Лицензирование

> В статье представлено описание доступных в Ideco Center лицензий.

Лицензия Ideco Center позволяет управлять доступом к функциям централизованного администрирования серверов Ideco Center. Если два Ideco Center объединяются в кластер, то на каждую ноду нужно приобретать отдельную лицензию.

Виды лицензий

В Ideco Center доступны лицензии:

- **Enterprise** - коммерческая лицензия.
- **Enterprise-demo** - бесплатная лицензия сроком на 44 дня. Формируется автоматически при регистрации сервера в MY.IDECO.

Подробнее о привязке лицензий - в статье.

После добавления лицензии модуль подключения к Ideco Center включается в лицензию Ideco NGFW и обеспечивает передачу политик и настроек из Ideco Center на серверы Ideco NGFW.

Подробнее о лицензиях в Ideco NGFW - в статье.

По истечении срока действия модуля:

- Политики и настройки, уже распространенные на Ideco NGFW, сохраняются и продолжают действовать.
- Новые настройки из Ideco Center не распространяются на Ideco NGFW до продления модуля.

Просмотр информации о лицензиях

Посмотреть информацию о лицензии можно:

- В MY.IDECO в разделе **Ideco Center**, нажав напротив нужного сервера.
- В Ideco Center в разделе **Управление сервером** → **Лицензия**.

Лицензия содержит сведения:

- Номер лицензии
- Тип лицензии
- Дата начала действия лицензии
- Окончание лицензии
- Окончание обновлений
- Окончание технической поддержки
- Количество пользователей
- Название компании
- Название сервера

Техническая поддержка

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

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

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

График работы

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

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

Способы обращения

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

Правила обращения

Техническая поддержка пользователей осуществляется в соответствии с регламентом.

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

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

Скачивание журнала системных событий

В веб-интерфейсе Ideco Center доступно скачивание журнала системных событий для передачи в техническую поддержку.

Журнал помогает диагностировать неудачное обновление: если после перехода на новую версию возникли проблемы и был выполнен возврат на предыдущую версию, журнал сохранит события проблемной версии. Эти данные помогают технической поддержке определить причину сбоя, даже когда продукт уже работает на прежней версии.

Для скачивания нажмите в правом верхнем углу экрана, а затем **Скачать** в блоке **Журнал событий системы**:

Журнал событий системы

Архив содержит записи системных событий. Отправьте его для анализа в техподдержку.

Скачать

Начнется загрузка архива в формате **zst**. Состав журнала зависит от того, выполнялся ли возврат к предыдущей версии:

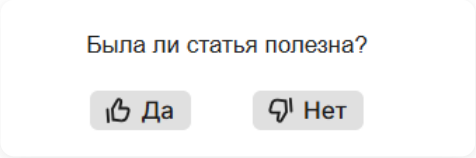
- Если установка первичная или возврата к предыдущей версии не было, файл содержит события текущей версии.
- Если был возврат к предыдущей версии, файл содержит события версии, с которой произошел возврат, и события текущей версии.

Обратная связь

Мы постоянно совершенствуем нашу документацию и всегда рады вашим отзывам.

Как оставить отзыв:

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

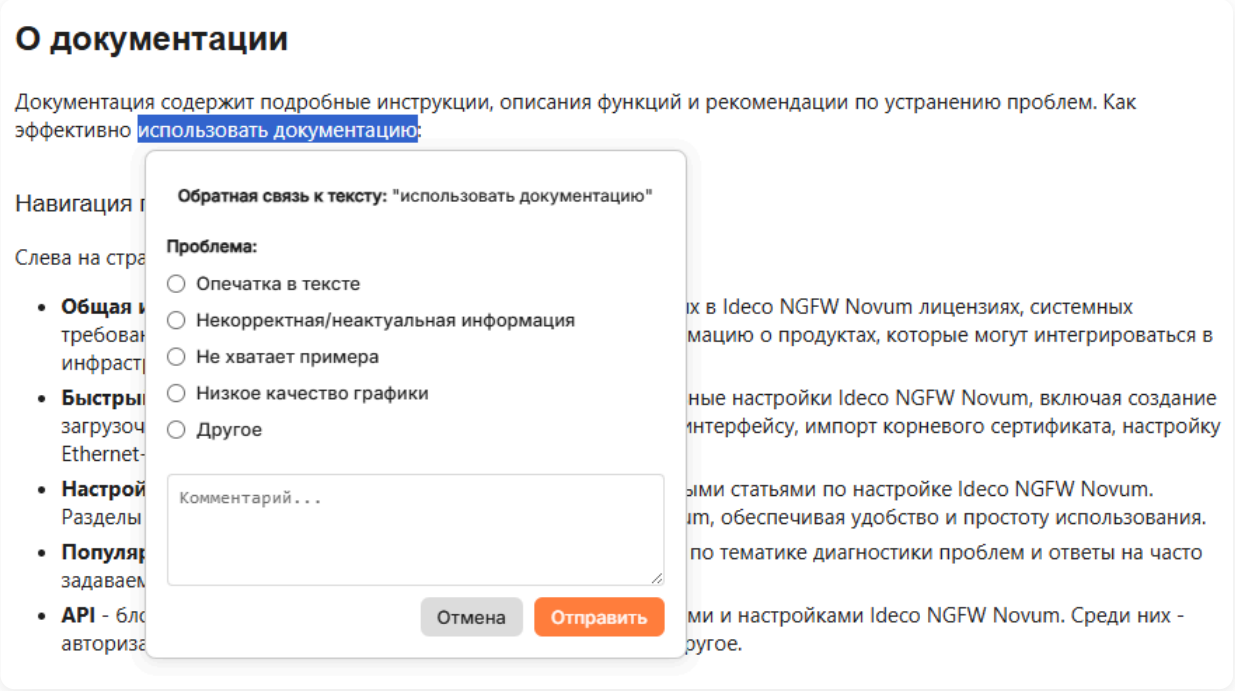


- Написать комментарий к фрагменту текста внутри статьи.

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

Чтобы написать комментарий:

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



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

3. Нажмите **Отправить**.

Описание Ideco Center

Название службы раздела **Ideco Center**: `ideco-central-console-backend`.

Список служб для других разделов доступен по ссылке.

Ideco Center - центральная консоль для управления несколькими серверами Ideco NGFW. Ideco Center автоматически распространяет политики безопасности на все подключенные Ideco NGFW.

Ideco NGFW Novum подключается к Ideco Center по порту 3151 в двух протоколах:

Протокол и порт	Назначение
TCP/3151	Подключение NGFW Novum и синхронизация объектов, правил и политик безопасности
UDP/3151	Туннель WireGuard: синхронизация базы данных отчетов и журналов с NGFW Novum и переход в его веб-интерфейс

Оба порта должны быть открыты на Ideco Center или перенаправлены на него через NAT. Если открыт только TCP/3151, NGFW Novum подключится и получит настройки, но синхронизация базы данных отчетов и журналов и переход в веб-интерфейс NGFW Novum работать не будут.

Подключение всегда устанавливает NGFW Novum, поэтому открывать входящие порты на стороне NGFW Novum не требуется.

Возможности Ideco Center

- ✅ Централизованное управление серверами Ideco NGFW, подключенными к Ideco Center
- ✅ Разделение по группам серверов Ideco NGFW
- ✅ Формирование иерархии из групп Ideco NGFW
- ✅ Создание объектов, политик и профилей безопасности и их назначение серверам Ideco NGFW
- ✅ Переход из Ideco Center в веб-интерфейс подключенных Ideco NGFW. Администраторы Ideco Center имеют доступ к подключенным Ideco NGFW, но администраторы подключенных Ideco NGFW не имеют доступа к Ideco Center
- ✅ Интеграция с Microsoft Active Directory/Samba DC

Подробнее о работе политик безопасности и объектов - в статьях Правила трафика и Объекты.

Источники данных Ideco Center

Ideco Center может обращаться к адресам для получения данных:

Тип запроса	Адрес
Отправка уведомлений в личный кабинет/телеграм-бот	api.ideco.ru
Обновление баз Контент-фильтра	• content-filter.v22.ideco.dev • mcs-vmc1.ideco.ru • mcs-vmc2.ideco.ru • mcs-vmc4.ideco.ru
Отправка анонимной статистики	gatherstat.v22.ideco.dev
Обновления баз GeoIP	• ip-list.v22.ideco.dev • mcs-vm.ideco.ru
Отправка отчетов по почте	api.ideco.ru
Обновления сигнатур IDS/IPS	suricata.v22.ideco.dev
Обновления системы	• api.ideco.ru • storage.yandexcloud.net
Синхронизация времени	ntp.ideco.ru

Чтобы все модули фильтрации Ideco Center работали правильно, доступ к указанным ресурсам должен быть разрешен в настройках.

Настройка гипервизора

Особенности

- Если при установке Ideco Center появилось окно с текстом **Installation in BIOS mode is not supported**, включите режим UEFI в настройках гипервизора.
- Не рекомендуем использовать LACP на виртуальных сетевых адаптерах в Center, так как системы виртуализации часто требуют нетривиальной настройки для работы LACP или вообще не поддерживают этот режим. Рекомендуем настраивать агрегацию каналов средствами гипервизора. Если сетевые карты проброшены в виртуальную машину на уровне PCI (PCI passthrough), LACP можно настраивать внутри Center.

Для обеспечения отказоустойчивости используются 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.

VMware ESXi 6.7

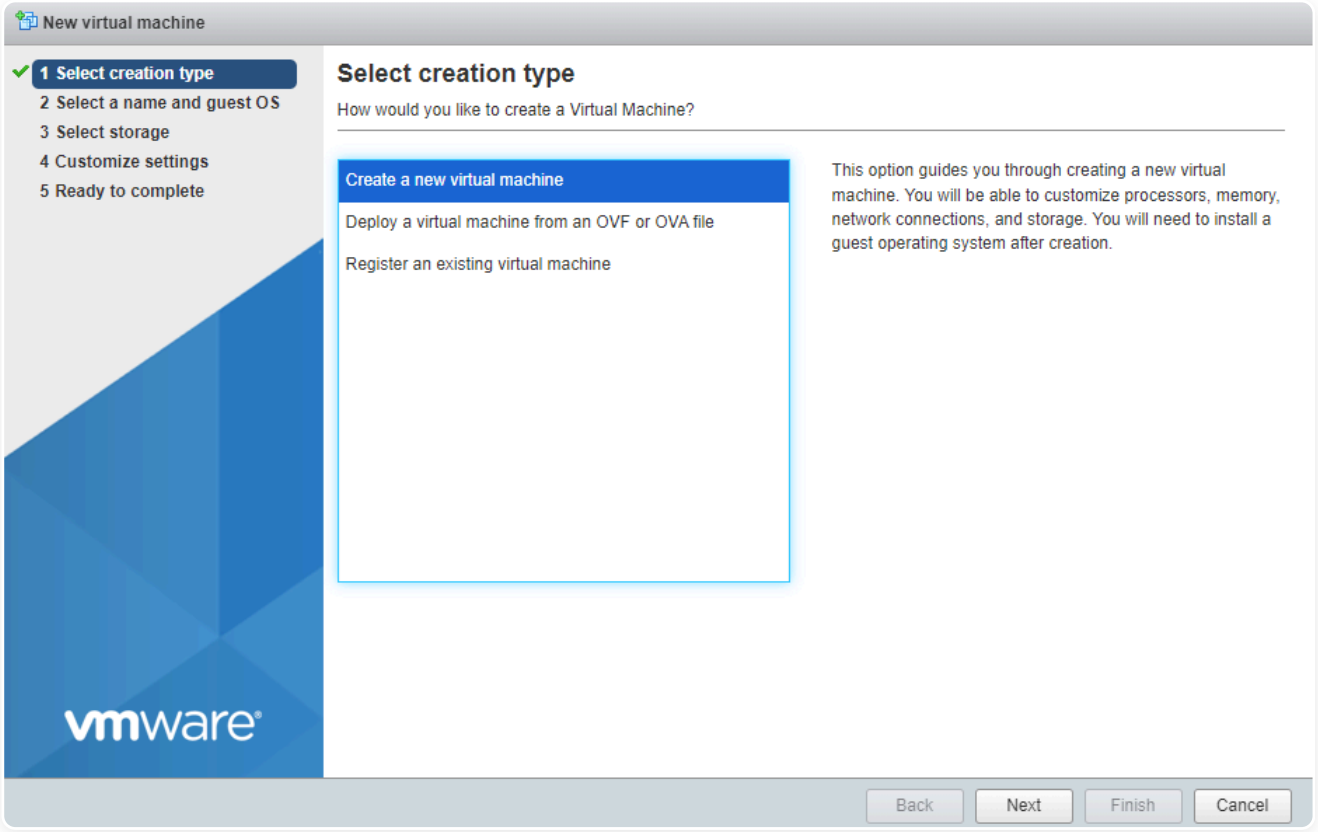
При установке Ideco Center на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

Настройка

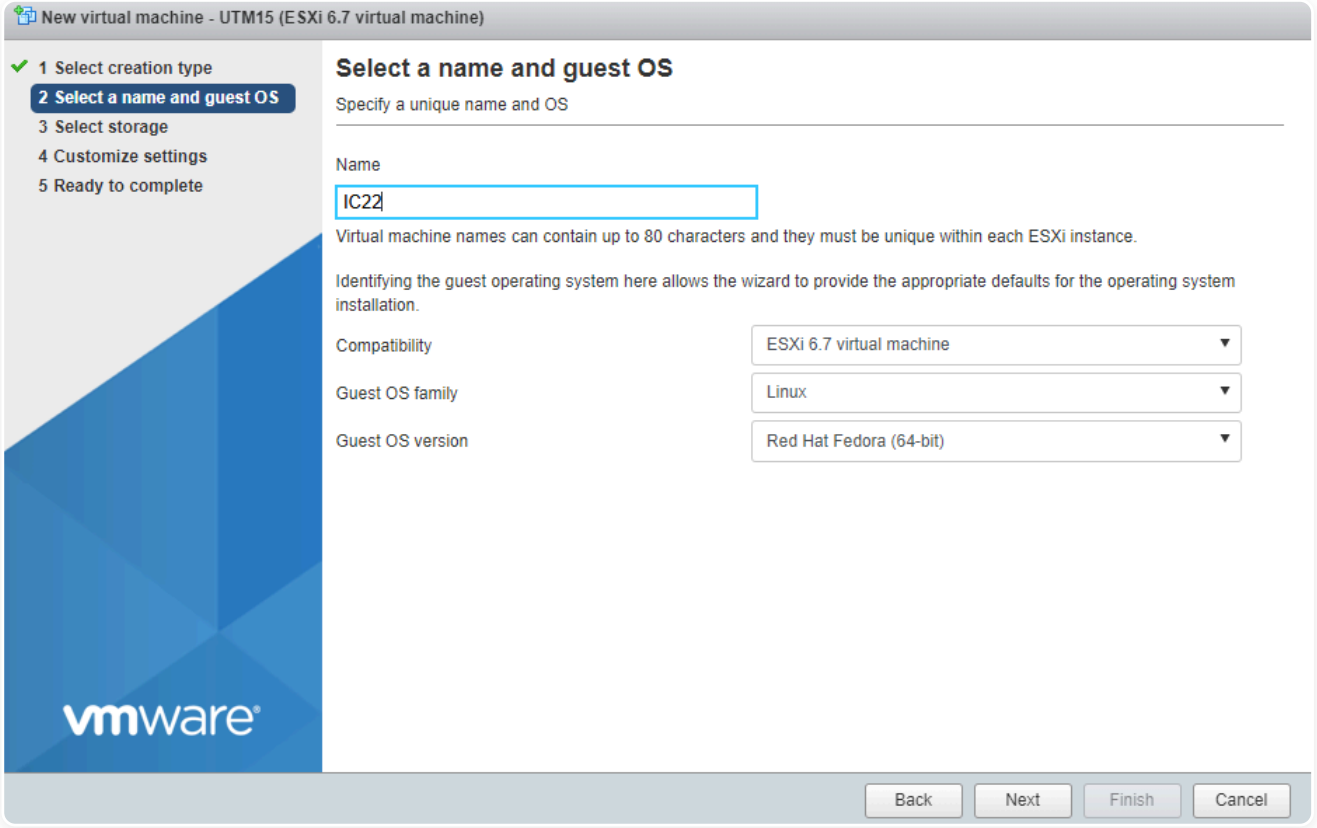
Перед установкой Ideco Center:

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

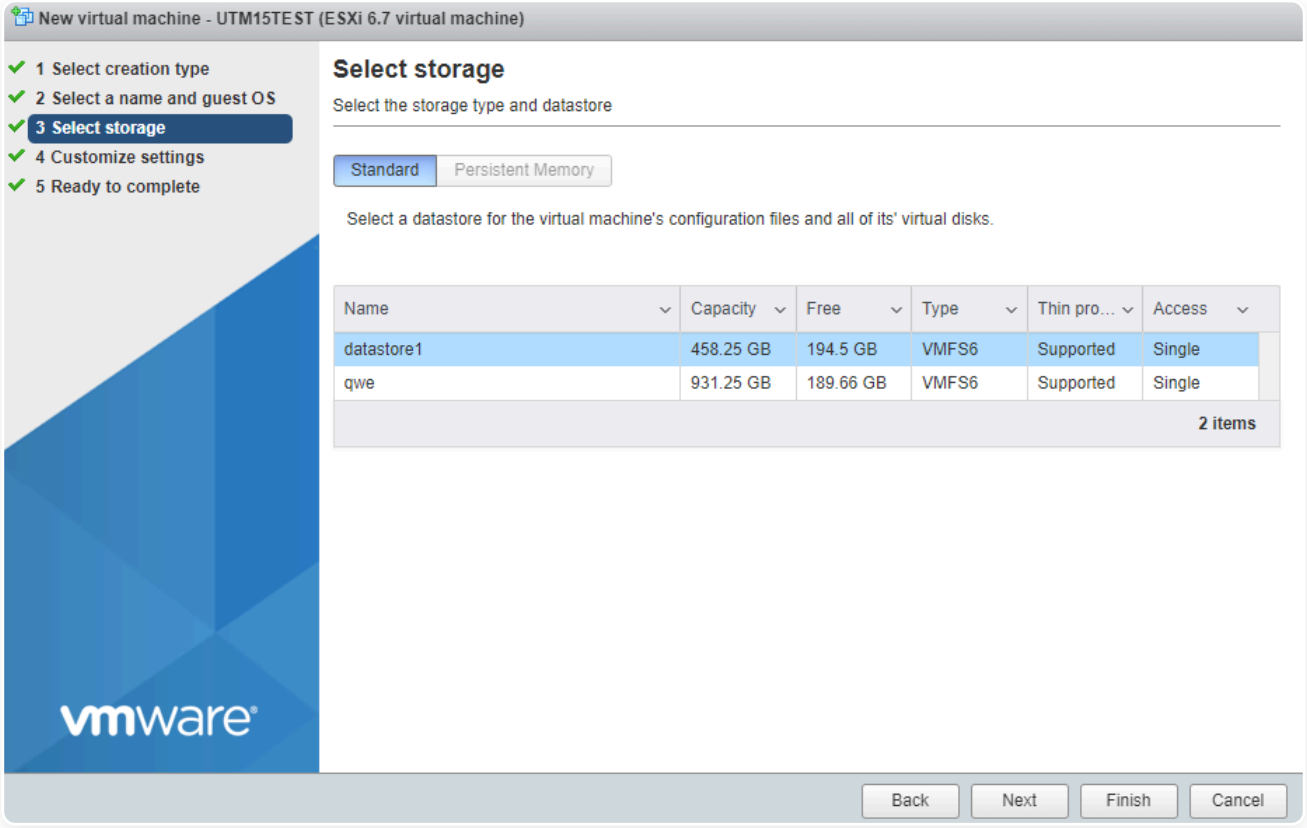
1. Создайте виртуальную машину:



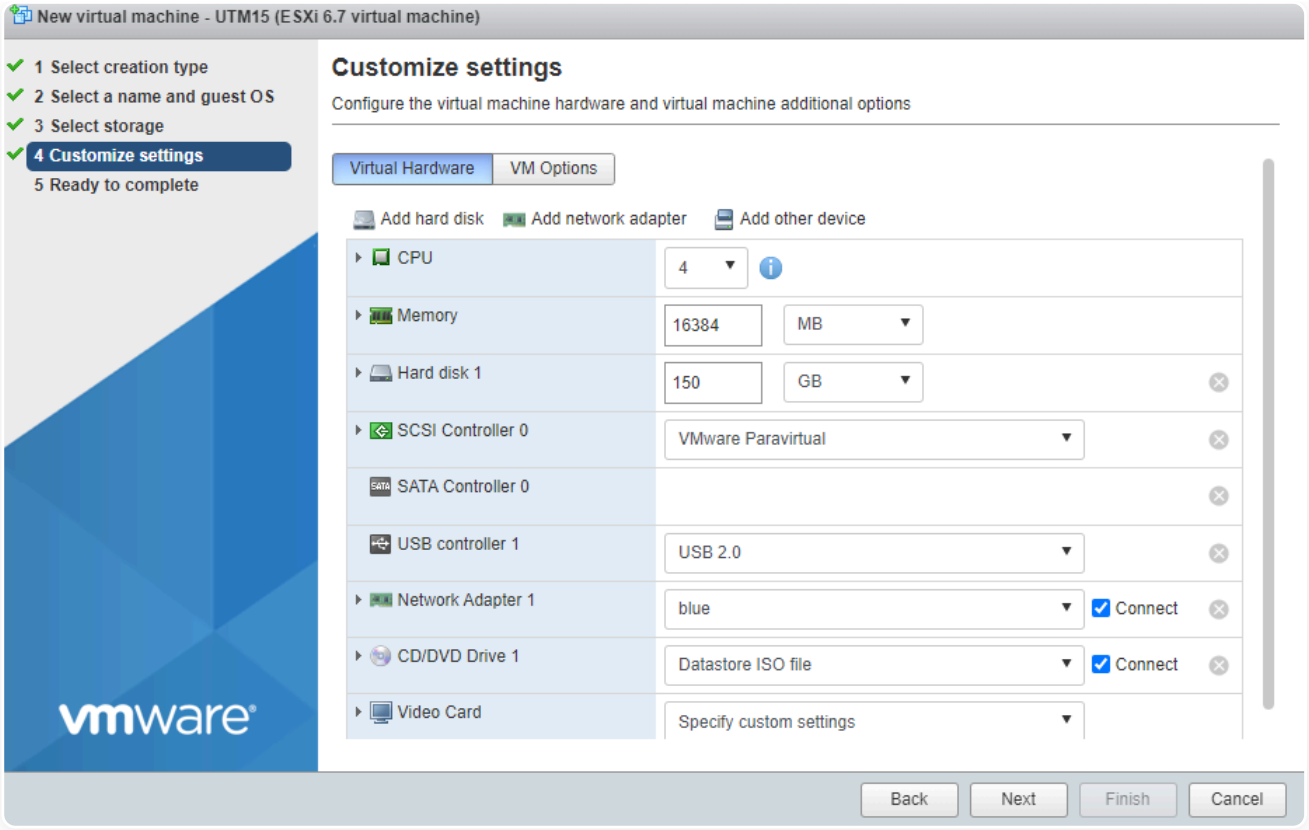
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



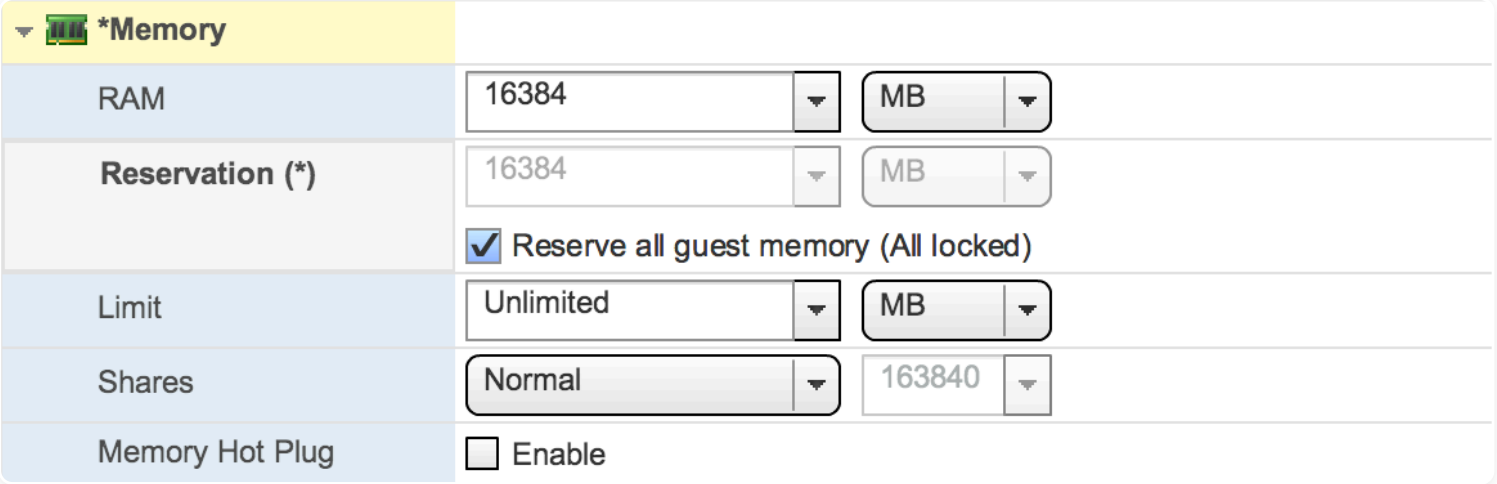
3. Выберите хранилище для виртуальной машины:



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

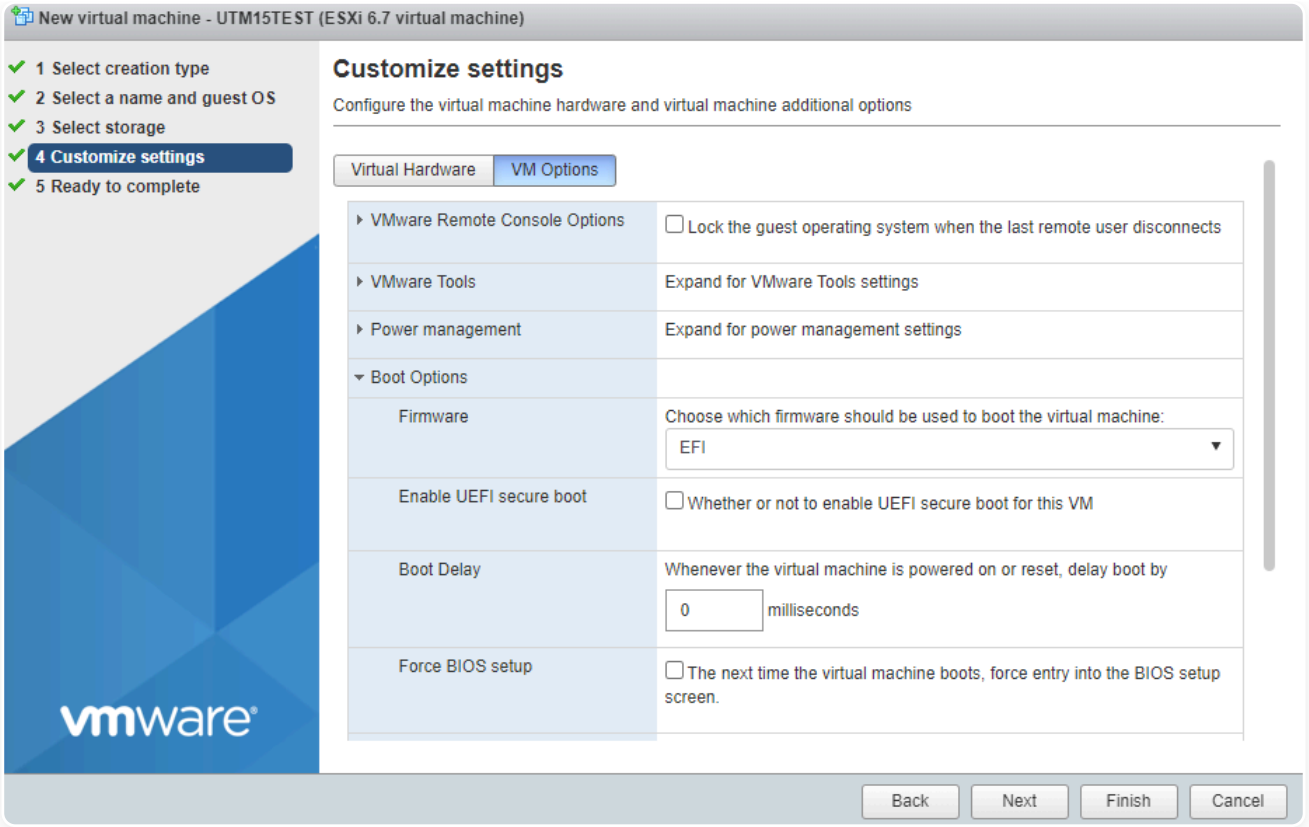


5. Разверните раздел **Memory** и включите опцию **Reserve all guest memory (All locked)**:



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

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



7. Нажмите **Finish**:

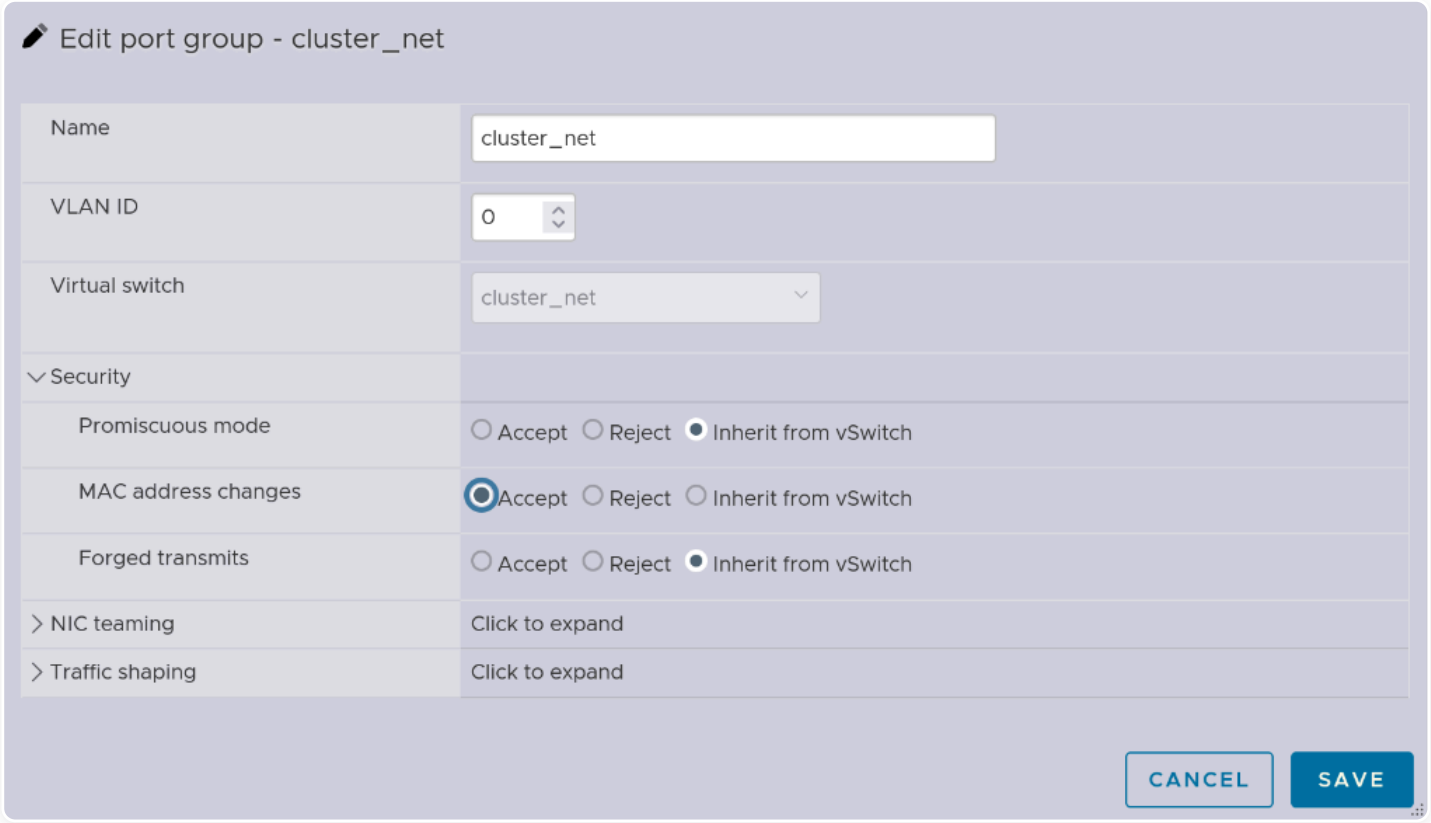
Настройка LACP-интерфейсов

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

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

2. Выберите группу портов, используемую для LACP.

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



4. Нажмите **Save**.

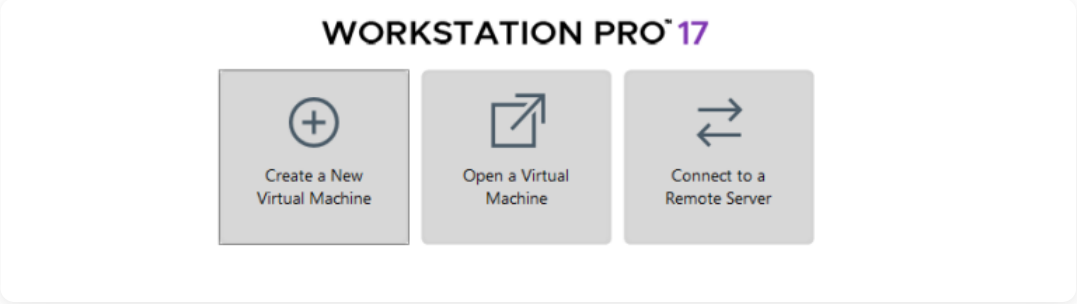
VMware Workstation 17.0

Настройка

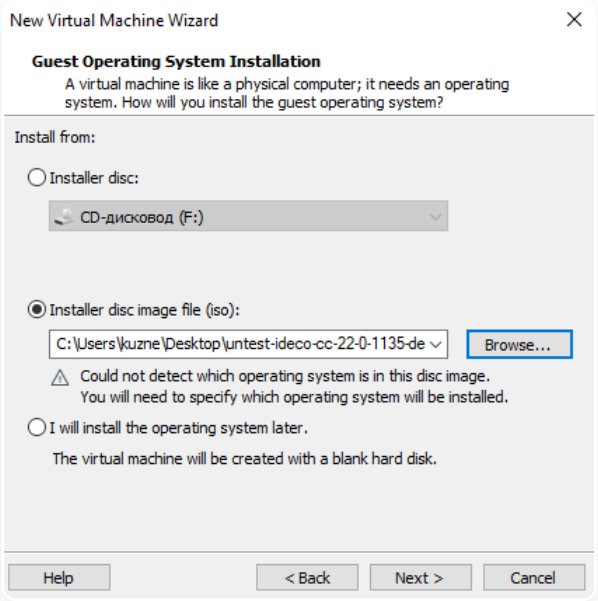
Перед установкой Ideco Center:

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

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

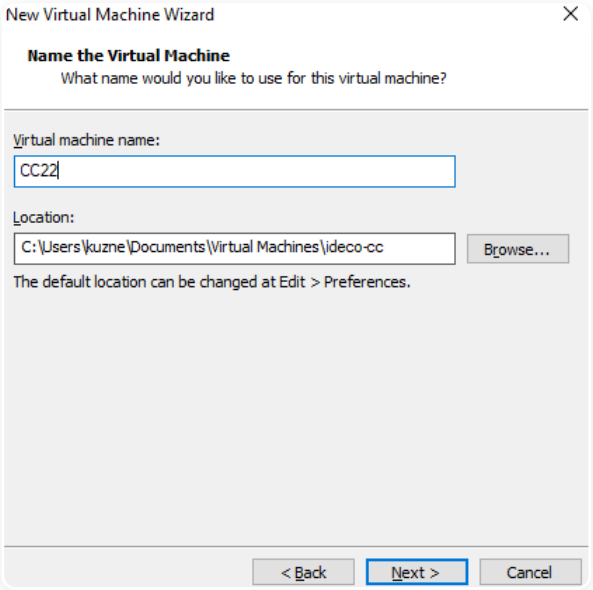


2. Укажите загрузочный ISO-образ:



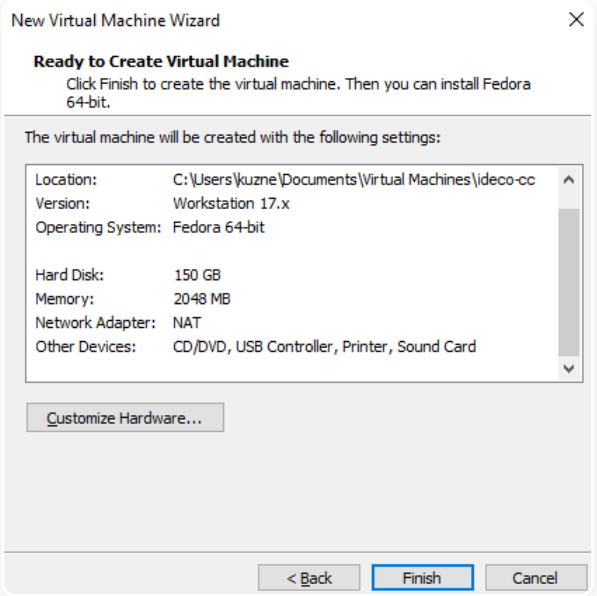
3. Выберите гостевую операционную систему **Linux** и в раскрывающемся списке укажите тип **Fedora 64-bit**:

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



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

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



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

8. Укажите количество ядер процессора, равное 4:

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

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

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

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

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

VirtualBox 7.0.12

Настройка

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

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

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

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

4. Нажмите **Готово**.

KVM

Настройка

Минимальные требования к виртуальной машине описаны в статье.

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

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

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

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

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

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

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

Proxmox

Настройка

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

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

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

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

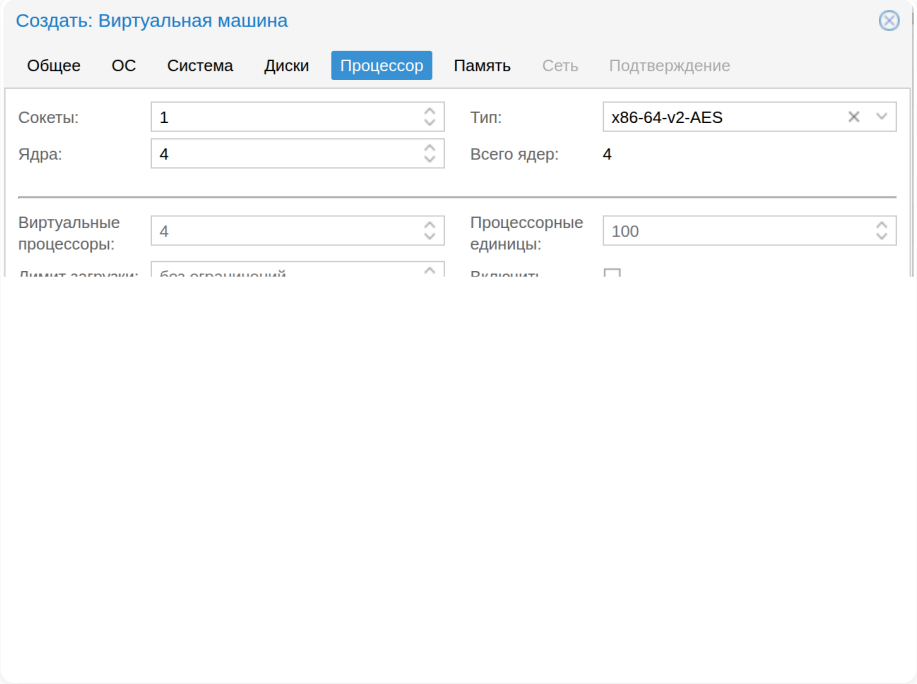
- **Машина** - q35.
- **BIOS** - OVMF.
- **Хранилище EFI** - хранилище для UEFI-диска.
- **Агент QEMU** - включите опцию, чтобы операционная система могла передавать гипервизору информацию о своих внутренних состояниях.
- **Предварительная загрузка ключей** - отключите опцию.

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

- **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.

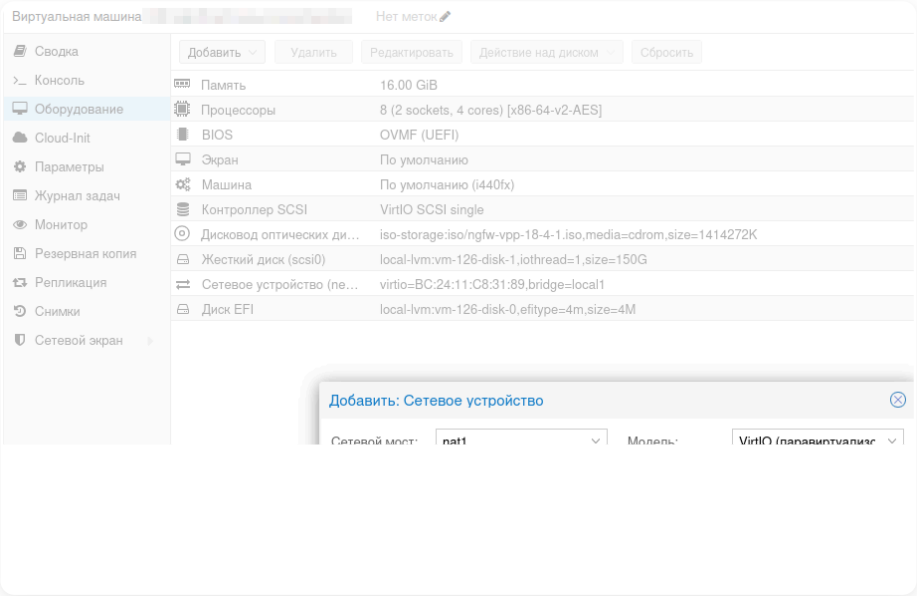
7. В разделе **Сеть** в поле **Сетевой мост** выберите сетевой мост для локального интерфейса:

Рекомендуем отключить опцию **Сетевой экран**, чтобы облегчить настройку и отладку сети Ideco Center и избежать конфликтов обработки трафика.

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

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

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



Microsoft Hyper-V

Настройка

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

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

Минимальные требования к виртуальной машине описаны в статье.

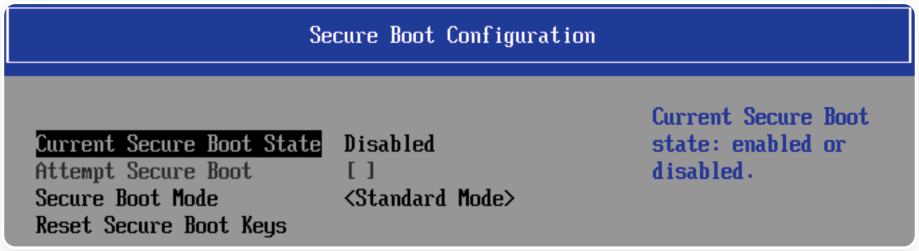
Шаги по установке Ideco Center после создания загрузочного USB-накопителя можно прочитать в статье Установка.

При использовании LACP-интерфейсов требуется дополнительная настройка:

1. Перейдите в **Hardware** → **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**:



Установка Ideco Center

Технические требования для серверов и виртуальных машин:

Требования	Характеристики
Процессор	• Intel i3/i5/i7/i9/Xeon минимум 4 поколения Haswell (2013г.) • AMD FX/Ryzen/EPYC • Поддержка SSE 4.2 • От 4 ядер
Объем оперативной памяти	• От 16 ГБ
Накопитель	• Объем 150 ГБ или более • SSD с интерфейсом SATA, mSATA, SAS, NVMe • Не гарантируется работа с аппаратными RAID-контроллерами (программные контроллеры, интегрированные в чипсет, не поддерживаются) • Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти
Сеть	• Одна сетевая карта. Рекомендуется использовать карты на чипах Intel
BIOS	• Поддержка UEFI • Отключенная опция Secure Boot в UEFI • Отключенный режим Legacy, может называться CSM (Compatibility Support Module)
Дополнительно	• Монитор и клавиатура

Файл для установки Ideco Center доступен для скачивания в MY.IDECO.

Процесс установки

При установке Ideco Center с загрузочного USB-диска выберите загрузку с USB-диска в настройках UEFI компьютера.

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

Для установки Ideco Center выполните действия:

1. Перейдите к установке, нажав **Install Ideco CC**:

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

```
Установка Ideco CC 22.0.1561
----------------------------

Для установки выбран диск '161 ГБ - QEMU HARDDISK (drive-scsi0)'.
ВНИМАНИЕ! Все данные на нём будут уничтожены!

Пожалуйста подтвердите ваш выбор.

Введите 'y' и нажмите Enter для подтверждения.
Введите 'c' и нажмите Enter для отмены.
#
```

3. Выберите временную зону, в которой находится сервер:

```
Выберите временную зону.

1. Алма-Ата                                    21. Магадан
2. Анадырь                                     22. Москва
3. Астрахань                                   23. Новокузнецк
4. Багдад                                      24. Новосибирск
5. Баку                                        25. Омск
6. Барнаул                                     26. Самара
7. Белград                                     27. Саратов
8. Бишкек                                      28. Сахалин
9. Владивосток                                 29. Симферополь
10. Волгоград                                  30. Ташкент
11. Екатеринбург                               31. Тбилиси
12. Ереван                                     32. Томск
13. Иркутск                                    33. Ульяновск
14. Калининград                                34. Чита
15. Камчатка                                   35. Якутск
16. Карачи                                     36. Аден
17. Киев                                       37. Актау
18. Киров                                      38. Актобе
19. Кишинёв                                    39. Амман
20. Красноярск                                 40. Амстердам

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
Нажмите Enter для вывода следующей страницы вариантов.
#
```

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

```
Текущая дата и время: 07 октября 2025, 06:49.

Данные указаны правильно?

Введите 'y' и нажмите Enter для подтверждения.
Введите 'n' и нажмите Enter для отказа.
Введите 'c' и нажмите Enter для отмены.
#
```

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

5. Не нажимайте никаких клавиш при появлении окна:

```
Ideco CC 22.0.1561
Kernel 6.18.7-100.1775716949.56.ef1e92dd.utm.x86_64 on x86_64 (tty1)

localhost login: _
```

После загрузки система автоматически перейдет к локальному интерфейсу Ideco Center.

Создание учетной записи администратора

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

```
Ideco CC 22.0.1561
------------------


Внимание! Аккаунт администратора отсутствует.
Требуется предварительно его создать.
Создание аккаунта администратора.

Введите новый логин и нажмите Enter.

# _
```

Требования к логину и паролю

Логин:

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

Пароль:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.
- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

> Если пароль не соответствует требованиям политики безопасности, то появится надпись с информацией, что пароль ненадежен. Потребуется ввести новый пароль с учетом требований.
>
> Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;`, `^[[4~;` и так далее.

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 MAC-адрес сетевой карты.

Для настройки Ideco Center через веб-интерфейс создайте интерфейс Control Plane в локальном меню. Control Plane - интерфейс администрирования, используется для настройки Ideco Center через браузер. Должен иметь свой выход в Интернет.

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

```
Управление сервером

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

Введите номер пункта и нажмите Enter.
# 3

1. Показать список и отредактировать интерфейс
2. Создать интерфейс
3. Включить/Отключить интерфейс
4. Удалить интерфейс

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 2
```

2. Выберите порт для доступа к веб-интерфейсу:

```
# 2

Выберите порт

-----------------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-----------------------------------------------------------------------------------------------------
  1    |  eth0_a6  |  bc:24:11:cc:7b:a6  |  Сервис        |  Red Hat, Inc. Virtio network device
-----------------------------------------------------------------------------------------------------

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
#
```

3. Введите имя интерфейса:

```
Введите имя интерфейса и нажмите Enter.

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

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

```
Настроить адресацию на интерфейсе

1. Автоматически через DHCP
2. Вручную
3. Без адресации
```

5. Если выбрали **Вручную**, 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.
# 192.168.100.20/24
Интерфейс успешно настроен.
```

6. После настройки интерфейса Control Plane можно перейти в веб-интерфейс.

Подключение к веб-интерфейсу Ideco Center

1. Запустите на любом компьютере в сети интерфейса Control Plane поддерживаемый браузер (современные версии Firefox, Chrome и браузеров, основанных на Chromium).

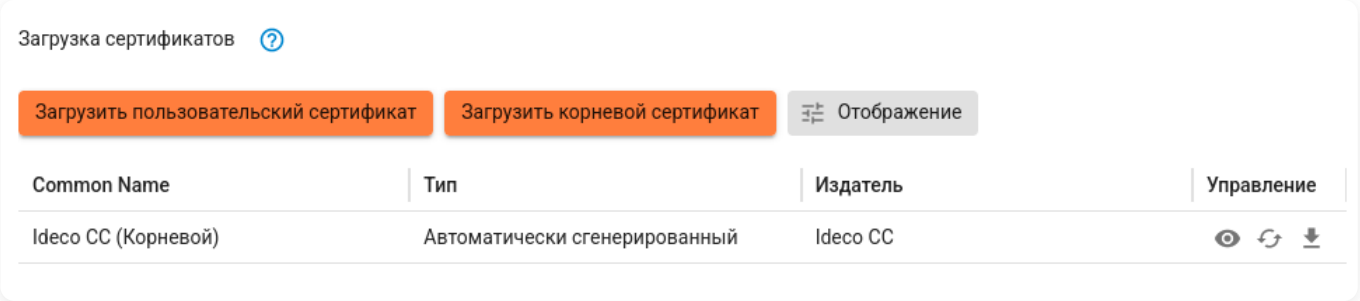
2. Введите в адресной строке IP-адрес, указанный при настройке интерфейса Control Plane, и порт `8443`.

Пример. `https://192.168.100.2:8443`

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

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

Скачать сертификат можно в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



Пример импорта сертификата для Windows

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

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

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

Серверы

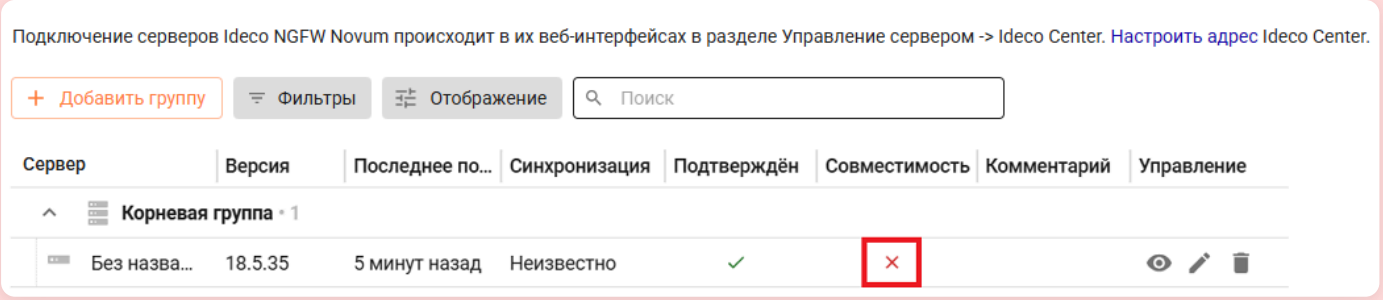
В разделе **Серверы** можно группировать синхронизированные серверы NGFW и формировать из них древовидную структуру. Группировка серверов позволяет применять правила и политики безопасности ко всем серверам каждой группы.

В статье описаны подключение и управление серверами Ideco NGFW.

Документация API

После обновления Ideco Center до версии 23 к нему смогут подключаться только серверы NGFW Novum версии 22.1 и выше. Подробнее – в статье.

Если Ideco Center и Ideco NGFW Novum имеют разные мажорные версии, синхронизация правил не происходит. В разделе **Серверы** отображается информация о несовместимости:



Особенности работы

Установка соединения

- Подключение всегда устанавливает Ideco NGFW Novum: соединение идет в направлении от NGFW Novum к Ideco Center. Поэтому связь работает и когда NGFW Novum находится за NAT, а открывать входящие порты на подключаемом NGFW Novum не требуется.
- Порты TCP/3151 и UDP/3151 должны быть доступны на стороне Ideco Center.
- Если Ideco Center находится за NAT без белого IP-адреса и к нему необходимо подключить Ideco NGFW из другой сети, настройте VPN между офисами через IPsec. Альтернативный способ – создать правило DNAT в веб-интерфейсе Ideco NGFW для проброса порта к Ideco Center.

Протоколы и шифрование

- Туннель WireGuard на UDP/3151 используется для синхронизации базы данных отчетов и журналов между NGFW и Ideco Center, а также для перехода в веб-интерфейс NGFW.
- WebSocket на TCP/3151 используется для остальных коммуникаций между NGFW и Ideco Center.
- Соединение между NGFW и Ideco Center шифруется по протоколу TLS 1.3. Старые версии протокола (TLS 1.0, TLS 1.1, TLS 1.2) отключены.

Обслуживание подключенных серверов

- Для настройки кластера Ideco NGFW Novum достаточно подключить активную ноду. Пассивная нода настроится автоматически.
- Для обновления NGFW, подключенных к Ideco Center, перейдите в интерфейс NGFW и воспользуйтесь статьей Обновления.

Работа с серверами Ideco NGFW

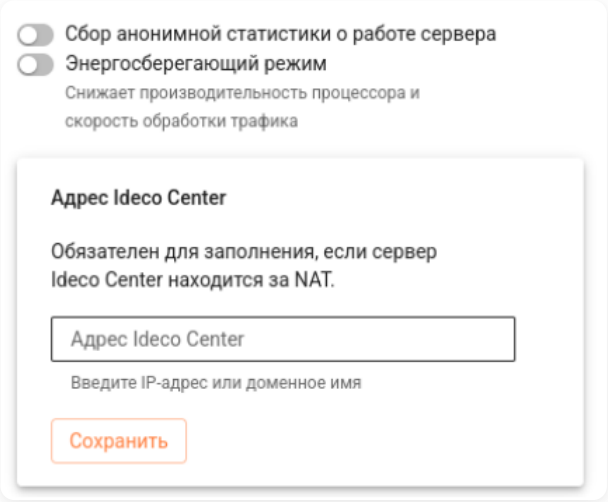
В версии 23 меняется логика привязки VCE к Ideco Center. Перед обновлением ознакомьтесь со статьей Подготовка VCE к обновлению на версию 23.

Настройка Ideco Center, если сервер находится за NAT

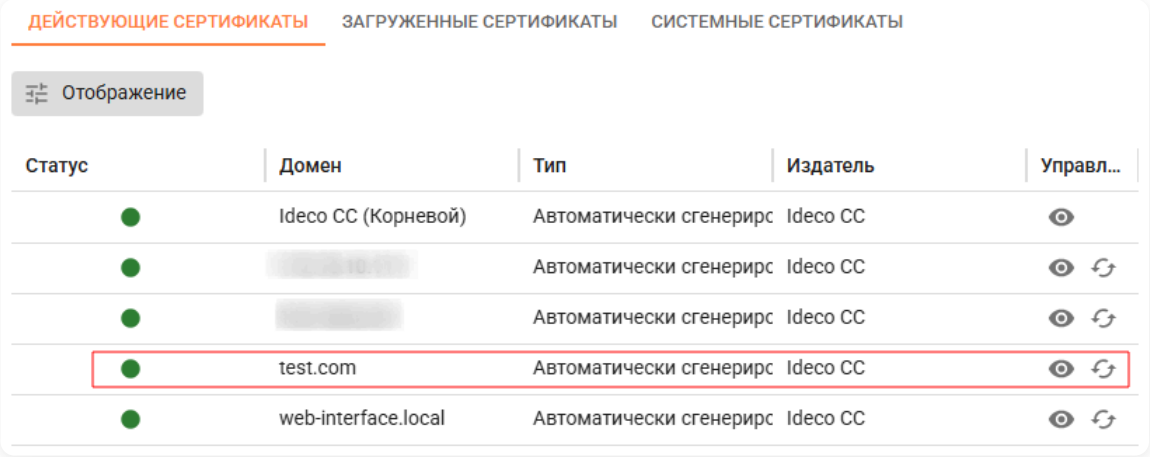
Если сервер Ideco Center находится за NAT:

1. Перейдите в **Управление сервером** → **Дополнительно**.

2. Укажите IP-адрес NAT-устройства или доменное имя в поле **Адрес Ideco Center**:



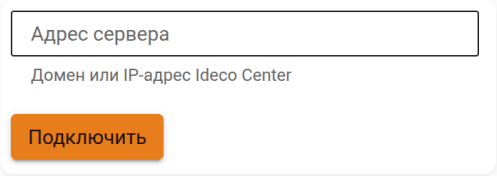
3. Нажмите **Сохранить**. Будет выпущен сертификат на IP-адрес или доменное имя сервера Ideco Center:



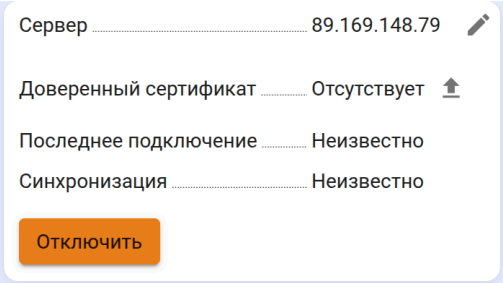
Подключение Ideco NGFW Novum или VCE к Ideco Center

1. В Ideco NGFW или VCE перейдите в **Управление сервером** → **Ideco Center**.

2. Введите IP-адрес или доменное имя в строке **Адрес сервера** и нажмите **Подключить**:

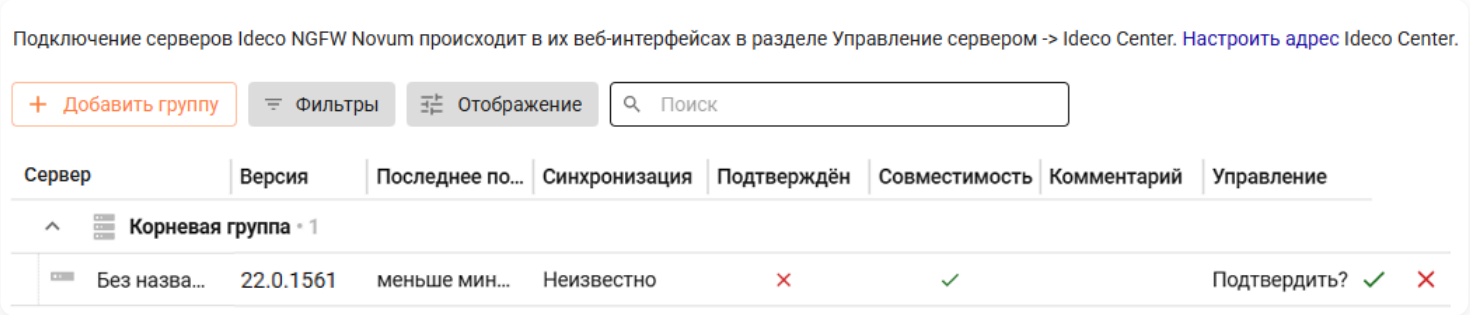


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW или VCE:



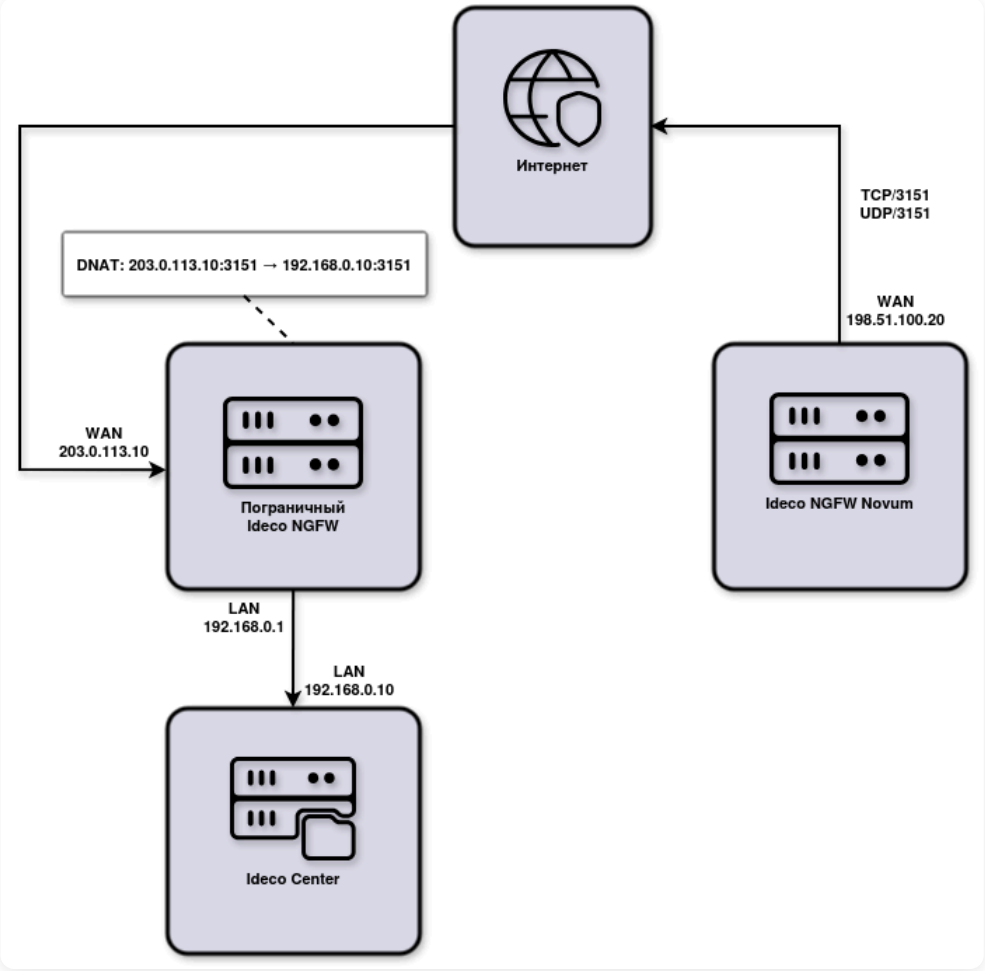
Скачать корневой сертификат можно в Ideco Center, раздел **Сервисы** → **Сертификаты**.

3. В интерфейсе Ideco Center перейдите в раздел **Серверы** и подтвердите подключение кнопкой ✓:

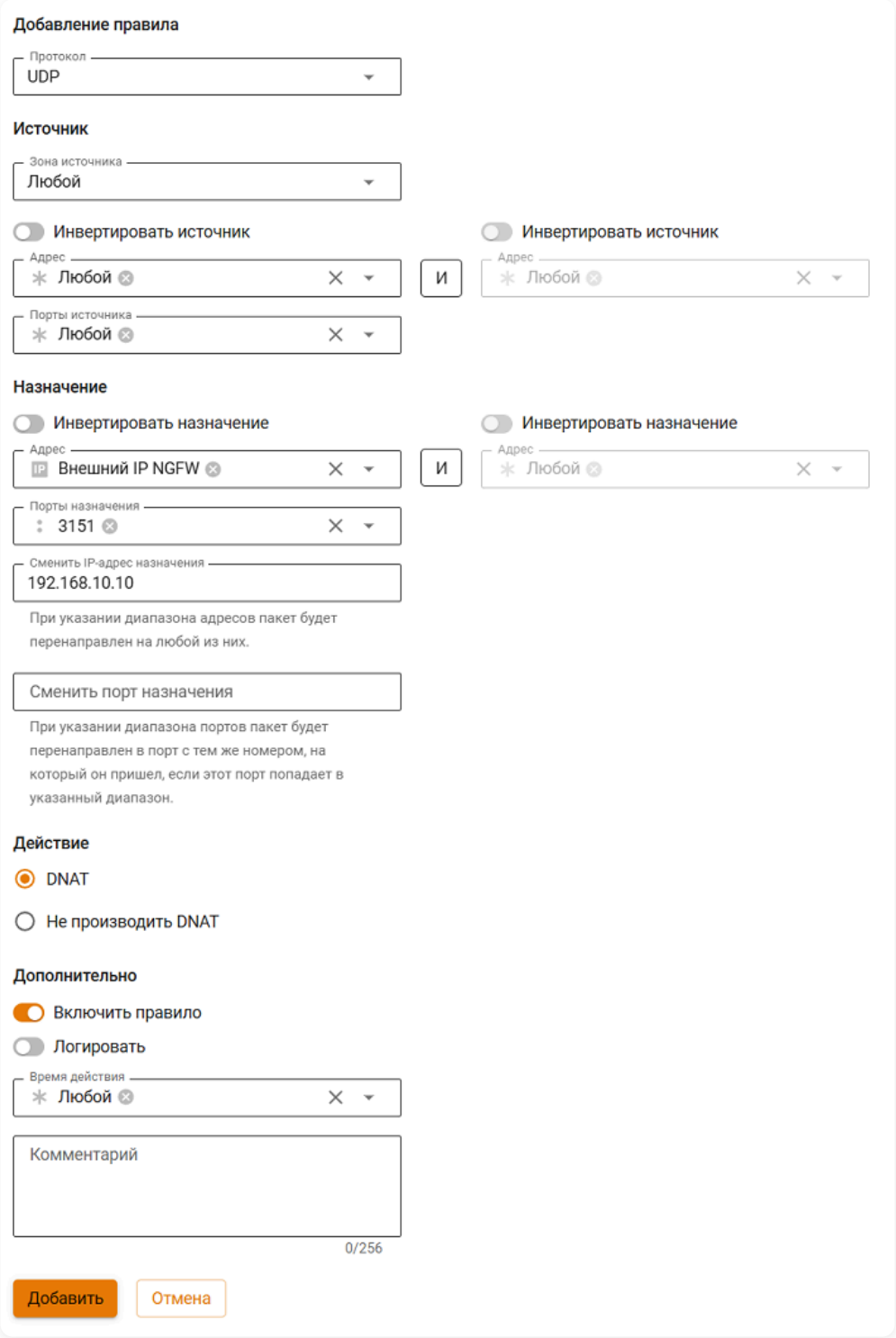


Портмаппинг при подключении Ideco NGFW к Ideco Center

Если Ideco Center находится в локальной сети, NGFW Novum подключается к нему из другой сети, а VPN между офисами нет, настройте проброс портов на пограничном Ideco NGFW, за которым стоит Ideco Center:



Создайте на пограничном NGFW два одинаковых правила для протоколов **UDP** и **TCP** в **Правила трафика** → **Межсетевой экран** → **DNAT**. По TCP идет подключение и синхронизация, по UDP работает туннель WireGuard, поэтому оба правила обязательны:



- **Назначение** – внешний IP-адрес Ideco NGFW.
- **Сменить IP-адрес назначения** – внутренний IP-адрес Ideco Center.
- **Порт** – только порт 3151.

После включения правил трафик будет проходить в локальную сеть через внешний интерфейс и перенаправляться в Ideco Center.

Удаление сервера Ideco NGFW из Ideco Center

При разрыве привязки из Ideco NGFW удаляются все объекты, профили, правила и политики, полученные с Ideco Center. Это может привести к нарушению работы сети.

Перед удалением убедитесь, что объекты, полученные с Ideco Center, не используются в локальных правилах Ideco NGFW, либо замените их локальными объектами.

Для удаления Ideco NGFW из Ideco Center нажмите напротив сервера:

Переход из веб-интерфейса Ideco Center в веб-интерфейс Ideco NGFW

В Ideco Center предусмотрено два способа перехода в Ideco NGFW:

1. В **Серверы** нажмите на напротив нужного сервера:

2. Нажмите на в левом верхнем углу и выберите нужный NGFW:

Чтобы перейти к веб-интерфейсу VCE подключенных серверов в Ideco Center:

1. Зайдите в веб-интерфейс NGFW, используя один из указанных способов.

2. Следуйте инструкциям из статьи.

> Если к Ideco Center версии 22 подключен Ideco NGFW Novum версии 23, перейти из Ideco Center можно только в веб-интерфейс **Системного контекста**.
>
> Прямой переход в веб-интерфейс VCE в этом случае невозможен и выполняется только через веб-интерфейс **Системного контекста**.

> При потере связи с Ideco Center синхронизированная конфигурация сохраняется на Ideco NGFW и продолжает применяться.

Работа с группами серверов Ideco NGFW

Структура групп серверов в Ideco Center предполагает три уровня вложенности. Первый - **Корневая группа**. Серверы NGFW, подключенные к Ideco Center, и группы, созданные в Ideco Center, являются частью **Корневой группы** и не могут быть вынесены оттуда.

При этом на Ideco NGFW будут распространяться правила и политики безопасности всех вышестоящих групп в соответствии с вложенностью.

Создание группы серверов

1. В разделе **Серверы** нажмите **Добавить группу**:

2. Укажите **Название группы** и выберите родительскую группу из раскрывающегося списка (если это первая создаваемая группа, в списке будет только **Корневая группа**):

3. Нажмите **Сохранить**.

Редактирование группы серверов

1. Нажмите на напротив нужной группы.

2. Отредактируйте название и родительскую группу:

Удаление группы серверов

Чтобы удалить группу серверов, нажмите на . Если в удаленной группе были серверы, то они переместятся в **Корневую группу** (удалить или отредактировать **Корневую группу** нельзя):

Перемещение серверов Ideco NGFW между группами

Чтобы переместить синхронизированный с Ideco Center сервер Ideco NGFW из одной группы в другую:

1. Нажмите на напротив названия группы.

2. Из раскрывающегося списка выберите группу, в которую хотите переместить сервер:

Подключенный к Ideco Center сервер, настройки которого восстановлены из бэкапа другого сервера, не появится в таблице серверов Ideco Center. Возникнет конфликт с донором бэкапа из-за одинакового `cluster_id`.

В случае возникновения такой проблемы обратитесь в Техническую поддержку.

Пользователи

> В разделе настраиваются интеграции Ideco Center с контроллером домена на базе Microsoft Active Directory (AD) и Samba DC.

Интеграция с Microsoft Active Directory/Samba DC

После настройки интеграции в центральной консоли появится возможность работать с учетными записями и группами безопасности AD в разделах Правила трафика и Объекты.

Поддерживаемые контроллеры домена

- Windows Server 2008 (только R2), 2012, 2016, 2019, 2022, 2025.
- Samba DC с версии 4.0.

Для ввода в домен на базе Windows 2025 перейдите в **Управление сервером** → **Терминал** и выполните команду:

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

Особенности интеграции с несколькими контроллерами домена:

- Учетные записи пользователей из разных доменов могут иметь одинаковые логины. При аутентификации пользователь будет точно определен по указанному домену. Если домен не был указан пользователем, будет указан **Каталог по умолчанию**.
- Пользователи всех интеграций отображаются в одном списке.
- Пользователи и группы безопасности будут видны и доступны к выбору в правилах трафика и поиске информации о пользователях AD, со всех интегрированных доменов. Список обновляется каждые 15 минут.

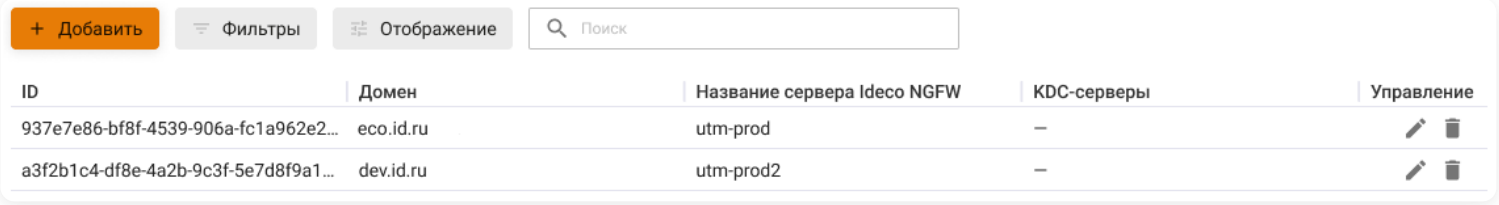
Ввод сервера в домен

Перед вводом в домен:

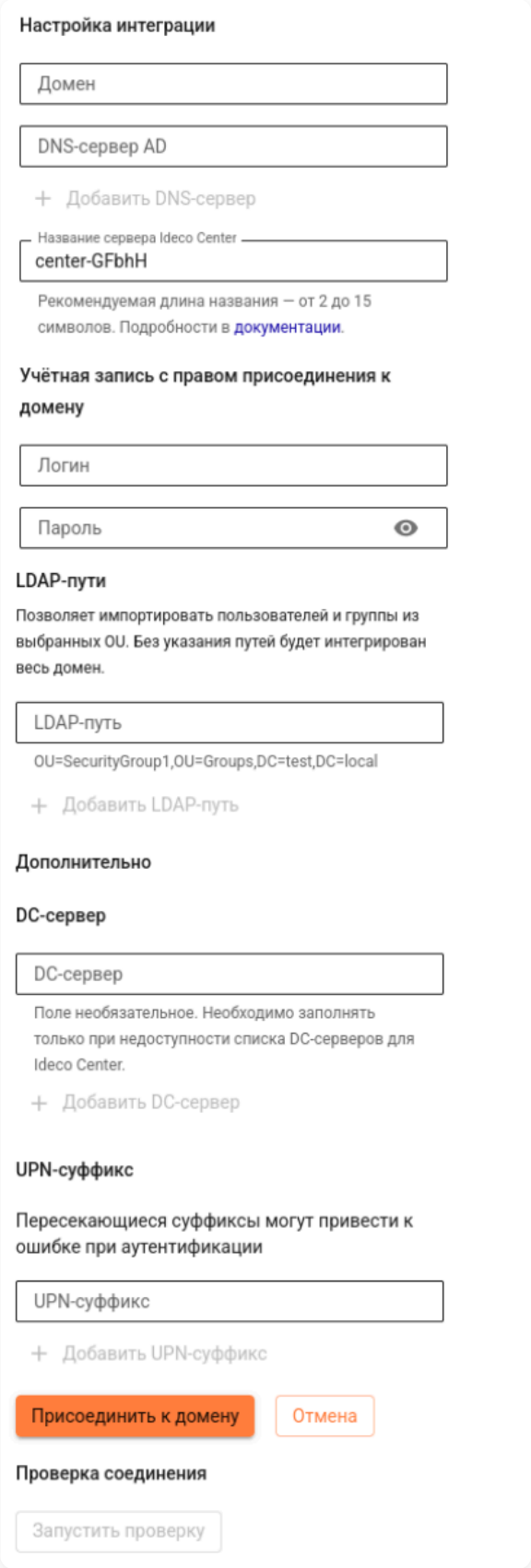
- Убедитесь, что время на контроллере домена и Ideco Center совпадает.
- Убедитесь, что хотя бы один контроллер домена находится в сети Ideco Center или доступен через локальный интерфейс с помощью настроенной маршрутизации.

Выполните действия:

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

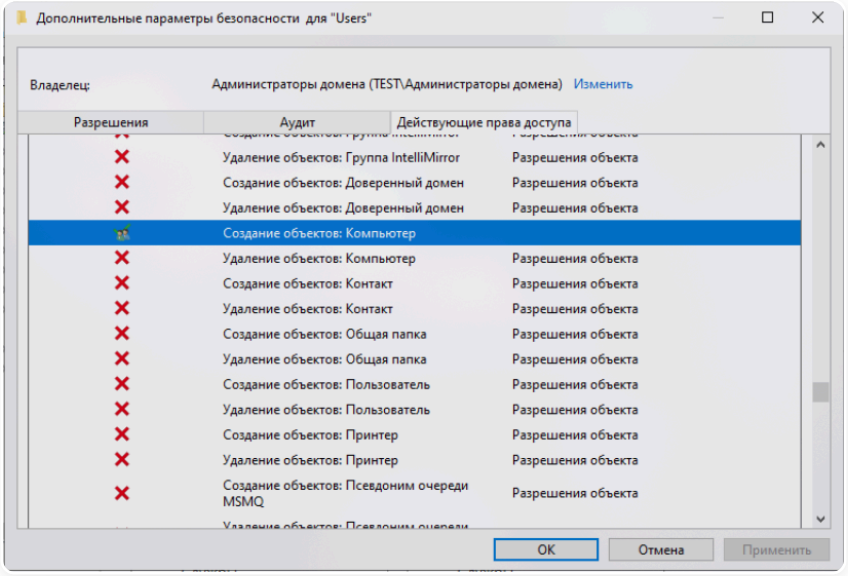


2. Нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Домен** – полное наименование домена, максимальная длина 64 символа. Например: `mydomain.example`.
- **DNS-сервер AD** – адрес сервера с ролью DNS в домене Active Directory. Должен быть доступен с любого интерфейса Ideco Center.
- **Название сервера Ideco Center** – имя компьютера, под которым Ideco Center будет введен в домен. Рекомендуемая длина – от 2 до 15 символов.
- **Учетная запись с правом присоединения к домену** – учетная запись AD с правами присоединения к домену (право **Создание объектов: Компьютер**). Данные учетной записи с правом присоединения к домену не сохраняются на сервере и используются один раз при вводе в домен:



- **LDAP-пути** – LDAP-пути для выбора пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет избежать синхронизации с Center всего дерева пользователей AD и выбрать только нужные группы.
- **DC-сервер** – контроллер домена. Необязательное поле, заполняется только при недоступности списка контроллеров домена для Ideco Center.
- **UPN-суффикс** – альтернативные суффиксы `userPrincipalName`. Указываются, если используются на контроллере домена. Пересекающиеся суффиксы могут привести к ошибке при аутентификации.

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

4. Нажмите **Запустить проверку** в блоке **Проверка соединения**, чтобы убедиться, что контроллер домена доступен с указанными настройками.

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

Мониторинг

В разделе можно настроить интеграцию Ideco Center с модулем SNMP для управления и мониторинга сетевых устройств, получения статистики трафика и/или Zabbix-агентом для детального мониторинга сервера, сбора статистики по ресурсам (CPU, память, диски).

SNMP

SNMP - это протокол для управления и мониторинга сетевых устройств, таких как маршрутизаторы, коммутаторы и межсетевые экраны.

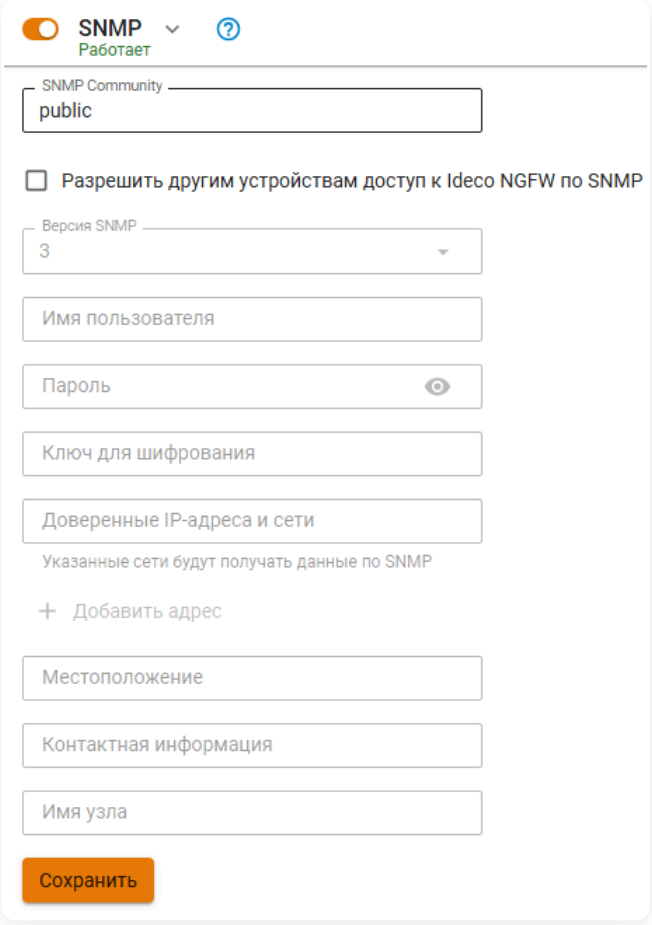
Модуль **SNMP** обеспечивает мониторинг работы Ideco Center по протоколу SNMP версий 1/2c и 3.
С помощью протокола SNMP передается информация:

- Загрузка центрального процессора и оперативной памяти.
- Занятое или свободное место на дисковом хранилище устройства.
- Объемы трафика.

> Для версии SNMPv1/v2 обязательно указывать поле **SNMP community**.
> Для версии SNMPv3 обязательно указывать поле **Имя пользователя** и **Пароль**.
> На сервере, с которым будет осуществляться соединение по SNMPv3, укажите алгоритмы Auth Algorithm MD5 и Crypto Algorithm AES.

Настройка подключения SNMP

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



Версия 1/2c

- **Имя пользователя**.
- **Пароль** (минимальное количество символов - 8).

- **Доверенные IP-адреса и сети**.

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

Версия 3

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

Поля **Местоположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.
Устройства в указанных доверенных сетях получат доступ к данным Ideco Center 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 языке описания SMI (Structure of Management Information). 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:

- По имени объекта (например, `sysUpTime`).
- По числовому OID (например, `.1.3.6.1.2.1.1.3`).

Zabbix-агент

Zabbix - это система мониторинга с открытым исходным кодом, которая контролирует оборудование и состояние сети в режиме реального времени.

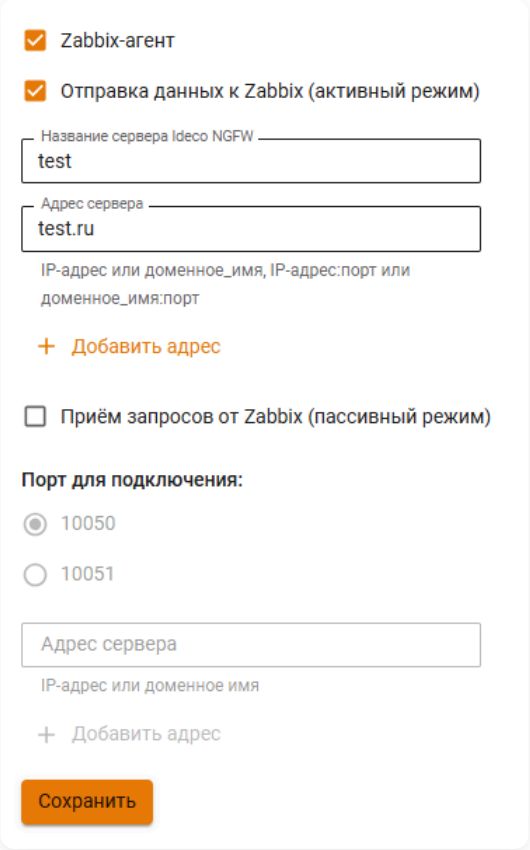
Настройка Zabbix-агента

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

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

Активный

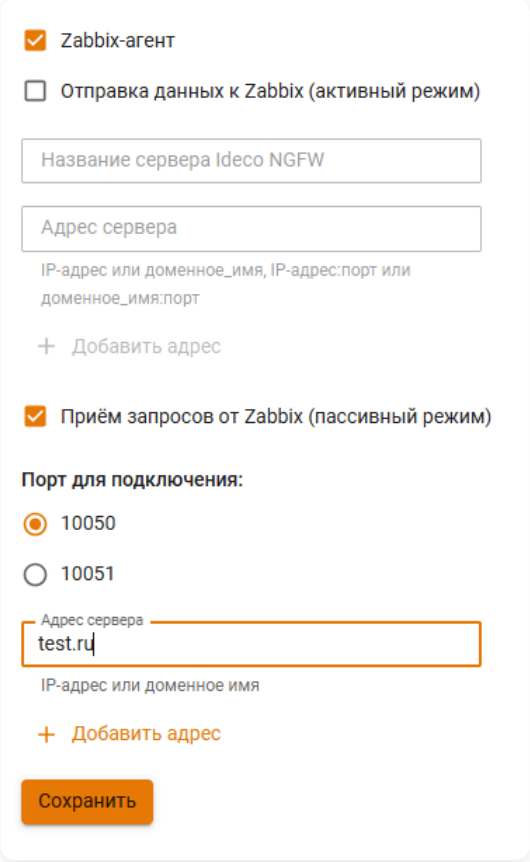
Соединение с Zabbix-сервером происходит со стороны Ideco Center. Для настройки заполните поля:



- **Имя сервера Ideco Center** - 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. Чтобы расширить список адресов, 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. Чтобы расширить список адресов, нажмите **Добавить адрес**.

Zabbix-сервер должен находиться внутри локальной сети Ideco Center. Подключение мониторинга возможно только к локальным интерфейсам (с ролью LAN). Это ограничение обусловлено системными правилами **Межсетевого экрана**, которые не отображаются в веб-интерфейсе, но имеют наивысший приоритет. Системные правила разрешают соединения на порты 10050/TCP и 10051/TCP только на локальных интерфейсах и блокируют их на внешних.

> В качестве шаблонов данных можно использовать стандартные шаблоны для Linux-серверов.

Полезные ссылки

- **Официальная страница Zabbix**
- **Zabbix как готовое решение**
- **Установка Zabbix**

Объекты

Объекты, созданные в Ideco Center, переносятся в подключенные NGFW Novum и VCE VPP. Администратор подключенного сервера может использовать эти объекты для создания правил.

При удалении объекта из Ideco Center, объект также удаляется из подключенных серверов. Если на подключенном сервере было создано правило с удаленным объектом, то этот объект будет отмечен Удалено.

Создание и удаление объектов в Ideco Center аналогично NGFW Novum. Подробнее можно узнать в статье Объекты.

Правила трафика

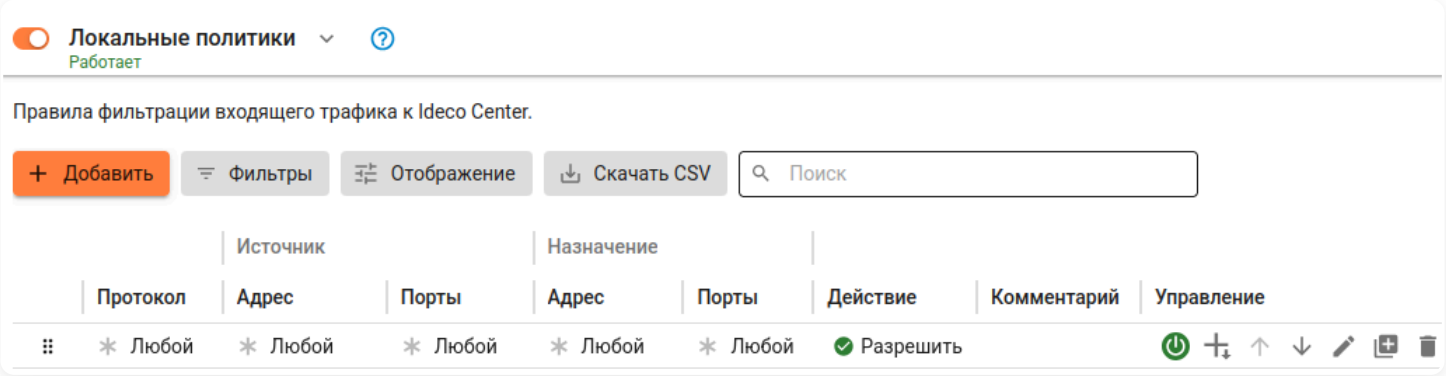
Настройка правил трафика зависит от типа подключенного сервера. Перейдите в раздел:

- Классические VCE (NGFW) - настройка **Межсетевого экрана**, **Контент-фильтра** и **Ограничения скорости**.
- Высокопроизводительные VCE (VPP) - настройка **Межсетевого экрана** и **Ограничения скорости**.

Локальные политики

Документация API

В разделе можно настроить правила фильтрации входящего (INPUT) трафика, направленного непосредственно на сервер Ideco Center:



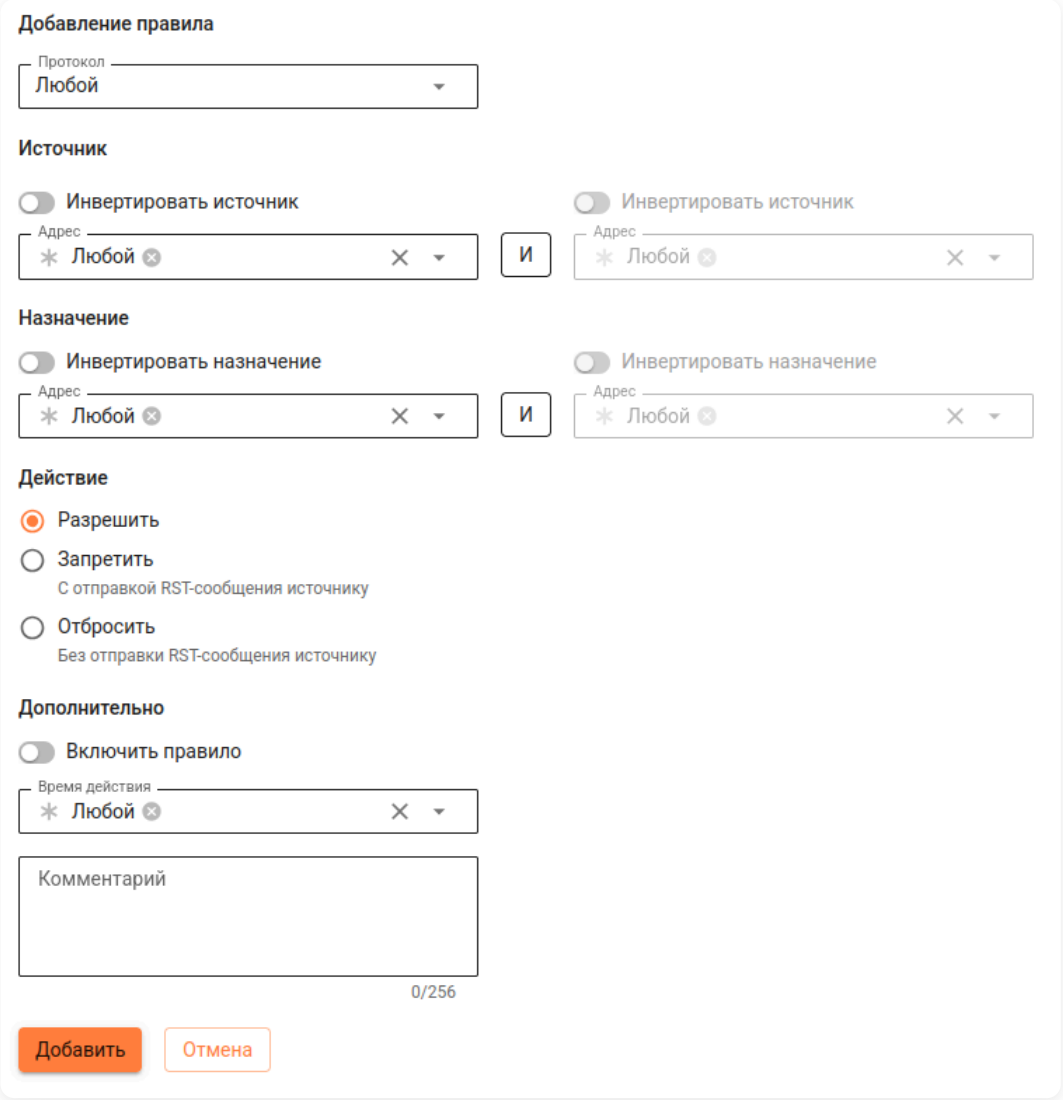
Правила имеют приоритет сверху вниз (то есть **верхнее правило приоритетнее нижнего**).

При наличии большого количества правил воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Создание правил

1. Нажмите кнопку **Добавить**.

2. Укажите необходимые параметры и нажмите кнопку **Добавить**:



Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP) или **Любой**.
- **Источник**:
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**) или страны. Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
  - **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
- **Назначение**:
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**) или страны. Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порт назначения** - указывается при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действие**:
  - **Разрешить** - разрешает трафик.
  - **Запретить** - запрещает трафик с отправкой RST-сообщения источнику. Рекомендуем использовать запрет с отправкой RST, так как это позволяет клиенту немедленно завершить попытку соединения, избежать долгих тайм-аутов и облегчает диагностику.
  - **Отбросить** - запрещает трафик без отправки RST-сообщения источнику.
- **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 256 символов.

Правило будет добавлено в конец списка.

Перемещение правил

Способы перемещения правил:

- Воспользуйтесь кнопками ↑ и ↓.
- Переместите правило через модальное окно.

Порядок перемещения

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:

- Переместите правило мышью: удерживайте ⠿ и перенесите правило в нужное место.

Классические VCE

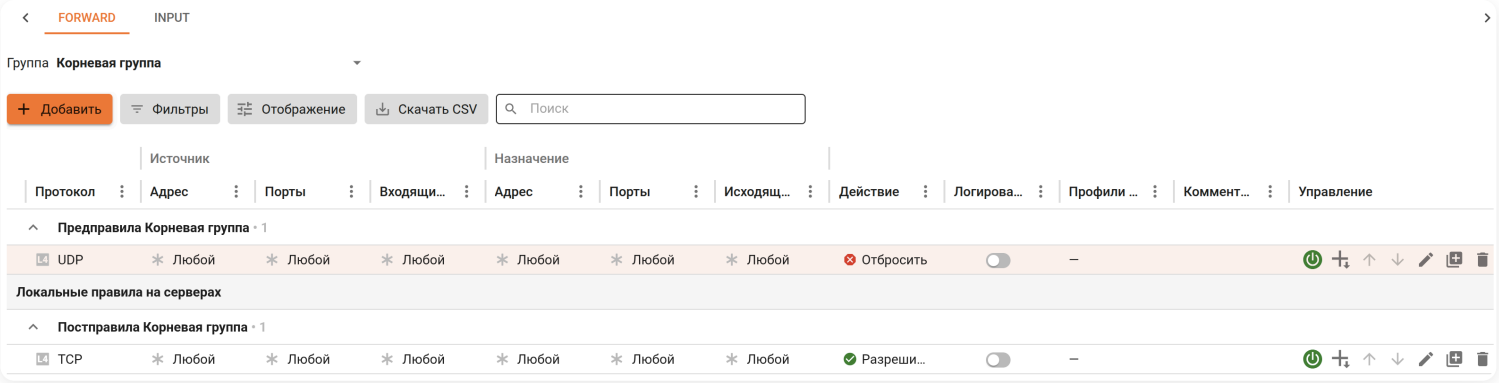
Принципы работы разделов **Межсетевой экран**, **Контент-фильтр** и **Ограничение скорости** с подключенными NGFW Novum идентичны.

Межсетевой экран

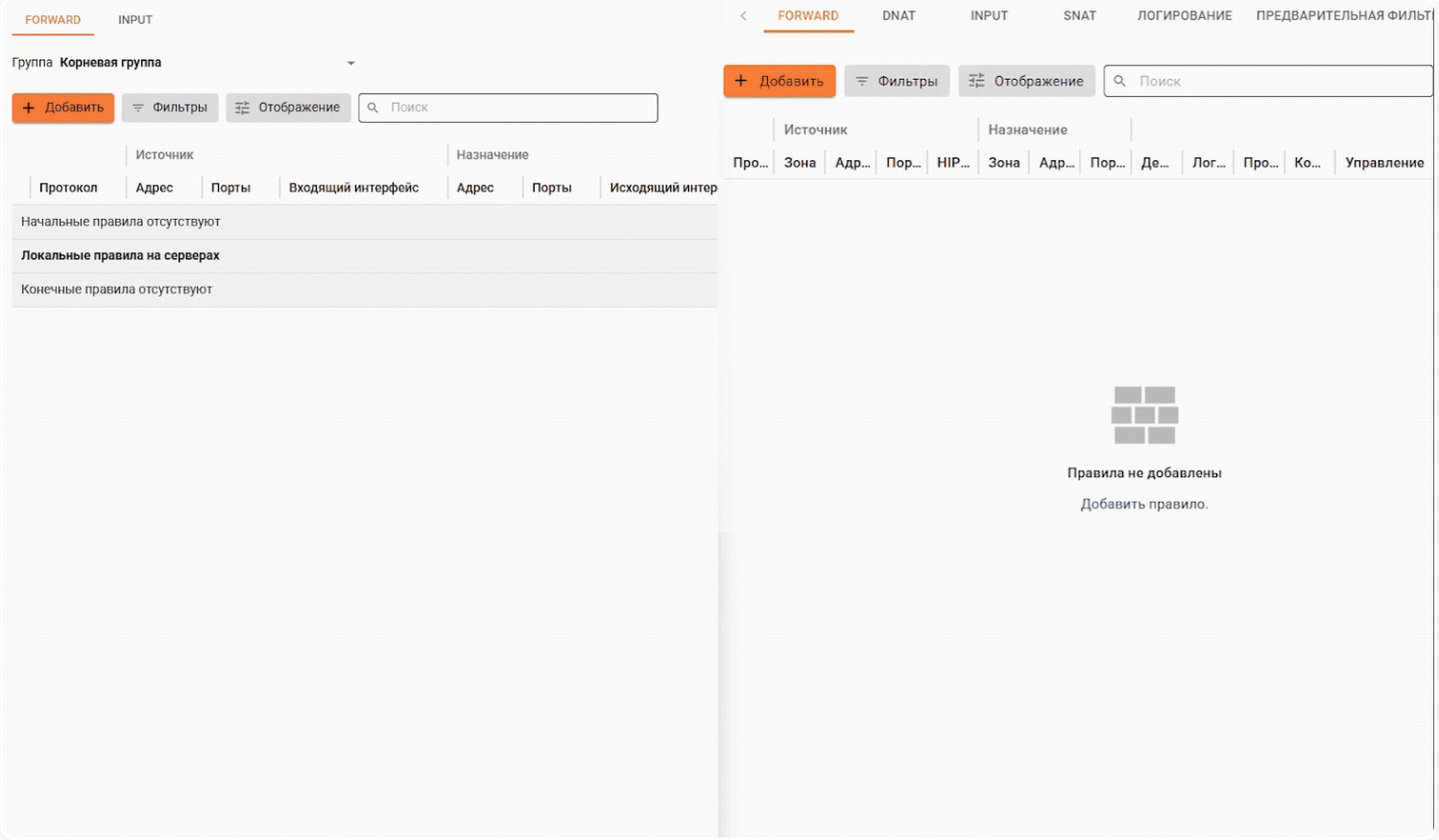
Документация API

Чтобы создать правила для пользователей или групп безопасности Active Directory/Samba DC, предварительно настройте интеграцию в **Пользователи -> Active Directory/Samba DC**.

Межсетевой экран Ideco Center содержит таблицы **FORWARD** и **INPUT**. Правила в них объединены в соответствии с группами серверов:



Пример добавления правил через Ideco Center. Слева - интерфейс Ideco Center, справа - интерфейс NGFW Novum:



В Ideco Center

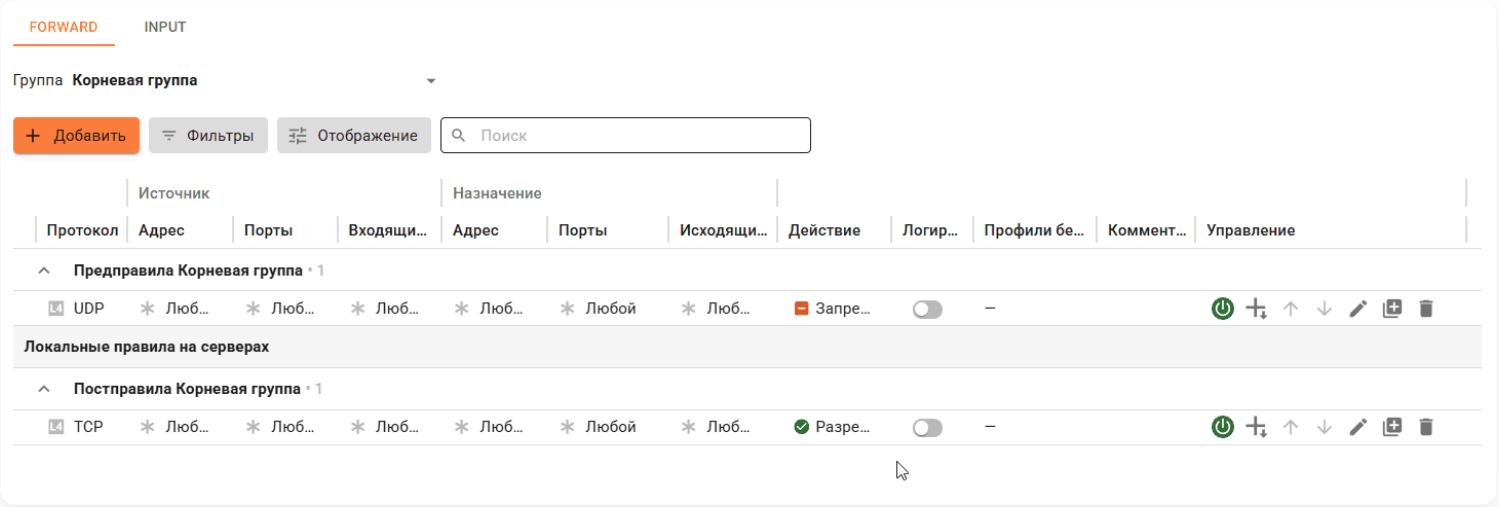
Созданные в Ideco Center правила FORWARD отображаются в виде двух таблиц: **Предправила** и **Постправила**. Правила применяются на подключенных NGFW Novum в следующем порядке: сначала - **Предправила** Ideco Center, затем - **Локальные правила** NGFW Novum, затем - **Постправила** Ideco Center.

Чтобы созданное правило попало в таблицу **Предправила**, укажите в строке **Вид правила** значение **Предправило**. Если правило требуется разместить в таблице **Постправила**, выберите значение **Постправило**.

Предправила и **Постправила** в Ideco Center создаются для определенной группы серверов. Группа указывается при создании правила в строке **Группа серверов**.

Правила можно включать и редактировать только в Ideco Center. В NGFW Novum правила доступны только для просмотра. Перемещать правила между таблицами **Предправила** и **Постправила** нельзя.

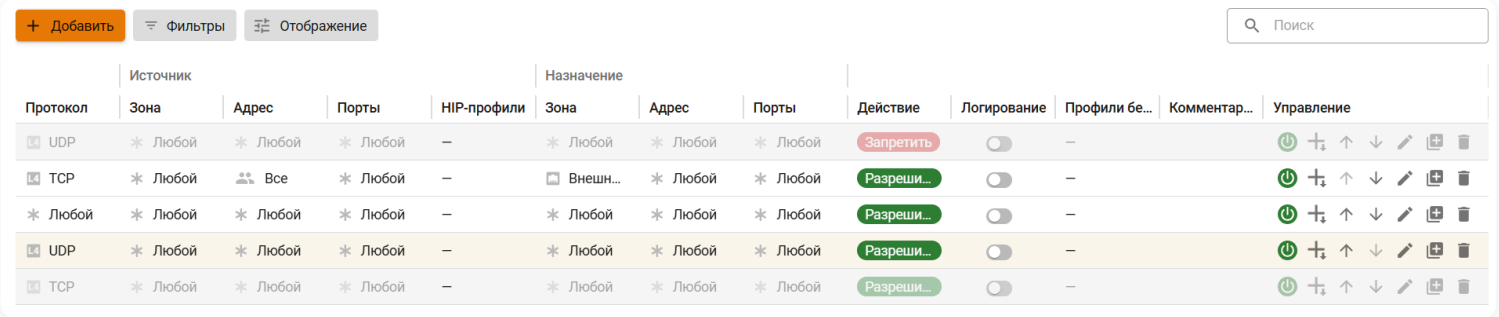
Чтобы увидеть все правила, распространяющиеся на группу серверов, выберите название группы над таблицей:



Чтобы изменить группу серверов, на которую распространяется правило, нажмите на и измените группу в соответствующей строке.

В NGFW Novum

Таблица в NGFW Novum визуально делится на верхнюю, среднюю и нижнюю части:



В верхнюю и нижнюю часть переносятся правила из подключенного Ideco Center. Управление этими правилами в NGFW Novum невозможно. Верхняя часть соответствует таблице **Предправила** в Ideco Center. Нижняя часть - таблице **Постправила**.

В средней части находятся **Локальные правила**, которые создаются администратором в самом NGFW Novum.

> **Локальные правила на серверах NGFW Novum** не видны в интерфейсе Ideco Center.
>
> Для просмотра перейдите в раздел **Серверы**, нажмите на в строке с нужным NGFW Novum и перейдите в раздел **Межсетевой экран**.

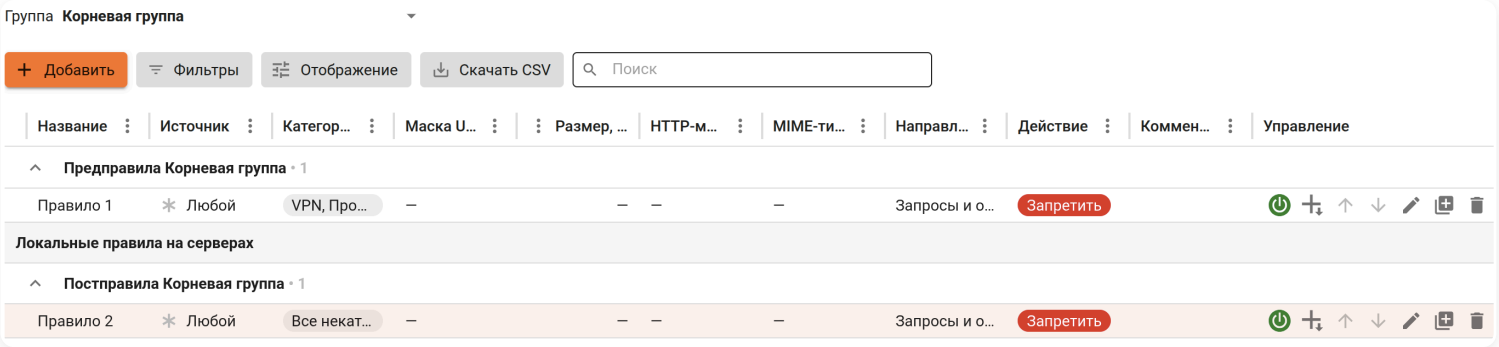
Контент-фильтр

Документация API

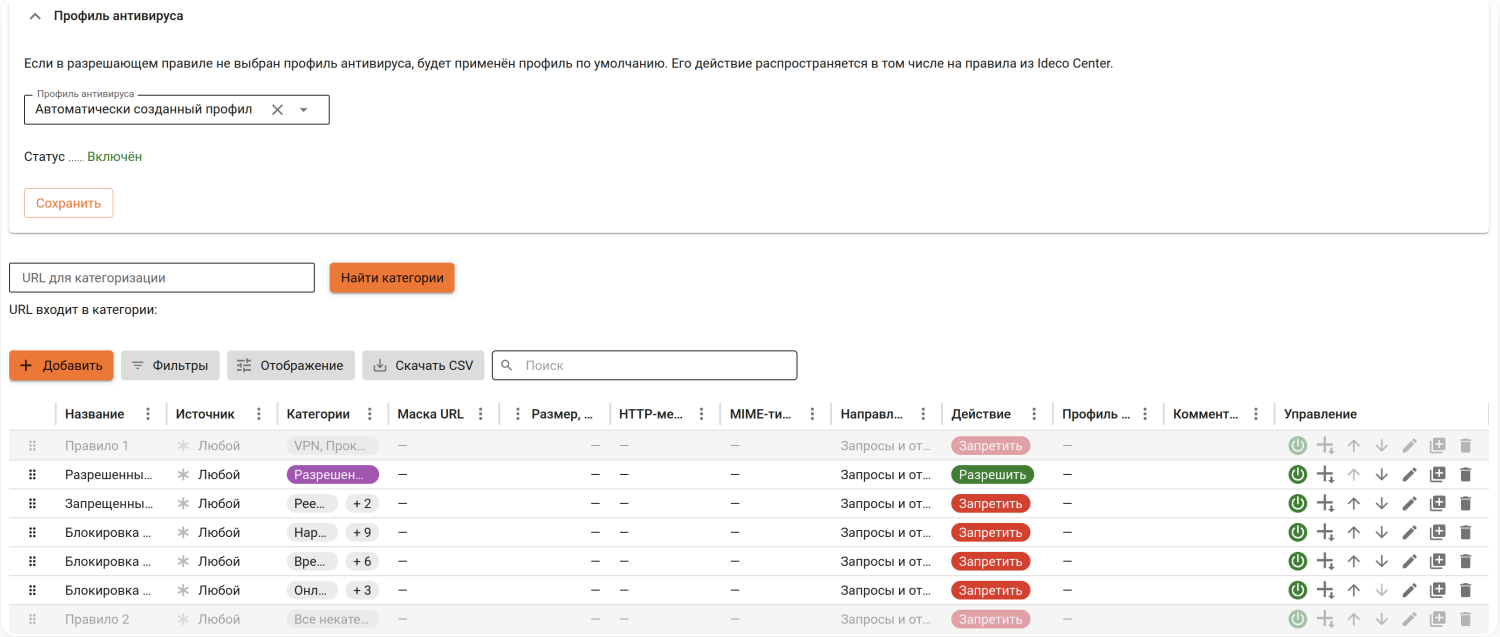
Создание правил в Ideco Center и в NGFW Novum аналогично. Созданные в Ideco Center правила **Контент-фильтра** переносятся в подключенные NGFW Novum в соответствии с группами серверов. Правила можно включать и редактировать только в Ideco Center. В NGFW Novum правила доступны только для просмотра.

Пример правила **Контент-фильтра**:

- В Ideco Center:



- В подключенном NGFW Novum:

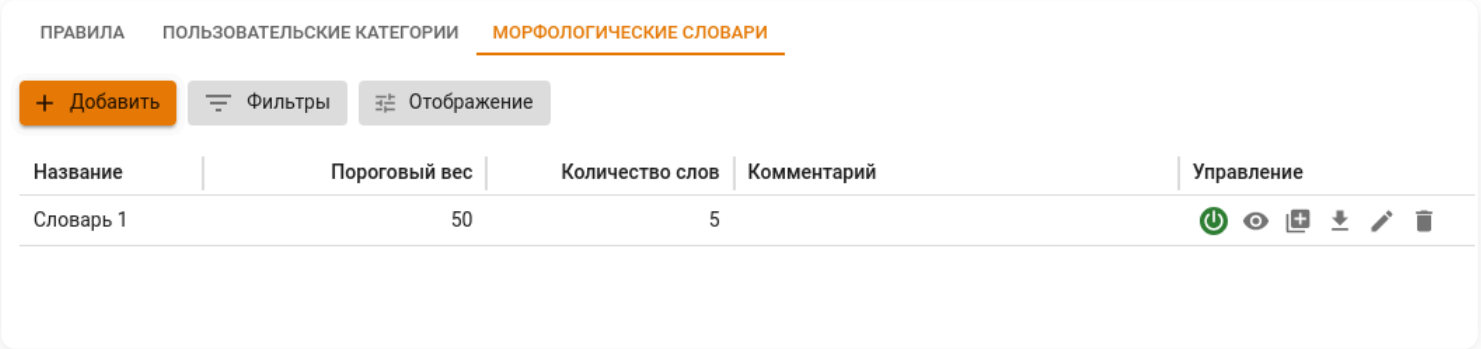


На вкладке **Морфологические словари** создаются и редактируются словари, которые можно использовать для проведения морфологического анализа сайтов в подключенных NGFW Novum. В Ideco Center включить морфологический анализ нельзя. Процессы создания **Морфологических словарей** в Ideco Center и в NGFW Novum аналогичны.

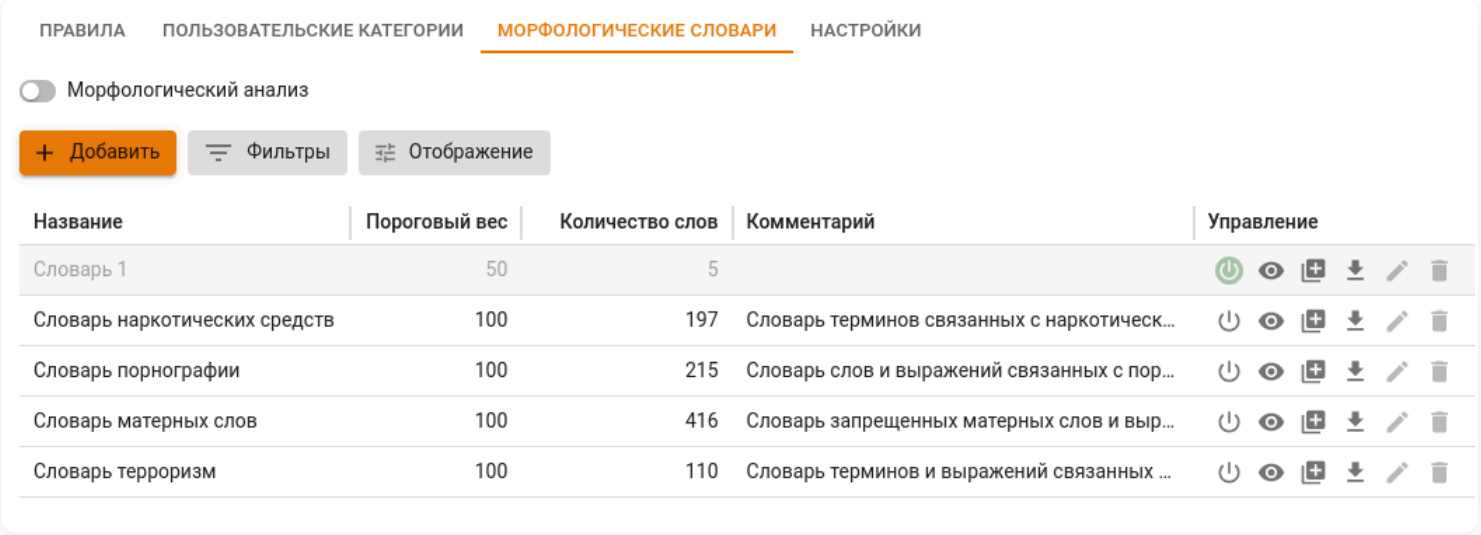
Созданные в Ideco Center **Морфологические словари** можно включать и редактировать только в Ideco Center. В NGFW Novum **Морфологические словари** доступны только для просмотра.

Пример словарей:

- В Ideco Center:



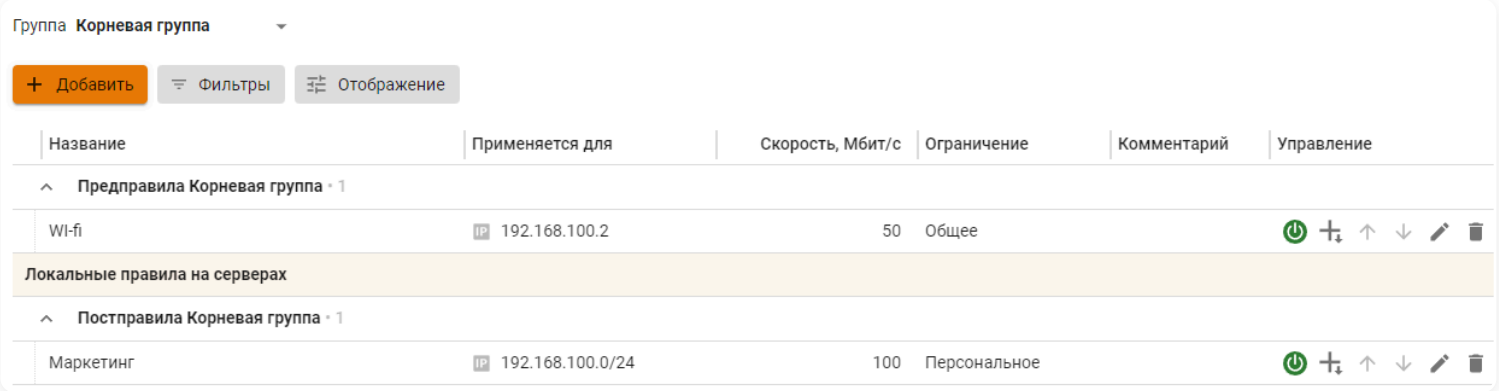
- В подключенном NGFW Novum:



Ограничение скорости

Раздел предназначен для ограничения скорости входящего интернет-трафика пользователей сети.

Процессы создания правил ограничения скорости в Ideco Center и в NGFW Novum аналогичны. Созданные в Ideco Center правила переносятся в подключенные NGFW Novum в соответствии с группами серверов:



Высокопроизводительные VCE

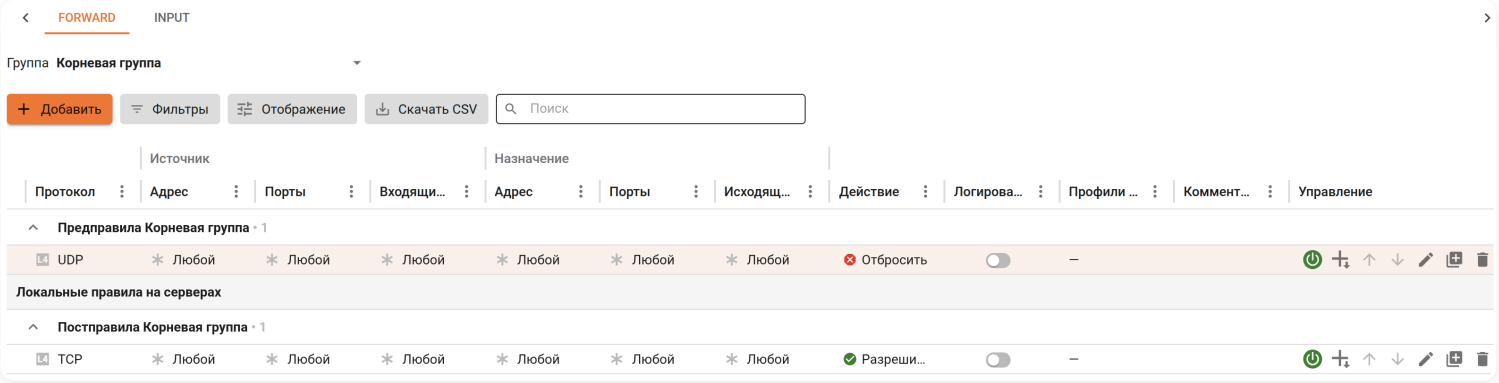
Принципы работы разделов **Межсетевой экран** и **Ограничение скорости** с подключенными VCE VPP идентичны.

Межсетевой экран

Документация API

> Чтобы создать правила для пользователей или групп безопасности Active Directory/Samba DC, предварительно настройте интеграцию в **Пользователи** → **Active Directory/Samba DC**.

Межсетевой экран Ideco Center содержит таблицы **FORWARD** и **INPUT**. Правила в них объединены в соответствии с группами серверов:



В Ideco Center

Созданные в Ideco Center правила FORWARD отображаются в виде двух таблиц: **Предправила** и **Постправила**. Правила применяются на подключенных VCE VPP в следующем порядке: сначала - **Предправила** Ideco Center, затем - **Локальные правила** VCE VPP, затем - **Постправила** Ideco Center.

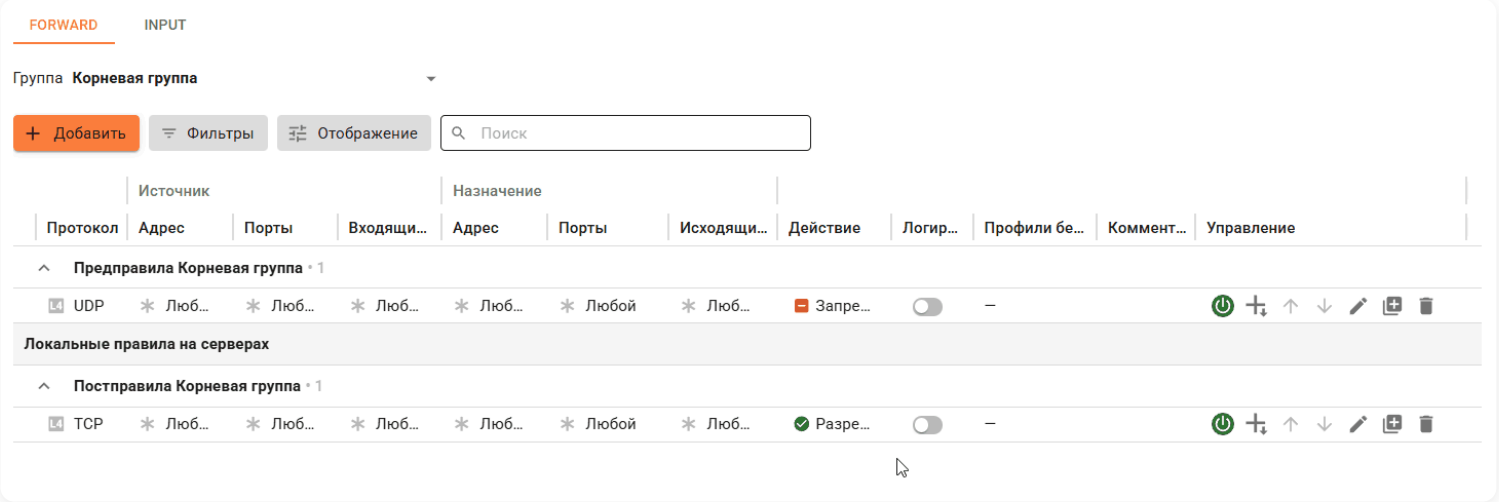
Чтобы созданное правило попало в таблицу **Предправила**, укажите в строке **Вид правила** значение **Предправило**. Если правило требуется разместить в таблице **Постправила**, выберите значение **Постправило**.

Предправила и **Постправила** в Ideco Center создаются для определенной группы серверов. Группа указывается при создании правила в поле **Группа серверов**.

Заполнение остальных полей и работа со значениями в Ideco Center и в VCE VPP идентичны.

Правила можно включать и редактировать только в Ideco Center. В VCE VPP правила доступны только для просмотра. Перемещать правила между таблицами **Предправила** и **Постправила** нельзя.

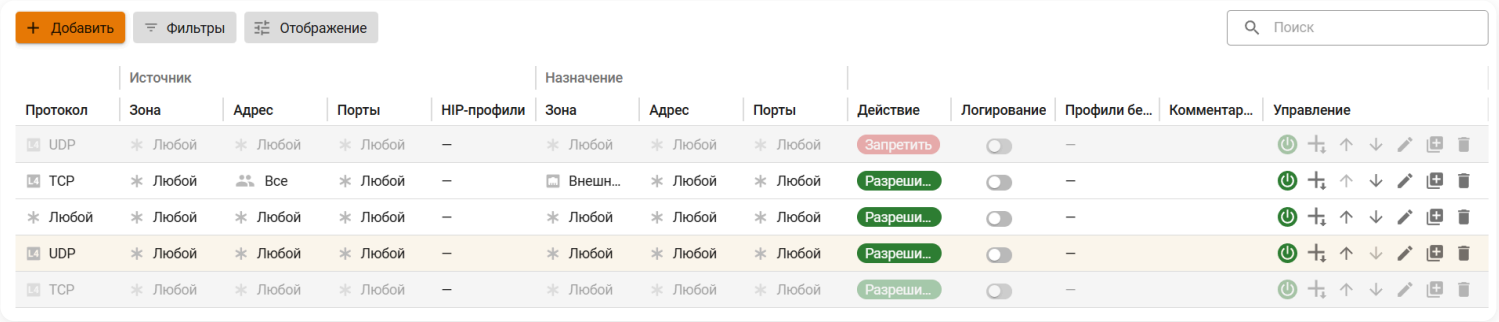
Чтобы увидеть все правила, распространяющиеся на группу серверов, выберите название группы над таблицей:



Чтобы изменить группу серверов, на которую распространяется правило, нажмите на и измените группу в соответствующей строке.

В VCE VPP

Таблица в VCE VPP визуально делится на верхнюю, среднюю и нижнюю части:



В верхнюю и нижнюю часть переносятся правила из подключенного Ideco Center. Управление этими правилами в VCE VPP невозможно. Верхняя часть соответствует таблице **Предправила** в Ideco Center. Нижняя часть - таблице **Постправила**.

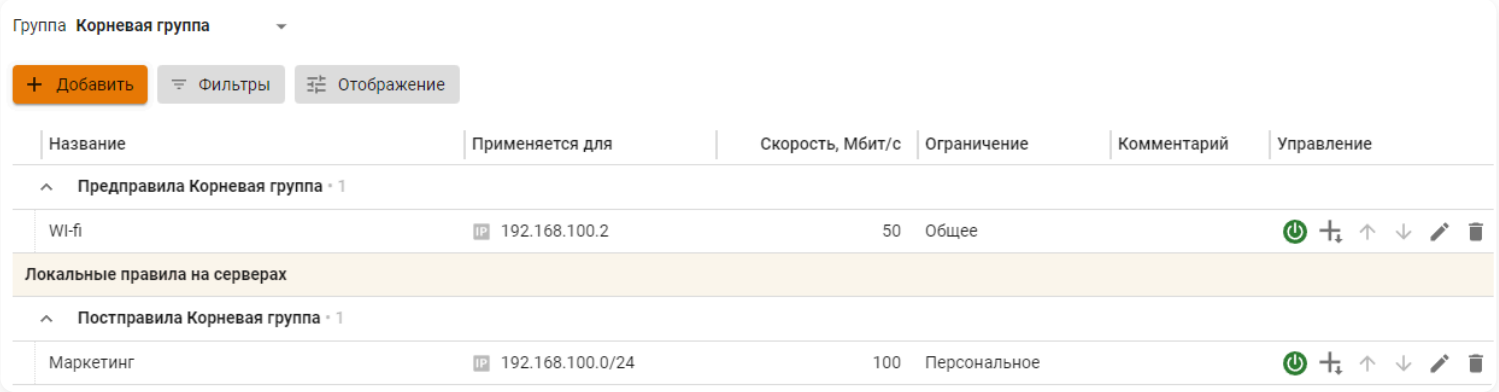
В средней части находятся **Локальные правила**, которые создаются администратором VCE VPP в самом VCE VPP.

> **Локальные правила на серверах VCE VPP** не видны в интерфейсе Ideco Center.
>
> Для просмотра перейдите в раздел **Серверы**, нажмите на в строке с нужным VCE VPP и перейдите в раздел **Межсетевой экран**.

Ограничение скорости

Раздел предназначен для ограничения скорости входящего трафика пользователей сети.

Процессы создания правил ограничения скорости в Ideco Center и в VCE VPP аналогичны. Созданные в Ideco Center правила переносятся в подключенные VCE VPP в соответствии с группами серверов:



Профили безопасности

Профили безопасности - это набор параметров, которые используются для настройки фильтрации трафика различными модулями. Они позволяют независимо друг от друга устанавливать различные политики безопасности и управлять ими, адаптируя под конкретные требования и задачи.

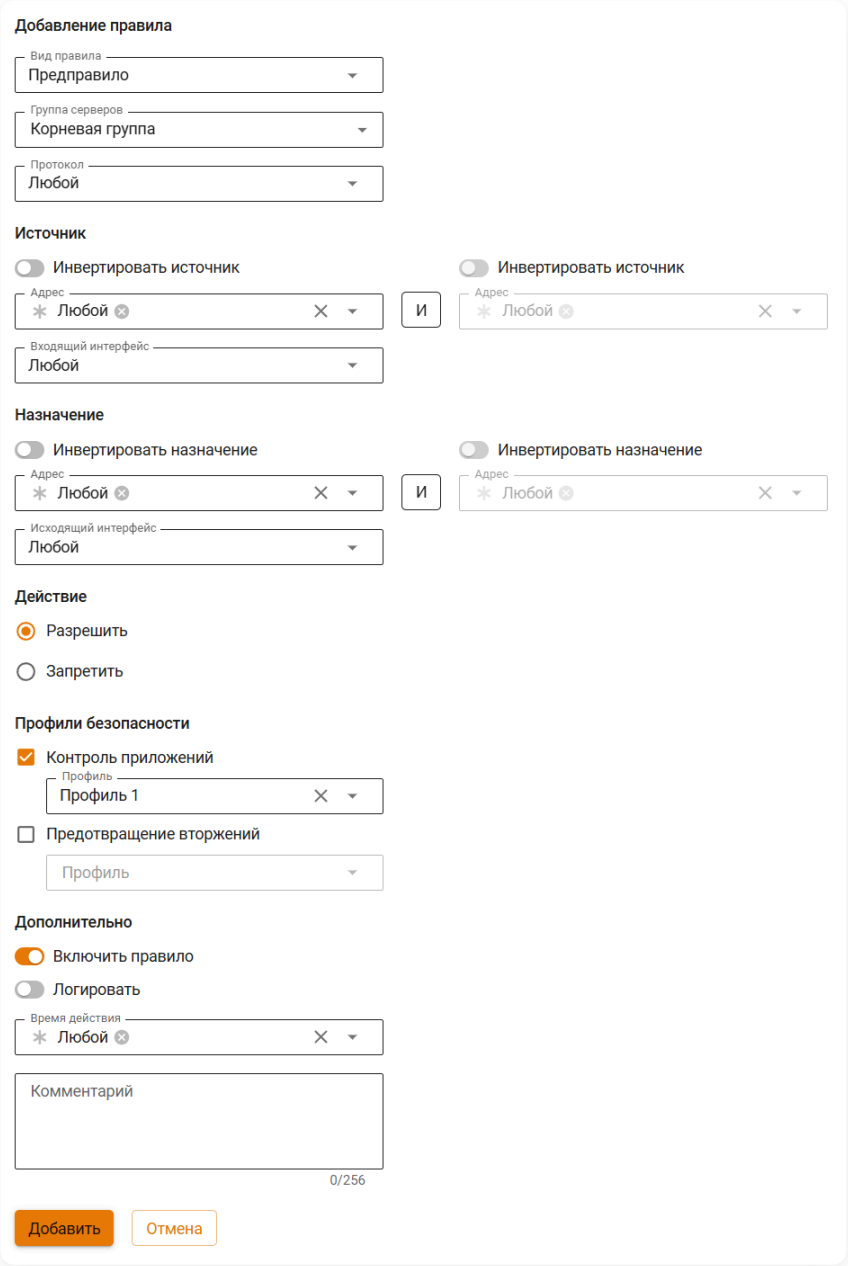
В Ideco Center можно управлять профилями безопасности для всех подключенных Ideco NGFW Novum.

Настройка профиля безопасности зависит от типа подключенного сервера. Перейдите в раздел:

- Классические VCE (NGFW Novum) - настройка профилей **Контроля приложений**, **Предотвращения вторжений** и **Web Application Firewall**.
- Высокопроизводительные VCE (VCE VPP) - настройка профилей **Контроля приложений**, **Предотвращения вторжений** и **Контент-фильтра**.

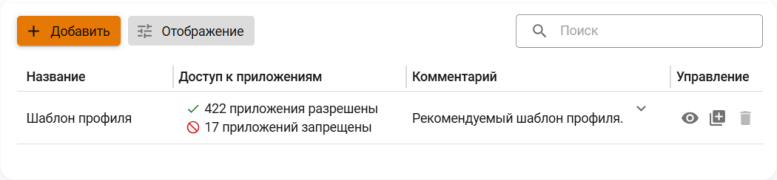
Классические VCE

Созданные в Ideco Center профили **Контроля приложений** и **Предотвращения вторжений** доступны при создании правил Межсетевого экрана:



Контроль приложений

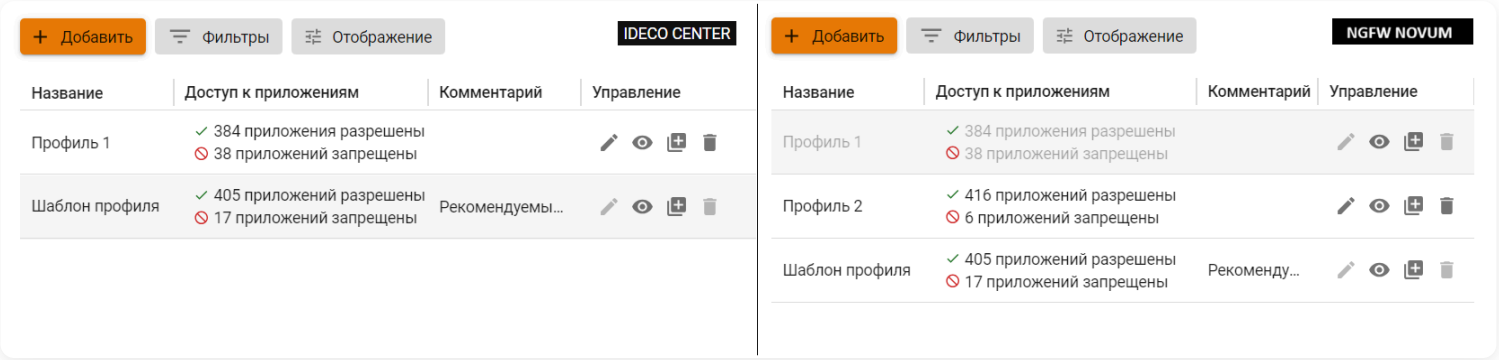
В **Профили безопасности** → **Контроль приложений** создаются профили, которые определяют, разрешен ли пользователю доступ к выбранным приложениям и протоколам:



Для определения протоколов приложений используется глубокий анализ трафика (Deep Packet Inspection - DPI).

Принцип создания и настройки профилей в Ideco Center соответствует принципам NGFW Novum. Подробное описание в статье Контроль приложений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе NGFW Novum доступен только для просмотра:

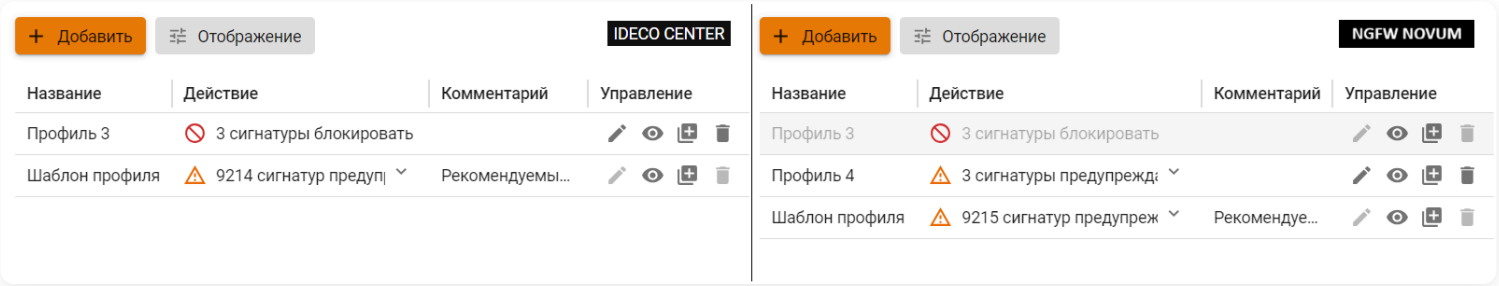


Предотвращение вторжений

В **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые подключенные NGFW будут применять к трафику, соответствующему этим сигнатурам.

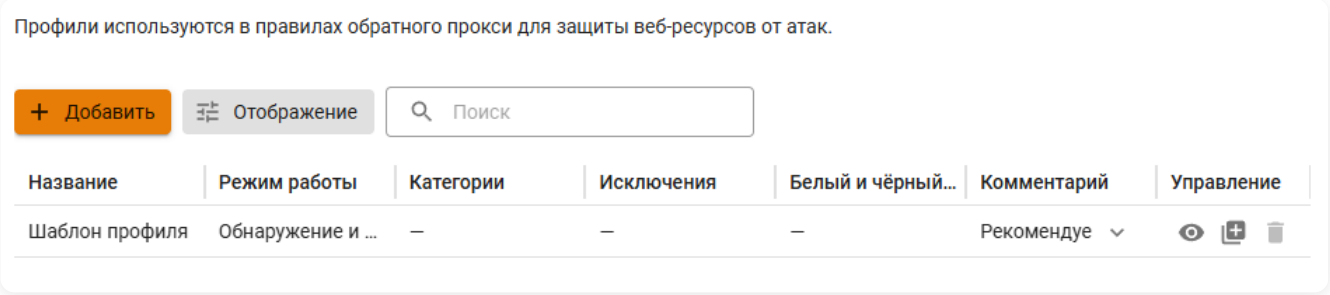
Принцип создания и использования профилей **Предотвращения вторжений** в Ideco Center аналогичен NGFW Novum. Подробнее можно узнать в статье Предотвращение вторжений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе NGFW Novum доступен только для просмотра:



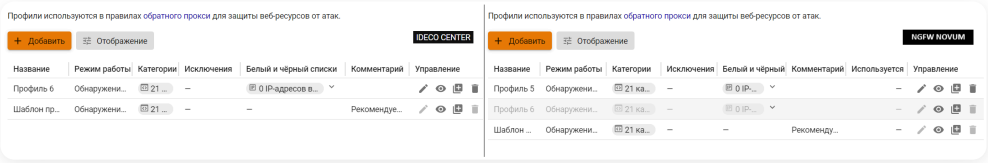
Web Application Firewall

Использование WAF-профилей позволит настроить параметры защиты для опубликованных веб-ресурсов. Профиль создается в **Профили безопасности** → **Web Application Firewall** и применяется в разделе Обратный прокси подключенного NGFW Novum:



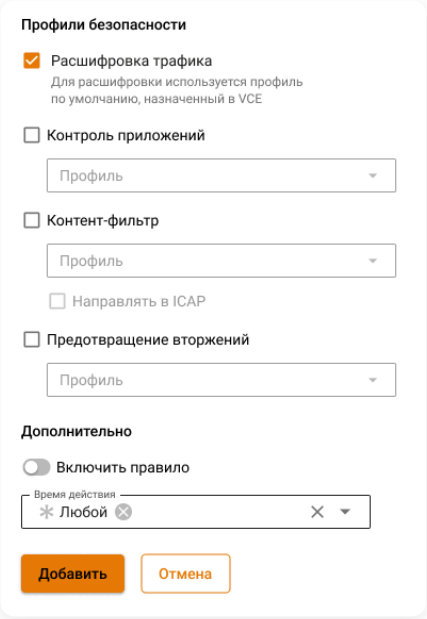
Принцип создания и использования профилей **Web Application Firewall** в Ideco Center аналогичен NGFW Novum. Подробнее можно узнать в статье Web Application Firewall.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе NGFW Novum доступен только для просмотра:



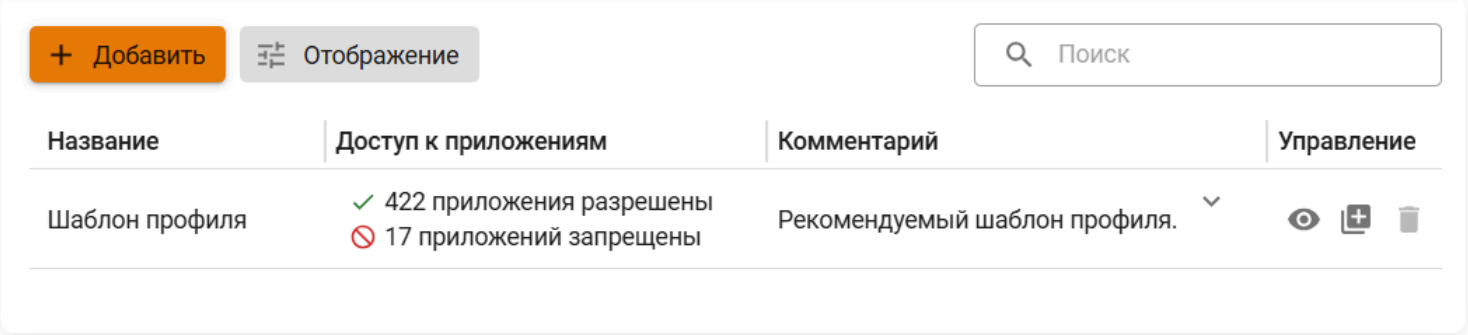
Высокопроизводительные VCE

Созданные в Ideco Center профили доступны при создании правил Межсетевого экрана:



Контроль приложений

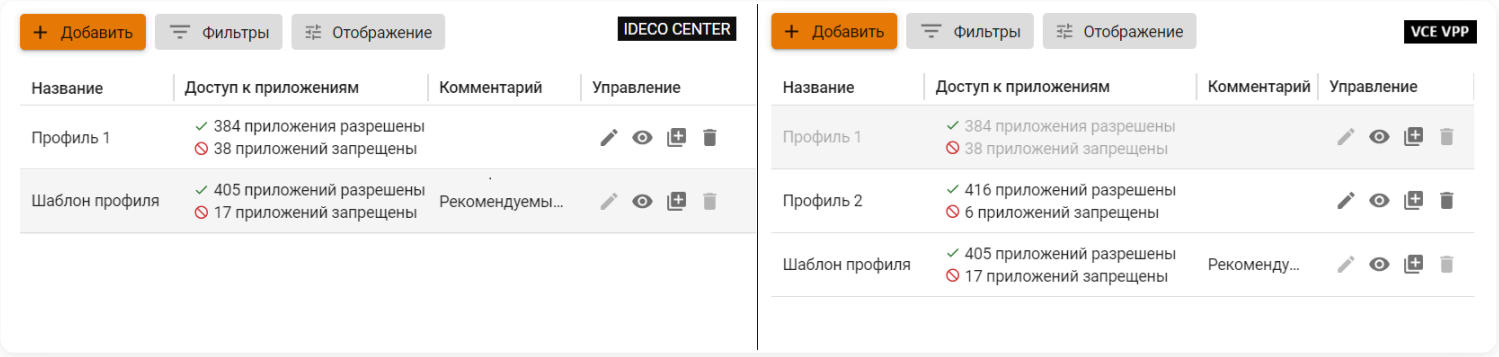
В **Профили безопасности** → **Контроль приложений** создаются профили, которые определяют, разрешен ли пользователю доступ к выбранным приложениям и протоколам:



Для определения протоколов приложений используется глубокий анализ трафика (Deep Packet Inspection - DPI).

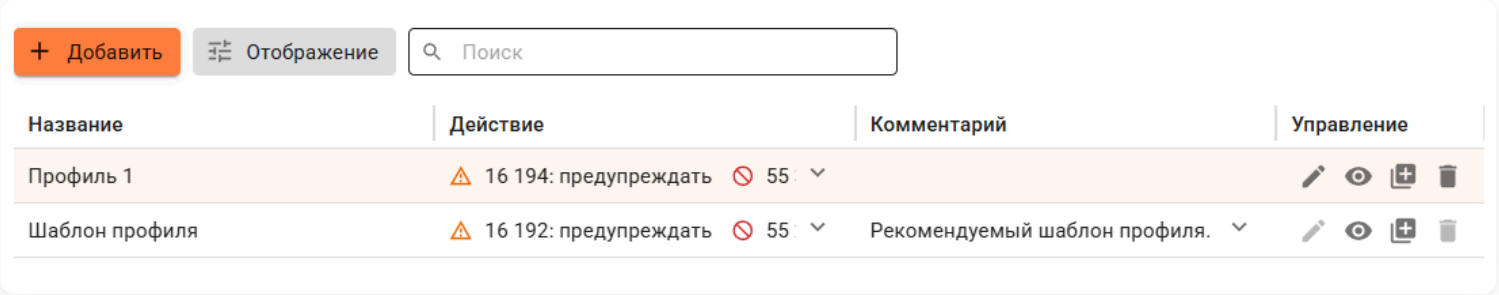
Принцип создания и настройки профилей в Ideco Center соответствует принципам VCE VPP. Подробное описание в статье Контроль приложений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе VCE VPP доступен только для просмотра:



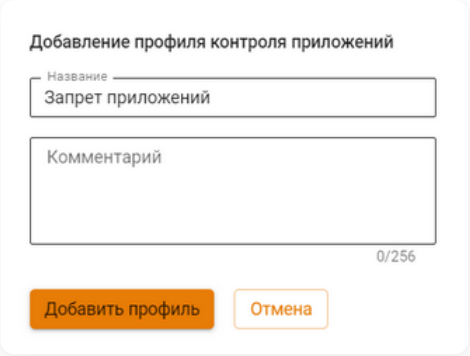
Предотвращение вторжений

В **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые синхронизированные Ideco NGFW Novum применяют к трафику, соответствующему этим сигнатурам:



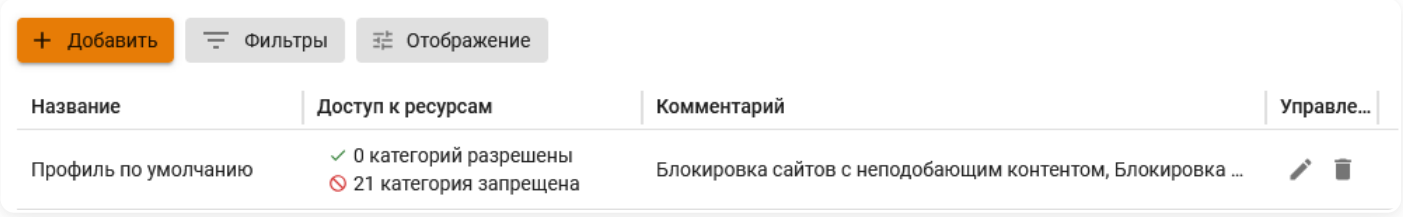
Принцип создания и использования профилей **Предотвращения вторжений** в Ideco Center аналогичен VCE VPP. Подробнее можно узнать в статье Предотвращение вторжений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе VCE VPP доступен только для просмотра:



Контент-фильтр

В **Профили безопасности** → **Контент-фильтр** создаются профили для ограничения пользователям доступа к интернет-ресурсам:



Чтобы трафик фильтровался модулем **Контент-фильтр**, создайте для локальных интерфейсов правило **FORWARD**, содержащее нужный профиль **Контент-фильтра** и включите в правиле опцию **Расшифровка трафика**. Опция использует профиль **TLS/SSL-инспекции** по умолчанию, назначенный в каждом подключенном VCE VPP.

Принцип создания и использования профилей **Контент-фильтр** в Ideco Center аналогичен VCE VPP. Подробнее можно узнать в статье Контент-фильтр.

Сервисы

Сетевые интерфейсы

При установке Ideco Center создается локальный интерфейс, через который происходит управление сервером. В отличие от Ideco NGFW Novum, в веб-интерфейсе Ideco Center можно создавать только внешние Ethernet-интерфейсы для выхода Ideco Center в интернет.

При обновлении Ideco Center с версии 21 на версию 22 роли всех сетевых интерфейсов, созданных через локальное меню, автоматически изменяются на **Control Plane**. Исключение: Loopback-интерфейсы, у которых роль остается **LAN**.

С версии 22 выбор роли интерфейсов на Ideco Center недоступен.

Для детального ознакомления с работой сетевых интерфейсов воспользуйтесь статьями:

- Физические порты
- Интерфейсы

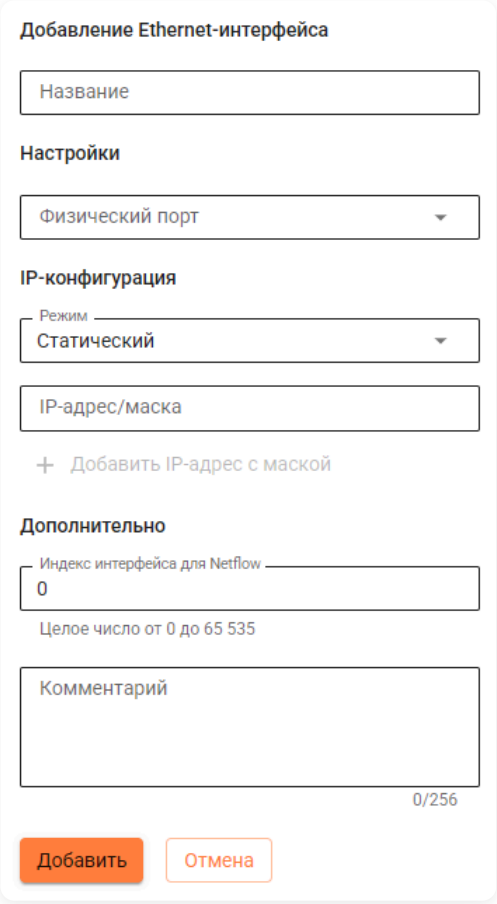
Ethernet

Ethernet - базовая технология проводных сетей, обеспечивающая передачу данных между устройствами. Технология поддерживает как прямое соединение устройств, так и работу через коммутаторы, обеспечивая гибкость и масштабируемость сетевой инфраструктуры.

Для настройки Ethernet-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Ethernet**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.
- **Физический порт** - порт на сетевом адаптере, который используется в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

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

VLAN

VLAN (Virtual Local Area Network) - виртуальный сетевой интерфейс, позволяющий создавать логические сегменты сети поверх существующей физической инфраструктуры и управлять ими. Данная технология дает возможность эффективно разделять сетевой трафик и организовывать изолированные сетевые сегменты в рамках единой сетевой структуры.

VLAN-интерфейс создается поверх родительского Ethernet-интерфейса и помечает все исходящие пакеты соответствующим тегом.

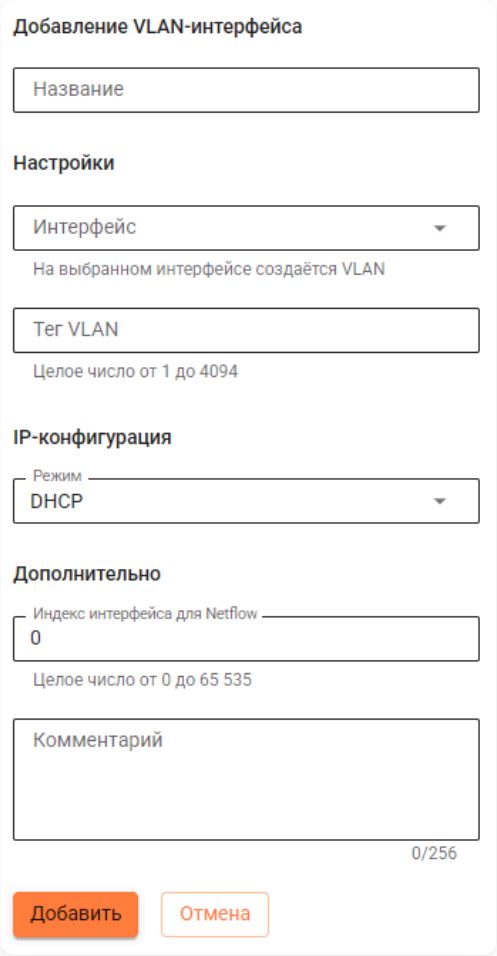
Для настройки VLAN-интерфейса выполните действия:

1. Создайте родительский Ethernet-интерфейс, если его еще нет.

> Если через физический порт должен передаваться только тегированный трафик VLAN, при настройке родительского интерфейса выберите режим **Без конфигурации**.

2. Нажмите **Добавить** и выберите **VLAN**.

3. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.

- **Интерфейс** - родительский Ethernet-интерфейс, на базе которого создается VLAN-интерфейс.
- **Тег VLAN** - числовой идентификатор VLAN (от 1 до 4094), которым помечаются все пакеты VLAN-интерфейса.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

4. Нажмите **Добавить**. VLAN-интерфейс появится в таблице интерфейсов.

LACP

LACP (Link Aggregation Control Protocol) - протокол агрегации каналов, предназначенный для объединения нескольких физических портов в единый логический интерфейс. Основное применение LACP заключается в увеличении общей пропускной способности канала и обеспечении отказоустойчивости сетевой инфраструктуры.

> Не рекомендуем использовать **LACP** на виртуальных сетевых адаптерах в Center, так как системы виртуализации часто требуют нетривиальной настройки для работы **LACP** или вообще не поддерживают этот режим. Рекомендуем настраивать агрегацию каналов средствами гипервизора.
>
> Если сетевые карты проброшены в виртуальную машину на уровне PCI (PCI passthrough), **LACP** можно настраивать внутри Center.

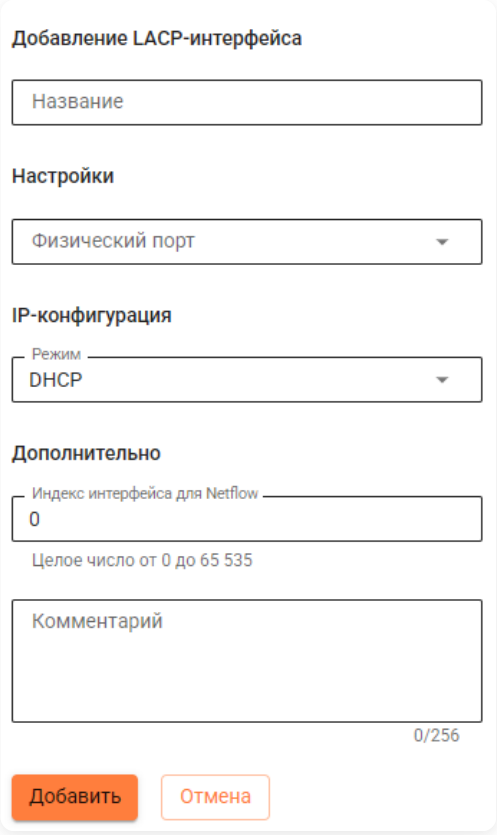
Особенности работы LACP-интерфейсов:

- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active** режим - постоянная рассылка LACP пакетов.
- Проверка соседства осуществляется в режиме **fast** - каждую секунду.
- Количество физических портов, объединяемых в агрегированный интерфейс, не ограничено со стороны Center, но также зависит от конфигурации аппаратных решений и организации сети.

Чтобы объединить несколько физических портов в один агрегированный LACP-интерфейс, выполните действия:

1. Нажмите **Добавить** и выберите **LACP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.
- **Физический порт** - порт на сетевом адаптере, который используется в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

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

Loopback

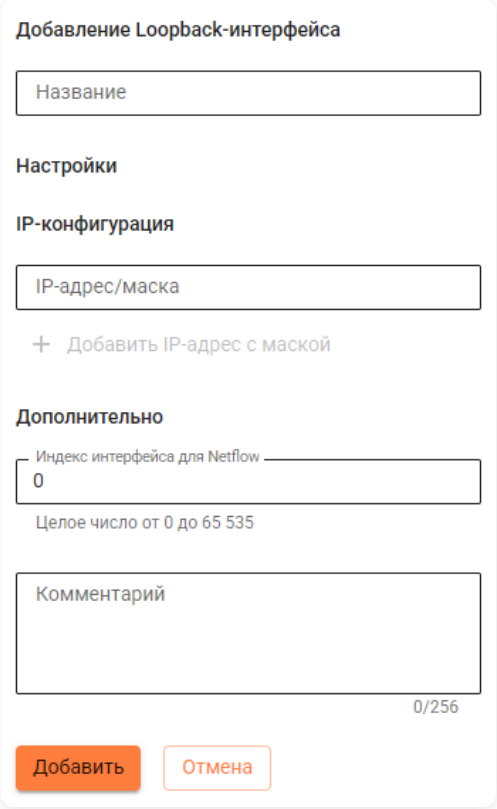
Loopback - виртуальный интерфейс, не привязанный к физическому сетевому порту. Основная задача Loopback-интерфейса - обеспечение стабильного IP-адреса для устройства, который остается доступным даже при сбоях физических соединений.

> Нельзя создавать Loopback-интерфейс в настроенном кластере. Если все же требуется использовать Loopback-интерфейс, настройте его до объединения в кластер.

Для настройки Loopback-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Loopback**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.
- **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

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

Перенастроить локальный интерфейс в Ideco Center можно через локальное меню.

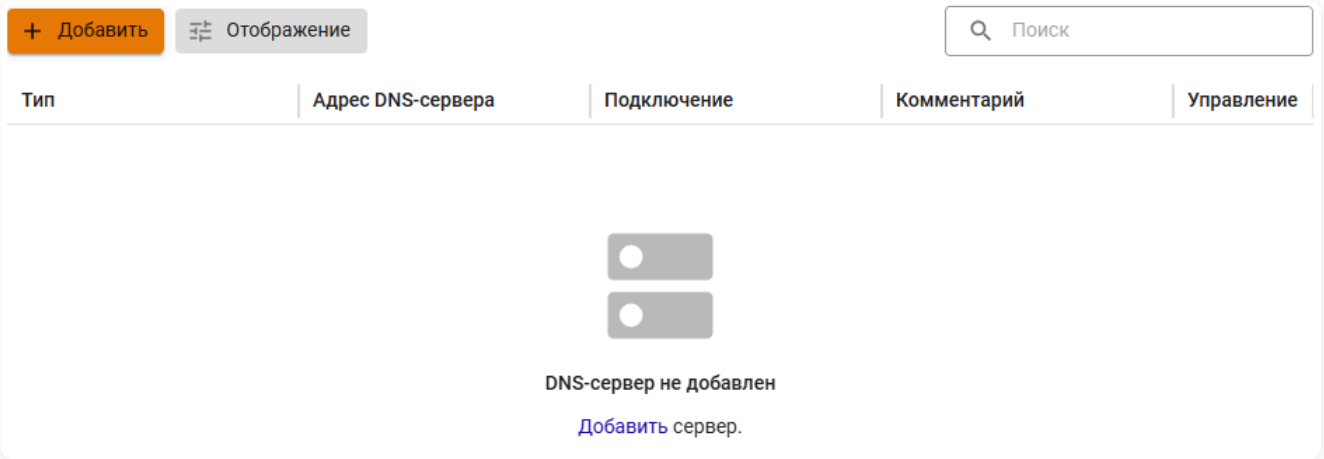
При создании, редактировании или удалении сетевого интерфейса перевыпускается SSL-сертификат, поэтому вероятно снижение скорости работы веб-интерфейса Ideco Center. В этом случае рекомендуем нажать `F5`.

DNS

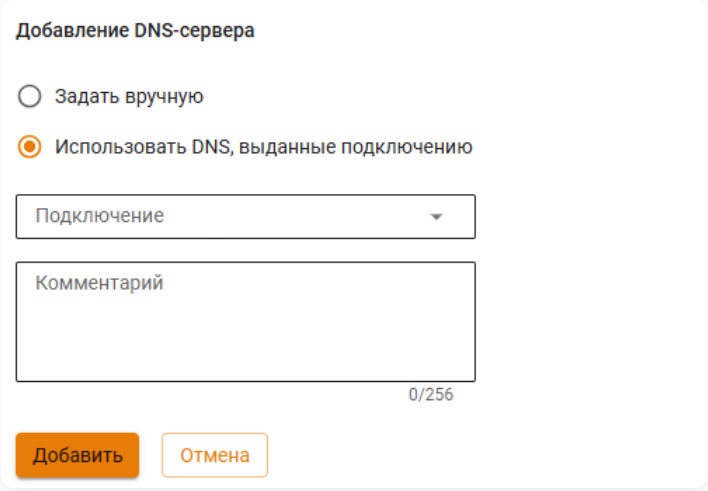
Внешние DNS-серверы

Принцип работы DNS-серверов в Ideco Center аналогичен принципу работы DNS-серверов в Ideco NGFW Novum.

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. Нажмите **Добавить**:



Выберите **Задать вручную** или **Использовать DNS, выданные подключению**, указав нужное подключение:



- Не указывайте `8.8.8.8`, `1.1.1.1` или другие известные DNS-серверы без необходимости.
- По возможности не используйте DNS, выданные интернет-провайдером, так как DNS, выданные интернет-провайдером, превышают TTL и долго отвечают.
- Укажите фильтрующие DNS-серверы, если необходимо (SkyDNS или Яндекс-DNS).
- Не используйте DNS-серверы контроллера домена, даже если домен может самостоятельно разрешать доменные имена в интернете. Это необходимо для эффективного разрешения внутренних имен домена при интеграции с AD. Для резолвинга особых зон, не связанных с AD, создайте Forward-зону вручную.

DDNS

Принцип работы DDNS в Ideco Center аналогичен принципу работы DDNS в Ideco NGFW Novum.

NTP-сервер

Настройка работы NTP-сервера в Ideco Center аналогична настройке NTP-сервера в Ideco NGFW Novum.

Сертификаты

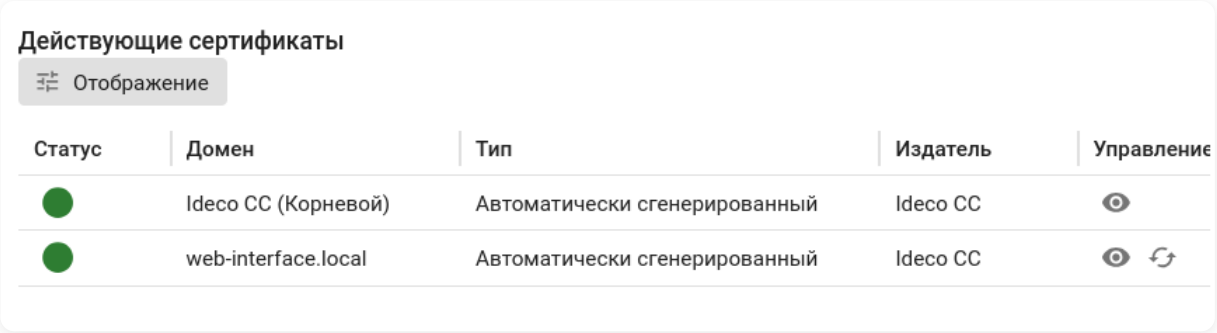
В разделе **Сертификаты** отображаются SSL-сертификаты или цепочки сертификатов, список которых формируется модулями Ideco Center.

Для просмотра основной информации о сертификате нажмите кнопку .

Процессы выпуска и перевыпуска сертификата в Ideco Center и Ideco NGFW Novum одинаковы и описаны в статье.

Действующие сертификаты

В таблице **Действующие сертификаты** отображаются:

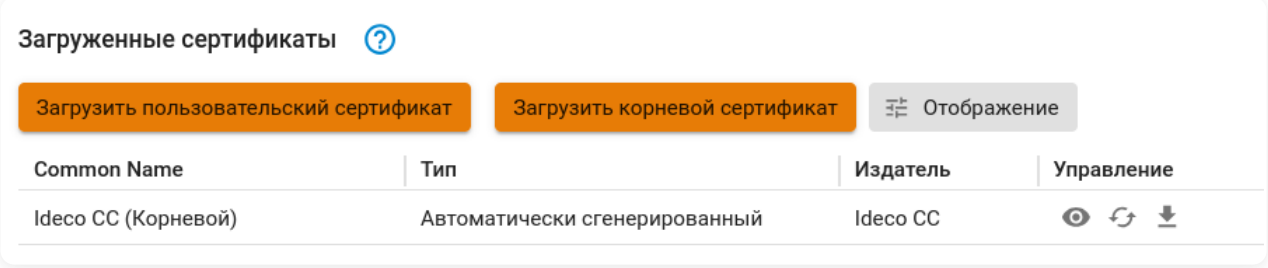


- Автоматически сгенерированные цепочки сертификатов.
- Загруженные цепочки сертификатов, используемые модулями Ideco Center.

> Если в таблице **Действующие сертификаты** одна и та же цепочка сертификатов указана в нескольких строках, то она используется несколькими модулями.

Загруженные сертификаты

В таблице **Загруженные сертификаты** отображаются:



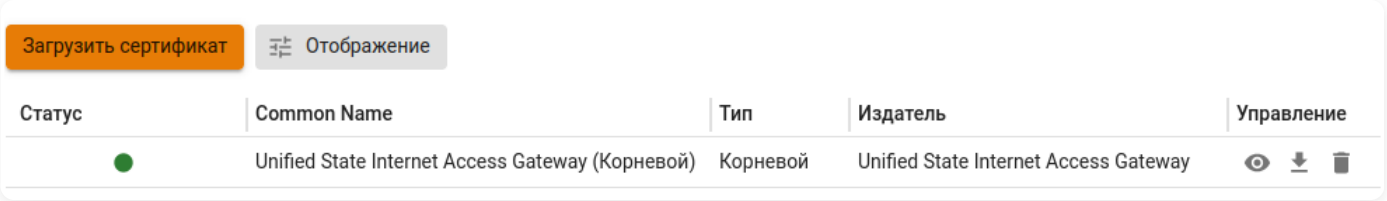
- Все загруженные цепочки сертификатов.
- Корневой сертификат Ideco Center.

> Загрузка SSL-сертификата на Ideco Center аналогична загрузке на Ideco NGFW Novum. Подробная инструкция - в статье.

На Ideco Center можно загрузить самоподписанные сертификаты, созданные в PowerShell.

Системные сертификаты

Раздел позволяет загружать свои сертификаты в хранилище доверенных сертификатов ОС Fedora на Ideco Center. Подробнее о системных сертификатах - по ссылке. После добавления сертификата в таблицу **Системные сертификаты** Ideco Center будет доверять загруженному сертификату и всем сертификатам, подписанным загруженным сертификатом:

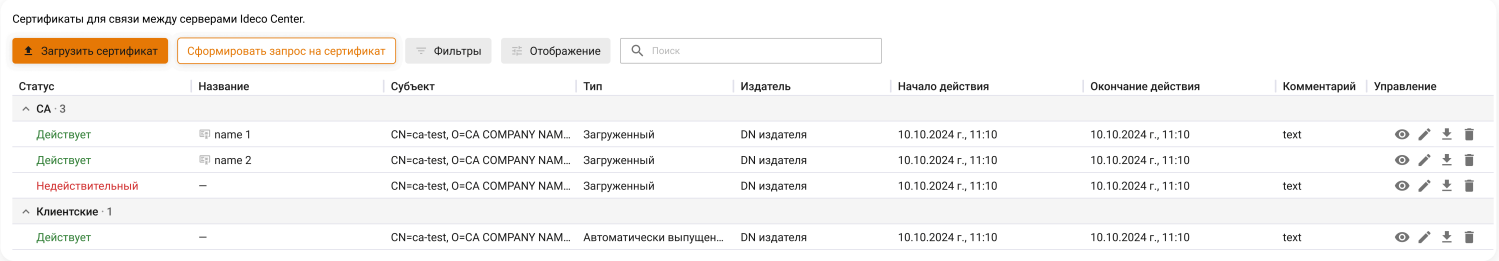


Кластеризация

В таблице **Кластеризация** отображаются сертификаты для взаимной аутентификации нод кластера. Сертификаты из этого раздела выбираются при настройке кластеризации.

Таблица разделена на две группы:

- **CA** - доверенные CA-сертификаты, загруженные вручную. Используются для проверки сертификатов другой ноды.
- **Клиентские** - клиентские сертификаты и запросы на их подпись. Используются при подключении текущей ноды к другой ноде.



Расшифровка столбцов

- **Статус** - текущее состояние сертификата:
  - **Действует** - сертификат действителен.
  - **Истекает** - до окончания срока действия осталось 30 дней или меньше.
  - **Недействительный** - срок действия истек или еще не начался.
  - **Не совпадает доменное имя** - доменное имя в сертификате не совпадает с доменным именем ноды из раздела **Управление сервером** → **Дополнительно**.
- **Название** - название сертификата.
- **Субъект** - DN (Distinguished Name) владельца сертификата.
- **Тип** - способ получения сертификата:
  - **Автоматически выпущенный** - сертификат создается и обновляется системой автоматически. Подписывается внутренним CA ноды.
  - **Загруженный** - готовый сертификат, загруженный вручную пользователем в формате `.pem`.
  - **Запрос на подпись сертификата** - промежуточный статус, когда был сформирован CSR (Certificate Signing Request), но еще не загружен подписанный сертификат. После загрузки подписанного сертификата тип поменяется на **Загруженный**.
- **Издатель** - DN (Distinguished Name) удостоверяющего центра, выпустившего сертификат.
- **Начало действия** - дата и время, с которого сертификат считается действительным.
- **Окончание действия** - дата и время истечения срока действия сертификата.
- **Комментарий** - произвольный текст, добавленный при создании или редактировании записи.
- **Управление** - действие с сертификатом:
  - - просмотр информации.
  - - редактирование названия и комментария.
  - - скачивание.
  - - удаление.

Клиентские сертификаты **CA-сертификаты**

Вкладка 5

Клиентский сертификат нода использует при подключении к другой ноде. Сертификат должен быть выпущен на доменное имя ноды, которое указывается в поле `subject.CommonName` или в расширении `subjectAltName`. Помимо самого сертификата хранится вся цепочка CA-сертификатов до корневого CA. Wildcard-сертификаты в качестве клиентских не поддерживаются.

Доступно три способа получения клиентского сертификата:

Автоматический выпуск сертификата

Автоматически выпущенный сертификат создается и обновляется системой автоматически, если в разделе **Управление сервером** → **Дополнительно** → **Адрес Ideco Center** задано доменное имя ноды. Подписывается внутренним CA ноды. Отображается с типом **Автоматически выпущенный**. Рекомендуемый вариант - дополнительных действий не требуется.

> Если автоматически выпущенный сертификат удалить, система перевыпустит его с тем же идентификатором.

Загрузка сертификата

Загрузка готового клиентского сертификата с приватным ключом и цепочкой CA-сертификатов в формате `.pem`. Для загрузки:

1. Нажмите **Загрузить сертификат** и выберите сохраненный ранее сертификат. При загрузке отобразится превью:

Расшифровка полей

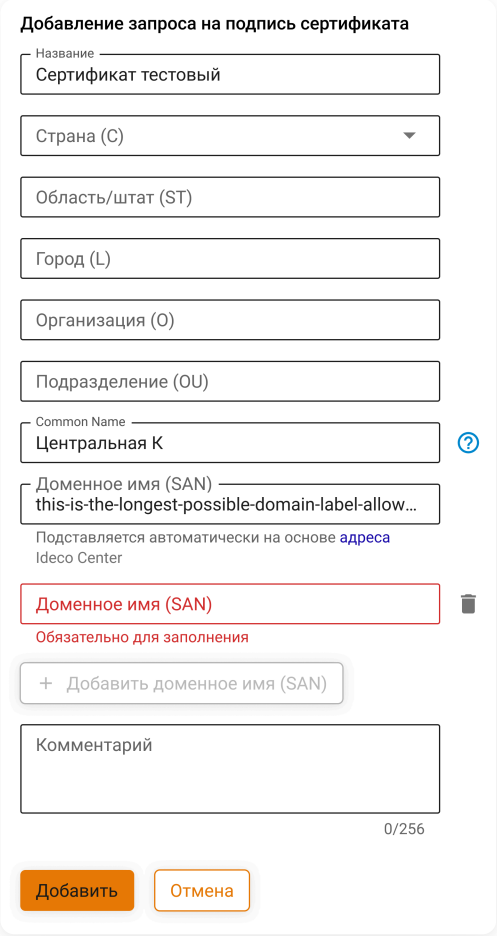
- **Тип** - способ получения сертификата: **Загруженный** или **Автоматически выпущенный**.
- **Субъект** - DN (Distinguished Name) владельца сертификата, содержащий доменное имя ноды.
- **Издатель** - DN удостоверяющего центра, подписавшего сертификат.
- **Вид ключа** - алгоритм криптографического ключа.
- **Срок действия** - период действия сертификата: дата начала и дата окончания.
- **Название** - укажите название сертификата. Обязательное поле.
- **CSR ID** - уникальный идентификатор CSR, на основе которого был выпущен сертификат. Отображается, если сертификат был создан на основе запроса из системы.
- **Комментарий** - произвольный текст.

2. Нажмите **Загрузить**, чтобы добавить сертификат в список.

Формирование запроса на сертификат

Формирование запроса на подпись клиентского сертификата. Для создания запроса:

1. Нажмите **Сформировать запрос на сертификат** и заполните поля:



Расшифровка полей

- **Название** - укажите название сертификата. Обязательное поле.
- **Страна (C)** - выберите страну из списка.
- **Область/штат (ST)** - введите название области, до 128 символов.
- **Город (L)** - введите название города, до 128 символов.
- **Организация (O)** - введите название организации, до 64 символов.
- **Подразделение (OU)** - введите название подразделения, до 64 символов.
- **Common Name** - предзаполняется названием сервера Ideco Center. Можно редактировать, до 64 символов. Обязательное поле.
- **Доменное имя (SAN)** - предзаполняется адресом Ideco Center из раздела **Управление сервером** → **Дополнительно**. Домены `.local` не допускаются. Только латинские буквы (допускается Punycode). Можно добавить до 3 доменных имен SAN, минимум 1. Обязательное поле.
- **Комментарий** - произвольный текст.

> Если в полях Common Name и Доменное имя (SAN) указаны одинаковые домены, они объединяются автоматически.

2. Нажмите **Добавить**. В списке появится запись со статусом **Запрос на подпись сертификата** в столбце **Тип**.

3. Нажмите в столбце **Управление** и скачайте CSR (Certificate Signing Request).

4. Выпустите на его основе сертификат.

5. Загрузите выпущенный сертификат согласно инструкции **Загрузка сертификата**.

Вкладка 6

CA-сертификаты используются для проверки сертификатов другой ноды. Списки доверенных CA (Certificate Authority) для проверки клиентского и серверного сертификатов задаются раздельно в настройках кластера.

В качестве доверенного CA можно использовать публичный, корпоративный или внутренний CA самой ноды. Дополнительно в настройках кластера доступен вариант **Все системные CA-сертификаты** - при его выборе используется все системное хранилище доверенных сертификатов.

CA-сертификаты загружаются вручную в формате `.pem` - без приватного ключа и цепочки. Поддерживаются как корневые, так и промежуточные CA-сертификаты.

Для загрузки CA-сертификата:

1. Нажмите **Загрузить сертификат**.

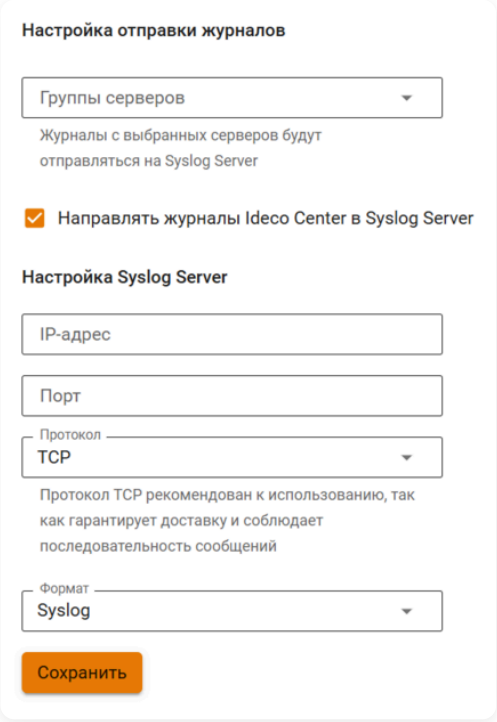
2. Выберите файл в формате `.pem`.

3. Нажмите **Загрузить**, чтобы добавить сертификат в список.

Syslog

Модуль позволяет отправлять все системные сообщения (syslog) с группы серверов Ideco NGFW Novum в сторонние коллекторы (Syslog Collector) или в SIEM-системы.

Чтобы настроить пересылку системных сообщений, перейдите в **Отчеты и журналы** → **Syslog** и выполните:



1. Выберите группу серверов NGFW, журналы с которых будут передаваться на Syslog Server.

> Опция **Направлять журналы Ideco Center в Syslog Server** позволяет отправлять журналы, генерируемые самой Ideco Center, на Syslog Server.

2. Укажите IP-адрес сервера-коллектора (любой локальный или публичный IP-адрес).

3. В поле **Порт** укажите порт, настроенный на сервере-коллекторе (в диапазоне от 1 до 65535).

4. Выберите протокол для передачи системных логов: TCP или UDP.

5. Выберите формат, в котором будут передаваться системные сообщения: Syslog или CEF.

6. Нажмите **Сохранить** и включите опцию **Syslog**.

Примеры расшифровки передаваемых логов представлены в статье.

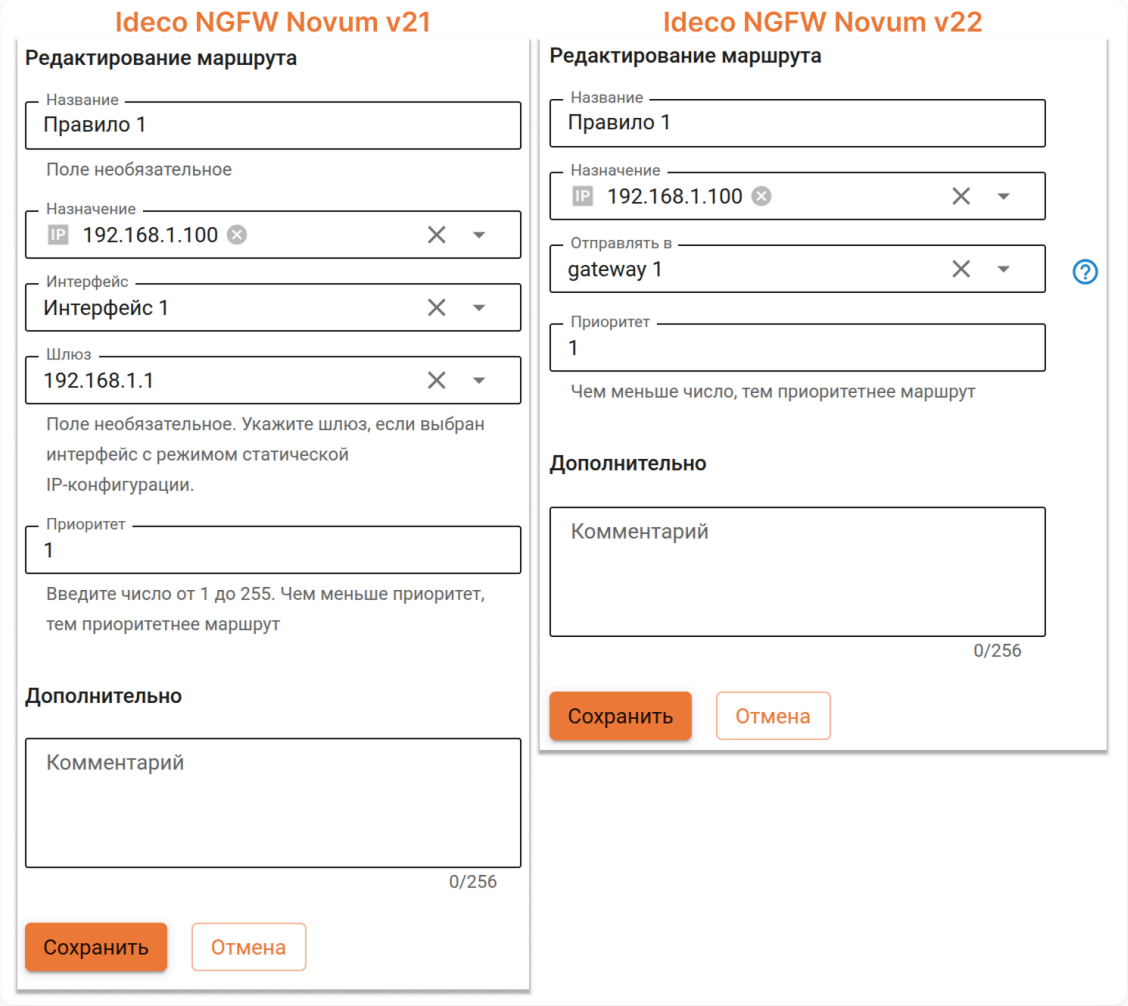
SD-WAN

SD-WAN (Software-Defined Wide Area Network) - технология программно-определяемых распределенных сетей, которая управляет WAN-каналами на основе политик и обеспечивает интеллектуальную маршрутизацию трафика между филиалами, центрами обработки данных и облачными сервисами.

Миграция при обновлении

Логика создания **Next hop** при миграции маршрутов зависит от исходной конфигурации:

- Если в маршруте был указан **Интерфейс** - автоматически создается **Next hop**. Пример правила статической маршрутизации:



- Если в маршруте не был указан **Интерфейс** - **Next hop** не создается, маршрут сохраняется в прежнем виде. Пример правила статической маршрутизации:

Ideco NGFW Novum v21

Редактирование маршрута

Название
Правило 1

Поле необязательное

Назначение
IP 192.168.1.100

Интерфейс

Шлюз
192.168.1.1

Поле необязательное. Укажите шлюз, если выбран интерфейс с режимом статической IP-конфигурации.

Приоритет
1

Введите число от 1 до 255. Чем меньше приоритет, тем приоритетнее маршрут

Дополнительно

Комментарий

0/256

Сохранить Отмена

Ideco NGFW Novum v22

Редактирование маршрута

Название
Правило 1

Назначение
IP 192.168.1.100

Отправлять в
192.168.1.1

Приоритет
1

Чем меньше число, тем приоритетнее маршрут

Дополнительно

Комментарий

0/256

Сохранить Отмена

Next hop

API

Next hop - это следующий узел маршрутизации, на который передается сетевой трафик для дальнейшей доставки к целевой сети. В рамках **SD-WAN** next hop определяется после выбора маршрута до точки назначения и задает, через какой интерфейс и шлюз будет отправляться трафик.

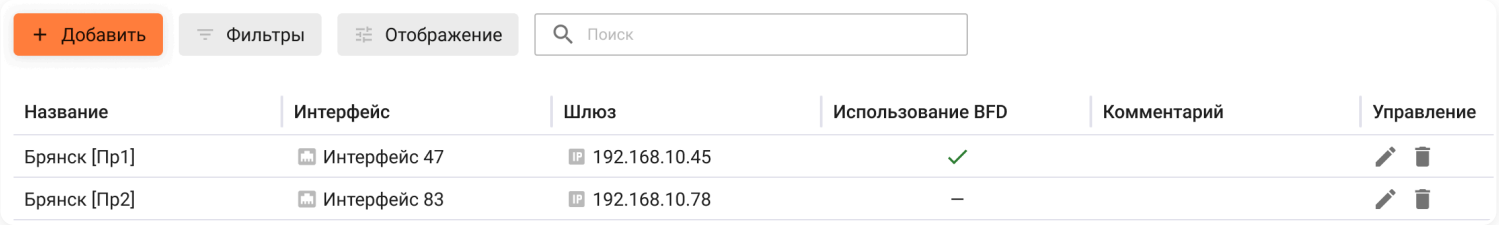
Next hop используется при настройке **Статической** маршрутизации.

Если нет необходимости в проверке доступности шлюза или резервировании, в поле **Отправить в** достаточно указать IP-адрес как **Объект** или **Значение**. Создайте **Next hop**, если:

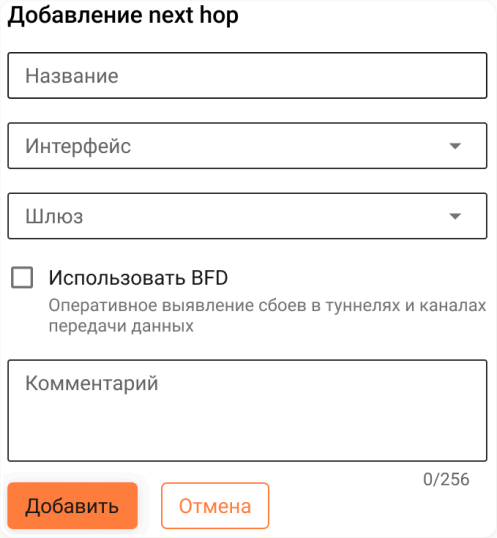
- Нужна проверка доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection).
- Планируется объединить несколько шлюзов в **Профиль next hop** для резервирования или балансировки трафика.
- При настройке **Статического** маршрута необходимо указать интерфейс.

Для добавления **Next hop** выполните действия:

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



2. Заполните поля:



- **Название** - укажите название.
- **Интерфейс** - выберите сетевой интерфейс, через который будет отправляться трафик к следующему узлу.
- **Шлюз** - укажите IP-адрес следующего узла маршрутизации (next hop), на который будет направляться трафик. Адрес шлюза должен находиться в сети выбранного интерфейса.
- **Использовать BFD** - включите опцию для проверки доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection). Поддерживается только для статических маршрутов. BFD должен быть включен и на стороне указанного шлюза.
- **Комментарий** - необязательное поле для описания **Next hop**.

Интерфейс с ролью **Control Plane** используется только для настройки и администрирования Center. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям Center.

Маршрутизация

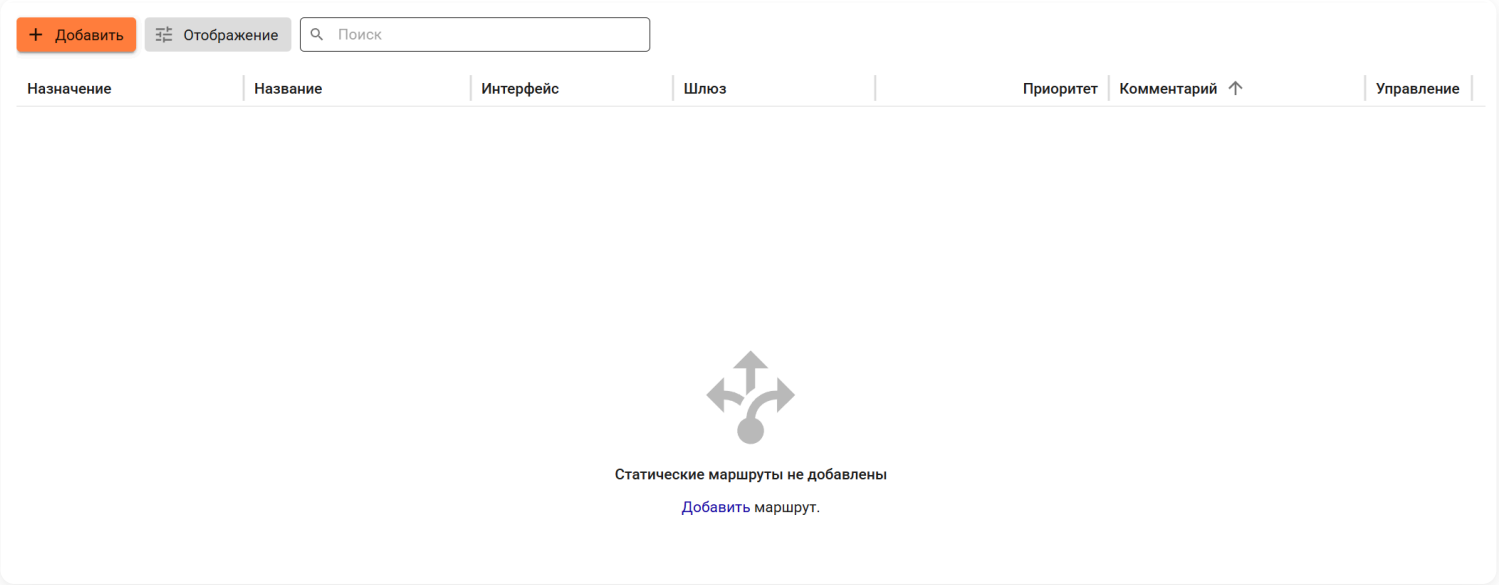
В разделе описана настройка статической маршрутизации.

Статическая маршрутизация

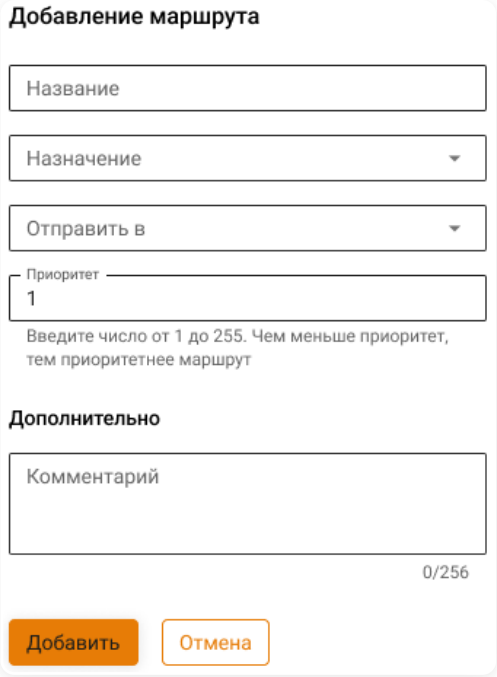
Статическая маршрутизация применяется в сценариях, где нет необходимости в сложной логике маршрутизации. Обработка статических маршрутов происходит после PBR, но до динамической маршрутизации и маршрутизации внешних сетей.

Для добавления статического маршрута выполните действия:

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



2. Заполните поля:



Расшифровка полей

- **Название** - укажите название правила.

- **Назначение** - выберите объекты, при обращении к которым будет применяться это правило. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
- **Отправить в** - выберите IP-адрес или Next hop, через который будет отправлен трафик. IP-адрес можно указать как **Объект** или **Значение**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

Отличие значений от объектов:

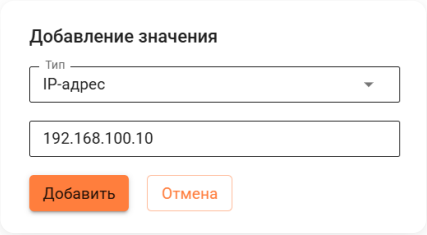
- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

Управление значениями

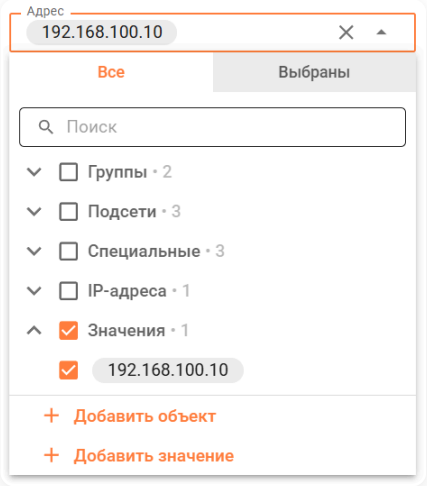
Добавление

1. В поле нажмите **Добавить значение**:

2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:



Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:

2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

Интерфейс с ролью **Control Plane** используется только для настройки и администрирования Center. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям Center.

- **Приоритет** - укажите приоритет маршрута. Чем меньше число, тем выше приоритет. При значении 255 трафик по этому маршруту будет заблокирован.
- **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

С версии 22 Ideco Center не поддерживает указание пользователя в поле **Шлюз**. Если в правиле был указан пользователь, перед обновлением замените его на IP-адрес вручную.

Особенности

- **Порядок обработки маршрутов:**
  Статические маршруты обрабатываются после PBR, но до динамической маршрутизации (BGP, OSPF и EIGRP). Если в статической маршрутизации задан шлюз по умолчанию, трафик будет отправлен через него и не дойдет до динамической маршрутизации и правил маршрутизации внешних сетей.
- **Резервные маршруты через приоритет:**
  Если установить приоритет статического маршрута в диапазоне от 200 до 254, он станет менее приоритетным, чем маршруты, полученные через протоколы динамической маршрутизации. Это позволяет использовать статические маршруты как резервные:
  - Если динамическая маршрутизация предоставляет путь к сети, будет использован динамический маршрут.
  - Если динамический маршрут отсутствует, трафик пойдет по статическому маршруту.
- **Балансировка нагрузки (ECMP):**
  Если создать два маршрута к одному назначению с одинаковым приоритетом, трафик будет распределен между ними по принципу ECMP (Equal-Cost Multi-Path).
- **Блокировка трафика:**
  При значении приоритета 255 трафик по маршруту блокируется.

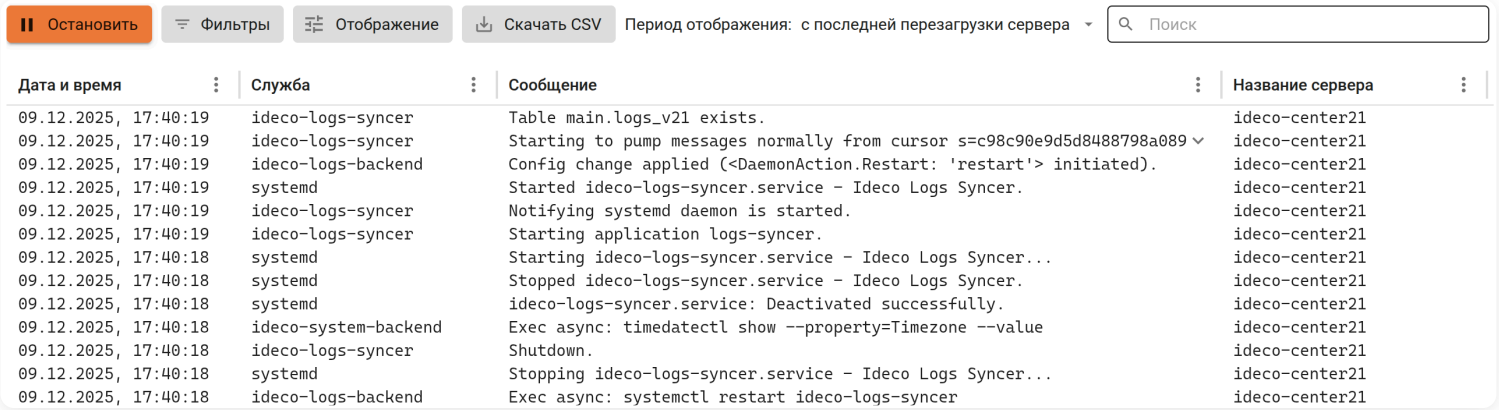
Отчеты и журналы

Система

Время хранения логов в разделе **Система** - 90 дней. После этого логи доступны в **Управление сервером -> Терминал**. Ограничение на размер журнала - 5 ГБ на каждый NGFW.

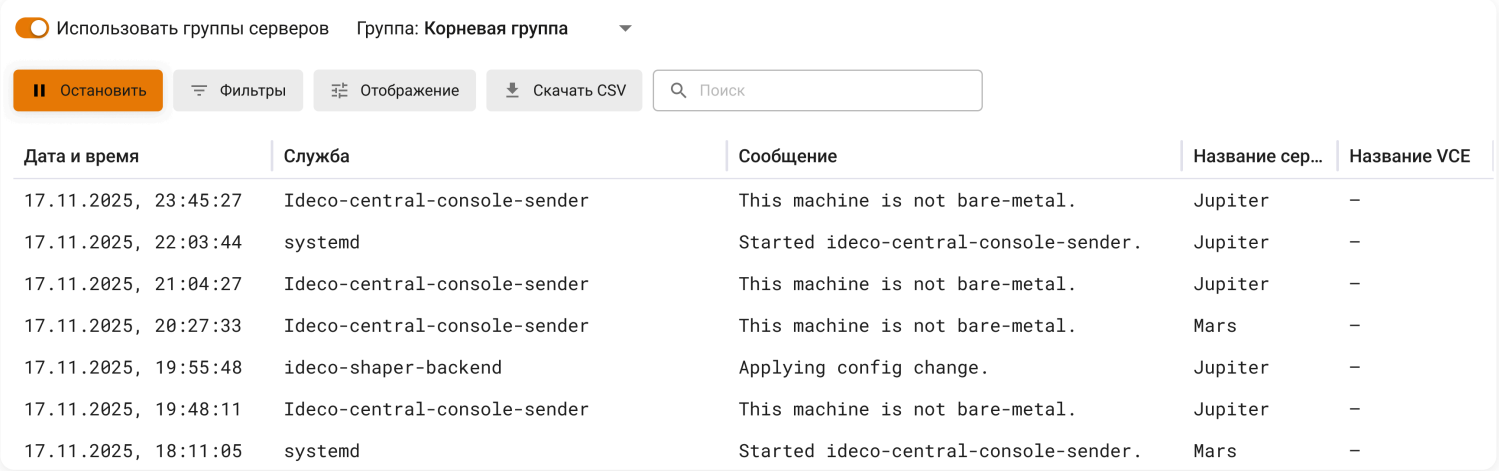
Журнал Ideco Center

На вкладке доступен просмотр логов Ideco Center:



Журнал серверов

На вкладке можно выбрать группу серверов для просмотра логов подключенных Ideco NGFW Novum:



- **Использовать группы серверов** - при включении опции отображаются данные серверов, находящихся в выбранной группе. При выключенной опции отображаются журналы всех системных и дочерних контекстов.

Включите опцию **Отправлять журналы на Ideco Center** в разделе **Управление сервером -> Ideco Center** на каждом Ideco NGFW Novum, чтобы в таблице отображались логи подключенных серверов.

Отправка журналов возможна только в **Системном контексте**. Корневой NGFW отправляет данные на Ideco Center со всех контекстов.

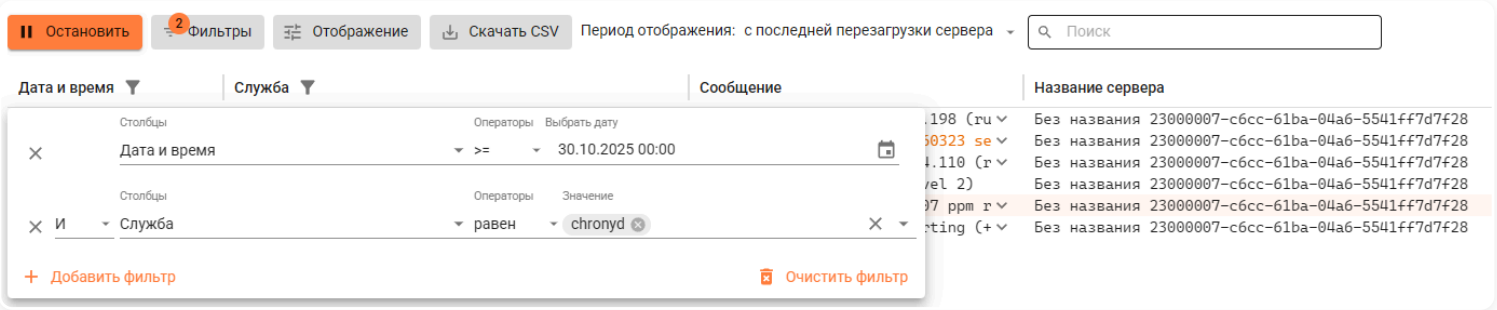
Отображение журналов в Ideco Center зависит от того, какие контексты подключены в разделе **Серверы**:

- **Системный контекст и VCE подключены** - доступны логи системного и дочерних контекстов.
- **Системный контекст подключен, VCE не подключен** - доступны логи только системного контекста. Для отображения логов VCE выключите опцию **Использовать группы серверов**.

- **Подключен только VCE** - логи не отправляются, VCE получает только правила фильтрации.

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.

Список служб, доступных в разделе

- **Серверы** - `ideco-servers-backend`, `ideco-servers-websocket`.
- **Межсетевой экран** - `ideco-firewall-backend`, `ideco-firewall-rest`.
- **Контент-фильтр** - `ideco-content-filter-backend`.
- **Предотвращение вторжений** - `ideco-suricata-backend`.
- **Объекты** - `ideco-alias-backend`.
- **Сетевые интерфейсы** - `ideco-network-backend`, `ideco-network-nic`.
- **Маршрутизация** - `ideco-routing-backend`, `ideco-routing-rest`.
- **Обратный прокси** - `ideco-reverse-backend`.
- **Защита и управление DNS** - `ideco-dns-backend`, `unbound`, `nsd`, `unbound-anchor`, `unbound-keygen`.
- **DHCP-сервер** - `ideco-dhclient`.
- **NTP-сервер** - `chronyd`.
- **Кластеризация** - `ideco-cluster-backend`.
- **Обновления** - `ideco-sysupdate-backend`.
- **Бэкапы** - `ideco-backup-backend`, `ideco-backup-create`.
- **Лицензия** - `ideco-license-backend`.
- **Syslog** - `ideco-logs-backend`, `ideco-monitor-backend`.
- **Отчеты и журналы** - `ideco-logs-backend`, `ideco-logs-syncer`.
- **Действия администраторов** - `ideco-audit-backend`.
- **Авторизация администраторов** - `ideco-web-backend`.
- **Сертификаты** - `ideco-cert-backend`.
- **Локальное меню** - `ideco-local-menu`.
- **Дополнительно** - `ideco-system-backend`.
- **Сбор анонимной статистики о работе сервера** - `ideco-gatherstat-backend`.
- **Защита от несанкционированного доступа, в т.ч. от брутфорс-атак (brute force - атака полным перебором)** - `fail2ban`.
- **REST API NGFW** - `ideco-rest-api-backend`.
- **Доступ по SSH** - `sshd`.

Служебное:

- **Сервер базы данных** - `clickhouse-server`.
- **Сервер управления nginx Ideco** - `nginx-control-plane`.
- **Сервис для очистки невалидных подключений** - `ideco-conndrop`.
- **Локальная база данных** - `ideco-etcd-runtime`, `ideco-etcd-permanent`.
- **Блокировка источников и назначений из файла** - `ideco-apply-manual-blocklist`.
- **Управление лицензиями в облачной среде** - `ideco-vk-cloud-license`.
- **Проверка целостности файлов** - `ideco-check-sums`.
- **Проверка прав пользователей на перезапуск служб systemd** - `ideco-policy-backend`.
- **Управление SWAP-разделами** - `ideco-system-swap`.
- **Сбор метрик и статистики** - `prometheus`, `prometheus-node-exporter`.

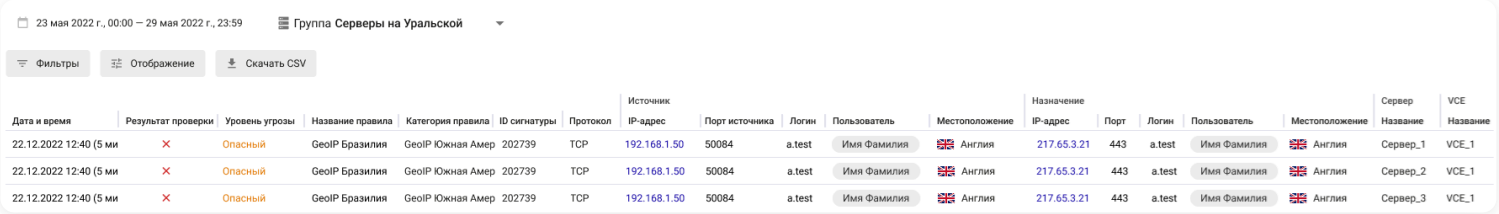
События безопасности

Документация API

В разделе отображаются события безопасности с подключенных серверов Ideco NGFW Novum. При подключении NGFW отправляются данные со всех его VCE. Чтобы посмотреть события конкретного VCE, подключите этот контекст отдельно.

Журнал IPS

Вкладка **Отчеты и журналы** → **События безопасности** → **Журнал IPS** содержит логи системы **Предотвращения вторжений**. Для просмотра событий выберите сервер или группу серверов:

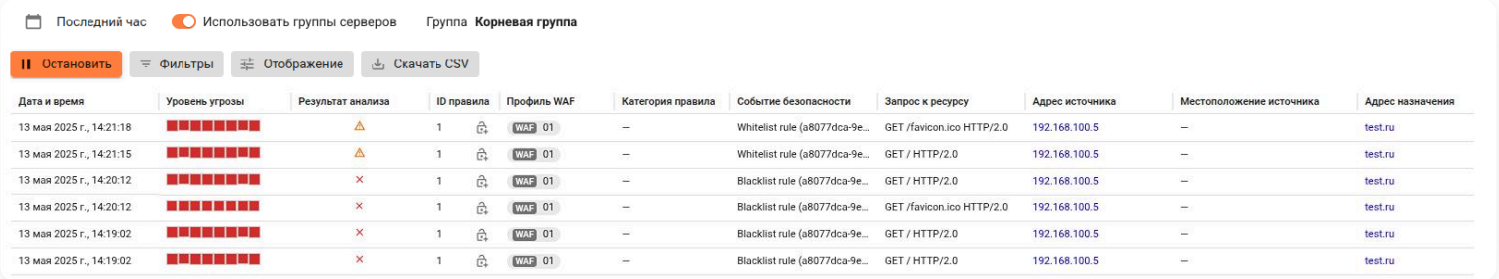


- Поле **Результат проверки** отображает действие системы:
  - `Blocked` - пакет блокирован.
  - Любая другая информация в этом поле - `Allowed`, информирование.
- В поле **Уровень угрозы** могут отображаться следующие значения:
  - Критичный
  - Опасный
  - Предупреждение
  - Не распознано
  - Не классифицировано

IP-адреса в столбцах **Источник** и **Назначение** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.

Web Application Firewall

Вкладка **Отчеты и журналы** → **События безопасности** → **Web Application Firewall** содержит информацию о срабатывании правил **Web Application Firewall** в виде таблицы:



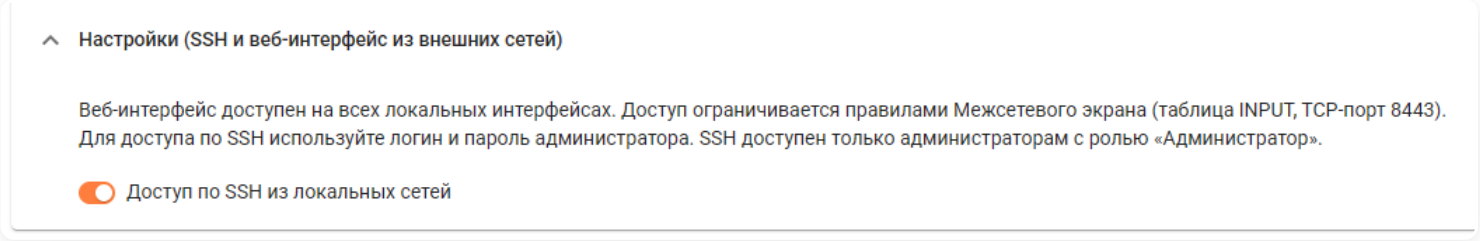
- **Использовать группы серверов** - при включении опции отображаются данные серверов, находящихся в выбранной группе. При выключенной опции отображаются журналы всех системных и дочерних контекстов.

Для проверки IP-адресов в столбцах **Адрес источника** и **Адрес назначения** скопируйте адрес и выполните его поиск в сервисе Whois.

На вкладке **Web Application Firewall** отображается профиль WAF, параметры которого вызвали блокировку доступа к ресурсу.

Действия администраторов

Ideco Center логирует действия администраторов, которые вносят изменения в конфигурацию Ideco Center из веб-интерфейса, локального меню и терминала:

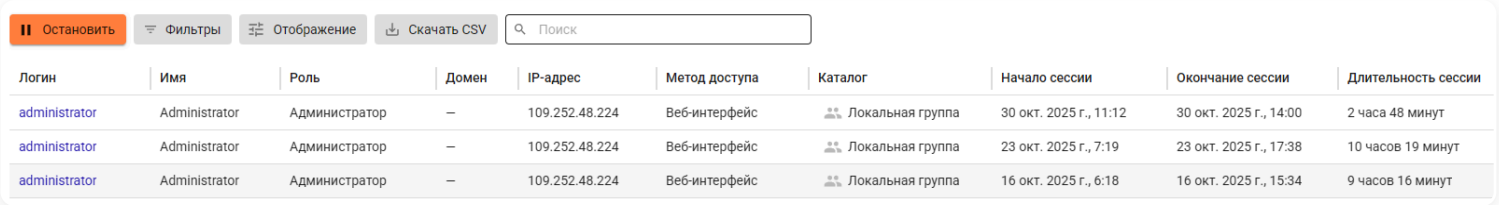


Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

Аутентификация администраторов

Время хранения данных в журнале **Аутентификация администраторов** - 1 год.

В разделе отображается список авторизованных администраторов:



Логин	Имя	Роль	Домен	IP-адрес	Метод доступа	Каталог	Начало сессии	Окончание сессии	Длительность сессии
administrator	Administrator	Администратор	–	109.252.48.224	Веб-интерфейс	Локальная группа	30 окт. 2025 г., 11:12	30 окт. 2025 г., 14:00	2 часа 48 минут
administrator	Administrator	Администратор	–	109.252.48.224	Веб-интерфейс	Локальная группа	23 окт. 2025 г., 7:19	23 окт. 2025 г., 17:38	10 часов 19 минут
administrator	Administrator	Администратор	–	109.252.48.224	Веб-интерфейс	Локальная группа	16 окт. 2025 г., 6:18	16 окт. 2025 г., 15:34	9 часов 16 минут

Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

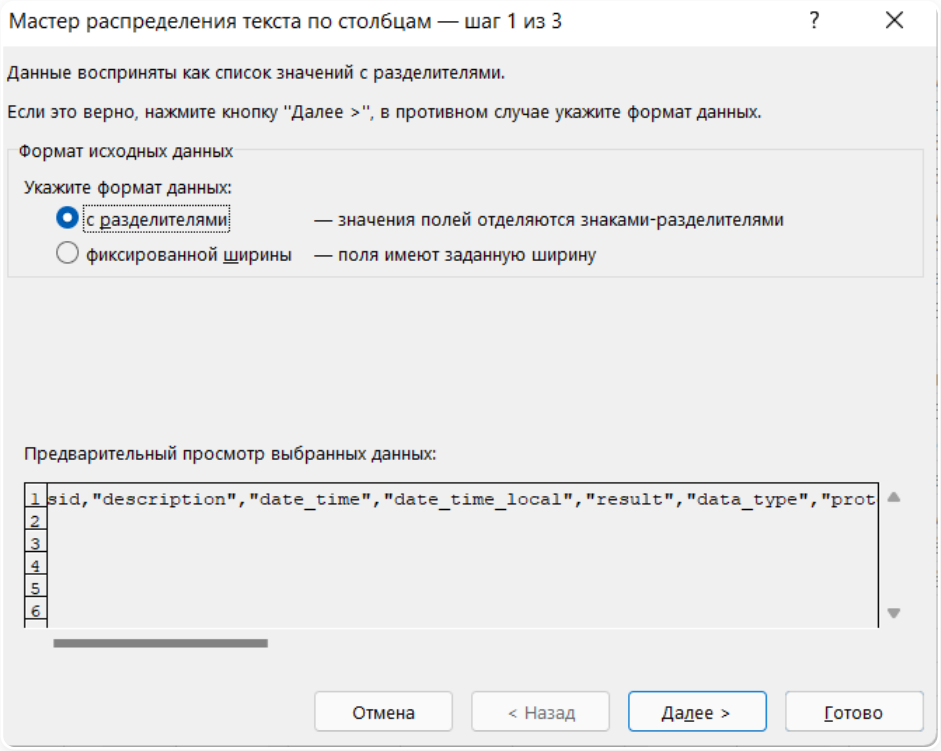
Для корректного отображения информации из CSV-файла

1. Скачайте CSV-файл с логами за определенный период по соответствующей кнопке.

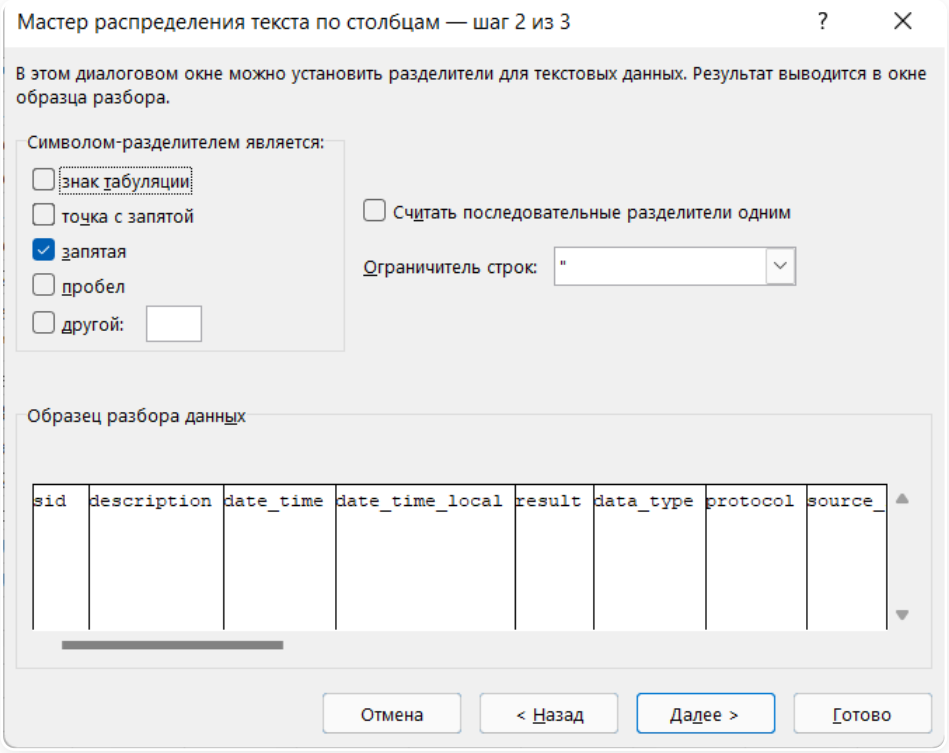
2. Откройте CSV-файл в MS Excel и выделите весь первый столбец.

3. Перейдите на вкладку **Данные** и нажмите **Текст по столбцам**.

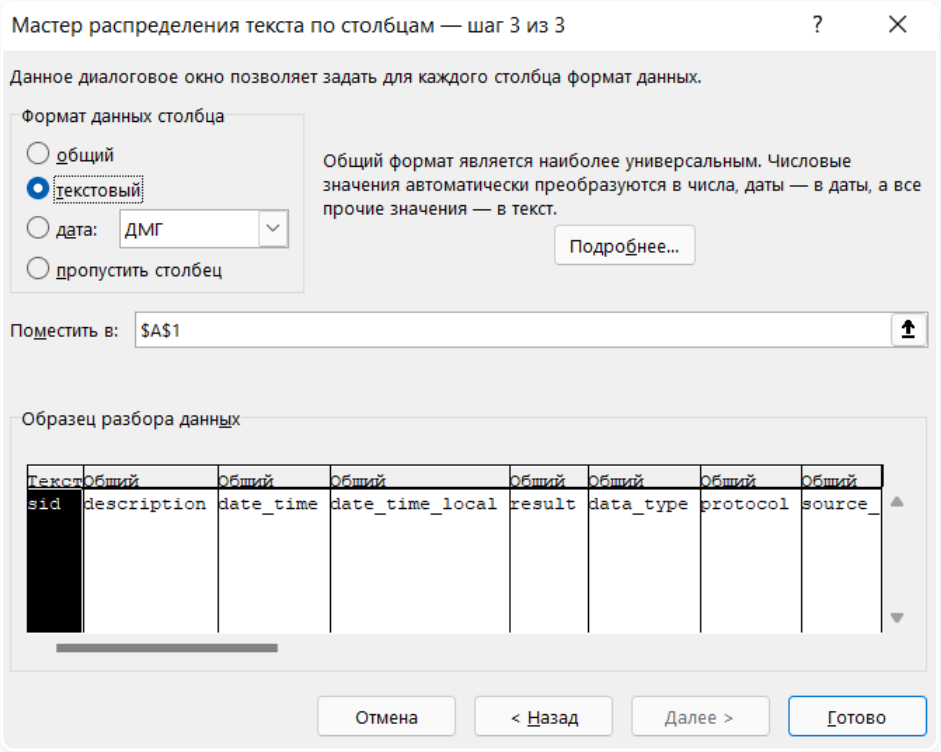
4. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:



5. В блоке **Символом-разделителем является:** выберите **запятая** и нажмите **Далее**:



6. В блоке **Формат данных столбца** выберите **Текстовый** и нажмите **Готово**:



Управление сервером

Администраторы

С версии 23 управление учетными записями администраторов и их доступами будет переведено на централизованную модель. Подробнее об изменениях и переносе настроек – в статье Подготовка к миграции администраторов из VCE в версии 23.

В Ideco Center можно создать локальных администраторов или интегрировать администраторов из сервисов Active Directory, RADIUS. Добавление администраторов в Ideco Center аналогично механизму в Ideco NGFW Novum.

Локальным администраторам могут быть назначены роли:

- **Администратор** - имеет доступ ко всем функциям Ideco Center.
- **Только просмотр** - не имеет возможности управлять правилами в Ideco Center (создавать, менять приоритет и др.).
- **Администратор ИБ** - имеет доступ к событиям безопасности.
- **Администратор межсетевого экрана** - может создавать учетные записи, настраивать правила фильтрации и управлять режимами работы **Межсетевого экрана**.
- **Администратор настройки доступов** - имеет доступ к настройкам сетевого взаимодействия пользователей **Межсетевого экрана**, субъектов доступа, информационных систем.

Удалять подключенные Ideco NGFW Novum из Ideco Center могут только администраторы с ролью **Администратор**.

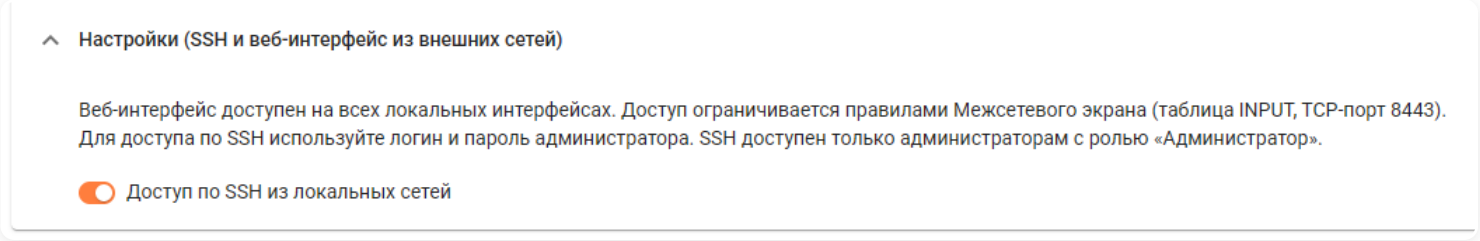
Авторизоваться в Ideco NGFW Novum с логином и паролем администратора Ideco Center **невозможно**.

Доступ к веб-интерфейсу из внешней сети и удаленный доступ по SSH

Для подключения по SSH из локальных сетей выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы**.

2. Активируйте настройку **Доступ по SSH из локальных сетей**.



3. Подключитесь к серверу с помощью любого SSH-клиента (для Windows, например, PuTTY), используя 22 порт. Необходимо указать логин и пароль **Администратора Ideco Center**.

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 ~]#
```

Попытки подбора паролей будут автоматически блокироваться.

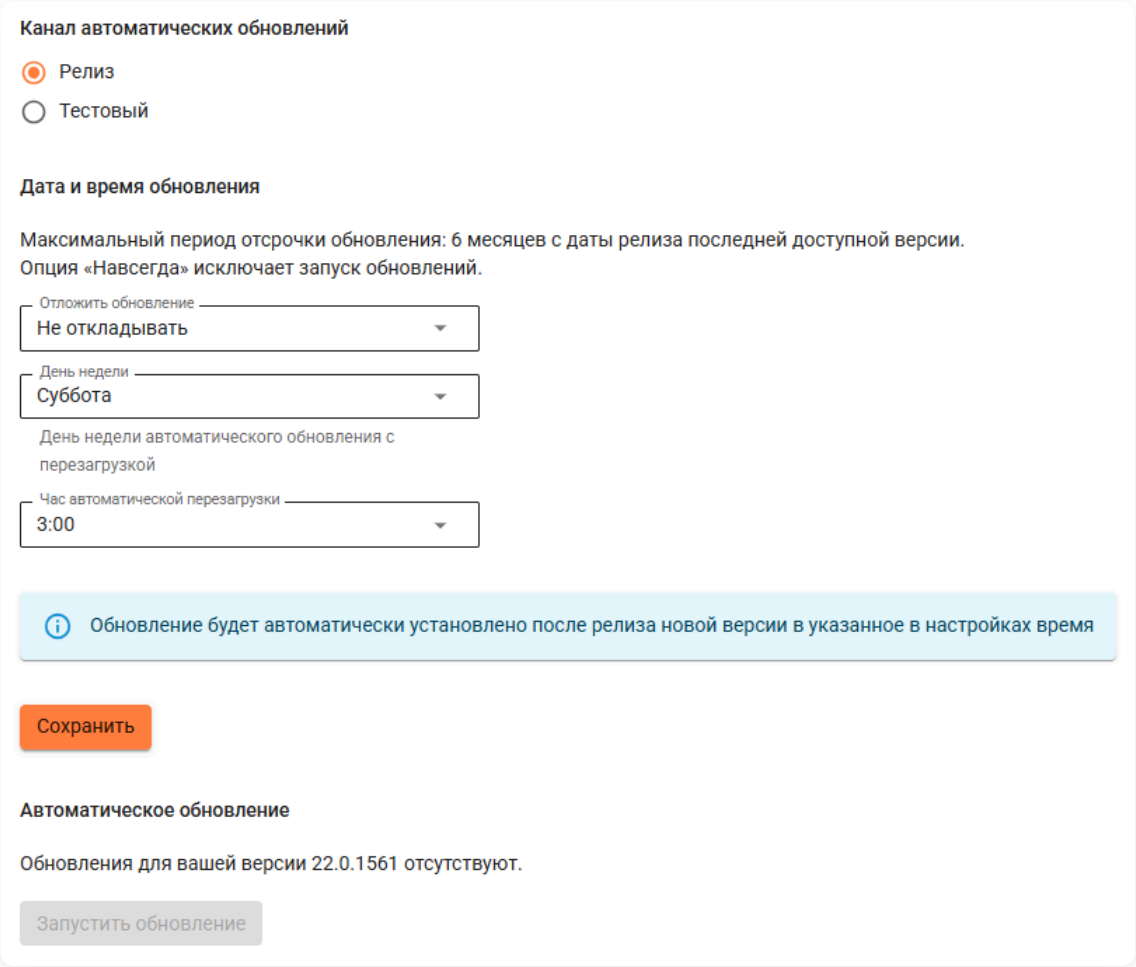
Обновления

Обновить систему Ideco Center можно как в офлайн-режиме, так и по сети. Настроить режим обновления можно в **Управление сервером** → **Обновления**.

> Для отключения автоматического обновления Ideco Center в строке **Отложить обновление** выберите **Навсегда**.

Автоматическое обновление

В режиме **Автоматического обновления** доступны следующие настройки:

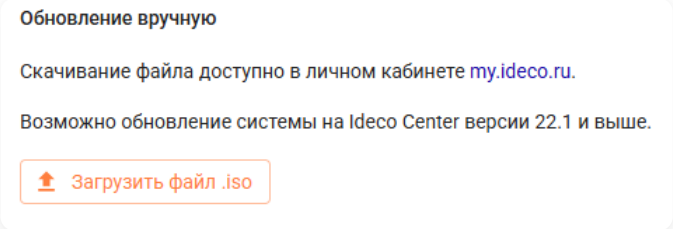


Расшифровка полей

- **Канал автоматических обновлений** - выберите **Релиз** или **Тестовый**. Канал **Релиз** позволяет обновляться на стабильно работающие версии. Канал **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** - позволяет выбрать час запуска автоматического обновления.
- **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

Ручное обновление

В режиме **Ручной загрузки** обновлений необходимо скачать ISO-образ новой версии Ideco Center в MY.IDECO и загрузить его с внешнего носителя:

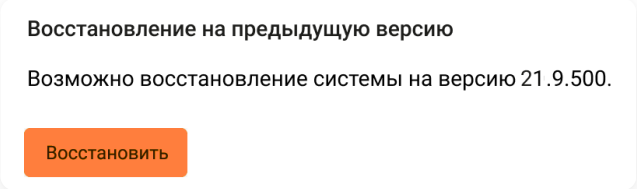


Кнопка принудительного обновления активна только после скачивания обновления и позволяет его применить. Скачивание нельзя инициировать. После применения обновления потребуется полная перезагрузка сервера.

После обновления новая версия будет отображаться в верхнем левом углу веб-интерфейса Ideco Center.

Восстановление на предыдущую версию

Кнопка **Восстановить** позволяет вернуться к предыдущей версии Ideco Center:



Система будет перезагружена, при этом текущие настройки будут потеряны. После восстановления отложите автоматическое обновление.

При восстановлении на предыдущую версию данные перенесены не будут. Ideco Center вернется в состояние, в котором был на момент обновления. Все изменения, внесенные после обновления, будут утеряны. Сохраните информацию на внешнем носителе. Ideco Center 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 Ideco Center не ниже той, на которой был создан.

Процесс выхода релизов в каналы обновлений

Тестовый канал обновлений позволяет быстрее обновляться до новых версий (релизных или бета-версий во время их активного тестирования). После выхода бета-версии Ideco Center в **Тестовый** канал ожидается обратная связь от пользователей по использованию новой версии продукта через Telegram. Обратная связь позволяет выявить недочеты и уязвимости в продукте. После их исправления происходит выкладка в канал **Релиз**.

Если в версии Ideco Center, вышедшей в канал **Релиз**, в ходе использования выявляются недочеты, то они исправляются ближайшими обновлениями версии. Обновление в канале **Релиз** появляется постепенно.

Особенности обновления Ideco Center

- 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 Ideco Center - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7).
- Автоматическое обновление Ideco Center до следующей мажорной версии возможно только после установки последней минорной версии, выпущенной в релиз. Например, можно обновить Center 17.2 до версии 17.9, а затем до версии 18.6.
- Ручное обновление Ideco Center до следующей мажорной версии можно выполнить с любой версии. Например, можно обновить Center 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 теперь отсчитываются с даты выхода последнего доступного минорного релиза.

Лицензия

В разделе **Ideco Center** MY.IDECO находится информация о зарегистрированных серверах и имеющихся лицензиях.

Доступные виды лицензий:

- **Enterprise** - коммерческая лицензия.
- **Enterprise-demo** - бесплатная лицензия сроком на 44 дня. Формируется автоматически при регистрации сервера в MY.IDECO.

Доступные действия для управления лицензиями:

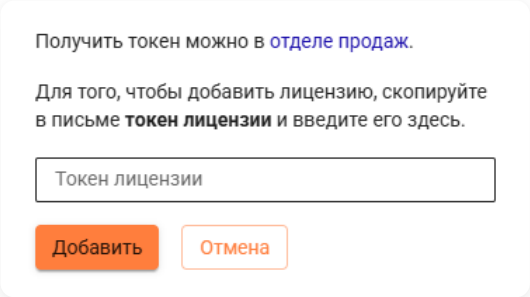
- Регистрация сервера.
- Добавление коммерческой или бесплатной лицензии.
- Привязка лицензии к серверу.
- Просмотр информации об имеющихся лицензиях.
- Офлайн-обновление лицензии и баз модулей фильтрации.

Добавление коммерческой (Enterprise) лицензии

1. Скопируйте токен лицензии из письма, отправленного после покупки лицензии. Формат токена: `owhYLGvT6Xmt819JyinSxREkJfvjVO63`.

2. В MY.IDECO перейдите в **Ideco Center** → **Лицензирование** и нажмите **Добавить лицензию**.

3. Введите токен в поле **Токен лицензии** и нажмите **Добавить**:

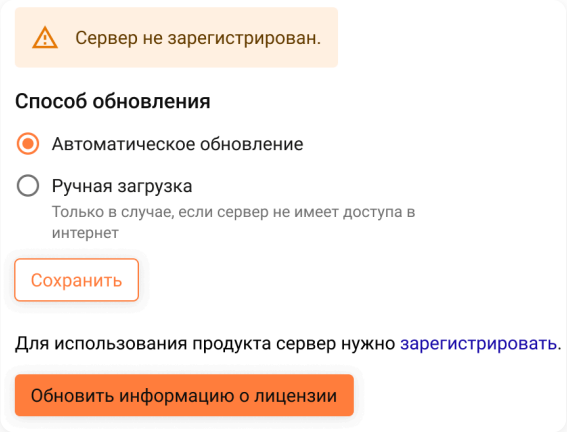


Токен станет недействительным, а в таблице **Непривязанные лицензии** отобразится купленная лицензия.

Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн:

- Для онлайн-привязки лицензии в разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco Center выберите опцию **Автоматическое обновление**. Онлайн-привязка проводится только в MY.IDECO.
- Для офлайн-привязки выберите опцию **Ручная загрузка**. Офлайн-привязка потребует доступ к веб-интерфейсу сервера:



Назначьте имеющиеся коммерческие лицензии на любой зарегистрированный сервер Ideco Center с учетом следующих ограничений:

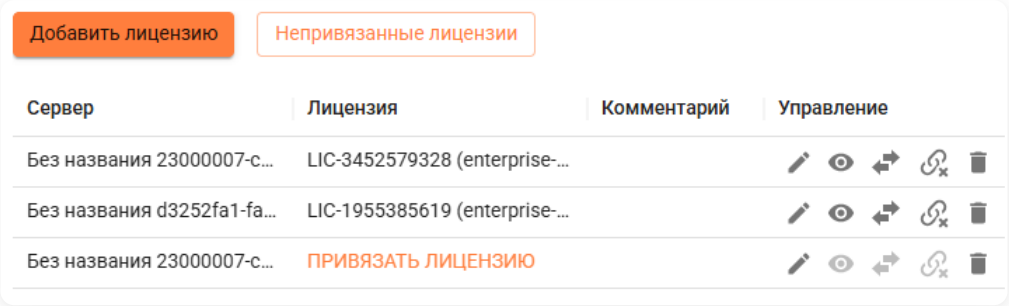
- Одна лицензия может быть привязана только к одному серверу.
- Демо-лицензию нельзя привязать к другому серверу.
- Демо-лицензию нельзя отвязать от сервера. Доступна только замена на другую лицензию.
- Демо-лицензия выдается только один раз для каждого экземпляра сервера.
- При удалении сервера с демо-лицензией также удаляется и лицензия.

После активации лицензия привязывается к оборудованию, на котором установлено программное обеспечение Ideco Center. При замене оборудования или частей оборудования лицензия отвязывается и требует повторной привязки. Демо-лицензия при этом теряется.

Онлайн-привязка лицензии

Перейдите в MY.IDECO и выберите удобный вариант привязки:

- В **Ideco Center** → **Лицензирование** нажмите **Привязать лицензию**:



В открывшемся окне выберите нужную лицензию и сохраните изменения.

- В **Ideco Center** → **Лицензирование** перейдите в **Непривязанные лицензии** и нажмите . Укажите нужный сервер и сохраните изменения, нажав **Привязать**:

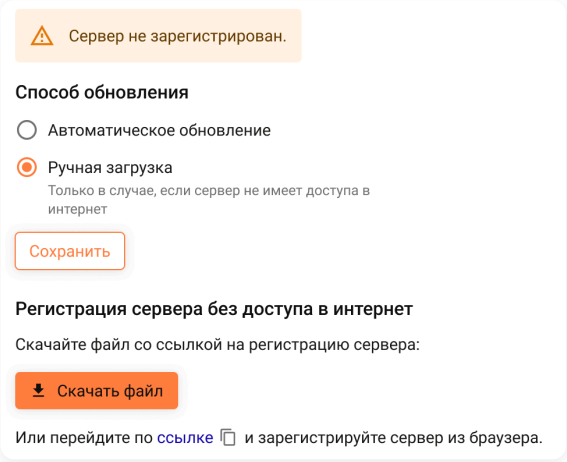
Офлайн-привязка лицензии

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

1. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco Center.

2. Выберите опцию **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

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

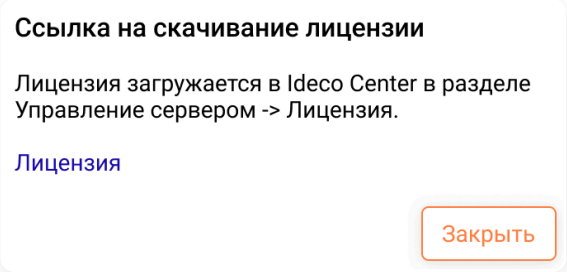


4. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

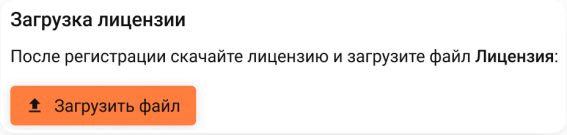
5. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

6. Перейдите в **Ideco Center** → **Лицензирование** в MY.IDECO. Нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `IC (IC Unknown)`.

7. Откройте ссылку из пункта 2, чтобы скачать файл лицензии:



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



Просмотр информации о лицензиях

Посмотреть информацию о лицензии можно:

- В разделе **Ideco Center** MY.IDECO, нажав напротив нужного сервера.
- В разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco Center.

Бэкапы

Бэкап - это предварительно созданная резервная копия данных, позволяющая восстановить большинство настроек и сохраненной информации.

В Ideco Center создается только полный бэкап, который включает в себя все настройки, созданные администратором в веб-интерфейсе.

Бэкапы не включают:

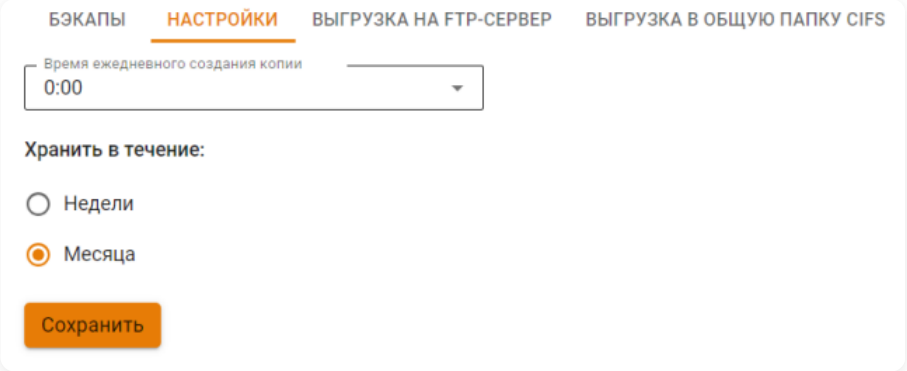
- Системный журнал.
- Любые кешируемые данные, базы антивирусов, правила IPS и т. п.
- Любые данные, автоматически генерируемые в процессе работы системы.

В Ideco Center 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.
>
> Для развертывания нового сервера рекомендуем:
>
> 1. Установить чистую версию Ideco NGFW Novum.
>
> 2. Подключить сервер к Ideco Center.
>
> Заданная конфигурация для сервера в Ideco Center (правила трафика, профили, объекты и т.д.) будет автоматически применена к новому серверу.

Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в **Управление сервером** → **Бэкапы** → **Настройки**:



Расшифровка полей

- **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.

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.

> 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. Ideco Center 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 Center. Команда создает автоматический бэкап в соответствии с заданными настройками сохранения.

Бэкапы на сетевое файловое хранилище

Ключевые параметры, необходимые для настройки бэкапа на **NetBIOS (CIFS)**:

- **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.

Бэкапы на удаленное файловое хранилище

Ключевые параметры, необходимые для настройки бэкапа на **FTP-сервер**:

- **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.

> Укажите путь к каталогу в UNIX-формате. К примеру, в ОС Windows каталог открывается по пути `\\192.168.1.1\dir_1\dir_2\backup`, значит, в поле **Путь к каталогу** пропишите `dir_1/dir_2/backup`.

Ручное создание бэкапа

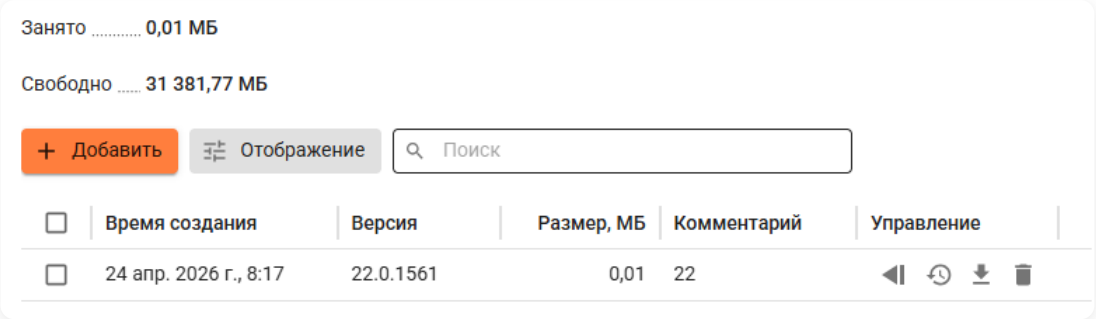
Через веб-интерфейс

Для создания бэкапа через интерфейс Ideco Center перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и выполните действия:

1. Нажмите **Добавить** → **Создать** или нажмите **Создать бэкап** в правом верхнем углу веб-интерфейса.

2. Введите комментарий и нажмите **Добавить**.

Новый бэкап появится в таблице:



Через локальное меню

Чтобы создать новый бэкап через локальное меню Ideco Center, выполните действия:

1. Выберите пункт **Создать новый бэкап** и нажмите **Enter**.

2. Введите комментарий для бэкапа и нажмите **Enter**.

Пример создания бэкапа через локальное меню приведен на скриншоте ниже:

```
Управление сервером

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

Введите номер пункта и нажмите Enter.
# 12

Введите комментарий для бэкапа или оставьте поле пустым. Затем нажмите Enter.

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

Настройка сохранения бэкапа в сетевом файловом хранилище возможна только через веб-интерфейс Ideco Center. Выгрузка на внешние сетевые хранилища производится только при автоматическом создании бэкапа.

Восстановление конфигурации из бэкапа

В Ideco Center возможно полное и мгновенное восстановление из бэкапа.

При выполнении полного восстановления система будет перезагружена для применения настроек сервера.

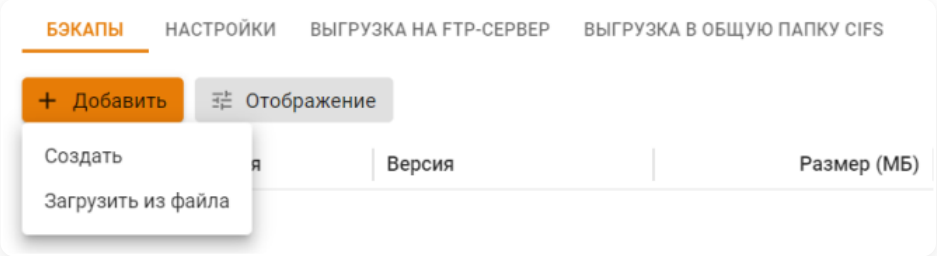
При выполнении мгновенного восстановления бэкап применится без перезагрузки. При этом не сохраняется статистика в отчетах.

> Полное восстановление возможно либо на текущую версию, либо на предыдущую мажорную версию. Например, на версии 17 возможно полное восстановление бэкапа версии 16 или версии 17.
>
> Мгновенное восстановление возможно только для бэкапа версии, полностью совпадающей с установленной 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 в **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

- **Восстановить из бэкапа** - восстановятся все настройки и перезагрузится сервер.
- **Мгновенно восстановить из бэкапа** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

  Нажмите **Enter**.

2. Выберите из списка бэкап, введя пункт нужной копии, и нажмите **Enter**.

3. Перезагрузите сервер при запуске полного восстановления, введя **y**, а затем **Enter**. При мгновенном восстановлении перезагрузка не нужна.

Пример восстановления из бэкапа через локальное меню:

```
Введите номер пункта и нажмите Enter.
# 14

Выберите бэкап для восстановления:

1.
Время:        24.04.2026 09:22:45
Версия:       Ideco CC 22.0.1561
Комментарий:

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1

Выбран бэкап

Время:        24.04.2026 09:22:45
Версия:       Ideco CC 22.0.1561
Комментарий:

Для восстановления из бэкапа необходима перезагрузка.
Перезагрузить сервер и восстановить настройки сейчас?

Пожалуйста подтвердите ваш выбор.

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

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 Center 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`).
- **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`.

Таблица служб

Раздел	Имя службы
Серверы	ideco-servers-backend, ideco-servers-websocket
Межсетевой экран	ideco-firewall-backend, ideco-firewall-rest
Контент-фильтр	ideco-content-filter-backend
Предотвращение вторжений	ideco-suricata-backend
Объекты	ideco-alias-backend
Сетевые интерфейсы	ideco-network-backend, ideco-network-nic
Маршрутизация	ideco-routing-backend, ideco-routing-rest
Обратный прокси	ideco-reverse-backend
Защита и управление DNS	ideco-dns-backend, unbound, nsd, unbound-anchor, unbound-keygen
DHCP-сервер	ideco-dhclient
NTP-сервер	chronyd
Кластеризация	ideco-cluster-backend
Обновления	ideco-sysupdate-backend
Бэкапы	ideco-backup-backend, ideco-backup-create
Лицензия	ideco-license-backend
Syslog	ideco-logs-backend, ideco-monitor-backend
Отчеты и журналы	ideco-logs-backend, ideco-logs-syncer
Действия администраторов	ideco-audit-backend
Авторизация администраторов	ideco-web-backend
Сертификаты	ideco-cert-backend
Локальное меню	ideco-local-menu
Дополнительно	ideco-system-backend
Сбор анонимной статистики о работе сервера	ideco-gatherstat-backend
Защита от несанкционированного доступа, в т.ч. от брутфорс-атак (brute force - атака полным перебором)	fail2ban
REST API NGFW	ideco-rest-api-backend
Доступ по SSH	sshd

Характеристики сервера

Раздел показывает спецификацию сервера, где развернут Ideco Center:

Гипервизор	Linux KVM kernel virtual machine
Доступно оперативной памяти	7.5 ГБ
Модель процессора	Intel Xeon Processor (Icelake)
Потоков	2
Потоков на ядро	2
Ядер на сокет	1
Сокеты	1
NUMA ноды	1
Версия BIOS	1.16.3-1
Дата выпуска BIOS	04/01/2014
Материнская плата	xeon-gold-6338

Скопировать

Управление питанием

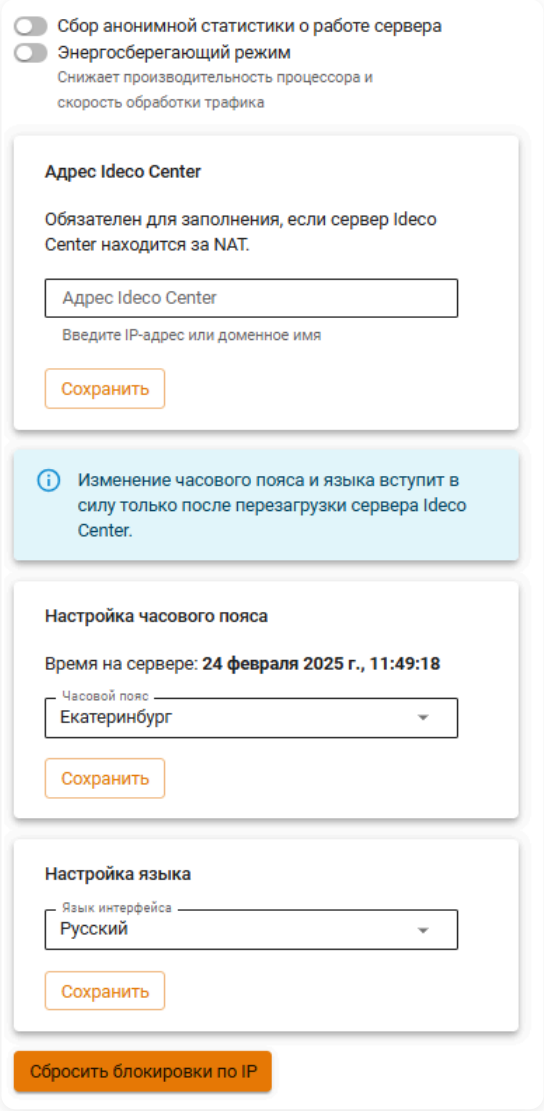
Позволяет перезагрузить или выключить Ideco Center через веб-интерфейс:

Перезагрузка

Выключение

Дополнительно

Настройка осуществляется через веб-интерфейс в **Управление сервером** → **Дополнительно**:



Расшифровка полей

- **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.
- **Адрес Ideco Center** - заполняется, если сервер Ideco Center находится за NAT. После нажатия **Сохранить** будет выпущен сертификат на IP-адрес или доменное имя сервера Ideco Center.
- **Настройка часового пояса** - изменения вступают в силу только после перезагрузки Ideco Center.
- **Настройки языка** - изменения вступают в силу только после перезагрузки Ideco Center.
- **Сбросить блокировки (fail2ban)** - используйте для сброса всех заблокированных IP-адресов. Если требуется разблокировать какой-то конкретный IP-адрес, воспользуйтесь командой `fail2ban-client unban <IP-адрес>` в терминале.

Кластеризация

В отличие от Ideco NGFW Novum, Ideco Center поддерживает георасределенное размещение узлов кластера.

Отказоустойчивый кластер – два Ideco Center, объединенные в режиме active-passive. Кластер позволяет:

- Сохранять управление NGFW при выходе из строя основного сервера.
- Размещать узлы кластера в территориально распределенной инфраструктуре.
- Переключать активный сервер вручную для планового обслуживания.

Каждое из устройств Ideco Center, объединенное в кластер, называется нодой и имеет одну из двух ролей:

- **Первичная нода** – активный сервер управления. Принимает подключения от NGFW, отправляет им конфигурацию. Единственное место, где можно изменять правила, объекты и политики.
- **Вторичная нода** – резервный сервер. Получает синхронизированную копию данных от первичной ноды, но не принимает подключения от NGFW. Все синхронизируемые данные на ней доступны только для чтения.

Роли назначаются при создании кластера. Подробнее о смене ролей – в статье.

Синхронизация данных

Между нодами синхронизируются данные, передаваемые на NGFW:

- Правила трафика
- Профили безопасности
- Объекты
- Группы серверов
- Список подключенных устройств
- Название кластера
- Пользовательские категории контент-фильтра

Не синхронизируются:

- Настройки ноды (интерфейсы, маршруты, сертификаты)
- Параметры кластеризации
- Журналы NGFW
- Настройки SNMP
- Настройки Syslog
- Настройки Zabbix
- Базы сигнатур (обновляются на каждой ноде независимо)

Подключение NGFW к кластеру

NGFW не обращаются к нодам по IP-адресу напрямую. Для обнаружения нод кластера используются SRV-записи, в которых указан список нод. Без SRV-записи NGFW Novum не будет знать о существовании другой ноды. Поэтому для подключения NGFW к кластеру:

1. В DNS-зоне создайте SRV-запись:

```
$ORIGIN cluster.example.com
_ideco_center._tcp 3600 IN SRV 1 0 0 cc1
_ideco_center._tcp 3600 IN SRV 2 0 0 cc2
```

- `cluster.example.com` – имя DNS-зоны, в которой размещаются SRV-записи кластера;
- `_ideco_center._tcp` – фиксированное имя сервиса;
- `3600` – TTL записи в секундах;
- `IN SRV` – тип записи;
- `1` / `2` – приоритет ноды, не используется при подключении;
- `0` – вес. Не используется, всегда указывайте `0`;

- `0` – порт. Не используется, всегда указывайте `0`;
- `cc1` / `cc2` – доменные имена нод кластера (соответствуют значениям из поля **Доменное имя** в настройках каждой ноды).

Если нода отклоняет соединение, NGFW автоматически переходит к следующей записи. Вес и приоритет записей игнорируется, ноды перебираются в лексикографическом порядке (по FQDN).

2. В интерфейсе NGFW в **Управление сервером** → **Ideco Center** в поле **Адрес сервера** укажите доменное имя кластера Ideco Center. Этот домен при добавлении префикса `_ideco_center._tcp` должен соответствовать имени, для которого созданы SRV-записи.

Проверить настройки DNS для подключения NGFW к кластеру

Чтобы убедиться, что DNS настроен правильно, из терминала NGFW проверьте:

1. Корректный резолв A-записей нод кластера:

```
nslookup cc1.cluster.example.com
nslookup cc2.cluster.example.com
```

- `cluster.example.com` – доменное имя кластера.
- `cc1` / `cc2` – доменные имена нод кластера (соответствуют значениям из поля **Доменное имя** в настройках каждой ноды).

2. Корректный резолв SRV-записей DNS-зоны:

```
nslookup -type=SRV _ideco_center._tcp.cluster.example.com
```

- `cluster.example.com` – доменное имя кластера (имя DNS-зоны, в которой размещаются SRV-записи кластера).

Полезные ссылки

- **Создание кластера**
- **Управление кластером**
- **Требования и ограничения для подключения NGFW к Ideco Center**
- **Сертификаты**

Создание кластера

> В статье описывается, как объединить два Ideco Center в кластер: настроить роли нод, выполнить взаимную аутентификацию и синхронизировать данные первичной ноды с вторичной.

Процедура объединения нод ограничена по времени. Если не завершить настройку на обеих нодах в течение 20 минут, запрос на объединение автоматически отменится.

Требования

Перед созданием кластера убедитесь, что соблюдены требования:

- У обеих нод задано доменное имя в разделе **Управление сервером** → **Дополнительно**. Использование IP-адресов для соединения нод не поддерживается.
- И мажорная, и минорная версии у обеих нод совпадают. Кластер с нодами разных версий не создается и не синхронизируется.
- Ноды доступны друг другу по HTTPS.
- В DNS-зоне NGFW Novum созданы SRV-записи для доменного имени кластера. Они используются NGFW Novum для обнаружения нод. Использование IP-адресов для подключения NGFW Novum к кластеру не поддерживается.
- Для корректной работы политик и объектов Active Directory при переключении ролей нод:
  - Подключение к контроллеру домена настроено отдельно на каждой ноде кластера.
  - Обе ноды подключены к одному и тому же контроллеру домена.

Сертификаты для связи между нодами

При создании кластера Ideco Center создается два подключения: от первичной ноды ко вторичной и от вторичной к первичной – каждая нода выступает клиентом в одном подключении и сервером в другом. Для взаимной аутентификации нод используется протокол mTLS. Каждая нода предъявляет свой клиентский сертификат при подключении и проверяет сертификат другой ноды. Используются два типа сертификатов:

- **Клиентские сертификаты** – для удостоверения каждой ноды. Нода-клиент предъявляет свой клиентский сертификат ноде-серверу при соединении.
- **CA-сертификаты** – определяют, каким клиентским сертификатам нода-сервер доверяет при проверке подключений.

Шаг 1. Подготовка сертификатов

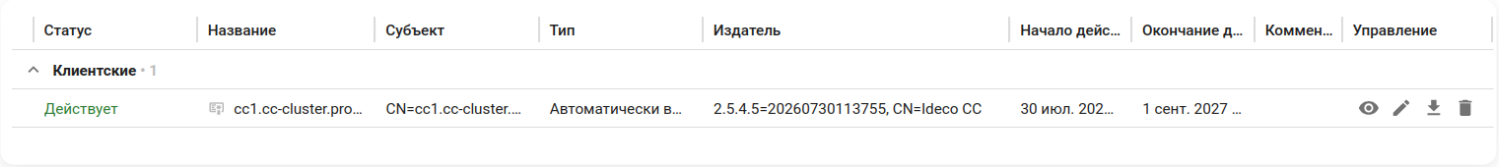
Обеспечьте наличие на обеих нодах:

- Клиентского сертификата на домен, который указан в разделе **Управление сервером** → **Дополнительно**. Сертификат будет сгенерирован автоматически и подписан корневым сертификатом Ideco Center. Также можно загрузить в **Сервисы** → **Сертификаты** клиентский сертификат, выданный вашим CA.
- CA-сертификата другой ноды. Это должен быть сертификат, которым подписан клиентский: корневой сертификат другой ноды Ideco Center или вашего CA.

Пример настройки:

1. У обеих нод в разделе **Управление сервером** → **Дополнительно** задайте доменное имя.

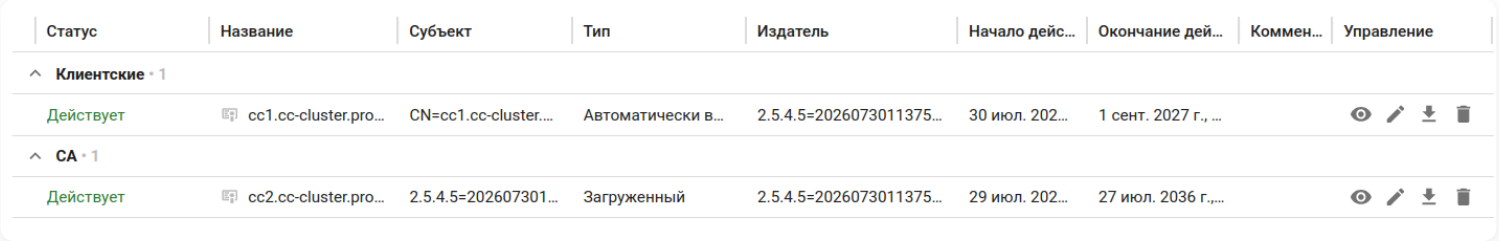
2. В разделе **Сервисы** → **Сертификаты** → **Кластеризация** текущей ноды убедитесь, что сервер выпустил клиентский сертификат на доменное имя из пункта 1. Источником подписи для сертификата будет выступать корневой сертификат Ideco Center:



Статус	Название	Субъект	Тип	Издатель	Начало дейс...	Окончание д...	Коммен...	Управление
Клиентские · 1								
Действует	cc1.cc-cluster.pro...	CN=cc1.cc-cluster....	Автоматически в...	2.5.4.5=20260730113755, CN=Ideco CC	30 июл. 202...	1 сент. 2027 ...		

3. В разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** скачайте корневой сертификат текущей ноды.

4. В веб-интерфейсе другой ноды **Сервисы** → **Сертификаты** → **Кластеризация** нажмите **Загрузить сертификат** и выберите корневой сертификат, скачанный в пункте 3:



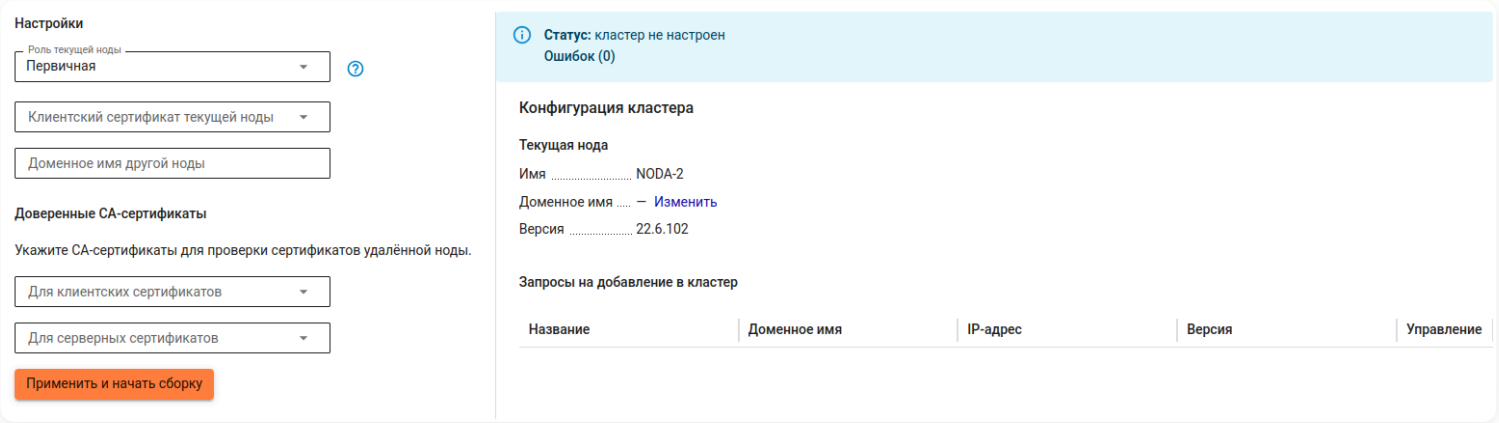
Повторите действия для другой ноды кластера.

Подробнее о работе сертификатов – в статье.

Шаг 2. Настройка и объединение нод

Определите, какой Ideco Center будет выполнять роль первичной ноды, а какой – вторичной, и на обеих нодах выполните действия:

1. Перейдите в раздел **Управление сервером** → **Кластеризация** и заполните поля:

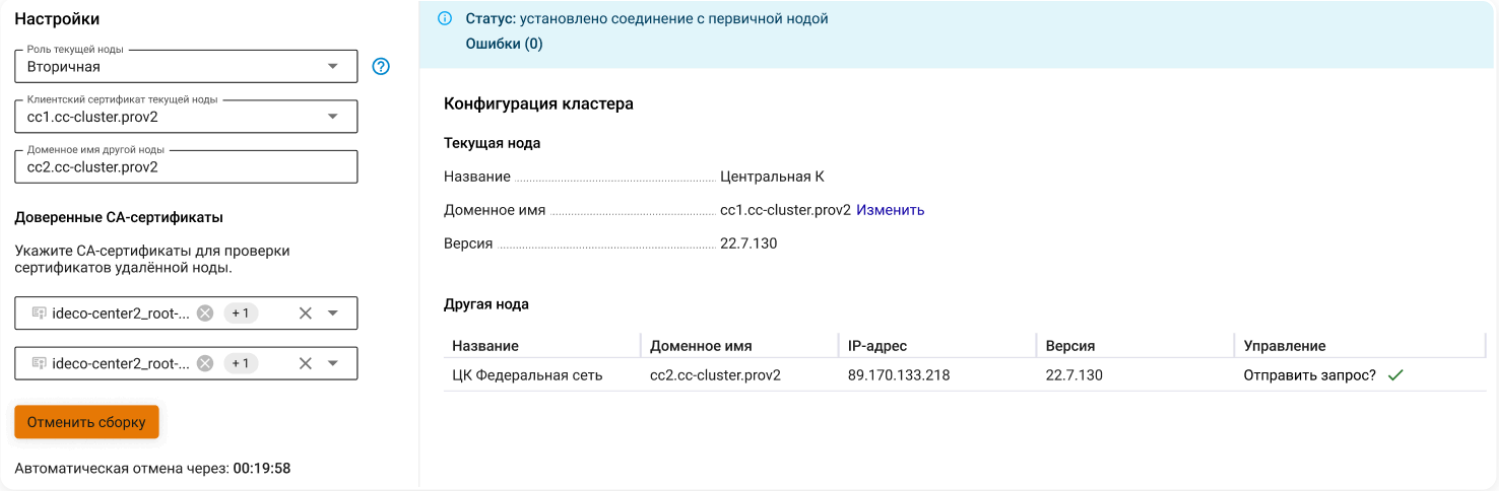


- **Роль текущей ноды** – выберите **Первичная** или **Вторичная**.
- **Клиентский сертификат текущей ноды** – выберите клиентский сертификат.
- **Доменное имя другой ноды** – введите доменное имя другой ноды.
- **Доверенные CA-сертификаты** – укажите CA-сертификаты, которым текущая нода будет доверять при проверке клиентских и серверных сертификатов другой ноды (для простейшей настройки в обоих полях выберите корневые сертификаты другой ноды, загруженные на шаге Подготовка сертификатов):
  - **Для клиентских сертификатов** – выберите CA-сертификат другой ноды.
  - **Для серверных сертификатов** – выберите CA-сертификат другой ноды.

2. Нажмите **Применить и начать сборку**.

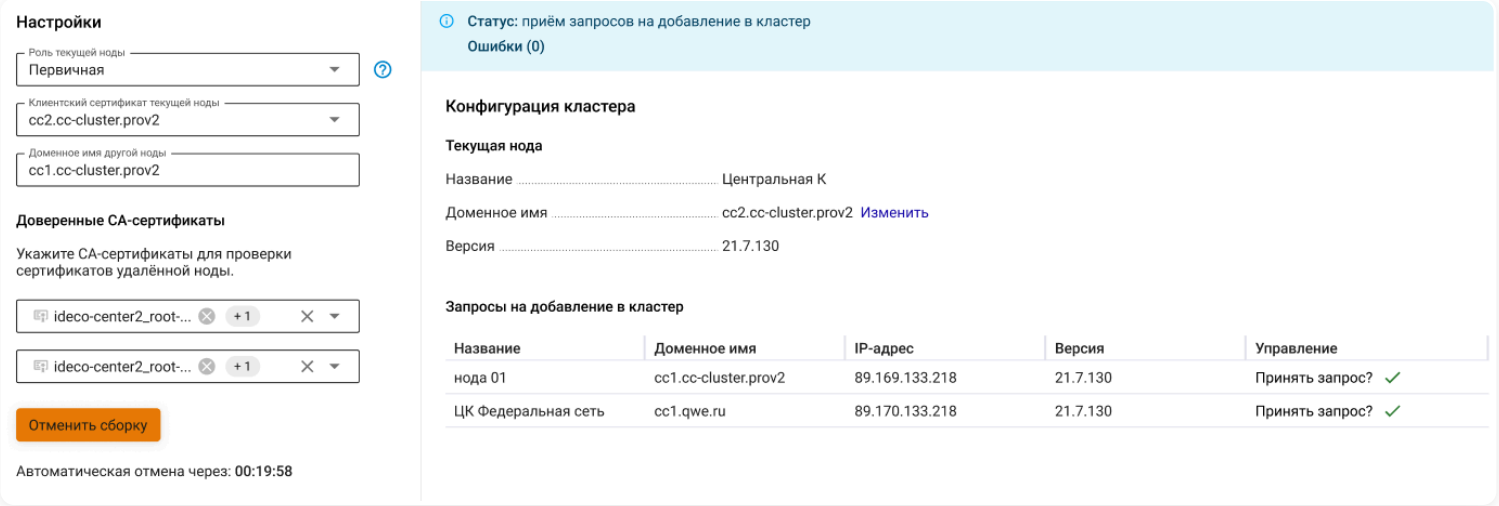
Первичная нода перейдет в режим ожидания – статус изменится на **Прием запросов на добавление в кластер**.

3. На вторичной ноде в таблице **Другая нода** появится строка с первичной нодой. Нажмите ✓, чтобы отправить запрос:



4. В открывшемся окне нажмите **Да, подтвердить**.

5. Вернитесь на первичную ноду. В таблице **Запросы на добавление в кластер** нажмите ✓, чтобы принять запрос:



6. В открывшемся окне **Подтвердить запрос на добавление в кластер** нажмите **Да, подтвердить**.

> После подтверждения все синхронизируемые данные на вторичной ноде будут удалены и заменены данными с первичной ноды. **Эта операция необратима.**

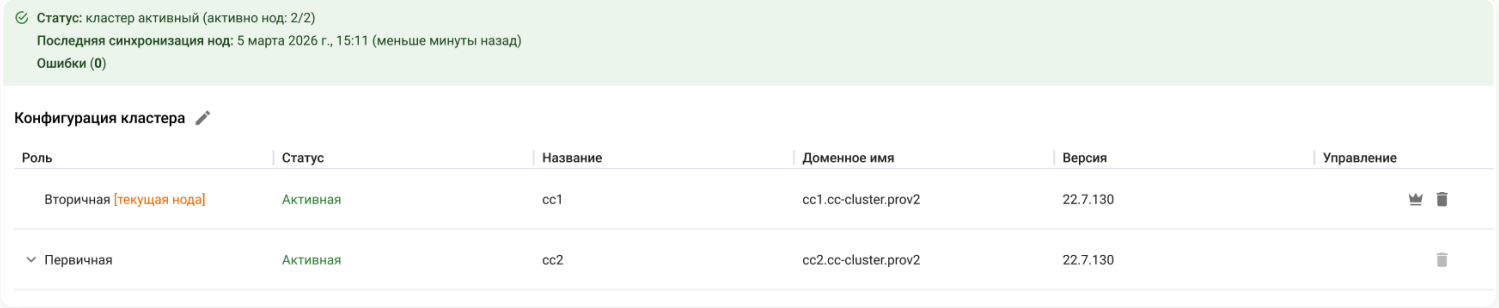
После взаимного подтверждения кластер считается созданным. Добавляемая нода получает данные с первичной и переходит в рабочий режим.

Полезные ссылки

- **Управление кластером**
- **Сертификаты**

Управление кластером

После создания кластера раздел **Управление сервером** → **Кластеризация** меняет вид. Форма настроек исчезает и отображается страница мониторинга:



Статусная строка

- **Статус** – текущее состояние кластера и число активных нод в формате N/2.
- **Последняя синхронизация нод** – время последней успешной синхронизации.
- **Ошибки** – счетчик текущих ошибок. При наличии ошибок рядом появляется ссылка **Показать** для раскрытия списка.

Статусы кластера

Статус кластера	Цвет панели	Значение
Кластер активный (активно нод: 2/2)	Зеленый	Обе ноды доступны, все соединения установлены
Кластер деградирован (активно нод: 2/2)	Оранжевый	Ноды доступны, но установлено менее двух соединений или есть ошибки
Кластер разъединен (активно нод: 1/2)	Красный	Одна нода недоступна – 0 соединений с ней
Инициализация кластера (активно нод: 0/2)	Синий	Переходное состояние: нода загружается или проходит первичную синхронизацию
Деинициализация кластера (активно нод: 0/2)	Синий	Нода выводится из кластера

Таблица Конфигурация кластера

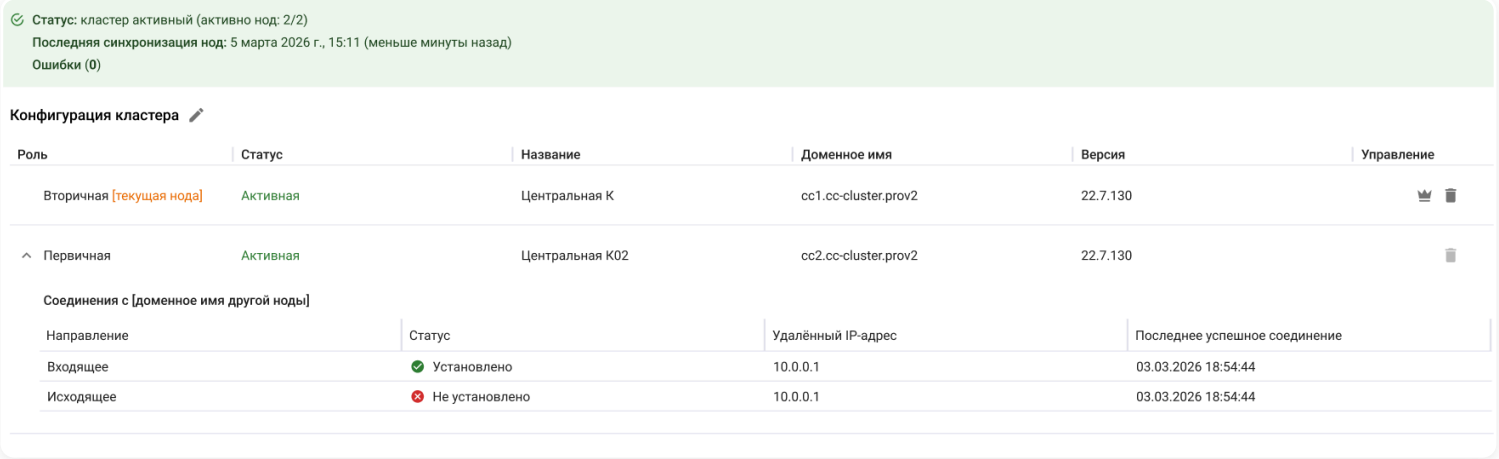
Таблица отображает информацию и состояние обеих нод кластера.

Описание столбцов

Информация о ноде:

- **Роль** – роль ноды. Текущая нода отображается первой и помечена меткой **[текущая нода]**.
- **Статус** – состояние ноды:
  - **Активная** – установлено хотя бы одно соединение.
  - **Неактивная** – соединения отсутствуют.
- **Название** – название ноды.
- **Доменное имя** – доменное имя ноды.
- **Версия** – версия ноды. При различии версий кластер не соберется, а уже собранный перейдет в состояние деградации.
- **Управление** – доступные действия для текущей ноды:
  - – назначить первичной (только на вторичной ноде).
  - – вывести из кластера.

При нажатии на ноду откроется таблица соединения этой ноды с другой нодой:



Описание столбцов

- **Направление** – направление соединения:
  - **Входящее** – другая нода подключается к текущей.
  - **Исходящее** – текущая нода инициирует подключение к другой.
- **Статус** – статус соединения:
  - **Установлено** – соединение установлено.
  - **Не установлено** – соединение не установлено.
- **Удаленный IP-адрес** – IP-адрес ноды, с которой установлено соединение.
- **Последнее успешное соединение** – дата и время последней успешной синхронизации.

Операции с кластером

Переключение ролей (захват управления)

Плановое переключение ролей может использоваться, например, для обслуживания первичной ноды.

> Прямая смена роли активной ноды недоступна – переключение выполняется захватом управления на вторичной ноде: она становится активной немедленно. Затем запускается процесс согласования со второй нодой:
>
> - Если связь между нодами есть, прежняя активная нода автоматически получает роль вторичной.
> - Если на момент захвата управления связи между нодами нет, обе ноды будут считать себя активными до восстановления связи.

Чтобы переключить роли нод, выполните действия:

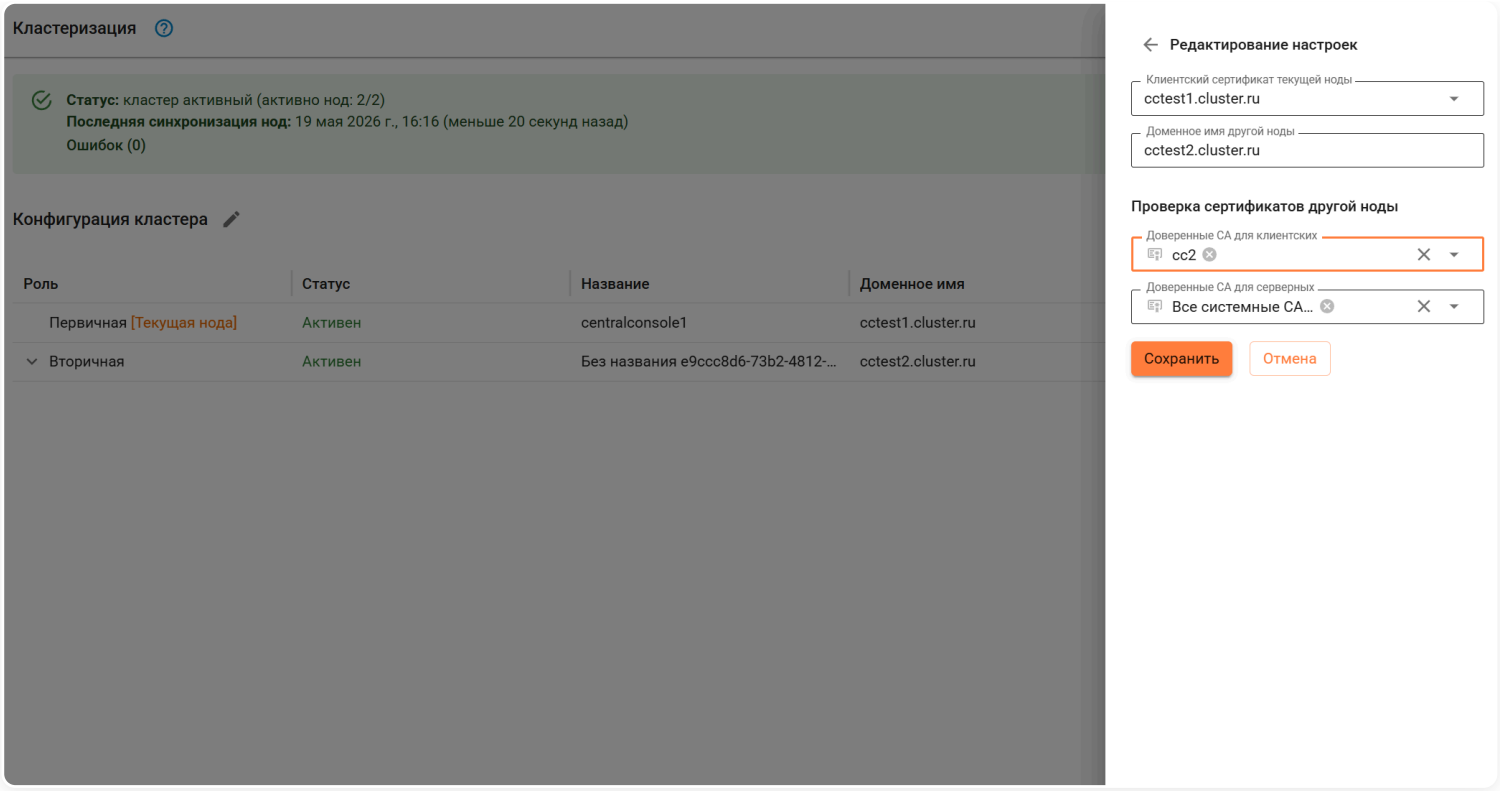
1. Убедитесь в наличии связи между нодами.

2. В столбце **Управление** напротив текущей ноды нажмите . Кнопка доступна только на вторичной ноде, если на ней уже есть синхронизированные данные.

Если на новой первичной ноде были изменения, они перезапишут данные на вторичной.

Редактирование настроек

Для редактирования настроек нажмите в заголовке таблицы:



Доступные для изменения поля:

- **Клиентский сертификат текущей ноды**
- **Доменное имя другой ноды**
- **Доверенные СА для клиентских**
- **Доверенные СА для серверных**

При необходимости внесите изменения и нажмите **Сохранить**. Соединение нод не будет разорвано.

Вывод ноды из кластера

Для вывода ноды из кластера нажмите 🗑 в столбце **Управление** в строке текущей ноды. Нода выйдет из кластера и продолжит работу как самостоятельный сервер управления.

Вывод из кластера – односторонняя операция. Вторая нода не получает уведомления и продолжает попытки подключения. Для полного разрушения кластера необходимо выполнить вывод на обеих нодах.

При выводе из кластера первичная нода сохраняет данные и подключенные устройства. Вторичная нода теряет синхронизированные данные.

Поведение кластера при сбоях

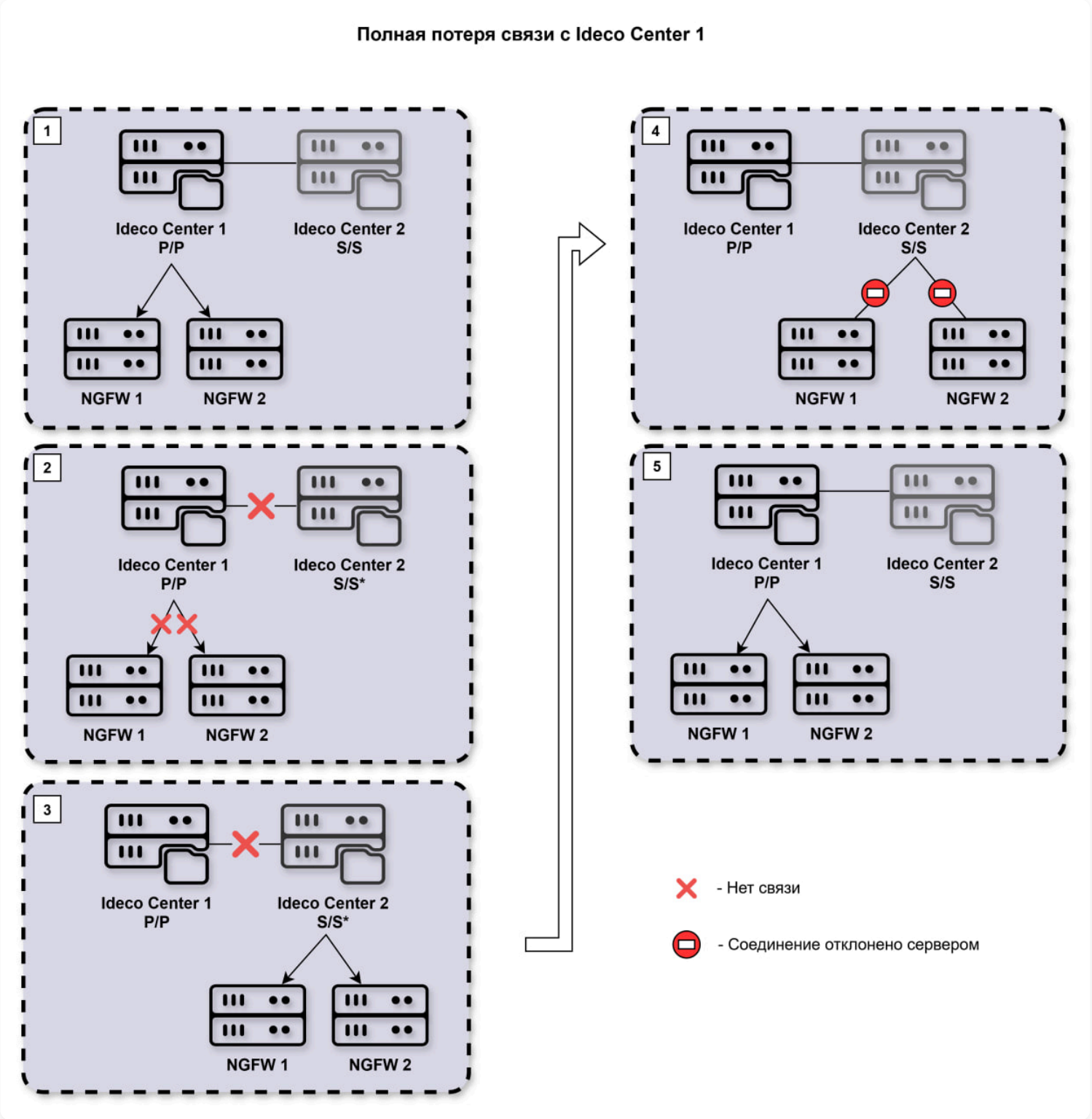
На диаграммах сценариев используются следующие обозначения:

Обозначение	Расшифровка	Поведение ноды
P/P	Первичная	Нода назначена первичной и работает в штатном режиме, принимая подключения от NGFW
S/S	Вторичная	Нода работает в штатном режиме. Нода синхронизируется с первичной, получает данные, но не принимает подключения от NGFW
S/S*	Вторичная-заместитель	Роль ноды – вторичная, но она потеряла связь с первичной и перешла в режим заместителя, начав принимать подключения от NGFW и выполнять функции первичной

Потеря связи с первичной нодой

Сценарий, при котором первичная нода становится недоступна, а вторичная нода берет на себя прием подключений от NGFW.

Возможные причины: выход из строя сервера первичной ноды, незапланированная перезагрузка, отключение электропитания, полная потеря сетевого подключения на стороне первичной ноды.



Последовательность:

1. Кластер работает штатно, NGFW подключены к Ideco Center 1 (первичная нода).

2. Ideco Center 1 (первичная нода) становится недоступен.

3. Соединение между Ideco Center 1 (первичная нода) и NGFW разрывается.

4. Ideco Center 2 (вторичная нода) после нескольких неудачных попыток восстановить соединение с Ideco Center 1 (первичная нода) переходит к роли вторичная-заместитель.

5. NGFW перебирают SRV-записи и подключаются к Ideco Center 2 (вторичная-заместитель).

6. Когда Ideco Center 1 (первичная нода) восстанавливается, Ideco Center 2 (вторичная-заместитель) обнаруживает появление первичной ноды и автоматически возвращается в режим вторичной ноды.

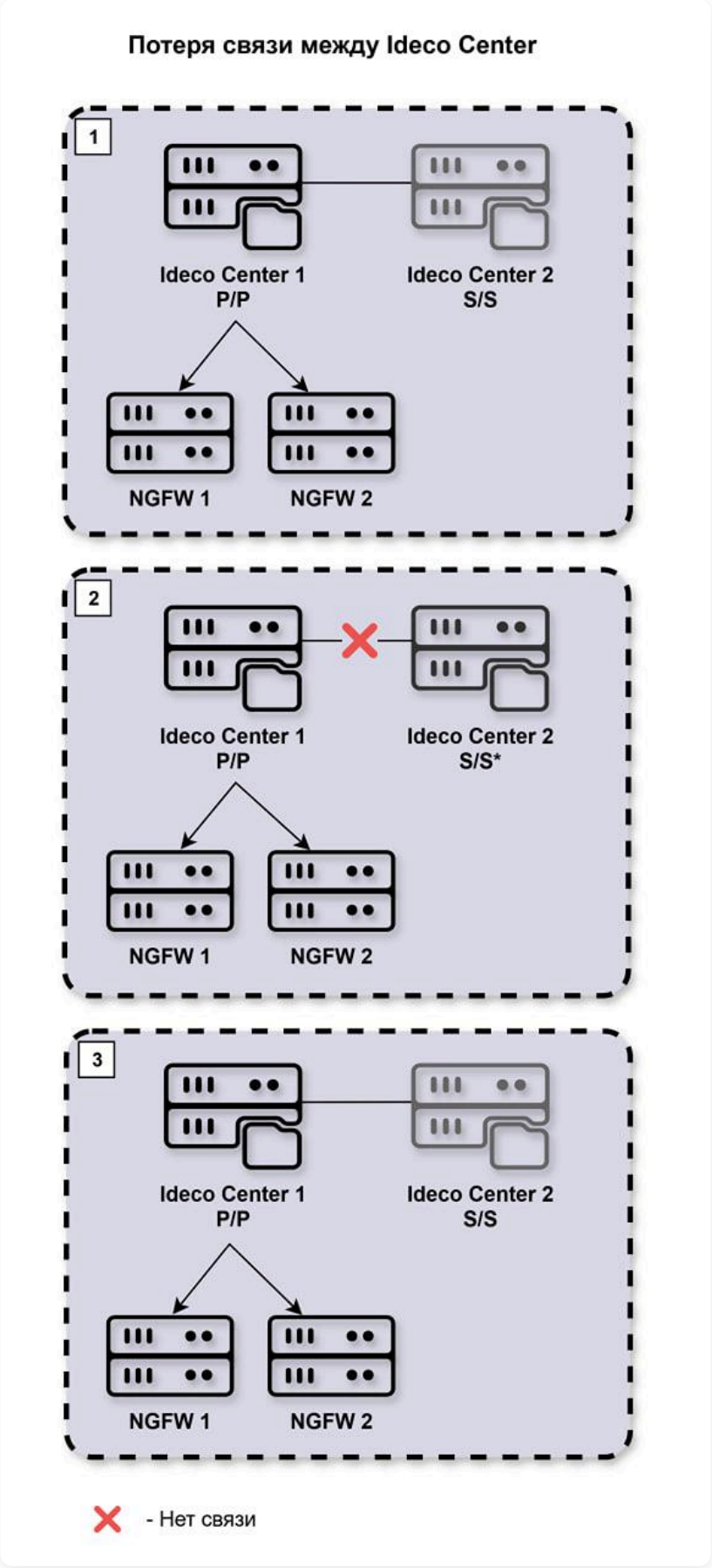
7. Все NGFW переподключаются к Ideco Center 1 (первичная нода).

На ноде с ролью вторичная-заместитель нельзя изменять конфигурацию. Если необходимо внести правки, воспользуйтесь захватом управления.

Потеря связи между нодами Ideco Center

Сценарий, при котором связь между нодами прерывается, но устройства NGFW по-прежнему видят первичную ноду.

Возможные причины: сбой на промежуточном сетевом оборудовании между нодами, проблемы с VPN-туннелем или WAN-каналом при территориально распределенном размещении, блокировка HTTPS-трафика между нодами правилами межсетевого экрана, истечение или отзыв mTLS-сертификата.



Последовательность:

1. Кластер работает штатно, NGFW подключены к Ideco Center 1 (первичная нода).

2. Связь между нодами разрывается.

3. Ideco Center 2 (вторичная нода) переходит к роли вторичная-заместитель и готов принимать подключения NGFW.

4. NGFW все еще видят Ideco Center 1 (первичная нода) и остаются подключенными к этой ноде.

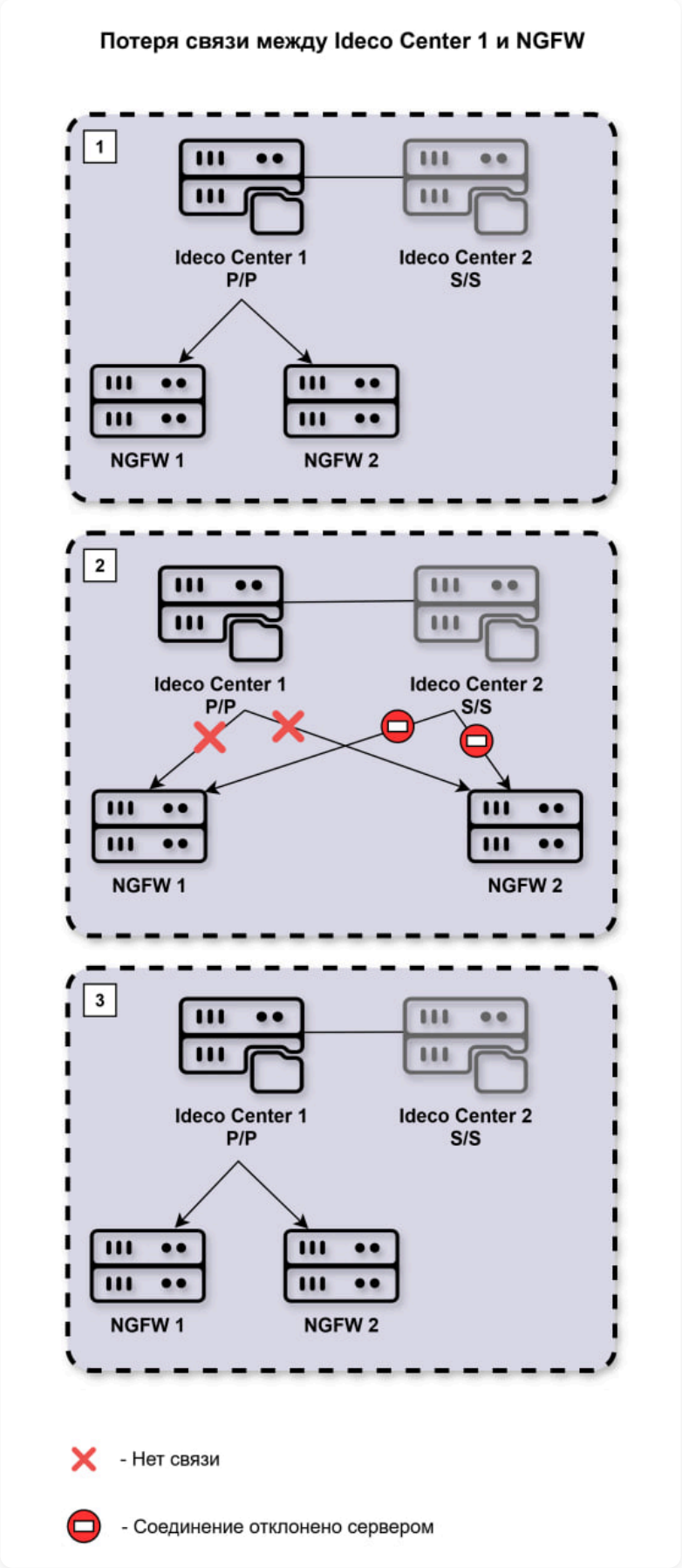
5. Когда соединение между нодами восстанавливается, Ideco Center 2 (вторичная-заместитель) возвращается к роли вторичной ноды, а кластер – в штатное состояние.

> Пока связь между нодами разорвана, синхронизация данных не выполняется. Изменения, внесенные на первичной ноде в этот период, будут переданы на вторичную при восстановлении соединения.

Потеря связи между первичной нодой и NGFW

Сценарий, при котором NGFW теряют связь с первичной нодой, но соединение между самими нодами Ideco Center сохраняется.

Возможные причины: сбой на сетевом оборудовании в сегменте между первичной нодой и NGFW, изменение маршрутов или правил фильтрации, затрагивающее трафик от NGFW к первичной ноде, проблемы с DNS-резолвингом на стороне NGFW.



Последовательность:

1. Кластер работает штатно, NGFW подключены к Ideco Center 1 (первичная нода).

2. NGFW теряют связь с Ideco Center 1 (первичная нода) и пытаются переключиться на Ideco Center 2 (вторичная нода).

3. Ideco Center 2 (вторичная нода) видит, что Ideco Center 1 (первичная нода) доступен, соединение между нодами не разорвано, поэтому не переходит к роли вторичная-заместитель и отклоняет подключения от NGFW.

4. NGFW временно не могут подключиться ни к одной ноде. Правила, примененные ранее, продолжают работать на самих устройствах.

5. При восстановлении связи NGFW переподключаются к Ideco Center 1 (первичная нода).

Это ожидаемое поведение системы. Кластер не переключается в аварийный режим, пока первичная нода доступна хотя бы по одному каналу – кластерному соединению.

Особые ситуации

Ситуация	Влияние на кластер	Как исправить
Несовпадение версий	Соединение между нодами устанавливается, но синхронизация данных не выполняется. Статус кластера изменяется на **Кластер деградирован**, в списке ошибок появляется соответствующее сообщение	Обновите обе ноды до одинаковой версии
Проблемы с сертификатами	Если сертификат истек, отозван или не проходит проверку, соединение между нодами разрывается	Замените сертификат и обновите списки доверенных CA. Соединение восстановится автоматически
Изменение доменного имени	Смена доменного имени является односторонней операцией. После смены соединение между нодами прерывается	Вручную обновите доменное имя другой ноды в настройках кластера на каждой ноде отдельно

Полезные ссылки

- **Создание кластера**
- **Сертификаты**

Требования к Ideco NGFW Novum при обновлении Center

После обновления Ideco Center до версии 23 к нему смогут подключаться только серверы NGFW Novum версии 22.1 и выше.

NGFW Novum версий ниже 22.1 после обновления Ideco Center будут отключены от него без возможности восстановления. Потребуется обновить серверы и подключить их вручную заново.

Чтобы подключенные серверы сохранились в Ideco Center, соблюдайте порядок обновления:

1. До обновления Ideco Center проверьте в разделе **Серверы** версии всех подключенных NGFW Novum и обновите серверы с версией ниже 22.1.

2. Дождитесь, пока обновленные серверы автоматически переподключатся к Ideco Center.

3. Обновите Ideco Center до версии 23. Настройки переподключившихся серверов сохранятся при миграции.

Полезные ссылки

- **Серверы**
- **Ideco Center**

Ideco Center 22.1.109

Дата выхода версии: 15.05.2026.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в телеграм-канале с разработчиками: https://telegram.me/idecoutm.
- Портал технической поддержки: support.ideco.ru.
- Telegram: ideco.bot.
- MAX: id6670208848_bot.

Скачать Ideco Center 22.

Примечание к релизу:

Ideco Center 22 предназначен для управления политиками фильтрации межсетевых экранов Ideco NGFW Novum версии 22.

С версии 22 Ideco Center лицензируется. Доступны лицензии Enterprise (коммерческая) и Enterprise-demo (бесплатная лицензия сроком на 44 дня). Подробности в статье Лицензирование.

Новые возможности

Функциональность	Описание
Управление высокопроизводительными контекстами	Добавлена поддержка централизованного управления двумя типами контекстов: классический и высокопроизводительный. Созданные правила и профили переносятся на подключенные серверы и доступны там только для просмотра. Подробности в статьях Правила трафика и Профили безопасности
Географически распределенный кластер для повышения отказоустойчивости и доступности	Добавлена возможность развертывания георасределенного кластера системы управления Ideco Center из двух нод. Конфигурация, внесенная на любом из экземпляров, автоматически синхронизируется между ними. Подробности в статьях Кластеризация и Сервисы
Сбор журналов IPS и WAF из Ideco NGFW	Доступен просмотр отчетности Ideco NGFW в Ideco Center: Журнал IPS и Web Application Firewall. Подробности в статье Отчеты и журналы
Локальные политики	Возможность настраивать правила фильтрации входящего (INPUT) трафика, направленного непосредственно на сервер Ideco Center. Подробности в статье Локальные политики

Исправленные ошибки

ID задачи	Описание
ICS-59777	Устранена ошибка, при которой переполнялись таблицы логов Ideco NGFW в Ideco Center

Ideco Center 22.6.105

Примечания к релизу

Дата выхода версии: 07.08.2026.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в Telegram-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Telegram: ideco.bot
- MAX: id6670208848_bot

Скачать Ideco Center 22

Если на подключенных серверах установлен Ideco NGFW Novum версии 22.4 или новее, для корректной передачи журналов серверов на Ideco Center обновите Центральную консоль до версии 22.6.

Подготовка к обновлению на версию 23

Изменения с версии 23:

- **Системный контекст** и все VCE могут быть подключены только к одному Ideco Center, а управление подключением выполняется только из **Системного контекста**. VCE с несовпадающими подключениями при обновлении будут автоматически отключены. Перед обновлением приведите конфигурацию к одному виду. Подробности – в статье Подготовка к обновлению VCE, подключенных к Ideco Center.
- Раздел **Администраторы** будет доступен только в **Системном контексте**. Управление учетными записями и доступами администраторов VCE станет централизованным. Ознакомьтесь с особенностями переноса администраторов из VCE в Системный контекст в статье Подготовка к миграции администраторов из VCE.
- К Ideco Center версии 23 смогут подключаться только серверы Ideco Center версии 22.1 и выше. Серверы более младших версий будут отключены от Ideco Center без возможности восстановления. Чтобы подключенные серверы сохранились, соблюдайте порядок обновления.

Безопасность

- Закрыты уязвимости CVE-2026-31431, CVE-2026-32792, CVE-2026-33278, CVE-2026-40622, CVE-2026-41292, CVE-2026-42534, CVE-2026-42923, CVE-2026-42944, CVE-2026-42959, CVE-2026-42960, CVE-2026-43333, CVE-2026-44390, CVE-2026-44608, CVE-2026-46300 в различных компонентах продукта.
- Исправлена уязвимость ядра Linux GRO Frag (класс Copy Fail) в подсистеме GRO, связанная с локальным повышением привилегий до root (не эксплуатируется удаленно, требует выполнения локально).

Улучшения и оптимизация

- В правилах **Межсетевого экрана** FORWARD для **Высокопроизводительных контекстов** добавлено поле **Название**.
- В правилах **Межсетевого экрана** для **Высокопроизводительных контекстов** во всплывающей подсказке профиля безопасности добавлена кнопка перехода к профилю.
- Добавлена поддержка сжатия данных в журнале **Межсетевого экрана**, что уменьшает занимаемое место на диске.
- Время истечения сертификатов в разделе **Сертификаты** теперь отображается по серверному времени.
- В форме добавления/редактирования **Внешнего DNS-сервера** доступны все сетевые интерфейсы.

Исправленные ошибки

ID задачи	Описание	Модуль
CC-844	Устранена ошибка, из-за которой при добавлении правила в **Контент-фильтр** пропадала пользовательская категория	Контент-фильтр

CC-960	Устранена ошибка при скрытии столбцов в таблице **Серверы**	Серверы
CC-866	Устранена ошибка, из-за которой группу с сервером внутри нельзя было переместить в другую группу	Серверы
CC-922 ICS-65098	Исправлен доступ в разделы веб-интерфейса для администраторов с ролями **Администратор межсетевого экрана** и **Администратор настройки доступа**	Администраторы
ICS-66932	Устранена ошибка, из-за которой в интерфейсе отображалось сообщение об отсутствии включенных модулей в лицензии	Лицензия
ICS-66376	Исправлена ошибка при применении фильтра в журнале **Система**	Отчеты и журналы
ICS-66265	Исправлена ошибка 404 при наведении на идентификатор сигнатуры в журнале IPS	Отчеты и журналы
ICS-64117	Исправлено отображение значений SD-WAN в snmpwalk: вместо алиасов теперь возвращаются реальные значения	SNMP

Лицензирование

> В статье представлено описание доступных в Ideco Center лицензий.

Лицензия Ideco Center позволяет управлять доступом к функциям централизованного администрирования серверов Ideco Center. Если два Ideco Center объединяются в кластер, то на каждую ноду нужно приобретать отдельную лицензию.

Виды лицензий

В Ideco Center доступны лицензии:

- **Enterprise** - коммерческая лицензия.
- **Enterprise-demo** - бесплатная лицензия сроком на 44 дня. Формируется автоматически при регистрации сервера в MY.IDECO.

Подробнее о привязке лицензий - в статье.

После добавления лицензии модуль подключения к Ideco Center включается в лицензию Ideco NGFW и обеспечивает передачу политик и настроек из Ideco Center на серверы Ideco NGFW.

Подробнее о лицензиях в Ideco NGFW - в статье.

По истечении срока действия модуля:

- Политики и настройки, уже распространенные на Ideco NGFW, сохраняются и продолжают действовать.
- Новые настройки из Ideco Center не распространяются на Ideco NGFW до продления модуля.

Просмотр информации о лицензиях

Посмотреть информацию о лицензии можно:

- В MY.IDECO в разделе **Ideco Center**, нажав напротив нужного сервера.
- В Ideco Center в разделе **Управление сервером** → **Лицензия**.

Лицензия содержит сведения:

- Номер лицензии
- Тип лицензии
- Дата начала действия лицензии
- Окончание лицензии
- Окончание обновлений
- Окончание технической поддержки
- Количество пользователей
- Название компании
- Название сервера

Техническая поддержка

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

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

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

График работы

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

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

Способы обращения

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

Правила обращения

Техническая поддержка пользователей осуществляется в соответствии с регламентом.

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

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

Скачивание журнала системных событий

В веб-интерфейсе Ideco Center доступно скачивание журнала системных событий для передачи в техническую поддержку.

Журнал помогает диагностировать неудачное обновление: если после перехода на новую версию возникли проблемы и был выполнен возврат на предыдущую версию, журнал сохранит события проблемной версии. Эти данные помогают технической поддержке определить причину сбоя, даже когда продукт уже работает на прежней версии.

Для скачивания нажмите в правом верхнем углу экрана, а затем **Скачать** в блоке **Журнал событий системы**:

Журнал событий системы

Архив содержит записи системных событий. Отправьте его для анализа в техподдержку.

Скачать

Начнется загрузка архива в формате **zst**. Состав журнала зависит от того, выполнялся ли возврат к предыдущей версии:

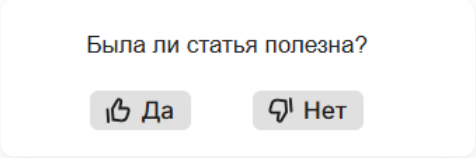
- Если установка первичная или возврата к предыдущей версии не было, файл содержит события текущей версии.
- Если был возврат к предыдущей версии, файл содержит события версии, с которой произошел возврат, и события текущей версии.

Обратная связь

Мы постоянно совершенствуем нашу документацию и всегда рады вашим отзывам.

Как оставить отзыв:

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

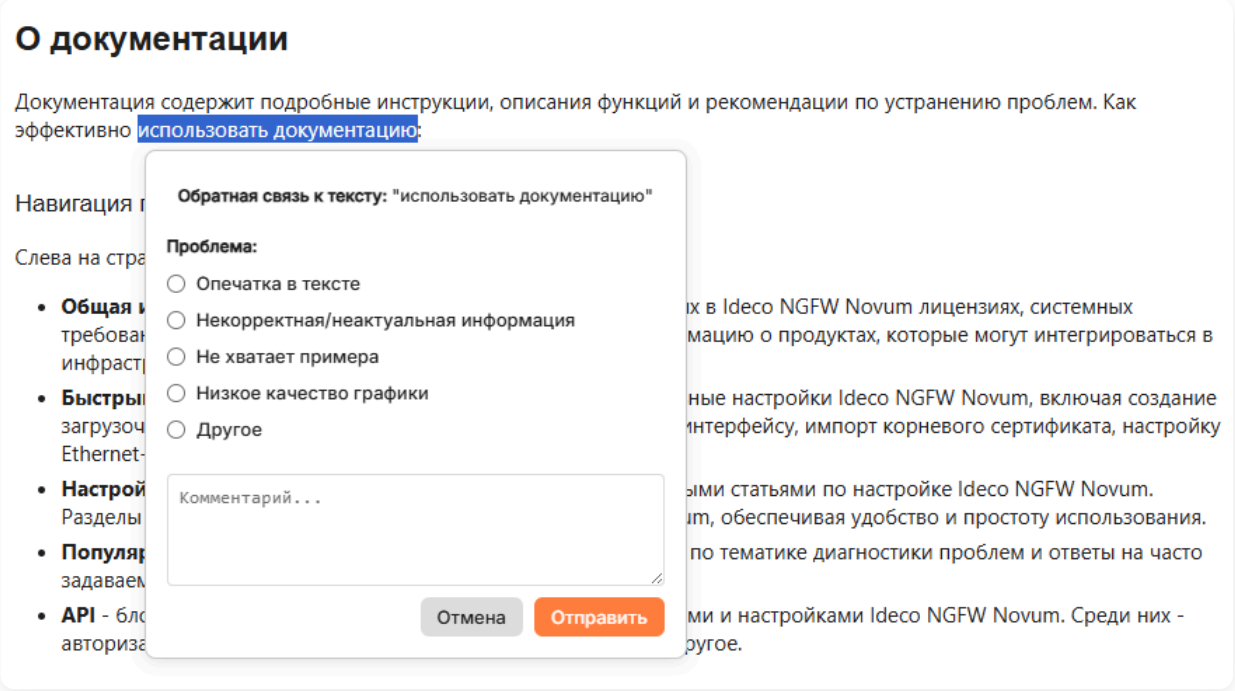


- Написать комментарий к фрагменту текста внутри статьи.

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

Чтобы написать комментарий:

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



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

3. Нажмите **Отправить**.

Описание Ideco Center

Название службы раздела **Ideco Center**: `ideco-central-console-backend`.

Список служб для других разделов доступен по ссылке.

Ideco Center - центральная консоль для управления несколькими серверами Ideco NGFW. Ideco Center автоматически распространяет политики безопасности на все подключенные Ideco NGFW.

Ideco NGFW Novum подключается к Ideco Center по порту 3151 в двух протоколах:

Протокол и порт	Назначение
TCP/3151	Подключение NGFW Novum и синхронизация объектов, правил и политик безопасности
UDP/3151	Туннель WireGuard: синхронизация базы данных отчетов и журналов с NGFW Novum и переход в его веб-интерфейс

Оба порта должны быть открыты на Ideco Center или перенаправлены на него через NAT. Если открыт только TCP/3151, NGFW Novum подключится и получит настройки, но синхронизация базы данных отчетов и журналов и переход в веб-интерфейс NGFW Novum работать не будут.

Подключение всегда устанавливает NGFW Novum, поэтому открывать входящие порты на стороне NGFW Novum не требуется.

Возможности Ideco Center

- ✅ Централизованное управление серверами Ideco NGFW, подключенными к Ideco Center
- ✅ Разделение по группам серверов Ideco NGFW
- ✅ Формирование иерархии из групп Ideco NGFW
- ✅ Создание объектов, политик и профилей безопасности и их назначение серверам Ideco NGFW
- ✅ Переход из Ideco Center в веб-интерфейс подключенных Ideco NGFW. Администраторы Ideco Center имеют доступ к подключенным Ideco NGFW, но администраторы подключенных Ideco NGFW не имеют доступа к Ideco Center
- ✅ Интеграция с Microsoft Active Directory/Samba DC

Подробнее о работе политик безопасности и объектов - в статьях Правила трафика и Объекты.

Источники данных Ideco Center

Ideco Center может обращаться к адресам для получения данных:

Тип запроса	Адрес
Отправка уведомлений в личный кабинет/телеграм-бот	api.ideco.ru
Обновление баз Контент-фильтра	• content-filter.v22.ideco.dev • mcs-vmc1.ideco.ru • mcs-vmc2.ideco.ru • mcs-vmc4.ideco.ru
Отправка анонимной статистики	gatherstat.v22.ideco.dev
Обновления баз GeoIP	• ip-list.v22.ideco.dev • mcs-vm.ideco.ru
Отправка отчетов по почте	api.ideco.ru
Обновления сигнатур IDS/IPS	suricata.v22.ideco.dev
Обновления системы	• api.ideco.ru • storage.yandexcloud.net
Синхронизация времени	ntp.ideco.ru

Чтобы все модули фильтрации Ideco Center работали правильно, доступ к указанным ресурсам должен быть разрешен в настройках.

Настройка гипервизора

Особенности

- Если при установке Ideco Center появилось окно с текстом **Installation in BIOS mode is not supported**, включите режим UEFI в настройках гипервизора.
- Не рекомендуем использовать LACP на виртуальных сетевых адаптерах в Center, так как системы виртуализации часто требуют нетривиальной настройки для работы LACP или вообще не поддерживают этот режим. Рекомендуем настраивать агрегацию каналов средствами гипервизора. Если сетевые карты проброшены в виртуальную машину на уровне PCI (PCI passthrough), LACP можно настраивать внутри Center.

Для обеспечения отказоустойчивости используются 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.

VMware ESXi 6.7

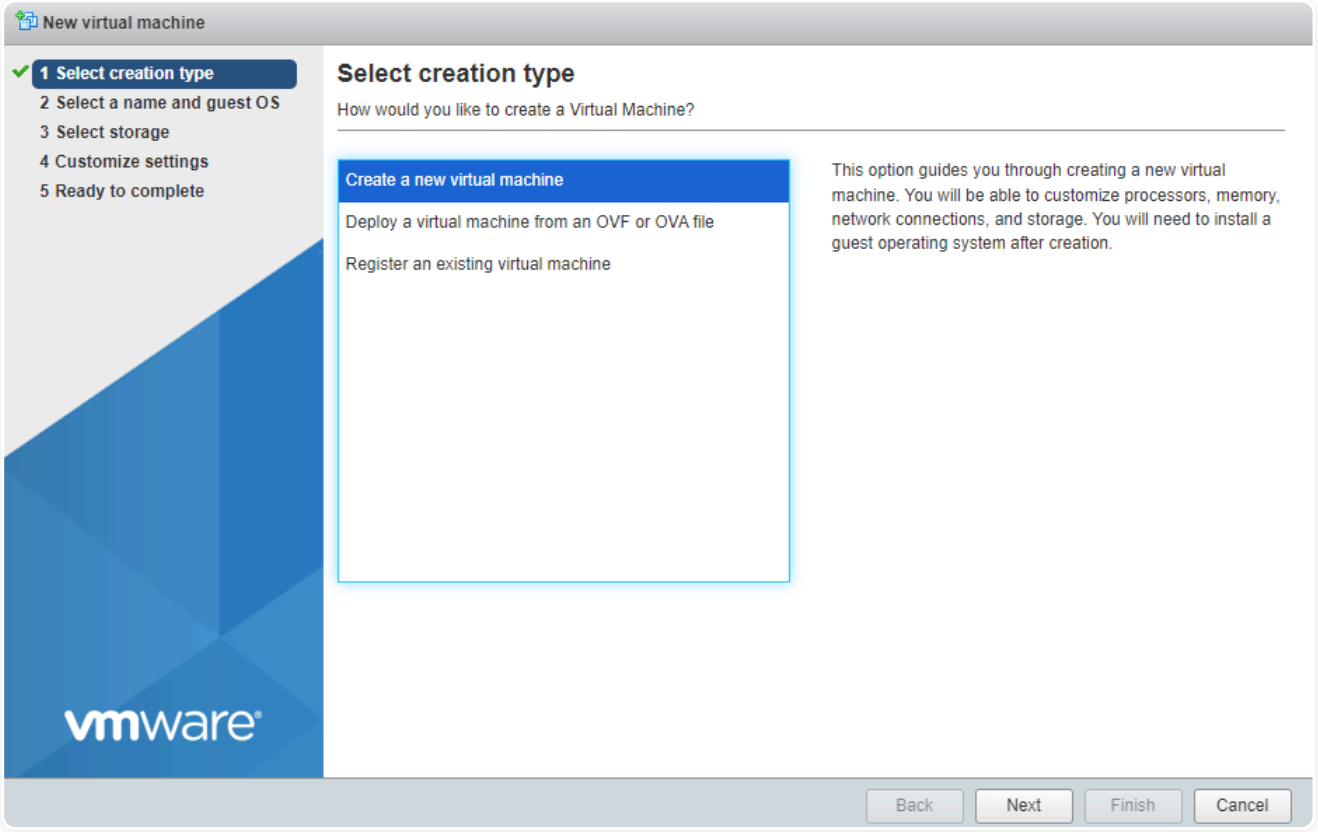
При установке Ideco Center на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

Настройка

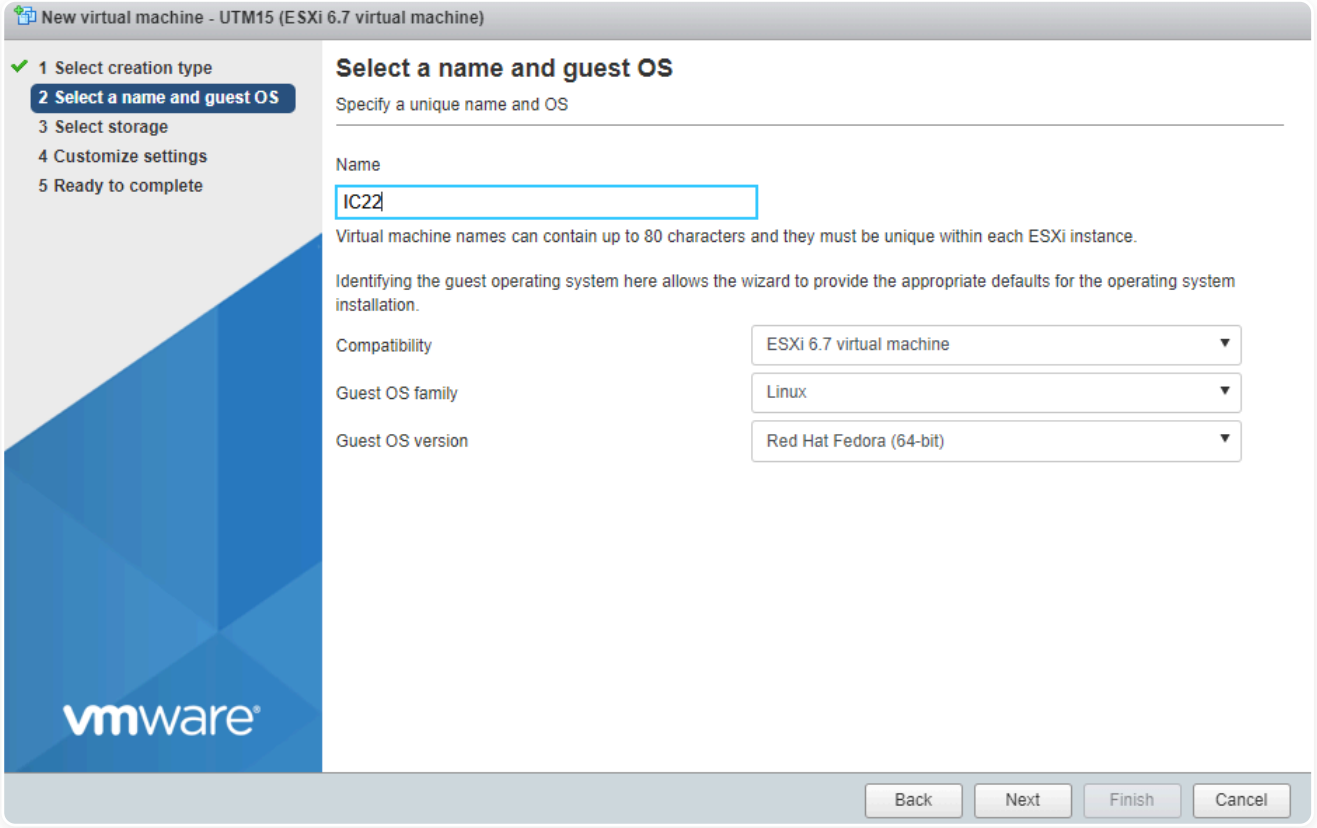
Перед установкой Ideco Center:

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

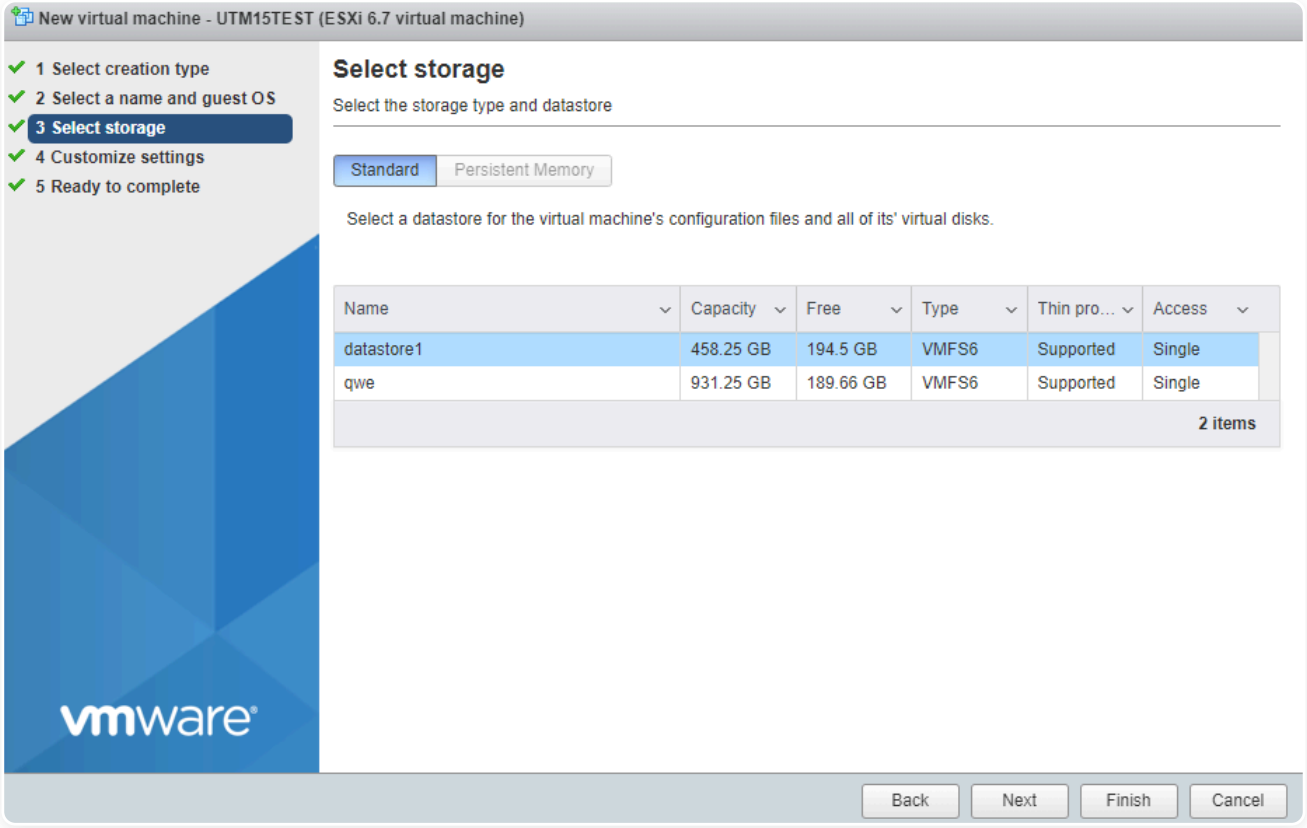
1. Создайте виртуальную машину:



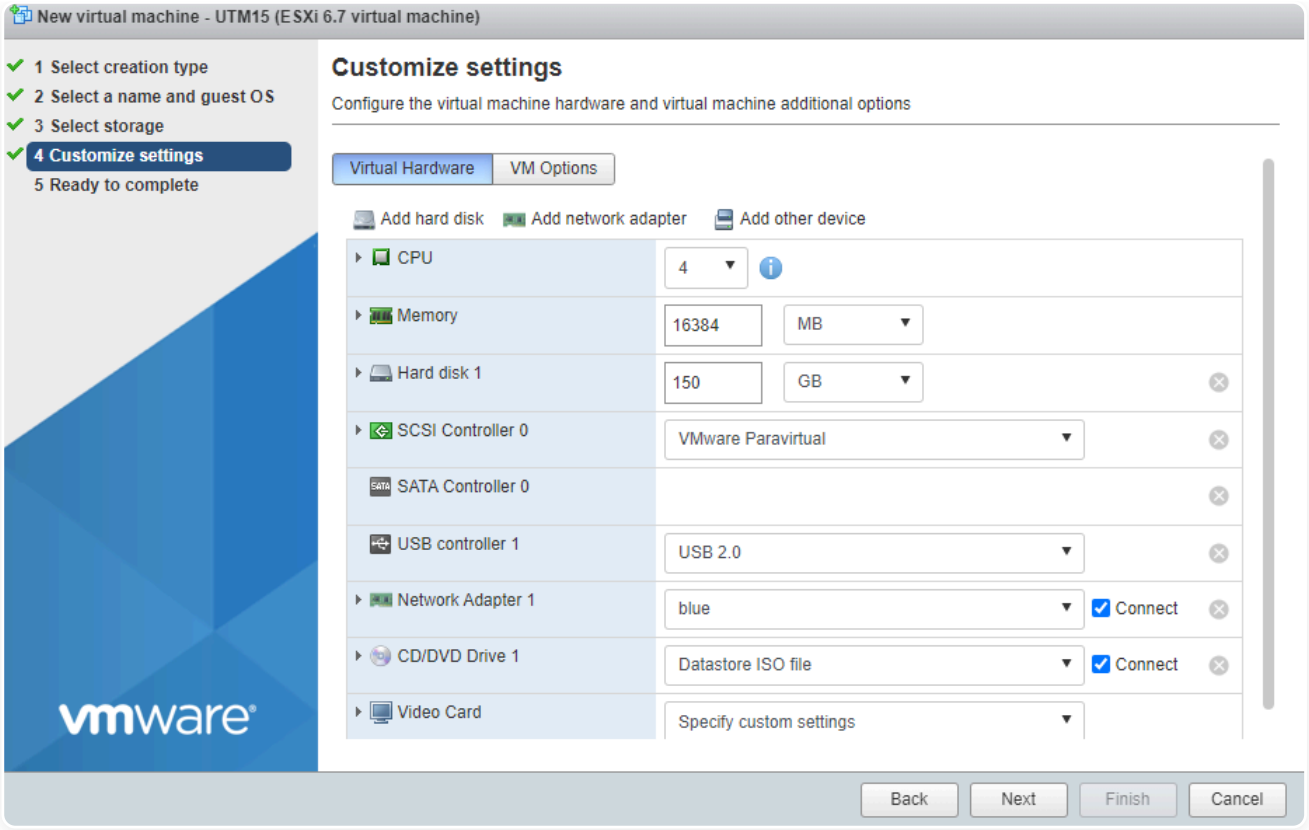
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



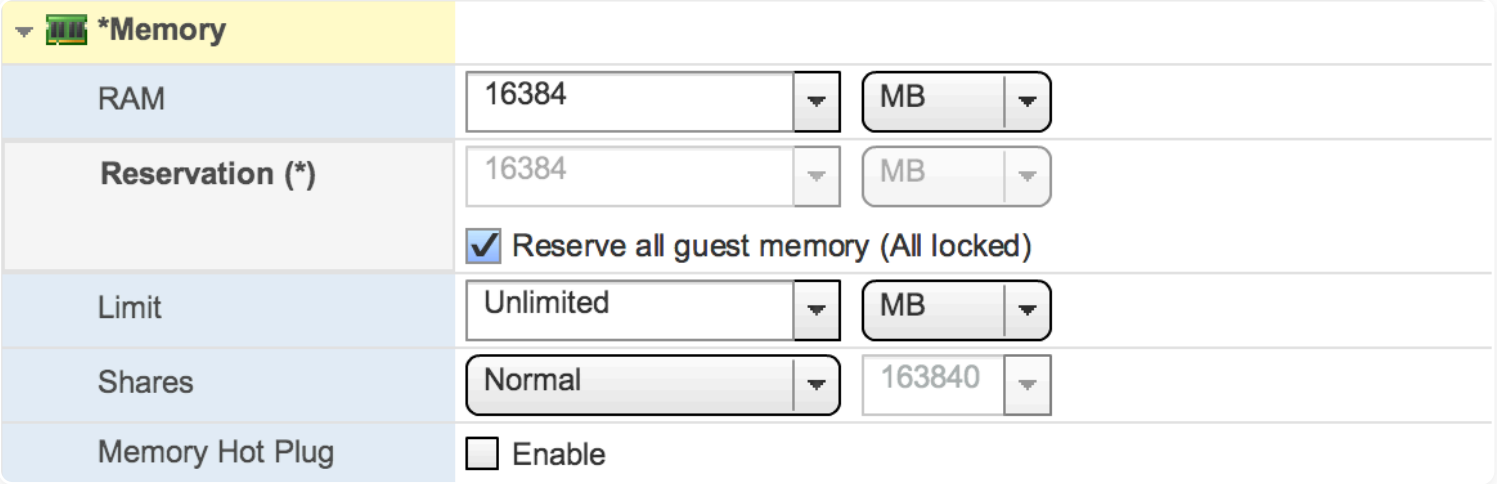
3. Выберите хранилище для виртуальной машины:



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

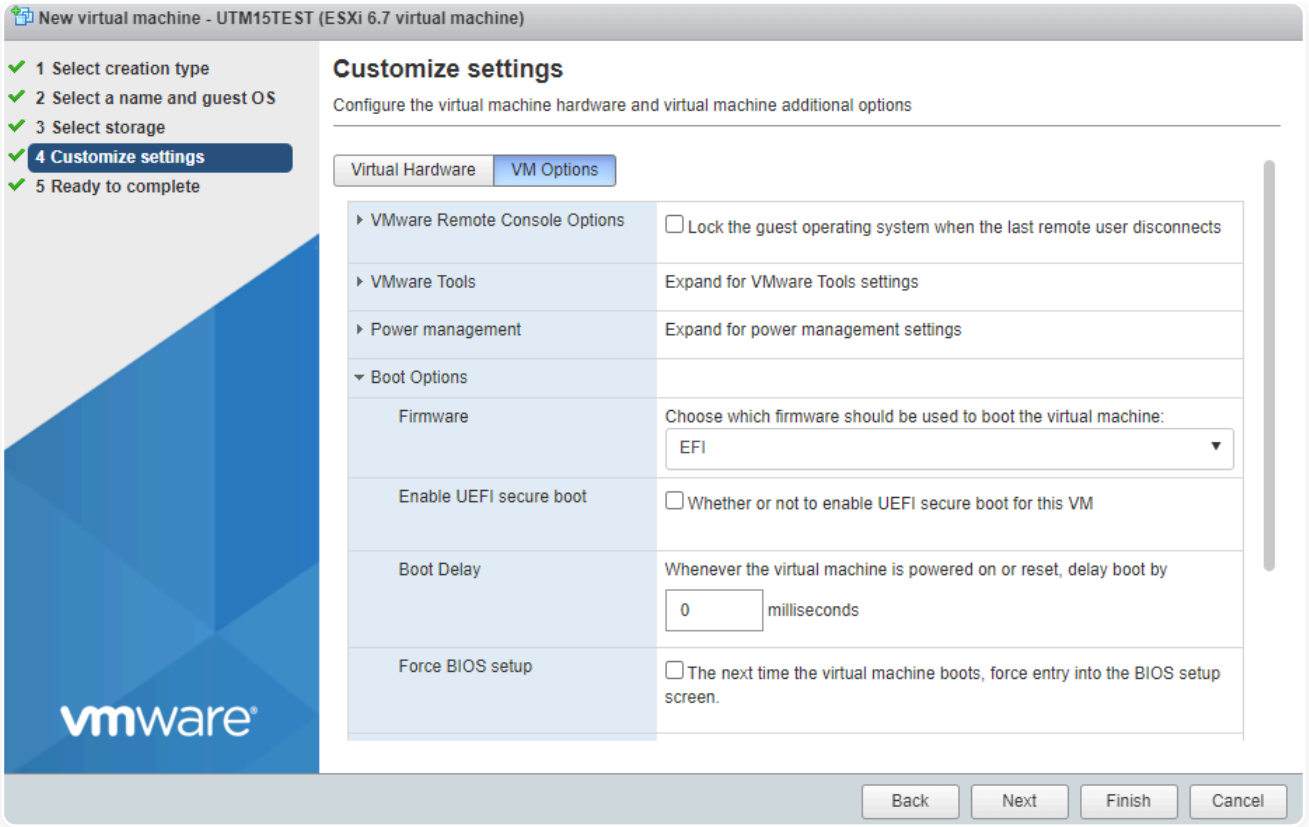


5. Разверните раздел **Memory** и включите опцию **Reserve all guest memory (All locked)**:



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

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



7. Нажмите **Finish**:

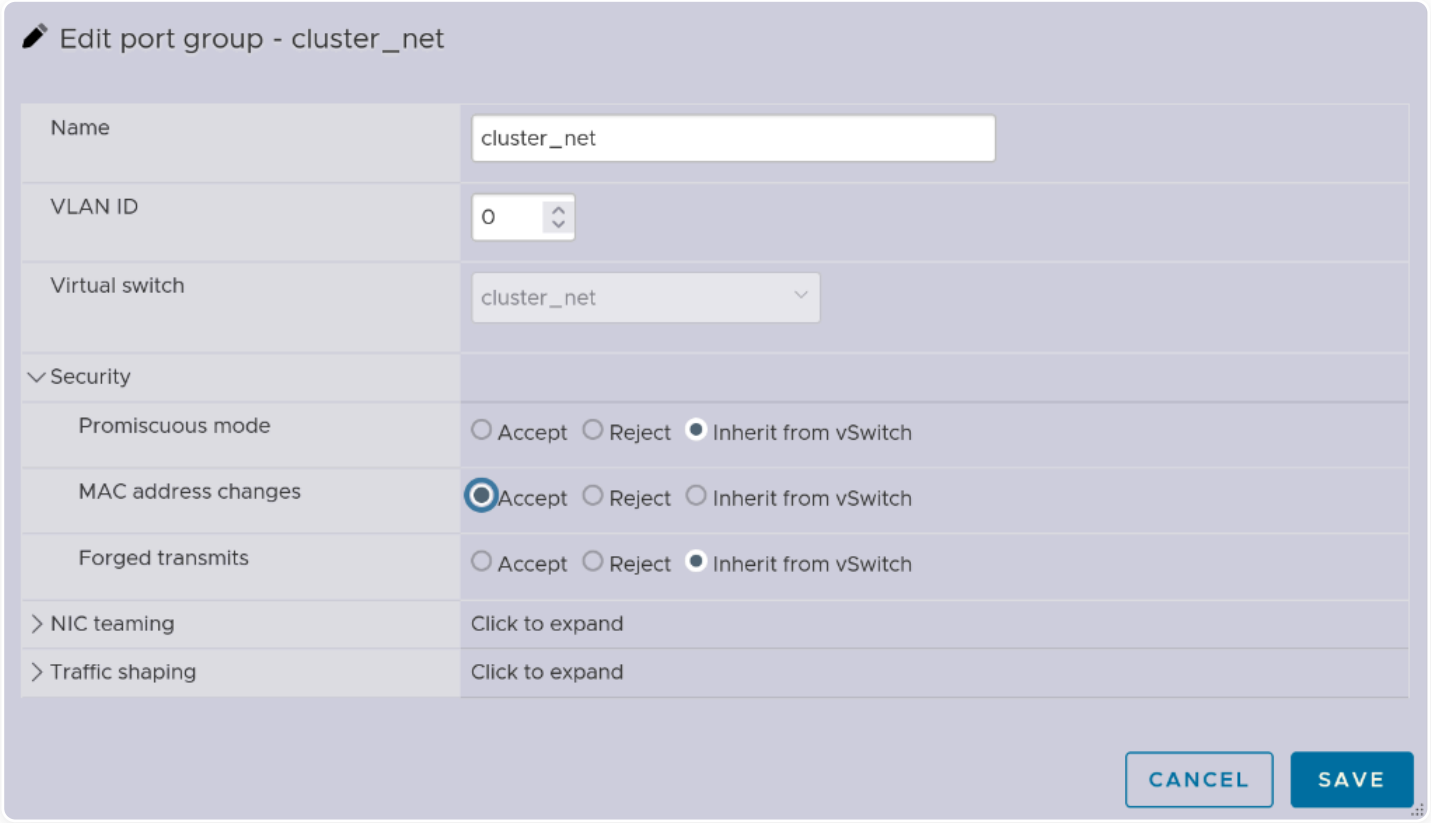
Настройка LACP-интерфейсов

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

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

2. Выберите группу портов, используемую для LACP.

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



4. Нажмите **Save**.

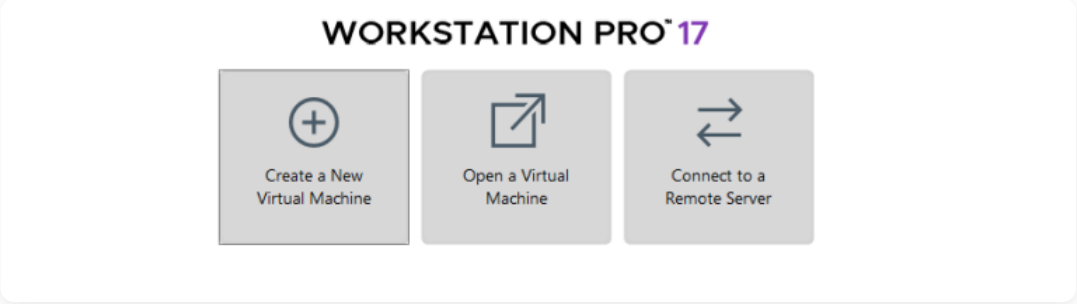
VMware Workstation 17.0

Настройка

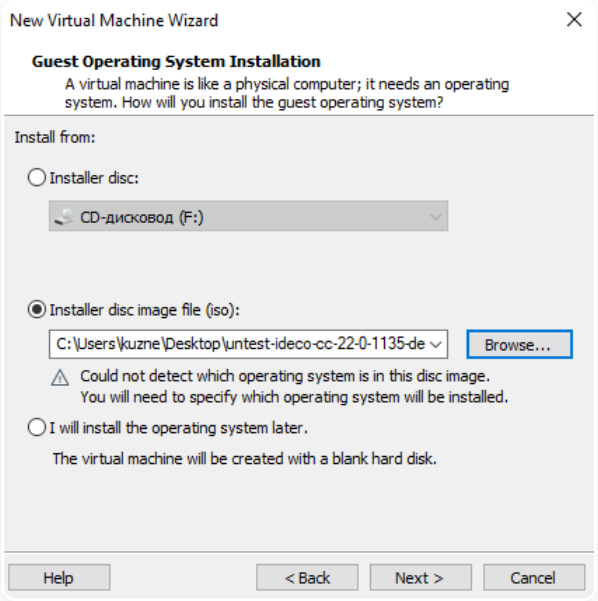
Перед установкой Ideco Center:

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

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

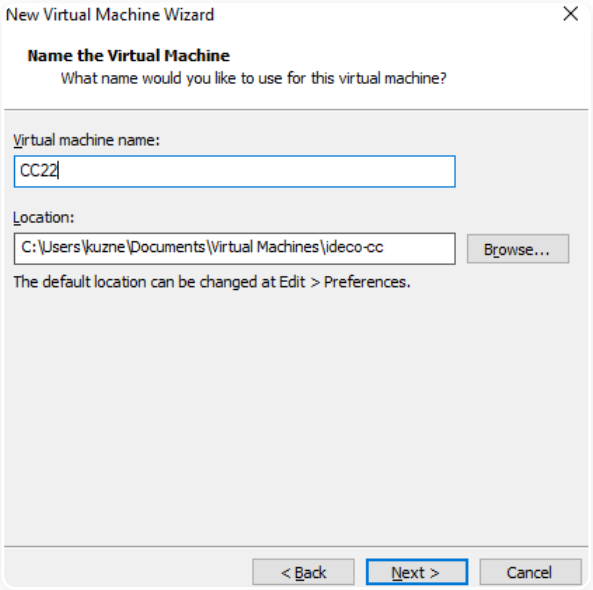


2. Укажите загрузочный ISO-образ:



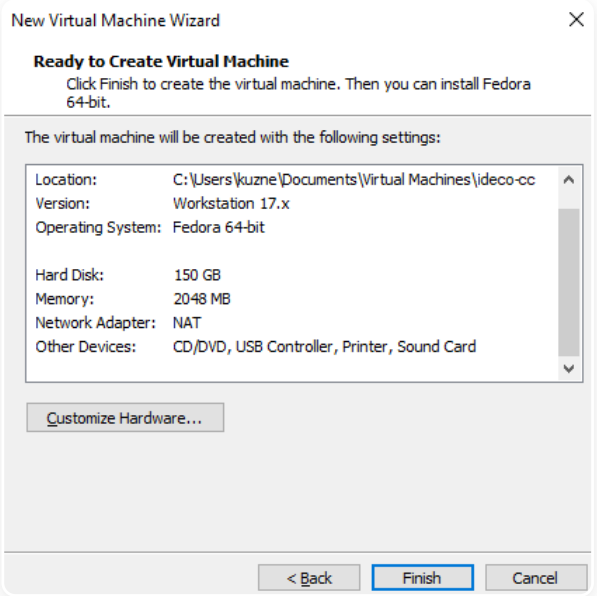
3. Выберите гостевую операционную систему **Linux** и в раскрывающемся списке укажите тип **Fedora 64-bit**:

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



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

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



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

8. Укажите количество ядер процессора, равное 4:

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

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

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

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

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

VirtualBox 7.0.12

Настройка

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

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

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

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

4. Нажмите **Готово**.

KVM

Настройка

Минимальные требования к виртуальной машине описаны в статье.

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

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

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

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

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

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

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

Proxmox

Настройка

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

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

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

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

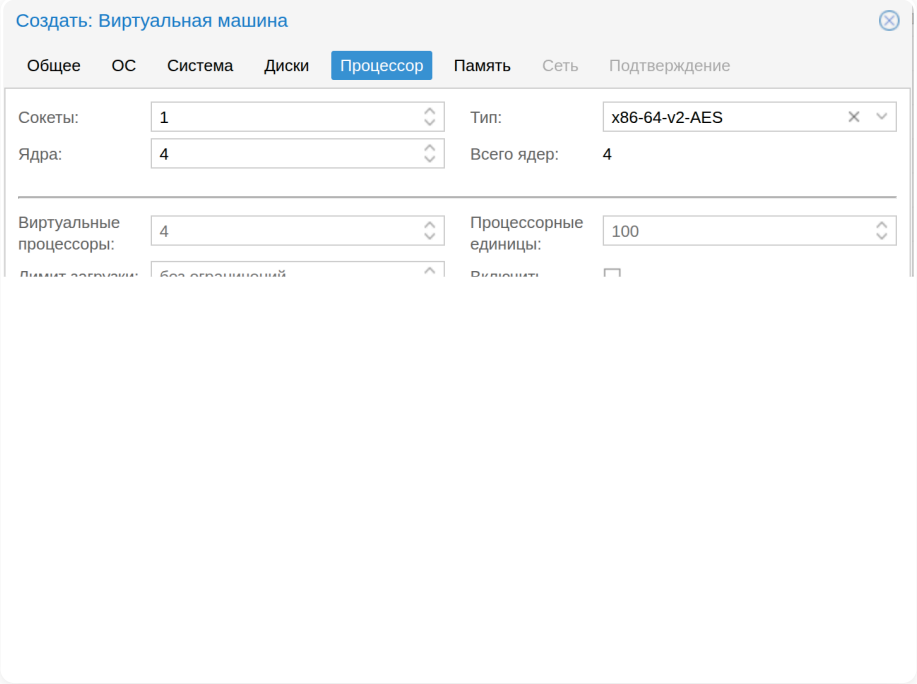
- **Машина** - q35.
- **BIOS** - OVMF.
- **Хранилище EFI** - хранилище для UEFI-диска.
- **Агент QEMU** - включите опцию, чтобы операционная система могла передавать гипервизору информацию о своих внутренних состояниях.
- **Предварительная загрузка ключей** - отключите опцию.

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

- **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.

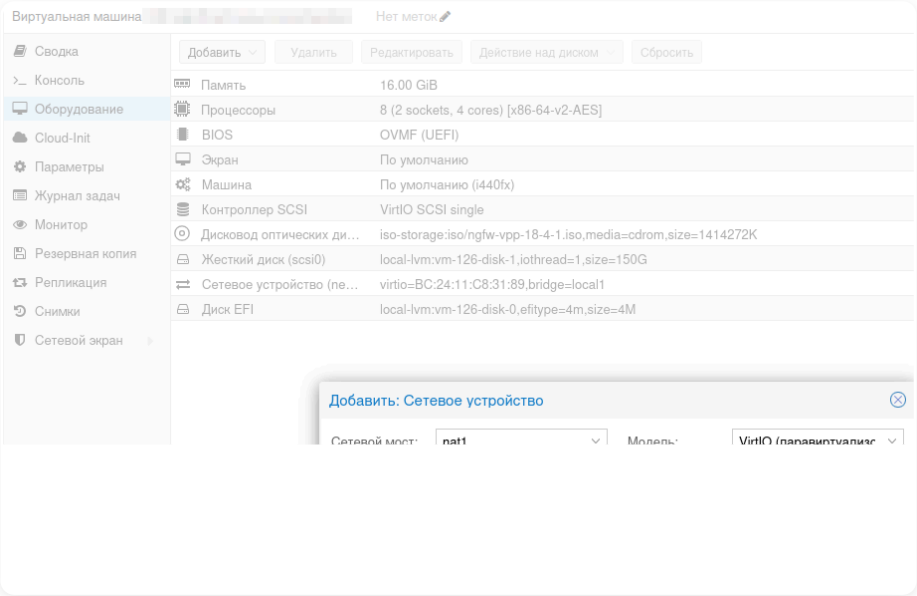
7. В разделе **Сеть** в поле **Сетевой мост** выберите сетевой мост для локального интерфейса:

Рекомендуем отключить опцию **Сетевой экран**, чтобы облегчить настройку и отладку сети Ideco Center и избежать конфликтов обработки трафика.

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

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

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



Microsoft Hyper-V

Настройка

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

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

Минимальные требования к виртуальной машине описаны в статье.

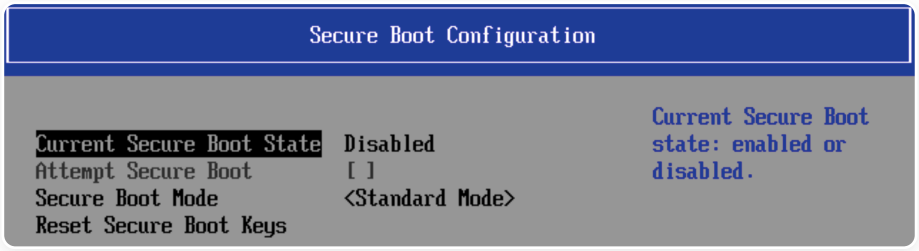
Шаги по установке Ideco Center после создания загрузочного USB-накопителя можно прочитать в статье Установка.

При использовании LACP-интерфейсов требуется дополнительная настройка:

1. Перейдите в **Hardware** → **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**:



Установка Ideco Center

Технические требования для серверов и виртуальных машин:

Требования	Характеристики
Процессор	• Intel i3/i5/i7/i9/Xeon минимум 4 поколения Haswell (2013г.) • AMD FX/Ryzen/EPYC • Поддержка SSE 4.2 • От 4 ядер
Объем оперативной памяти	• От 16 ГБ
Накопитель	• Объем 150 ГБ или более • SSD с интерфейсом SATA, mSATA, SAS, NVMe • Не гарантируется работа с аппаратными RAID-контроллерами (программные контроллеры, интегрированные в чипсет, не поддерживаются) • Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти
Сеть	• Одна сетевая карта. Рекомендуется использовать карты на чипах Intel
BIOS	• Поддержка UEFI • Отключенная опция Secure Boot в UEFI • Отключенный режим Legacy, может называться CSM (Compatibility Support Module)
Дополнительно	• Монитор и клавиатура

Файл для установки Ideco Center доступен для скачивания в MY.IDECO.

Процесс установки

При установке Ideco Center с загрузочного USB-диска выберите загрузку с USB-диска в настройках UEFI компьютера.

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

Для установки Ideco Center выполните действия:

1. Перейдите к установке, нажав **Install Ideco CC**:

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

```
Установка Ideco CC 22.0.1561
----------------------------

Для установки выбран диск '161 ГБ - QEMU HARDDISK (drive-scsi0)'.
ВНИМАНИЕ! Все данные на нём будут уничтожены!

Пожалуйста подтвердите ваш выбор.

Введите 'y' и нажмите Enter для подтверждения.
Введите 'c' и нажмите Enter для отмены.
#
```

3. Выберите временную зону, в которой находится сервер:

```
Выберите временную зону.

1. Алма-Ата                                    21. Магадан
2. Анадырь                                     22. Москва
3. Астрахань                                   23. Новокузнецк
4. Багдад                                      24. Новосибирск
5. Баку                                        25. Омск
6. Барнаул                                     26. Самара
7. Белград                                     27. Саратов
8. Бишкек                                      28. Сахалин
9. Владивосток                                 29. Симферополь
10. Волгоград                                  30. Ташкент
11. Екатеринбург                               31. Тбилиси
12. Ереван                                     32. Томск
13. Иркутск                                    33. Ульяновск
14. Калининград                                34. Чита
15. Камчатка                                   35. Якутск
16. Карачи                                     36. Аден
17. Киев                                       37. Актау
18. Киров                                      38. Актобе
19. Кишинёв                                    39. Амман
20. Красноярск                                 40. Амстердам

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
Нажмите Enter для вывода следующей страницы вариантов.
#
```

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

```
Текущая дата и время: 07 октября 2025, 06:49.

Данные указаны правильно?

Введите 'y' и нажмите Enter для подтверждения.
Введите 'n' и нажмите Enter для отказа.
Введите 'c' и нажмите Enter для отмены.
#
```

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

5. Не нажимайте никаких клавиш при появлении окна:

```
Ideco CC 22.0.1561
Kernel 6.18.7-100.1775716949.56.ef1e92dd.utm.x86_64 on x86_64 (tty1)

localhost login: _
```

После загрузки система автоматически перейдет к локальному интерфейсу Ideco Center.

Создание учетной записи администратора

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

```
Ideco CC 22.0.1561
------------------


Внимание! Аккаунт администратора отсутствует.
Требуется предварительно его создать.
Создание аккаунта администратора.

Введите новый логин и нажмите Enter.

# _
```

Требования к логину и паролю

Логин:

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

Пароль:

- Минимальная длина пароля - 12 символов.
- Содержит строчные и заглавные латинские буквы.
- Содержит цифры.
- Содержит специальные символы (! # $ % & ' * + и другие).

> Если пароль не соответствует требованиям политики безопасности, то появится надпись с информацией, что пароль ненадежен. Потребуется ввести новый пароль с учетом требований.
>
> Не используйте Numpad при вводе пароля, так как в консоли эти клавиши интерпретируются как Escape-последовательности: `^[[2~;`, `^[[4~;` и так далее.

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 MAC-адрес сетевой карты.

Для настройки Ideco Center через веб-интерфейс создайте интерфейс Control Plane в локальном меню. Control Plane - интерфейс администрирования, используется для настройки Ideco Center через браузер. Должен иметь свой выход в Интернет.

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

```
Управление сервером

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

Введите номер пункта и нажмите Enter.
# 3

1. Показать список и отредактировать интерфейс
2. Создать интерфейс
3. Включить/Отключить интерфейс
4. Удалить интерфейс

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 2
```

2. Выберите порт для доступа к веб-интерфейсу:

```
# 2

Выберите порт

-----------------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-----------------------------------------------------------------------------------------------------
  1    |  eth0_a6  |  bc:24:11:cc:7b:a6  |  Сервис        |  Red Hat, Inc. Virtio network device
-----------------------------------------------------------------------------------------------------

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
#
```

3. Введите имя интерфейса:

```
Введите имя интерфейса и нажмите Enter.

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

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

```
Настроить адресацию на интерфейсе

1. Автоматически через DHCP
2. Вручную
3. Без адресации
```

5. Если выбрали **Вручную**, 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.
# 192.168.100.20/24
Интерфейс успешно настроен.
```

6. После настройки интерфейса Control Plane можно перейти в веб-интерфейс.

Подключение к веб-интерфейсу Ideco Center

1. Запустите на любом компьютере в сети интерфейса Control Plane поддерживаемый браузер (современные версии Firefox, Chrome и браузеров, основанных на Chromium).

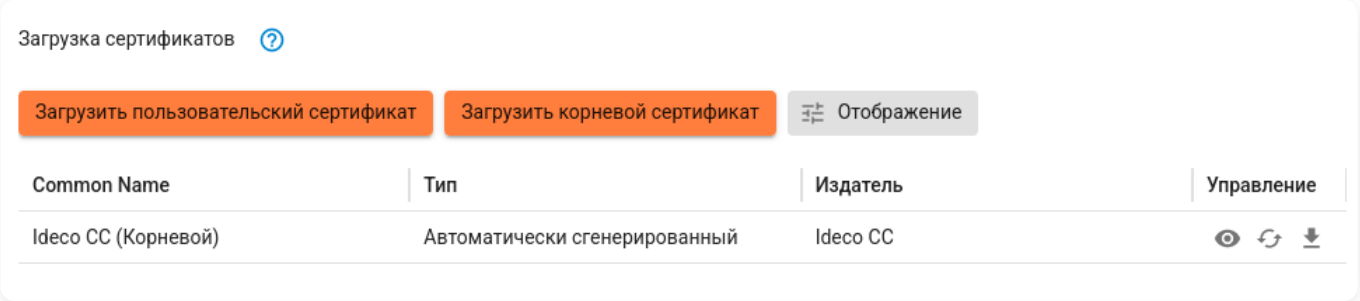
2. Введите в адресной строке IP-адрес, указанный при настройке интерфейса Control Plane, и порт `8443`.

Пример. `https://192.168.100.2:8443`

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

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

Скачать сертификат можно в **Сервисы** → **Сертификаты** → **Загруженные сертификаты**:



Пример импорта сертификата для Windows

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

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

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

Серверы

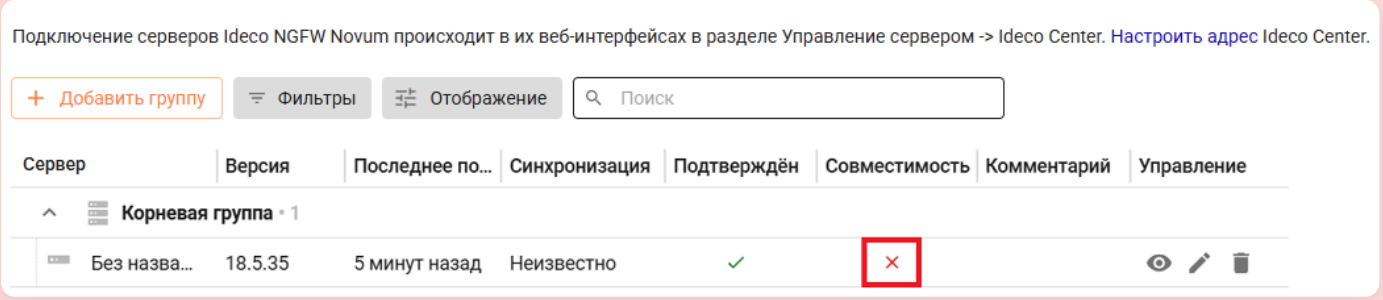
В разделе **Серверы** можно группировать синхронизированные серверы NGFW и формировать из них древовидную структуру. Группировка серверов позволяет применять правила и политики безопасности ко всем серверам каждой группы.

В статье описаны подключение и управление серверами Ideco NGFW.

Документация API

После обновления Ideco Center до версии 23 к нему смогут подключаться только серверы NGFW Novum версии 22.1 и выше. Подробнее – в статье.

Если Ideco Center и Ideco NGFW Novum имеют разные мажорные версии, синхронизация правил не происходит. В разделе **Серверы** отображается информация о несовместимости:



Особенности работы

Установка соединения

- Подключение всегда устанавливает Ideco NGFW Novum: соединение идет в направлении от NGFW Novum к Ideco Center. Поэтому связь работает и когда NGFW Novum находится за NAT, а открывать входящие порты на подключаемом NGFW Novum не требуется.
- Порты TCP/3151 и UDP/3151 должны быть доступны на стороне Ideco Center.
- Если Ideco Center находится за NAT без белого IP-адреса и к нему необходимо подключить Ideco NGFW из другой сети, настройте VPN между офисами через IPsec. Альтернативный способ – создать правило DNAT в веб-интерфейсе Ideco NGFW для проброса порта к Ideco Center.

Протоколы и шифрование

- Туннель WireGuard на UDP/3151 используется для синхронизации базы данных отчетов и журналов между NGFW и Ideco Center, а также для перехода в веб-интерфейс NGFW.
- WebSocket на TCP/3151 используется для остальных коммуникаций между NGFW и Ideco Center.
- Соединение между NGFW и Ideco Center шифруется по протоколу TLS 1.3. Старые версии протокола (TLS 1.0, TLS 1.1, TLS 1.2) отключены.

Обслуживание подключенных серверов

- Для настройки кластера Ideco NGFW Novum достаточно подключить активную ноду. Пассивная нода настроится автоматически.
- Для обновления NGFW, подключенных к Ideco Center, перейдите в интерфейс NGFW и воспользуйтесь статьей Обновления.

Работа с серверами Ideco NGFW

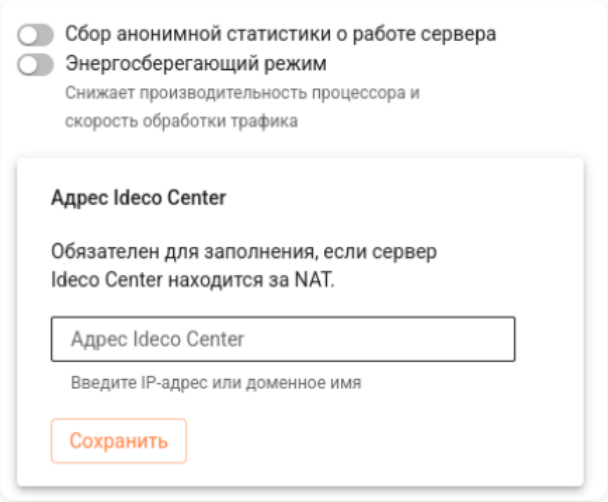
В версии 23 меняется логика привязки VCE к Ideco Center. Перед обновлением ознакомьтесь со статьей Подготовка VCE к обновлению на версию 23.

Настройка Ideco Center, если сервер находится за NAT

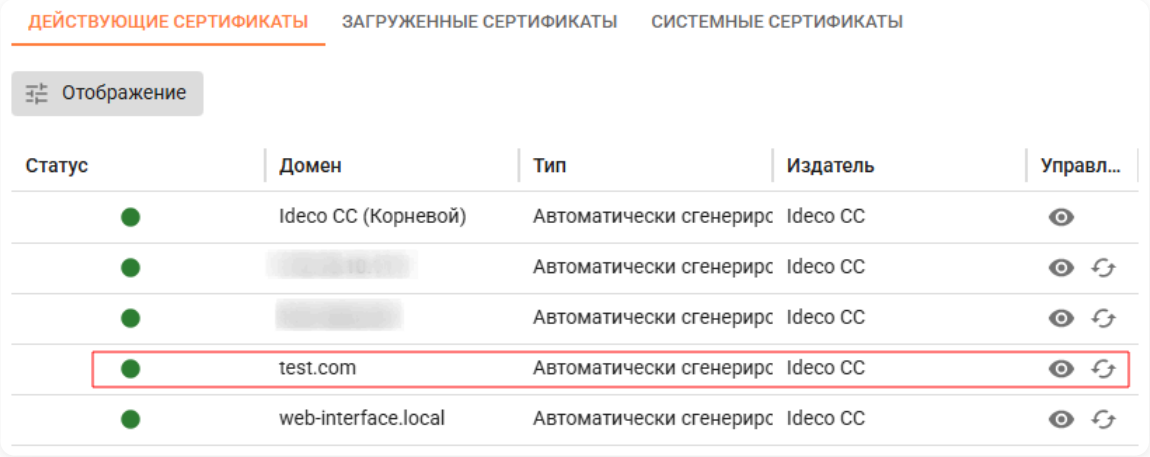
Если сервер Ideco Center находится за NAT:

1. Перейдите в **Управление сервером** → **Дополнительно**.

2. Укажите IP-адрес NAT-устройства или доменное имя в поле **Адрес Ideco Center**:



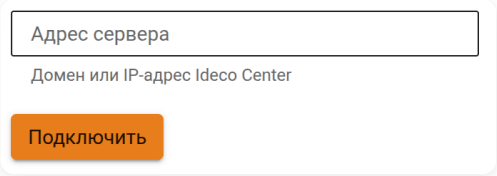
3. Нажмите **Сохранить**. Будет выпущен сертификат на IP-адрес или доменное имя сервера Ideco Center:



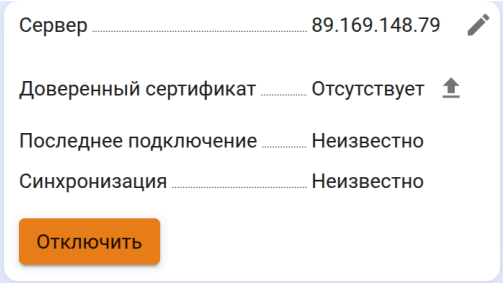
Подключение Ideco NGFW Novum или VCE к Ideco Center

1. В Ideco NGFW или VCE перейдите в **Управление сервером** → **Ideco Center**.

2. Введите IP-адрес или доменное имя в строке **Адрес сервера** и нажмите **Подключить**:

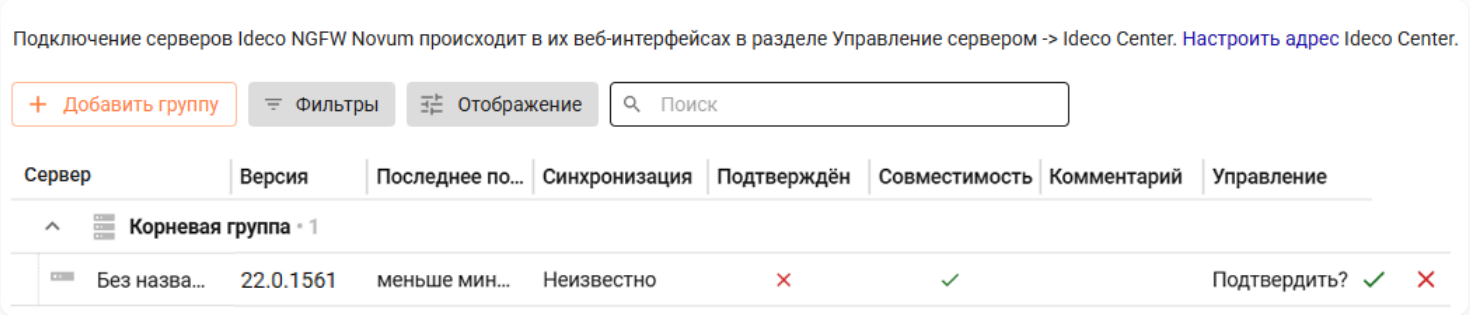


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW или VCE:



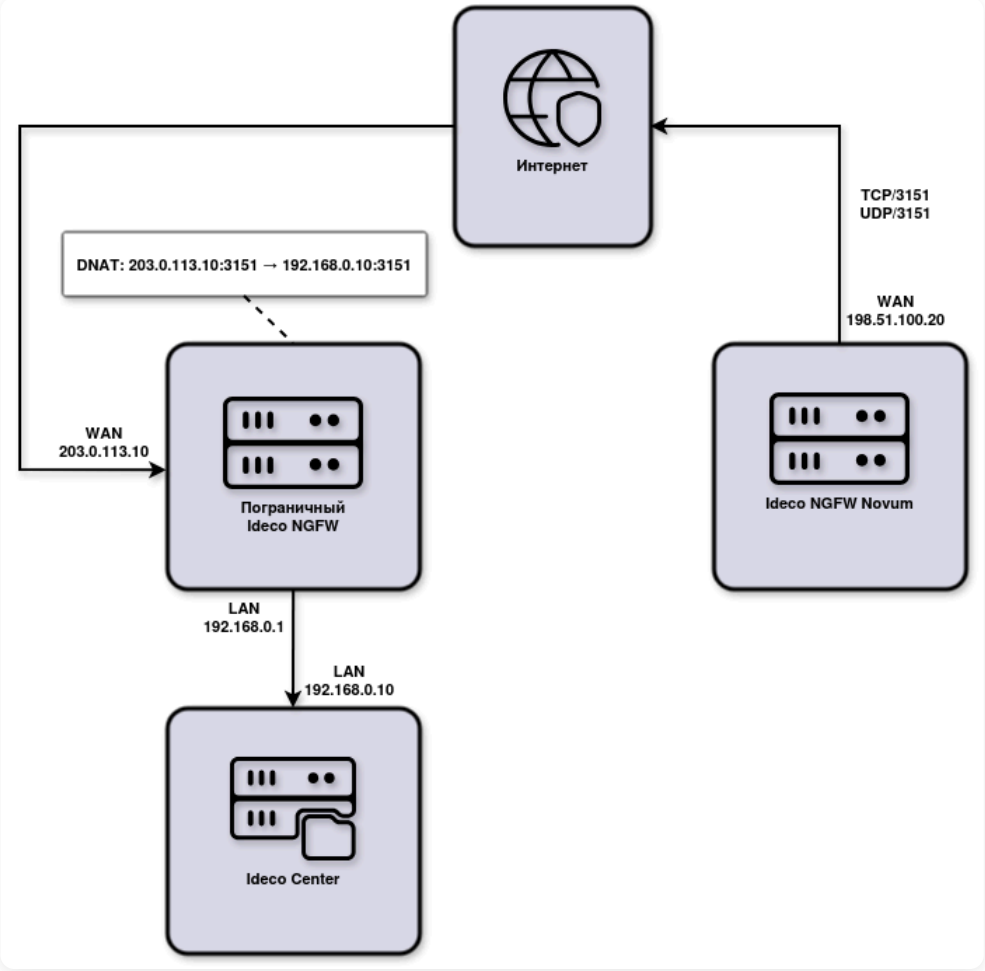
Скачать корневой сертификат можно в Ideco Center, раздел **Сервисы** → **Сертификаты**.

3. В интерфейсе Ideco Center перейдите в раздел **Серверы** и подтвердите подключение кнопкой ✓:

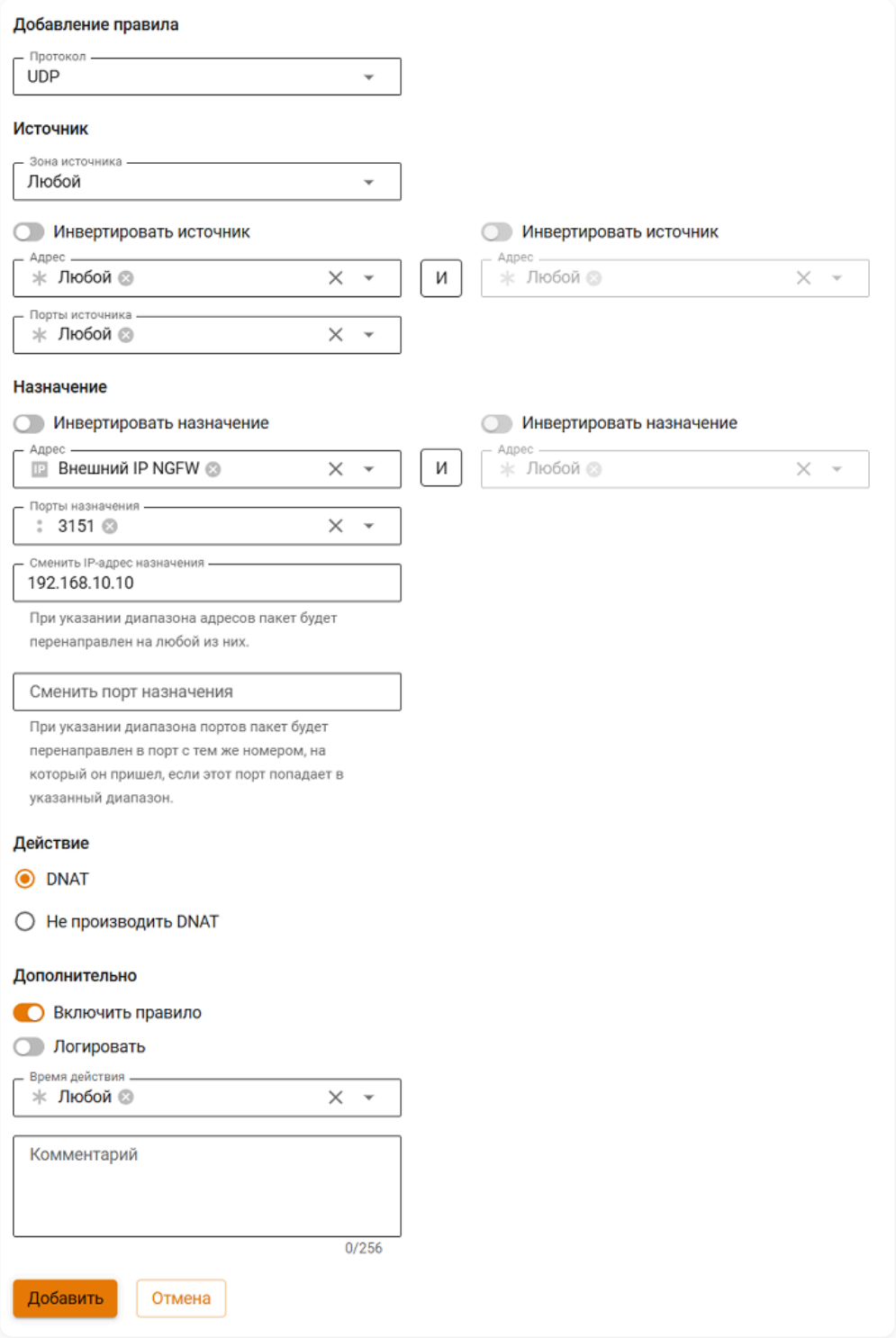


Портмаппинг при подключении Ideco NGFW к Ideco Center

Если Ideco Center находится в локальной сети, NGFW Novum подключается к нему из другой сети, а VPN между офисами нет, настройте проброс портов на пограничном Ideco NGFW, за которым стоит Ideco Center:



Создайте на пограничном NGFW два одинаковых правила для протоколов **UDP** и **TCP** в **Правила трафика** → **Межсетевой экран** → **DNAT**. По TCP идет подключение и синхронизация, по UDP работает туннель WireGuard, поэтому оба правила обязательны:



- **Назначение** – внешний IP-адрес Ideco NGFW.
- **Сменить IP-адрес назначения** – внутренний IP-адрес Ideco Center.
- **Порт** – только порт 3151.

После включения правил трафик будет проходить в локальную сеть через внешний интерфейс и перенаправляться в Ideco Center.

Удаление сервера Ideco NGFW из Ideco Center

При разрыве привязки из Ideco NGFW удаляются все объекты, профили, правила и политики, полученные с Ideco Center. Это может привести к нарушению работы сети.

Перед удалением убедитесь, что объекты, полученные с Ideco Center, не используются в локальных правилах Ideco NGFW, либо замените их локальными объектами.

Для удаления Ideco NGFW из Ideco Center нажмите напротив сервера:

Переход из веб-интерфейса Ideco Center в веб-интерфейс Ideco NGFW

В Ideco Center предусмотрено два способа перехода в Ideco NGFW:

1. В **Серверы** нажмите на напротив нужного сервера:

2. Нажмите на в левом верхнем углу и выберите нужный NGFW:

Чтобы перейти к веб-интерфейсу VCE подключенных серверов в Ideco Center:

1. Зайдите в веб-интерфейс NGFW, используя один из указанных способов.

2. Следуйте инструкциям из статьи.

> Если к Ideco Center версии 22 подключен Ideco NGFW Novum версии 23, перейти из Ideco Center можно только в веб-интерфейс **Системного контекста**.
>
> Прямой переход в веб-интерфейс VCE в этом случае невозможен и выполняется только через веб-интерфейс **Системного контекста**.

> При потере связи с Ideco Center синхронизированная конфигурация сохраняется на Ideco NGFW и продолжает применяться.

Работа с группами серверов Ideco NGFW

Структура групп серверов в Ideco Center предполагает три уровня вложенности. Первый - **Корневая группа**. Серверы NGFW, подключенные к Ideco Center, и группы, созданные в Ideco Center, являются частью **Корневой группы** и не могут быть вынесены оттуда.

При этом на Ideco NGFW будут распространяться правила и политики безопасности всех вышестоящих групп в соответствии с вложенностью.

Создание группы серверов

1. В разделе **Серверы** нажмите **Добавить группу**:

2. Укажите **Название группы** и выберите родительскую группу из раскрывающегося списка (если это первая создаваемая группа, в списке будет только **Корневая группа**):

3. Нажмите **Сохранить**.

Редактирование группы серверов

1. Нажмите на напротив нужной группы.

2. Отредактируйте название и родительскую группу:

Удаление группы серверов

Чтобы удалить группу серверов, нажмите на . Если в удаленной группе были серверы, то они переместятся в **Корневую группу** (удалить или отредактировать **Корневую группу** нельзя):

Перемещение серверов Ideco NGFW между группами

Чтобы переместить синхронизированный с Ideco Center сервер Ideco NGFW из одной группы в другую:

1. Нажмите на напротив названия группы.

2. Из раскрывающегося списка выберите группу, в которую хотите переместить сервер:

Подключенный к Ideco Center сервер, настройки которого восстановлены из бэкапа другого сервера, не появится в таблице серверов Ideco Center. Возникнет конфликт с донором бэкапа из-за одинакового `cluster_id`.

В случае возникновения такой проблемы обратитесь в Техническую поддержку.

Пользователи

> В разделе настраиваются интеграции Ideco Center с контроллером домена на базе Microsoft Active Directory (AD) и Samba DC.

Интеграция с Microsoft Active Directory/Samba DC

После настройки интеграции в центральной консоли появится возможность работать с учетными записями и группами безопасности AD в разделах Правила трафика и Объекты.

Поддерживаемые контроллеры домена

- Windows Server 2008 (только R2), 2012, 2016, 2019, 2022, 2025.
- Samba DC с версии 4.0.

Для ввода в домен на базе Windows 2025 перейдите в **Управление сервером** → **Терминал** и выполните команду:

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

Особенности интеграции с несколькими контроллерами домена:

- Учетные записи пользователей из разных доменов могут иметь одинаковые логины. При аутентификации пользователь будет точно определен по указанному домену. Если домен не был указан пользователем, будет указан **Каталог по умолчанию**.
- Пользователи всех интеграций отображаются в одном списке.
- Пользователи и группы безопасности будут видны и доступны к выбору в правилах трафика и поиске информации о пользователях AD, со всех интегрированных доменов. Список обновляется каждые 15 минут.

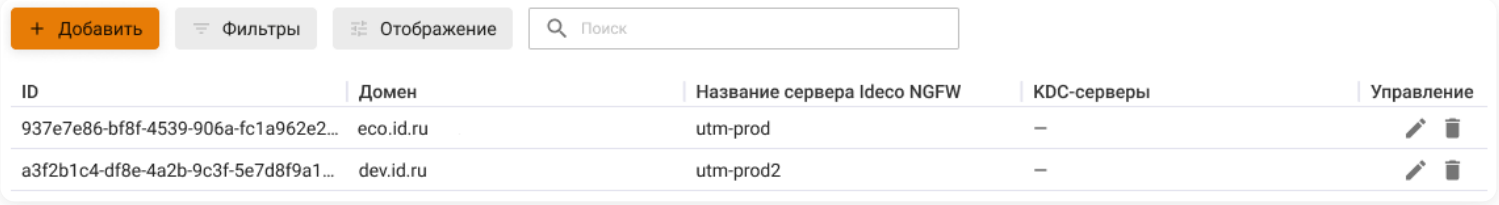
Ввод сервера в домен

Перед вводом в домен:

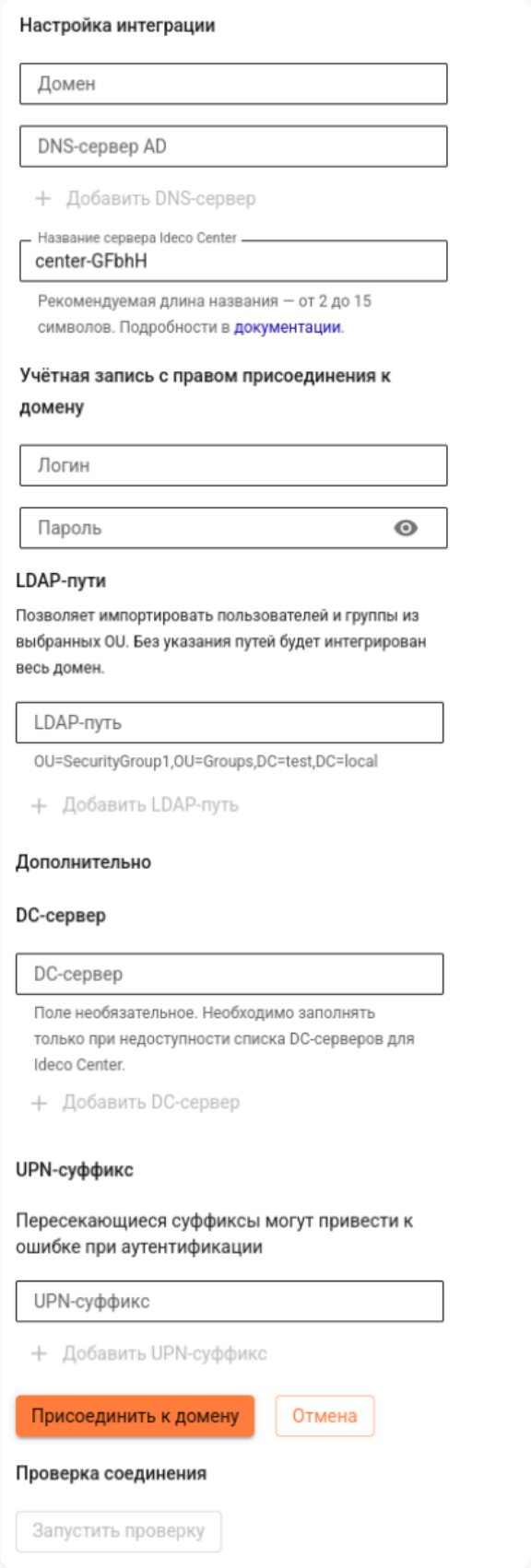
- Убедитесь, что время на контроллере домена и Ideco Center совпадает.
- Убедитесь, что хотя бы один контроллер домена находится в сети Ideco Center или доступен через локальный интерфейс с помощью настроенной маршрутизации.

Выполните действия:

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

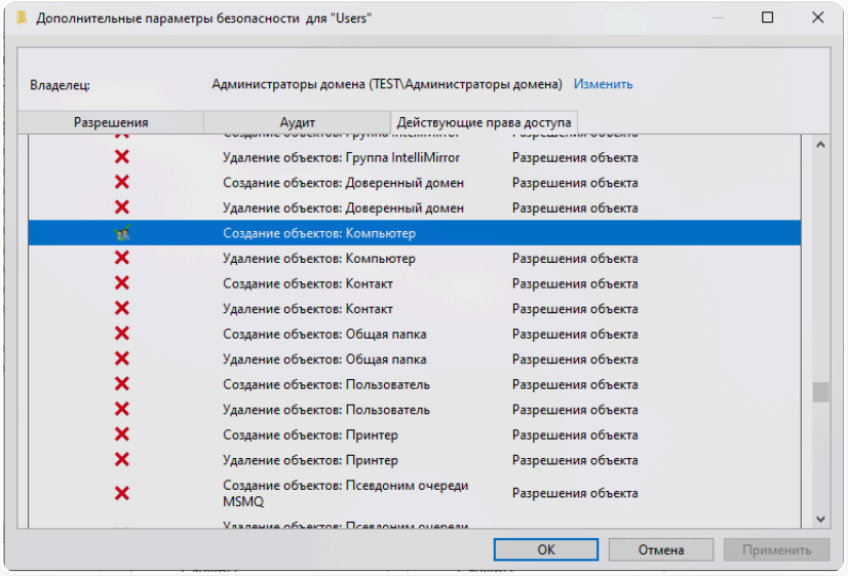


2. Нажмите **Добавить** и заполните поля:



Расшифровка полей

- **Домен** – полное наименование домена, максимальная длина 64 символа. Например: `mydomain.example`.
- **DNS-сервер AD** – адрес сервера с ролью DNS в домене Active Directory. Должен быть доступен с любого интерфейса Ideco Center.
- **Название сервера Ideco Center** – имя компьютера, под которым Ideco Center будет введен в домен. Рекомендуемая длина – от 2 до 15 символов.
- **Учетная запись с правом присоединения к домену** – учетная запись AD с правами присоединения к домену (право **Создание объектов: Компьютер**). Данные учетной записи с правом присоединения к домену не сохраняются на сервере и используются один раз при вводе в домен:



- **LDAP-пути** – LDAP-пути для выбора пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет избежать синхронизации с Center всего дерева пользователей AD и выбрать только нужные группы.
- **DC-сервер** – контроллер домена. Необязательное поле, заполняется только при недоступности списка контроллеров домена для Ideco Center.
- **UPN-суффикс** – альтернативные суффиксы `userPrincipalName`. Указываются, если используются на контроллере домена. Пересекающиеся суффиксы могут привести к ошибке при аутентификации.

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

4. Нажмите **Запустить проверку** в блоке **Проверка соединения**, чтобы убедиться, что контроллер домена доступен с указанными настройками.

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

Мониторинг

В разделе можно настроить интеграцию Ideco Center с модулем SNMP для управления и мониторинга сетевых устройств, получения статистики трафика и/или Zabbix-агентом для детального мониторинга сервера, сбора статистики по ресурсам (CPU, память, диски).

SNMP

SNMP - это протокол для управления и мониторинга сетевых устройств, таких как маршрутизаторы, коммутаторы и межсетевые экраны.

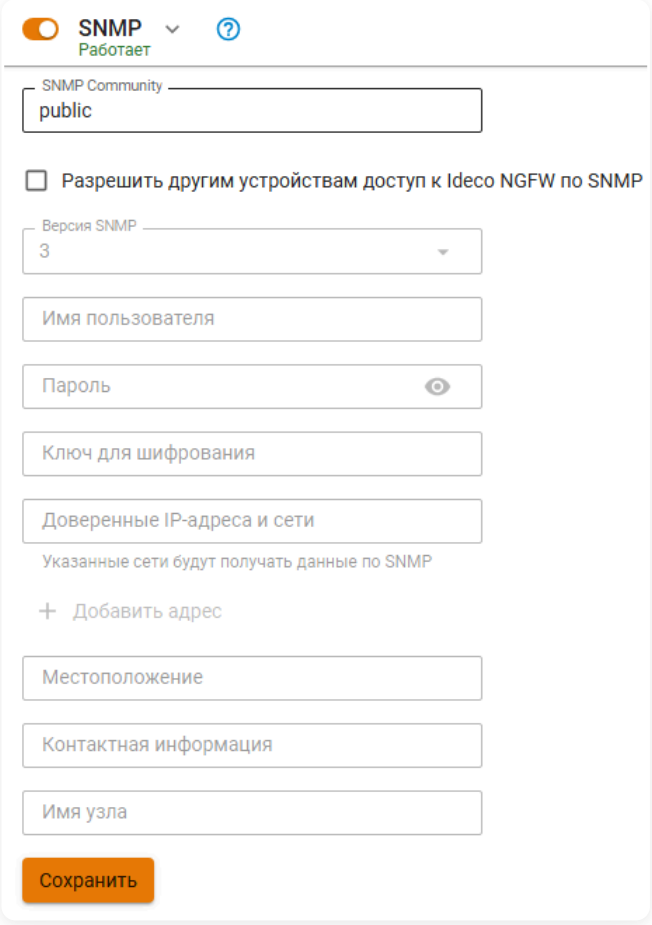
Модуль **SNMP** обеспечивает мониторинг работы Ideco Center по протоколу SNMP версий 1/2c и 3.
С помощью протокола SNMP передается информация:

- Загрузка центрального процессора и оперативной памяти.
- Занятое или свободное место на дисковом хранилище устройства.
- Объемы трафика.

> Для версии SNMPv1/v2 обязательно указывать поле **SNMP community**.
> Для версии SNMPv3 обязательно указывать поле **Имя пользователя** и **Пароль**.
> На сервере, с которым будет осуществляться соединение по SNMPv3, укажите алгоритмы Auth Algorithm MD5 и Crypto Algorithm AES.

Настройка подключения SNMP

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



Версия 1/2c

- **Имя пользователя**.
- **Пароль** (минимальное количество символов - 8).

- **Доверенные IP-адреса и сети**.

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

Версия 3

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

Поля **Местоположение**, **Контактная информация** и **Имя узла** носят информационный характер и необязательны.
Устройства в указанных доверенных сетях получат доступ к данным Ideco Center 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 языке описания SMI (Structure of Management Information). 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:

- По имени объекта (например, `sysUpTime`).
- По числовому OID (например, `.1.3.6.1.2.1.1.3`).

Zabbix-агент

Zabbix - это система мониторинга с открытым исходным кодом, которая контролирует оборудование и состояние сети в режиме реального времени.

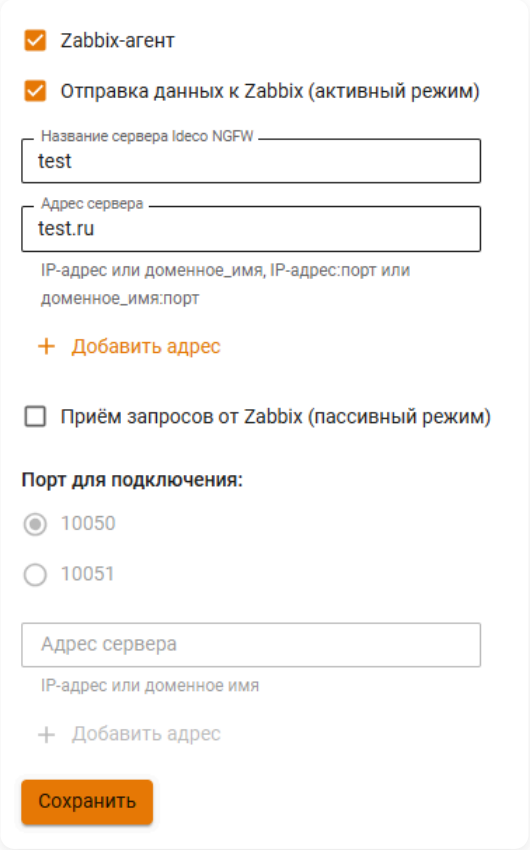
Настройка Zabbix-агента

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

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

Активный

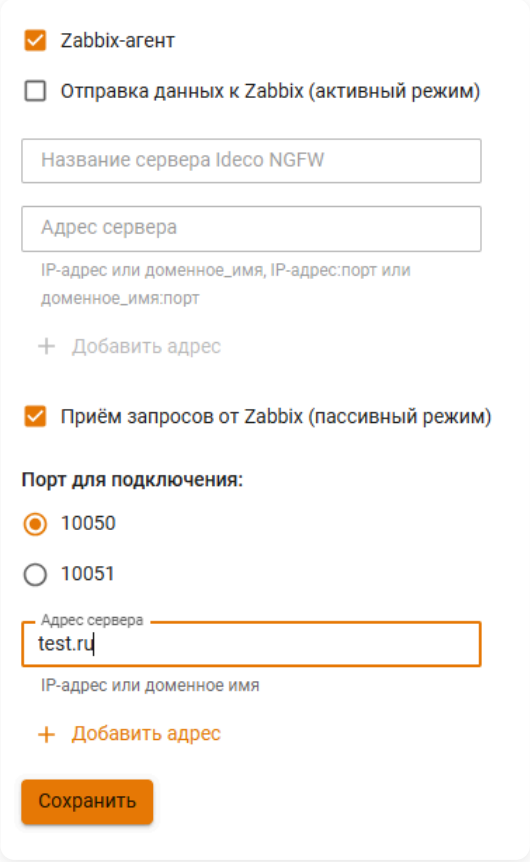
Соединение с Zabbix-сервером происходит со стороны Ideco Center. Для настройки заполните поля:



- **Имя сервера Ideco Center** - 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. Чтобы расширить список адресов, 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. Чтобы расширить список адресов, нажмите **Добавить адрес**.

Zabbix-сервер должен находиться внутри локальной сети Ideco Center. Подключение мониторинга возможно только к локальным интерфейсам (с ролью LAN). Это ограничение обусловлено системными правилами **Межсетевого экрана**, которые не отображаются в веб-интерфейсе, но имеют наивысший приоритет. Системные правила разрешают соединения на порты 10050/TCP и 10051/TCP только на локальных интерфейсах и блокируют их на внешних.

> В качестве шаблонов данных можно использовать стандартные шаблоны для Linux-серверов.

Полезные ссылки

- **Официальная страница Zabbix**
- **Zabbix как готовое решение**
- **Установка Zabbix**

Объекты

Объекты, созданные в Ideco Center, переносятся в подключенные NGFW Novum и VCE VPP. Администратор подключенного сервера может использовать эти объекты для создания правил.

При удалении объекта из Ideco Center, объект также удаляется из подключенных серверов. Если на подключенном сервере было создано правило с удаленным объектом, то этот объект будет отмечен Удалено.

Создание и удаление объектов в Ideco Center аналогично NGFW Novum. Подробнее можно узнать в статье Объекты.

Правила трафика

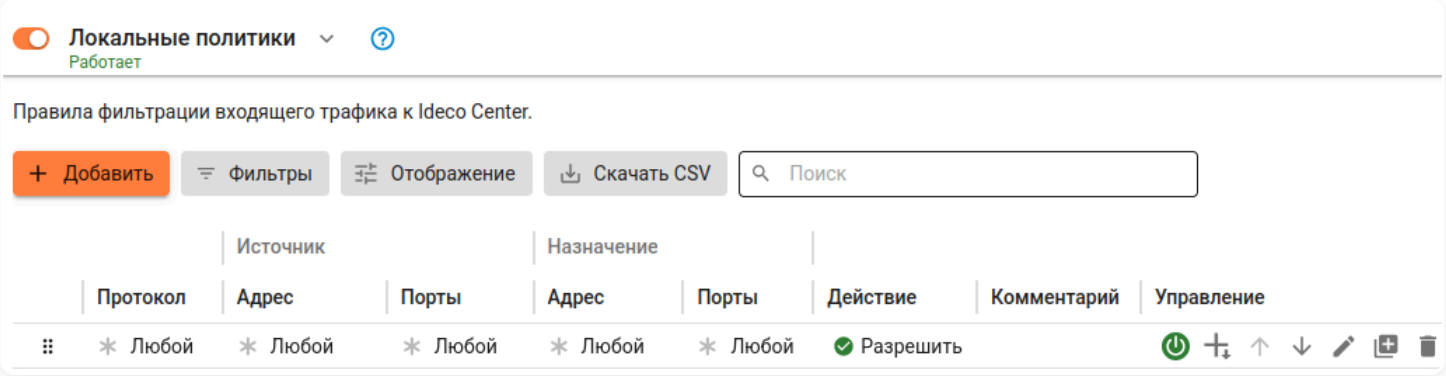
Настройка правил трафика зависит от типа подключенного сервера. Перейдите в раздел:

- Классические VCE (NGFW) - настройка **Межсетевого экрана**, **Контент-фильтра** и **Ограничения скорости**.
- Высокопроизводительные VCE (VPP) - настройка **Межсетевого экрана** и **Ограничения скорости**.

Локальные политики

Документация API

В разделе можно настроить правила фильтрации входящего (INPUT) трафика, направленного непосредственно на сервер Ideco Center:



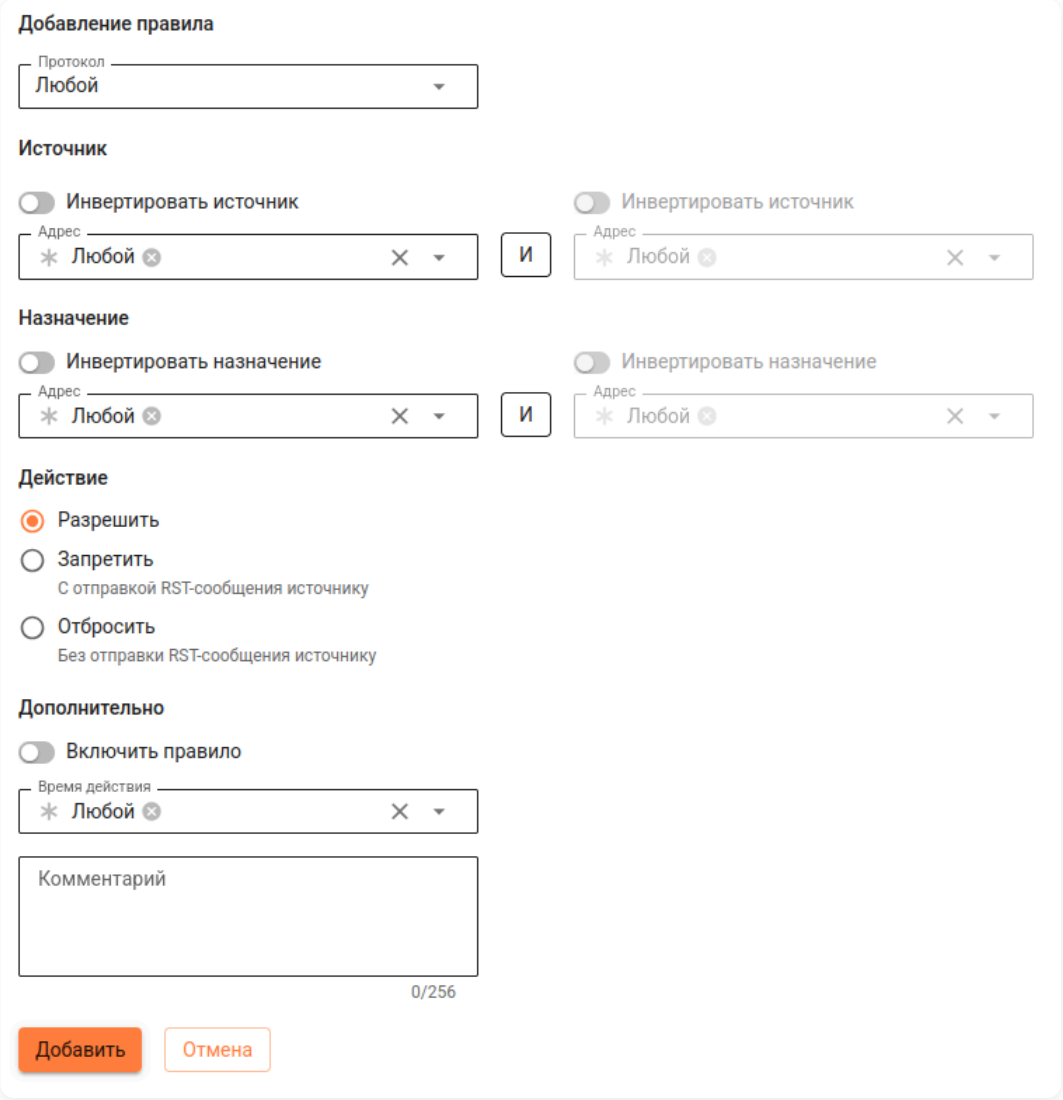
Правила имеют приоритет сверху вниз (то есть **верхнее правило приоритетнее нижнего**).

При наличии большого количества правил воспользуйтесь кнопкой **Фильтры**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

Создание правил

1. Нажмите кнопку **Добавить**.

2. Укажите необходимые параметры и нажмите кнопку **Добавить**:



Расшифровка полей

- **Протокол** - протокол передачи данных. В поле могут быть выбраны типы: AH, ESP, GRE, ICMP, TCP, UDP, TCP/UDP (TCP или UDP) или **Любой**.
- **Источник**:
  - **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес источника трафика. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**) или страны. Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Источнику**.
  - **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.
- **Назначение**:
  - **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в поле **Адрес**.
  - **Адрес** - IP-адрес назначения трафика. В поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел **Объекты**) или страны. Максимальное количество объектов в поле - 200.
  - **Оператор** `И` - позволяет выбрать второе условие для трафика. При выборе второго условия правило срабатывает только в случае, если оба условия соответствуют **Назначению**.
  - **Порт назначения** - указывается при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в **Объектах**. Максимальное количество объектов в поле - 200.
- **Действие**:
  - **Разрешить** - разрешает трафик.
  - **Запретить** - запрещает трафик с отправкой RST-сообщения источнику. Рекомендуем использовать запрет с отправкой RST, так как это позволяет клиенту немедленно завершить попытку соединения, избежать долгих тайм-аутов и облегчает диагностику.
  - **Отбросить** - запрещает трафик без отправки RST-сообщения источнику.
- **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 256 символов.

Правило будет добавлено в конец списка.

Перемещение правил

Способы перемещения правил:

- Воспользуйтесь кнопками ↑ и ↓.
- Переместите правило через модальное окно.

Порядок перемещения

1. Выберите правило, нажав на него.

2. Нажмите в левом нижнем углу **Переместить**.

3. Укажите ID другого правила и выберите, где разместить правило из пункта 1:

- Переместите правило мышью: удерживайте ⠿ и перенесите правило в нужное место.

Классические VCE

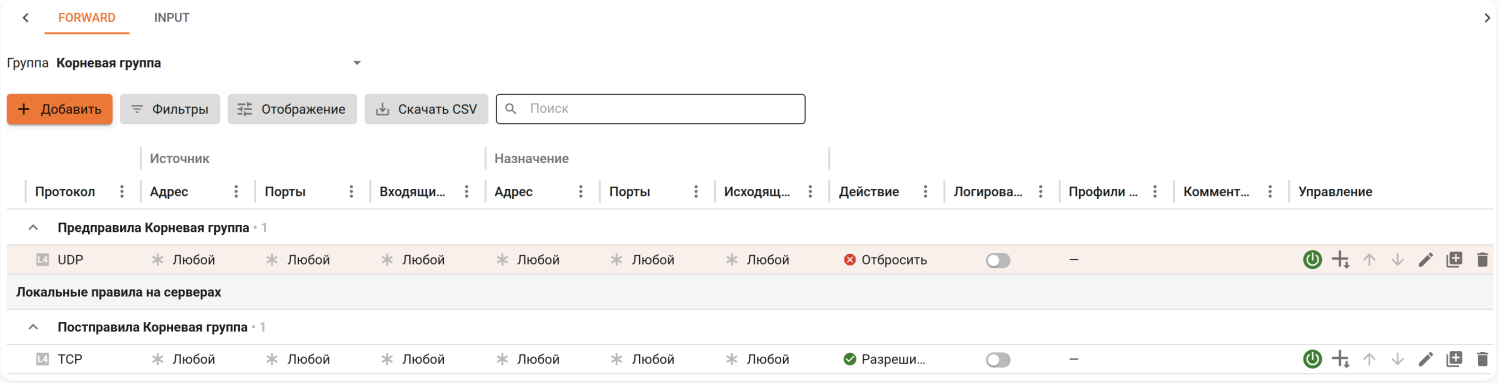
Принципы работы разделов **Межсетевой экран**, **Контент-фильтр** и **Ограничение скорости** с подключенными NGFW Novum идентичны.

Межсетевой экран

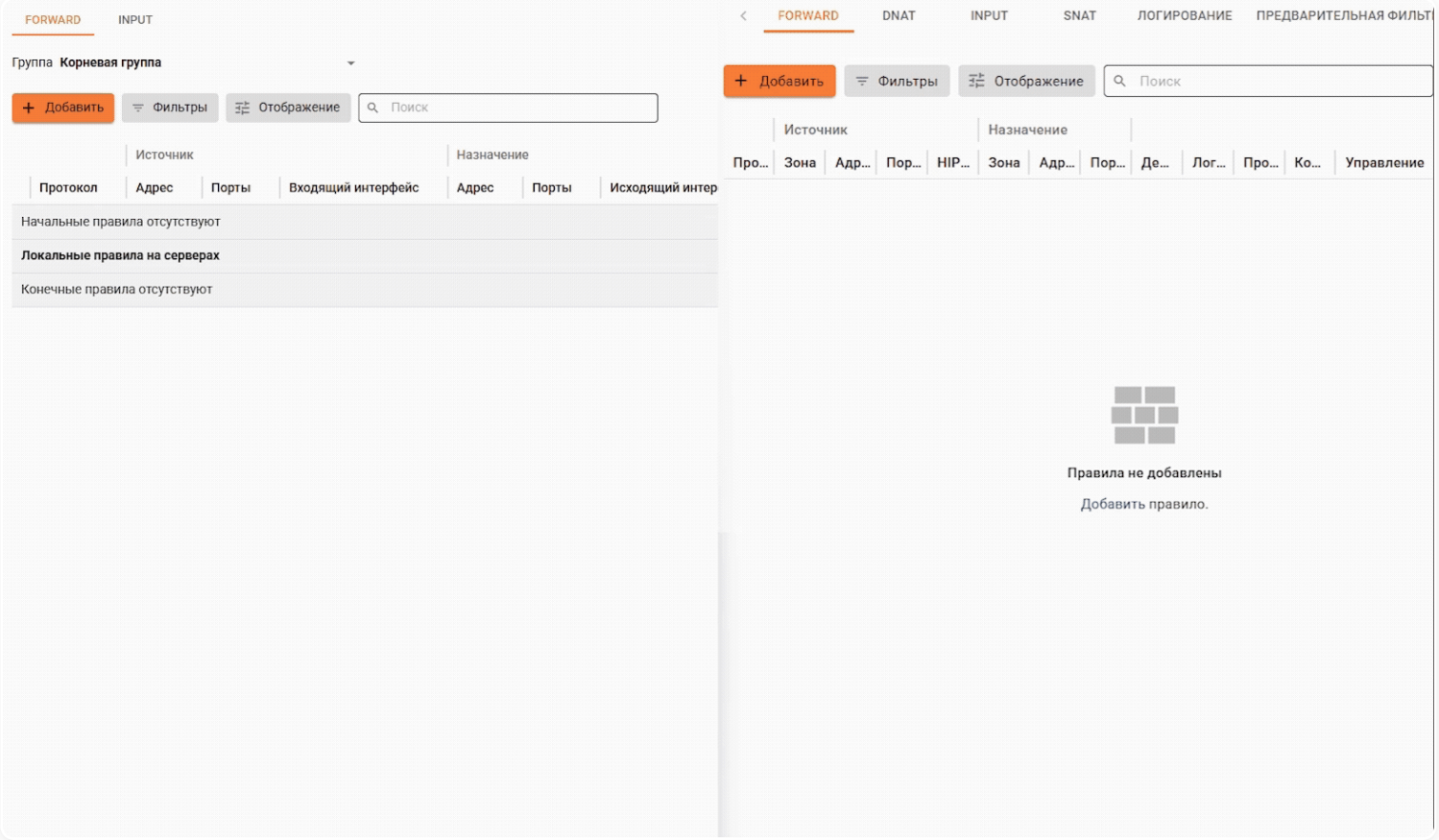
Документация API

Чтобы создать правила для пользователей или групп безопасности Active Directory/Samba DC, предварительно настройте интеграцию в **Пользователи -> Active Directory/Samba DC**.

Межсетевой экран Ideco Center содержит таблицы **FORWARD** и **INPUT**. Правила в них объединены в соответствии с группами серверов:



Пример добавления правил через Ideco Center. Слева - интерфейс Ideco Center, справа - интерфейс NGFW Novum:



В Ideco Center

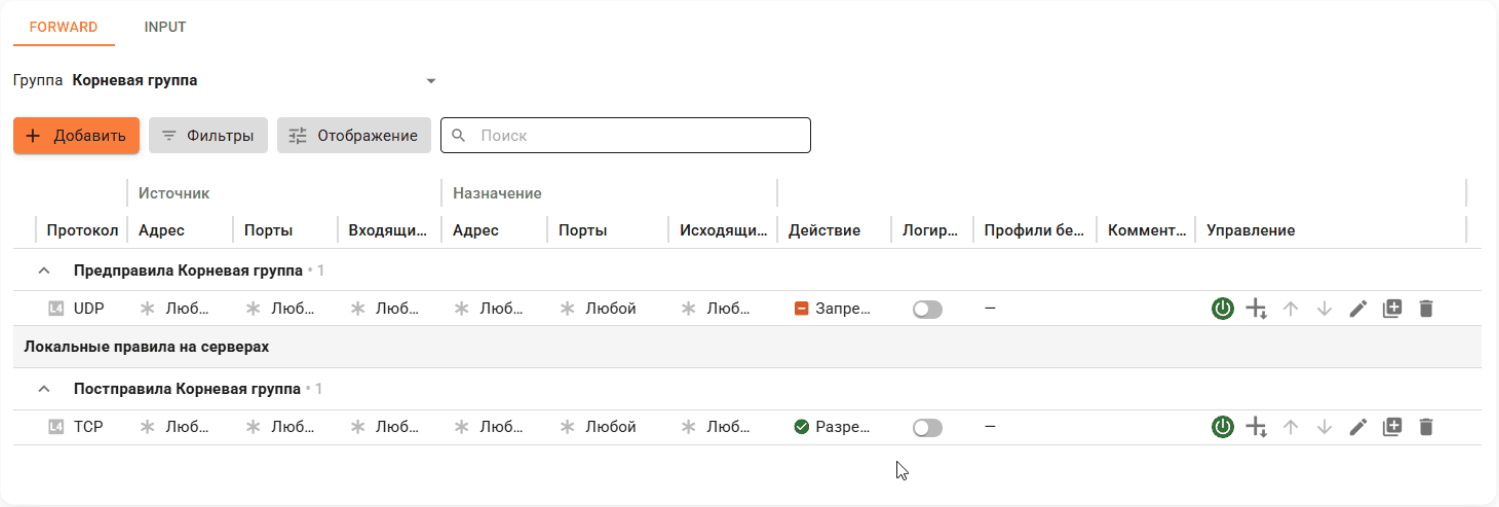
Созданные в Ideco Center правила FORWARD отображаются в виде двух таблиц: **Предправила** и **Постправила**. Правила применяются на подключенных NGFW Novum в следующем порядке: сначала - **Предправила** Ideco Center, затем - **Локальные правила** NGFW Novum, затем - **Постправила** Ideco Center.

Чтобы созданное правило попало в таблицу **Предправила**, укажите в строке **Вид правила** значение **Предправило**. Если правило требуется разместить в таблице **Постправила**, выберите значение **Постправило**.

Предправила и **Постправила** в Ideco Center создаются для определенной группы серверов. Группа указывается при создании правила в строке **Группа серверов**.

Правила можно включать и редактировать только в Ideco Center. В NGFW Novum правила доступны только для просмотра. Перемещать правила между таблицами **Предправила** и **Постправила** нельзя.

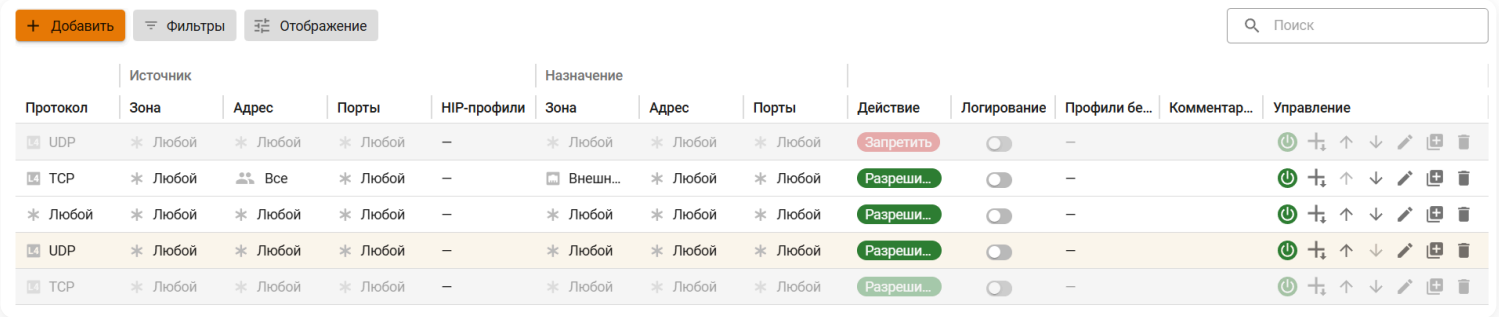
Чтобы увидеть все правила, распространяющиеся на группу серверов, выберите название группы над таблицей:



Чтобы изменить группу серверов, на которую распространяется правило, нажмите на и измените группу в соответствующей строке.

В NGFW Novum

Таблица в NGFW Novum визуально делится на верхнюю, среднюю и нижнюю части:



В верхнюю и нижнюю часть переносятся правила из подключенного Ideco Center. Управление этими правилами в NGFW Novum невозможно. Верхняя часть соответствует таблице **Предправила** в Ideco Center. Нижняя часть - таблице **Постправила**.

В средней части находятся **Локальные правила**, которые создаются администратором в самом NGFW Novum.

> **Локальные правила на серверах NGFW Novum** не видны в интерфейсе Ideco Center.
>
> Для просмотра перейдите в раздел **Серверы**, нажмите на в строке с нужным NGFW Novum и перейдите в раздел **Межсетевой экран**.

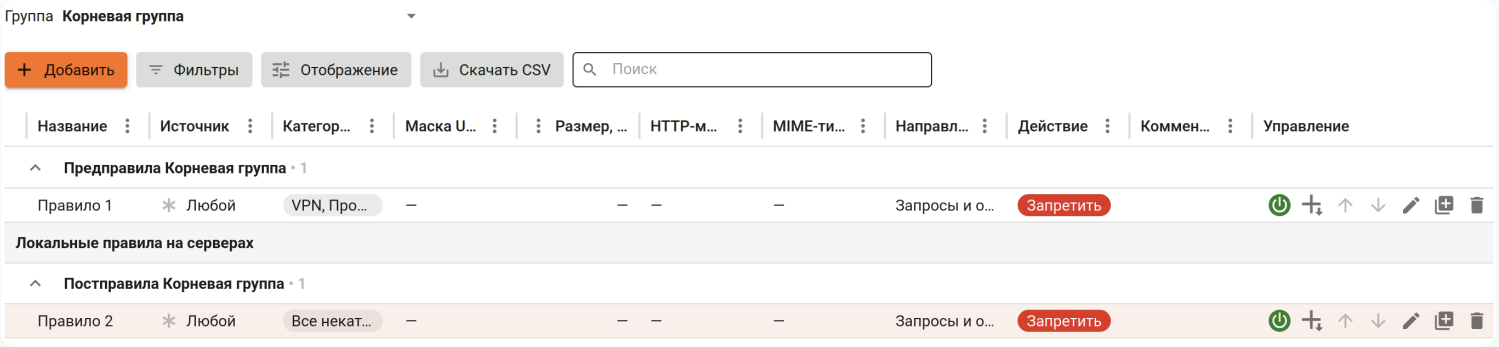
Контент-фильтр

Документация API

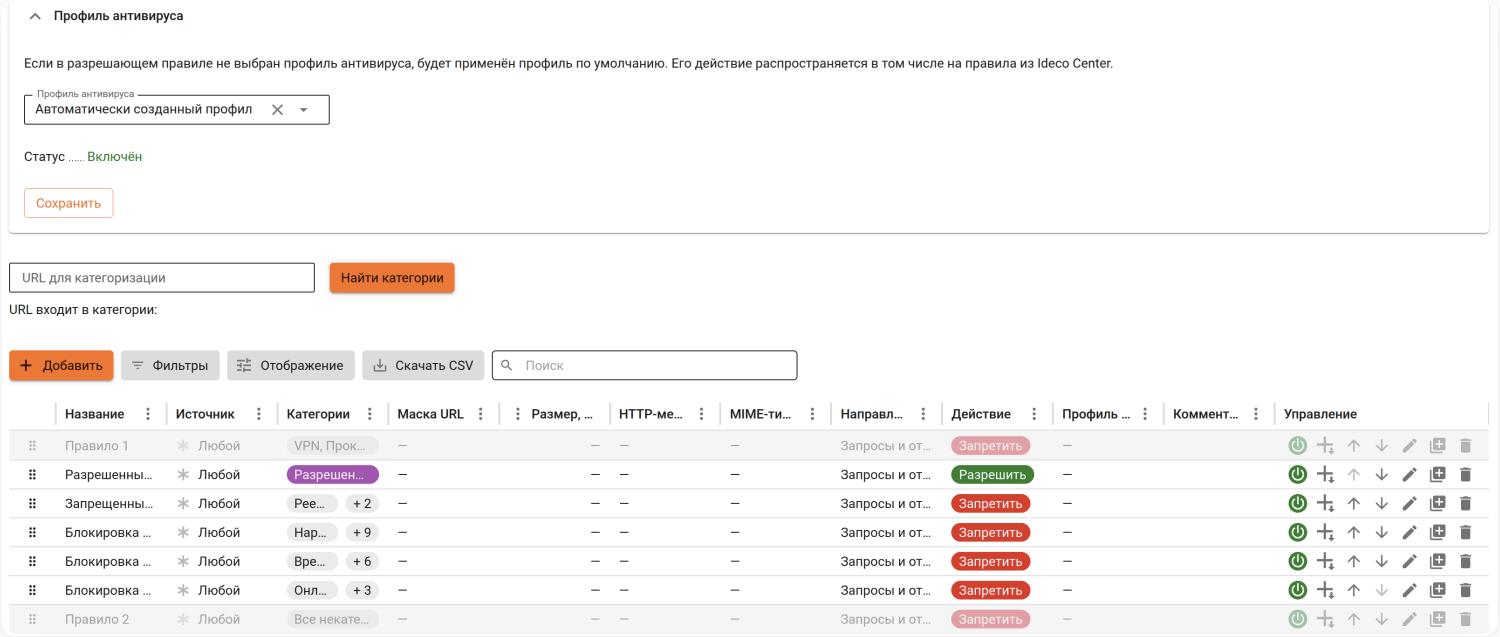
Создание правил в Ideco Center и в NGFW Novum аналогично. Созданные в Ideco Center правила **Контент-фильтра** переносятся в подключенные NGFW Novum в соответствии с группами серверов. Правила можно включать и редактировать только в Ideco Center. В NGFW Novum правила доступны только для просмотра.

Пример правила **Контент-фильтра**:

- В Ideco Center:



- В подключенном NGFW Novum:

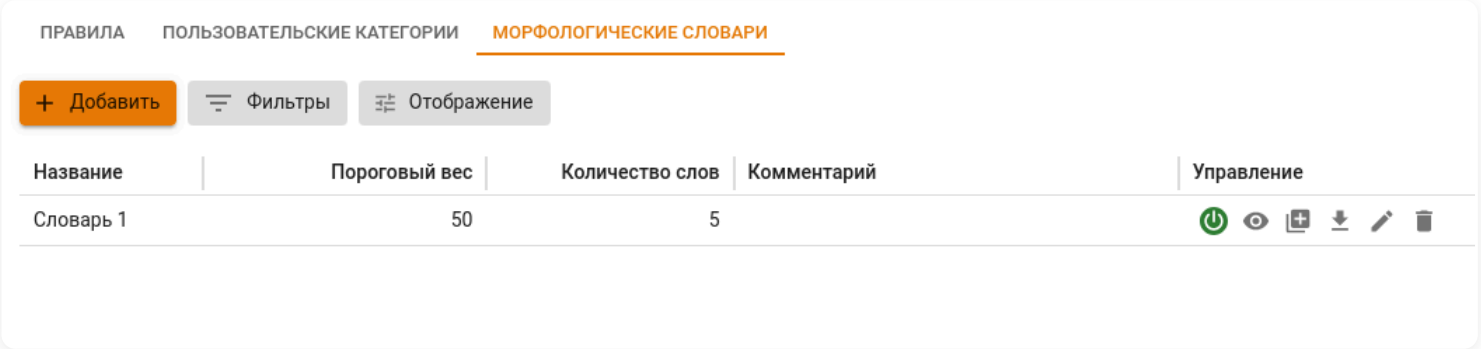


На вкладке **Морфологические словари** создаются и редактируются словари, которые можно использовать для проведения морфологического анализа сайтов в подключенных NGFW Novum. В Ideco Center включить морфологический анализ нельзя. Процессы создания **Морфологических словарей** в Ideco Center и в NGFW Novum аналогичны.

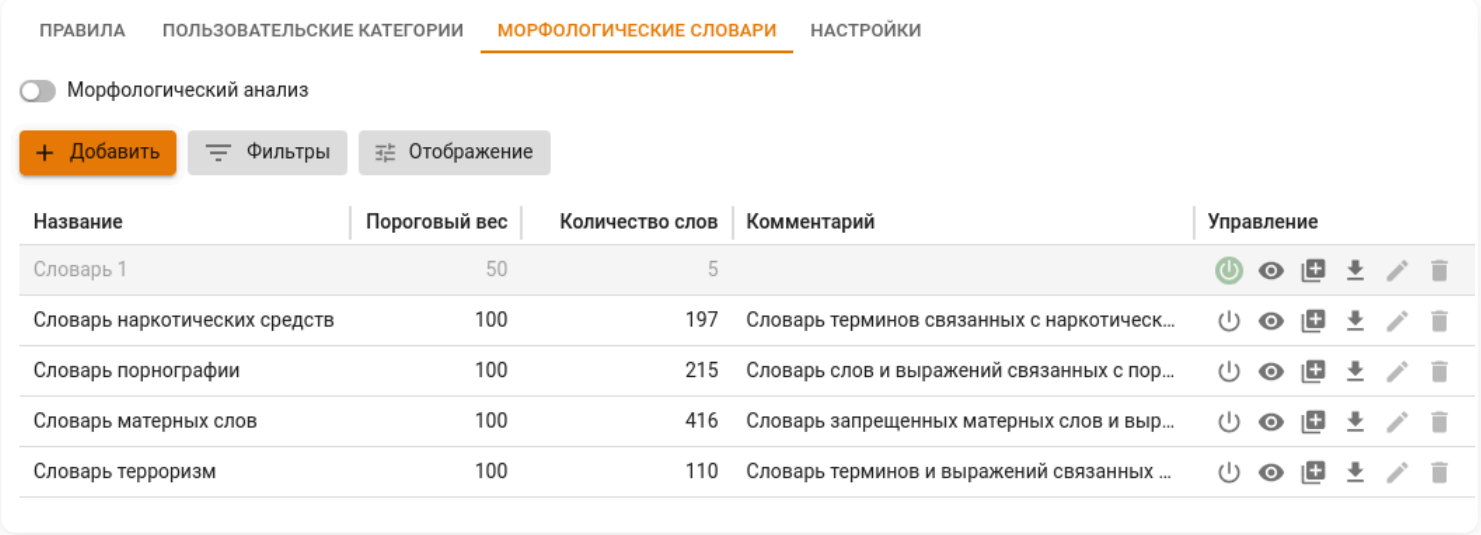
Созданные в Ideco Center **Морфологические словари** можно включать и редактировать только в Ideco Center. В NGFW Novum **Морфологические словари** доступны только для просмотра.

Пример словарей:

- В Ideco Center:



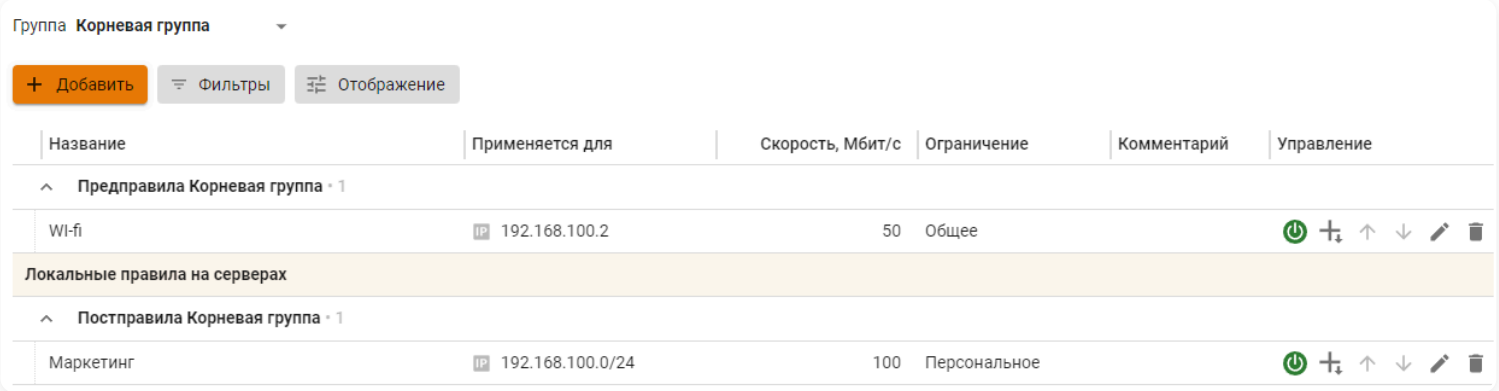
- В подключенном NGFW Novum:



Ограничение скорости

Раздел предназначен для ограничения скорости входящего интернет-трафика пользователей сети.

Процессы создания правил ограничения скорости в Ideco Center и в NGFW Novum аналогичны. Созданные в Ideco Center правила переносятся в подключенные NGFW Novum в соответствии с группами серверов:



Высокопроизводительные VCE

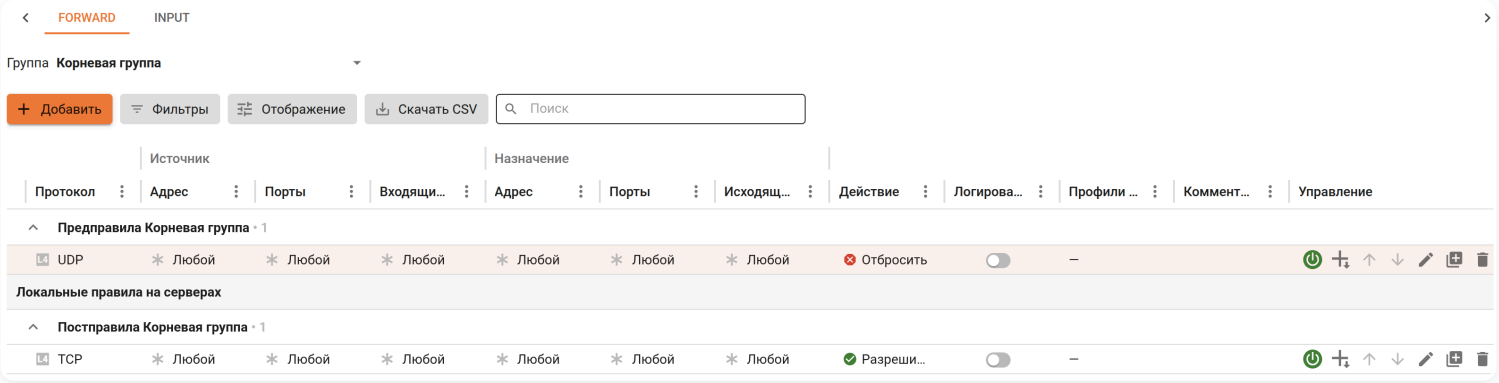
Принципы работы разделов **Межсетевой экран** и **Ограничение скорости** с подключенными VCE VPP идентичны.

Межсетевой экран

Документация API

> Чтобы создать правила для пользователей или групп безопасности Active Directory/Samba DC, предварительно настройте интеграцию в **Пользователи** → **Active Directory/Samba DC**.

Межсетевой экран Ideco Center содержит таблицы **FORWARD** и **INPUT**. Правила в них объединены в соответствии с группами серверов:



В Ideco Center

Созданные в Ideco Center правила FORWARD отображаются в виде двух таблиц: **Предправила** и **Постправила**. Правила применяются на подключенных VCE VPP в следующем порядке: сначала - **Предправила** Ideco Center, затем - **Локальные правила** VCE VPP, затем - **Постправила** Ideco Center.

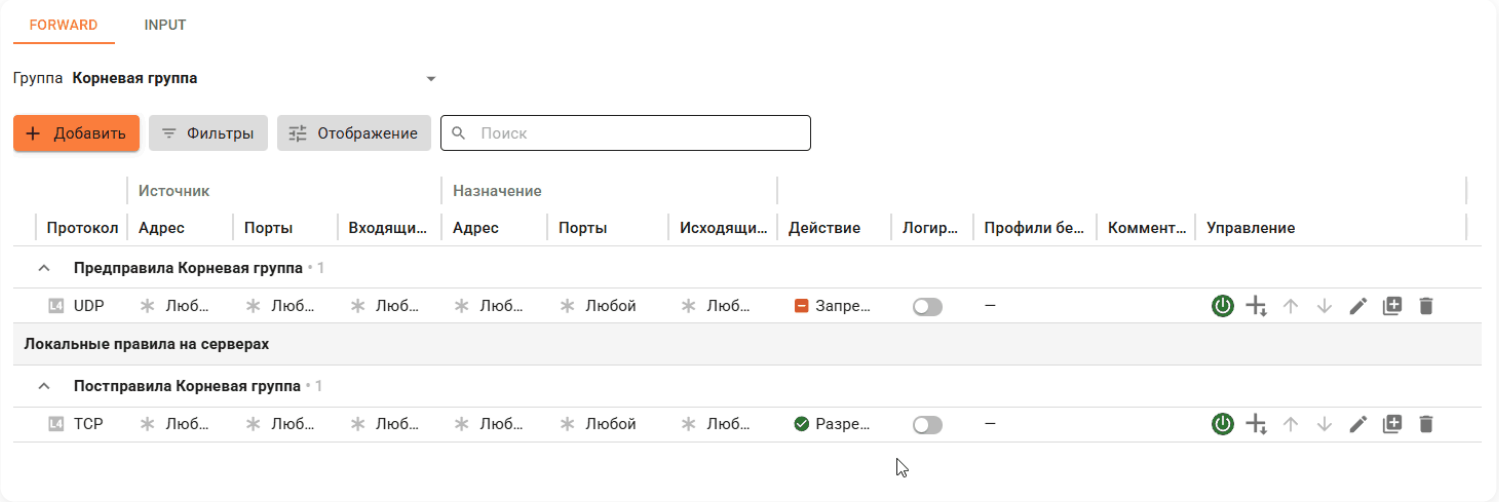
Чтобы созданное правило попало в таблицу **Предправила**, укажите в строке **Вид правила** значение **Предправило**. Если правило требуется разместить в таблице **Постправила**, выберите значение **Постправило**.

Предправила и **Постправила** в Ideco Center создаются для определенной группы серверов. Группа указывается при создании правила в поле **Группа серверов**.

Заполнение остальных полей и работа со значениями в Ideco Center и в VCE VPP идентичны.

Правила можно включать и редактировать только в Ideco Center. В VCE VPP правила доступны только для просмотра. Перемещать правила между таблицами **Предправила** и **Постправила** нельзя.

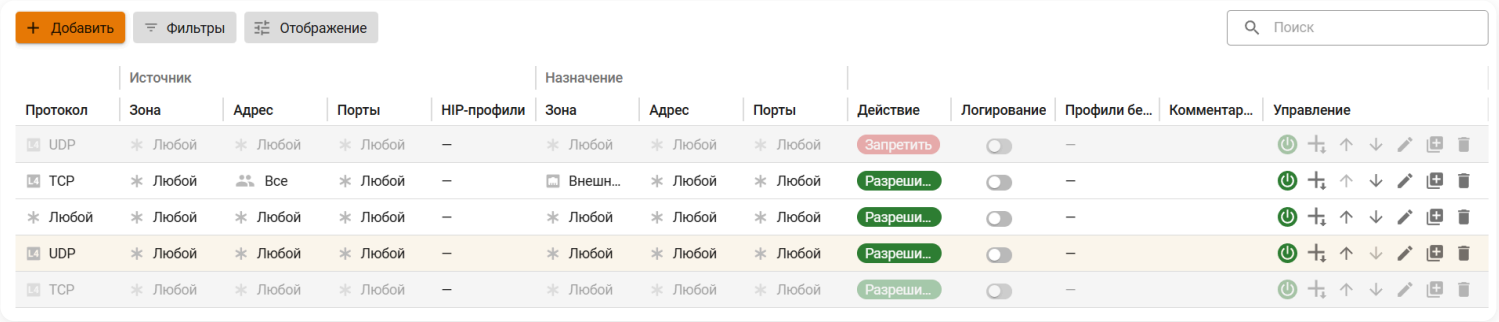
Чтобы увидеть все правила, распространяющиеся на группу серверов, выберите название группы над таблицей:



Чтобы изменить группу серверов, на которую распространяется правило, нажмите на и измените группу в соответствующей строке.

В VCE VPP

Таблица в VCE VPP визуально делится на верхнюю, среднюю и нижнюю части:



В верхнюю и нижнюю часть переносятся правила из подключенного Ideco Center. Управление этими правилами в VCE VPP невозможно. Верхняя часть соответствует таблице **Предправила** в Ideco Center. Нижняя часть - таблице **Постправила**.

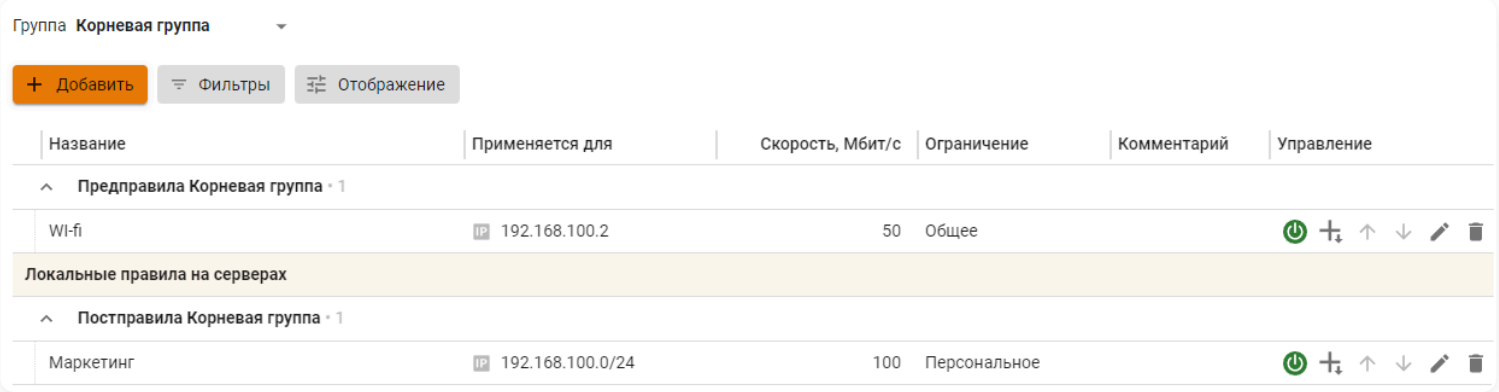
В средней части находятся **Локальные правила**, которые создаются администратором VCE VPP в самом VCE VPP.

> **Локальные правила на серверах VCE VPP** не видны в интерфейсе Ideco Center.
>
> Для просмотра перейдите в раздел **Серверы**, нажмите на в строке с нужным VCE VPP и перейдите в раздел **Межсетевой экран**.

Ограничение скорости

Раздел предназначен для ограничения скорости входящего трафика пользователей сети.

Процессы создания правил ограничения скорости в Ideco Center и в VCE VPP аналогичны. Созданные в Ideco Center правила переносятся в подключенные VCE VPP в соответствии с группами серверов:



Профили безопасности

Профили безопасности - это набор параметров, которые используются для настройки фильтрации трафика различными модулями. Они позволяют независимо друг от друга устанавливать различные политики безопасности и управлять ими, адаптируя под конкретные требования и задачи.

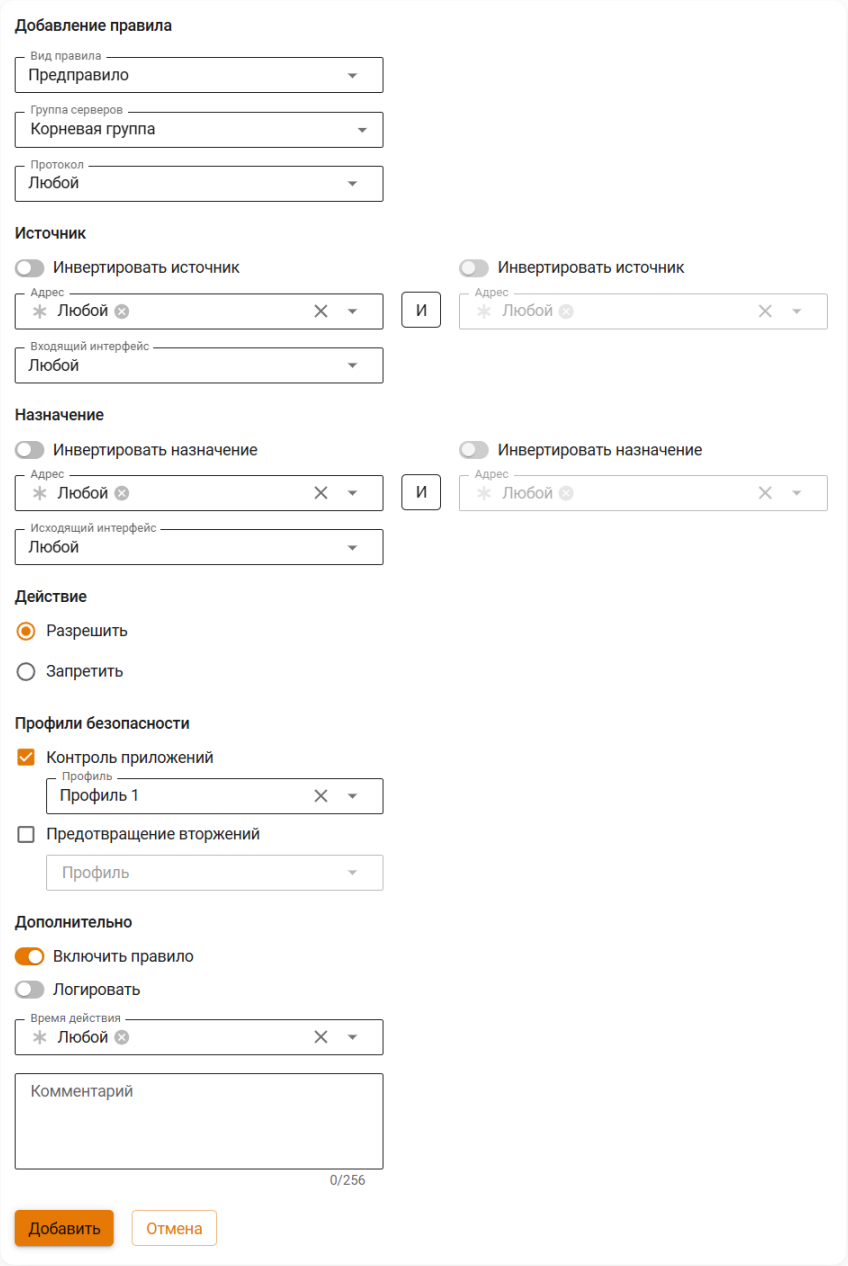
В Ideco Center можно управлять профилями безопасности для всех подключенных Ideco NGFW Novum.

Настройка профиля безопасности зависит от типа подключенного сервера. Перейдите в раздел:

- Классические VCE (NGFW Novum) - настройка профилей **Контроля приложений**, **Предотвращения вторжений** и **Web Application Firewall**.
- Высокопроизводительные VCE (VCE VPP) - настройка профилей **Контроля приложений**, **Предотвращения вторжений** и **Контент-фильтра**.

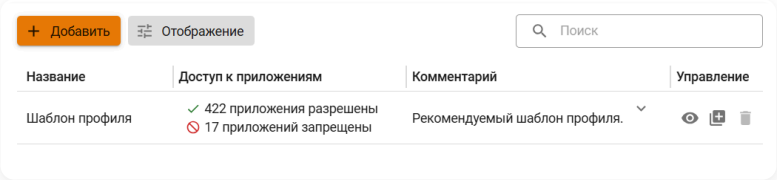
Классические VCE

Созданные в Ideco Center профили **Контроля приложений** и **Предотвращения вторжений** доступны при создании правил Межсетевого экрана:



Контроль приложений

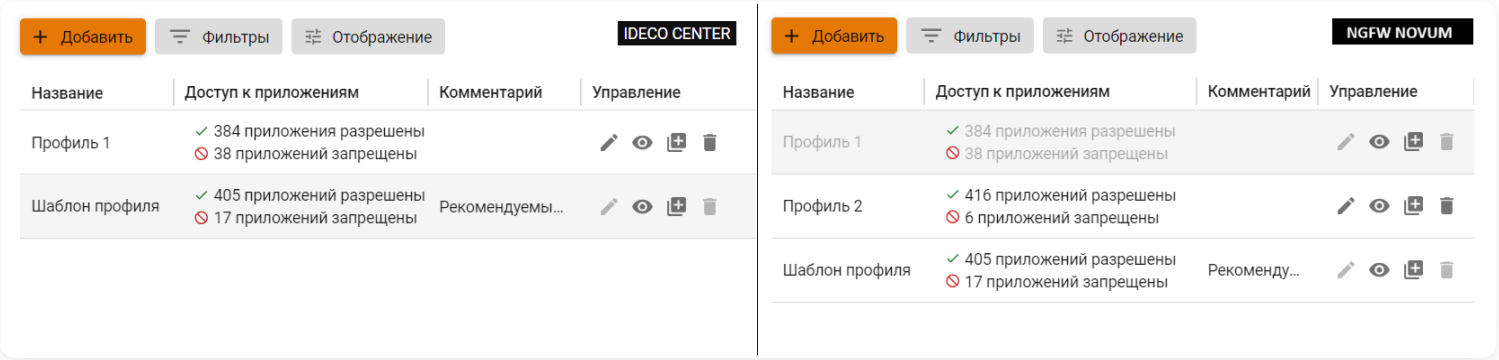
В **Профили безопасности** → **Контроль приложений** создаются профили, которые определяют, разрешен ли пользователю доступ к выбранным приложениям и протоколам:



Для определения протоколов приложений используется глубокий анализ трафика (Deep Packet Inspection - DPI).

Принцип создания и настройки профилей в Ideco Center соответствует принципам NGFW Novum. Подробное описание в статье Контроль приложений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе NGFW Novum доступен только для просмотра:

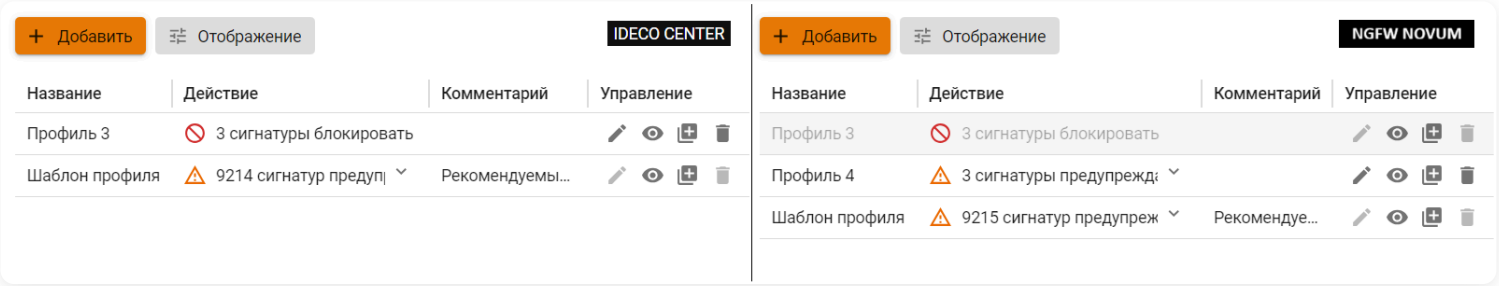


Предотвращение вторжений

В **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые подключенные NGFW будут применять к трафику, соответствующему этим сигнатурам.

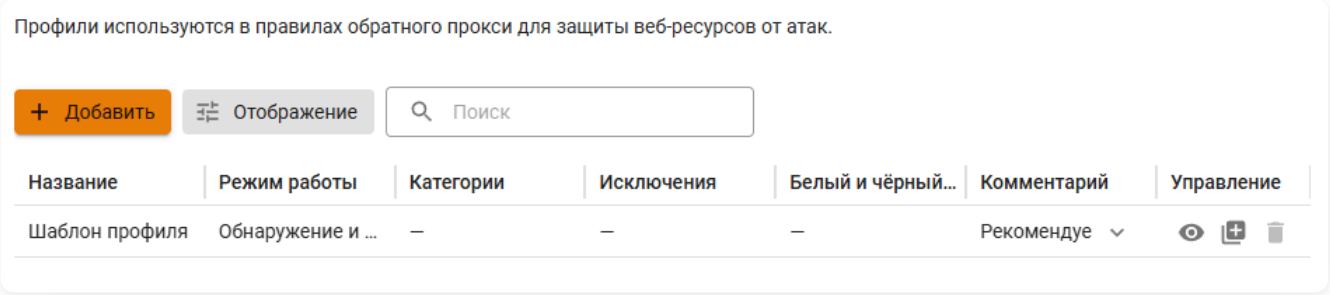
Принцип создания и использования профилей **Предотвращения вторжений** в Ideco Center аналогичен NGFW Novum. Подробнее можно узнать в статье Предотвращение вторжений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе NGFW Novum доступен только для просмотра:



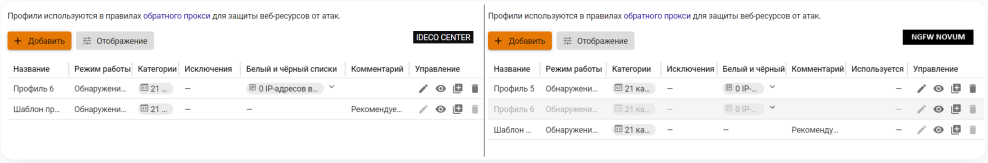
Web Application Firewall

Использование WAF-профилей позволит настроить параметры защиты для опубликованных веб-ресурсов. Профиль создается в **Профили безопасности** → **Web Application Firewall** и применяется в разделе Обратный прокси подключенного NGFW Novum:



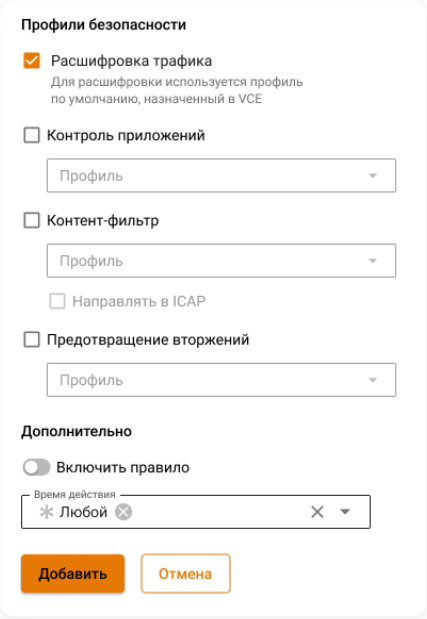
Принцип создания и использования профилей **Web Application Firewall** в Ideco Center аналогичен NGFW Novum. Подробнее можно узнать в статье Web Application Firewall.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе NGFW Novum доступен только для просмотра:



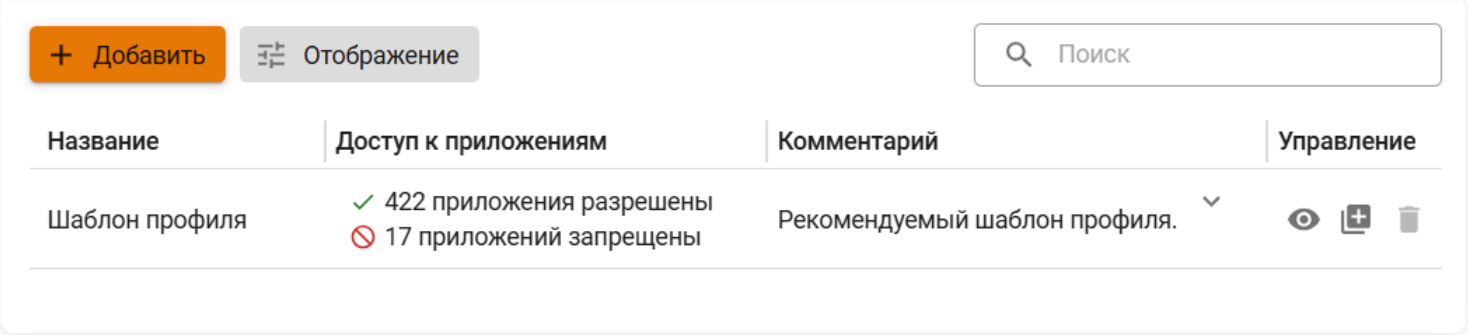
Высокопроизводительные VCE

Созданные в Ideco Center профили доступны при создании правил Межсетевого экрана:



Контроль приложений

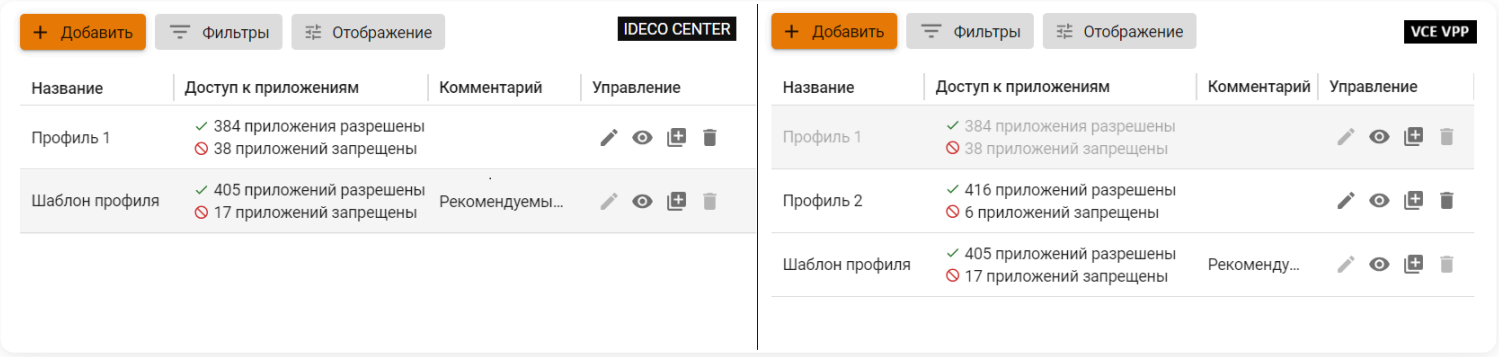
В **Профили безопасности** → **Контроль приложений** создаются профили, которые определяют, разрешен ли пользователю доступ к выбранным приложениям и протоколам:



Для определения протоколов приложений используется глубокий анализ трафика (Deep Packet Inspection - DPI).

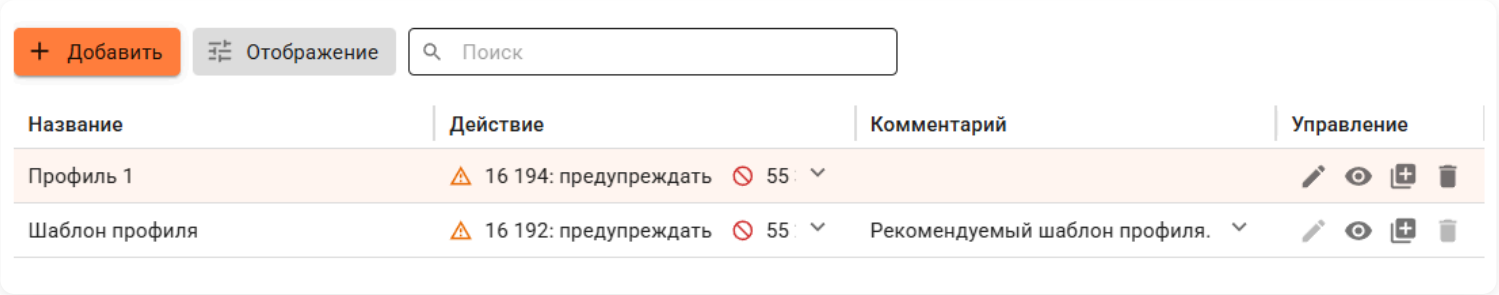
Принцип создания и настройки профилей в Ideco Center соответствует принципам VCE VPP. Подробное описание в статье Контроль приложений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе VCE VPP доступен только для просмотра:



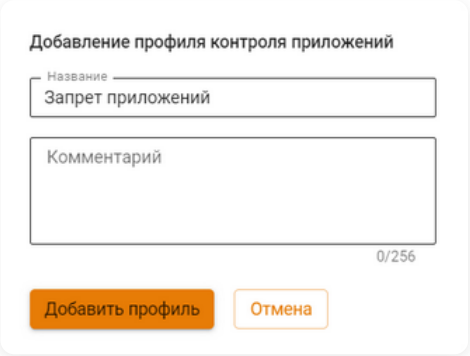
Предотвращение вторжений

В **Профили безопасности** → **Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые синхронизированные Ideco NGFW Novum применяют к трафику, соответствующему этим сигнатурам:



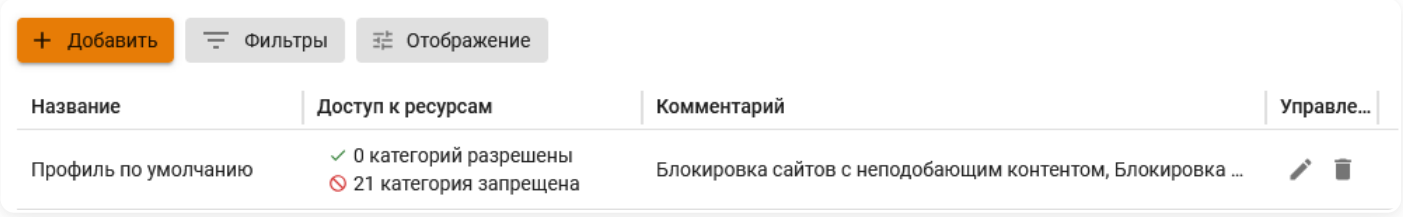
Принцип создания и использования профилей **Предотвращения вторжений** в Ideco Center аналогичен VCE VPP. Подробнее можно узнать в статье Предотвращение вторжений.

Созданный в Ideco Center профиль можно редактировать только в Ideco Center, в интерфейсе VCE VPP доступен только для просмотра:



Контент-фильтр

В **Профили безопасности** → **Контент-фильтр** создаются профили для ограничения пользователям доступа к интернет-ресурсам:



Чтобы трафик фильтровался модулем **Контент-фильтр**, создайте для локальных интерфейсов правило **FORWARD**, содержащее нужный профиль **Контент-фильтра** и включите в правиле опцию **Расшифровка трафика**. Опция использует профиль **TLS/SSL-инспекции** по умолчанию, назначенный в каждом подключенном VCE VPP.

Принцип создания и использования профилей **Контент-фильтр** в Ideco Center аналогичен VCE VPP. Подробнее можно узнать в статье Контент-фильтр.

Сервисы

Сетевые интерфейсы

При установке Ideco Center создается локальный интерфейс, через который происходит управление сервером. В отличие от Ideco NGFW Novum, в веб-интерфейсе Ideco Center можно создавать только внешние Ethernet-интерфейсы для выхода Ideco Center в интернет.

При обновлении Ideco Center с версии 21 на версию 22 роли всех сетевых интерфейсов, созданных через локальное меню, автоматически изменяются на **Control Plane**. Исключение: Loopback-интерфейсы, у которых роль остается **LAN**.

С версии 22 выбор роли интерфейсов на Ideco Center недоступен.

Для детального ознакомления с работой сетевых интерфейсов воспользуйтесь статьями:

- Физические порты
- Интерфейсы

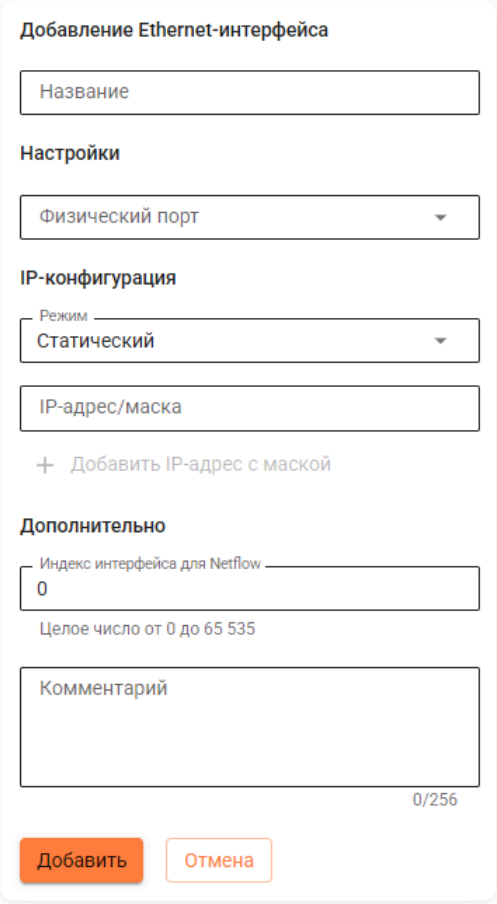
Ethernet

Ethernet - базовая технология проводных сетей, обеспечивающая передачу данных между устройствами. Технология поддерживает как прямое соединение устройств, так и работу через коммутаторы, обеспечивая гибкость и масштабируемость сетевой инфраструктуры.

Для настройки Ethernet-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Ethernet**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.
- **Физический порт** - порт на сетевом адаптере, который используется в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

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

VLAN

VLAN (Virtual Local Area Network) - виртуальный сетевой интерфейс, позволяющий создавать логические сегменты сети поверх существующей физической инфраструктуры и управлять ими. Данная технология дает возможность эффективно разделять сетевой трафик и организовывать изолированные сетевые сегменты в рамках единой сетевой структуры.

VLAN-интерфейс создается поверх родительского Ethernet-интерфейса и помечает все исходящие пакеты соответствующим тегом.

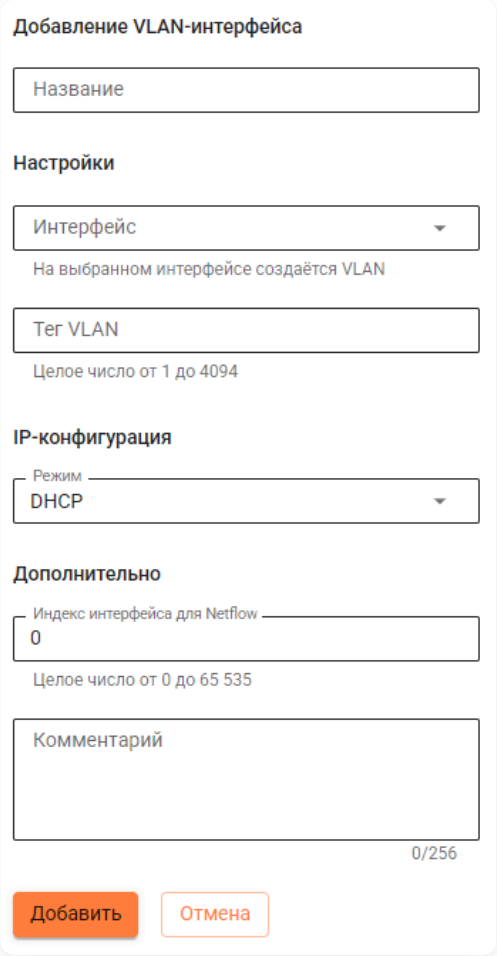
Для настройки VLAN-интерфейса выполните действия:

1. Создайте родительский Ethernet-интерфейс, если его еще нет.

> Если через физический порт должен передаваться только тегированный трафик VLAN, при настройке родительского интерфейса выберите режим **Без конфигурации**.

2. Нажмите **Добавить** и выберите **VLAN**.

3. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.

- **Интерфейс** - родительский Ethernet-интерфейс, на базе которого создается VLAN-интерфейс.
- **Тег VLAN** - числовой идентификатор VLAN (от 1 до 4094), которым помечаются все пакеты VLAN-интерфейса.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Без конфигурации** - настройка, при которой не выдаются IP-адреса.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

4. Нажмите **Добавить**. VLAN-интерфейс появится в таблице интерфейсов.

LACP

LACP (Link Aggregation Control Protocol) - протокол агрегации каналов, предназначенный для объединения нескольких физических портов в единый логический интерфейс. Основное применение LACP заключается в увеличении общей пропускной способности канала и обеспечении отказоустойчивости сетевой инфраструктуры.

> Не рекомендуем использовать **LACP** на виртуальных сетевых адаптерах в Center, так как системы виртуализации часто требуют нетривиальной настройки для работы **LACP** или вообще не поддерживают этот режим. Рекомендуем настраивать агрегацию каналов средствами гипервизора.
>
> Если сетевые карты проброшены в виртуальную машину на уровне PCI (PCI passthrough), **LACP** можно настраивать внутри Center.

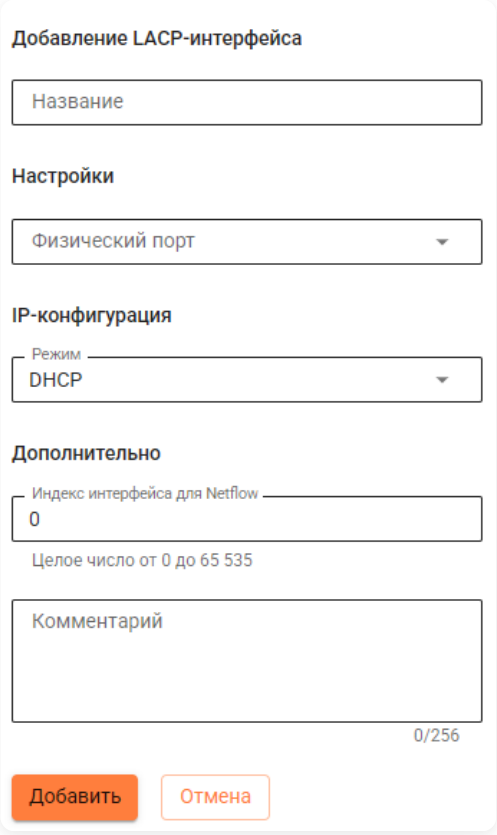
Особенности работы LACP-интерфейсов:

- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active** режим - постоянная рассылка LACP пакетов.
- Проверка соседства осуществляется в режиме **fast** - каждую секунду.
- Количество физических портов, объединяемых в агрегированный интерфейс, не ограничено со стороны Center, но также зависит от конфигурации аппаратных решений и организации сети.

Чтобы объединить несколько физических портов в один агрегированный LACP-интерфейс, выполните действия:

1. Нажмите **Добавить** и выберите **LACP**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.
- **Физический порт** - порт на сетевом адаптере, который используется в созданном интерфейсе.
- **Режим** - режим настройки IP-конфигурации:
  - **DHCP** - автоматическая настройка IP-адреса устройством при подключении к сети.
  - **Статический** - ручная настройка IP-адреса, который остается неизменным:
    - **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

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

Loopback

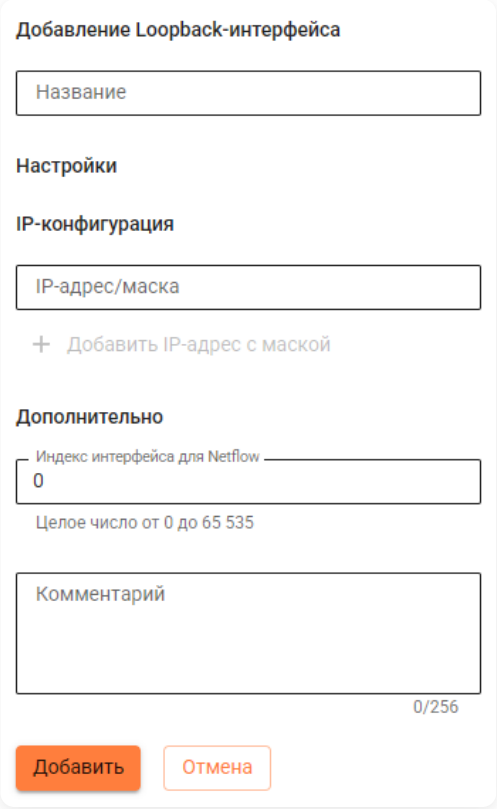
Loopback - виртуальный интерфейс, не привязанный к физическому сетевому порту. Основная задача Loopback-интерфейса - обеспечение стабильного IP-адреса для устройства, который остается доступным даже при сбоях физических соединений.

> Нельзя создавать Loopback-интерфейс в настроенном кластере. Если все же требуется использовать Loopback-интерфейс, настройте его до объединения в кластер.

Для настройки Loopback-интерфейса выполните действия:

1. Нажмите **Добавить** и выберите **Loopback**.

2. Заполните поля:



Расшифровка полей

- **Название** - имя для идентификации интерфейса.
- **IP-адрес/маска** - IP-адрес с маской в формате `x.x.x.x/x`, назначаемый на интерфейс.
- **Индекс интерфейса для Netflow** - индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.
- **Комментарий** - произвольный текст. Не более 256 символов.

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

Перенастроить локальный интерфейс в Ideco Center можно через локальное меню.

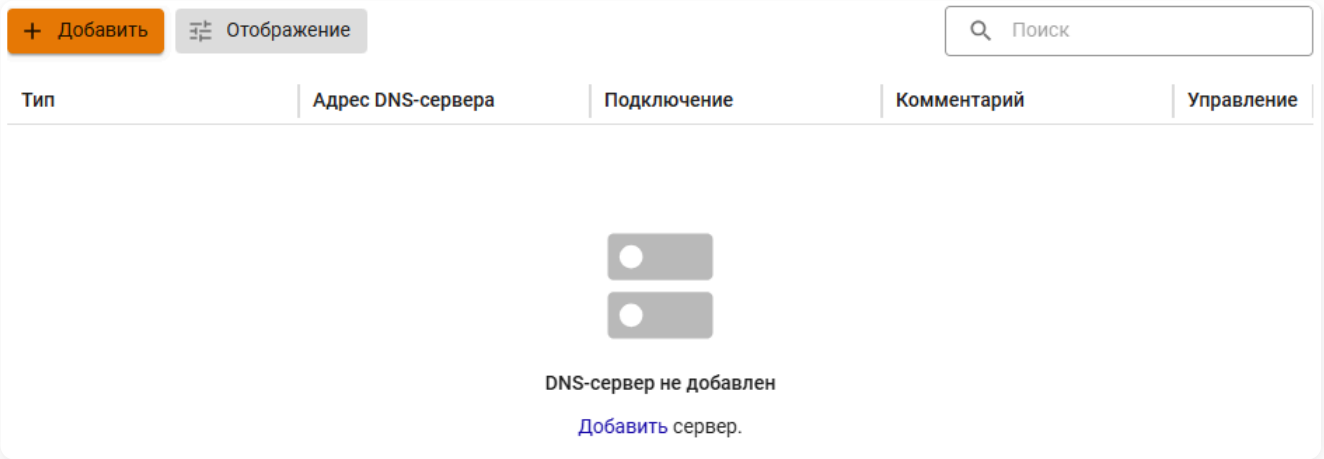
При создании, редактировании или удалении сетевого интерфейса перевыпускается SSL-сертификат, поэтому вероятно снижение скорости работы веб-интерфейса Ideco Center. В этом случае рекомендуем нажать `F5`.

DNS

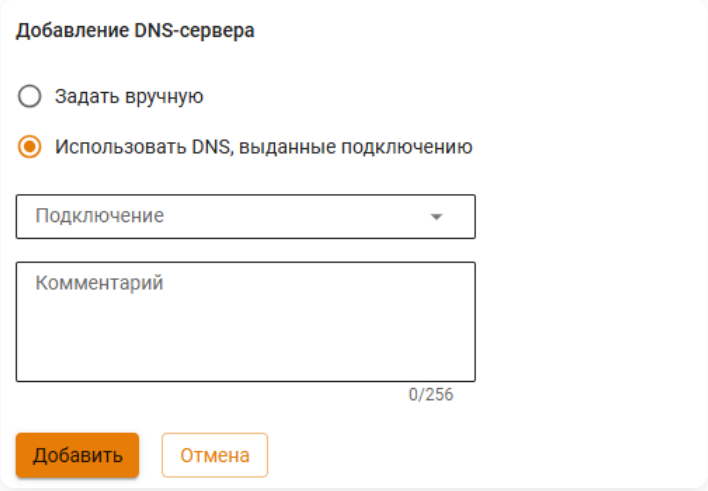
Внешние DNS-серверы

Принцип работы DNS-серверов в Ideco Center аналогичен принципу работы DNS-серверов в Ideco NGFW Novum.

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. Нажмите **Добавить**:



Выберите **Задать вручную** или **Использовать DNS, выданные подключению**, указав нужное подключение:



- Не указывайте `8.8.8.8`, `1.1.1.1` или другие известные DNS-серверы без необходимости.
- По возможности не используйте DNS, выданные интернет-провайдером, так как DNS, выданные интернет-провайдером, превышают TTL и долго отвечают.
- Укажите фильтрующие DNS-серверы, если необходимо (SkyDNS или Яндекс-DNS).
- Не используйте DNS-серверы контроллера домена, даже если домен может самостоятельно разрешать доменные имена в интернете. Это необходимо для эффективного разрешения внутренних имен домена при интеграции с AD. Для резолвинга особых зон, не связанных с AD, создайте Forward-зону вручную.

DDNS

Принцип работы DDNS в Ideco Center аналогичен принципу работы DDNS в Ideco NGFW Novum.

NTP-сервер

Настройка работы NTP-сервера в Ideco Center аналогична настройке NTP-сервера в Ideco NGFW Novum.

Сертификаты

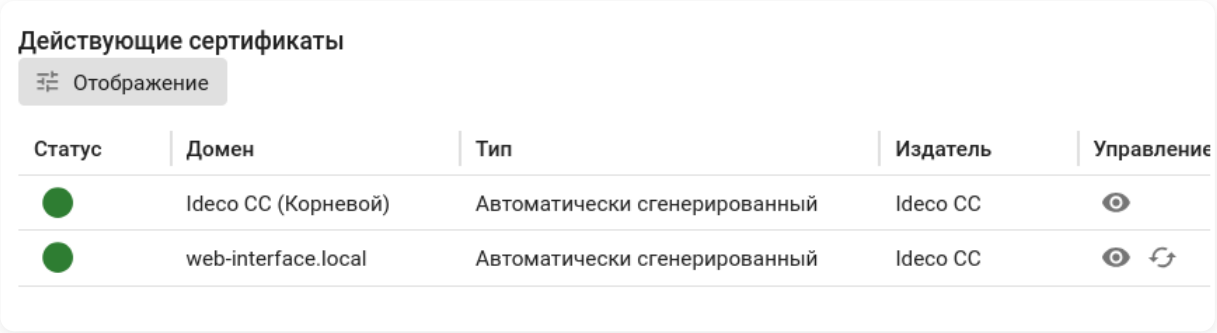
В разделе **Сертификаты** отображаются SSL-сертификаты или цепочки сертификатов, список которых формируется модулями Ideco Center.

Для просмотра основной информации о сертификате нажмите кнопку .

Процессы выпуска и перевыпуска сертификата в Ideco Center и Ideco NGFW Novum одинаковы и описаны в статье.

Действующие сертификаты

В таблице **Действующие сертификаты** отображаются:

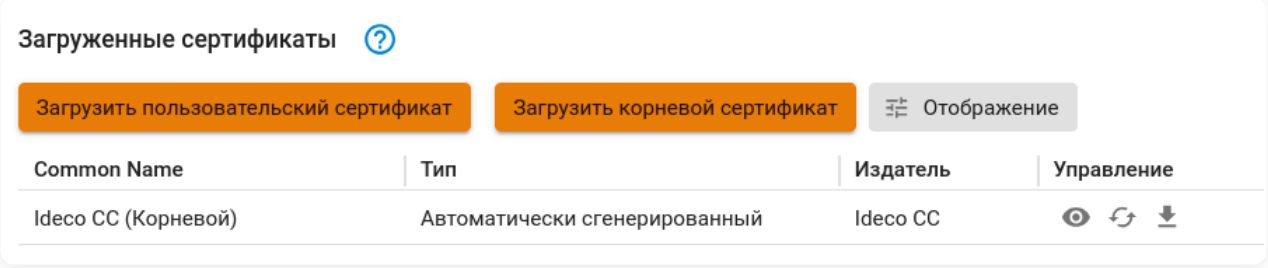


- Автоматически сгенерированные цепочки сертификатов.
- Загруженные цепочки сертификатов, используемые модулями Ideco Center.

> Если в таблице **Действующие сертификаты** одна и та же цепочка сертификатов указана в нескольких строках, то она используется несколькими модулями.

Загруженные сертификаты

В таблице **Загруженные сертификаты** отображаются:



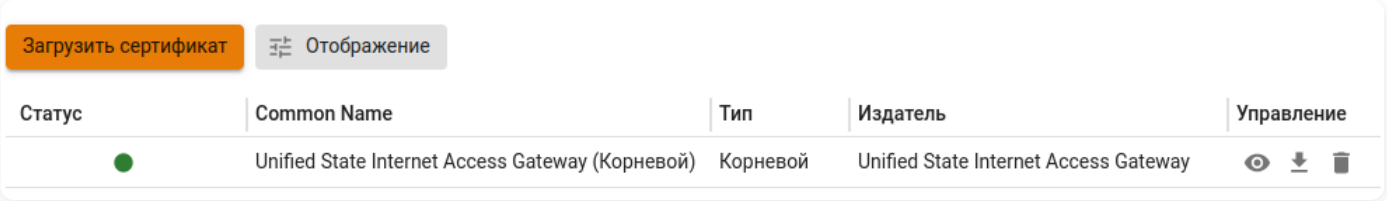
- Все загруженные цепочки сертификатов.
- Корневой сертификат Ideco Center.

> Загрузка SSL-сертификата на Ideco Center аналогична загрузке на Ideco NGFW Novum. Подробная инструкция - в статье.

На Ideco Center можно загрузить самоподписанные сертификаты, созданные в PowerShell.

Системные сертификаты

Раздел позволяет загружать свои сертификаты в хранилище доверенных сертификатов ОС Fedora на Ideco Center. Подробнее о системных сертификатах - по ссылке. После добавления сертификата в таблицу **Системные сертификаты** Ideco Center будет доверять загруженному сертификату и всем сертификатам, подписанным загруженным сертификатом:

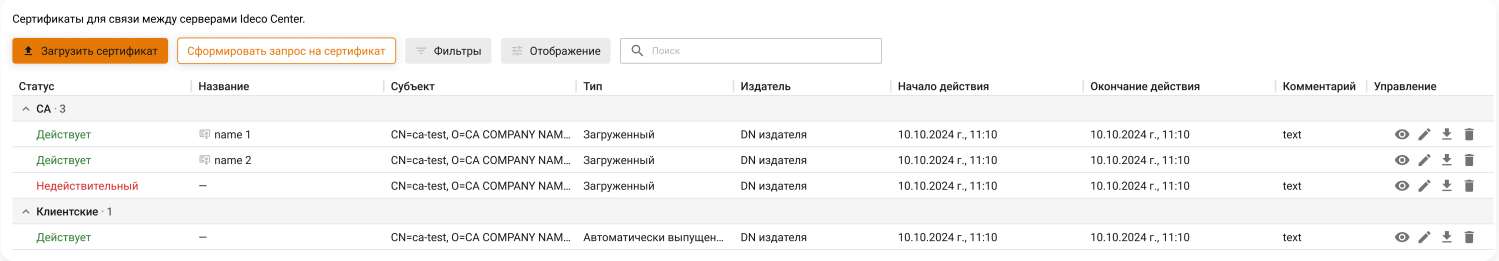


Кластеризация

В таблице **Кластеризация** отображаются сертификаты для взаимной аутентификации нод кластера. Сертификаты из этого раздела выбираются при настройке кластеризации.

Таблица разделена на две группы:

- **CA** - доверенные CA-сертификаты, загруженные вручную. Используются для проверки сертификатов другой ноды.
- **Клиентские** - клиентские сертификаты и запросы на их подпись. Используются при подключении текущей ноды к другой ноде.



Расшифровка столбцов

- **Статус** - текущее состояние сертификата:
  - **Действует** - сертификат действителен.
  - **Истекает** - до окончания срока действия осталось 30 дней или меньше.
  - **Недействительный** - срок действия истек или еще не начался.
  - **Не совпадает доменное имя** - доменное имя в сертификате не совпадает с доменным именем ноды из раздела **Управление сервером** → **Дополнительно**.
- **Название** - название сертификата.
- **Субъект** - DN (Distinguished Name) владельца сертификата.
- **Тип** - способ получения сертификата:
  - **Автоматически выпущенный** - сертификат создается и обновляется системой автоматически. Подписывается внутренним CA ноды.
  - **Загруженный** - готовый сертификат, загруженный вручную пользователем в формате `.pem`.
  - **Запрос на подпись сертификата** - промежуточный статус, когда был сформирован CSR (Certificate Signing Request), но еще не загружен подписанный сертификат. После загрузки подписанного сертификата тип поменяется на **Загруженный**.
- **Издатель** - DN (Distinguished Name) удостоверяющего центра, выпустившего сертификат.
- **Начало действия** - дата и время, с которого сертификат считается действительным.
- **Окончание действия** - дата и время истечения срока действия сертификата.
- **Комментарий** - произвольный текст, добавленный при создании или редактировании записи.
- **Управление** - действие с сертификатом:
  - - просмотр информации.
  - - редактирование названия и комментария.
  - - скачивание.
  - - удаление.

Клиентские сертификаты **CA-сертификаты**

Вкладка 5

Клиентский сертификат нода использует при подключении к другой ноде. Сертификат должен быть выпущен на доменное имя ноды, которое указывается в поле `subject.CommonName` или в расширении `subjectAltName`. Помимо самого сертификата хранится вся цепочка CA-сертификатов до корневого CA. Wildcard-сертификаты в качестве клиентских не поддерживаются.

Доступно три способа получения клиентского сертификата:

Автоматический выпуск сертификата

Автоматически выпущенный сертификат создается и обновляется системой автоматически, если в разделе **Управление сервером** → **Дополнительно** → **Адрес Ideco Center** задано доменное имя ноды. Подписывается внутренним CA ноды. Отображается с типом **Автоматически выпущенный**. Рекомендуемый вариант - дополнительных действий не требуется.

> Если автоматически выпущенный сертификат удалить, система перевыпустит его с тем же идентификатором.

Загрузка сертификата

Загрузка готового клиентского сертификата с приватным ключом и цепочкой CA-сертификатов в формате `.pem`. Для загрузки:

1. Нажмите **Загрузить сертификат** и выберите сохраненный ранее сертификат. При загрузке отобразится превью:

Расшифровка полей

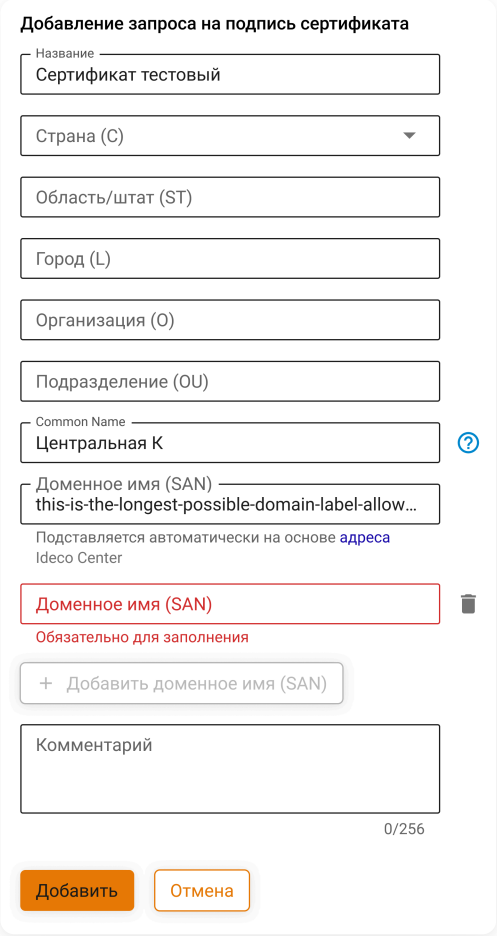
- **Тип** - способ получения сертификата: **Загруженный** или **Автоматически выпущенный**.
- **Субъект** - DN (Distinguished Name) владельца сертификата, содержащий доменное имя ноды.
- **Издатель** - DN удостоверяющего центра, подписавшего сертификат.
- **Вид ключа** - алгоритм криптографического ключа.
- **Срок действия** - период действия сертификата: дата начала и дата окончания.
- **Название** - укажите название сертификата. Обязательное поле.
- **CSR ID** - уникальный идентификатор CSR, на основе которого был выпущен сертификат. Отображается, если сертификат был создан на основе запроса из системы.
- **Комментарий** - произвольный текст.

2. Нажмите **Загрузить**, чтобы добавить сертификат в список.

Формирование запроса на сертификат

Формирование запроса на подпись клиентского сертификата. Для создания запроса:

1. Нажмите **Сформировать запрос на сертификат** и заполните поля:



Расшифровка полей

- **Название** - укажите название сертификата. Обязательное поле.
- **Страна (C)** - выберите страну из списка.
- **Область/штат (ST)** - введите название области, до 128 символов.
- **Город (L)** - введите название города, до 128 символов.
- **Организация (O)** - введите название организации, до 64 символов.
- **Подразделение (OU)** - введите название подразделения, до 64 символов.
- **Common Name** - предзаполняется названием сервера Ideco Center. Можно редактировать, до 64 символов. Обязательное поле.
- **Доменное имя (SAN)** - предзаполняется адресом Ideco Center из раздела **Управление сервером** → **Дополнительно**. Домены `.local` не допускаются. Только латинские буквы (допускается Punycode). Можно добавить до 3 доменных имен SAN, минимум 1. Обязательное поле.
- **Комментарий** - произвольный текст.

> Если в полях Common Name и Доменное имя (SAN) указаны одинаковые домены, они объединяются автоматически.

2. Нажмите **Добавить**. В списке появится запись со статусом **Запрос на подпись сертификата** в столбце **Тип**.

3. Нажмите в столбце **Управление** и скачайте CSR (Certificate Signing Request).

4. Выпустите на его основе сертификат.

5. Загрузите выпущенный сертификат согласно инструкции **Загрузка сертификата**.

Вкладка 6

CA-сертификаты используются для проверки сертификатов другой ноды. Списки доверенных CA (Certificate Authority) для проверки клиентского и серверного сертификатов задаются раздельно в настройках кластера.

В качестве доверенного CA можно использовать публичный, корпоративный или внутренний CA самой ноды. Дополнительно в настройках кластера доступен вариант **Все системные CA-сертификаты** - при его выборе используется все системное хранилище доверенных сертификатов.

CA-сертификаты загружаются вручную в формате `.pem` - без приватного ключа и цепочки. Поддерживаются как корневые, так и промежуточные CA-сертификаты.

Для загрузки CA-сертификата:

1. Нажмите **Загрузить сертификат**.

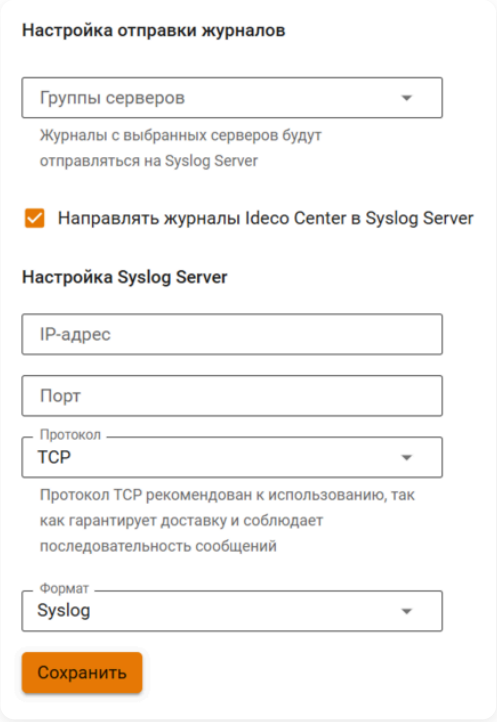
2. Выберите файл в формате `.pem`.

3. Нажмите **Загрузить**, чтобы добавить сертификат в список.

Syslog

Модуль позволяет отправлять все системные сообщения (syslog) с группы серверов Ideco NGFW Novum в сторонние коллекторы (Syslog Collector) или в SIEM-системы.

Чтобы настроить пересылку системных сообщений, перейдите в **Отчеты и журналы** → **Syslog** и выполните:



1. Выберите группу серверов NGFW, журналы с которых будут передаваться на Syslog Server.

> Опция **Направлять журналы Ideco Center в Syslog Server** позволяет отправлять журналы, генерируемые самой Ideco Center, на Syslog Server.

2. Укажите IP-адрес сервера-коллектора (любой локальный или публичный IP-адрес).

3. В поле **Порт** укажите порт, настроенный на сервере-коллекторе (в диапазоне от 1 до 65535).

4. Выберите протокол для передачи системных логов: TCP или UDP.

5. Выберите формат, в котором будут передаваться системные сообщения: Syslog или CEF.

6. Нажмите **Сохранить** и включите опцию **Syslog**.

Примеры расшифровки передаваемых логов представлены в статье.

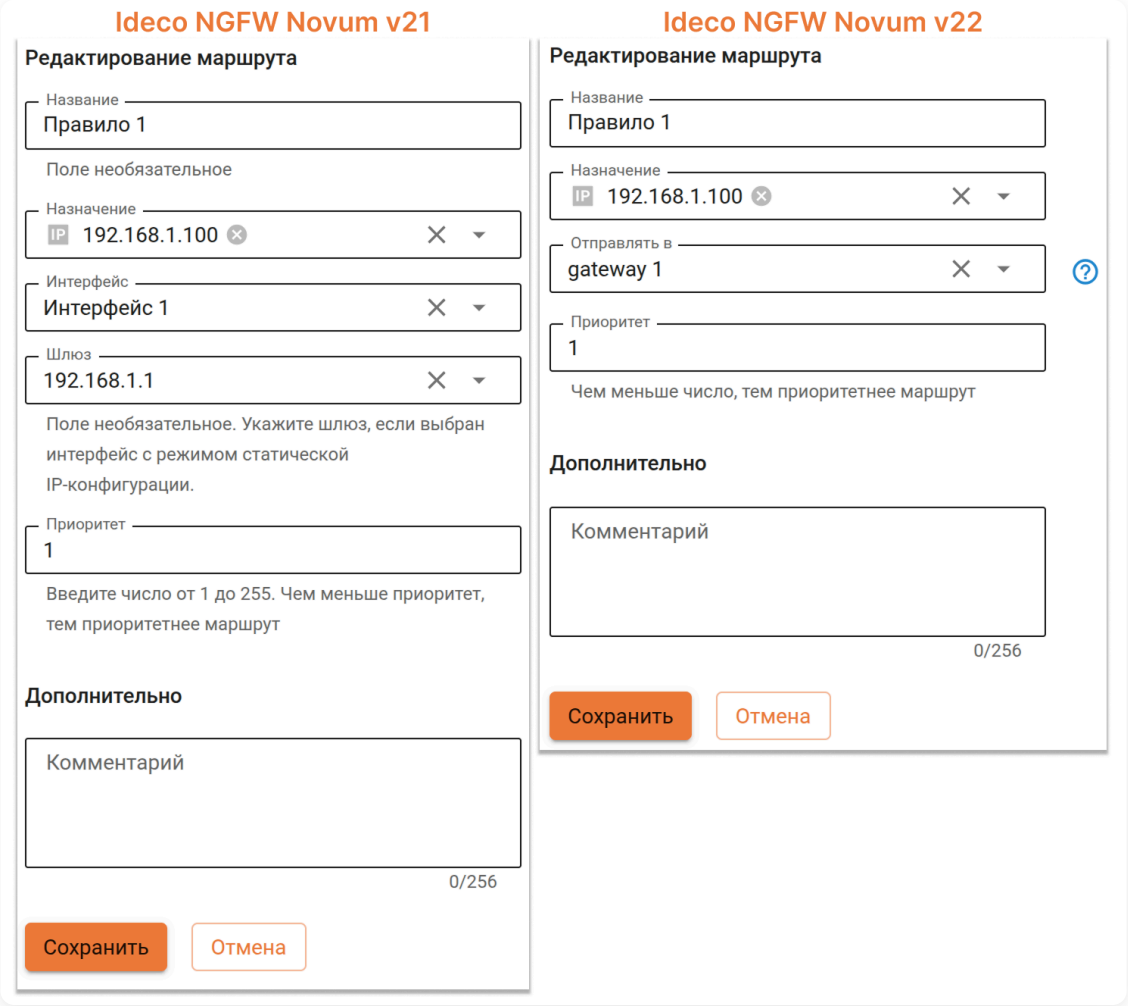
SD-WAN

SD-WAN (Software-Defined Wide Area Network) - технология программно-определяемых распределенных сетей, которая управляет WAN-каналами на основе политик и обеспечивает интеллектуальную маршрутизацию трафика между филиалами, центрами обработки данных и облачными сервисами.

Миграция при обновлении

Логика создания **Next hop** при миграции маршрутов зависит от исходной конфигурации:

- Если в маршруте был указан **Интерфейс** - автоматически создается **Next hop**. Пример правила статической маршрутизации:



- Если в маршруте не был указан **Интерфейс** - **Next hop** не создается, маршрут сохраняется в прежнем виде. Пример правила статической маршрутизации:

Ideco NGFW Novum v21

Редактирование маршрута

Название
Правило 1

Поле необязательное

Назначение
IP 192.168.1.100

Интерфейс

Шлюз
192.168.1.1

Поле необязательное. Укажите шлюз, если выбран интерфейс с режимом статической IP-конфигурации.

Приоритет
1

Введите число от 1 до 255. Чем меньше приоритет, тем приоритетнее маршрут

Дополнительно

Комментарий

0/256

Сохранить Отмена

Ideco NGFW Novum v22

Редактирование маршрута

Название
Правило 1

Назначение
IP 192.168.1.100

Отправлять в
192.168.1.1

Приоритет
1

Чем меньше число, тем приоритетнее маршрут

Дополнительно

Комментарий

0/256

Сохранить Отмена

Next hop

API

Next hop - это следующий узел маршрутизации, на который передается сетевой трафик для дальнейшей доставки к целевой сети. В рамках **SD-WAN** next hop определяется после выбора маршрута до точки назначения и задает, через какой интерфейс и шлюз будет отправляться трафик.

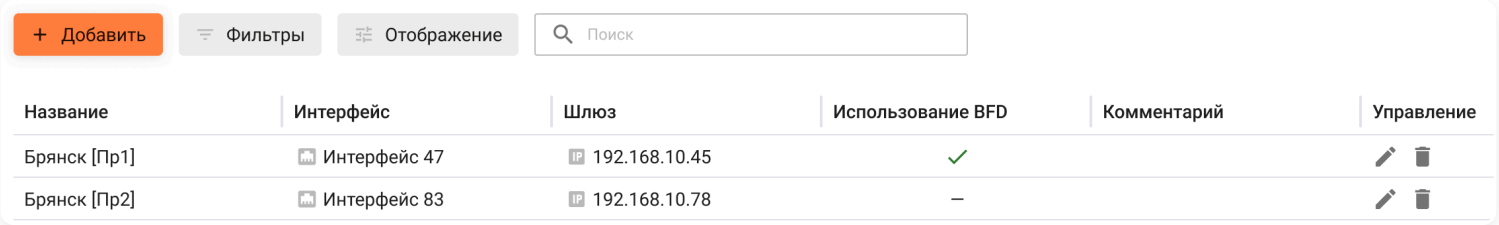
Next hop используется при настройке **Статической** маршрутизации.

Если нет необходимости в проверке доступности шлюза или резервировании, в поле **Отправить в** достаточно указать IP-адрес как **Объект** или **Значение**. Создайте **Next hop**, если:

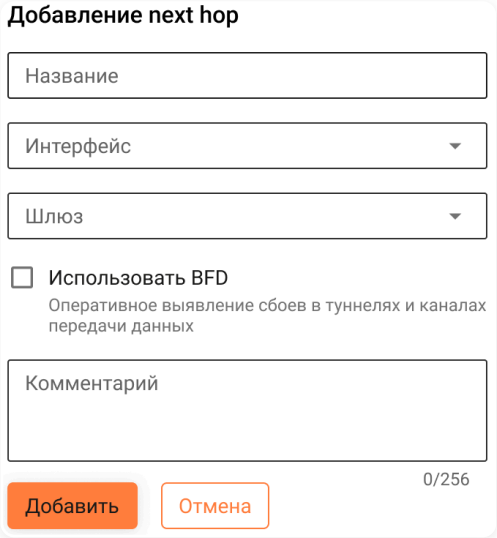
- Нужна проверка доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection).
- Планируется объединить несколько шлюзов в **Профиль next hop** для резервирования или балансировки трафика.
- При настройке **Статического** маршрута необходимо указать интерфейс.

Для добавления **Next hop** выполните действия:

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



2. Заполните поля:



- **Название** - укажите название.
- **Интерфейс** - выберите сетевой интерфейс, через который будет отправляться трафик к следующему узлу.
- **Шлюз** - укажите IP-адрес следующего узла маршрутизации (next hop), на который будет направляться трафик. Адрес шлюза должен находиться в сети выбранного интерфейса.
- **Использовать BFD** - включите опцию для проверки доступности шлюза по протоколу BFD (Bidirectional Forwarding Detection). Поддерживается только для статических маршрутов. BFD должен быть включен и на стороне указанного шлюза.
- **Комментарий** - необязательное поле для описания **Next hop**.

Интерфейс с ролью **Control Plane** используется только для настройки и администрирования Center. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям Center.

Маршрутизация

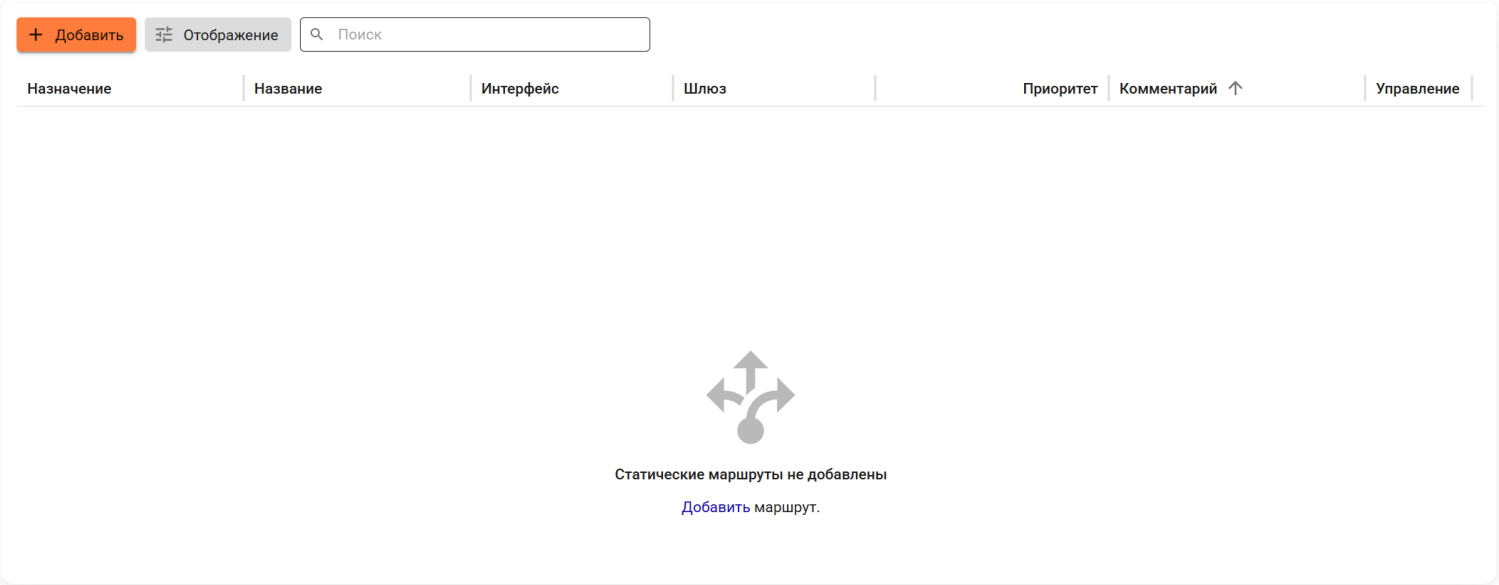
В разделе описана настройка статической маршрутизации.

Статическая маршрутизация

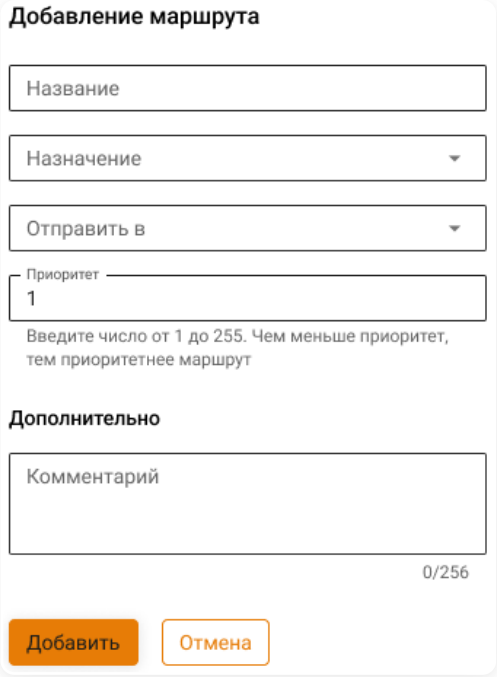
Статическая маршрутизация применяется в сценариях, где нет необходимости в сложной логике маршрутизации. Обработка статических маршрутов происходит после PBR, но до динамической маршрутизации и маршрутизации внешних сетей.

Для добавления статического маршрута выполните действия:

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



2. Заполните поля:



Расшифровка полей

- **Название** - укажите название правила.

- **Назначение** - выберите объекты, при обращении к которым будет применяться это правило. Возможные типы объектов: Пользователь, IP-адрес, Домен, Группа, Подсеть, Список IP-объектов, Диапазон IP-адресов.
- **Отправить в** - выберите IP-адрес или Next hop, через который будет отправлен трафик. IP-адрес можно указать как **Объект** или **Значение**.

Работа со значениями

Значения - это данные, которые добавляются в правило напрямую без создания **Объекта**. Подходят для быстрой загрузки большого количества правил, а также для ситуаций, когда элемент (например, IP-адрес) нужен только в одном конкретном правиле и больше нигде не будет использоваться.

Отличие значений от объектов:

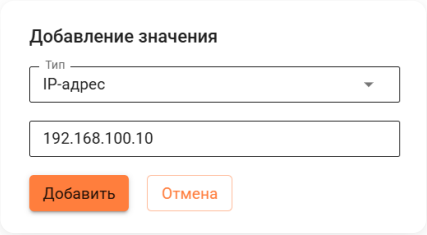
- **Значения** хранятся только в правиле, где были добавлены.
- **Объекты** хранятся в разделе **Объекты**, доступны для повторного использования в разных правилах и управляются централизованно.

Управление значениями

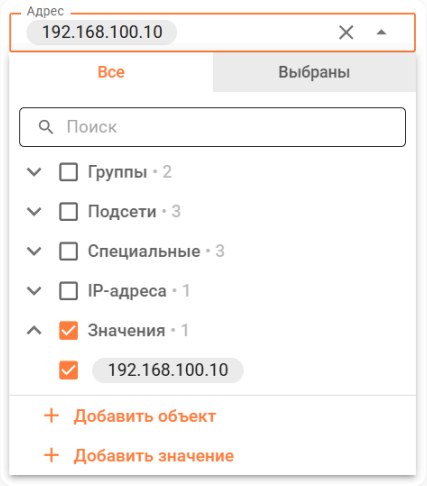
Добавление

1. В поле нажмите **Добавить значение**:

2. Выберите нужный тип и введите значение:



3. Нажмите **Добавить**. Значение будет автоматически выбрано в поле:



Особенности:

- Значения фиксируются только после сохранения правила.
- При обновлении страницы без сохранения правила незафиксированные ранее значения удалятся.

Удаление

1. В поле снимите отметку со значения или выберите другое значение для полей с одиночным выбором:

2. Сохраните правило. После сохранения все невыбранные значения автоматически удалятся.

Интерфейс с ролью **Control Plane** используется только для настройки и администрирования Center. Он не предназначен для использования в качестве сетевого шлюза и через него недоступна маршрутизация к другим сетям Center.

- **Приоритет** - укажите приоритет маршрута. Чем меньше число, тем выше приоритет. При значении 255 трафик по этому маршруту будет заблокирован.
- **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 256 символов.

С версии 22 Ideco Center не поддерживает указание пользователя в поле **Шлюз**. Если в правиле был указан пользователь, перед обновлением замените его на IP-адрес вручную.

Особенности

- **Порядок обработки маршрутов:**
  Статические маршруты обрабатываются после PBR, но до динамической маршрутизации (BGP, OSPF и EIGRP). Если в статической маршрутизации задан шлюз по умолчанию, трафик будет отправлен через него и не дойдет до динамической маршрутизации и правил маршрутизации внешних сетей.
- **Резервные маршруты через приоритет:**
  Если установить приоритет статического маршрута в диапазоне от 200 до 254, он станет менее приоритетным, чем маршруты, полученные через протоколы динамической маршрутизации. Это позволяет использовать статические маршруты как резервные:
  - Если динамическая маршрутизация предоставляет путь к сети, будет использован динамический маршрут.
  - Если динамический маршрут отсутствует, трафик пойдет по статическому маршруту.
- **Балансировка нагрузки (ECMP):**
  Если создать два маршрута к одному назначению с одинаковым приоритетом, трафик будет распределен между ними по принципу ECMP (Equal-Cost Multi-Path).
- **Блокировка трафика:**
  При значении приоритета 255 трафик по маршруту блокируется.

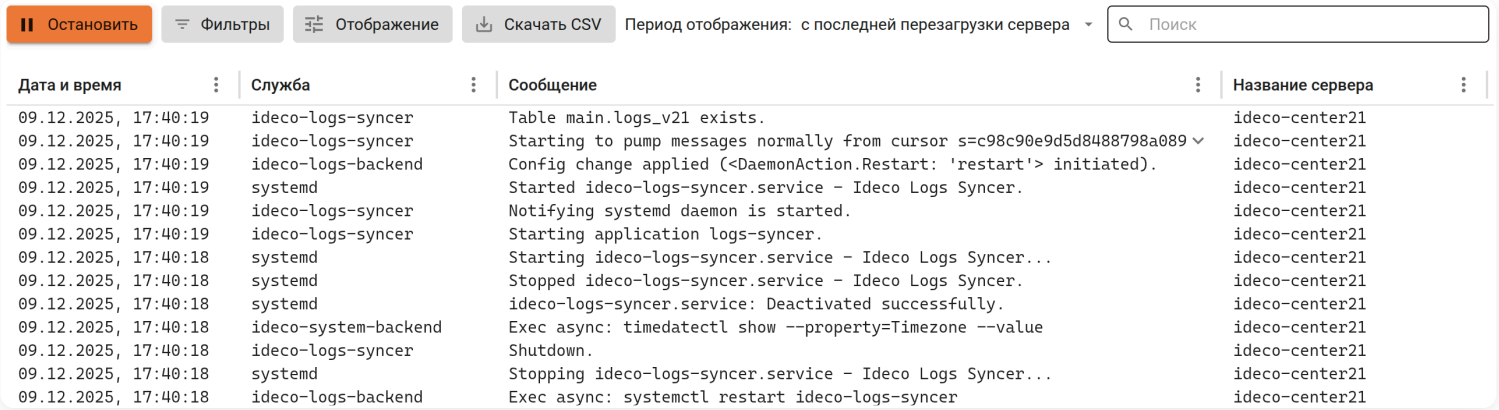
Отчеты и журналы

Система

Время хранения логов в разделе **Система** - 90 дней. После этого логи доступны в **Управление сервером -> Терминал**. Ограничение на размер журнала - 5 ГБ на каждый NGFW.

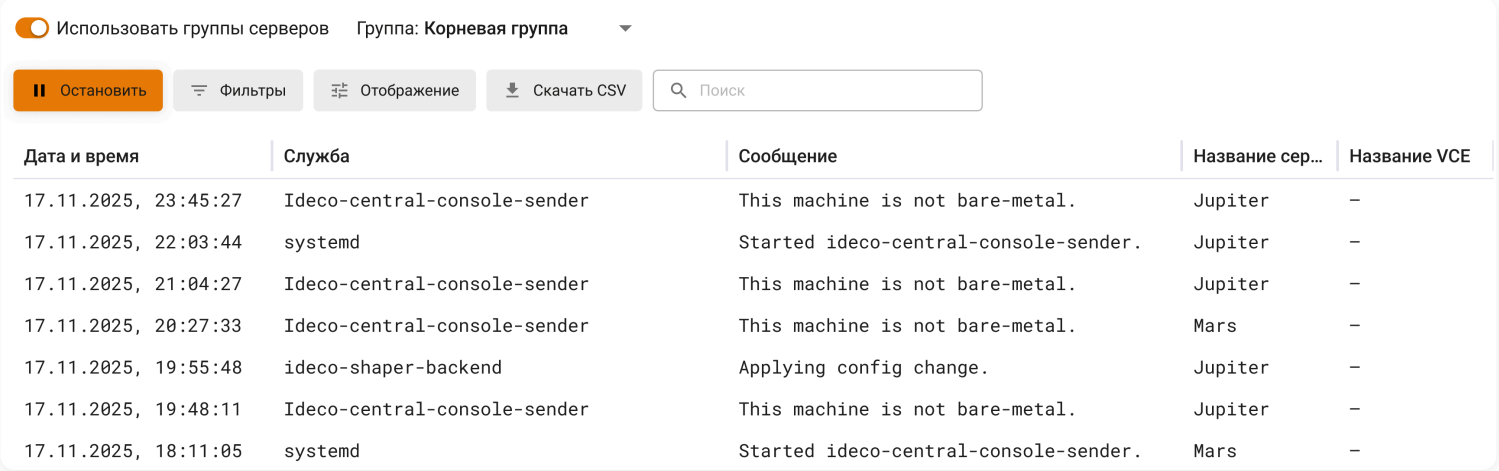
Журнал Ideco Center

На вкладке доступен просмотр логов Ideco Center:



Журнал серверов

На вкладке можно выбрать группу серверов для просмотра логов подключенных Ideco NGFW Novum:



- **Использовать группы серверов** - при включении опции отображаются данные серверов, находящихся в выбранной группе. При выключенной опции отображаются журналы всех системных и дочерних контекстов.

Включите опцию **Отправлять журналы на Ideco Center** в разделе **Управление сервером -> Ideco Center** на каждом Ideco NGFW Novum, чтобы в таблице отображались логи подключенных серверов.

Отправка журналов возможна только в **Системном контексте**. Корневой NGFW отправляет данные на Ideco Center со всех контекстов.

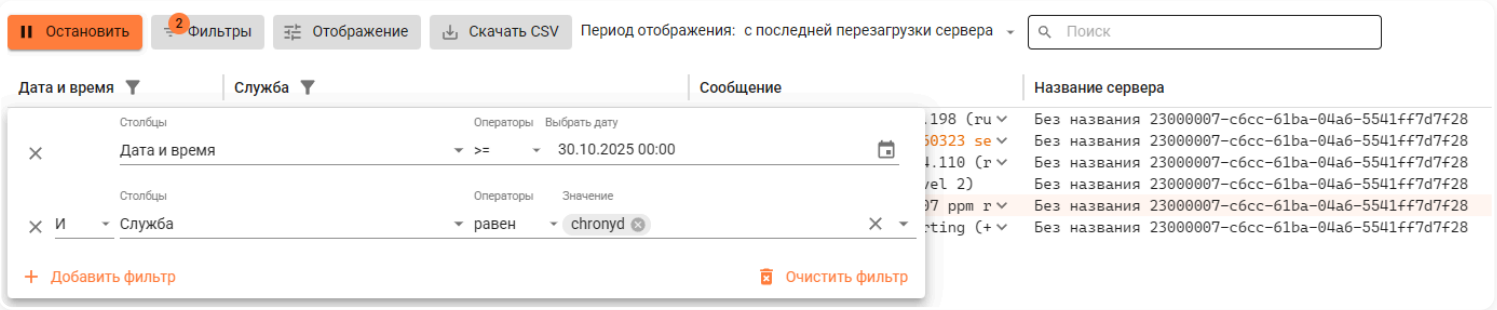
Отображение журналов в Ideco Center зависит от того, какие контексты подключены в разделе **Серверы**:

- **Системный контекст и VCE подключены** - доступны логи системного и дочерних контекстов.
- **Системный контекст подключен, VCE не подключен** - доступны логи только системного контекста. Для отображения логов VCE выключите опцию **Использовать группы серверов**.

- **Подключен только VCE** - логи не отправляются, VCE получает только правила фильтрации.

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.

Список служб, доступных в разделе

- **Серверы** - `ideco-servers-backend`, `ideco-servers-websocket`.
- **Межсетевой экран** - `ideco-firewall-backend`, `ideco-firewall-rest`.
- **Контент-фильтр** - `ideco-content-filter-backend`.
- **Предотвращение вторжений** - `ideco-suricata-backend`.
- **Объекты** - `ideco-alias-backend`.
- **Сетевые интерфейсы** - `ideco-network-backend`, `ideco-network-nic`.
- **Маршрутизация** - `ideco-routing-backend`, `ideco-routing-rest`.
- **Обратный прокси** - `ideco-reverse-backend`.
- **Защита и управление DNS** - `ideco-dns-backend`, `unbound`, `nsd`, `unbound-anchor`, `unbound-keygen`.
- **DHCP-сервер** - `ideco-dhclient`.
- **NTP-сервер** - `chronyd`.
- **Кластеризация** - `ideco-cluster-backend`.
- **Обновления** - `ideco-sysupdate-backend`.
- **Бэкапы** - `ideco-backup-backend`, `ideco-backup-create`.
- **Лицензия** - `ideco-license-backend`.
- **Syslog** - `ideco-logs-backend`, `ideco-monitor-backend`.
- **Отчеты и журналы** - `ideco-logs-backend`, `ideco-logs-syncer`.
- **Действия администраторов** - `ideco-audit-backend`.
- **Авторизация администраторов** - `ideco-web-backend`.
- **Сертификаты** - `ideco-cert-backend`.
- **Локальное меню** - `ideco-local-menu`.
- **Дополнительно** - `ideco-system-backend`.
- **Сбор анонимной статистики о работе сервера** - `ideco-gatherstat-backend`.
- **Защита от несанкционированного доступа, в т.ч. от брутфорс-атак (brute force - атака полным перебором)** - `fail2ban`.
- **REST API NGFW** - `ideco-rest-api-backend`.
- **Доступ по SSH** - `sshd`.

Служебное:

- **Сервер базы данных** - `clickhouse-server`.
- **Сервер управления nginx Ideco** - `nginx-control-plane`.
- **Сервис для очистки невалидных подключений** - `ideco-conndrop`.
- **Локальная база данных** - `ideco-etcd-runtime`, `ideco-etcd-permanent`.
- **Блокировка источников и назначений из файла** - `ideco-apply-manual-blocklist`.
- **Управление лицензиями в облачной среде** - `ideco-vk-cloud-license`.
- **Проверка целостности файлов** - `ideco-check-sums`.
- **Проверка прав пользователей на перезапуск служб systemd** - `ideco-policy-backend`.
- **Управление SWAP-разделами** - `ideco-system-swap`.
- **Сбор метрик и статистики** - `prometheus`, `prometheus-node-exporter`.

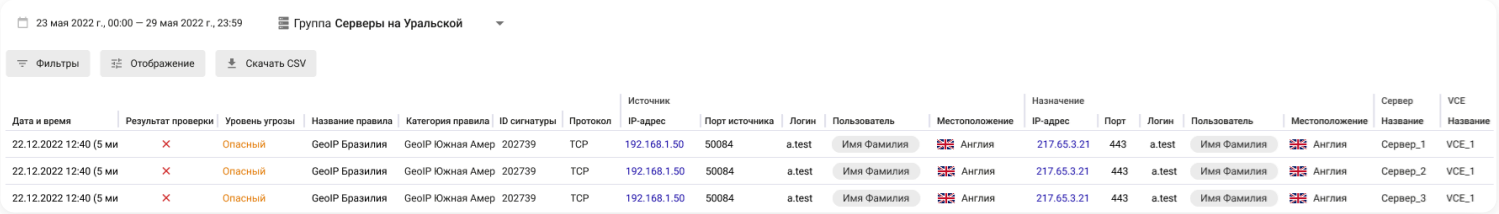
События безопасности

Документация API

В разделе отображаются события безопасности с подключенных серверов Ideco NGFW Novum. При подключении NGFW отправляются данные со всех его VCE. Чтобы посмотреть события конкретного VCE, подключите этот контекст отдельно.

Журнал IPS

Вкладка **Отчеты и журналы** → **События безопасности** → **Журнал IPS** содержит логи системы **Предотвращения вторжений**. Для просмотра событий выберите сервер или группу серверов:

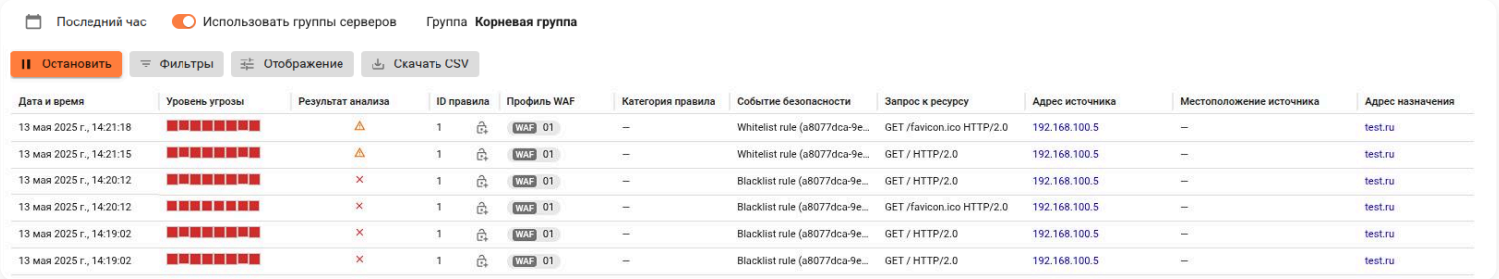


- Поле **Результат проверки** отображает действие системы:
  - `Blocked` - пакет блокирован.
  - Любая другая информация в этом поле - `Allowed`, информирование.
- В поле **Уровень угрозы** могут отображаться следующие значения:
  - Критичный
  - Опасный
  - Предупреждение
  - Не распознано
  - Не классифицировано

IP-адреса в столбцах **Источник** и **Назначение** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.

Web Application Firewall

Вкладка **Отчеты и журналы** → **События безопасности** → **Web Application Firewall** содержит информацию о срабатывании правил **Web Application Firewall** в виде таблицы:



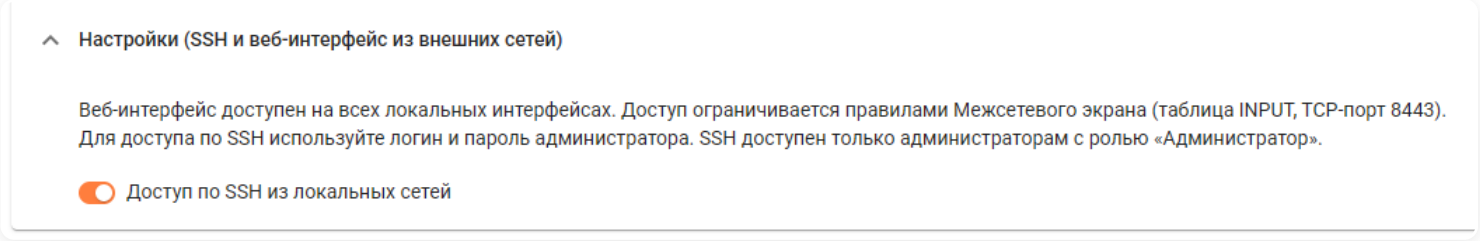
- **Использовать группы серверов** - при включении опции отображаются данные серверов, находящихся в выбранной группе. При выключенной опции отображаются журналы всех системных и дочерних контекстов.

Для проверки IP-адресов в столбцах **Адрес источника** и **Адрес назначения** скопируйте адрес и выполните его поиск в сервисе Whois.

На вкладке **Web Application Firewall** отображается профиль WAF, параметры которого вызвали блокировку доступа к ресурсу.

Действия администраторов

Ideco Center логирует действия администраторов, которые вносят изменения в конфигурацию Ideco Center из веб-интерфейса, локального меню и терминала:

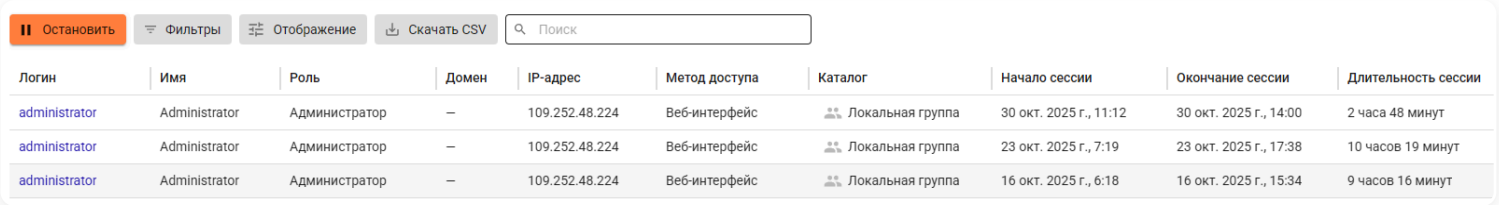


Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

Аутентификация администраторов

Время хранения данных в журнале **Аутентификация администраторов** - 1 год.

В разделе отображается список авторизованных администраторов:



Логин	Имя	Роль	Домен	IP-адрес	Метод доступа	Каталог	Начало сессии	Окончание сессии	Длительность сессии
administrator	Administrator	Администратор	–	109.252.48.224	Веб-интерфейс	Локальная группа	30 окт. 2025 г., 11:12	30 окт. 2025 г., 14:00	2 часа 48 минут
administrator	Administrator	Администратор	–	109.252.48.224	Веб-интерфейс	Локальная группа	23 окт. 2025 г., 7:19	23 окт. 2025 г., 17:38	10 часов 19 минут
administrator	Administrator	Администратор	–	109.252.48.224	Веб-интерфейс	Локальная группа	16 окт. 2025 г., 6:18	16 окт. 2025 г., 15:34	9 часов 16 минут

Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

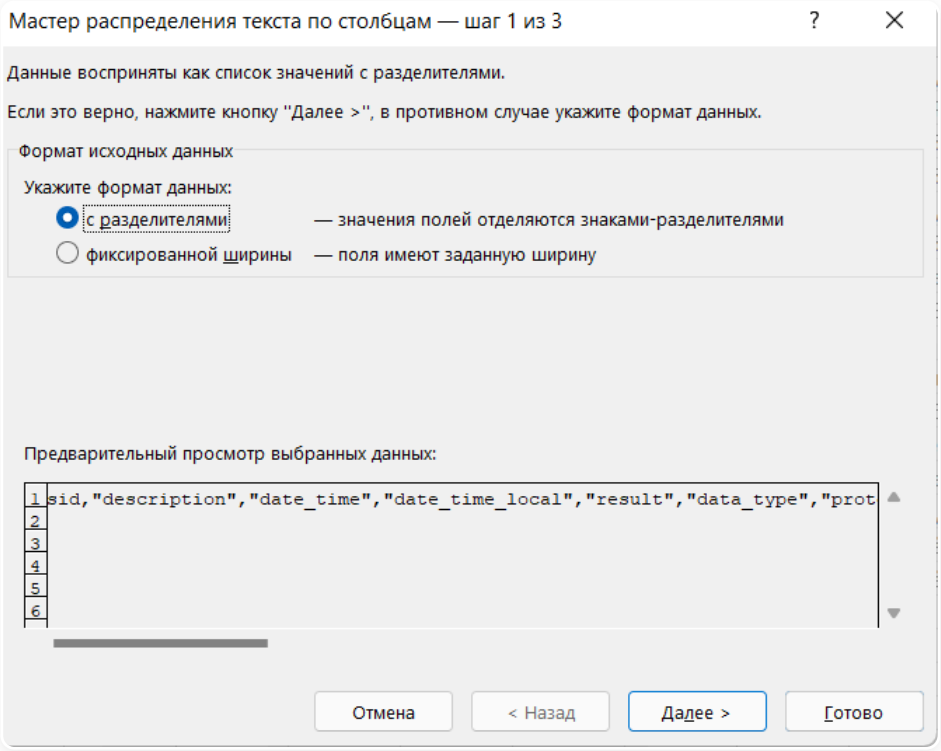
Для корректного отображения информации из CSV-файла

1. Скачайте CSV-файл с логами за определенный период по соответствующей кнопке.

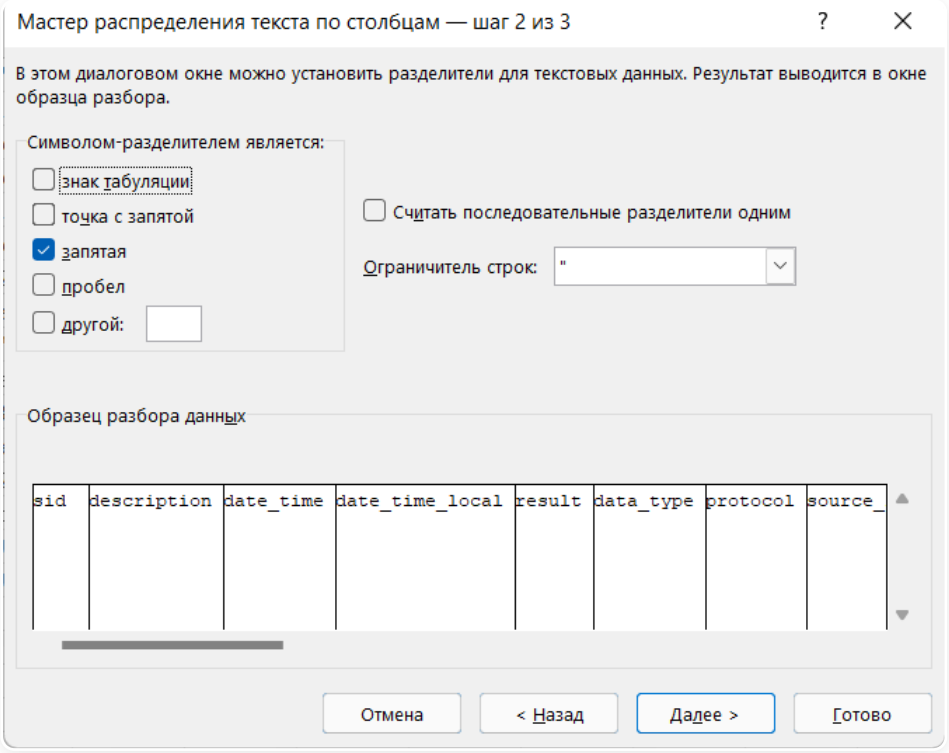
2. Откройте CSV-файл в MS Excel и выделите весь первый столбец.

3. Перейдите на вкладку **Данные** и нажмите **Текст по столбцам**.

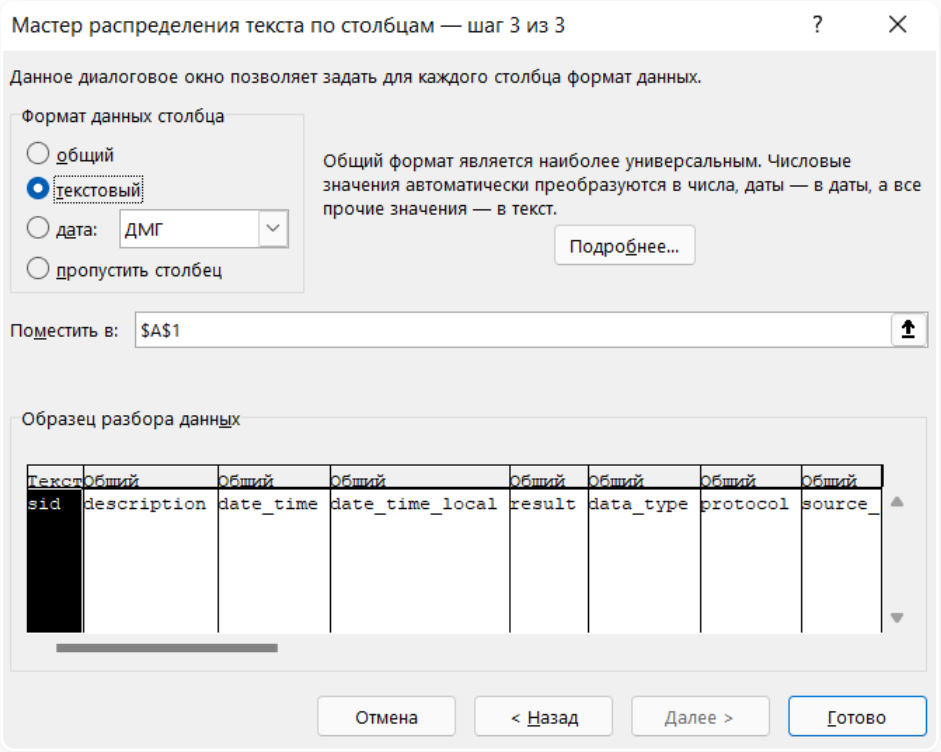
4. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:



5. В блоке **Символом-разделителем является:** выберите **запятая** и нажмите **Далее**:



6. В блоке **Формат данных столбца** выберите **Текстовый** и нажмите **Готово**:



Управление сервером

Администраторы

С версии 23 управление учетными записями администраторов и их доступами будет переведено на централизованную модель. Подробнее об изменениях и переносе настроек – в статье Подготовка к миграции администраторов из VCE в версии 23.

В Ideco Center можно создать локальных администраторов или интегрировать администраторов из сервисов Active Directory, RADIUS. Добавление администраторов в Ideco Center аналогично механизму в Ideco NGFW Novum.

Локальным администраторам могут быть назначены роли:

- **Администратор** - имеет доступ ко всем функциям Ideco Center.
- **Только просмотр** - не имеет возможности управлять правилами в Ideco Center (создавать, менять приоритет и др.).
- **Администратор ИБ** - имеет доступ к событиям безопасности.
- **Администратор межсетевого экрана** - может создавать учетные записи, настраивать правила фильтрации и управлять режимами работы **Межсетевого экрана**.
- **Администратор настройки доступов** - имеет доступ к настройкам сетевого взаимодействия пользователей **Межсетевого экрана**, субъектов доступа, информационных систем.

Удалять подключенные Ideco NGFW Novum из Ideco Center могут только администраторы с ролью **Администратор**.

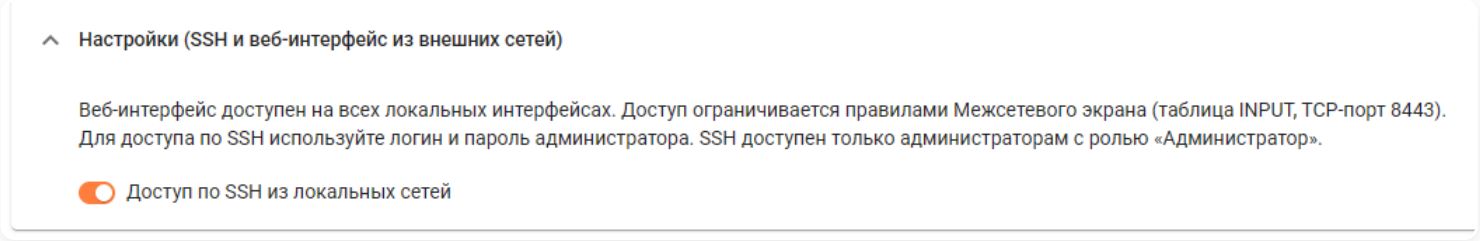
Авторизоваться в Ideco NGFW Novum с логином и паролем администратора Ideco Center **невозможно**.

Доступ к веб-интерфейсу из внешней сети и удаленный доступ по SSH

Для подключения по SSH из локальных сетей выполните действия:

1. Перейдите в **Управление сервером** → **Администраторы**.

2. Активируйте настройку **Доступ по SSH из локальных сетей**.



3. Подключитесь к серверу с помощью любого SSH-клиента (для Windows, например, PuTTY), используя 22 порт. Необходимо указать логин и пароль **Администратора Ideco Center**.

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 ~]#
```

Попытки подбора паролей будут автоматически блокироваться.

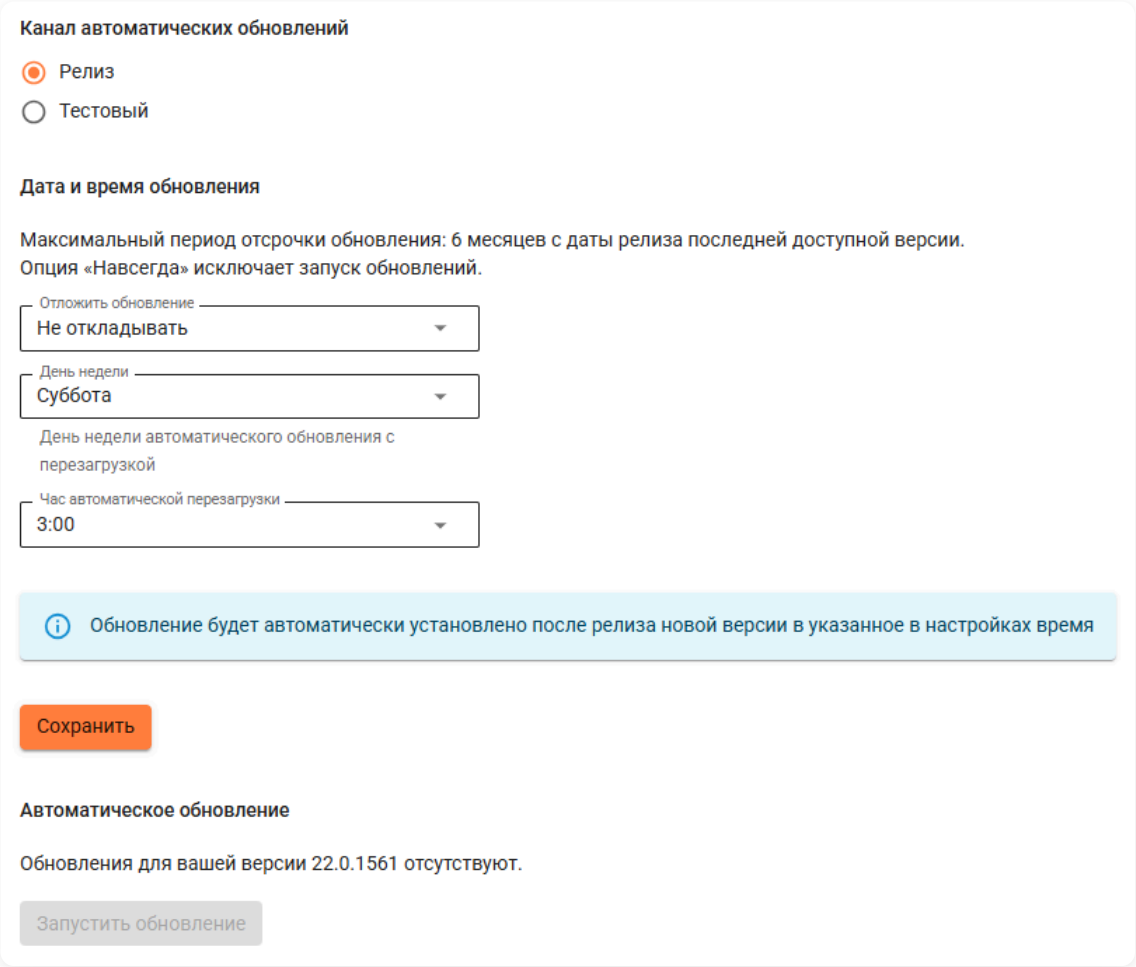
Обновления

Обновить систему Ideco Center можно как в офлайн-режиме, так и по сети. Настроить режим обновления можно в **Управление сервером** → **Обновления**.

> Для отключения автоматического обновления Ideco Center в строке **Отложить обновление** выберите **Навсегда**.

Автоматическое обновление

В режиме **Автоматического обновления** доступны следующие настройки:

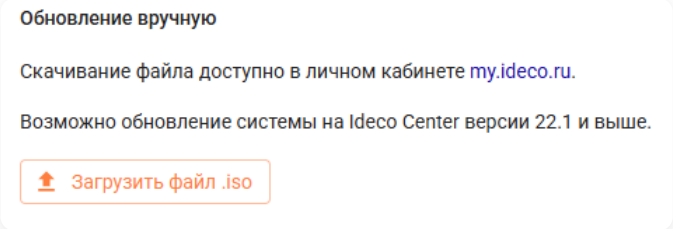


Расшифровка полей

- **Канал автоматических обновлений** - выберите **Релиз** или **Тестовый**. Канал **Релиз** позволяет обновляться на стабильно работающие версии. Канал **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** - позволяет выбрать час запуска автоматического обновления.
- **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

Ручное обновление

В режиме **Ручной загрузки** обновлений необходимо скачать ISO-образ новой версии Ideco Center в MY.IDECO и загрузить его с внешнего носителя:

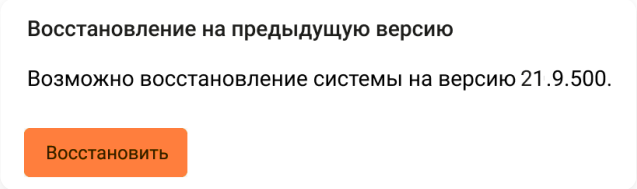


Кнопка принудительного обновления активна только после скачивания обновления и позволяет его применить. Скачивание нельзя инициировать. После применения обновления потребуется полная перезагрузка сервера.

После обновления новая версия будет отображаться в верхнем левом углу веб-интерфейса Ideco Center.

Восстановление на предыдущую версию

Кнопка **Восстановить** позволяет вернуться к предыдущей версии Ideco Center:



Система будет перезагружена, при этом текущие настройки будут потеряны. После восстановления отложите автоматическое обновление.

При восстановлении на предыдущую версию данные перенесены не будут. Ideco Center вернется в состояние, в котором был на момент обновления. Все изменения, внесенные после обновления, будут утеряны. Сохраните информацию на внешнем носителе. Ideco Center 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 Ideco Center не ниже той, на которой был создан.

Процесс выхода релизов в каналы обновлений

Тестовый канал обновлений позволяет быстрее обновляться до новых версий (релизных или бета-версий во время их активного тестирования). После выхода бета-версии Ideco Center в **Тестовый** канал ожидается обратная связь от пользователей по использованию новой версии продукта через Telegram. Обратная связь позволяет выявить недочеты и уязвимости в продукте. После их исправления происходит выкладка в канал **Релиз**.

Если в версии Ideco Center, вышедшей в канал **Релиз**, в ходе использования выявляются недочеты, то они исправляются ближайшими обновлениями версии. Обновление в канале **Релиз** появляется постепенно.

Особенности обновления Ideco Center

- 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 Ideco Center - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7).
- Автоматическое обновление Ideco Center до следующей мажорной версии возможно только после установки последней минорной версии, выпущенной в релиз. Например, можно обновить Center 17.2 до версии 17.9, а затем до версии 18.6.
- Ручное обновление Ideco Center до следующей мажорной версии можно выполнить с любой версии. Например, можно обновить Center 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 теперь отсчитываются с даты выхода последнего доступного минорного релиза.

Лицензия

В разделе **Ideco Center** MY.IDECO находится информация о зарегистрированных серверах и имеющихся лицензиях.

Доступные виды лицензий:

- **Enterprise** - коммерческая лицензия.
- **Enterprise-demo** - бесплатная лицензия сроком на 44 дня. Формируется автоматически при регистрации сервера в MY.IDECO.

Доступные действия для управления лицензиями:

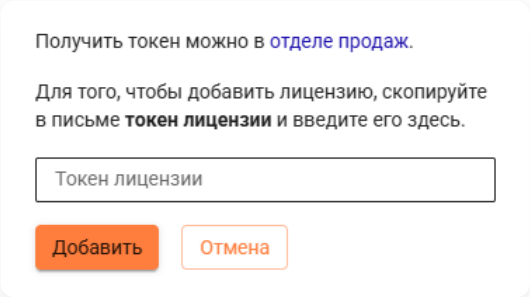
- Регистрация сервера.
- Добавление коммерческой или бесплатной лицензии.
- Привязка лицензии к серверу.
- Просмотр информации об имеющихся лицензиях.
- Офлайн-обновление лицензии и баз модулей фильтрации.

Добавление коммерческой (Enterprise) лицензии

1. Скопируйте токен лицензии из письма, отправленного после покупки лицензии. Формат токена: `owhYLGvT6Xmt819JyinSxREkJfvjVO63`.

2. В MY.IDECO перейдите в **Ideco Center** → **Лицензирование** и нажмите **Добавить лицензию**.

3. Введите токен в поле **Токен лицензии** и нажмите **Добавить**:

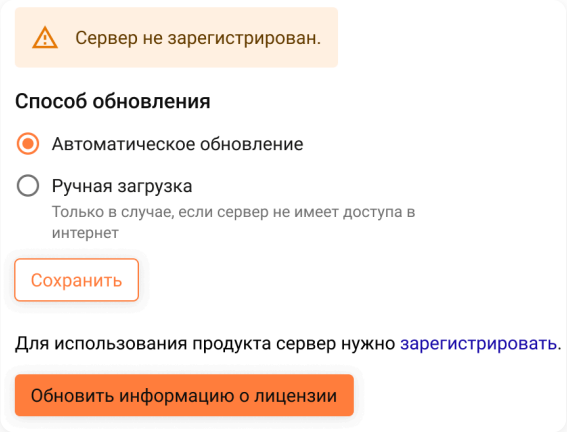


Токен станет недействительным, а в таблице **Непривязанные лицензии** отобразится купленная лицензия.

Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн:

- Для онлайн-привязки лицензии в разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco Center выберите опцию **Автоматическое обновление**. Онлайн-привязка проводится только в MY.IDECO.
- Для офлайн-привязки выберите опцию **Ручная загрузка**. Офлайн-привязка потребует доступ к веб-интерфейсу сервера:



Назначьте имеющиеся коммерческие лицензии на любой зарегистрированный сервер Ideco Center с учетом следующих ограничений:

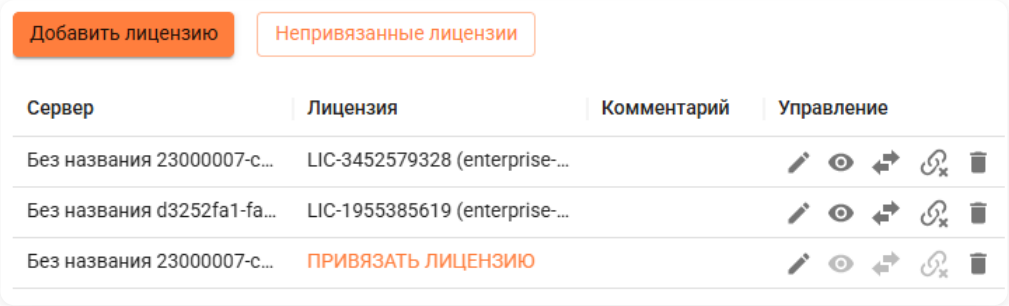
- Одна лицензия может быть привязана только к одному серверу.
- Демо-лицензию нельзя привязать к другому серверу.
- Демо-лицензию нельзя отвязать от сервера. Доступна только замена на другую лицензию.
- Демо-лицензия выдается только один раз для каждого экземпляра сервера.
- При удалении сервера с демо-лицензией также удаляется и лицензия.

После активации лицензия привязывается к оборудованию, на котором установлено программное обеспечение Ideco Center. При замене оборудования или частей оборудования лицензия отвязывается и требует повторной привязки. Демо-лицензия при этом теряется.

Онлайн-привязка лицензии

Перейдите в MY.IDECO и выберите удобный вариант привязки:

- В **Ideco Center** → **Лицензирование** нажмите **Привязать лицензию**:



В открывшемся окне выберите нужную лицензию и сохраните изменения.

- В **Ideco Center** → **Лицензирование** перейдите в **Непривязанные лицензии** и нажмите . Укажите нужный сервер и сохраните изменения, нажав **Привязать**:

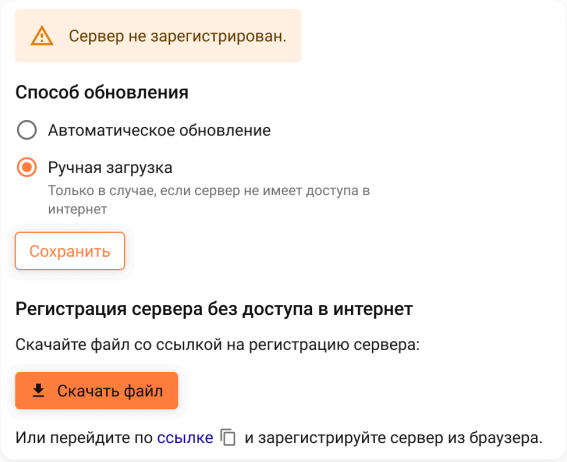
Офлайн-привязка лицензии

Для офлайн-регистрации сервера и привязки лицензии выполните действия:

1. Перейдите в **Управление сервером** → **Лицензия** веб-интерфейса Ideco Center.

2. Выберите опцию **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

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

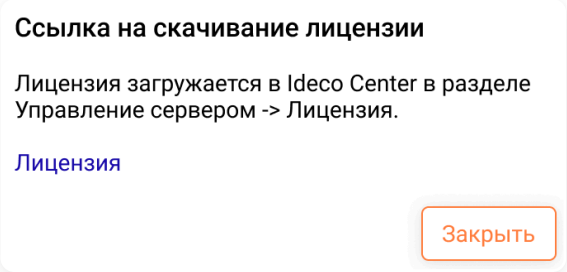


4. Откройте ссылку из пункта 2 на устройстве с доступом к интернету. Сервер автоматически появится в списке серверов в MY.IDECO.

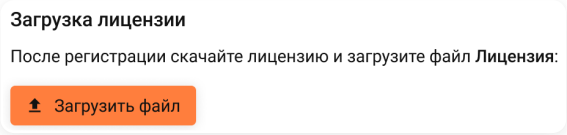
5. Обратитесь к вашему менеджеру для предоставления офлайн-лицензии.

6. Перейдите в **Ideco Center** → **Лицензирование** в MY.IDECO. Нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `IC (IC Unknown)`.

7. Откройте ссылку из пункта 2, чтобы скачать файл лицензии:



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



Просмотр информации о лицензиях

Посмотреть информацию о лицензии можно:

- В разделе **Ideco Center** MY.IDECO, нажав напротив нужного сервера.
- В разделе **Управление сервером** → **Лицензия** веб-интерфейса Ideco Center.

Бэкапы

Бэкап - это предварительно созданная резервная копия данных, позволяющая восстановить большинство настроек и сохраненной информации.

В Ideco Center создается только полный бэкап, который включает в себя все настройки, созданные администратором в веб-интерфейсе.

Бэкапы не включают:

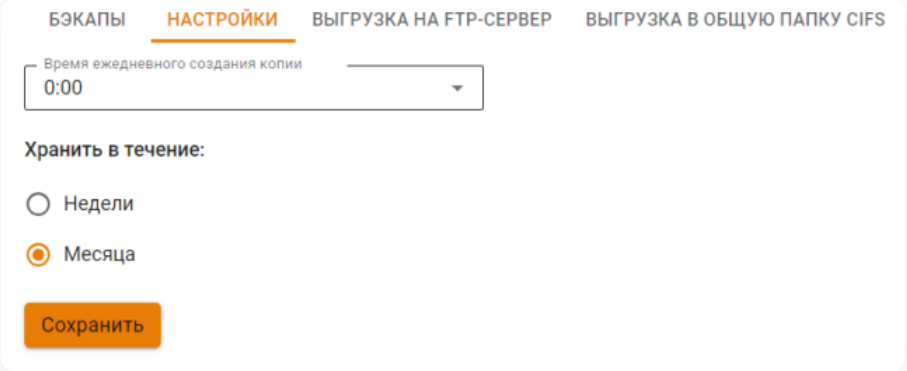
- Системный журнал.
- Любые кешируемые данные, базы антивирусов, правила IPS и т. п.
- Любые данные, автоматически генерируемые в процессе работы системы.

В Ideco Center 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.
>
> Для развертывания нового сервера рекомендуем:
>
> 1. Установить чистую версию Ideco NGFW Novum.
>
> 2. Подключить сервер к Ideco Center.
>
> Заданная конфигурация для сервера в Ideco Center (правила трафика, профили, объекты и т.д.) будет автоматически применена к новому серверу.

Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в **Управление сервером** → **Бэкапы** → **Настройки**:



Расшифровка полей

- **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.

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.

> 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. Ideco Center 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 Center. Команда создает автоматический бэкап в соответствии с заданными настройками сохранения.

Бэкапы на сетевое файловое хранилище

Ключевые параметры, необходимые для настройки бэкапа на **NetBIOS (CIFS)**:

- **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.

Бэкапы на удаленное файловое хранилище

Ключевые параметры, необходимые для настройки бэкапа на **FTP-сервер**:

- **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.

> Укажите путь к каталогу в UNIX-формате. К примеру, в ОС Windows каталог открывается по пути `\\192.168.1.1\dir_1\dir_2\backup`, значит, в поле **Путь к каталогу** пропишите `dir_1/dir_2/backup`.

Ручное создание бэкапа

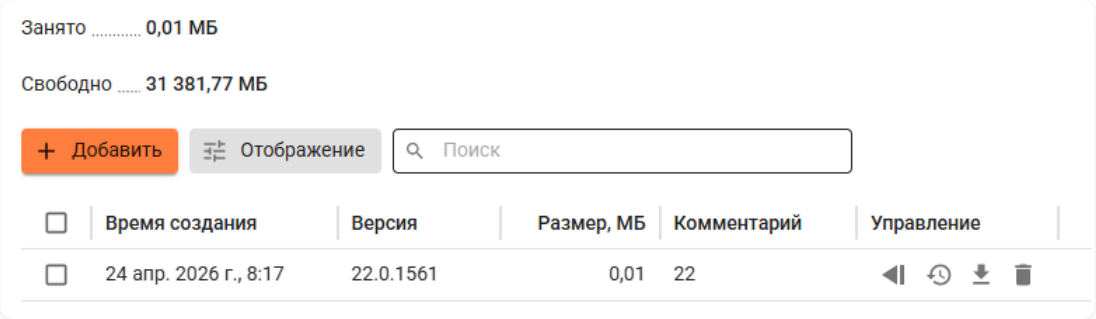
Через веб-интерфейс

Для создания бэкапа через интерфейс Ideco Center перейдите в **Управление сервером** → **Бэкапы** → **Бэкапы** и выполните действия:

1. Нажмите **Добавить** → **Создать** или нажмите **Создать бэкап** в правом верхнем углу веб-интерфейса.

2. Введите комментарий и нажмите **Добавить**.

Новый бэкап появится в таблице:



Через локальное меню

Чтобы создать новый бэкап через локальное меню Ideco Center, выполните действия:

1. Выберите пункт **Создать новый бэкап** и нажмите **Enter**.

2. Введите комментарий для бэкапа и нажмите **Enter**.

Пример создания бэкапа через локальное меню приведен на скриншоте ниже:

```
Управление сервером

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

Введите номер пункта и нажмите Enter.
# 12

Введите комментарий для бэкапа или оставьте поле пустым. Затем нажмите Enter.

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

Настройка сохранения бэкапа в сетевом файловом хранилище возможна только через веб-интерфейс Ideco Center. Выгрузка на внешние сетевые хранилища производится только при автоматическом создании бэкапа.

Восстановление конфигурации из бэкапа

В Ideco Center возможно полное и мгновенное восстановление из бэкапа.

При выполнении полного восстановления система будет перезагружена для применения настроек сервера.

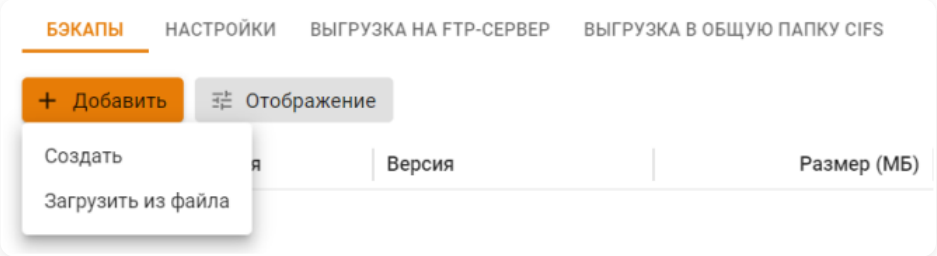
При выполнении мгновенного восстановления бэкап применится без перезагрузки. При этом не сохраняется статистика в отчетах.

> Полное восстановление возможно либо на текущую версию, либо на предыдущую мажорную версию. Например, на версии 17 возможно полное восстановление бэкапа версии 16 или версии 17.
>
> Мгновенное восстановление возможно только для бэкапа версии, полностью совпадающей с установленной 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 в **Управление сервером** → **Бэкапы** → **Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

- **Восстановить из бэкапа** - восстановятся все настройки и перезагрузится сервер.
- **Мгновенно восстановить из бэкапа** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

  Нажмите **Enter**.

2. Выберите из списка бэкап, введя пункт нужной копии, и нажмите **Enter**.

3. Перезагрузите сервер при запуске полного восстановления, введя **y**, а затем **Enter**. При мгновенном восстановлении перезагрузка не нужна.

Пример восстановления из бэкапа через локальное меню:

```
Введите номер пункта и нажмите Enter.
# 14

Выберите бэкап для восстановления:

1.
Время:        24.04.2026 09:22:45
Версия:       Ideco CC 22.0.1561
Комментарий:

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1

Выбран бэкап

Время:        24.04.2026 09:22:45
Версия:       Ideco CC 22.0.1561
Комментарий:

Для восстановления из бэкапа необходима перезагрузка.
Перезагрузить сервер и восстановить настройки сейчас?

Пожалуйста подтвердите ваш выбор.

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

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 Center 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`).
- **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`.

Таблица служб

Раздел	Имя службы
Серверы	ideco-servers-backend, ideco-servers-websocket
Межсетевой экран	ideco-firewall-backend, ideco-firewall-rest
Контент-фильтр	ideco-content-filter-backend
Предотвращение вторжений	ideco-suricata-backend
Объекты	ideco-alias-backend
Сетевые интерфейсы	ideco-network-backend, ideco-network-nic
Маршрутизация	ideco-routing-backend, ideco-routing-rest
Обратный прокси	ideco-reverse-backend
Защита и управление DNS	ideco-dns-backend, unbound, nsd, unbound-anchor, unbound-keygen
DHCP-сервер	ideco-dhclient
NTP-сервер	chronyd
Кластеризация	ideco-cluster-backend
Обновления	ideco-sysupdate-backend
Бэкапы	ideco-backup-backend, ideco-backup-create
Лицензия	ideco-license-backend
Syslog	ideco-logs-backend, ideco-monitor-backend
Отчеты и журналы	ideco-logs-backend, ideco-logs-syncer
Действия администраторов	ideco-audit-backend
Авторизация администраторов	ideco-web-backend
Сертификаты	ideco-cert-backend
Локальное меню	ideco-local-menu
Дополнительно	ideco-system-backend
Сбор анонимной статистики о работе сервера	ideco-gatherstat-backend
Защита от несанкционированного доступа, в т.ч. от брутфорс-атак (brute force - атака полным перебором)	fail2ban
REST API NGFW	ideco-rest-api-backend
Доступ по SSH	sshd

Характеристики сервера

Раздел показывает спецификацию сервера, где развернут Ideco Center:

Гипервизор	Linux KVM kernel virtual machine
Доступно оперативной памяти	7.5 ГБ
Модель процессора	Intel Xeon Processor (Icelake)
Потоков	2
Потоков на ядро	2
Ядер на сокет	1
Сокеты	1
NUMA ноды	1
Версия BIOS	1.16.3-1
Дата выпуска BIOS	04/01/2014
Материнская плата	xeon-gold-6338

Скопировать

Управление питанием

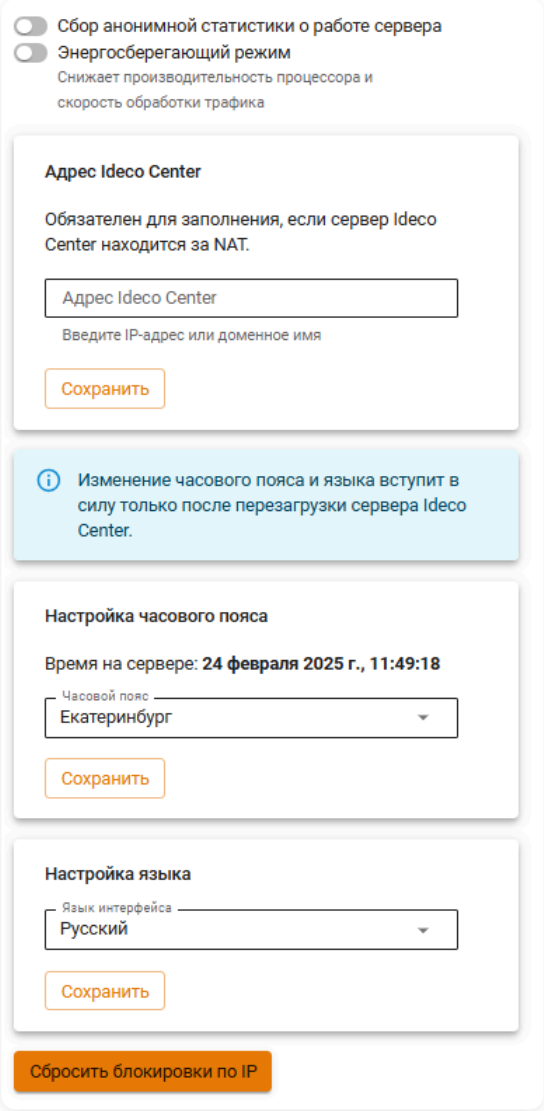
Позволяет перезагрузить или выключить Ideco Center через веб-интерфейс:

Перезагрузка

Выключение

Дополнительно

Настройка осуществляется через веб-интерфейс в **Управление сервером** → **Дополнительно**:



Расшифровка полей

- **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.
- **Адрес Ideco Center** - заполняется, если сервер Ideco Center находится за NAT. После нажатия **Сохранить** будет выпущен сертификат на IP-адрес или доменное имя сервера Ideco Center.
- **Настройка часового пояса** - изменения вступают в силу только после перезагрузки Ideco Center.
- **Настройки языка** - изменения вступают в силу только после перезагрузки Ideco Center.
- **Сбросить блокировки (fail2ban)** - используйте для сброса всех заблокированных IP-адресов. Если требуется разблокировать какой-то конкретный IP-адрес, воспользуйтесь командой `fail2ban-client unban <IP-адрес>` в терминале.

Кластеризация

В отличие от Ideco NGFW Novum, Ideco Center поддерживает георасределенное размещение узлов кластера.

Отказоустойчивый кластер – два Ideco Center, объединенные в режиме active-passive. Кластер позволяет:

- Сохранять управление NGFW при выходе из строя основного сервера.
- Размещать узлы кластера в территориально распределенной инфраструктуре.
- Переключать активный сервер вручную для планового обслуживания.

Каждое из устройств Ideco Center, объединенное в кластер, называется нодой и имеет одну из двух ролей:

- **Первичная нода** – активный сервер управления. Принимает подключения от NGFW, отправляет им конфигурацию. Единственное место, где можно изменять правила, объекты и политики.
- **Вторичная нода** – резервный сервер. Получает синхронизированную копию данных от первичной ноды, но не принимает подключения от NGFW. Все синхронизируемые данные на ней доступны только для чтения.

Роли назначаются при создании кластера. Подробнее о смене ролей – в статье.

Синхронизация данных

Между нодами синхронизируются данные, передаваемые на NGFW:

- Правила трафика
- Профили безопасности
- Объекты
- Группы серверов
- Список подключенных устройств
- Название кластера
- Пользовательские категории контент-фильтра

Не синхронизируются:

- Настройки ноды (интерфейсы, маршруты, сертификаты)
- Параметры кластеризации
- Журналы NGFW
- Настройки SNMP
- Настройки Syslog
- Настройки Zabbix
- Базы сигнатур (обновляются на каждой ноде независимо)

Подключение NGFW к кластеру

NGFW не обращаются к нодам по IP-адресу напрямую. Для обнаружения нод кластера используются SRV-записи, в которых указан список нод. Без SRV-записи NGFW Novum не будет знать о существовании другой ноды. Поэтому для подключения NGFW к кластеру:

1. В DNS-зоне создайте SRV-запись:

```
$ORIGIN cluster.example.com
_ideco_center._tcp 3600 IN SRV 1 0 0 cc1
_ideco_center._tcp 3600 IN SRV 2 0 0 cc2
```

- `cluster.example.com` – имя DNS-зоны, в которой размещаются SRV-записи кластера;
- `_ideco_center._tcp` – фиксированное имя сервиса;
- `3600` – TTL записи в секундах;
- `IN SRV` – тип записи;
- `1` / `2` – приоритет ноды, не используется при подключении;
- `0` – вес. Не используется, всегда указывайте `0`;

- `0` – порт. Не используется, всегда указывайте `0`;
- `cc1` / `cc2` – доменные имена нод кластера (соответствуют значениям из поля **Доменное имя** в настройках каждой ноды).

Если нода отклоняет соединение, NGFW автоматически переходит к следующей записи. Вес и приоритет записей игнорируется, ноды перебираются в лексикографическом порядке (по FQDN).

2. В интерфейсе NGFW в **Управление сервером** → **Ideco Center** в поле **Адрес сервера** укажите доменное имя кластера Ideco Center. Этот домен при добавлении префикса `_ideco_center._tcp` должен соответствовать имени, для которого созданы SRV-записи.

Проверить настройки DNS для подключения NGFW к кластеру

Чтобы убедиться, что DNS настроен правильно, из терминала NGFW проверьте:

1. Корректный резолв A-записей нод кластера:

```
nslookup cc1.cluster.example.com
nslookup cc2.cluster.example.com
```

- `cluster.example.com` – доменное имя кластера.
- `cc1` / `cc2` – доменные имена нод кластера (соответствуют значениям из поля **Доменное имя** в настройках каждой ноды).

2. Корректный резолв SRV-записей DNS-зоны:

```
nslookup -type=SRV _ideco_center._tcp.cluster.example.com
```

- `cluster.example.com` – доменное имя кластера (имя DNS-зоны, в которой размещаются SRV-записи кластера).

Полезные ссылки

- **Создание кластера**
- **Управление кластером**
- **Требования и ограничения для подключения NGFW к Ideco Center**
- **Сертификаты**

Создание кластера

> В статье описывается, как объединить два Ideco Center в кластер: настроить роли нод, выполнить взаимную аутентификацию и синхронизировать данные первичной ноды с вторичной.

Процедура объединения нод ограничена по времени. Если не завершить настройку на обеих нодах в течение 20 минут, запрос на объединение автоматически отменится.

Требования

Перед созданием кластера убедитесь, что соблюдены требования:

- У обеих нод задано доменное имя в разделе **Управление сервером** → **Дополнительно**. Использование IP-адресов для соединения нод не поддерживается.
- И мажорная, и минорная версии у обеих нод совпадают. Кластер с нодами разных версий не создается и не синхронизируется.
- Ноды доступны друг другу по HTTPS.
- В DNS-зоне NGFW Novum созданы SRV-записи для доменного имени кластера. Они используются NGFW Novum для обнаружения нод. Использование IP-адресов для подключения NGFW Novum к кластеру не поддерживается.
- Для корректной работы политик и объектов Active Directory при переключении ролей нод:
  - Подключение к контроллеру домена настроено отдельно на каждой ноде кластера.
  - Обе ноды подключены к одному и тому же контроллеру домена.

Сертификаты для связи между нодами

При создании кластера Ideco Center создается два подключения: от первичной ноды ко вторичной и от вторичной к первичной – каждая нода выступает клиентом в одном подключении и сервером в другом. Для взаимной аутентификации нод используется протокол mTLS. Каждая нода предъявляет свой клиентский сертификат при подключении и проверяет сертификат другой ноды. Используются два типа сертификатов:

- **Клиентские сертификаты** – для удостоверения каждой ноды. Нода-клиент предъявляет свой клиентский сертификат ноде-серверу при соединении.
- **CA-сертификаты** – определяют, каким клиентским сертификатам нода-сервер доверяет при проверке подключений.

Шаг 1. Подготовка сертификатов

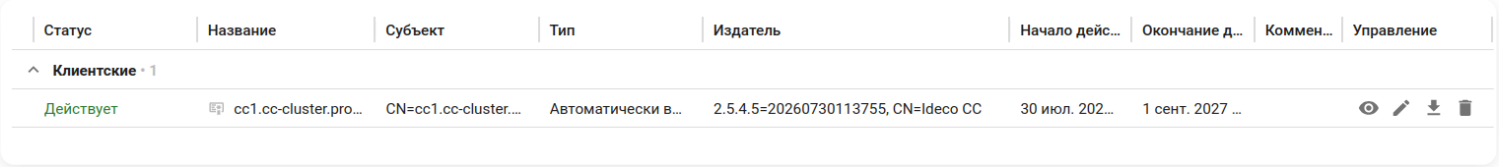
Обеспечьте наличие на обеих нодах:

- Клиентского сертификата на домен, который указан в разделе **Управление сервером** → **Дополнительно**. Сертификат будет сгенерирован автоматически и подписан корневым сертификатом Ideco Center. Также можно загрузить в **Сервисы** → **Сертификаты** клиентский сертификат, выданный вашим CA.
- CA-сертификата другой ноды. Это должен быть сертификат, которым подписан клиентский: корневой сертификат другой ноды Ideco Center или вашего CA.

Пример настройки:

1. У обеих нод в разделе **Управление сервером** → **Дополнительно** задайте доменное имя.

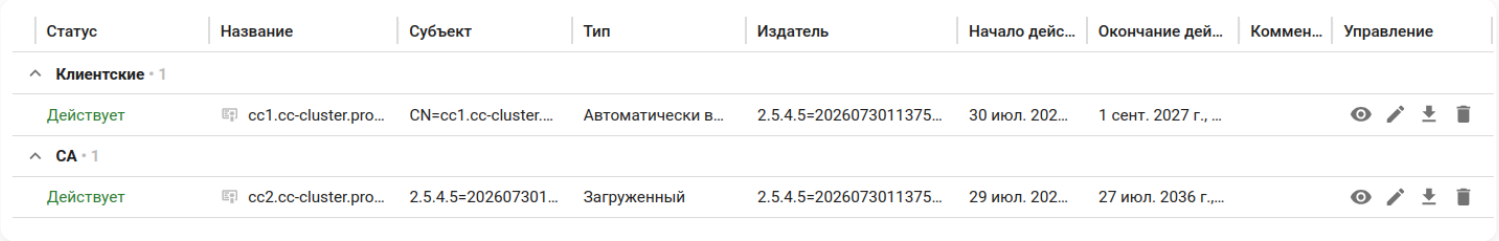
2. В разделе **Сервисы** → **Сертификаты** → **Кластеризация** текущей ноды убедитесь, что сервер выпустил клиентский сертификат на доменное имя из пункта 1. Источником подписи для сертификата будет выступать корневой сертификат Ideco Center:



Статус	Название	Субъект	Тип	Издатель	Начало дейс...	Окончание д...	Коммен...	Управление
Клиентские · 1								
Действует	cc1.cc-cluster.pro...	CN=cc1.cc-cluster....	Автоматически в...	2.5.4.5=20260730113755, CN=Ideco CC	30 июл. 202...	1 сент. 2027 ...		

3. В разделе **Сервисы** → **Сертификаты** → **Загруженные сертификаты** скачайте корневой сертификат текущей ноды.

4. В веб-интерфейсе другой ноды **Сервисы** → **Сертификаты** → **Кластеризация** нажмите **Загрузить сертификат** и выберите корневой сертификат, скачанный в пункте 3:



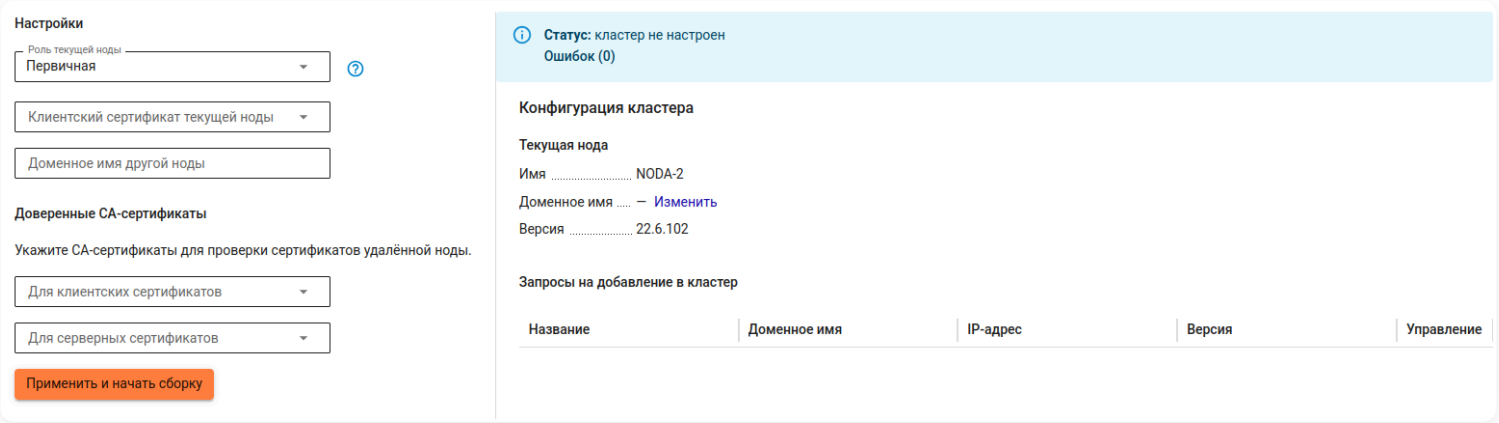
Повторите действия для другой ноды кластера.

Подробнее о работе сертификатов – в статье.

Шаг 2. Настройка и объединение нод

Определите, какой Ideco Center будет выполнять роль первичной ноды, а какой – вторичной, и на обеих нодах выполните действия:

1. Перейдите в раздел **Управление сервером** → **Кластеризация** и заполните поля:

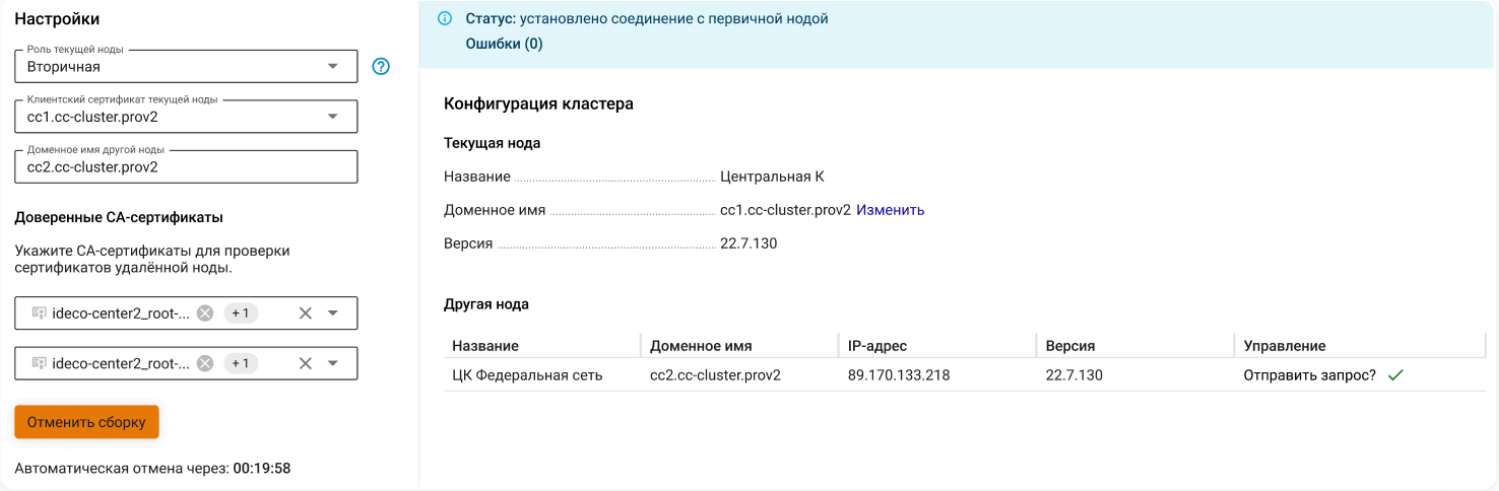


- **Роль текущей ноды** – выберите **Первичная** или **Вторичная**.
- **Клиентский сертификат текущей ноды** – выберите клиентский сертификат.
- **Доменное имя другой ноды** – введите доменное имя другой ноды.
- **Доверенные CA-сертификаты** – укажите CA-сертификаты, которым текущая нода будет доверять при проверке клиентских и серверных сертификатов другой ноды (для простейшей настройки в обоих полях выберите корневые сертификаты другой ноды, загруженные на шаге Подготовка сертификатов):
  - **Для клиентских сертификатов** – выберите CA-сертификат другой ноды.
  - **Для серверных сертификатов** – выберите CA-сертификат другой ноды.

2. Нажмите **Применить и начать сборку**.

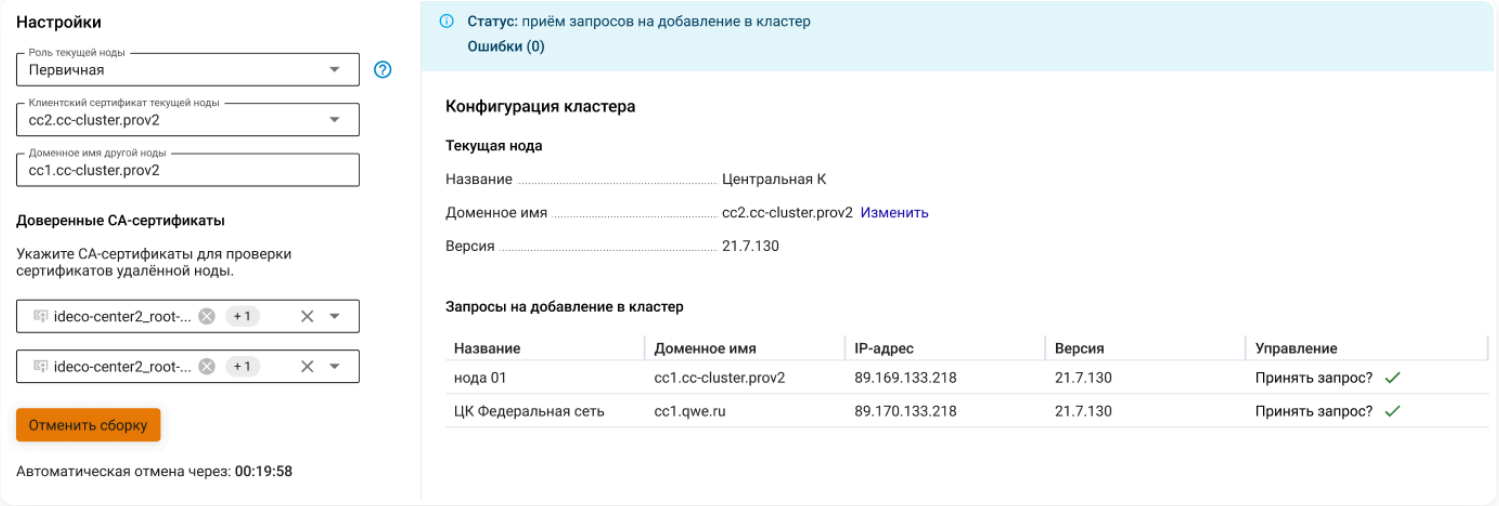
Первичная нода перейдет в режим ожидания – статус изменится на **Прием запросов на добавление в кластер**.

3. На вторичной ноде в таблице **Другая нода** появится строка с первичной нодой. Нажмите ✓, чтобы отправить запрос:



4. В открывшемся окне нажмите **Да, подтвердить**.

5. Вернитесь на первичную ноду. В таблице **Запросы на добавление в кластер** нажмите ✓, чтобы принять запрос:



6. В открывшемся окне **Подтвердить запрос на добавление в кластер** нажмите **Да, подтвердить**.

> После подтверждения все синхронизируемые данные на вторичной ноде будут удалены и заменены данными с первичной ноды. **Эта операция необратима.**

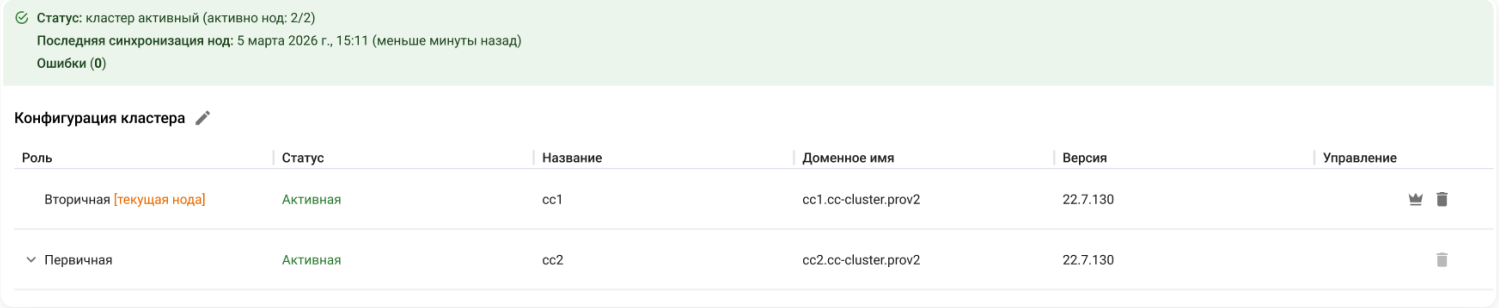
После взаимного подтверждения кластер считается созданным. Добавляемая нода получает данные с первичной и переходит в рабочий режим.

Полезные ссылки

- **Управление кластером**
- **Сертификаты**

Управление кластером

После создания кластера раздел **Управление сервером** → **Кластеризация** меняет вид. Форма настроек исчезает и отображается страница мониторинга:



Статусная строка

- **Статус** – текущее состояние кластера и число активных нод в формате N/2.
- **Последняя синхронизация нод** – время последней успешной синхронизации.
- **Ошибки** – счетчик текущих ошибок. При наличии ошибок рядом появляется ссылка **Показать** для раскрытия списка.

Статусы кластера

Статус кластера	Цвет панели	Значение
Кластер активный (активно нод: 2/2)	Зеленый	Обе ноды доступны, все соединения установлены
Кластер деградирован (активно нод: 2/2)	Оранжевый	Ноды доступны, но установлено менее двух соединений или есть ошибки
Кластер разъединен (активно нод: 1/2)	Красный	Одна нода недоступна – 0 соединений с ней
Инициализация кластера (активно нод: 0/2)	Синий	Переходное состояние: нода загружается или проходит первичную синхронизацию
Деинициализация кластера (активно нод: 0/2)	Синий	Нода выводится из кластера

Таблица Конфигурация кластера

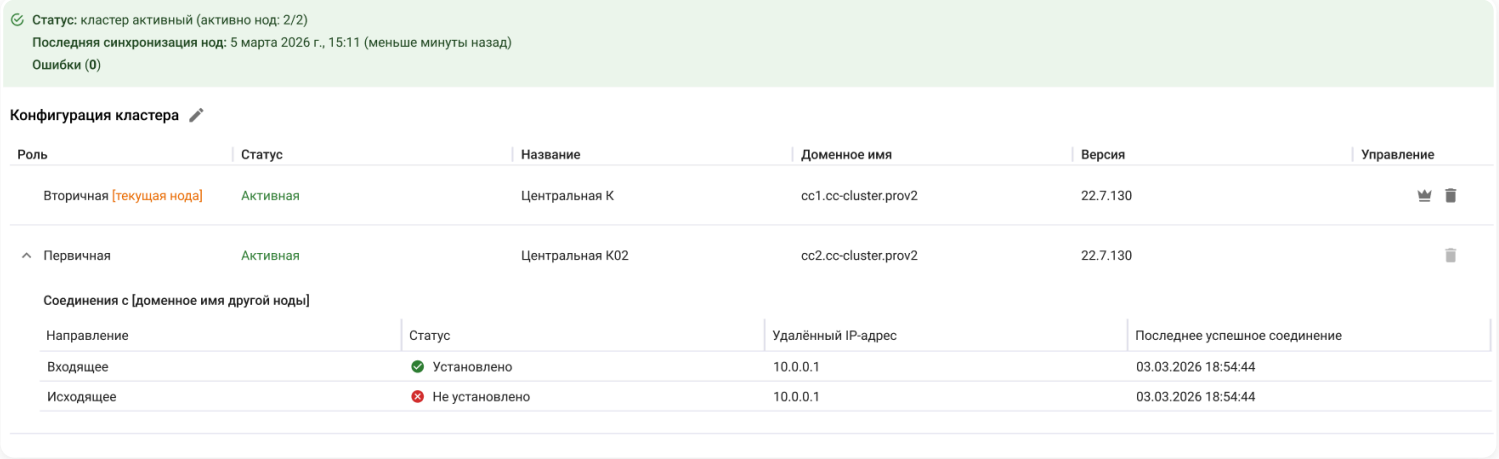
Таблица отображает информацию и состояние обеих нод кластера.

Описание столбцов

Информация о ноде:

- **Роль** – роль ноды. Текущая нода отображается первой и помечена меткой **[текущая нода]**.
- **Статус** – состояние ноды:
  - **Активная** – установлено хотя бы одно соединение.
  - **Неактивная** – соединения отсутствуют.
- **Название** – название ноды.
- **Доменное имя** – доменное имя ноды.
- **Версия** – версия ноды. При различии версий кластер не соберется, а уже собранный перейдет в состояние деградации.
- **Управление** – доступные действия для текущей ноды:
  - – назначить первичной (только на вторичной ноде).
  - – вывести из кластера.

При нажатии на ноду откроется таблица соединения этой ноды с другой нодой:



Описание столбцов

- **Направление** – направление соединения:
  - **Входящее** – другая нода подключается к текущей.
  - **Исходящее** – текущая нода инициирует подключение к другой.
- **Статус** – статус соединения:
  - **Установлено** – соединение установлено.
  - **Не установлено** – соединение не установлено.
- **Удаленный IP-адрес** – IP-адрес ноды, с которой установлено соединение.
- **Последнее успешное соединение** – дата и время последней успешной синхронизации.

Операции с кластером

Переключение ролей (захват управления)

Плановое переключение ролей может использоваться, например, для обслуживания первичной ноды.

> Прямая смена роли активной ноды недоступна – переключение выполняется захватом управления на вторичной ноде: она становится активной немедленно. Затем запускается процесс согласования со второй нодой:
>
> - Если связь между нодами есть, прежняя активная нода автоматически получает роль вторичной.
> - Если на момент захвата управления связи между нодами нет, обе ноды будут считать себя активными до восстановления связи.

Чтобы переключить роли нод, выполните действия:

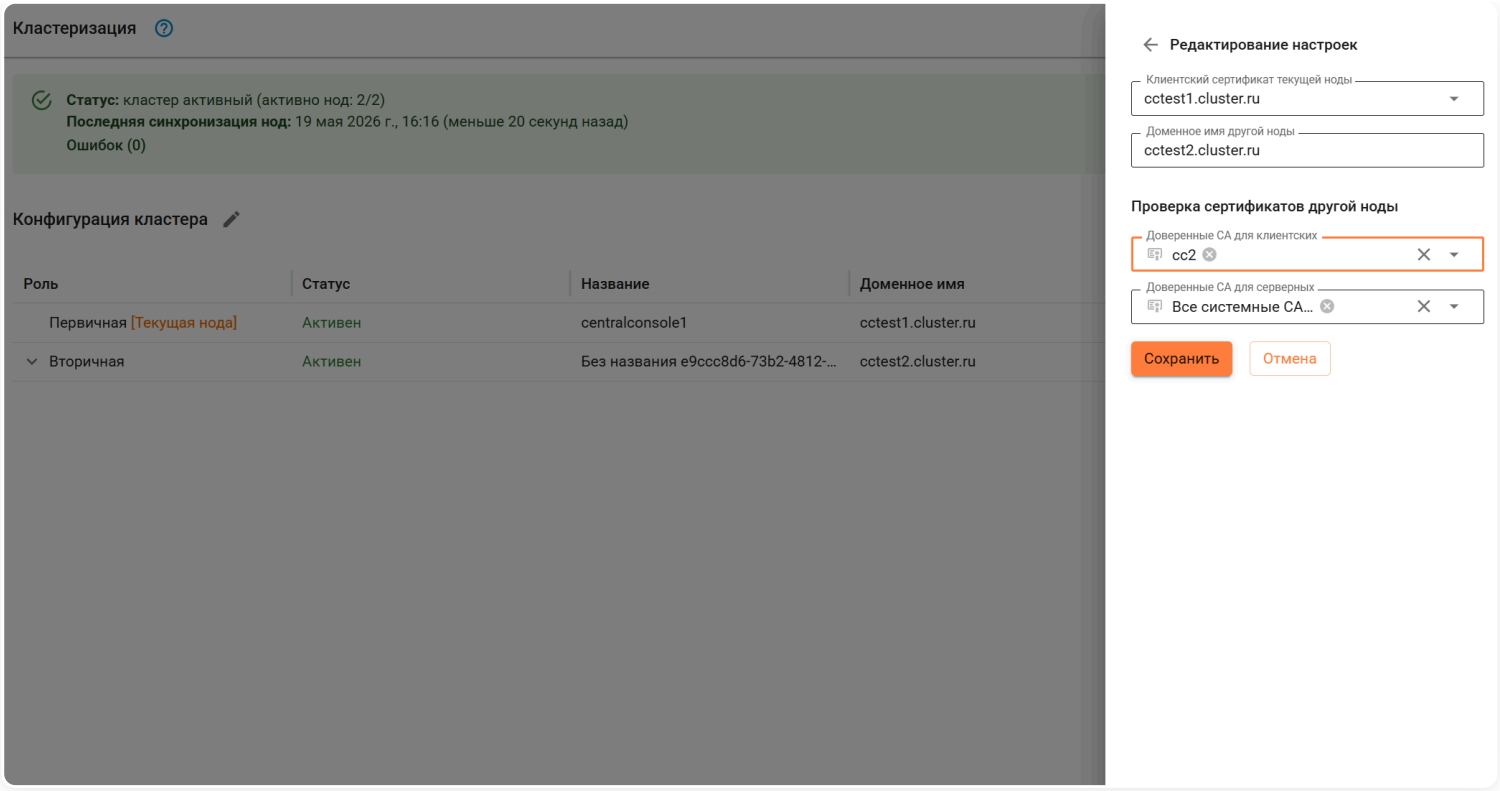
1. Убедитесь в наличии связи между нодами.

2. В столбце **Управление** напротив текущей ноды нажмите . Кнопка доступна только на вторичной ноде, если на ней уже есть синхронизированные данные.

Если на новой первичной ноде были изменения, они перезапишут данные на вторичной.

Редактирование настроек

Для редактирования настроек нажмите в заголовке таблицы:



Доступные для изменения поля:

- **Клиентский сертификат текущей ноды**
- **Доменное имя другой ноды**
- **Доверенные СА для клиентских**
- **Доверенные СА для серверных**

При необходимости внесите изменения и нажмите **Сохранить**. Соединение нод не будет разорвано.

Вывод ноды из кластера

Для вывода ноды из кластера нажмите 🗑 в столбце **Управление** в строке текущей ноды. Нода выйдет из кластера и продолжит работу как самостоятельный сервер управления.

Вывод из кластера – односторонняя операция. Вторая нода не получает уведомления и продолжает попытки подключения. Для полного разрушения кластера необходимо выполнить вывод на обеих нодах.

При выводе из кластера первичная нода сохраняет данные и подключенные устройства. Вторичная нода теряет синхронизированные данные.

Поведение кластера при сбоях

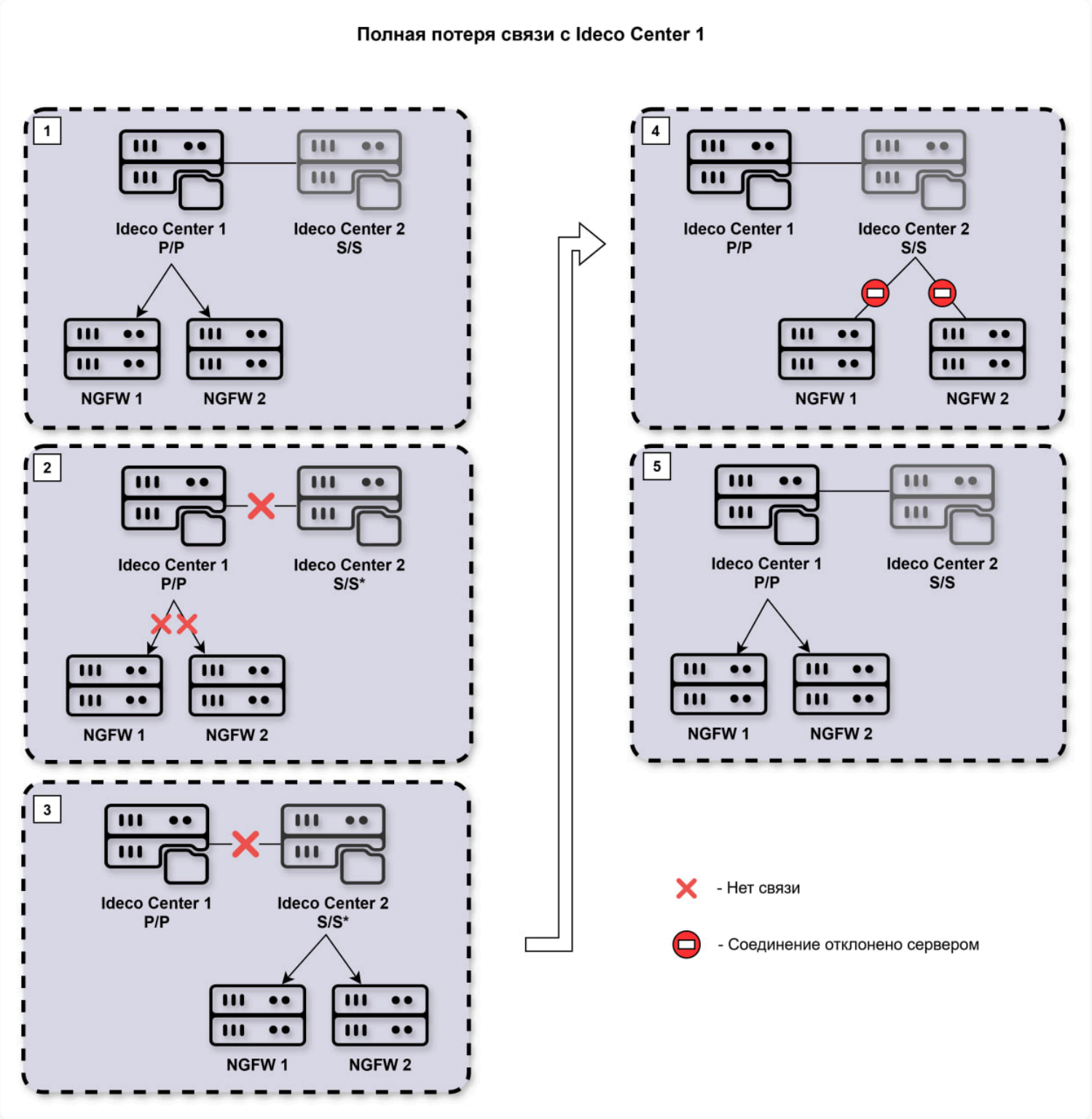
На диаграммах сценариев используются следующие обозначения:

Обозначение	Расшифровка	Поведение ноды
P/P	Первичная	Нода назначена первичной и работает в штатном режиме, принимая подключения от NGFW
S/S	Вторичная	Нода работает в штатном режиме. Нода синхронизируется с первичной, получает данные, но не принимает подключения от NGFW
S/S*	Вторичная-заместитель	Роль ноды – вторичная, но она потеряла связь с первичной и перешла в режим заместителя, начав принимать подключения от NGFW и выполнять функции первичной

Потеря связи с первичной нодой

Сценарий, при котором первичная нода становится недоступна, а вторичная нода берет на себя прием подключений от NGFW.

Возможные причины: выход из строя сервера первичной ноды, незапланированная перезагрузка, отключение электропитания, полная потеря сетевого подключения на стороне первичной ноды.



Последовательность:

1. Кластер работает штатно, NGFW подключены к Ideco Center 1 (первичная нода).

2. Ideco Center 1 (первичная нода) становится недоступен.

3. Соединение между Ideco Center 1 (первичная нода) и NGFW разрывается.

4. Ideco Center 2 (вторичная нода) после нескольких неудачных попыток восстановить соединение с Ideco Center 1 (первичная нода) переходит к роли вторичная-заместитель.

5. NGFW перебирают SRV-записи и подключаются к Ideco Center 2 (вторичная-заместитель).

6. Когда Ideco Center 1 (первичная нода) восстанавливается, Ideco Center 2 (вторичная-заместитель) обнаруживает появление первичной ноды и автоматически возвращается в режим вторичной ноды.

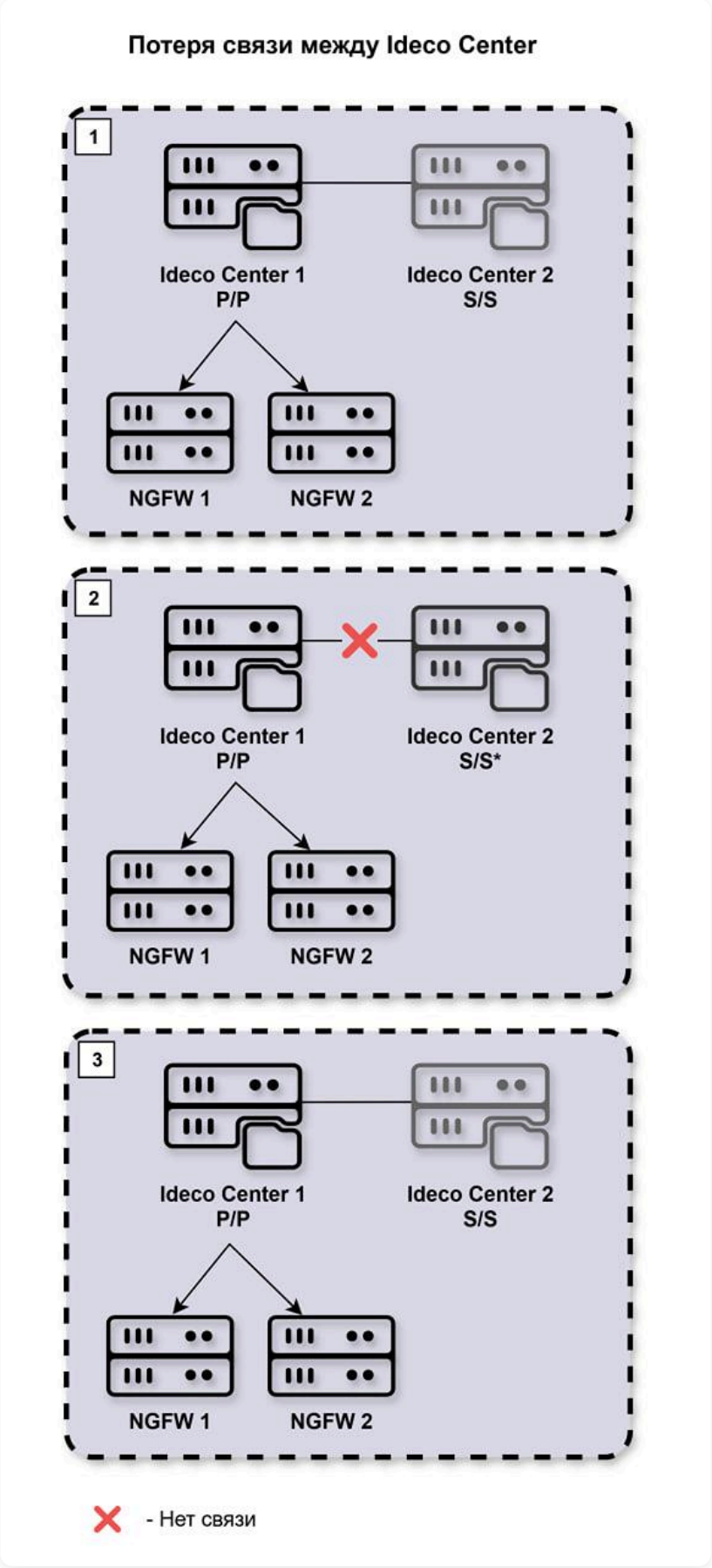
7. Все NGFW переподключаются к Ideco Center 1 (первичная нода).

На ноде с ролью вторичная-заместитель нельзя изменять конфигурацию. Если необходимо внести правки, воспользуйтесь захватом управления.

Потеря связи между нодами Ideco Center

Сценарий, при котором связь между нодами прерывается, но устройства NGFW по-прежнему видят первичную ноду.

Возможные причины: сбой на промежуточном сетевом оборудовании между нодами, проблемы с VPN-туннелем или WAN-каналом при территориально распределенном размещении, блокировка HTTPS-трафика между нодами правилами межсетевого экрана, истечение или отзыв mTLS-сертификата.



Последовательность:

1. Кластер работает штатно, NGFW подключены к Ideco Center 1 (первичная нода).

2. Связь между нодами разрывается.

3. Ideco Center 2 (вторичная нода) переходит к роли вторичная-заместитель и готов принимать подключения NGFW.

4. NGFW все еще видят Ideco Center 1 (первичная нода) и остаются подключенными к этой ноде.

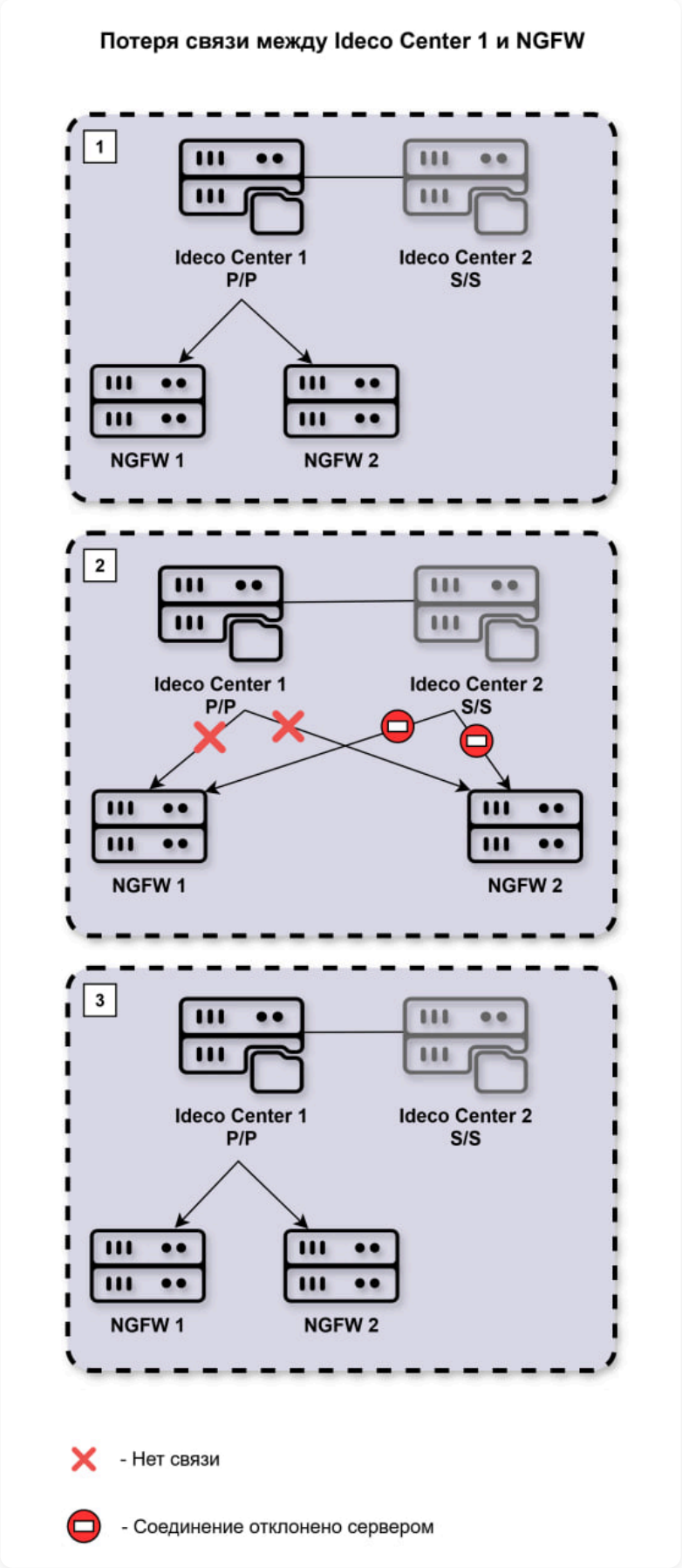
5. Когда соединение между нодами восстанавливается, Ideco Center 2 (вторичная-заместитель) возвращается к роли вторичной ноды, а кластер – в штатное состояние.

> Пока связь между нодами разорвана, синхронизация данных не выполняется. Изменения, внесенные на первичной ноде в этот период, будут переданы на вторичную при восстановлении соединения.

Потеря связи между первичной нодой и NGFW

Сценарий, при котором NGFW теряют связь с первичной нодой, но соединение между самими нодами Ideco Center сохраняется.

Возможные причины: сбой на сетевом оборудовании в сегменте между первичной нодой и NGFW, изменение маршрутов или правил фильтрации, затрагивающее трафик от NGFW к первичной ноде, проблемы с DNS-резолвингом на стороне NGFW.



Последовательность:

1. Кластер работает штатно, NGFW подключены к Ideco Center 1 (первичная нода).

2. NGFW теряют связь с Ideco Center 1 (первичная нода) и пытаются переключиться на Ideco Center 2 (вторичная нода).

3. Ideco Center 2 (вторичная нода) видит, что Ideco Center 1 (первичная нода) доступен, соединение между нодами не разорвано, поэтому не переходит к роли вторичная-заместитель и отклоняет подключения от NGFW.

4. NGFW временно не могут подключиться ни к одной ноде. Правила, примененные ранее, продолжают работать на самих устройствах.

5. При восстановлении связи NGFW переподключаются к Ideco Center 1 (первичная нода).

Это ожидаемое поведение системы. Кластер не переключается в аварийный режим, пока первичная нода доступна хотя бы по одному каналу – кластерному соединению.

Особые ситуации

Ситуация	Влияние на кластер	Как исправить
Несовпадение версий	Соединение между нодами устанавливается, но синхронизация данных не выполняется. Статус кластера изменяется на **Кластер деградирован**, в списке ошибок появляется соответствующее сообщение	Обновите обе ноды до одинаковой версии
Проблемы с сертификатами	Если сертификат истек, отозван или не проходит проверку, соединение между нодами разрывается	Замените сертификат и обновите списки доверенных CA. Соединение восстановится автоматически
Изменение доменного имени	Смена доменного имени является односторонней операцией. После смены соединение между нодами прерывается	Вручную обновите доменное имя другой ноды в настройках кластера на каждой ноде отдельно

Полезные ссылки

- **Создание кластера**
- **Сертификаты**

Требования к Ideco NGFW Novum при обновлении Center

После обновления Ideco Center до версии 23 к нему смогут подключаться только серверы NGFW Novum версии 22.1 и выше.

NGFW Novum версий ниже 22.1 после обновления Ideco Center будут отключены от него без возможности восстановления. Потребуется обновить серверы и подключить их вручную заново.

Чтобы подключенные серверы сохранились в Ideco Center, соблюдайте порядок обновления:

1. До обновления Ideco Center проверьте в разделе **Серверы** версии всех подключенных NGFW Novum и обновите серверы с версией ниже 22.1.

2. Дождитесь, пока обновленные серверы автоматически переподключатся к Ideco Center.

3. Обновите Ideco Center до версии 23. Настройки переподключившихся серверов сохранятся при миграции.

Полезные ссылки

- **Серверы**
- **Ideco Center**

Ideco Center 22.1.109

Дата выхода версии: 15.05.2026.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в телеграм-канале с разработчиками: https://telegram.me/idecoutm.
- Портал технической поддержки: support.ideco.ru.
- Telegram: ideco.bot.
- MAX: id6670208848_bot.

Скачать Ideco Center 22.

Примечание к релизу:

Ideco Center 22 предназначен для управления политиками фильтрации межсетевых экранов Ideco NGFW Novum версии 22.

С версии 22 Ideco Center лицензируется. Доступны лицензии Enterprise (коммерческая) и Enterprise-demo (бесплатная лицензия сроком на 44 дня). Подробности в статье Лицензирование.

Новые возможности

Функциональность	Описание
Управление высокопроизводительными контекстами	Добавлена поддержка централизованного управления двумя типами контекстов: классический и высокопроизводительный. Созданные правила и профили переносятся на подключенные серверы и доступны там только для просмотра. Подробности в статьях Правила трафика и Профили безопасности
Географически распределенный кластер для повышения отказоустойчивости и доступности	Добавлена возможность развертывания георасределенного кластера системы управления Ideco Center из двух нод. Конфигурация, внесенная на любом из экземпляров, автоматически синхронизируется между ними. Подробности в статьях Кластеризация и Сервисы
Сбор журналов IPS и WAF из Ideco NGFW	Доступен просмотр отчетности Ideco NGFW в Ideco Center: Журнал IPS и Web Application Firewall. Подробности в статье Отчеты и журналы
Локальные политики	Возможность настраивать правила фильтрации входящего (INPUT) трафика, направленного непосредственно на сервер Ideco Center. Подробности в статье Локальные политики

Исправленные ошибки

ID задачи	Описание
ICS-59777	Устранена ошибка, при которой переполнялись таблицы логов Ideco NGFW в Ideco Center

Ideco Center 22.6.105

Примечания к релизу

Дата выхода версии: 07.08.2026.

Техническая поддержка и обратная связь (поможет нам улучшить продукт):

- Обсудить версию в Telegram-канале с разработчиками: https://t.me/idecoutm
- Портал технической поддержки: https://support.ideco.ru/
- Telegram: ideco.bot
- MAX: id6670208848_bot

Скачать Ideco Center 22

Если на подключенных серверах установлен Ideco NGFW Novum версии 22.4 или новее, для корректной передачи журналов серверов на Ideco Center обновите Центральную консоль до версии 22.6.

Подготовка к обновлению на версию 23

Изменения с версии 23:

- **Системный контекст** и все VCE могут быть подключены только к одному Ideco Center, а управление подключением выполняется только из **Системного контекста**. VCE с несовпадающими подключениями при обновлении будут автоматически отключены. Перед обновлением приведите конфигурацию к одному виду. Подробности – в статье Подготовка к обновлению VCE, подключенных к Ideco Center.
- Раздел **Администраторы** будет доступен только в **Системном контексте**. Управление учетными записями и доступами администраторов VCE станет централизованным. Ознакомьтесь с особенностями переноса администраторов из VCE в Системный контекст в статье Подготовка к миграции администраторов из VCE.
- К Ideco Center версии 23 смогут подключаться только серверы Ideco Center версии 22.1 и выше. Серверы более младших версий будут отключены от Ideco Center без возможности восстановления. Чтобы подключенные серверы сохранились, соблюдайте порядок обновления.

Безопасность

- Закрыты уязвимости CVE-2026-31431, CVE-2026-32792, CVE-2026-33278, CVE-2026-40622, CVE-2026-41292, CVE-2026-42534, CVE-2026-42923, CVE-2026-42944, CVE-2026-42959, CVE-2026-42960, CVE-2026-43333, CVE-2026-44390, CVE-2026-44608, CVE-2026-46300 в различных компонентах продукта.
- Исправлена уязвимость ядра Linux GRO Frag (класс Copy Fail) в подсистеме GRO, связанная с локальным повышением привилегий до root (не эксплуатируется удаленно, требует выполнения локально).

Улучшения и оптимизация

- В правилах **Межсетевого экрана** FORWARD для **Высокопроизводительных контекстов** добавлено поле **Название**.
- В правилах **Межсетевого экрана** для **Высокопроизводительных контекстов** во всплывающей подсказке профиля безопасности добавлена кнопка перехода к профилю.
- Добавлена поддержка сжатия данных в журнале **Межсетевого экрана**, что уменьшает занимаемое место на диске.
- Время истечения сертификатов в разделе **Сертификаты** теперь отображается по серверному времени.
- В форме добавления/редактирования **Внешнего DNS-сервера** доступны все сетевые интерфейсы.

Исправленные ошибки

ID задачи	Описание	Модуль
CC-844	Устранена ошибка, из-за которой при добавлении правила в **Контент-фильтр** пропадала пользовательская категория	Контент-фильтр

CC-960	Устранена ошибка при скрытии столбцов в таблице **Серверы**	Серверы
CC-866	Устранена ошибка, из-за которой группу с сервером внутри нельзя было переместить в другую группу	Серверы
CC-922 ICS-65098	Исправлен доступ в разделы веб-интерфейса для администраторов с ролями **Администратор межсетевого экрана** и **Администратор настройки доступа**	Администраторы
ICS-66932	Устранена ошибка, из-за которой в интерфейсе отображалось сообщение об отсутствии включенных модулей в лицензии	Лицензия
ICS-66376	Исправлена ошибка при применении фильтра в журнале **Система**	Отчеты и журналы
ICS-66265	Исправлена ошибка 404 при наведении на идентификатор сигнатуры в журнале IPS	Отчеты и журналы
ICS-64117	Исправлено отображение значений SD-WAN в snmpwalk: вместо алиасов теперь возвращаются реальные значения	SNMP