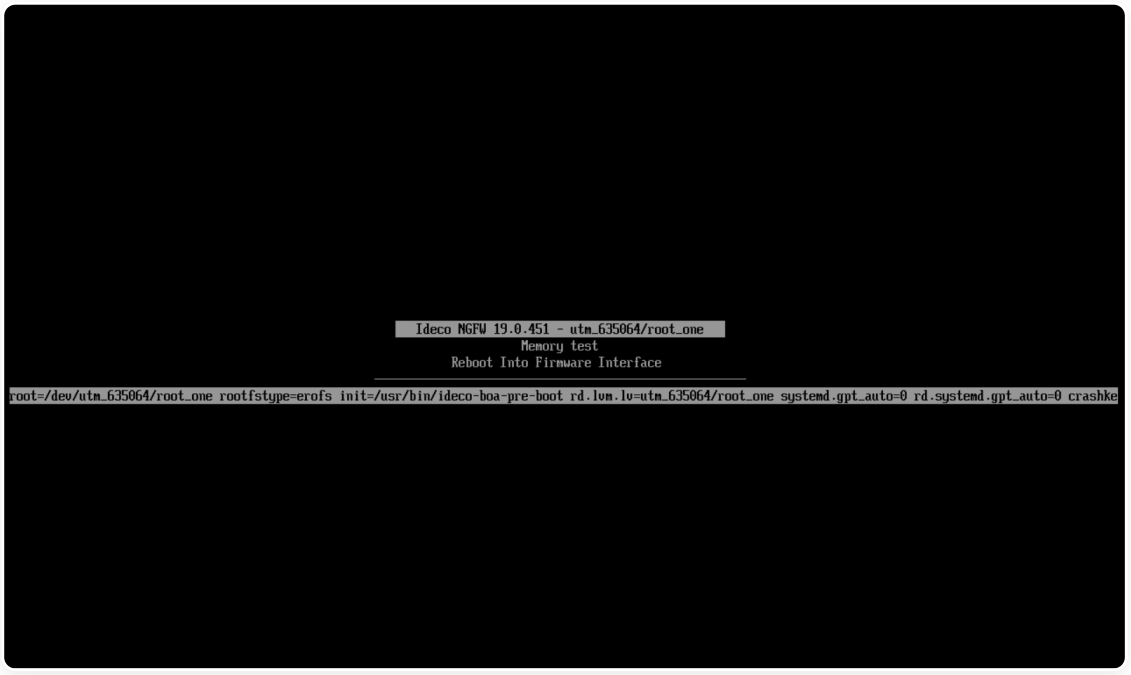
Как восстановить доступ к Ideco NGFW

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:

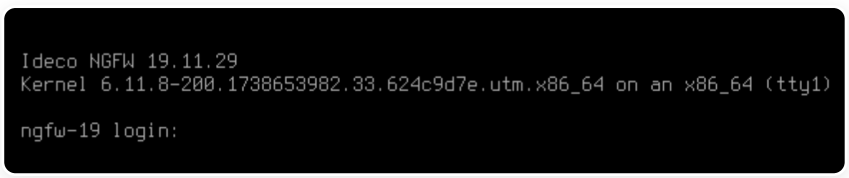


2. Откроется окно параметров ядра с возможностью редактирования. Переместите указатель стрелками на клавиатуре вправо до слова `quiet` и допишите текст `p=1`:



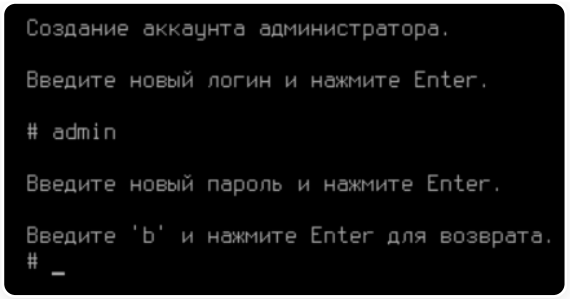
3. Нажмите `Enter`.

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:

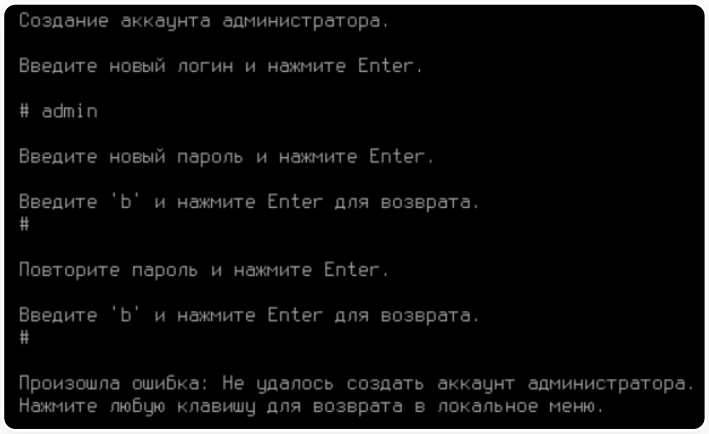


Требования к созданию пароля администратора:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.
- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

Если при создании нового логина администратора он 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 восстановиться на прошлую версию после обновления Ideco NGFW

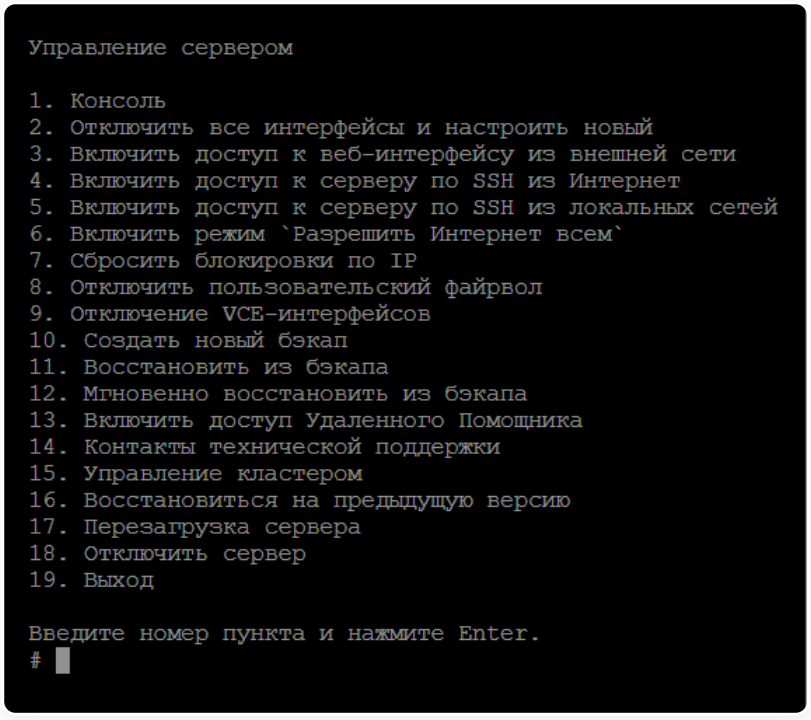
При восстановлении на предыдущую версию данные перенесены не будут. Сохраните бэкап на внешнем носителе. Информация о работе с API бэкапа описана в статье Бэкап.

Для восстановления на предыдущую версию выполните действия:

1. Перейдите в локальное меню Ideco NGFW.

2. Введите логин и пароль администратора.

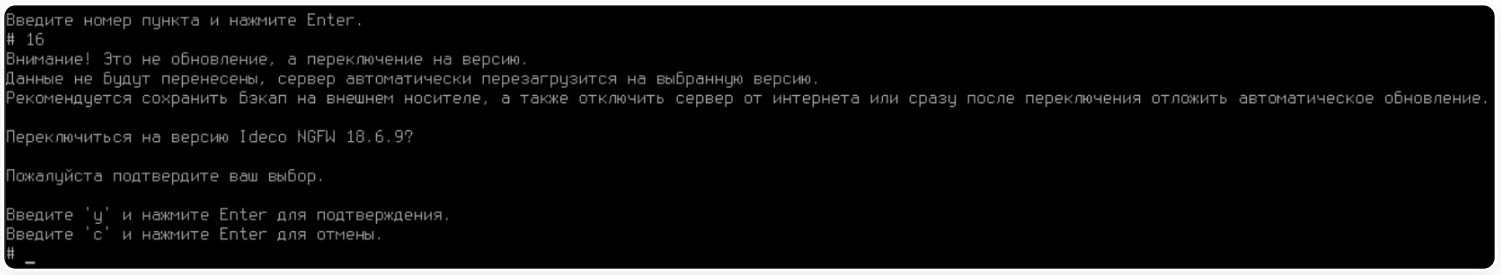
3. Укажите номер пункта 16 и нажмите Enter:



Появится окно с предупреждением и описанием версии, на которую произойдет переключение.

Если в Ideco NGFW 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 переключится на предыдущую версию.

Поддержка устаревших алгоритмов шифрования

Ideco NGFW основан на операционной системе Fedora. В Ideco NGFW используется Fedora 40. Подробнее об изменениях политики алгоритмов можно прочитать в статье.

Устаревшие алгоритмы, как (криптографическое) хеширование и шифрование, обычно имеют время жизни, по истечении которого они 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. Это можно сделать из локального меню, по ssh или через веб-интерфейс Ideco NGFW.

2. Введите в терминале команду `update-crypto-policies --set DEFAULT:FEDORA32`.

3. Перезагрузите Ideco NGFW.



Мы настоятельно не рекомендуем использовать данную настройку, так как при следующем обновлении Ideco NGFW настройки режима совместимости будут сброшены. В более новых версиях данная возможность будет отключена.

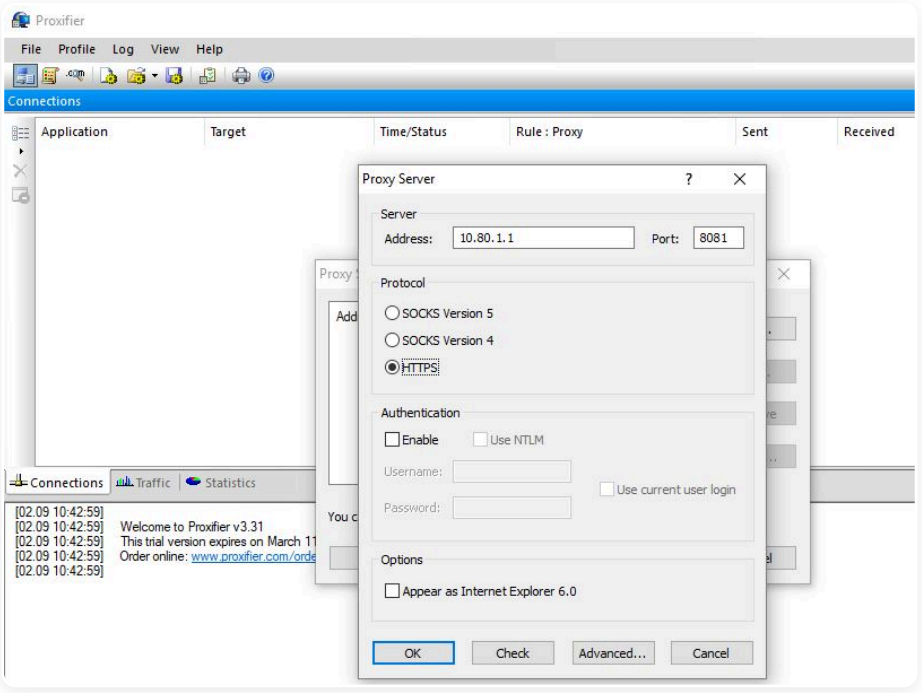
Настройка программы Proxifier для прямых подключений к прокси серверу

Скачать Proxifier можно с сайта разработчика.

Настройка

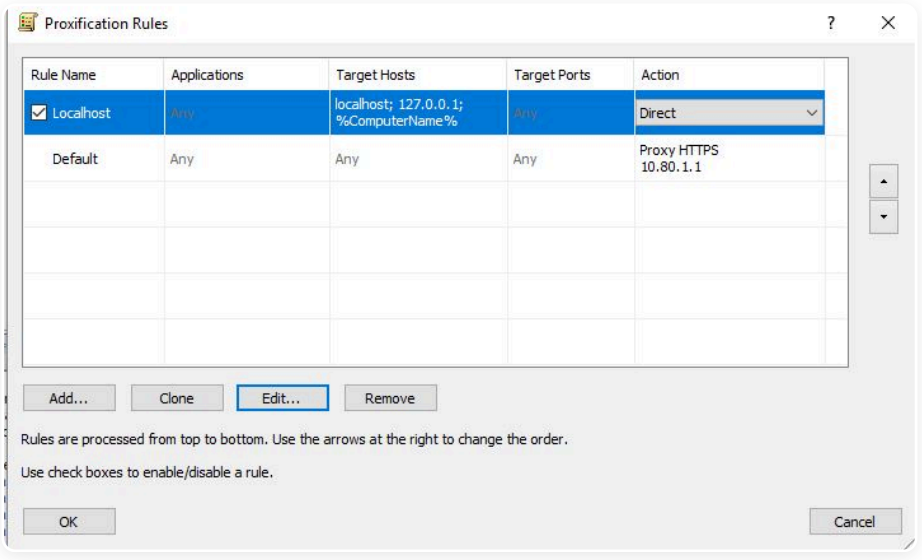
Выполните стандартные настройки браузера для прямых подключений к прокси-серверу, а затем настройте программу для перенаправления остального трафика на прокси-сервер.

Пропишите в настройках прокси-сервера в Proxyfier IP-адрес локального интерфейса Ideco NGFW 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:



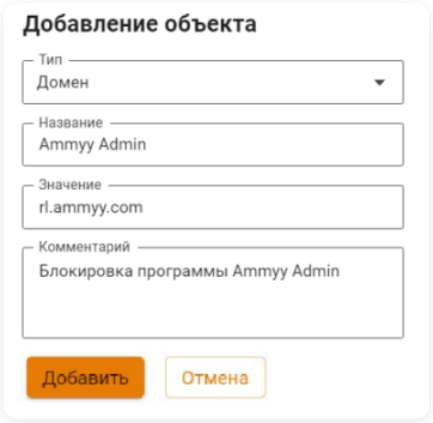
Настройка закончена, программы будут выходить в интернет через заданный прокси-сервер.

Блокировка популярных ресурсов

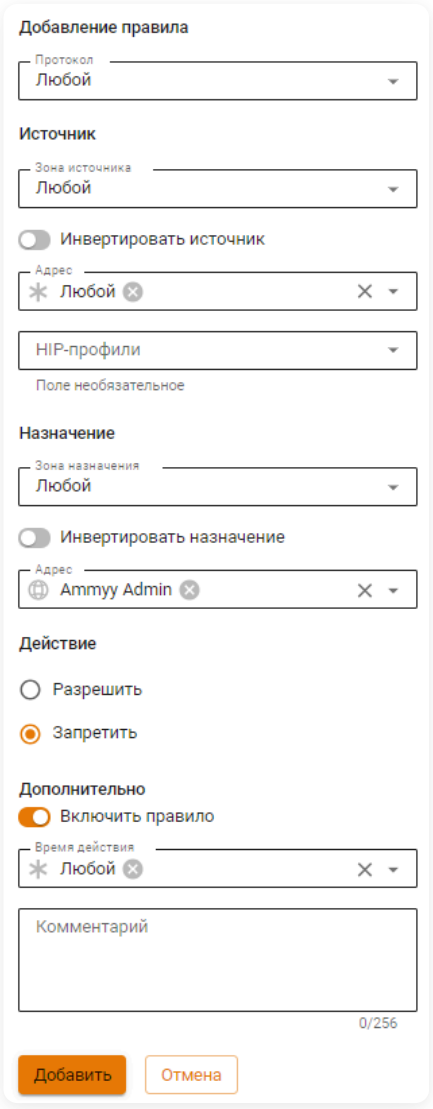
Блокировка Ammyy Admin

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:



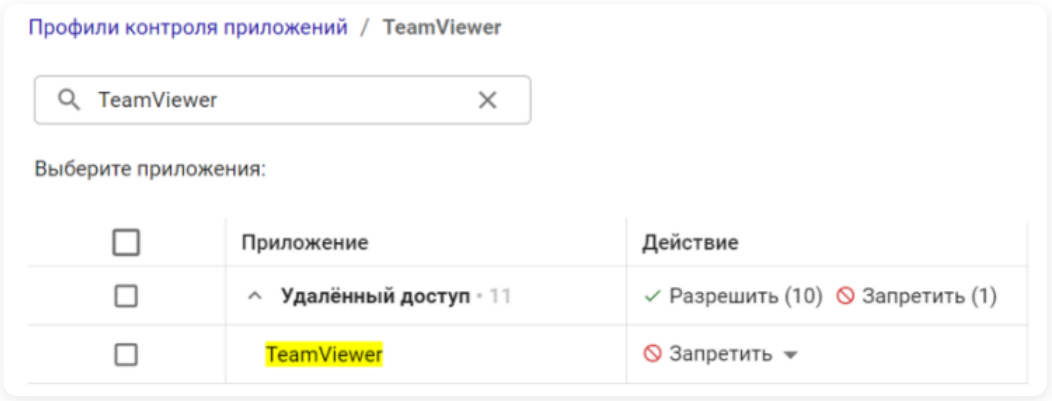
2. Перейдите на вкладку **Правила трафика** → **Файрвол** → **FORWARD**, создайте и включите правило запрета для нужных пользователей или групп. В поле **Назначение** выберите объект, созданный в пункте 1:



Блокировка TeamViewer

TeamViewer - это программное обеспечение для удаленного доступа и управления компьютерами. Его можно заблокировать с помощью Контроля приложений.

1. Перейдите в раздел **Профили безопасности** → **Контроль приложений**. Создайте новый профиль для TeamViewer с действием **Запретить**:

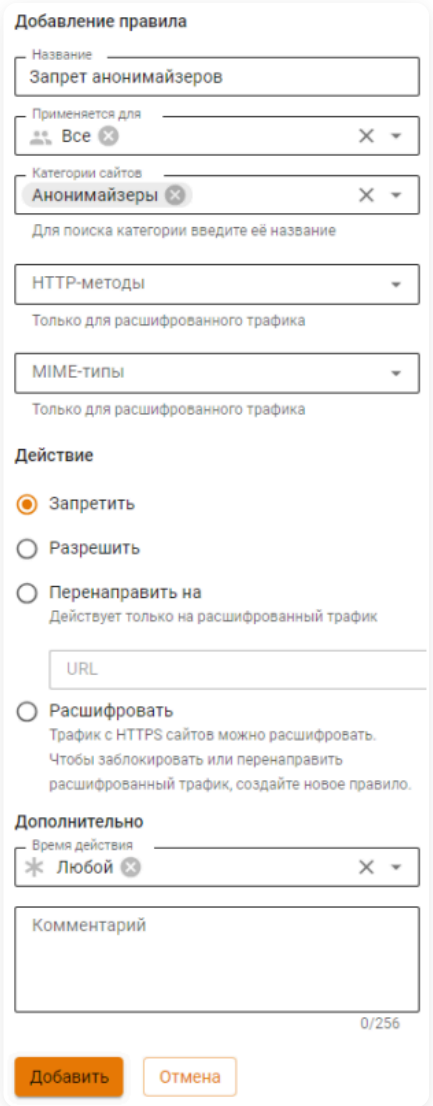


2. В разделе **Правила трафика** → **Файрвол** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

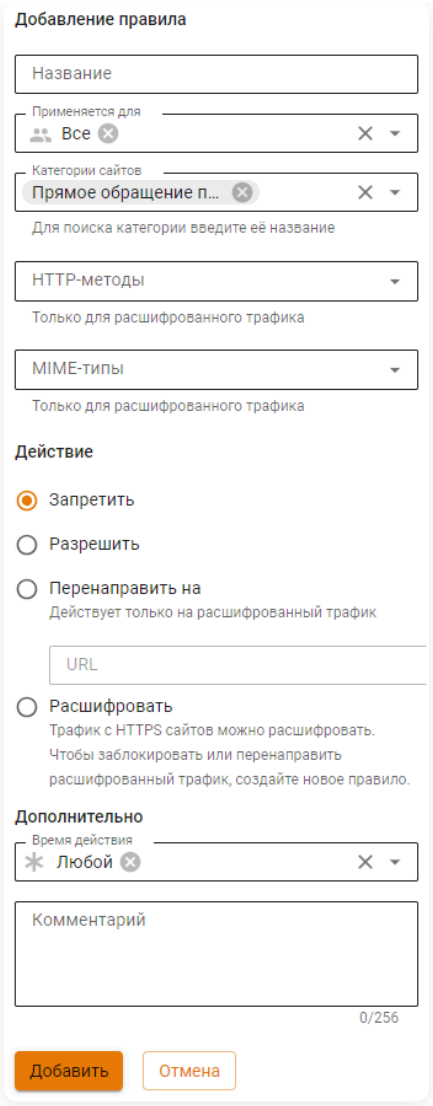
Блокировка анонимайзеров

Заблокировать анонимайзеры можно в разделе **Правила трафика** тремя способами:

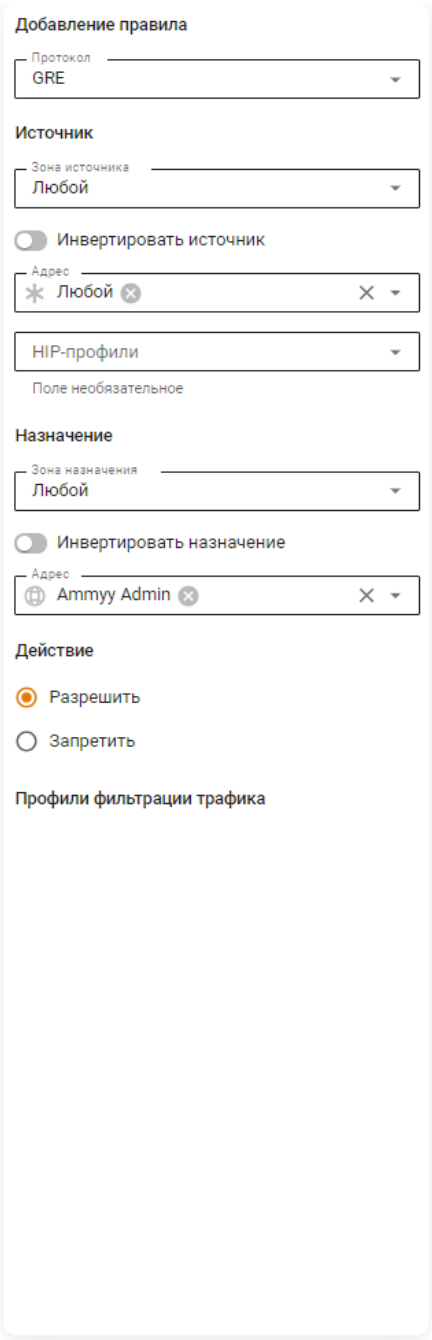
1. Анонимайзеры, работающие по протоколам HTTP(S), блокируются в разделе **Правила трафика** → **Контент-фильтр**. Для этого создайте правило, в котором запретите категорию сайтов **Анонимайзеры**:



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 **Файрвола**:



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 раздел **Профили безопасности** → **Предотвращение вторжений**. Создайте новый профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило, блокирующее группу сигнатур **Анонимайзеры**:

3. Нажмите **Добавить**.

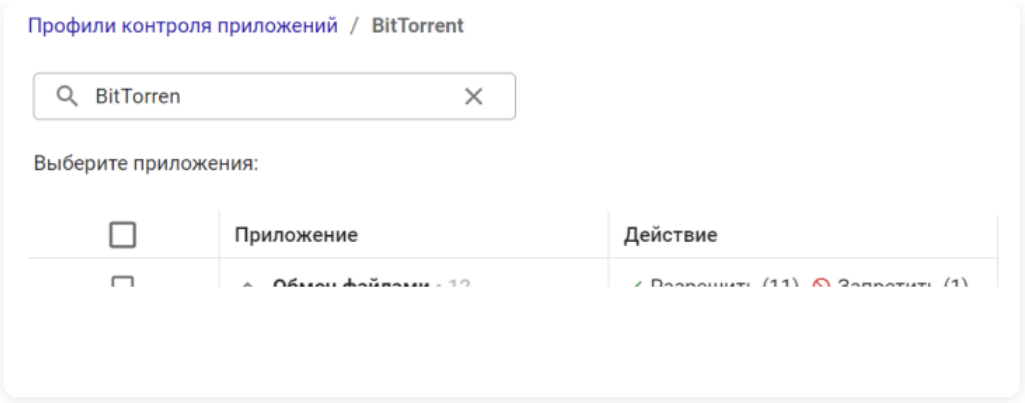
4. В разделе **Правила трафика** → **Файрвол** добавьте и включите разрешающее правило с профилем, созданным ранее.

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 разделе **Профили безопасности** → **Контроль приложений**:



2. В разделе **Правила трафика** → **Файрвол** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

3. Разрешите нужные TCP и UDP порты пользователям. Затем создайте и включите в разделе **Правила трафика** → **Файрвол** → **FORWARD** правило, которое запрещает все протоколы (правила действуют сверху вниз).

4. В разделе Контент-фильтр заблокируйте доступ к сайтам-каталогам и торрент-файлам. Для этого запретите категории **Торрент-трекеры** и **Torrent-файлы**:

5. В разделе **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 разделе **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**:

Настройка почтовых клиентов

Примечание

В Ideco NGFW 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.

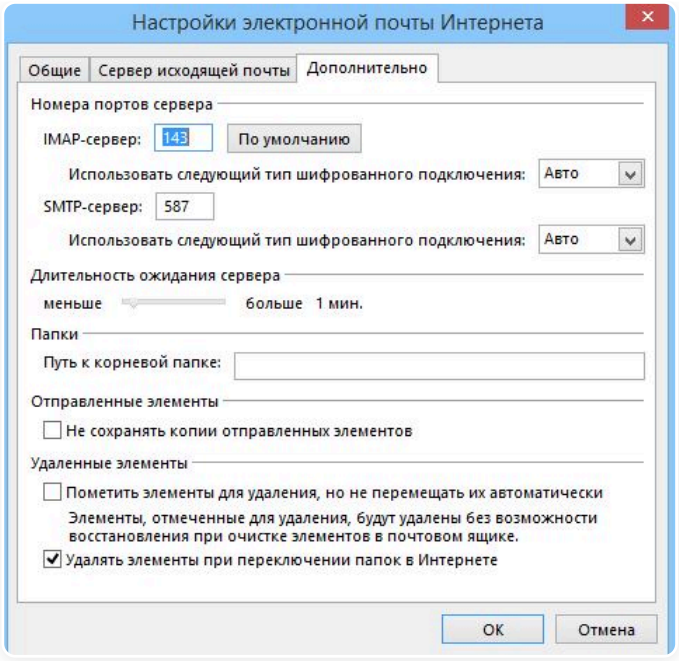
2. Сервер исходящей почты работает только с авторизацией и шифрованием. Необходимо использовать 587 порт для подключения (а не 25). Тип шифрования, логин и пароль указываются аналогично серверу входящей почты.

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

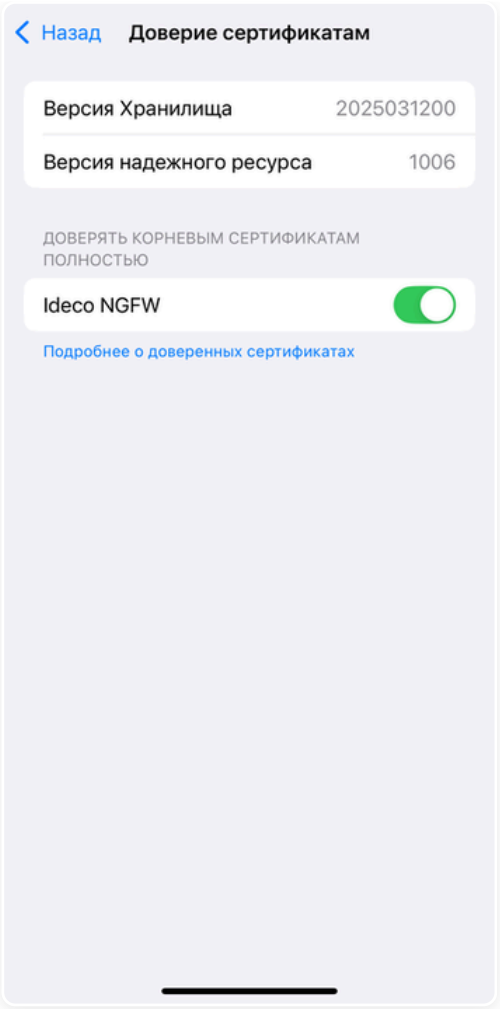
1. Скачайте сертификат в **Сервисы** → **Сертификаты** и перенесите на настраиваемое устройство (например, отправив по почте).

2. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством**.

3. Выберите сертификат и нажмите кнопку **Установить**:

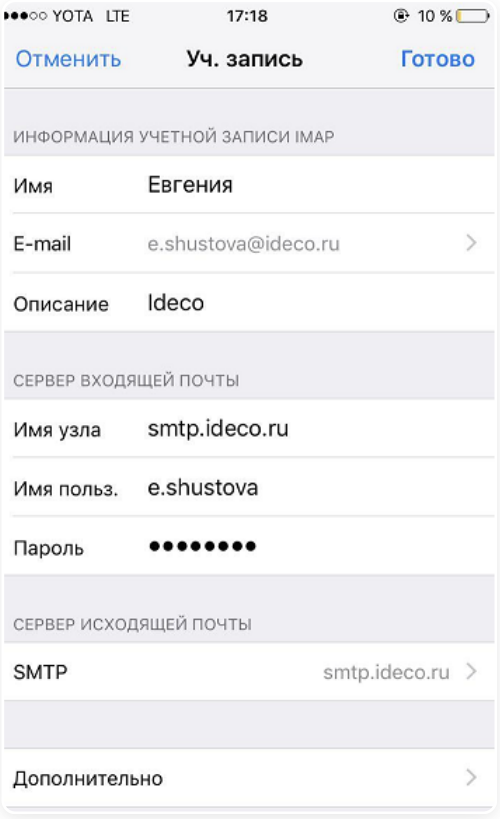
4. Зайдите в **Настройки** → **Основные** → **Об этом устройстве** и выберите **Доверие сертификатов**.

5. Включите опцию **Доверять корневым сертификатам полностью**:

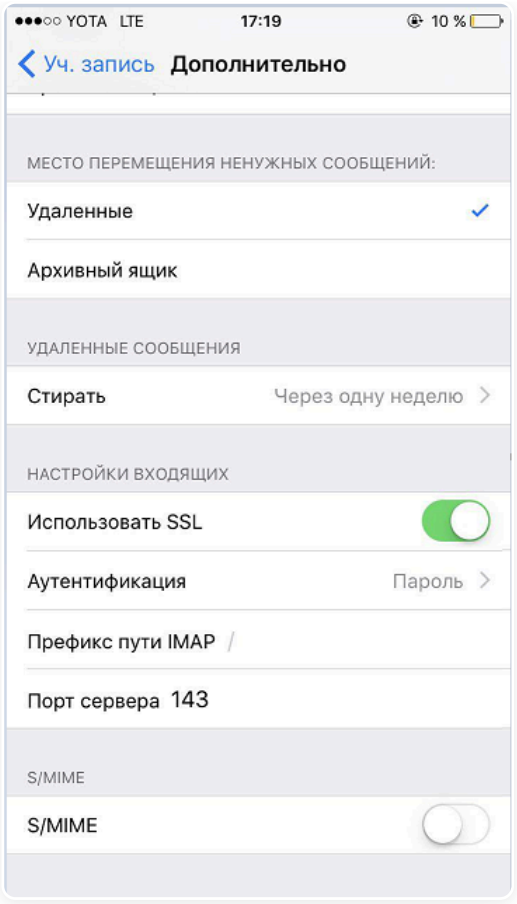


Настройка почтового ящика

1. Перейдите в Учетную запись почты и нажмите **Дополнительно**:



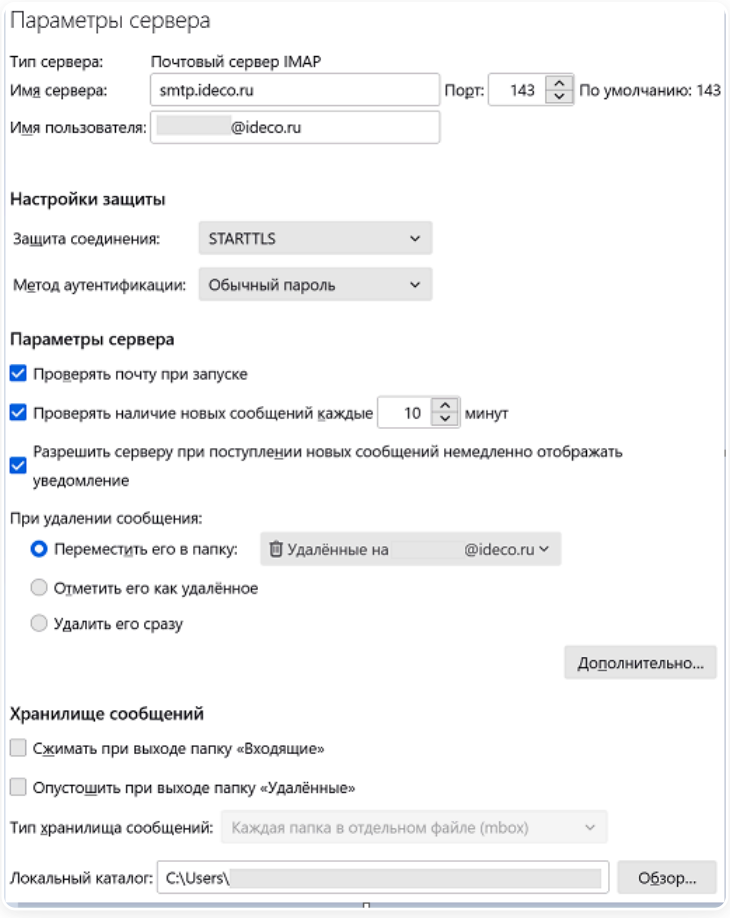
2. Скорректируйте настройки:



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**.

Настройка прозрачной авторизации на Astra Linux

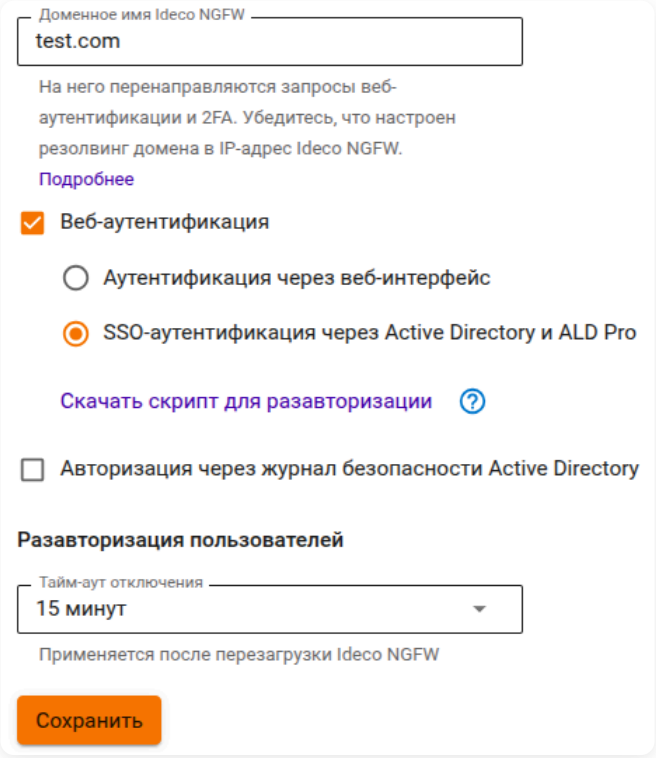
Решение подходит для браузеров **Yandex**, **Chromium** и **Firefox.**

1. Установите и настройте NGFW на устройстве администратора, получите лицензию.

2. Введите Astra Linux в домен (например, через Active Directory).

3. Введите NGFW в тот же домен и импортируйте пользователей (в том числе Astra Linux) в группу.

4. Включите в NGFW **SSO-аутентификацию через Active Directory и ALD Pro** в разделе **Пользователи** → **Авторизация** → **Веб-аутентификация**:



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.

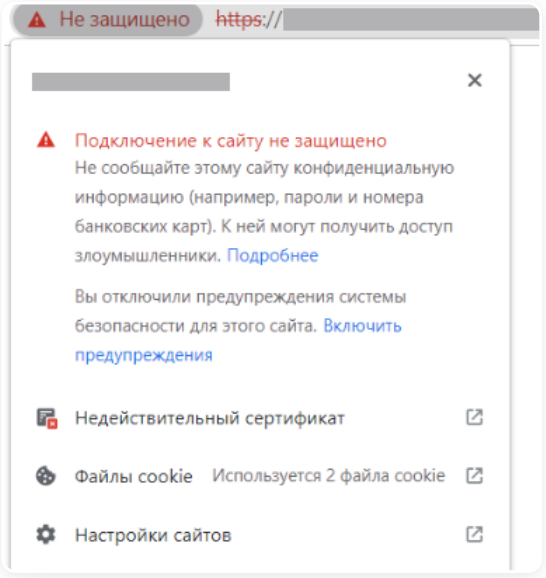
Для браузера Firefox

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:

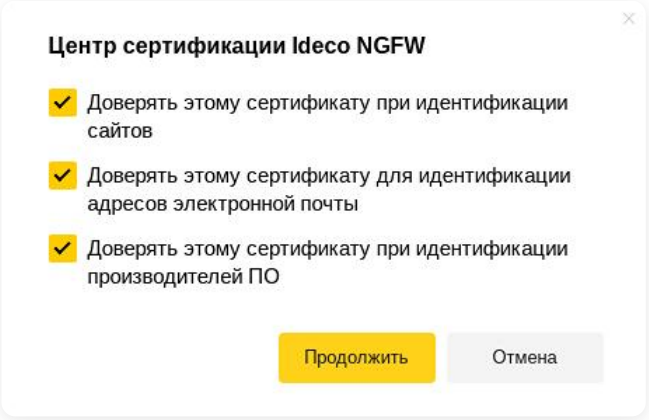


Для браузера Yandex

1. Скачайте корневой сертификат.

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

3. Включите опции доверия для сертификата:

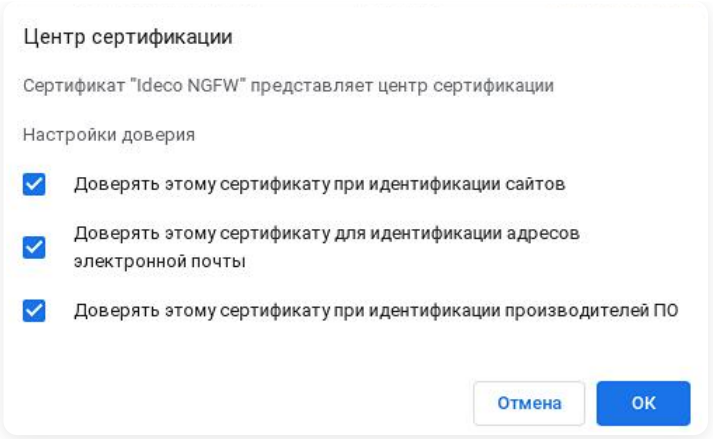


Для браузера Chromium

1. Скачайте корневой сертификат.

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

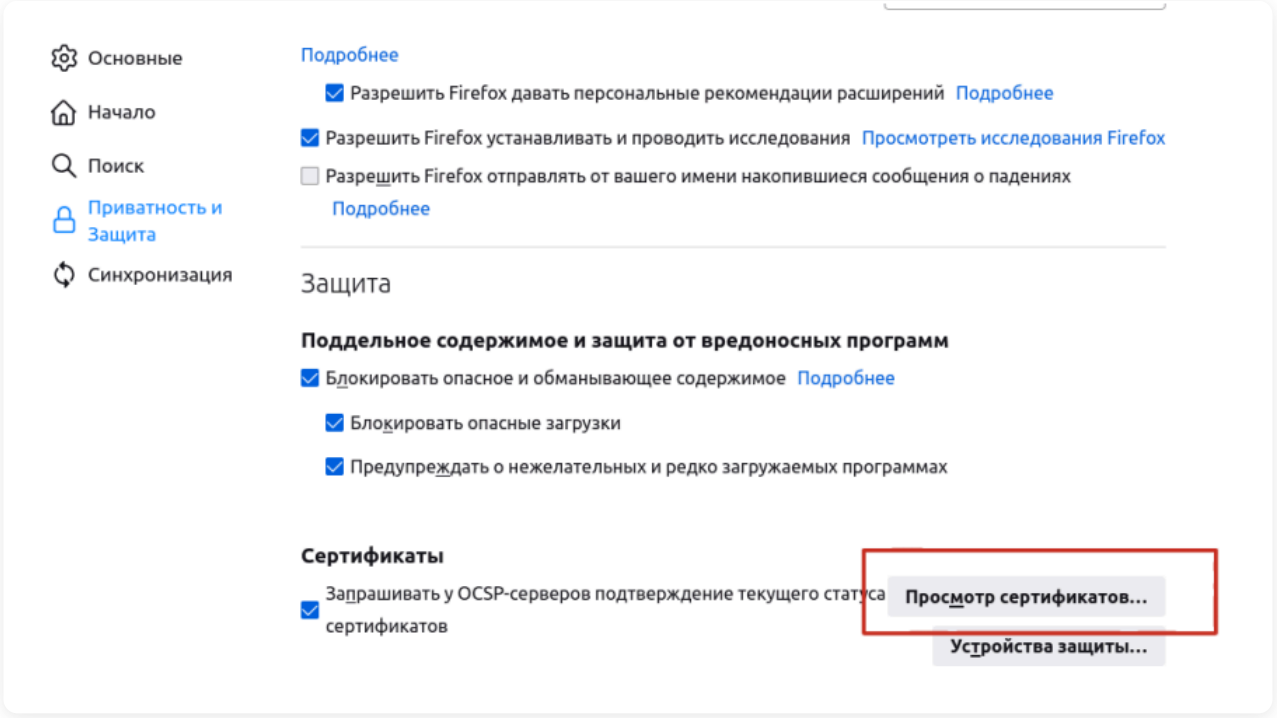
3. Включите опции доверия для сертификата:



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.

Инструкция по настройке автоматической веб-аутентификации на Ideco NGFW

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 каталог `ideco-utm`. Можно воспользоваться командой:

```
mkdir -p ~/.config/ideco-utm
```

3. Скачайте корневой сертификат NGFW `root_ca.crt` (подробнее в статье) и поместите его в каталог, созданный на предыдущем шаге.

4. Создайте в папке `ideco-utm` файл `auth.conf`. Добавьте в него содержимое (введите логин и пароль пользователя) в формате:

```
login=логин_пользователя
password=пароль_пользователя
```

5. Рекомендуем ограничить права доступа к файлу `auth.conf`:

```
chmod 0600 ~/.config/ideco-utm/auth.conf
```

6. Скачайте скрипт на компьютер пользователя по ссылке или воспользуйтесь командой:

```
curl -O https://docs.ideco.ru/scripts/auto-web-auth-linux.py
```

7. Настройте автозагрузку в соответствии с описанным ниже алгоритмом.

Для корректной работы скрипта имя корневого сертификата должно быть `root_ca.crt`.

Пути к файлам и другие параметры можно менять с помощью ключей запуска. Используйте ключ `-h` или `--help` для вывода справки.

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

[Install]
WantedBy=multi-user.target
```

Введите имя пользователя Linux и полный путь до скрипта.

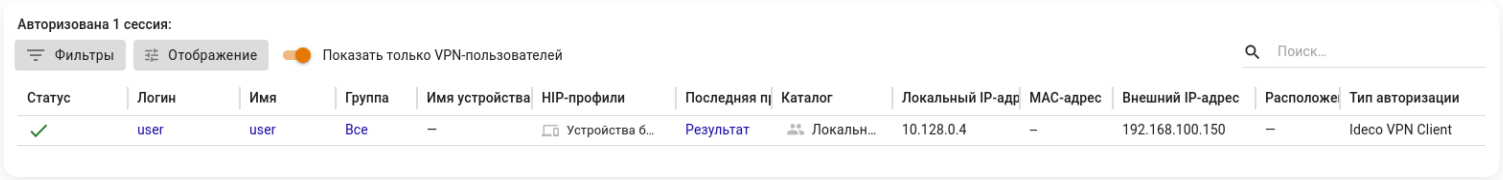
3. Сохраните файл и выйдите из редактора.

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. 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 свой выбор.



Если выйти из сессии на устройстве пользователя и повторно открыть браузер, то запрос на авторизацию появиться не должен.

Порядок обработки веб-трафика в Ideco NGFW

Порядок обработки веб-трафика:

1. Ограничение скорости.

2. DNS.

3. Захват трафика для фильтрации (прокси-сервер):

- Контент-фильтр.
- Антивирус веб-трафика.

4. Файрвол.

5. Контроль приложений.

6. Система Предотвращения вторжений.

INPUT-правила Файрвола обрабатывают трафик раньше DNS (если включен перехват DNS-запросов) и прокси-сервера.

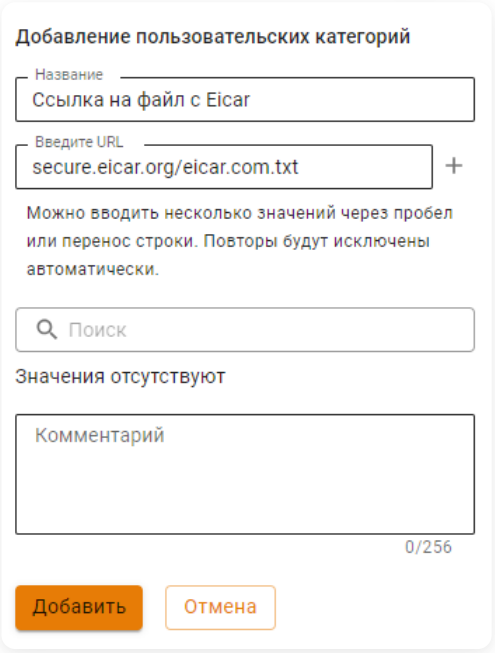
В модули **Контроль приложений** и **Предотвращение вторжений** отправится только тот трафик, который попадает под разрешающее правило **Файрвола** с включенной проверкой через профиль контроля приложений и профиль предотвращения вторжений соответственно.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика?

Для примера использовался тестовый файл с Eicar, доступный для скачивания по ссылке.

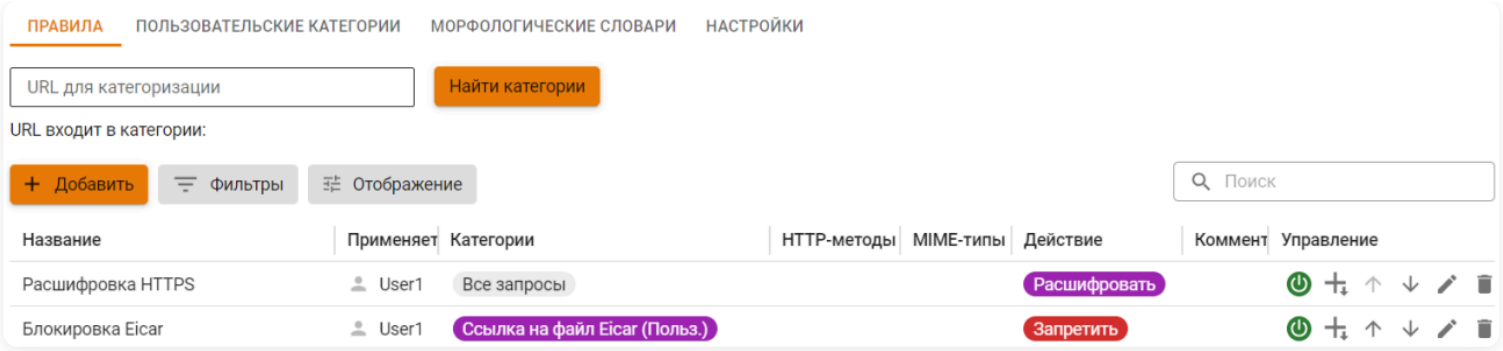
1. Перейдите в раздел **Правила трафика** → **Контент-фильтр** → **Пользовательские категории**. Нажмите **Добавить**.

2. Введите ссылку на ресурс и нажмите + :



3. Перейдите на вкладку **Правила** и создайте два правила для **User1**:

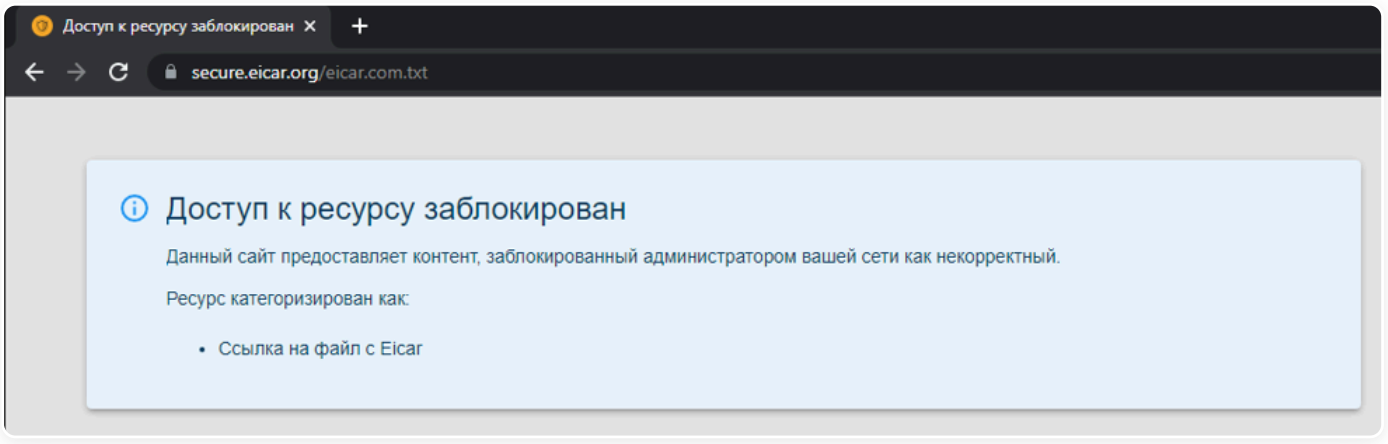
- Правило расшифровки всех HTTPS-запросов, чтобы антивирус мог работать с HTTPS-трафиком.
- Правило блокировки созданной пользовательской категории:



4. Убедитесь, что опция **Антивирус** переведена в положение **Включен**.

5. Авторизуйте пользователя и перейдите по ссылке на скачивание Eicar.

Откроется страница блокировки **Контент-фильтра**:



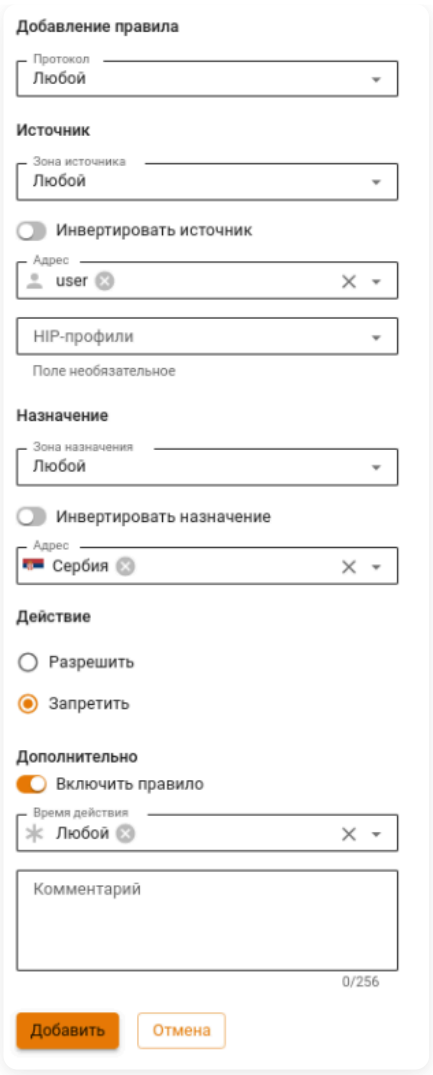
Контент-фильтр обрабатывает трафик приоритетнее, чем антивирусы. Просмотреть информацию о срабатывании правил **Контент-фильтра** можно в **Отчеты** → **Трафик** → **Топ сайтов**.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Файрвол?

Для примера заблокируем пользователю `user` сайт `rts.rs`.

1. Перейдите в раздел **Правила трафика** → **Файрвол**, на вкладку **FORWARD** и нажмите **Добавить**.

2. Заполните поля:

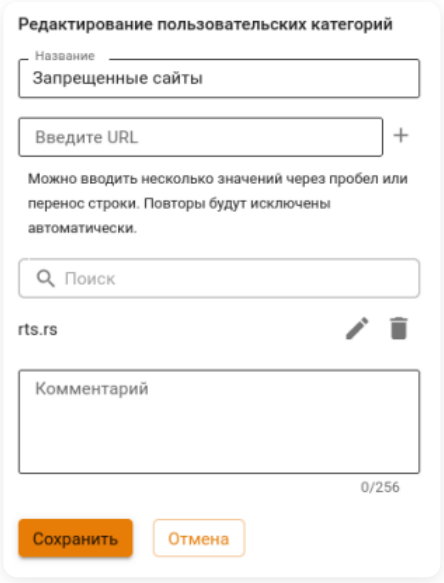


- **Протокол** - выберите **Любой**.
- **Адрес** источника - выберите пользователя `user`.
- **Адрес** назначения - выберите страну **Сербия**.
- **Действие** - выберите **Запретить**.

3. Нажимити **Добавить**.

4. Перейдите в раздел **Контент-фильтр** на вкладку **Пользовательские категории** и нажмите на  напротив категории **Запрещенные сайты**.

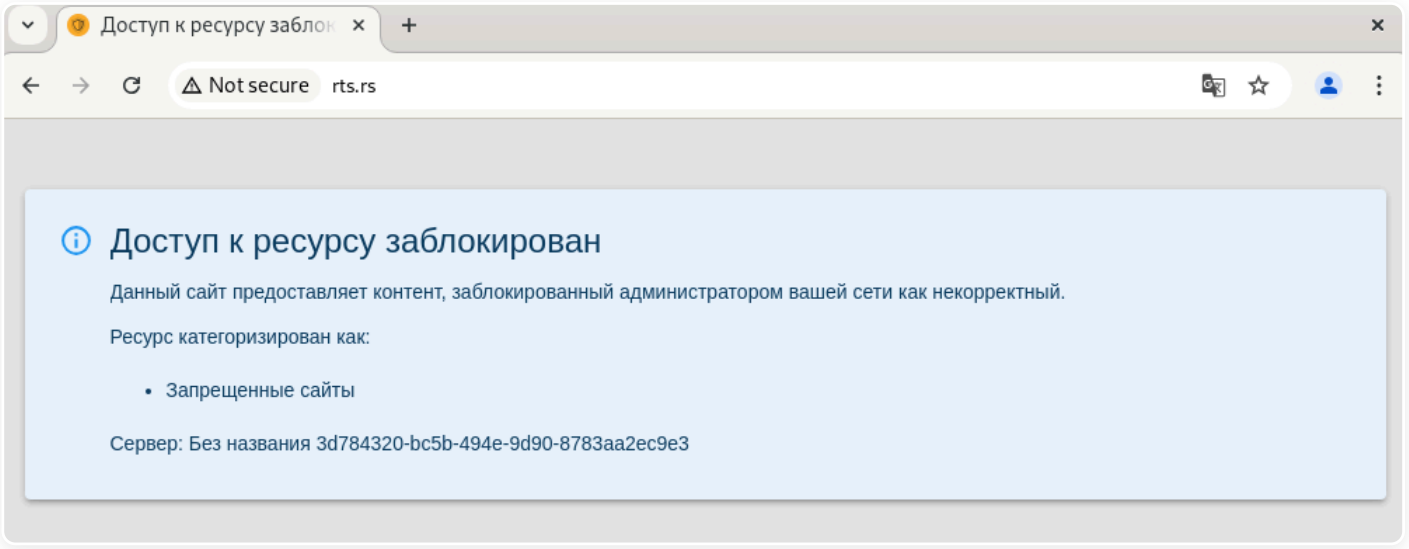
5. Добавьте ссылку на сайт `rts.rs` и нажмите **Сохранить**:



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 **Файрвол**.

Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG

В Ideco NGFW 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. Брокер будет самостоятельно балансировать трафик устройств в локальной сети между нодами созданного кластера.

При падении одной ноды трафик перебалансируется между остальными Ideco NGFW без перерыва в связи. Это реализует схему кластера Active/Active.

Объединять в кластер устройства Ideco NGFW между собой не нужно.

Для корректной работы нод установите одинаковые настройки.

Для централизованного управления нодами Ideco NGFW воспользуйтесь Ideco Center.

Особенности использования схемы:

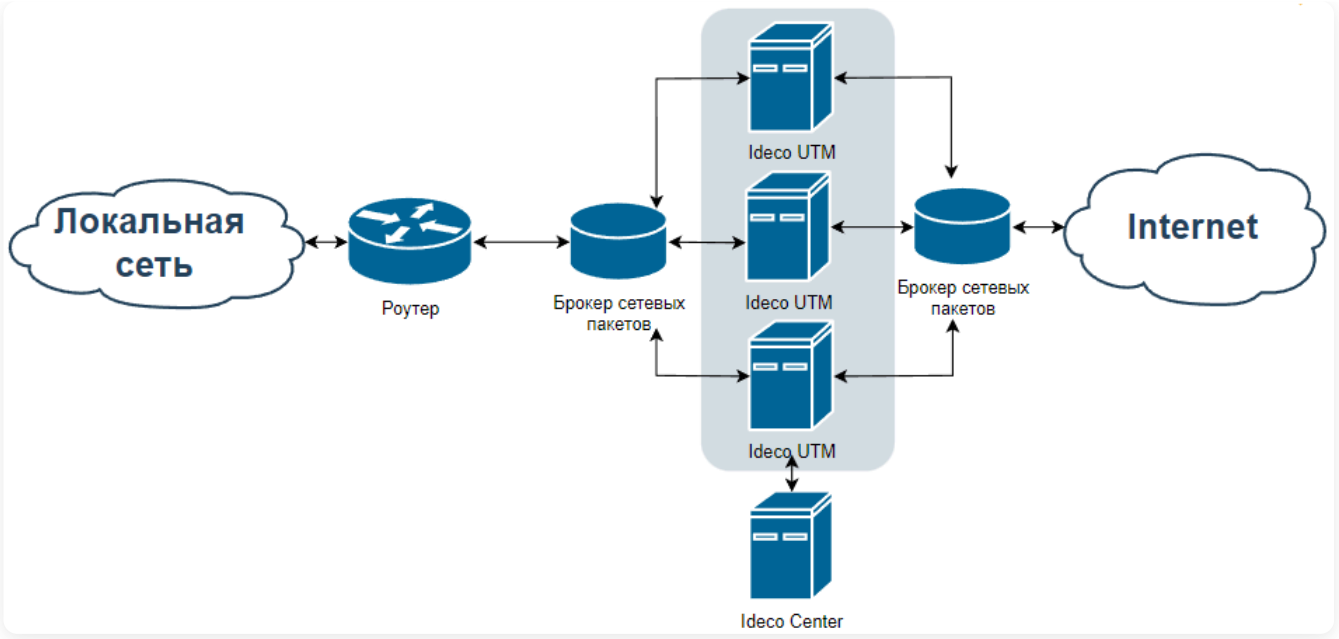
- Настройки, которые нельзя распространить через Ideco Center, придется вручную изменять на каждом Ideco NGFW;
- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено;
- Данные отчетности, логов и мониторинга не синхронизируются между нодами. В каждой ноде 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 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 ниже. На этой основе встройте оба решения в свою сеть.

На каждом Ideco NGFW 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



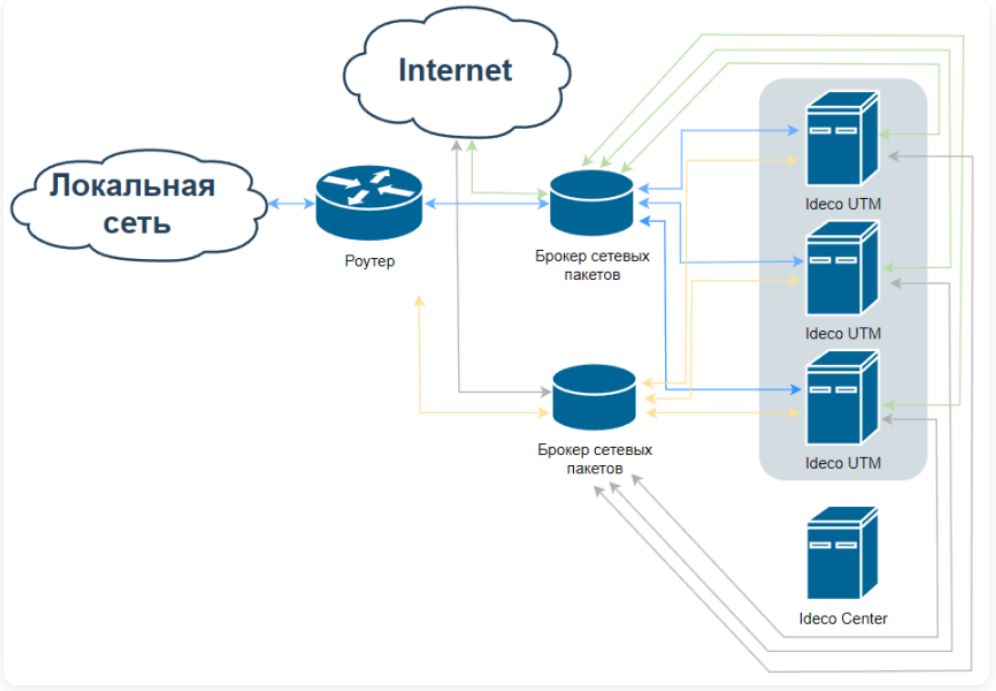
Настройка Ideco NGFW:

На каждом устройстве Ideco NGFW 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.

На каждом Ideco NGFW в качестве шлюза внешнего интерфейса нужно использовать IP-адрес, полученный от провайдера.

Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW



Настройка Ideco NGFW

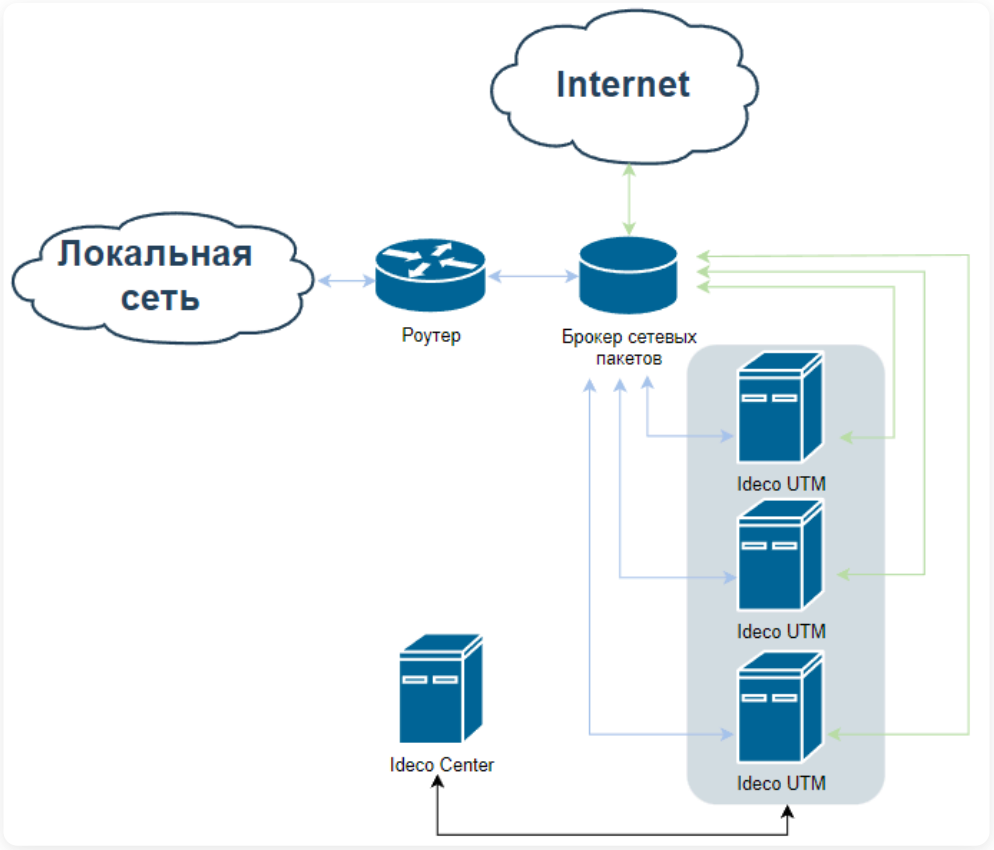
На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW;
- На каждом NGFW будет два локальных и два внешних интерфейса. Шлюзом внешних интерфейсов нужно указать IP-адрес, полученный от провайдера.

На Ideco NGFW в этой конфигурации в разделе Балансировка и резервирование должен быть активирован режим резервирования. Приоритетным внешним интерфейсом должен быть выбран тот, который идет к основному брокеру сетевых пакетов.

Пример 3 - Один брокер, расположенный перед Ideco NGFW



Настройка Ideco NGFW

На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

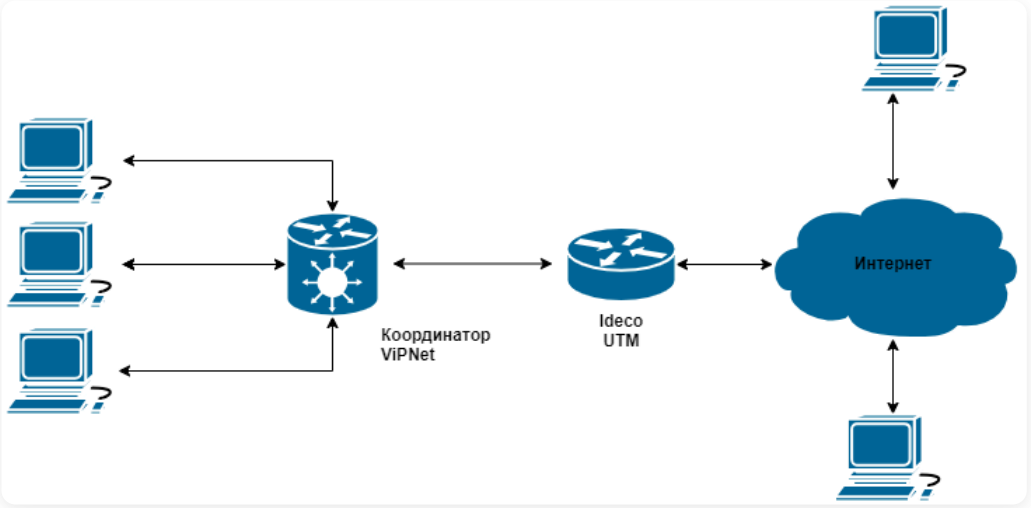
Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW;
- Шлюзом внешнего интерфейса нужно указать IP-адрес, полученный от провайдера.

Рекомендации по настройке NGFW для работы совместно с ViPNet-координатором

ViPNet-координатор используется для шифрования трафика подсети, в которой он является шлюзом. Шифрование позволяет обеспечить конфиденциальность информации, передаваемой по незащищенному каналу.

Схема совместной работы Ideco NGFW с ViPNet-координатором:



Настройка Ideco NGFW и ViPNet-координатора

Для корректной работы Координатора совместно с NGFW выполните действия:

1. Настройте проброс порта udp 55777 на IP адрес координатора в разделе **Файрвол → DNAT (перенаправление портов)**.

2. Переведите Координатор в режим **Со статической трансляцией адресов**.

Работа Координатора в режиме динамической трансляции адресов совместно с Ideco NGFW не гарантируется.

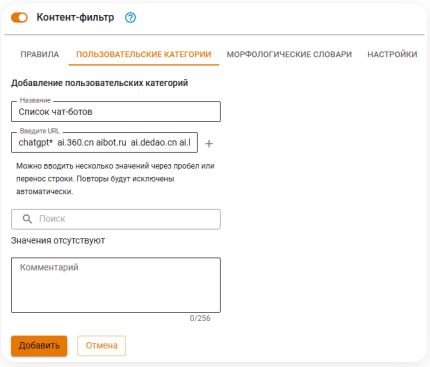
Более подробно о настройке ViPNet можно узнать в статье.

Блокировка чат-ботов

Для блокировки ресурсов, которые взаимодействуют с чат-ботами, необходимо создать правило в **Контент-фильтре**:

1. Перейдите на вкладку **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.

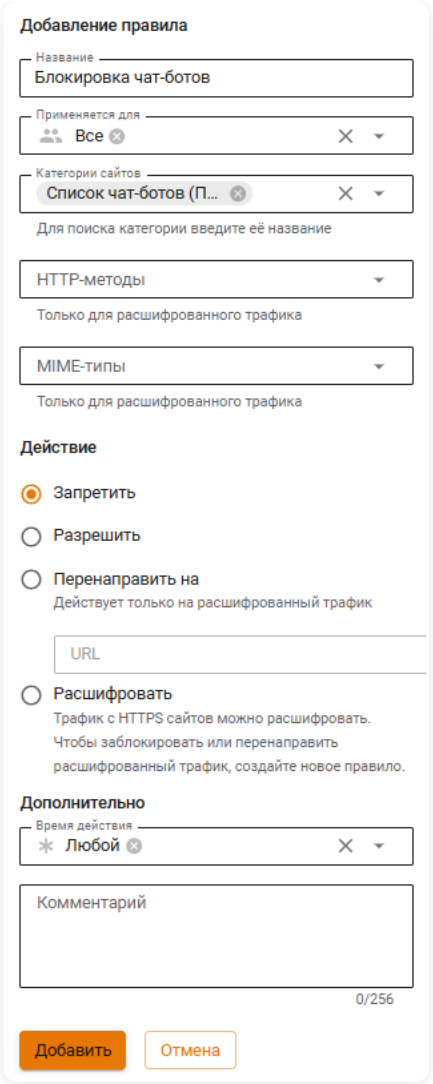
Список URL

```
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 на вкладку **Правила** и добавьте новое правило с действием **Запретить**:



Полезные ссылки

Правила

Описание категорий Контент-фильтра

Таблица портов Ideco NGFW, 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 и настройки интерфейсов.
- TCP-порты 80 и 443, открытые во внешнюю и локальную сеть сразу после установки Ideco NGFW 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	14765 TCP, 3051 UDP
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
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.

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**:

1. Отправляет запрос на адрес https://host:14765/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 `14765`;
- 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:14765/connect`, к которому будет подключаться **Ideco Client**;
- Если ответа со статусом 302 от адреса `https://host:14765/connect` нет, то **Ideco Client** подключится к NGFW по адресу `wss://host:14765/connect`.

Пример правильного редиректа, полученный с помощью утилиты **curl**:

1. **Запрос**: `curl -il https://host.dev:14765/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:14765/connect`.

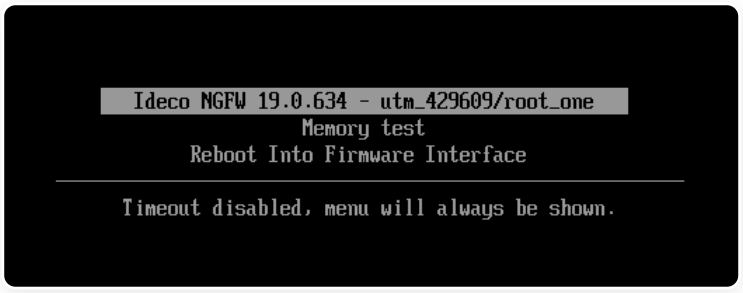
3. Если при попытке доступа к URL-адресу `https://host.dev:14765/connect` не будет получен ответ с кодом 302, то **Ideco Client** подключится к NGFW по адресу `wss://host.dev:14765/connect`.

Как включить таймер при загрузке Ideco NGFW?

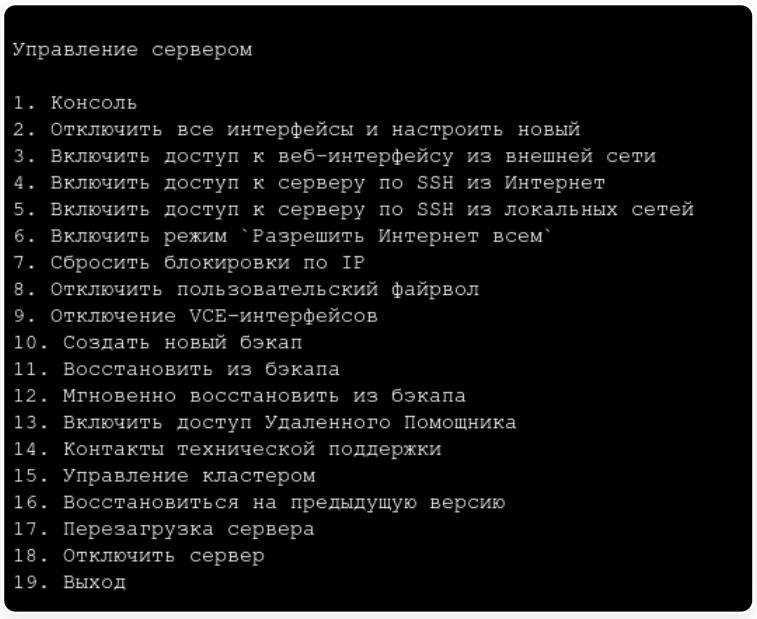
При отключении таймера также отключается автоматический выбор пункта меню. В этом случае система не загрузится сама после обновления, рестарта или переключения ноды в режиме кластеризации до момента нажатия **Enter**.

Для включения таймера выполните действия:

1. При загрузке сервера выберите Ideco NGFW, 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**.

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
```

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
```

Добавление IP-адреса в белый список fail2ban

Система защиты fail2ban блокирует IP-адреса при обнаружении подозрительной активности. В редких случаях заблокирован может быть и доверенный адрес. Чтобы предотвратить такую блокировку, добавьте IP-адрес в белый список fail2ban. 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 доверенный IP-адрес с маской `/32` или подсеть с нужной маской в конец строки через пробел. Для добавления нескольких IP-адресов укажите их последовательно через пробел:

```
# ICS-27477: Здесь можно добавить IP-адреса в исключения для fail2ban.
# Этот файл будет переноситься с бэкапом при обновлении на новую версию.
[DEFAULT]
ignoreip = 127.0.0.1/8 ::1 92.167.132.63/32 43.156.101.90/32
```

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.

Как настроить автоматическое включение аппаратного комплекса Ideco NGFW после сбоя питания

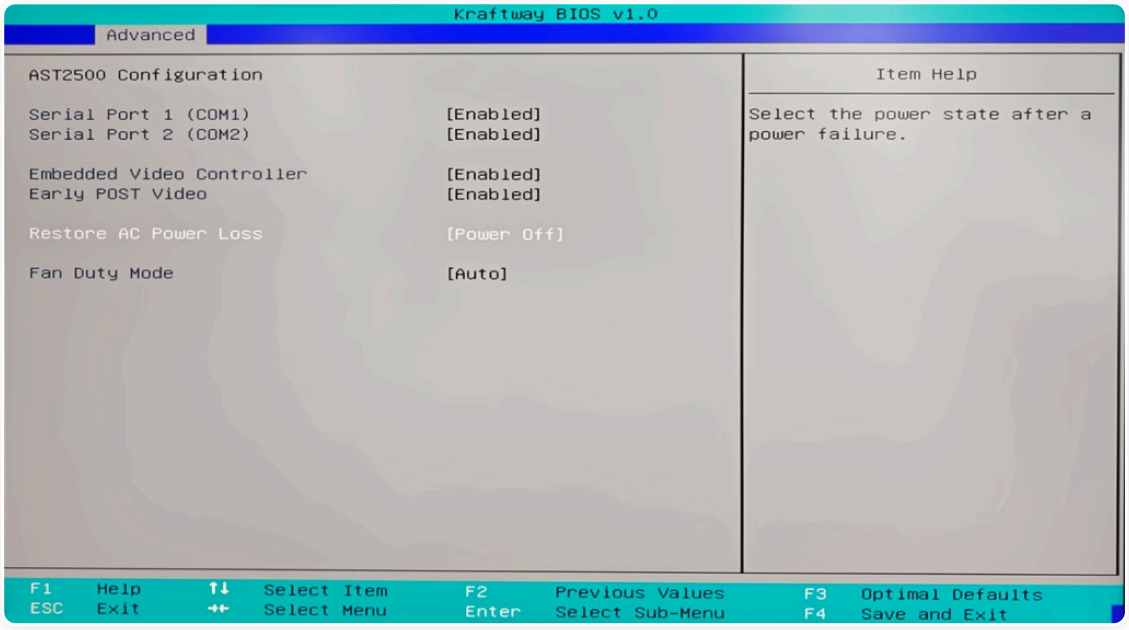
Решение подходит для всех моделей аппаратных комплексов Ideco NGFW.

Для автоматического восстановления работы аппаратного комплекса Ideco NGFW после сбоя электропитания необходимо активировать опцию **Restore AC Power Loss (Восстановления питания после сбоя)** в BIOS. Для включения опции:

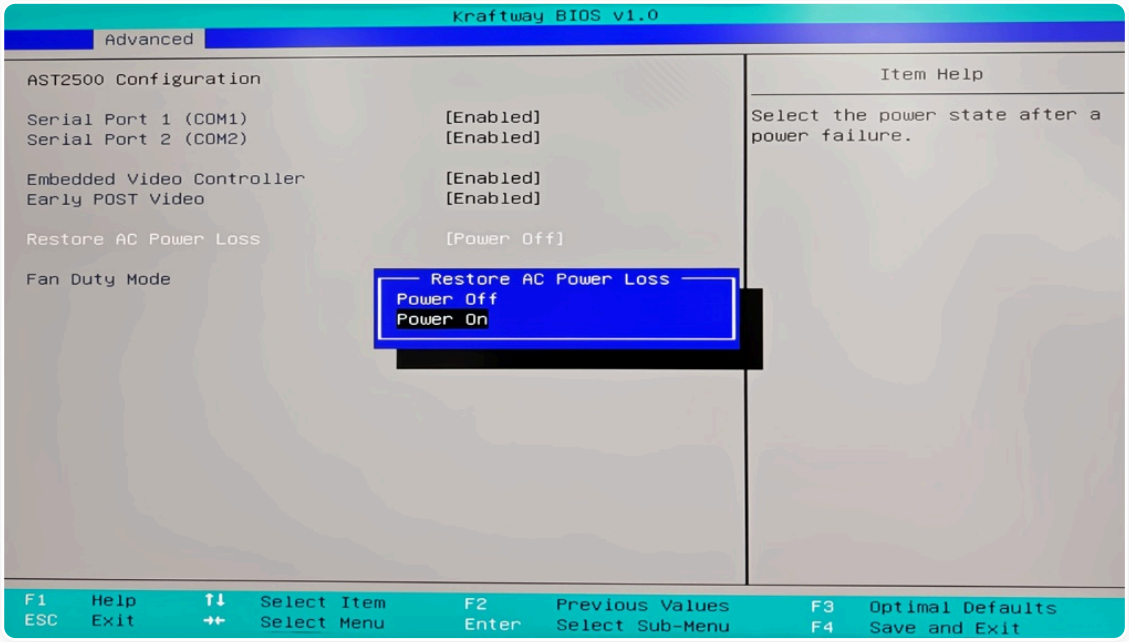
1. Запустите перезагрузку сервера.

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.

Использование собственного CA-сертификата в Контент-фильтре

В **Контент-фильтре** возможно использование не корневого сертификата Ideco NGFW, 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.

3. Загрузка CA-сертификата на сервер NGFW.

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) [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 []:
```

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 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-----
```

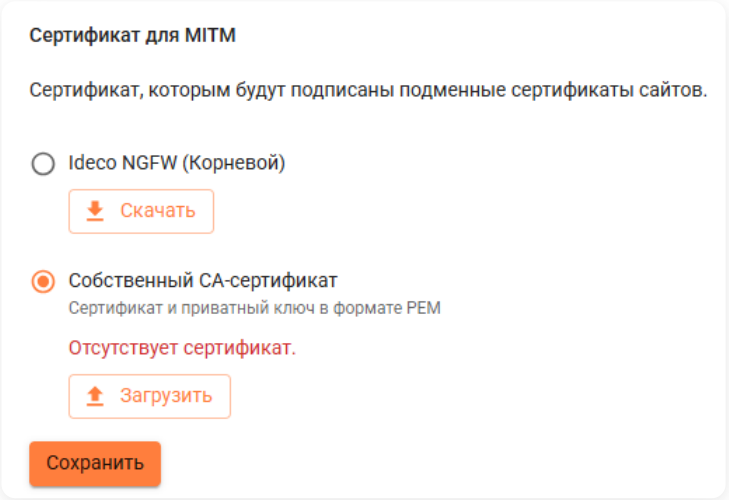
4. Сохраните файл бандла с именем, отличным от PEM-файла CA-сертификата, и расширением **.pem**, например, `ideco-cf_root-ca-key.pem`.

Шаг 3. Загрузка сертификата на сервер

Загрузите файл бандла на Ideco NGFW. 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**:

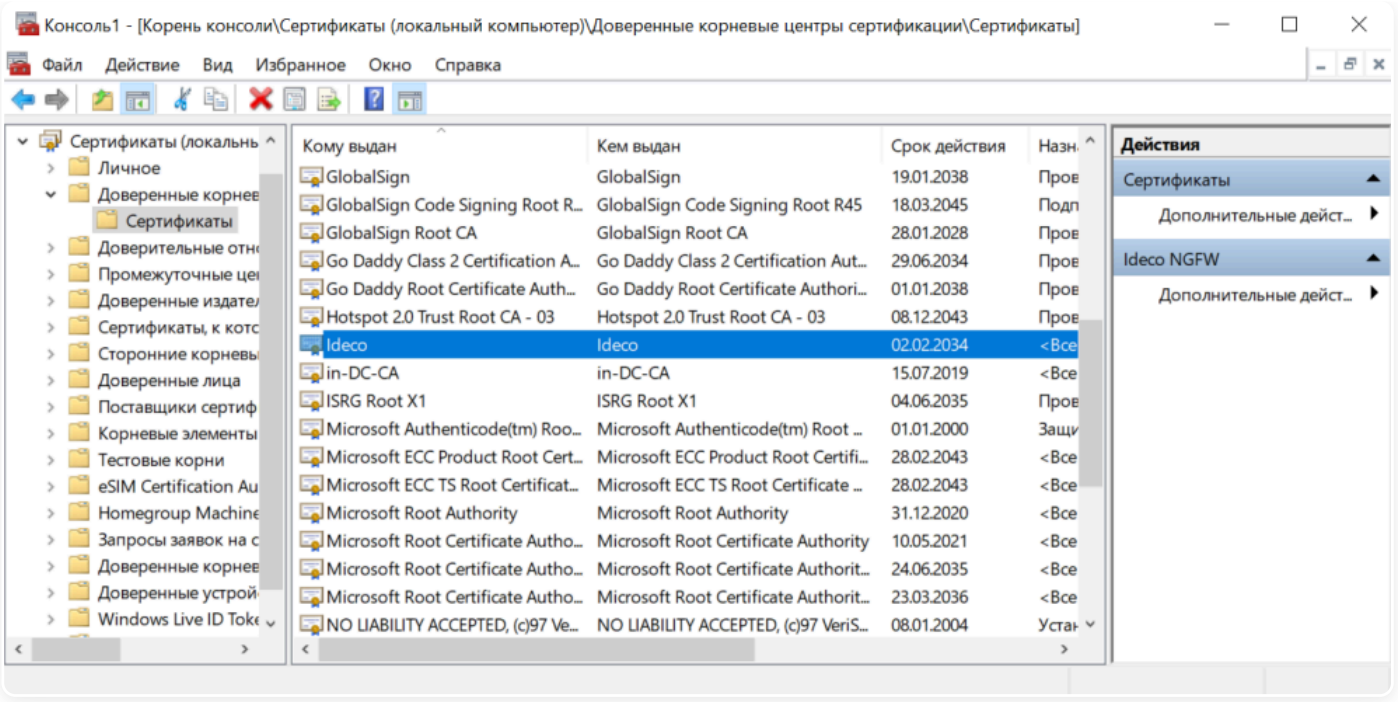
4. В открывшемся окне выберите пункт **Учетной записи компьютера** и нажмите **Далее**:

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:



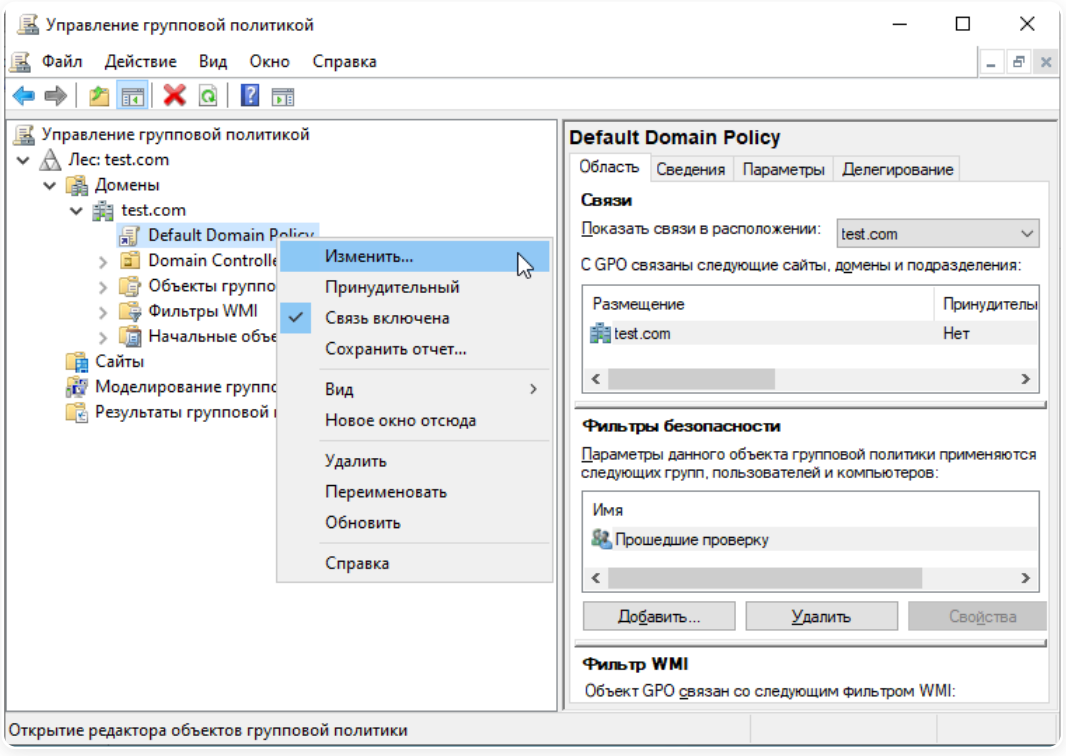
Автоматическая установка CA-сертификата через Active Directory

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, можно установить сертификат Ideco NGFW для всех пользователей автоматически:

1. Зайдите на контроллер домена с правами администратора.

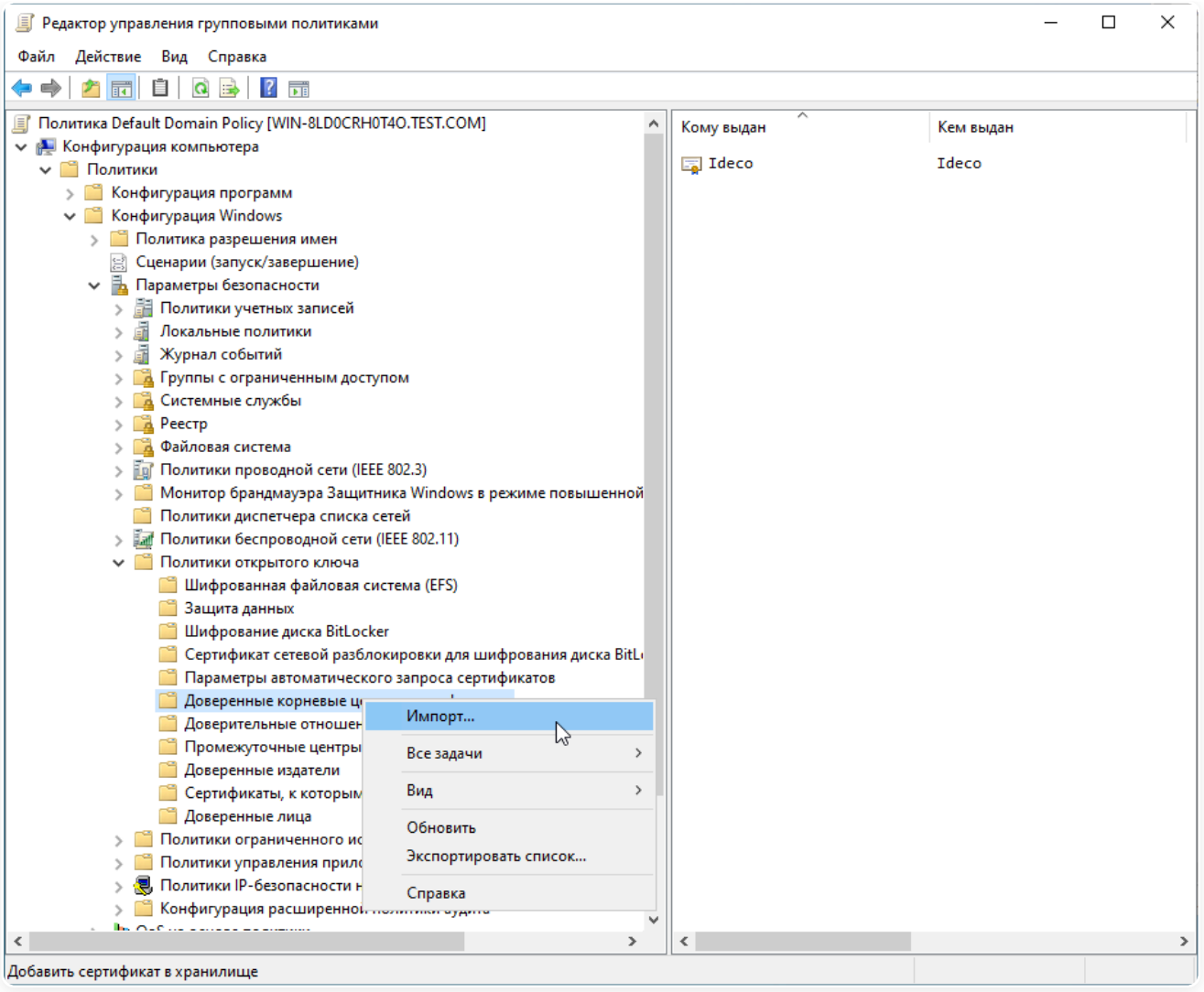
2. Запустите оснастку **Управление групповой политикой**, выполнив команду **gpmc.msc**.

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:



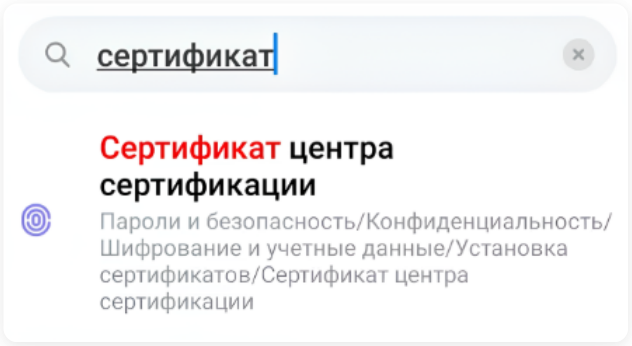
6. После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Как установить сертификат Ideco NGFW на Android

1. Скачайте сертификат Ideco NGFW на Android-устройство.

2. Перейдите в **Настройки**.

3. В поиске введите `Сертификат`:

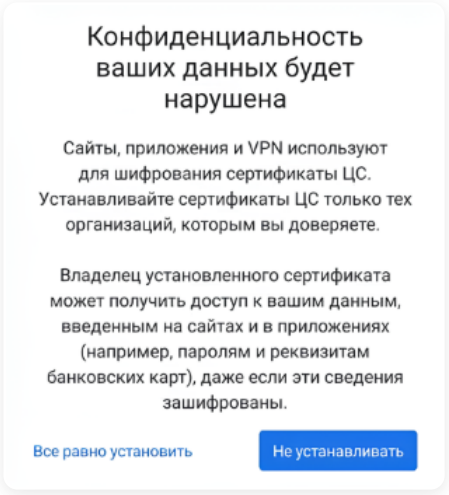


4. Выберите **Сертификат центра сертификации**.

> В зависимости от версии Android и версии оболочки путь может отличаться. Ориентируйтесь на расположение **Пароли и безопасность/ Конфиденциальность/Шифрование и учетные данные**.

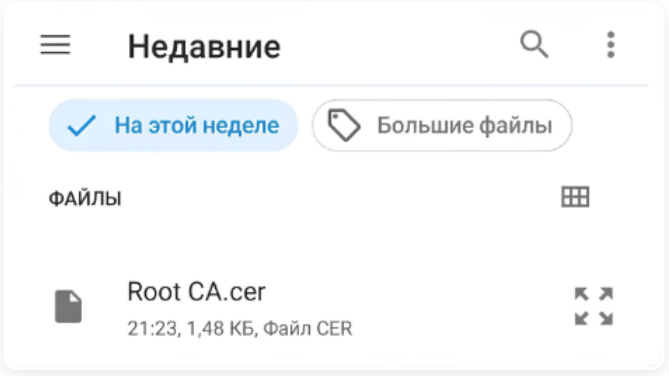
5. Если появится окно **Укажите название сертификата**, введите удобное вам название.

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**.

Как публиковать веб-приложения

Публикация веб-серверов возможна через обратный прокси-сервер.

Сброс пароля IPMI на сервере NGFW

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`. Данный метод позволяет изменить пароль для существующей учетной записи.

Для сброса пароля выполните действия:

Шаг 1. Установка ipmitool

Установка утилиты `ipmitool` на сервер NGFW возможна только через техническую поддержку Ideco.

Шаг 2. Смена пароля

После установки `ipmitool` выполните действия:

1. Для смены пароля потребуется узнать ID пользователя. В терминале NGFW 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 3. 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.

Диагностика проблем

Ошибка при открытии сайта "ERR_CONNECTION_TIMED_OUT" или "Не открывается сайт"

Перейти >

Что делать, если не работает интернет

Перейти >

Ошибка при авторизации "The browser is outdated"

Перейти >

Если соединение по IPsec не устанавливается

Перейти >

Ошибка "400 Bad Request Request Header Or Cookie Too Large" при авторизации в браузерах

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Видеоинструкцию смотрите по ссылкам:

- Youtube
- docs.ideco.ru

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.

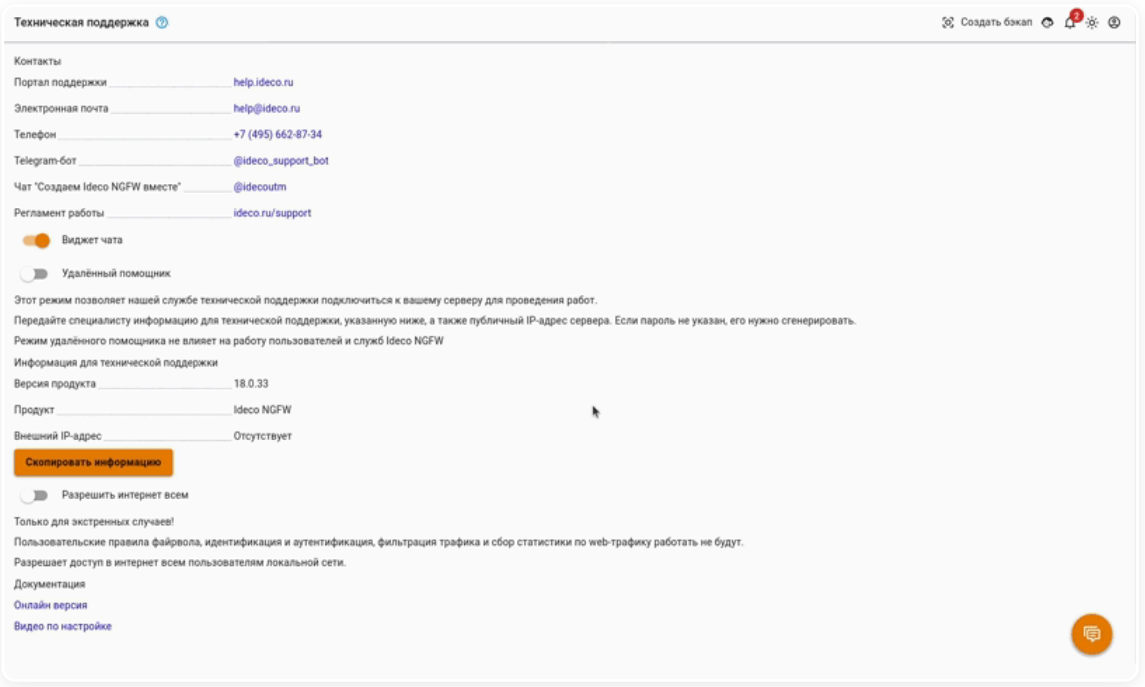
Откройте сайт с устройства вне локальной сети NGFW. Например, со смартфона через мобильный интернет. Если сайт доступен, перейдите в веб-интерфейс NGFW.

Для определения модуля фильтрации, блокирующего сайт, можно проверить логи в разделах Системный журнал. Это может помочь определить причину возникшей проблемы и более точно ее диагностировать.

Шаг 1. Проверьте, открывается ли сайт в режиме **Разрешить интернет всем**

1. Нажмите на в верхней правой части веб-интерфейса NGFW.

2. Переведите опцию **Разрешить интернет всем** в положение **Включен**:



3. Откройте сайт.

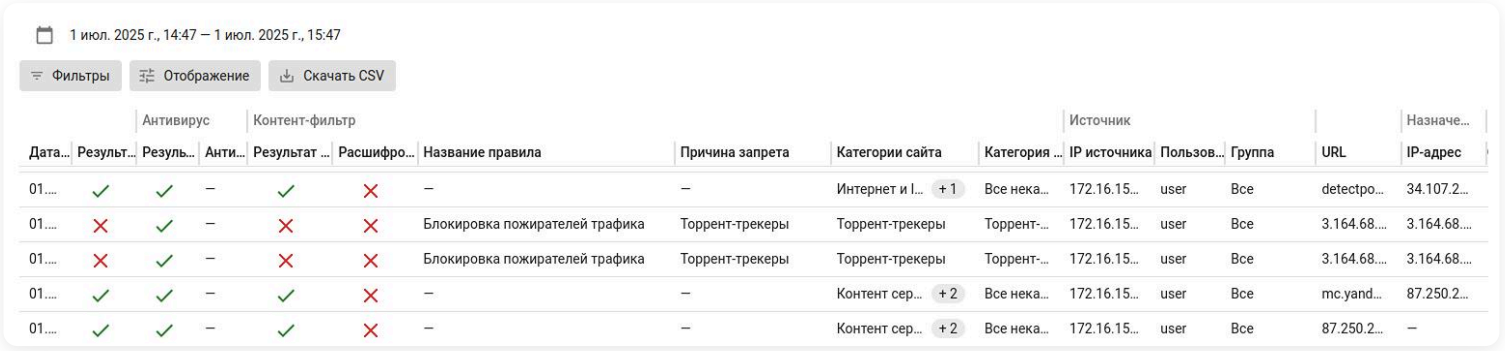
Если сайт не открывается, проверьте, откроется ли сайт на другом устройстве с того же IP-адреса:

- Если не открывается, рекомендуем обратиться к провайдеру. Скорее всего, провайдер блокирует IP-адрес или адрес сайта;
- Если сайт открывается, проверьте настройки устройства пользователя.

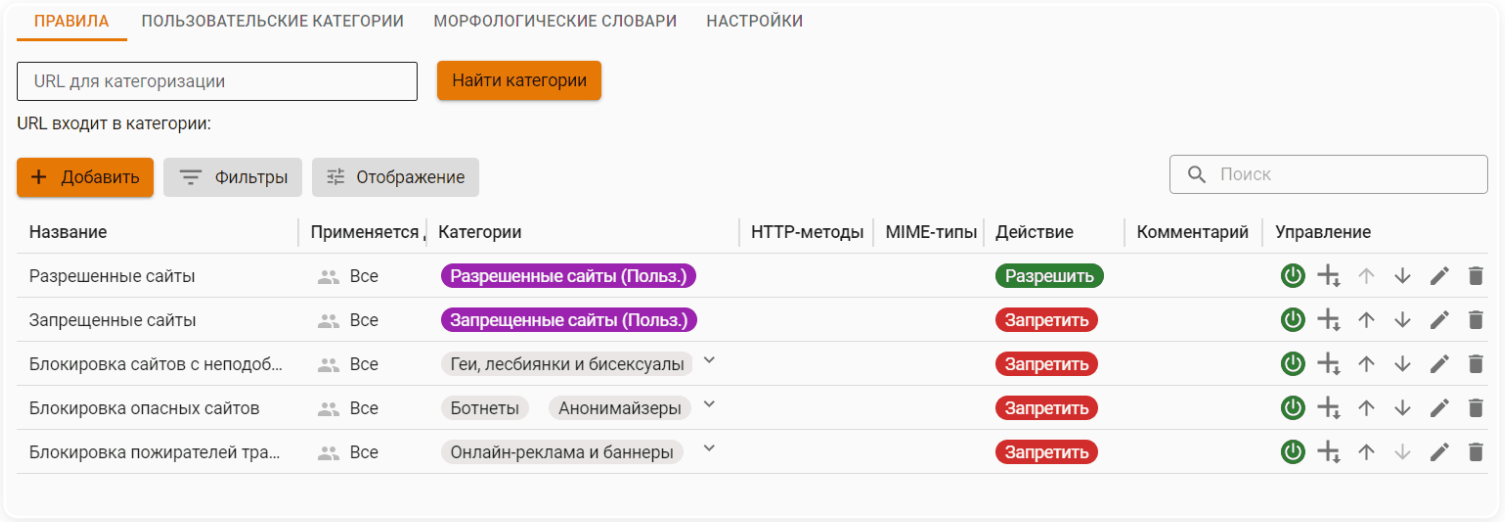
Шаг 2. Проверьте, не блокируется ли сайт правилом Контент-фильтра

1. Откройте сайт с устройства пользователя.

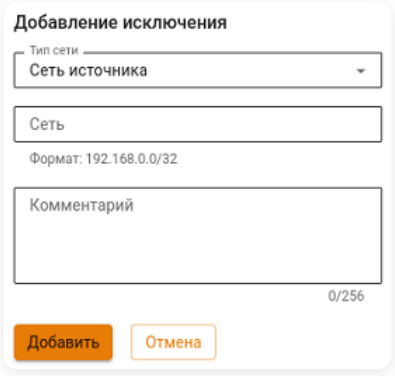
2. В NGFW перейдите в раздел **Отчеты и журналы** → **Журнал веб-трафика** и посмотрите, какое правило блокирует сайт:



3. Для поиска блокирующего правила также можно ввести URL сайта в строку поиска категорий **Контент-фильтра** на вкладке **Правила** в разделе **Правила трафика** → **Контент-фильтр**:



4. Если сайт блокируется правилом **Контент-фильтра**, измените его настройки или добавьте сайт в исключения в разделе **Сервисы** → **Прокси** на вкладке **Исключения**:



В раздел **Сервисы** → **Прокси** → **Исключения** рекомендуем добавлять заведомо надежные сервисы.

Добавлять в исключения адреса клиентов вашей сети не рекомендуется, так как в этом случае их веб-трафик не будет фильтроваться правилами **Контент-фильтра** и не будет попадать в отчеты.

Шаг 3. Проверьте, не блокирует ли сайт правило **Файрвола**

Найдите блокирующее правило одним из способов:

Первый способ. Счетчик срабатываний

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **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 раздел **Правила трафика** → **Файрвол** → **FORWARD**.

2. Создайте тестовое правило, разрешающее любой трафик:

3. Правило добавится в конец таблицы. Поместите созданное правило на одну позицию вверх, нажав на кнопку .

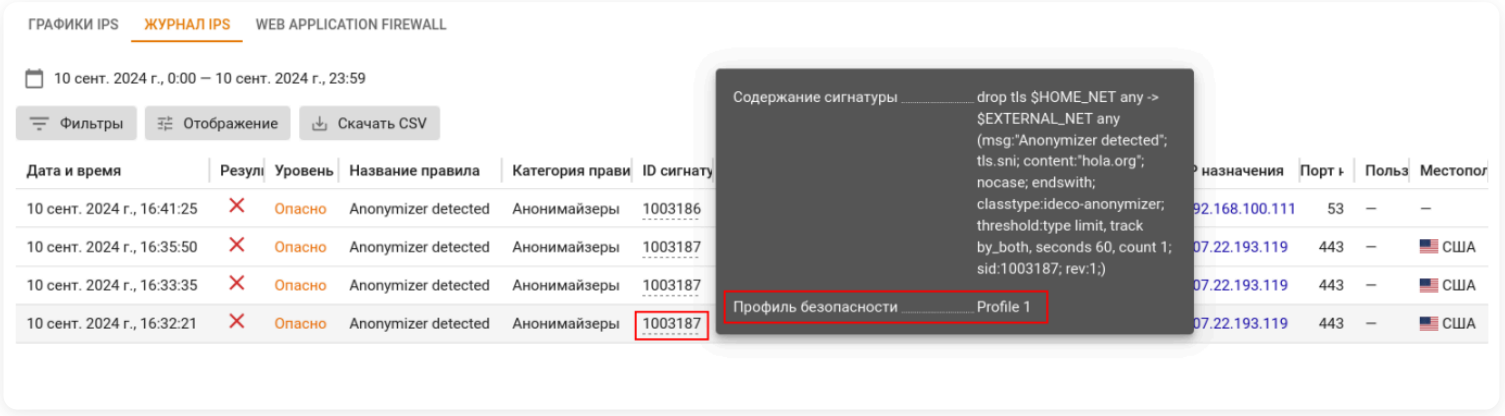
4. Откройте сайт с устройства пользователя.

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:

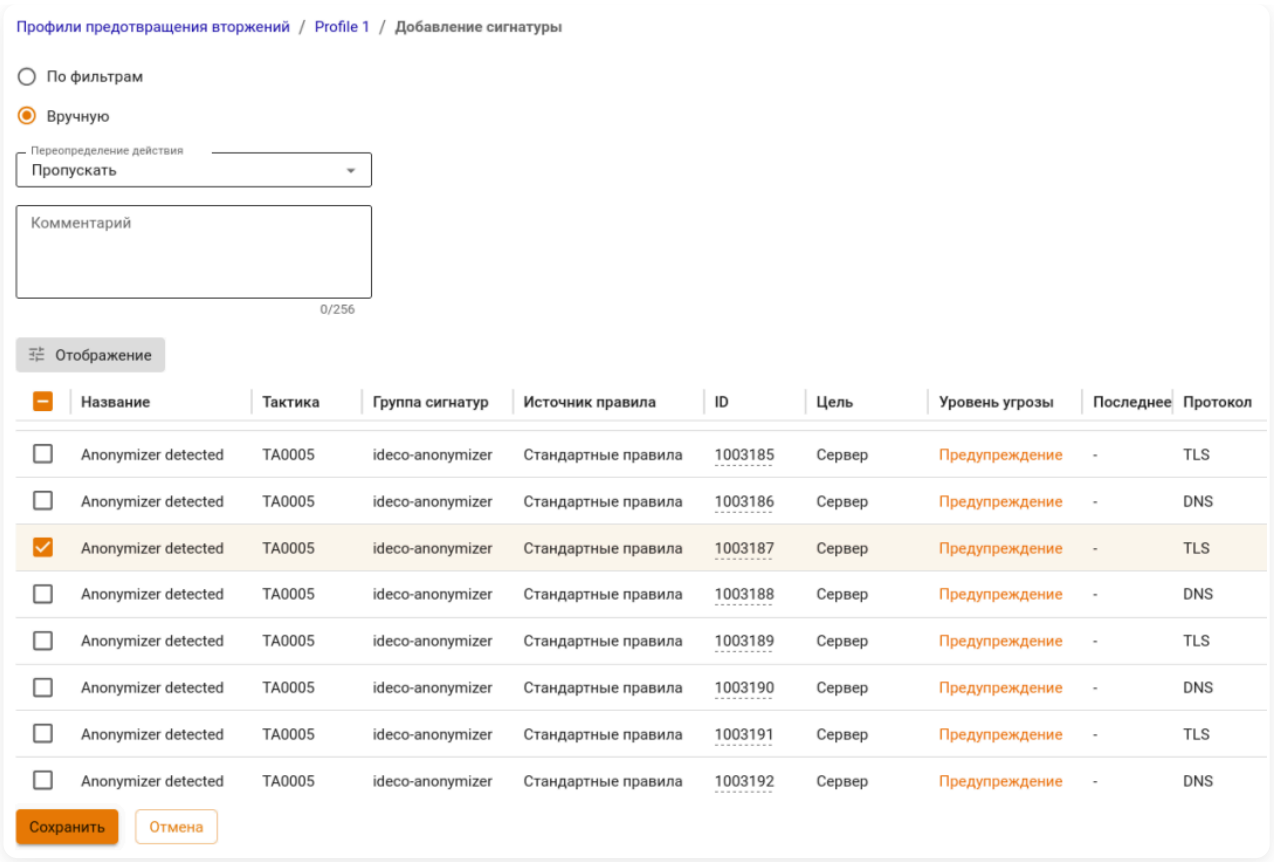
1. Перейдите в раздел **Отчеты и журналы** → **События безопасности** на вкладку **Журнал IPS** и найдите в таблице ID сигнатуры, заблокировавшей сайт, и название профиля, к которому она относится:



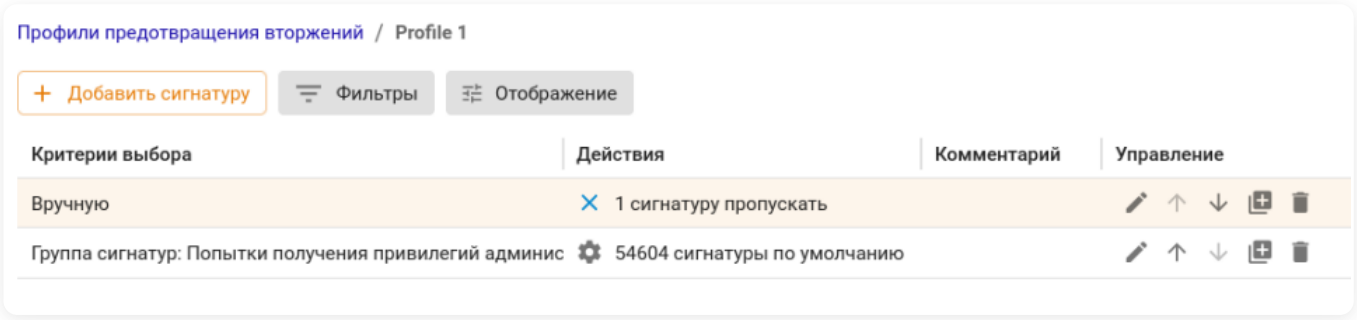
2. Перейдите в раздел **Профили безопасности** → **Предотвращение вторжений**, нажмите на напротив профиля, заблокировавшего сайт, и выберите **Сигнатуры**.

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 раздел **Отчеты и журналы** → **Трафик**.

2. В виджете **Топ заблокированных протоколов** найдите протоколы, которые блокируются **Контролем приложений**.

3. Перейдите в раздел **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 раздел **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 у пользователей отсутствует интернет, выполните шаги для диагностики и решения проблемы.

Шаг 1. Проверьте лицензию

Перейдите в раздел **Управление сервером** → **Лицензия** и проверьте, привязана ли лицензия к серверу.

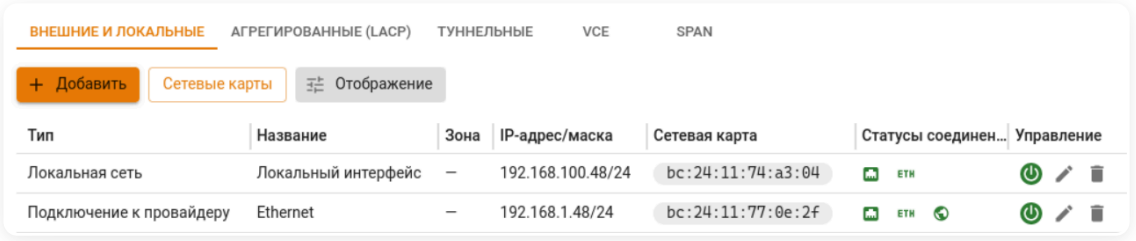
Шаг 2. Проверьте настройки Файрвола

Перейдите в раздел **Правила трафика** → **Файрвол** и отключите в разделах **FORWARD** и **INPUT** правила, запрещающие все.

Шаг 3. Проверьте настройки интерфейсов

Проверьте, правильно ли настроен внешний интерфейс

Перейдите в **Сервисы** → **Сетевые интерфейсы**. Если Ideco NGFW использует выделенный интерфейс для подключения к провайдеру и не работает только как прокси, установите тип **Подключение к провайдеру**. При типе **Локальный интерфейс** удалите и добавьте интерфейс заново с типом **Подключение к провайдеру**:



Проверьте статус подключения

В созданном подключении иконка должна быть , в ином случае:

1. Проверьте настройку VLAN:

- Если провайдер требует VLAN, убедитесь, что тег указан.
- Если в реквизитах провайдера VLAN не указан, убедитесь, что тег не указан.

2. Проверьте ICMP-запросы.

Выполните команду `ping` до адреса, указанного в разделе **Сервисы** → **Балансировка и резервирование** → **Адреса для проверки связи**. Если провайдер блокирует ICMP-запросы, то значок останется , Ideco NGFW не сможет построить внешние маршруты, и интернет работать не будет. В этом случае:

- Удалите все адреса из списка.
- 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 Разрешить интернет всем

> Используйте опцию только для диагностики.

В правой верхней части окна Ideco NGFW нажмите на иконку технической поддержки,а затем нажмите **Разрешить интернет всем**. После включения:

- Сбор веб-статистики будет отключен.

- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включён автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Файрвола** и DNAT.

Цикл обработки трафика в Ideco NGFW описан в статье.

Если интернет появился, то проблема в неверно настроенной авторизации, правилах файрвола или маршрутизации.

Шаг 5. Проверьте настройки пользователей

Проверьте авторизацию пользователей

- В Ideco NGFW 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 Active Directory должны быть выгружены в Ideco NGFW.
- Интеграция с RADIUS должна быть настроена.
- Сопоставление IP-адреса и пользователя не требуется для авторизации пользователей терминального сервера через прямой прокси.

Проверьте тип авторизации

Если пользователь успешно авторизован в системе, то проверьте, какой тип авторизации используют:

- Если используется **MAC и IP+MAC авторизация**, то на компьютере клиента шлюзом по умолчанию должен быть указан Ideco NGFW. Если шлюз не настроен корректно, авторизация не будет работать.
- Если используется **Веб-аутентификация**, то пользователю необходимо открыть браузер и попытаться перейти на любой внешний сайт (например, google.com).
- Если используется **Авторизация по логам**, то проверьте настройки на стороне контроллера домена. Не рекомендуем использовать этот тип авторизации.

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 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 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

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 >= 90;
- Firefox версия >= 78;
- Safari версия >= 14.

Рекомендуем обновить браузер до минимально поддерживаемой версии.

Для продолжения авторизации несмотря на риски потребуется нажать **I understand the risks and wish to continue**.

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 раздел **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.

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:

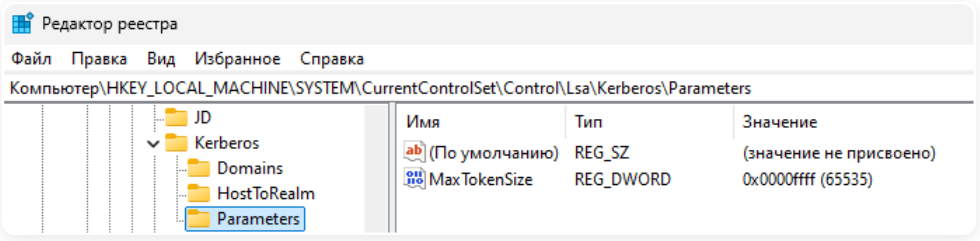
- **Windows 7 и Windows Server 2008R2** - 12000 байт;
- **Windows 8 и Windows Server 2012 (включая Windows Server 2022 и Windows 11)** - 48000 байт.

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
```

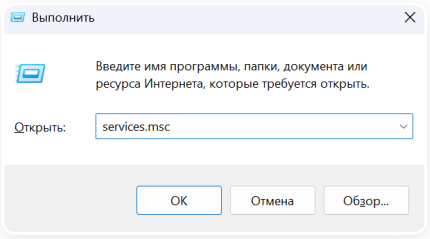
Как включить режим отладки для Ideco Client

При возникновении ошибки в работе Ideco Client включите режим отладки для записи подробных логов. Эти данные помогут в диагностике проблемы и при обращении в техническую поддержку.

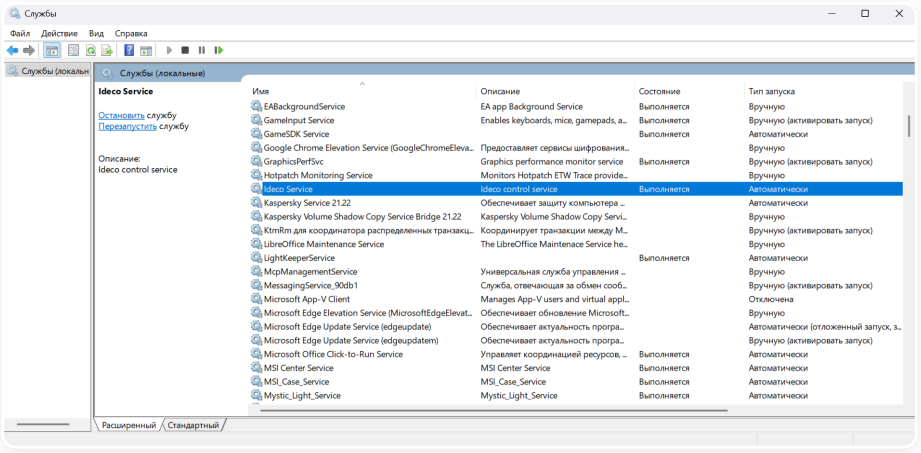
Необходима учетная запись с правами администратора.

Для включения режима:

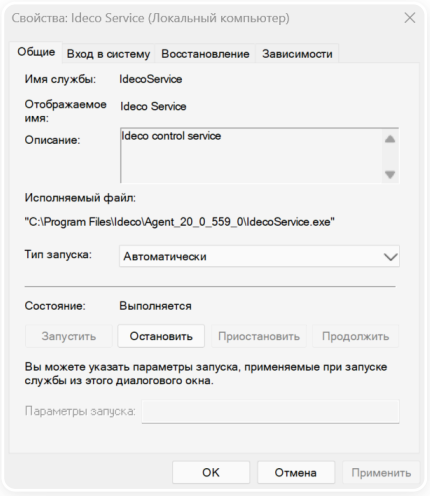
1. Нажмите **Win+R**, введите `services.msc` и нажмите **Ок**:



2. Найдите службу **Ideco Service**:

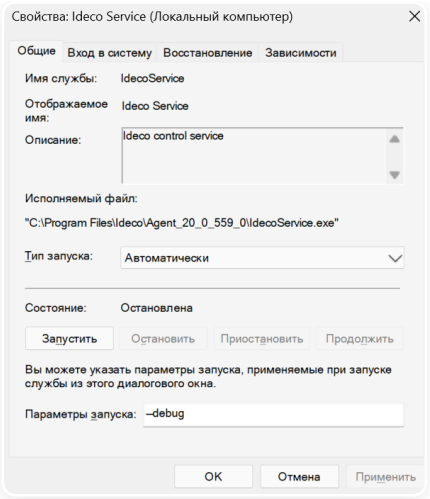


3. Двойным кликом откройте свойства, нажмите **Остановить** и дождитесь остановки службы:



Если произошла ошибка остановки службы, дождитесь запуска службы и остановите службу повторно.

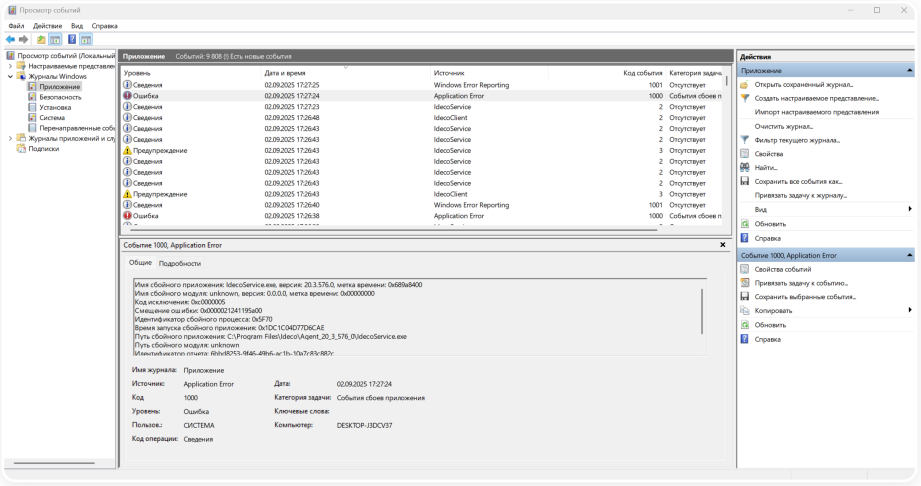
4. В поле **Параметры запуска** введите `--debug` и нажмите **Запустить** для старта службы:



Не закрывайте окно **Свойства: Ideco Service**, иначе режим отладки работать не будет.

5. Запустите Ideco Client, чтобы воспроизвести ошибку.

6. Чтобы посмотреть логи, нажмите **Пуск**, откройте **Просмотр событий**, перейдите в раздел **Журналы Windows** → **Приложения** и найдите запись с ошибкой:



При необходимости обратитесь в техническую поддержку.

Контроль целостности бинарных файлов и целостности конфигурации версии ФСТЭК

Многофункциональный межсетевой экран уровня сети проверяет контрольные суммы исполняемых файлов, входящих в его состав, а также конфигурационных файлов в модуле **etcd** с периодичностью в 30 секунд.

Цели выполнения тестовой процедуры

Подтверждение реализации механизма, обеспечивающего:

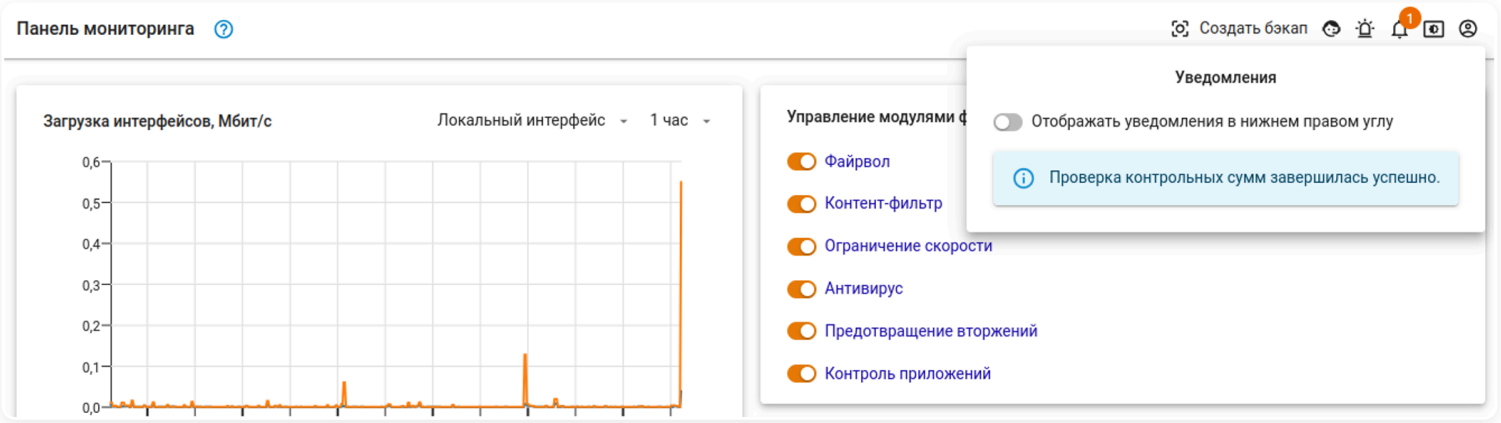
- Запуск программ самотестирования для демонстрации правильного выполнения функций безопасности.
- Возможность верифицировать уполномоченным пользователям целостность данных.
- Возможность верифицировать целостность хранимого выполняемого кода функций безопасности.

Описание тестовой процедуры

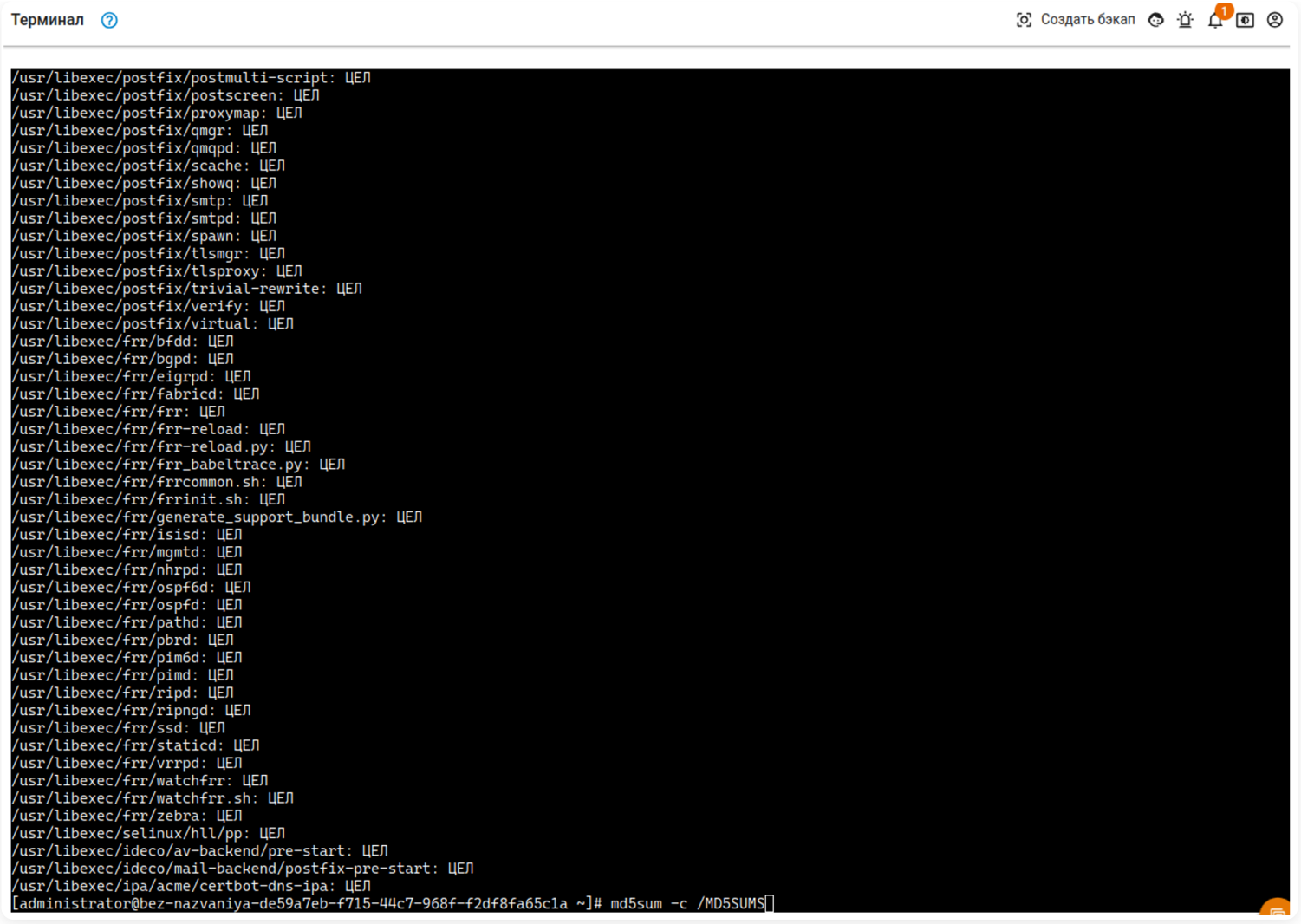
Проверка системы

1. Перезагрузите сервер, на котором работает Ideco NGFW.

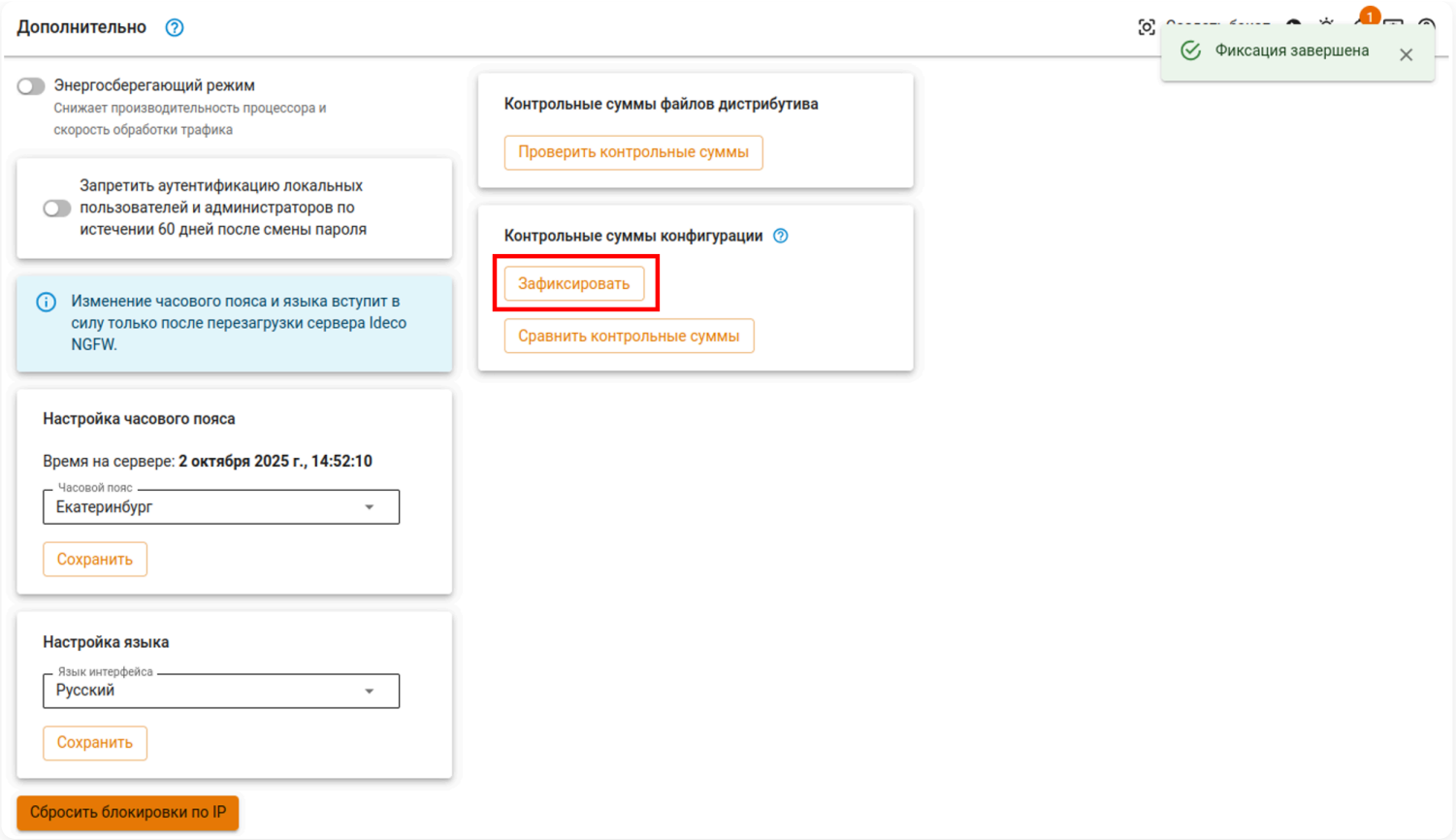
2. Выполните авторизацию в веб-интерфейсе сервера управления Ideco NGFW (`https://192.168.100.2:8443`), используя учетную запись, обладающую ролью **Администратор**. Убедитесь, что по итогу проверки контрольных сумм появляется уведомление **Проверка контрольных сумм завершена успешно**:



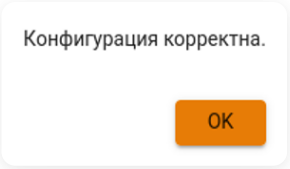
3. Перейдите в **Управление сервером** → **Терминал**. Выполните команду `md5sum -c /MD5SUMS` для проверки неизменности системных файлов. Убедитесь, что команда выполнилась без ошибок:



4. Перейдите в **Управление сервером** → **Дополнительно**. Для проверки неизменности правил фильтрации и настройки параметров NGFW нажмите **Зафиксировать**:

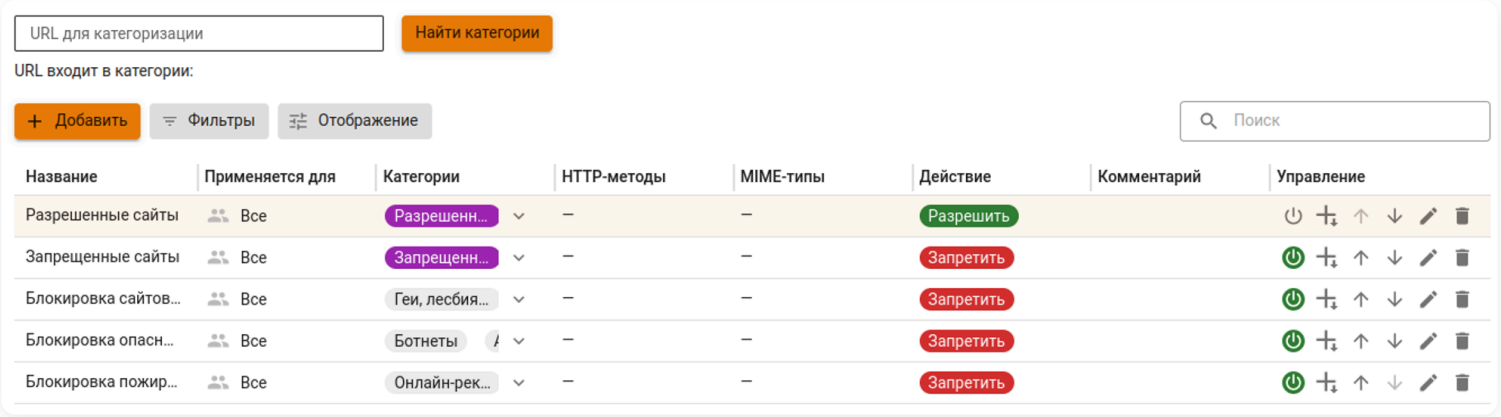


5. Нажмите **Сравнить контрольные суммы**. Убедитесь, что проверка целостности конфигурации завершается успешно:

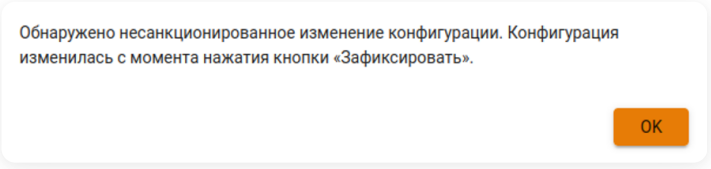


Проверка реакции на изменение конфигурации

1. Перейдите в **Правила трафика** → **Контент-фильтр**. Отключите правило контентной фильтрации:



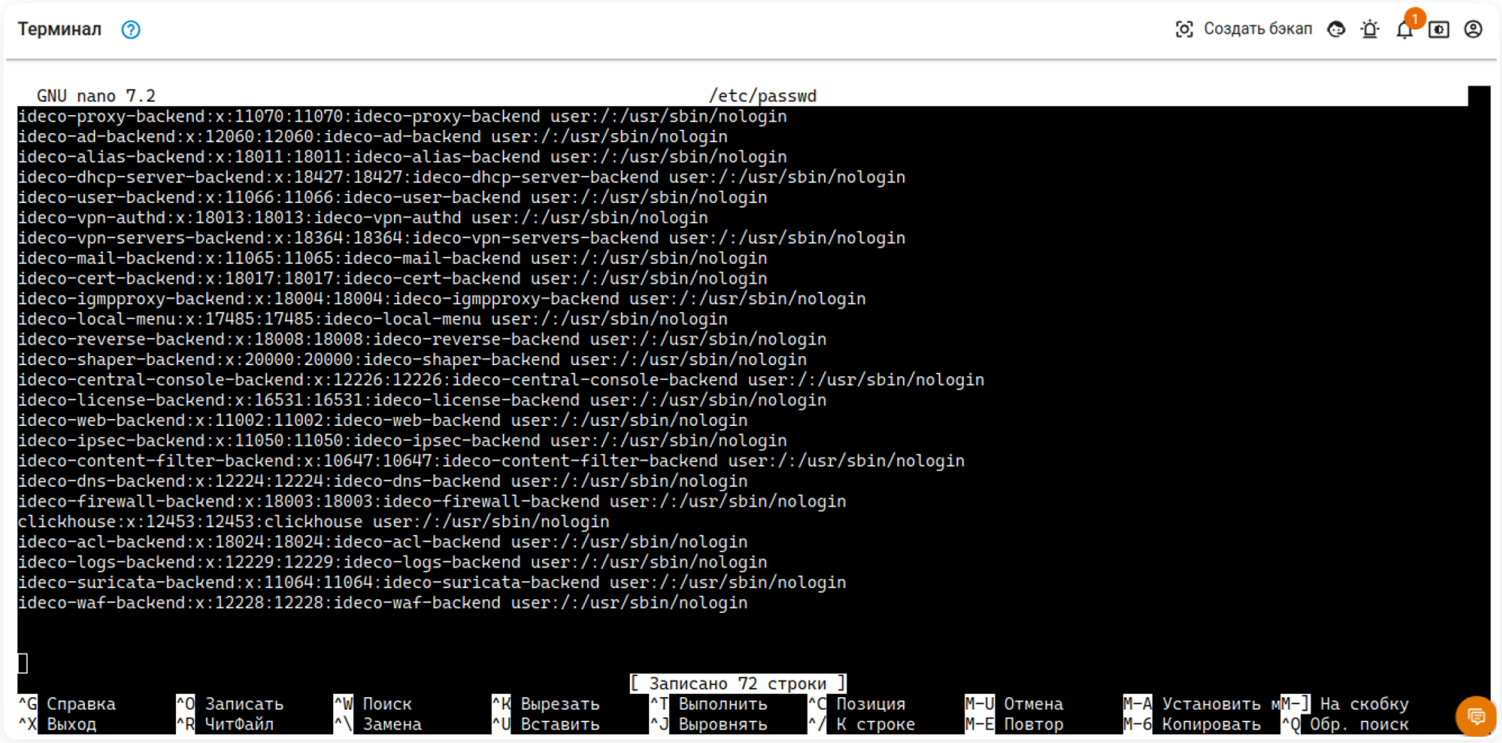
2. Перейдите в **Управление сервером** → **Дополнительно**. Нажмите **Проверить целостность**. Убедитесь, что проверка целостности конфигурации завершается с ошибкой, так как была изменена конфигурация:



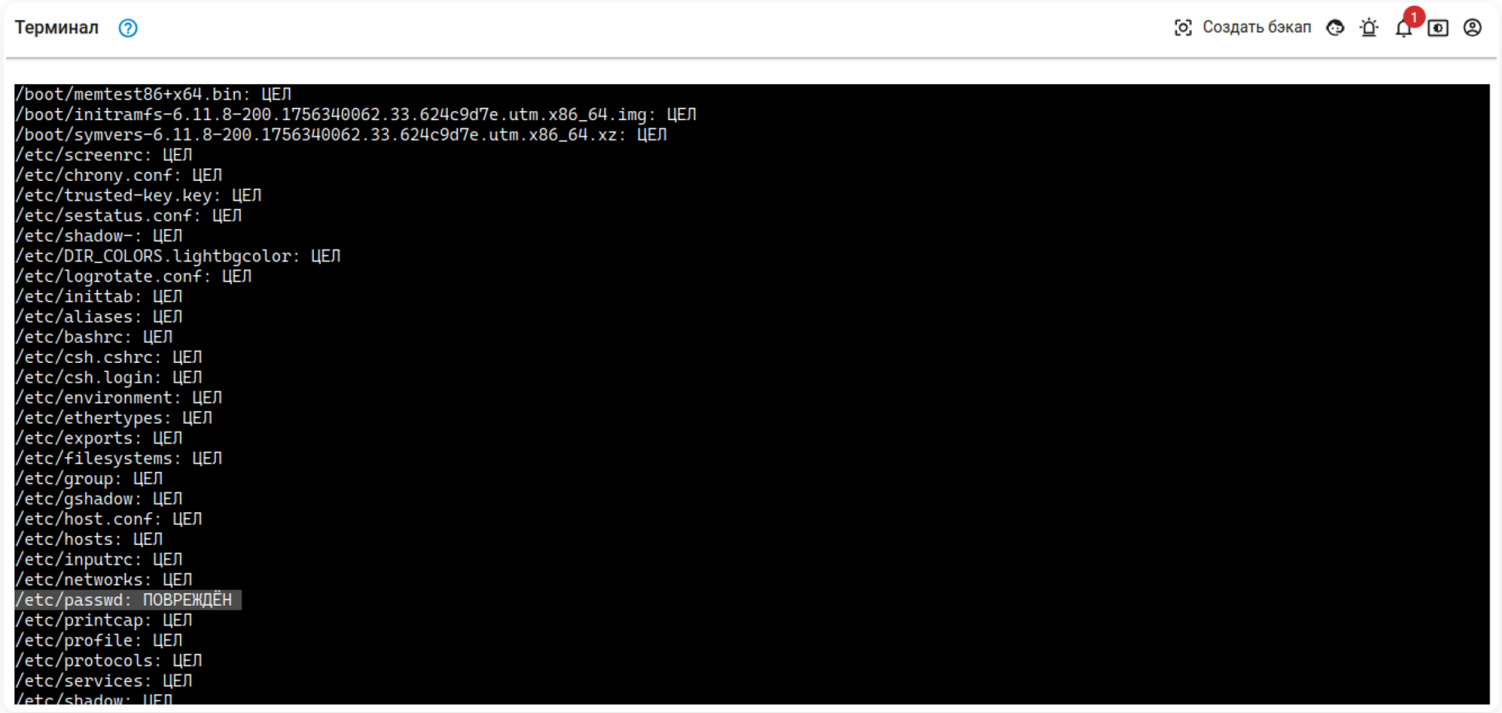
Проверка реакции на изменение системного файла

1. Перейдите в **Управление сервером** → **Терминал**.

2. Добавьте пробел в конец файла `/etc/passwd`:

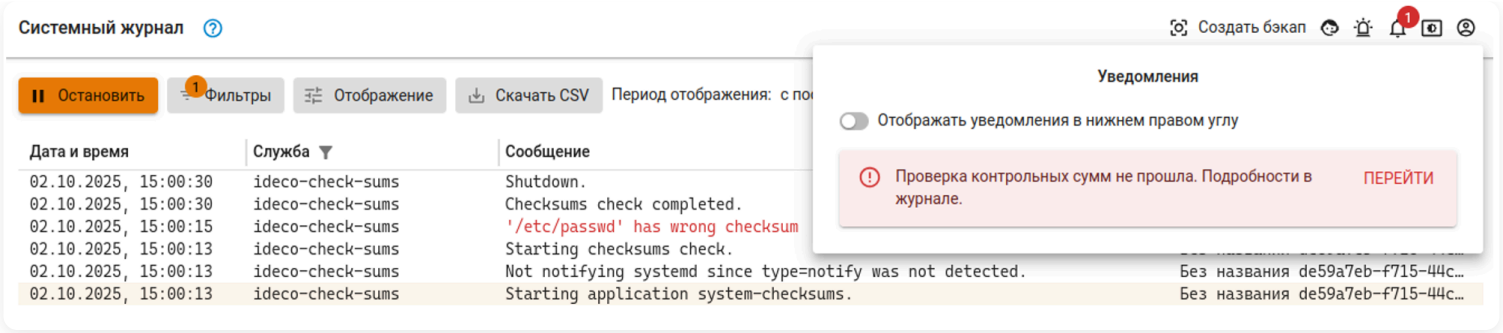


3. Выполните команду `md5sum -c /MD5SUMS`. Убедитесь, что выводится сообщение о нарушении контрольной суммы файла `/etc/passwd`:



4. Перезагрузите Ideco NGFW.

5. После перезагрузки выполните авторизацию в веб-интерфейсе сервера управления Ideco NGFW (`https://192.168.100.2:8443`), используя учетную запись, обладающей ролью **Администратор**. Убедитесь, что по итогу проверки контрольных сумм появляется уведомление **Проверка контрольных сумм завершена с ошибкой**:



6. Завершите сеанс работы с рабочей станцией АРМ.

Критерии успешного выполнения проверки

Результаты выполнения каждого из шагов проверки совпадают с ожидаемыми результатами. Ideco NGFW обеспечивает:

- Выполнение самотестирования при запуске системы.
- Возможность уполномоченным пользователям верифицировать целостность данных.
- Возможность уполномоченным пользователям верифицировать целостность хранимого выполняемого кода функций безопасности.

При необходимости обратитесь в техническую поддержку.

Ideco NGFW 19.X

Примечания к релизу Ideco NGFW 19.0 сборка 634

Дата выхода версии: 12.03.2025.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в телеграмм-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Telegram: ideco.bot

Скачать Ideco NGFW 19.

Автоматическая регистрация тестовой лицензии: my.ideco.ru (полная функциональность на 44 дней и 10 000 пользователей).

Обновление с релизов Ideco UTM 8.12 и старше:

Обновление с релиза Ideco UTM 13 возможно через автоматические обновления (тестовый канал, будет доступна в ближайшее время).

Обновление с релизов 8.x, 9.x, 10.x, 11.x, 12.x возможно через автоматические обновления с промежуточным обновлением до версий 9.11, 10.7, 11.10, 12.8.

После обновлении на Ideco UTM 15 приостанавливается синхронизация с Active Directory, если локальные пользователи Ideco UTM находятся в группах Active Directory.

Обновление с версии Ideco UTM 7.9.9:

Прямое обновление до версии 19 невозможно.

Возможна миграция настроек (загрузка бэкапа настроек) на предварительно установленную версию 9.11 и дальнейшее обновление до версии 18.0 с помощью автоматического обновления.

IDECO NGFW 19.16 сборка 23 (30.01.2026)

Безопасность

- Обновлен модуль системы предотвращения вторжений.

Исправления и изменения

- Повышена стабильность IPsec-подключений.
- Исправлена ошибка при загрузке баз офлайн-обновлений.
- Появилась возможность добавлять правила SNAT для IPsec через веб-интерфейс.
- Доступен раздел **Техническая поддержка** для пользователей с ролью **Администратор Межсетевого экрана**.
- Исправлена проблема доступа в интернет при переопределении действия Flowbit-сигнатуры.
- Косметические изменения веб-интерфейса.

IDECO NGFW 19.13 сборка 22 (23.10.2025)

Безопасность

- Обновлен модуль системы предотвращения вторжений (в том числе исправлена уязвимость CVE-2025-59147/BDU:2025-12460).

Исправления и изменения

- Исправлена работа обратного прокси при добавлении ресурса в ЛК/Портал SSL VPN (только для Ideco NGFW).
- Исправлена валидация ввода IP-адресов и масок.
- Исправлена работа фильтров при поиске по тексту.
- Исправлено некорректное отображение скорости в мониторе трафика.

IDECO NGFW 19.11 сборка 29 (04.09.2025)

Исправления и изменения

- Исправлена работа монитора трафика при большой нагрузке.
- Исправлено излишнее логирование при использовании фильтрации по серым спискам в почтовом релее.
- Улучшено определение приложений модулем Контроль приложений.
- Исправлены проблемы с разрешением имен DNS-сервером в некоторых случаях.
- Исправлены большие задержки трафика в ГОСТ VPN.
- Исправлено создание маршрута для IPsec (доступна настройка адреса источника).
- Обновлен модуль веб-антивируса Касперского.
- Исправлены проблемы при авторизации большого количества пользователей из Active Directory.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.9 сборка 35 (25.07.2025)

Примечания к релизу

Обновление обязательно для использующих модуль антивируса Касперского для веб-трафика из-за обновления общего ключа модуля. Рекомендуем обновиться до 29.07.2025.

Безопасность

- Обновлен модуль системы Предотвращения вторжений (включая исправления CVE-2025-53537, CVE-2025-53538);
- Исправлены потенциальные уязвимости, найденные с помощью статанализа в различных модулях (67 патчей).

Исправления и изменения

- Обновлен ключ антивируса Касперского для проверки веб-трафика (в "старых" версиях будет работать до 29.07.2025);
- Обновлена информация с контактами технической поддержки;
- Исправлена работа с зонами в правилах Файрвола при изменении в интерфейсах;
- Оптимизировано использование ресурсов сервера при использовании WAF при публикации веб-ресурсов;
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.8 сборка 18 (04.07.2025)

Безопасность

- Исправлены потенциальные уязвимости, найденные с помощью фаззинга и статанализа в различных модулях (72 патча).

Исправления и изменения

- Исправлен доступ на сайт rosreestr.gov.ru при включенной расшифровке трафика.
- Повышена стабильность работы Ideco Client.
- Исправлено создание GRE-интерфейса на PPPoE-интерфейсе.
- Исправлена работа чата с технической поддержкой при включенной расшифровке HTTPS-трафика.
- Ускорена работа поиска пользователей при создании правил с большим количеством пользователей.
- Ускорена работа журнала веб-трафика при скроллинге и фильтрации.
- Повышена стабильность модуля авторизации пользователей.
- Исправлена загрузка на серверах Aquarius T40 S33.
- Улучшено логирование правил Файрвола.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.7 сборка 19 (19.06.2025)

Безопасность

- Обновлен модуль веб-почты (исправлена уязвимость CVE-2025-49113).
- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модуле Zabbix.

Исправления и изменения

- Новый виджет онлайн-чата технической поддержки.
- Исправлен доступ к публикации личного кабинета с использованием групп безопасности Active Directory при изменении пользователей в группах.
- Улучшен механизм синхронизации изменений пользователей в группах безопасности Active Directory при использовании групп безопасности в правилах доступа по VPN.
- Исправлено мгновенное восстановление из бэкапов в некоторых ситуациях.
- Исправлена ошибка веб-интерфейса при выключении удаленного помощника.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.6 сборка 66 (04.06.2025)

Безопасность

- Исправлена возможность скачивания бэкапа администратором с ролью "только просмотр".
- Добавлен разрыв установленных SSH-сессий при отключении доступа по SSH или "удаленного помощника".

Исправления и изменения

- Повышена производительность модулей обработки трафика.
- Исправлена работа модуля контроля приложений под нагрузкой.
- Исправлена выгрузка отчетов журнала трафика в CSV при включенных фильтрах.
- Исправлена работа OSPF при переключении провайдеров.
- Добавлена возможность использования "белых" IP-адресов в сети для VPN-подключений.
- Исправлена работа кластера при наличии loopback-интерфейса.
- Исправлена передача цепочки SSL-сертификатов при подключении по SSTP.
- Исправлено действие профиля, применяемое к новым протоколам Контроля приложений при обновлении с 18-ой версии (будет выбрано то же действие, что было назначено протоколу "Unknown").
- Исправлено формирование отчета "Список посещенных адресов" в конструкторе отчетов.
- Исправлена авторизация пользователей доверенных доменов Active Directory.
- Улучшена работа с большим количеством (десятки тысяч) групп безопасности Active Directory.
- Исправлены ошибки в логах после авторизации администратора через RADIUS.
- Исправлено формирование больших отчетов по трафику в CSV.
- Из системного журнала убраны логи контроля приложений (в 19-ой версии они есть в Журнале трафика).
- Ускорено обновление кластера.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.5 сборка 19 (24.04.2025)

Безопасность

- Исправлена уязвимость CVE-2024-11236 (актуальна при использовании веб-почты в NGFW).
- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модулях BGP и DNS-сервере.
- Исправлено отображение учетных данных администратора в тексте ошибки при окончании сессии администратора VCE.

Исправления и изменения

- Исправлено обновление с прошлых версий при наличии активных VCE.
- Исправлено обновление с прошлых версий при особенностях UEFI на сервере.
- Исправлено отображение диапазонов портов в правилах Файрвола.
- Исправлено скачивание баз Контент-фильтра при выключенном модуле контентной фильтрации.
- Добавлена возможность, позволяющая интегрировать Ideco NGFW в домен Microsoft Windows 2025 (при возникновении ошибки входа в домен необходимо выполнить в терминале NGFW команду `touch /run/ideco-ad-backend/ldap-passwd`).
- Повышена надежность БД отчетности.
- Исправлена обработка событий изменения наличия пользователя в группах безопасности AD/ALD для сессий личного кабинета (теперь при удалении пользователя из группы для которой предоставлен доступ сессия будет автоматически разрываться).
- Исправлено создание кластера при наличии loopback-интерфейсов.

- Небольшие исправления веб-интерфейса и логирования служб.

IDECO NGFW 19.3 сборка 19 (8.04.2025)

Безопасность

- Исправлено потенциальное раскрытие информации в логах при использовании VCE.
- Обновлен модуль системы Предотвращения вторжений (исправлены уязвимости CVE-2025-29915, CVE-2025-29917, CVE-2025-29918, CVE-2025-29916).
- Обновлен модуль OpenSSH (исправлена уязвимость CVE-2025-26466).

Исправления и изменения

- Исправлено сообщение при блокировке по словарю морфологического анализа.
- Исправлены проблемы аутентификации пользователей ALD/Samba по VPN.
- Исправлена ошибочная блокировка доп. запросов сайта при правиле, блокирующем все запросы в Контент-фильтре.
- Добавлен порт 8090 для прямых подключений к прокси-серверу.
- Повышена производительность Файрвола.
- Исправлено накопление временных файлов обновлений Контент-фильтра (при появлении нового обновления во время скачивания "старого").
- Исправлена 2FA для пользователей из RADIUS.
- Исправлена работа правила DNAT с использованием зоны источника.
- Исправлены падения службы Контроля приложений при некоторых условиях.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.0 сборка 634 (12.03.2025)

Новая функциональность

- Структурированный Журнал трафика: Файрвол (включая DNAT и SNAT), IPS, Контроль приложений.
- Netflow-сенсор для передачи информации netflow-коллектору.
- Портал SSL VPN (публикация HTTPS-, HTTP-, SSH-, RDP-ресурсов).
- Отправка журналов на Ideco Center.
- ГОСТ VPN для site-to-site между Ideco NGFW.
- Аппаратная фильтрация трафика по MAC-адресам (для поддерживаемых сетевых карт).
- Обработка трафика Файрволом на основе ACL (настраивается по API): до 100 000 записей суммарно во всех ACL, максимальное количество записей в одном ACL - 10 000.

Ideco Client

- 2FA в интерфейсе Ideco Client.
- Балансировка подключений к серверам.
- Подключение к доступным серверам перебором SRV-записей в DNS.
- Кастомная настройка конфигурации: запрет “сохранения пароля”, предустановленные профили, настройка профиля по-умолчанию.
- Улучшенное журналирование подключения в Системный журнал.

Сеть

- Возможность использования пула IP-адресов для SNAT.
- Loopback-интерфейс для GRE-, GRE/IPsec-туннелей.
- Возможность фильтрации трафика между локальными интерфейсами с помощью профилей Контроля приложений и Предотвращения вторжений.

Оптимизации

- Ускорена работа с большим количеством объектов Active Directory.
- Ускорена работа веб-интерфейса с большим количеством пользователей и правил.
- Уменьшено потребление ОЗУ модулями.
- Добавлена поддержка ESN в IPSec (лучше производительность при больших объемах трафика).
- Ускорена установка.

Обновления

- Обновлено ядро Linux (до версии 6.11) и ключевые используемые пакеты.
- Обновлен модуль Контроля приложений.
- Обновлен модуль Предотвращения вторжений.

Разное

- Убран модуль Квоты для работы с квотами трафика.
- Добавлено поле Комментарий в разделе Мониторинг аренды DHCP-сервера.
- Возможность добавления системных доверенных сертификатов.
- В логах авторизации пользователей теперь указывается и логин.
- Добавлена кнопка Сбросить блокировки по IP в разделе **Управление сервером → Дополнительно**.
- Добавлена колонка Расположение в Мониторинг сессий администраторов (по GeoIP).
- Возможность публикации веб-интерфейса как внутреннего сервиса через Обратный прокси-сервер.
- Возможность указания конкретного контроллера домена Active Directory для подключения NGFW.
- Добавлена возможность восстановления на предыдущую версию из раздела Обновления.
- Возможность аутентификации пользователей из Active Directory по RADIUS.
- В антиспаме Касперского включена проверка SPF и DMARC для лучшей фильтрации спама и фишинговых писем.
- При включении заблокированного пользователя в Active Directory он разблокируется в Ideco NGFW (ранее нужно было разблокировать вручную). Отключена возможность ручной блокировки авторизации пользователей Active Directory в Ideco NGFW.
- Добавлена возможность выключения Теста скорости для Личного кабинета пользователей.
- Многочисленные исправления и улучшения веб-интерфейса.

ФСТЭК Ideco UTM 19.X

Описание сертифицированной версии

Примечания к релизу ФСТЭК Ideco UTM 19.1 сборка 51

Дата выхода версии: 28.03.2025.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в телеграм-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Telegram: ideco.bot

Для ФСТЭК-версии включено автоматическое обновление с версии 11.13 путем нескольких обновлений: 11.13 → 12.11 → 13.11 → 14.3 → 15.7 → 16.9 → 17.7 → 18.7 → 19.1.

Обязательно нужно последовательно обновиться и использовать версию 19.1 (не останавливаясь на промежуточных версиях, нужных только для обновления).

С 19 версии профили Контроля приложений и Предотвращения вторжений проверяют и локальный сетевой трафик между сегментами (могут его блокировать в зависимости от настроек правил Файрвола). Проверьте настройки фильтрации трафика после обновления. В версии содержатся важные исправления безопасности компонентов.

ФСТЭК Ideco UTM 19.16 сборка 22 (30.01.2026)

Безопасность

- Обновлен модуль системы предотвращения вторжений.

Исправления и изменения

- Повышена стабильность IPsec-подключений.
- Исправлена ошибка при загрузке баз офлайн-обновлений.
- Появилась возможность добавлять правила SNAT для IPsec через веб-интерфейс.
- Доступен раздел **Техническая поддержка** для пользователей с ролью **Администратор Межсетевого экрана**.
- Исправлена проблема доступа в интернет при переопределении действия Flowbit-сигнатуры.
- Косметические изменения веб-интерфейса.

ФСТЭК Ideco UTM 19.14 сборка 45 (11.12.2025)

Безопасность

- Обновлен модуль системы предотвращения вторжений (в том числе исправлены уязвимости CVE-2025-64344, CVE-2025-64333, CVE-2025-64332, CVE-2025-64331, CVE-2025-64330).
- Исправлена уязвимость CVE-2025-62168/BDU:2025-13226 в модуле прокси-сервера.
- Исправлено некорректное логирование правил Межсетевого экрана с действием **Запретить** при отключенном SSH на внешних интерфейсах.

Исправления и изменения

- Восстановлено переключение нод при отключении внешнего/локального линка на активной ноде при использовании VLAN.
- Исправлена некорректная расшифровка TLS 1.3 при обращении по IP-адресу в **Контент-фильтре**.
- Ограничена роль **Администратор Межсетевого экрана** в некоторых разделах (Почтовый релей, Ограничение скорости, Управление сервером, Обратный прокси и др.).
- Параметр KDC-сервер переименован в DC-сервер.
- Восстановлена работа SIP-телефонии при перезагрузке или обновлении Ideco.

ФСТЭК Ideco UTM 19.13 сборка 23 (23.10.2025)

Безопасность

- Обновлен модуль системы предотвращения вторжений (в том числе исправлена уязвимость CVE-2025-59147/BDU:2025-12460).

Исправления и изменения

- Исправлена работа обратного прокси при добавлении ресурса в ЛК/Портал SSL VPN (только для Ideco NGFW).
- Исправлена валидация ввода IP-адресов и масок.
- Исправлена работа фильтров при поиске по тексту.
- Исправлено некорректное отображение скорости в мониторе трафика.

ФСТЭК Ideco UTM 19.12 сборка 4 (10.09.2025)

Исправления и изменения

- Исправлена работа монитора трафика при большой нагрузке.
- Исправлено излишнее логирование при использовании фильтрации по серым спискам в почтовом релее.
- Улучшено определение приложений модулем Контроль приложений.
- Исправлены проблемы с разрешением имен DNS-сервером в некоторых случаях.
- Исправлено создание маршрута для IPsec (доступна настройка адреса источника).
- Исправлены проблемы при авторизации большого количества пользователей из Active Directory.
- Косметические исправления веб-интерфейса.

ФСТЭК Ideco UTM 19.10 сборка 2 (28.07.2025)

Безопасность

- Обновлен модуль системы Предотвращения вторжений (включая исправления CVE-2025-53537, CVE-2025-53538);
- Исправлены потенциальные уязвимости, найденные с помощью статанализа в различных модулях (67 патчей).

Исправления и изменения

- Обновлена информация с контактами технической поддержки;
- Исправлена работа с зонами в правилах файрвола при изменении в интерфейсах;
- Косметические исправления веб-интерфейса.

ФСТЭК Ideco UTM 19.8 сборка 19 (04.07.2025)

Безопасность

- Исправлены потенциальные уязвимости, найденные с помощью фаззинга и статанализа в различных модулях (72 патча).

Исправления и изменения

- Исправлен доступ на сайт rosreestr.gov.ru при включенной расшифровке трафика.
- Исправлено создание GRE-интерфейса на PPPoE-интерфейсе.
- Исправлена работа чата с технической поддержкой при включенной расшифровке HTTPS-трафика.
- Ускорена работа поиска пользователей при создании правил при большом количестве пользователей.
- Ускорена работа журнала веб-трафика при скроллинге и фильтрации.
- Повышена стабильность модуля авторизации пользователей.
- Исправлена загрузка на серверах Aquarius T40 S33.
- Улучшено логирование правил файрвола.
- Косметические исправления веб-интерфейса.

ФСТЭК Ideco UTM 19.7 сборка 20 (19.06.2025)

Безопасность

- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модуле Zabbix.

Исправления и изменения

- Новый виджет онлайн-чата технической поддержки.
- Исправлен доступ к публикации личного кабинета с использованием групп безопасности Active Directory при изменении пользователей в группах.
- Улучшен механизм синхронизации изменений пользователей в группах безопасности Active Directory при использовании групп безопасности в правилах доступа по VPN.
- Исправлено мгновенное восстановление из бэкапов в некоторых ситуациях.
- Исправлена ошибка веб-интерфейса при выключении удаленного помощника.
- Косметические исправления веб-интерфейса.

ФСТЭК IDECO UTM 19.6 сборка 67 (04.06.2025)

Безопасность

- Исправлена возможность скачивания бэкапа администратором с ролью "только просмотр".
- Добавлен разрыв установленных SSH-сессий при отключении доступа по SSH или "удаленного помощника".

Исправления и изменения

- Повышена производительность модулей обработки трафика.
- Исправлена работа модуля контроля приложений под нагрузкой.
- Исправлена выгрузка отчетов журнала трафика в CSV при включенных фильтрах.
- Исправлена работа OSPF при переключении провайдеров.
- Добавлена возможность использования "белых" IP-адресов в сети для VPN-подключений.
- Исправлена работа кластера при наличии loopback-интерфейса.
- Исправлена передача цепочки SSL-сертификатов при подключении по SSTP.
- Исправлено действие профиля, применяемое к новым протоколам Контроля приложений при обновлении с 18-ой версии (будет выбрано то же действие, что было назначено протоколу "Unknown").
- Исправлено формирование отчета "Список посещенных адресов" в конструкторе отчетов.
- Исправлена авторизация пользователей доверенных доменов Active Directory.
- Улучшена работа с большим количеством (десятки тысяч) групп безопасности Active Directory.
- Исправлены ошибки в логах после авторизации администратора через RADIUS.
- Исправлено формирование больших отчетов по трафику в CSV.
- Из системного журнала убраны логи контроля приложений (в 19-ой версии они есть в Журнале трафика).
- Ускорено обновление кластера.
- Косметические исправления веб-интерфейса.

ФСТЭК IDECO UTM 19.5 сборка 20 (24.04.2025)

Безопасность

- Обновлен модуль системы Предотвращения вторжений (исправлены уязвимости CVE-2025-29915, CVE-2025-29917, CVE-2025-29918, CVE-2025-29916).
- Обновлен модуль OpenSSH (исправлена уязвимость CVE-2025-26466).
- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модулях BGP и DNS-сервере.

Исправления и изменения

- Исправлено сообщение при блокировке по словарю морфологического анализа.
- Исправлены проблемы аутентификации пользователей ALD/Samba по VPN.
- Добавлен порт 8090 для прямых подключений к прокси-серверу.
- Исправлено накопление временных файлов обновлений Контент-фильтра (при появлении нового обновления во время скачивания "старого").
- Исправлена 2FA для пользователей из RADIUS.
- Исправлена работа правила DNAT с использованием зоны источника.
- Исправлены падения службы Контроля приложений при некоторых условиях.
- Исправлено скачивание баз Контент-фильтра при выключенном модуле контентной фильтрации.
- Исправлено создание кластера при наличии loopback-интерфейсов.

- Добавлена возможность, позволяющая интегрировать Ideco UTM в домен Microsoft Windows 2025 (при возникновении ошибки входа в домен необходимо выполнить в терминале NGFW команду `touch /run/ideco-ad-backend/ldap-passwd`).
- Повышена надежность БД отчетности.
- Косметические исправления веб-интерфейса.

ФСТЭК IDECO UTM 19.1 сборка 51 (28.03.2025)

Новая функциональность

- Структурированный Журнал трафика: Файрвол (включая DNAT и SNAT), IPS, Контроль приложений.
- Netflow-сенсор для передачи информации netflow-коллектору.
- Отправка журналов на Ideco Center.
- Аппаратная фильтрация трафика по MAC-адресам (для поддерживаемых сетевых карт).
- Обработка трафика файрволом на основе ACL (настраивается по API): до 100 000 записей суммарно во всех ACL, максимальное количество записей в одном ACL - 10 000.
- Виртуальные контексты VCE.

Сеть

- Возможность использования пула IP-адресов для SNAT.
- Loopback-интерфейс для GRE, GRE/IPsec-туннелей.
- Возможность фильтрации трафика между локальными интерфейсами с помощью профилей Контроля приложений и IPS.

Оптимизации

- Ускорена работа с большим количеством объектов Active Directory.
- Ускорена работа веб-интерфейса с большим количеством пользователей и правил.
- Уменьшено потребление ОЗУ модулями.
- Добавлена поддержка ESN в IPSec (лучше производительность при больших объемах трафика).
- Ускорена установка.
- Ускорена обработка трафика Файрволом.

Обновления

- Обновлено ядро Linux (до версии 6.11) и ключевые используемые пакеты.
- Обновлен модуль Контроля приложений.
- Обновлен модуль Предотвращения вторжений (в т.ч. исправлены все известные уязвимости).

Разное

- Убран модуль Квоты для работы с квотами трафика.
- Добавлено поле Комментарий в разделе Мониторинг аренды DHCP-сервера.
- Возможность добавления системных доверенных сертификатов.
- В логах авторизации пользователей теперь указывается и логин.
- Добавлена кнопка Сбросить блокировки по IP в меню Управление сервером → Дополнительно.
- Добавлена колонка Расположение в Мониторинг сессий администраторов (по GeoIP).
- Возможность публикации веб-интерфейса как внутреннего сервиса через Обратный прокси-сервер.
- Возможность указания конкретного контроллера домена Active Directory для подключения UTM.
- Добавлена возможность восстановления на предыдущую версию из раздела Обновления.
- Возможность аутентификации пользователей из Active Directory по RADIUS.
- При включении заблокированного пользователя в Active Directory он разблокируется в Ideco UTM (ранее нужно было разблокировать вручную). Отключена возможность ручной "блокировки" авторизации пользователей Active Directory в Ideco UTM.
- Многочисленные исправления и улучшения веб-интерфейса.

Новое в документации

Февраль 2026

Популярные инструкции и диагностика проблем

Как избежать проблем с подключением VPN-клиентов при использовании нескольких серверов Ideco NGFW

Настройка корневого и подчиненного центра сертификации с помощью AD CS

Использование собственного CA-сертификата в Контент-фильтре

Январь 2026

Общая информация

Настройка двухфакторной аутентификации с использованием TOTP-токенов

Обратная связь

Популярные инструкции и диагностика проблем

Сброс пароля IPMI на сервере NGFW Novum

Об Ideco NGFW

> Межсетевой экран Ideco NGFW - современное программное решение для защиты сетевого периметра, которое позволяет сделать доступ в интернет абсолютно управляемым, безопасным и надежным.

Возможности Ideco NGFW:

- Межсетевой экран
- Система предотвращения вторжений
- Контент-фильтр
- Контроль приложений
- Антивирусная и антиспам-проверка трафика
- Защита от ботнетов, фишинга и шпионского ПО
- VPN site-to-site (GRE, IPSec, ГОСТ VPN) и client-to-site (IKEv2/IPSec, L2TP/IPSec, SSTP, Wireguard) с 2FA
- Логирование действий администратора
- Управление через Центральную консоль
- 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, которые позволяют создать надежный барьер для защиты локальной сети от современных угроз безопасности.

Техническое описание Ideco NGFW доступно по ссылке.

Online-документация актуальна для версий Ideco UTM начиная с 7.9 и Ideco NGFW с 16.0 (выбрать нужную версию можно в верхней части меню).

Скачать Ideco NGFW можно в личном кабинете.

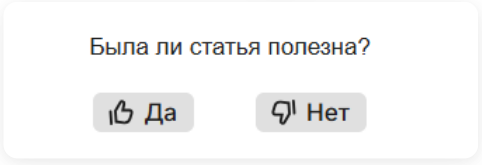
Видеодокументация доступна на YouTube и Rutube.

Обратная связь

Мы постоянно совершенствуем нашу документацию и всегда рады вашим отзывам.

Как оставить отзыв:

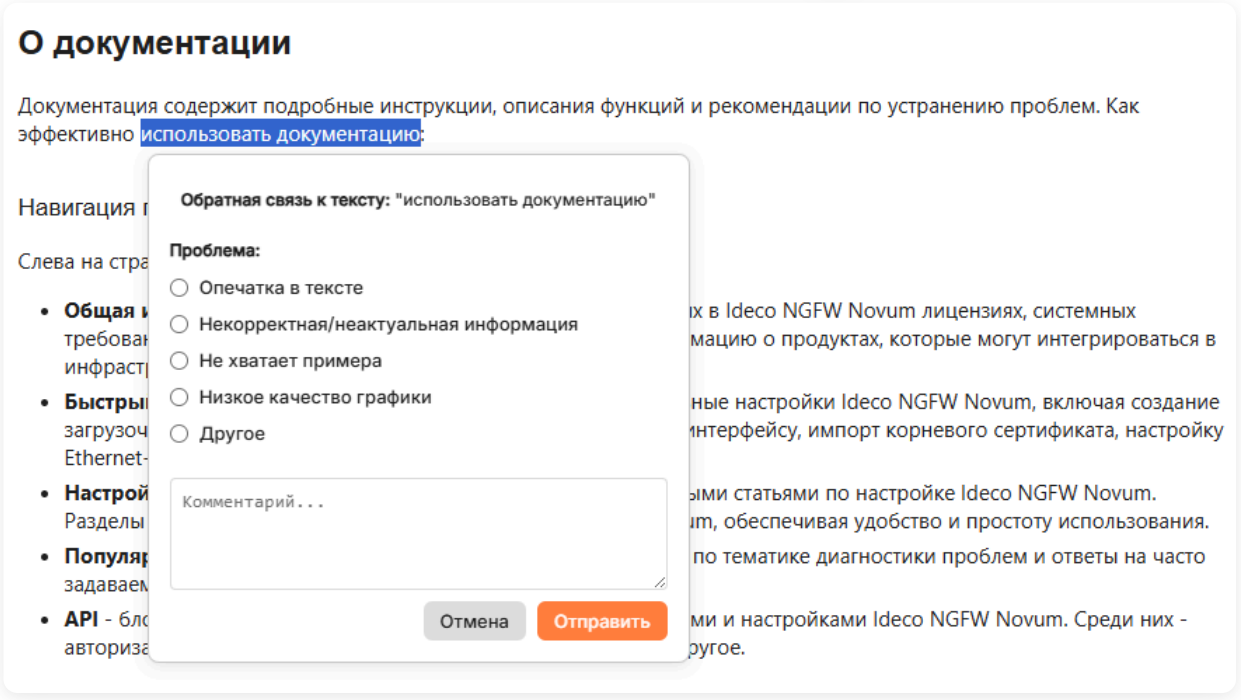
- Поставить реакцию в правом верхнем углу или в конце любой статьи:



- Написать комментарий к фрагменту текста внутри статьи.

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 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 есть три основные характеристики:

- **Количество пользователей Ideco NGFW** - авторизованные пользователи локальной сети или подключенные по VPN пользователи, трафик которых проверяется и контролируется шлюзом.
- **Редакция Ideco NGFW (вид лицензии)** - набор доступных к использованию модулей в системе и особенности их работы.
- **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 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**.

Виды лицензий

В Ideco NGFW доступны лицензии:

Enterprise

Enterprise - коммерческая лицензия.

- ☑ Бессрочное право на использование Ideco NGFW
- ☑ Включает в себя годовую подписку **Security Update**
- ☑ Лицензирование по числу активных пользователей или по количеству ядер виртуальной машины
- ☑ 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.
- 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:

- **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.

> ℹ Для использования кластера Ideco NGFW потребуется дополнительная лицензия на кластеризацию.

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:

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокированы FORWARD- и INPUT-трафик. Кроме доступа до 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 **Свободные лицензии**.

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

- Отключена авторизация пользователей и фильтрация трафика.
- Заблокированы FORWARD- и INPUT-трафик. Кроме доступа до 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.

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:

- В личном кабинете MY.IDECO. 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.

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

Системные требования

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

- 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 четвертого класса защиты используется только ПАК.

Производительность платформы

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

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

- Задействованные компоненты NGFW (**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 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 на аппаратной платформе.

Программно-аппаратный комплекс

Работа Ideco NGFW 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 MX2/LX/LX+ - номер записи 10465633, ссылка.
- Для Ideco NGFW 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).

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	- 16 ГБ (16-64 ГБ в зависимости от количества пользователей).
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 (Compatability Support Module).
Дополнительно	- Монитор и клавиатура (не требуется, если используется IPMI).

На каждый VCE требуется минимум:

- Процессор: 2 ядра.
- Оперативная память: 8 ГБ.

- 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. Встроенные в материнские платы программные и полуаппаратные RAID-контроллеры 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 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 4K 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 (Compatability Support Module).
Дополнительно	- Внутренние часы виртуальной машины должны быть настроены на хранение времени во временной зоне UTC.

На каждый VCE требуется минимум:

- Процессор: 2 ядра.
- Оперативная память: 8 ГБ.
- 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

> Условия и график работы технической поддержки компании "Айдеко", доступной по подписке, а также способы обращения и необходимые данные для помощи.

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 почитать на сайте компании "Айдеко".

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
Интерактивный онлайн-чат со специалистом технической поддержки	https://my.ideco.ru/, https://ideco.ru/, веб-интерфейс Ideco NGFW

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.

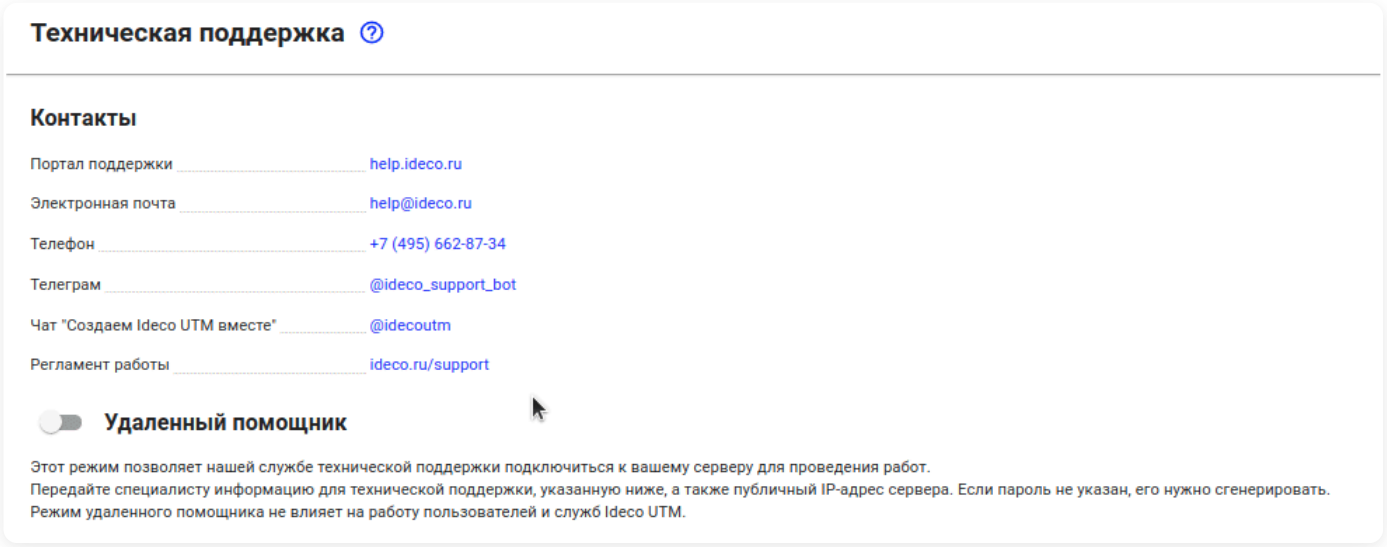
При обращении необходимо предоставить следующую информацию: название организации, ваши контактные данные, номер лицензии.

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 файрвола. При этом становится доступно подключение по SSH из локальных и внешних сетей.



Включение режима удаленного помощника из веб-интерфейса

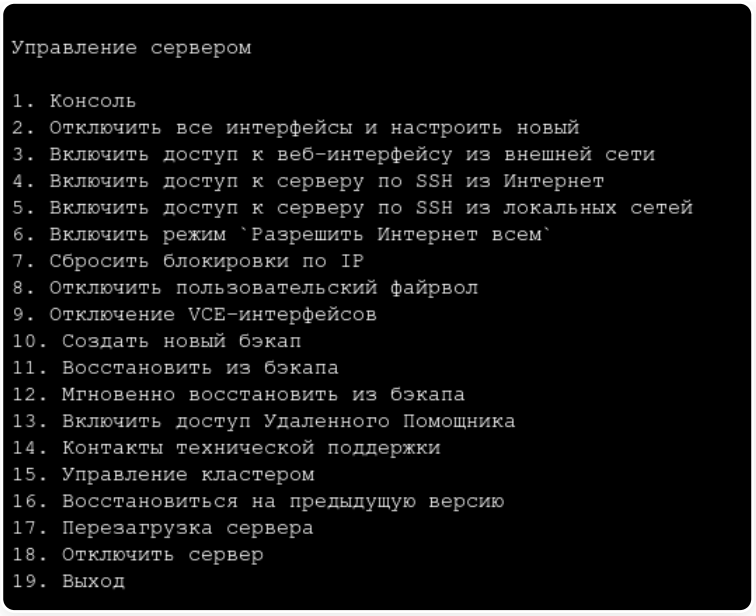
Для подключения специалиста технической поддержки сообщите ему **Информацию для технической поддержки**, нажав кнопку **Скопировать**. Также нужно отдельно передать публичный IP-адрес сервера. Если сервер подключен не напрямую к Ideco NGFW, выполните проброс с внешнего маршрутизатора до 22-го порта на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

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

Включение режима удаленного помощника из локального меню сервера

Чтобы включить режим удаленного помощника, в локальном меню Ideco NGFW выберите пункт **Включить доступ Удаленного помощника**, введя пункт **13**, 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, и скачать ее 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.

Разрешить интернет всем: диагностика неполадок

Используйте режим только для диагностики.

Режим **Разрешить интернет всем** не отключается автоматически и продолжает работать, пока его не отключить вручную.

При включении:

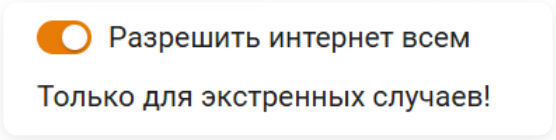
- Сбор веб-статистики будет отключен.
- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включён автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Файрвола** и DNAT.

Цикл обработки трафика в Ideco NGFW описан в статье.

Включить режим можно через:

Веб-интерфейс

Нажмите на иконку технической поддержки в верхней правой части окна и включите **Разрешить интернет всем**:



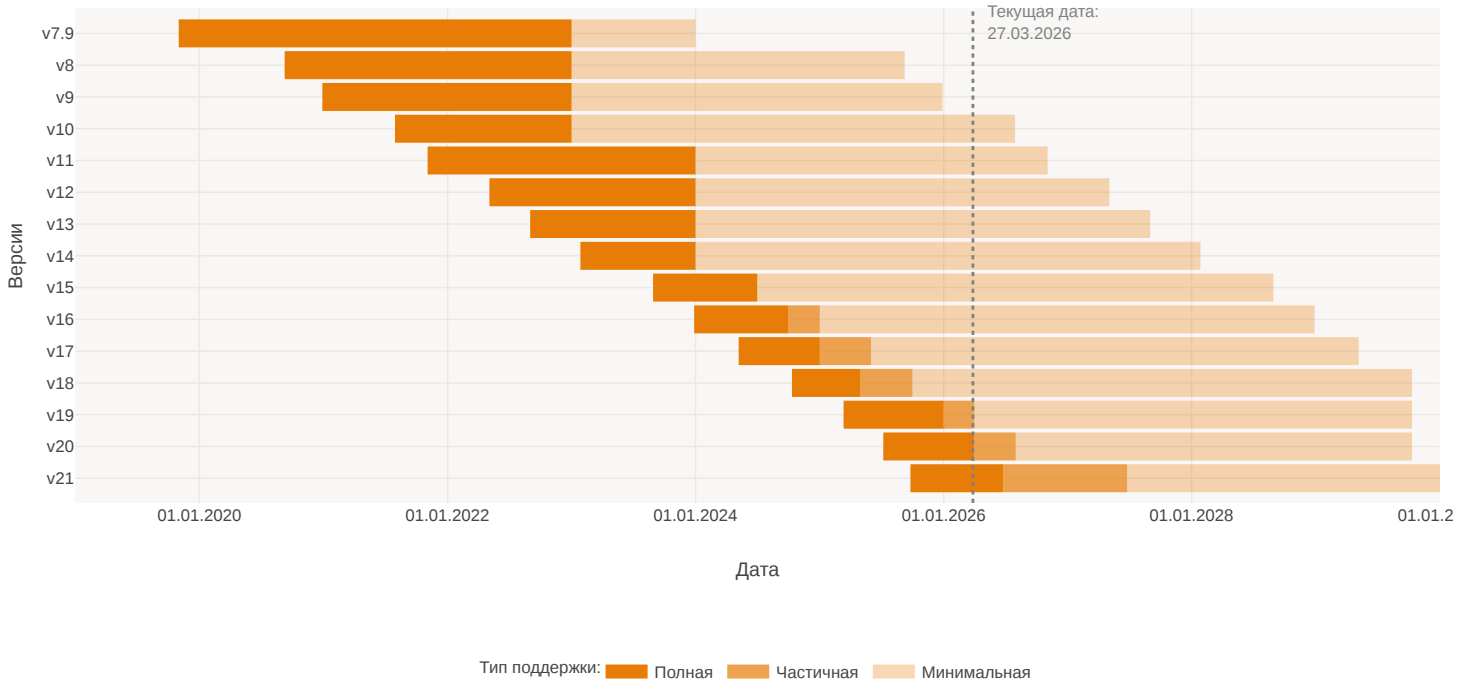
Локальное меню

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

Информация о поддержке версий Ideco NGFW

В статье описываются типы поддержки Ideco NGFW 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

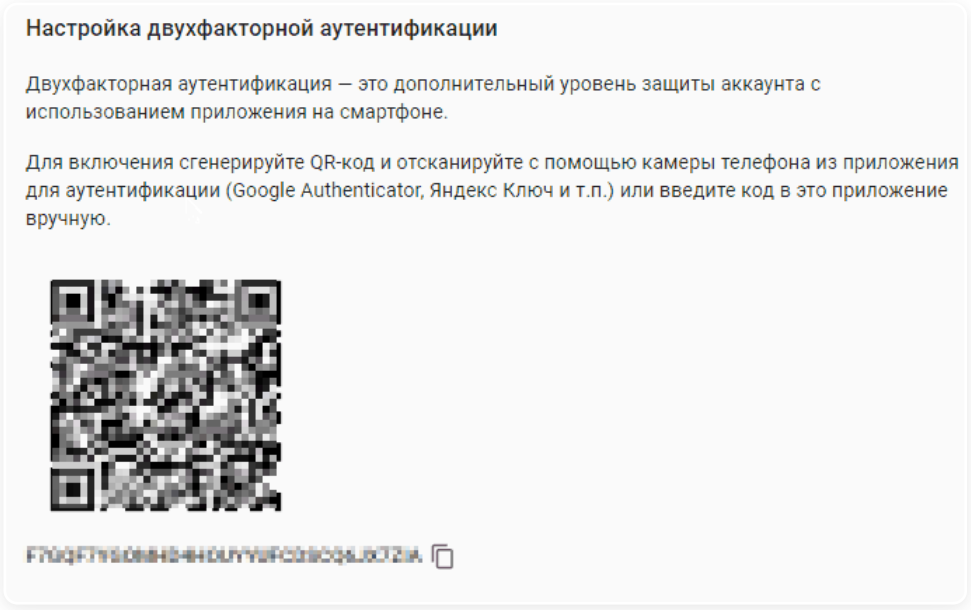
TOTP (Time-based One-Time Password) - это временные одноразовые пароли, которые меняются каждые 30 секунд. Метод аутентификации с использованием TOTP-токенов обеспечивает дополнительный уровень безопасности для ваших аккаунтов.

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. Подробнее - в статье. Система отобразит QR-код и секретный ключ (строка букв и цифр):

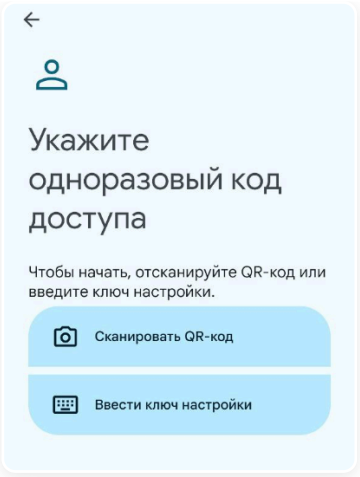


3. Добавьте аккаунт в приложение.

Google Authenticator

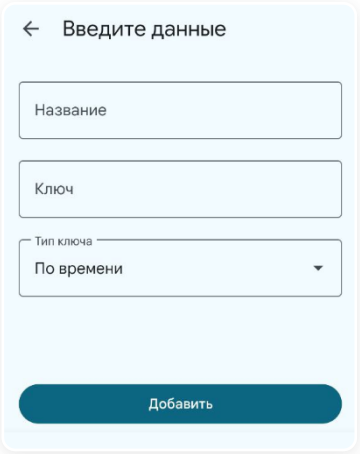
1. Запустите приложение и нажмите **Начать**.

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**.

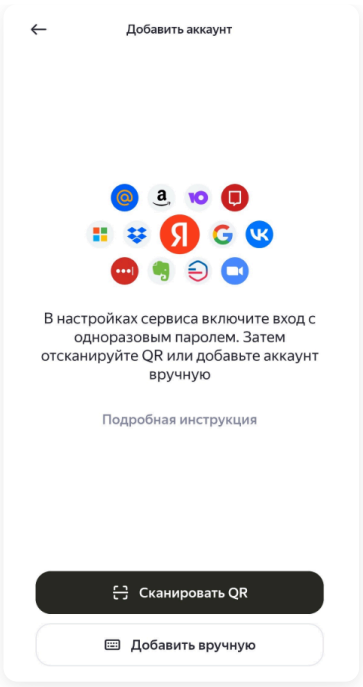
4. Нажмите **Добавить**.

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

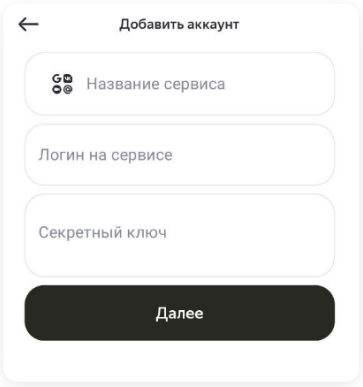
Яндекс ID

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.

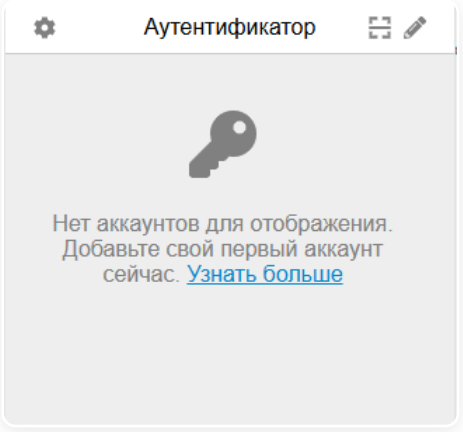
3. Нажмите **Далее**.

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

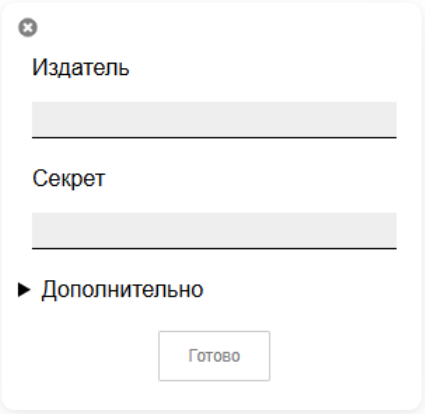
Расширение Аутентификатор

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 таблице представлена информация о продуктах других вендоров, протестированных на совместимость и возможность интеграции с продуктами Ideco.

Продукт	Компания	Класс продукта
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
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
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
Multifactor	ООО "Мультифактор"	Система двухфакторной аутентификации и контроля доступа
SKY DNS	"СкайДНС"	Решение DNS Security и фильтрация контента
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
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
Антивирус Касперского	ЗАО "Лаборатория Касперского"	Антивирус
Контур Staffcop Enterprise	ООО "АТОМ Безопасность"	Система расследования инцидентов внутренней информационной безопасности
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

Источники данных

Ideco NGFW 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.v19.ideco.dev	443 TCP-порт
Отправка анонимной статистики	gatherstat.v19.ideco.dev	443 TCP-порт
Обновления баз GeoIP	ip-list.v19.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.v19.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

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 необходимо, чтобы доступ к вышеуказанным ресурсам был разрешен настройками фильтрации.

Учитывайте при обновлении, что `v19` в домене соответствует версии Ideco NGFW. Эту часть можно заменить символом `*` при настройке фильтрации (пример: `license.*.ideco.dev`).

Рекомендации при первоначальной настройке

Рекомендуемая последовательность шагов для минимальной настройки Ideco NGFW:

1. Зарегистрируйтесь на 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, и выполните предварительные действия. Ideco NGFW можно устанавливать как на виртуальную машину.

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

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

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

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

Подготовка платформы к установке

Установка на гипервизор

Перейти >

Создание загрузочного USB-накопителя

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Настройка гипервизора

Если при установке Ideco NGFW 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

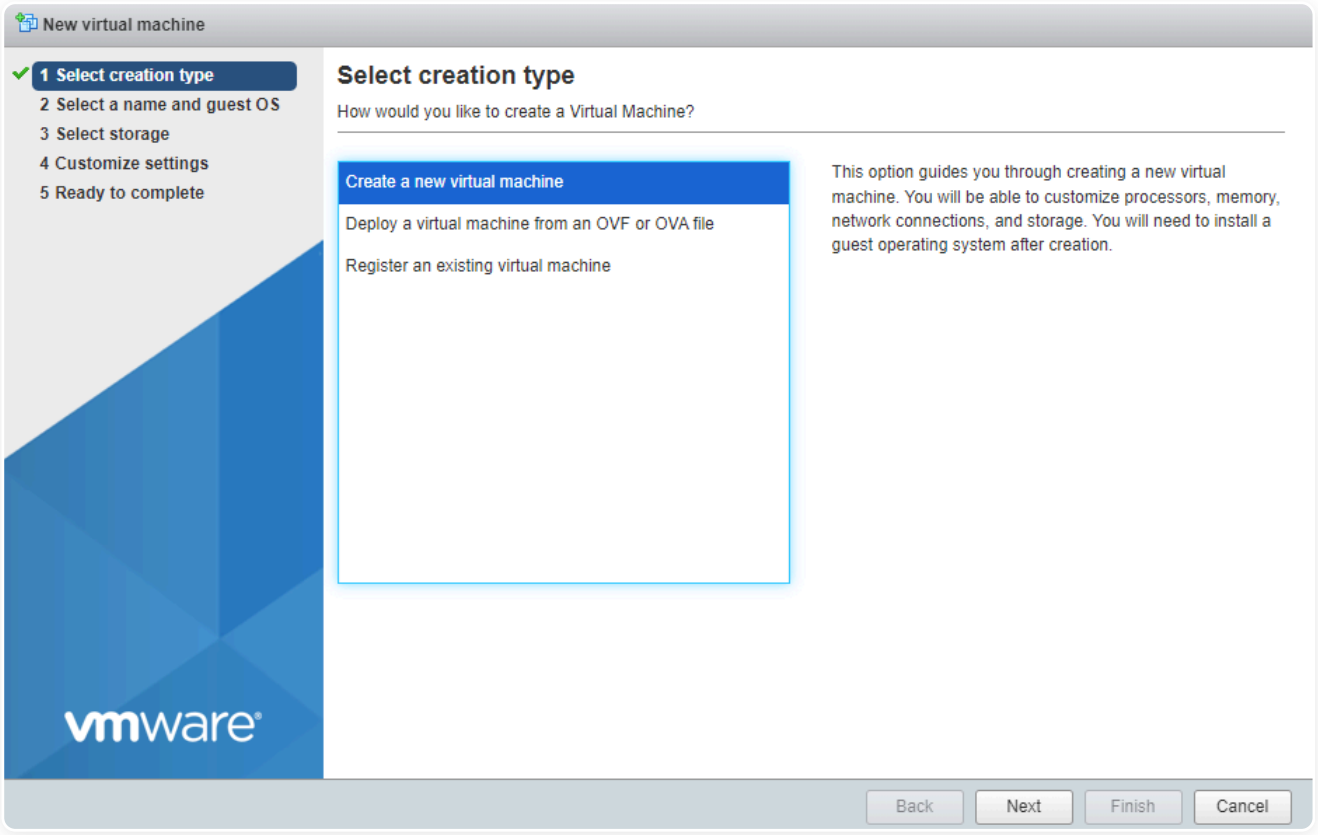
При установке Ideco NGFW на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

Настройка

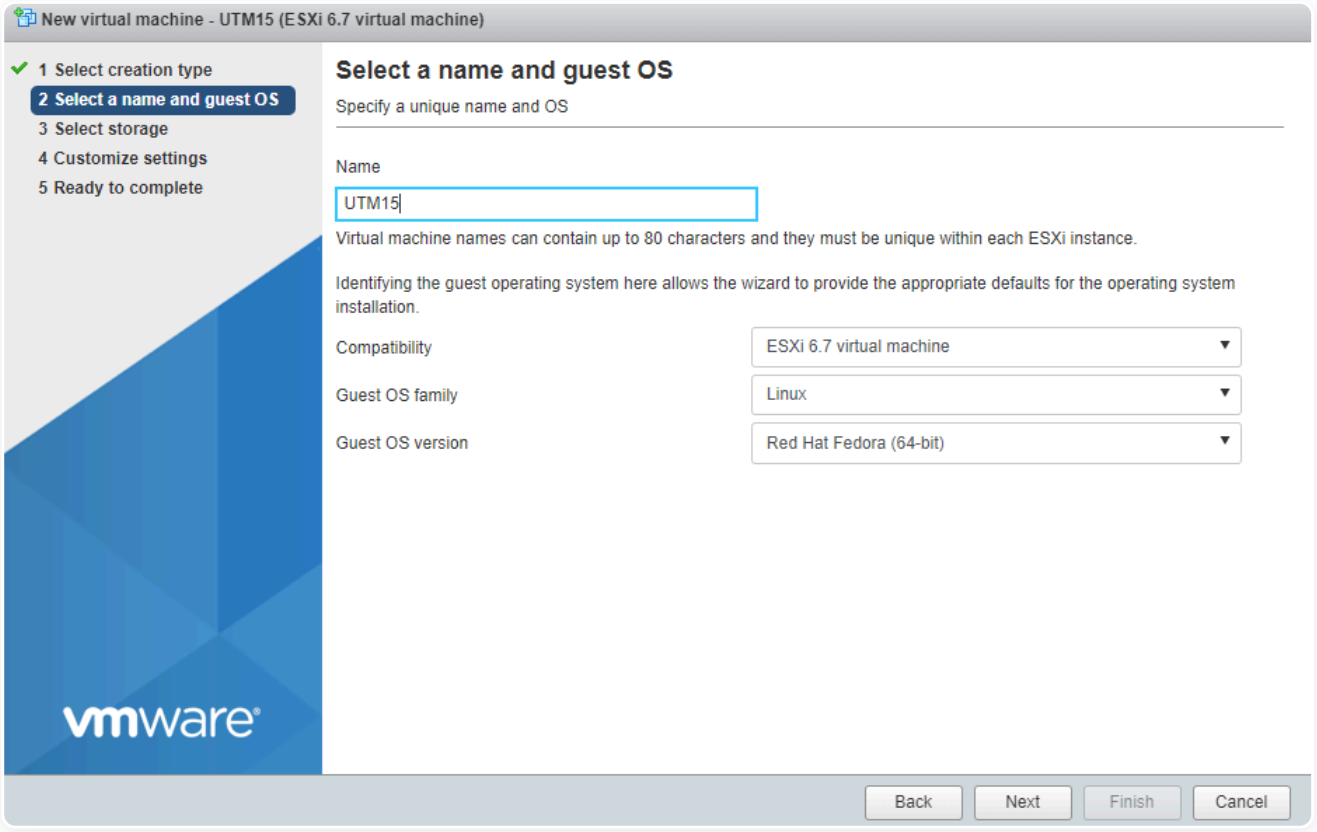
Перед установкой Ideco NGFW:

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

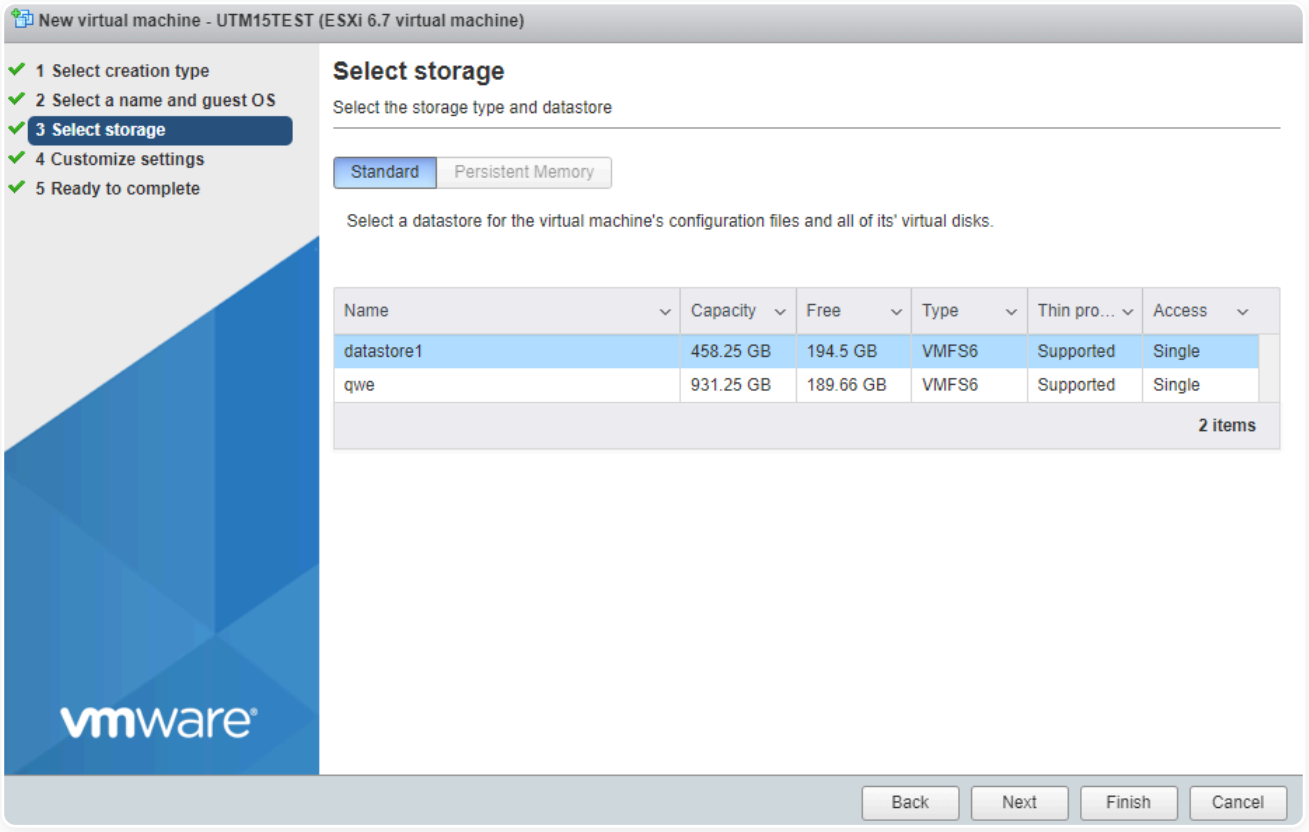
1. Создайте виртуальную машину:



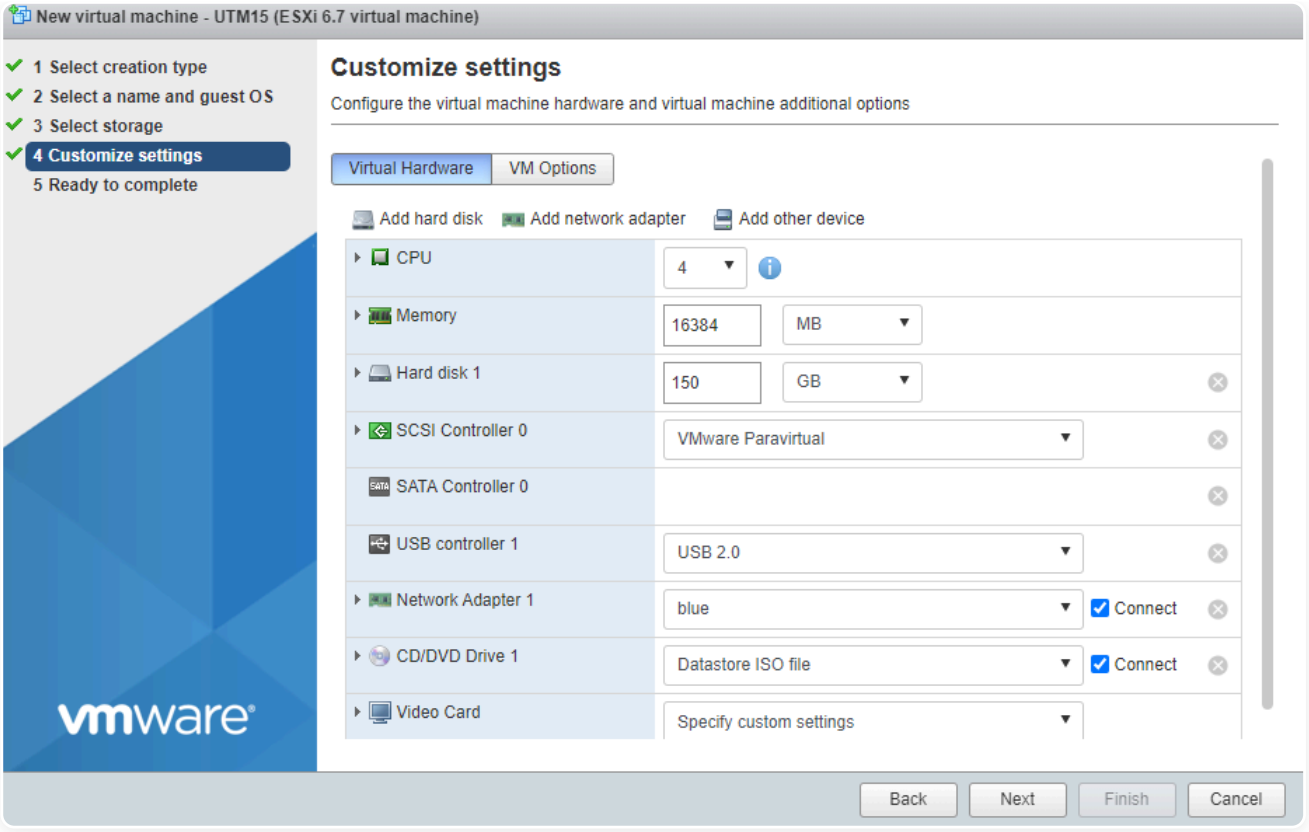
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



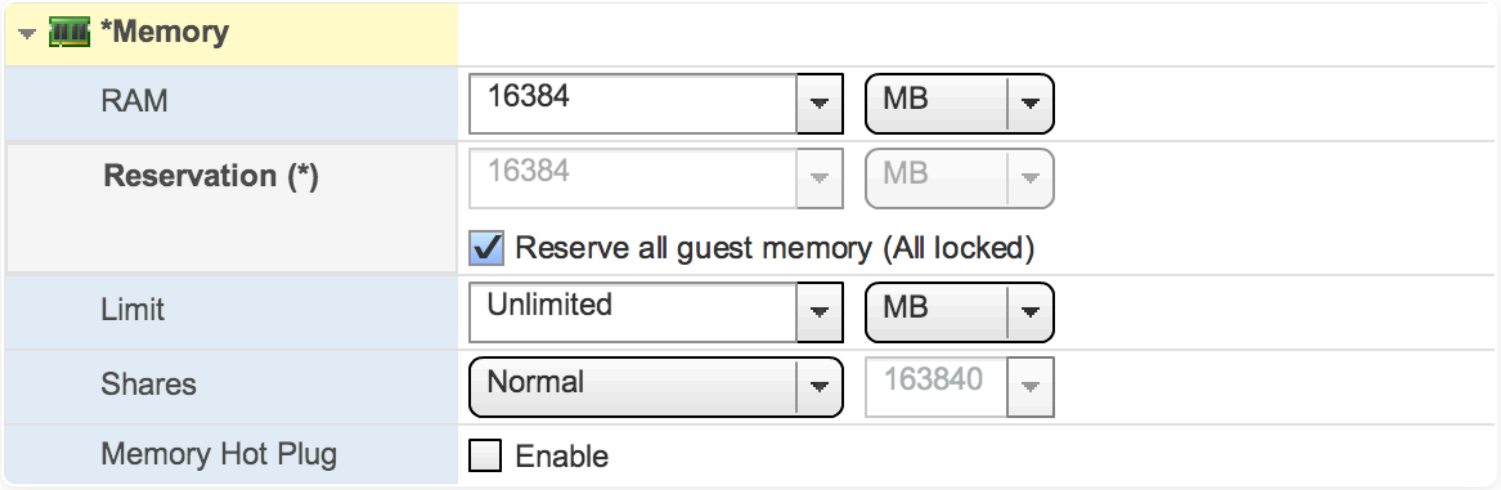
3. Выберите хранилище для виртуальной машины:



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

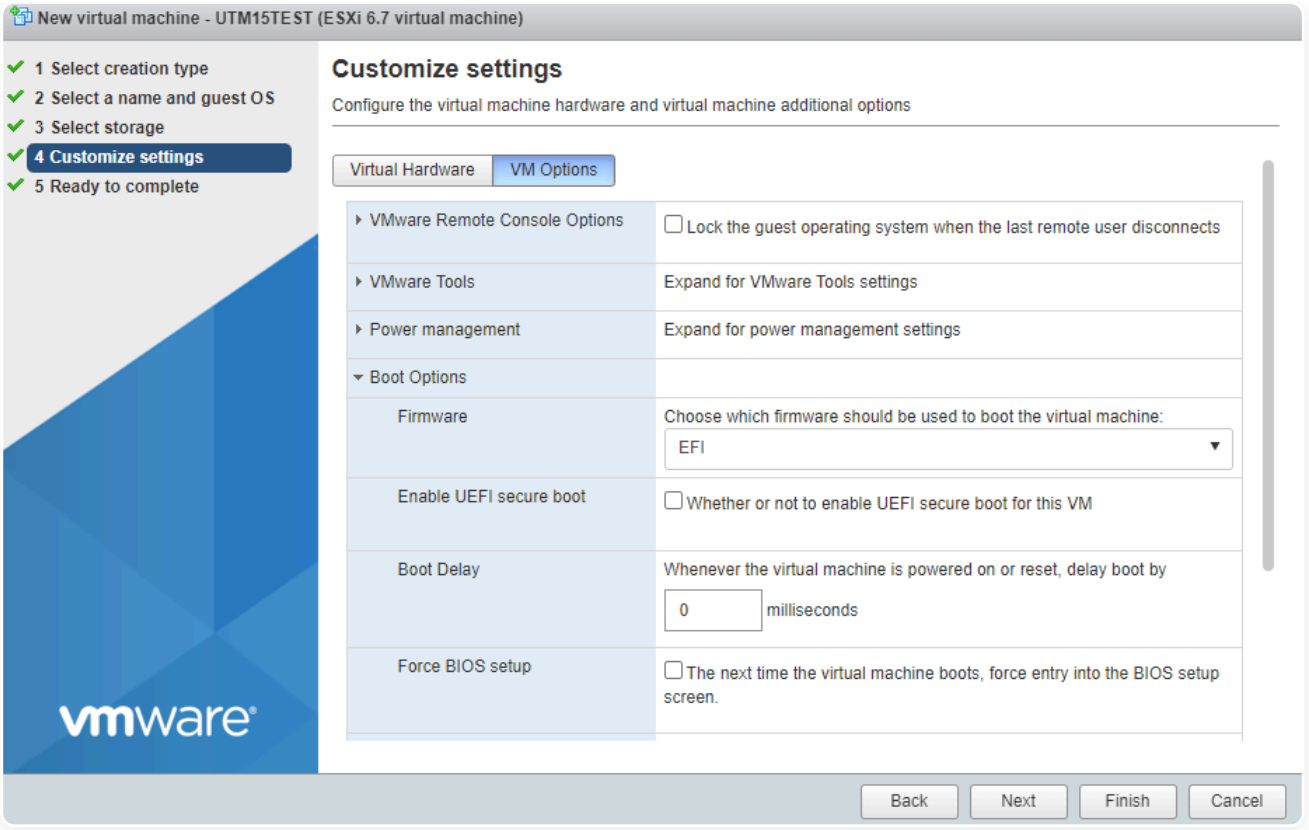


5. Разверните раздел **Memory** и включите опцию **Reserve all guest memory (All locked)**:

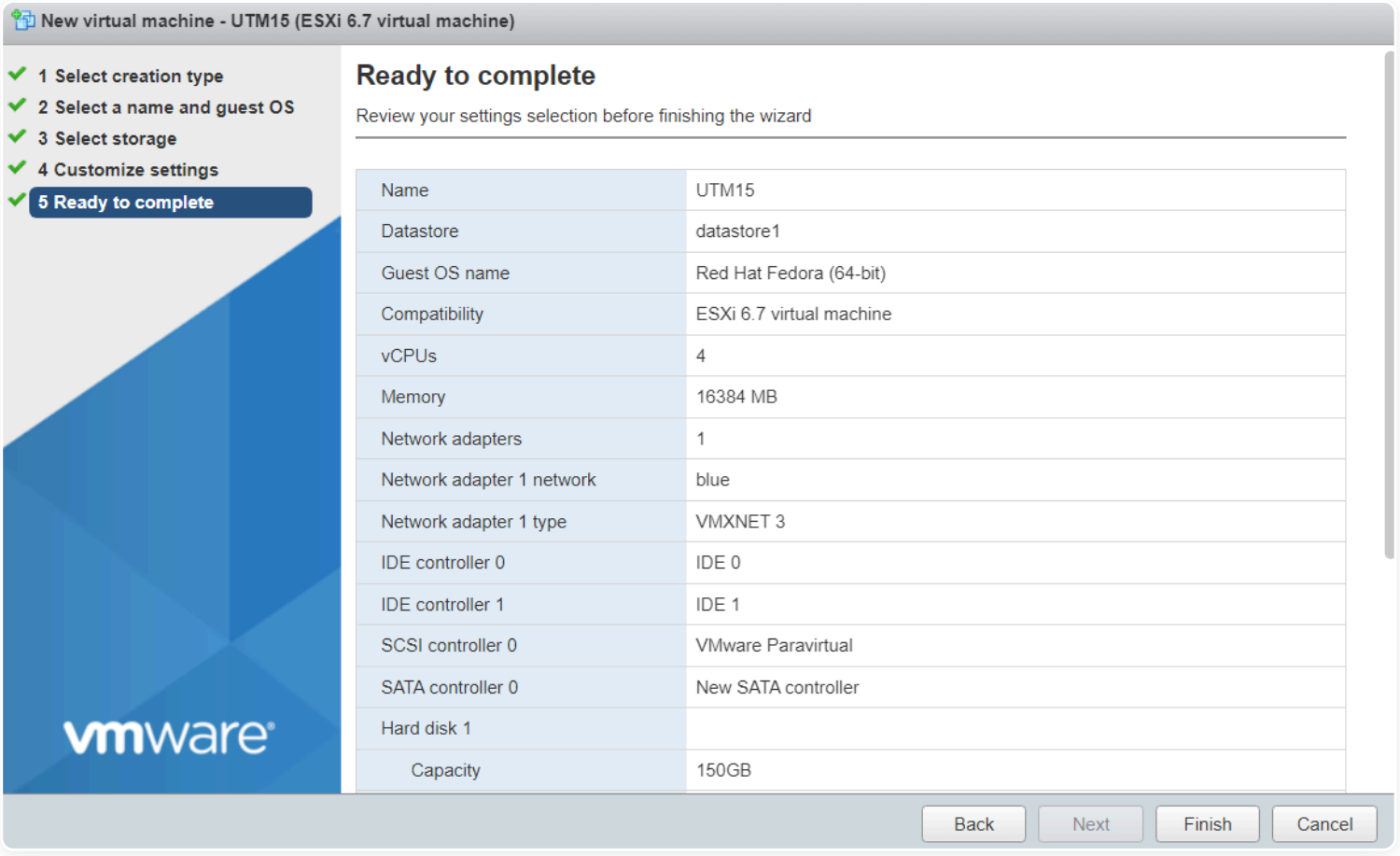


- **Reserve all guest memory (All locked)** - если опция выключена, гипервизор динамически распределяет доступную оперативную память между всеми виртуальными машинами.

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



7. Нажмите **Finish**:



VMware Workstation 17.0

Настройка

Перед установкой Ideco NGFW:

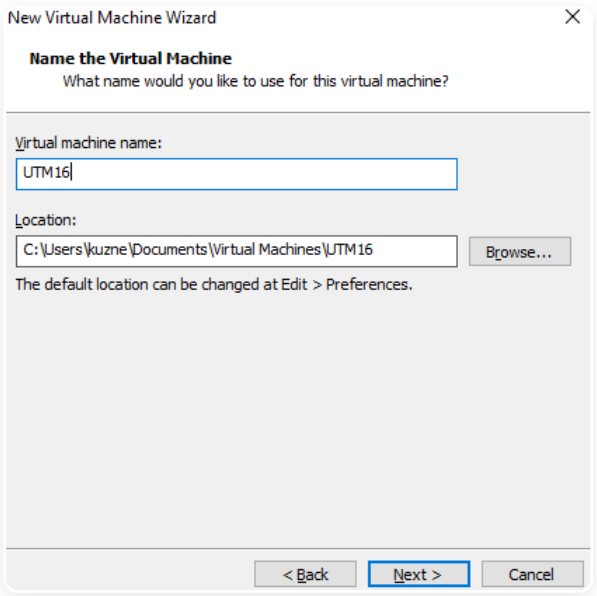
- Увеличьте размер видеопамяти для виртуальной машины до 16 МБ.
- Используйте виртуальные сетевые адаптеры **vmxnet3**.

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

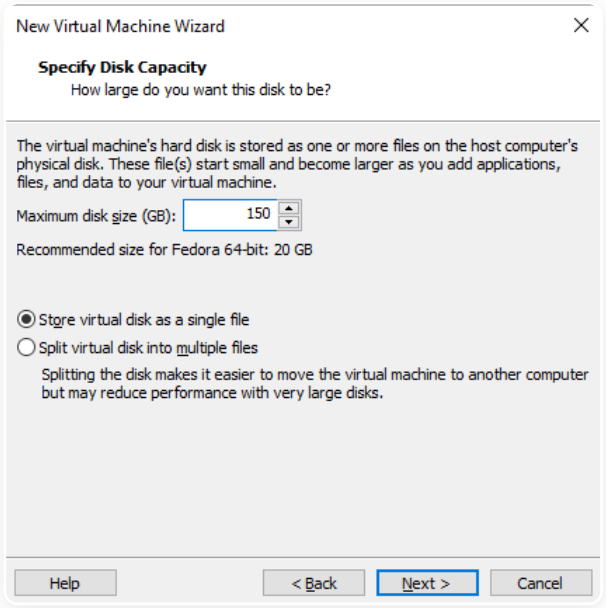
2. Укажите загрузочный ISO-образ:

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

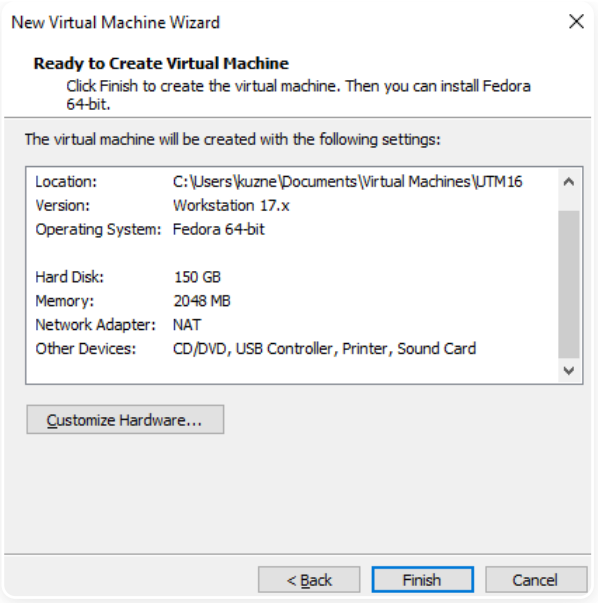
4. Укажите имя виртуальной машины и директорию для создания виртуального диска:



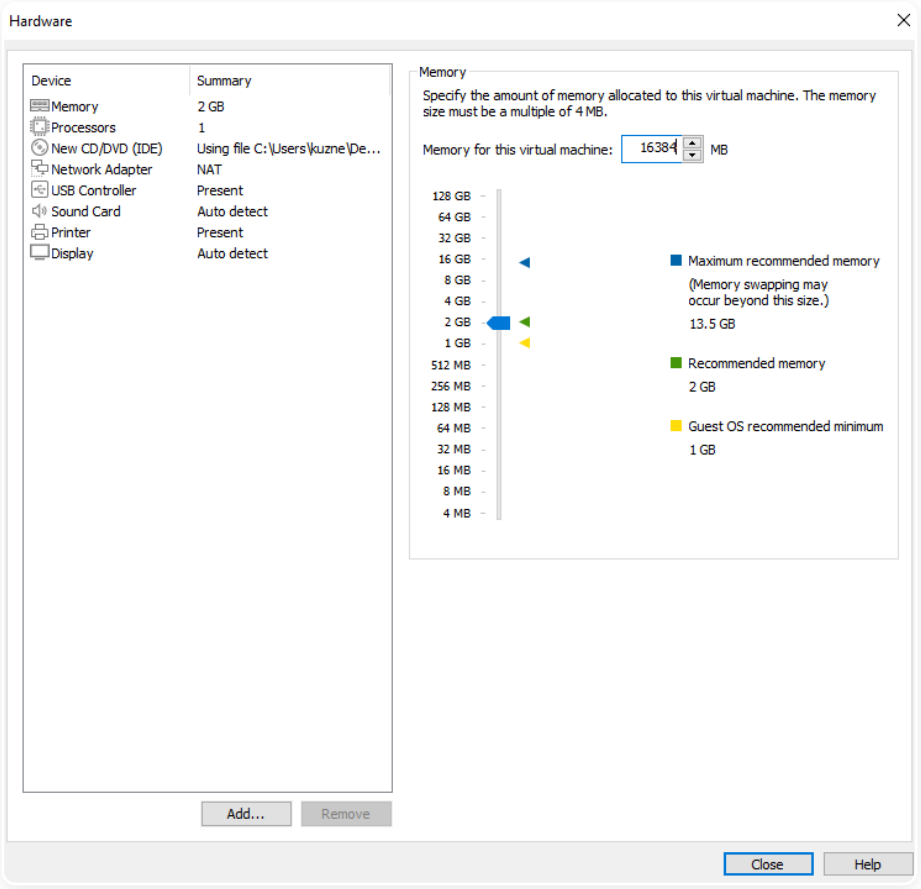
5. Укажите размер вирутального жесткого диска **150 ГБ**:



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

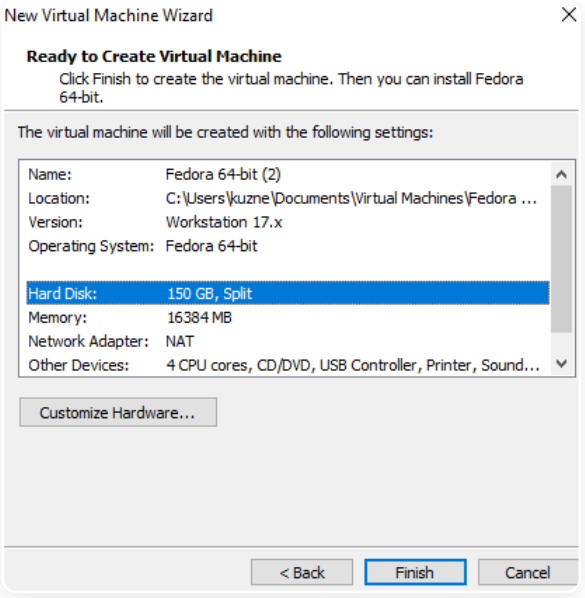


7. Укажите размер виртуальной оперативной памяти **16384 МБ**:

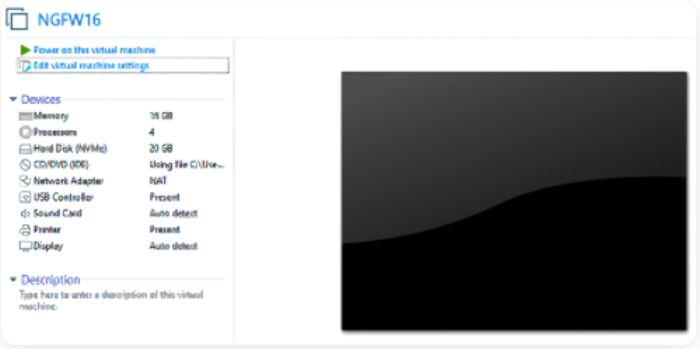


8. Укажите количество ядер процесса равное 4:

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.

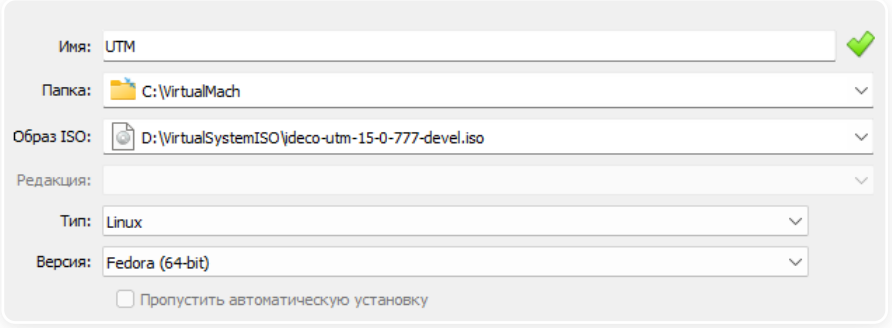
12. Нажмите **OK** для завершения настройки виртуальной машины.

VirtualBox 7.0.12

Настройка

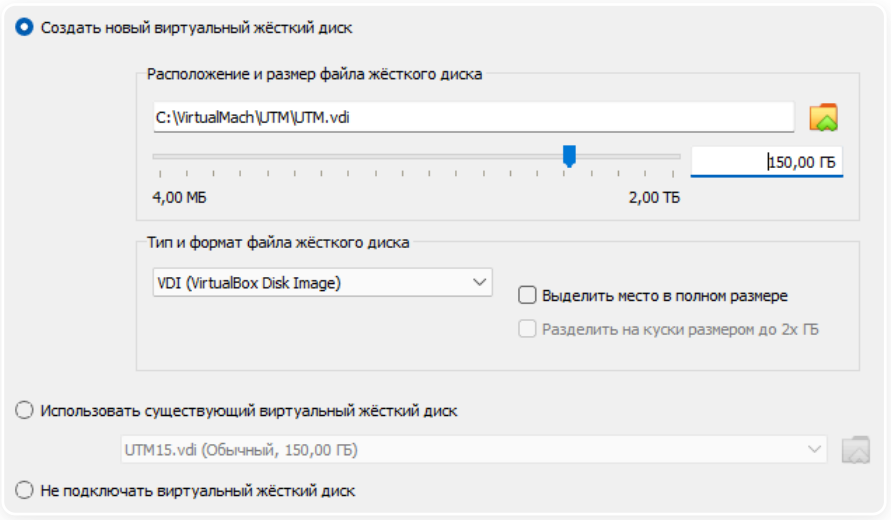
> По умолчанию при создании виртуальной машины создается одна сетевая карта с типом подключения **NAT**.

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



2. Установите размер оперативной памяти ВМ (**16 ГБ**) и нажмите **Включить EFI**:

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



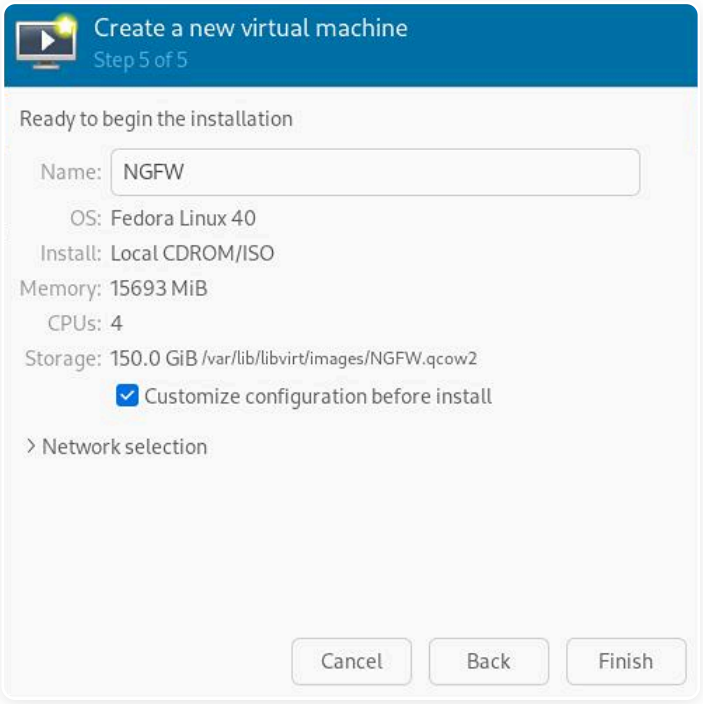
4. Нажмите **Готово**

KVM

Настройка

1. При установке Ideco NGFW 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.

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 этот пакет 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.
- **Гостевая ОС**:
  - **Тип** - Linux.
  - **Версия** - 6.x - 2.0 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:

- **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:

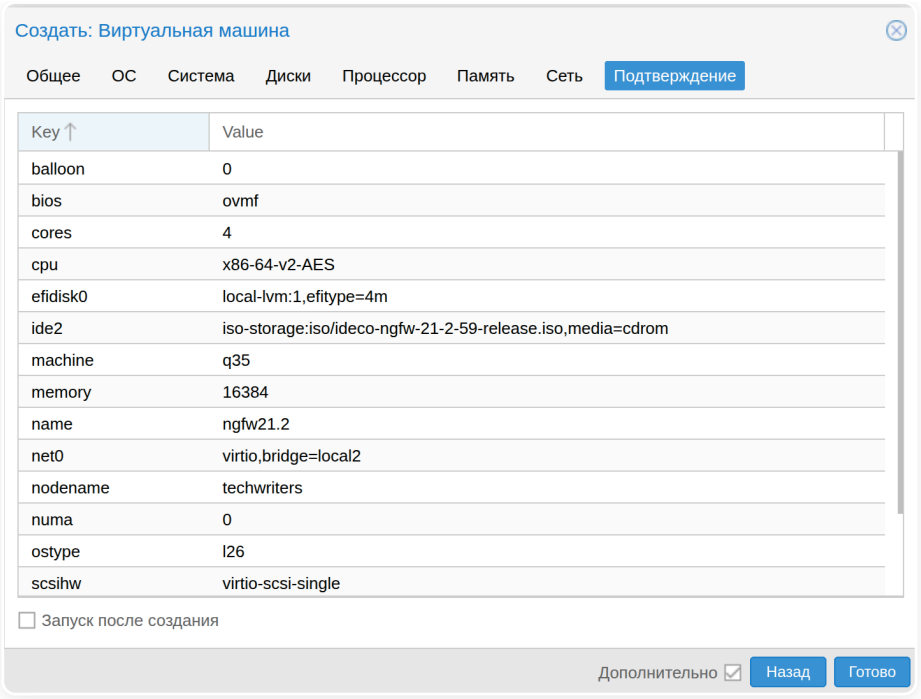
6. В разделе **Память** укажите объем оперативной памяти (не менее 16 ГБ):

- **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 файрвола в Ideco NGFW 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 NGFW 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

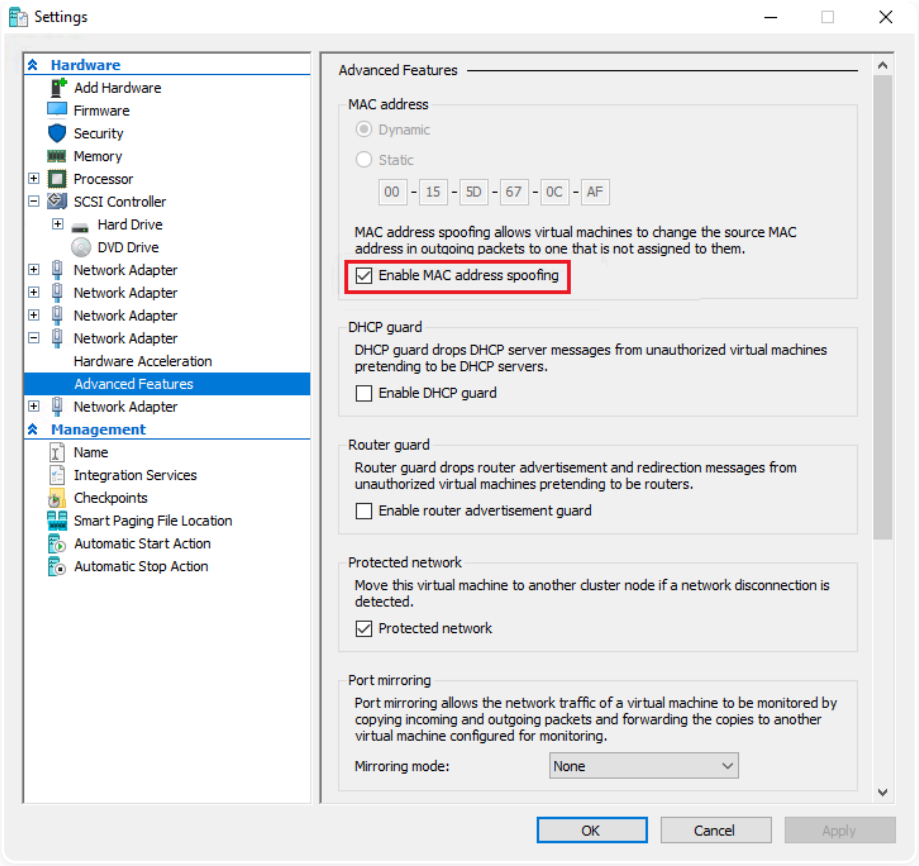
- Поддерживается только второе поколение виртуальных машин под Windows Server 2012 R2 или выше.
- Отключите опцию **Secure Boot (Безопасная загрузка)**.
- Отключите опцию **Dynamic memory (Динамическая память)**.
- Используйте **Network Adapter (Сетевой адаптер)**.

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

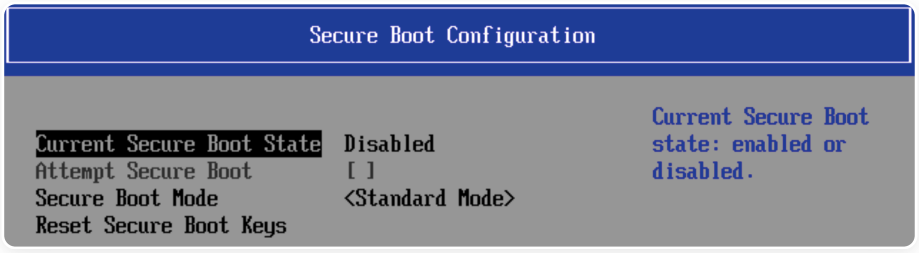
Для корректной работы кластерной сети, а также при использовании LACP-интерфейсов требуется дополнительная настройка на обеих нодах:

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

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



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



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.

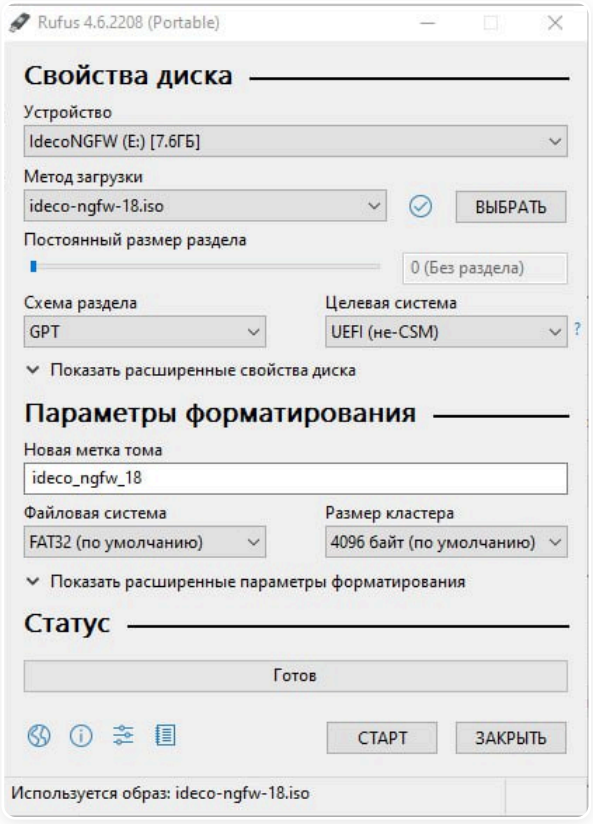
3. Выберите нужный USB-накопитель в пункте **Устройство**.

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

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

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>"
```

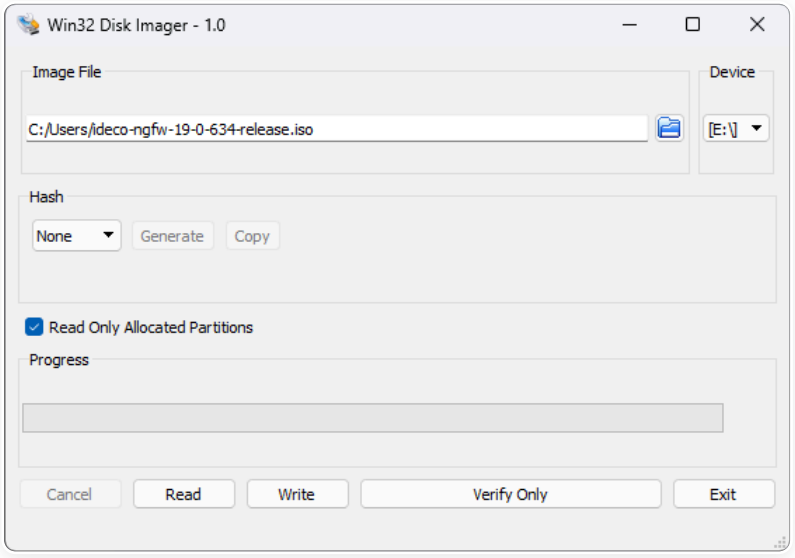
2. Установите программу Win32diskimager и запустите.

3. Нажмите на значок синей папки и выберите ISO-файл, который вы 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-19-11-29-release.iso" | sha256sum -c
```

2. Найдите USB-носитель в системе:

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

Ответ:

```
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-19-11-29-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 после создания загрузочного USB-накопителя можно прочитать в статье Установка.

Установка

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube

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

Процесс установки

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

Для установки Ideco NGFW выполните действия:

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

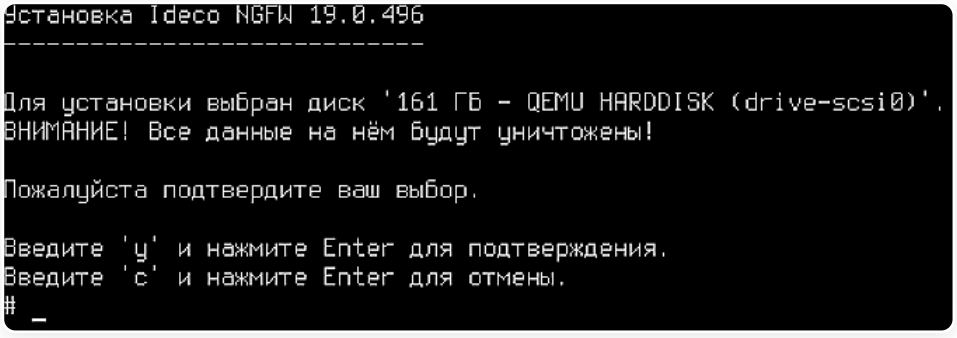


При установке или загрузке сервера Ideco NGFW не рекомендуем нажимать на клавиатуре:

- `-` - 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**.

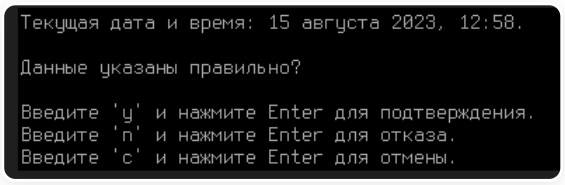
2. Выберите диск и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой находится сервер:



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



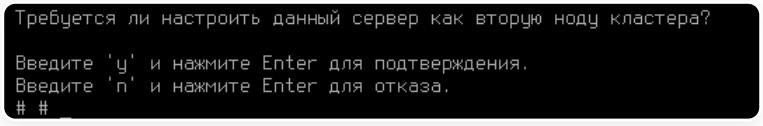
Извлеките USB-диск после установки Ideco NGFW, чтобы загрузка с него не началась заново.

5. Не нажимайте никаких клавиш при появлении окна:

После загрузки система автоматически перейдет к локальному интерфейсу Ideco NGFW.

Настройка второй ноды кластера

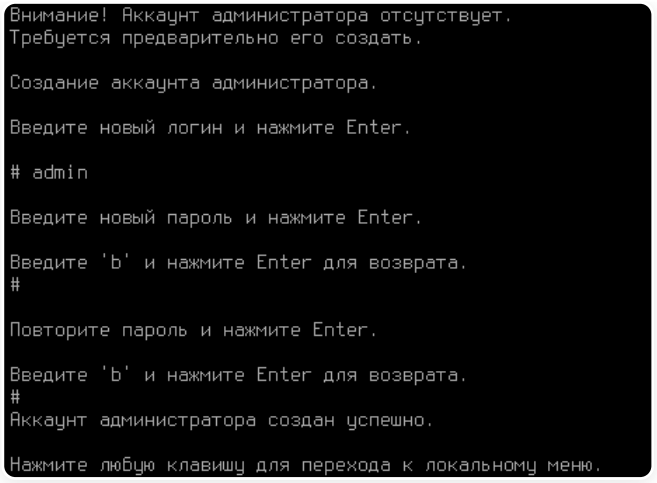
1. Введите **y** для начала настройки NGFW как второй ноды кластера:



2. Для продолжения настройки воспользуйтесь статьей Кластеризация.

Создание учетной записи администратора

Для входа в веб-интерфейс (после уведомления "*Создание аккаунта администратора*") создайте учетную запись администратора, соблюдая требования к паролю:



Требования к паролю

- 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.

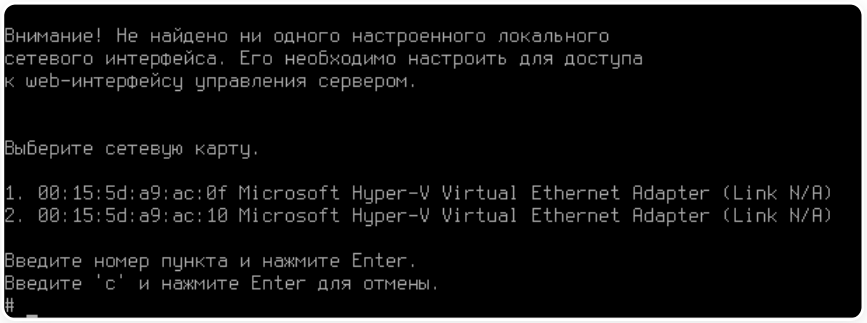
Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;`, `^[[4~;` и т.д.

Настройка локального интерфейса

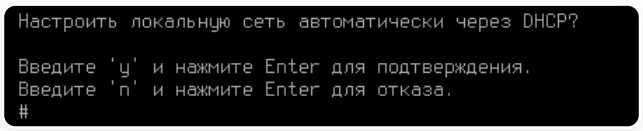
При использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса.
Для корректной идентификации сетевой карты используйте ее MAC-адрес.

Для настройки Ideco NGFW через веб-интерфейс настройте локальный интерфейс в локальном меню шлюза:

1. Введите номер сетевого адаптера под локальный интерфейс:



2. Настройте локальную сеть автоматически через DHCP, введя **y**, или вручную, введя **n**:



3. Введите локальный IP-адрес и маску подсети в формате `ip/маска` и нажмите **Enter**:

```
Введите IP/префикс и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# 10.10.0.185/24
```

4. Введите адрес шлюза или оставьте поле пустым:

- При настройке **Ideco NGFW в качестве шлюза** оставьте поле шлюз пустым:

```
Введите адрес шлюза (или оставьте пустым) и нажмите Enter.

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

- При настройке **Ideco NGFW в качестве прокси** введите шлюз с доступом в интернет:

```
Введите адрес шлюза (или оставьте пустым) и нажмите Enter.

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

5. Задайте тег VLAN (стандарт VLAN 802.3q) или оставьте поле пустым:

```
Введите VLAN тэг (или оставьте пустым) и нажмите Enter.

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

После создания локального интерфейса откроется локальное меню управления сервером:

```
Управление сервером

1. Консоль
2. Отключить все интерфейсы и настроить новый
3. Включить доступ к веб-интерфейсу из внешней сети
4. Включить доступ к серверу по SSH из Интернет
5. Включить доступ к серверу по SSH из локальных сетей
6. Включить режим `Разрешить Интернет всем`
7. Сбросить блокировки по IP
8. Отключить пользовательский файрвол
9. Отключение VCE-интерфейсов
10. Создать новый бэкап
11. Восстановить из бэкапа
12. Мгновенно восстановить из бэкапа
13. Включить доступ Удаленного Помощника
14. Контакты технической поддержки
15. Управление кластером
16. Восстановиться на предыдущую версию
17. Перезагрузка сервера
18. Отключить сервер
19. Выход
```

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

Полезные ссылки

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

Первоначальная настройка

Для получения доступа в интернет и настроить авторизацию. В противном случае доступ в интернет для устройства с установленным Ideco NGFW будет заблокирован.

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

Подключение к веб-интерфейсу Ideco NGFW

1. Запустите на любом компьютере в локальной сети поддерживаемый интернет-браузер (современные версии браузеров Firefox, Chrome и браузеров, основанных на Chromium).

2. Введите в адресной строке IP-адрес, указанный при настройке локального 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 NGFW.

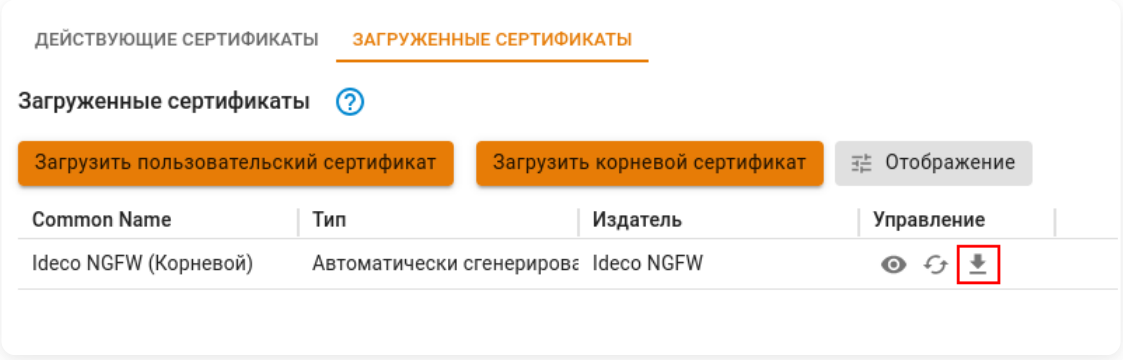
Импорт корневого сертификата NGFW

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

1. Скачайте сертификат одним из способов:

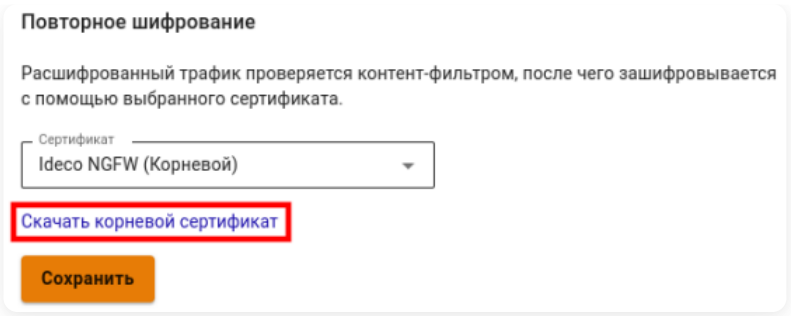
Из раздела Сервисы

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



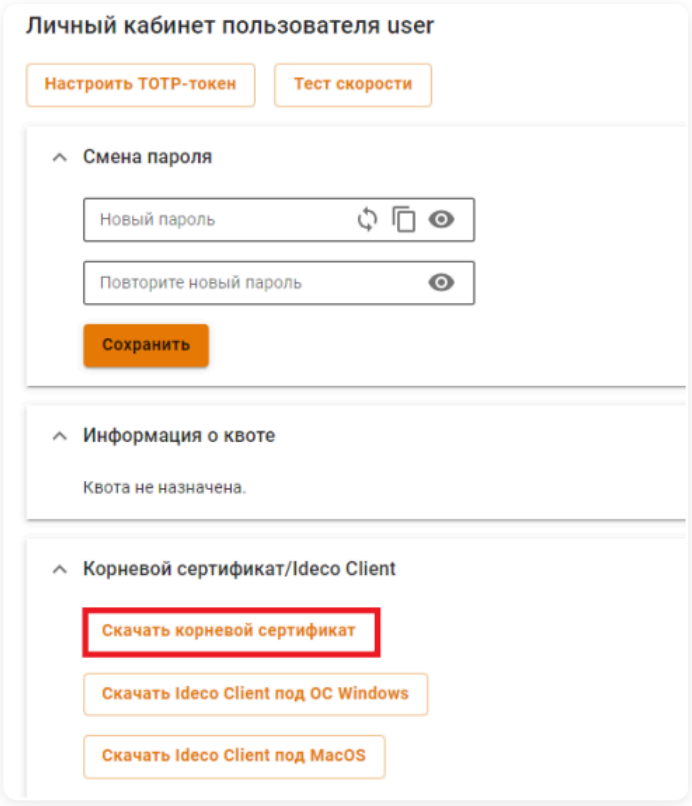
Из раздела Правила трафика

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



Из личного кабинета пользователя

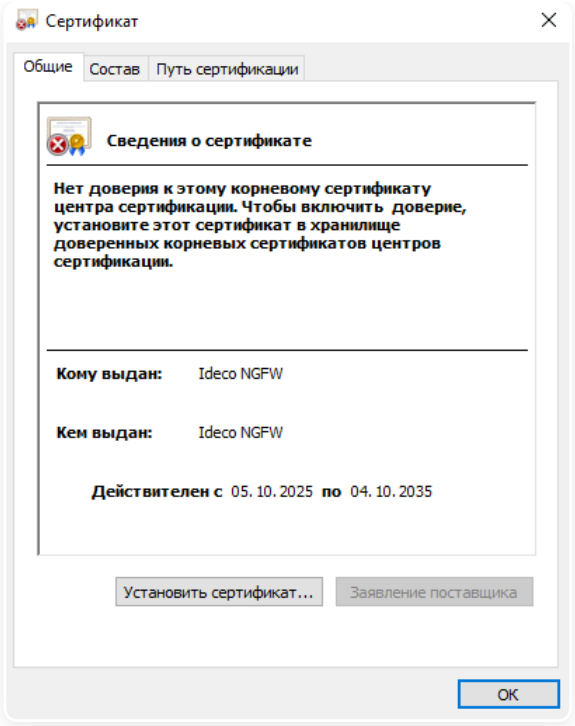
В личном кабинете Ideco NGFW под учетной записью одного из пользователей перейдите на вкладку **Корневой сертификат/Ideco Client** и нажмите **Скачать корневой сертификат**:



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

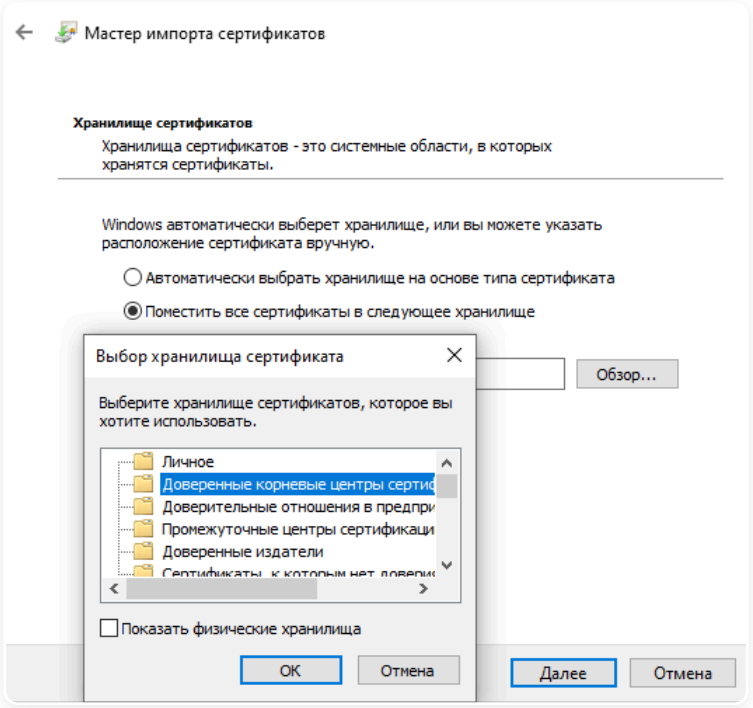
Пример для Windows

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

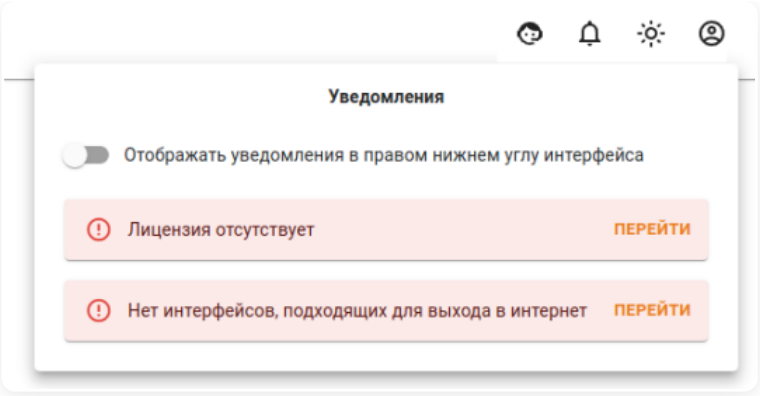


2. Выберите расположение хранилища **Локальный компьютер**:

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:



Настройка Ethernet-подключения для доступа в интернет

При создании, редактировании или удалении сетевого интерфейса перевыпускается SSL-сертификат, поэтому вероятно снижение скорости работы веб-интерфейса Ideco NGFW. В этом случае рекомендуем нажать F5.

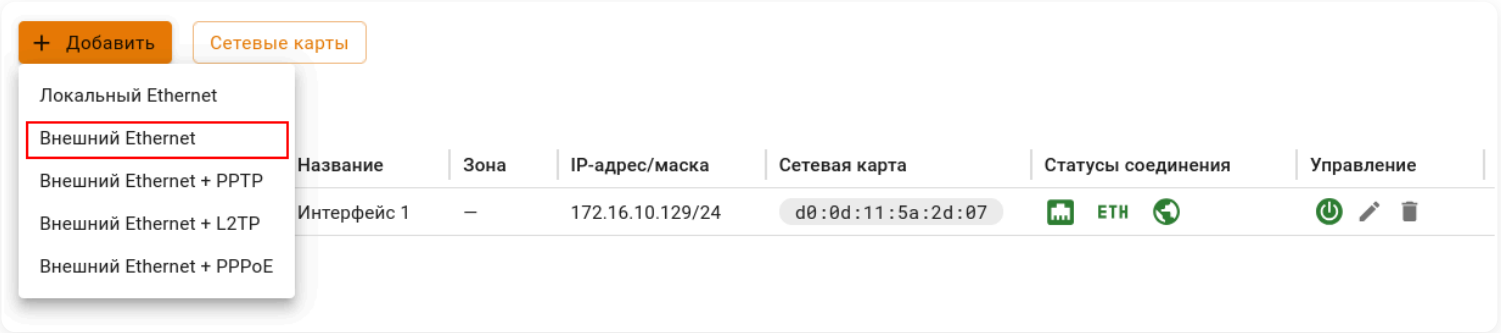
Этот тип подключения требует настройки параметров, описанных ниже в таблице.

Параметр	Примечание
Сетевая карта	Укажите сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру. Для идентификации адаптера ориентируйтесь на наименование производителя или MAC-адрес
IP-адрес и маска	Укажите сетевые реквизиты, которые были назначены провайдером. Укажите IP-адрес и сетевую маску в формате CIDR или четырех октетов
Шлюз по умолчанию	Укажите IP-адрес шлюза интернет-провайдера, через который будет осуществляться подключение к сети интернет

Для настройки Ethernet-подключения выполните:

1. Перейдите в раздел **Сервисы** → **Сетевые интерфейсы**.

2. Нажмите **Добавить** и выберите пункт **Внешний Ethernet**:



Будьте внимательны!

При выборе пункта **Локальный Ethernet** и заполнении поля **Шлюз** доступ в интернет будет отсутствовать. Шлюз указывается только если NGFW работает в режиме прямого прокси с одним интерфейсом.

3. Выберите подходящую сетевую карту.

4. Заполните необходимые поля и нажмите **Добавить**.

Включите опцию **Автоматическая конфигурация через DHCP** если провайдер поддерживает автоматическое конфигурирование внешнего сетевого интерфейса с помощью протокола DHCP.

Настройка других типов подключений

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

- Внешние и локальные интерфейсы;
- Одновременное подключение к нескольким провайдерам.

Регистрация сервера

Для активации лицензии необходима обязательная регистрация сервера в личном кабинете.

Выберите удобный способ получения лицензии:

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

Онлайн-регистрация

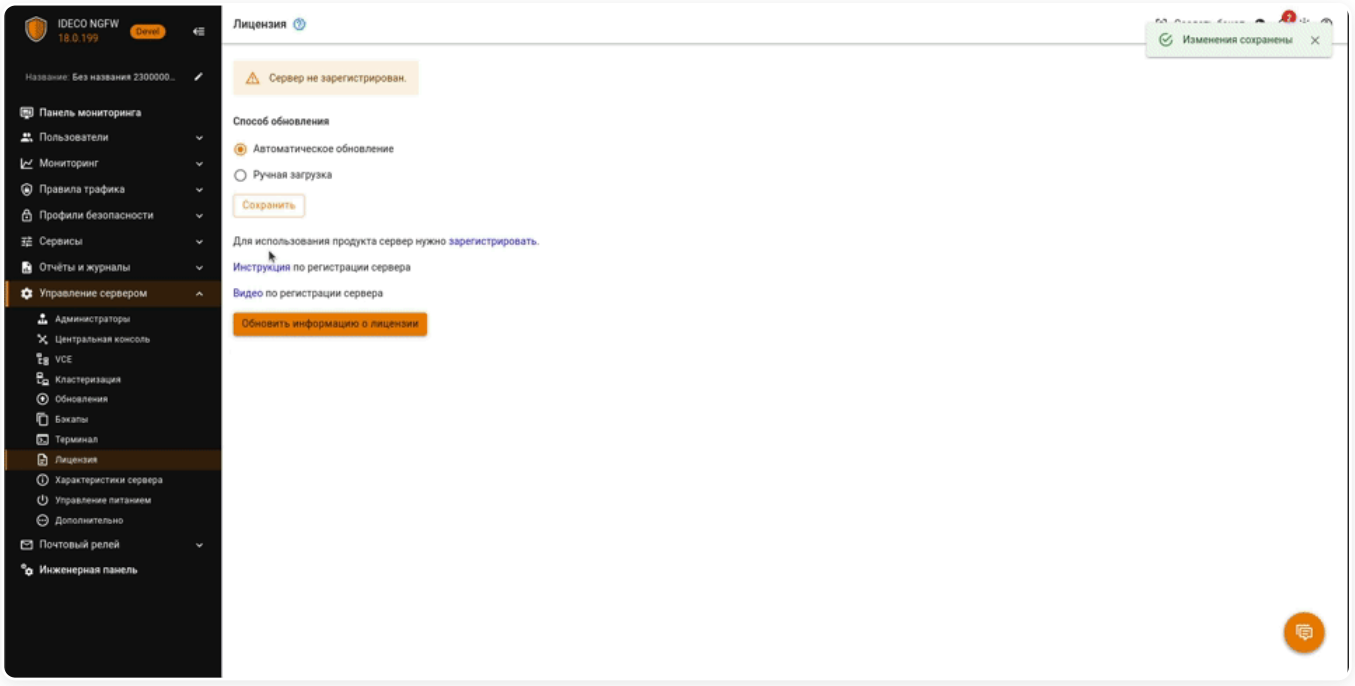
Перед онлайн-регистрацией создайте **Внешний Ethernet-интерфейс** для выхода в интернет. Затем активируйте опцию **Разрешить интернет всем**. Не забудьте отключить опцию после получения лицензии.

Шаги онлайн-регистрации сервера и привязки лицензии:

1. Перейдите в веб-интерфейс Ideco NGFW в раздел **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:

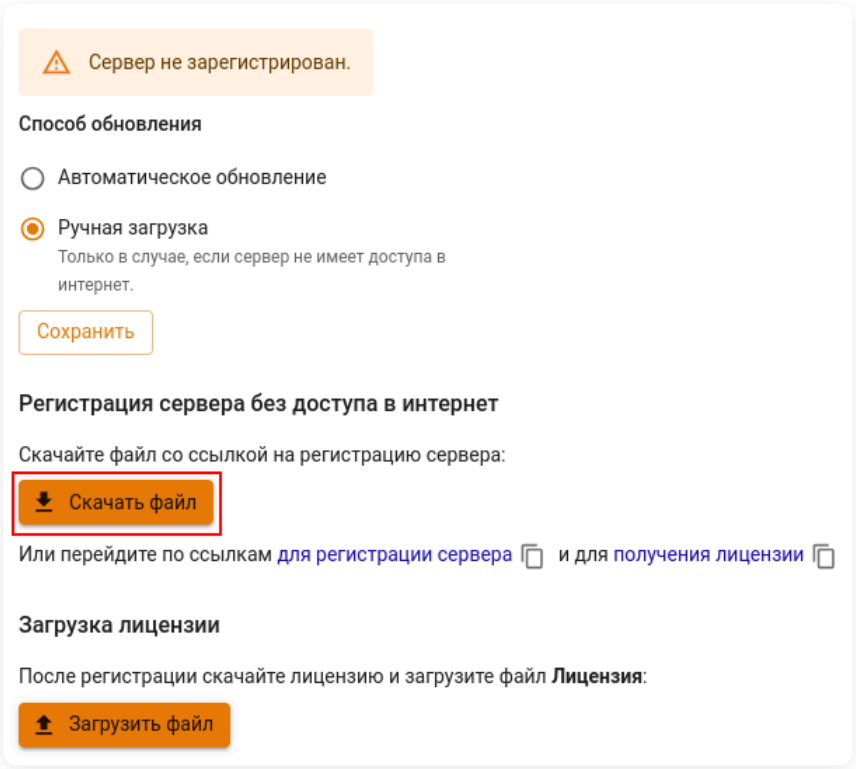
- Rutube

- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

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

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Это можно сделать, нажав на кнопку, или скопировать ссылку из веб-интерфейса:

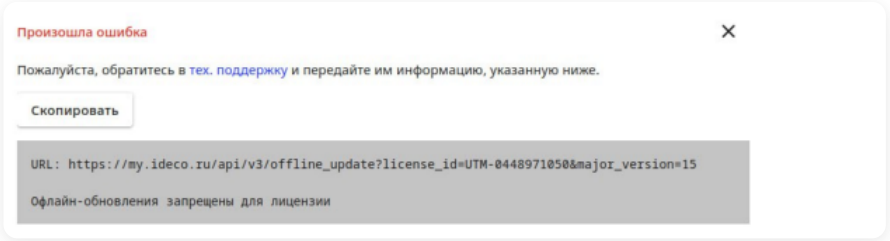


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

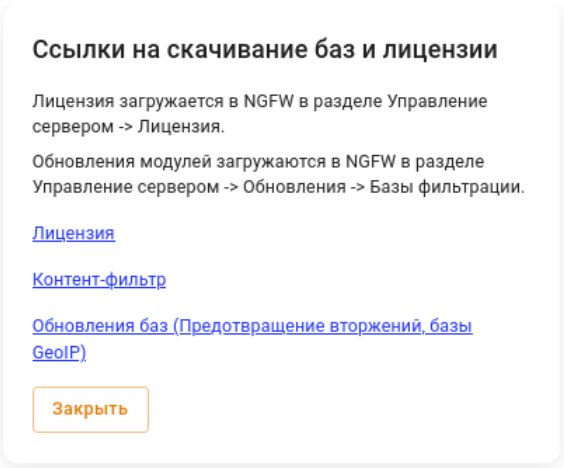
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

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:

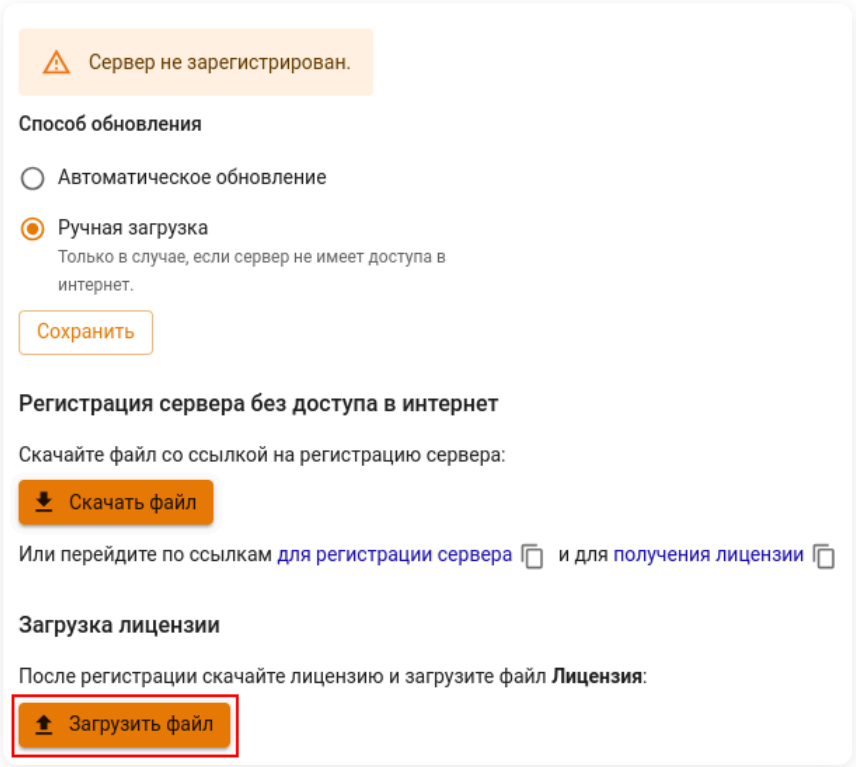


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



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** в веб-интерфейсе Ideco NGFW и загрузите файл с лицензией, скачанный в пункте 6:



Повторная регистрация сервера после удаления

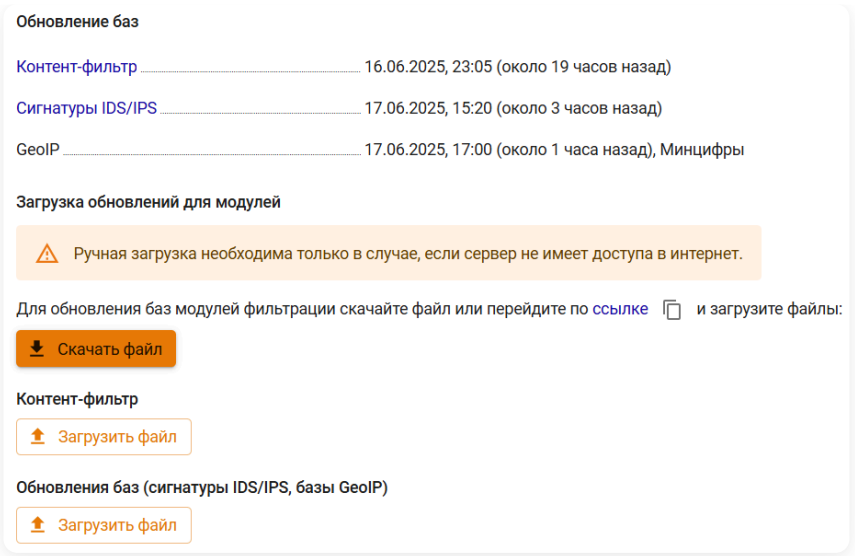
1. Откройте терминал и введите команду:

```
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 в раздел **Управление сервером** → **Обновления** → **Базы фильтрации** и загрузите скачанные в шестом пункте Офлайн-регистрации файлы, нажав на соответствующие кнопки:



Базы фильтрации Ideco NGFW могут меняться ежедневно, поэтому при ручной загрузке обновляйте их 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.

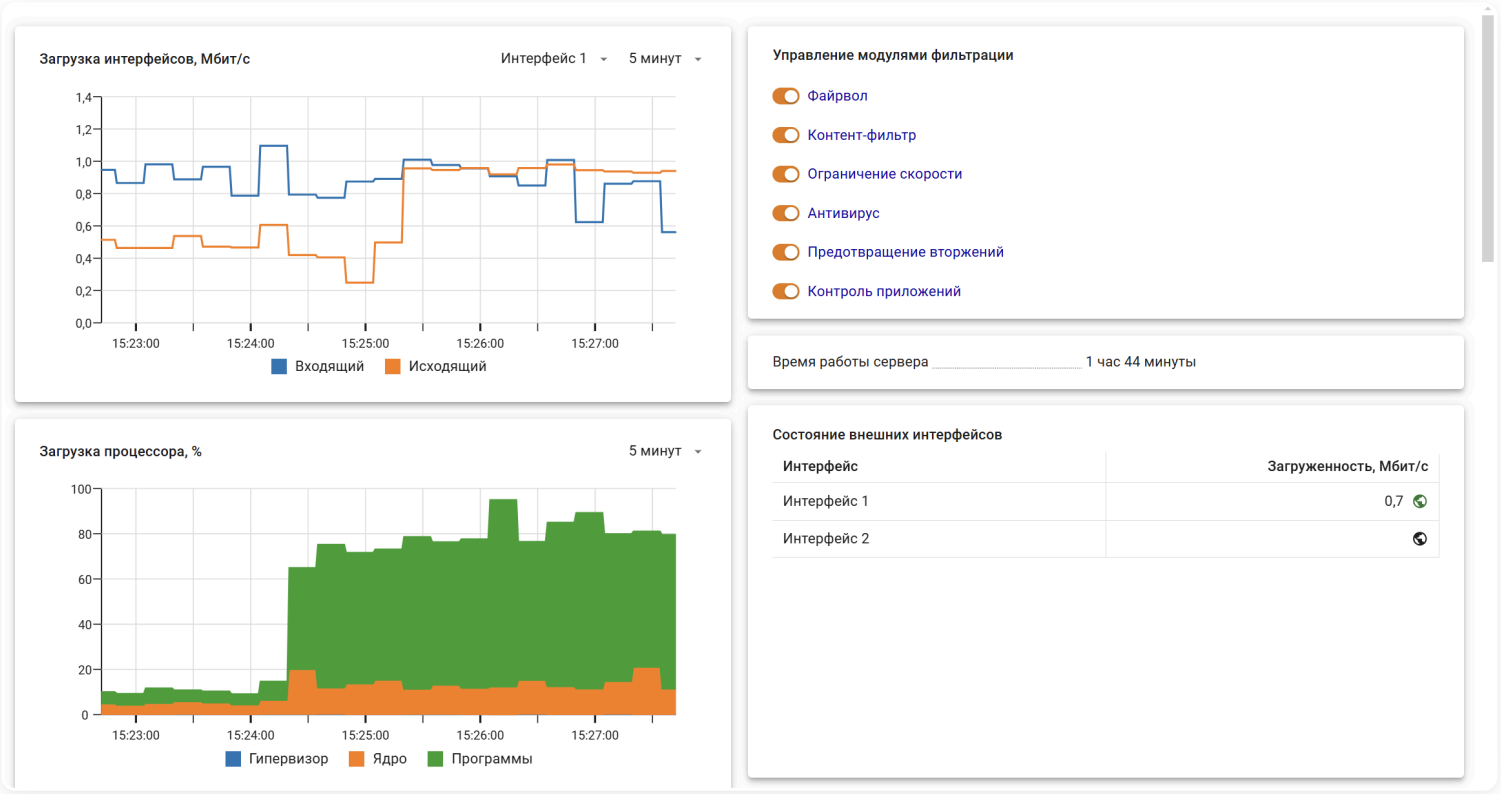
- **IP и MAC авторизация** - способ авторизации, при котором пользователь получает доступ в интернет без ввода логина и пароля:
  - **Авторизация по IP-адресу**. Проверьте, чтобы IP-адрес устройства пользователя совпадал с IP-адресом, указанным администратором в настройках учетной записи пользователя 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.

Панель мониторинга

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



Отображение оперативной информации

- Загрузка сетевых 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.

Управление модулями фильтрации

Блок позволяет включить или выключить соответствующие модули фильтрации:

- Файрвол.
- 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 **Контроля приложений**. При этом учитывается служебный трафик NGFW (`169.254.1.1`):
  - DNS-запросы для резолвинга доменных имен из **Правила трафика** → **Объекты**.
  - ICMP-проверки доступности адресов из **Сервисы** → **Балансировка и резервирование** → **Адреса для проверки связи**.
  - Служебные запросы:
    - Выпуск Let's Encrypt сертификатов.
    - Проверка лицензии MY.IDECO.
    - Загрузка баз **Контент-фильтра** и IPS.
    - Скачивание ISO-образов обновлений.
  - Любые запросы, выполняемые через терминал NGFW.

Пользователи

Учетные записи
Создание и управление учетными записями пользователей

Перейти >

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

Перейти >

Двухфакторная аутентификация
Типы двухфакторной аутентификации и особенности их настройки

Перейти >

VPN-подключение
Настройка VPN-подключения с использованием протоколов: PPTP, 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 >

Active Directory/Samba DC
Настройка односторонней синхронизации с контроллером домена на базе Microsoft Active Directory и Samba DC

Перейти >

ALD Pro
Настройка односторонней синхронизации с системой управления каталогами ALD Pro

Перейти >

RADIUS
Настройка RADIUS-сервера, двухфакторная аутентификация пользователей и управление учетными записями

Перейти >

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

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Учетные записи

В веб-интерфейсе Ideco NGFW пользователи отображаются в виде дерева и могут быть организованы в группы с неограниченной вложенностью. Дерево учетных записей доступно в разделе **Пользователи → Учетные записи**.

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

В Ideco NGFW реализован принцип наследования, которое позволяет задавать и изменять общие параметры для всех пользователей группы через родительскую группу. Это упрощает управление и настройки для всей группы одновременно.

> Все пользователи Ideco NGFW по умолчанию входят в группу **Все**. Если при создании какого-либо правила в параметрах будет выбрана группа **Все**, правило будет распространяться на всех пользователей NGFW.

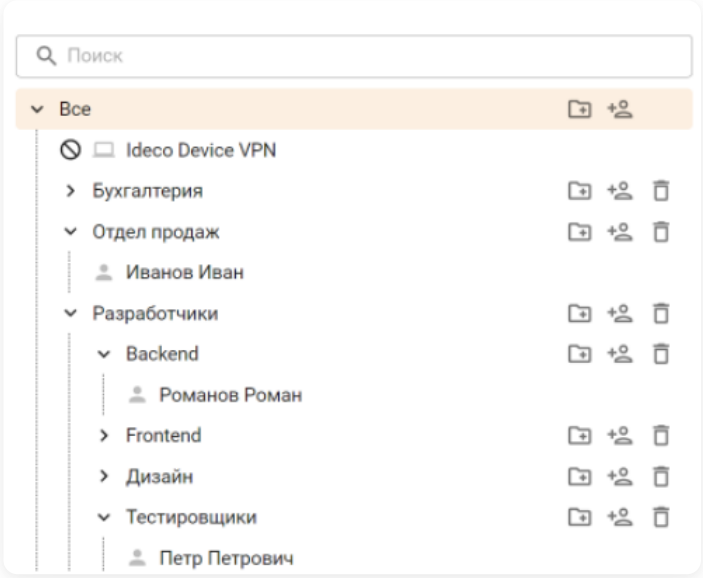
Цвет пиктограммы пользователя зависит от состояния учетной записи пользователя:

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

Пример дерева пользователей:



Управление учетными записями и группами

Создание учетной записи пользователя

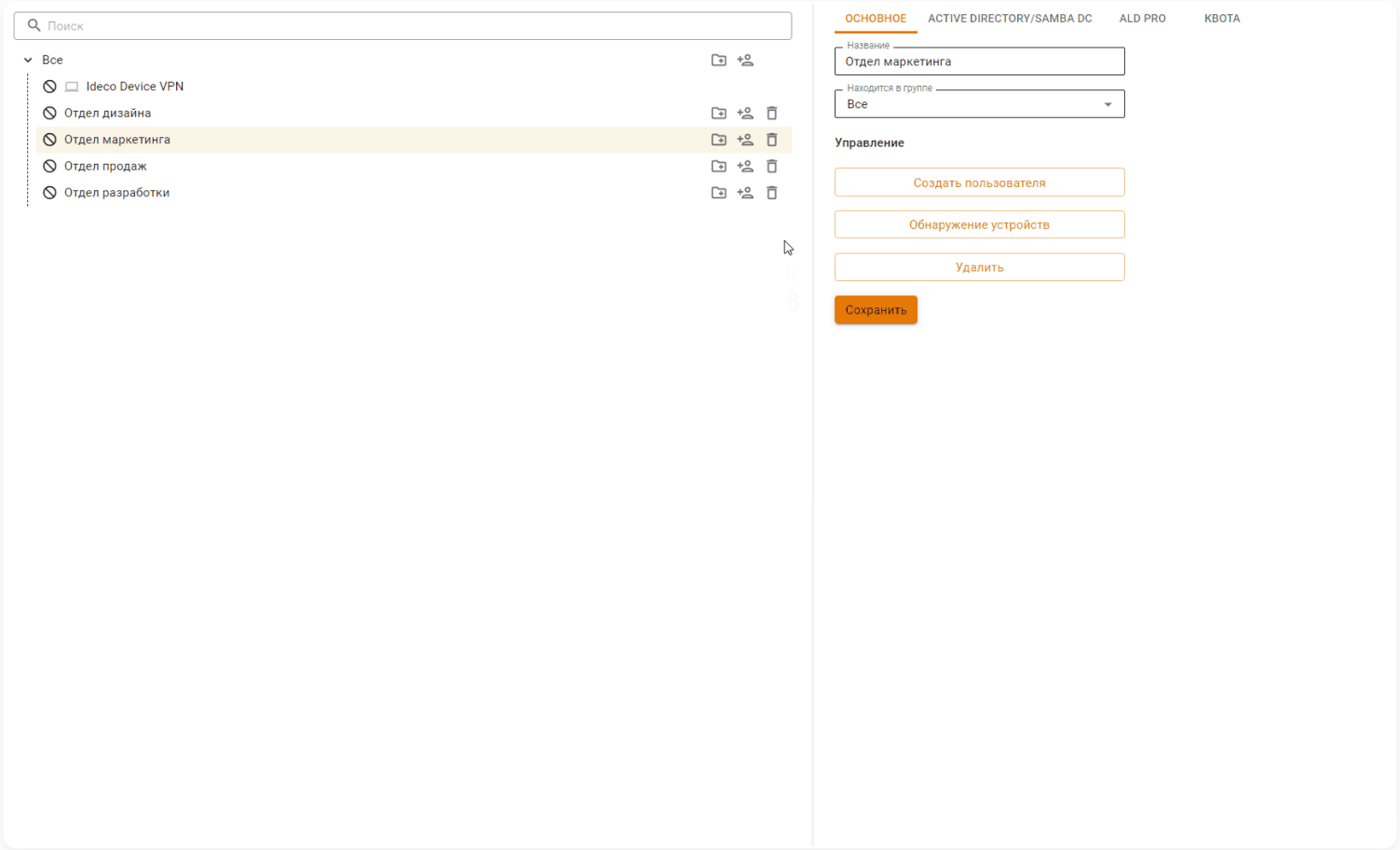
Не используйте в качестве логина пользователя IP-адрес, так как возникнет ошибка при подключении по IKEv2.

Способы создания учетной записи пользователя и группы:

Пользователь в определенной группе

1. Выберите группу, в которую добавится пользователь.

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



3. Заполните поля:

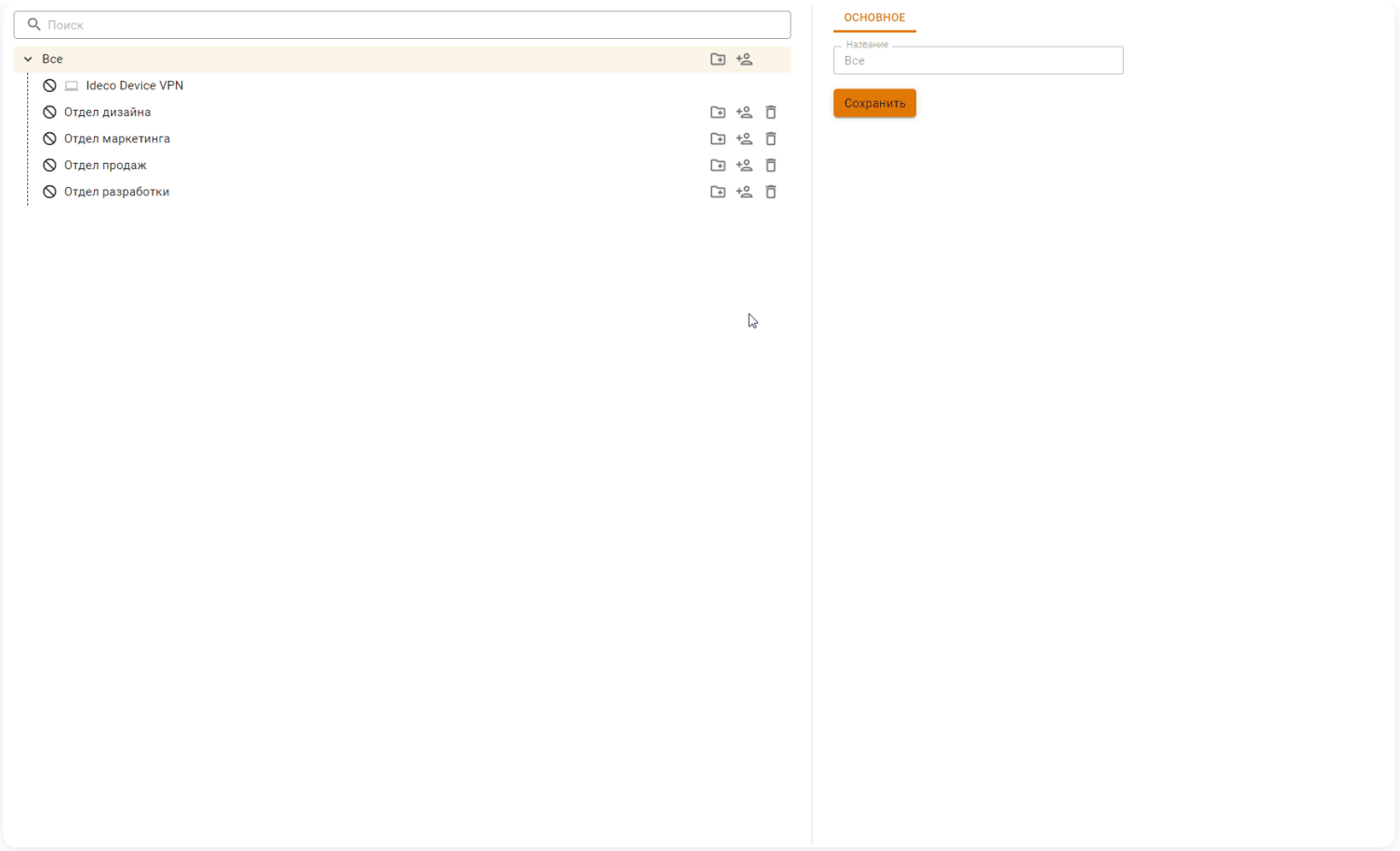
- **Имя пользователя** - имя пользователя. Например, Иванов Иван. Максимальное количество символов - 128.
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - пароль, который содержит комбинацию цифр и букв.
- **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 разделе **Пользователи → Авторизации → IP и MAC авторизация Ideco NGFW.

4. Нажмите **Добавить**.

Пользователь вне групп

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

2. Нажмите :



3. Заполните поля:

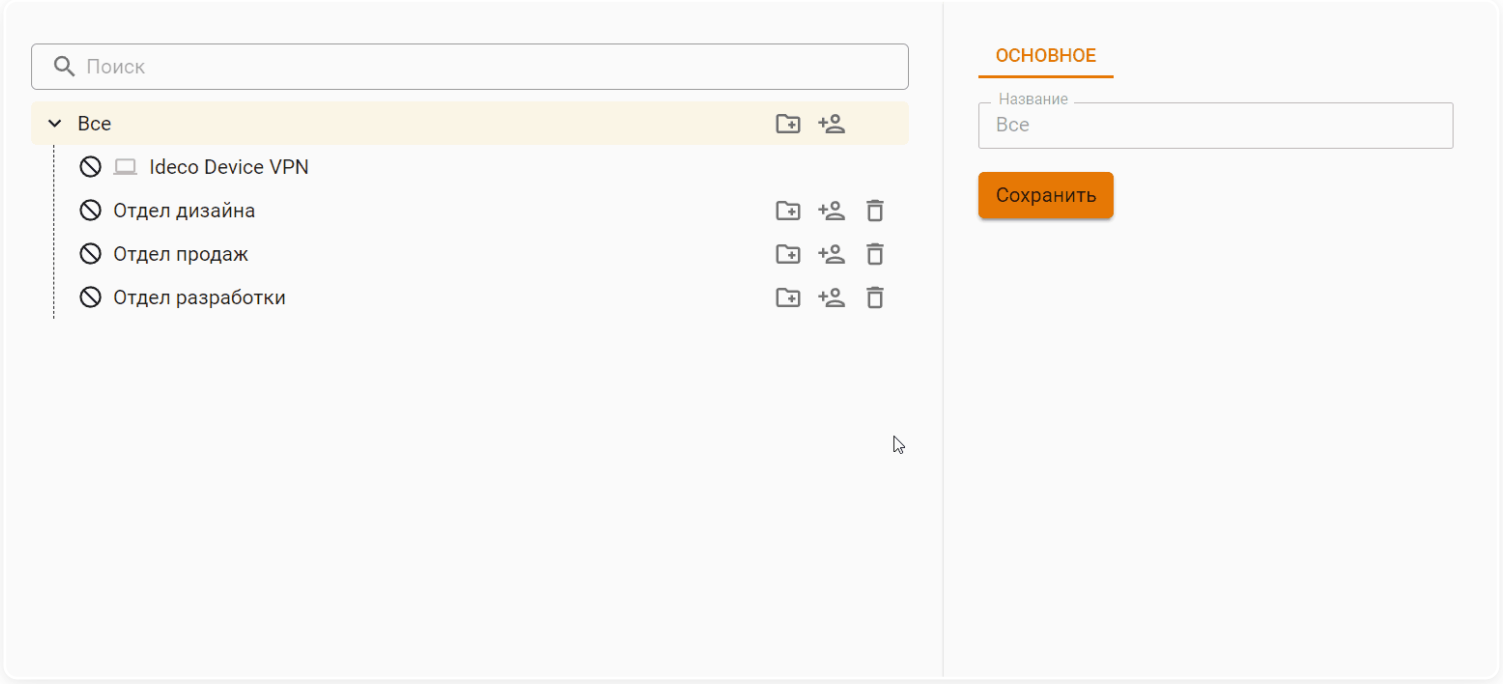
- **Имя пользователя** - имя пользователя. Например, Иванов Иван. Максимальное количество символов - 128.
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32.
- **Пароль** и **Повторите пароль** - пароль, который содержит комбинацию цифр и букв.
- **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 разделе **Пользователи → Авторизации → IP и MAC авторизация Ideco NGFW.

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, импортированных из Active Directory, проверка пароля осуществляется средствами Active Directory.

Рекомендации к созданию сложности паролей

Доступна автоматическая генерация пароля!

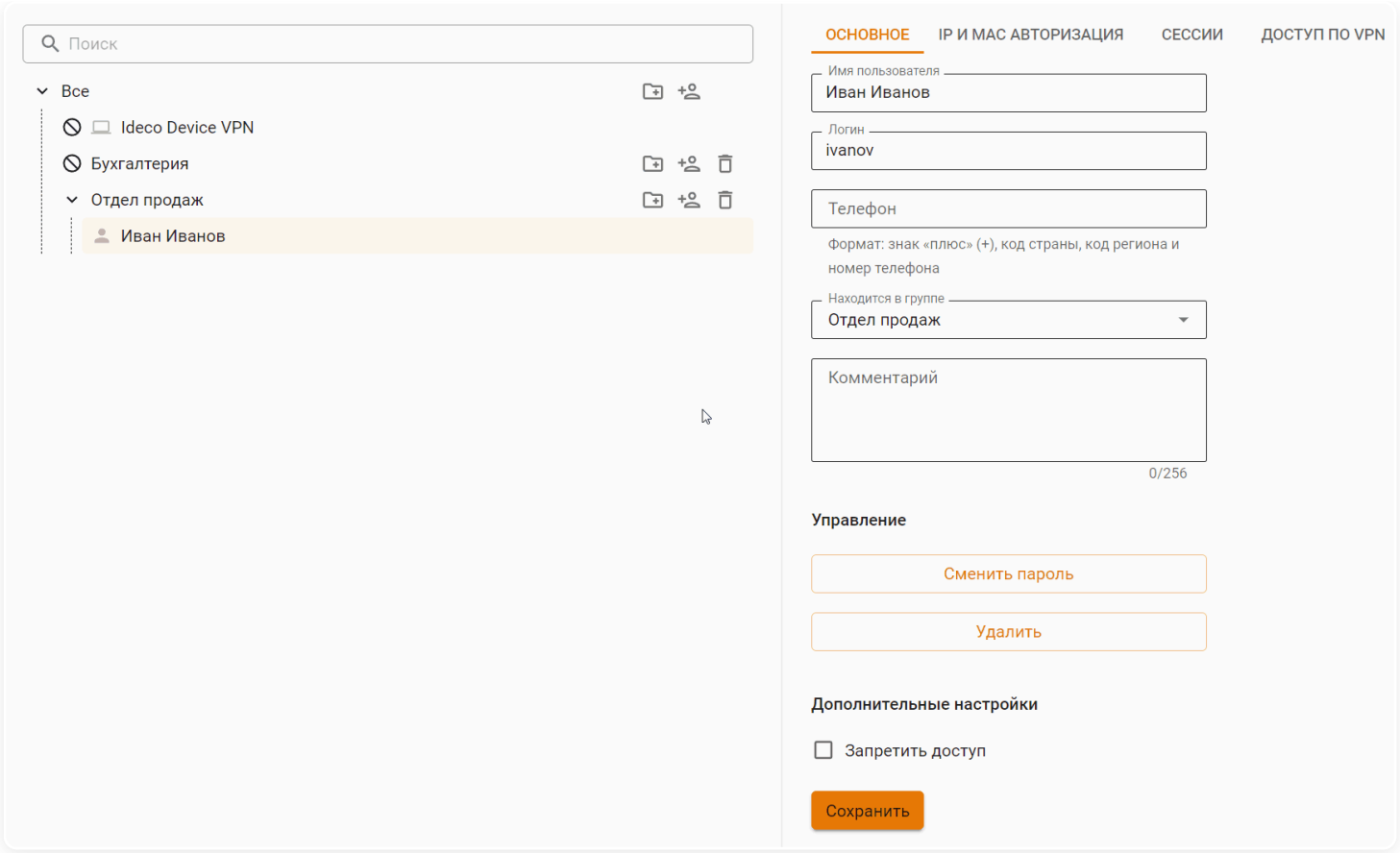
- Минимальная длина - 12 символов.
- Использование строчных и заглавных латинских символов.
- Использование цифр и специальных символов.

Создать пользователя Ideco NGFW в группу Active Directory нельзя. Если требуется добавить дополнительного пользователя в группу Active Directory, это необходимо делать в дереве пользователей на контроллере домена.

Удаление учетной записи пользователя или группы

Реализовано два варианта удаления:

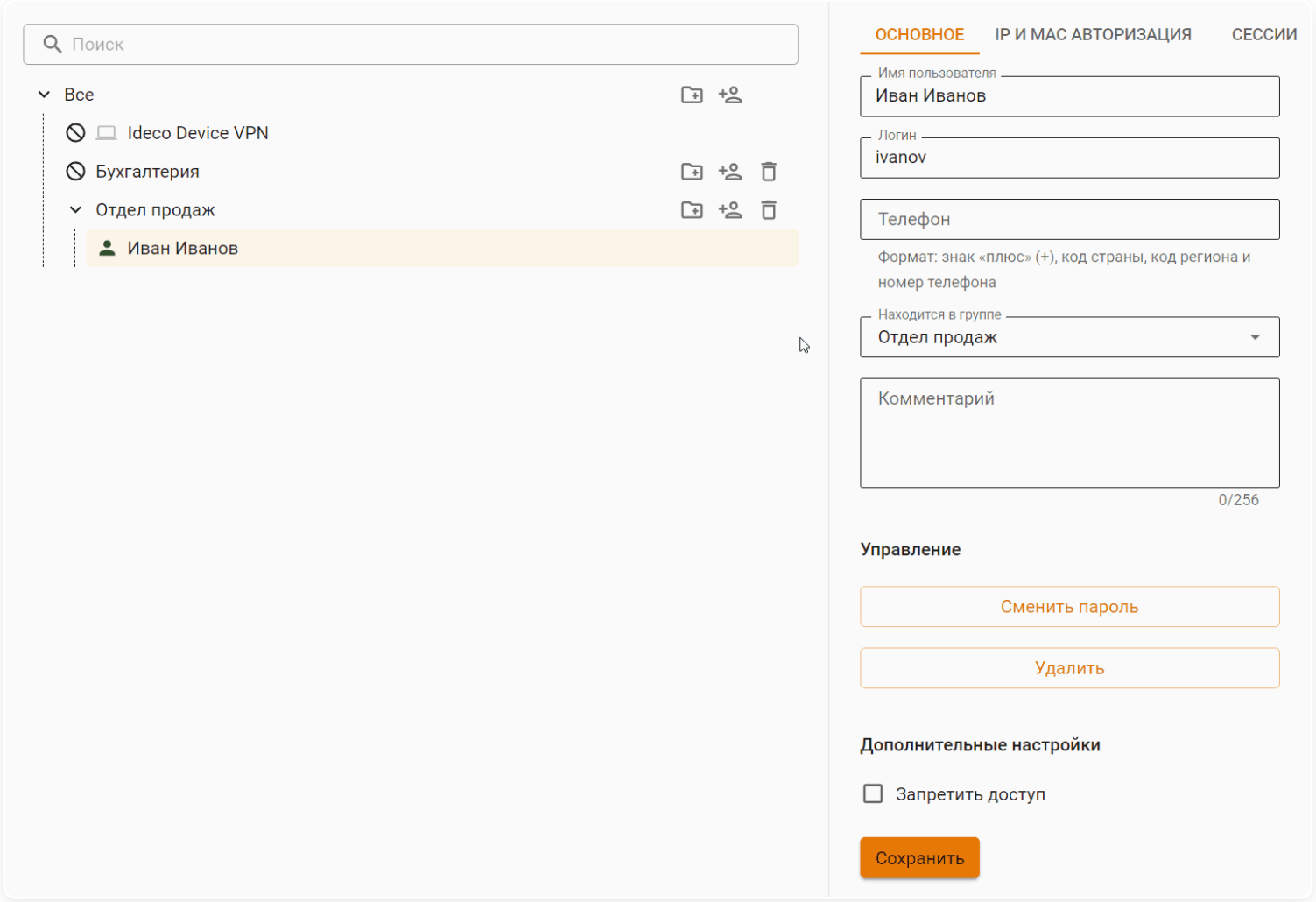
- Наведите курсор на пользователя и нажмите на .
- Нажмите на **Удалить** на вкладке **Основное**:



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.

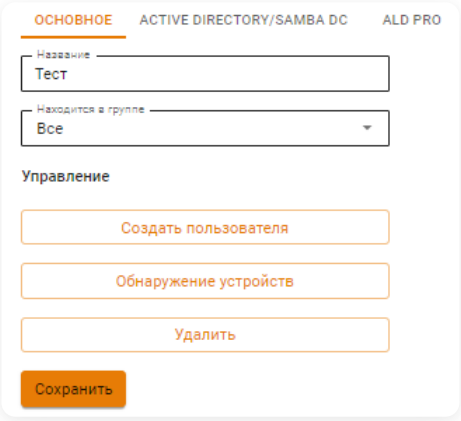
Настройка пользователей

Чтобы изменить параметры учетной записи 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. Настройки, заданные для группы, автоматически применяются ко всем ее участникам.

Основное



- **Изменить название и вложенность группы**. Для этого в соответствующем поле введите новое название и укажите группу, в которую требуется переместить эту группу;
- **Создать пользователя**. При нажатии на одноименную кнопку появится форма создания пользователя;
- **Обнаружение устройств**. При нажатии на одноименную кнопку откроется раздел Обнаружение устройств;
- **Удаление группы**. Вместе с группой удаляются учетные записи пользователей группы и привязки по IP- и MAC-адресам.

Active Directory/Samba DC

Категория содержит информацию об имени домена и типе группы. Процесс настройки синхронизации с Active Directory/Samba DC и импорт пользователей описан в статье Интеграция с Active Directory/Samba DC.

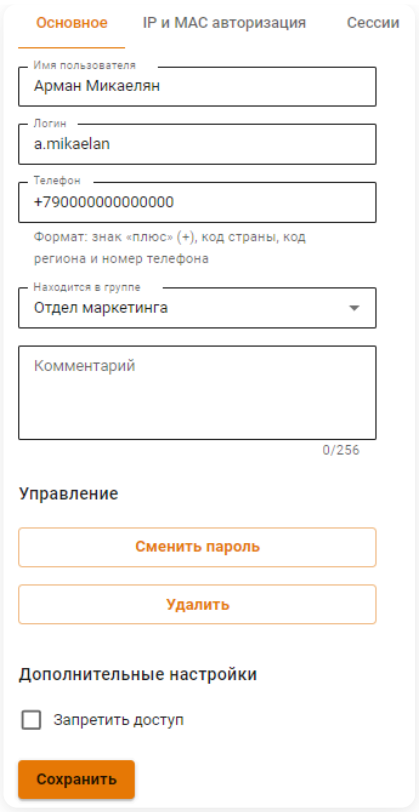
ALD Pro

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 пользователей

Основное

Основные настройки включают параметры, определяющие статус учетных записей пользователя. Базовые параметры:



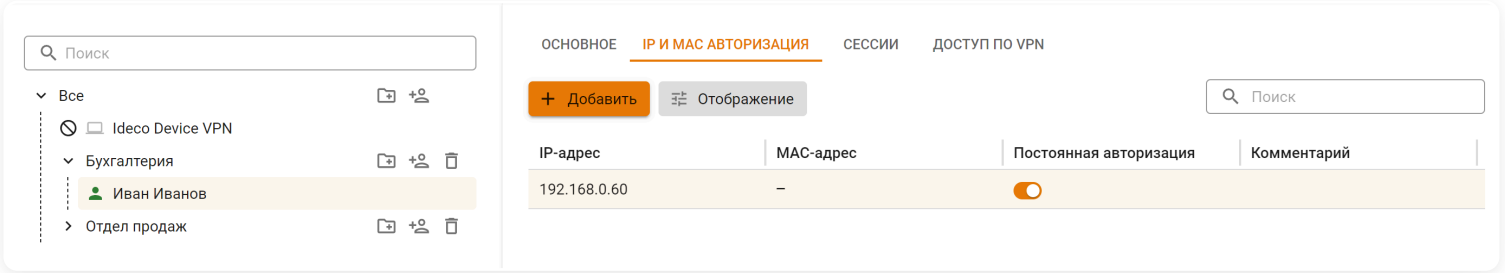
- **Имя пользователя** - имя пользователя, например, Иванов Иван. Максимальное количество символов - 128;
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32;
- **Телефон** - телефон для двухфакторной аутентификации. Формат: +, код страны, код региона и номер телефона;
- **Находится в группе** - используйте это поле для перемещения пользователя в другую группу;
- **Запретить доступ** - при установке этого флага пользователь не сможет авторизоваться, соответственно - пользоваться ресурсами интернета, почтой и личным кабинетом.

Для пользователей из Active Directory на вкладке **Основное** нельзя редактировать имя, логин, телефон, менять группу или пароль.

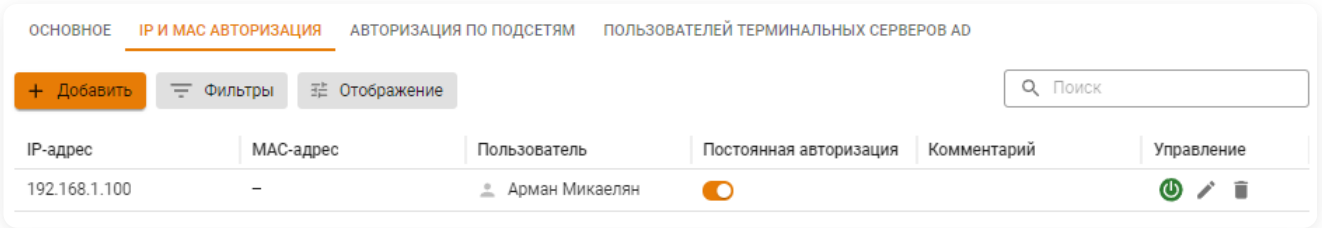
IP и MAC авторизация

Категория содержит правила авторизации по IP и MAC, созданные для определенного пользователя в двух разделах:

- **Пользователи → Учетные записи → IP и MAC авторизация**:



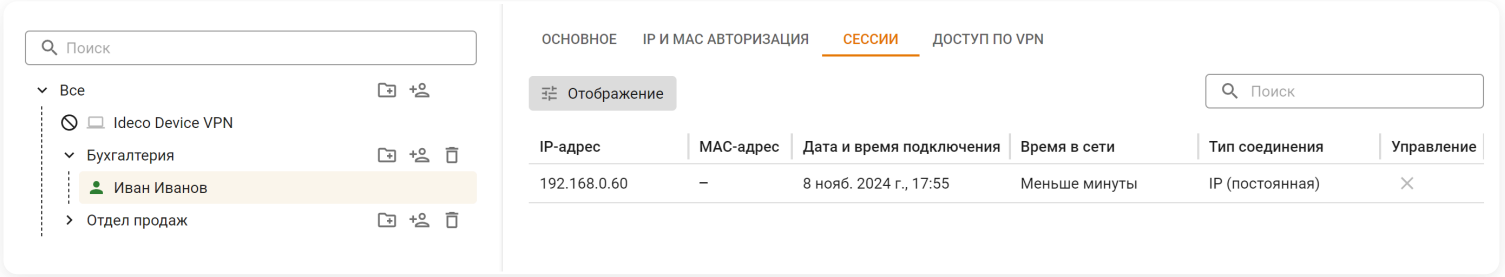
- **Пользователи → Авторизации**:



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

Сессии

Содержит таблицу с информацией обо всех активных сессиях пользователях:



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 разделе **VPN-подключения** → **Доступ по VPN**.

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

Авторизация пользователей

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 с возможностью контроля его трафика оно должно быть авторизовано на NGFW под учетной записью пользователя.

Особенности авторизации пользователей в Ideco NGFW:

- Количество приобретенных по лицензии учетных записей ограничивает число авторизованных пользователей.
- Сессия авторизации учетной записи привязана к IP-адресам хостов на протяжении действия сессии.
- Неавторизованный на NGFW хост не имеет доступа во внешние сети.
- Сессии авторизации пользователя, не проявляющего активность, завершаются по тайм-ауту и могут быть заняты новыми сессиями пользователей.

Для настройки автоматической авторизации пользователей при входе в систему воспользуйтесь статьей.

Общая информация

Все виды авторизации на Ideco NGFW являются IP-based (работают на основе IP-адреса хоста), и любая сессия авторизации привязана к IP-адресу хоста, с которого она установлена.

Под одной пользовательской учетной записью возможна одновременная авторизация **до пяти устройств**. При авторизации шестого устройства будет автоматически разорвана первая сессия. Например:

При авторизации по VPN

Если при авторизации первой сессии использовался VPN, включая Ideco Client, то при попытке входа в шестую сессию пользователь будет авторизован, а первая сессия будет автоматически разорвана.

При авторизации по IP, MAC, IP+MAC, WEB, NTLM, Ideco Agent, Log, Kerberos

Если в первой сессии использовались методы авторизации IP, MAC, IP+MAC, WEB, NTLM, Ideco Agent, Log, Kerberos, то в шестой сессии пользователь проходит авторизацию. При этом статус первой сессии в разделе **Сессии пользователей**. Это означает, что сессия вышла за пределы лицензии и будет автоматически разорвана.

Если разорвать шестую сессию, то первая сессия снова станет активной, а иконка исчезнет.
Сессия пользователя автоматически завершается при неактивности (отсутствии соединений с интернетом) в течение указанного в настройках времени (кроме подключений по VPN).

Трафик может генерировать и сама операционная система без участия пользователя (например, телеметрия Windows). Из-за этого тайм-аут для пользователя будет постоянно сбрасываться.

Время автоматического завершения сессии пользователя можно изменить с помощью настройки **Тайм-аут отключения** в разделе **Пользователи → Авторизация**:



Для применения нового тайм-аута отключения требуется перезагрузка Ideco NGFW.

Также можно авторизовать пользователей, которые подключаются по VPN с помощью протоколов IPsec IKEv2, SSTP, L2TP IPsec, PPTP. Инструкция по запуску PowerShell скриптов представлена в статье.

Полезные ссылки

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

Веб-аутентификация

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

Список служб для других разделов доступен по ссылке.

Веб-аутентификация в Ideco NGFW - тип авторизации, который предполагает, что отправленный через веб-браузер запрос неавторизованного пользователя будет переадресован на страницу авторизации Ideco NGFW. 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;
- 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.

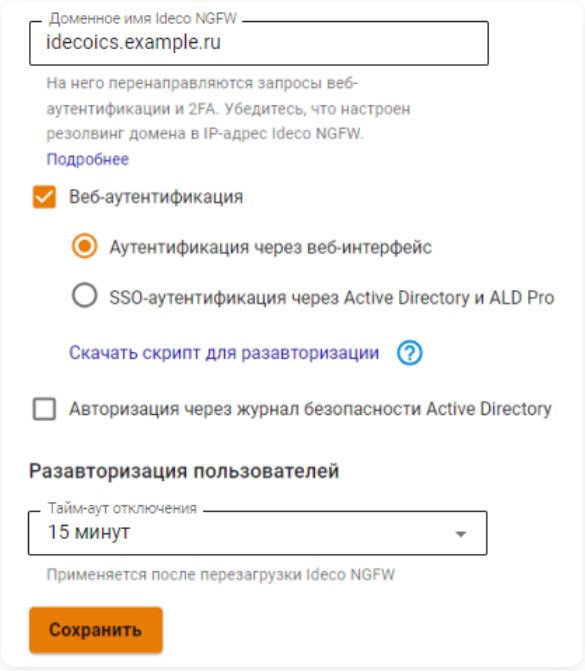
Рекомендуемые настройки для корректной работы веб-аутентификации:

- При входе на HTTPS-сайт пользователь должен подтвердить доверие к сертификату Ideco NGFW, либо сертификат должен быть добавлен в доверенные корневые центры сертификации на устройстве (например, через политики домена);
- Рекомендуется указывать в качестве DNS-сервера на компьютерах и устройствах локальной сети IP-адрес локального интерфейса Ideco NGFW.

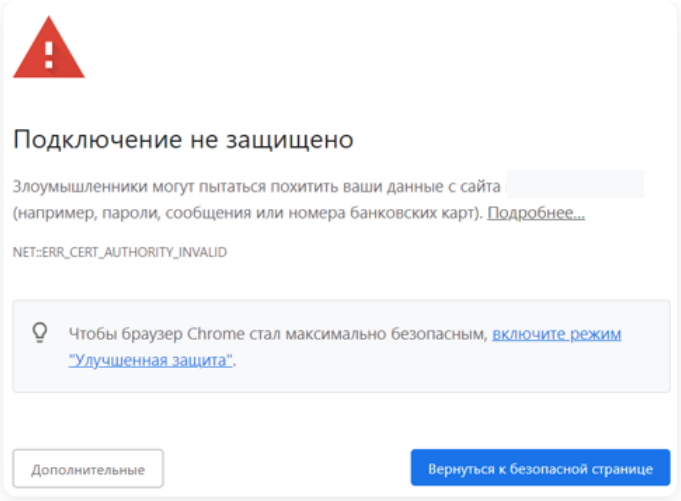
Аутентификация через веб-интерфейс

Чтобы настроить авторизацию через веб-интерфейс, выполните действия:

1. В разделе **Пользователи** → **Авторизация** выберите пункты **Веб-аутентификация** → **Аутентификация через веб-интерфейс**:



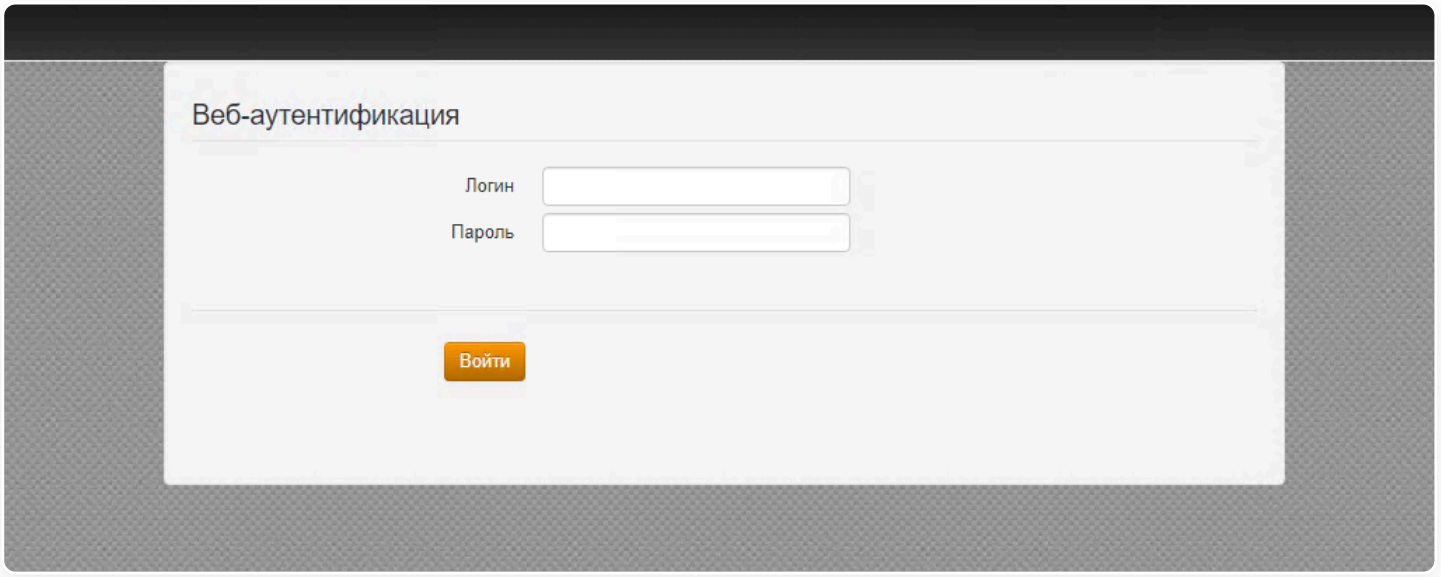
После заполнения поля **Имя домена** и сохранения настроек будет выдан Let's Encrypt сертификат. Пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



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

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

2. Откройте веб-браузер с устройства пользователя. Должно появиться окно авторизации, где необходимо ввести логин и пароль от созданной на Ideco NGFW 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**

IP и MAC авторизация

В Ideco NGFW можно создать правила авторизации по IP, MAC и IP+MAC.

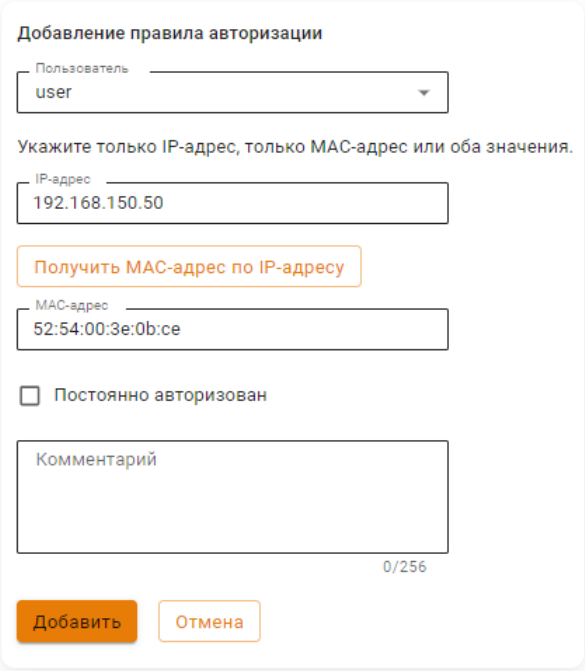
Правила **IP и MAC авторизации** создают аналогичную привязку в DHCP-сервере Ideco NGFW. Но если одни и те же IP- и MAC-адреса будут использоваться во включенных правилах DHCP-сервера, то правила DHCP-сервера будут выполняться в первую очередь.

Созданные в разделе **Авторизация → IP и MAC авторизация** правила отражаются в карточке пользователя.

Для настройки IP и MAC авторизации выполните действия:

1. В разделе **Авторизация → IP и MAC авторизация** нажмите **Добавить**.

2. Создать правило привязки **IP и MAC авторизации**:



При наличии большого количества правил привязки в таблице воспользуйтесь кнопкой **Фильтры**.

3. Если требуется обеспечить непрерывный доступ в интернет, установите флаг **Постоянно авторизован**. 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.

Статьи об авторизации пользователей только по IP- или MAC-адресу:

Авторизация по IP-адресу

Авторизация по MAC-адресу

Авторизация по IP-адресу

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 широковещательных доменах и требуют доступ в интернет.

Если устройством является маршрутизатор, в котором включен SNAT, при авторизации его внешнего IP на NGFW все пользователи за этим маршрутизатором получат доступ в интернет.

Пользователи, которые находятся за маршрутизатором в локальной сети NGFW, не могут авторизоваться по IP+MAC, так как маршрутизатор не обрабатывает трафик уровня L2.

Если настроена авторизация по IP-адресу, то этот IP не будет выдаваться DHCP.

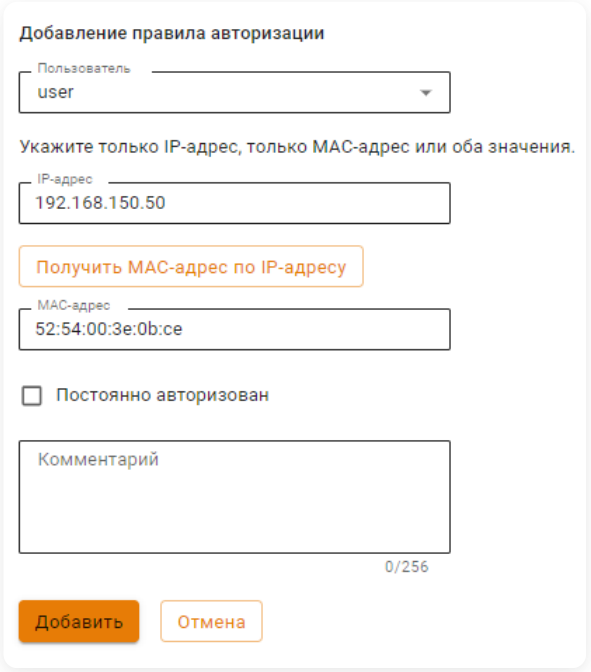
Настройка авторизации по IP

Для авторизации пользователя по IP-адресу выполните действия:

1. Создайте пользователя.

2. Перейдите в раздел **Пользователи** → **Учетные записи** → **Карточка пользователя** → **IP и MAC авторизация** или **Пользователи** → **Авторизация** → **IP и MAC авторизация**.

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 пользователя и IP Ideco NGFW в одной подсети.

Рекомендации по использованию авторизации по IP-адресу:

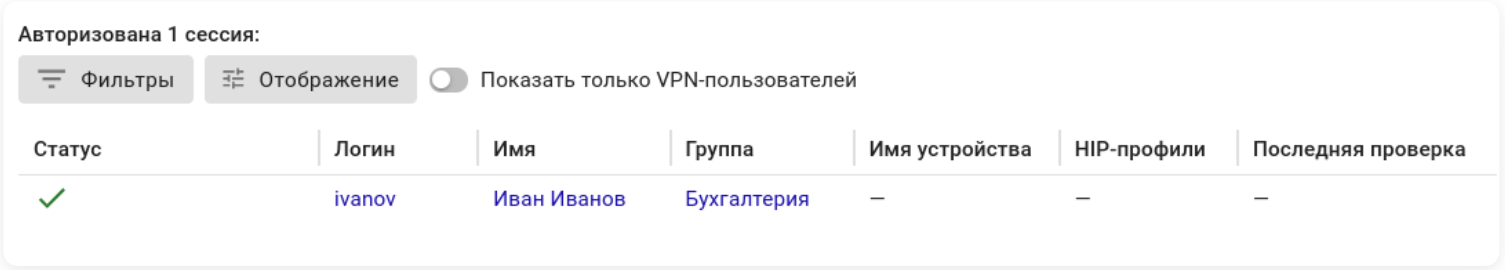
- Настройте для пользователя, которым является сетевое оборудование, **Постоянную авторизацию**. Это позволит NGFW создать сессию, а сетевому оборудованию не потребуется делать запрос в интернет;
- Настройте статический IP-адрес или DHCP с привязкой по IP-адресу. Это требуется, например, для ресурсов, опубликованных через DNAT;
- Воспользуйтесь поиском устройств для автоматического создания пользователей при попытке выхода в интернет. Подробнее о настройке читайте 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 NGFW 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

Этот тип авторизации подойдет для тех устройств, у которых время от времени меняется местоположение между локальными сетями внутри организации (например, рабочие ноутбуки сотрудников) или сетевых устройств, на которых не настроена привязка IP+MAC и выдается IP-адрес через DHCP.

Для авторизации пользователя на NGFW по MAC-адресу оба устройства должны находиться в одном широковещательном домене, а NGFW должен выступать шлюзом для устройств.

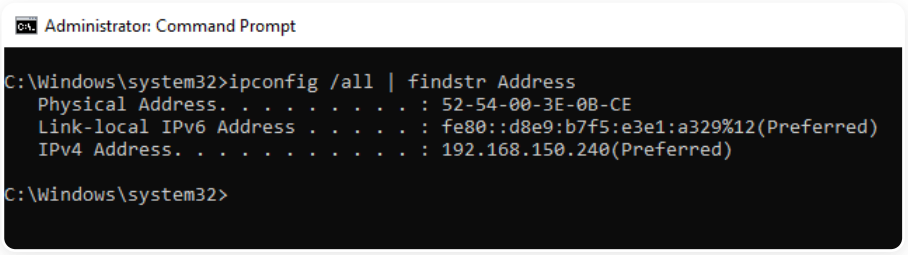
Пользователи, находящиеся за роутером в локальной сети NGFW, не могут авторизоваться по MAC-адресу, так как роутер разделяет широковещательные домены и не обрабатывает трафик уровня L2. Такие пользователи могут авторизоваться только по IP-адресу.

Для работы MAC-авторизации необходимо, чтобы NGFW и пользователь находились в одном L2-сегменте сети.

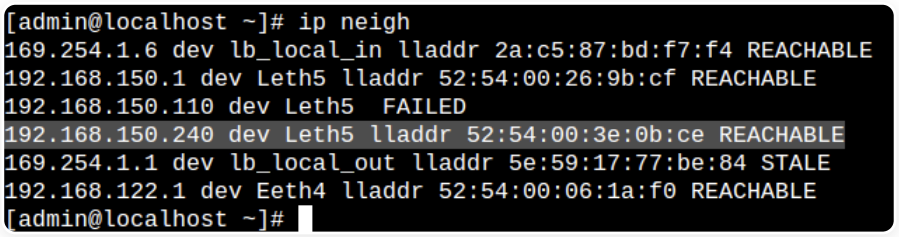
Настройка авторизации по MAC

Для авторизации пользователя по MAC-адресу выполните действия:

1. Узнайте MAC-адрес устройства. Для этого в командной строке Windows введите `ipconfig /all | findstr Address` или `ipconfig /all | findstr адрес` (для русскоязычной версии):



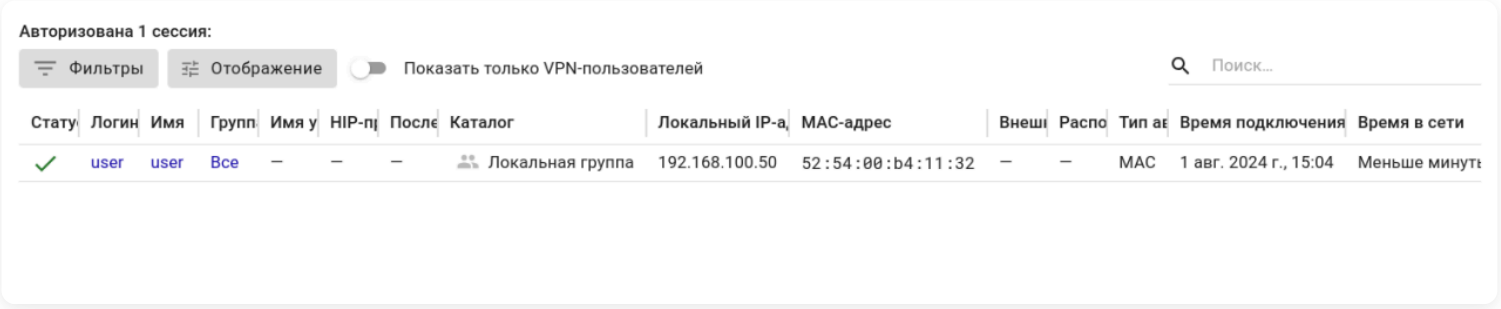
2. Удостоверьтесь, что устройство пользователя и NGFW находятся в одном широковещательном домене. Для этого в разделе **Управление сервером → Терминал** веб-интерфейса NGFW введите команду `ip neigh`:



Эта команда выводит ARP-таблицу NGFW. Наличие записи с MAC-адресом устройства и статусом REACHEBLE - маркер L2-доступности между NGFW и устройством пользователя.

3. Создайте правило-связку **Пользователь <--> MAC-адрес** в разделе **Пользователи → Авторизация → IP и MAC авторизация**.

Сессия с типом авторизации `MAC` отобразится в разделе **Мониторинг → Сессии пользователей**:



Для MAC-адресов невозможно настроить постоянную авторизацию, т. к. для создания авторизованной сессии необходим IP-адрес.

Рекомендуем использовать MAC-авторизацию в комбинации с DHCP-сервером.

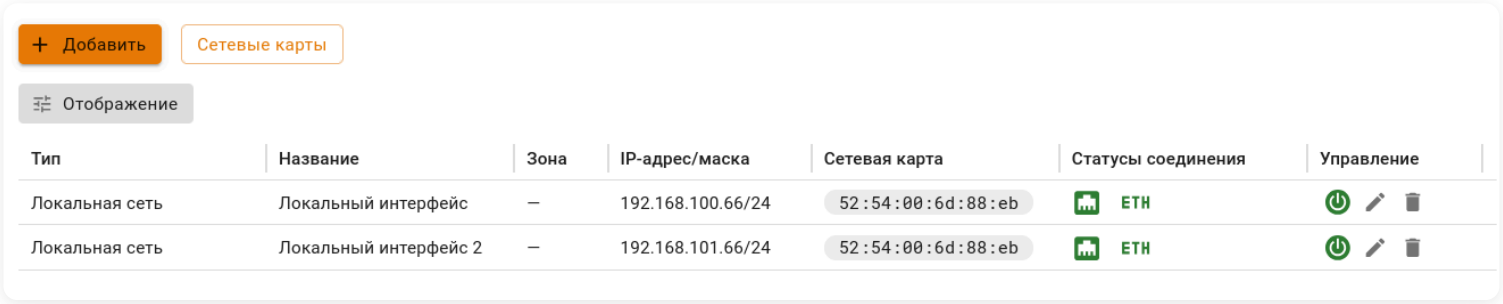
Поведение MAC-авторизации при перемещении устройства между локальными сетями

В организациях часто возникает ситуация, когда необходимо перемещаться между локальными сетями с ноутбуком и при этом всегда оставаться в сети. В таких случаях рекомендуем использовать авторизацию по MAC-адресу.

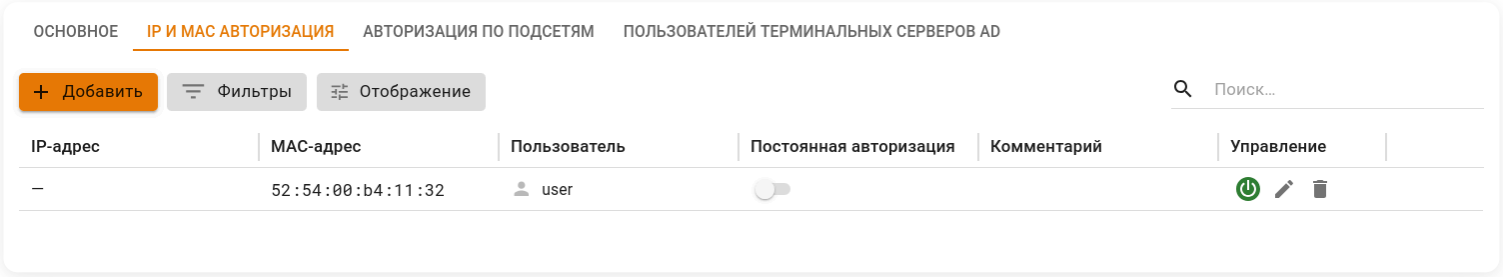
Для авторизации по MAC настройте DHCP-сервер (собственный или на NGFW). В раздаваемых реквизитах шлюзом должен выступать локальный интерфейс NGFW.

Пример. Пользователю `user` понадобилось переместиться с ноутбуком между локальными сетями:

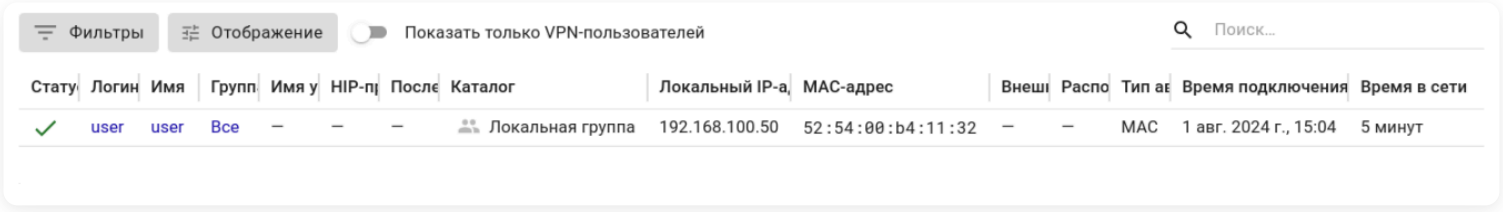
- На NGFW настроены локальные интерфейсы:



- 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. 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.

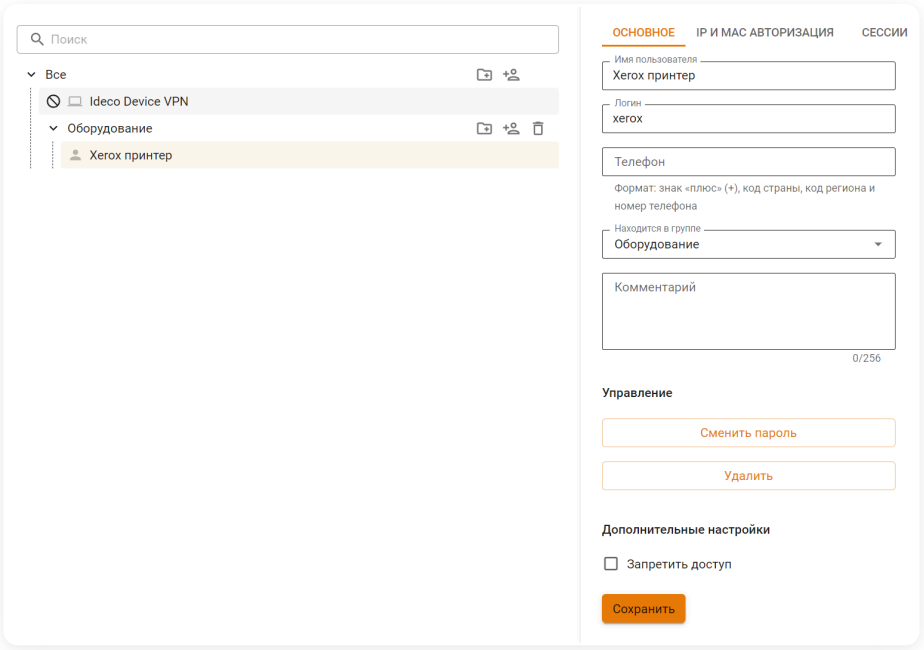
Сбросьте старые сетевые реквизиты от DHCP-сервера и получите новые с помощью команд:

- Windows - `ipconfig /release && ipconfig /renew`;
- Linux - `sudo dhclient -r <имя_интерфейса>`.

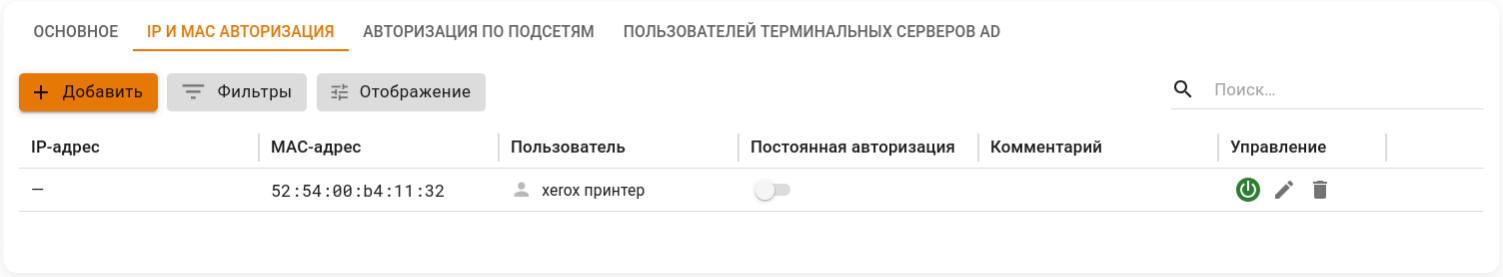
Настройка авторизации по MAC-адресу для сетевого принтера и других сетевых устройств

Сетевые устройства, которым необходим доступ в интернет, должны быть авторизованы на NGFW. Такие устройства можно назвать статическими, для них подойдет авторизация по MAC-адресу.

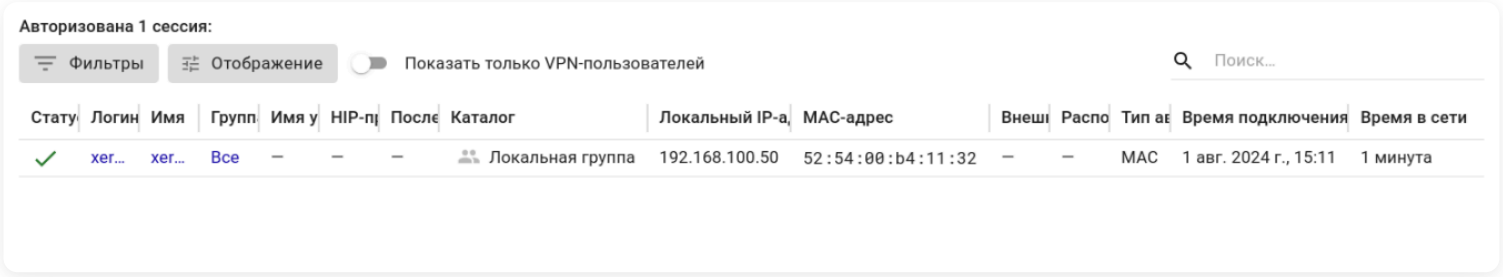
Чтобы авторизовать сетевой принтер, необходимо создать пользователя на NGFW вручную или через Обнаружение устройств:



В разделе **Пользователи** → **Авторизация** → **IP и MAC авторизация** 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 эту опцию отключать либо использовать другие типы авторизации (например, Веб-аутентификацию

Авторизация по подсетям

Чтобы не регистрировать каждое устройство как отдельного пользователя NGFW и не задавать для него факторы авторизации, создайте правило на вкладке **Пользователи** → **Авторизация** → **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.

Будьте внимательны при создании правил Авторизации по подсетям! Любое **пересечение сетей** при авторизации может привести к проблемам. Например:

- на вкладке **Авторизация по подсетям** для разных пользователей созданы правила с пересекающимися сетями;
- в разделе **Пользователи** → **Учетные записи** создан пользователь с IP-адресом из подсети в правилах **Авторизации по подсетям**;
- на вкладке **VPN-подключения** → **Правила выдачи IP-адресов** добавлена привязка к IP-адресам из подсети в правилах **Авторизации по подсетям**;
- на вкладке **Авторизация по подсетям** создано правило с подсетью, частично пересекающейся с диапазоном IP-адресов для выдачи в разделе **Сервисы** → **DHCP**.

Работа DHCP возможна в случае, если диапазон выдачи IP-адресов не превышает количество адресов в подсети, указанной в правиле **Авторизация по подсетям**.

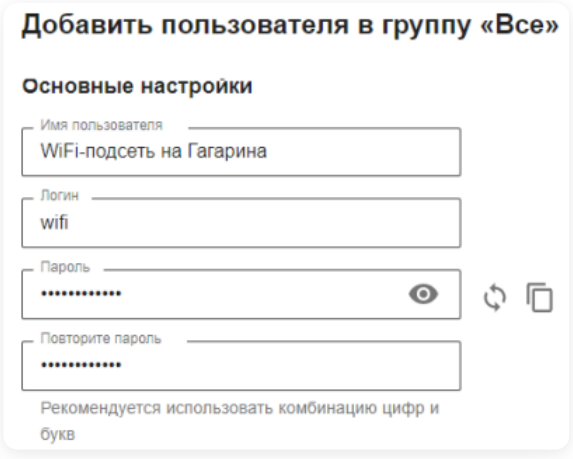
Пример использования

Есть Wi-Fi-подсеть 192.168.10.0/24, для устройств которой требуется авторизация.

Для создания правила авторизации выполните действия:

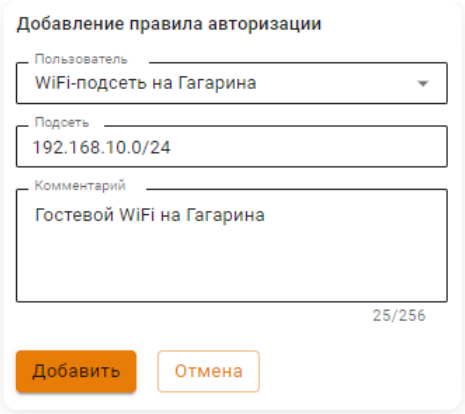
1. Перейдите в раздел **Пользователи** → **Учетные записи** и нажмите .

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



3. Перейдите на вкладку **Пользователи** → **Авторизация** → **Авторизация по подсетям** и нажмите **Добавить**.

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



- **Пользователь** - выберите созданного в п. 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.

Авторизация пользователей терминальных серверов

Особенности работы для пользователей терминальных серверов AD:

- Пользователи имеют один IP-адрес, поэтому правила **Файрвола** и **Контроля приложений**, примененные для одного пользователя, будут действовать на всех;
- **Контент-фильтр** распознает этих пользователей, поэтому его правила применяются для отдельных пользователей и групп;
- Сессии авторизации не создаются, так как пользователи терминальных серверов обращаются с одним IP-адресом;
- Работает только при прямых подключениях к прокси;
- В **Журнале веб-доступа** не отображаются события по терминальным пользователям.

Для авторизации пользователей терминальных серверов установите флаг **Авторизовать пользователей терминальных серверов** и укажите IP-адрес терминального сервера в одноименной строке. Отправляющие запросы с этих IP-адресов пользователи считаются пользователями терминальных серверов и авторизуются через SSO.

Обратите внимание, что при большом количестве пользователей на сервере терминалов может потребоваться увеличить количество одновременных сессий с одного адреса в дополнительных параметрах безопасности.

Возможна **раздельная авторизация пользователей** терминального сервера, работающего под управлением ОС Windows Server, с помощью авторизации через SSO. При этом сам сервер по IP авторизовывать не нужно.

Для раздельной авторизации пользователей терминального сервера:

- На сервере терминалов настройте **Remote Desktop IP Virtualization**.
- На сервере Ideco NGFW настройте авторизацию пользователей через SSO.

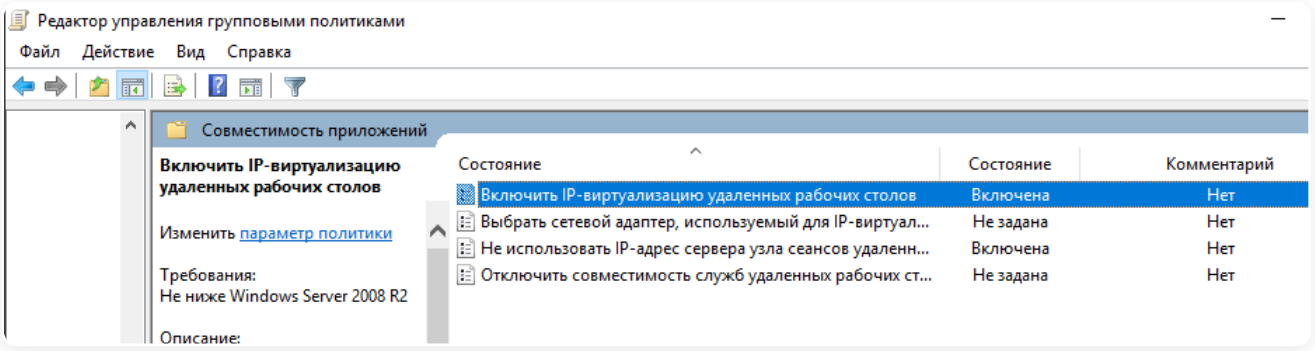
> Авторизация пользователей терминального сервера по логам контроллера домена AD пока не реализована.

Настройка Remote Desktop IP Virtualization на Windows Server 2012

Для работы функции Remote Desktop IP Virtualization на одном из Windows-серверов должна быть добавлена роль DHCP-сервера (с другими DHCP-серверами эта функция может работать некорректно) и выделена область IP-адресов для пользователей терминального сервера.

В **Редакторе управления групповыми политиками** перейдите по пути: **Computer Configation → Policies → Administrative Templates → Windows Components → Remote Desktop Service → Remote Desktop Session Host → Application Compatibility**.

Путь для русскоязычной версии: **Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Служба удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Совместимость приложений**. Включите опцию **Turn on Remote Desktop IP Virtualization (Включить IP-виртуализацию удаленных рабочих столов)** в групповой политике с параметром **Per Session (Для сеансов)**:



Рекомендуется включить опцию **Do not use Remote Desktop Session Host server IP address when virtual IP address is not available (Не использовать IP-адрес сервера узла сеансов удаленных рабочих столов, если виртуальный IP-адрес недоступен)**.

Командой `gpupdate /force` выполнить обновление всех политик.

Проверьте изменение настроек командой в PowerShell:

```
Get-WmiObject -Namespace root\cimv2\TerminalServices -query "select * from Win32_TSVirtualIP"
```

Значения:

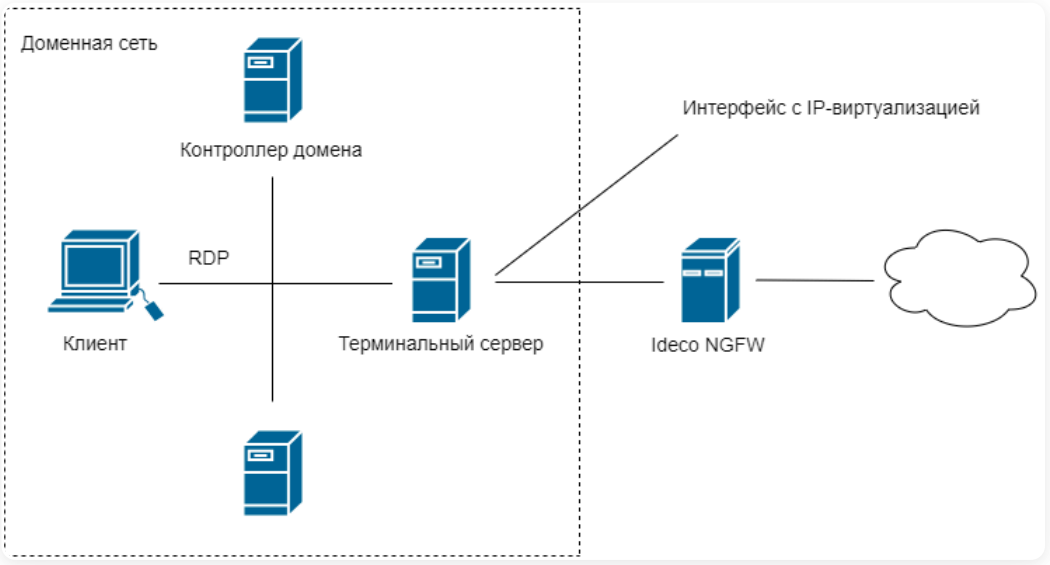
- `VirtualIPActive = 1` - вкл. виртуализация;

- `VirtualIPMode=0` - для сессии.

Настройка Remote Desktop IP Virtualization на Windows Server 2022

> Не подтверждено, что Remote Desktop IP Virtualization работает на Windows Server 2019. Рекомендуем обновить терминальный сервер до Windows Server 2022.

Условия



1. Windows Server 2022 с ролью контроллера домена;

2. Windows Server 2022 с ролью терминального сервера. Отдельный сервер опционален, можно добавить эту роль серверу с ролью контроллера домена;

3. Ideco NGFW, введен в домен опционально;

4. Клиентские Windows-машины, введенные в домен;

5. (опционально) Windows Server 2022 с ролью DHCP-сервера для динамической раздачи виртуальных IP-адресов. Конфликтует в ролью терминального сервера, поэтому DHCP-сервер и терминальный сервер должны быть разными машинами. DHCP-сервер используется на базе Windows Server. DHCP-сервер на Ideco NGFW, например, не подойдет.

Настройка

> Все настройки выполняются от имени администратора.

Установите все последние обновления Windows Server и перезагрузите серверы.

На сервере с ролью терминального сервера выполните следующие действия:

1. Отключите WinSock2. Переместите (рекомендуется) или удалите раздел реестра по указанному пути с помощью **Редактора реестра** (regedit):

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\AppId_Catalog\2C69D9F1

2. Включите компонент IPFilterBitmaps:

Добавление параметра через глобальную политику реестра с помощью Редактора реестра (regedit) (рекомендуется)

Путь: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

Ключ: IPFilterBitmaps

Тип: REG_DWORD

Значение: 1

Добавление параметра через групповую политику реестра с помощью Редактора реестра (regedit)

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAppSrv\VirtualIP

Ключ: IPFilterBitmaps

Тип: REG_DWORD

Значение: 1
3. Перезагрузите сервер.

4. Настройте IP-виртуализацию удаленных рабочих столов на сервере с ролью терминального сервера.

Далее описана настройка для режима **Для сеансов**, который выдает виртуальный IP-адрес каждой пользовательской сессии:

Через редактирование объекта WMI-инфраструктуры (глобальную политику реестра) в PowerShell (рекомендуется)

Значение для метода SelectNetworkAdapter - MAC-адрес сетевого интерфейса, который будет использоваться для IP-виртуализации. Выполните команду:

```
$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TSVirtualIP
$obj.SelectNetworkAdapter('52-54-00-00-90-01')
$obj.SetVirtualMode(0)
$obj.SetVirtualIPActive(1)
```

После выполнения команды убедитесь, что все параметры выставлены правильно, введя `$obj`.

Через групповую политику с помощью Редактора локальной групповой политики (gpedit.msc)

1. Перейдите в раздел **Политика Локальный компьютер → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Совместимость приложений**.

Путь для англоязычной версии: **Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Application Compatibility**.

2. Включите параметр политики **Включить IP-виртуализацию удаленных рабочих столов** с параметром **Для сеансов**.

Англоязычная версия: **Turn on Remote Desktop IP Virtualization** с параметром **Per Session**.

3. Включите параметр политики **Выбрать сетевой адаптер, используемый для IP-виртуализации удаленных рабочих столов** в параметр **IP-адрес с маской сетевого интерфейса, который будет использоваться для IP-виртуализации** (например, 192.168.100.200/24).

Англоязычная версия: **Select the network adapter to be used for Remote Desktop IP Virtualization** в параметр **IP adress and network mask corresponding to the network adapter to be used for Remote Desktop IP Virtualization**.

4. (опционально) Включите параметр политики **Не использовать IP-адрес сервера узла сеансов рабочих столов, если IP-адрес недоступен** (**Do not use Remote Desktop Session Host server IP address when virtual IP address is not available**).

5. Повторно перезагрузите сервер.

Настройте выдачу виртуальных IP-адресов:

{% cut "Для статической выдачи виртуальных IP-адресов на сервере с ролью терминального сервера" %}{# dlya-staticheskoj-vydachi-virtualnyh-ip-adresov-na-servere-s-rolyu-terminalnogo-servera}

Включите компонент IPPool. Через групповую политику реестра с помощью **Редактора реестра** (regedit) добавьте параметр:

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAPPSrv\VirtualIP

Ключ: IPPool

Тип: REG_SZ (строковый параметр)

Значение: `%SystemRoot%\system32\TSVIPool.dll`

Настройте статический диапазон IP-адресов:

1. Создайте новый раздел IPPool по пути HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAPPSrv\VirtualIP через групповую политику реестра с помощью **Редактора реестра** (regedit).

2. Добавьте в новый раздел параметры типа REG_SZ (строковый параметр):

- Ключ Start, значение - начало диапазона IP-адресов (например, 192.168.100.200);
- Ключ End, значение - конец диапазона IP-адресов (например, 192.168.100.210);
- Ключ SubnetMask, значение - маска подсети (например, 255.255.255.0).

3. Перезагрузите сервер с ролью терминального сервера.

Для динамической выдачи виртуальных IP-адресов на сервере с ролью DHCP-сервера

Выдайте DHCP-серверу необходимые привилегии через групповую политику реестра с помощью **Редактора реестра»** (regedit):

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp

Ключ: RequiredPrivileges

Тип: REG_MULTI_SZ (многострочный параметр)

Значение:

```
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
```

Перезагрузите сервер с ролью DHCP-сервера.
В случае успешной настройки на интерфейс, выбранный для IP-виртуализации, при подключении клиентов будут выдаваться виртуальные IP-адреса, которые исходящие запросы будут использовать в качестве источника.

```
Локальный IPv6-адрес канала . . . : fe80::ac9e:64f3:5cba:891b%14
IPv4-адрес. . . . . . . . . . . . : 192.168.100.90(Основной)
Маска подсети . . . . . . . . . . : 255.255.255.0
IPv4-адрес. . . . . . . . . . . . : 192.168.100.161(Устаревший)
Маска подсети . . . . . . . . . . : 255.255.255.0
```

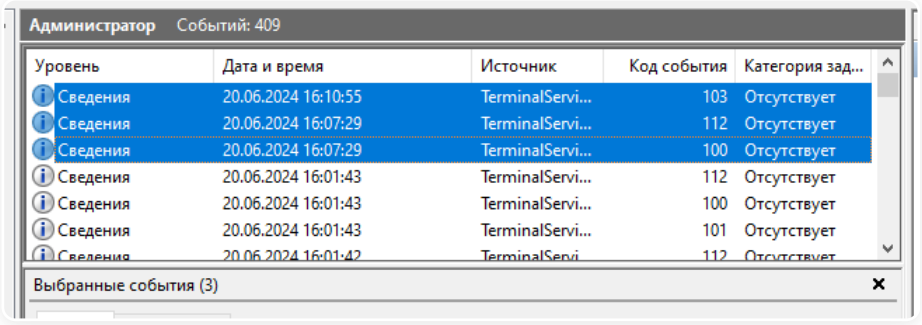
Диагностика

Виртуальные IP-адреса не выдаются

На сервере с ролью терминального сервера проверьте работоспособность службы IP-виртуализации. Для этого перейдите в раздел **Просмотр событий (локальный компьютер) → Журналы приложений и служб → Microsoft → Windows → Terminal Services-TSAppSrv-TSVIP → Администратор**.

Путь для англоязычной версии: **Event Viewer (Local) → Applications and Services Logs → Misrosoft → Windows → Terminal Services-TSAppSrv-TSVIP → Administrator**.

Успешно запущенная служба произведет события 100 и 112 после запуска и 103, 104 при подключении/отключении клиента:



В объекте WMI-инфраструктуры (независимо от вида настройки самой IP-виртуализации) в PowerShell выполните:

```
$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TSVirtualIP
$obj
```

Убедитесь, что параметр `IP.VirtualIPActive` = 1.

```
__PATH                          : \\WIN-RHQ28K71VT1\Root\CIMV2\TerminalServices:Win32_TSVirtual
                                  IP.VirtualIPActive=1
```

Если что-то отличается, убедитесь, что все инструкции по настройке выполнены правильно, а DHCP-сервер работает исправно. При необходимости выполните настройку заново рекомендуемыми способами.

Подключения используют основной IP-адрес терминального сервера

Использовать IP-виртуализацию будут только Windows-приложения, работающие на WinSock, то есть приложения, использующие протоколы TCP или UDP. ICMP-приложения вроде `ping` не будут использовать IP-виртуализацию.

Подключения будут использовать основной IP-адрес терминального сервера также в случае, когда запрашиваемый адрес недоступен (например, `Destination Unreachable`).

IP-виртуализация работает только для пользователей, подключенных к терминальному серверу через службу mstsc (**Подключение к удаленному рабочему столу**).

Двухфакторная аутентификация

Название службы раздела **Двухфакторная аутентификация**: `ideco-web-authd`.

Список служб для других разделов доступен по ссылке.

Двухфакторная аутентификация позволяет аутентифицировать пользователей только внешних сетей (VPN) с использованием второго фактора.

В Ideco NGFW реализовано три 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.

Для входа в личный кабинет Ideco NGFW с использованием **Мультифактора** необходим доступ в интернет.

Двухфакторная аутентификация для пользователей **RADIUS-сервера** работает только при авторизации через **Ideco Client**. Для этого нужно настроить двухфакторную аутентификацию на **RADIUS-сервере**, о настройке Ideco NGFW - в статье.

Настройки Ideco NGFW с разными типами аутентификации

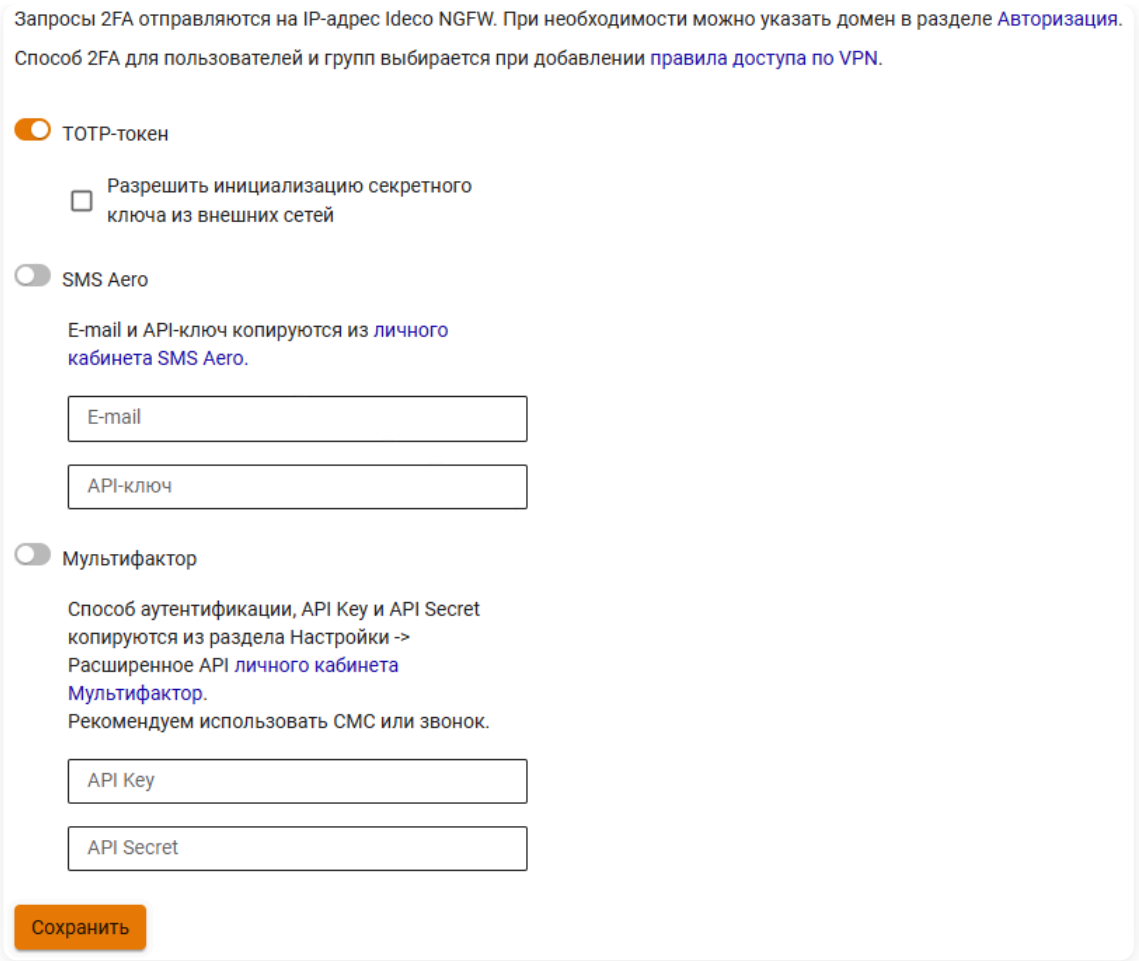
Для работы двухфакторной аутентификации выполните действия:

1. Укажите домен Ideco NGFW, чтобы на сервер перенаправлялись запросы двухфакторной аутентификации:

- Перейдите в раздел **Пользователи** → **Авторизация**.
- Включите веб-аутентификацию.
- Введите домен в поле **Доменное имя Ideco NGFW**.

2. Настройте VPN-подключение в разделе **Пользователи** → **VPN-подключения** → **Основное**, воспользовавшись инструкцией.

3. Перейдите в раздел **Пользователи** → **Двухфакторная аутентификация**. Включите необходимые типы аутентификации и заполните соответствующие поля:



TOTP-токен

Опция **Разрешить инициализацию секретного ключа из внешних сетей** разрешит генерацию QR-кода в личном кабинете пользователя из внешней сети.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW с использованием TOTP-токена смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

SMS Aero

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. Нажмите **Сохранить**.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW с использованием SMS Aero смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Мультифактор

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 его, отсканировав QR-код.

1. Заполните **API Key** и **API Secret**. Для этого скопируйте значение полей в личном кабинете пользователя Multifactor в разделе **Настройки** → **Расширенное API** → **Включить API**.

2. Нажмите **Сохранить**.

Для корректной работы двухфакторной аутентификации через Мультифактор необходимо обеспечить доступ к следующим подсетям:

- 37.220.160.0/21
- 46.235.184.0/21
- 93.93.88.0/21
- 78.41.104.0/21
- 185.17.168.0/22
- 212.193.144.0/20
- 195.208.30.60/30
- 195.209.64.0/21
- 195.209.80.0/20
- 195.208.64.0/20
- 195.209.75.0/25
- 195.209.74.0/24

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**.

Видеоинструкцию по настройке двухфакторной аутентификации Ideco NGFW с использованием Мультифактора смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

4. Разрешите доступ по VPN нужным группам пользователей в разделе **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

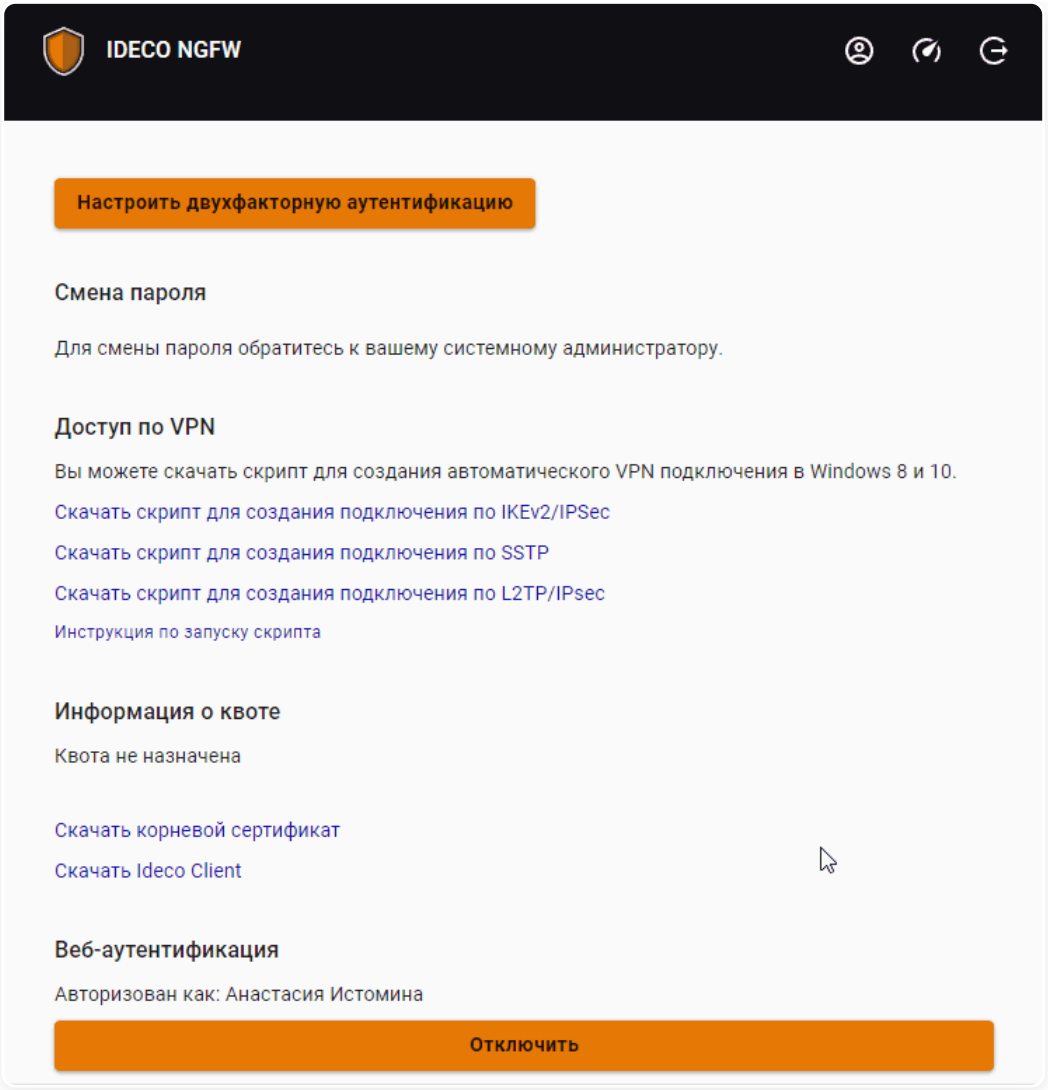
Для настройки двухфакторной аутентификации на устройстве пользователя воспользуйтесь инструкциями:

TOTP-токен

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Войдите в личный кабинет NGFW, указав логин и пароль пользователя.

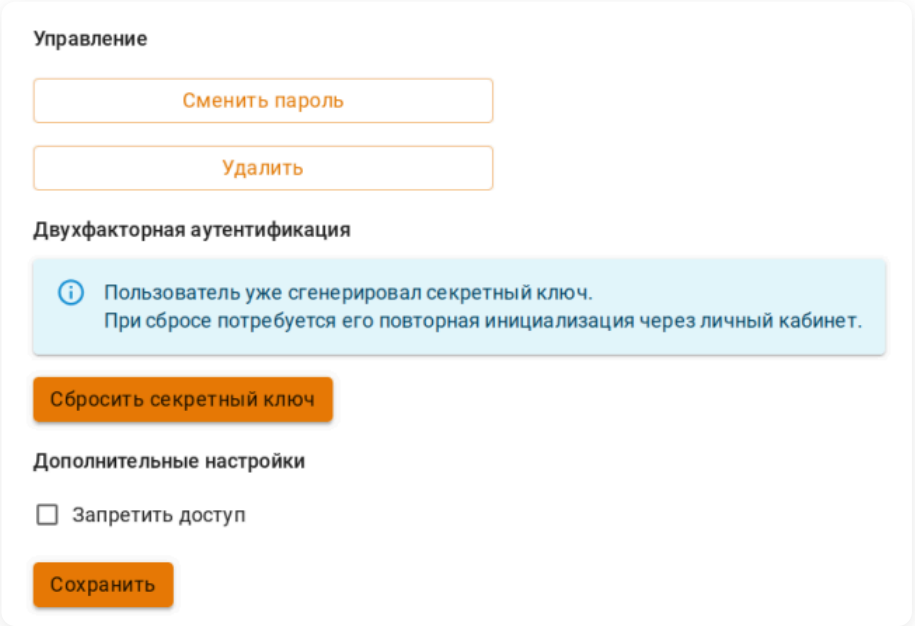
3. Нажмите кнопку **Настроить двухфакторную аутентификацию** и выберите **Сгенерировать QR-код**:



4. Войдите в приложение для аутентификации (Яндекс ID, Google Authenticator или Microsoft Authenticator и т.п.), отсканируйте 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.

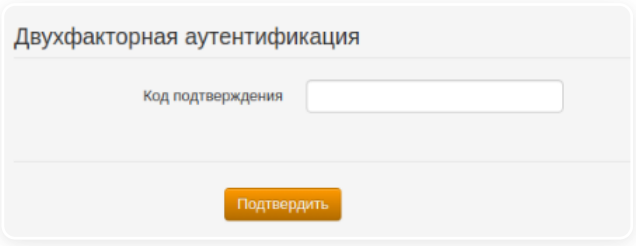
Если вернуться в личный кабинет, не отсканировав QR-код, то повторно он появится только после сброса секретного ключа в карточке пользователя.

Чтобы сбросить секретный ключ, перейдите в раздел **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 вы получили в приложении:



Особенности использования TOTP-токена:

- Для корректной работы необходимо, чтобы время на Ideco NGFW и устройстве пользователя было синхронизировано с точностью до минуты.
- Если секретный ключ был сброшен во время аутентификации пользователя и он не смог ее пройти, 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:

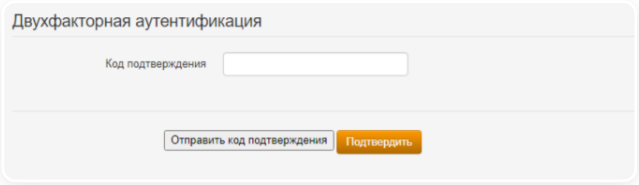
- Откройте параметры и перейдите в раздел **Сеть и Интернет** → **VPN** → **Настройка параметров адаптера**.
- Нажмите правой кнопкой мыши по созданному подключению и выберите **Свойства**.
- Перейдите на вкладку **Сеть**.
- Нажмите на **IP версии 4 (TCP/IPv4)** → **Свойства** → **Дополнительно**.
- Снимите флаг с пункта **Использовать основной шлюз в удаленной сети**.
- Нажмите **ОК**.

Для Ubuntu:

- Перейдите в раздел **Настройки** → **Сеть**.
- Откройте настройки VPN-подключения.
- Перейдите на вкладку **IPv4**.
- Установите флаг в пункте **Использовать это подключение для ресурсов этой сети**.

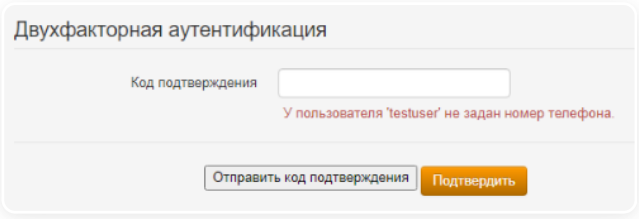
3. Включите созданное VPN-подключение.

4. Перейдете в браузер, откроется страница аутентификации:

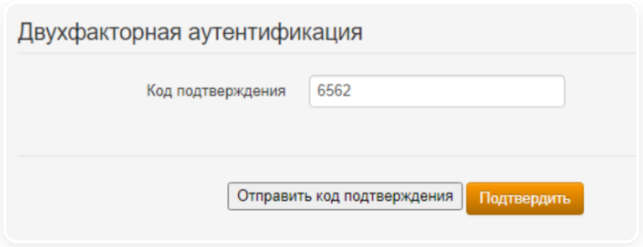


5. Нажмите **Отправить код подтверждения**. На номер телефона, указанный в учетной записи, придет SMS с кодом:

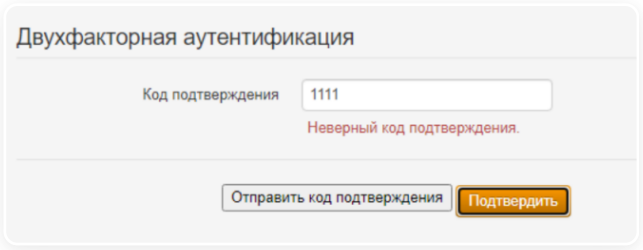
- Если номер телефона в карточке пользователя отсутствует, то на странице аутентификации появится предупреждение:



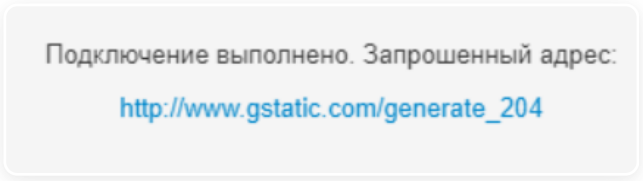
- Если номер телефона сохранен, то на указанный номер телефона поступит SMS. Введите код из SMS и нажмите **Подтвердить**:



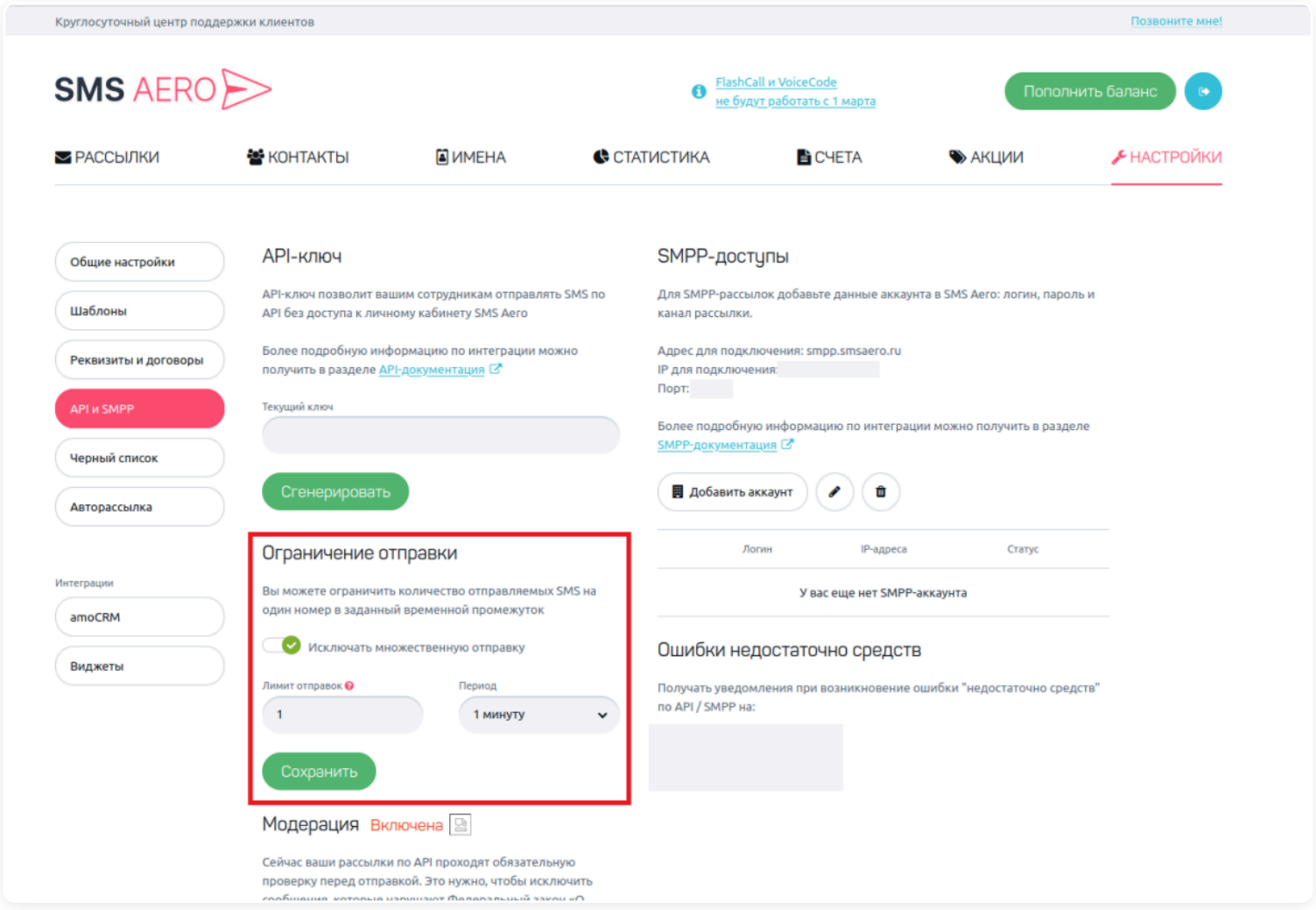
- Если код введен неверно, то появится соответствующее предупреждение:



- 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:

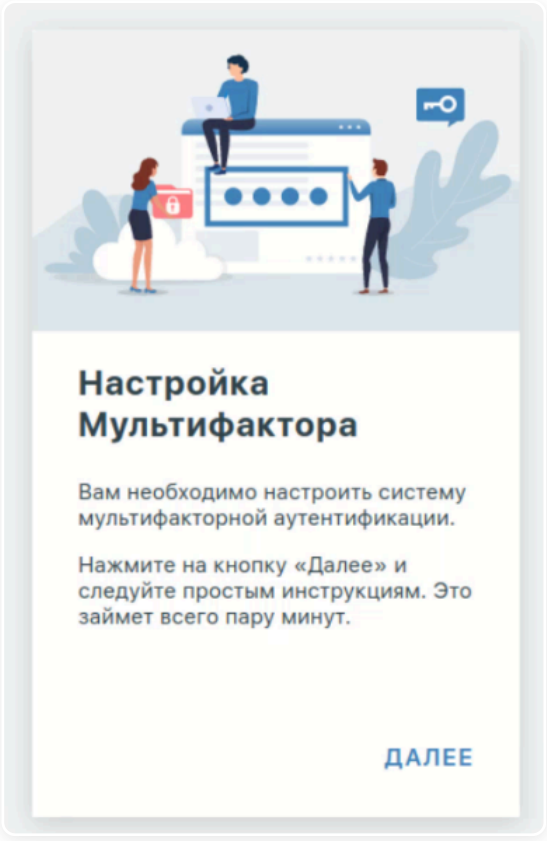


Мультифактор

1. Настройте VPN-подключение на устройстве пользователя, воспользовавшись инструкцией.

2. Включите созданное VPN-подключение.

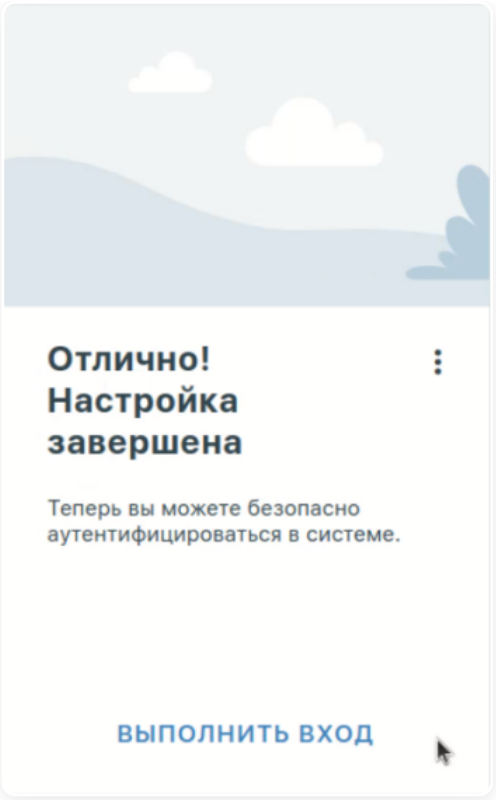
3. При переходе в браузер откроется страница аутентификации:



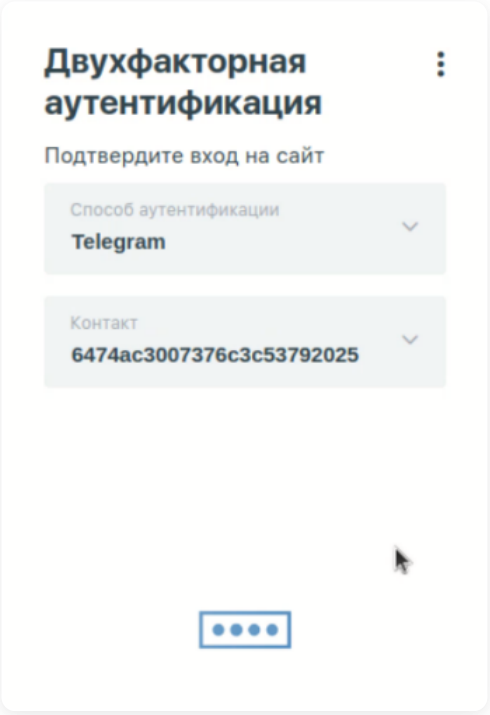
4. После нажатия **Далее** появится страница с предложением установить приложение на устройство пользователя. Если приложение установлено, нажмите **Далее**.

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.

VPN-подключения

Название службы раздела **VPN-подключения**: `ideco-accel-l2tp`; `ideco-accel-pptp`; `ideco-accel-sstp`; `ideco-vpn-servers-backend`; `ideco-vpn-authd`; `ideco-vpn-dhcp-backend`.

Список служб для других разделов доступен по ссылке.

Для получения доступа к локальной сети компании необходимо настроить VPN-сервер и подключиться через него. Можно использовать VPN-клиент, который уже есть в операционной системе, или установить отдельный.

В Ideco NGFW нет разделения локальных интерфейсов на VPN-интерфейсы и Ethernet, поскольку Ideco NGFW не имеет локальных VPN-интерфейсов.

Настройка VPN-сервера происходит в несколько этапов:

- Настройка протоколов, маршрутов и адресации.
- Настройка политик доступа из внешних сетей.
- Настройка двухфакторной аутентификации (опционально).

Поддерживаемые протоколы

Ideco NGFW поддерживает четыре протокола туннельных соединений:

- 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.
- PPTP - не рекомендуется. Этот способ подключения **крайне небезопасен** и оставлен исключительно для совместимости со старыми решениями.

Предварительные требования

Чтобы VPN-подключение работало на устройствах пользователей, необходимо загрузить корневой сертификат:

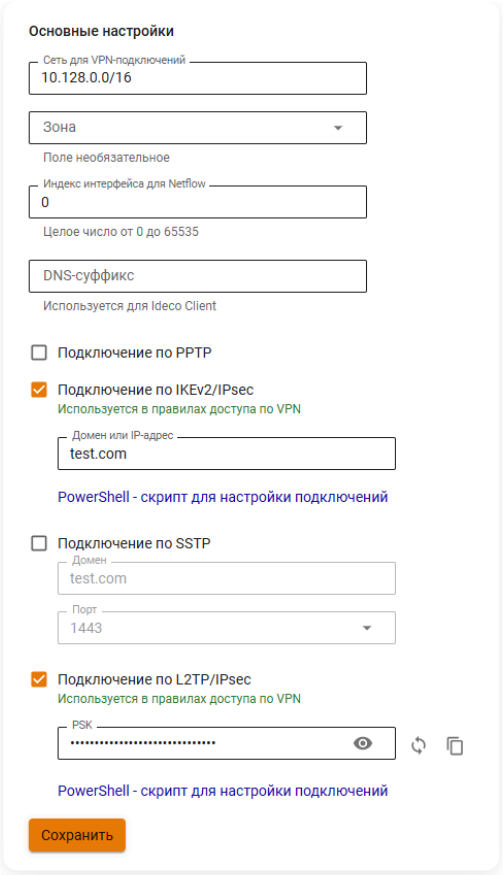
- Корневые сертификаты Ideco NGFW действительны в течение 10 лет.
- Если используется сертификат Let's Encrypt, обновление будет происходить автоматически.

Настройка VPN-подключения

Для настройки VPN-подключения перейдите в **Пользователи** → **VPN-подключения**.

Основное

На вкладке настраиваются протоколы, маршруты и адресация VPN-подключений. Для настройки заполните поля:



Расшифровка полей

- **Сеть для VPN-подключений** - укажите подсеть, в рамках которой будут динамически назначаться IP-адреса. 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. Подробнее об объекте **Зона** в статье.

Если требуется настроить VPN-подключение к Loopback-интерфейсу, оставьте поле **Зона** пустым.

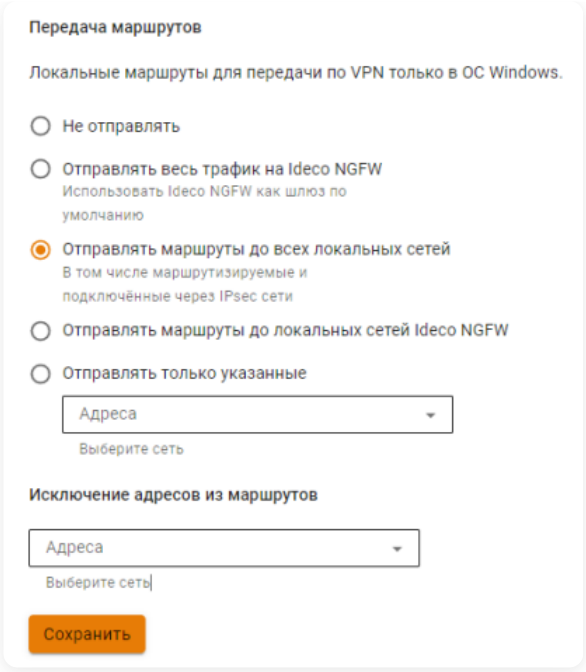
- **DNS-суффикс** - укажите DNS-суффикс, если для подключения по VPN используется Ideco Client.
- Выберите, какой протокол подключения будет использоваться.

Начиная с версии 16.0, 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.

В блоке **Передача маршрутов** укажите, как будут передаваться маршруты:



Маршруты, переданные Ideco NGFW для VPN-клиента, имеют меньшую метрику (т. е. высокий приоритет)

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.

Расшифровка полей

- **Не отправлять** - никакие маршруты не передаются клиенту, никакой трафик не будет проходить через NGFW.
- **Отправлять весь трафик на Ideco NGFW** - передается маршрут 0.0.0.0/0, весь трафик направляется через NGFW.
- **Отправлять маршруты до всех локальных сетей** - передаются маршруты до всех локальных сетей NGFW, в том числе подключенных через IPsec и маршрутизируемых, кроме маршрутов: **OSPF**, **BGP**, и **Маршрутизации внешних сетей**.
- **Отправлять маршруты до локальных сетей Ideco NGFW** - передаются только маршруты до локальных сетей NGFW, без учета IPsec и маршрутизируемых.
- **Отправлять только указанные** - выберите сети, до которых будут передаваться маршруты.

Если маршруты VPN-клиентов пересекаются с маршрутами, передаваемыми Ideco NGFW, то выберите **Не отправлять** или **Отправлять только указанные**.

Если при подключении по VPN (SSTP, IKEv2, PPTP, L2TP) не удается получить маршруты до сетей Ideco NGFW, то это связано с тем, что 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-server**.

Если пакет DHCP превышает 576 байт, то он может быть проигнорирован клиентом DHCP и применение маршрутов не произойдет (зависит от реализации клиента).

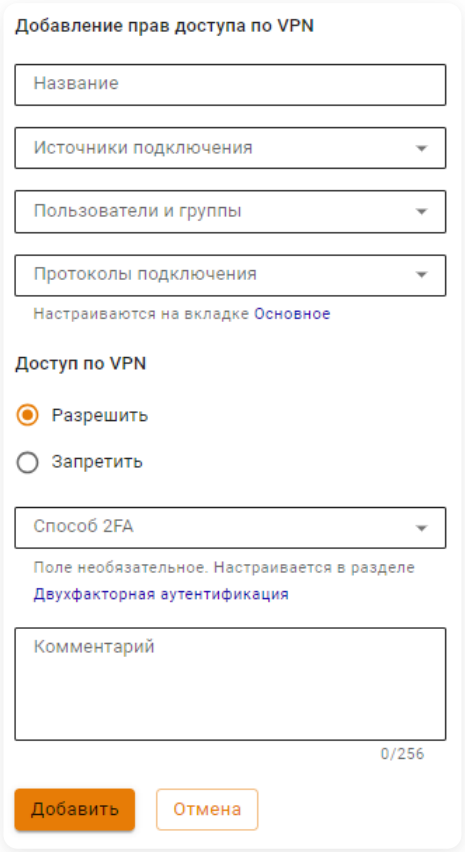
Доступ по VPN

На вкладке настраиваются правила доступа для пользователей и групп на внешние интерфейсы NGFW.

При совпадении условий (**Источник подключения**, **Пользователи и группы**, **Протокол подключения**) выполняется действие, выбранное при создании правил. Созданные правила применяются сверху вниз.

В правилах можно использовать как группы пользователей Ideco NGFW, так и группы безопасности AD. Для добавления группы безопасности AD для VPN не требуется импорт в дерево пользователей. Введите Ideco NGFW в домен и при создании правила **Доступ по VPN** в поле **Пользователи и группы** выберите необходимую группу безопасности.

Для настройки правил доступа, перейдите на вкладку **Пользователи** → **VPN-подключения** → **Доступ по VPN** и нажмите **Добавить**.



Расшифровка полей

- **Название** - укажите название правила.
- **Источники подключения** - выберите, откуда будет производиться подключение по VPN (IP-адреса, подсети, страны).
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Протоколы подключения** - выберите протокол (настраивается на вкладке **Основное**).
- **Доступ по VPN** - разрешите или запретите доступ по созданному правилу.
- **Способ 2FA** - выберите способ двухфакторной аутентификации.
- **Комментарий** - добавьте комментарий (опционально).

Для разных групп пользователей возможно указать разные типы двухфакторной аутентификации. Для настройки двухфакторной аутентификации воспользуйтесь статьей.

Правила выдачи IP-адресов

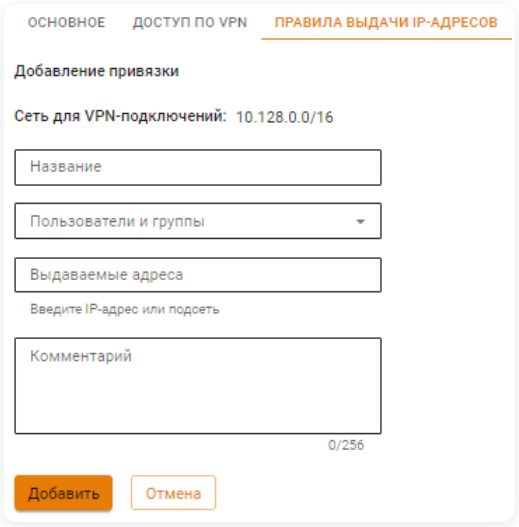
На вкладке можно создать правила для выдачи IP-адресов пользователям, подключающимся по VPN.

NGFW 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 и он уже используется в текущей сессии, то указанный в правиле пользователь не сможет установить второе VPN-подключение - оно 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 перейдите на вкладку **Пользователи → VPN-подключения → Правила выдачи IP-адресов** и нажмите **Добавить**.



Расшифровка полей

- **Название** - укажите название правила.
- **Пользователи и группы** - выберите, для каких пользователей будет применяться правило.
- **Выдаваемые адреса** - укажите фиксированный IP-адрес или подсеть, которые будут выдаваться пользователям.
- **Комментарий** - укажите комментарий к правилу (опционально).

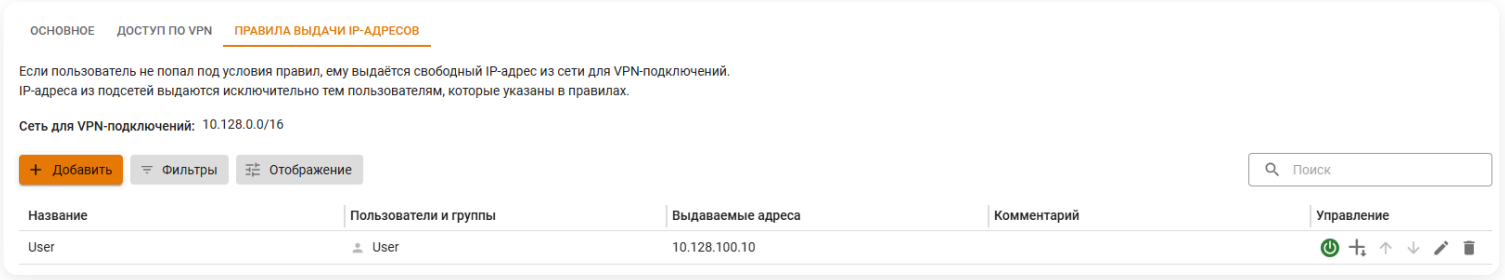
При наличии большого количества правил выдачи IP-адресов в таблице воспользуйтесь кнопкой **Фильтры**.

Чтобы отключить правило, нажмите на в столбце управления. Чтобы удалить правило, нажмите .

Статическая привязка IP-адресов

IP-адрес пользователю назначается автоматически из пула адресов для VPN, настраиваемого в разделе **Пользователи → VPN-подключения** (например 10.128.0.0/16).

Чтобы настроить **статическую** привязку адресов, выдаваемых по VPN определенным пользователям, нужно перейти в раздел **Пользователи → VPN-подключения → Правила выдачи IP-адресов**, нажать **Добавить** и указать нужного пользователя и IP-адрес. Пример настройки фиксированного IP-адреса VPN представлен ниже:



Полезные ссылки

- Инструкции по созданию VPN-подключений.

Подключение по PPTP

Не используйте этот тип подключения, он крайне небезопасен, оставлен исключительно для совместимости со старыми решениями. Используйте IKEv2/IPsec.

Подключение по протоколу PPTP предполагает авторизацию по защищенному сетевому туннелю между сетевым устройством пользователя и интернет-шлюзом Ideco NGFW.

Для аутентификации пользователя применяется связка логин/пароль пользователя Ideco NGFW или пользователя из Active Directory.

Для авторизации по протоколу PPTP необходимо назначить IP-адрес сетевому устройству, а также настроить на нем подключение по протоколу PPTP с указанием IP-адреса интернет-шлюза Ideco NGFW в качестве адреса PPTP-сервера.

При успешной аутентификации и установлении PPTP-туннеля сетевому устройству будет автоматически назначен дополнительный IP-адрес для получения доступа к ресурсам интернета. Использование авторизации по PPTP никак не отражается на возможности доступа сетевого устройства к ресурсам локальной сети.

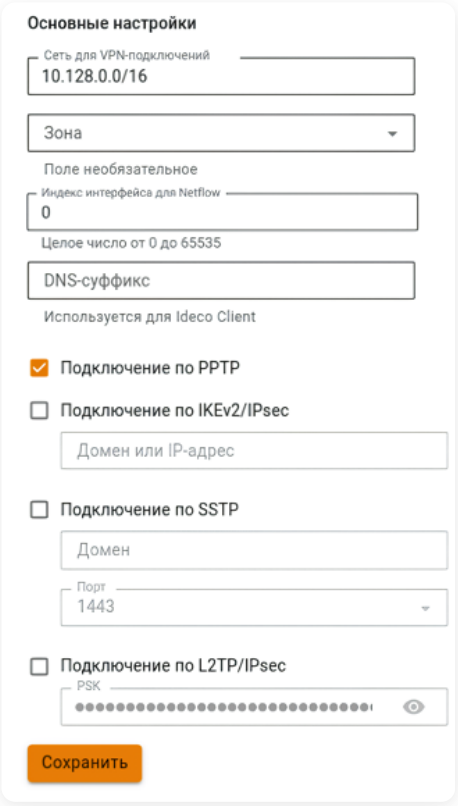
Не рекомендуем использовать для VPN-подключений кириллические логины.

Настройка Ideco NGFW

Основные настройки

Для настройки авторизации по протоколу PPTP выполните действия:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение по PPTP**.

3. В поле **Индекс интерфейса для Netflow** введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

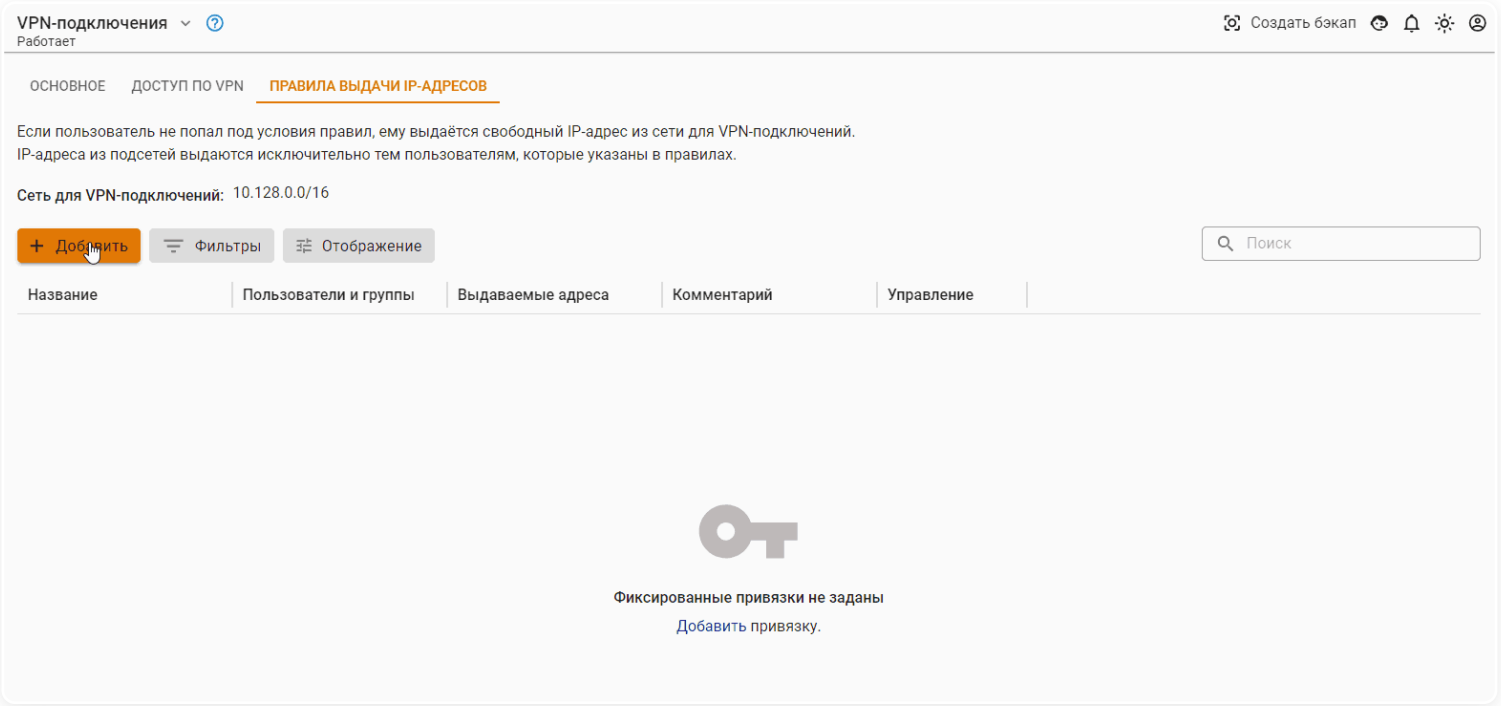
4. Нажмите **Сохранить**.

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).

Чтобы настроить **статическую** привязку адресов, выдаваемых по VPN определенным пользователям:

1. Перейдите в раздел **Пользователи → VPN-подключения → Правила выдачи IP-адресов**:



2. Нажмите **Добавить** и укажите название сети, нужного пользователя и IP-адрес.

3. Нажмите **Добавить**, чтобы сохранить изменения:

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи → VPN-подключения → Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключение.

Возможные неполадки

- Провайдер блокирует GRE-протокол, используемый в PPTP-соединении, что приводит к **ошибке 619** при подключении к внешнему адресу IdecoNGFW. Определить сторону проблемы можно, подключаясь с разных мест и от разных провайдеров. Если из некоторых мест подключение удается, значит, проблема на стороне клиента. Определив провайдера, нужно попытаться решить проблему с ним либо использовать IPsec-IKEv2 или SSTP;
- Заблокирован порт 1723 TCP. Проверить доступность можно с помощью стандартных утилит, таких как telnet. Если соединения нет, то туннель не может быть установлен;
- Неправильно указаны логин или пароль пользователя. Если это происходит, то часто при повторном соединении предлагается указать домен. Рекомендуется использовать для паролей латинские символы и цифры. При ошибке ввода пароля более 6 раз IP-адрес пользователя блокируется службой защиты от подбора паролей;
- При подключении через клиента ОС Windows убедитесь, что в настройках подключения включена опция **Использовать основной шлюз в удаленной сети** в разделе **Свойства подключения VPN → Вкладка Сеть → Свойства опции "Протокол интернета версии 4 (TCP/IPv4)" → Дополнительно**. Если маршрутизировать все пакеты в этот интерфейс не обязательно, то маршрут надо писать вручную;
- При возникновении ошибки **Подключение было закрыто удаленным компьютером** необходимо включить поддержку MPPE 128-bit (в Windows эта опция включена по умолчанию) и среди протоколов аутентификации отметить только MSCHAPV2.

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.

Подключение по IKEv2/IPsec

Видеоинструкцию смотрите по ссылкам:

- Youtube
- docs.ideco.ru

IKEv2/IPsec - протокол, который используется для создания защищенного соединения между двумя устройствами в сети.

Данный протокол VPN является предпочтительным и рекомендованным для всех сценариев использования.

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 или пользователя из Active Directory.

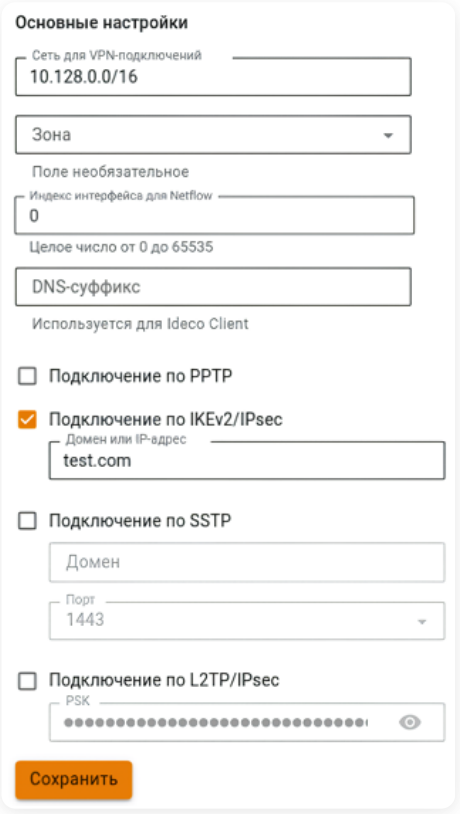
Не применяйте Wildcard-сертификаты для IKEv2/IPsec. Эти сертификаты не поддерживаются IPsec-клиентами из-за ограничений в проверке доменных имен.

Настройка Ideco NGFW

Не рекомендуем использовать для VPN-подключений кириллические логины и пароли, а так же указывать в качестве логина IP-адрес.

Основные настройки

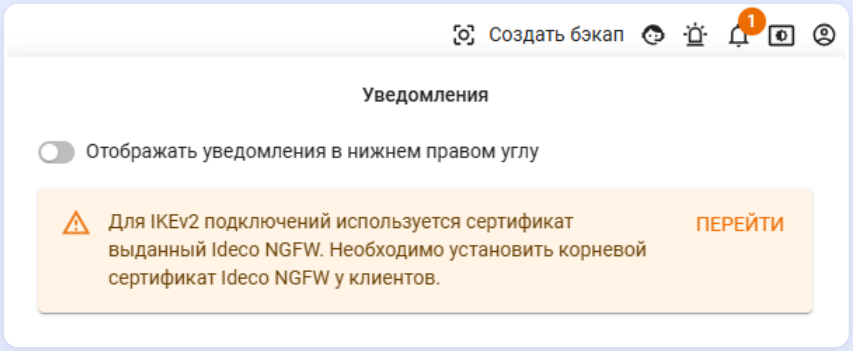
1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение по IKEv2/IPsec**.

3. В соответствующем поле укажите доменное имя или IP-адрес и 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 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 разделе **Сервисы → Сертификаты → Загруженные сертификаты**.

4. Если используете Netflow, то в поле **Индекс интерфейса для Netflow** введите целое число от 0 до 65535 для идентификации интерфейса.

5. Передача клиентам маршрутов до ваших локальных сетей происходит автоматически. Для управления доступом к сетям используйте Файрвол.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи → VPN-подключения → Доступ по VPN** разрешающее правило. Подробнее - в статье VPN-подключение.

Поддержка IKEv2/IPsec в клиентских 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.
- **KeeneticOS 3.5** и выше. Инструкция по настройке.
- MikroTik.
- Cisco routers.

Подключение по SSTP

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

По возможности не используйте этот тип подключения. Этот способ подключения 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 или пользователя из Active Directory.

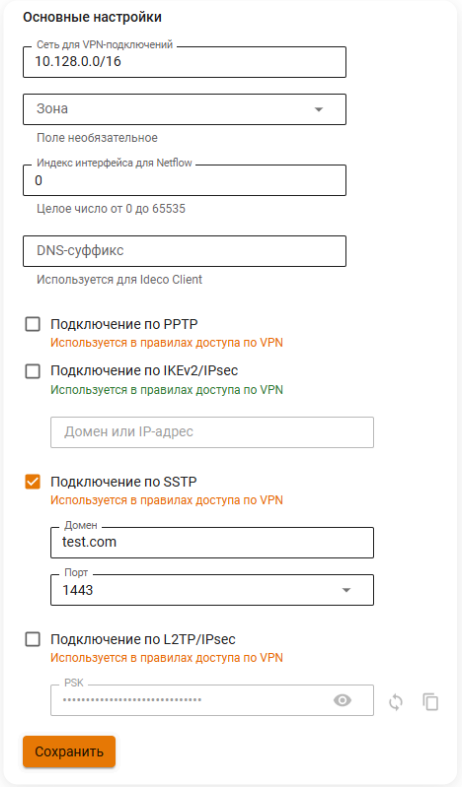
Особенности работы:

- 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 не поддерживает подключение MikroTik по SSTP, так как MikroTik использует устаревший и небезопасный алгоритм SHA-1.

Настройка Ideco NGFW

Основные настройки

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение SSTP**.

3. Подключение возможно только по DNS-имени, поэтому IP-адрес внешнего интерфейса Ideco NGFW должен резолвиться в одно из имен вашей внешней доменной зоны. В поле **Домен** укажите данное DNS-имя (используйте реальное имя с правильной A-записью, т. к. оно необходимо для выписки сертификата Let's Encrypt).

4. В поле **Индекс интерфейса для Netflow** введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. **Порт** - выберите предлагаемый порт (из вариантов: 1443, 2443, 3443, 4443).

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. 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.

Подключение по L2TP/IPsec

Видеоинструкцию смотрите по ссылкам:

- Youtube
- docs.ideco.ru

По возможности не используйте этот тип подключения. Он 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.

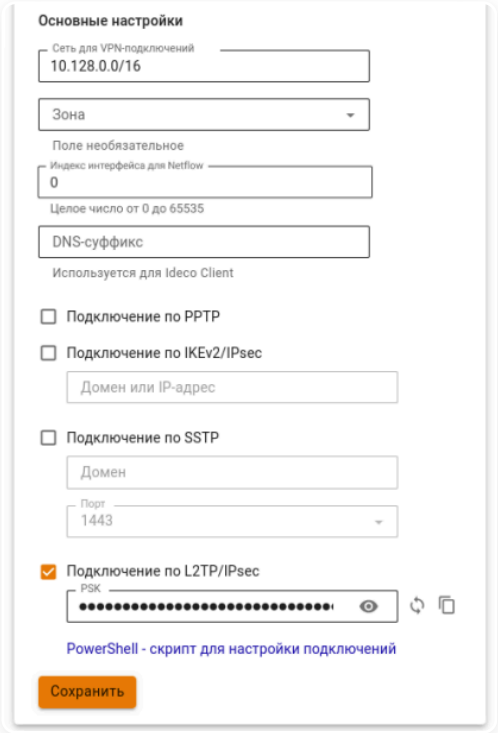
Для аутентификации используется связка логин/пароль пользователя Ideco NGFW или пользователя из Active Directory, а также PSK-ключ, который был указан при настройке соединения.

Не рекомендуем использовать для VPN-подключений кириллические логины. А так же указывать в качестве логина IP-адрес.

Настройка Ideco NGFW

Основные настройки

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



2. Включите опцию **Подключение по L2TP/IPsec**.

3. Укажите секретную фразу (PSK-ключ).

4. В поле **Индекс интерфейса для Netflow** введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Нажмите **Сохранить**.

Настройка доступа по VPN

Разрешите пользователю подключение по VPN из интернета, создав в разделе **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее правило. Подробнее в статье VPN-подключение.

Полезные ссылки

- L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их 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.

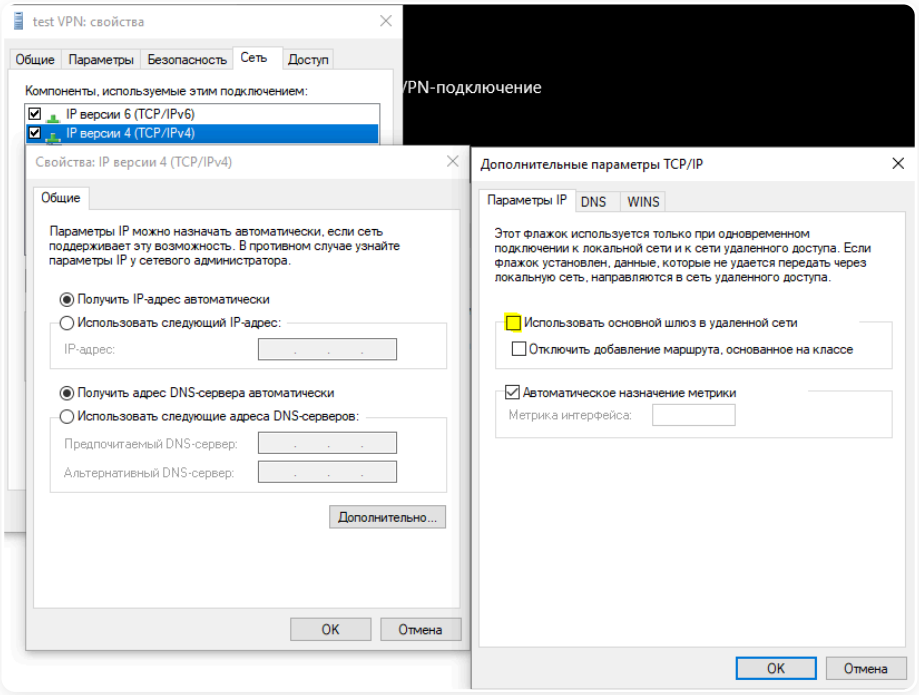
Особенности маршрутизации и организации доступа

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.

Организация доступа по VPN только к ресурсам локальной сети

Для организации доступа выполните действия:

1. На вкладке **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 добавить передачу IP-адреса VPN-сервера NGFW (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:

```
===========================================================================
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
        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 и добавленной публикацией IP NGFW:

```
===========================================================================
IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес          Маска сети      Адрес шлюза       Интерфейс  Метрика
```

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 либо добавить его в список публикуемых маршрутов на стороне NGFW. 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, 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

Для получения доступа к компьютерам в локальной сети Ideco NGFW 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);

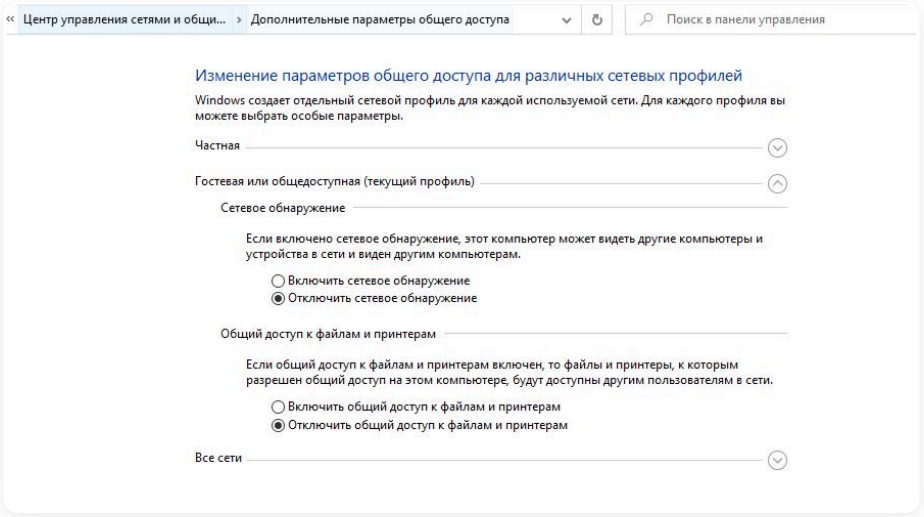
2. На компьютерах локальной сети основным шлюзом должен быть Ideco NGFW. Если это не так, то вручную необходимо прописать соответствующий маршрут, чтобы сетевые пакеты шли на Ideco NGFW для VPN-сети. **Например**:

```
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 (настраивается в разделе **Пользователи** → **VPN-подключения**);
- `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW.

3. На Ideco NGFW в разделе **Файрвол** → **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:

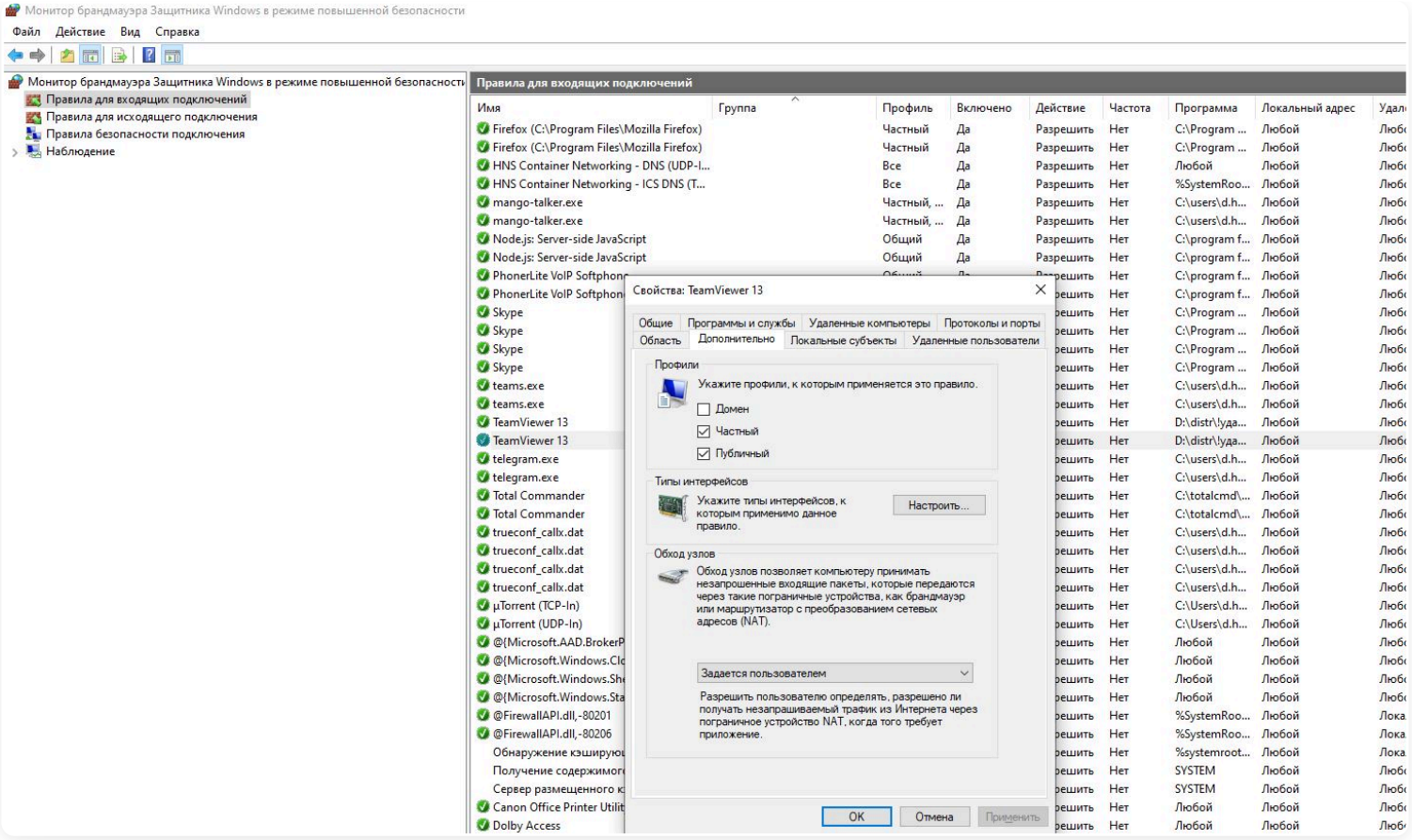
1. Перейдите в PowerShell (запустите его с повышением прав до администратора).

2. Выполните команду: `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`.

Возможные проблемы:

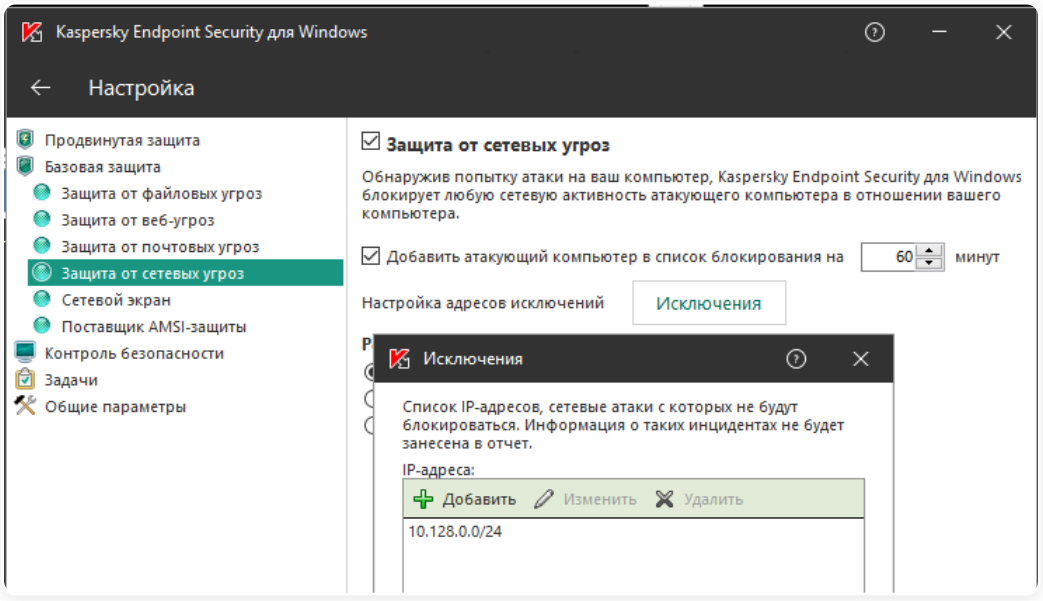
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей.

  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 не пересекаются. Затем проверьте настройки основного NGFW, следуя инструкциям, описанным в статье.

Получение доступа до хостов локальной сети, если за NGFW 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 (`172.16.0.1`).

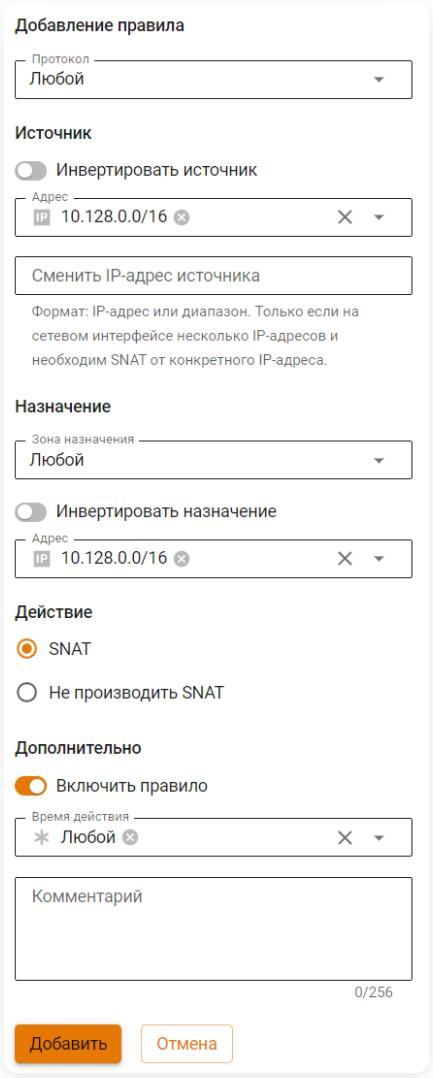
Если настроить на роутере маршрут невозможно, можно создать на NGFW SNAT-правило:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **SNAT** и нажмите **Добавить**.

2. Укажите следующие 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 подменит IP-адрес источника своим. За счет этого роутер направит ответ от хоста в локальной сети на NGFW, 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`.

Инструкция по запуску PowerShell скриптов

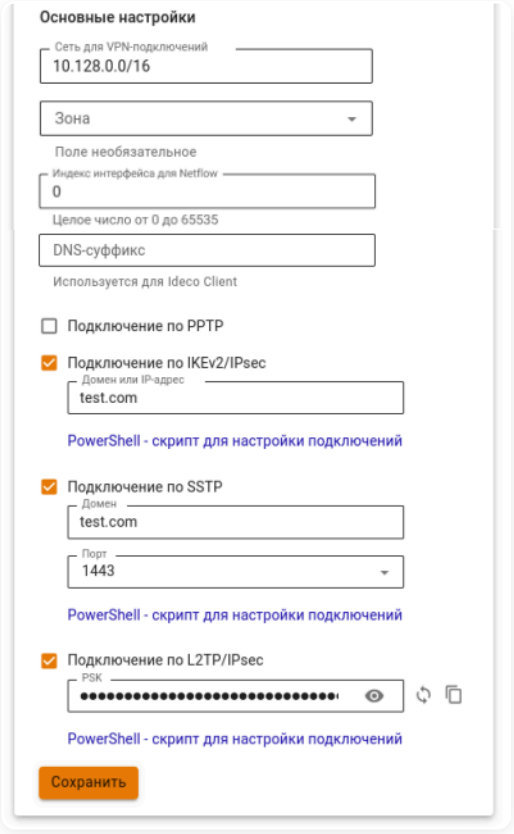
Для подключения по VPN к Ideco NGFW с белым IP адресом достаточно действий, указанных ниже. Если Ideco NGFW выходит в интернет через маршрутизатор, воспользуйтесь пунктом Подключение по VPN к Ideco NGFW с доступом в интернет через маршрутизатор.

Запуск PowerShell-скрипта

1. Скачайте скрипт одним из способов:

Из Ideco NGFW:

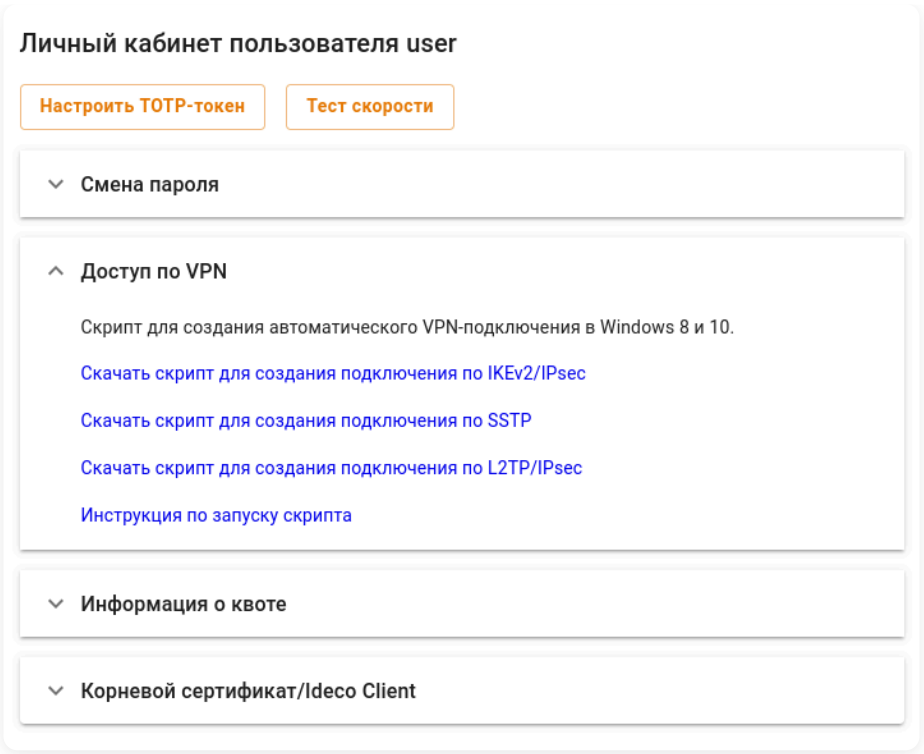
- Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**:



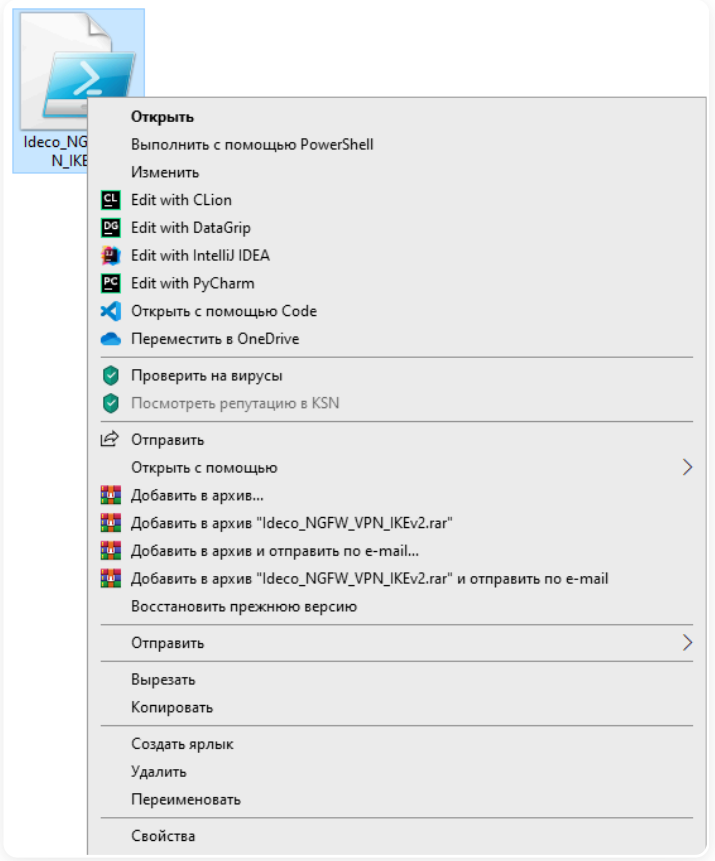
- Включите и настройте требуемый протокол подключения.
- Перейдите по ссылке **PowerShell - скрипт для настройки подключений**.
- Перенесите скачанный файл на устройство, на котором требуется создать VPN-подключение.

В личном кабинете пользователя:

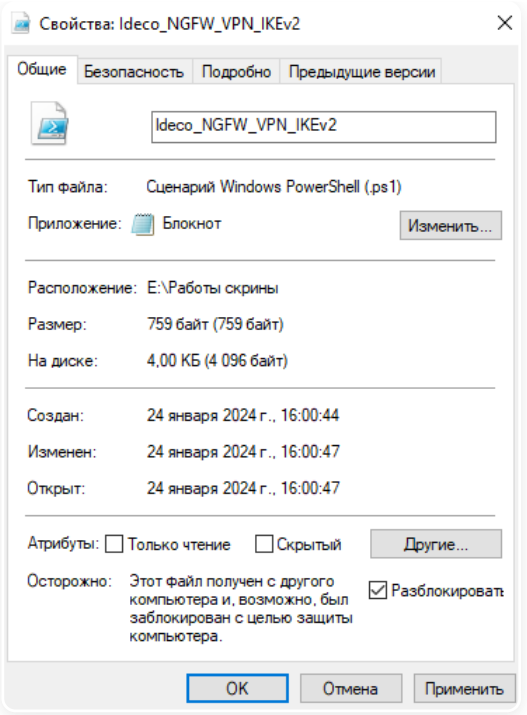
- Скачайте скрипт, перейдя по ссылке **Скачать скрипт для создания подключения**:



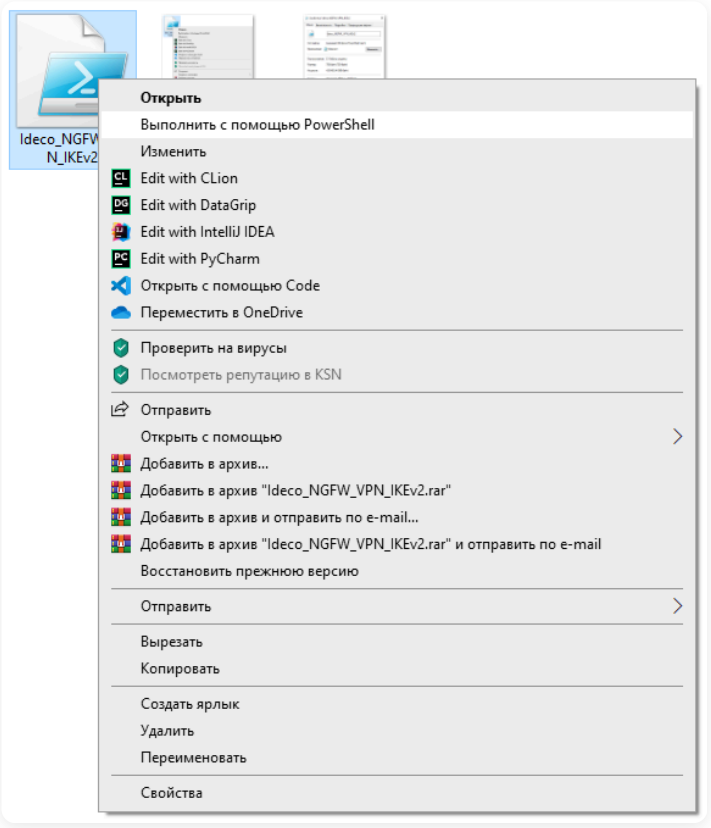
2. Нажмите правой кнопкой мыши по скачанному файлу и в контекстном меню выберите **Свойства**:



3. Включите опцию **Разблокировать** справа в нижнем углу свойств файла (по умолчанию ОС блокирует выполнение скачанных из интернета файлов):

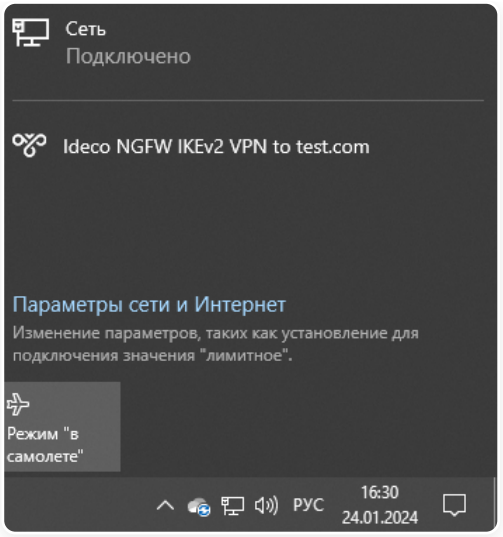


4. Нажмите правой кнопкой мыши на файл и выберите пункт **Выполнить в PowerShell**. Затем подтвердите действие, нажав **Да** на вопрос о внесении изменений в компьютер:



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 отключение создано, нажмите **Подключиться** в списке сетей.



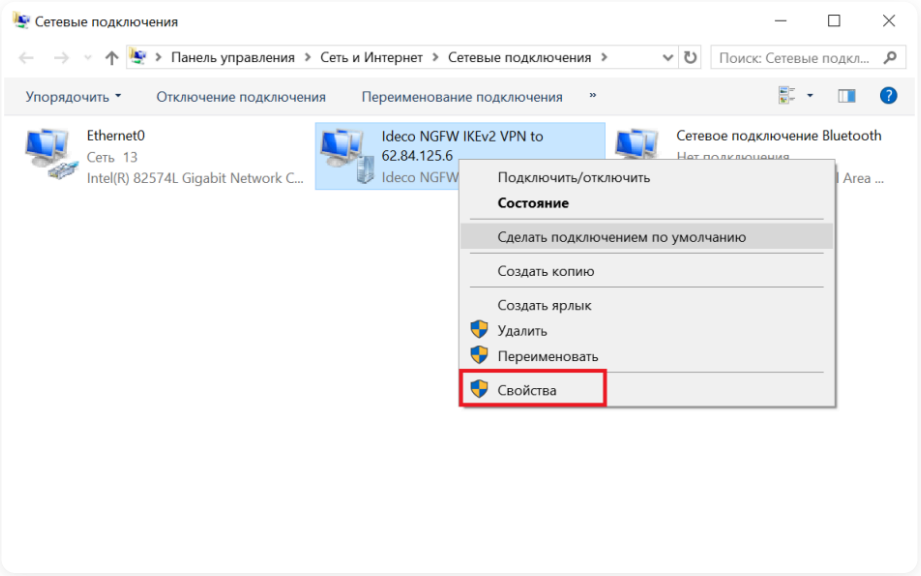
DNS-суффиксы для VPN-подключений

PowerShell-скрипты прописывают основной DNS-суффикс для создаваемого VPN-подключения. Он соответствует домену, в который введен Ideco NGFW. Это позволяет обращаться к устройствам за VPN по короткому имени.

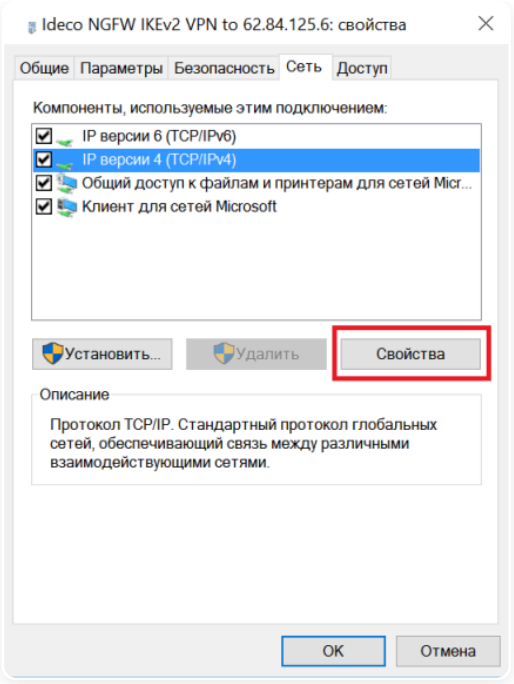
> Если Ideco NGFW введен в несколько доменов, то DNS-суффиксы в PowerShell-скриптах не прописываются, их необходимо настраивать вручную на подключенном по VPN устройстве.

Чтобы настроить DNS-суффиксы для созданного VPN-подключения в Windows, выполните действия:

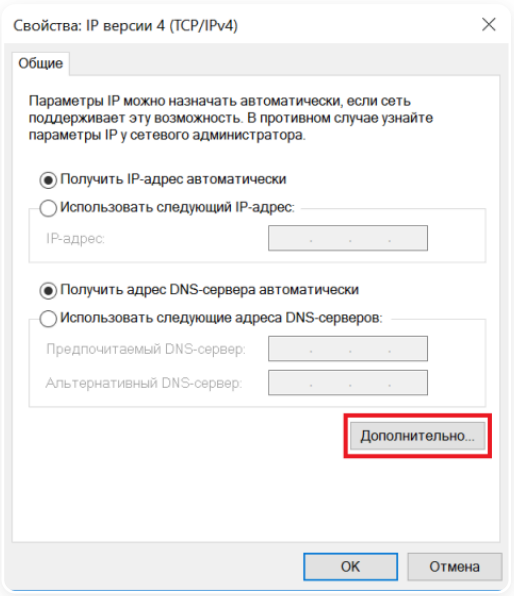
1. Перейдите в **Сетевые подключения**, нажмите правой кнопкой мыши по нужному VPN-подключению и выберите **Свойства**:



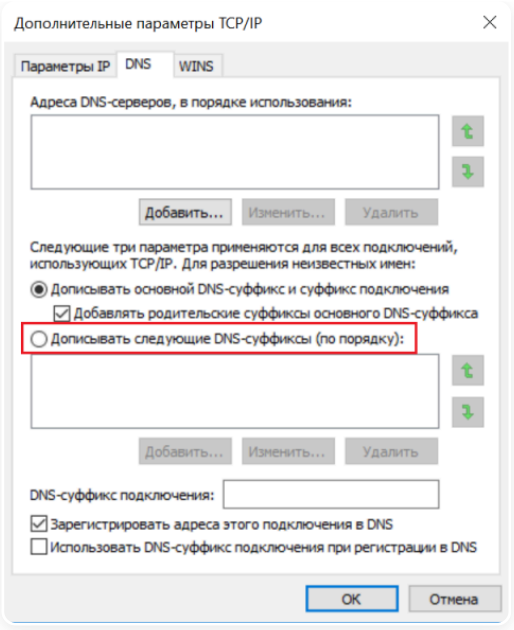
2. В открывшемся окне перейдите на вкладку **Сеть**, выберите компонент **IP версии 4 (TCP/IPv4)** и нажмите **Свойства**:



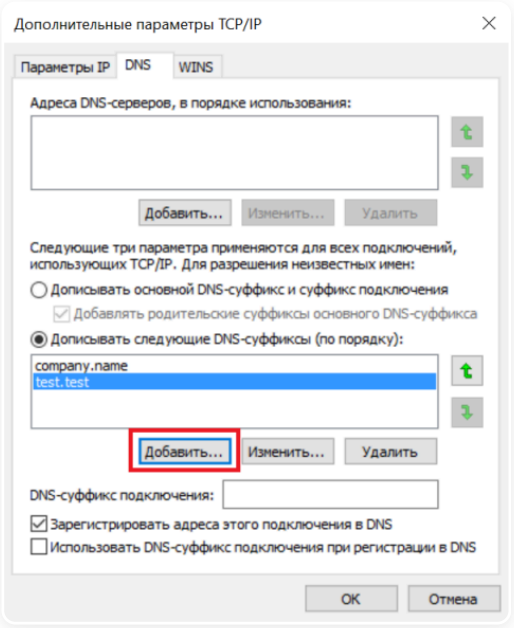
3. В открывшемся окне нажмите **Дополнительно**:



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. Этот порядок можно менять стрелками.

Подключение по VPN к Ideco NGFW 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 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 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 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

Название службы раздела **Ideco Client**: `ideco-agent-backend`; `ideco-agent-websocket`.

Список служб для других разделов доступен по ссылке.

Ideco Client - программа-клиент, которая управляет авторизацией пользователей при подключении к NGFW.

Ideco Client использует протокол WireGuard, но наша реализация WireGuard совместима только с Ideco NGFW: Ideco Client не является универсальным клиентом WireGuard, а поддержка WireGuard в Ideco NGFW ограничена.

Ideco Client недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

Возможности Ideco Client

- [x] Авторизация в локальной сети
- [x] VPN-подключение из внешних сетей
- [x] VPN-подключение из локальных сетей
- [x] Двухфакторная аутентификация
- [x] Режим работы Device VPN
- [x] Сбор данных о подключающихся устройствах

Сбор данных о подключающихся устройствах позволяет задавать критерии проверки - HIP-профили - и использовать их в правилах **Файрвола**.

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.

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	+	+	+
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	+	+	+

Ввод двухфакторной аутентификации	Показать окно ввода двухфакторной аутентификации при запросе от NGFW 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. Файрвол	Проверка Файрволом	+		
ZTNA. Антивирус	Проверка Антивирусами	+	+	
Версия	Проверка актуальной версии Ideco Client	+	+	+
Терминальный сервер	Поддержка работы терминальных серверов	+		
Балансировка Active-Active 302 Редирект	Подключение к Ideco NGFW по выданному балансировщиком адресу или другому серверу	+	+	+
Кастомная настройка	Кастомная настройка конфигурации Ideco Client: автосоздание профилей, запрет редактирования профилей и т.д.	+	+	+

Файрвол

Windows

Вендор	**Продукт**
Microsoft	Windows Firewall

Антивирус

Windows

Вендор	**Продукт**
Microsoft	Windows Defender
Kaspersky Lab	• Kaspersky Free • Kaspersky Small Office Security • Kaspersky Internet Security • Kaspersky Endpoint Security
Dr.Web	Dr.Web Security Space
Comodo	Comodo Internet Security

macOS

Вендор	**Продукт**
Kaspersky Lab	• Kaspersky Free • Kaspersky Endpoint Security Все остальные продукты Kaspersky Lab по умолчанию определяются как Kaspersky Free.
DrWeb	Dr.Web для macOS

Поддерживаемые версии ОС и порты подключения

Поддерживаемые версии ОС	• Windows 10 22H2 и выше **Важно:** Ideco Client не работает на ОС Windows 11 версии 24H2. Варианты решения описаны ниже • macOS версии 12.7 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 за NAT	• 80 TCP - для работы сертификатов Let's Encrypt • 14765 TCP и 3051 UDP - для работы Ideco Client

Настройки в Ideco NGFW

Перейдите в **Пользователи** → **Ideco Client** → **Основное**:

- В поле **Домен** укажите доменное имя или IP-адрес Ideco NGFW. Например: `example.ru`, `ideco.example.ru` или `52.251.83.117`
- Для подключения пользователей локальных сетей по VPN включите опцию **Создавать туннель при подключении из локальной сети**. Включение или выключении опции разрывает текущие сессии из локальных сетей.
- Для настройки Device VPN включите опцию **Принимать подключения в режиме Device VPN** Подробнее в статье.

Для корректного подключения из внешней сети создайте правило в **Пользователи** → **VPN-подключения** → **Доступ по VPN** разрешающее пользователю VPN-подключение.

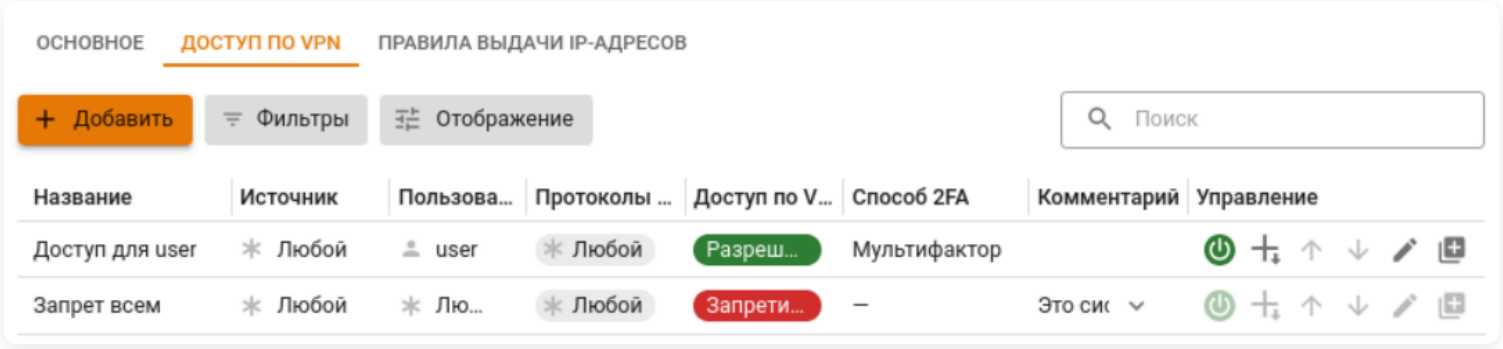
Настройка двухфакторной аутентификации в Ideco Client

В веб-интерфейсе Ideco NGFW:

1. Создайте учетную запись пользователя в разделе **Пользователи** → **Учетные записи**.

2. Перейдите в раздел **Пользователи** → **Двухфакторная аутентификация** и выберите подходящие типы. Настройте двухфакторную аутентификацию способами, указанными в статье.

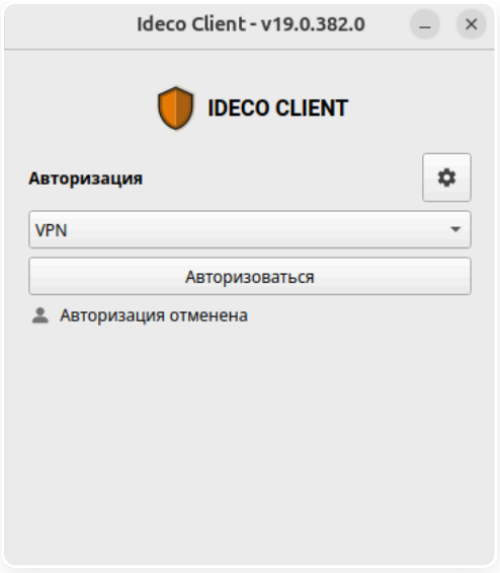
3. Добавьте правило в разделе **Пользователи** → **VPN-подключения** → **Доступ по VPN**. В настройках правила укажите созданную учетную запись пользователя и тип двухфакторной аутентификации, выбранный в шаге 2. В поле **Протоколы** укажите значение **Любой**:



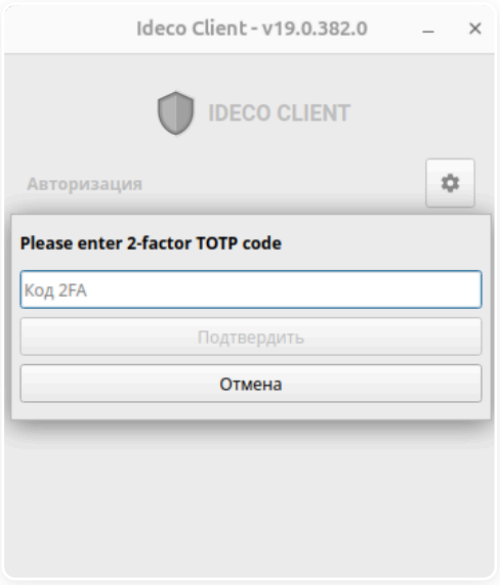
На устройстве пользователя:

1. Установите и запустите приложение Ideco Client. Инструкции по установке: Windows.

2. Авторизуйтесь через настроенную учетную запись пользователя:

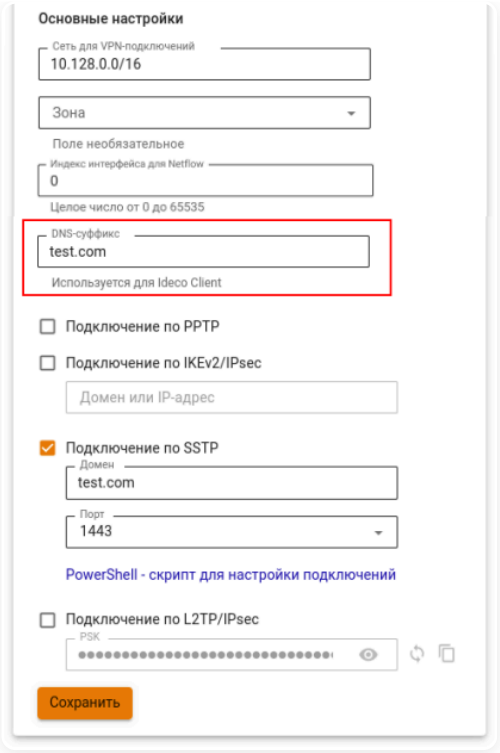


3. Введите код двухфакторной аутентификации:



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**:

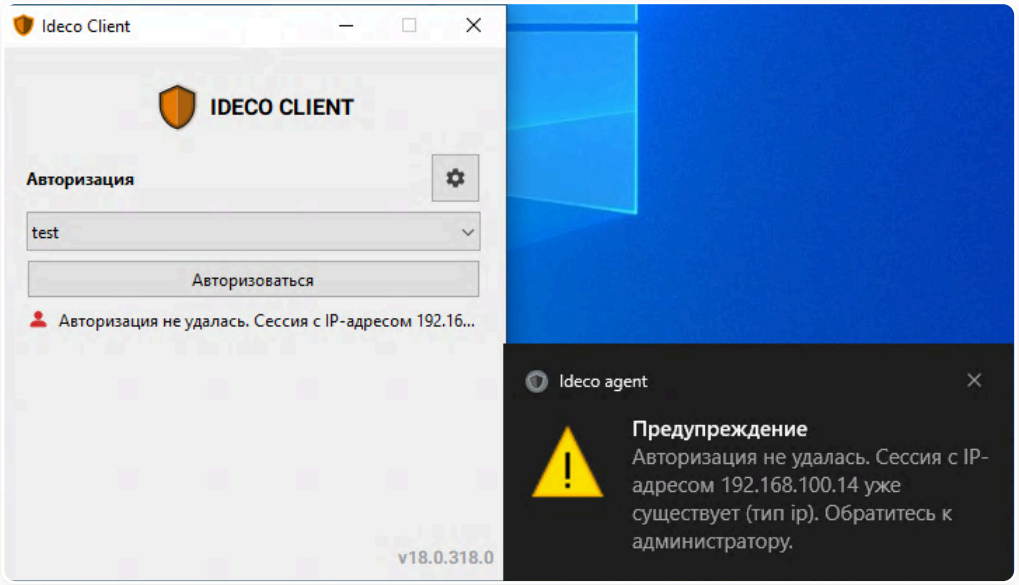


Суффикс будет передан устройствам через Ideco Client и позволит использовать короткие имена серверов (например, server-1c вместо server-1c.company.lan). Без суффикса разрешение таких имен работать не будет.

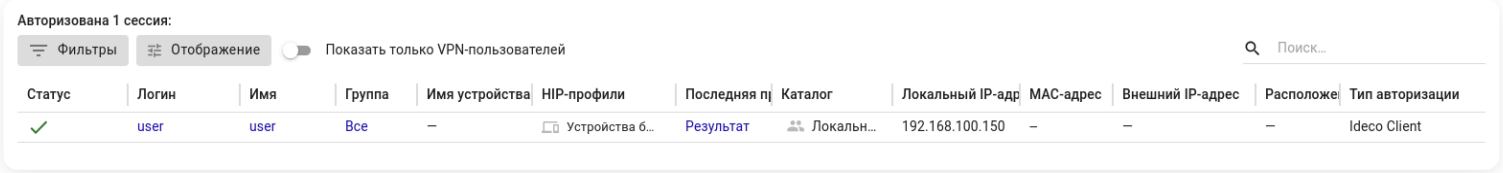
Ideco NGFW поддерживает только один DNS-суффикс. Не указывайте DNS-суффикс, если NGFW введен в несколько доменов.

Особенности работы Ideco Client

- Только один профиль может быть с опцией автоподключения. Если активировать автоподключение для другого профиля, у предыдущего эта опция отключится.
- SSO-аутентификация в IdecoClient не будет работать для доверенных доменов.* 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: `IdecoAgent.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:



DNS-запросы 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** сеть до NGFW 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).
- При VPN-подключении через Ideco Client DNS-запросы идут на адрес NGFW, но в передаваемом на Ideco Client списке нет маршрута до DNS NGFW.

Рекомендуем при выборе типа передачи маршрутов **Отправлять только указанные сети** добавить в список DNS NGFW, чтобы клиент VPN построил таблицу маршрутизации до этой сети.

Особенности маршрутизации и организации доступа по VPN к ресурсам локальной сети описаны в статье.

Балансировка и редиректы VPN-подключений

Device VPN

Device VPN - режим работы Ideco Client, в котором клиентское устройство авторизуется на Ideco NGFW 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

Для авторизации через Device VPN используется корневой сертификат с приватным ключом. На основе этого ключа администратор создает пользовательские сертификаты для конечных устройств.

Как работает перенос настроек с профилями при смене версии

При запуске Ideco Client выполняет последовательность действий:

1. Ideco Client проверяет наличие настроек в ключе реестра текущей версии.

2. Если настройки найдены, они применяются.

3. Если настройки текущей версии отсутствуют, ищет в ключах реестра прошлых версий (от новой к старой).

4. При нахождении настроек в предыдущих версиях они копируются в ключ реестра текущей версии Ideco Client.

5. Если настройки не найдены, то в ключе реестра текущей версии создаются настройки с параметрами по умолчанию.

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 ключ реестра текущей версии, то при следующем запуске Ideco Client инициирует поиск и копирование настроек. Если настройки не будут найдены в ключах реестра предыдущих версий, то будет создан ключ с настройками по умолчанию.

Примеры работы переноса настроек

Первая установка Ideco Client

Ideco Client не установлен и в реестре компьютера нет настроек Ideco Client:

1. При запуске Ideco Client создает в реестре ключ текущей версии Ideco Client с настройками по умолчанию. Например, `\HKEY_CURRENT_USER\Software\Ideco\Agent\19.1.3`.

2. Копирование не выполняется.

Обновление Ideco Client на следующую версию

Пользователь обновляет Ideco Client с 18.3.2 до 19.0.1:

1. Ideco Client проверяет наличие настроек в ключе реестра версии 19.0.1 - `\HKEY_CURRENT_USER\Software\Ideco\Agent\19.0.1`.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в ключах реестра предыдущих версий от более новой к более старой.

4. Если настройки найдены в ключе реестра одной из прошлых версий, то они копируются в ключ реестра версии 19.0.1.

5. Если настройки не найдены, то создается ключ реестра версии 19.0.1 с параметрами по умолчанию.

Возврат Ideco Client на предыдущую версию

Возврат Ideco Client с версии 19.0.2 на 19.0.1:

1. При запуске Ideco Client ищет настройки в ключе реестра версии, на которую происходит возврат - `\HKEY_CURRENT_USER\Software\Ideco\Agent\19.0.1`.

2. Если настройки найдены, применяет их.

3. Если настройки не найдены, то поиск продолжается в ключах реестра предыдущих версий от более новой к более старой.

4. Если настройки найдены, они копируются в ключ реестра версии 19.0.1.

5. Если настройки не найдены, то создается ключ реестра версии 19.0.1 с параметрами по умолчанию.

> Копирование не происходит назад по версиям, поэтому копирование настроек из версии 19.0.2 на 19.0.1 невозможно.

Повторное обновление Ideco Client после возврата на предыдущую версию

1. Пользователь использовал версию 19.0.2.

2. Выполнен возврат на версию 19.0.1.

3. Пользователь создал новый профиль в версии 19.0.1

4. Выполнено обновление до версии 19.0.2.

5. При запуске Ideco Client настройки и профили из версии 19.0.1 не будут перенесены в версию 19.0.2, поскольку в ключе реестра уже существуют настройки, созданные при первом запуске версии 19.0.2.

Решение проблемы с подключением на ОС Windows 11 версии 24H2/25H2

Вариант 1. Включить компонент **Virtual Machine Platform**:

1. Установите последнюю версию MS Visual C++ Redistributable.

2. Нажмите комбинацию клавиш **Windows + R** и введите команду `appwiz.cpl`.

3. В левой части окна выберите **Включение или отключение компонентов Windows**.

4. Включите функцию **Virtual Machine Platform** (**Платформа виртуальной машины**).

5. Нажмите **ОК** и перезагрузите компьютер.

Вариант 2. Вернуть предыдущую версию операционной системы Windows 11 23H2.

Вариант 3. Использовать альтернативный способ VPN-подключения.

Ideco Client не работает, если внутренние ресурсы опубликованы через DNAT

> Видеоинструкцию смотрите по ссылкам:
>
> - Rutube

- Youtube
- docs.ideco.ru

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.

Полезные ссылки

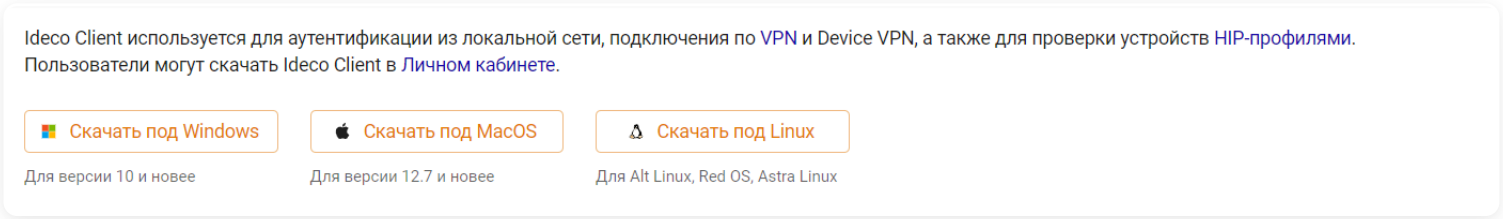
- **Балансировка VPN-подключений**
- **Настройка Device VPN**
- **Создание сертификатов для Device VPN**
- **Кастомная настройка Ideco Client**
- **Как включить режим отладки для Ideco Client**

Установка и настройка Ideco Client на Windows

Скачивание

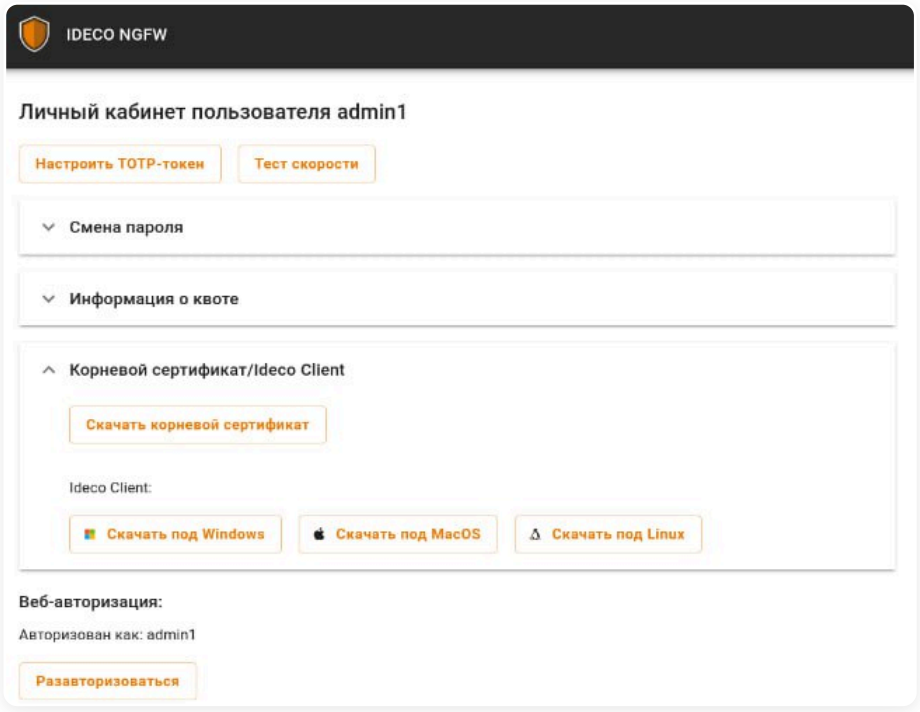
Для администратора

Перейдите в раздел **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Windows**:



Для пользователя

Нажмите на кнопку **Скачать под Windows** в личном кабинете пользователя:



Установка

Сохраните и запустите файл установки *IdecoAgent.msi*.

Если требуется заранее установить адрес подключения, в командной строке перейдите в директорию с файлом `cd [путь до файла]` и откройте файл `IdecoAgent.msi` с ключом `utm_address`, в котором нужно указать адрес Ideco NGFW (команда: `IdecoAgent.msi utm_address=адрес_ngfw`).

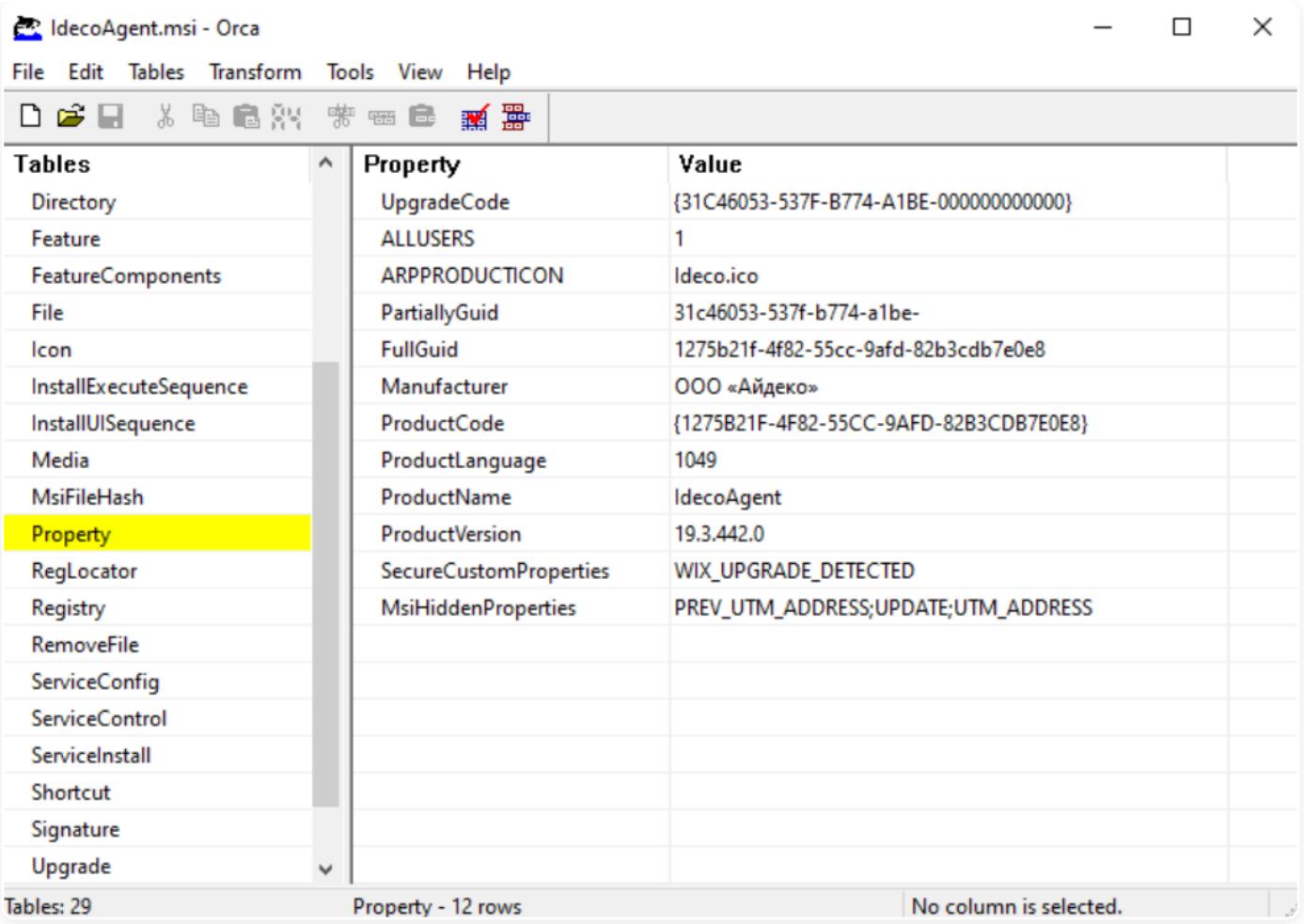
Чтобы оптимизировать процесс установки Ideco Client с помощью GPO, добавьте параметр адреса Ideco NGFW `IdecoAgent.msi UTM_ADDRESS=адрес_ngfw` в установочный файл `IdecoAgent.msi`. Для этого воспользуйтесь утилитой Orca.

Как добавить параметр в Orca

1. Запустите Orca.

2. Нажмите **File** → **Open** и откройте `IdecoAgent.msi`.

3. В дереве таблиц найдите **Property**:



4. Нажмите **Tables** → **Add Row**, чтобы добавить новую запись.

5. В поле **Property** введите `UTM_ADDRESS`, в поле **Value** - IP-адрес или доменное имя Ideco NGFW. Нажмите **Ок**.

6. Нажмите **File** → **Save**, чтобы сохранить изменения.

7. Закройте Orca.
В этом случае *msi-файл* будет установлен с уже заполненным полем **Хост**, а авторизация компьютера будет происходить через SSO-профиль по умолчанию в "тихом" режиме автоподключения.

Если Kaspersky Plus блокирует установку и обновление

1. Откройте **Настройки** → **Настройки безопасности** → **Исключения и действия с найденными объектами** → **Указать доверенные приложения**:

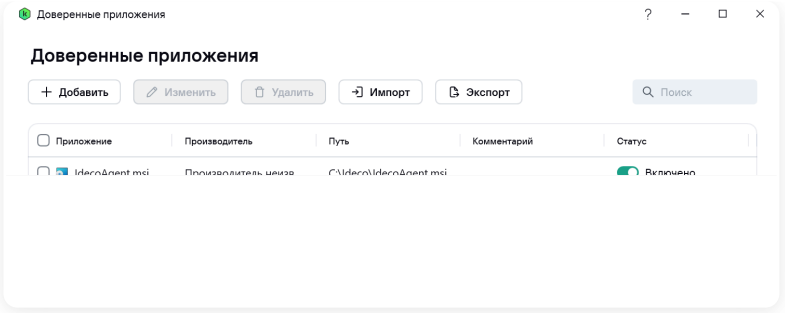
2. Нажмите **Добавить**, выберите скачанный msi-файл Ideco Client и нажмите **Выбрать**:

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:



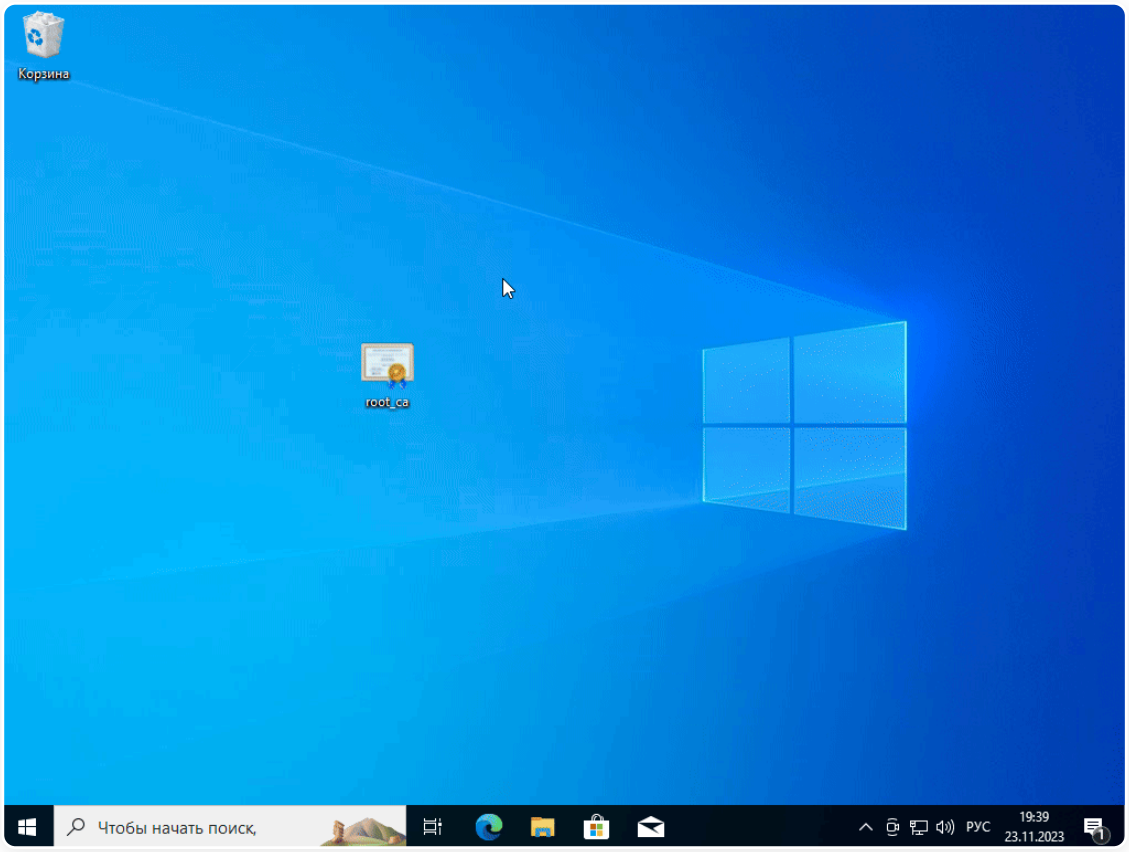
7. Откройте **Настройки** → **Настройки безопасности** → **Настройки сети** и настройте раздел:

8. Нажмите **Сохранить**.

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt, импортируйте корневой сертификат Ideco NGFW 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**.

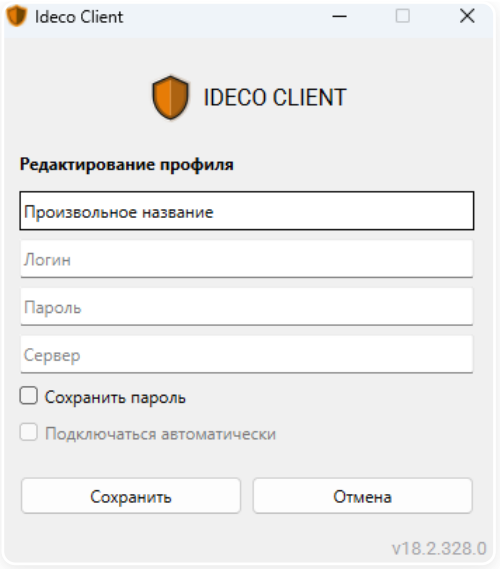
4. Выберите пункт **Поместить все сертификаты в следующее хранилище**, нажмите **Обзор** и выберите папку **Доверенные корневые центры сертификации**.

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 хост в зависимости от количества доменов, в которые введен NGFW:

NGFW введен в один домен

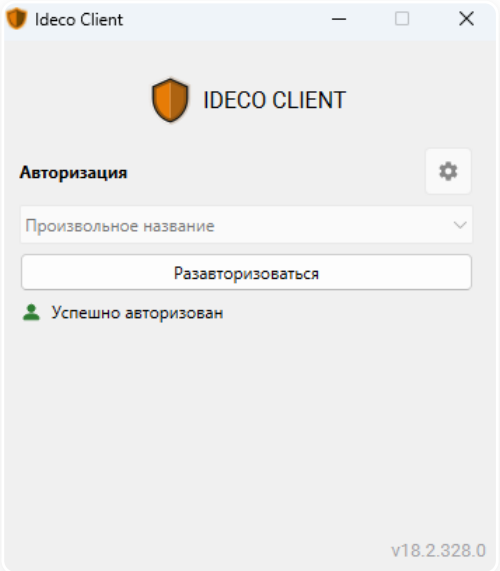
Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:

NGFW введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW**:

3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



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**.

Полезные ссылки

- **Кастомная настройка Ideco Client**
- **Как включить режим отладки для Ideco Client**

Установка и настройка Ideco Client на MacOS

Особенности работы Ideco Client на MacOS

- Ideco Client для MacOS требует версии системы 12.7 и выше;
- HIP-профили на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

- ОС;
- процесс;
- антивирус (Kaspersky).

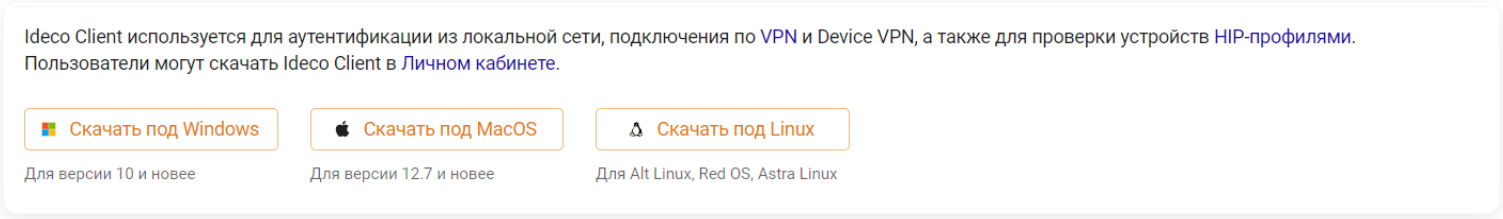
Недоступные HIP-профили

- домен;
- межсетевой экран;
- реестр (всегда только Windows);
- службы (всегда только Windows);
- пакет обновлений Knowledge Base (всегда только Windows).

Скачивание

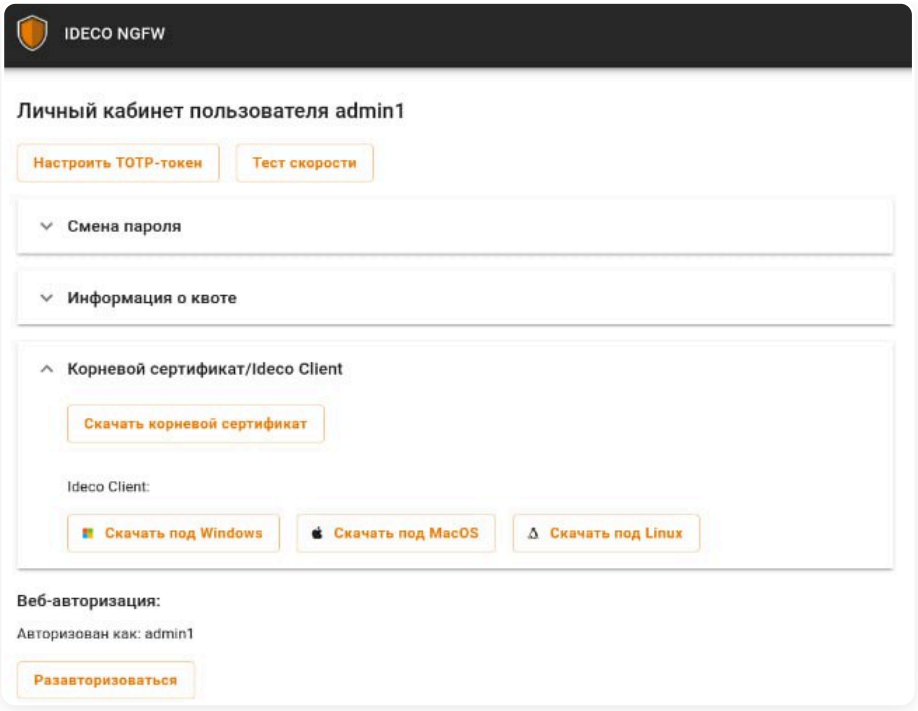
Для администратора

Перейдите в раздел **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под MacOS**:



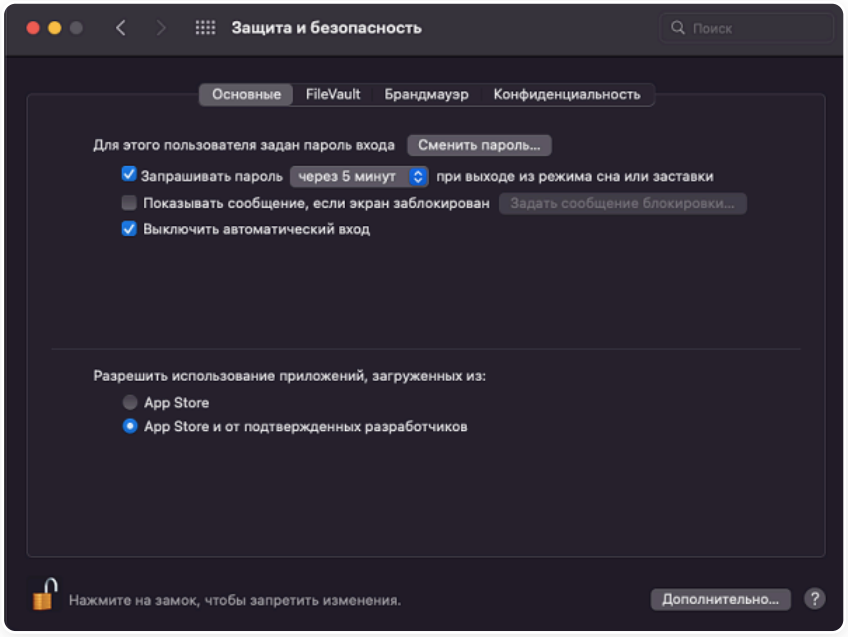
Для пользователя

Нажмите кнопку **Скачать под MacOS** в личном кабинете пользователя:



Установка

В некоторых версиях MacOS необходимо явно разрешить установку приложения не из App Store. Для этого перейдите в раздел **Защита и безопасность** → **Основные** и разрешите использование приложений, загруженных из **App Store и от подтвержденных разработчиков**:

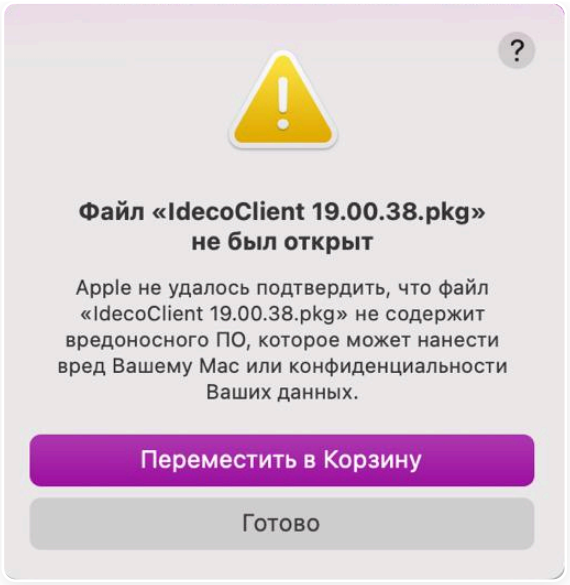


Чтобы установить **Ideco Client** на MacOS, выполните действия:

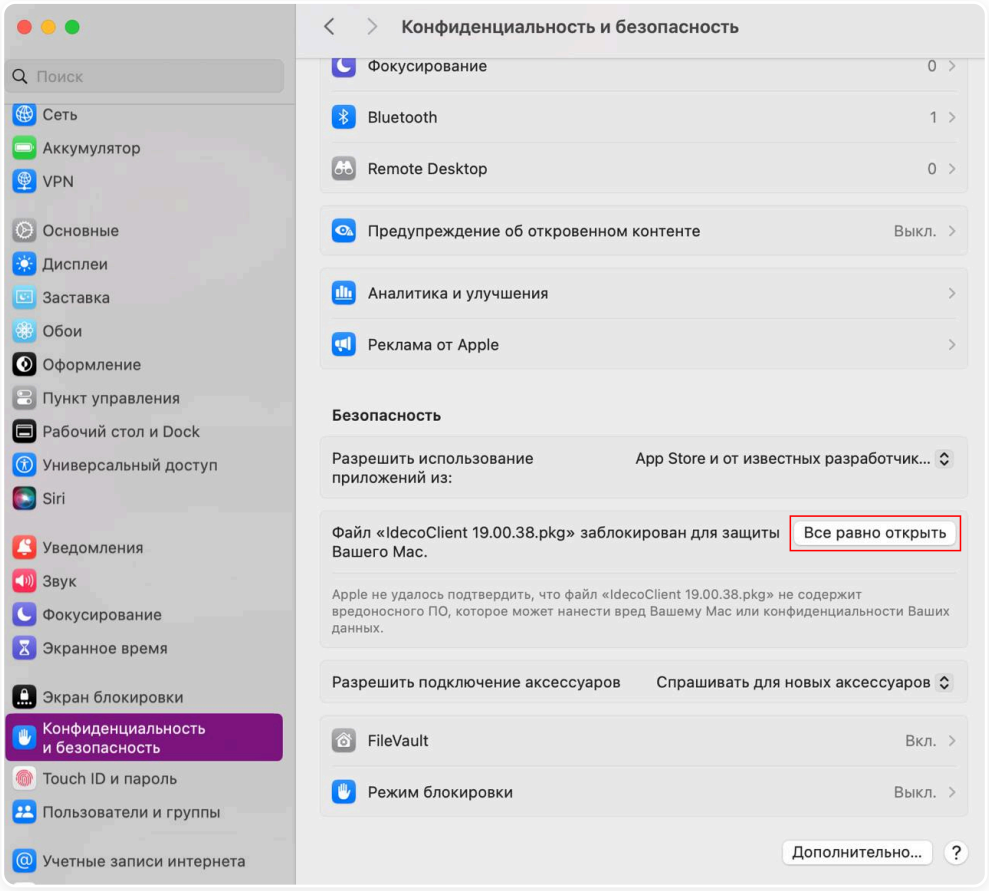
1. Кликните по файлу *IdecoClient.pkg* правой кнопкой мыши и выберите **Открыть**.

MacOS Sequoia

1. При открытии файла *IdecoClient.pkg* система сообщит о потенциальной опасности приложения. Нажмите **Готово**:



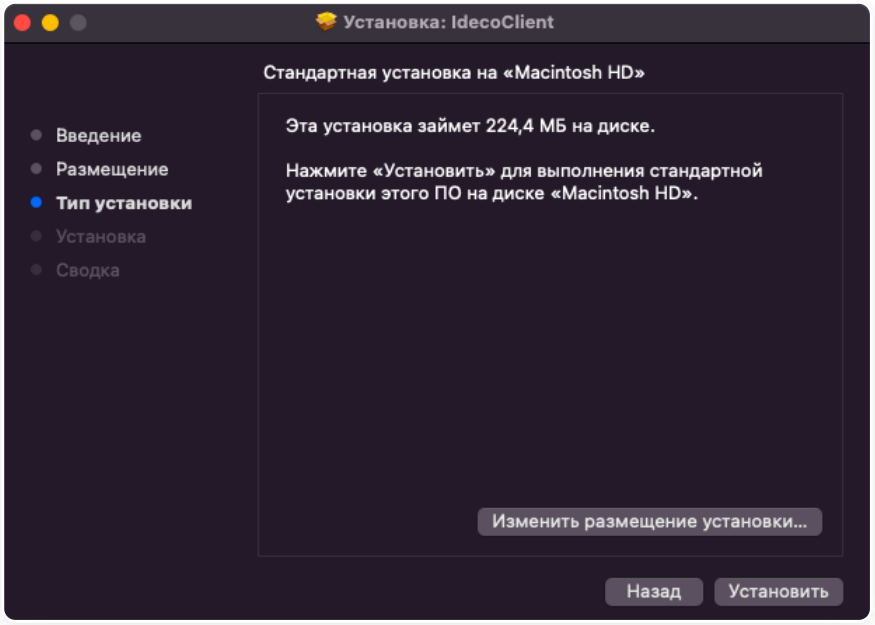
2. Перейдите в раздел **Конфиденциальность и безопасность** и нажмите **Все равно открыть** рядом с именем файла:



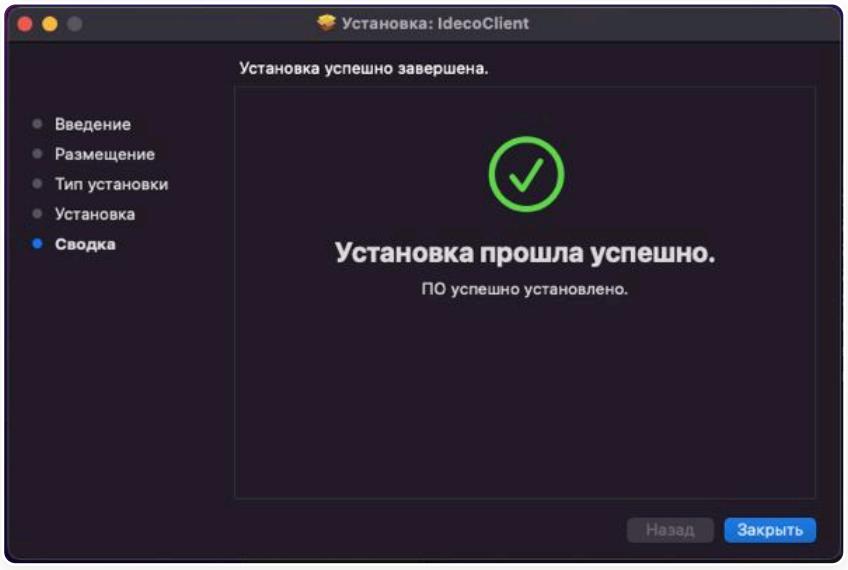
MacOS Monterey и MacOS Sonoma

При открытии файла *IdecoClient.pkg* система выдаст предупреждение. Подтвердите действие:

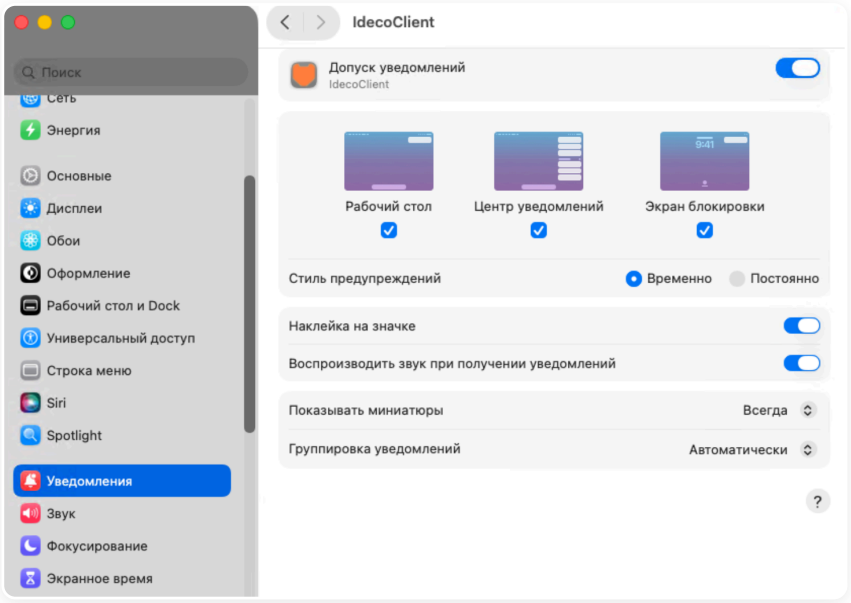
2. Нажмите **Продолжить**. В открывшемся окне нажмите **Установить**:



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 по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt убедитесь, что срок действия оконечного сертификата на этот домен или IP-адрес составляет не более 825 дней. Если это так, то импортируйте **корневой** сертификат Ideco NGFW на компьютер. Если срок действия оконечного сертификата на этот домен или IP-адрес превышает 825 дней, загрузите на NGFW свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

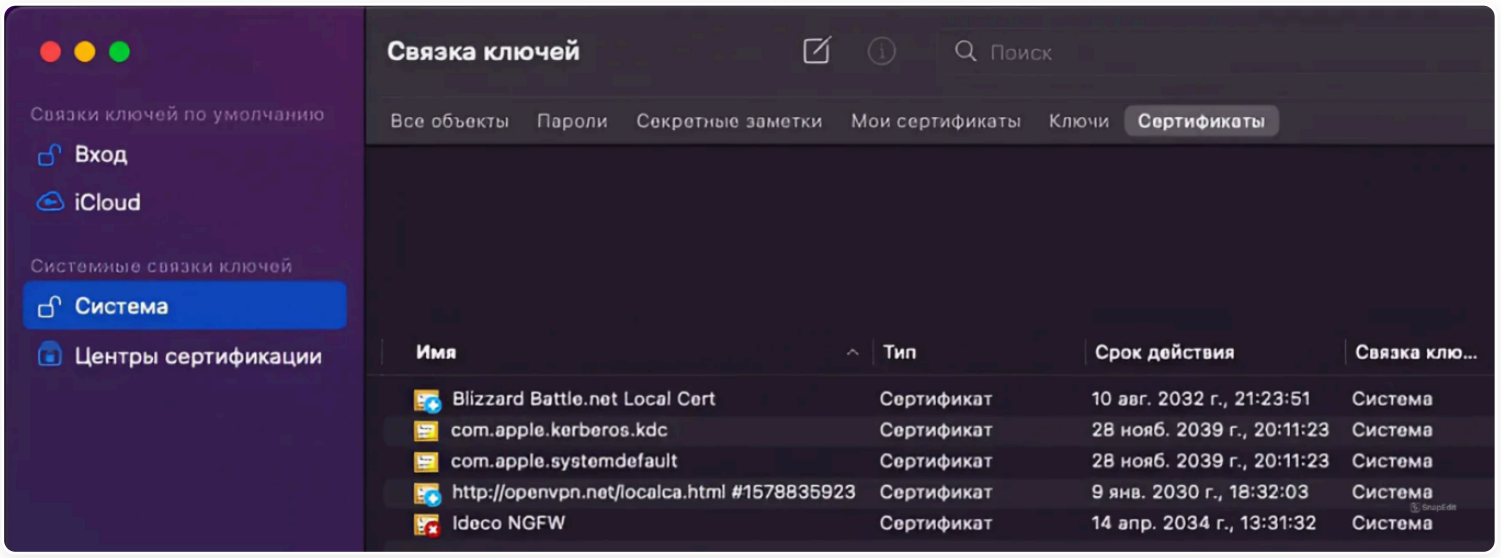
Установка корневого сертификата Ideco NGFW на MacOS

Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW 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 получить доступ к этим файлам и прочитать их. Рекомендуем сохранить файлы в другую директорию, например, в корневую директорию домашней папки пользователя.

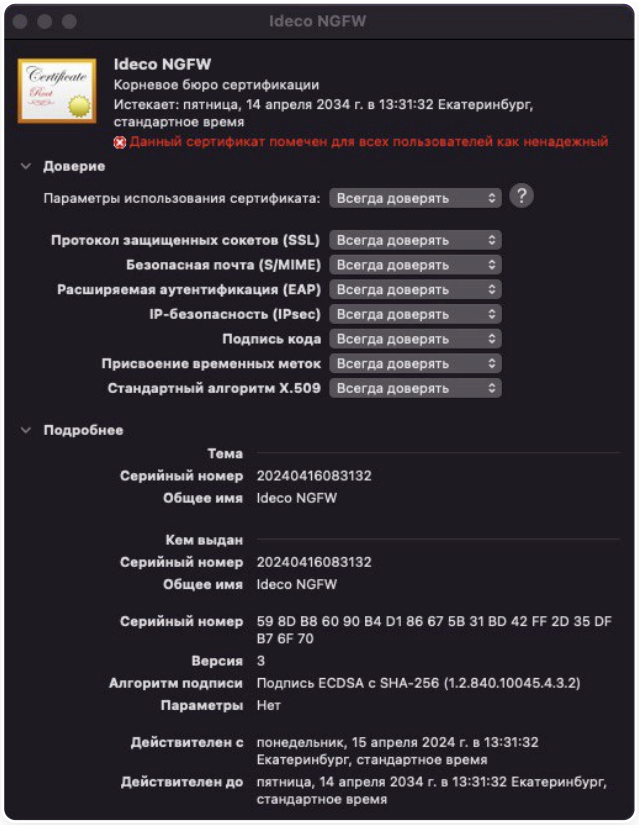
Установка через Связку ключей

1. Откройте скачанный файл *root_ca.crt* в приложении **Связка ключей**, сертификат Ideco NGFW появится в папке **Система**:

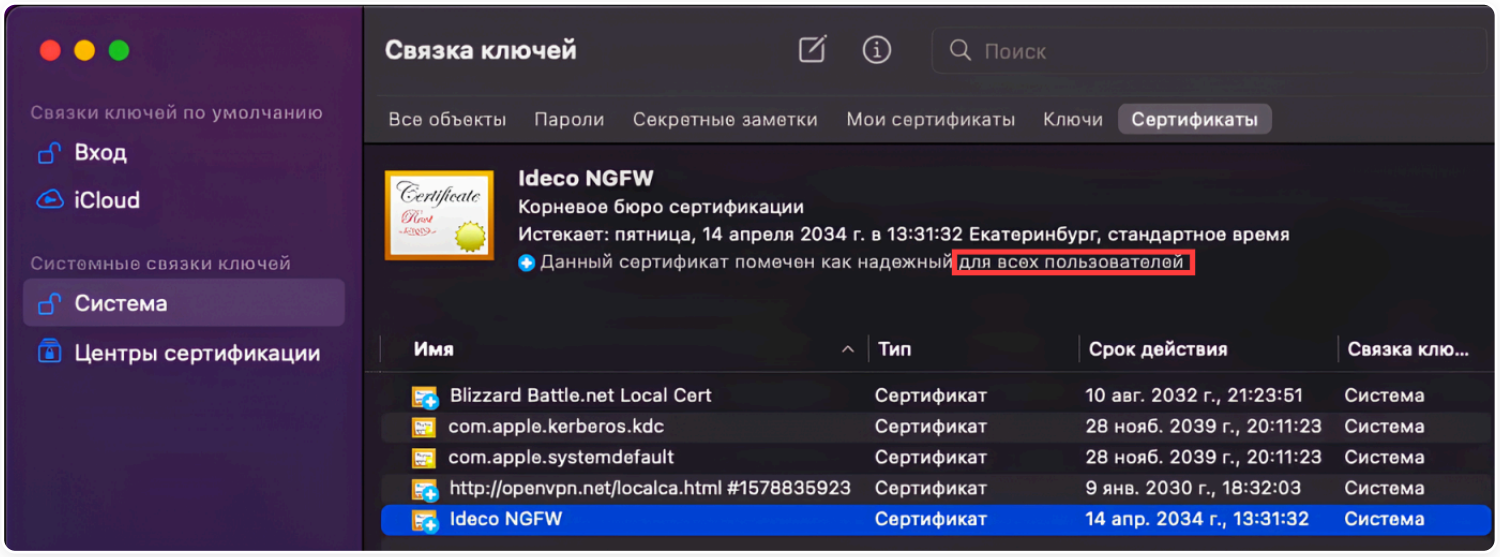


2. Нажмите по сертификату правой кнопкой мыши и выберите **Свойства**.

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:

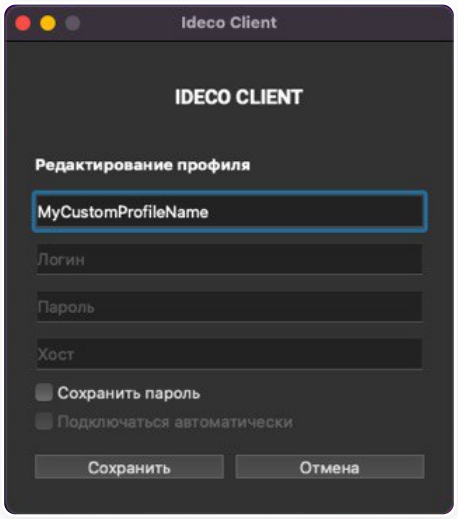
```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <путь к сертификату>/root_ca.crt
```

2. Перезагрузите компьютер.

Первый запуск

1. Запустите Ideco Client.

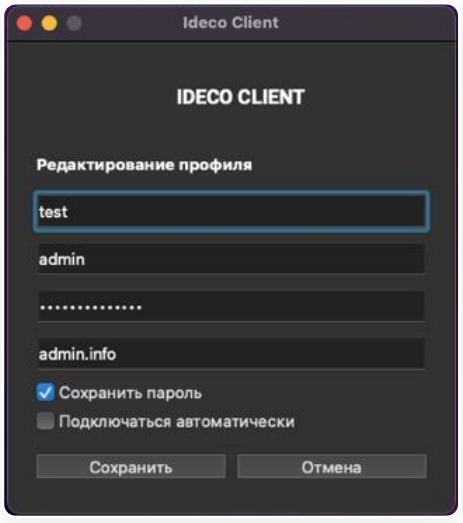
2. Введите данные:



- **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 в зависимости от количества доменов, в которые введен NGFW:

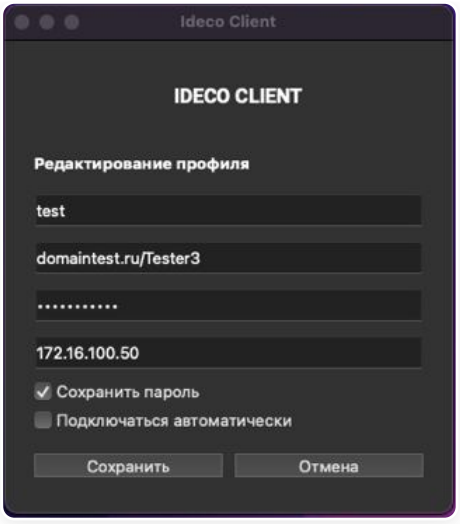
NGFW введен в один домен

Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес:



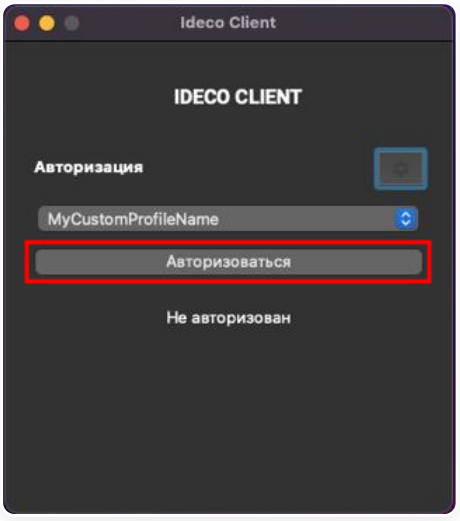
NGFW введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW**:



3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



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**.

Установка и настройка Ideco Client на Linux

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:

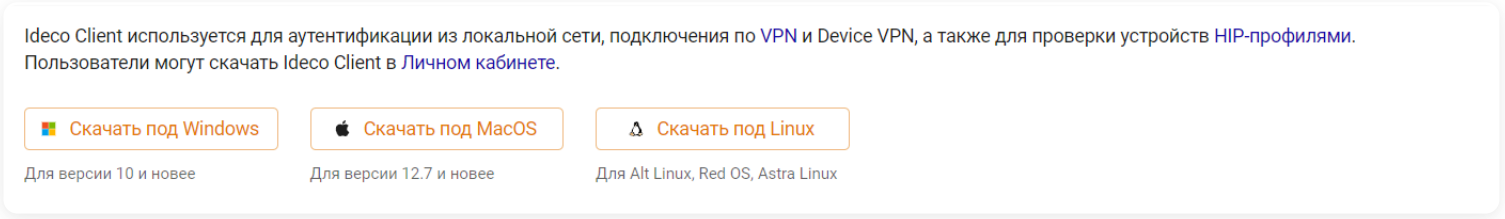
```
bool os_specific::isProcessExist(const std::string &processName)
```

Длина строки `processName` составляет не более 15 символов. Если название процесса длиннее, оно будет обрезано до максимально доступного числа символов. В этом случае проверка не будет выполнена корректно.

Скачивание

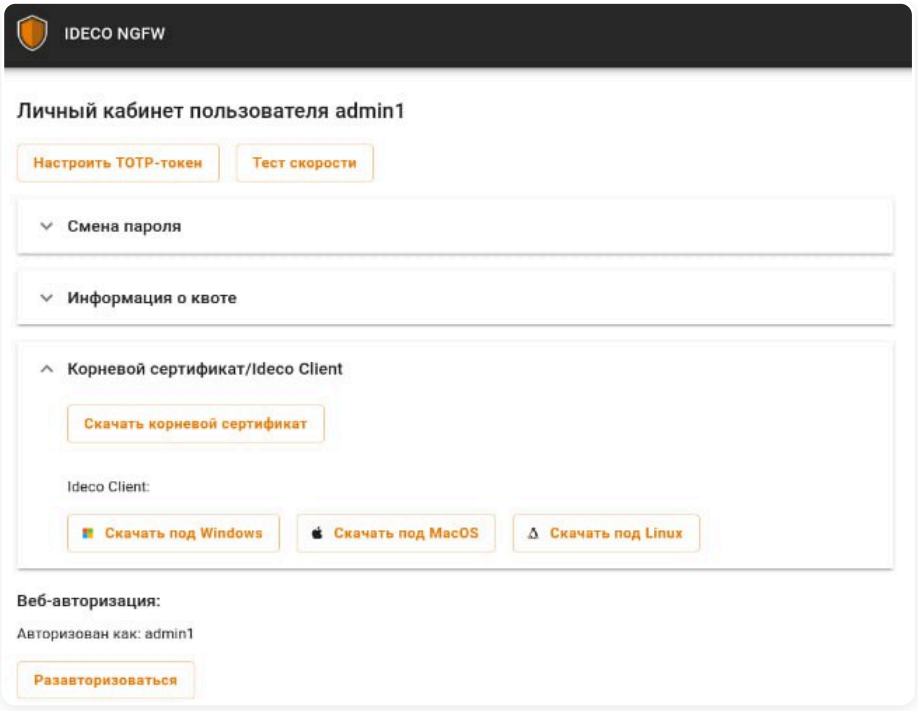
Для администратора

Перейдите в раздел **Пользователи** → **Ideco-Client**, переведите опцию **Ideco Client** в положение **Включен**, нажмите **Скачать под Linux**:



Для пользователя

Перейдите в личный кабинет пользователя и нажмите **Скачать под Linux**:



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 IdecoAgent.sh
```

3. Запустите файл установки Ideco Client:

```
./IdecoAgent.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 на Astra Linux удалите настройку службы IdecoService:

```
sudo rm /etc/systemd/system/IdecoService.service
```

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW 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 на компьютер. Если срок действия сертификата на этот домен или IP-адрес превышает 825 дней, загрузите на NGFW свой сертификат со сроком действия, не превышающим 825 дней или перевыпустите автоматически сгенерированный сертификат.

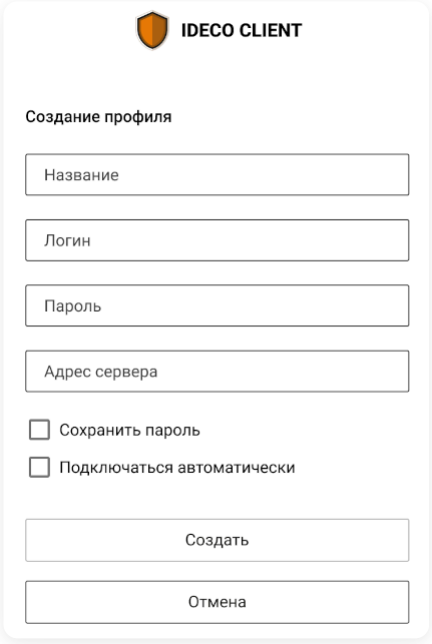
Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- 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.

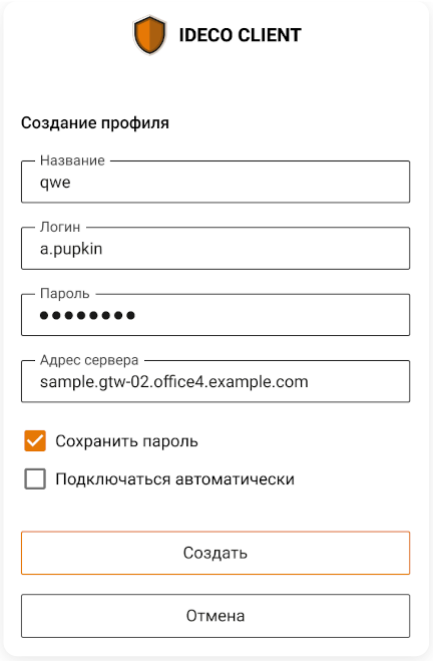
2. Введите данные:



- **Имя профиля** - может не совпадать с логином и будет использоваться при выборе профиля для авторизации.
- **Пароль** - укажите пароль пользователя.
- **Логин** и **Хост** - укажите логин и хост в зависимости от количества доменов, в которые введен NGFW:

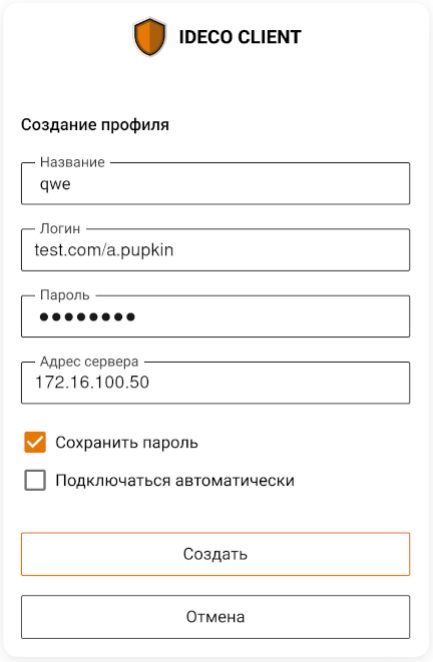
NGFW введен в один домен

Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес.



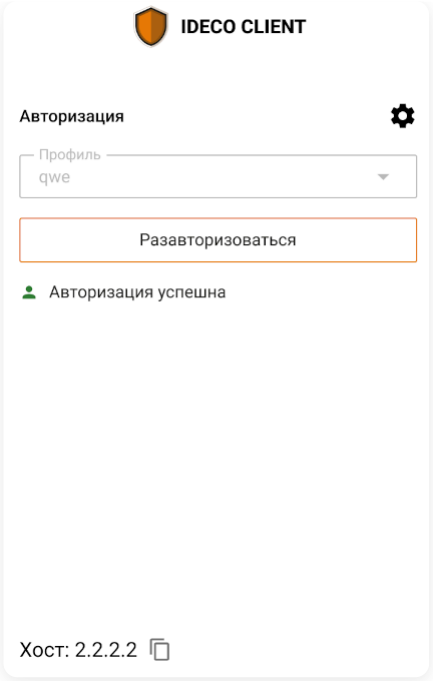
NGFW введен в несколько доменов

Введите **логин** в формате **имя_домена/имя_пользователя**, в качестве **хоста** укажите **IP NGFW**.



3. Нажмите **Сохранить**.

4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**:



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>
```

2. Запустите файл удаления Ideco Client:

```
./uninstall.sh
```

Настройка Device VPN

Device VPN позволяет получить доступ к устройству даже когда пользователь не использует Ideco Client, и устройство имеет доступ в интернет или до Ideco NGFW. Это позволяет осуществлять удаленное администрирование, обновление ПО и антивирусов, мониторинг.

В качестве **Сертификата устройства** Device VPN можно использовать:

- Самоподписанные сертификаты.
- Сертификаты, выданные Центрами сертификации (Certificate Authority, CA).

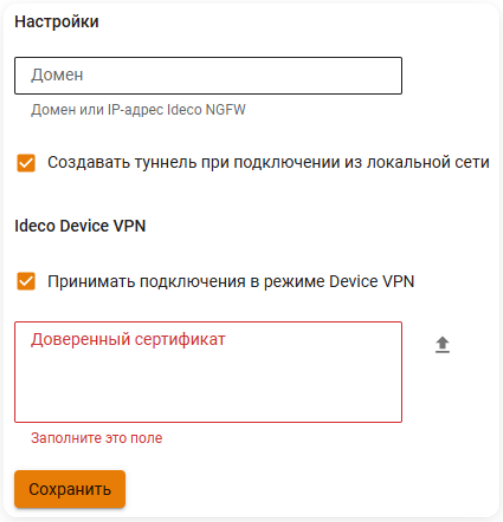
Чтобы подключить устройство к Ideco NGFW в режиме Device VPN, выполните действия:

1. Перейдите в раздел **Пользователи → Ideco Client**.

2. Введите домен или IP-адрес Ideco NGFW и включите настройку **Создавать туннель при подключении из локальной сети**, если устройства пользователей находятся в локальной сети.

3. Включите настройку **Принимать подключения в режиме Device VPN**.

4. Загрузите доверенный сертификат в формате `.pem` и нажмите **Сохранить**. Процесс создания сертификата описан в статье Создание сертификатов для Device VPN:



5. Установите Ideco Client на устройство пользователя.

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.

> 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:

Для Windows

Откройте командную строку от имени администратора и введите:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --set-devicevpn-cert-path=<абсолютный путь до файла сертификата> --set-devic
```

Для вывода заданных параметров в командную строку воспользуйтесь командой:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --print-devicevpn-config=True
```

Для Linux

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient.sh --set-devicevpn-cert-path=<абсолютный путь до файла сертификата> --set-d
```

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-devicevpn-cert-path=<абсолютный путь до файла сертификата> --set-devi
```

Для вывода заданных параметров в консоль воспользуйтесь командой:

```
(sudo) <абсолютный путь до IdecoClient>/IdecoClient --print-devicevpn-config=True
```

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 в дальнейшем. Ideco NGFW извлекает имя пользователя из поля **Common Name** сертификата.

При неудачной конфигурации Device VPN служба Ideco Client будет постоянно пытаться подключиться к Ideco NGFW. 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 убедиться, что подключение Device VPN выполнено.

Создание сертификатов для Device VPN

> В статье описан процесс создания сертификатов с использованием OpenSSL для подключения по Device VPN между Ideco NGFW 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*:

```
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.

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:

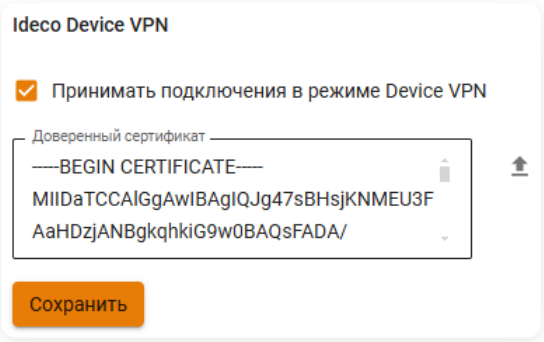
- **A challenge password []** - пароль для дополнительной аутентификации. Рекомендуем оставить поле пустым.
- **An optional company name []:** - полное юридическое название организации.

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.

5. В разделе **Пользователи** → **Ideco Client** в поле **Доверенный сертификат** загрузите созданый сертификат `ideco-dvpn_root-ca.pem` без приватного ключа:



После этого корневой сертификат будет необходим для создания пользовательских сертификатов.

Создание пользовательского сертификата для конечного устройства

1. Сгенерируйте приватный ключ без применения шифрования (в дальнейшем незашифрованный ключ размещается 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.

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)** - название региона или области (например, Moscow).
- **Locality Name (eg, city) [Default City]** - название города (например, Saint Petersburg).
- **Organization Name (eg, company) [Default Company Ltd]** - название организации.
- **Organizational Unit Name (eg, section) []** - название подразделения организации.
- **Common Name (eg, your name or your server's hostname) []** - 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. Создайте файл **client1-dvpn.ext** для генерации сертификата. Включите в него параметры:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
```

5. 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.

6. Проверьте, что сертификат был успешно создан командой:

```
openssl x509 -text -noout -in client1-dvpn.crt
```

- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат;
- Сертификат должен иметь атрибут `CA:FALSE` и `Subject Key Identifier`.

7. Объедините приватный ключ и сертификат пользовательского устройства:

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

```
Get-Content client1-dvpn.key, client1-dvpn.crt | Set-Content 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.

8. Сертификат `client1-dvpn.pem` с приватным ключом внутри, полученный на этом этапе, устанавливается на пользовательском устройстве и используется в параметрах Ideco Client.

Балансировка и редиректы VPN-подключений

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.

При указании в параметре `target` SRV-записи `.` подключение происходить не будет, и 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 кнопки **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. Затем происходит сортировка сначала по параметру SRV-записи `priority`, затем при равенстве параметров `priority` у двух и более записей происходит сортировка 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.

Алгоритм работы Ideco Client при редиректах

После формирования списка для подключения Ideco Client пытается подключиться к серверам из списка. Если при попытке подключения отправлен редирект с кодом ответа 302, то Ideco Client будет пытаться подключиться по указанному в редиректе адресу до первой успешной установки соединения.

Если при подключении к серверу в ответе приходит редирект с кодом ответа 302, то для полученного в редиректе адреса поиск SRV-записей производиться не будет. 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.

Подробнее о работе Ideco Client при редиректе в статье. Обработка запросов с редиректом позволяет использовать VPN-балансировщик для распределения нагрузки между несколькими NGFW.

Кастомная настройка Ideco Client

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

- Запрет на создание новых профилей;
- Запрет на сохранение пароля;
- Запрет на редактирование профиля;
- Установка профиля по умолчанию;
- 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:

```
{
    "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.
- `"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 его значение 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.

Ideco NGFW использует имя входа пользователей AD с атрибутом `sAMAccountName` (SAM). Если на AD используется атрибут `userPrincipalName` (UPN), необходимо, чтобы атрибуты SAM и UPN были идентичны. Различия в SAM и UPN приведут к проблемам с аутентификацией пользователей на NGFW.

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.

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 True
```

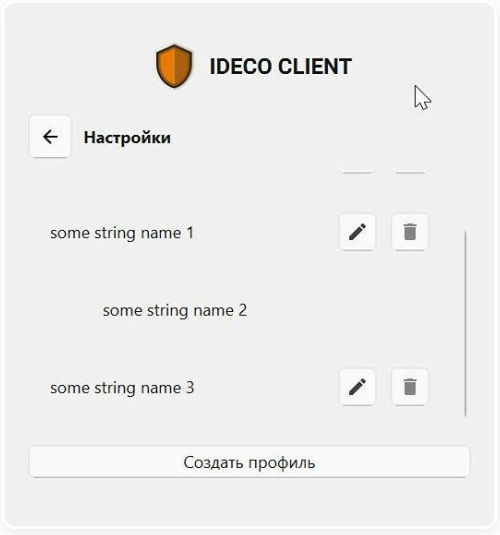
Linux или MacOS

Откройте терминал и выполните команду:

```
sudo IdecoClient --reset-json-config True
```

Примеры настроек файла конфигурации

Запретить пользователю редактировать преднастроенный профиль



Профиль **some string name 2** создан в файле конфигурации и его 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 и их можно редактировать или удалять.

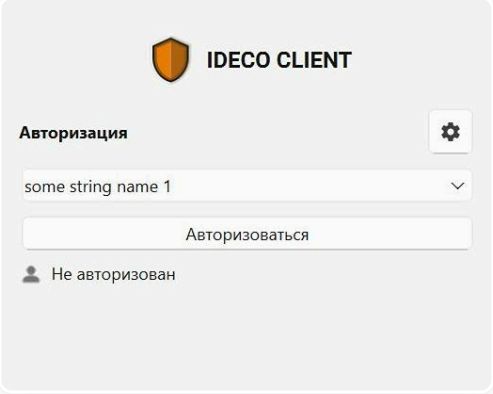
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "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.
- `"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.
- `"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.
- `"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:

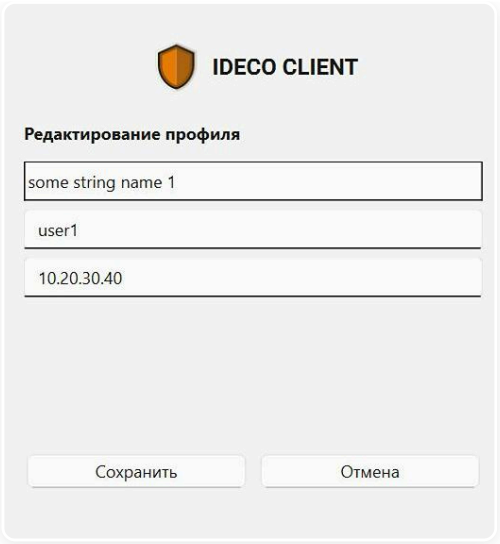
```
{
    "profiles": [
        {
            "id": "a78cb502-f0d5-4ce5-84ab-aaf7a90kkac6",
            "source": "json",
            "name": "some string name 2",
            "data": {
                "login": "user2",
                "type": "password",
                "server": "10.20.30.40"
            },
            "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.
- `"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.
- `"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.
- `"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.
- `"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.

Профили устройств

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

- 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

- Операционная система
- Пакет обновлений Windows
- Антивирус
- Межсетевой экран
- Процесс, запущенный на устройстве
- Запущенная служба Windows
- Ключ реестра Windows

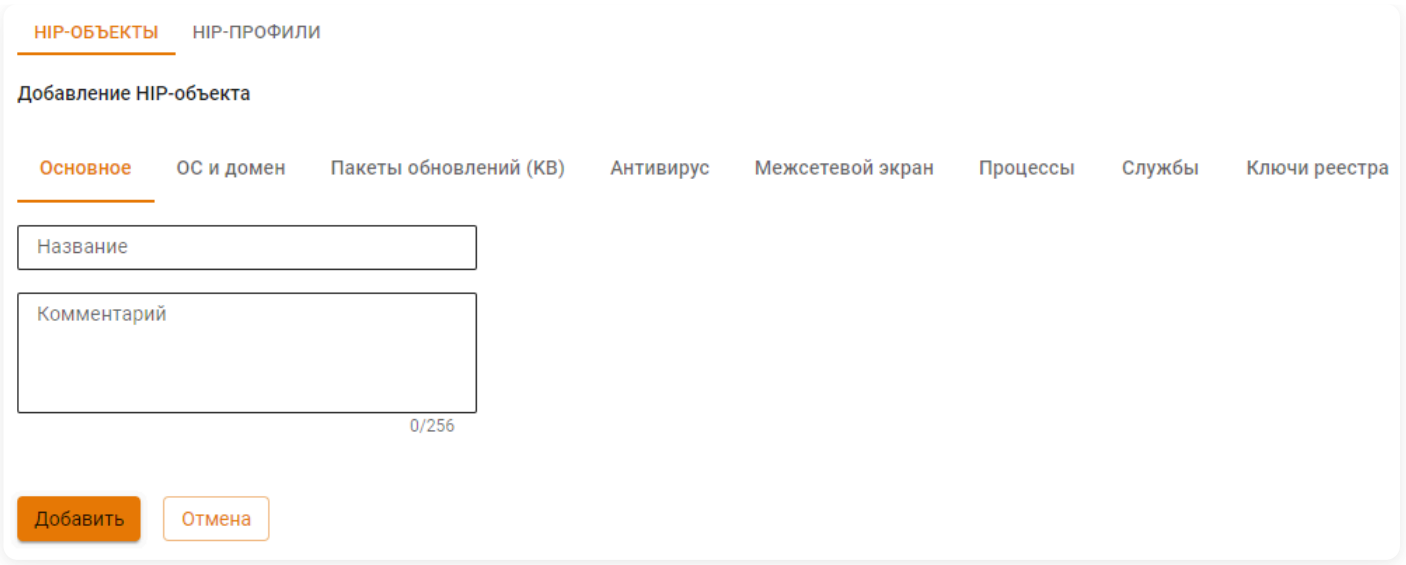
HIP-объекты

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.

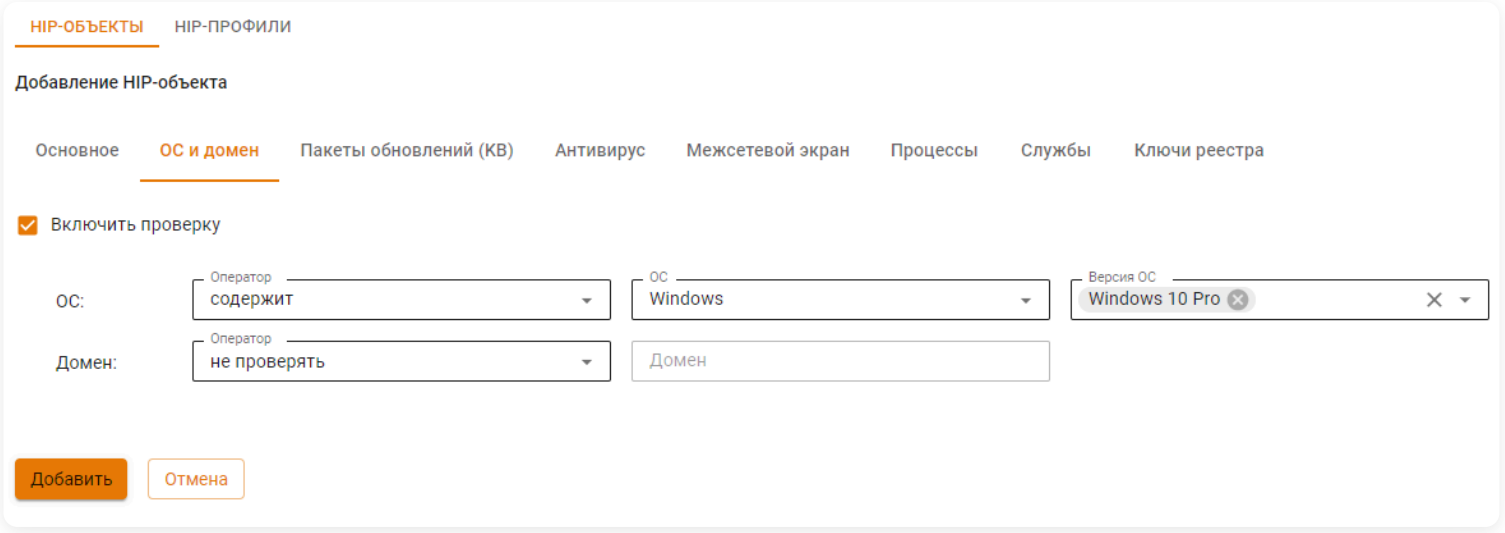
Для создания HIP-объекта выполните действия:

1. Перейдите в **Профили устройств** → **HIP-объекты** и нажмите **Добавить**.

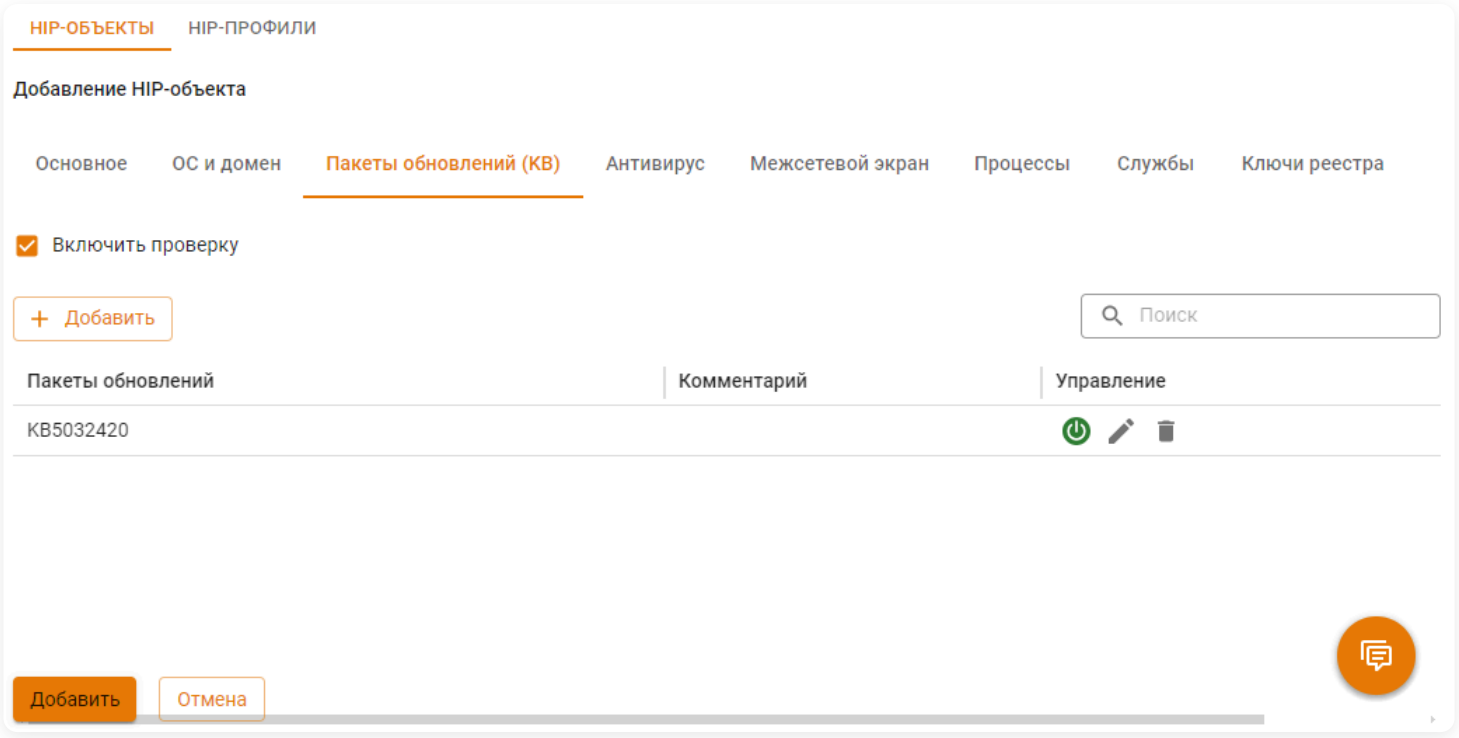
2. Введите **Название HIP-объекта** и выберите критерии для проверки:



3. Нажмите **Включить проверку** для проверки выбранного критерия и заполните поля, указав оператор (**Содержит**, **Не содержит**, **Не проверять**):



Критерий может не содержать оператор:



4. После этого 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

HIP-профили

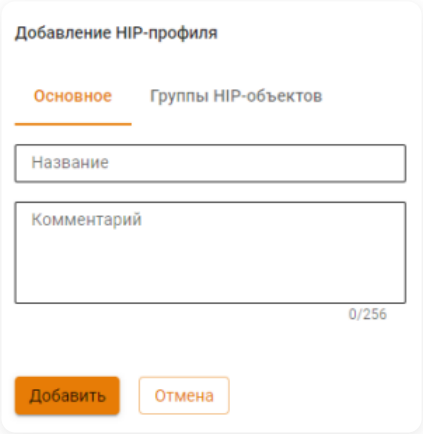
На вкладке создаются HIP-профили, состоящие из сгруппированных с помощью логических операций HIP-объектов И/ИЛИ.

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.

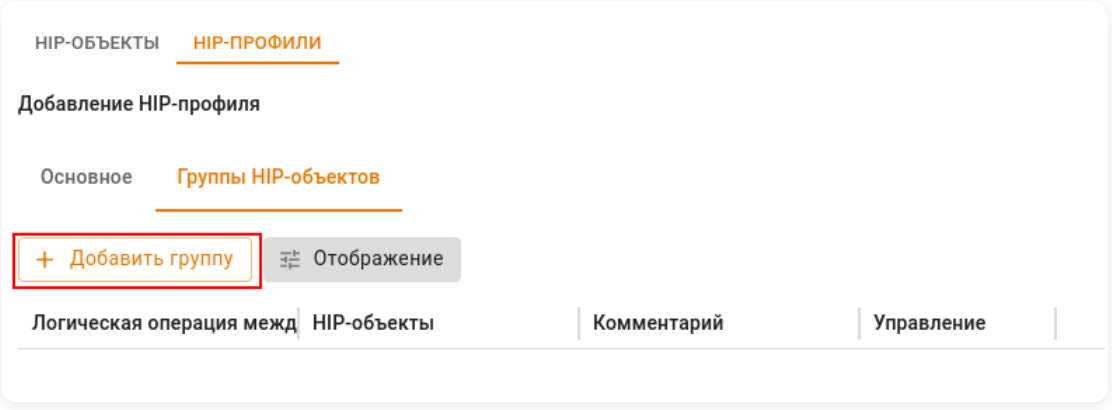
Для создания HIP-профиля выполните действия:

1. Перейдите в раздел **Профили устройств** → **HIP-профили** и нажмите **Добавить**.

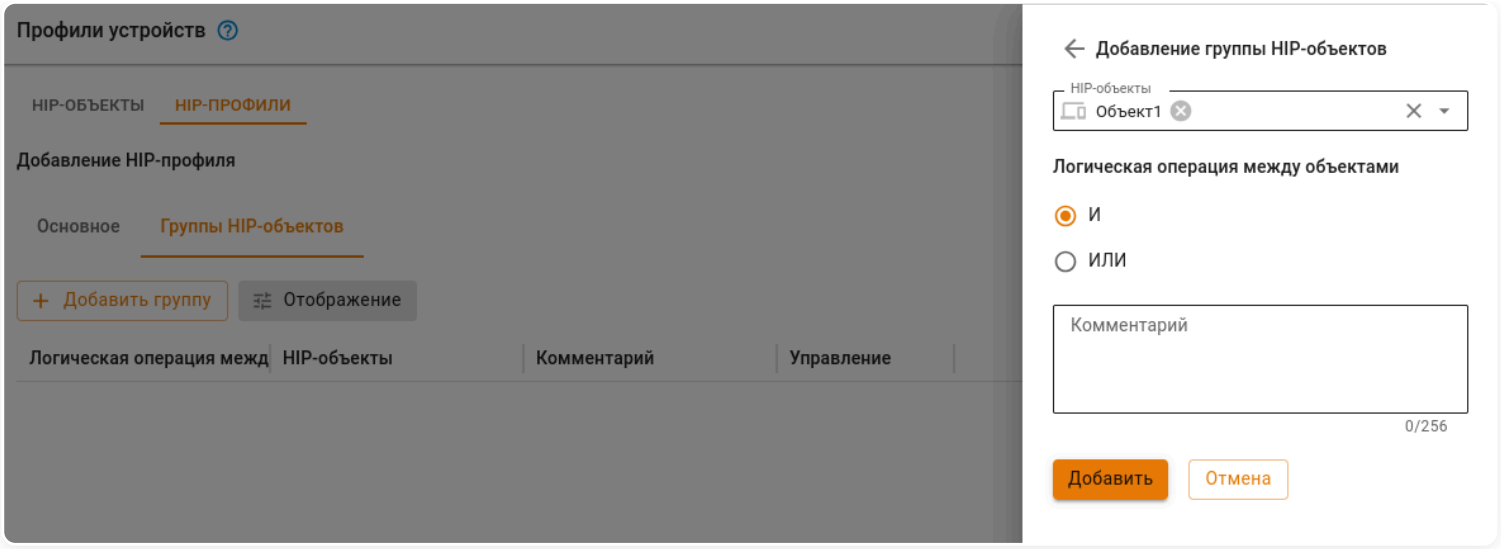
2. Введите **Название HIP-профиля**:



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 правиле FORWARD **Файрвола**. 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 **Файрвола**. Чтобы с помощью профилей ограничить или разрешить доступ к ресурсами сети, необходимо:

1. Создать HIP-объекты.

2. Сгруппировать созданные HIP-объекты в HIP-профилей.

3. В разделе **Правила трафика** → **Файрвол** → **FORWARD** создать и включить правило с использованием одного или нескольких профилей, созданных в пункте 2.

Проверка профилей происходит каждые 15 минут.

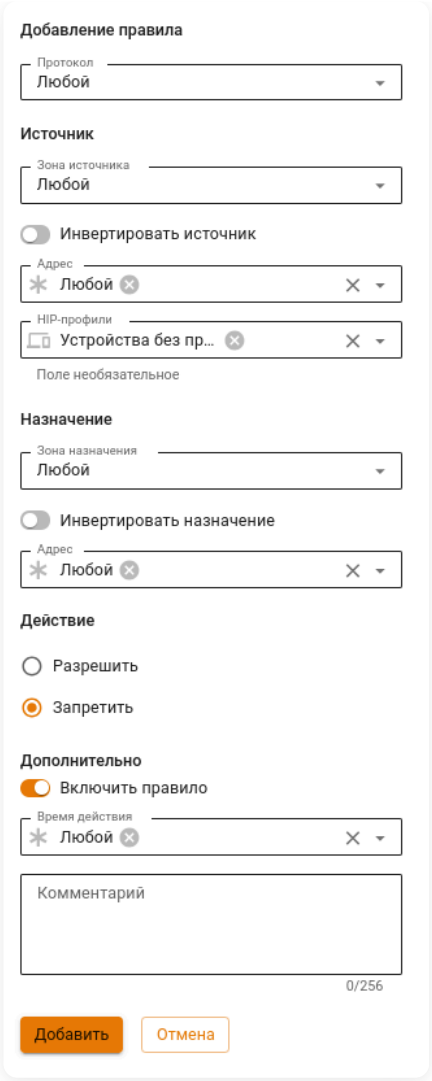
Примеры использования

Запрет доступа к сети устройствам без профиля

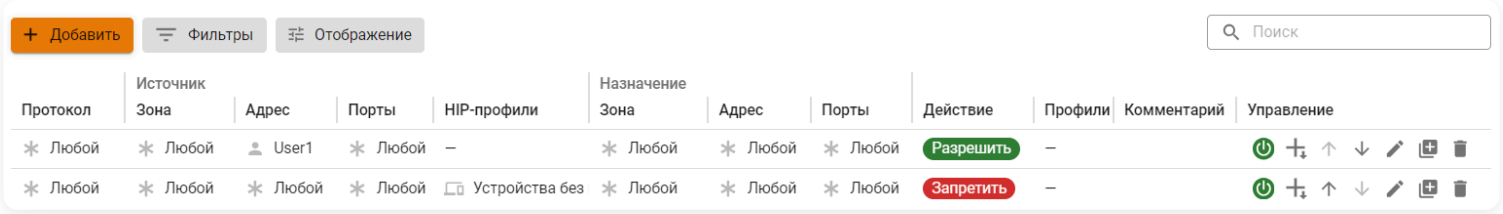
Устройствам, которые не прошли проверку на соответствие ни одному из созданных HIP-профилей, назначается специальный HIP-профиль **Устройство без профиля**. Доступ таких устройств к сети можно ограничить правилом **Файрвола**. Для этого:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD**.

2. Создайте и включите правило вида:



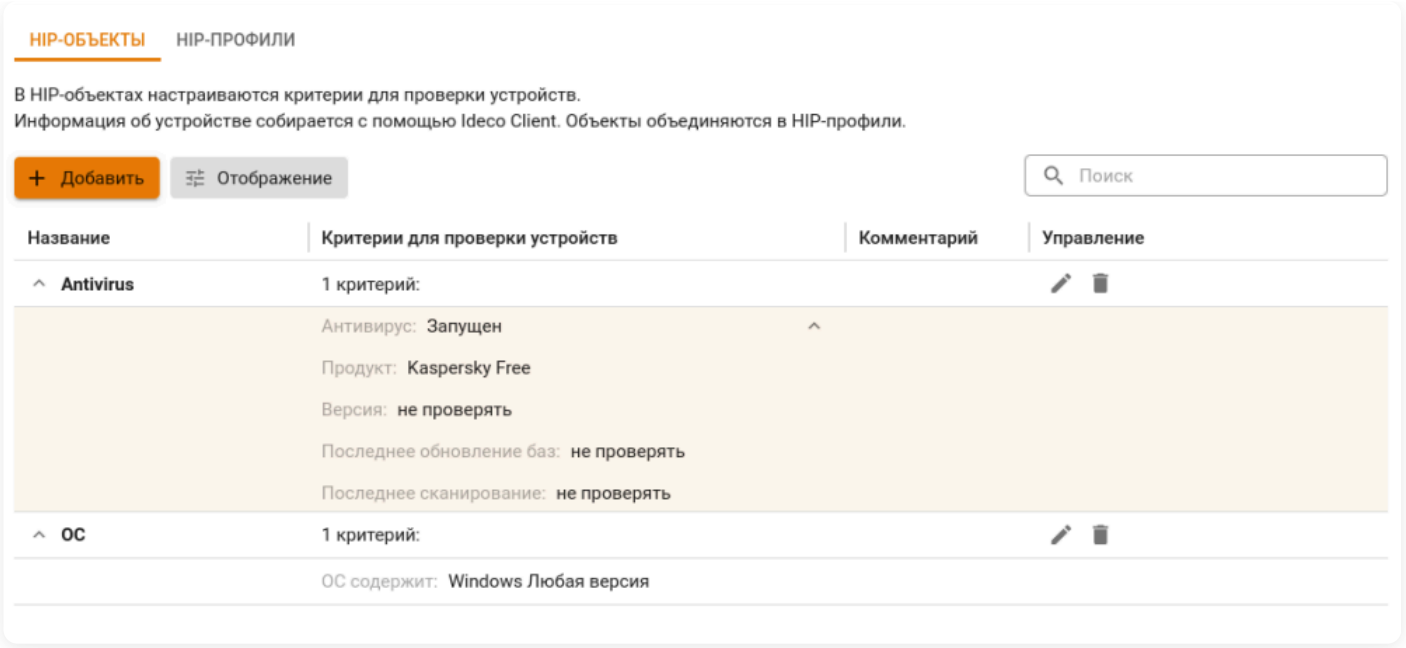
Важно!
Если в таблице правил **Файрвола** выше запрещающего правило находится другое правило, которому соответствует трафик одного или нескольких устройств без профиля (например, правило для пользователя или группы пользователей без указания HIP-профиля), то к трафику будет применено правило, расположенное выше в таблице. Например:



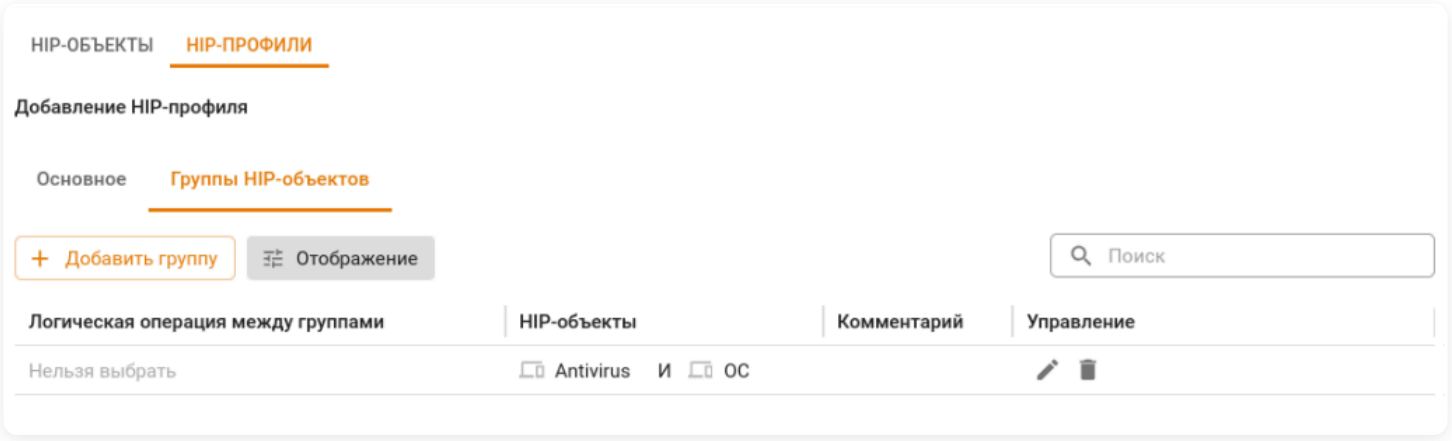
Ограничение доступа устройств к сети

В качестве примера настроим **Файрвол** так, чтобы пользователи имели доступ к сети, только если их устройства соответствуют HIP-профилю `Profile1`. Для этого:

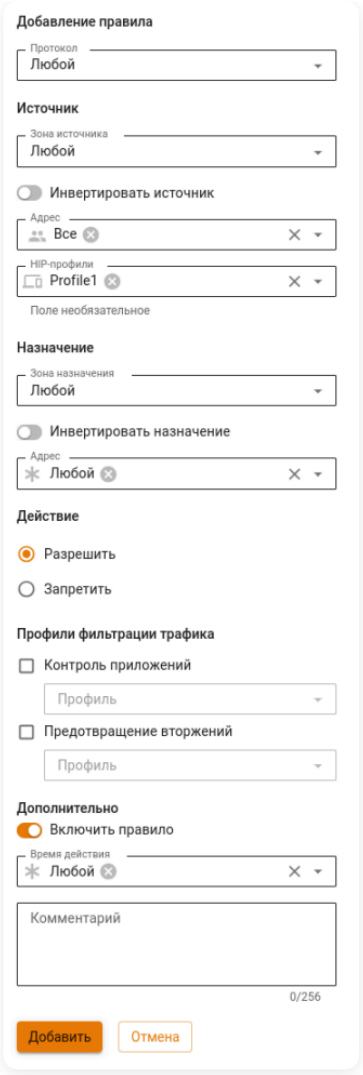
1. Перейдите в раздел **Пользователи** → **Профили устройств** → **HIP-объекты** и создайте требуемые HIP-объекты:



2. Перейдите на вкладку **HIP-профили** и создайте профиль с созданными ранее HIP-объектами:



3. Перейдите в раздел **Правила трафика** → **Файрвол** → **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.

Active Directory/Samba DC

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Название службы раздела **Active Directory/Samba DC**: `ideco-ad-backend`, `ideco-ad-log-collector@<имя домена>`.

Список служб для других разделов доступен по ссылке.

При интеграции импортируются учетные записи и номера телефонов пользователей, исключая пароли. При аутентификации пользователей проверка осуществляется средствами Active Directory или Samba DC соответственно.

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, перейдите в раздел Управление сервером → Терминал и выполните команду:

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

Особенности интеграции с несколькими доменами

- Из дерева контроллеров домена в Ideco NGFW импортируются данные только того контроллера, для которого был запущен импорт пользователей.
- При импорте пользователей из разных доменов необходимо убедиться, что учетные записи не имеют одинаковых логинов. В противном случае система выдаст сообщение об ошибке.
- 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 Ideco NGFW).

Ввод сервера в домен

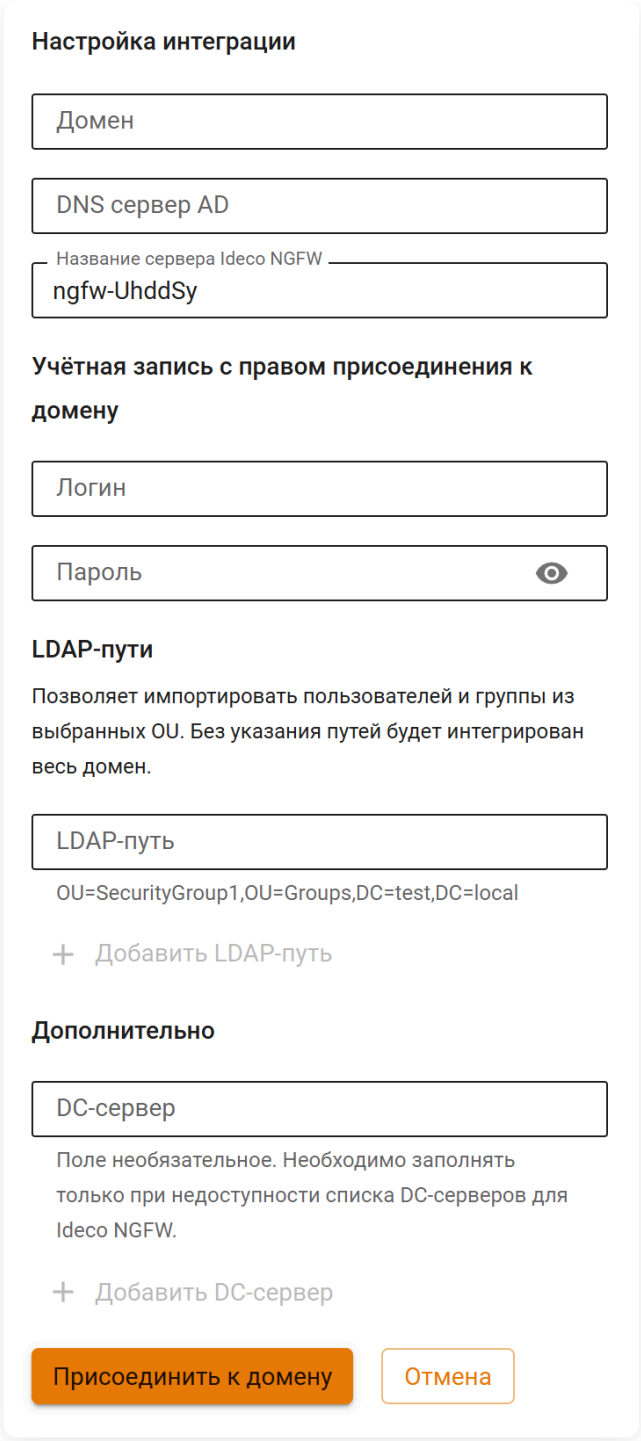
Перед вводом в домен:

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

Выполните действия:

1. Перейдите на вкладку **Пользователи** → **Active Directory/Samba DC**.

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



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

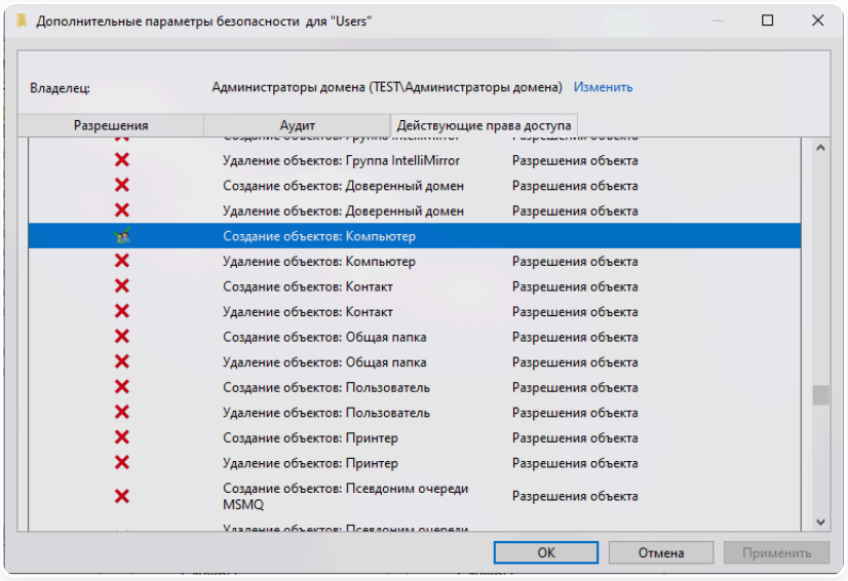
- **SSO через AD и ALD Pro** с токенами NTLM.
- VPN (IKEv2, SSTP, L2TP/IPsec, PPTP).
- Ideco Client с аутентификаций по логину и паролю.

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, длина которого не должна превышать 64 символа. Например: `mydomain.example`.
- **DNS-сервер AD** - адрес сервера, обладающий ролью DNS-сервера в контроллере домена, доступный с локального интерфейса Ideco NGFW.
- **Название сервера Ideco NGFW** - имя компьютера, под которым Ideco NGFW 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. 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**.

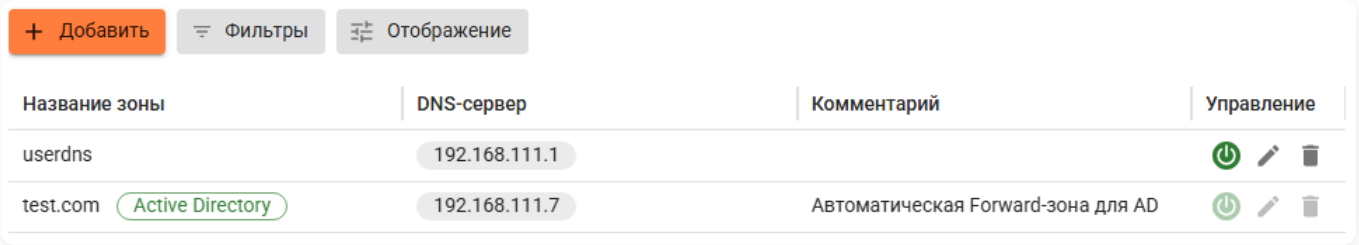
- **LDAP-пути** - LDAP-пути для импорта пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет импортировать только нужные группы пользователей, чтобы избежать импорта всего дерева пользователей AD.
- **DC-сервер** - контроллер домена. Заполняется только при недоступности контроллера домена для Ideco NGFW.

3. Нажмите **Присоединить к домену**. Процесс присоединения к домену может занять до одной минуты.

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

Настройка DNS для разрешения имен локального домена

В Ideco NGFW Forward-зона DNS создается в **Сервисы** → **Защита и управление DNS** → **Forward-зоны** автоматически при вводе сервера в домен:



При такой настройке компьютеры могут использовать Ideco NGFW 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 из домена перейдите в **Пользователи** → **Active Directory/Samba DC** и нажмите напротив интеграции. После подтверждения:

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

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

Полезные ссылки

Импорт пользователей

Аутентификация пользователей AD/Samba DC

Импорт пользователей

Ideco NGFW также поддерживает интеграцию с AD-администраторами. Подробные инструкции по настройке описаны в статье Администраторы.

Импортировать группы пользователей контроллера домена можно в специально созданные группы пользователей в Ideco NGFW. Их название может быть произвольным.

Особенности импорта пользователей в Ideco NGFW

- После импорта пользователи будут автоматически синхронизироваться с контроллером домена каждые 15 минут.
- Можно импортировать разные группы пользователей контроллера домена в различные группы Ideco NGFW. Это позволит удобно назначать правила фильтрации для каждого модуля фильтрации.
- Пользователи контроллера домена могут быть импортированы только в одну группу Ideco NGFW. При этом пользователь будет добавлен в группу, в которую был импортирован последним.
- В процессе импорта пользователей также импортируются номера телефонов, которые можно использовать для двухфакторной аутентификации.

Перед импортом пользователей убедитесь, что:

- Учетные записи AD не имеют одинаковых логинов с локальными учетными записями. В противном случае система выдаст сообщение об ошибке.
- Права устройств пользователей не ограничены на чтение.

Импорт учетных записей из LDAP-каталога

В Ideco NGFW можно импортировать учетные записи из LDAP-каталога. Для этого используются протоколы LDAP и LDAPS. При этом последний не требует дополнительных настроек на стороне NGFW и используется автоматически в случае использования его на контроллере домена.

Для импорта пользователей выполните действия:

1. Создайте группу в дереве пользователей Ideco NGFW. Подробнее о создании групп - в статье **Управление пользователями**.

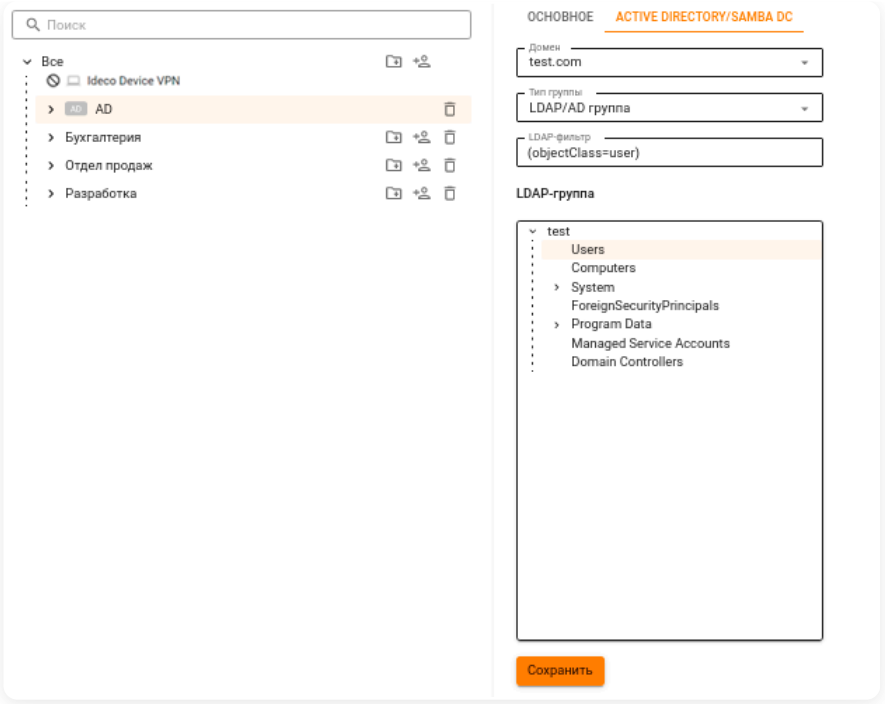
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC** в правой части экрана.

3. Выберите домен, из которого требуется импортировать пользователей.

4. В поле **Тип группы** выберите LDAP/AD группа.

5. При нажатии на поле **LDAP группа** будет отображен либо весь домен, либо группы, которые были указаны при вводе NGFW в домен. Выберите из него необходимую группу для импорта (можно выбрать корневую группу для импорта всего дерева).

6. Нажмите **Сохранить** (будет произведен импорт пользователей):



При необходимости воспользуйтесь фильтром запросов. Например, если в одних и тех же контейнерах находятся пользователи и компьютеры, а импортировать нужно только пользователей, то в поле **LDAP-фильтр** напишите: `(&(objectCategory=person)(objectClass=user))`

> Не стоит импортировать подгруппы уже импортированной группы, потому что они автоматически будут импортированы вместе с основной группой.

Импорт учетных записей из групп безопасности

1. Создайте группу в дереве пользователей Ideco NGFW.

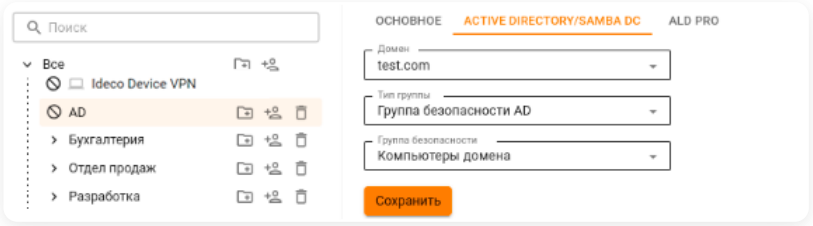
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC**.

3. В поле **Имя домена** выберите нужный домен.

4. В поле **Тип группы** выберите **Группа безопасности AD**.

5. В поле ниже из раскрывающегося списка выберите нужную группу безопасности.

6. Нажмите на кнопку **Сохранить**.



Если импортировались не все пользователи

Если импортировались не все пользователи, то включите режим совместимости. **Важно**: включенный режим совместимости импортирует пользователей медленнее.

Примеры включения через терминал и браузер:

Терминал

1. Авторизуйтесь командой:

```
curl -c /tmp/cookie -b /tmp/cookie -X POST https://адрес_сервера/web/auth/login -d '{"login": "логин", "password": "пароль",
```

2. Отправьте запрос на включение режима:

```
curl -c /tmp/cookie -b /tmp/cookie -X PATCH https://адрес_сервера/ad_backend/security_group_import_settings -d '{"compatibili
```

Браузер

1. Откройте веб-интерфейс Ideco NGFW и нажмите F12.

2. Перейдите на вкладку **Сеть** и нажмите на любой запрос.

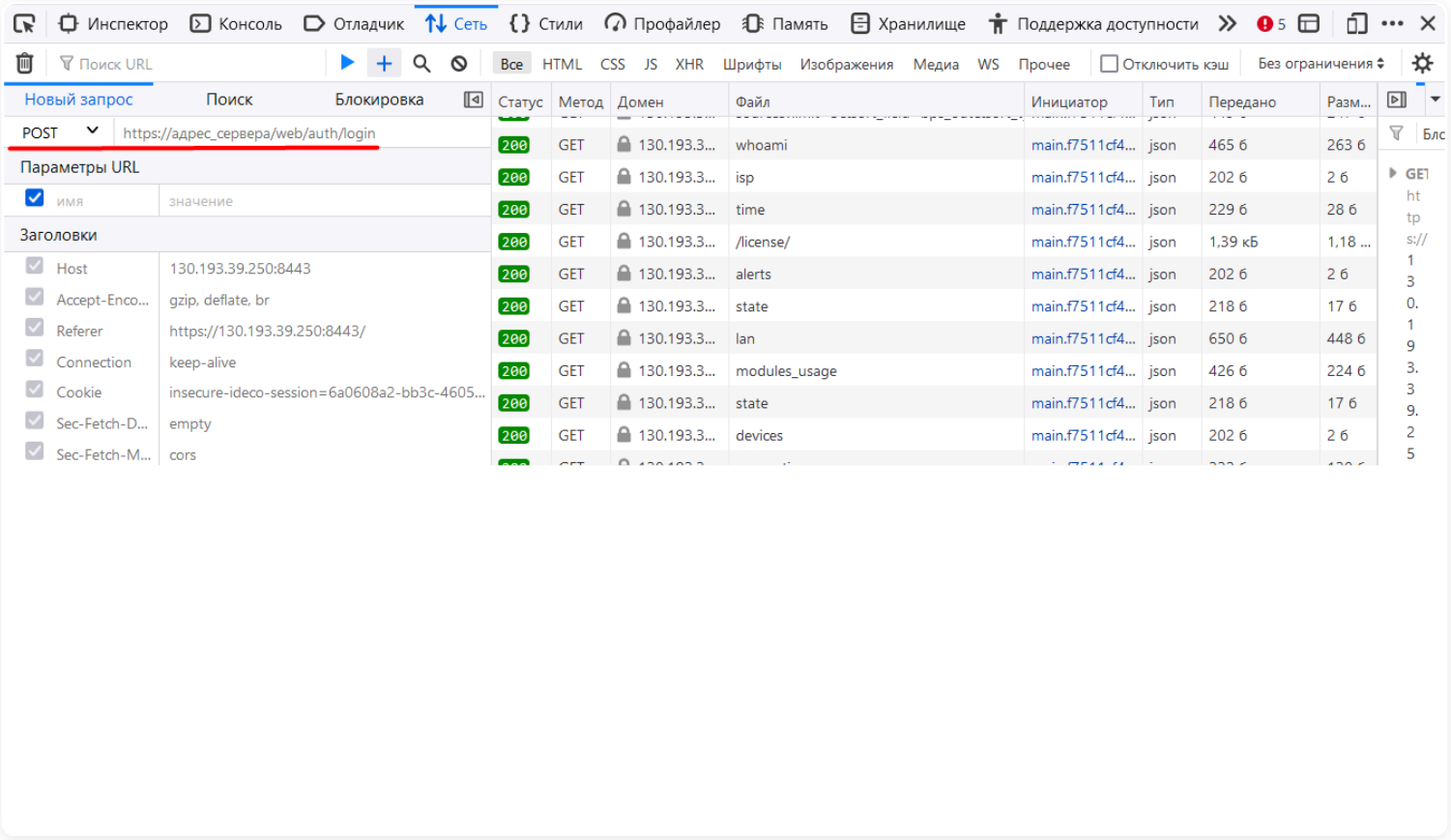
3. В появившемся окне перейдите на вкладку **Новый запрос**.

4. Отправьте запрос авторизации:

```
POST https://адрес_сервера/web/auth/login
```

Тело запроса:

```
{
    "login": "логин", "password": "пароль", "rest_path": "/"
}
```

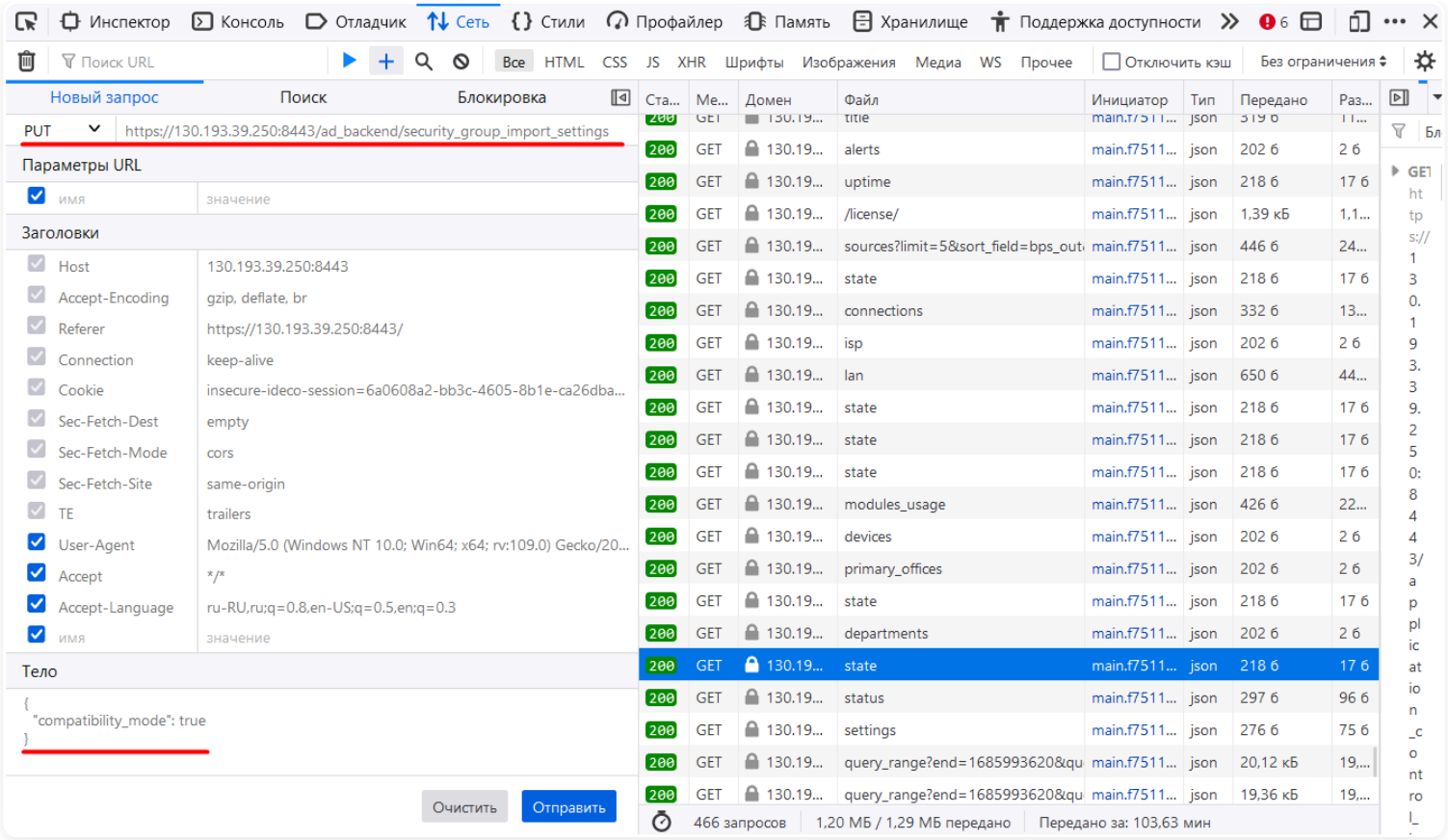


5. Отправьте запрос на включение режима:

```
PATCH /ad_backend/security_group_import_settings
```

Тело запроса:

```
{
  "compatibility_mode": true
}
```



Для выключения режима совместимости в теле запроса вместо `true` укажите `false`.

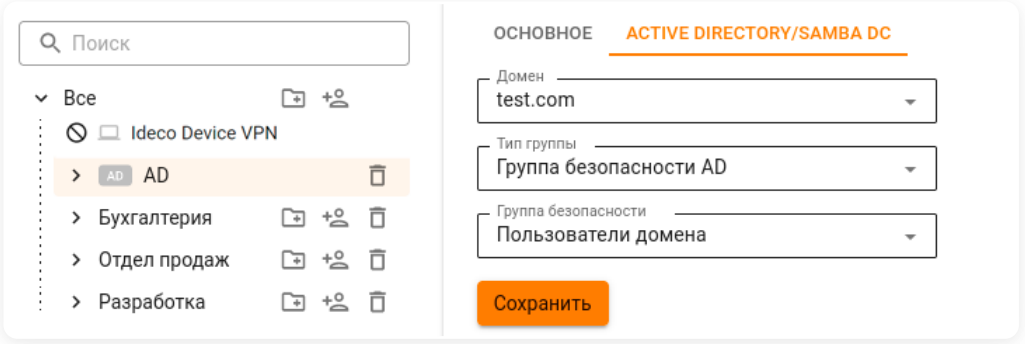
Настройка учетных записей и групп безопасности в качестве объектов фильтрации

Импортированные из AD/Samba группы безопасности и учетные записи можно использовать в качестве объектов фильтрации в разделах:

- Файрвол
- Контент-фильтр
- Ограничение скорости

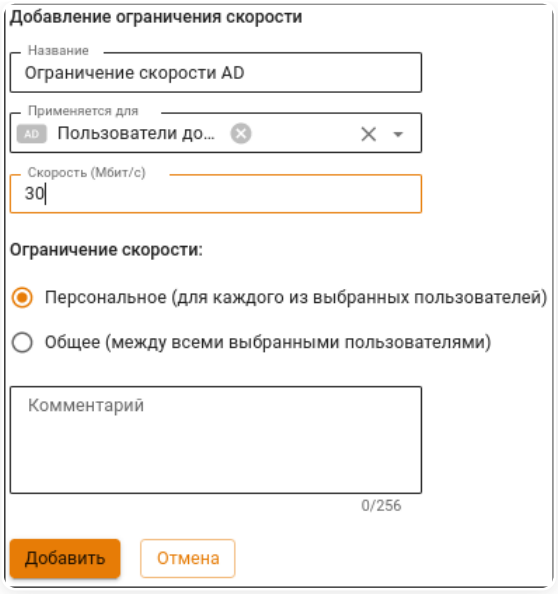
Пример использования учетной записи, импортированной из Active Directory, для ограничения скорости

1. Импортируйте из AD учетные записи или группы безопасности в разделе **Пользователи** → **Учетные записи** (подробнее в статье Импорт пользователей). В этом примере импортируется группа безопасности AD **Пользователи домена**:



2. Перейдите в раздел, в котором требуется использовать импортированную из AD группу или учетную запись. Например, в **Ограничение скорости**.

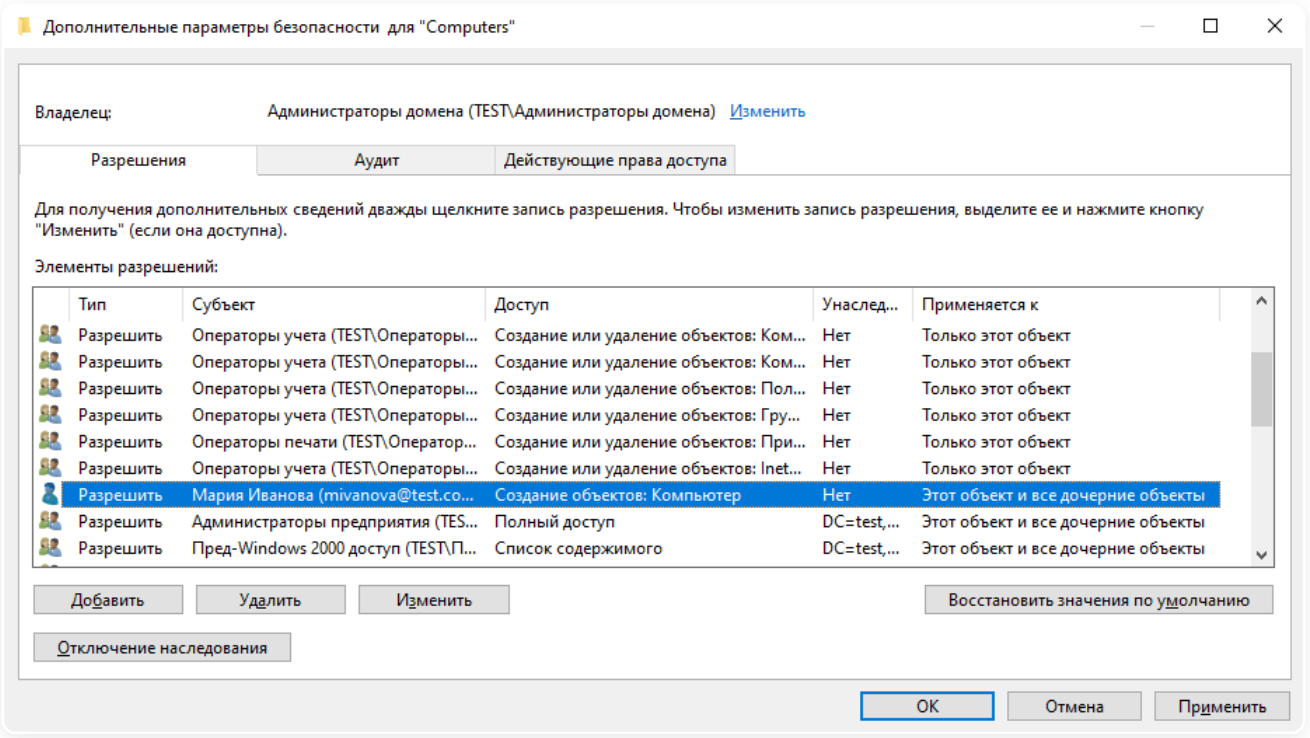
3. Заполните поля и нажмите **Добавить**:



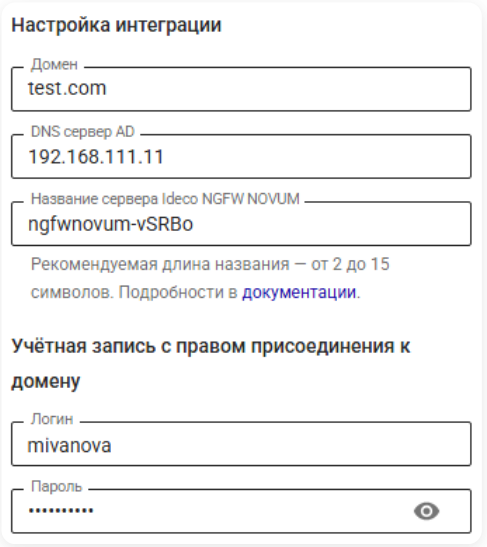
- **Название** - введите название правила, например, Ограничение для менеджеров.
- **Применяются для** - выберите из выпадающего списка отдельного пользователя и/или группу.
- **Скорость** (Мбит/с) - лимит скорости для выбранных пользователей.

Настройка прав для интеграции Active Directory

Для интеграции Ideco NGFW 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 в **Пользователи** → **Active Directory/Samba DC**:



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

Область применения	Необходимые права и атрибуты

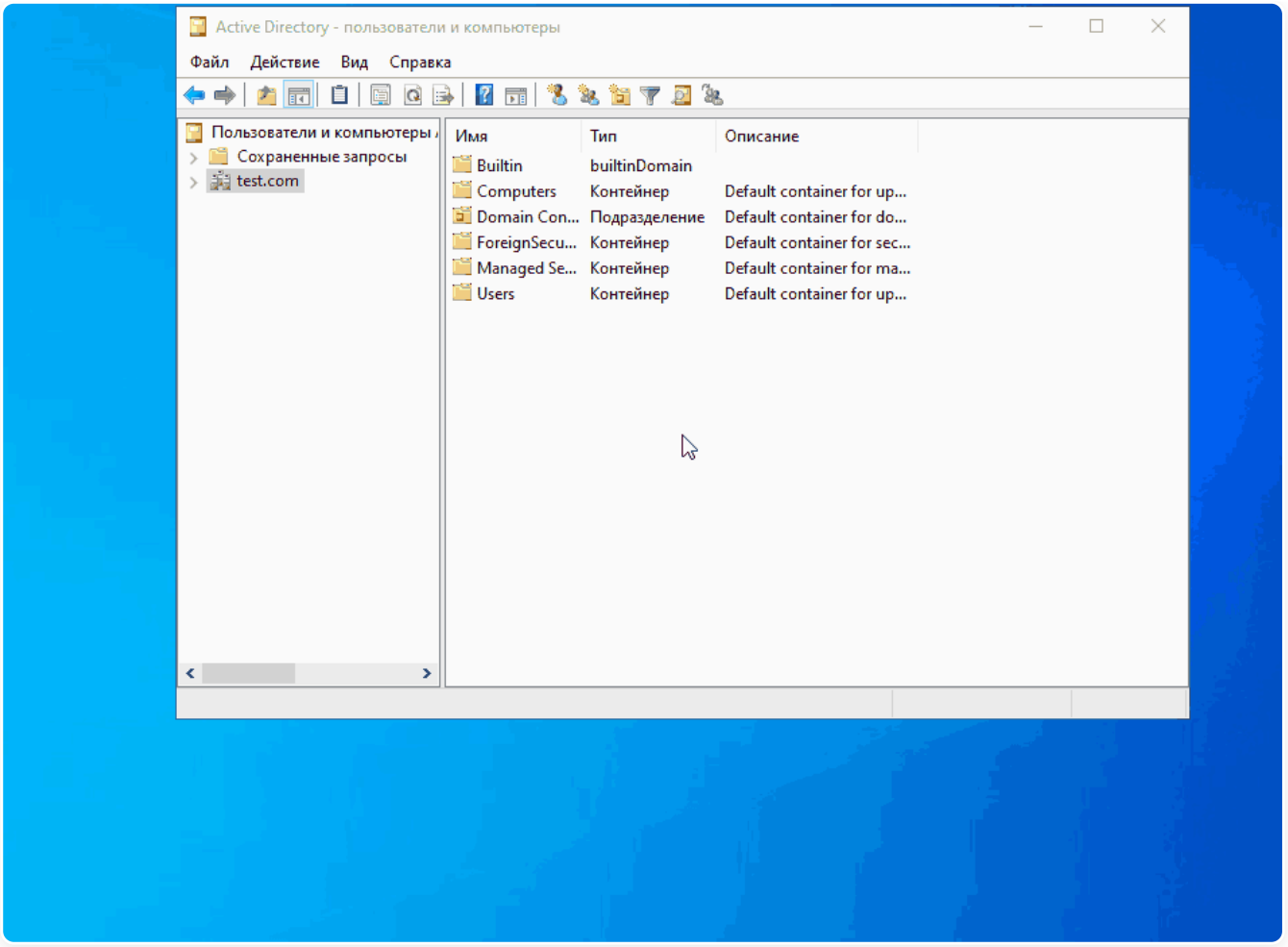
Поиск пользователей	• Предоставляет доступ **ReadProperty** к чтению атрибутов:
	  ◦ name
	  ◦ modifyTimeStamp
	  ◦ objectGUID
	  ◦ objectSid
	  ◦ cn
	  ◦ displayName
	  ◦ login
	  ◦ mobile
	  ◦ objectClass
	  ◦ userAccountControl
	  ◦ sAMAccountName
	  ◦ userPrincipalName
	  ◦ accountExpires
	  ◦ msDS-UserPasswordExpiryTimeComputed
	  ◦ 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**).

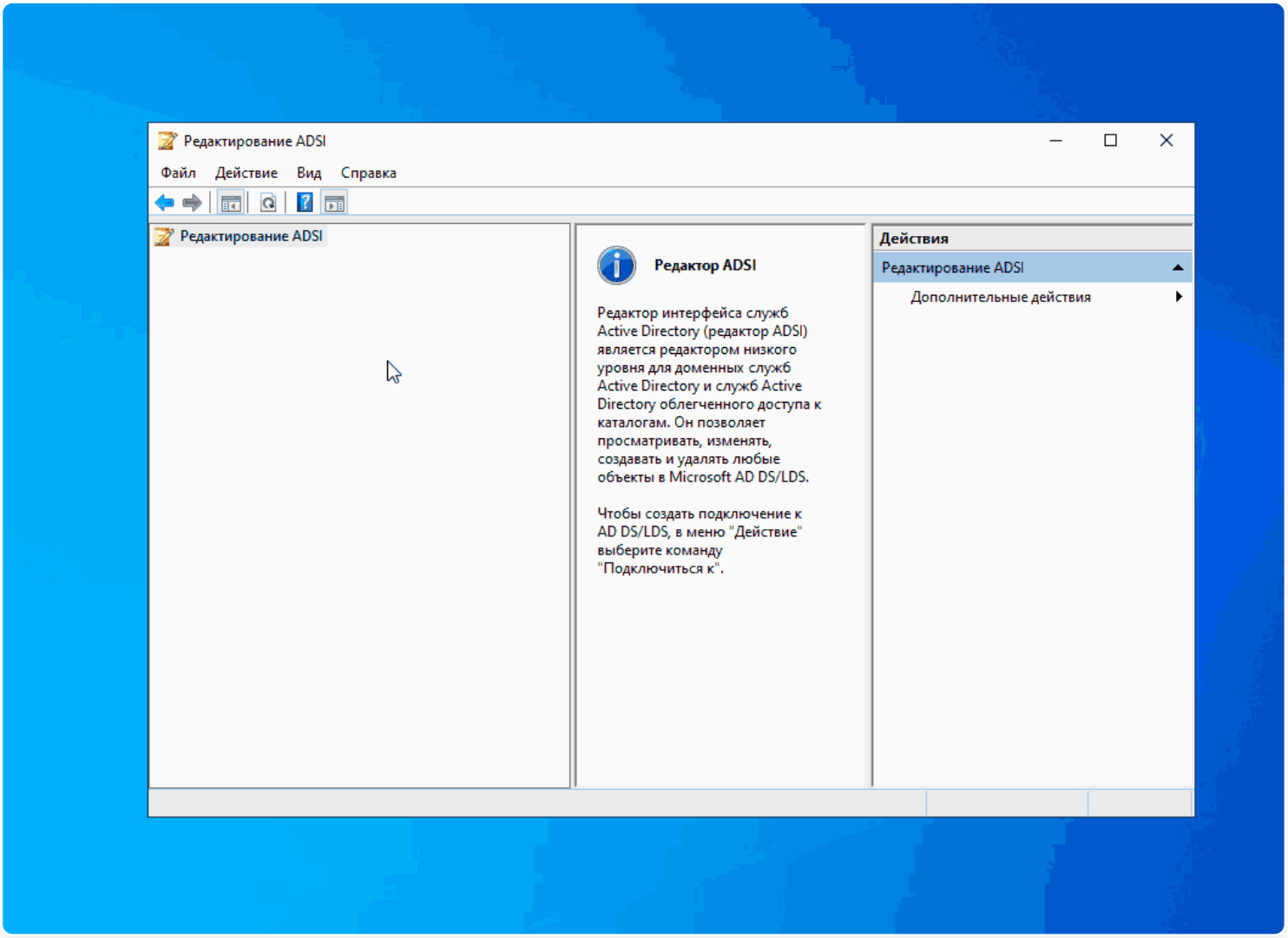
2. Нажмите правой кнопкой на объекте домена, выберите **Properties** → **Security** → **Advanced** (**Свойства** → **Безопасность** → **Дополнительно**).

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 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 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 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

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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

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

Ideco NGFW использует имя входа пользователей AD с атрибутом `sAMAccountName` (SAM). Если на AD используется атрибут `userPrincipalName` (UPN), необходимо, чтобы атрибуты SAM и UPN были идентичны. Различия в SAM и UPN приведут к проблемам с аутентификацией пользователей на NGFW.

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 пользователей терминальных серверов (с использованием Remote Desktop IP Virtualization на терминальном сервере).
- **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.

Особенности авторизации пользователей доверенных доменов

Если у домена, в который введен NGFW, настроено доверие с другим доменом, то пользователи доверенного домена смогут авторизоваться на NGFW 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

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

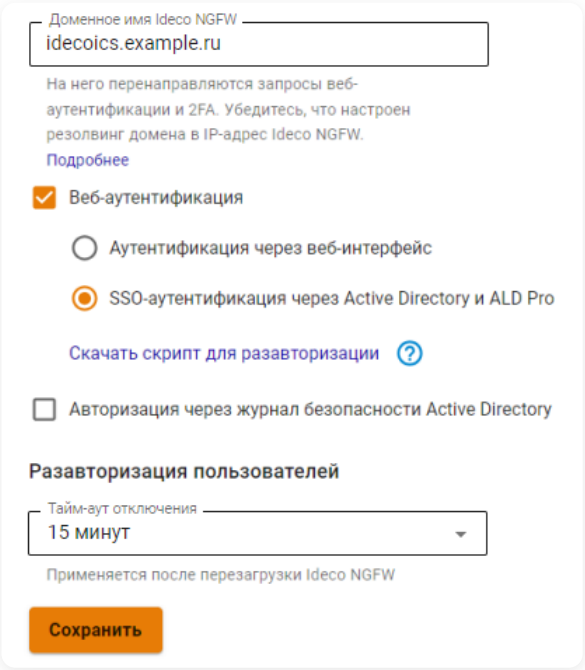
Настройка SSO-аутентификации

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

Список служб для других разделов доступен по ссылке.

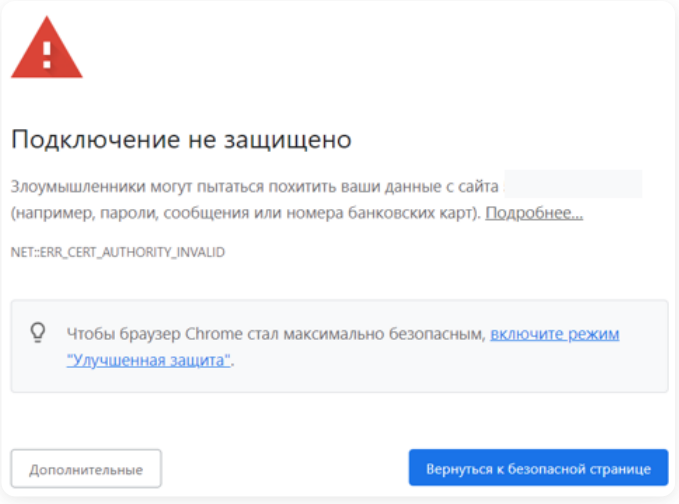
Настройка SSO-аутентификации на стороне NGFW

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



- **Доменное имя Ideco NGFW** - укажите доменное имя Ideco NGFW.
- **Веб-аутентификация** - включите настройку и выберите **SSO-аутентификация через Active Directory и ALD Pro** для авторизации с использованием токенов Kerberos или NTLM.
- **Авторизация через журнал безопасности Active Directory** - включите, если требуется, чтобы Ideco NGFW отслеживал события успешного входа в журнале безопасности AD и авторизовывал пользователя по ним, если трафик идет с того же IP-адреса.
- **Тайм-аут отключения** - установите тайм-аут разавторизации 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.

Для работы аутентификации через веб-браузер с использованием Kerberos или NTLM настройте Internet Explorer (остальные браузеры получат его настройки).

Настройка на стороне сервера Active Directory

Настройка аутентификации через веб-браузер

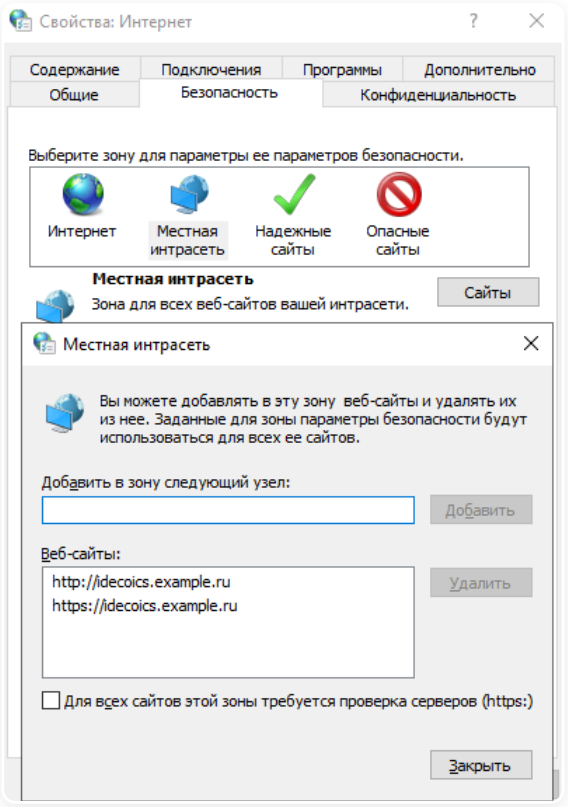
1. В поиск введите **Изменение параметров временных файлов Интернета**.

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

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

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

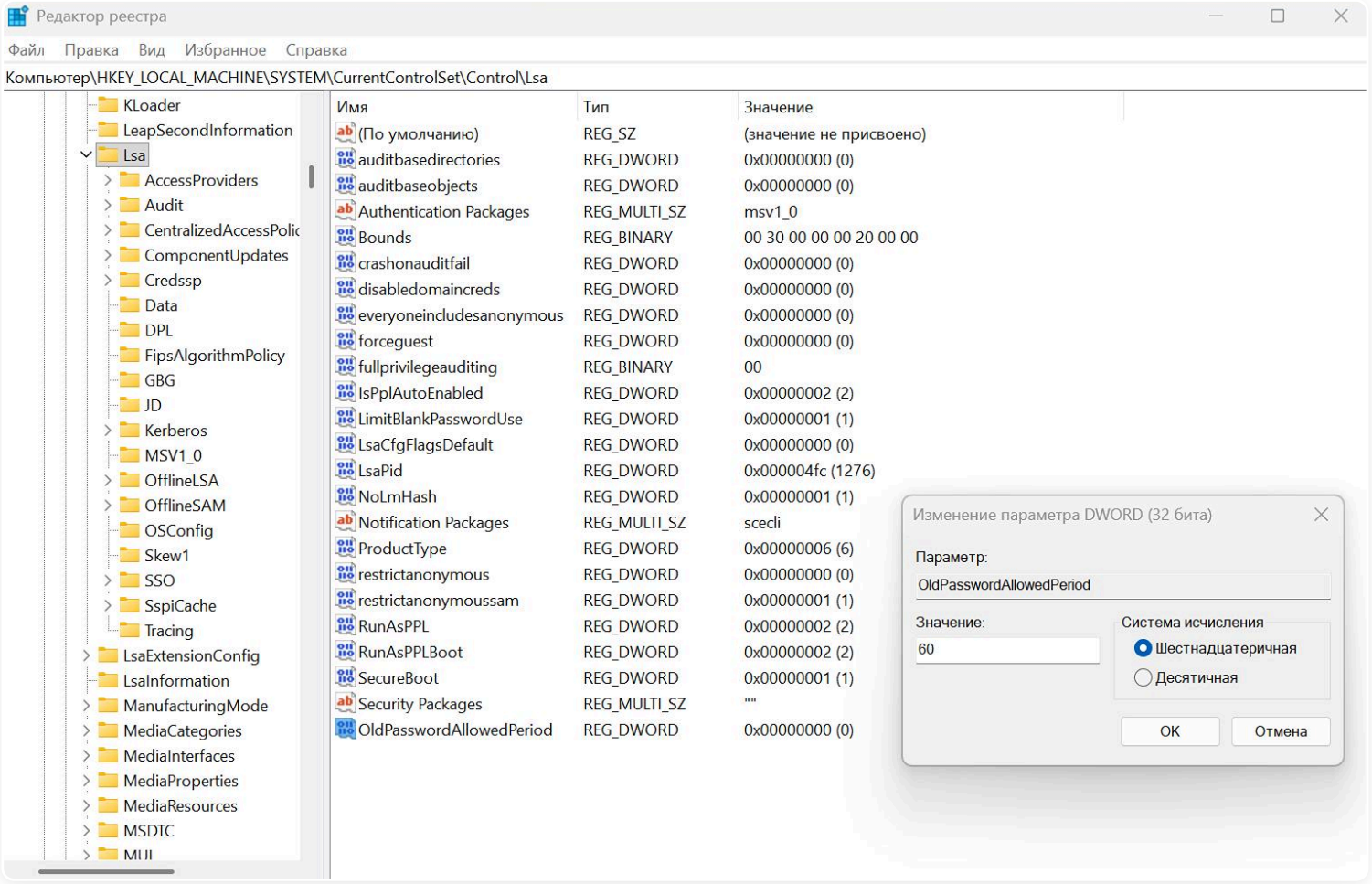
Пример ввода Ideco NGFW в домен `example.ru` под именем `idecoics`:



Особенности использования NTLM токенов

При использовании NTLM токенов для веб-аутентификации, а так же 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:



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.

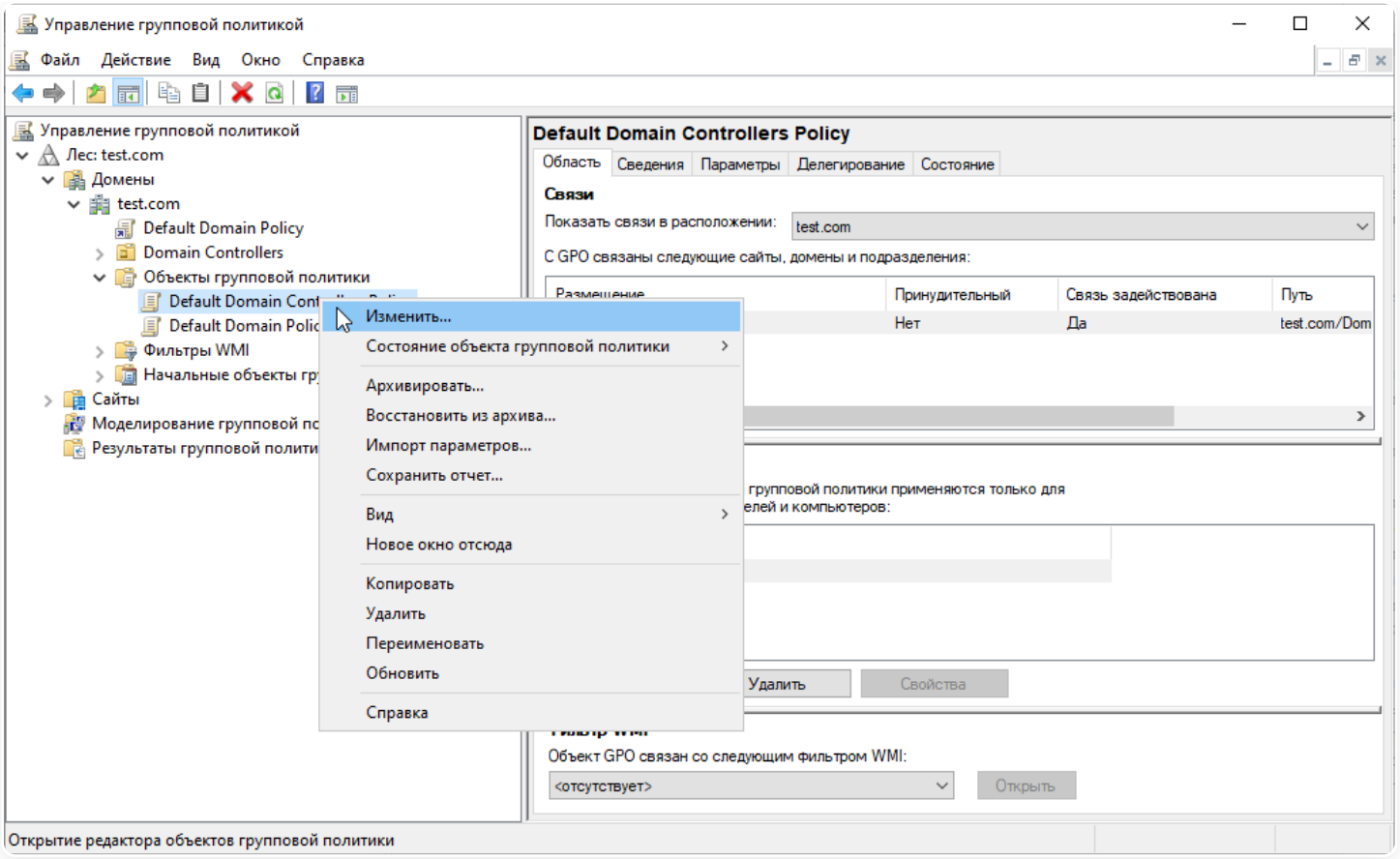
2. Перейдите по пути:

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:

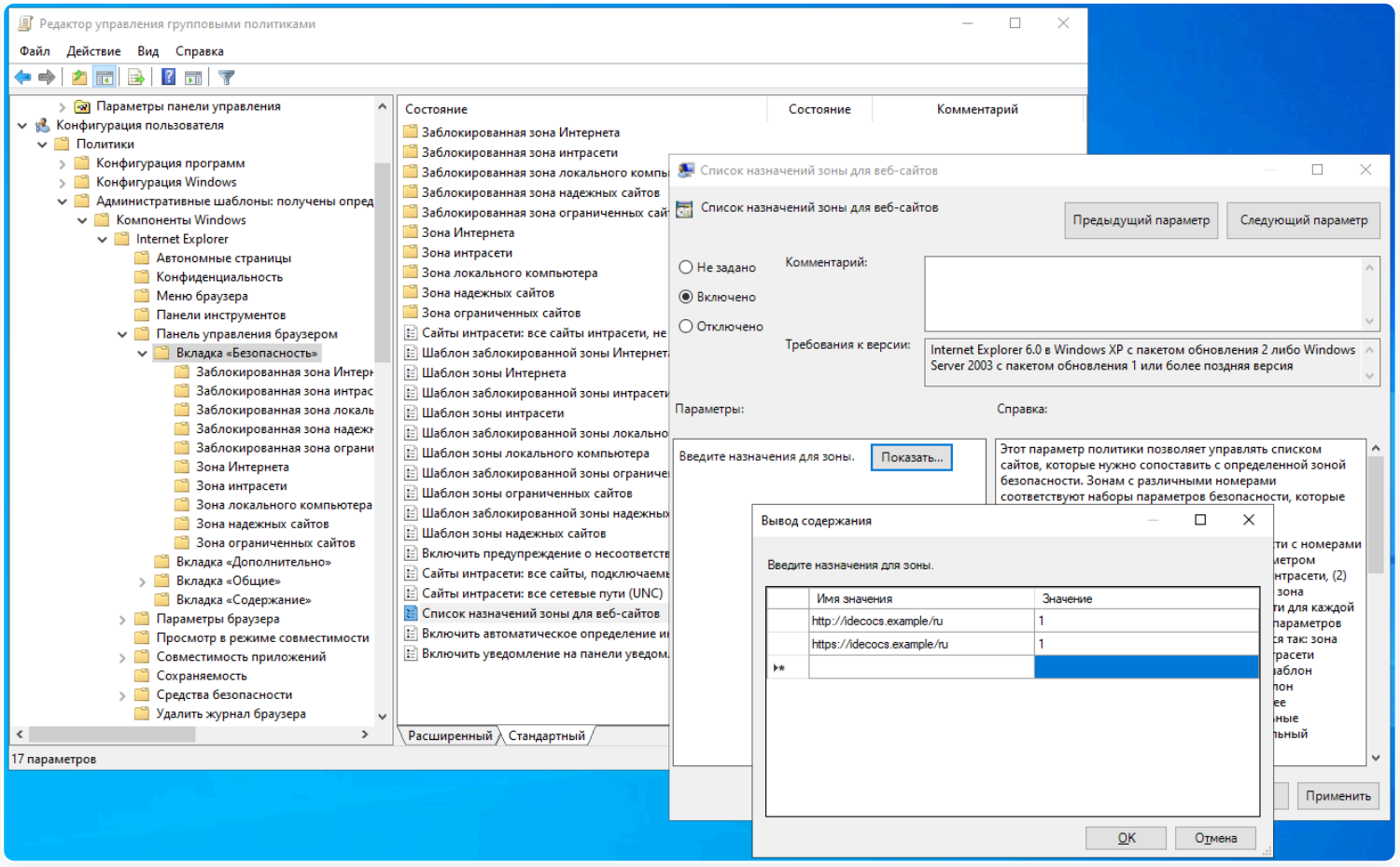
Англоязычная версия

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.

3. Введите назначение зоны для DNS-имени Ideco NGFW (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. Чтобы не делать это каждый раз, можно добавить корневой сертификат Ideco NGFW в доверенные корневые сертификаты устройства.

Настройка браузера Mozilla Firefox для веб-аутентификации по SSO или NTLM

Для использования браузера **Mozilla Firefox** на странице настроек (введите *about:config* в адресной строке) укажите следующие параметры:

- **network.automatic-ntlm-auth.trusted-uris** и **network.negotiate-auth.trusted-uris** добавьте адрес локального интерфейса Ideco NGFW (например, `idecoUTM.example.ru`).
- **security.enterprise_roots.enabled** в значении `true` позволит Firefox доверять системным сертификатам и авторизовать пользователей при переходе на HTTPS-сайты.

Настройка браузера Chromium для веб-аутентификации по SSO или NTLM

1. Откройте **Редактор реестра**.

2. Перейдите по пути `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Chromium` (для компьютера) или `HKEY_CURRENT_USER\SOFTWARE\Policies\Chromium` (для конкретного пользователя).

3. Создайте два новых ключа:

- Первый ключ должен иметь тип `REG_SZ`, имя `AuthServerAllowlist` и значение `*.имя_домена`.
- Второй ключ также должен иметь тип `REG_SZ`, имя `AuthNegotiateDelegateAllowlist` и значение `*.имя_домена`.

Настройка браузера Яндекс для веб-аутентификации по SSO или NTLM

1. Откройте **Редактор реестра**.

2. Перейдите по пути `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\YandexBrowser` (для компьютера) или `HKEY_CURRENT_USER\SOFTWARE\Policies\YandexBrowser` (для конкретного пользователя).

3. Создайте два новых ключа:

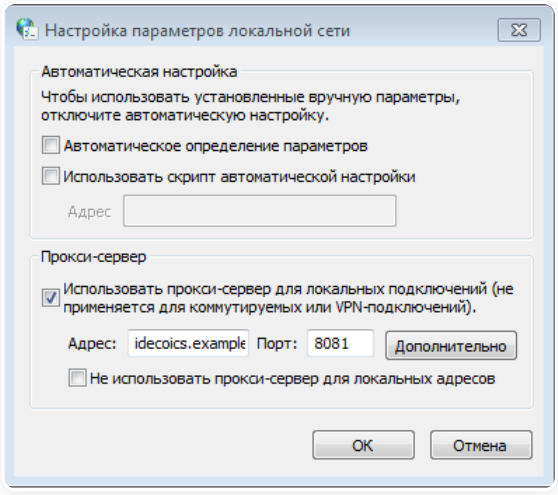
- Первый ключ должен иметь тип `REG_SZ`, имя `AuthServerAllowlist` и значение `*.имя_домена`.
- Второй ключ также должен иметь тип `REG_SZ`, имя `AuthNegotiateDelegateAllowlist` и значение `*.имя_домена`.

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**.

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



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:

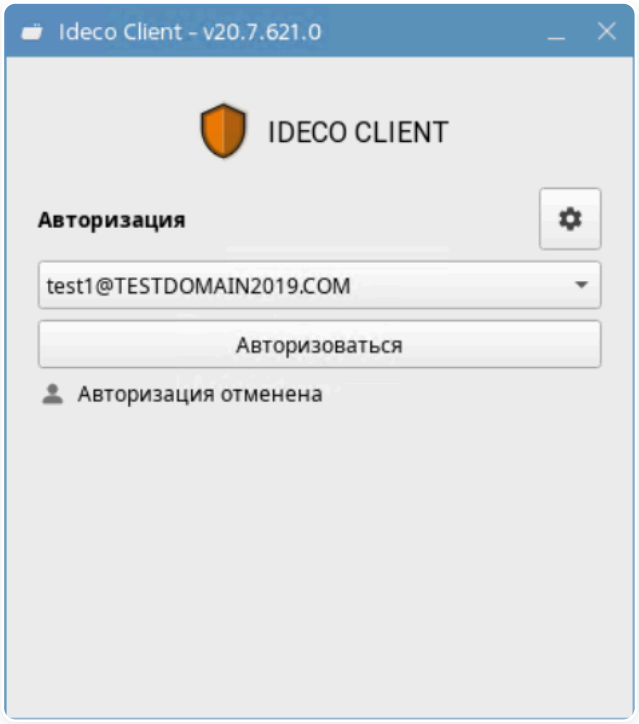
- **network.automatic-ntlm-auth.allow-proxies** = false.
- **network.negotiate-auth.allow-proxies** = false.

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 с Active Directory. Ideco Client пытается получить токен для авторизации на NGFW. Но NGFW 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 на контроллере домена не удалена и имеет необходимые права.

3. Проверьте, что настройки интеграции пользовательского компьютера с AD и NGFW 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` (подробнее в статье). Проверьте логи (например, с помощью `journalctl`, `KSystemLog` или `logcheck`) на ошибки получения SSO-токенов вида:

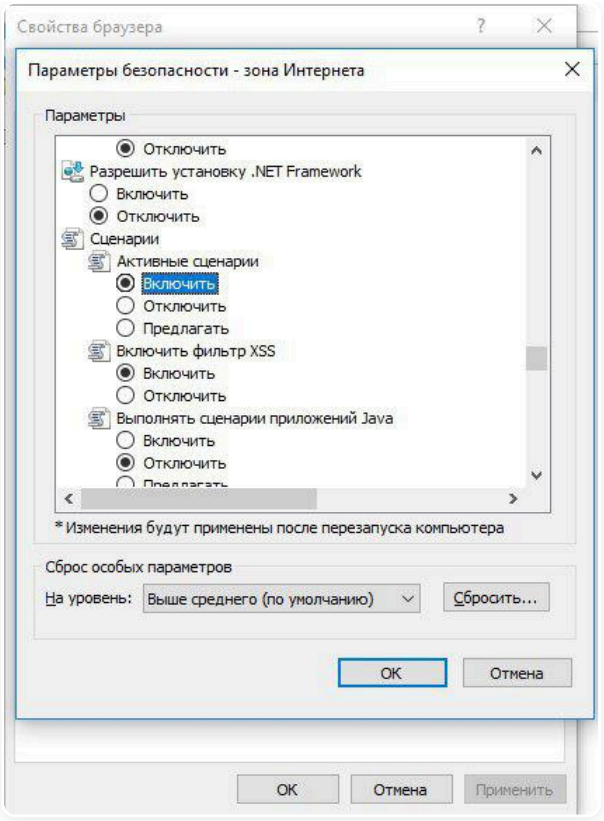
```
SSOGenToken завершился с ошибкой: 'genTokenInternal: <major error string> (<minor error string>)'
```

- `<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.

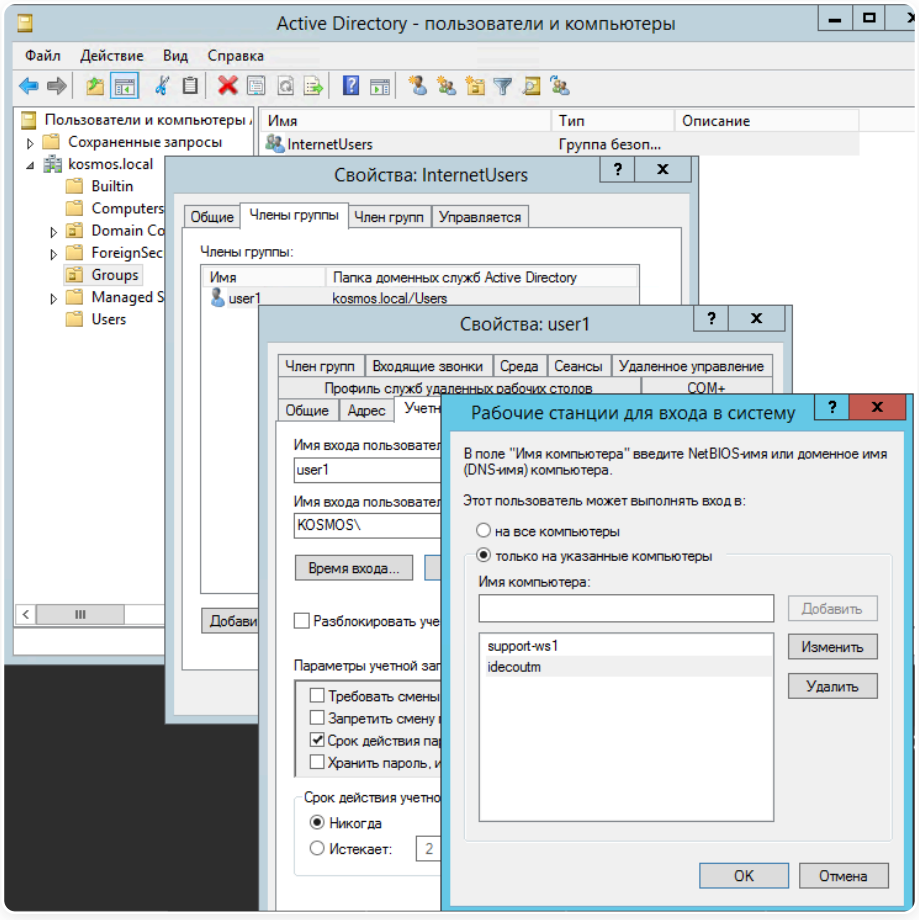
Для получения доступа требуется аутентификация

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. На контроллере домена зайдите в свойства выбранных пользователей на вкладку **Учетная запись → Вход на...**, выберите пункт **только на указанные компьютеры** и пропишите имя рабочей станции для входа в систему.

Пример такой настройки представлен на скриншоте ниже:



Полезные ссылки

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

Настройка авторизации через журнал безопасности

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

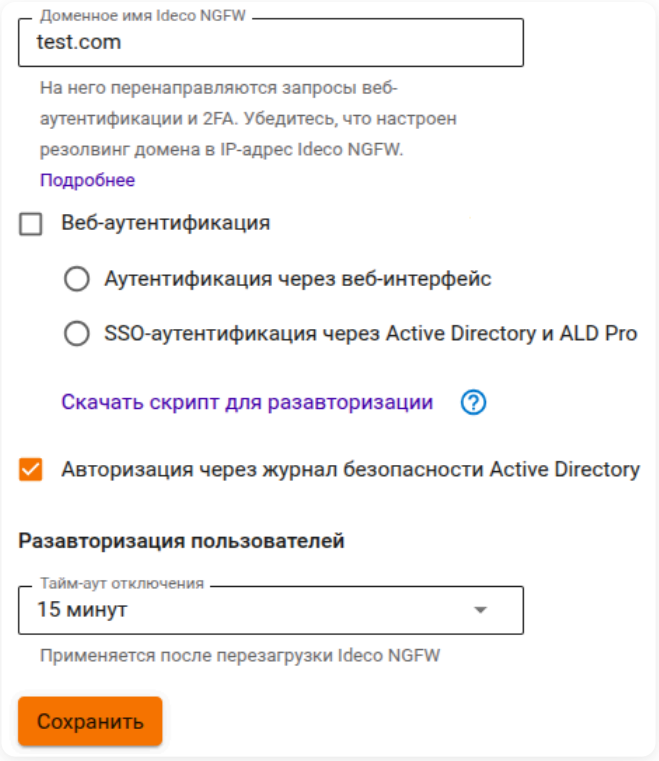
Авторизацию через журнал безопасности Active Directory рекомендуется использовать совместно с SSO-аутентификацией. Авторизация только через журнал безопасности может ограничить возможности управления и настройки прав доступа.

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

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

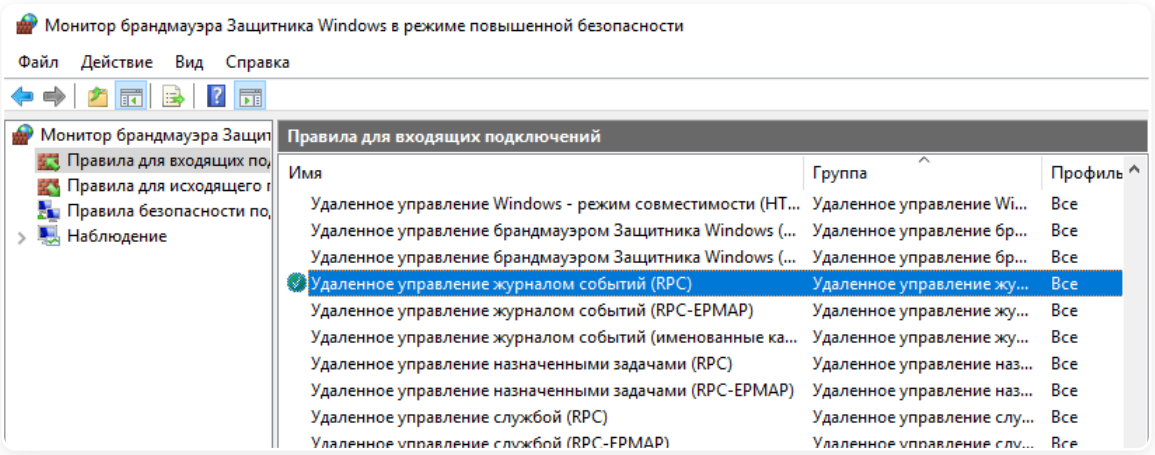


- **Доменное имя Ideco NGFW** - не требуется, если используется только авторизация через журнал безопасности AD.
- **Веб-аутентификация** - не требуется. Авторизация через журнал безопасности AD обеспечивает аутентификацию.
- **Авторизация через журнал безопасности Active Directory** - включите, чтобы Ideco NGFW 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.
- **Тайм-аут отключения** - установите тайм-аут разавторизации пользователей. Значение по умолчанию - 15 минут. Диапазон доступных значений - от 10 минут до 1 дня.

Настройка на стороне сервера Active Directory

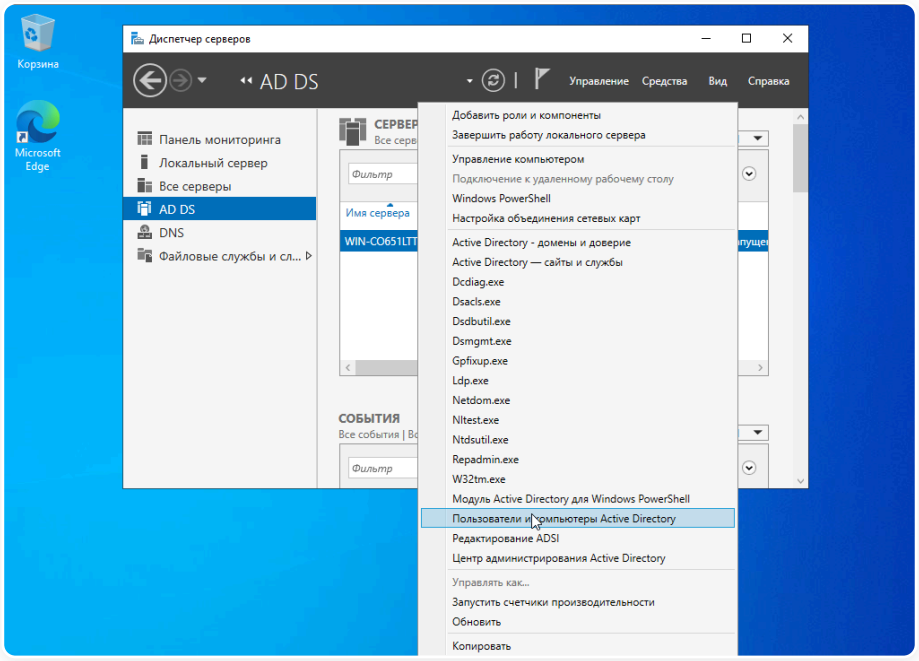
Перед настройкой убедитесь, что Ideco NGFW уже введен в домен.

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

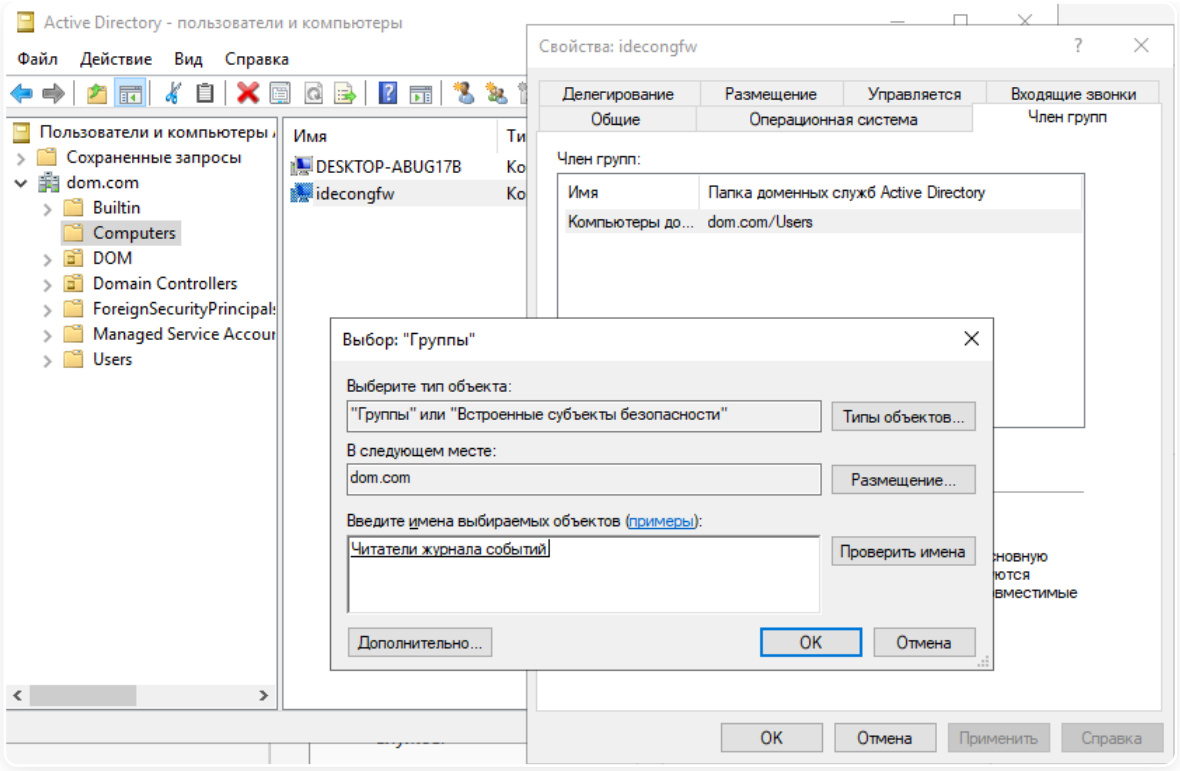


2. Добавьте Ideco NGFW в группу безопасности **Читатели журнала событий (Event Log Readers)**. Чтобы это сделать:

- 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 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. 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 **ОК**.

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 автоматической разавторизации

При переходе с более ранних версий на Ideco NGFW v17 изменился скрипт автоматической разавторизации. Чтобы избежать ошибок, скачайте и перенастройте скрипт в соответствии с инструкцией ниже.

Разавторизация пользователей возможна в полностью автоматическом режиме. Для этого настройте скрипт (logout), который будет запускаться при выходе пользователей из системы с помощью групповых политик домена (GPO).

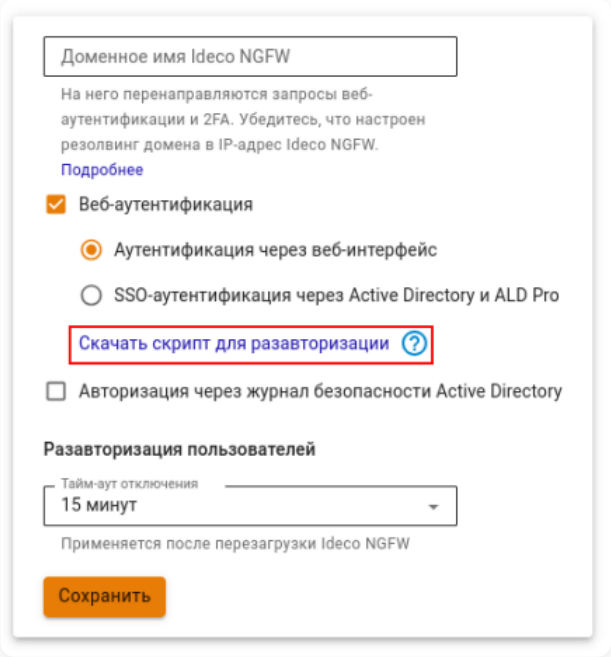
Для работы скрипта выполните все настройки политик безопасности домена и браузера, описанные в статье Авторизация пользователей.

Для авторизации по SSO используйте Ideco Client.

Разавторизация пользователя

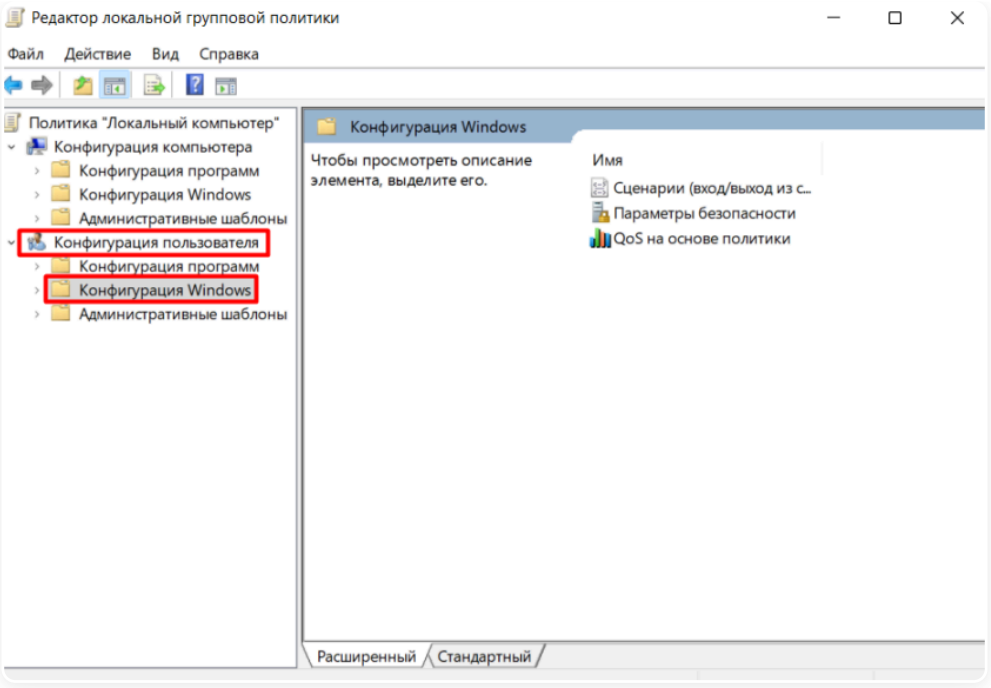
Чтобы скрипт разавторизации работал корректно, установите на компьютеры пользователей корневой сертификат сервера Ideco NGFW и сделайте его доверенным. Это можно сделать как локально, так и через групповые политики домена, следуя инструкции.

1. Чтобы скачать скрипт, перейдите в раздел **Пользователи** → **Авторизация** → **Основное**. Включите опцию **Веб-аутентификация**, после чего появится кнопка **Скачать скрипт для разавторизации**:



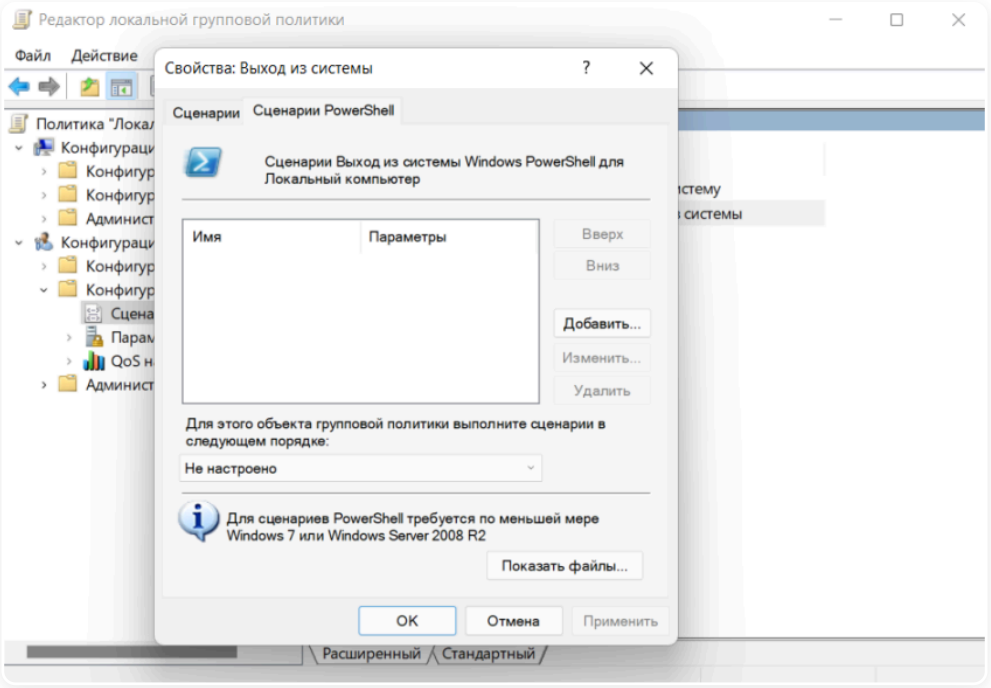
2. Откройте групповые политики (gpedit.msc) от имени администратора на устройстве пользователя.

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

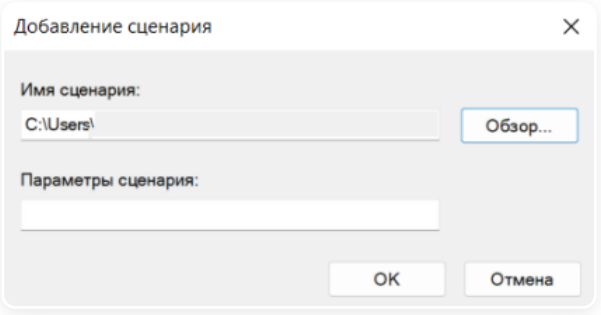


4. Нажмите **Сценарии (вход/выход из системы)**.

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



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

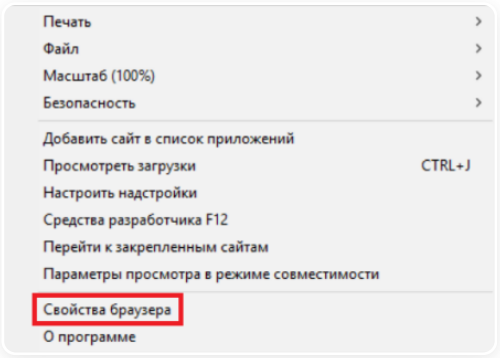


7. Откройте командную строку и обновите групповые политики, введя команду `gpupdate /force`.

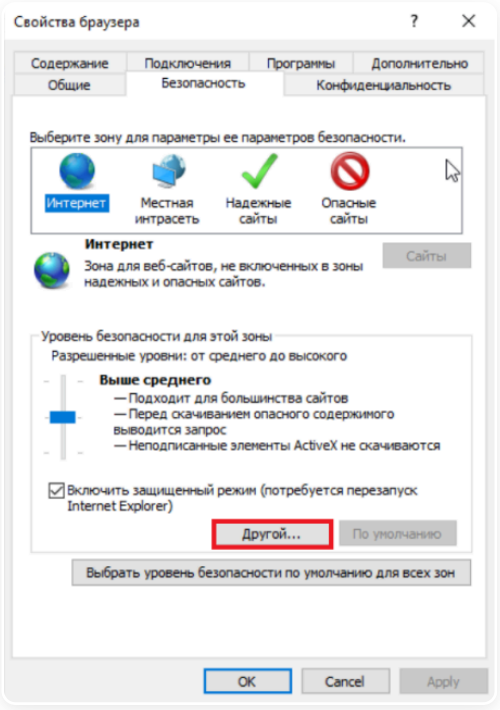
Если в вашем браузере появляется окно с текстом **Для получения доступа требуется аутентификация** и авторизация происходит только при ручном переходе по ссылке, включите JavaScript. Ниже представлены настройки для разных браузеров:

Internet Explorer

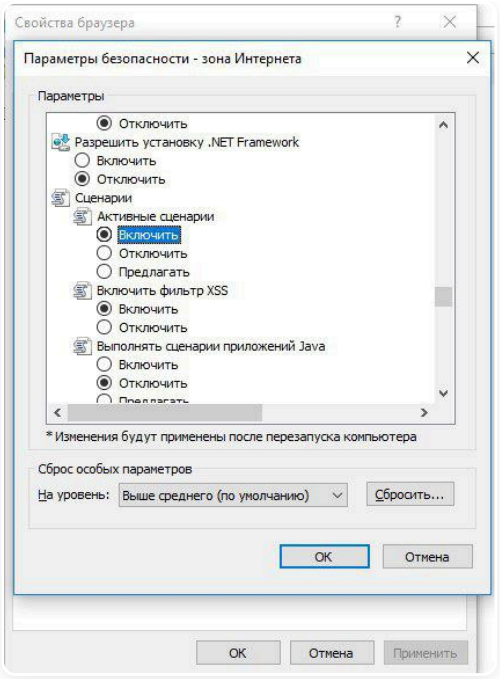
1. В правом верхнем углу браузера нажмите на кнопку **Сервис** в виде шестерни или комбинацию клавиш Alt+X. В выпадающем меню выберите **Свойства браузера**:



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

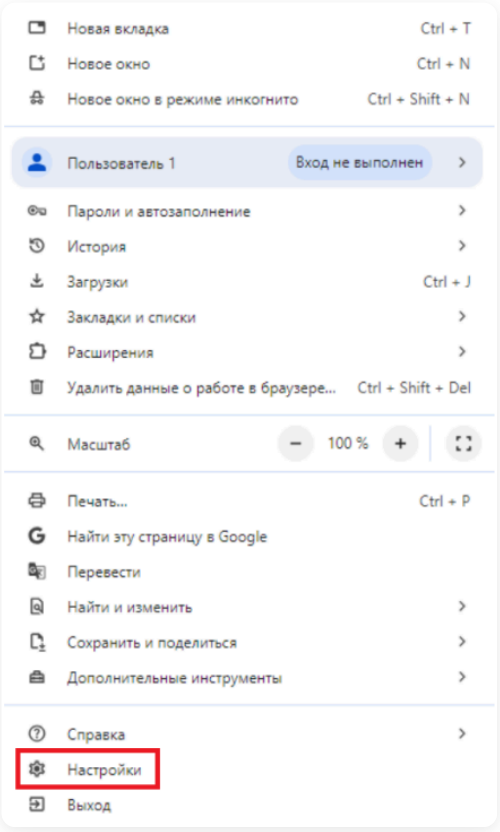


3. В окне **Параметры** переключите параметр **Активные сценарии** в значение **Включить**:

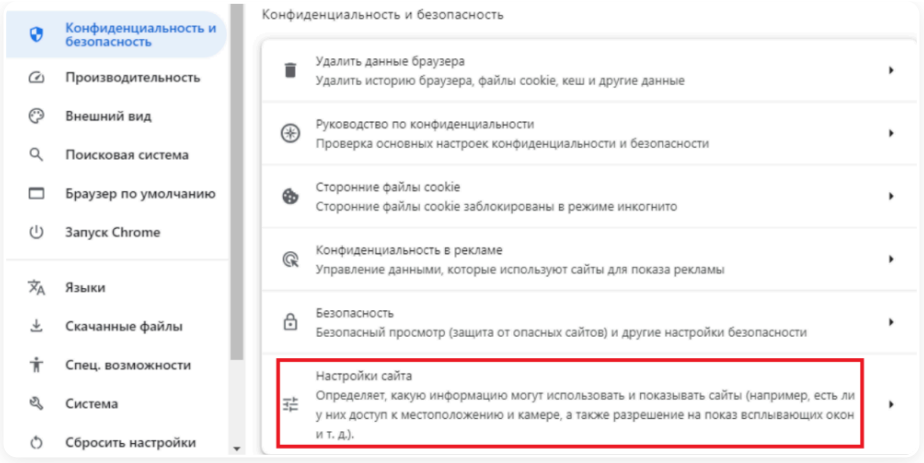


Google Chrome

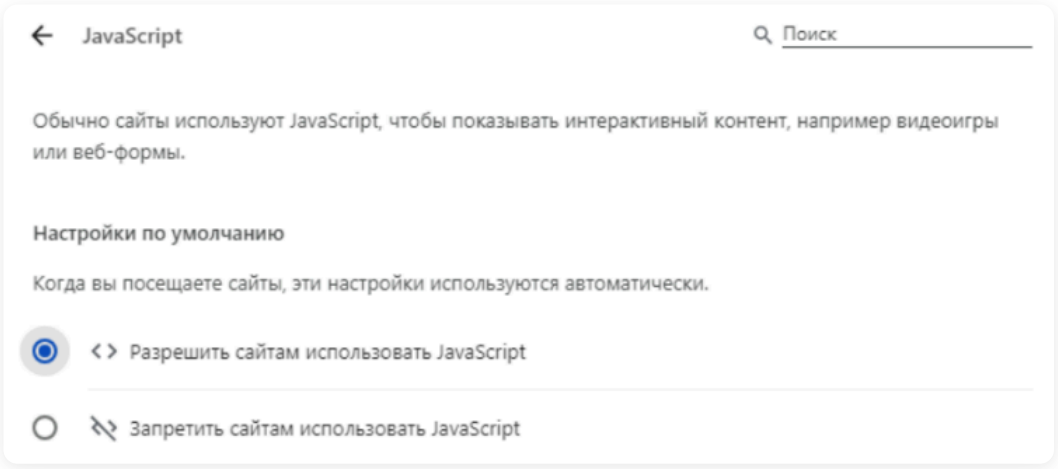
1. В правом верхнем углу браузера нажмите на кнопку с тремя точками и выберите **Настройки** в выпадающем меню:



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

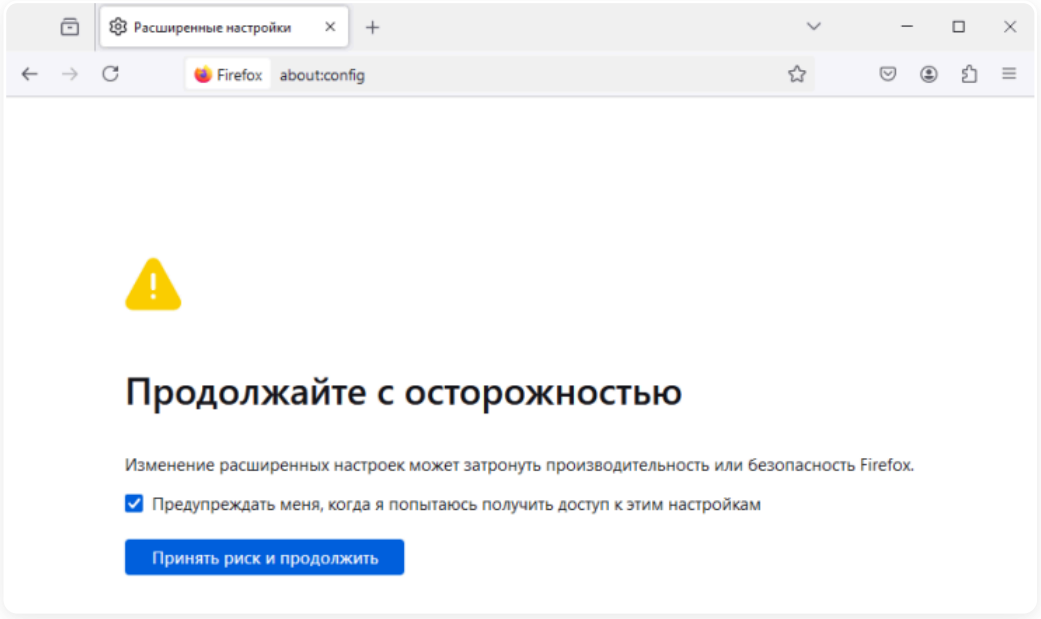


3. В настройках **JavaScript** разрешите сайтам использовать JavaScript:

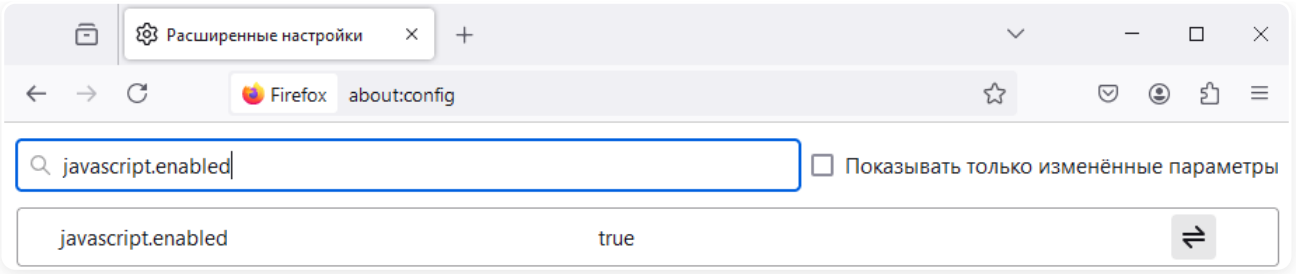


Firefox

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

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

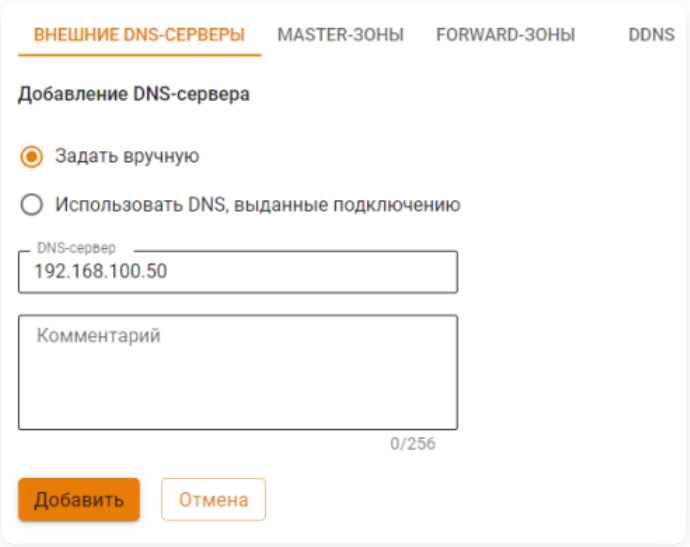
Список служб для других разделов доступен по ссылке.

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

Ideco NGFW поддерживает версии ALD Pro от 1.4.

Ввод сервера в домен

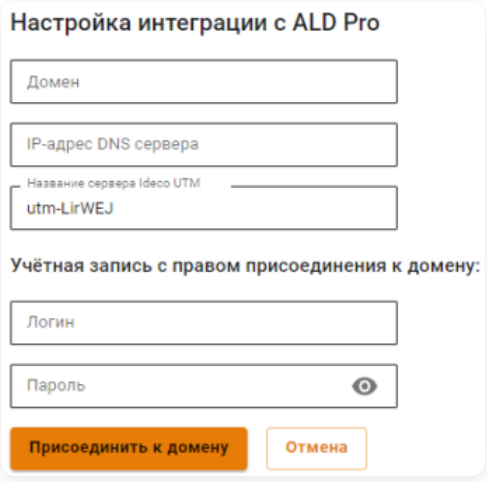
1. Перейдите в раздел **Сервисы** → **Защита и управление DNS** → **Внешние DNS-серверы** и добавьте IP-адрес устройства с установленной системой ALD Pro:



2. Перейдите в **Пользователи** → **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.

- **Имя сервера Ideco NGFW** - 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 без блокировки и считаются **активными**.

Для импорта пользователей выполните действия:

1. Перейдите в раздел **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 **Файрволе**).

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

Пользователь может быть импортирован только в одну группу Ideco NGFW. 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.

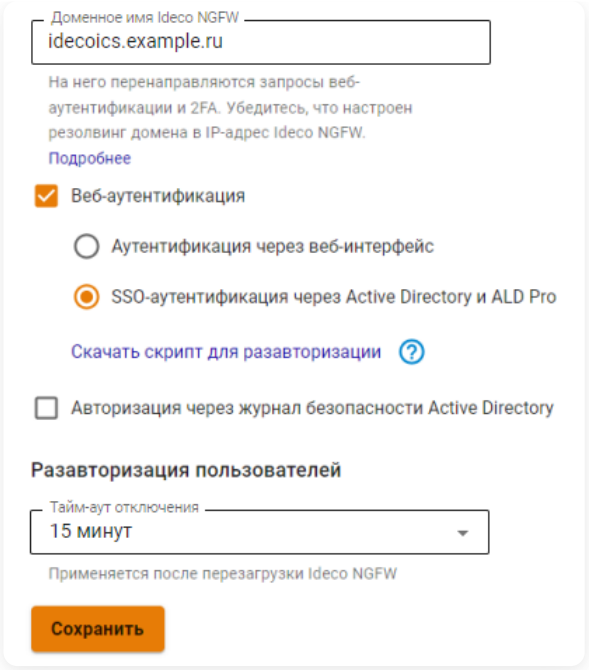
Настройка Ideco NGFW

Для настройки аутентификации выполните действия:

1. Перейдите в **Пользователи** → **Авторизация** → **Настройки**.

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

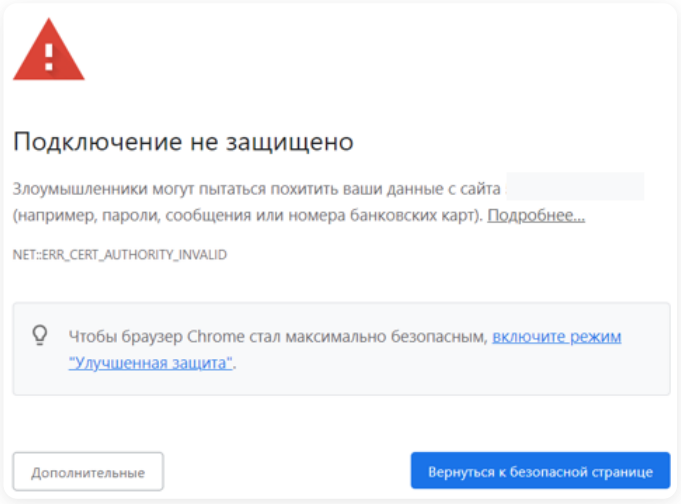
3. Выберите **Тип** входа в систему:



- **Аутентификация через веб-интерфейс** - вход по логину/паролю.
- **SSO-аутентификация через Active Directory и ALD Pro** - вход через SSO.

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

После заполнения поля **Доменное имя Ideco NGFW** 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 не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW, то страница авторизации будет подписана корневым сертификатом NGFW.

5. Настройте способы авторизации импортированных пользователей. Доступные способы:

- 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 в случаях, когда 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

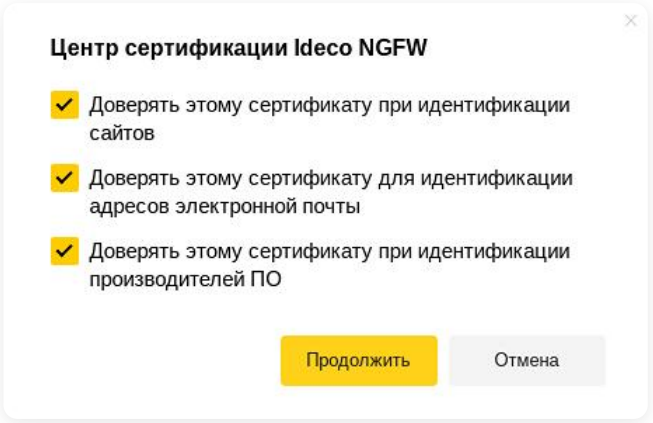
1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и добавьте строки:

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

2. Скачайте корневой сертификат.

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

4. Включите опции доверия для сертификата:



Настройка браузера Google Chrome

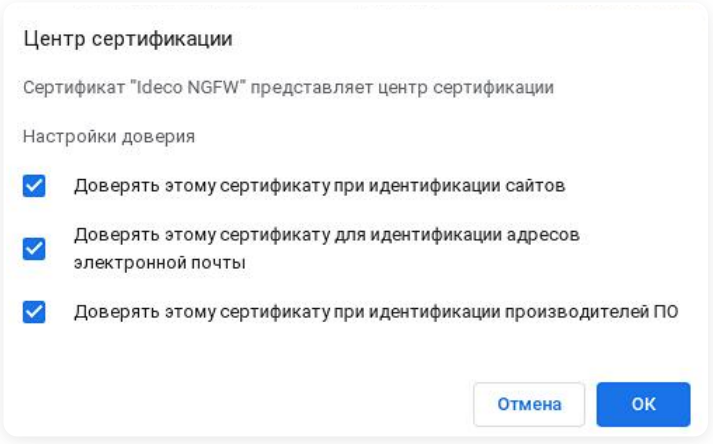
1. Создайте файл **mydomain.json** в директории `/etc/opt/chrome/policies/managed/` и добавьте строки:

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

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите на вкладку **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

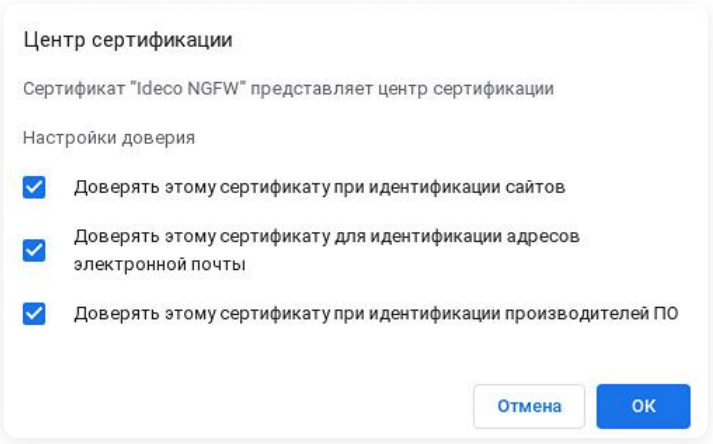
1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и добавьте строки:

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

2. Скачайте корневой сертификат.

3. В браузере Chromium перейдите на вкладку **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

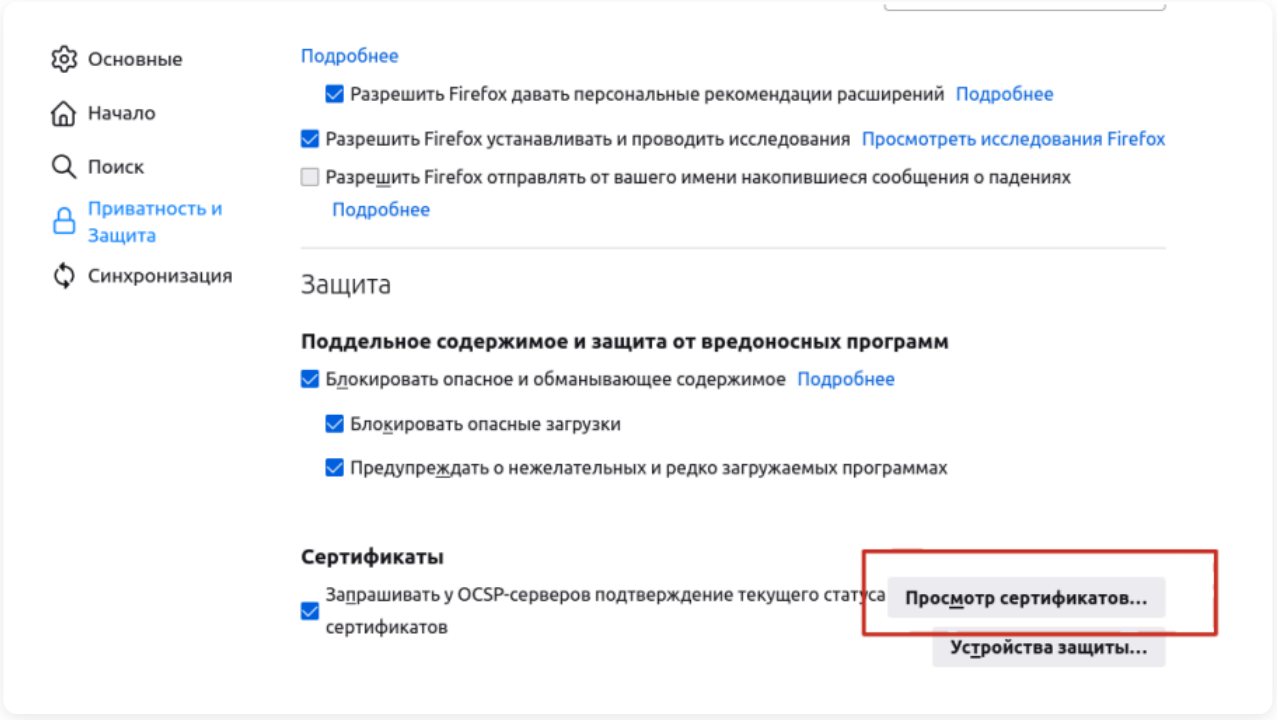
1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

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 локального интерфейса и доменное имя Ideco NGFW в директорию `/etc/hosts`.
Пример: `192.168.100.10 ngfw.domain.ald`.

Руководства по эксплуатации ALD Pro доступны на официальном сайте.

RADIUS

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.
- Пользователи RADIUS могут авторизоваться с помощью Ideco Client без установления VPN-туннеля.
- При отключенной интеграции с RADIUS-сервером пользователи RADIUS не смогут аутентифицироваться на Ideco NGFW.
- 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 поддерживает интеграцию с RADIUS-администраторами. Подробные инструкции по настройке описаны в статье Администраторы.

Настройка интеграции

Для настройки интеграции с RADIUS-сервером выполните действия:

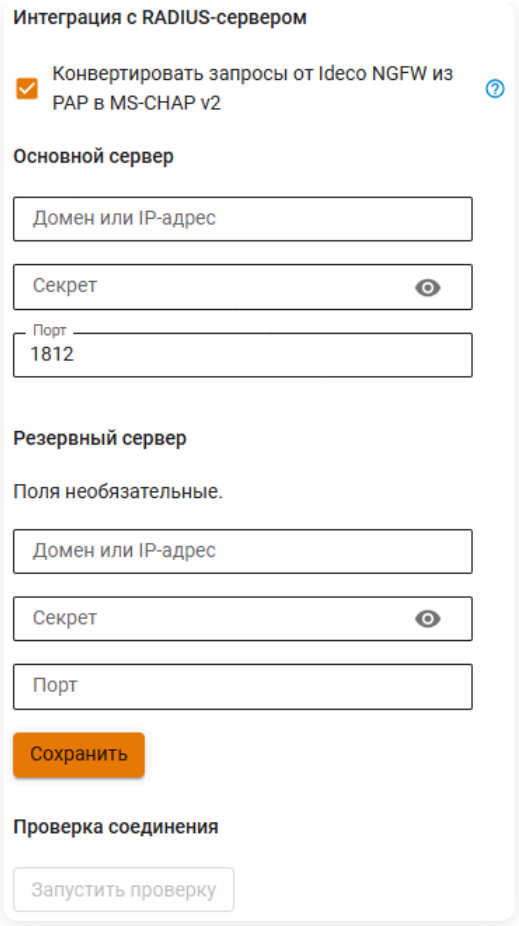
1. Перейдите в **Пользователи** → **RADIUS** и включите опцию **RADIUS**.

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

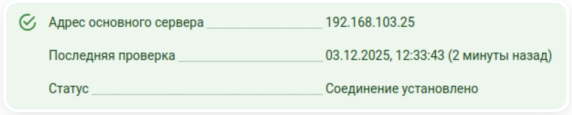
2. Включите опцию **Конвертировать запросы от Ideco NGFW из PAP в MS-CHAP v2**. Опция повышает безопасность и защиту от перехвата паролей между NGFW и RADIUS-сервером, или когда RADIUS-сервер поддерживает только MS-CHAP v2. Выключите опцию только если необходимо настроить двухфакторную аутентификацию для пользователей RADIUS-сервера.

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

2. Заполните поля:



- **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. По умолчанию используется порт 1812.
- **Резервный сервер** - при наличии в сети двух RADIUS-серверов настройте один как резервный с указанием порта подключения. При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.
- **Проверка соединения** - нажмите **Запустить проверку**, чтобы проверить соединение с RADIUS-сервером. При успешной проверке будет показано, что соединение установлено:



3. Нажмите **Сохранить**.

Добавление пользователей в дерево пользователей Ideco NGFW

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

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

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

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

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

Ограничения для группы и пользователей RADIUS:

- Запрещено менять параметры пользователя (в том числе поля **Имя** и **Комментарий**), за исключением опции **Запретить доступ**.
- Разрешено удалять и переименовывать группу **RADIUS**.
- Запрещено перемещать пользователей в другие группы.
- Запрещено перемещать других пользователей NGFW 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 только 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 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:

1. В веб-интерфейсе Ideco NGFW в **Пользователи** → **RADIUS** отключите опцию **Конвертировать запросы от Ideco NGFW 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.

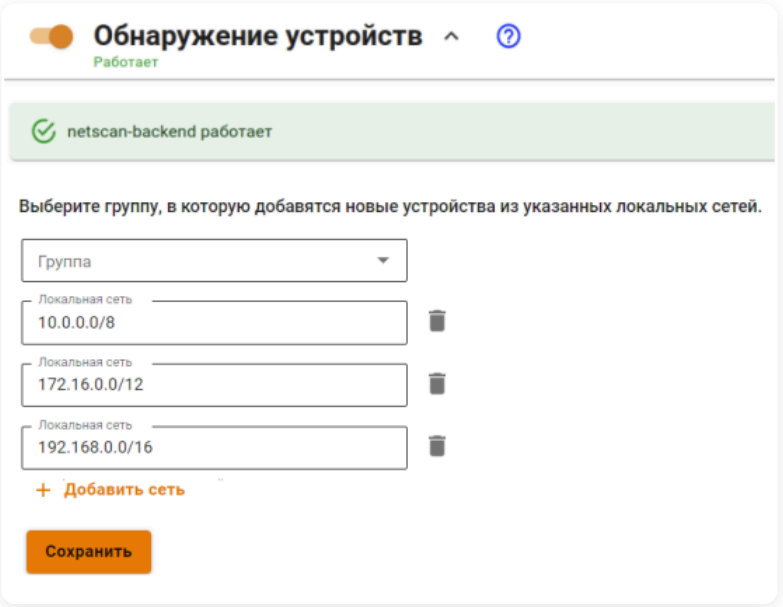
3. Настройте на RADIUS-сервере механизм двухфакторной аутентификации. Настраивать 2FA на Ideco NGFW не нужно.

Обнаружение устройств

Совет

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. 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 уже есть учетная запись с логином, равным NetBIOS-имени машины, то NGFW использует данные пользователя без обновления его параметров (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 этом 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 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 >

Telegram-бот

В статье описана настройка оповещений от Ideco Monitoring Bot

Перейти >

SNMP

В статье описана настройка доступа к Ideco NGFW по протоколу SNMP

Перейти >

Zabbix-агент

В статье описана интеграция Zabbix-агента в Ideco NGFW

Перейти >

Netflow

В статье описана настройка экспорта статистики трафика на коллектор во внешней или локальной сети по протоколу Netflow.

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

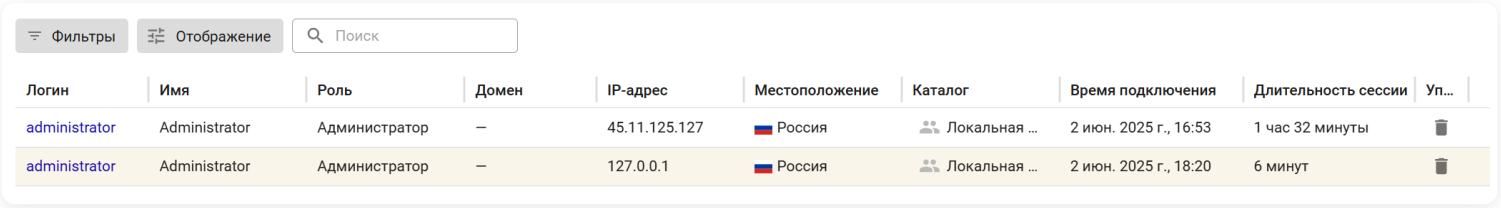
Раздел содержит список всех сессий администраторов в NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS.

Сессии администраторов, подключенных через Ideco Center, не отображаются в разделе.

Сессии администраторов

Сессия с IP-адресом 127.0.0.1 - сессия администратора, работающего в локальном меню сервера.

Таблица сессий авторизованных администраторов в NGFW:



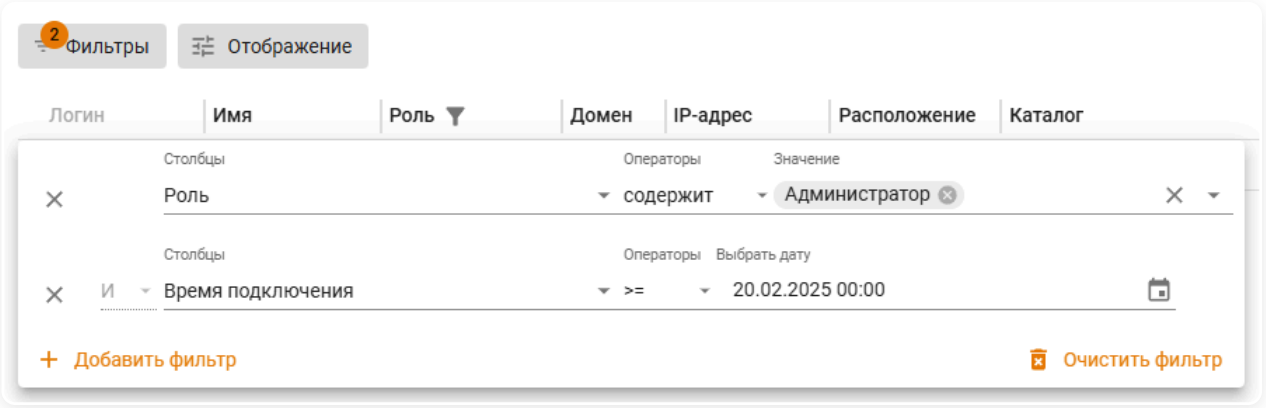
- **Роль** - возможные роли: Администратор, Только просмотр, Администратор ИБ, Администратор файрвола, Администратор настройки доступов, Просмотр отчетов, Создание отчетов.
- **Домен** - доменное имя, если администратор импортирован из Active Directory или ALD PRO. В ином случае в ячейке прочерк.
- **IP-адрес** - IP-адрес устройства, с которого авторизован администратор.
- **Расположение** - географическое расположение администратора.
- **Каталог** - тип администратора в зависимости от источника добавления: Локальная группа, AD, ALD, 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 завершить сессию любого администратора из интерфейса Ideco NGFW.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока сессия администратора будет автоматически завершена.

В столбце **Управление** администратор может завершить свою сессию.

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:



Полезные ссылки

Администраторы

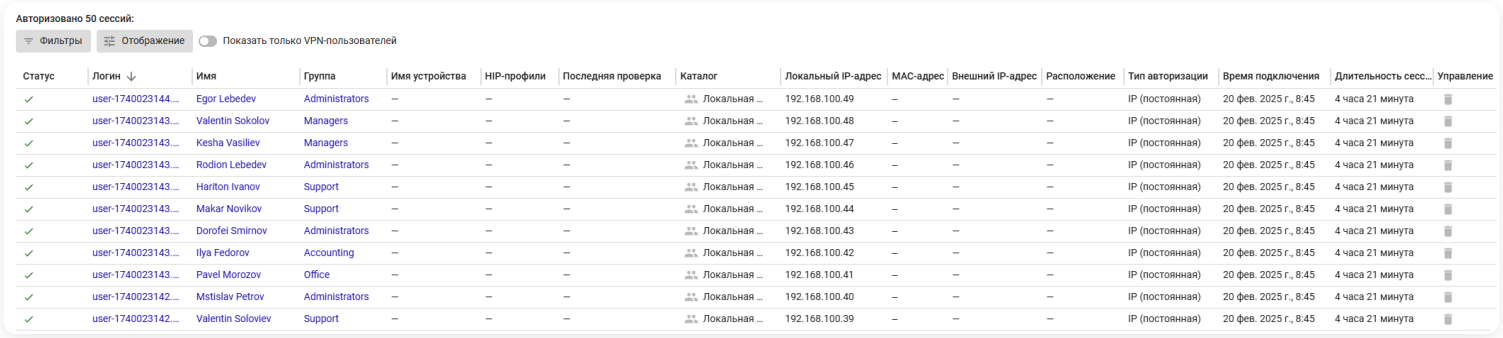
Действия администраторов

Сессии пользователей

Раздел содержит список всех сессий пользователей, которые авторизовались в NGFW, включая локальных, из Active Directory, ALD PRO и RADIUS.

Количество сессий в мониторинге не является показателем занимаемых лицензий, так как под одной пользовательской учетной записью возможно одновременное авторизация до 5 устройств, что учитывается как одна лицензия.

Таблица сессий авторизованных пользователей в NGFW:



Статусы подключения пользователей

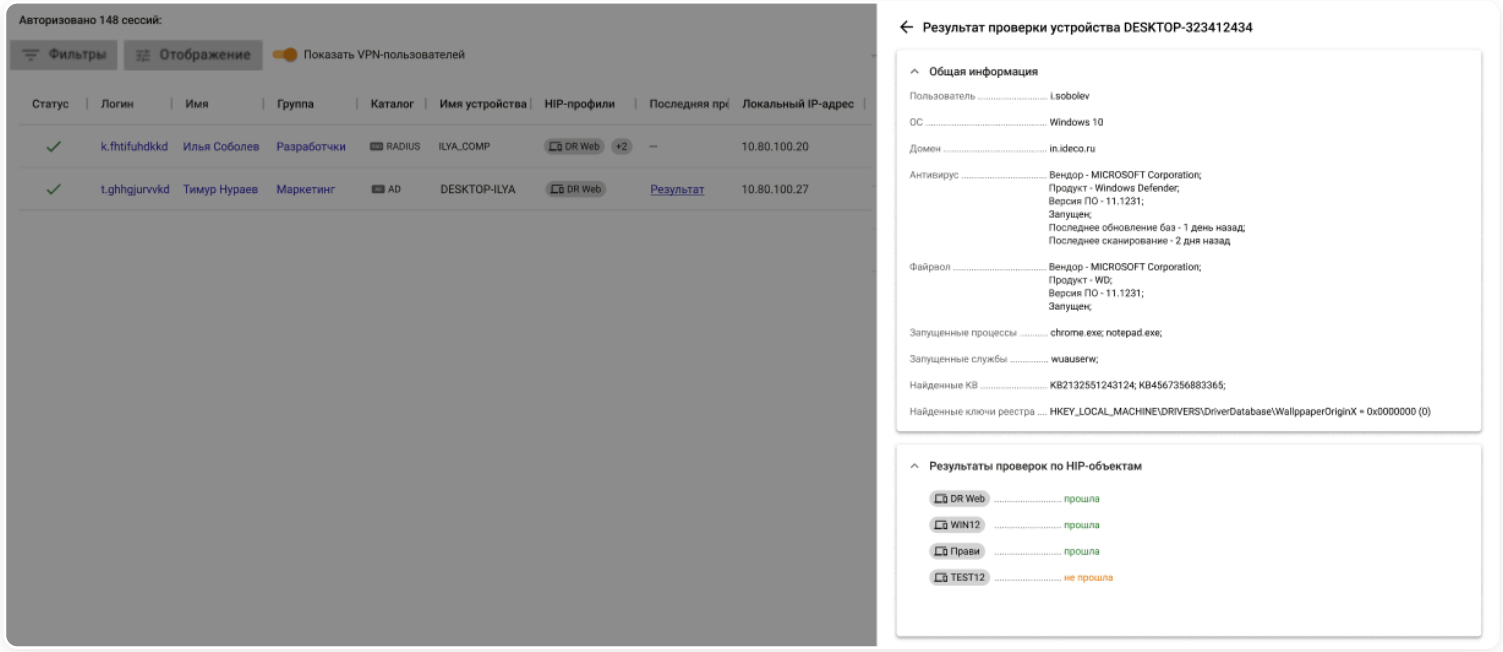
- **Подключено**. Пользователь авторизован;

- **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 активные 5 сессий;

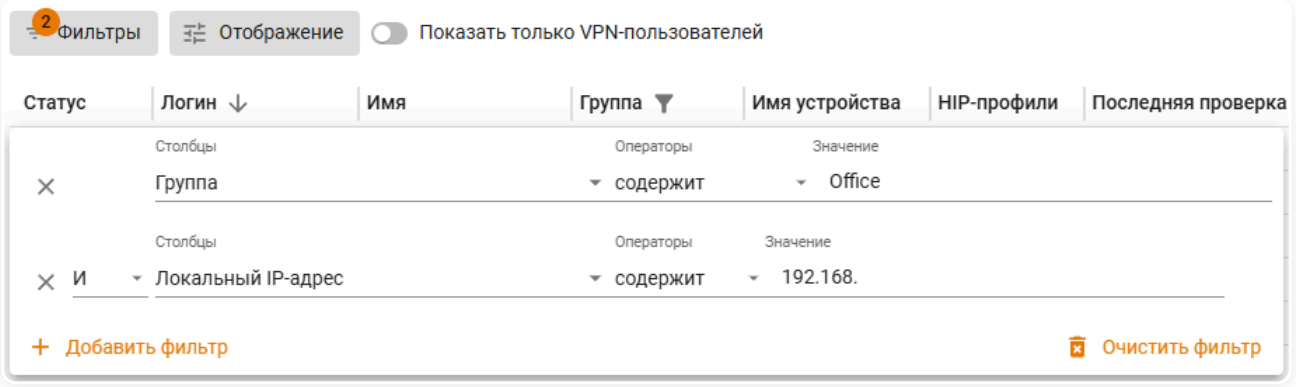
- **Сессия удаляется**. Появляется при разрыве сессии с динамическим IP-адресом. Сессия с таким статусом будет удалена через 30 секунд.

Для просмотра результата проверки устройства, подключенного через Ideco Client, кликните 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:



Опция **Показать только VPN-пользователей** позволяет отображать в таблице журнала только тех пользователей, которые подключены к NGFW через VPN.

Полезные ссылки

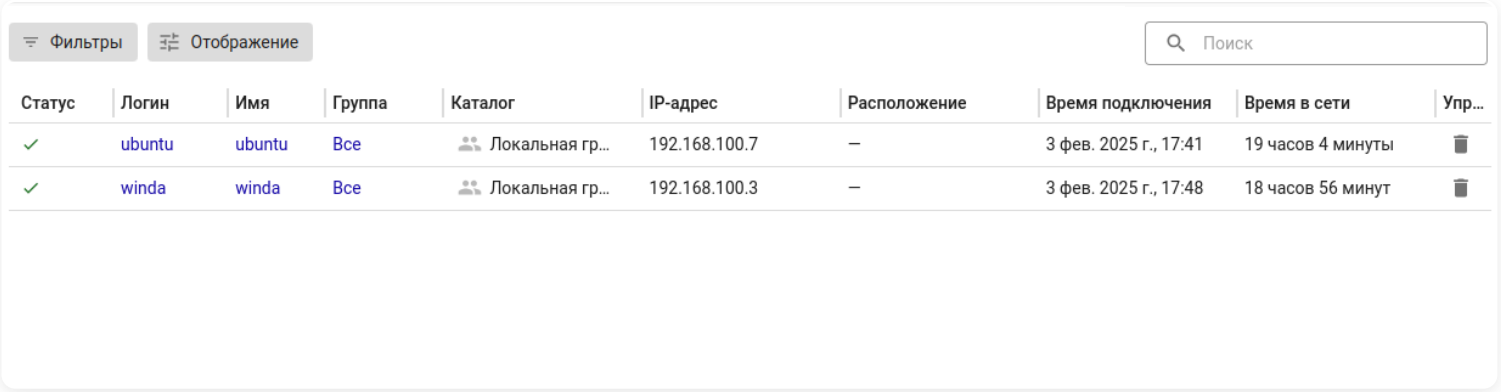
Авторизация пользователей

Сессии ЛК

Сессии ЛК - таблица активных сессий в личном кабинете Ideco NGFW. 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 разделе **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 и каталог), таблица активных сессий содержит столбцы:

- **Статус** - доступные значения: авторизован, 2FA (ожидает 2FA, генерация TOTP для прохождения 2FA);
- **IP-адрес** - IP-адрес, с которого произведена начальная аутентификация сессии в ЛК;
- **Расположение** - 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 **Расположение** 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 и его значение;
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Графики загруженности

Модуль **Графики загруженности** позволяет просматривать данные о состоянии Ideco NGFW 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, 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%);
- 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, статической и динамической балансировки.

Диски

Содержит статистику об объеме записанной и прочитанной информации в определенный промежуток времени (график **Диск**) и количестве обращений к диску за это же время (график **Операции ввода-вывода**). Дает оценку интенсивности использования диска. Информация о свободном и занятом объеме на диске доступна в разделе Бэкапы.

VPN

Содержит информацию о количестве подключений пользователей по протоколам L2TP/IPsec, PPTP и IKEv2.

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.

Полезные ссылки

- Сетевые интерфейсы
- Балансировка и резервирование
- Кластеризация
- Бэкапы
- ГОСТ VPN

- Инструкции по созданию VPN-подключений

Монитор трафика

В разделе **Мониторинг → Монитор трафика** можно просматривать данные о трафике (вх./исх. скорость, количество сессий), проходящем через Ideco NGFW в режиме реального времени.

Для работы **Монитора трафика** необходимо необходимо включить Контроль приложений.

Раздел **Монитор трафика** состоит из вкладок:

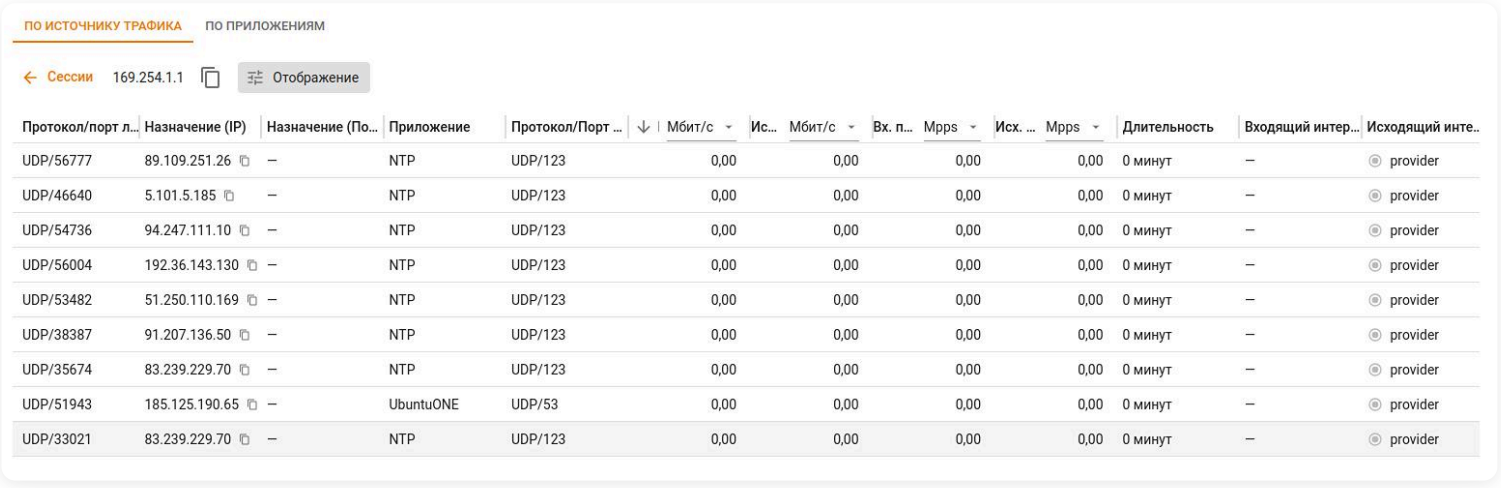
По источнику трафика

Вкладка **По источнику трафика** позволяет отслеживать активность пользователей сети и выявлять тех, кто нагружает канал трафиком:



Источник (IP)	Источник (Пользователь)	Источник (Объекты)	Сессии	Вх. скор... Мбит/с	Исх. скорость Мбит/с	Вх. пакеты Mpps	Исх. пакеты Mpps
169.254.1.1	–	–	70	0,01	0,01	0,00	0,00
172.16.50.3	–	–	6	0,00	0,00	0,00	0,00
172.16.50.255	–	–	1	0,00	0,00	0,00	0,00
192.168.100.1	–	–	10	0,00	0,00	0,00	0,00

Для просмотра информации об активности определенного узла локальной сети нажмите на **количество сессий** в таблице:



Протокол/порт л...	Назначение (IP)	Назначение (По...	Приложение	Протокол/Порт ...	Мбит/с	Ис... Мбит/с	Вх. п... Mpps	Исх. ... Mpps	Длительность	Входящий интер...	Исходящий инте..
UDP/56777	89.109.251.26	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/46640	5.101.5.185	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/54736	94.247.111.10	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/56004	192.36.143.130	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/53482	51.250.110.169	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/38387	91.207.136.50	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/35674	83.239.229.70	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/51943	185.125.190.65	–	UbuntuONE	UDP/53	0,00	0,00	0,00	0,00	0 минут	–	provider
UDP/33021	83.239.229.70	–	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	–	provider

По приложениям

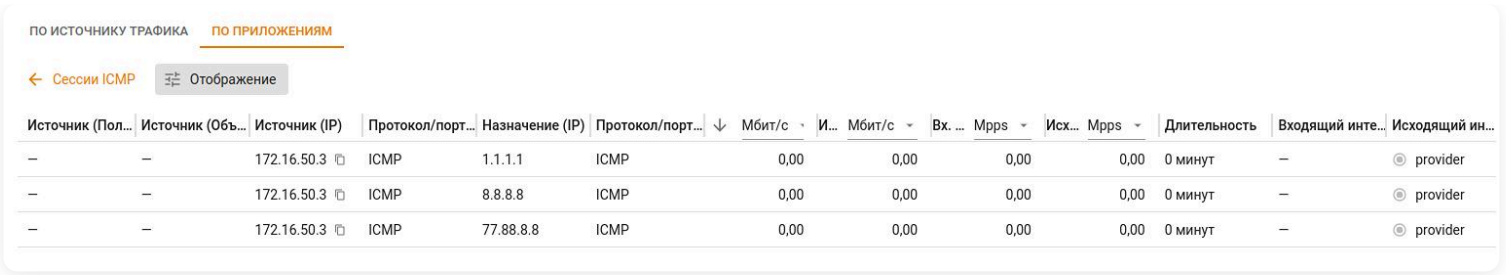
Вкладка **По приложениям** позволяет отслеживать активность приложений.

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:



Приложение	Сессии	Вх. скорость Мбит/с	Исх. скорость Мбит/с	Вх. пакеты Mpps	Исх. пакеты Mpps
ICMP	3	0,00	0,00	0,00	0,00
NTP	13	0,00	0,00	0,00	0,00
Unknown	2	0,00	0,00	0,00	0,00
TLS	1	0,00	0,00	0,00	0,00
Dropbox	2	0,00	0,00	0,00	0,00

Для просмотра подробной информации об активности определенного приложения нажмите на **количество сессий** в таблице:



Полезные ссылки

- Контроль приложений

Telegram-бот

Ideco Monitoring Bot - это Telegram-бот, который отправляет уведомления о событиях в Ideco NGFW (уведомления из колокольчика):

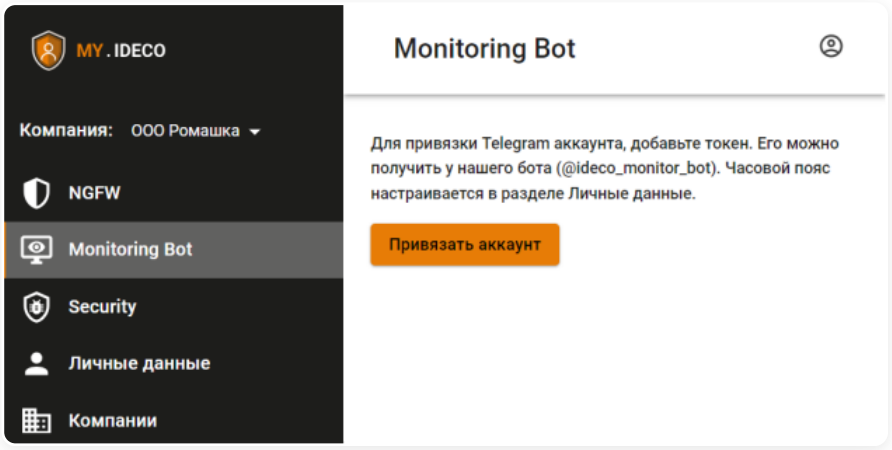
- В личные сообщения;
- В беседы, где 2 и более участников (groups).

Привязка бота и настройка оповещений Ideco Monitoring Bot осуществляется в личном кабинете.

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 личном кабинете.
5. Нажмите **Привязать аккаунт**.
6. Введите код в поле **Токен Telegram-аккаунта** и нажмите **Привязать**:

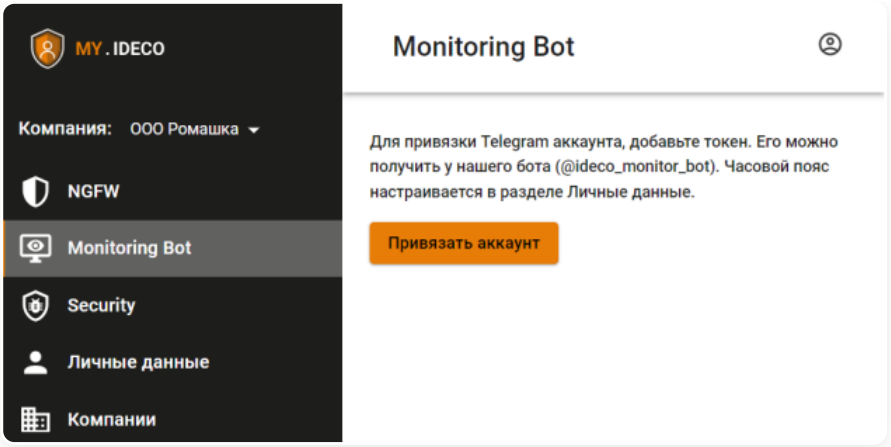


Уведомления начнут приходить в Telegram-аккаунт.

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 личном кабинете.
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 личном кабинете.
2. Выберите аккаунт или группу и нажмите .
3. Выберите уведомления, которые хотели бы получать.

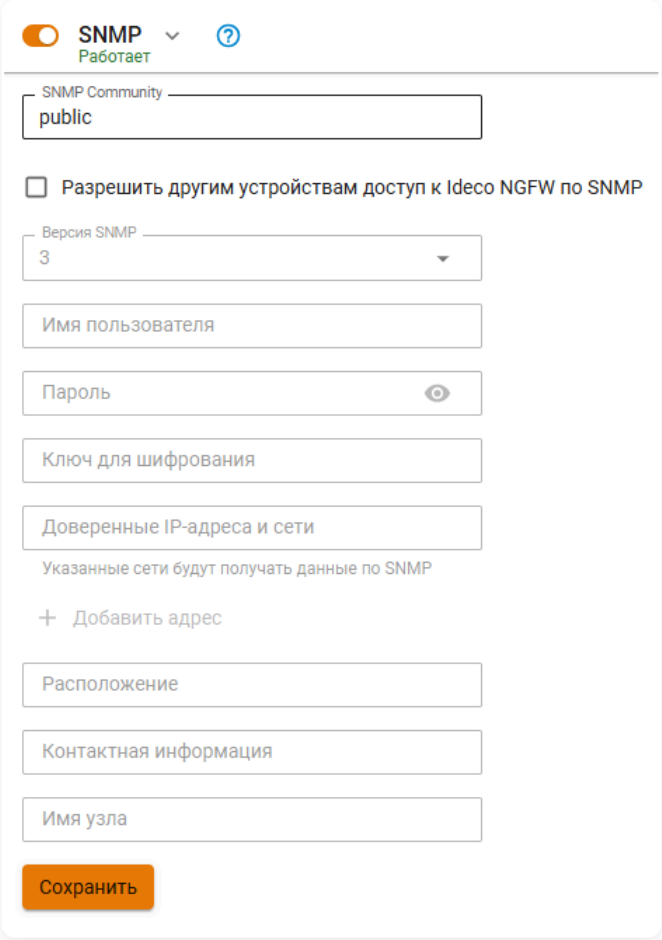
Если требуется временно отключить отправку уведомлений, нажмите на . Оповещения перестанут приходить, пока снова не нажмете на эту иконку.

SNMP

SNMP - это протокол для управления и мониторинга сетевых устройств, таких как маршрутизаторы, коммутаторы и фаерволы.
Модуль **SNMP** обеспечивает мониторинг работы Ideco NGFW по протоколу SNMP версий 1/2c и 3.

Настройка подключения

Для подключения по протоколу SNMP в разделе **Мониторинг** → **SNMP** включите опцию и заполните поля:



Версия 1/2c

- **Имя пользователя**;
- **Пароль** (минимальное количество символов - 8);
- **Доверенные IP-адреса и сети**.

Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и являются необязательными.

Версия 3

- **Имя пользователя**;
- **Пароль** (минимальное количество символов - 8);
- **Ключ шифрования**;
- **Доверенные IP-адреса и сети**.

Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.

Рекомендуем: На сервере, с которым будет установлено соединение по SNMPv3, укажите 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 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`).

Интеграция с Zabbix

Zabbix - система с открытым исходным кодом для мониторинга параметров сети, состояния и работоспособности серверов.

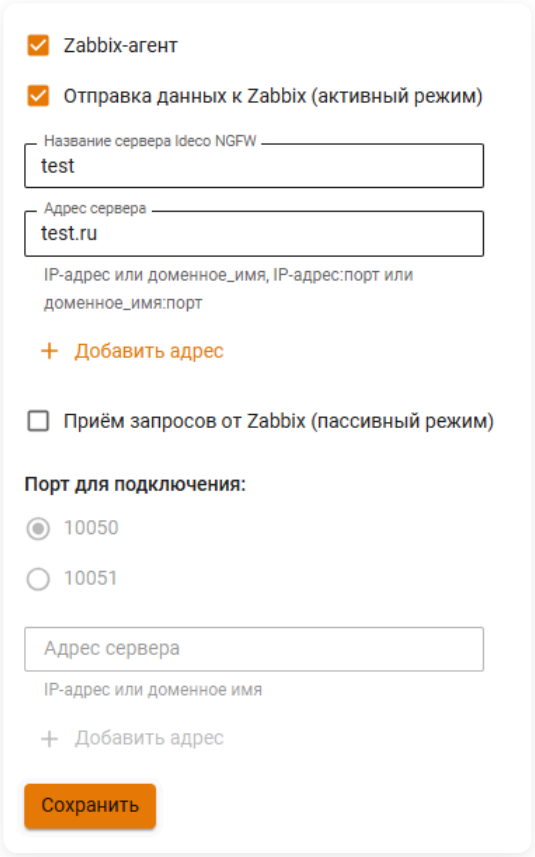
Настройка Zabbix-агента

Для работы системы мониторинга Zabbix в Ideco NGFW активируйте опцию **Zabbix-агент** после настройки интеграции с Zabbix.

Интеграция с системой мониторинга Zabbix возможна в двух режимах: **Активный** и **Пассивный**.

Активный

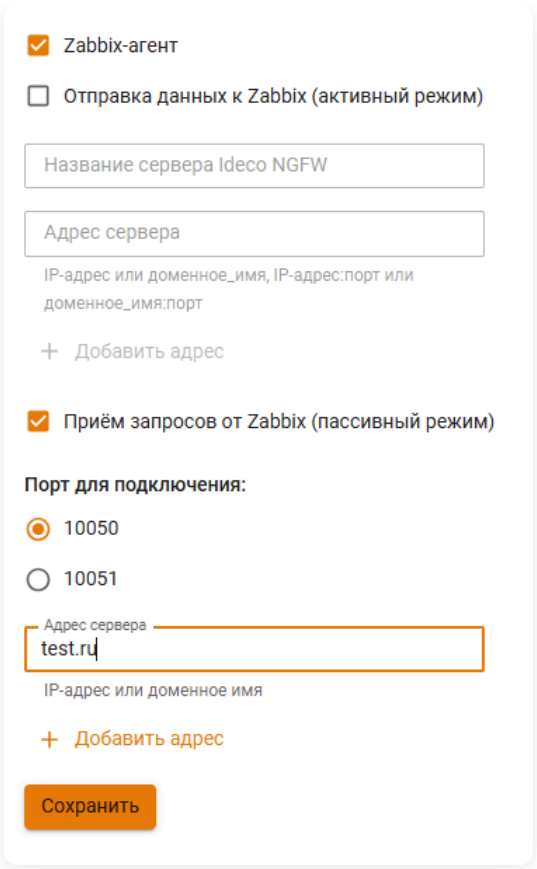
Соединение с Zabbix-сервером происходит со стороны Ideco NGFW. Для настройки заполните поля:



- **Имя сервера Ideco NGFW** - 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 может находиться как внутри локальной сети Ideco NGFW, так и за ее пределами. Подключение мониторинга возможно как к локальным, так и к внешним интерфейсам.

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

Netflow

Netflow - проприетарный открытый протокол, разработанный Cisco для мониторинга статистики трафика в сети. Ideco NGFW выступает в качестве сенсора-экспортера, который собирает статистику при прохождении через него трафика.

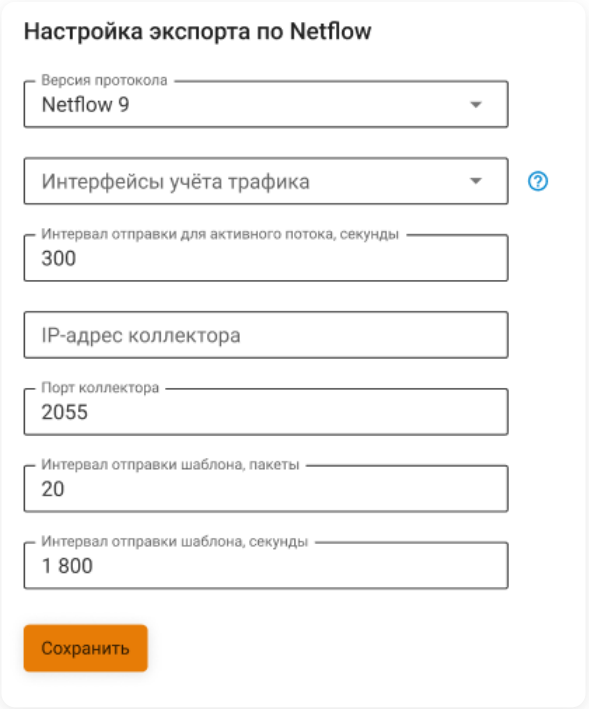
Netflow обеспечивает сбор информации об IP-трафике, обрабатываемом сетевыми устройствами (L3-коммутаторы, маршрутизаторы, сенсоры). Каждый поток является однонаправленным, т.е. каждое двунаправленное соединение **src <--> dst** интерпретируется как два потока: **src -> dst** и **dst -> src**.

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 на вкладку **Мониторинг** → **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 мониторить (доступны Ethernet-интерфейсы. Если не заполнены, статистика не будет экспортироваться;
- **Интервал отправки для активного потока, секунды** - введите временной интервал, через который NGFW будет отправлять на коллектор отчеты по потокам, которые не успели завершиться (информация о завершенных потоках отправляется по завершении). От 60 до 3600 секунд, 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. Минимум 10, максимум 6000, 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. Минимум 60, максимум 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 потере связи с коллектором или его перезагрузке.

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

Правила трафика

В этом разделе описывается настройка служб, определяющих основные правила фильтрации трафика в Ideco NGFW.

Файрвол

Создание правил Файрвола, 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 >

Антивирус

Интеграция Kaspersky Anti-Virus Software Development Kit в Ideco NGFW

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 **Файрвола**, **Контент-фильтра**, **Контроля приложений**, **Маршрутизации**

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Файрвол

Название службы раздела **Файрвол**: `ideco-firewall-backend`.

Список имен служб для других разделов доступен по ссылке.

Файрвол - средство управления трафиком на сервере (межсетевой экран). Поддерживает фильтрацию пакетов с контролем состояния соединений (Stateful Inspection) - решение о блокировке принимается на все соединение.

Файрвол 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 **Файрвола** можно создавать наборы правил, которые разграничивают трафик между различными сетями: локальными, VPN и публичными (интернет). В Ideco NGFW 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**).

Файрвол 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

Файрвол 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.

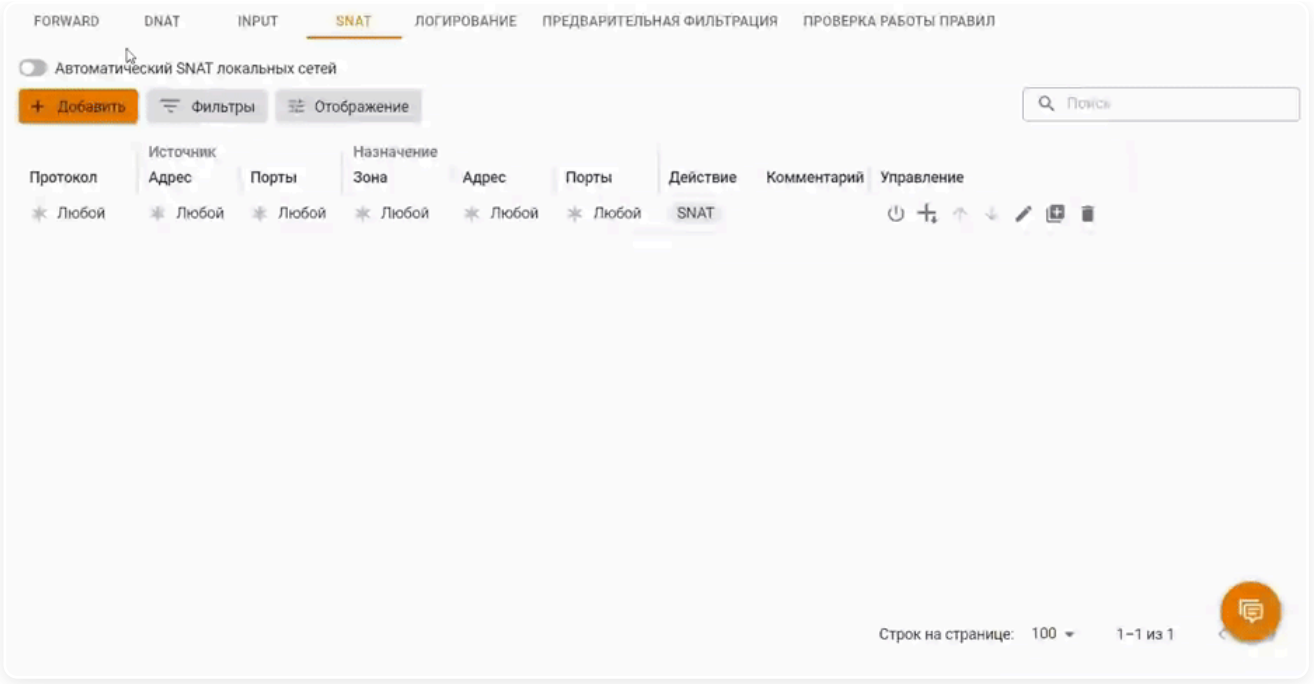
Для работы DPI/IPS в правилах **Файрвола** можно подключить **Профили безопасности**, создав разрешающее правило с включенной проверкой через **Контроль приложений** и/или систему **Предотвращения вторжений**. Профили настраиваются в разделе **Профили безопасности**.

Настройка и управление правилами

Настройка производится в разделе веб-интерфейса **Правила трафика** → **Файрвол**. На вкладках раздела добавляются правила управления трафиком, которые отображаются в таблицах **Файрвола**. При наличии большого количества правил используйте кнопку **Фильтры**.

Если необходимо использовать большое количество правил, можно использовать API. Эти правила не будут отображаться в веб-интерфейсе, но будут работать значительно быстрее.

Включите опцию **Счетчик срабатываний** для подсчета количества срабатываний правил **Файрвола**. После включения опции в таблице появится соответствующий столбец:



Особенности

- Включение режима удаленного помощника изменяет таблицу правил **Файрвола**, разрешая подключение по SSH из локальных и внешних сетей.
- В Ideco NGFW 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 **Файрволе** 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 файрвол** и нажмите Enter:

```
Управление сервером

1. Консоль
2. Отключить все интерфейсы и настроить новый
3. Включить доступ к веб-интерфейсу из внешней сети
4. Включить доступ к серверу по SSH из Интернет
5. Включить доступ к серверу по SSH из локальных сетей
6. Включить режим `Разрешить Интернет всем`
7. Сбросить блокировки по IP
8. Отключить пользовательский файрвол
9. Отключение VCE-интерфейсов
10. Создать новый бэкап
11. Восстановить из бэкапа
12. Мгновенно восстановить из бэкапа
13. Включить доступ Удаленного Помощника
14. Контакты технической поддержки
15. Управление кластером
16. Восстановиться на предыдущую версию
17. Перезагрузка сервера
18. Отключить сервер
19. Выход

Введите номер пункта и нажмите Enter.
# 8
```

При отключении пользовательского файрвола в веб-интерфейсе системные правила продолжают работу.

Полезные ссылки

Настройка Файрвола

- **Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT)**;
- **Примеры создания правил файрвола**;
- **Логирование**;
- **Тестирование правил**;
- **Предварительная фильтрация**;
- **Аппаратная фильтрация**.

Профили безопасности

- **Контроль приложений**;
- **Предотвращение вторжений**.

Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT)

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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 сервера (например, почтового сервера);
- **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 **Файрвола** воспользуйтесь кнопкой **Фильтры**.

Создание правил

Для создания правила в нужной таблице нажмите кнопку **Добавить**.

Укажите необходимые параметры, действия правила и нажмите кнопку **Добавить**. Правило будет добавлено в конец списка. Если необходимо, измените его приоритет кнопками ↑ ↓.

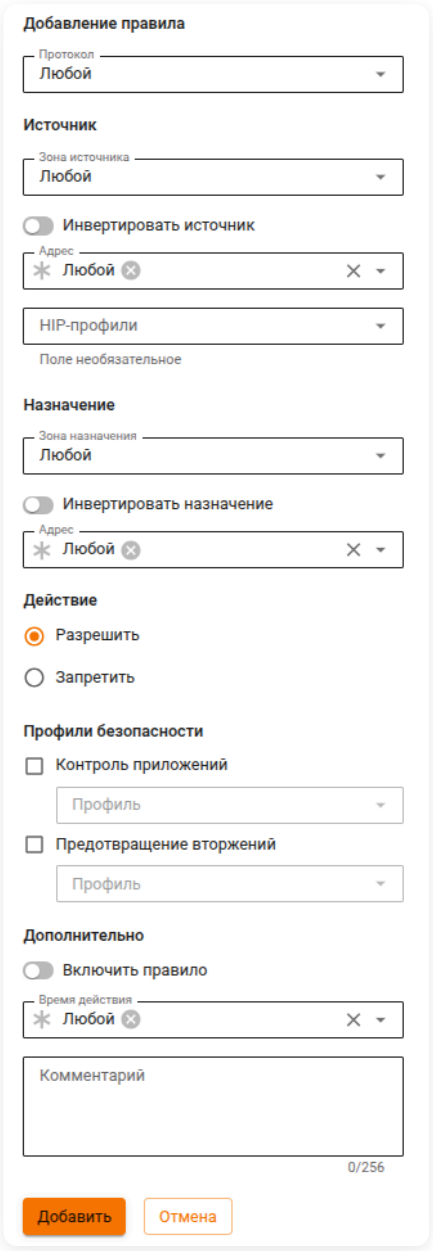
В качестве **Зоны источника** или **Зоны назначения** можно выбрать **Специальные** типы:

Специальные типы

- **Внешние интерфейсы** - все интерфейсы, используемые для подключения к интернету.
- **Внешние Ethernet-интерфейсы** - все Ethernet-интерфейсы, используемые для подключения к интернету.
- **Внешние VPN-интерфейсы** - все туннельные интерфейсы для подключения к интернету (Ethernet+PPPoE, Ethernet+PPTP, Ethernet+L2TP).
- **IPsec-интерфейсы** - все IPsec-интерфейсы, используемые для site-to-site-подключений к удаленным офисам.
- **Локальные интерфейсы** - все интерфейсы, используемые для подключения к клиентам в локальной сети.
- **Исходящий трафик устройства** - используется для фильтрации исходящего трафика самого устройства Ideco NGFW.
- **Клиентский VPN-трафик** - используется для фильтрации трафика, идущего от клиентов, подключившихся к NGFW по VPN.
- **Любой** - не фильтровать трафик по какому-либо типу интерфейса или зоны.

В Ideco NGFW нет подразделения локальных интерфейсов на VPN-интерфейсы и Ethernet, поскольку Ideco NGFW не имеет локальных VPN-интерфейсов.

FORWARD



Расшифровка полей

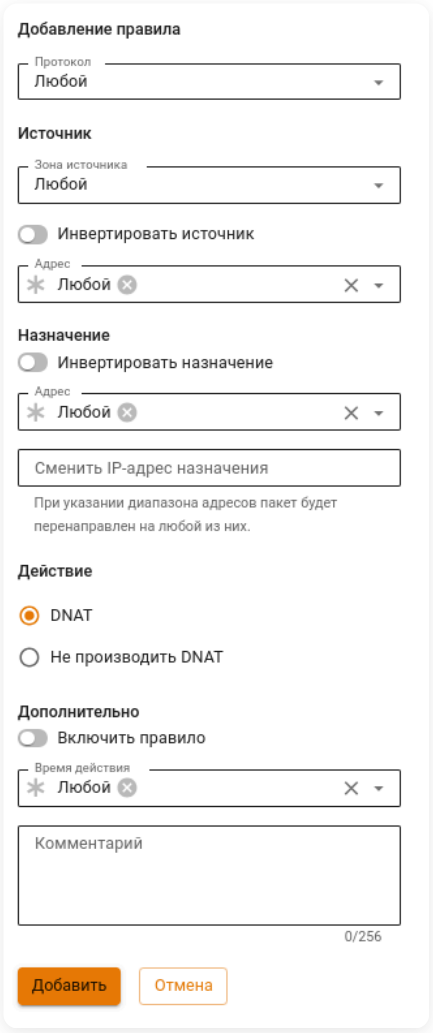
- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны или **Специальные типы**.
  - **Инвертировать 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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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.
  - **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 или **Специальные типы**.
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **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 их IP-адресов, файрвол автоматически это учтет).

Максимальное количество объектов в поле - 200.

- **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**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
- **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.
  - **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

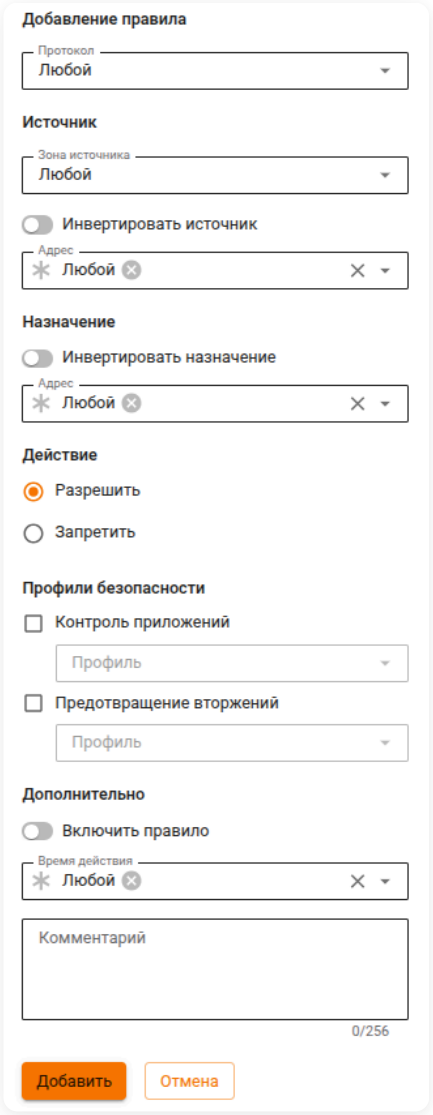


Расшифровка полей

- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).
- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны 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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 строке **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 их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 он пришел, если этот порт попадает в указанный диапазон.
- **Действия**:
  - **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.
  - **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 (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).

- **Источник**:
  - **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны 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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 строке **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 их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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.
- **Действия**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
- **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.
  - **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.

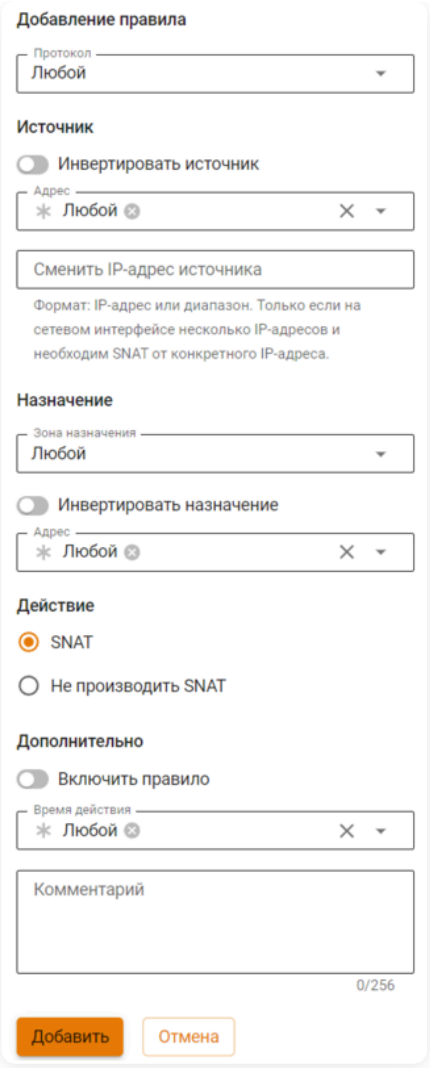
SNAT

> 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**.

> Пользовательские правила **SNAT** имеют приоритет над автоматическим **SNAT** для локальных сетей.



Расшифровка полей

- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).
- **Источник**:
  - **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 их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
  - **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 или **Специальные типы**.
- **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **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 их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200.
- **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.
  - **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.

Использование профилей безопасности

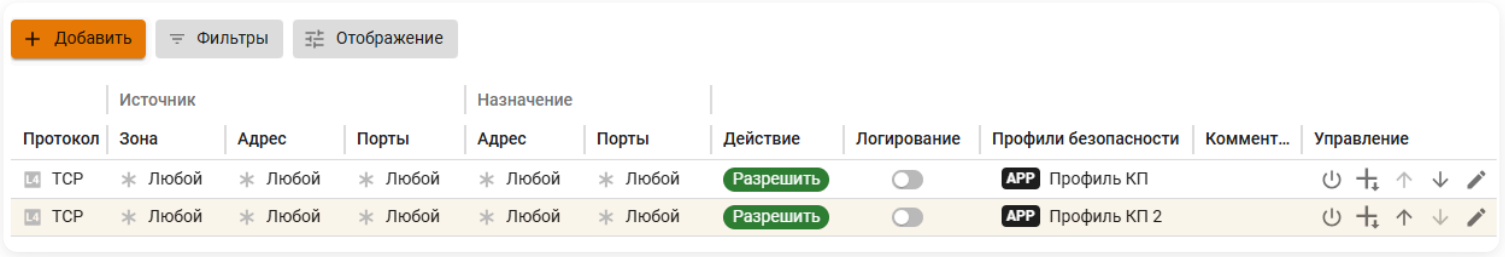
Файрвол Ideco NGFW обрабатывает правила последовательно, сверху вниз. Первое правило, условия которого совпадают с характеристиками проходящего трафика, определяет:

- 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".

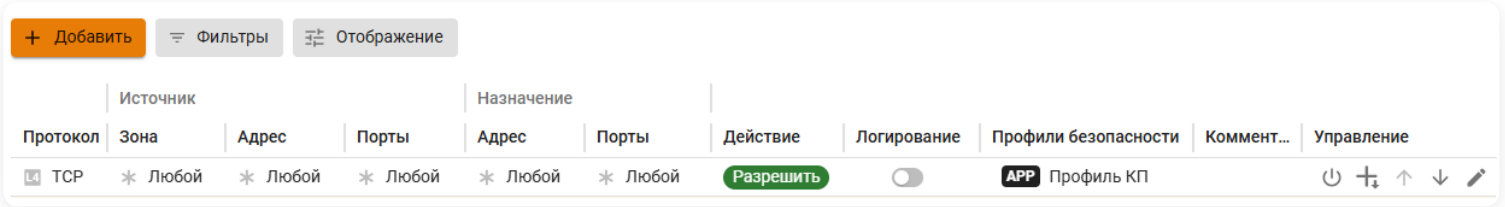


В этом случае при возникновении соответствующего трафика сотрудникам будет ограничен доступ только к социальным сетям - второе правило не будет применено, потому что трафик уже обработан вышестоящим правилом.

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 **Файрвол** → **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, т.к. **INPUT**-правила Файрвола 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, но **зона интерфейса источника сохраняется**.
- Не используйте зону, указанную в разделе **VPN-подключения** → **Основное**, для блокировки TCP. В противном случае HTTP- и HTTPS-трафик через эту зону не будет заблокирован.

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. Для предотвращения блокировки клиентского HTTP/HTTPS-трафика **рекомендуем**:
  - Создать правило, разрешающее трафик от пользователя.
  - Создать правило, разрешающее трафик для специальной зоны источника **Исходящий трафик устройства**.
- При создании правил **Файрвола** 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

- **Полный цикл обработки трафика в Ideco NGFW**
- **Порядок обработки веб-трафика в Ideco NGFW**
- **Объекты**
- **Профили устройств**
- **Логирование**
- **Контроль приложений**
- **Предотвращение вторжений**

Примеры создания правил файрвола

Настройка правил файрвола для IPsec-подключений

Чтобы настроить правило **Файрвола** 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 файрвола

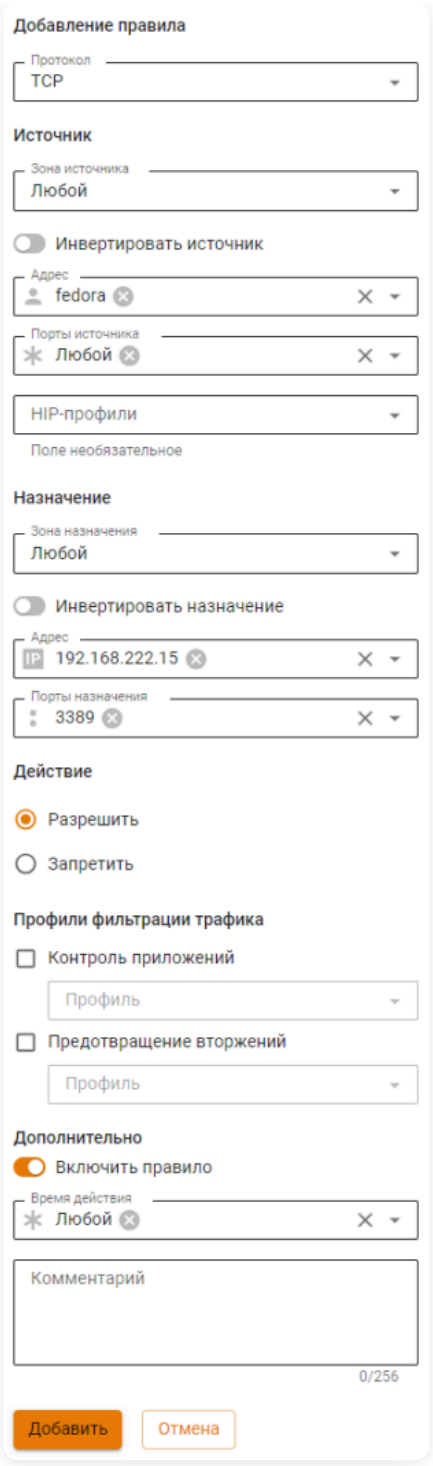
Вопросы блокировки программ удаленного управления (AmmyAdmin и TeamViewer), мессенджеров и другого ПО - описаны в статье Блокировка популярных ресурсов.

Доступ к терминальному серверу для определенного пользователя

1. На вкладке **Правила трафика** → **Файрвол** → **FORWARD** нажмите **Добавить**.

2. Заполните поля:

- **Протокол** - выберите TCP.
- **Адрес** - выберите пользователя или группу пользователей.
- **Назначения** - укажите адрес терминального сервера.
- **Порты назначения** - укажите порт 3389.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

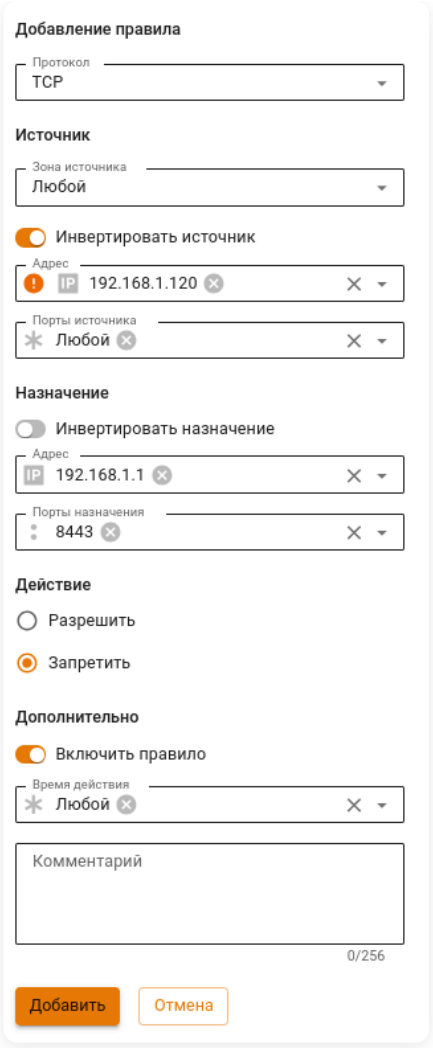


3. Нажмите **Добавить**.

Блокировка доступа к веб-интерфейсу (порт 8443) всем, кроме определенного адреса

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:



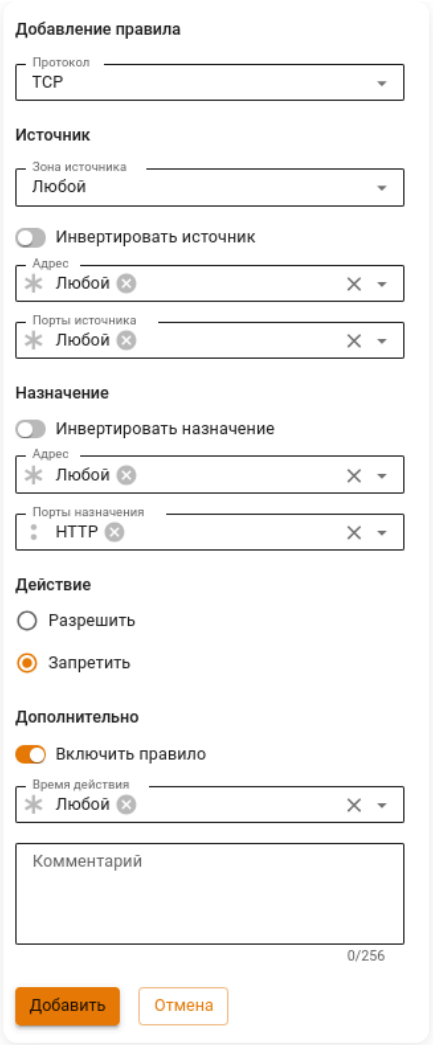
- Доступ к веб-интерфейсу будет разрешен только с IP-адреса **192.168.1.120**.
- **192.168.1.1** - IP-адрес Ideco NGFW в локальной сети.

Блокировка 80 порта Ideco NGFW

80 TCP порт используется для выпуска сертификатов Let`s Encrypt.

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **INPUT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:



Разрешение DNS-запросов через внешние DNS

ВАЖНО: Рекомендуем использовать в качестве DNS-сервер Ideco NGFW. Но если необходимо использовать внешний DNS-сервер, то выполните действия:

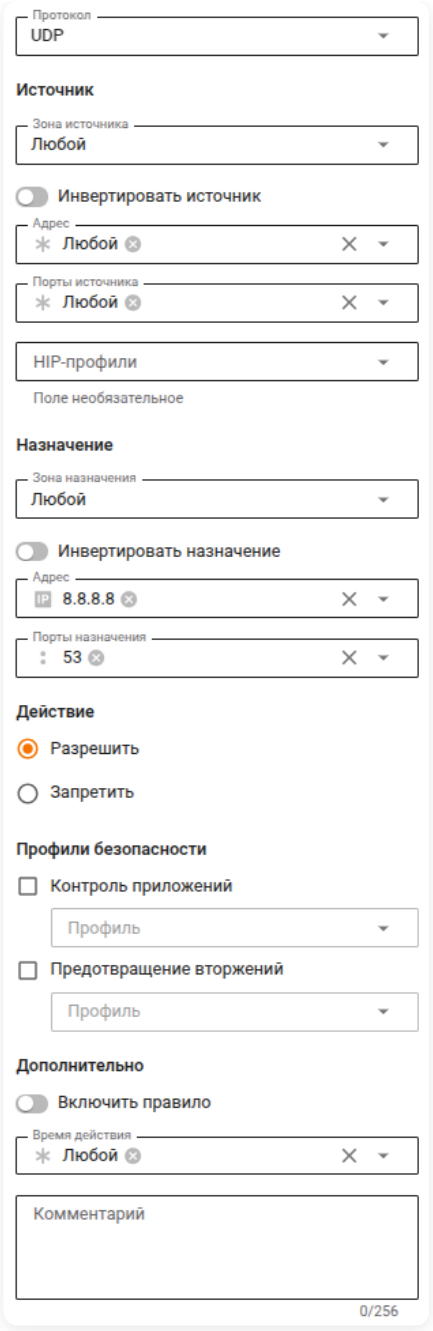
1. На вкладке **Защита и управление DNS** → **Внешние DNS** выключите **Перехват пользовательских DNS-запросов**.

2. Добавьте внешний DNS-сервер.

3. Перейдите на вкладку **Правила трафика** → **Файрвол** → **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.

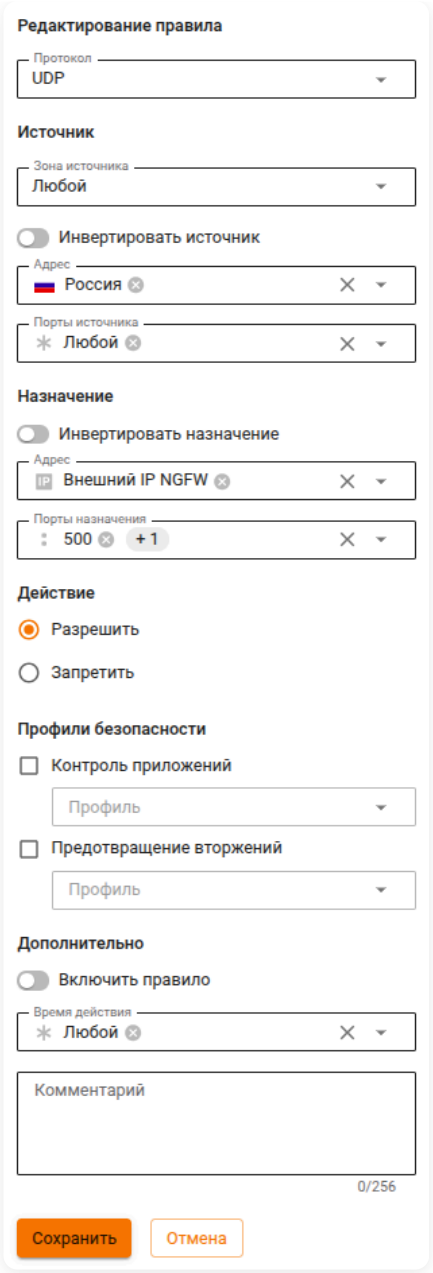
Доступ до Ideco NGFW только из определенной внешней сети по IKEv2/IPsec

Пример: нужно разрешить доступ до Ideco NGFW из России по VPN через IKEv2/IPsec.

ВАЖНО: Правило актуально, если на вкладке **INPUT** есть правило **Запретить все**.

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **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.
  - **Порт назначения** - укажите порты 500 и 4500.
- **Действие** - Разрешить.
- **Дополнительно** - включите правило.

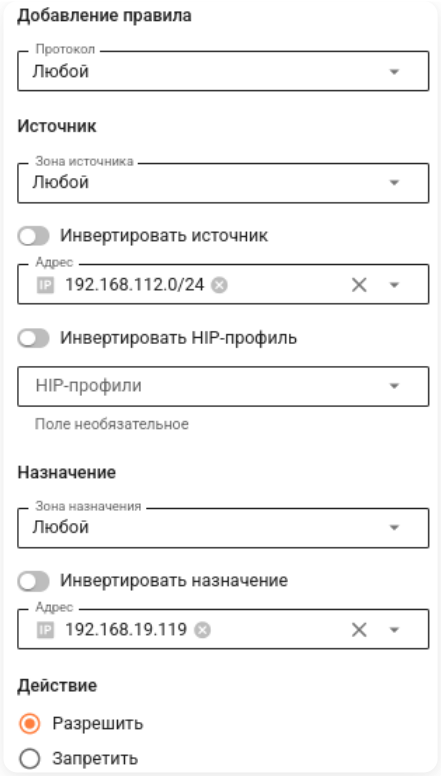
Разрешение доступа к конкретным ресурсам при наличии запрещающего весь трафик правила

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 на вкладку **Правила трафика → Файрвол → DNAT**.

2. Создайте правило, заполнив поля, как на скриншоте, и включите его:

- **5.120.1.25** - IP-адрес Ideco NGFW 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.

Логирование

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 Файрвола. 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 **Файрвола**: 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 раздел **Отчеты и журналы → Журнал трафика.

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 трафика** 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 трафика** при срабатывании правила **Файрвола**.

Действие **Не логировать** позволяет снять метку логирования.

Пример 1. Настройка логирования всего трафика на yandex.ru, кроме трафика от Иванова Ивана

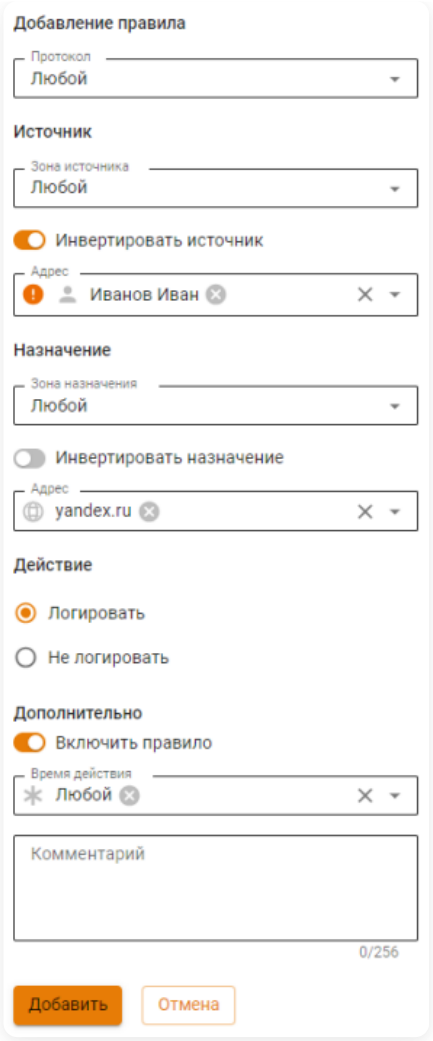
Настройте правило:

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:



Тестирование правил

На вкладке создаются тесты для проверки работы правил таблицы FORWARD и INPUT.

Тест - это конкретный пример, в котором проверяется доступ до определенного IP-адреса с учетом правил таблицы **Файрвола**. Во время тестирования NGFW генерирует тестовый пакет с заданным источником и назначением, после чего проверяет, как пакет проходит через **Файрвол**.

Рекомендуем использовать для источника порты из диапазона 49152 - 65535 (динамически выделяемые или частные порты, которые не регистрируются IANA).

Создание тестов

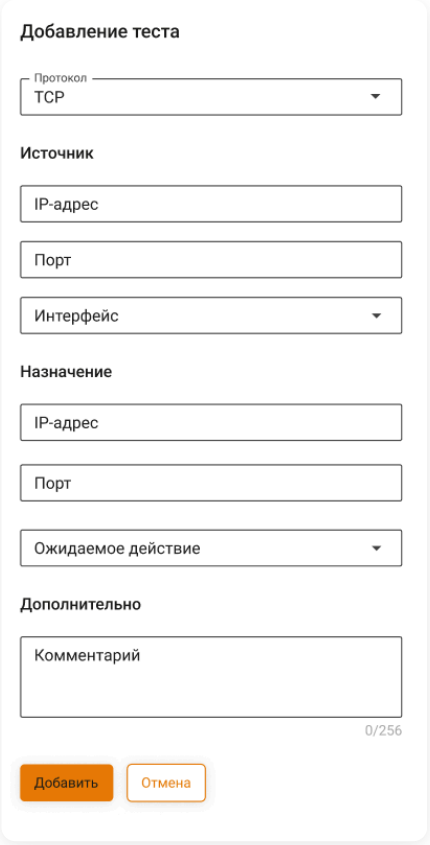
В качестве интерфейса источника можно выбрать:

- Туннельный (GRE).
- Локальный Ethernet.
- Внешний Ethernet.
- Внешний Ethernet + PPTP.
- Внешний Ethernet + L2TP.
- Внешний Ethernet + PPPoE.

Для создания теста выполните действия:

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **Тестирование правил** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

- **Протокол** (**TCP**/**UDP**).
- **IP-адрес** - адрес источника и назначения.
- **Порт** - порт источника и назначения.

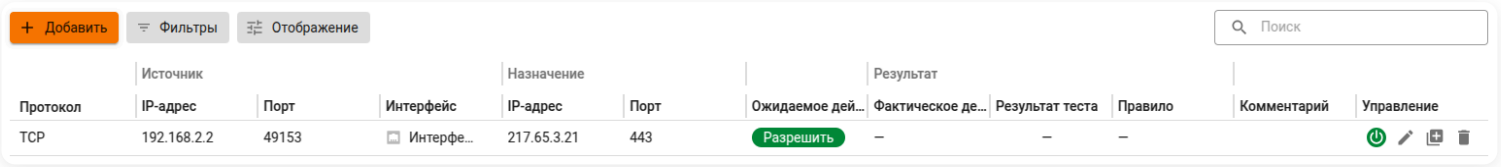
- **Интерфейс** - сетевой интерфейс источника.

> Выбранный интерфейс должен быть настроен и подключен. Если интерфейс отключен, Ideco NGFW не сможет выполнить тестирование.

- **Ожидаемое действие** - Разрешить или Запретить.
- **Комментарий** - необязательное поле.

3. Нажмите **Добавить**.

Созданные тесты добавляются в таблицу:



Запуск и результат тестирования

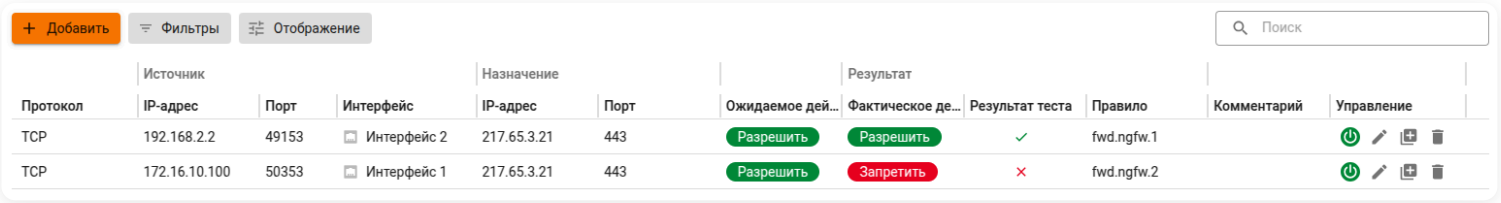
Запуск теста не происходит автоматически при его добавлении. Для запуска:

1. Включите нужный тест .

2. Нажмите **Запустить тестирование** в левом нижнем углу вкладки.

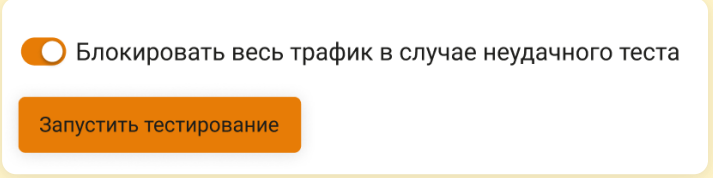
> Если тест выключен, то его тестирование запускаться не будет.

При совпадении ожидаемого и фактического действия тестирование считается успешным:

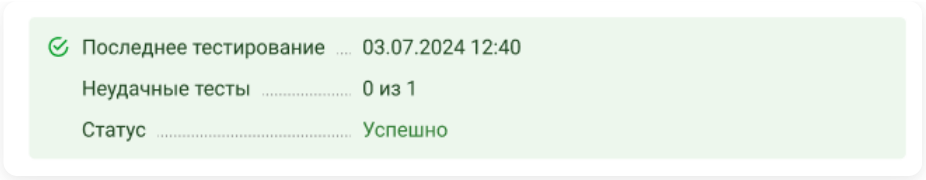


Залогированные правила вида `fwd.sys.xxx`, `inp.sys.xxx`, `out.sys.xxx` в столбце **Правило** - результат срабатывания системного правила, которое разрешило или запретило прохождение трафика в рамках проверки, если не сработало ни одно пользовательское правило. Это правила **Файрвола**, которыми нельзя управлять из веб-интерфейса Ideco NGFW, они всегда включены. Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Файрвола**. Посмотреть системное правило, которое сработало, можно через Терминал.

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 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.

Предварительная фильтрация

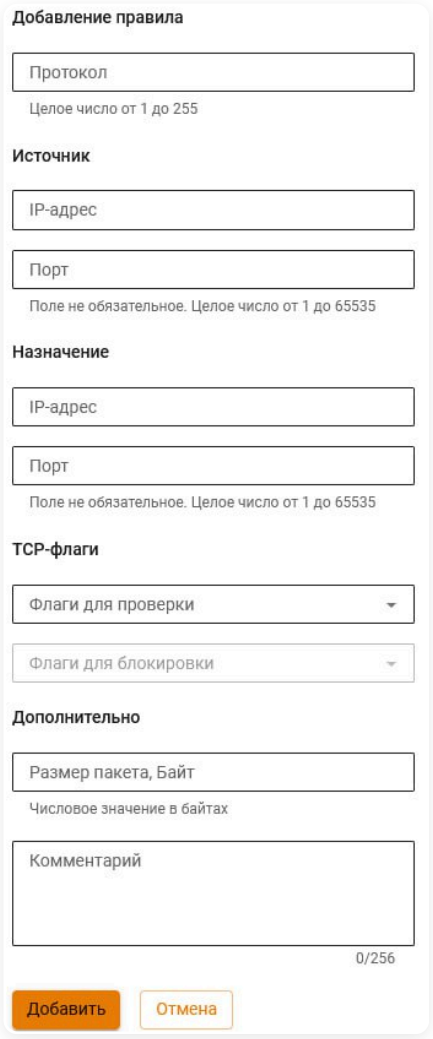
Вкладка **Предварительная фильтрация** позволяет заблокировать весь трафик, попадающий под условия таблицы, до просмотра таблиц **Файрвола** (например, **FORWARD** или **INPUT**). Используйте этот раздел, если требуется фильтрация пакетов на уровне TCP/IP.

Включение хотя бы одного правила **Предварительной фильтрации** может привести к снижению сетевой производительности NGFW примерно на 20%.
При выключении правила производительность сразу восстановится.

Создание правил

1. Перейдите на вкладку **Правила трафика** → **Файрвол** → **Предварительная фильтрация** и нажмите **Добавить**.

2. Заполните поля правила:



Расшифрока 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 он 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 **Разрешить интернет всем**.

Аппаратная фильтрация

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 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.

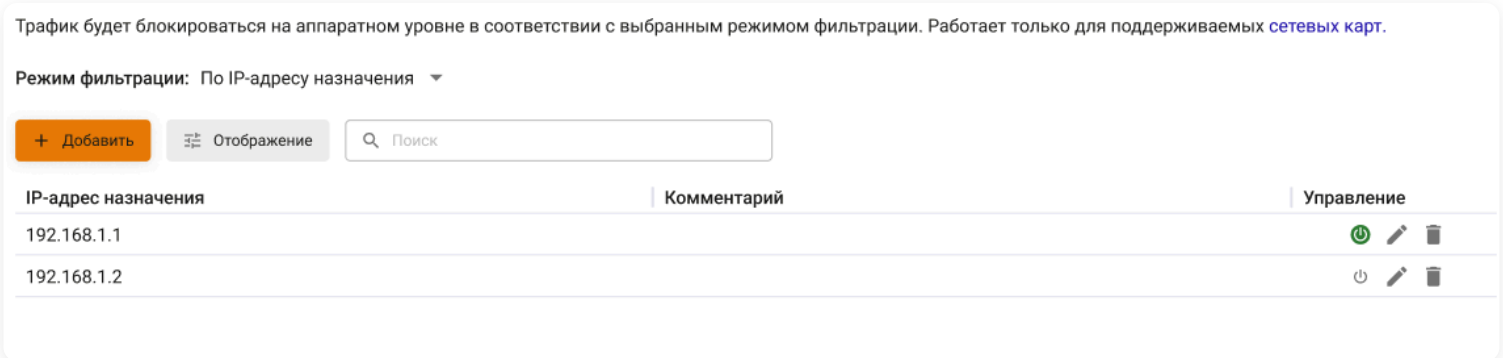
Список поддерживаемых сетевых карт

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

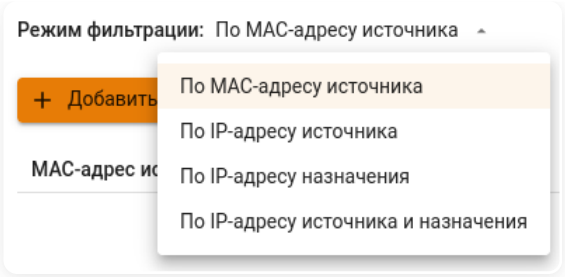
Администратор может создать не более 2500 правил каждого типа фильтрации.

Созданные правила отображаются в таблице в зависимости от выбранного режима фильтрации:



Чтобы создать правило определенного типа, выполните действия:

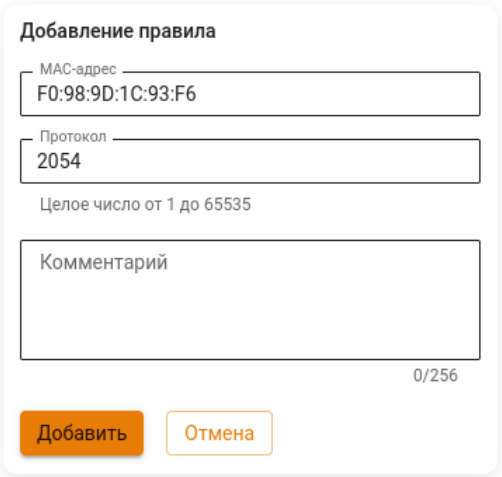
1. Выберите режим фильтрации, нажмав на кнопку в левом верхнем углу:



- По MAC-адресу источника;
- По IP-адресу источника;
- По IP-адресу назначения;
- По IP-адресу источника и назначения.

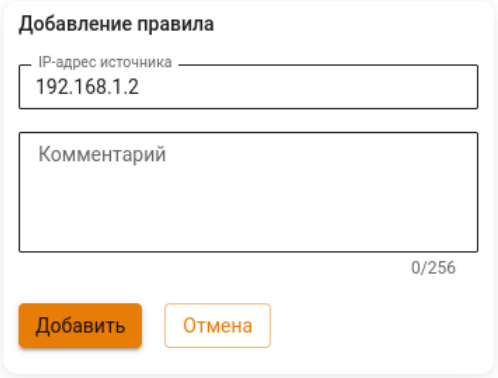
2. Нажмите **Добавить** и заполните поля:

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*;
- **Коментарий** - поле необязательное.

Фильтрация по IP-адресу источника

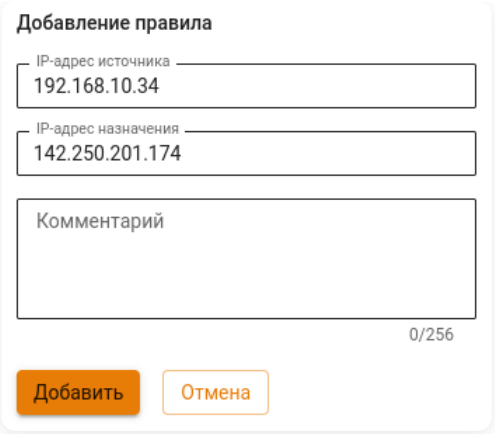


- **IP-адрес источника** - введите IP-адрес источника трафика;
- **Коментарий** - поле необязательное.

Фильтрация по IP-адресу назначения

- IP-адрес назначения - введите IP-адрес назначения трафика;
- Коментарий - 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;
- **Коментарий** - поле необязательное.

3. Нажмите **Добавить**.

4. Включите правило или оставьте его выключенным.

Отключить аппаратную фильтрацию можно, выключив опцию **Файрвол** в соответствующем разделе.

Контент-фильтр

Название службы раздела **Контент-фильтра**: `ideco-content-filter-backend`.

Список имен служб для других разделов доступен по ссылке.

Контент-фильтр проверяет запрашиваемые сайты в базе URL-адресов из пользовательских категорий Ideco NGFW. 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 Файрвол.

Контент-фильтр включает четыре вкладки:

- Правила - создание и управление правилами фильтрации.
- Пользовательские категории - управление собственных списков.
- 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 поставьте флаг **Включить логирование** на вкладке **Сервисы → Прокси → Основное**.

Для изменения страницы блокировки **Контент-фильтра** обратитесь в Техническую поддержку.

Полезные ссылки

- Файрвол
- Настройка фильтрации HTTPS
- Блокировка чат-ботов

- Техническая поддержка

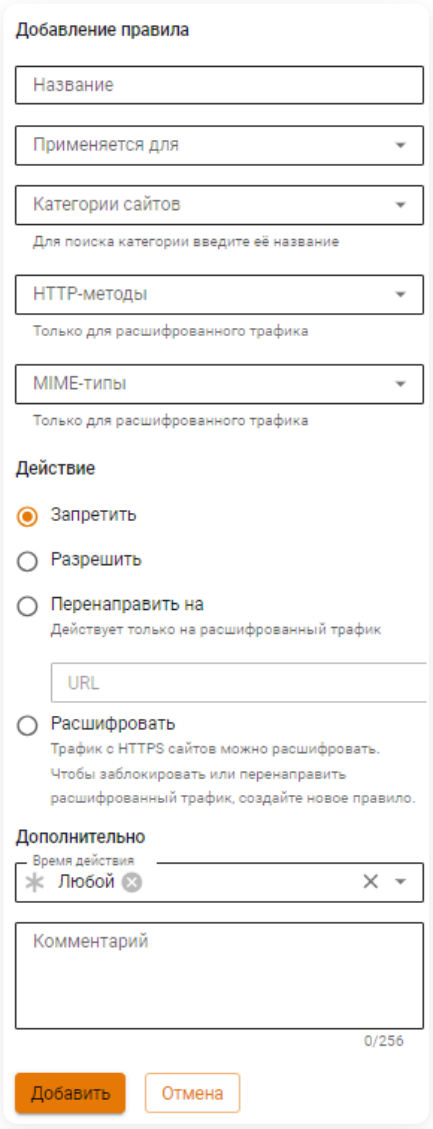
Правила

Правила создаются на вкладке **Правила трафика → Контент-фильтр → Правила**. Помимо возможности добавления правил **Контент-фильтра**, вкладка содержит:

- **Строку поиска категории URL для категоризации**. Позволяет найти, к какой категории относится URL для создания правила.
- **Таблицу созданных правил**. Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. Таким образом, если вышестоящим правилом будет разрешен какой-то ресурс для определенной группы пользователей, то правила ниже применяться не будут. Можно создавать гибкие настройки фильтрации, исключая нужных пользователей вышестоящими правилами из правил блокировки. Аналогичным образом действуют правила расшифровки HTTPS.

Создание правил

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



Расшифровка полей

- **Название** - название добавляемого правила.
- **Применяется для** - пользователь или группа пользователей, IP-адреса или список IP-объектов, для которых применяется правило.
- **Категории сайтов** - поле для выбора предустановленной или пользовательской категории, перечень ресурсов, на которые распространяется действие правила.

Для расшифрованного трафика при создании и редактировании правила **Контент-фильтра** доступны более детальные настройки доступа к ресурсам с помощью HTTP-методов запроса и MIME-типов. Если поля остаются пустыми, проверка по ним не осуществляется.

- **HTTP-методы** - методы запроса, которые будут применяться для всего HTTP- или HTTPS-трафика. Используются для более точной фильтрации трафика, например, для ограничения скачивание чего-либо на сайтах, заполнение 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.
- **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.
- **Действия**:
  - **Запретить** - запрещает трафик.
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.
  - **Перенаправить на** - позволяет указать URL, на который будет перенаправлен расшифрованный трафик.
  - **Расшифровать** - расшифровывает трафик с HTTPS сайтов.

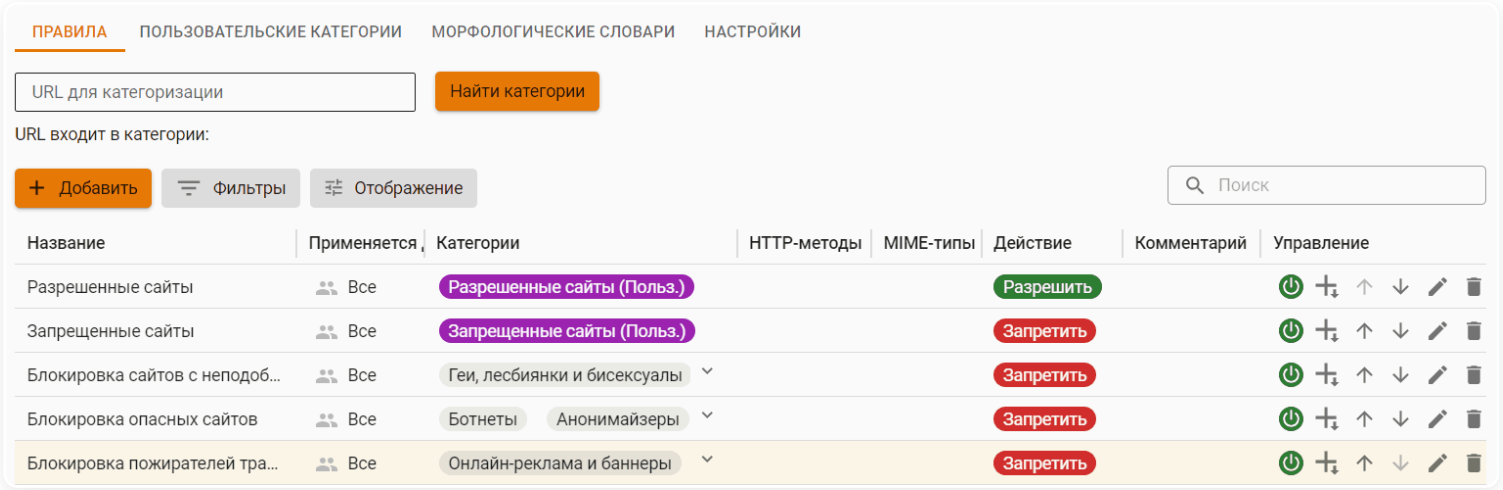
Если выбрать действие **Перенаправить на**, то нужно создать аналогичное правило с действием **Расшифровать** и поместить его выше перенаправляющего правила.

- **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**.

Управление правилами

В столбце **Управление** можно включать или выключать правило, менять его приоритет, редактировать и удалять. Правила контентной фильтрации применяются сразу после создания или включения:



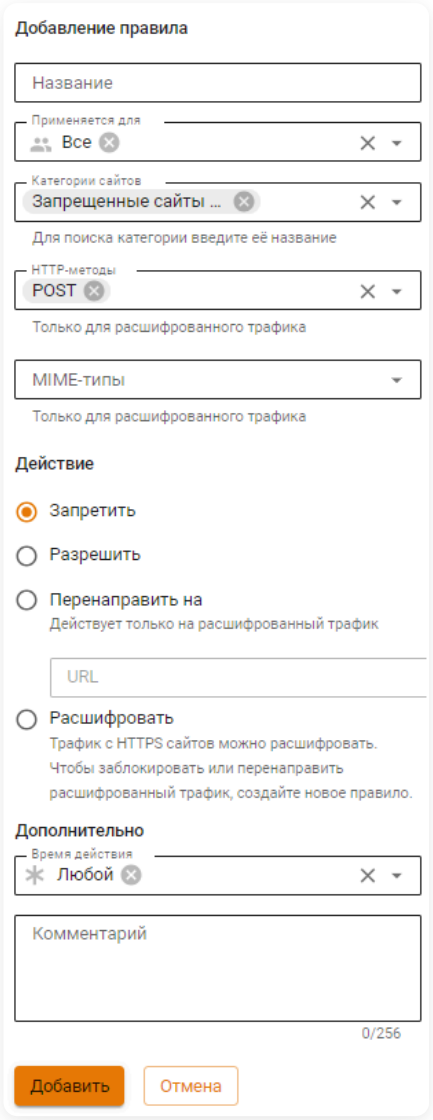
При наличии большого количества правил **Контент-фильтра** в таблице воспользуйтесь кнопкой **Фильтры**.

Дополнительно

Пример настройки HTTP-метода

Необходимо запретить пользователям вводить данные на запрещенных сайтах.

Перейдите в раздел **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**. Заполните поля:



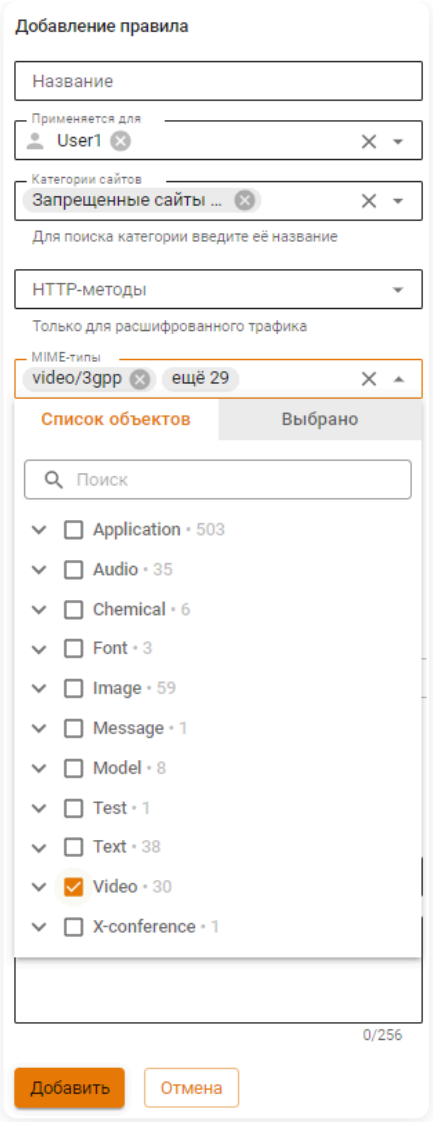
- **Применяется для** - выберите пользователей, для которых будет работать правило.
- **Категории сайтов** - выберите категорию сайтов, для которых должно работать правило, например, **Запрещенные сайты**.
- **HTTP-методы** - выберите метод `POST`, чтобы запретить отправку данных на определенный ресурс.
- 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).

Пример настройки MIME-типов

Необходимо запретить конкретному пользователю (например, User1) воспроизводить видеоконтент на запрещенных сайтах.

Перейдите в раздел **Правила трафика** → **Контент-фильтр** → **Правила** и нажмите **Добавить**. Заполните поля:

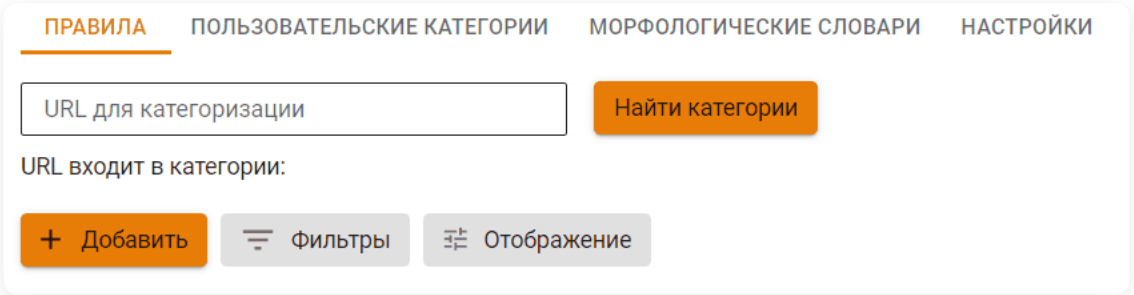


В поле **Категории сайтов** укажите предварительно созданную пользовательскую категорию **Запрещенные сайты**. В поле **MIME-типы** выберите все форматы группы **Video**. Примените действие правила **Запретить**. При сохранении правила сайт откроется, если трафик не заблокирован другим правилом, но видеоконтент не воспроизведется.

Диагностика

Если правила контентной фильтрации не действуют, проверьте следующие параметры в настройках:

- IP-адрес компьютера пользователя должен соответствовать его адресу в авторизации (раздел **Мониторинг - Сессии пользователей**), пользователь должен находиться в нужной группе, на которую назначено правило.
- IP-адрес пользователя и ресурса, к которому обращается, не должен входить в исключения прокси-сервера.
- Проверьте правильность категоризации ресурса, к которому обращаетесь, в поле **URL для категоризации** на вкладке **Правила**:



- В браузере и на компьютере пользователя не используются функции или плагины VPN, не прописаны сторонние прокси-серверы.

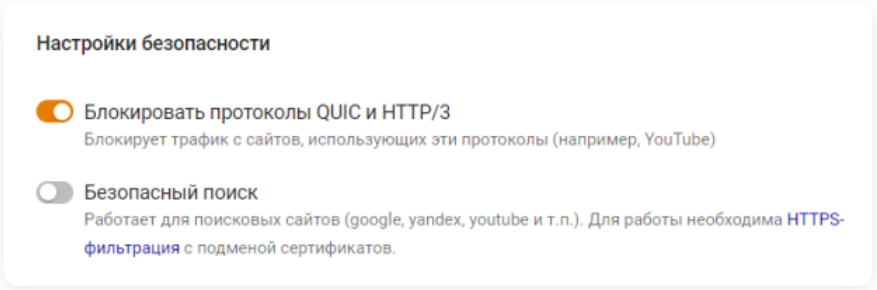
Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

Блокировка загрузки файлов в файлообменники

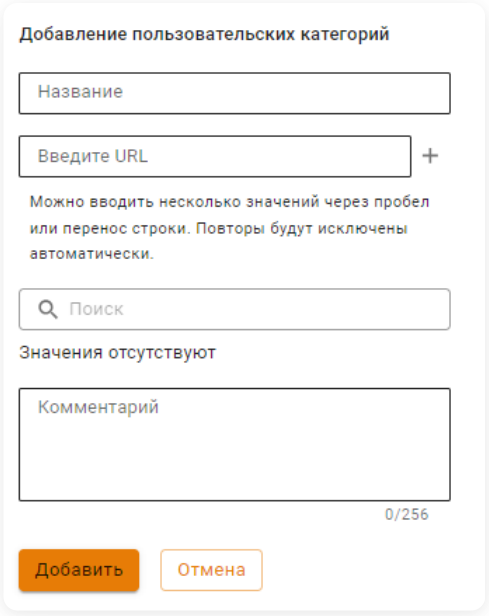
Блокирование этой категории требует особой настройки правил **Контент-фильтра**. В случае с файлообменниками расшифровки трафика может быть недостаточно у категорий: **Файлообменники, Файловые хранилища, Файловые архивы** и **Загрузка файлов в файлообменники**.

Чтобы заблокировать загрузку файлов в облака через браузер, выполните действия:

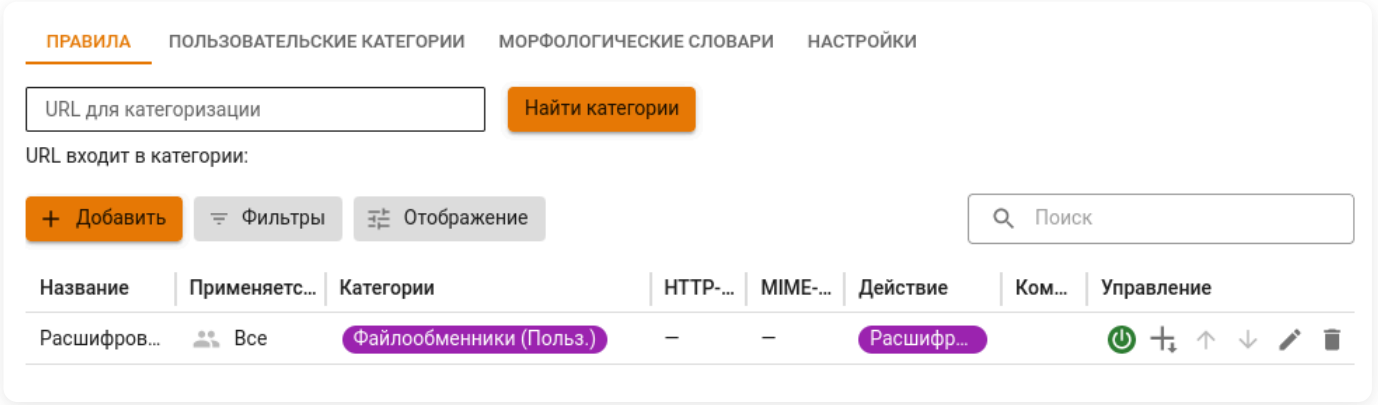
1. Включите **Блокировку протоколов Quic/HTTP3** на вкладке **Контент-фильтр** → **Настройки**:



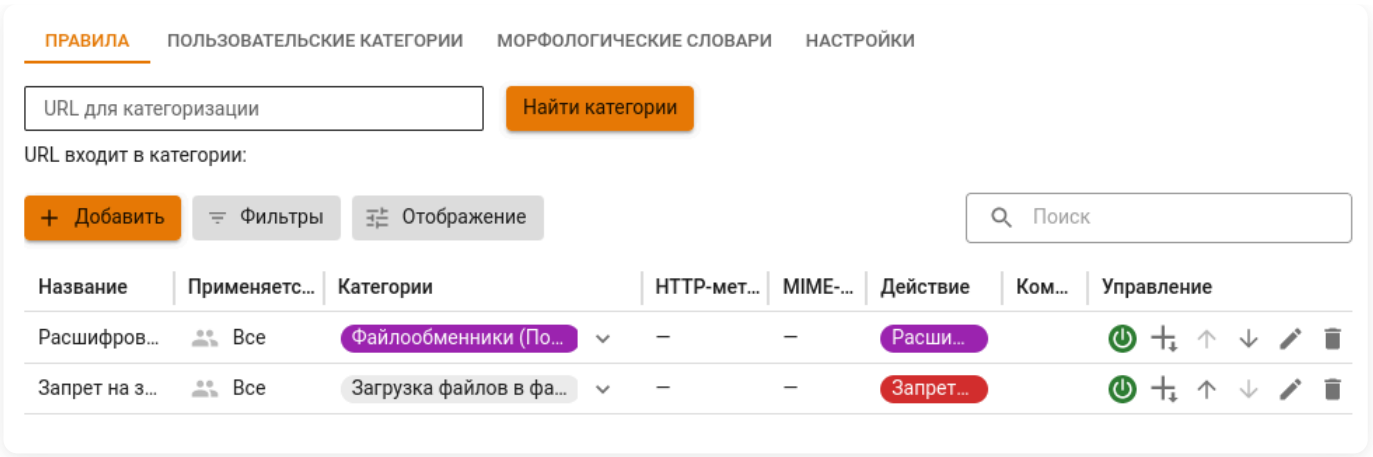
2. Создайте пользовательскую категорию для расшифровки трафика и укажите домены нужных файлообменников, используя маску `example.com`:



3. Создайте правило, расшифровывающее трафик созданной в п. 2 категории:



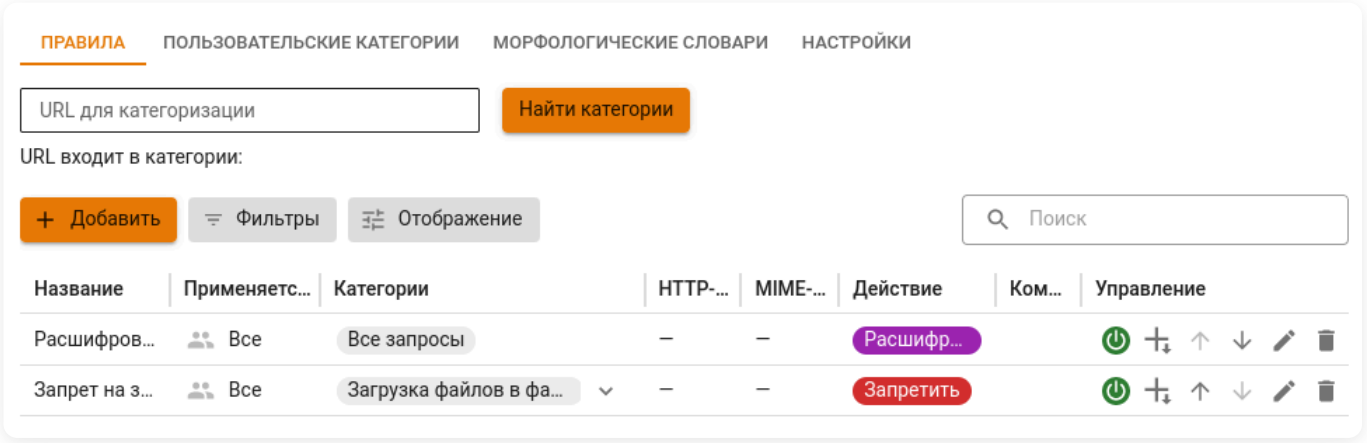
4. Ниже создайте запрещающее правило для категории **Загрузка файлов в файлообменник**:



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.

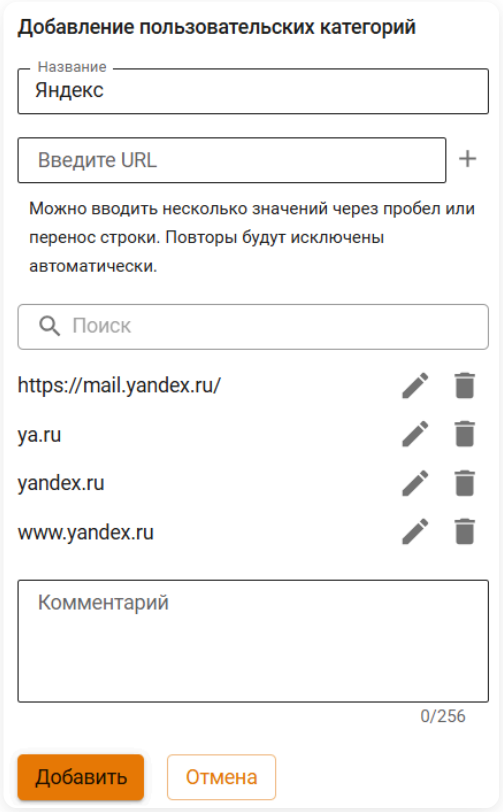
Описание категорий Контент-фильтра

В Ideco NGFW категории сайтов разделены на следующие виды:

- **Пользовательские** - категории, созданные на вкладке **Пользовательские категории**.
- **Специальные** - системные категории для фильтрации запросов.
- **Расширенные** - автоматически пополняемые списки сайтов, отсортированные по темам.
- **Файлы** - восемь сформированных категорий файлов, блокируемых по расширениям и MIME-типами. Предустановленные группы файлов (Исполняемые файлы, Архивы, Видеофайлы, Аудиофайлы, Flash-видео, Active-X, Torrent-файлы, Документы) нельзя редактировать. Для фильтрации HTTPS-трафика по категории файлов требуется настроить 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 его включить достаточно указать домен test.ru (все его поддомены также попадут под это правило).

Если URL или домен содержит специальные символы (。 или •), оставьте их в исходном виде. Адрес будут автоматически закодирован в

формат punycode.

- **Поиск** - поле поиска добавленных URL.
- **Комментарий** - можно заполнить или оставить пустым.

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) в 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

База URL-адресов, отсортированных по тематикам. Для обновления расширенных категорий включите опцию **Расширенная база категорий** на вкладке **Настройки**.

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
Юмор	Юмористические и развлекательные сайты

В версии 20 Ideco NGFW состав категорий контент-фильтра изменен. Часть категорий удалены, часть объединены в общие категории.

При переходе Ideco NGFW с версии 19 на 20 в правилах применятся новые категории в соответствии с таблицей **Изменение категорий**. Если в версии 20 нужная категория отсутствует, то поле **Категории сайтов** останется пустым, а правило перестанет работать.

Категории без изменений

- Войска и вооружения
- Знакомства
- ИИ Чат-боты
- Интернет-магазины
- Искусство
- Казино, лотереи, тотализаторы
- Компьютерные игры
- Наркотики
- Недвижимость
- Неизвестные сайты
- Некоммерческие организации
- Образование и учебные учреждения
- Онлайн-реклама и баннеры
- Платные сайты мобильных операторов
- Поисковые системы
- Правительство
- Сайты для детей
- Социальные сети
- Спорт
- Туризм
- Форумы
- Фотогалереи
- Юмор

Удаленные категории

- Взлом.
- Высокий уровень риска
- Криминальные навыки/хакинг
- Оплата за серфинг
- Пиратство и хищение авторских прав
- Природа и ее сохранение
- Системы централизованной аутентификации
- Страхование
- Частные IP-адреса

Изменение категорий

v19	v20
Web-почта	Веб-почта
Аборты	Здоровье и здравоохранение

v19	v20
Аборты - одобрение	Здоровье и здравоохранение
Аборты - осуждение	Здоровье и здравоохранение
Автомобили/Транспорт	Автомобили и транспорт
Алкоголь	Алкоголь и табак
Анонимайзеры	Прокси и анонимайзеры
Архитектура	Наука и технологии
Астрология и гороскопы	Астрология
Атеизм и агностицизм	Религия и атеизм
Аудио для прослушивания и скачивания	Радио и музыка онлайн
Аукционы и рынки	Торговля и покупки
Банки	Финансы и финансовые учреждения
Безопасность	Порталы
Бизнес и услуги (общая)	Бизнес, экономика, маркетинг
Бизнес/Сервисы	Бизнес, экономика, маркетинг
Биотехнологии	Наука и технологии
Благотворительные учреждения	Некоммерческие организации
Ботнеты	Сети зараженных устройств и управляющие серверы
Веб-хостинг, интернет-провайдеры и телекоммуникационные компании	Компьютеры и Интернет
Видео для прослушивания и скачивания	Фильмы и видео онлайн
Виртуальные открытки	Досуг и развлечения
Возможный риск	Неизвестные сайты
Вооруженные силы	Войска и вооружения
Геи, лесбиянки и бисексуалы	Сайты для взрослых
Готовые домашние задания	Плагиат и рефераты
Для взрослых	Сайты для взрослых
Дом, сад и семья	Дом, семья, хобби
Дом/Отдых	Дом, семья, хобби
Дома престарелых и уход за больными	Здоровье и здравоохранение
Домашние животные	Дом, семья, хобби
Доставка и логистика	Бизнес, экономика, маркетинг
Еда и рестораны	Досуг и развлечения
Законодательство и политика	Политика, общество, закон
Запаркованные	Неиспользуемые домены
Здоровье	Здоровье и здравоохранение
Здравоохранение и медицина	Здоровье и здравоохранение
Игрушки	Торговля и покупки
Изображения жестокого обращения с детьми	Сексуальное насилие над детьми (Arachnid)
Интернет и IP-телефония	Компьютеры и Интернет
Информационная безопасность	Компьютеры и Интернет
Каталоги	Порталы
Компьютеры и технологии	Компьютеры и Интернет
Конкурсы и опросы	Досуг и развлечения
Контент серверы	Content Delivery Networks
Криминальные навыки	Агрессия, расизм, терроризм
Купальные костюмы	Торговля и покупки
Купоны	Досуг и развлечения
Литература и книги	Интернет-библиотеки
Марихуана	Наркотики

v19	v20
Маркетинговые услуги	Торговля и покупки
Мгновенные сообщения	Чаты и мессенджеры
Мебель для дома и офиса	Торговля и покупки
Мобильные телефоны	Компьютеры и Интернет
Мода и красота	Досуг и развлечения
Музыка	Радио и музыка онлайн
Мультфильмы, аниме и комиксы	Аниме
Насилие	Агрессия, расизм, терроризм
Не для детского просмотра	Сайты для взрослых
Недоступные	Неизвестные сайты
Неизвестный уровень риска	Неизвестные сайты
Нераспознаваемый контент	Неизвестные сайты
Нетрадиционные религии и оккультные верования	Религия и атеизм
Новости	Новости и СМИ
Обзоры продукции и Сравнение цен	Порталы
Оборудование, ПО, электроника	Компьютеры и Интернет
Онлайн-офисы	Порталы
Онлайн-торговля акциями	Финансы и финансовые учреждения
Онлайн-управление информацией	Порталы
Откровенные изображения	Сайты для взрослых
Парки, зоны отдыха и спортивные залы	Досуг и развлечения
Переадресация	Запаркованные домены
Переводчики	Образование и учебные учреждения
Персональные страницы	Блоги и персональные сайты
Персональные страницы и блоги	Блоги и персональные сайты
Пиринговые сети	Торренты и P2P-сети
Питание и диеты	Здоровье и здравоохранение
Пищевые добавки и витамины	Здоровье и здравоохранение
Поиск работы	Работа и найм
Поисковики изображений	Поисковые системы
Политика и закон	Политика, общество, закон
Порнография	Порнография и секс
Порнография/секс	Порнография и секс
Порталы	Порталы
Производство	Наука и технологии
Профессиональные сообщества	Форумы
Развлекательные места и события	Туризм
Развлекательные новости и сайты про знаменитостей	Досуг и развлечения
Развлечения и видео	Категория разделена на две: Фильмы и видео онлайн; Досуг и развлечения
Разное	Неизвестные сайты
Религии	Религия и атеизм
Рестораны	Торговля и покупки
Сайты сообществ	Форумы
Самопомощь и зависимости	Здоровье и здравоохранение
Секс и Эротика	Порнография и секс
Сексуальное воспитание и образование	Сайты для взрослых
Сельское хозяйство	Бизнес, экономика, маркетинг
Сквернословие	Грубость, матершина, непристойность

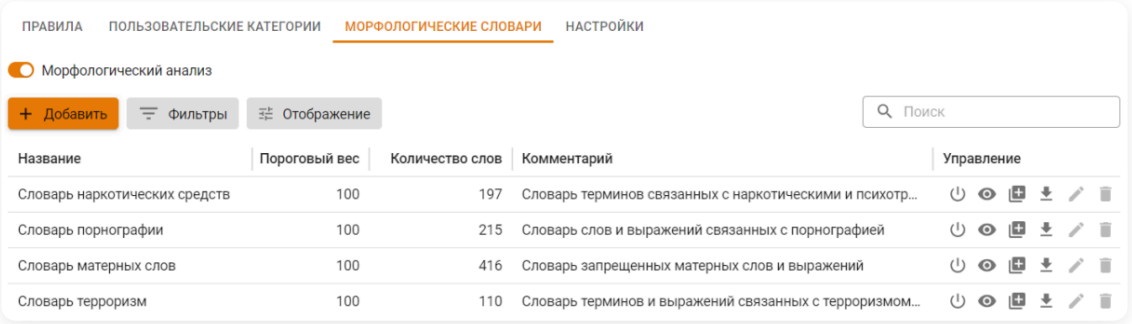
v19	v20
Скомпрометированные	Вредоносное ПО
Сообщества лоббистов и торговые ассоциации	Торговля и покупки
Социальные сообщества	Социальные сети
Спам	Онлайн-реклама и баннеры
Список Минюста	Федеральный список Минюста
Спонсируемые государством	Правительство
Спорт и отдых	Спорт
Спортивная охота	Спорт
Спортивные соревнования	Спорт
Справочные материалы и карты	Порталы
Средний уровень риска	Неизвестные сайты
Табак	Алкоголь и табак
Тайный сбор информации	Вредоносное ПО
Текстовые сообщения	Чаты и мессенджеры
Телевидение и фильмы	Фильмы и видео онлайн
Технологии (в целом)	Наука и технологии
Только для взрослых (18+)	Сайты для взрослых
Торговля и покупки	Интернет-магазины
Торрент-трекеры	Торренты и P2P-сети
Транспортные средства	Автомобили и транспорт
Удаленный доступ	Компьютеры и Интернет
Учебные заведения	Образование и учебные учреждения
Учебные материалы и исследования	Образование и учебные учреждения
Файловые архивы	Категория разделена на две: Фотогалереи; Компьютеры и Интернет
Файловые хранилища	Файловые архивы
Файлообменники	Торренты и P2P-сети
Фармацевтика	Здоровье и здравоохранение
Финансовые инструменты и котировки	Финансы и финансовые учреждения
Финансы	Финансы и финансовые учреждения
Финансы (в целом)	Финансы и финансовые учреждения
Фитнес и Отдых	Досуг и развлечения
Фишинг/мошенничество	Фишинг и поддельные сайты
Хобби и Досуг	Дом, семья, хобби
Центры распространения вредоносного ПО	Вредоносное ПО
Центры управления и контроля	Сети зараженных устройств и управляющие серверы
Чаты	Чаты и мессенджеры
Чаты/Мессенджеры	Чаты и мессенджеры
Шпионские и опасные сайты	Вредоносное ПО
Шпионское и сомнительное ПО	Вредоносное ПО
Экстремизм	Агрессия, расизм, терроризм
Эротика	Сайты для взрослых

При нахождении несоответствия сайта и категории обратитесь в техническую поддержку

Морфологические словари

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 предустановлены четыре словаря (по умолчанию отключены):

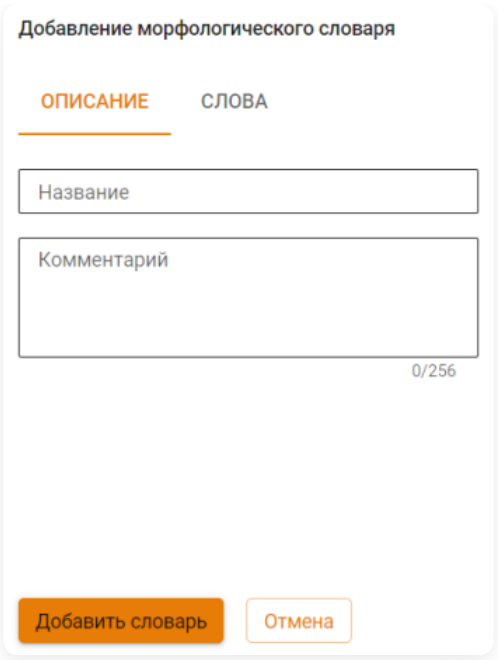
- Словарь наркотических средств
- Словарь порнографии
- Словарь матерных слов
- Словарь терроризм

Предустановленные словари можно включать или отключать, но нельзя редактировать и удалять.

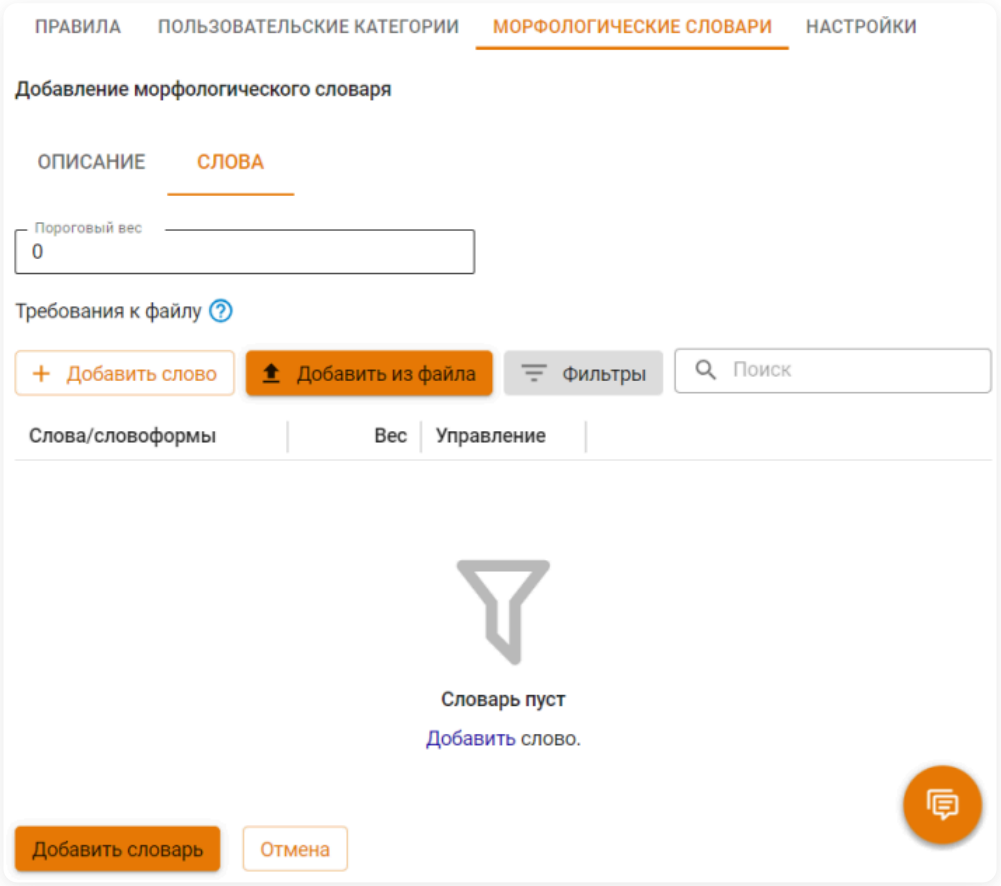
Добавление морфологического словаря

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

- На вкладке **Описание**:
  - **Название** - название добавляемого словаря.
  - **Комментарий** - произвольный текст. Значение не должно быть длиннее 255 символов:



- На вкладке **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:



2. 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.

Чтобы снизить вероятность блокировки сайта из-за морфологического анализа, уменьшите вес слов. Для повышения вероятности блокировки - увеличьте вес.

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/словосочению 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").

3. Для сохранения настроек нажмите **Добавить словарь**.

Если в таблице большое количество морфологических словарей, воспользуйтесь кнопкой **Фильтры**.

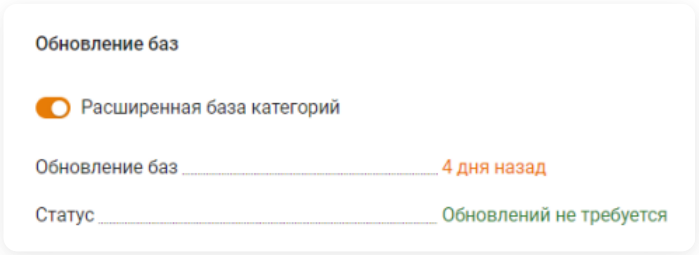
Результат морфологического анализа представлен в разделе **Отчеты и журналы** → **Журнал веб-трафика**:

		Антивирус		Контент-фильтр					
Дата и время	Резу...	Резу...	Анти...	Результат проверки	Расшифровка	Название правила	Причина запрета	Категории сайта	Категория сработки
02.06.2025, 17:12:04	✗	✓	–	✗	✗	–	Словарь порнографии	Все некатегоризирован...	Все некатегоризированные
02.06.2025, 17:12:04	✗	✓	–	✗	✗	–	Словарь порнографии	Все некатегоризирован...	Все некатегоризированные

Настройки

Обновление баз

Активация опции **Расширенная база категорий** включает более 140 автоматически обновляемых категорий, доступных только при активной подписке в платных версиях продукта:



Если отключить опцию **Расширенная база категорий**, то все правила, включающие в себя 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 на вкладке **Прокси** → **Исключения**.

Безопасный поиск - принудительно включает безопасный поиск в поисковых системах (Google, Yandex, YouTube, Yahoo, Bing, Rambler).

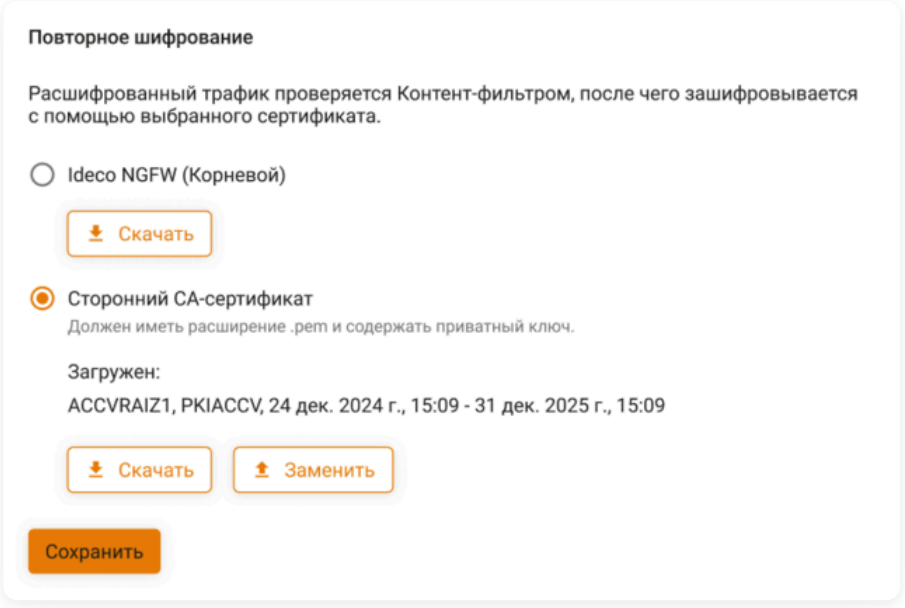
Для корректной работы необходимо включить HTTPS-фильтрацию с подменой сертификата для этих сервисов.

Повторное шифрование

Если для повторного шифрования требуется использовать сторонний сертификат (не корневой сертификат Ideco NGFW):

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 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**. Таким образом, передающийся по защищенному HTTPS-соединению трафик становится доступным для обработки всем модулям Ideco NGFW: антивирусу Касперского, внешним ICAP-сервисам и Контент-фильтру (можно категоризировать полный URL запроса и MIME-тип контента).

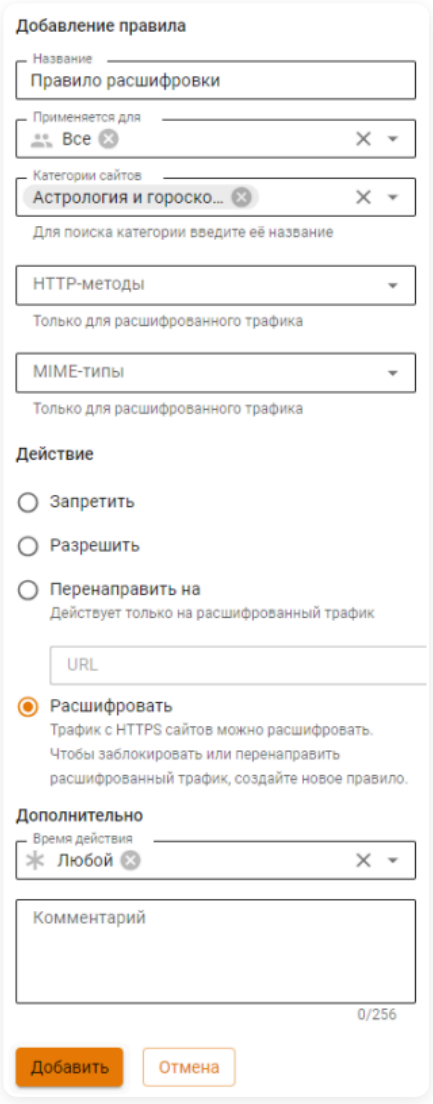
Настройка сервера и рабочих станций

Для работы SSL-bump требуется **настройка на обеих сторонах подключения**: сервера Ideco NGFW и рабочей станции каждого пользователя в локальной сети.

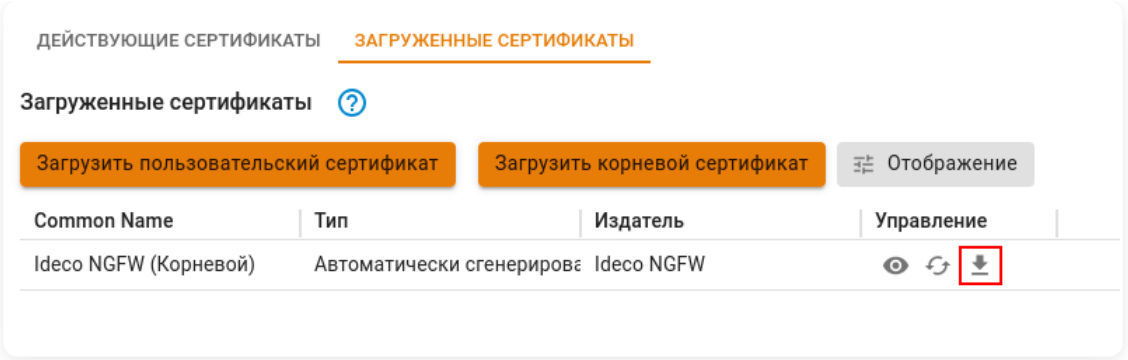
Настройка сервера Ideco NGFW

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 на вкладке **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 в операционной системе.

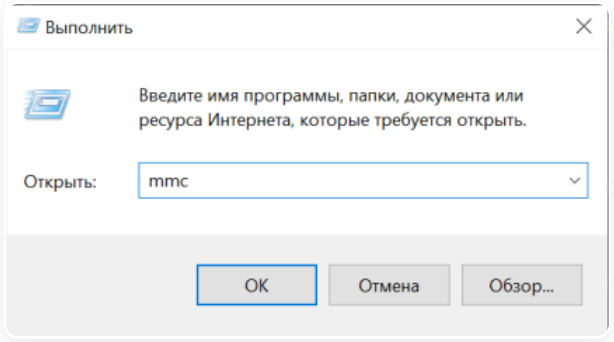
Установка сертификата на Linux

Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

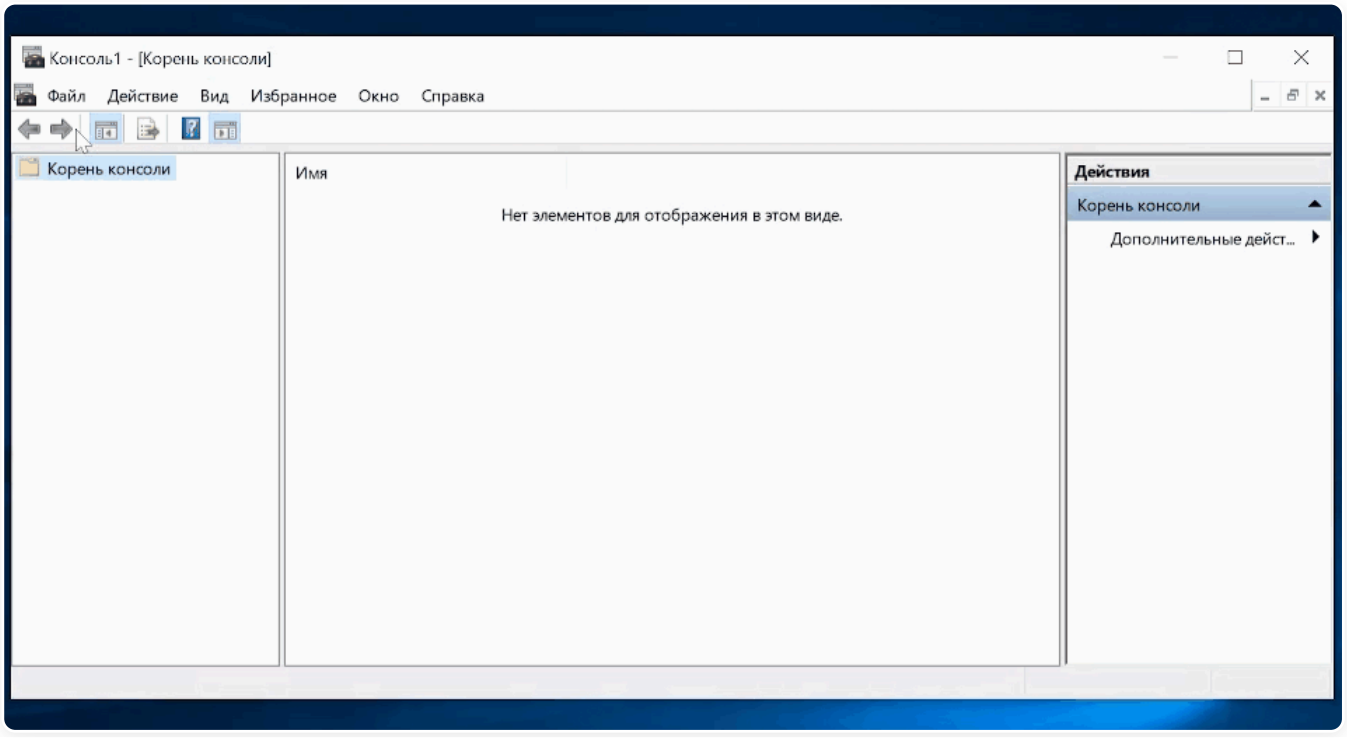
- Установка корневого сертификата на Astra Linux
- Установка корневого сертификата на Alt Linux
- Установка корневого сертификата на Red OS
- Установка корневого сертификата на Ubuntu/Debian

Установка сертификата на Windows

1. Откройте на рабочей станции центр управления сертификатами: **Пуск** → **Выполнить**, выполнив в диалоге команду **mmc**:

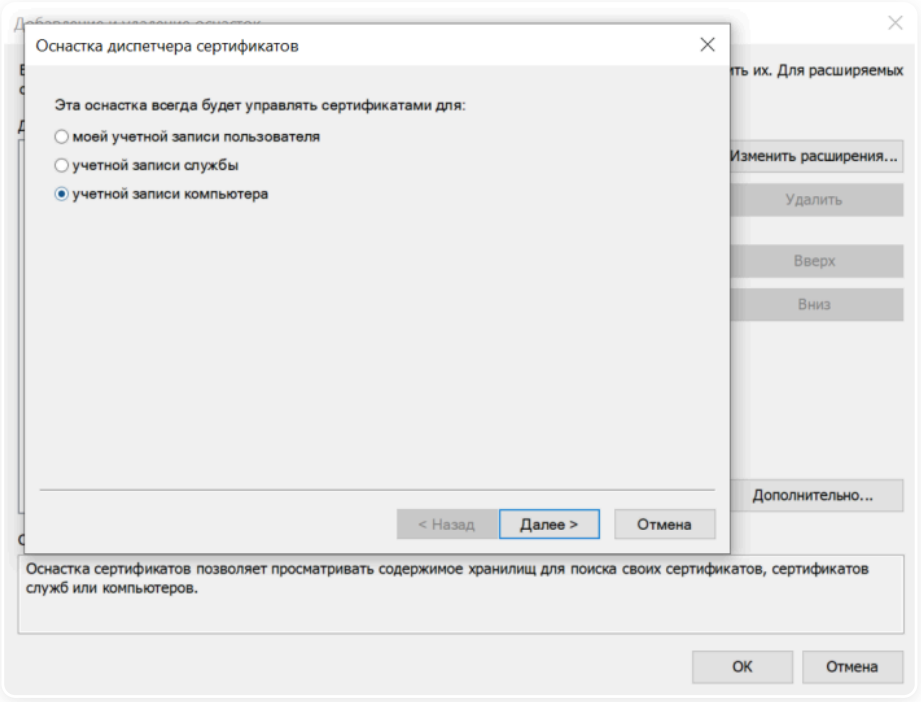


2. В меню **Файл** выберите **Добавить или удалить оснастку**:



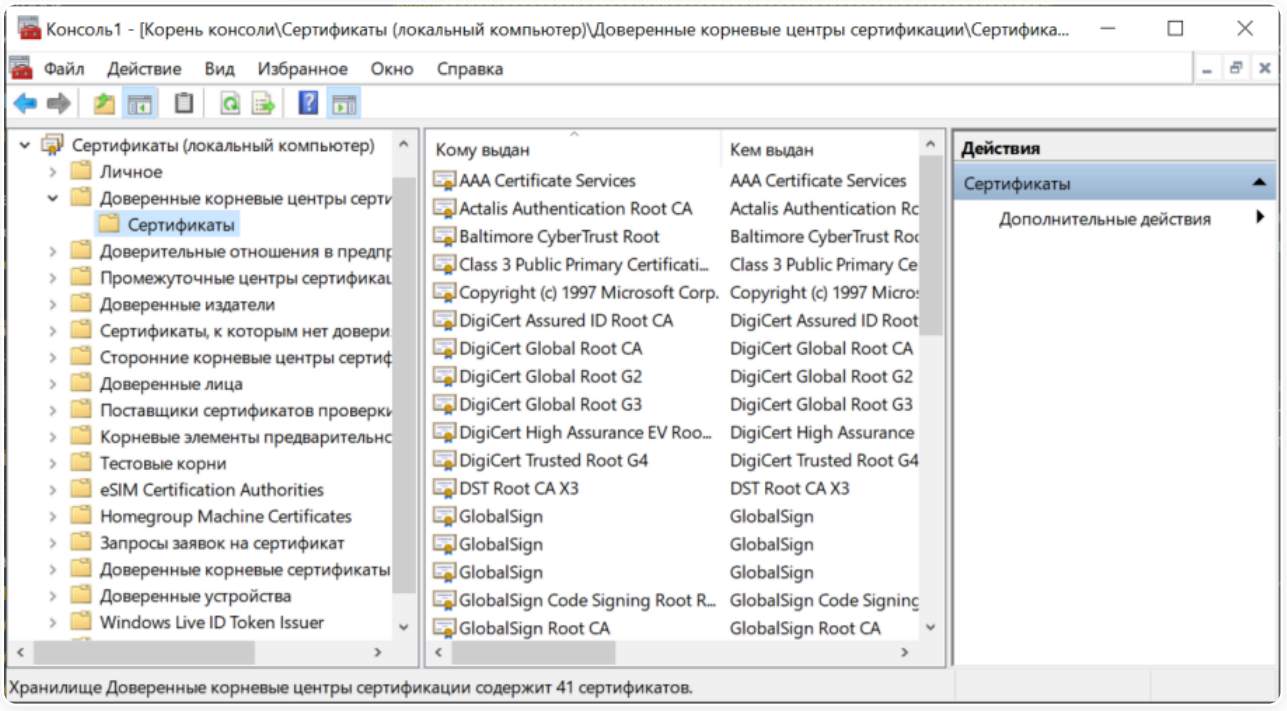
3. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите кнопку **Добавить**:

4. В открывшемся окне выберите пункт **Учетная запись 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. 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 для всех пользователей автоматически с помощью Active Directory. Для этого необходимо выполнить действия:

1. Скачайте корневой SSL-сертификат, открыв раздел веб-интерфейса Ideco NGFW **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



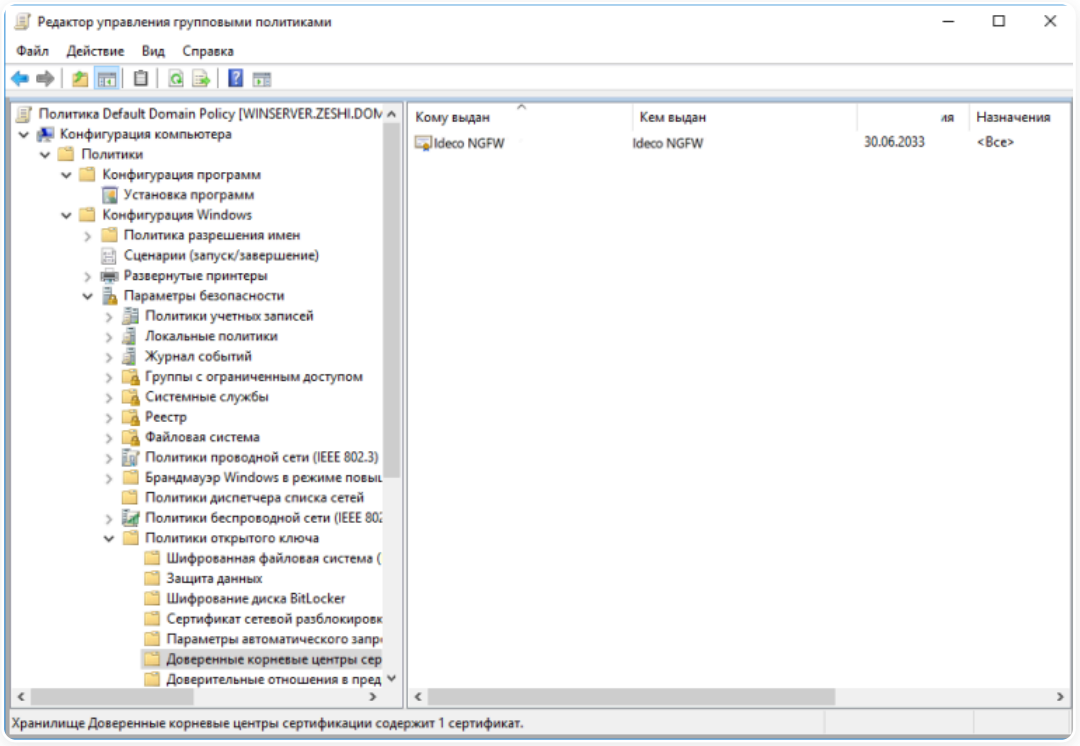
2. Зайдите на контроллер домена с правами администратора.

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.



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. На вкладке **Сервисы** → **Сертификаты** → **Загруженные сертификаты** загрузите сертификат, который будет использоваться для шифрования.

2. Перейдите на вкладку **Правила трафика** → **Контент-фильтр** → **Настройки**.

3. Выберите в пункте **Повторное шифрование** 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

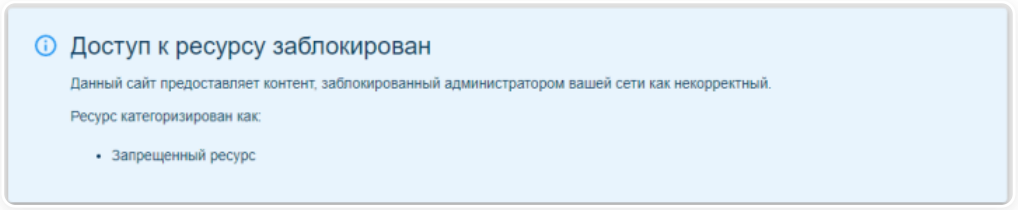
Проблема	Решение
Включения расшифровки трафика может быть недостаточно для подмены сертификата некоторых сайтов (например, `ya.ru`, `google.com`).	Включить опцию **Блокировать протоколы QUIC и HTTP/3** на вкладке **Правила трафика** → **Контент-фильтр** → **Настройки**.
Браузер не использует системное хранилище сертификатов.	1. Добавить сертификат Ideco NGFW 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 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 (даже при включенной только SNI-фильтрации), так как при блокировке HTTPS-ресурса будет применен SSL-bumping с подстановкой SSL-сертификата NGFW для подмены контента ресурса страницей о его 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**

Изменение страницы блокировки Контент-фильтра

Страница блокировки Контент-фильтра по умолчанию содержит уведомление о блокировке доступа к ресурсу и категоризацию:



В процессе обновления Ideco NGFW все ранее настроенные параметры шаблона блокировки могут быть сброшены.

Все внесенные изменения в шаблоны рекомендуется сохранить вне NGFW, чтобы избежать их потери при обновлении. После обновления может потребоваться адаптация шаблонов под новую версию системы.

Для создания персонализированного шаблона страницы выполните действия:

1. Чтобы изменить фавикон, загрузите новый файл в директорию **/usr/share/ideco/vendor/**. Для этого перейдите в раздел **Управление сервером → Администраторы** и убедитесь, что доступ по SSH разрешен. Затем откройте терминал на компьютере и введите следующую 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 компьютере.
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW.
- Файл обязательно должен называться **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 компьютере.
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW.
- Файлы обязательно должны называться **IDECO_ICON_ERROR.svg, IDECO_ICON_INFO.svg, IDECO_ICON_SUCCESS.svg, IDECO_ICON_WARNING.svg**.

3. Отредактируйте CSS-файл, чтобы изменить стили для страниц ошибок. Перейдите в **Управление сервером -> Терминал** и откройте файл **style.css** из директории **/usr/share/ideco/proxy-backend/error_page_templates/** 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 страницу блокировки. Перейдите в директорию **/usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU/error_content/** и откройте файл **ERR_CF_BLOCK_PAGE** в текстовом редакторе:

```
nano /usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU/error_content/ERR_CF_BLOCK_PAGE
```

Пример изменения файла ERR_CF_BLOCK_PAGE

```
<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://telegram.im/@admin">Отправить заявку в Telegram</a></p>
    </div>
  </div>
  <div class="blocked_content">
    <h1>Контент заблокирован</h1>
  </div>
</body>
```

Результат:

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

Название службы раздела *Ограничение скорости*: `ideco-shaper-backend`.

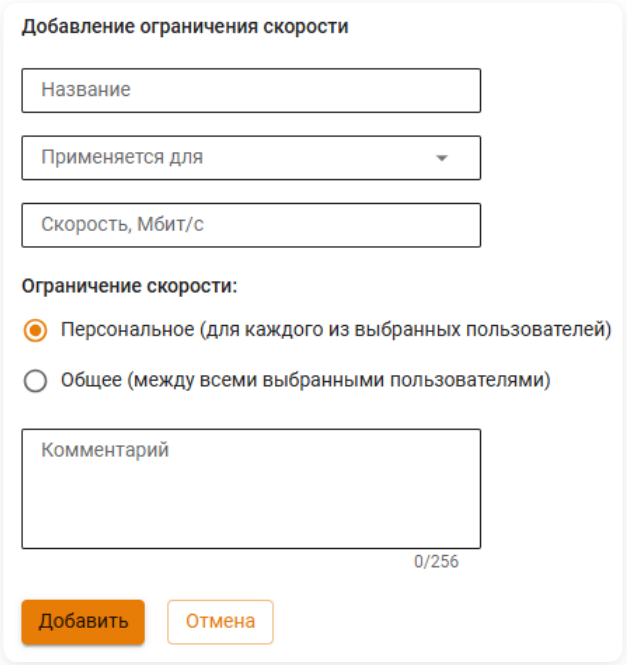
Список имен служб для других разделов, доступен по ссылке.

В разделе **Ограничение скорости** создаются правила, позволяющие ограничить скорость входящего интернет-трафика для пользователей сети.

Для исключения пользователя или групп пользователей из обработки правил **Ограничения скорости** добавьте соответствующее правило в разделе Исключения.

Настройка ограничения скорости

1. Для создания правила в разделе **Правила трафика** → **Ограничение скорости** нажмите **Добавить** и заполните поля:

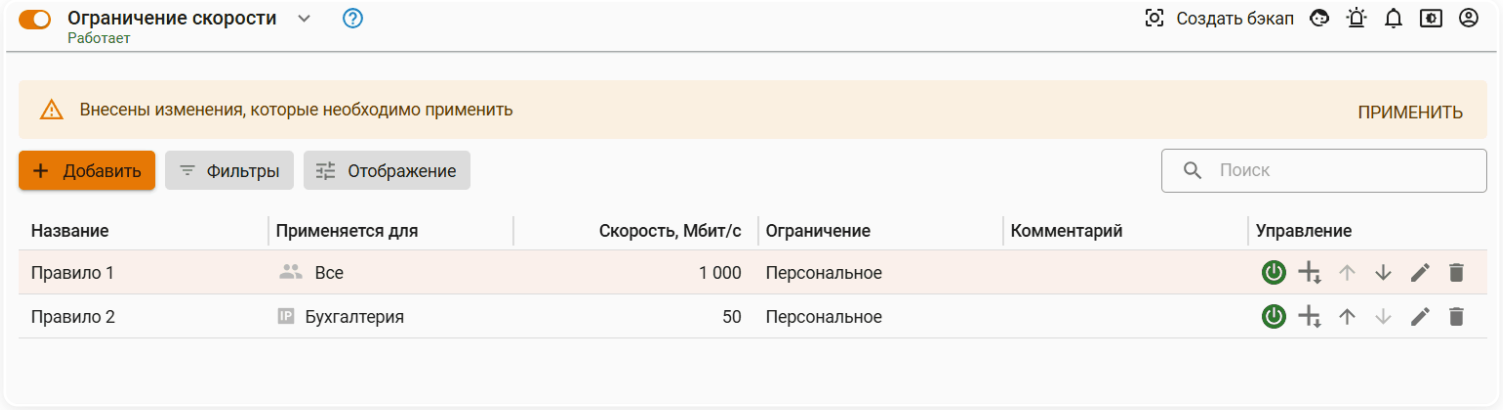


Расшифровка полей

- **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.
  - **Общее** - скорость будет ограничена и разделится между всеми выбранными пользователями.

2. Нажмите **Добавить**.

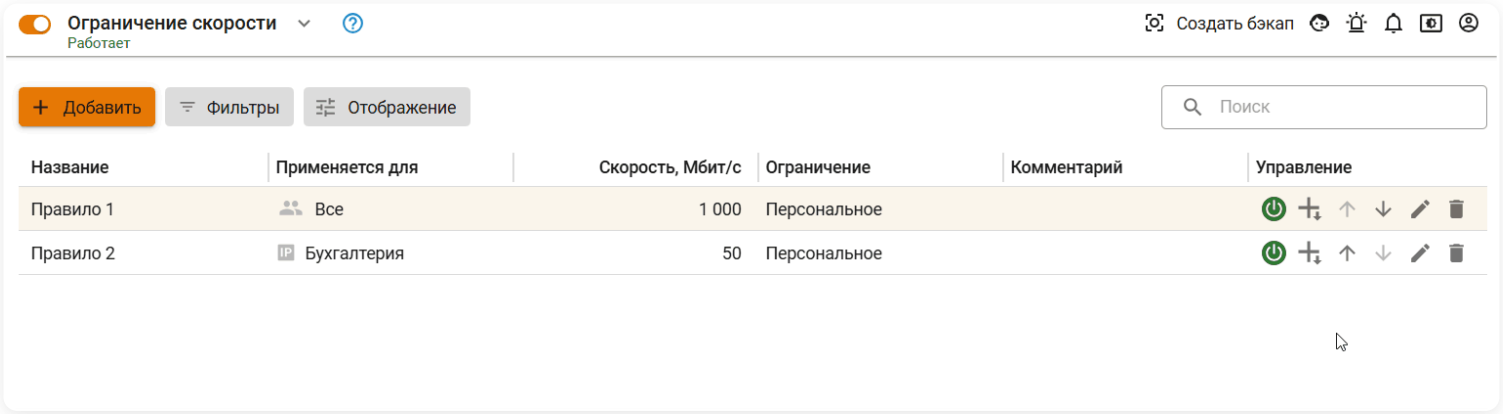
3. Для применения созданного правила нажмите **Применить** над таблицей:



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.

Включить или выключить правило, изменить его приоритет, редактировать или удалить можно кнопками управления в столбце **Управление**:



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.

Примеры использования

Персональное ограничение

При выборе персонального ограничения скорости лимит скорости для каждого менеджера будет равен 1 Мбит/с:

Общее ограничение

При выборе общего ограничения ширина канала для всей бухгалтерии будет равна 10 Мбит/с:

Полезные ссылки

- Исключения
- Объекты
- Учетные записи

Антивирус

Название службы раздела **Антивирус**: `ideco-av-backend`.

Список имен служб для других разделов доступен по ссылке.

Антивирус в продукте создан на базе Kaspersky Anti-Virus Software Development Kit. Антивирус приобретается отдельно от Ideco NGFW, использование может быть ограничено условиями лицензии. Для покупки обратитесь в отдел продаж.

Корпоративные ключи, предназначенные для других продуктов Лаборатории Касперского, не могут быть использованы для активации антивируса.

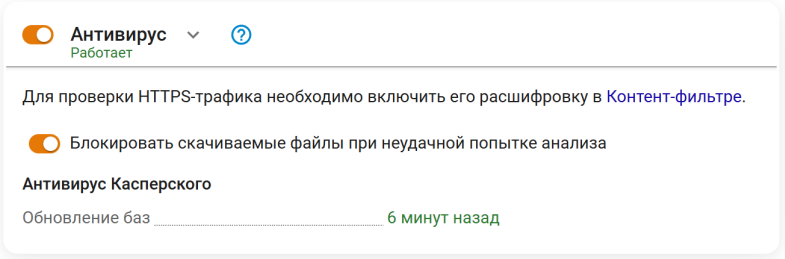
Модуль **Антивирус** связан с прокси-сервером и **Контент-фильтром**, поэтому фильтрует веб-трафик при выполнении следующих условий:

- **Включена расшифровка трафика.** В разделе **Контент-фильтр** настроена расшифровка веб-трафика. HTTPS-сайт проверяется только в случае расшифровки HTTPS-трафика **Контент-фильтром**.
- **Отсутствуют исключения в прокси-сервере.** Веб-ресурс не должен находиться в списках исключений прокси-сервера по назначению, а пользователь - в списках исключений по источнику. Трафик, попадающий в эти исключения, не направляется на антивирусную проверку.

Настройка

Для работы **Антивируса** выполните действия:

1. Перейдите в **Правила трафика** → **Антивирус** и включите модуль:

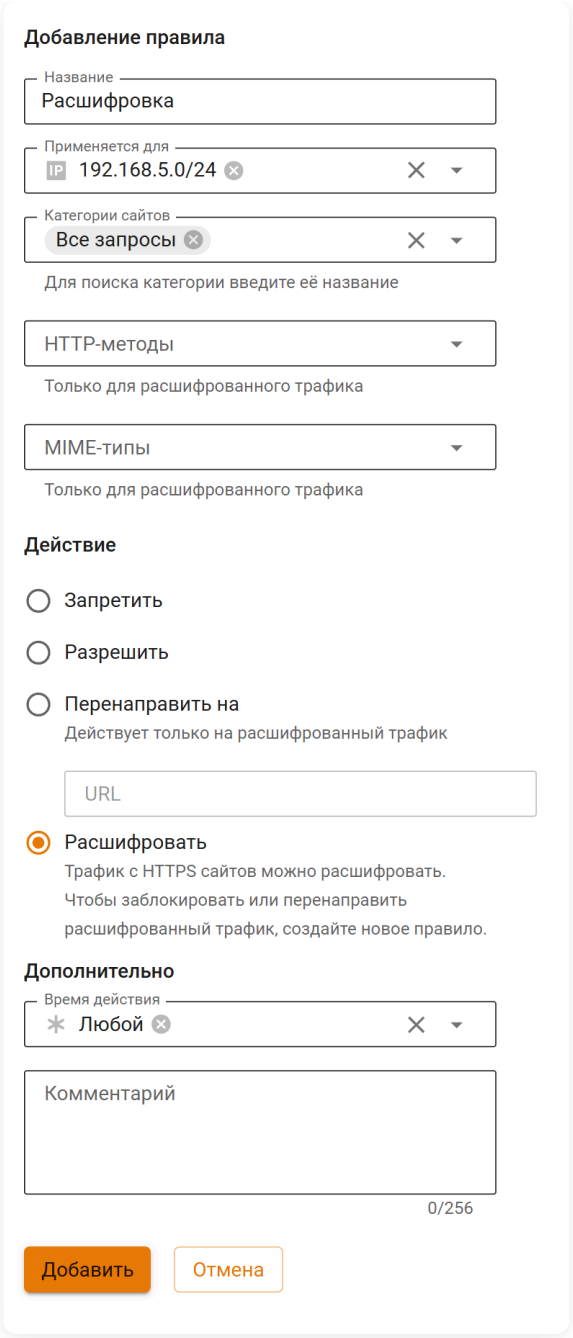


При необходимости включите опцию **Блокировать скачиваемые файлы при неудачной попытке анализа** для блокировки скачиваемых файлов, если не удается провести анализ файла.

2. Перейдите в **Правила трафика** → **Контент-фильтр** → **Правила** и создайте правило расшифровки HTTPS-трафика. Настройка расшифровки представлена в статье.

Пример правила расшифровки

Необходимо проверять антивирусом весь веб-трафик пользователей подсети `192.168.5.0/24`. Для этого создано правило **Контент-фильтра** с действием **Расшифровать**:



Правило применяется к сети `192.168.5.0/24` (поле **Применяется для**) и категории **Все запросы** (поле **Категории сайтов**) для проверки всех сайтов.

3. Если нужно отключить проверку для определенного HTTPS-трафика, перейдите в **Сервисы** → **Прокси** → **Исключения** и добавьте исключения:

- Сеть веб-ресурса - в списки по назначению.
- Сеть пользователя - в списки по источнику.

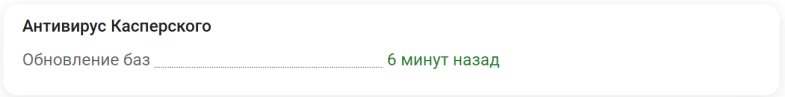
> Добавленные сети исключаются из обработки модулями **Прокси**, **Контент-фильтр** и не попадают в **Веб-трафик**.

Настройки антивирусной фильтрации не требуют ручного конфигурирования и при необходимости оптимизируются в обновлениях версий Ideco NGFW.

Результат проверки трафика антивирусом представлен в Журнале веб-трафика.

Обновление баз

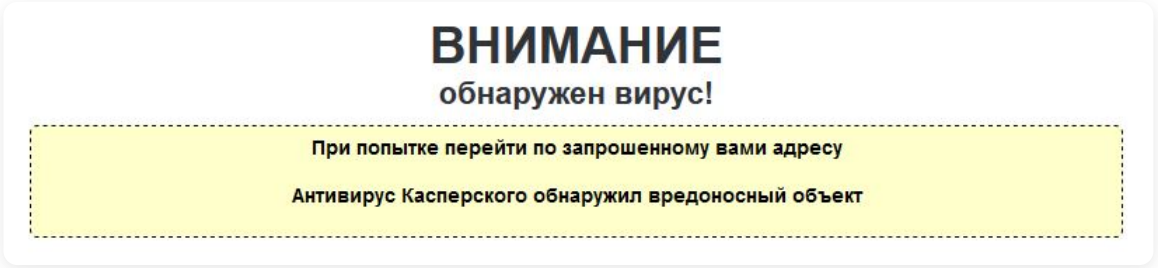
В разделе **Антивирус** можно посмотреть информацию о последнем обновлении баз антивируса Касперского:



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:



Предотвращение вторжений

Название службы раздела **Предотвращение вторжений**: `ideco-suricata-backend`; `ideco-suricata`; `ideco-suricata-event-syncer`; `ideco-suricata-profiles-syncer`.

Список имен служб для других разделов доступен по ссылке.

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Система **Предотвращения вторжений** (IDS/IPS, Intrusion detection system / Intrusion prevention system) предназначена для:

- ☑ Обнаружения
- ☑ Журналирования
- ☑ 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 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 Файрвола и системы Предотвращение вторжений

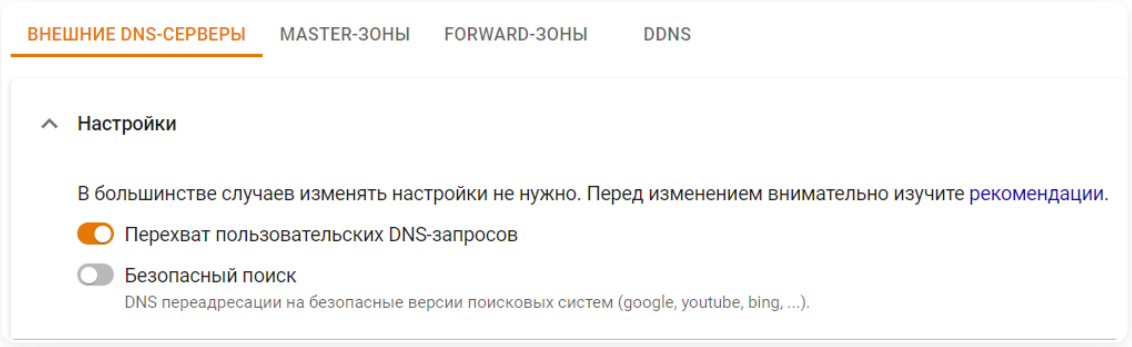
- **Файрвол** Ideco NGFW анализирует трафик для поиска подходящего правила и применяет его. Если в таблице есть несколько правил с одними и теми же условиями, применяется правило, стоящее выше по списку. Запрещающие правила **Файрвола** сразу блокируют соответствующий трафик, он не проходит дополнительную 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 **Файрволе** правило с источником **Любой** и назначением **Любой**, разместив его в конец таблицы. В этом случае трафик, который не был найден в правилах **Файрвола**, но соответствует профилям IPS, пройдет проверку системой **Предотвращения вторжений**.
- Если в одном правиле **Файрвола** 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 механизм работы системы **Предотвращения вторжений** изменился, появились возможности:

- ☑ Работать с правилами IPS на уровне сигнатур, фильтровать их и просматривать в удобном виде
- ☑ Составлять независимые друг от друга наборы правил IPS и применять их только к необходимому трафику с помощью профилей системы **Предотвращения вторжений**, которые назначаются в правилах **Файрвола**

Особенности обработки DNS-запросов

При включенной опции **Перехват пользовательских DNS-запросов** в разделе **Сервисы** → **Защита и управление DNS** → **Внешние DNS-серверы** трафик обрабатывается не как **FORWARD**, а как **INPUT**:

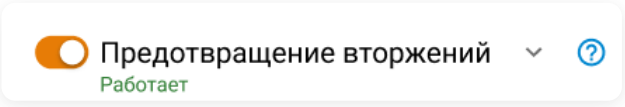


Если опция **Перехват пользовательских DNS-запросов** включена (по умолчанию включена), создайте правила **INPUT** для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

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 разделе **Профили безопасности** → **Предотвращение вторжений**.

3. Примените их в правилах Файрвола.

В обработку трафика не попадают:

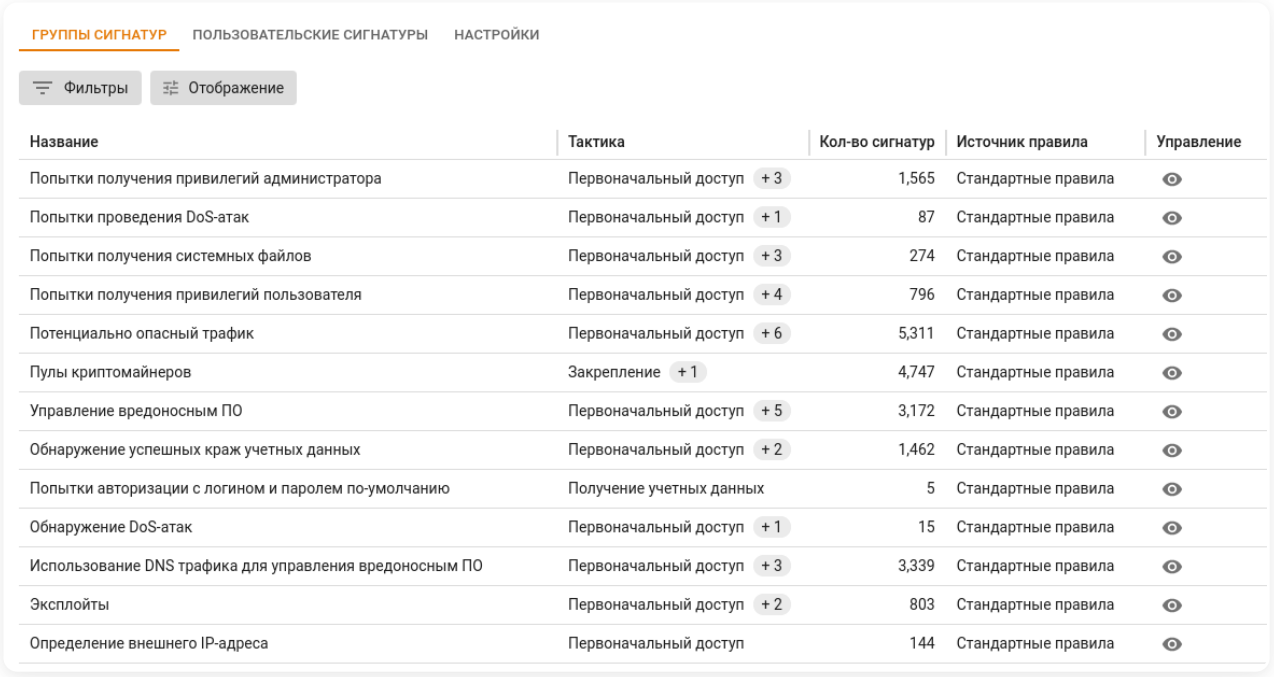
- Сигнатуры, не включенные ни в один профиль.
- Профили, не используемые в правилах **Файрвола**.

Полезные ссылки

Подробнее о Load Average

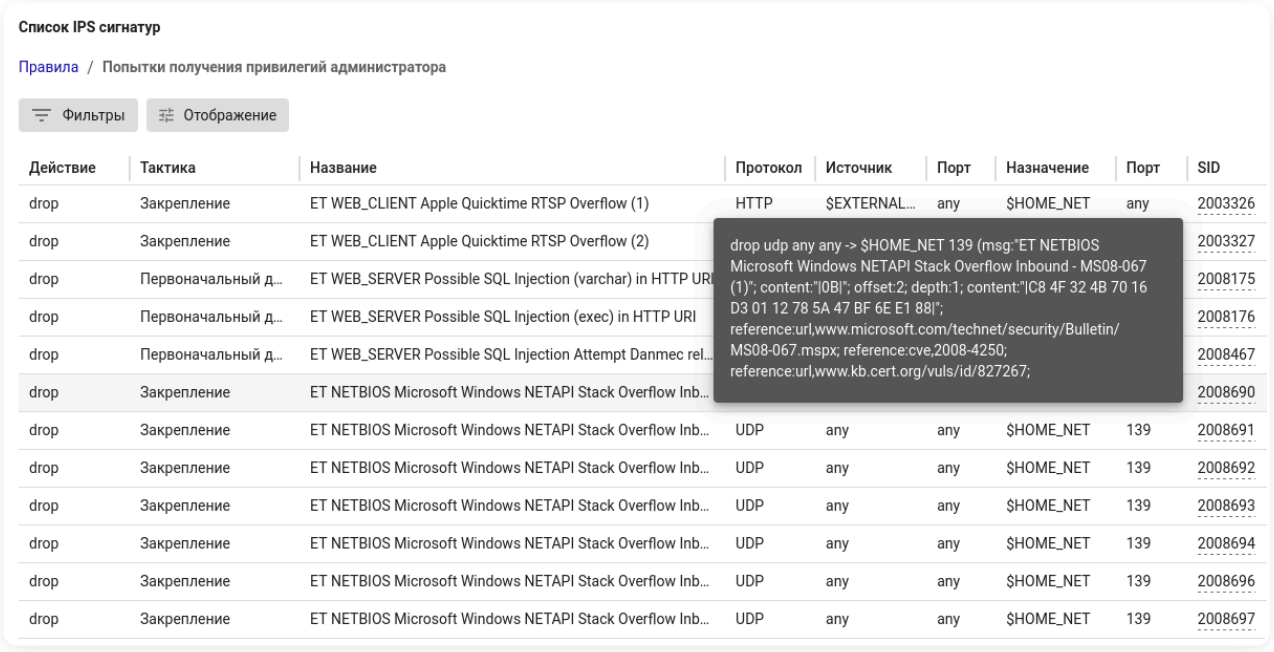
Группы сигнатур

На вкладке **Группы сигнатур** доступны для просмотра пользовательские и предустановленные сигнатуры:



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:



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

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.
- **GeoIP Страны Восточной Европы** - обнаруживает попытки доступа к IP-адресам, соответствующим различным странам. Система анализирует исходящий и входящий трафик и определяет подключения, соответствующие геолокационным критериям, которые могут свидетельствовать о потенциальных угрозах. Такой механизм фильтрации помогает блокировать несанкционированный доступ, атаки и прочую активность.

- **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. Они 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.
- **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-хэшей, 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.
- **Черный список IP-адресов** - обнаруживает трафик, направленный к IP-адресам, внесенным в черный список различных баз (НКЦКИ, открытые источники и тд). Система анализирует входящий и исходящий трафик, сравнивая адреса с известными источниками угроз и вредоносных операций. При обнаружении совпадений соединения блокируются, что предотвращает доступ к ресурсам, участвующим в фишинге, ботнет-активности, спаме и других киберугрозах, тем самым повышая общий уровень сетевой безопасности.
- **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

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 **Файрвола**.

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; htt
```

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, его 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 их необходимо указать. 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 их использования в значениях опций.

Создание пользовательской сигнатуры

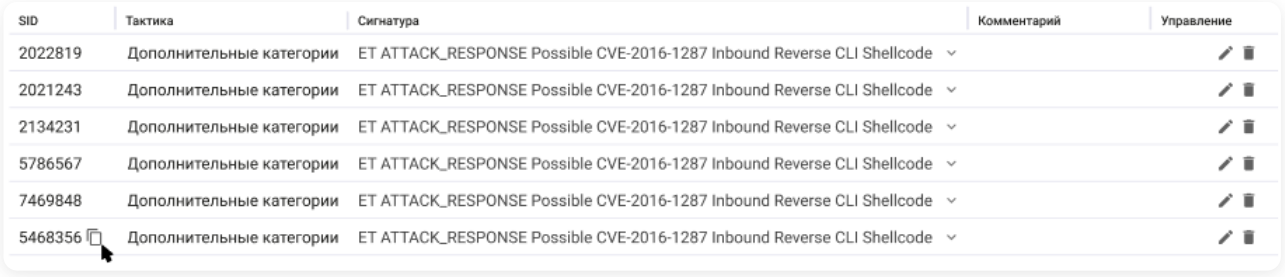
Нажмите **Добавить** и выберите способ добавления:

Вручную

В открывшейся форме введите комментарий, сигнатуру 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 раздел **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 раздел **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.st
```

Пример пользовательской сигнатуры:

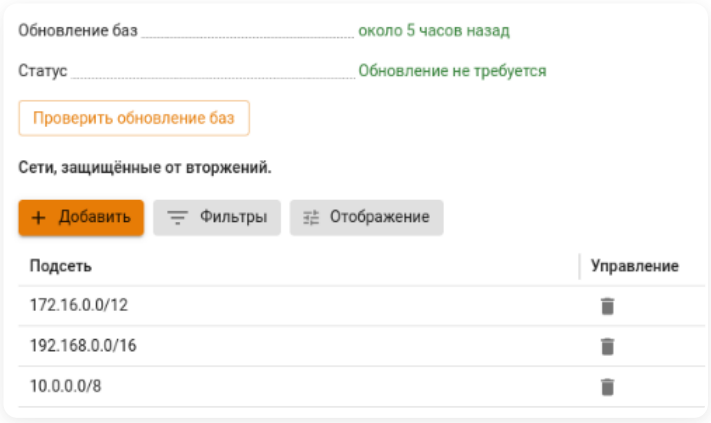
```
pass http 192.168.10.10 any -> 1.1.1.1 any (flow:established,to_client; http.stat_code; content:"200"; http.server; content:"
```

Полезные ссылки

Полная документация по форматам сигнатур.

Настройки

На вкладке можно проверить статус обновления баз системы **Предотвращение вторжений** и отредактировать список сетей, защищенных от вторжений:



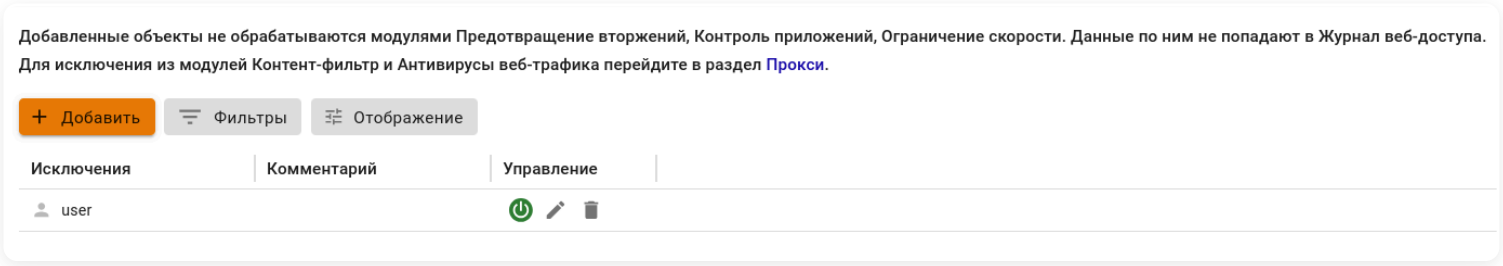
Для добавления подсети в список защищенных нажмите **Добавить** и в поле **Подсеть** укажите локальные сети, обслуживаемые NGFW (сети локальных интерфейсов NGFW, маршрутизируемые на них сети удаленных сегментов локальной сети предприятия).

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 в качестве единственного DNS-сервера.
  - В настройках DNS-сервера на NGFW указать Forward-зону для локального домена.

Исключения

Правила в разделе **Исключения** отключают трафик из обработки системы Предотвращения вторжений, Контроля приложений, данные по ним не попадают в монитор трафика:



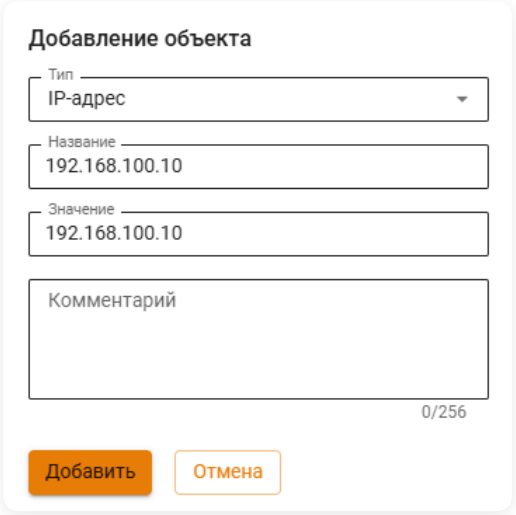
При наличии большого количества исключений в таблице воспользуйтесь кнопкой **Фильтры**.

Добавление исключения

Для предотвращения обработки трафика необходимо добавить объект в исключения:

1. Перейдите в раздел **Правила трафика** → **Исключения** и нажмите **Добавить**.

2. Выберите существующий объект или создайте новый, указав его тип, название и значение объекта. По желанию можно указать произвольный комментарий:



3. Нажмите **Добавить**.

Если в качестве DNS-сервера у пользователя указан локальный адрес сервера Ideco NGFW, то исключения работать не будут. Весь трафик, идущий на адреса локальных и VPN-интерфейсов Ideco NGFW, всегда обрабатывается службой фильтрации трафика.

Особенность работы исключений по домену

1. При добавлении исключения по домену NGFW выполняет DNS-резолв указанного домена.

2. Полученные в результате резолва IP-адреса добавляются в список IP-адресов, используемый правилами фильтрации.

3. Клиент при обращении к ресурсу выполняет собственный DNS-резолв домена.

4. В зависимости от региона, балансировки нагрузки или времени клиент может получить другие IP-адреса того же домена.

5. Если IP-адрес, полученный клиентом, отсутствует в списке IP-адресов NGFW, исключение не применяется и трафик блокируется.

Для корректной работы исключений рекомендуем включить **Перехват пользовательских DNS-запросов** в **Сервисы** → **DNS** → **Внешние DNS-серверы**. Но даже в этом случае возможны кратковременные блокировки из-за DNS-кэша и задержек обновления списка IP-адресов,

используемого правилами фильтрации (ipset).

Объекты

Название службы раздела *Объекты*: `ideco-alias-backend`.

Список имен служб для других разделов доступен по ссылке.

Типы объектов

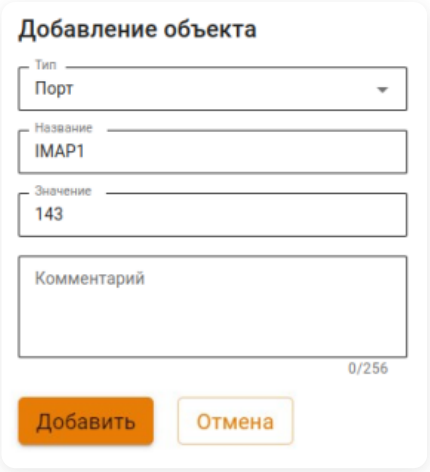
- **Зона** - логическое объединение сетевых интерфейсов. Используется для настройки правила файрвола на несколько интерфейсов.
- **IP-адрес** - IP-адрес IPv4. Пример: 10.0.0.1.
- **Диапазон IP-адресов** - диапазон IP-адресов от первого до последнего, указанного в диапазоне. Пример: 10.0.0.1-10.0.0.25.
- **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 и домен. Пример: 10.0.0.1, 10.0.0.4, 10.0.0.126.
- **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** - группа объектов, содержащая GeoIP.

Создание объектов

Чтобы создать объект, необходимо выполнить следующие действия:

1. Перейдите в раздел **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 файрвола, введя нужный IP-адрес или порт в соответствующих полях.



В Ideco NGFW также используется специальный алиас - **Любой**. Если при создании правила в каком-либо из полей выбран этот алиас, правило будет распространяться на все объекты, доступные к выбору в том же поле.

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 Файрвол.

Web Application Firewall

Создание WAF-профилей для защиты опубликованных веб-ресурсов от атак

Перейти >

Контроль приложений

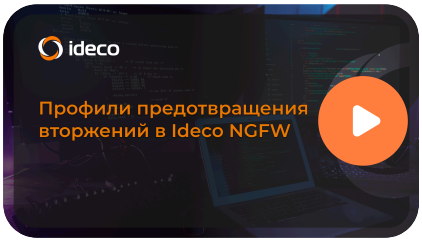
Создание, настройка и примеры использования профилей **Контроля приложений**

Перейти >

Предотвращение вторжений

Создание, настройка и примеры использования профилей **Предотвращение вторжений**

Перейти >



Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Web Application Firewall

Название служб раздела **Web Application Firewall**: `ideco-waf-backend`; `ideco-waf-event-syncer`.

Список служб для других разделов доступен по ссылке.

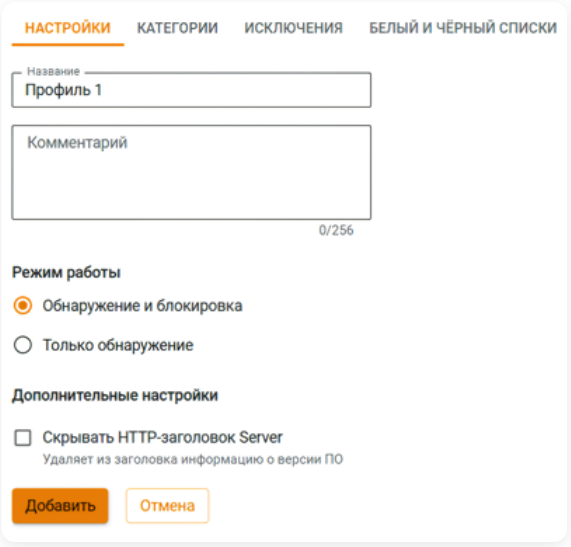
Использование WAF-профилей позволит настроить параметры защиты для опубликованного веб-ресурса. Профиль создается в разделе **Профили безопасности → Web Application Firewall**. Подробные описания сигнатур можно найти в документации ModSecurity.

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:

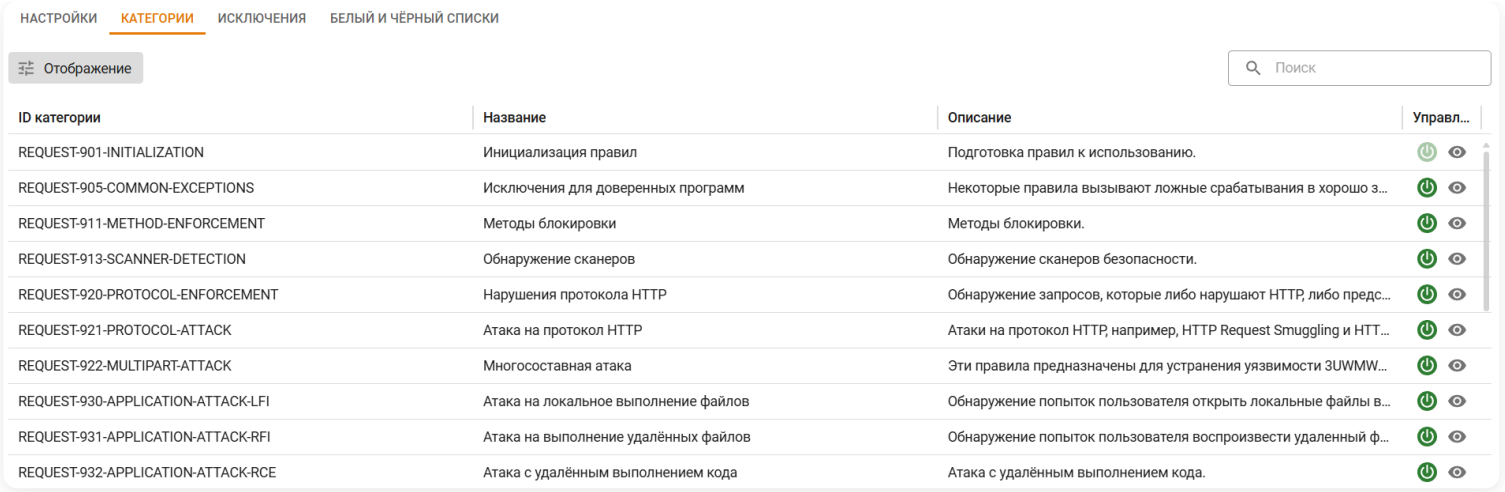


Расшифровка полей

- **Название** - введите название профиля.
- **Комментарий** - введите пояснение для профиля.
- **Режим работы**:
  - **Обнаружение и блокировка** - подозрительные запросы будут блокироваться и логироваться WAF.
  - **Только обнаружение** - подозрительные запросы будут логироваться WAF, но не будут блокироваться.
- **Дополнительные настройки**:
  - **Скрывать HTTP-заголовок Server** - позволяет скрыть данные, идентифицирующие сервер.

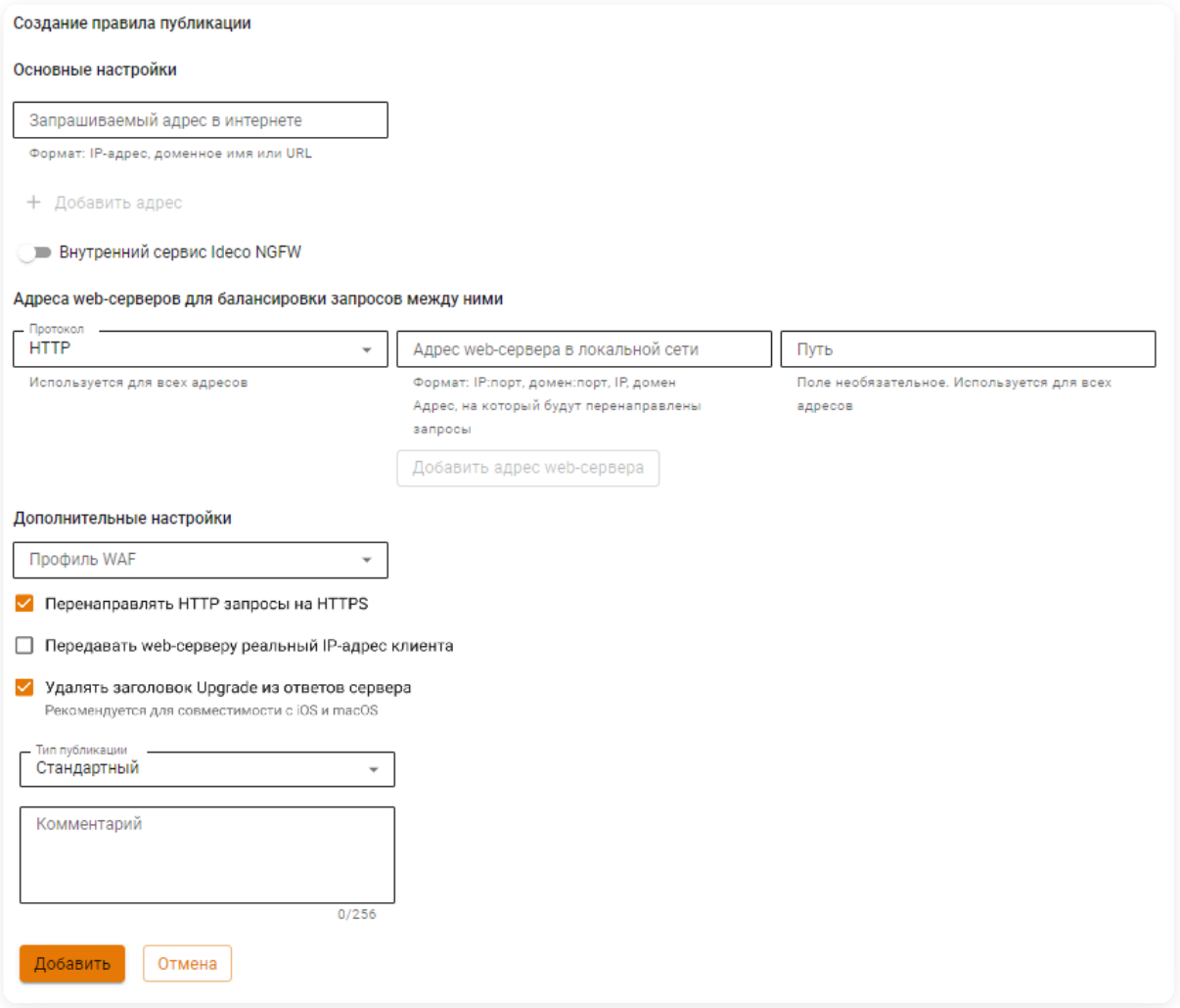
2. Нажмите **Добавить**.

3. На вкладке **Категории** включите или отключите правила:



Использование профиля WAF в правиле Обратного прокси

1. Перейдите в раздел **Сервисы** → **Обратный прокси**, нажмите **Добавить** и заполните поля:



Расшифровка полей

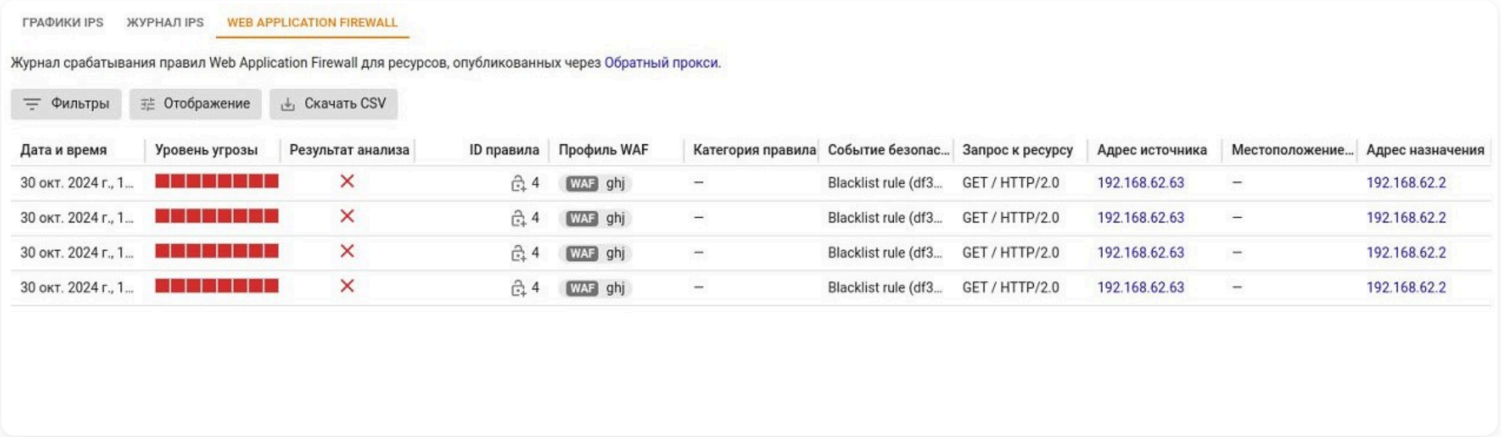
- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных адресов нажмите кнопку **Добавить адрес**.
- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Адрес web-сервера в локальной сети** - 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.

2. Нажмите **Добавить**.

Диагностика и добавление исключений

Срабатывание правил **Web Application Firewall** отображается на вкладке **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**:



Добавить правило в исключение можно двумя способами:

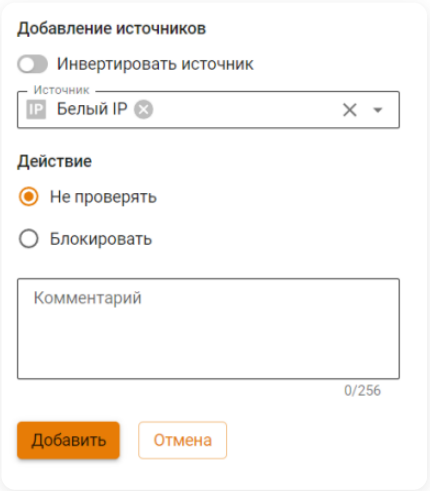
По IP-адресу

1. Перейдите в раздел **Web Application Firewall** и у правила нажмите на  .

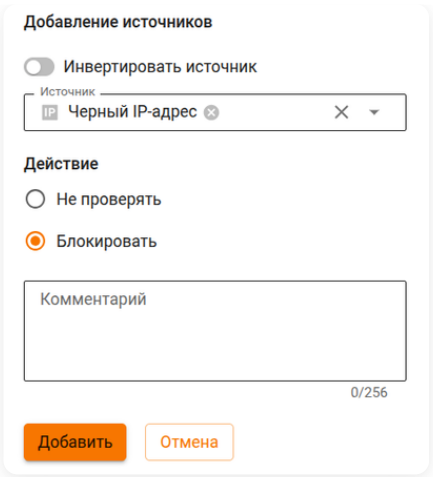
2. На вкладке **Белый и черный списки** нажмите **Добавить источник**:

> 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 на вкладке **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 **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 на вкладке **Отчеты и журналы** → **События безопасности** → **Web Application Firewall**.

На вкладке Web Application Firewall

1. Перейдите на вкладку **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.

Чтобы пользовательские правила WAF сохранялись при обновлении, в Ideco NGFW предусмотрен специальный файл (after-секция) для пользовательских правил и исключений. Он позволяет встроиться в процесс обработки запроса для добавления пользовательских проверок или изменения поведения системы после отработки стандартных правил.

Для внесения правил в after-секцию:

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"
```

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`.

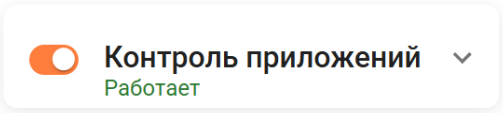
Контроль приложений

Названия служб раздела **Контроль приложений**: `ideco-app-backend` и `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 **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:

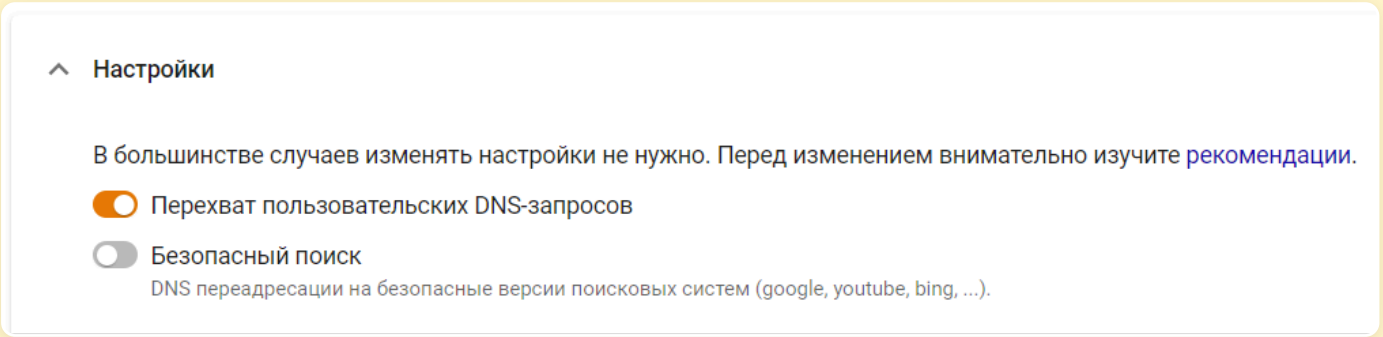
- В правиле **FORWARD** или **INPUT** раздела **Межсетевой экран** включена опция **Контроль приложений**.
- В этом правиле выбран профиль безопасности.

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 **Контролем 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** → **Защита и управление 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**.

При наличии большого количества профилей в таблице воспользуйтесь кнопкой **Фильтры**.

Особенности обработки трафика с помощью профиля Контроля приложений

Контроль приложений проверяет только тот трафик, который соответствует разрешающему правилу **Файрвола** с включенной опцией **Контроля приложений** и выбранным профилем.

Порядок применения правил Файрвола

- **Файрвол** Ideco NGFW анализирует трафик, ищет подходящее правило в таблице (сверху вниз) и применяет его.
- Если в списке несколько правил с одинаковыми условиями, применяется правило, которое выше в таблице.
- Трафик не проходит дополнительную проверку **Контролем приложений**, если заблокирован запрещающим правилом **Файрвола**.

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 Socialg 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 теле-радиовещания 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 **Файрвола**:

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 Файрвол.
2. Создайте правило Файрвола, 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

Особенности создания профилей

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.

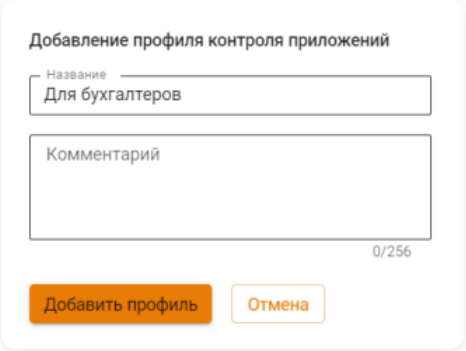
Создание профилей и добавление в правила Файрвола

Пример. Необходимо ограничить доступ к социальным сетям пользователям группы "Бухгалтерия".

Создание профиля Контроля приложений

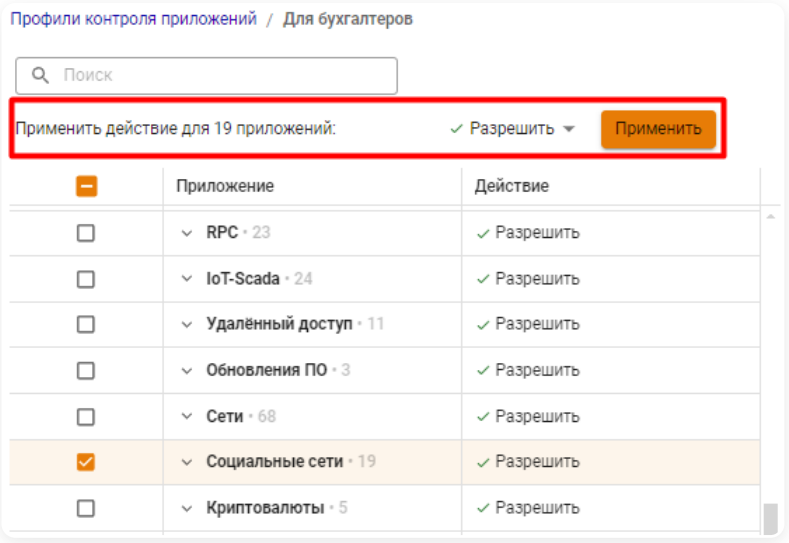
1. Перейдите в раздел **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Заполните **Название**, **Комментарий** (необязательно) и добавьте профиль:

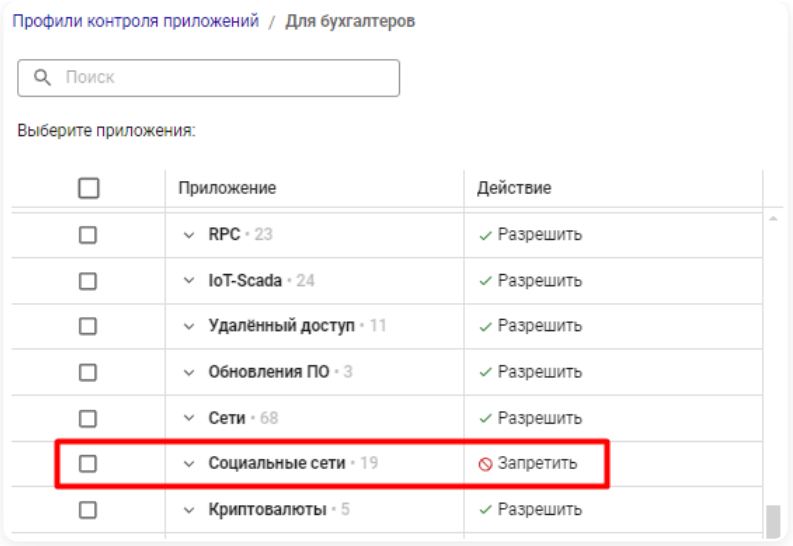


3. Нажмите в столбце **Управление** на  , затем **Доступ к приложениям**.

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:



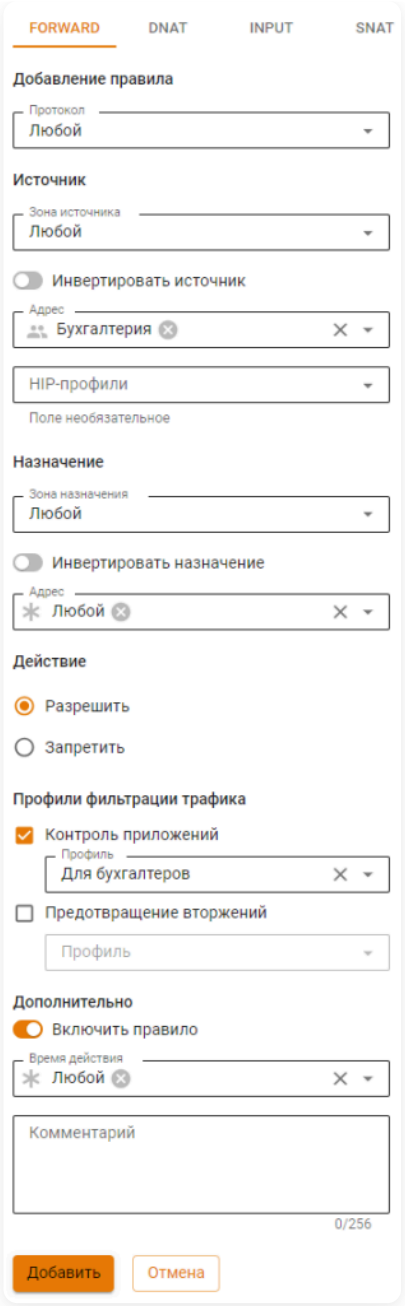
К неизвестным источникам по умолчанию применяется действие **Разрешить** (доступно для редактирования).

6. Нажмите **Сохранить**.

Добавление профиля в правила Файрвола

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать с помощью профиля **Контроля приложений**;
- **Источник** - выберите **Адрес**, **Зону** и **HIP-профиль** источника трафика;
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика;
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** и в разделе **Профили для фильтрации** из раскрывающегося списка выберите профиль, запрещающий социальные сети сотрудникам бухгалтерии.

4. Включите правило или оставьте его выключенным.

5. Нажмите **Добавить**.

6. Если в разделе **Сервисы → Защита и управление 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 он 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

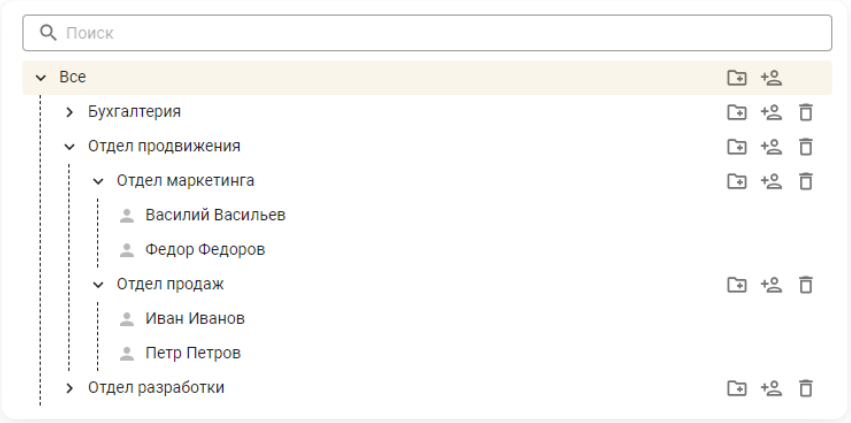
Настройка фильтрации трафика, для которого в таблице FORWARD нет правил

Пример создания иерархической структуры

Пример. 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.

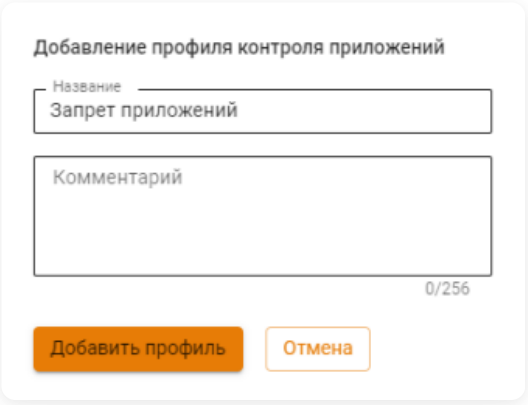
В описанном примере Федор Федоров - сотрудник Отдела маркетинга, а Отдел маркетинга - структурное подразделение Отдела продвижения:



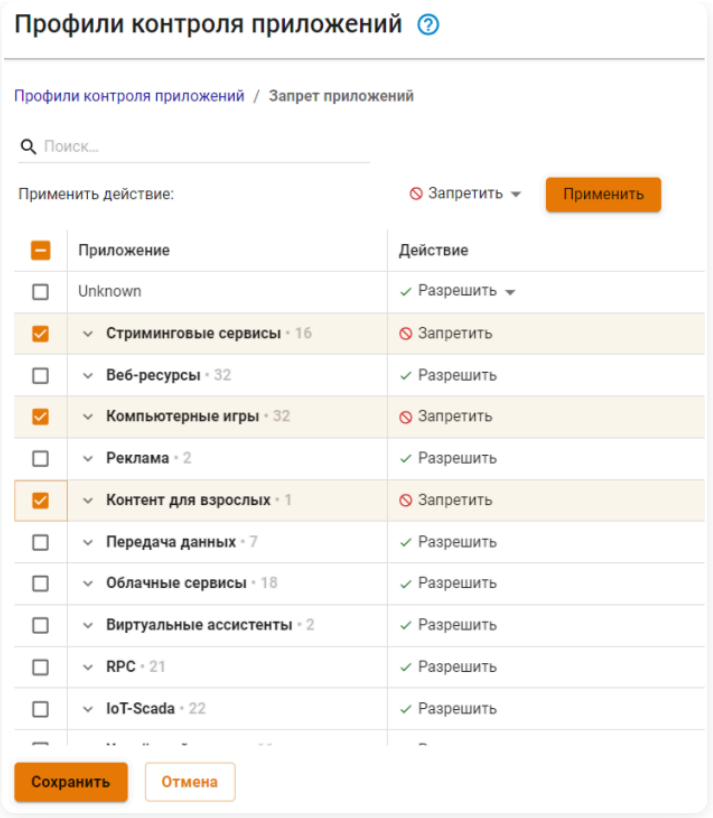
Создание профилей Контроля приложений

Создайте профили в соответствии с условиями примера:

1. Перейдите в раздел **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:



- Нажмите в столбце **Управление** на , а затем **Доступ к приложениям**;
- 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** в левом нижнем углу.

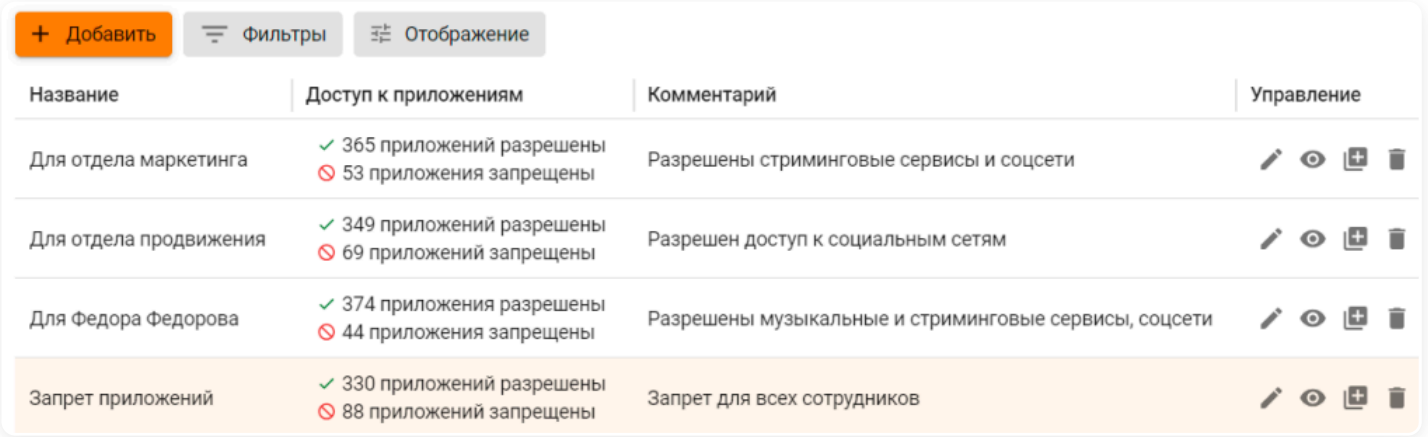
3. Создайте профиль для Отдела продвижения, разрешающий доступ к социальным сетям. Для этого:

- 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:

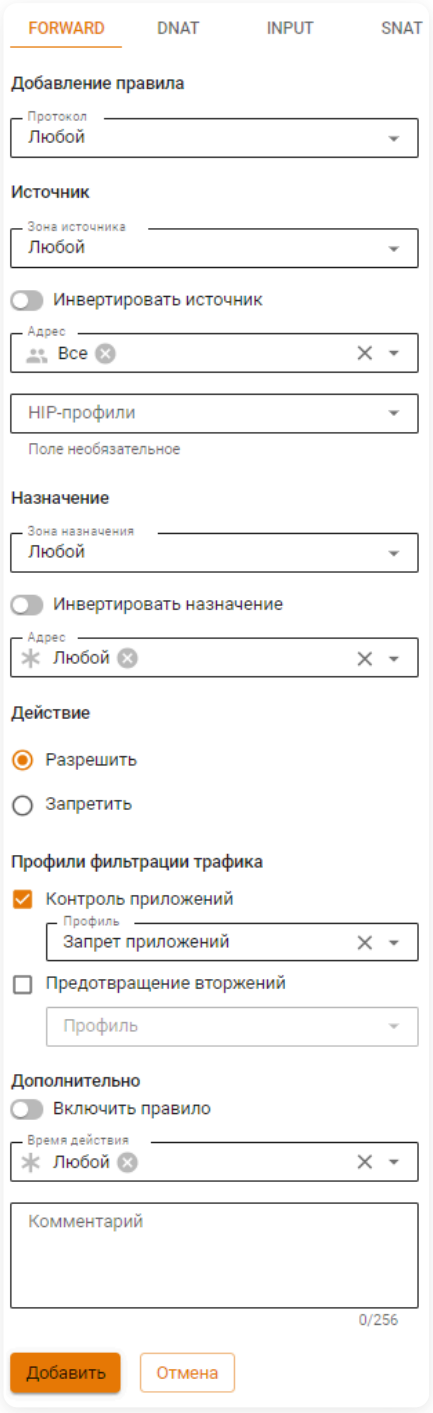


Создание правил Файрвола

Теперь необходимо создать и включить правила в **Файрволе**, чтобы применить настройки для конкретных групп пользователей и установить приоритет прохождения трафика:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

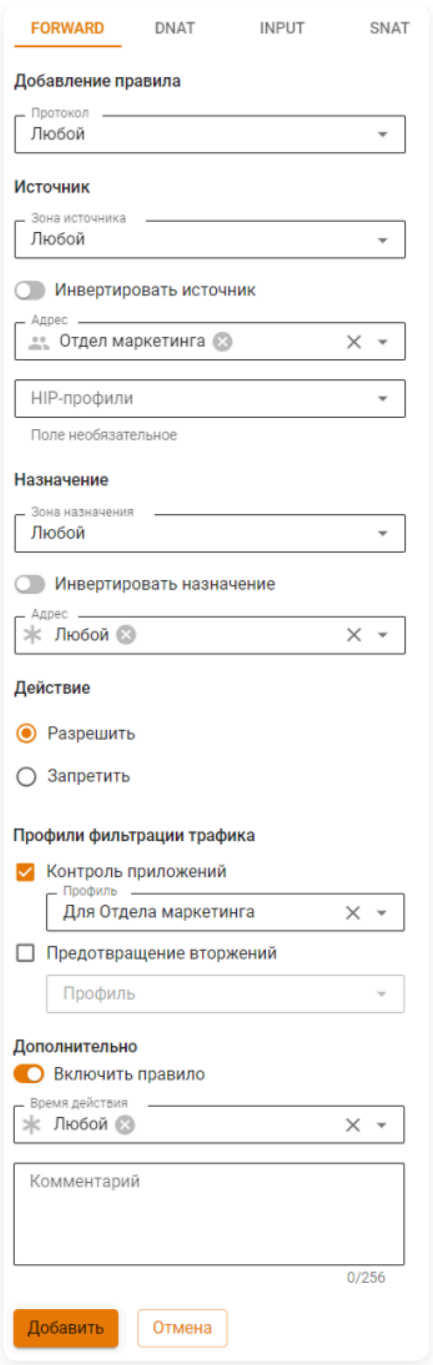
2. Заполните поля:



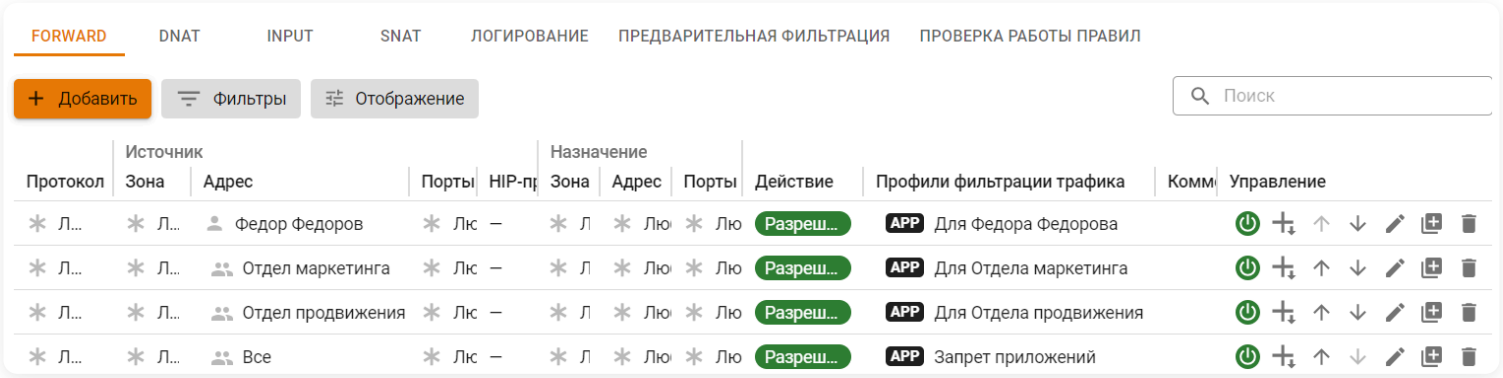
- **Адрес источника** - группа пользователей **Все**;
- **Действие** - **Разрешить**;
- **Профили безопасности** - **Контроль приложений**, профиль **Запрет приложений**;

3. Включите правило и нажмите **Добавить**.

4. Аналогично создайте правила для каждого профиля. При создании правила **Файрвола** укажите соответствующий профилю адрес источника. Например, при создании правила с профилем фильтрации **Для Отдела маркетинга** выберите в поле **Адрес** раздела **Источник** группу Отдел маркетинга:



5. Чтобы трафик проходил в соответствии с условиями примера, установите в **Файрволе** следующую последовательность правил:



Чем выше в таблице стоит правило, тем выше его приоритет.

Разрешающее правило для сотрудника не сработает, если выше в таблице **Файрвола** находится правило, запрещающее трафик для отдела, в котором работает этот сотрудник.

6. Если в разделе **Сервисы** → **Защита и управление 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 он направляется в INPUT.

Настройка фильтрации трафика

Создайте профиль **Контроля приложений**, соответствующий нужным правилам:

1. Перейдите в раздел **Профили безопасности** → **Контроль приложений** и нажмите **Добавить**.

2. Введите **Название** профиля, **Комментарий** и добавьте профиль.

3. Нажмите в столбце **Управление** на , затем **Доступ к приложениям**.

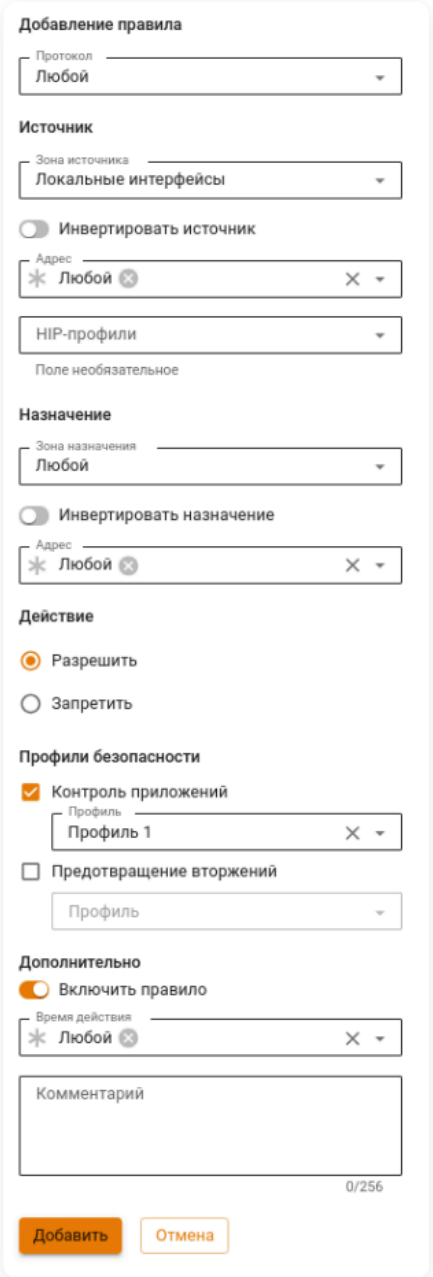
4. Выберите протоколы или группы протоколов и действия (**Запретить** или **Разрешить**), которые будут к ним применяться, затем нажмите **Применить**.

5. Нажмите **Сохранить** в левом нижнем углу.

Далее создайте правило **Файрвола** с созданным профилем **Контроля приложений**:

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите **Любой**;

- **Источник**:
  - **Зона источника** - выберите **Локальные интерфейсы**;
  - При необходимости укажите **Адрес** и **HIP-профиль** источника трафика.
- **Назначение**:
  - **Зона назначения** - выберите **Любой**;
  - При необходимости укажите **Адрес** назначения трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** в профилях безопасности и из раскрывающегося списка выберите созданный ранее профиль.

4. Включите правило и нажмите **Добавить**.

5. Поместите правило в конец таблицы **Файрвола**. Если в таблице есть правило, запрещающее все, поместите правило с профилем **Контроля приложений** над ним.

6. Если в разделе **Сервисы → Защита и управление 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 он направляется в INPUT.

Предотвращение вторжений

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

В разделе **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые NGFW будет применять к трафику, соответствующему этим сигнатурам.

Профили **Предотвращения вторжений** применяются при создании правил в разделе **Правила трафика** → **Файрвол**.

Если профиль не добавлен в правила таблицы **FORWARD** или **INPUT** раздела **Правила трафика** → **Файрвол**, трафик не будет фильтроваться системой **Предотвращения вторжений**.

В отбработке трафика не участвуют:

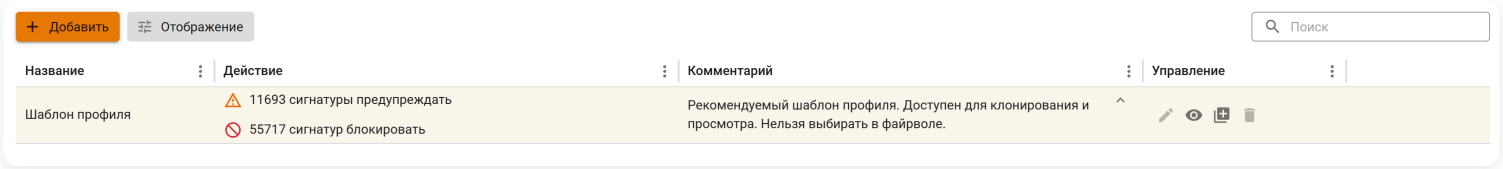
- Сигнатуры, не используемые в профилях.
- Профили, не используемые в правилах **Файрвола**.

Создание профилей

1. Перейдите в **Профили безопасности** → **Предотвращение вторжений** и нажмите **Добавить**.

Создание профиля через шаблон

1. Для клонирования нажмите :



- **Шаблон профиля** - подходит для максимальной защиты от кибератак. Включает динамически обновляемые черные списки хостов и эффективно очищает трафик из внешних сетей.

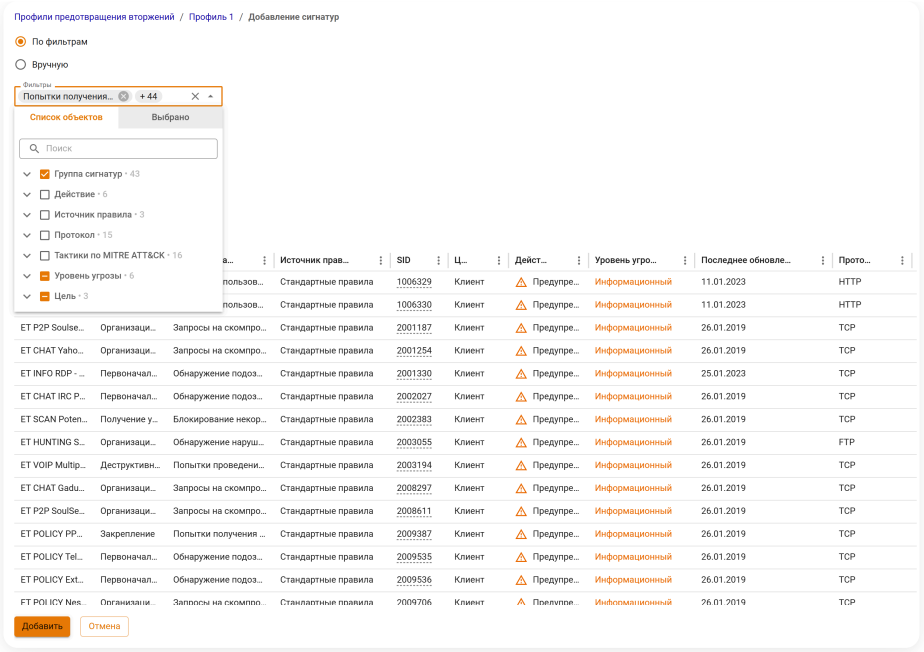
2. Чтобы просмотреть или изменить созданный профиль (описание и правила выбора сигнатур), нажмите или .
2. Введите название профиля, комментарий и нажмите **Добавить**.

3. Перейдите на вкладку **Сигнатуры** и нажмите **Добавить сигнатуры**.

4. Выберите способ добавления сигнатур в профиль:

По фильтрам

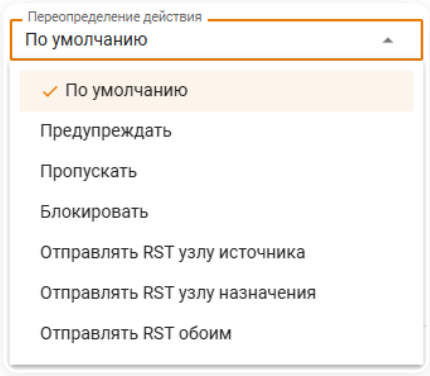
5. Выберите **Фильтры**. В таблице ниже отобразятся сигнатуры, соответствующие каждому из выбранных фильтров:



Доступные фильтры

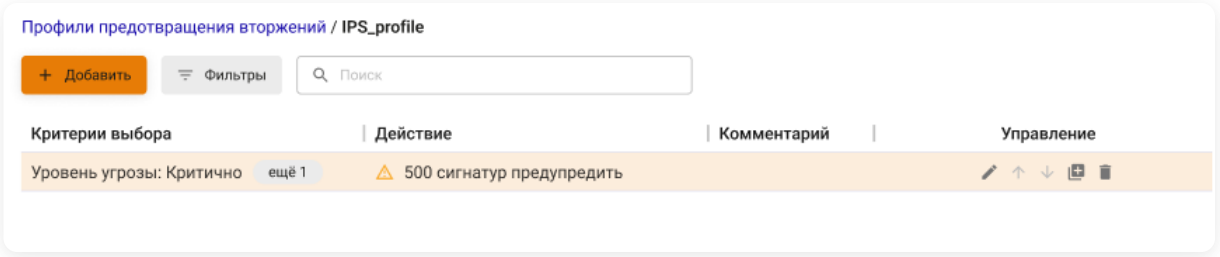
- **Группа сигнатур** - фильтр по готовым наборам сигнатур, сгруппированным по типу угроз.
- **Действие** - фильтр по действию, которое Ideco NGFW применит к трафику, соответствующему сигнатуре.
- **Источник правила** - фильтр по источнику сигнатуры.
- **Протокол** - фильтр по сетевому протоколу, который 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**:



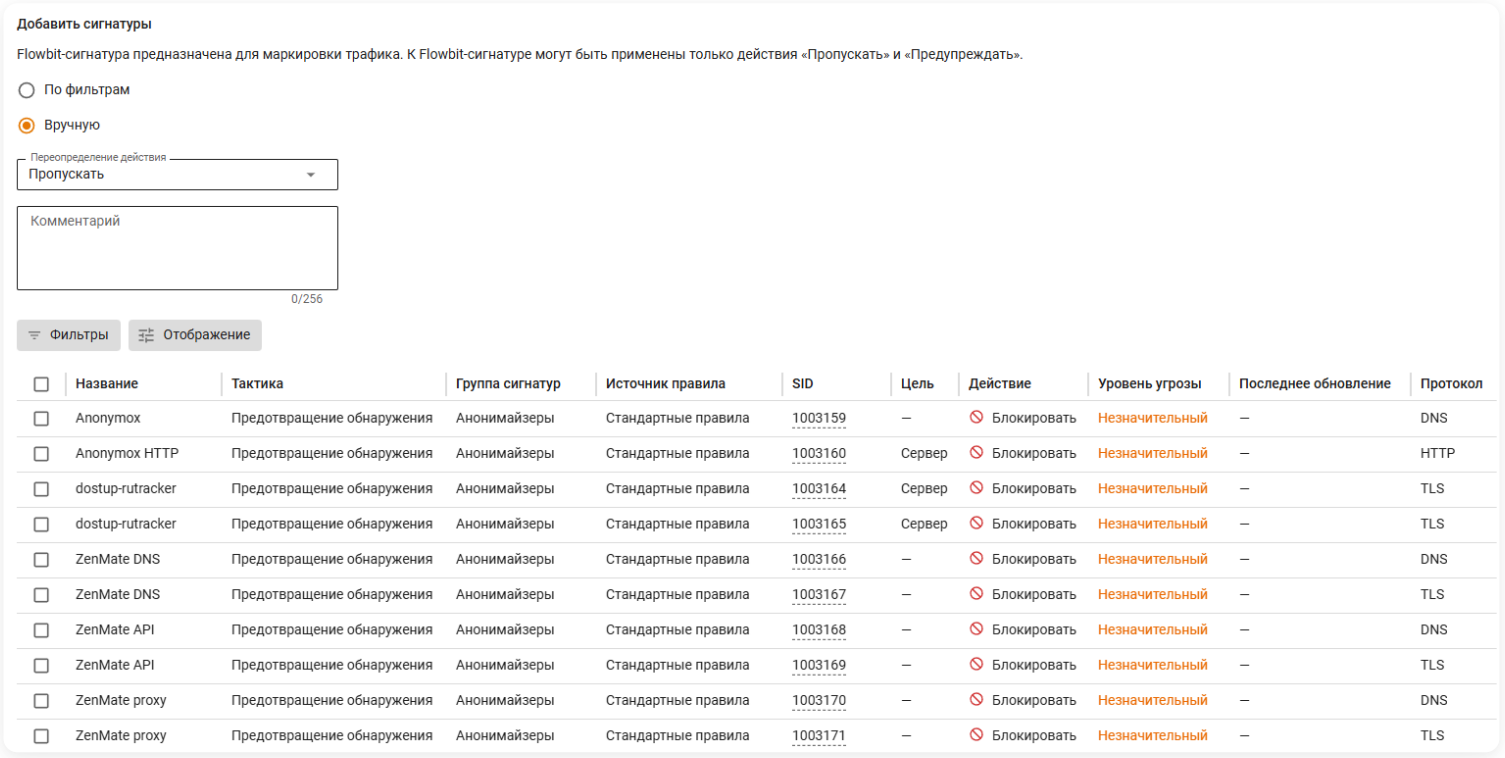
- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения.
- **Блокировать** - отбросить пакет и сгенерировать предупреждение.
- **Отправлять RST 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.

7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

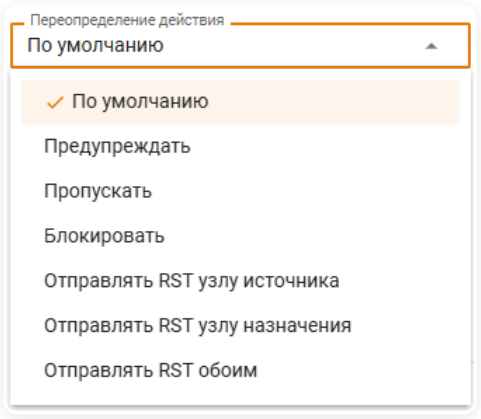


Вручную

5. В таблице отметьте сигнатуры, которые хотите добавить в профиль.При необходимости используйте **Фильтры**:

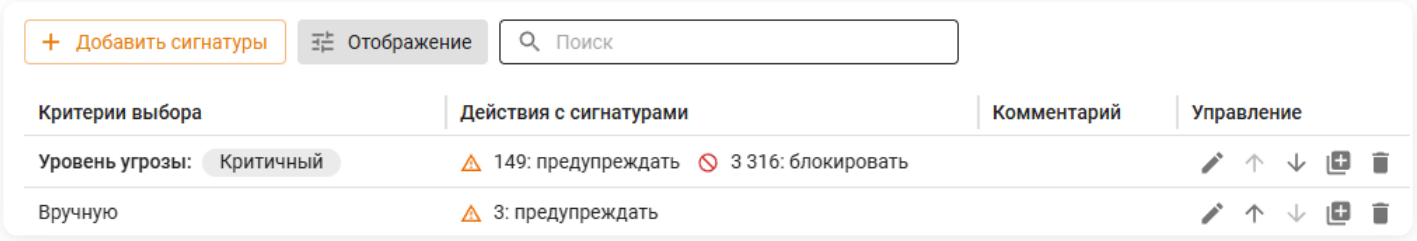


6. Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие **По умолчанию**:



- **По умолчанию** - предустановленное действие, указанное в базе правил при обновлении.
- **Предупреждать** - пропустить пакет и сгенерировать предупреждение.
- **Пропускать** - пропустить пакет без предупреждения.
- **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.

7. Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

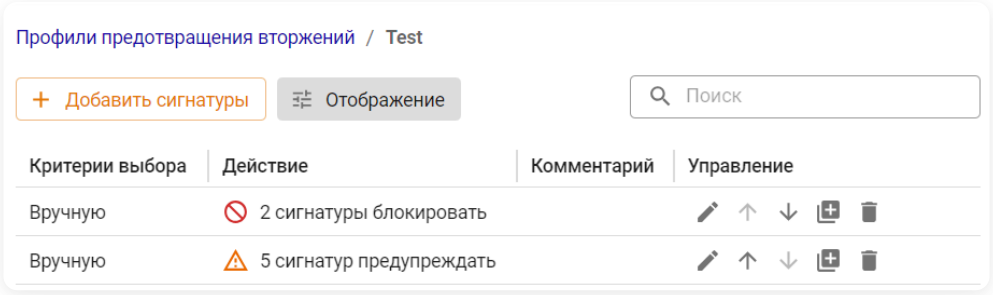


Количество сигнатур, отображаемых в таблице профилей, не всегда соответствует количеству сигнатур, добавленных при создании профиля. Это связано с тем, что для каждой сигнатуры может быть настроено несколько действий, но применяется только приоритетное. Приоритет определяется порядком правил внутри профиля.

В один профиль **Предотвращения вторжений** можно добавить несколько правил выбора сигнатур. Их приоритет можно менять в таблице профиля кнопками ↑ и ↓.

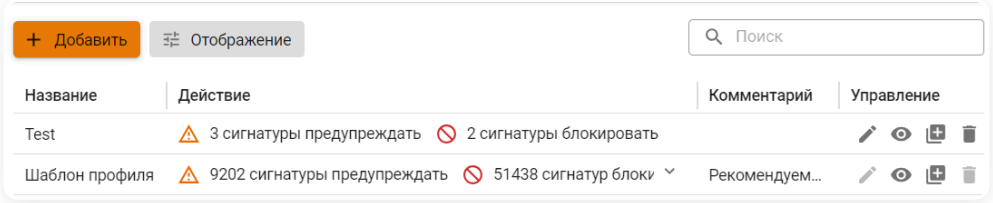
Пример отображения профиля при выборе нескольких действий сигнатур

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 **Профили безопасности** → **Предотвращение вторжений** в профиле Test отображаются две сигнатуры с действием **Блокировать** и три сигнатуры с действием **Предупреждать**, потому что фактически для дублирующихся сигнатур применяется более приоритетное правило:

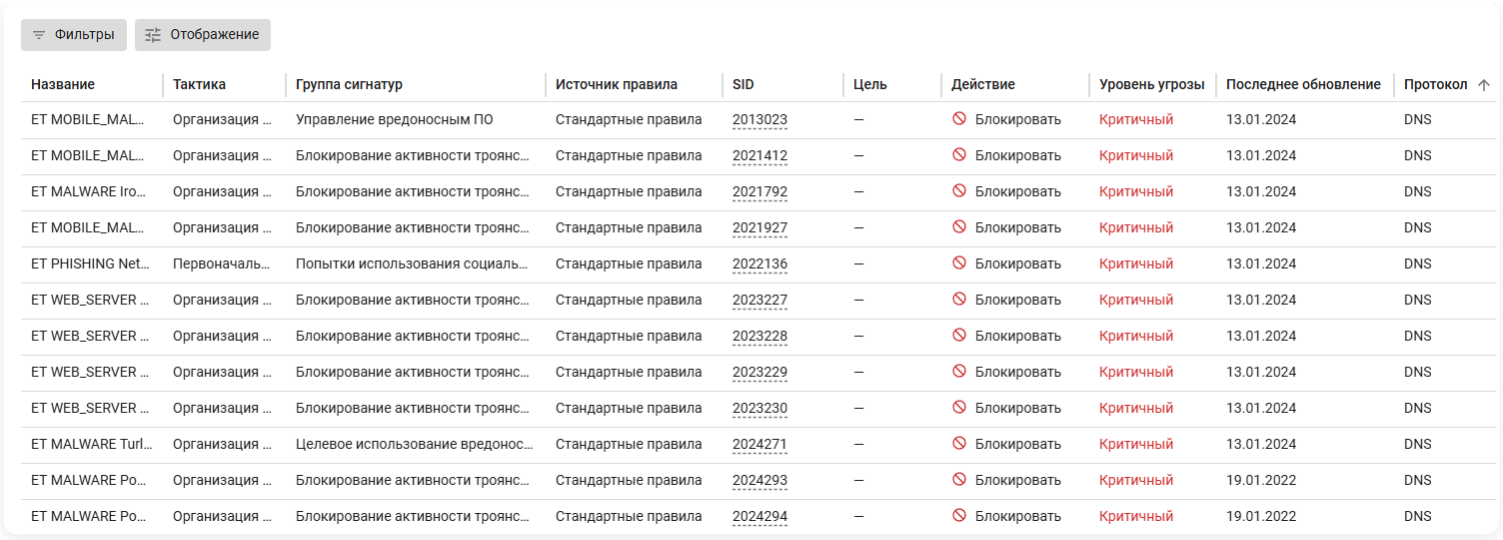


Использование оперативной памяти:

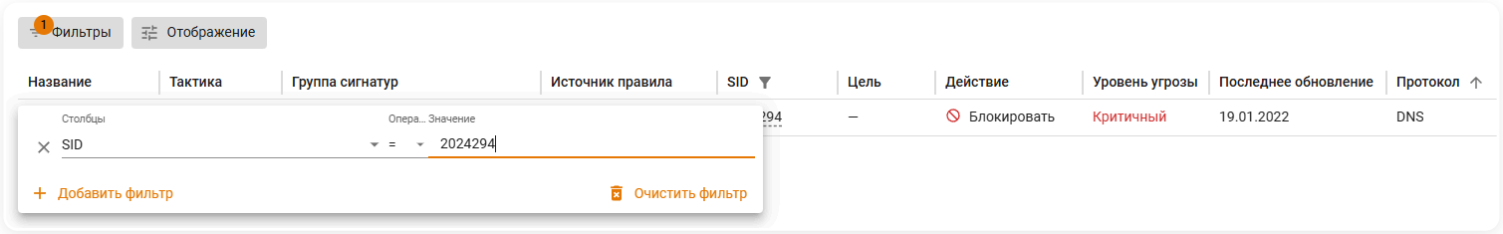
- Шаблон профиля не потребляет оперативную память.
- Настроенный профиль потребляет оперативную память, даже если не задействован в правилах Файрвола.
- Объем оперативной памяти, потребляемый одним профилем, зависит от количества сигнатур. Профиль, настроенный по рекомендуемому шаблону, использует ~450 МБ. Указано примерное значение, так как сигнатуры обновляются.

Изменение и просмотр профилей

Чтобы просмотреть созданный профиль (описание и правила выбора сигнатур), нажмите ✎. На вкладке **Выбранные сигнатуры** представлены все сигнатуры, для которых настроено одно или несколько действий:



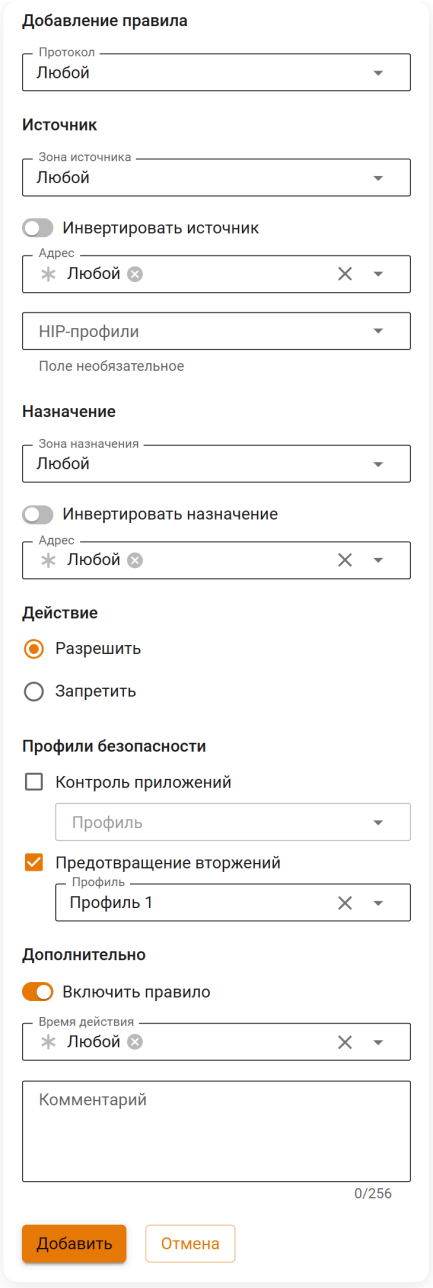
Для удобного поиска используйте **Фильтры**. Например, чтобы найти нужную сигнатуру по идентификатору:



Добавление профилей в правила Файрвола

1. Перейдите в **Правила трафика** → **Файрвол** → **FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, трафик которого требуется фильтровать системой **Предотвращения вторжений**.
- **Источник** - выберите **Адрес**, **Зону** и **HIP-профиль** источника трафика.
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Предотвращение вторжений** в разделе **Профили фильтрации трафика** и выберите необходимый профиль из раскрывающегося списка.

4. Включите правило или оставьте его выключенным.

5. Нажмите **Добавить**.

6. 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.

Сервисы

В этом 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 >

Балансировка и резервирование

Настройка резервирования каналов, статической и динамической балансировки

Перейти >

Маршрутизация

Настройка маршрутизации сетевого трафика, проходящего через Ideco NGFW.

Перейти >

BGP

Настройка BGP для обмена информацией о доступности сетей

Перейти >

OSPF

Настройка BGP для обмена информацией о доступности сетей

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 они стали доступны потребителям из сети интернет

Перейти >

ЛК/Портал SSL VPN

Настройка личного кабинета пользователя в Ideco NGFW (публикация и управление доступом пользователей)

Перейти >

Защита и управление 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 >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Сетевые интерфейсы

Название службы раздела *Сетевые интерфейсы*: `ideco-network-backend`; `ideco-network-nic`.

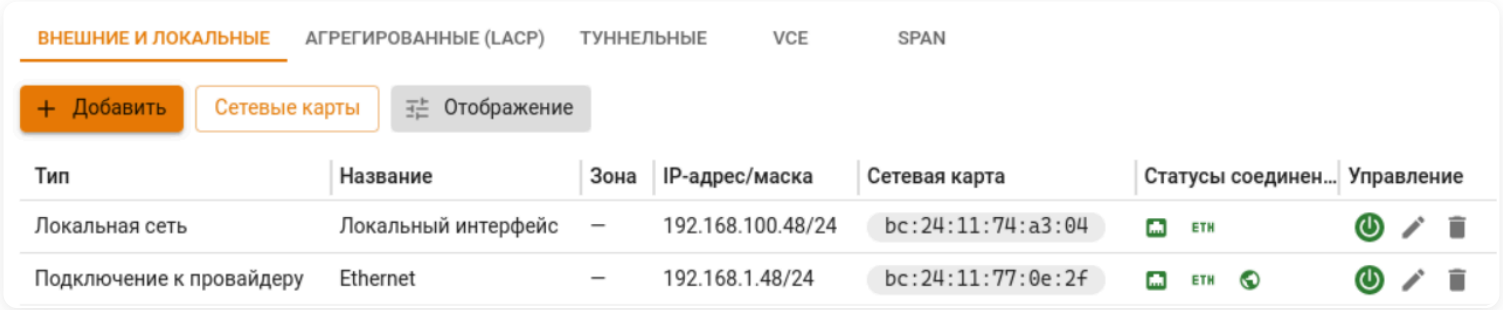
Список имен служб для других разделов доступен по ссылке.

Сетевой порт становится активным только после создания сетевого интерфейса (внешнего или локального). До этого момента индикаторы на подключенных сетевых портах не горят и Ethernet-кадры не передаются.

Для создания сетевых интерфейсов воспользуйтесь статьями:

- **Внешние и локальные интерфейсы**
- **Агрегированные интерфейсы (LACP)**
- **Туннельные интерфейфсы (GRE)**
- **VCE-интерфейсы**
- **SPAN-интерфейсы**

Все созданные интерфейсы представлены в виде таблиц на пяти вкладках:



Статусы соединения

- Сигнал есть

- Статус сигнала не определен

- Сигнала нет

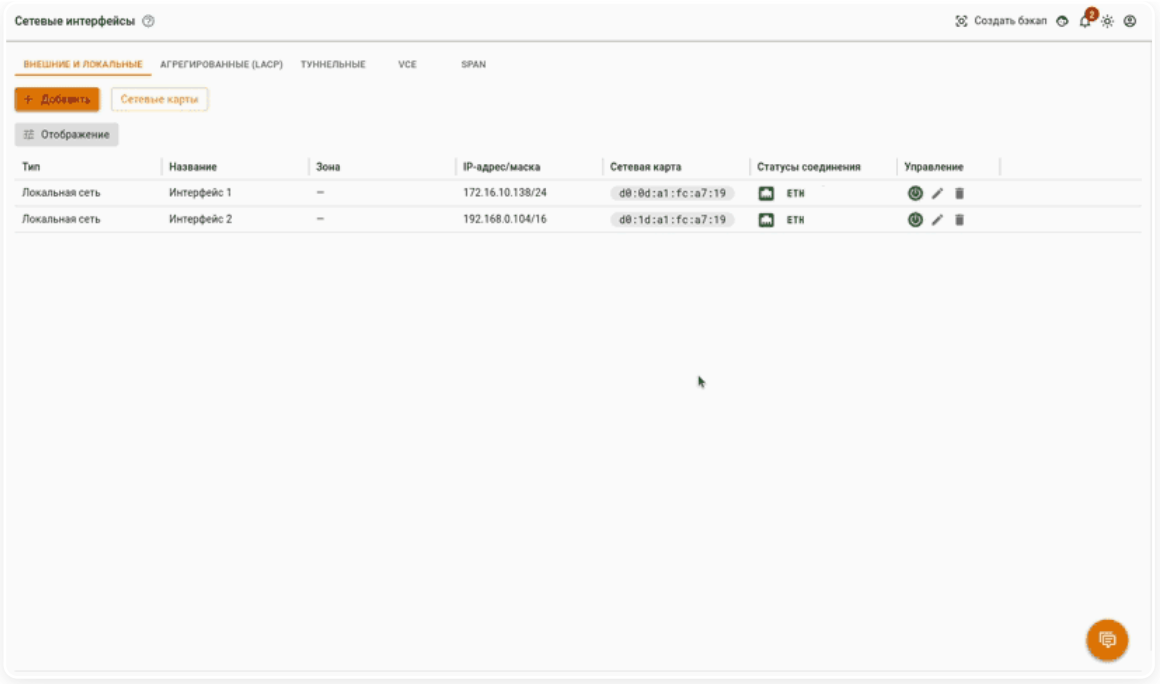
- IP-адрес назначен

- Соединение с интернетом установлено

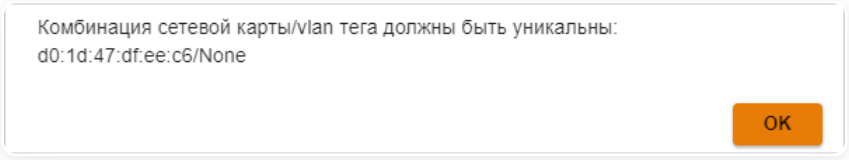
- Соединение с интернетом отсутствует

Редактирование сетевых интерфейсов

В режиме редактирования доступно изменение названия, сетевой карты (по кнопке), зоны, индекса интерфейса для Netflow и настроек конфигурации (вручную или автоматически):



Если сетевая карта уже используется каким-либо интерфейсом, то NGFW выведет окно с ошибкой:



При создании, редактировании или удалении сетевого интерфейса перевыпускается SSL-сертификат, поэтому вероятно снижение скорости работы веб-интерфейса Ideco NGFW. В этом случае рекомендуем нажать F5.

Миграция NGFW

При миграции NGFW с одной физической машины на другую (перенос диска или восстановление бэкапа на новом оборудовании), будут восстановлены настройки всех сетевых интерфейсов, указанные до миграции. Для удаления ненужных интерфейсов воспользуйтесь кнопкой .

Например: исходная версия NGFW 17.X → провели миграцию NGFW на новое оборудование → настроили новое оборудование → провели обновление → в разделе Сетевые интерфейсы будут отображаться старые (до миграции) и новые (после миграции и настройки) сетевые интерфейсы.

Ограничения сетевых интерфейсов

В зависимости от объема оперативной памяти на сервере в Ideco NGFW есть ограничения на количество сетевых интерфейсов:

- Количество сетевых интерфейсов (не VLAN):
  - до 16 ГБ - **40 сетевых интерфейсов**.
- Количество сетевых VLAN-интерфейсов:
  - до 8 ГБ - **14 VLAN-интерфейсов**;
  - от 8 до 16 ГБ - **33 VLAN-интерфейса**;
  - 16 ГБ и более - **66 VLAN-интерфейсов**.

При создании большего количества VLAN-интерфейсов могут возникнуть проблемы в работе Контроля приложений и Ограничения скорости.

В Ideco NGFW нет подразделения локальных интерфейсов на VPN-интерфейсы и Ethernet, поскольку Ideco NGFW не содержит локальных VPN-интерфейсов.

Внешние и локальные интерфейсы

На вкладке **Внешние и локальные** настраиваются Ethernet-интерфейсы:

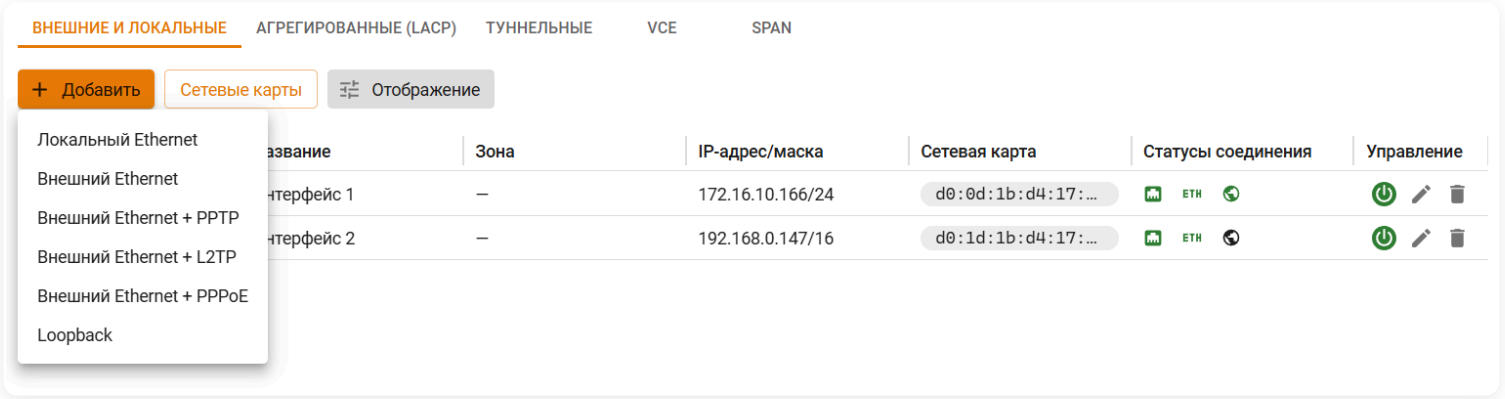
- **Локальный Ethernet** - настройка локальной сети.
- **Внешний Ethernet** - настройка подключения к интернету. Как правило, вся необходимая информация для настройки содержится в договоре с интернет-провайдером.
- **Подключение по PPTP** (Point-to-Point Tunneling Protocol) - один из старейших VPN-протоколов, разработанный для обеспечения защищенного доступа через интернет. Основан на использовании протокола PPP (Point-to-Point Protocol) для аутентификации и шифрования данных.
- **Подключение по L2TP** - подключение с применением протокола L2TP иногда используется интернет-провайдерами в целях обеспечения более надежной авторизации.
- **Подключение по PPPoE** - подключение с применением протокола PPPoE традиционно используется провайдерами, предлагающими подключение через xDSL.
- **Loopback-интерфейс** - виртуальный интерфейс, который может использоваться для динамической маршрутизации (BGP и OSPF), удаленного администрирования и подключения пользователей по VPN. Преимущество Loopback-интерфейса в том, что он никогда не перестанет работать, пока его не отключат административно.

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 считаются локальными и не подлежат публичной маршрутизации в интернете.
Для настройки внешних и локальных интерфейсов нажмите **Добавить**:



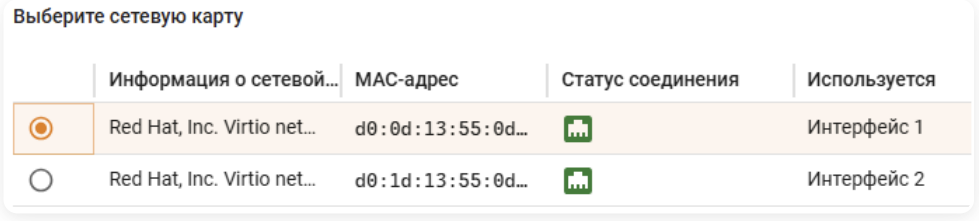
Выберите нужный интерфейс и следуйте инструкции:

Локальный Ethernet

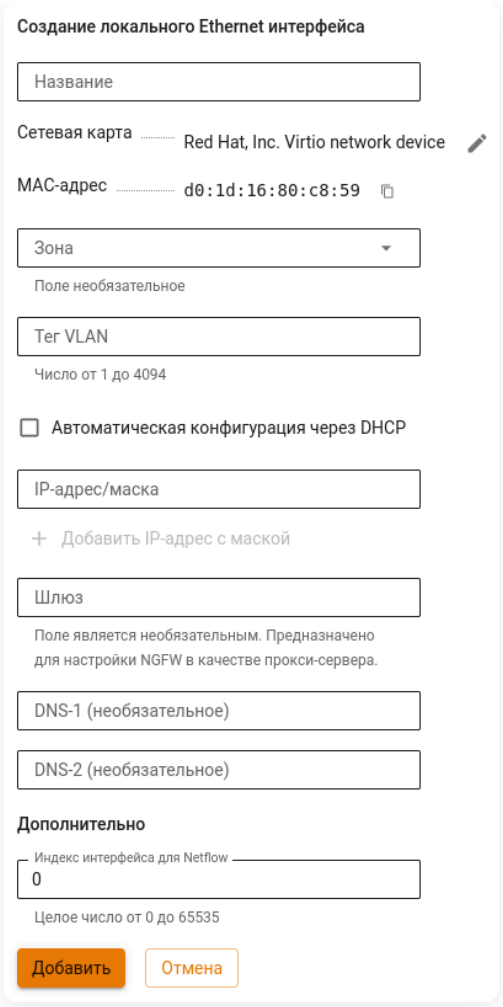
Ручная настройка

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название интерфейса** - имя для идентификации интерфейса.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Тег VLAN** - VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется в том случае, если сетевая карта уже используется.
- **Автоматическая настройка через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Как минимум, должен быть указан хотя бы один IP-адрес.
- **Шлюз** - IP-адрес шлюза.
- **DNS** - доступно два поля для указания DNS сервера (необязательно).
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

При выборе пункта **Локальный Ethernet** и заполнении поля **Шлюз** доступ в интернет будет отсутствовать.

Поле **Шлюз** в Локальном интерфейсе задается только если:

- Нет Внешнего интерфейса NGFW;
- NGFW используется как прокси-сервер.

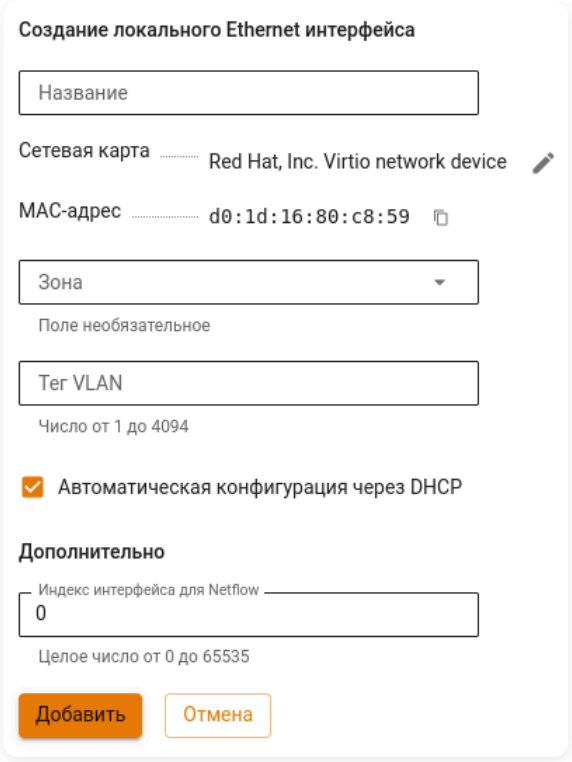
3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Автоматическая настройка

Используется, если ваш интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

1. Выберите сетевую карту.

2. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется:



3. При необходимости выберите объект типа **Зона** в одноименном поле.

4. Включите настройку **Автоматическая конфигурация через DHCP**.

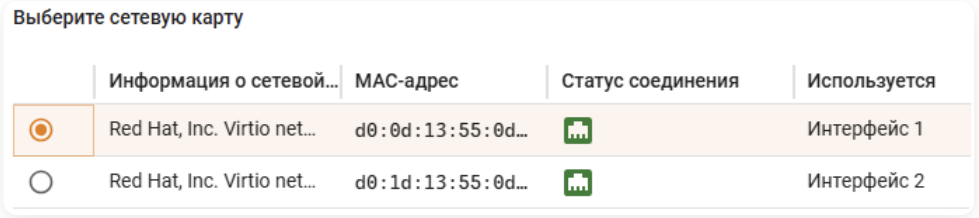
5. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Внешний Ethernet

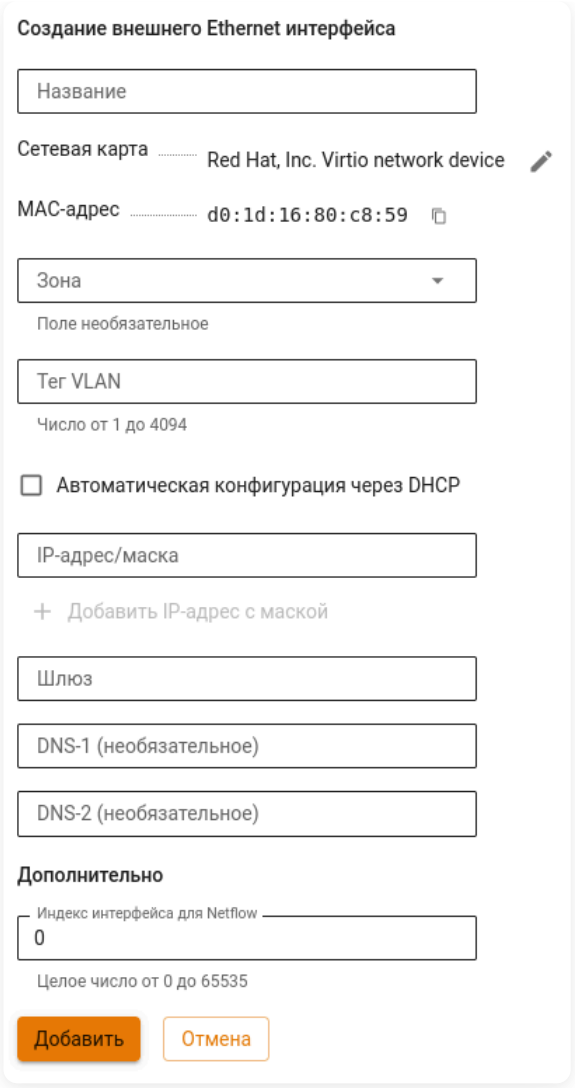
Ручная настройка

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название интерфейса** - имя, с помощью которого возможно в дальнейшем идентифицировать интерфейс.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется только в том случае, если сетевая карта уже используется.
- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес.
- **Шлюз** - укажите IP-адрес шлюза интернет-провайдера, через который будет осуществляться подключение к сети интернет.
- **DNS** - доступно два поля для указания DNS-сервера (необязательно).
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Автоматическая настройка

Используется, если интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

1. Выберите сетевую карту.

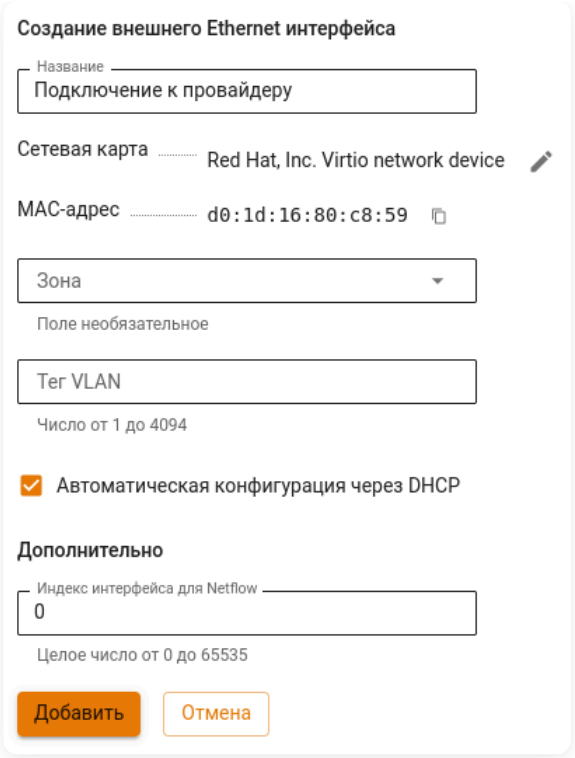
2. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется.

3. При необходимости выберите объект типа **Зона** в одноименном поле.

4. Включите настройку **Автоматическая конфигурация через DHCP**.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Пример настройки:



Подключение по 3G и 4G

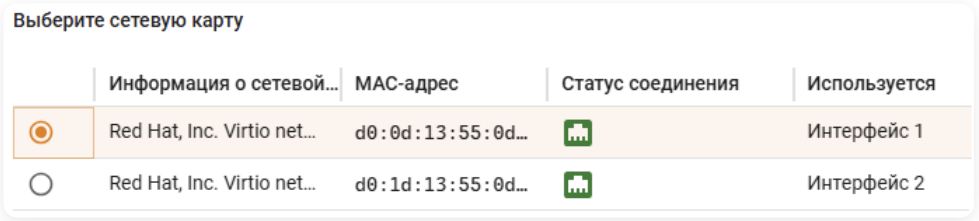
Сервер Ideco NGFW поддерживает некоторые модели USB-модемов, например, **Huawei E8372**. При подключении USB-модем будет отображаться в Ideco NGFW как новый ethernet-интерфейс.

Ideco NGFW поддерживает модели USB-модемов с Network Communication типа **CDC-Ethernet**. Список таких модемов представлен в таблице Список поддерживаемых USB-модемов.

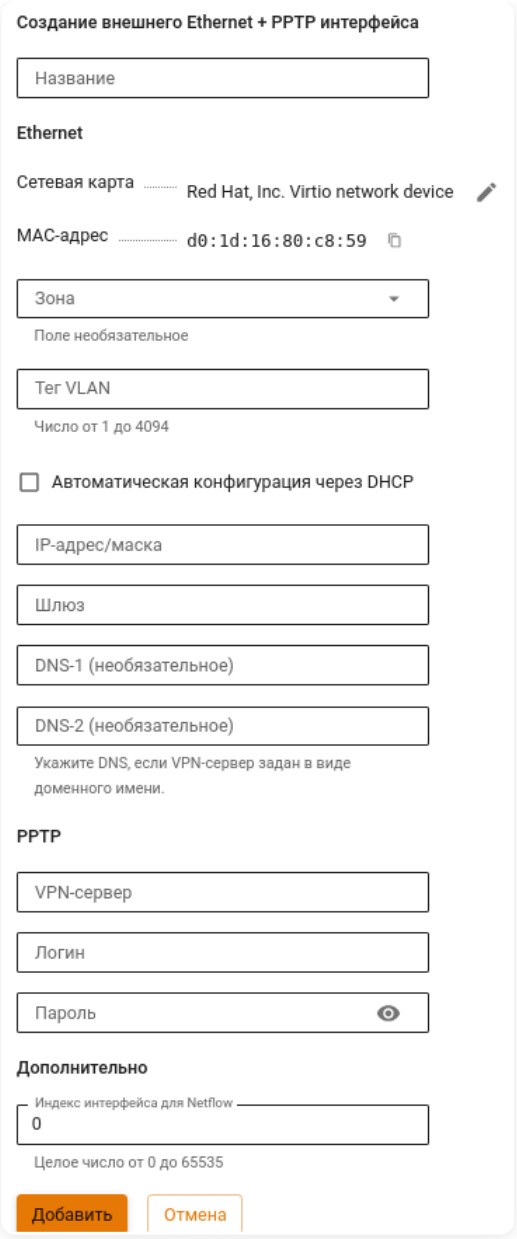
PPTP

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



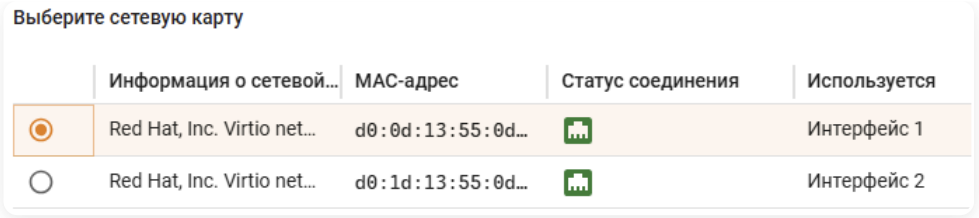
- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q.
- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес.
- **Шлюз** - IP-адрес шлюза.
- **DNS** - доступно два поля для указания DNS-сервера (необязательно).
- **VPN-сервер** - IP-адрес или доменное имя PPTP-сервера.
- **Логин** - имя пользователя для подключения по PPTP.
- **Пароль** - пароль для подключения по PPTP.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

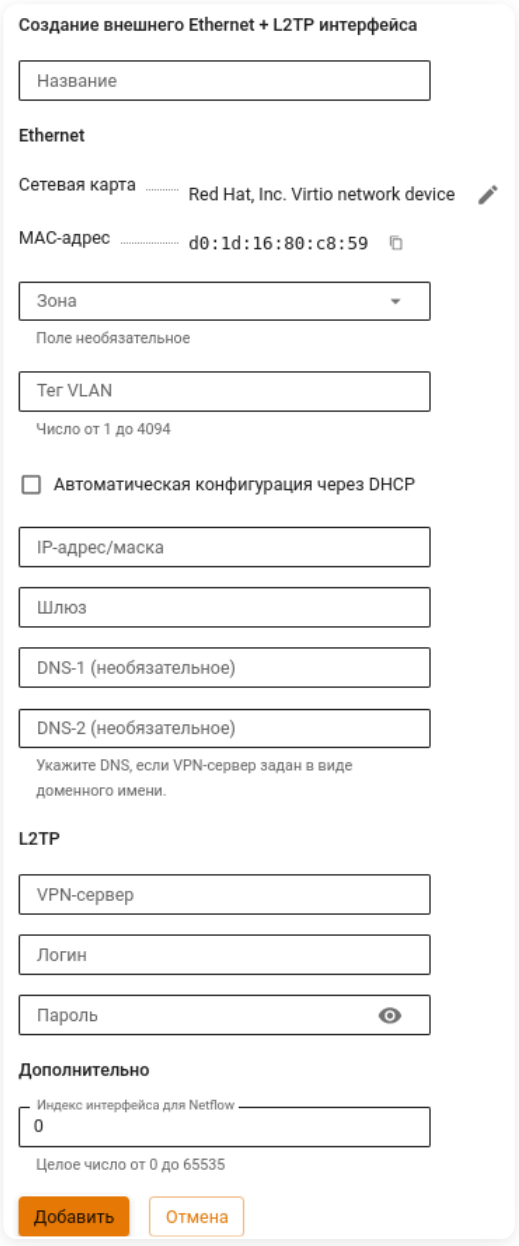
L2TP

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае если сетевая карта уже используется. Стандарт VLAN 802.3q.
- **Автоматическая конфигурация через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP.
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес.
- **Шлюз** - IP-адрес шлюза.
- **DNS** - доступно два поля для указания DNS-сервера (необязательно).
- **VPN-сервер** - IP-адрес или доменное имя L2TP-сервера.
- **Логин** - имя пользователя для подключения по L2TP.
- **Пароль** - пароль для подключения по L2TP.

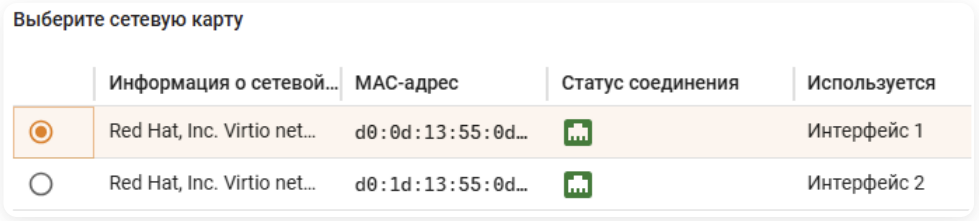
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

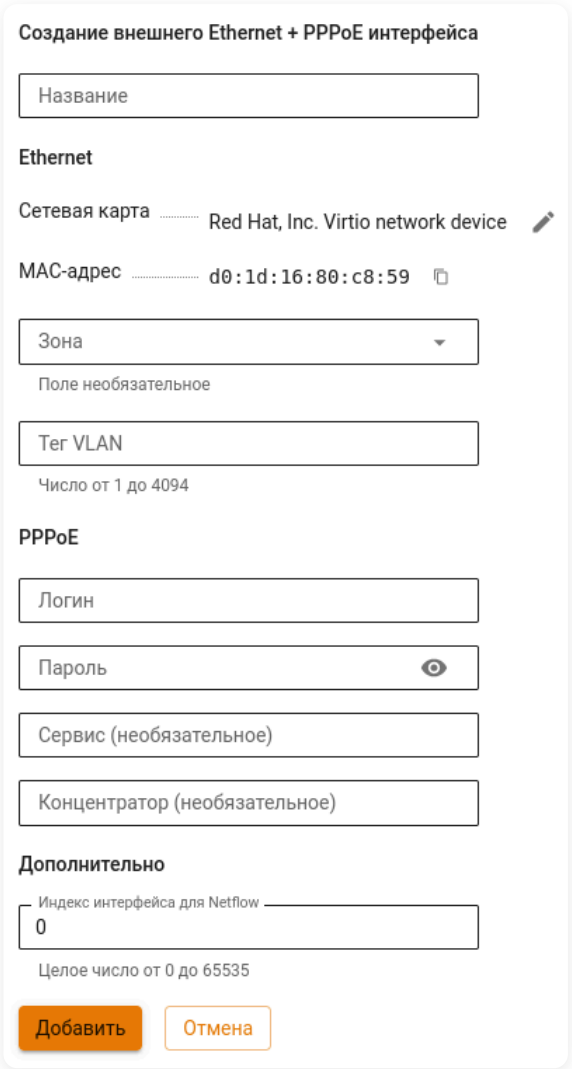
PPPoE

Для настройки такого подключения в веб-интерфейсе выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42.
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру.
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64. Список предустановленных зон приведен в статье.
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q.
- **Логин** - имя пользователя для подключения по PPPoE.
- **Пароль** - пароль 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.

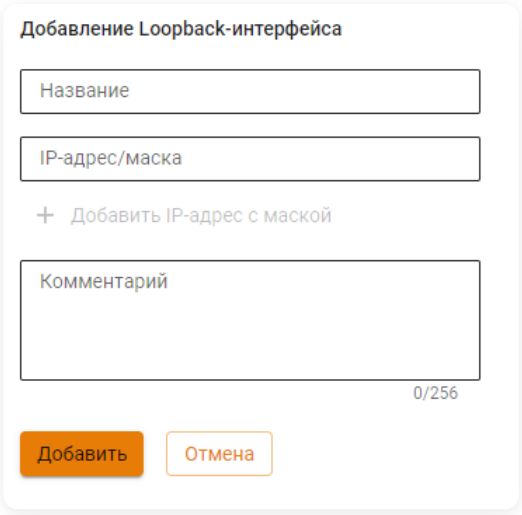
3. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

При подключении к провайдеру с использованием протокола PPPoE настройте DNS-сервер вручную, воспользовавшись статьей.

Loopback

> Нельзя создавать Loopback-интерфейс в настроенном кластере. Если все же требуется использовать Loopback-интерфейс, настройте его до объединения в кластер.

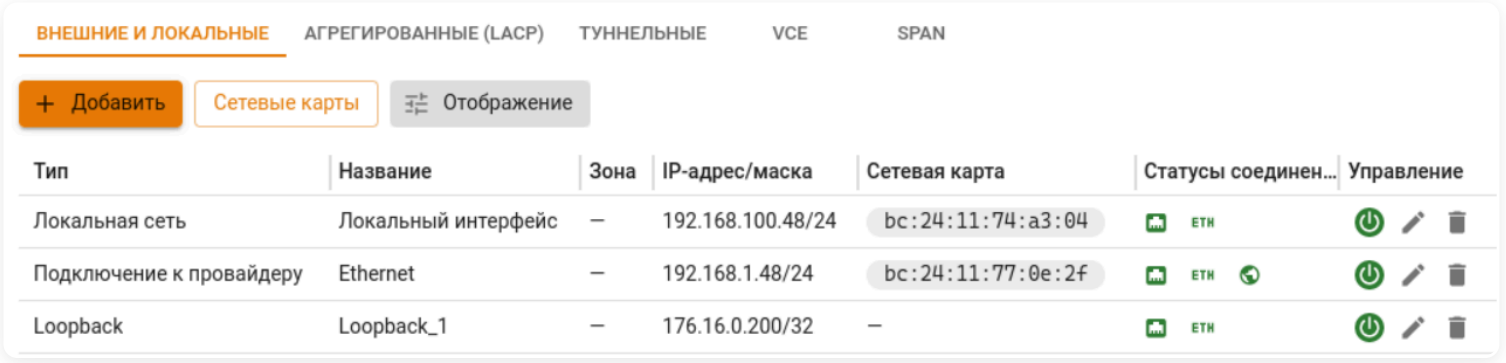
1. Заполните поля:



- **Название** - введите название интерфейса;
- **IP-адрес/маска** - введите IP-адрес, который требуется назначить на Loopback-интерфейс, с маской в формате `x.x.x.x/x`;
- **Комментарий** - поле не обязательное.

> 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`

2. Нажмите **Добавить**. Loopback-интерфейс появится в таблице внешних и локальных интерфейсов:



Особенности настройки Loopback-интерфейса

При работе с Loopback-интерфейсом используйте правила:

- Для доступа к веб-интерфейсу Ideco NGFW 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 **Файрвола** в поле **Адрес назначения** укажите IP-адрес, назначенный на Loopback-интерфейс. Опубликованные ресурсы будут доступны по IP-адресу Loopback-интерфейса.
- При создании SNAT-правила **Файрвола** 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.

Агрегированные интерфейсы

LACP-интерфейсы (Link Aggregation Control Protocol) - протокол, предназначенный для объединения нескольких физических каналов в один логический в сетях Ethernet.

Особенности работы агрегированных интерфейсов

Агрегированные каналы LACP используются как для повышения пропускной способности, так и для повышения отказоустойчивости.

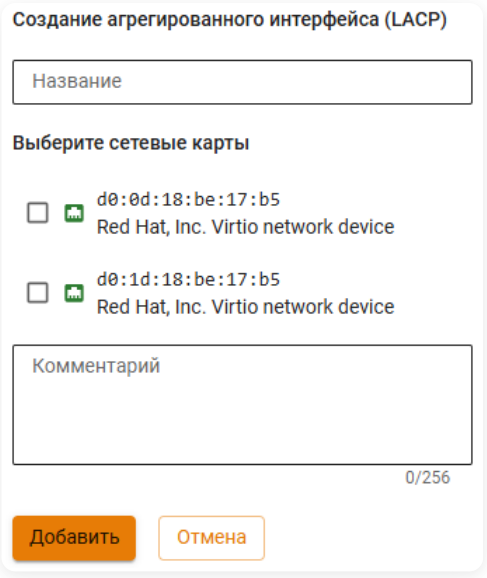
Не рекомендуем использовать **LACP** на виртуальных сетевых адаптерах, так как системы виртуализации некорректно обрабатывают работу **LACP** на таких интерфейсах или вовсе не поддерживают этот режим.

Особенности работы LACP-интерфейсов:

- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active** режим - постоянная рассылка LACP пакетов.
- Проверка соседства осуществляется в режиме **slow** - раз в 30 секунд.
- Количество сетевых карт, объединяемых в агрегированный интерфейс, не ограничено.
- Нельзя добавлять в VCE LACP-интерфейсы и логические VLAN-интерфейсы, созданные на агрегированном интерфейсе.
- Нельзя добавлять LACP-интерфейсы в кластерном режиме.

Настройка агрегированного интерфейса

Чтобы объединить несколько сетевых интерфейсов в один агрегированный, перейдите в **Сервисы** → **Сетевые интерфейсы** → **Агрегированные (LACP)**, нажмите **Добавить** и выполните действия:



1. Укажите название для последующей идентификации интерфейса.

2. Выберите сетевые карты.

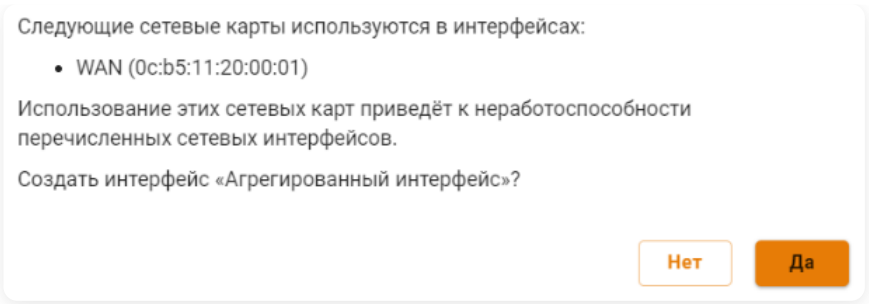
3. Нажмите **Добавить**.

Статусы сетевых карт

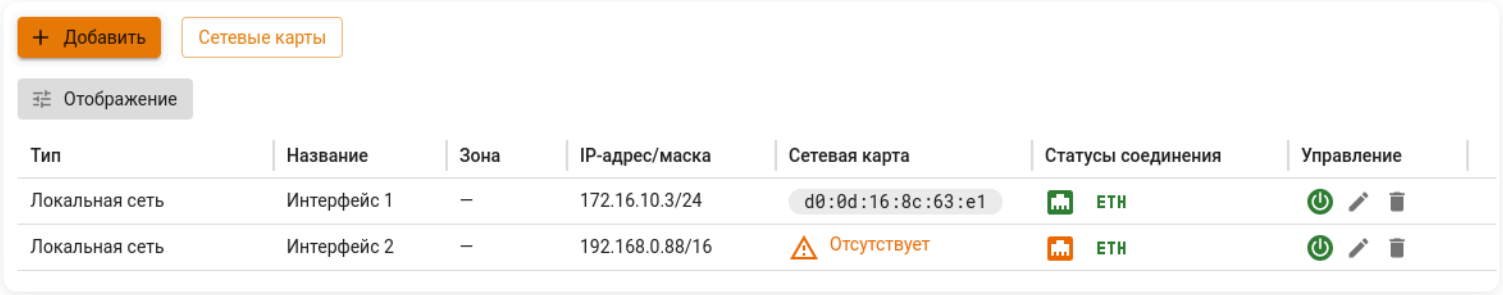
- Сетевая карта уже используется другим интерфейсом

- Сетевая карта не используется

Если были выбраны уже использующиеся сетевые карты, то при нажатии на кнопку **Добавить** появится сообщение:

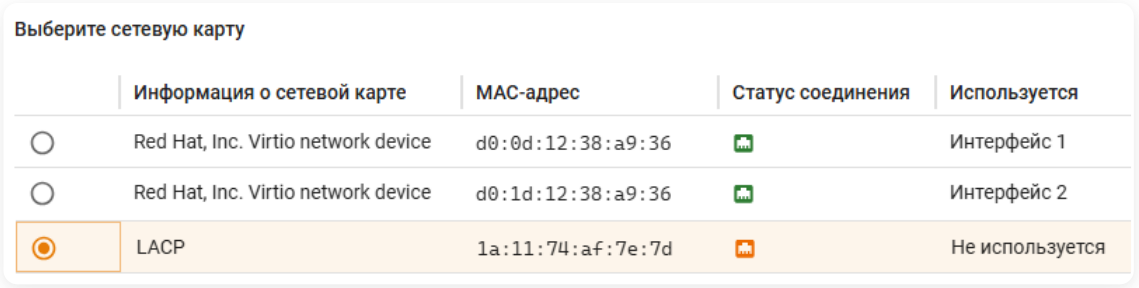


При выборе **Да** сетевая карта будет использоваться агрегированным интерфейсом и станет недоступна для ранее созданного сетевого интерфейса:



Создание логического интерфейса

На основе созданного агрегированного интерфейса можно добавить любой логический интерфейс, в том числе с указанием VLAN. Для этого перейдите в **Сервисы** → **Сетевые интерфейсы** → **Внешние и локальные** и создайте Ethernet-интерфейс, выбрав в качестве сетевой карты добавленный на предыдущем шаге LACP-интерфейс:

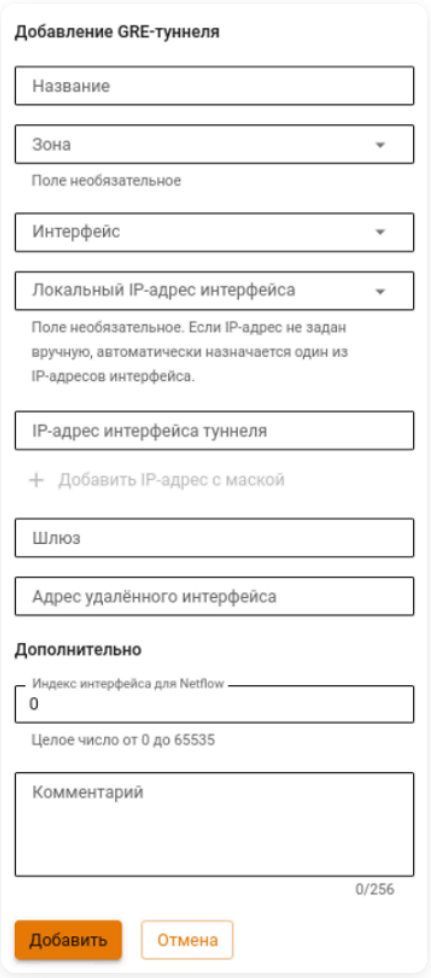


Туннельные интерфейсы

GRE-туннель - это соединение точка-точка с возможностью передавать широковещательный трафик. На таких интерфейсах может работать протокол динамической маршрутизации OSPF. Пакеты, проходящие внутри GRE, не шифруются.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе Туннельные. 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 добавления GRE-туннеля нажмите **Добавить**, заполните поля и нажмите **Добавить**:



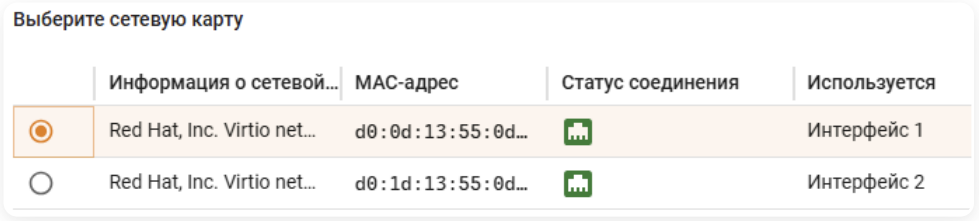
- **Название** - введите название туннельного интерфейса.
- **Зона** - выберите объект типа **Зона**, в состав которого будет входить создаваемый туннельный интерфейс. Список предустановленных зон приведен в статье.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение.
- **Локальный IP-адрес интерфейса** - укажите IP-адрес родительского интерфейса запущенного туннеля.
- **Адрес удаленного интерфейса** - укажите IP-адрес интерфейса для подключения.
- **IP-адрес/маска** - 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** - необязательное поле.

VCE-интерфейсы

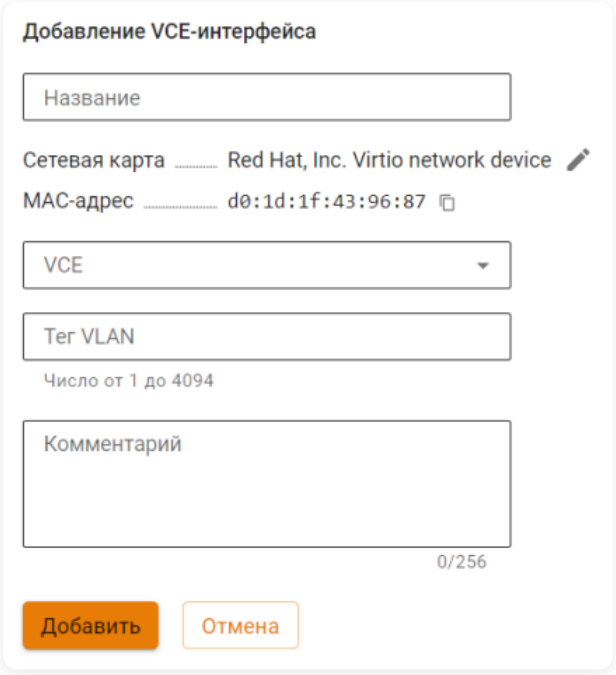
В Ideco NGFW есть возможность пробросить сетевые карты и VLAN-интерфейсы Ideco NGFW в виртуальные серверы, созданные в разделе **Управление сервером** → **VCE**.

Чтобы назначить сетевую карту или VLAN-интерфейс VCE, нажмите **Добавить** и выполните действия:

1. Выберите сетевую карту:



2. Заполните поля:



- **Название** - введите название VCE-интерфейса;
- **VCE** - выберите из списка VCE, созданный в разделе **Управление сервером** → **VCE**;
- **Тег VLAN** - если нужно пробросить в VCE порт сетевой карты, оставьте поле пустым. Если нужно пробросить только VLAN, укажите тег VLAN - число от 1 до 4094;
- **Комментарий** - поле может быть пустым.

Не присваивайте VCE сетевые карты, которые используются корневым NGFW, без указания тега VLAN. В противном случае доступ к веб-интерфейсу NGFW будет потерян.

3. Нажмите **Добавить**.

При наличии большого количества VCE-интерфейсов в таблице воспользуйтесь кнопкой **Фильтры**.

По кнопке **Сетевые карты** доступны все сетевые карты корневого VCE, еще не проброшенные в дочерние VCE.

Переданная VCE сетевая карта будет недоступна для использования корневым NGFW. Также невозможно будет назначить эту карту другому VCE без указания тега VLAN.

SPAN-интерфейсы

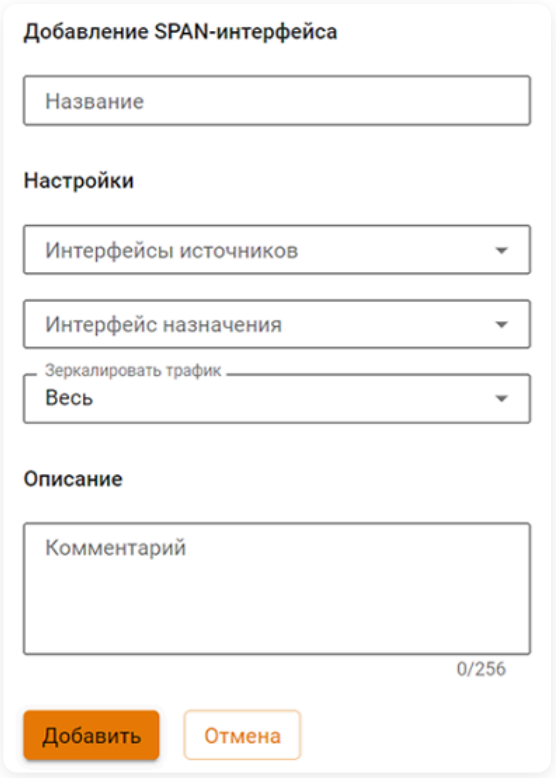
SPAN (Switch Port ANalyzer) - функция, позволяющая копировать пакеты с порта или группы портов коммутатора или маршрутизатора (порт зеркалирования) и отправлять на выбранный порт (порт мониторинга). В Ideco NGFW SPAN-интерфейс позволяет дублировать трафик локальных и внешних интерфейсов на отдельное внешнее устройство для его мониторинга, анализа и выявления угроз.

SPAN-интерфейс должен быть свободным Ethernet-интерфейсом, не используемым для других целей.

Чтобы создать SPAN-интерфейс, выполните действия:

1. Перейдите в раздел **Сервисы** → **Сетевые интерфейсы** → **SPAN** и нажмите **Добавить**.

2. Заполните поля:



- **Название** - введите название SPAN-интерфейса;
- **Интерфейсы источников** - выберите интерфейсы, трафик которых хотите дублировать. Доступные варианты: Ethernet (как внешние, так и локальные, за исключением PPPoE, L2TP и PPTP), VLAN, а также клиентский VPN-трафик;
- **Интерфейс назначения** - выберите интерфейс, на который будет дублироваться трафик;

Не указывайте в полях **Интерфейс источника** и **Интерфейс назначения** интерфейсы Ethernet + L2TP/PPTP/PPPoE. Этот тип интерфейсов не поддерживается в настройках SPAN.

- **Зеркалировать трафик** - выберите тип трафика, который хотите дублировать. Доступные варианты: Весь, Только входящий или Исходящий;
- **Комментарий** - поле может быть пустым.

3. Нажмите **Добавить**.

SPAN-интерфейс может быть перегружен при большом количестве наблюдаемых интерфейсов.

Балансировка и резервирование

Название службы раздела **Балансировка и резервирование**: `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

При наличии нескольких подключений к интернет-провайдерам балансировку и резервирование можно осуществлять следующими способами:

- **Резервирование** - при отключении основного интерфейса трафик будет направлен через все доступные.
- **Статическая балансировка** - трафик между несколькими подключениями будет разделен согласно правилам маршрутизации.
- **Динамическая балансировка** - подключения будут поочередно переключаться в зависимости от нагрузки, при этом сессии пользователей будут равномерно распределяться между доступными подключениями.

Перед настройкой резервирования каналов, динамической и статической балансировки, убедитесь, что на сервере созданы минимум два подключения к интернету. Если подключение одно, создайте дополнительное. Подробнее - в статье Внешние и локальные интерфейсы.

Если на внешний интерфейс назначено более одного IP-адреса, то при использовании режимов балансировки и резервирования будет использоваться IP-адрес, выбранный случайным образом при запуске Ideco NGFW.

Для балансировки и резервирования в Ideco NGFW важно учитывать настройки маршрутизации и NAT.

Практические последствия неправильной настройки:

- Нарушение балансировки трафика между каналами из-за некорректных маршрутов.
- Проблемы с возвратом пакетов при использовании NAT без учета маршрутов.
- Потеря резервирования каналов при неправильной настройке приоритетов.
- Снижение производительности сети из-за неоптимальных путей прохождения трафика.

Правильная настройка маршрутизации и NAT позволяет эффективно использовать возможности Ideco NGFW по балансировке и резервированию трафика, обеспечивая высокую доступность и производительность сетевой инфраструктуры.

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Основное

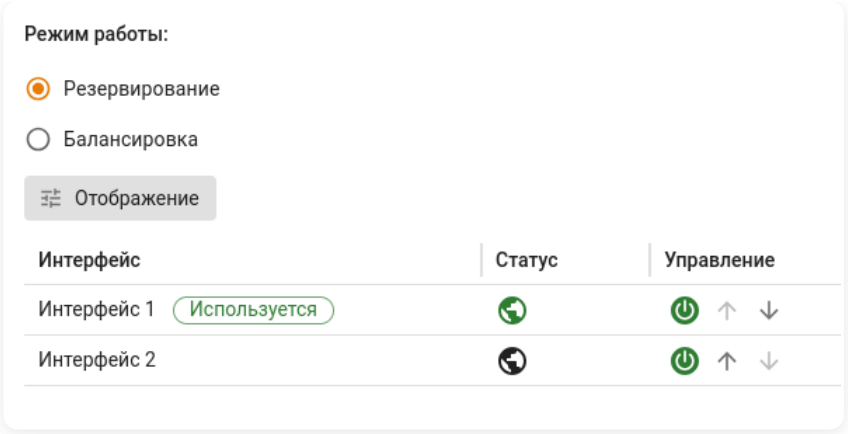
На вкладке доступен выбор режимов - **Балансировка** или **Резервирование**.

При **Резервировании** Ideco NGFW использует каналы в соответствии с их приоритетом. Приоритет задается порядком подключений в таблице, сверху вниз. Если интернет стал недоступен через используемое подключение, то Ideco NGFW будет перебирать подключения сверху вниз до первого активного.

При **Балансировке** Ideco NGFW балансирует трафик в зависимости от загрузки подключений.

Резервирование каналов

Перейдите в раздел **Сервисы** → **Балансировка и резервирование** и выберите режим **Резервирование**.



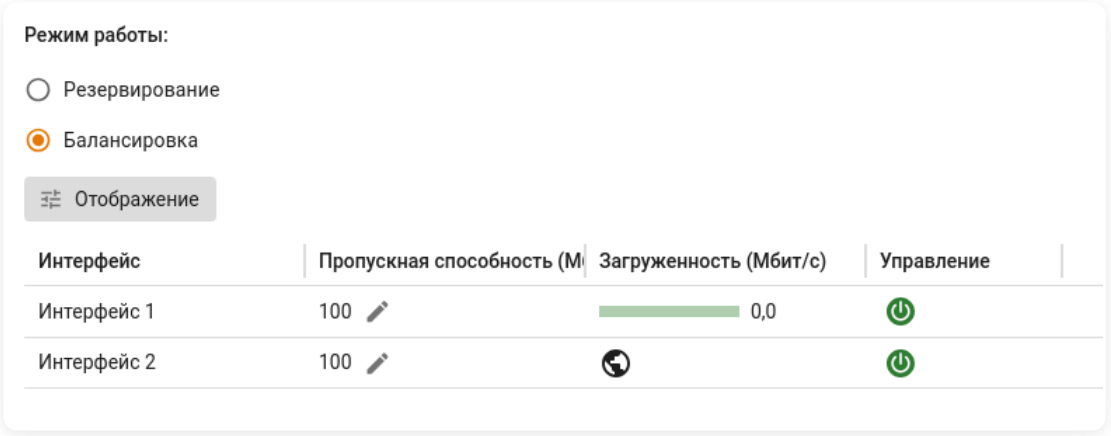
Подключение, которое используется в данный момент, отмечено тегом **Используется**. Для смены приоритета используйте соответствующие элементы управления ( ).

Динамическая балансировка. Распределение нагрузки по нескольким подключениям

Действия для настройки:

1. Перейдите в раздел **Сервисы** → **Балансировка и резервирование**.

2. Выберите режим работы **Балансировка**.



Для равномерного распределения сессий между подключениями необходимо указать значение **Пропускной способности** - максимальной скорости интернета по тарифам провайдеров. Ideco NGFW будет автоматически балансировать трафик в зависимости от загрузки подключений.

Трафик балансируется автоматически без дополнительных настроек, включая тарфик прокси-сервера.

Статическая балансировка. Доступ к сети интернет через определенное подключение к провайдеру

Способы применения:

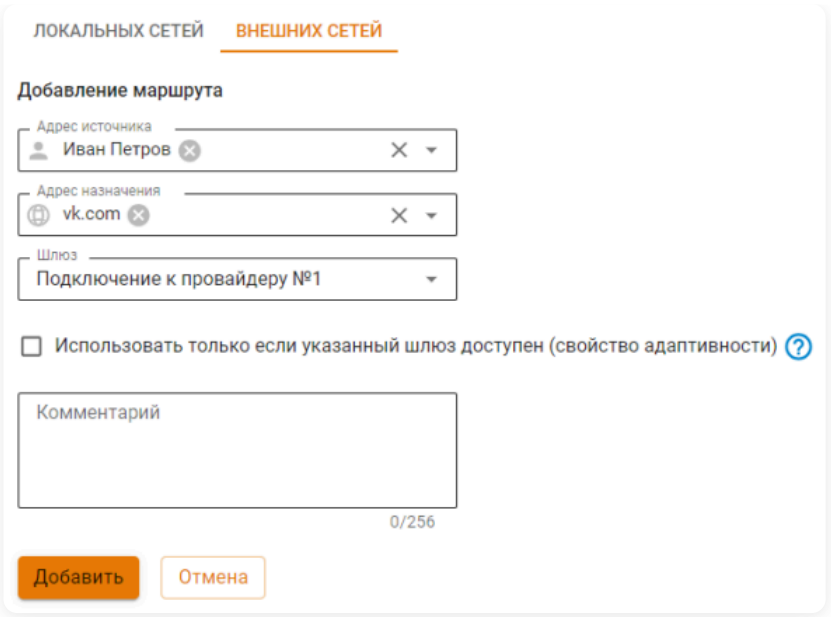
- Направление части трафика через интернет-провайдера, чья тарификация для этого трафика дешевле.
- Предоставление доступа к внутренним сетям одного из провайдеров для определенных пользователей/групп пользователей.

Действия для настройки:

1. Перейдите в раздел меню **Сервисы** → **Маршрутизация** → **Внешних сетей**.

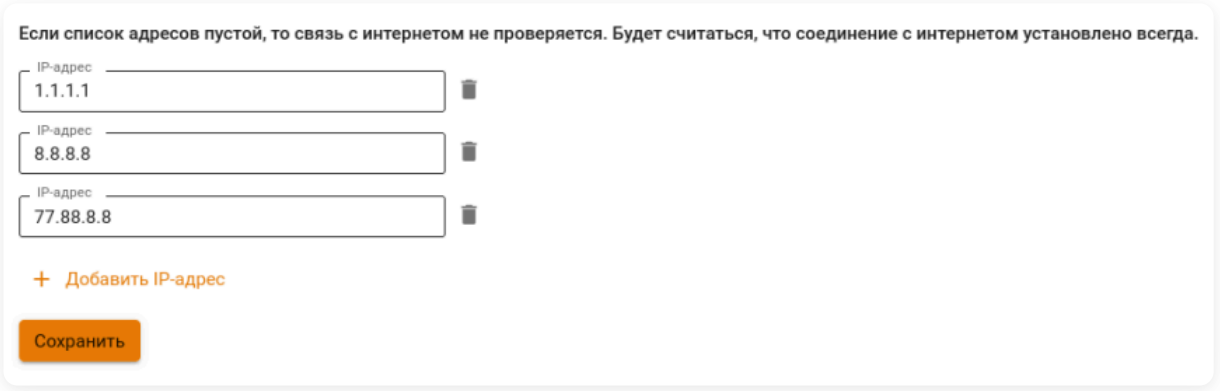
2. Добавьте правила маршрутизации для определенного списка ресурсов, трафик к которым необходимо направить через нужное подключение к провайдеру, нажав кнопку **Добавить**.

Пример направления трафика к ресурсу **vk.com** от пользователя **Иван Петров** через подключение к провайдеру **Подключение к провайдеру №1**:



Адреса для проверки связи

На вкладке задаются IP-адреса, которые Ideco NGFW будет использовать для проверки связи с интернетом. По умолчанию заданы три IP-адреса - DNS-серверы Cloudflare, Google и Яндекс:



Ideco NGFW посылает на эти адреса ping-запросы. Соединение с интернетом считается установленным, если проходит пинг хотя бы до одного адреса из списка. Если этого не происходит, Ideco NGFW считает, что соединение с интернетом у интерфейса отсутствует - статус интерфейса меняется с на . Полный цикл проверки, включая определение доступности нового шлюза после изменения настроек, занимает до 30 секунд.

Если список IP-адресов пуст, проверка интернет-соединения не выполняется. NGFW считает, что интернет всегда доступен. В этом случае:

- Режим **Резервирование** не будет работать.
- Режим **Балансировка** будет работать некорректно, если на одном из интерфейсов отсутствует интернет.

Маршрутизация

Название службы раздела **Маршрутизация**: `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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.
- Автоматически переключаться на альтернативный маршрут при недоступности шлюза или интерфейса (адаптивность).
- Обеспечить корректную доставку как исходящего, так и ответного трафика.

Доступность шлюза проверяется с помощью отправки ARP-запроса на получение MAC-адреса для IP, указанного в качестве шлюза.

В веб-интерфейсе Ideco NGFW есть возможность маршрутизировать локальные и внешние сети. Создавать и редактировать маршруты можно в разделе **Сервисы → Маршрутизация**.

Для организации доступа в удаленные сети через роутер в локальной сети читайте статью по ссылке.

При маршрутизации локальных и внешних сетей доступны GRE-интерфейсы в качестве шлюза.

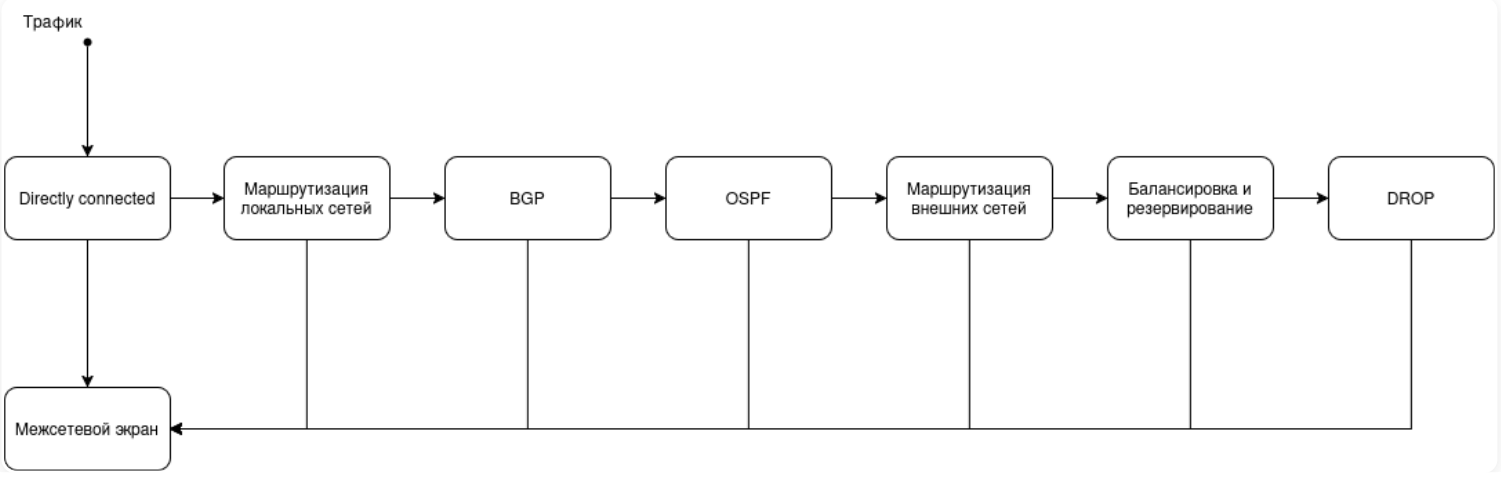
Обработка трафика

В процессе маршрутизации пакет проходит через несколько последовательных этапов:

- Если маршрут найден на каком-либо из этапов, пакет передается в модуль фильтрации **Межсетевой экран**.
- Если маршрут не найден, поиск продолжается в таблицах следующего блока.

После определения маршрута результат маршрутизации сохраняется. Путь пакета фиксируется и не изменяется при последующей обработке.

Этапы обработки пакета



1. **Directly connected** - проверяется, принадлежит ли адрес назначения одной из локально доступных подсетей.

2. **Маршрутизация локальных сетей** - выполняется поиск маршрута в таблицах маршрутизации локальных сетей.

3. **BGP** - выполняется поиск маршрута в таблице динамического протокола BGP.

4. **OSPF** - выполняется поиск маршрута в таблице динамического протокола OSPF.

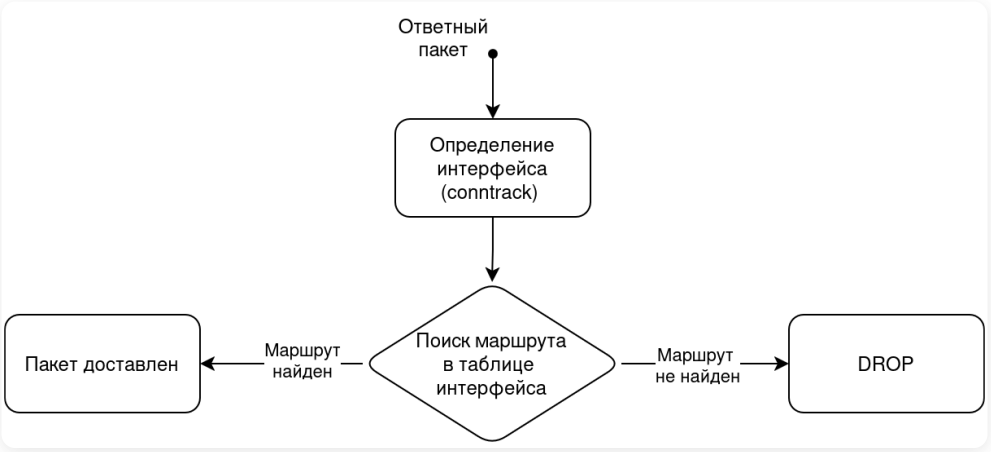
5. **Маршрутизация внешних сетей** - используются политики маршрутизации, определяющие, по каким условиям (например, по источнику или интерфейсу) будет направляться сетевой трафик. В соответствии с найденной политикой пакет перенаправляется на указанный маршрут. В качестве одного из вариантов действия правила может быть перенаправление в **Балансировку и резервирование**.

6. **Балансировка и резервирование** - выполняется распределение трафика между несколькими шлюзами или выбор резервного маршрута.

В маршрутизации **Внешних сетей** 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.

Настройка маршрутизации

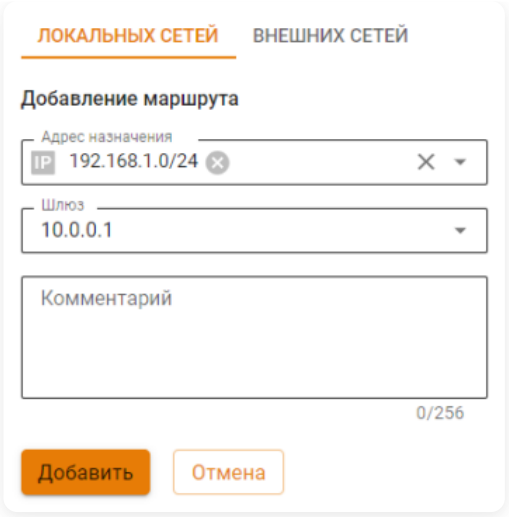
Маршрутизация локальных сетей

Для маршрутизации локальных сетей при добавлении маршрута отсутствует поле **Адрес источника**, так как сеть внутренняя.

Для добавления нового маршрута:

1. Перейдите в раздел **Сервисы** → **Маршрутизация** → **Локальных сетей** и нажмите **Добавить**.

2. Заполните поля:



- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться правило. Возможные типы объектов: IP-адрес, подсеть, домен, список IP-объектов, диапазон IP-адресов.
- **Шлюз** - выберите объект, через который направляется трафик. Возможные типы объектов: IP-адрес, пользователь.
- **Комментарий** - необязательное поле описания маршрута. Значение не должно быть длиннее 128 символов.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

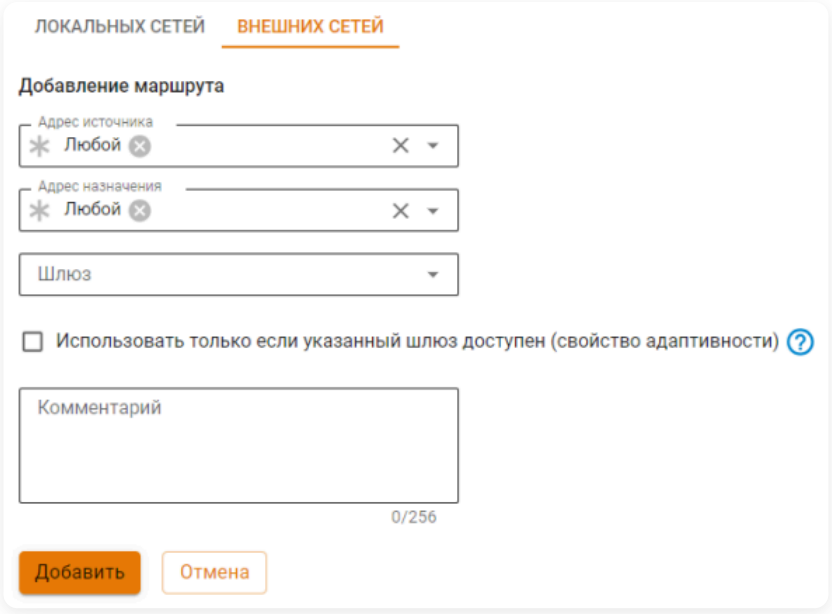
При создании IPsec-подключения в разделе **Сервисы** → **IPsec** с включенной опцией **Автоматическое создание маршрутов** будут добавляться маршруты до локальных сетей Ideco NGFW в таблицу **Маршрутизации локальных сетей**.

Маршрутизация внешних сетей

Для добавления нового маршрута:

1. Перейдите в раздел **Сервисы** → **Маршрутизация** → **Внешних сетей** и нажмите кнопку **Добавить**.

2. Заполните поля:

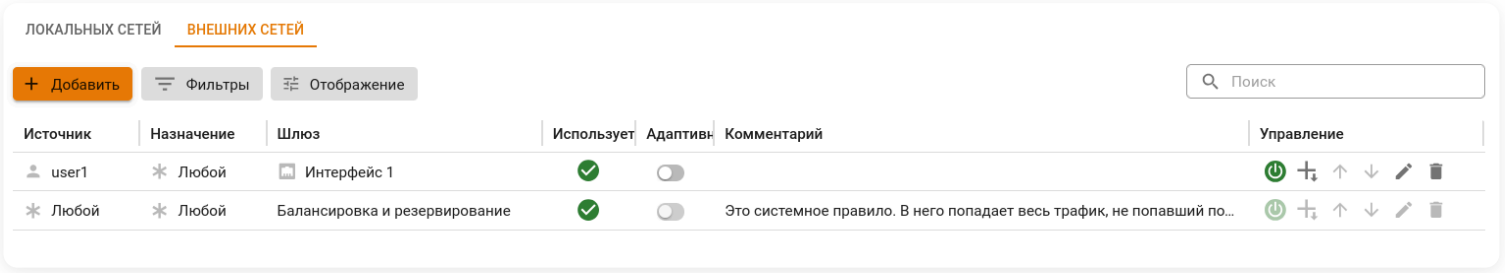


- **Адрес источника** - выберите объекты, для которых будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен.
- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен.
- **Шлюз** - выберите объект, через который будет направлен трафик. Возможные типы объектов: сетевой интерфейс, IP-адрес.
- **Использовать только если указанный шлюз доступен (свойство адаптивности)** - если свойство включено, то при недоступности шлюза или интерфейса поиск маршрута продолжится по следующим правилам маршрутизации. Если свойство отключено (по умолчанию), то трафик

отправляется в выбранный шлюз или интерфейс. Если шлюз недоступен или интерфейс не работает, то трафик будет отброшен (destination unreachable).

- **Комментарий** - необязательное поле описания маршрута. Значение не должно быть длиннее 128 символов.

После сохранения маршрута страница выглядит так:



Кнопки ↓ и ↑ повышают или понижают приоритет правила.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

Статусы в столбце **Используется**:

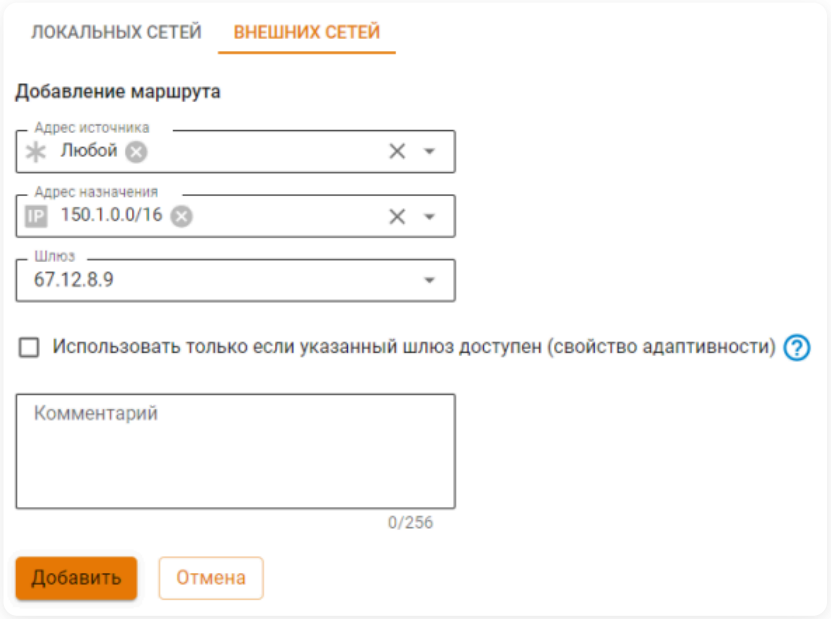
- маршрут активен и трафик, попадающий под условия маршрута, будет перенаправлен в указанный **Шлюз**;
- маршрут не активен и трафик, попадающий под условия маршрута, не будет обработан правилом.

Трафик, не попавший под условия правил маршрутизации, или с объектом **Любой** в качестве шлюза, будет отправлен в Балансировку и резервирование.

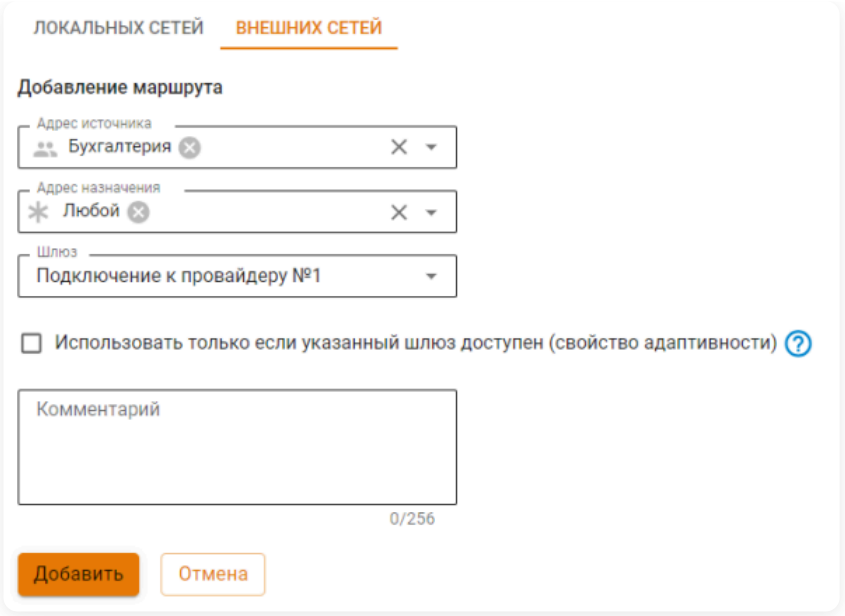
Примеры популярных маршрутов

При маршрутизации трафика через подключения к провайдеру важно понимать, что чаще всего одного маршрута недостаточно. Понадобится также переопределить адрес с помощью SNAT, иначе такой маршрут не будет работать. SNAT можно настроить с помощью Файрвола.

Задача: любой трафик в подсеть 150.1.0.0/16 направлять на шлюз 67.12.8.9



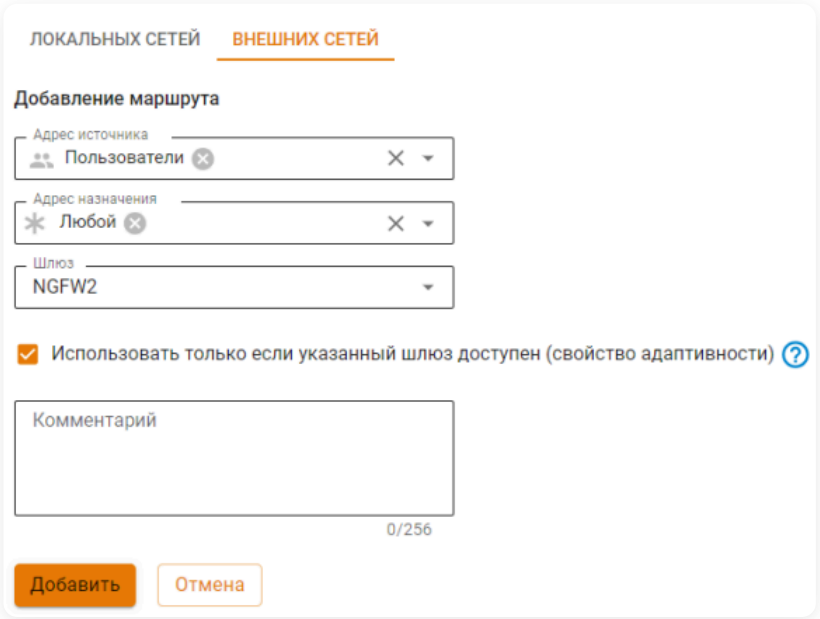
Задача: весь трафик пользователей из группы Бухгалтерия направить через шлюз выбранного сетевого интерфейса



Если настраивается маршрут в удаленную сеть через дополнительный роутер, расположенный в одной локальной сети с клиентами, то убедитесь, что нет "асимметричной маршрутизации" и роутер вынесен в DMZ. Подробнее в статье Как избавиться от асимметричной маршрутизации трафика.

Задача: предоставить доступ в интернет пользователям NGFW1, подключенного по IPsec к NGFW2, через внешний интерфейс NGFW2

Для доступа в интернет пользователям NGFW1 укажите в качестве шлюза IPsec-подключение к NGFW2:



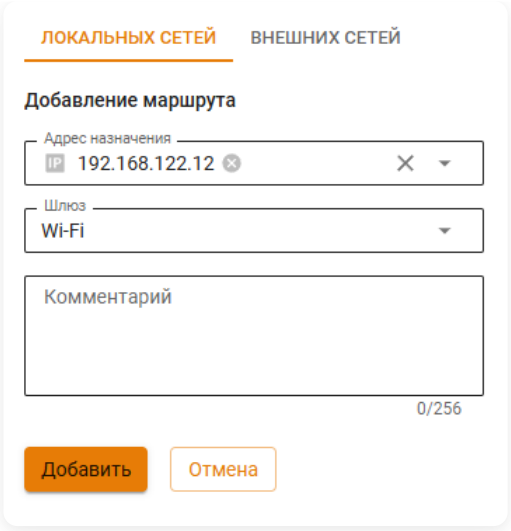
Задача: создать правило маршрутизации до сетей филиала через подключение client-to-site

Если установка подключения site-to-site до сетей филиала недоступна, в Ideco NGFW можно настроить подключение роутера client-to-site. В этом случае при добавлении маршрута локальных сетей в качестве шлюза используется роутер, который подключается по VPN.

Для настройки подключения выполните действия:

1. В разделе **Пользователи** → **Учетные записи** создайте учетную запись для роутера с разрешенным доступом к VPN.

2. При добавлении маршрута в разделе **Сервисы** → **Маршрутизация** → **Локальных сетей** выберите созданного пользователя в поле **Шлюз**:



Сети за роутером станут доступны после установки VPN-подключения через Ideco NGFW.

Информация об особенностях маршрутизации и организации доступа при настроенном VPN-подключении представлена в статье.

Полезные ссылки

- **OSPF**
- **BGP**
- **Балансировка и резервирование**
- **Особенности маршрутизации и организации доступа**
- **Как избавиться от асимметричной маршрутизации трафика**

BGP

Название службы раздела **BGP**: `frr`; `ideco-routing-backend`.

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:

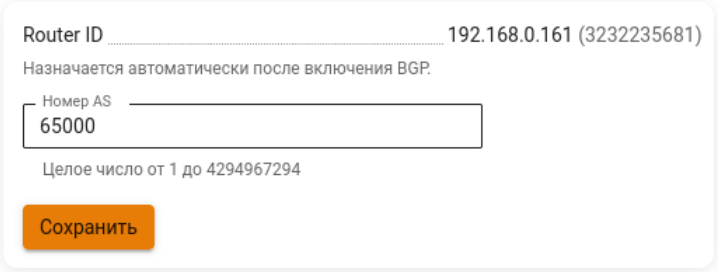
- Указать номер автономной системы.
- Создать и включить как минимум одного BGP-соседа.

На Ideco NGFW 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.

Настройка автономной системы

Перейдите в раздел **Сервисы** → **BGP** и заполните поля:

1. Введите номер автономной системы в строку **Номер AS** и нажмите **Сохранить**:

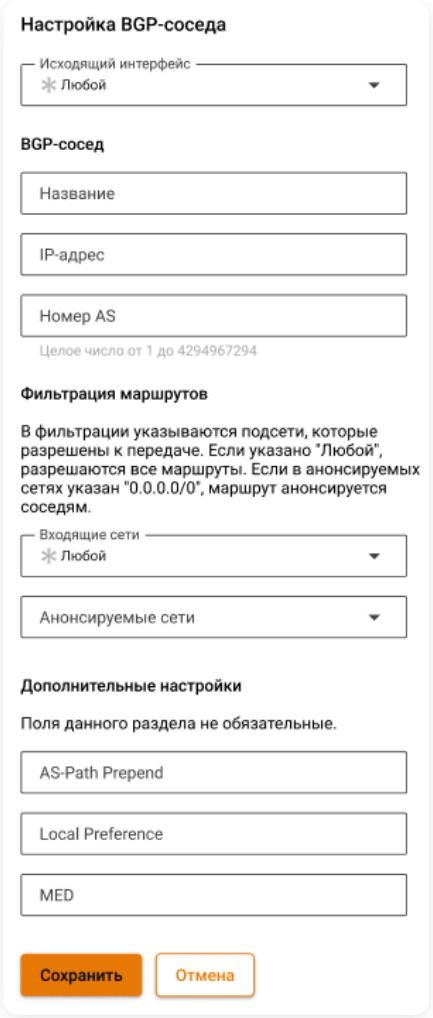


Ideco NGFW автоматически заполняет поле **Router ID** значением наибольшего IP-адреса локальной сети, указанного в разделе Сетевые интерфейсы.

2. Включите модуль **BGP**.

Настройка BGP-соседей

Для добавления BGP-соседа нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Исходящий интерфейс** - интерфейс Ideco NGFW, 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.
- **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 (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 объектов фильтрации

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, соединенных по IPSec в тунельном режиме, воспользуйтесь BGP. Подробнее про настройку подключения двух NGFW по IPSec - в статье.

Для **Входящих сетей** и **Анонсируемых сетей** объект **Любой** не может быть установлен одновременно с другими фильтрами.

Полезные ссылки

- Сетевые интерфейсы
- Внешние и локальные интерфейсы
- Подключение между двумя Ideco NGFW в транспортном режиме работы

OSPF

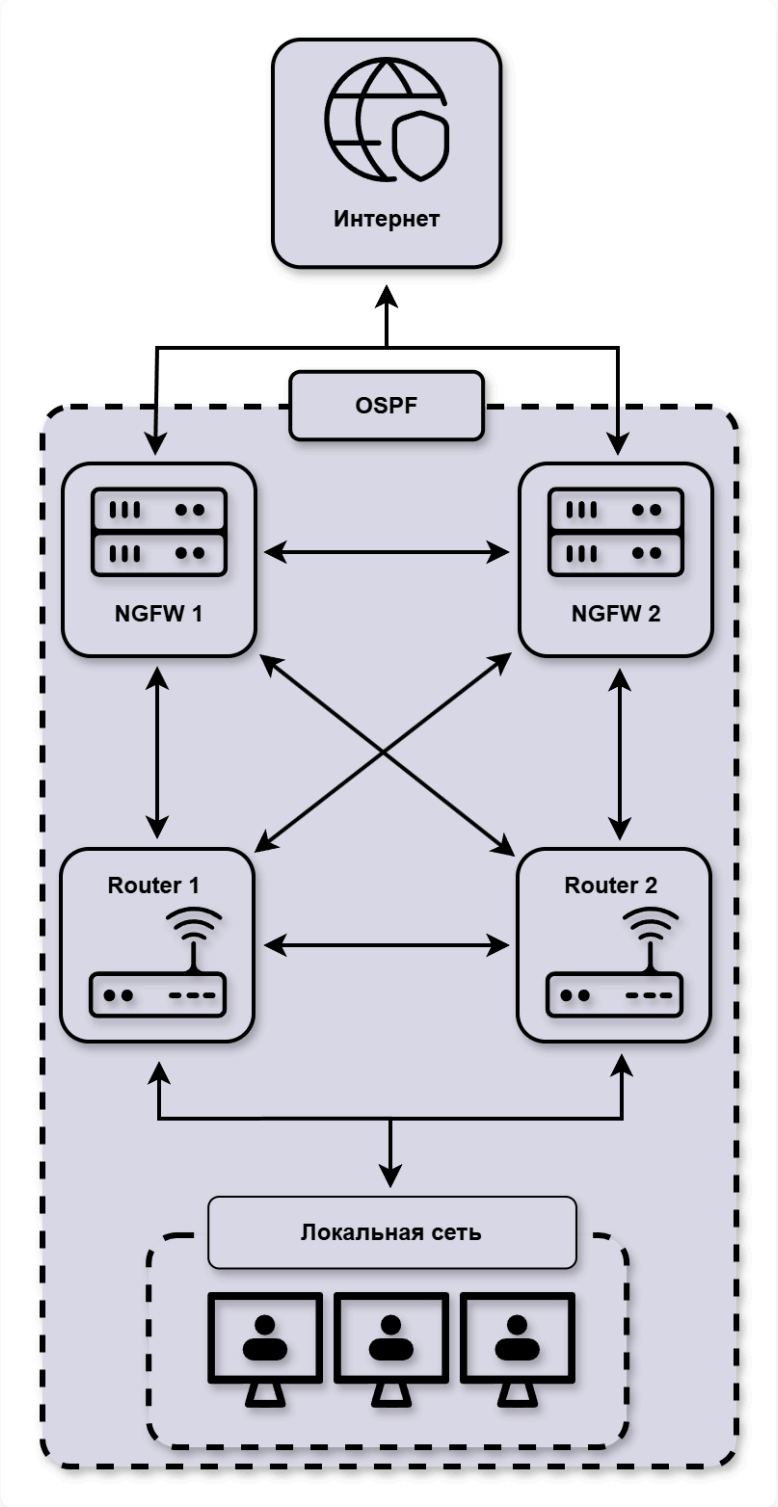
Название службы раздела **OSPF**: `frr`; `ideco-routing-backend`.

Список служб для других разделов доступен по ссылке.

Ideco NGFW 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.

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.

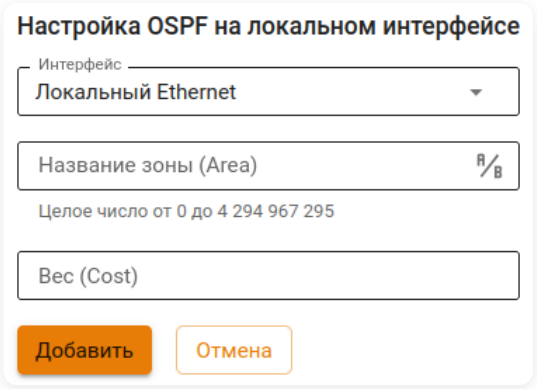
Настройка OSPF

Для настройки OSPF в Ideco NGFW перейдите в раздел **Сервисы** → **OSPF** и выполните действия на вкладках:

Основные

Router ID - IP-адрес маршрутизатора. Присваивается автоматически в виде наибольшего IP-адреса локальной сети, заданной в разделе Сетевые интерфейсы.

1. Нажмите кнопку **Добавить** и заполните поля:

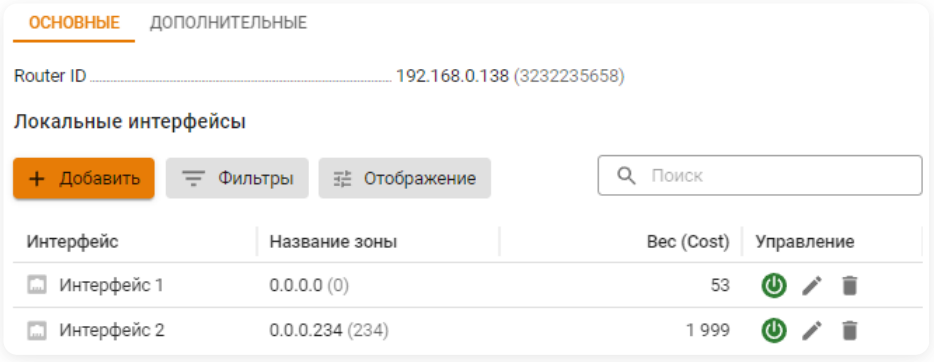


- **Интерфейс** - локальный или Loopback-интерфейс Ideco NGFW, IP-адрес которого будет использован для обмена маршрутами.
- **Название зоны** - номер зоны (значение `area`, для небольших сетей введите `0`). Можно ввести в виде числа или IP-адреса, нажав A/B.
- **Вес** - стоимость маршрута.

2. Нажмите **Добавить**.

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

Включите настройки (по умолчанию включены):

- **Redistribute default** - маршруты по умолчанию. Устройство, принявшее эту информацию, будет отправлять на NGFW весь трафик.
- **Redistribute static** - статические маршруты, указанные на вкладке **Локальных сетей** в разделе **Сервисы** → **Маршрутизация**.
- **Redistribute connected** - 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.

> Для передачи маршрутов до VPN-сети через OSPF необходимо в разделе **OSPF** → **Дополнительные** включить опцию **Redistribute static (передача статических маршрутов)**.

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**. 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 п. 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>
```

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`:

6. Для вывода таблицы маршрутизации введите команду `show ip route` (в таблице должны появиться маршруты до сетей NGFW):

Особенности работы OSPF в Ideco NGFW

- Ideco NGFW всегда будет являться шлюзом по умолчанию для других устройств. Считать другие устройства шлюзом по умолчанию NGFW не сможет.
- OSPF работает только на локальных интерфейсах: Локальные Ethernet-интерфейсы.
- Значение *Tuna cemu* (*Network Type*) в Ideco NGFW 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-1** в Филиале 1 и **NGFW-2** в Филиале 2 настраивается GRE-over-IPsec и OSPF.
- Каждый NGFW 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-1**, и **NGFW-2** используются в качестве шлюза по умолчанию.
- Между балансировщиком и каждым из NGFW настроена OSPF.

Преимущества настройки:

- Трафик балансируется между **NGFW-1** и **NGFW-2**: часть пользователей из Локальной сети выходят в интернет через **NGFW-1**, часть - через **NGFW-2**.
- При неисправности одного из NGFW трафик автоматически смаршрутизируется через другое соединение.
- Отсутствует необходимость вручную настраивать маршруты для хостов в Локальной сети.

Полезные ссылки

- Сетевые интерфейсы
- Внешние и локальные интерфейсы
- Подключение между двумя Ideco NGFW в транспортном режиме работы

IGMP Proxy

Название службы раздела **IGMP Proxy**: `ideco-igmpproxy-backend`, `ideco-igmpproxy`.

Список служб для других разделов доступен по ссылке.

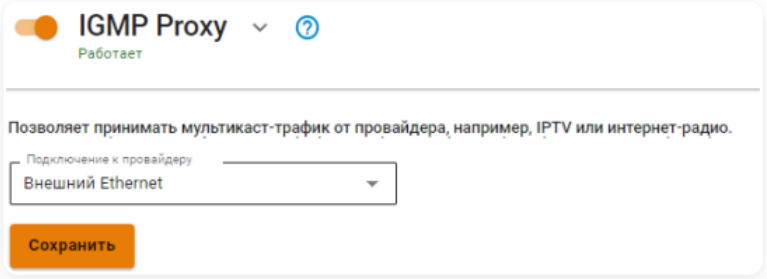
IGMP Proxy - служба, которая проксирует (передает) мультикаст-трафик сквозь роутер. Это сокращает объем трафика, что влияет на скорость работы и нагрузку сети.

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

Для настройки перейдите в раздел **Сервисы** → **IGMP Proxy**. Включите опцию **IGMP Proxy**. В строке **Подключение к провайдеру** выберите Ethernet-подключение.



Принцип работы

На примере подключения двух пользователей к мультикаст-потоку одного источника:

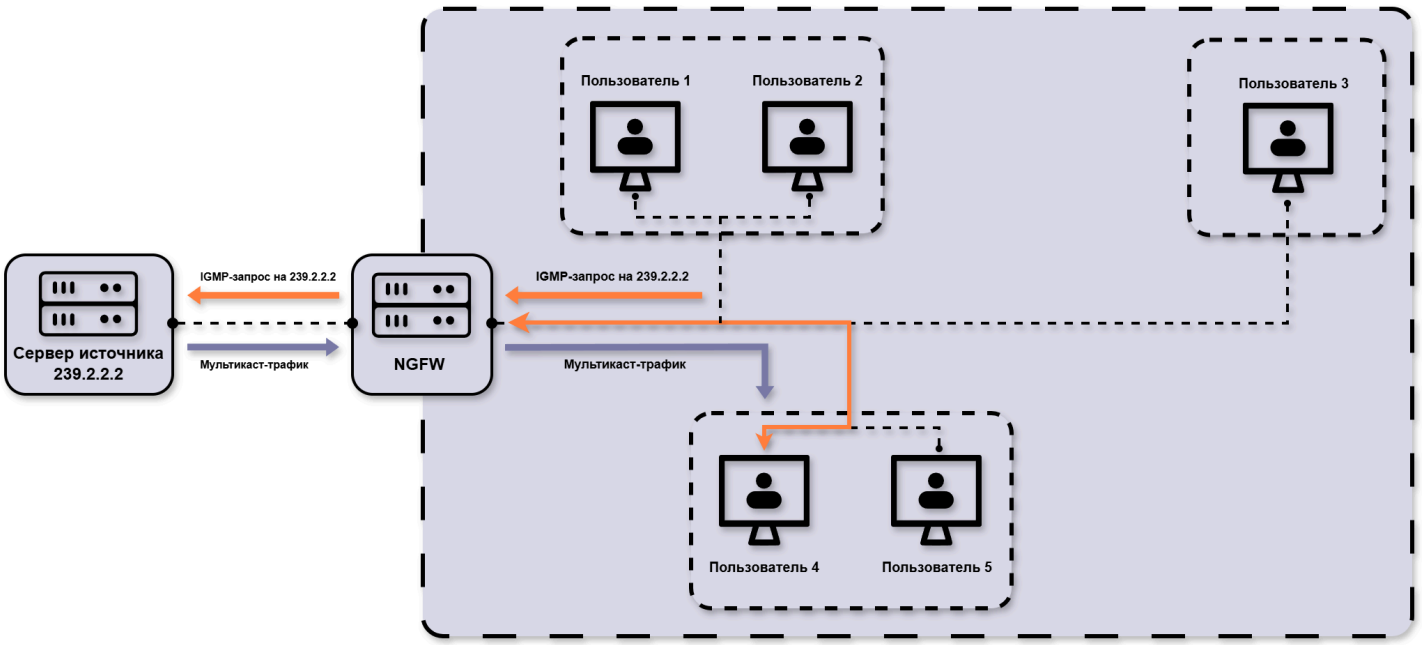
1. **Сервер источника** начинает трансляцию мультикаст-трафика с адреса из диапазона 224.0.0.0/4.

2. **Пользователь 4** хочет подключиться к трафику и генерирует IGMP-запрос (Join) на **Ideco NGFW** для получения мультикаст-трафика от сервера источника.

3. **Ideco NGFW** получает IGMP-запрос и отправляет аналогичный запрос к серверу источника.

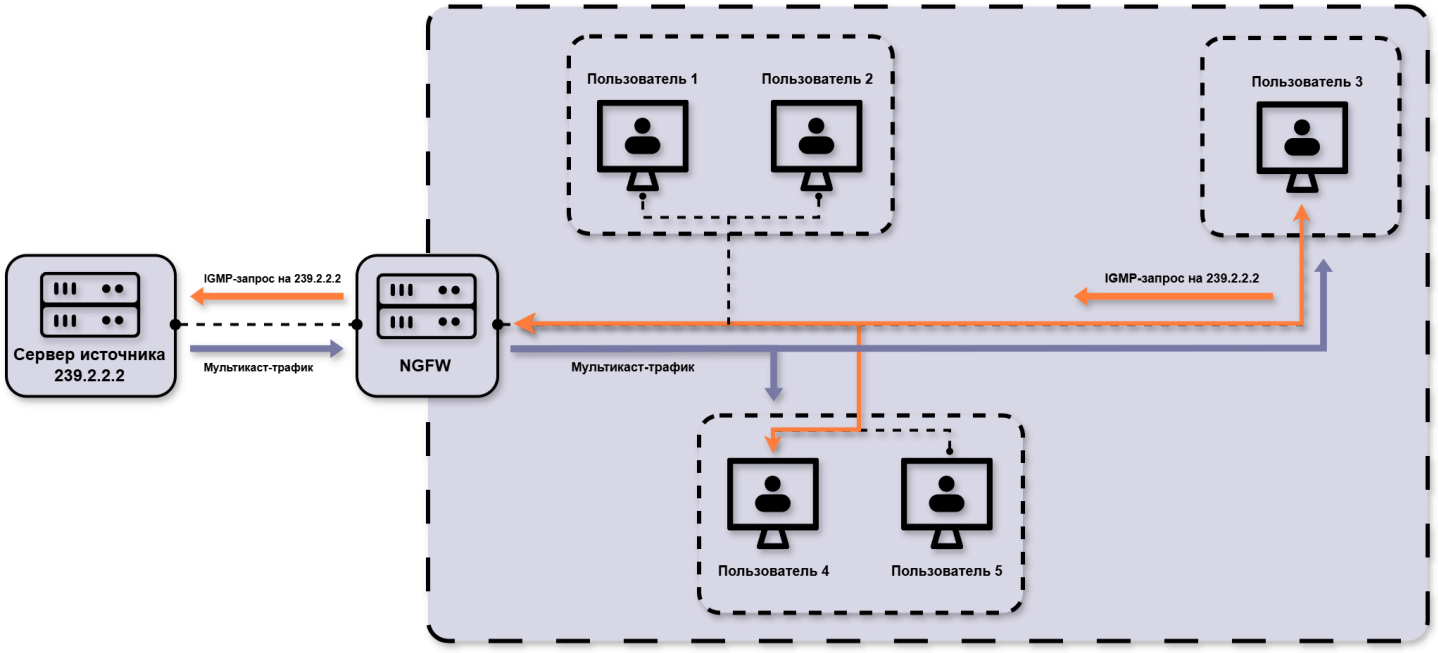
4. Сервер источника получает запрос и начинает транслировать мультикаст-трафик на **Ideco NGFW**.

5. **Ideco NGFW** пропускает трафик с адреса 239.2.2.2 в подсеть с **Пользователем 4**, и **Пользователь 4** становится его получателем:



6. **Пользователь 3**, находящийся в другой подсети, также решает подключиться к этой трансляции и генерирует IGMP-запрос (Join) на Ideco NGFW.

7. **Ideco NGFW** получает этот запрос и дублирует **Пользователю 3** трафик, поступающий **Пользователю 4**:



Ideco NGFW периодически проверяет, есть ли получатели, отправляя пользователям IGMP-запрос (Query). Пользователи в ответ отправляют Join, как при подключении.

Если на Ideco NGFW приходит хотя бы один Join, то мультикаст-трафик продолжает транслироваться получателям.

Прокси

Название службы раздела **Прокси**: `ideco-proxy-backend`, `squid`.

Список служб для других разделов доступен по ссылке.

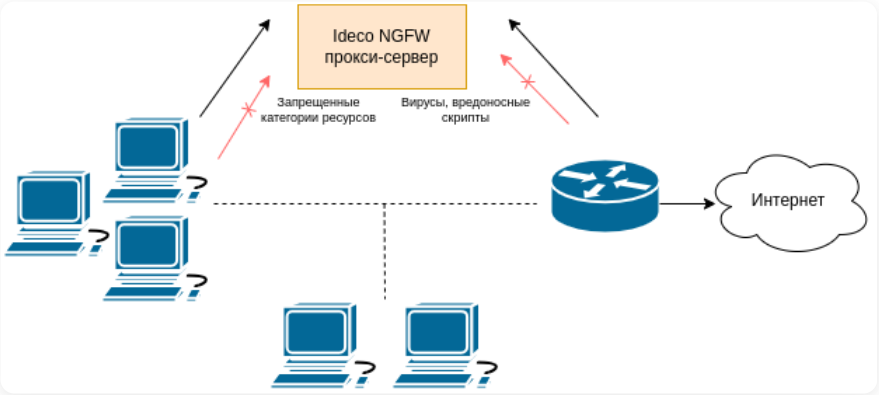
Прокси-сервер используется не только для проксирования веб-трафика, но и для передачи трафика сервисам:

- 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 в качестве шлюза по умолчанию для устройств в сети.

Для настройки фильтрации HTTPS-трафика нужно добавить корневой сертификат NGFW на компьютеры пользователей. Подробнее в статье Настройка фильтрации HTTPS.



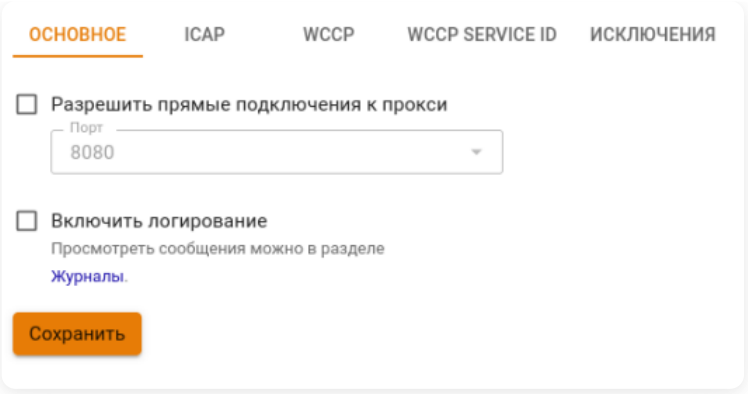
При использовании Ideco NGFW в качестве прокси-сервера с прямыми подключениями к прокси большинство функций будет работать с некоторыми особенностями:

- В правилах **Файрвола** для пользователей необходимо указывать цепочки INPUT вместо FORWARD.
- Глубокий анализ трафика системой предотвращения вторжений и модулем контроля 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.

Основное

На вкладке **Основное** предоставлены возможности:

- **Разрешить прямые подключения к прокси** - применяется, когда Ideco NGFW не является шлюзом по умолчанию для клиентов сети. Порт, указанный на стороне NGFW, следует указать на сетевых устройствах локальной сети, веб-трафик которых нужно пропускать через прокси.
- **Включить журналирование** - применяется для записи логов **Контент-фильтра** и **Антивируса**.



О настройке прямого подключения к прокси и прокси с одним интерфейсом читайте в статье.

ICAP

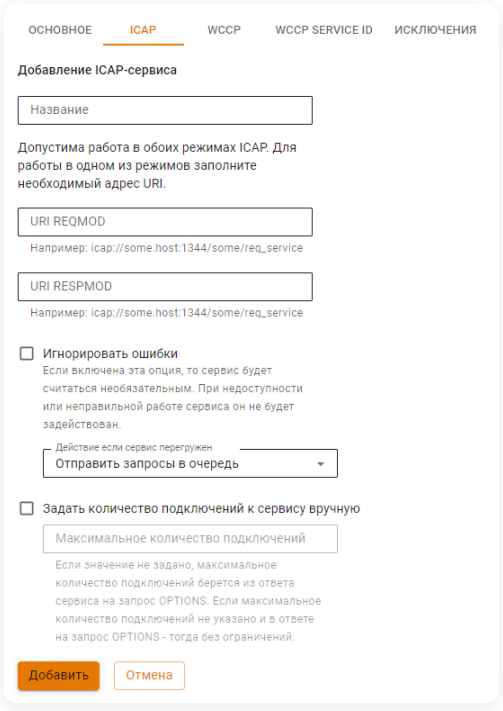
Протокол ICAP позволяет отправлять HTTP(S)-трафик в расшифрованном виде на сторонние серверы. ICAP-сервисы обрабатывают трафик после работы Антивируса и Контент-фильтра Ideco NGFW, блокируя запросы в соответствии с установленными политиками сервиса.

Если трафик попадает под любое запрещающее правило Ideco NGFW или ICAP-сервиса, трафик будет заблокирован.

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.
- **Игнорировать ошибки** - если включена эта опция, то сервис будет считаться необязательным. При недоступности или неправильной работе сервис не будет задействован.
- **Действие если сервис перегружен** - опция позволяет выбрать сценарий действий при перегруженности ICAP-сервиса.
- **Задать количество подключений к сервису вручную** - 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 **Задать количество подключений к сервису вручную** значение меньше четырех, то клиентские подключения могут быть нестабильными.



Для корректной работы ICAP-сервиса должна быть настроена расшифровка HTTPS-трафика в **Контент-фильтре**.

WCCP

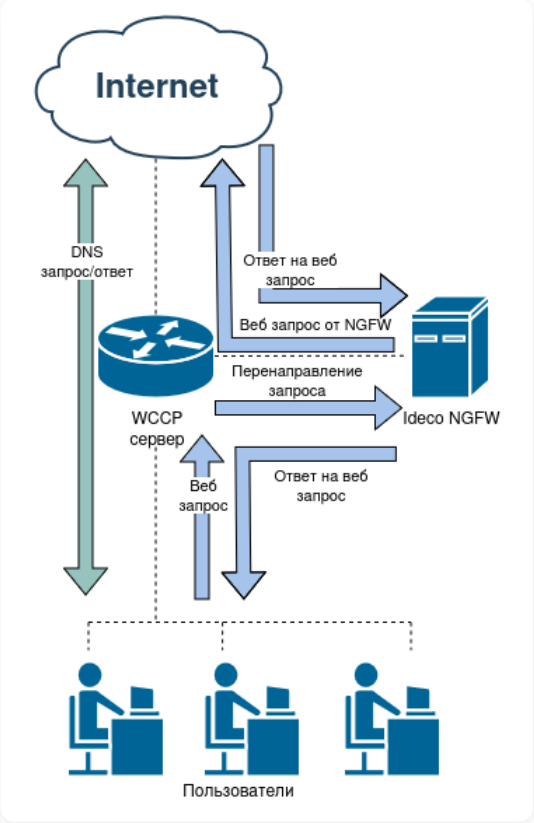
Протокол WCCP используется для перенаправления трафика на Ideco NGFW. По умолчанию перенаправляется только HTTP/HTTPS-трафик.

Для активации WCCP включите опцию **Включить перенаправление трафика с WCCP-серверов на Ideco NGFW**. Ideco NGFW запустит процесс согласования параметров с WCCP-сервером.

В NGFW предусмотрено два режима работы WCCP - L2 и GRE:

L2

Режим L2 используется, если WCCP-сервер и Ideco NGFW находятся в одном сетевом сегменте:



Последовательность обработки веб-запросов на уровне L2:

1. Пользователь отправляет веб-запрос.

2. Запрос перенаправляется сервером на Ideco NGFW.

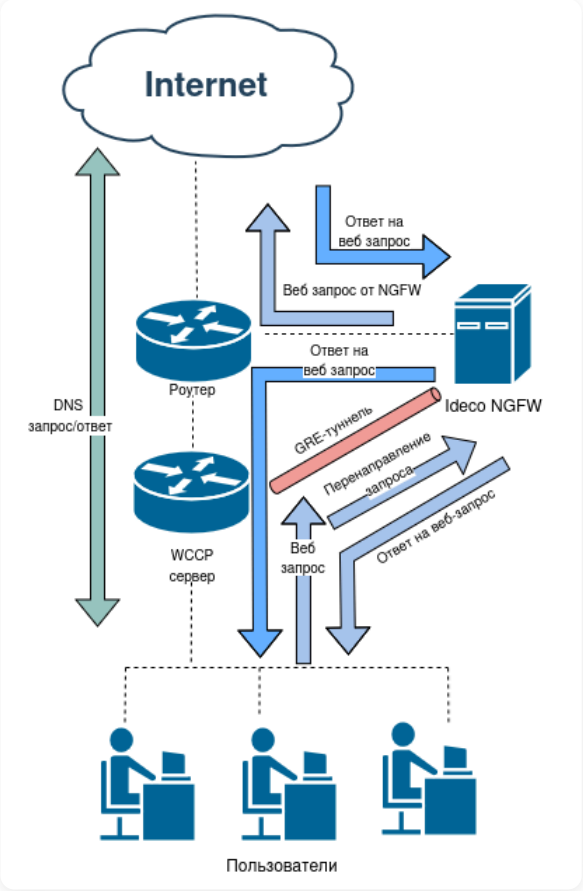
3. Ideco NGFW обрабатывает запрос:

- Если запрос заблокирован, информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается обратно по тому же пути, по которому уходил на внешний сервер.

GRE

Режим GRE используется, если WCCP-сервер и Ideco NGFW находятся в разных сетевых сегментах:



Последовательность обработки веб-запросов на уровне GRE:

1. Пользователь отправляет веб-запрос.

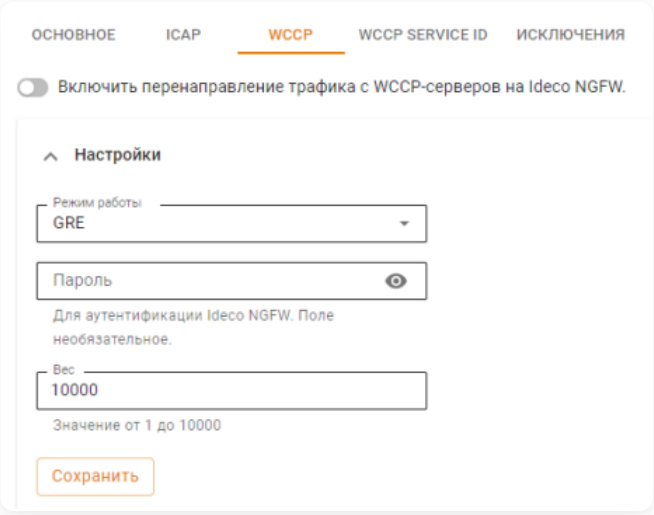
2. Запрос перенаправляется по GRE-туннелю на Ideco NGFW.

3. Ideco NGFW обрабатывает запрос:

- Если запрос заблокирован, то информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

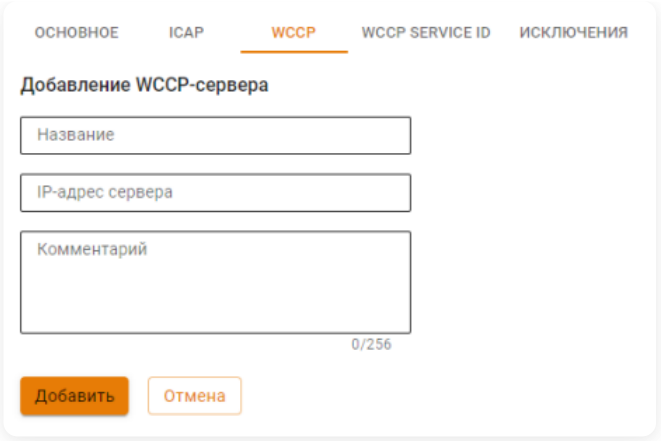
Ответ возвращается напрямую от Ideco NGFW пользователю, минуя GRE-туннель.
Для выбора режима раскройте блок **Настройки**.

Если на WCCP-сервере задан пароль, сохраните его в соответствующем поле:



Если WCCP использует несколько Ideco NGFW, настройте распределение трафика с помощью указания приоритета в поле **Вес**. Допустимые значения - от 1 до 10000.

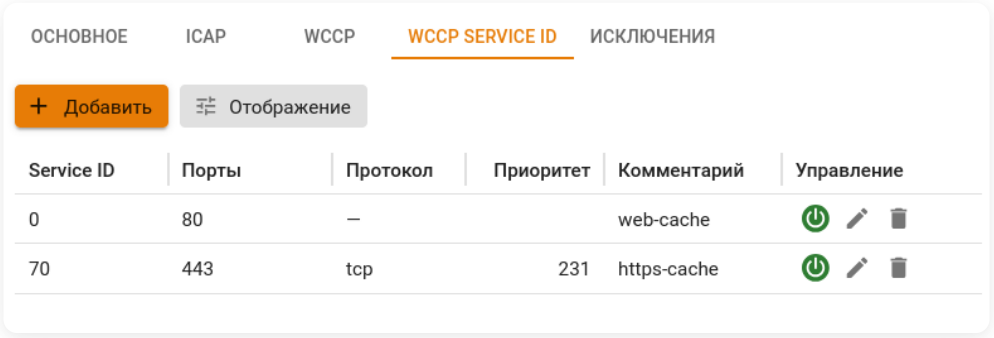
Для добавления WCCP-сервера нажмите кнопку **Добавить** и укажите IP-адрес сервера:



WCCP Service ID

Service ID - идентификаторы сервисной группы. Настройки на этой вкладке позволяют выбрать службы, трафик которых сервер WCCP будет перенаправлять на Ideco NGFW.

По умолчанию настроены сервисы для HTTP/HTTPS-трафика:

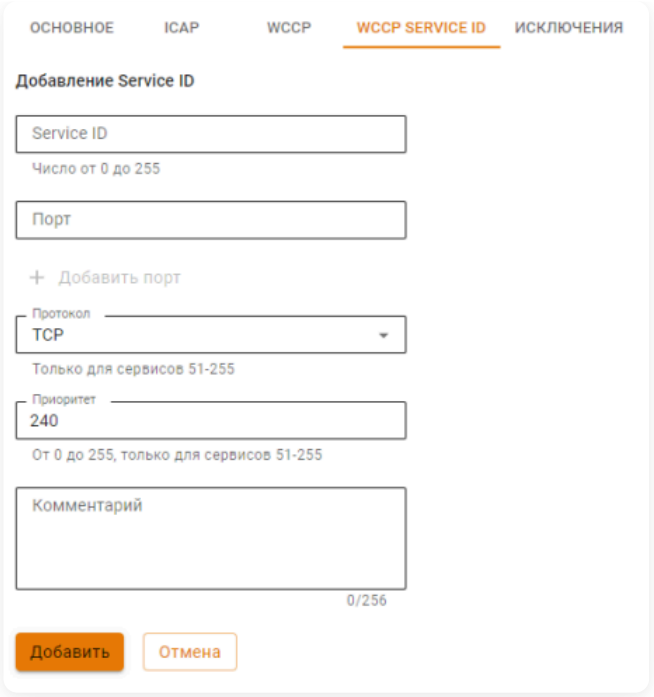


> Service ID с 0 по 50 зарезервированы под фиксированные сервисы. Для них выбирать порты и протоколы нельзя.
>
> Service ID 70 - общепринятое значение для HTTPS-трафика на 443 TCP-порт.

Чтобы настроить Service ID, выполните действия:

1. На вкладке **WCCP Service ID** нажмите кнопку **Добавить**.

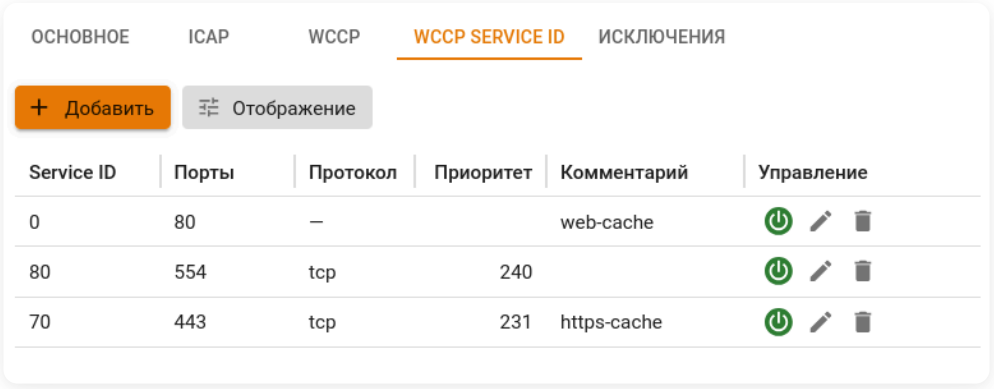
2. В открывшейся форме укажите следующие значения:



- **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 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.

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.

На вкладке **Исключения** можно исключить ресурсы из обработки прокси-сервером и всеми связанными службами (контент-фильтр, веб-отчетность, антивирусы):

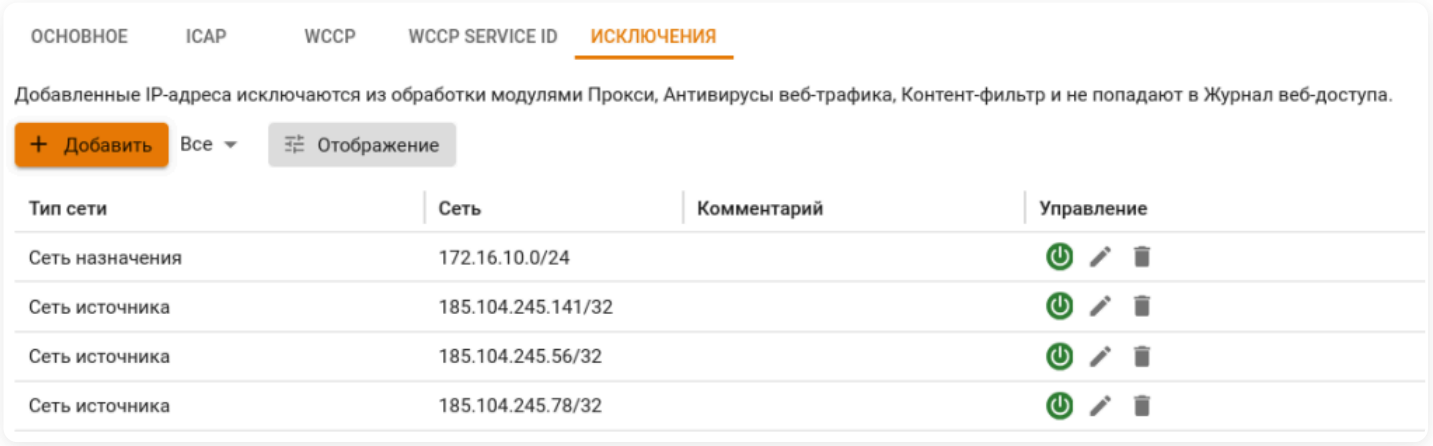
- **Сети источника** - указываются сети, трафик из которых исключается из обработки прокси-сервером;
- **Сети назначения** - указываются внешние сети или IP-адреса (как правило, адреса веб-сайтов или веб-сервисов), трафик до которых из всех локальных сетей NGFW исключается из обработки прокси-сервером.

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).

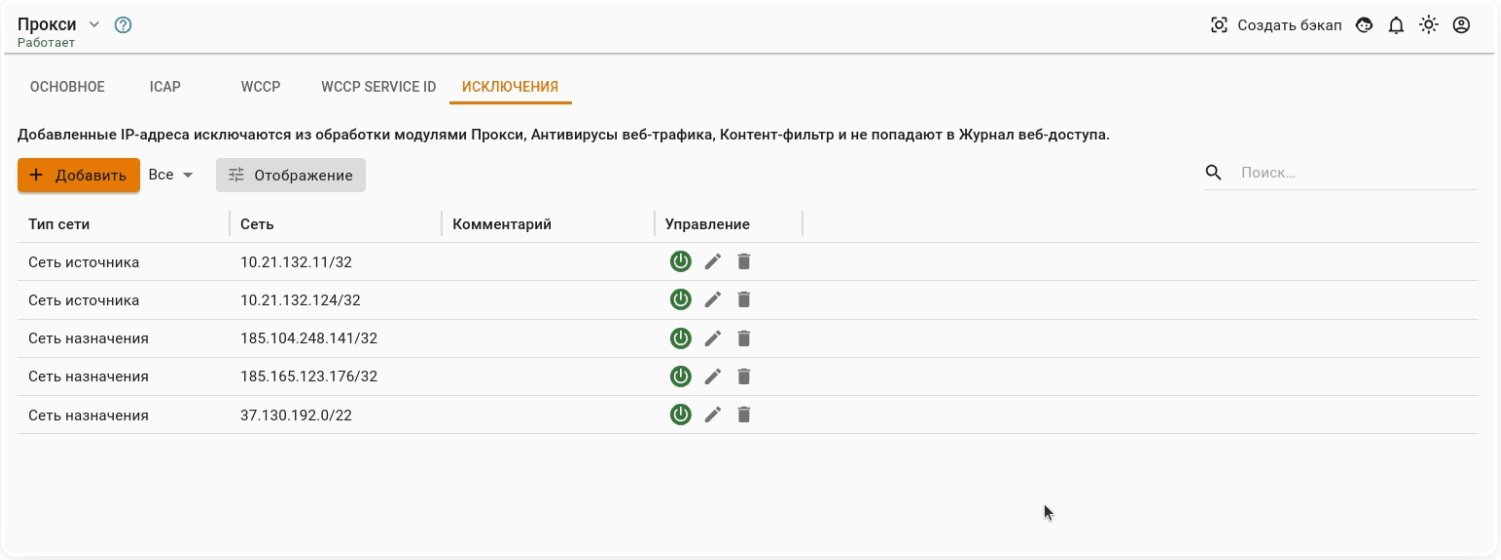
При создании исключений можно указывать только IP-адреса или IP-сети.

Трафик, исключенный из обработки прокси, не будет участвовать в **Отчетах**, проверяться на вирусы и обрабатываться модулем **Контент-фильтра**. В то же время такой трафик будет проверен **Файрволом**, модулями **Предотвращение вторжений** и **Контроль приложений**.



Поиск по таблице исключений

Над таблицей исключений расположена строка поиска. Она позволяет 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

- 194.54.15.90/32
- 194.186.207.124/32
- 194.186.207.182/32
- 195.8.62.178/32
- 194.54.15.90/32
- 10.21.132.124/32
- 92.38.2.37/24

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.

Настройка прямого подключения к прокси

Для настройки выполните действия:

1. Укажите IP-адрес локального интерфейса Ideco NGFW в качестве веб-прокси в локальной сети на клиентских устройствах.

2. В настройках прокси на Ideco NGFW укажите порт для прямых подключений к прокси (возможен выбор портов из списка: 3128, 1080, 8000, 8080, 8888, 8081, 8088, 10080).

В таком режиме NGFW сможет предоставлять клиентским устройствам веб-трафик по другим портам (по умолчанию - по всем, при необходимости можно закрыть порты Файрволом).

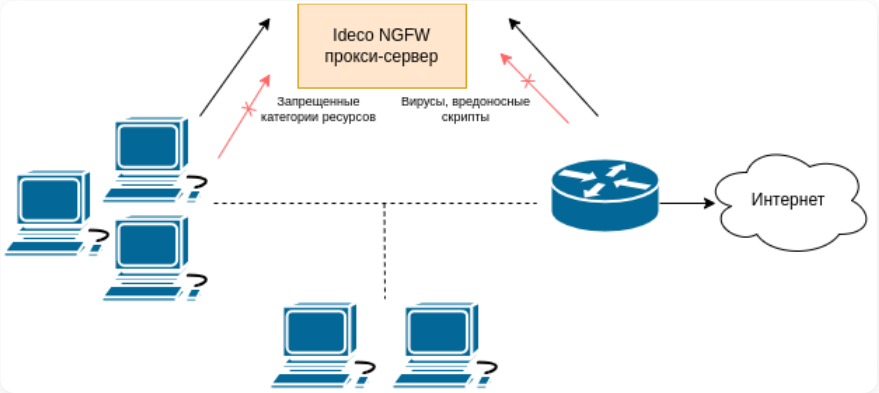
Если прямое подключение к прокси требуется только части клиентских устройств или части локальных интерфейсов, то создайте INPUT-правило **Файрвола**. Пример приведен ниже.

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 **Файрвола**.

Для учета, контроля и проверки веб-трафика на вирусы, требуется соблюдение следующих условий:

- Локальная подсеть не пересекается с внешним интерфейсом NGFW.
- У сервера Ideco NGFW есть доступ в интернет.
- На клиентских устройствах указан адрес веб-прокси (в настройках прокси-сервера в браузерах).



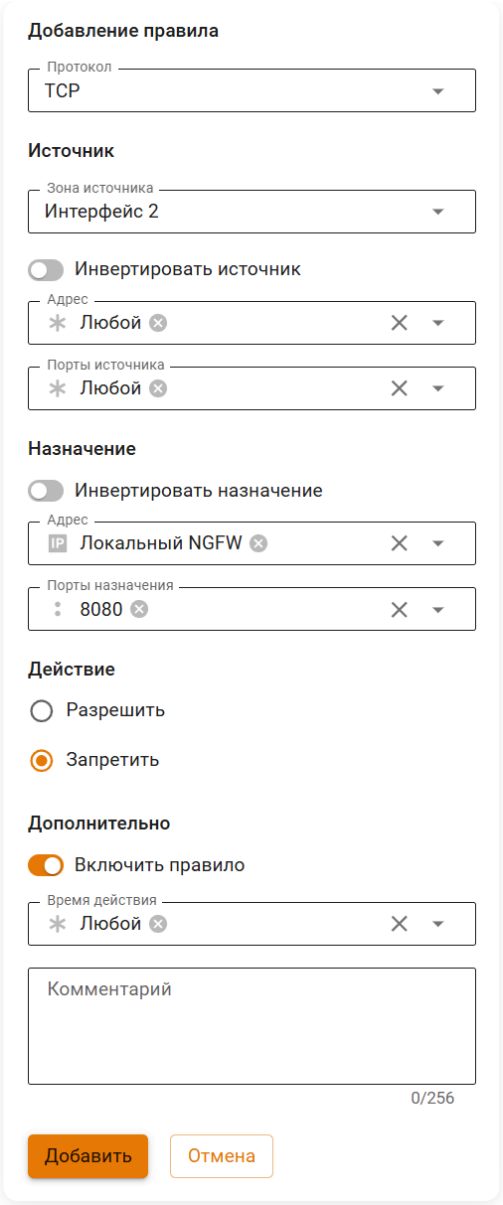
Если в настройках программы под ОС Windows или MacOS X нет возможности указать прокси-сервер, воспользуйтесь сторонним ПО для маршрутизации всего трафика рабочей станции на прокси-сервер. Такую возможность предоставляет программа **Proxifier**, которую можно настроить для прямых подключений к прокси, воспользовавшись статьей.

Пример настройки INPUT-правила

1. Перейдите в **Правила трафика** → **Файрвол** → **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:

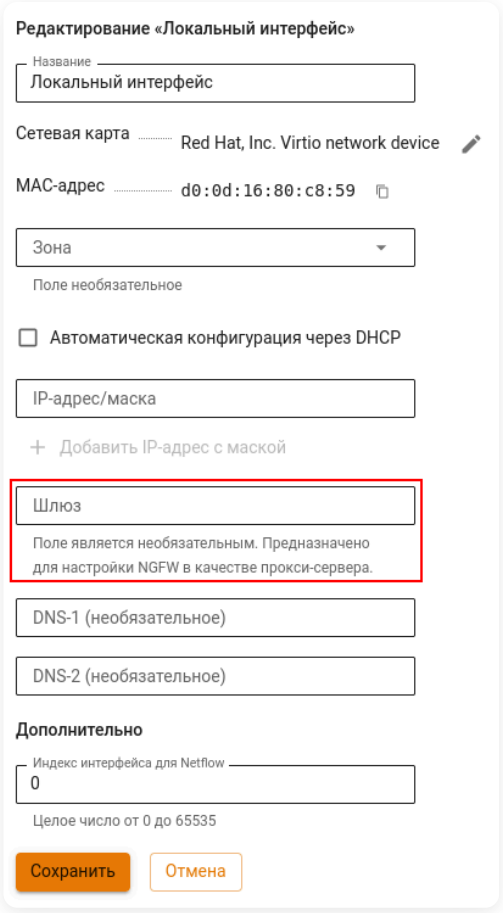


- **Протокол** - TCP.
- **Источник**:
  - **Зона источника** - локальный интерфейс или конкретные интерфейсы.
  - **Адрес** - **Любой**. Доступ будет запрещен всем, кроме адресов в разрешающем правиле.
- **Назначение**:
  - **Адрес** - IP-адрес локального интерфейса NGFW.
  - **Порт назначения** - порт, указанный в настройках **Прокси**.
- **Действия** - **Запретить**.

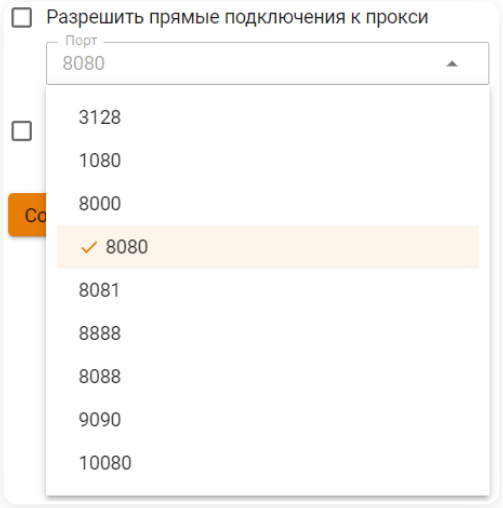
Настройка прокси с одним интерфейсом

При необходимости можно использовать Ideco NGFW в качестве прокси-сервера с прямыми подключениями клиентов к прокси, с одним интерфейсом. Для этого выполните действия:

1. При создании локального интерфейса в разделе **Сервисы** → **Сетевые интерфейсы** укажите **Шлюз**:



2. Разрешите прямые подключения к прокси-серверу в разделе **Сервисы** → **Прокси**, выбрав нужный порт из списка:



Обратный прокси

Название службы раздела **Обратный прокси**: `ideco-reverse-backend`.

Список служб для других разделов доступен по ссылке.

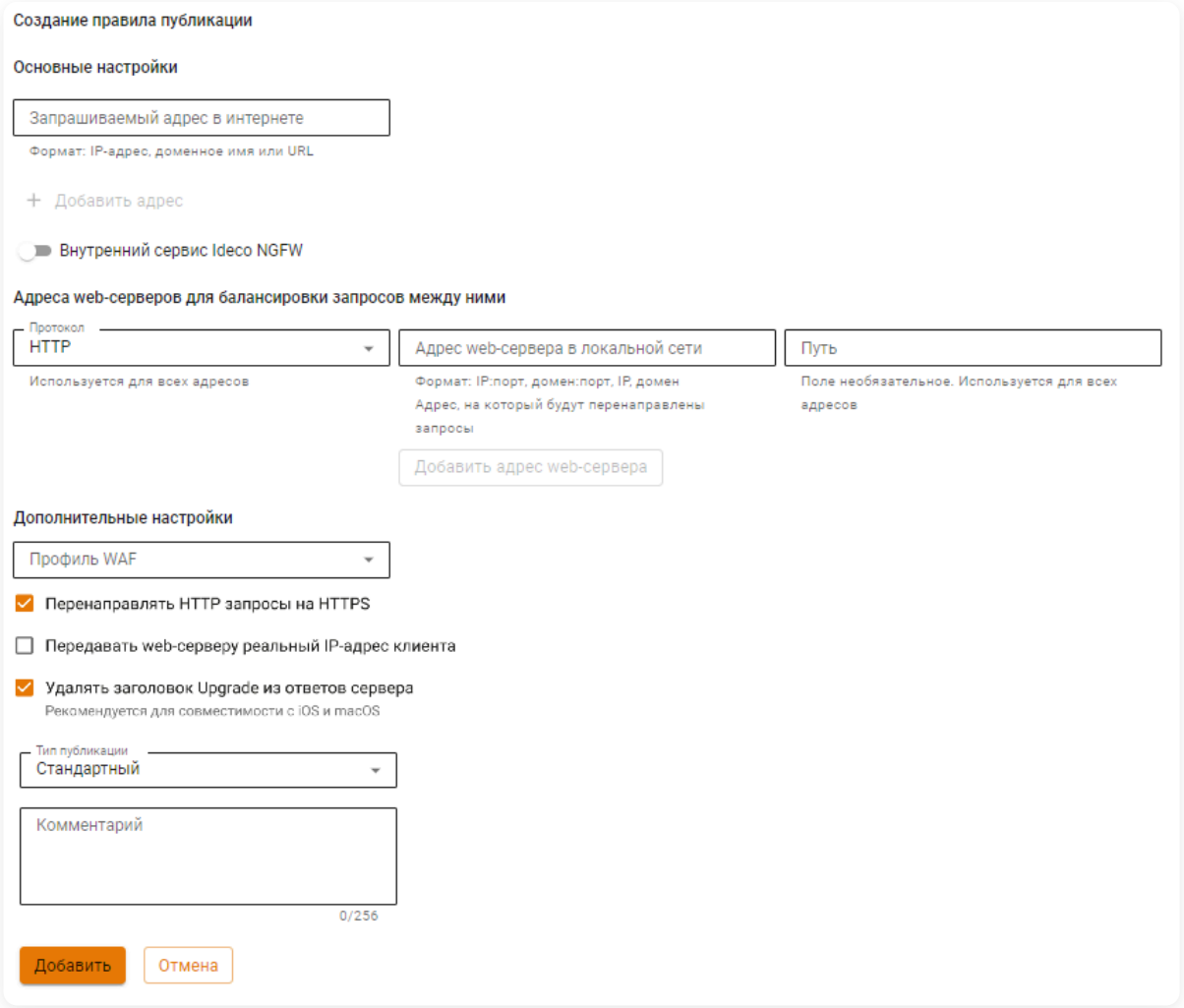
Технология обратного прокси позволяет проксировать веб-трафик из сети интернет в локальную сеть. Отличается от DNAT тем, что работает на более высоком уровне (прикладной протокол HTTP вместо сетевого протокола IP) и позволяет более гибко реализовать публикацию ресурсов.

Обратный прокси позволяет смаршрутизировать запрос на HTTP-сервер в локальной сети из внешней сети. Таким образом, имея одну ресурсную A-запись для внешнего сетевого интерфейса NGFW, можно опубликовать несколько ресурсов в локальной сети, распределив их по нескольким входящим URL.

Создание и настройка правила

Настройка сертификатов для публикуемых ресурсов не требует их ручной загрузки. Ideco NGFW сам отправляет запрос на выпуск сертификата Let's Encrypt. Выпуск сертификата может занять до 20 минут. Выпущенные сертификаты будут доступны в разделе Сертификаты.

Для создания правила перейдите в раздел **Сервисы** → **Обратный прокси** и нажмите на кнопку **Добавить**. Форма добавления правила разделена на три подраздела: **Основные настройки**, **Адреса web-серверов для балансировки запросов между ними** и **Дополнительные настройки**.



Основные настройки

- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных 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** - включите опцию и выберите для публикации один из сервисов Ideco NGFW: Личный кабинет/Портал SSL VPN.

Адреса web-серверов для балансировки запросов между ними

- **Протокол** - выбранный протокол используется для всех адресов в правиле.
- **Адрес web-сервера в локальной сети** - адрес, на который будут перенаправлены запросы.
- **Путь** - поле необязательное и используется для всех адресов.

Если указать в поле **Запрашиваемый адрес в интернете** *0.0.0.0*, перенаправление будет работать со всех внешних IP-адресов Ideco NGFW на адрес из поля **Адрес web-сервера в локальной сети**.

Чтобы перенаправление работало с доменов Ideco NGFW на адрес из поля **Адрес web-сервера в локальной сети**, необходимо явно указать домены в поле **Запрашиваемый адрес в интернете**.

Дополнительные настройки

- **Профиль WAF** - позволяет задать параметры защиты веб-ресурса при указании WAF-профиля.
- **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. 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 (в частности, типы атак, входящие в OWASP TOP-10). При активации этого модуля также будут блокироваться злоумышленники, ведущие сканирование сайта на уязвимости, с помощью модуля защиты от brute force атак.

Не рекомендуем использовать проброс веб-интерфейса NGFW через WAF, так как при попытке входа пользователь может быть заблокирован средствами WAF.

- **Удалять заголовок Upgrade из ответов сервера** - включите опцию, если сайт недоступен на устройствах Apple. Опция уберет запрещенный стандартом `RFC 7540` заголовок `Upgrade` из ответов `HTTP/2`, предотвращая разрыв соединения.
- Поле **Тип публикации** позволяет выбрать один из типов: **Стандартный** и **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 резолвиться во внешний IP-адрес сервера NGFW. Доменные имена, указываемые в поле **Адрес в локальной сети**, должны резолвиться в IP-адреса публикуемых ресурсов самим сервером NGFW.

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 NGFW 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 NGFW.
- На локальном сервере, в админ-панели WordPress должен быть настроен домен `wordpress.mydomain.ru` на стандартном порту HTTP.
- Добавить в обратный прокси правило публикации `wordpress.mydomain.ru` -> `wordpress.mydomain.ru`.

Защита от DoS-атак

Включение опции **Защита от DoS-атак** ограничивает трафик, если:

- скорость - более 200 запросов в секунду с одного IP-адреса.
- количество подключений с одного IP-адреса - более 1000.
- размер запроса - более 50 Мб.
- время ожидания на чтение заголовка и тела запроса - более 5 секунд.



Чтобы исключить IP-адрес из обработки **Защитой от DoS-атак**, обратитесь в Техническую поддержку.

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;
}
```

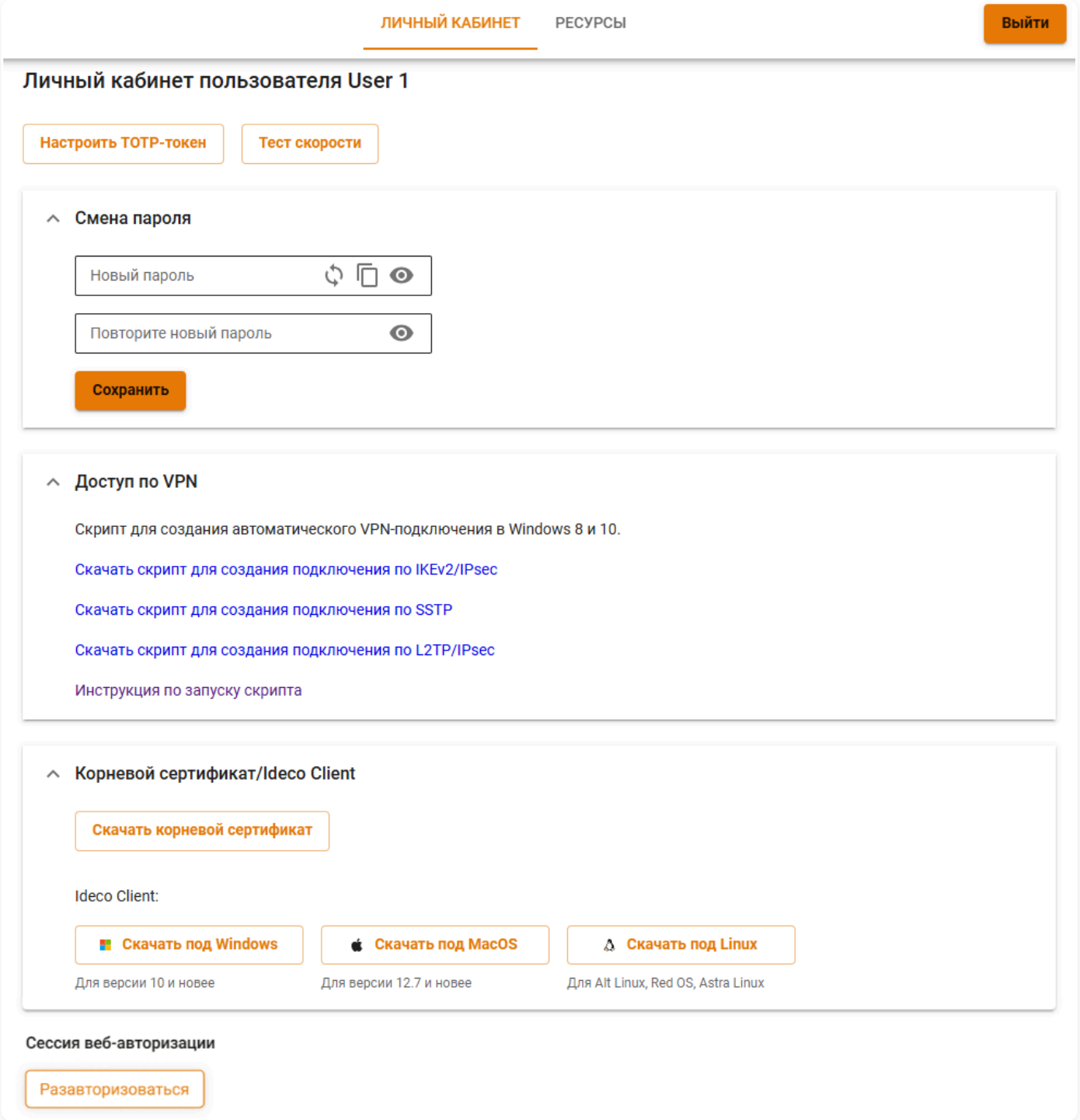
При использовании NGINX Proxy Manager добавьте в **Custom Nginx Configuration** → **Advanced Settings** запись `proxy_hide_header Upgrade;`, иначе мобильные устройства от Apple будут получать сообщение об ошибке **Connection Closed**.

ЛК/Портал SSL VPN

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:

- **Генерация TOTP-токена**. Для настройки двухфакторной аутентификации воспользуйтесь статьей.
- **Тестирование скорости**. При нажатии на Тест скорости в веб-интерфейсе личного кабинета откроется меню тестирования скорости между хостом и NGFW.
- **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 корневого сертификата**.
- **Скачивание Ideco Client**. Подробнее о работе в Ideco Client - в статье.
- **Разавторизация**. Завершение сессии пользователя в сети NGFW, если он был авторизован через Web/SSO.



Поддерживаемые версии браузеров:

- Google Chrome версия 76 и выше
- Firefox версия 71 и выше
- Safari версия 13 и выше

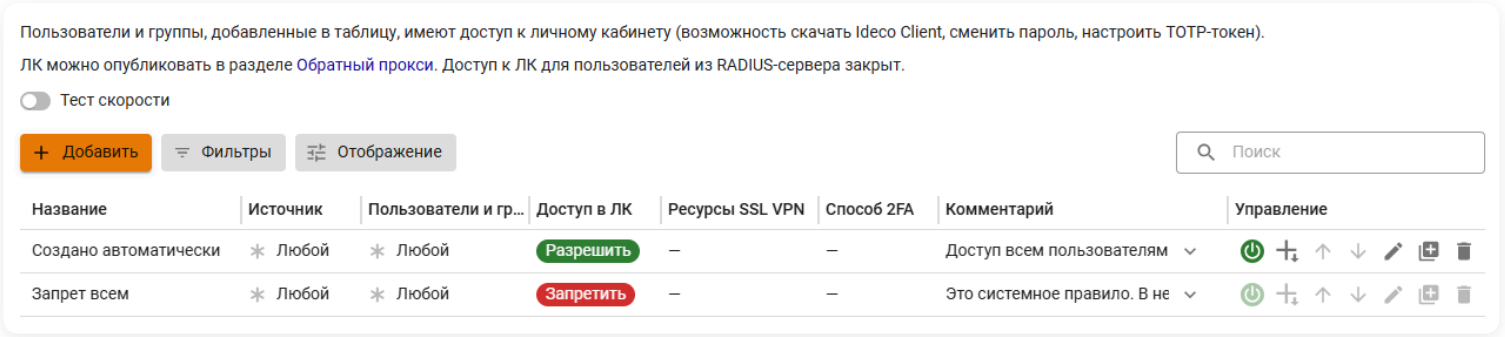
Настроить доступ пользователей в личный кабинет можно на вкладке **Сервисы** → **ЛК/Портал SSL VPN** → **Правила доступа**. Для этого необходимо создать **Правило доступа**, а затем опубликовать личный кабинет через **Обратный прокси**, чтобы пользователи получили к нему доступ. VPN-подключение не требуется, пользователь авторизуется через логин и пароль.

Настройка доступа в личный кабинет Ideco NGFW

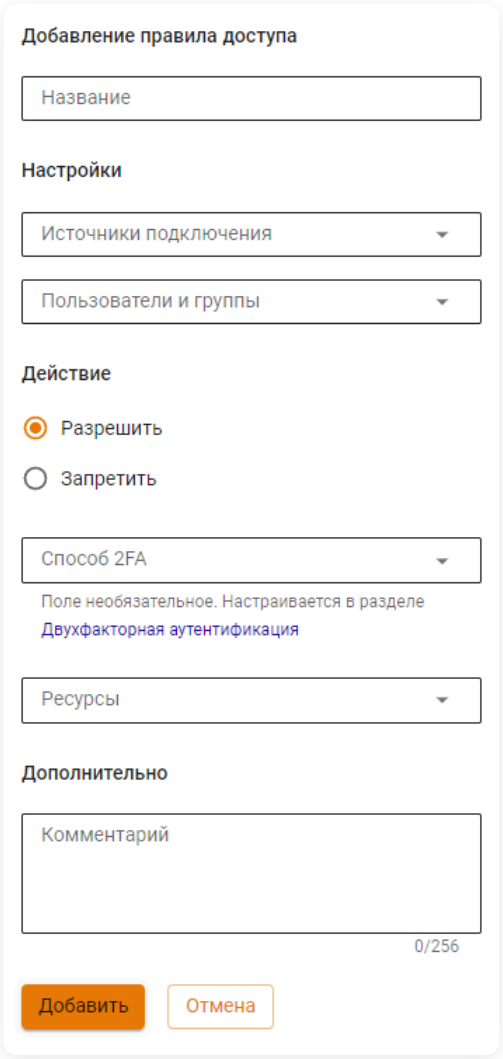
В разделе **Сервисы** → **ЛК/Портал SSL VPN** можно настроить доступ в личный кабинет.

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.

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**.

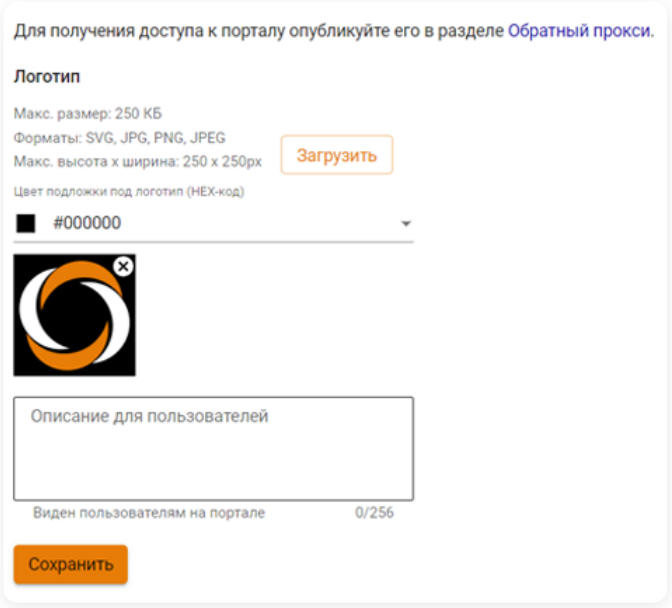
2. Если правило разрешающее, то доступные пользователю в ЛК ресурсы определяются этим правилом. Последующие правила с такими же полями учитываться не будут.

3. Доступ пользователя или группы пользователей к ресурсу определяется заново при изменении таблицы, пользователей и состава групп.

Опция **Тест скорости** позволяет добавить в личный кабинет функцию проверки скорости интернет-соединения.

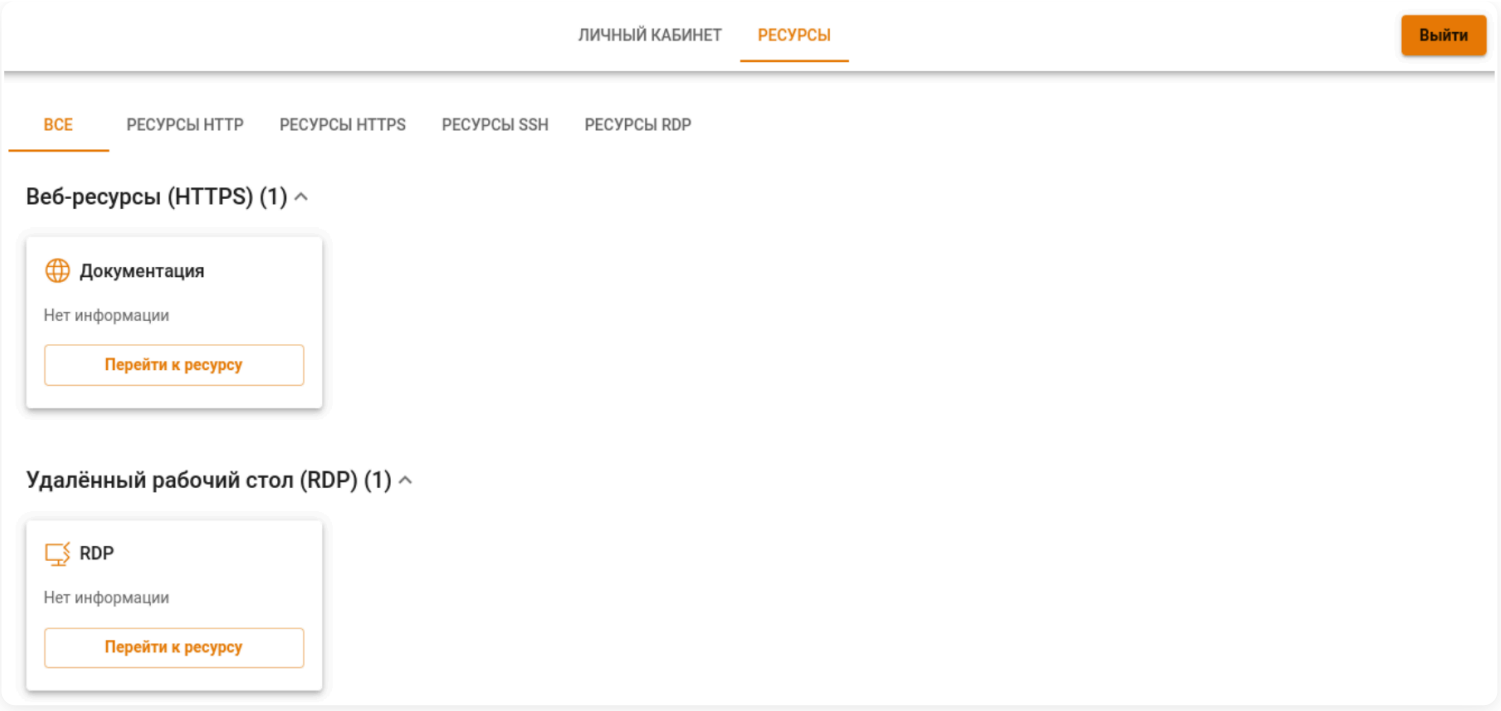
Внешний вид

На вкладке можно настроить внешний вид портала: изменить логотип и добавить описание, которое отображается рядом с логотипом:



Ресурсы

В личном кабинете Ideco NGFW размещаются только внутренние ресурсы, доступные из локальной сети NGFW. Ресурсы становятся доступны пользователям только после успешной авторизации и при наличии соответствующего разрешения в правилах доступа:

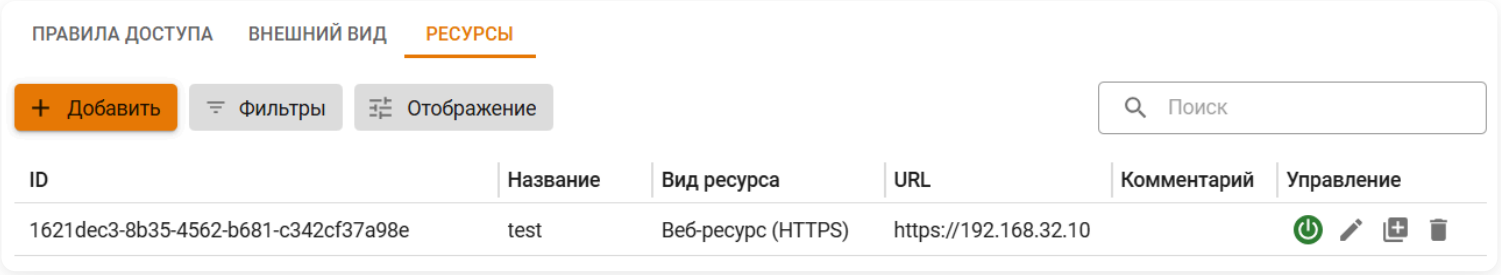


Веб-ресурсы HTTP(S) в SSL VPN работают по принципу **Обратного прокси** ЛК/SSL VPN.

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.
- 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**:

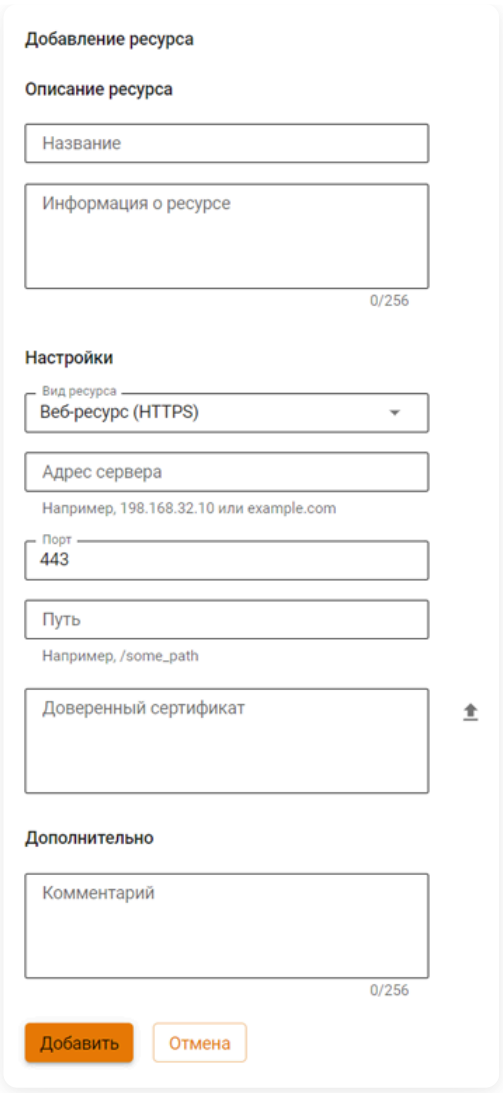


В случае несоответствия URL перечисленным требованиям публикуемый ресурс будет отображаться некорректно, т.к. браузер пользователя не сможет получить некоторые данные с этих URL (например, файлы CSS и JS).

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.

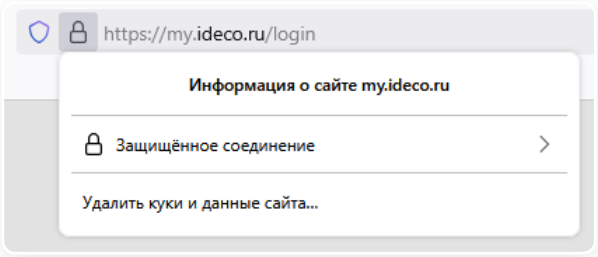
Настройки:

- **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.

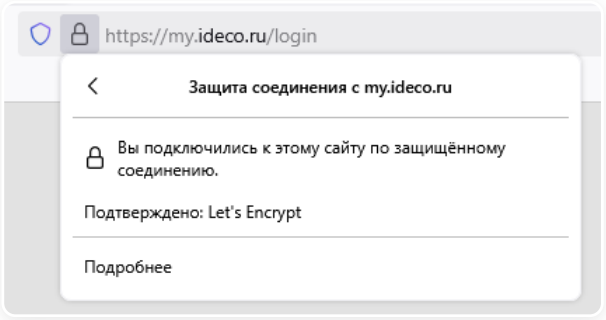
Где скачать доверенный сертификат

Пример скачивания сертификата в браузере Firefox:

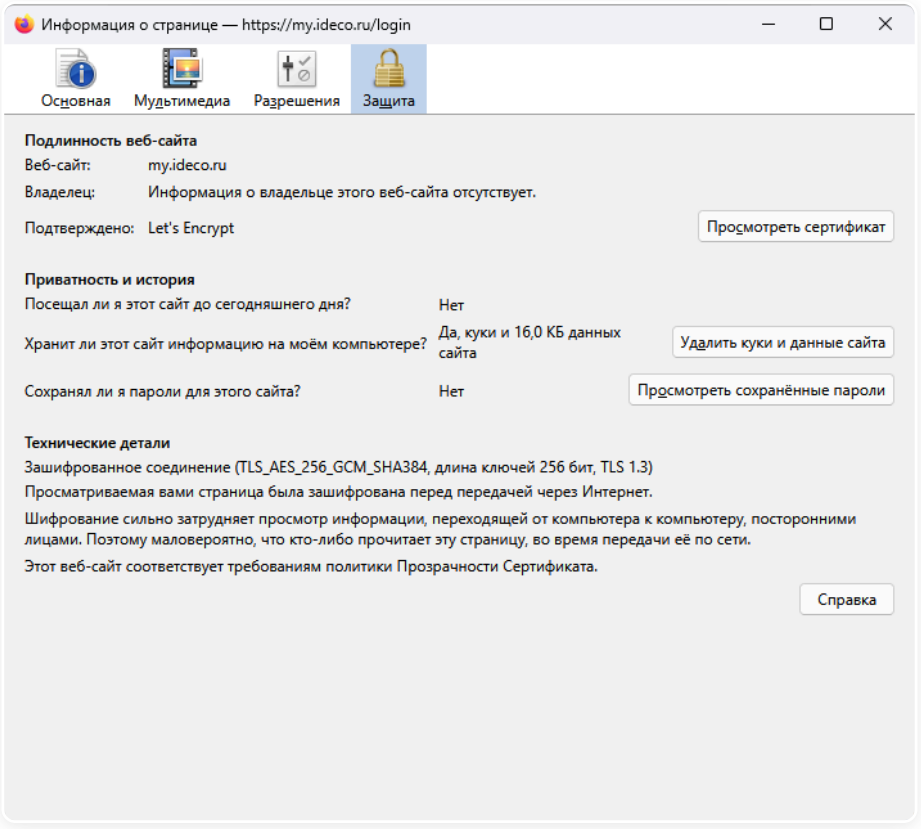
1. Нажмите в адресной строке браузера на значок с замком и выберите **Защищенное соединение**:



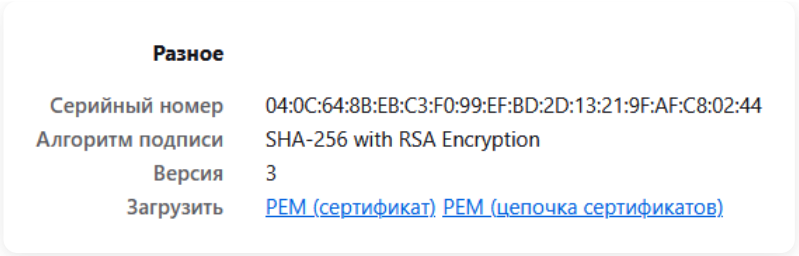
2. Нажмите **Подробнее**:



3. На вкладке **Защита** нажмите **Просмотреть сертификат**:



4. В разделе **Разное** скачайте сертификат из строки **Загрузить**:



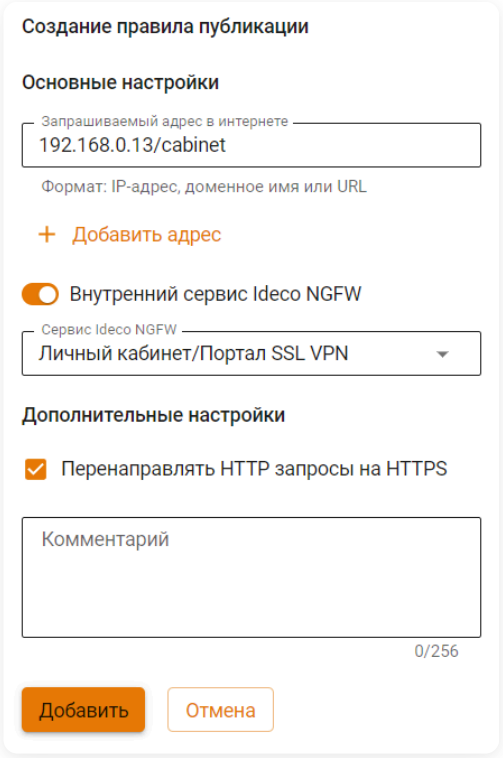
Адреса, на которые ссылается HTTP/HTTPS-ресурс, должны быть относительными во избежание нарушения CORS. Подробнее про CORS.

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**.

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**.

После этого пользователь сможет зайти в личный кабинет по логину и паролю либо через авторизацию в сети NGFW.

Вход в личный кабинет Ideco NGFW

Личный кабинет пользователя будет доступен по ссылке, указанной при публикации через **Обратный прокси**.

Чтобы зайти в личный кабинет, выполните действия:

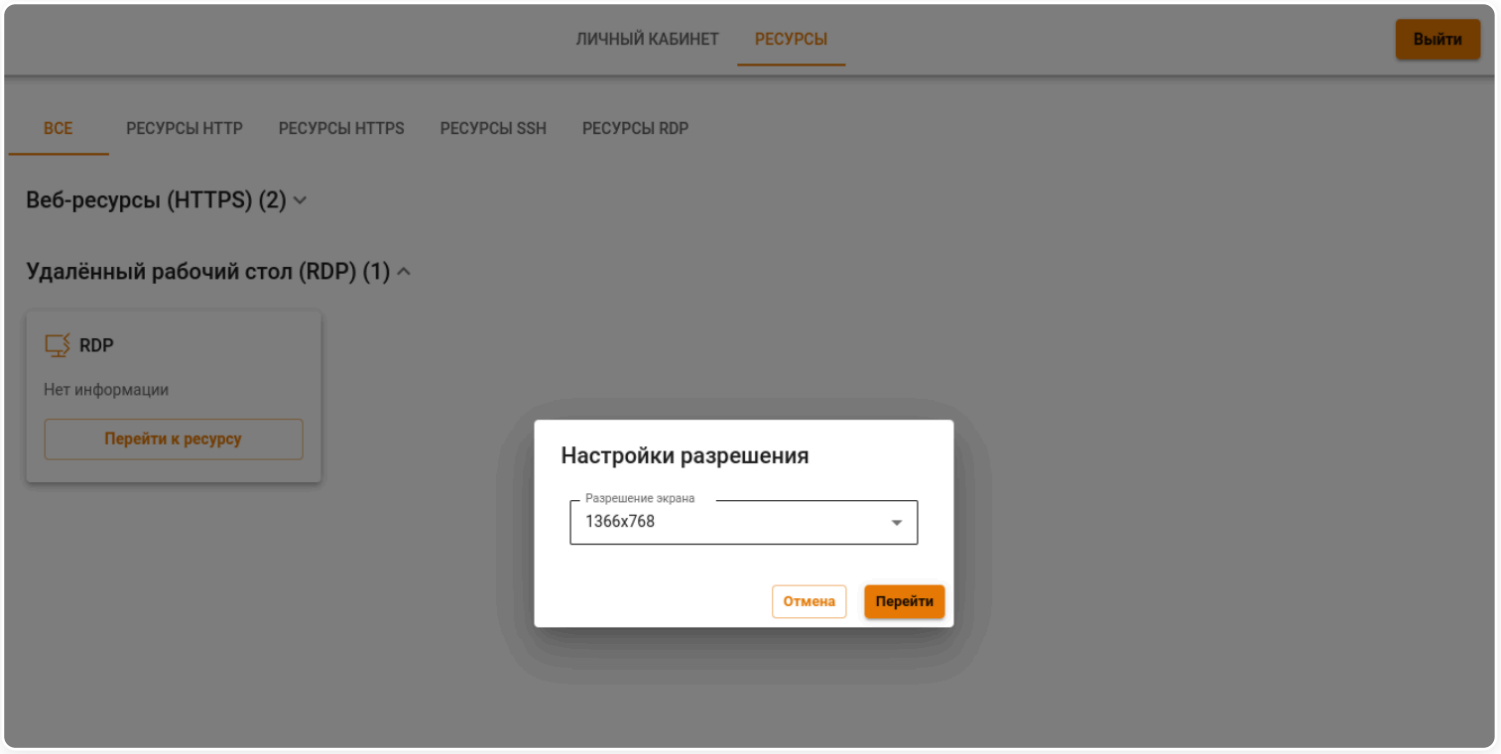
1. Перейдите по ссылке, указанной в правиле публикации личного кабинета.

2. В открывшейся форме авторизации введите логин и пароль пользователя.

Если пользователь уже авторизован в сети NGFW, 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

Защита и управление DNS

Название службы раздела **Защита и управление DNS**: `ideco-unbound`; `ideco-dns-backend; nsd`.

Список служб для других разделов доступен по ссылке.

Настройка производится в разделе **Сервер** → **Защита и управление DNS** на следующих 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.

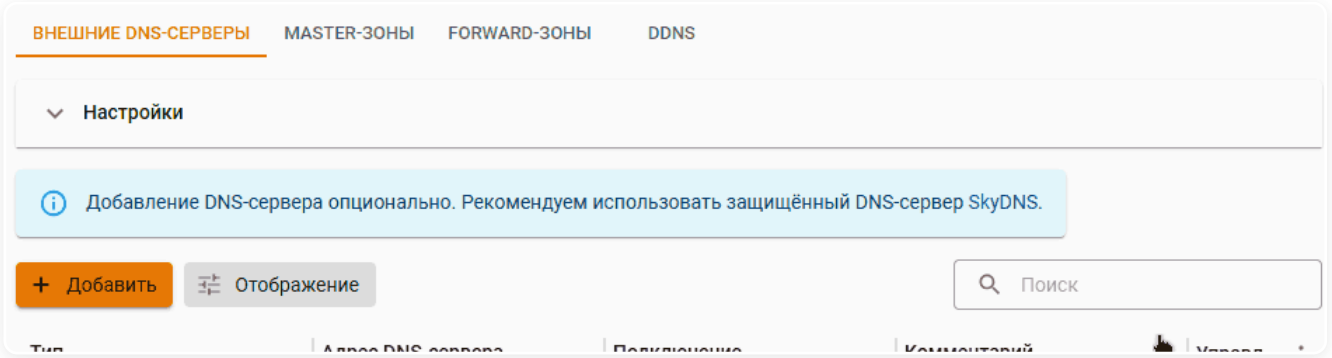
При наличии большого количества Forward- и Master-зон в таблицах воспользуйтесь кнопкой **Фильтры**.

Внешние DNS-серверы

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, если на рабочей станции пользователя указаны сторонние DNS-серверы (например, с целью обхода блокировок). Опция работает глобально для всех хостов в локальной сети и предупреждает возможную подмену адреса ресурса при резолвинге домена. Запрос перенаправляется на DNS-сервер NGFW, который формирует ответ вместо исходного DNS-сервера.

Для VPN-пользователей опция **Перехват пользовательских DNS-запросов** будет работать только если в настройках VPN включена опция **Отправлять весь трафик на Ideco NGFW**.

Включение перехвата пользовательских DNS-запросов блокирует использование DNS-over-TLS (DoT), DNS-over-QUIC (DoQ) и DNS-over-HTTPS (DoH).

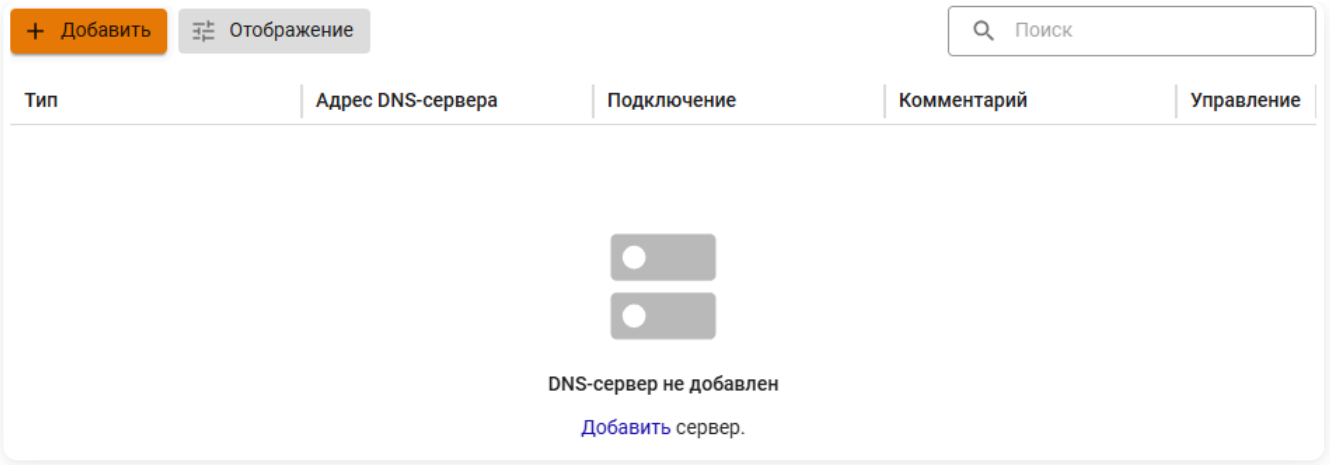
При включенной опции **Перехват пользовательских DNS-запросов** трафик обрабатывается не как FORWARD, а как INPUT. Поэтому для корректной фильтрации трафика модулями **Контроль приложений** создайте правила INPUT для протоколов TCP и UDP с тем же профилем безопасности, источником и портом 53 в разделе **Назначение**.

- **Безопасный поиск** - при резолвинге NGFW будет возвращать адреса поисковых систем (Google, Youtube, Bing) с включенной фильтрацией нежелательного контента.

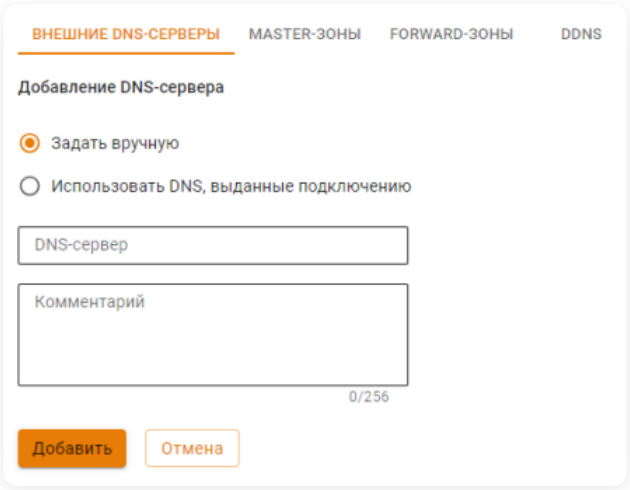
Рекомендации

- В Ideco NGFW встроен кеширующий DNS-сервер. Рекомендуется использовать его в качестве DNS-сервера для локальной сети. Достаточно прописать IP-адрес Ideco NGFW 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 справится с резолвингом самостоятельно.
- Не указывайте DNS-серверы контроллера домена, даже если он может самостоятельно резолвить доменные имена в интернете. При интеграции с AD для работы AD и резолвинга внутренних имен домена. Для резолвинга особых зон, не связанных с AD, создайте Forward-зону вручную.
- По возможности не используйте DNS, выданные интернет-провайдером, так как они превышают TTL и долго отвечают. Ideco NGFW 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).

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`.
- Open DNS `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`.

Master-зоны

Master-зоны позволяют использовать Ideco NGFW как сервер имен и переводить IP-адреса в доменные имена внутри сети.

DNS-сервер в Ideco NGFW 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.

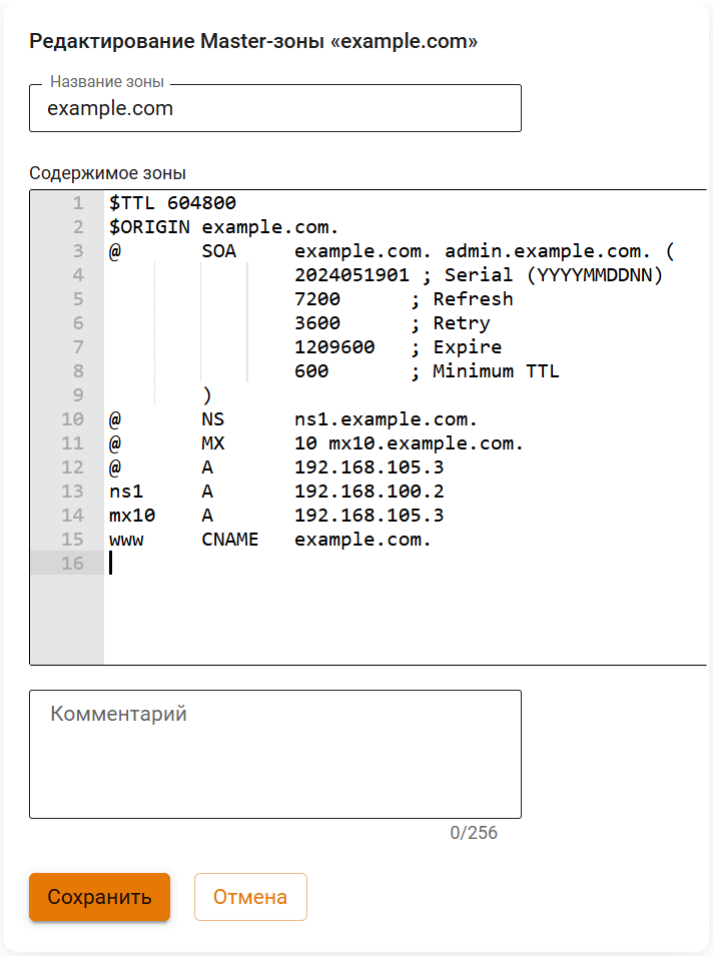
Описание параметров записи

- **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 @
```

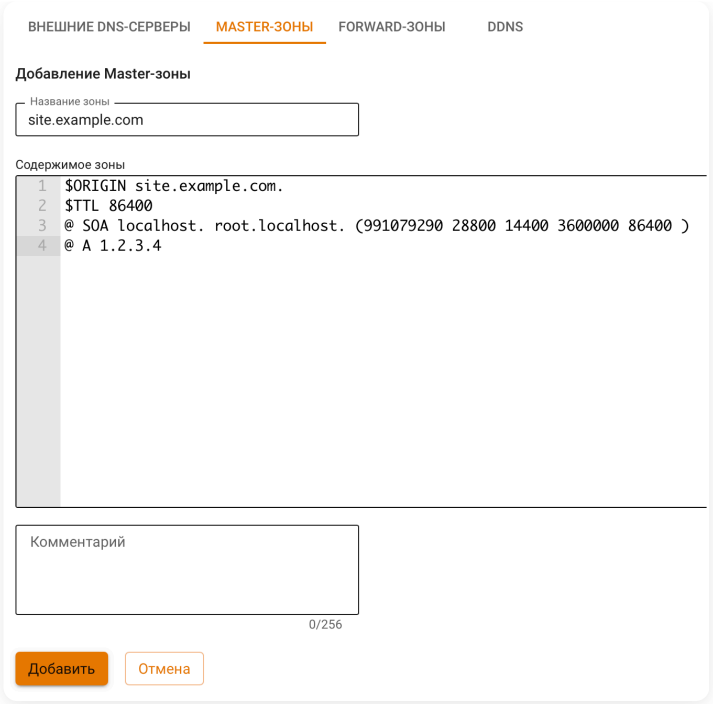
2. Имя зоны: example.com

```
$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 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.

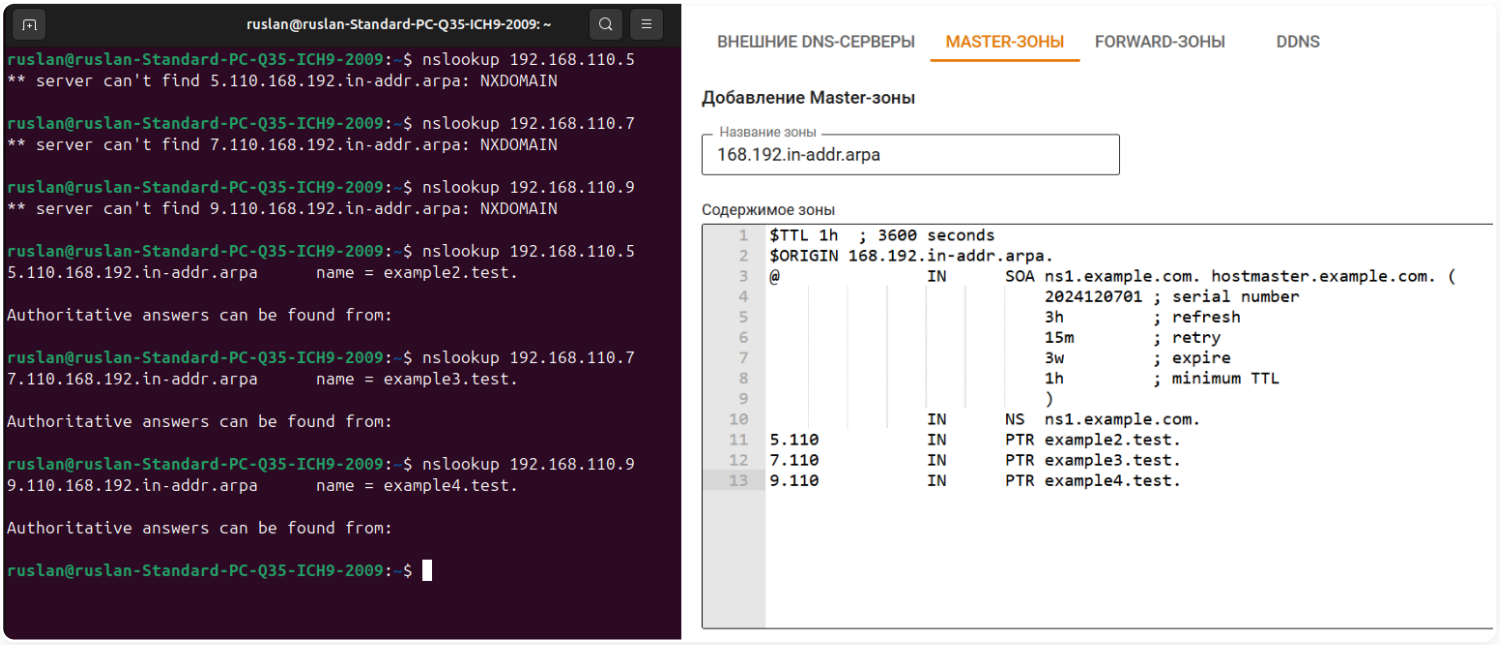
2. При создании содержимого Master-зоны используйте преобразованное в формат **Punycode** доменное имя.

> 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 их 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.
```

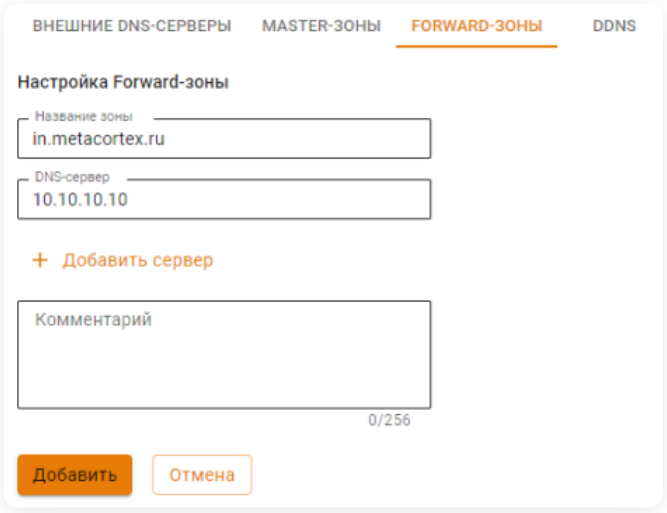
Forward-зоны

Позволяет задать DNS-сервер для разрешения имен конкретной DNS-зоны. Указав доступный в сети DNS-сервер и обслуживаемую зону, клиенты сети Ideco NGFW получают возможность обращаться к ресурсам этой зоны по именам домена.

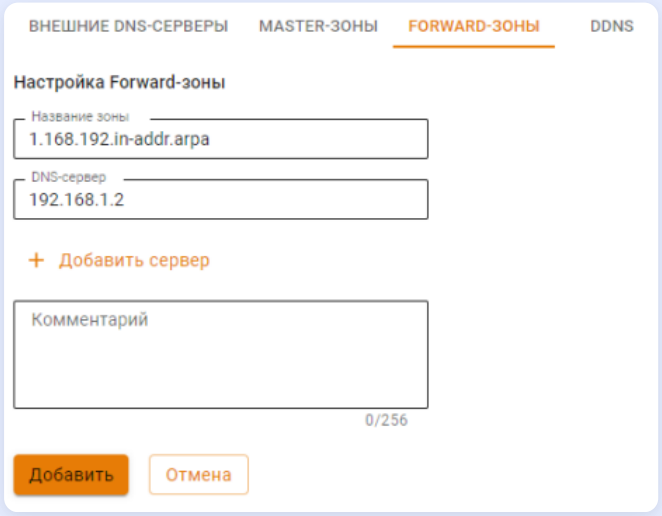
Пользовательские Forward-зоны DNS всегда имеют приоритет над автоматически созданной Forward-зоной для Active Directory.

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**:



DDNS

Название службы раздела **DDNS**: `ideco-dns-backend`.

Список служб для других разделов доступен по ссылке.

DDNS в Ideco NGFW реализован через интеграцию с хостингом RU-CENTER. Перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.

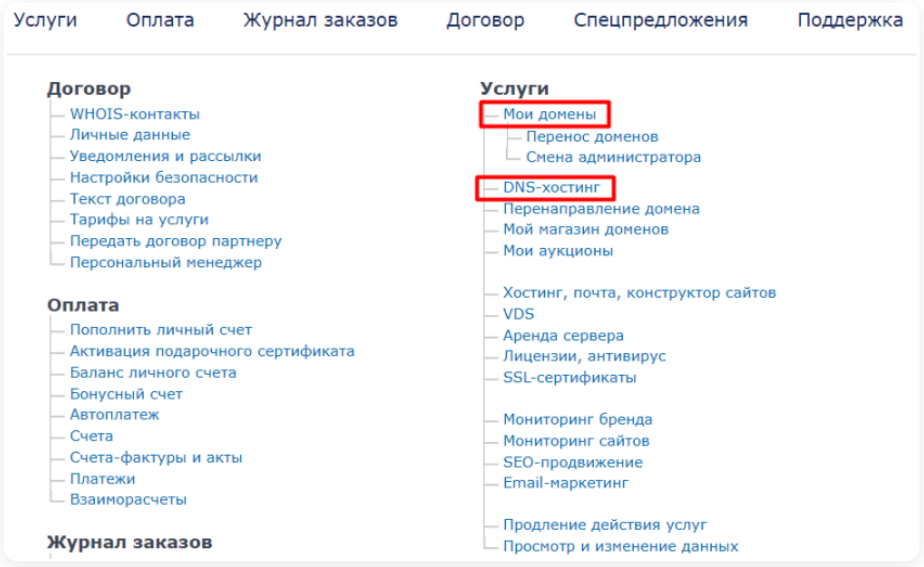
Для решения вопросов по работе с хостингом воспользуйтесь страницей помощи.

Настройка DDNS

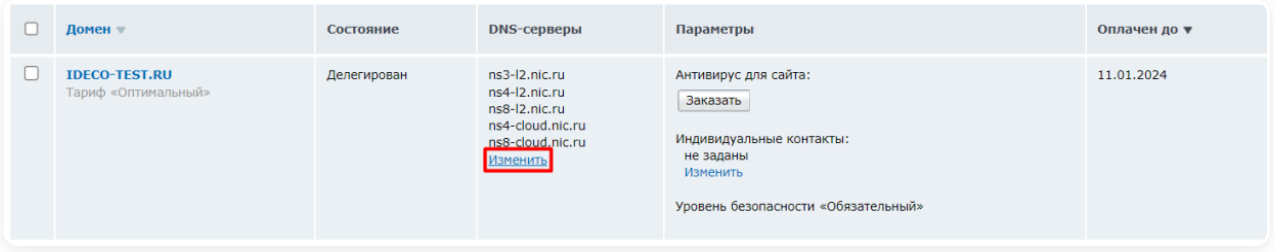
DDNS не будет работать:

- 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**:



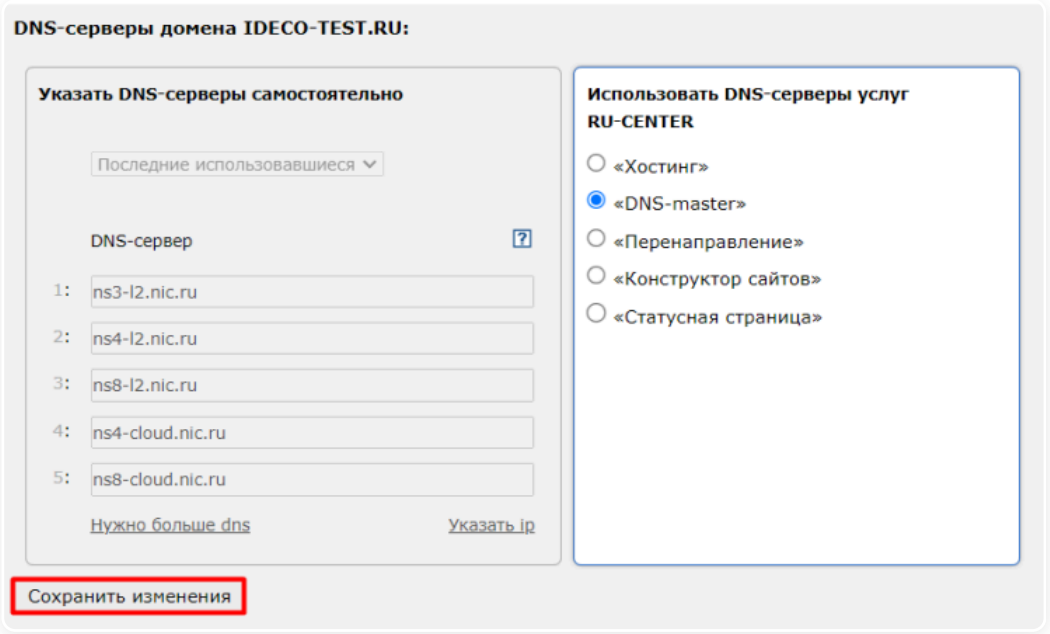
2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:



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.

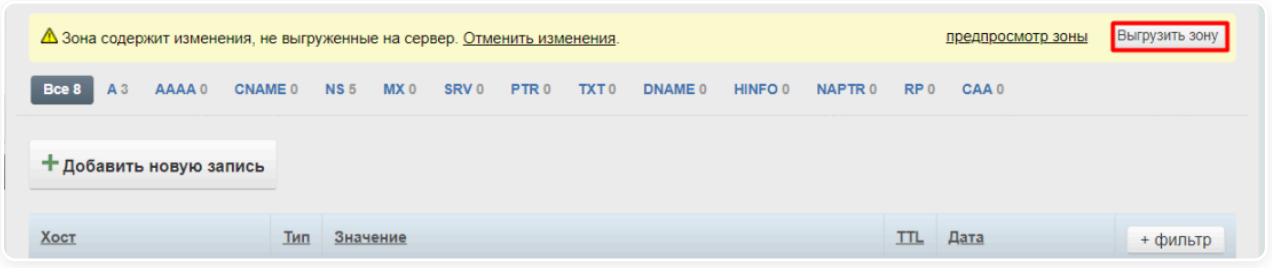
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

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**:

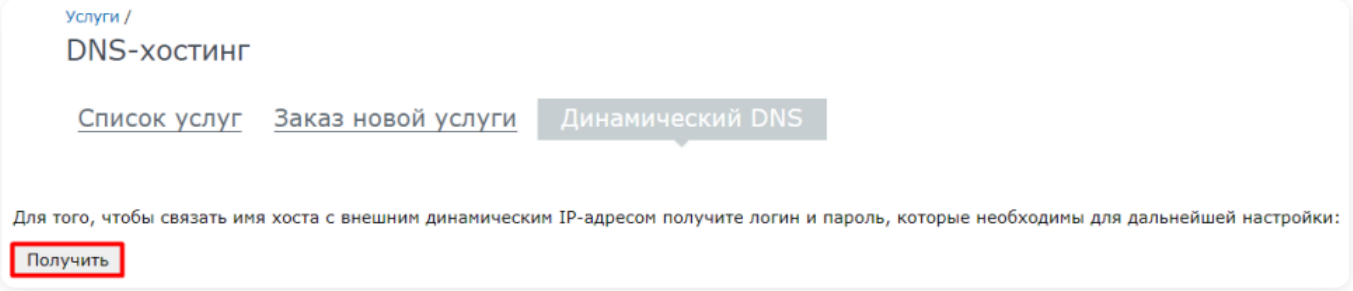
- Первая запись:
  - Name - укажите знак `@`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco NGFW (указывается в разделе *Техническая поддержка* → *Информация для технической поддержки*);
  - TTL - оставьте не заполненным.
- Вторая запись:
  - Name - укажите `www`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco NGFW;
  - TTL - оставьте не заполненным.

7. Нажмите кнопку **Выгрузить зону**:



8. Перейдите в раздел **DDNS** в Ideco NGFW 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, нажав соответствующую кнопку.

DHCP-сервер

Название службы раздела **DHCP**: `ideco-dnsmasq`.

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 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

- **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 управления настройками DHCP-сервера перейдите в раздел **Сервисы** → **DHCP-сервер**.

На локальном интерфейсе Ideco NGFW, участвующем в раздаче адресов, должен быть настроен статический IP-адрес.

При использовании DHCP-сервера включите опцию в левом верхнем углу:



Настройки

Если Ideco NGFW является шлюзом и DNS-сервером для всех сетевых устройств локальной сети, то настройка службы ограничивается определением диапазона IP-адресов.

Если на Ideco NGFW 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:

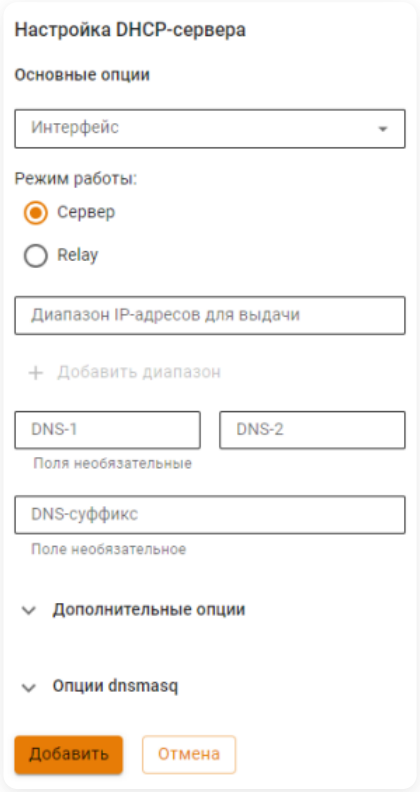
- **Основные опции** - задаются диапазоны IP-адресов и DNS-серверы.
- **Дополнительные опции** - статические маршруты, адреса WINS-серверов, время аренды, PXE Boot и WPAD.
- **Опции dnsmasq** - предназначены для ручного задания опций DHCP, передаваемых сервером клиенту при получении сетевых реквизитов от DHCP-сервера.

Основные опции

Если в разделе **Файрвол** 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

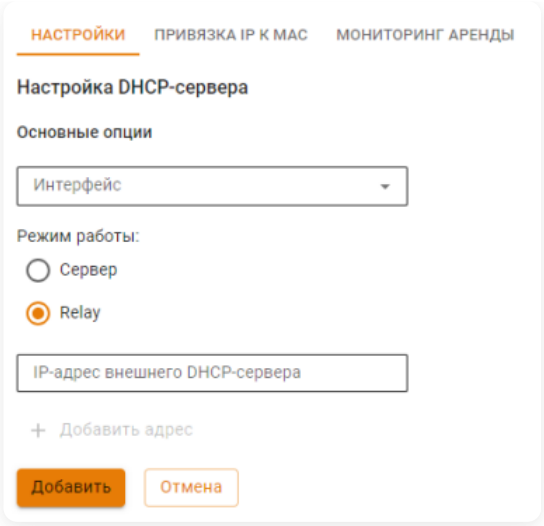
Выберите режим работы **Сервер**, чтобы настроить выдачу IP-адресов на Ideco NGFW. Заполните поля:



- **Интерфейс** - выберите интерфейс, который будет участвовать в раздаче адресов.
- **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.
- **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.

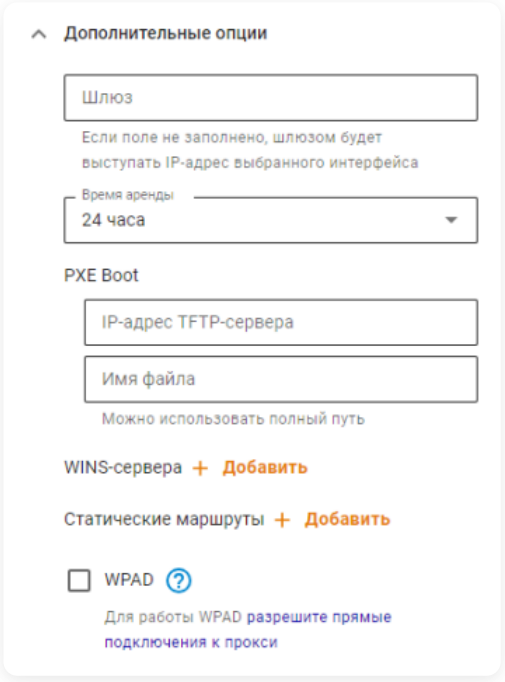
Режим работы Relay

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

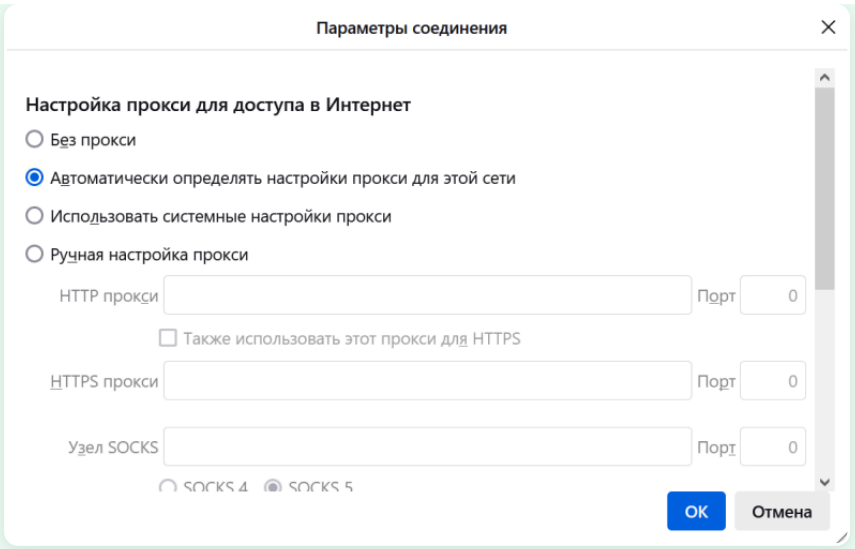


- **Шлюз** - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса.
- **Время аренды** - время, на которое выдается IP-адрес.
- **PXE Boot** - IP-адрес TFTP-сервера для настройки загрузки образа по сети.
- **WINS-сервера** - IP-адрес WINS-сервера.
- **Статические маршруты** - подсеть и шлюз для указания статического маршрута.
- **WPAD** - протокол автоматической настройки прокси.

При включении опции WPAD Ideco NGFW 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**.

Строка **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 он ее не запрашивал.

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 раздел **Отчеты и журналы** → **Системный журнал**.
- 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 раздел **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. Она используется для указания голосового сервера:

```
176,"MCIPADD=1.2.3.4,MCPORT=1719"
```

4. После добавления 176 опции добавьте 242. Она 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.

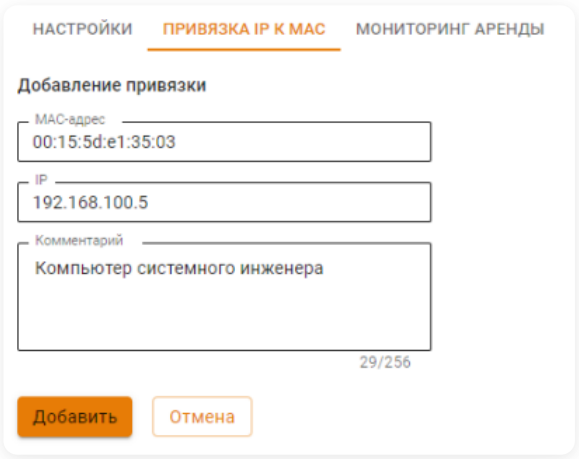
Привязка IP к MAC

> 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.

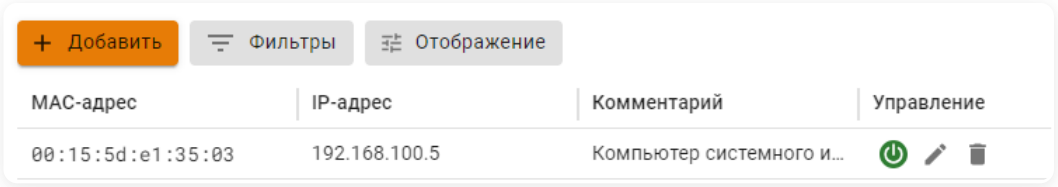
Для настройки в DHCP-сервере привязки IP-адреса к MAC-адресу необходимо:

1. В разделе **Сервисы** → **DHCP** выберите вкладку **Привязка IP к MAC**.

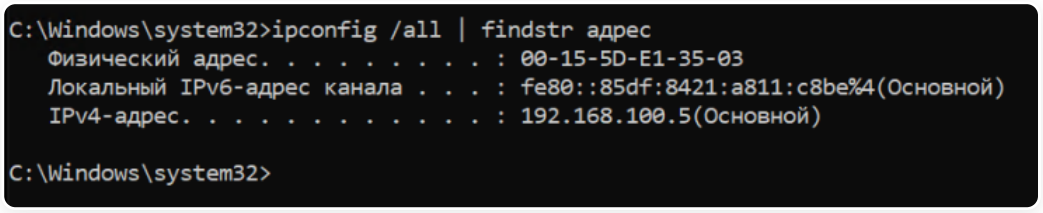
2. Создайте правило привязки **IP к MAC**:



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**.

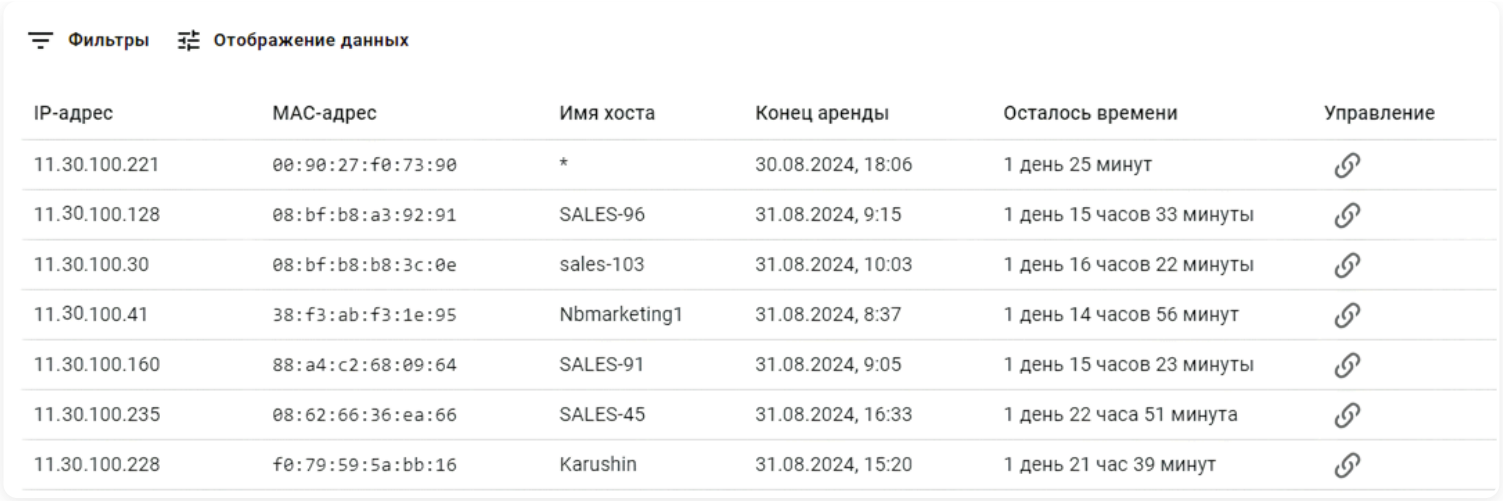
> Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW.
>
> Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (`01-02-03-04-05-06`). В настройках Ideco NGFW октеты MAC-адреса разделяются только двоеточиями (`01:02:03:04:05:06`).

Настройка DHCP-сервера для Wi-Fi сетей:

При настройке Wi-Fi сетей может понадобиться настройка DHCP-сервера. Для получения подробной информации перейдите в статью.

Мониторинг аренды

Содержит информацию об аренде IP-адресов для устройств. Для поиска воспользуйтесь кнопкой **Фильтры**:



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.

NTP-сервер

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-порту.

Принцип работы

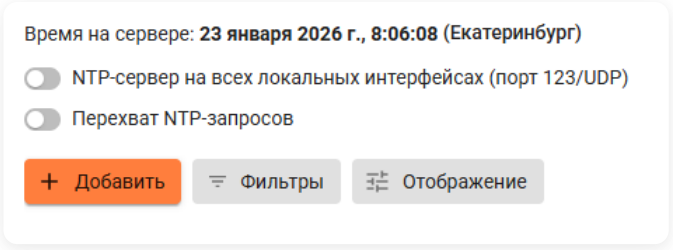
Серверы времени, используемые в NTP, имеют свою иерархию:

- 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 по умолчанию работает как NTP-клиент, получая точное время от эталонных серверов верхнего уровня. При этом Ideco NGFW также может быть настроен как локальный NTP-сервер для устройств во внутренней сети.

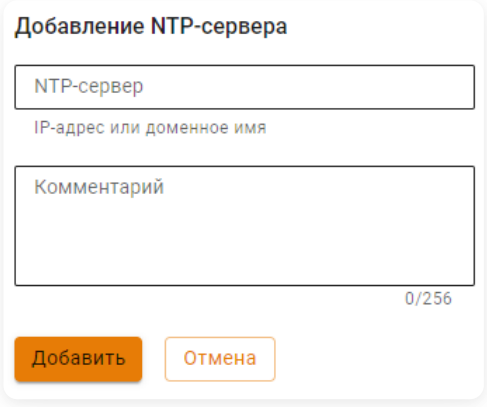
Настройка Ideco NGFW

В **Сервисы** → **NTP-сервер** доступны настройки:



- **NTP-сервер на всех локальных интерфейсах (порт 123/UDP)** - при включении опции NGFW будет доступен в качестве NTP-сервера для локальных клиентов. В этом случае NGFW 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, даже если были отправлены на другой NTP-сервер. В результате все устройства в сети будут получать время только от NGFW, независимо от их собственных настроек.
- Таблица внешних NTP-серверов - в таблице можно вручную указать NTP-серверы, с которыми необходимо синхронизировать время NGFW:
  - Если таблица пуста, NGFW синхронизирует время с сервером `ntp.ideco.ru`.
  - Если в таблице есть записи, NGFW будет синхронизироваться только с указанными серверами.

Чтобы создать запись в таблице, нажмите **Добавить** и введите IP-адрес или доменное имя в поле **NTP-сервер**:



При наличии большого количества NTP-серверов в таблице воспользуйтесь кнопкой **Фильтры**.

IPsec

Название службы раздела **IPsec**: `ideco-ipsec-backend`, `strongswan`.

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. Они позволяют сгенерировать конфиг, запуск которого на удаленном устройстве установит заранее подготовленные настройки IPsec.

Особенности подключений IPsec

В туннельном режиме:

- Интерфейсы без выхода в интернет имеют меньший приоритет по сравнению с интерфейсами с доступом в интернет.
- Поддерживается неограниченное число туннелируемых IP-адресов.
- Для создания туннелей используются все внешние интерфейсы со шлюзом по умолчанию и все **Адреса удаленного устройства**, указанные при создании IPsec-подключений.
- Для каждого **Адреса удаленного устройства** создается столько туннелей, сколько имеется внешних интерфейсов.
- Выбор конкретного туннеля для обмена трафиком зависит от приоритета внешнего интерфейса в таблице раздела **Балансировка и резервирование**. Приоритет интерфейса определяется местом в таблице: чем выше интерфейс, тем больше у него приоритет.

Необходимо заполнять поле **IP-адрес интерфейса туннеля** для обеспечения доступа Ideco NGFW к удаленным сетям за другим устройством (например, для доступа к Ideco Center или Active Directory). В будущих версиях Ideco NGFW без указания IP-адреса доступность удаленных ресурсов через IPsec не будет гарантирована.

Туннельный режим не пропускает широковещательные рассылки, поэтому в таком режиме настроить OSPF не получится.

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.

IPsec использует протокол UDP, порты 500 и 4500. По умолчанию они открыты, но если настроено запрещающее правило во вкладке **INPUT** раздела **Файрвол**, не забудьте добавить разрешение для IPsec.

Исходящие и входящие подключения

Настройте исходящее подключение, если Ideco NGFW 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 при создании подключения, отправляется удаленному устройству и подписанный возвращается для настройки NGFW. • Корневой сертификат удаленного устройства. • Список домашних локальных сетей NGFW, которые будут видны противоположной стороне. • Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	• PSK-ключ. Генерируется на NGFW при создании подключения. • Идентификатор ключа, который потребуется удаленному устройству для идентификации подключения. • Список локальных сетей NGFW, 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, 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 для идентификации входящего подключения. • Список локальных сетей NGFW, которые будут видны противоположной стороне. • Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

Выбор алгоритмов шифрования на удаленных устройствах

При настройке сторонних устройств необходимо явно указать алгоритмы шифрования, используемые для подключения.

Ideco NGFW 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, SHA256, SHA384**.
  - 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)**.
    - **modp1024 (group 2)**.
  - Таймауты:
    - **Lifetime**: 14400 сек.
    - **DPD Timeout** (для L2TP/IPsec): 40 сек.
    - **DPD Delay**: 30 сек.
- **Phase 2 (ESP):**
  - encryption (шифрование):

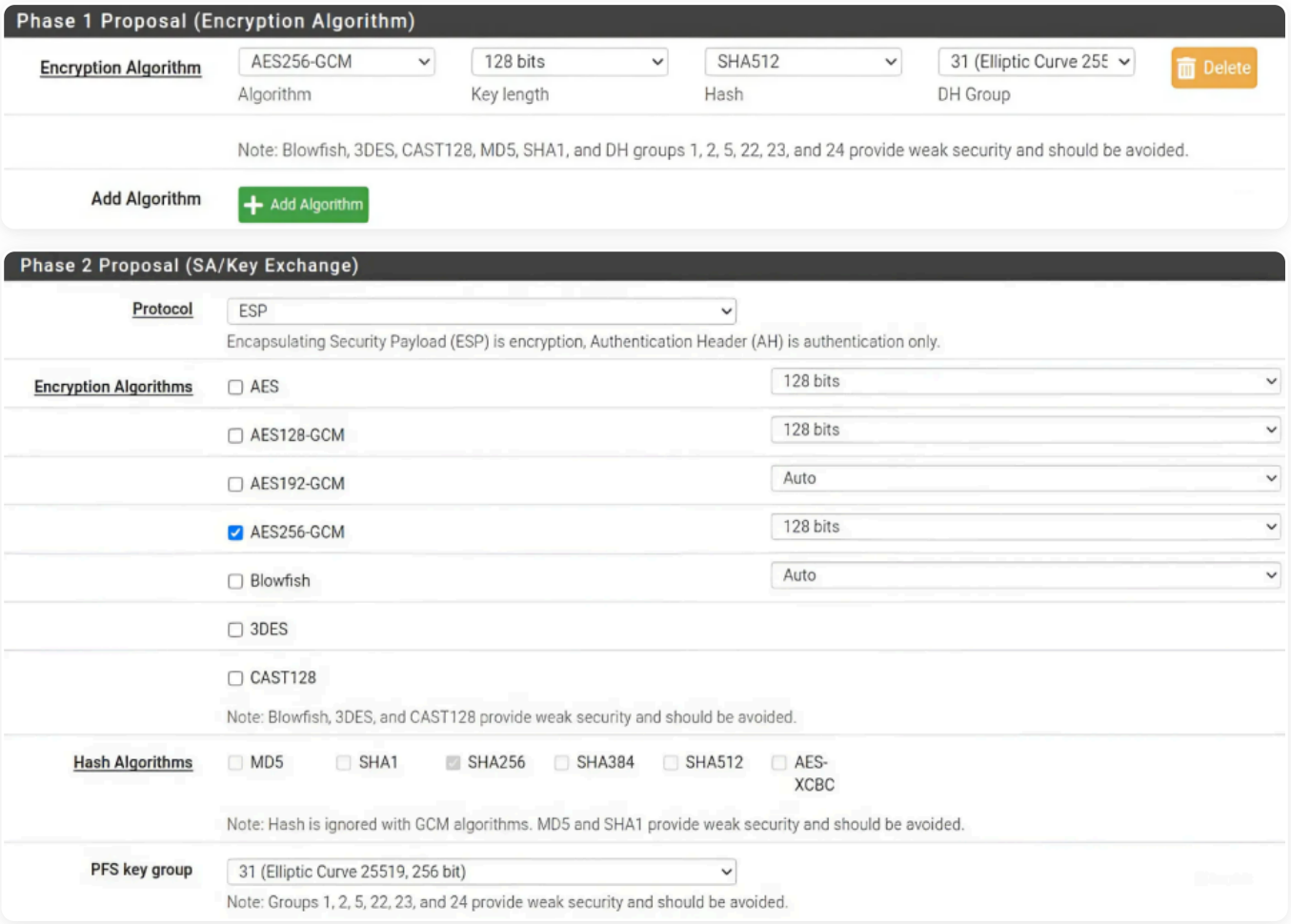
        - **AES256-GCM**.
        - **AES256 (AES256-CBC)**.
    - integrity (целостность):
        - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
        - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
    - DH (Группа Diffie-Hellman, 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)**.
        - **modp1024 (group 2)**.
    - 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 по IPsec:



В Ideco NGFW 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.

Мониторинг производительности сети

В Ideco NGFW 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 для каждого активного соединения отображаются метрики:

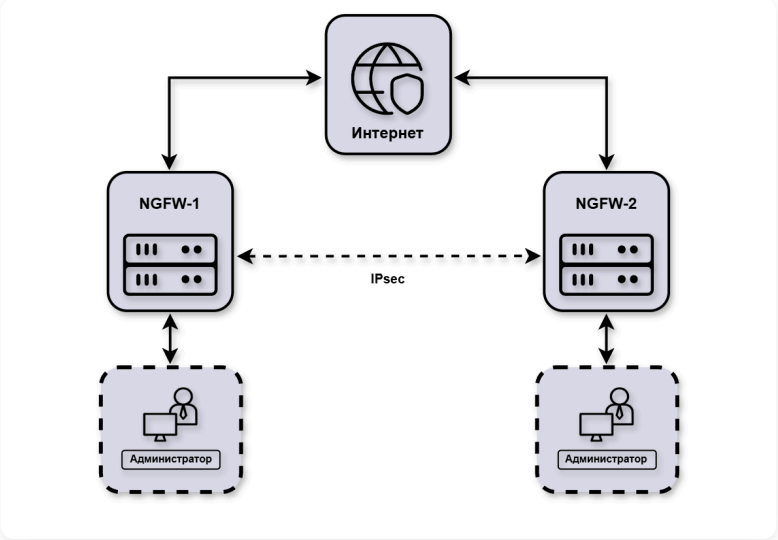
- **Вх. скорость, Мбит/с** - скорость приема данных через туннель.
- **Исх. скорость, Мбит/с** - скорость передачи данных через туннель.
- **Средняя задержка, мс** - время, за которое пакет доходит до удаленной стороны туннеля и возвращается обратно.
- **Потеря пакетов, шт.** - количество количество 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.

Подключение между двумя Ideco NGFW в туннельном режиме работы

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru



Для создания IPsec-подключения между Ideco NGFW 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.

Шаг 1. Проверка условий подключения

Перед созданием подключения убедитесь, что:

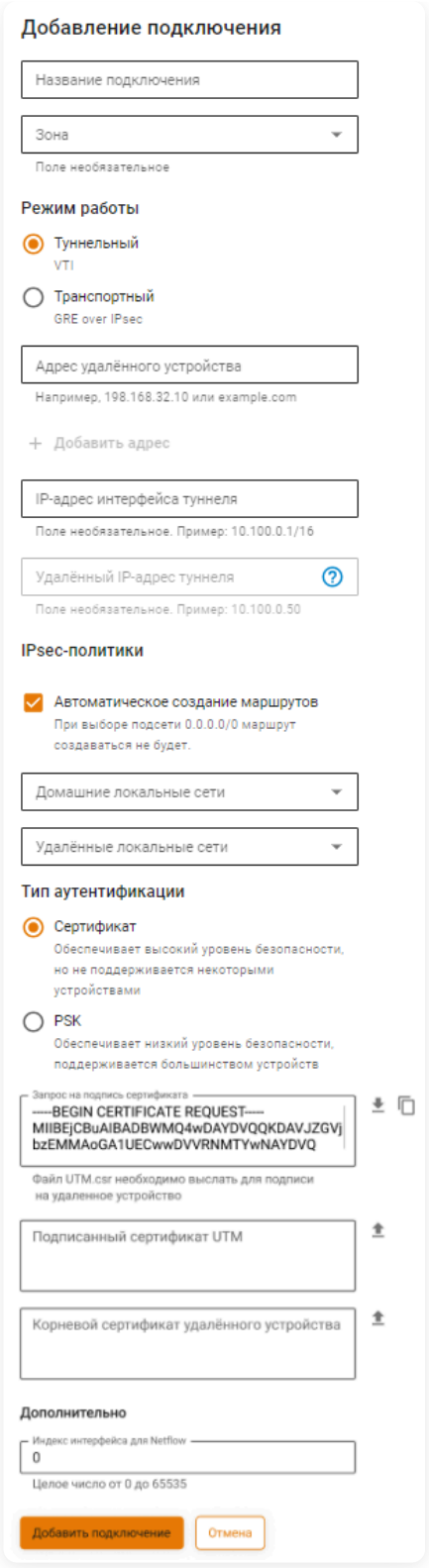
- На **NGFW-1** и **NGFW-2 правильно настроены временные зоны**. Без этого подключение не установится.
- Для работы IPsec все подсети, участвующие в соединениях, не пересекаются.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. **Входящее подключение должно настраиваться на сервере с белым IP-адресом**.
- Пользовательские правила из раздела **Правила трафика** → **Файрвол** → **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 раздел **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 **Туннельный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес. Адресов может быть несколько. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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 к удаленным сетям за другим устройством.

- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW.
- **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 UTM**.



Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они 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 разделе **Сервисы** → **Маршрутизация** или динамическую маршрутизацию через BGP в разделе **Сервисы** → **BGP**.

3. Выполните действие для нужного типа аутентификации:

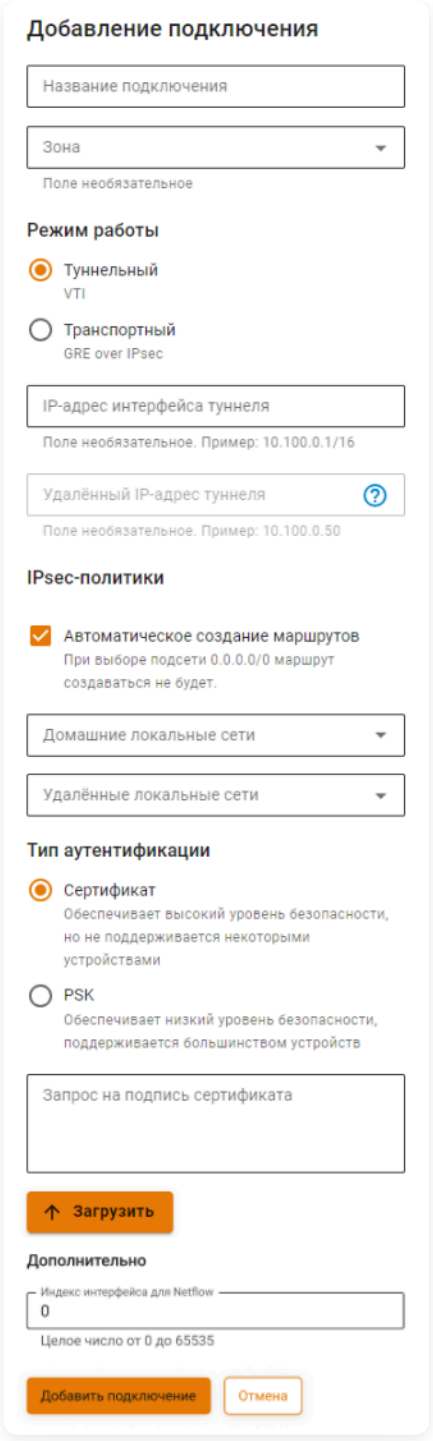
- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 3**.
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 3** для настройки входящего подключения на **NGFW-2**.

Шаг 3. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **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**.
- **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 к удаленным сетям за другим устройством.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-1**. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    - При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW.
    - При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW.

- **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW.

- **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 в разделе **Сервисы** → **Маршрутизация** или динамическую маршрутизацию через BGP в разделе **Сервисы** → **BGP**.

3. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

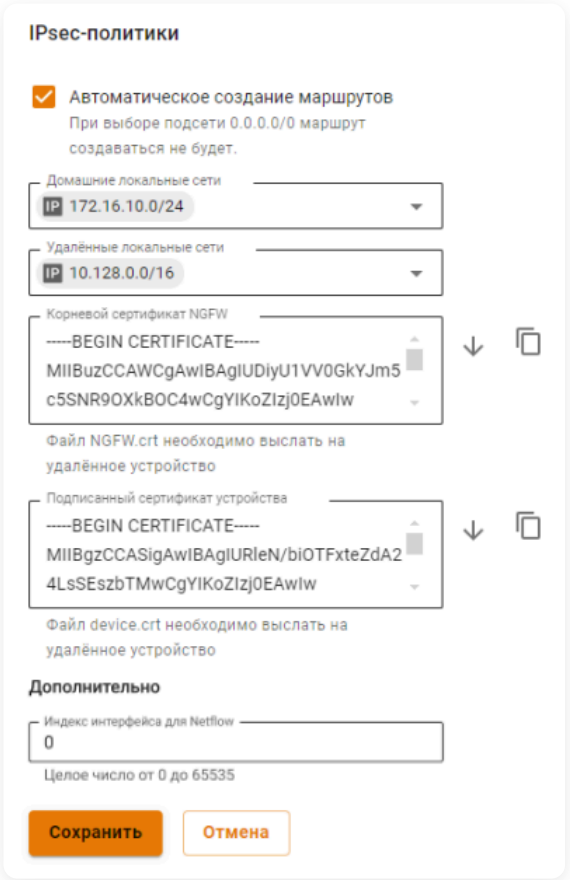
Если был выбран тип аутентификации **PSK**, то настройка завершена.

Если был выбран тип аутентификации **Сертификат**, то выполните **Шаг 4**.

Шаг 4. Донастройка исходящего подключения с типом аутентификации Сертификат

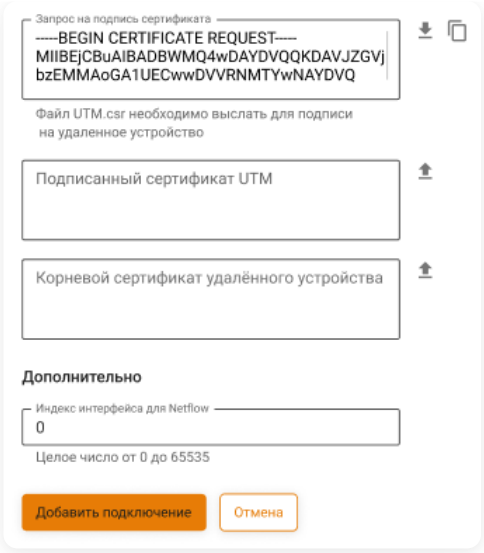
1. В **NGFW-2** перейдите в раздел **Сервисы** → **IPsec** → **Входящие подключения** и нажмите по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **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**.

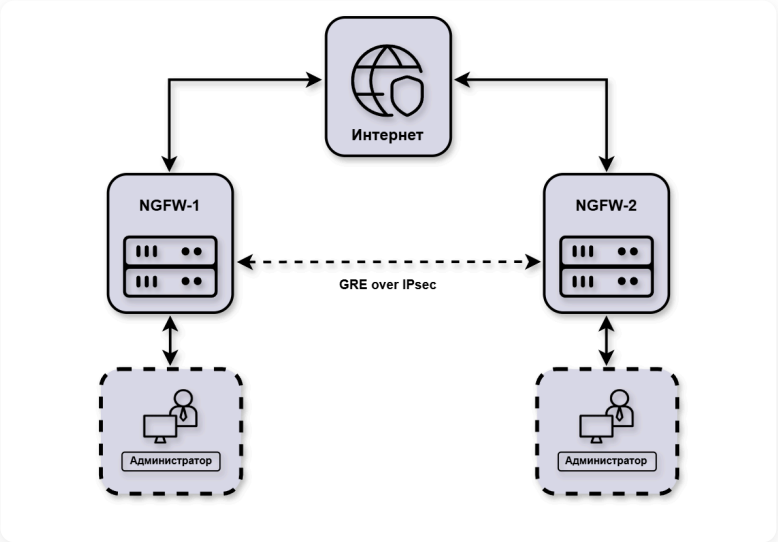
2. Укажите в поле **Домашние локальные сети** сеть, используемую для VPN в **NGFW-2**.

> В Ideco NGFW 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 в транспортном режиме работы

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru



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 их 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** → **Файрвол** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протоколов ESP и UDP (порты 500 и 4500).
- Пользовательские правила из раздела **Правила трафика** → **Файрвол** → **INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протокола GRE.
- Ни один Ideco NGFW не находится за NAT, так как в таком случае подключение двух Ideco NGFW 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 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.

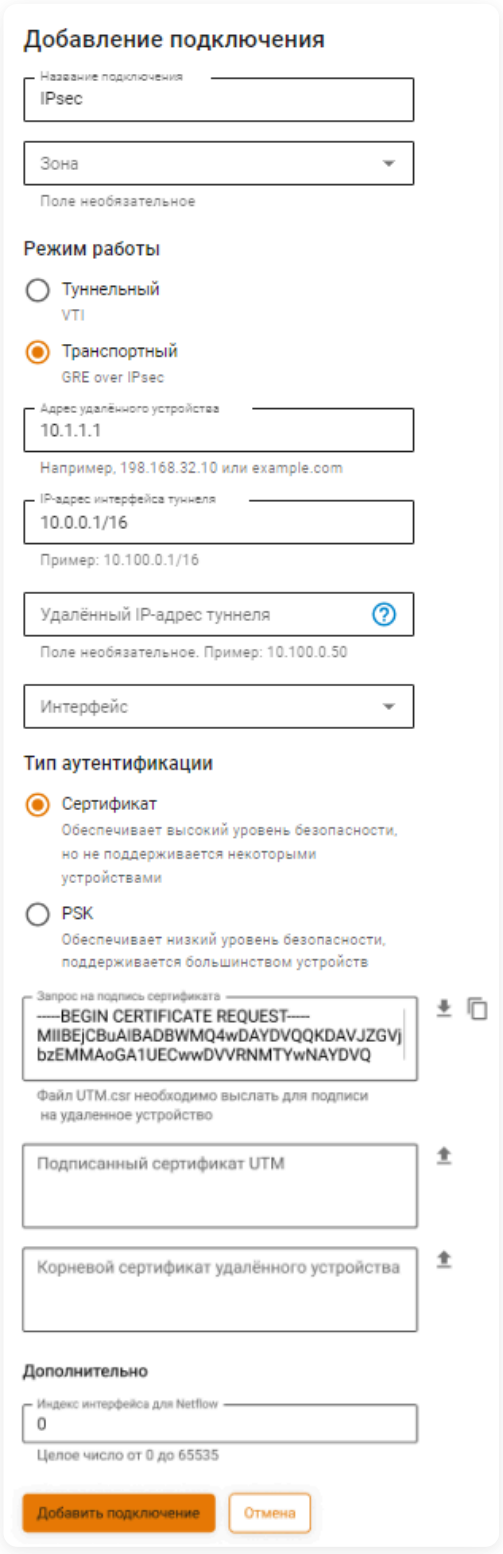
Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе Туннельные. Рекомендуем отключать такой GRE-туннель на время подключения к удаленному серверу через GRE over IPSec, либо использовать разные адреса для 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 раздел **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 или его белый IP-адрес.
- **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.
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его IP-адрес, доступный с сетевого интерфейса, указанного в поле выше.
- **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.

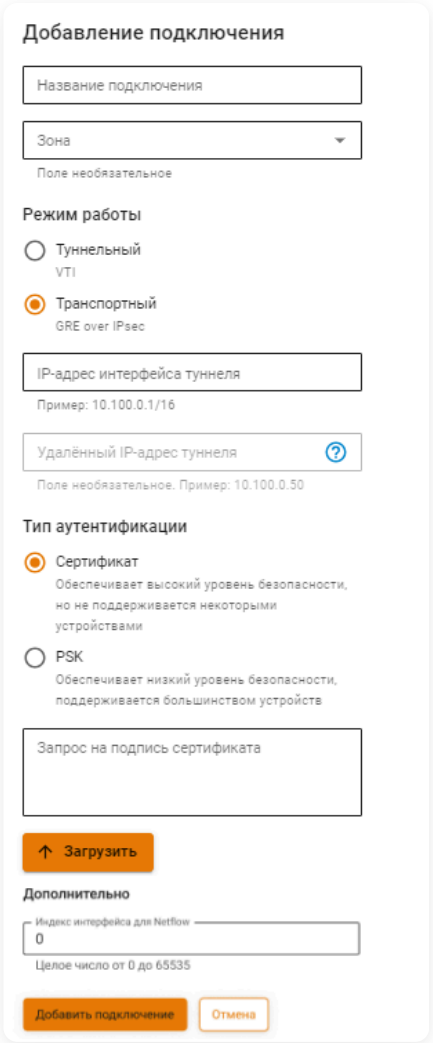
4. Если тип аутентификации - **PSK**, проверьте правильность заполнения полей и нажмите **Добавить подключение** и перейдите к **Шагу 2**. Если тип аутентификации - **Сертификат**, **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 2** для настройки входящего подключения на другом NGFW.

Шаг 2. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **Сервисы** → **IPsec** → **Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей

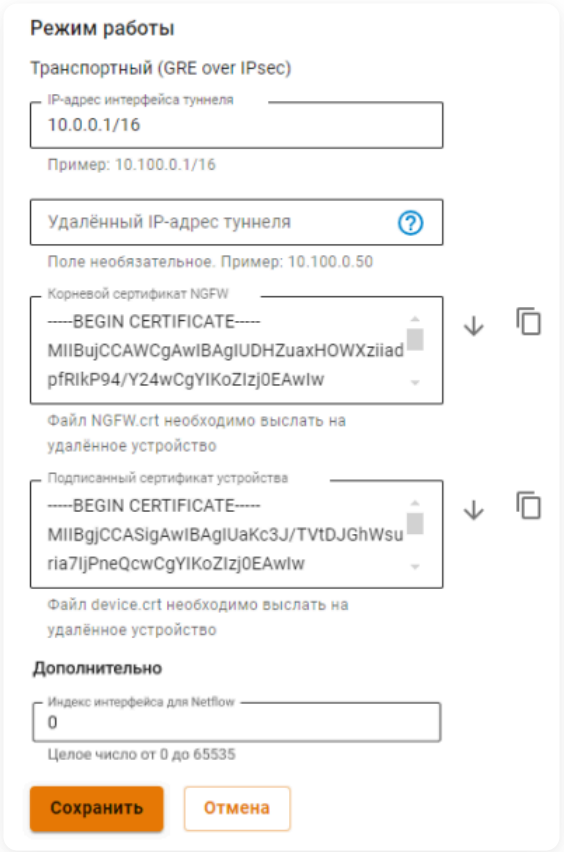
- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым. Список предустановленных зон приведен в статье.
- **Режим работы** - выберите **Транспортный**.
- **IP-адрес интерфейса туннеля** - укажите 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 интрефейса 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

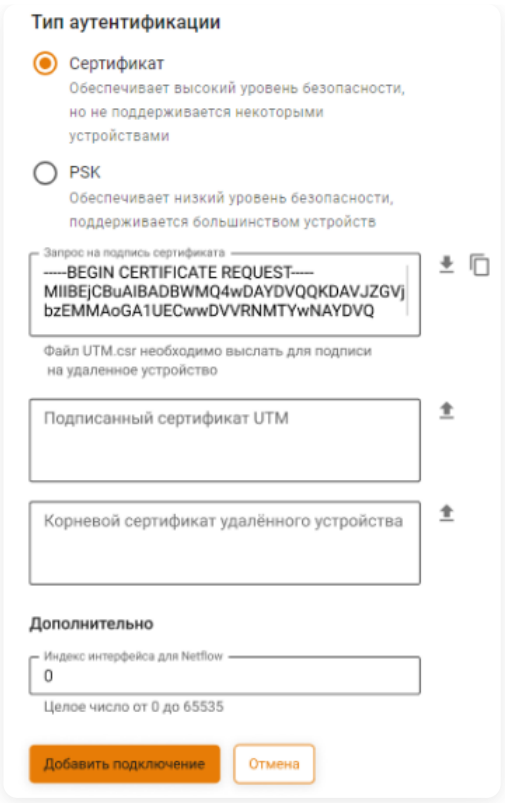
1. В **NGFW-2** перейдите в раздел **Сервисы** → **IPsec** → **Входящие подключения** и нажмите по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **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 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 и MikroTik по IPsec в туннельном режиме

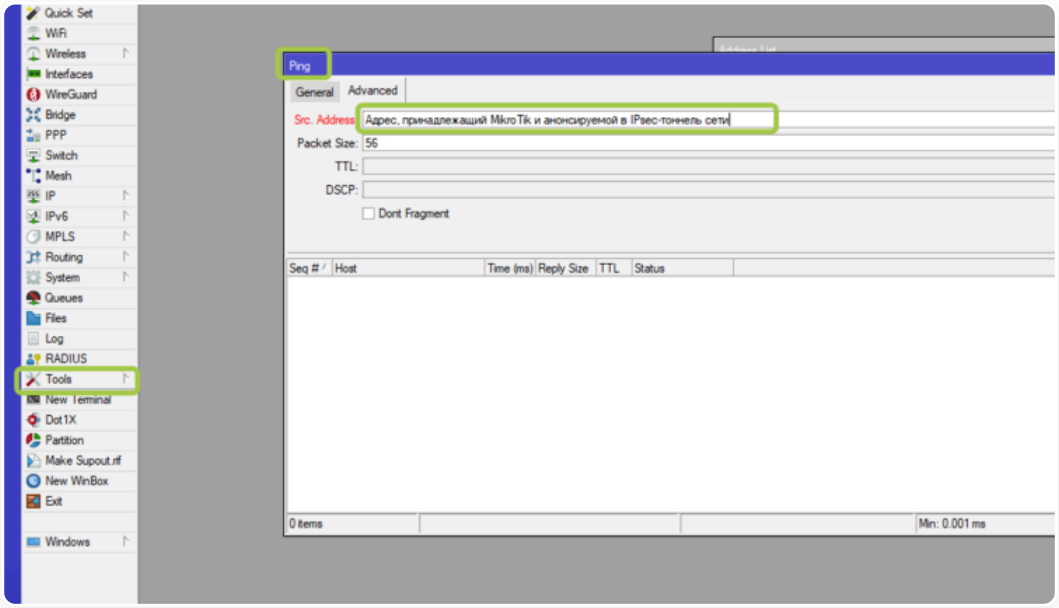
В статье описана настройка IPsec-подключения между Ideco NGFW и MikroTik с аутентификацией по сертификатам или PSK.

Требования и подготовка

Основные требования:

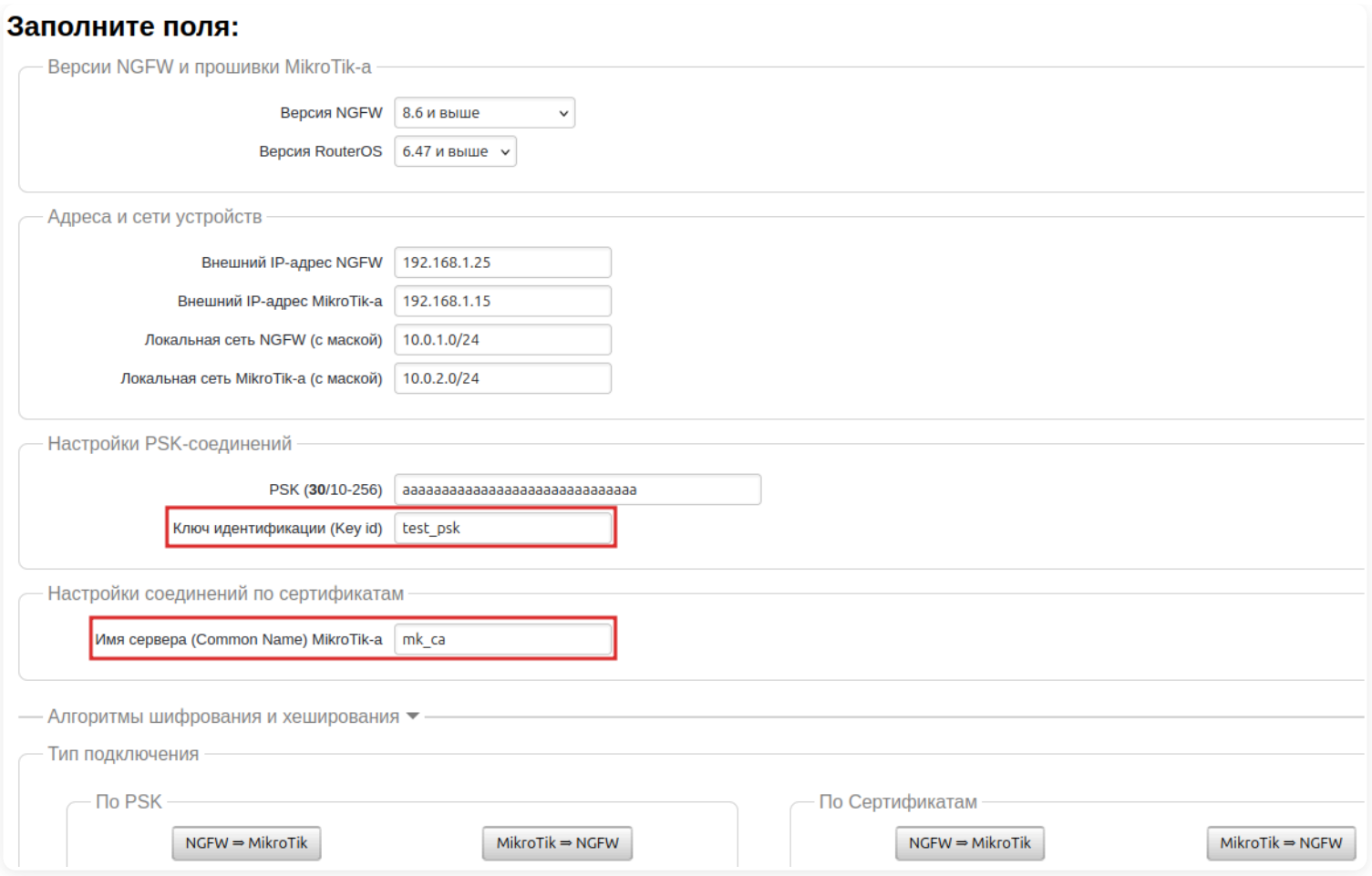
- Локальные сети в разных офисах не должны пересекаться.
- Для корректной работы подключений по сертификатам синхронизируйте время на MikroTik по NTP (например, предоставьте доступ в интернет).
- IPsec-подключения от Ideco NGFW к MikroTik версии 6.45 и ниже по сертификатам не работают, так как нельзя использовать современные криптоалгоритмы.

Для проверки доступности анонсируемых сетей Ideco NGFW с MikroTik указывайте IP-адрес источника:



При подключении нескольких устройств MikroTik к одному Ideco NGFW **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 к MikroTik

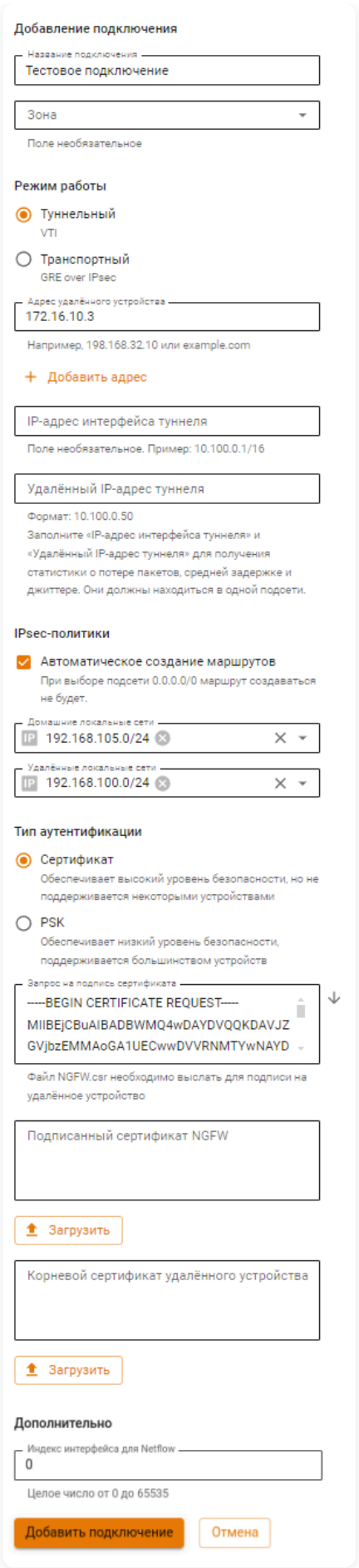
Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

Шаг 1. Настройка Ideco NGFW (исходящее подключение)

Сгенерируйте запрос на подпись сертификата:

1. В Ideco NGFW 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. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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.

> **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, необходимо загрузить в файловое хранилище MikroTik:

1. Откройте раздел **File**.

2. Нажмите кнопку **Browse**.

3. Выберите файл и загрузите его.

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

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW.

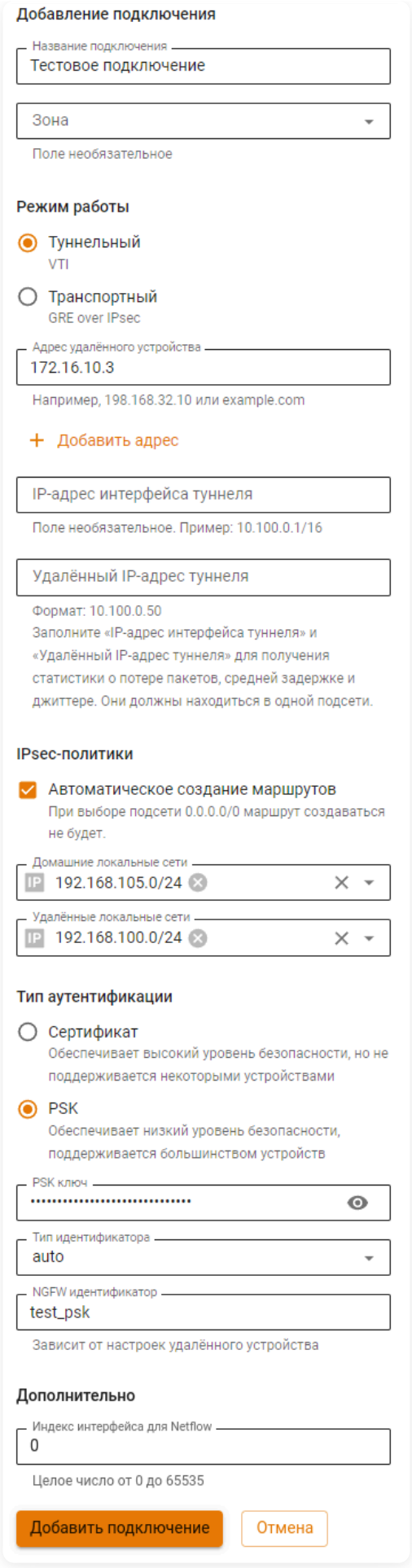
1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

PSK

Шаг 1. Настройка Ideco NGFW (исходящее подключение)

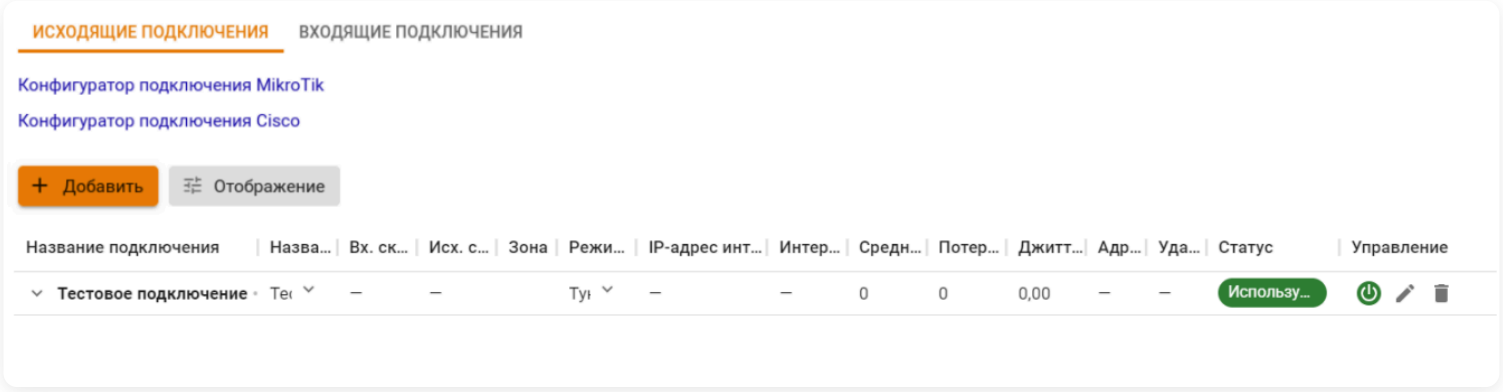
1. Откройте **Сервисы** → **IPsec** → **Исходящие подключения**, нажмите **Добавить** и заполните поля:



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 устройства MikroTik. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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. Он потребуется 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

Выполните настройку в соответствии с типом аутентификации:

Сертификат (рекомендуется)

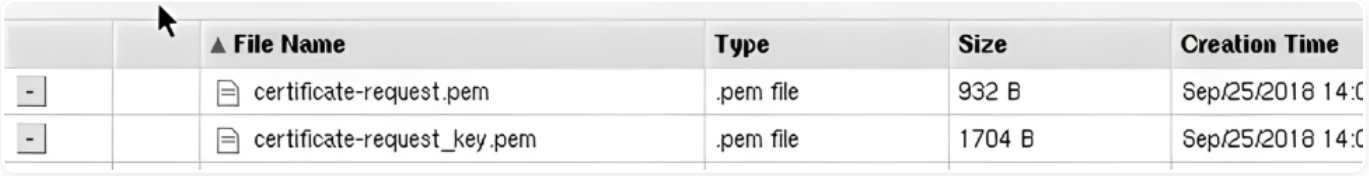
Шаг 1. Предварительная настройка MikroTik

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.

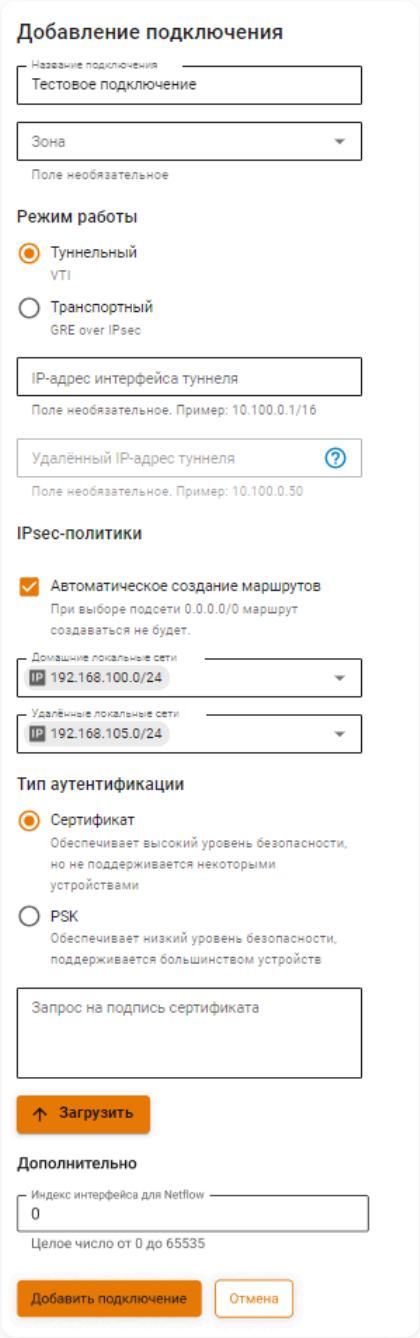
Перед настройкой необходимо запустить первый скрипт для запроса на подпись сертификата. После чего в файловом хранилище MikroTik появятся два файла, которые необходимо скачать. Файлы потребуются для дальнейшей настройки:



- Файл `certificate-request.pem` - запрос на подпись сертификата.
- Файл `certificate-request_key.pem` - приватный ключ.

Шаг 2. Настройка Ideco NGFW (входящее подключение)

1. В Ideco NGFW откройте **Сервисы** → **IPsec** → **Входящие подключения**, нажмите **Добавить** и заполните поля:



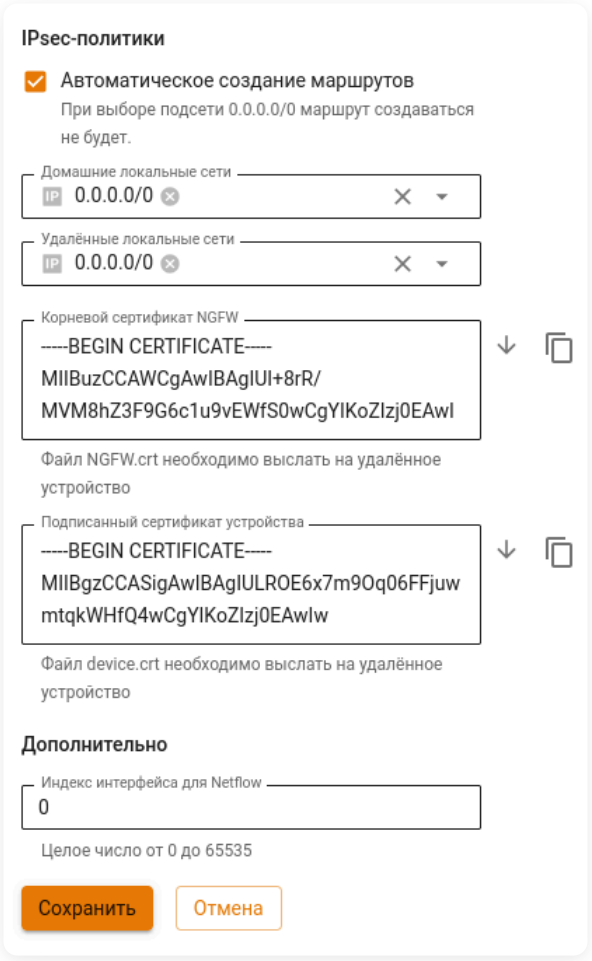
Расшифровка полей

- **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**.
- **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 **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.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)

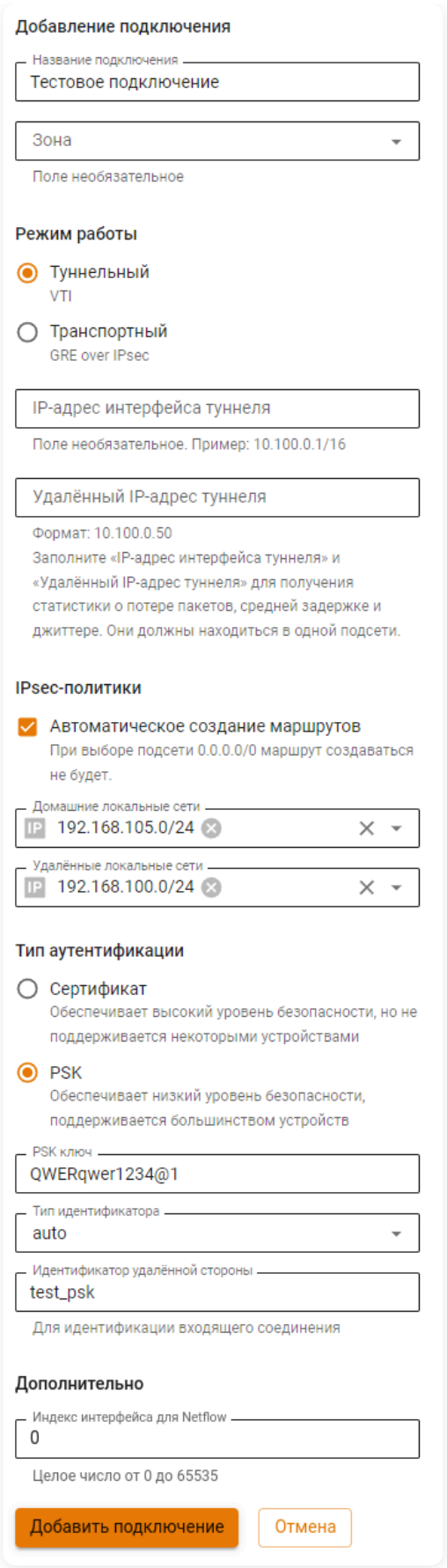
Настроить устройство MikroTik можно через:

- 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 (входящее подключение)

1. В Ideco NGFW 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**.

- **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 **auto**.
- **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**.

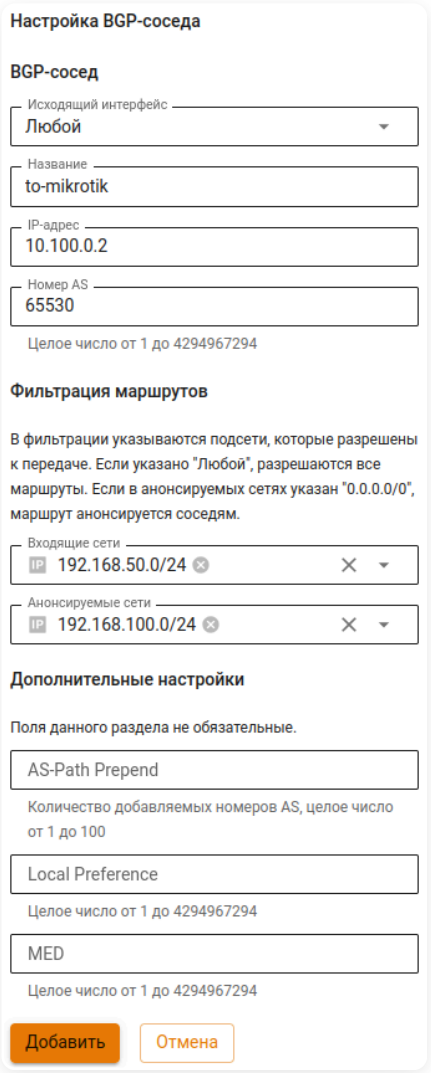
Настройка динамической маршрутизации (BGP)

Настройка Ideco NGFW

1. Перейдите в **Сервисы** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в строку **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.

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:

```
/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. 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

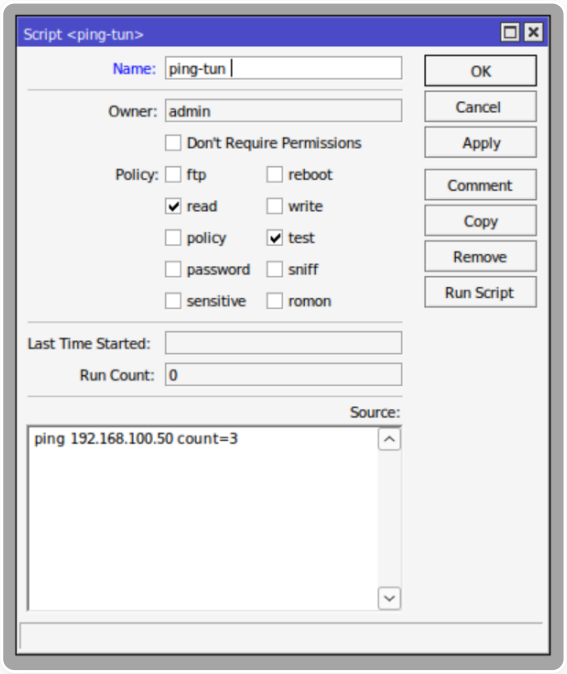
При работе туннеля между Ideco NGFW и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW.

Для автоматизации процесса поддержания соединения создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в **System** → **Scripts**.

3. Нажмите кнопку **+** для создания нового скрипта и заполните поля:



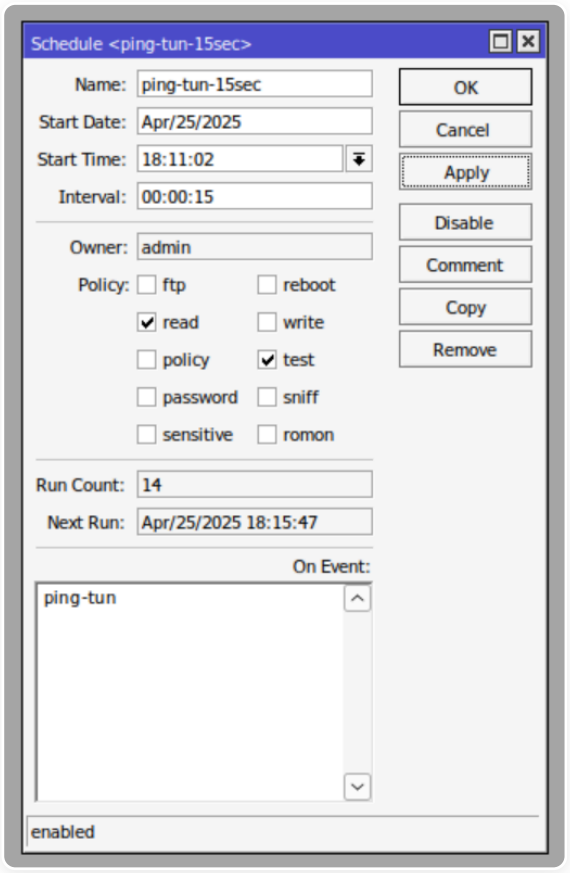
- **Name** - название скрипта (не поддерживаются пробелы и нижние подчеркивания).
- **Policy** - включите опции **read** и **test**.
- **Source** - введите команду `ping <IP-адрес Ideco NGFW> count=3`.

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. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.

> В Ideco NGFW 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 и MikroTik по IPsec в транспортном режиме

При объединении сетей с помощью VPN локальные сети в разных офисах не должны пересекаться.

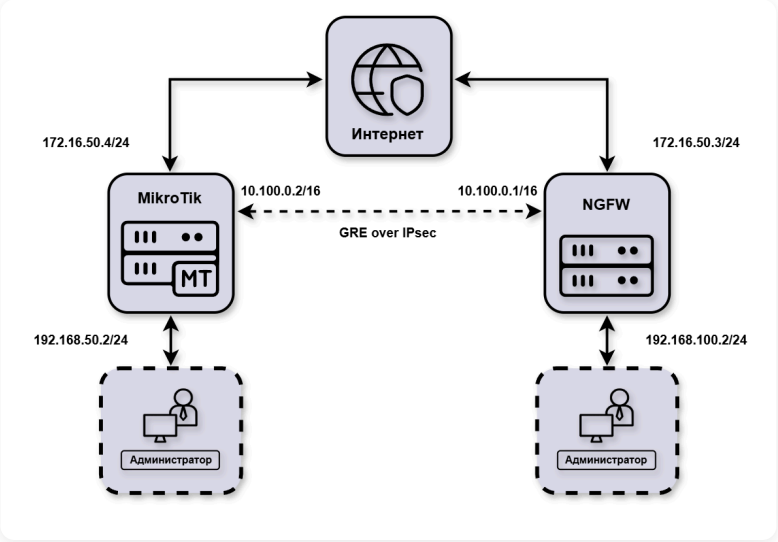
Для корректной работы подключений по сертификатам синхронизируйте время на MikroTik по NTP (например, предоставьте доступ в интернет).

IPsec-подключения от Ideco NGFW 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 следуйте инструкции в каждом из пунктов.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используются другим, уже действующим GRE-туннелем в разделе Туннельные. 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 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
```

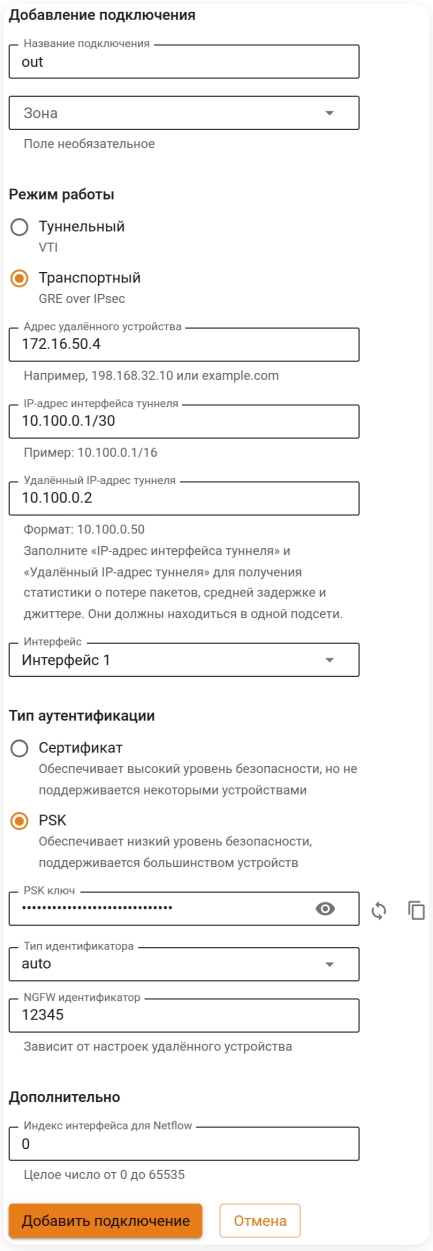
2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/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

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.
- **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.
- **Интерфейс** - выберите внешний интерфейс NGFW.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - будет сгенерирован случайный PSK-ключ. Он потребуется 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.
```

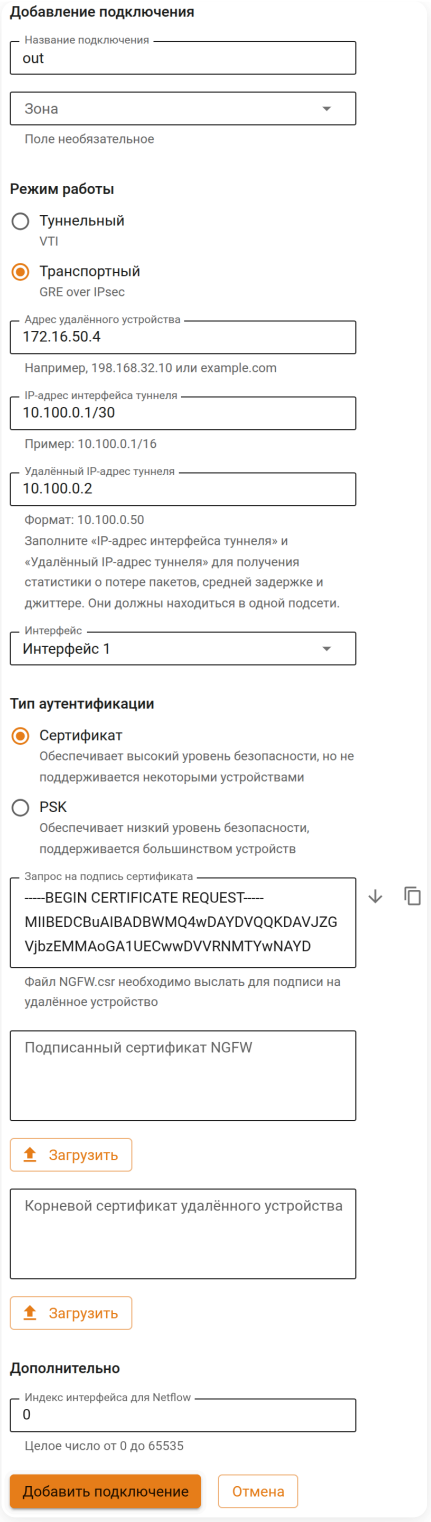
2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Тип аутентификации Сертификат

Настройка исходящего IPsec-подключения на Ideco NGFW

1. Перейдите в раздел **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.
- **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.
- **Интерфейс** - выберите интерфейс NGFW.
- **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 и сделайте его 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

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW.

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

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
```

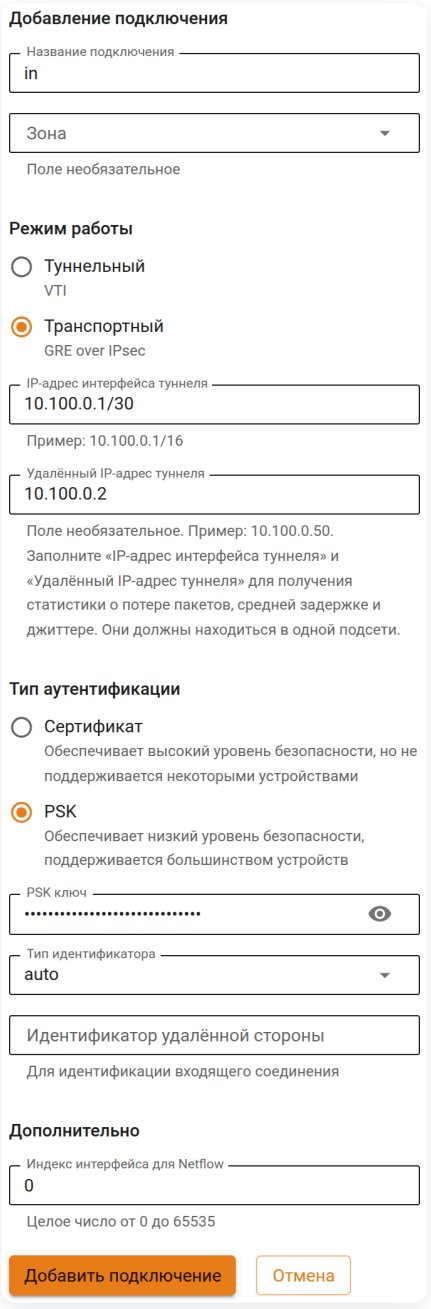
3. Настройте IPsec-подключение со стороны MikroTik:

```
/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

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.
- **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:

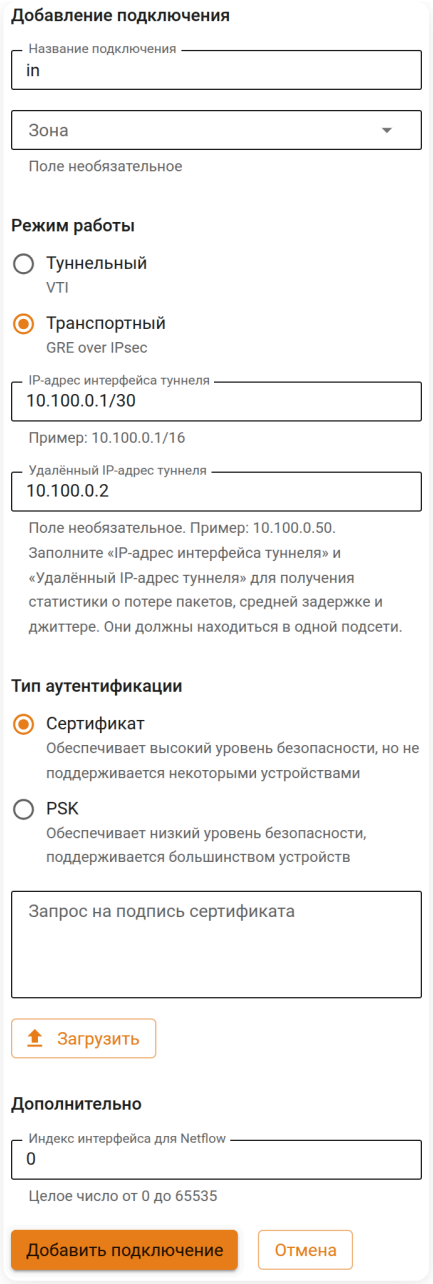
```
/certificate add name=mk_ca common-name=mk_ca key-usage=digital-signature,content-commitment
/certificate create-certificate-request key-passphrase="" template=mk_ca
```

4. Загрузите файл `certificate-request.pem` с MikroTik через WinBox или по SHH.

Настройка входящего IPsec-подключения на Ideco NGFW

1. Перейдите в раздел **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.
- **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.

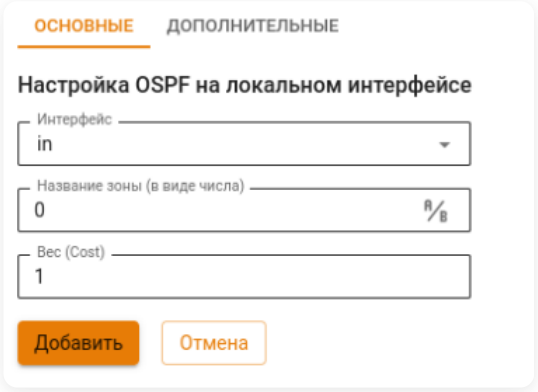
Настройка динамической маршрутизации

OSPF

Настройка на Ideco NGFW

1. Перейдите в раздел **Сервисы** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW, настроенный ранее.
- **Название зоны** - введите номер зоны (значение `area`, должно совпадать на NGFW и Mikrotik). Можно ввести в виде числа или IP-адреса, нажав иконку .
- **Вес** - введите стоимость маршрута.

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

1. Перейдите в раздел **Сервисы** → **BGP** и нажмите **Добавить**.

2. Введите номер автономной системы в строку **Номер AS** и нажмите **Сохранить**.

3. Заполните поля:

- **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.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

5. Включите модуль **BGP**.

Настройка на 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:

```
/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 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. 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 и MikroTik может происходить обрыв соединения. Чтобы восстановить соединение, необходимо отправить какой-либо трафик с MikroTik в сторону Ideco NGFW.

Для автоматизации процесса поддержания соединения, создайте на MikroTik скрипт, который будет отправлять ping-запросы по расписанию планировщика к Ideco NGFW:

1. Откройте веб-интерфейс MikroTik или подключитесь через WinBox.

2. Перейдите в раздел **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> count=3`.

4. Нажмите **Apply**, затем **Ok**.

Далее настройте запуск скрипта по расписанию в планировщике заданий:

1. Перейдите в раздел **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. Это позволит автоматически восстанавливать туннельное соединение в случае обрыва.



В Ideco NGFW 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.

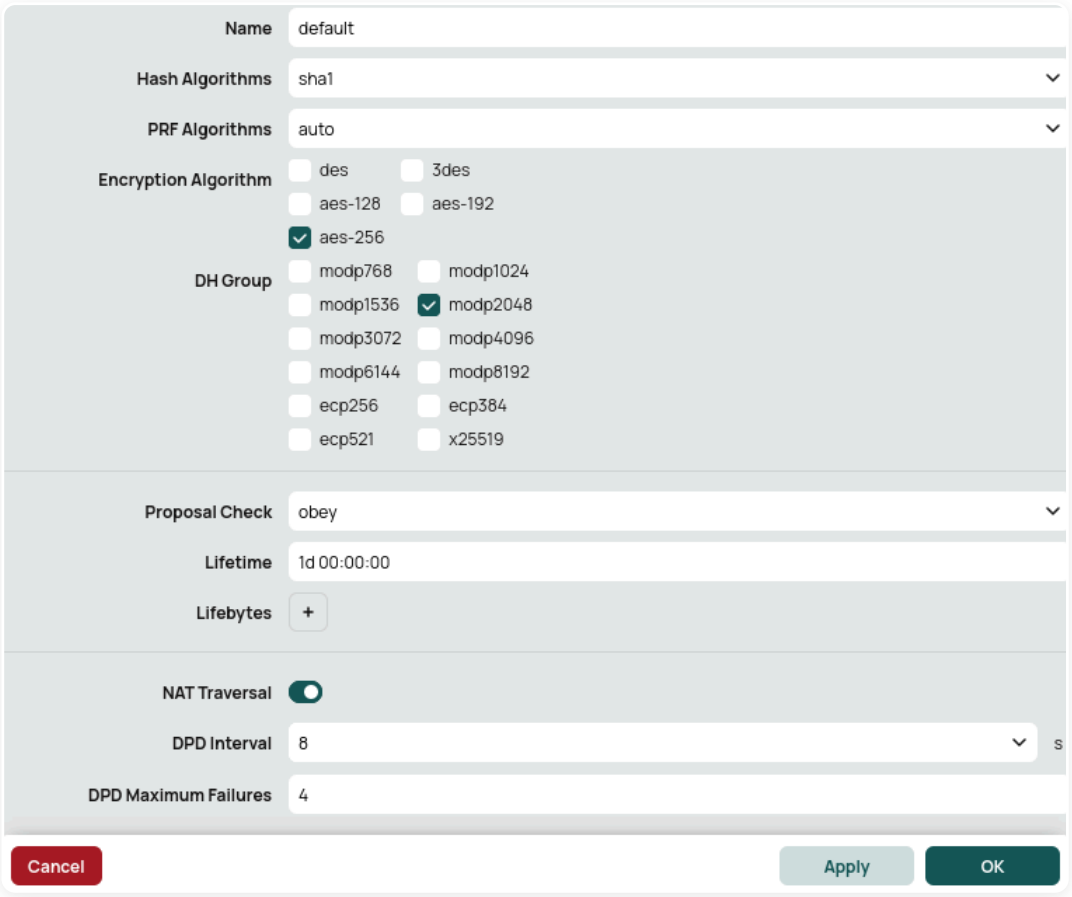
Подключение MikroTik и Ideco NGFW по L2TP/IPsec

Подключение MikroTik к Ideco NGFW по L2TP/IPsec

- Настройте VPN-сервер на Ideco NGFW в разделе **Пользователи** → **VPN-подключения**. Подробная инструкция по настройке - в статье Подключение по L2TP/IPsec;
- Настройте подключение на MikroTik:

Веб-интерфейс

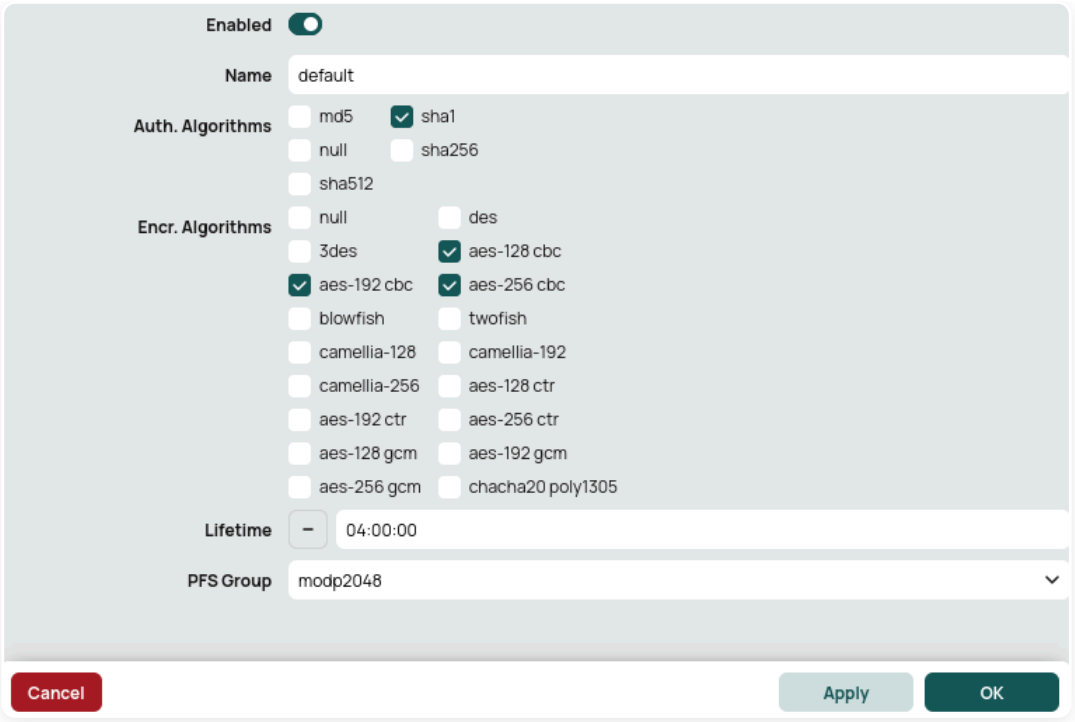
1. Перейдите в раздел **IP** → **IPsec** → **Profiles**, выберите профиль **default** и заполните поля:



- **Hash Algorithms** - `sha1`.
- **Encryption Algorithm** - `aes-256`.
- **DH Group** - `modp2048`.

2. Нажмите **OK**.

3. Перейдите в раздел **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 раздел **Interfaces**, нажмите **New** и выберите **L2TP Client**.

6. Заполните поля:

Расшифровка полей

- **Dial Out**:
  - **Connect To** - IP-адрес Ideco NGFW.
  - **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 раздел **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:

```
interface l2tp-client add connect-to=<server> profile=default disabled=no name=<interface_name> password="<password>" user="<
```

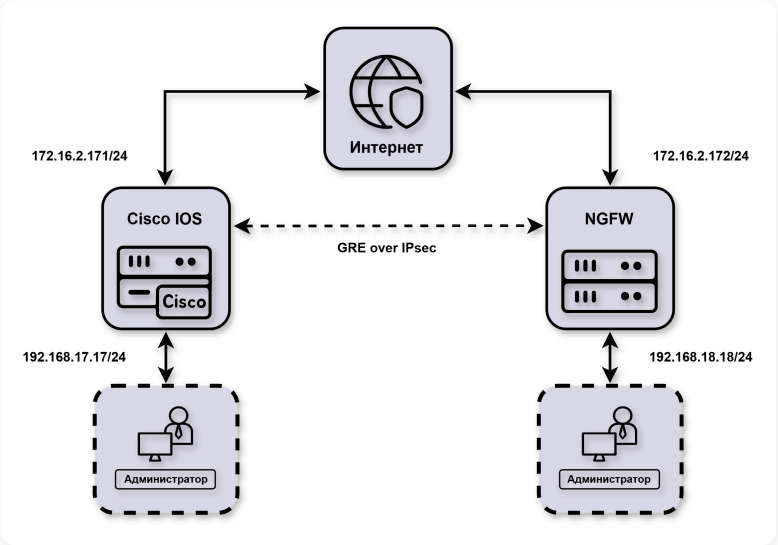
4. Добавьте маршрут до первого адреса VPN-сети NGFW (remote VPN subnet):

```
ip route add dst-address=<remote VPN subnet> gateway=l2tp-out1
```

В Ideco NGFW 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 по IPsec в туннельном режиме

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 следуйте инструкции ниже.

Первоначальная настройка Ideco NGFW и Cisco IOS

Настройка Ideco NGFW

Настройте на Ideco NGFW 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 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 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 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:

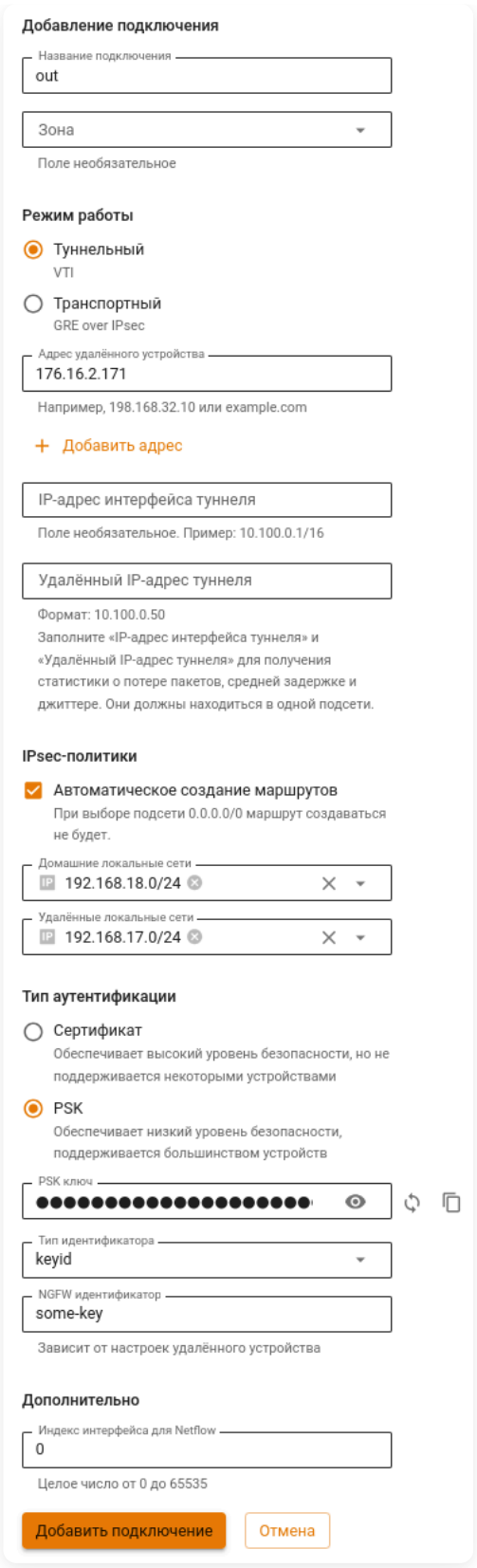
```
write memory
```

Настройка исходящего подключения на Ideco NGFW

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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 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 интрефейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной

подсети.

- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW.
- **Удаленные локальные сети** - укажите локальную сеть Cisco.
- **Тип аутентификации** - PSK.
- **PSK** - будет сгенерирован случайный PSK-ключ. Он потребуется, чтобы настроить подключение 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.

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 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

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:

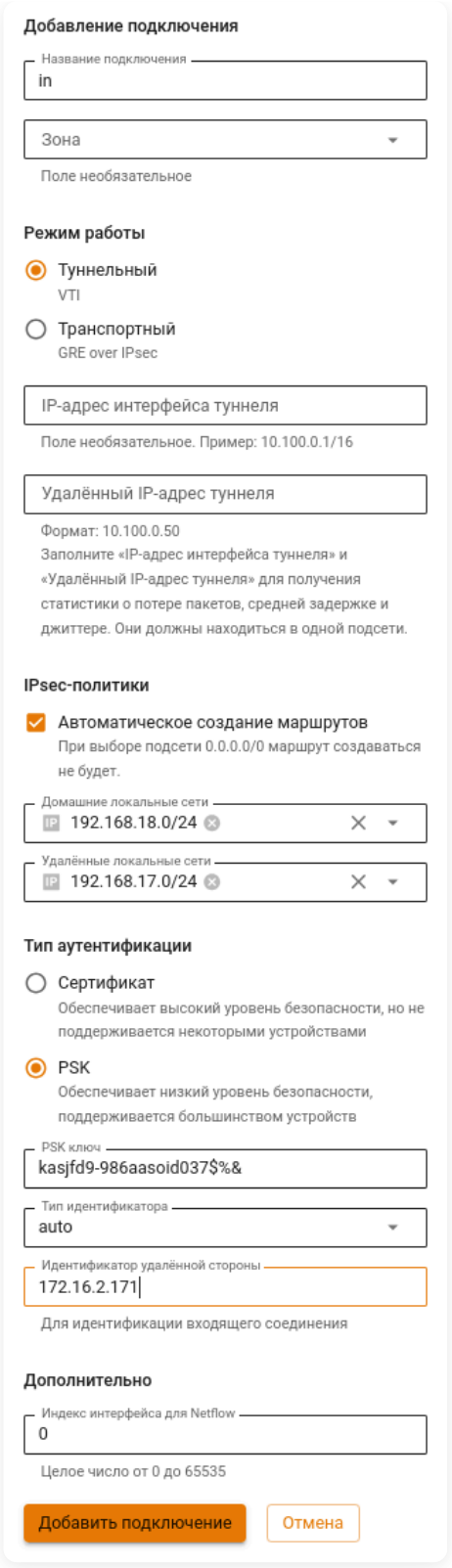
```
write memory
```

Настройка входящего подключения на Ideco NGFW

Для настройки входящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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**.
- **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 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 интрефейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети. заполняется для получения статистики обмена пакетами.
- **Автоматическое создание маршрутов** - включите опцию.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW.
- **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.

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

```
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

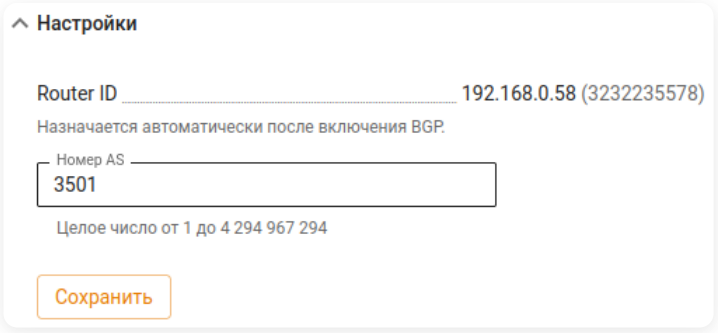
Настройте BGP на роутере:

```
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
```

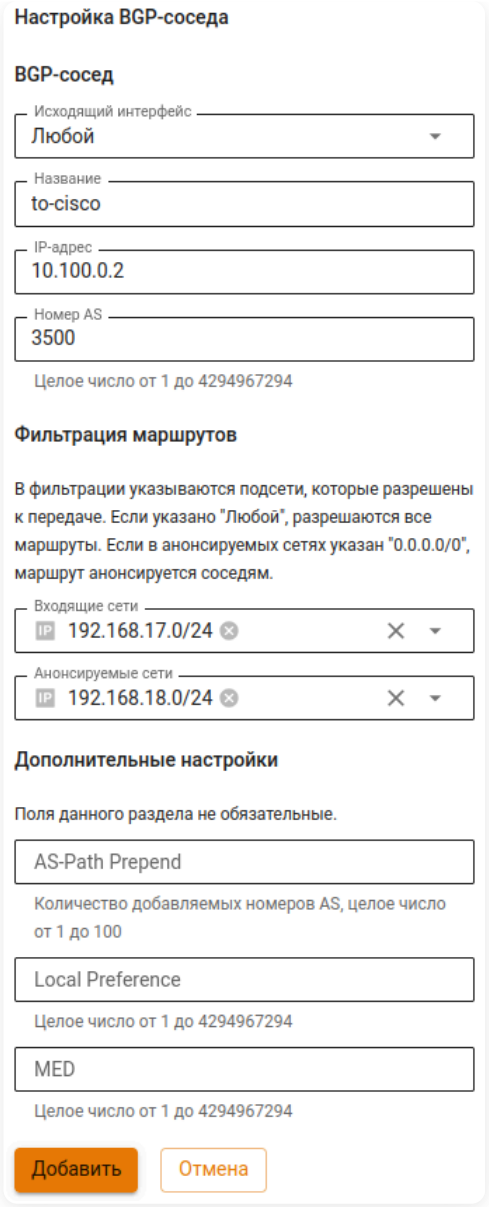
Настройка на Ideco NGFW

1. Перейдите в **Сервисы** → **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.
- **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 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.

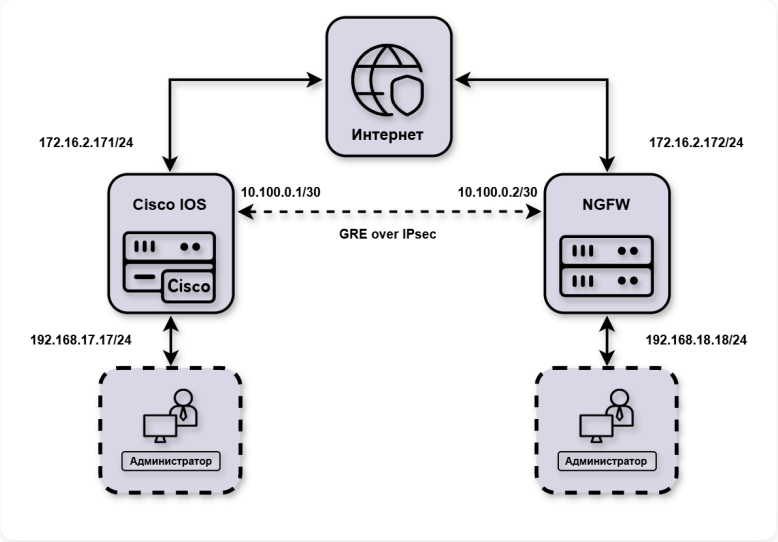
Подключение Cisco IOS и Ideco NGFW по IPsec в транспортном режиме

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 следуйте инструкции ниже.

Перед настройкой подключения убедитесь, что удаленный и локальный IP-адрес GRE-туннеля не используется другим, уже действующим GRE-туннелем в разделе Туннельные. 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 и Cisco IOS

Настройка Ideco NGFW

Настройте на Ideco NGFW 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 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 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 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):

- Для подключения от Ideco NGFW 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:

```
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):

- Для подключения от Ideco NGFW 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:

```
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:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

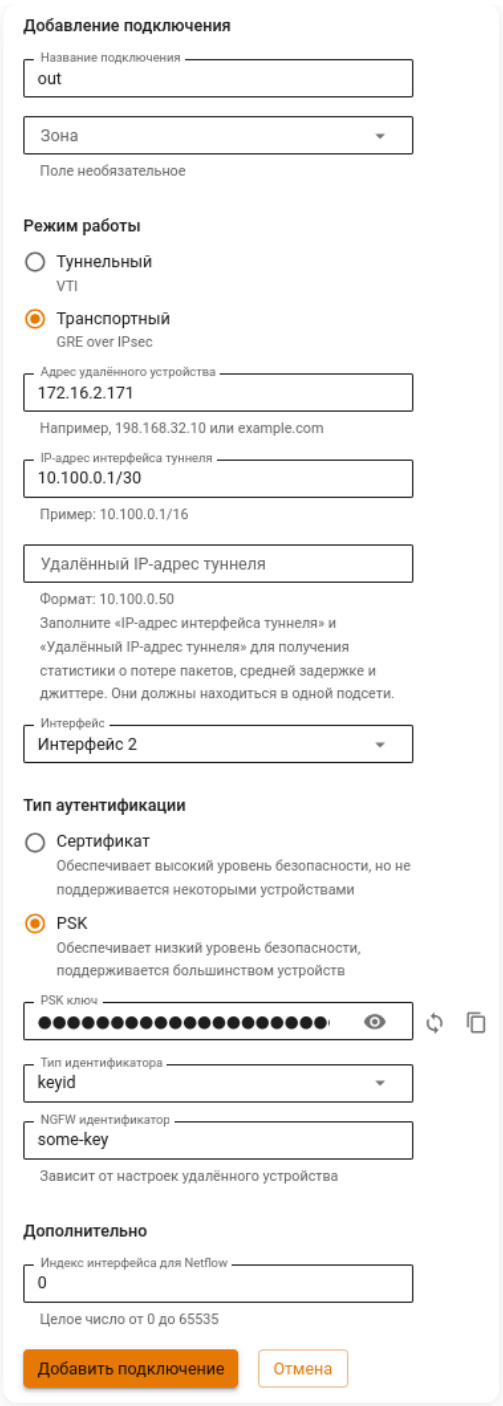
```
write memory
```

Настройка исходящего подключения на Ideco NGFW

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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.
- **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. Он потребуется, чтобы настроить подключение в Cisco.
- **NGFW идентификатор** - 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.

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 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

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):

```
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):

```
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:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP интерфейса туннеля NGFW>
```

9. Сохраните настройки конфигурации:

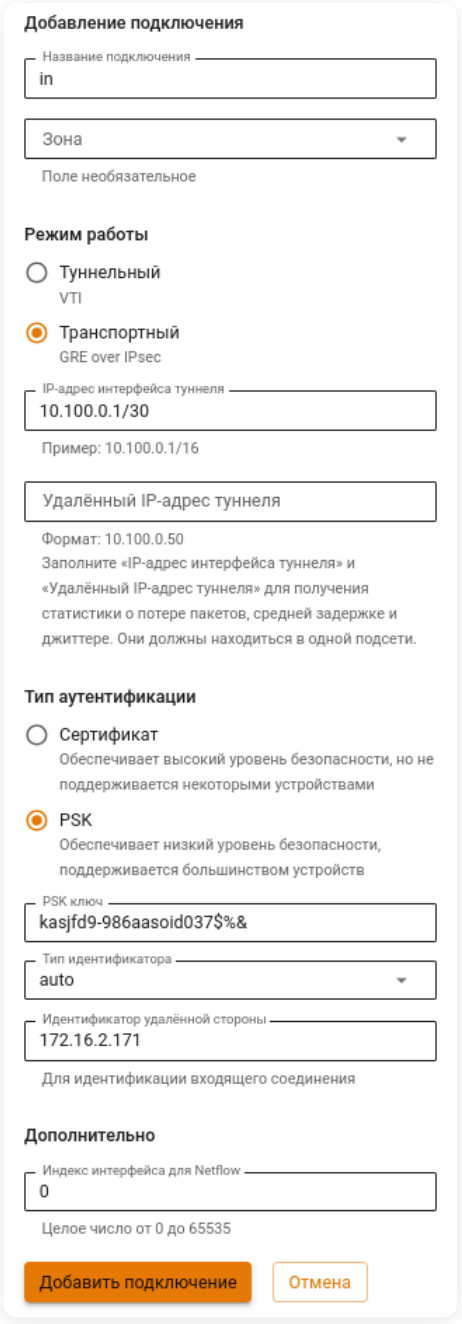
```
write memory
```

Настройка входящего подключения на Ideco NGFW

Для настройки входящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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**.

- **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

```
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

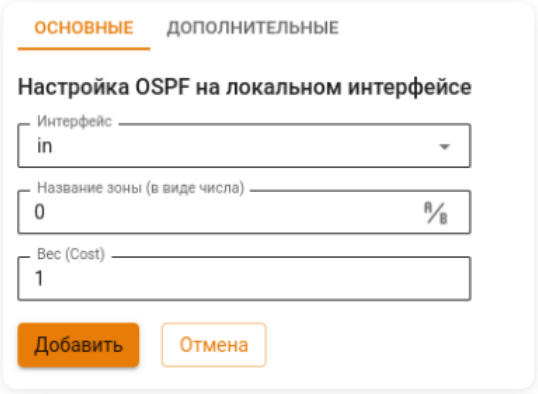
Настройте процесс OSPF на роутере (значение `area` должно совпадать на Cisco и NGFW):

```
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

1. Перейдите в раздел **Сервисы** → **OSPF** и нажмите **Добавить**.

2. Заполните поля:



- **Интерфейс** - выберите GRE-over-Ipsec интерфейс Ideco NGFW, настроенный ранее.
- **Название зоны** - введите номер зоны (значение `area`, должно совпадать на NGFW и Cisco). Можно ввести в виде числа или IP-адреса, нажав иконку A/B.
- **Вес** - введите стоимость маршрута.

3. Нажмите **Сохранить**.

4. Включите модуль **OSPF**.

Для подключения нескольких устройств Cisco к одному Ideco NGFW и передачи маршрутов между всеми устройствами:

1. Создайте для каждого Cisco Gre-over-IPsec подключение к Ideco NGFW.

2. Подключите каждое устройство Cisco по OSPF.

При такой конфигурации локальные сети каждого Cisco будут доступны с Ideco NGFW и других устройств Cisco.

BGP

Настройка на Cisco

Настройте процесс BGP на роутере:

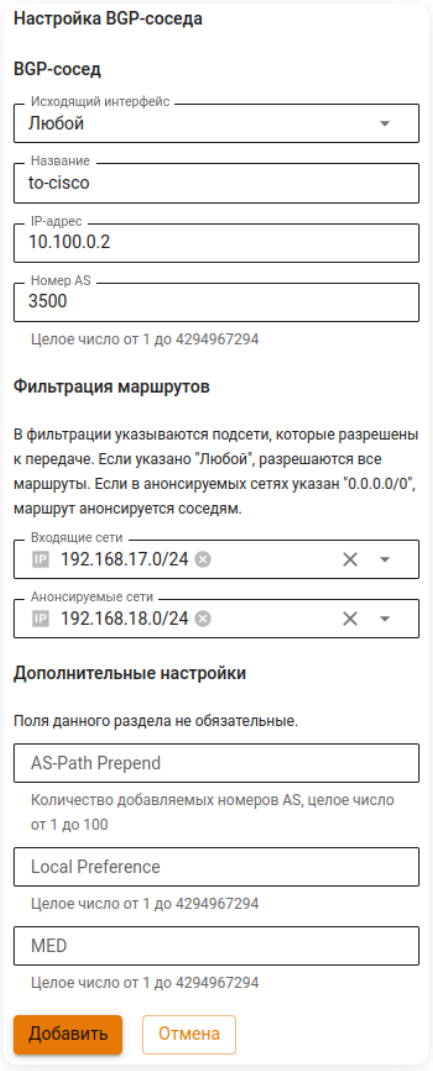
```
conf t
router bgp 3500
 neighbor <IP интерфейса туннеля NGFW> remote-as 3501
 neighbor <IP интерфейса туннеля NGFW> ebgp-multihop 2
 neighbor <IP интерфейса туннеля NGFW> update-source Tunnel0
 !
 address-family ipv4
  network <локальная подсеть Cisco> mask <маска подсети>
  neighbor <IP интерфейса туннеля NGFW> activate
 exit-address-family
```

Настройка на Ideco NGFW

1. Перейдите в раздел **Сервисы** → **BGP** и нажмите **Добавить**.

2. В **Настройках** введите номер автономной системы в строку **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.

4. Заполните **Дополнительные настройки** BGP и нажмите **Сохранить**.

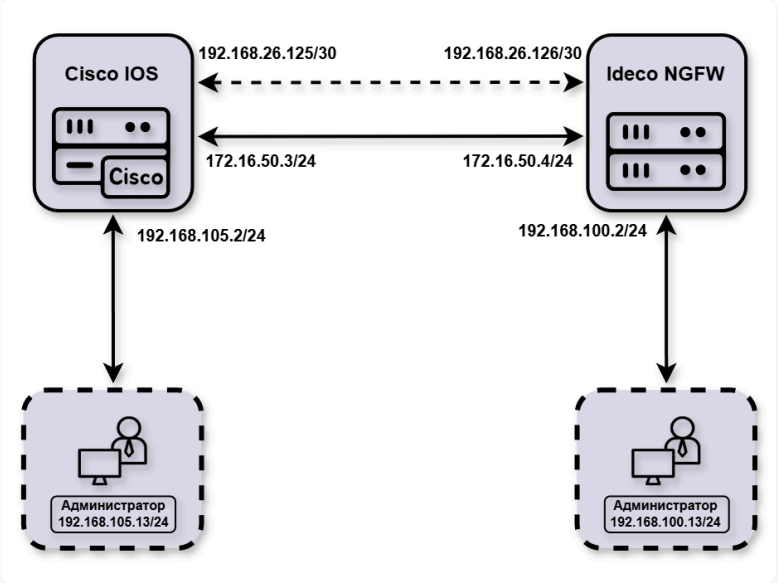
5. Включите модуль **BGP**.



В Ideco NGFW 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 по route-based IPsec

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.

Первоначальная настройка Ideco NGFW и Cisco IOS

Настройка Ideco NGFW

Настройте на Ideco NGFW 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:

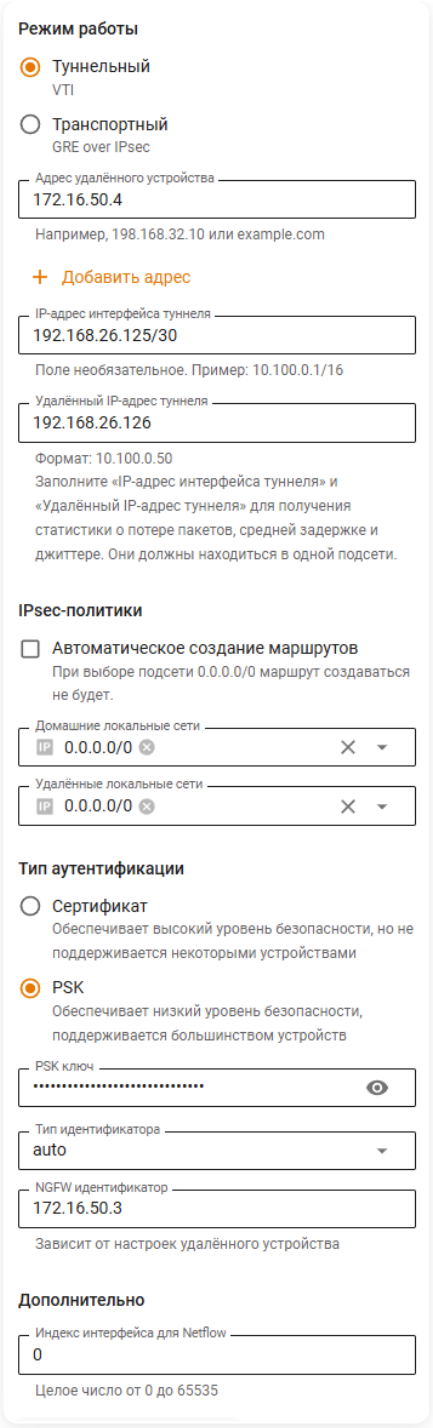
```
write
```

Настройка исходящего подключения на Ideco NGFW

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW 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.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Они должны находиться в одной подсети. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW.
- **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.
- **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 локальными сетями (TCP и web).

Итоговая конфигурация route-based IPsec на Cisco должна выглядеть следующим образом:

Для подключения от Cisco к Ideco NGFW

```
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 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 pfSense к Ideco NGFW по IPsec

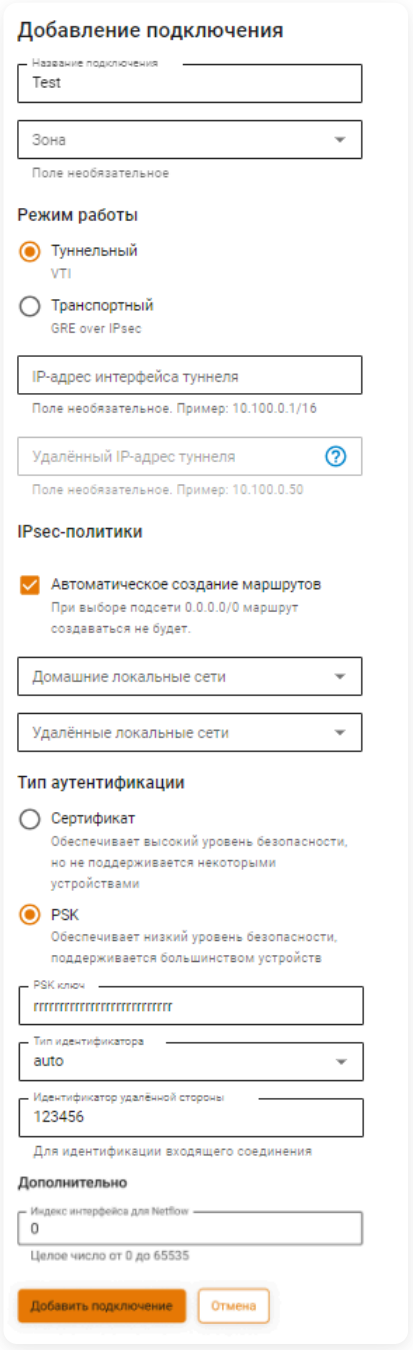
Объединяемые локальные сети не должны пересекаться!

Настройка входящего подключения

Для настройки Ideco NGFW следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW 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**.
- **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** - PSK.
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения.
- **Идентификатор удаленной стороны** - любой.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

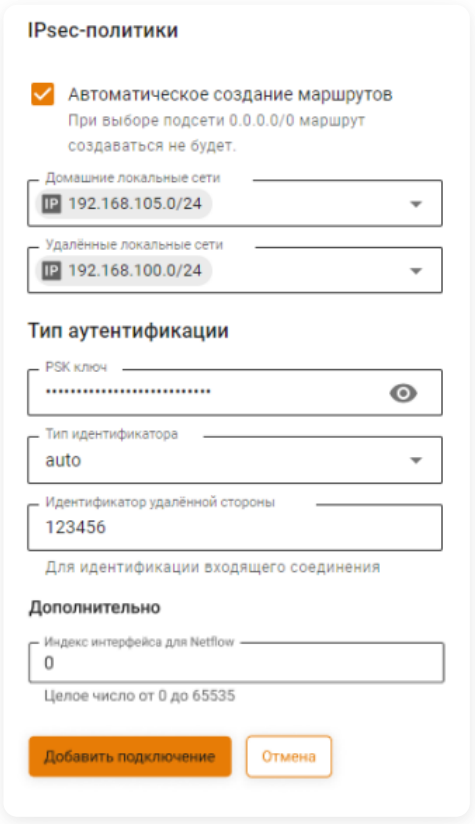
> Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

3. Сохраните созданное подключение, нажмите на кнопку **Включить**.

4. Скопируйте значение идентификатора удаленной стороны одним из способов:

В интерфейсе NGFW

На вкладке **Сервисы** → **IPsec** → **Входящие подключения** в строке **Идентификатор удаленной стороны**:



Через терминал

На Ideco NGFW 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):

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 на вкладку **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;
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;
- **Authentication Method** - Mutual PSK;
- **My identifier и Peer identifier** - сюда вставьте значение строки `id` на Ideco NGFW (см. шаг 4 в настройке Ideco NGFW);
- **Pre-Shared Key** - вставьте PSK-ключ, который ранее прописывали на Ideco NGFW;
- **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;
- **Remote Network** - локальную сеть Ideco NGFW, 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 в настройках файрвола pfSense (переходим на вкладку **Firewall → Rules → IPsec** и создаем два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense).

Обращаем внимание на раздел файрвола WAN - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

7. Теперь переходим на вкладку **Status → IPsec** (там должно появится созданное подключение), нажимаем на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы указали 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 следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW 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.
- **Адрес удаленного устройства** - укажите адрес удаленного устройства.
- **Тип аутентификации** - PSK.
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения.
- **NGFW идентификатор** - любой.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense.
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP.
- **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 на вкладку **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;
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;
- **Description** - любое;
- **Authentication Method** - Mutual PSK;
- **My identifier** - My ip address;
- **Peer identifier** - KeyID tag. Введите идентификатор удаленной стороны, т. е. Ideco NGFW;
- **Pre-Shared Key** - введите PSK-ключ;
- **Encryption Algorithm**:
  - Для **Ideco UTM версии 10.0 и Ideco NGFW 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 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;
- **Remote Network** - локальную сеть Ideco NGFW, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. В настройках файрвола pfSense перейдите на вкладку **Firewall** → **Rules** → **IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense.

7. Обратите внимание на раздел файрвола **WAN** - в нем по умолчанию запрещен входящий трафик из "серых" подсетей, который требуется разрешить.

8. Перейдите на вкладку **Status** → **IPsec** (там должно появится созданное подключение), нажмите на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы 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 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 Kerio Control и Ideco NGFW по IPsec

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.

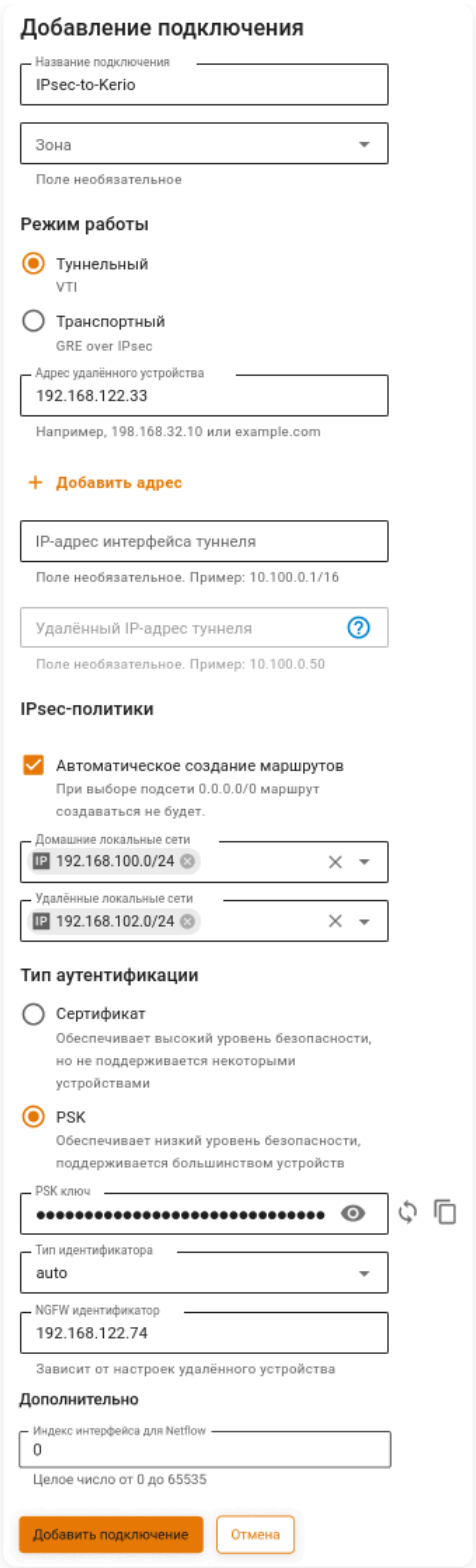
2. В разделе **Правила трафика** разрешите трафик VPN-служб.

Подключение от Ideco NGFW к Kerio Control

Настройка исходящего подключения на Ideco NGFW

1. В веб-интерфейсе Ideco NGFW 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. Можно указать несколько адресов. NGFW установит отдельные туннели с каждого своего WAN-интерфейса на каждый адрес из списка. Если необходимо резервирование туннелей, настройте для каждого адреса отдельное IPsec-подключение.
- **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, которая будет видна из подсети Kerio Control.
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW.
- **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, 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**. Они должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

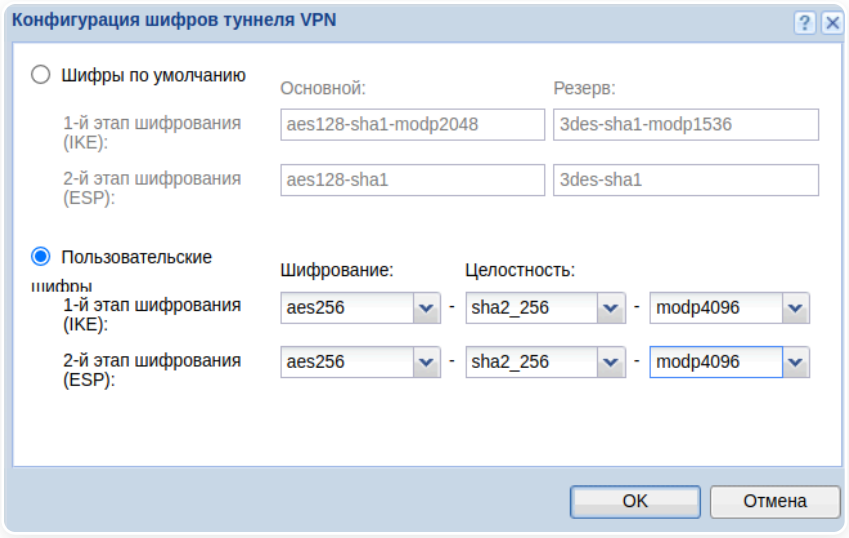
Настройка завершена, теперь переходим к настройке Kerio Control.

Настройка входящего подключения на Kerio Control

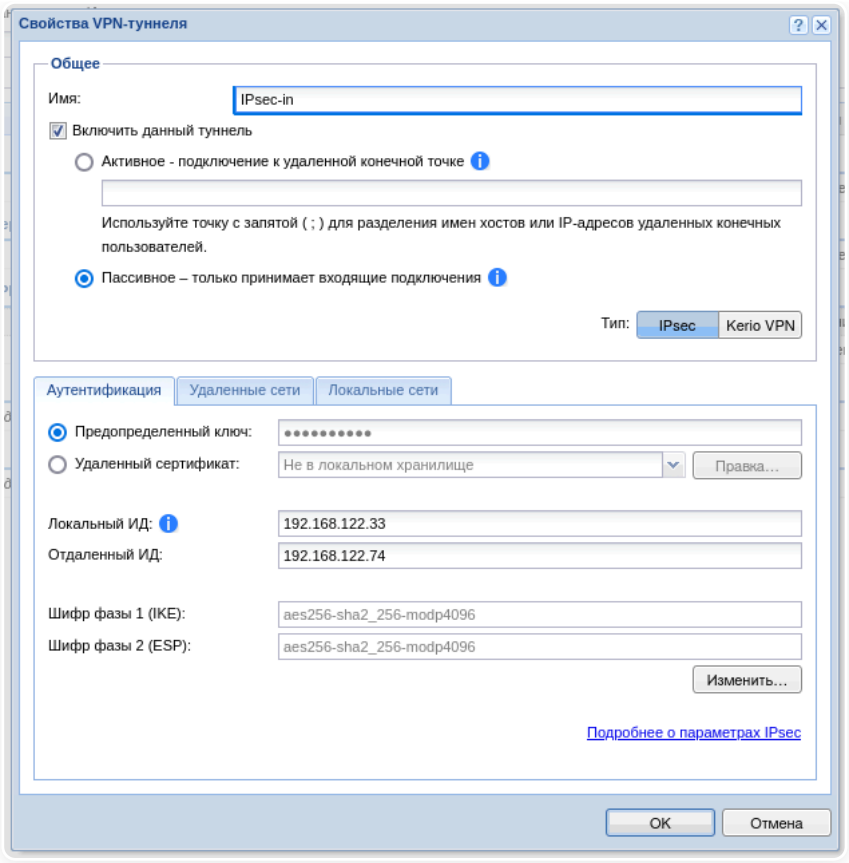
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель...**.

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;
- **Локальный ИД** - укажите IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения;
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW;
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



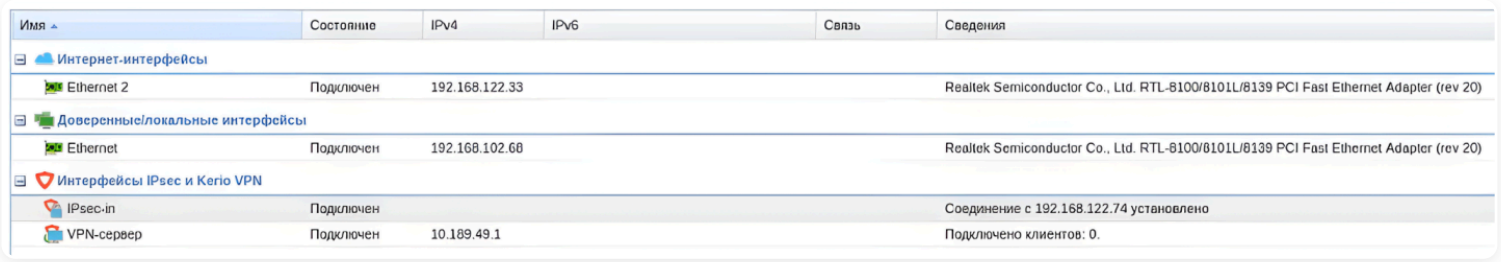
Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW, которая будет видна из подсети Kerio Control.

4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице:



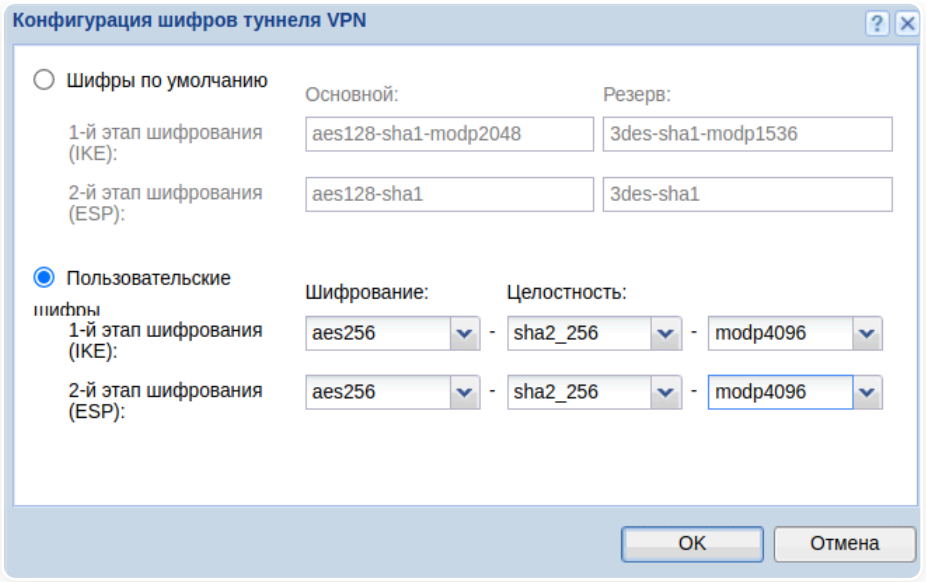
Подключение от Kerio Control к Ideco NGFW

Настройка исходящего подключения на Kerio Control

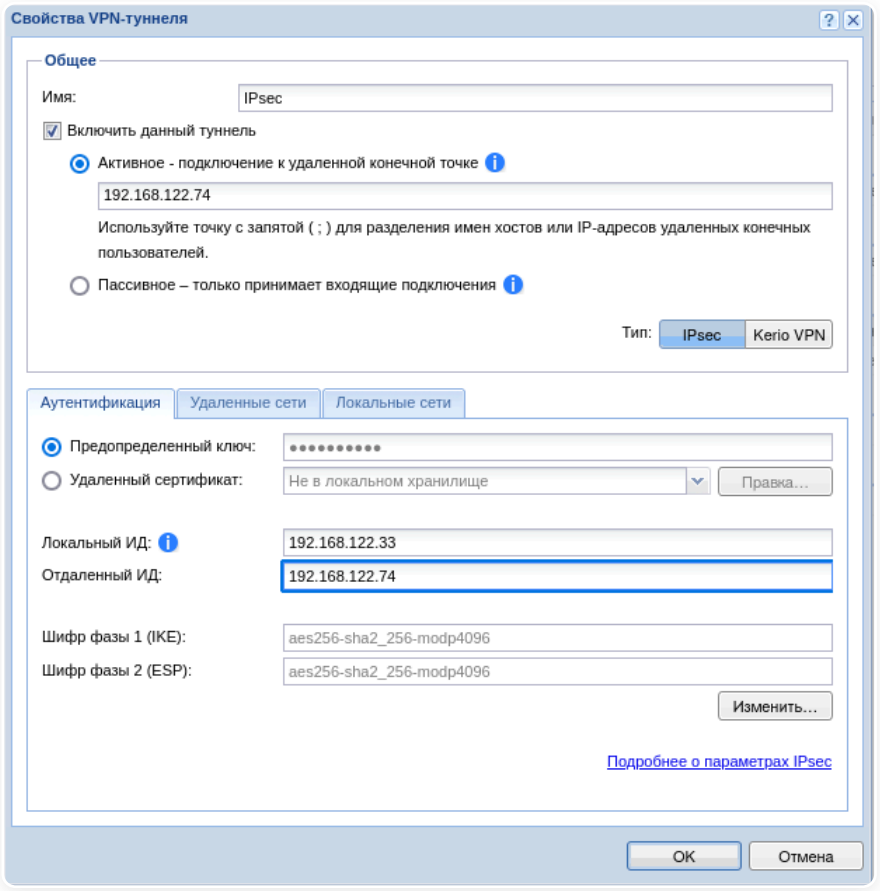
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель...**.

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, 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, 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, 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, которая будет видна из подсети Kerio Control.

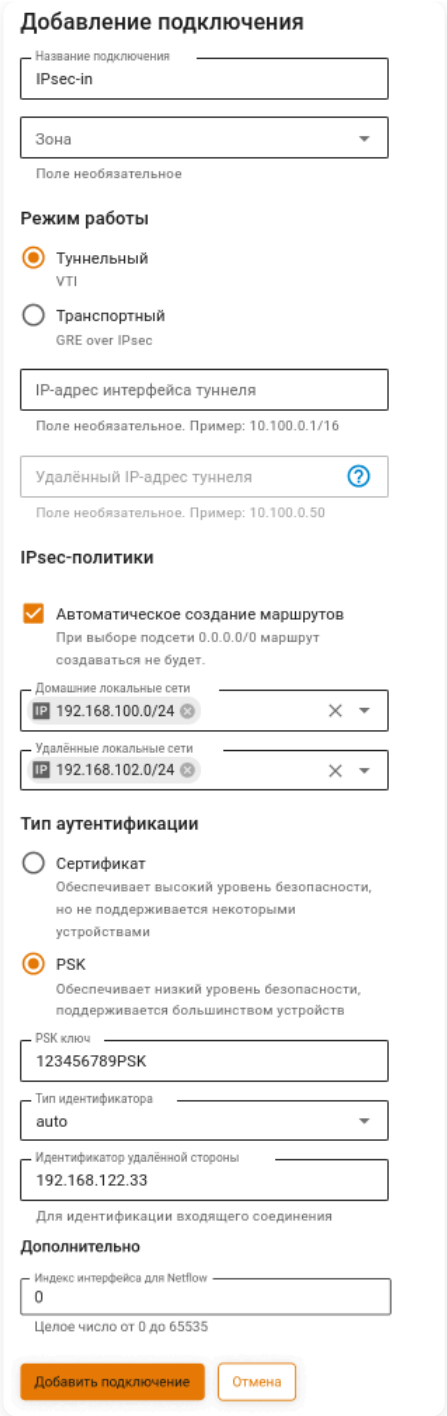
4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице.

Настройка входящего подключения на Ideco NGFW

1. В веб-интерфейсе Ideco NGFW 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**.
- **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, которая будет видна из подсети Kerio Control.
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW.
- **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. Они 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 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 Keenetic по SSTP или IPsec

> В статье описана настройка VPN-соединения между маршрутизатором Keenetic и Ideco NGFW.

Для создания подключения используются протоколы:

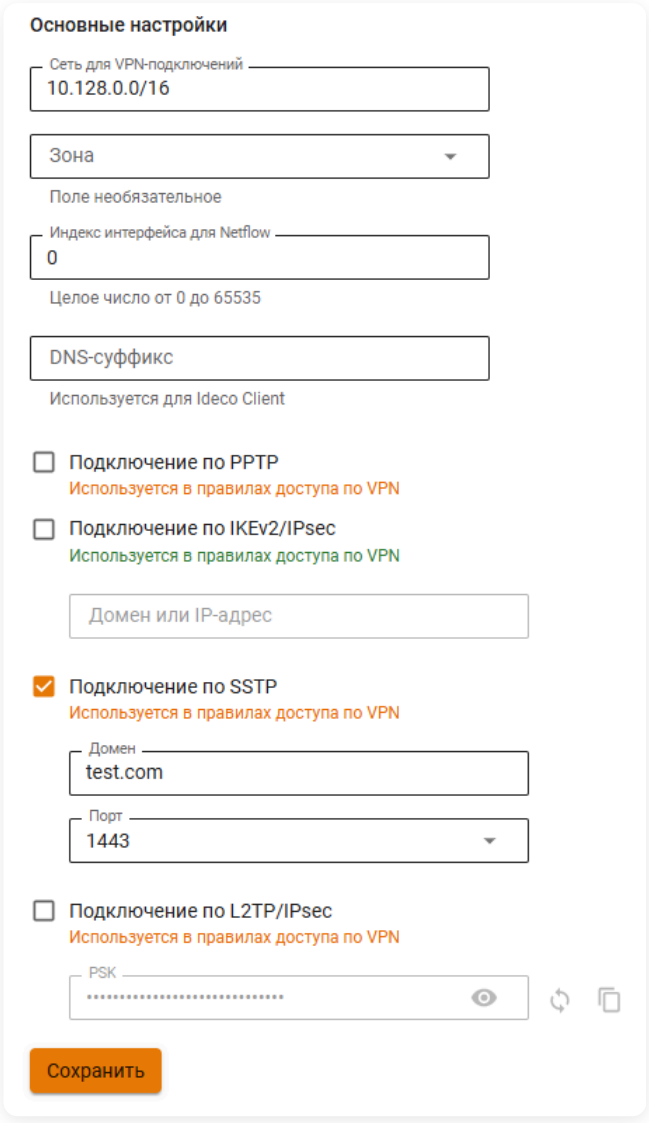
- **SSTP** - для безопасного соединения между клиентом и сервером.
- **IPsec** - для безопасной передачи данных в IP-сетях.

Подключение по SSTP

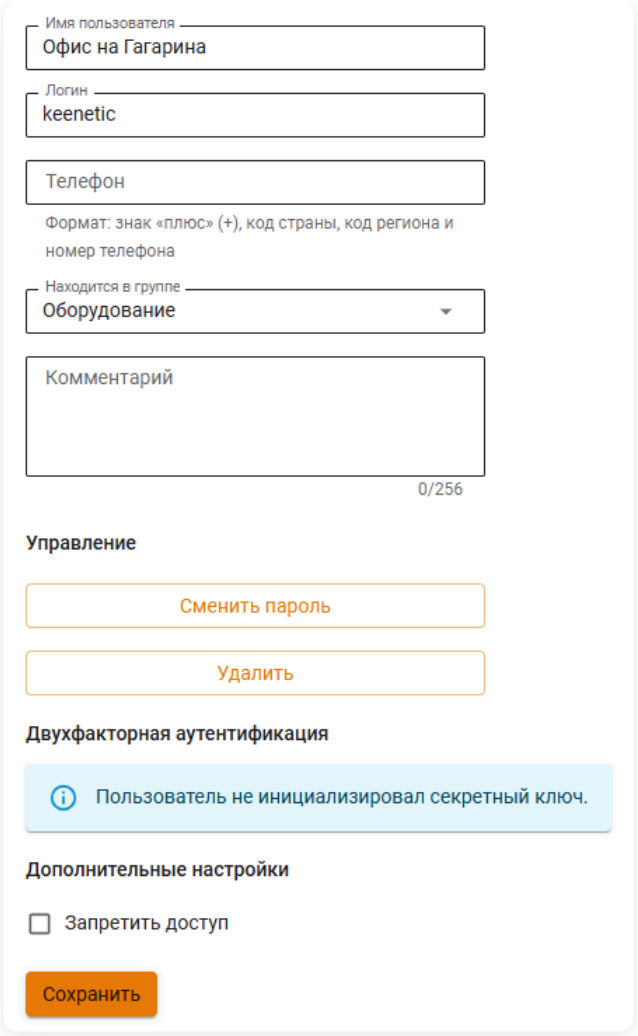
Если доступ из центрального офиса в сеть за Keenetic не нужен, воспользуйтесь инструкцией по подключению в режиме client-to-site.

Настройка Ideco NGFW

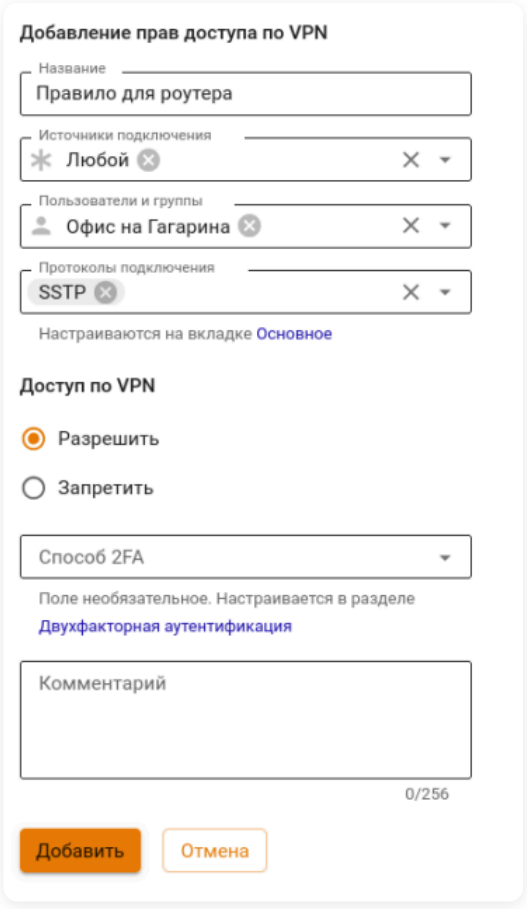
1. Перейдите в **Пользователи** → **VPN-подключения** → **Основное**, включите настройку SSTP, укажите домен и порт для подключения:



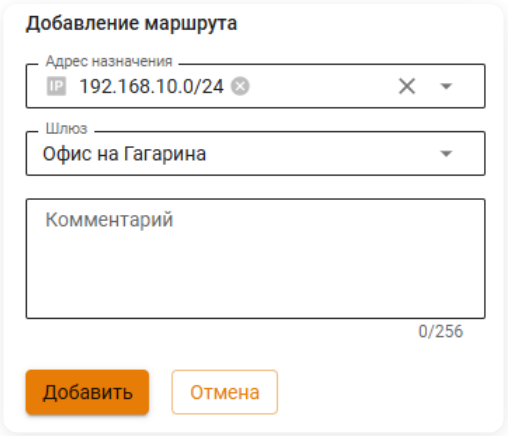
2. Перейдите в **Пользователи** → **Учетные записи** и создайте специального пользователя для удаленного роутера. Логин и пароль пользователя будут использоваться на роутере:



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 **Сервисы** → **Маршрутизация** → **Локальные сети**:



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.

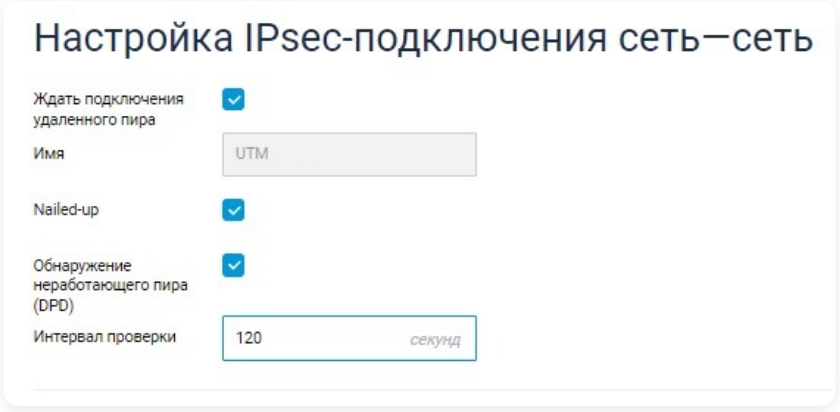
Доступ часто блокируется в Windows из-за настроек сетевых профилей.

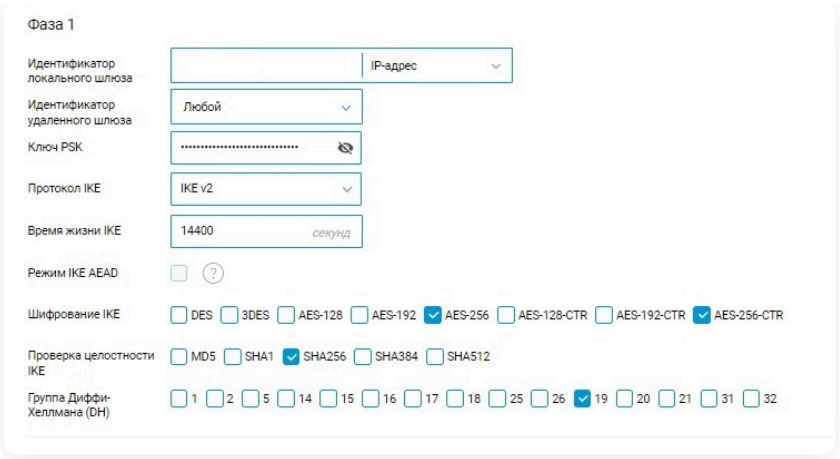
Разрешите доступ до внешних сетей во всех профилях, выполнив команду в PowerShell (запущенного с правами администратора):
`Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`

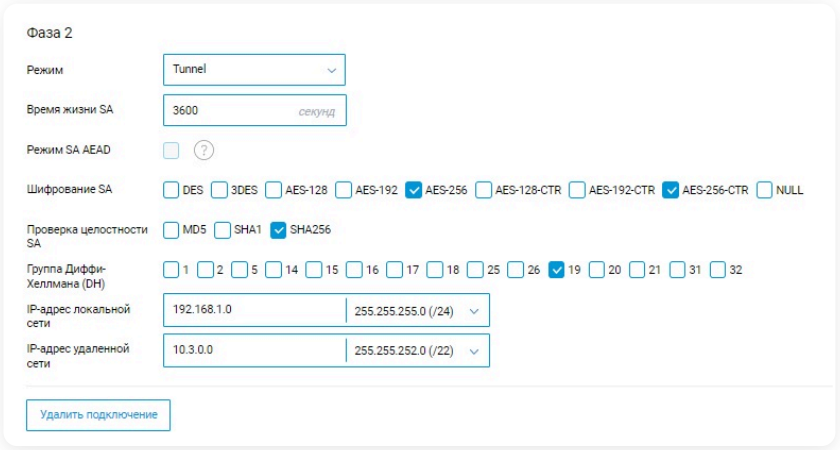
Подключение по IPsec

На стороне Ideco NGFW 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 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**

ГОСТ VPN

ГОСТ VPN - это сервис для организации защищенных каналов связи между несколькими Ideco NGFW с использованием технологии виртуальной частной сети. Соединение шифруется согласно требованиям ФСБ по ГОСТ-алгоритмам с применением российского сертифицированного решения от компании Рутокен.

Раздел **ГОСТ VPN** недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

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

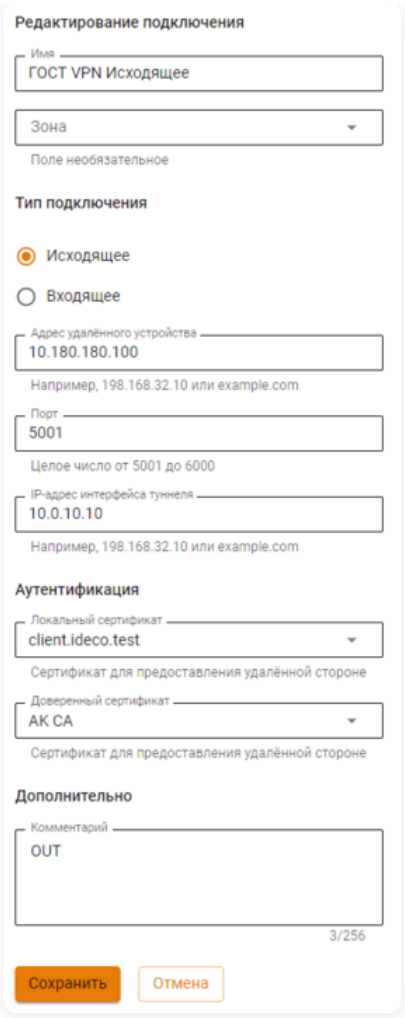
Для настройки ГОСТ VPN необходимо подготовить два USB-токена в соответствии с инструкцией, представленной в статье, и подключить токены к USB-портам серверов.

В случае извлечения USB-токена или истечения срока действия сертификатов, хранящихся на USB-токене, VPN-соединение будет разорвано.

Настройка исходящего подключения

1. Перейдите в раздел **Сервисы** → **ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



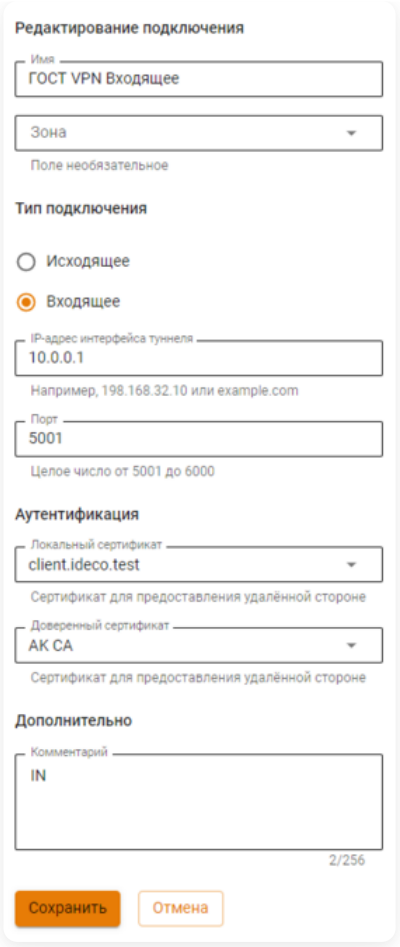
Расшифровка полей

- **Имя** - введите имя подключения, максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым.
- **Тип подключения** - выберите **Исходящее**.
- **Адрес удаленного устройства** - введите доменное имя или белый IP-адрес удаленного Ideco NGFW.
- **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 раздел **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.
- **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.

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

Сертификаты

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

Логика работы

NGFW позволяет выпустить или загрузить корневые и некорневые (пользовательские) сертификаты:

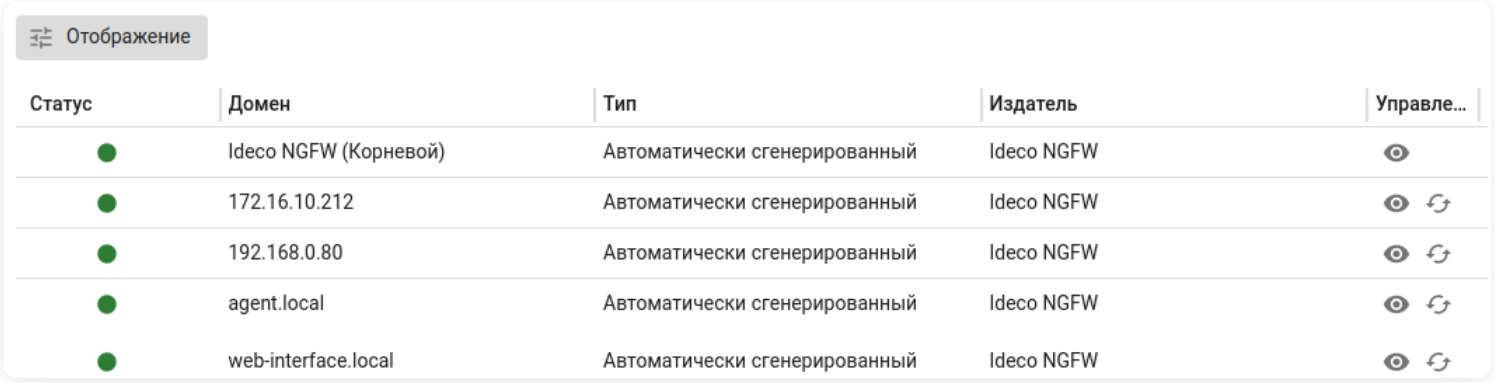
- **Корневые сертификаты** обязательно должны содержать атрибут **X509v3 Basic Constraints: CA: TRUE** для выпуска дочерних сертификатов. При первоначальной установке и запуске NGFW корневой (самоподписанный) сертификат генерируется автоматически. Сертификат можно скачать, перейдя в **Сервисы** → **Сертификаты** → **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).

NGFW 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:

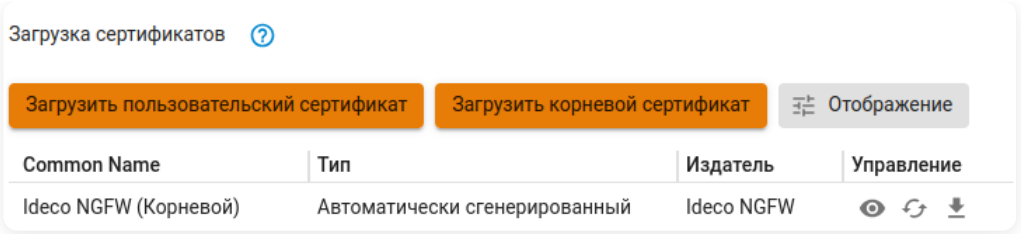


Если в таблице **Действующие сертификаты** одна и та же цепочка сертификатов указана в нескольких строках, значит, она используется несколькими модулями.

Загруженные сертификаты

В таблице **Загруженные сертификаты** отображаются:

- Все загруженные цепочки сертификатов.
- Корневой сертификат Ideco NGFW:

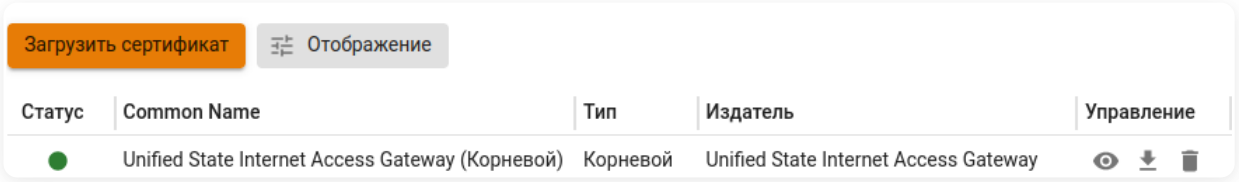


Требования к SSL-сертификатам и инструкция по загрузке в статье.

Системные сертификаты

Раздел позволяет загружать свои сертификаты в хранилище доверенных сертификатов ОС Fedora на NGFW. Подробнее о системных сертификатах - по ссылке.

После добавления сертификата в таблицу **Системные сертификаты** перезагрузите Ideco NGFW. После перезагрузки Ideco NGFW будет доверять загруженному сертификату и всем сертификатам, подписанным загруженным сертификатом:



Загрузка в **Системные сертификаты** необходима, если Ideco NGFW взаимодействует с сервисами, защищенными сертификатом от корпоративного или самоподписанного центра сертификации (CA). Чтобы Ideco NGFW 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.

Управление сертификатами

- просмотр основной информации о сертификате.
- перевыпуск сертификата.
- скачать сертификат.
- удалить загруженный сертификат.

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 NGFW для выпуска и подписания дочерних сертификатов.

Процесс выпуска сертификата

NGFW 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.
- Открытый 80 TCP-порт на внешнем интерфейсе. После установки Ideco NGFW 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** 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 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 автоматически сгенерированные NGFW 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

Некорневая цепочка сертификатов

Чтобы перевыпустить некорневую цепочку сертификатов, нажмите в столбце **Управление** таблицы **Действующие сертификаты**. NGFW 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 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**. NGFW заменит ее на автоматически сгенерированный корневой сертификат.

Для работы Ideco Client под MacOS необходимо, чтобы срок действия сертификата на домен или IP-адрес NGFW, введенный в разделе **Пользователи** → **Ideco Client**, не превышал 825 дней.

Проверить, что срок действия загруженного пользовательского или сгенерированного NGFW 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 NGFW, нажав .

Чтобы проверить, перевыпустился ли сертификат на новый срок, нажмите .

Загрузка SSL-сертификата на сервер

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Требования к сертификату

Перед загрузкой корневого или пользовательского сертификата на Ideco NGFW 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 NGFW**.

Если вы хотите загрузить сертификат как корневой, удостоверьтесь, что он может выдавать дочерние сертификаты: **X509v3 Basic Constraints: CA: TRUE** (это можно проверить в открытом ключе сертификата).

Загрузка SSL-сертификата на NGFW

Если сертификат удовлетворяет всем перечисленным выше условиям, загрузите его на NGFW. Для этого:

1. Перейдите в раздел **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 NGFW. 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 в качестве корневого. Это позволит выстроить цепочку доверия для автоматически выданных сертификатов до корневого центра сертификации. Пользовательские компьютеры будут доверять сертификатам, выданным на стороне NGFW.

Подготовка SSL-сертификата для загрузки на NGFW

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 NGFW.

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 он имеет структуру:

```
-----BEGIN CERTIFICATE-----
..............
..............
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
..............
..............
-----END PRIVATE KEY-----
```

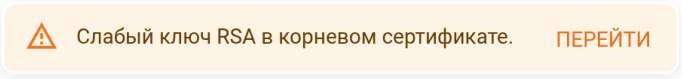
Если в сертификате написано `--BEGIN ENCRYPTED PRIVATE KEY--`, расшифруйте его, введя в OpenSSL команду

`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

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.

```
Установите последнюю версию PowerShell для новых функций и улучшения! https://aka.ms/PSWindows

PS C:\Users\a.istomina> New-SelfSignedCertificate -DnsName test.ideco.com -TextExtension @("2.5.29.19={text}CA=true") -C
ertStoreLocation cert:\LocalMachine\My


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
2284919151C5C624341D7B75FE034B00DF6A44FA  CN=test.ideco.com
```

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 его корректность 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

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

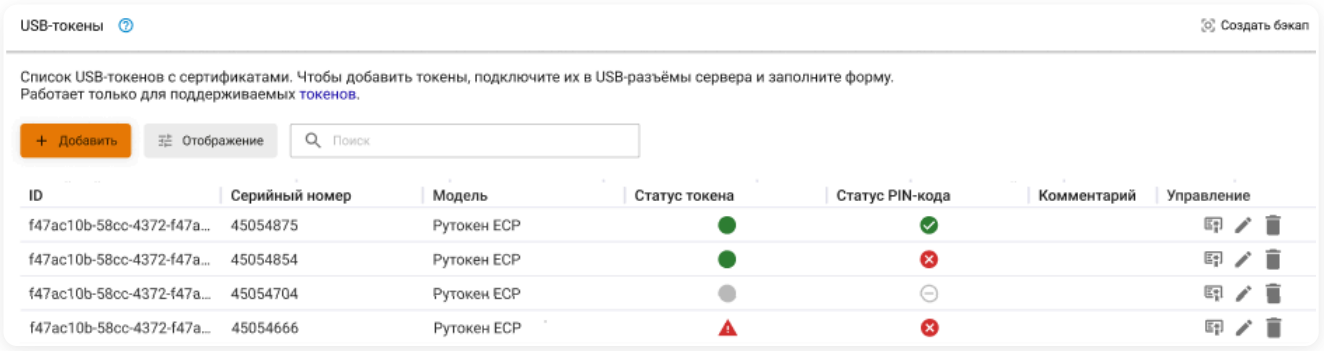
USB-токены

USB-токен - это аппаратное устройство для безопасного хранения цифровых сертификатов и работы с приватными ключами.

Раздел **USB-токены** недоступен в Ideco UTM ФСТЭК. Функциональность появится в следующих сертифицированных версиях.

Ideco NGFW поддерживает только USB-токен модели **Рутокен ЭЦП 3.0**. USB-токены других моделей могут не отображаться в веб-интерфейсе **Ideco NGFW**.

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 его 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.

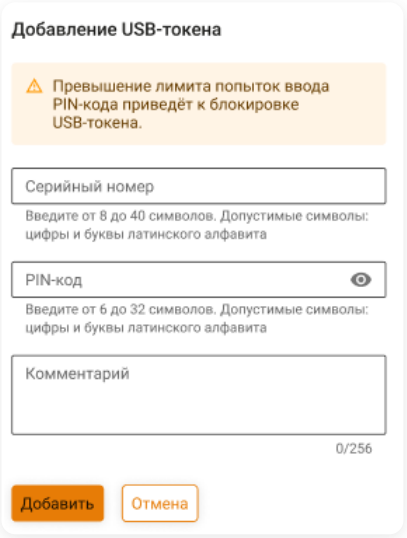
Если требуется сгенерировать сертификаты для тестирования ГОСТ VPN, рекомендуем воспользоваться статьей от производителя.

Настройка USB-токена на Ideco NGFW

Для работы Ideco NGFW с USB-токеном введите корректный PIN-код. После этого NGFW сможет использовать токен для настройки ГОСТ VPN.

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`.
- **PIN-код** - на токенах от компании Рутокен установлен PIN-код по умолчанию: `12345678`.
- **Комментарий** - необязательное поле.

Отчеты и журналы

В этом разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

Трафик

В разделе представлена статистика из **Контроля приложений** и **Контент-фильтра**

Перейти >

Системный журнал

Таблица логов работы служб

Перейти >

Журнал веб-трафика

В разделе представлен результат проверки трафика антивирусом и модулем **Контент-фильтр**

Перейти >

Журнал трафика

В разделе представлена таблица о срабатывании правил **Файрвола**

Перейти >

События безопасности

Статистика событий модулей WAF и IPS, а также графики событий IPS

Перейти >

Действия администраторов

В разделе представлена таблица о действиях администраторов в Ideco NGFW

Перейти >

Аутентификация администраторов

Таблица аутентифицированных на Ideco NGFW администраторов

Перейти >

Журнал аутентификации

В разделе представлена таблица аутентифицированных на Ideco NGFW пользователей

Перейти >

Журнал авторизации ЛК

В разделе представлена таблица сессий пользователей, авторизованных в личном кабинете Ideco NGFW

Перейти >

Конструктор отчетов

Создание шаблонов отчетов и настройка рассылки на электронную почту

Перейти >

Syslog

Настройка передачи системных сообщений (syslog) Ideco NGFW в сторонние коллекторы или в SIEM-системы

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Трафик

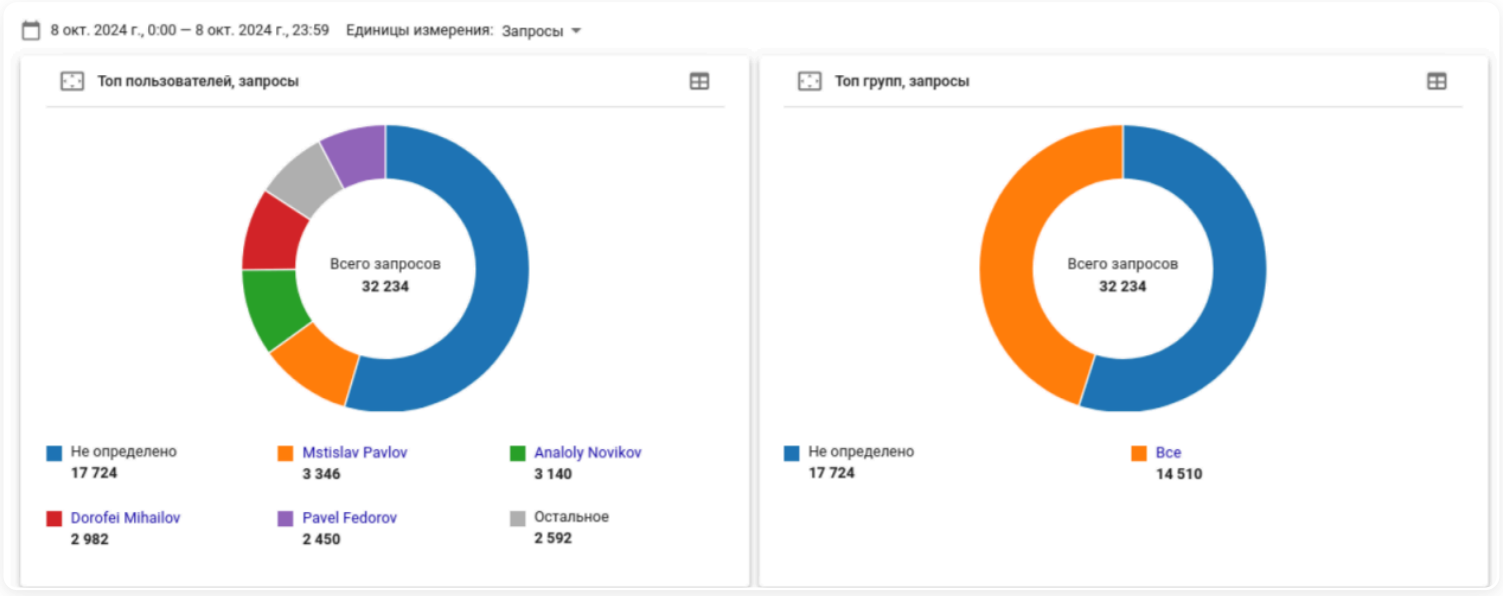
При переводе ползунка **Трафик** в левом верхнем углу в положение **Включен** раздел начинает собирать статистику из Контент-фильтра и отображается в виде виджетов.

Способы отображения информации:

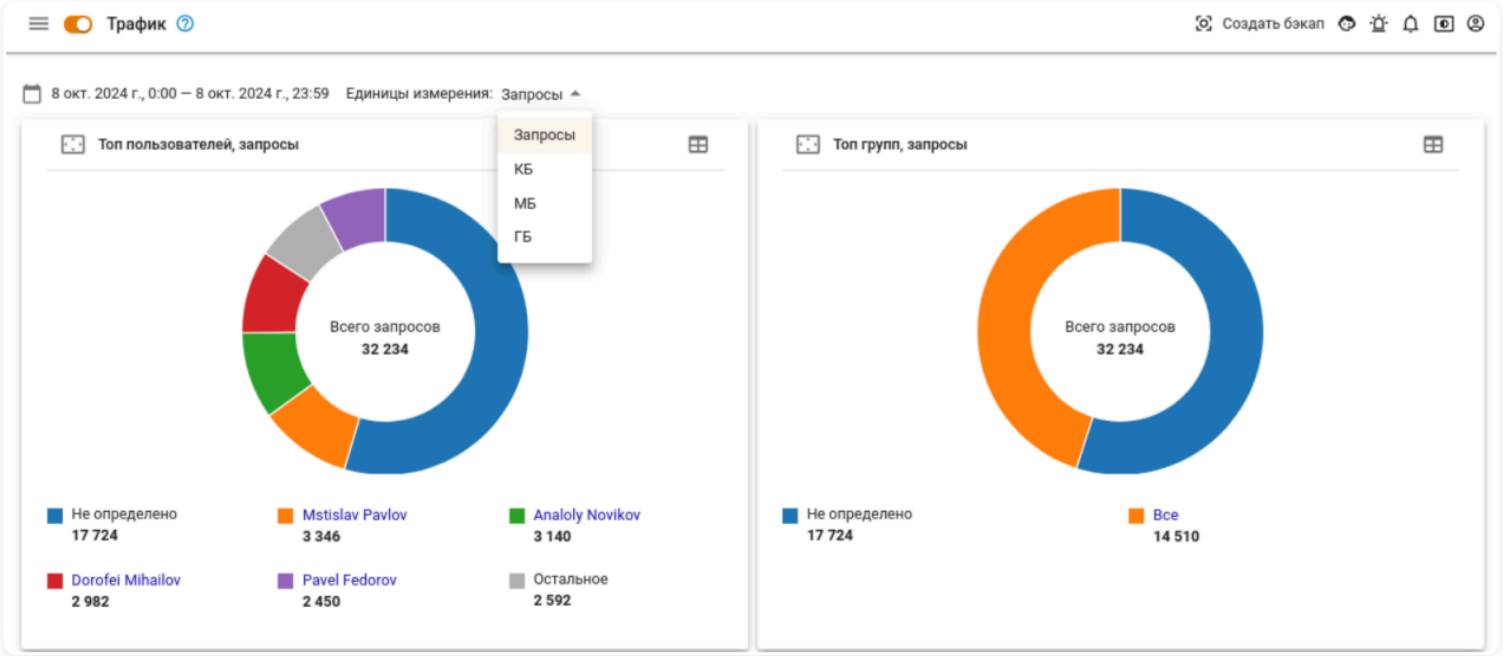
- Круговая диаграмма ( ) и таблица ( );
- Развернутый режим ( ).

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:

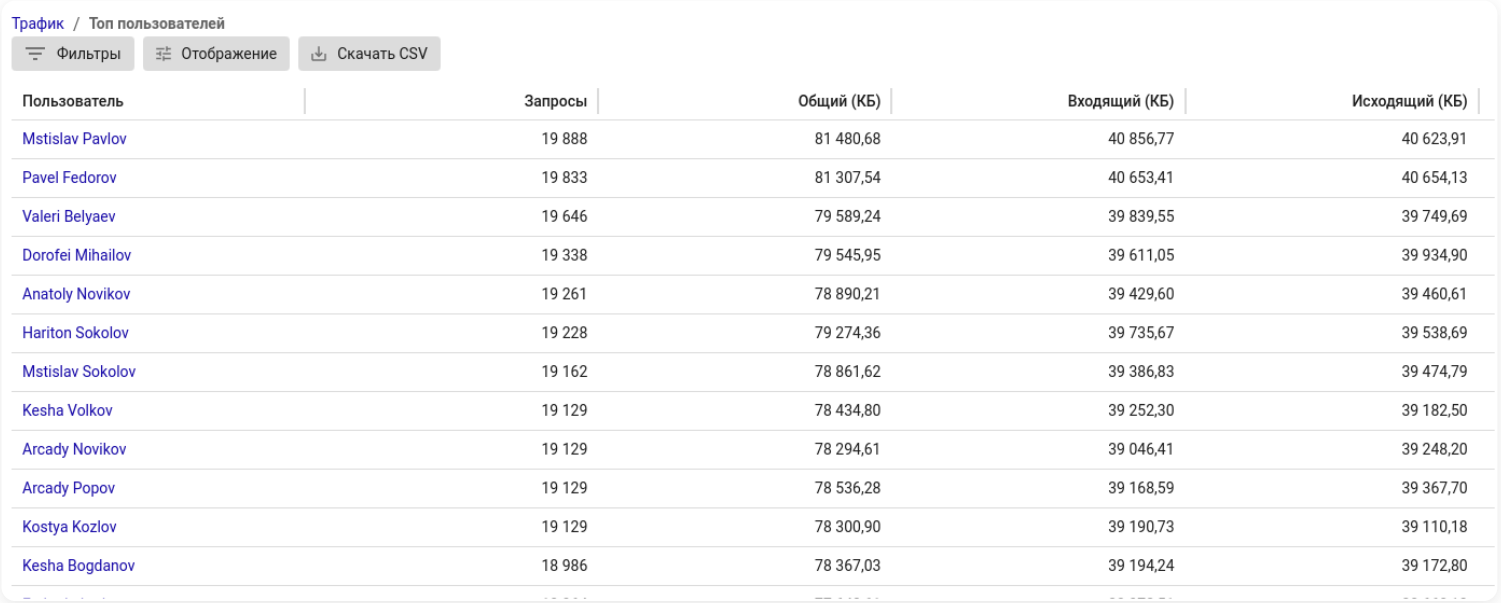


Не определено (трафик с неизвестным адресом и пользователем) - это любой трафик от самого Ideco NGFW. Например, скачивание баз

Контент-фильтра, GeoIP, сигнатур и т.д.

Развернутый режим

Содержит данные по всем объектам из топа. Для поиска по объектам воспользуйтесь **Фильтром** (Фильтры).


Трафик / Топ пользователей

Фильтры | Отображение | Скачать CSV

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 кликните по нему.

  Если пользователя нет в списке, то нажмите **Развернуть** ( ) в левом верхнем углу виджета (откроется список всех пользователей);
- В виджете **Топ заблокированных сайтов** NGFW 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 кликните по нему. Если его нет в списке, то нажмите **Развернуть** ( );
- Чтобы увидеть список всех пользователей, у которых был заблокирован этот протокол, на открывшейся странице найдите виджет **Топ пользователей**

  и нажмите **Развернуть** ( ).

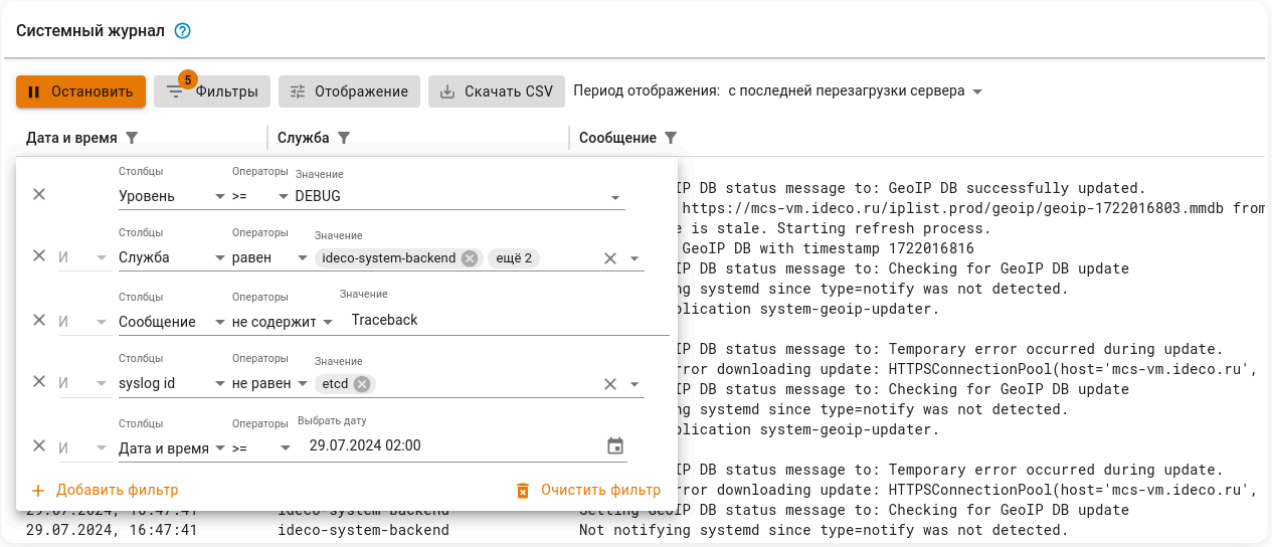
Подробнее о создании собственных шаблонов со статистикой - в статье Конструктор отчетов.

Системный журнал

Время хранения логов в разделе **Журналы** - 90 дней. Для событий служб **strongswan**, **squid**, **ideco-app-control**, **fail2ban** срок хранения - 14 дней, для **ideco-conndrop** - 2 дня.

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 **Файрвола**.

Алгоритм работы службы:

1. Присваивает соединению метку `ideco-irreversible-drop` при срабатывании запрещающего правила **Файрвола**.
2. Каждую минуту выполняет фильтрацию записей с меткой `ideco-irreversible-drop` и удаляет их.

Защита от брутфорс-атак

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
Веб-интерфейс	ideco-web-interface
Двухфакторная аутентификация	ideco-two-factor-codes

Модуль	Имя службы
Личный кабинет пользователя	ideco-user-cabinet
Обратный прокси	ideco-reverse-proxy, ideco-reverse-proxy-conn, ideco-reverse-proxy-req
Почтовые службы	ideco-dovecot, ideco-postfix-connrate, ideco-postscreen-prgrt, ideco-roundcube, ideco-smtp, ideco-smtp-rcpt

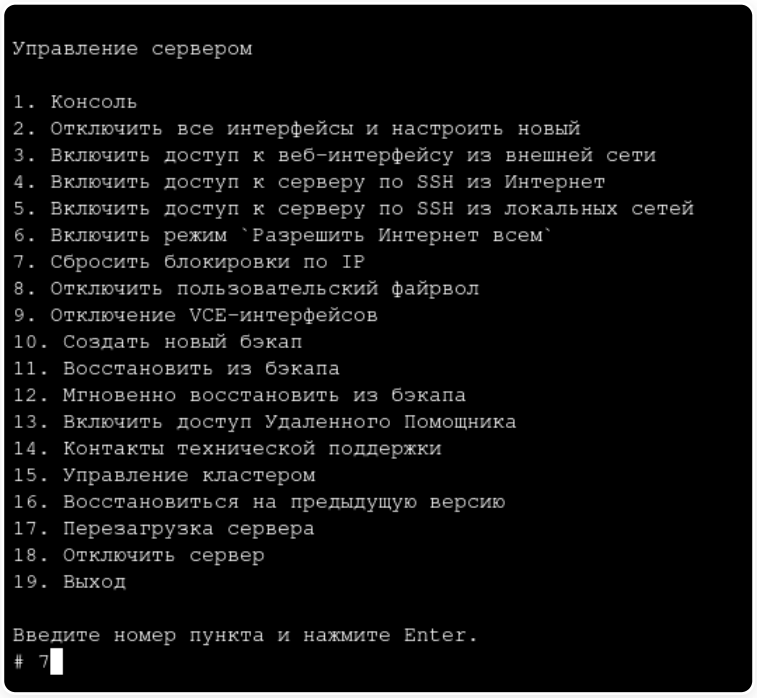
Логи службы `fail2ban` можно увидеть:

- В веб-интерфейсе в разделе **Отчеты и журналы** → **Системный журнал**, задав фильтр `fail2ban`.
- В разделе **Управление сервером** → **Терминал**, введя команду `journalctl -u fail2ban`.

Для разблокировки через терминал используйте команды:

- `fail2ban-client unban --all` - команда используется для снятия всех блокировок;
- `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса, указав нужный IP-адрес в качестве аргумента.

Блокировки можно сбросить из локального меню шлюза, выбрав опцию **Сбросить блокировки по IP**:



Список служб

Логи представленных служб доступны в разделе Система:

Модуль	Имя службы
Active Directory	ideco-ad-backend
ALD Pro	ideco-ald-rest, ideco-ald-backend
DHCP	ideco-dhclient, ideco-dhcp-server-backend
DNS	ideco-dns-backend, unbound, nsd, unbound-anchor, unbound-keygen, ideco-dns-dnstap-reader
DDNS	ideco-dns-backend
Ideco Center	ideco-central-console-backend
Ideco Client	ideco-agent-websocket, ideco-agent-backend, ideco-app-stats
IGMP Proxy	ideco-igmpproxy-backend, ideco-igmpproxy-rest
IPsec	ideco-ipsec-backend
NTP	chronyd
Syslog	ideco-logs-backend
VCE	ideco-vce-backend, ideco-vce-rest
VPN-подключения	ideco-vpn-authd, ideco-vpn-dhcp-backend, ideco-vpn-servers-backend, ideco-vpn-netns, ideco-vpn-sessions-sync
Web Application Firewall	ideco-waf-backend, ideco-waf-event-syncer
Авторизация	ideco-auth-backend
Антивирус	ideco-av-backend
Бэкапы	ideco-backup-backend, ideco-backup-create, ideco-backup-rotate
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-authd
Действия администраторов	ideco-audit-backend
Дополнительно (язык, часовой пояс, включение особых режимов работы)	ideco-system-backend
Доступ по SSH	sshd
Защита от повторяющихся вредоносных или подозрительных действиях, в т.ч. от брутфорс-атак (brute force - атака полным перебором)	fail2ban
Кластеризация	ideco-cluster-backend
Контент-фильтр	ideco-content-filter-backend
Контроль приложений	ideco-app-backend, ideco-app-control-nfq
Личный кабинет пользователя	ideco-user-cabinet-backend
Лицензия	ideco-license-backend
Локальное меню	ideco-local-menu
Маршрутизация	ideco-routing-backend, ideco-routing-rest
Обновления	ideco-sysupdate-backend
Обнаружение устройств	ideco-netscan-backend
Объекты	ideco-alias-backend
Ограничение скорости	ideco-shaper-backend
Обратный прокси	ideco-reverse-backend
Отправка оповещений через телеграм-бота	ideco-mir-alerts
Отчеты и журналы	ideco-logs-backend, ideco-reports-backend, ideco-logs-syncer
Почтовый релей	ideco-mail-backend
Предотвращение вторжений	ideco-suricata, ideco-suricata-backend, ideco-suricata-event-syncer, ideco-suricata-profiles-syncer-backend
Проверка скорости	ideco-speedtest

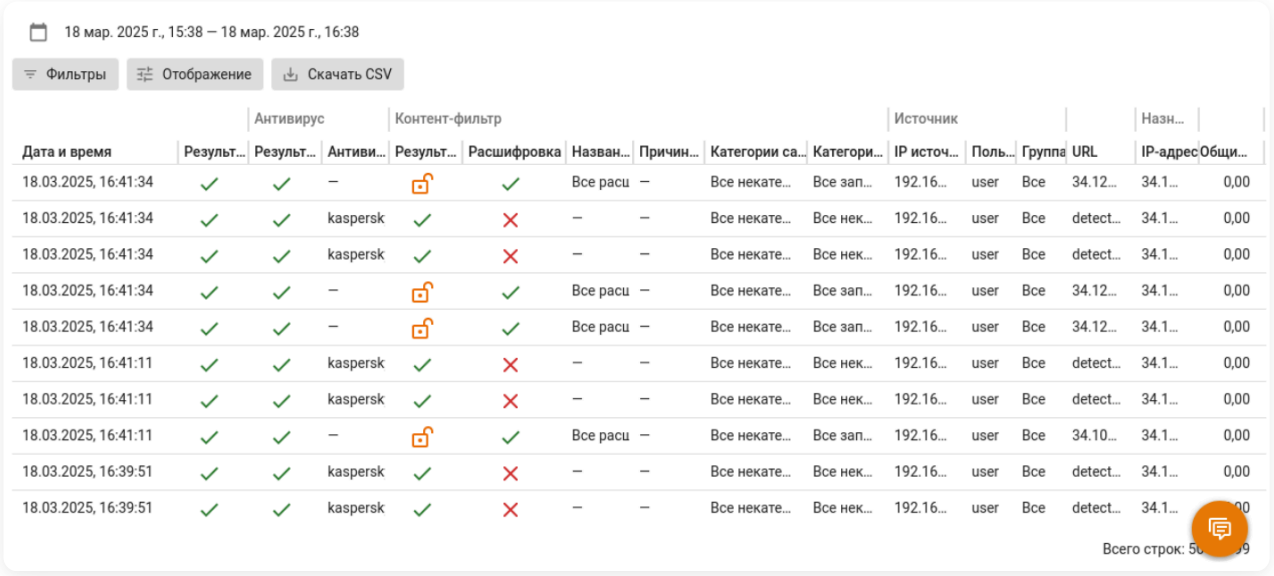
Модуль	Имя службы
Прокси	ideco-proxy-backend, squid
Сбор анонимной статистики о работе сервера	ideco-gatherstat-backend
Сертификаты	ideco-cert-backend
Сетевые интерфейсы	ideco-network-backend, ideco-network-nic
Учетные записи	ideco-user-backend
Файрвол	ideco-firewall-backend

Служебные:

Модуль	Имя службы
Локальная база данных	ideco-etcd-runtime, ideco-etcd-permanent
Сбор метрик и статистики	prometheus, prometheus-node-exporter
Сервер базы данных	clickhouse-server

Журнал веб-трафика

В разделе представлен результат проверки трафика антивирусом и модулем **Контент-фильтр**. Для просмотра отчета перейдите в раздел **Отчеты и Журналы → Журнал веб-трафика**:



Для настройки столбцов журнала нажмите **Отображение**.

Описание столбцов

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 проверки	Результат работы Контент-фильтра: разрешено/расшифровано/запрещено/перенаправлено
Расшифровка	Производилась или нет расшифровка запроса
ID	Идентификатор правила контент-фильтра
Правило из Ideco Center	При наличии Ideco Center - постправило/предправило/локальное правило или прочерк
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 проверки	Результат работы Антивируса: разрешено/расшифровано/запрещено/перенаправлено
ID	Идентификатор профиля антивируса
Профиль	Профиль антивируса
Серьезность угрозы	Указанная антивирусом серьезность угрозы: информационный, низкий, средний, высокий
Тип блокируемого контента	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

Результаты проверки

- **Разрешено**
- **Расшифровано**
- **Запрещено**
- **Перенаправлено на**

Расшифровка

- **Трафик расшифрован**
- **Трафик не расшифрован**

Если с устройства пользователя недоступен какой-либо интернет-ресурс, в разделе **Журнал веб-трафика** можно найти правило, блокирующее этот ресурс.

Для просмотра блокировок по конкретному правилу воспользуйтесь кнопкой **Фильтры**, указав в форме наименование правила и оператор.

Журнал трафика

На вкладке отображается информация о срабатывании правил **Файрвола** (таблицы FORWARD, DNAT, SNAT и INPUT), в том числе - о профилях **Предотвращения вторжений** и **Контроля приложений**.

Раздел позволяет быстро выявить модуль фильтрации, который блокирует трафик, а также 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 трафика** 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.

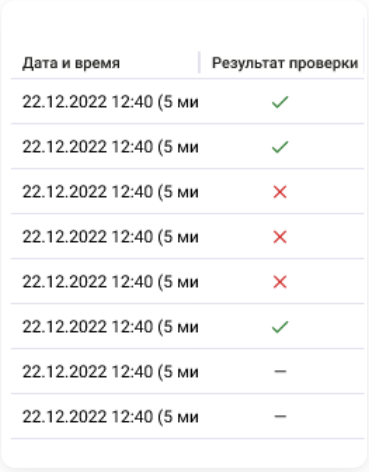
Чтобы отрегулировать столбцы, отображаемые в таблице, воспользуйтесь кнопкой **Отображение**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

При наличии большого количества строк в таблице воспользуйтесь кнопкой **Фильтры**.

При фильтрации по **Таблице правил (Файрвол)** можно вывести срабатывния системных правил (Forward System и Input System). Это правила **Файрвола**, которыми нельзя управлять из веб-интерфейса Ideco NGFW, они всегда включены. Правила Forward System и Input System имеют приоритет над пользовательскими правилами **Файрвола**. По вопросам срабатывания системных правил обращайтесь в Техническую поддержку.

В таблице отображаются группы:

Общее



- **Дата и время** - дата и время срабатывания правила;
- **Результат проверки** - совокупный результат проверки трафика тремя модулями фильтрации: **Файрвол**, **Предотвращение вторжений**, **Контроль приложений**.

Файрвол

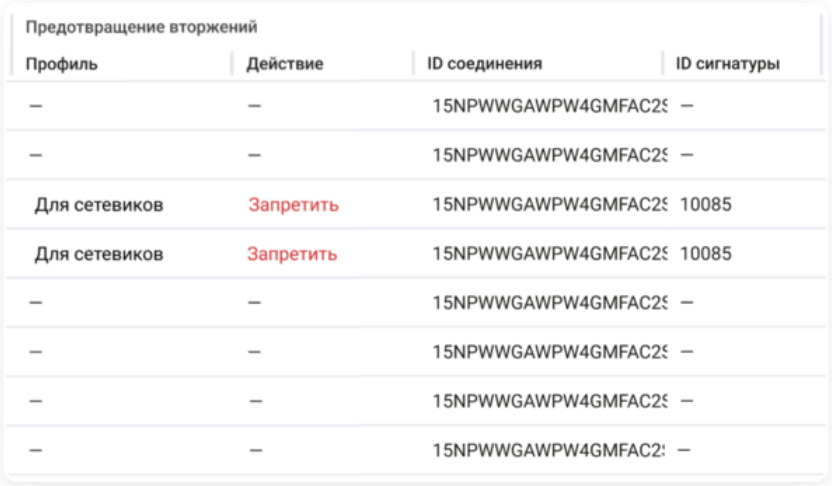
В группе **Файрвол** логируются **только** FORWARD и INPUT правила. Для просмотра правил DNAT и SNAT перейдите к соответствующей группе.

- **ID правила** - идентификатор сработавшего правила таблицы **FORWARD** и **INPUT**.
- **Таблица правил** - правила, которые сработали:
  - **FORWARD** - таблица **FORWARD** раздела **Файрвол** Ideco NGFW.

- **FORWARD BEFORE** - предправило FORWARD Ideco Center.
- **FORWARD AFTER** - постправило FORWARD Ideco Center.
- **FORWARD SYSTEM** - системное правило FORWARD.
- **INPUT** - таблица **INPUT** раздела **Файрвол** Ideco NGFW.
- **INPUT BEFORE** - предправило INPUT Ideco Center.
- **INPUT AFTER** - постправило INPUT Ideco Center.
- **INPUT SYSTEM** - системное правило INPUT.

- **Действие правила** - действие, определенное для трафика, подпадающего под сработавшее правило. Возможные действия: Разрешить, Запретить, Перенаправить в профиль.
- **Протокол** - протокол соединения.

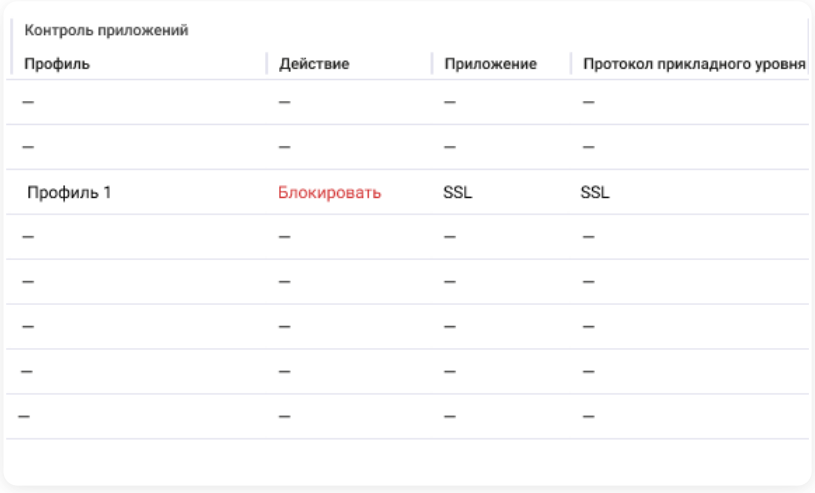
Предотвращение вторжений


Предотвращение вторжений

Профиль	Действие	ID соединения	ID сигнатуры
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
Для сетевиков	Запретить	15NPWWGAWPW4GMFAC2S	10085
Для сетевиков	Запретить	15NPWWGAWPW4GMFAC2S	10085
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–

- **Профиль** - название профиля **Предотвращения вторжений**, использованного в правиле **Файрвола**.
- **Действие** - действие для трафика, определенное профилем (*Разрешить*, *Запретить*, -).
- **ID соединения** - идентификатор соединения, трафик которого был обработан **Предотвращением вторжений**. Просмотреть логи системы Предотвращения вторжений можно в **Отчеты и журналы** → **События безопасности** → **Журнал IPS**.
- **ID сигнатуры** - идентификатор сигнатуры, которой соответствует трафик.

Контроль приложений


Контроль приложений

Профиль	Действие	Приложение	Протокол прикладного уровня
–	–	–	–
–	–	–	–
Профиль 1	Блокировать	SSL	SSL
–	–	–	–
–	–	–	–
–	–	–	–
–	–	–	–
–	–	–	–

- **Профиль** - название профиля **Контроля приложений**, использованного в правиле **Файрвола**;
- **Действие** - действие для трафика, определенное профилем;
- **Приложение** - приложение, действие для которого определено профилем;
- **Протокол прикладного уровня** - протокол, к которому применяется действие, определенное профилем.

Источник

Источник

IP-адрес	Порт	Зона	Логин	Пользователь	Группа	Местоположение
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	Англия
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.136	43612	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.136	43612	Любой	a.qwertyy	Имя Фамилия	Разработка	–

- **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).

Назначение

Назначение

IP-адрес	Порт	Зона	Логин	Пользователь	Группа	Местоположение
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	Англия
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.201	2222	–	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.201	2222	–	a.qwertyy	Имя Фамилия	Разработка	–

- **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/SNAT

DNAT			SNAT	
ID правила	Новый IP назначения	Новый порт назначения	ID правила	Новый IP источника
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
17	217.65.3.21	443	–	–
–	–	–	2	217.65.3.21

DNAT:

- **ID правила** - идентификатор сработавшего правила таблицы **DNAT**;
- **Новый IP назначения** - IP-адрес, на который файрвол поменял **IP-адрес назначения**;
- **Новый порт назначения** - порт, на который файрвол поменял **Порт назначения**.

SNAT:

- **ID правила** - идентификатор сработавшего правила таблицы **SNAT**;
- **Новый IP источника** - IP-адрес, на который файрвол поменял **IP-адрес источника**.

Кластер/VCE

Кластер		VCE	
ID	Название	ID	Название
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1

Кластер:

- **ID** - идентификатор кластера (если он настроен на NGFW);
- **Название** - название кластера (если он настроен на NGFW).

VCE:

- **ID** - идентификатор VCE;
- **Название** - название VCE.

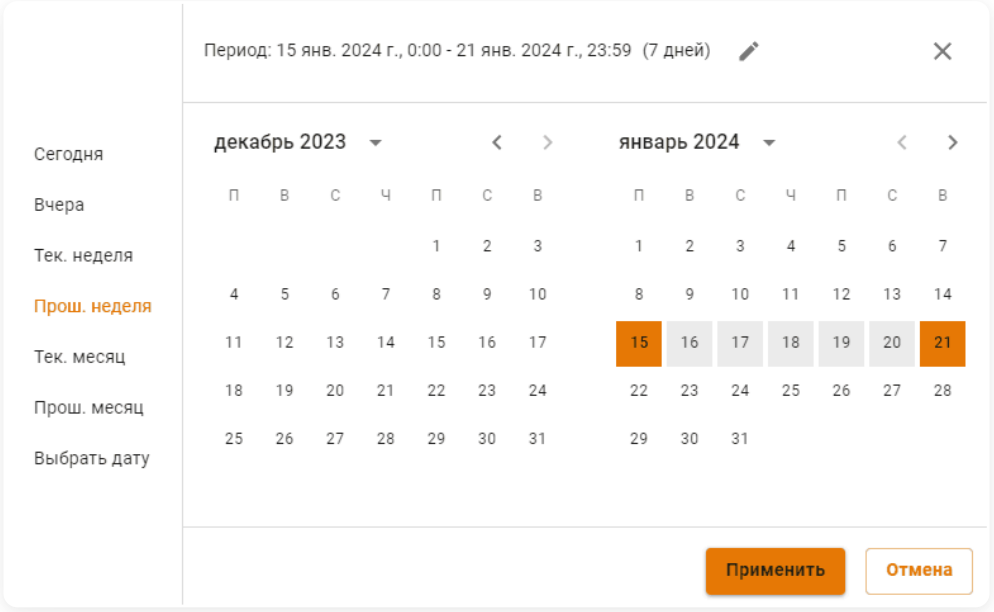
События безопасности

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** 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.

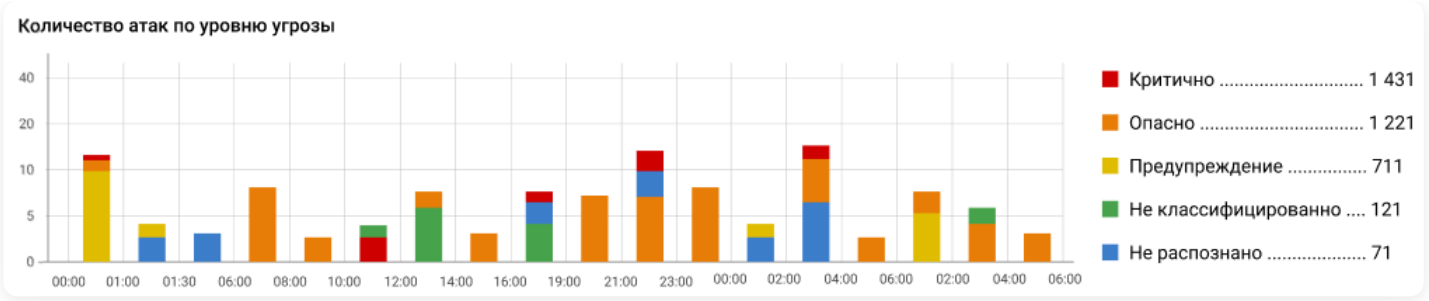
График Количество атак по уровню угрозы

Информация представлена в виде графика с пятью значениями угрозы безопасности:

- **Критично** - уровень угрозы 1;
- **Важно** - уровень угрозы 2;
- **Предупреждение** - уровень угрозы 3;
- **Не классифицировано** - уровень угрозы 4;
- **Не распознано** - уровень угрозы 255.

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, такой адрес не отображается в виджете.

По этой причине локальные IP-адреса не отображаются в виджете.

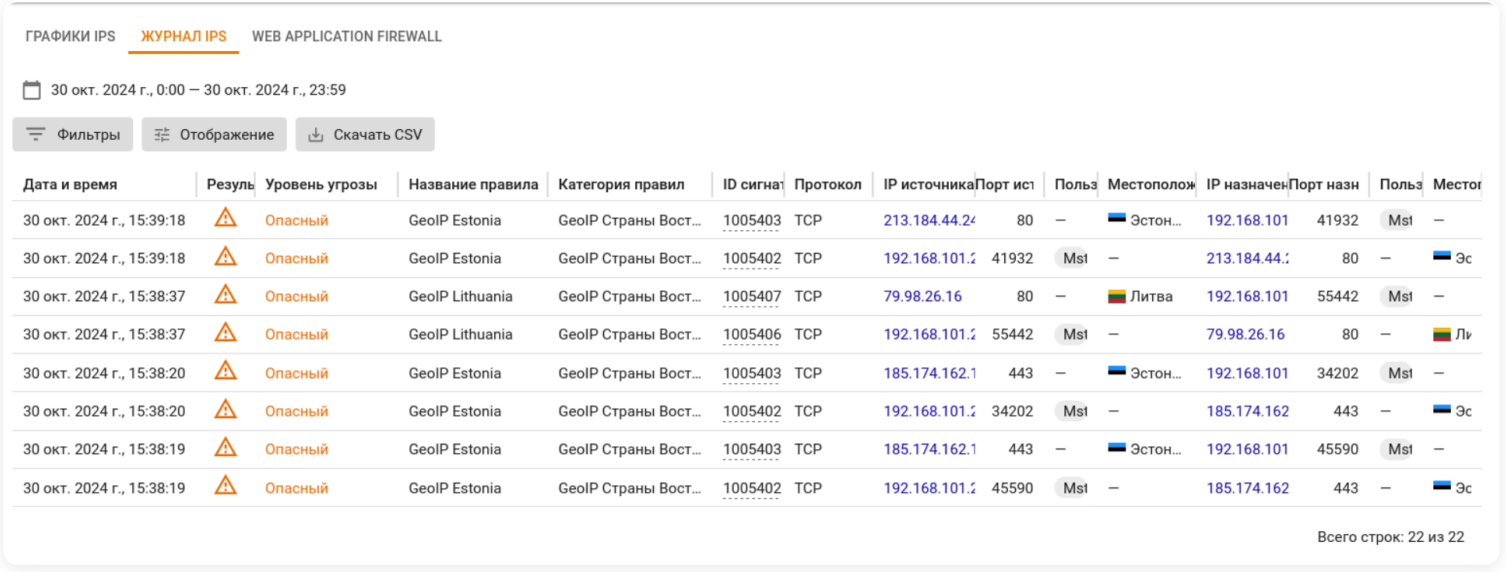
Топ подозрительных локальных узлов

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 разделе **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:
  - Критично;
  - Опасно;
  - Предупреждение;
  - Не распознано;
  - Не классифицировано

IP-адреса в столбцах **Источник** и **Назначение** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.

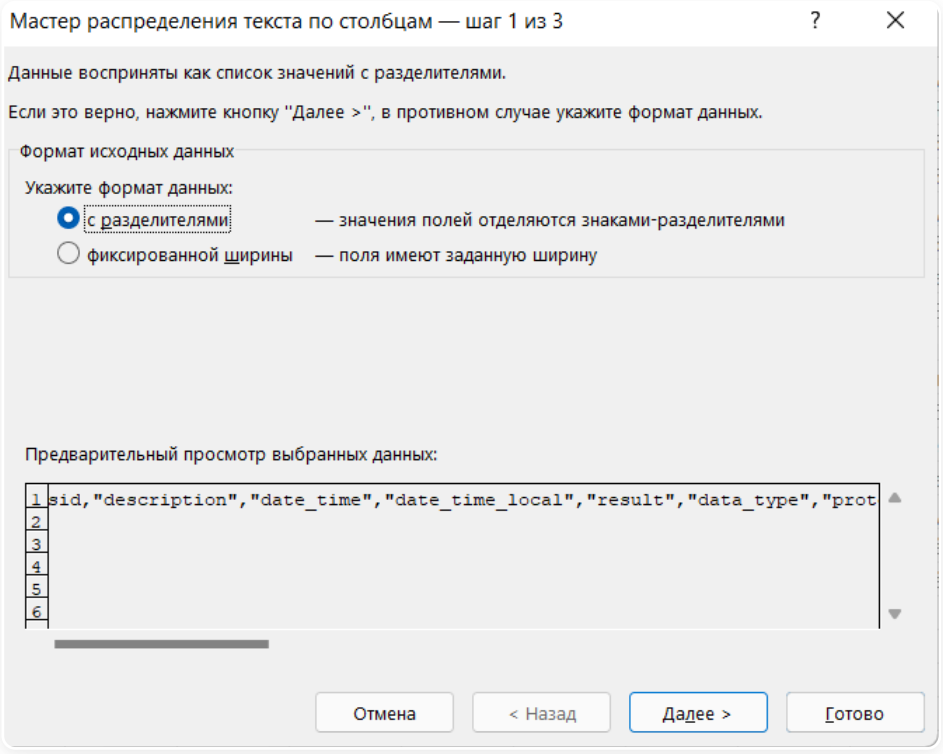
Для корректного отображения информации из CSV-файла выполните действия:

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.

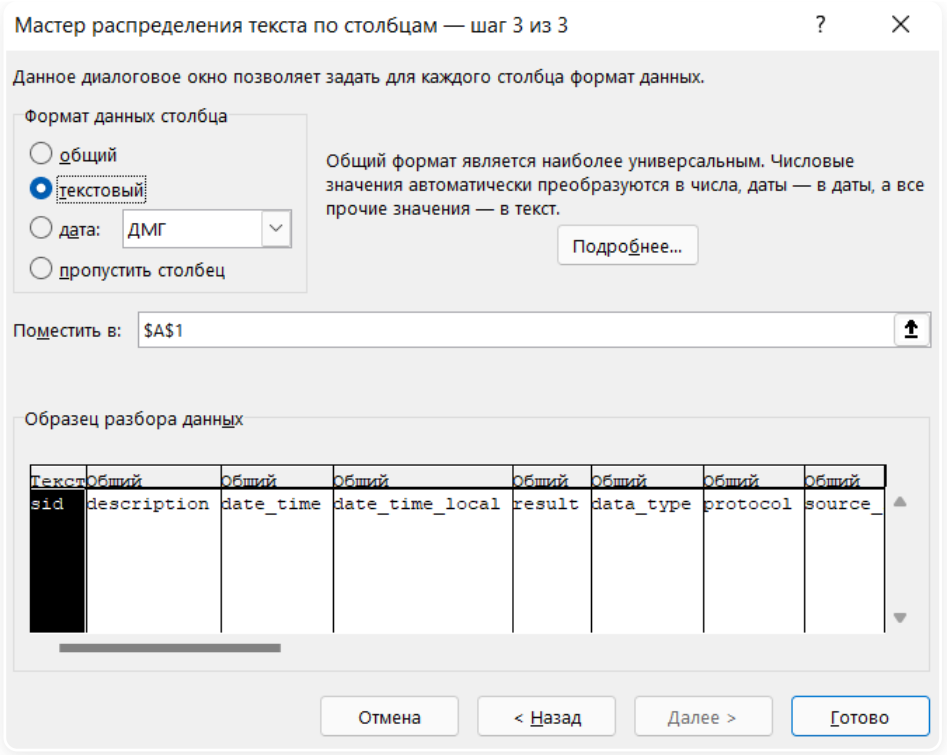
3. Перейдите на вкладку **Данные** и нажмите кнопку **Текст по столбцам**.

4. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:



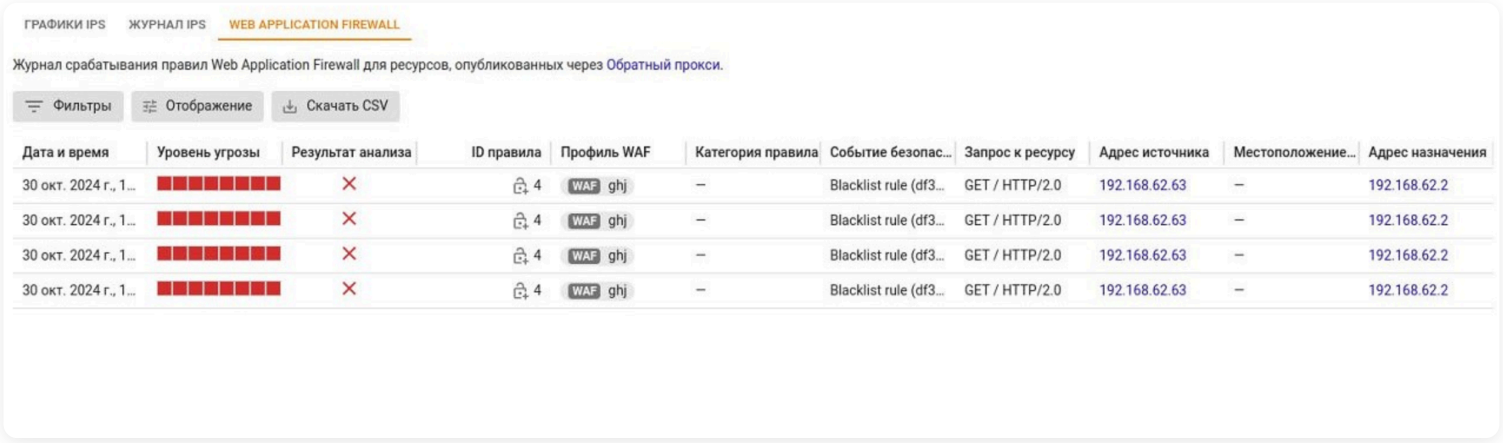
5. В блоке **Символом-разделителем является:** выберите **запятая** и нажмите **Далее**:

6. В блоке **Формат данных столбца** выберите **Текстовый** и нажмите **Готово**:



Web Application Firewall

Раздел **Отчеты и журналы** → **События безопасности** → **Web Application Firewall** содержит информацию о срабатывании правил Web Application Firewall в виде таблицы:

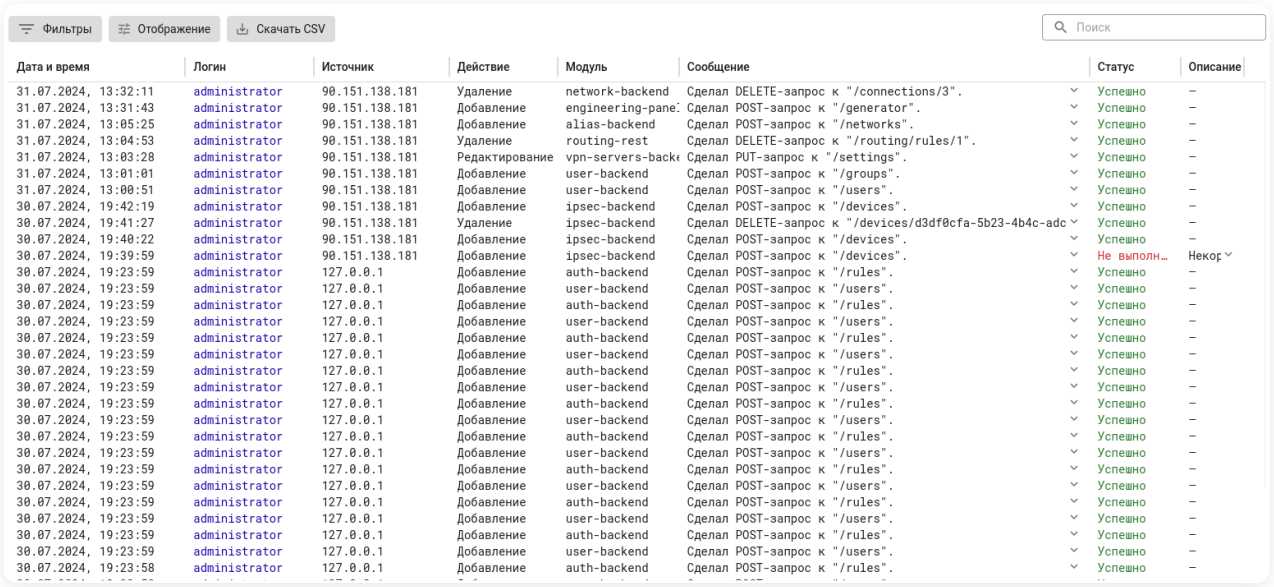


IP-адреса в столбцах **Адрес источника** и **Адрес назначения** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.

На вкладке **Web Application Firewall** отображается профиль WAF, параметры которого вызвали блокировку доступа к ресурсу.

Действия администраторов

Ideco NGFW логирует действия администраторов, которые вносят изменения в конфигурацию NGFW из веб-интерфейса, локального интерфейса и терминала. Действия, осуществляемые через локальное меню NGFW, отображаются в журнале действий администраторов с источником 127.0.0.1:



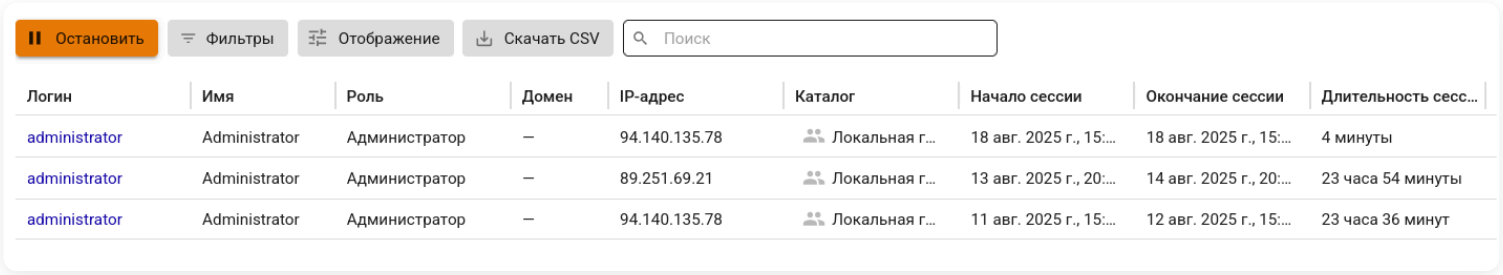
Дата и время	Логин	Источник	Действие	Модуль	Сообщение	Статус	Описание
31.07.2024, 13:32:11	administrator	90.151.138.181	Удаление	network-backend	Сделал DELETE-запрос к "/connections/3".	Успешно	–
31.07.2024, 13:31:43	administrator	90.151.138.181	Добавление	engineering-pane	Сделал POST-запрос к "/generator".	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-back	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, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	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

Время хранения данных в журнале **Аутентификация администраторов** составляет 1 год.



Для поиска авторизованных администраторов нажмите **Фильтры** и укажите:

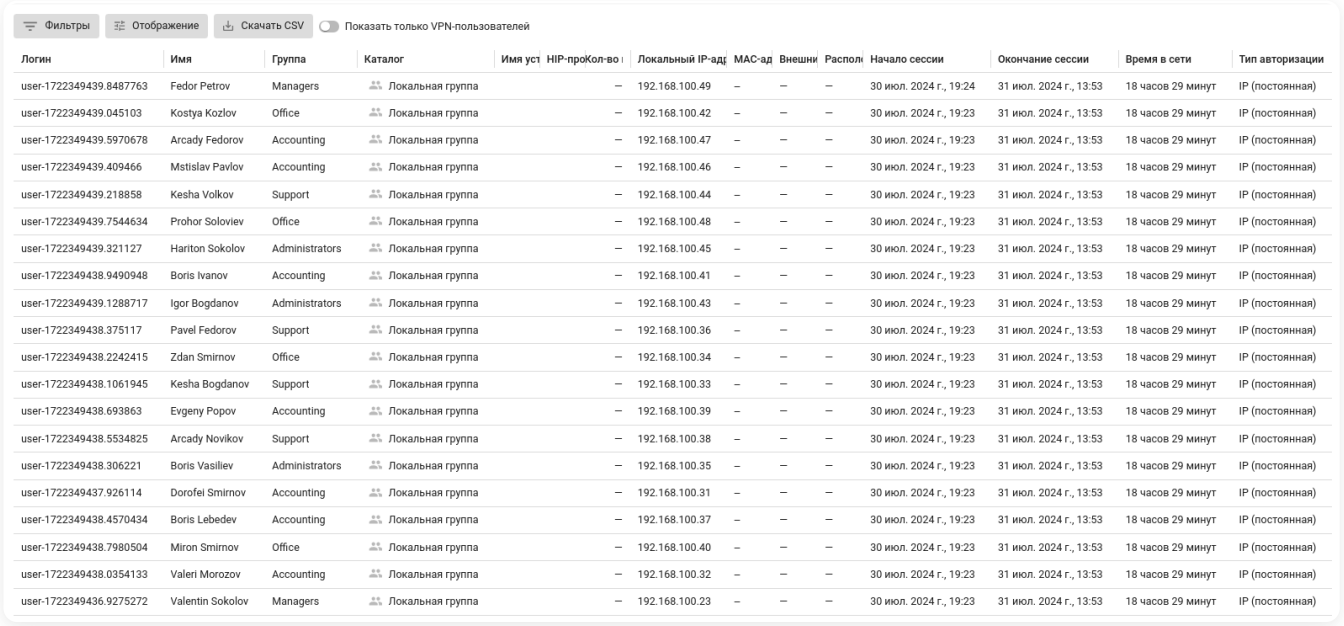
- В поле **Столбец** - требуемый параметр поиска.
- В последнем поле - значение.

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.

Журнал аутентификации

Время хранения данных в **Журнале аутентификации** составляет 180 дней.



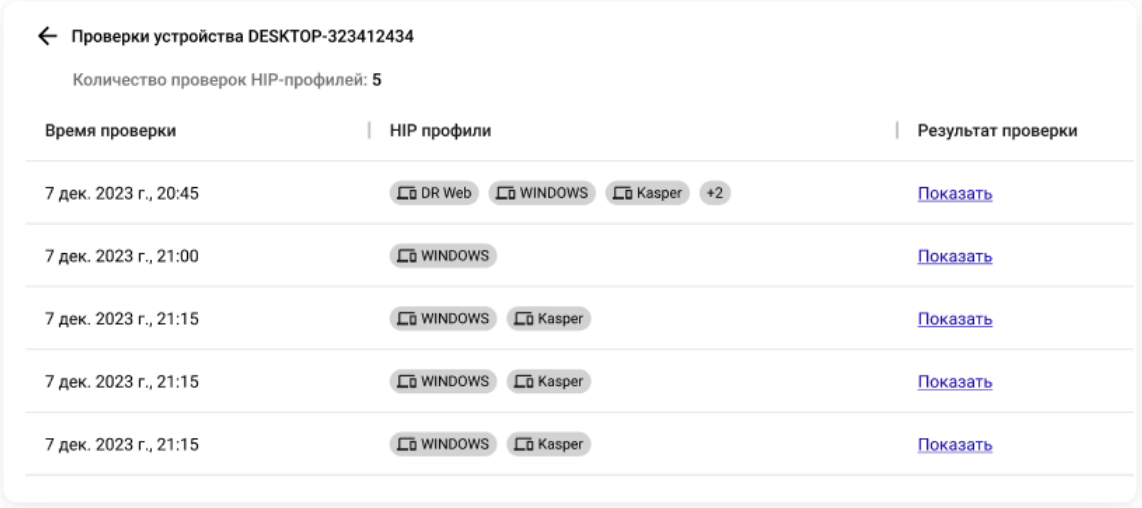
Логин	Имя	Группа	Каталог	Имя уст	HIP-про	Кол-во	Локальный IP-адр	MAC-ад	Внешни	Распол	Начало сессии	Окончание сессии	Время в сети	Тип авторизации
user-1722349439.8487763	Fedor Petrov	Managers	Локальная группа			–	192.168.100.49	–	–	–	30 июл. 2024 г., 19:24	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.045103	Kostya Kozlov	Office	Локальная группа			–	192.168.100.42	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.5970678	Arcady Fedorov	Accounting	Локальная группа			–	192.168.100.47	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.409466	Mstislav Pavlov	Accounting	Локальная группа			–	192.168.100.46	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.218858	Kesha Volkov	Support	Локальная группа			–	192.168.100.44	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.7544634	Prohor Soloviev	Office	Локальная группа			–	192.168.100.48	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.321127	Hariton Sokolov	Administrators	Локальная группа			–	192.168.100.45	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.9490948	Boris Ivanov	Accounting	Локальная группа			–	192.168.100.41	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.1288717	Igor Bogdanov	Administrators	Локальная группа			–	192.168.100.43	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.375117	Pavel Fedorov	Support	Локальная группа			–	192.168.100.36	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.2242415	Zdan Smirnov	Office	Локальная группа			–	192.168.100.34	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.1061945	Kesha Bogdanov	Support	Локальная группа			–	192.168.100.33	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.693863	Evgeny Popov	Accounting	Локальная группа			–	192.168.100.39	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.5534825	Arcady Novikov	Support	Локальная группа			–	192.168.100.38	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.306221	Boris Vasiliev	Administrators	Локальная группа			–	192.168.100.35	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349437.926114	Dorofei Smirnov	Accounting	Локальная группа			–	192.168.100.31	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.4570434	Boris Lebedev	Accounting	Локальная группа			–	192.168.100.37	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.7980504	Miron Smirnov	Office	Локальная группа			–	192.168.100.40	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.0354133	Valeri Morozov	Accounting	Локальная группа			–	192.168.100.32	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349436.9275272	Valentin Sokolov	Managers	Локальная группа			–	192.168.100.23	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)

Для поиска авторизованных пользователей нажмите на **Фильтры**, укажите в поле **Столбец** требуемый параметр поиска и в последнем поле - его значение.

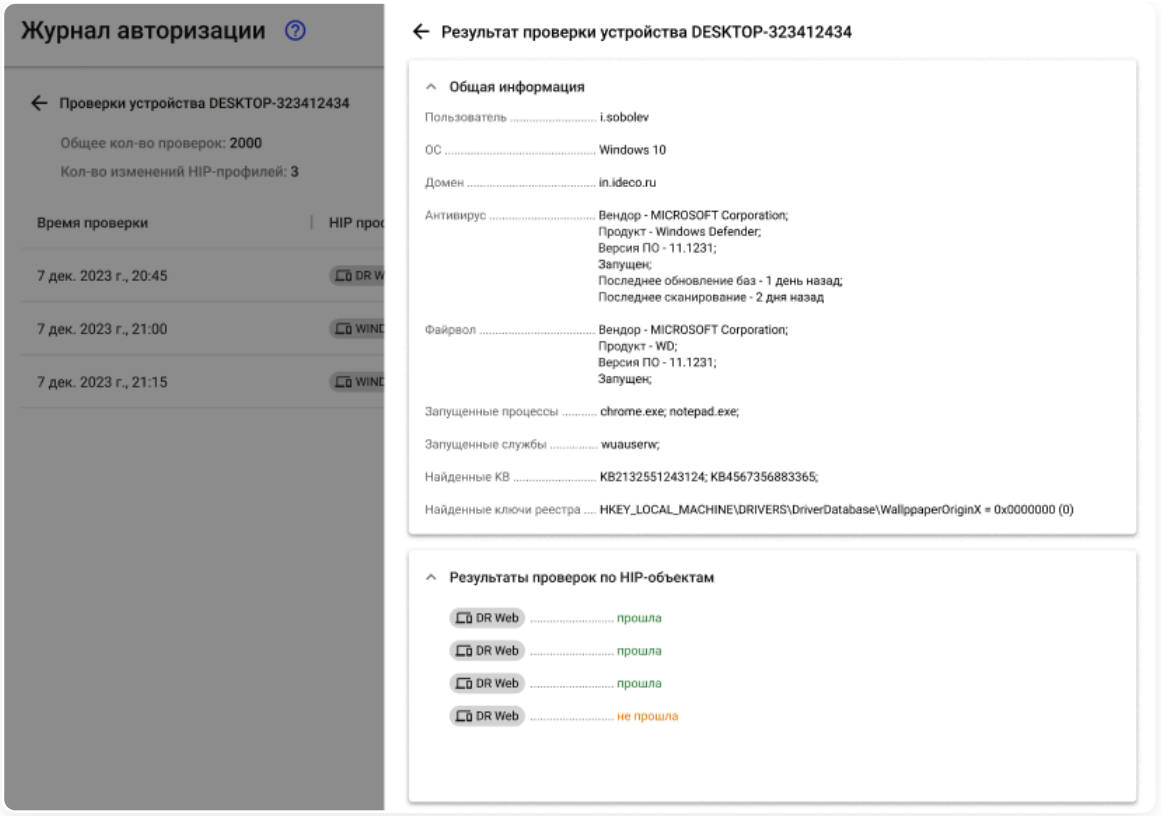
В столбце **Кол-во изменений профилей** указано количество изменений HIP-профилей, зафиксированных в результате проверок устройств, подключенных через Ideco Client. Изменения фиксируются при редактировании HIP-профиля в веб-интерфейсе или изменении соответствия устройств настроенным профилям.

Для просмотра результатов проверок устройств, подключенных через Ideco Client, выполните действия:

1. Кликните на число в столбце **Кол-во изменений профилей**. Откроется список проверок:



2. Кликните **Показать** в столбце **Результат**, чтобы увидеть общую информацию и результат проверки по HIP-объектам:



Особенности работы Журнала аутентификации:

- 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.

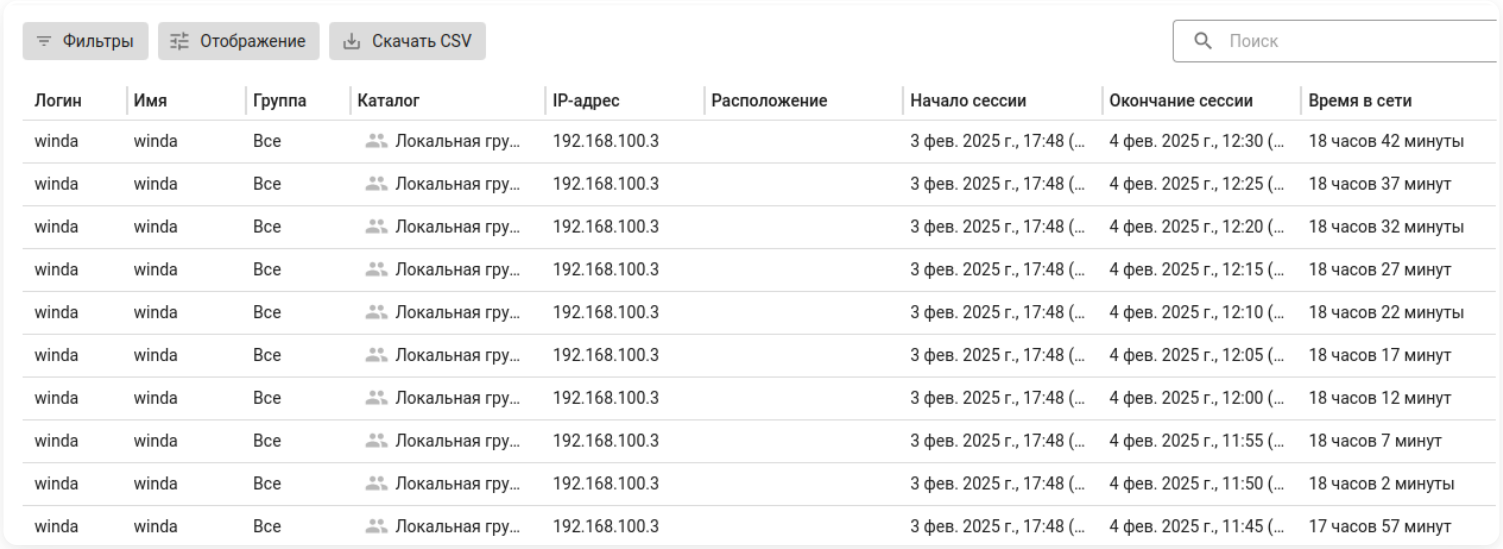
Включение опции **Показать VPN-пользователей** отфильтрует в таблице журнала информацию обо всех VPN-сессиях по всем протоколам.

Журнал аутентификации ЛК

Журнал аутентификации ЛК представляет собой историю сессий пользователей, авторизованных в личном кабинете пользователя Ideco NGFW.

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	Расположение	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;
- **Расположение** - 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:

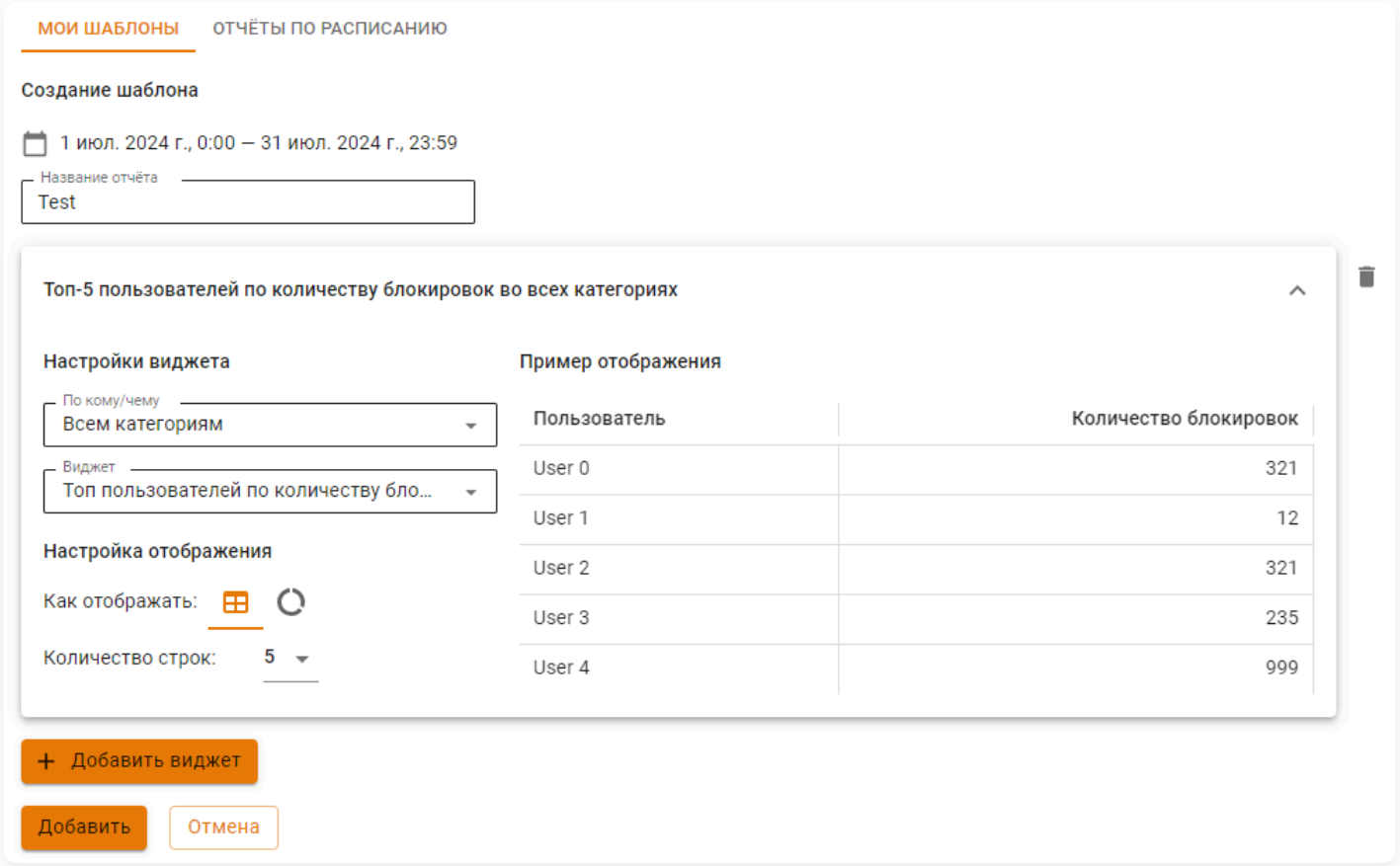
- Нажмите кнопку **Фильтры**, установите параметр поиска (все наименования доступных столбцов) и его значение;
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

Конструктор отчетов

Мои шаблоны

На этой вкладке создаются шаблоны со статистикой, которые можно посмотреть в браузере, отправить на электронную почту и сохранить в формате PDF или CSV.

Для создания шаблона нажмите **Добавить** в левом верхнем углу. Откроется меню настройки шаблона. Задайте временной промежуток и название отчета, нажмите **Добавить виджет**:



- В строке **По кому/чему** выберите объект, по которому будет собираться статистика. Если выбираете **Определенный** объект (например, *Определенный пользователь* или *Определенная группа*), то появится дополнительная строка **Объекты**, где можно выбрать несколько объектов;
- В строке **Виджет** укажите, какую информацию хотите видеть по выбранному объекту. Один шаблон может содержать несколько виджетов;
- Задайте **Настройки отображения**.

После окончания настройки шаблона нажмите **Добавить**.

Ideco NGFW хранит данные в течение определенного времени, по прошествии которого они безвозвратно удаляются и не могут быть включены в отчеты.

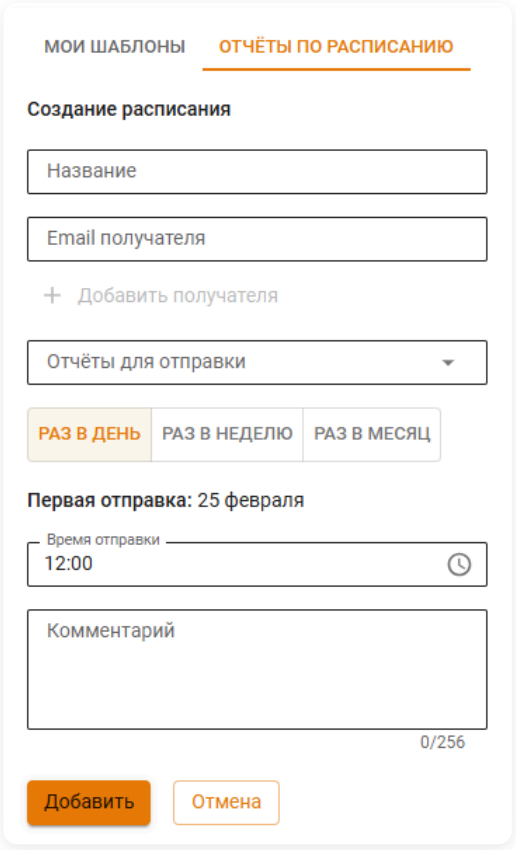
Сроки хранения данных по разделам:

- Системный журнал - 90 дней;
- Логи служб - 14 дней;
- Данные веб-трафика (Журнал веб-трафика, а также посещенные сайты) - 1 месяц;
- События безопасности (Журнал IPS и Web application firewall) - 3 месяца;
- Действия администраторов и Авторизация администраторов - 1 год;
- Журнал аутентификации - 180 дней.

Отчеты по расписанию

На этой вкладке создаются и редактируются настройки для отправки рассылки на электронную почту. Отчеты отправляются в формате PDF.

Для создания настройки нажмите **Отчеты по расписанию** → **Добавить** в левом верхнем углу. В одной настройке можно указать несколько почтовых адресов (кнопка **Добавить получателя**) и несколько отчетов (поле **Отчеты для отправки**):



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-е число, но в месяце меньше дней, то выбирается последнее число месяца.

Текст, добавленный в поле **Комментарий**, не будет отправляться в отчетах и отображается только в Ideco NGFW.

NGFW сохранит все пользовательские настройки времени отправки во всех фильтрах (раз в день, раз в неделю и раз в месяц) после нажатия на кнопку **Комментарий**, но отправляться шаблон будет только в период, выбранный пользователем.

Отчет создается выключенным. Чтобы его включить нажмите на . Если в таблице большое количество отчетов, воспользуйтесь кнопкой **Фильтры**.

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, из предложенных фильтров или укажите даты нажав **Выберите дату**.

3. Укажите название отчета (строка *Название отчета*).

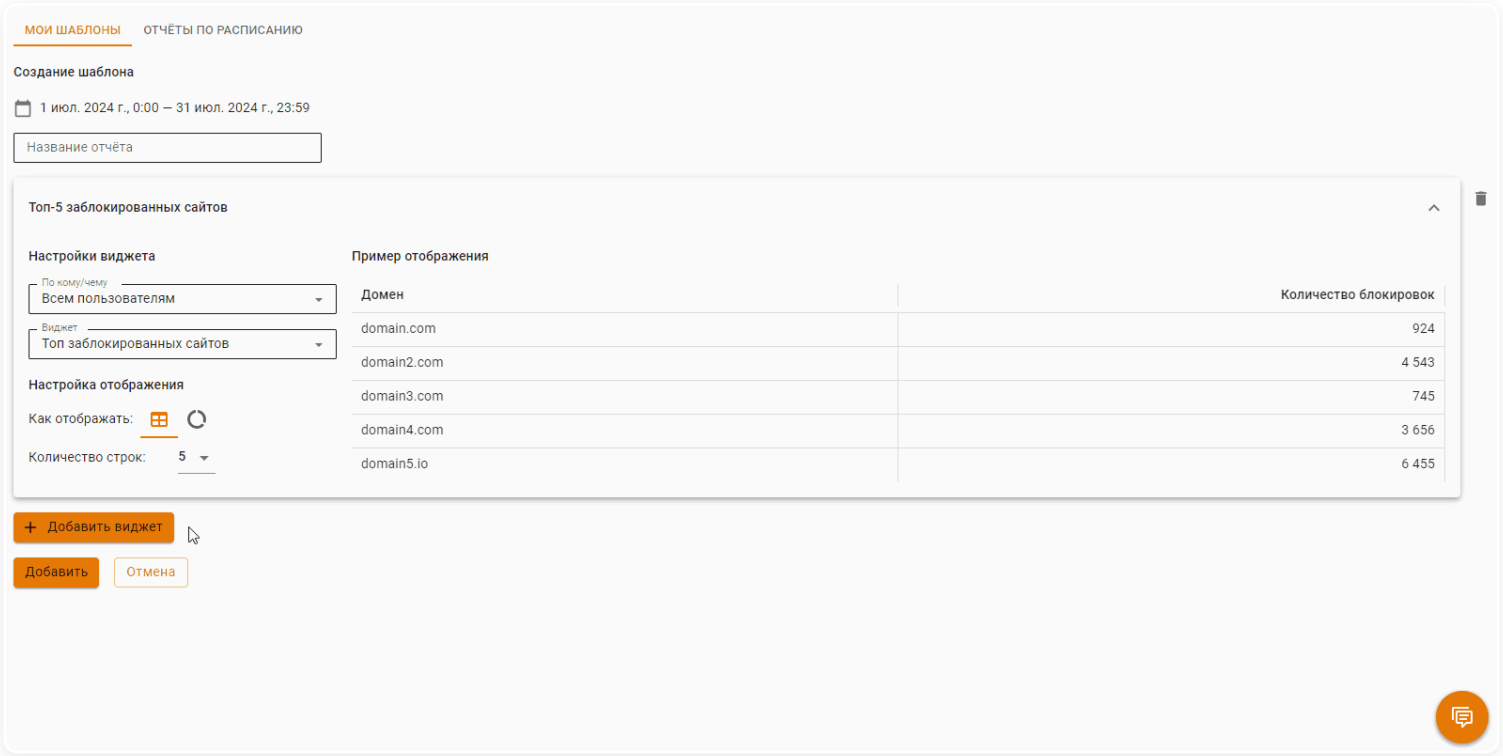
4. Кликните по кнопке **Добавить виджет**.

5. Заполните строки:

- **По кому/чему** - выберите **Всем пользователям**;

- **Виджет** - выберите **Топ заблокированных сайтов**;

6. Укажите **Настройки отображения** в виде таблицы или круговой диаграммы:



7. Сохраните шаблон по кнопке **Добавить**.

Создайте правило, по которому шаблон отчета будет отправляться на электронную почту:

1. Нажмите **Добавить** на вкладке **Отчеты по расписанию**.

2. Заполните строки:

- **Название** - любое название, которое поможет идентифицировать правило расписания;
- **Email получателя** - электронная почта получателя отчета. Если нужно отправлять отчет нескольким получателям, укажите дополнительные адреса по кнопке **Добавить получателя**.

3. Выберите нужный шаблон в поле **Отчеты для отправки**.

4. Укажите настройки даты/дня и времени отправки отчета получателю (раз в месяц, каждый 1-й день месяца).

Syslog

Название службы раздела **Syslog**: `ideco-logs-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 **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 **Отчеты и журналы** → **Syslog** и выполните действия:

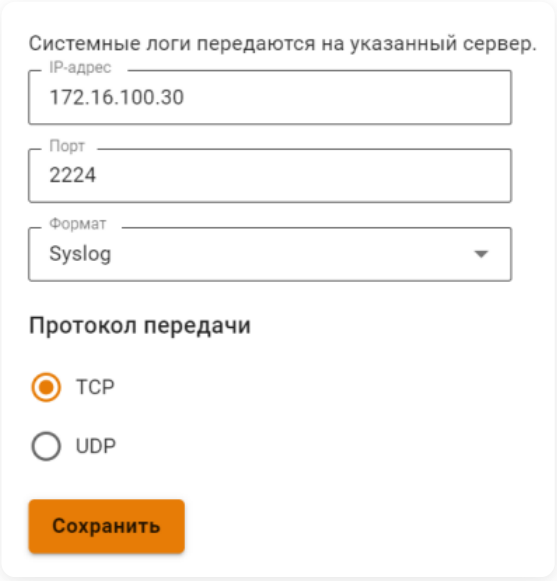
1. Укажите IP-адрес сервера-коллектора (любой локальный или публичный IP-адрес).

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.

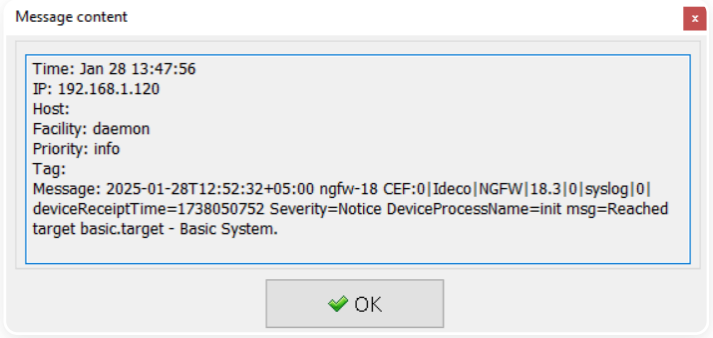
5. Нажмите **Сохранить** и включите опцию **Syslog**:



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

```
2025-10-15T15:38:54+05:00 ideco-ngfw CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=17605272289 Severity=Informational
```

где:

- `2025-10-15T15:38:54+05:00` - время события в Ideco NGFW;
- `ideco-ngfw` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `CEF:0` - версия формата CEF;
- `Ideco` - вендор;
- `NGFW` - название продукта;
- `19.0` - версия продукта;
- `0|syslog|0` - идентификатор лога, постоянный для NGFW. Состоит из трех полей: идентификатор типа события, описание события, важность события;
- `deviceReceiptTime` - время события в системе NGFW, 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;
- `ideco-ngfw` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса.

Журнал Трафик

CEF:

```
2025-10-16T16:32:06+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1760614326 Severity Informational device
```

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 службы.

outcome	result	Общий результат проверки. Возможные значения: • `absent` - отсутствие значения; • `accept` - разрешение; • `drop` - запрет.
deviceEventClassId	rule_id	Идентификатор правила **Файрвола**. Пустая строка означает отсутствие значения.
name	table	Название таблицы, в которой сработало правило. Возможные значения: • `absent` - отсутствие значения; • `fwd` - таблица **FORWARD** раздела **Файрвол** Ideco NGFW; • `fwd_a` - постправило FORWARD Ideco Center; • `fwd_b` - предправило FORWARD Ideco Center; • `fwd_s` - системное правило FORWARD; • `inp` - таблица **INPUT** раздела **Файрвол** Ideco NGFW; • `inp_a` - постправило INPUT Ideco Center; • `inp_b` - предправило INPUT Ideco Center; • `inp_s` - системное правило INPUT.
act	action	Действие правила **Файрвола**. 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 протокола прикладного уровня.
app	dpi_protocol	Название приложения.
proto	protocol	Название протокола.
sourceAddress	src_ip	IP-адрес источника.
sourcePort	src_port	Порт источника. Значение `0` означает 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.
cs4	dst_location_name	Название локации назначения.
-	dst_location_code	Код локации назначения.
destinationAddress	dst_ip	IP-адрес назначения.
destinationPort	dst_port	Порт назначения. Значение `0` означает 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.

cs5	dst_location_name	Название локации назначения.
cs6	dst_location_code	Код локации назначения.
flexNumber1	dnat_rule_id	Идентификатор DNAT правила. Пустая строка означает отсутствие значения.
destinationTranslatedAddress	dnat_ip	IP-адрес, на который был изменен адрес назначения.
destinationTranslatedPort	dnat_port	Порт, на который был изменен порт назначения.
flexNumber2	snat_rule_id	Идентификатор SNAT правила. Пустая строка означает 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:

```
2025-10-16T17:02:26+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.7|0|syslog|0|deviceReceiptTime=1760616146 Severity=Informational Device
```

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**	**Описание**
DeviceProcessName	web-proxy	Название службы.
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.
DeviceCustomString1	redirected_to	Если запрос попал под правило перенаправления, отображает url куда перенаправило, если нет - пустая строка.
DeviceCustomString2	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` означает 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` означает отсутствие данных.
DeviceCustomString3	mime	Content-Type HTTP запроса. Отсутствие данных отображается пустой строкой.
requestClientApplication	useragent	User-Agent HTTP запроса. Отсутствие данных отображается пустой строкой.
DeviceCustomString4	user_name	Имя пользователя, который авторизован с IP источника.
-	login	Логин пользователя.

DeviceCustomString5	group_name	Имя группы, в которую входит пользователь.
DeviceCustomString6	referer	Referer HTTP запроса. Отсутствие данных отображается пустой строкой.

Предотвращение вторжений

CEF:

```
2025-10-15T18:21:45+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.7|0|syslog|0|deviceReceiptTime=1760534505 Severity=Warning DeviceCustom
```

Syslog:

```
2025-08-25T16:38:36+05:00 ideco-ngfw suricata - - - flow_id:1344232018329395, in_iface:, sensor_name:ideco-ips, event_type:al
```

где:

Ключ CEF	**Ключ Syslog**	**Описание**
-	suricata	Название службы.
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 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 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.
EndTime	flow.end	Окончание.
FlexNumber3	flow.age	Возраст.
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 TCP-пакета, указывающий, что пакет получен.
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.

Из сообщений модулей, перечисленных ниже, SIEM не сможет извлечь ключевые поля для последующего анализа. Такие сообщения доступны только для просмотра в исходном виде.

Контент-фильтр

Логирование включается в разделе **Сервисы** → **Прокси** → **Основное**. Просмотр логов доступен в веб-интерфейсе в разделе **Отчеты и журналы** → **Системный журнал**. Название служб для фильтрации: `ideco-content-filter-backend` и `squid`.

CEF:

```
2025-08-25T17:31:18+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1760540338 Severity=Notice DeviceProcess
```

Syslog:

```
2025-08-25T17:31:18+05:00 ideco-ngfw squid - - - {192.168.100.11 - - [25/Aug/2025:17:31:18 +0500] "GET http://porno365.plus/c
```

Ключ CEF	Ключ Syslog	Описание
DeviceProcessName	web-proxy	Название службы.

Информация в сообщении:

- `192.168.100.11` - IP-адрес пользователя;

- `[25/Aug/2025:17:31:18 +0500]` - дата/время события блокировки;
- `GET` - метод;
- `http://porno365.plus/categories` - URL заблокированного ресурса;
- `HTTP/1.1` - протокол;
- `403` - код состояния HTTP;
- `7470` - передано байт (в ответ, включая HTTP-заголовок);
- `https://www.google.com/` - HTTP referer;
- `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0` - цифровой отпечаток браузера;
- `TCP_DENIED:HIER_NONE` - техническое сообщение от squid;
- `Custom deny 3 P‘P»PsPєPёCЂPsPIPєP° CЃP°P№C,PsPI CЃ PSPµPїPsPґPsP±P°CЂC‰PёPj PєPsPSC,PµPSC,PsPj cf_extended.id.16 group.id.1  0` - сообщение о запрете из-за пользовательской категории;
- `"av_name"` - название антивируса, если он включен, в примере антивирус отключен;
- `"av_object_infected"` - результат проверки антивирусом, пустое поле - вирус не обнаружен;
- `"av_object_size"` - размер проверяемого объекта;
- `"av_virus_name"` - название обнаруженного вируса;
- `"x_infection_found"` - подтверждение, что запрос был обработан ICAP-оберткой для антивируса (Касперский);
- `"x_virus_id"` - идентификатор вируса/вредоносной программы;
- `"x_av_verifed"` - результат проверки антивирусом;
- `"morph-action"` - результат проверки **Морфологическим анализом**;
- `"morph-dict-id"` - название морфологического словаря, указывается в случае запрета **Морфологическим анализом**.

Авторизация через журнал безопасности AD

CEF:

```
2025-10-15T18:21:45+05:00 ngfw-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1721305222 Severity=Notice DeviceProcess
```

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 службы.

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-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731923661 Severity=Notice DeviceProces
```

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 службы.

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-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731937903 Severity=Notice DeviceProces
```

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 службы.

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|18.0|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 службы.

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-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731938874 Severity=Notice DeviceProces
```

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 службы.

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'`).

Подключение по VPN

CEF:

```
2024-11-18T19:16:18+05:00 ideco-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731939378 Severity=Notice DeviceProces
```

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 службы.

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'`).

Служба fail2ban

CEF:

```
2024-11-18T19:26:57+05:00 ideco-19 CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Notice DeviceProces

2024-11-18T19:26:57+05:00 ideco-ngfw CEF:0|Ideco|NGFW|19.0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Warning DevicePro
```

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 службы.

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.

Управление сервером

В этом разделе можно получить данные об авторизованных на сервере пользователях, загрузке процессора и интерфейсов, а также посмотреть данные о трафике в режиме реального времени.

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 даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Администраторы

В Ideco NGFW вы можете создать локальных администраторов или интегрировать администраторов из сервисов Active Directory, ALD PRO, RADIUS.

Сведения об авторизованных администраторах представлены в разделах **Аутентификация администраторов** и **Сессии администраторов**.

Сессия администратора действует в течение 24 часов и не может быть продлена никакими действиями. По истечении этого срока сессия администратора будет автоматчиески завершена.

Роли администраторов

Роль	Возможности
Администратор	• Полный доступ ко всем настройкам NGFW, возможность создания новых настроек, правил, учетных записей других пользователей NGFW, а также редактирования, управления и удаления их • Создание пользователей с правами администратора
Только просмотр	• Полный доступ к просмотру всех настроек NGFW без возможности создания новых настроек, правил, учетных записей других пользователей NGFW, а также редактирования, управления и удаления их

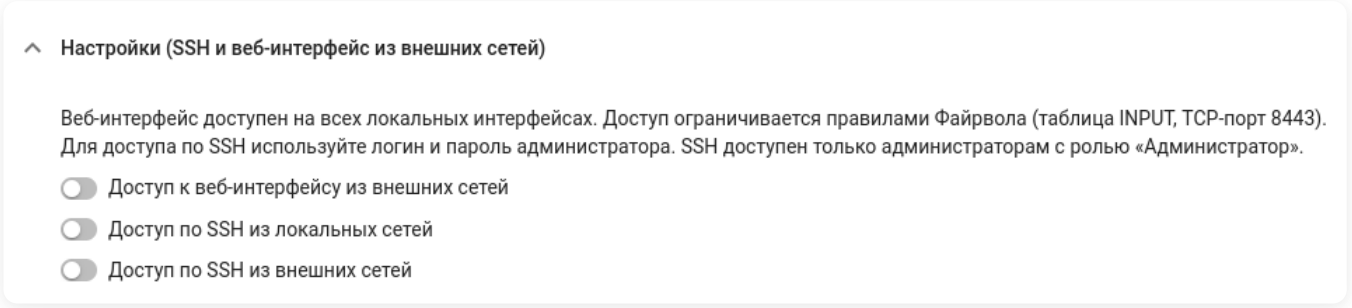
Администратор ИБ	• Выбор событий безопасности, подлежащих регистрации в журнале **События безопасности**
	• Чтение журнала **События безопасности**
	• Настройка параметров выгрузки информации о событиях безопасности, зарегистрированных в NGFW
	• Формирование отчетов в формате `.csv` с учетом заданных критериев отбора и выгрузка их из журнала событий безопасности NGFW
	• Настройка и получение оповещений в веб-интерфейсе NGFW 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 файрвола	• Создание учетных записей других пользователей NGFW.
	• Управление учетными записями пользователей NGFW, 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, 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
	• Применение правил фильтрации к:
	  ◦ сетевым интерфейсам NGFW
	  ◦ идентифицированным пользователям NGFW
	  ◦ 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
	• Изменение конфигурации NGFW
	• Тестирование NGFW

Администратор настройки доступов	• Создание учетных записей других пользователей NGFW • Управление учетными записями пользователей NGFW, 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, определяемых их ролями • Определение периода неактивности пользователя, по истечении которого сессия пользователя завершится (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**, **Журнал событий**, **Журнал веб-трафика**, **События безопасности** и **Журнал аутентификации**
Создание отчетов	• Просмотр, настройка и выгрузка отчетов в формате .csv для следующих журналов: **Трафик**, **Журнал событий**, **Журнал веб-трафика**, **События безопасности**, **Журнал аутентификации** и **Конструктор отчетов**

Доступ к веб-интерфейсу из внешней сети и удаленный доступ по SSH

- Для получения доступа к Ideco NGFW из внешней сети включите опцию **Доступ к веб-интерфейсу из внешней сети**. Эта функция помогает администрировать Ideco NGFW удаленно. Попытки подбора паролей блокируются автоматически.
- Для получения доступа к Ideco NGFW по SSH из локальной или внешних сетей включите соответствующие опции. Доступ осуществляется по 22 TCP-порту. Попытки подбора паролей также будут автоматически блокироваться:



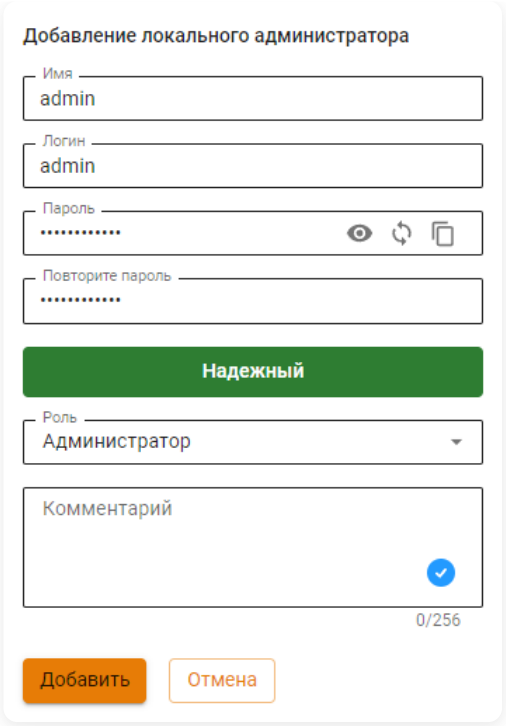
Подробнее о настройке подключения к веб-интерфейсу при удаленном доступе смотрите в статье Удаленный доступ для управления сервером.

Управление локальными администраторами

Чтобы добавить нового локального администратора выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **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 превышать 42 символа и не должно состоять только из цифр.
- **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).
- **Роль** - выберите роль.

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**.

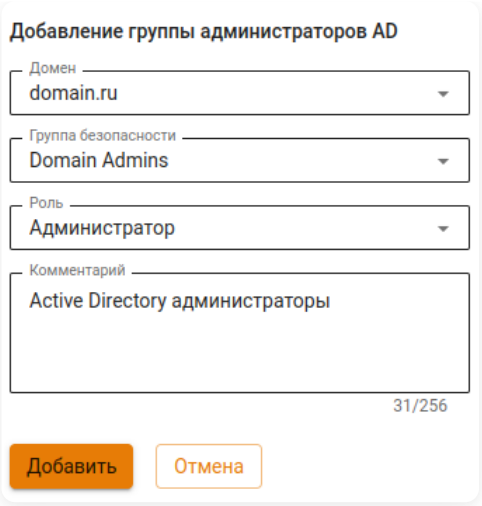
Управление AD/ALD администраторами

Чтобы добавить администраторов, необходимо ввести NGFW в домен Active Directory. При удалении домена AD/ALD из Ideco NGFW будут удалены сессии администраторов.

Чтобы интегрировать администраторов Active Directory или ALD Pro с Ideco NGFW, выполните действия:

1. Перейдите в **Управление сервером** → **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 администраторов идентичны ролям локальных администраторов.

3. Нажмите **Добавить**.

Особенности работы:

- Если администратор был авторизован по правилу или группе безопасности, которые были удалены, его сессия будет удалена. Это произойдет только после синхронизации групп безопасности на Ideco NGFW, которая выполняется каждые 5 минут.
- Если администратора исключить из группы безопасности, он не будет удален сразу. Его сессия завершится через некоторое время, и при следующей попытке авторизации он 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 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.

Чтобы узнать ID роли RADIUS-администратора:

1. Перейдите в **Управление сервером** → **Администраторы** → **Роли**.

2. Нажмите на **Отображение** и включите столбец ID. ID роли появится в левом столбце таблицы.

ID роли администраторов

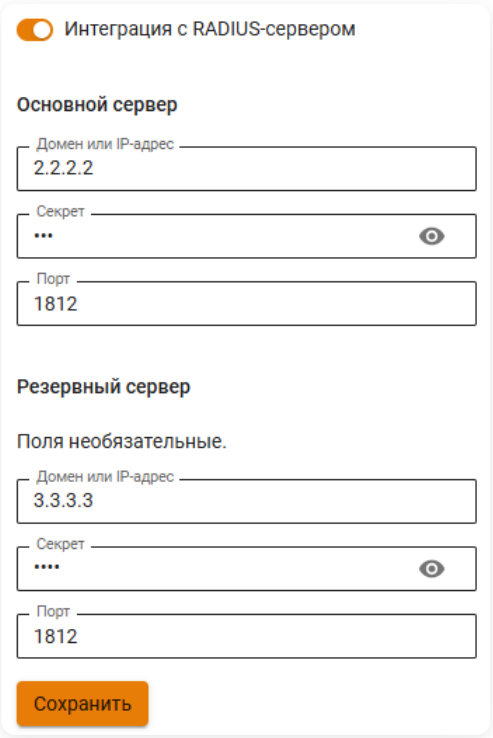
- `predefined_admin_write` - Администратор.
- `predefined_admin_readonly` - Только просмотр.
- `predefined_security_admin` - Администратор информационной безопасности.
- `predefined_firewall_admin` - Администратор файрвола.
- `predefined_access_settings_admin` - Администратор настройки доступов.
- `predefined_reports_view` - Просмотр отчетов.
- `predefined_reports_change` - Создание отчетов.

Интеграция администраторов RADIUS с Ideco NGFW

Выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы** → **RADIUS** и включите опцию **Интеграция с RADIUS-сервером**.

2. Укажите доменное имя или IP-адрес внутреннего RADIUS-сервера и секрет (пароль доступа). Если требуется, поменяйте порт, по которому будет происходить подключение к серверу:



При наличии в сети двух RADIUS-серверов настройте один как резервный с указанием порта подключения.
При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.

3. Нажмите **Сохранить**.

Особенности удаления администраторов

- Если администратора удалить из раздела **Администраторы**, его сессия будет автоматически завершена, и он 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 на 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 будет потерян. Если это произошло, обратитесь в Техническую поддержку.

Аутентификация администраторов

Ideco NGFW 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 считает попытку авторизации неудачной и блокирует доступ, если количество неудачных попыток превышает шесть.

Чтобы получить доступ к веб-интерфейсу Ideco NGFW, администратору нужно выполнить процедуру аутентификации, указав логин и пароль.

Для разных групп администраторов предусмотрены разные логины:

- **Локальный администратор** - логин в формат `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.

Ideco Center

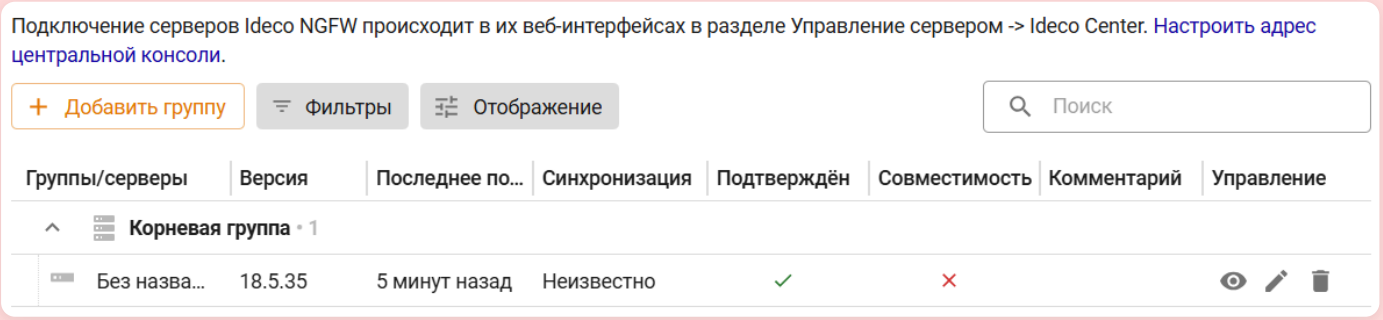
Название службы раздела **Ideco Center**: `ideco-central-console-backend`.

Список служб для других разделов доступен по ссылке.

Ideco Center - это центральная консоль, которая поможет в администрировании нескольких серверов Ideco NGFW. На данный момент не требует лицензирования и не имеет ограничений к использованию. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW, даже если они были подключены после того, как политики были настроены.

Подключение Ideco NGFW к Ideco Center

При синхронизации Ideco Center и Ideco NGFW 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 несовместимы:

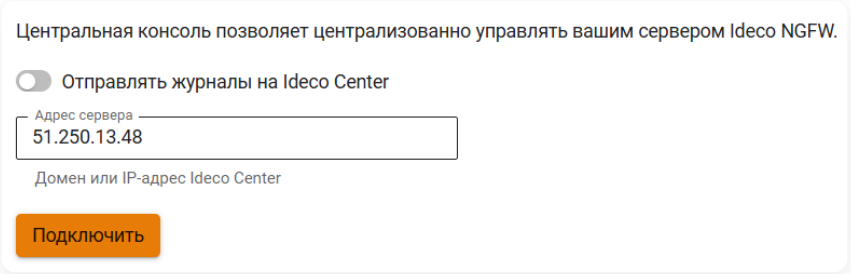


Особенности работы:

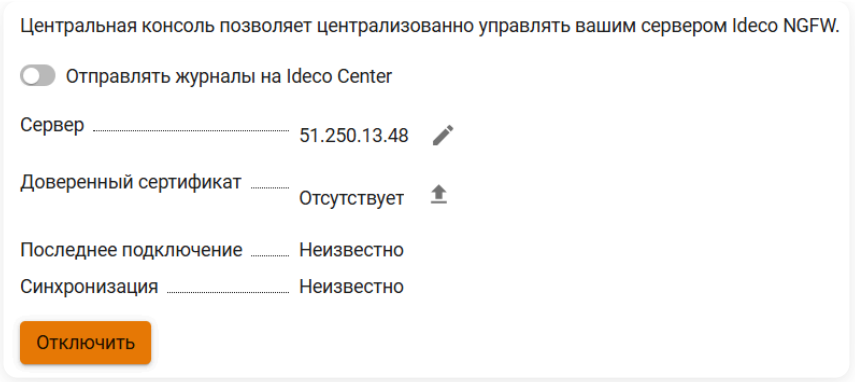
- Если в подключаемом Ideco NGFW используется кластер, достаточно подключить только активную ноду, пассивная автоматически примет эту настройку;
- Сетевое подключение производится в направлении от Ideco NGFW к Ideco Center, т. е. возможна связь и когда Ideco NGFW за NAT;
- Если сервер Ideco Center находится за NAT, укажите IP-адрес NAT-устройства или доменное имя, перейдя в Ideco Center в раздел **Управление сервером → Дополнительно → Адрес Ideco Center**.

1. Перейдите в раздел **Управление сервером → Ideco Center**.

2. Введите IP-адрес или доменное имя в строке **Адрес сервера** и нажмите **Подключить**:

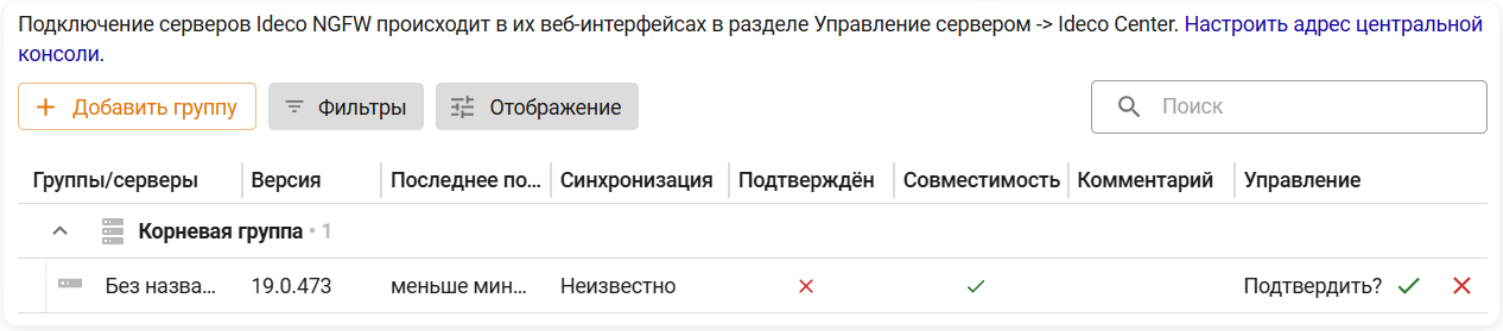


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW:

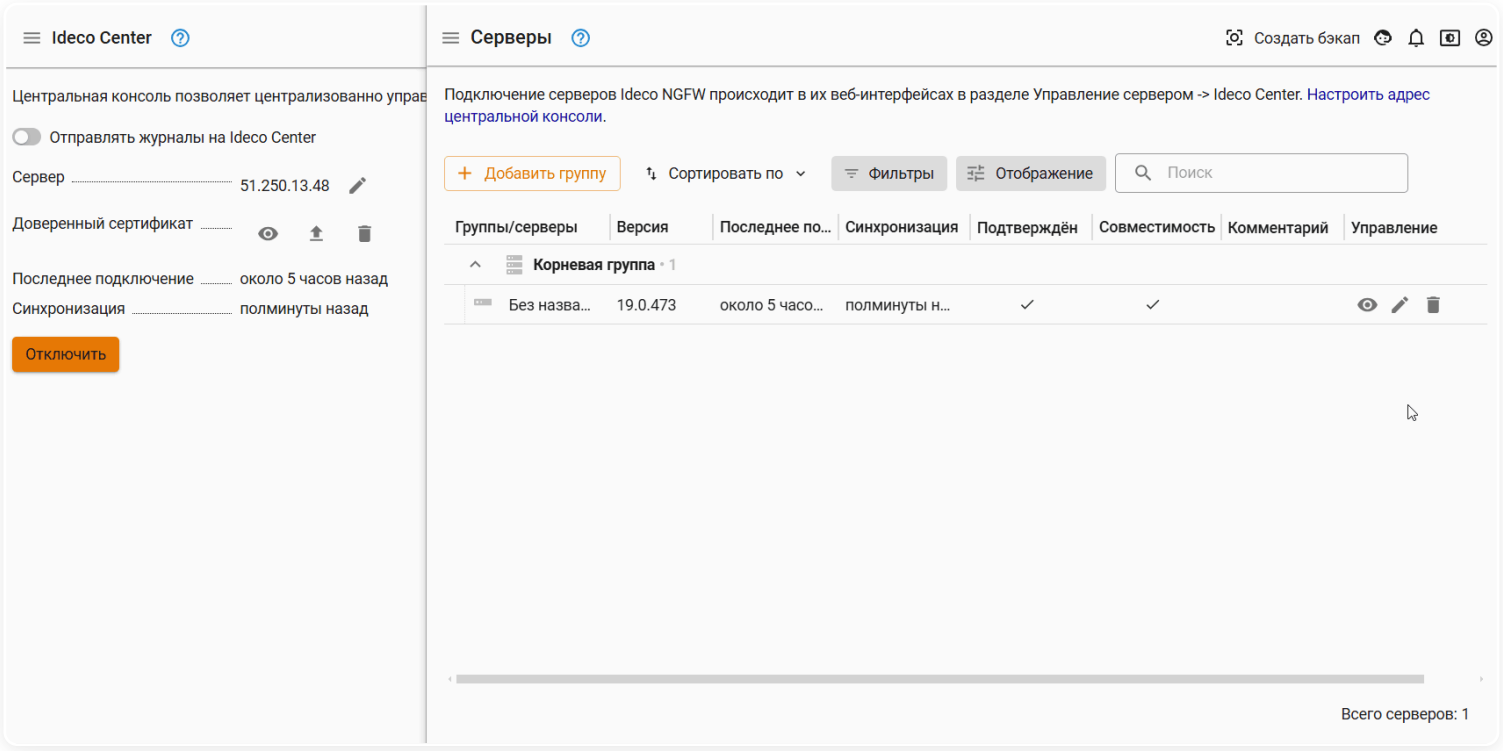


Скачать корневой сертификат можно в Ideco Center, раздел **Сервисы** → **Сертификаты**.

3. В интерфейсе Ideco Center перейдите в раздел **Серверы** и подтвердите подключение кнопкой :



Для удаления сервера Ideco NGFW из Ideco Center разорвите привязку в интерфейсе Ideco Center:



Настройка просмотра логов

Для отображения логов Ideco NGFW в разделе **Отчеты и журналы** Ideco Center необходимо включить опцию **Отправлять журналы на Ideco Center**:

Центральная консоль позволяет централизованно управлять вашим сервером Ideco NGFW.

Отправлять журналы на Ideco Center

Сервер 158.160.58.43

Доверенный сертификат .....

Последнее подключение ..... около 3 часов назад

Синхронизация ..... полминуты назад

Отключить

VCE

Название службы раздела **VCE**: `ideco-vce-backend`.

Список служб для других разделов доступен по ссылке.

VCE (virtual context engine) - это функциональность Ideco NGFW, реализованная с помощью контейнеров Linux на базе systemd-nspawn, которая позволяет создавать виртуальные серверы (контексты) на одном корневом NGFW. 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.

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.

Сейчас для каждого созданного VCE загружается файл лицензии корневой системы. Это значит, что на Ideco NGFW с лицензией на 100 пользователей можно создать неограниченное количество VCE, каждый из которых также будет поддерживать по 100 пользователей.

Функциональность созданных внутри NGFW виртуальных VCE почти не отличается от функциональности NGFW.

Возможности VCE:

- Создание виртуальных серверов Ideco NGFW и настройка независимых сетевых интерфейсов.
- Независимая настройка политик безопасности и прав доступа различным виртуальным NGFW.
- Связь с Ideco Center.
- Запуск и остановка виртуальных серверов с одного корневого NGFW.

В интерфейсе VCE недоступно:

- Создание кластера.
- Обновление.
- Переход в **Профиль** через иконку в шапке веб-интерфейса (настраивается в корневой системе).
- Возможность выключения и перезагрузки (настраивается в корневой системе).
- Энергосберегающий режим (настраивается в корневой системе).
- Изменение настроек часового пояса и языка (настраивается в корневой системе).

Важные моменты работы VCE:

- В бэкап корневого 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.
- Нельзя добавлять в VCE LACP-интерфейсы.
- **Не рекомендуем создавать VCE на нодах кластера.** Если на одной из нод кластера создан VCE, со второй нодой будут синхронизироваться только данные таблицы раздела **Управление сервером -> VCE**. После переключения на пассивной ноде будет создан VCE с тем же именем и комментарием, но внутренние настройки VCE (администраторы, сетевые интерфейсы, политики безопасности и т. д.) не перенесутся.

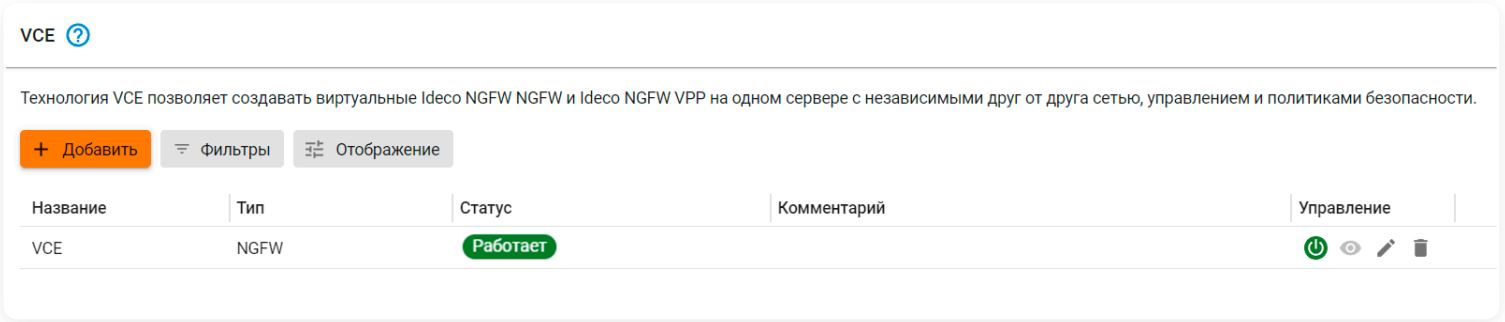
Создание VCE

Для работы VCE требуется минимум 8 ГБ оперативной памяти, а максимум можно выделить 16 ГБ.

Чтобы создать виртуальный сервер в рамках VCE, перейдите в раздел **Управление сервером** → **VCE** и выполните действия:

1. Нажмите кнопку **Добавить**.

2. Введите название сервера и нажмите **Добавить**. Виртуальный сервер появится в таблице:



3. Перейдите в раздел **Сервисы → Сетевые интерфейсы** и на вкладке **VCE** создайте интерфейс для виртуального сервера. Для работы VCE нужен минимум один сетевой интерфейс. Подробнее о создании VCE-интерфейсов в статье.

Сетевой интерфейс без тега VLAN, подключенный к VCE, будет недоступен для использования корневым NGFW.

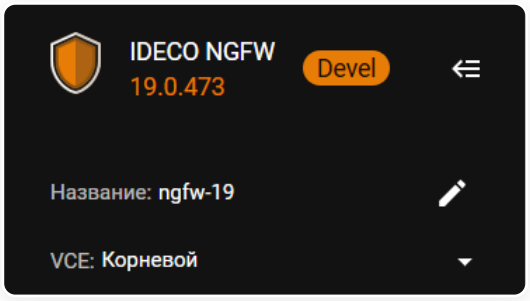
Если VCE выключен, переданные ему сетевые интерфейсы становятся вновь доступны корневому NGFW, их можно использовать для создания нового виртуального сервера. При этом VCE, которому они принадлежали ранее, станет недоступен после включения.

Чтобы отредактировать VCE, нажмите на . При редактировании можно менять название виртуального сервера. Редактирование доступно в том числе для работающего VCE.

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

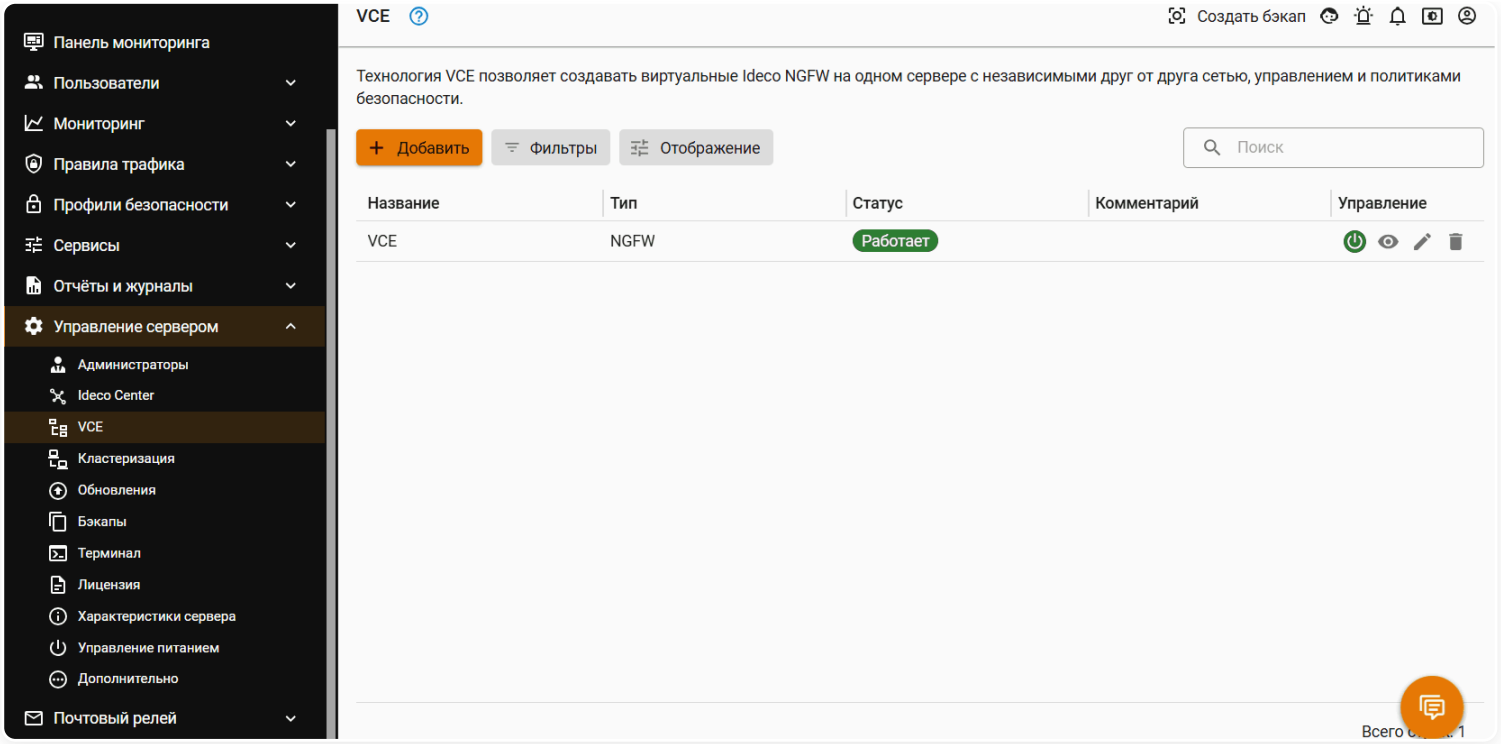
Переход в веб-интерфейс VCE

После создания VCE текущий сервер NGFW, в котором VCE был создан, будет обозначен как корневой:



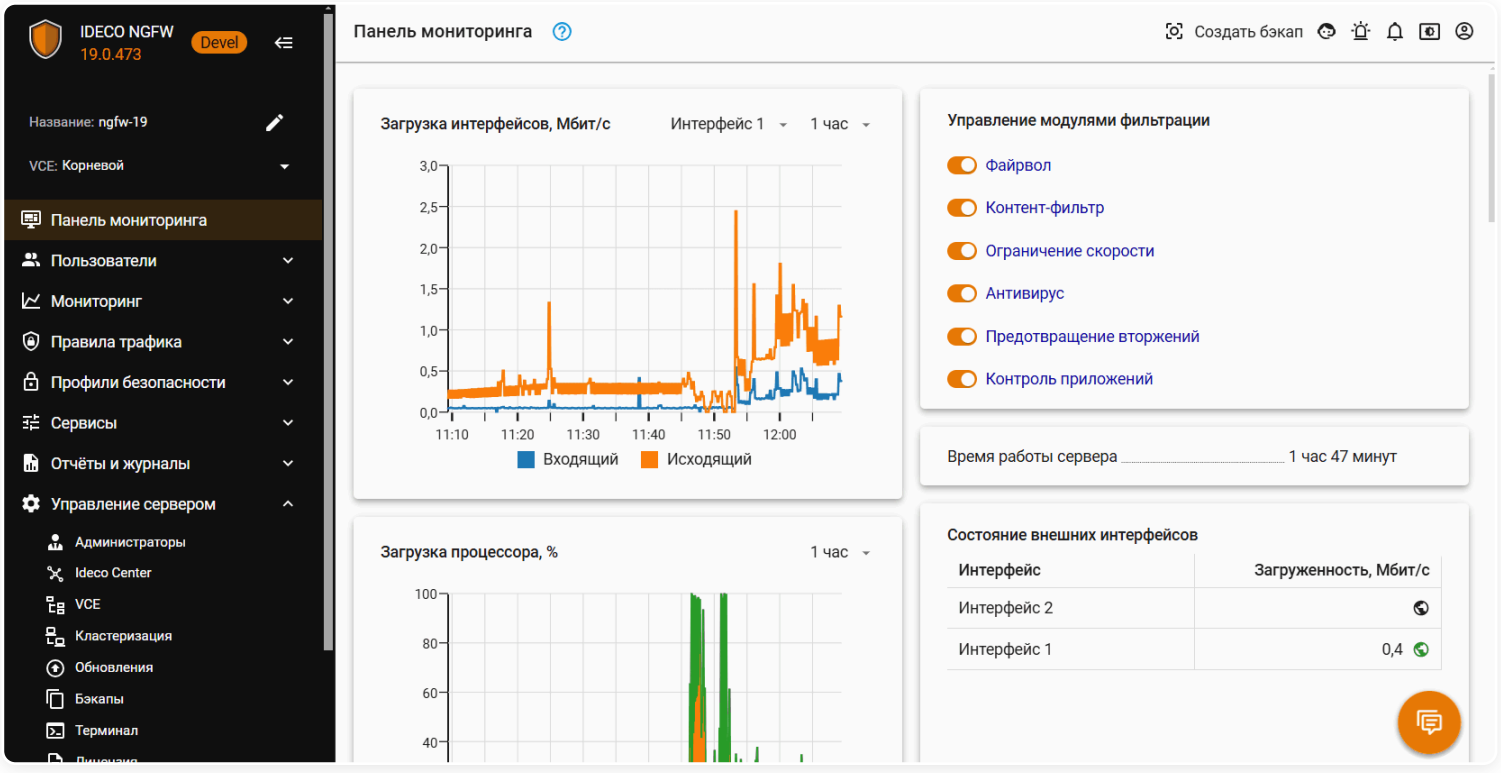
Перейти в веб-интерфейс созданного VCE из веб-интерфейса NGFW можно двумя способами:

1. Перейдите в **Управление сервером → VCE** и нажмите на :



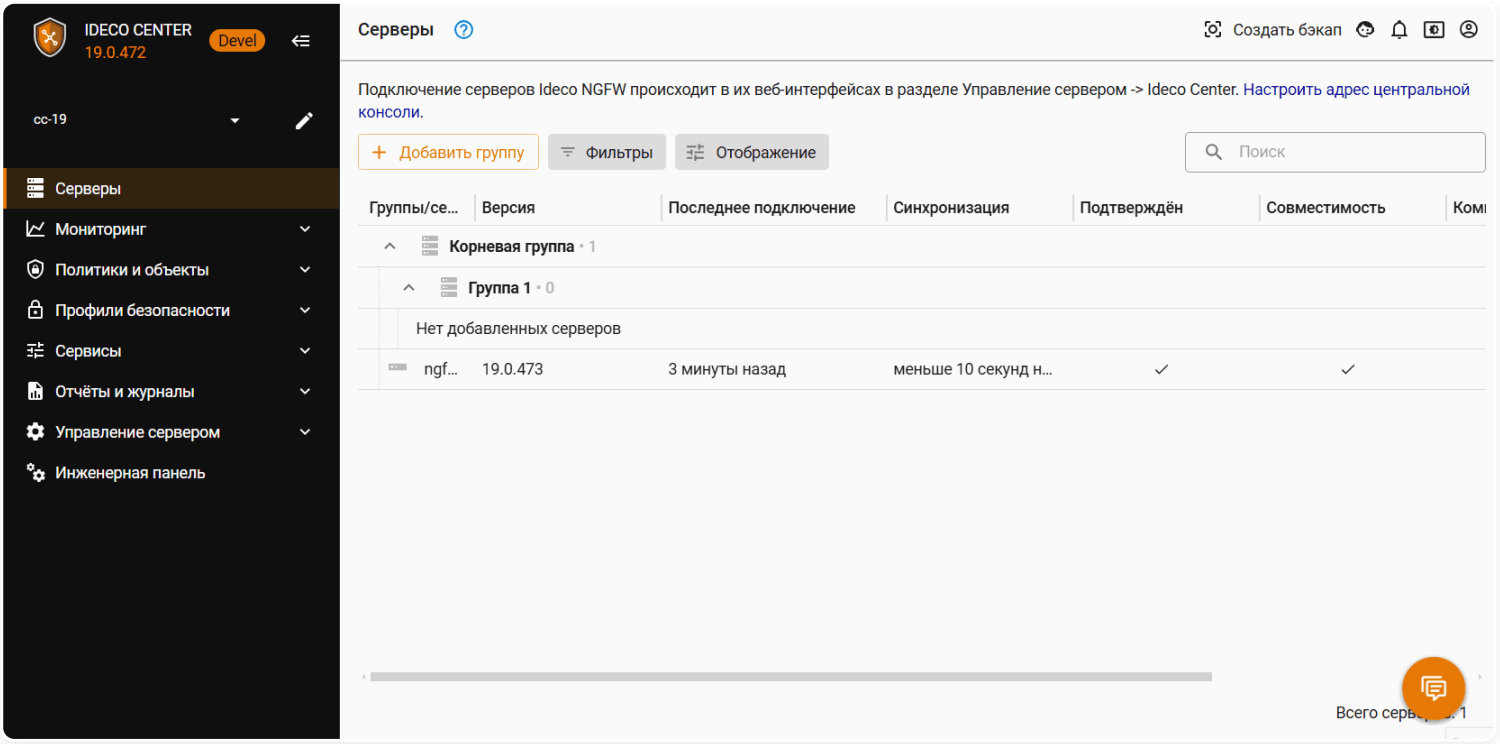
В новой вкладке откроется веб-интерфейс VCE.

2. Нажмите на  в левом верхнем углу и выберите нужный VCE:



Также перейти в веб-интерфейс VCE можно из веб-интерфейса Ideco Center. Для этого сначала перейдите из интерфейса Ideco Center в интерфейс корневого NGFW одним из способов, указанных в статье.

Пример перехода:



Удаление VCE

Удалить VCE можно, нажав на в корневом VCE.

После удаления VCE все его настройки, журналы и внутренние данные будут безвозвратно утеряны. Восстановить их будет невозможно.

Кластеризация

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, 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.

В любой момент обрабатывать трафик может только одна из нод.

Административно переключить ноды нельзя.

Критерии выбора активной ноды

- **Процент сетевых интерфейсов с линком** - отношение количества настроенных физических сетевых интерфейсов, находящихся в состоянии `up` и имеющих подключение (`carrier`), к общему числу настроенных физических интерфейсов. Значение `1.0` означает, что подключение присутствует на всех интерфейсах.
- **Количество деградаций сети** - число ухудшений значения показателя **Процент сетевых интерфейсов с линком**. Деградацией считается любое уменьшение значения относительно предыдущего максимума (например, `0.5` → `1.0` → `0.2` → `0.5` - одна деградация). Показатель используется для снижения вероятности переключений при нестабильных (мигающих) подключениях.
- **Uptime** - время непрерывной работы ноды с момента последней загрузки. Более высокий `uptime` означает более длительную и стабильную работу ноды без сбоев.

Сетевое взаимодействие между нодами осуществляется по *Кластерной сети*. Это физический канал, под который на каждой из нод резервируется по одному физическому порту. При переключении нод резервная нода становится активной.

Если IP-адреса кластера настроены вручную, то он 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.

Процесс синхронизации нод в кластере

- При синхронизации двух NGFW данные активной ноды копируются в резервную ноду. Вся информация на резервной ноде перезаписывается.
- 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.

Для корректной работы кластера необходимо постоянное наличие связи между нодами. Для моментального переключения ноды следует соединять прямым сетевым соединением, не используя мост или коммутатор.

Обмен данными между нодами кластера происходит раз в три минуты. 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

Имя сервера активной ноды отображается в левом верхнем углу веб-интерфейса, под именем кластера.

Для проверки статуса текущей ноды:

1. Перейдите в раздел **Управление сервером** → **Терминал** веб-интерфейса NGFW или в консоль в локальном меню.

2. Введите команду:

```
etcdctl_rt get /cluster/status/v1/record
```

Вывод команды:

- `{"state": "ACTIVE"}` - текущая нода - активная;
- `{"state": "RESERVE"}` - текущая нода - резервная;
- `{"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 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 раздел **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>` - для проверки статуса служб Ideco NGFW.

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.
- Время переключения нод - 15 секунд. При потери связи между нодами переключение происходит моментально.
- 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.

Возможные проблемы при работе двух Ideco NGFW 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 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 несовместим с агрегацией интерфейсов (LACP)**. При добавленном LACP-интерефейсе настройка кластера будет невозможна. В работающем кластере нельзя создать LACP-интерфейсы.

Для перехода между режимами требуется:

- Либо разрушить кластер (для создания LACP-интерфейса).
- Либо удалить агрегированные интерфейсы (для настройки кластера).

Не рекомендуем создавать VCE на нодах кластера. Если на одной из нод кластера создан VCE, со второй нодой будут синхронизироваться только данные таблицы раздела **Управление сервером -> VCE**. После переключения на пассивной ноде будет создан VCE с тем же именем и комментарием, но внутренние настройки VCE (администраторы, сетевые интерфейсы, политики безопасности и т. д.) не перенесутся.

Настройка кластера

Если на момент создания кластера у вас уже есть настроенный Ideco NGFW, рекомендуем выбрать его в качестве активной ноды. Все настройки резервной ноды в процессе создания кластера будут удалены.

Требования

Для создания кластера необходимо соблюдение следующих требований:

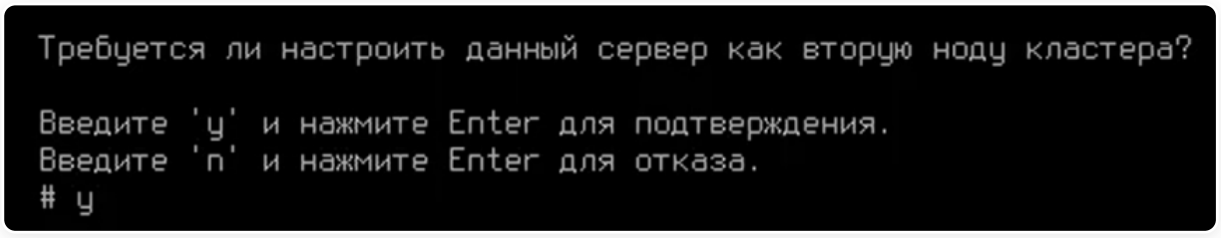
- В кластере может быть только две ноды Ideco NGFW;
- Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки;
- Количество **используемых** физических сетевых портов на обоих серверах должно совпадать. В ином случае создать кластер нельзя. При этом само наличие дополнительных физических сетевых портов на нодах на создание кластера никак не влияет;
- 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;
- Не рекомендуется объединять в кластер георазпределенные ноды;
- При работе NGFW на гипервизорах используйте средства отказоустойчивости гипервизора.

- Интерфейсы для создания кластерной сети на каждом Ideco NGFW 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 сетевой порт, предназначенный для связи между нодами, подключен к изолированной IPv6 сети.
- Запрещено добавлять сетевые интерфейсы, но РАЗРЕШЕНО отключать и редактировать. Удаление сетевого интерфейса, использующегося для связи между нодами, разрушит кластер.

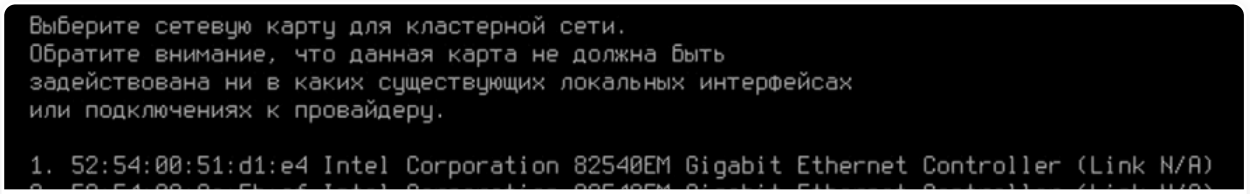
Шаг 1 - Конфигурация резервной ноды

Если только установили сервер Ideco NGFW

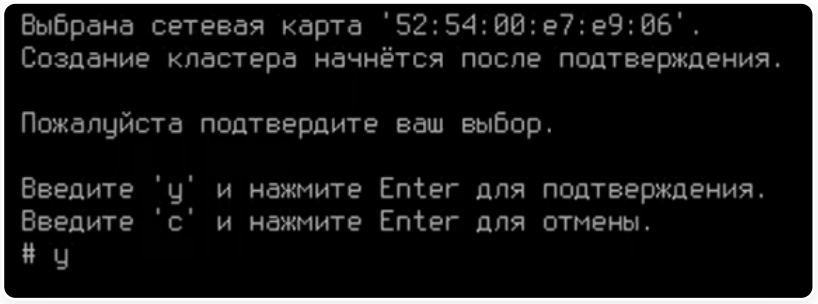
1. При входе в локальное меню резервной ноды, увидев следующее сообщение, введите **y** и нажмите **Enter**:



2. Выберите сетевой порт:

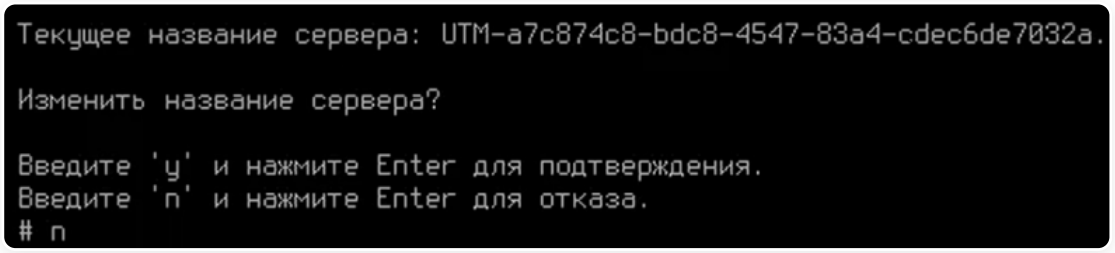


3. Подтвердите создание кластера, введя **y** и нажав **Enter**:



4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *Изменить название сервера?*, появится надпись с предложением ввести новое название.

Допустимое количество символов в названии - от 2 до 62:



После ввода нового названия нажмите **Enter** для продолжения.

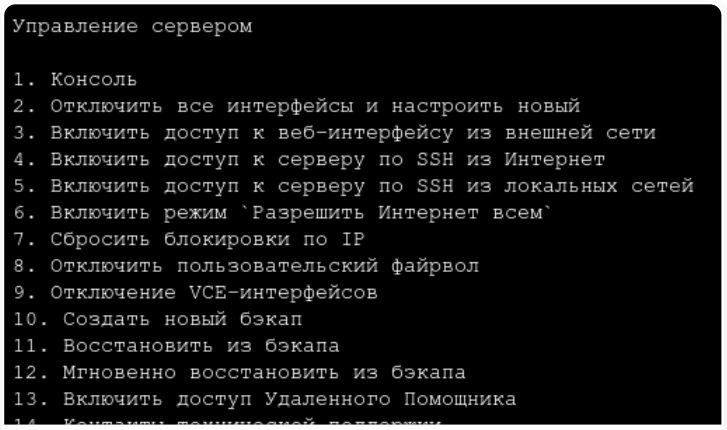
5. Появится сообщение, что процесс создания кластера запущен:

Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Если создаете резервную ноду из уже установленного сервера Ideco NGFW с лицензией и доступом в интернет

1. Перейдите в локальное меню;

2. Выберите пункт **Управление кластером**. Подтвердите создание кластера, введя **y** и нажав **Enter**:



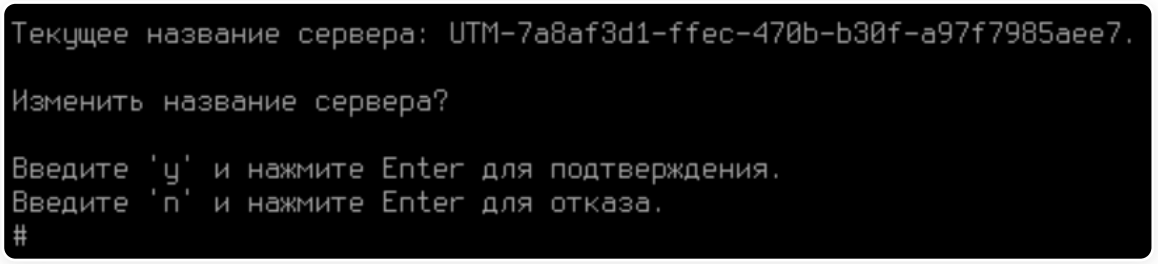
Если на ноде нет свободных сетевых портов, создание кластера будет недоступно.

Если кластер на ноде уже настроен, при выборе пункта *Управление кластером* будет доступно только его разрушение.

3. Выберите свободный физический сетевой порт для создания кластерной сети и подтвердите выбор:

4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *"Изменить название сервера?"* появится надпись с предложением ввести новое название.

Допустимое количество символов в названии - от 2 до 42:



После ввода нового названия нажмите **Enter** для продолжения.

5. Появится сообщение, что процесс создания кластера запущен:

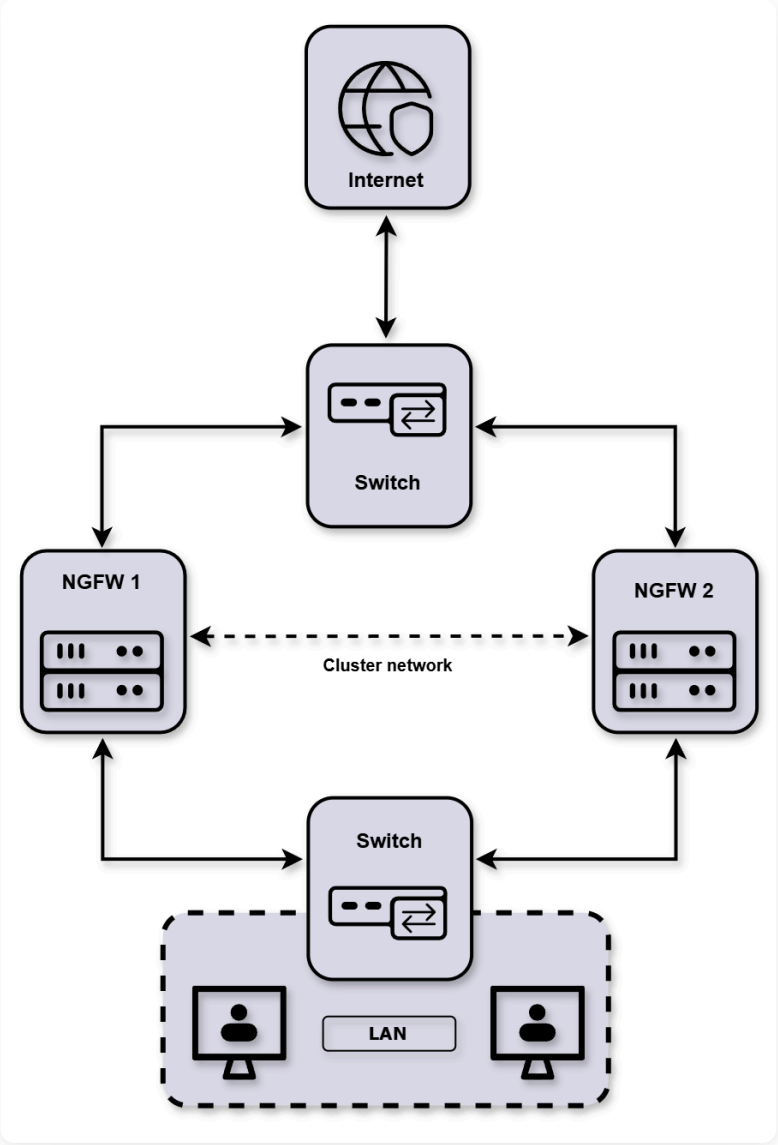
Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Шаг 2 - Конфигурация активной ноды

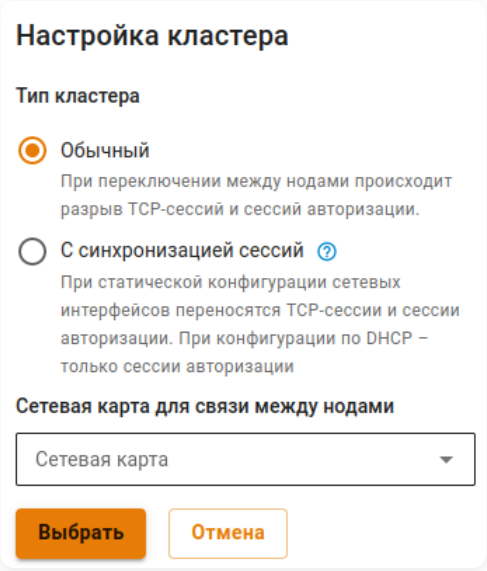
Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW выполните следующие действия:

1. Перейдите в раздел **Управление сервером** → **Кластеризация** и нажмите кнопку **Настроить кластер отказоустойчивости**.

2. Подтвердите, что топология сети соответствует схеме:



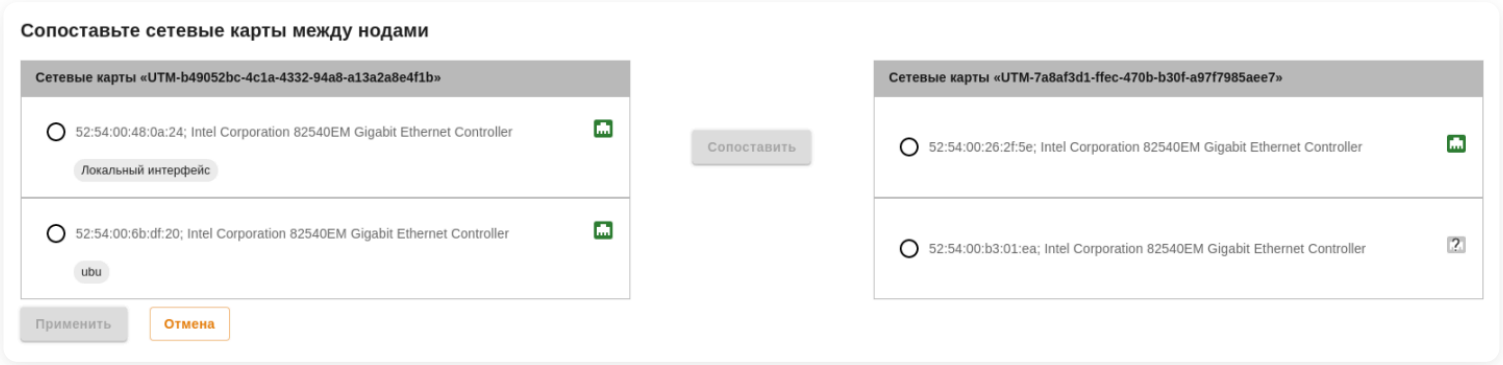
3. Выберите тип кластера и сетевой порт для соединения между нодами:



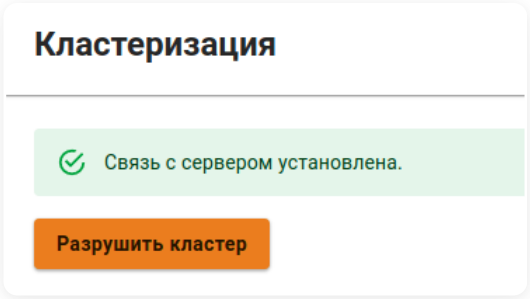
Если был настроен **Обычный** тип кластера, то при переключении между нодами происходит разрыв TCP-сессий пользователей и сессий авторизации.

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.

4. Сопоставьте сетевые порты. Для этого выберите в каждом столбце по одному сетевому порту и нажмите **Сопоставить**:



5. После применения настроек резервная нода перезагрузится, и в веб-интерфейсе активной ноды отобразится информация о том, что связь с сервером установлена.

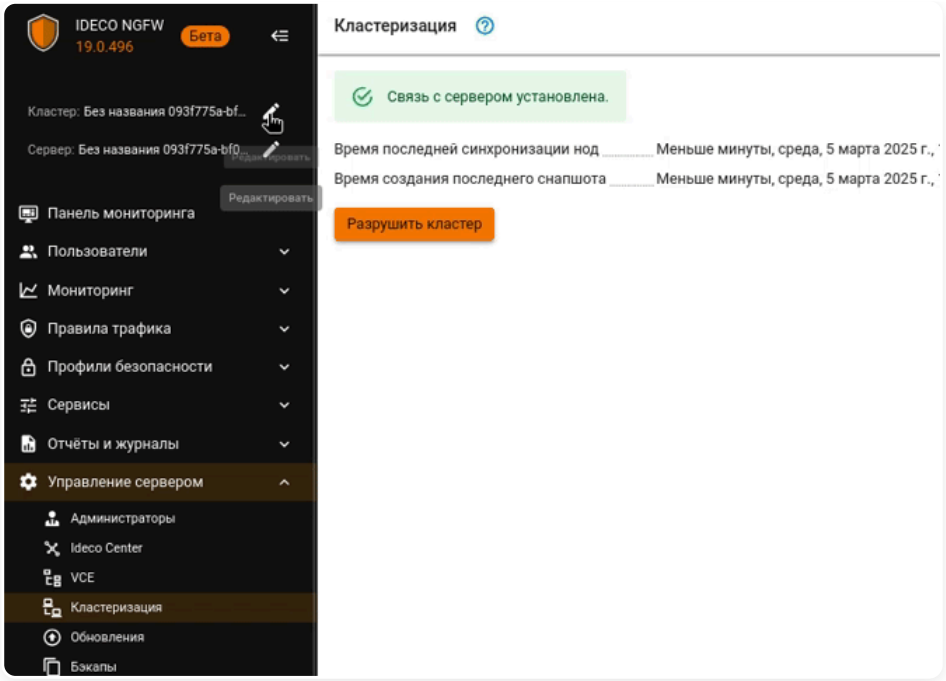


Во время перезагрузки резервной ноды в веб-интерфейсе активной ноды может временно отображаться статус о потере связи. Соединение восстановится автоматически после завершения загрузки резервной ноды.

Локальное меню резервной ноды недоступно в NGFW, начиная с версии 16.0.

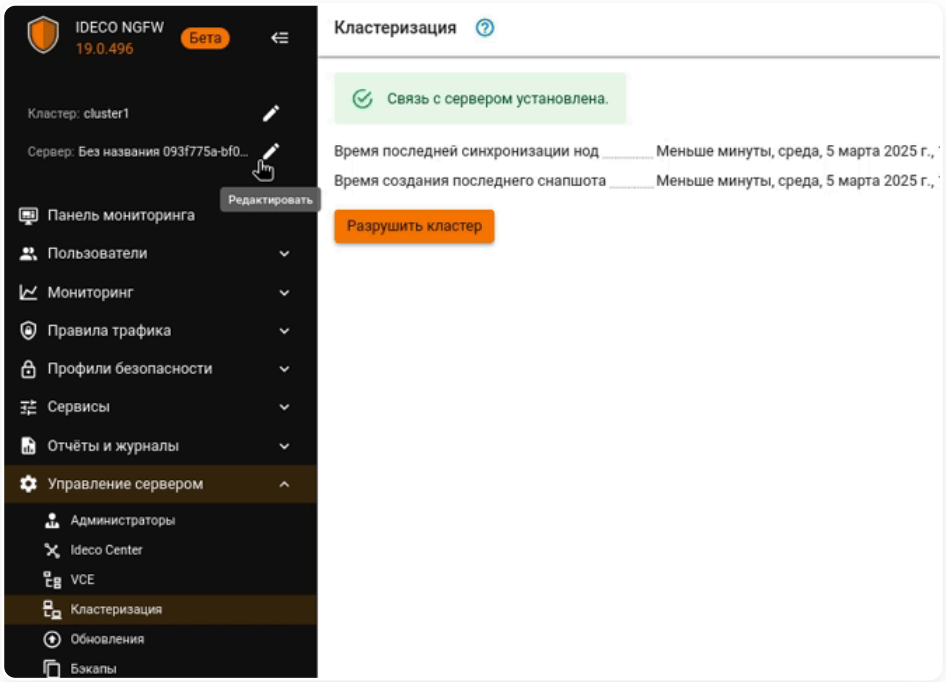
Изменение названия кластера

Изменить название кластера можно в веб-интерфейсе активной ноды, нажав на кнопку **Редактировать** рядом с названием кластера в левом верхнем углу экрана:



Изменение названия сервера

Изменить название сервера можно у активной ноды из веб-интерфейса, нажав кнопку **Редактировать** рядом с названием сервера в левом верхнем углу экрана:

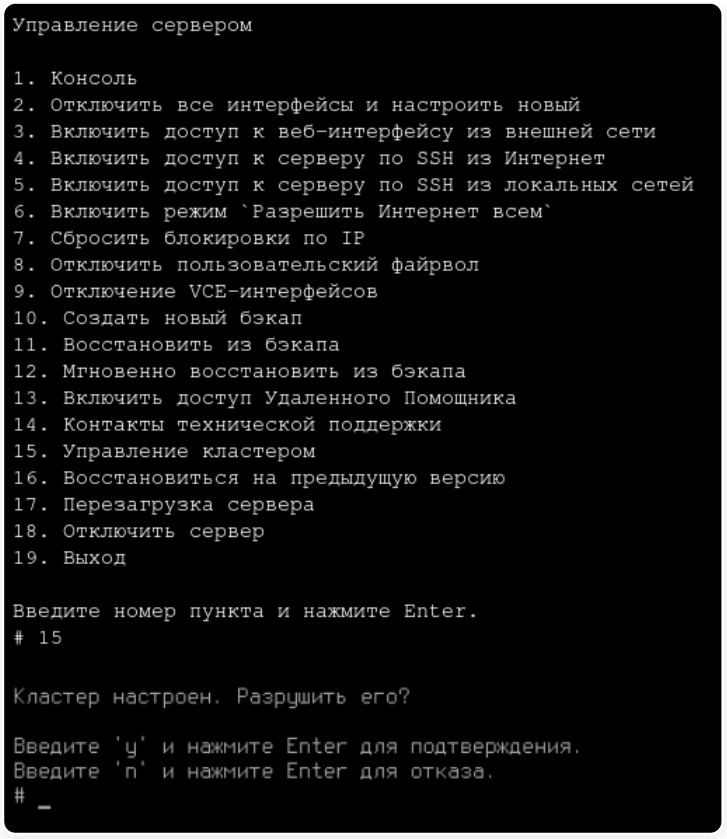


Разрушение кластера

Разрушить кластер можно только из локального меню или веб-интерфейса *активной* ноды. При этом она продолжит работать, а вторая нода (резервная) сбросит настройки до состояния только что установленного Ideco NGFW.

Разрушение кластера из локального меню:

1. Выберите пункт локального меню **Управление кластером**, введите **y** и нажмите **Enter**;

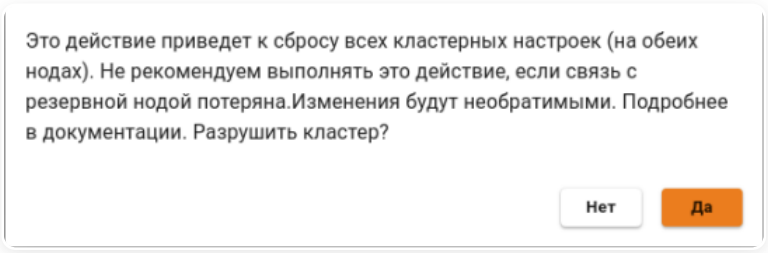


2. Подтвердите выбор.

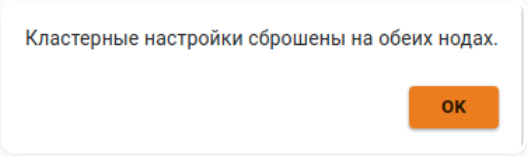
Разрушение кластера из веб-интерфейса:

1. Перейдите в раздел **Управление сервером** → **Кластеризация** и нажмите кнопку **Разрушить кластер**.

2. Появится окно с предупреждением:



3. Нажмите **ОК**:



Обновление кластера

Процесс обновления Ideco NGFW 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 разделе **Управление сервером** → **Обновление**. Сработает алгоритм обновления кластера Ideco NGFW:

- 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 она 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

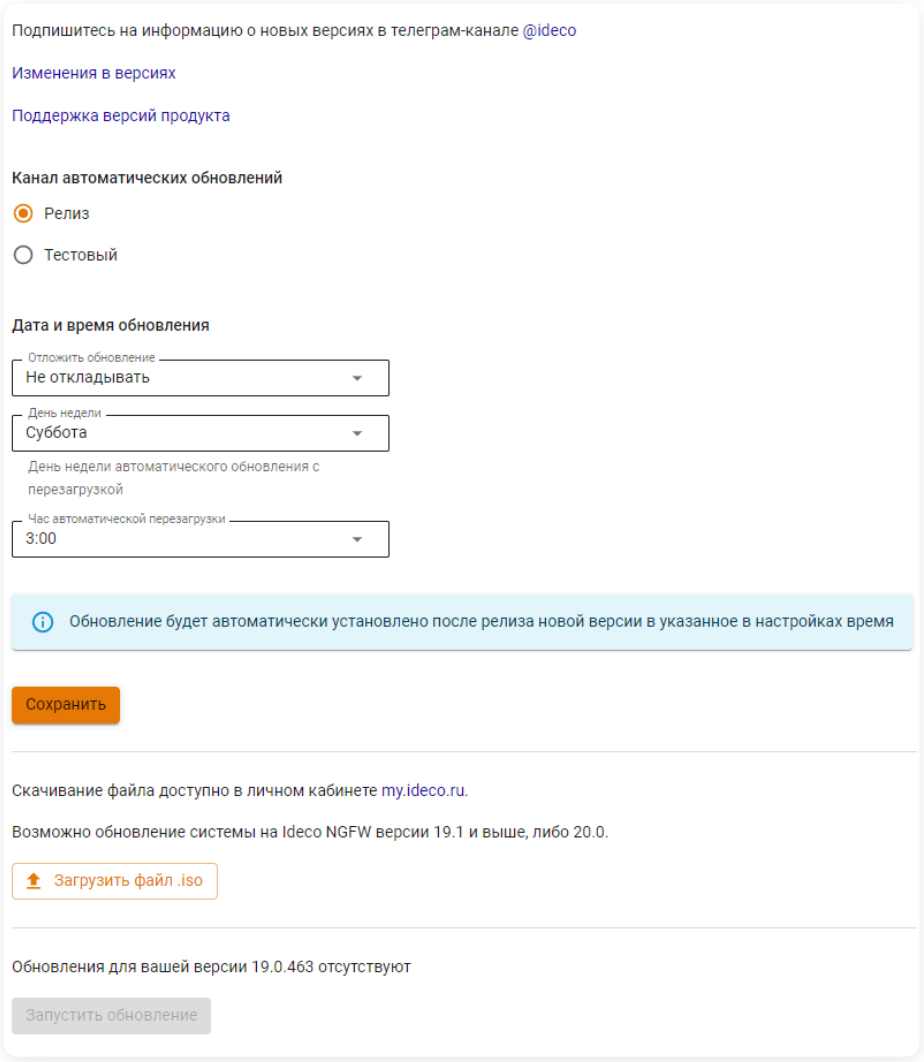
Название службы раздела **Обновления**: `ideco-sysupdate-backend`.

Список служб для других разделов доступен по ссылке.

Система

Обновить систему Ideco NGFW можно как в офлайн-режиме, так и через интернет. Отрегулировать режим обновления можно в разделе **Управление сервером → Лицензия**.

В режиме **Автоматического обновления** доступны следующие настройки:



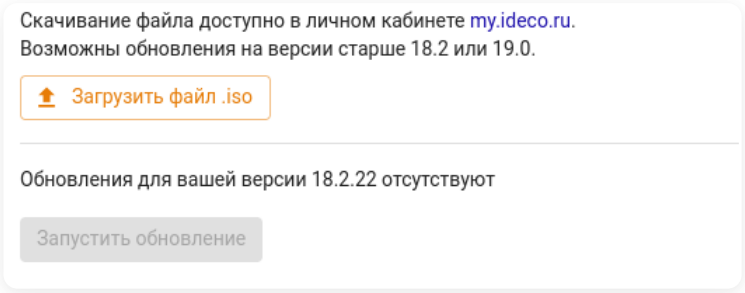
Расшифровка полей

- **Канал обновлений** - пункт **Релиз** позволяет обновляться на стабильно работающие версии. Пункт **Тестовый** позволяет быстрее обновляться как на релизные версии, так и на последние бета-версии продукта во время коротких периодов бета-тестирования новых мажорных версий. По умолчанию выбран пункт **Релиз**.
- **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.
- **Загрузить файл .iso** - позволяет обновить Ideco NGFW путем загрузки ISO-образа необходимой версии.
- **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

По умолчанию сервер обновляется по субботам в 3:00. Чтобы выполнять обновление Ideco NGFW 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.

В режиме **Ручной загрузки** обновлений необходимо скачать ISO-образ новой версии Ideco NGFW в личном кабинете MY.IDECO и загрузить его с внешнего носителя:



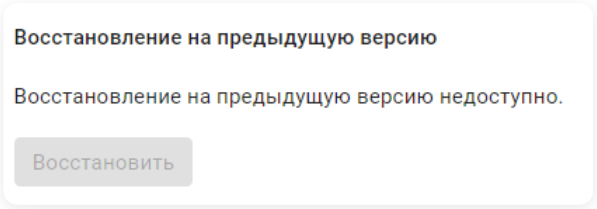
Кнопка принудительного обновления активна, когда обновление уже скачано, и только применяет его, инициировать скачивание нельзя.

После принудительного обновления потребуется полная перезагрузка сервера.

После проведения процедуры обновления новая версия будет отображаться в верхнем левом углу веб-интерфейса NGFW.

Обновить серверы Ideco NGFW, подключенные к центральной консоли, можно через Ideco Center. Для этого нужно перейти в интерфейс NGFW одним из способов, указанных в разделе Ideco Center.

Восстановление на предыдущую версию



Кнопка **Восстановить** позволяет вернуться к предыдущей версии NGFW. Система будет перезагружена, при этом текущие настройки будут потеряны. После восстановления отложите автоматическое обновление.

Если в **Ideco NGFW** настроен кластер, то в веб-интерфейсе будет отсутствовать пункт **Восстановление на предыдущую версию**.

При восстановлении на предыдущую версию данные перенесены не будут. NGFW 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 не ниже той, на которой он был создан.

Процесс выхода релизов в каналы обновлений

Тестовый канал обновлений позволяет быстрее обновляться до новых версий (релизных или бета-версий во время их активного тестирования). После выхода бета-версии NGFW в **Тестовый** канал ожидается обратная связь от пользователей по использованию новой версии продукта. Обратная связь позволяет выявить недочеты и уязвимости в продукте. После их исправления происходит выкладка в канал **Релиз**.

Если в версии NGFW, вышедшей в канал **Релиз**, в ходе использования выявляются недочеты, то они исправляются ближайшими обновлениями версии. Обновление в канале **Релиз** появляется постепенно.

Особенности обновления

NGFW

- 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 Changelog.
- Номер мажорной версии NGFW - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7).
- Автоматическое обновление Ideco NGFW до следующей мажорной версии возможно только после установки последней минорной версии, выпущенной в релиз. Например, можно обновить NGFW 17.2 до версии 17.9, а затем до версии 18.6.
- Ручное обновление Ideco NGFW до следующей мажорной версии можно выполнить с любой версии. Например, можно обновить NGFW 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 все включенные VCE автоматически обновляются вместе с корневым NGFW.
- Если в системе есть выключенные VCE, которые созданы в младшей версии корневого NGFW и не запускались после обновления, то обновление корневого NGFW на следующую мажорную версию будет заблокировано.

Пример: Если в NGFW версии 18.3 создали VCE, затем выключили его и обновили корневой NGFW 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.

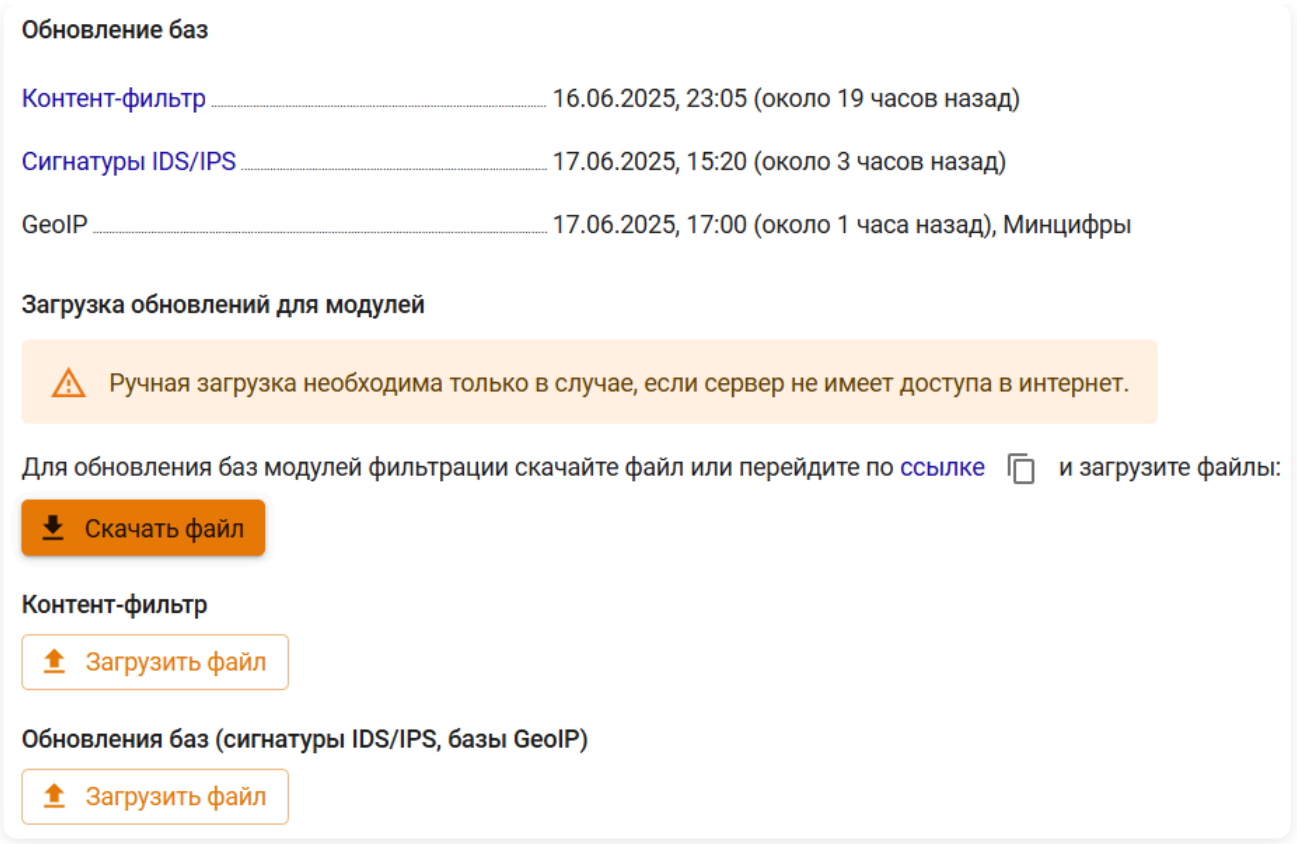
- Если VCE не включался после обновления корневого NGFW, то:
  - VCE останется на предыдущей версии.
  - Корневой NGFW можно обновить в рамках текущей мажорной версии.

  Пример: корневой NGFW 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.

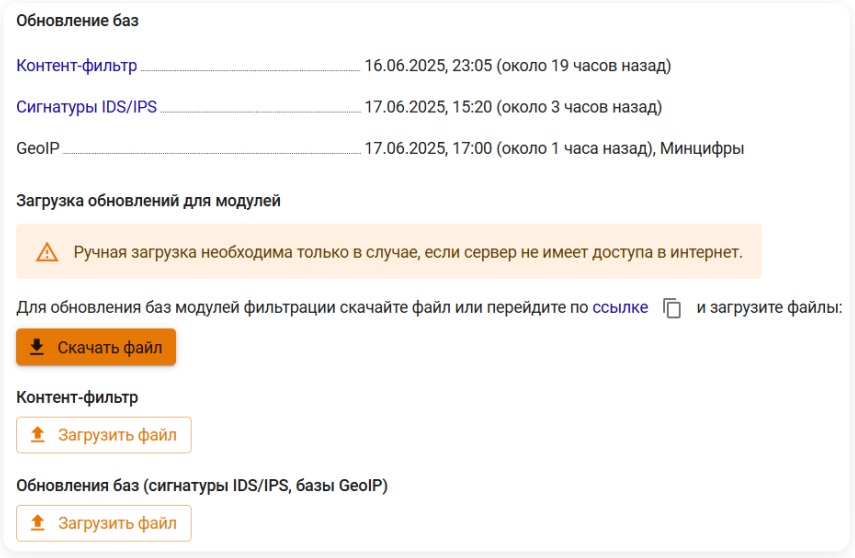
Базы фильтрации



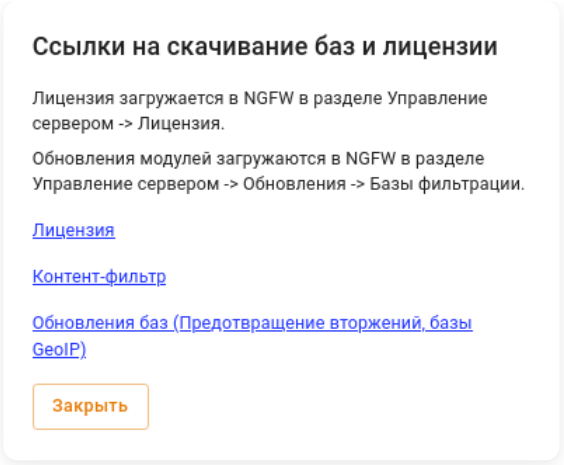
На вкладке доступны обновления баз модулей фильтрации Ideco NGFW - баз **Контент-фильтра** и модуля **Предотвращения вторжений**, а также баз соответствия подсетей и стран (GeoIP).

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 выполните действия:

1. В интерфейсе Ideco NGFW 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.

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

Полезные ссылки

- **Источники данных**

Бэкапы

Бэкап - это предварительно созданная резервная копия данных, позволяющая восстановить большинство настроек и сохраненной информации.

Название служб раздела **Бэкапы**: `ideco-backup-backend`; `ideco-backup-create`; `ideco-backup-restore`; `ideco-backup-rotate`.

Список служб для других разделов доступен по ссылке.

В NGFW создается только полный бэкап, который включают в себя 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 корневого VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте бэкап отдельно по корневому VCE и по каждому из дочерних VCE.

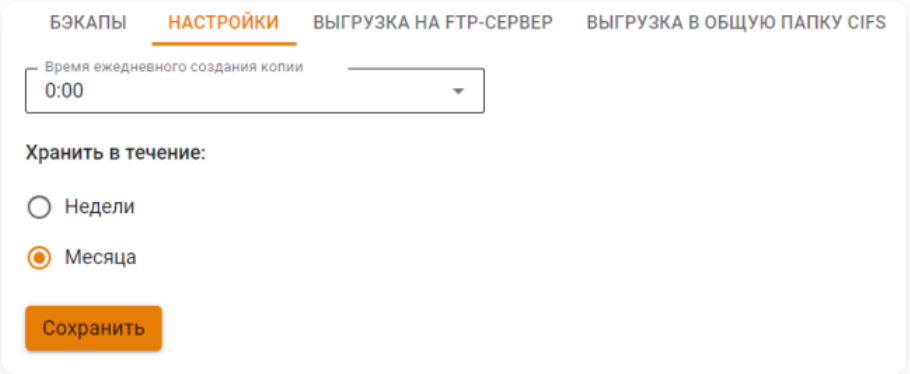
В NGFW бэкап создается как автоматически, так и вручную.

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 на контроллере домена. При каждом изменении настроек интеграции информация для аутентификации NGFW обновляется. Для решения проблемы интеграции NGFW с AD, ALD сделайте переинтеграцию NGFW с соответствующим сервисом.

Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в раздел **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** - 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 предоставляет возможность выгружать бэкапы:

- на сетевое файловое хранилище по протоколу FTP;
- на сетевое файловое хранилище по протоколу NetBIOS (CIFS);
- на 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. 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)

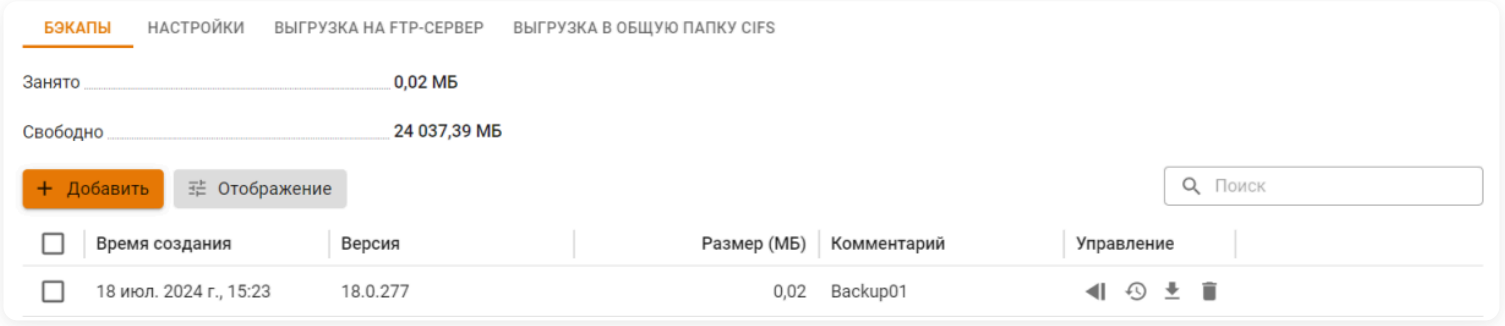
Ключевые параметры, необходимые для настройки бэкапа на NetBIOS-сервер, описаны в таблице:

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 перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и нажмите **Добавить** → **Создать**. Введите комментарий и нажмите **Добавить** или нажмите **Создать бэкап** в правом верхнем углу веб-интерфейса. Новый бэкап появится в таблице:



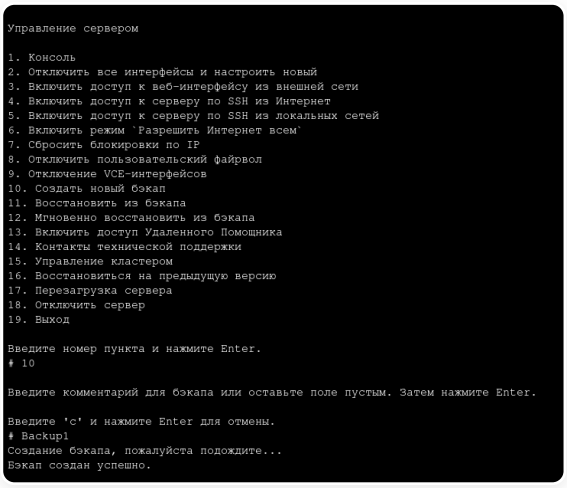
Через локальное меню

Чтобы создать новый бэкап через локальное меню Ideco NGFW, выполните действия:

1. Выберите пункт **10** 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. Выгрузка на внешние сетевые хранилища производится только при автоматическом создании бэкапа.

Восстановление конфигурации из бэкапа

В рамках одного сервера

В NGFW восстановление из бэкапа возможно полное и мгновенное.

При выполнении полного восстановления система будет перезагружена для применения настроек сервера. При мгновенном восстановлении бэкап применяется без перезагрузки.

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 автоматически отправит запрос в MY.IDECO для обновления лицензии. Если используется офлайн-лицензия, ее необходимо загрузить самостоятельно.

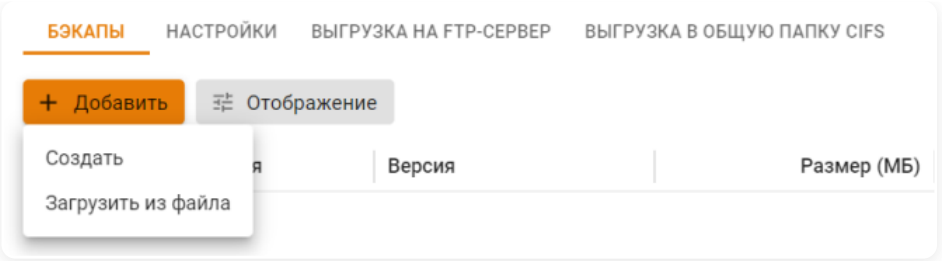
Полное восстановление конфигурации возможно только из бэкапов, версия которых не превышает версию текущей установленной системы.
Например, для Ideco NGFW версии 20 подойдут бэкапы с 19 или 20 версии. При этом важно учитывать минорные версии: например, в версии 19.13 невозможно восстановление из бэкапа, 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** → **вкладка Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

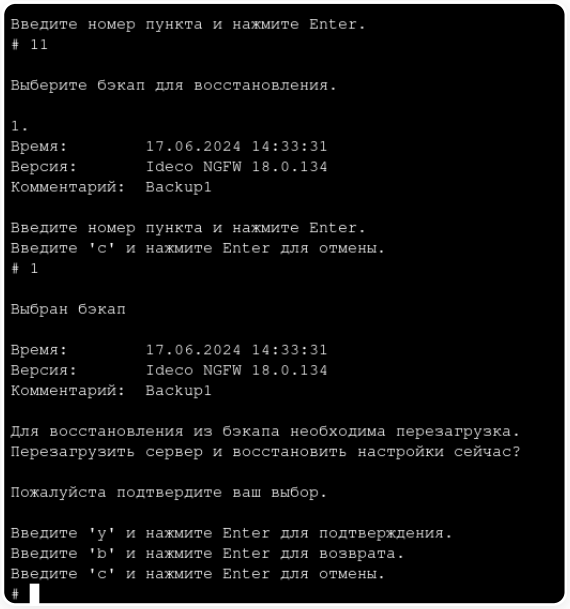
- **11** - восстановятся все настройки и перезагрузится сервер.
- **12** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

  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:



На другом сервере

Если необходимо восстановить конфигурацию из бэкапа на другом сервере, установите Ideco NGFW на новый сервер и выполните шаги по восстановлению данных:

1. На новом сервере перейдите в **Сервисы** → **Сетевые интерфейсы** и запишите MAC-адрес локальной сетевой карты, он потребуется для перенастройки локального интерфейса.

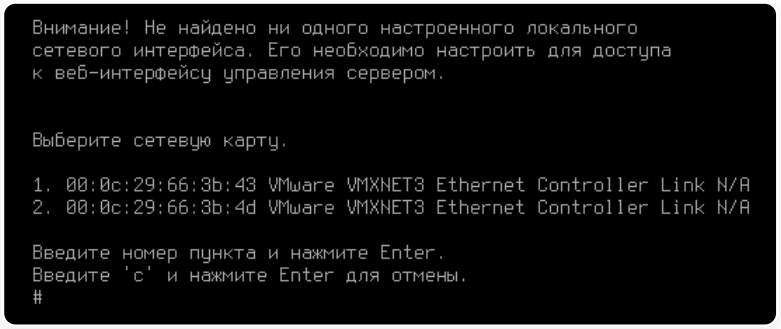
2. Перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите **Добавить** → **Загрузить из файла** и выберите созданный на другом сервере бэкап.

3. Нажмите кнопку в столбце **Управление**. Система будет перезагружена для применения настроек сервера.

После перезагрузки веб-интерфейс будет недоступен, поскольку ни один локальный интерфейс не настроен.

4. Зайдите в локальное меню Ideco NGFW, введите логин и пароль.

5. Выберите сетевую карту с MAC-адресом, который записали ранее, и настройте локальный интерфейс следуя инструкции в статье Процесс установки:



После настройки локального интерфейса обязательно перезагрузите сервер, иначе восстановление пройдет некорректно.

6. Перейдите в веб-интерфейс в **Сервисы** → **Сетевые интерфейсы** и настройте интерфейсы, восстановленные из бэкапа, привязав к ним сетевые карты:

7. Проверьте корректность настроек в разделах:

- **Сервисы** → **Защита и управление DNS** - выданные подключению внешние DNS-серверы.
- **Сервисы** → **DHCP** - опции DHCP-сервера.
- **Сервисы** → **OSPF** - настройки интерфейсов.
- **Правила трафика** → **Файрвол** - зоны источника и зоны назначения в правилах.
- **Сервисы** → **Маршрутизация** → **Внешних сетей** - правила маршрутизации.

Привязка лицензии к новому серверу

Если сервер переносится из-за неисправности старого, необходимо перепривязать лицензию. Для этого:

1. Перейдите в MY.IDECO.

2. Отвяжите лицензию от неисправного сервера, нажав на .

3. Отвяжите demo-лицензию от нового сервера, нажав на .

4. Привяжите enterprise-лицензию к новому серверу, нажав **Привязать лицензию**.

При подключении к Ideco Center клон сервера, восстановленный из бэкапа, не появится в таблице серверов Ideco Center. Изменится только **Последнее подключение** в строке неисправного сервера. Это происходит из-за конфликта с донором бэкапа, если у них одинаковый cluster_id. Сервер-клон подменяет собой уже подключенный Ideco NGFW.

В случае возникновения такой проблемы 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 на физический диск.

3. Подключите второй физический диск, который будет использоваться для хранения почты.

4. В веб-интерфейсе Ideco NGFW перейдите в **Почтовый релей** → **Основные настройки**, выберите диск для хранения почты и отформатируйте его.

5. Разрешите доступ по SSH из локальных сетей в разделе **Управление сервером** → **Администраторы**.

6. Подключитесь к NGFW, 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 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.

Терминал

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`).
- **Проверка скорости интернета:** `speedtest-cli`.
- **Просмотр ARP-таблицы:** `ip neigh show`.
- **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 Файрвола:**
  - `iptables -L |grep fwd.sys.<id правила>` - для просмотра системных правил Forward.
  - `iptables -L |grep inp.sys.<id правила>` - для просмотра системных правил Input.
- **Вызов локального меню:** `ideco-local-menu --debug` - команда используется для доступа к локальному меню Ideco NGFW.

Таблица служб

Раздел	Имя службы
Файрвол	ideco-nflog;ideco-firewall-backend
Профили контроля приложений	ideco-app-backend; ideco-app-control-nfq
Контент-фильтр	ideco-content-filter-backend
Ограничение скорости	ideco-shaper-backend
Антивирус	ideco-av-backend
Предотвращение вторжений	ideco-suricata-backend; ideco-suricata; ideco-suricata-event-syncer; ideco-suricata-profiles-syncer
Объекты	ideco-alias-backend
Сетевые интерфейсы	ideco-network-backend; ideco-network-nic
Балансировка и резервирование, Маршрутизация	ideco-routing-backend
BGP, OSPF	frr; ideco-routing-backend
Прокси	ideco-proxy-backend; squid
Обратный прокси	ideco-reverse-backend
DNS	ideco-dns-backend; unbound; nsd
DDNS	ideco-dns-backend
DHCP	ideco-dnsmasq
NTP	chronyd
IPsec	ideco-ipsec-backend; strongswan
Ideco Center	ideco-central-console-backend
VCE	ideco-vce-backend
Кластеризация	ideco-cluster-backend; ideco-cluster-backup-pusher
Обновления	ideco-sysupdate-backend

Раздел	Имя службы
Бэкапы	ideco-backup-backend; ideco-backup-create; ideco-backup-restore; ideco-backup-rotate
Лицензия	ideco-license-backend
VPN-подключения	ideco-accel-l2tp; ideco-accel-pptp; ideco-accel-sstp; ideco-vpn-servers-backend; ideco-vpn-authd; ideco-vpn-dhcp-backend
Авторизация	ideco-auth-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-authd
Active Directory	ideco-ad-backend; ideco-ad-log-collector@<имя домена>
ALD Pro	ideco-ald-rest; ideco-ald-backend
Ideco Client	ideco-agent-backend; ideco-agent-websocket
Syslog	ideco-logs-backend
Обнаружение устройств	ideco-netscan-backend
Web Application Firewall	ideco-waf-backend; ideco-waf-event-syncer
IGMP Proxy	ideco-igmpproxy-backend; ideco-igmpproxy

Примеры использования утилит

Примеры использования утилиты vtysh

Просмотр таблицы маршрутизации

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в раздел **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.

Просмотр конфигурации FRR

Убедитесь, что включен модуль OSPF и/или BGP.

1. Перейдите в раздел **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 раздел **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 раздел **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
```

Лицензия

Название службы раздела **Лицензия**: `ideco-license-backend`.

Список служб для других разделов доступен по ссылке.

В разделе **NGFW** личного кабинета 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.

Добавление коммерческой (Enterprise) лицензии

1. Скопируйте токен лицензии из письма, отправленного после покупки лицензии. Формат токена: `owhYLGvT6Xmt819JyinSxREkJfvjVO63`.

2. Перейдите в личный кабинет MY.IDECO в раздел **NGFW** → **Лицензирование** и нажмите **Добавить коммерческую лицензию**.

3. Введите токен в поле **Токен лицензии** и нажмите **Добавить**.

Токен станет недействительным, а в таблице **Свободные лицензии** отобразится купленная лицензия.

Если требуется перепривязать купленную лицензию к серверу с уже установленной тестовой лицензией, воспользуйтесь статьей.

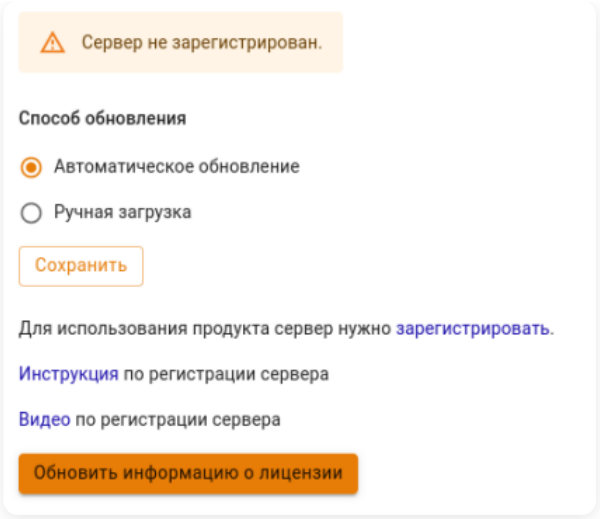
Добавление FREE (бесплатной) лицензии

Для добавления FREE-лицензии нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Свободные лицензии**.

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.

Чтобы выбрать онлайн-привязку, в веб-интерфейсе Ideco NGFW в разделе **Управление сервером** → **Лицензия** выберите способ обновления **Автоматическое обновление**, для офлайн-привязки выберите **Ручную загрузку**:



Назначьте имеющиеся коммерческие лицензии на любой зарегистрированный сервер Ideco NGFW с учетом следующих ограничений:

- Одна лицензия может быть привязана только к одному серверу.
- Демо-лицензию нельзя привязать к другому серверу.
- 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. При замене оборудования или его частей она отвязывается и требует повторной привязки. Демо-лицензия при этом теряется.

Онлайн-привязка лицензии

В MY.IDECO на вкладке **Лицензирование** нажмите **Привязать лицензию**. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения.

Офлайн-привязка лицензии

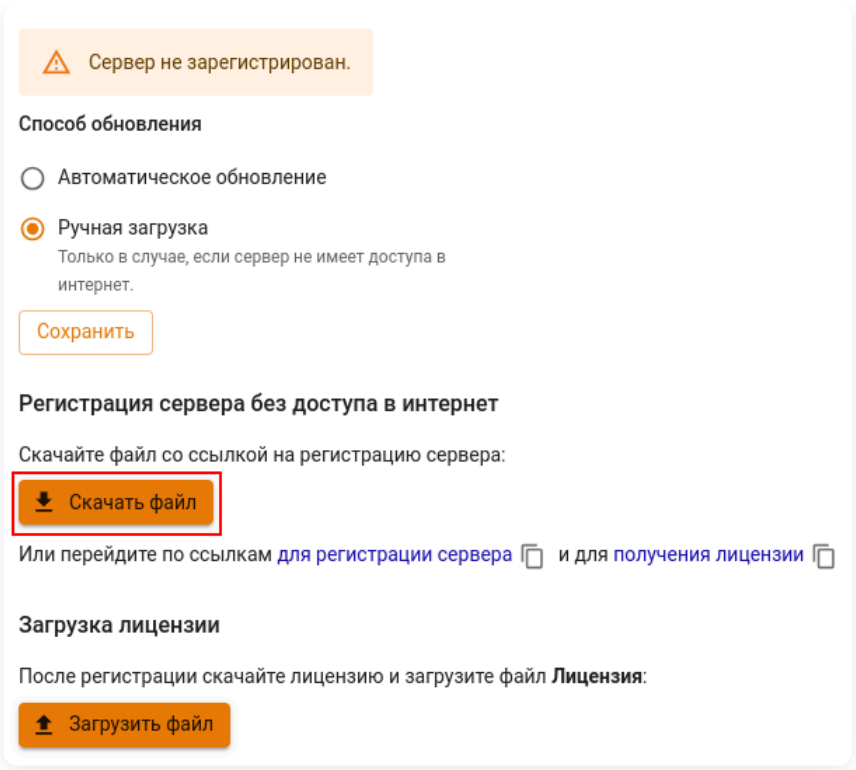
Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

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

2. Скачайте файл со ссылкой для регистрации сервера, загрузки баз данных и получения лицензии. Это можно сделать, нажав на кнопку, или скопировать ссылку из веб-интерфейса:

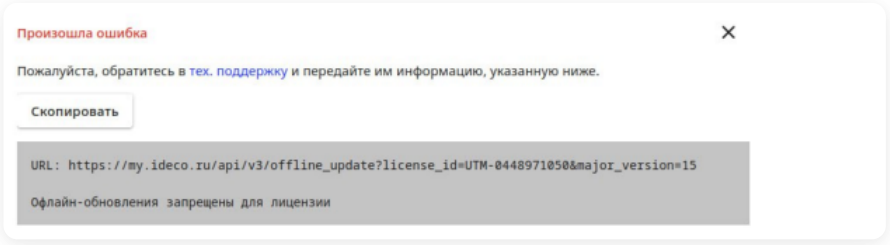


3. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

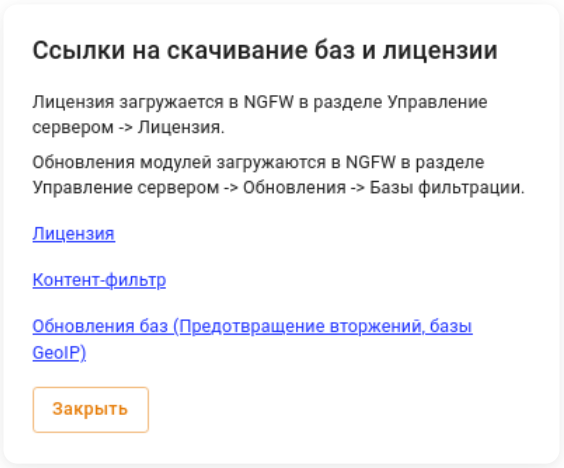
4. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

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:

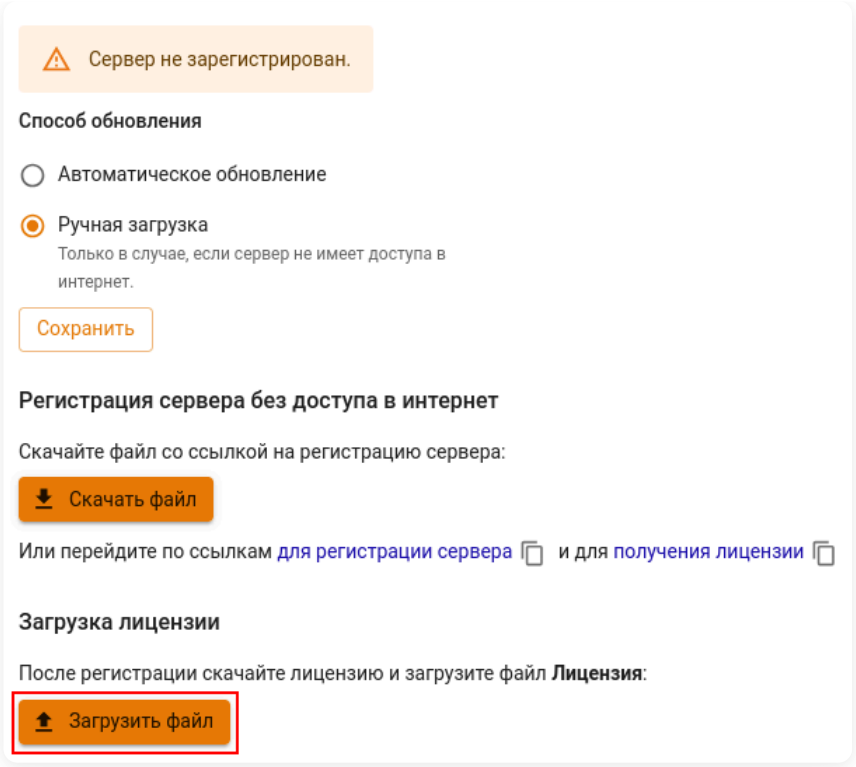


6. Перейдите по ссылке из пункта 2, чтобы скачать файлы баз фильтрации и лицензии. Выберите в новом окне необходимую базу для загрузки:



> 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** в веб-интерфейсе Ideco NGFW 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 личном кабинете MY.IDECO напротив нужного сервера;
- В веб-интерфейсе Ideco NGFW, в разделе **Управление сервером** → **Лицензия**.

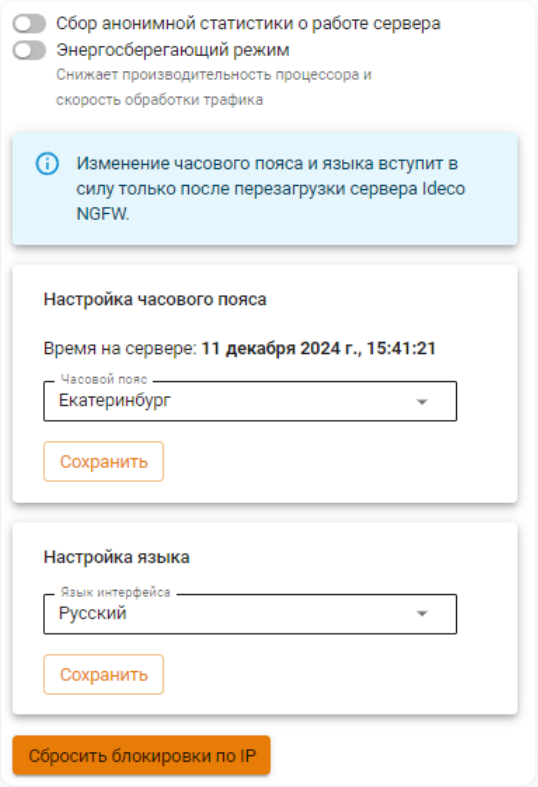
Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др.

Дополнительно

Изменение часового пояса вступит в силу только после перезагрузки сервера Ideco NGFW.

В интерфейсе VCE изменение настроек часового пояса и языка недоступно.

Настройка осуществляется через веб-интерфейс в разделе **Управление сервером** → **Дополнительно**.



- **Настройка часового пояса** - установите часовой пояс для корректного сбора логов и статистики.
- **Сбор анонимной статистики о работе сервера** - включение этого параметра разрешает серверу отправлять информацию об используемых модулях. При этом не отправляется информация о пользователях, проходящем через сервер трафике, сетевых интерфейсах и идентификаторах сервера и лицензии.
- **Энергосберегающий режим** - включение этого режима снижает производительность процессора и 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 по IP** - 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

Все возможности по фильтрации почтового трафика можно также применить к внутреннему почтовому серверу, опубликовав его 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, 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 даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

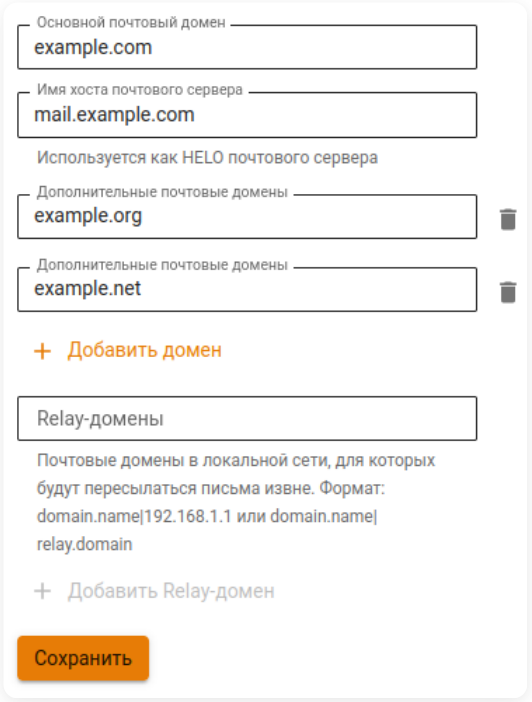
OK

Настройка почтового сервера

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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.

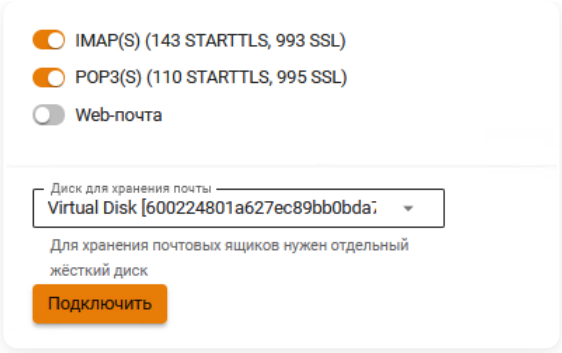
2. Включите почтовый сервер Ideco NGFW:



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, начиная с Ideco UTM версии 7.9.0. 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.

SSL-сертификат для почтового домена

После сохранения настроек почтового сервера Ideco NGFW 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 он 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 должен получить 10 баллов из 10.

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

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

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.

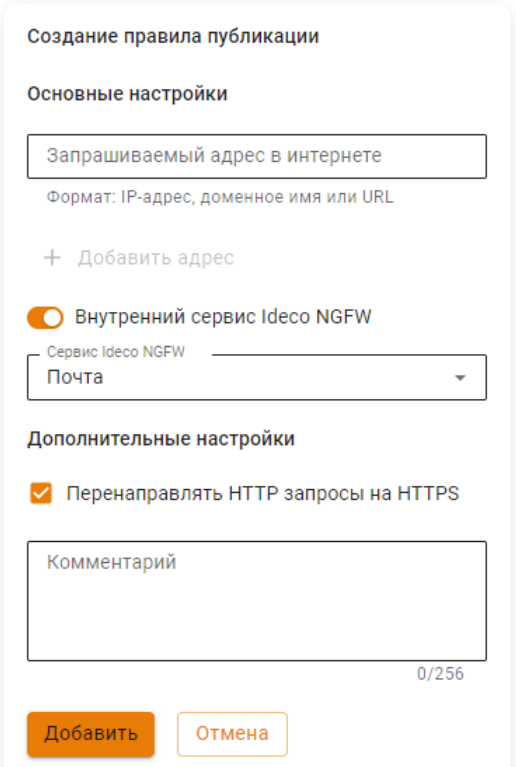
Перед настройкой веб-почты убедитесь, что на Ideco NGFW включен почтовый сервер:



Для работы веб-почты необходимо:

1. Активировать опцию **Web-почта** в **Почтовый релей** → **Основные настройки**.

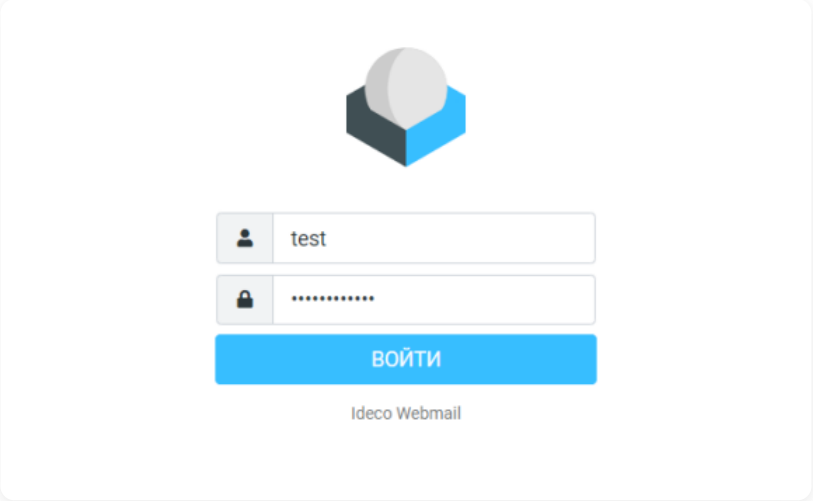
2. Создать и добавить правило публикации в **Сервисы** → **Обратный прокси**:



- 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**.
- В качестве сервиса выберите **Почта**.
- В блоке **Дополнительные настройки** включите опцию **Перенаправлять HTTP запросы на HTTPS**.

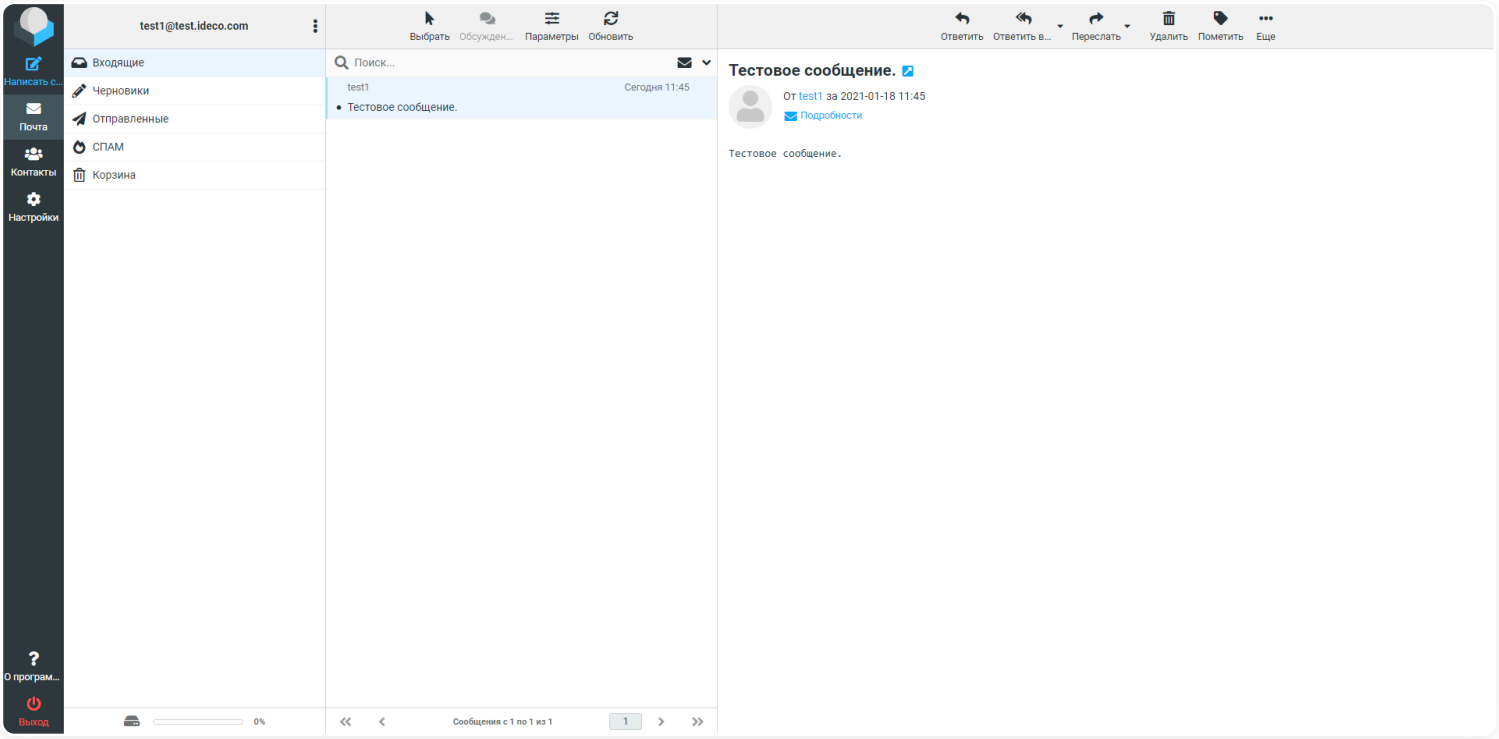
- Чтобы пользователи имели доступ к веб-почте из внешней сети, в правиле публикации в поле **Запрашиваемый адрес в интернете** укажите **белый IP-адрес или зарегистрированный домен**.
- Для подключения обязательно используйте HTTPS.
- С версии 17 Ideco NGFW веб-почта не доступна через `IP-адрес_или_домен_веб-интерфейса:8443/webmail`, 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

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Работа в режиме открытого почтового релея невозможна, поэтому Ideco NGFW 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 (A- и MX-записи в DNS-зоне).

NGFW не поддерживает кириллические почтовые домены.

Перед настройкой почтового релея убедитесь, что на Ideco NGFW включен почтовый сервер:

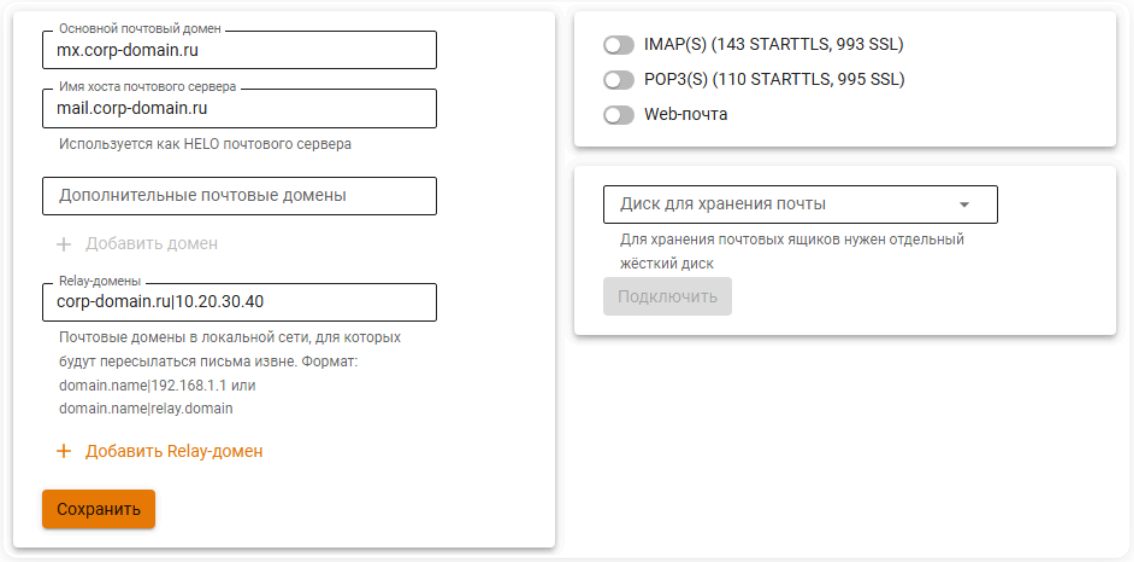


Настройка пересылки почты

Для пересылки почты с почтового сервера в локальной сети через Ideco NGFW 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 и имя хоста почтового сервера должны отличаться от Relay-доменов. Если Ideco NGFW 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`:

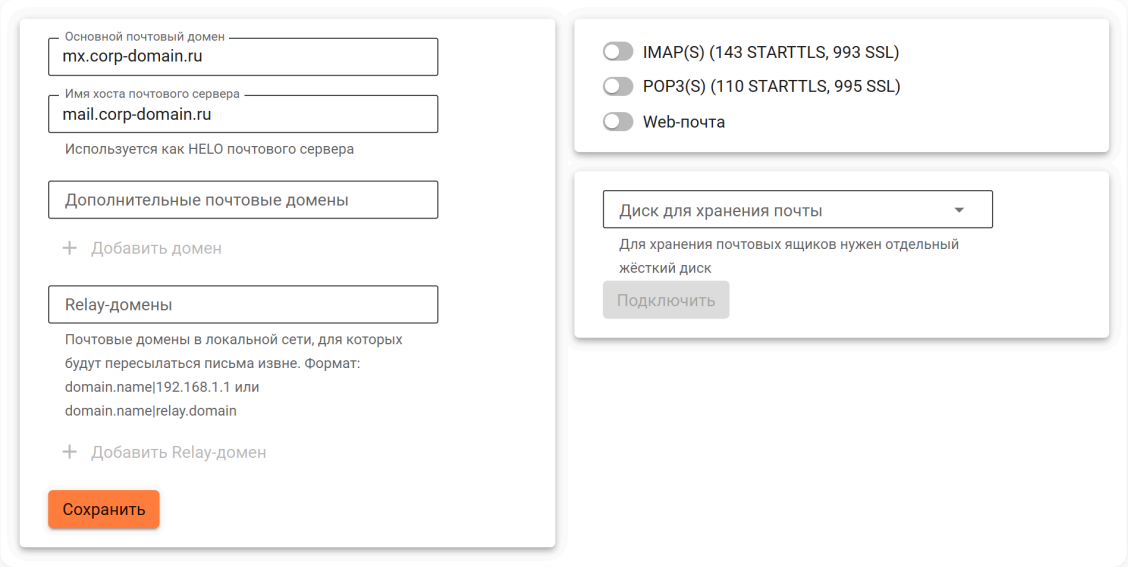
- `corp-domain.ru` - почтовый домен, зарегистрированный в интернете на публичный адрес Ideco NGFW.
- `10.20.30.40` - адрес почтового сервера в локальной сети.

3. Если требуется проверка почты на спам и вирусы, перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

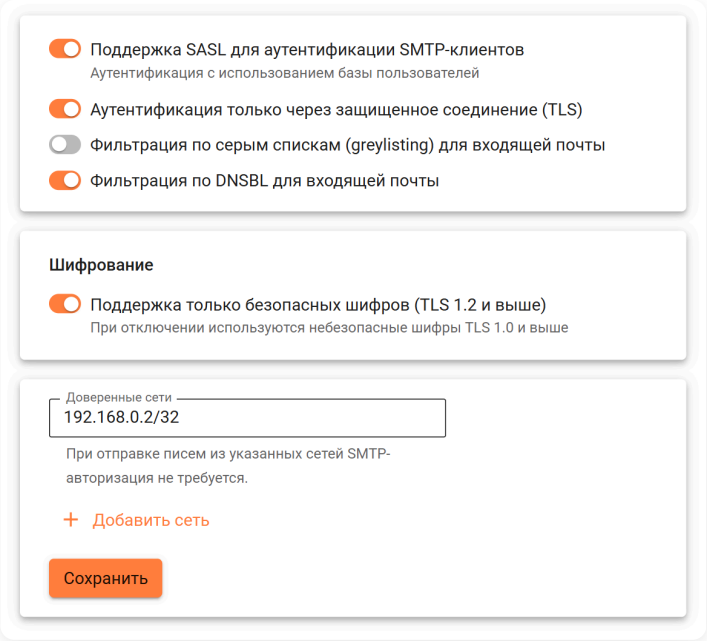
Исходящая

Для пересылки исходящей почты дополнительных настроек на стороне NGFW 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:



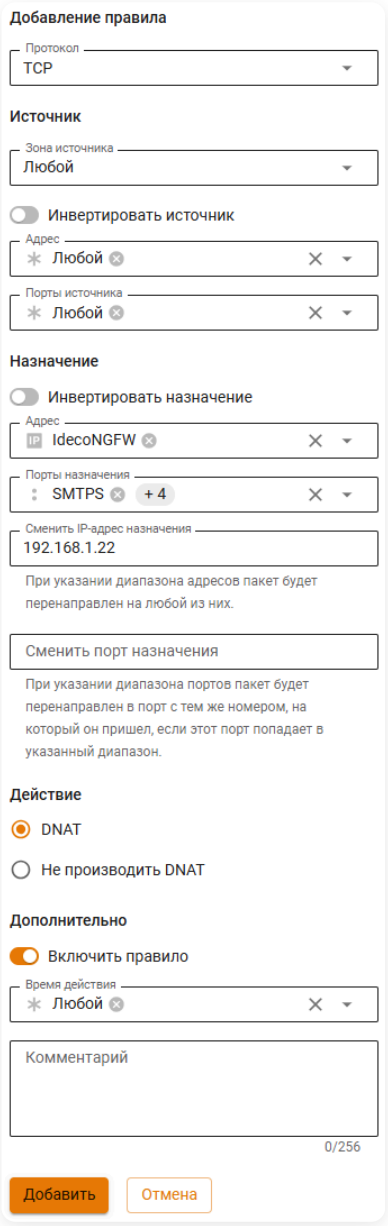
3. Перейдите в **Почтовый релей** → **Антиспам и антивирус**, включите опцию и загрузите ключ.

4. На почтовом сервере клиента в настройках отправки исходящей почты по протоколу SMTP укажите внешний IP-адрес Ideco NGFW.

Настройка доступа почтовых клиентов

Доступ из внешней сети

Для подключения почтовых клиентов из внешней сети, перейдите в **Правила трафика** → **Файрвол** → **DNAT**, создайте и включите правило проброса портов POP3(S), IMAP(S) и SMTPS:



Расшифровка полей

- **Протокол** - укажите TCP.
- **Назначение**:
  - **Адрес** - внешний IP-адрес Ideco NGFW.
  - **Порты назначения** - порты, которые использует ваш почтовый клиент (POP3, IMAP, SMTPS, 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.

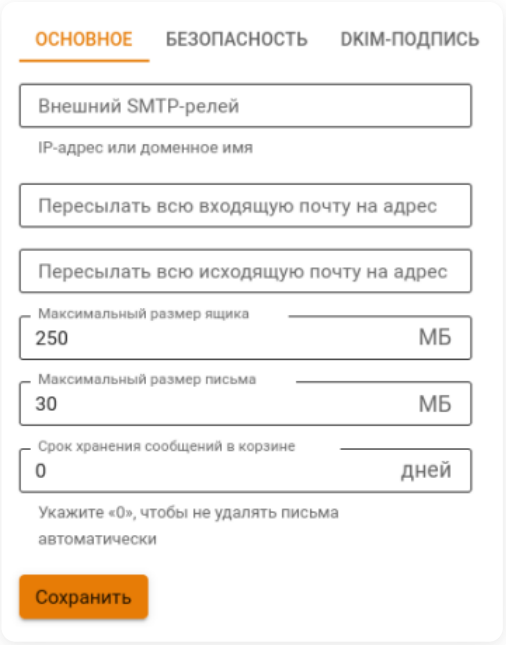
Доступ по VPN

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

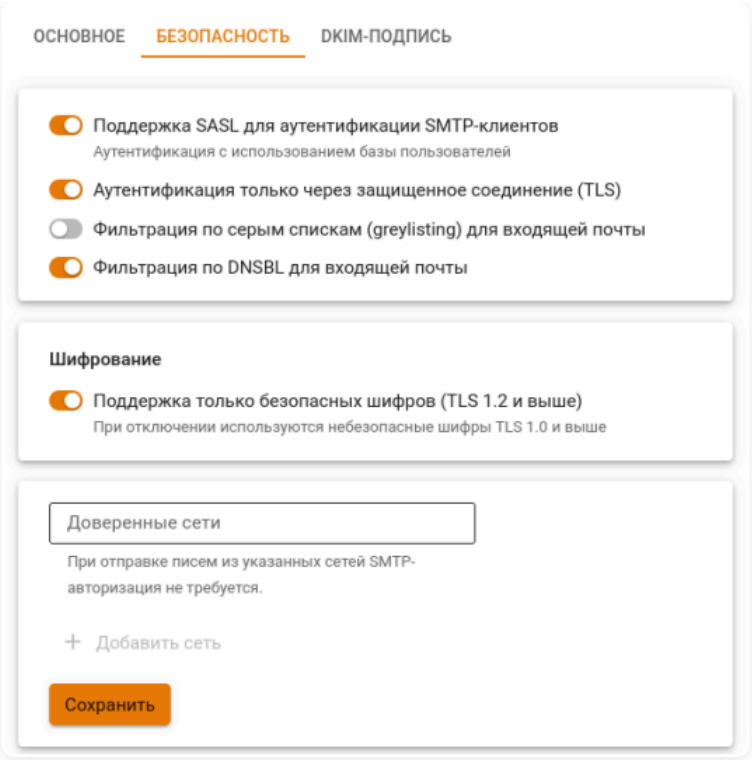
Раздел **Расширенные настройки** состоит из трех подразделов: **Основное, Безопасность, DKIM-подпись**.

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 мегабайтах (**100 ГБ - максимальное значение**).
- **Максимальный размер письма.** Ограничение на максимальный размер формируемого сервером письма в мегабайтах (**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

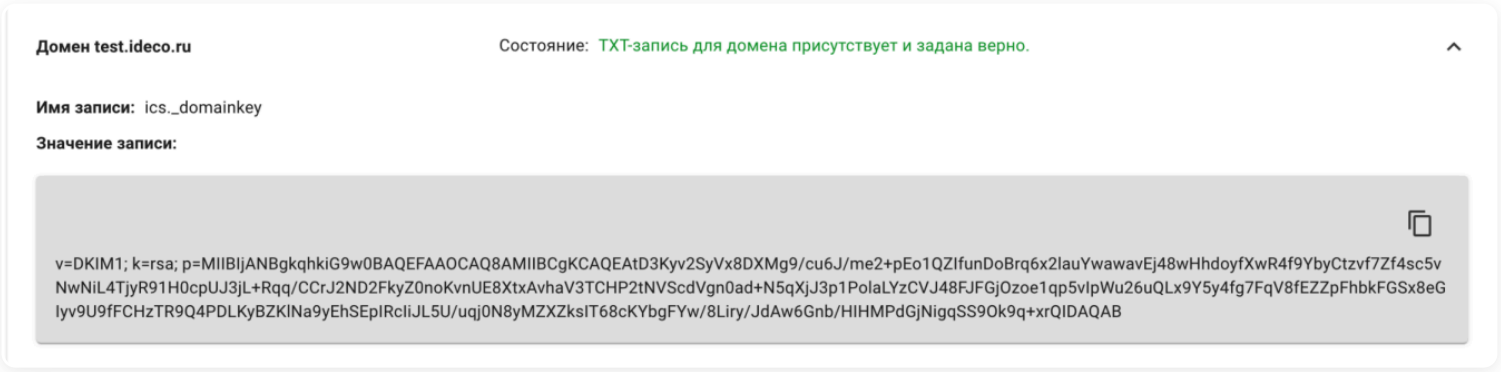


- **Поддержка SASL для аутентификации SMTP-клиентов.** Подключиться к почтовому ящику из интернета и отправить письмо, используя SMTP сервер Ideco, можно будет только, пройдя авторизацию по логину и паролю, заданному для этой учетной записи пользователя на сервере. **Не включайте этот параметр, если используете NGFW в качестве почтового релея**.
- **Разрешить аутентификацию только через защищенное соединение (TLS).** Запрещает незащищенную передачу учетных данных клиента при аутентификации на SMTP сервере.
- **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 разделе **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, и дополнительных почтовых доменов (если указаны). Сервер также проверит, правильно ли была указана запись и резолвится ли она 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 они 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 его 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. **Убедитесь, что на внешнем интерфейсе NGFW назначен публичный адрес, доступный из сети интернет.**

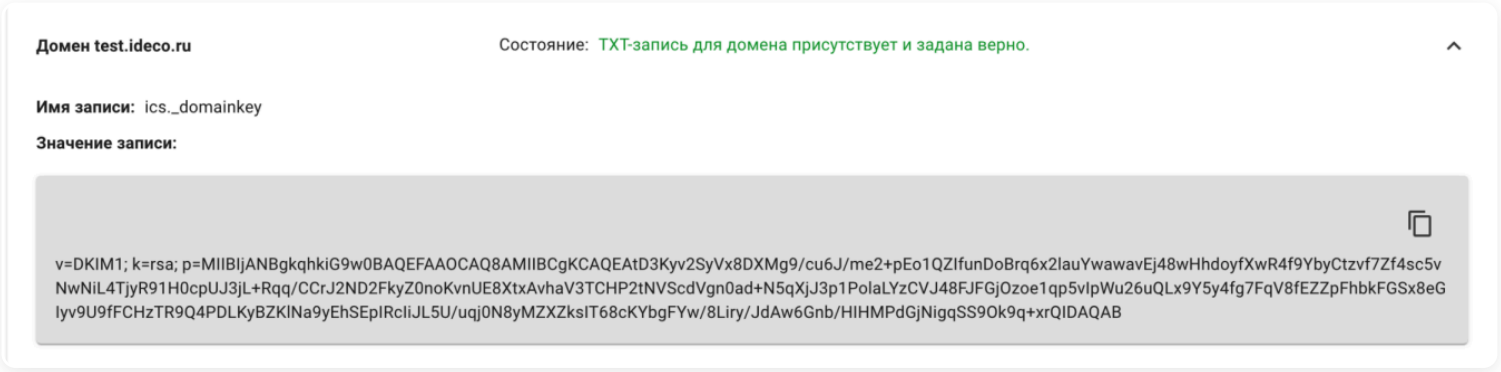
2. Добавьте ресурсную запись типа MX, указывающую на A-запись, которая была создана на предыдущем шаге. Запись типа MX указывает на сетевой узел, который занимается обработкой почтовых сообщений для домена. Она должна ссылаться на доменное имя почтового сервера, а не на IP-адрес.

Рекомендуем:

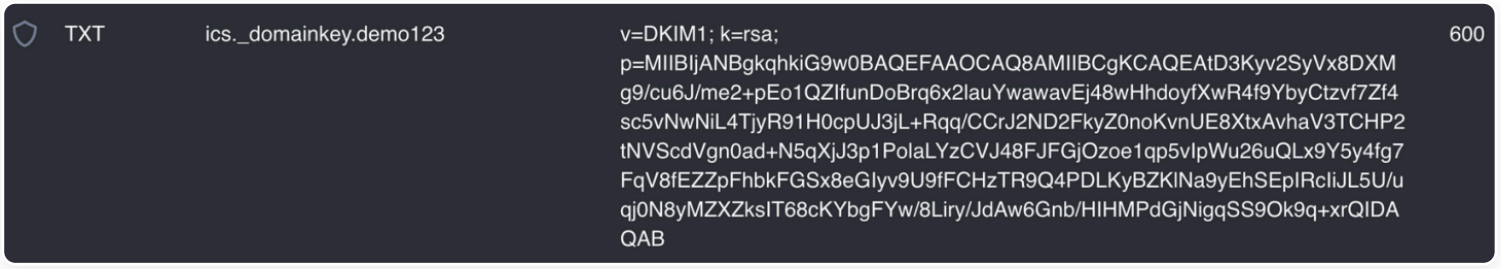
3. Добавить обратную ресурсную запись типа PTR. Эта запись должна быть прописана в файле обратной зоны. Эти изменения должны быть сделаны на стороне интернет-провайдера. Обратитесь к нему с просьбой прописать обратную ресурсную запись для IP-адреса, которая должна ссылаться на запись типа MX.

4. Настроить SPF-запись для почтового сервера.

5. После настройки почтового сервера настроить также DKIM-подпись почтовых сообщений. Для этого перейдите в раздел **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 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.
- MX-запись вида: `example.net. MX 10 mail.example.net`.
- Обратитесь на свой 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 в себя 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.

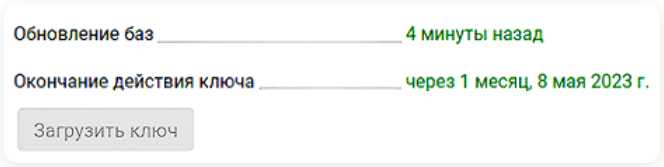
Антиспам и антивирус

Видеоинструкцию смотрите по ссылкам:

- Rutube
- Youtube
- docs.ideco.ru

Раздел **Антиспам и антивирус** состоит из вкладок: **Основное** и **Настройки фильтрации**.

Основное



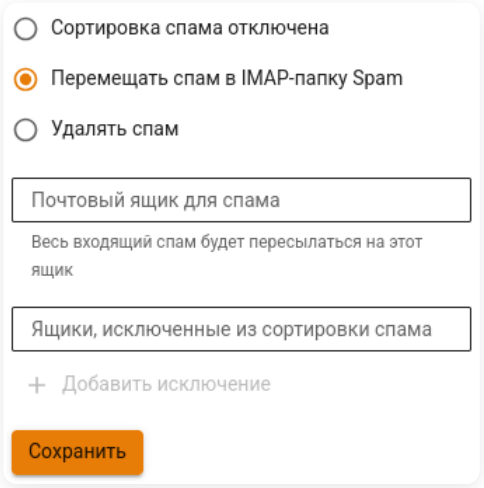
Позволяет управлять работой службы антиспама и антивируса почтового сервера на базе Kaspersky Security for Linux Mail Server с функцией машинного обучения и искусственного интеллекта. Также на вкладке предоставлена возможность добавления лицензионного ключа антиспама. Ключ поставляется в файле, имеющем 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 в **Правила** → **Разрешенные адреса**. Адреса, добавленные на вкладке **Запрещенные адреса**, обрабатываются только NGFW.

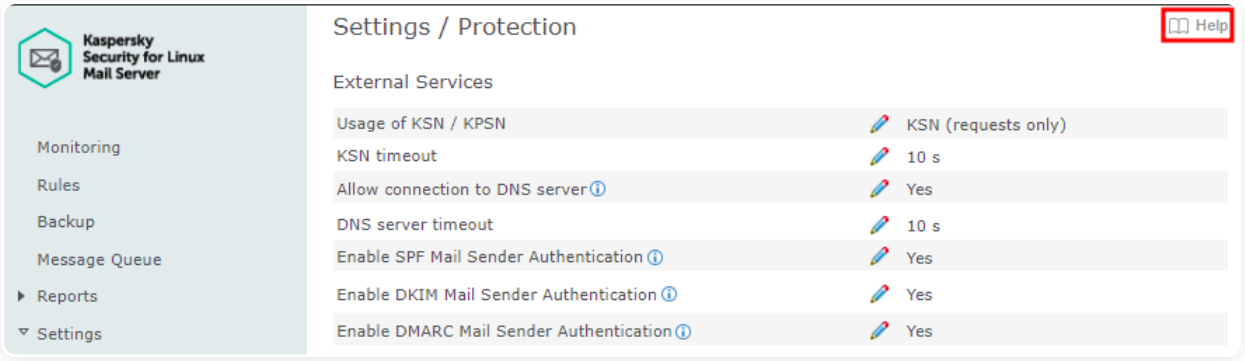
Веб-интерфейс для Антиспама

> 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**:



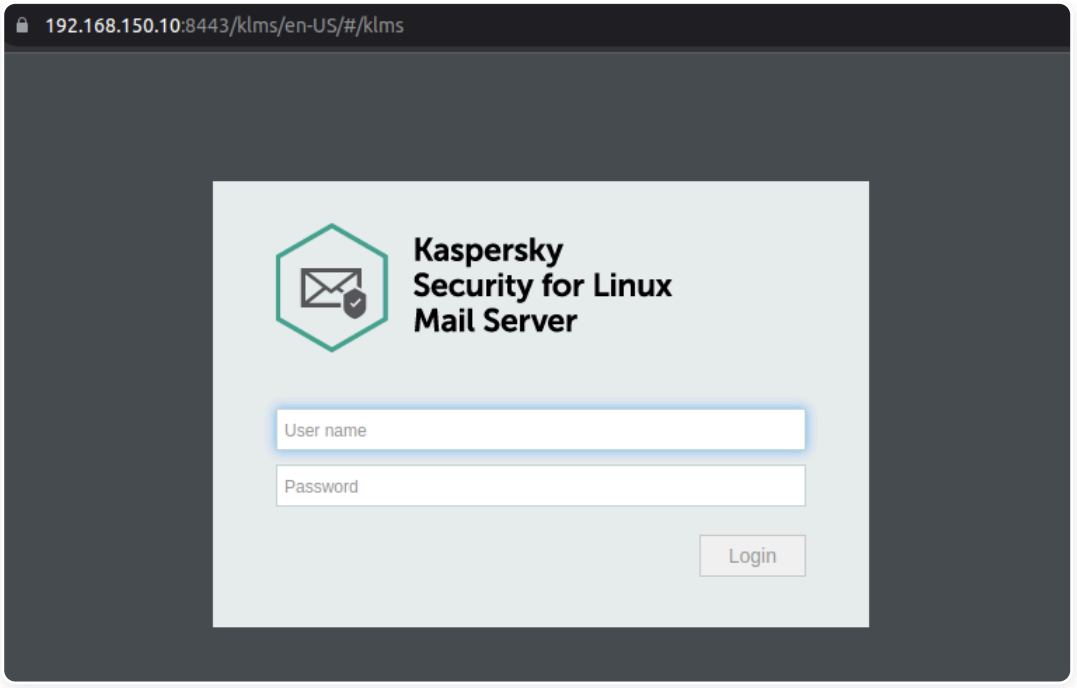
Чтобы включить веб-интерфейс для Антиспама:

1. Перейдите в раздел **Управление сервером** → **Терминал** и выполните команду `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`

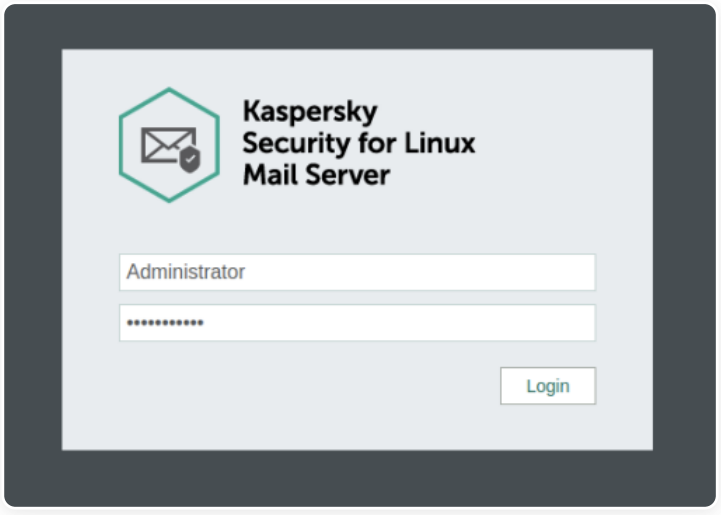
2. Задайте пароль для стандартного аккаунта **Administrator**, состоящий минимум из 8 символов: строчных букв, заглавных букв, специальных символов, чисел.

```
[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 ~]#
```

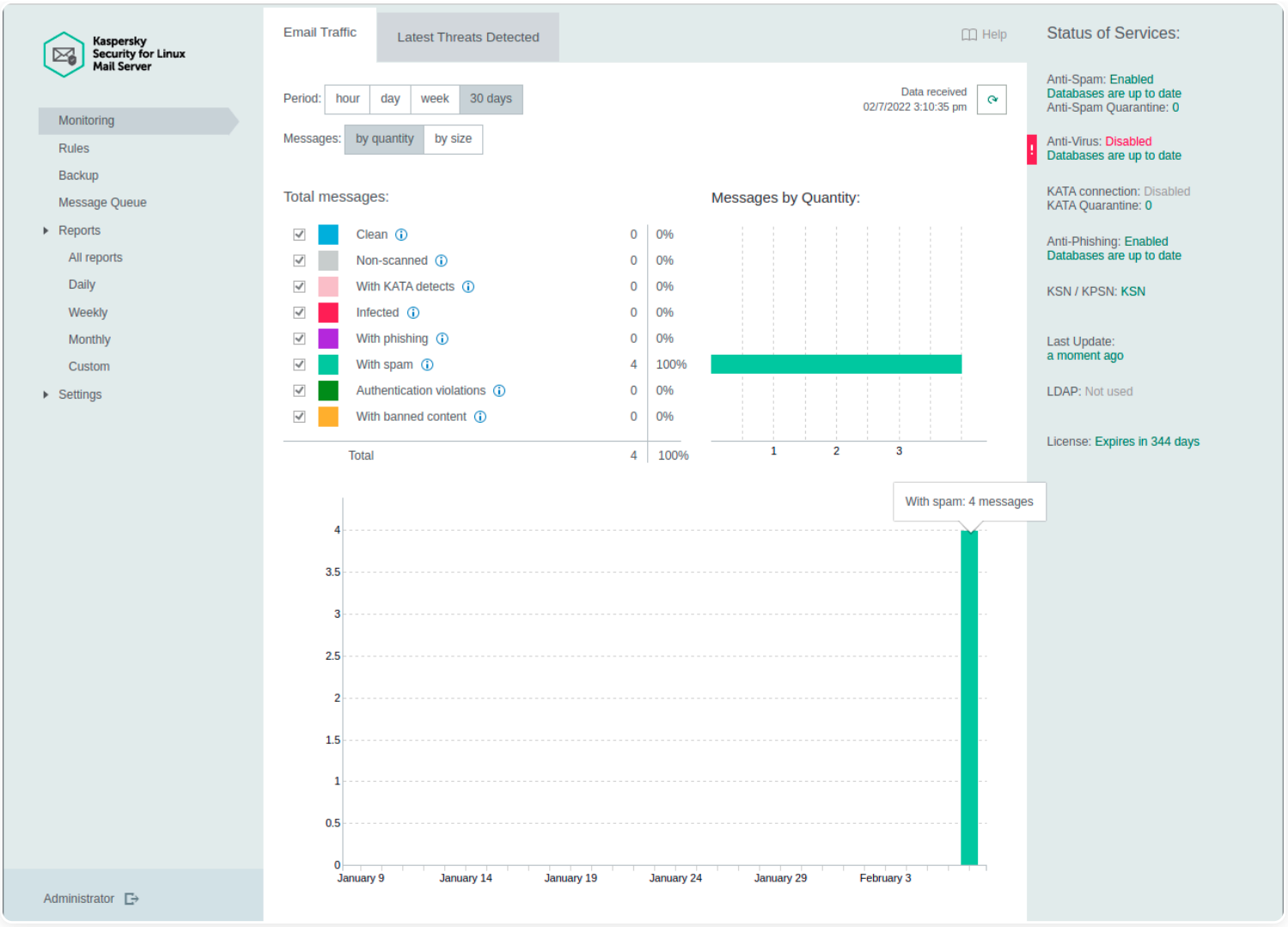
3. Перейдите в адресной строке по пути `ngfw_ip_address:8443/klms/` чтобы получить доступ к веб-интерфейсу:



4. Войдите в веб-интерфейс с учетной записью **Administrator** и ранее заданным в терминале паролем:



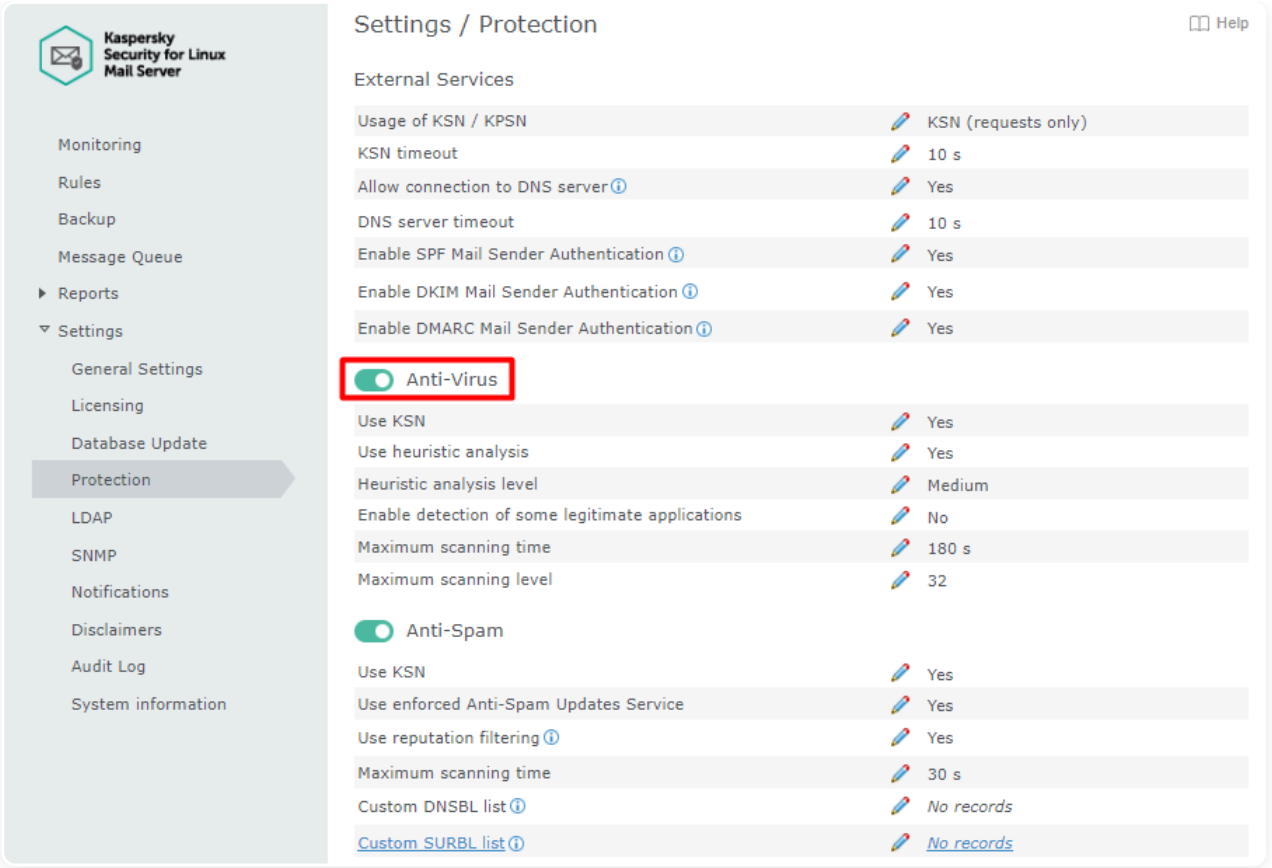
После успешного входа будет отображен дашборд со статистикой работы Антиспама:



Включение Антивируса почтового сервера

1. Перейдите в веб-интерфейс Антиспама.

2. Включите антивирус почтового сервера, перейдите в раздел **Settings** → **Protection** и активируйте опцию **Anti-Virus**:



Службы антиспама и антивируса почтового сервера преднастроены для оптимальной работы в составе Ideco NGFW. Не рекомендуем вносить какие-либо изменения в раздел **Settings**. Веб-интерфейс решения Kaspersky Security for Linux Mail Server предусмотрен только для работы с отчётностью и для внесения изменений, описанных в этой статье.

Правила

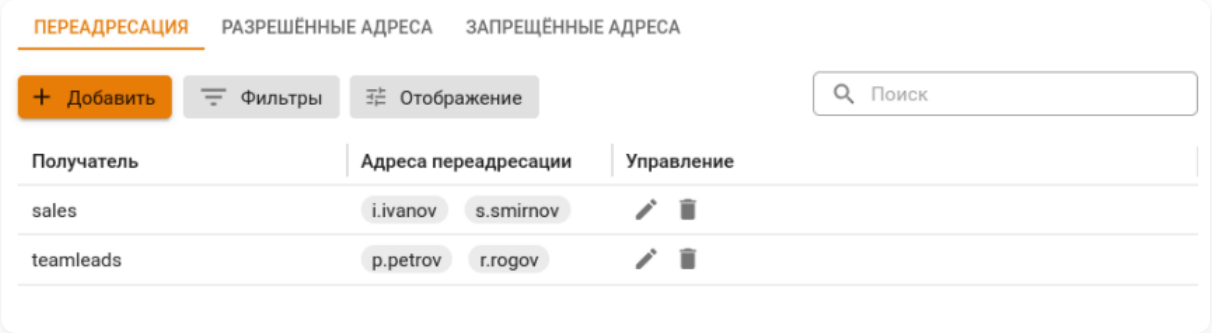
Раздел **Правила** состоит из трех вкладок: **Переадресация, Разрешенные адреса, Запрещенные адреса**. На каждой вкладке доступна фильтрация по кнопке **Фильтры**.

Переадресация

Позволяет настроить переадресацию почты на сервере с помощью почтовых алиасов.

Алиасы, в отличие от почтовых ящиков, не требуют логинов и паролей, они закрепляются за ящиком и служат его копией 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.

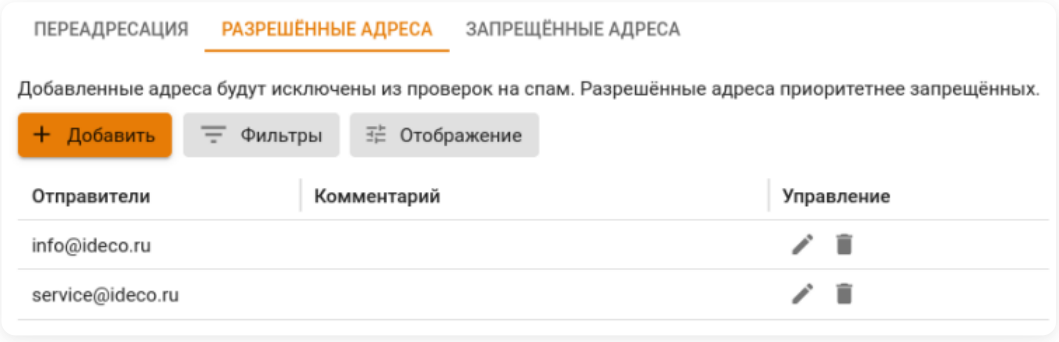
Подробнее с документацией по настройке почтовых алиасов на Ideco NGFW ознакомьтесь в статье Переадресация почты.



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 он 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.

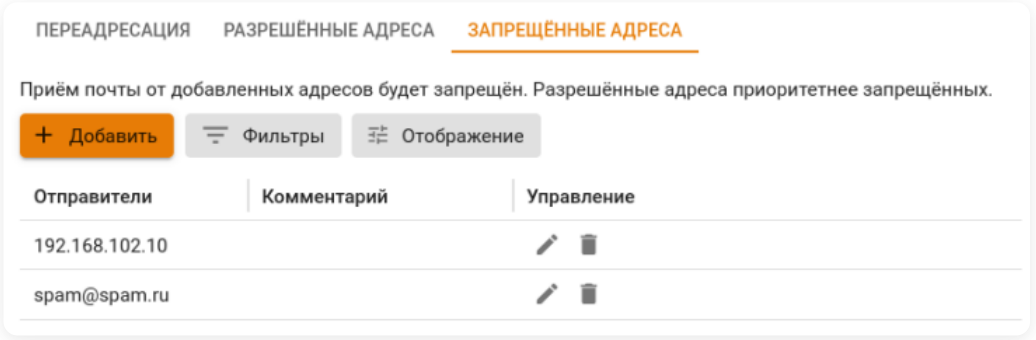
Еще один пример: в **Разрешенные адреса** внесен домен, в **Запрещенные адреса** - ящик из этого домена. Тогда письма с ящика будут заблокированы.

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.



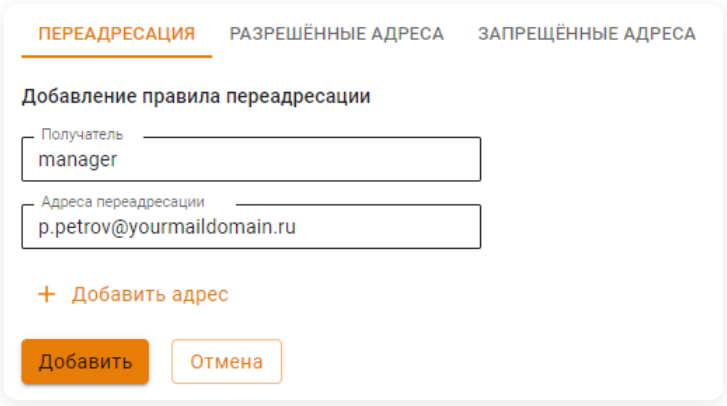
Переадресация почты

Чтобы создавать и редактировать почтовые правила переадресации (алиасы), перейдите в раздел **Почтовый релей** → **Правила** → **Переадресация**.

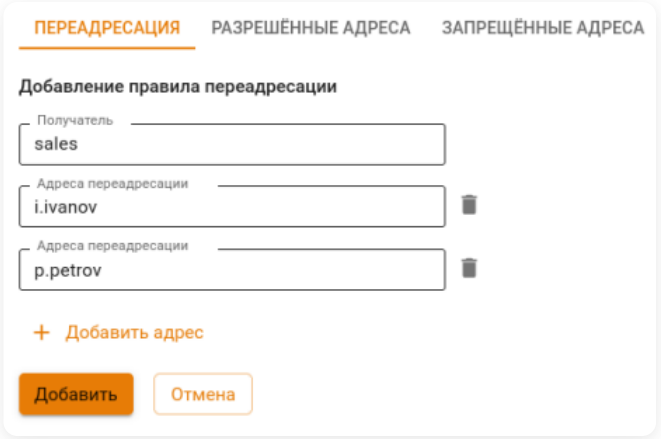
Почтовые алиасы отличаются от почтовых ящиков тем, что не требуют логинов и паролей. Они закрепляются за ящиком и служат его копией с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, можно сказать что алиас - это группа почтовых ящиков или группа рассылки. Поступающая на алиас 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. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в поле **Получатель**, должен реально существовать.

Примеры:

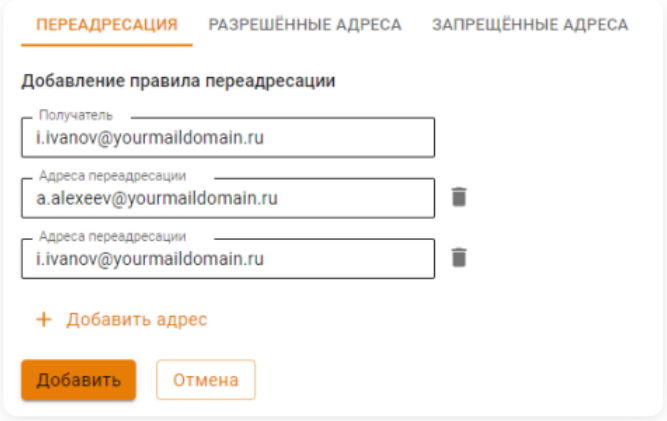
- Создать алиас `manager@yourdomain.ru` для ящика менеджера компании для связи с клиентами и партнерами, у которого реальный почтовый ящик имеет имя `p.petrov@yourmaildomain.ru`:



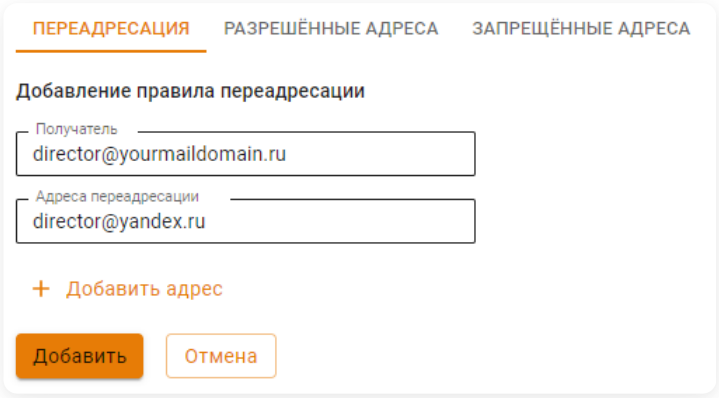
- Создать корпоративный алиас для отдела продаж `sales@yourmaildomail.ru`, чтобы почта пересылалась на всех сотрудников этого отдела:



- Создать временный алиас для переадресации почты сотрудника, который находится в отпуске `i.ivanov@yourmaildomail.ru`, на ящик его 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.

Почтовая очередь

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 оно будет удалено из почтовой очереди и не будет доставлено получателю.

При обновлении Ideco NGFW 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 должен получить 10 баллов из 10.

Публикация ресурсов

Доступ из внешних сетей без NAT

Перейти >

Настройка публичного IP-адреса на компьютере в локальной сети

Перейти >

Портмаппинг (проброс портов, DNAT)

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

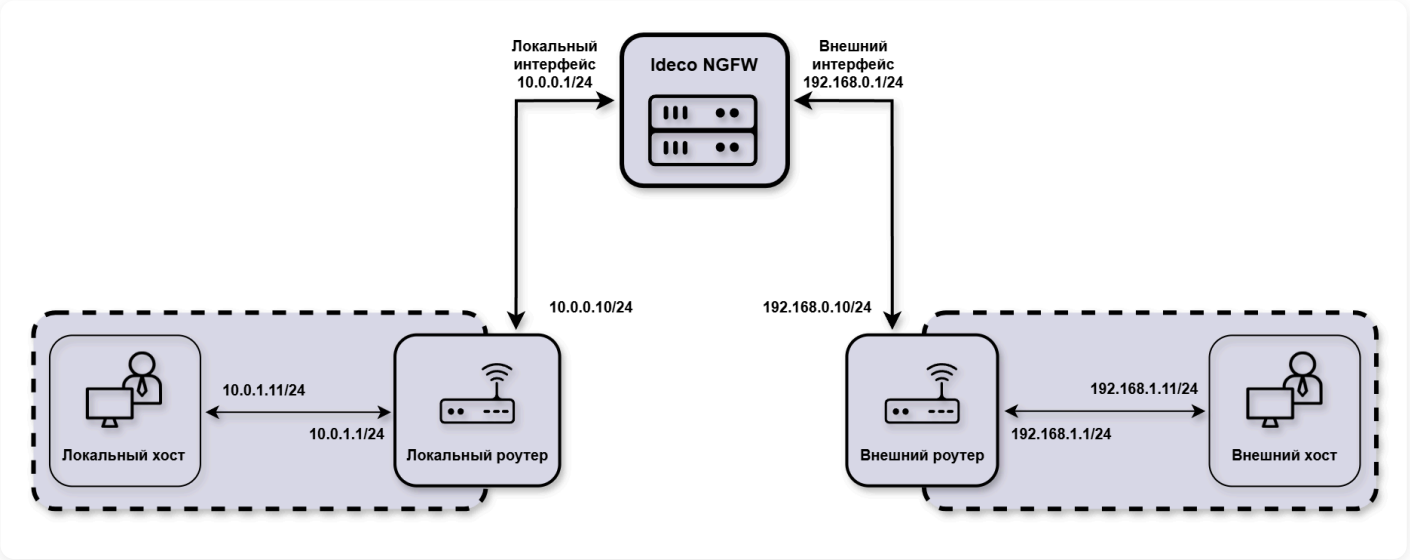
OK

Доступ из внешних сетей без NAT

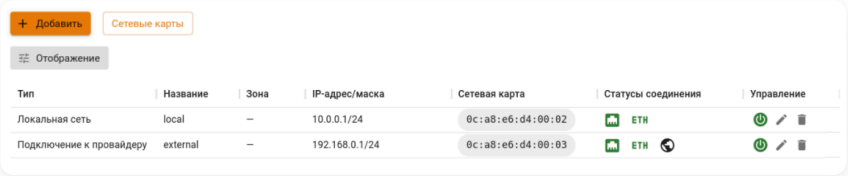
При необходимости (как правило, когда Ideco NGFW расположен внутри локальной сети, а не на границе с интернетом) возможно:

- Организовать прямой доступ к ресурсам внешних по отношению к Ideco NGFW сетей без использования NAT.
- Разрешить доступ из внешних относительно Ideco NGFW сетей в локальную сеть с прямым обращением к локальным IP-адресам.

Для примера разберем настройку Ideco NGFW для доступа без NAT в следующей конфигурации сети:



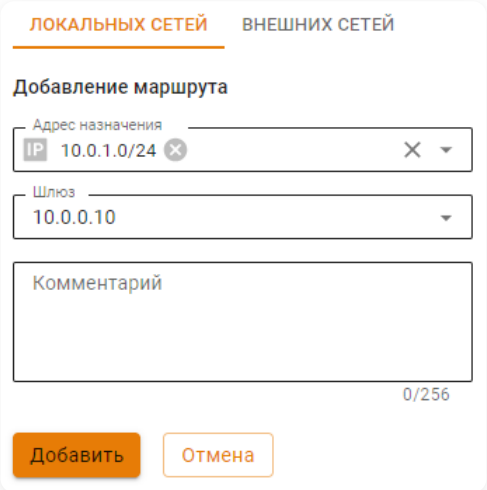
1. Настройте сетевые интерфейсы в разделе **Сервисы** → **Сетевые интерфейсы** на Ideco NGFW:



- **local** - интерфейс для доступа в пользовательскую локальную сеть.
- **external** - интерфейс для доступа в пользовательскую внешнюю сеть пользователей.

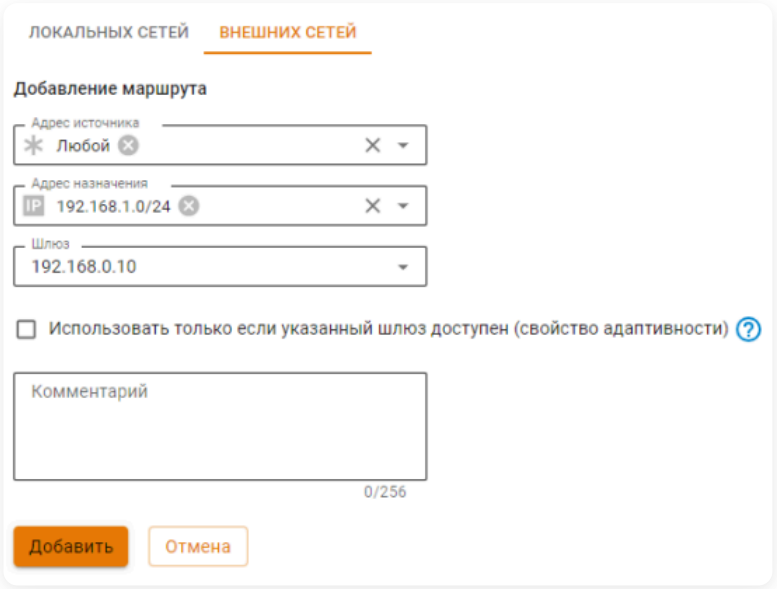
2. Перейдите в раздел **Сервисы** → **Маршрутизация** и создайте правила для доступа к IP-адресам пользователей, которые находятся за маршрутизаторами:

- Для **Локальных сетей**:



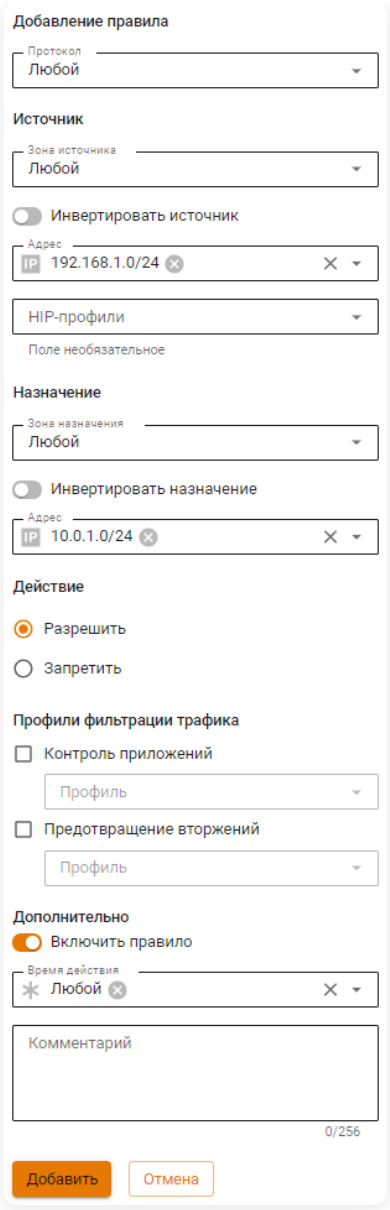
- **Адрес назначения** - адрес локальной сети за маршрутизатором (`10.0.1.0/24`).
- **Шлюз** - адрес машрутизатора (`10.0.0.10`).

- Для **Внешних сетей**:



- **Источник** - Любой.
- **Адрес назначения** - адрес внешней сети за маршрутизатором (`192.168.1.0/24`).
- **Шлюз** - адрес машрутизатора (`192.168.0.10`).

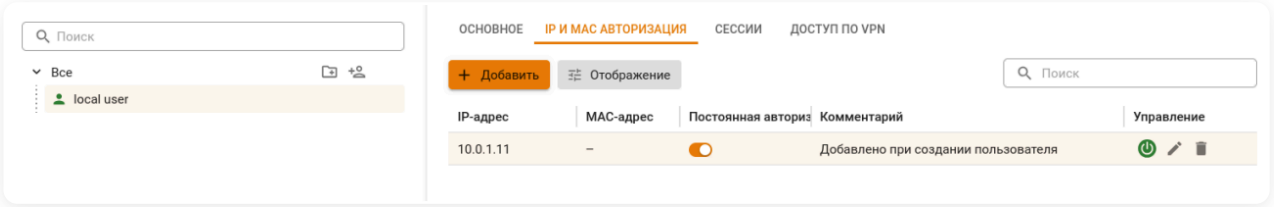
3. Перейдите в раздел **Правила трафика** → **Файрвол** → **FORWARD**, создайте и включите правило для доступа хостов из внешней сети `192.168.1.0/24` до IP-адресов пользователей локальной сети `10.0.1.0/24`:



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 раздел **Правила трафика** → **Файрвол** → **SNAT** и отключите опцию **Автоматический SNAT локальных сетей**.

5. Перейдите в раздел **Пользователи** → **Учетные записи** и включите опцию **Постоянная авторизация** для пользователей локальной сети `10.0.1.0/24`. 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.

Правила трафика Ideco NGFW будут работать только для трафика, приходящего из внешней сети в локальную сеть.

Настройка публичного IP-адреса 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 их диапазон от 0 до 65535 для получения эффекта присутствия локального сервера на внешнем IP-адресе.

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 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 добавьте правило в разделе **Правила трафика** → **Файрвол** → **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 их публикации воспользуйтесь обратным прокси-сервером.

Особенности создания правил DNAT в версии 18

- В предыдущих версиях профили безопасности настраивались в отдельных разделах. В версии 18 **Контроль приложений** настраиваются в правилах **Файрвола**.
- 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**.

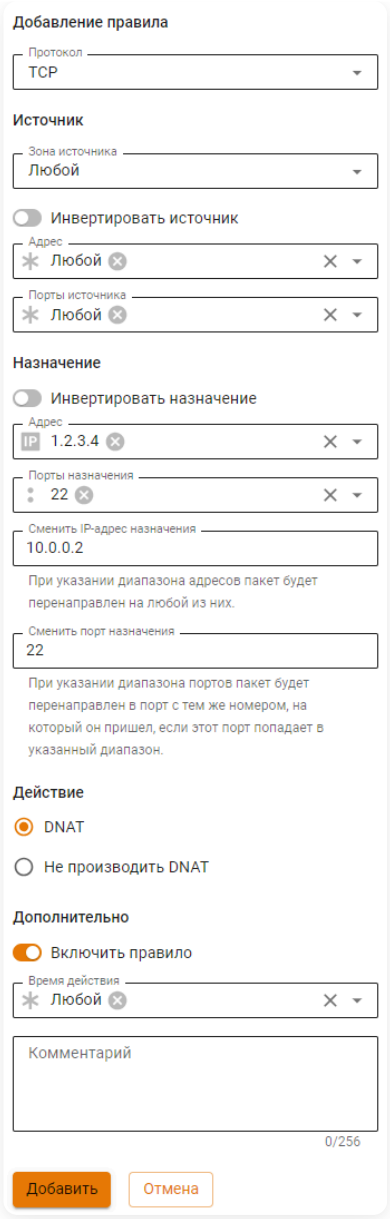
Создание правил DNAT и FORWARD в Файрволе Ideco NGFW

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 на устройство в локальной сети перейдите в раздел **Правила трафика** → **Файрвол** → **DNAT** и нажмите **Добавить**.

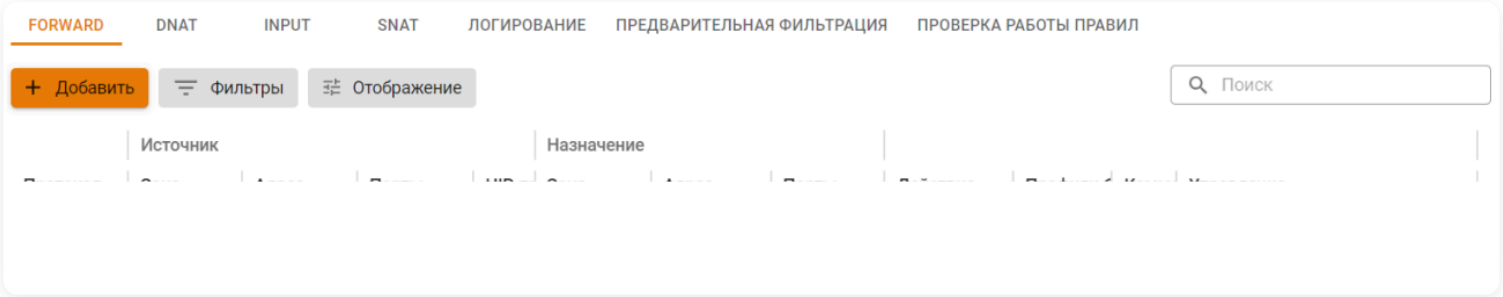
Заполните поля в соответствии с характеристиками, указанными в примере:



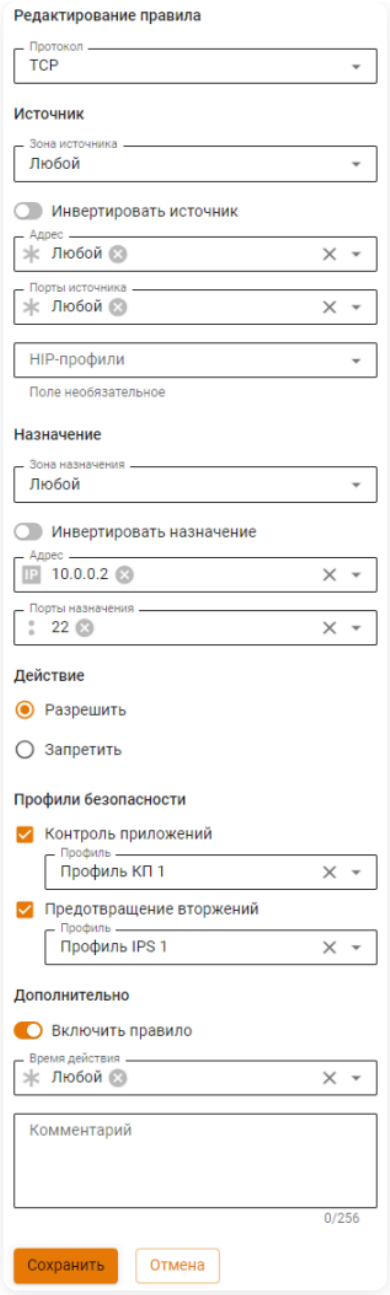
Вид правила в таблице после сохранения:

Проверьте наличие запрещающих правил в таблице FORWARD. При необходимости создайте правило, разрешающее трафик:

Поместите созданное правило выше запрещающего трафик:



Если вы хотите, чтобы трафик проверялся профилями безопасности, включите в созданном правиле соответствующие настройки:



Настройки **Файрвола** применяются сразу при создании правил.

Частые ошибки

- Если включен режим **Разрешить интернет всем**, правила **Файрвола**, 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.
- Если в одной локальной сети находятся пользователи и сервер с опубликованным при помощи DNAT-правила ресурсом, вероятна асимметричная маршрутизация. Информация о способах устранения асимметричной маршрутизации трафика представлена в статье.

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, 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 его IP-адресу в локальной сети. Альтернативный вариант - вынесите ресурс в отдельную локальную сеть, DMZ и обращайтесь к ресурсу из локальной сети клиентов по внешнему IP-адресу.

Интеграция NGFW и SkyDNS

Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

Чем может быть полезна интеграция:

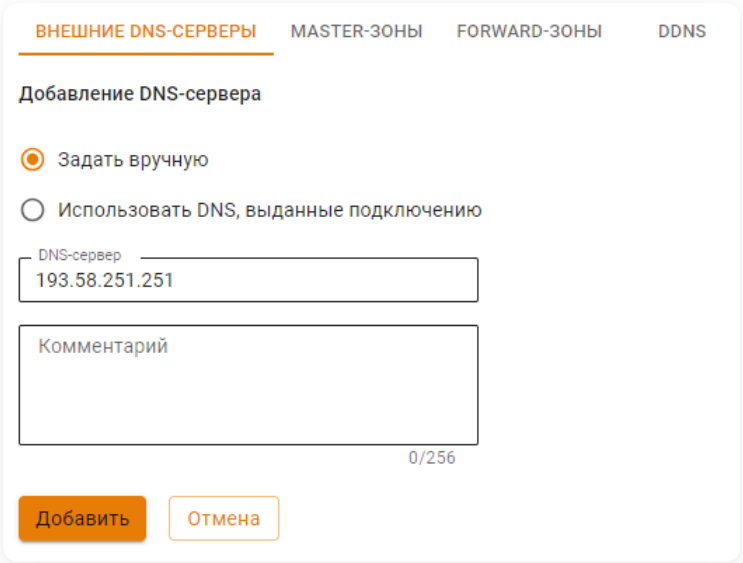
- **Защита от зараженных сайтов**. Вредоносные скрипты могут содержать сайты, как взломанные злоумышленниками, так и созданные специально для распространения вредоносного ПО.
- **Защита от бот-сетей**. Созданные из зараженных вредоносными программами компьютеров сети используются в DDoS-атаках на серверы, 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 он 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 и SkyDNS

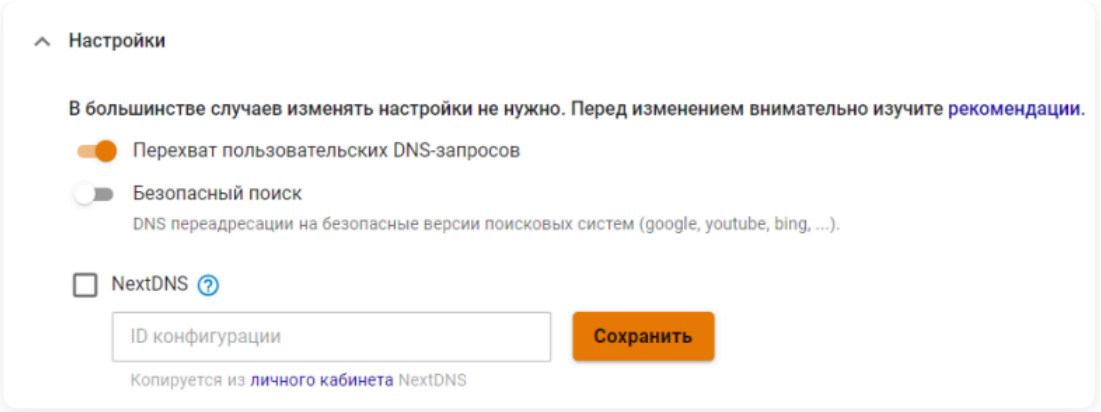
Чтобы настроить интеграцию со SkyDNS, выполните действия:

1. Перейдите в раздел **Сервисы** → **Защита и управление 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**:

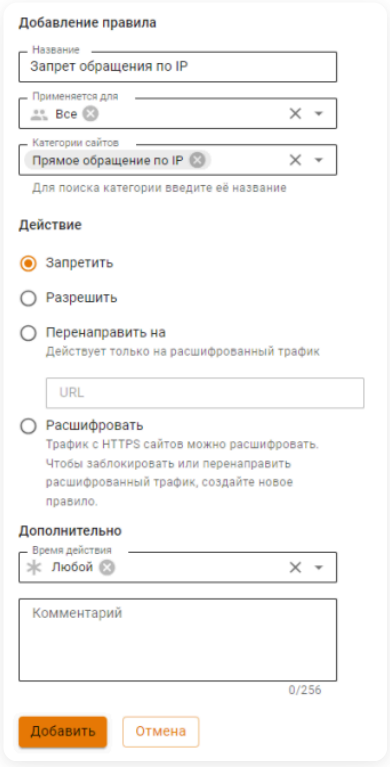


3. В настройках DNS включите опцию **Перехват пользовательских DNS-запросов** для запрета обращения к другим DNS-серверам (если фильтрация через SkyDNS обязательна для всей сети):



4. Если внутри локальной сети или внутри сети провайдера есть внутренняя DNS-зона, не обслуживаемая внешними DNS-серверами (например, домен Active Directory), укажите ее в разделе **Защита и управление DNS** → **FORWARD-ЗОНЫ**.

5. Перейдите в раздел **Правила трафика** → **Контент-фильтр** и создайте правило запрета прямого обращения к сайтам по IP-адресу:



6. Пропишите IP-адрес локального интерфейса Ideco NGFW в качестве единственного DNS-сервера в сетевых настройках на всех устройствах, которые требуется защитить.

Пользователи, получающие адреса автоматически через DHCP-сервер Ideco NGFW 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 статического белого IP-адреса привяжите этот 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

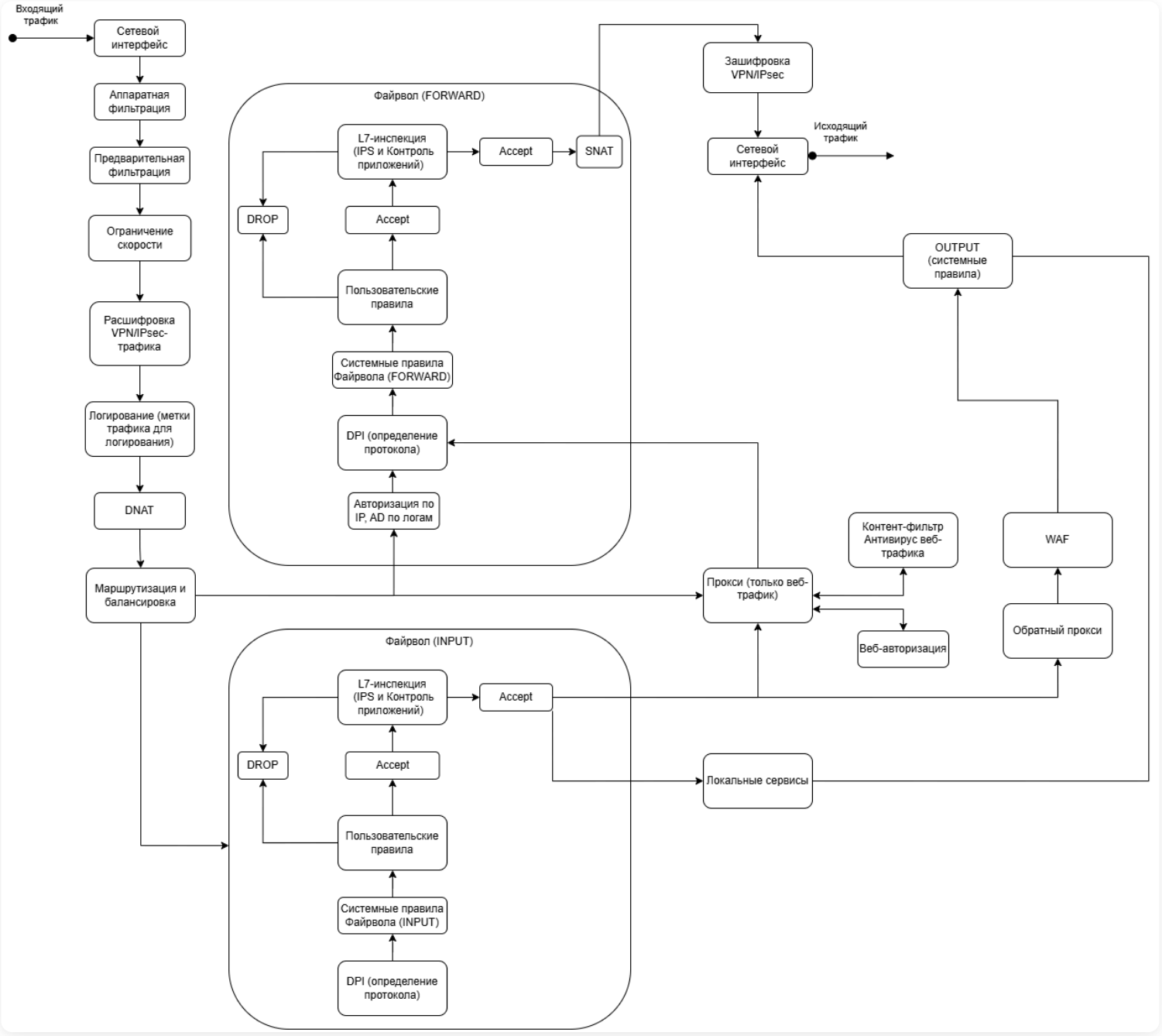


Полный цикл обработки трафика в Ideco NGFW

Статья описывает цикл, который проходят пакеты трафика в Ideco NGFW, в зависимости от сценария.

Обработку трафика условно можно разделить на три стадии:

- Предварительная;
- Файрвол;
- Завершающая.



К **Предварительной стадии** можно отнести Аппаратную, он проходит маршрутизацию и балансировку.

На второй стадии трафик проходит либо таблицу **INPUT**, либо таблицу **FORWARD** **Файрвола**:

- В первом случае - одно из двух:
  - Трафик проходит таблицу **INPUT** (системные и пользовательские правила, L7-фильтрацию) и направляется в локальные сервисы NGFW (например, DNS, NTP);

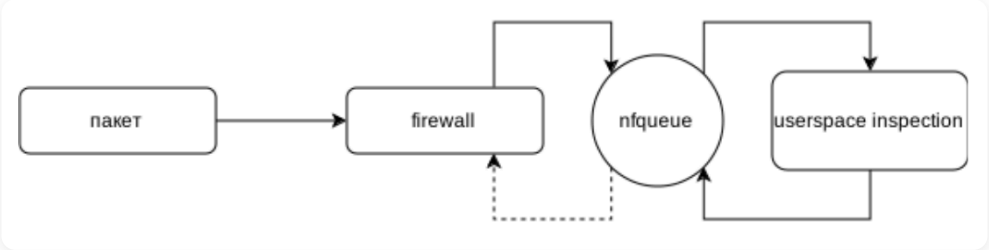
    - Трафик направляется в **Прокси** или **Обратный прокси**, обрабатывается соответствующими модулями и направляется в таблицу **FORWARD** (от **Прокси**) или в **OUTPUT** (от **Обратного прокси**).
- Во втором случае трафик проходит таблицу **FORWARD** (системные и пользовательские правила, L7-фильтрацию).

На **Завершающей стадии** трафик после обработки зашифровывается (при необходимости) и направляется получателю.

Принцип работы L7-инспекций

Трафик на обработку Предотвращением вторжений из Файрвола передается через NFQUEUE.

NFQUEUE - это технология интеграции файрвола linux с userspace-процессами, выполняющими инспекцию. Она позволяет выполнять L7-инспекции после L3-правил **Файрвола**:



Примеры прохождения трафика

Транзит трафика с фильтрацией и прозрачным прокси

1. Трафик пользователя попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию, Ограничение скорости (если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет).

2. Если пользователь подключился через VPN, трафик будет расшифрован.

3. Будет проверена DNAT-таблица **Файрвола**: 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 **Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, 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, 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 **Файрвола**: 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 она настроена).

4. Трафик направляется в **FORWARD**-таблицу **Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, Контроль приложений).

5. Запрос направляется ресурсу, на который обратился пользователь, ответ направляется пользователю (трафик вновь проходит п. 1 - п. 4).

Публикация ресурсов через обратный прокси

1. Трафик из внешней сети попадает на Ideco NGFW, 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 **Файрвола**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, 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.

Разрешить интернет всем

1. Трафик пользователя попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию, Ограничение скорости. Если трафик подпадает под правила - он может быть заблокирован и дальше не пойдет.

2. Пользователи могут подключаться через VPN, включая шифрованные подключения.

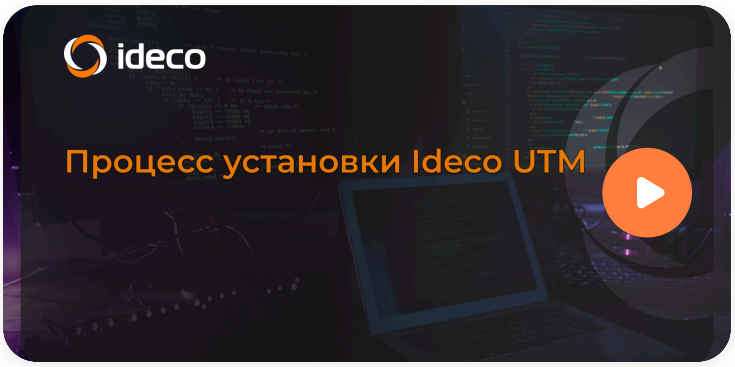
3. DNAT-таблица **Файрвола** не проверяется: даже если трафик подпадет под правила - IP-адрес или порт назначения не изменится.

4. Трафик, минуя стадию авторизации, пройдет таблицу **FORWARD** и не будет отброшен вне зависимости от созданных там правил фильтрации.

В статье представлен полный перечень видеоинструкций по продуктам Ideco

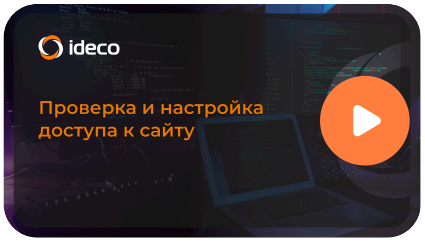
Ссылки на другие ресурсы

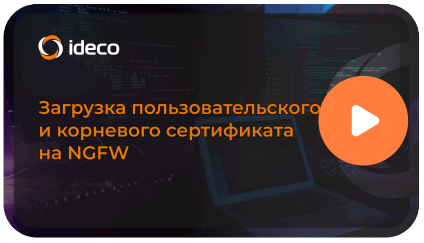
YouTube RUTUBE VK Видео



Последние видео







Видеоинструкции NGFW

Список видеоинструкции разбитые по разделам

Пользователи | Правила трафика | Профили безопасности | Сервисы | Управление сервером | Почтовый релей

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

FAQ

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 ?

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 и брокера сетевых пакетов DS Integrity NG - по ссылке.

Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW?

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 он 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 сети за роутером, находящимся после NGFW, не доступны по VPN?

Для решения вопроса воспользуйтесь статьей Доступ в удаленные сети через роутер в локальной сети.

Что делать, если ваш IP попал в черные списки DNSBL?

Если вы 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 его восстановить?

При утере пароля администратора можно его восстановить, имея физический доступ к серверу. Подробнее о процессе восстановления в статье Как восстановить доступ к Ideco NGFW.

После обновления потребовалось вернуть предыдущую версию со всеми настройками. Как это сделать?

Возможность восстановиться на предыдущую версию после обновления Ideco NGFW доступна с 12.X версий. Подробнее о процессе восстановления в статье Как восстановиться на прошлую версию после обновления Ideco NGFW.

Как подобрать аппаратную платформу для Ideco NGFW?

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 40 и содержит ядро Linux с набором драйверов от этой ОС с небольшими изменениями с нашей стороны. Таким образом, Ideco NGFW можно установить на большую часть оборудования, поддерживающего Fedora 40. Подробнее в статье Выбор аппаратной платформы для Ideco NGFW.

Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW?

Для настройки Ideco NGFW 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 до первоначальных настроек?

Для возврата к первоначальным настройкам используйте бэкап, созданный после установки Ideco NGFW. Если бэкапа нет - переустановите Ideco NGFW.

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 >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Инструкция по созданию VPN-подключения в Alt Linux

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 раздел **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

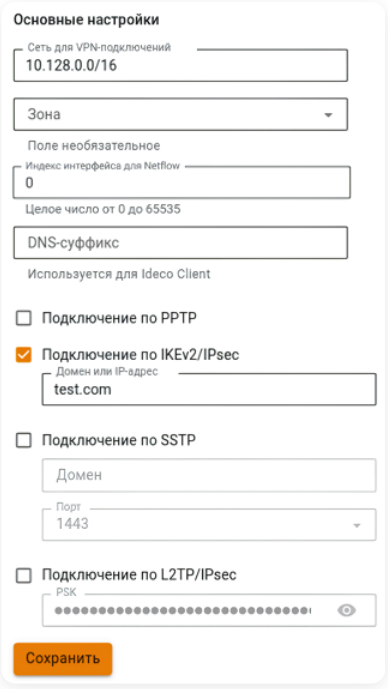
Не рекомендуем использовать для VPN-подключений кириллические логины.

Протокол IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите опцию **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

Создание подключения Alt Linux:

1. Откройте терминал сочетанием клавиш Ctrl+Alt+T и установите необходимые пакеты:

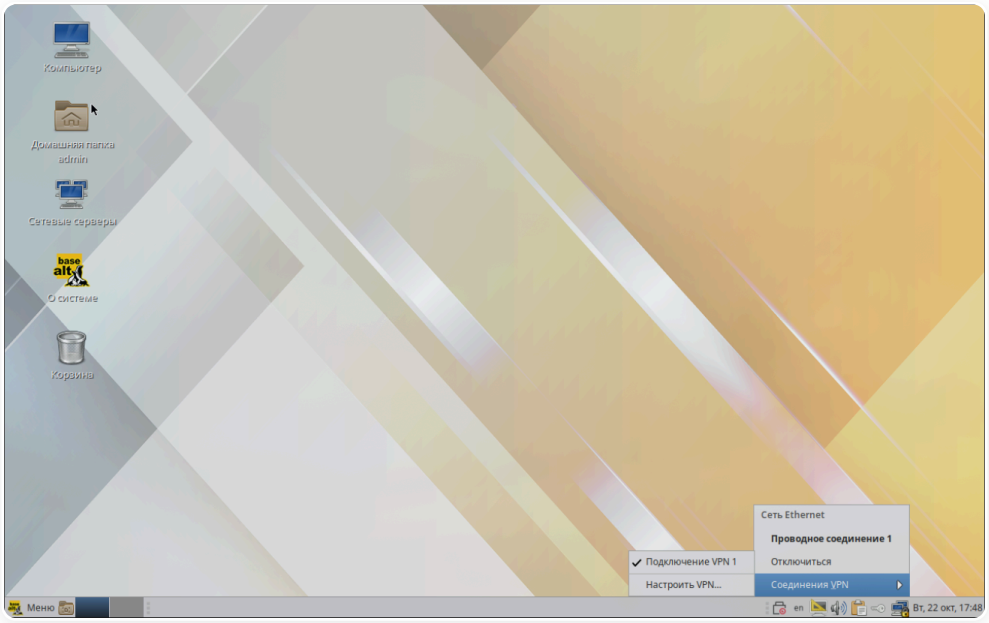
```
apt-get update && apt-get dist-upgrade && apt-get install NetworkManager-strongswan NetworkManager-strongswan-gnome strongswa
```

2. Установите корневой сертификат на рабочую станцию:

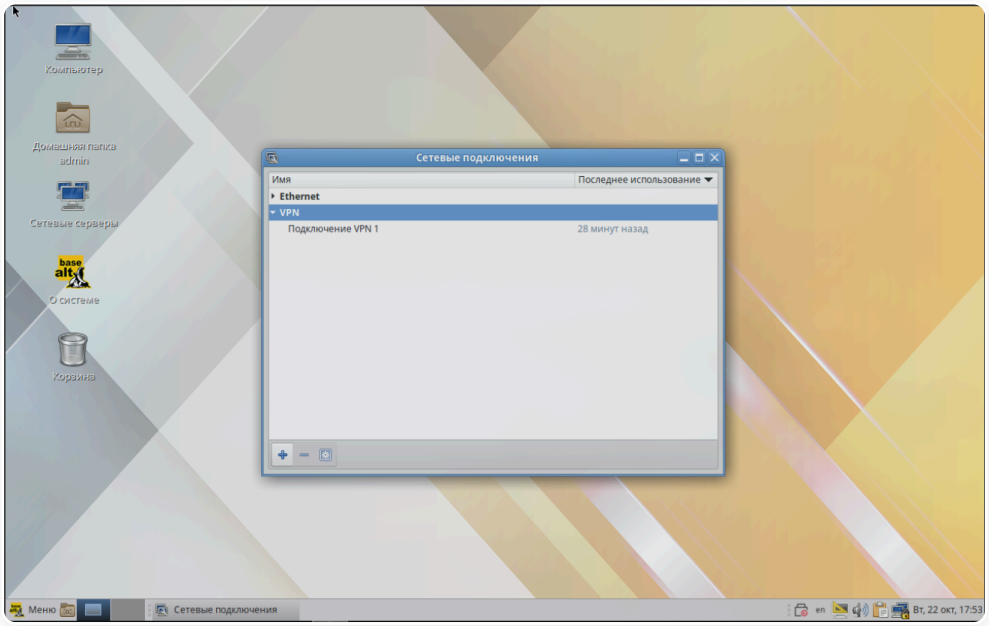
```
cp root-ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

- `root-ca.crt` - путь к сертификату.

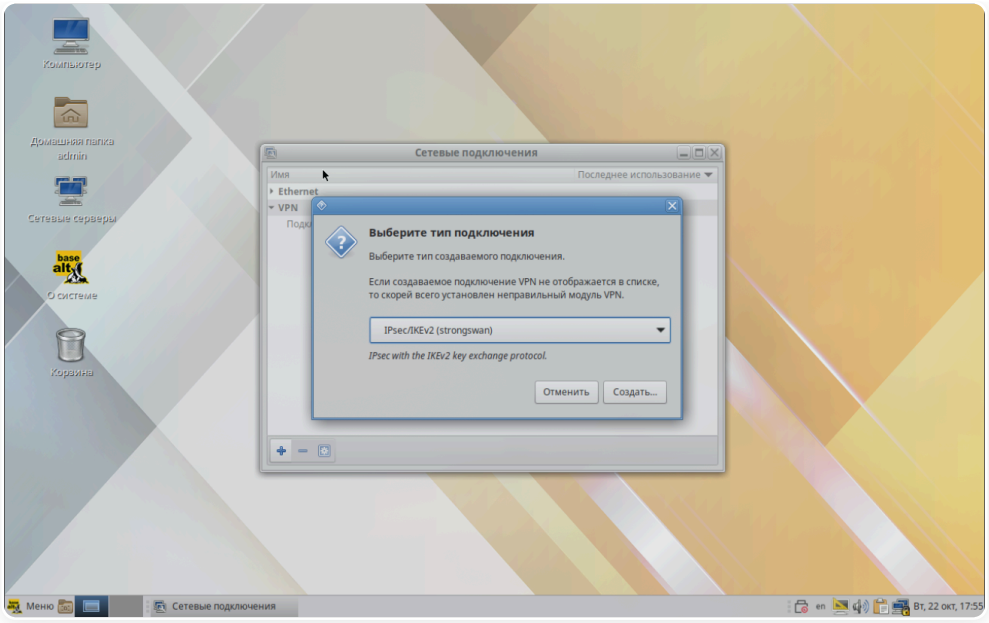
3. Перейдите в **Соединения VPN** и нажмите **Настроить VPN**:



4. Добавьте новое VPN-подключение:

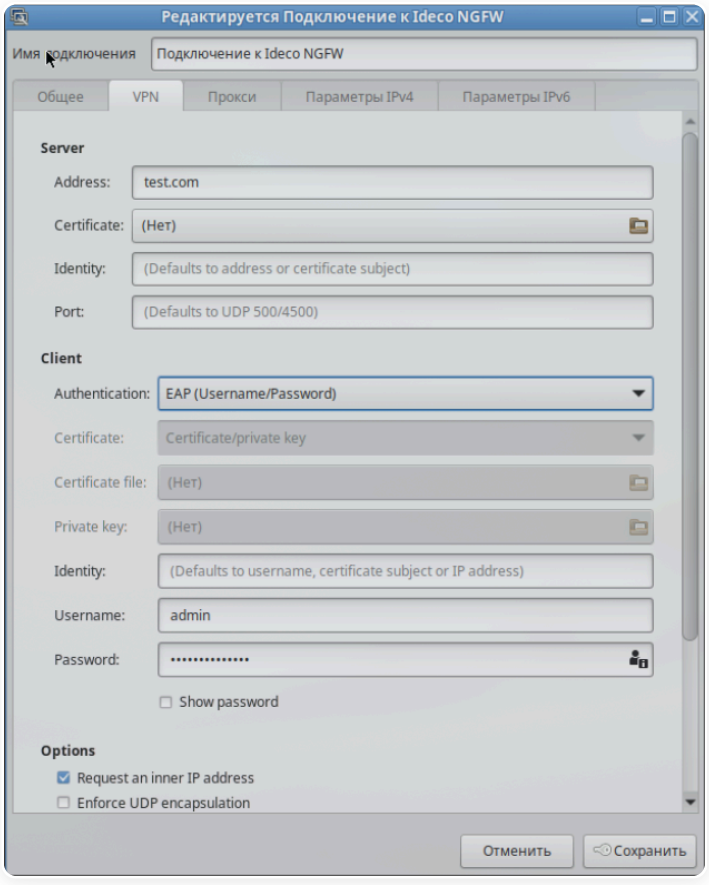


5. Выберите тип VPN-подключения `IPsec/IKEv2 (strongswan)` и нажмите **Создать**:

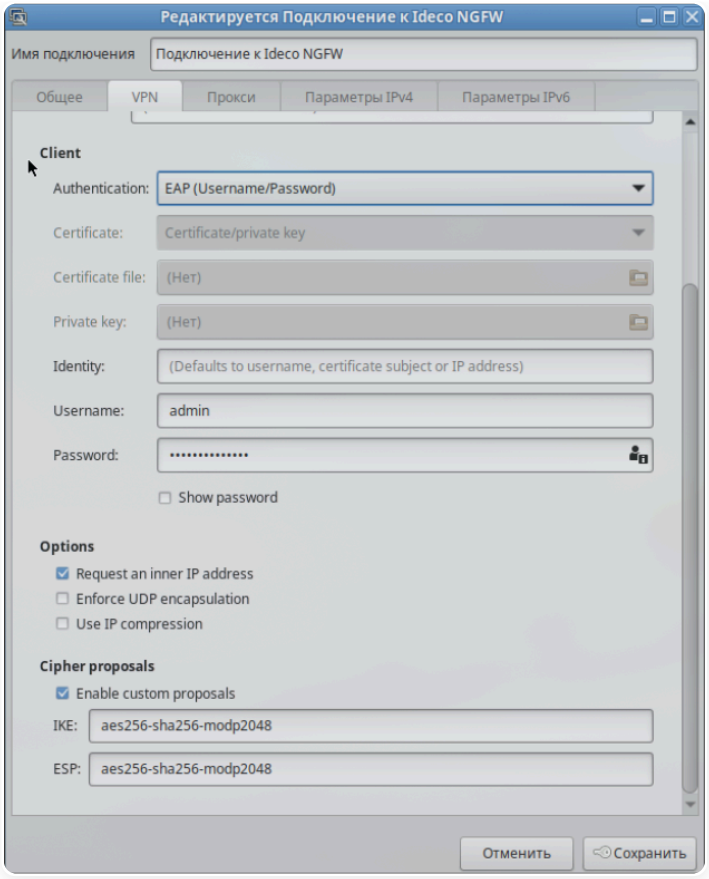


6. Заполните необходимые поля для создания VPN-подключения, как на скриншоте:

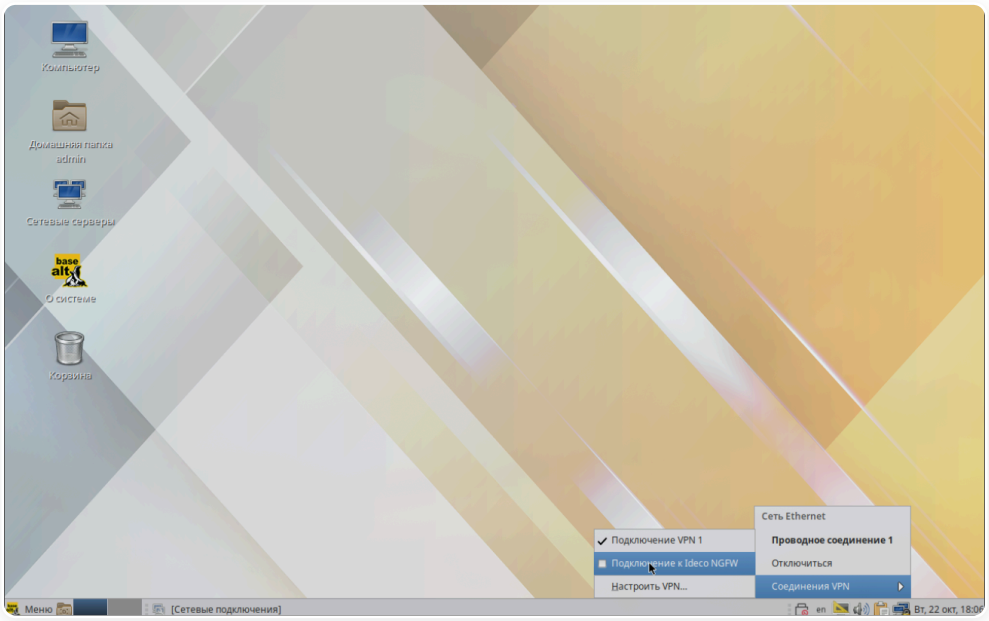
- Address - адрес шлюза;
- Authentication - тип аутентификации;
- Username - логин пользователя на Ideco NGFW;
- Password - пароль пользователя на Ideco NGFW.



7. Заполните параметры шифрования, как на скриншоте, и нажмите **Сохранить**:



8. Включите созданное VPN-подключение:



Создание VPN-подключения в Ubuntu

Перед настройкой VPN-подключения перейдите в раздел **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.

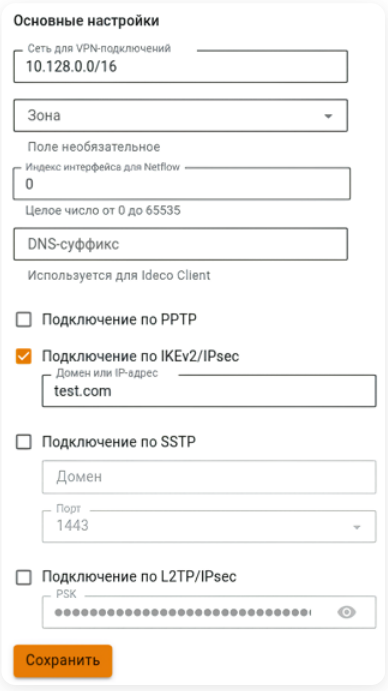
Инструкция актуальна для версии Ubuntu 24.04 LTS.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен или IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе 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 в хранилище доверенных сертификатов Ubuntu:

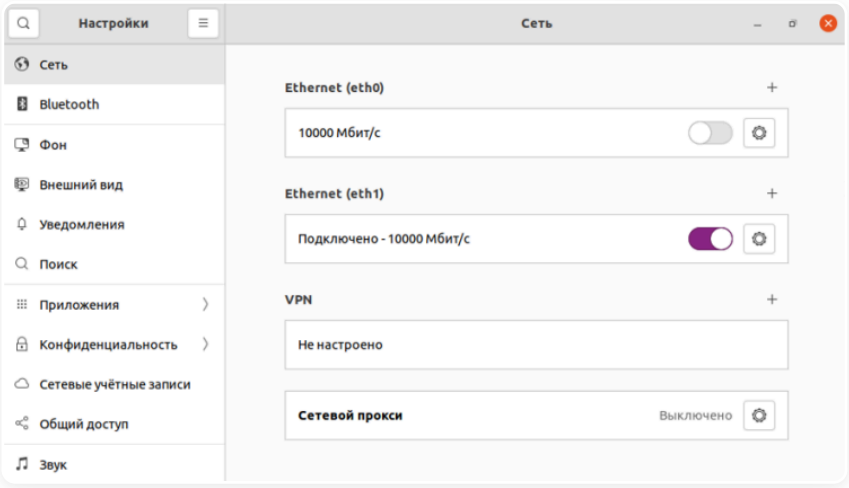
```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

- `ca.crt` - имя скачанного сертификата.

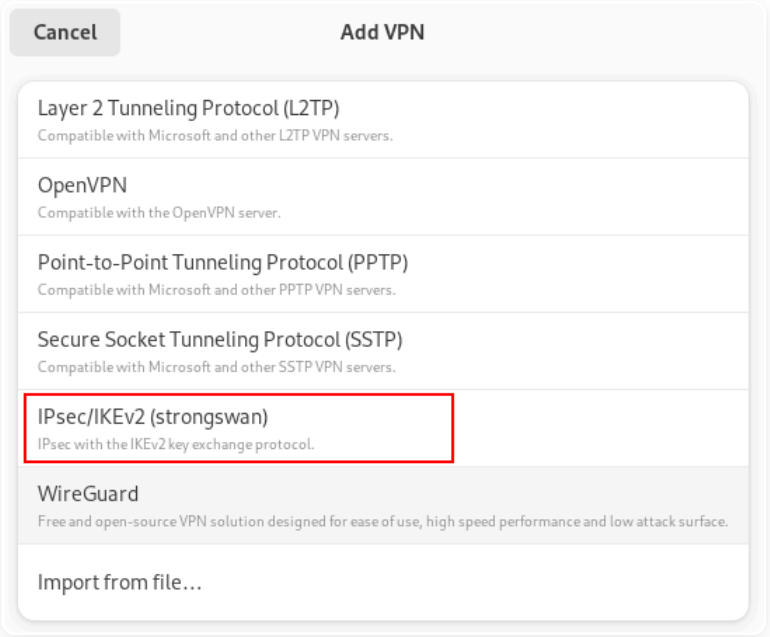
5. Для обновления сертификатов устройства выполните команду:

```
sudo update-ca-certificates
```

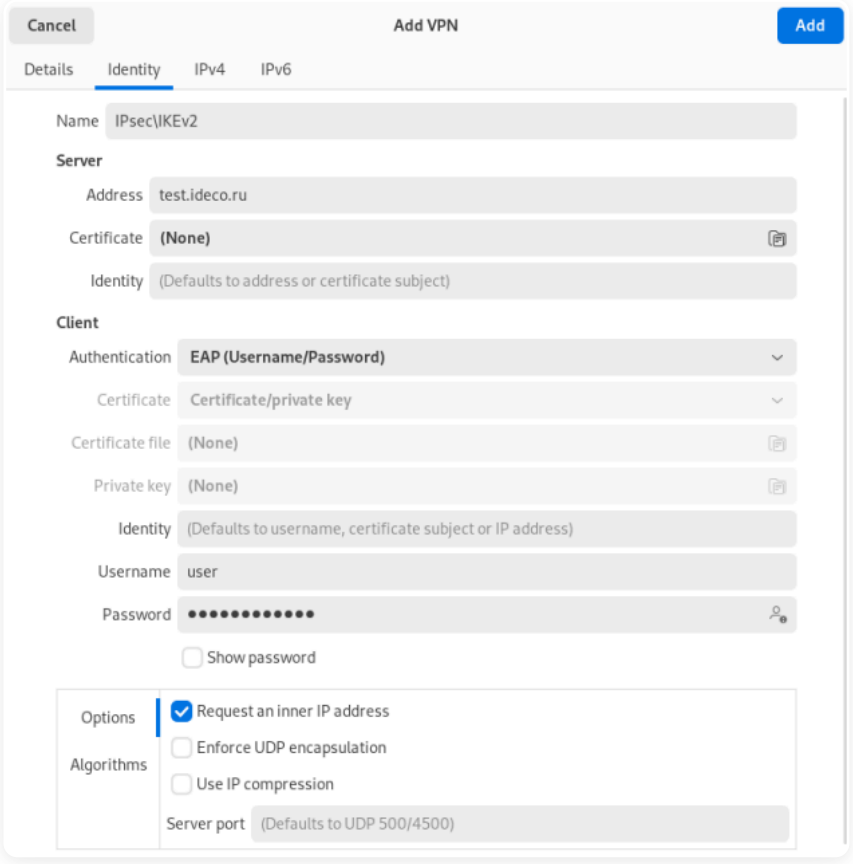
6. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋:



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** → **Подключение по 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.

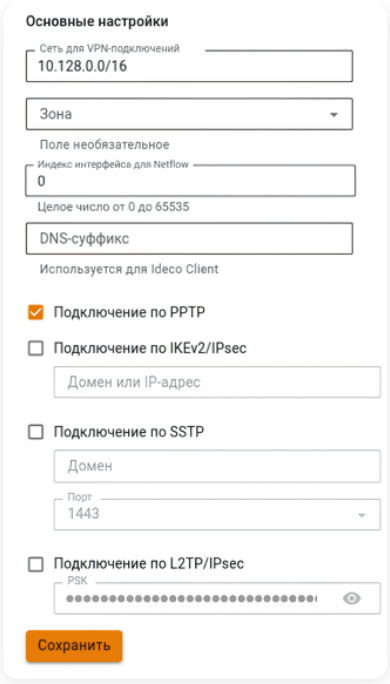
Установите флаг **Request an inner IP address** и нажмите **Добавить**.

9. Включите созданное VPN-подключение.

PPTP

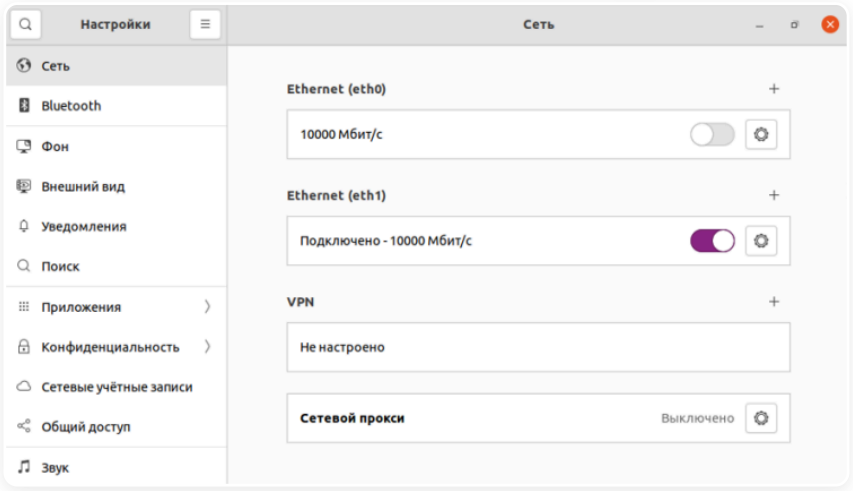
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное** и установите флаг **Подключение по PPTP**:



Создание подключения в Ubuntu:

1. Перейдите в **Настройки** → **Сеть** и в разделе **VPN** нажмите ＋:



2. В появившемся окне выберите **Туннельный протокол типа точка-точка (PPTP)**:

3. На вкладке **Идентификация** заполните поля:

- **Название** - имя подключения.
- **Шлюз** - домен или IP-адрес Ideco 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.

Рекомендуем нажать **Дополнительно** и установить флаги на пунктах:

- **Разрешить следующие методы аутентификации** - установите флаг на *MSCHAPv2*.
- **Использовать шифрование MPPE** - в строке *Шифрование* выберите 128-бит (наиболее защищенное).
- **Использовать для данных сжатие BSD**.
- **Использовать для данных сжатие Deflate**.
- **Использовать сжатие заголовков TCP**.

4. Нажмите **ОК** и **Добавить**.

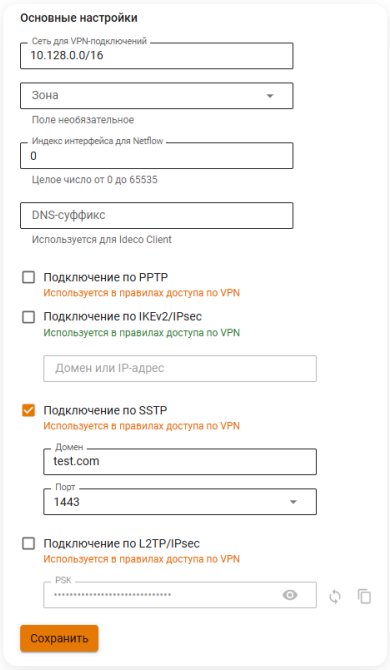
5. Включите созданное VPN-подключение:

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе 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 их более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **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
```

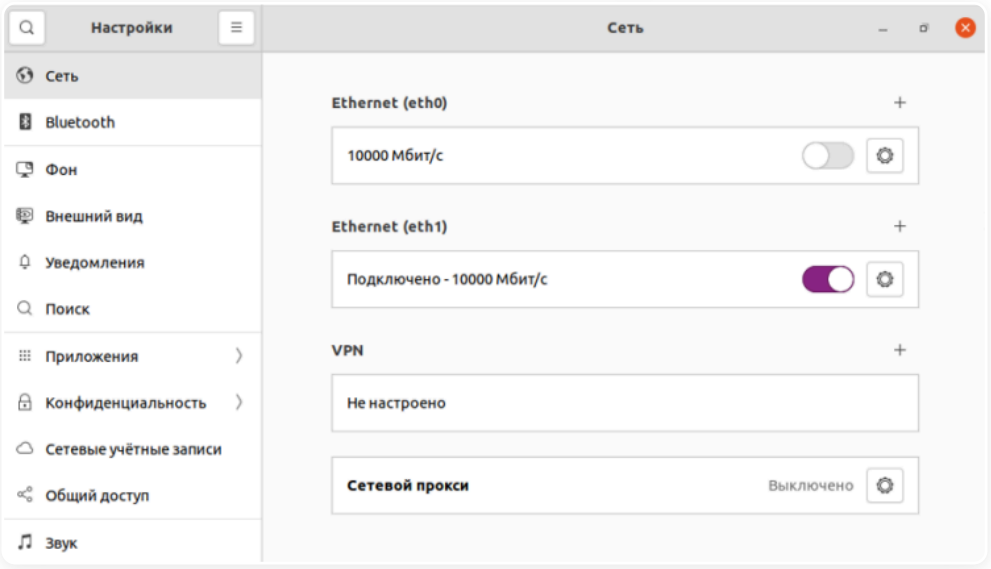
4. Проверьте установленные пакеты:

```
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.
- **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:

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 раздел **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте правило разрешающее VPN-подключение.

2. Загрузите на устройство корневой сертификат Ideco NGFW. Файл сертификата должен находиться в общедоступном каталоге.

Загружать сертификат **ISRG_ROOT_X1** не требуется, так как он уже есть в Fedora 40 и находится в каталоге `/etc/ssl/certs`.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен или IP-адрес**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW 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, 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 разделе **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.

PPTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное** и установите флаг **Подключение по PPTP**:

Создание подключения в Fedora:

1. Перейдите в **Настройки** → **Сети** и в строке **VPN** нажмите +.

2. В окне создания подключений выберите пункт **Туннельный протокол типа точка-точка (PPTP)**.

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

- **Имя** - название VPN-подключения;
- **Gateway** - доменное имя или IP-адрес NGFW;
- **User name** - логин пользователя, которому разрешено подключение по VPN;
- **Password** - пароль пользователя.

Рекомендуем нажать **Advanced** и установить флаги на пунктах:

- **Разрешить следующие методы аутентификации** - на *MSCHAPv2*;
- **Использовать шифрование MPPE** - в строке *Шифрование* выберите 128-бит (наиболее защищенное);
- **Использовать для данных сжатие BSD**;
- **Использовать для данных сжатие Deflate**;
- **Использовать сжатие заголовков TCP**.

5. Нажмите **Apply**, затем **Применить**.

6. Включите созданное VPN-подключение.

Если подключение по PPTP не устанавливается:

1. Выполните команду `sestatus`, чтобы узнать текущий режим SELinux. Если режим **Enforcing**, SELinux может блокировать работу PPTP.

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 PPTP. 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.

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **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;
- **Password** - пароль пользователя на Ideco NGFW.

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 их более одного. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **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.

Инструкция по созданию подключения в Astra Linux

Установка маршрутов по умолчанию поддерживается только для Windows-клиентов и для Ideco Client.
В Linux маршруты нужно добавлять вручную при конфигурировании подключения.

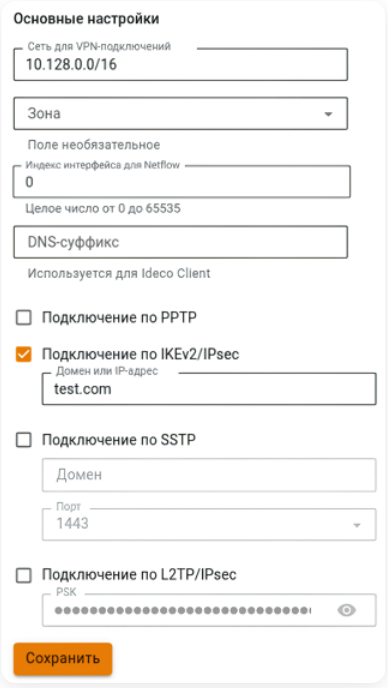
Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** и создайте разрешающее VPN-подключение правило.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите на вкладку **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW на вкладке **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

Создание подключения в Astra Linux:

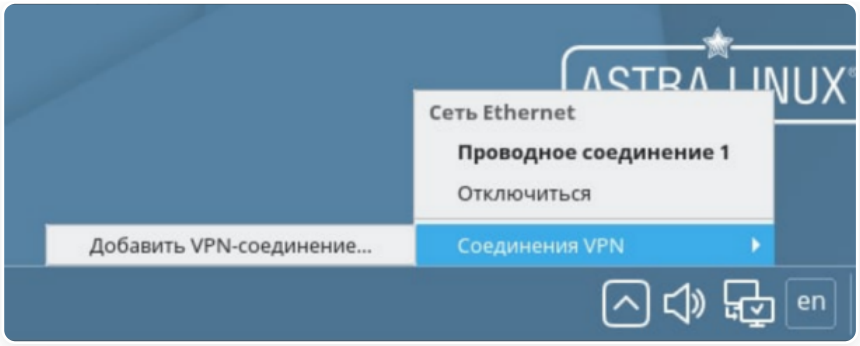
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt install libcharon-extra-plugins
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-extra-plugins
```

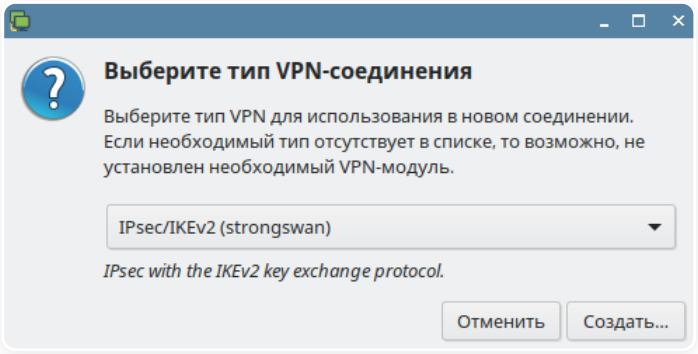
2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. В настройках сети выберите **Соединения VPN** → **Добавить VPN-соединение**:



4. Выберите тип соединения **IPsec/IKEv2 (strongswan)** и нажмите **Создать**:

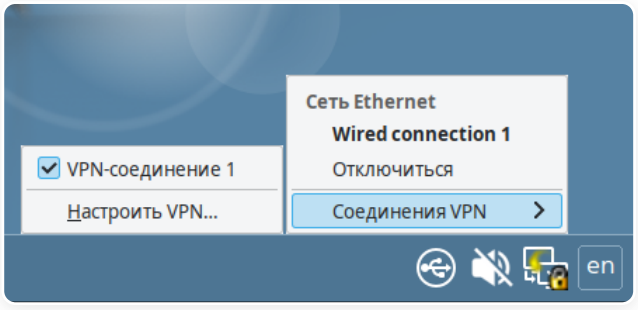


5. На вкладке **VPN** заполните поля:

- **Имя соединения** - имя подключения;
- **Address** - введите домен или IP-адрес, который указан в настройках **Пользователи → VPN-подключения → Основное → Подключение по 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
```

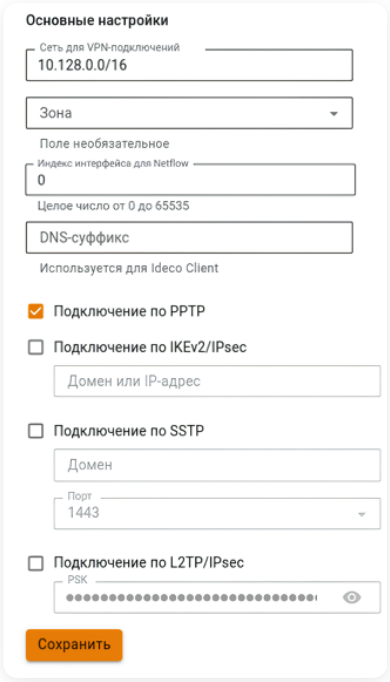
- для Phase1 Algorithm ищите значения **proposals=**;
- для Phase2 Algorithms ищите значения **esp_proposals=**.

PPTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по PPTP**:



Создание подключения в Astra Linux:

1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
sudo apt update
sudo apt install network-manager-pptp network-manager-pptp-gnome pptp-linux
```

2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

3. В настройках сети выберите **Соединения VPN** → **Добавить VPN-соединение**:

4. Выберите тип соединения **Туннельный протокол типа точка-точка (PPTP)** и нажмите **Создать**:

5. На вкладке **VPN** заполните поля и нажмите **Сохранить**:

- **Имя соединения** - имя подключения;
- **Шлюз** - IP-адрес или домен внешнего интерфейса Ideco NGFW;
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля веберите вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

6. В настройках сети выберите **Соединения VPN** и установите флаг в строке с созданным соединением:

L2TP/IPsec

Настройка Ideco NGFW:

1. Перейдите на вкладку **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

Создание подключения в Astra Linux:

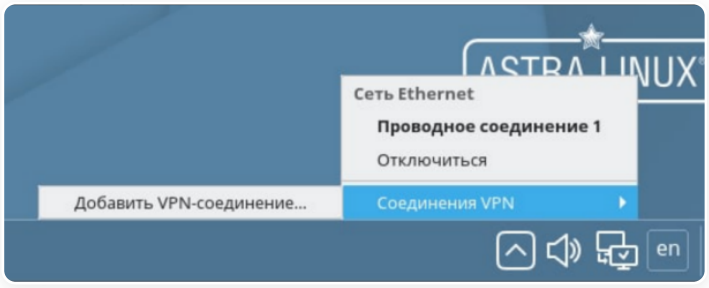
1. Откройте терминал и установите необходимые пакеты, выполнив команды:

```
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;
- **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 (**Пользователи** → **VPN-подключение** → **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**:

Инструкция по созданию подключения в Windows

Перед настройкой VPN-подключения перейдите в раздел **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 на вкладку **Сеть** → **IP версии 4 (TCP/IPv4)** → **Дополнительно**.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

4. Импортируйте сертификат Ideco NGFW:

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 иконке 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 IKEv2.

- **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).
- **Протокол расширенной проверки подлинности (EAP)** - Microsoft защищенный пароль (EAP MSCHAPV2).

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**.

PPTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное** и установите флаг **Подключение по PPTP**:

Создание подключения в Windows:

1. Кликните на иконке 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 PPTP.
- **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**.

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:

3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе Сервисы → Сертификаты → Загруженные сертификаты.

4. Импортируйте сертификат Ideco NGFW:

Пример для Windows

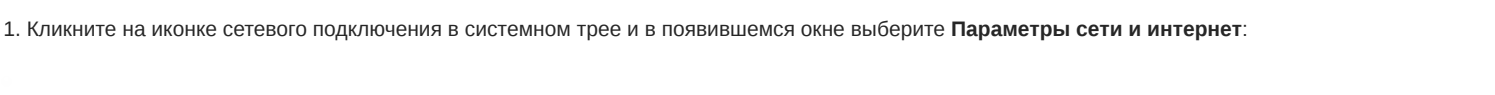
1. Откройте скачанный сертификат и нажмите **Установить сертификат**:



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



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

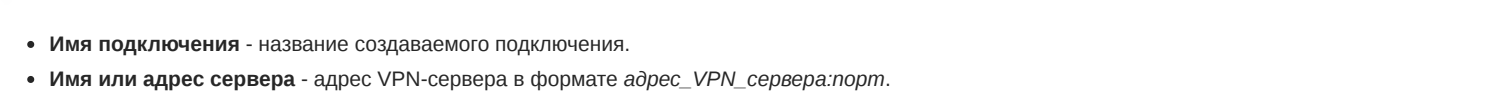


Создание подключения в Windows:

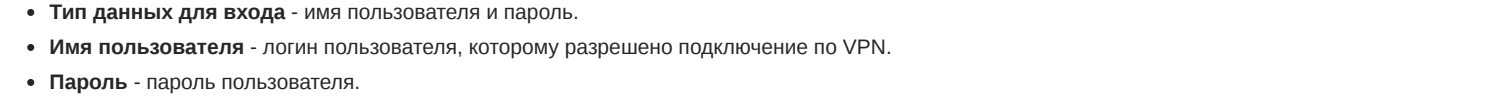
1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



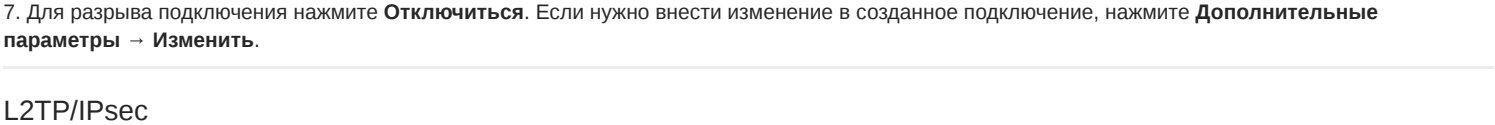
- **Имя подключения** - название создаваемого подключения.
- **Имя или адрес сервера** - адрес VPN-сервера в формате *адрес_VPN_сервера:порт*.
- **Тип VPN** - протокол SSTP.
- **Тип данных для входа** - имя пользователя и пароль.
- **Имя пользователя** - логин пользователя, которому разрешено подключение 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**.

L2TP/IPsec

Важно: L2TP/IPsec клиенты, находящиеся за одним NAT, могут испытывать проблемы подключения, если их более одного. В решении проблемы поможет инструкция. Рекомендуем вместо L2TP/IPsec использовать IKEv2/IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Windows:

1. Кликните на иконке 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 строки **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 разделе **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 не имеет "белого" IP-адреса, а необходимые для работы порты (500 и 4500) "проброшены" на внешний интерфейс устройства, расположенного перед Ideco NGFW 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 и указать на внешнем интерфейсе Ideco NGFW "белый" IP-адрес, к которому в итоге и будут осуществляться L2TP/IPsec-подключения. Либо используйте протокол SSTP - его 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. Оно 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 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 на мобильных устройствах по протоколам IKEv2/IPsec, L2TP/IPsec, SSTP и PPTP.

Перед настройкой VPN-подключения перейдите в **Пользователи** → **VPN-подключения** → **Доступ по VPN** в Ideco NGFW 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

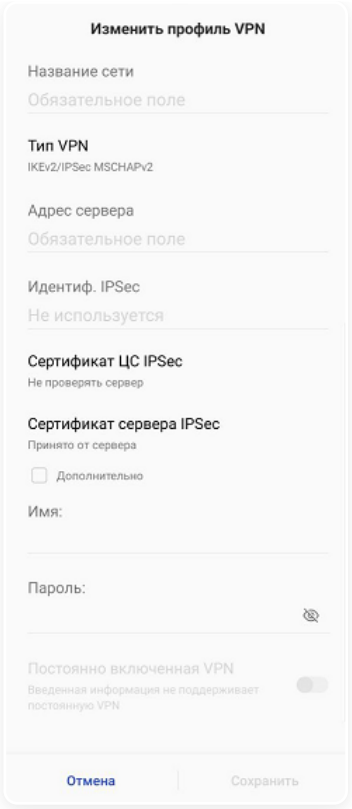
Android

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:

Для IKEv2/IPsec MSCHAPv2:

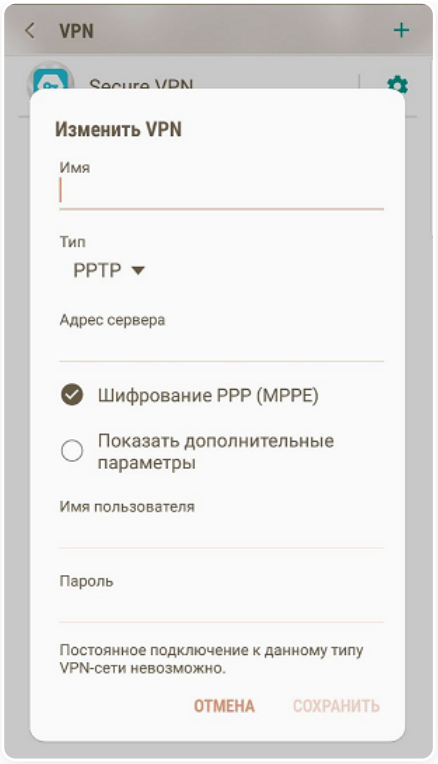


Расшифровка полей

- **Название сети** - имя подключения.
- **Адрес сервера** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по 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.

Для PPTP:

Начиная с версии Android 12 прекращена поддержка протокола PPTP. Не рекомендуем использовать PPTP, так как подключение крайне небезопасно.

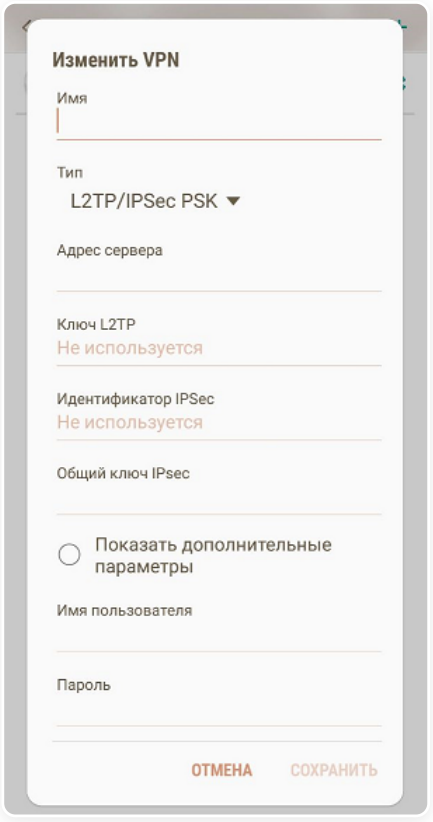


Расшифровка полей

- **Имя** - имя подключения.
- **Адрес сервера** - домен или IP-адрес Ideco NGFW.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

Для L2TP/IPsec PSK:

Начиная с версии Android 12 прекращена поддержка протокола L2TP. Не рекомендуем использовать L2TP, так как подключение крайне небезопасно.



Расшифровка полей

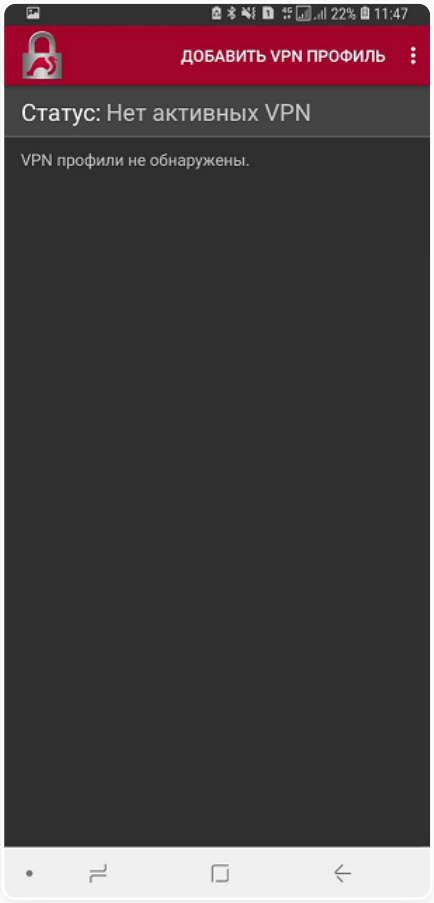
- **Имя** - имя подключения.
- **Адрес сервера** - домен или IP-адрес Ideco NGFW.
- **Общий ключ IPsec** - значение поля **PSK** в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по L2TP/IPsec** в Ideco NGFW.

3. Нажмите **Сохранить** и активируйте подключение.

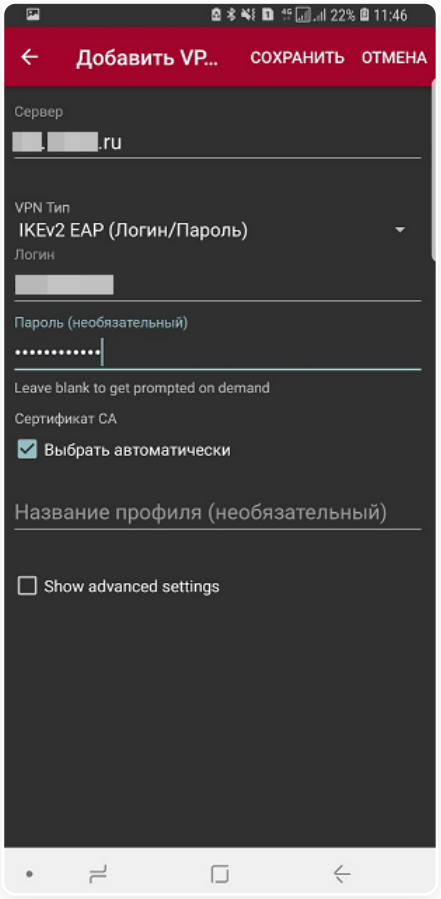
StrongSwan

Приложение StrongSwan позволяет создавать VPN-подключение только через протокол IKEv2.

1. Нажмите **Добавить VPN профиль**:



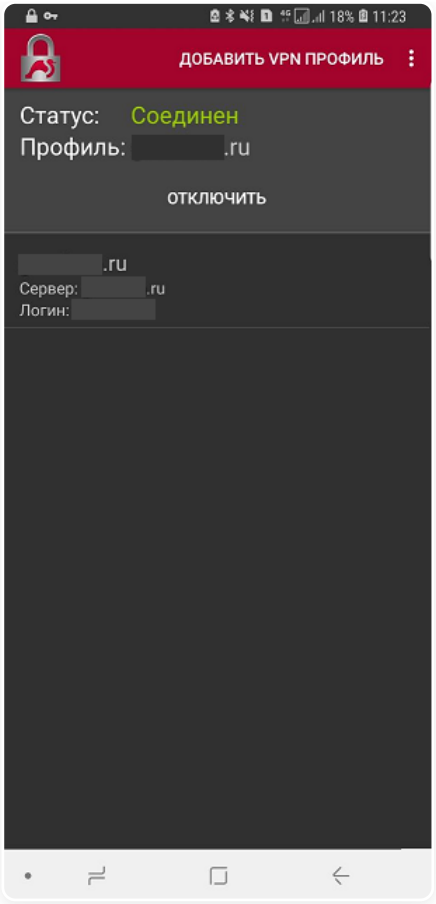
2. Заполните поля:



Расшифровка полей

- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи** → **VPN-подключения** → **Основное** → **Подключение по IKEv2/IPsec**.
- **VPN тип** - IKEv2 EAP (Логин/Пароль).
- **Логин** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

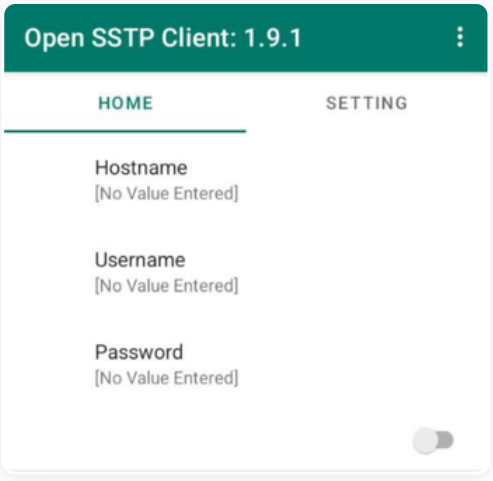
3. Нажмите **Сохранить** и перейдите по созданному подключению:



Open SSTP Client

Приложение Open SSTP Client позволяет создавать VPN-подключение через протокол SSTP.

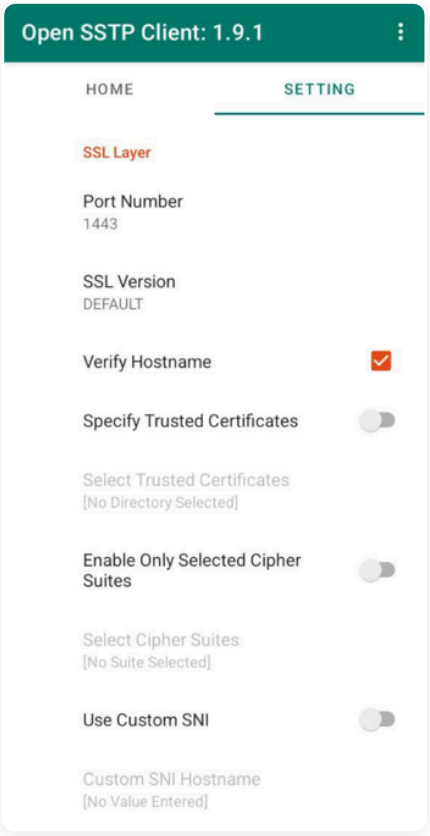
1. Откройте приложение и заполните поля:



Расшифровка полей

- **Hostname** - домен, указанный в Ideco NGFW 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.



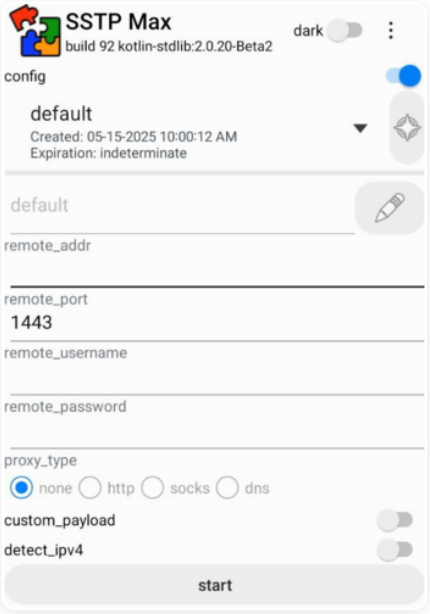
Для автоматического подключения включите опцию **Enable Reconnection** на вкладке **SETTING**.

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 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.

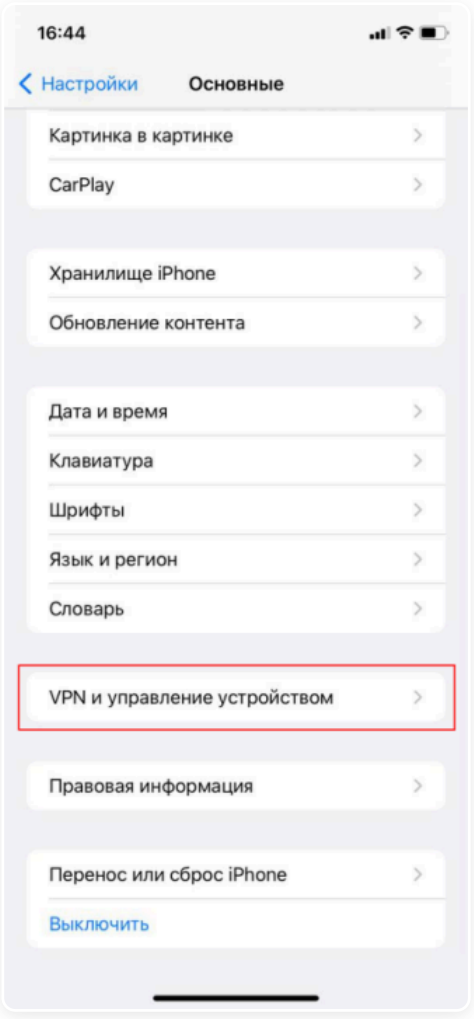
2. Нажмите start.

---

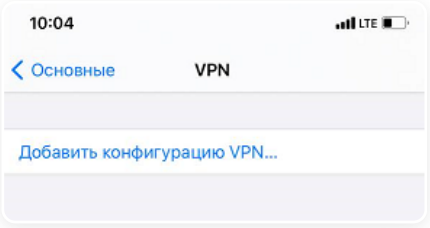
iOS

iOS

1. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством** → **VPN**:



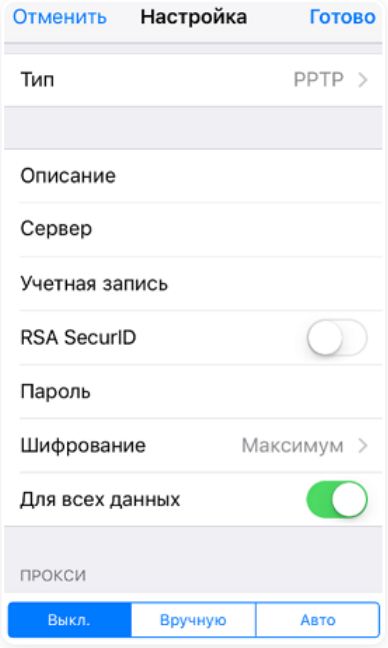
2. Нажмите **Добавить конфигурацию VPN**:



3. Выберите **Тип** подключения и заполните поля:

Для PPTP:

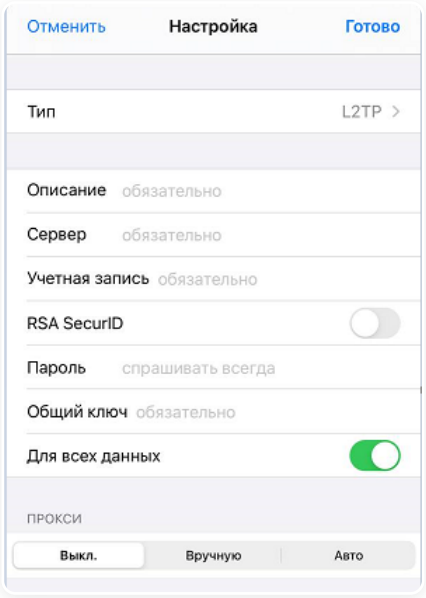
> Начиная с версии iOS 10 прекращена поддержка протокола PPTP. Не рекомендуем использовать PPTP, так как подключение крайне небезопасно.



Расшифровка полей

- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес Ideco NGFW.
- **Учетная запись** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

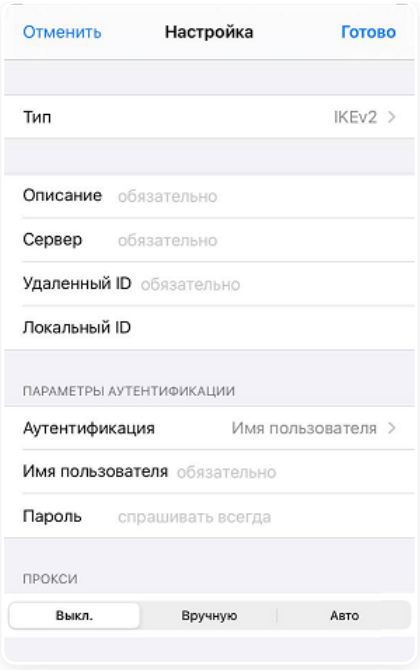
Для L2TP:



Расшифровка полей

- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес Ideco NGFW.
- **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.

Для IKEv2:

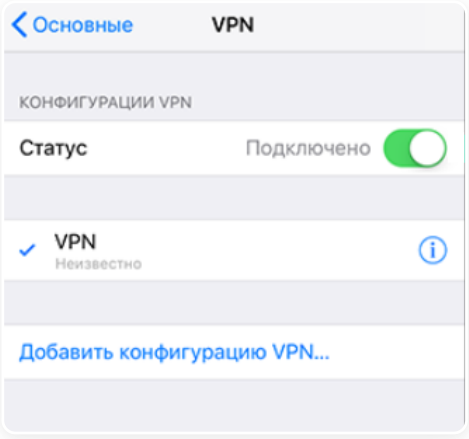


Расшифровка полей

- **Описание** - название соединения.
- **Сервер** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи → VPN-подключения → Основное → Подключение по IKEv2/IPsec**.
- **Удаленный ID** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи → VPN-подключения → Основное → Подключение по IKEv2/IPsec**.
- **Имя пользователя** - логин пользователя, которому разрешено подключение по VPN.
- **Пароль** - пароль пользователя.

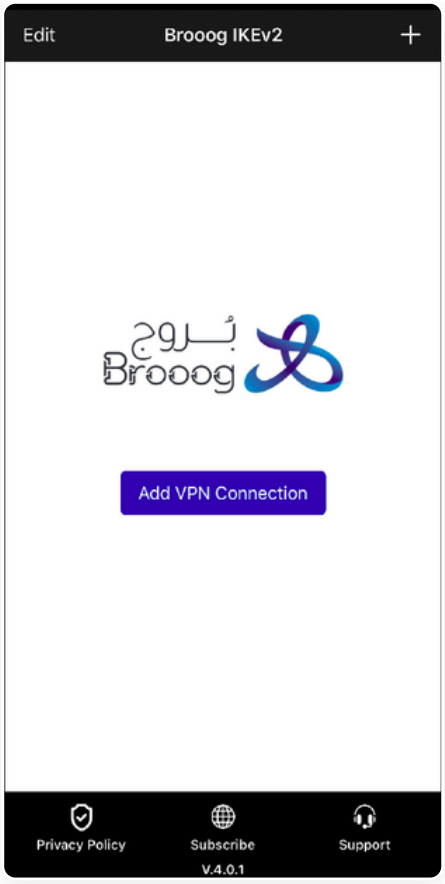
4. Нажмите **Готово**.

5. Включите опцию **Статус**:

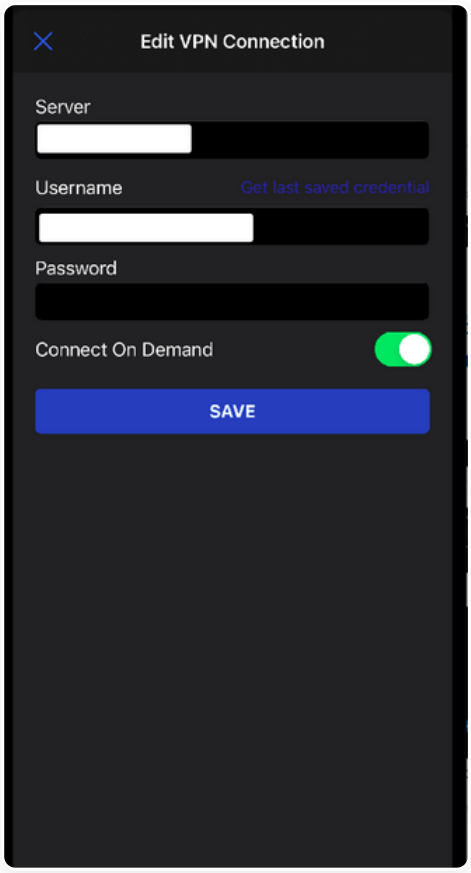


Brooog IKEv2

1. Нажмите **Add VPN Connection**:



2. Заполните поля и включите опцию **Connect on Demand**:

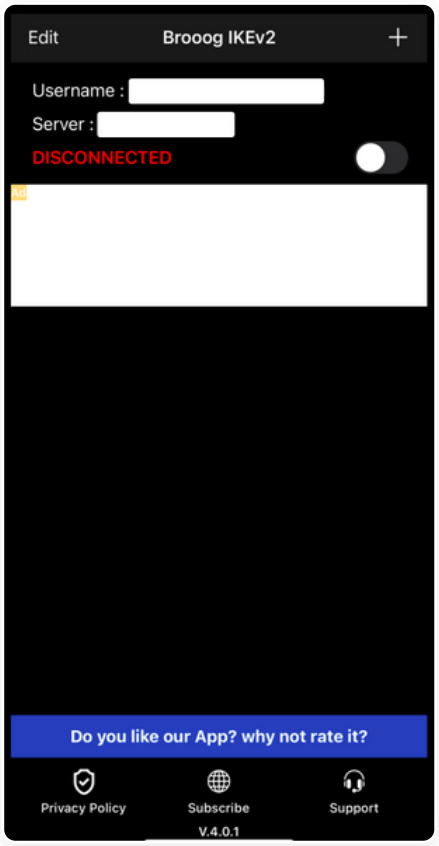


Расшифровка полей

- **Server** - домен или IP-адрес, указанный в Ideco NGFW в разделе **Пользователи → VPN-подключения → Основное → Подключение по IKEv2/IPsec**.
- **Username** - логин пользователя, которому разрешено подключение по VPN.

- **Password** - пароль пользователя.

3. Нажмите **Save** и переведите опцию в режим **CONNECTED**:



Инструкция по созданию подключения в Mac OS

Перед настройкой VPN-подключения перейдите в раздел **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:

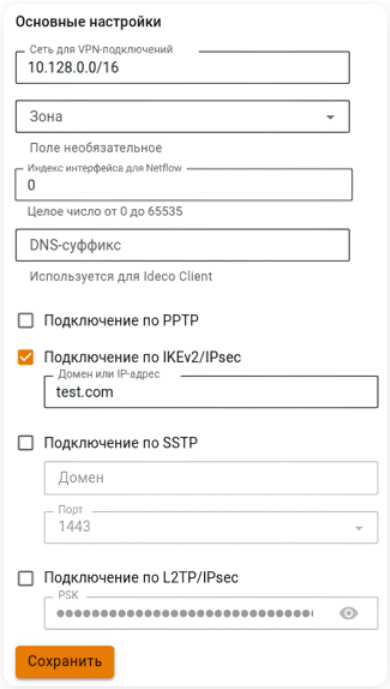
1. Проверить, что в качестве VPN-сервера указано его доменное имя в разделе **Пользователи** → **VPN-подключения**.
2. Проверить, что на доменное имя VPN-сервера выдан сертификат Let's Encrypt.

IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен или IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Применение сертификатов:

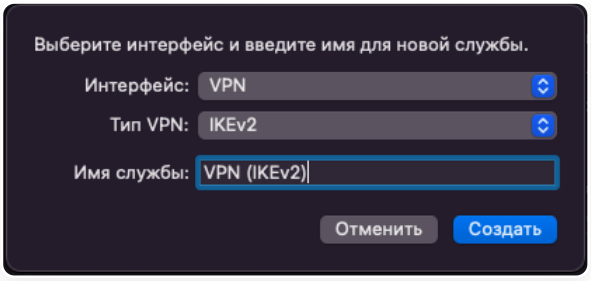
- Если сертификат для VPN-подключений издан NGFW, установите корневой сертификат NGFW на устройство пользователя.
- Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.
- Если используется сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле Subject Alternative Name (SAN). Загрузите сертификат как пользовательский в разделе Сервисы → Сертификаты → Загруженные сертификаты.

Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки** → **Сеть**.

2. Нажмите **Добавить** в левом нижнем углу (иконка +).

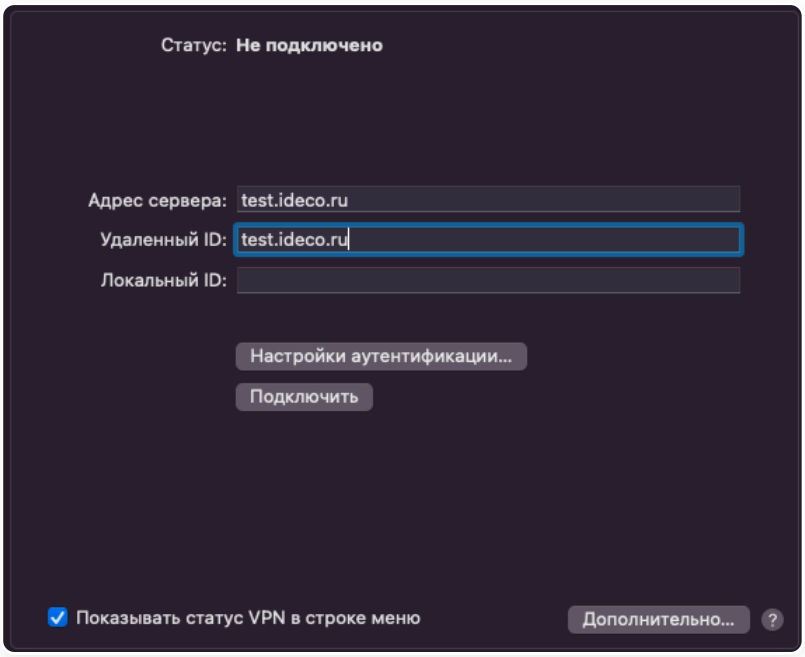
3. Заполните поля:



- **Интерфейс** - VPN;
- **Тип VPN** - IKEv2;
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

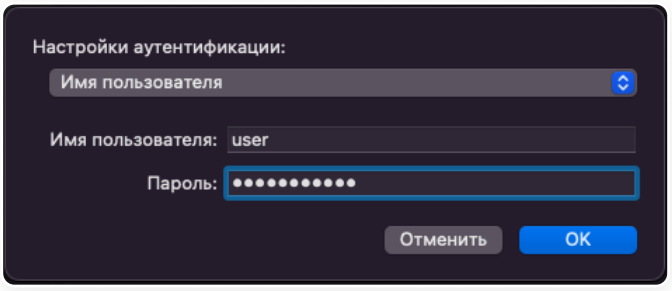
5. Установите параметры подключения:



- **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**.

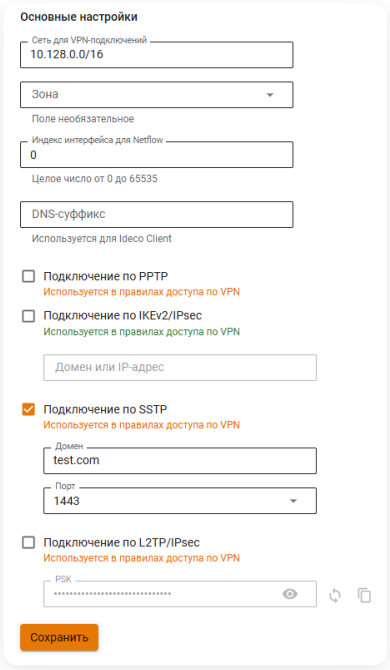
9. Поставьте флаг в пункте **Показывать статус VPN в строке меню**, нажмите **Применить** и включите соединение.

SSTP

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи → VPN-подключения → Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **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 разделе 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 командой:

```
sudo /usr/local/sbin/sstpc --cert-warn --tls-ext --user <логин пользователя Ideco NGFW> --password <Пароль пользователя Ideco
```

- 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 маршрутизация 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 оно было установлено, и нажмите **Ctrl+C**.

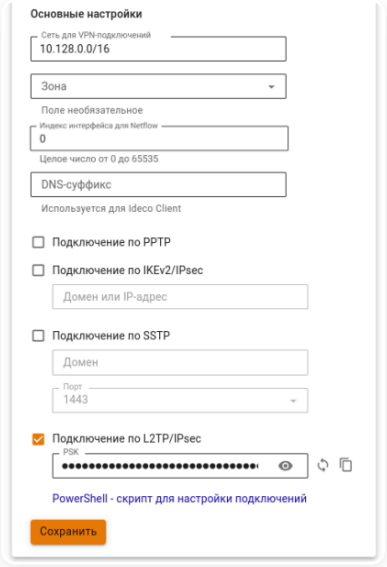
L2TP/IPsec

Важно: L2TP IPsec-клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их более одного. Рекомендуем вместо L2TP IPsec использовать IKEv2 IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи** → **VPN-подключения** → **Основное**.

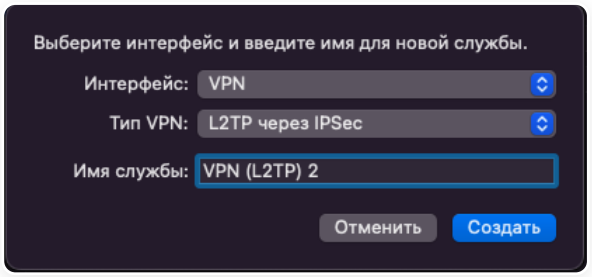
2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки** → **Сеть** и нажмите **Добавить** в левом нижнем углу (иконка (+)).

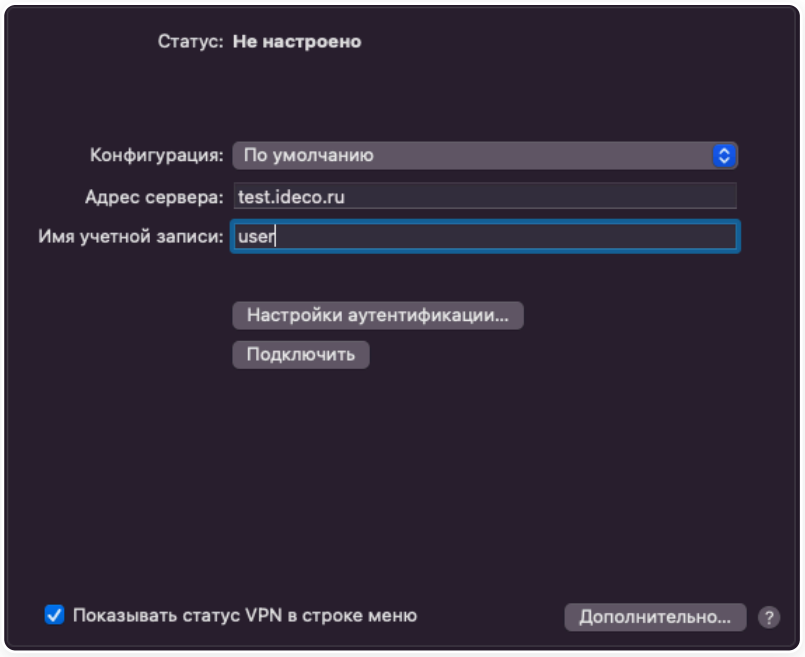
3. Заполните поля:



- **Интерфейс** - VPN;
- **Тип VPN** - L2TP через IPsec;
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

5. Заполните **Адрес сервера** и **Имя учетной записи**:



6. Поставьте флаг на пункте **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.

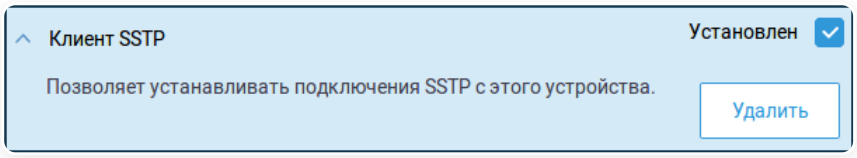
Подключение по SSTP Wi-Fi-роутеров Keenetic

Поддерживаются все роутеры на базе KeeneticOS 3.x.x.

1. Выполните настройку пользователей в Ideco NGFW и включите SSTP в разделе **Пользователи** → **VPN-подключения** → **Основное**.

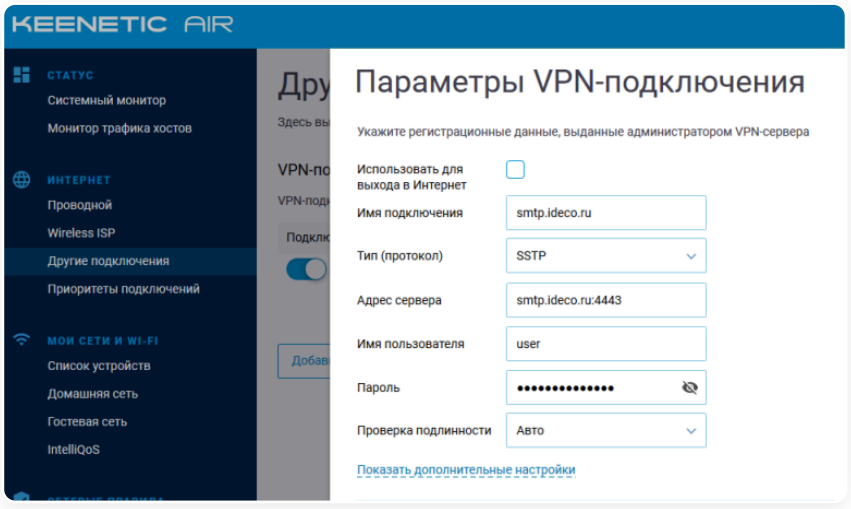
2. Зайдите в веб-интерфейс управления Keenetic: `http://my.keenetic.net`.

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.

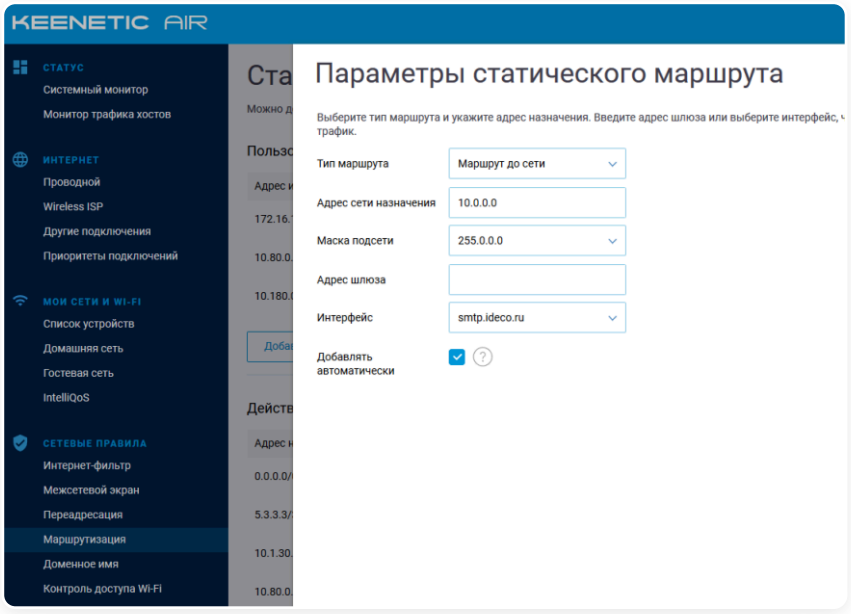
4. Создайте подключение в разделе **Интернет** → **Другие подключения** нажмите кнопку **Добавить подключение**



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.

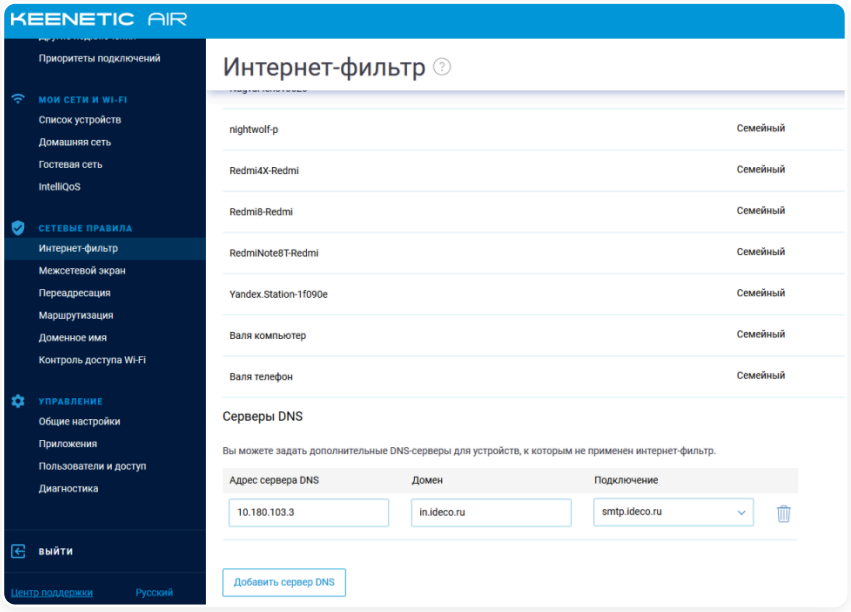
5. В разделе **Сетевые правила** → **Маршруты** добавьте маршруты в рабочую сеть. Например, если сеть офиса `10.0.0.0/8`, добавьте маршрут:



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 разделе **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.

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.

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.

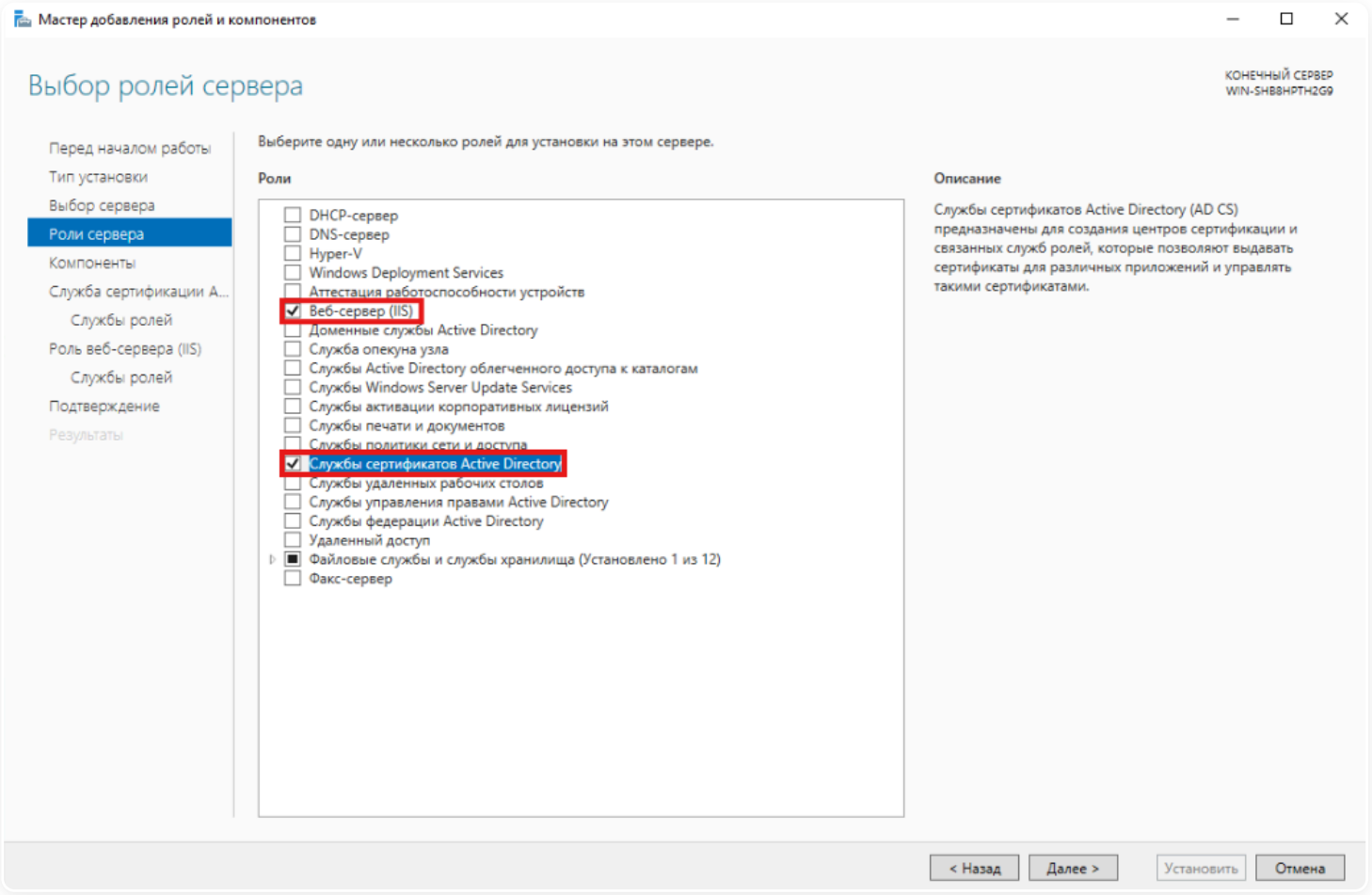
AuthorityInformationAccess

- `Empty=True` - не добавляет URL-адрес AIA в сертификаты, выданные центром сертификации.

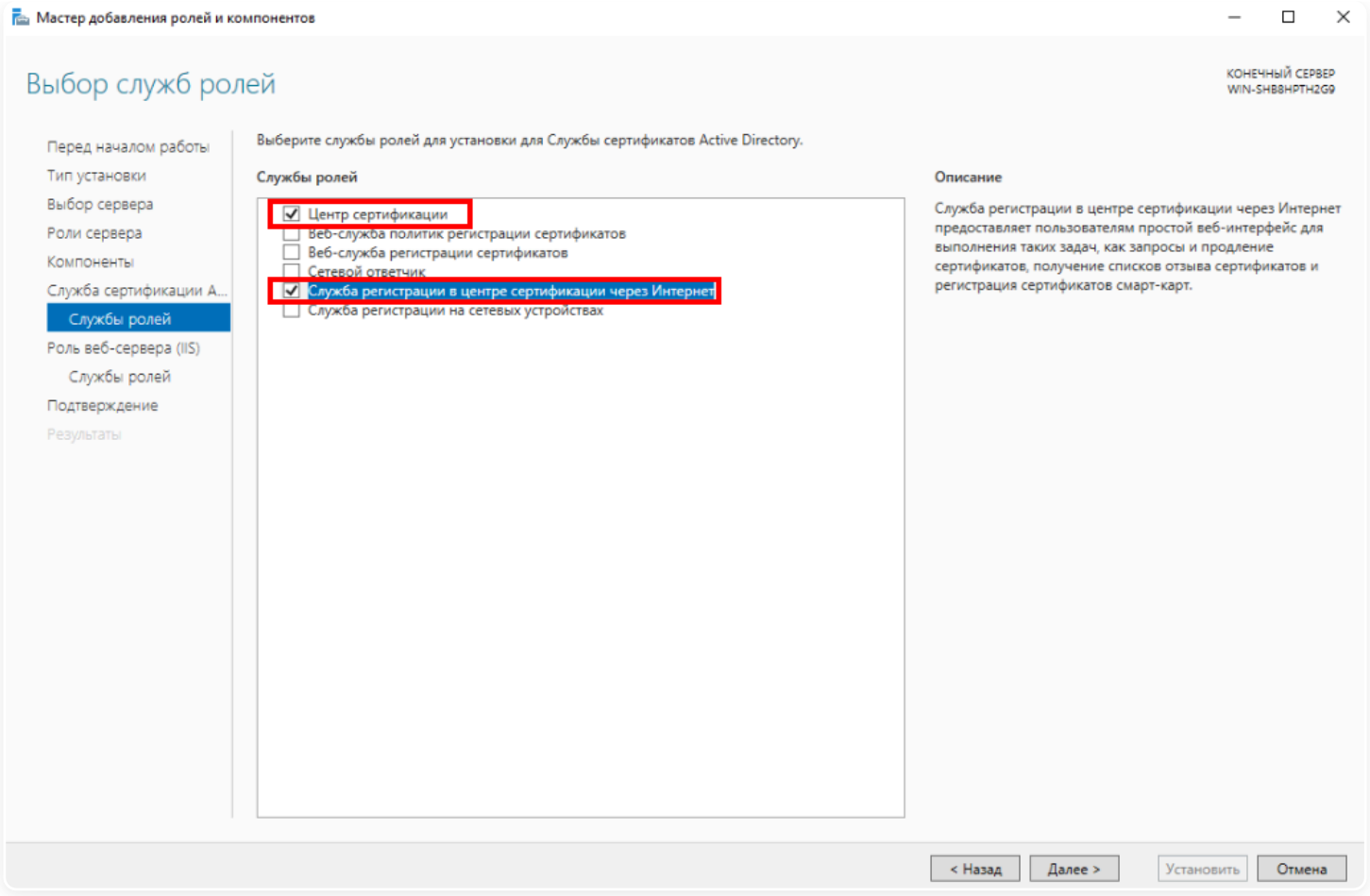
Шаг 2. Установка ролей служб сертификации

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**:

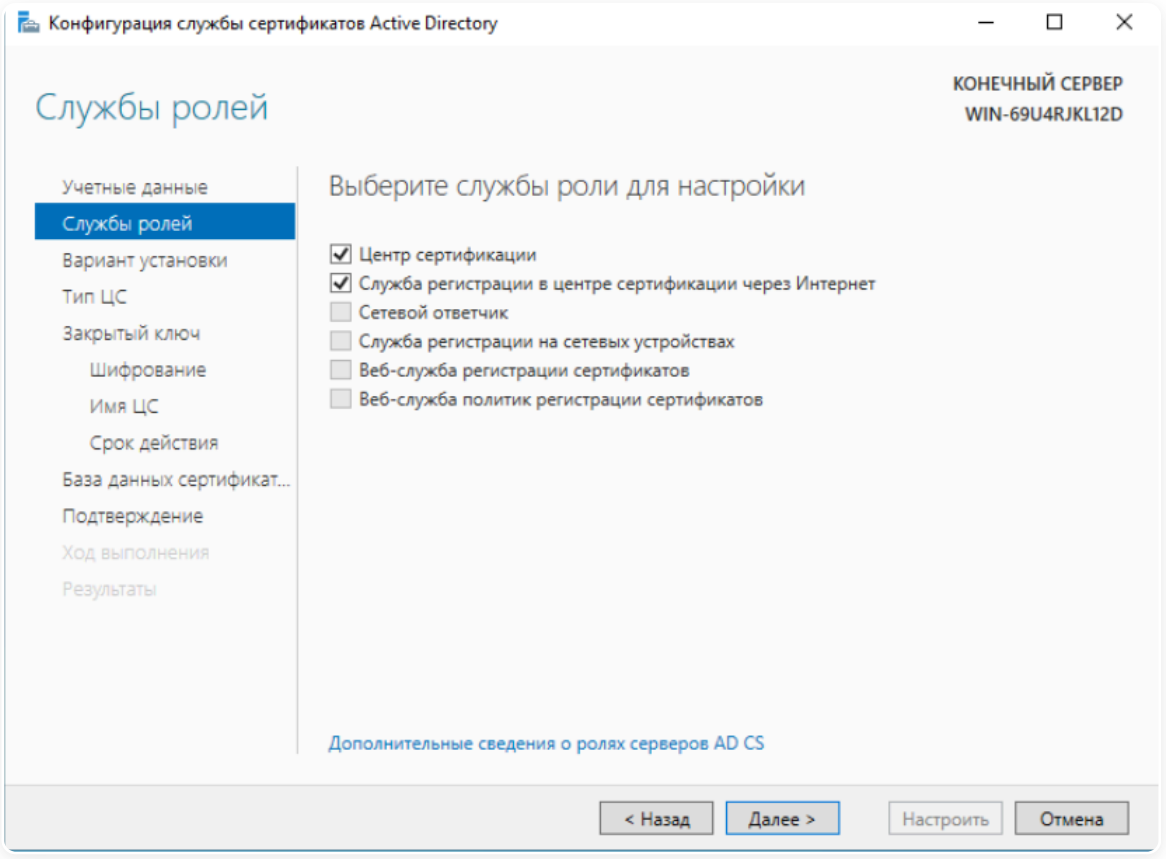


4. Завершите установку.

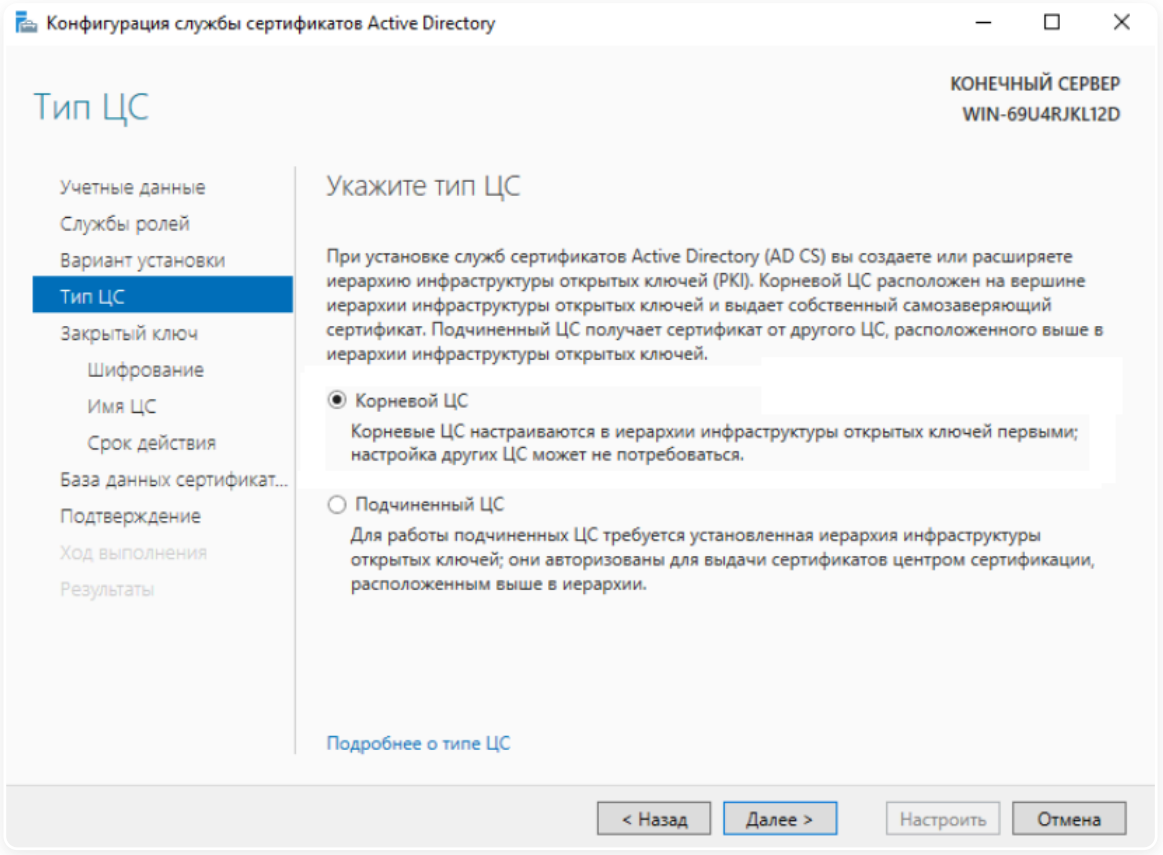
Шаг 3. Настройка служб сертификации

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

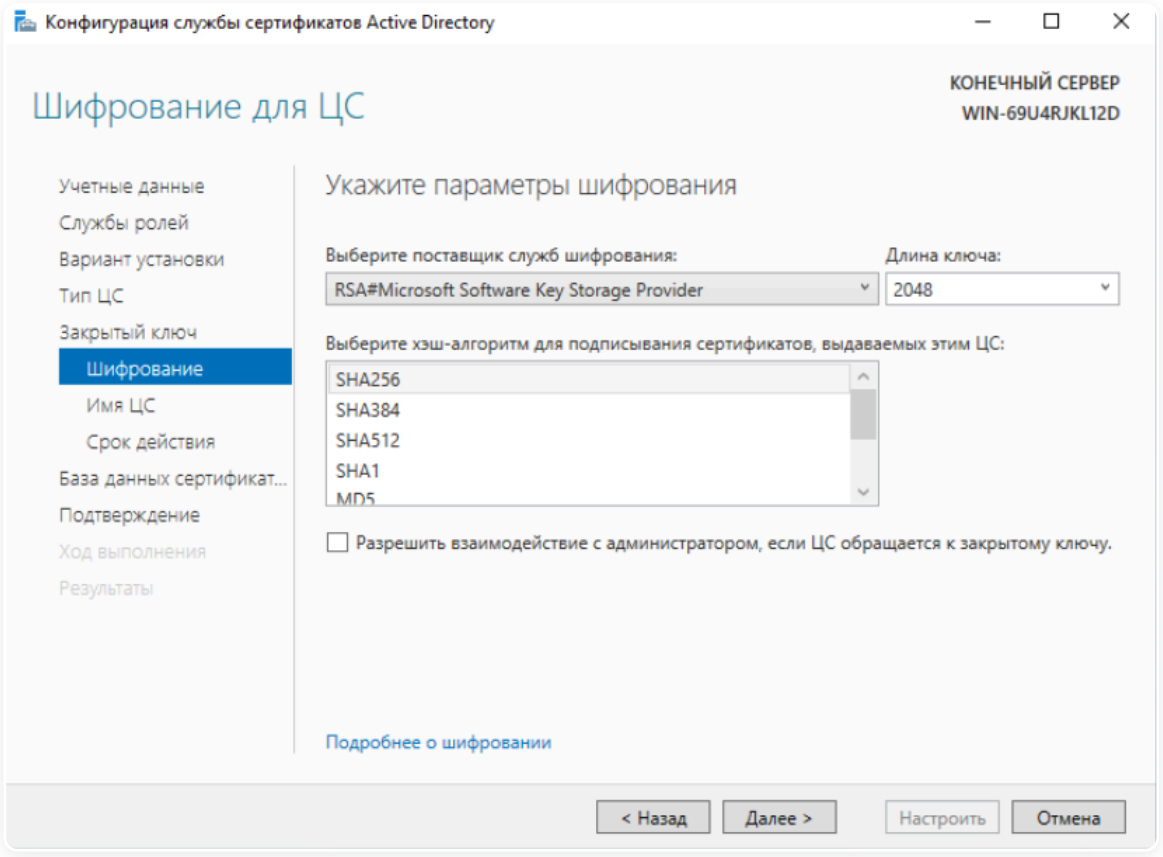
2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



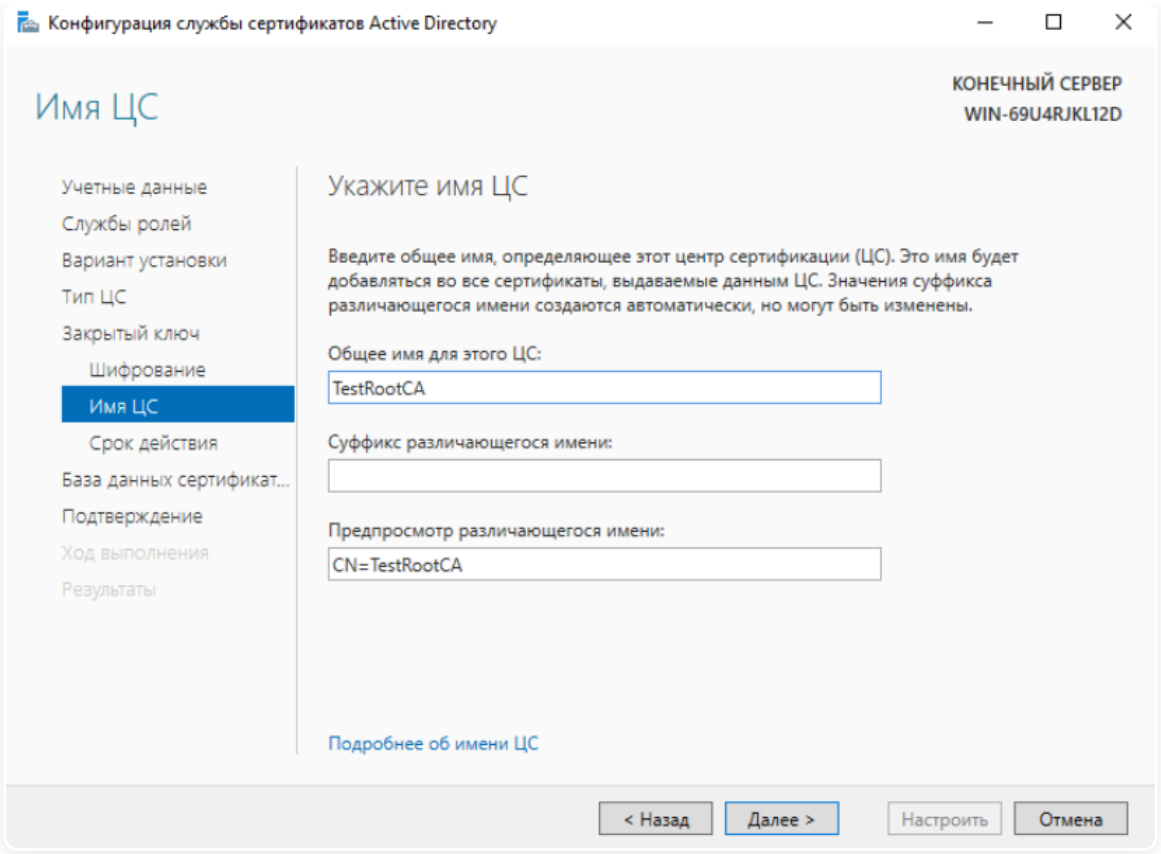
3. На этапе **Тип ЦС** выберите **Корневой ЦС**:



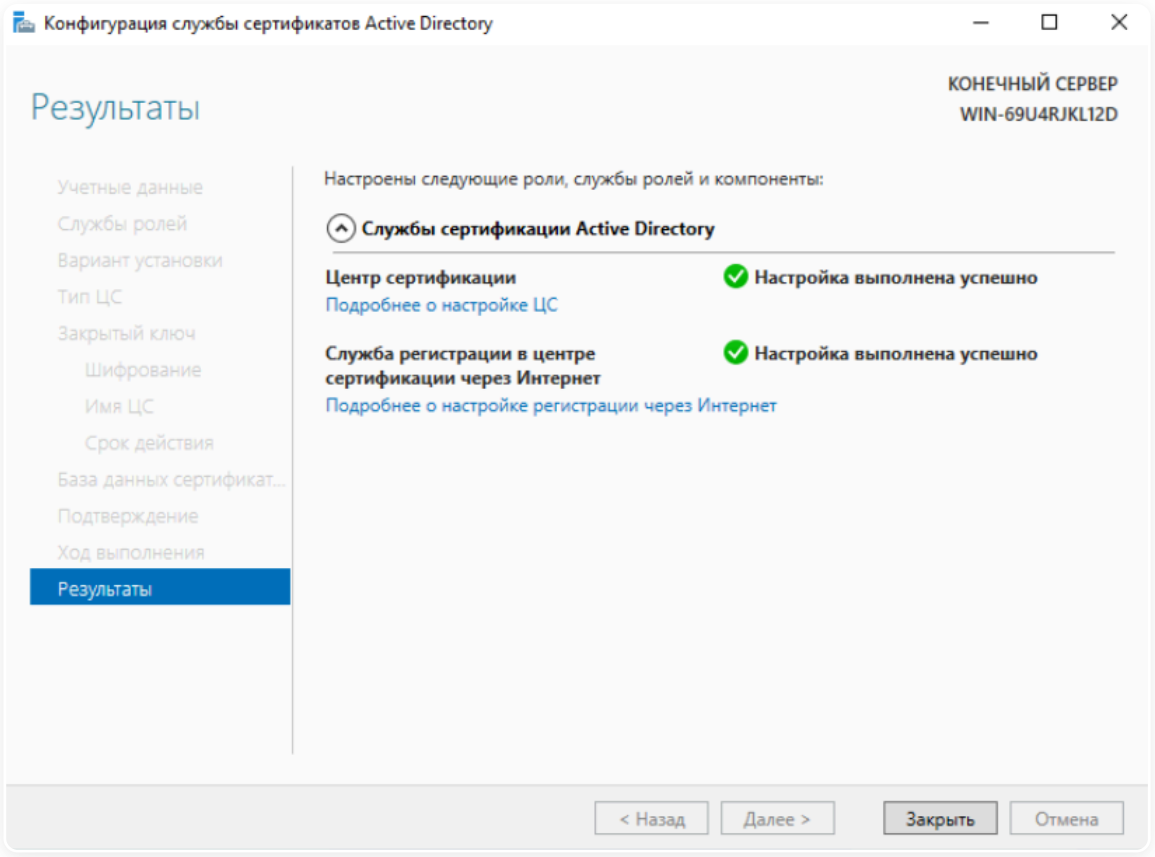
4. На этапе **Шифрование** убедитесь, что выбран алгоритм **SHA256**:



5. На этапе **Имя ЦС** задайте имя (например, `TestRootCA`):



6. Завершите настройку:



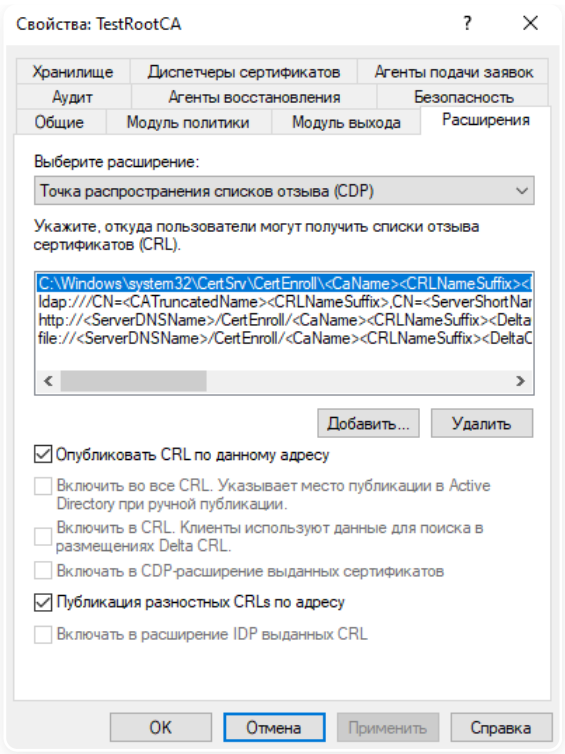
Шаг 4. Настройка точек распространения (CDP/AIA)

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**.

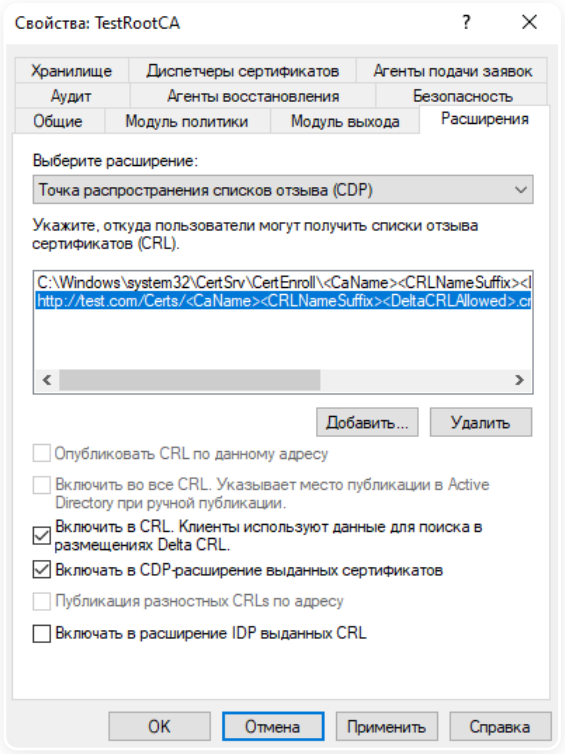
3. На вкладке **Расширения** выберите расширение **Точка распространения списков отзыва (CDP)**.

4. Удалите пути, начинающиеся с `ldap://`, `file://` и `http://`:



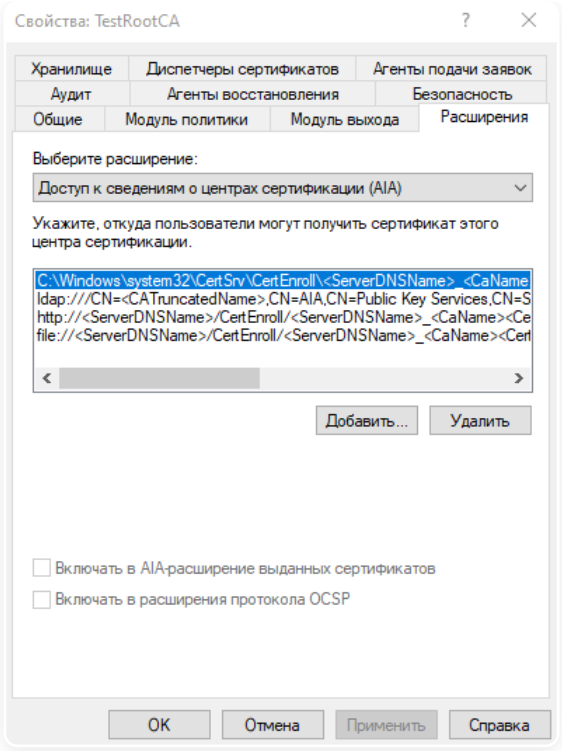
5. Нажмите **Добавить** и введите URL `http://<домен-сервера>/Certs/`. Затем добавьте переменные `<CaName>`, `<CRLNameSuffix>` и `<DeltaCRLAllowed>` после `Certs/`. Конечный путь будет выглядеть так: `http://test.com/Certs/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`.

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 → OK**.

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)

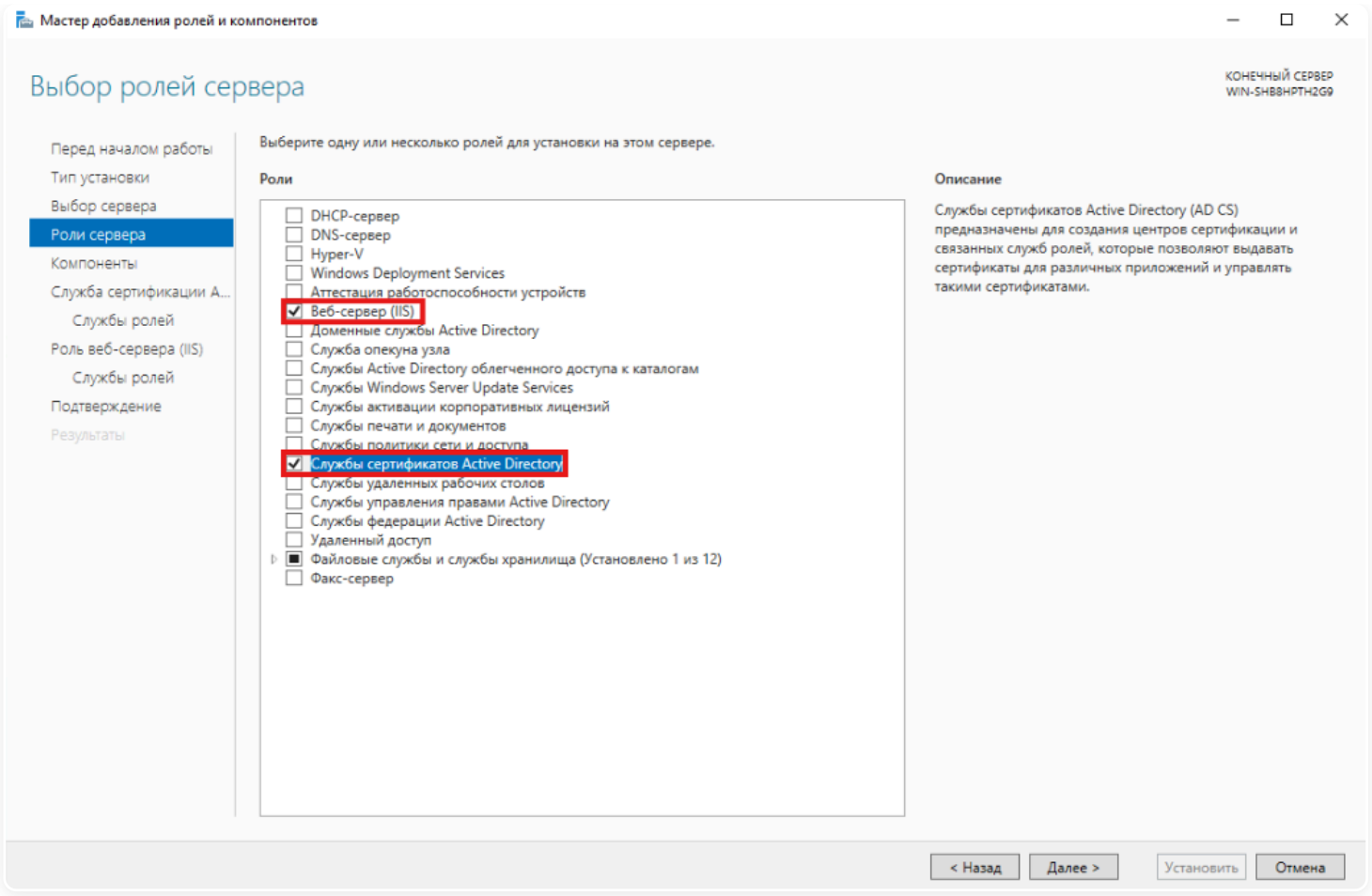
Шаг 1. Установка доверия к корню и установка ролей

На подчиненном центре сертификации (контроллере домена):

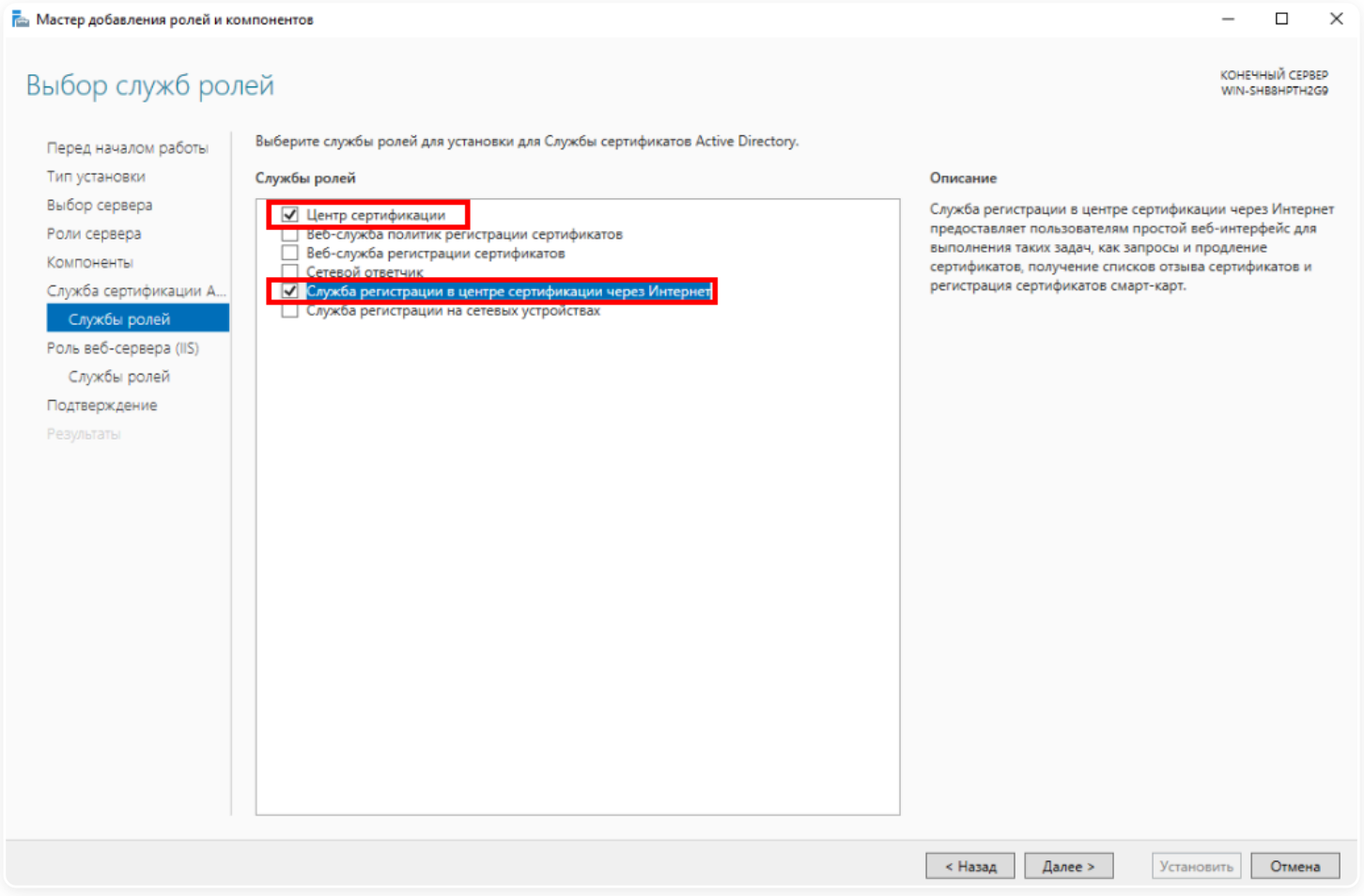
1. Установите сертификат `Root_CA.cer` в хранилище **Доверенные корневые центры сертификации** для локального компьютера.

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**:

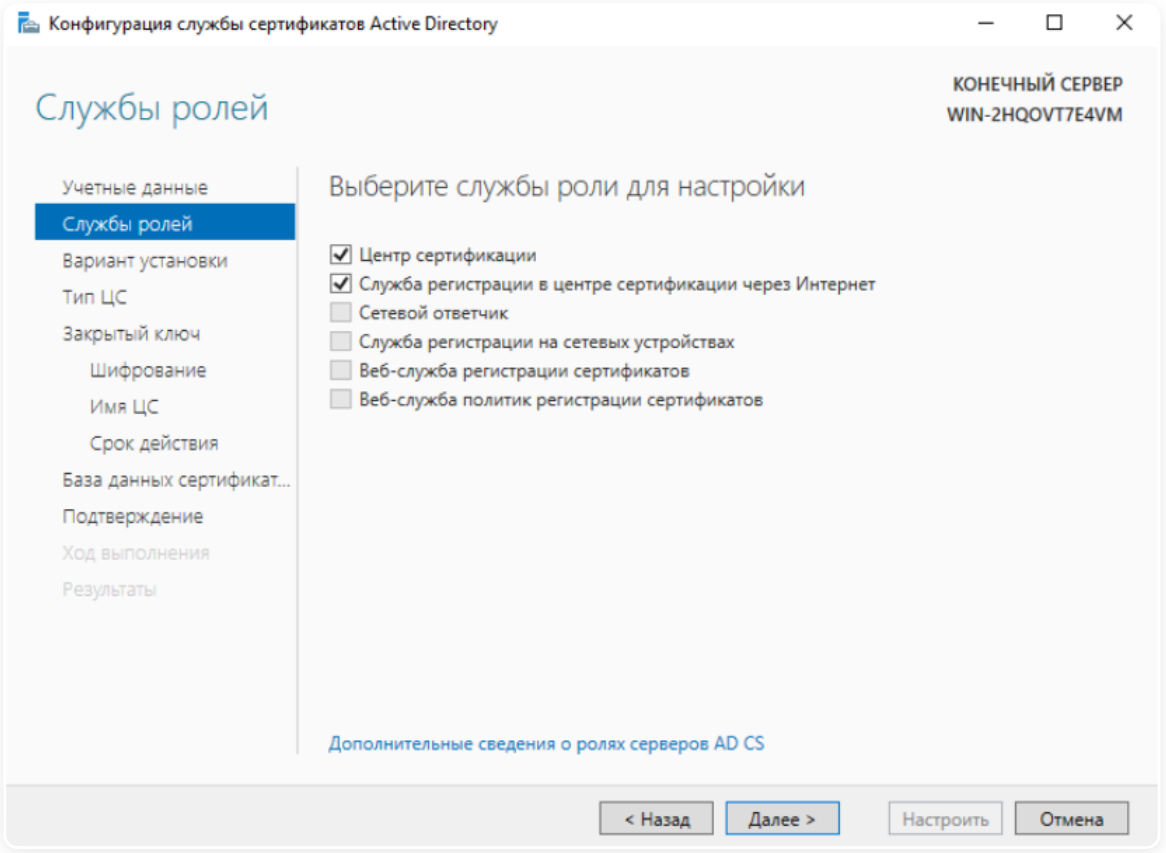


5. Завершите установку.

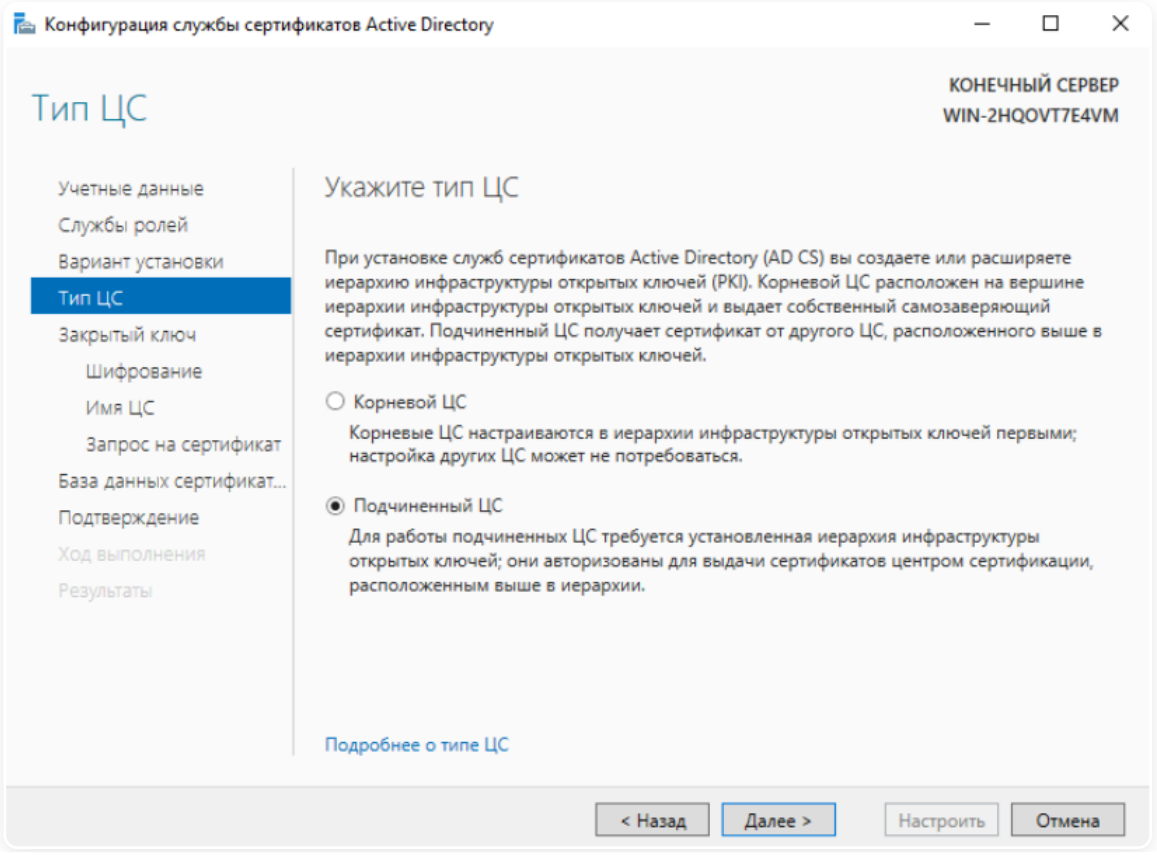
Шаг 2. Настройка подчиненного центра сертификации и создание запроса (CSR)

1. Откройте **Диспетчер серверов**, нажмите на значок уведомления и выберите **Настроить службы сертификатов Active Directory**.

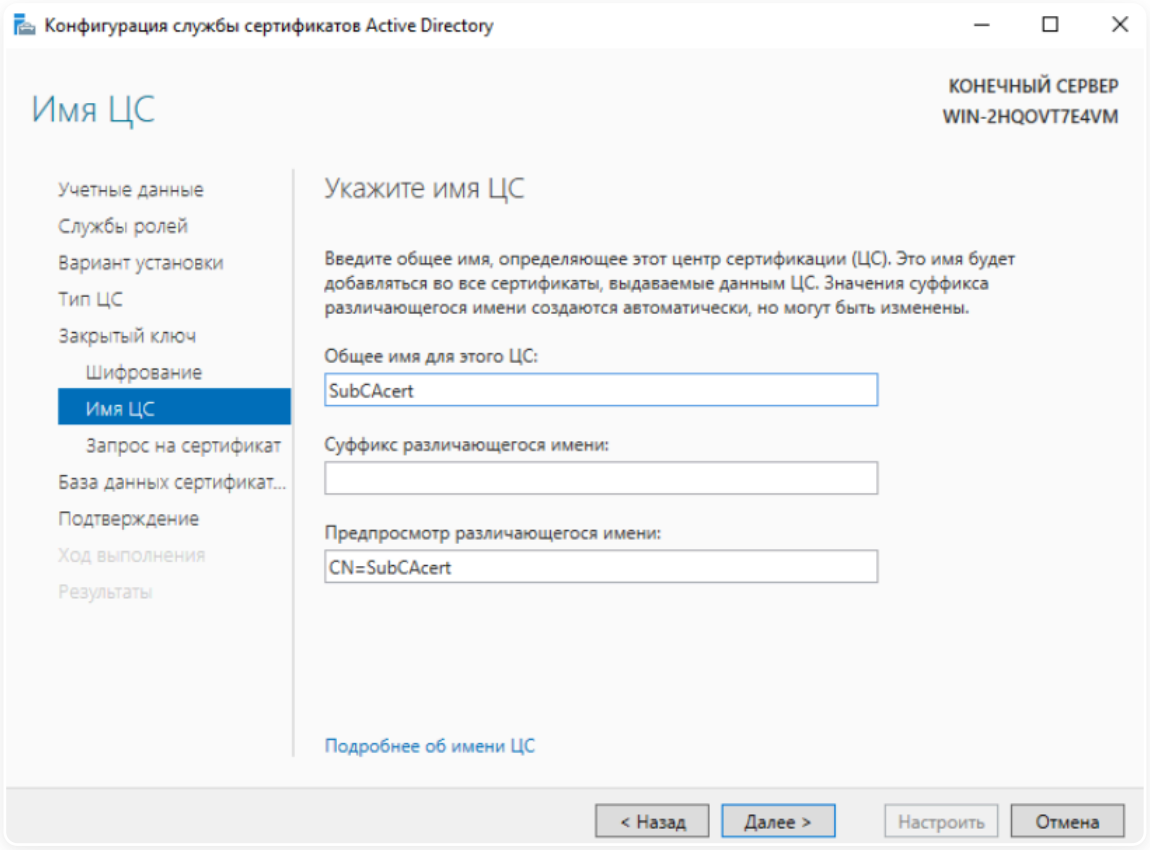
2. На этапе **Службы ролей** выберите службы **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет**:



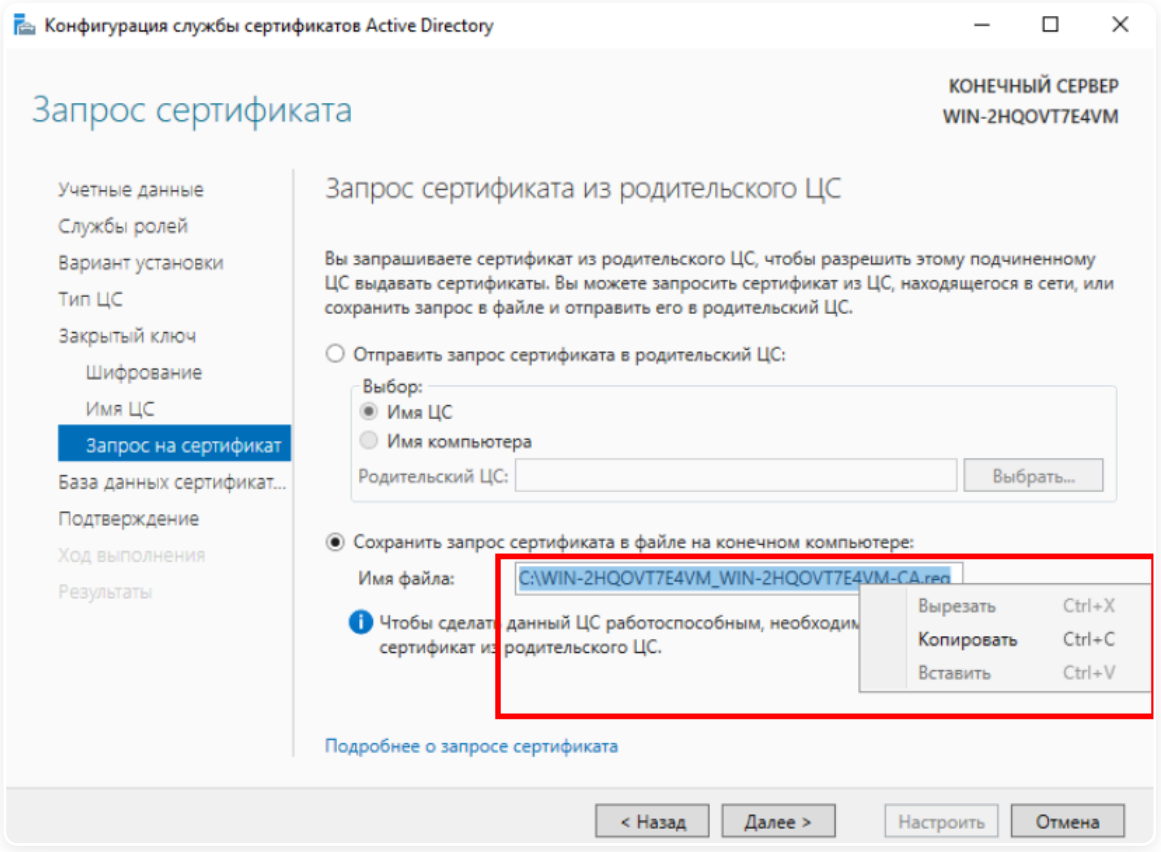
3. На этапе **Тип ЦС** выберите **Подчиненный ЦС**:



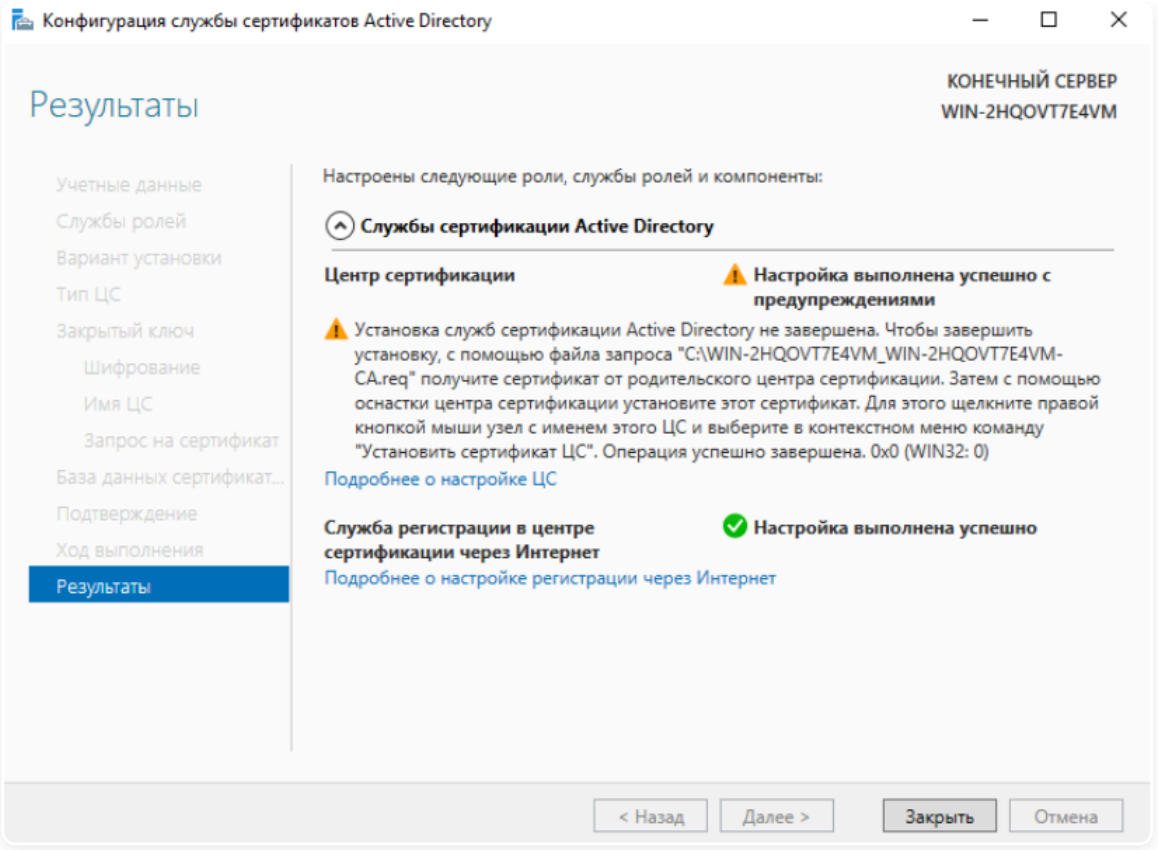
4. На этапе **Имя ЦС** задайте имя (например, `SubCAcert`):



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

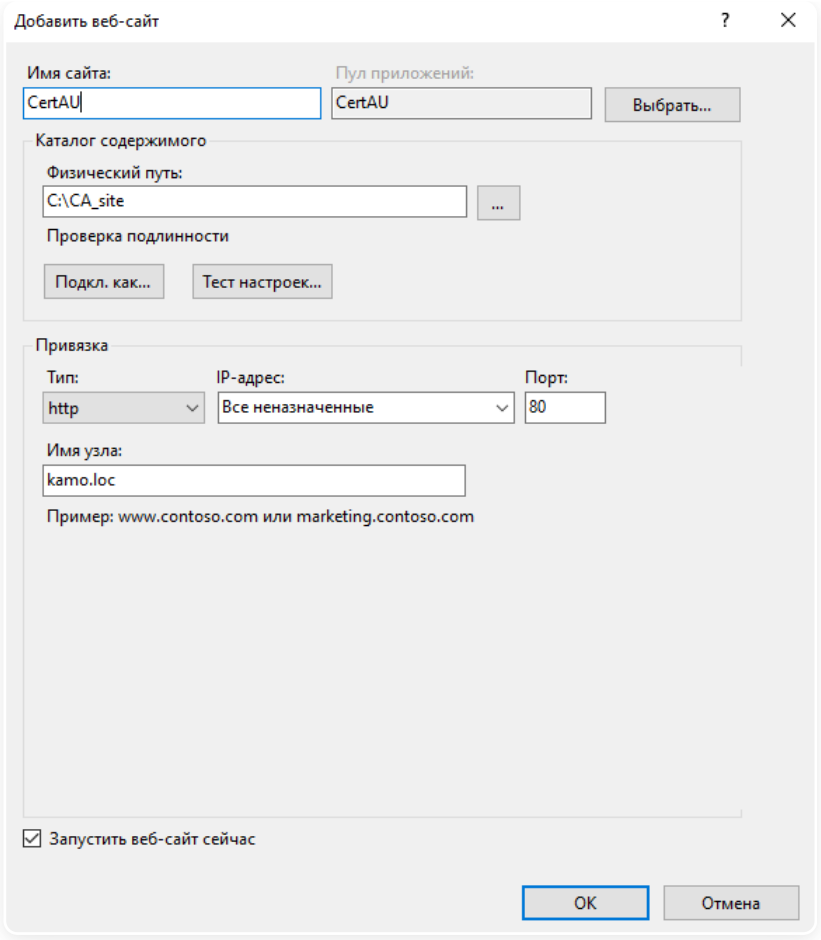
1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. На подчиненном центре сертификации нажмите правой кнопкой мыши **Установить сертификат ЦС** и выберите скачанный файл. Установите файл в папку **Доверенные корневые центры сертификации**.

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

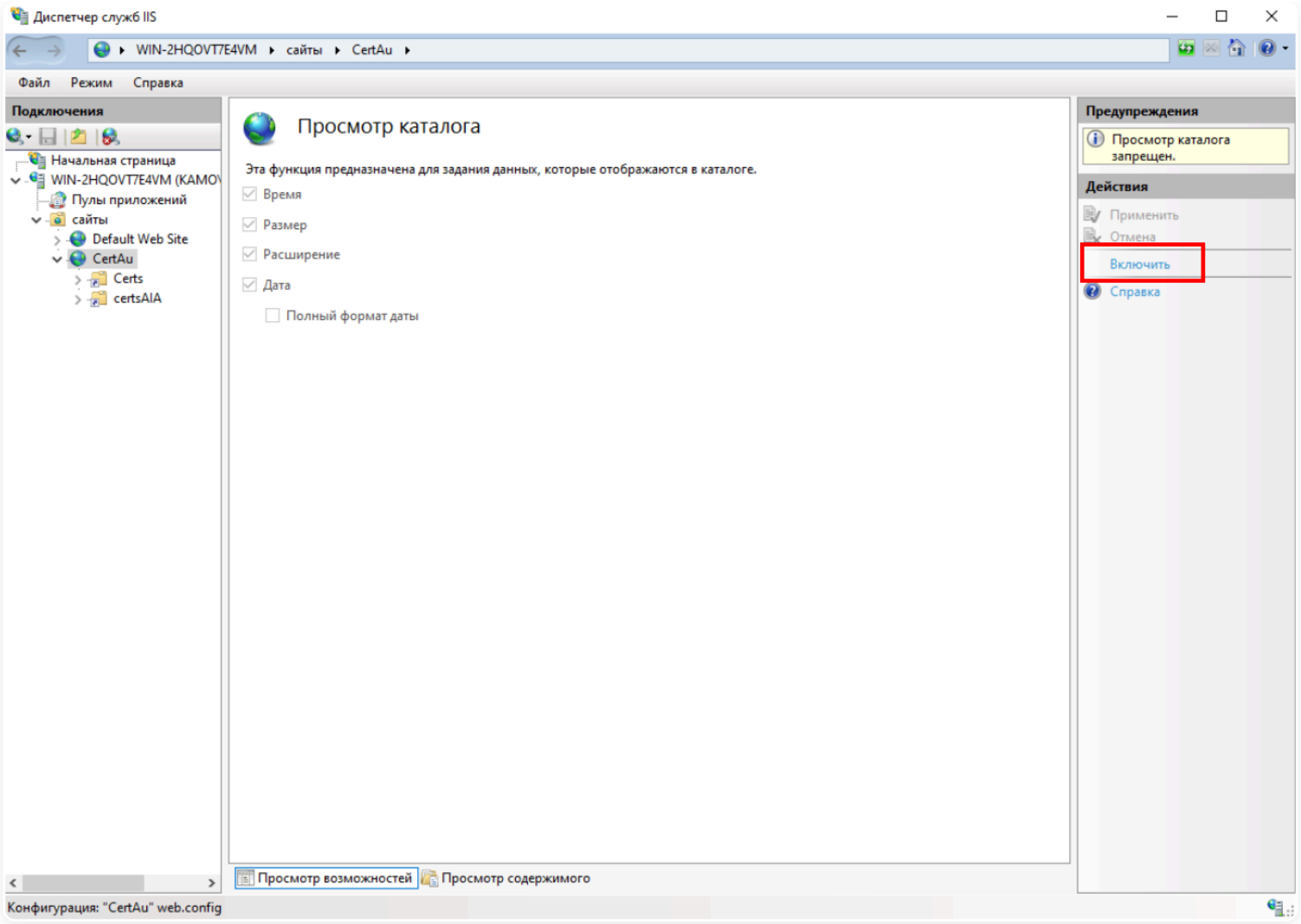
1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Диспетчер служб IIS**.

2. Нажмите правой кнопкой мыши по узлу сервера, выберите **Добавить веб-сайт** и заполните поля:

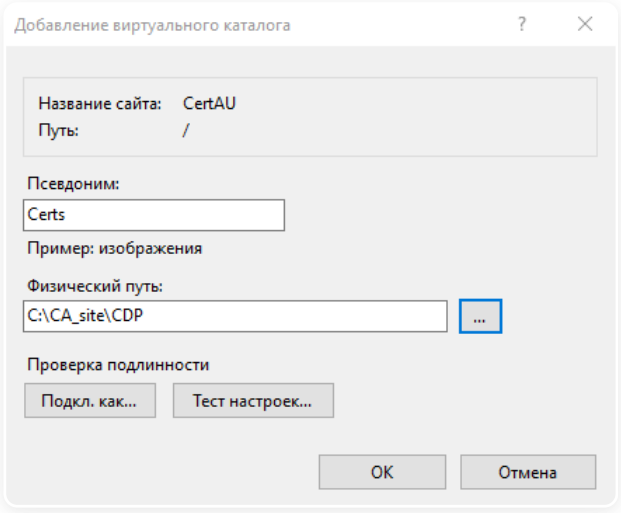


- **Имя сайта** - введите `CertAU`.
- **Физический путь** - создайте новую папку `CA_site` по пути `C:\CA_site`.
- **Имя узла** - укажите доменное имя, по которому будет доступен сайт, например, `marketing.contoso.com`.

3. После добавления веб-сайта перейдите в раздел **Просмотр каталогов** и нажимите **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:

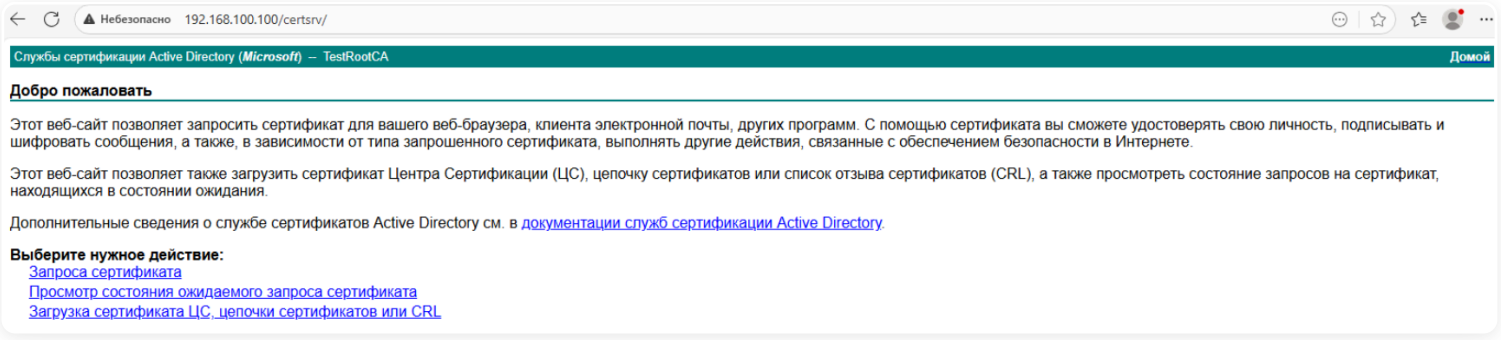
- Для CDP: **Включить в CRL** и **Включать в CDP-расширение выданных сертификатов**.
- Для AIA: **Включать в AIA-расширение выданных сертификатов**.

Шаг 6. Получение сертификата от корневого центра сертификации

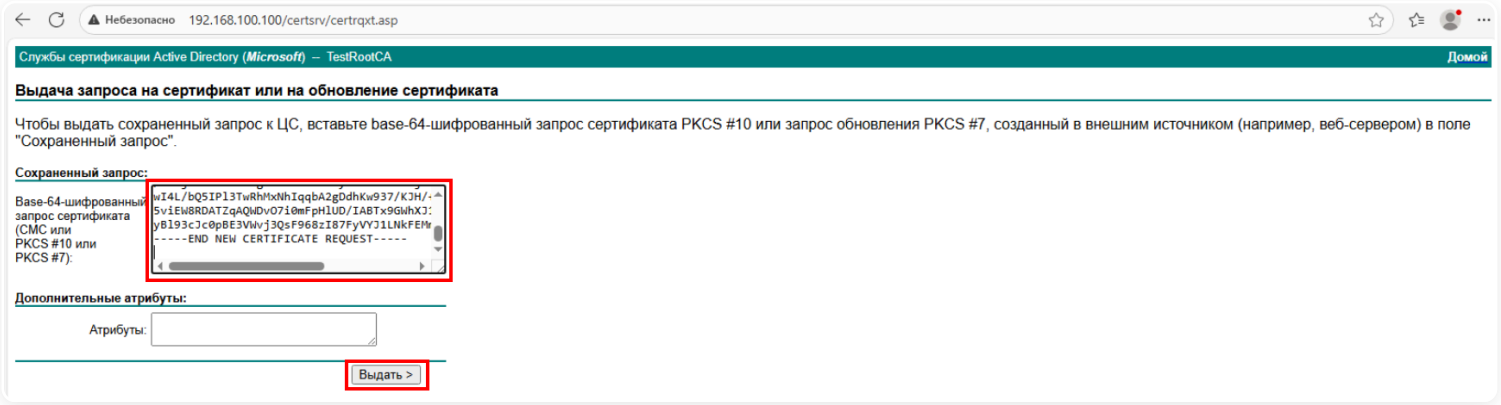
1. Откройте файл `.req` в блокноте и скопируйте текст.

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.

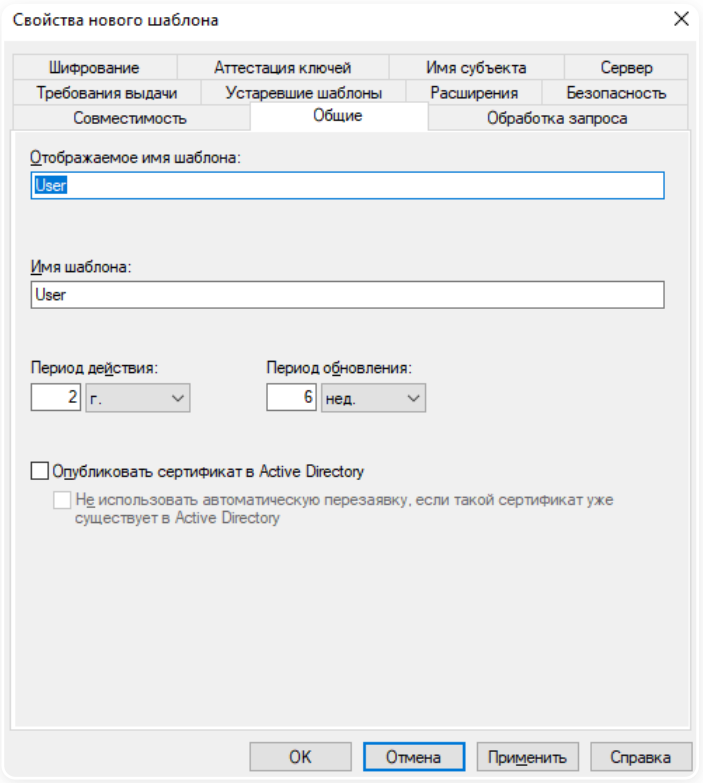
Создание шаблона сертификата и тестовая выдача

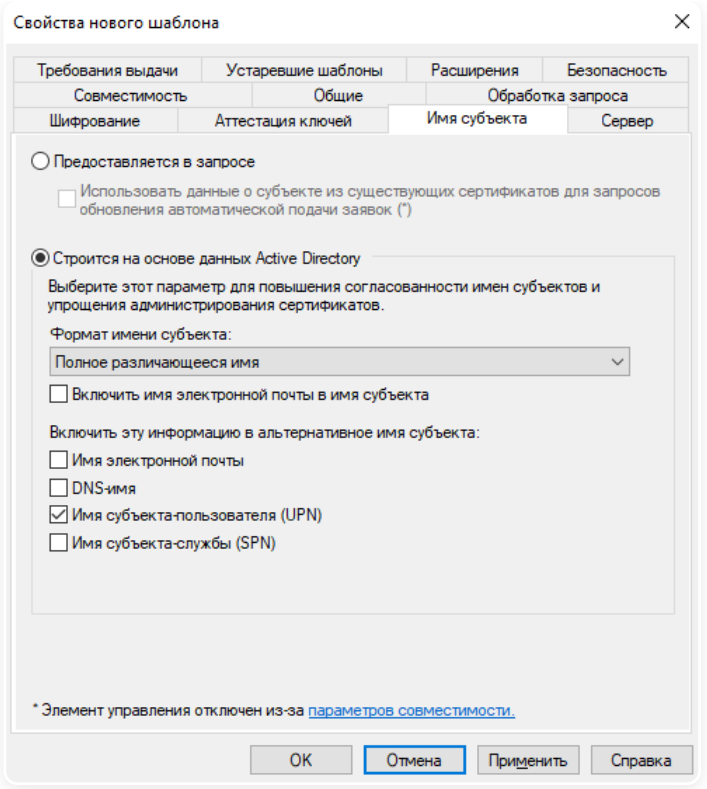
Шаг 1. Создание шаблона сертификата

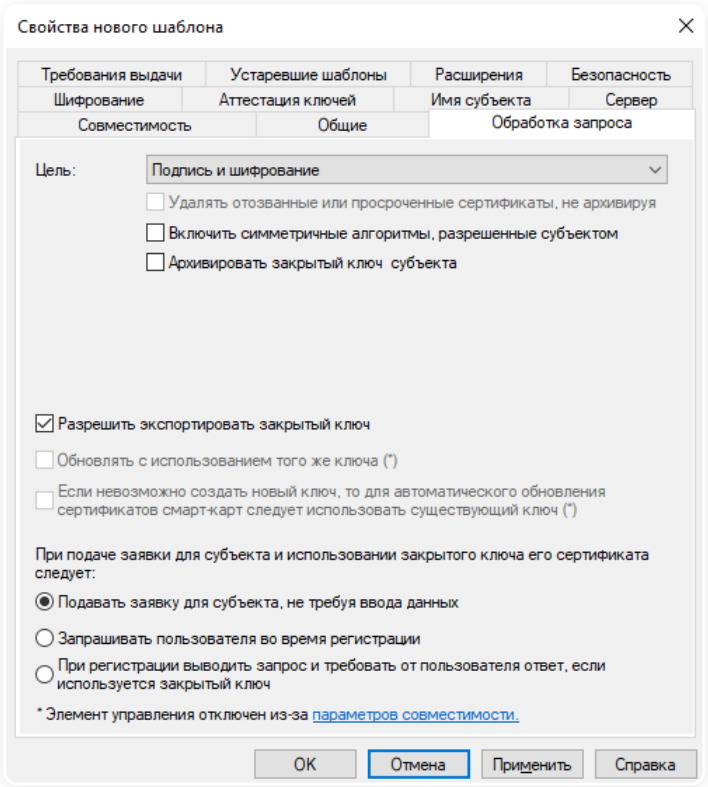
1. Откройте **Диспетчер серверов** и перейдите в **Средства** → **Центр сертификации**. Нажмите правой кнопкой мыши на папку **Шаблоны сертификатов** и выберите **Управление**.

2. Найдите шаблон **Пользователь**, нажмите правой кнопкой мыши и выберите **Скопировать шаблон**.

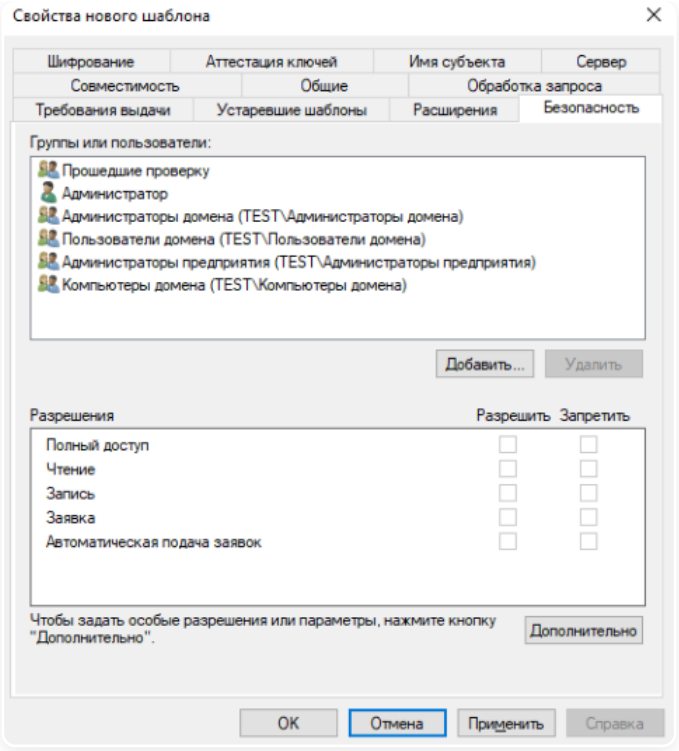
3. Настройте шаблон в соответствии с вашими требованиями (имя, срок действия, криптопровайдеры и так далее):







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**.

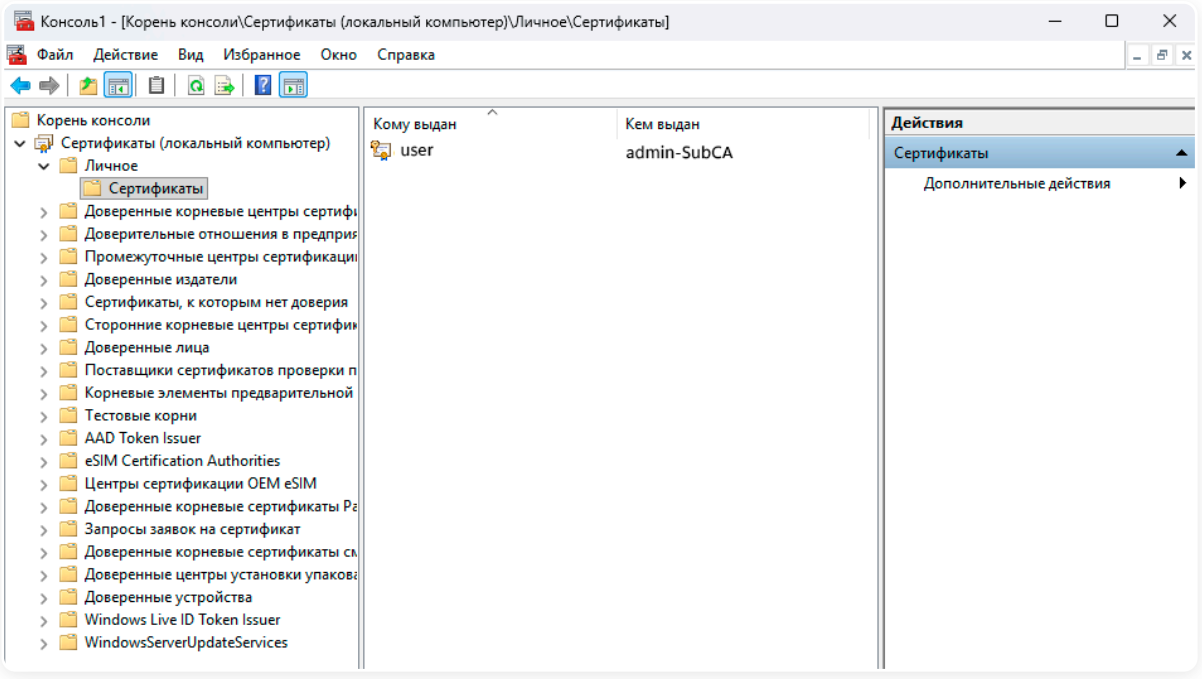
4. Выберите **Сертификаты** и нажмите **Добавить**.

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:



Настройка Wi-Fi-сети

В текущей версии Ideco NGFW 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. Способ авторизации зависит от режима работы маршрутизатора.

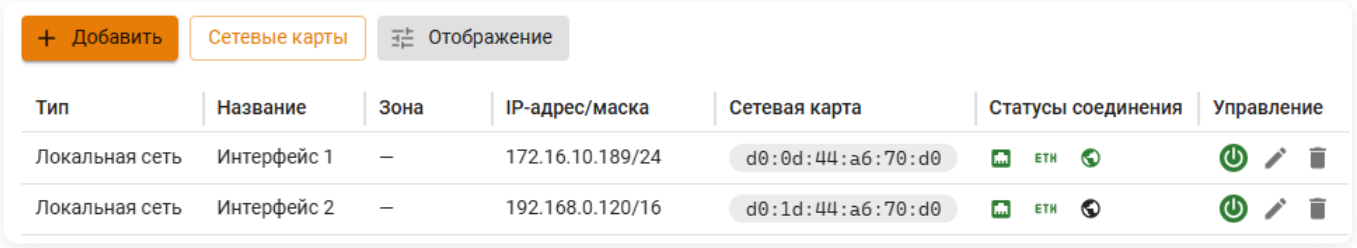
Режим точки доступа или bridge

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 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 и укажите 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, то в **Файрволе** запретите доступ из беспроводной сети в локальную сеть.

Пример настройки интерфейса для клиентов, подключающихся по Wi-Fi:



- **172.16.10.189/24** - шлюз для беспроводной Wi-Fi-сети.
- **192.168.0.120/16** - шлюз для локальной Ethernet-сети.

Настройка DHCP

1. В **Сервисы** → **Сетевые интерфейсы** создайте отдельный интерфейс для клиентов Wi-Fi с автоматической конфигурацией через 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**.

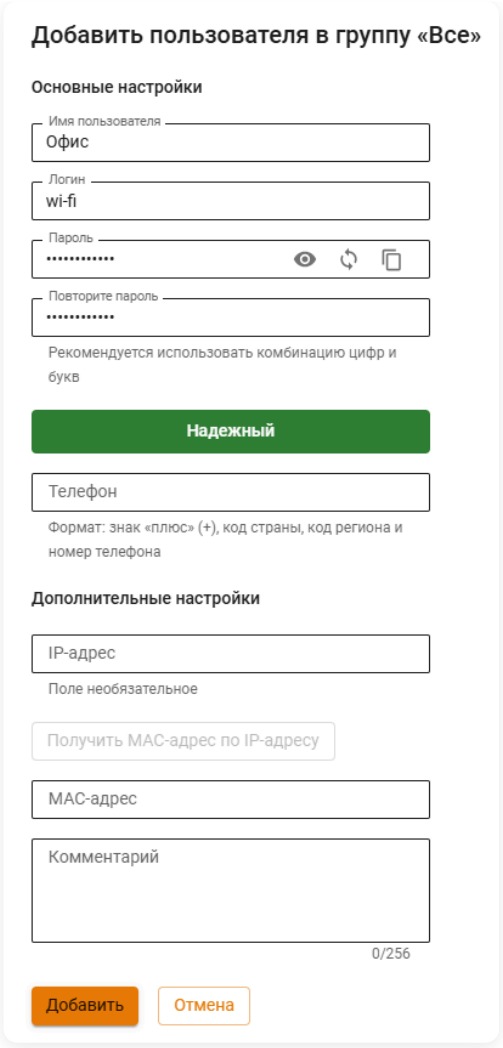
Для индивидуальной авторизации Wi-Fi-пользователей и учета их трафика и статистики воспользуйтесь авторизацией через веб-браузер. При таком способе авторизации Ideco NGFW будет учитывать каждого пользователя, подключившегося по Wi-Fi. Это следует принять во внимание при планировании лицензирования Ideco NGFW.

Режим роутера

В режиме роутера устройство Wi-Fi скрывает за NAT устройства беспроводной сети. Таким образом, для Ideco NGFW 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 авторизация**.

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, поскольку 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 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.

Подключение к Ideco NGFW по COM-порту

Установка Ideco NGFW по COM-порту

COM-порт по умолчанию включен.

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

Шаг 1. Создание загрузочного USB-накопителя

Создайте загрузочный USB-накопитель Ideco NGFW. 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, если опция **Console Redirection** отсутствует в BIOS или выключена.
> - Процесс загрузки сервера, начиная с BIOS и заканчивая установщиком Ideco NGFW, если опция **Console Redirection** включена.

2. Выполните установку Ideco NGFW.

Управление Ideco NGFW 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 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**

Анализ трафика

Используйте утилиту `tcpdump` для анализа трафика на NGFW в разделе **Управление сервером → Терминал**.

Утилита `tcpdump` предустановлена в продукт Ideco NGFW.

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 его 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

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:

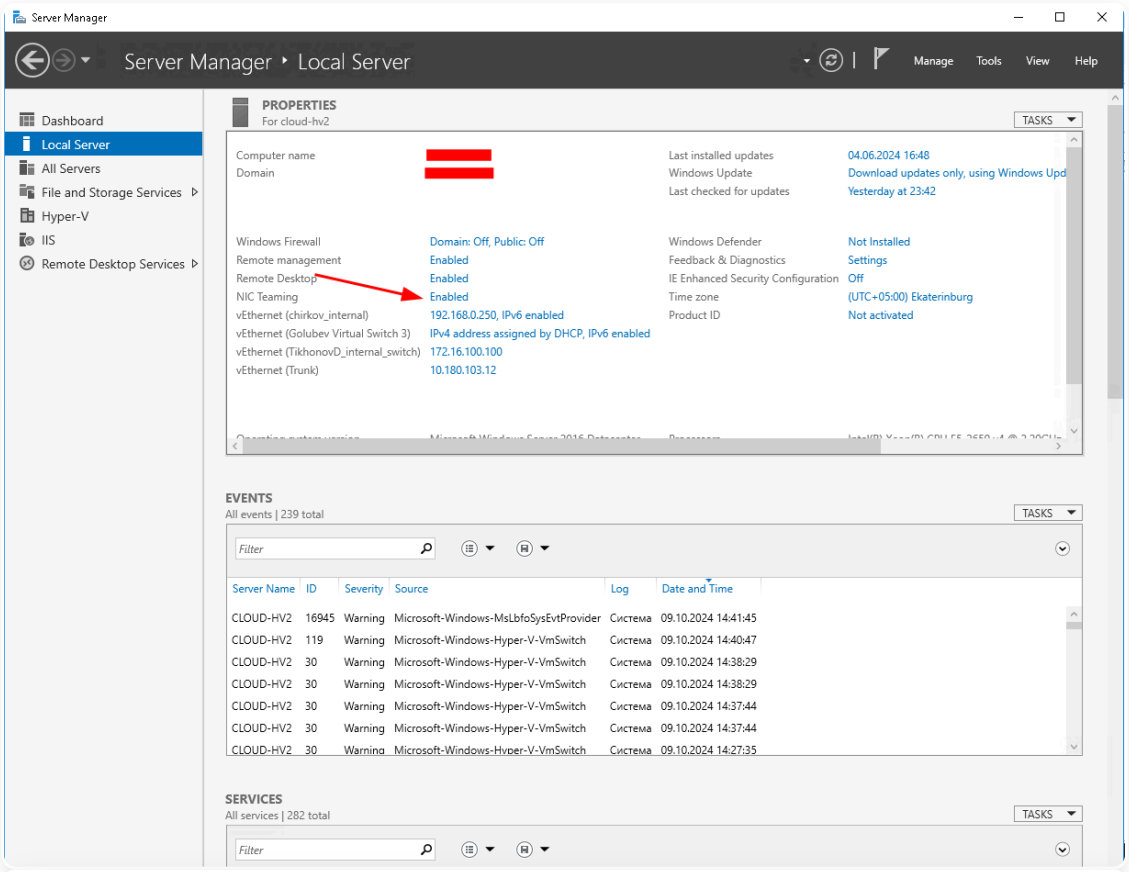
```
tcpdump -i any port 500
```

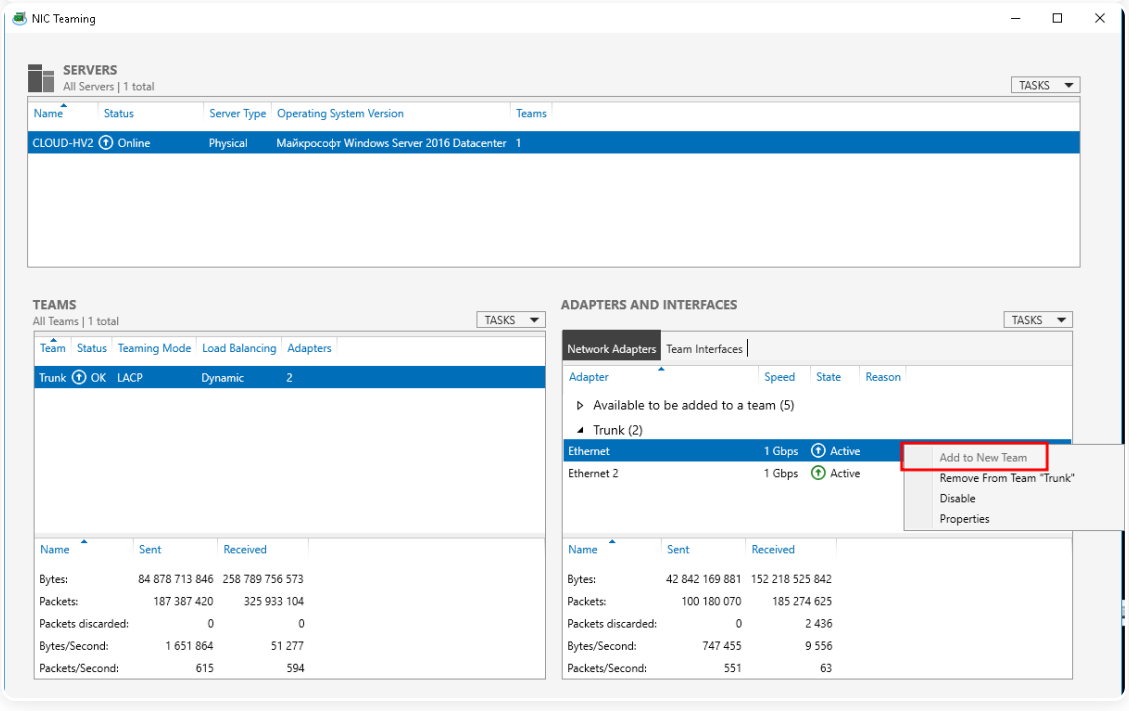
Настройка LACP на Hyper-V

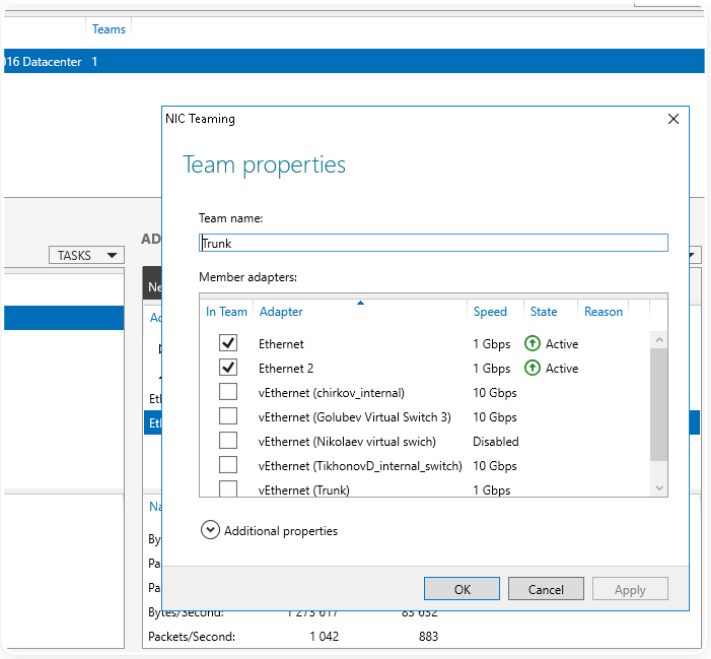
Для настройки LACP на гипервизоре Hyper-V существуют два способа:

Настройка на хост системе

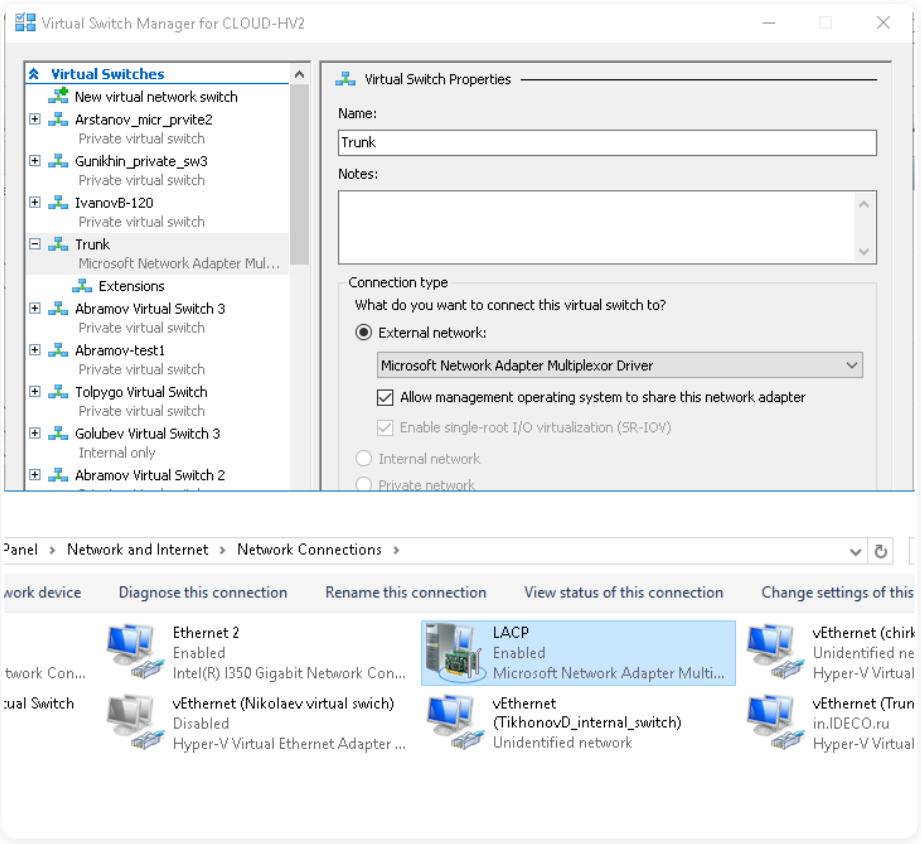
1. Объедините физические интерфейсы:







2. Выберите созданный интерфейс при настройке виртуального свитча:



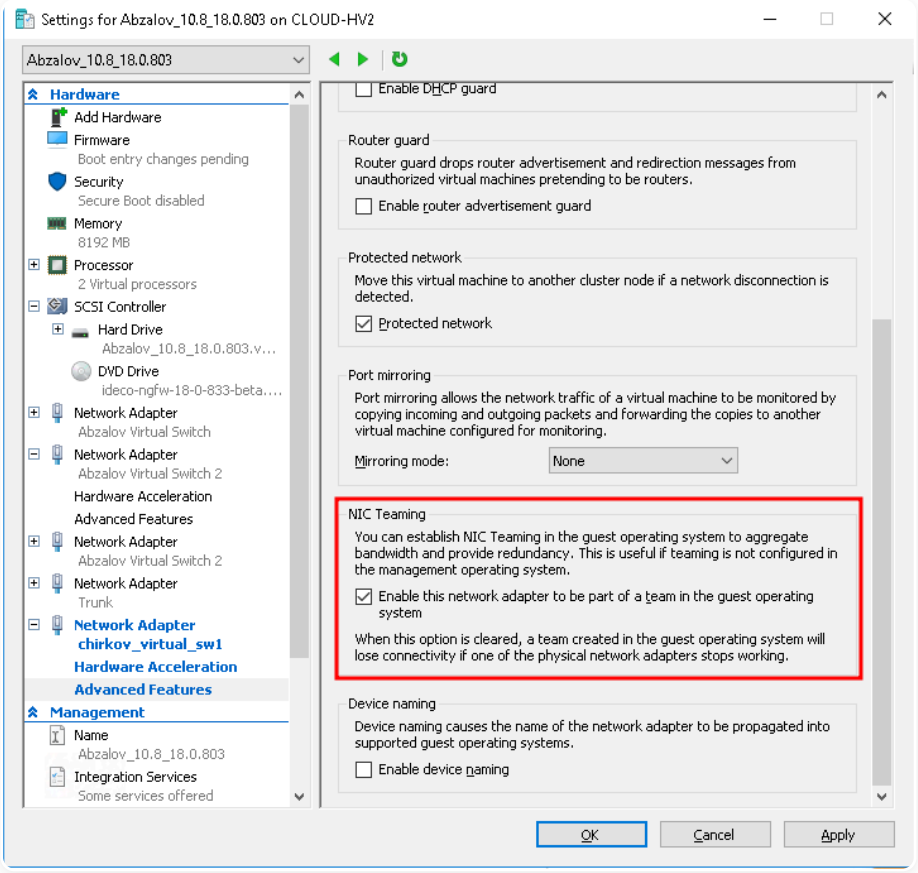
Получившийся виртуальный свитч можно использовать для добавления новых интерфейсов в LACP на гостевую систему.

3. Настройте подключение на вкладке **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 разделе **Сетевые интерфейсы → Агрегированные(LACP)**.

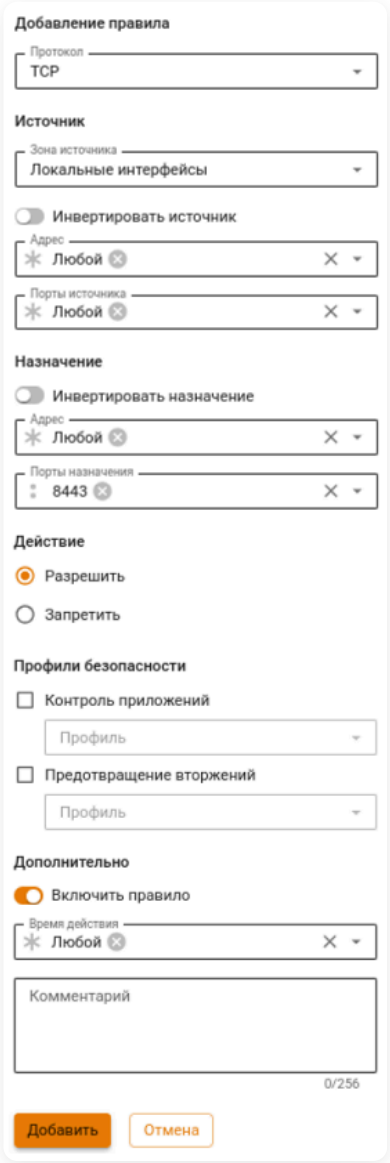
4. Настройте подключения на вкладке **Сетевые интерфейсы → Внешние и локальные**.

Как разрешить доступ к ресурсам в ограниченной сети

Разрешить доступ к веб-интерфейсу Ideco NGFW из локальной сети

Пример. Необходимо ограничить доступ ко всем внутренним ресурсам Ideco NGFW, кроме веб-интерфейса администратора Ideco NGFW.

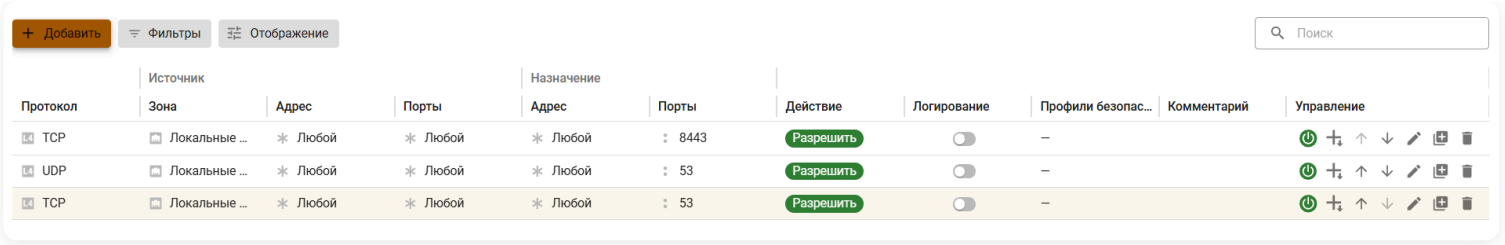
1. В разделе **Правила трафика** → **Файрвол** → **INPUT** создайте разрешающее правило, заполнив поля:



- **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.
- **Порт** - 8443.

Включите правило и нажмите **Добавить**.

2. Если Ideco NGFW 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:



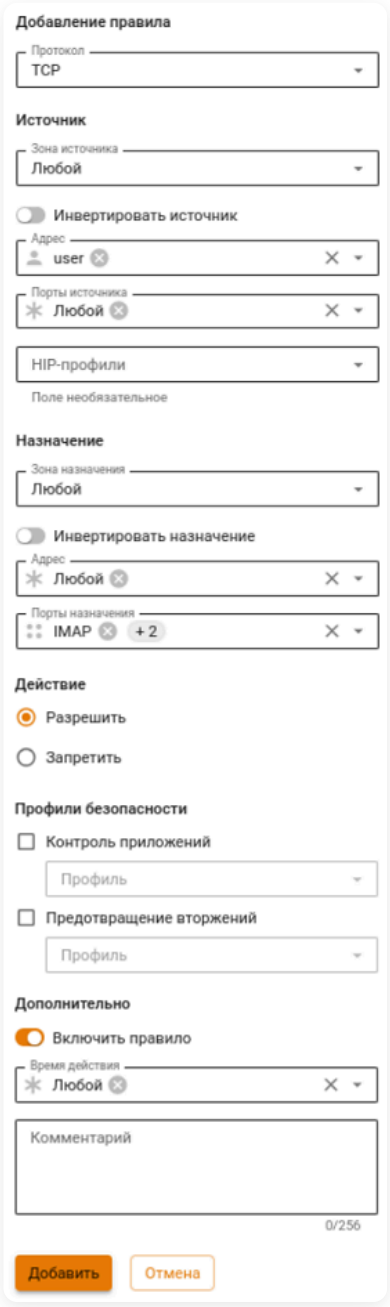
3. Создайте запрещающее весь трафик правило INPUT. При создании правила доступна опция **Включить правило** в разделе **Дополнительно**. Не включайте его, пока не убедитесь, что в таблице разрешающее правило находится выше запрещающего.

При потере доступа к веб-интерфейсу Ideco NGFW воспользуйтесь опцией **Включить режим 'Разрешить интернет всем'**.

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 разделе **Правила трафика** → **Файрвол** → **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 и их защищенных версий).

Включите правило и нажмите **Добавить**.

2. Создайте запрещающее весь трафик правило FORWARD. В таблице поместите разрешающее правило выше запрещающего.

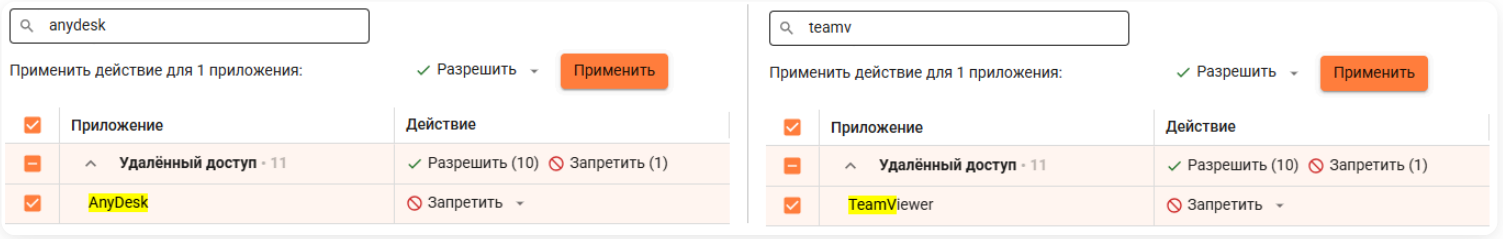
Разрешить трафик из локальной во внешнюю сеть, но запретить конкретные приложения

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.

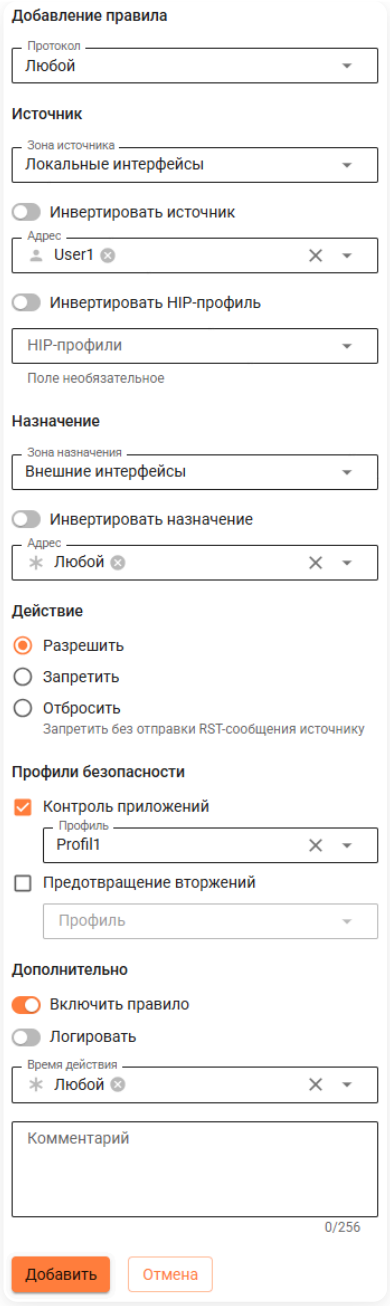
> Для успешного запрета доступа к приложениям удаленного доступа AnyDesk и TeamViewer до настройки на NGFW необходимо полностью удалить данные об этих приложениях в системе, если они запускались пользователями ранее.

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** → **Файрвол** → **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`:

Добавление правила

Протокол
Любой

Источник

Зона источника
Исходящий трафик устройства

Инвертировать источник

Адрес
Любой

Инвертировать HIP-профиль

HIP-профили

Поле необязательное

Назначение

Зона назначения
Любой

Инвертировать назначение

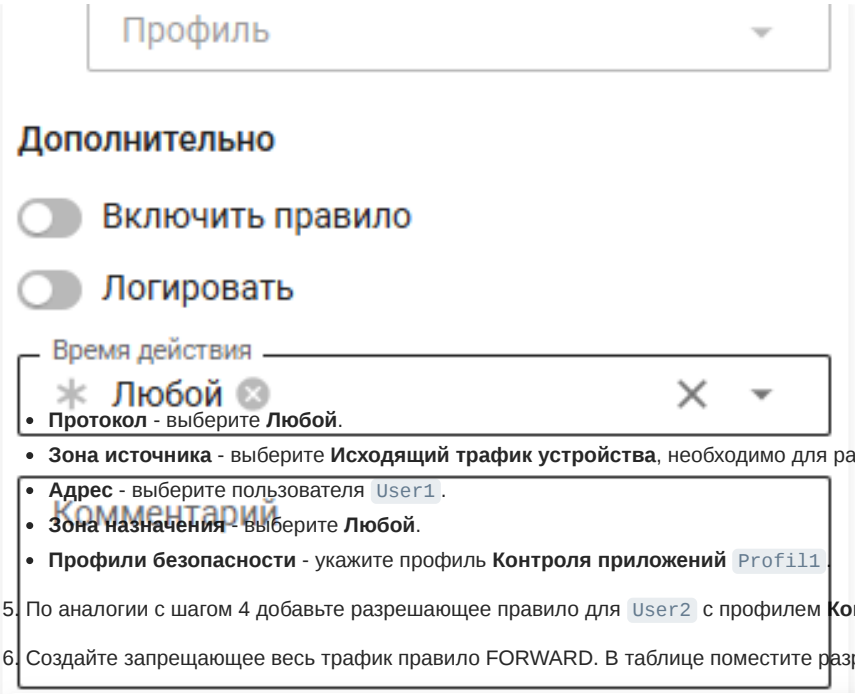
Адрес
User1

Действие

- (•) Разрешить
- ( ) Запретить
- ( ) Отбросить
  Запретить без отправки RST-сообщения источнику

Профили безопасности

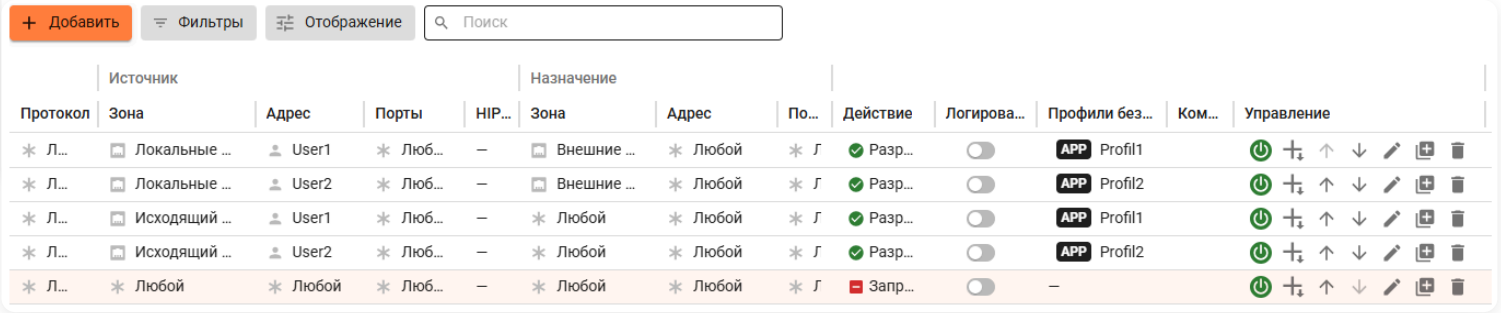
- [x] Контроль приложений
  Профиль
  Profil1
- [ ] Предотвращение вторжений



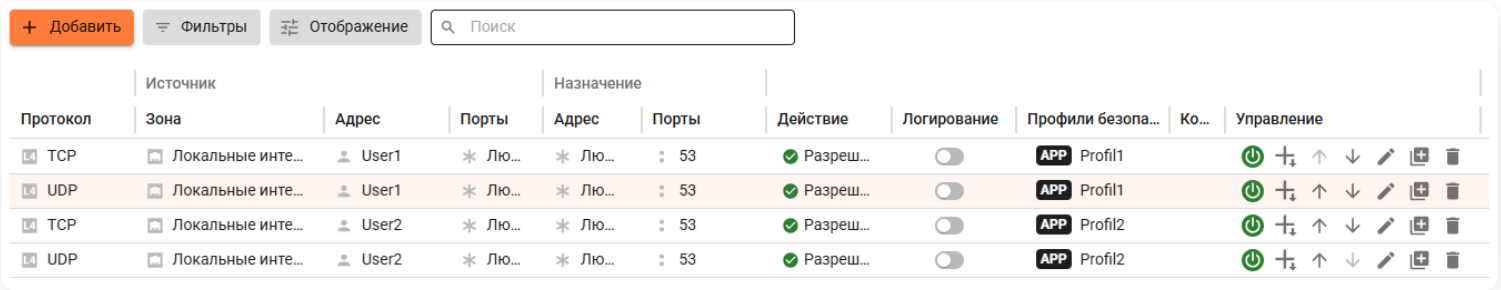
- **Протокол** - выберите **Любой**.
- **Зона источника** - выберите **Исходящий трафик устройства**, необходимо для работы прямого и прозрачного прокси, веб-трафика.
- **Адрес** - выберите пользователя `User1`.
- **Зона назначения** - выберите **Любой**.
- **Профили безопасности** - укажите профиль **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** → **Защита и управление 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:



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 раздел **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 **Администратора** и его пароль.

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 разделе **Управление сервером** → **Администраторы**. Для доступа введите внешний IP-адрес Ideco NGFW и порт 8443.

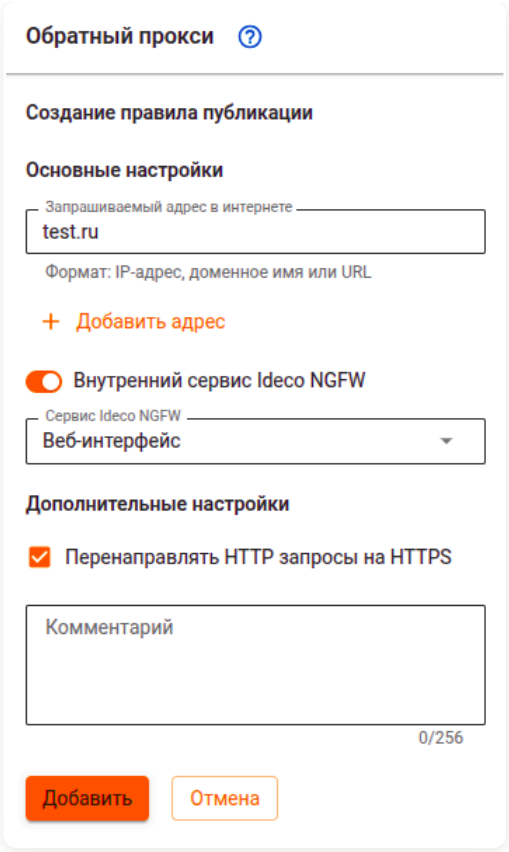
Доступ по VPN:

- 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 раздел **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**.

Тестирование оперативной памяти сервера

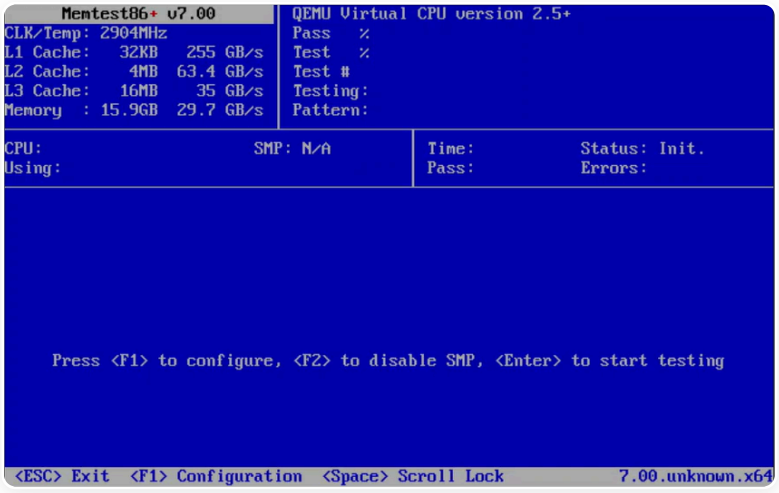
Для нормальной работы сервера все его аппаратные компоненты должны функционировать исправно.
Тестирование памяти помогает выявить и исключить проблемы с оперативной памятью сервера при поиске неисправностей.

При загрузке GRUB используйте Memtest86+ для тестирования оперативной памяти.
Для запуска тестирования выполните действия:

1. При загрузке сервера выберите **Memory test**:



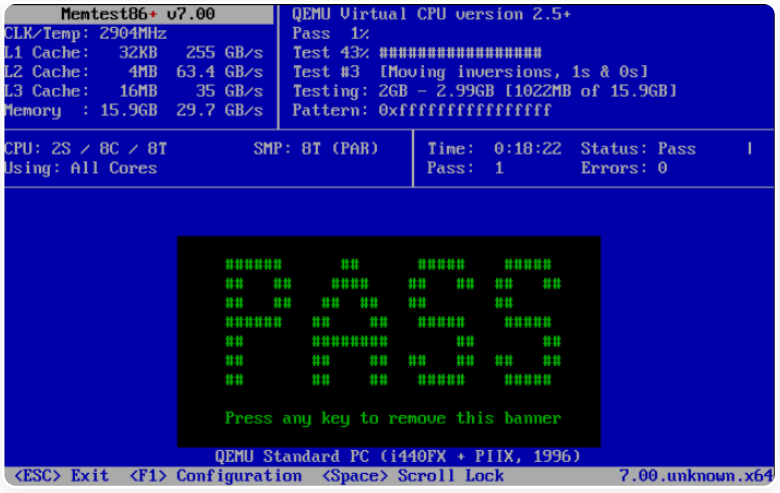
2. Нажмите **Enter** или подождите 5 секунд для автоматического запуска тестирования:



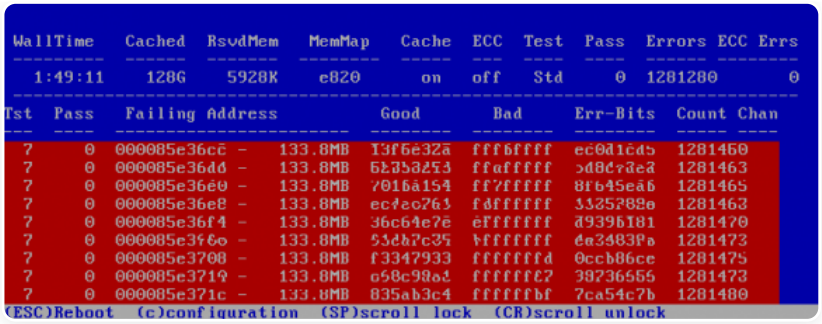
Для выбора режима диагностики **Fail-Safe Mode** нажмите **F1**.

Для выбора режима диагностики **Multi-Threading(SMP)** нажмите **F2**.

- Если появится запись **PASS**, тесты памяти пройдены успешно:



- При ошибке памяти появится запись вида:


WallTime Cached RsvdMem MemMap Cache ECC Test Pass Errors ECC Errs
1:49:11 128G 5928K e820 on off Std 0 1281280 0
Tst Pass Failing Address Good Bad Err-Bits Count Chan
7 0 000085e36cc - 133.8MB 13f6e32a fffbffff ec0d1cd5 1281460
7 0 000085e36dd - 133.8MB 6b3b3d53 ffaffffff 3d8c7ded 1281463
7 0 000085e36e0 - 133.8MB 7016a154 ff7fffff 8f645ea6 1281465
7 0 000085e36e8 - 133.8MB ec7ec763 fdffffff 3335788e 1281463
7 0 000085e36f4 - 133.8MB 36c64e7e efffffff d939b181 1281470
7 0 000085e3f6c - 133.8MB 53db7c35 bfffffff 6a3483fa 1281473
7 0 000085e3708 - 133.8MB f3347933 fffffffd 0ccb86ce 1281475
7 0 000085e3719 - 133.8MB a58c98a2 ffffffc7 38736555 1281473
7 0 000085e371c - 133.8MB 835ab3c4 ffffffbf 7ca54c7b 1281480
(ESC)Reboot (c)configuration (SP)scroll lock (CR)scroll unlock

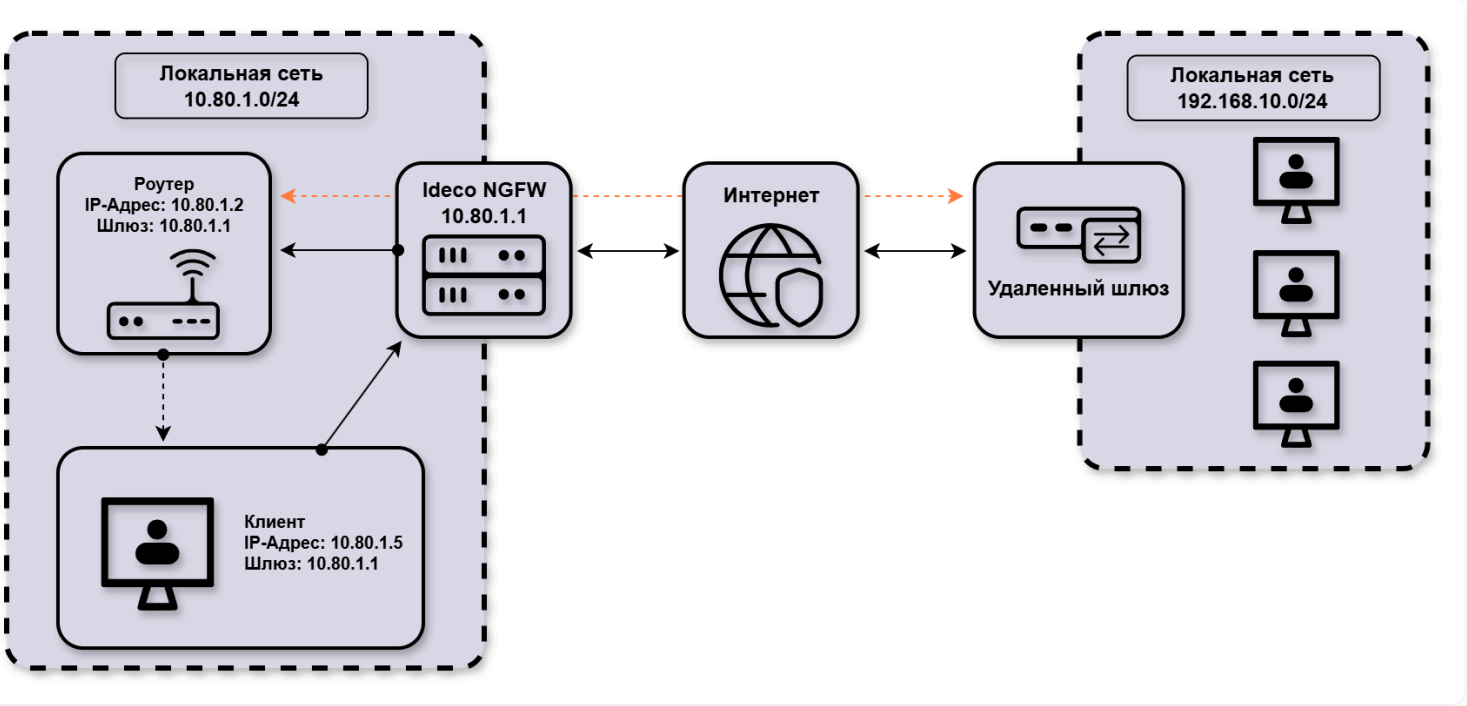
Как избавиться от асимметричной маршрутизации трафика

При попытке настроить доступ в удаленные сети через роутер 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 используется роутер, устанавливающий связь с другими сетями. NGFW - шлюз по умолчанию для клиентов сети. Требуется настроить маршрутизацию на NGFW так, чтобы клиенты сети `10.80.1.0/24` получали доступ в удаленную сеть `192.168.10.0/24` и обратно через роутер.

Асимметричная маршрутизация при наличии роутера в локальной сети

Неправильная топология сети, способствующая асимметричной маршрутизации:

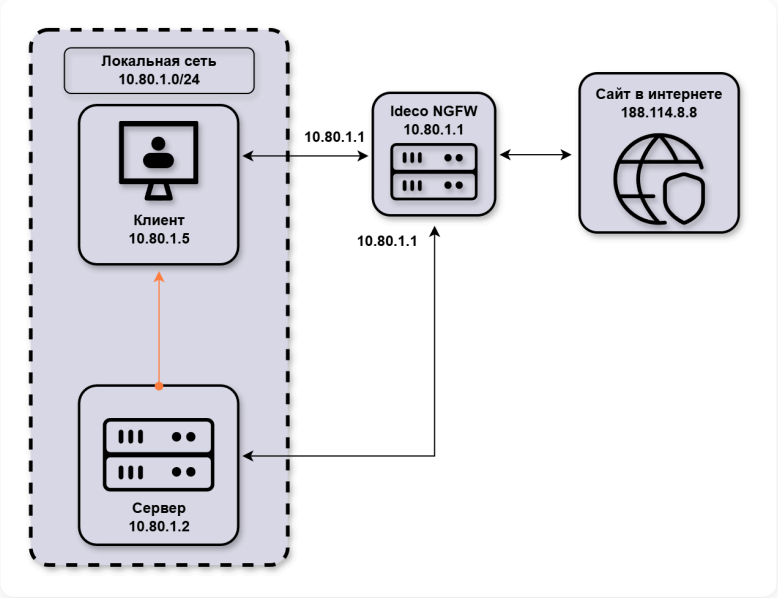


- `10.80.1.1` - шлюз для локальной сети `10.80.1.0/24`.
- `10.80.1.2` - роутер, имеющий доступ в удаленную сеть `192.168.10.0/24`.
- `10.80.1.5` - адрес хоста в локальной сети.
- **Оранжевая стрелка** - двусторонняя связь роутера с удаленным шлюзом или роутером, обеспечивающая доступ к удаленной сети `192.168.10.0/24` (туннель к шлюзу, маршрут до роутера 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 (`10.80.1.1`) и роутер (`10.80.1.2`).
- **Пунктирная стрелка** - трафик, который роутер возвращает хостам локальной сети в обход NGFW, поэтому хосты этот трафик обратно не принимают.

Часть трафика от клиентов до роутера идет через шлюз, а часть - непосредственно от роутера до абонентов сети. Разная маршрутизация на разных участках делает прохождение пакетов между двумя локальными сетями невозможной.

Асимметричная маршрутизация при публикации сайтов через DNAT

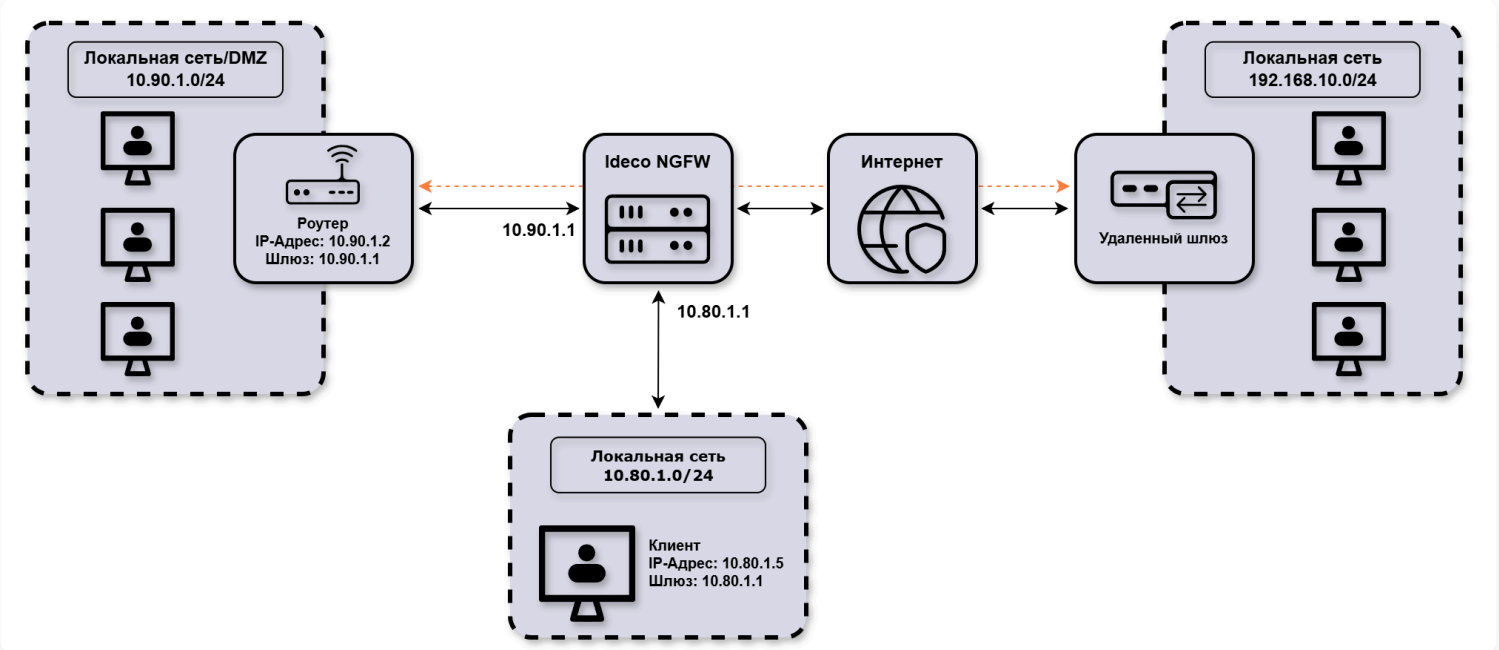
Асимметричная маршрутизация также возникает, когда в одной локальной сети находится хост и сервер, на котором расположен опубликованный при помощи DNAT-правила ресурс:



- `10.80.1.1` - адрес Ideco NGFW 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 сайта в интернете.
- **Оранжевая стрелка** - ответ напрямую от сервера хосту в локальной сети.

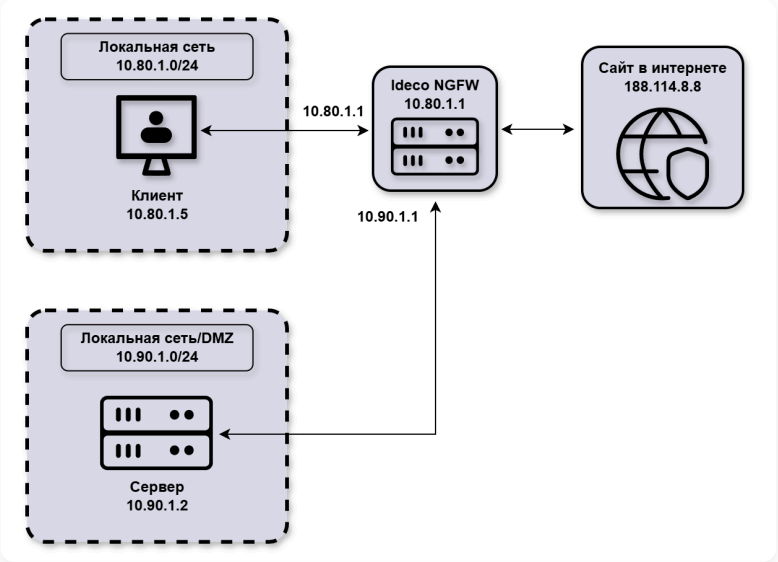
Когда хост `10.80.1.5` обращается на сайт по внешнему адресу `188.114.8.8` (например, в случае обращения по доменному имени, которое разрешено во внешнем IP), трафик проходит через NGFW. На NGFW срабатывает правило DNAT и перенаправляет трафик на сервер `10.80.1.2`, а сервер отвечает хосту, минуя NGFW.

Правильная топология сети:



Для правильной работы схемы потребуется:

1. Вынести роутер в отдельную локальную сеть (DMZ `10.90.1.0/24`), чтобы избежать асимметричной маршрутизации между роутером и клиентами локальной сети:



2. Настроить DMZ на NGFW, добавив на локальный интерфейс NGFW еще один IP-адрес (`10.90.1.0/24`), к локальной сети которого подключен роутер.

3. Настроить IP-адрес на роутере из адресного пространства новой сети `10.90.1.2`. Шлюзом указать дополнительный IP-адрес, настроенный на локальном интерфейсе NGFW из этой сети `10.90.1.1`.

Физически роутер 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 и роутера:

- Подключите к Ideco NGFW дополнительную сетевую карту;
- Настройте на сетевой карте дополнительный локальный интерфейс и отдельную IP-адресацию в этой сети;
- Укажите в качестве шлюза для роутера адрес, настроенный на дополнительном локальном интерфейсе.

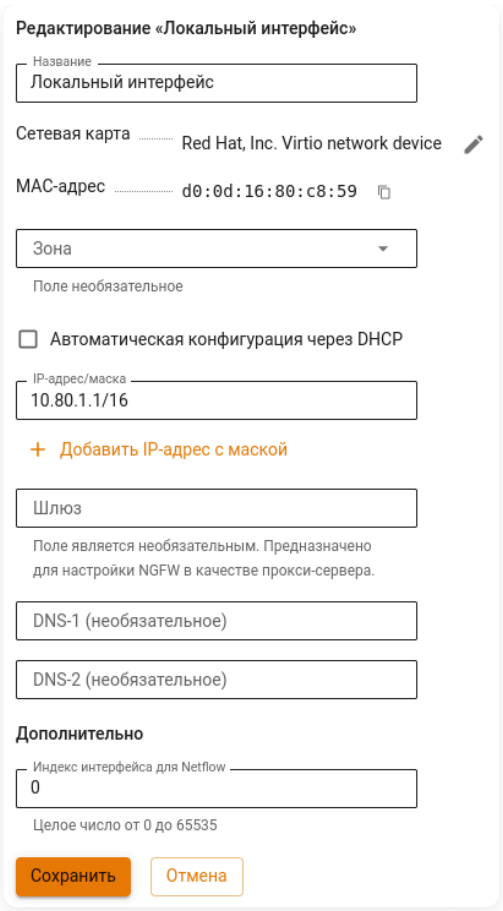
Физически роутер будет находиться в сегменте дополнительной сетевой карты.

Настройка NGFW

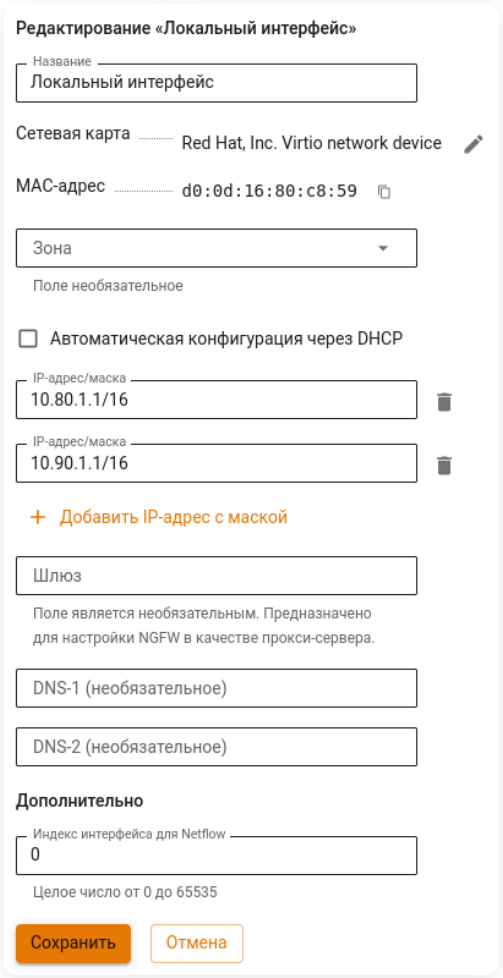
Для настройки нескольких виртуальных локальных сетей на одном физическом локальном интерфейсе NGFW перейдите в раздел **Сервисы** → **Сетевые интерфейсы** и выполните действия:

1. Откройте в режиме редактирования **Локальный интерфейс**, к которому подключены пользователи нужной вам локальной сети (`10.80.1.1/24`), нажав на напротив его названия.

2. Если IP-адрес вашей локальной сети был автоматически сконфигурирован через DHCP, отключите опцию и введите его вручную:



3. Нажмите на **+ Добавить IP-адрес с маской** и введите IP-адрес DMZ для изоляции роутера:

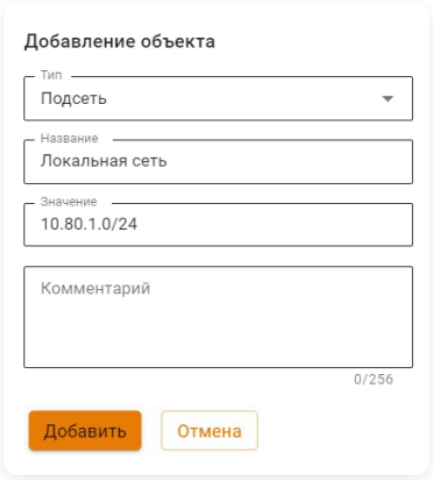


4. Нажмите **Сохранить**.

После изоляции роутера в DMZ нужно указать маршрут на NGFW до удаленной сети. Для этого перейдите в **Сервисы** → **Маршрутизация** и выполните действия:

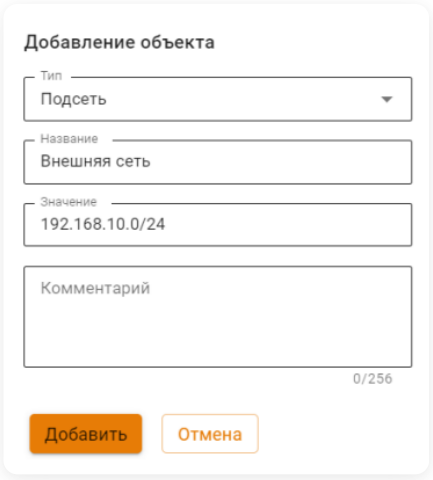
1. Перейдите на вкладку **Внешних сетей** нажмите кнопку **Добавить**.

2. В поле **Адрес источника** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес вашей локальной сети (`10.80.1.0/24`):



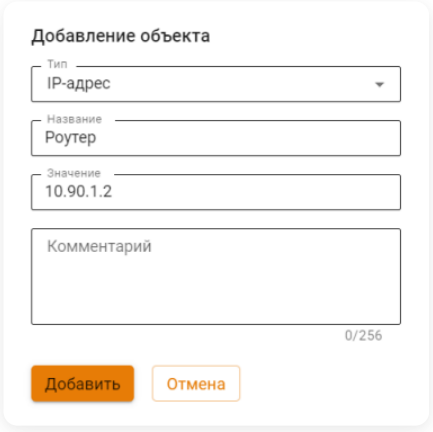
Выберите в качестве источника только что созданный объект.

3. В поле **Адрес назначения** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес внешней сети (`192.168.10.0/24`), в которую нужно настроить доступ:

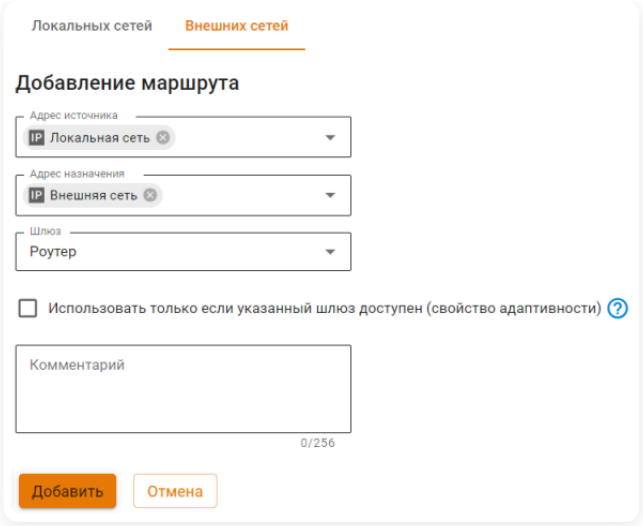


Выберите в качестве назначения только что созданный объект.

4. В поле **Шлюз** нажмите **Добавить объект**, выберите тип **IP-адрес** и введите адрес роутера в DMZ (`10.90.1.2`):



5. Сохраните маршрут вида:



Теперь трафик между сетями NGFW (`10.80.1.0/24` и `192.168.10.0/24`) во всех направлениях будет направляться через NGFW и роутер.

Настройка клиентских машин

Хосты сетей, которые теперь обслуживает NGFW (`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, укажите:

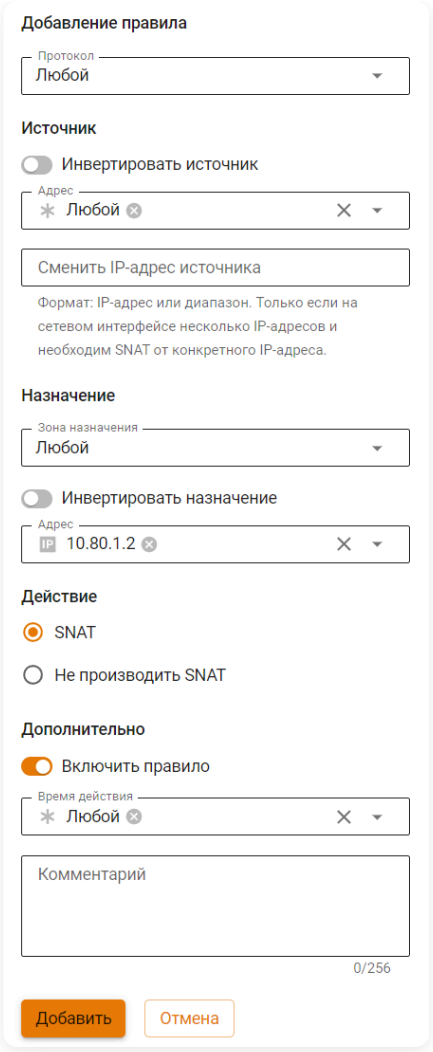
1. Для хостов из подсети `10.80.1.0/24` значение шлюза и DNS-сервера - `10.80.1.1`.

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 специальное SNAT-правило.

Создание на NGFW SNAT-правила для избежания асимметричной маршрутизации

Чтобы сервер `10.80.1.2` не отвечал напрямую на `10.80.1.5`, а посылал ответ на NGFW `10.80.1.1`, нужно в разделе **Правила трафика** → **Файрвол** → **SNAT** создать и включить правило вида:



Заполните поля:

- Назначение - `10.80.1.2`;
- Зона назначения - Локальные интерфейсы.

В этом случае трафик хоста `10.80.1.5` на внешний адрес сайта `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 - пакет приобретет вид: `scr 10.80.1.1 dst 10.80.1.2`. Ответ от сервера также пройдет через NGFW - пакет `scr 10.80.1.2 dst 10.80.1.1`.

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 его 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

Наше решение обладает всей функциональностью, обеспечивающей максимальную защиту от спам-ботов, ботнет-клиентов и предотвращение вирусной активности в сети.

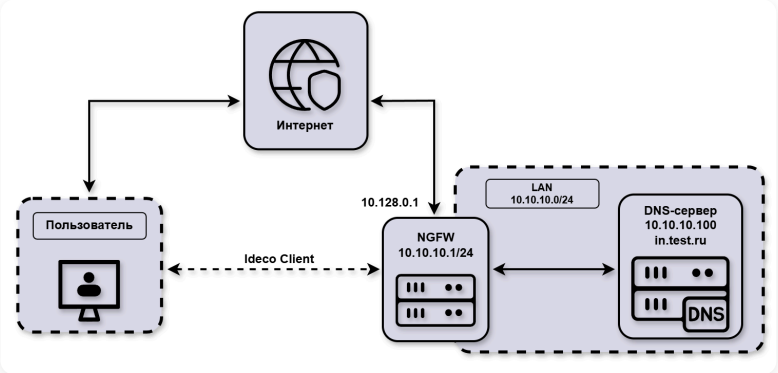
До 22 пользователей - решение предоставляется бесплатно. Для 10000 пользователей доступна 40-дневная пробная версия.

Скачать Ideco NGFW

Подключение через Ideco Client к внутреннему DNS

Клиенты, подключающиеся к NGFW из внешней сети через Ideco Client, изначально не видят внутренний DNS-сервер.

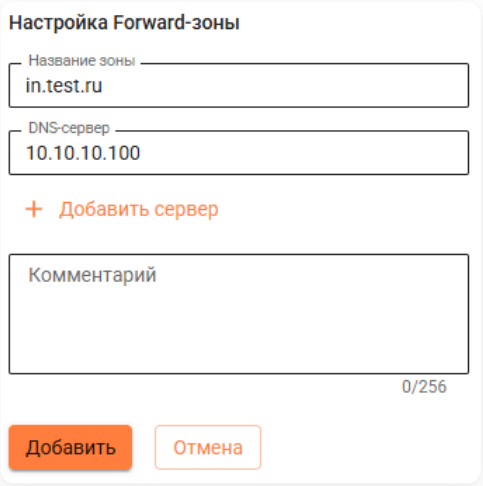
Схема сети:



Для настройки подключения к внутреннему DNS-серверу выполните действия:

1. Перейдите в **Сервисы** → **Защита и управление DNS** → **FORWARD-ЗОНЫ** и нажмите **Добавить**.

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

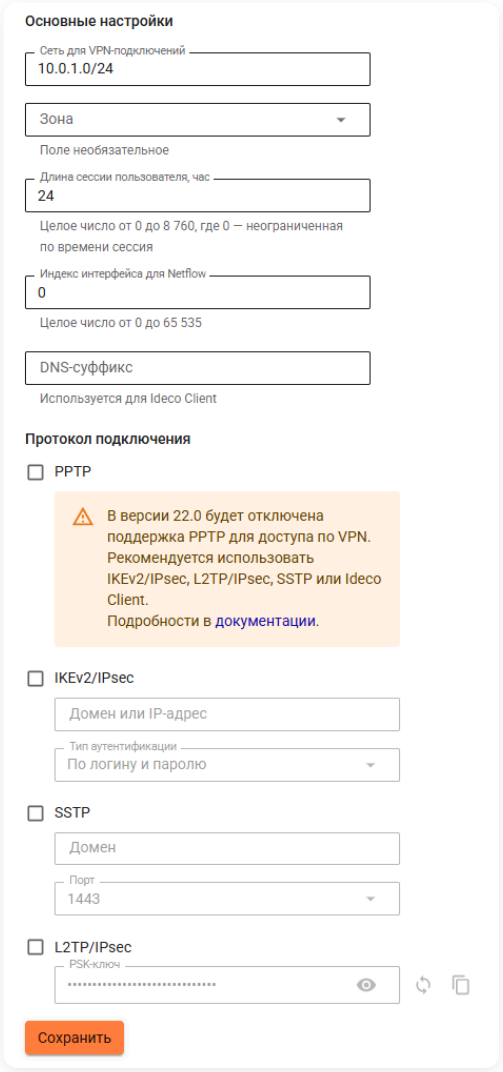


После настройки NGFW клиенты, подключающиеся к NGFW с помощью Ideco Client из интернета, смогут использовать внутренний DNS-сервер.

Как избежать проблем с подключением VPN-клиентов при использовании нескольких серверов Ideco NGFW

При использовании нескольких серверов Ideco NGFW 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.

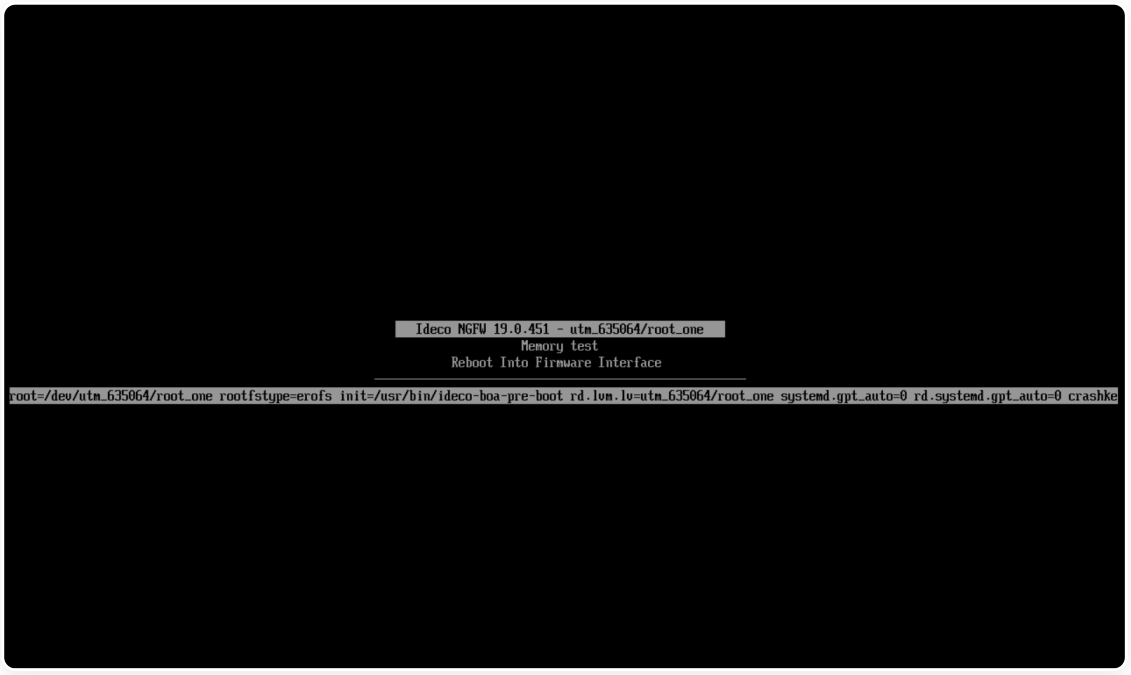
Как восстановить доступ к Ideco NGFW

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:

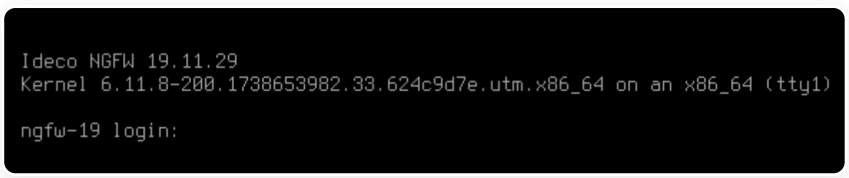


2. Откроется окно параметров ядра с возможностью редактирования. Переместите указатель стрелками на клавиатуре вправо до слова `quiet` и допишите текст `p=1`:



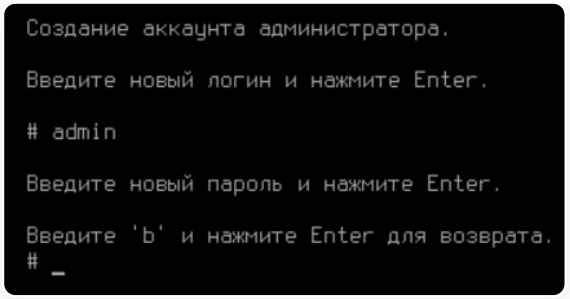
3. Нажмите `Enter`.

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:

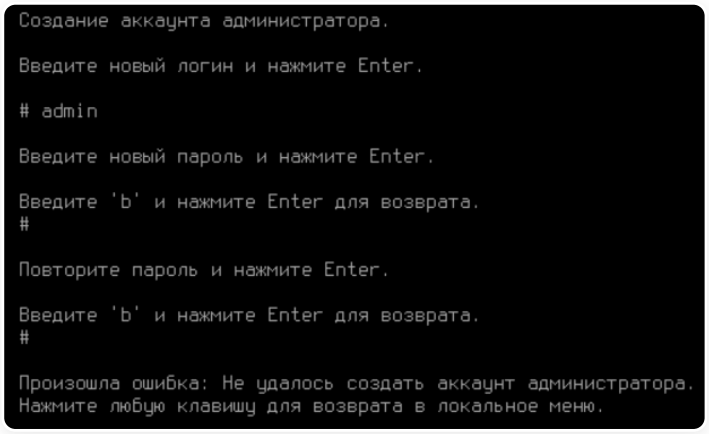


Требования к созданию пароля администратора:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.
- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

Если при создании нового логина администратора он 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 восстановиться на прошлую версию после обновления Ideco NGFW

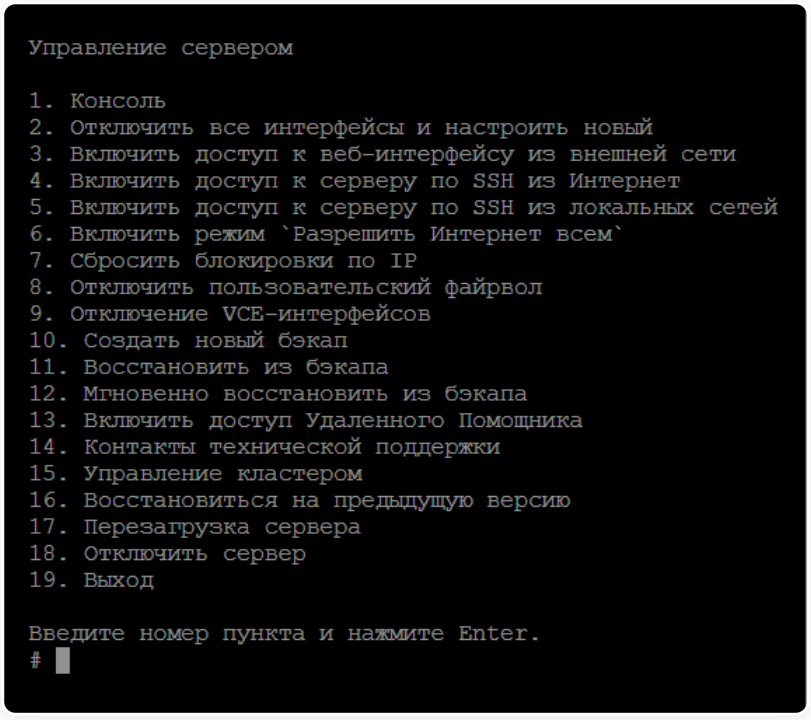
При восстановлении на предыдущую версию данные перенесены не будут. Сохраните бэкап на внешнем носителе. Информация о работе с API бэкапа описана в статье Бэкап.

Для восстановления на предыдущую версию выполните действия:

1. Перейдите в локальное меню Ideco NGFW.

2. Введите логин и пароль администратора.

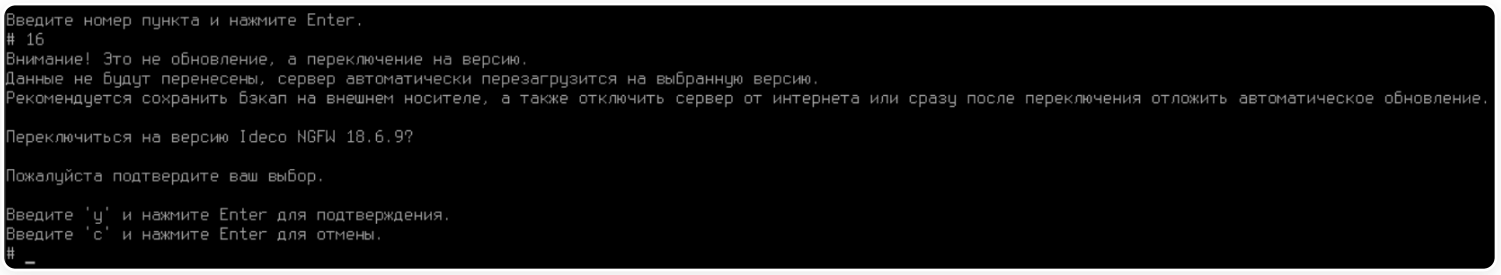
3. Укажите номер пункта 16 и нажмите Enter:



Появится окно с предупреждением и описанием версии, на которую произойдет переключение.

Если в Ideco NGFW 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 переключится на предыдущую версию.

Поддержка устаревших алгоритмов шифрования

Ideco NGFW основан на операционной системе Fedora. В Ideco NGFW используется Fedora 40. Подробнее об изменениях политики алгоритмов можно прочитать в статье.

Устаревшие алгоритмы, как (криптографическое) хеширование и шифрование, обычно имеют время жизни, по истечении которого они 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. Это можно сделать из локального меню, по ssh или через веб-интерфейс Ideco NGFW.

2. Введите в терминале команду `update-crypto-policies --set DEFAULT:FEDORA32`.

3. Перезагрузите Ideco NGFW.



Мы настоятельно не рекомендуем использовать данную настройку, так как при следующем обновлении Ideco NGFW настройки режима совместимости будут сброшены. В более новых версиях данная возможность будет отключена.

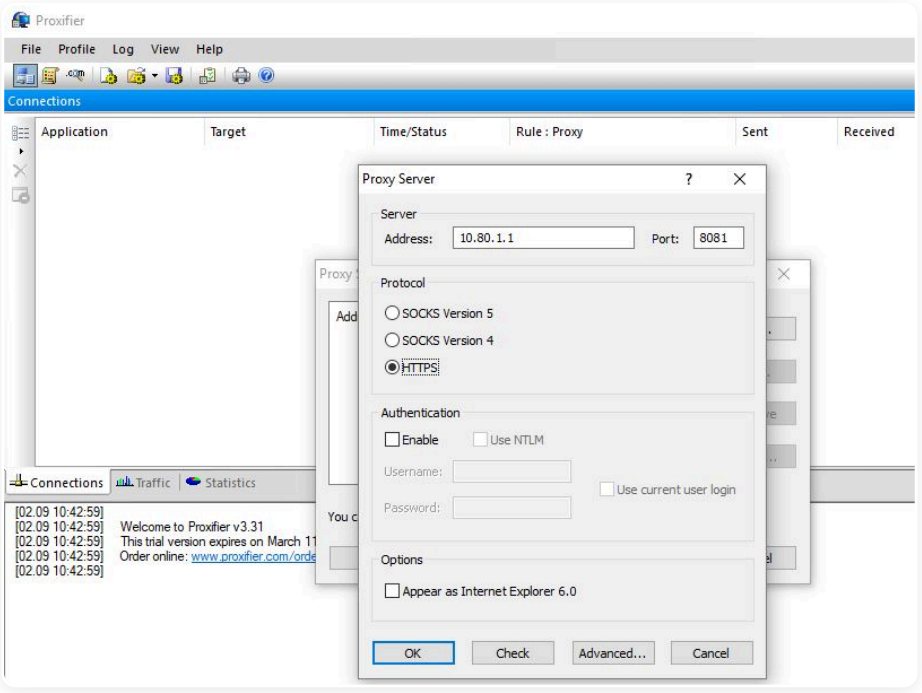
Настройка программы Proxifier для прямых подключений к прокси серверу

Скачать Proxifier можно с сайта разработчика.

Настройка

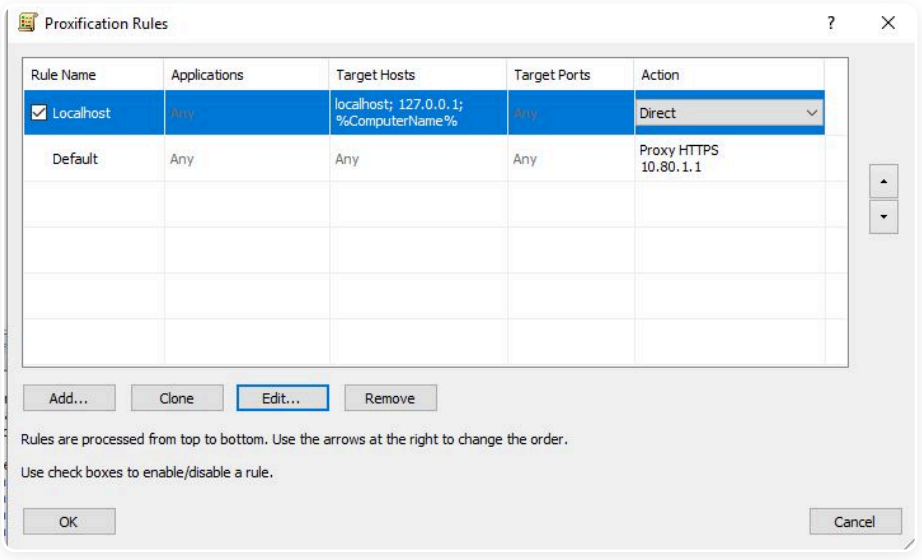
Выполните стандартные настройки браузера для прямых подключений к прокси-серверу, а затем настройте программу для перенаправления остального трафика на прокси-сервер.

Пропишите в настройках прокси-сервера в Proxyfier IP-адрес локального интерфейса Ideco NGFW 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:



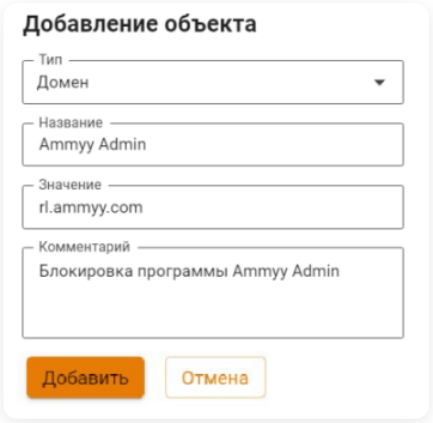
Настройка закончена, программы будут выходить в интернет через заданный прокси-сервер.

Блокировка популярных ресурсов

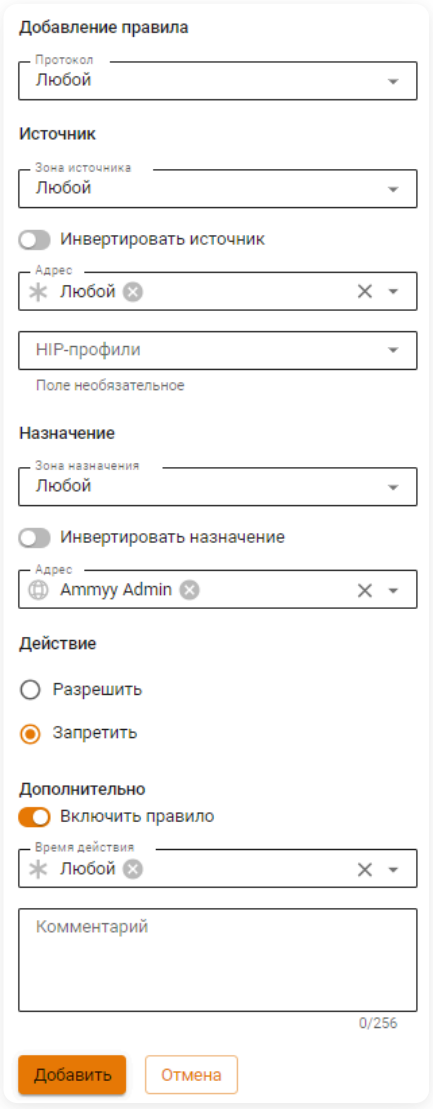
Блокировка Ammyy Admin

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:



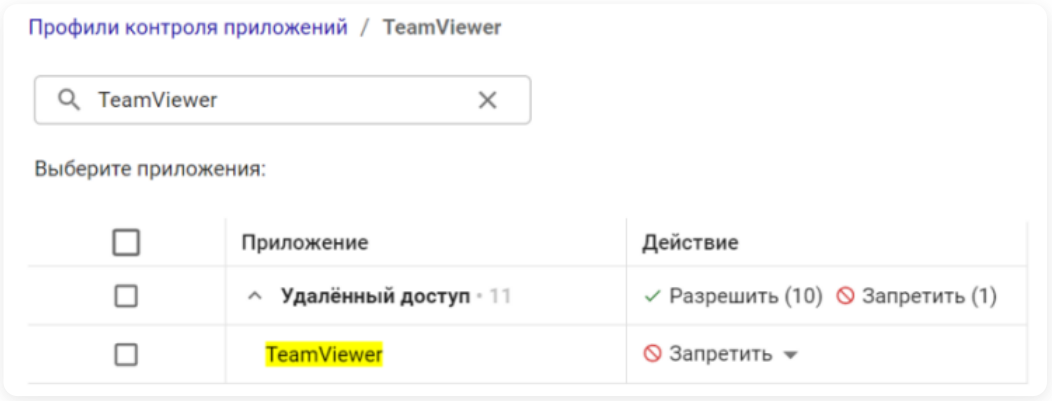
2. Перейдите на вкладку **Правила трафика** → **Файрвол** → **FORWARD**, создайте и включите правило запрета для нужных пользователей или групп. В поле **Назначение** выберите объект, созданный в пункте 1:



Блокировка TeamViewer

TeamViewer - это программное обеспечение для удаленного доступа и управления компьютерами. Его можно заблокировать с помощью Контроля приложений.

1. Перейдите в раздел **Профили безопасности** → **Контроль приложений**. Создайте новый профиль для TeamViewer с действием **Запретить**:

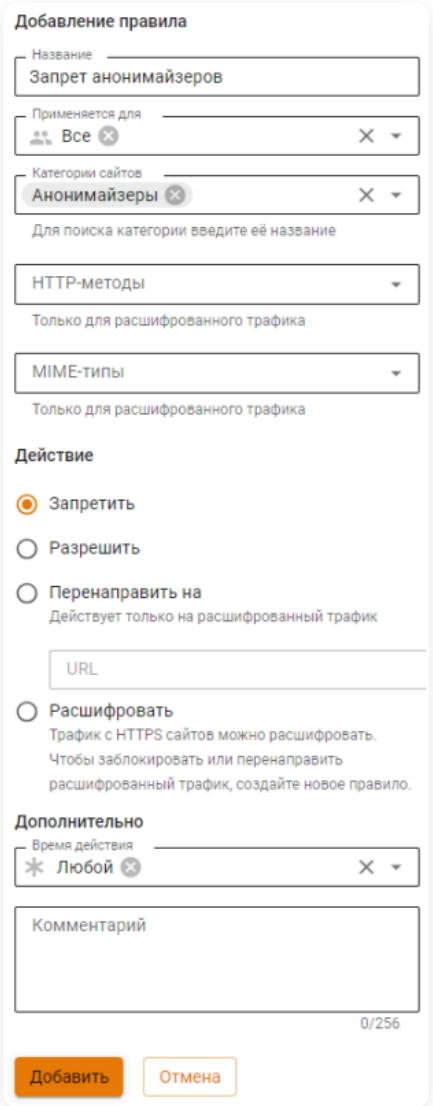


2. В разделе **Правила трафика** → **Файрвол** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

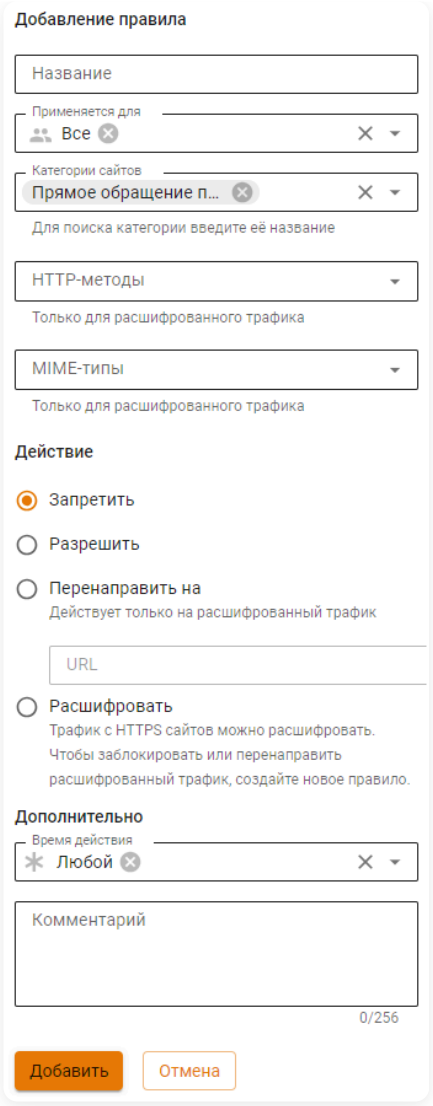
Блокировка анонимайзеров

Заблокировать анонимайзеры можно в разделе **Правила трафика** тремя способами:

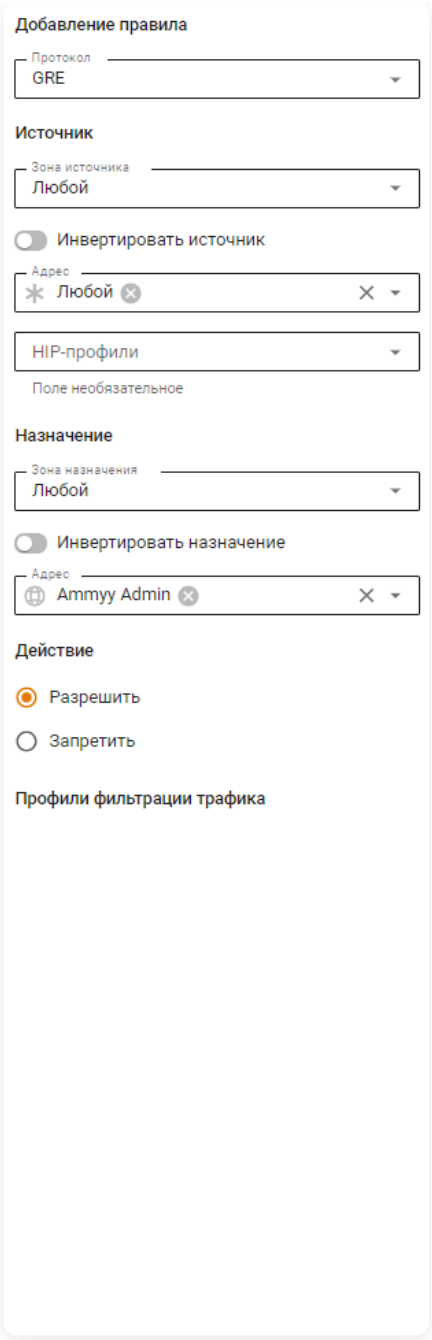
1. Анонимайзеры, работающие по протоколам HTTP(S), блокируются в разделе **Правила трафика** → **Контент-фильтр**. Для этого создайте правило, в котором запретите категорию сайтов **Анонимайзеры**:



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 **Файрвола**:



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 раздел **Профили безопасности** → **Предотвращение вторжений**. Создайте новый профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило, блокирующее группу сигнатур **Анонимайзеры**:

3. Нажмите **Добавить**.

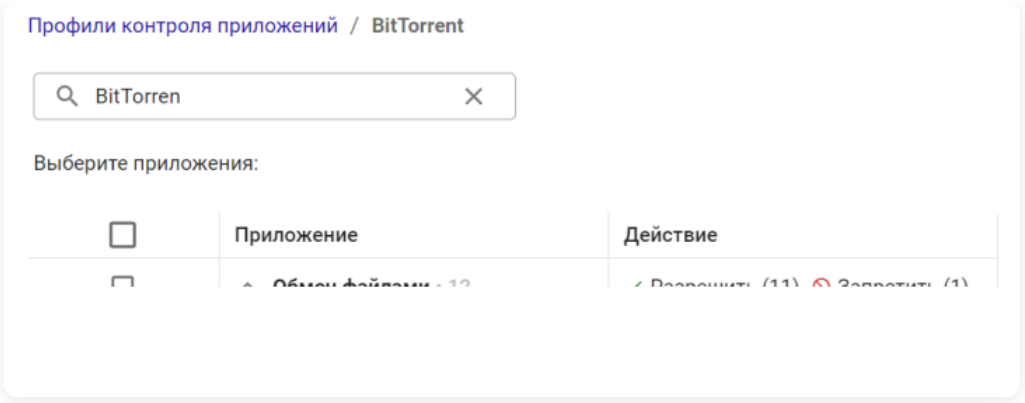
4. В разделе **Правила трафика** → **Файрвол** добавьте и включите разрешающее правило с профилем, созданным ранее.

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 разделе **Профили безопасности** → **Контроль приложений**:



2. В разделе **Правила трафика** → **Файрвол** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

3. Разрешите нужные TCP и UDP порты пользователям. Затем создайте и включите в разделе **Правила трафика** → **Файрвол** → **FORWARD** правило, которое запрещает все протоколы (правила действуют сверху вниз).

4. В разделе Контент-фильтр заблокируйте доступ к сайтам-каталогам и торрент-файлам. Для этого запретите категории **Торрент-трекеры** и **Torrent-файлы**:

5. В разделе **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 разделе **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**:

Настройка почтовых клиентов

Примечание

В Ideco NGFW 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.

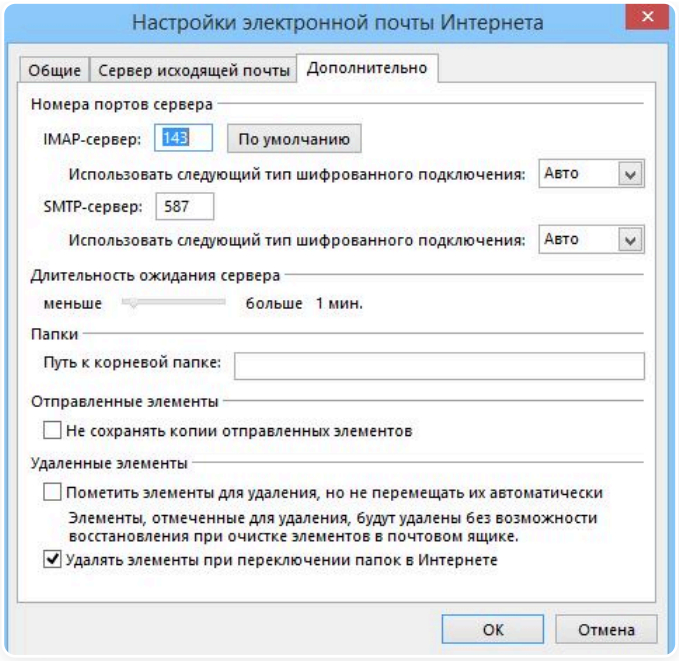
2. Сервер исходящей почты работает только с авторизацией и шифрованием. Необходимо использовать 587 порт для подключения (а не 25). Тип шифрования, логин и пароль указываются аналогично серверу входящей почты.

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

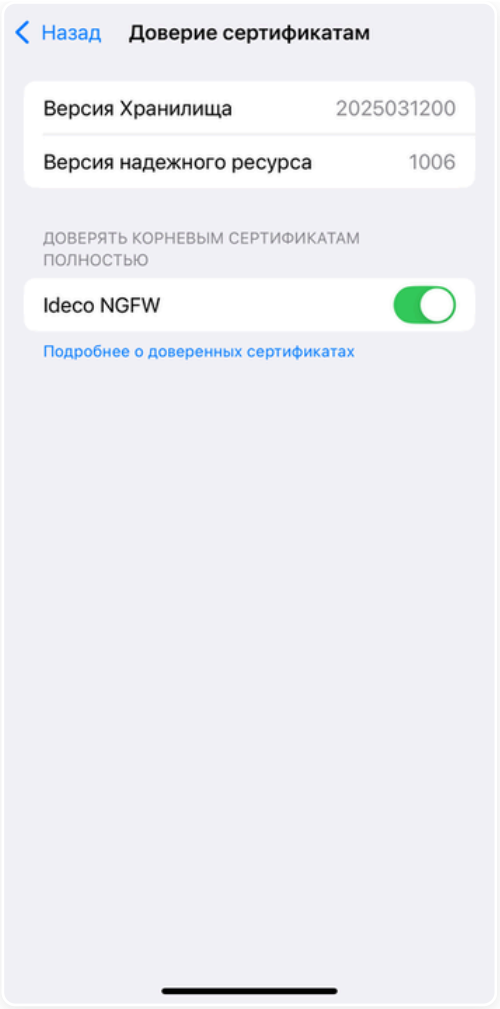
1. Скачайте сертификат в **Сервисы** → **Сертификаты** и перенесите на настраиваемое устройство (например, отправив по почте).

2. Перейдите в **Настройки** → **Основные** → **VPN и управление устройством**.

3. Выберите сертификат и нажмите кнопку **Установить**:

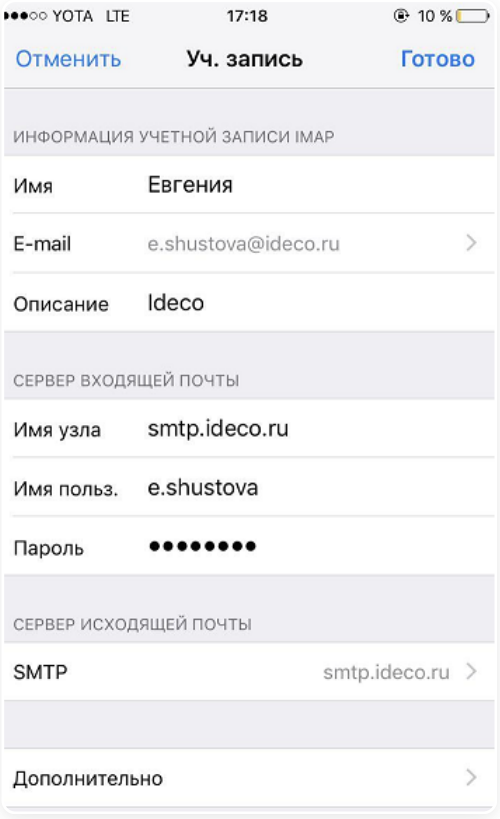
4. Зайдите в **Настройки** → **Основные** → **Об этом устройстве** и выберите **Доверие сертификатов**.

5. Включите опцию **Доверять корневым сертификатам полностью**:

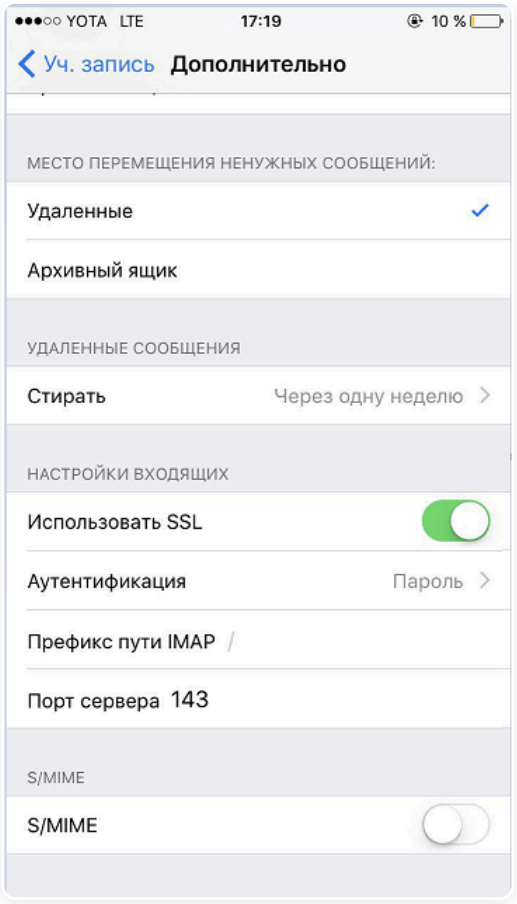


Настройка почтового ящика

1. Перейдите в Учетную запись почты и нажмите **Дополнительно**:



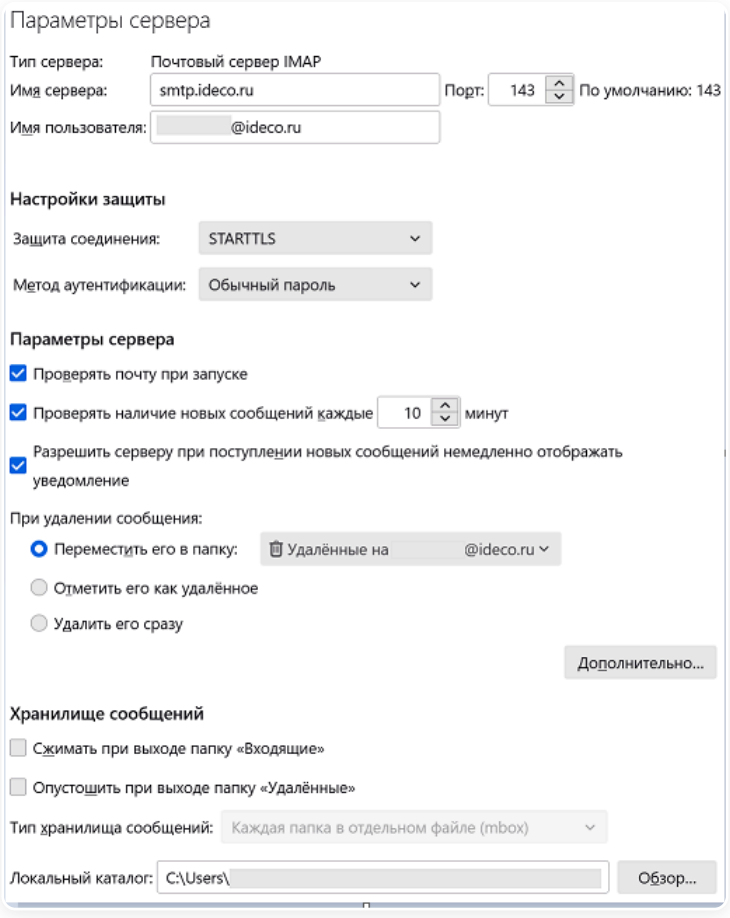
2. Скорректируйте настройки:



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**.

Настройка прозрачной авторизации на Astra Linux

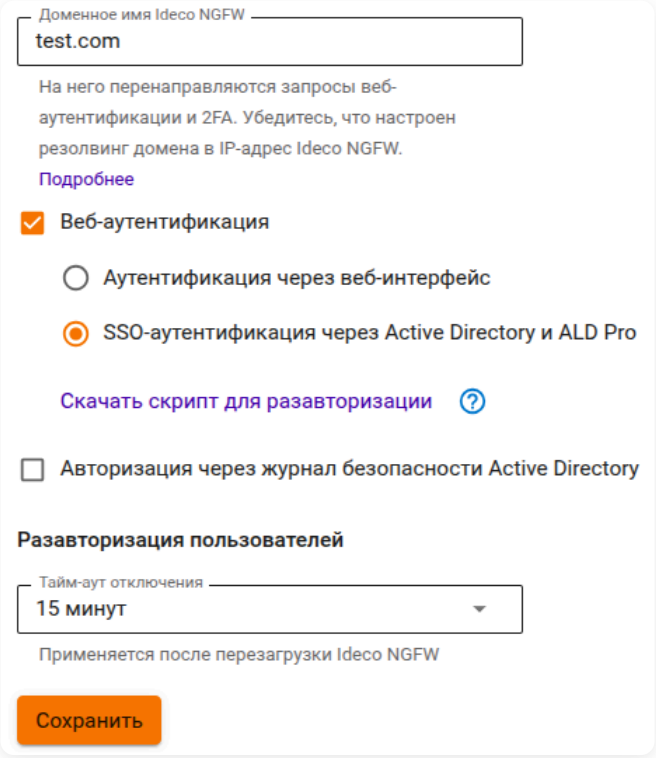
Решение подходит для браузеров **Yandex**, **Chromium** и **Firefox.**

1. Установите и настройте NGFW на устройстве администратора, получите лицензию.

2. Введите Astra Linux в домен (например, через Active Directory).

3. Введите NGFW в тот же домен и импортируйте пользователей (в том числе Astra Linux) в группу.

4. Включите в NGFW **SSO-аутентификацию через Active Directory и ALD Pro** в разделе **Пользователи** → **Авторизация** → **Веб-аутентификация**:



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.

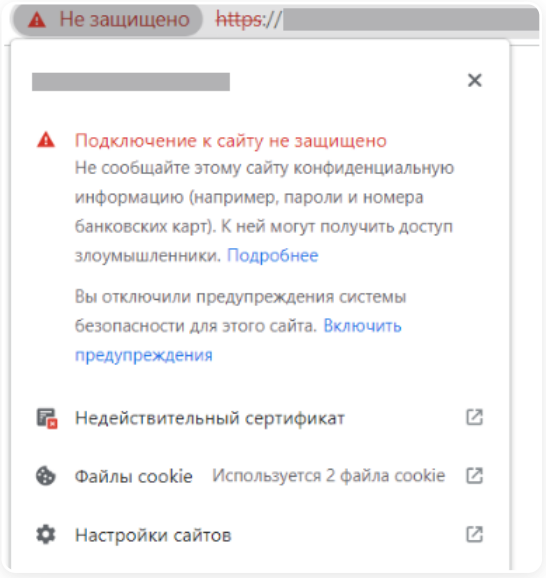
Для браузера Firefox

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:

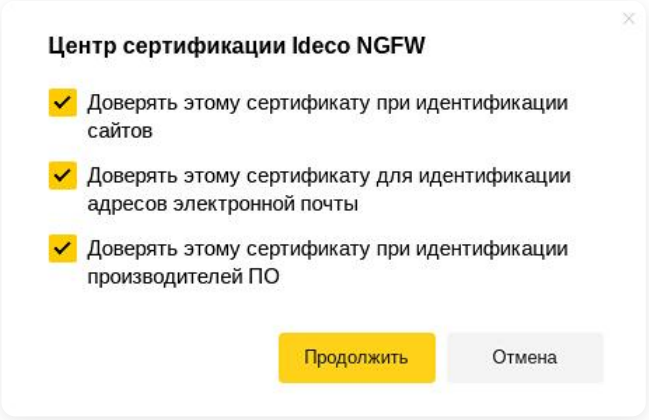


Для браузера Yandex

1. Скачайте корневой сертификат.

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

3. Включите опции доверия для сертификата:

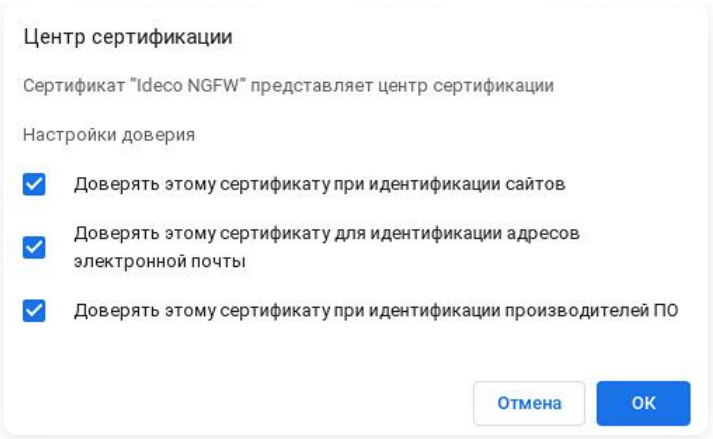


Для браузера Chromium

1. Скачайте корневой сертификат.

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

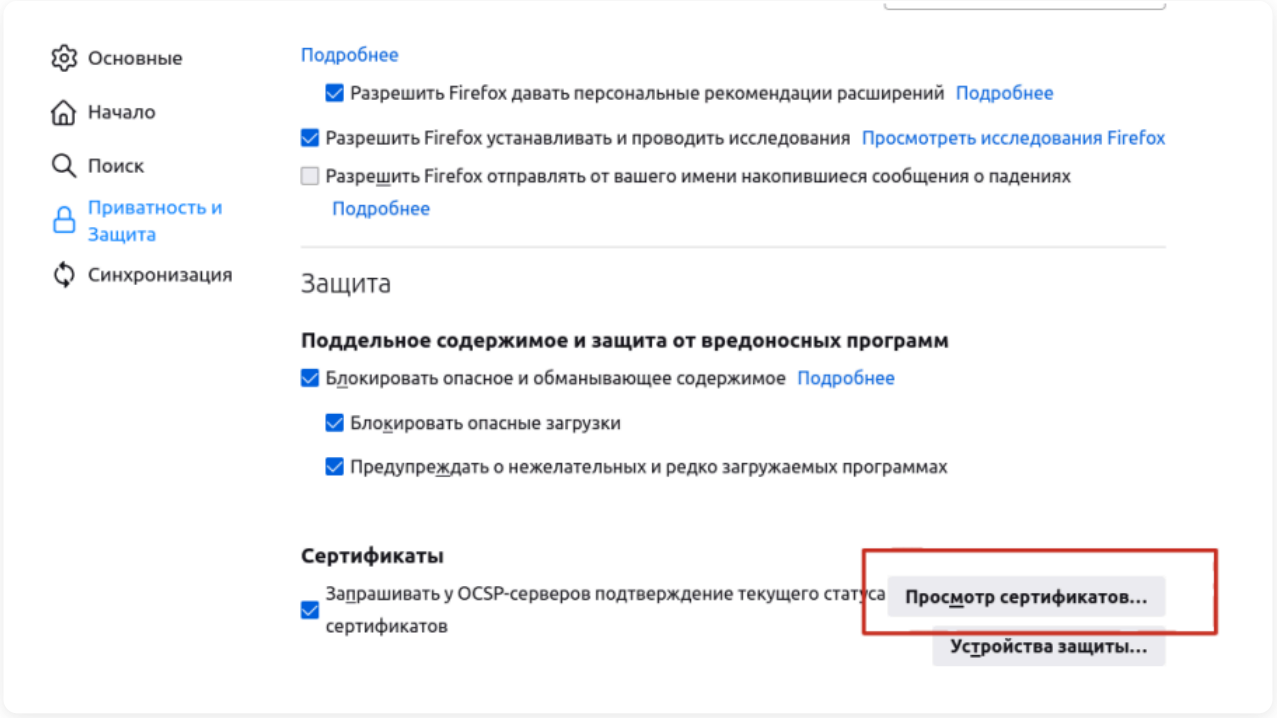
3. Включите опции доверия для сертификата:



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.

Инструкция по настройке автоматической веб-аутентификации на Ideco NGFW

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 каталог `ideco-utm`. Можно воспользоваться командой:

```
mkdir -p ~/.config/ideco-utm
```

3. Скачайте корневой сертификат NGFW `root_ca.crt` (подробнее в статье) и поместите его в каталог, созданный на предыдущем шаге.

4. Создайте в папке `ideco-utm` файл `auth.conf`. Добавьте в него содержимое (введите логин и пароль пользователя) в формате:

```
login=логин_пользователя
password=пароль_пользователя
```

5. Рекомендуем ограничить права доступа к файлу `auth.conf`:

```
chmod 0600 ~/.config/ideco-utm/auth.conf
```

6. Скачайте скрипт на компьютер пользователя по ссылке или воспользуйтесь командой:

```
curl -O https://docs.ideco.ru/scripts/auto-web-auth-linux.py
```

7. Настройте автозагрузку в соответствии с описанным ниже алгоритмом.

Для корректной работы скрипта имя корневого сертификата должно быть `root_ca.crt`.

Пути к файлам и другие параметры можно менять с помощью ключей запуска. Используйте ключ `-h` или `--help` для вывода справки.

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

[Install]
WantedBy=multi-user.target
```

Введите имя пользователя Linux и полный путь до скрипта.

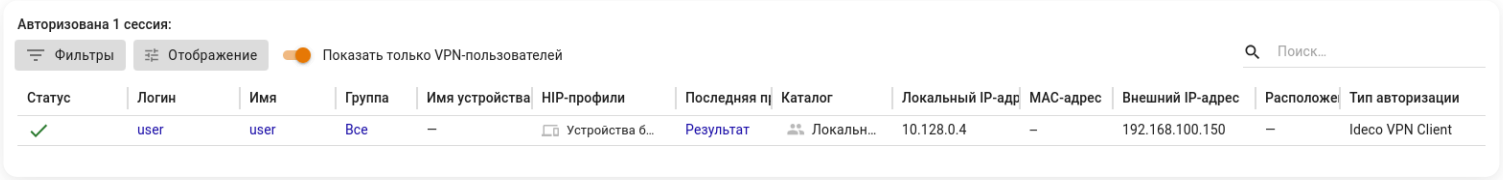
3. Сохраните файл и выйдите из редактора.

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. 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 свой выбор.



Если выйти из сессии на устройстве пользователя и повторно открыть браузер, то запрос на авторизацию появиться не должен.

Порядок обработки веб-трафика в Ideco NGFW

Порядок обработки веб-трафика:

1. Ограничение скорости.

2. DNS.

3. Захват трафика для фильтрации (прокси-сервер):

- Контент-фильтр.
- Антивирус веб-трафика.

4. Файрвол.

5. Контроль приложений.

6. Система Предотвращения вторжений.

INPUT-правила Файрвола обрабатывают трафик раньше DNS (если включен перехват DNS-запросов) и прокси-сервера.

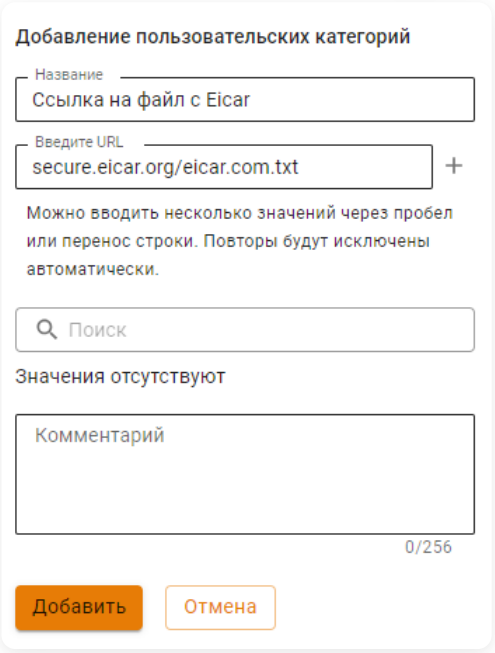
В модули **Контроль приложений** и **Предотвращение вторжений** отправится только тот трафик, который попадает под разрешающее правило **Файрвола** с включенной проверкой через профиль контроля приложений и профиль предотвращения вторжений соответственно.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика?

Для примера использовался тестовый файл с Eicar, доступный для скачивания по ссылке.

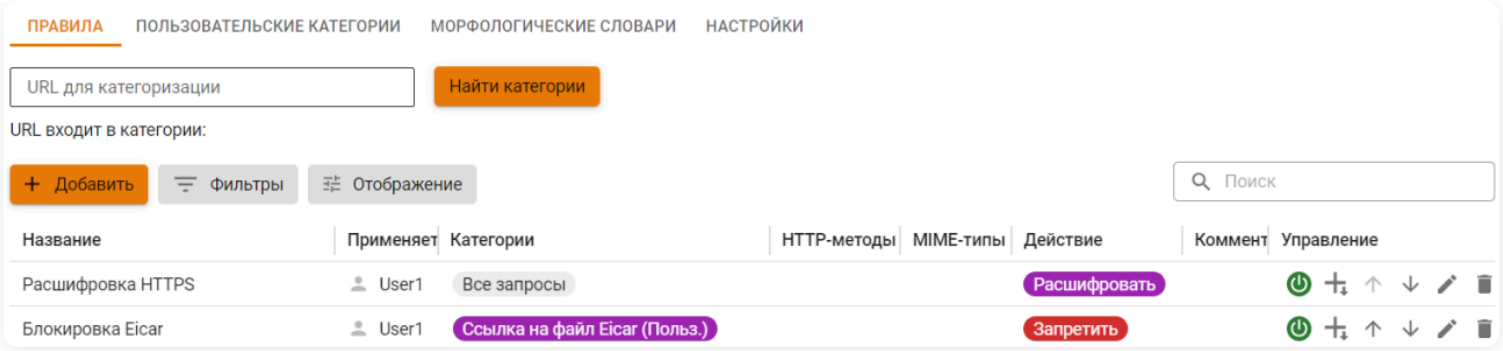
1. Перейдите в раздел **Правила трафика** → **Контент-фильтр** → **Пользовательские категории**. Нажмите **Добавить**.

2. Введите ссылку на ресурс и нажмите + :



3. Перейдите на вкладку **Правила** и создайте два правила для **User1**:

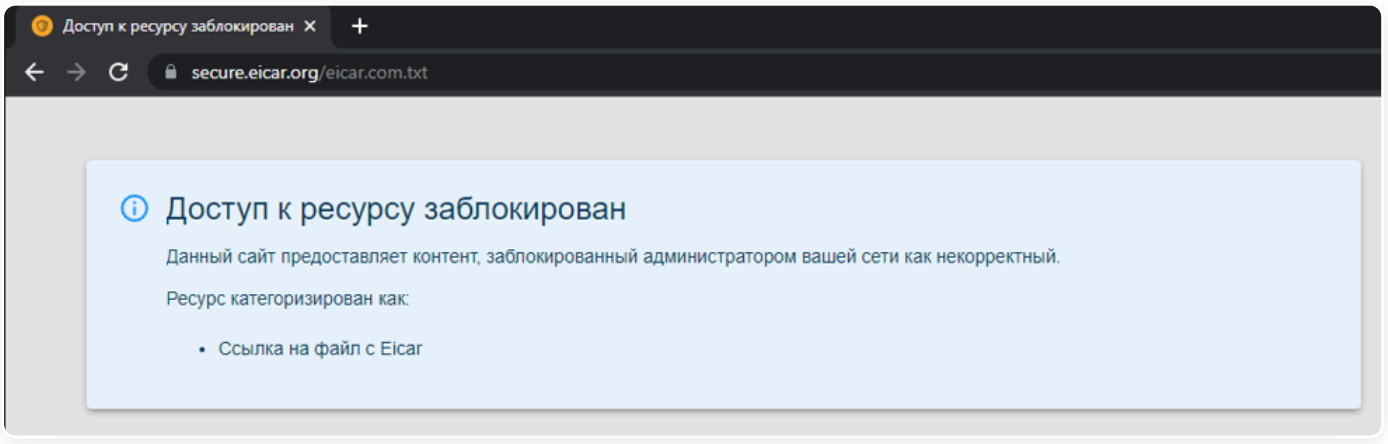
- Правило расшифровки всех HTTPS-запросов, чтобы антивирус мог работать с HTTPS-трафиком.
- Правило блокировки созданной пользовательской категории:



4. Убедитесь, что опция **Антивирус** переведена в положение **Включен**.

5. Авторизуйте пользователя и перейдите по ссылке на скачивание Eicar.

Откроется страница блокировки **Контент-фильтра**:



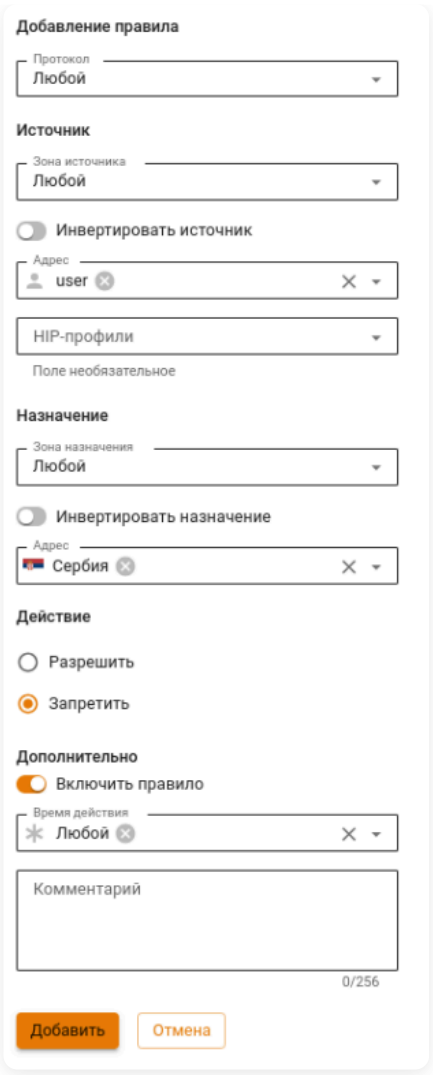
Контент-фильтр обрабатывает трафик приоритетнее, чем антивирусы. Просмотреть информацию о срабатывании правил **Контент-фильтра** можно в **Отчеты** → **Трафик** → **Топ сайтов**.

Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Файрвол?

Для примера заблокируем пользователю `user` сайт `rts.rs`.

1. Перейдите в раздел **Правила трафика** → **Файрвол**, на вкладку **FORWARD** и нажмите **Добавить**.

2. Заполните поля:

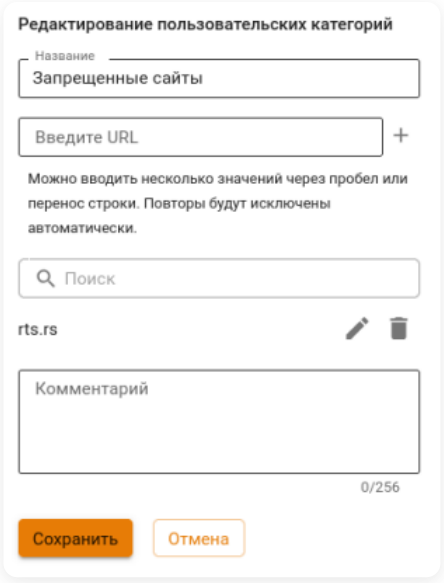


- **Протокол** - выберите **Любой**.
- **Адрес** источника - выберите пользователя `user`.
- **Адрес** назначения - выберите страну **Сербия**.
- **Действие** - выберите **Запретить**.

3. Нажимити **Добавить**.

4. Перейдите в раздел **Контент-фильтр** на вкладку **Пользовательские категории** и нажмите на  напротив категории **Запрещенные сайты**.

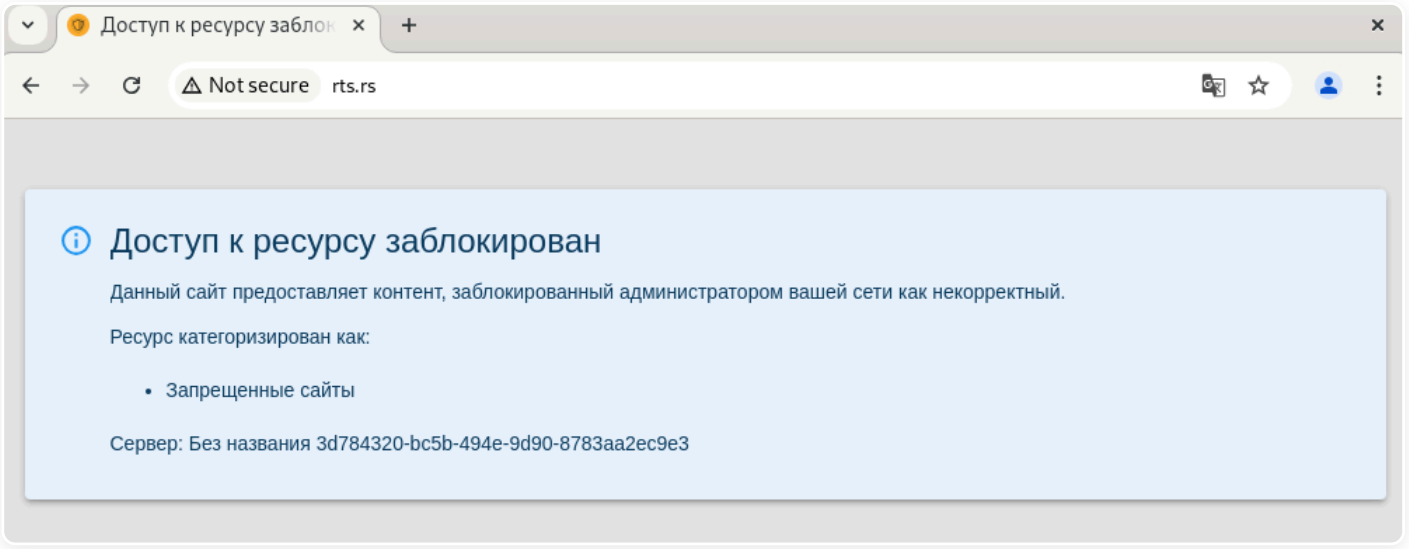
5. Добавьте ссылку на сайт `rts.rs` и нажмите **Сохранить**:



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 **Файрвол**.

Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG

В Ideco NGFW 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. Брокер будет самостоятельно балансировать трафик устройств в локальной сети между нодами созданного кластера.

При падении одной ноды трафик перебалансируется между остальными Ideco NGFW без перерыва в связи. Это реализует схему кластера Active/Active.

Объединять в кластер устройства Ideco NGFW между собой не нужно.

Для корректной работы нод установите одинаковые настройки.

Для централизованного управления нодами Ideco NGFW воспользуйтесь Ideco Center.

Особенности использования схемы:

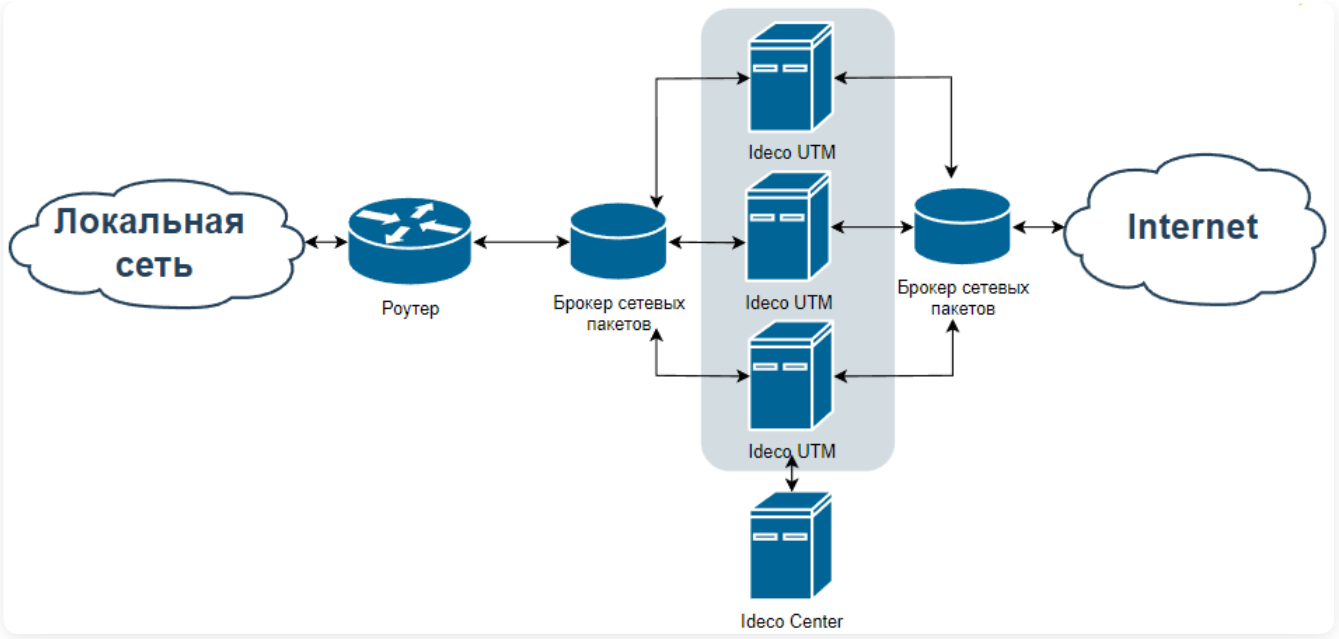
- Настройки, которые нельзя распространить через Ideco Center, придется вручную изменять на каждом Ideco NGFW;
- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено;
- Данные отчетности, логов и мониторинга не синхронизируются между нодами. В каждой ноде 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 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 ниже. На этой основе встройте оба решения в свою сеть.

На каждом Ideco NGFW 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



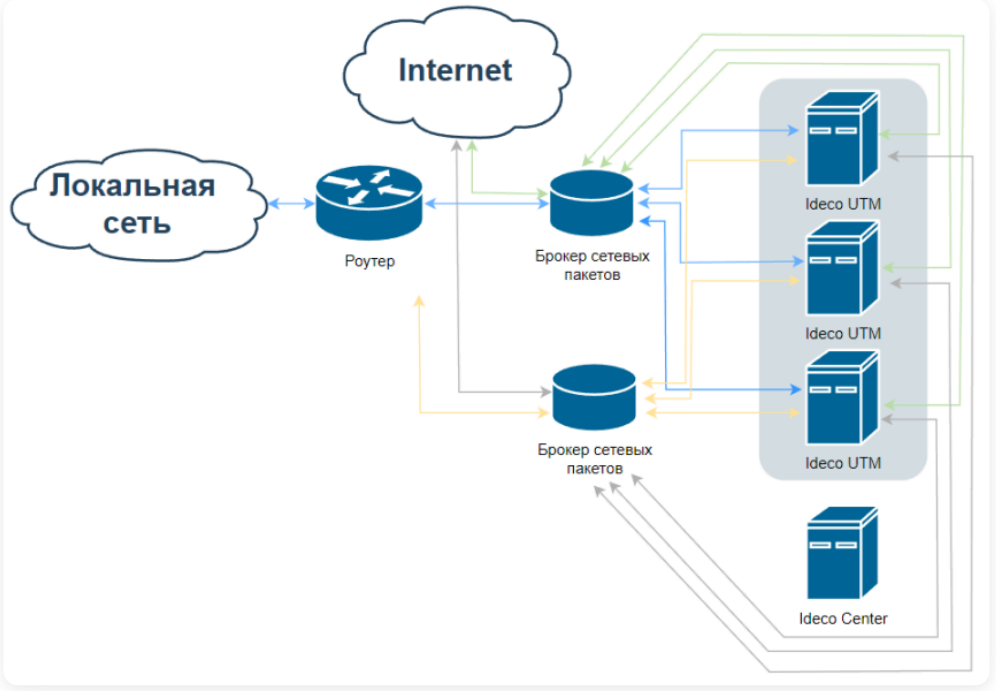
Настройка Ideco NGFW:

На каждом устройстве Ideco NGFW 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.

На каждом Ideco NGFW в качестве шлюза внешнего интерфейса нужно использовать IP-адрес, полученный от провайдера.

Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW



Настройка Ideco NGFW

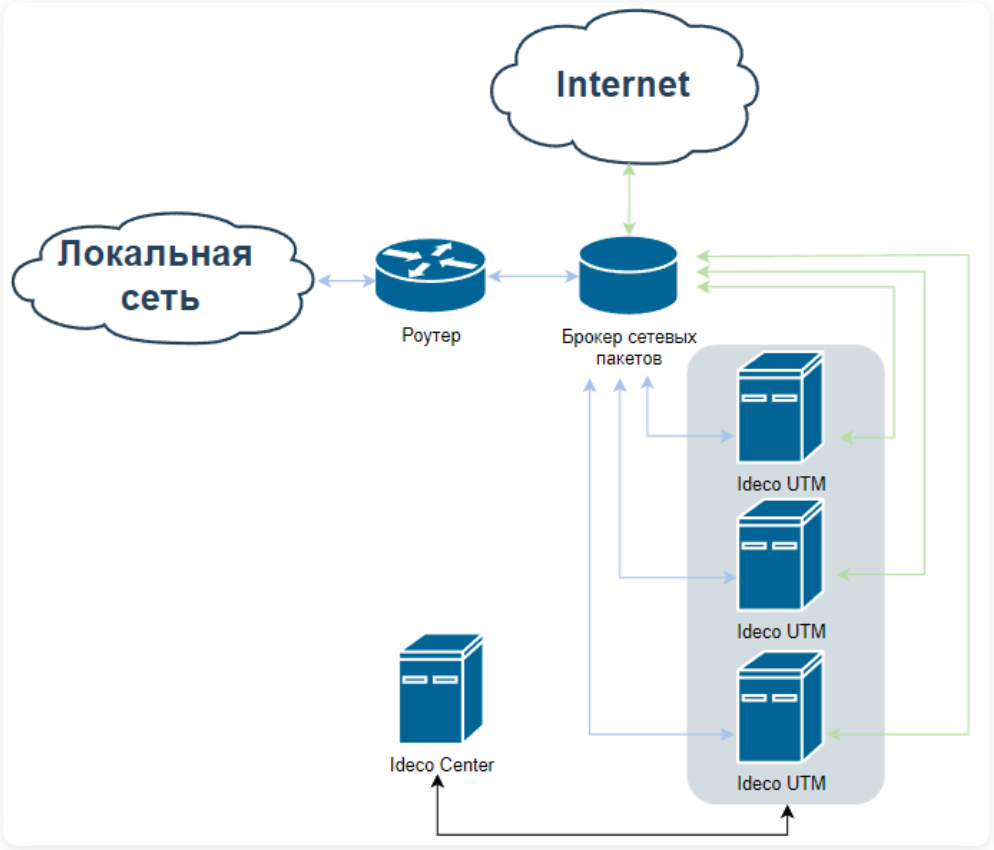
На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW;
- На каждом NGFW будет два локальных и два внешних интерфейса. Шлюзом внешних интерфейсов нужно указать IP-адрес, полученный от провайдера.

На Ideco NGFW в этой конфигурации в разделе Балансировка и резервирование должен быть активирован режим резервирования. Приоритетным внешним интерфейсом должен быть выбран тот, который идет к основному брокеру сетевых пакетов.

Пример 3 - Один брокер, расположенный перед Ideco NGFW



Настройка Ideco NGFW

На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку внешнего и локального интерфейсов.

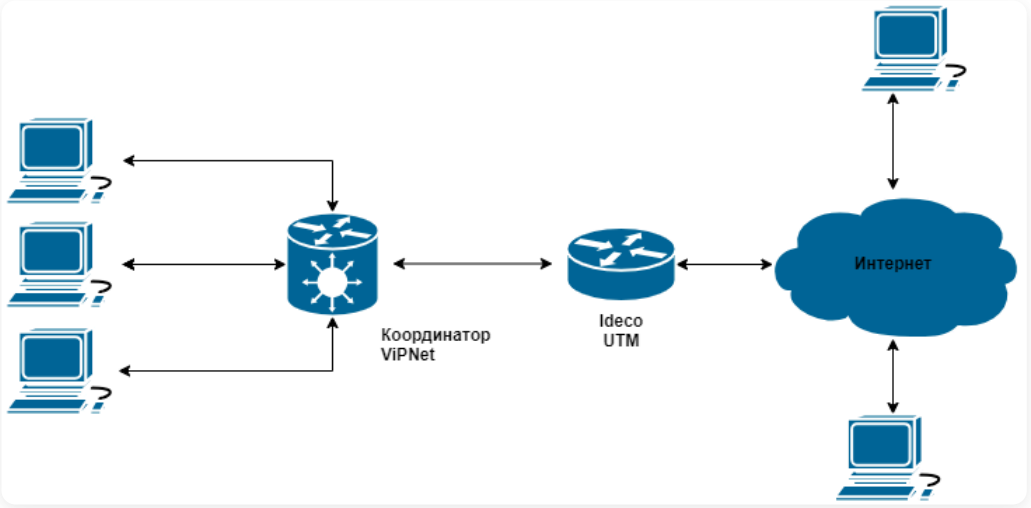
Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW;
- Шлюзом внешнего интерфейса нужно указать IP-адрес, полученный от провайдера.

Рекомендации по настройке NGFW для работы совместно с ViPNet-координатором

ViPNet-координатор используется для шифрования трафика подсети, в которой он является шлюзом. Шифрование позволяет обеспечить конфиденциальность информации, передаваемой по незащищенному каналу.

Схема совместной работы Ideco NGFW с ViPNet-координатором:



Настройка Ideco NGFW и ViPNet-координатора

Для корректной работы Координатора совместно с NGFW выполните действия:

1. Настройте проброс порта udp 55777 на IP адрес координатора в разделе **Файрвол → DNAT (перенаправление портов)**.

2. Переведите Координатор в режим **Со статической трансляцией адресов**.

Работа Координатора в режиме динамической трансляции адресов совместно с Ideco NGFW не гарантируется.

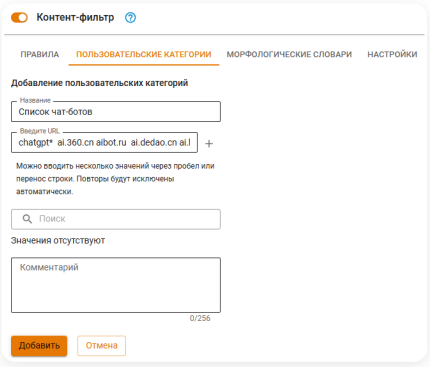
Более подробно о настройке ViPNet можно узнать в статье.

Блокировка чат-ботов

Для блокировки ресурсов, которые взаимодействуют с чат-ботами, необходимо создать правило в **Контент-фильтре**:

1. Перейдите на вкладку **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.

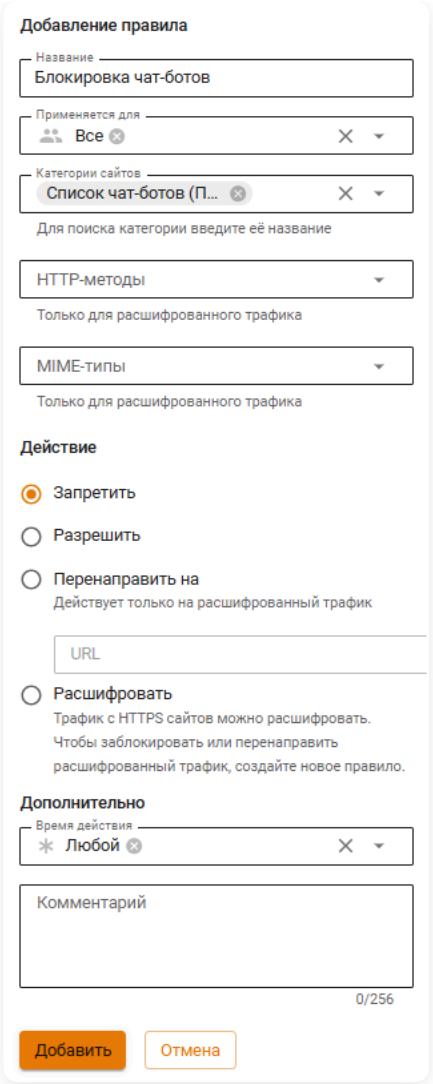
Список URL

```
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 на вкладку **Правила** и добавьте новое правило с действием **Запретить**:



Полезные ссылки

Правила

Описание категорий Контент-фильтра

Таблица портов Ideco NGFW, 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 и настройки интерфейсов.
- TCP-порты 80 и 443, открытые во внешнюю и локальную сеть сразу после установки Ideco NGFW 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	14765 TCP, 3051 UDP
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
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.

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**:

1. Отправляет запрос на адрес https://host:14765/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 `14765`;
- 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:14765/connect`, к которому будет подключаться **Ideco Client**;
- Если ответа со статусом 302 от адреса `https://host:14765/connect` нет, то **Ideco Client** подключится к NGFW по адресу `wss://host:14765/connect`.

Пример правильного редиректа, полученный с помощью утилиты **curl**:

1. **Запрос**: `curl -il https://host.dev:14765/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:14765/connect`.

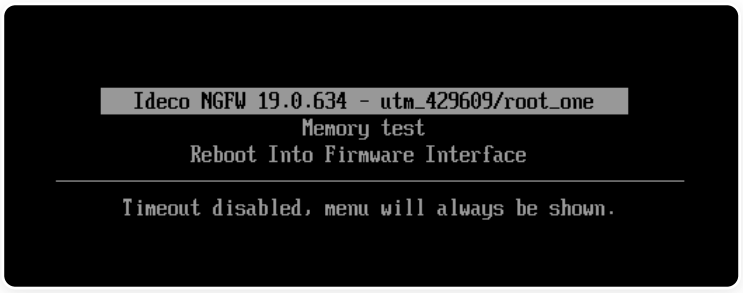
3. Если при попытке доступа к URL-адресу `https://host.dev:14765/connect` не будет получен ответ с кодом 302, то **Ideco Client** подключится к NGFW по адресу `wss://host.dev:14765/connect`.

Как включить таймер при загрузке Ideco NGFW?

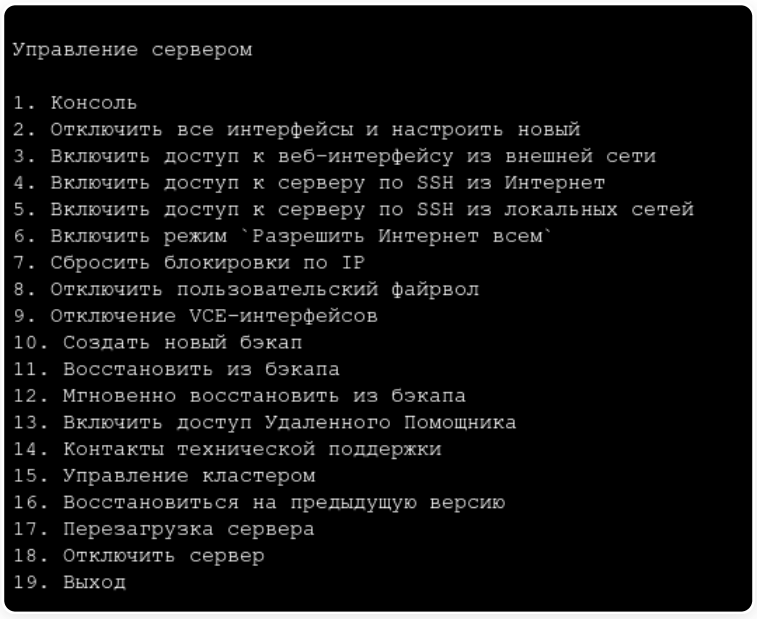
При отключении таймера также отключается автоматический выбор пункта меню. В этом случае система не загрузится сама после обновления, рестарта или переключения ноды в режиме кластеризации до момента нажатия **Enter**.

Для включения таймера выполните действия:

1. При загрузке сервера выберите Ideco NGFW, 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**.

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
```

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
```

Добавление IP-адреса в белый список fail2ban

Система защиты fail2ban блокирует IP-адреса при обнаружении подозрительной активности. В редких случаях заблокирован может быть и доверенный адрес. Чтобы предотвратить такую блокировку, добавьте IP-адрес в белый список fail2ban. 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 доверенный IP-адрес с маской `/32` или подсеть с нужной маской в конец строки через пробел. Для добавления нескольких IP-адресов укажите их последовательно через пробел:

```
# ICS-27477: Здесь можно добавить IP-адреса в исключения для fail2ban.
# Этот файл будет переноситься с бэкапом при обновлении на новую версию.
[DEFAULT]
ignoreip = 127.0.0.1/8 ::1 92.167.132.63/32 43.156.101.90/32
```

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.

Как настроить автоматическое включение аппаратного комплекса Ideco NGFW после сбоя питания

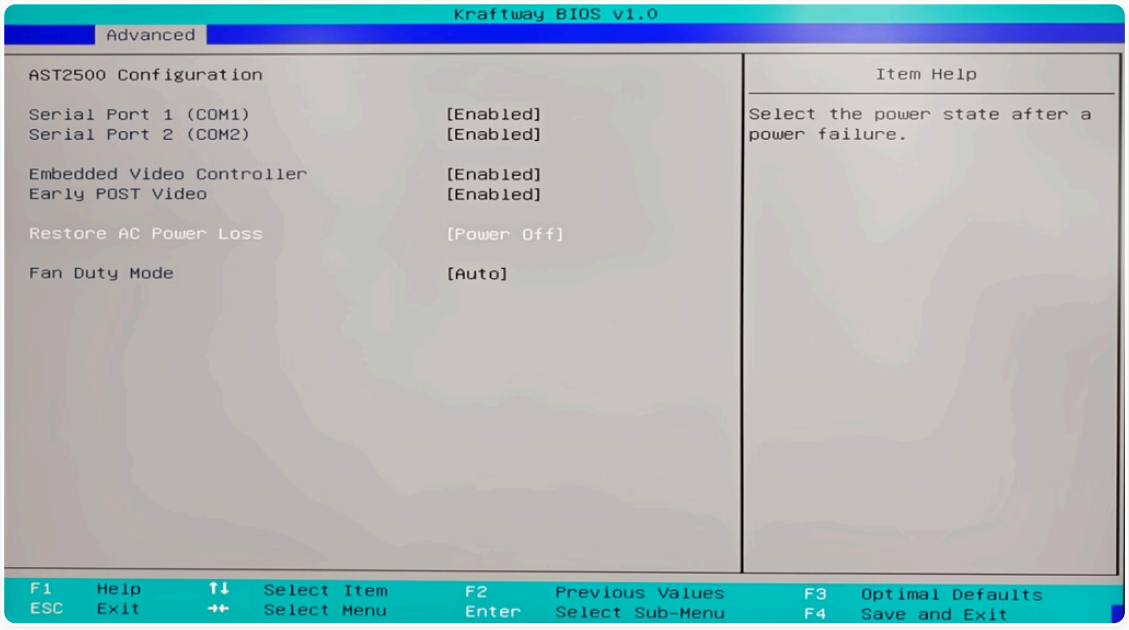
Решение подходит для всех моделей аппаратных комплексов Ideco NGFW.

Для автоматического восстановления работы аппаратного комплекса Ideco NGFW после сбоя электропитания необходимо активировать опцию **Restore AC Power Loss (Восстановления питания после сбоя)** в BIOS. Для включения опции:

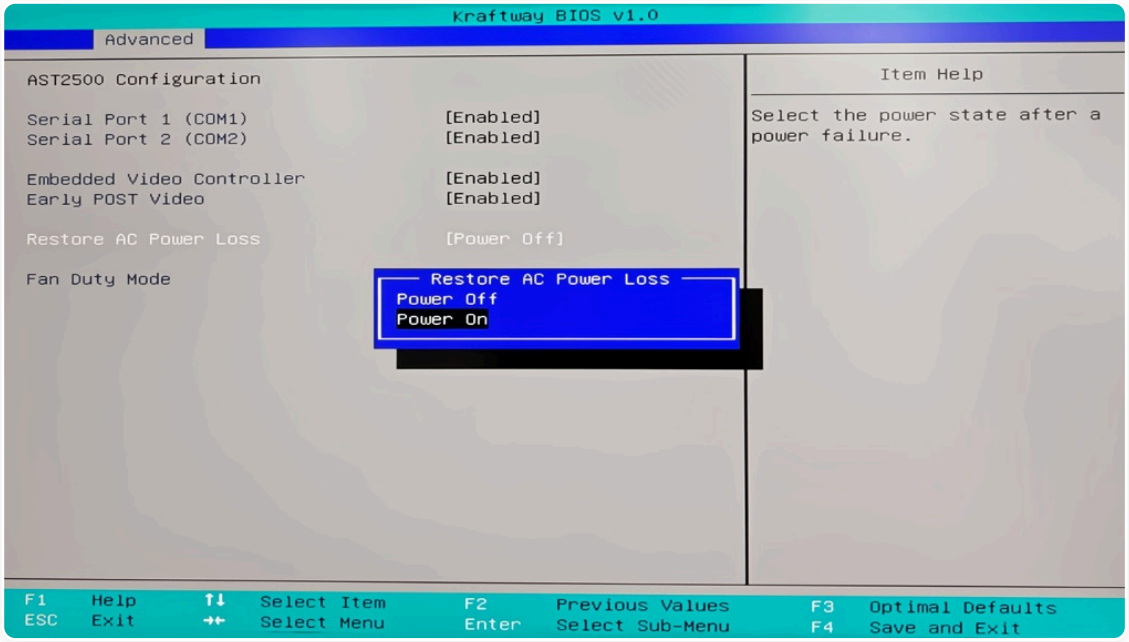
1. Запустите перезагрузку сервера.

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.

Использование собственного CA-сертификата в Контент-фильтре

В **Контент-фильтре** возможно использование не корневого сертификата Ideco NGFW, 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.

3. Загрузка CA-сертификата на сервер NGFW.

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) [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 []:
```

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 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-----
```

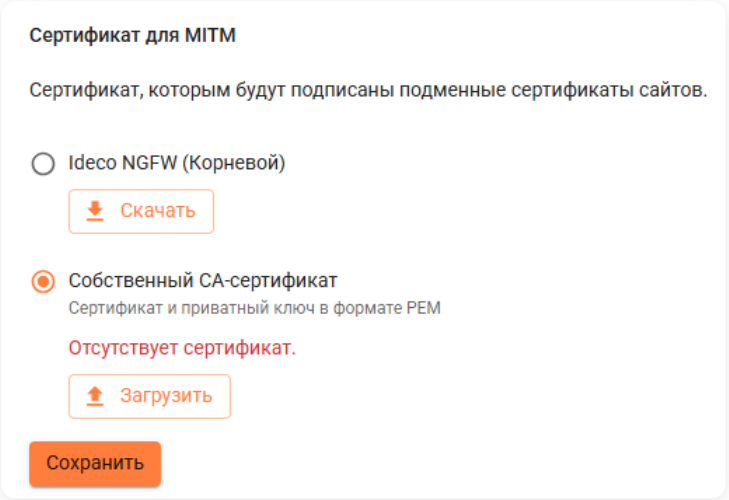
4. Сохраните файл бандла с именем, отличным от PEM-файла CA-сертификата, и расширением **.pem**, например, `ideco-cf_root-ca-key.pem`.

Шаг 3. Загрузка сертификата на сервер

Загрузите файл бандла на Ideco NGFW. 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**:

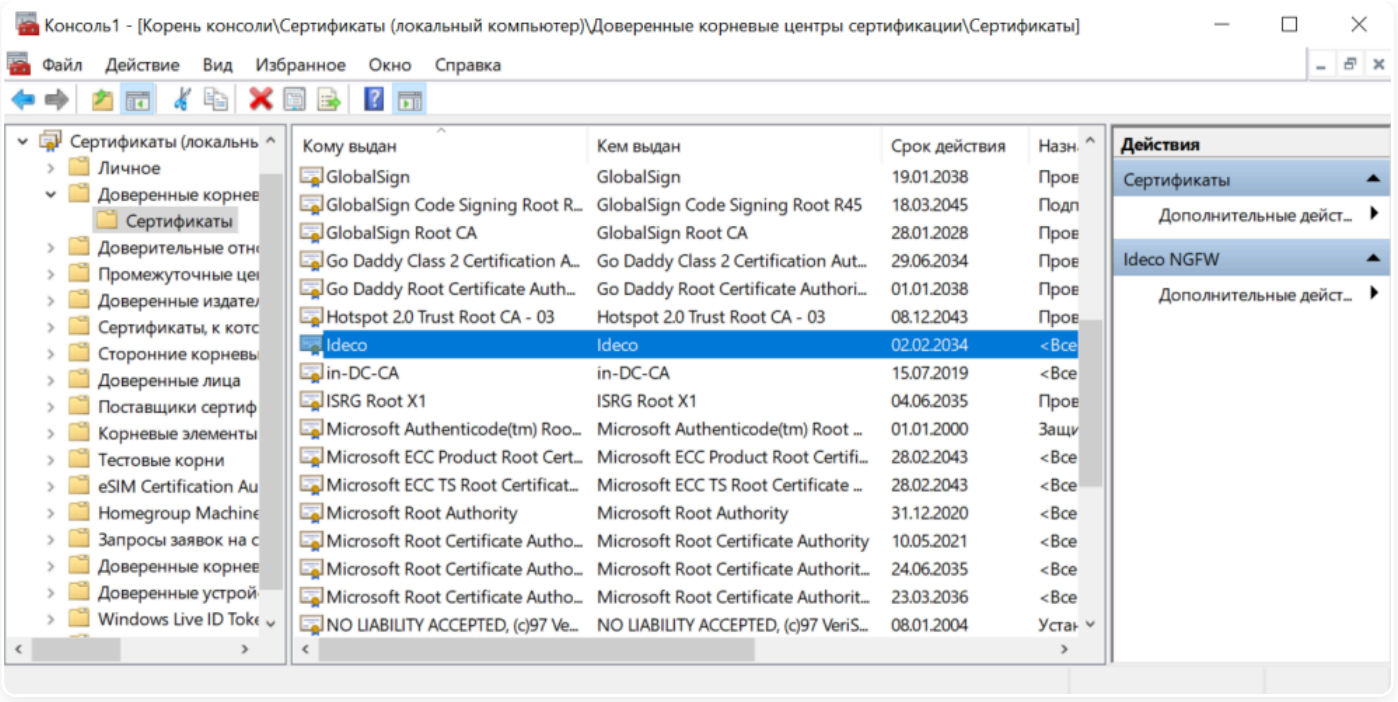
4. В открывшемся окне выберите пункт **Учетной записи компьютера** и нажмите **Далее**:

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:



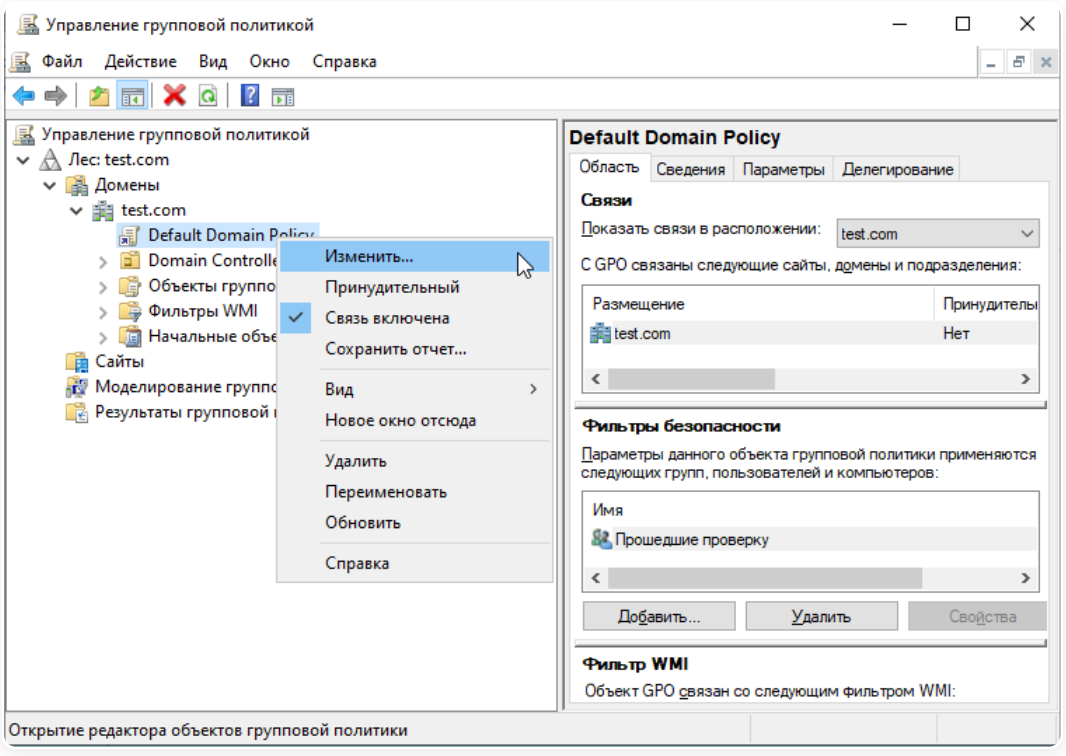
Автоматическая установка CA-сертификата через Active Directory

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, можно установить сертификат Ideco NGFW для всех пользователей автоматически:

1. Зайдите на контроллер домена с правами администратора.

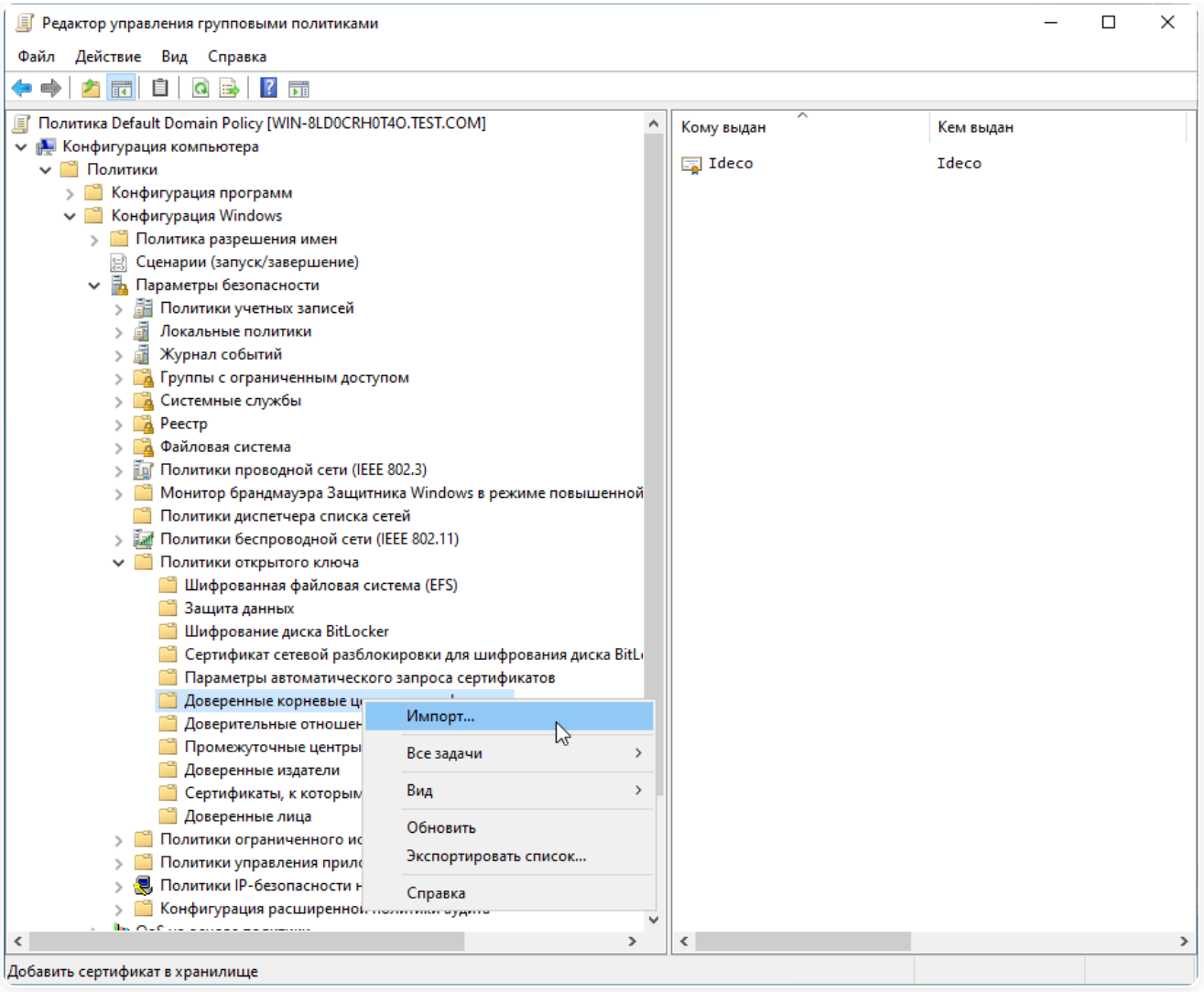
2. Запустите оснастку **Управление групповой политикой**, выполнив команду **gpmc.msc**.

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:



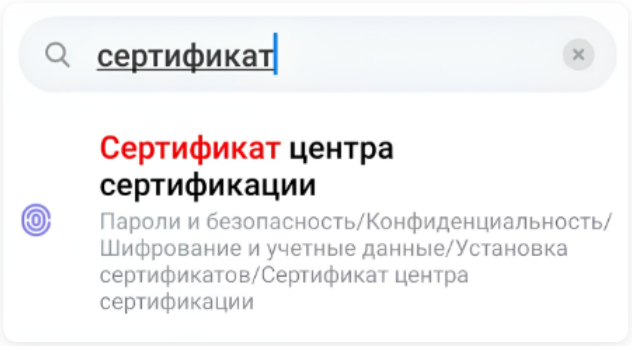
6. После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Как установить сертификат Ideco NGFW на Android

1. Скачайте сертификат Ideco NGFW на Android-устройство.

2. Перейдите в **Настройки**.

3. В поиске введите `Сертификат`:

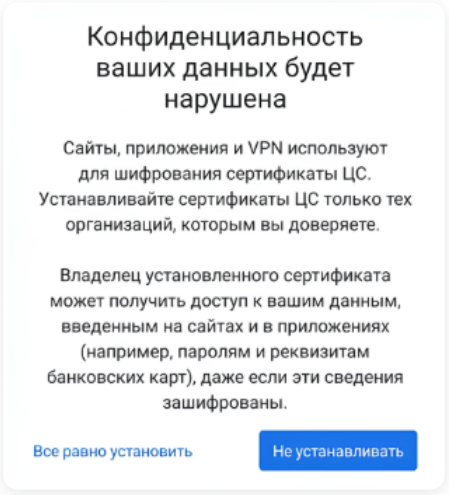


4. Выберите **Сертификат центра сертификации**.

> В зависимости от версии Android и версии оболочки путь может отличаться. Ориентируйтесь на расположение **Пароли и безопасность/ Конфиденциальность/Шифрование и учетные данные**.

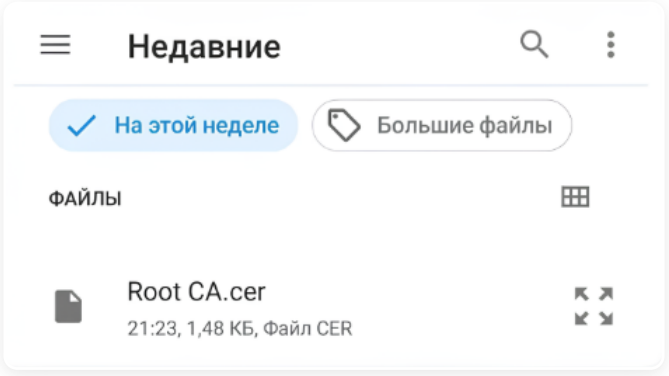
5. Если появится окно **Укажите название сертификата**, введите удобное вам название.

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**.

Как публиковать веб-приложения

Публикация веб-серверов возможна через обратный прокси-сервер.

Сброс пароля IPMI на сервере NGFW

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`. Данный метод позволяет изменить пароль для существующей учетной записи.

Для сброса пароля выполните действия:

Шаг 1. Установка ipmitool

Установка утилиты `ipmitool` на сервер NGFW возможна только через техническую поддержку Ideco.

Шаг 2. Смена пароля

После установки `ipmitool` выполните действия:

1. Для смены пароля потребуется узнать ID пользователя. В терминале NGFW 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 3. 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.

Диагностика проблем

Ошибка при открытии сайта "ERR_CONNECTION_TIMED_OUT" или "Не открывается сайт"

Перейти >

Что делать, если не работает интернет

Перейти >

Ошибка при авторизации "The browser is outdated"

Перейти >

Если соединение по IPsec не устанавливается

Перейти >

Ошибка "400 Bad Request Request Header Or Cookie Too Large" при авторизации в браузерах

Перейти >

Продолжая использовать сайт, вы даёте согласие на использование cookie. Мы используем cookie для повышения удобства пользования сайтом, улучшения пользовательского опыта и других целей, предусмотренных политикой обработки персональных данных.

OK

Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Видеоинструкцию смотрите по ссылкам:

- Youtube
- docs.ideco.ru

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.

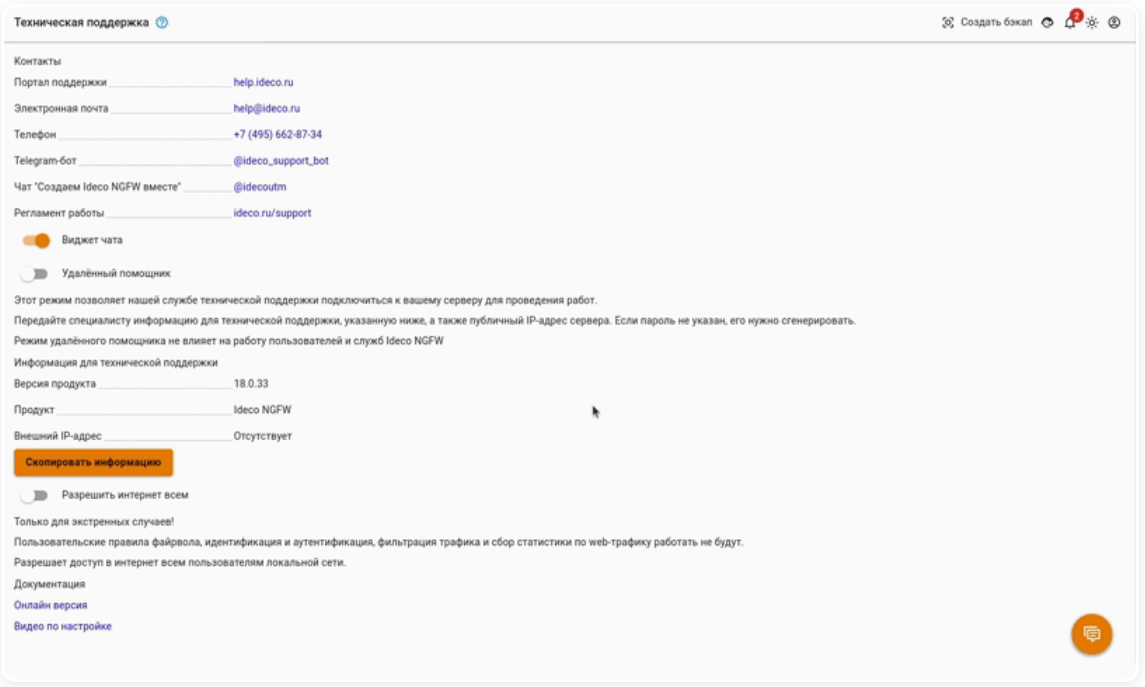
Откройте сайт с устройства вне локальной сети NGFW. Например, со смартфона через мобильный интернет. Если сайт доступен, перейдите в веб-интерфейс NGFW.

Для определения модуля фильтрации, блокирующего сайт, можно проверить логи в разделах Системный журнал. Это может помочь определить причину возникшей проблемы и более точно ее диагностировать.

Шаг 1. Проверьте, открывается ли сайт в режиме **Разрешить интернет всем**

1. Нажмите на в верхней правой части веб-интерфейса NGFW.

2. Переведите опцию **Разрешить интернет всем** в положение **Включен**:



3. Откройте сайт.

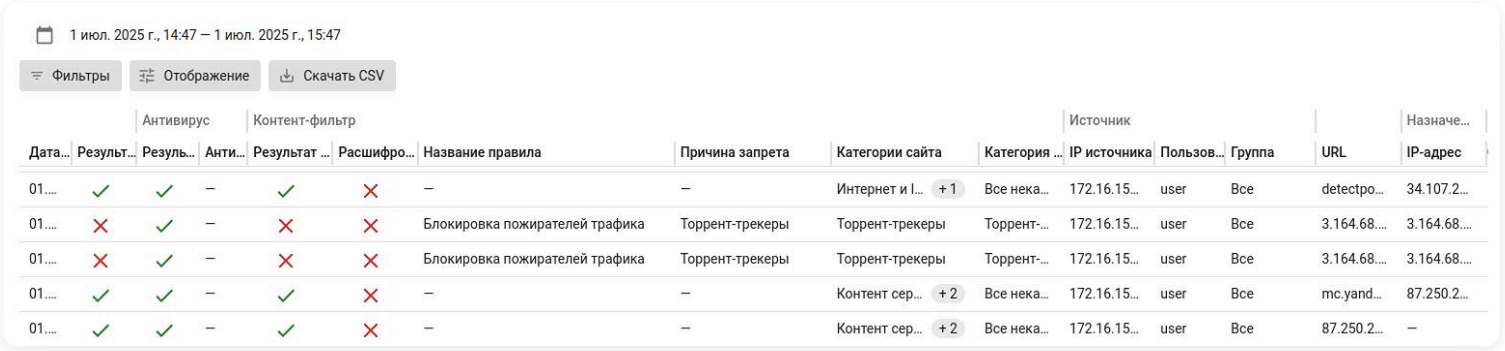
Если сайт не открывается, проверьте, откроется ли сайт на другом устройстве с того же IP-адреса:

- Если не открывается, рекомендуем обратиться к провайдеру. Скорее всего, провайдер блокирует IP-адрес или адрес сайта;
- Если сайт открывается, проверьте настройки устройства пользователя.

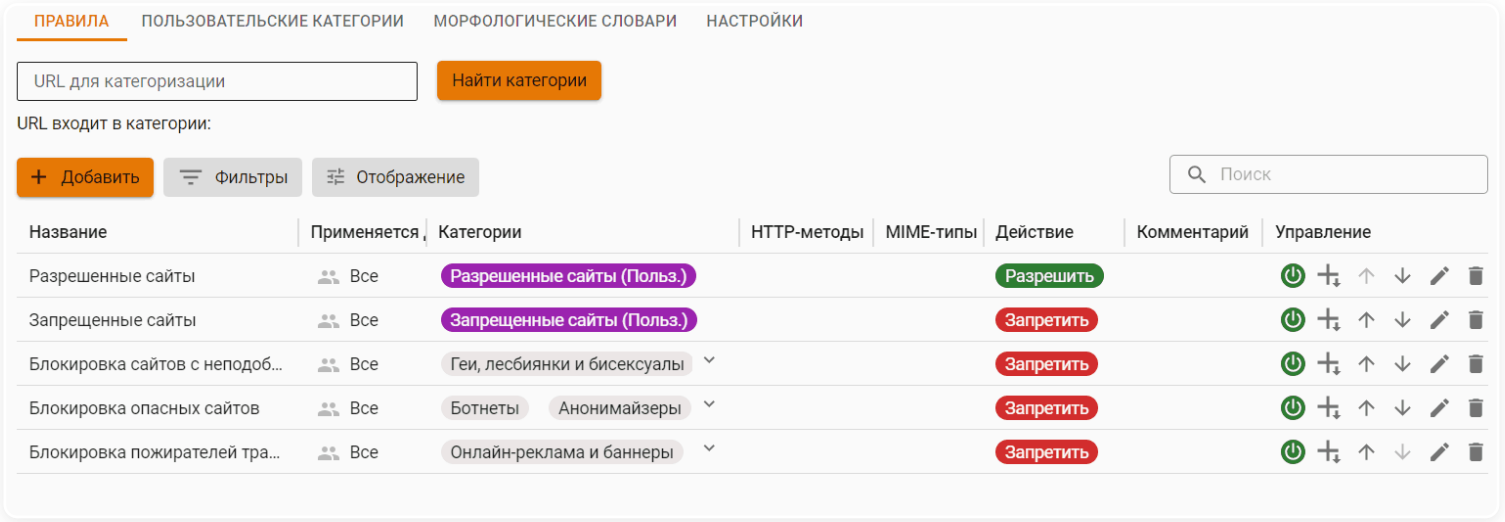
Шаг 2. Проверьте, не блокируется ли сайт правилом Контент-фильтра

1. Откройте сайт с устройства пользователя.

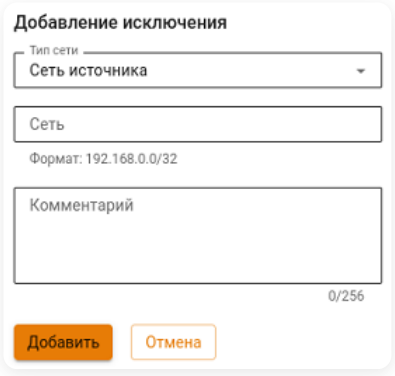
2. В NGFW перейдите в раздел **Отчеты и журналы** → **Журнал веб-трафика** и посмотрите, какое правило блокирует сайт:



3. Для поиска блокирующего правила также можно ввести URL сайта в строку поиска категорий **Контент-фильтра** на вкладке **Правила** в разделе **Правила трафика** → **Контент-фильтр**:



4. Если сайт блокируется правилом **Контент-фильтра**, измените его настройки или добавьте сайт в исключения в разделе **Сервисы** → **Прокси** на вкладке **Исключения**:



В раздел **Сервисы** → **Прокси** → **Исключения** рекомендуем добавлять заведомо надежные сервисы.

Добавлять в исключения адреса клиентов вашей сети не рекомендуется, так как в этом случае их веб-трафик не будет фильтроваться правилами **Контент-фильтра** и не будет попадать в отчеты.

Шаг 3. Проверьте, не блокирует ли сайт правило **Файрвола**

Найдите блокирующее правило одним из способов:

Первый способ. Счетчик срабатываний

1. Перейдите в раздел **Правила трафика** → **Файрвол** → **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 раздел **Правила трафика** → **Файрвол** → **FORWARD**.

2. Создайте тестовое правило, разрешающее любой трафик:

3. Правило добавится в конец таблицы. Поместите созданное правило на одну позицию вверх, нажав на кнопку .

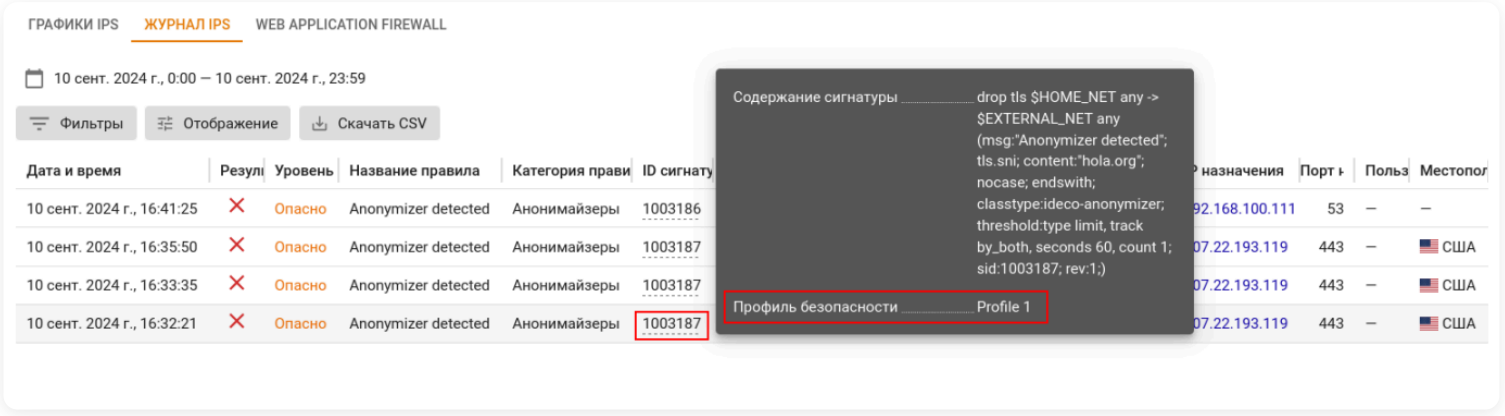
4. Откройте сайт с устройства пользователя.

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:

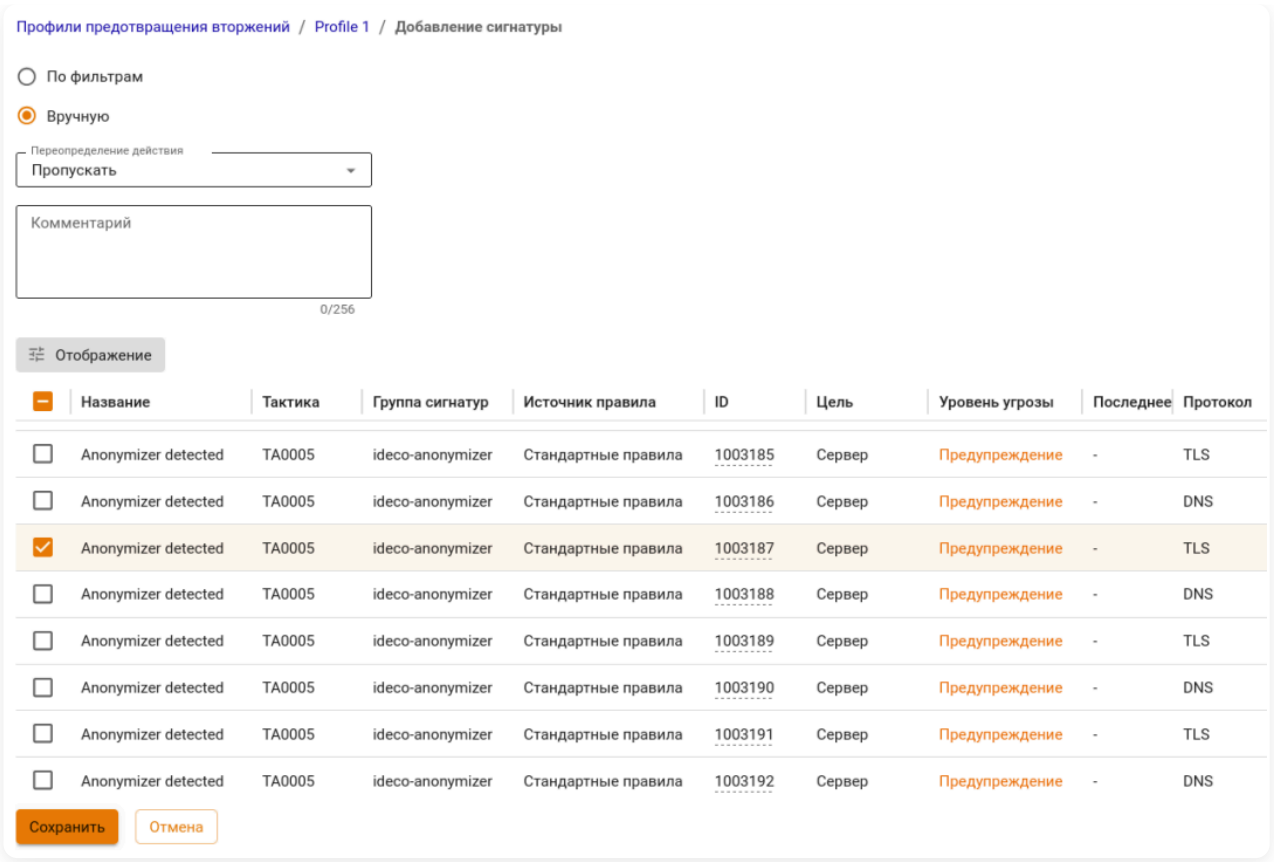
1. Перейдите в раздел **Отчеты и журналы** → **События безопасности** на вкладку **Журнал IPS** и найдите в таблице ID сигнатуры, заблокировавшей сайт, и название профиля, к которому она относится:



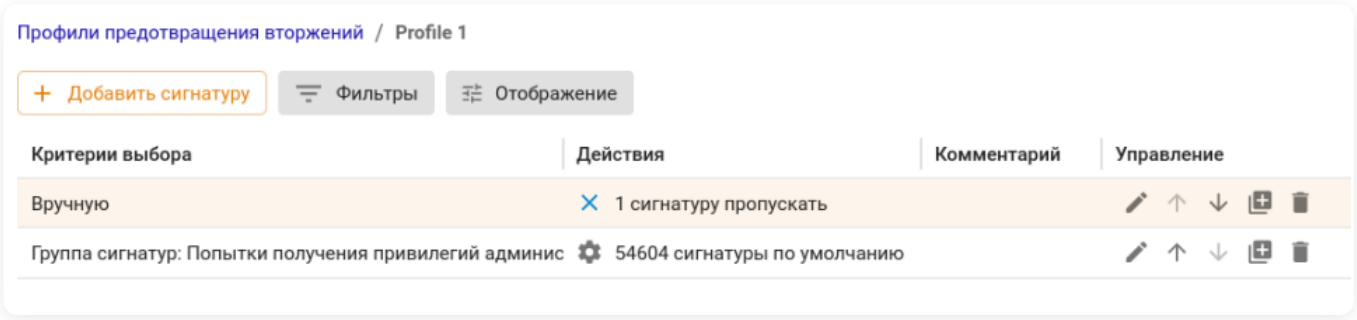
2. Перейдите в раздел **Профили безопасности** → **Предотвращение вторжений**, нажмите на напротив профиля, заблокировавшего сайт, и выберите **Сигнатуры**.

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 раздел **Отчеты и журналы** → **Трафик**.

2. В виджете **Топ заблокированных протоколов** найдите протоколы, которые блокируются **Контролем приложений**.

3. Перейдите в раздел **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 раздел **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 у пользователей отсутствует интернет, выполните шаги для диагностики и решения проблемы.

Шаг 1. Проверьте лицензию

Перейдите в раздел **Управление сервером** → **Лицензия** и проверьте, привязана ли лицензия к серверу.

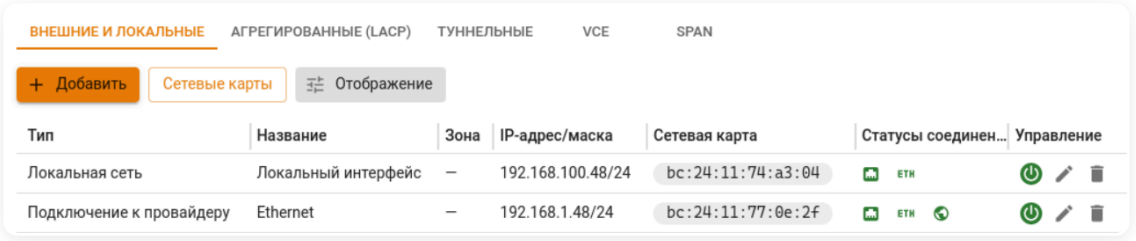
Шаг 2. Проверьте настройки Файрвола

Перейдите в раздел **Правила трафика** → **Файрвол** и отключите в разделах **FORWARD** и **INPUT** правила, запрещающие все.

Шаг 3. Проверьте настройки интерфейсов

Проверьте, правильно ли настроен внешний интерфейс

Перейдите в **Сервисы** → **Сетевые интерфейсы**. Если Ideco NGFW использует выделенный интерфейс для подключения к провайдеру и не работает только как прокси, установите тип **Подключение к провайдеру**. При типе **Локальный интерфейс** удалите и добавьте интерфейс заново с типом **Подключение к провайдеру**:



Проверьте статус подключения

В созданном подключении иконка должна быть , в ином случае:

1. Проверьте настройку VLAN:

- Если провайдер требует VLAN, убедитесь, что тег указан.
- Если в реквизитах провайдера VLAN не указан, убедитесь, что тег не указан.

2. Проверьте ICMP-запросы.

Выполните команду `ping` до адреса, указанного в разделе **Сервисы** → **Балансировка и резервирование** → **Адреса для проверки связи**. Если провайдер блокирует ICMP-запросы, то значок останется , Ideco NGFW не сможет построить внешние маршруты, и интернет работать не будет. В этом случае:

- Удалите все адреса из списка.
- 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 Разрешить интернет всем

> Используйте опцию только для диагностики.

В правой верхней части окна Ideco NGFW нажмите на иконку технической поддержки,а затем нажмите **Разрешить интернет всем**. После включения:

- Сбор веб-статистики будет отключен.

- Пользователям будет разрешен доступ в интернет без авторизации.
- Будет включён автоматический SNAT для пользователей, обращающихся в интернет.
- Не будут работать пользовательские правила **Файрвола** и DNAT.

Цикл обработки трафика в Ideco NGFW описан в статье.

Если интернет появился, то проблема в неверно настроенной авторизации, правилах файрвола или маршрутизации.

Шаг 5. Проверьте настройки пользователей

Проверьте авторизацию пользователей

- В Ideco NGFW 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 Active Directory должны быть выгружены в Ideco NGFW.
- Интеграция с RADIUS должна быть настроена.
- Сопоставление IP-адреса и пользователя не требуется для авторизации пользователей терминального сервера через прямой прокси.

Проверьте тип авторизации

Если пользователь успешно авторизован в системе, то проверьте, какой тип авторизации используют:

- Если используется **MAC и IP+MAC авторизация**, то на компьютере клиента шлюзом по умолчанию должен быть указан Ideco NGFW. Если шлюз не настроен корректно, авторизация не будет работать.
- Если используется **Веб-аутентификация**, то пользователю необходимо открыть браузер и попытаться перейти на любой внешний сайт (например, google.com).
- Если используется **Авторизация по логам**, то проверьте настройки на стороне контроллера домена. Не рекомендуем использовать этот тип авторизации.

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 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 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

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 >= 90;
- Firefox версия >= 78;
- Safari версия >= 14.

Рекомендуем обновить браузер до минимально поддерживаемой версии.

Для продолжения авторизации несмотря на риски потребуется нажать **I understand the risks and wish to continue**.

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 раздел **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.

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:

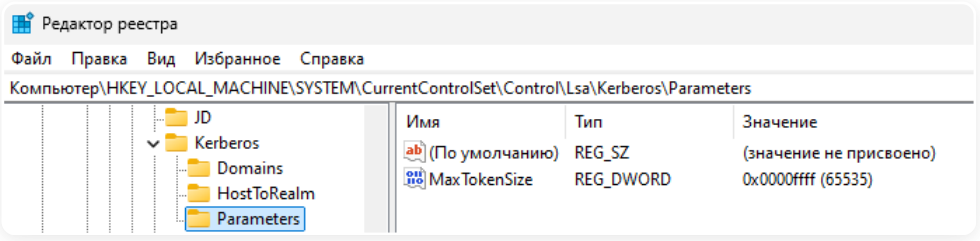
- **Windows 7 и Windows Server 2008R2** - 12000 байт;
- **Windows 8 и Windows Server 2012 (включая Windows Server 2022 и Windows 11)** - 48000 байт.

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
```

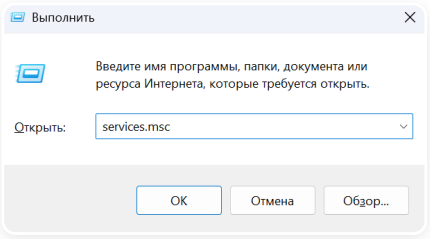
Как включить режим отладки для Ideco Client

При возникновении ошибки в работе Ideco Client включите режим отладки для записи подробных логов. Эти данные помогут в диагностике проблемы и при обращении в техническую поддержку.

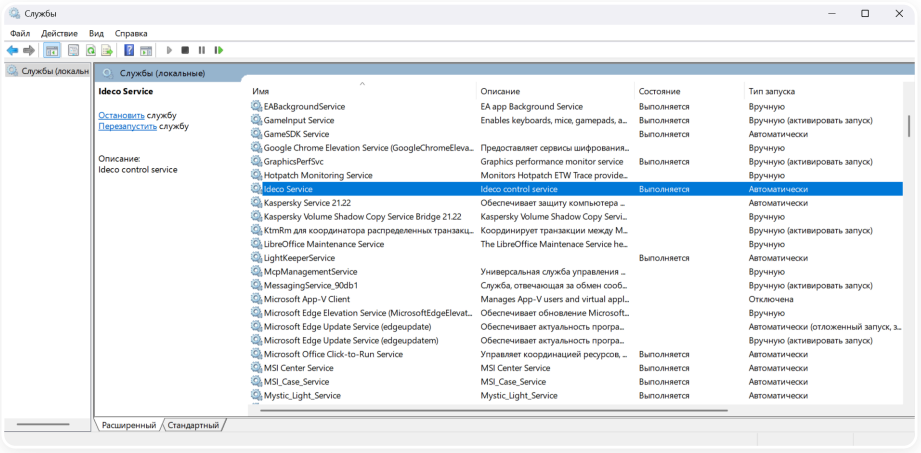
Необходима учетная запись с правами администратора.

Для включения режима:

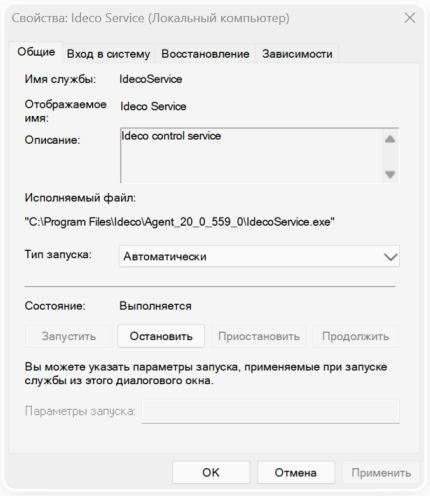
1. Нажмите **Win+R**, введите `services.msc` и нажмите **Ок**:



2. Найдите службу **Ideco Service**:

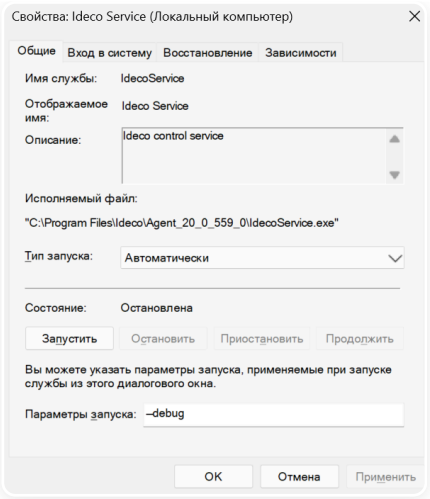


3. Двойным кликом откройте свойства, нажмите **Остановить** и дождитесь остановки службы:



Если произошла ошибка остановки службы, дождитесь запуска службы и остановите службу повторно.

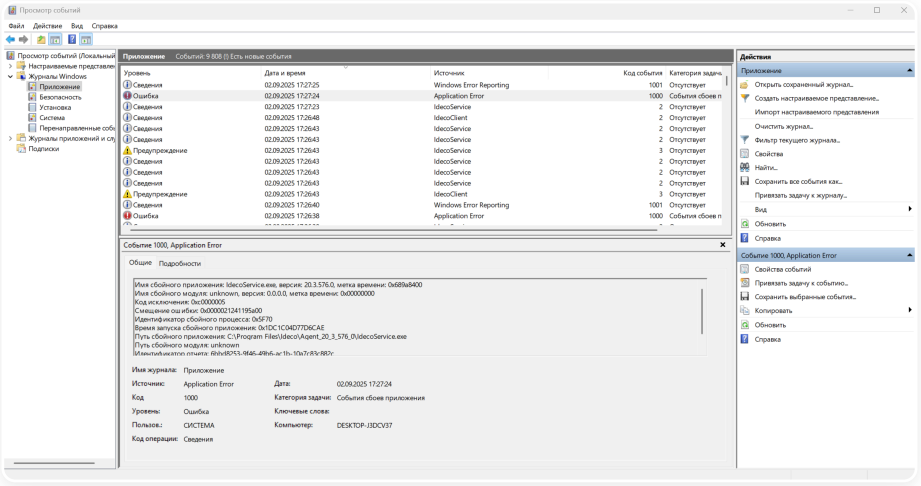
4. В поле **Параметры запуска** введите `--debug` и нажмите **Запустить** для старта службы:



Не закрывайте окно **Свойства: Ideco Service**, иначе режим отладки работать не будет.

5. Запустите Ideco Client, чтобы воспроизвести ошибку.

6. Чтобы посмотреть логи, нажмите **Пуск**, откройте **Просмотр событий**, перейдите в раздел **Журналы Windows** → **Приложения** и найдите запись с ошибкой:



При необходимости обратитесь в техническую поддержку.

Контроль целостности бинарных файлов и целостности конфигурации версии ФСТЭК

Многофункциональный межсетевой экран уровня сети проверяет контрольные суммы исполняемых файлов, входящих в его состав, а также конфигурационных файлов в модуле **etcd** с периодичностью в 30 секунд.

Цели выполнения тестовой процедуры

Подтверждение реализации механизма, обеспечивающего:

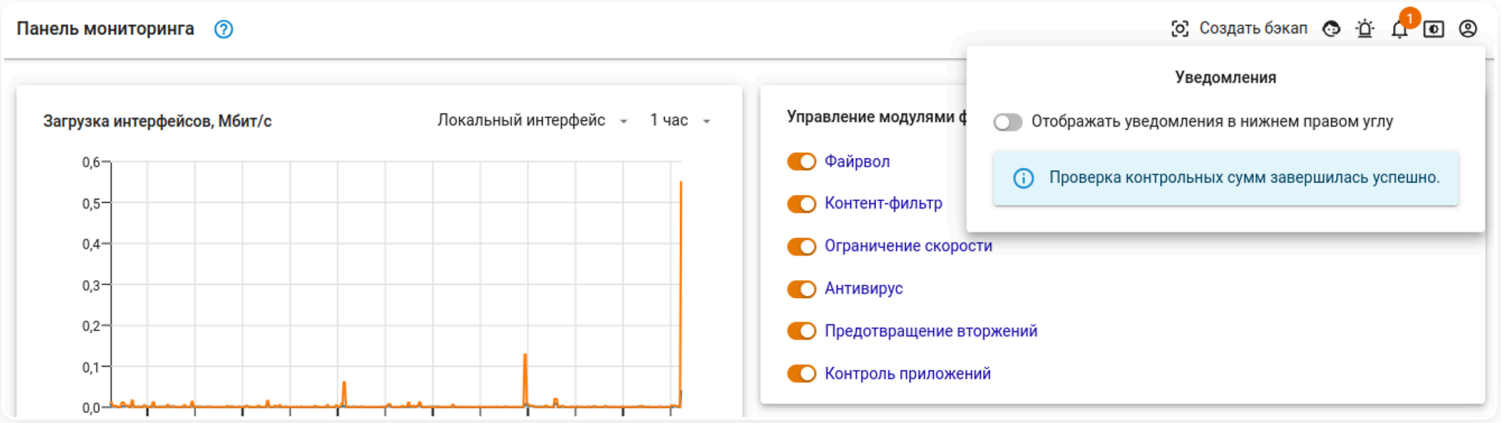
- Запуск программ самотестирования для демонстрации правильного выполнения функций безопасности.
- Возможность верифицировать уполномоченным пользователям целостность данных.
- Возможность верифицировать целостность хранимого выполняемого кода функций безопасности.

Описание тестовой процедуры

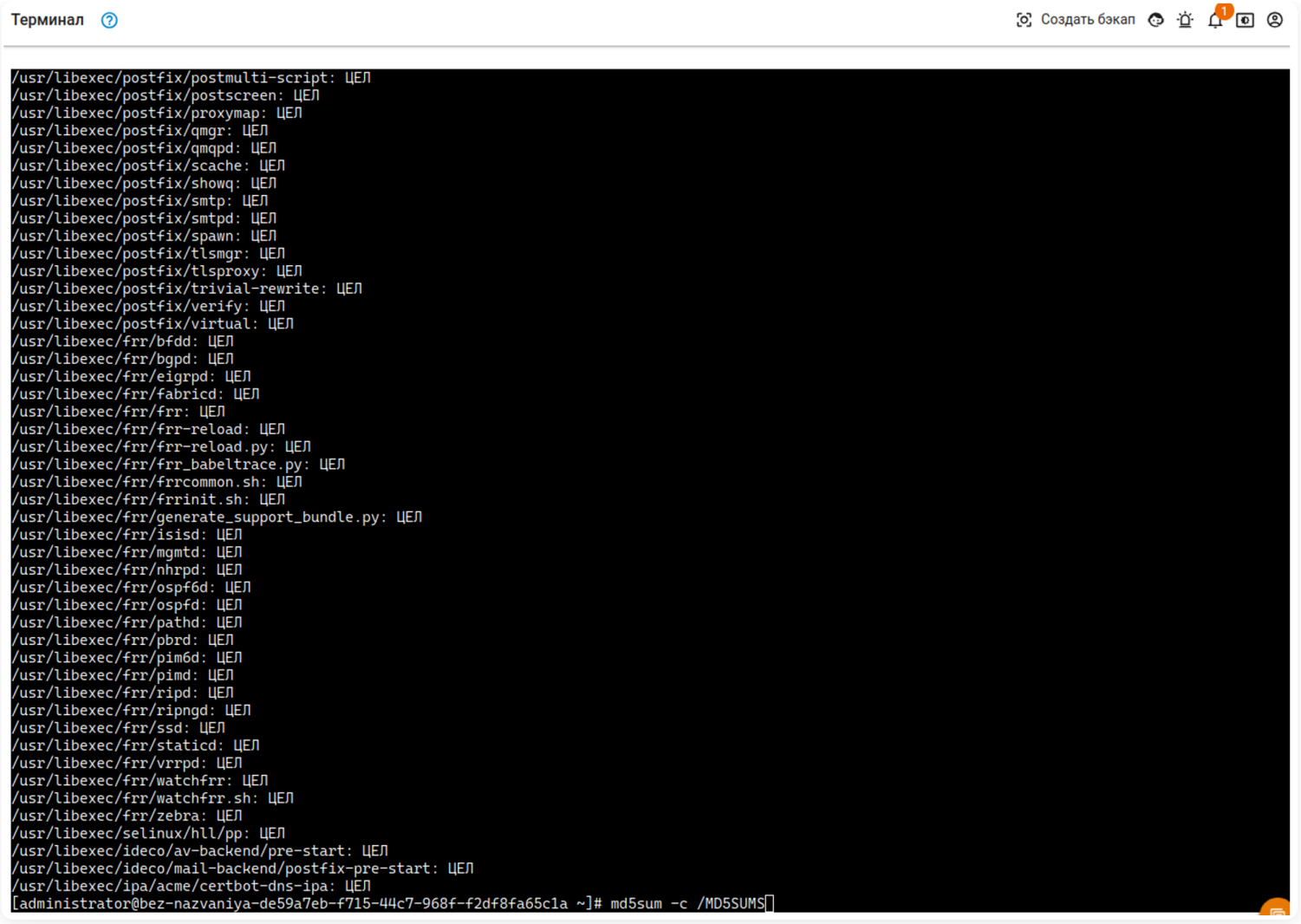
Проверка системы

1. Перезагрузите сервер, на котором работает Ideco NGFW.

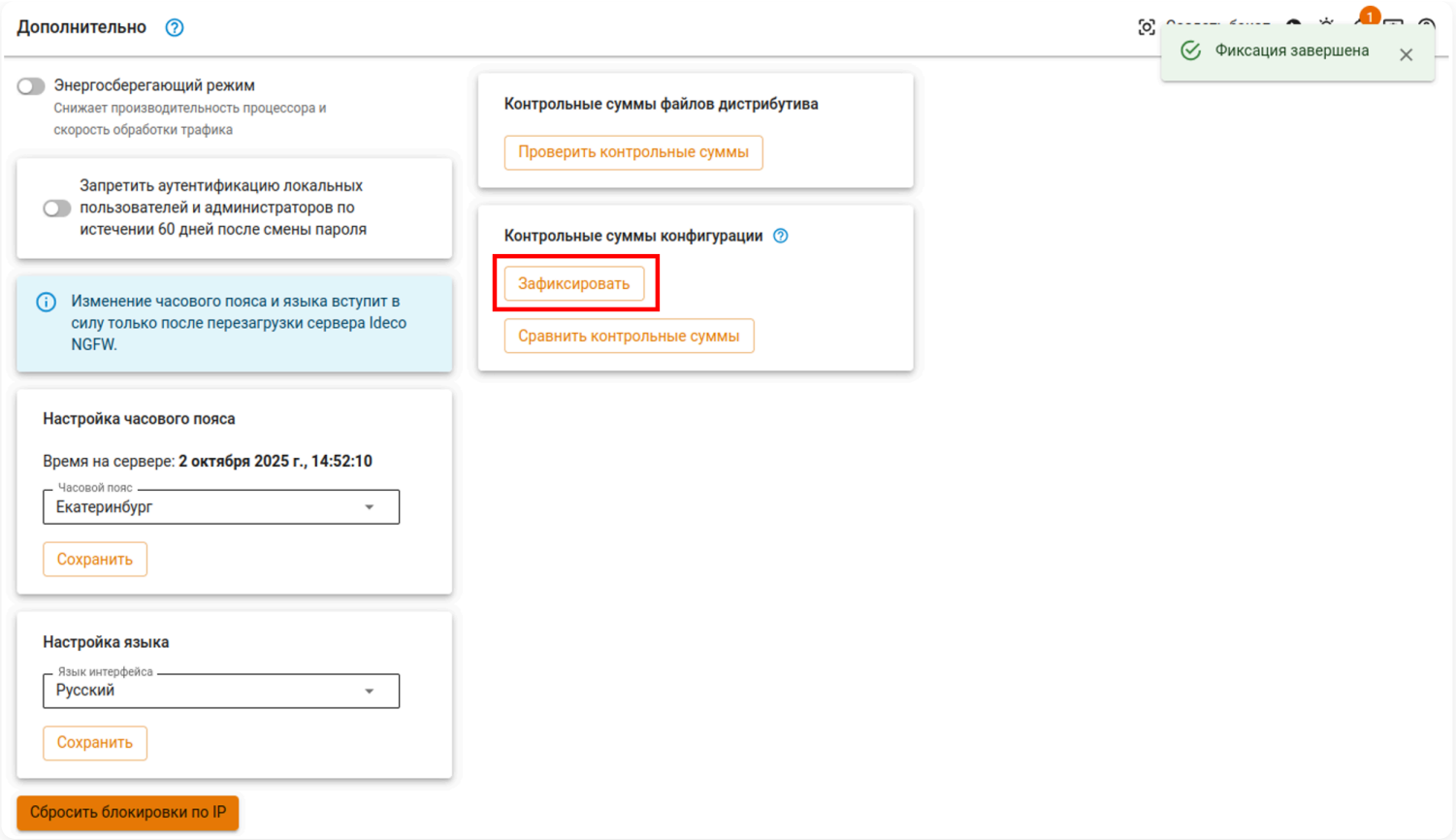
2. Выполните авторизацию в веб-интерфейсе сервера управления Ideco NGFW (`https://192.168.100.2:8443`), используя учетную запись, обладающую ролью **Администратор**. Убедитесь, что по итогу проверки контрольных сумм появляется уведомление **Проверка контрольных сумм завершена успешно**:



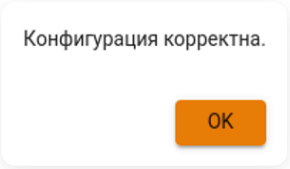
3. Перейдите в **Управление сервером** → **Терминал**. Выполните команду `md5sum -c /MD5SUMS` для проверки неизменности системных файлов. Убедитесь, что команда выполнилась без ошибок:



4. Перейдите в **Управление сервером** → **Дополнительно**. Для проверки неизменности правил фильтрации и настройки параметров NGFW нажмите **Зафиксировать**:

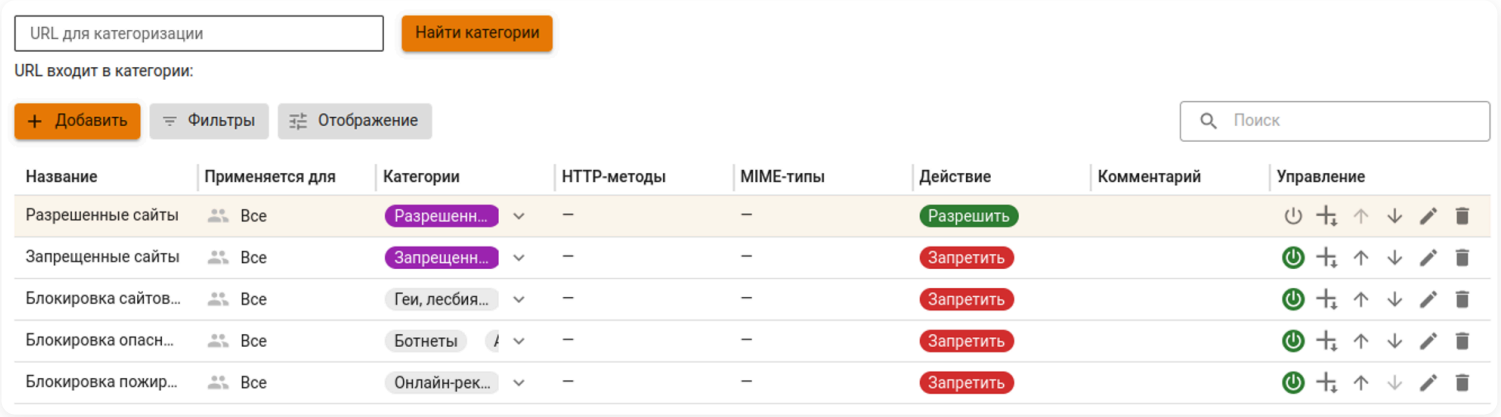


5. Нажмите **Сравнить контрольные суммы**. Убедитесь, что проверка целостности конфигурации завершается успешно:

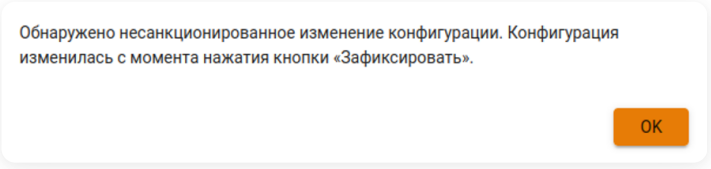


Проверка реакции на изменение конфигурации

1. Перейдите в **Правила трафика** → **Контент-фильтр**. Отключите правило контентной фильтрации:



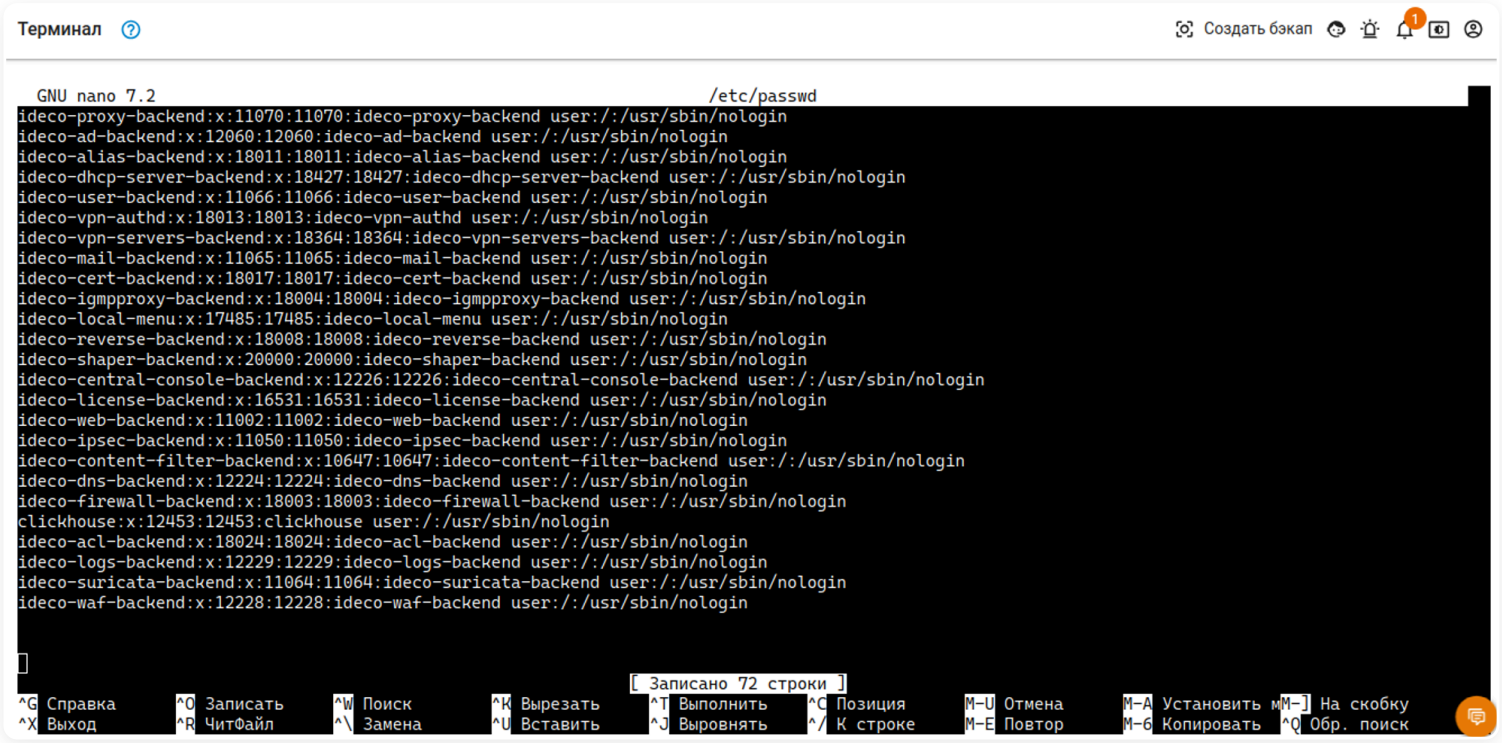
2. Перейдите в **Управление сервером** → **Дополнительно**. Нажмите **Проверить целостность**. Убедитесь, что проверка целостности конфигурации завершается с ошибкой, так как была изменена конфигурация:



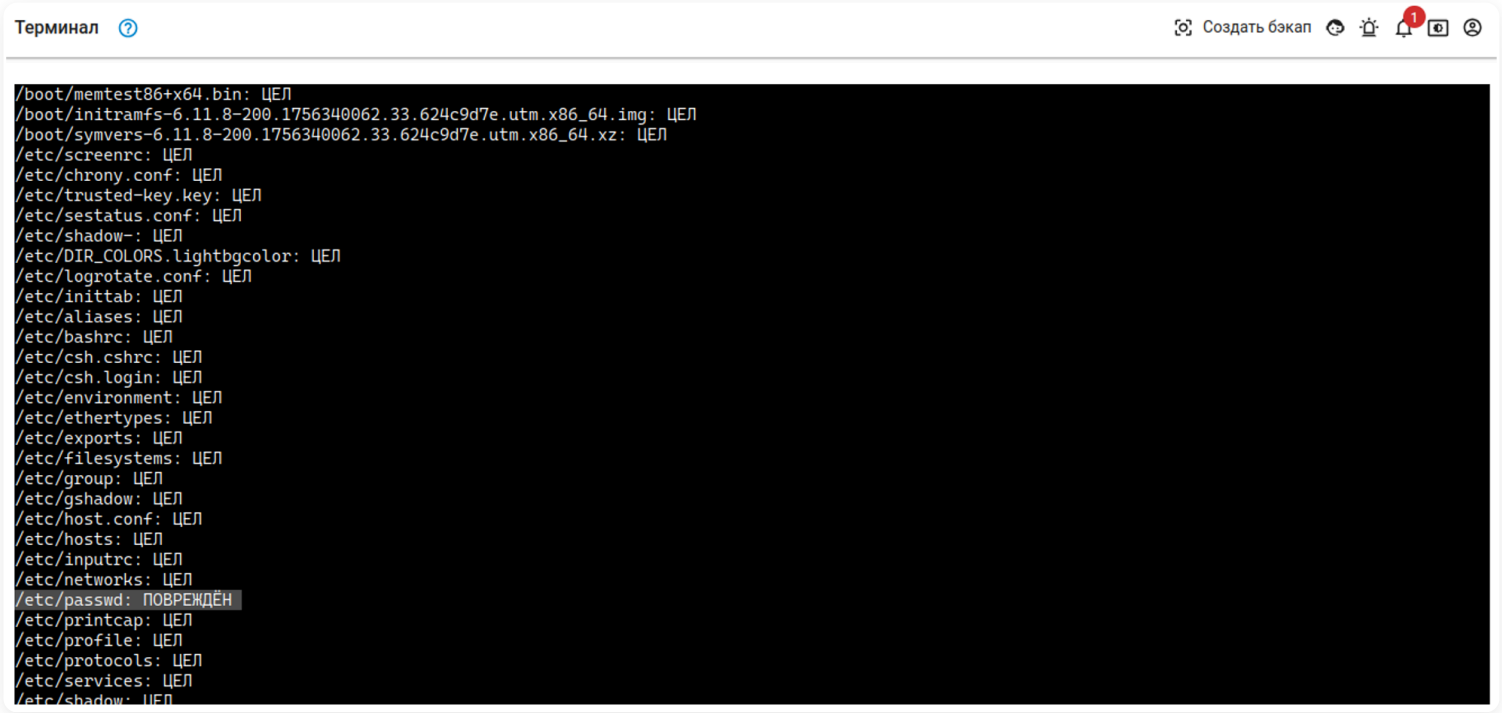
Проверка реакции на изменение системного файла

1. Перейдите в **Управление сервером** → **Терминал**.

2. Добавьте пробел в конец файла `/etc/passwd`:

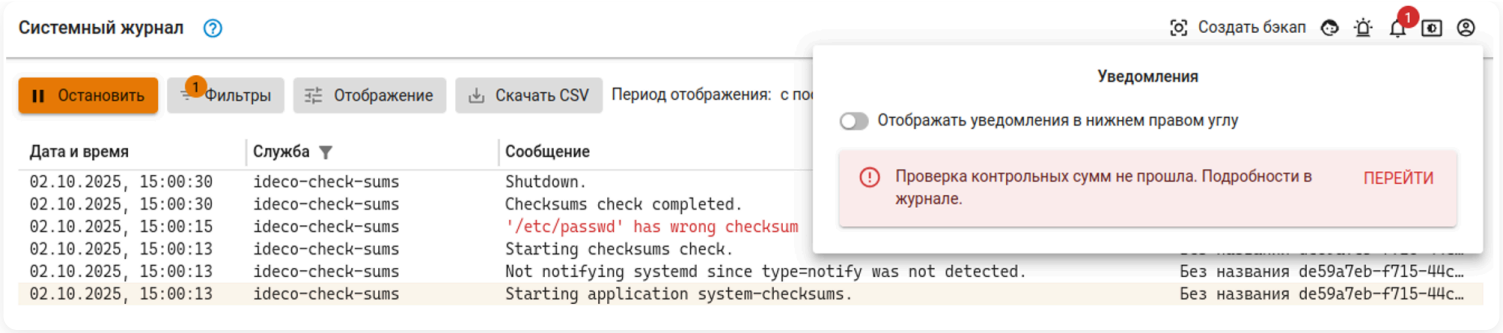


3. Выполните команду `md5sum -c /MD5SUMS`. Убедитесь, что выводится сообщение о нарушении контрольной суммы файла `/etc/passwd`:



4. Перезагрузите Ideco NGFW.

5. После перезагрузки выполните авторизацию в веб-интерфейсе сервера управления Ideco NGFW (`https://192.168.100.2:8443`), используя учетную запись, обладающей ролью **Администратор**. Убедитесь, что по итогу проверки контрольных сумм появляется уведомление **Проверка контрольных сумм завершена с ошибкой**:



6. Завершите сеанс работы с рабочей станцией АРМ.

Критерии успешного выполнения проверки

Результаты выполнения каждого из шагов проверки совпадают с ожидаемыми результатами. Ideco NGFW обеспечивает:

- Выполнение самотестирования при запуске системы.
- Возможность уполномоченным пользователям верифицировать целостность данных.
- Возможность уполномоченным пользователям верифицировать целостность хранимого выполняемого кода функций безопасности.

При необходимости обратитесь в техническую поддержку.

Ideco NGFW 19.X

Примечания к релизу Ideco NGFW 19.0 сборка 634

Дата выхода версии: 12.03.2025.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в телеграмм-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Telegram: ideco.bot

Скачать Ideco NGFW 19.

Автоматическая регистрация тестовой лицензии: my.ideco.ru (полная функциональность на 44 дней и 10 000 пользователей).

Обновление с релизов Ideco UTM 8.12 и старше:

Обновление с релиза Ideco UTM 13 возможно через автоматические обновления (тестовый канал, будет доступна в ближайшее время).

Обновление с релизов 8.x, 9.x, 10.x, 11.x, 12.x возможно через автоматические обновления с промежуточным обновлением до версий 9.11, 10.7, 11.10, 12.8.

После обновлении на Ideco UTM 15 приостанавливается синхронизация с Active Directory, если локальные пользователи Ideco UTM находятся в группах Active Directory.

Обновление с версии Ideco UTM 7.9.9:

Прямое обновление до версии 19 невозможно.

Возможна миграция настроек (загрузка бэкапа настроек) на предварительно установленную версию 9.11 и дальнейшее обновление до версии 18.0 с помощью автоматического обновления.

IDECO NGFW 19.16 сборка 23 (30.01.2026)

Безопасность

- Обновлен модуль системы предотвращения вторжений.

Исправления и изменения

- Повышена стабильность IPsec-подключений.
- Исправлена ошибка при загрузке баз офлайн-обновлений.
- Появилась возможность добавлять правила SNAT для IPsec через веб-интерфейс.
- Доступен раздел **Техническая поддержка** для пользователей с ролью **Администратор Межсетевого экрана**.
- Исправлена проблема доступа в интернет при переопределении действия Flowbit-сигнатуры.
- Косметические изменения веб-интерфейса.

IDECO NGFW 19.13 сборка 22 (23.10.2025)

Безопасность

- Обновлен модуль системы предотвращения вторжений (в том числе исправлена уязвимость CVE-2025-59147/BDU:2025-12460).

Исправления и изменения

- Исправлена работа обратного прокси при добавлении ресурса в ЛК/Портал SSL VPN (только для Ideco NGFW).
- Исправлена валидация ввода IP-адресов и масок.
- Исправлена работа фильтров при поиске по тексту.
- Исправлено некорректное отображение скорости в мониторе трафика.

IDECO NGFW 19.11 сборка 29 (04.09.2025)

Исправления и изменения

- Исправлена работа монитора трафика при большой нагрузке.
- Исправлено излишнее логирование при использовании фильтрации по серым спискам в почтовом релее.
- Улучшено определение приложений модулем Контроль приложений.
- Исправлены проблемы с разрешением имен DNS-сервером в некоторых случаях.
- Исправлены большие задержки трафика в ГОСТ VPN.
- Исправлено создание маршрута для IPsec (доступна настройка адреса источника).
- Обновлен модуль веб-антивируса Касперского.
- Исправлены проблемы при авторизации большого количества пользователей из Active Directory.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.9 сборка 35 (25.07.2025)

Примечания к релизу

Обновление обязательно для использующих модуль антивируса Касперского для веб-трафика из-за обновления общего ключа модуля. Рекомендуем обновиться до 29.07.2025.

Безопасность

- Обновлен модуль системы Предотвращения вторжений (включая исправления CVE-2025-53537, CVE-2025-53538);
- Исправлены потенциальные уязвимости, найденные с помощью статанализа в различных модулях (67 патчей).

Исправления и изменения

- Обновлен ключ антивируса Касперского для проверки веб-трафика (в "старых" версиях будет работать до 29.07.2025);
- Обновлена информация с контактами технической поддержки;
- Исправлена работа с зонами в правилах Файрвола при изменении в интерфейсах;
- Оптимизировано использование ресурсов сервера при использовании WAF при публикации веб-ресурсов;
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.8 сборка 18 (04.07.2025)

Безопасность

- Исправлены потенциальные уязвимости, найденные с помощью фаззинга и статанализа в различных модулях (72 патча).

Исправления и изменения

- Исправлен доступ на сайт rosreestr.gov.ru при включенной расшифровке трафика.
- Повышена стабильность работы Ideco Client.
- Исправлено создание GRE-интерфейса на PPPoE-интерфейсе.
- Исправлена работа чата с технической поддержкой при включенной расшифровке HTTPS-трафика.
- Ускорена работа поиска пользователей при создании правил с большим количеством пользователей.
- Ускорена работа журнала веб-трафика при скроллинге и фильтрации.
- Повышена стабильность модуля авторизации пользователей.
- Исправлена загрузка на серверах Aquarius T40 S33.
- Улучшено логирование правил Файрвола.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.7 сборка 19 (19.06.2025)

Безопасность

- Обновлен модуль веб-почты (исправлена уязвимость CVE-2025-49113).
- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модуле Zabbix.

Исправления и изменения

- Новый виджет онлайн-чата технической поддержки.
- Исправлен доступ к публикации личного кабинета с использованием групп безопасности Active Directory при изменении пользователей в группах.
- Улучшен механизм синхронизации изменений пользователей в группах безопасности Active Directory при использовании групп безопасности в правилах доступа по VPN.
- Исправлено мгновенное восстановление из бэкапов в некоторых ситуациях.
- Исправлена ошибка веб-интерфейса при выключении удаленного помощника.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.6 сборка 66 (04.06.2025)

Безопасность

- Исправлена возможность скачивания бэкапа администратором с ролью "только просмотр".
- Добавлен разрыв установленных SSH-сессий при отключении доступа по SSH или "удаленного помощника".

Исправления и изменения

- Повышена производительность модулей обработки трафика.
- Исправлена работа модуля контроля приложений под нагрузкой.
- Исправлена выгрузка отчетов журнала трафика в CSV при включенных фильтрах.
- Исправлена работа OSPF при переключении провайдеров.
- Добавлена возможность использования "белых" IP-адресов в сети для VPN-подключений.
- Исправлена работа кластера при наличии loopback-интерфейса.
- Исправлена передача цепочки SSL-сертификатов при подключении по SSTP.
- Исправлено действие профиля, применяемое к новым протоколам Контроля приложений при обновлении с 18-ой версии (будет выбрано то же действие, что было назначено протоколу "Unknown").
- Исправлено формирование отчета "Список посещенных адресов" в конструкторе отчетов.
- Исправлена авторизация пользователей доверенных доменов Active Directory.
- Улучшена работа с большим количеством (десятки тысяч) групп безопасности Active Directory.
- Исправлены ошибки в логах после авторизации администратора через RADIUS.
- Исправлено формирование больших отчетов по трафику в CSV.
- Из системного журнала убраны логи контроля приложений (в 19-ой версии они есть в Журнале трафика).
- Ускорено обновление кластера.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.5 сборка 19 (24.04.2025)

Безопасность

- Исправлена уязвимость CVE-2024-11236 (актуальна при использовании веб-почты в NGFW).
- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модулях BGP и DNS-сервере.
- Исправлено отображение учетных данных администратора в тексте ошибки при окончании сессии администратора VCE.

Исправления и изменения

- Исправлено обновление с прошлых версий при наличии активных VCE.
- Исправлено обновление с прошлых версий при особенностях UEFI на сервере.
- Исправлено отображение диапазонов портов в правилах Файрвола.
- Исправлено скачивание баз Контент-фильтра при выключенном модуле контентной фильтрации.
- Добавлена возможность, позволяющая интегрировать Ideco NGFW в домен Microsoft Windows 2025 (при возникновении ошибки входа в домен необходимо выполнить в терминале NGFW команду `touch /run/ideco-ad-backend/ldap-passwd`).
- Повышена надежность БД отчетности.
- Исправлена обработка событий изменения наличия пользователя в группах безопасности AD/ALD для сессий личного кабинета (теперь при удалении пользователя из группы для которой предоставлен доступ сессия будет автоматически разрываться).
- Исправлено создание кластера при наличии loopback-интерфейсов.

- Небольшие исправления веб-интерфейса и логирования служб.

IDECO NGFW 19.3 сборка 19 (8.04.2025)

Безопасность

- Исправлено потенциальное раскрытие информации в логах при использовании VCE.
- Обновлен модуль системы Предотвращения вторжений (исправлены уязвимости CVE-2025-29915, CVE-2025-29917, CVE-2025-29918, CVE-2025-29916).
- Обновлен модуль OpenSSH (исправлена уязвимость CVE-2025-26466).

Исправления и изменения

- Исправлено сообщение при блокировке по словарю морфологического анализа.
- Исправлены проблемы аутентификации пользователей ALD/Samba по VPN.
- Исправлена ошибочная блокировка доп. запросов сайта при правиле, блокирующем все запросы в Контент-фильтре.
- Добавлен порт 8090 для прямых подключений к прокси-серверу.
- Повышена производительность Файрвола.
- Исправлено накопление временных файлов обновлений Контент-фильтра (при появлении нового обновления во время скачивания "старого").
- Исправлена 2FA для пользователей из RADIUS.
- Исправлена работа правила DNAT с использованием зоны источника.
- Исправлены падения службы Контроля приложений при некоторых условиях.
- Косметические исправления веб-интерфейса.

IDECO NGFW 19.0 сборка 634 (12.03.2025)

Новая функциональность

- Структурированный Журнал трафика: Файрвол (включая DNAT и SNAT), IPS, Контроль приложений.
- Netflow-сенсор для передачи информации netflow-коллектору.
- Портал SSL VPN (публикация HTTPS-, HTTP-, SSH-, RDP-ресурсов).
- Отправка журналов на Ideco Center.
- ГОСТ VPN для site-to-site между Ideco NGFW.
- Аппаратная фильтрация трафика по MAC-адресам (для поддерживаемых сетевых карт).
- Обработка трафика Файрволом на основе ACL (настраивается по API): до 100 000 записей суммарно во всех ACL, максимальное количество записей в одном ACL - 10 000.

Ideco Client

- 2FA в интерфейсе Ideco Client.
- Балансировка подключений к серверам.
- Подключение к доступным серверам перебором SRV-записей в DNS.
- Кастомная настройка конфигурации: запрет “сохранения пароля”, предустановленные профили, настройка профиля по-умолчанию.
- Улучшенное журналирование подключения в Системный журнал.

Сеть

- Возможность использования пула IP-адресов для SNAT.
- Loopback-интерфейс для GRE-, GRE/IPsec-туннелей.
- Возможность фильтрации трафика между локальными интерфейсами с помощью профилей Контроля приложений и Предотвращения вторжений.

Оптимизации

- Ускорена работа с большим количеством объектов Active Directory.
- Ускорена работа веб-интерфейса с большим количеством пользователей и правил.
- Уменьшено потребление ОЗУ модулями.
- Добавлена поддержка ESN в IPSec (лучше производительность при больших объемах трафика).
- Ускорена установка.

Обновления

- Обновлено ядро Linux (до версии 6.11) и ключевые используемые пакеты.
- Обновлен модуль Контроля приложений.
- Обновлен модуль Предотвращения вторжений.

Разное

- Убран модуль Квоты для работы с квотами трафика.
- Добавлено поле Комментарий в разделе Мониторинг аренды DHCP-сервера.
- Возможность добавления системных доверенных сертификатов.
- В логах авторизации пользователей теперь указывается и логин.
- Добавлена кнопка Сбросить блокировки по IP в разделе **Управление сервером → Дополнительно**.
- Добавлена колонка Расположение в Мониторинг сессий администраторов (по GeoIP).
- Возможность публикации веб-интерфейса как внутреннего сервиса через Обратный прокси-сервер.
- Возможность указания конкретного контроллера домена Active Directory для подключения NGFW.
- Добавлена возможность восстановления на предыдущую версию из раздела Обновления.
- Возможность аутентификации пользователей из Active Directory по RADIUS.
- В антиспаме Касперского включена проверка SPF и DMARC для лучшей фильтрации спама и фишинговых писем.
- При включении заблокированного пользователя в Active Directory он разблокируется в Ideco NGFW (ранее нужно было разблокировать вручную). Отключена возможность ручной блокировки авторизации пользователей Active Directory в Ideco NGFW.
- Добавлена возможность выключения Теста скорости для Личного кабинета пользователей.
- Многочисленные исправления и улучшения веб-интерфейса.

ФСТЭК Ideco UTM 19.X

Описание сертифицированной версии

Примечания к релизу ФСТЭК Ideco UTM 19.1 сборка 51

Дата выхода версии: 28.03.2025.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в телеграм-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Telegram: ideco.bot

Для ФСТЭК-версии включено автоматическое обновление с версии 11.13 путем нескольких обновлений: 11.13 → 12.11 → 13.11 → 14.3 → 15.7 → 16.9 → 17.7 → 18.7 → 19.1.

Обязательно нужно последовательно обновиться и использовать версию 19.1 (не останавливаясь на промежуточных версиях, нужных только для обновления).

С 19 версии профили Контроля приложений и Предотвращения вторжений проверяют и локальный сетевой трафик между сегментами (могут его блокировать в зависимости от настроек правил Файрвола). Проверьте настройки фильтрации трафика после обновления. В версии содержатся важные исправления безопасности компонентов.

ФСТЭК Ideco UTM 19.16 сборка 22 (30.01.2026)

Безопасность

- Обновлен модуль системы предотвращения вторжений.

Исправления и изменения

- Повышена стабильность IPsec-подключений.
- Исправлена ошибка при загрузке баз офлайн-обновлений.
- Появилась возможность добавлять правила SNAT для IPsec через веб-интерфейс.
- Доступен раздел **Техническая поддержка** для пользователей с ролью **Администратор Межсетевого экрана**.
- Исправлена проблема доступа в интернет при переопределении действия Flowbit-сигнатуры.
- Косметические изменения веб-интерфейса.

ФСТЭК Ideco UTM 19.14 сборка 45 (11.12.2025)

Безопасность

- Обновлен модуль системы предотвращения вторжений (в том числе исправлены уязвимости CVE-2025-64344, CVE-2025-64333, CVE-2025-64332, CVE-2025-64331, CVE-2025-64330).
- Исправлена уязвимость CVE-2025-62168/BDU:2025-13226 в модуле прокси-сервера.
- Исправлено некорректное логирование правил Межсетевого экрана с действием **Запретить** при отключенном SSH на внешних интерфейсах.

Исправления и изменения

- Восстановлено переключение нод при отключении внешнего/локального линка на активной ноде при использовании VLAN.
- Исправлена некорректная расшифровка TLS 1.3 при обращении по IP-адресу в **Контент-фильтре**.
- Ограничена роль **Администратор Межсетевого экрана** в некоторых разделах (Почтовый релей, Ограничение скорости, Управление сервером, Обратный прокси и др.).
- Параметр KDC-сервер переименован в DC-сервер.
- Восстановлена работа SIP-телефонии при перезагрузке или обновлении Ideco.

ФСТЭК Ideco UTM 19.13 сборка 23 (23.10.2025)

Безопасность

- Обновлен модуль системы предотвращения вторжений (в том числе исправлена уязвимость CVE-2025-59147/BDU:2025-12460).

Исправления и изменения

- Исправлена работа обратного прокси при добавлении ресурса в ЛК/Портал SSL VPN (только для Ideco NGFW).
- Исправлена валидация ввода IP-адресов и масок.
- Исправлена работа фильтров при поиске по тексту.
- Исправлено некорректное отображение скорости в мониторе трафика.

ФСТЭК Ideco UTM 19.12 сборка 4 (10.09.2025)

Исправления и изменения

- Исправлена работа монитора трафика при большой нагрузке.
- Исправлено излишнее логирование при использовании фильтрации по серым спискам в почтовом релее.
- Улучшено определение приложений модулем Контроль приложений.
- Исправлены проблемы с разрешением имен DNS-сервером в некоторых случаях.
- Исправлено создание маршрута для IPsec (доступна настройка адреса источника).
- Исправлены проблемы при авторизации большого количества пользователей из Active Directory.
- Косметические исправления веб-интерфейса.

ФСТЭК Ideco UTM 19.10 сборка 2 (28.07.2025)

Безопасность

- Обновлен модуль системы Предотвращения вторжений (включая исправления CVE-2025-53537, CVE-2025-53538);
- Исправлены потенциальные уязвимости, найденные с помощью статанализа в различных модулях (67 патчей).

Исправления и изменения

- Обновлена информация с контактами технической поддержки;
- Исправлена работа с зонами в правилах файрвола при изменении в интерфейсах;
- Косметические исправления веб-интерфейса.

ФСТЭК Ideco UTM 19.8 сборка 19 (04.07.2025)

Безопасность

- Исправлены потенциальные уязвимости, найденные с помощью фаззинга и статанализа в различных модулях (72 патча).

Исправления и изменения

- Исправлен доступ на сайт rosreestr.gov.ru при включенной расшифровке трафика.
- Исправлено создание GRE-интерфейса на PPPoE-интерфейсе.
- Исправлена работа чата с технической поддержкой при включенной расшифровке HTTPS-трафика.
- Ускорена работа поиска пользователей при создании правил при большом количестве пользователей.
- Ускорена работа журнала веб-трафика при скроллинге и фильтрации.
- Повышена стабильность модуля авторизации пользователей.
- Исправлена загрузка на серверах Aquarius T40 S33.
- Улучшено логирование правил файрвола.
- Косметические исправления веб-интерфейса.

ФСТЭК Ideco UTM 19.7 сборка 20 (19.06.2025)

Безопасность

- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модуле Zabbix.

Исправления и изменения

- Новый виджет онлайн-чата технической поддержки.
- Исправлен доступ к публикации личного кабинета с использованием групп безопасности Active Directory при изменении пользователей в группах.
- Улучшен механизм синхронизации изменений пользователей в группах безопасности Active Directory при использовании групп безопасности в правилах доступа по VPN.
- Исправлено мгновенное восстановление из бэкапов в некоторых ситуациях.
- Исправлена ошибка веб-интерфейса при выключении удаленного помощника.
- Косметические исправления веб-интерфейса.

ФСТЭК IDECO UTM 19.6 сборка 67 (04.06.2025)

Безопасность

- Исправлена возможность скачивания бэкапа администратором с ролью "только просмотр".
- Добавлен разрыв установленных SSH-сессий при отключении доступа по SSH или "удаленного помощника".

Исправления и изменения

- Повышена производительность модулей обработки трафика.
- Исправлена работа модуля контроля приложений под нагрузкой.
- Исправлена выгрузка отчетов журнала трафика в CSV при включенных фильтрах.
- Исправлена работа OSPF при переключении провайдеров.
- Добавлена возможность использования "белых" IP-адресов в сети для VPN-подключений.
- Исправлена работа кластера при наличии loopback-интерфейса.
- Исправлена передача цепочки SSL-сертификатов при подключении по SSTP.
- Исправлено действие профиля, применяемое к новым протоколам Контроля приложений при обновлении с 18-ой версии (будет выбрано то же действие, что было назначено протоколу "Unknown").
- Исправлено формирование отчета "Список посещенных адресов" в конструкторе отчетов.
- Исправлена авторизация пользователей доверенных доменов Active Directory.
- Улучшена работа с большим количеством (десятки тысяч) групп безопасности Active Directory.
- Исправлены ошибки в логах после авторизации администратора через RADIUS.
- Исправлено формирование больших отчетов по трафику в CSV.
- Из системного журнала убраны логи контроля приложений (в 19-ой версии они есть в Журнале трафика).
- Ускорено обновление кластера.
- Косметические исправления веб-интерфейса.

ФСТЭК IDECO UTM 19.5 сборка 20 (24.04.2025)

Безопасность

- Обновлен модуль системы Предотвращения вторжений (исправлены уязвимости CVE-2025-29915, CVE-2025-29917, CVE-2025-29918, CVE-2025-29916).
- Обновлен модуль OpenSSH (исправлена уязвимость CVE-2025-26466).
- Исправлены потенциальные уязвимости, найденные с помощью фаззинга в модулях BGP и DNS-сервере.

Исправления и изменения

- Исправлено сообщение при блокировке по словарю морфологического анализа.
- Исправлены проблемы аутентификации пользователей ALD/Samba по VPN.
- Добавлен порт 8090 для прямых подключений к прокси-серверу.
- Исправлено накопление временных файлов обновлений Контент-фильтра (при появлении нового обновления во время скачивания "старого").
- Исправлена 2FA для пользователей из RADIUS.
- Исправлена работа правила DNAT с использованием зоны источника.
- Исправлены падения службы Контроля приложений при некоторых условиях.
- Исправлено скачивание баз Контент-фильтра при выключенном модуле контентной фильтрации.
- Исправлено создание кластера при наличии loopback-интерфейсов.

- Добавлена возможность, позволяющая интегрировать Ideco UTM в домен Microsoft Windows 2025 (при возникновении ошибки входа в домен необходимо выполнить в терминале NGFW команду `touch /run/ideco-ad-backend/ldap-passwd`).
- Повышена надежность БД отчетности.
- Косметические исправления веб-интерфейса.

ФСТЭК IDECO UTM 19.1 сборка 51 (28.03.2025)

Новая функциональность

- Структурированный Журнал трафика: Файрвол (включая DNAT и SNAT), IPS, Контроль приложений.
- Netflow-сенсор для передачи информации netflow-коллектору.
- Отправка журналов на Ideco Center.
- Аппаратная фильтрация трафика по MAC-адресам (для поддерживаемых сетевых карт).
- Обработка трафика файрволом на основе ACL (настраивается по API): до 100 000 записей суммарно во всех ACL, максимальное количество записей в одном ACL - 10 000.
- Виртуальные контексты VCE.

Сеть

- Возможность использования пула IP-адресов для SNAT.
- Loopback-интерфейс для GRE, GRE/IPsec-туннелей.
- Возможность фильтрации трафика между локальными интерфейсами с помощью профилей Контроля приложений и IPS.

Оптимизации

- Ускорена работа с большим количеством объектов Active Directory.
- Ускорена работа веб-интерфейса с большим количеством пользователей и правил.
- Уменьшено потребление ОЗУ модулями.
- Добавлена поддержка ESN в IPSec (лучше производительность при больших объемах трафика).
- Ускорена установка.
- Ускорена обработка трафика Файрволом.

Обновления

- Обновлено ядро Linux (до версии 6.11) и ключевые используемые пакеты.
- Обновлен модуль Контроля приложений.
- Обновлен модуль Предотвращения вторжений (в т.ч. исправлены все известные уязвимости).

Разное

- Убран модуль Квоты для работы с квотами трафика.
- Добавлено поле Комментарий в разделе Мониторинг аренды DHCP-сервера.
- Возможность добавления системных доверенных сертификатов.
- В логах авторизации пользователей теперь указывается и логин.
- Добавлена кнопка Сбросить блокировки по IP в меню Управление сервером → Дополнительно.
- Добавлена колонка Расположение в Мониторинг сессий администраторов (по GeoIP).
- Возможность публикации веб-интерфейса как внутреннего сервиса через Обратный прокси-сервер.
- Возможность указания конкретного контроллера домена Active Directory для подключения UTM.
- Добавлена возможность восстановления на предыдущую версию из раздела Обновления.
- Возможность аутентификации пользователей из Active Directory по RADIUS.
- При включении заблокированного пользователя в Active Directory он разблокируется в Ideco UTM (ранее нужно было разблокировать вручную). Отключена возможность ручной "блокировки" авторизации пользователей Active Directory в Ideco UTM.
- Многочисленные исправления и улучшения веб-интерфейса.

Новое в документации

Февраль 2026

Популярные инструкции и диагностика проблем

Как избежать проблем с подключением VPN-клиентов при использовании нескольких серверов Ideco NGFW

Настройка корневого и подчиненного центра сертификации с помощью AD CS

Использование собственного CA-сертификата в Контент-фильтре

Январь 2026

Общая информация

Настройка двухфакторной аутентификации с использованием TOTP-токенов

Обратная связь

Популярные инструкции и диагностика проблем

Сброс пароля IPMI на сервере NGFW Novum