Пользовательская документация

Ideco NGFW

февр. 19, 2025

Оглавление

,

1. Возможности Ideco NGFW:

- Межсетевой экран
- Система предотвращения вторжений
- Контент-фильтр
- Контроль приложений
- Многоуровневая антивирусная и антиспам-проверка трафика
- Защита от ботнетов, фишинга и spyware
- VPN site-to-site (GRE, IPSec) и client-to-site (IKEv2/IPSec, L2TP/IPSec, SSTP, Wireguard) с 2FA
- Логирование действий администратора
- Управление через Ideco Center
- Отчетность по трафику пользователей и событиям безопасности
- Интеграция с Microsoft Active Directory, ALD Pro, Samba DC, SIEM и DLP-системами

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

Техническое описание Ideco NGFW доступно по ссылке.

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

Скачать Ideco NGFW можно в личном кабинете.

Видеодокументация доступна на нашем YouTube-канале.

2. Лицензирование

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

У лицензии Ideco NGFW есть три основные характеристики:

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

Подсказка: Особенности лицензирования:

- Количество приобретенных по лицензии учетных записей ограничивает число авторизованных пользователей;

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

2.1 Виды лицензий

В Ideco NGFW доступны лицензии:

Enterprise-demo

Enterprise-demo - бесплатная лицензия сроком на 40 дней.

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

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

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

- Отключена авторизация пользователей и фильтрация трафика;
- Заблокированы FORWARD- и INPUT-трафик. Кроме доступа до my.ideco.ru;
- Доступен перехват DNS-запросов и подключение по SSH при включении удаленного помощника.

Enterprise

Enterprise - коммерческая лицензия.

- Количество авторизованных пользователей ограничено лицензией
- Бессрочное право на использование Ideco NGFW
- Включает в себя годовую подписку **Security Update**

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

- Обновления на новые версии Ideco NGFW;
- Расширенный модуль **Контент-фильтр**;
- Модуль **Предотвращение вторжений**;
- Модуль **Контроль приложений**;
- Автоматическое обновление баз модулей;
- Техническая поддержка.

Технологии Лаборатории Касперского приобретаются отдельно в отделе продаж.

2.1.1 По истечении срока подписки Security Update доступ к большинству функций Ideco NGFW сохраняется. Исключением являются:

- **Контроль приложений** - работа модуля отключается;
- **Контент-фильтр** - доступны только пользовательские категории;
- **Предотвращение вторжений** - доступна старая отчетность, но защита периметра отключается;
- **Техническая поддержка** - недоступна.

Free

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

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

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

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

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

- Отключена авторизация пользователей и фильтрация трафика;
- Заблокированы FORWARD- и INPUT-трафик. Кроме доступа до my.ideco.ru;
- Доступен перехват DNS-запросов и подключение по SSH при включении удаленного помощника.

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

2.1.2 Просмотр информации о лицензиях

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

- В личном кабинете *MY.IDECO* в разделе **NGFW -> Лицензирование**. Здесь также можно получить лицензию, посмотреть информацию о зарегистрированных серверах и настроить связь лицензий с серверами;
- В разделе **Управление сервером -> Лицензия** веб-интерфейса Ideco NGFW.

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

3. Системные требования и источники обновления данных Ideco NGFW

Обязательные условия для работы с Ideco NGFW:

1. Поддержка UEFI;

2. Для виртуальных машин используется фиксированный, а не динамический размера хранилища и оперативной памяти;

3. Отключенный режим Legacy, может называться CSM (Compatability Support Module);

4. Отключенная опция Secure Boot в UEFI.

3.1 Минимальные системные требования

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

Комплектующие	Системные требования
Процессор	Intel i3/i5/i7/i9/Xeon и AMD FX/Ryzen/EPYC с поддержкой SSE 4.2 (минимум 4 ядра)
Объем оперативной памяти	16 ГБ (16-64 ГБ в зависимости от количества пользователей)
Дисковая подсистема	SSD объемом 150 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe. Дополнительный SSD при использовании почтового сервера
Сеть	Две сетевые карты (или два сетевых порта) 1/10/100 ГБ. Рекомендуется использовать карты на чипах Intel
Гипервизоры	VMware, Microsoft Hyper-V (виртуальные машины 2-го поколения), VirtualBox, KVM, Citrix XenServer, Proxmox VE
Дополнительно	Монитор и клавиатура
Замечания	Обязательна поддержка UEFI. 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

Для оптимального выбора аппаратной платформы обратите внимание на *рекомендации* по подбору оборудования для Ideco NGFW. Примерный объем необходимого места на диске для хранения статистики веб-отчетности для 1000 пользователей за 1 год составляет 10-15 Гб.

Подсказка: Рекомендуем использовать процессоры Intel минимум 4 поколения Haswell (2013г.).

Предупреждение: Гарантируем работу Ideco NGFW с конечными устройствами только на версиях ОС с последними обновлениями.

3.2 Примеры конфигураций

Примеры нескольких типов конфигураций в зависимости от количества пользователей представлены ниже в таблице.

Подсказка: Представленные типы конфигураций относятся ко всем функциональностям продукта.

Количество пользователей	Модель процессора	Объем оперативной памяти	Дисковая подсистема	Сетевые адаптеры
до 100	Intel Core i3 или совместимый	16 ГБ	150 ГБ	2 шт.
до 350	Intel Core i5 или совместимый	16 ГБ	240 ГБ	2 шт.
до 1000	Intel Core i7, Xeon-E, Xeon Scalable от 8 ядер или совместимый	32 ГБ	480 ГБ	2 шт.
от 1000 до 3000	Intel Xeon Silver 4214R или совместимый	64 ГБ	480 ГБ	2 шт.
от 3000	Xeon Gold 6238R 28 Cores или совместимый	64 ГБ	480 ГБ	2 шт.

Подсказка: Рекомендуемая дисковая подсистема - PLP, SSD с защитой данных при сбое в питании. Например, Kingston DC1000B (SEDC1000BM8/240G).

3.3 Источники обновлений данных

Ideco NGFW получает обновления из следующих источников:

- Отсылка уведомлений в личный кабинет/телеграм-бот: alerts.v18.ideco.dev;
- Обновление баз **Контент-фильтра**: content-filter.v18.ideco.dev;
- Отсылка анонимной статистики: gatherstat.v18.ideco.dev;
- Обновления баз GeoIP: ip-list.v18.ideco.dev;
- Обмен информации о лицензии: license.v18.ideco.dev;
- Отправка отчетов по почте: send-reports.v18.ideco.dev;
- Обновления suricata: suricata.v18.ideco.dev;
- Обновления системы: sysupdate.v18.ideco.dev;
- Синхронизация времени: ntp.ideco.ru;
- Антивирус Касперского для обновления баз использует список серверов, указанный на официальном сайте «Лаборатории Касперского».

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

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

3.4 Программно-аппаратный комплекс (ПАК)

Описание линейки программно-аппаратных комплексов доступно по ссылке.

Сертифицированные ПАК не имеют интеллектуальный интерфейс управления платформой (IPMI).

4. Техническая поддержка

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.

Подсказка: Подробнее о подписке на техническую поддержку и обновления можно почитать на сайте компании «Айдеко».

4.1 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.

4.2 Способы обращения

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

4.3 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.

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

4.4 Информация о поддержке версий Ideco NGFW

4.4.1 Уровни поддержки

Обозначения:

- ❓ - поддержка не гарантируется. Стараемся поддерживать максимально долго, но гарантий нет;
- ✅ - поддержка гарантируется.

-	Полная поддержка	Частичная поддержка	Минимальная поддержка
Автообновление системы	✅	✅	✅
Обновление баз: - Предотвращение вторжений;- Контент фильтр, - IPLIST;- GeoIP;- ClamAV (до 17 версии включительно)	✅	❓	❓
Антивирус Касперского	Узнавать в Лаборатории Касперского	Узнавать в Лаборатории Касперского	Узнавать в Лаборатории Касперского
Антивирус и антиспам Касперского для почты	Узнавать в Лаборатории Касперского	Узнавать в Лаборатории Касперского	Узнавать в Лаборатории Касперского
Сигнатуры IPS	Узнавать в Лаборатории Касперского	Узнавать в Лаборатории Касперского	Узнавать в Лаборатории Касперского
Исправление не критичных багов (например, ошибка в тексте)	✅	❓	❓
Баги безопасности (CVE)	✅	✅	❓
Исправление критических багов (влияют работу продукта в целом или отдельного модуля)	✅	✅	❓
Техническая поддержка (простое обращение)	✅	✅	❓
Техническая поддержка (сложное обращение)	✅	❓	❓
Документация	✅	✅	❓

4.4.2 Сроки поддержки

Версия Ideco NGFW	Дата релиза	Полная поддержка	Частичная поддержка	Минимальная поддержка
7.9.X	01.11.2019	01.01.2023	01.01.2023	01.11.2024
8	08.09.2020	01.01.2023	01.01.2023	08.09.2025
9	28.12.2020	01.01.2023	01.01.2023	28.12.2025
10	30.07.2021	01.01.2023	01.01.2023	30.07.2026
11	03.11.2021	01.01.2024	01.01.2024	03.11.2026
12	04.05.2022	01.01.2024	01.01.2024	04.05.2027
13	01.09.2022	01.01.2024	01.01.2024	01.09.2027
14	27.01.2023	01.01.2024	01.01.2024	27.01.2028
15	29.08.2023	01.07.2024	01.07.2024	29.08.2028
16	28.12.2023	01.10.2024	01.01.2025	28.12.2028
17	07.05.2024	01.01.2025	01.06.2025	07.05.2029
18	11.10.2024	01.05.2025	01.10.2025	11.10.2029

5. Рекомендации при первоначальной настройке

5.1 Основное

Рекомендуемая последовательность шагов для минимальной настройки Ideco NGFW:

1. Зарегистрируйтесь на my.ideco.ru. Это позволит управлять лицензиями, скачивать загрузочные образы всех продуктов, разрабатываемых компанией Айдеко, и другое.

2. Скачайте загрузочный образ продукта из *личного кабинета MY.IDECO*.

3. Определитесь с устройством, на которое собираетесь устанавливать Ideco NGFW, и выполните предварительные действия. Ideco NGFW можно устанавливать как на гипервизоры, так и на отдельный сервер.

4. Установите Ideco NGFW на устройства, создайте учетную запись администратора.

5. Выполните первоначальную настройку Ideco NGFW.

6. Зарегистрируйте сервер на my.ideco.ru и получите лицензию.

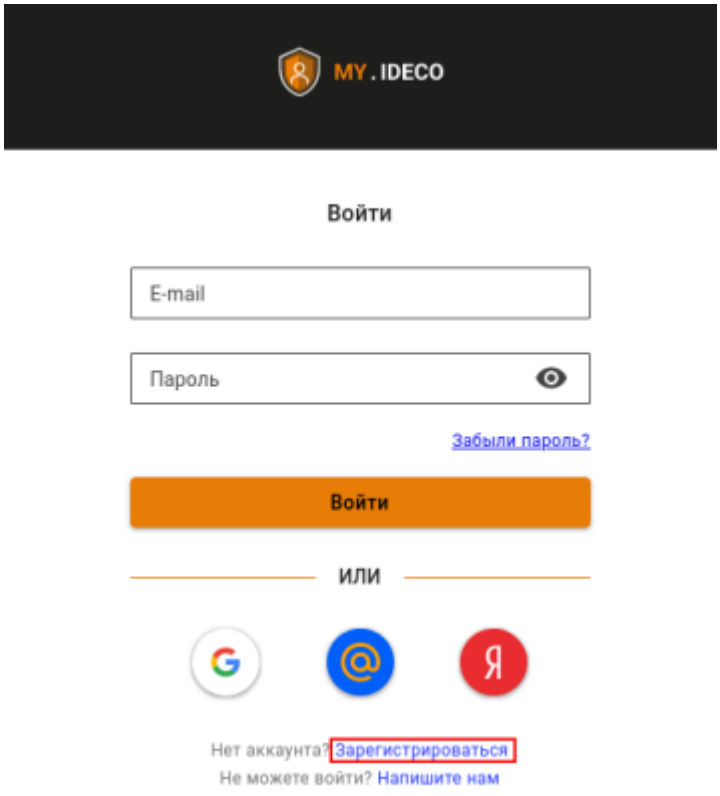
7. Создайте учетные записи пользователей и настройте авторизацию, чтобы получить доступ в интернет через Ideco NGFW. Более подробная информация представлена в *статье*.

6. MY.IDECO.RU

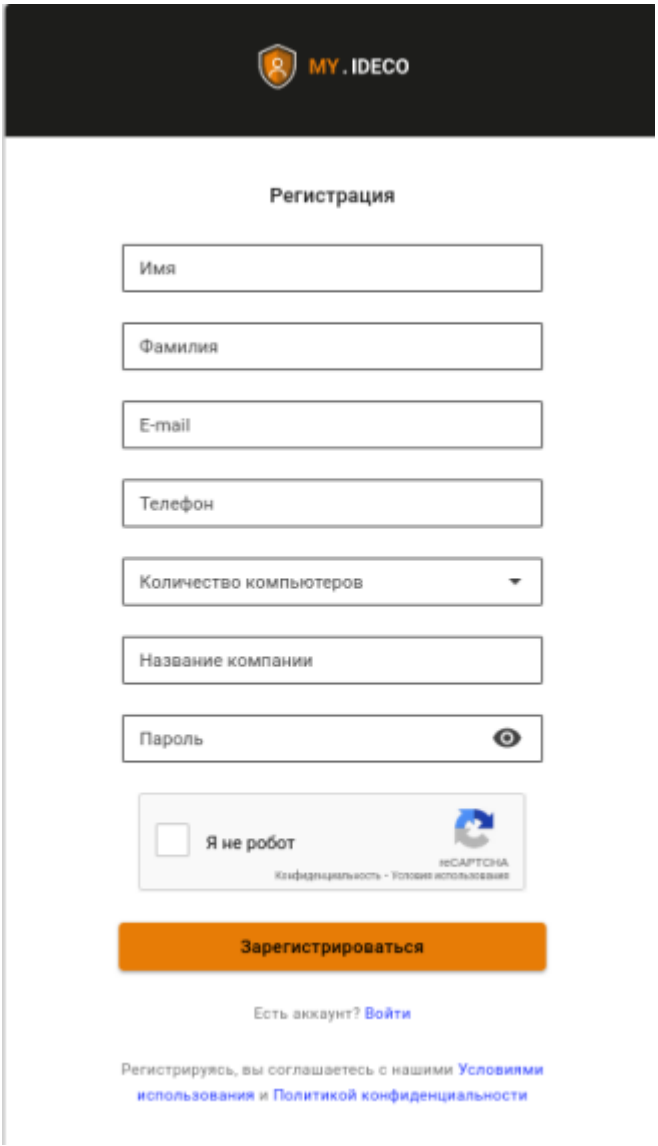
Возможности MY.IDECO

Перед загрузкой образа системы зарегистрируйтесь на my.ideco.ru:

1. Зайдите на my.ideco.ru и нажмите **Зарегистрироваться**:



2. Укажите свои личные данные и данные компании:



3. Подтвердите электронную почту, следуя инструкциям в письме.

Подсказка: Адрес электронной почты используется в качестве логина на **my.ideco.ru** и для восстановления пароля.

6.1 Загрузка образа Ideco NGFW

Перед установкой на устройство скачайте образ системы с my.ideco.ru:

1. Перейдите в раздел **NGFW** на вкладку **Скачать**.

2. Найдите образ Ideco NGFW и нажмите **Скачать**.

Для установки на устройство следуйте шагам в *статье*.

7. Настройка программно-аппаратных комплексов Ideco NGFW

Если вы используете ПАК Ideco NGFW, для удаленного управления аппаратной платформой можно использовать IPMI (Intelligent Platform Management Interface) - интеллектуальный интерфейс для управления

и администрирования серверов.

IPMI поддерживают модели:

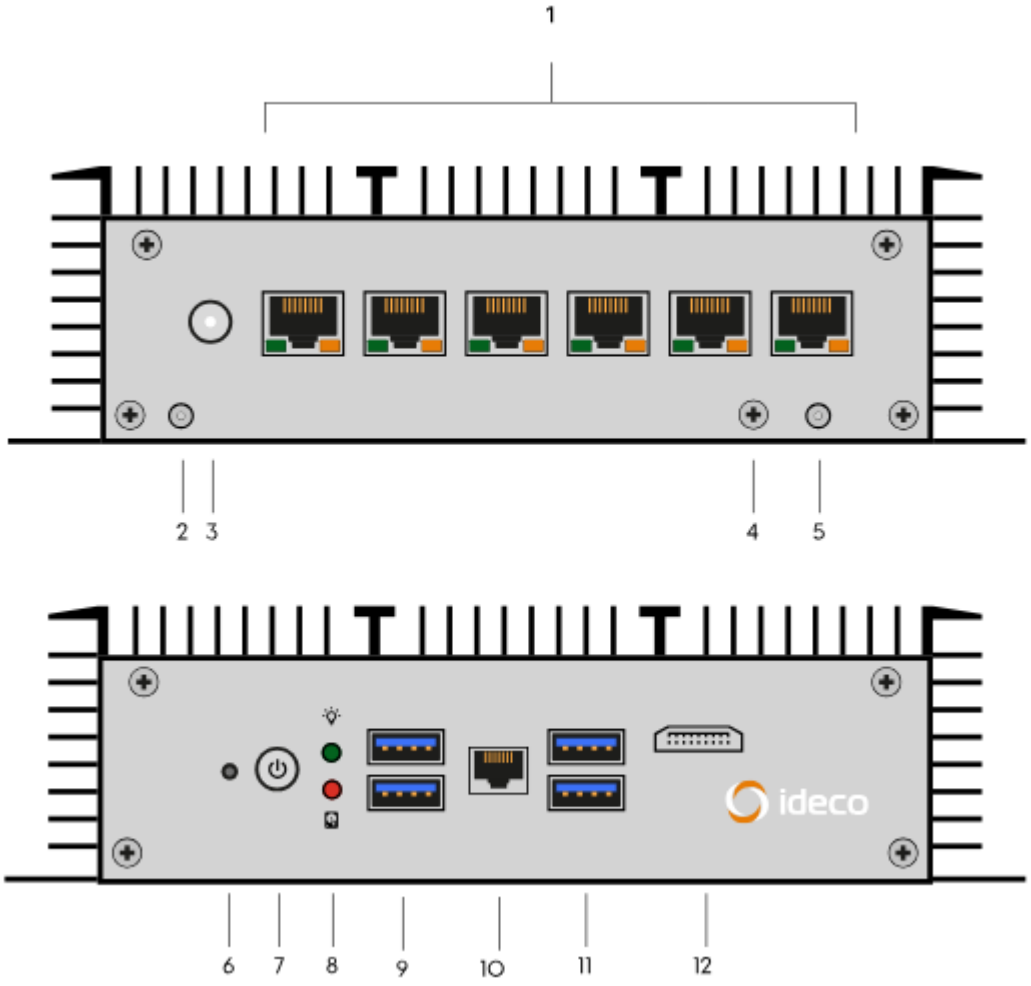
- Ideco NGFW MX;
- Ideco NGFW LX;
- Ideco NGFW LX+.

Для настройки Ideco NGFW SX+ перейдите к *разделу*.

7.1 Описание панелей программно-аппаратных комплексов Ideco NGFW

Внешний вид серверов может отличаться от иллюстраций.

Ideco NGFW SX+:



1. Шесть портов LAN (RJ-45);
2. Заглушка для антенны Wi-Fi (RF-разъем);
3. Входной разъем постоянного тока (DC input);
4. Крепление для заземления;
5. Заглушка для антенны Wi-Fi (RF-разъем);
6. Кнопка перезагрузки;
7. Кнопка питания;

8. Светодиодные индикаторы: * жесткий диск; * питание.

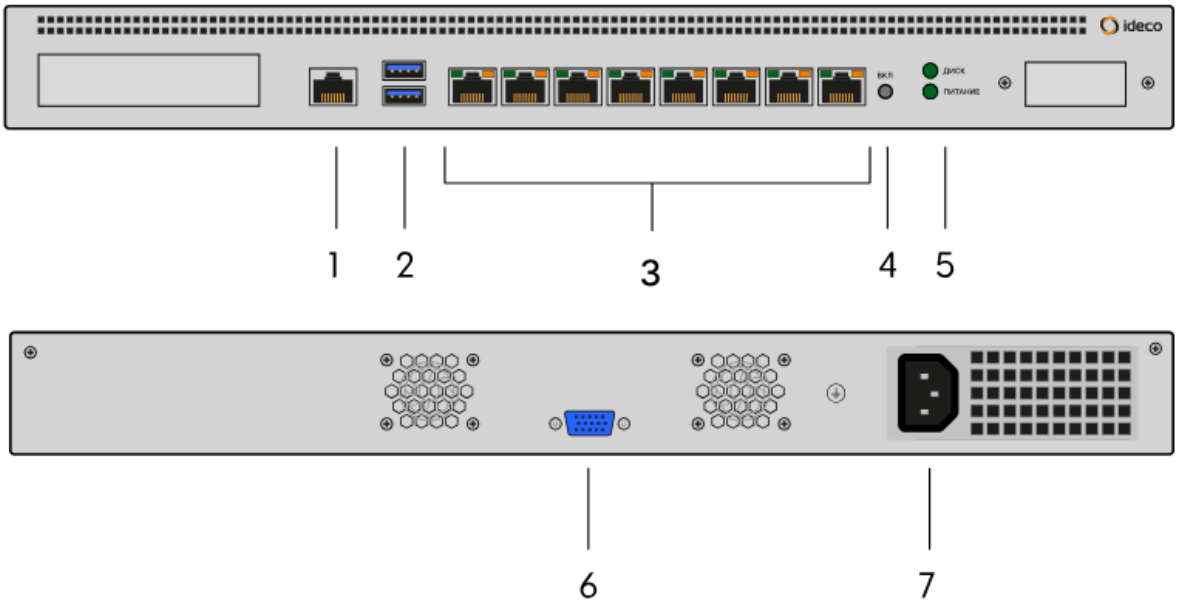
9. Порт USB 3.0;

10. Консольный порт (COM);

11. Порт USB 3.0;

12. HDMI-разъем.

Ideco NGFW MX:



1. Консольный порт;

2. Два порта USB 3.0;

3. Восемь портов LAN (RJ-45);

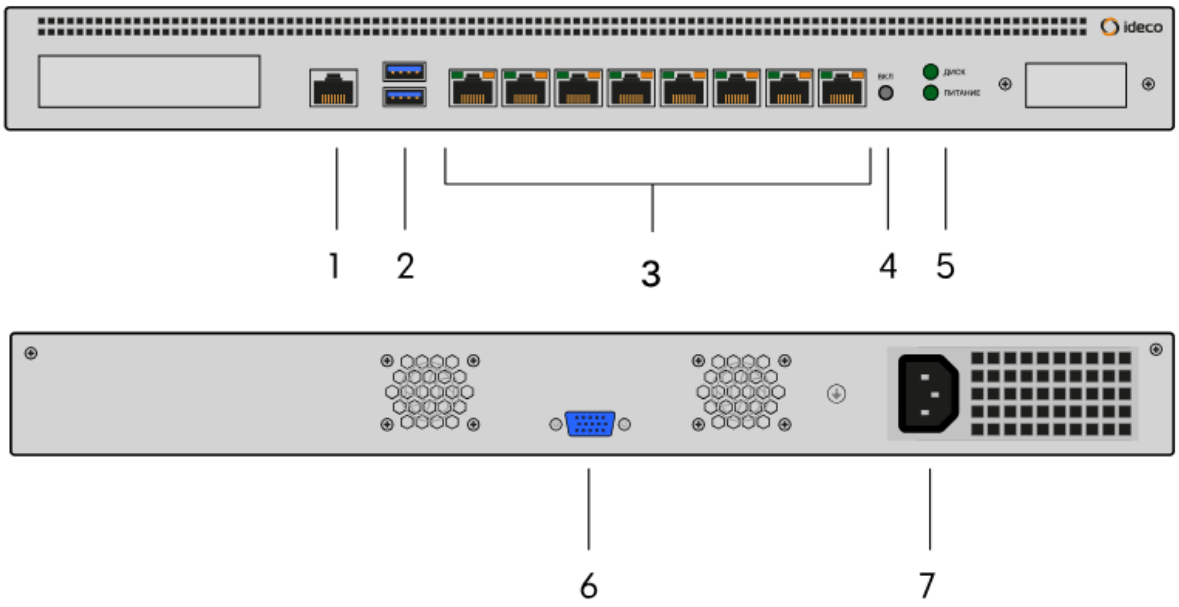
4. Кнопка питания;

5. Светодиодные индикаторы: * жесткий диск; * питание.

6. Разъем VGA;

7. Входной разъем питания IEC C14.

Ideco NGFW LX:



1. Консольный порт;

2. Два порта USB 3.0;

3. Восемь портов LAN (RJ-45);

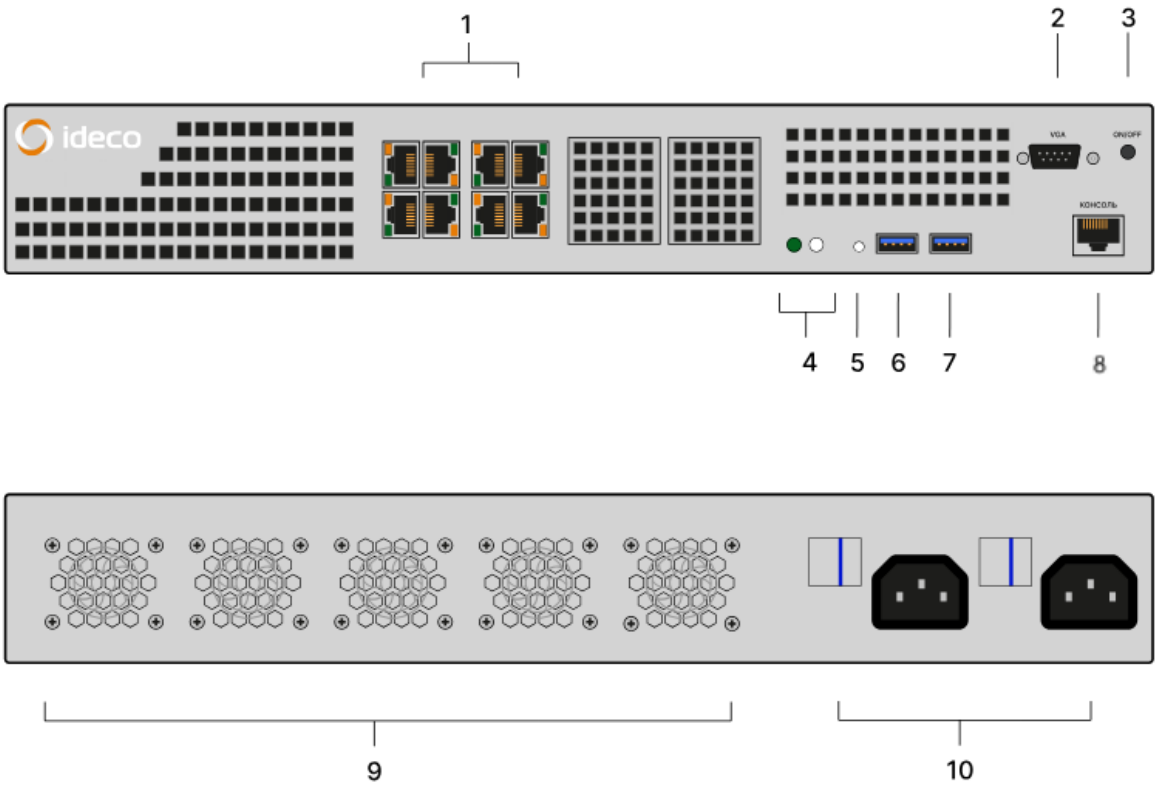
4. Кнопка питания;

5. Светодиодные индикаторы: * жесткий диск; * питание.

6. Разъем VGA;

7. Входной разъем питания IEC C14.

Ideco NGFW LX+:



1. Восемь портов LAN (RJ-45);

2. Разъем VGA;

3. Кнопка включения/выключения;

4. Индикаторы: * питание; * sys.

5. Кнопка перезагрузки;

6. Порт USB 3.0;

7. Порт USB 2.0;

8. Консольный порт;

9. Вентиляторы;

10. Два входных разъема питания IEC C14.

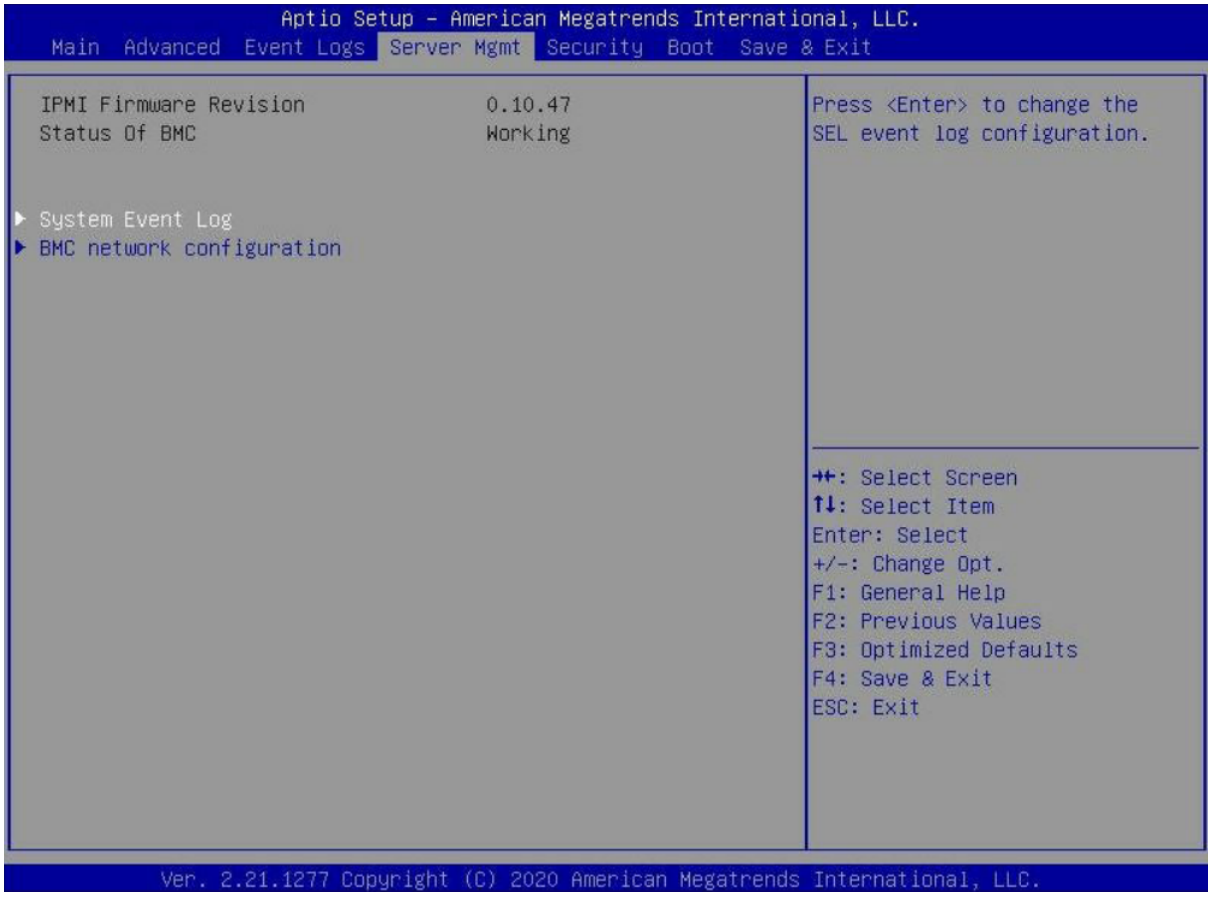
Подсказка: Внешний вид интерфейса UEFI может различаться в зависимости от версии прошивки UEFI или модели/ревизии аппаратной платформы Ideco.

7.2 Настройка IPMI

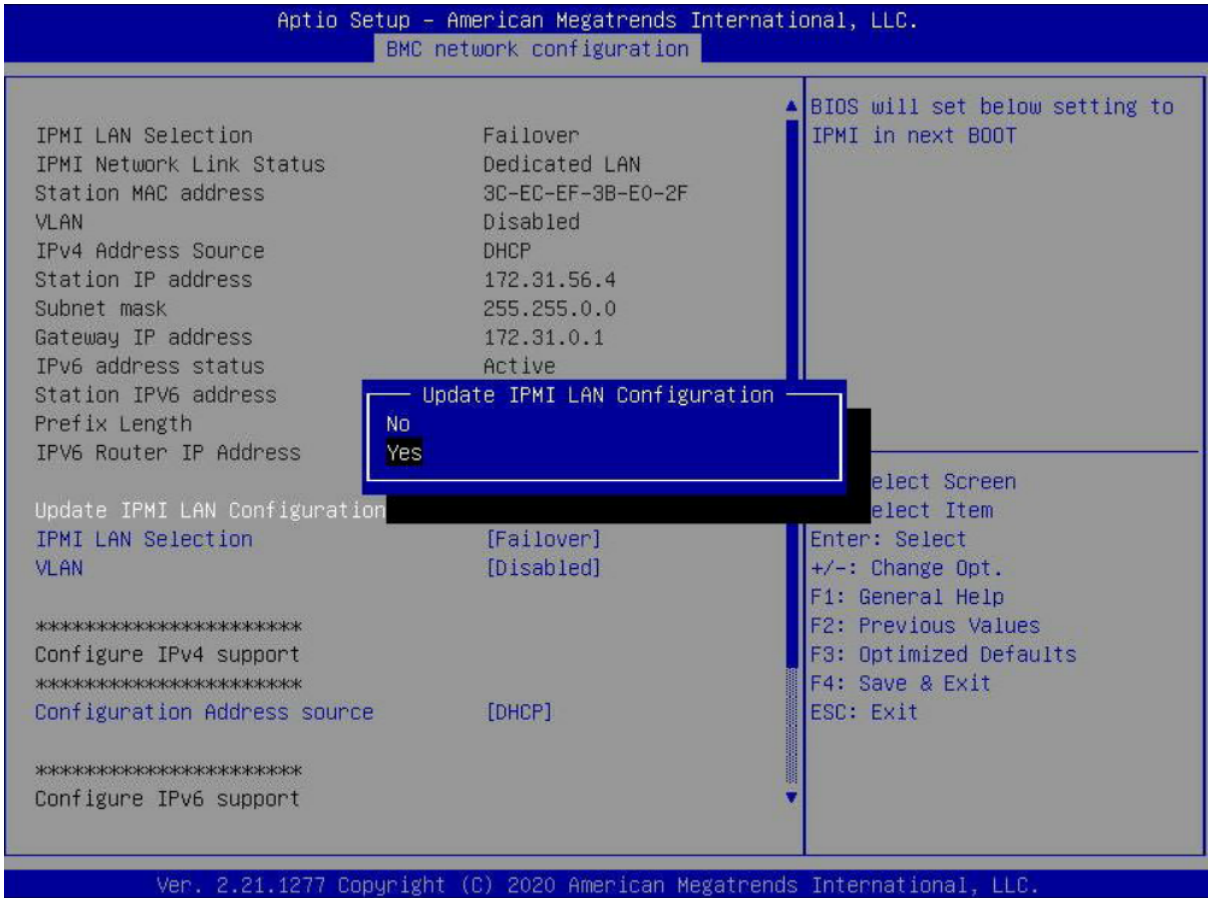
1. Подключите ноутбук или другое устройство к порту IPMI/SHARED сервера.

2. Включите сервер, нажав клавишу *Del*, чтобы войти в меню UEFI (для модели SX+ - клавиша *F2*).

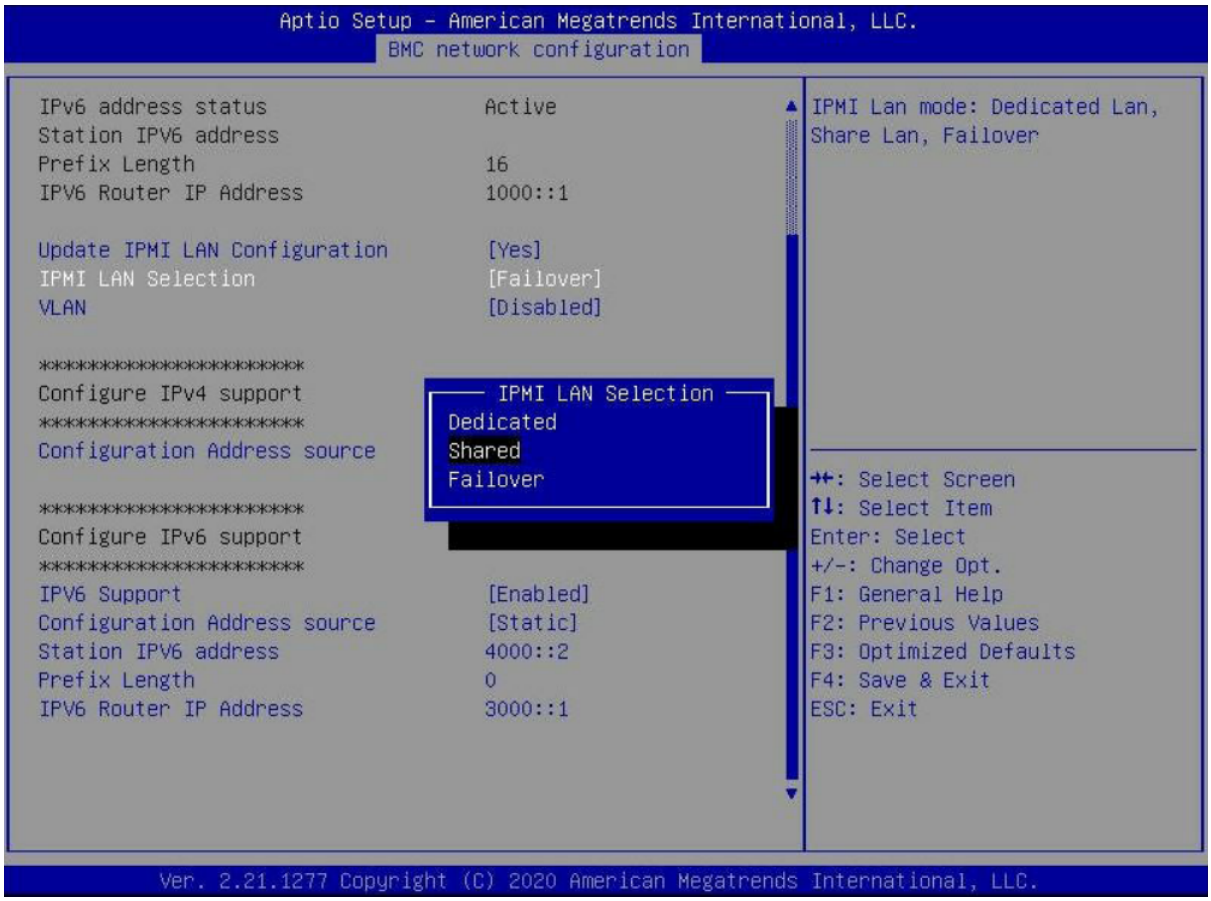
3. Перейдите на вкладку **Server Mgmt** (для навигации в UEFI используйте клавиши со стрелками, для выбора - *Enter*, для возврата к предыдущим экранам - *Esc*) и выберите **BMC Network Configuration**:



4. Перейдите к пункту **Update IPMI LAN Configuration** и выберите **Yes**:

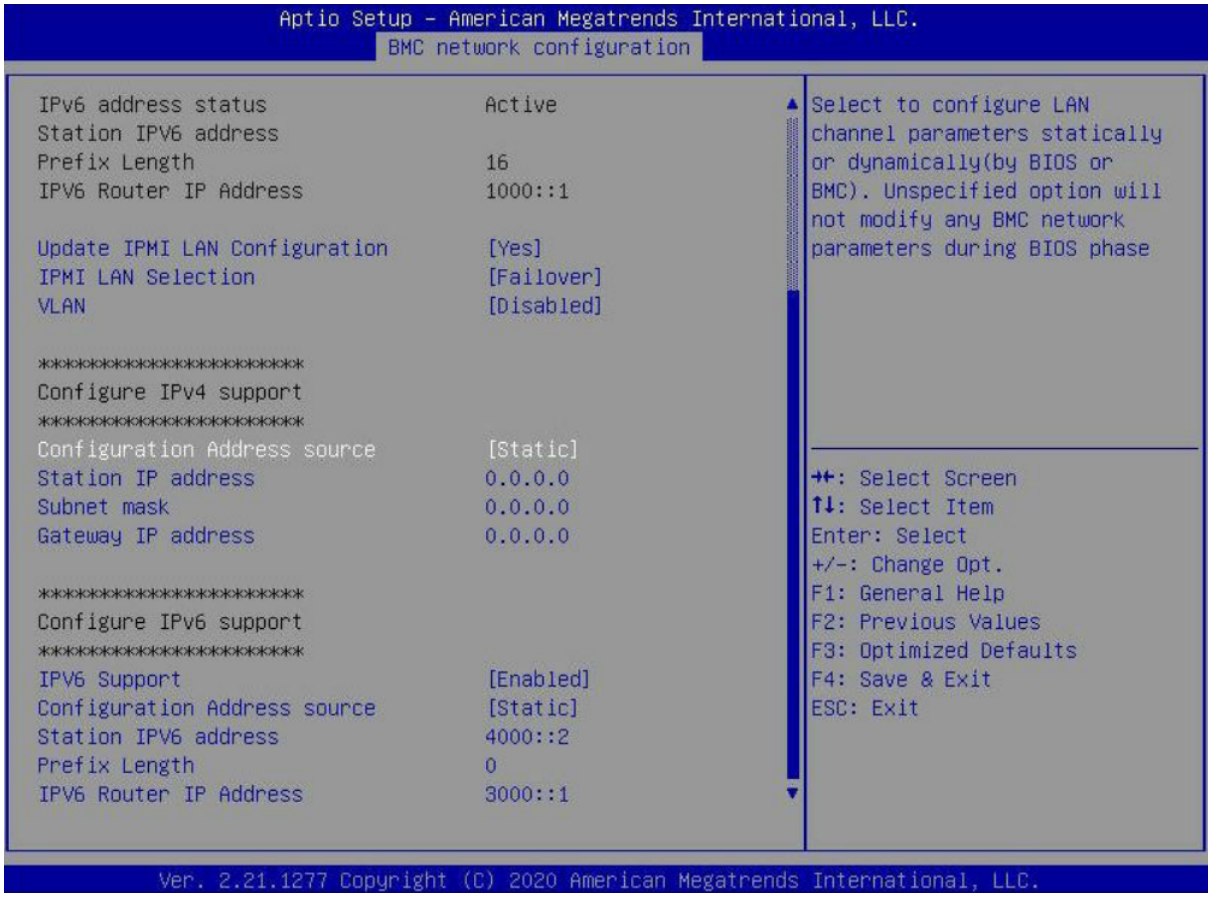


5. Перейдите к пункту **IPMI LAN Selection**, выберите необходимый режим:



- **Dedicated** - используется выделенный сетевой интерфейс на материнской плате для IPMI;
- **Shared** - используется сетевой интерфейс LAN1 для IPMI и для основного трафика;
- **Failover** - если сетевой интерфейс IPMI подключен (link up), то он и будет использоваться; если не подключен, то будет использоваться сетевой интерфейс LAN1.

6. Выберите **Configuration Address Source** и установите значение **Static** или **DHCP**. Если в полях **Station IP Address**, **Subnet Mask** и **Gateway IP Address** отобразятся `0.0.0.0`, то эти поля готовы к изменению значений. Введите значения и нажмите *Enter*:



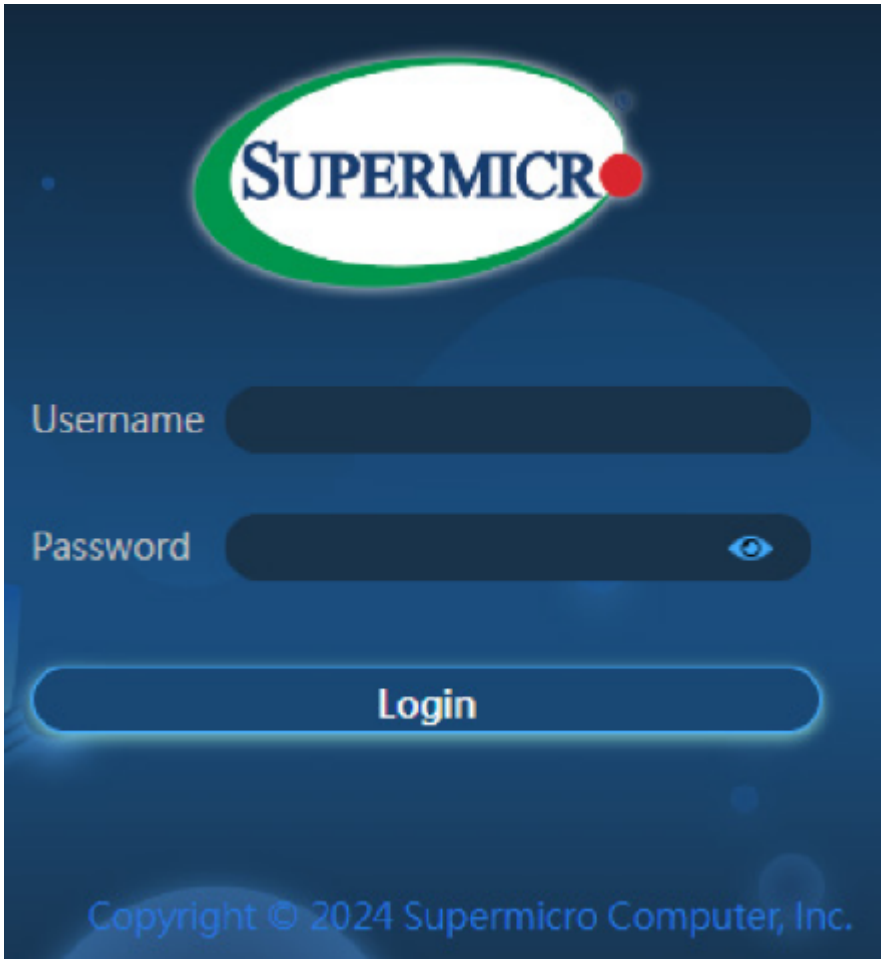
Внимание: Будьте внимательны! IP-адрес IPMI не должен совпадать с IP-адресами локальных или внешних интерфейсов.

7. Сохраните конфигурацию и выйдите из интерфейса UEFI.

8. Откройте терминал или командную строку на компьютере, который имеет доступ к подсети IP-адреса IPMI, и проверьте доступность этого IP-адреса - введите команду:

```
ping <ip-адрес станции>
```

8. Если IP-адрес доступен, откройте на компьютере браузер и введите этот IP-адрес в адресной строке. Появится экран входа в систему:



9. Введите имя пользователя (по умолчанию - ADMIN) и пароль.

Пароль администратора можно найти на специальной наклейке со штрихкодом: одна наклейка расположена рядом с микросхемой BMC или рядом с наклейкой с серийным номером материнской платы, другая - на крышке сокета CPU1. На некоторых моделях аппаратных платформ Ideco на лицевой панели есть извлекаемый язычок с паролем.

7.3 Настройка ПАК Ideco NGFW SX+

Модель SX+ не поддерживает IPMI. Для ее настройки выполните действия:

1. Включите сервер, подключив к нему монитор и клавиатуру.

2. Если на сервер уже загружен Ideco NGFW, перейдите к статье *Установка*.

3. Если Ideco NGFW не загружен:

- Скачайте последнюю актуальную версию с сайта my.ideco.ru;
- Смонтируйте устновочный диск на *USB-накопитель*.

4. Перейдите к статье *Установка*.

8. Подготовка к установке на устройство

8.1 Основное

После регистрации и загрузки образа Ideco NGFW с my.ideco.ru определите устройство, на которое собираетесь установить Ideco NGFW:

- *Установка на гипервизор*;
- *Установка на сервер*.

8.2 Настройка гипервизора

Обязательные условия для работы Ideco NGFW:

- Тип ОС для создания виртуальной машины: **Linux Fedora 64 bit**;
- Минимальный объем жесткого диска: **150 ГБ**;
- Минимальное количество оперативной памяти: **16 ГБ**;
- Минимальное количество ядер: **4**;
- Включение режима UEFI;
- Отключение опции Secure Boot в UEFI;
- Отключение режима Legacy загрузки (он также может называться CSM);
- Внутренние часы виртуальной машины должны быть настроены на хранение времени в временной зоне UTC.

Возможные проблемы:

- Если при установке Ideco NGFW появилась ошибка **Требуется не менее 16 ГБ оперативной памяти** и при этом указан рекомендуемый размер оперативной памяти. В таком случае необходимо уменьшить размер ресурсов, выделенных под видеопамять.
- При установке Ideco NGFW появилось окно с текстом **Installation in BIOS mode is not supported**. В этом случае необходимо проверить включение режима UEFI в настройках.

Ideco NGFW совместим с указанными гипервизорами:

- Microsoft Hyper-V (2-го поколения);
- VMware (Workstation и ESXi) версии не ниже 6.5.0;
- VirtualBox версии не ниже 7.0.0;
- KVM версии не ниже 1.2.0;
- Citrix XenServer.

8.2.1 VMware ESXi 6.7

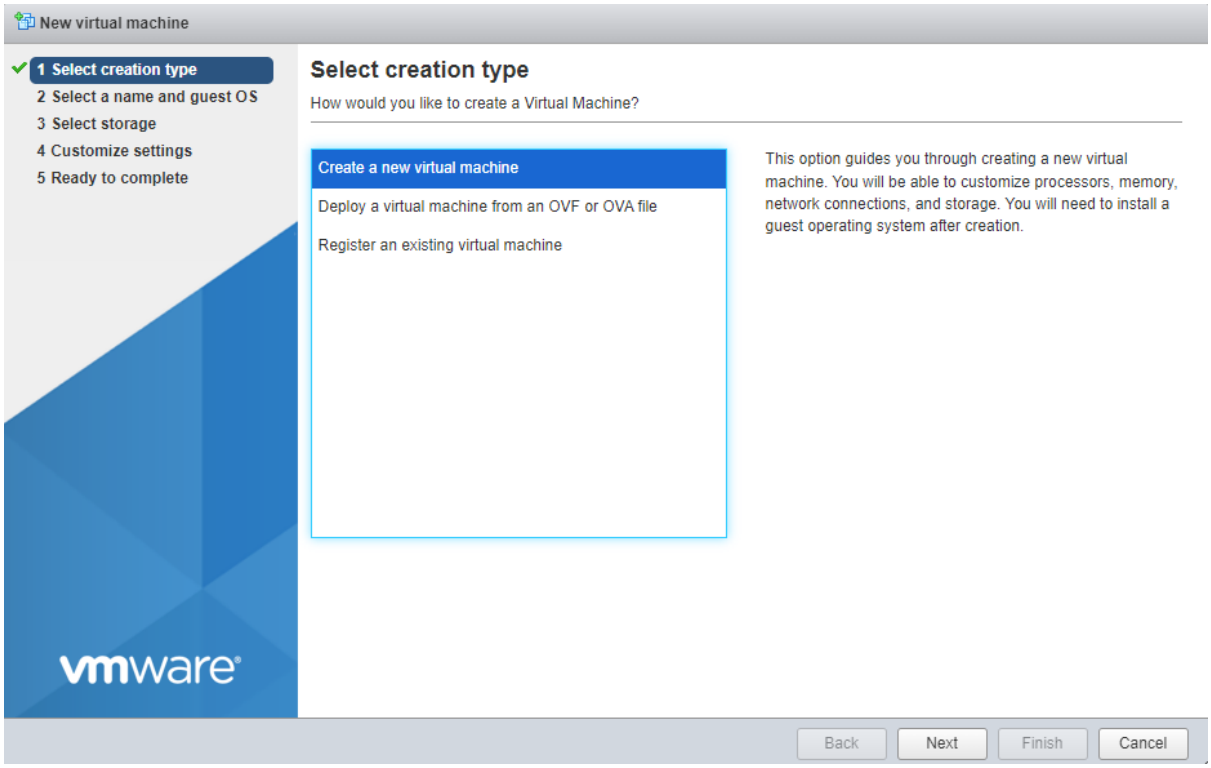
Подсказка: При установке Ideco NGFW на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

Настройка:

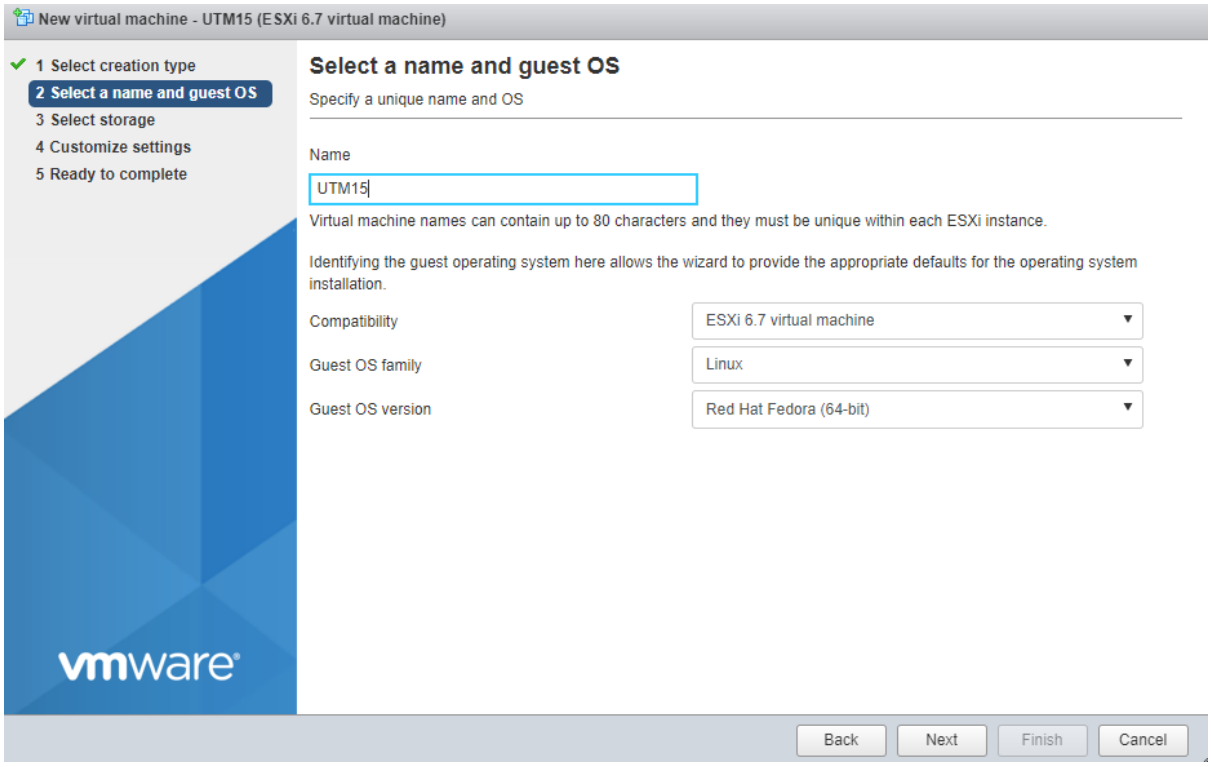
Перед установкой Ideco NGFW:

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

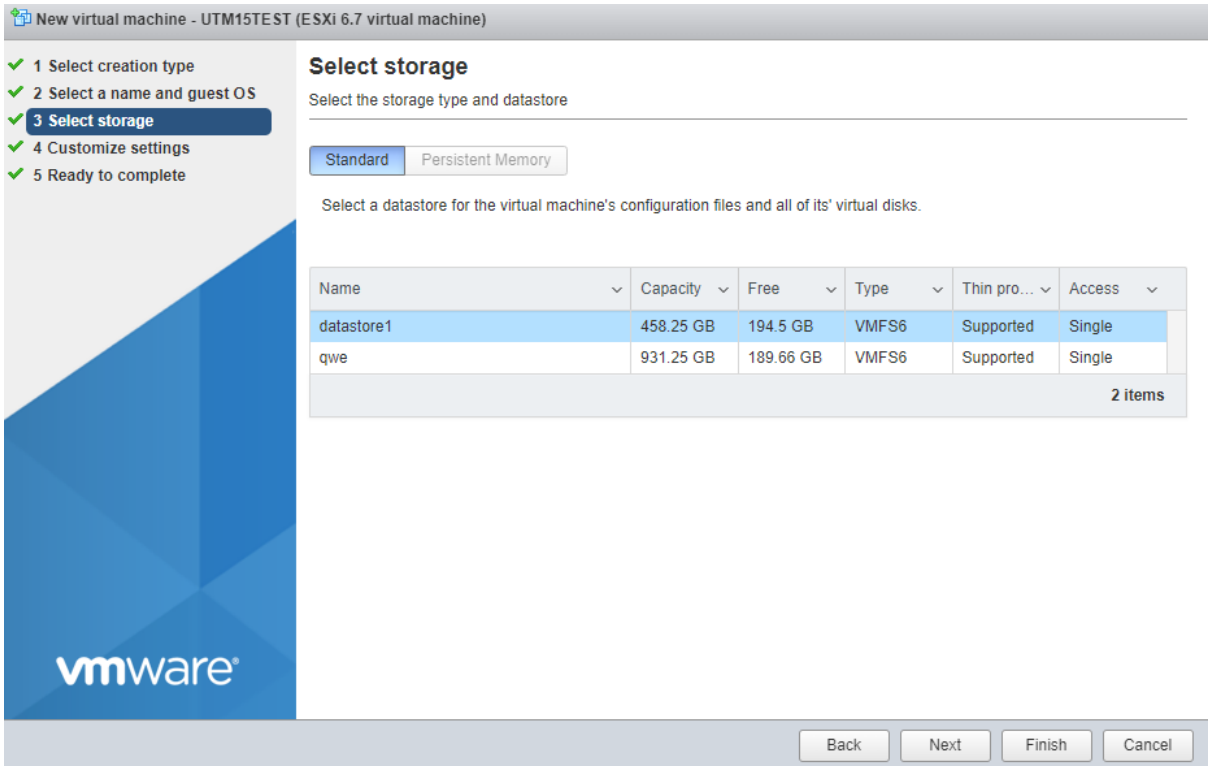
1. Создайте виртуальную машину:



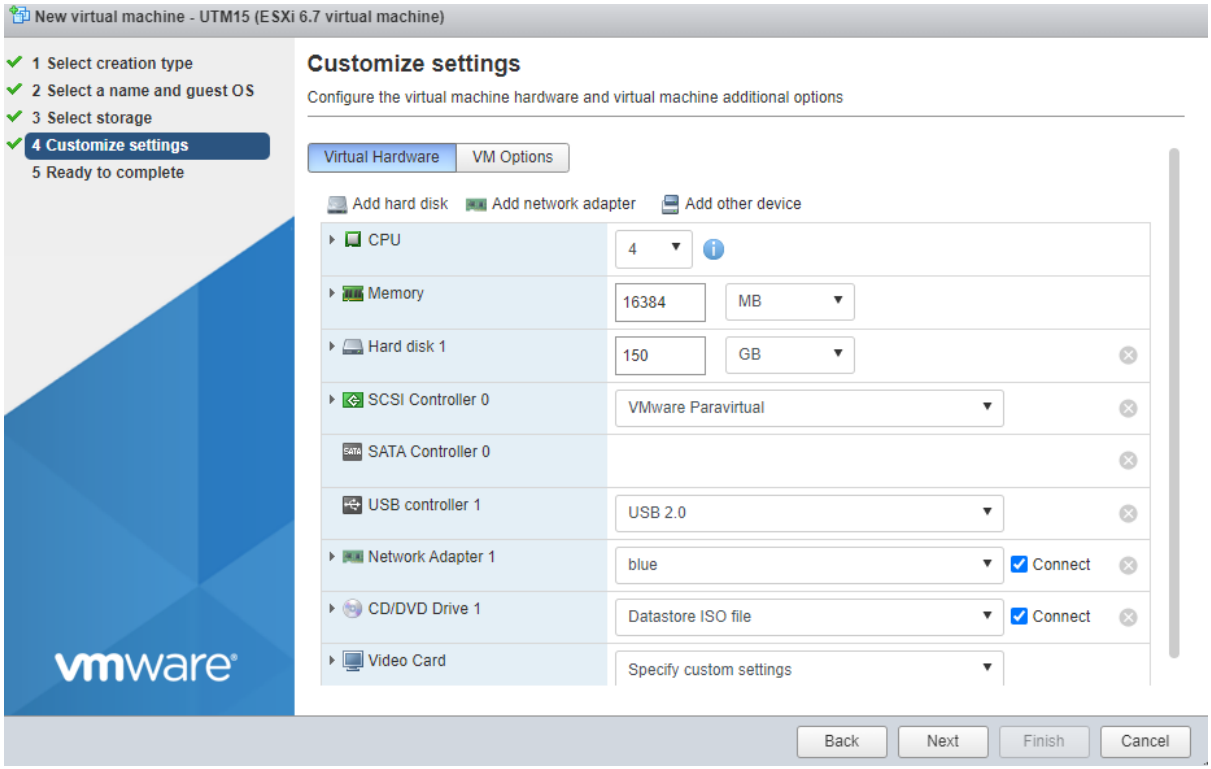
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



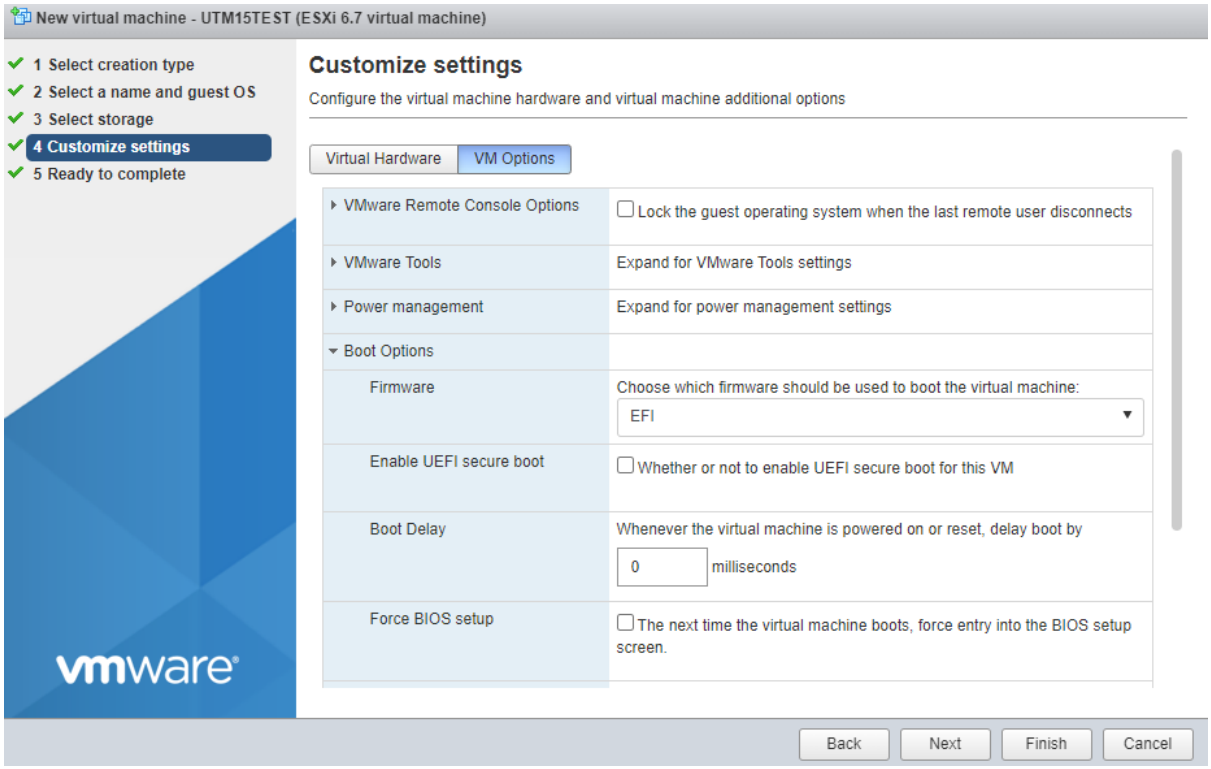
3. Выберите хранилище для виртуальной машины:



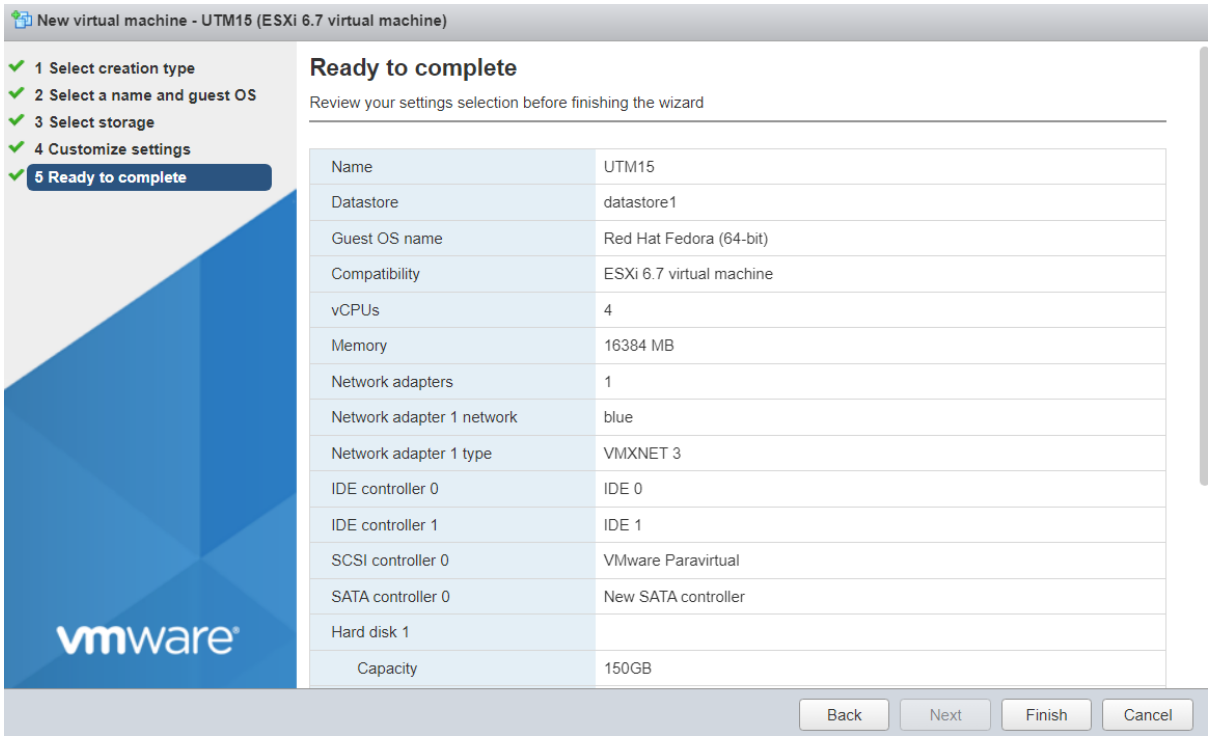
4. Установите размер оперативной памяти **16ГБ** и размер диска **150ГБ**. После выберите в поле **CD/DVD Drive** Datastore ISO file и укажите путь к загрузочному образу:



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



6. Нажмите **Finish**:



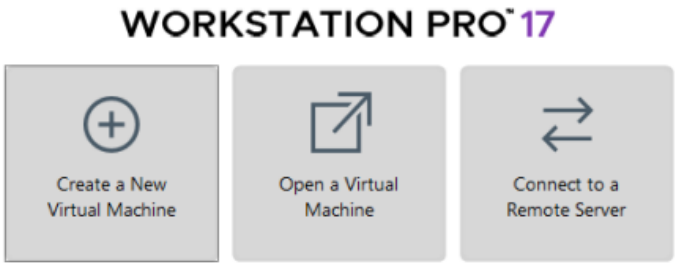
8.2.2 VMware Workstation 17.0

Настройка:

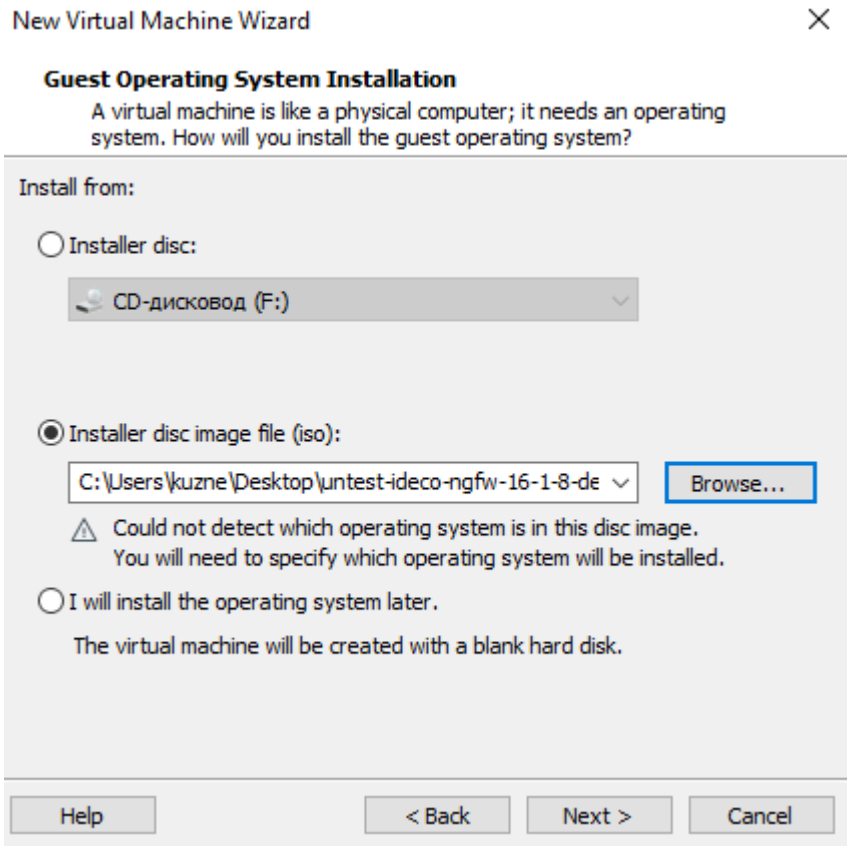
Перед установкой Ideco NGFW:

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

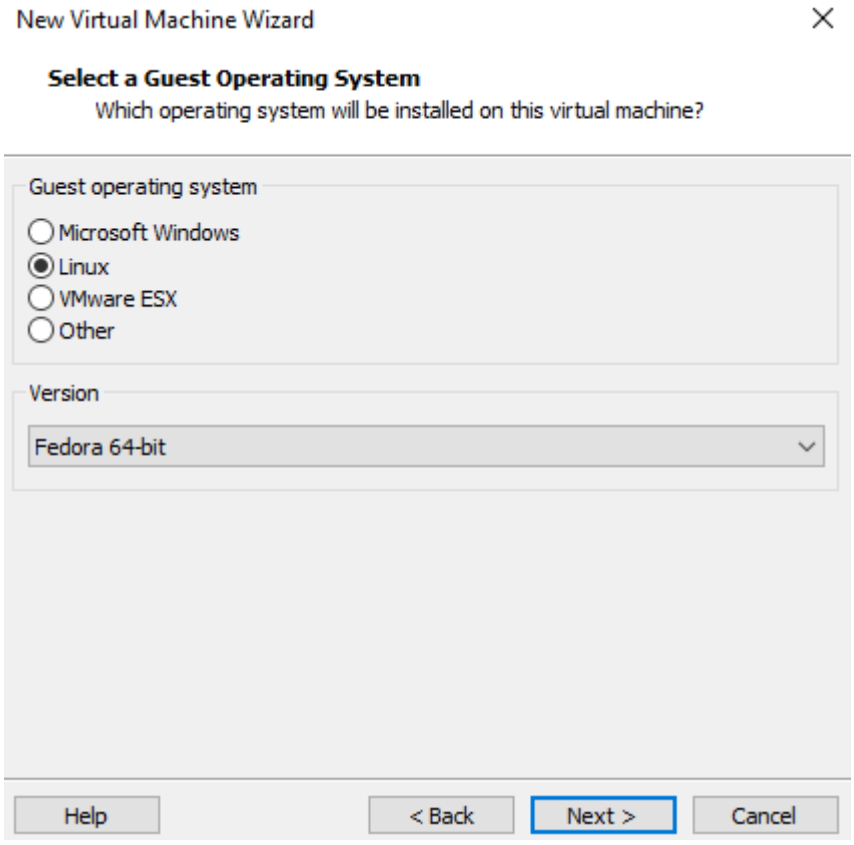
1. Создайте виртуальную машину, нажав **Create a New Virtual Machine**:



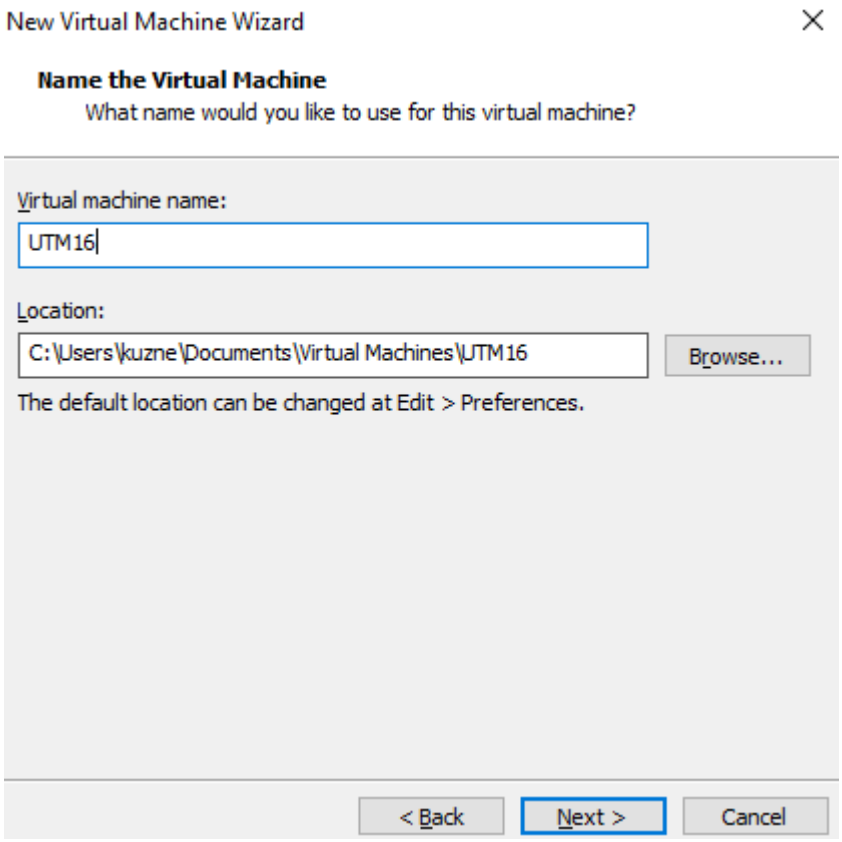
2. Укажите загрузочный ISO-образ:



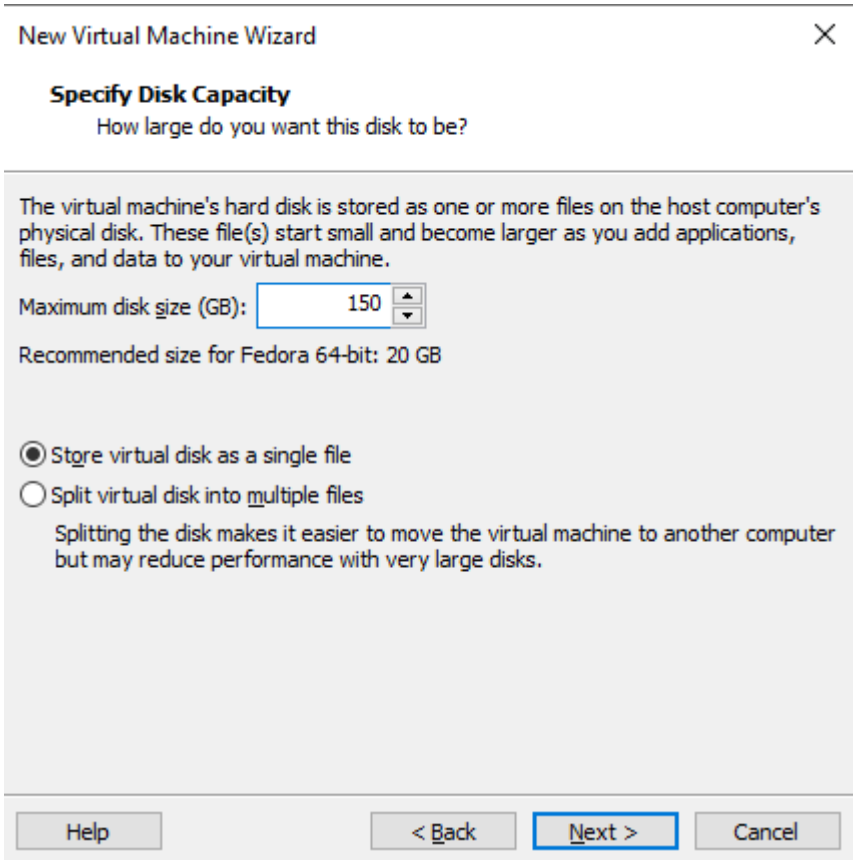
3. Выберите гостевую операционную систему **Linux** и в раскрывающемся списке укажите тип **Fedora 64-bit**:



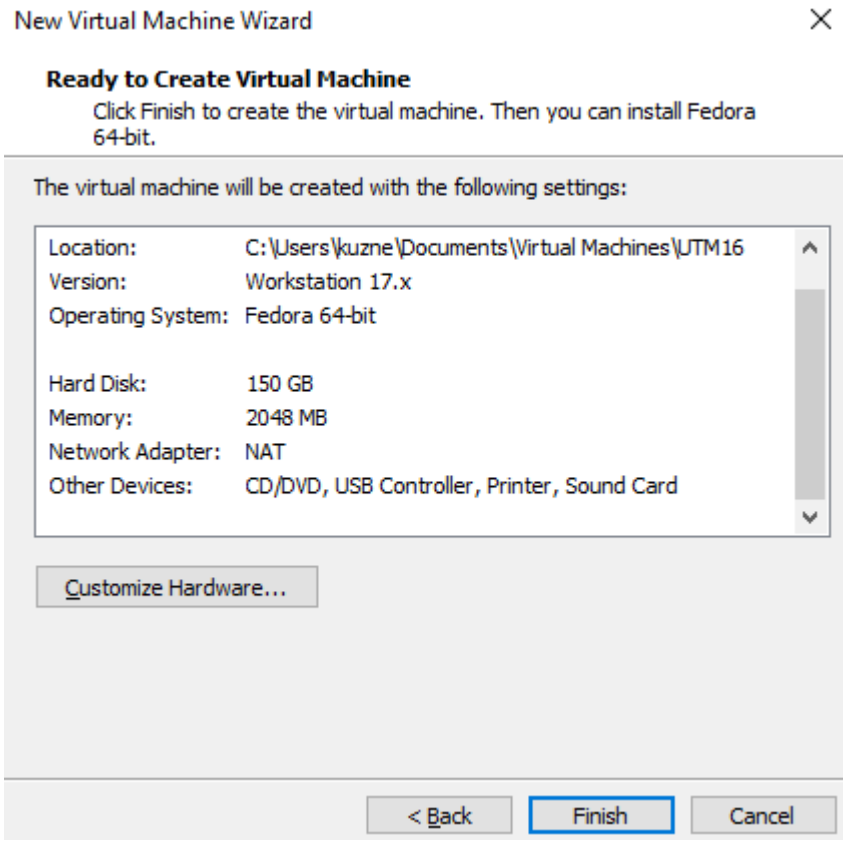
4. Укажите имя виртуальной машины и директорию для создания виртуального диска:



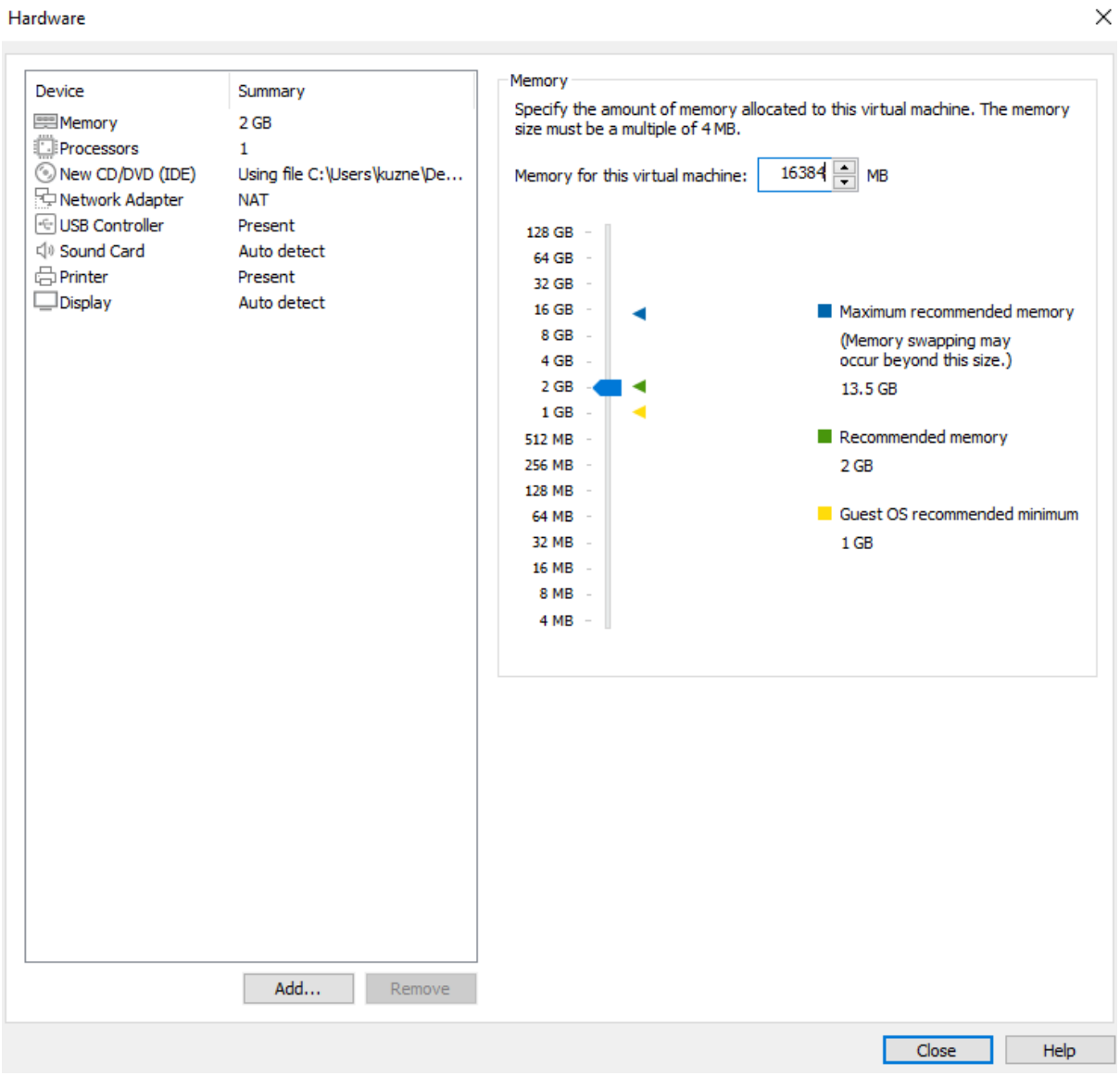
5. Укажите размер вирутального жесткого диска **150ГБ**:



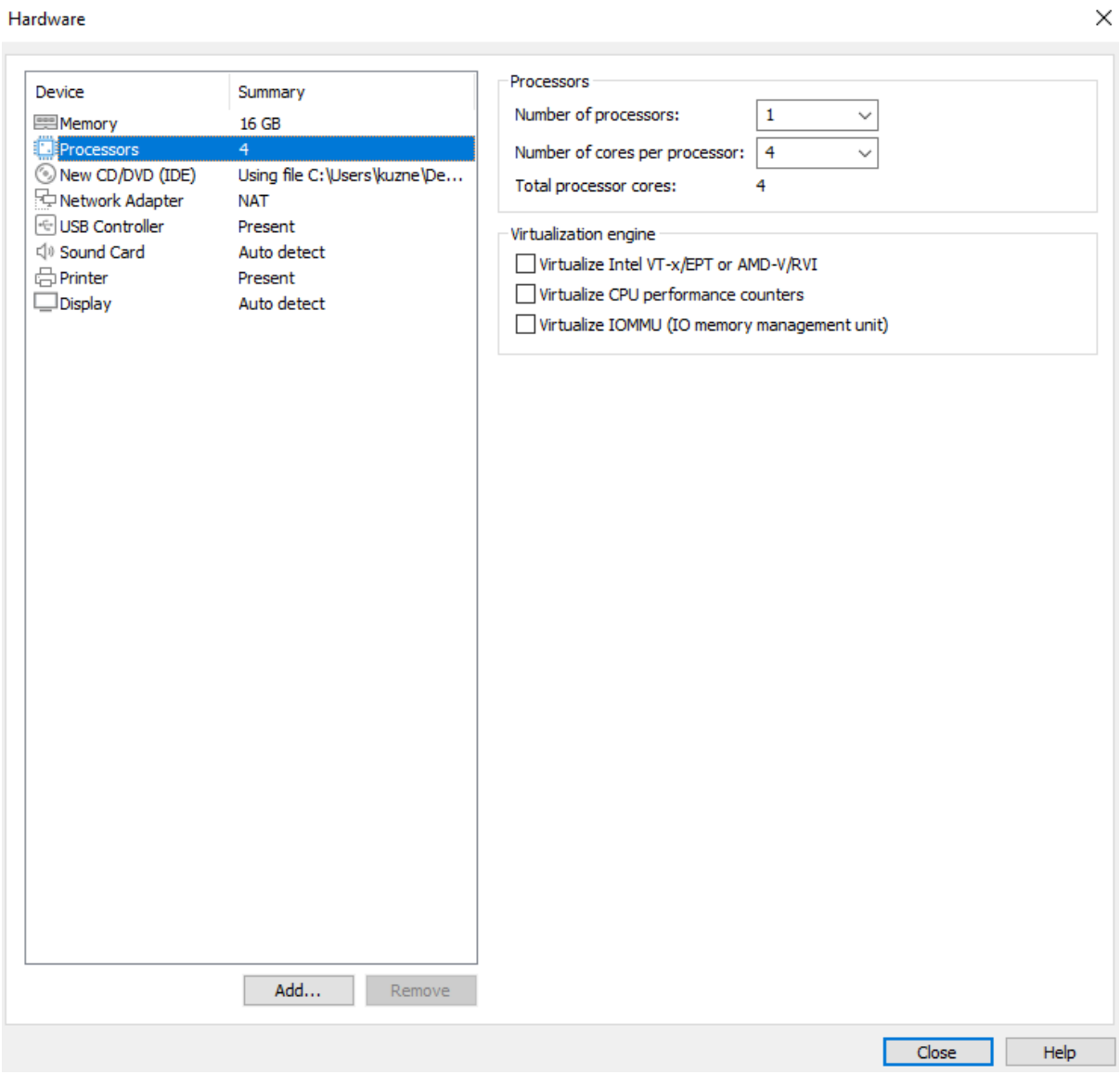
6. Выберите **Customize Hardware** для изменения настроек виртуальной машины:



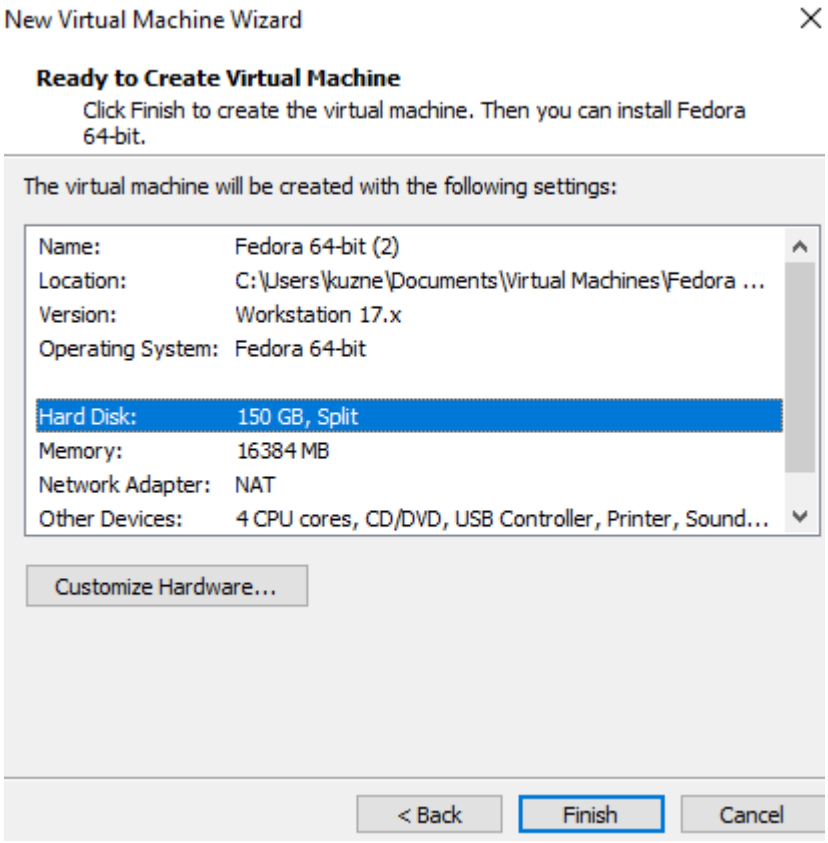
7. Укажите размер виртуальной оперативной памяти **16384МБ**:



8. Укажите количество ядер процесса равное 4:

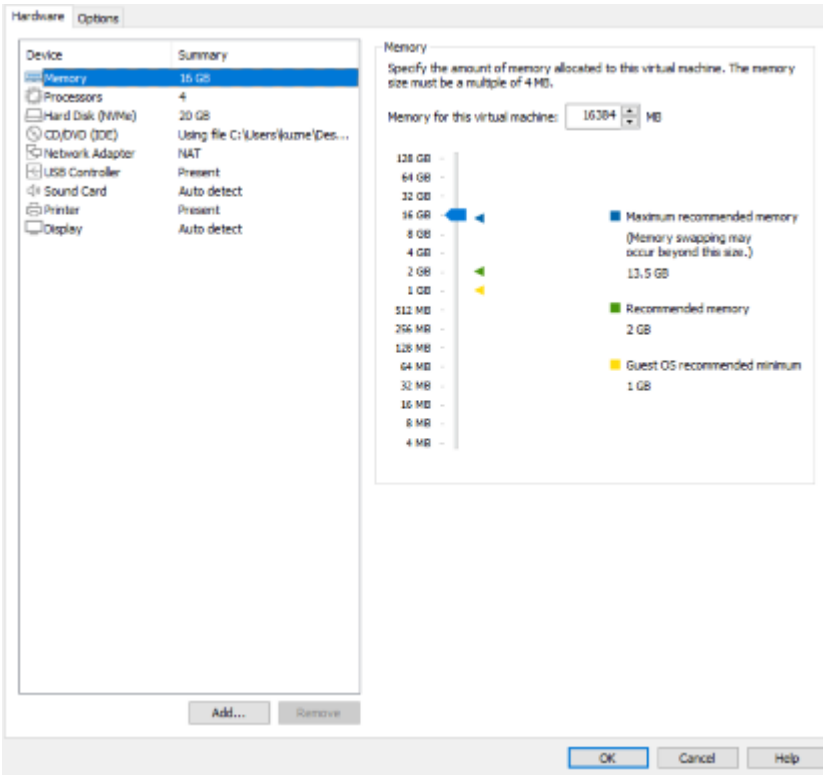


9. Выйдите из меню и нажмите **Finish** для окончания настройки:

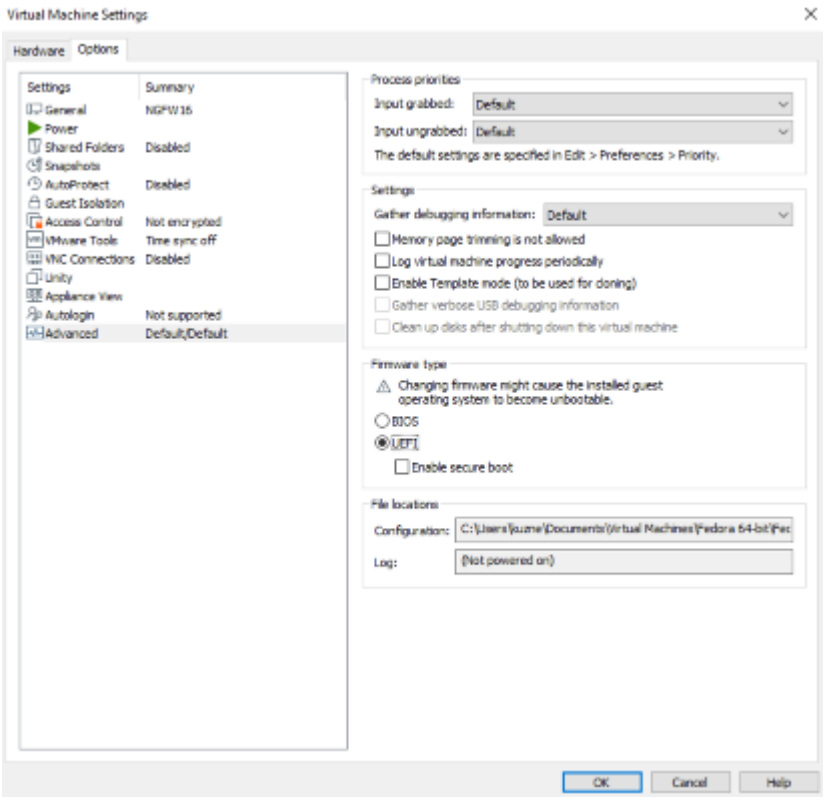


10. Перейдите в окно виртуальной машины и нажмите **Edit virtual machine settings**:

11. Перейдите на вкладку **Options**:



12. Выберите опцию **Advanced** и установите для параметра Firmware Type значение **UEFI**:



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

8.2.3 Citrix XenServer

Настройка:

Если xenserver не загружается с установочного образа:

1. Выполните команду `xe vm-list`. Она отобразит список виртуальных машин на xenserver;

2. Выберите виртуальную машину с NGFW и запомните ее UUID;

3. Выполните команду. После этого начнется загрузка с установочного носителя:

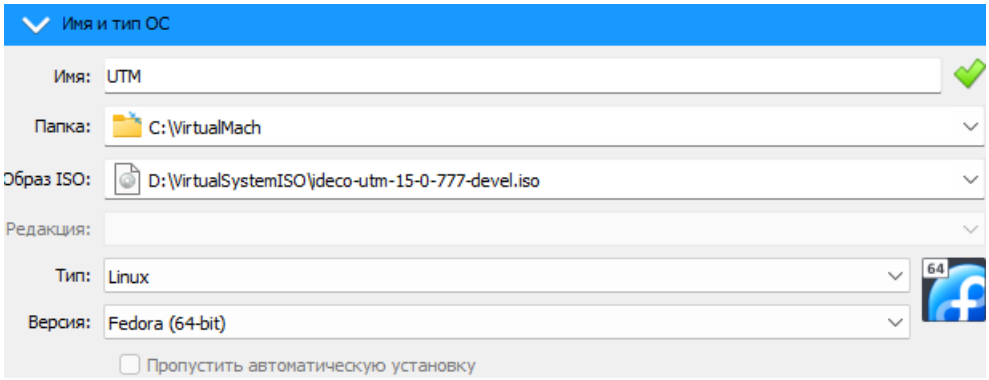
```
xe vm-param-set uuid=<UUID> HVM-boot-policy=BIOS\ order HVM-boot-params:order=dc
```

8.2.4 VirtualBox 7.0.12

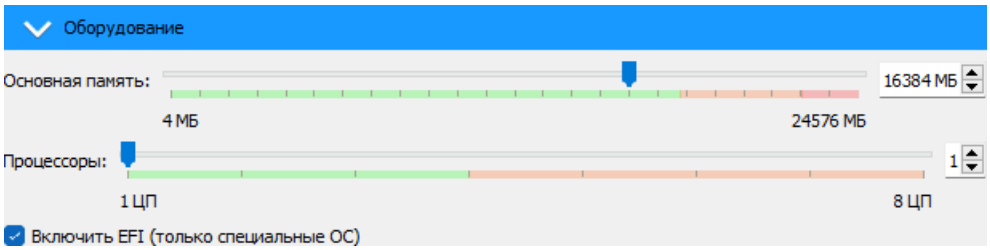
Настройка:

- По умолчанию при создании виртуальной машины создается 1 сетевая карта с типом подключения **NAT**.

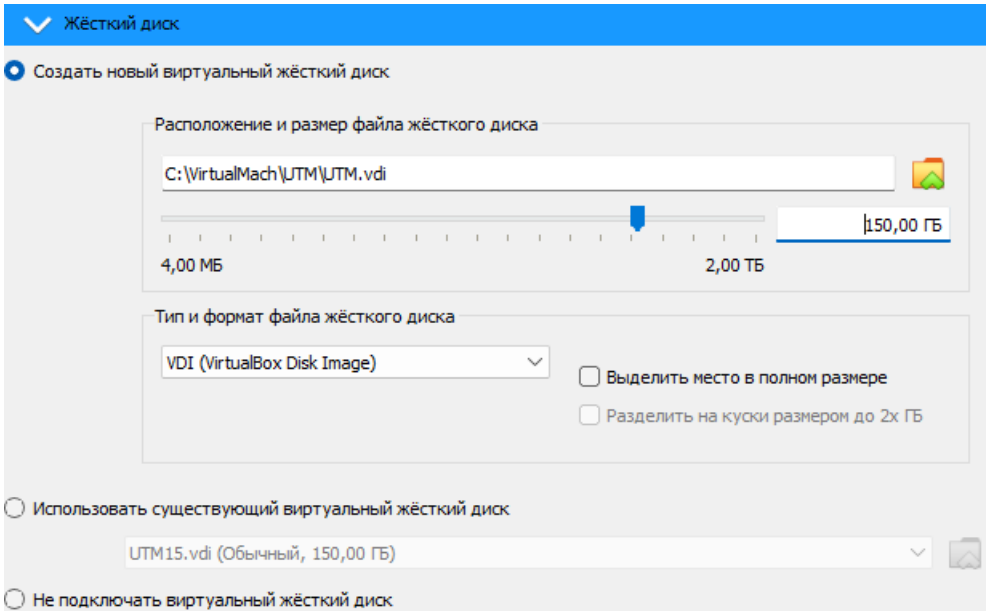
1. Укажите **Имя** виртуальной машины (ВМ), выберите директорию для ВМ и установите путь до загрузочного образа NGFW. Остальные параметры установите как на скриншоте:



2. Установите размер оперативной памяти ВМ (**16 ГБ**) и нажмите **Включить EFI**:



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



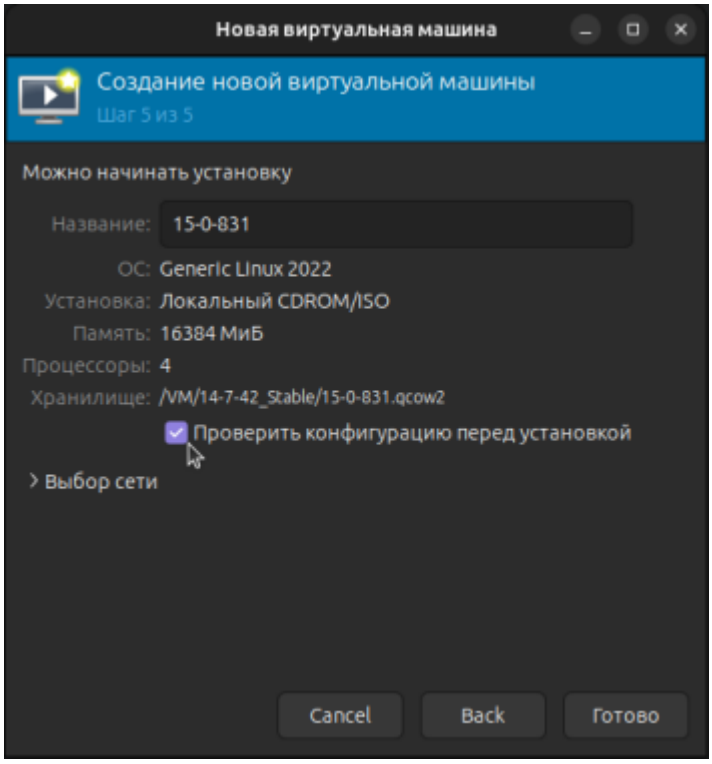
4. Нажмите **Готово**

8.2.5 KVM

Настройка:

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

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

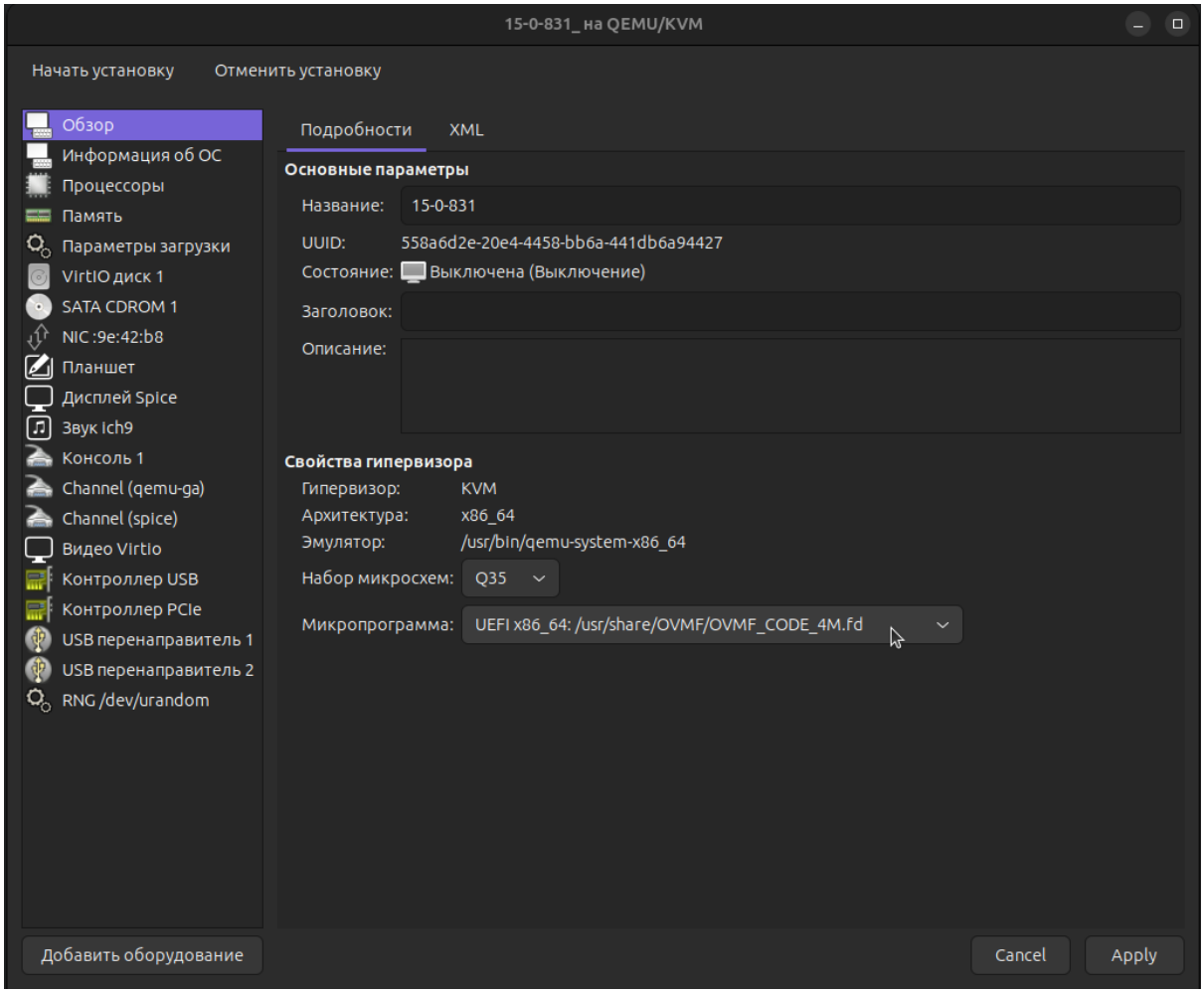


3. Измените интерфейс на **virtio** для дисков и сетевых карт.

4. Используйте режим кеширования **writeback**, если диски хранятся в qcow2 или raw-файлах.
Если нет - проконсультируйтесь у администратора хранилища или нашей технической поддержки относи-

тельно выбора режима кеширования.

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



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

8.2.6 Microsoft Hyper-V

- Поддерживается только второе поколение виртуальных машин под Windows Server 2012 R2 или выше;
- Отключите опцию **Secure Boot** (безопасная загрузка);
- Используйте обычный виртуальный сетевой адаптер (Network Adapter).

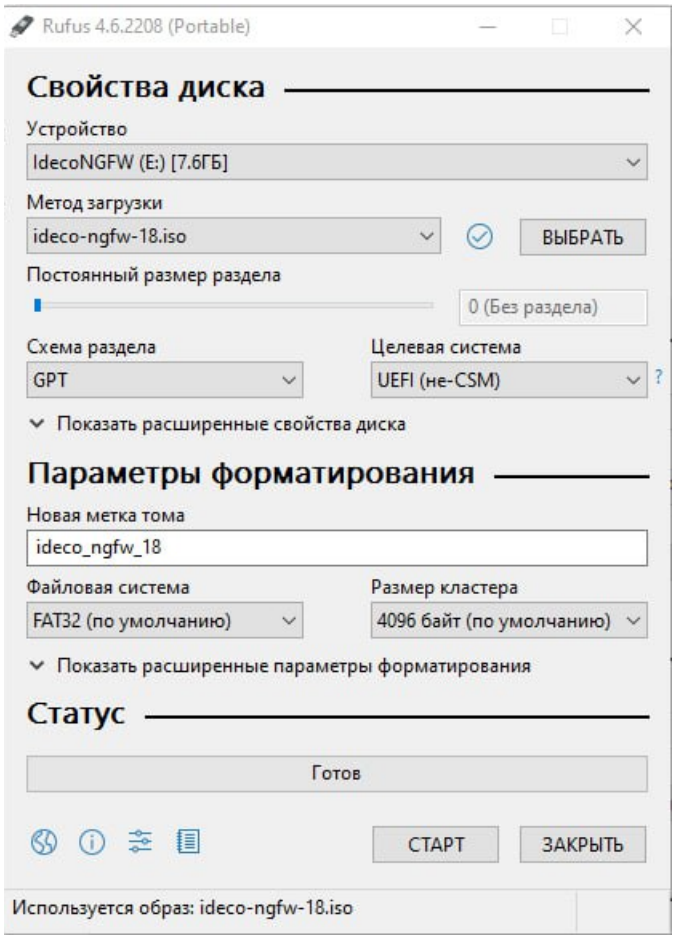
Подсказка: Шаги по установке Ideco NGFW после создания загрузочного USB-накопителя можно прочитать в статье *Установка*.

8.3 Создание загрузочного USB-накопителя

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

8.3.1 В среде Windows

1. Скачайте программу Rufus и запустите скачанный файл.
2. Выберите нужный USB-накопитель в пункте **Устройство**:
3. Выберите метод загрузки **Диск или ISO-образ**.
4. Нажмите на кнопку **Выбрать** и откройте скачанный образ Ideco NGFW.
5. Нажмите **Старт** и в появившемся окне выберите пункт **Запись в режиме DD-образ**.
6. В диалоговом окне подтвердите запись.



8.3.2 В среде Linux

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

1. Проверьте целостность образа (хеш-сумма должна совпадать с суммой в личном кабинете):

```
md5sum <путь_к_скачанному_загрузочному_образу>
8c872cb6b720f6fd6683107681645156  /home/ideco/IdecoUTM.iso
```

2. Найдите USB-носитель в системе:

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

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

3. Отмонтируйте файловую систему:

```
sudo umount <точка_монтирования>
sudo umount /run/media/ideco/D661-82E2
```

4. Запишите образ на носитель:

```
sudo dd if=<путь_к_загрузочному_образу> of=<имя_устройства> bs=1M oflag=direct␣
↪status=progress
sudo dd if=/home/ideco/IdecoUTM.iso of=/dev/sdx bs=1M oflag=direct status=progress
```

5. Подготовьте носитель к извлечению:

```
sudo eject <имя_устройства>
sudo eject /dev/sdx
```

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

9. Установка

Ссылка на видеоинструкцию по установке Ideco NGFW

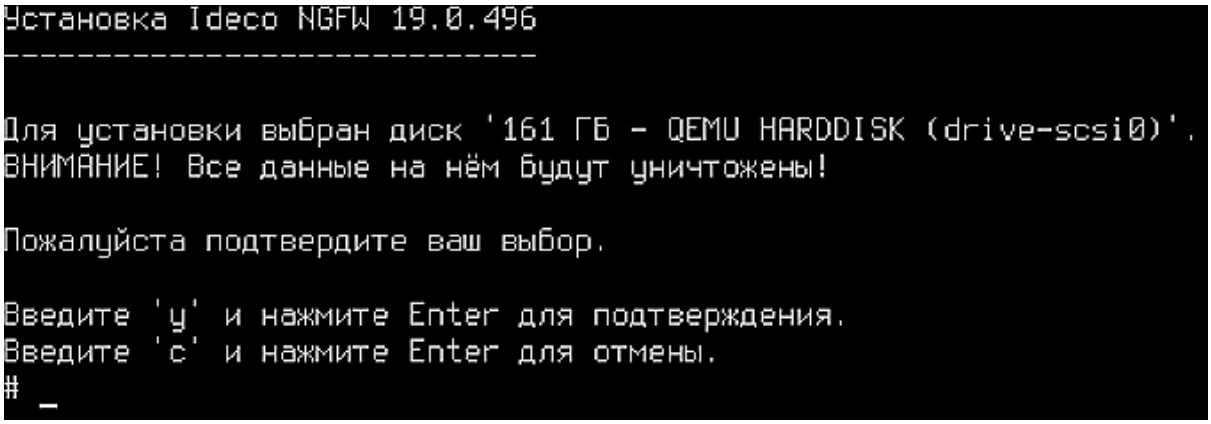
9.1 Процесс установки

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

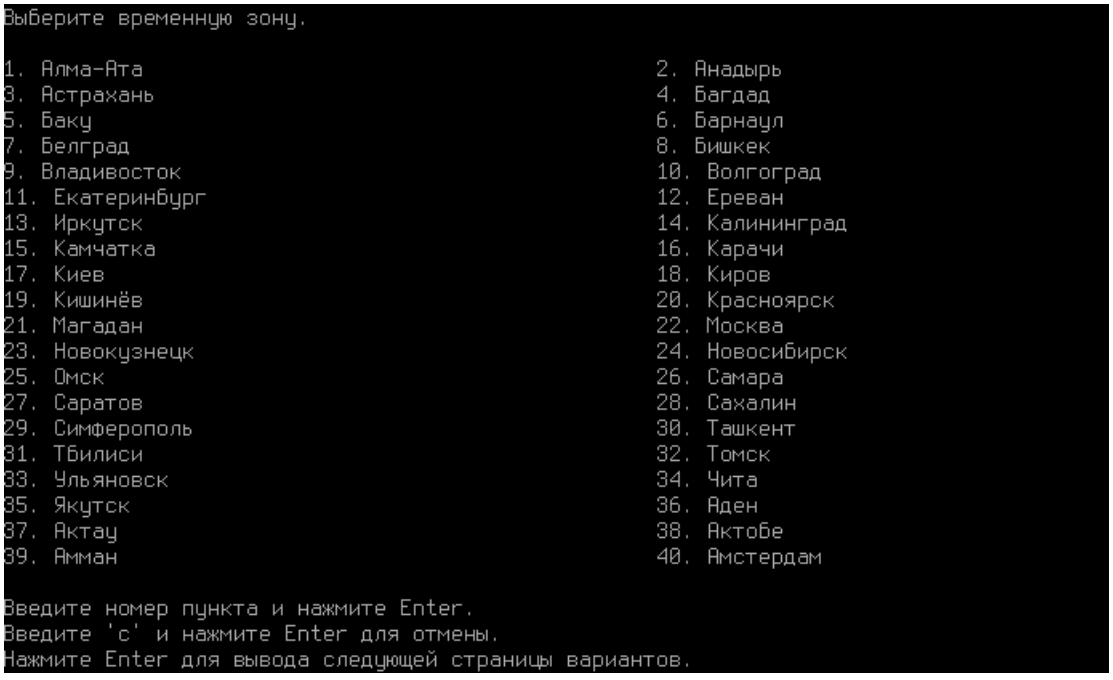
Для установки Ideco NGFW выполните действия:

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

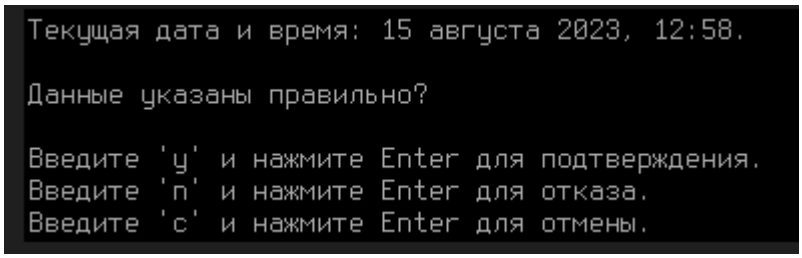
2. Выберите диск и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой находится сервер:



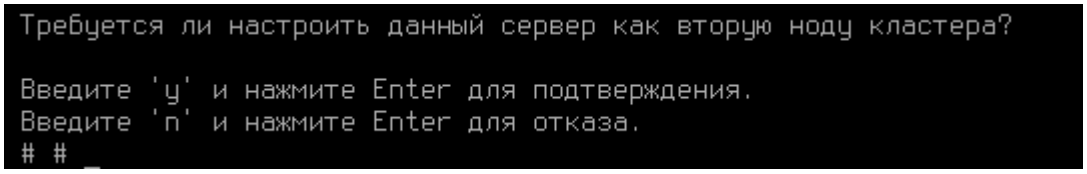
4. **Обязательно проверьте правильность даты и времени.** При необходимости настройте дату и время в соотвествии с временной зоной сервера:



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

9.2 Настройка второй ноды кластера

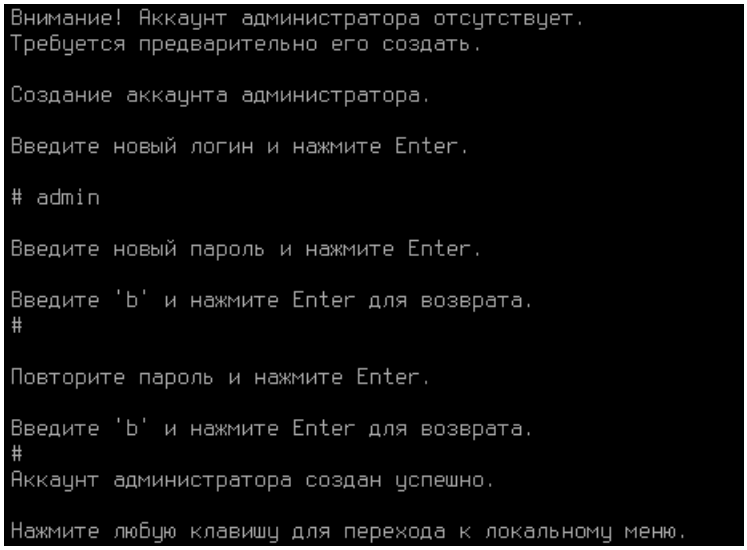
1. Введите **y** для начала настройки NGFW как второй ноды кластера:



2. Для продолжения настройки воспользуйтесь статьей *Кластеризация*.

9.3 Создание учетной записи администратора

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



Требования к паролю:

- **Минимальная длина пароля** - 11 символов;
- **Содержит строчные и заглавные латинские буквы**;
- **Содержит цифры**;
- **Содержит специальные символы** (! # $ % & „ * + и другие).

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

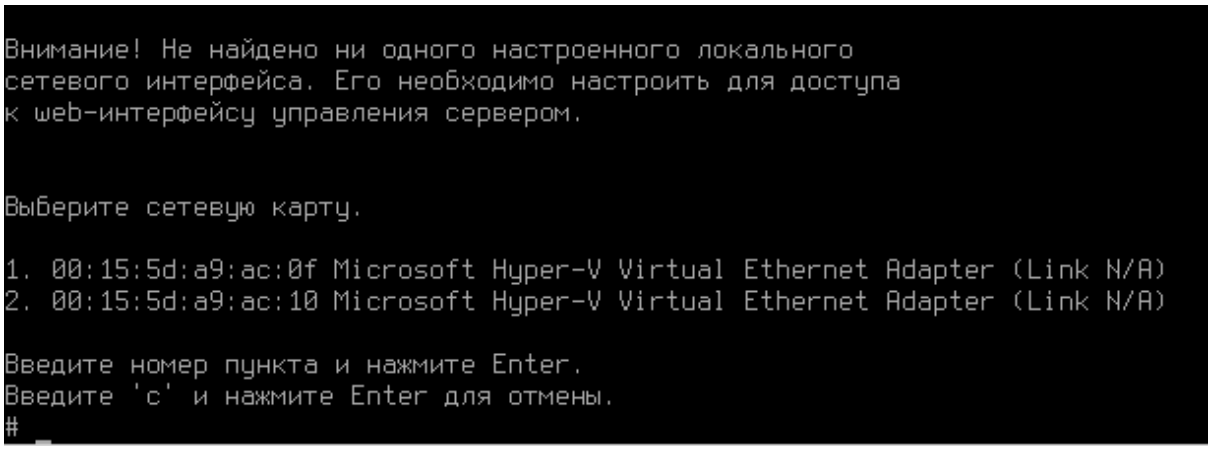
Не используйте Numpad при вводе пароля, поскольку в будущем это может привести к проблемам при авторизации администратора.

9.4 Настройка локального интерфейса

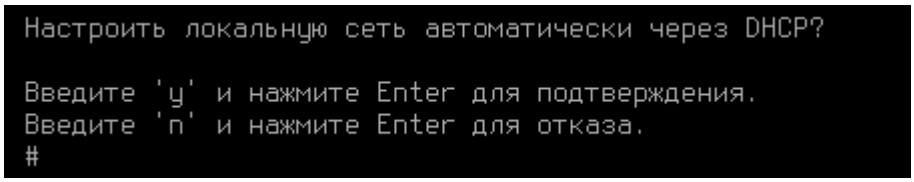
Подсказка: При использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса. Для корректной идентификации сетевой карты используйте ее MAC-адрес.

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

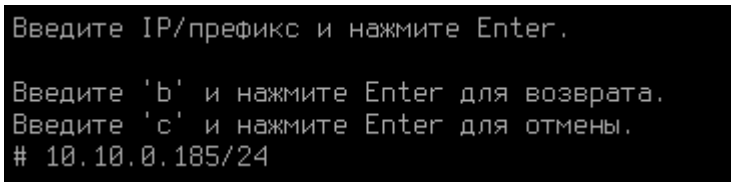
1. Введите номер сетевого адаптера под локальный интерфейс:



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

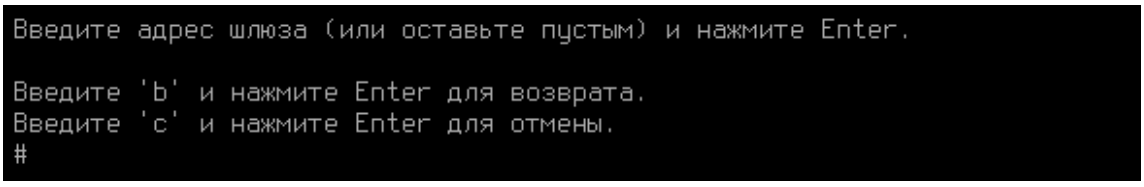


3. Введите локальный IP-адрес и маску подсети в формате `ip/маска` и нажмите **Enter**:

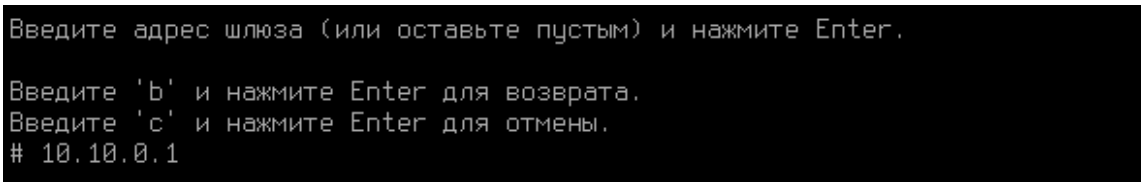


4. Введите адрес шлюза или оставьте поле пустым:

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



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



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

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

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

После создания локального интерфейса откроется локальное меню управления сервером:

```
Управление сервером

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

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

---

10. Первоначальная настройка

Внимание: Для *получения доступа в интернет* через Ideco NGFW необходимо создать учетную запись (администратора/пользователя) и настроить авторизацию. В противном случае доступ в интернет для устройства с установленным Ideco NGFW будет заблокирован.

10.1 Подключение к веб-интерфейсу Ideco NGFW

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

2. Введите в адресной строке IP-адрес, указанный при настройке локального интерфейса, и порт 8443.
Пример: `192.168.100.2:8443`

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

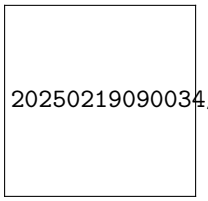
10.2 Импорт корневого сертификата NGFW в браузер

Для устранения предупреждения в браузере при входе в веб-интерфейс импортируйте корневой сертификат NGFW или добавьте в доверенные корневые центры сертификации устройства, скачав сертификат одним из способов:

**

Из раздела Сервисы:**

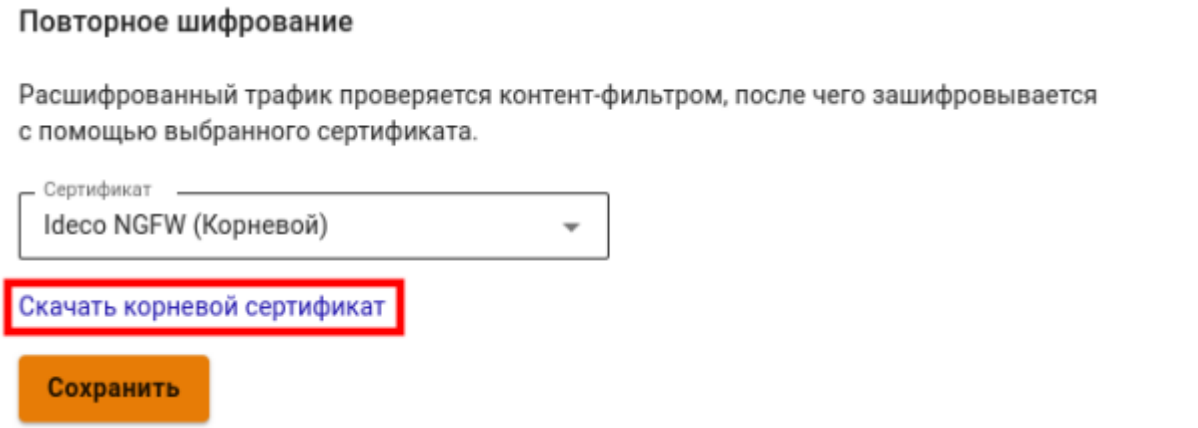
В разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** нажмите на стрелку для скачивания:



**

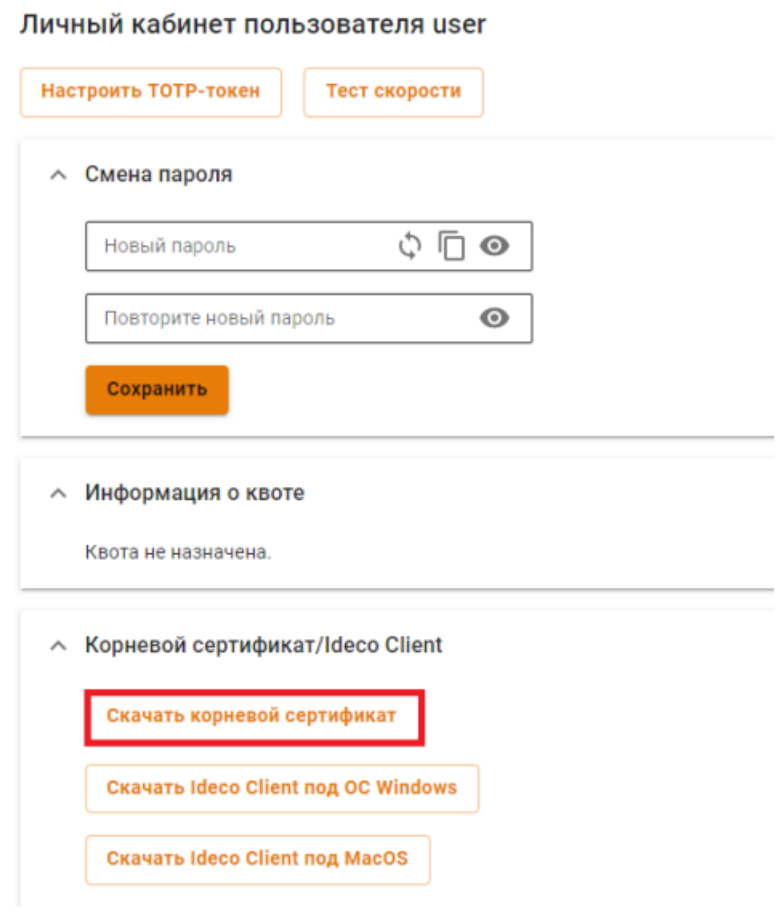
Из раздела Правила трафика:**

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



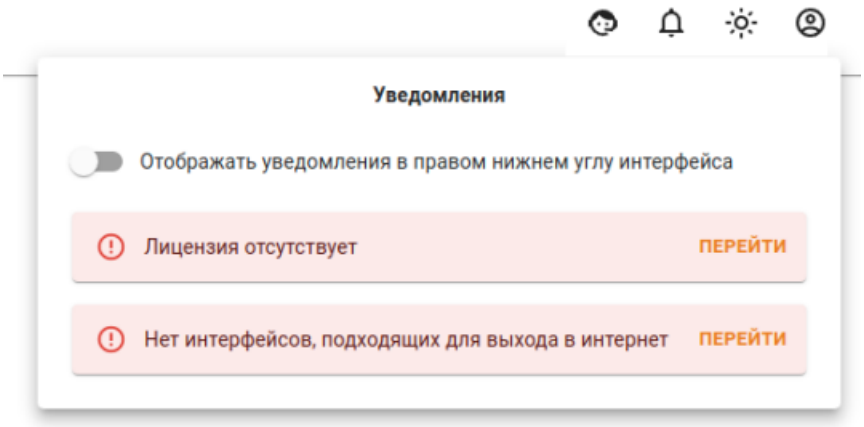
Из личного кабинета пользователя:

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



Для публикации личного кабинета пользователя воспользуйтесь *статьей*.

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



10.3 Настройка Ethernet-подключения

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

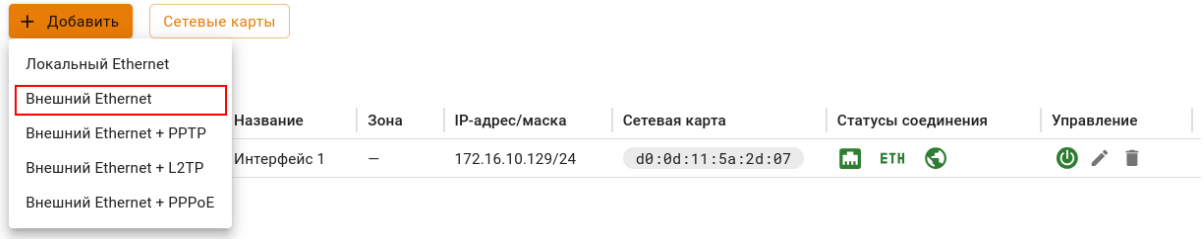
Этот тип подключения требует настройки параметров, описанных ниже в таблице.

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

Для настройки Ethernet-подключения выполните:

1. Перейдите в раздел **Сервисы -> Сетевые интерфейсы**.

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



Внимание: Будьте внимательны!

При выборе пункта **Локальный Ethernet** и заполнении поля **Шлюз** доступ в интернет будет отсутствовать. Шлюз указывается для маршрутизации внутри локальной сети или в режиме прямого прокси.

3. Выберите подходящую сетевую карту.

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

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

10.3.1 Настройка других типов подключений

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

- *Подключение по протоколу PPPoE*;
- *Подключение по технологии VPN (с использованием протокола PPTP)*;
- *Подключение по L2TP*;
- *Подключение Локального Ethernet*;
- *Подключение по 3G и 4G*;
- *Одновременное подключение к нескольким провайдерам*.

11. Регистрация сервера

Подсказка: Для активации лицензии необходима обязательная регистрация сервера в личном кабинете.

11.1 Онлайн-регистрация

Предупреждение: Для привязки лицензии сервер должен иметь выход в интернет.

Шаги онлайн-регистрации сервера и привязки лицензии:

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

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

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

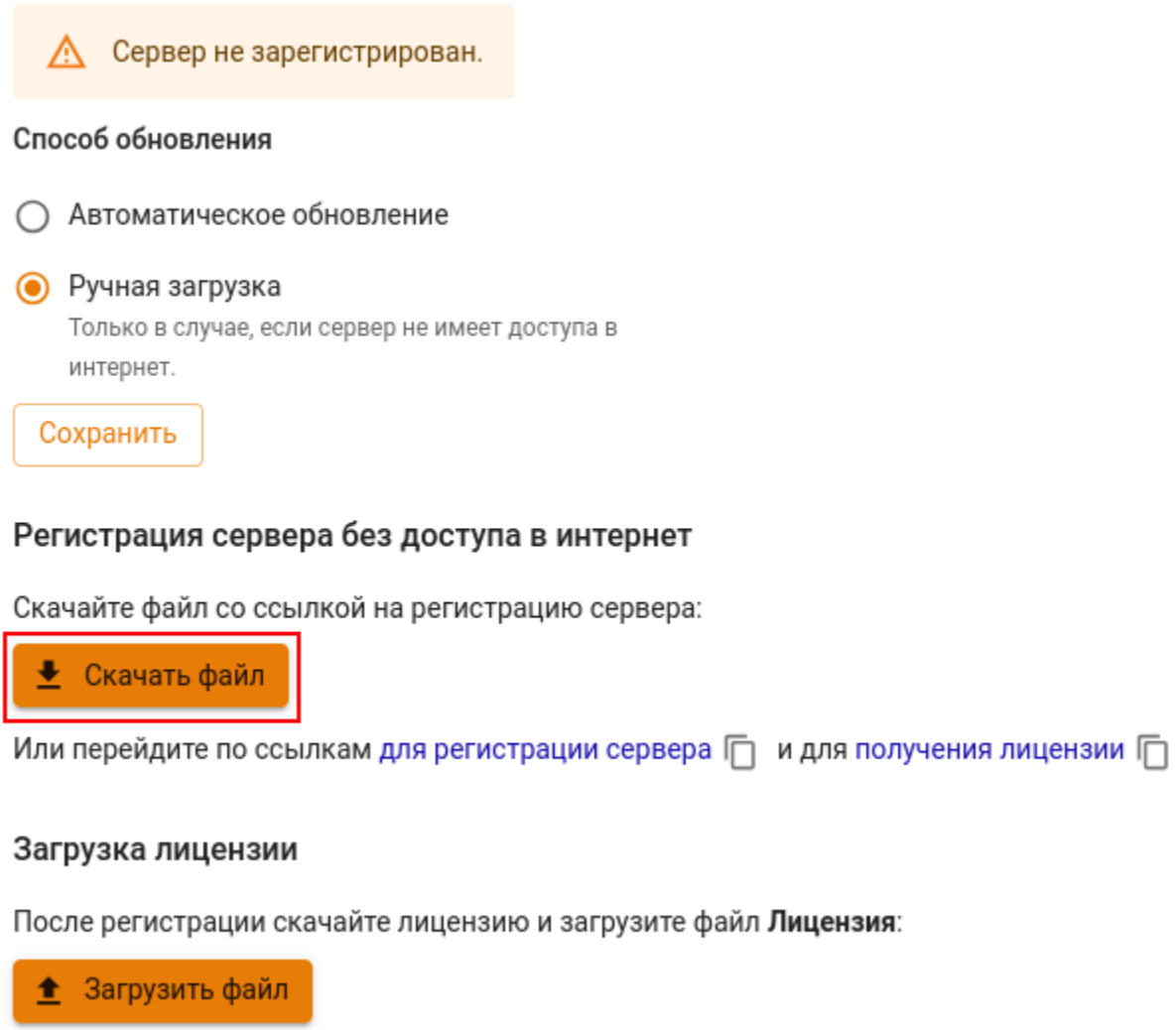
На странице отобразится информация о лицензии и ее модулях.

11.2 Офлайн-регистрация

Шаги офлайн-регистрации сервера и привязки лицензии:

1. В веб-интерфейсе Ideco NGFW перейдите в раздел **Управление сервером -> Лицензия**, выберите **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

2. Скачайте файл со ссылками на регистрацию сервера и скачивание баз и лицензии, нажав на кнопку, или скопируйте эти ссылки из веб-интерфейса:

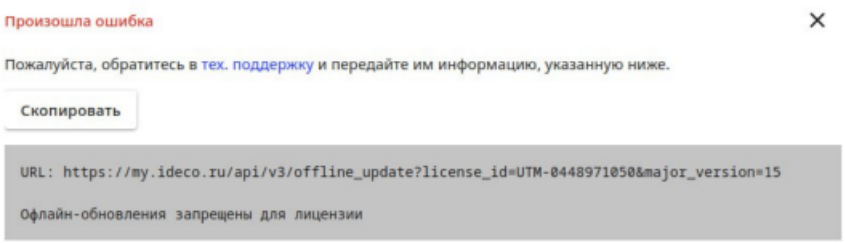


3. На устройстве с доступом к интернету перейдите по ссылке для регистрации сервера, полученной в пункте 2. Сервер автоматически появится в списке серверов в MY.IDECO.

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

5. В личном кабинете MY.IDECO перейдите в раздел **NGFW -> Лицензирование** и нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `UTM (UTM Unknown)`.

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

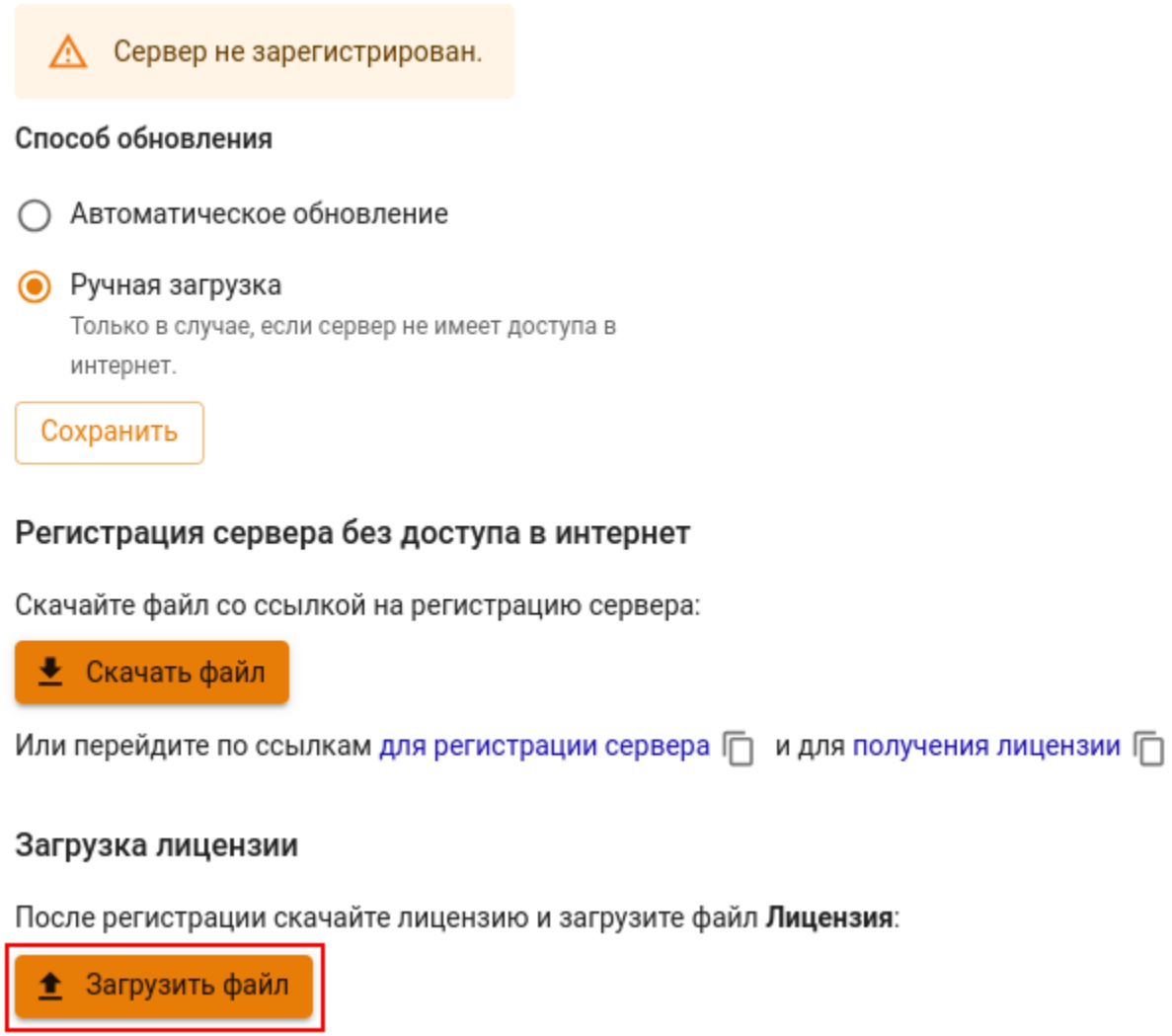


6. Получите файлы лицензии и баз фильтрации одним из способов:

- Перейдите по ссылке для скачивания баз и лицензии из пункта 2 и скачайте файлы, нажав на соответствующие ссылки в открывшейся форме:

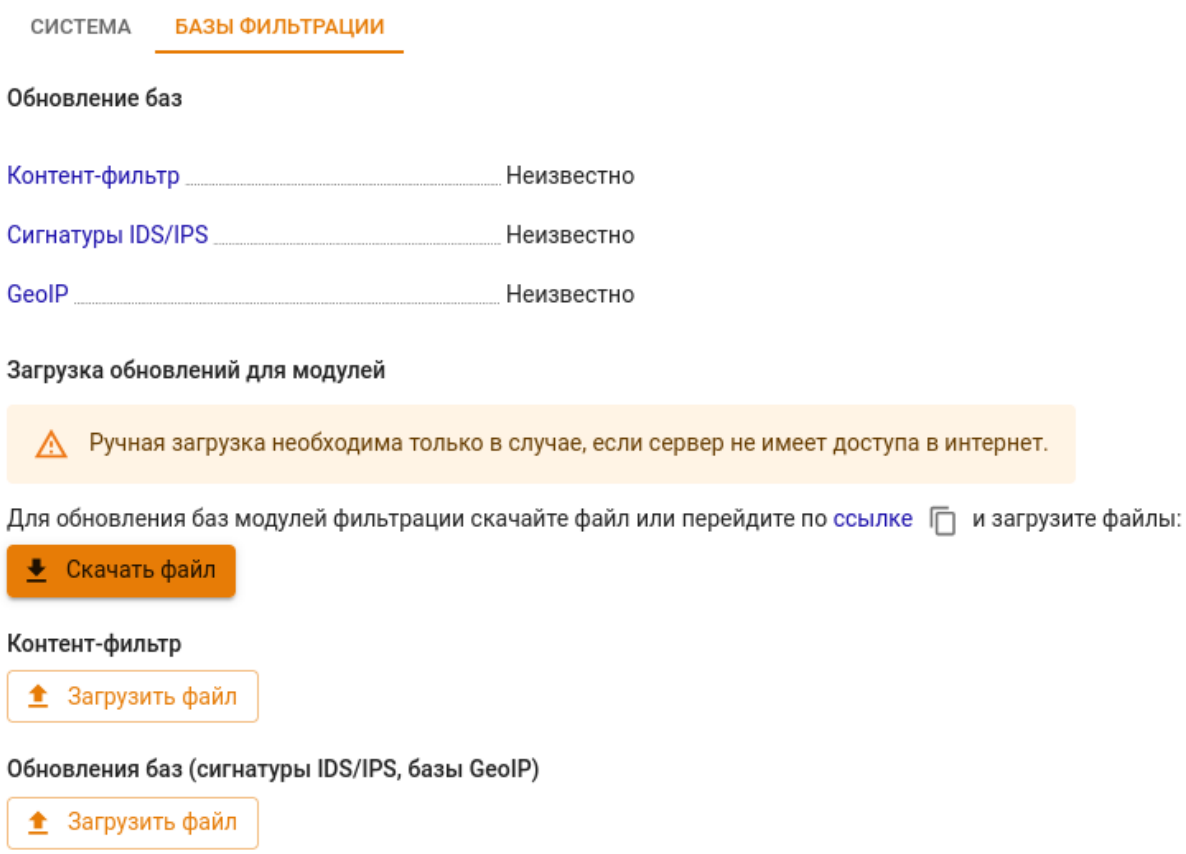
- В интерфейсе MY.IDECO напротив названия сервера нажмите и вставьте ссылку, скопированную в разделе **Обновления -> Базы фильтрации**, в открывшуюся форму. Скачайте файлы.

7. В веб-интерфейсе Ideco NGFW перейдите в раздел **Управление сервером -> Лицензия** и загрузите файл с лицензией, скачанный в пункте 6:



11.3 Офлайн-обновление баз модулей безопасности

Чтобы обновить базы модулей безопасности в режиме офлайн, перейдите в веб-интерфейс Ideco NGFW в раздел **Управление сервером -> Обновления -> Базы фильтрации** и загрузите скачанные в пункте 6 *Офлайн-регистрации* файлы, нажав на соответствующие кнопки:



Внимание: Базы фильтрации Ideco NGFW могут меняться ежедневно, поэтому при ручной загрузке обновляйте их как можно чаще.

12. Получение доступа в интернет

12.1 Основное

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

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

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

2. Убедитесь, что в веб-интерфейсе NGFW выбран нужный способ *авторизации* и настроена *учетная запись пользователя*.

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

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

  - Для авторизации пользователей Active Directory воспользуйтесь статьей ***Аутентификация пользователей AD/Samba DC***, для авторизации пользователей ALD Pro - статьей ***ALD Pro***.

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

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

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

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

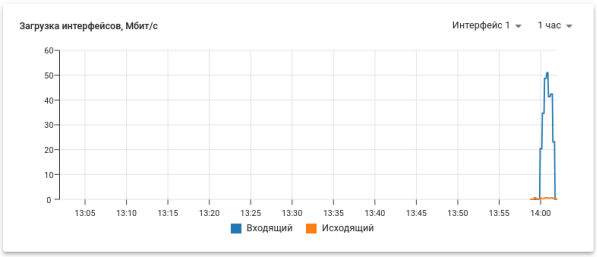
13. Панель мониторинга

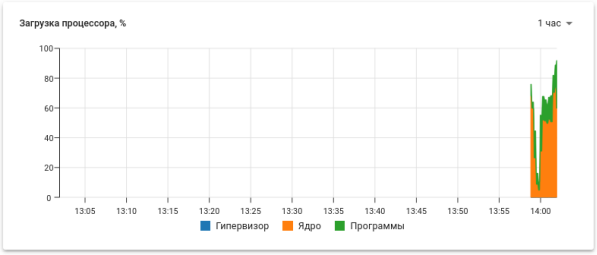
Данный модуль позволяет просматривать информацию о состоянии сервера за определенный промежуток времени (5 минут, час, 6 часов, 1 день, 7 дней).

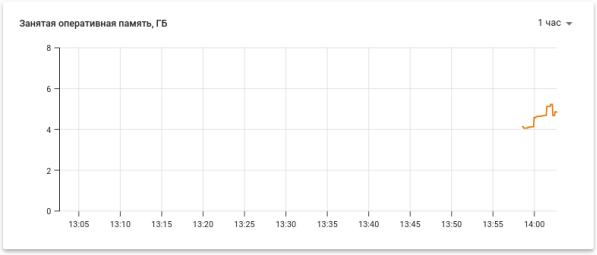
Параметры модуля Панель мониторинга:

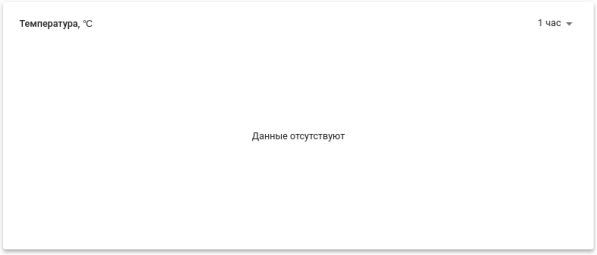
- Время работы сервера;
- Основная информация о *лицензии*;
- Загрузка процессора;
- Занятая оперативная память;
- Управление модулями фильтрации (можно включить или отключить нужные модули);
- Загрузка интерфейсов, включая информацию по каждому интерфейсу;
- Топ 5 хостов (входящая скорость);
- Топ 5 хостов (исходящая скорость);
- IPSec (исходящие);
- IPSec (входящие).

Пример окна модуля **Панель мониторинга** представлен на скриншоте ниже:









Управление модулями фильтрации

- Файрвол
- Контент-фильтр
- Ограничение скорости
- Антивирусы веб-трафика
- Предотвращение вторжений
- Профили контроля приложений

Состояние внешних интерфейсов

Интерфейс	Загруженность (Мбит/с)
Интерфейс 2	
Интерфейс 1	0,1

Время работы сервера ..... 6 минут

Топ-5 хостов (входящая скорость), Мбит/с — Топ 5

Пользователь	IP-адрес	Вх. скорость	Сессии
–	–	0,00	1
–	–	0,00	1
–	–	0,00	1
–	–	0,00	1
–	–	0,00	17

Топ-5 хостов (исходящая скорость), Мбит/с — Топ 5

Пользователь	IP-адрес	Исх. скорость	Сессии
–	–	0,00	2
–	–	0,00	17
–	–	0,00	1
–	–	0,00	1
–	–	0,00	1

Лицензия

Номер лицензии LIC-3067789070

Окончание лицензии ..... 27 октября 2024 г., 13:59

Окончание обновлений ..... 27 октября 2024 г., 13:59

Окончание технической поддержки ..... 27 октября 2024 г., 13:59

Количество пользователей ..... 0 из 10 000

Информация о модулях:

Антивирус Касперского для веб-трафика ..... 27 октября 2024 г., 13:59

Интеграция с Active Directory/Samba DC ..... 27 октября 2024 г., 13:59 (не используется)

Контроль приложений ..... 27 октября 2024 г., 13:59

Предотвращение вторжений ..... 27 октября 2024 г., 13:59

Правила IPS от Лаборатории Касперского ..... 27 октября 2024 г., 13:59

Расширенный Контент-фильтр ..... 27 октября 2024 г., 13:59

IPsec (входящие)

Статус	Название	Вх. скорость, Мбит/с	Исх. скорость, Мбит/с	Средняя задержка, мс	Потеря пакетов, %	Джиттер, мс
	IPsec1	–	–	–	–	–

Загрузка IPsec (входящие), Мбит/с

Данные отсутствуют

13.1 Особенности отображения информации:

- График загрузки интерфейсов включает весь трафик NGFW, в том числе служебный;
- При выборе разных промежутков времени отображаемые максимальные значения на графике могут отличаться;
- Таблица **Топ 5 хостов** включает только 5 пользователей с наибольшей скоростью входящего (исходящего) трафика соответственно. При формировании статистики по хостам учитываются протоколы, определенные модулем контроля приложений. При этом не учитывается служебный трафик NGFW.

14. Пользователи

14.1 Учетные записи

14.1.1 Основное

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

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

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

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

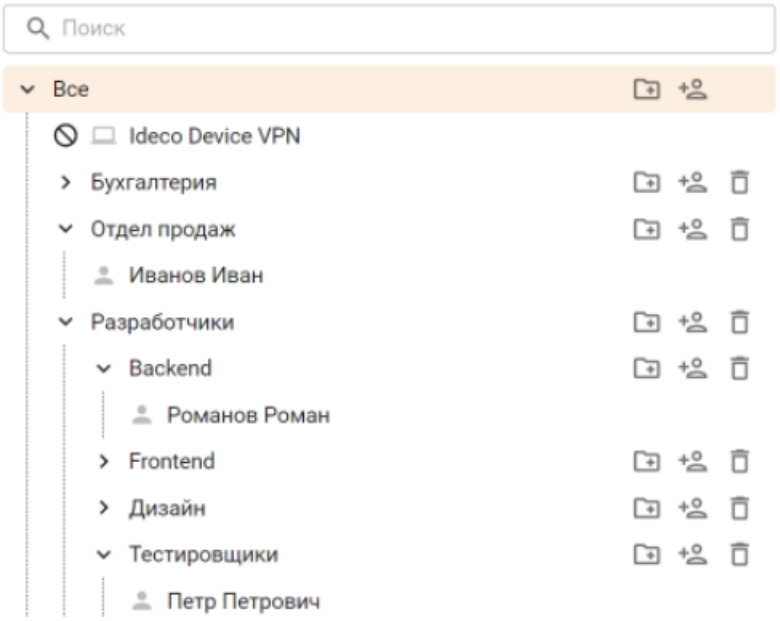
Цвет пиктограммы пользователя зависит от состояния учетной записи пользователя:

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

Элементы управления в дереве пользователей:

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

Пример дерева пользователей:



14.1.2 Управление учетными записями и группами

Создание учетной записи пользователя

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

Способы создания учетной записи пользователя и группы:

Пользователь в определенной группе

1. Выберите группу, в которую добавится пользователя.

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

3. Заполните поля:

- **Имя пользователя** - имя пользователя, например, Иванов Иван. Максимальное количество символов - 128;
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32;
- **Пароль** и **Повторите пароль** -

- **Телефон** - телефон для *двухфакторной аутентификации*. Формат: +, код страны, код региона и номер телефона;
- **IP-адрес** и **MAC-адрес** - при заполнении этих полей создается правило авторизации в разделе **Пользователи -> Авторизации ->** ***IP и MAC авторизация*** и создается аналогичная привязка в *DHCP-сервере* Ideco NGFW.

4. Нажмите **Добавить**.

Пользователь вне групп

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

2. Нажмите  :

3. Заполните поля:

- **Имя пользователя** - имя пользователя, например, Иванов Иван. Максимальное количество символов - 128;
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.** Максимальное количество символов - 32;
- **Пароль** и **Повторите пароль** -
- **Телефон** - телефон для *двухфакторной аутентификации*. Формат: +, код страны, код региона и номер телефона;
- **IP-адрес** и **MAC-адрес** - при заполнении этих полей создается правило авторизации в разделе **Пользователи -> Авторизации ->** ***IP и MAC авторизация*** и создается аналогичная привязка в *DHCP-сервере* Ideco NGFW.

4. Нажмите **Добавить**.

Создание группы

1. Нажмите  справа от названия группы.

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

Предупреждение: Не используйте Numpad при введении пароля. Это может привести к проблемам при авторизации пользователя.

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

Для учетных записей, импортированных из Active Directory, проверка пароля осуществляется средствами Active Directory.

Рекомендации к созданию сложности паролей:

Доступна автоматическая генерация пароля!

- минимальная длина - 11 символов;
- использование строчных и заглавных латинских символов;
- использование цифр и специальных символов.

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

Удаление учетной записи пользователя или группы

Реализовано два варианта удаления:

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

Перемещение учетной записи пользователя

1. Выберите учетную запись или группу.

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

Редактирование учетной записи пользователя

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

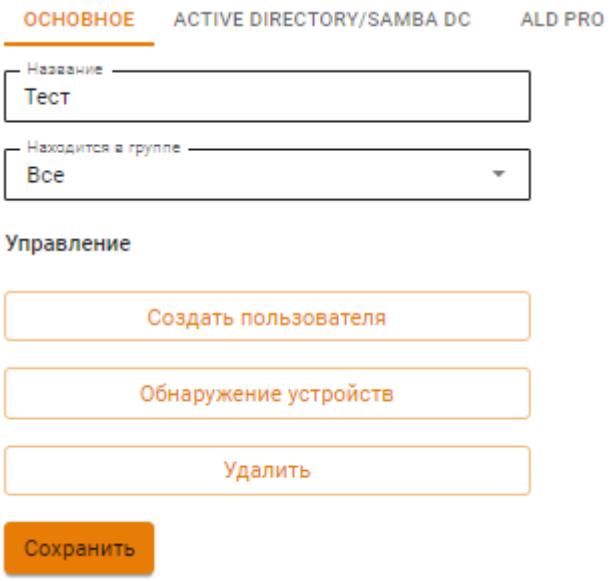
14.1.3 Настройка пользователей

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

Группы пользователей

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

Основное



- **Изменить название и вложенность группы**. Для этого в соответствующем поле введите новое название и укажите группу, в которую требуется переместить эту группу;
- **Создать пользователя**. При нажатии на одноименную кнопку появится форма создания пользователя;

- **Обнаружение устройств**. При нажатии на одноименную кнопку откроется раздел *Обнаружение устройств*;
- **Удаление группы**. Вместе с группой удаляются учетные записи пользователей группы и привязки по IP- и MAC-адресам.

Active Directory/Samba DC

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

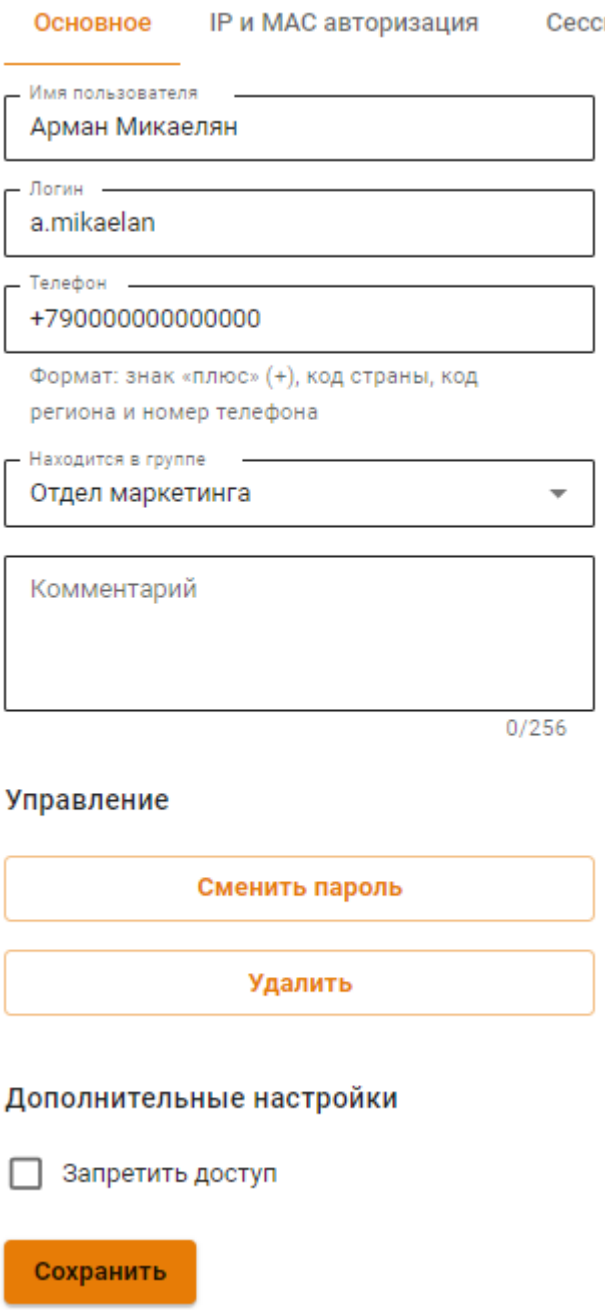
ALD Pro

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

УЗ пользователей

Основное

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



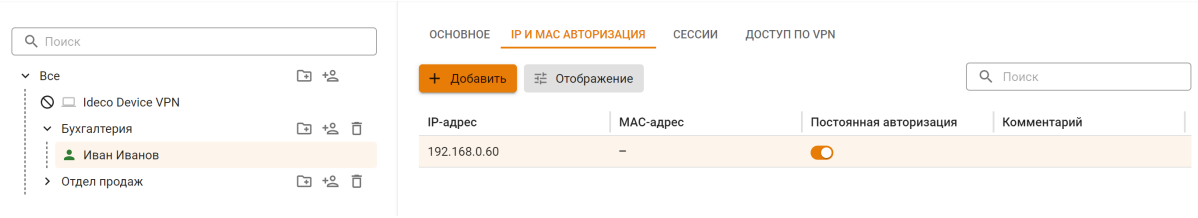
- **Имя пользователя** - имя пользователя, например, Иванов Иван. Максимальное количество символов - 128;
- **Логин** - будет применяться пользователем для авторизации в различных службах Ideco NGFW. Логин необходимо вводить латинскими символами в нижнем регистре. **Не используйте в качестве логина IP-адрес.**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

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

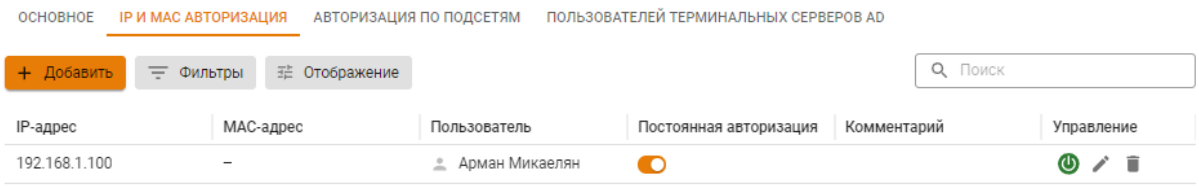
IP и MAC авторизация

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

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



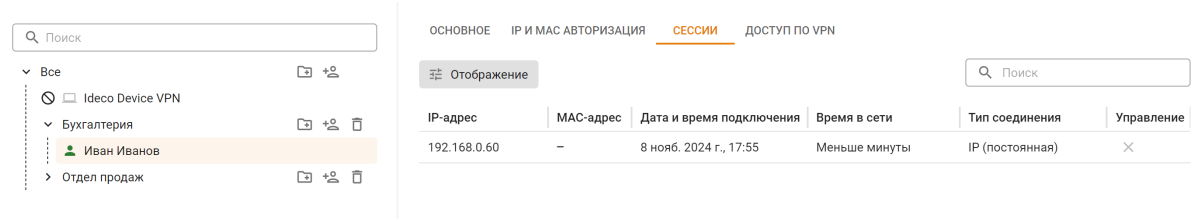
- **Пользователи -> *Авторизации* -> *IP и MAC авторизация***:



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

Сессии

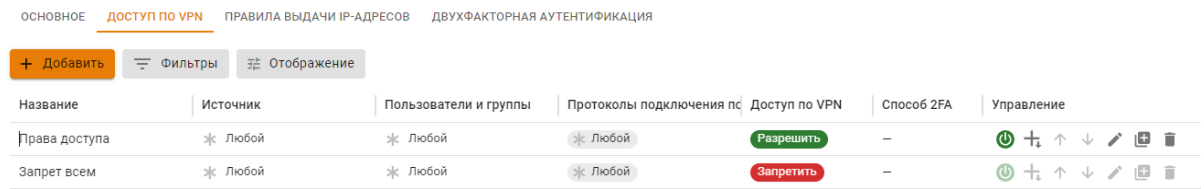
Содержит таблицу с информацией обо всех активных сессиях пользователях:



При нажатии на ✕ в столбце **Управление** NGFW разорвет сессию пользователя.
Аналогичная таблица расположена в разделе **Мониторинг -> *Авторизованные пользователи***.

Доступ по VPN

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



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

14.2 Авторизация пользователей

Подсказка: Название службы раздела **Авторизация**: `ideco-auth-backend`.
Список служб для других разделов доступен по *ссылке*.

Авторизация - необходимое условие для доступа пользователя в интернет. Для работы в пределах локальной сети авторизация не требуется.

Для доступа сетевого устройства (хоста) в интернет через NGFW с возможностью контроля его трафика оно должно быть авторизовано на NGFW под учетной записью пользователя.

Особенности авторизации пользователей в Ideco NGFW:

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

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

14.2.1 Общая информация

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

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

При авторизации по VPN:

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

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

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

Если разорвать шестую сессию, то первая сессия снова станет активной, а иконка исчезнет.

Пользователь автоматически разавторизуется при неактивности (отсутствии соединений с интернетом) в течение указанного в настройках времени (кроме подключений по VPN).

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

Время автоматической разавторизации можно изменить с помощью настройки **Тайм-аут отключения** в разделе **Пользователи -> Авторизация**:

В нижней части формы в раскрывающемся списке выберите требуемое значение **Тайм-аута отключения**.

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

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

14.2.2 Веб-аутентификация

Основное

Подсказка: Название службы раздела **Веб-аутентификация**: `ideco-web-authd`.
Список служб для других разделов доступен по *ссылке*.

Подсказка: Поддерживаемые браузеры:

- Google Chrome, версия >= 90;
- Firefox, версия >= 78;
- Safari, версия >= 14.

Веб-аутентификация в Ideco NGFW - тип авторизации, который предполагает, что отправленный через веб-браузер запрос неавторизованного пользователя будет переадресован на страницу авторизации Ideco NGFW. Переход по указанному запросу произойдет после успешной авторизации.

Для этого типа авторизации должны быть выполнены условия:

- На сетевой карте у пользователя в качестве шлюза/объединенных в цепочку нескольких шлюзов или при прямых подключениях к прокси по умолчанию указан IP-адрес локального сетевого интерфейса Ideco NGFW;
- До подключения к интернету работает **DNS-резолвинг адресов**. Иначе запрос браузера на адрес *example.com* не будет перенаправлен на шлюз, и в браузере не появится запрос логина и пароля.

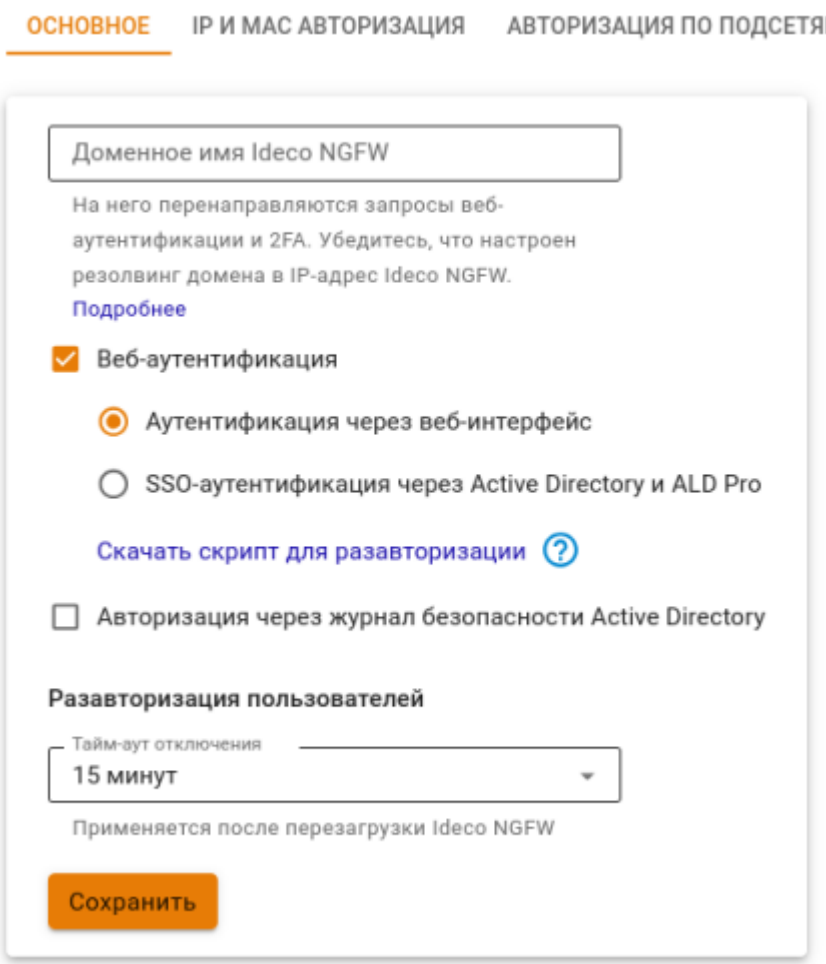
Проверить разрешение имен в Windows можно командой: `nslookup ya.ru`. Вывод данной команды должен содержать IP-адреса.

Подсказка: Рекомендуемые настройки для корректной работы веб-аутентификации:

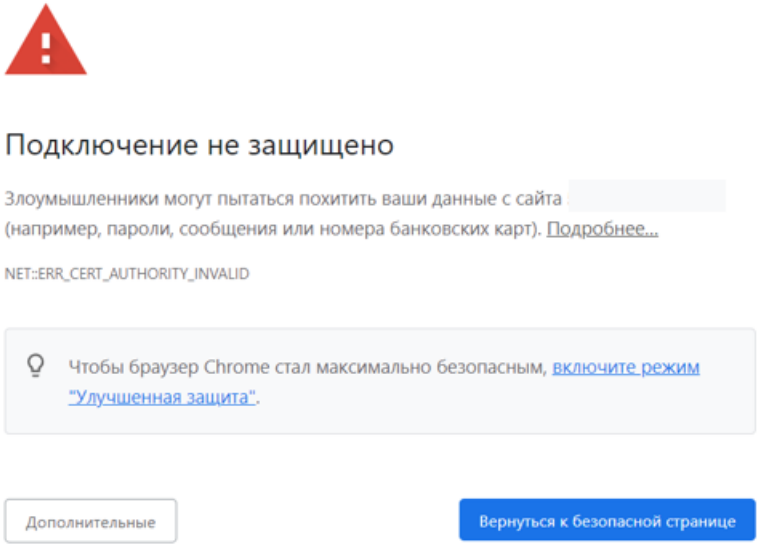
- При входе на HTTPS-сайт пользователь должен подтвердить доверие к сертификату Ideco NGFW, либо сертификат должен быть добавлен в доверенные корневые центры сертификации на устройстве (например, через политики домена);
- Рекомендуется указывать в качестве DNS-сервера на компьютерах и устройствах локальной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

Чтобы настроить авторизацию через веб-интерфейс, выполните действия:

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



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

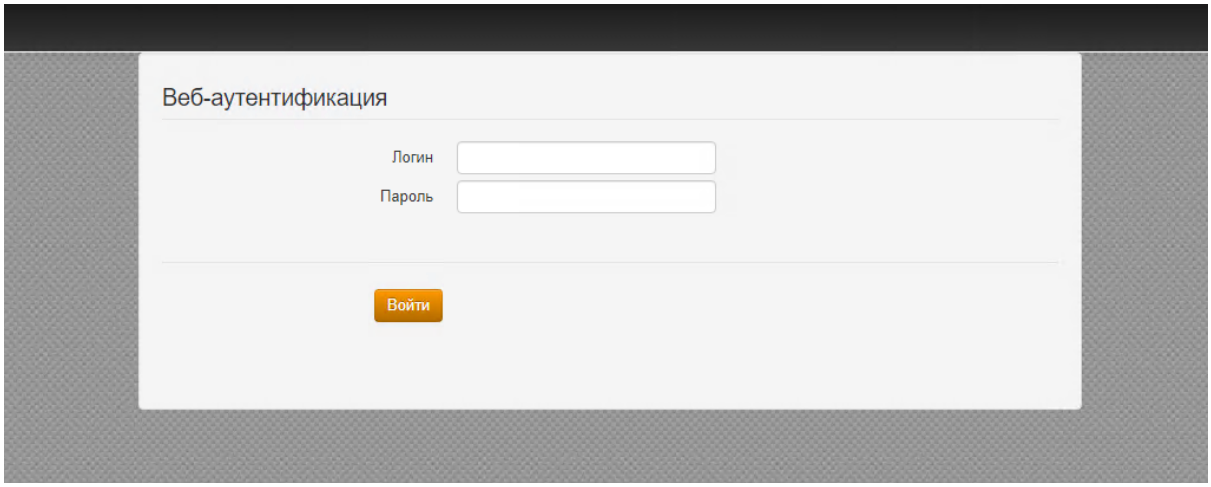


Подсказка: Если NGFW не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW, страница авторизации будет подписана корневым сертификатом NGFW.

Если сертификат для такого домена уже загружен в разделе *Сертификаты*, то будет использоваться он,

новый сертификат выдаваться не будет.

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



После прохождения пользователем веб-аутентификации доступ в интернет будет предоставлен до тех пор, пока авторизация не будет принудительно отменена или прекращена по неактивности пользователя.

Статьи с информацией об опции **SSO-аутентификация через Active Directory и ALD Pro**:

- *Аутентификация пользователей AD/Samba DC*;
- *ALD Pro*.

14.2.3 IP и MAC авторизация

Основное

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

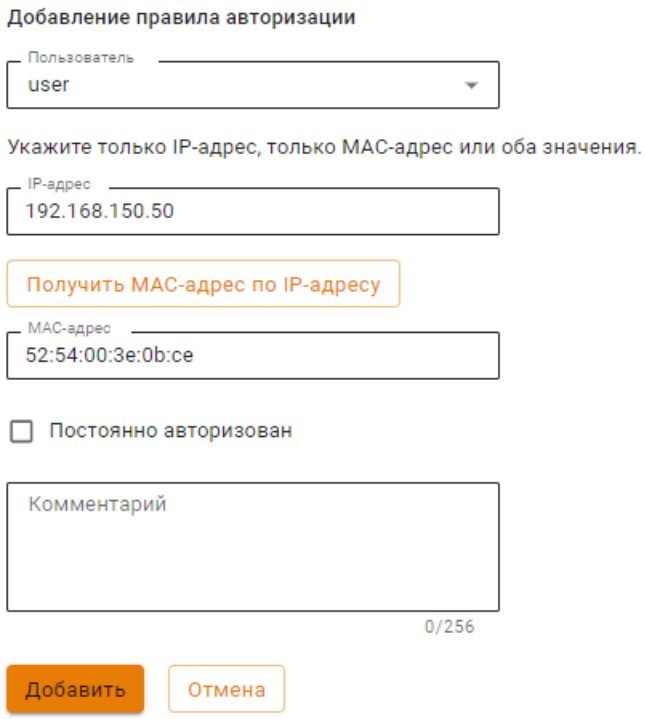
Правила **IP и MAC авторизации** создают аналогичную привязку в *DHCP-сервере* Ideco NGFW. Но если одни и те же IP- и MAC-адреса будут использоваться во включенных правилах DHCP-сервера, то правила DHCP-сервера будут выполняться в первую очередь.

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

Для настройки IP и MAC авторизации выполните действия:

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

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



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

3. Если вы хотите обеспечить непрерывный доступ в интернет, даже если пользователь не активен, установите флаг **Постоянно авторизован**.

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

Авторизация по IP-адресу

При авторизации по IP пользователь получает доступ в интернет без ввода логина и пароля сразу после инициации подключения.

Доступна авторизация сетевых устройств (камеры видеонаблюдения, сетевые принтеры и прочее), которые находятся в разных с Ideco NGFW широковещательных доменах и требуют доступ в интернет.

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

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

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

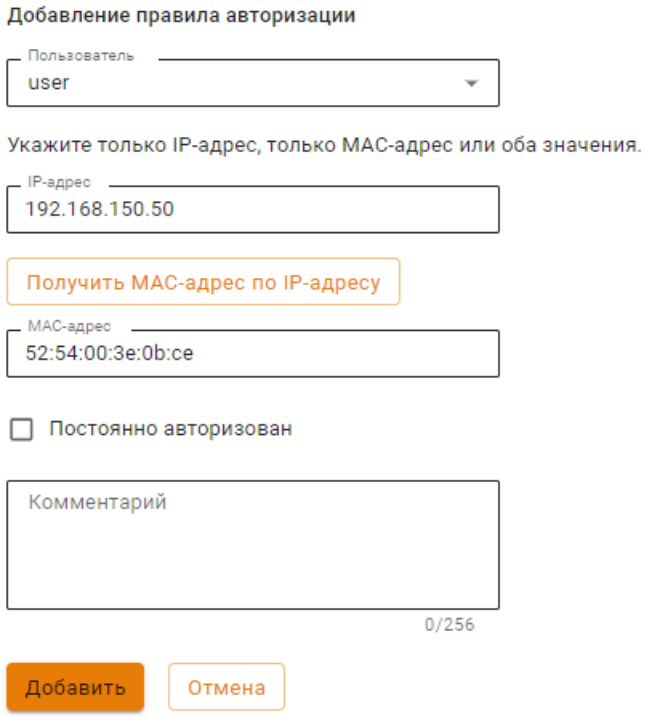
Настройка авторизации по IP

Для авторизации пользователя по IP-адресу выполните действия:

1. Создайте *пользователя* для авторизации по IP в Ideco NGFW или импортируйте его, например, из *Active Directory*.

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

3. Создайте правило-связку **IP-адрес < Пользователь**:



IP-адрес на устройстве, с которого инициируется сессия, должен совпадать с указанным в правиле. Кнопка **Получить MAC по IP** будет активна, если IP пользователя и IP Ideco NGFW в одной подсети.

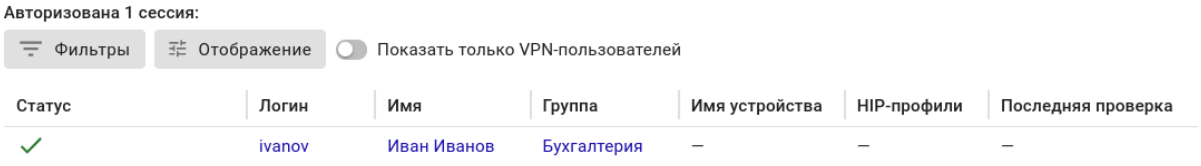
Рекомендации по использованию авторизации по IP-адресу:

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

Предупреждение: При использовании авторизации по IP со статической привязкой в DHCP рекомендуем перенести такие правила на *авторизацию по MAC-адресу*.

Просмотр сессии

После запроса пользователя в интернет на NGFW в разделе **Мониторинг -> Авторизованные пользователи** автоматически создается сессия с типом авторизации `IP`:



У сессий с типом `IP` не заполняется поле **MAC-адрес**, так как уже указан IP-адрес, необходимый для создания сессии.

Авторизация по MAC-адресу

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

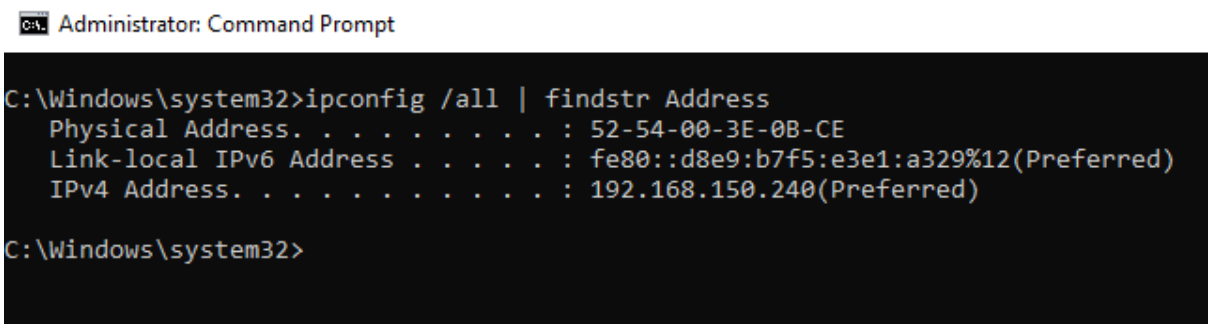
Для авторизации пользователя на NGFW по MAC-адресу оба устройства должны находиться в одном широковещательном домене, а NGFW должен выступать шлюзом для устройств.

Подсказка: Пользователи, находящиеся за роутером в локальной сети NGFW, не могут авторизоваться по MAC-адресу, так как роутер разделяет широковещательные домены и не обрабатывает трафик уровня L2. Такие пользователи могут авторизоваться только по IP-адресу.
Для работы MAC-авторизации необходимо, чтобы NGFW и пользователь находились в одном L2-сегменте сети.

Настройка авторизации по MAC

Для авторизации пользователя по MAC-адресу выполните действия:

1. Узнайте MAC-адрес устройства. Для этого в командной строке Windows введите `ipconfig /all | findstr Address` или `ipconfig /all | findstr адрес` (для русскоязычной версии):



2. Удостоверьтесь, что устройство пользователя и NGFW находятся в одном широковещательном домене. Для этого в разделе **Управление сервером -> Терминал** веб-интерфейса NGFW введите команду `ip neigh`:

```
[admin@localhost ~]# ip neigh
169.254.1.6 dev lb_local_in lladdr 2a:c5:87:bd:f7:f4 REACHABLE
192.168.150.1 dev Leth5 lladdr 52:54:00:26:9b:cf REACHABLE
192.168.150.110 dev Leth5  FAILED
192.168.150.240 dev Leth5 lladdr 52:54:00:3e:0b:ce REACHABLE
169.254.1.1 dev lb_local_out lladdr 5e:59:17:77:be:84 STALE
192.168.122.1 dev Eeth4 lladdr 52:54:00:06:1a:f0 REACHABLE
[admin@localhost ~]#
```

Эта команда выводит ARP-таблицу NGFW. Наличие записи с MAC-адресом устройства и статусом REACHEBLE - маркер L2-доступности между NGFW и устройством пользователя.

3. Создайте правило-связку **Пользователь < MAC-адрес** в разделе **Пользователи -> Авторизация -> IP и MAC авторизация**.

Сессия с типом авторизации `MAC` отобразится в разделе **Мониторинг -> Авторизованные пользователи**:

Предупреждение: Для MAC-адресов невозможно настроить постоянную авторизацию, т. к. для создания авторизованной сессии необходим IP-адрес. Рекомендуем использовать MAC-авторизацию в комбинации с *DHCP-сервером*.

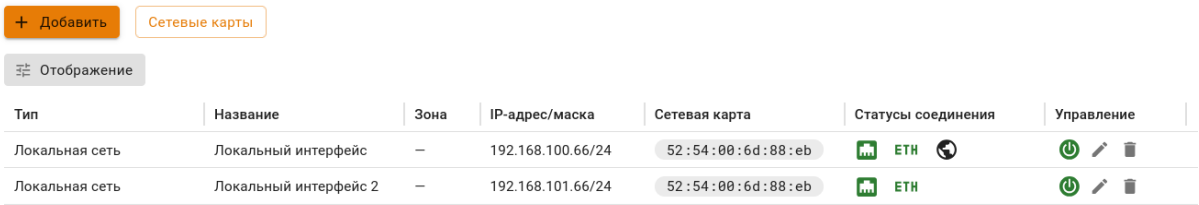
Поведение MAC-авторизации при перемещении устройства между локальными сетями

В организациях часто возникает ситуация, когда необходимо перемещаться между локальными сетями с ноутбуком и при этом всегда оставаться в сети. В таких случаях рекомендуем использовать авторизацию по MAC-адресу.

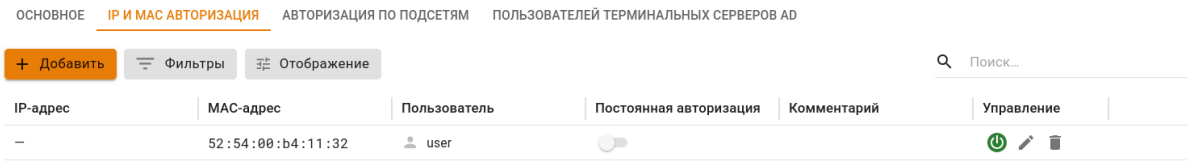
Для авторизации по MAC настройте DHCP-сервер (собственный или на NGFW). В раздаваемых реквизитах шлюзом должен выступать локальный интерфейс NGFW.

Пример. Пользователю `user` понадобилось переместиться с ноутбуком между локальными сетями:

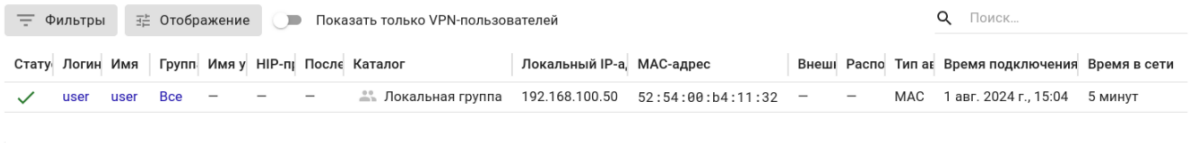
- На NGFW настроены локальные интерфейсы:



- Настроено правило авторизации пользователя по MAC-адресу:



- У пользователя одна активная сессия в разделе **Авторизованные пользователи**:



При переходе пользователя из одной локальной сети в другую ему выдаются другие сетевые реквизиты от DHCP-сервера, в которых шлюзом указан NGFW. При обнаружении любой активности пользователя появится вторая сессия авторизации по MAC-адресу:

Подсказка: Если у пользователя не появляется доступ и вторая сессия с авторизацией по MAC-адресу, следует обновить сетевые реквизиты.

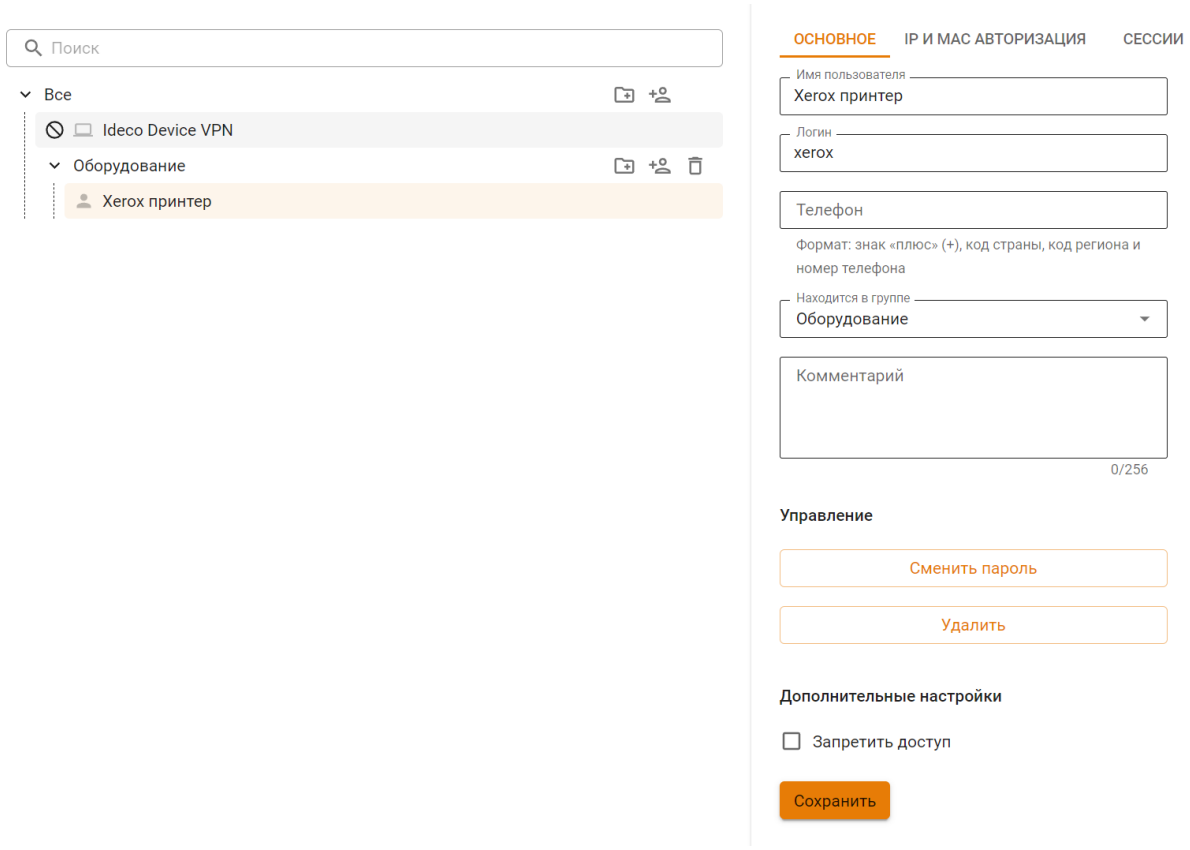
Сбросьте старые сетевые реквизиты от DHCP-сервера и получите новые с помощью команд:

- Windows - `ipconfig /release && ipconfig /renew`;
- Linux - `sudo dhclient -r <имя_интерфейса>`.

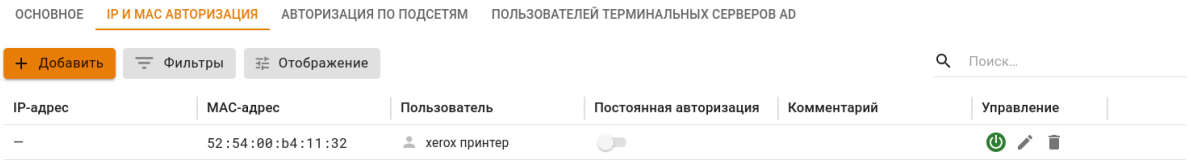
Настройка авторизации по MAC-адресу для сетевого принтера и других сетевых устройств

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

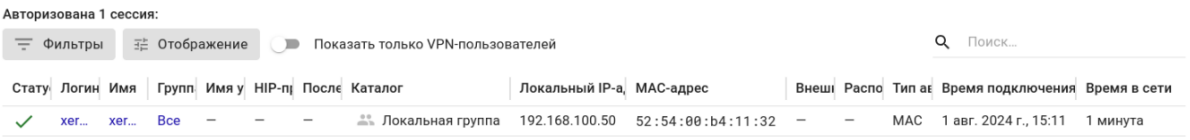
Чтобы авторизовать сетевой принтер, необходимо создать пользователя на NGFW вручную или через *Обнаружение устройств*:



В разделе **Пользователи -> Авторизация -> IP и MAC авторизация** для сетевого принтера необходимо создать правило **Пользователь < MAC-адрес**:



При обнаружении активности от сетевого принтера или другого устройства сессия пользователя появится в **Мониторинг -> Авторизованные пользователи**:



Подсказка: Опция **Рандомизация MAC-адреса** будет мешать при авторизации мобильного устройства по MAC-адресу. Рекомендуется эту опцию отключать либо использовать другие типы авторизации (например, *Веб-аутентификацию*)

14.2.4 Авторизация по подсетям

Основное

Чтобы не регистрировать каждое устройство в виде отдельного пользователя NGFW и не фиксировать для него факторы авторизации, можно создать правило авторизации на вкладке **Авторизация по подсетям**.

Эта функция позволяет пользователю NGFW авторизоваться автоматически из требуемой подсети без привязки к конкретному IP/MAC-адресу. Правила авторизации по подсетям полезны, когда требуется автоматически авторизовать большое количество устройств. Трафик по всей подсети фиксируется на одного пользователя.

Будьте внимательны при создании правил Авторизации по подсетям! Возможны проблемы, если:

- Для разных пользователей созданы пересекающиеся сети;
- В правиле **Авторизации по подсетям** созданы правила авторизации пользователей по IP-адресам из подсети;
- В подразделе **Правила выдачи IP-адресов** созданы правила с привязкой к IP-адресу из подсети правила **Авторизации по подсетям**.

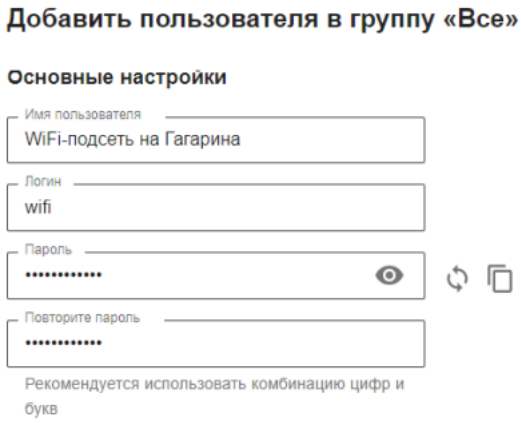
Подсказка: В сети, для которой создано правило **Авторизации по подсетям**, возможна работа DHCP.

Пример. В подсети 192.168.10.0/24 есть Wi-Fi-подсеть, устройствам из которой нужно позволить авторизоваться.

Для создания правила авторизации выполните действия:

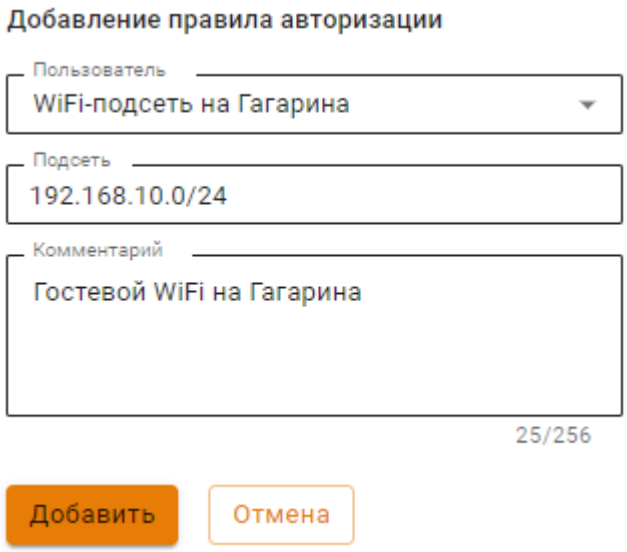
1. Перейдите в раздел **Пользователи –> Учетные записи** и нажмите **Добавить пользователя**.

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



3. Перейдите в раздел **Пользователи –> Авторизация –> Авторизация по подсетям** и нажмите **Добавить** в левом верхнем углу.

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



- **Пользователь** - выберите созданного в п. 2 пользователя;
- **Подсеть** - введите IP и маску подсети;
- **Комментарий** - необязательное поле.

Подсказка: При включении или отключении опции авторизации по подсетям может наблюдаться задержка в работе Ideco NGFW.

14.2.5 Авторизация пользователей терминальных серверов

Особенности работы для пользователей терминальных серверов AD:

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

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

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

Возможна **раздельная авторизация пользователей** терминального сервера, работающего под управлением ОС Windows Server 2008 R2 и Windows Server 2012, с помощью авторизации через *Ideco Client* или по *SSO (NTLM)*. При этом сам сервер по IP авторизовывать не нужно.

Для раздельной авторизации пользователей терминального сервера:

- На сервере терминалов настройте **Remote Desktop IP Virtualization**;

- На сервере Ideco NGFW настройте авторизацию пользователей через *Ideco Client* или *веб-аутентификацию (SSO или NTLM)*.

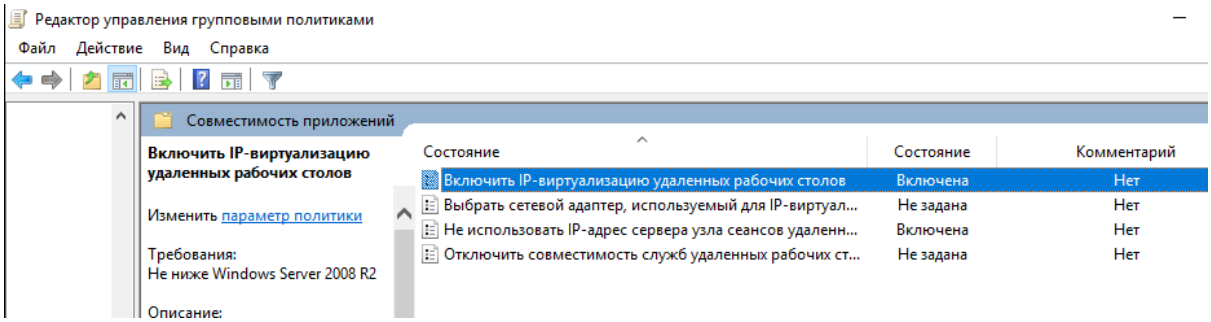
Подсказка: Авторизация пользователей терминального сервера по логам контроллера домена AD пока не реализована.

Настройка Remote Desktop IP Virtualization на Windows Server 2012

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

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

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



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

Командой `gpupdate /force` выполнить обновление всех политик.

Проверьте изменение настроек командой в PowerShell:

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

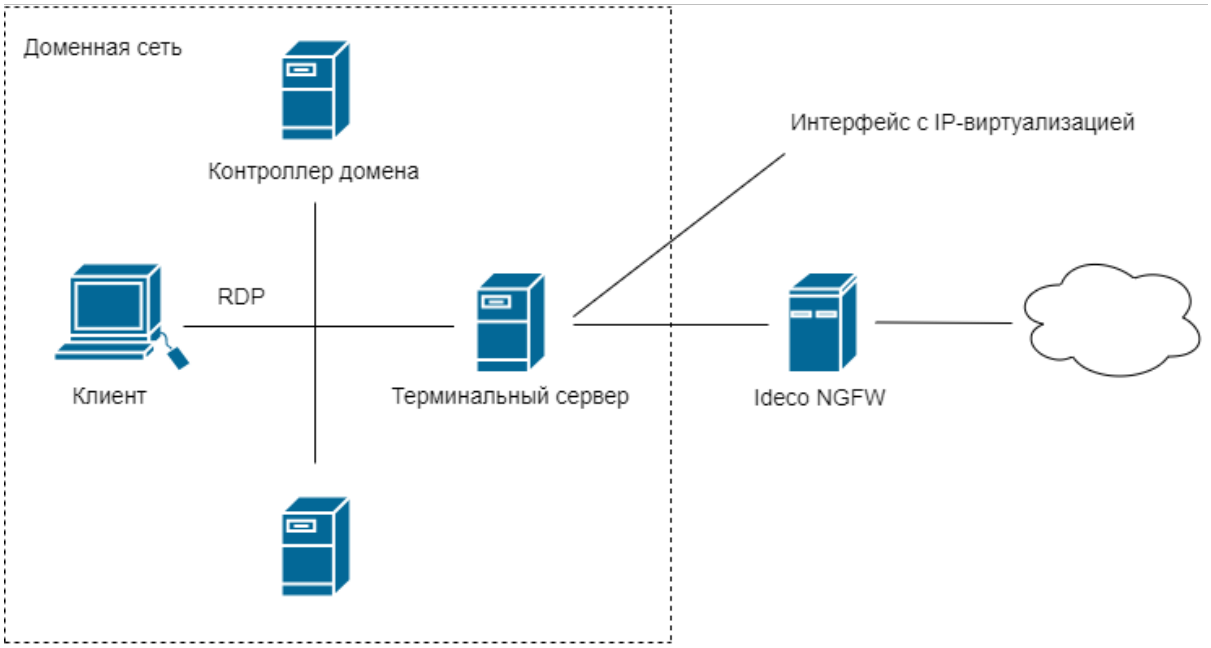
Значения:

- `VirtualIPActive = 1` - вкл. виртуализация;
- `VirtualIPMode=0` - для сессии.

Настройка Remote Desktop IP Virtualization на Windows Server 2022

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

Условия



1. Windows Server 2022 с ролью контроллера домена;

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

3. Ideco NGFW, введен в домен опционально;

4. Клиентские Windows-машины, введенные в домен;

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

Настройка

Подсказка: Все настройки выполняются от имени администратора.

Установите все последние обновления Windows Server и перезагрузите серверы.

На сервере с ролью терминального сервера выполните следующие действия:

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

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

2. Включите компонент IPFilterBitmaps:

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

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

Ключ: IPFilterBitmaps

Тип: REG_DWORD

Значение: 1

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

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

Ключ: IPFilterBitmaps

Тип: REG_DWORD

Значение: 1

3. Перезагрузите сервер.

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

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

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

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

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

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

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

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

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

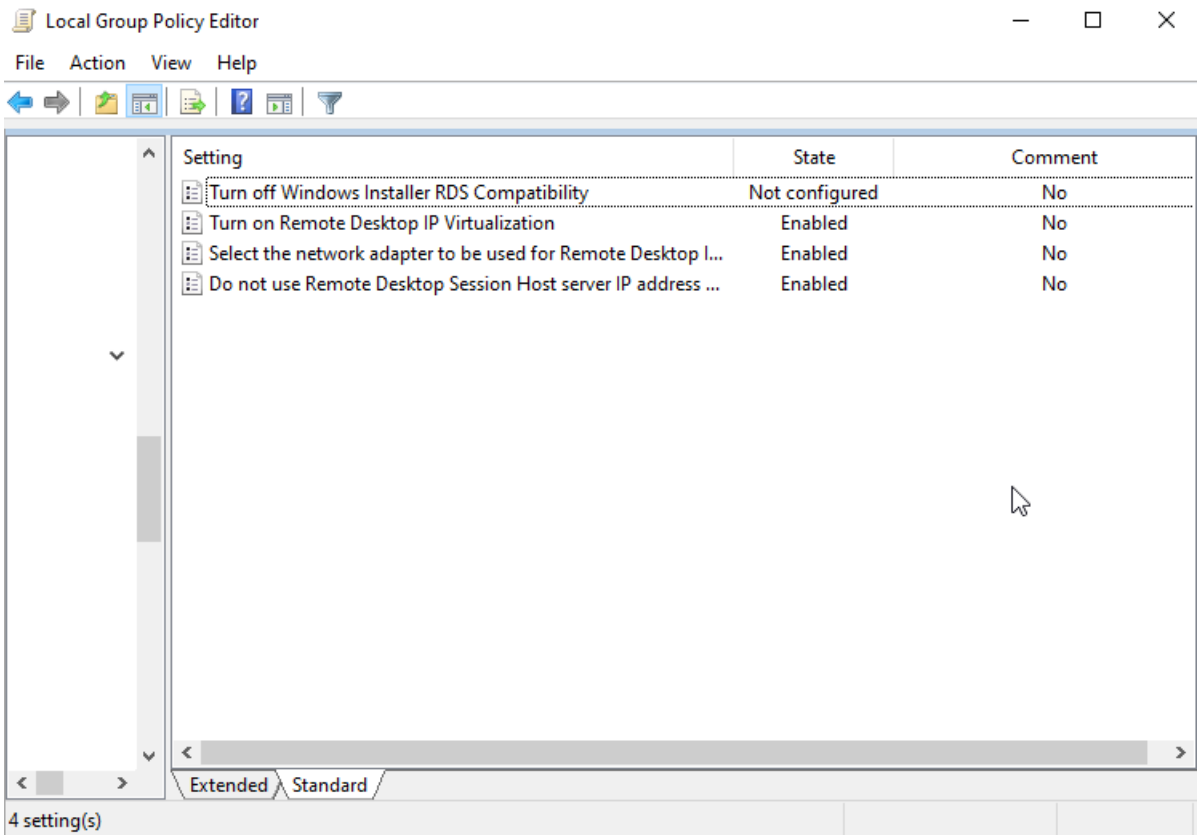
2. Включите параметр политики **Включить IP-виртуализацию удаленных рабочих столов** с параметром **Для сеансов**.

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

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

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

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



5. Повторно перезагрузите сервер.

Настройте выдачу виртуальных IP-адресов:

Для статической выдачи виртуальных IP-адресов на сервере с ролью терминального сервера:

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

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

Ключ: IPPool

Тип: REG_SZ (строковый параметр)

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

Настройте статический диапазон IP-адресов:

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

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

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

3. Перезагрузите сервер с ролью терминального сервера.

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

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

Путь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp

Ключ: RequiredPrivileges

Тип: REG_MULTI_SZ (многострочный параметр)

Значение:

```
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
```

Перезагрузите сервер с ролью DHCP-сервера.

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

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

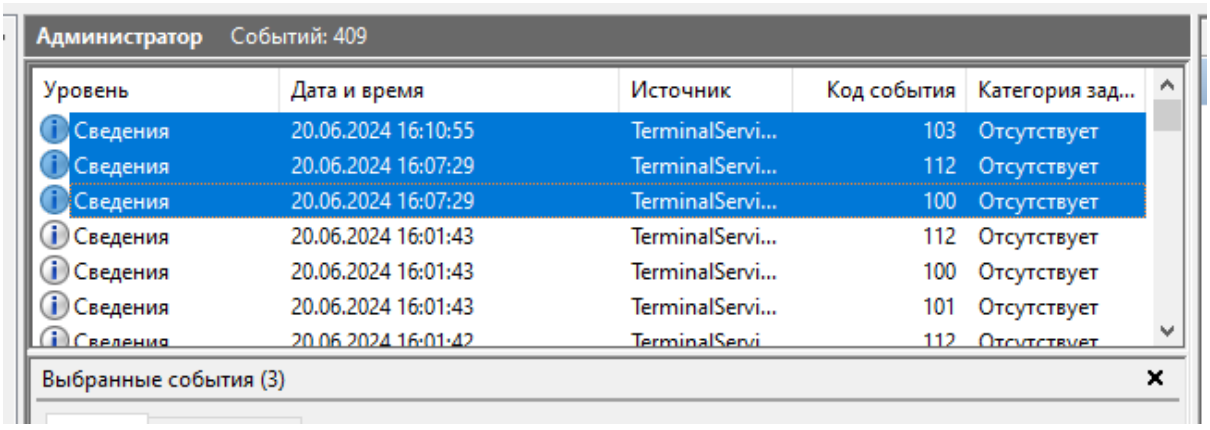
Диагностика

Виртуальные IP-адреса не выдаются

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

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

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



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

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

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

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

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

Подключения используют основной IP-адрес терминального сервера

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

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

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

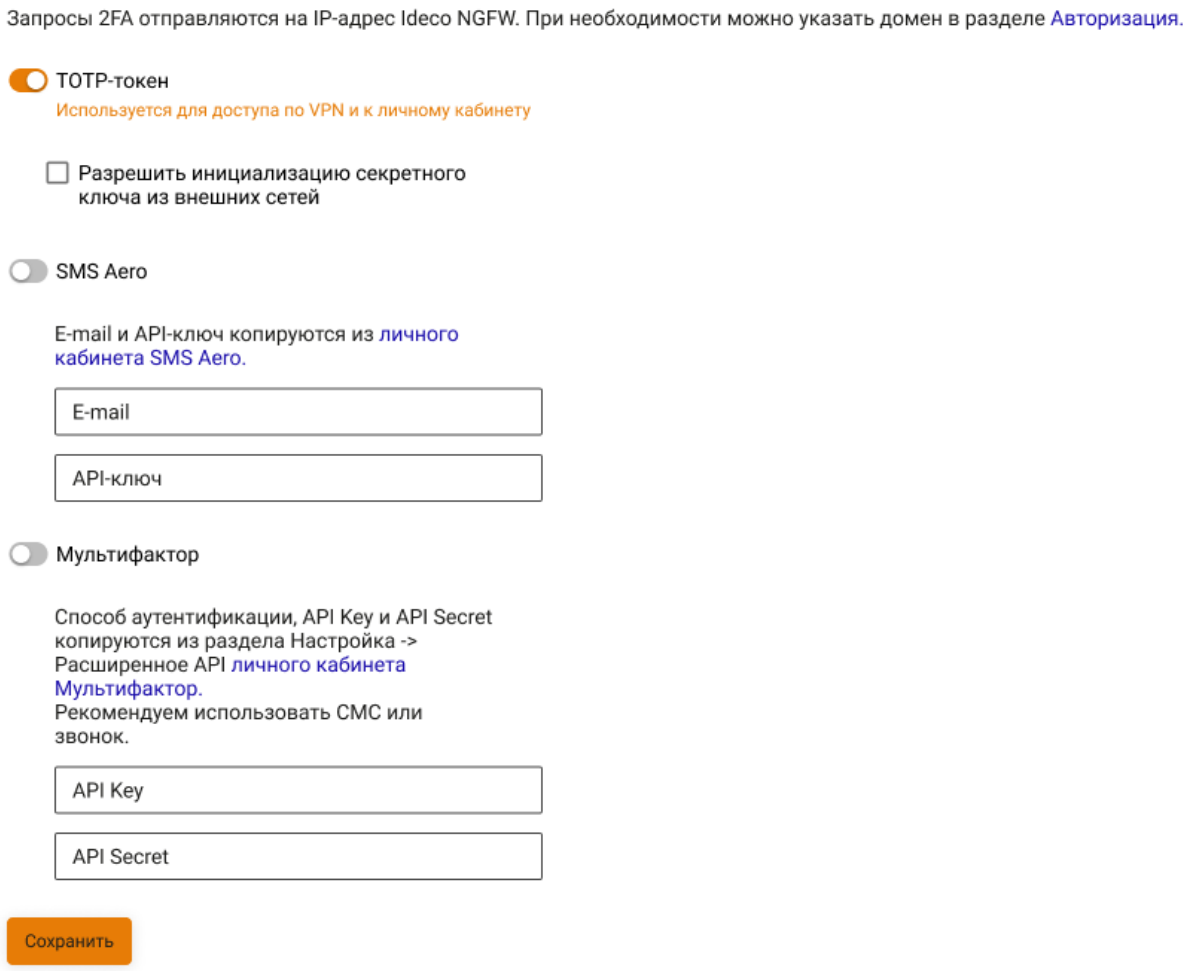
14.3 Двухфакторная аутентификация

Подсказка: Название службы раздела **Двухфакторная аутентификация**: `ideco-web-authd`.
Список служб для других разделов доступен по *ссылке*.

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

В Ideco NGFW реализовано три типа двухфакторной аутентификации:

- **TOTP-токен** - сканированием QR-кода или с помощью токена;
- **SMS Aero** - при помощи ввода кода из SMS;
- **Мультифактор** - путем подтверждения личности в приложении.



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

14.3.1 Настройки Ideco NGFW с разными типами аутентификации

Для работы двухфакторной аутентификации выполните действия:

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

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

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

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

TOTP-токен:

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

Видеоинструкция по настройке двухфакторной аутентификации Ideco NGFW с использованием TOTP-токена:

Ссылка на видеоинструкцию настройке двухфакторной аутентификации Ideco NGFW с использованием TOTP-токена

SMS Aero:

1. Зарегистрируйтесь в личном кабинете SMS Aero.

2. Введите E-mail и API-ключ от личного кабинета SMS Aero. API-ключ можно найти в разделе **Настройки -> API и SMPPI**.

3. Нажмите **Сохранить**.

Видеоинструкция по настройке двухфакторной аутентификации Ideco NGFW с использованием SMS Aero:

Ссылка на видеоинструкцию настройке двухфакторной аутентификации Ideco NGFW с использованием SMSAero

Мультифактор:

Помимо приложения Multifactor для аутентификации можно использовать Telegram, Яндекс.Ключ, Биометрию и U2F. Подробное описание регистрации и аутентификации этими методами доступно в документации Multifactor.

1. Зарегистрируйтесь в системе управления Мультифактором, установите приложение Multifactor и активируйте его, отсканировав QR-код.

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

3. Нажмите **Сохранить**.

Для дальнейшей аутентификации пользователям потребуется установить и настроить приложения, указанные администратором в настройках группы. Корректировать способы аутентификации для пользователей можно в личном кабинете Multifactor, в разделе **Группы -> Параметры -> Редактировать**.

Видеоинструкция по настройке двухфакторной аутентификации Ideco NGFW с использованием Мультифактора:

Ссылка на видеоинструкцию настройке двухфакторной аутентификации Ideco NGFW с использованием Мультифактора

4. Разрешите доступ по VPN нужным группам пользователей в разделе **Пользователи -> VPN-подключения -> Доступ по VPN**, воспользовавшись *инструкцией*.

Подсказка: При отключении типа аутентификации, который используется в таблице **Доступ по VPN**, будет выведено предупреждение **Используется для доступа по VPN**. При этом аутентификация пройдет без второго фактора.

14.3.2 Настройка аутентификации на пользовательских устройствах

Для настройки двухфакторной аутентификации на устройстве пользователя воспользуйтесь инструкциями:

TOTP-токен:

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

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

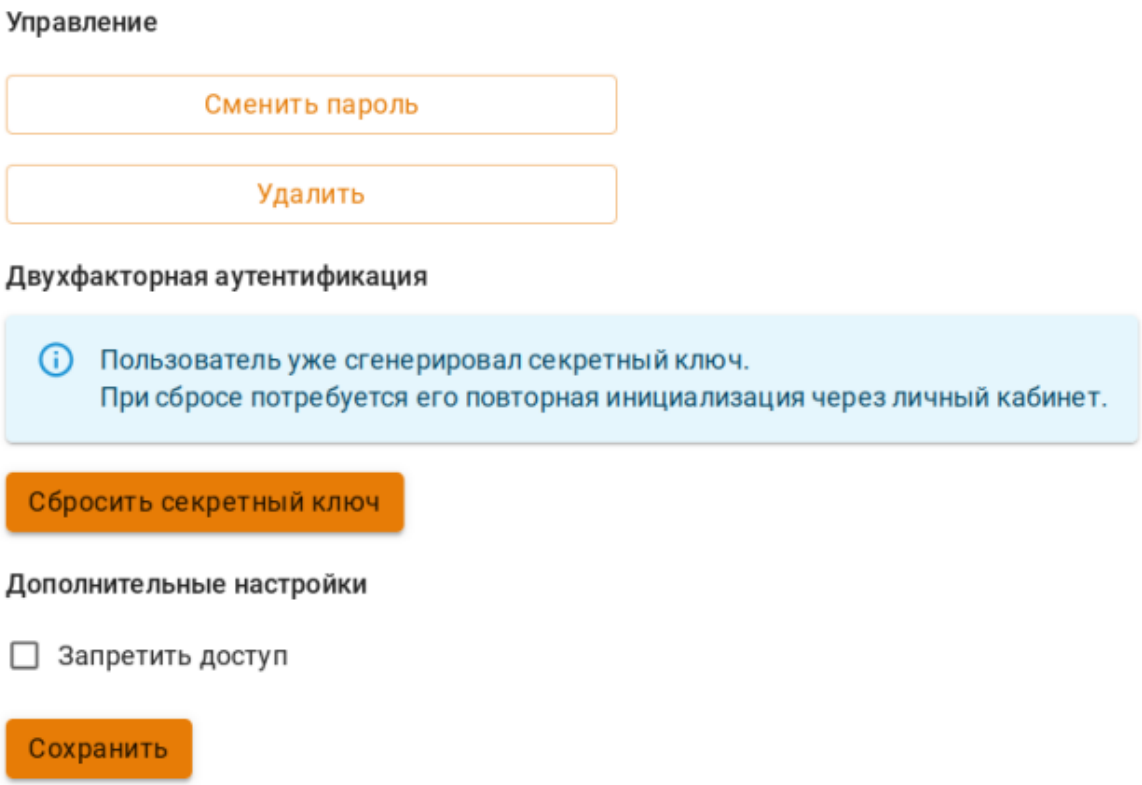
3. Нажмите кнопку **Настроить двухфакторную аутентификацию** и выберите **Сгенерировать QR-код**:

Сгенерированный QR-код появится на экране.

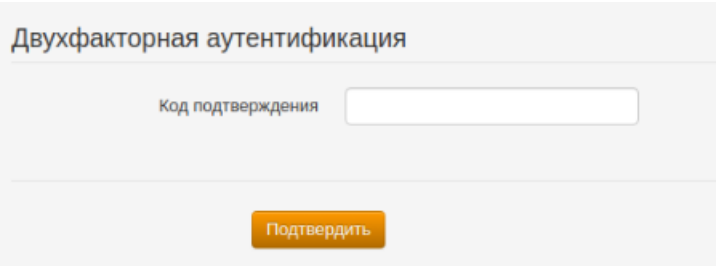
4. Войдите в приложение для аутентификации (Яндекс Ключ, Google Authenticator или Microsoft Authenticator и т.п.), отсканируйте код или введите секретный ключ, который находится под QR-кодом. При вводе ключа выберите тип ключа **По времени**. Если выбрать тип **По счетчику**, то пользователь не сможет пройти аутентификацию.

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

Чтобы сбросить секретный ключ, перейдите в раздел **Пользователи -> Учетные записи**. Выберите нужного пользователя и нажмите **Сбросить секретный ключ**:



5. Подключитесь к VPN и откройте любой сайт, не использующий **HSTS** (например, neverssl.com). В появившемся поле введите код, который вы получили в приложении:



Особенности использования TOTP-токена:

- Для корректной работы необходимо, чтобы время на Ideco NGFW и устройстве пользователя было синхронизировано с точностью до минуты;
- Если секретный ключ был сброшен во время аутентификации пользователя и он не смог ее пройти, необходимо удалить сессию пользователя в разделе **Мониторинг -> Авторизованные пользователи**. Сессия будет автоматически завершена по истечении десяти минут бездействия.

SMS Aero:

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

2. Если требуется использовать подключение только для ресурсов подключаемой сети, убедитесь, что настройки VPN-подключения соответствуют требованиям:

Для Windows 10:

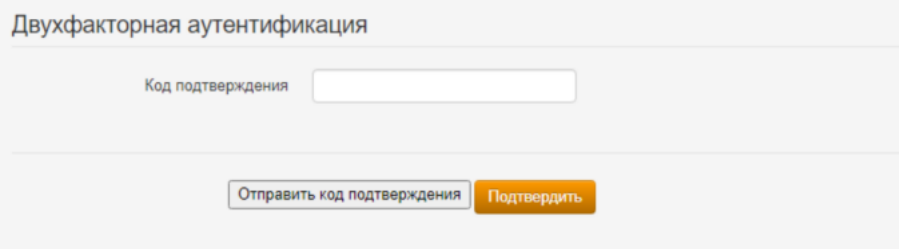
- Откройте параметры и перейдите в раздел **Сеть и Интернет -> VPN -> Настройка параметров адаптера**;
- Нажмите правой кнопкой мыши по созданному подключению и выберите **Свойства**;
- Перейдите на вкладку **Сеть**;
- Нажмите на **IP версии 4 (TCP/IPv4) -> Свойства -> Дополнительно**;
- Снимите флаг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

Для Ubuntu:

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

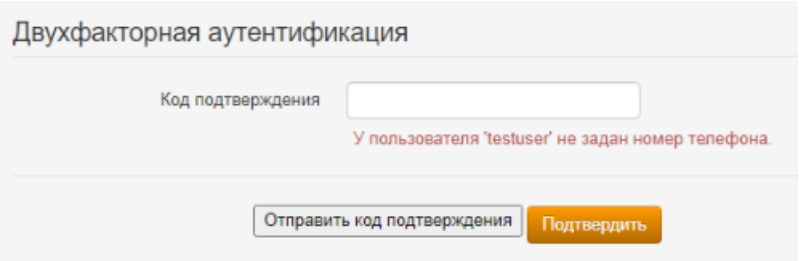
3. Включите созданное VPN-подключение.

4. Перейдете в браузер, откроется страница аутентификации:

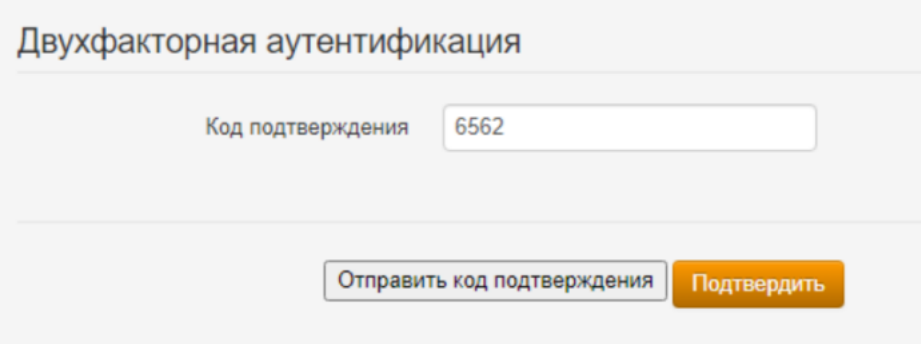


5. Нажмите **Отправить код подтверждения**. На номер телефона, указанный в учетной записи, придет SMS с кодом:

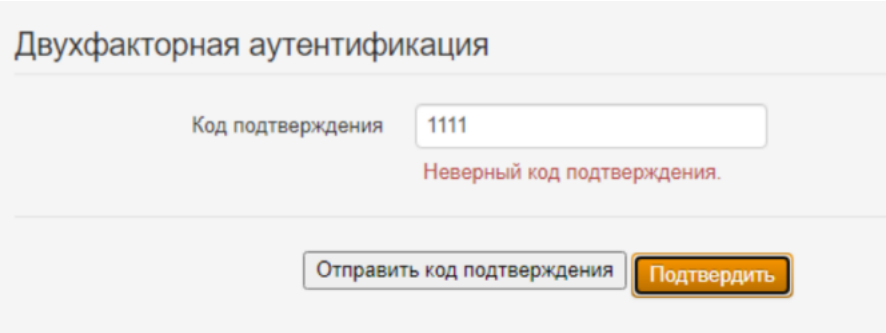
- Если номер телефона в карточке пользователя отсутствует, то на странице аутентификации появится предупреждение:



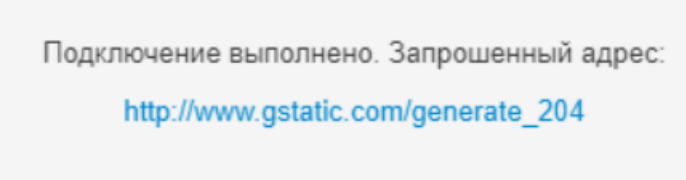
- Если номер телефона сохранен, то на указанный номер телефона поступит SMS. Введите код из SMS и нажмите **Подтвердить**:



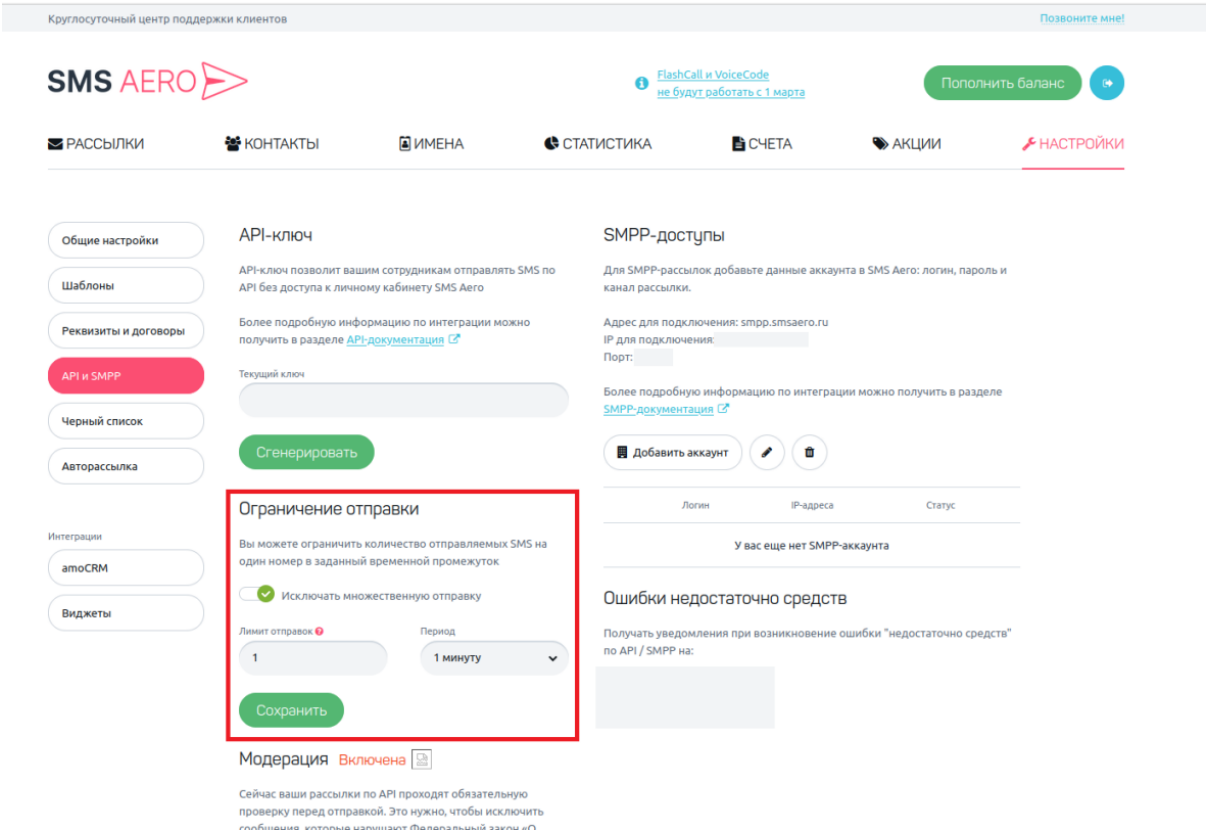
- Если код введен неверно, то появится соответствующее предупреждение:



- Если код введен верно, то появится окно:



Для настройки таймкодов отправки сообщений перейдите в личный кабинет SMS Aero на вкладку **Настройки** и переведите опцию **Исключать множественную отправку** в положение **Включен**. Затем введите лимит и период отправки сообщений:

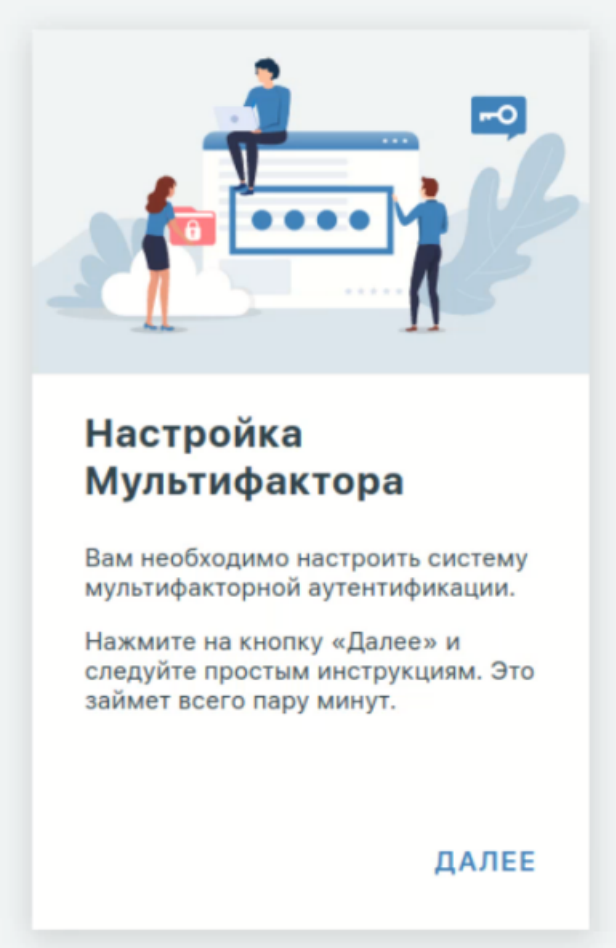


Мультифактор:

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

2. Включите созданное VPN-подключение.

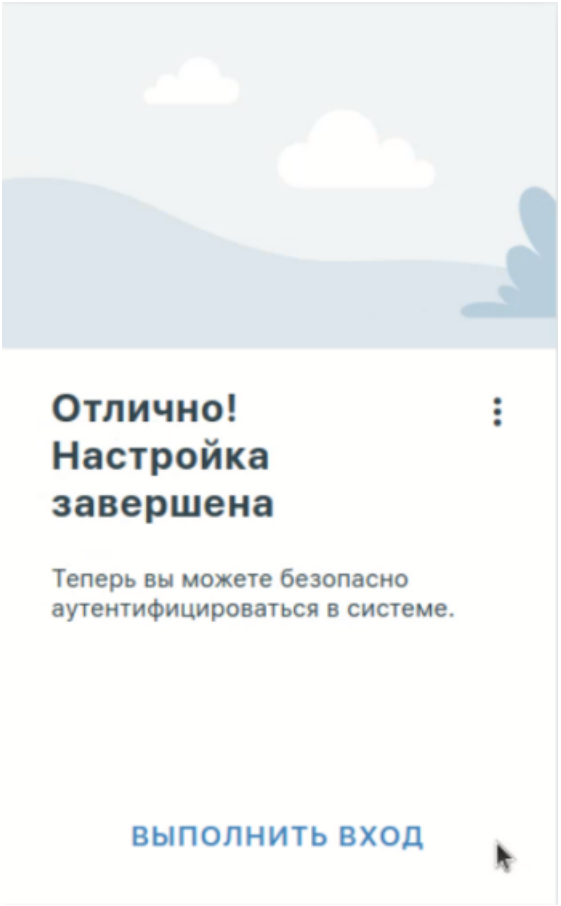
3. При переходе в браузер откроется страница аутентификации:



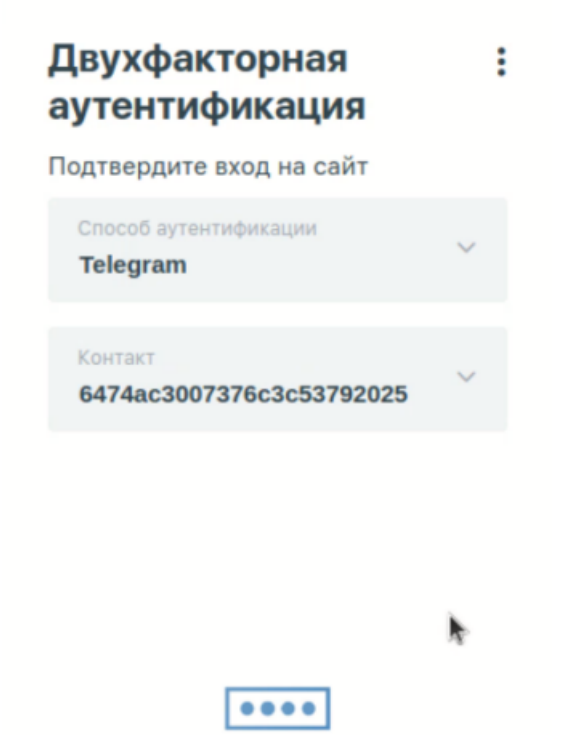
4. После нажатия **Далее** появится страница с предложением установить приложение на устройство пользователя. Если приложение установлено, нажмите **Далее**.

5. Отсканируйте QR-код или откройте ссылку, которая появится на экране.

6. Нажмите **Выполнить вход**:



7. В окне **Двухфакторная аутентификация** выберите способ аутентификации:



8. В зависимости от выбранного способа подтвердите вход.

14.4 VPN-подключение

Подсказка: Название службы раздела **VPN-подключения**: `ideco-accel-l2tp`; `ideco-accel-pptp`; `ideco-accel-sstp`; `ideco-vpn-servers-backend`; `ideco-vpn-authd`; `ideco-vpn-dhcp-backend`. Список служб для других разделов доступен по *ссылке*.

Для настройки VPN-сервера можно использовать VPN-клиент, который уже есть в операционной системе, или установить отдельный.

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

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

Настройка VPN-сервера происходит в несколько этапов:

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

14.4.1 Поддерживаемые протоколы

Ideco NGFW поддерживает четыре протокола туннельных соединений:

- *IKEv2* - рекомендуемый протокол с точки зрения скорости и безопасности;
- *SSTP* - подходит для использования в средах с ограничениями на порты;
- *L2TP/IPsec* - обеспечивает баланс между безопасностью и совместимостью;
- *PPTP* - не рекомендуется. Этот способ подключения **крайне небезопасен** и оставлен исключительно для совместимости со старыми решениями.

14.4.2 Предварительные требования

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

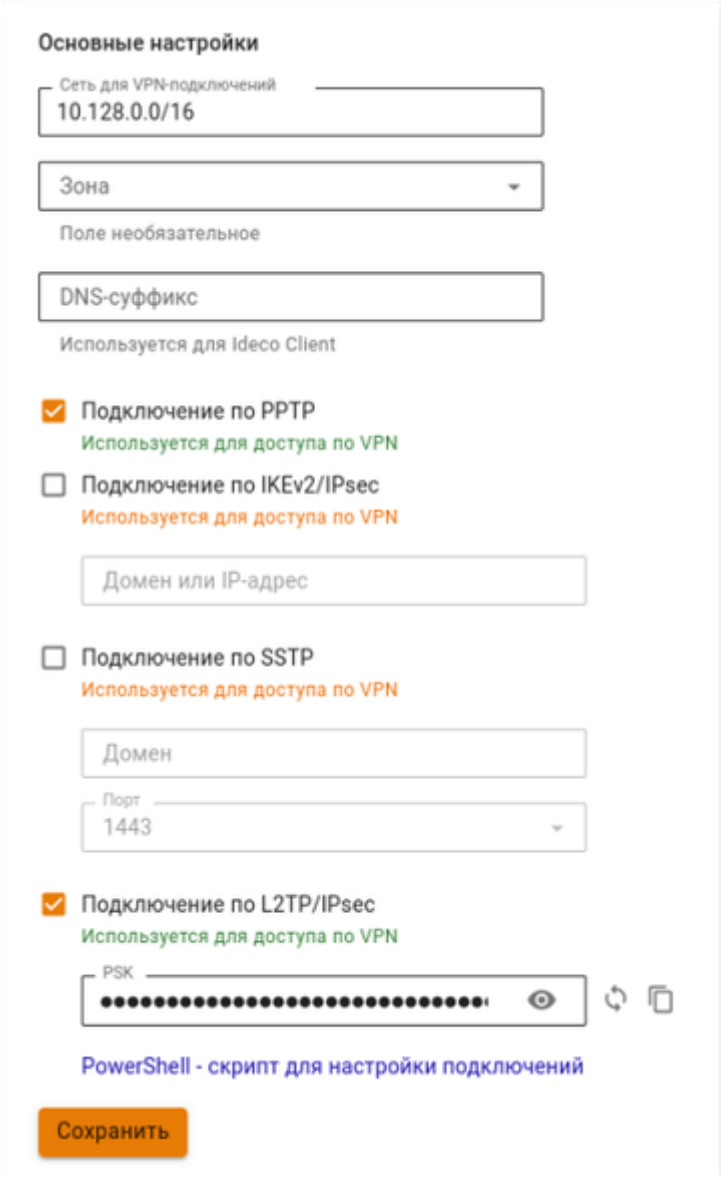
- Корневые сертификаты Ideco NGFW действительны в течение 10 лет;
- Если используется сертификат Let's Encrypt, обновление будет происходить автоматически.

14.4.3 Настройка VPN-подключения

Для настройки VPN-подключения перейдите в **Пользователи -> VPN-подключения**

Основное

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



- **Сеть для VPN-подключений** - укажите подсеть, в рамках которой будут динамически назначаться IP-адреса. Маска подсети должна быть в диапазоне от 16 до 30 бит.
- **Зона** - добавьте сетевые интерфейсы для подключения по VPN (опционально).
- В поле **Зона** добавьте сетевые интерфейсы для подключения по VPN (опционально).

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

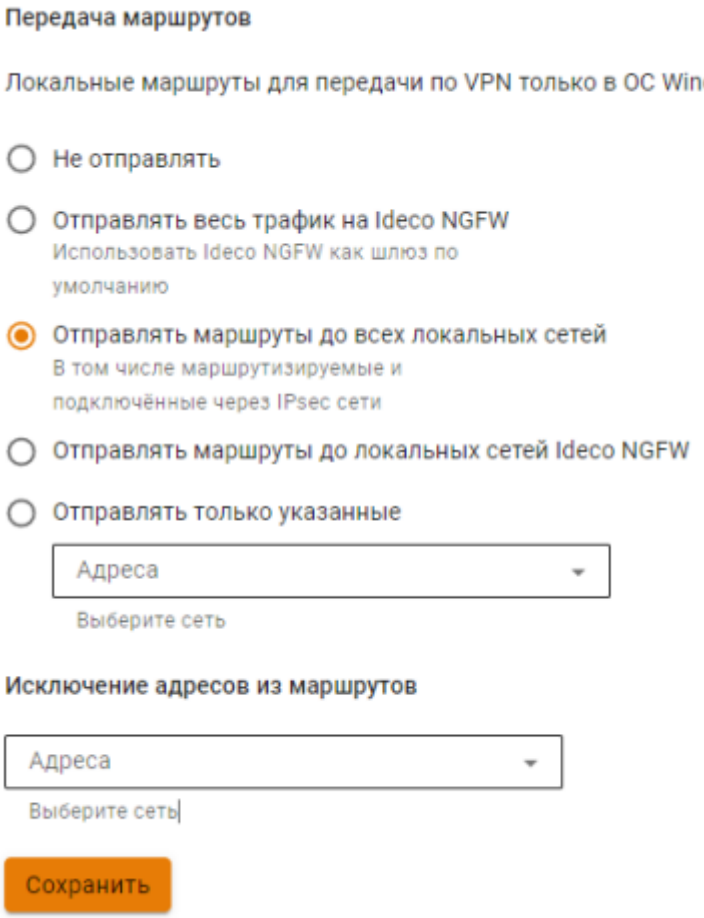
- **DNS-суффикс** - укажите DNS-суффикс, если для подключения по VPN используется *Ideco Client* (опционально).
- Выберите, какой какой протокол подключения будет использоваться.

Подсказка: Начиная с версии 16.0, для каждого протокола VPN-подключения отображается статус использования. Статусы отображаются в виде подсказок под названиями протоколов:

Зеленый статус: протокол включен и используется.

Оранжевый статус: протокол отключен, но используется в правилах доступа по VPN.

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



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

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

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

Предупреждение: Если при подключении по VPN (SSTP, IKEv2, PPTP, L2TP) не удается получить маршруты до сетей Ideco NGFW, то это связано с тем, что указанное число маршрутов не вмещается в опции DHCP-пакета.

При исключении подсети, IP-адреса, домена из передаваемого маршрута может возникнуть разбиение на несколько маршрутов. Это может привести к тому, что все маршруты не вместятся в опции DHCP-пакета.

Если количество байт в опции маршрутов превышает 255, то маршруты не передаются службой **ideco-vpn-dhcp-server**.

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

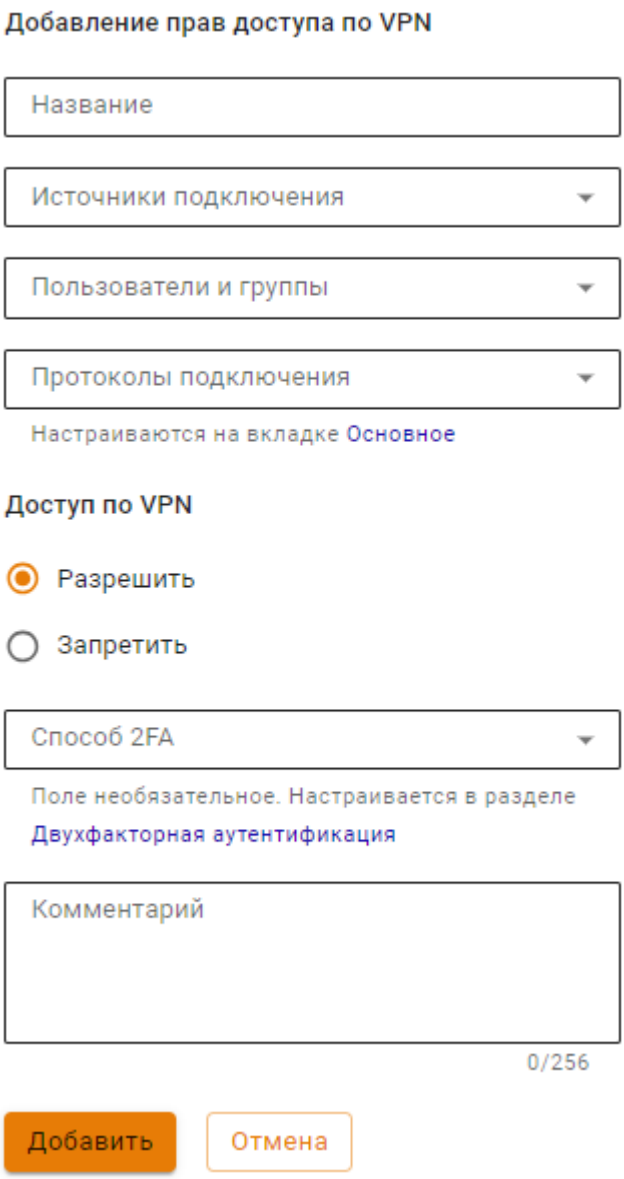
Доступ по VPN

На вкладке настраиваются правила доступа для пользователей и групп.

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

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

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



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

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

14.4.4 Правила выдачи IP-адресов

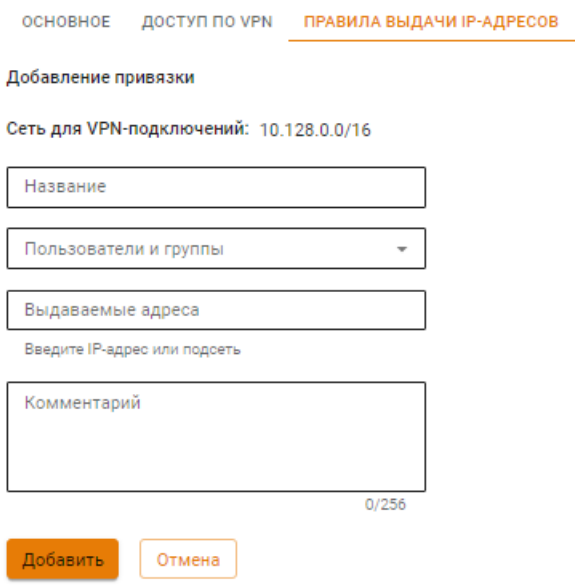
На вкладке можно создать правила для выдачи IP-адресов пользователям, подключающимся по VPN.

NGFW проверяет таблицу правил сверху вниз до первого совпадения пользователя. Если пользователь не попал под условия правил, IP-адрес назначается автоматически из пула адресов VPN, настраиваемого в разделе **Пользователи -> VPN-подключения** (например, 10.128.0.0/16). Из пула исключаются все подсети и одиночные адреса, указанные во всех правилах таблицы выдачи IP-адресов и используемые в текущих сессиях. Если адресов не осталось, соединение разрывается.

Предупреждение: Важно:

- Подсеть, указанная в правиле, должна полностью входить в сеть для VPN-подключений. В противном случае правило считается невалидным, адрес выдать невозможно, соединение разрывается.
- В двух разных правилах нельзя указать одну и ту же сеть.
- Если в разных правилах указаны пересекающиеся сети (например, сеть `10.128.1.0/24` является подсетью сети `10.128.0.0/20`), то:
  - адреса из сети `10.128.1.0/24` никогда не будут выдаваться;
  - при выдаче адресов сети `10.128.0.0/20` из нее будут исключаться адреса подсети `10.128.1.0/24`.
- Если указать в правилах сеть, совпадающую с сетью для VPN-подключений, то все пользователи VPN, для которых не совпадет ни одно правило таблицы, не смогут получить адрес и подключиться.
- Количество одновременных VPN-подключений от одного пользователя в том числе будет ограничиваться размером сети, указанной для него в правилах.
- Если в правиле указан один IP-адрес и он уже используется в текущей сессии, то указанный в правиле пользователь не сможет установить второе VPN-подключение - оно не сможет получить адрес;
- Если в правиле указана сеть с префиксом /30 (или маской 255.255.255.252) и более широкие сети (например, `10.128.2.0/24`), то при выдаче адреса из таких сетей адрес самой сети и широковещательный адрес (`10.128.2.0` и `10.128.2.255`) использоваться не будут.

Для создания правила перейдите на вкладку **Пользователи -> VPN-подключения -> Правила выдачи IP-адресов** и нажмите **Добавить**.



- **Название** - укажите название правила.

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

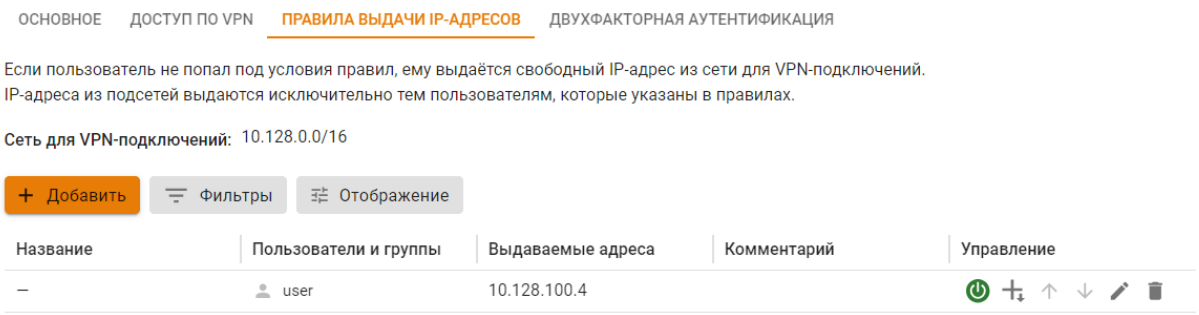
При наличии большого количества правил выдачи IP-адресов в таблице воспользуйтесь кнопкой **Фильтры**.

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

Статическая привязка IP-адресов

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

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



14.4.5 Полезные ссылки

Инструкции по настройке VPN-подключений на разных ОС доступны по *ссылке*.

14.4.6 Подключение по PPTP

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

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

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

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

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

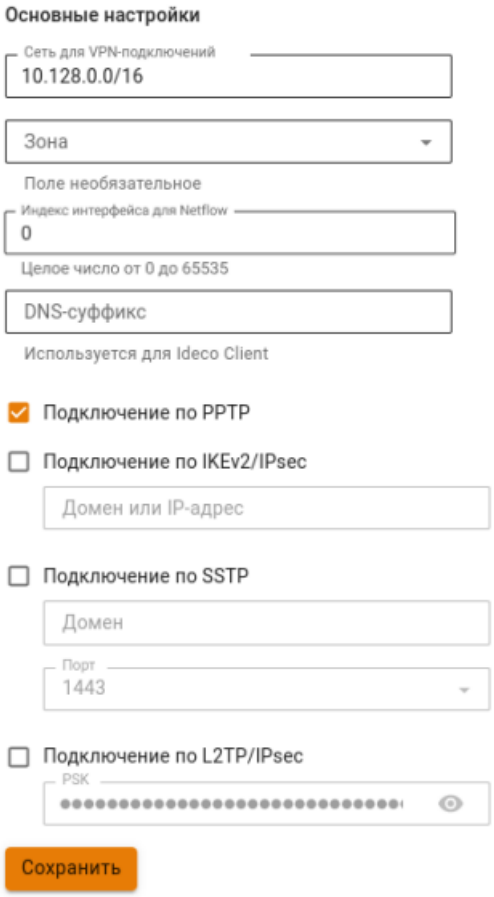
Подсказка: Не рекомендуем использовать для VPN-подключений кириллические логины.

Настройка Ideco NGFW

Основные настройки

Для настройки авторизации по протоколу PPTP выполните действия:

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



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

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

4. Нажмите **Сохранить**.

Правила выдачи IP-адресов

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

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

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

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

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

Настройка доступа по VPN

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

Возможные неполадки

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

Полезные ссылки

- В случае, если установлено VPN-соединение, но не удается получить доступ к ресурсам локальной сети, рекомендуется обратиться к статье *Особенности маршрутизации и организации доступа*;
- Инструкции по настройке VPN-подключений на разных ОС доступны по *ссылке*.

14.4.7 Подключение по IKEv2/IPsec

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

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

Протокол использует корневой сертификат для проверки подлинности участников соединения. Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство пользователя не требуется.

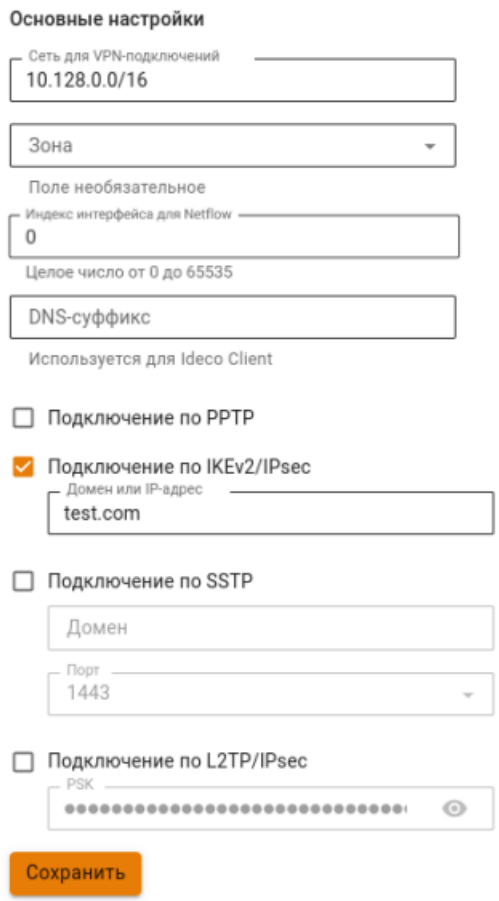
Для аутентификации применяется связка логин и пароль пользователя Ideco NGFW или пользователя из Active Directory.

Настройка Ideco NGFW

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

Основные настройки

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



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

3. В соответствующем поле укажите доменное имя или IP-адрес и нажмите **Сохранить**.

Важно: в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** загрузите сертификат с указанием полного доменного имени в расширении SAN.

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

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

Настройка доступа по VPN

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

Поддержка IKEv2/IPsec в клиентских ОС

- Microsoft **Windows 10** и выше. Требует установки корневого сертификата Let's Encrypt. *Инструкция по настройке*;
- Apple **MacOS X 10.11** «El Capitan» (2015 г.) и выше. *Инструкции по настройке*;
- Linux NetworkManager plugin (с 2008 г.). Инструкция по настройке *Alt Linux*, *Ubuntu*, *Astra Linux* и *Fedora*;
- Google **Android 11** (2020 г.) и выше. На более ранних версиях можно использовать приложение StrongSwan. *Инструкция по настройке*;
- Apple **iOS 9** (iPhone 4S, 2015 г.) и выше. *Инструкция по настройке*;
- **KeeneticOS 3.5** и выше. *Инструкция по настройке*;
- MikroTik;
- Cisco routers.

14.4.8 Подключение по SSTP

Внимание: По возможности не используйте этот тип подключения. Этот способ подключения лучше других проходит через NAT, но при нестабильном качестве связи работает значительно хуже, чем другие VPN (особенно при передаче звука/видео), так как инкапсулирует все данные внутри TCP. Рекомендуется использовать *IKEv2/IPsec*.

SSTP - протокол туннелирования трафика, который обеспечивает безопасное соединение между клиентом и сервером через интернет.

Протокол использует корневой сертификат для проверки подлинности участников соединения. Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство пользователя не требуется.

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

Особенности работы:

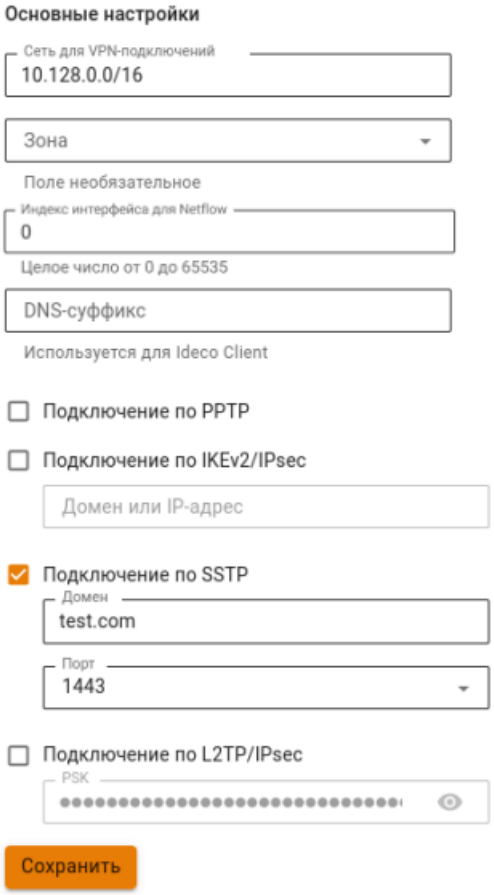
- Запрещено использовать домен `.local`. Подключение по SSTP поддерживается только из внешних сетей;
- Не рекомендуется использовать логины на кириллице для VPN-подключений. Это может привести к проблемам с подключением;

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

Настройка Ideco NGFW

Основные настройки

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



2. Включите опцию **Подключение SSTP**.

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

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

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

Настройка доступа по VPN

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

Полезные ссылки

- В случае, если установлено VPN-соединение, но не удается получить доступ к ресурсам локальной сети, рекомендуется обратиться к статье *Особенности маршрутизации и организации доступа*;
- Инструкции по настройке VPN-подключений на разных ОС доступны по *ссылке*.

14.4.9 Подключение по L2TP/IPsec

Внимание: По возможности не используйте этот тип подключения. Он может работать нестабильно, обладает огромной избыточностью, низкой производительностью и поддерживает не самое сильное шифрование. Вместо этого рекомендуется *IKEv2/IPsec*. Все современные ОС поддерживают IKEv2, либо для них есть приложения.

L2TP/IPsec — протокол позволяет создавать защищенные VPN-соединения между устройствами, обеспечивая конфиденциальность и целостность передаваемых данных.

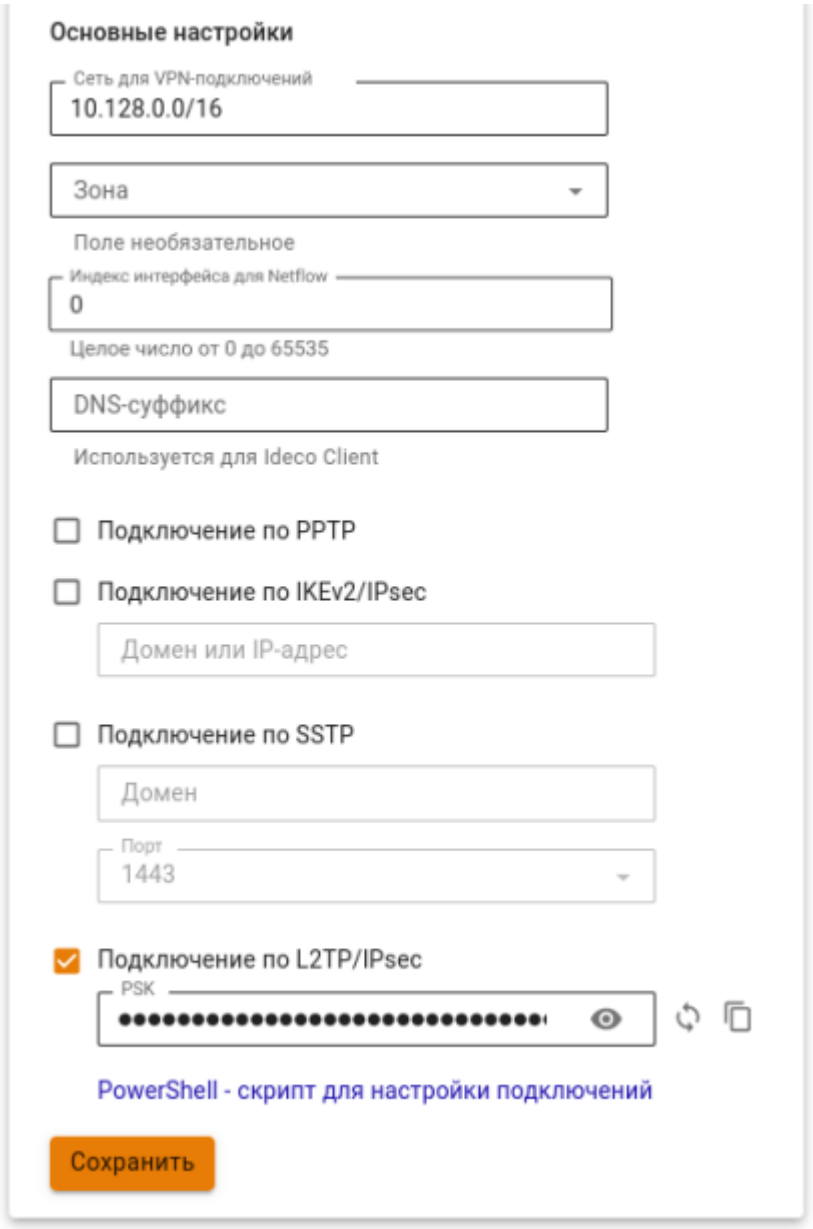
Для аутентификации используется связка логин/пароль пользователя Ideco NGFW или пользователя из Active Directory, а также PSK-ключ, который был указан при настройке соединения.

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

Настройка Ideco NGFW

Основные настройки

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



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

3. Укажите секретную фразу (PSK-ключ).

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

5. Нажмите **Сохранить**.

Настройка доступа по VPN

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

Полезные ссылки

- L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их больше одного. Решить проблему может помочь инструкция;
- В случае, если установлено VPN-соединение, но не удается получить доступ к ресурсам локальной сети, рекомендуется обратиться к статье *Особенности маршрутизации и организации доступа*;
- Инструкции по настройке VPN-подключений на разных ОС доступны по *ссылке*.

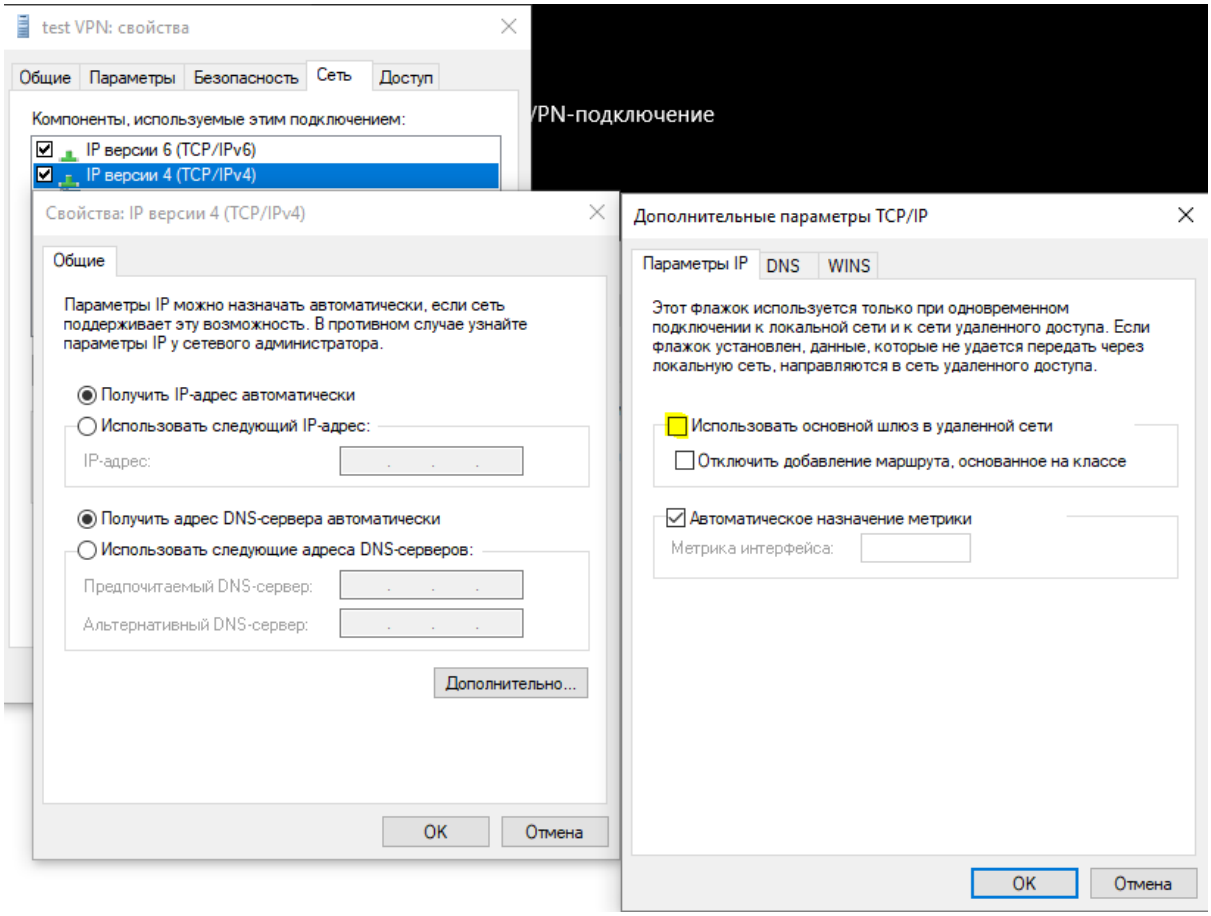
14.4.10 Особенности маршрутизации и организации доступа

В статье рассматриваются потенциальные проблемы, связанные с доступом к ресурсам локальной сети через VPN, и предлагаются решения, такие как настройка маршрутов, исключение определенных сетей в антивирусном ПО и создание правил SNAT на NGFW.

Организация доступа по VPN только к ресурсам локальной сети

Для организации доступа выполните действия:

1. На вкладке **Сеть -> IP версии 4 -> Дополнительно -> Параметры IP** уберите флаг **Использовать основной шлюз в удаленной сети**:



Особенности VPN-соединения с доступом только к ресурсам локальной сети:

При выборе типа передачи маршрутов **Отправлять только указанные сети** маршрут до VPN-сервера и DNS-сервера построен не будет.

Если в NGFW добавить передачу IP-адреса VPN-сервера NGFW (DNS), то маршрут восстановится, а домен будет преобразовываться со следующими особенностями:

- Таблица с включенным шлюзом:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255        On-link        10.200.0.5      5
        127.0.0.0        255.0.0.0        On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255        On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255        On-link         127.0.0.1    331
    192.168.100.2  255.255.255.255        On-link        10.200.0.5      5
  192.168.100.130  255.255.255.255        On-link        10.200.0.5      5
    192.168.122.0    255.255.255.0        On-link    192.168.122.10    281
   192.168.122.10  255.255.255.255        On-link    192.168.122.10    281
  192.168.122.255  255.255.255.255        On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0        On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0        On-link    192.168.122.10    281
  255.255.255.255  255.255.255.255        On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255        On-link    192.168.122.10    281
===========================================================================
```

- Таблица с отключенным шлюзом:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
        127.0.0.0        255.0.0.0        On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255        On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255        On-link         127.0.0.1    331
    192.168.100.2  255.255.255.255        On-link        10.200.0.5      5
  192.168.100.130  255.255.255.255        On-link        10.200.0.5      5
    192.168.122.0    255.255.255.0        On-link    192.168.122.10    281
   192.168.122.10  255.255.255.255        On-link    192.168.122.10    281
  192.168.122.255  255.255.255.255        On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0        On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0        On-link    192.168.122.10    281
  255.255.255.255  255.255.255.255        On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255        On-link    192.168.122.10    281
===========================================================================
```

- Таблица с отключенным шлюзом и добавленной публикацией IP NGFW:

```
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.122.1   192.168.122.10     25
       10.200.0.1  255.255.255.255         On-link        10.200.0.4     26
       10.200.0.4  255.255.255.255         On-link        10.200.0.4    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.100.2  255.255.255.255         On-link        10.200.0.4     26
  192.168.100.130  255.255.255.255         On-link        10.200.0.4     26
    192.168.122.0    255.255.255.0         On-link    192.168.122.10    281
   192.168.122.10  255.255.255.255         On-link    192.168.122.10    281
  192.168.122.210  255.255.255.255         On-link    192.168.122.10     26
  192.168.122.255  255.255.255.255         On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.122.10    281
        224.0.0.0        240.0.0.0         On-link        10.200.0.4    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.122.10    281
  255.255.255.255  255.255.255.255         On-link        10.200.0.4    281
===========================================================================
```

Маршрут до сервера (в примере - 10.200.0.1) добавляется, но имеет более низкий приоритет, чем маршрут по-умолчанию. Соответственно запросы обрабатываются с задержкой и не обрабатываются при перехвате маршрутом по-умолчанию.

Рекомендуем вручную указать маршрут до DNS NGFW либо добавить его в список публикуемых маршрутов на стороне NGFW. Также можно использовать сторонний DNS-сервер.

2. Пропишите маршрут до корпоративной сети. В Windows 8, 8.1, 10 автоматически создается маршрут на основе класса, в зависимости от адреса, полученного по VPN. Для IPsec-IKEv2 можно настроить автоматическое получение маршрута.

Пример маршрута: если корпоративная сеть имеет адрес `172.16.0.0/16`, а сеть для VPN-подключений, настроенная на Ideco NGFW, имеет адрес `10.128.0.0/16`:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1
```

Маршрут может не работать, когда есть пинг до интерфейса `10.128.0.1`, но нет пинга до хостов в локальной сети. В этом случае при создании маршрута нужно указать номер интерфейса VPN-подключения:

```
route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn
```

- `nn` - номер интерфейса VPN-подключения, посмотреть который можно при активном VPN-подключении в выводе в консоли команды `route print` раздел «Список интерфейсов».

Не удается получить доступ к компьютерам в локальной сети Ideco NGFW

Для получения доступа к компьютерам в локальной сети Ideco NGFW убедитесь, что:

1. Локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. В противном случае доступ к сети организации будет невозможен (трафик будет идти через физический интерфейс, а не через VPN);

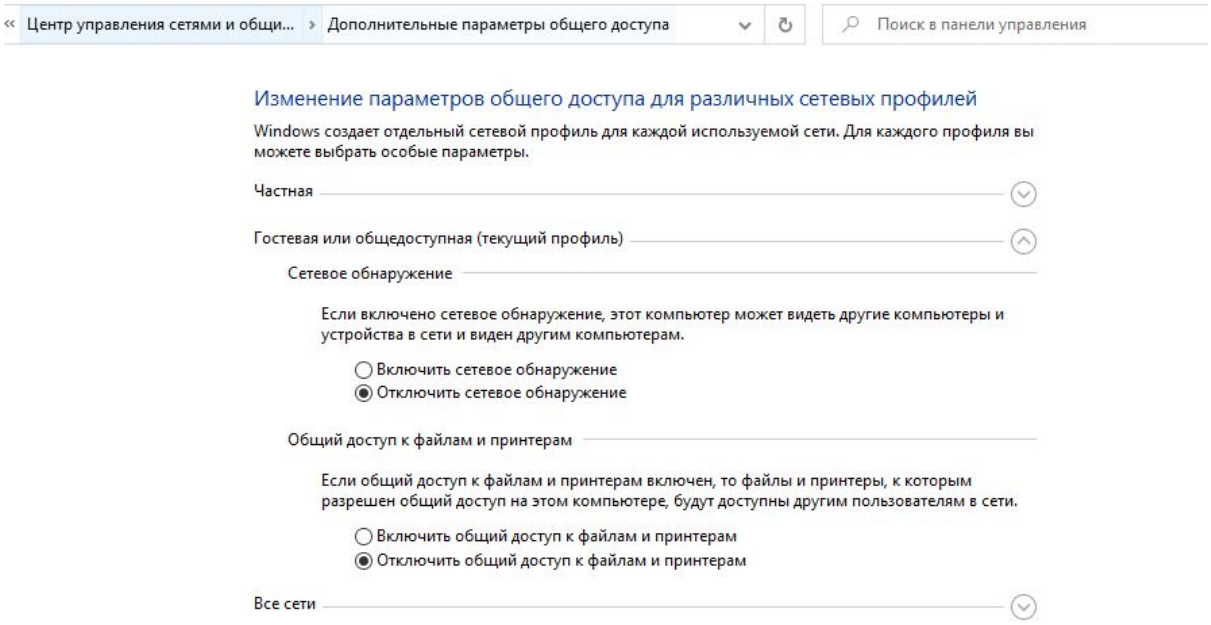
2. На компьютерах локальной сети основным шлюзом должен быть Ideco NGFW. Если это не так, то вручную необходимо прописать соответствующий маршрут, чтобы сетевые пакеты шли на Ideco NGFW для VPN-сети. **Например**:

```
route -p add 10.128.0.0 mask 255.255.0.0 10.1.1.1
```

- `10.128.0.0/16` - адрес VPN-сети Ideco NGFW (настраивается в разделе **Пользователи -> VPN-подключения**);
- `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW.

3. На Ideco NGFW в разделе **Файрвол -> FORWARD** нет запрещающих правил;

4. Компьютеры и серверы на Windows не ограничивают доступ к сетевым папкам с помощью правил настроек профилей сети (как на стороне подключающегося по VPN компьютера, так и на стороне компьютеров и серверов локальной сети):



Получение доступа к файлам и принтерам для профиля «Все сети» и «Частные сети»

Для получения доступа выполните действия:

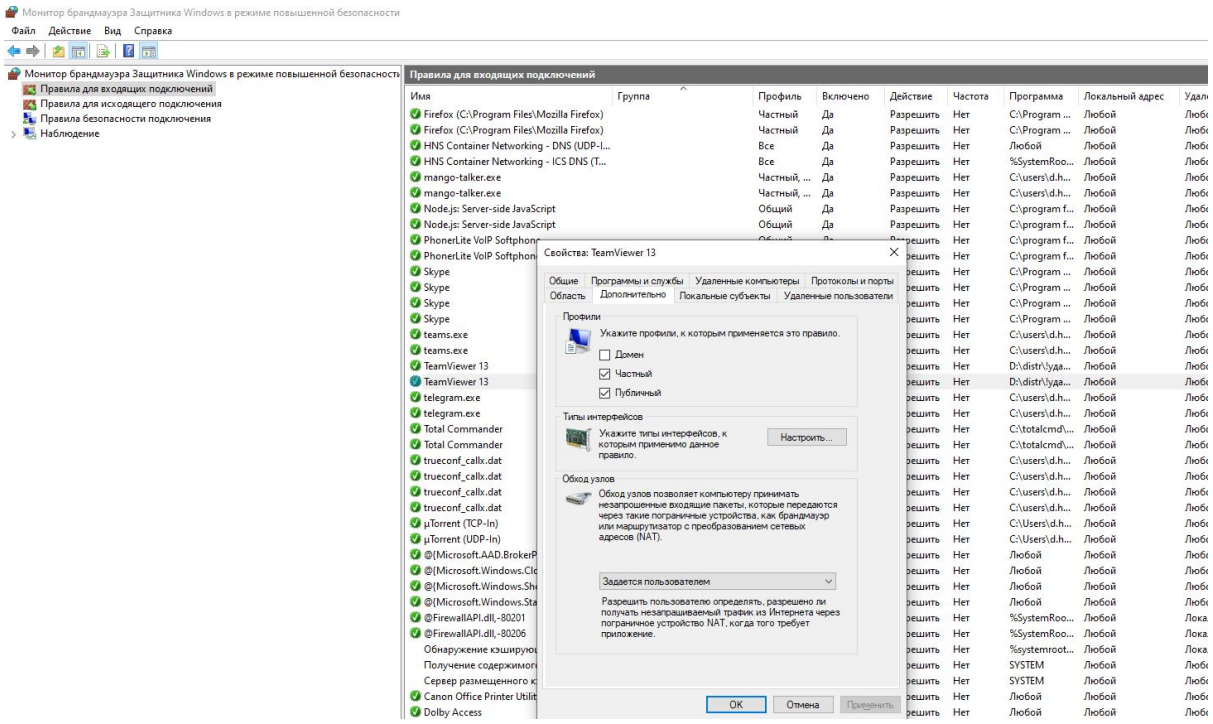
1. Перейдите в PowerShell (запустите его с повышением прав до администратора).

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

Возможные проблемы:

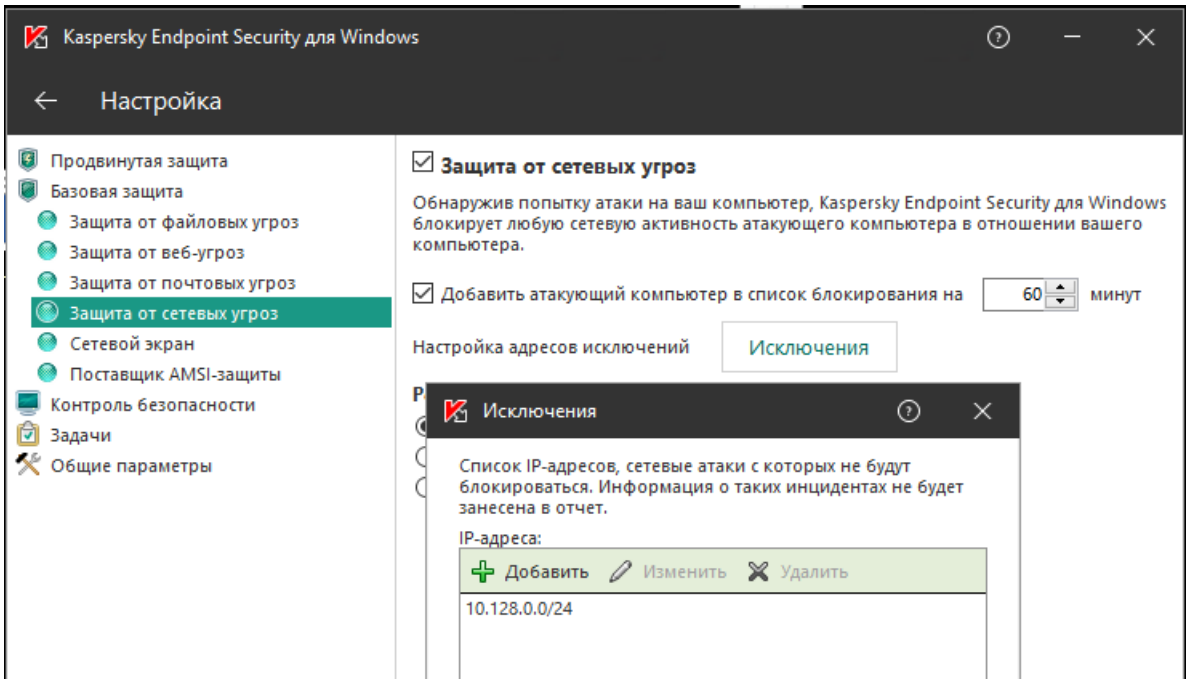
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей.

  Проверьте это в настройках входящих и исходящих подключений (необходимо разрешить доступ из частных и локальных сетей):



- Антивирусное ПО на компьютере может блокировать доступ из нелокальных сетей. Либо блокировать доступ конкретных программ.

  Например, для **Kaspersky Endpoint Security** нужно добавить сеть для VPN-подключений (по умолчанию `10.128.0.0/16`) в исключения:



Получение доступа к локальной сети Филиала

Чтобы обеспечить доступ, убедитесь, что VPN-сети обоих NGFW не пересекаются. Затем проверьте настройки основного NGFW, следуя инструкциям, описанным в *статье*.

Получение доступа до хостов локальной сети, если за NGFW есть маршрутизатор, выступающий в качестве ядра локальной сети

Чтобы обеспечить доступ, нужно настроить на роутере маршрут от нужной локальной сети до VPN-сети. Для настройки маршрута на роутере укажите в качестве назначения VPN-сеть (`10.128.0.0/16`), в качестве шлюза - NGFW (`172.16.0.1`).

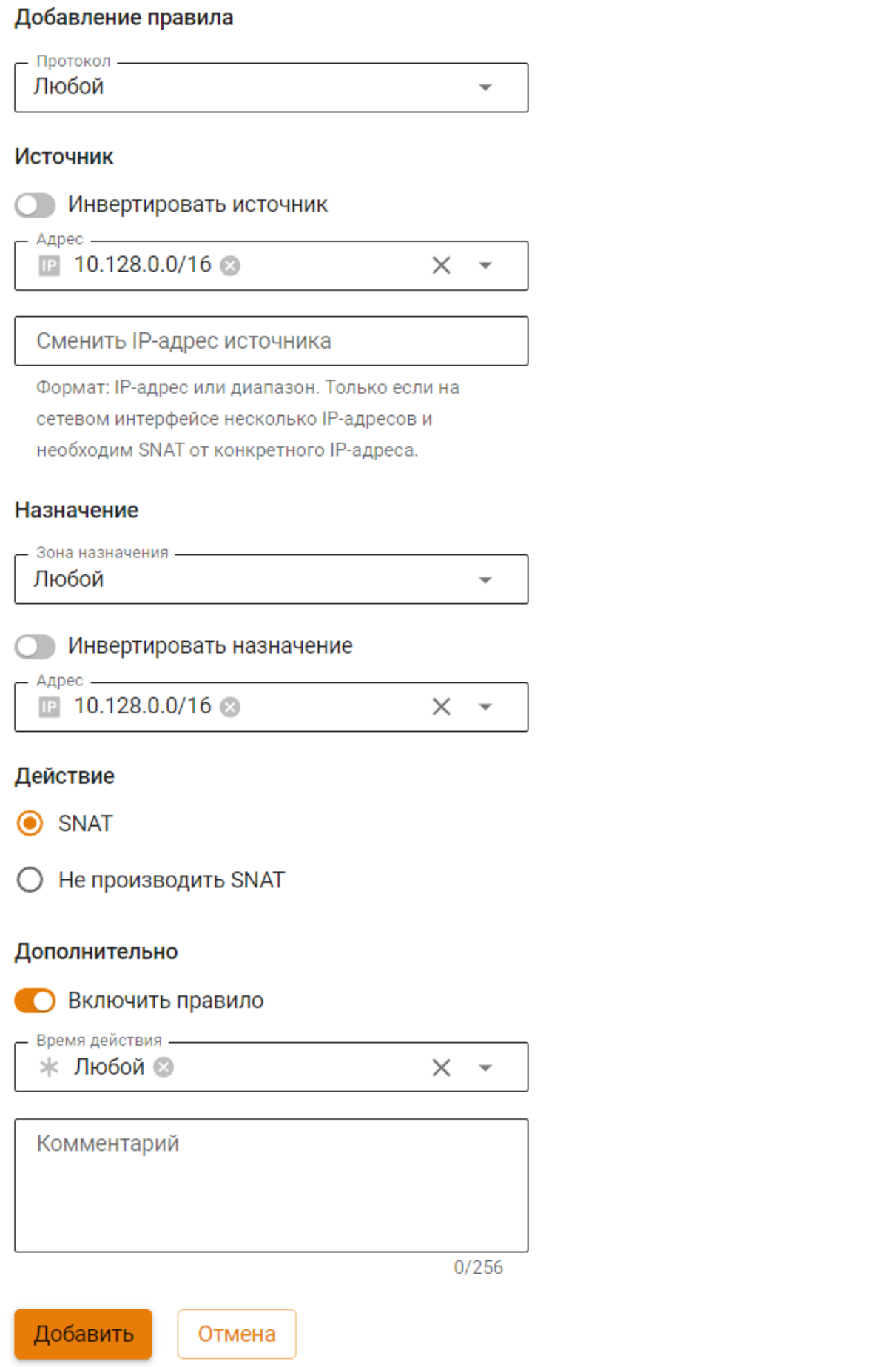
Если настроить на роутере маршрут невозможно, можно создать на NGFW SNAT-правило:

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

2. Укажите следующие параметры:

   - Источник - VPN-сеть (`10.128.0.0/16`);
   - Назначение - сеть за роутером, к которой требуется получить доступ из VPN-сети (`192.168.0.0/24`).

3. Нажмите **Добавить**.


Добавление правила
Протокол
Любой
Источник
Инвертировать источник
Адрес
10.128.0.0/16
Сменить IP-адрес источника
Формат: IP-адрес или диапазон. Только если на сетевом интерфейсе несколько IP-адресов и необходим SNAT от конкретного IP-адреса.
Назначение
Зона назначения
Любой
Инвертировать назначение
Адрес
10.128.0.0/16
Действие
SNAT
Не производить SNAT
Дополнительно
Включить правило
Время действия
Любой
Комментарий
0/256
Добавить
Отмена

В этом случае при отправке пакетов на роутер NGFW подменит IP-адрес источника своим. За счет этого роутер направит ответ от хоста в локальной сети на NGFW, который затем перенаправит его в VPN-сеть.

У хостов из локальной сети `192.168.0.0/24` не будет доступа к VPN-сети `10.128.0.0/16`.

14.4.11 Инструкция по запуску PowerShell скриптов

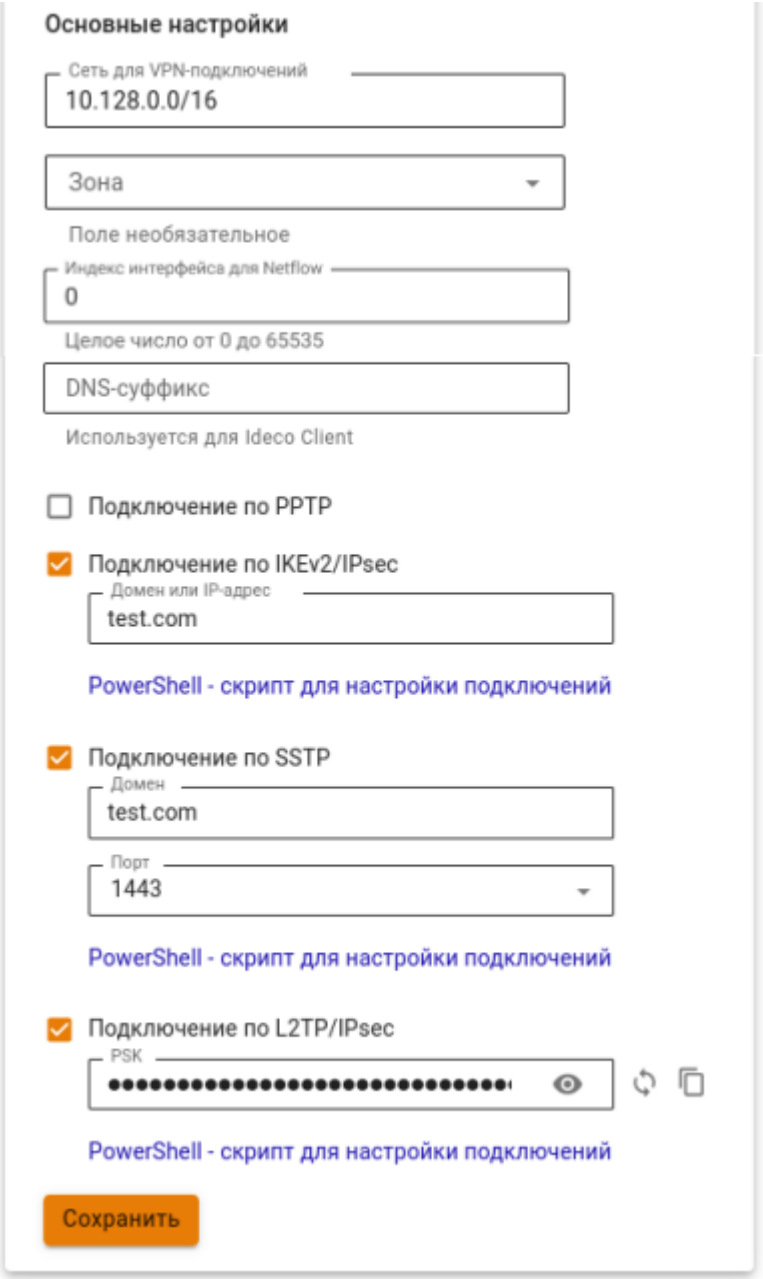
Для подключения по VPN к Ideco NGFW с белым IP адресом достаточно действий, указанных ниже. Если Ideco NGFW выходит в интернет через маршрутизатор, воспользуйтесь пунктом *Подключение по VPN к Ideco NGFW с доступом в интернет через маршрутизатор*.

Запуск PowerShell-скрипта

1. Скачайте скрипт одним из способов:

Из Ideco NGFW:

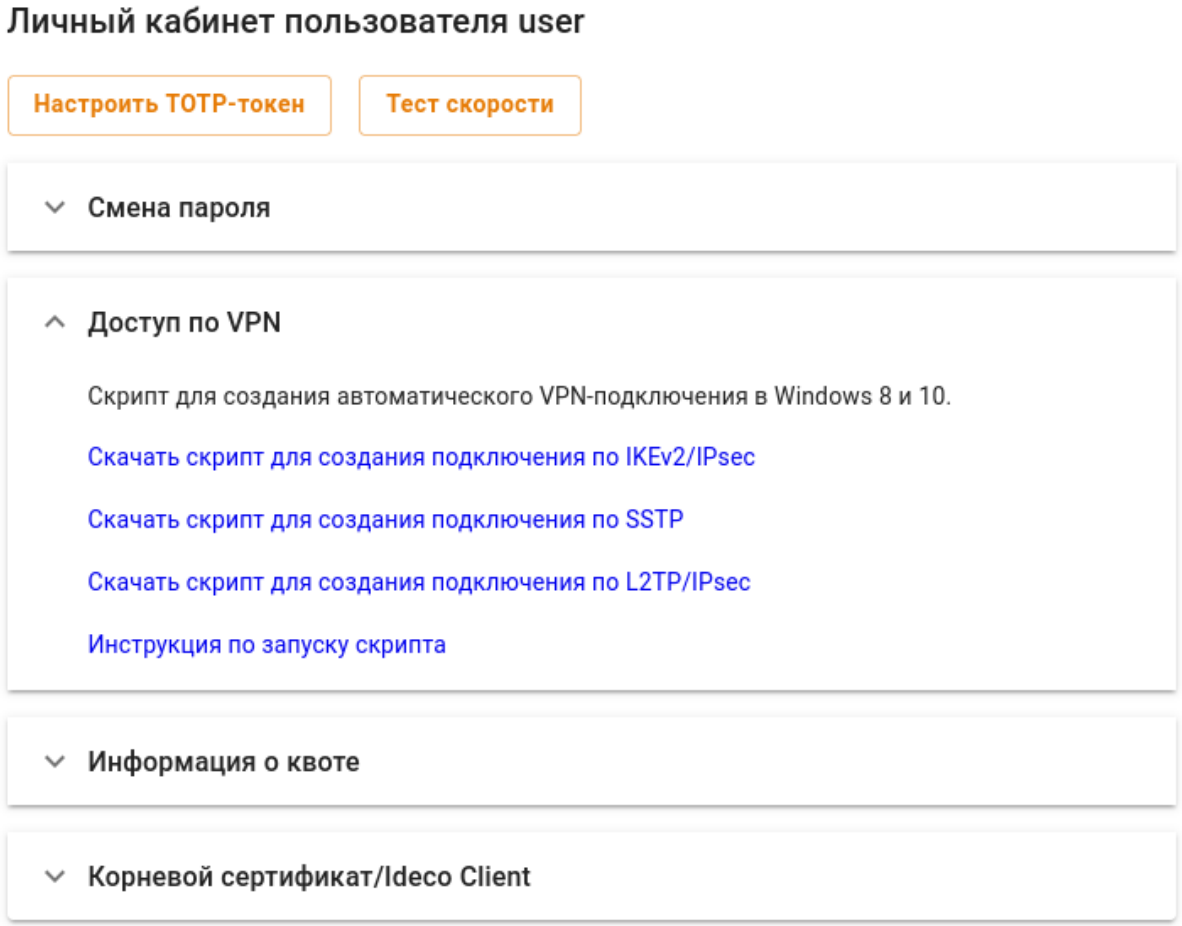
- Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**:



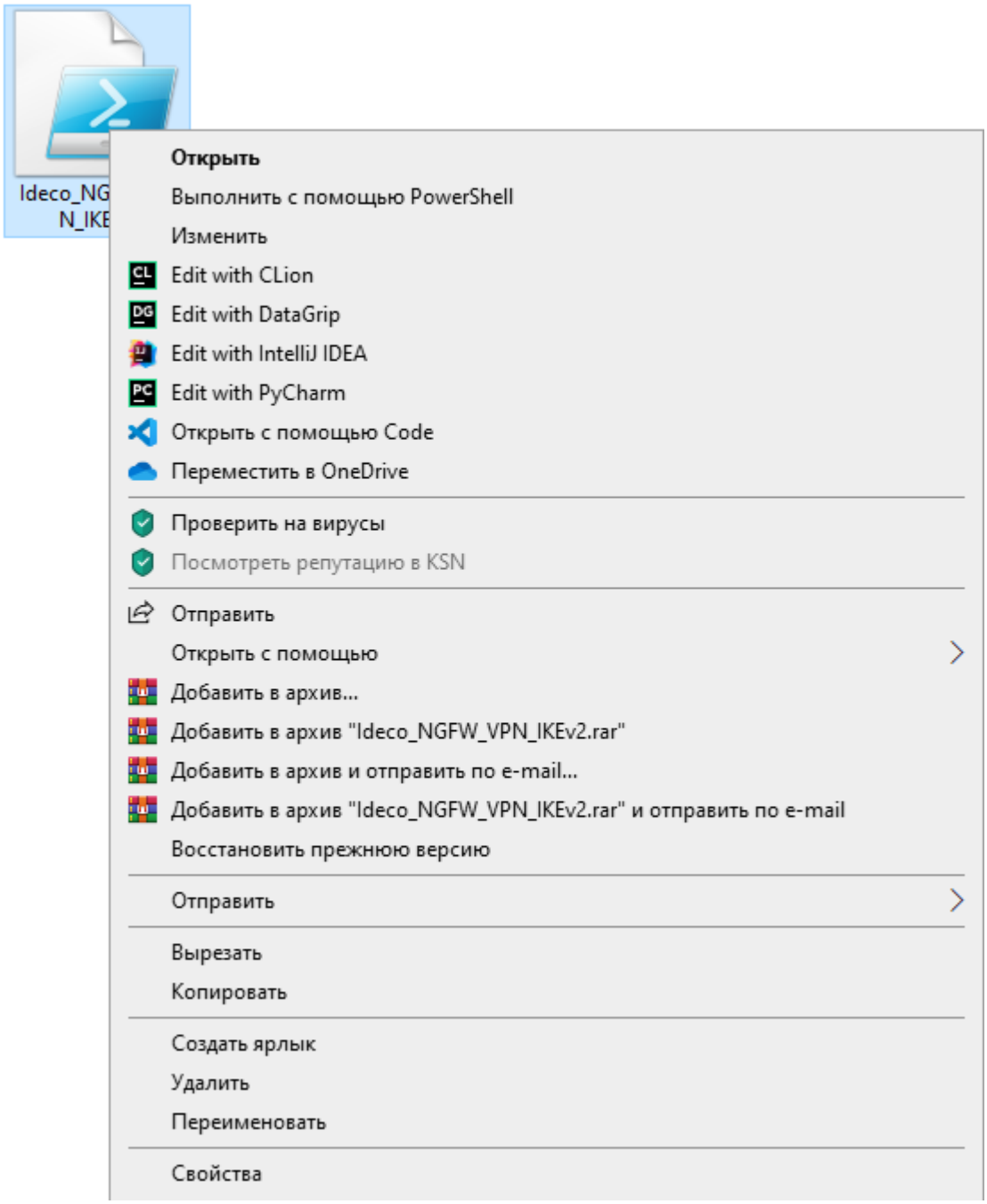
- Включите и настройте требуемый протокол подключения;
- Перейдите по ссылке **PowerShell - скрипт для настройки подключений**;
- Перенесите скачанный файл на устройство, на котором требуется создать VPN-подключение.

В личном кабинете пользователя:

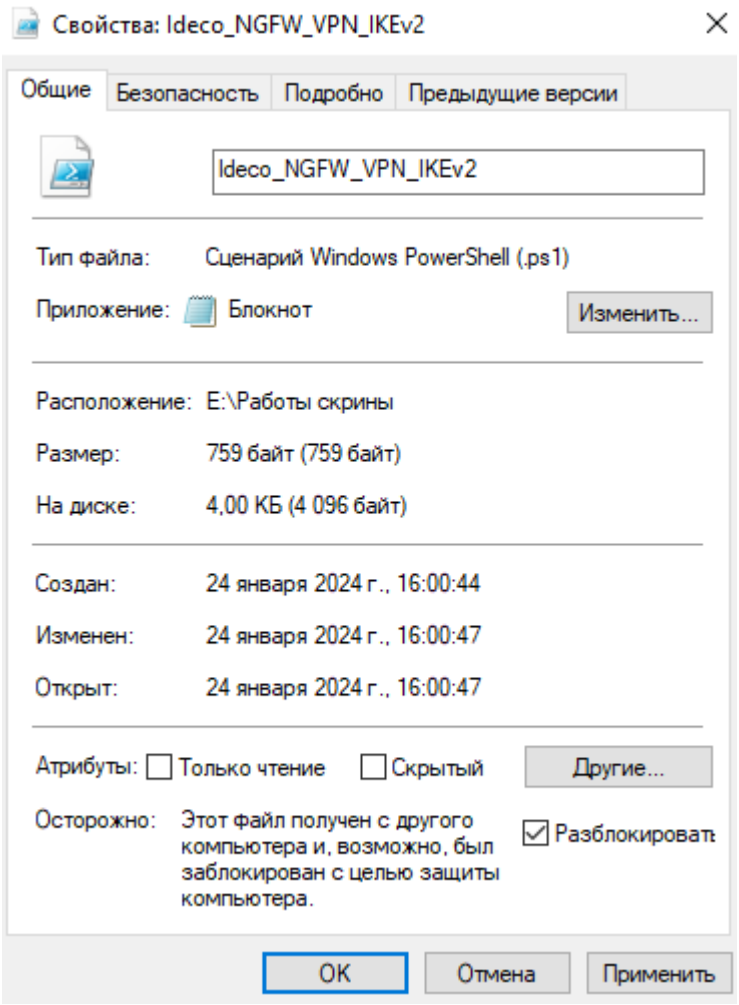
- Скачайте скрипт, перейдя по ссылке **Скачать скрипт для создания подключения**:



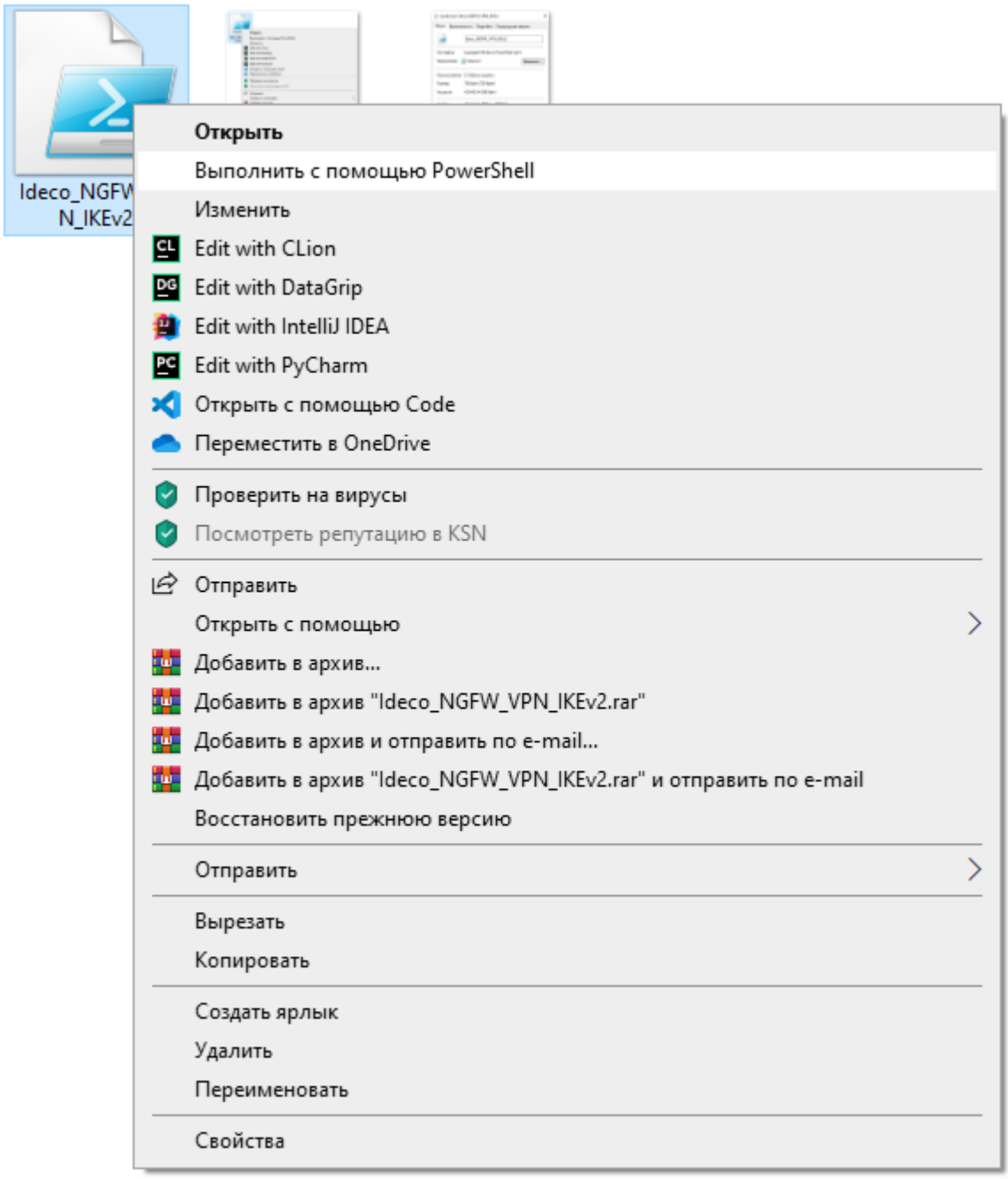
2. Щелкните правой кнопкой мыши по скачанному файлу и в контекстном меню выберите **Свойства**.



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

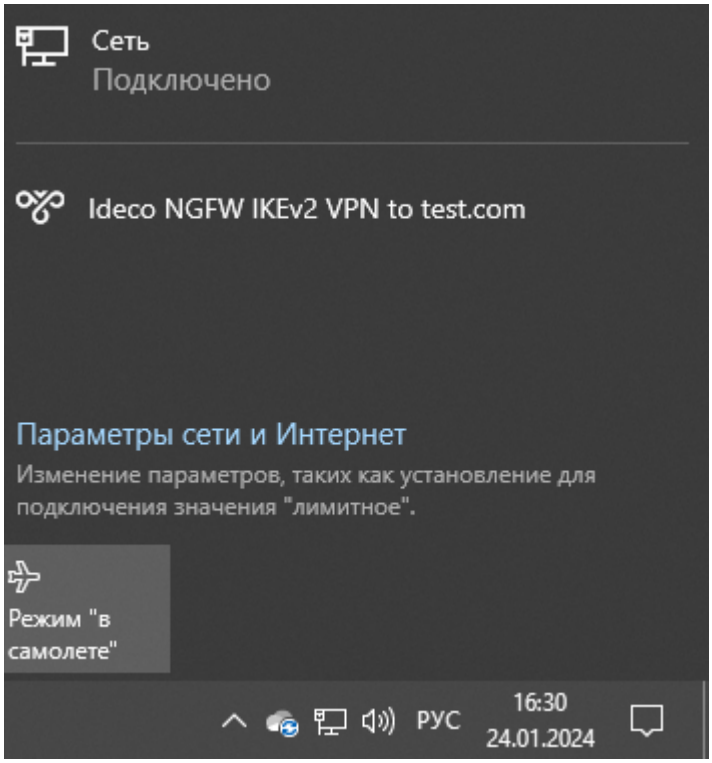


4. Нажмите правой кнопкой мыши на файл и выберите пункт **Выполнить в PowerShell**. Затем подтвердите действие, нажав **Да** на вопрос о внесении изменений в компьютер:



Подсказка: При появлении ошибки **Выполнение сценариев отключено в этой системе** откройте PowerShell с правами администратора, выполните команду для разрешения запуска скриптов `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`, в том же окне заново выполните скрипт для создания подключения и закройте консоль.

5. Когда одключение создано, нажмите **Подключиться** в списке сетей.



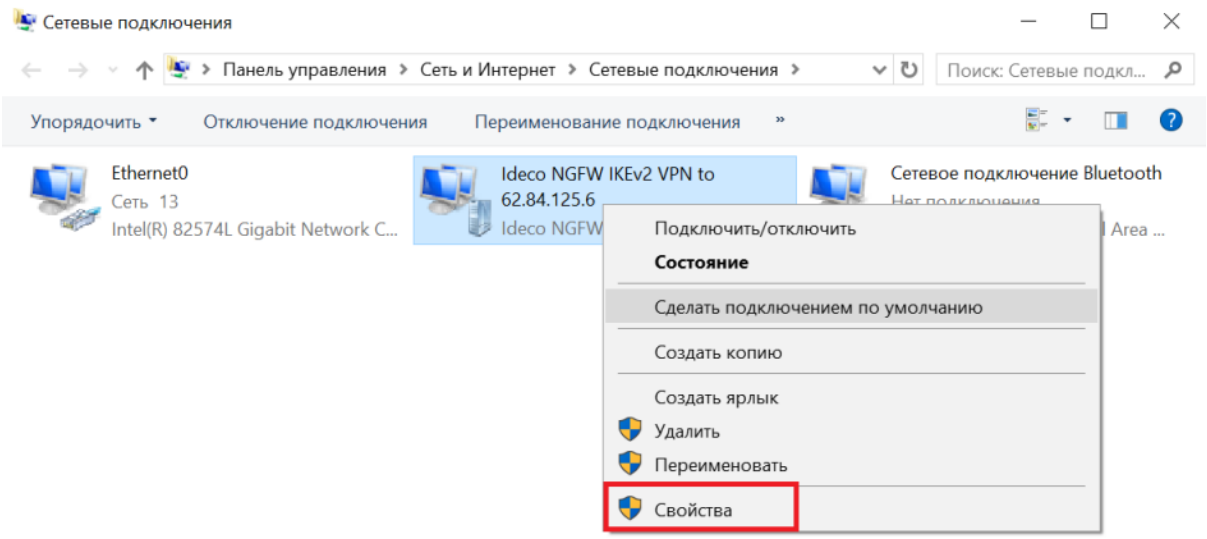
DNS-суффиксы для VPN-подключений

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

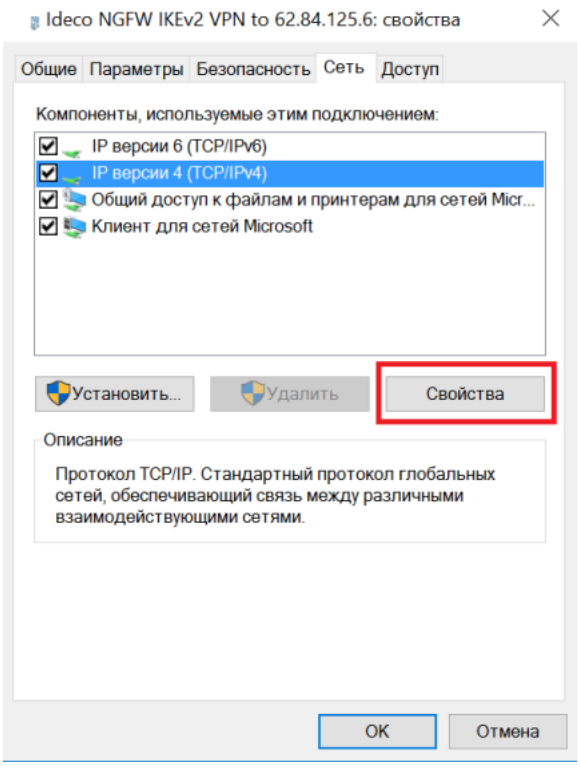
Предупреждение: Если Ideco NGFW введен в несколько доменов, то DNS-суффиксы в PowerShell-скриптах не прописываются, их необходимо настраивать вручную на подключенном по VPN устройстве.

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

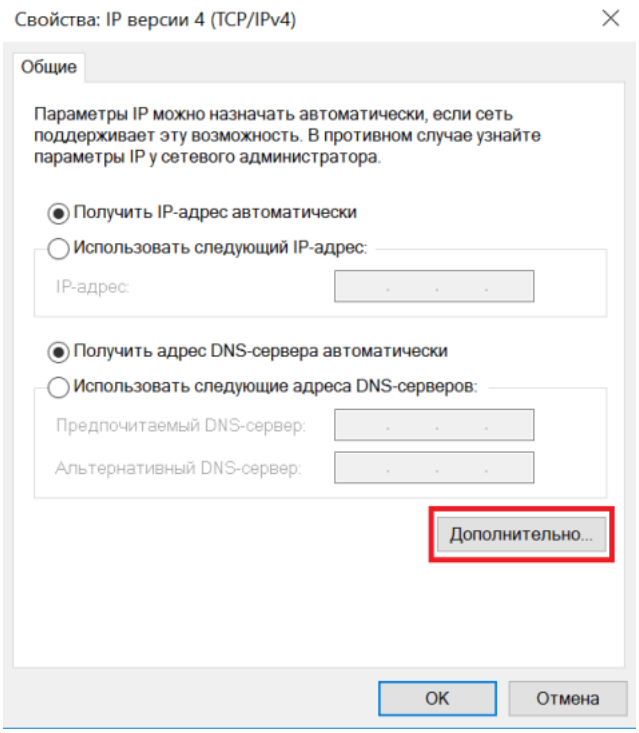
1. Перейдите в **Сетевые подключения**, нажмите правой кнопкой мыши по нужному VPN-подключению и выберите **Свойства**:



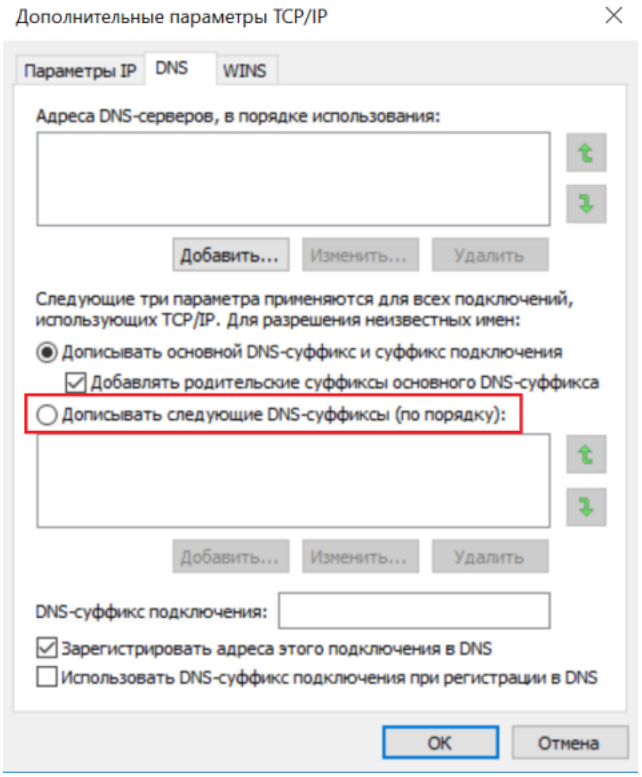
2. В открывшемся окне перейдите на вкладку **Сеть**, выберите компонент **IP версии 4 (TCP/IPv4)** и нажмите **Свойства**:



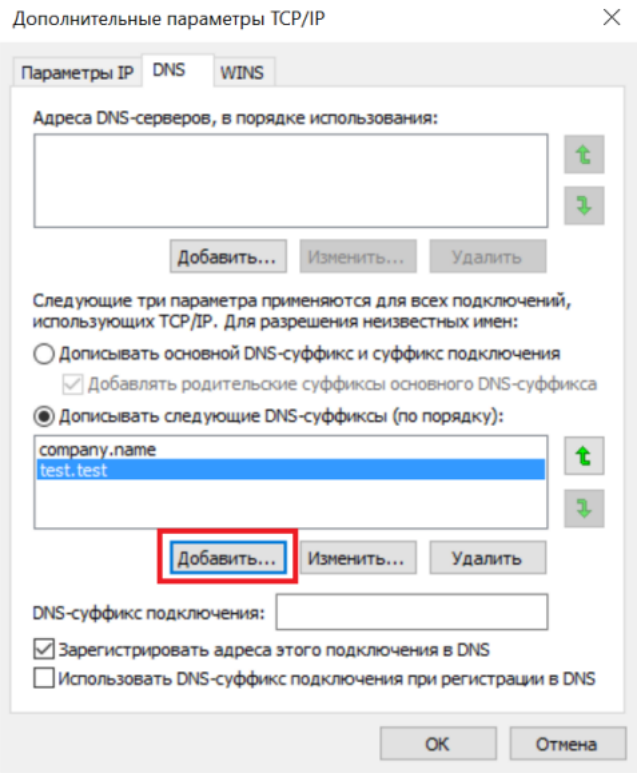
3. В открывшемся окне нажмите **Дополнительно**:



4. Перейдите на вкладку **DNS** и включите опцию **Дописывать следующие DNS-суффиксы (по порядку)**:



5. Нажмите **Добавить** и введите необходимые DNS-суффиксы:



Подсказка: При обращении к компьютеру по короткому имени DNS-суффиксы будут перебираться в порядке расположения. Этот порядок можно менять стрелками.

Подключение по VPN к Ideco NGFW с доступом в интернет через маршрутизатор:

Для работы скрипта подключения по VPN выполните действия:

1. Сделайте проброс портов 4500 и 500 в IP-адрес Ideco NGFW в локальной сети маршрутизатора.

2. Загрузите скрипт на компьютер, воспользовавшись 1 пунктом инструкции *Запуск PowerShell-скрипта*.

3. Поменяйте в загруженном скрипте IP-адрес Ideco NGFW на внешний IP-адрес маршрутизатора:

В строках:

- `Name "Ideco NGFW L2TP VPN to 46.36.23.99"` замените на `Name "Ideco NGFW L2TP VPN to 5.189.21.1"`;
- `ServerAddress 46.36.23.99` замените на `ServerAddress 5.189.21.1`.
- **46.36.23.99** - IP-адрес Ideco NGFW в локальной сети маршрутизатора;
- **5.189.21.1** - внешний IP-адрес маршрутизатора.

4. После выполнения действий следуйте инструкции *Запуск PowerShell-скрипта* с 4 пункта.

Решение проблем запуска PowerShell-скрипта:

Для запуска Powershell-скрипта убедитесь, что:

- Вам хватает прав на запуск скрипта;
- PowerShell установлен в системе.

Подсказка: Если не удалось решить проблему запуска PowerShell-скрипта, воспользуйтесь инструкцией для создания подключения в *Windows 10* вручную.

14.5 Ideco Client

Подсказка: Название службы раздела **Ideco Client**: `ideco-agent-backend`; `ideco-agent-websocket`. Список служб для других разделов доступен по *ссылке*.

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

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

14.5.1 Возможности Ideco Client

- Авторизация в локальной сети;
- VPN-подключение из внешних сетей;
- VPN-подключение из локальных сетей;
- Двухфакторная аутентификация;
- Режим работы *Device VPN*;
- Сбор данных о подключающихся устройствах.

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

HIP-профили помогают реализовать ZTNA (Zero Trust Network Access) - технологию, которая обеспечивает безопасный доступ к сети на основе принципа *нулевого доверия*. ZTNA контролирует и аутентифицирует устройства пользователей перед предоставлением доступа к ресурсам сети.

14.5.2 Поддерживаемые версии ОС и порты подключения

Поддерживаемые версии ОС	- Windows с 10 версии и выше;- MacOS версии 12.7 и выше. При этом Ideco Client работает с *некоторыми ограничениями*;- Astra Linux 1.7.0 и выше;- РЕД ОС 8.0 и выше;- Alt OS (Alt Workstation) 9.0 и выше;- Fedora 35 и выше;- Ubuntu 18.04 LTS (23.04) и выше.**Важно**: Ideco Client не работает на ОС Windows 11 версии 24H2. Варианты решения *описаны ниже*.
Порты для подключения, если NGFW за NAT	- 80 TCP - для работы сертификатов Let's Encrypt;- 14765 TCP и 3051 UDP - для работы Ideco Client.

Варианты решения проблем на ОС Windows 11 версии 24H2:

- Включить компонент **Virtual Machine Platform**:

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

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

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

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

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

- Вернуть предыдущую версию операционной системы Windows 11 23H2;
- Использовать альтернативный способ *VPN-подключения*.

14.5.3 Настройки в Ideco NGFW

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

Для подключения пользователей локальных сетей по VPN активируйте настройку **Создавать туннель при подключении из локальной сети** в разделе **Ideco Client**. Изменение этой настройки разрывает текущие сессии из локальных сетей. Повторное подключение будет соответствовать новому значению настройки.

Настройка двухфакторной аутентификации в Ideco Client:

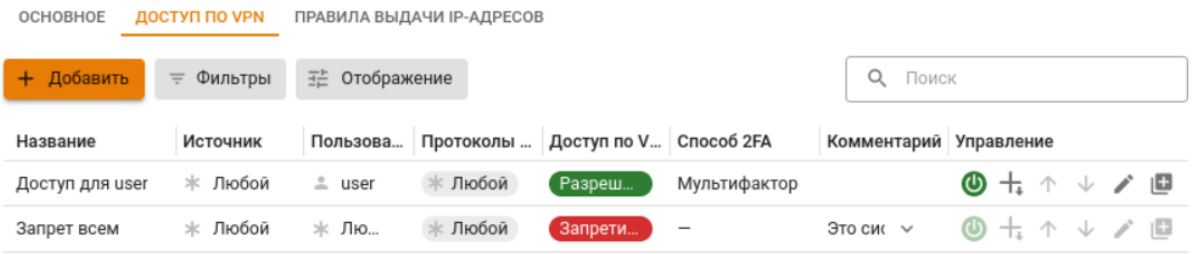
Выполните действия:

- В веб-интерфейсе Ideco NGFW:

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

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

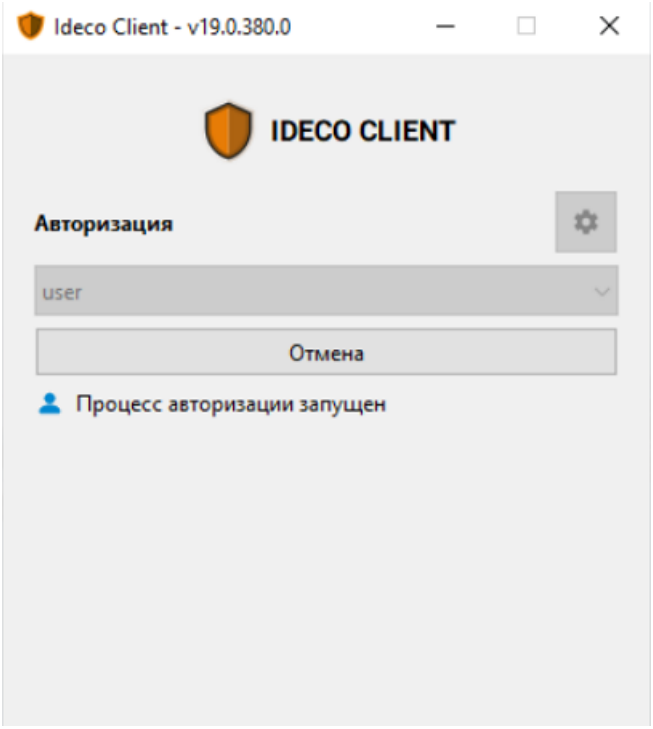
3. Добавьте правило в разделе **Пользователи -> VPN-подключения -> Доступ по VPN**. В настройках правила укажите созданную учетную запись пользователя и тип двухфакторной аутентификации, выбранный в шаге 2. В поле **Протоколы** укажите значение **Любой**:



- На устройстве пользователя:

1. Установите и запустите приложение Ideco Client. Инструкции по установке: *Windows*, *MacOS*, *Linux*.

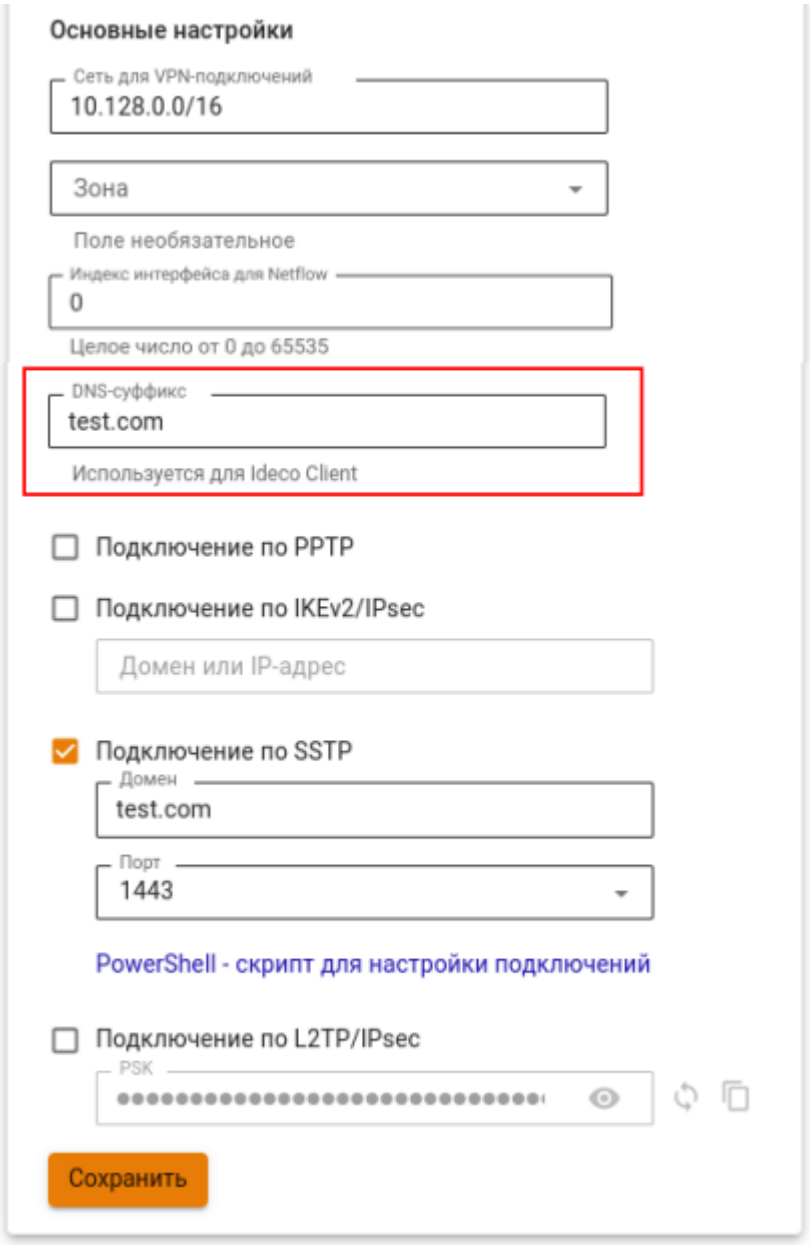
2. Авторизуйтесь через настроенную учетную запись пользователя:



3. Пройдите двухфакторную аутентификацию.

DNS-суффиксы для VPN-подключений по протоколу WireGuard

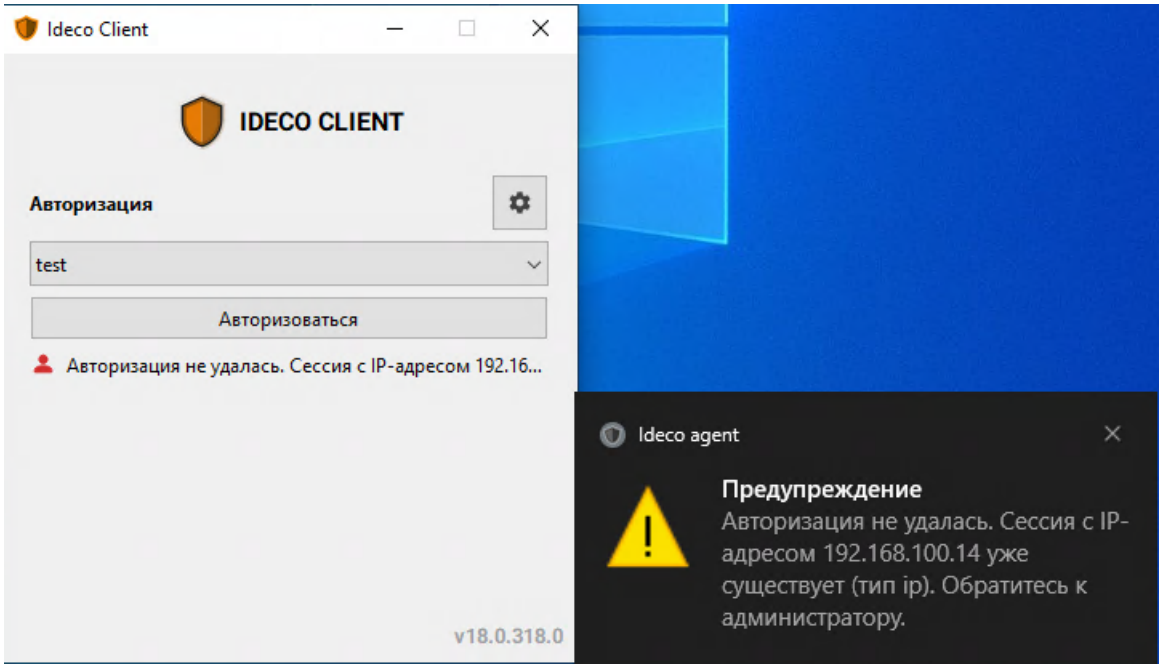
Чтобы указать DNS-суффикс для домена, в который введен Ideco NGFW, перейдите в **Пользователи -> VPN-подключения -> Основное**, заполните поле для суффикса и нажмите **Сохранить**:



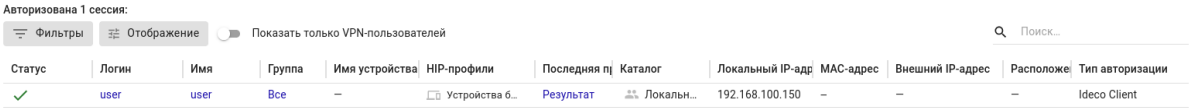
Подсказка: Ideco NGFW поддерживает только один DNS-суффикс. Не указывайте DNS-суффикс, если NGFW введен в несколько доменов.

14.5.4 Особенности работы Ideco Client

- Только один профиль может быть с опцией автоподключения. Если активировать автоподключение для другого профиля, у предыдущего эта опция отключится.
- Чтобы использовать SSO-профиль с автоподключением, вручную укажите доменное имя в поле **Хост**. Для предварительной настройки адреса подключения используйте групповую политику или запустите файл через командную строку с ключом: `IdecoAgent.msi utm_address=адрес_ngfw`;
- При попытке повторной авторизации пользователя, который уже авторизован по IP, появляется предупреждение:



- После каждого обновления приложение Ideco Client запускается автоматически;
- Информация о сессиях пользователей отображается в разделе *Авторизованные пользователи*:



14.5.5 DNS-запросы при VPN-подключении через Ideco Client

При подключении через Ideco Client DNS-запросы могут не проходить, если выбран тип передачи маршрутов **Отправлять только указанные сети**. При выборе **Отправлять маршруты до локальных сетей Ideco NGFW** сеть до NGFW отправляется автоматически. Это связано с особенностями построения таблицы маршрутизации при подключении через Ideco Client:

- При VPN-подключении без Ideco Client DNS-запросы идут на DNS, прописанный в настройках подключения (как правило, адрес NGFW);
- При VPN-подключении через Ideco Client DNS-запросы идут на адрес NGFW, но в передаваемом на Ideco Client списке нет маршрута до DNS NGFW.

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

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

14.5.6 Device VPN

Device VPN - режим работы Ideco Client, в котором клиентское устройство авторизуется на Ideco NGFW без входа пользователя в систему. Такое соединение позволяет:

- Устанавливать на устройства программы и обновления
- Получать доступ к внутренней инфраструктуре
- Применять групповые политики
- Блокировать/разблокировать устройства и пользователей
- Отслеживать активность устройств и управлять устройствами за пределами внутренних сетей

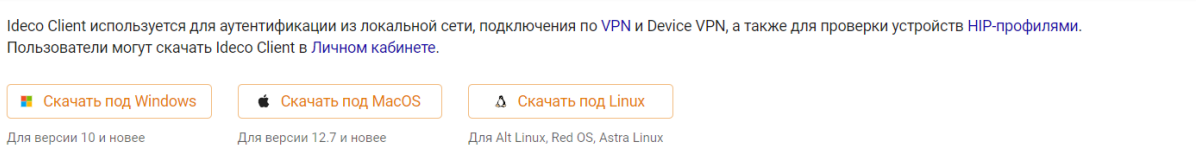
Для авторизации через Device VPN используется корневой сертификат с приватным ключом. На основе этого ключа администратор создает пользовательские сертификаты для конечных устройств.

14.5.7 Установка и настройка Ideco Client на Windows

Скачивание

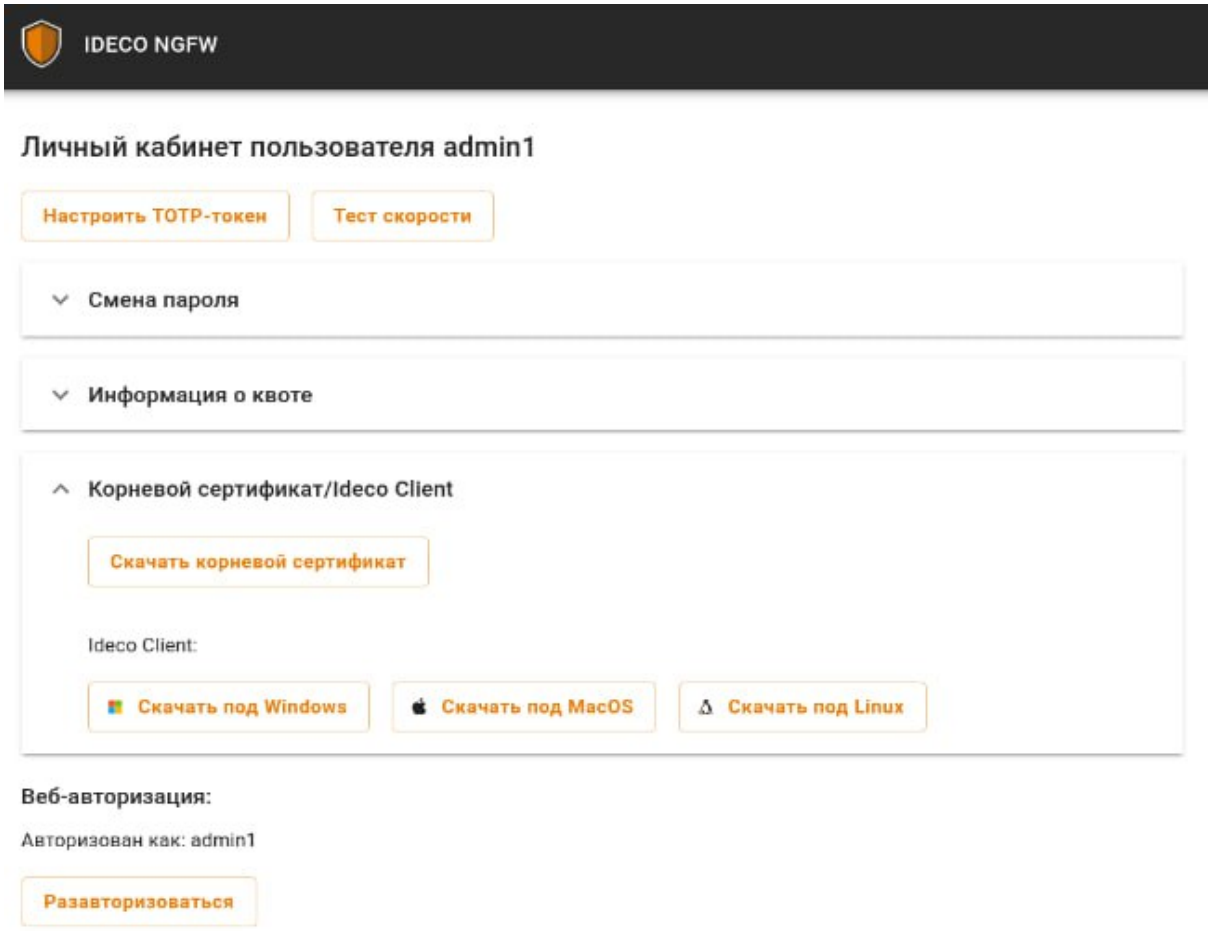
Для администратора

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



Для пользователя

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



Установка

Сохраните и запустите файл установки *IdecoAgent.msi*.

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

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

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

Настройка профиля для первого запуска

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

Для импорта сертификата на компьютер выполните действия:

1. Дважды кликните на скачанный файл сертификата.

2. В открывшемся окне выберите **Установить сертификат**.

3. Откроется **Мастер импорта сертификатов**. В качестве **Расположения хранилища** выберите **Локальный компьютер**.

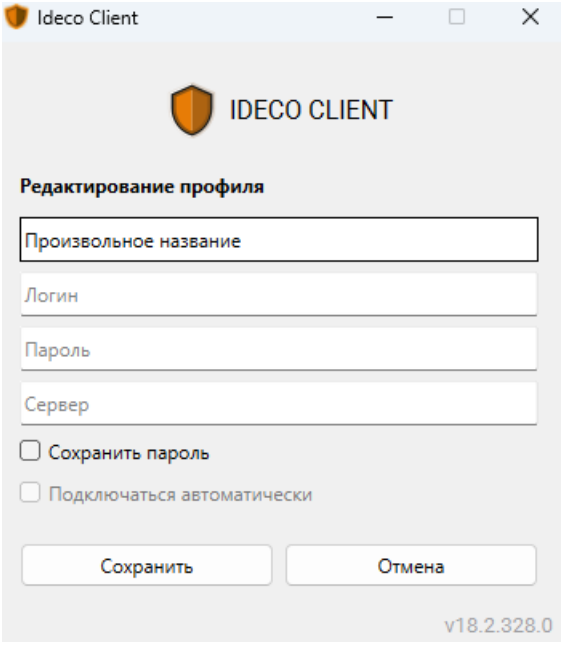
4. Выберите пункт **Поместить все сертификаты в следующее хранилище**, нажмите **Обзор** и выберите папку **Доверенные корневые центры сертификации**.

5. Нажмите **Ок -> Далее -> Готово**.

Первый запуск

1. Запустите Ideco Client. Программа установит связь с сервером.

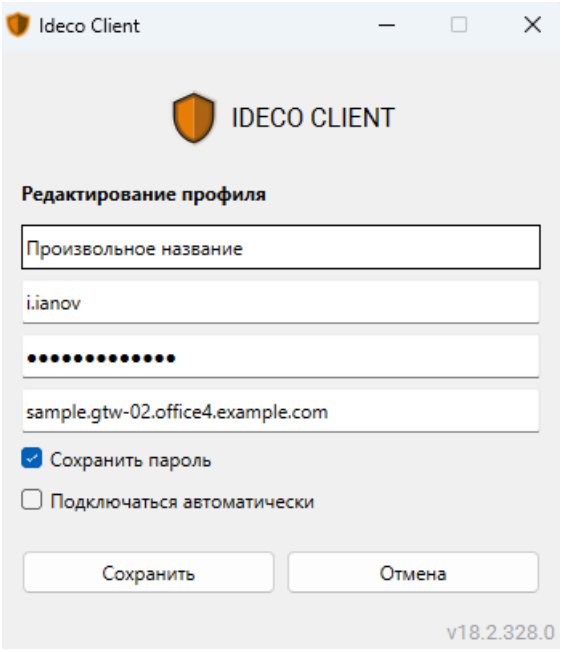
2. Введите данные:



- **Название профиля** - введите произвольное название профиля, который будет доступен для выбора при подключении. Может не совпадать с логином;
- **Пароль** - укажите пароль пользователя;
- **Логин** и **Адрес сервера** - укажите логин и хост в зависимости от количества доменов, в которые введен NGFW:

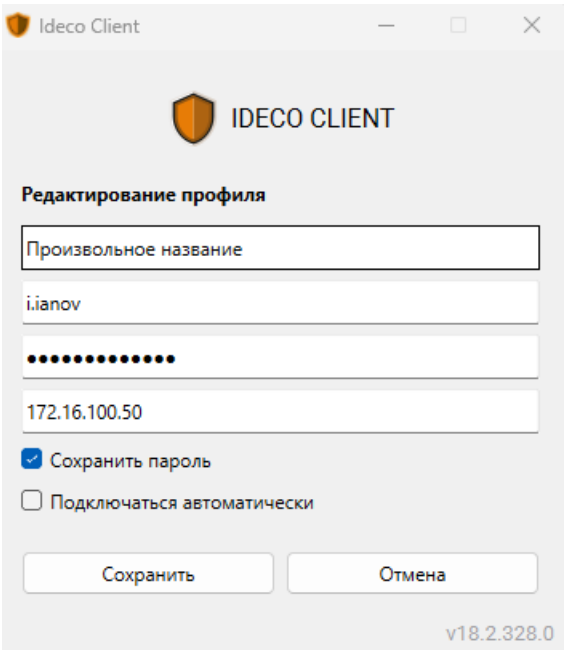
NGFW введен в один домен:

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



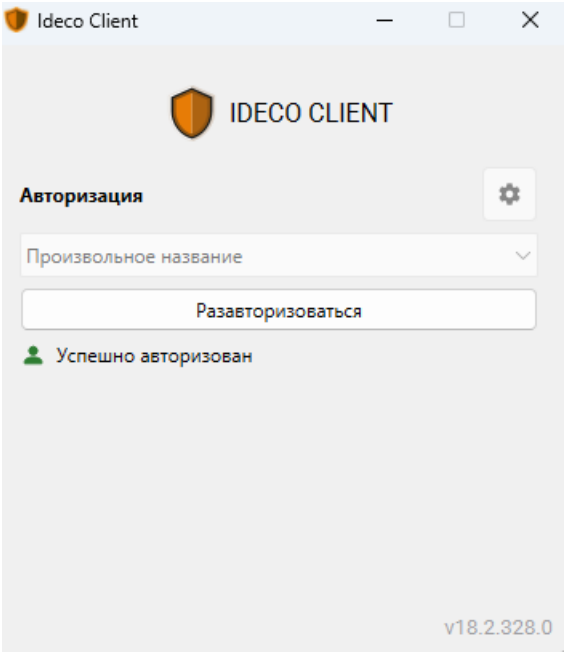
NGFW введен в несколько доменов:

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



3. Нажмите **Сохранить**.

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



Редактирование профиля

1. Перейдите в раздел **Настройки**, кликнув по .

2. Выберите профиль для редактирования, нажав , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

14.5.8 Установка и настройка Ideco Client на MacOS

Особенности работы Ideco Client на MacOS

- Ideco Client для MacOS требует версии системы 12.7 и выше;
- Чтобы трафик клиента при подключении через Ideco Client шел через Ideco NGFW, необходимо в разделе **Пользователи -> VPN-подключения -> Передача маршрутов** выбрать настройку **Отправлять весь трафик на Ideco NGFW (Использовать Ideco NGFW как шлюз по умолчанию)**;
- *HIP-профили* на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

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

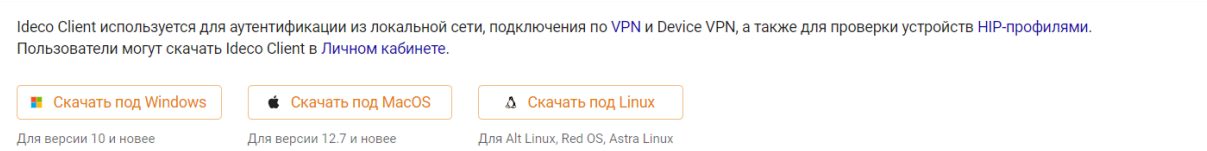
Недоступные HIP-профили

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

Скачивание

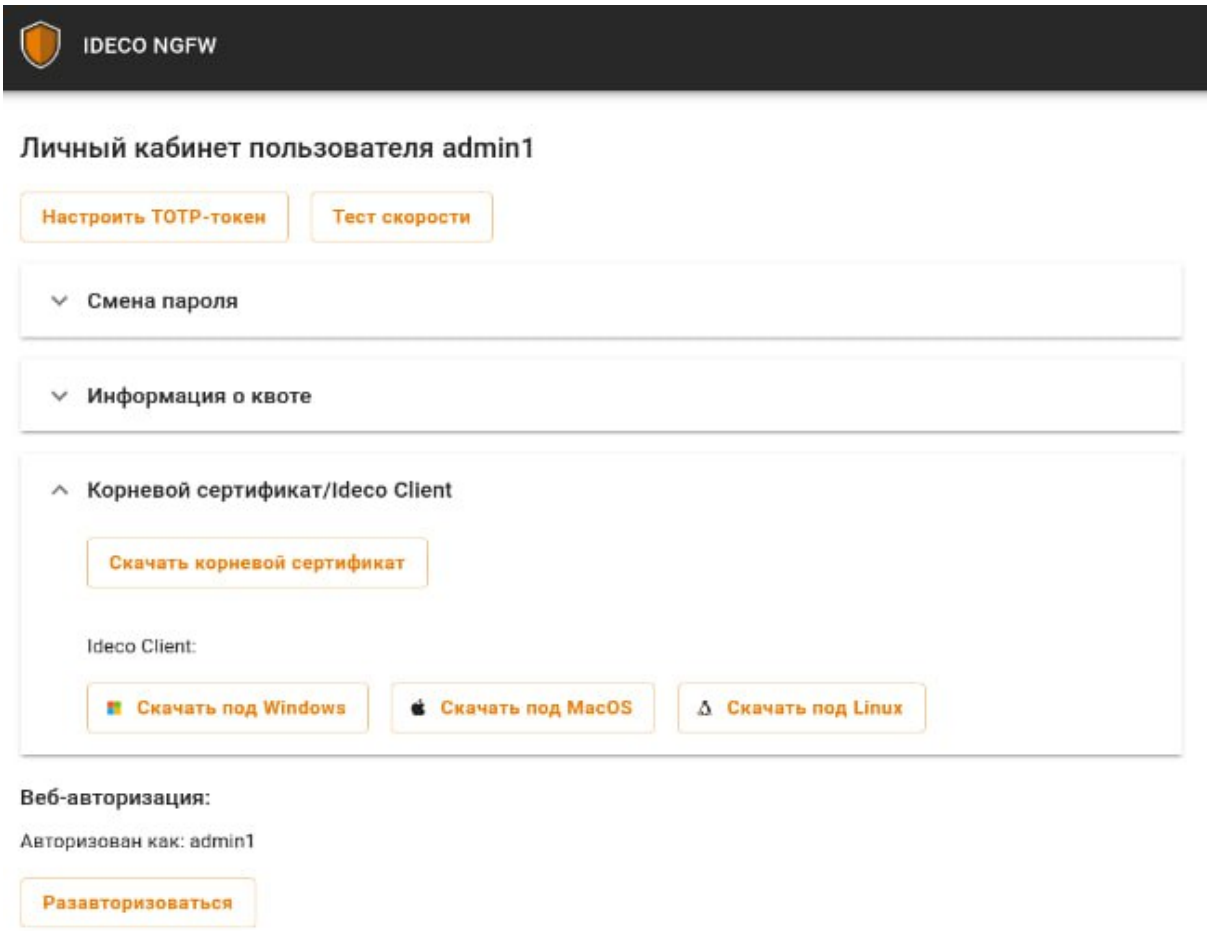
Для администратора

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



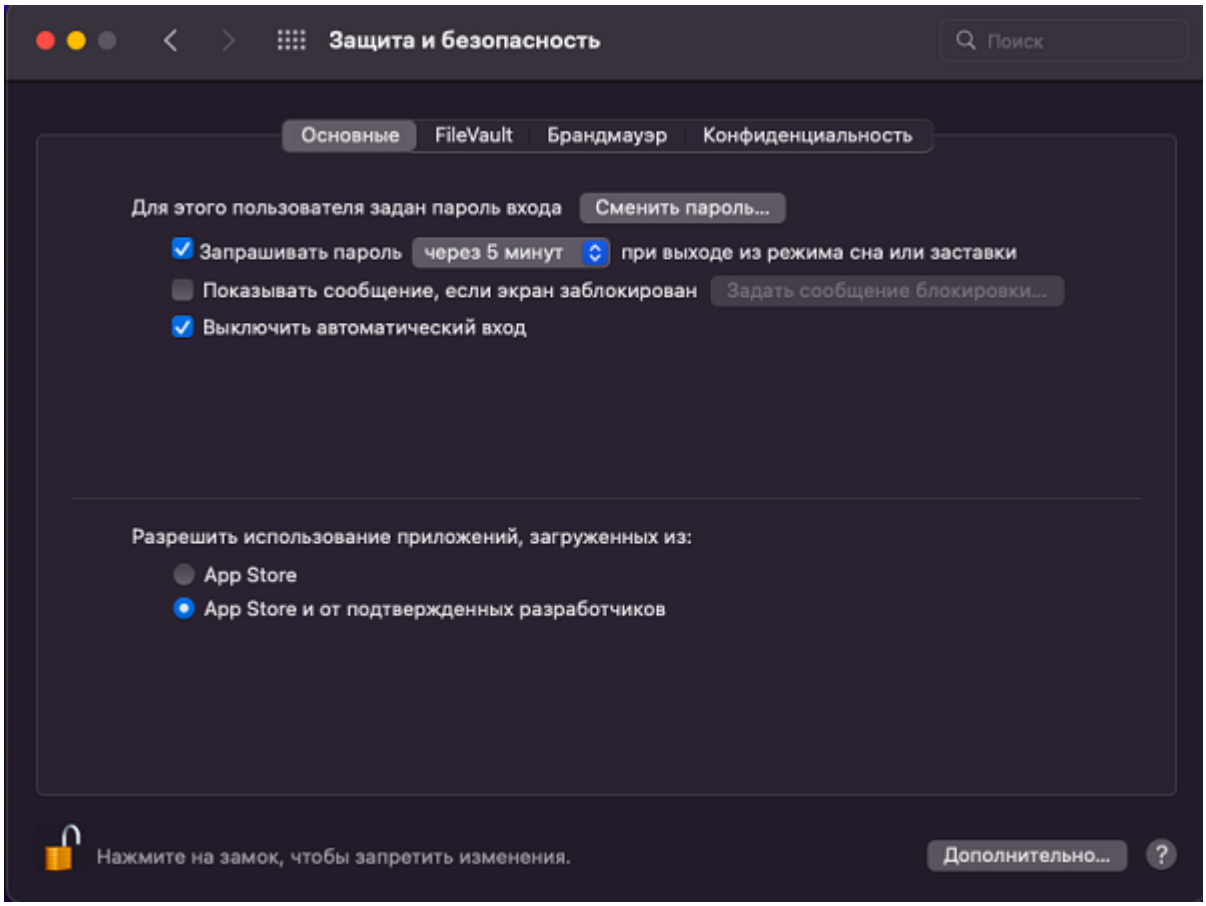
Для пользователя

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



Установка

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

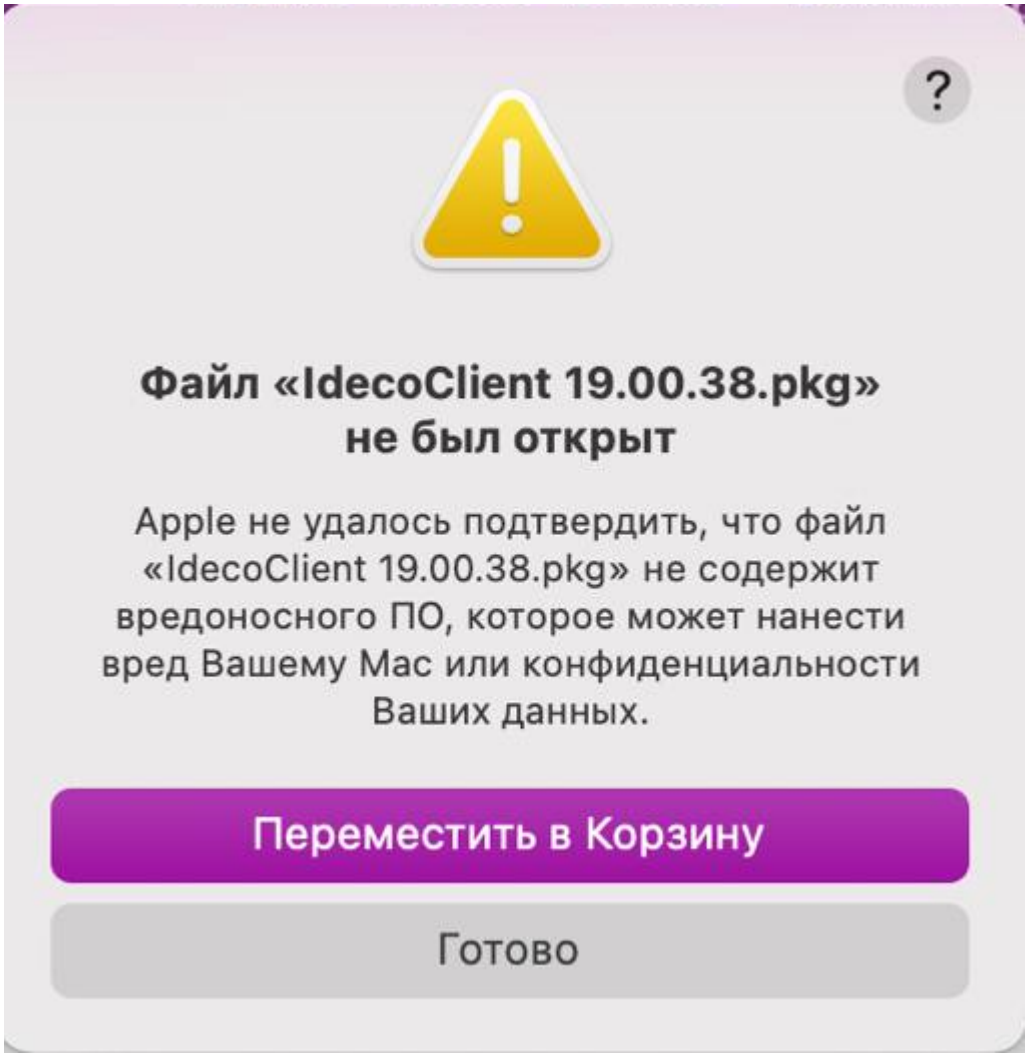


Чтобы установить **Ideco Client** на MacOS, выполните действия:

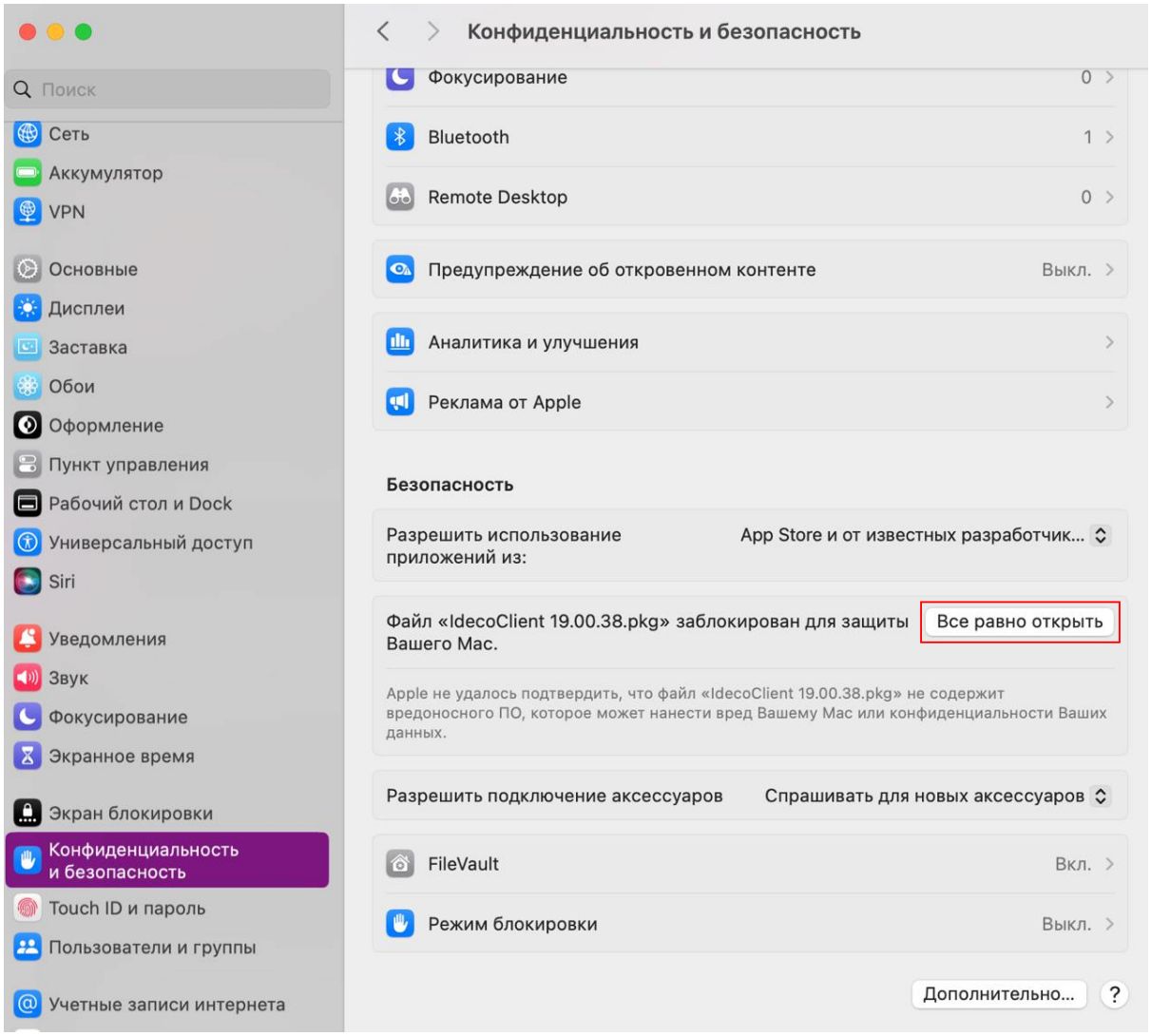
1. Кликните по файлу *IdecoClient.pkg* правой кнопкой мыши и выберите **Открыть**.

MacOS Sequoia:

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

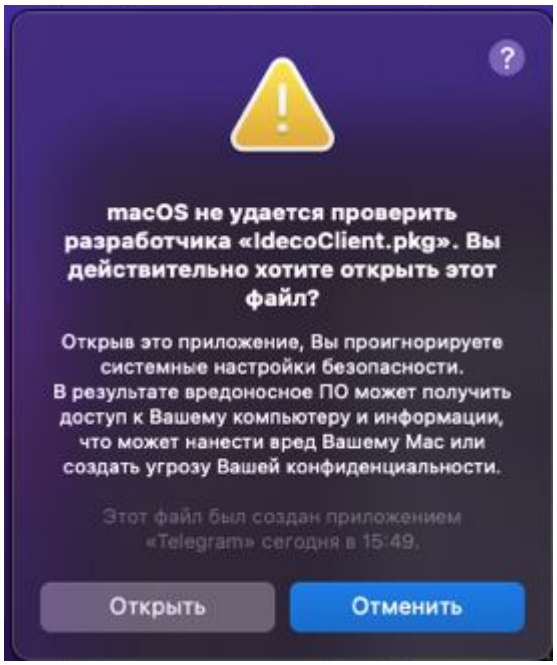


2. Перейдите в раздел **Конфиденциальность и безопасность** и нажмите **Все равно открыть** рядом с именем файла:

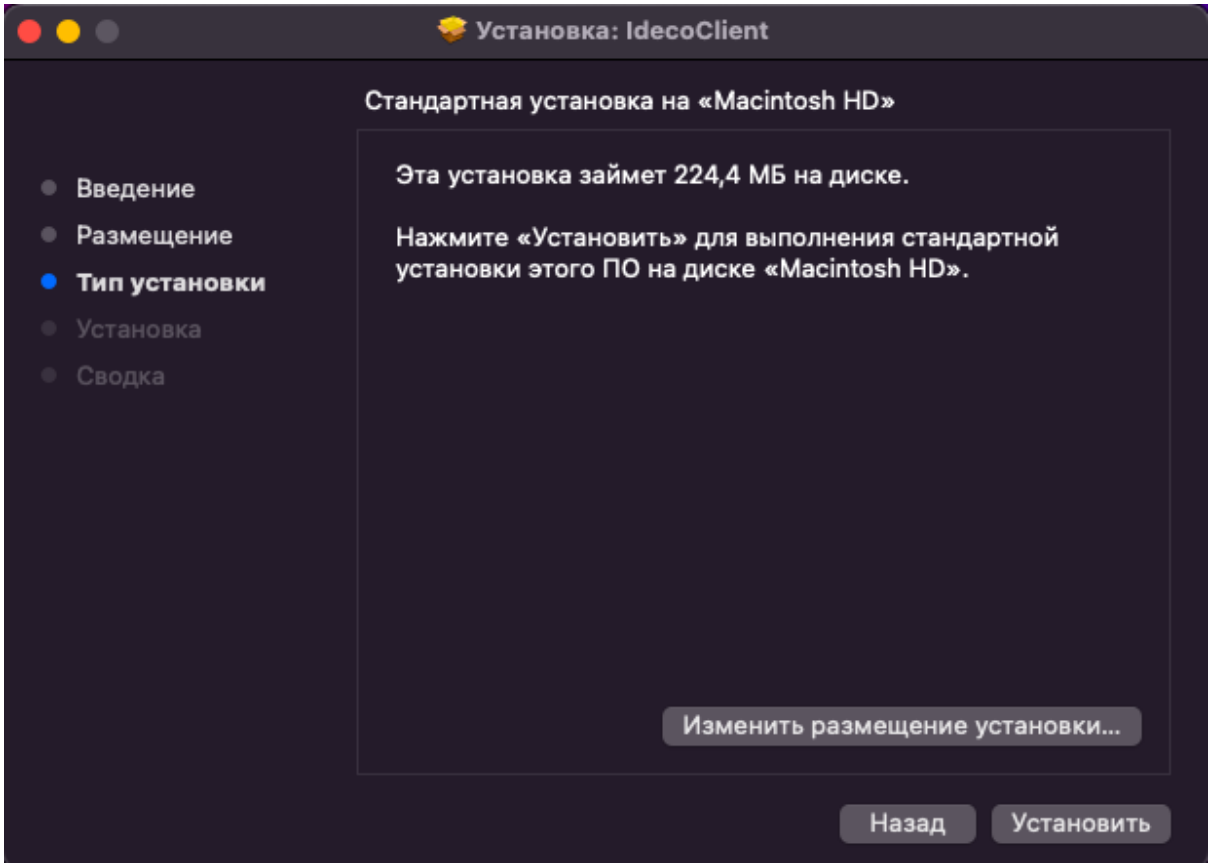


MacOS Monterey и MacOS Sonoma:

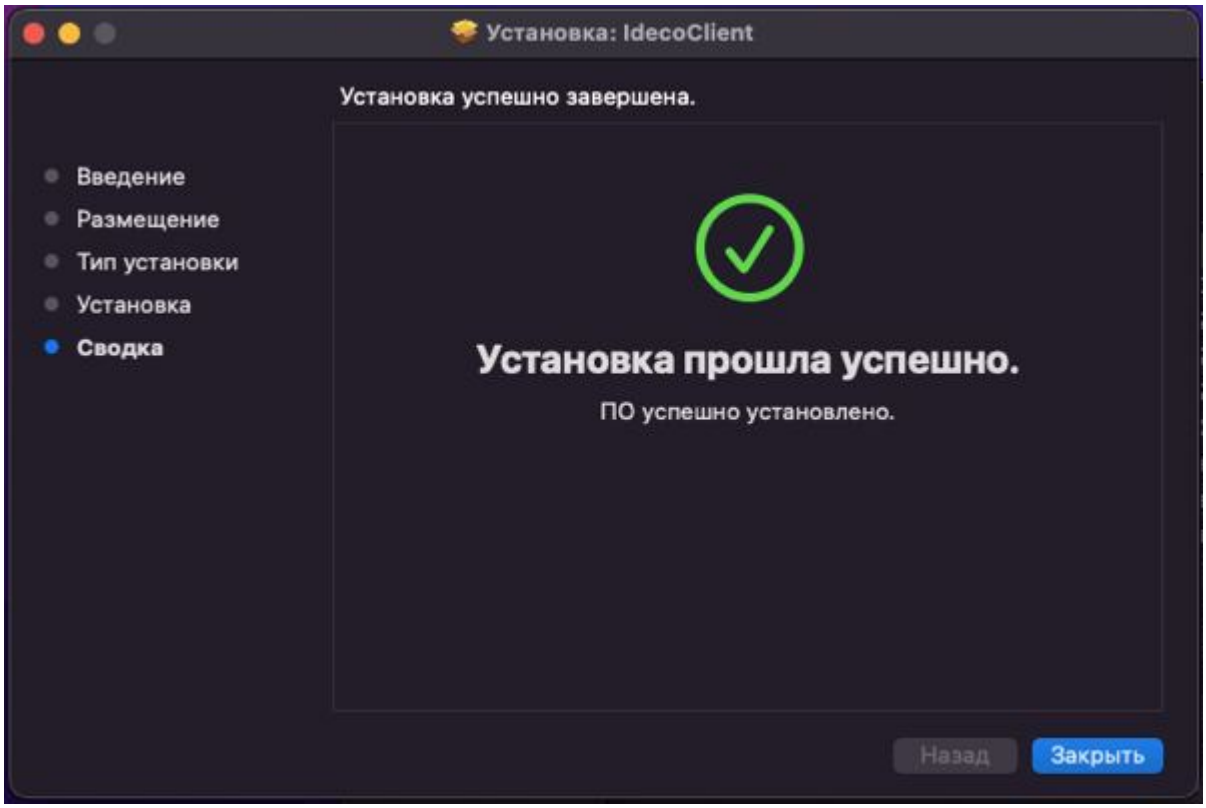
При открытии файла *IdecoClient.pkg* система выдаст предупреждение. Подтвердите действие:



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



3. Если установка завершилась успешно, на экране появится соответствующее сообщение:



Настройка профиля для первого запуска

Перед подключением к Ideco NGFW по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt импортируйте корневой сертификат Ideco NGFW на компьютер и убедитесь, что срок действия сертификата на домен или IP-адрес составляет **825 дней**.

Если срок действия сертификата превышает 825 дней, *загрузите* на Ideco NGFW сертификат со сроком действия, не превышающим 825 дней, или *перевыпустите* автоматически сгенерированный сертификат.

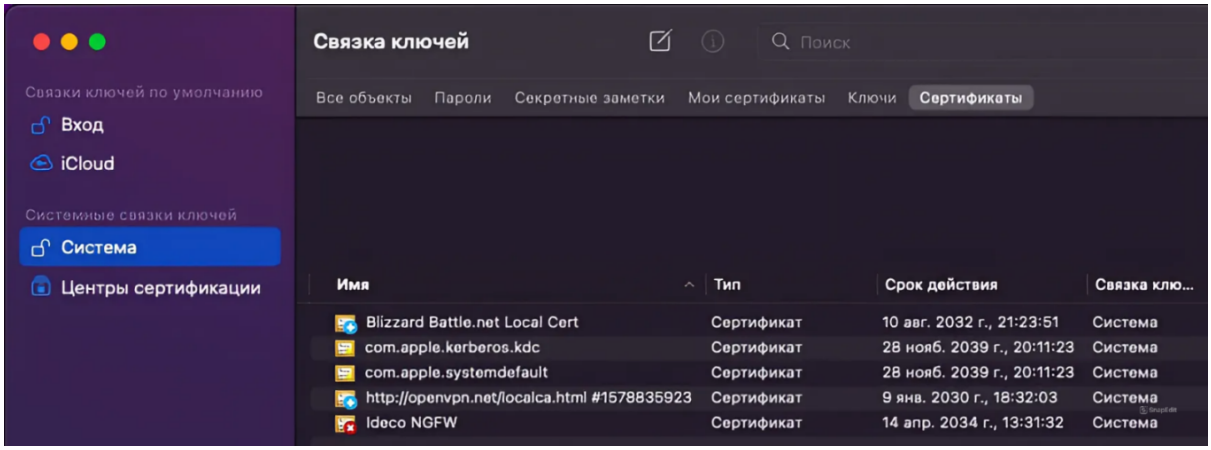
Установка корневого сертификата Ideco NGFW на MacOS:

Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Важно! Не храните файл сертификата в директориях *Desktop*, *Documents* и *Downloads*: в этом случае Ideco Client не сможет получить доступ к этим файлам и прочитать их. Рекомендуем сохранить файлы в другую директорию, например, в корневую директорию домашней папки пользователя.

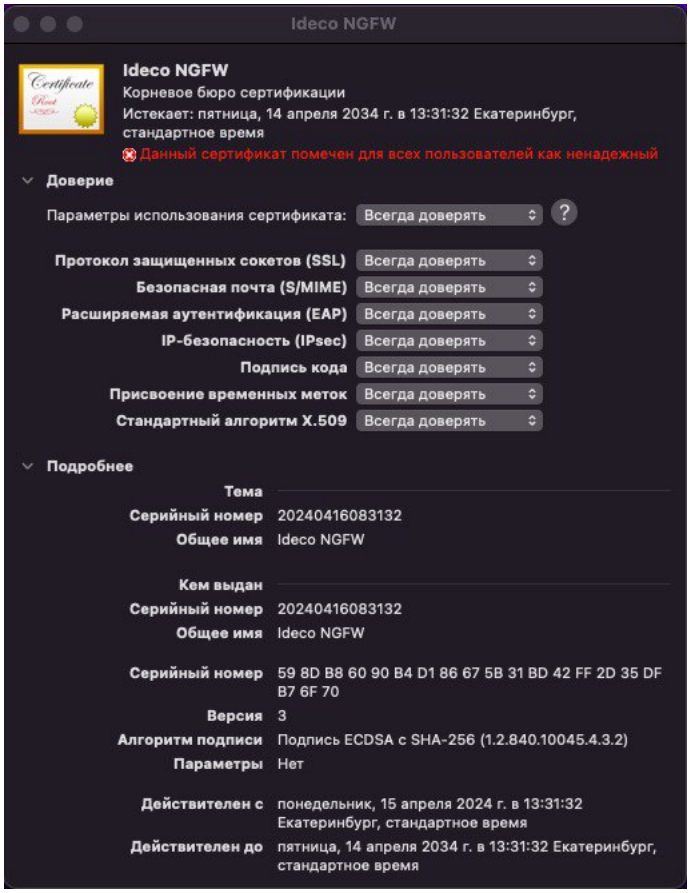
Чтобы установить сертификат на MacOS, выполните действия:

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

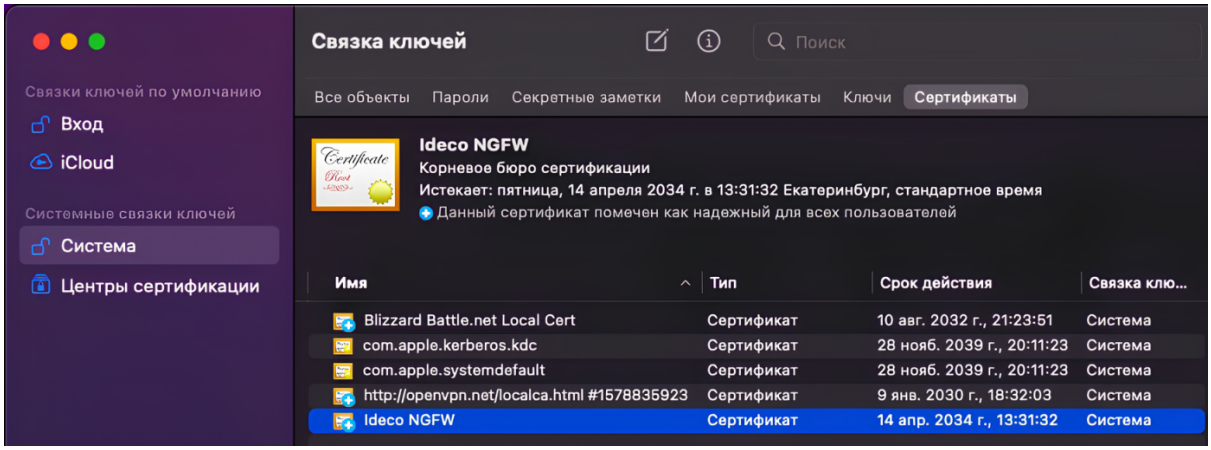


2. Нажмите по сертификату правой кнопкой мыши и выберите **Свойства**.

3. Установите в поле **Параметры использования сертификата** действие **Всегда доверять**:



4. Закройте окно свойств сертификата. Теперь сертификат помечен как надежный для всех пользователей устройства:



Также сертификат можно добавить с помощью команды:

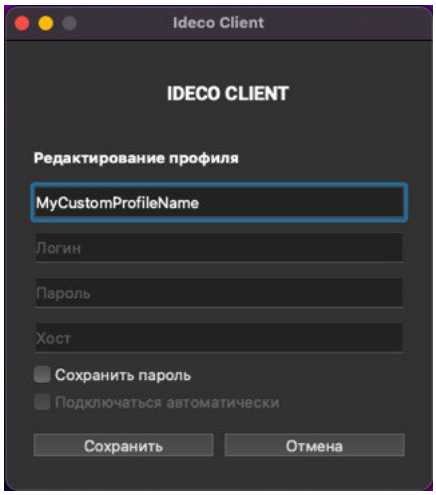
```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain/
↪Users/<учетная запись>/Downloads/root_ca.crt
```

5. Перезагрузите компьютер.

Первый запуск

1. Запустите Ideco Client. Программа установит связь с сервером.

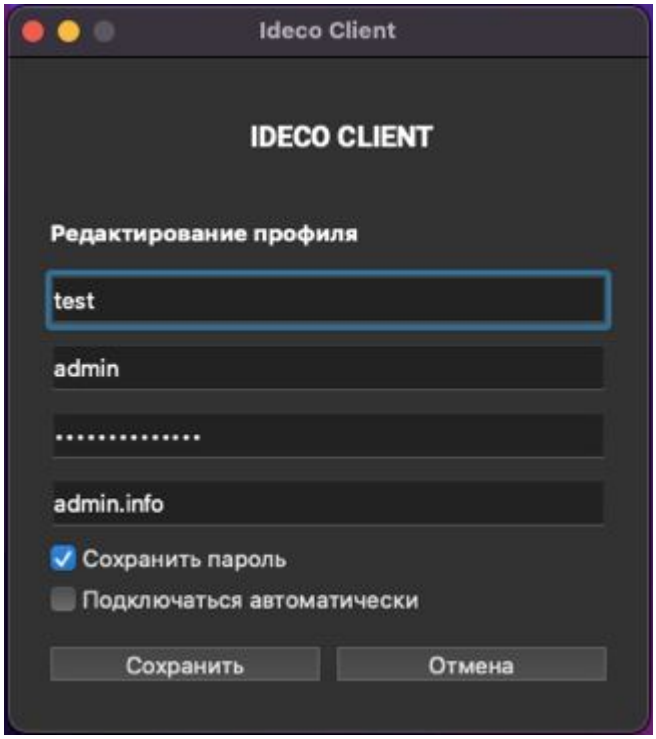
2. Введите данные:



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

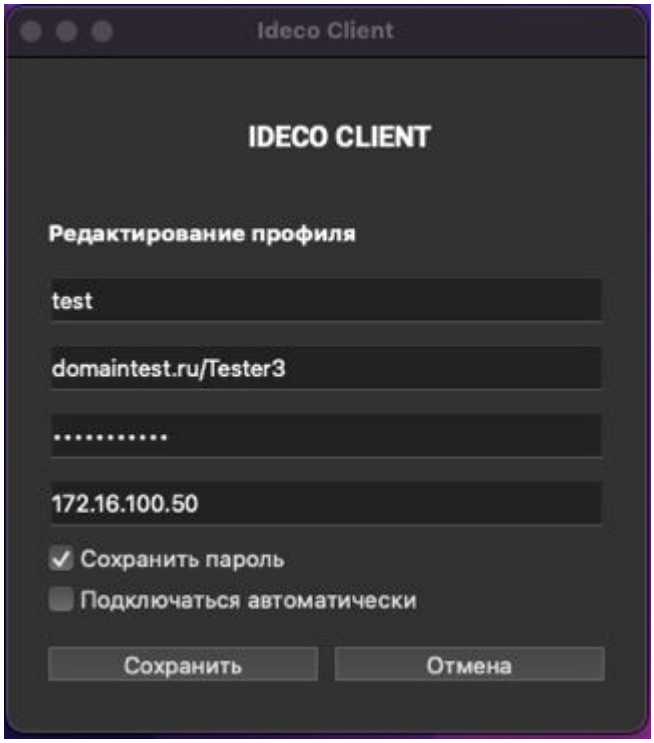
NGFW введен в один домен:

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



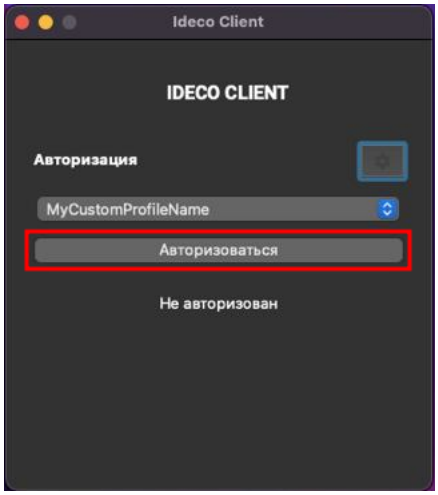
NGFW введен в несколько доменов:

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



3. Нажмите **Сохранить**.

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



Редактирование профиля

1. Перейдите в раздел **Настройки**, кликнув по .

2. Выберите профиль для редактирования, нажав , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

14.5.9 Установка и настройка Ideco Client на Linux

Особенности работы Ideco Client на Linux

- Ideco Client гарантированно работает на Alt Linux, РЕД ОС, Astra Linux, Fedora, Ubuntu. Для остальных дистрибутивов работа не гарантируется;
- *HIP-профили* на стороне агента поддерживаются **не в полном объеме**:

Доступные HIP-профили

- ОС;
- процесс.

Недоступные HIP-профили

- антивирус;
- домен;
- межсетевой экран;
- реестр (всегда только Windows);
- службы (всегда только Windows);
- пакет обновлений Knowledge Base (всегда только Windows).
- Для проверки запуска процесса с заданным именем в системе (ZTNA) используется функция:

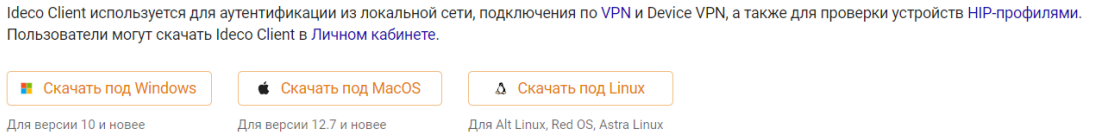
```
bool os_specific::isProcessExist(const std::string &processName)
```

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

Скачивание

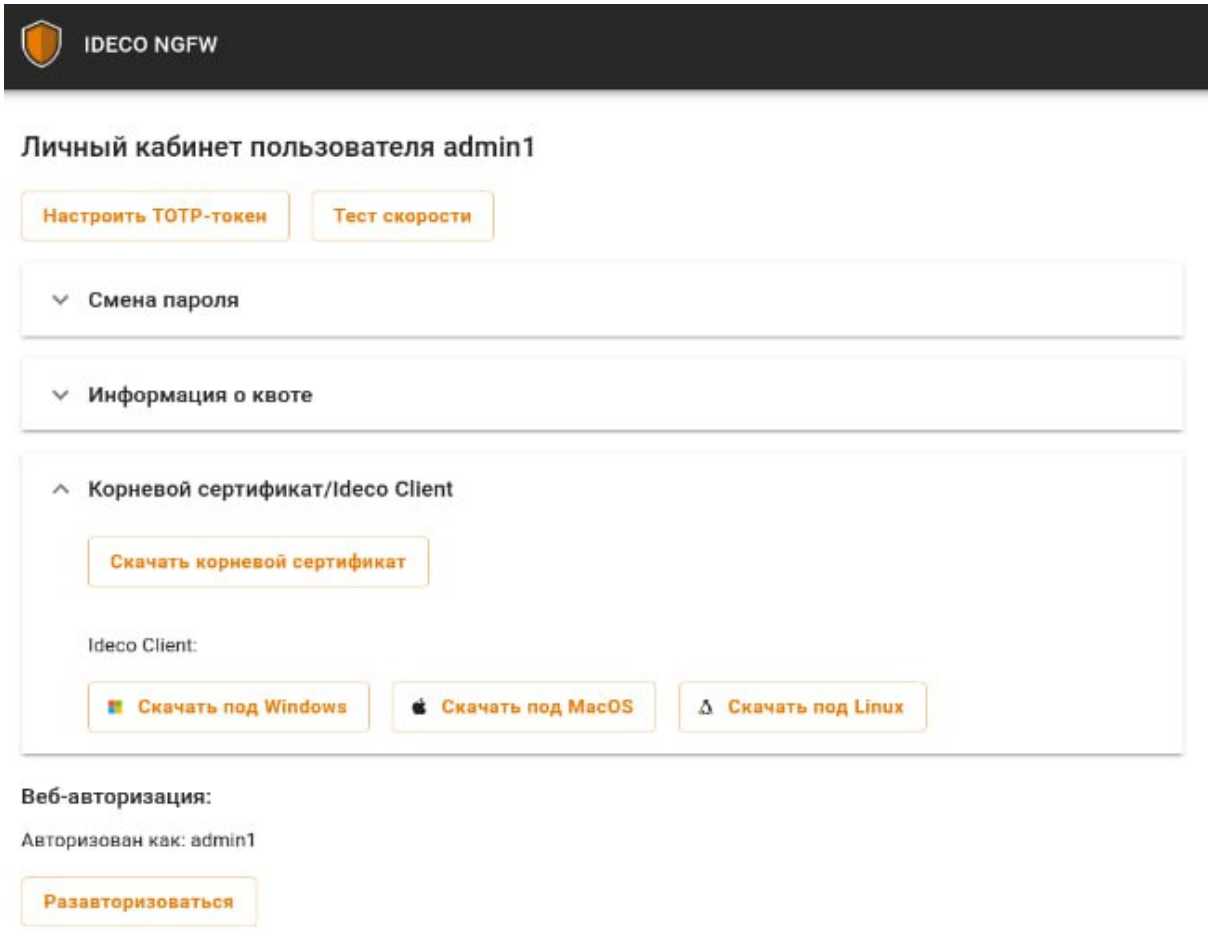
Для администратора

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



Для пользователя

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



Установка

Для установки Ideco Client на Linux выполните действия:

1. Перейдите в папку со скачанным файлом установки Ideco Client:

```
cd "Путь до директории с установочным файлом"
```

2. Предоставьте файлу разрешение на исполнение, выполнив в терминале команду:

```
chmod +x IdecoAgent.sh
```

3. Запустите файл установки Ideco Client:

```
./IdecoAgent.sh
```

4. После установки проверьте статус службы IdecoService, выполнив команду:

```
systemctl status IdecoService.service
```

5. Убедитесь, что служба IdecoService запущена и работает:

Подсказка: Для добавления службы в автозагрузку выполните команду:

```
systemctl enable IdecoService.service
```

Предупреждение: Для корректной работы Ideco Client на Astra Linux удалите настройку службы IdecoService:

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

Настройка профиля для первого запуска

Перед подключением к Ideco NGFW по внешнему IP-адресу или доменному имени без сертификата Let's Encrypt импортируйте корневой сертификат Ideco NGFW на компьютер и убедитесь, что срок действия сертификата на домен или IP-адрес составляет **825 дней**.

Если срок действия сертификата превышает 825 дней, *загрузите* на Ideco NGFW сертификат со сроком действия, не превышающим 825 дней, или *перевыпустите* автоматически сгенерированный сертификат.

Для импорта корневого сертификата на конкретный дистрибутив воспользуйтесь статьями:

- Установка корневого сертификата на Astra Linux;
- Установка корневого сертификата на Alt Linux;
- Установка корневого сертификата на Red OS;
- Установка корневого сертификата на Ubuntu/Debian.

Первый запуск

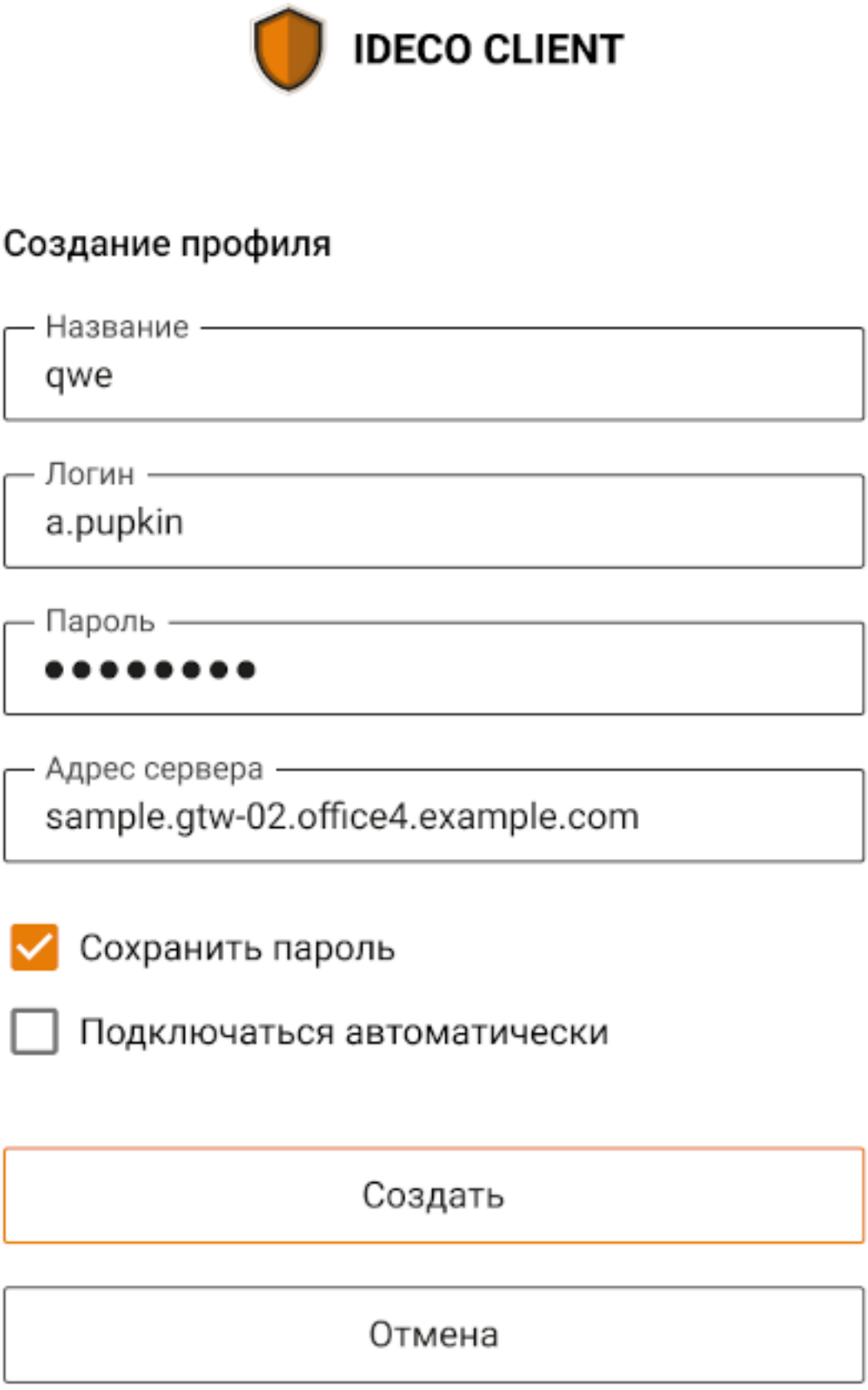
1. Запустите Ideco Client. Программа установит связь с сервером.

2. Введите данные:

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

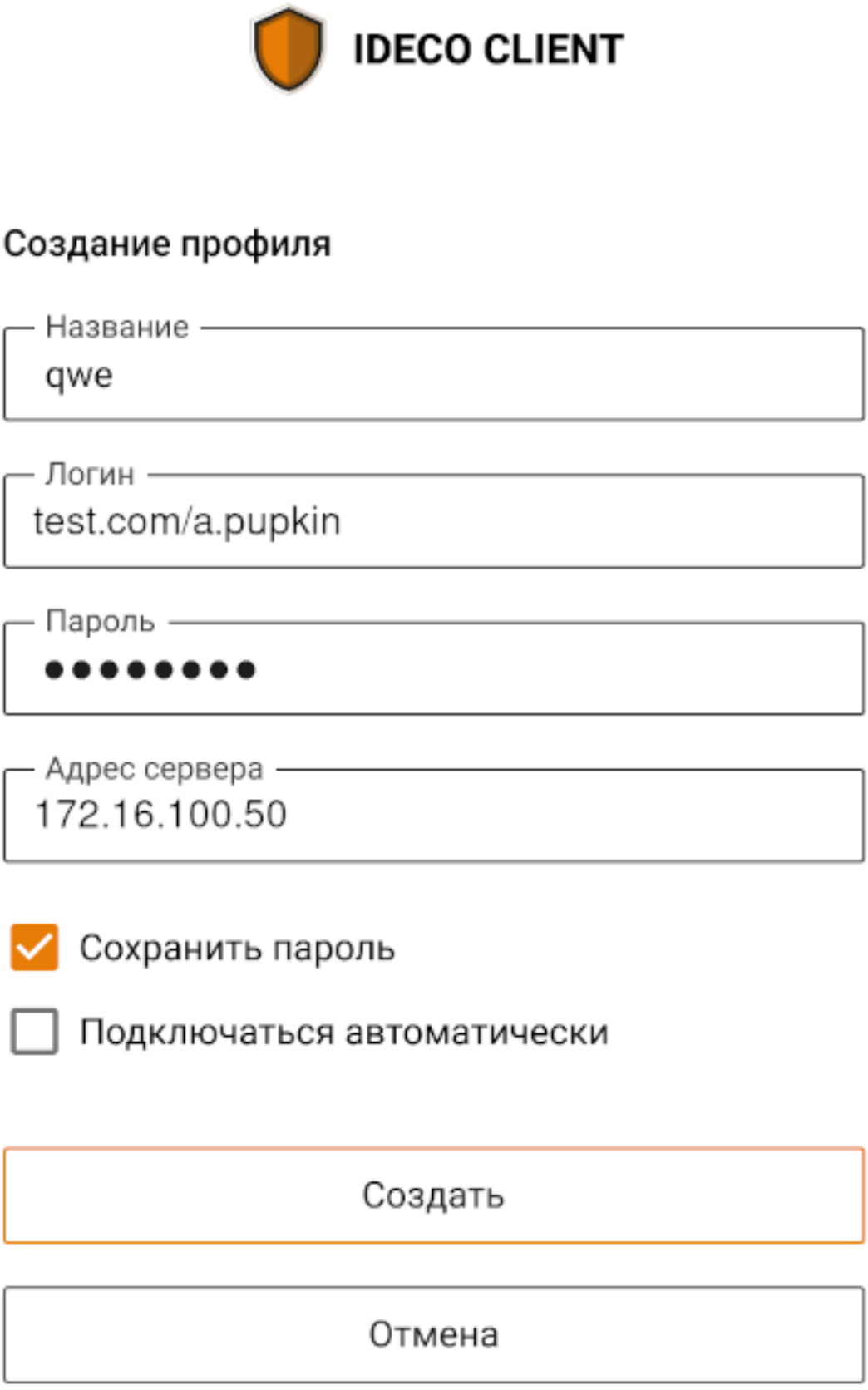
NGFW введен в один домен:

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



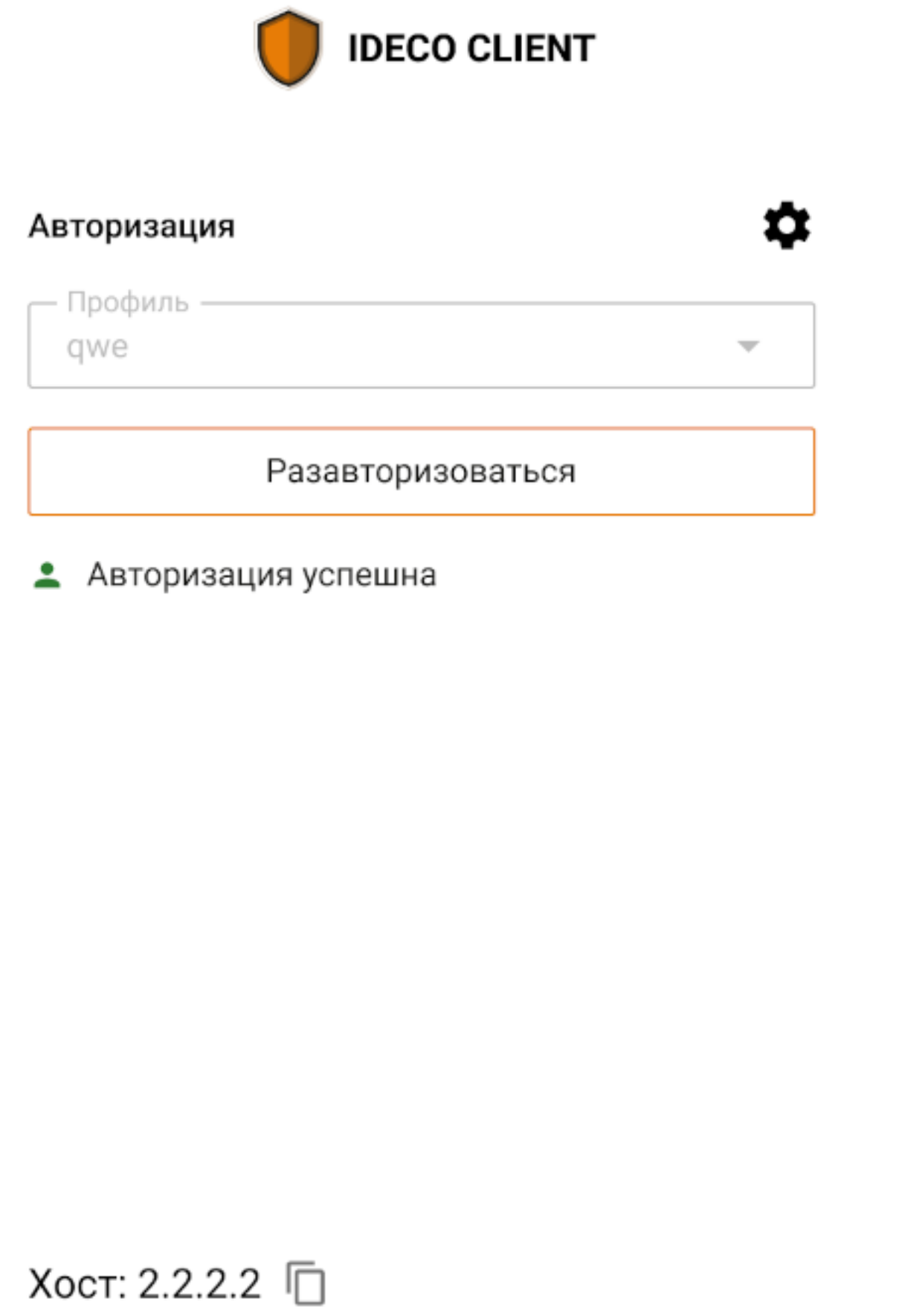
NGFW введен в несколько доменов:

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



3. Нажмите **Сохранить**.

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


IDECO CLIENT
Авторизация
Профиль
qwe
Разавторизоваться
Авторизация успешна
Хост: 2.2.2.2

Редактирование профиля

1. Перейдите в раздел **Настройки**, кликнув по .

2. Выберите профиль для редактирования, нажав , и внесите изменения в поля формы.

3. Сохраните изменения в полях формы, нажав кнопку **Сохранить**.

14.5.10 Настройка Device VPN

Основное

На Ideco NGFW необходимо загрузить доверенный сертификат, который будет использоваться для подписи сертификата авторизации устройства. Если для авторизации будет использоваться самоподписанный сертификат, его также можно загрузить в качестве доверенного.

Если для проверки подлинности используется промежуточный сертификат, то на Ideco NGFW нужно загрузить файл, содержащий всю цепочку сертификатов, начиная с корневого. Структура этого файла похожа на *структуру* файла для загрузки SSL-сертификата на сервер.

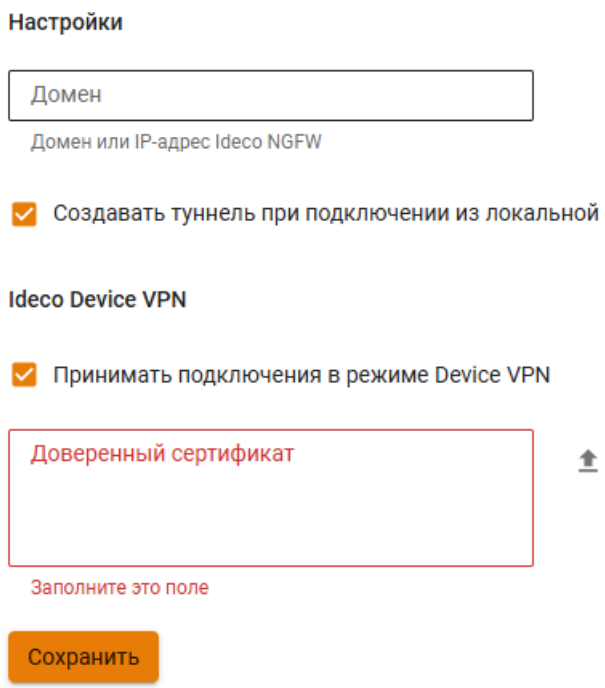
Чтобы подключить устройство к Ideco NGFW в режиме Device VPN, выполните действия:

1. В веб-интерфейсе Ideco NGFW перейдите в раздел **Пользователи -> Ideco Client**.

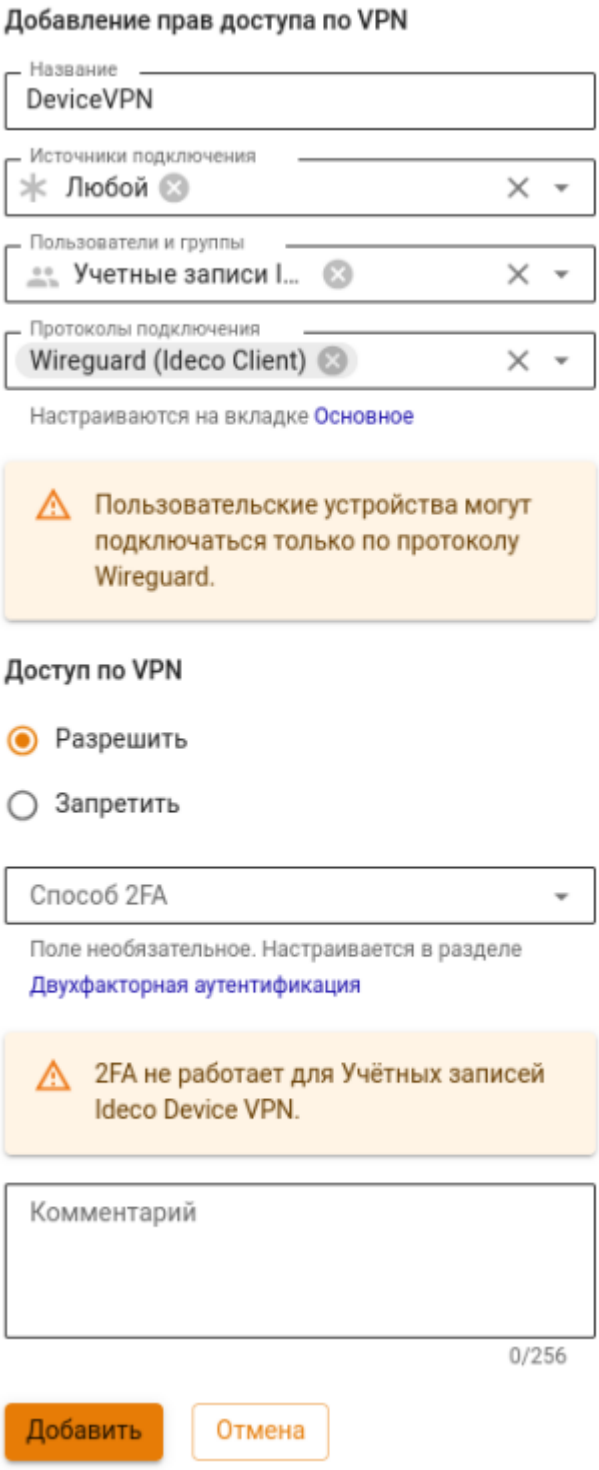
2. Введите домен или IP-адрес Ideco NGFW, включите настройку **Создавать туннель при подключении из локальной сети** (если устройства пользователей находятся в локальной сети).

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

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



5. Перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте правило, разрешающее учетным записям Ideco Device VPN подключение по протоколу Wireguard:



Подсказка: Если в таблице **Доступ по VPN** устройству из группы Device VPN запрещен доступ, на короткое время подключение из внешней сети будет установлено. За это время может пройти определенный объем трафика. Позже подключение будет разорвано. Это связано с тем, что проверка по таблице доступа VPN для Device VPN происходит не в момент подключения, а позже.

6. Установите Ideco Client на устройство пользователя (*Windows*, *Linux*, *MacOS*).

7. Загрузите на устройство пользователя сертификат с расширением .pem, который содержит приватный ключ и подписан доверенным сертификатом. Процесс создания сертификата описан в статье *Создание сертификатов для Device VPN*.

Внимание: Рекомендуем для безопасности хранить сертификаты в директориях, к которым есть доступ только у администратора. Например:

- Для Linux - это home-каталог `/root`, в который имеет доступ только администратор;
- Для Windows нужно создать новую папку. В свойствах папки в разделе **Безопасность** нужно разрешить доступ только для пользователя Система/System.

8. Запустите установленный Ideco Client:

Для Windows:

Откройте командную строку от имени администратора и введите:

```
<абсолютный путь до IdecoClient>\IdecoClient.exe --set-devicevpn-cert-path=
↪<абсолютный путь до файла сертификата> --set-devicevpn-host=<адрес NGFW> --set-
↪enable-devicevpn=True
```

Для Linux:

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/ld.so --argv0 IdecoClient --library-path
↪<абсолютный путь до IdecoClient>/lib <абсолютный путь до IdecoClient>/IdecoClient --
↪set-devicevpn-cert-path=<абсолютный путь до файла сертификата> --set-devicevpn-host=
↪<адрес NGFW> --set-enable-devicevpn=True
```

Для вывода заданных параметров в консоль воспользуйтесь командой:

```
sudo <абсолютный путь до IdecoClient>/ld.so --argv0 IdecoClient --library-path
↪<абсолютный путь до IdecoClient>/lib <абсолютный путь до IdecoClient>/IdecoClient --
↪print-devicevpn-config=True
```

Для MacOS:

Откройте терминал и введите:

```
sudo <абсолютный путь до IdecoClient>/IdecoClient --set-devicevpn-cert-path=
↪<абсолютный путь до файла сертификата> --set-devicevpn-host=<адрес NGFW> --set-
↪enable-devicevpn=True
```

Для вывода заданных параметров в консоль воспользуйтесь командой:

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

Предупреждение: При неудачном подключении Device VPN попытка соединения будет бесконечной, даже если закрыть Ideco Client или перезапустить службу.

Для решения проблемы необходимо:

- Выключить Device VPN: выполнить команду по настройке Device VPN с единственным параметром `--set-enable-devicevpn=False`;
- Исправить проблему подключения (загрузить правильный сертификат, определить корректность пути до него);
- Настроить и активировать Device VPN: выполнить команду по настройке Device VPN и параметром `--set-enable-devicevpn=True`.
- В интерфейсе Ideco NGFW убедиться, что подключение Device VPN выполнено.

14.5.11 Создание сертификатов для Device VPN

В статье описан процесс создания сертификатов с использованием OpenSSL для подключения по *Device VPN* между Ideco NGFW и Ideco Client. Процесс включает в себя два этапа:

1. Создание корневого сертификата с защищенным приватным ключом.

2. Создание сертификатов для пользовательских устройств на основе этого корневого сертификата.

Создание корневого сертификата

1. Сгенерируйте приватный ключ корневого сертификата, защищенный *passphrase*:

```
openssl genrsa -des3 -out ideco-dvpn_root-ca.key 4096
```

- `-des3` - приватный ключ зашифрован алгоритмом Triple DES (3DES);
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ.

2. Сгенерируйте корневой сертификат, используя приватный ключ корневого сертификата:

```
openssl req -x509 -new -sha256 -days 1825 -key ideco-dvpn_root-ca.key -nodes -out␣
↪ideco-dvpn_root-ca.pem
```

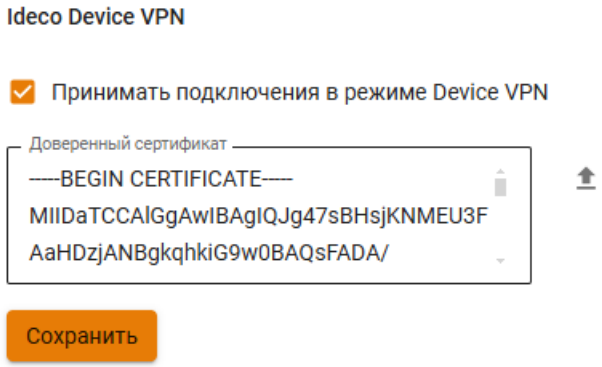
- `-nodes` - не шифровать приватный ключ сертификата;
- `-sha256` - использовать алгоритм SHA256 при создании сертификата;
- `-days 1825` - срок действия сертификата в днях;
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ корневого сертификата;
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат.

3. Проверьте, что сертификат был успешно создан командой:

```
openssl x509 -text -noout -in ideco-dvpn_root-ca.pem
```

- Корневой сертификат должен иметь атрибут `CA:TRUE`;
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат.

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



После этого корневой сертификат будет необходим для создания пользовательских сертификатов.

Создание пользовательского сертификата для конечного устройства

1. Сгенерируйте приватный ключ без применения шифрования (в дальнейшем незашифрованный ключ размещается в пользовательском пространстве администратора, куда у пользователей не будет доступа):

```
openssl genrsa -out client1-dvpn.key 4096
```

- `client1-dvpn.key` - файл, содержащий приватный ключ.

2. Сгенерируйте запрос на выпуск пользовательского сертификата с использованием приватного ключа:

```
openssl req -new -key client1-dvpn.key -out client1-dvpn.csr
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.csr` - файл, содержащий зашифрованный запрос на выпуск сертификата.

3. Создайте файл расширений сертификата для использования в генерации сертификата:

```
File: client1-dvpn.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = client1.lan1.ru
```

- В этом файле используется subjectAltName (SAN) и указывается DNS-имя пользовательского устройства. DNS-имя используется в качестве имени пользователя Device VPN на Ideco NGFW.

4. Сгенерируйте сертификат пользовательского устройства от *корневого сертификата для Device VPN* от корневого сертификата для Device VPN:

```
openssl x509 -req -in client1-dvpn.csr -CA ideco-dvpn_root-ca.pem -CAkey ideco-dvpn_
↪root-ca.key -CAcreateserial -out client1-dvpn.crt -days 825 -sha256 -extfile␣
↪client1-dvpn.ext
```

- `client1-dvpn.csr` - файл, содержащий зашифрованный запрос на выпуск сертификата;
- `ideco-dvpn_root-ca.pem` - файл, содержащий корневой сертификат;
- `ideco-dvpn_root-ca.key` - файл, содержащий приватный ключ корневого сертификата;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат.

5. Проверьте, что сертификат был успешно создан командой:

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

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

6. Объедините приватный ключ и сертификат пользовательского устройства:

```
cat client1-dvpn.key client1-dvpn.crt > client1-dvpn.pem
```

- `client1-dvpn.key` - файл, содержащий приватный ключ;
- `client1-dvpn.crt` - файл, содержащий пользовательский сертификат;
- `client1-dvpn.pem` - файл, содержащий пользовательский сертификат с приватным ключом внутри.

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

14.5.12 Балансировка VPN-подключений

Балансировка VPN-подключений происходит на стороне Ideco Client с использованием SRV-записей DNS.

Внимание: В SRV-записи DNS нельзя указывать IP-адрес, только FQDN (полностью определенное доменное имя, не имеющее неоднозначностей в определении). При указании IP-адреса в SRV-записи он будет распознан как поддомен зоны. Подробнее про SRV-записи в RFC-2782.

Если при подключении к серверу в ответе приходит редирект с кодом ответа 302, то для полученного в редиректе адреса поиск SRV-записей производиться не будет. Ideco Client сразу подключится по адресу, полученному в редиректе.

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

При указании в параметре `target` SRV-записи `.` подключение происходить не будет, и появится сообщение, что сервис недоступен. Этот параметр может настраиваться при регистрации доменного имени или при конфигурации записей для доменного имени.

Алгоритм работы Ideco Client при балансировке

При нажатии кнопки **Подключиться** Ideco Client проверяет адрес сервера, заданный в настройках профиля, и составляет список для подключения, основываясь на следующих правилах:

1. Если адрес сервера является IP-адресом, то сразу происходит подключение Ideco Client по этому адресу. 2. Если адрес сервера является FQDN, то происходит запрос SRV-записей вида `_ideco-client._tcp.<FQDN домена>` для указанного FQDN:

- Если для текущего FQDN есть SRV-записи, то происходит их добавление в список для подключения. Затем происходит сортировка сначала по параметру SRV-записи `priority`, затем при равенстве параметров `priority` у двух и более записей происходит сортировка по параметру `weight`. Подробнее про сортировку `weight` в RFC-2782.
- Если для текущего FQDN нет SRV-записей, то происходит разрешение FQDN в IP-адрес с помощью записи типа A и Ideco Client подключается по этому IP-адресу.

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

Подсказка: При попытке подключения к хостам из списка могут возникнуть циклические редиректы. На Ideco Client есть ограничение в пять редиректов. При шестом редиректе подключение к текущему серверу считается неуспешным.

14.6 Профили устройств

Профили устройств позволяют задать критерии проверки устройств, которые подключаются к NGFW только через *Ideco Client*. Для других сессий авторизации профили не назначаются.

С помощью HIP-профилей реализуется ZTNA (Zero Trust Network Access) - технология обеспечения безопасного доступа к сети, основанная на принципе *нулевого доверия*. ZTNA позволяет контролировать и аутентифицировать устройства пользователей перед предоставлением доступа к ресурсам сети.

Предупреждение: Если подключенное устройство соответствует какому-либо HIP-профилю, за сессией авторизации закрепляется этот профиль, информация об этом отображается в таблице *Авторизованные пользователи*.

Если ни один HIP-профиль в таблице HIP-профилей не совпал с сессией авторизации, то на сессию авторизации назначается специальный HIP-профиль **Устройство без профиля**. Эта информация также отображается в таблице **Авторизованные пользователи**.

Информация, собираемая Ideco Client

- Версия Windows;
- Наличие установленного пакета обновлений;
- Наличие установленного антивируса;
- Наличие актуальной базы антивируса;
- Дата последней проверки антивируса;
- Версия межсетевого экрана и вендор;
- Информация о процессах, запущенных на устройстве;
- Информация о запущенных службах;
- Информация о ключах реестра;
- Добавление устройства в домен.

Критерии проверки, доступные на NGFW

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

HIP-объекты и профили не влияют на правила трафика до момента их использования в правилах **Файрвола**. Чтобы с помощью профилей ограничить или разрешить доступ к ресурсами сети, необходимо:

1. В разделе **Профили устройств -> HIP-объекты** создать HIP-объекты.

2. В разделе **Профили устройств -> HIP-профили** сгруппировать созданные в пункте 1 объекты в профили.

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

Подсказка: Проверка профилей происходит каждые 15 минут.

14.6.1 HIP-объекты

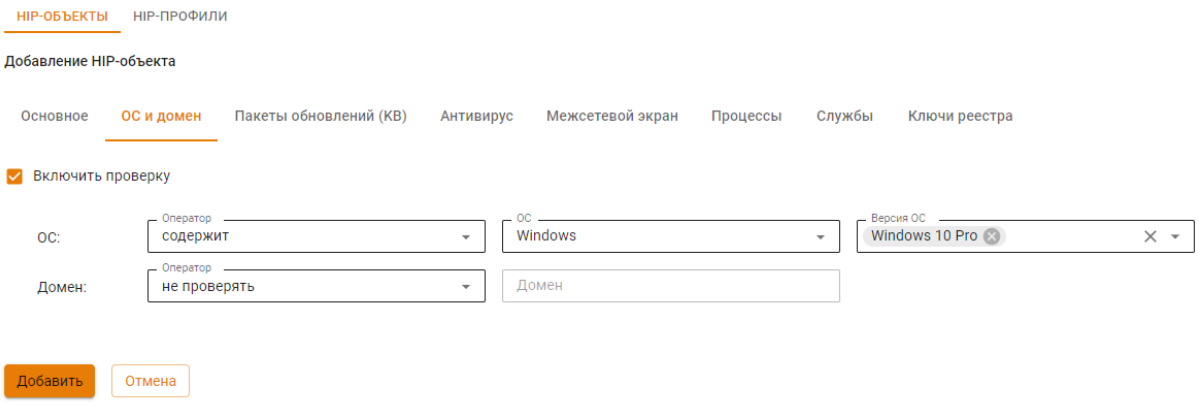
На вкладке создаются объекты, каждый из которых - совокупность критериев проверки устройства. HIP-объекты используются для создания HIP-профиля.

Для создания HIP-объекта выполните действия:

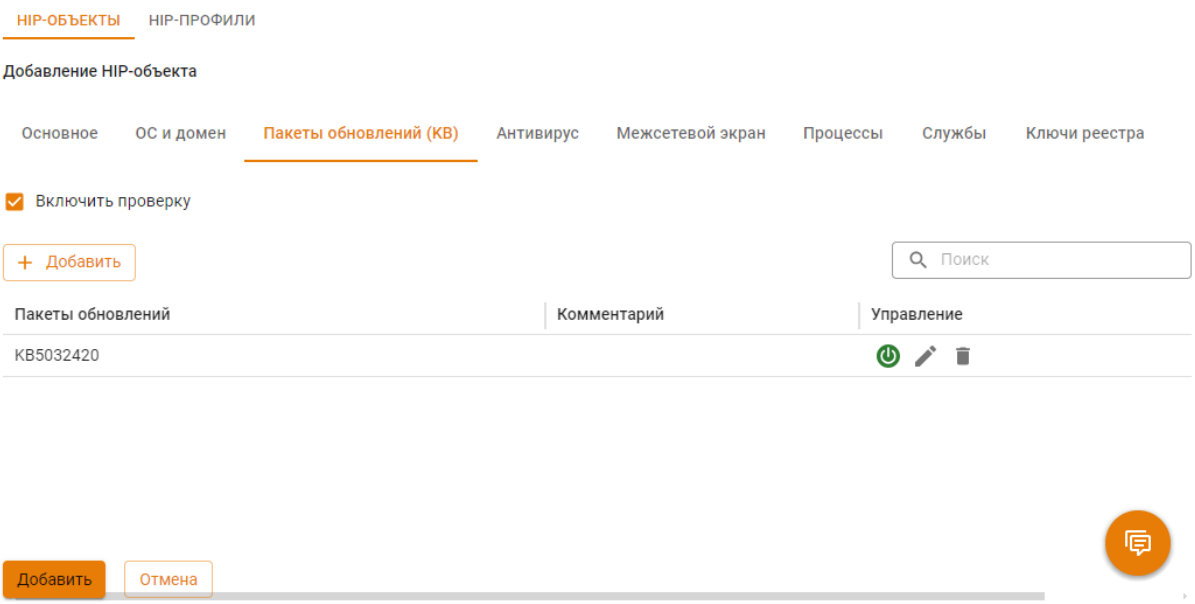
1. Перейдите в раздел **Профили устройств -> HIP-объекты** и нажмите **Добавить**.

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

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



Критерий может не содержать операторов:



4. После этого нажмите **Добавить**.

Подсказка: При создании критерия проверки **Ключи реестра** используйте корневые разделы реестра Windows:

- HKEY_LOCAL_MACHINE;
- HKEY_CURRENT_USER;
- HKEY_CLASSES_ROOT;
- HKEY_USERS;
- HKEY_CURRENT_CONFIG.

Каждый из HIP-объектов возвращает логическое значение. Если критерии HIP-объекта выполнены, то объект возвращает положительный результат.

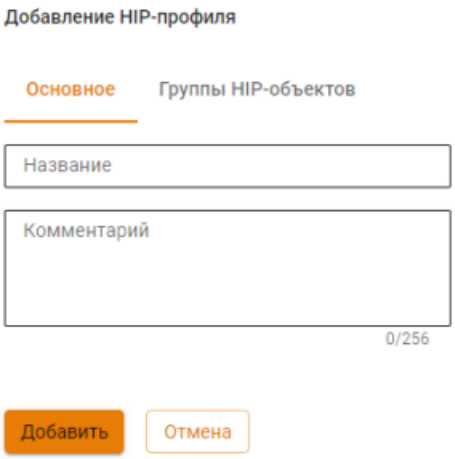
14.6.2 HIP-профили

На вкладке создаются HIP-профили, каждый из которых - совокупность HIP-объектов, сгруппированных с помощью логических операций **И/ИЛИ**. Если при проверке устройства пользователя логическое выражение HIP-профиля возвращает положительный результат, то этот профиль закрепляется за сессией авторизации этого пользователя и отображается в таблице *Авторизованные пользователи*. На одну сессию авторизации может быть назначено несколько профилей при совпадении.

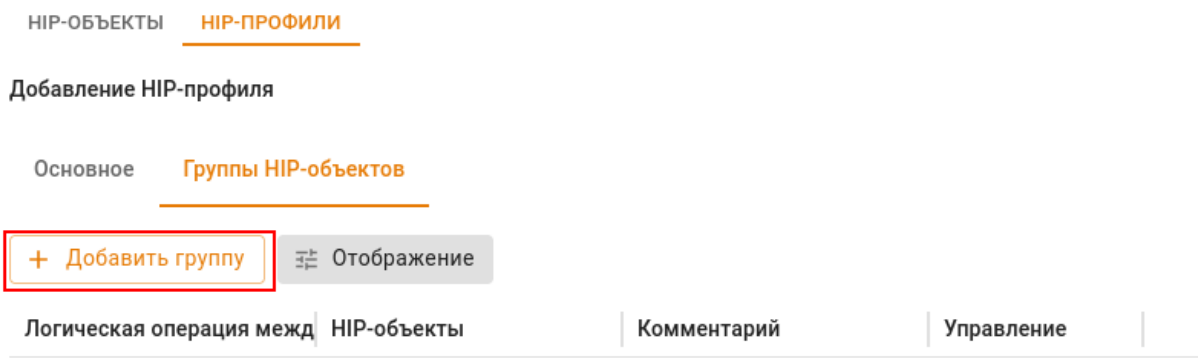
Для создания HIP-профиля выполните действия:

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

2. Введите **Название HIP-профиля**:



3. Перейдите на вкладку **Группы HIP-объектов**, нажмите **Добавить группу**:



4. Выберите HIP-объекты, указав логическую операцию между объектами **И/ИЛИ**:

5. Нажмите **Добавить**.

Подсказка: HIP-профили можно использовать в качестве дополнительного условия в правиле FORWARD **Файрвола**. Правило сработает, если трафик исходит от устройства, которому назначен хотя бы один профиль, указанный в правиле.

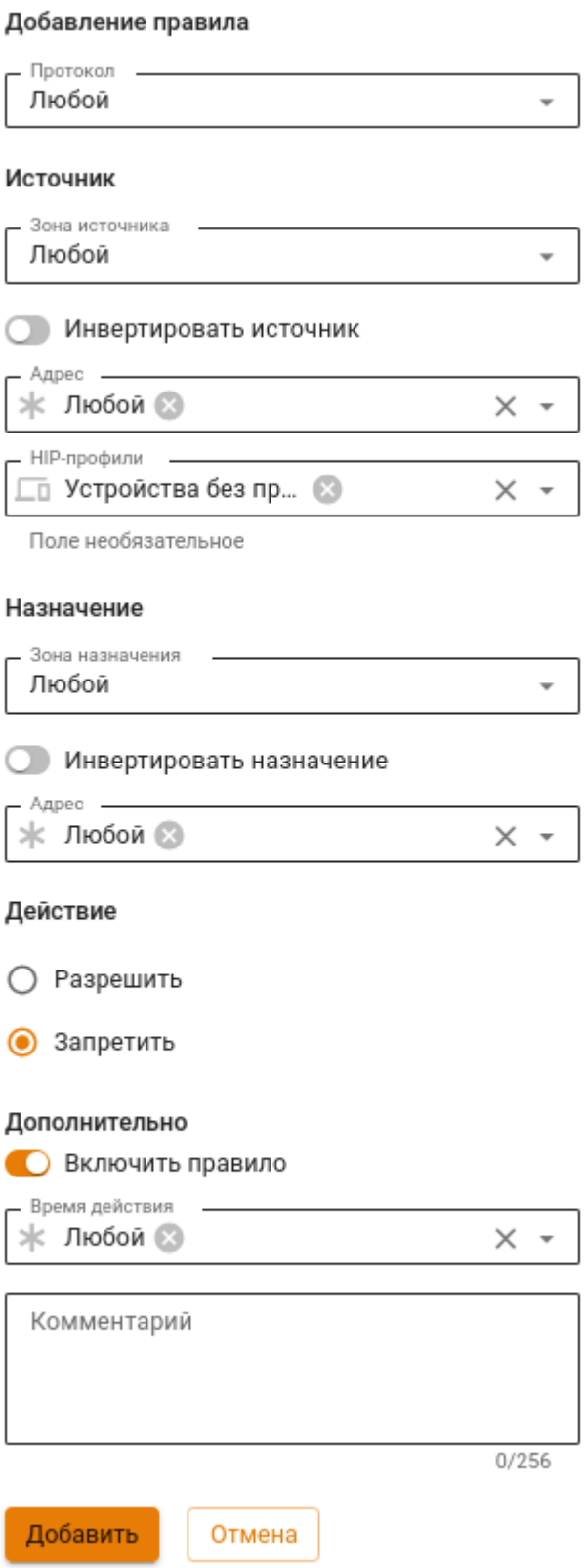
14.6.3 Примеры использования

Запрет доступа к сети устройствам без профиля:

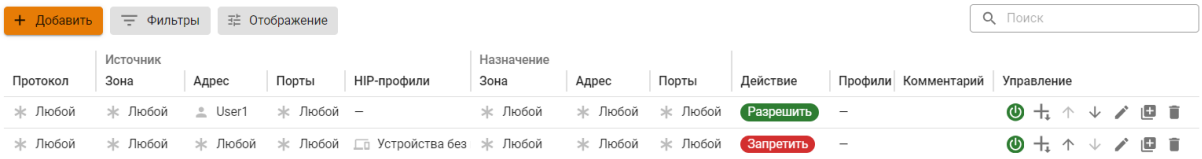
Устройствам, которые не прошли проверку на соответствие ни одному из созданных HIP-профилей, назначается специальный HIP-профиль **Устройство без профиля**. Доступ таких устройств к сети можно ограничить правилом **Файрвола**. Для этого:

1. Перейдем в раздел **Правила трафика -> Файрвол -> FORWARD**.

2. Создадим и включим правило вида:



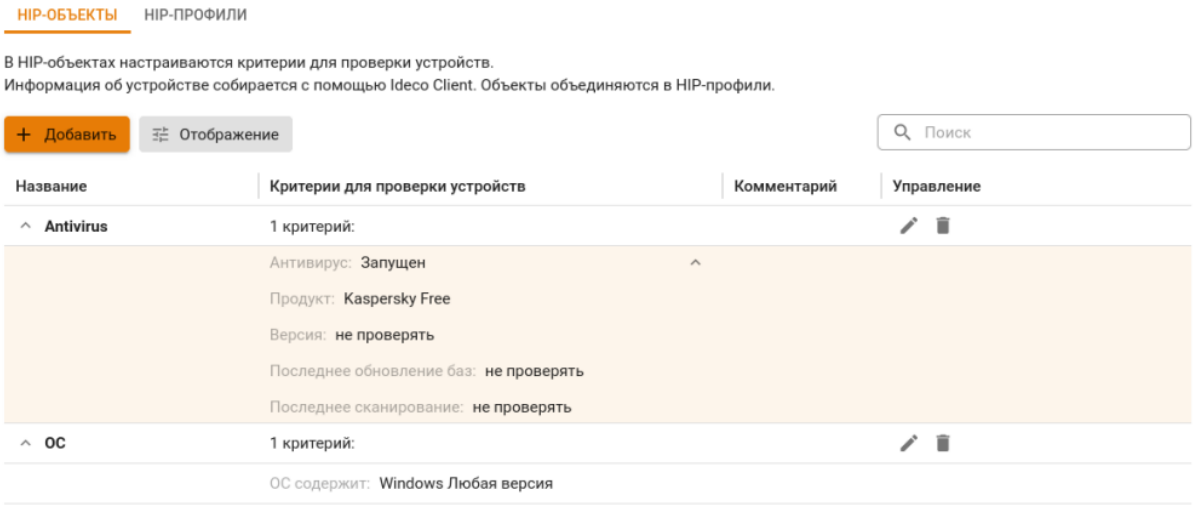
Важно! Если в таблице правил **Файрвола** выше запрещающего правило находится другое правило, которому соответствует трафик одного или нескольких устройств без профиля (например, правило для пользователя или группы пользователей без указания HIP-профиля), то к трафику будет применено правило, расположенное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



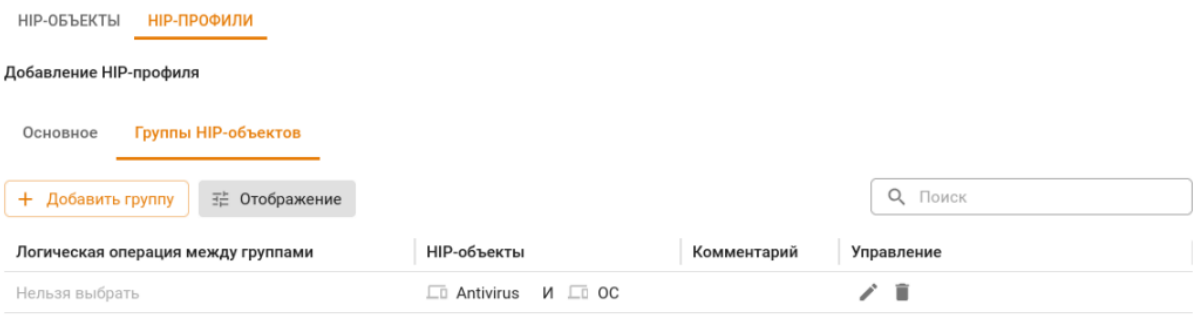
Ограничение доступа устройств к сети:

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

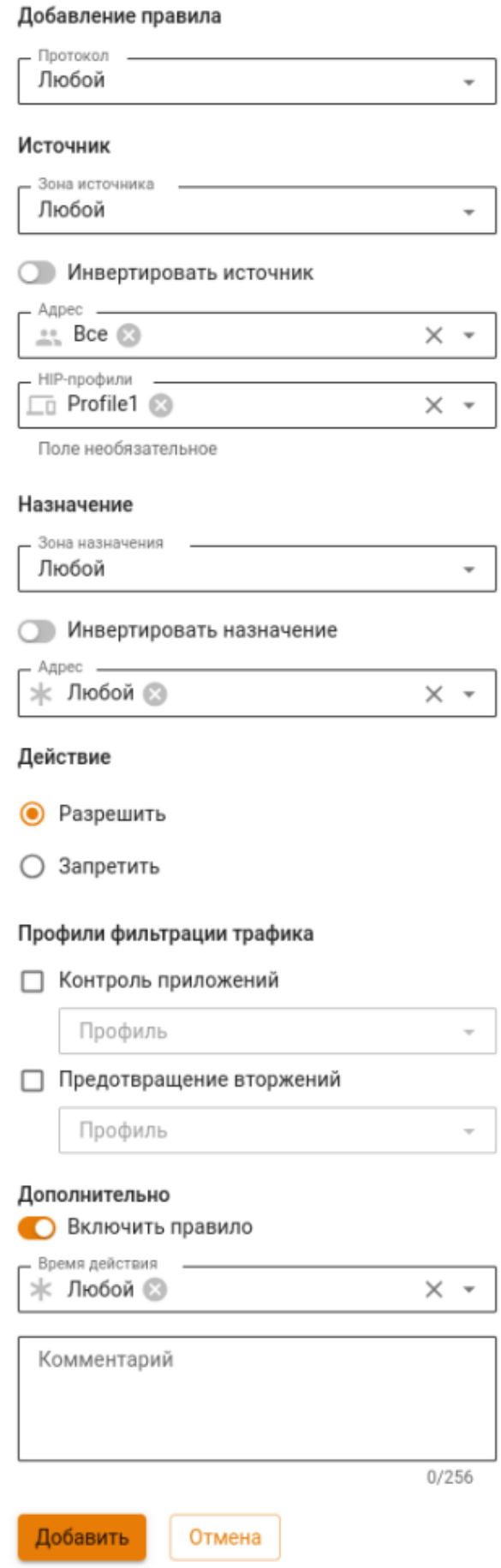
1. Перейдите в раздел **Пользователи -> Профили устройств -> HIP-объекты** и создайте требуемые HIP-объекты:



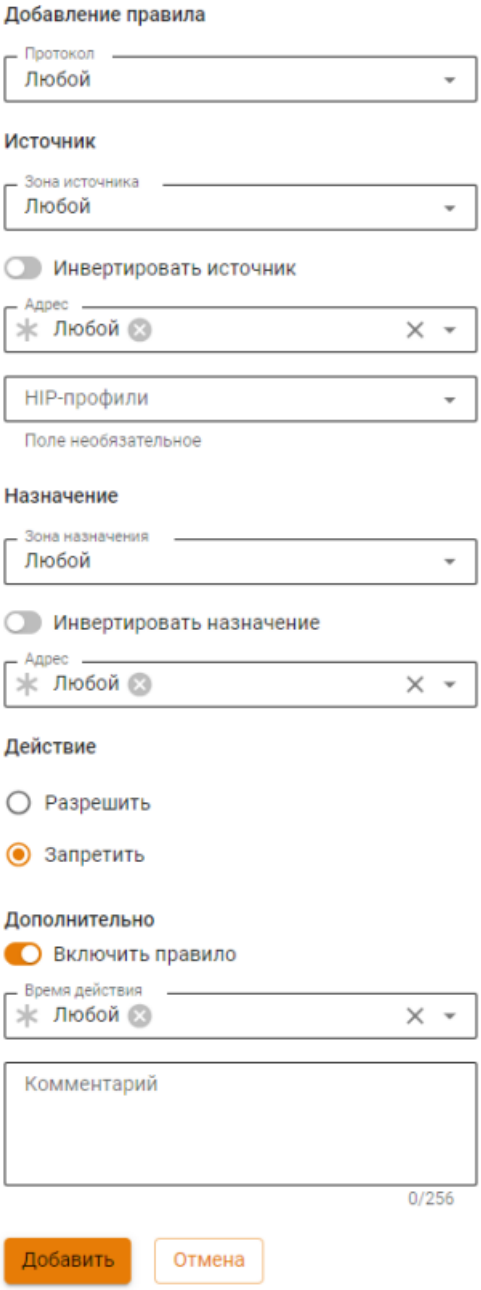
2. Перейдите на вкладку **HIP-профили** и создайте профиль с созданными ранее HIP-объектами:



3. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD**, создайте и включите правило, разрешающее доступ к сети всем пользователям, чьи устройства соответствуют профилю `Profile1`:


Добавление правила
Протокол
Любой
Источник
Зона источника
Любой
Инвертировать источник
Адрес
Все
HIP-профили
Profile1
Поле необязательное
Назначение
Зона назначения
Любой
Инвертировать назначение
Адрес
Любой
Действие
Разрешить
Запретить
Профили фильтрации трафика
Контроль приложений
Профиль
Предотвращение вторжений
Профиль
Дополнительно
Включить правило
Время действия
Любой
Комментарий
0/256
Добавить
Отмена

4. Ниже создайте и включите правило, запрещающее весь трафик:



В результате трафик всех пользователей, чьи устройства соответствуют HIP-профилю `Profile1`, подпадет под разрешающее правило. Остальной трафик подпадет под запрещающее правило.

14.7 Интеграция с Active Directory/Samba DC

Подсказка: Название службы раздела **Active Directory/Samba DC**: `ideco-ad-backend`; `ideco-ad-log-collector@<имя домена>`.
Список служб для других разделов доступен по *ссылке*.

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

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

14.7.1 Поддерживаемые контроллеры домена:

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

14.7.2 Особенности интеграции с несколькими контроллерами домена

- Из дерева контроллеров домена в Ideco NGFW импортируются данные только того контроллера, для которого был запущен импорт пользователей;
- При импорте пользователей из разных доменов необходимо убедиться, что учетные записи не имеют одинаковых логинов. В противном случае система выдаст сообщение об ошибке;
- При SSO-авторизации и первом открытии браузера пользователю будет предложен выбор домена для аутентификации. Выбор будет сохранен с помощью cookie и использован при следующей авторизации. Если требуется изменить домен, очистите cookie (для локального IP-адреса Ideco NGFW).

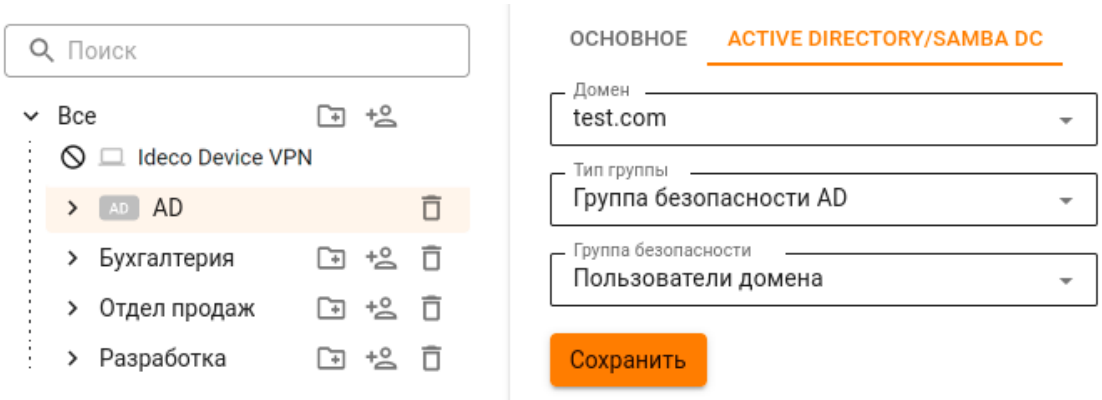
14.7.3 Настройка учетных записей и групп безопасности в качестве объектов фильтрации

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

- *Файрвол*;
- *Контент-фильтр*;
- *Ограничение скорости*.

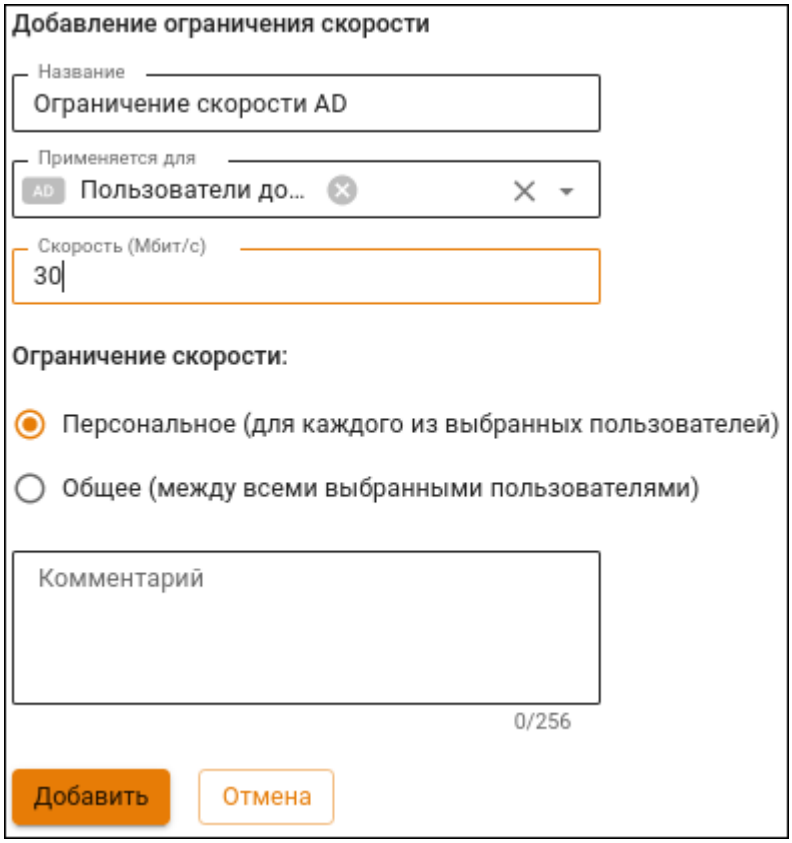
Пример использования учетной записи, импортированной из Active Directory, для ограничения скорости:

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



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

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



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

14.7.4 Ввод сервера в домен

Подсказка: Перед вводом в домен убедитесь, что время на контроллере домена и Ideco NGFW совпадает.

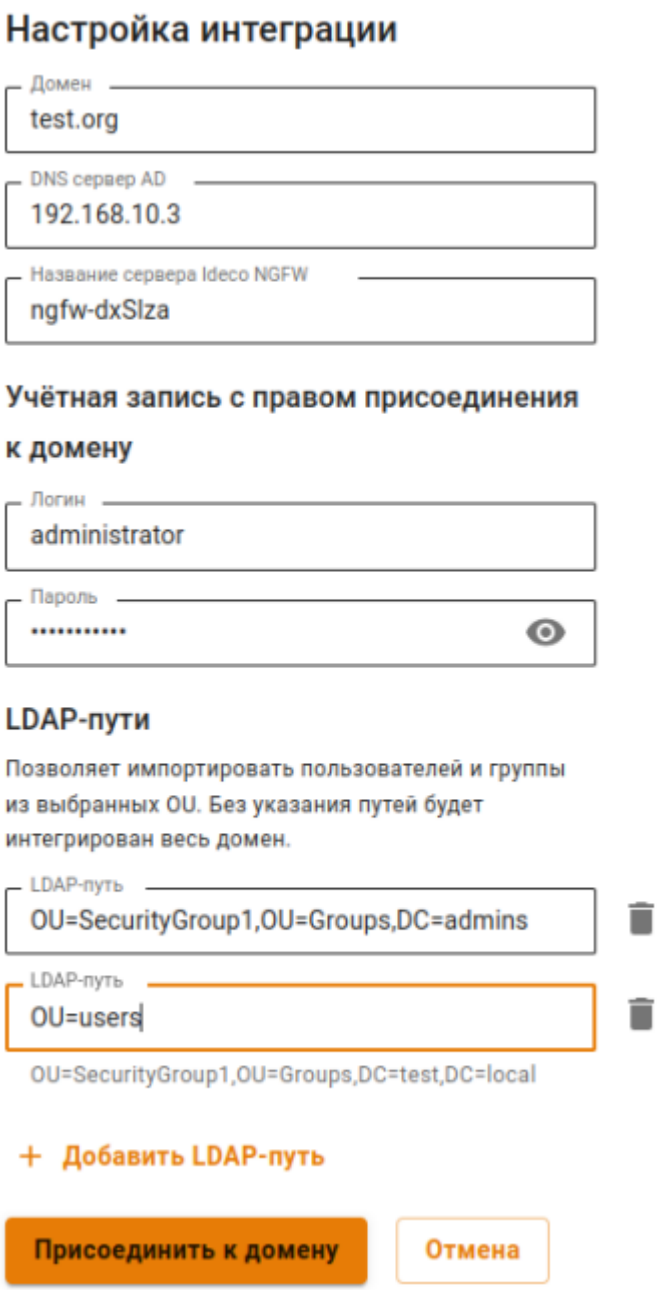
Предупреждение: Хотябы один контроллер домена должен находиться в локальной сети Ideco NGFW или быть доступен через локальный интерфейс с помощью настроенной маршрутизации.

Для ввода сервера в домен выполните действия:

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

2. Нажмите **Добавить**.

3. Заполните поля:



- **Домен** - введите полное наименование домена, длина которого не должна превышать 64 символа. Например: `mydomain.example`;
- **DNS-сервер AD** - введите адрес сервера, обладающий ролью DNS-сервера в контроллере домена, доступный с локального интерфейса Ideco NGFW;
- **Название сервера Ideco NGFW** - введите имя компьютера, под которым Ideco NGFW будет введен в домен;
- **Учетная запись с правом присоединения к домену** - введите учетную 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** - укажите LDAP-пути для импорта пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет импортировать только нужные группы пользователей, чтобы избежать импорта всего дерева пользователей AD.

Процесс присоединения к домену после нажатия одноименной кнопки может занять до одной минуты. Особенности использования NGFW с несколькими контроллерами домена описаны в *статье*.

Предупреждение: При выводе Ideco NGFW из домена удаляются все пользователи и группы, импортированные из него.

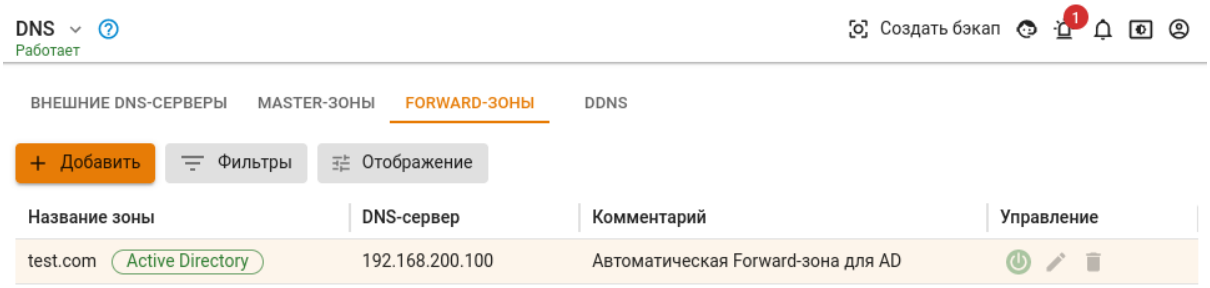
Настройка DNS для разрешения имен локального домена

Подсказка: В Ideco NGFW Forward-зона DNS создается автоматически при вводе сервера в домен. Создавайте ее вручную, только если по ошибке удалили данную зону из настроек DNS-сервера или если не получилось присоединить сервер к домену.

Для корректной работы синхронизации и авторизации пользователей на Ideco NGFW настройте разрешение имен локального домена в настройках DNS:

1. Пропишите Forward-зону в настройках DNS.

2. Пропишите DNS-серверы для Forward-зоны (адреса основного и резервного контроллера домена).



В примере:

- **ad2.loc** - имя домена;
- **192.168.10.3** - IP-адрес DNS-сервера.

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

14.7.5 Аутентификация пользователей AD/Samba DC

[Ссылка на видеоинструкцию по настройке аутентификации пользователей Active Directory с Ideco NGFW (https://rutube.ru/video/590d482c7e412deb0dcfbe945e1448e4/)

Настройка авторизации пользователей

Для пользователей, импортированных из Active Directory, доступны все типы авторизации.

Подсказка: Авторизацию через журнал безопасности Active Directory рекомендуется использовать совместно с SSO-авторизацией.

Для пользователей, импортированных из SambaDC, доступны **все типы авторизации**, кроме **авторизации через журнал безопасности**.

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

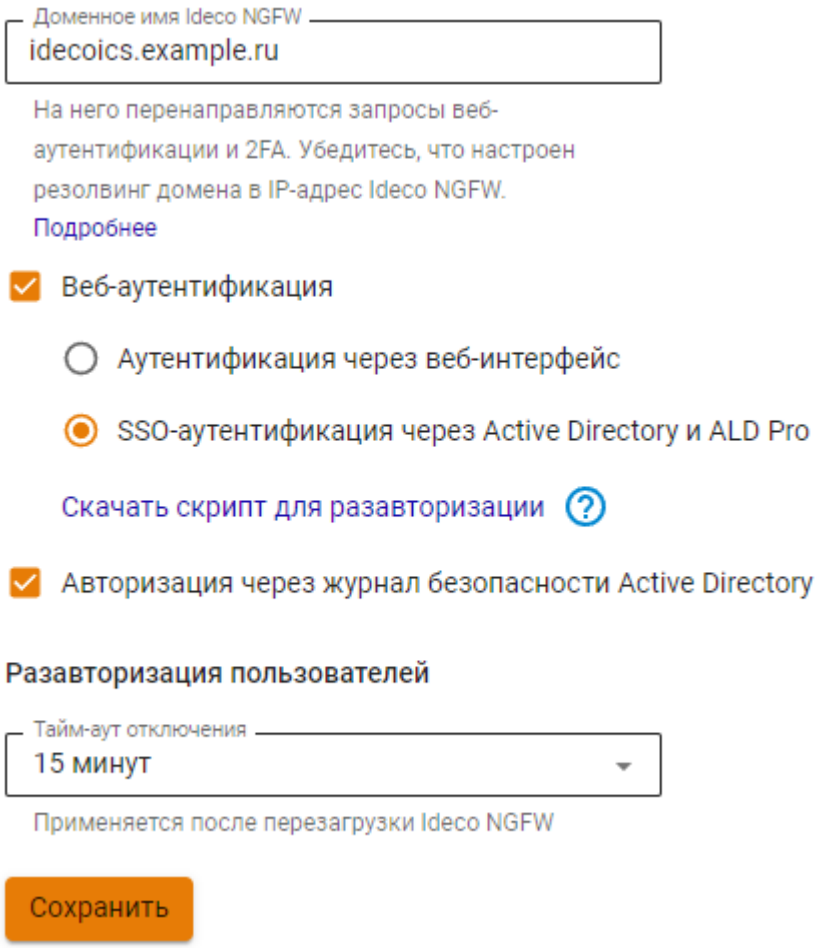
Подсказка: Если у домена, в который введен **NGFW**, настроено доверие с другим доменом, то пользователи доверенного домена смогут авторизоваться на **NGFW** при выполнении условий:

- Для аутентификации пользователей домена используется **SSO-аутентификация**;
- Пользователь доверенного домена должен быть в локальной группе AD на контроллере домена, и эта группа должна быть импортирована на NGFW.

После авторизации пользователи доверенного домена будут добавлены в группу AD **Пользователи из доверенных доменов** в дереве пользователей NGFW.

Настройка Ideco NGFW

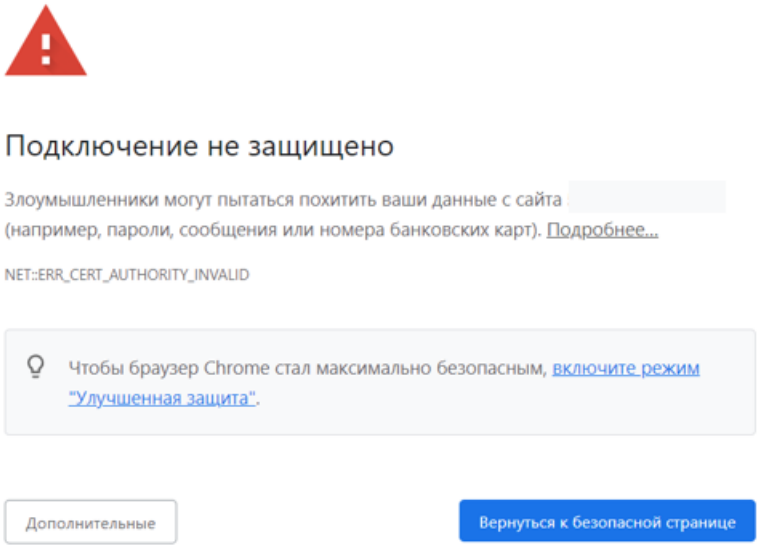
Для включения **SSO-аутентификации** и **Авторизации через журнал безопасности Active Directory** перейдите на вкладку **Пользователи -> Авторизация -> Основное** и заполните поля:



- Для корректной работы SSO-аутентификации используйте **Доменное имя Ideco NGFW** длиной не более 15 символов.
- Включите настройку **Веб-аутентификация** и выберите **SSO-аутентификация через Active Directory и ALD Pro**.
- Включите настройку **Авторизации через журнал безопасности Active Directory**.
- Установите тайм-аут разавторизации пользователей. Значение по умолчанию - 15 минут. Диапазон доступных значений - от 10 минут до 1 дня.

После внесенных изменений нажмите кнопку **Сохранить**.

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



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

Настройка сервера Microsoft Active Directory

При авторизации через журнал безопасности контроллера домена AD пользователи будут аутентифицированы при попытке выхода в интернет. Автоматической аутентификации без прохождения трафика через NGFW не происходит, т. к. используется конкурентная политика аутентификации.

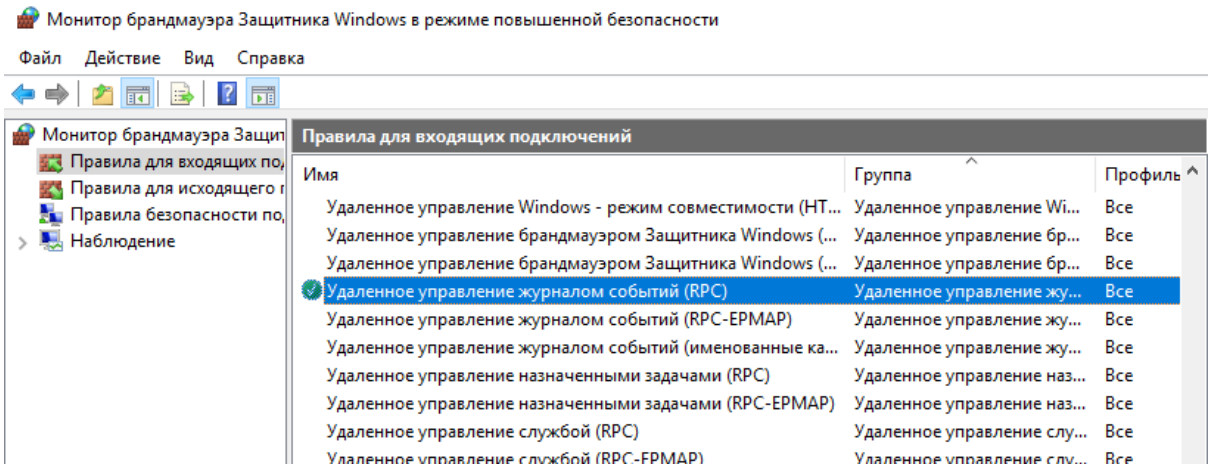
Подсказка: Особенности работы авторизации через журнал безопасности Active Directory:

- При включении (перезагрузке) компьютера в домене AD происходит автоматическая аутентификация под последним аутентифицированным пользователем.
- При смене пользователя компьютера в домене AD служба аутентификации `ideco-auth-backend` не будет аутентифицировать нового пользователя. Для аутентификации пользователя перезагрузите службу `ideco-auth-backend`.

Используйте Ideco Client совместно с SSO-аутентификацией на Ideco NGFW.

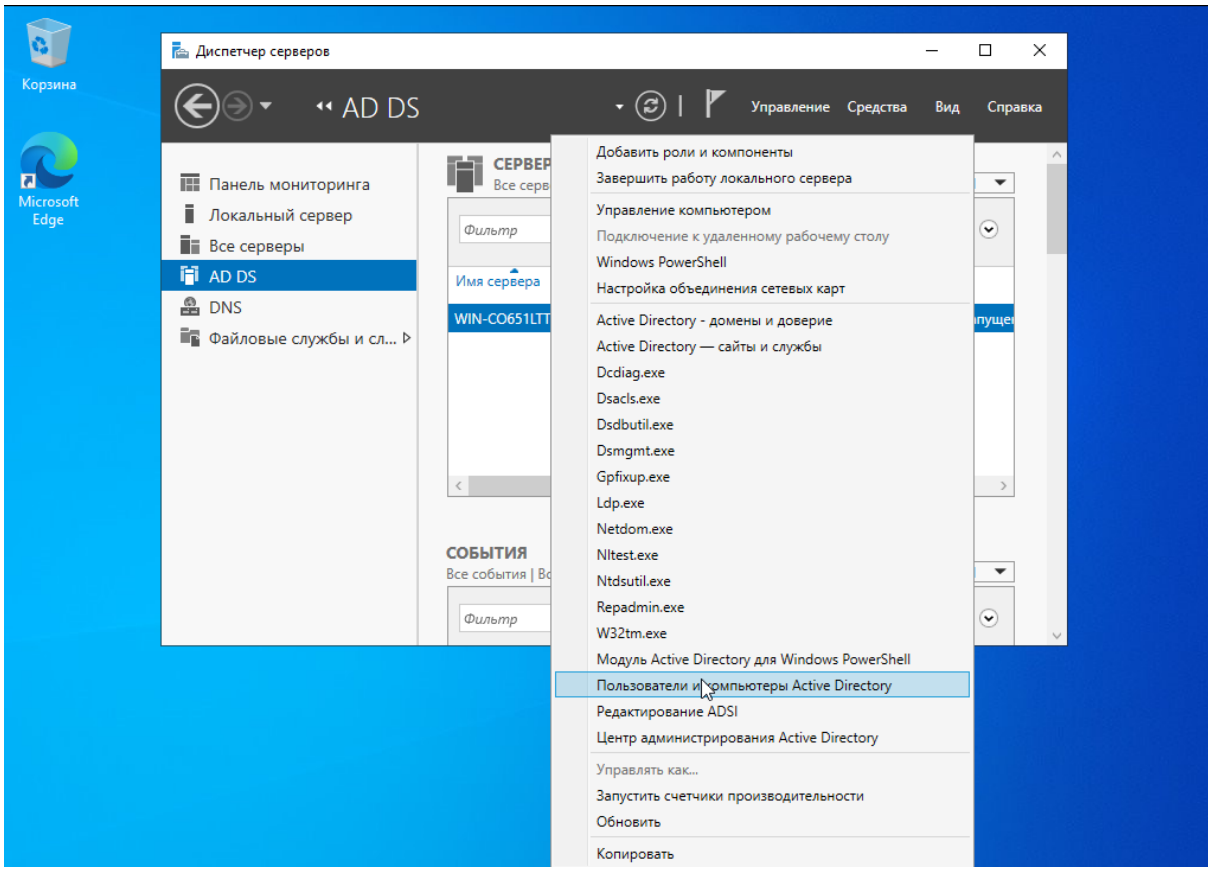
Для работы авторизации через журнал безопасности выполните настройку контроллера домена:

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

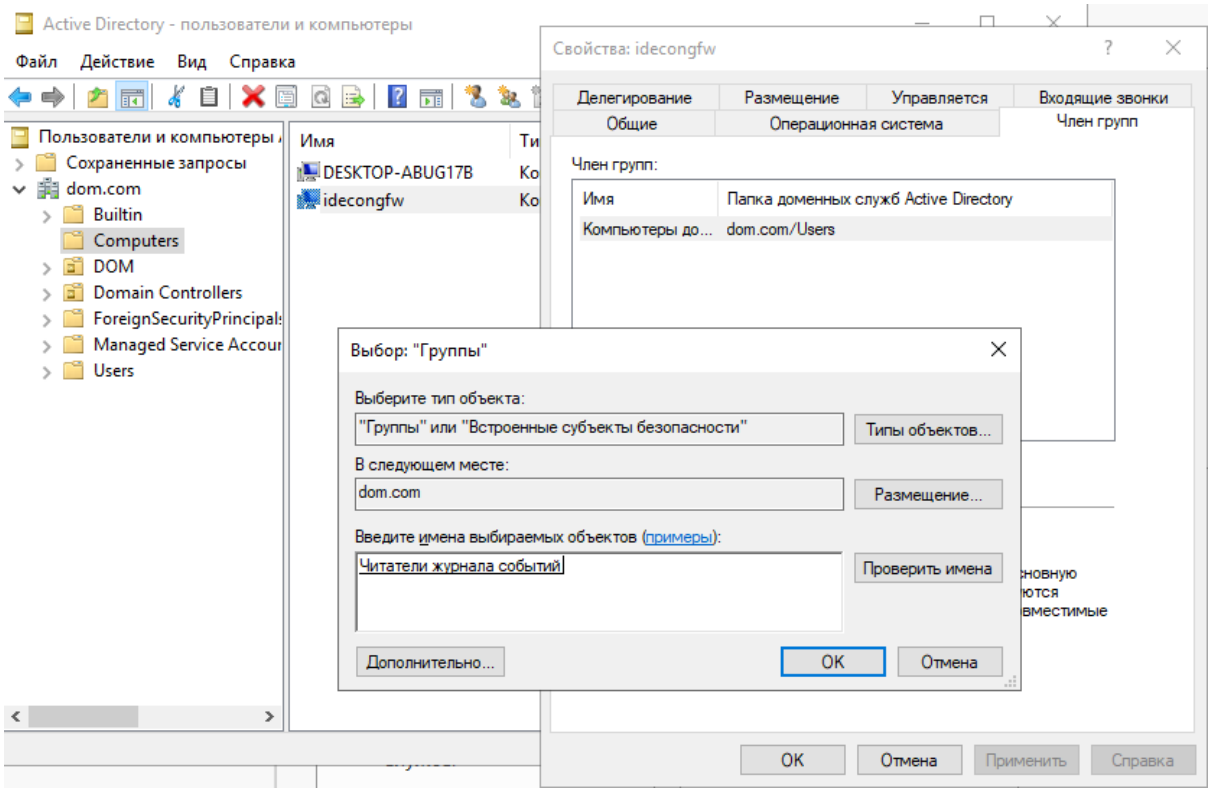


2. Добавьте Ideco NGFW в группу безопасности **Читатели журнала событий (Event Log Readers)**. Чтобы это сделать:

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



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



3. Перезапустите службу **Авторизация через журнал безопасности Active Directory** на Ideco NGFW. Для этого отключите эту опцию, а затем снова включите.

При изменении стандартной политики безопасности контроллеров домена выполните действия:

Англоязычная версия:

1. Откройте **Group policy management**.

2. Выберите **Forest: Доменное имя AD -> Domains -> Доменное имя AD**.

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

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

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

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

7. Нажмите **Apply** и **OK**.

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

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

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

Русскоязычная версия:

1. Откройте **Управление групповой политикой**.

2. Выберите **Лес: Доменное имя AD -> Домены -> Доменное имя AD**.

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

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

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

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

7. Нажмите **Применить** и **OK**.

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

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

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

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

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

Настройка клиентских машин для веб-аутентификации (SSO или NTLM)

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

Внимание: Обязательно используйте настройки веб-аутентификации, т. к. в некоторых случаях будет необходима аутентификация пользователей через браузер (даже при авторизации через журнал безопасности).

Причины:

- Логи NTLM обычно содержат только имя пользователя, IP-адрес и время входа и не содержат всей информации, необходимой для полноценной авторизации: группы безопасности, права доступа и другие атрибуты пользователя;
- Любые проблемы с журналом, такие как повреждение, потеря данных или задержки в записи, могут привести к проблемам с авторизацией;
- Авторизация только на основе логов может быть менее безопасной, так как логи могут быть подделаны или изменены злоумышленниками;
- Логи могут быть записаны с задержкой, и трудно гарантировать, что все данные актуальны и согласованы в любой момент времени;
- Авторизация на основе логов может потребовать сложной логики для обработки и анализа логов, что может увеличить вероятность ошибок и затруднить поддержку;
- Использование только логов может не обеспечить полную интеграцию с Active Directory и привести к ограниченным возможностям управления и настройки прав доступа.

Для настройки аутентификации через веб-браузер выполните следующие действия:

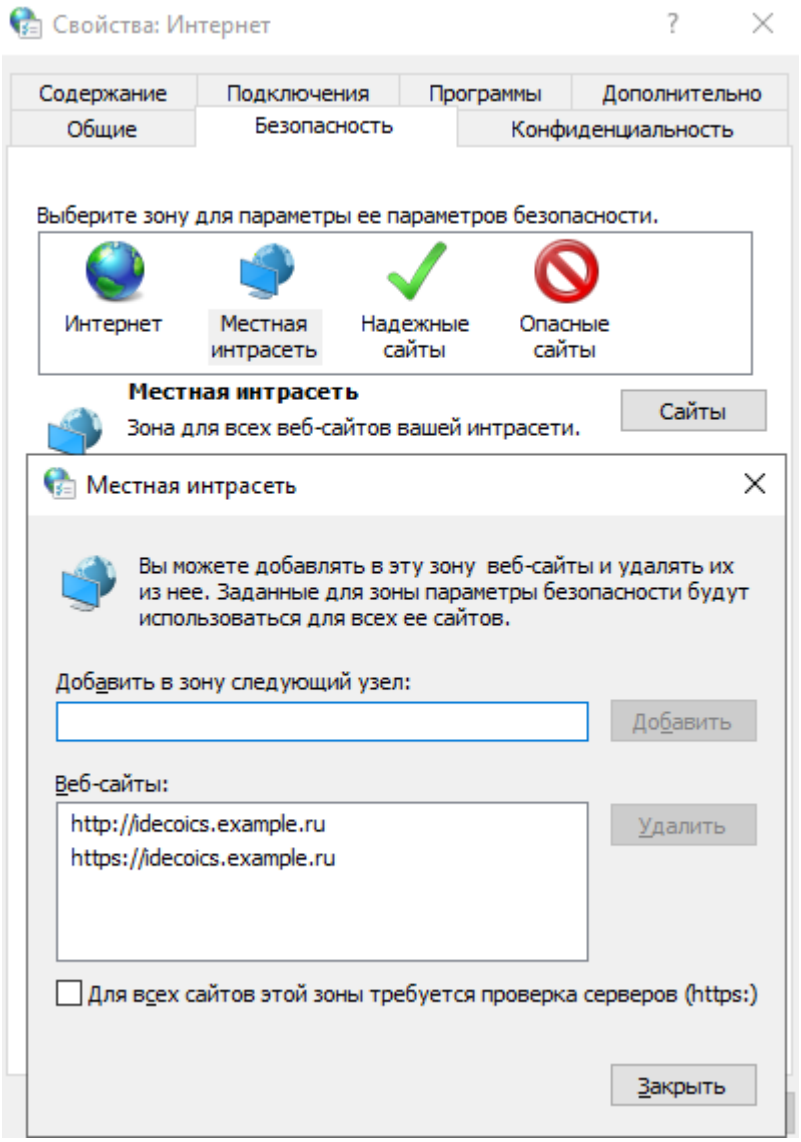
1. В поиск введите **Изменение параметров временных файлов Интернета**.

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

3. Выберите **Местная интрасеть -> Сайты**.

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

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



Для применения настройки ко всем пользователям на клиентской машине выполните действия:

1. Откройте **Редактор локальной групповой политики**. Это можно сделать, нажав клавиши **Win + R** и введя в появившемся окне команду gpedit.msc.

2. Перейдите по пути:

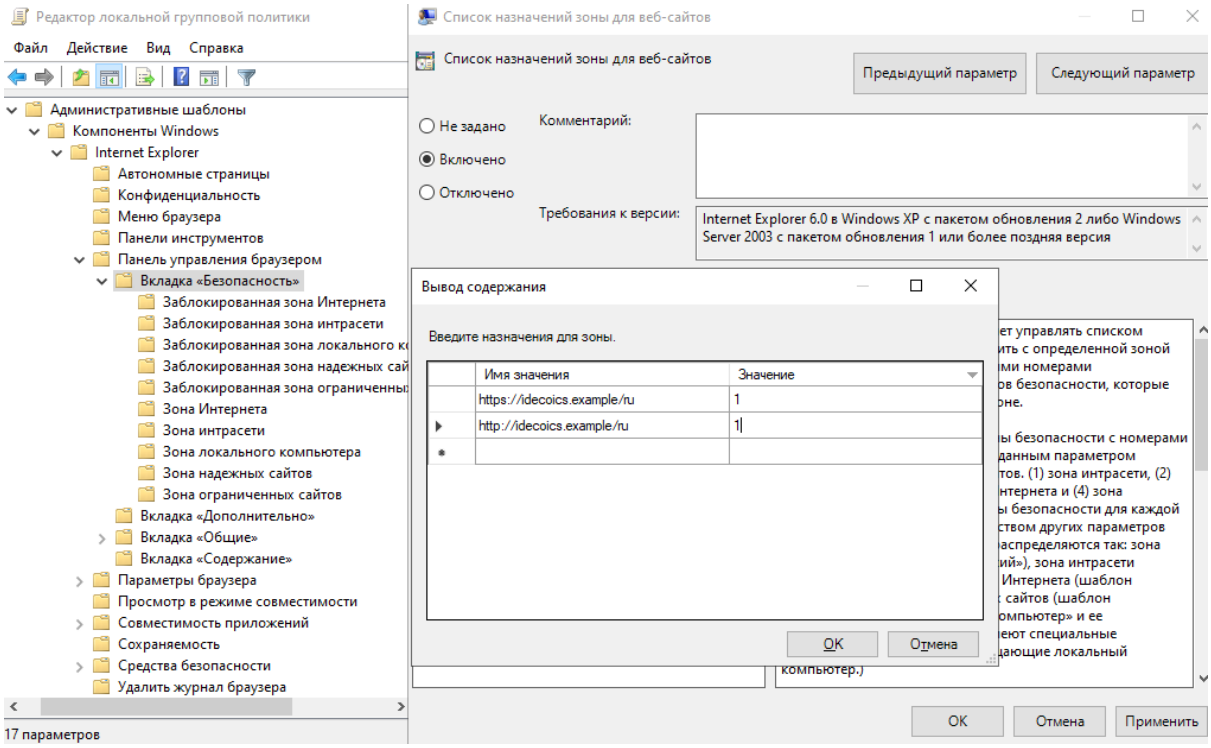
Англоязычная версия:

Local Group Policy Editor -> User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Site to Zone Assignment List.

Русскоязычная версия:

Политика «Локальный компьютер» -> Конфигурация пользователя -> Административные шаблоны -> Компоненты Windows -> Internet Explorer -> Панель управления браузером -> Вкладка «Безопасность» -> Список назначений зоны для веб-сайтов.

3. Введите назначение зоны для DNS-имени Ideco NGFW (в примере idecoics.example.ru) со значением 1 (интрасеть). Укажите два назначения для схем работы по http и https:



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

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

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

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

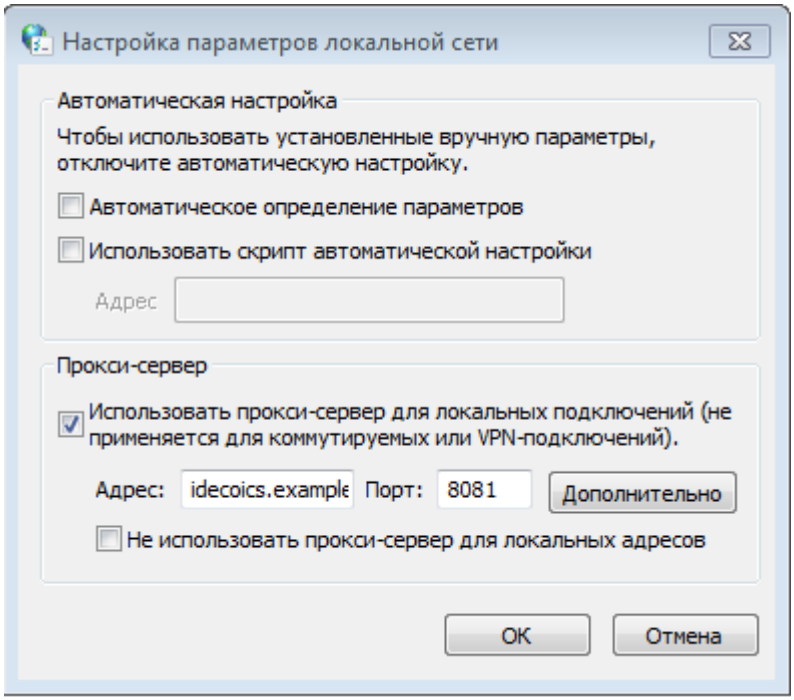
Способы аутентификации импортированных пользователей:

- **Через Ideco Agent** - подходит для аутентификации пользователей терминальных серверов (с использованием Remote Desktop IP Virtualization на терминальном сервере);
- **Авторизация по IP-адресу** - подходит для пользователей с фиксированным IP-адресом. IP-адреса на NGFW необходимо прописать вручную каждому пользователю;
- **Авторизация по VPN** - подходит для аутентификации пользователей удаленных сетей.

Настройка аутентификации пользователей при прямых подключениях к прокси-серверу

Настройка прозрачной аутентификации пользователей при прямых подключениях к прокси-серверу аналогична настройке прозрачной **SSO-аутентификации**.
Единственная особенность - указание в качестве адреса прокси-сервера **DNS-имени Ideco NGFW**.

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



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

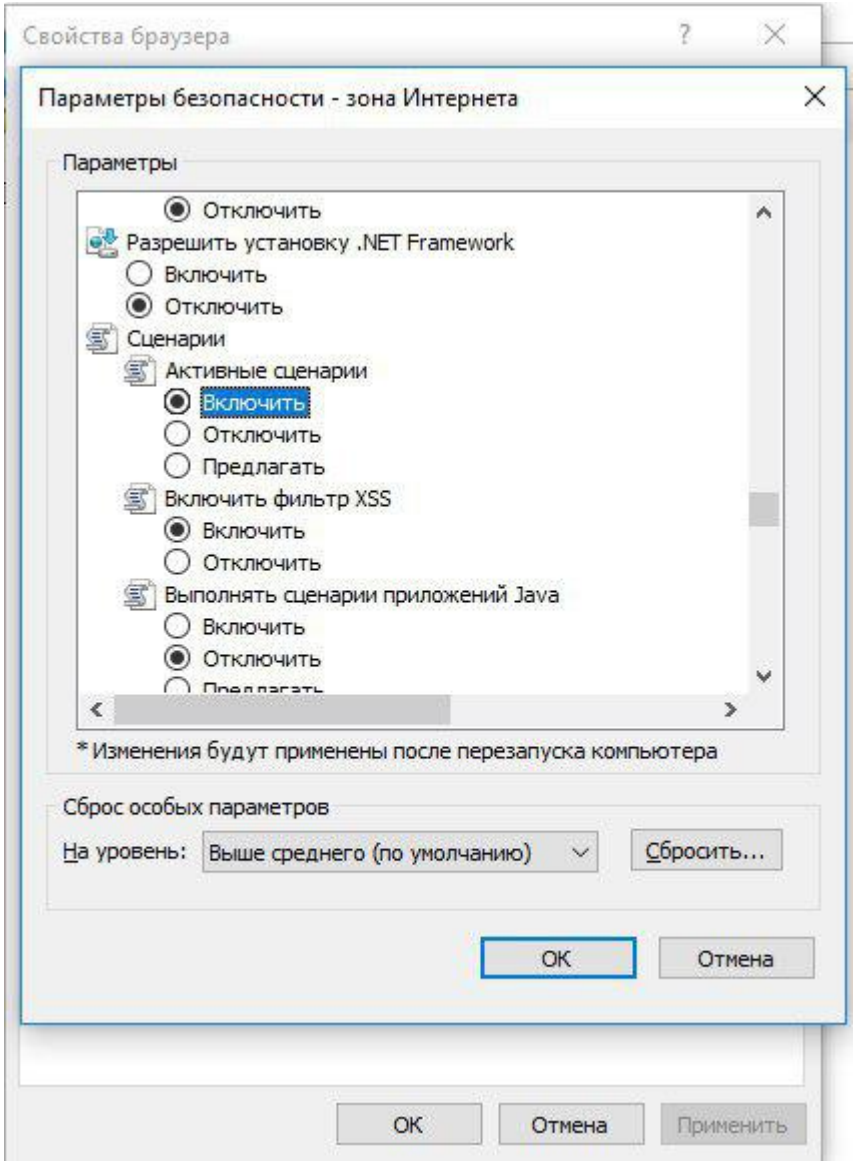
Для аутентификации компьютеров, которые **не находятся в домене**, под доменным пользовательским аккаунтом на странице настроек браузера **Mozilla Firefox** (введите *about:config* в адресной строке) укажите следующие параметры:

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

Не отключайте эти опции для компьютеров, входящих в домен, т. к. в таком случае будет использоваться устаревший метод авторизации по NTLM.

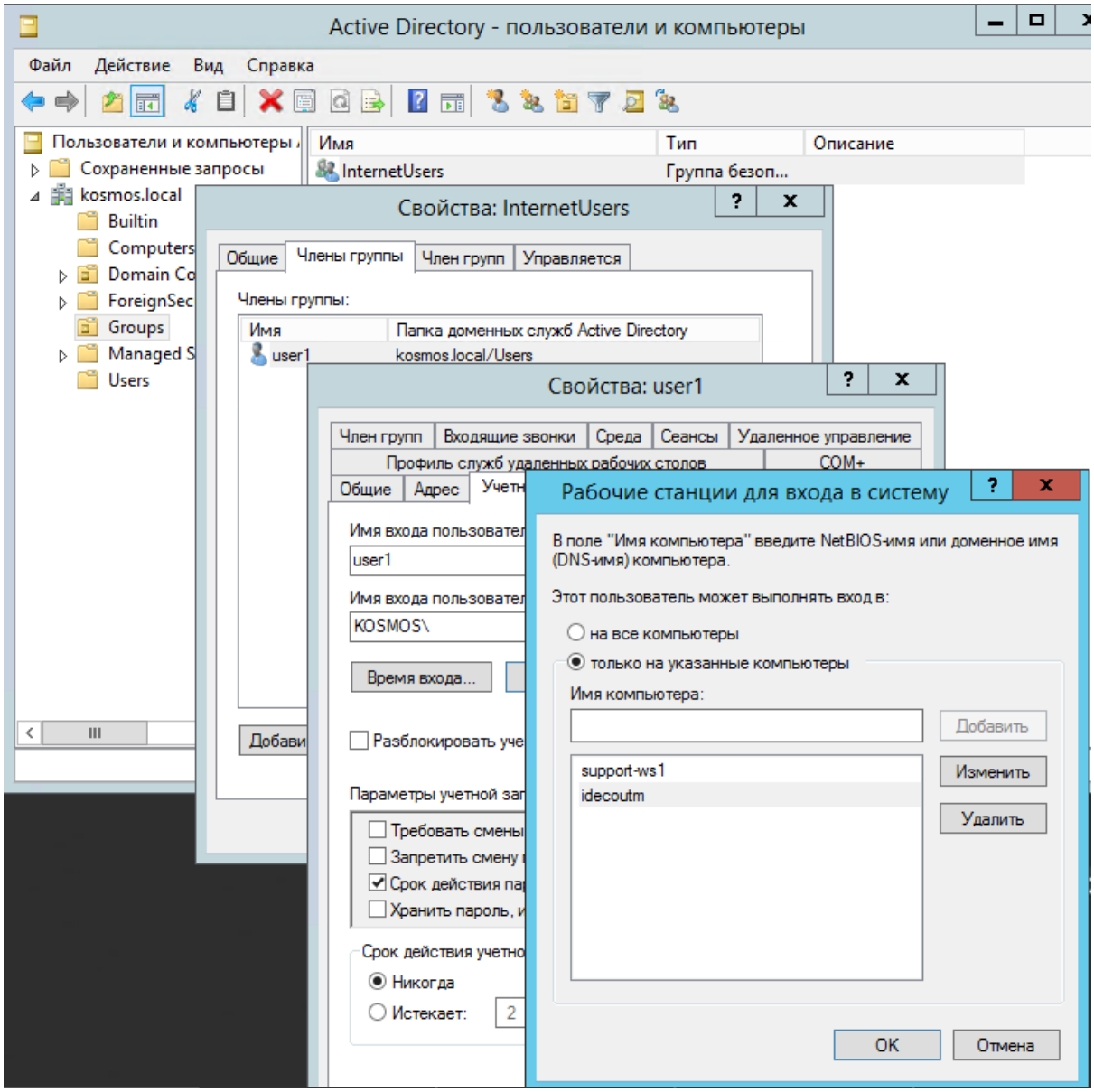
Возможные проблемы:

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



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

Пример такой настройки представлен на скриншоте ниже:



14.7.6 Скрипты автоматической разавторизации

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

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

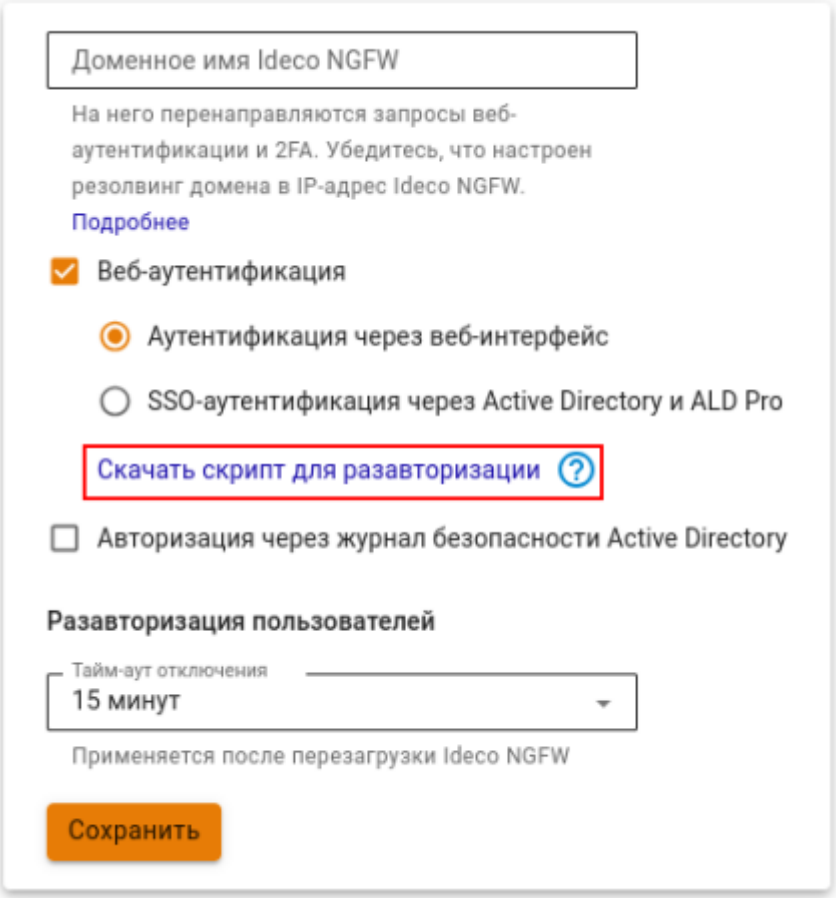
Подсказка: Для работы скрипта выполните все настройки политик безопасности домена и браузера, описанные в статье *Авторизация пользователей*.

Для авторизации по SSO используйте *Ideco Client*.

Разавторизация пользователя

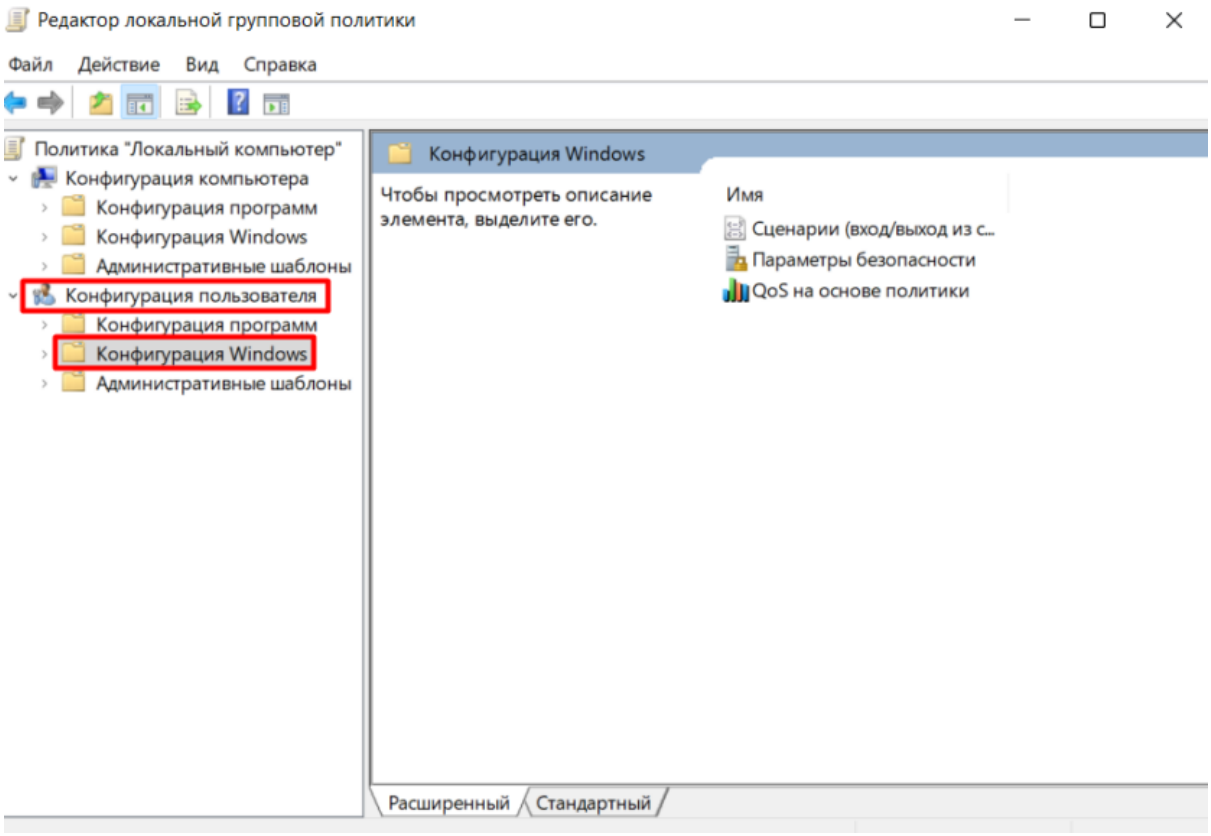
Подсказка: Чтобы скрипт разавторизации работал корректно, установите на компьютеры пользователей корневой сертификат сервера Ideco NGFW и сделайте его доверенным. Это можно сделать как локально, так и через групповые политики домена, следуя *инструкции*.

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



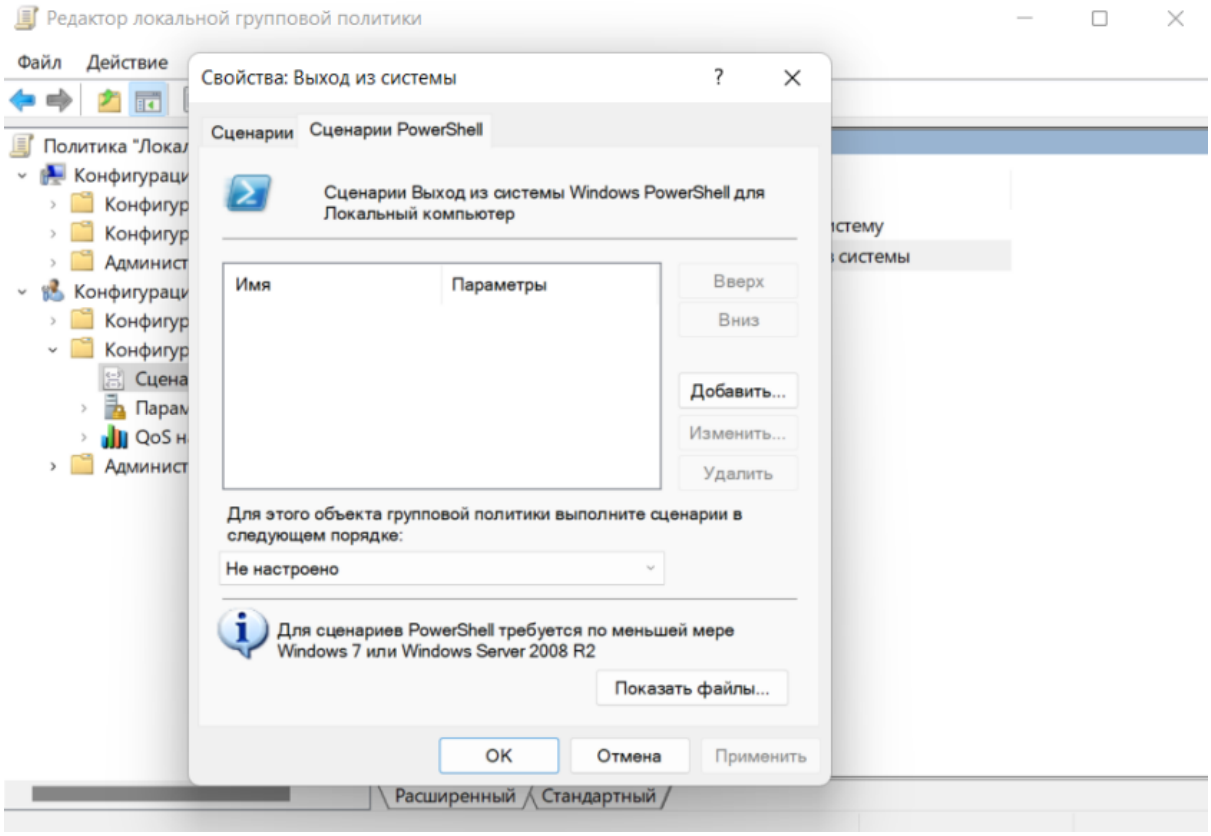
2. Откройте групповые политики (gpedit.msc) от имени администратора на устройстве пользователя.

3. Перейдите в **Конфигурации пользователя -> Конфигурации Windows**:

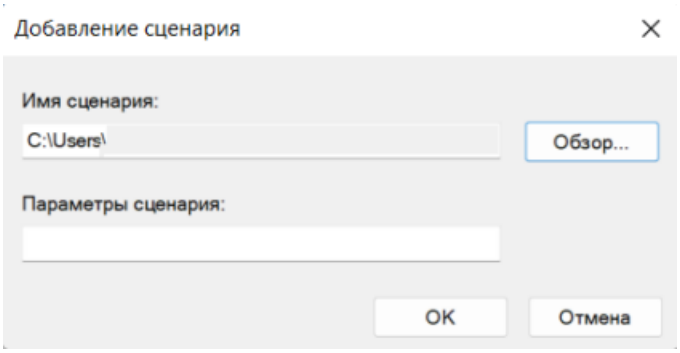


4. Нажмите **Сценарии (вход/выход из системы)**.

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



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

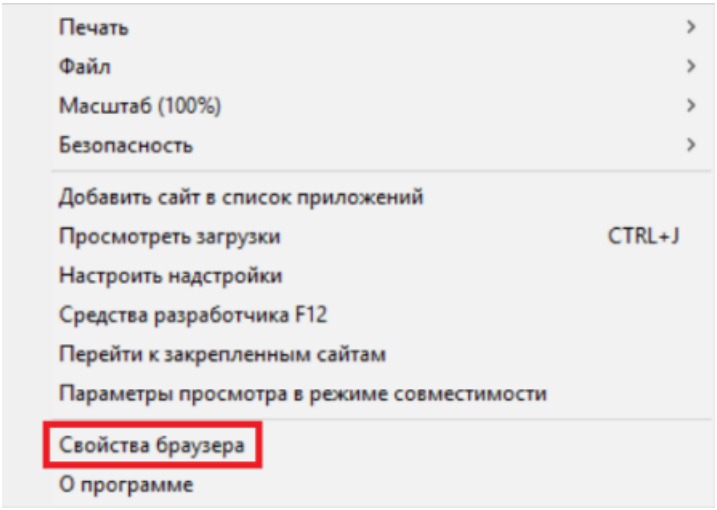


7. Откройте командную строку и обновите групповые политики, введя команду `gpupdate /force`.

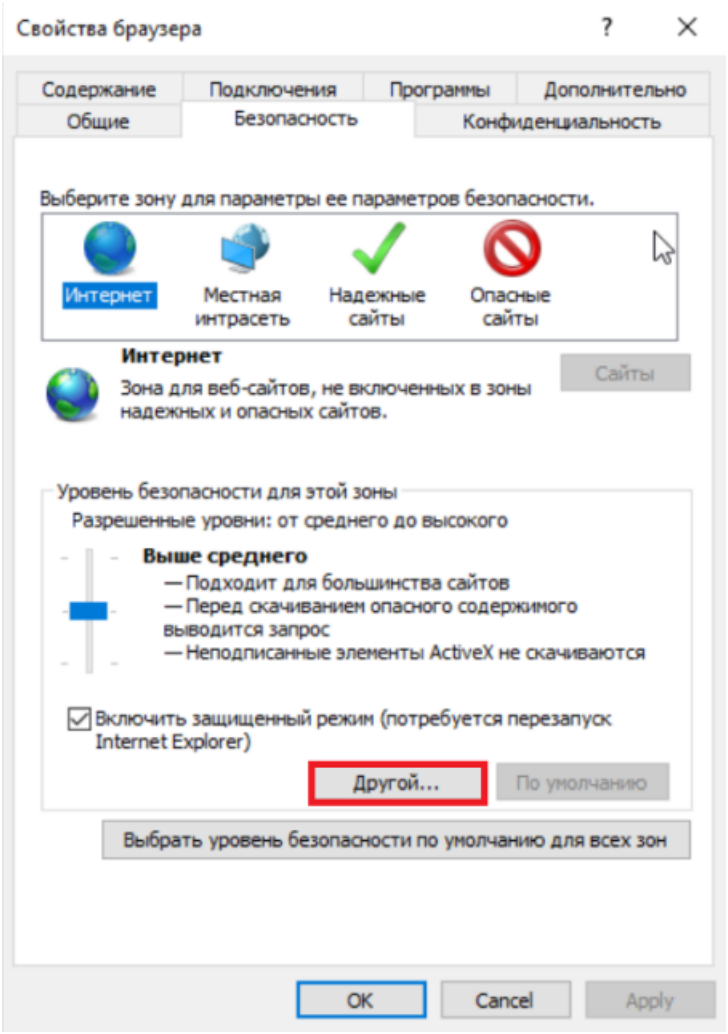
Если в вашем браузере появляется окно с текстом **Для получения доступа требуется аутентификация** и авторизация происходит только при ручном переходе по ссылке, включите JavaScript. Ниже представлены настройки для разных браузеров:

Internet Explorer:

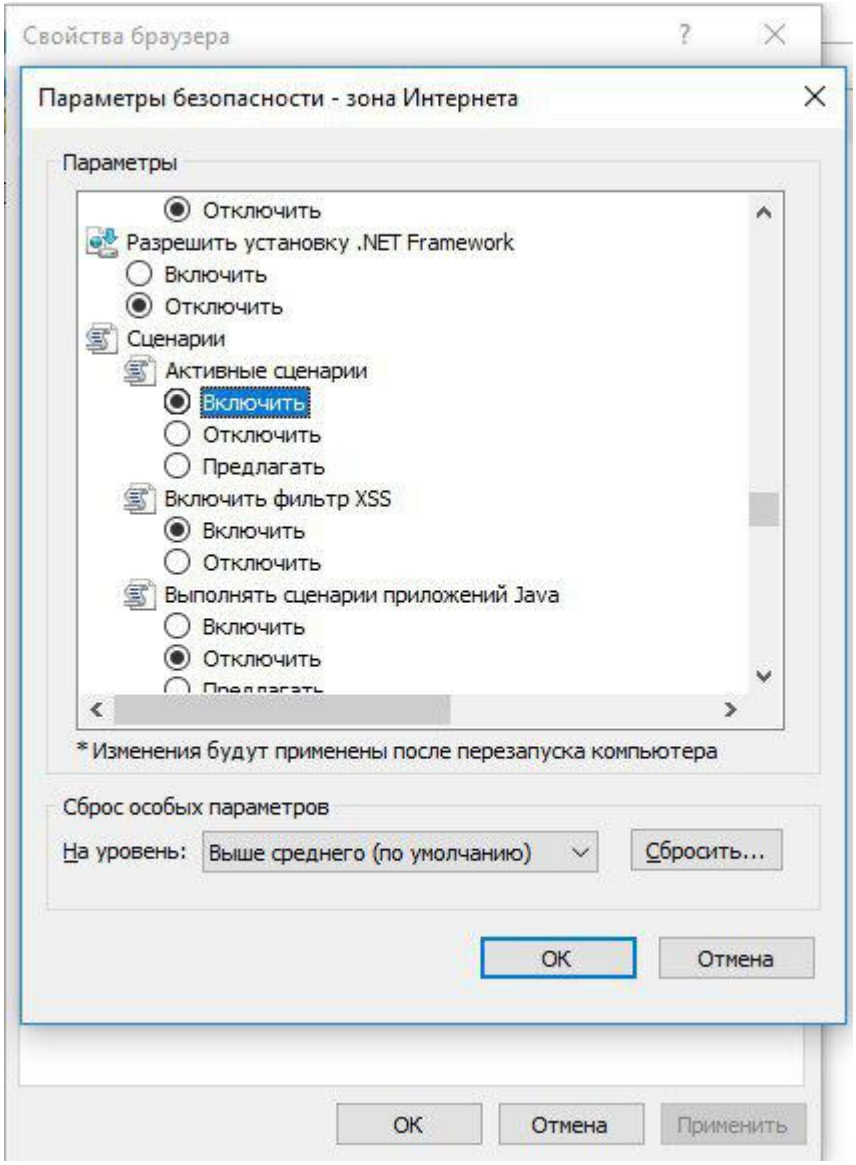
1. В правом верхнем углу браузера нажмите на кнопку **Сервис** в виде шестерни или комбинацию клавиш Alt+X. В выпадающем меню выберите **Свойства браузера**:



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

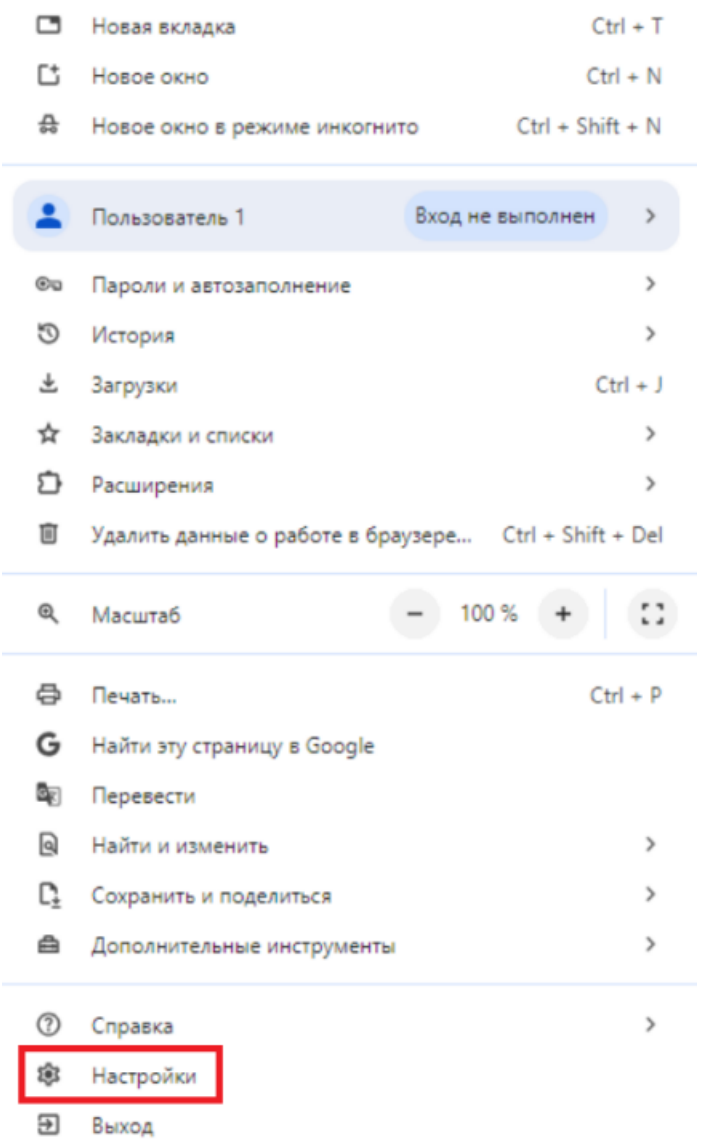


3. В окне **Параметры** переключите параметр **Активные сценарии** в значение **Включить**:

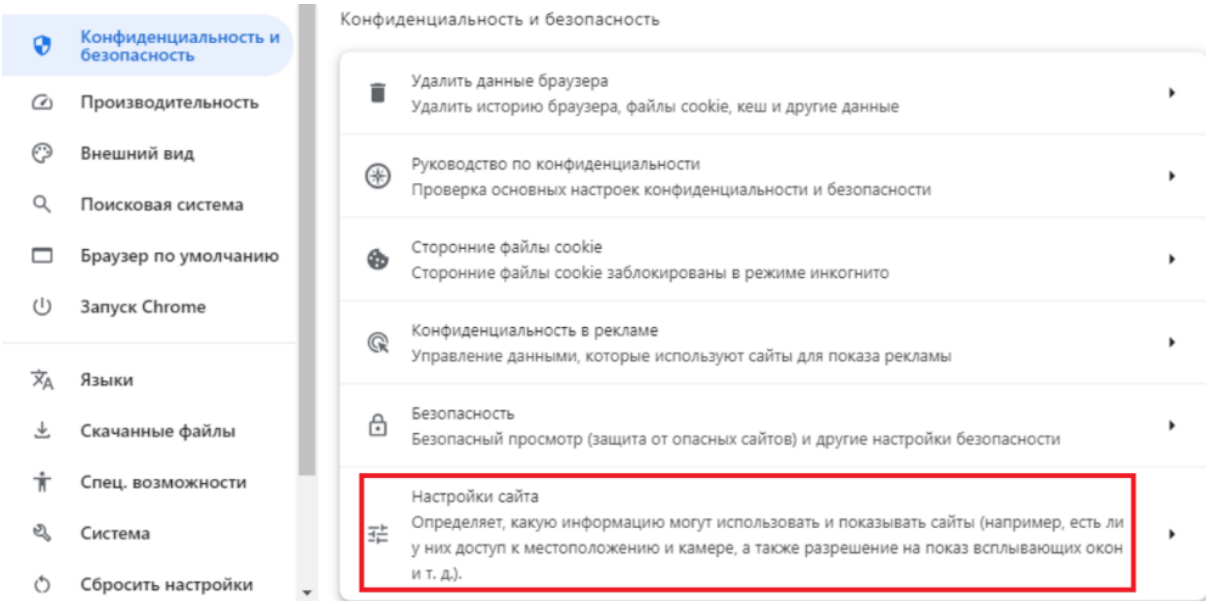


Google Chrome:

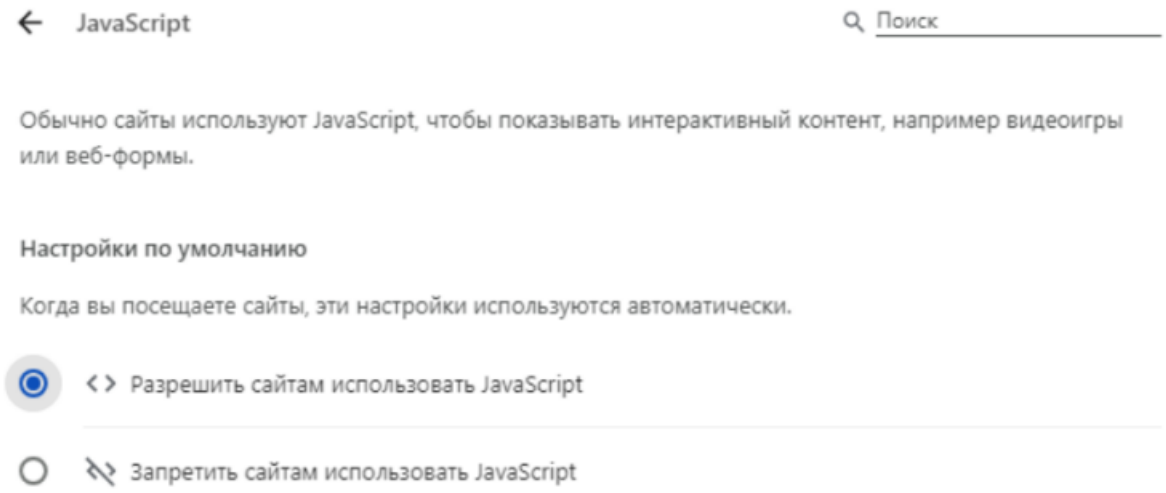
1. В правом верхнем углу браузера нажмите на кнопку с тремя точками и выберите **Настройки** в выпадающем меню:



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

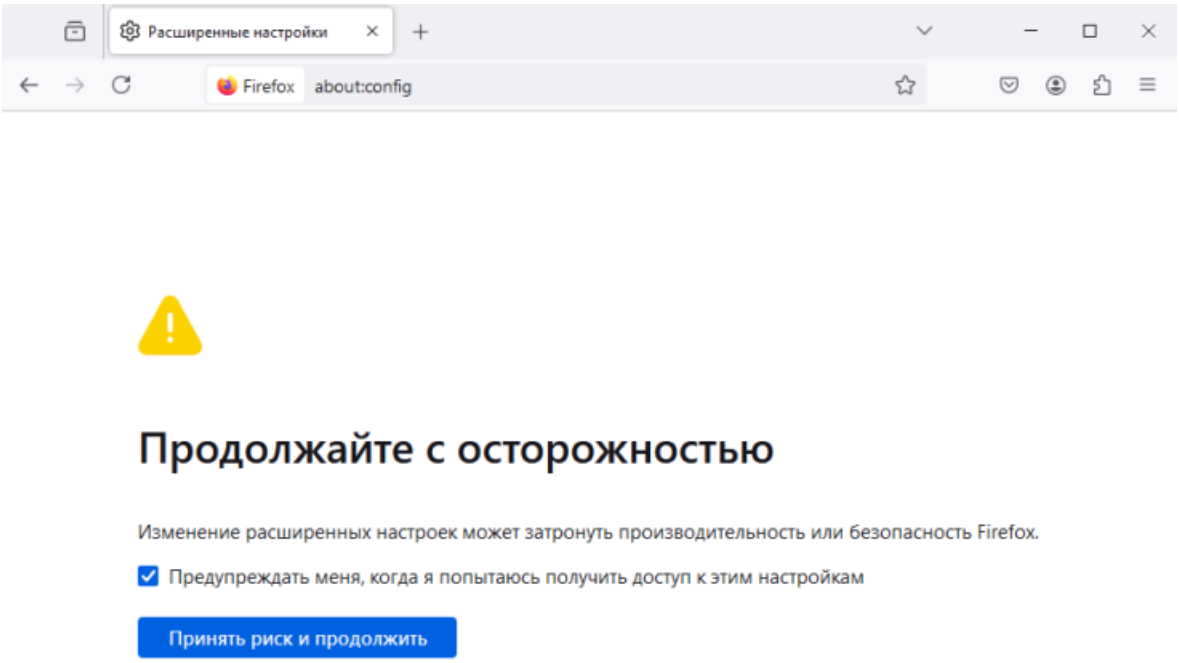


3. В настройках **JavaScript** разрешите сайтам использовать JavaScript:

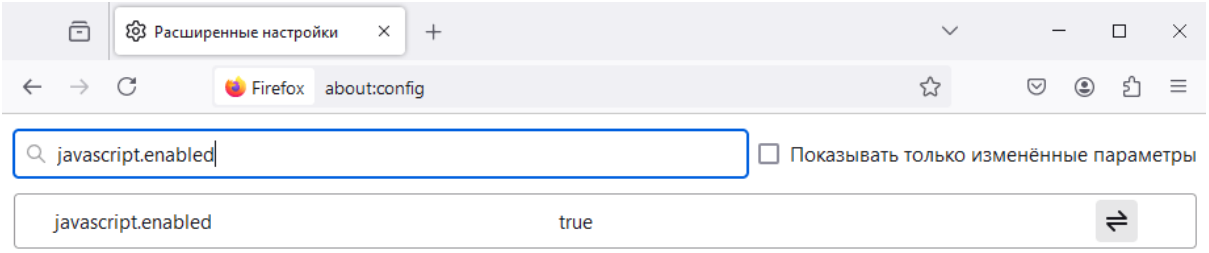


Firefox:

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



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



3. Обновите страницу в браузере.

14.7.7 Импорт пользователей

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

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

Импорт учетных записей из LDAP-каталога

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

Для импорта пользователей выполните действия:

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

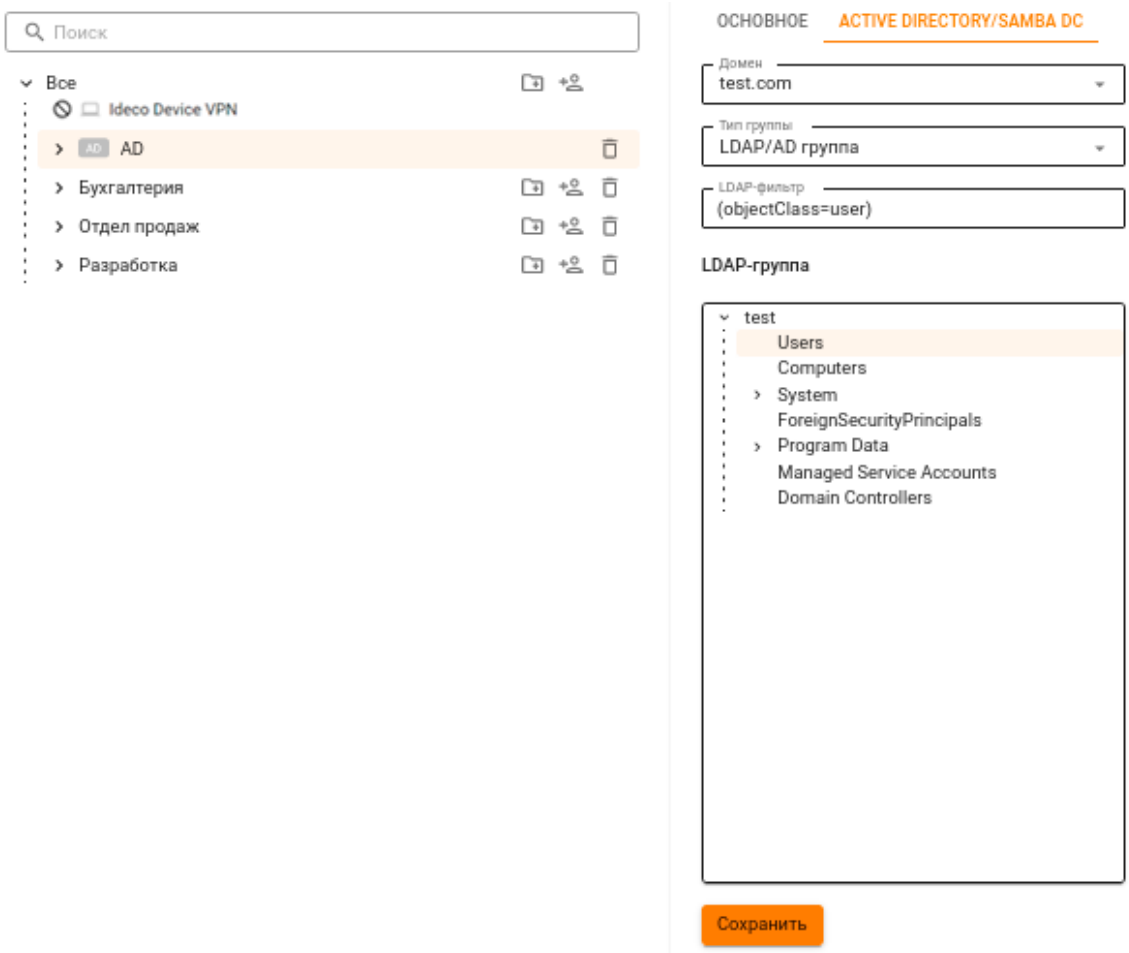
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC** в правой части экрана.

3. Выберите домен, из которого требуется импортировать пользователей.

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

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

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

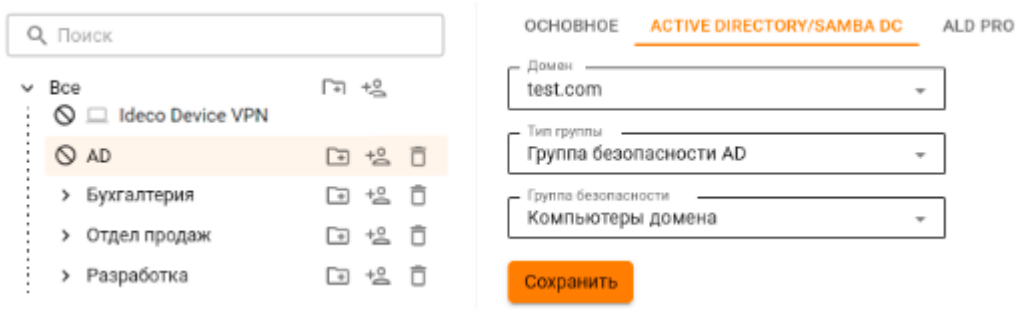


При необходимости воспользуйтесь фильтром запросов. Например, если в одних и тех же контейнерах находятся пользователи и компьютеры, а импортировать нужно только пользователей, то в поле **LDAP-фильтр** напишите: `(&(objectCategory=person)(objectClass=user))`

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

Импорт учетных записей из групп безопасности

1. Создайте группу в дереве пользователей Ideco NGFW.
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC**.
3. В поле **Имя домена** выберите нужный домен.
4. В поле **Тип группы** выберите **Группа безопасности AD**.
5. В поле ниже из раскрывающегося списка выберите нужную группу безопасности.
6. Нажмите на кнопку **Сохранить**.



Если импортировались не все пользователи:

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

Примеры включения через терминал и браузер:

Терминал

1. Авторизуйтесь командой:

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

2. Отправьте запрос на включение режима:

```
curl -c /tmp/cookie -b /tmp/cookie -X PATCH https://адрес_сервера/ad_backend/security_
↪group_import_settings -d '{"compatibility_mode": true}' -i -k -H 'Content-type:␣
↪application/json'
```

Браузер

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

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

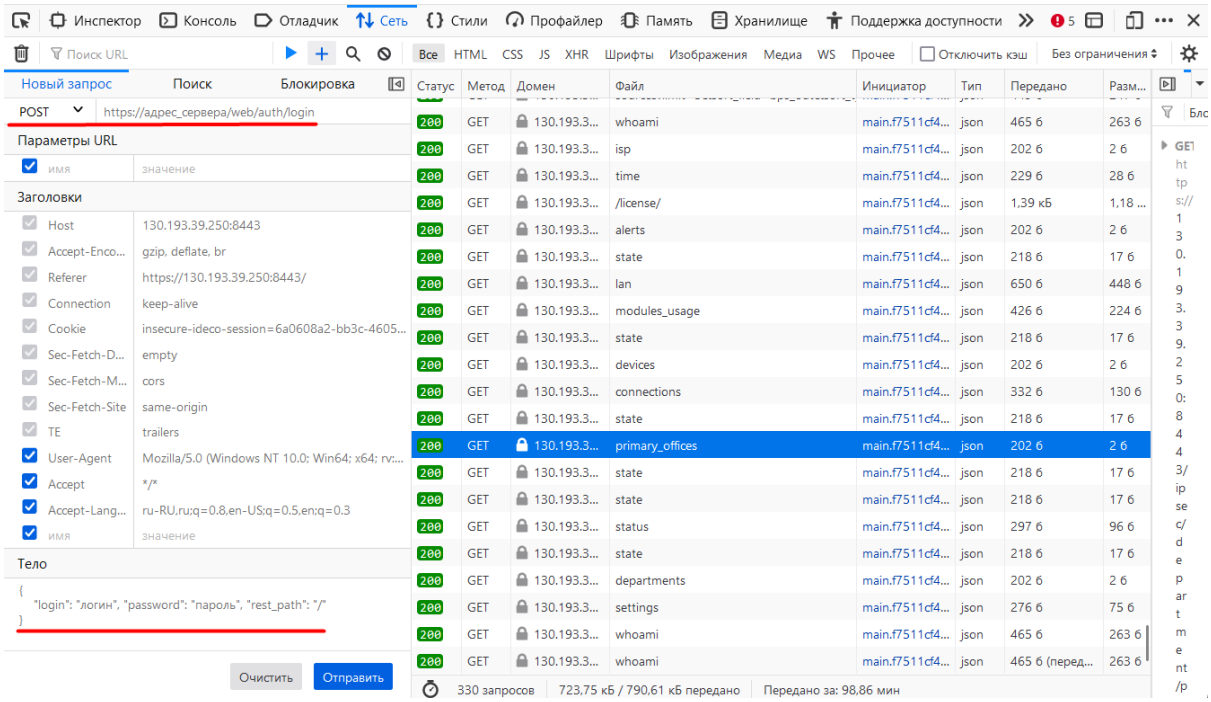
3. В появившемся окне перейдите на вкладку **Новый запрос**.

4. Отправьте запрос авторизации:

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

Тело запроса:

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

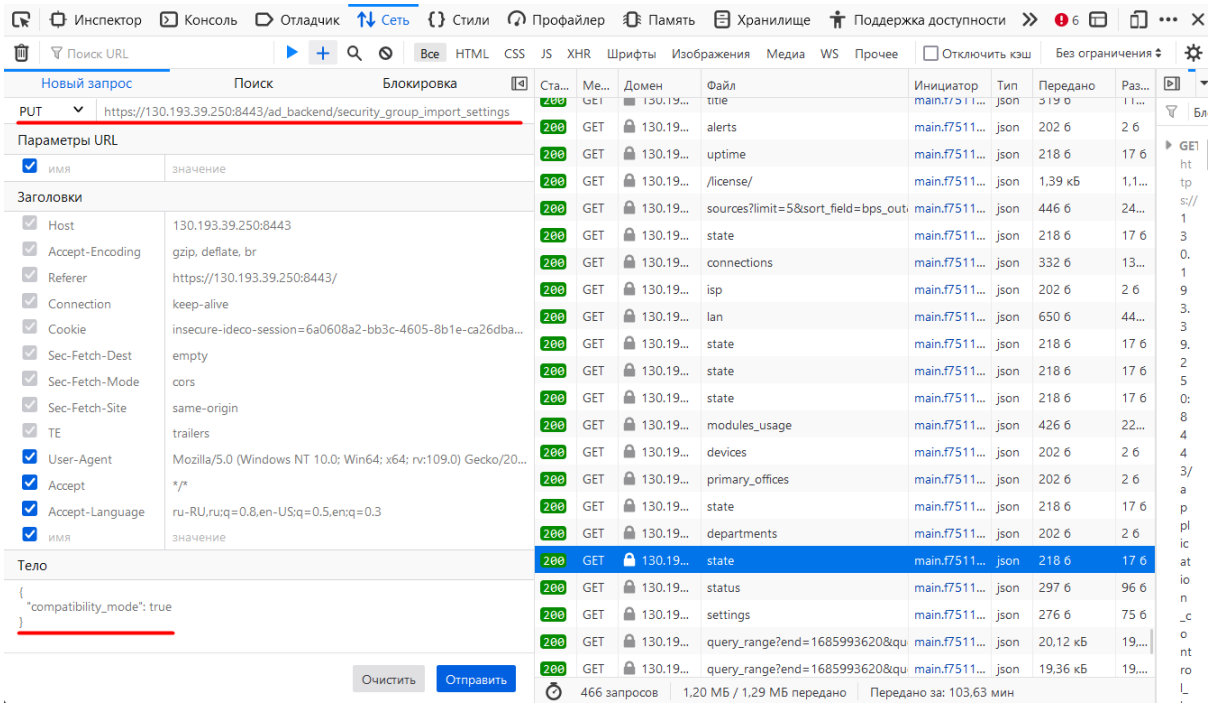


5. Отправьте запрос на включение режима:

```
PATCH /ad_backend/security_group_import_settings
```

Тело запроса:

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



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

Особенности при импорте пользователей в Ideco NGFW:

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

14.8 Интеграция с RADIUS-сервером

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

14.8.1 Настройка интеграции

Подсказка: Через RADIUS-сервер доступна аутентификация только VPN-пользователей NGFW.

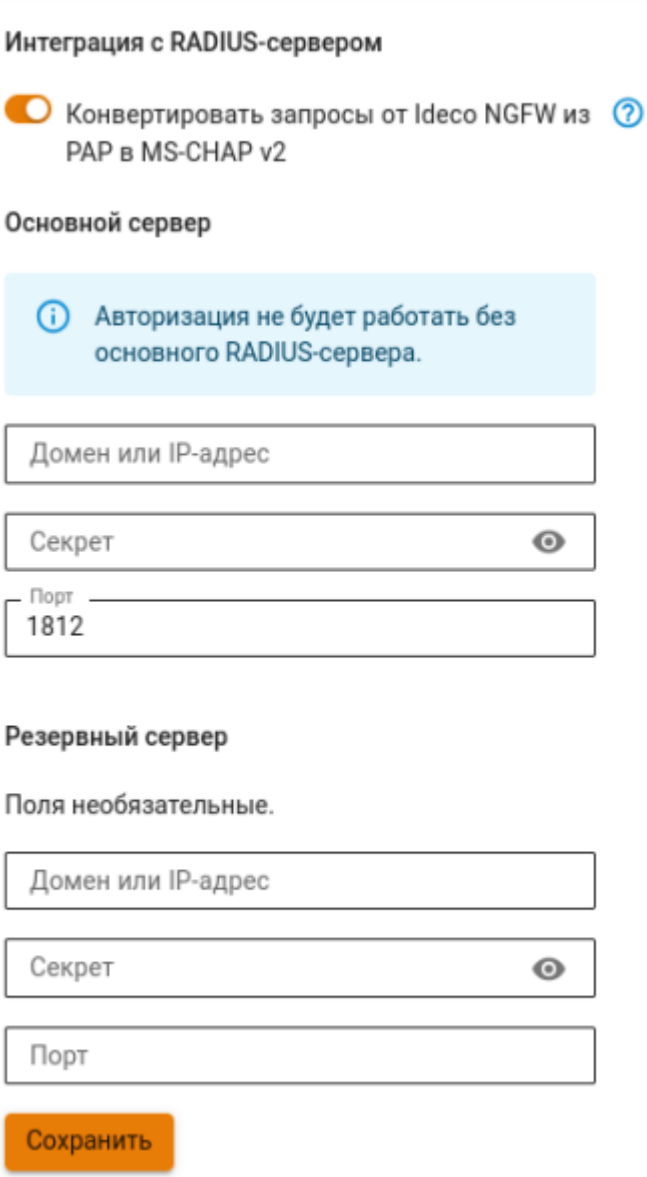
Для взаимодействия с основным RADIUS-сервером по умолчанию используется порт 1812.

Для настройки интеграции с RADIUS-сервером выполните действия:

1. Перейдите в раздел **Пользователи -> RADIUS** и включите опцию **RADIUS**.

2. Оставьте опцию Конвертировать запросы от Ideco NGFW из PAP в MS-CHAP v2 включенной или отключите ее и настройте на RADIUS-сервере двухфакторную аутентификацию.

3. Заполните поля:



- **Домен или IP-адрес** - домен или IP-адрес внутреннего RADIUS-сервера;
- **Секрет** - ключ-пароль, который устанавливается на этапе конфигурации RADIUS-сервера;
- **Порт** - порт, по которому будет происходить подключение к серверу. Поменяйте при необходимости.

4. Нажмите **Сохранить**.

Подсказка: При наличии в сети двух RADIUS-серверов настройте один как резервный с указанием порта подключения.

При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.

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

14.8.2 Двухфакторная аутентификация

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

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

Если необходимо обеспечить для пользователей RADIUS-сервера двухфакторную аутентификацию:

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

2. Настройте RADIUS-сервер на работу с протоколом PAP. **Важно:** даже если внешний сервер настроен на аутентификацию по PAP, Ideco NGFW не поддерживает этот протокол для прочих типов VPN-подключений.

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

Предупреждение: Не отключайте опцию **Конвертировать запросы от Ideco NGFW из PAP в MS-CHAP v2**, если:

- Требуется защита от перехвата пароля между NGFW и RADIUS-сервером;
- RADIUS-сервер поддерживает только MS-CHAP v2.

Опция **Конвертировать запросы от Ideco NGFW из PAP в MS-CHAP v2** влияет только на подключения через Ideco Client, ее переключение никак не влияет на подключение пользователей по другим типам *VPN*.

14.8.3 Механизм добавления пользователей в дерево Ideco NFGW

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

2. Если пользователь не будет найден в дереве NGFW, NGFW отправит запрос к RADIUS-серверу на аутентификацию пользователя.

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

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

Если пользователь уже есть в группе **RADIUS**, то запрос на аутентификацию сразу будет отправлен на **RADIUS-сервер**.

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

Предупреждение: Ограничения для группы и пользователей RADIUS:

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

- Запрещено перемещать других пользователей NGFW в группу **RADIUS**;
- Запрещена настройка IP и MAC авторизации для пользователей группы;
- Недоступна авторизация пользователей группы в личном кабинете и веб-почте.

14.9 ALD Pro

Подсказка: Название службы раздела **ALD Pro**: `ideco-ald-rest`; `ideco-ald-backend`.
Список служб для других разделов доступен по *ссылке*.

Ideco NGFW поддерживает версии ALD Pro от 1.4.

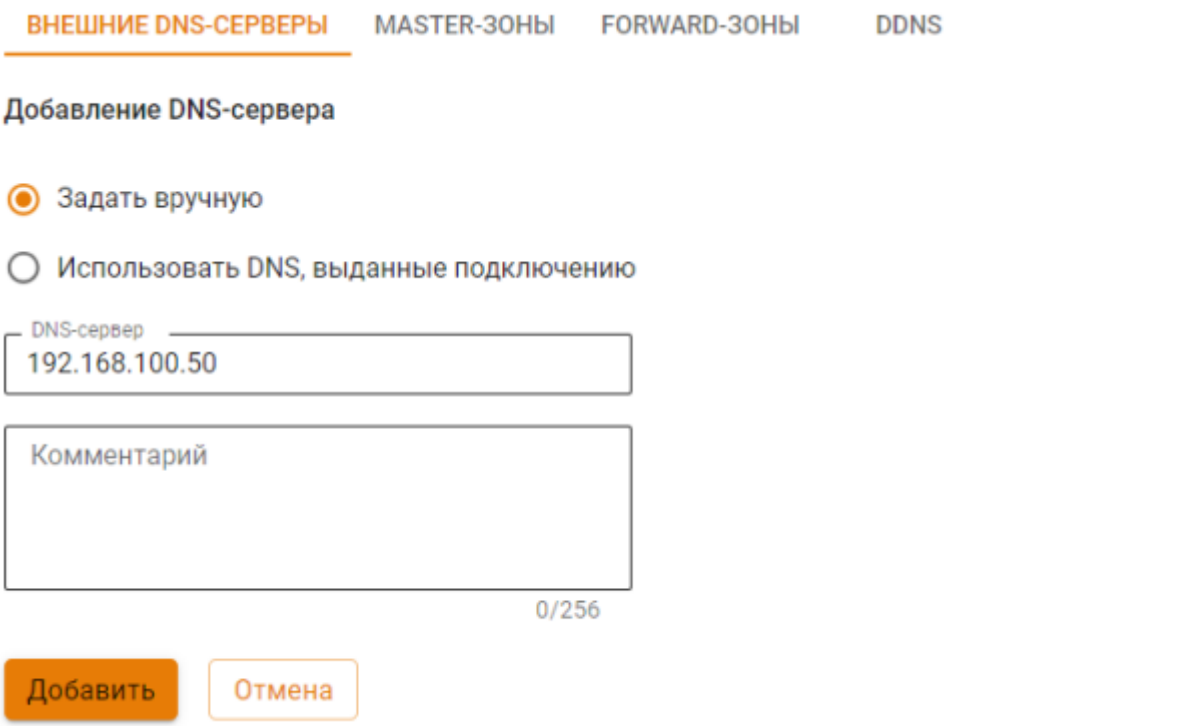
Система ALD Pro предназначена для централизованного управления ресурсами на базе ОС Astra Linux и может использоваться в организациях различного масштаба.

Руководства по эксплуатации ALD Pro доступны на официальном сайте.

Подсказка: Синхронизация с ALD Pro приостанавливается, если локальные пользователи Ideco NGFW находятся в группах AD. Для возобновления синхронизации вынесите локальных пользователей из групп ALD Pro. Автоматическая синхронизация произойдет через 15 минут.

14.9.1 Ввод сервера в домен

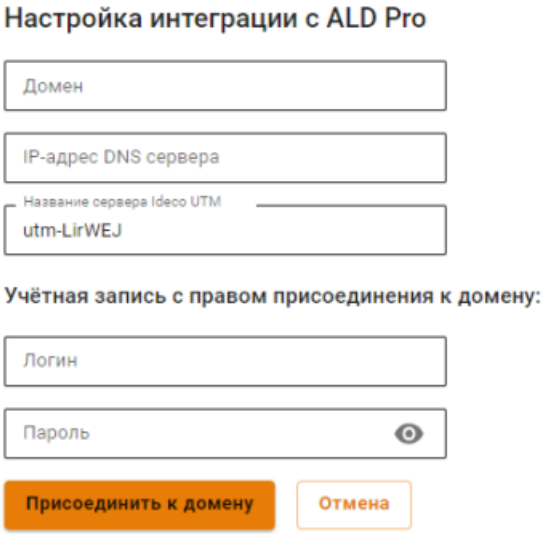
1. Перейдите в раздел **Сервисы -> DNS -> Внешние DNS-серверы** и добавьте IP-адрес устройства с установленной системой ALD Pro:



2. Перейдите на вкладку **Пользователи -> ALD Pro**.

2. Нажмите на кнопку **Добавить**.

3. Заполните поля:



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

Подсказка: Инструкции по развертыванию и управлению ресурсами через ALD Pro доступны на официальном сайте.

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

14.9.2 Импорт пользователей

> **Предупреждение:** Ideco NGFW также поддерживает интеграцию с ALD-администраторами. Подробные инструкции по настройке описаны в статье *Администраторы*.

ALD Pro поддерживает импорт двух типов групп:

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

Для импорта пользователей выполните действия:

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

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

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

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

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

14.9.3 Аутентификация пользователей

При аутентификации пользователей проверка осуществляется средствами Kerberos.

ALD Pro поддерживает два типа входа в систему:

- вход по логину/паролю;
- вход через SSO.

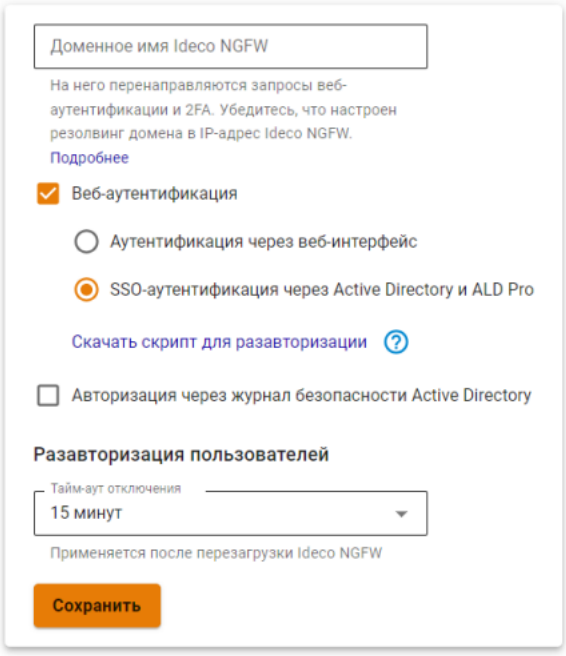
Настройка Ideco NGFW

Для настройки аутентификации выполните действия:

1. Перейдите в раздел **Пользователи -> Авторизация -> Основное**.

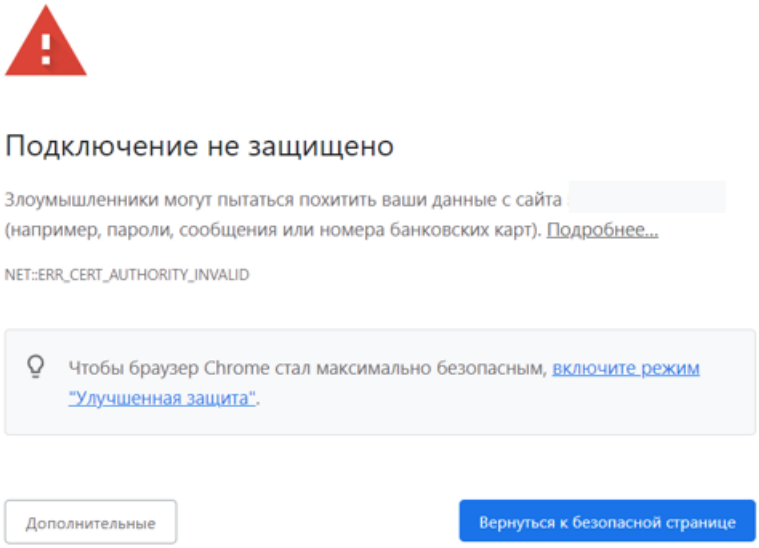
2. Активируйте опцию **Веб-аутентификация**.

3. Выберите тип входа в систему:



- Для входа по логину/паролю активируйте опцию **Аутентификация через веб-интерфейс**;
- Для входа через SSO активируйте опцию **SSO-аутентификация через Active Directory и ALD Pro**.

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



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

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

---

4. Настройте способы аутентификации импортированных пользователей. Доступные способы:

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

Подсказка: Для настройки авторизации по VPN воспользуйтесь статьей *VPN-подключения*.

Настройка клиентских машин для SSO-авторизации

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

На странице настроек браузера Mozilla Firefox (about:config в адресной строке) настройте следующие параметры:

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

1. Загрузите корневой сертификат и добавьте его в доверенные.

2. На машине ALD-клиента, введенной в домен ALD Pro, добавьте IP локального интерфейса и доменное имя Ideco NGFW в /etc/hosts. Пример: `192.168.100.10 domain.ald`.

14.10 Обнаружение устройств

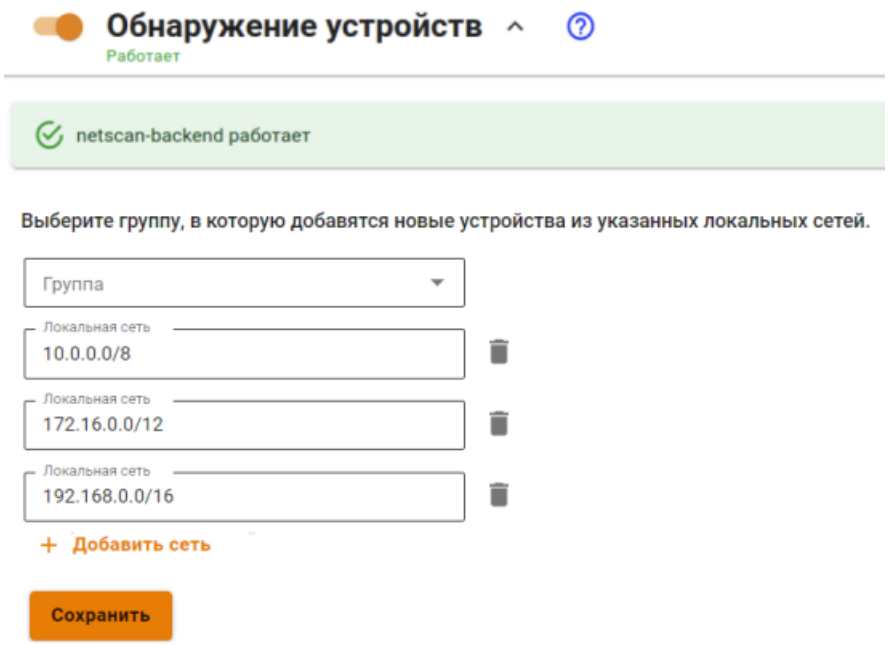
14.10.1 Основное

Подсказка: Название службы раздела **Обнаружение устройств**: `ideco-netscan-backend`.
Список служб для других разделов доступен по *ссылке*.

Данный модуль не осуществляет сканирования сети в поисках устройств, а работает в пассивном режиме.

Обнаружение устройств создает авторизацию по MAC для локальных адресов в одном Ethernet-сегменте. Если устройство находится в локальной сети за роутером, то будет создана авторизация по IP-адресу.

При попытке выхода в интернет будет создан пользователь в указанной группе с именем, соответствующим NetBIOS-имени компьютера. Если NetBIOS-имя определить не удалось, то в поле **Имя пользователя** будет записан IP-адрес найденного устройства:



При необходимости можно ограничить локальные сети, пользователи из которых будут автоматически добавлены и авторизованы на Ideco NGFW. Например, так можно авторизовать пользователей, подключающихся по Wi-Fi или другой открытой сети.

Подсказка: При подключении к NGFW как к прокси серверу система обнаружения устройств работать не будет.

14.11 Wi-Fi-сети

В текущей версии Ideco NGFW не поддерживает Wi-Fi-адаптеры. Для работы беспроводных клиентов необходимо использовать беспроводные точки доступа или Wi-Fi-маршрутизаторы.

Для выхода в интернет пользователей, подключающихся по Wi-Fi, необходима их авторизация на NGFW или авторизация Wi-Fi-роутера - это зависит от режима работы маршрутизатора.

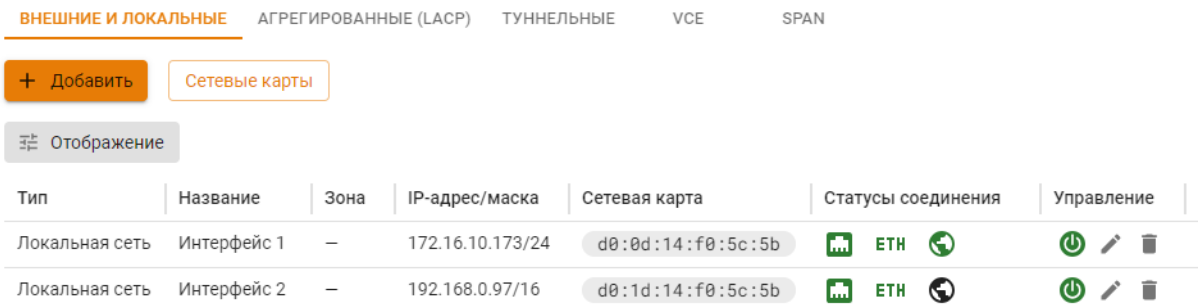
Режим точки доступа или bridge

В режиме точки доступа или bridge устройство Wi-Fi позволяет беспроводным клиентам подключаться к локальной сети.

Для этого индивидуально авторизуйте всех беспроводных клиентов на Ideco NGFW с помощью IP-авторизации. Воспользуйтесь рекомендациями по настройке:

- Используйте отдельную логическую сеть для клиентов Wi-Fi с настроенным *DHCP-сервером*. При этом на локальный интерфейс Ideco NGFW добавьте IP-адрес, служащий шлюзом для этой сети;
- *Создайте группу*;
- С помощью *Контент-фильтра* и *Файрвола* настройте необходимые ограничения для пользователей Wi-Fi;
- Если Wi-Fi-роутер подключен к отдельному физическому интерфейсу NGFW, то в файрволе запретите доступ из беспроводной сети в локальную сеть.

Пример настройки интерфейса для клиентов, подключающихся по Wi-Fi:



- **172.16.10.173/24** - шлюз для беспроводной Wi-Fi-сети;
- **192.168.0.97/16** - шлюз для локальной Ethernet-сети.

14.11.1 Настройка DHCP:

1. Добавьте отдельную логическую сеть для клиентов Wi-Fi.

2. Добавьте в сетевые интерфейсы шлюз созданной сети.

3. Перейдите в раздел **Сервисы -> DHCP-сервер** и выберите сетевой интерфейс, настроенный на прошлом шаге.

4. Назначьте диапазон IP-адресов для DHCP-сервера и нажмите **Сохранить**.

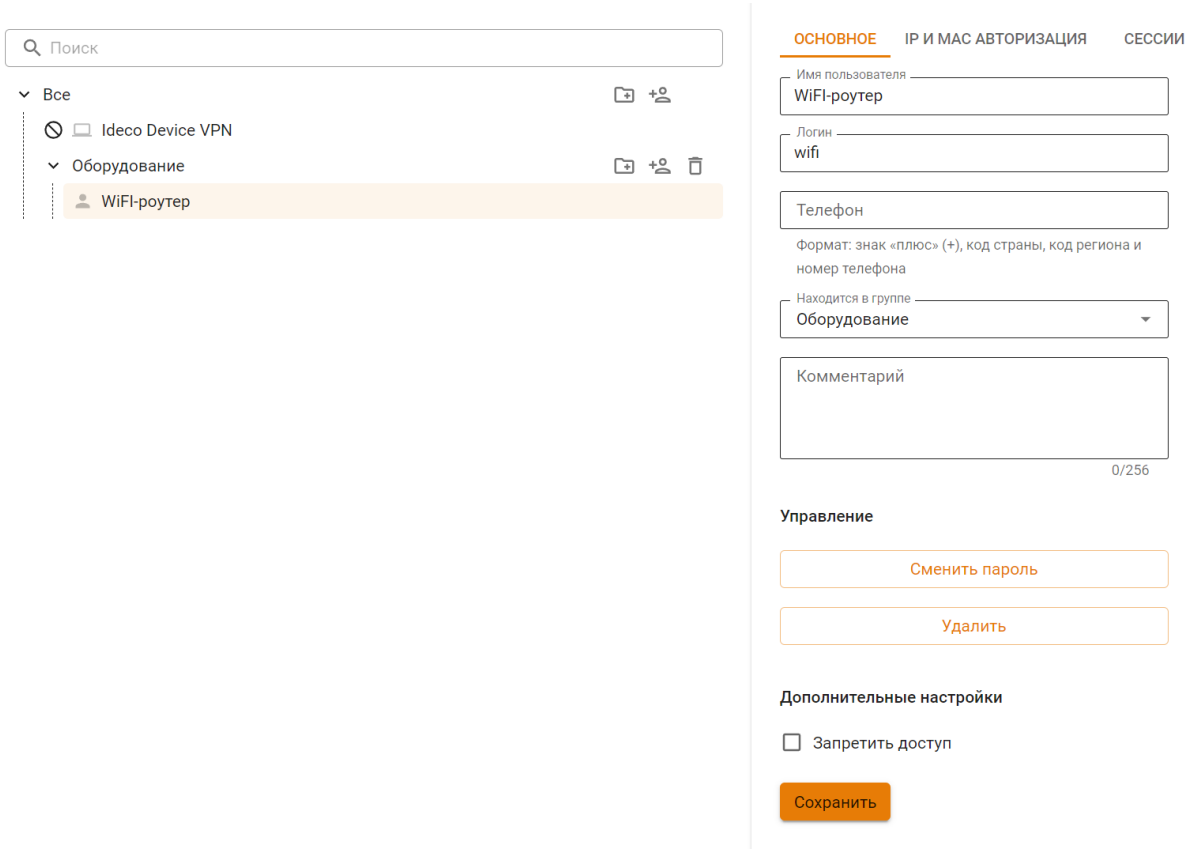
При необходимости индивидуальной авторизации Wi-Fi-пользователей (учета трафика и статистики каждого конкретного пользователя устройств) воспользуйтесь *авторизацией через веб-браузер*. При таком способе авторизации Ideco NGFW будет учитывать каждого пользователя, подключившегося по Wi-Fi. Учтите этот момент при планировании лицензирования Ideco NGFW.

Режим роутера

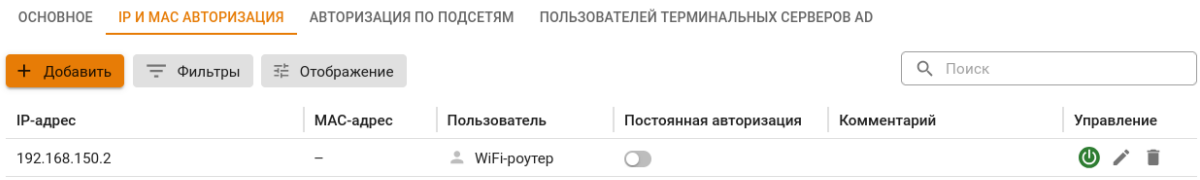
В данном режиме устройство Wi-Fi скрывает за NAT устройства беспроводной сети. Таким образом, для Ideco NGFW достаточно будет авторизовать только точку доступа как одного из пользователей.

Пример настройки пользователя в режиме роутера:

1. В разделе **Пользователи -> Учётные записи** создайте пользователя для Wi-Fi-роутера:



2. В разделе **Пользователи -> Авторизация -> IP и MAC авторизация** создайте правило:



К пользователю необходимо применить общие ограничения *Контент-фильтра* и *Файрвола* для Wi-Fi-сети.

14.11.2 Настройка DHCP:

При работе маршрутизатора в таком режиме не требуется дополнительной настройки DHCP-сервера Ideco NGFW, поскольку работает встроенный DHCP-сервер маршрутизатора. Если у вас не получилось подключиться к Wi-Fi-сети, то нужно проверить работу DHCP-сервера маршрутизатора.

При этом способе авторизации Ideco NGFW будет использоваться одна лицензия на точку доступа Wi-Fi. Отдельно настроить фильтрацию трафика и считать статистику по трафику в отчетах для отдельных

клиентов Wi-Fi будет невозможно.

15. Мониторинг

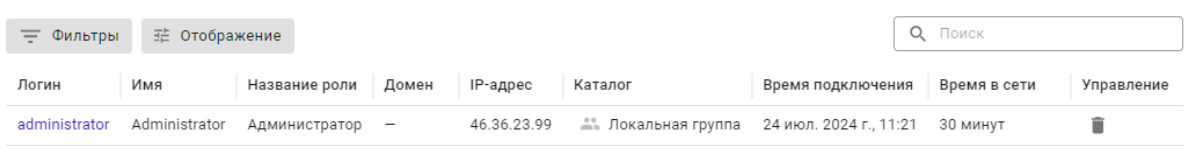
15.1 Сессии администраторов

15.1.1 Основное

В разделе **Мониторинг -> Сессии администраторов** представлен список всех сессий администраторов, авторизованных в NGFW. В таблице представлены не только локальные администраторы, но и администраторы, импортированные из групп безопасности Active Directory, групп пользователей ALD PRO и RADIUS.

Формы добавления администраторов представлены в разделе **Управление сервером -> Администраторы**. С подробной информацией о создании администраторов можно ознакомиться по *ссылке*.

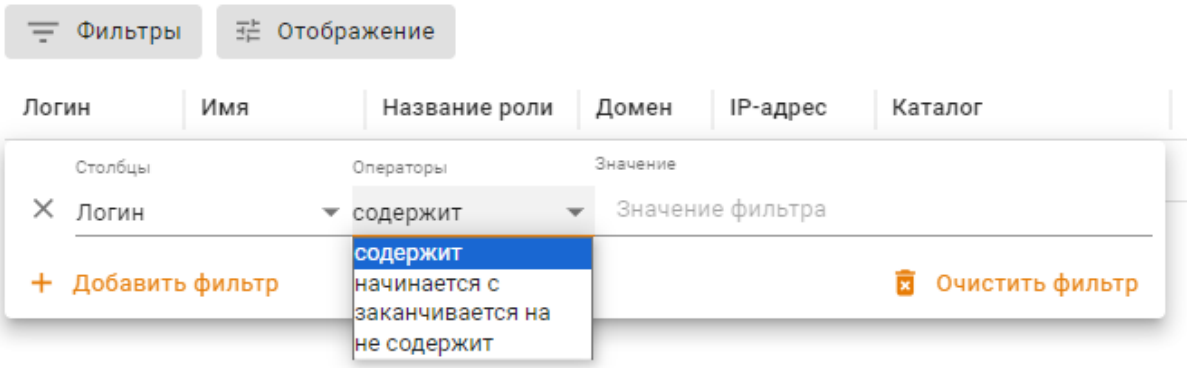
Пример таблицы сессий администраторов:



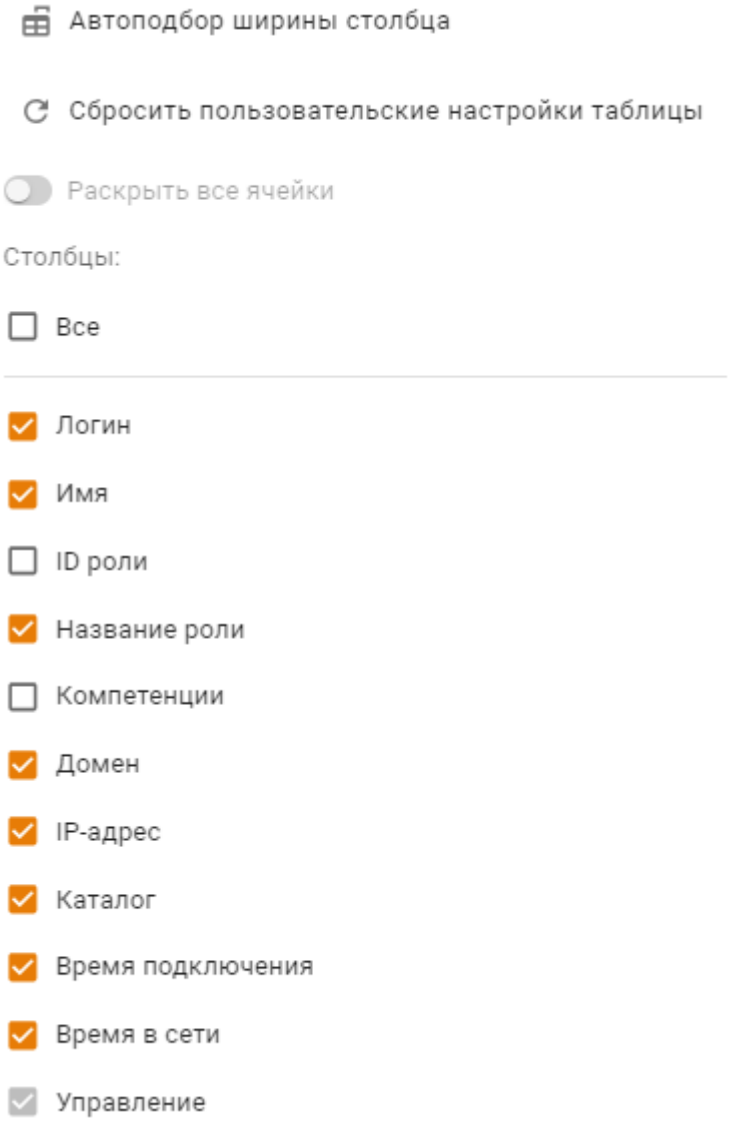
- **Логин** - при создании логина локального администратора запрещено указывать символ @;
- **Название роли** - возможные роли: Администратор, Только просмотр, Просмотр отчетов, Создание отчетов;
- **Домен** - указано имя домена, если администратор импортирован из Active Directory или ALD PRO. В ином случае в ячейке прочерк;
- **IP-адрес** - IP-адрес устройства, с которого авторизован администратор;
- **Каталог** - тип администратора в зависимости от источника добавления: Локальная группа, AD, ALD, RAD;
- **Время подключения** - момент запуска сессии с указанием даты в формате день/месяц/год и времени в формате час/минута;
- **Время в сети** - продолжительность сессии администратора с момента запуска, указанного в столбце **Время подключения**;
- **Управление** - возможность разавторизовать любого администратора из интерфейса Ideco NGFW.

Подсказка: В столбце **Управление** администратор может разавторизовать самого себя.

Кнопка **Фильтры** позволяет выбрать нужные сессии. Фильтрация возможна по всем столбцам, кроме **Время в сети** и **Управление**, а также с использованием нескольких переменных:



Кнопка **Отображение** позволяет скрывать и раскрывать столбцы с дополнительной информацией. По умолчанию в таблице представлены все столбцы, кроме **ID роли** и **Компетенции**:



В столбце **Компетенции** представлены доступные администратору возможности: чтение, редактирование, доступ к терминалу, просмотр и изменение отчетов.

Подсказка: В разделе **Отчеты и журналы ->** ***Действия администраторов*** представлены логи действий администраторов. Действия, осуществляемые через локальное меню NGFW, отображаются в журнале с

источником 127.0.0.1.

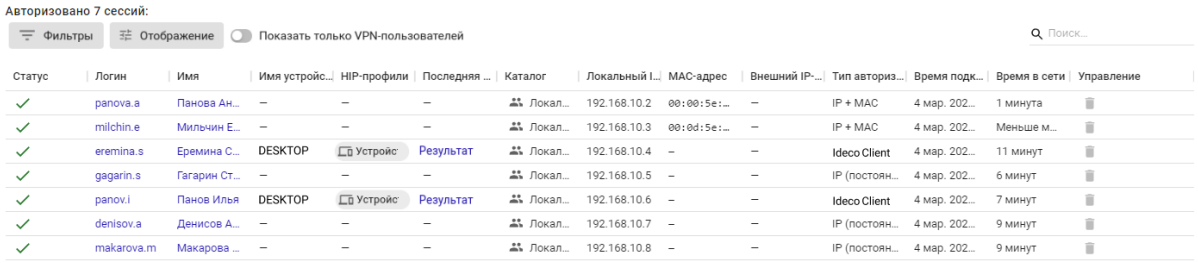
15.2 Авторизованные пользователи

15.2.1 Основное

В разделе **Мониторинг -> Авторизованные пользователи** отображен список всех сессий пользователей, которые авторизовались в NGFW.

Статус	Описание
✓	**Подключено**. Пользователь авторизован
2FA	**Ожидает второй фактор авторизации**. Пользователь создал и активировал VPN-подключение, но не прошел двухфакторную аутентификацию (подробнее в *статье*)
	Превышен лимит лицензии. Данная сессия заблокирована. Появляется в случае, если превышено количество пользователей по лицензий или у пользователя уже есть активные 5 сессий
	Сессия удаляется. Появляется в случае, если была разорвана сессия с динамическим IP-адресом. Сессия с таким статусом будет удалена через 30 секунд

Пример пользователей, авторизованных разными способами:

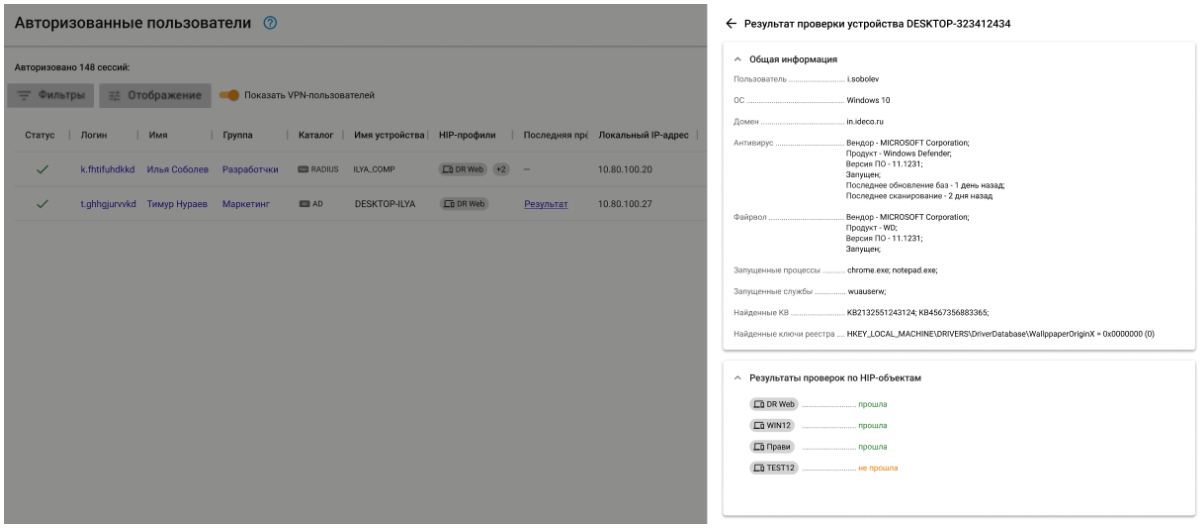


В столбце **Управление** можно разавторизовать пользователя при необходимости.

При наличии большого количества авторизованных пользователей в таблице воспользуйтесь кнопкой **Фильтры**. Включение опции **Показать только VPN-пользователей** отфильтрует в таблице журнала информацию обо всех VPN-сессиях по всем протоколам.

Подсказка: Количество сессий в мониторинге не является количеством занимаемых лицензий, так как под одной пользовательской учетной записью возможна одновременная авторизация до 5 устройств (динамическими способами авторизации, по веб, Kerberos/NTLM, логам безопасности контроллеров домена Active Directory, VPN), что будет считаться как одна пользовательская лицензия.

Для просмотра результата проверки устройства, подключенного через Ideco Client, кликните на **Результат** в столбце **Последняя проверка**, откроется соответствующее окно с общей информацией и результатами проверок по *HIP-объектам*:



15.3 Сессии ЛК

15.3.1 Основное

Сессии ЛК - таблица активных сессий в личном кабинете Ideco NGFW. Для аутентификации пользователей используется логин и пароль, возможно использование технологии 2FA (двухфакторная аутентификация). Доступ к ресурсам в локальной сети пользователи получают через веб-браузер по HTTPS без установки отдельного туннельного соединения (технология SSL VPN).

Записи в журнале появляются после авторизации пользователей в личном кабинете, настроенном в разделе **Сервисы ->** ***ЛК/Портале SSL VPN***.

Записи доступны для управления и остаются в таблице до завершения сессии:

Помимо общих сведений об учетной записи пользователя (логин, имя, группа и каталог), таблица активных сессий содержит столбцы:

- **Статус** - доступные значения: авторизован, 2FA (ожидает 2FA, генерация TOTP для прохождения 2FA);
- **IP-адрес** - IP-адрес, с которого произведена начальная аутентификация сессии в ЛК;
- **Расположение** - страна IP-адреса, с которого произведена начальная аутентификация сессии в ЛК. Значение пустое, если:
  - Отсутствует лицензия;
  - Невозможно получить базу GeoIP;
  - IP-адрес локальный.
- **Время подключения** - момент аутентификации в ЛК с указанием даты в формате день/месяц/год и времени в формате час/минута;

- **Время в сети** - длительность сессии аутентификации в ЛК, разница между временем подключения и текущим временем.
- **Управление** - доступно только действие **Отключить** для завершения сессии аутентификации.

Подсказка: **IP-адрес** и **Расположение** могут меняться, т.к. сессия авторизации привязана к cookie и браузеру, а не к IP-адресу.

Столбцы в таблице можно отрегулировать кнопкой **Отображение**.

Чтобы найти нужную сессию, воспользуйтесь одним из способов:

- Нажмите кнопку **Фильтры**, выберите один из параметров поиска и его значение;
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

15.4 График загруженности

Этот модуль позволяет просматривать графики о состоянии NGFW в **режиме реального времени**. Горизонтальной шкалой графика всегда является *время* (в зависимости от выбранного интервала).

Подсказка: Статистика хранится до 90 дней.

Когда резервная нода в *Кластере* становится активной, статистика с предыдущей активной ноды не передается новой, но продолжает храниться до 90 дней.

Предупреждение: Обратите внимание, что при отключении опции **Сбор метрик** в некоторых графиках может наблюдаться несогласованность данных по времени. Это связано с внутренней реализацией модуля.

15.4.1 Система

Содержит информацию:

- О количестве авторизованных пользователей;
- Процент загрузки процессора (максимальное значение загрузки процессора - 100%);
- Объем используемой оперативной памяти в ГБ;
- Среднее значение загрузки системы;
- Количество всех установленных сетевых соединений.

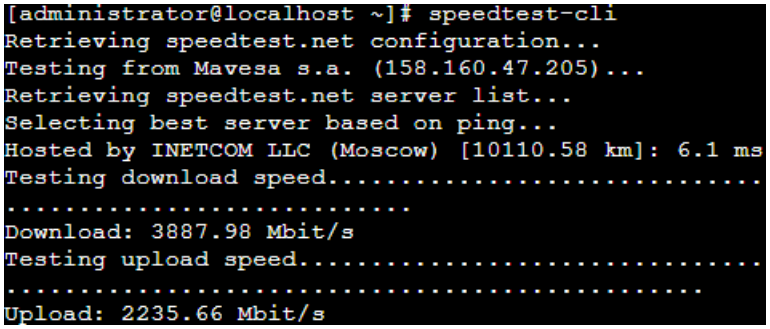
15.4.2 Сеть

Содержит суммарную информацию о входящем и исходящем трафике за определенное время, передаваемом через NGFW по всем интерфейсам, заданным в разделе *Сетевые интерфейсы*.

Эта статистика может помочь в настройке резервирования каналов, статической и динамической *балансировки*.

Подсказка: Для проверки скорости сети внешнего Ethernet перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:



15.4.3 Диски

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

15.4.4 VPN

Содержит информацию о количестве подключений пользователей по протоколам L2TP/IPsec, PPTP и IKEv2. Инструкция по VPN-подключению пользователей доступна по *ссылке*.

15.4.5 IPsec

Содержит информацию о входящих, исходящих IPsec-подключениях Ideco NFGW. Показывает загрузку входящего и исходящего IPsec-канала.

15.4.6 WCCP GRE

Содержит информацию о входящей скорости GRE-туннелей.

Подсказка: Нельзя получить исходящую скорость для GRE-туннелей из-за особенности протокола GRE.

15.4.7 ГОСТ VPN

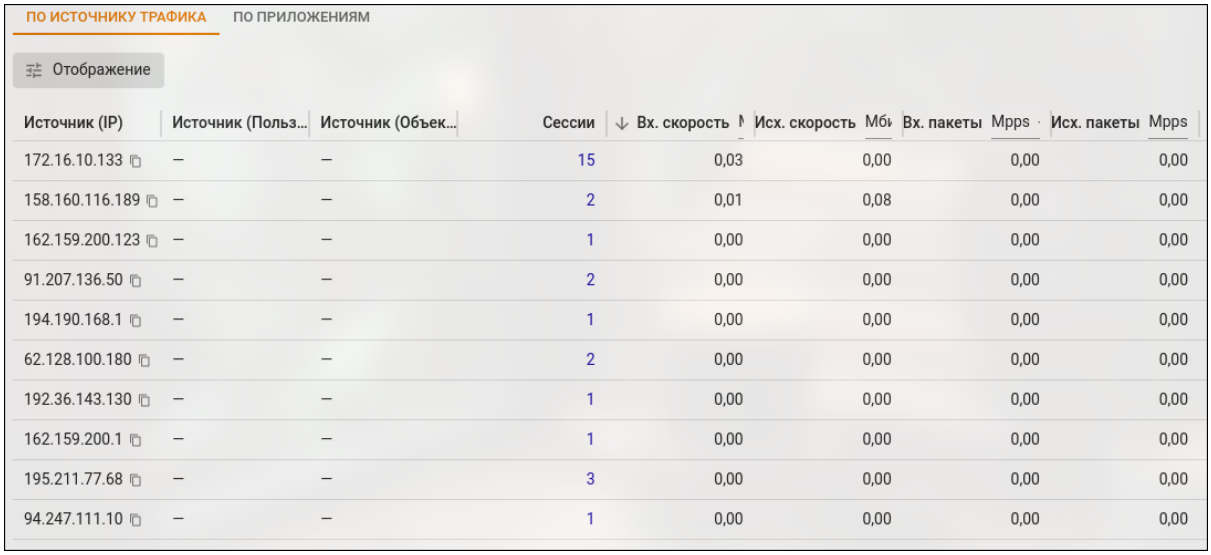
Содержит информацию о входящих и исходящих соединениях ГОСТ VPN в Ideco NFGW. Отображает график входящего и исходящего трафика за выбранный период времени. Инструкция по настройке ГОСТ VPN доступна по *ссылке*.

15.5 Монитор трафика

Подсказка: Для включения мониторинга трафика необходимо запустить модуль *Контроля приложений*.

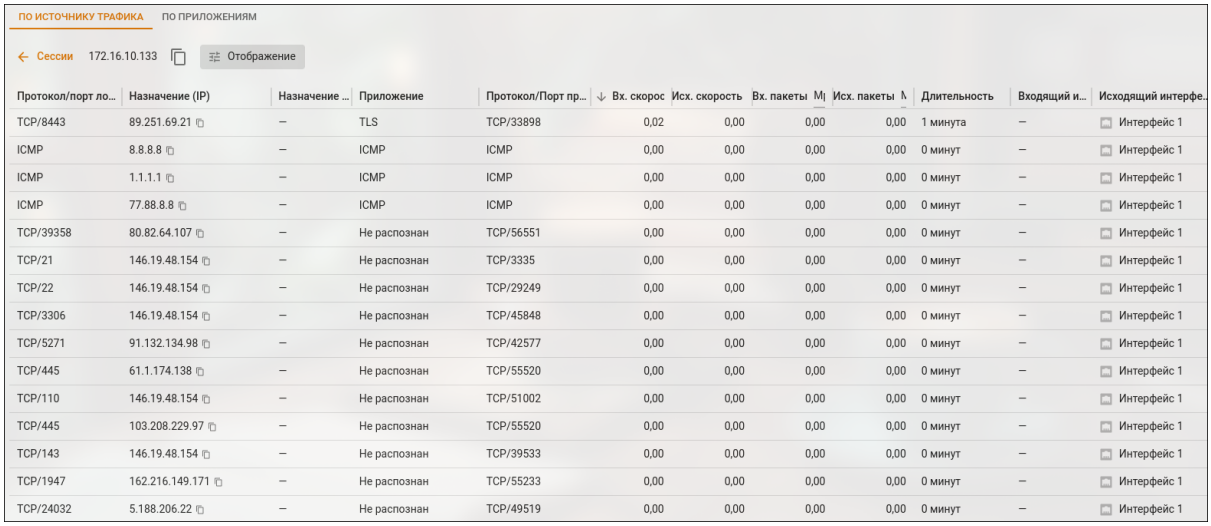
15.5.1 По источнику трафика

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



Источник (IP)	Источник (Польз...	Источник (Объек...	Сессии	Вх. скорость	Исх. скорость Мб	Вх. пакеты Mpps	Исх. пакеты Mpps
172.16.10.133	–	–	15	0,03	0,00	0,00	0,00
158.160.116.189	–	–	2	0,01	0,08	0,00	0,00
162.159.200.123	–	–	1	0,00	0,00	0,00	0,00
91.207.136.50	–	–	2	0,00	0,00	0,00	0,00
194.190.168.1	–	–	1	0,00	0,00	0,00	0,00
62.128.100.180	–	–	2	0,00	0,00	0,00	0,00
192.36.143.130	–	–	1	0,00	0,00	0,00	0,00
162.159.200.1	–	–	1	0,00	0,00	0,00	0,00
195.211.77.68	–	–	3	0,00	0,00	0,00	0,00
94.247.111.10	–	–	1	0,00	0,00	0,00	0,00

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

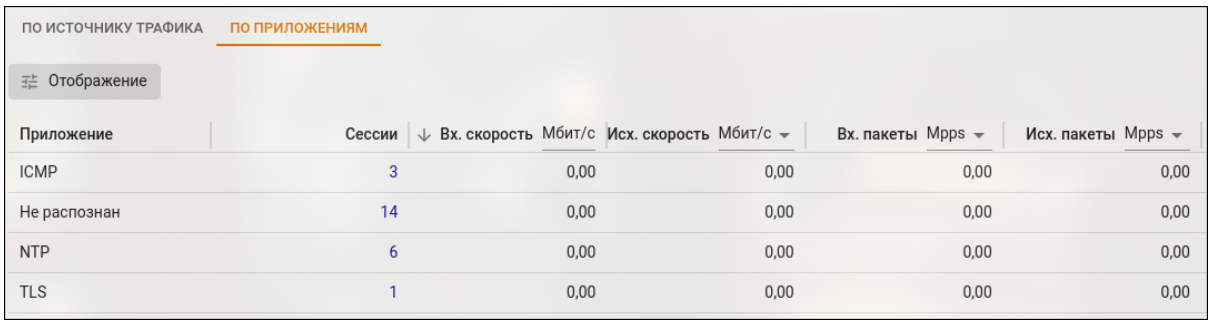


Протокол/порт ло...	Назначение (IP)	Назначение ...	Приложение	Протокол/Порт пр...	Вх. скорос	Исх. скорость	Вх. пакеты	Мр	Исх. пакеты	Длительность	Входящий и...	Исходящий интерфе...
TCP/8443	89.251.69.21	–	TLS	TCP/33898	0,02	0,00	0,00		0,00	1 минута	–	Интерфейс 1
ICMP	8.8.8.8	–	ICMP	ICMP	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
ICMP	1.1.1.1	–	ICMP	ICMP	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
ICMP	77.88.8.8	–	ICMP	ICMP	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/39358	80.82.64.107	–	Не распознан	TCP/56551	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/21	146.19.48.154	–	Не распознан	TCP/3335	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/22	146.19.48.154	–	Не распознан	TCP/29249	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/3306	146.19.48.154	–	Не распознан	TCP/45848	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/5271	91.132.134.98	–	Не распознан	TCP/42577	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/445	61.1.174.138	–	Не распознан	TCP/55520	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/110	146.19.48.154	–	Не распознан	TCP/51002	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/445	103.208.229.97	–	Не распознан	TCP/55520	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/143	146.19.48.154	–	Не распознан	TCP/39533	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/1947	162.216.149.171	–	Не распознан	TCP/55233	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1
TCP/24032	5.188.206.22	–	Не распознан	TCP/49519	0,00	0,00	0,00		0,00	0 минут	–	Интерфейс 1

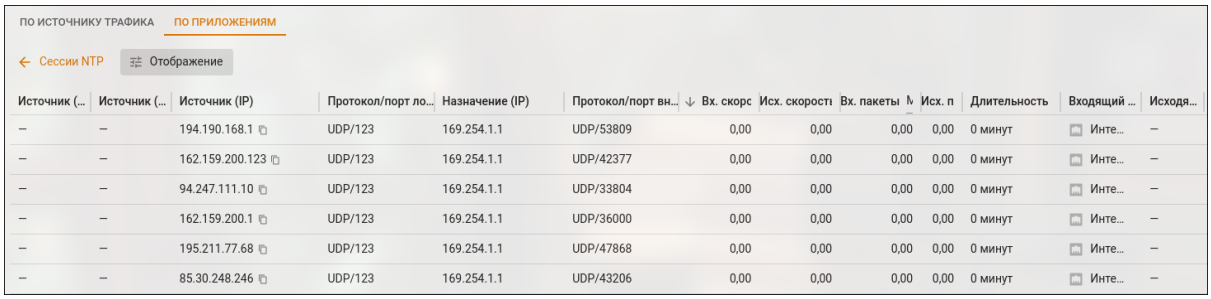
15.5.2 По приложениям

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

Например, если пользователь не загружает канал трафиком, но в таблице **По источнику трафика** присутствует большое количество пакетов данных, то на вкладке **По приложениям** можно выявить приложение с подозрительной активностью.



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



15.6 Telegram-бот

Бот может отправлять оповещения:

- в личные сообщения;
- в беседы, где 2 и более пользователей (groups).

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

15.6.1 Привязка Ideco Monitoring Bot

Настройка привязки Ideco Monitoring Bot к одному пользователю:

1. Настроить интернет на Ideco NGFW.

2. *Привязать лицензию* к серверу.

3. Перейти к диалогу с ботом: @ideco_monitor_bot.

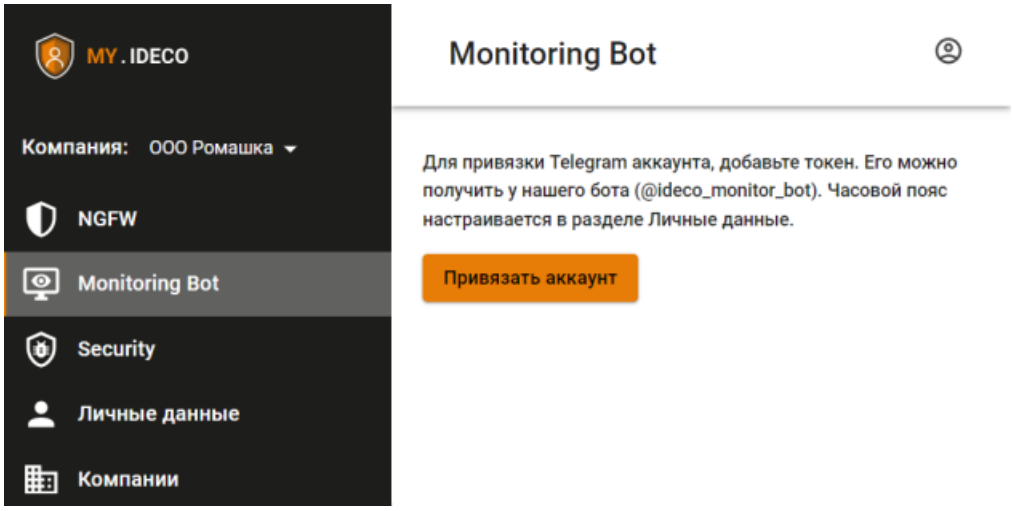
4. Написать боту `/start`.

5. Скопировать код привязки к аккаунту.

6. Перейти в раздел **Ideco Monitoring Bot** в личном кабинете.

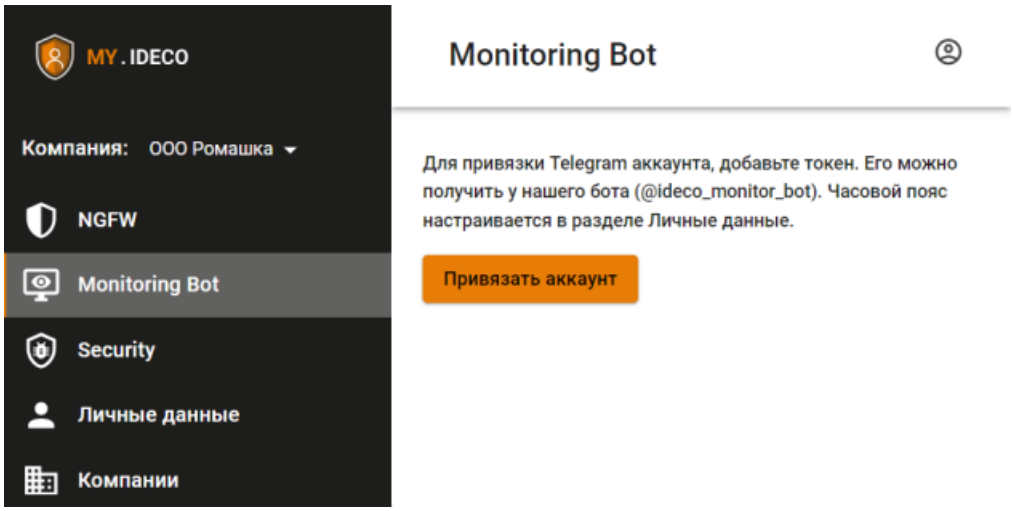
7. Нажать на кнопку **Привязать аккаунт**.

8. Ввести код в соответствующее поле и нажать на кнопку **Привязать**.



Настройка привязки Ideco Monitoring Bot к беседе:

1. Настроить интернет на Ideco NGFW.
2. *Привязать лицензию* к серверу.
3. Перейти в группу и добавить пользователя @ideco_monitoring_bot.
4. Написать `/start` в группе.
5. Скопировать код привязки к аккаунту.
6. Перейти в раздел **Ideco Monitoring Bot** в личном кабинете.
7. Нажать на кнопку **Привязать аккаунт**.
8. Ввести код в соответствующее поле и нажать на кнопку **Привязать**.



Подсказка: При настройке подключения Ideco Monitoring Bot к беседе нельзя использовать подсказки для команд, поскольку требуется ввод команды `/start` вручную.

Подсказка: Уведомления начнут приходить в телеграм-аккаунт.

15.6.2 Настройка оповещений Ideco Monitoring Bot

Настройте оповещения, которые приходят от Ideco Monitoring Bot, для каждой отдельной беседы.

Для настройки оповещений:

1. Перейдите в раздел настройки, нажав на иконку  .

2. Выберите уведомления, которые хотели бы получать в выбранной беседе.

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

15.7 SNMP

15.7.1 Основное

Подсказка: Для перевода раздела в рабочий режим переведите опцию в положение **Включен**.

Опция переключается в положение Включен

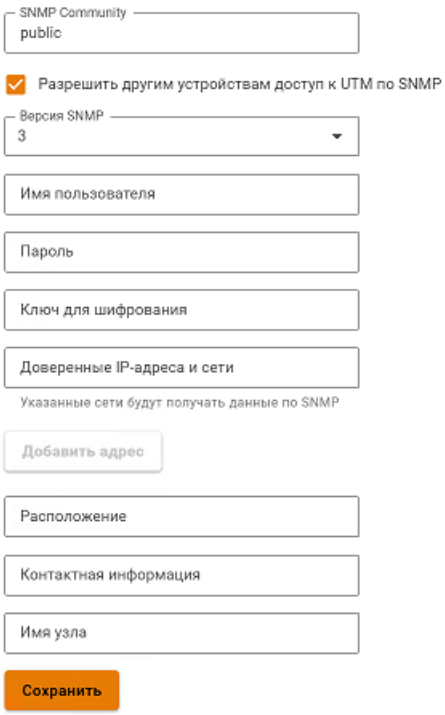
Этот модуль позволяет осуществлять мониторинг работы Ideco NGFW по протоколу SNMP версий 1/2c и 3. Для настройки подключения по протоколу SNMP необходимо:

- Для версии 1/2c указать:
  - Имя пользователя;
  - Пароль (минимальное количество символов - 8);
  - **Доверенные IP-адреса и сети**.
- Для версии 3 указать:
  - Имя пользователя;
  - Пароль (минимальное количество символов - 8);
  - Ключ шифрования;
  - **Доверенные IP-адреса и сети**.

Подсказка: **Рекомендуем**: На сервере, с которым будет осуществляться соединение по SNMPv3, указать алгоритмы: Auth Algorithm MD5 и Crypto Algorithm AES.

Поле SNMP community для SNMPv3 необязательно для заполнения.

После заполнения поля **Доверенные IP-адреса и сети** устройства, находящиеся в указанных доверенных сетях, получат доступ к данным с Ideco NGFW. Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и являются необязательными:



15.8 Zabbix-агент

Zabbix - это решение распределенного мониторинга корпоративного класса с открытыми исходными кодами.

Ознакомиться с Zabbix можно на официальной странице Zabbix.

Опробуйте Zabbix в виде готового решения или установить его, воспользовавшись документацией Zabbix.

15.8.1 Интеграция с Zabbix

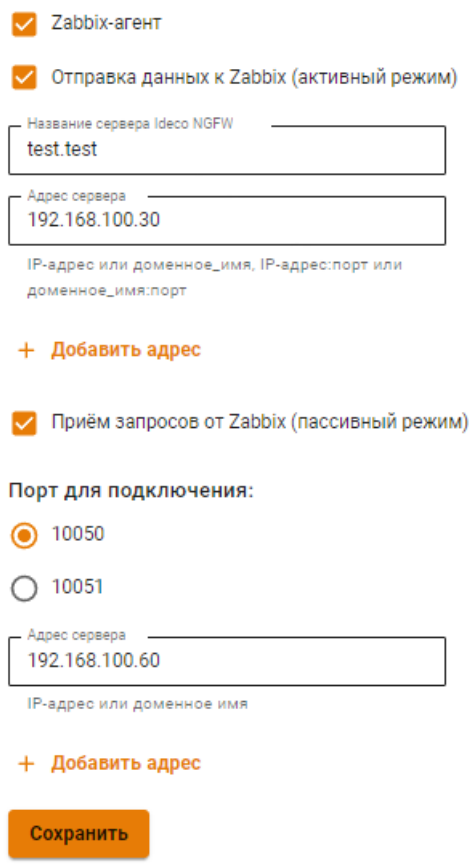
Предупреждение: Для работы системы мониторинга Zabbix активируйте опцию **Zabbix-агент** после настройки интеграции с Zabbix.

Интеграция с системой мониторинга Zabbix возможна в двух режимах:

1. **Активный режим** - соединение с Zabbix-сервером происходит со стороны Ideco NGFW. Для настройки этого режима заполните следующие поля:

- **Имя сервера Ideco NGFW** - имя, которое будет отображаться на сервере мониторинга;
- **Адрес сервера** - IP-адрес, доменное имя, либо `IP-адрес:порт`, `доменное имя:порт`, если используется не стандартный для Zabbix входящий порт. Для добавления еще одного адреса нажмите на кнопку **Добавить адрес**.

2. **Пассивный режим** - подключение происходит со стороны Zabbix-сервера. Для настройки этого режима заполните следующие поля:



- **Порт для подключения** - выберите 10050 или 10051 порт;
- **Адрес сервера** - IP-адрес или доменное имя Zabbix-серверов. Для добавления еще одного адреса нажмите на кнопку **Добавить адрес**.

В обоих случаях интеграции Zabbix-сервер должен находиться внутри локальной сети Ideco NGFW. Подключение мониторинга возможно только к локальным интерфейсам.

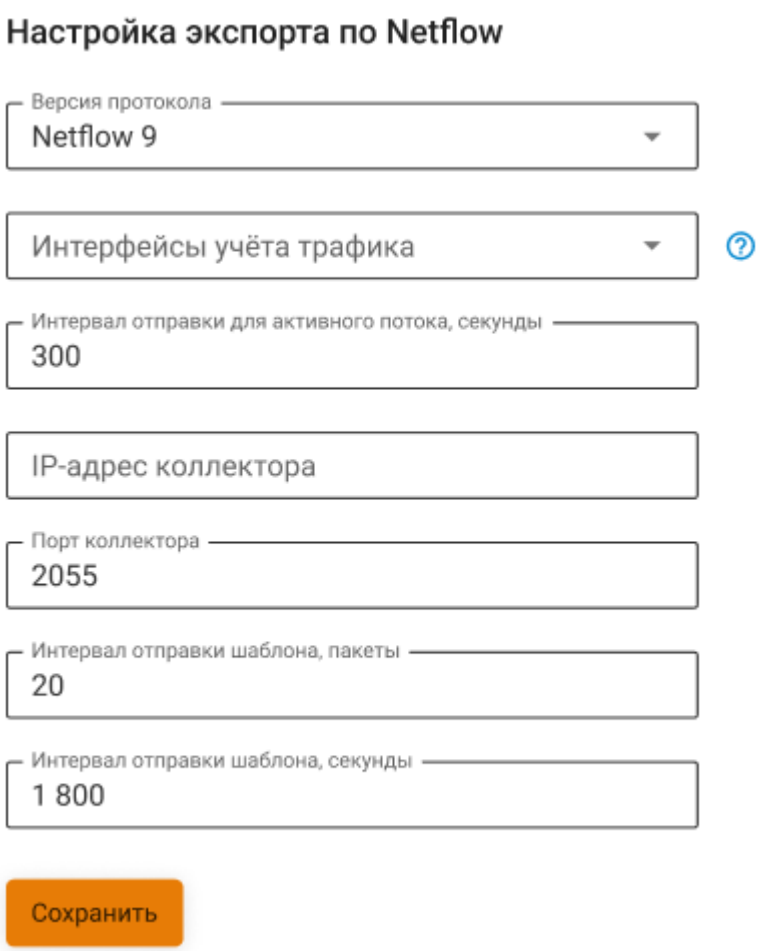
Подсказка: В качестве шаблонов данных можно использовать стандартные шаблоны для Linux-серверов.

15.9 Netflow

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

Netflow экспортирует статистику по потокам данных L3. Каждый поток является однонаправленным, т.е. каждое двунаправленное соединение интерпретируется как два потока: **src -> dst** и **dst -> src**.

Предупреждение: При включении Netflow рекомендуем настроить индексы Netflow для интерфейсов, статистику по которым планируется передавать. Это можно сделать в настройках сетевых интерфейсов, значение по умолчанию - 0. Индексы Netflow выступают идентификаторами и не меняются при включении/выключении или изменении интерфейса.



- **Версия протокола** - выберите версию протокола Netflow. Доступны Netflow 5, Netflow 9 (по умолчанию) и Netflow 10 (IPFIX);
- **Интерфейсы учета трафика** - выберите интерфейсы, трафик которых хотите мониторить (доступны *Ethernet-интерфейсы*, Ethernet + *PPTP*/*L2TP*/*PPPoE*, *GRE*. Если не заполнены, статистика не будет экспортироваться;
- **Интервал отправки для активного потока, секунды** - введите временной интервал, через который NGFW будет отправлять на коллектор отчеты по потокам, которые не успели завершиться (информация о завершенных потоках отправляется по завершении). От 60 до 3600 секунд, по умолчанию - 300;
- **IP-адрес коллектора** - введите IP-адрес коллектора данных. Если не заполнен, статистика не будет экспортироваться;
- **Порт коллектора** - введите номер UDP-порта коллектора данных, используемого для приема пакетов Netflow;
- **Интервал отправки шаблона, пакеты** - количество пакетов, через которое на коллектор будет послан шаблон. Минимум 10, максимум 6000, по умолчанию - 20. Доступно только при выборе Netflow 9 или Netflow 10 (IPFIX) в поле **Версия протокола**;
- **Интервал отправки шаблона, секунды** - количество секунд, через которое на коллектор будет послан шаблон. Минимум 60, максимум 86400, по умолчанию - 1800. Доступно только при выборе Netflow 9 или Netflow 10 (IPFIX) в поле **Версия протокола**.

Подсказка: При сборе статистики с интерфейсов Ethernet + PPTP/L2TP/PPPoE будет учитываться трафик не на родительском Veth, а на PPP-интерфейсе (Eppp), трафик с которого инкапсулируется в родительский.

Предупреждение: Данные в Netflow передаются по протоколу UDP.

При выборе в поле **Версия протокола** Netflow 9 или Netflow 10 (IPFIX) поля **Интервал отправки шаблона** фактически отображают допустимые потери данных при потере связи с коллектором или его перезагрузке: пока коллектор не получит шаблон передаваемых данных, отчеты будут игнорироваться.

15.9.1 Структура передаваемых на коллектор данных

Структура заголовка и записей для Netflow 5 доступна по ссылке.

Структура шаблона для Netflow 9 и Netflow 10 (IPFIX) представлена в таблице:

Поле	Код поля	Длина поля, байт	Описание
IPV4_SRC_ADDR	8	4	IP-адрес источника
IPV4_DST_ADDR	12	4	IP-адрес назначения
INPUT_SNMP	10	2	Индекс входящего интерфейса
OUTPUT_SNMP	14	2	Индекс исходящего интерфейса
IN_BYTES	1	8	Количество байт, переданных в потоке
IN_PKTS	2	8	Количество пакетов переданных в потоке
FIRST_SWITCHED	22	4	Время начала потока (sys uptime ms)
LAST_SWITCHED	21	4	Время последнего прохождения трафика в потоке (sys uptime ms)
L4_SRC_PORT	7	2	Порт источника
L4_DST_PORT	11	2	Порт назначения
TCP_FLAGS	6	1	Флаги TCP (суммарно зафиксированные за время наблюдения потока)
PROTOCOL	4	1	Код протокола
SRC_MASK	9	1	Маска IP-адреса источника
DST_MASK	13	1	Маска IP-адреса назначения

16. Правила трафика

16.1 Файрвол

Подсказка: Название службы раздела *Файрвол*: `ideco-firewall-backend`.
Список имен служб для других разделов доступен по *ссылке*.

Принцип работы **Файрвола** – анализ заголовков IP-пакетов и TCP-сегментов, проходящих через интерфейсы сервера, и дальнейшая фильтрация трафика на основании параметров заголовков (IP-адреса, TCP/UDP-порты и флаги).

С помощью **Файрвола** можно создать наборы правил, которые будут разграничивать трафик между различными сетями: локальными, VPN и публичными (интернет). На клиентских устройствах в сетевых параметрах рекомендуется указывать в роли шлюза IP-адрес Ideco NGFW для оптимальной работы политик безопасности (модулей **Контроль приложений** и **Предотвращение вторжений**).

Файрвол Ideco NGFW использует для фильтрации трафика как отдельные интерфейсы, так и зоны - логические объединения сетевых интерфейсов.

Преимущества такого подхода:

- Можно гибко управлять правилами при большом количестве интерфейсов;
- При добавлении/удалении интерфейсов нет необходимости копировать/удалять большое количество правил, достаточно изменить состав нужной зоны;
- Можно выбрать удобные названия для зон (например, **Разработчики**, **Гости**), что сделает правила **Файрвола** более читаемыми.

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

Подсказка: При необходимости добавить большое количество правил Файрвола используйте *отдельное API*.
Правила не будут отображаться в веб-интерфейсе, но будут значительно быстрее работать.

Для обеспечения защиты в NGFW есть преднастроенные и автоматически включаемые системные правила. Используйте пользовательские правила для фильтрации трафика локальной сети и публикации ресурсов.

Для работы инспекций DPI/IPS в правилах **Файрвола** можно подключить **Профили фильтрации трафика** - создать в **Файрволе** разрешающее правило с включенной проверкой через **Контроль приложений** и/или систему **Предотвращения вторжений**. Сами профили настраиваются в разделе *Профили безопасности*.

Предупреждение: Сетевой экран не предназначен для решения связанных с контролем доступа к ресурсам задач исходя из:

- адреса URL;
- доменного имени;
- типа контента на веб-сайтах.

Эти задачи, обычно касающиеся веб-трафика, решаются с помощью *Контент-фильтра*.

Предупреждение: Включение режима удаленного помощника изменяет таблицу правил **Файрвола**. При этом становится доступно подключение по SSH из локальных и внешних сетей.

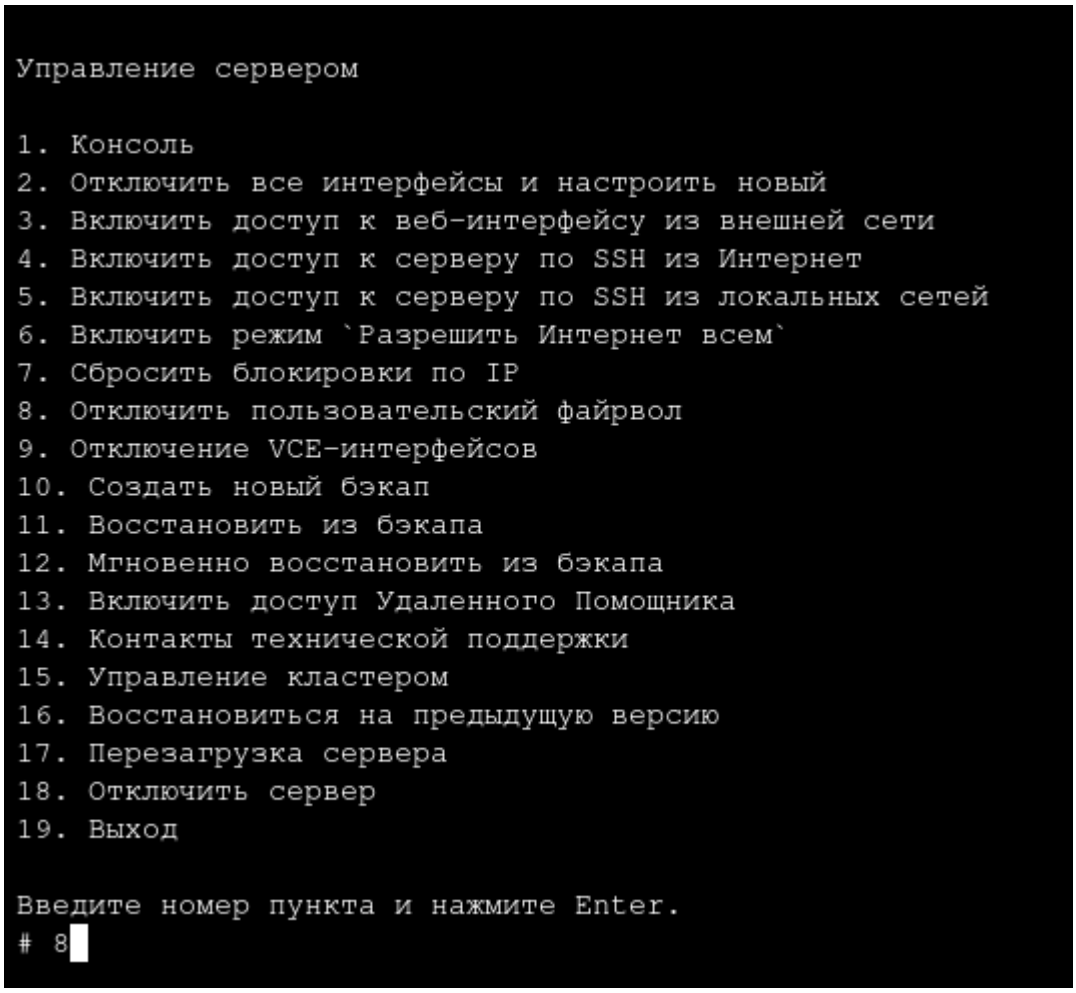
Подсказка: В Ideco NGFW включены connection tracking helpers для протоколов: ftp, sip, netbios-ns, pptp, h323. Для иных протоколов, использующих несколько портов при установлении соединения, работа через NAT не гарантируется.

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

При использовании зон в **Файрволе** следует учесть, что одна зона не может содержать более 64 интерфейсов. Под интерфейсом понимается сетевой интерфейс, настроенный в разделе **Сервисы -> Сетевые интерфейсы**, а также IPsec- и VPN-подключения.

В случае создания некорректных правил (например, запрет доступа в веб-интерфейс Ideco NGFW), отключите пользовательский файрвол из локального меню сервера. Для этого выберите пункт **Отключить**

пользовательский файрвол (введя цифру 8) и нажмите **Enter**:



16.1.1 Счетчик срабатываний

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

Включить опцию можно, нажав на **Отображение данных**.

16.1.2 Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT)

Подсказка: Правила в таблицах имеют приоритет сверху вниз (т. е. верхнее правило приоритетнее нижнего).
По умолчанию используется политика **РАЗРЕШИТЬ**. Если не будут созданы запрещающие правила, все порты и протоколы для пользователей будут разрешены.

Предупреждение: Не рекомендуем создавать FORWARD- и INPUT-правила, запрещающие весь трафик, без предварительного создания разрешающих правил. Это может привести к блокировке доступа к серверу и его функциям.

Для предотвращения блокировки клиентского HTTP/HTTPS-трафика необходимо:

- Создать правило, разрешающее трафик от пользователя;

- Создать правило, разрешающее трафик для специальной зоны источника **Исходящий трафик устройства**.

Для удобства управления правилами в интерфейсе они разбиты на четыре таблицы: FORWARD, DNAT, INPUT и SNAT.

Подсказка: Не рекомендуется при создании правил файрвола с протоколом TCP или UDP указывать порт источника. Это связано с тем, что:

- Порт источника выбирается случайно, и лишь некоторые приложения работают с фиксированным портом;
- Порт источника может подмениться другим при прохождении пакета через NAT.

При создании правил **Файрвола** в качестве **зоны источника** или **зоны назначения** можно выбрать **Специальные** типы:

- **Внешние интерфейсы** - все интерфейсы, используемые для подключения к интернету;
- **Внешние Ethernet-интерфейсы** - все Ethernet-интерфейсы, используемые для подключения к интернету;
- **Внешние VPN-интерфейсы** - все туннельные интерфейсы для подключения к интернету (Ethernet+PPPoE, Ethernet+PPTP, Ethernet+L2TP);
- **IPsec-интерфейсы** - все IPsec-интерфейсы, используемые для site-to-site-подключений к удаленным офисам;
- **Локальные интерфейсы** - все интерфейсы, используемые для подключения к клиентам в локальной сети;
- **Исходящий трафик устройства** - используется для фильтрации исходящего трафика самого устройства Ideco NGFW;
- **Клиентский VPN-трафик** - используется для фильтрации трафика, идущего от клиентов, подключившихся к NGFW по VPN;
- **Любой** - не фильтровать трафик по какому-либо типу интерфейса или зоны.

При наличии большого количества правил в таблицах **Файрвола** воспользуйтесь кнопкой **Фильтры**.

FORWARD

Правила в данной таблице действуют на трафик, проходящий между зонами сервера, т. е. сетью интернет и локальной сетью, а также между локальными сетями. Это основная таблица, в которую могут быть добавлены правила, ограничивающие трафик пользователей.

DNAT (перенаправление портов)

Правила этой таблицы используются для прямого перенаправления портов с внешней зоны на определенные ресурсы во внутренней зоне. Такие правила часто называются правилами проброса портов (port forwarding, port-mapping).

INPUT

Таблица для правил входящего трафика на зоны сервера. Как правило, это трафик для служб сервера (например, почтового сервера).

SNAT

Таблица пользовательских правил для управления трансляцией сетевых адресов.

Чтобы активировать автоматический SNAT для локальных сетей, переведите соответствующую опцию в положение **Включен**. Автоматический SNAT подменяет адреса источников только для следующих диапазонов: `192.168.0.0/16`, `172.16.0.0/12` и `10.0.0.0/8`.

Чтобы подменять адреса источников для других диапазонов или допустить устройства в сеть без сетевой трансляции адресов (правилом «не SNAT»), создайте правило SNAT, нажав на кнопку **Добавить**. Пользовательские правила SNAT имеют приоритет над автоматическим SNAT для локальных сетей.

Создание правил

Для создания правила в нужной таблице нажмите кнопку **Добавить** в левом верхнем углу экрана.

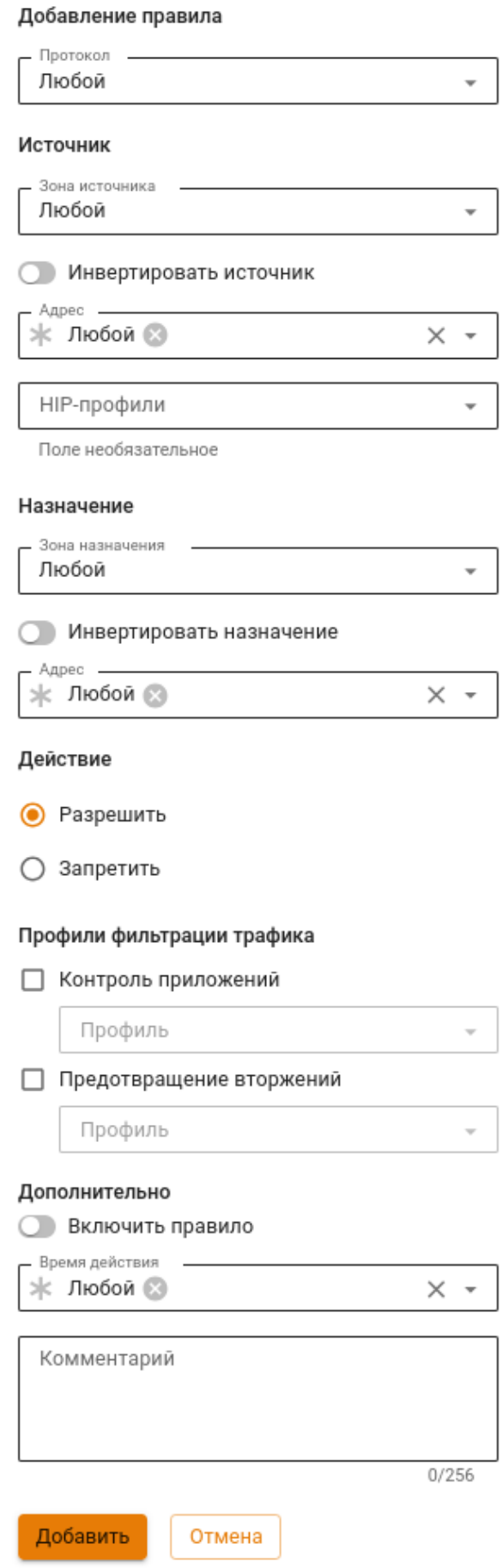
Укажите необходимые параметры и действия правила и нажмите кнопку **Добавить**. Правило будет добавлено в конец списка. Если необходимо, измените его приоритет кнопками ↑ ↓.

Подсказка: Если в строке **Протокол** выбрать из списка параметр **Любой**, то правило будет действовать на весь трафик.

Внимание: Важные моменты при создании правил:

- При создании правил для фильтрации веб-трафика из локальных сетей (80, 443 TCP-порты) для полноценной работы правила в поле **Зона источника** должен указываться объект **Любой**. Если будет указан иной объект, то правило не будет обрабатывать веб-трафик;
- Не используйте зону, указанную в разделе **VPN-подключения -> Основное**, для блокировки TCP. В противном случае HTTP- и HTTPS-трафик через эту зону не будет заблокирован.

Создание FORWARD-правила:


Добавление правила
Протокол
Любой
Источник
Зона источника
Любой
Инвертировать источник
Адрес
Любой
HIP-профили
Поле необязательное
Назначение
Зона назначения
Любой
Инвертировать назначение
Адрес
Любой
Действие
Разрешить
Запретить
Профили фильтрации трафика
Контроль приложений
Профиль
Предотвращение вторжений
Профиль
Дополнительно
Включить правило
Время действия
Любой
Комментарий
0/256
Добавить
Отмена

- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).

Источник

- **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, *созданные пользователем зоны* или **Специальные** типы;
- **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**;
- **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200;
- **HIP-профили** - профиль, соответствующий устройству, от которого исходит трафик.

Назначение

- **Зона назначения** - интерфейс или группа интерфейсов, в которые входит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны или **Специальные типы**;
- **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**;
- **Адрес** - в этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. Максимальное количество объектов в поле - 200.

Действия

- **Запретить** - запрещает трафик;
- **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.

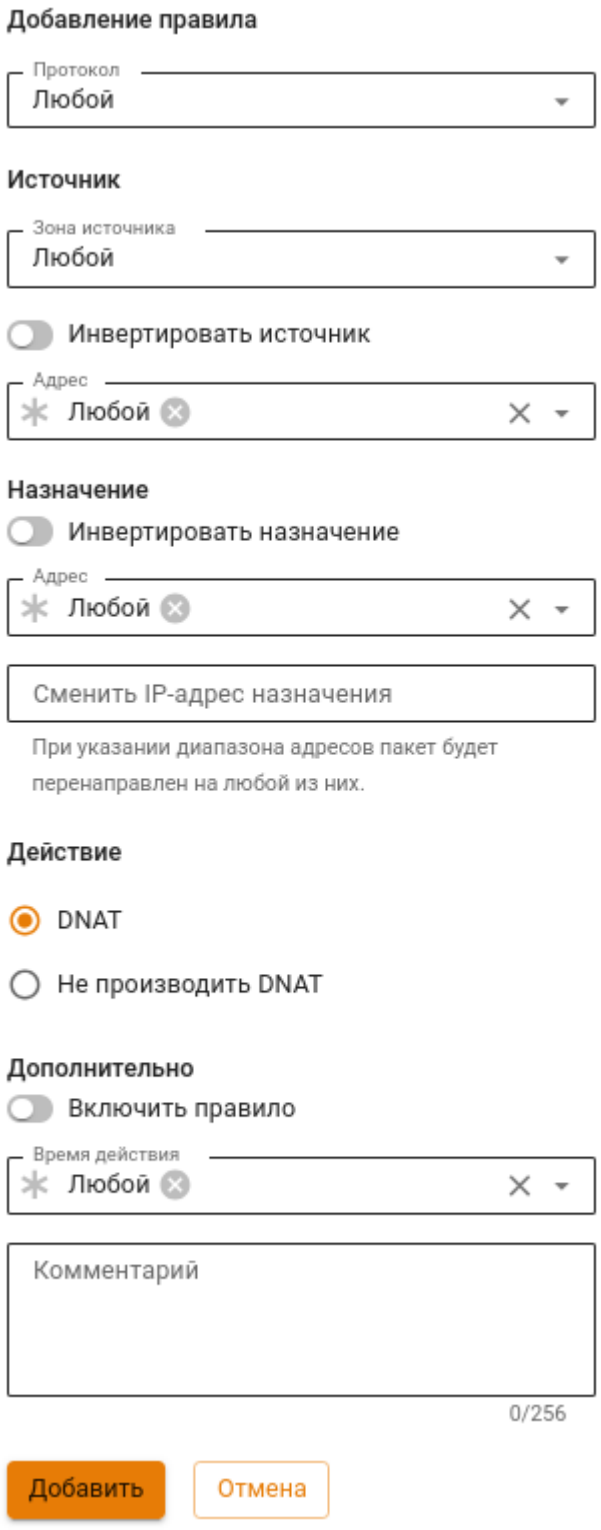
Профили фильтрации трафика

- **Контроль приложений** - выберите профиль *Контроля приложений*, которым требуется фильтровать трафик;
- **Предотвращение вторжений** - выберите профиль системы *Предотвращения вторжений*, которым требуется фильтровать трафик.

Дополнительно

- **Включить правило** - опция позволяет выбрать, будет ли правило включено или выключено при создании. По умолчанию правило выключено;
- **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в *Объектах*;
- **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

Создание DNAT-правила:



- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).

Источник

- **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, *созданные пользователем зоны* или **Специальные** типы:
  - **Внешние интерфейсы** - все интерфейсы, используемые для подключения к интернету;
  - **Внешние Ethernet-интерфейсы** - все Ethernet-интерфейсы, используемые для подключения к

интернету;

  - **Внешние VPN-интерфейсы** - все туннельные интерфейсы для подключения к интернету (Ethernet+PPPoE, Ethernet+PPTP, Ethernet+L2TP);
  - **IPsec-интерфейсы** - все IPsec-интерфейсы, используемые для site-to-site-подключений к удаленным офисам;
  - **Локальные интерфейсы** - все интерфейсы, используемые для подключения к клиентам в локальной сети;
  - **Исходящий трафик устройства** - используется для фильтрации исходящего трафика самого устройства Ideco NGFW;
  - **Клиентский VPN-трафик** - используется для фильтрации трафика, идущего от клиентов, подключившихся к NGFW по VPN;
  - **Любой** - не фильтровать трафик по какому-либо типу интерфейса или зоны.

- **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**;
- **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.

Назначение

- **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**;
- **Адрес** - в этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. Максимальное количество объектов в поле - 200;
- **Сменить IP-адрес назначения** - при указании диапазона адресов пакет будет перенаправлен на любой из них;
- **Сменить порт назначения** - при указании диапазона портов пакет будет перенаправлен в порт с тем же номером, на который он пришел, если этот порт попадает в указанный диапазон.

Действия

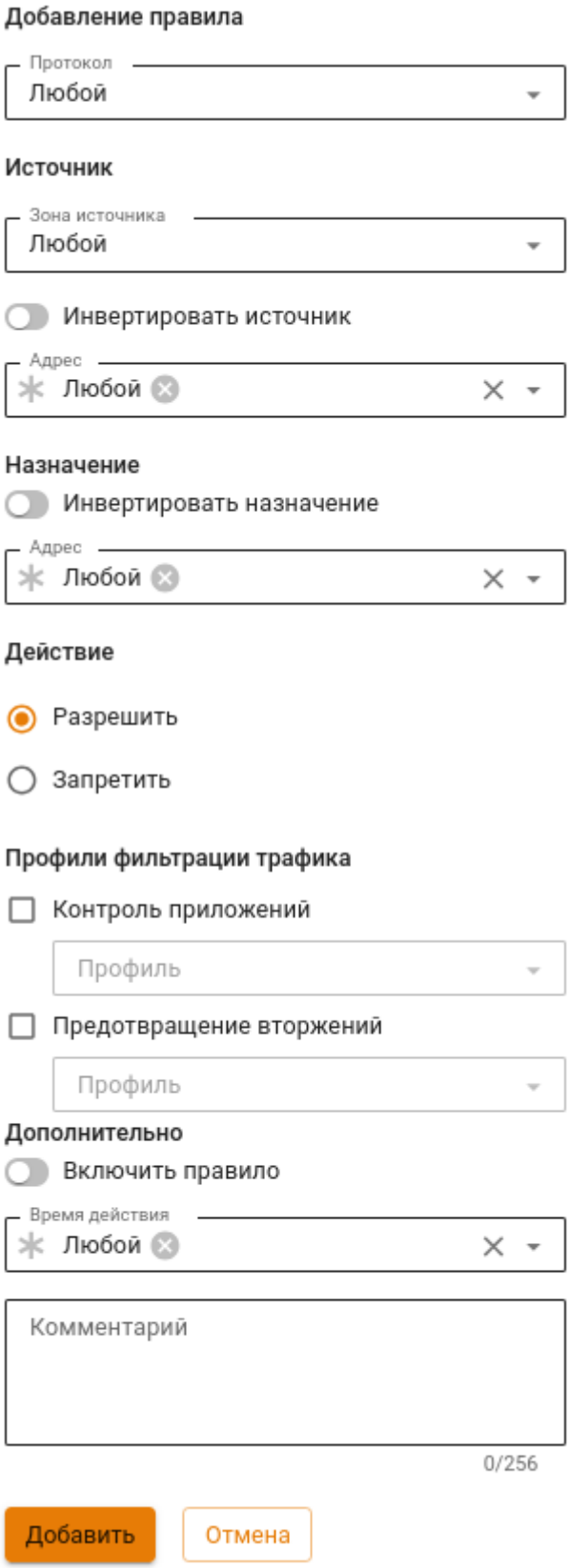
- **DNAT** - транслирует адреса назначения, тем самым позволяет перенаправить входящий трафик. Ниже в поле **Изменить IP-адрес назначения** можно указать один IP-адрес или диапазон (при указании диапазона IP-адресов пакет будет перенаправлен на любой из них). Аналогично, если при создании правила были указаны протоколы TCP или UDP, то появится поле **Сменить порт назначения**. С помощью этой возможности можно прозрачно переадресовать входящий трафик на другой адрес или порт;
- **Не производить DNAT** - отменяет действие DNAT для трафика, удовлетворяющего критериям правила.

Дополнительно

- **Включить правило** - опция позволяет выбрать, будет ли правило включено или выключено при создании. По умолчанию правило выключено;
- **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в *Объектах*;

- **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

Создание INPUT-правила:



- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).

Источник

- **Зона источника** - интерфейс или группа интерфейсов, из которых приходит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, *созданные пользователем зоны* или **Специальные** типы:
  - **Внешние интерфейсы** - все интерфейсы, используемые для подключения к интернету;
  - **Внешние Ethernet-интерфейсы** - все Ethernet-интерфейсы, используемые для подключения к интернету;
  - **Внешние VPN-интерфейсы** - все внешние VPN-интерфейсы (PPPoE, PPTP, L2TP), используемые для подключения к интернету;
  - **IPsec-интерфейсы** - все IPsec-интерфейсы, используемые для site-to-site-подключений к удаленным офисам;
  - **Локальные интерфейсы** - все интерфейсы, используемые для подключения к клиентам в локальной сети;
  - **Исходящий трафик устройства** - используется для фильтрации исходящего трафика самого устройства Ideco NGFW;
  - **Клиентский VPN-трафик** - используется для фильтрации трафика, идущего от клиентов, подключившихся к NGFW по VPN;
  - **Любой** - не фильтровать трафик по какому-либо типу интерфейса или зоны.
- **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**;
- **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200.

Назначение

- **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**;
- **Адрес** - в этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порт назначения** - указывается при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. Максимальное количество объектов в поле - 200.

Действия

- **Запретить** - запрещает трафик;
- **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика.

Профили фильтрации трафика

- **Контроль приложений** - выберите профиль *Контроля приложений*, которым требуется фильтровать трафик;
- **Предотвращение вторжений** - выберите профиль системы *Предотвращения вторжений*, которым требуется фильтровать трафик.

Дополнительно

- **Включить правило** - опция позволяет выбрать, будет ли правило включено или выключено при создании. По умолчанию правило выключено;

- **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в *Объектах*;
- **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

Создание SNAT-правила:

Добавление правила

Протокол
Любой

Источник

Инвертировать источник

Адрес
Любой

Сменить IP-адрес источника

Формат: IP-адрес или диапазон. Только если на сетевом интерфейсе несколько IP-адресов и необходим SNAT от конкретного IP-адреса.

Назначение

Зона назначения
Любой

Инвертировать назначение

Адрес
Любой

Действие

SNAT

Не производить SNAT

Дополнительно

Включить правило

Время действия
Любой

Комментарий

0/256

Добавить Отмена

- **Протокол** - протокол передачи данных (UDP/TCP/ICMP/GRE/ESP/AH, либо **Любой**).

Источник

- **Инвертировать источник** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Источник**;
- **Адрес** - IP-адрес источника трафика (src), проходящего через шлюз. В этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порты источника** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. **Указывать не рекомендуем**. Максимальное количество объектов в поле - 200;
- **Сменить IP-адрес источника** - заполняется, только если на сетевом интерфейсе несколько IP-адресов и необходим SNAT от конкретного IP-адреса. Можно указать IP-адрес или диапазон IP-адресов, например, 192.168.10.2-192.168.10.15.

Назначение

- **Зона назначения** - интерфейс или группа интерфейсов, в которые входит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, *созданные пользователем зоны* или **Специальные** типы:
  - **Внешние интерфейсы** - все интерфейсы, используемые для подключения к интернету;
  - **Внешние Ethernet-интерфейсы** - все Ethernet-интерфейсы, используемые для подключения к интернету;
  - **Внешние VPN-интерфейсы** - все внешние VPN-интерфейсы (PPPoE, PPTP, L2TP), используемые для подключения к интернету;
  - **IPsec-интерфейсы** - все IPsec-интерфейсы, используемые для site-to-site-подключений к удаленным офисам;
  - **Локальные интерфейсы** - все интерфейсы, используемые для подключения к клиентам в локальной сети;
  - **Исходящий трафик устройства** - используется для фильтрации исходящего трафика самого устройства Ideco NGFW;
  - **Клиентский VPN-трафик** - используется для фильтрации трафика, идущего от клиентов, подключившихся к NGFW по VPN;
  - **Любой** - не фильтровать трафик по какому-либо типу интерфейса или зоны.
- **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Адрес**;
- **Адрес** - в этом поле могут быть указаны IP-адреса, диапазоны IP-адресов, сети, домены (раздел *Объекты*), страны или пользователи и группы (при смене их IP-адресов, файрвол автоматически это учтет). Максимальное количество объектов в поле - 200;
- **Порты назначения** - указываются при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*. Максимальное количество объектов в поле - 200.

Действия

- **SNAT** - транслирует адреса источника;
- **Не производить SNAT** - отменяет действие SNAT для трафика, удовлетворяющего критериям правила.

Дополнительно

- **Включить правило** - опция позволяет выбрать, будет ли правило включено или выключено при создании. По умолчанию правило выключено;

- **Время действия** - время действия правила. Указываются временные промежутки (например, **рабочее время**), которые определяются в *Объектах*;
- **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

Внимание: С 18 версии NGFW правила Файрвола, которые блокировали трафик за счет перехвата DNS в предыдущих версиях, не смогут его блокировать. Чтобы это исправить, создайте и включите правила с профилями IPS и DPI в разделе **Правила трафика -> Файрвол -> INPUT**.

16.1.3 Примеры создания правил файрвола

Основное

Настройка правил файрвола для IPsec-подключений:

Чтобы настроить правило файрвола для IPsec-подключений, выберите в поле **Зона источника** или **Зона назначения** настроенное IPsec-подключение.

Портмаппинг, DNAT, публикация сервера в локальной сети:

Примеры данных настроек подробно описаны в статьях раздела *Публикация ресурсов*.

Блокировка различных ресурсов средствами файрвола:

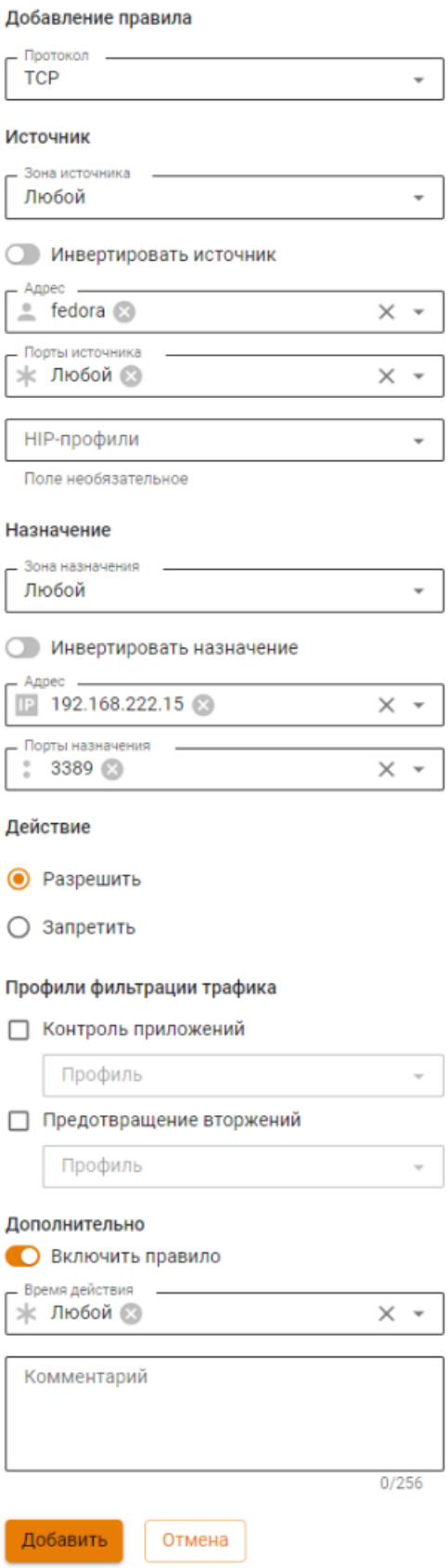
Вопросы блокировки различных ресурсов: программ удаленного управления (AmmyAdmin и TeamViewer), мессенджеров и другого ПО - описаны в разделе *Блокировка популярных ресурсов*.

Доступ к терминальному серверу для определенного пользователя:

1. На вкладке **FORWARD** нажмите **Добавить**.

2. Заполните следующие поля:

- **Протокол** - выберите TCP;
- **Адрес** - выберите пользователя или группу пользователей;
- **Назначения** - укажите адрес терминального сервера;
- **Порты назначения** - укажите порт 3389;
- **Действие** - Разрешить;
- **Дополнительно** - включите правило.



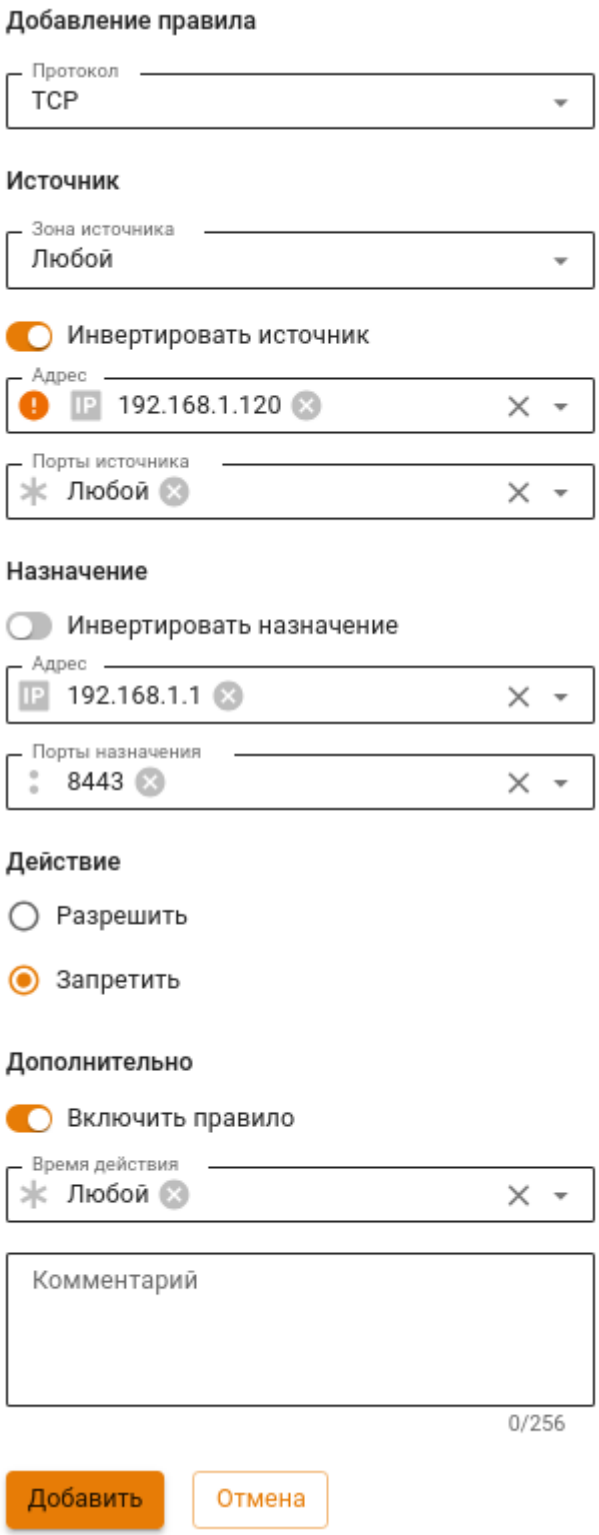
3. Нажмите **Добавить**.

Блокировка доступа к веб-интерфейсу (порт 8443) всем, кроме определенного адреса:

1. Перейдите в раздел **Правил трафика -> Файрвол**.

2. Перейдите на вкладку **INPUT**.

3. Создайте правило, заполнив поля, как на скриншоте, и включите его:



- Доступ к веб-интерфейсу будет разрешен только с IP-адреса **192.168.1.120**.
- **192.168.1.1** - IP-адрес Ideco NGFW в локальной сети.

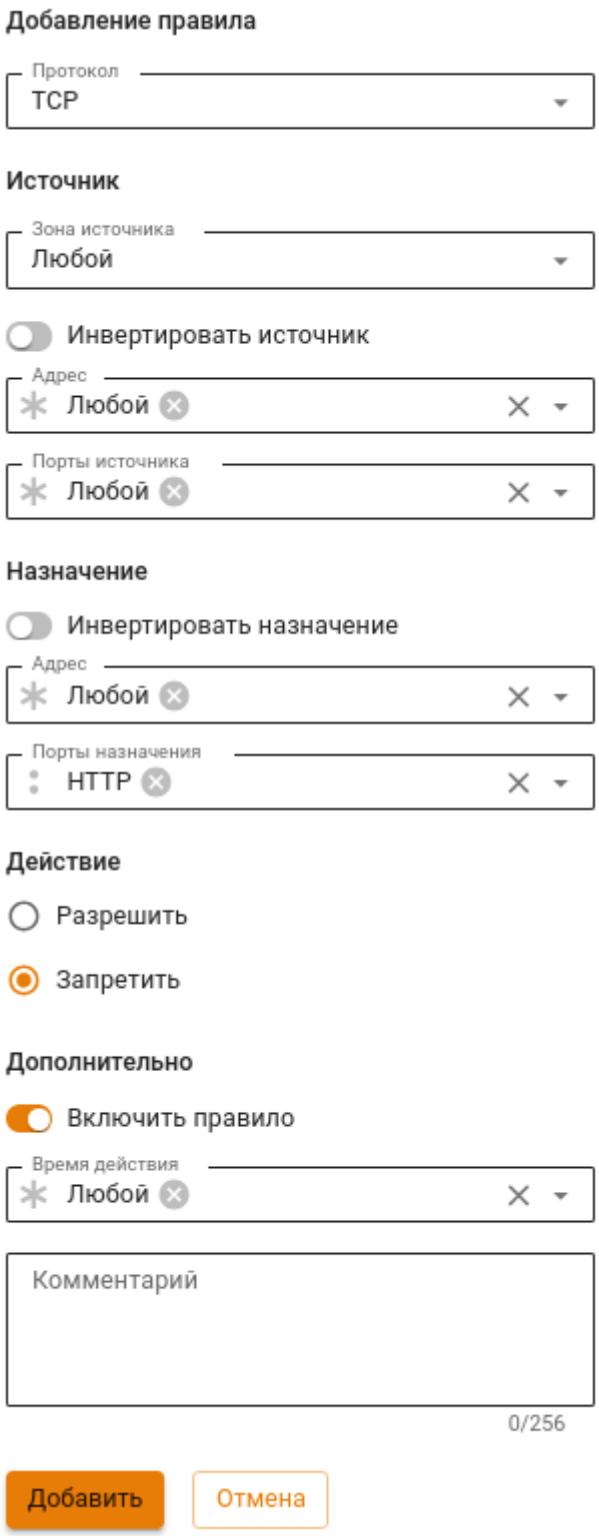
Блокировка 80 порта Ideco NGFW:

80 TCP порт используется для выпуска сертификатов Let`s Encrypt.

1. Перейдите в раздел **Правил трафика -> Файрвол**.

2. Перейдите на вкладку **INPUT**.

3. Создайте правило, заполнив поля, как на скриншоте, и включите его:

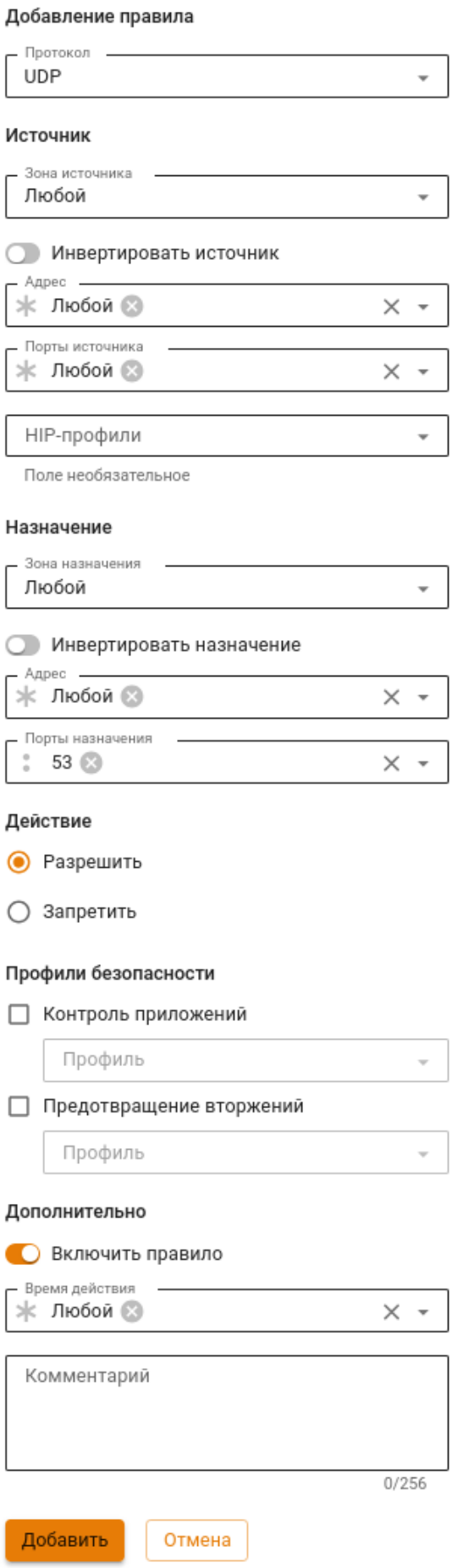


Разрешение DNS-запросов:

1. Перейдите в раздел **Правил трафика -> Файрвол**.

2. Перейдите на вкладку **FORWARD**.

3. Создайте правило, заполнив поля, как на скриншоте, и включите его:


Добавление правила
Протокол
UDP
Источник
Зона источника
Любой
Инвертировать источник
Адрес
Любой
Порты источника
Любой
HIP-профили
Поле необязательное
Назначение
Зона назначения
Любой
Инвертировать назначение
Адрес
Любой
Порты назначения
53
Действие
Разрешить
Запретить
Профили безопасности
Контроль приложений
Профиль
Предотвращение вторжений
Профиль
Дополнительно
Включить правило
Время действия
Любой
Комментарий
0/256
Добавить
Отмена

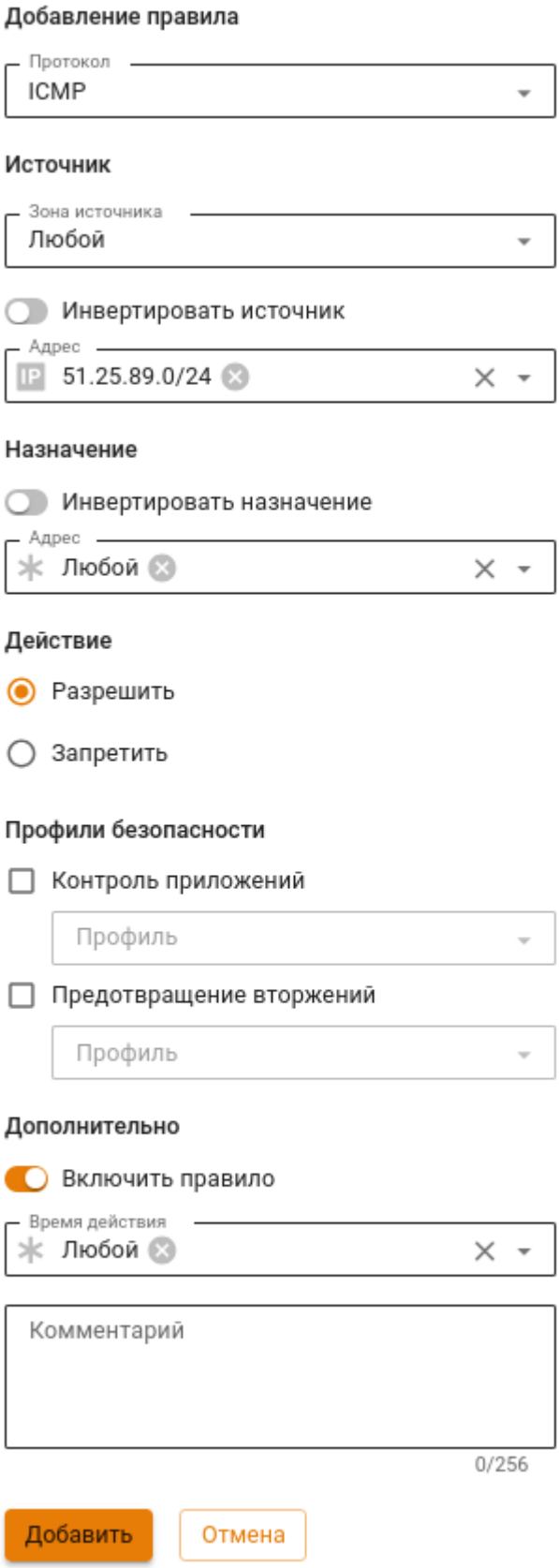
Для работы протокола DNS может быть не достаточно правила с протоколом UDP, поскольку DNS использует в качестве транспорта не только UDP, но и TCP. Для решения задачи создайте аналогичное правило с протоколом TCP, используя кнопку **Клонировать** в таблице правил.

Доступ до Ideco NGFW только из определенной внешней сетей:

1. Перейдите в раздел **Правил трафика -> Файрвол**.

2. Перейдите на вкладку **INPUT**.

3. Создайте правило, заполнив поля, как на скриншоте, и включите его:



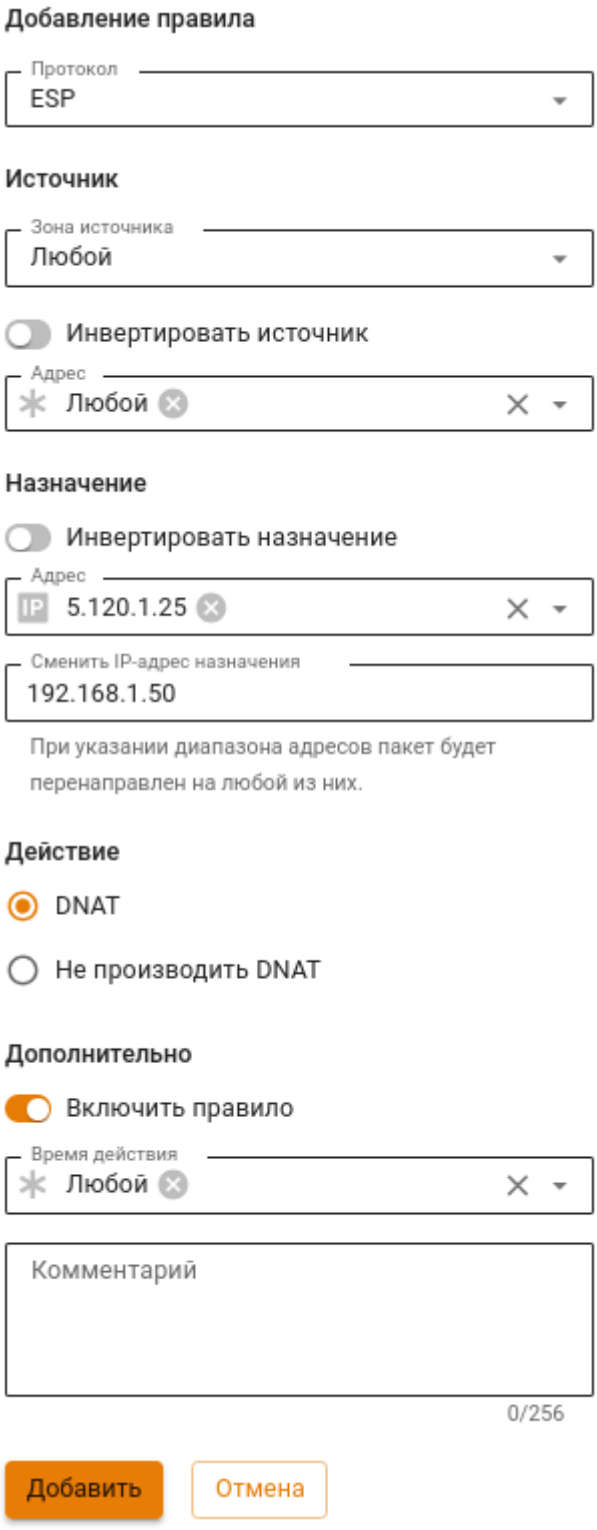
Правило разрешит трафик до Ideco NGFW из внешней сети 51.25.89.0/24.

DNAT-правило для работы site-to-site IPsec с устройством в локальной сети:

1. Перейдите в раздел **Правил трафика -> Файрвол**.

2. Перейдите на вкладку **DNAT**.

3. Создайте правило, заполнив поля, как на скриншоте, и включите его:



- **5.120.1.25** - IP-адрес Ideco NGFW во внешней сети.
- **192.168.1.50** - IP-адрес устройства в локальной сети.

Для полноценной работы IPsec создайте такое же правило с протоколом AH, нажав Клонировать. Помимо этого нужно создать DNAT-правило с протоколом UDP и портами 500,4500.

16.1.4 Логирование

Принцип работы

Весь поступающий трафик в первую очередь проходит через правила вкладки **Логирование**. Если трафик соответствует критериям таблицы **Трафик для логирования**, то на пакете ставится виртуальная метка о необходимости логирования. По умолчанию метки нет.

Далее трафик проходит через правила в *таблицах Файрвола*. Если при срабатывании правила на трафике стояла метка логирования, то в логи попадают следующие данные:

- стандартные поля логирования;
- атрибуты пакета, с которым произошло событие (протокол, порты и IP-адреса);
- название таблицы **Файрвола**;
- идентификатор правила **Файрвола**;
- действие, которое произошло.

Для просмотра логов перейдите в раздел **Отчеты и журналы -> *Системный журнал*** и настройте фильтр событий (Служба - равен - ideco-nflog). Логи могут отправляться в сторонние коллекторы через *syslog*.

Подсказка: Включите опцию **Логировать срабатывания правил** для начала логирования.

Такая система ограничений нужна для исключения неподходящих правил **Файрвола** из логирования. Логирование срабатываний всех правил **Файрвола** требует дополнительных ресурсов на сервере и затрудняет отладку правил. Если для нормальной работы логирование не требуется, рекомендуем его отключить.

Трафик для логирования

Создайте и включите в таблице правило для трафика. Если сработает правило **Файрвола** с трафиком, подходящим под правило логирования, то срабатывание правила **Файрвола** будет залогировано.

> **Внимание:** Если ни одно правило в таблице не задано, срабатывание правил логироваться не будет.
>
> Правила отметки трафика могут снять отметку с помощью действия **Не логировать** для трафика, помеченного ранее действием **Логировать**.

Предоставляется возможность гибкой выборки трафика, который подлежит логированию, за счет правил таблицы **Логирование**.

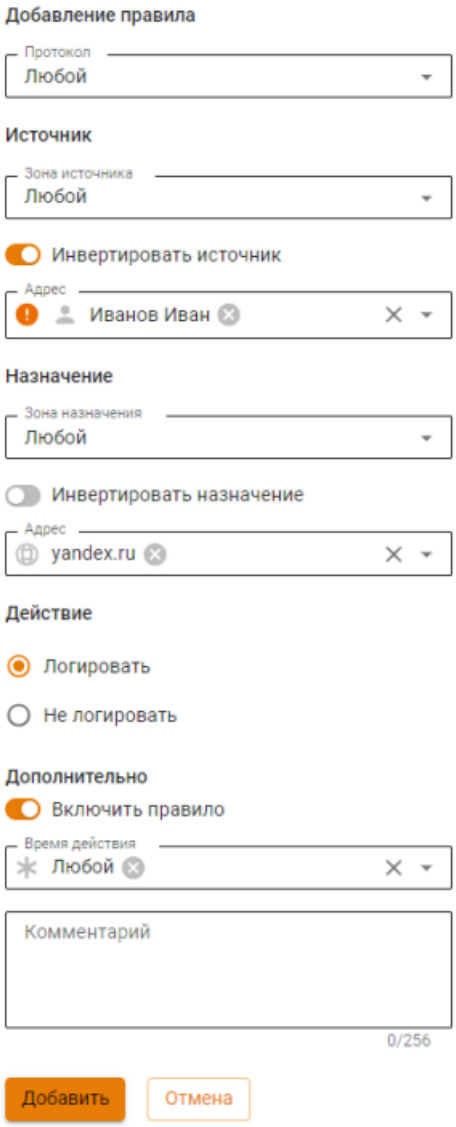
Пример: требуется настроить логирование всего трафика на yandex.ru, кроме трафика от пользователя Иванова Ивана:

1. В поле **Источник** выберите *Иванова Ивана* и переведите опцию **Инвертировать источник** в положение **Включен**.

2. В поле **Назначение** выберите `yandex.ru`.

3. Выберите действие **Логировать**.

4. В поле **Дополнительно** включите правило:



16.1.5 Тестирование правил

На вкладке создаются кейсы для тестирования правил таблицы FORWARD и INPUT.

Тест (кейс) - это конкретный пример, в котором происходит тестирование доступа до определенного IP-адреса с учетом правил таблицы **Файрвола**. Кейс является единицей тестирования.

Создание тестов

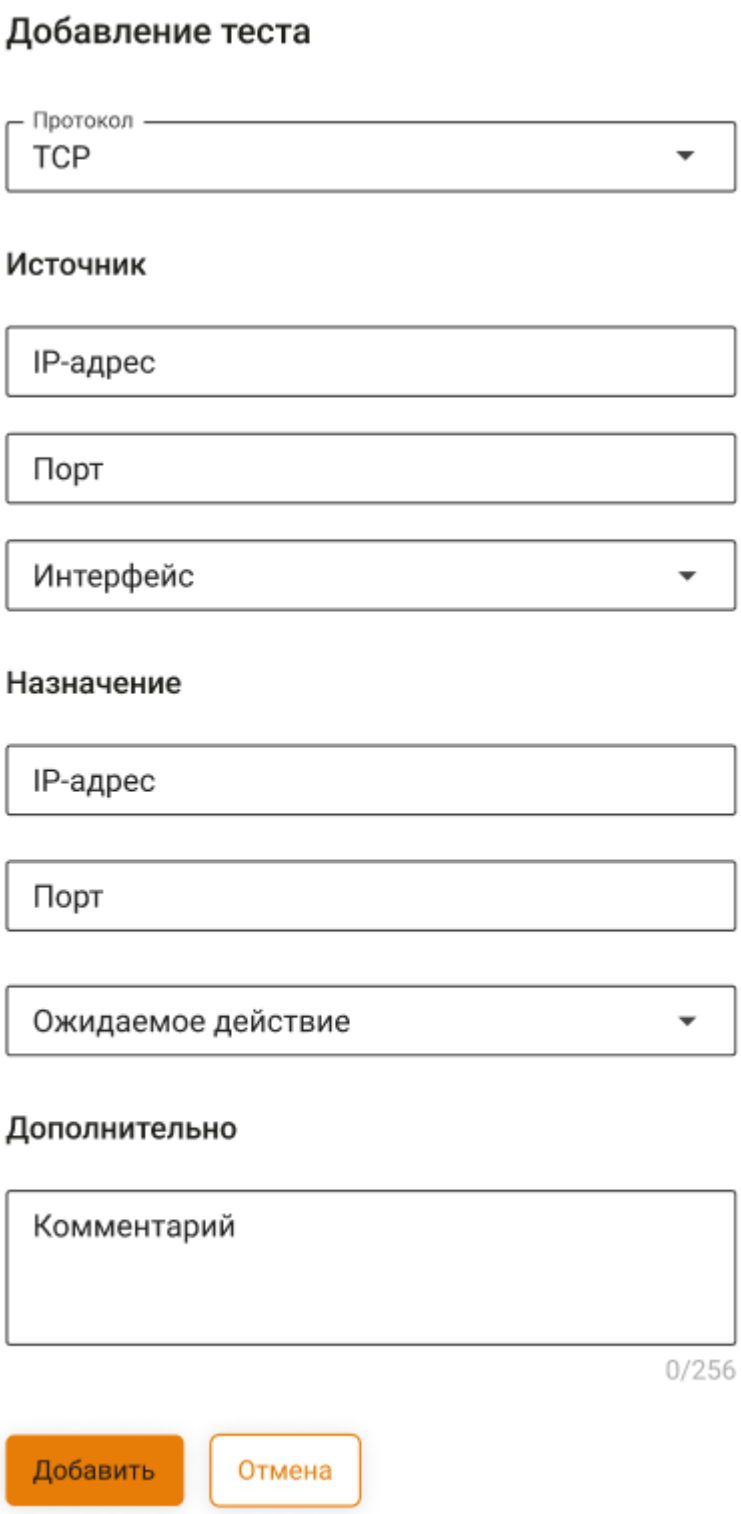
Подсказка: В качестве интерфейса источника можно выбрать следующие типы интерфейсов:

- Тунельные (GRE)
- Локальный Ethernet
- Внешний Ethernet
- Внешний Ethernet + PPTP
- Внешний Ethernet + L2TP
- Внешний Ethernet + PPPoE

Для создания теста выполните действия:

1. Перейдите в раздел **Правила трафика -> Файрвол -> Тестирование правил** и нажмите **Добавить**:

2. Заполните поля:

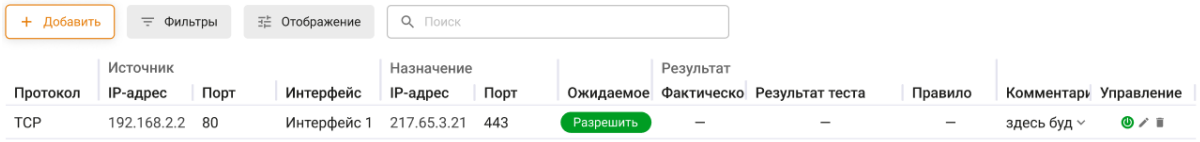


- **Протокол** (**TCP/UDP**);

- **IP-адрес** источника и назначения;
- **Порт** источника и назначения;
- **Интерфейс** источника;
- **Ожидаемое действие** (Разрешить или Запретить);
- **Комментарий**.

3. Нажмите **Добавить**.

Созданные тесты добавляются в таблицу:



Запуск и результат тестирования кейса

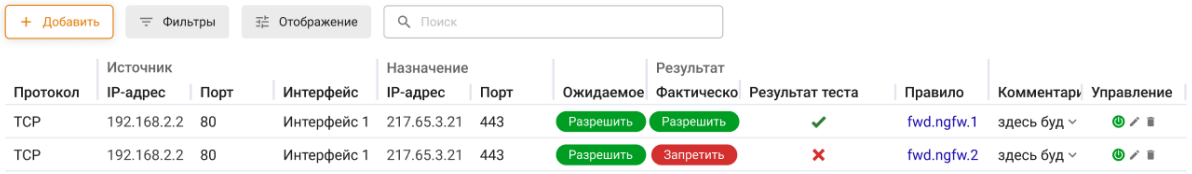
Запуск тестирования кейса не происходит автоматически при его добавлении. Для запуска:

1. Включите нужный кейс  .

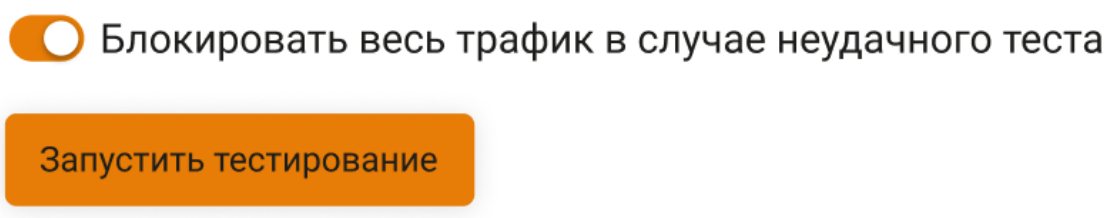
2. Нажмите **Запустить тестирование** в левом нижнем углу вкладки.

> **Предупреждение:** Если кейс не включить, то его тестирование осуществляться не будет.

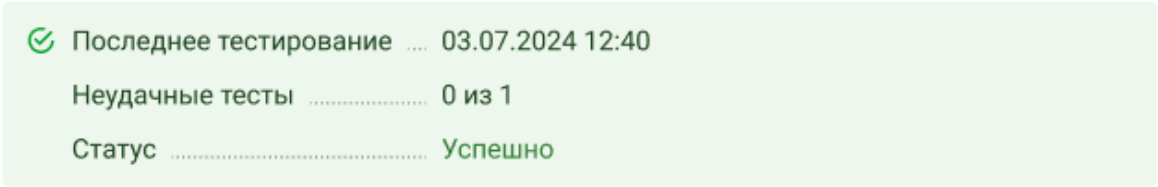
При совпадении ожидаемого и фактического действия тестирование кейса считается успешным:



Если у выбранного кейса **Интерфейс** источника был удален (отображается **Удалено** в столбце **Интерфейс**), тестирование кейса завершится с фактическим действием **Запретить**.

> **Предупреждение:** Если опция **Блокировать весь трафик в случае неудачного теста** включена (**не рекомендуем**), то любой неуспешный результат теста (обозначен ) приведет к блокировке всего трафика через NGFW. Единственный способ снятия блокировки - тестирование кейса без ошибок. Отключение опции нажатием на переключатель не сработает:
>
> 
>

В правом нижнем углу вкладки представлены сведения о последнем тестировании: текущий статус (**Успешно/Ошибка**), время проведения и количество неуспешных кейсов (из числа включенных в столбце **Управление**):



Повторный запуск сбрасывает результаты предыдущего тестирования.

16.1.6 Предварительная фильтрация

Основное

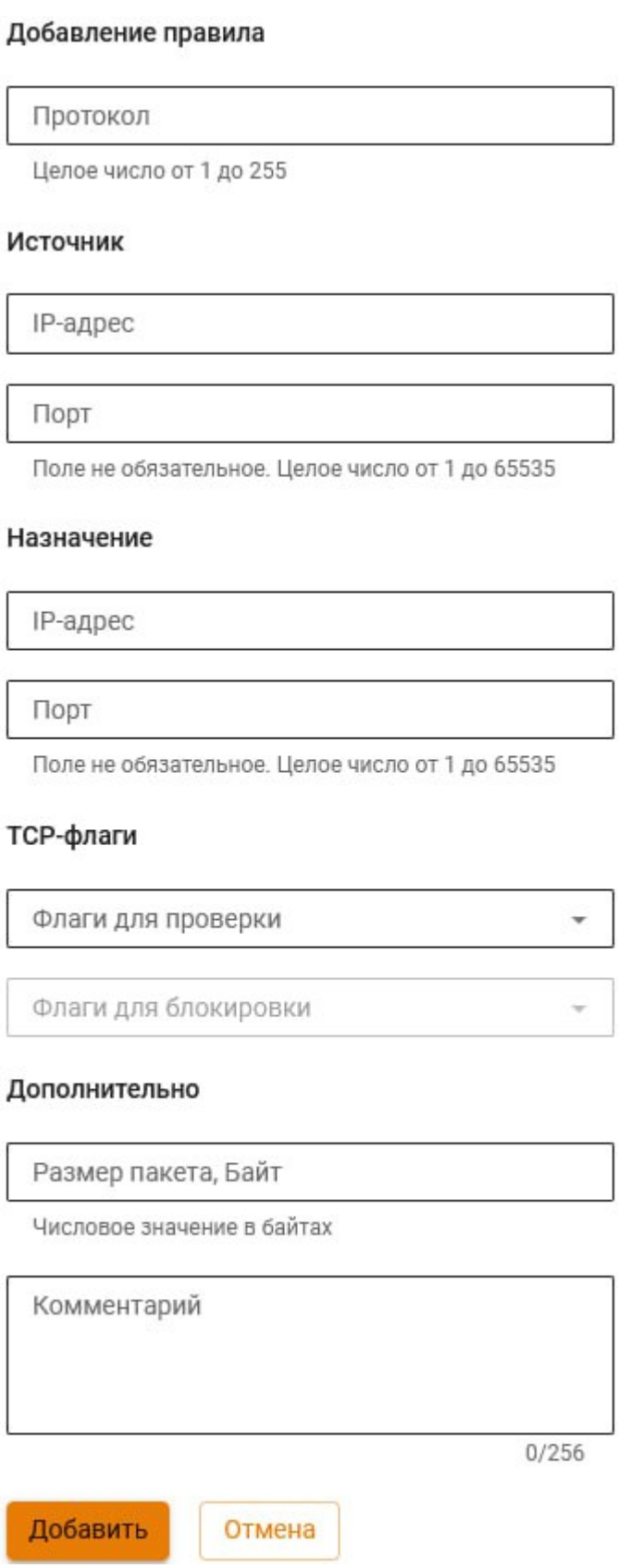
Вкладка **Предварительная фильтрация** позволяет заблокировать весь трафик, попадающий под условия таблицы, до просмотра таблиц **Файрвола** (например, **FORWARD** или **INPUT**). Используйте этот раздел, если требуется фильтрация пакетов на уровне TCP/IP.

Подсказка: При неправильно созданных правилах доступ к веб-интерфейсу может быть заблокирован (например, блокировка протокола TCP с проверкой и блокировкой флага **SYN**). Для возвращения доступа к веб-интерфейсу отключите **Пользовательский файрвол** через локальное меню сервера или включите режим **Разрешить интернет всем**.

Для создания правила выполните действия:

1. Перейдите в раздел **Правила трафика -> Файрвол -> Предварительная фильтрация** и нажмите **Добавить**.

2. Заполните поля правила:



- **Протокол** - укажите номер протокола из таблицы. Номер может быть в диапазоне от 0 до 146 включительно;
- **Источник**:
  - **IP-адрес** - укажите IP-адрес источника;

- **Порт** - укажите порт источника;

- **Назначение**:
  - **IP-адрес** - укажите IP-адрес назначения;
  - **Порт** - укажите порт назначения;
- **TCP-флаги**:
  - **Флаги для проверки** - укажите флаги TCP, которые будут проверяться. В этом поле могут быть указаны флаги: **SYN**, **ACK**, **FIN**, **RST**, **URG**, **PSH**;
  - **Флаги для блокировки** - укажите флаги TCP, которые будут заблокированы. Флаг будет доступен для блокировки, только если он содержится в поле **Флаги для проверки**;
- **Дополнительно**:
  - **Размер пакета, Байт** - укажите размер пакета в байтах;
  - **Комментарий**.

3. Нажмите **Добавить**.

16.1.7 Аппаратная фильтрация

На вкладке можно настроить пакетную фильтрацию трафика на основе сетевых и физических адресов отправителей и (или) получателей. Пакеты будут блокироваться на аппаратном уровне без участия центрального процессора, с использованием вычислительных мощностей сетевой карты.

В Ideco NGFW блокировка будет происходить в соответствии с выбранным режимом фильтрации. Одновременно может работать фильтрация по MAC-адресу источника или один из видов фильтрации по IP.

Созданные на вкладке правила применяются сразу ко всем поддерживаемым сетевым адаптерам, найденным в системе.

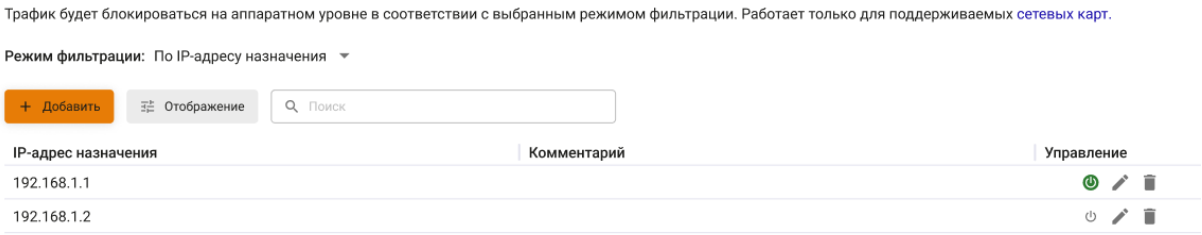
Список поддерживаемых сетевых карт

PCI-идентификатор	Модель адаптера
0x8086:0x0CF8	Ethernet Controller X710 Intel(R) FPGA Programmable Acceleration Card N3000 for Networking
0x8086:0x0D58	Ethernet Controller XXV710 Intel(R) FPGA Programmable Acceleration Card N3000 for Networking
0x8086:0x1572	Ethernet Controller X710 for 10GbE SFP+
0x8086:0x1574	Ethernet Controller XL710 Emulation
0x8086:0x1580	Ethernet Controller XL710 for 40GbE backplane
0x8086:0x1581	Ethernet Controller X710 for 10GbE backplane
0x8086:0x1583	Ethernet Controller XL710 for 40GbE QSFP+
0x8086:0x1584	Ethernet Controller XL710 for 40GbE QSFP+
0x8086:0x1585	Ethernet Controller X710 for 10GbE QSFP+
0x8086:0x1586	Ethernet Controller X710 for 10GBASE-T
0x8086:0x1587	Ethernet Controller XL710 for 20GbE backplane
0x8086:0x1588	Ethernet Controller XL710 for 20GbE backplane
0x8086:0x158A	Ethernet Controller XXV710 for 25GbE backplane
0x8086:0x158B	Ethernet Controller XXV710 for 25GbE SFP28
0x8086:0x15FF	Ethernet Controller X710 for 10GBASE-T
0x8086:0x104F	Ethernet Controller X710 for 10 Gigabit backplane
0x8086:0x104E	Ethernet Controller X710 for 10 Gigabit SFP+
0x8086:0x0DD2	Ethernet Network Adapter I710

Создание правил

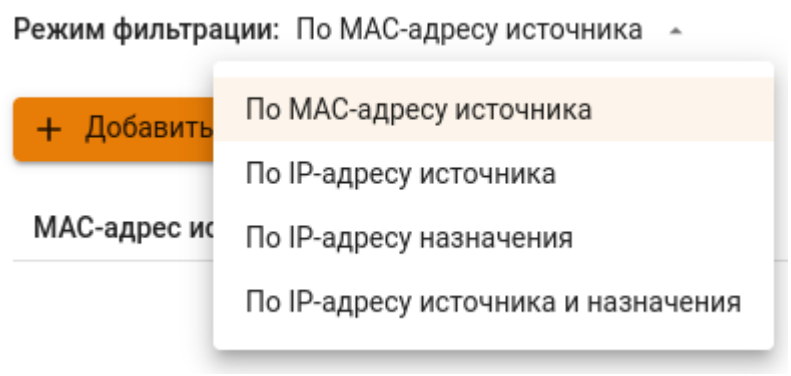
Подсказка: Администратор может создать не более 2500 правил каждого типа фильтрации.

Созданные правила отображаются в таблице в зависимости от выбранного режима фильтрации:



Чтобы создать правило определенного типа, выполните действия:

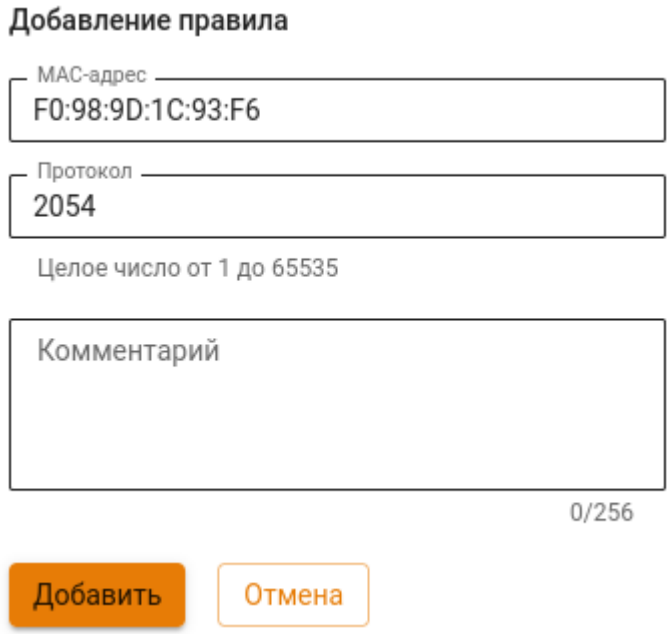
1. Выберите режим фильтрации, нажмав на кнопку в левом верхнем углу:



- По MAC-адресу источника;
- По IP-адресу источника;
- По IP-адресу назначения;
- По IP-адресу источника и назначения.

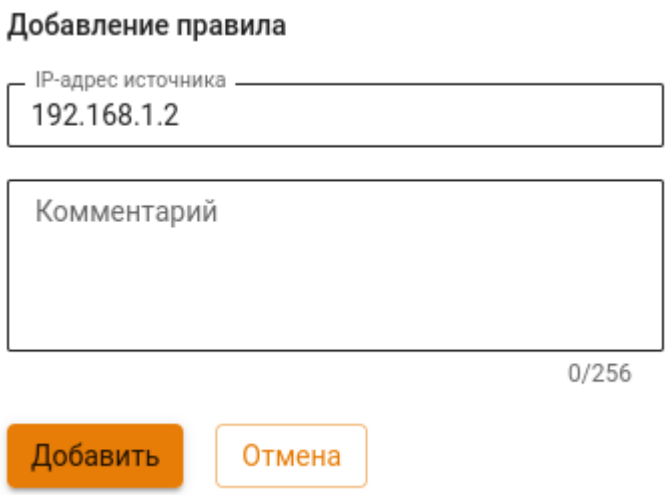
2. Нажмите **Добавить** и заполните поля:

Фильтрация по MAC-адресу источника:



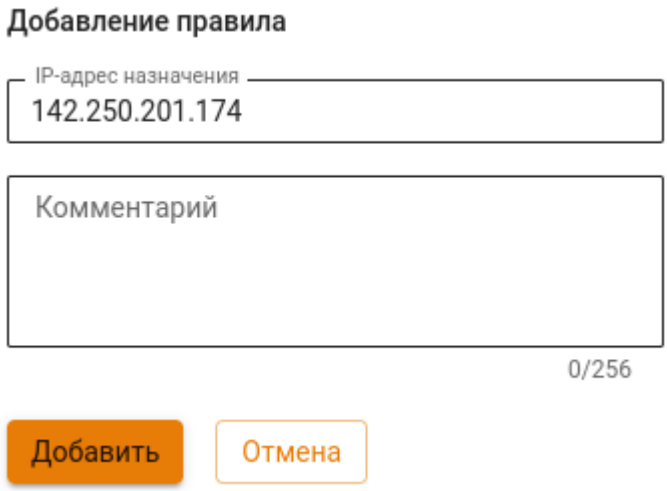
- **MAC-адрес** - введите физический адрес источника трафика;
- **Протокол** - введите номер протокола сетевого уровня. **Не указывайте протокол IPv4** (значение 2048), для фильтрации на сетевом уровне используйте правила *По IP-адресу источника*, *По IP-адресу назначения*, *По IP-адресу источника и назначения*;
- **Коментарий** - поле необязательное.

Фильтрация по IP-адресу источника:



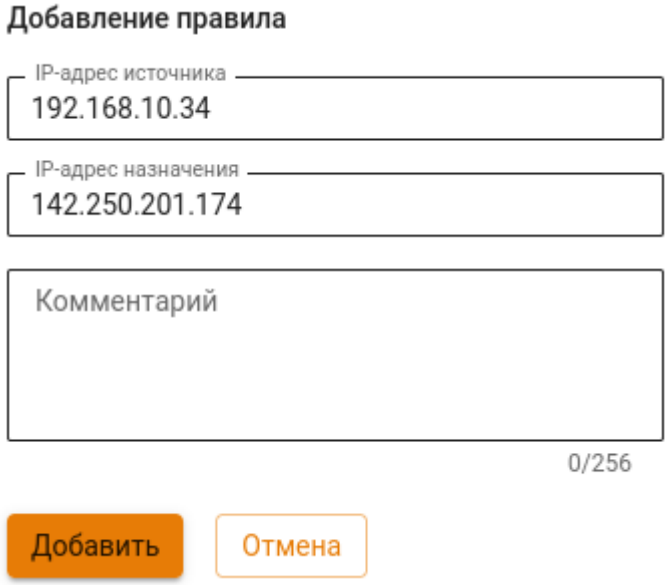
- **IP-адрес источника** - введите IP-адрес источника трафика;
- **Коментарий** - поле необязательное.

Фильтрация по IP-адресу назначения:



- IP-адрес назначения - введите IP-адрес назначения трафика;
- Коментарий - поле необязательное.

Фильтрация по IP-адресу источника и назначения:



- **IP-адрес источника** - введите IP-адрес источника трафика;
- **IP-адрес назначения** - введите IP-адрес назначения трафика;
- **Коментарий** - поле необязательное.

3. Нажмите **Добавить**.

4. Включите правило или оставьте его выключенным.

Подсказка: Отключить аппаратную фильтрацию можно, выключив опцию **Файрвол** в соответствующем разделе.

16.2 Контент-фильтр

16.2.1 Основное

Подсказка: Название службы раздела *Контент-фильтра*: `ideco-content-filter-backend`.
Список имен служб для других разделов доступен по *ссылке*.

Для записи логов поставьте флаг строке **Включить журналирование** в разделе **Сервисы -> Прокси -> Основное**.

Контент-фильтр проверяет наличие сайта, который хочет открыть пользователь, в списках ресурсов Ideco NGFW. Если адрес находится в этих списках, то применяются настроенные правила фильтрации.

Контент-фильтр состоит из четырех вкладок: правила, пользовательские категории, морфологические словари и настройки:

Подсказка: HTTPS-сайты без расшифровки трафика фильтруются только по домену (а не по полному URL), правила категории **Файлы** на них также применить невозможно. Для полной фильтрации HTTPS создайте правила расшифровки HTTPS-трафика нужных категорий.

Предупреждение: Для фильтрации по IP-адресам используйте *Файрвол*.

Фильтрация по IP-адресам в **Контент-фильтре** будет работать:

- Для HTTP-запросов к IP-адресам напрямую;
- Для расшифрованных HTTPS-запросов к IP-адресам;
- Для HTTPS-запросов к ресурсам, сертификат которых содержит IP-адрес в поле Common Name сертификата.

Файрвол анализирует пакет на сетевом уровне (L3), а **Контент-фильтр** - на прикладном уровне (L7). Информация об IP-адресах на прикладном уровне (L7) неточная, поэтому для блокировки IP-адресов нужно использовать **Файрвол**.

Подробная информация о методах фильтрации HTTPS представлена в статье:

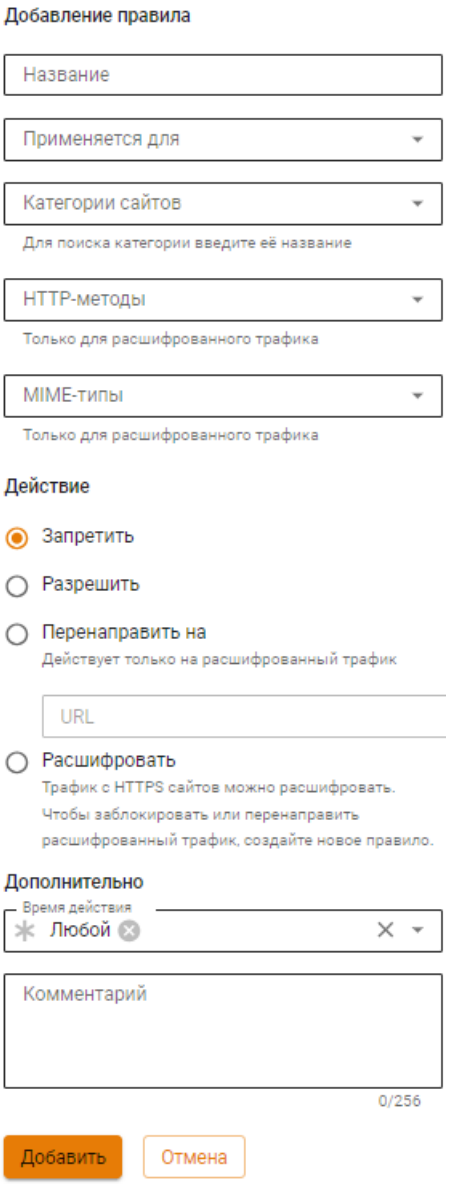
Порядок действий для изменения страницы блокировки Контент-фильтра описан в статье:

Подсказка: Процесс блокировки ресурсов, взаимодействующих с чат-ботами, описан в *статье*

16.2.2 Правила

Основное

Для добавления правила **Контент-фильтра** перейдите в раздел **Правила трафика -> Контент-фильтр -> Правила**, нажмите **Добавить** и заполните поля:



- **Название** - название добавляемого правила.
- **Применяется для** - пользователь или группа пользователей, IP-адреса или список IP-объектов, для которых применяется правило.
- **Категории сайтов** - поле для выбора *предустановленной или пользовательской категории*, перечень ресурсов, на которые распространяется действие правила.

Подсказка: Для расшифрованного трафика при создании и редактировании правила **Контент-фильтра** доступны более детальные настройки доступа к ресурсам с помощью HTTP-методов запроса и MIME-типов. Если поля остаются пустыми, проверка по ним не осуществляется.

- **HTTP-методы** - методы запроса, которые будут применяться для всего HTTP- или HTTPS-трафика. Доступные методы:
  - GET - извлечение данных ресурса, содержащих тело ответа;
  - HEAD - извлечение данных ресурса, не содержащих тело ответа;
  - POST - отправка данных на определенный ресурс;
  - PUT - замена текущих значений ресурса;

  - DELETE - удаление ресурса;
  - OPTIONS - описание параметров соединения с ресурсом;
  - PATCH - частичное изменение ресурса;
  - TRACE - вызов возвращаемого тестового сообщения с ресурса;
  - CONNECT - установка соединения с ресурсом.

- **MIME-типы** - форматы содержимого, к которым будет применяться правило. Форматы объединены в группы в зависимости от типа контента. Например, Audio (mp4, wav, wave и др.), Video (jpeg, mpeg, jmp и др.), Image (bmp, gif, png и др.). Настройки можно применить как к группе форматов, так и каждому формату отдельно.
- **Действия**:
  - **Запретить** - запрещает трафик;
  - **Разрешить** - разрешает трафик или направляет его в модули фильтрации трафика;
  - **Перенаправить на** - позволяет указать URL, на который будет перенаправлен расшифрованный трафик;
  - **Расшифровать** - расшифровывает трафик с HTTPS сайтов.

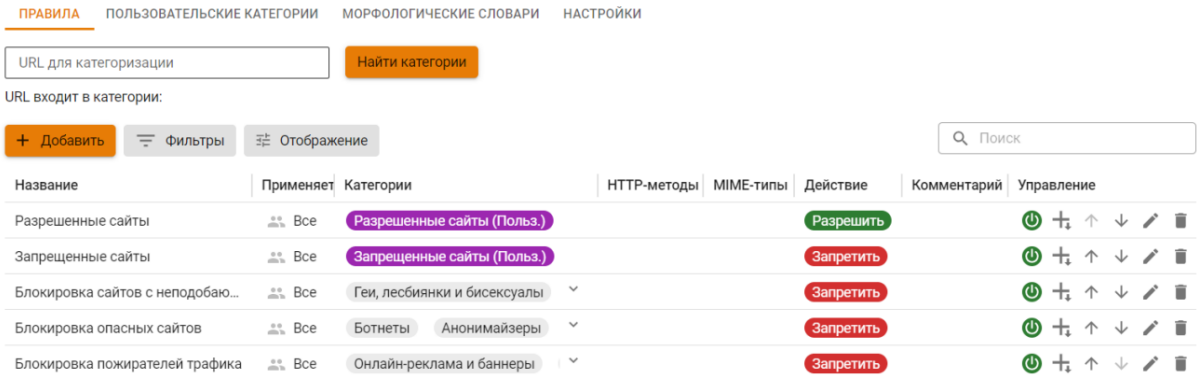
Подсказка: Если выбрать действие **Перенаправить на**, то нужно создать аналогичное правило с действием **Расшифровать** и поместить его выше перенаправляющего правила.

- **Дополнительно**:
  - **Время действия** - время действия правила. Указываются временные промежутки (например, **Рабочее время**), которые определяются в *Объектах*. По умолчанию установлено значение **Любой**;
  - **Комментарий** - произвольный текст, поясняющий цель действия правила. Значение не должно быть длиннее 255 символов.

Для подтверждения создания правила нажмите **Добавить**.

Помимо возможности добавления правил Контент-фильтра, вкладка содержит:

- **Строку поиска категории URL для категоризации**. Позволяет по URL найти категорию, в которой этот URL состоит, для дальнейшего создания правила;
- **Таблицу созданных правил**. Правила в таблице действуют сверху вниз. То есть, если вверху расположено правило, разрешающее контент, а внизу - запрещающее этот контент, будет работать только верхнее правило. Для перемещения правил используйте стрелки ↑ и ↓:

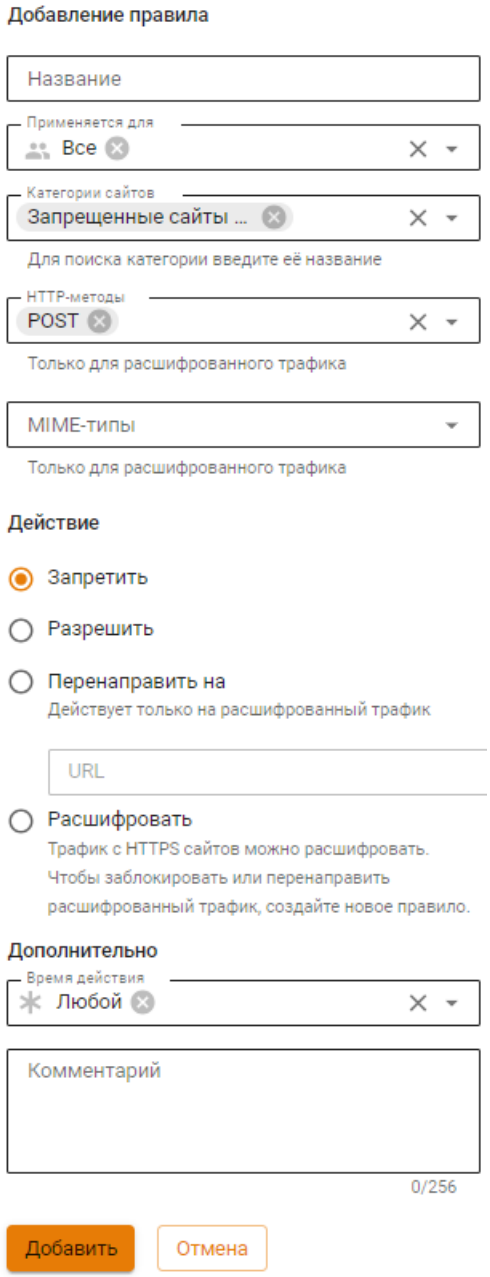


При наличии большого количества правил **Контент-фильтра** в таблице воспользуйтесь кнопкой **Фильтры**.

Пример настройки HTTP-метода:

Пример. Необходимо запретить всем пользователям отправлять данные на запрещенные сайты.

Перейдите в раздел **Правила трафика -> Контент-фильтр -> Правила** и нажмите **Добавить**. Заполните поля, как на скриншоте:

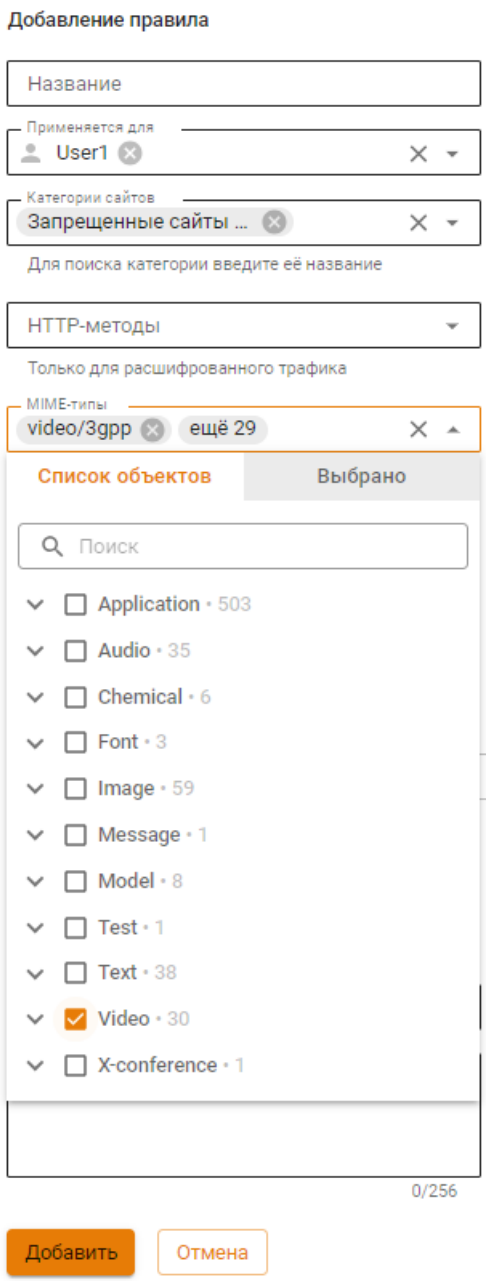


В поле **Категории сайтов** укажите предварительно созданную пользовательскую категорию **Запрещенные сайты**. При сохранении правила сайты откроются, если трафик не заблокирован другим правилом, но пользователь не сможет отправить данные (например, форму обратной связи).

Пример настройки MIME-типов:

Пример. Необходимо запретить конкретному пользователю (например, User1) воспроизводить видеоконтент на запрещенных сайтах.

Перейдите в раздел **Правила трафика -> Контент-фильтр -> Правила** и нажмите **Добавить**. Заполните поля, как на скриншоте:



В поле **Категории сайтов** укажите предварительно созданную пользовательскую категорию **Запрещенные сайты**. В поле **MIME-типы** выберите все форматы группы **Video**. Примените действие правила **Запретить**. При сохранении правила сайт откроется, если трафик не заблокирован другим правилом, но видеоконтент не воспроизведется.

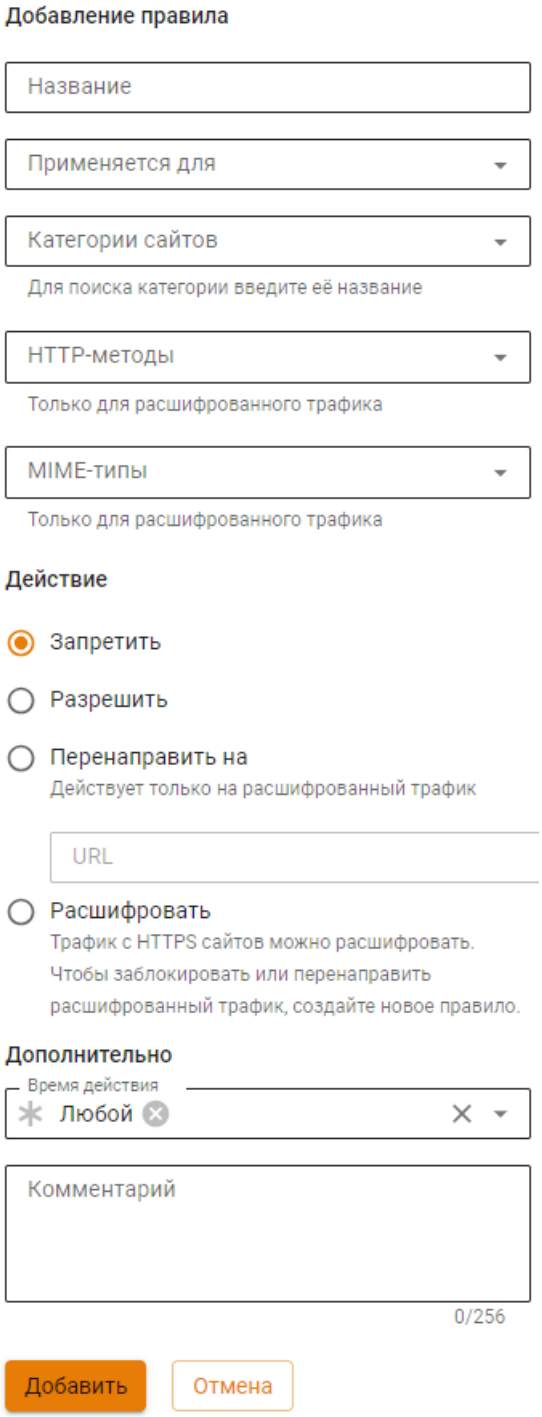
Применение правил фильтрации для пользователей:

Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. Таким образом, если вышестоящим правилом будет разрешен какой-то ресурс для определенной группы пользователей, то правила ниже применяться не будут. Так можно создавать гибкие настройки фильтрации, исключая нужных пользователей вышестоящими правилами из правил блокировки. Аналогичным образом действуют правила расшифровки HTTPS.

В столбце **Управление** можно активировать или деактивировать правило, менять его приоритет, редактировать и удалять. Правила контентной фильтрации применяются сразу после их создания или включения.

Чтобы создать новое правило, нажмите **Добавить** в левом верхнем углу над таблицей.

Заполните следующие поля:



- **Название** - наименование правила в списке. Значение не должно быть длиннее 42 символов;
- **Применяется для** - можно выбрать объекты типа: пользователь, группа пользователей, IP-адрес, диапазон IP-адресов, подсеть, список IP-адресов;
- **Категории сайтов** - пользовательские, специальные и расширенные категории веб-ресурсов;
- **Действие** - действие данного правила на веб-запросы. Можно запретить, разрешить или расшифровать HTTPS-трафик;
- Также можно дополнительно указать **Время действия** правила.

Диагностика:

Если правила контентной фильтрации не действуют, проверьте следующие параметры в настройках:

1. IP-адрес компьютера пользователя должен соответствовать его адресу в авторизации (раздел **Мониторинг - Авторизованные пользователи**), пользователь должен находиться в нужной группе, на которую назначено правило.

2. IP-адрес пользователя и ресурса, к которому он обращается, не должен входить в исключения прокси-сервера.

3. Проверьте правильность категоризации ресурса, к которому обращаетесь, в поле **URL для категоризации** на вкладке **Правила**:

Для этого вставьте в поле ссылку на ресурс, который требуется категоризировать, и нажмите **Найти категории**. Категории, в которые входит URL, отобразится ниже.

Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

4. В браузере и на компьютере пользователя не используются функции или плагины VPN, не прописаны сторонние прокси-серверы.

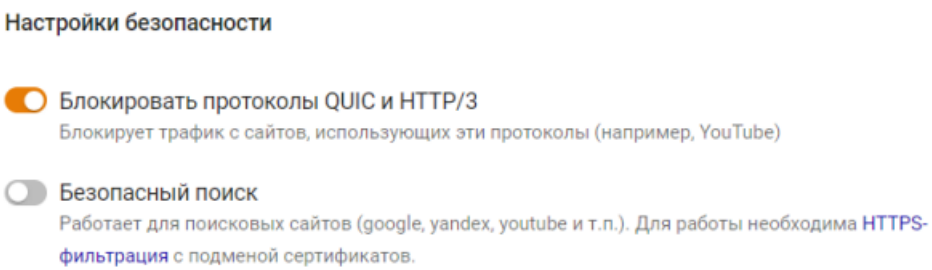
5. Проверить настройки контентной фильтрации по блокировке опасных и потенциально опасных файлов можно с помощью сервиса security.ideco.ru.

Блокировка загрузки файлов в файлообменники:

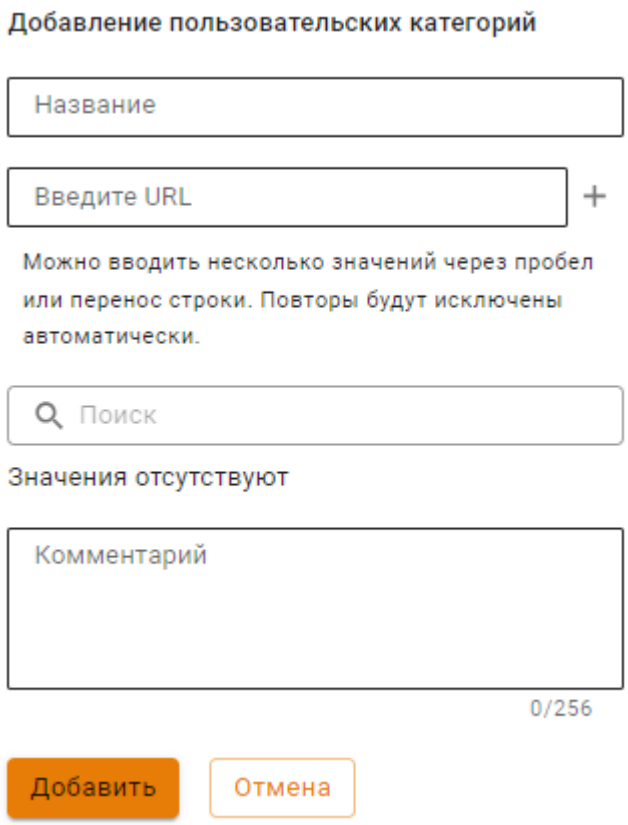
Блокирование этой категории требует особой настройки правил Контент-фильтра. В случае с файлообменниками (Google Drive, Яндекс.Диск, облако Mail.ru, Dropbox.com) расшифровки трафика категорий *Файлообменники*, *Файловые хранилища*, *Файловые архивы* и *Загрузка файлов в файлообменники* может быть недостаточно.

Чтобы заблокировать загрузку файлов в облака через браузер, выполните действия:

1. Включите **Блокировку протоколов Quic/HTTP3** на вкладке **Контент-фильтр -> Настройки**:

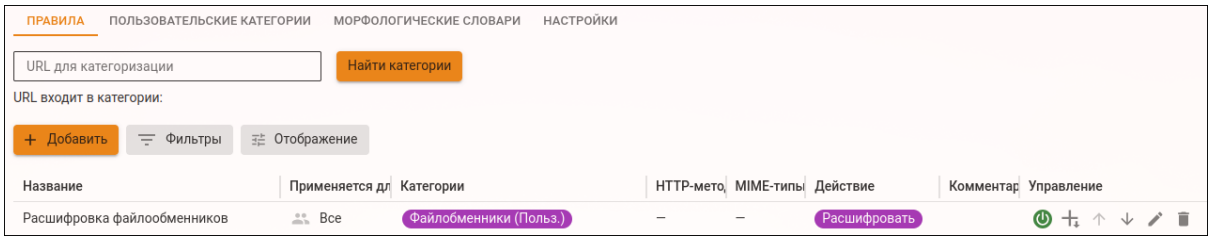


2. Создайте пользовательскую категорию для расшифровки трафика, указав домены нужных файлообменников:

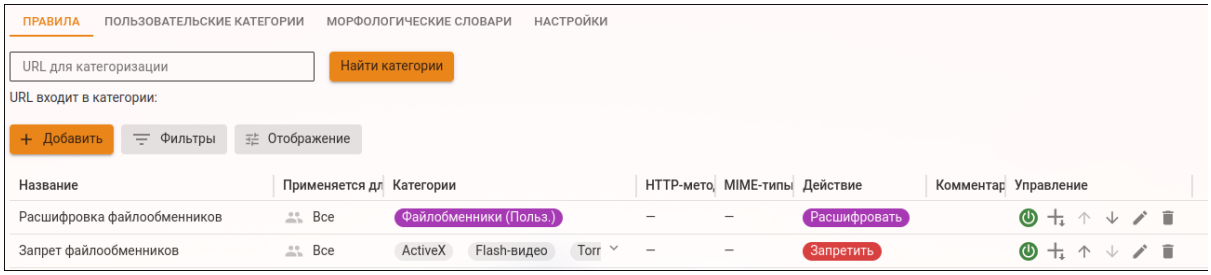


Для указания доменов используйте маски: `*.cloud.mail.ru`, `cloud.mail.ru/home`, `*.mail.ru`, `cloud.mail.ru`.

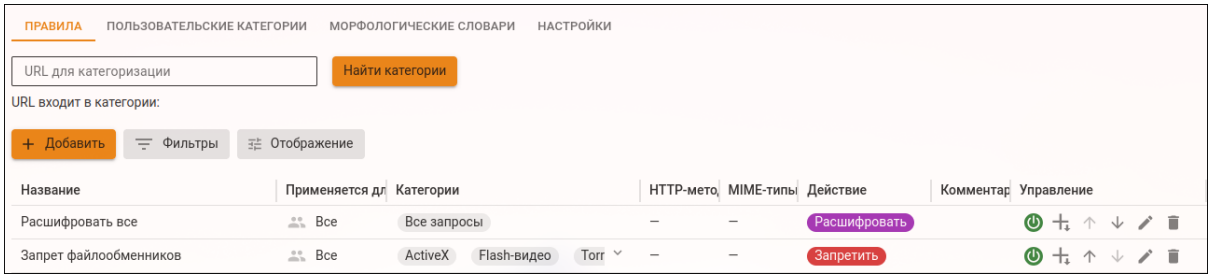
3. Создайте правило, расшифровывающее трафик созданной в п. 2 категории:



4. Ниже создайте правило, запрещающее загрузку файлов:



5. Проверьте, работает ли блокировка: с устройства пользователя, для которого она настроена, зайдите на сайты нужных файлообменников и попробуйте загрузить файлы.
Если загрузка проходит, создайте в **Контент-фильтре** правило, расшифровывающее весь трафик пользователя, а ниже - правило, запрещающее загрузку файлов в файлообменники:



16.2.3 Описание категорий контент-фильтра

Категории сайтов делятся на четыре вида:

1. **Пользовательские**. Включают категории, созданные на вкладке **Пользовательские категории**;

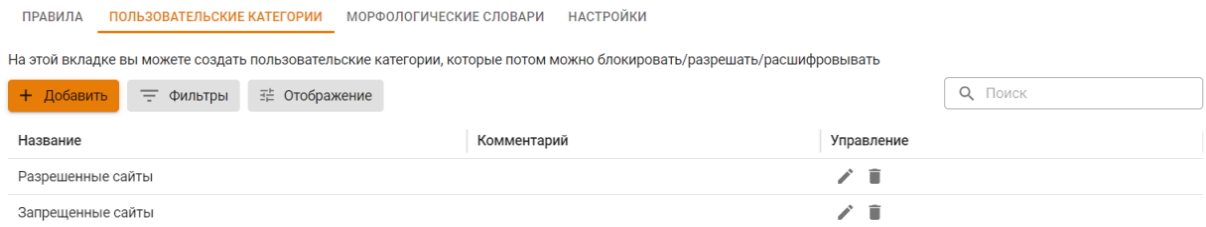
2. **Специальные**. Включает 4 категории: все запросы, все категоризированные запросы, все некатегоризированные запросы и запросы с прямыми обращениями по IP-адресам;

3. **Расширенные**. Правила, включающие расширенные категории, работают только с включенной опцией **Расширенная база категорий** на вкладке **Настройки**;

4. **Файлы**. Восемь сформированных категорий файлов, блокируемых по расширениям и MIME-type. Предустановленные группы файлов (Исполняемые файлы, Архивы, Видеофайлы, Аудиофайлы, Flash-видео, Active-X, Torrent-файлы, Документы) нельзя редактировать. Работа по фильтрации HTTPS-трафика по этому типу категорий возможна только при его расшифровке.

Пользовательские категории

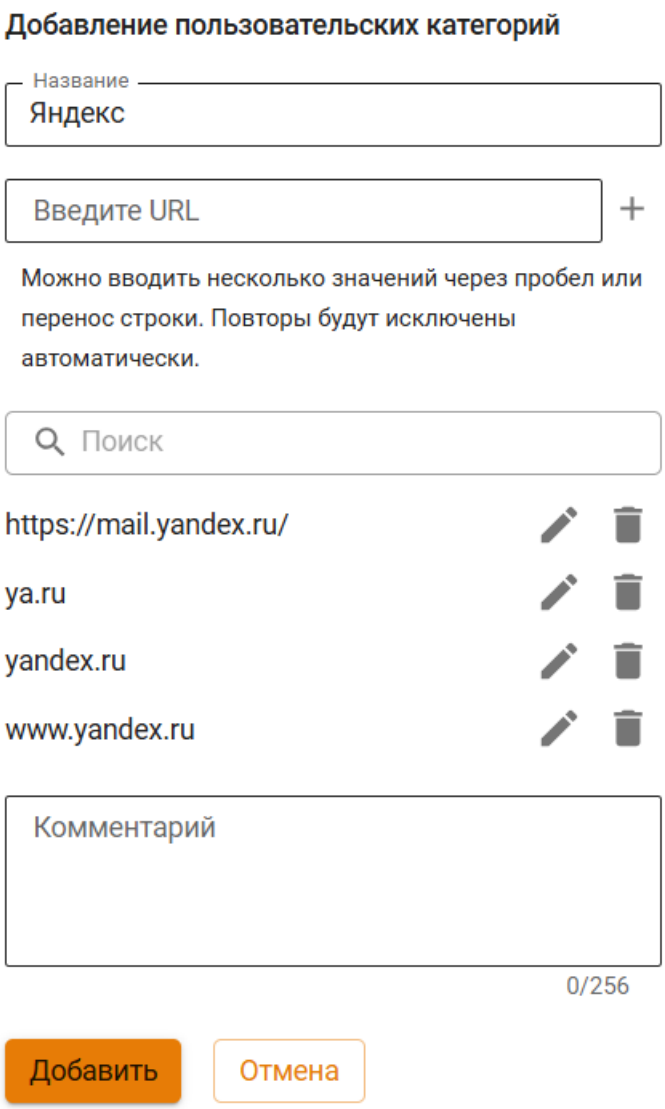
На одноименной вкладке создаются собственные категории правил.



При создании пользовательской категории потребуется ввести URL (одно или несколько значений через пробел). Используйте следующие маски:

- `test.ru`;
- `www.test.ru`;
- `http://www.test.ru/` или `https://www.test.ru/`;
- `https://www.test.ru:8080` ;
- `https://xn--41a.xn-p1acf/` - punycode;
- `*.test.ru` - для всех доменов третьего и выше уровней. Важно: такая маска не включает домен второго уровня test.ru, чтобы его включить достаточно указать домен test.ru (все его поддомены также попадут под это правило);
- `1.1.1.1` - любой IP-адрес.

Пример создания пользовательской категории:



- **Название** - название пользовательской категории, которое будет использоваться при настройке правила **Контент-фильтра**;
- **Введите URL** - адрес сайта/страницы или доменное имя;
- **Поиск** - поле поиска добавленных URL;
- **Комментарий** - можно заполнить или оставить пустым.

Если в таблице большое количество пользовательских категорий, воспользуйтесь кнопкой **Фильтры**.

Внимание: При создании пользовательских категорий обратите внимание на алгоритм работы **Контент-фильтра**.

Если создать пользовательскую категорию с доменом domain.ru, которая используется в правиле **Контент-фильтра**, то это правило будет корректно работать для domain.ru, www.domain.ru и *.domain.ru.

Однако если создать еще одну пользовательскую категорию с таким же доменом (например, www.domain.ru или *.domain.ru), то правило с пользовательской категорией domain.ru перестанет работать для доменов www.domain.ru и *.domain.ru, **даже если эта созданная категория не используется ни в одном правиле**.

Подсказка: Если URL или домен содержит специальные символы (или •), оставьте их в исходном виде. Адрес будут автоматически закодирован в формат punycode.

Специальные категории

- **Все запросы** - под эту категорию попадают все запросы к веб-ресурсам;
- **Все категоризированные запросы** - все запросы к веб-ресурсам, категоризированные по встроенным или пользовательским категориям;
- **Все не категоризированные запросы** - все запросы к веб-ресурсам, которые не были категоризированы по встроенным или пользовательским категориям;
- **Прямое обращение по IP** - запросы к веб-ресурсам по IP-адресу (http://84.201.128.105/).

Расширенные категории

Категория	Описание
Аборты	Веб-страницы, на которых обсуждаются аборты с медицинской, юридической, исторической и других точек зрения
Аборты — одобрение	Веб-сайты, одобряющие применение абортов
Аборты — осуждение	Веб-сайты, осуждающие применение абортов
Автомобили/Транспорт	Категория не содержит адресов и будет удалена в будущем
Активность в социальных сетях	Возможность писать/добавлять/загружать что-то в социальные сети
Алкоголь	Веб-сайты, призывающие к употреблению алкоголя (или оправдывающие его употребление), а также сайты, осуществляющие продажу алкогольной продукции, включая пиво, вина и т. д.
Анонимайзеры	Веб-сайты, предназначенные для обхода сетевых фильтров. Такие ресурсы могут быть использованы сотрудниками компании с целью посещения запрещенных сайтов
Архитектура	Веб-сайты, посвященные строительству, проектированию зданий и сооружений, архитектуре, а также организациям или услугам, связанным с дизайном, строительством и строительным проектированием
Астрология и гороскопы	Веб-сайты об астрологии, гороскопах, а также предсказаниях по звездам или знаку зодиака
Атеизм и агностицизм	Веб-сайты, ведущие антирелигиозную пропаганду или подвергающие сомнению религиозные, духовные, метафизические, или сверхъестественные воззрения
Аудио для прослушивания и скачивания	Сайты-хранилища, вещающие музыку или другой аудио контент (может потребить всю доступную ширину канала компании)
Аукционы и рынки	Веб-сайты, посвященные продажам товаров и услуг через объявления, онлайн-аукционы или через другие нетрадиционные каналы

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Банки	Веб-сайты банков и иных кредитных учреждений, включая сайты интернет-банков. В эту категорию не входят сайты организаций, предлагающих брокерские услуги
Безопасность	Сайты, относящиеся к продуктам и услугам, касающимся безопасности, за исключением компьютерной
Бизнес и услуги (общая)	Веб-сайты о бизнесе и услугах. В эту категорию включены ресурсы, которые не подлежат более точному категорированию, чем бизнес и услуги
Бизнес/Сервисы	Категория не содержит адресов и будет удалена в будущем
Биотехнологии	Веб-сайты, посвященные исследованиям в области генетики, а также сайты исследовательских институтов и организаций, работающих в сфере биотехнологий
Благотворительные учреждения	Сайты с информацией о благотворительных учреждениях и других некоммерческих филантропических организациях
Ботнеты	Категория не содержит адресов и будет удалена в будущем
Веб-почта	Службы, предоставляющие пользователям веб-доступ к почтовым ящикам. Как правило, речь идет о бесплатных ящиках
Веб-хостинг, интернет-провайдеры и телекоммуникационные компании	Сайты, предлагающие услуги веб-хостинга, блог-хостинга, интернет-провайдеры и телекоммуникационные компании
Взлом	Веб-сайты, содержащие информацию или утилиты, которые могут быть использованы для совершения онлайн-преступлений
Видео для прослушивания и скачивания	Сайты-хранилища, вещающие видео, в том числе в браузере (может потребить всю доступную ширину канала компании)
Виртуальные открытки	Сайты, позволяющие пользователям отправлять и принимать открытки
Возможный риск	Категория не содержит адресов и будет удалена в будущем
Войска и вооружения	Веб-сайты об оружии и силовых структурах
Вооруженные силы	Веб-сайты, спонсируемые вооруженными силами и иными государственными военными учреждениями
Высокий уровень риска	Категория не содержит адресов и будет удалена в будущем
Геи, лесбиянки и бисексуалы	Веб-сайты, на которых обсуждаются вопросы, связанные с нетрадиционной сексуальной ориентацией
Готовые домашние задания	Сайты с ответами к тестам, готовыми сочинениями, пошаговыми решениями задач и аналогичные ресурсы, которые могут использоваться для списывания
Для взрослых	Категория не содержит адресов и будет удалена в будущем

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Дом, сад и семья	Веб-сайты, которые раскрывают вопросы о семейных отношениях и обустройства дома, включая информацию о воспитании, внутреннем украшении, озеленении, уборке, семье и т. д.
Дом/Отдых	Категория не содержит адресов и будет удалена в будущем
Дома престарелых и уход за больными	Сайты о домах престарелых и тематические сообщества, включая уход за больными и хосписную помощь
Домашние животные	Сайты, содержащие информацию, продукты и услуги для домашних животных
Доставка и логистика	Сайты об управлении запасами, включая транспортировку, склад, дистрибуцию, хранение, выполнение и доставку заказов
Еда и рестораны	Сайты о еде: от ресторанов и кафе до рецептов и советов по готовке
Загрузка файлов в файлообменники	Загрузка файлов в файлообменники через браузер, например, в Google Drive, Яндекс.Диск, облако Mail.ru, Dropbox.com
Законодательство и политика	Сайты о законодательстве, политике, партиях, выборах, их результатах и мнениях
Запаркованные	Веб-сайты, которые используются в качестве «заглушек» для приобретенных, но не используемых доменных имен
Здоровье	Категория не содержит адресов и будет удалена в будущем
Здравоохранение и медицина	Веб-сайты, посвященные личному здоровью, медицинским услугам, медицинскому оборудованию, процедурам, психическому здоровью, больницам и клиникам
Знакомства	Веб-сайты, посвященные знакомствам, браку и т. д.
Игрушки	Сайты производителей игрушек, а также маркетинговые ресурсы и онлайн-магазины игрушек
Изображения жестокого обращения с детьми	Веб-сайты с изображениями физического или сексуального насилия над детьми
Интернет и IP-телефония	Веб-сайты, позволяющие совершать звонки через web или сайты программных продуктов, которые предназначены для совершения звонков через интернет
Интернет-магазины	Интернет-магазины и иные сайты, предлагающие совершить онлайн-покупки
Информационная безопасность	Веб-сайты организаций, предоставляющих услуги в сфере информационной безопасности
Искусство	Категория не содержит адресов и будет удалена в будущем
Казино, лотереи, тотализаторы	Сайты казино и прочих игровых систем
Каталоги	Веб-сайты с продуктовыми списками и каталогами без возможности совершить онлайн-покупку
Компьютерные игры	Веб-сайты, посвященные компьютерным играм, а также сайты с онлайн-играми
Компьютеры и технологии	Категория не содержит адресов и будет удалена в будущем

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Конкурсы и опросы	Веб-сайты, посвященные онлайн-тотализаторам, соревнованиям, распродажам и лотереям, которые создаются для изучения потребительских предпочтений, а также могут использоваться в качестве элемента различной маркетинговой деятельности
Контент-серверы	CDN-серверы, на которых кешируется часть контента или страница целиком
Криминальные навыки	Веб-сайты, предоставляющие информацию о том, как совершить незаконную деятельность, такую как кража, убийство, создание бомбы, вскрытие замка и т. д.
Криминальные навыки/хакинг	Категория не содержит адресов и будет удалена в будущем
Купальные костюмы	Сайты, содержащие изображения людей в купальных костюмах. Изображения самих костюмов не попадают в эту категорию
Купоны	Веб-сайты, предлагающие приобретение скидочных купонов (купонаторы)
Литература и книги	Сайты, на которых представлена литература, включая беллетристику и документальные романы, стихи и биографии
Марихуана	Сайты, на которых представлена информация о марихуане, ее выращивании или курении, включая сайты, посвященные легальному использованию марихуаны, например, в медицине
Маркетинговые услуги	Сайты рекламных и маркетинговых агентств, кроме баннерных сетей
Мгновенные сообщения	Веб-сайты служб мгновенных сообщений, а также сайтов, призывающих поддерживать контакты с друзьями через сервисы обмена сообщениями
Мебель для дома и офиса	Веб-сайты, которые включают информацию о производителях мебели, розничных магазинах по продаже мебели, столов, стульев, кабинетов и т. д.
Мобильные телефоны	Сайты производителей мобильных телефонов, включая сайты, осуществляющие продажу мобильных телефонов и аксессуаров к ним
Мода и красота	Веб-сайты, посвященные моде и красоте, включая сайты, связанные с модой и содержащие информацию об одежде, ювелирных украшениях, косметике и парфюме
Музыка	Веб-сайты, посвященные музыке. Интернет-радио, файлы в формате mp3, информация о музыкальных группах, клипы и т. д.
Мультфильмы, аниме и комиксы	Веб-сайты, на которых размещены мультипликационные ТВ-шоу, фильмы, комиксы
Наркотики	Веб-сайты, призывающие к употреблению наркотических веществ, включая неправильное употребление лекарственных препаратов
Насилие	Веб-сайты, содержащие призывы к сомнительным действиям, таким как насилие и агрессия
Не для детского просмотра	Материалы, неуместные для детей: безвкусные, жестокие (в том числе, по отношению к животным), туалетный юмор и т. п.

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Недвижимость	Веб-сайты, посвященные вопросам, связанным с недвижимостью (приобретение, продажа, аренда и т. д.)
Недоступные	Категория не содержит адресов и будет удалена в будущем
Неизвестные сайты	Категория не содержит адресов и будет удалена в будущем
Неизвестный уровень риска	Категория не содержит адресов и будет удалена в будущем
Некоммерческие организации	Категория не содержит адресов и будет удалена в будущем
Нераспознаваемый контент	Сайты с нераспознаваемым контентом, что не позволяет их категоризировать
Нетрадиционные религии и оккультные верования	Сайты, посвященные религиям, не находящимся в мейнстриме или не входящим в ТОП-10 мировых религий (народные религии, мистика, культы и секты)
Новости	Новостные веб-ресурсы. Сайты газет, журналов, новостные ленты
Обзоры продукции и сравнение цен	Сайты, призванные помочь покупателям сравнить магазины, продукты и цены, но не торгующие онлайн
Оборудование, ПО, электроника	Сайты о компьютерном оборудовании, ПО, периферии, сетях данных, электронике, а также ресурсы производителей соответствующих товаров и услуг
Образование и учебные учреждения	Сайты и ресурсы сообществ, создающих информационные документы, доступные на редактирование всем участникам
Онлайн-офисы	Сайты брокерских компаний, осуществляющих онлайн-торговлю ценными бумагами и т. д.
Онлайн-реклама и баннеры	Веб-страницы, строго посвященные рекламе, баннерам или выскакивающим окнам с рекламой
Онлайн-торговля акциями	Сайты фондовых рынков
Онлайн-управление информацией	Сайты, посвященные программам для управления личной информацией, например, приложения для управления со списками задач, календарями, адресные книги и т. д.
Откровенные изображения	Сайты с фотографиями и видеороликами, на которых изображены девушки в сексуальной провокационной одежде, например, в дамском белье
Парки, зоны отдыха и спортивные залы	Сайты, посвященные паркам и иным зонам, предназначенным для оздоровительных активностей, таких как плавание, скейтбординг, альпинизм и т. д.
Переадресация	Сайты, перенаправляющие посетителя на другие ресурсы
Переводчики	Словари и переводчики с иностранных языков
Персональные страницы	Категория не содержит адресов и будет удалена в будущем
Персональные страницы и блоги	Персональные страницы, включая блоги и другие средства обмена новостями, мнениями и информацией об авторе, а также домашние и семейные страницы

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Пиратство и хищение авторских прав	Сайты, предоставляющие доступ к незаконному контенту, например, пиратскому программному обеспечению (warez), пиратским фильмам, музыке и т. д.
Пиринговые сети	Сайты пиринговых сетей
Питание и диеты	Сайты с информацией о здоровом питании, похудении, диетах, программах похудения и пищевой аллергии
Пищевые добавки и витамины	Сайты, содержащие сведения о витаминах и других веществах нерегулируемого оборота
Плата за серфинг	Сайты компаний, предлагающих оплату за просмотр рекламы в их специализированных приложениях
Платные сайты мобильных операторов	Сайты сотовых операторов, за доступ к которым взимается отдельная плата с абонента
Поиск работы	Веб-сайты, посвященные поиску работы, включая рекрутинговые агентства
Поисковики изображений	Сайты и поисковые машины, используемые для поиска изображений и возвращающие результаты, содержащие миниатюры последних
Поисковые системы	Поисковые системы, осуществляющие поиск по веб-сайтам, новостным группам, картинкам и другому контенту
Политика и закон	Категория не содержит адресов и будет удалена в будущем
Порнография	Сайты, содержащие изображения или видео с откровенной демонстрацией полового акта или обнаженного тела
Порнография/секс	Категория не содержит адресов и будет удалена в будущем
Порталы	Веб-ресурсы, предоставляющие доступ к настраиваемым персональным порталам, включая «желтые страницы» и другие каталоги
Правительство	Категория не содержит адресов и будет удалена в будущем
Природа и ее сохранение	Веб-сайты с информацией об окружающей среде, экологии и т. д.
Производство	Сайты, посвященные бизнесу, связанному с промышленным производством
Профессиональные сообщества	Сайты социальных сетей, ориентированных на профессионалов и выстраивание деловых отношений
Развлекательные места и события	Веб-сайты, посвященные культурным заведениям, таким как театры, кинотеатры, ночные клубы, фестивали и т. д.
Развлекательные новости и сайты про знаменитостей	Веб-сайты, посвященные новостям о знаменитостях, телешоу, фильмах и шоу-бизнесе в целом
Развлечения и видео	Категория не содержит адресов и будет удалена в будущем
Разное	Веб-сайты, которые не могут быть однозначно отнесены ни к одной из категорий
Религии	Сайты об основных мировых религиях, а также общерелигиозной тематики и теологические
Религия	Категория не содержит адресов и будет удалена в будущем

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Рестораны	Категория не содержит адресов и будет удалена в будущем
Сайты для детей	Сайты, предназначенные для маленьких детей (до 10 лет), включая игры и развлекательные страницы
Сайты сообществ	Категория не содержит адресов и будет удалена в будущем
Самопомощь и зависимости	Сайты, предлагающие информацию и помощь при алкогольной, наркотической, игровой зависимостях, а также расстройствах пищевого поведения (анорексия и пр.)
Секс и Эротика	Сайты, предлагающие продукты и услуги, связанные с сексом, но не содержащие обнаженной натуры и других откровенных изображений
Сексуальное воспитание и образование	Сайты с обучающими материалами и клиническими пояснениями о сексе, безопасном сексе, беременности, родам и т. п., ориентированные на детей и подростков
Сельское хозяйство	Веб-сайты, посвященные науке, искусству и бизнесу, связанному с сельским хозяйством (производство зерновых культур, подъем домашнего скота, продуктов, услуг и т. д.).
Системы централизованной аутентификации	Сайты, которые используются для единой аутентификации и получения доступа к большому разнообразию услуг. Например, такие системы, как Yahoo или Google
Сквернословие	Сайты с непристойными, бранными словами
Скомпрометированные	Веб-сайты, которые были скомпрометированы злоумышленниками и выглядят как официальные ресурсы, но на самом деле содержат вредоносный код
Сообщества лоббистов и торговые ассоциации	Веб-сайты, посвященные промышленным торговым группам, лоббистам, союзам, профессиональным организациям и другим ассоциациям, включая сообщества единомышленников
Социальные сети	Сайты социальных сетей — сообществ, в которых люди «дружат» между собой
Социальные сообщества	Социальные сети, а также веб-сайты различных онлайн-сообществ
Спам	Веб-сайты, рекламируемые с помощью спама
Список Минюста	Федеральный список экстремистских материалов, составленный Министерством юстиции РФ
Спонсируемые государством	Веб-сайты, посвященные государственным организациям, включая полицию, пожарные службы, избирательные комиссии, спонсируемые государством исследования и программы
Спорт	Сайты о соревновательных видах спорта, где люди или команды состязаются в атлетических (например, футбол) и прочих (бильярд) дисциплинах
Спорт и отдых	Категория не содержит адресов и будет удалена в будущем
Спортивная охота	Сайты о любительской охоте на живых животных
Спортивные соревнования	Сайты, посвященные тренировкам и соревнованиям по боевым искусствам: бокс, борьба, фехтование и т. п.

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Справочные материалы и карты	Сайты, содержащие справочные материалы и наборы данных: атласы, словари, энциклопедии, переписи и т. п.
Средний уровень риска	Категория не содержит адресов и будет удалена в будущем
Страхование	Веб-сайты, посвященные всем типам страхования, включая медицинское, государственное, страхование имущества и т. д.
Табак	Веб-сайты, призывающие к употреблению табачной продукции (сигареты, сигары, трубки и т. д.)
Тайный сбор информации	Сайты, идентифицированные как шпионские, пересылающие информацию о посетителях по специальному адресу
Текстовые сообщения	Сайты, предназначенные для обмена короткими текстовыми сообщениями (SMS) между веб-страницей и мобильным телефоном
Телевидение и фильмы	Сайты о телешоу и фильмах, включая обзоры, программы передач, сюжеты, обсуждения, трейлеры, маркетинг и т. п.
Технологии (в целом)	Веб-сайты, посвященные веб-дизайну, стандартизации в интернете (например, RFC), спецификациям протоколов, новостям и другим широким обсуждениям технологий
Только для взрослых (18+)	Сайты, в содержании которых обязательно содержится материал, предназначенный только для взрослой аудитории. Там может быть затронута сексуальная тематика или не учебные материалы
Торговля и покупки	Категория не содержит адресов и будет удалена в будущем
Торрент-трекеры	Сайты, размещающие торрент-файлы, позволяющие загрузить потенциально большие файлы по P2P-сетям
Транспортные средства	Сайты о транспортных средствах, включая продажу, продвижение, обсуждение, ресурсы производителей и онлайн-магазины
Туризм	Сайты гостиниц, туристических агентств и операторов
Удаленный доступ	Сайты, предоставляющие удаленный доступ к частным компьютерам и сетям, ресурсам интернета (файлам и веб-приложениям)
Учебные заведения	Веб-сайты школ, университетов и иных образовательных учреждений
Учебные материалы и исследования	Веб-сайты, на которых размещены академические публикации, журналы, результаты исследований, учебные планы, а также онлайн-курсы, учебники и т. д.
Файловые архивы	Категория не содержит адресов и будет удалена в будущем
Файловые хранилища	Веб-сайты с каталогами программного обеспечения, включая условно-бесплатное, бесплатное и свободно распространяемое программное обеспечение
Файлообменники	Сайты файлообменников

continues on next page

Таблица 1 – продолжение с предыдущей страницы

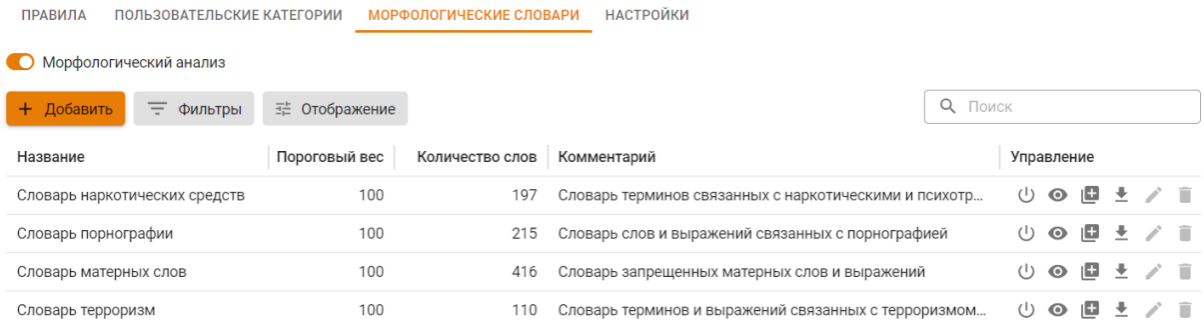
Категория	Описание
Фармацевтика	Веб-сайты, содержащие информацию о лекарственных препаратах (включая легальные наркотические вещества), а также их применении
Финансовые инструменты и котировки	Сайты, содержащие информацию о финансовых котировках, а также инструменты финансового анализа и бюджетного планирования, такие как ипотечные калькуляторы, программное обеспечение для формирования налоговой отчетности и т. д.
Финансы	Категория не содержит адресов и будет удалена в будущем
Финансы (в целом)	Веб-сайты, на страницах которых обсуждаются экономические вопросы, инвестиционные стратегии, пенсионное и налоговое планирование
Фитнес и отдых	Веб-сайты, посвященные фитнесу и другим оздоровительным активностям
Фишинг/мошенничество	Веб-сайты, используемые для мошенничества, также известны как фишинговые. Как правило, представляются официальными веб-страницами финансовых или иных учреждений с целью несанкционированного доступа к конфиденциальной информации, например, пин-кодам банковских карт
Форумы	Сайты форумов, новостных групп, архивы списков рассылки, доски объявлений и аналогичные ресурсы сообществ
Фотогалереи	Сайты с архивами фотографий, фотостоки
Хобби и Досуг	Веб-сайты, содержащие информацию о различных ремеслах и хобби, таких как вышивание, коллекционирование, авиамоделирование и т. д.
Центры распространения вредоносного ПО	Сайты, на которых размещены вирусы, эксплоиты и другое вредоносное ПО
Центры управления и контроля	Интернет-серверы, использующиеся для управления ботнетами
Частные IP-адреса	Сайты, обслуживаемые на частных IP-адресах, зарезервированных для использования внутри организаций и дома
Чаты	Онлайн-чаты
Чаты/Мессенджеры	Категория не содержит адресов и будет удалена в будущем
Шпионские и опасные сайты	Категория не содержит адресов и будет удалена в будущем
Шпионское и сомнительное ПО	Сайты с ПО, пересылающим информацию на центральный сервер, включая шпионское ПО и клавиатурные шпионы
Экстремизм	Веб-сайты, призывающие к экстремизму, дискриминации по половому, расовому, религиозному и другим признакам
Эротика	Веб-сайты, содержащие материалы эротического характера (частичное или полное обнажение), исключая порнографические материалы
Юмор	Веб-сайты, содержащие информацию юмористического характера, такую как комиксы, шутки, смешные картинки

16.2.4 Морфологические словари

Основное

На вкладке создаются и редактируются словари для проведения морфологического анализа сайтов. Если в тексте анализируемого сайта содержится достаточное для блокировки количество предварительно заданных слов и словосочетаний, доступ к ресурсу блокируется.

Опция **Морфологический анализ** включается в левом верхнем углу вкладки **Морфологические словари**:



При этом морфологический анализ проводится только с использованием включенных словарей. Если ни один словарь не включен, морфологический анализ не проводится.

Подсказка: Проверка морфологическими словарями распространяется на весь расшифрованный трафик, поэтому для работы морфологического анализа необходимо создать в **Контент-фильтре** правило расшифровки трафика.

По умолчанию в таблицу добавлены четыре словаря, которые нельзя отредактировать или удалить:

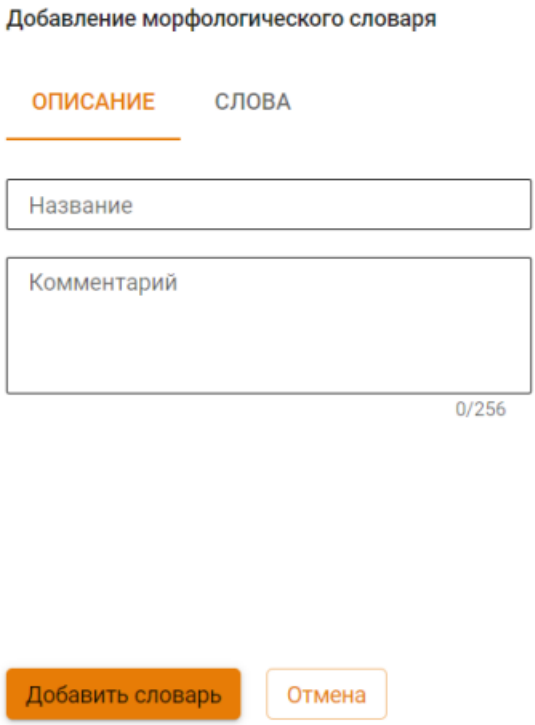
- Словарь наркотических средств;
- Словарь порнографии;
- Словарь матерных слов;
- Словарь терроризм.

По умолчанию предустановленные словари отключены.

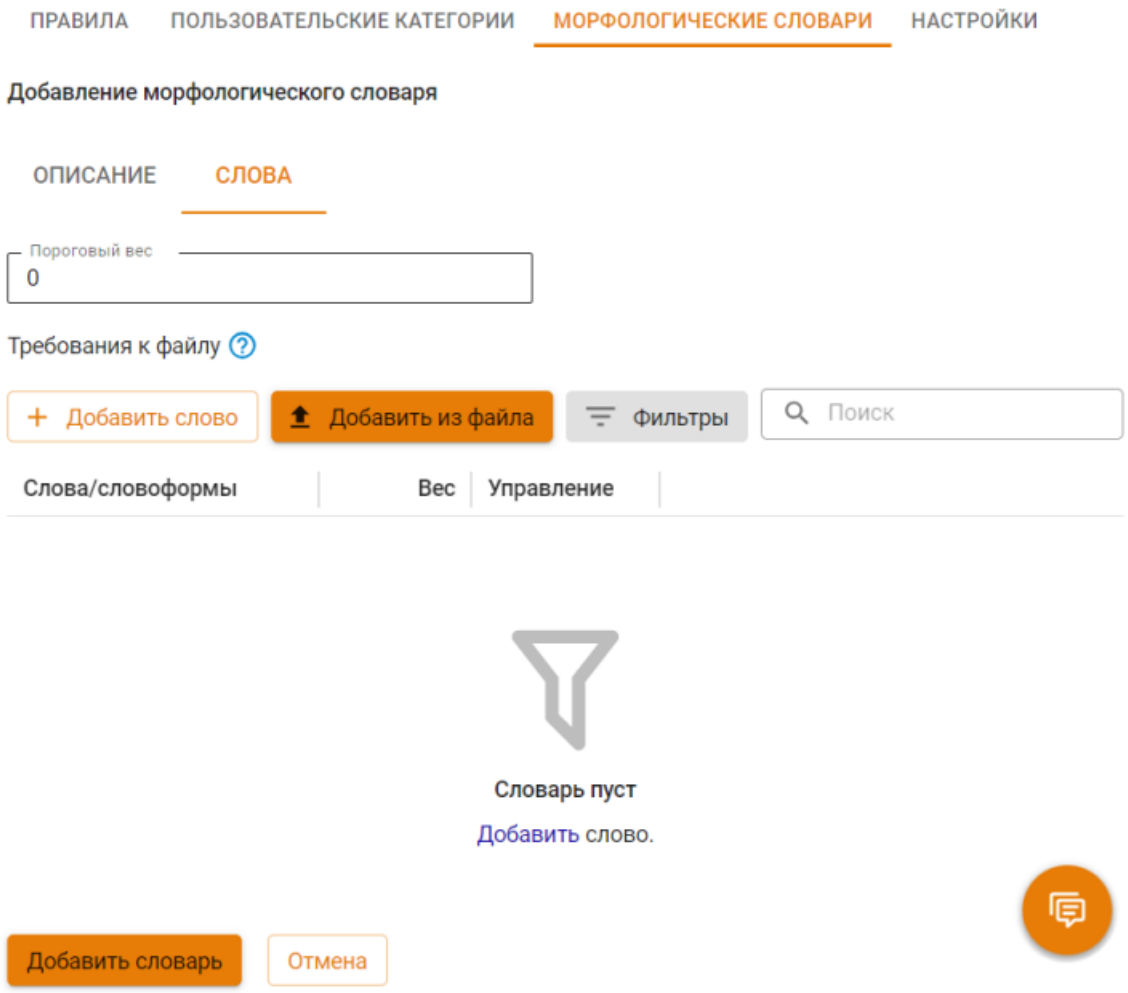
Для создания морфологического словаря выполните действия:

1. Перейдите в раздел **Правила трафика -> Контент-фильтр -> Морфологические словари** и нажмите **Добавить**.

2. На вкладке **Описание** введите название словаря и комментарий:



3. На вкладке **Слова** добавьте слова для блокировки трафика вручную или загрузите из файла:

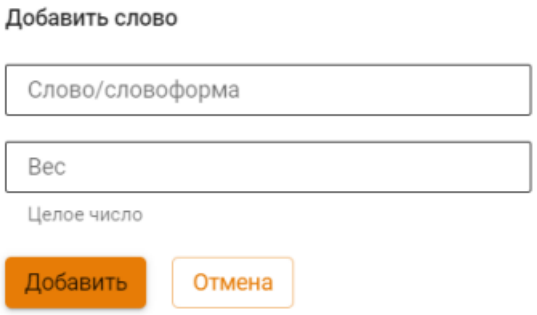


При добавлении слов вручную:

- Введите значение в поле **Пороговый вес**;

Подсказка: Пороговый вес - общий вес указанных в настройках словаря слов (целое число от 0 до 2 147 483 648). Если при проверке сайта общий вес найденных на нем слов превысит пороговый, доступ к сайту будет заблокирован.

- Нажмите **Добавить слова**;
- Заполните поля **Слово/словосочетание** и **Вес** при добавлении каждого слова:



При загрузке слов из файла нажмите **Добавить из файла** и выберите загружаемый файл. В один словарь можно загружать несколько файлов. В этом случае дублирующиеся слова будут удалены, останется только одно вхождение с установленным весом. Значение в поле **Пороговый вес** указывается автоматически.

Требования к загрузке из файла:

- Формат файла - CSV, кодировка - UTF-8;
- В одной строке должно быть одно слово или словосочетание и вес, разделенные точкой с запятой;
- Допустимо не указывать вес слова. В этом случае по умолчанию к каждому слову/словосочению без веса применится значение 20, а файл будет представлять собой список без разделителей.

При неудачной загрузке файла появится окно с уведомлением **Файл не соответствует требованиям**.

Примеры файлов:

С указанием веса:

```
слово;20
словосочетание;20
```

Без указания веса:

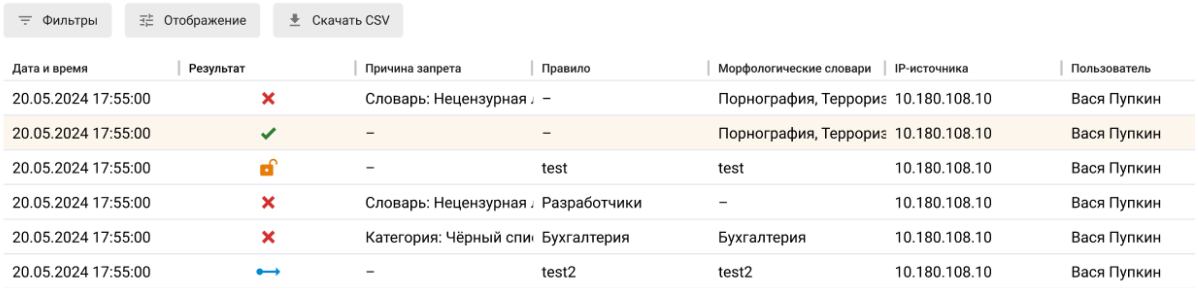
```
слово
словосочетание
```

При загрузке указанных выше файлов и при **Пороговом значении** = 100 доступ к сайту будет заблокирован, если на нем 5 и более раз упоминается «слово» и/или «словосочетание».

4. Для сохранения настроек нажмите **Добавить словарь**.

Если в таблице большое количество морфологических словарей, воспользуйтесь кнопкой **Фильтры**.

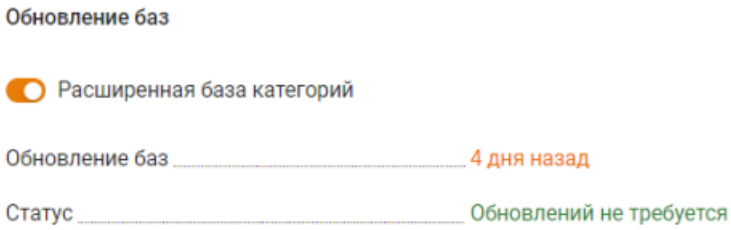
Результат морфологического анализа представлен в разделе **Отчеты и журналы -> Журнал веб-трафика**. В журнале также отображаются дата и время, причина запрета, название правила, название морфологического словаря, IP источника и имя пользователя:



16.2.5 Настройки

Настройки

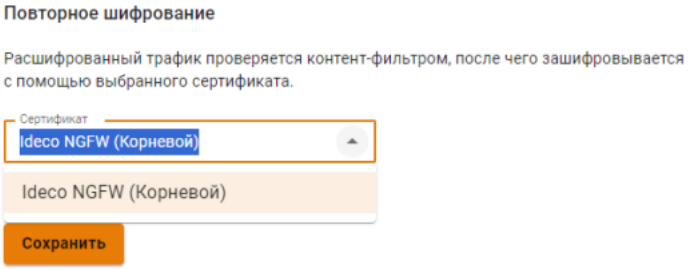
Если включить опцию **Расширенная база категорий**, то будет включена работа более 140 категорий, автоматически обновляемых сервером. Эти категории работают только при активной подписке на обновления в коммерческих редакциях:



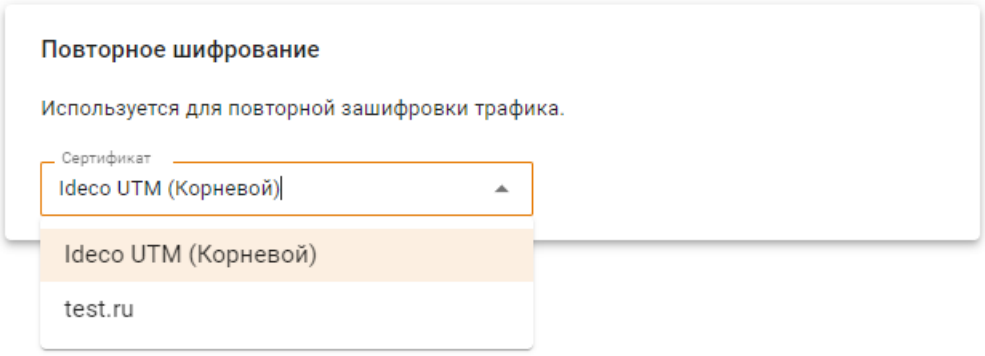
Подсказка: Если отключить опцию **Расширенная база категорий**, то все правила, включающие в себя расширенные категории, перестанут срабатывать.

На вкладке **Настройки** можно настроить дополнительные параметры фильтрации:

- **Блокировать протоколы QUIC и HTTP/3.** Протокол, используемый современными браузерами для доступа к некоторым ресурсам (например, Google, YouTube). Рекомендуется блокировать его, т. к. иначе фильтрация ресурсов, работающих по этому протоколу, будет невозможна. Заблокированный трафик нельзя исключить, добавив IP-адрес в списки исключений на вкладке **Прокси -> Исключения**;
- **Безопасный поиск.** Принудительно включает безопасный поиск в поисковых системах (Google, Yandex, YouTube, Yahoo, Bing, Rambler). **Для работы этой функции нужно включить HTTPS-фильтрацию методом подмены сертификата для данных ресурсов**.



Если для повторного шифрования требуется использовать сертификат, отличный от корневого в NGFW, загрузите нужный сертификат в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** и выберите его для повторного шифрования:



16.2.6 Настройка фильтрации HTTPS

Фильтрация реализуется несколькими методами:

- **Анализ заголовков Server Name Indication (SNI)** - благодаря этому методу возможен анализ домена, к которому подключается клиент, без подмены сертификата и вмешательства в HTTPS-трафик. Также анализируются домены, указанные в сертификате;
- **Метод SSL-bump** - фильтрация происходит путем подмены «на лету» сертификата, которым подписан запрашиваемый сайт. Оригинальный сертификат сайта подменяется новым, подписанным не центром сертификации, а корневым сертификатом Ideco NGFW. Таким образом, передающийся по защищенному HTTPS-соединению трафик становится доступным для обработки всем модулям Ideco NGFW: антивирусам Касперского, внешним ICAP-сервисам и контент-фильтру (можно категоризировать полный URL запроса и MIME-type контента).

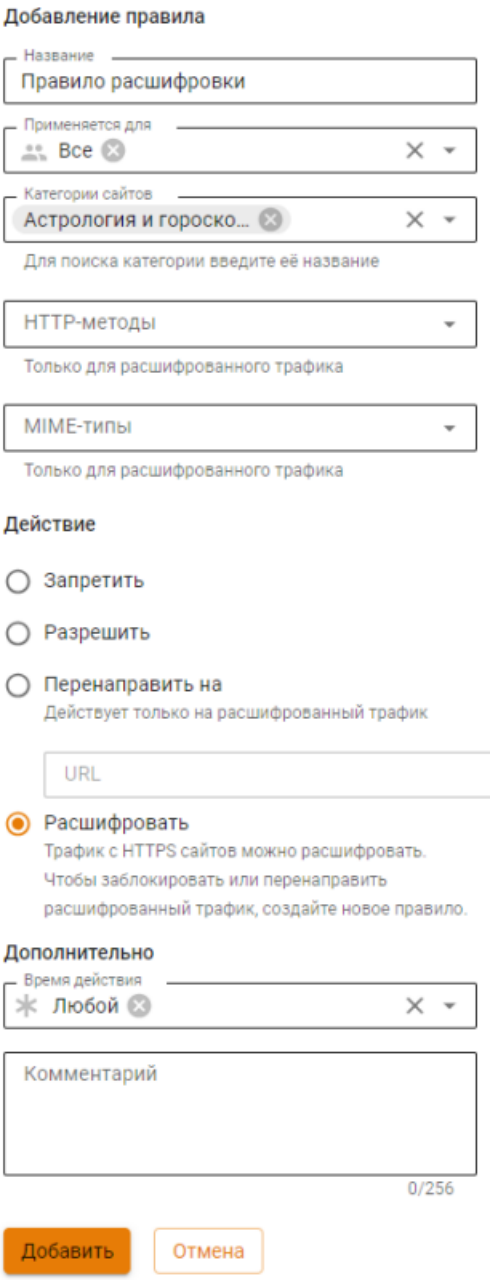
Подсказка: Специфика фильтрации HTTPS-трафика с подменой сертификата требует настройки обеих сторон подключения: сервера Ideco NGFW и рабочей станции каждого пользователя в локальной сети.

Настройка сервера Ideco NGFW

По умолчанию сервер фильтрует HTTPS без подмены сертификатов с помощью анализа SNI и доменов в сертификате.

Дешифрация HTTPS-трафика настраивается в разделе **Правила трафика -> Контент-фильтр -> Правила** с помощью создаваемых администратором правил с действием **Расшифровать**.

Пример правила для расшифровки:



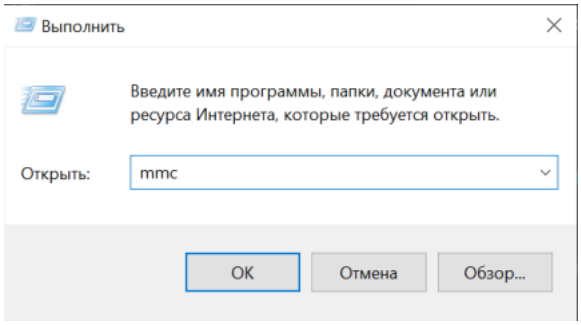
Настройка рабочей станции пользователя

При включенной опции расшифровки HTTPS-трафика браузер, антивирусы, клиенты IM и другое сетевое ПО на рабочей станции пользователя потребуют явного подтверждения на использование подменного сертификата, созданного и выданного сервером Ideco NGFW. Чтобы повысить удобство работы пользователя, установите в операционную систему рабочей станции корневой сертификат сервера Ideco NGFW и сделайте его доверенным. Для этого выполните действия:

1. Скачайте корневой SSL-сертификат, открыв раздел веб-интерфейса Ideco NGFW **Сервисы -> Сертификаты -> Загруженные сертификаты**:

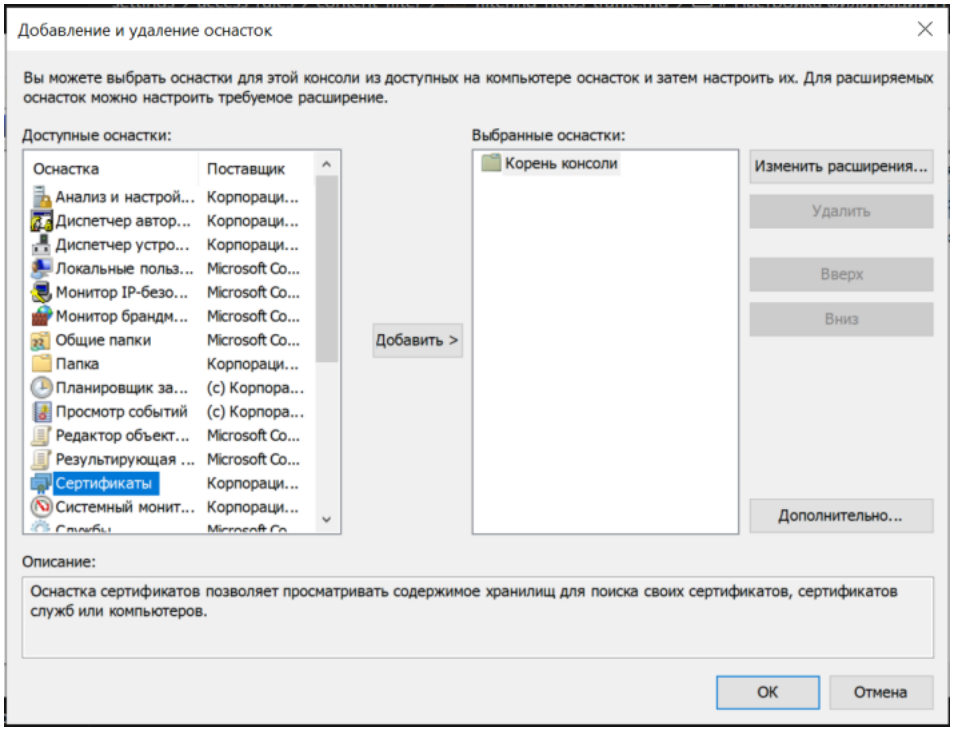
20250219090034/docsUTM/.gitbook/assets/certs1.png

2. Откройте на рабочей станции центр управления сертификатами: **Пуск -> Выполнить**, выполнив в диалоге команду **mmc**:

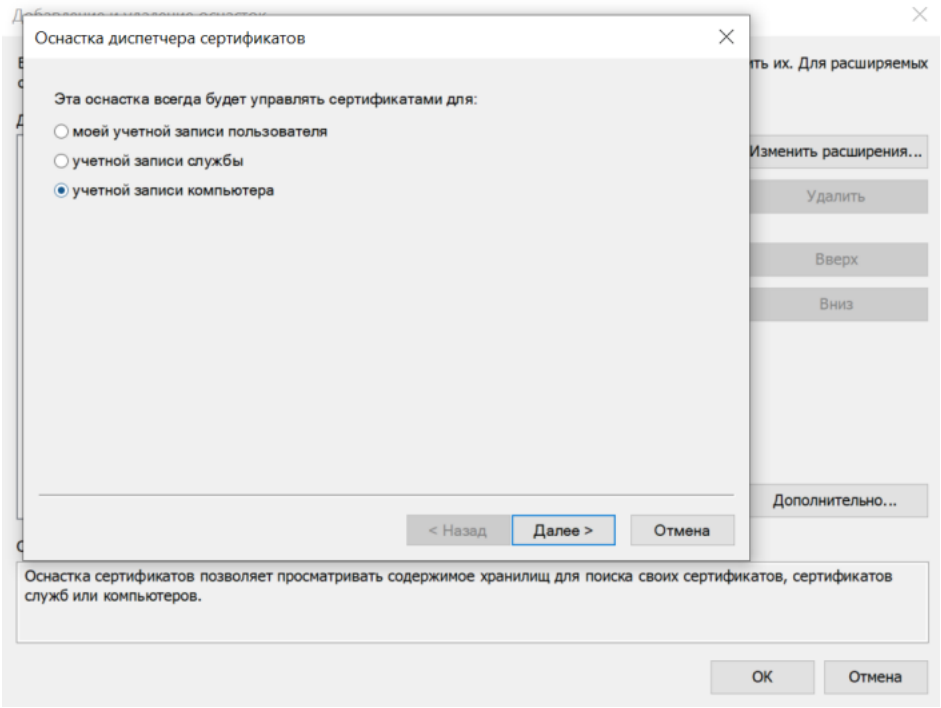


3. В меню **Файл** выберите **Добавить или удалить оснастку**:

4. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите кнопку **Добавить**:

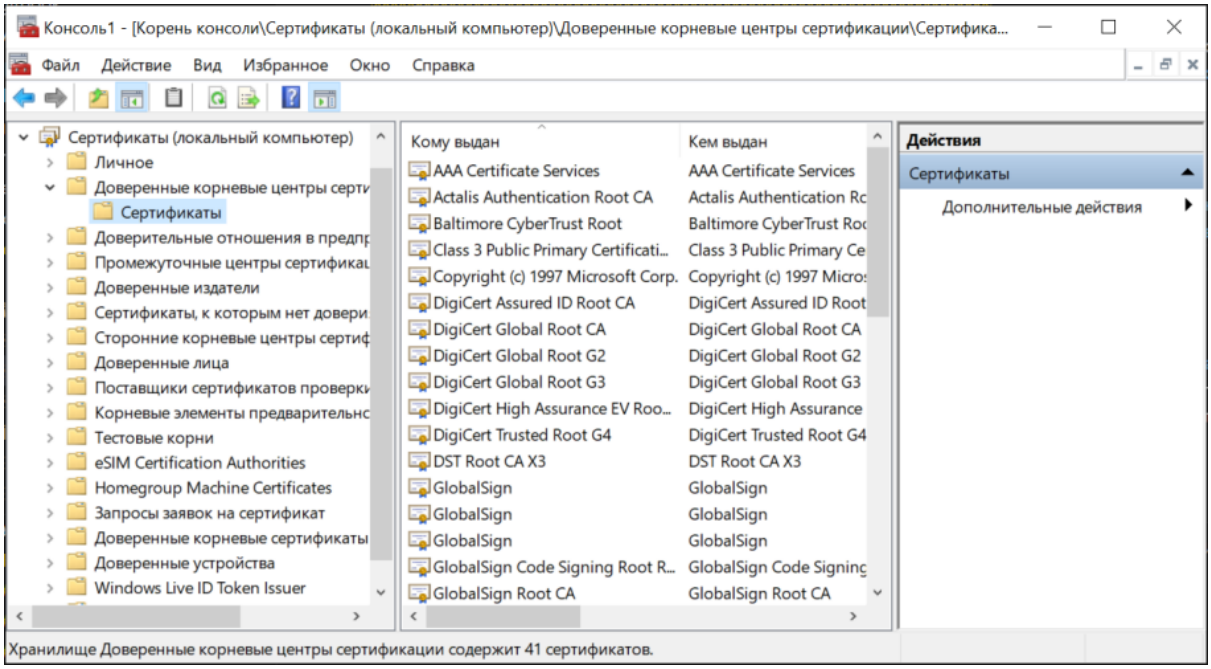


5. В открывшемся окне выберите пункт **Учетная запись компьютера** и нажмите кнопку **Далее**:



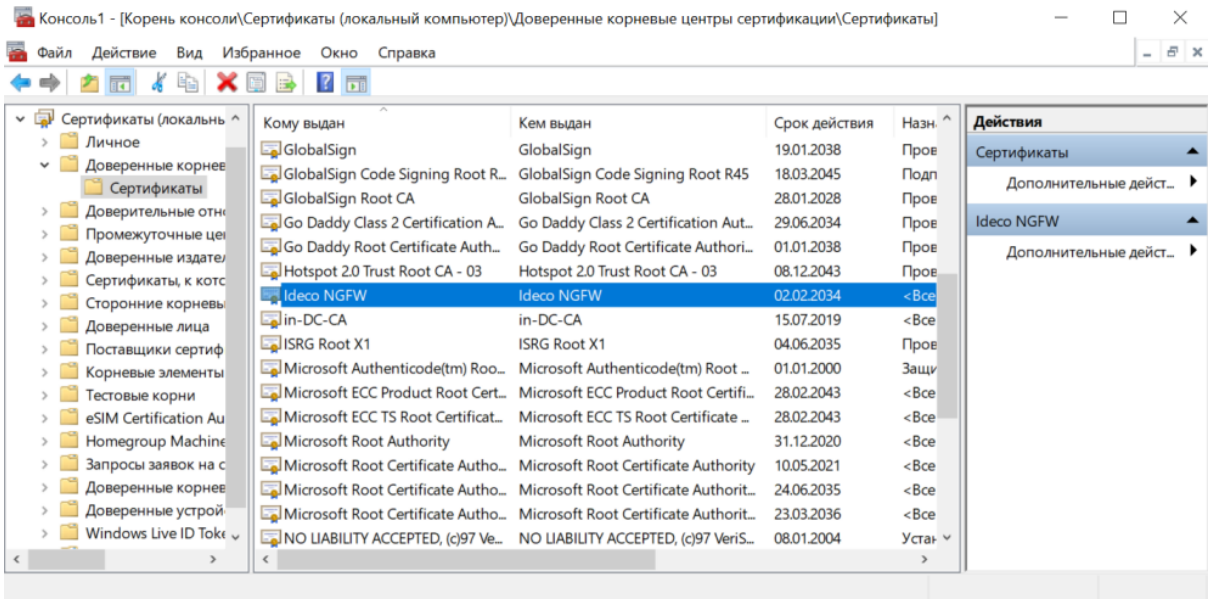
6. В окне **Выбор компьютера** оставьте флаг **Локальный компьютер** и нажмите кнопку **Готово**.

7. В левой части окна нажмите на стрелку рядом с директорией **Сертификаты (локальный компьютер) -> Доверенные корневые сертификаты -> Сертификаты**:



8. В меню **Действие** выберите **Все задачи -> Импорт**:

9. Следуя инструкциям Мастера импорта сертификатов, импортируйте корневой сертификат сервера Ideco NGFW. Импортированный сертификат появится в списке в правой части окна:



Добавление сертификата через политики домена Microsoft Active Directory

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, можно установить сертификат Ideco NGFW для всех пользователей автоматически с помощью Active Directory. Для этого необходимо выполнить действия:

1. Скачать корневой SSL-сертификат, открыв раздел веб-интерфейса Ideco NGFW **Сервисы -> Сертификаты -> Загруженные сертификаты**:

20250219090034/docsUTM/.gitbook/assets/certs1.png

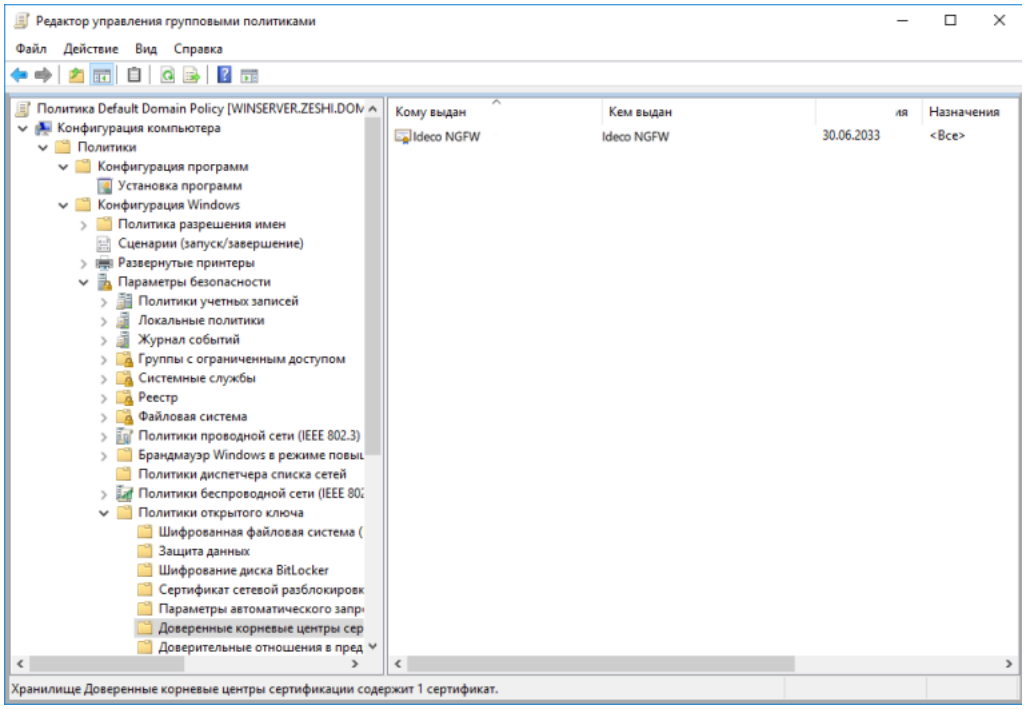
2. Зайдите на контроллер домена с правами администратора.

3. Запустите оснастку управления групповой политикой, выполнив команду **gpmc.msc**.

4. Найдите **политику домена**, использующуюся на компьютерах пользователей в **Объектах групповой политики** (Default Domain Policy). Нажмите на нее правой кнопкой мышки и выберите **Изменить**.

5. В открывшемся редакторе управления групповыми политиками выберите: **Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Политики открытого ключа -> Доверенные корневые центры сертификации**.

6. Нажмите правой кнопкой мыши по открывшемуся списку, выберите **Импорт** и импортируйте ключ Ideco NGFW.



7. После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Настройка повторной зашифровки трафика с помощью отдельного сертификата

1. Загрузите сертификат, который будет использоваться для зашифровки, в раздел **Сервисы -> Сертификаты -> Загруженные сертификаты**.

2. Перейдите в раздел **Правила трафика -> Контент-фильтр -> Настройки**.

3. Выберите в пункте **Повторное шифрование** сертификат, загруженный на 1 шаге.

Подсказка: Для получения информации, расшифрованной Контент-фильтром, у клиента должен быть установлен загруженный сертификат в хранилище сертификатов пользователя. Рекомендации по настройке компьютера пользователя можно найти в разделе **Настройка рабочей станции пользователя**.

Возможные проблемы и методы их решения

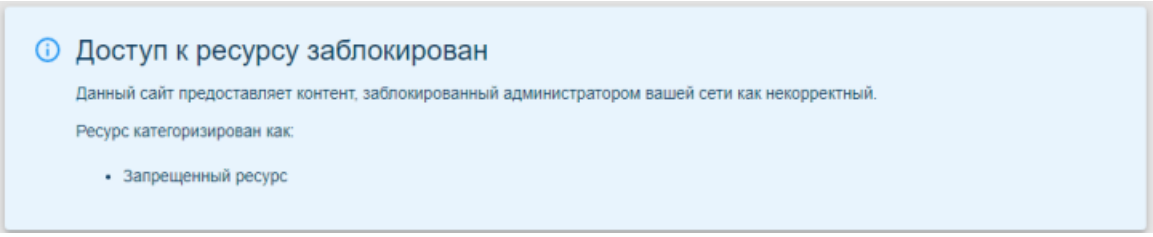
- Включения расшифровки трафика может быть недостаточно для подмены сертификата некоторых сайтов (например, `ya.ru`, `google.com`). В этом случае необходимо включить опцию **Блокировать протоколы QUIC и HTTP/3** на вкладке **Настройки** раздела **Контент-фильтр**;
- Если браузер не использует системное хранилище сертификатов, нужно добавить сертификат Ideco NGFW в доверенные сертификаты браузера. В Mozilla Firefox также можно присвоить параметру `security.enterprise\_roots.enabled` (в **about:config**) значение `true` для доверия системным сертификатам;
- Если на локальной машине используется антивирус, проверяющий HTTPS-трафик методом подмены сертификатов, сайты могут не открываться из-за двойной подмены сертификатов. Нужно отключить в настройках антивируса проверку HTTPS-трафика;
- При включенной SNI-фильтрации сервер не будет пропускать по HTTPS-порту трафик, отличный от HTTPS-трафика. В результате могут возникнуть проблемы с программами, пытающимися это сделать. Для их работы необходимо разрешить обход прокси-сервера к нужным им ресурсам;

- При блокировке HTTPS-ресурсов для отображения страницы блокировки необходимо настроить доверие корневому SSL-сертификату NGFW, даже если включена только SNI-фильтрация, т. к. в случае срабатывания блокировки ресурса, открываемого по HTTPS, будет применен SSL-bumping с подстановкой SSL-сертификата NGFW для подмены контента ресурса страницей о его блокировке сервером.

16.2.7 Изменение страницы блокировки Контент-фильтра

Основное

Страница блокировки Контент-фильтра по умолчанию содержит уведомление о блокировке доступа к ресурсу и категоризацию:



Внимание: В процессе обновления Ideco NGFW все ранее настроенные параметры шаблона блокировки будут сброшены.

Для создания персонализированного шаблона страницы выполните действия:

1. Удалите директорию, в которой хранятся файлы кеша страниц ошибок:

```
rm -R /var/cache/ideco/proxy-backend/error_pages
```

2. Чтобы изменить фавикон, загрузите новый файл в директорию **/usr/share/ideco/vendor/**. Для этого перейдите в раздел **Управление сервером -> Администраторы** и убедитесь, что доступ по SSH разрешен. Затем откройте терминал на компьютере и введите следующую команду:

```
scp C:\Users\Admin\Downloads\favicon.png admin@192.168.0.23:/usr/share/ideco/vendor
```

- `C:\Users\Admin\Downloads\favicon.png` - путь к файлу на вашем компьютере;
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW;
- Файл обязательно должен иметь имя **favicon.png**.

3. Чтобы изменить иконки предупреждения, загрузите новые файлы в директорию **/usr/share/ideco/proxy-backend/error_page_templates/images**. Для этого откройте терминал на компьютере и введите следующую команду:

```
scp C:\Users\Admin\Downloads\IDECO_ICON_INFO.svg admin@192.168.0.23:/usr/share/ideco/
↪proxy-backend/error_page_templates/images
```

- `C:\Users\Admin\Downloads\favicon.png` - путь к файлу на вашем компьютере;
- `admin@192.168.0.23` - логин администратора и IP-адрес или домен NGFW;
- Файлы обязательно должны иметь имя **IDECO_ICON_ERROR.svg, IDECO_ICON_INFO.svg, IDECO_ICON_SUCCESS.svg, IDECO_ICON_WARNING.svg**.

4. Чтобы изменить CSS-файл стилей для страниц ошибок, перейдите в директорию **/usr/share/ideco/proxy-backend/error_page_templates/** и откройте файл **style.css** в текстовом редакторе:

```
nano /usr/share/ideco/proxy-backend/error_page_templates/style.css
```

Пример изменения файла style.css:

Чтобы изменить цвет текста и фона, отредактируйте блоки `error`, `warning`, `info`, `success`:

```
.error {
  background-color: #E6E2DD;
  color: #373A36;
}

.warning {
  background-color: #E6E2DD;
  color: #373A36;
}

.info {
  background-color: #E6E2DD;
  color: #373A36;
}

.success {
  background-color: #E6E2DD;
  color: #373A36;
}
```

Чтобы изменить цвет страницы, размер и отступы текста, отредактируйте блок `body`:

```
body {
  padding: 5% 12px;
  box-sizing: border-box;
  overflow: auto;
  background-color: #E6E2DD;
  font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
  font-size: 10px;
  line-height: 14px;
}
```

Чтобы изменить размер шрифта, отредактируйте блоки `h1` и `p`:

```
h1 {
  margin: 0;
  padding-bottom: 8px;
  font-weight: 500;
  font-size: 24px;
  line-height: 25px;
}

p {
  margin: 0;
  padding: 8px 0;
  font-style: normal;
  font-weight: normal;
  font-size: 14px;
  line-height: 16px;
}
```

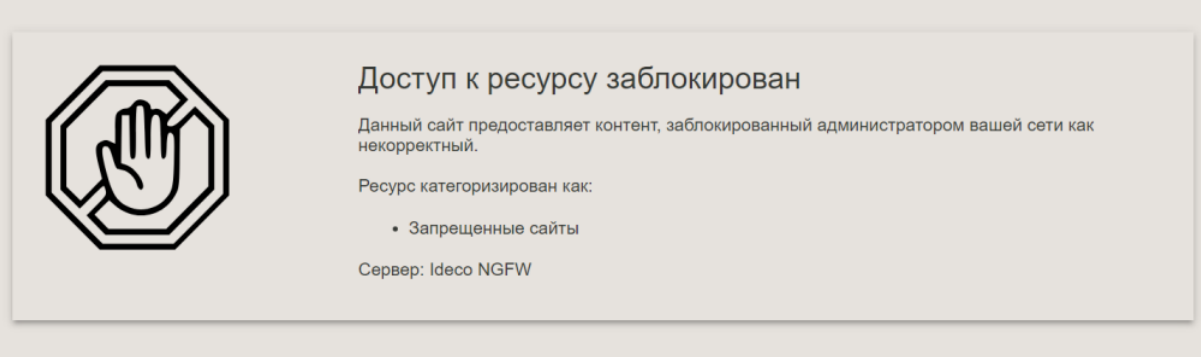
Чтобы изменить цвет гиперссылок, отредактируйте блок `a`:

```
a {
  color: #D48166;
  text-decoration: none;
}
```

Чтобы изменить размер логотипа, отредактируйте блок `.icon`:

```
.icon {
  width: 150px;
  min-width: 150px;
  height: 150px;
  min-height: 150px;
  margin-right: 100px;
  background-position: center;
  background-size: cover;
}
```

Пример страницы:



5. Чтобы изменить общий шаблон для страниц ошибок, отредактируйте HTML-файл. Перейдите в директорию **/usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU** и откройте файл **ERR_TEMPLATE.html** в текстовом редакторе:

```
nano /usr/share/ideco/proxy-backend/error_page_templates/langs/ru_RU/ERR_TEMPLATE.html
```

Пример изменения файла ERR_TEMPLATE.html:

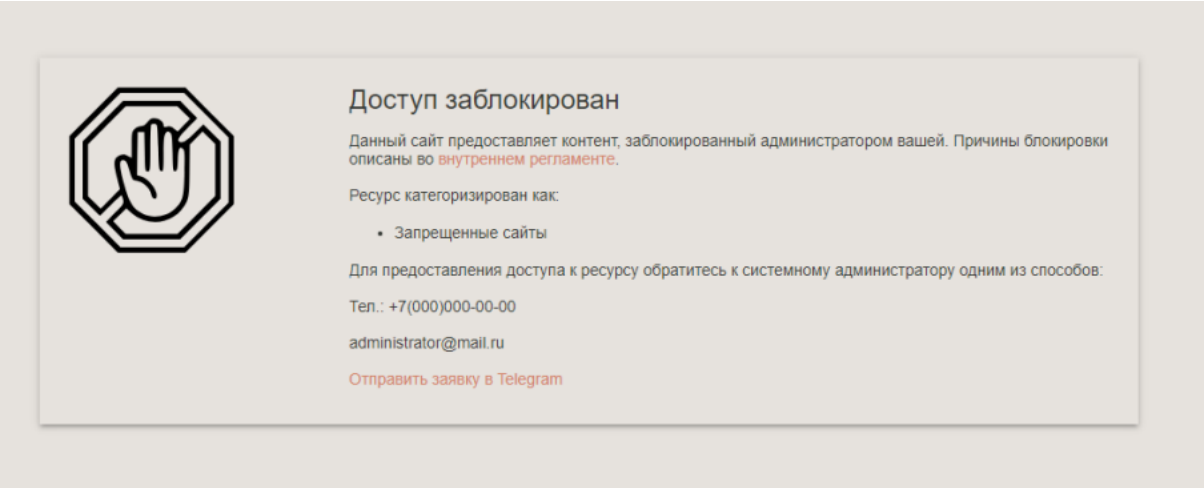
```
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width" />
  <link rel="icon" type="image/x-icon" href="IDECO_ICON_FAVICON">
  <link rel="apple-touch-icon" href="IDECO_ICON_FAVICON">
  <title>Доступ заблокирован</title>
  <style type="text/css">%l</style>
</head>

<body>
  <div class="widget info viewport_big">
    <span class="icon"></span>
    <div class="widget_content">
      <h1>Доступ заблокирован</h1>
      <p>Данный сайт предоставляет контент, заблокированный администратором. Причины␣
↪блокировки описаны во <a href="https://test.ru">внутреннем регламенте</a>.</p>
      <p>Ресурс категоризирован как:</p>
      %0
      <p>Для предоставления доступа к ресурсу обратитесь к системному администратору␣
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪одним из способов:</p>
      <p>Тел.: +7(000)000-00-00</p>
      <p>administrator@mail.ru</p>
      <p><a href="https://telegram.im/@admin">Отправить заявку в Telegram</a></p>
    </div>
  </div>
  <div class="blocked_content">
    <h1>Контент заблокирован</h1>
  </div>
</body>
```

Пример страницы:



6. Перезапустите сервис ideco-proxy-backend:

```
systemctl restart ideco-proxy-backend.service
```

7. Проверьте, корректно ли работают страницы ошибок, перейдя по запрещенным ссылкам.

16.3 Ограничение скорости

Подсказка: Название службы раздела *Ограничение скорости*: `ideco-shaper-backend`.
Список имен служб для других разделов, доступен по *ссылке*.

Подсказка: Правила *Предотвращения вторжений*, *Контроля приложений* и **Ограничение скорости** не обрабатывают трафик между локальными сетями и сетями филиалов.

Для исключения пользователя или групп пользователей из обработки правил *Предотвращения вторжений*, *Контроля приложений* и **Ограничения скорости** добавьте соответствующее правило в **Правила трафика -> Исключения**.

16.3.1 Настройка ограничения скорости

Для создания правила, необходимо перейти в раздел **Правила трафика -> Ограничение скорости** и нажать кнопку **Добавить**.

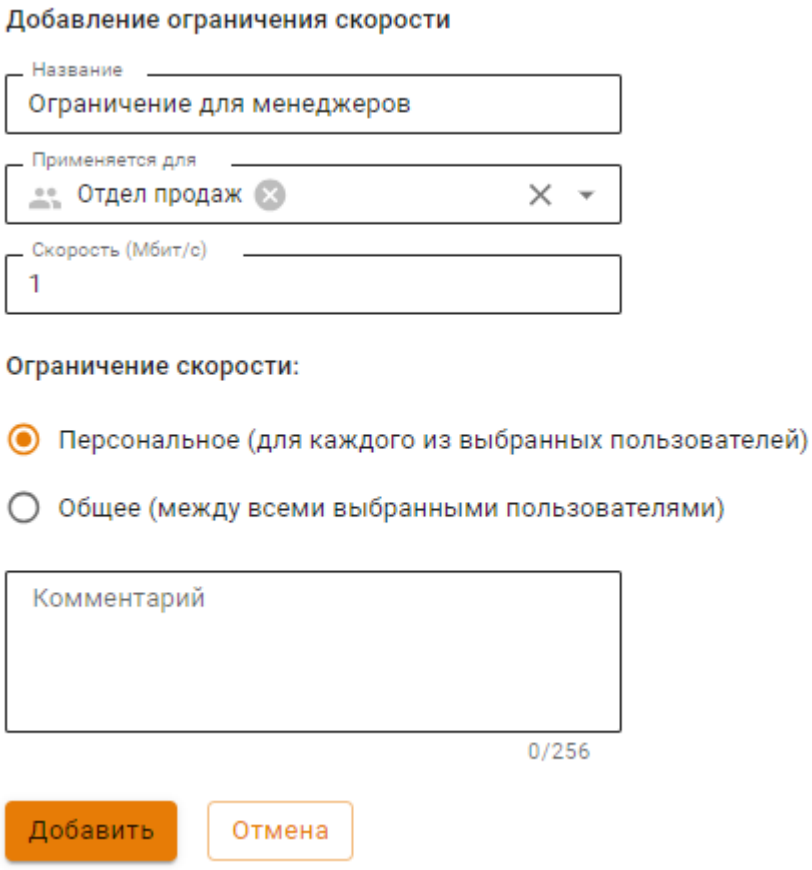
Далее заполните следующие поля:

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

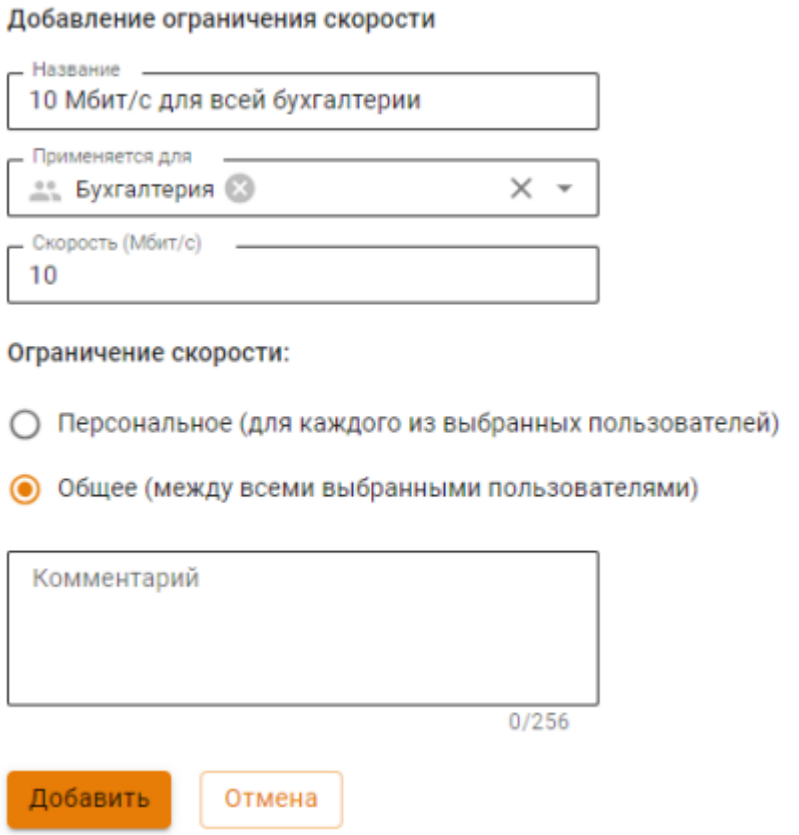
Для удобства настройки существует два типа ограничения скорости. Они могут быть применены для пользователей, групп, IP-адресов.

- **Персональное** - скорость будет ограничена для каждого из выбранных пользователей;
- **Общее** - скорость будет ограничена и разделится между всеми выбранными пользователями.

Например, при выборе персонального ограничения скорости, как на скриншоте ниже, лимит скорости для каждого менеджера будет равен 1 Мбит/с:



При выборе общего ограничения, как в следующем примере, ширина канала для всей бухгалтерии будет равна 10 Мбит/с:



Подсказка: При добавлении или редактировании правила, для его сохранения и применения нажмите кнопку **Применить** сверху над списком правил. Настройки будут применены.

Чтобы модуль работал, переведите ползунок в верхней части экрана около надписи **Ограничение скорости** в положение **Включен**.

Подсказка: Если не нажать кнопку **Применить** сверху над списком правил и покинуть раздел **Ограничение скорости**, то созданное правило сохранится, но не будет применяться. Для применения правила вернитесь в раздел **Ограничение скорости** и нажмите кнопку **Применить**.

Также сохраненные, но не примененные правила потеряются в случаях:

- При перезагрузке сервера;
- В случае переключения на другую ноду кластера.

Включить или выключить правило, изменить его приоритет, редактировать или удалить можно кнопками управления в столбце **Управление**:

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

16.3.2 Порядок применения правил

Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. То есть, если пользователь одновременно находится в нескольких группах, то к нему применяется правило, которое находится выше в списке правил.

16.3.3 Особенности

При подключениях пользователей по VPN к Ideco UTM из сети Интернет, скорость трафика в локальную сеть за Ideco UTM для них может быть ограничена в соответствии с правилами по ограничению скорости для конечного устройства в локальной сети.

При авторизации пользователей из локальной сети по VPN правила ограничения скорости для них применяться не будут.

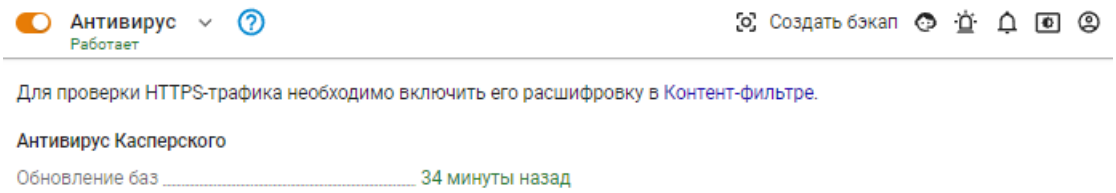
16.4 Антивирус

16.4.1 Основное

Подсказка: Название службы раздела *Антивирус*: `ideco-av-backend`.
Список имен служб для других разделов доступен по *ссылке*.

Для удобства администрирования оптимальные настройки производительности антивирусных модулей и настроек антивирусной фильтрации преднастроены в продукте и не требуют ручного конфигурирования. При необходимости настройки оптимизируются в обновлениях версий Ideco NGFW.

В разделе можно включить антивирус от Лаборатории Касперского. Антивирус лицензируется отдельно, его использование может быть ограничено условиями лицензии:



Модуль антивируса связан с прокси-сервером и **Контент-фильтром**, поэтому фильтрует веб-трафик при выполнении следующих условий:

- В разделе *Контент-фильтр* настроена расшифровка веб-трафика. HTTPS-сайт проверяется только в случае расшифровки HTTPS-трафика **Контент-фильтром**. Рекомендации по настройке фильтрации HTTPS представлены в *статье*;
- Веб-ресурс не находится в списках исключений прокси-сервера по назначению;
- Пользователь, к которому поступает трафик, не включен в исключения прокси-сервера по источнику.

Лицензирование антивируса Касперского:

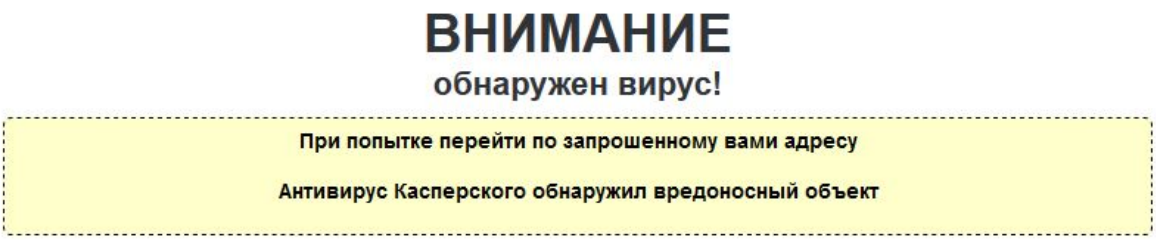
Данный модуль в нашем продукте создан на базе Kaspersky Anti-Virus Software Development Kit и приобретаются отдельно от Ideco NGFW. Для покупки обратитесь в отдел продаж.

Корпоративные ключи для других продуктов Лаборатории Касперского не могут быть использованы для его активации.

Проверка работы антивируса:

Можно попробовать скачать тестовые файлы с сайта: https://www.eicar.org/download-anti-malware-testfile.

В случае правильной настройки браузер выведет ошибку доступа:



16.5 Предотвращение вторжений

16.5.1 Основное

Подсказка: Система **Предотвращения вторжений** доступна только в **Enterprise-версии Ideco NGFW** для пользователей с активной подпиской на обновления.

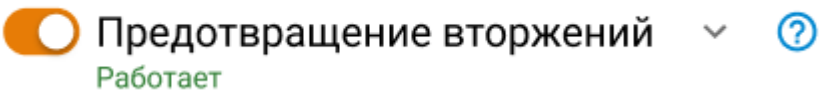
Профили **Предотвращения вторжений** и *Контроля приложений*, а также правила *Ограничения скорости* не обрабатывают трафик между локальными сетями и сетями филиалов.

Система предотвращения вторжений (IDS/IPS, Intrusion detection system / Intrusion prevention system) предназначена для:

- Обнаружения;
- Журналирования;
- Предотвращения атак злоумышленников на сервер, интегрированные службы и локальную сеть.

Предустановленные группы правил - сигнатур - включают блокирование активности троянских программ, шпионского ПО, бот-сетей, клиентов P2P и **торрент-трекеров**, вирусов, сети **TOR** (используемой для обхода правил фильтрации), анонимайзеров и т. д.

Для настройки системы перейдите на вкладку **Правила трафика -> Предотвращение вторжений**, включите или выключите опцию:



Раздел состоит из трех вкладок:

- *Группы сигнатур* - содержит список предустановленных групп сигнатур, либо распределенных по тактикам в соответствии с матрицей MITRE ATT&CK (матрица тактик и техник кибератак), либо в табличном виде;
- *Пользовательские сигнатуры* - позволяет добавить сигнатуры для обработки системой **Предотвращения вторжений**;
- *Настройки* - содержит информацию об обновлении баз IPS и сетях, защищенных от вторжений.

С 18 версии Ideco NGFW механизм работы системы **Предотвращения вторжений** изменился, появились возможности:

- Работать с правилами IPS на уровне сигнатур, фильтровать их и просматривать в удобном виде.
- Составлять независимые друг от друга наборы правил IPS и применять их только к необходимому трафику. Это стало возможным за счет появления профилей системы **Предотвращения вторжений**, которые назначаются на правила **Файрвола**.

Внимание: Чтобы модуль обрабатывал трафик, необходимо сначала создать профили IPS в разделе **Профили безопасности ->** *Предотвращение вторжений*, а затем использовать их в правилах **Файрвола**.

Сигнатуры, не используемые в профилях, и профили, не используемые в правилах **Файрвола**, не участвуют в обработке трафика!

Технические требования:

Для работы системы предотвращения вторжений требуются значительные вычислительные ресурсы. Предпочтительным являются многоядерные (4 и более ядер) процессоры. Минимальное количество оперативной памяти для использования системы: 16 Гб.

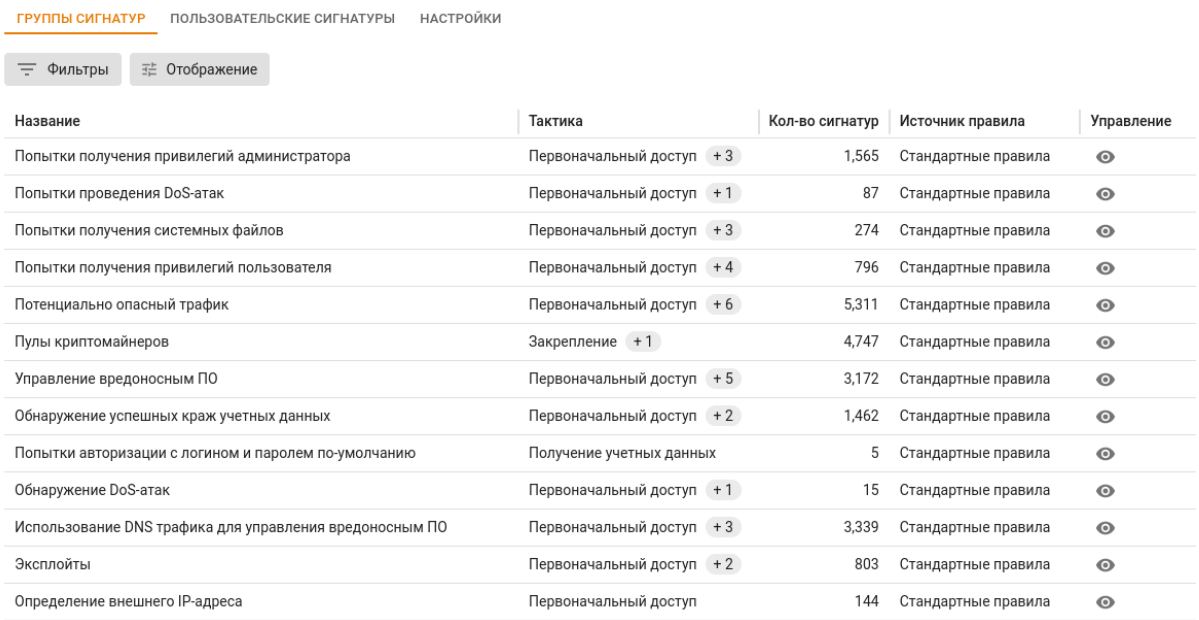
После включения системы проконтролируйте, что мощности вашего процессора достаточно для проверки трафика, следующего через шлюз.
В разделе **Мониторинг -> Графики загруженности** выберите параметр средняя загрузка (за 1, 5 и 15 минут).

Подробнее о Load Average.

16.5.2 Группы сигнатур

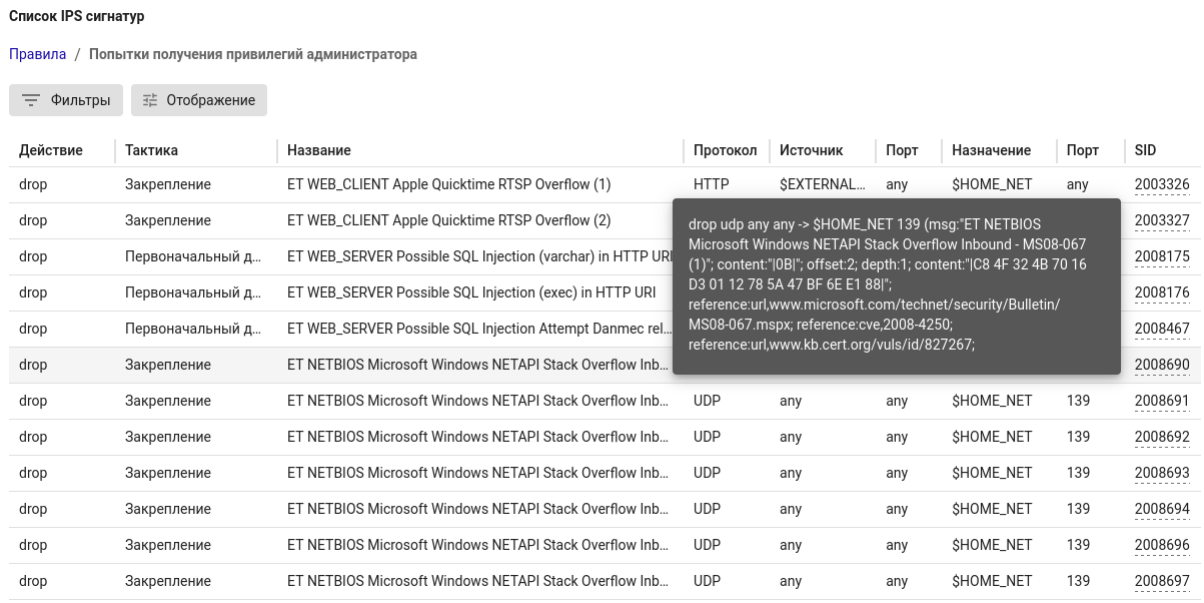
Основное

На вкладке **Группы сигнатур** доступны для просмотра предустановленные и *пользовательские* группы правил системы **Предотвращения вторжений**, распределенные по тактикам в соответствии с матрицей MITRE ATT&CK (матрица тактик и техник кибератак):



Название	Тактика	Кол-во сигнатур	Источник правила	Управление
Попытки получения привилегий администратора	Первоначальный доступ +3	1,565	Стандартные правила	
Попытки проведения DoS-атак	Первоначальный доступ +1	87	Стандартные правила	
Попытки получения системных файлов	Первоначальный доступ +3	274	Стандартные правила	
Попытки получения привилегий пользователя	Первоначальный доступ +4	796	Стандартные правила	
Потенциально опасный трафик	Первоначальный доступ +6	5,311	Стандартные правила	
Пулы криптомайнеров	Закрепление +1	4,747	Стандартные правила	
Управление вредоносным ПО	Первоначальный доступ +5	3,172	Стандартные правила	
Обнаружение успешных краж учетных данных	Первоначальный доступ +2	1,462	Стандартные правила	
Попытки авторизации с логином и паролем по-умолчанию	Получение учетных данных	5	Стандартные правила	
Обнаружение DoS-атак	Первоначальный доступ +1	15	Стандартные правила	
Использование DNS трафика для управления вредоносным ПО	Первоначальный доступ +3	3,339	Стандартные правила	
Эксплойты	Первоначальный доступ +2	803	Стандартные правила	
Определение внешнего IP-адреса	Первоначальный доступ	144	Стандартные правила	

Чтобы увидеть сигнатуры, входящие в группу, нажмите на . Чтобы увидеть содержание сигнатуры, наведите курсор мыши на SID:



Действие	Тактика	Название	Протокол	Источник	Порт	Назначение	Порт	SID
drop	Закрепление	ET WEB_CLIENT Apple Quicktime RTSP Overflow (1)	HTTP	$EXTERNAL...	any	$HOME_NET	any	2003326
drop	Закрепление	ET WEB_CLIENT Apple Quicktime RTSP Overflow (2)						2003327
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection (varchar) in HTTP URI						2008175
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection (exec) in HTTP URI						2008176
drop	Первоначальный д...	ET WEB_SERVER Possible SQL Injection Attempt Danmec rel...						2008467
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...						2008690
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008691
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008692
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008693
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008694
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008696
drop	Закрепление	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inb...	UDP	any	any	$HOME_NET	139	2008697

Описание групп сигнатур:

- **DNS поверх HTTPS** - обнаруживает/блокирует попытки сокрытия DNS-запросов по седьмому уровню TLS/SSL.
- **GeoIP Страны Восточной Европы** - обнаруживает/блокирует попытки доступа к IP-адресам, основываясь на базе данных MaxMind's GeoIP databases.
- **SSL-сертификаты, используемые вредоносным ПО и ботнетами** - обнаруживает/блокирует связь с командными центрами злоумышленников (C2).
- **Авторизация с подозрительным логином**
- **Анонимайзеры** - обнаруживает/блокирует анонимайзеры.
- **Атаки на получение прав пользователя** - обнаруживает/блокирует попытки получить учетные данные пользователя.
- **Атаки на получение привилегий администратора** - обнаруживает/блокирует попытки получить привилегии администратора.
- **Блокирование активности троянских программ** - обнаруживает/блокирует вредоносные трояны.
- **Блокирование атак** - обнаруживает/блокирует подозрительные IP-адреса (IP Reputation).
- **Блокирование крупных утечек информации** - обнаруживает/блокирует попытки получить данные и информацию.
- **Блокирование некорректных попыток получения привилегий пользователя** - обнаруживает/блокирует попытки получить привилегии пользователя.
- **Блокирование подозрительных RPC-запросов** - обнаруживает/блокирует удаленный вызов процедур (обычно используется для вызова удаленных функций на сервере, требующих результата действия).
- **Блокирование попыток запуска исполняемого кода** - обнаруживает/блокирует Remote Code Execution (RCE).
- **Блокирование утечек информации** - обнаруживает/блокирует попытки получить данные и информацию.
- **Запросы на скомпрометированные ресурсы** - обнаруживает/блокирует связи с командными центрами злоумышленников (C2).
- **Использование DNS-трафика для управления вредоносным ПО** - обнаруживает/блокирует связь с инфраструктурой управления и контроля (C2).

- **Нежелательное программное обеспечение** - обнаруживает/блокирует вредоносное ПО.
- **Неизвестный тип трафика** - обнаруживает/блокирует неопознанный/вредоносный трафик.
- **Нецелевое использование стандартных портов** - обнаруживает/блокирует использование стандартных портов в нелегитимных целях.
- **Обнаружение нарушений стандартов сетевых протоколов** - обнаруживает/блокирует обращения по нестандартным/прошитым протоколам.
- **Обнаружение подозрительной сетевой активности** - обнаруживает/блокирует аномалии или нестандартные действия легитимных пользователей в сети.
- **Обнаружение подозрительных команд** - обнаруживает/блокирует нестандартные команды, не характерные системам.
- **Обнаружение успешных краж учетных данных** - обнаруживает/блокирует кражи учетных данных.
- **Определение внешнего IP-адреса** - обнаруживает/блокирует попытки взаимодействия с инфраструктурой из внешних сетей.
- **Ошибки в сетевых протоколах** - обнаруживает/блокирует ошибки сетевых протоколов.
- **Подозрительное обращение к файлам** - обнаруживает/блокирует нестандартное обращение к файлам системы.
- **Попытки авторизации с логином и паролем по-умолчанию** - обнаруживает/блокирует попытки зайти под учетными данными с простыми паролями (аналогично брутфорс-атакам).
- **Попытки использования социальной инженерии** - обнаруживает/блокирует «атаку на человека».
- **Попытки получения привилегий администратора** - обнаруживает/блокирует попытки повысить привилегии до администратора и получить учетные данные администратора.
- **Попытки получения привилегий пользователя** - обнаруживает/блокирует попытки повысить привилегии и получить учетные данные пользователей.
- **Попытки получения системных файлов** - обнаруживает/блокирует системные конфигурации.
- **Попытки проведения DoS-атак** - обнаруживает/блокирует попытки провести атаки типа «отказ в обслуживании» (denial-of-service attack).
- **Попытки сканирования сети** - обнаруживает/блокирует сканирование сети.
- **Потенциально опасный трафик** - обнаруживает/блокирует зашифрованный или запутанный трафик, нестандартные запросы.
- **Пулы криптомайнеров** - обнаруживает/блокирует взаимодействие с сетями криптомайнеров и обращения для передачи нагрузки, которые криптомайнеры используют для майнинга.
- **Расширенная база правил (от Лаборатории Касперского)** - набор правил по обнаружению/блокировке от Лаборатории Касперского.
- **Телеметрия Windows** - обнаруживает/блокирует Телеметрию Windows.
- **Трафик устаревшего уязвимого ПО** - обнаруживает/блокирует связи с командными центрами злоумышленников (C2).
- **Управление вредоносным ПО** - обнаруживает/блокирует связь с инфраструктурой управления и контроля (C2), которую злоумышленники используют для управления зараженными устройствами и кражи конфиденциальных данных.
- **Целевое использование вредоносного ПО** - обнаруживает/блокирует вредоносное программное обеспечение.
- **Черный список IP-адресов** - обнаруживает/блокирует трафик к IP-адресам из баз safe-surf.ru и cinsarmy.com.
- **Эксплойты** - обнаруживает/блокирует использование уязвимостей систем (с индификатором CVE-XXXX-XXXXX).

История изменений групп сигнатур:

31.01.2024

- Улучшена блокировка Hola VPN и Browsec VPN **14.12.2023**
- Оптимизированы правила блокировки анонимайзеров **11.12.2023**
- Удалена категория Попытки выполнить системный вызов из IPS **07.12.2023**
- Добавлены новые правила для Windows Telemetry
- Не блокируется VPN-Browsec (добавлены новые правила для блокировки VPN-Browsec)
- Удалена категория Защита SMTP
- Телеметрия Windows блокирует Skype (убраны 2 правила телеметрии, которые блокировали функции Skype) **23.11.2023**
- Ошибка в формировании правил пула криптомайнеров (исправлена ошибка правил, блокирующая легитимные ресурсы по типу www.fr) **31.10.2023**
- Удалено правило «ET EXPLOIT Cisco IOS XE Web Server Possible Authentication Bypass Attempt (CVE-2023-20198) (Outbound)» из-за некорректности обработки **30.10.2023**
- Удаление из обработки ET категории web-app-attack (Атаки на веб-приложения) **12.10.2023**
- Удалена категория PT Open **02.10.2023**
- Убраны устаревшие и/или неработающие правила **20.09.2023**
- Оптимизация расширенных правил **21.07.2023**
- Отключено правило, блокирующее вход в AD. **21.06.2023:**
- Исправление входа в Active Directory **05.06.2023:**
- Улучшение блокировки криптомайнеров **30.05.2023:**
- Улучшение блокировки DoH-запросов **17.05.2023:**
- Добавлена блокировка эксплойта MSMQ-серверов (CVE-2023-21554) **06.04.2023:**
- Обновление черного списка
- Обновление источников детектирования DoH **09.03.2023:**
- Улучшение блокировки пулов криптомайнеров **06.03.2023:**
- Оптимизация срабатывания правил **02.03.2023:**
- Исправление работы FreeDNS
- Улучшение блокировки TOR и анонимайзеров **01.03.2023:**
- Исправление работы DropBox **21.02.2023:**
- Обновление источников черного списка IP-адресов
- Исправление работы Windows Store **13.02.2023:**
- Добавлен список SSL-сертификатов вредоносного ПО **06.02.2023:**
- Исправление доступа к Skype for Business **26.01.2023:**
- Исправление доступа к Autodesk Fusion 360 **29.12.2022:**
- Обновлен черный список IP-адресов **26.12.2022:**
- Обновлен список адресов криптомайнеров **13.12.2022:**
- Блокировка источников ВПО уязвимости нулевого дня в продуктах Microsoft Exchange Server **29.11.2022:**
- Исправления доступа к ipinfo.io **26.10.2022:**

- Удалена отдельная категория правил **Список НКЦКИ**
  Источник данных атакующих НКЦКИ остается в составе баз, являясь частью «Черного списка IP-адресов» **21.10.2022:**
- Удалена группа **Активные ботнеты**
  Актуальные угрозы блокируются с помощью «Черных списков IP-адресов»

16.5.3 Пользовательские сигнатуры

На вкладке можно добавить кастомные сигнатуры **Предотвращения вторжений**. Сигнатура - это шаблон, который позволяет идентифицировать определенные виды вредоносного трафика, аномалий в протоколах или известных атак.

> **Внимание:** Сигнатуры, не используемые в профилях **Предотвращения вторжений**, и профили, не используемые в правилах **Файрвола**, не участвуют в обработке трафика!

Если добавленные пользователем сигнатуры валидны, они также появятся в таблице *Группы сигнатур*, их можно будет использовать при создании *профилей* ***Предотвращения вторжений***.

Описание валидной сигнатуры

Валидная сигнатура состоит из трех основных частей:

- Действие при совпадении правила;
- Заголовок, определяющий протокол, IP-адреса или сети отправителя и получателя сетевых пакетов, порты и направление трафика;
- Опции, определяющие специфику сигнатуры.

> **Внимание:** Проверка валидности сигнатур может занять некоторое время. Если одна из сигнатур не пройдет проверку, появится сообщение об ошибке у названия системы **Предотвращения вторжений**. Подробности можно будет увидеть в логах службы.

Пример валидной сигнатуры. Генерирует предупреждение, если обнаружен HTTP GET-запрос, в URI которого встречается слово `rule`:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request Containing Rule␣
↪in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:
↪"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1;)
```

где:

- `alert` - действие. Перечень валидных действий:
  - `alert`- сгенерировать предупреждение;
  - `pass` - принять пакет;
  - `drop` - отбросить пакет и сгенерировать предупреждение;
  - `reject` - отправить ошибку `RST/ICMP unreach` отправителю пакета;
  - `rejectdst` - отправить пакет с ошибкой `RST/ICMP error` получателю исходного пакета;
  - `rejectboth` - отправить пакеты с ошибкой `RST/ICMP error` отправителю и получателю исходного пакета.
- `http $HOME_NET any -> $EXTERNAL_NET any` - заголовок, в том числе:

- `http` - протокол. Валидные протоколы: сетевого уровня (`ip`, `icmp`), транспортного уровня (`tcp`, `udp`), уровня представления (`tls`, `ssl`), прикладного уровня (`http`, `dns`, `ssh`, `ftp` и другие);
- `$HOME_NET` - сети отправителя, указанные в настройках в **Правила трафика -> Предотвращение вторжений -> Настройки -> Сети, защищенные от вторжений**;
- `any` - порты отправителя/получателя;
- `->` - направление трафика. Два валидных значения: `->` - проверка трафика слева направо, `<>`- проверка трафика в обоих направлениях. Значение `<-` не является валидным. Например, при проверке пакетов, идущих из сети A в сеть B, валидное значение в сигнатуре - `сеть A -> сеть B`, невалидное значение - `сеть B <- сеть A`;
- `$EXTERNAL_NET` - сети получателя (значения, которые не попадают в `$HOME_NET`).

- `(msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1;)` - опции, заключенные в скобки и разделенные точкой с запятой.

Особенности опций валидной сигнатуры:

Порядок опций важен, его изменение влияет на порядок обработки. Например, указанная в примере опция `content:"GET"` относится к опции `http.method`, а опция `content:"rule"` - к опции `http.uri`.

Опции бывают двух основных видов:

- Влияющие на инспекцию трафика. При добавлении сигнатуры их необходимо указать. Описание некоторых опций из примера:
  - `flow` - состояние соединения, направление следования пакета и др.;
  - `content` - содержимое пакета, по которому производится сопоставление.
- Метаопции - опции, не влияющие на инспекцию трафика, но влияющие на способ информирования о срабатывании сигнатуры. Список некоторых метаопций из примера:
  - `msg` - информация о сигнатуре и возможном алерте;
  - `classtype` - информация о классе правил и алертов (короткое и длинное название, приоритет);
  - `sid` - уникальный номер сигнатуры;
  - `rev` - версия сигнатуры;
  - `metadata` - дополнительная информация о сигнатуре. Формат `metadata`:

```
metadata: key value;
metadata: key value, key value;
```

Примеры указания тактики MITRE:

1. Формат в правилах Касперского - `metadata: MITRE TA0001`:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (metadata: MITRE TA0001; msg:""; sid:1;)
```

- `TA0001` - MITRE_ID

2. Формат в Emerging Threats - `metadata: mitre_tactic_id TA0001`:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (metadata: mitre_tactic_id TA0001; msg:"
↪"; sid:1;)
```

- `TA0001` - MITRE_ID

Предупреждение: Символы `;` и `"` имеют специальное значение и должны быть экранированы с помощью символа `\` в случае их использования в значениях опций.

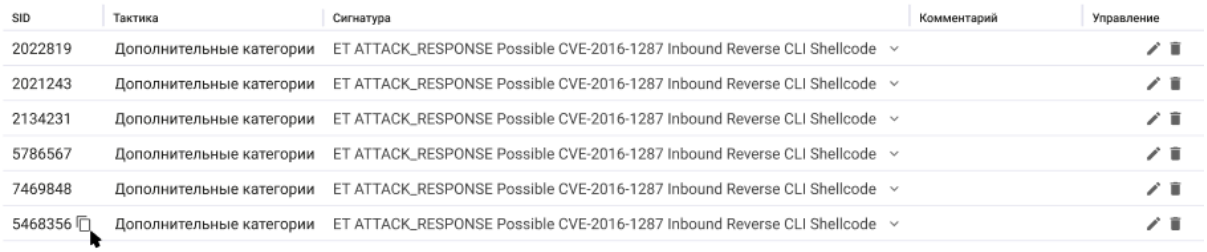
Полная документация по форматам сигнатур представлена по ссылке.

Создание пользовательской сигнатуры

Чтобы добавить сигнатуру, выполните действия:

1. Нажмите **Добавить** и выберите способ добавления: **Вручную** или **Из файла**.

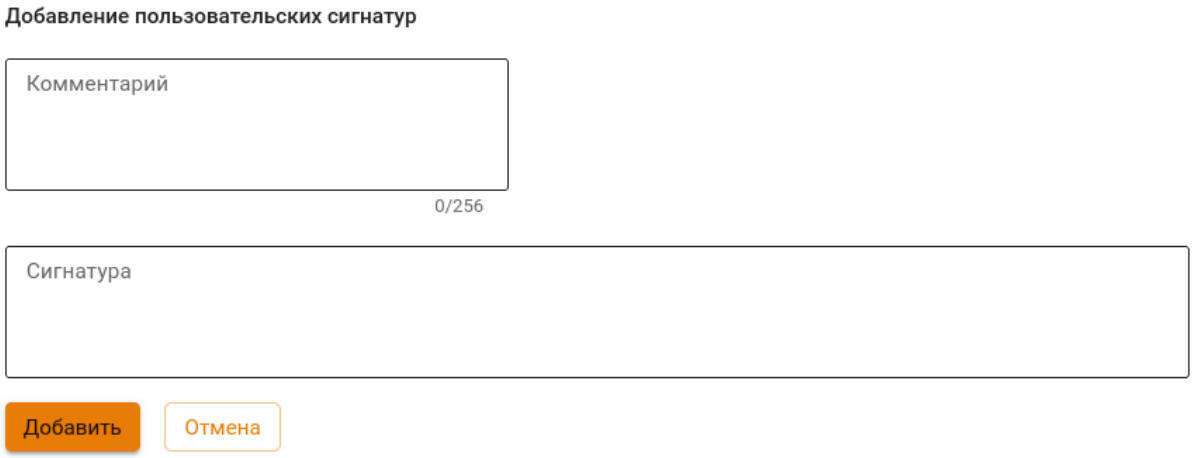
2. Если выбран способ **Из файла**, в открывшемся окне выберите необходимый текстовый файл. Если сигнатуры соответствуют требуемой структуре, а значения SID у всех сигнатур в файле уникальны и находятся в нужном диапазоне, то эти сигнатуры появятся в таблице:



Подсказка: Значения SID добавляемых вручную или из файла сигнатур должны быть уникальными и находиться в диапазоне 1-999999.

Если структура сигнатур не соответствует нужной, Ideco NGFW выдаст ошибку с указанием номеров строк файла, где найдены ошибки.

3. Если был выбран способ **Вручную**, в открывшейся форме введите комментарий, сигнатуру и нажмите **Добавить**:



При наличии большого количества сигнатур в таблице воспользуйтесь кнопкой **Фильтры**.

Пример создания исключения с конкретным адресом и сигнатурой:

Описание примера. Пользователю необходимо добавить в исключения передачу трафика, который блокируется конкретной сигнатурой **Предотвращения вторжений**, для конкретного отправителя (192.168.10.10) и получателя (1.1.1.1).

Если пользователь добавит в исключения конкретную сигнатуру, то разрешит этот трафик для всех адресов. Если же он создаст исключение в разделе **Правила трафика -> Исключения**, то исключается конкретный адрес для всех сигнатур.

Пользовательская сигнатура позволит создать исключение для конкретного адреса и конкретной сигнатуры одновременно. Для добавления такой сигнатуры:

1. Перейдите в раздел **Отчеты и журналы -> События безопасности** и найдите ID сигнатуры, которую необходимо добавить в исключения.

2. Скопируйте содержание выбранной сигнатуры, которое отобразится при наведении мыши на ID.

3. Перейдите в раздел **Правила трафика -> Предотвращение вторжений -> Пользовательские сигнатуры** и нажмите **Добавить -> Вручную**.

4. Вставьте скопированный лог в поле **Сигнатура** и измените в нем:

- Действие `drop` на `pass`;
- Значения `$HOME_NET` и/или `$EXTERNAL_NET` на нужный адрес отправителя/получателя;
- Значение `sid` на любое уникальное в диапазоне 1-999999.

Опции, не влияющие на инспекцию трафика, из сигнатуры можно удалить. Если при добавлении сигнатуры оставить опцию `msg`, то в разделе **Отчеты и журналы -> События безопасности** будут сохраняться логи по данной сигнатуре.

4. Нажмите **Добавить**.

Пример содержания сигнатуры в разделе **Отчеты и журналы -> События безопасности**:

```
drop http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET HUNTING DDoS-Guard Hosted␣
↪Content"; flow:established,to_client; http.stat_code; content:"200"; http.server;␣
↪content:"DDoS-Guard"; nocase; bsize:10; fast_pattern; reference:url,malwarebytes.
↪com/blog/threat-intelligence/2023/01/crypto-inspired-magecart-skimmer-surfaces-via-
↪digital-crime-haven; classtype:bad-unknown; sid:2043310; rev:1; metadata:attack_
↪target Client_Endpoint, created_at 2023_01_17, deployment Perimeter, performance_
↪impact Moderate, confidence Low, signature_severity Minor, updated_at 2023_01_17,␣
↪reviewed_at 2024_10_14;)
```

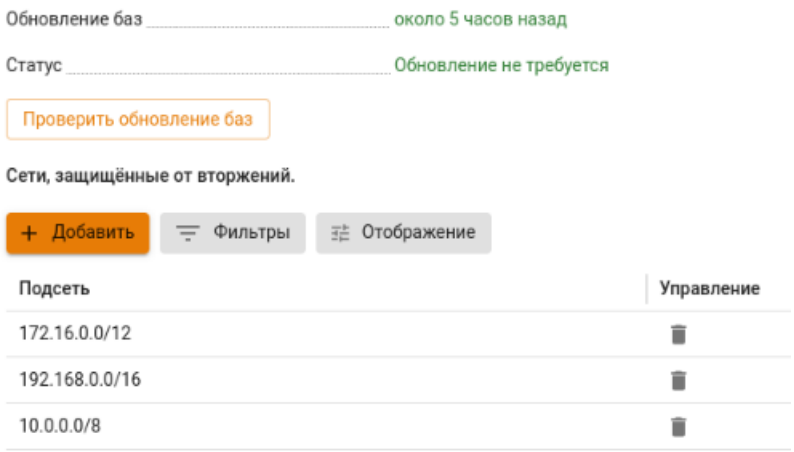
Пример пользовательской сигнатуры:

```
pass http 192.168.10.10 any -> 1.1.1.1 any (flow:established,to_client; http.stat_
↪code; content:"200"; http.server; content:"DDoS-Guard"; nocase; bsize:10; fast_
↪pattern; sid:234;)
```

16.5.4 Настройки

Основное

На вкладке можно проверить статус обновления баз системы **Предотвращение вторжений** и отредактировать список сетей, защищенных от вторжений:



Для добавления подсети в список защищенных нажмите **Добавить** и в поле **Подсеть** укажите локальные сети, обслуживаемые NGFW (сети локальных интерфейсов NGFW, маршрутизируемые на них сети удаленных сегментов локальной сети предприятия).

При наличии большого количества подсетей в таблице воспользуйтесь кнопкой **Фильтры**.

Предупреждение: **Не указывайте** сети, принадлежащие внешним сетевым интерфейсам NGFW и внешним сетям. Указанные здесь сети участвуют в правилах системы **Предотвращения вторжений** как локальные.

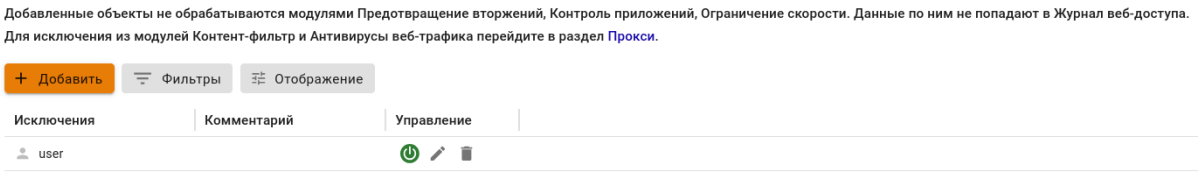
Предупреждение: При работе системы **Предотвращения вторжений не используйте** сторонние DNS-серверы для компьютеров, т.к служба определяет зараженные устройства по DNS-запросам, проходящим через нее.
При использовании внутреннего домена AD рекомендуется:

- В компьютерах указать DNS-сервер Ideco NGFW в качестве единственного DNS-сервера;
- В настройках DNS-сервера на NGFW указать Forward-зону для локального домена.

16.6 Исключения

16.6.1 Основное

Правила в разделе **Исключения** отключают трафик из обработки системы *Предотвращения вторжений*, *Контроля приложений* и *Ограничение скорости*, данные по ним не попадают в монитор трафика.



Если после исключения объекта из обработки доступ к ресурсу не появился, проверьте, не блокируется ли DNS-запрос. Для этого перейдите в раздел **Отчеты и журналы -> События безопасности -> Журнал IPS**. Если запрос блокируется, то в журнале срабатываний наведите на строку и нажмите .

При наличии большого количества исключений в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Если в качестве DNS-сервера у пользователя указан локальный адрес сервера Ideco NGFW, то исключения работать не будут. Весь трафик, идущий на адреса локальных и VPN-интерфейсов Ideco NGFW, всегда обрабатывается службой фильтрации трафика.

16.7 Объекты

Подсказка: Название службы раздела *Объекты*: `ideco-alias-backend`.
Список имен служб для других разделов доступен по *ссылке*.

Типы объектов:

Список IP-адресов Список стран

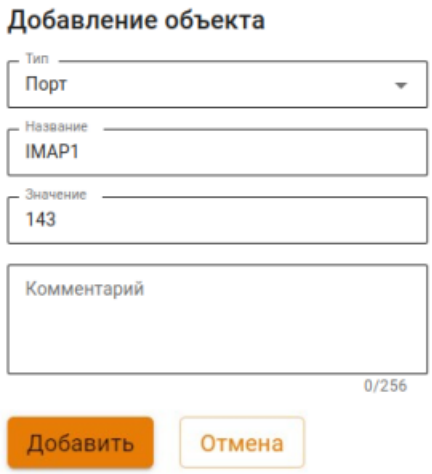
- **Зона** - логическое объединение сетевых интерфейсов. Используется для настройки правила файрвола на несколько интерфейсов.
- **IP-адрес** - IP-адрес IPv4. Пример: 10.0.0.1;
- **Диапазон IP-адресов** - диапазон IP-адресов от первого до последнего, указанного в диапазоне. Пример: 10.0.0.1-10.0.0.25;
- **Подсеть** - логический блок IP-адресации. Префикс маршрутизации выражается в нотации CIDR. Пример: 10.0.0.0/24;
- **Домен** - символьное имя, служащее для идентификации объектов в интернете. Пример: ideco.ru;
- **Порт** - номер порта от 1 до 65535. Пример: 3389;
- **Диапазон портов** - диапазон портов от первого до последнего, указанного в диапазоне. Пример: 1024-65535;
- **Время** - диапазон времени. Пример: ПН 9:00-18:00 ;
- **Список IP-объектов** - группа объектов, состоящая из отдельных объектов, таких как IP-адрес, диапазон IP-адресов, подсеть и домен. Пример: 10.0.0.1, 10.0.0.4, 10.0.0.126;
- **Список IP-адресов** - объект, состоящий из списка IP-адресов. Для создания объекта требуется загрузить любой текстовый файл (например: TXT/CSV). При этом в одной строке должен быть один адрес. Также допускается использование маски /24 или 255.255.255.0
- **Порты** - группа портов. Пример: 25, 110, 143, 445, 465, 587, 993, 995;
- **Расписание** - группа диапазонов времени. Пример: ПН 9:00-12:00, ВТ 13:00-18:00;
- **Список стран** - группа объектов, содержащая GeoIP.

16.7.1 Создание объектов

Чтобы создать объект, необходимо выполнить следующие действия:

1. Перейдите в раздел **Правила трафика -> Объекты** и нажмите кнопку **Добавить** в левом верхнем углу экрана.

2. Выберите тип, название и значение объекта. По желанию можно указать произвольный комментарий не длиннее 128 символов.



3. Нажмите кнопку **Добавить**.

При наличии большого количества объектов в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Важно:

- Для создания групп объектов предварительно необходимо создать сами объекты. К группам объектов относятся: список IP-адресов, порты и расписание.
- Для создания объекта типа **Список IP-адресов** используйте любой текстовый файл (например: TXT/CSV), в котором будут перечислены нужные IP-адреса. Правила заполнения:
  - в строке должен быть один адрес;
  - допускается использование маски /24 или 255.255.255.0.
- Для создания объекта типа **Зона** необходимо:
  - Создать соответствующий объект в разделе **Правила трафика -> Объекты**;
  - Перейти в раздел **Сервисы -> Сетевые интерфейсы** и при редактировании интерфейса добавить его в нужную зону.
- Зоны для IPsec-подключений создаются автоматически при создании соответствующих подключений.
- Объекты типа **IP-адрес** и **Порт** можно создавать непосредственно при создании правил файрвола, введя нужный IP-адрес или порт в соответствующих полях.

Подсказка: В Ideco NGFW также используется специальный алиас - **Любой**. Если при создании правила в каком-либо из полей выбран этот алиас, правило будет распространяться на все объекты, доступные к выбору в том же поле.

---

17. Профили безопасности

Профили безопасности это наборы параметров для фильтрации трафика различными модулями и позволяет настраивать разные политики безопасности независимо друг от друга.

Профили WAF будут использоваться только в публикациях сервисов в разделе *Обратный прокси*. Остальные профили - в правилах раздела *Файрвол*.
Один и тот же профиль будет использоваться в нескольких правилах.

17.1 Что позволят делать профили

- Выбирать, какой трафик отправлять на глубокий анализ и фильтрацию. Это позволит уменьшить нагрузку на модули фильтрации.
- Настраивать независимые друг от друга политики безопасности для модулей фильтрации.

17.2 Web Application Firewall

Подсказка: Название служб раздела **Web Application Firewall**: `ideco-waf-backend`; `ideco-waf-event-syncer`.
Список служб для других разделов доступен по *ссылке*.

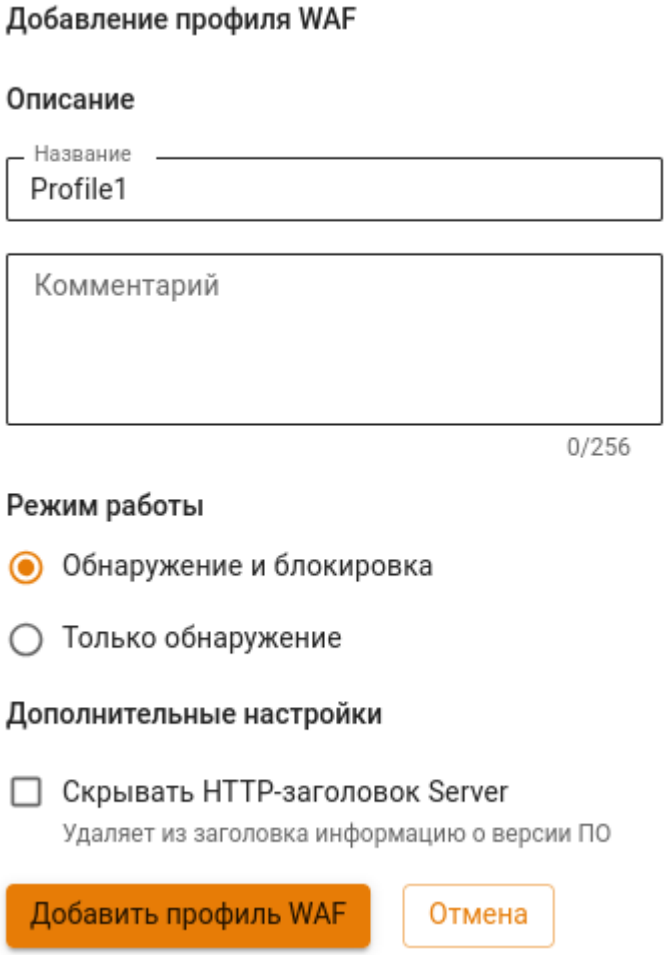
Использование WAF-профилей позволит настроить параметры защиты для опубликованного веб-ресурса. Профиль создается в разделе **Профили безопасности -> Web Application Firewall**.

Предупреждение: Создание WAF-профилей не влияет на фильтрацию трафика. Чтобы включить фильтрацию, нужно использовать WAF-профили в разделе ***Обратный прокси*** при создании правила.

17.2.1 Создание профиля WAF

Для создания профиля WAF выполните действия:

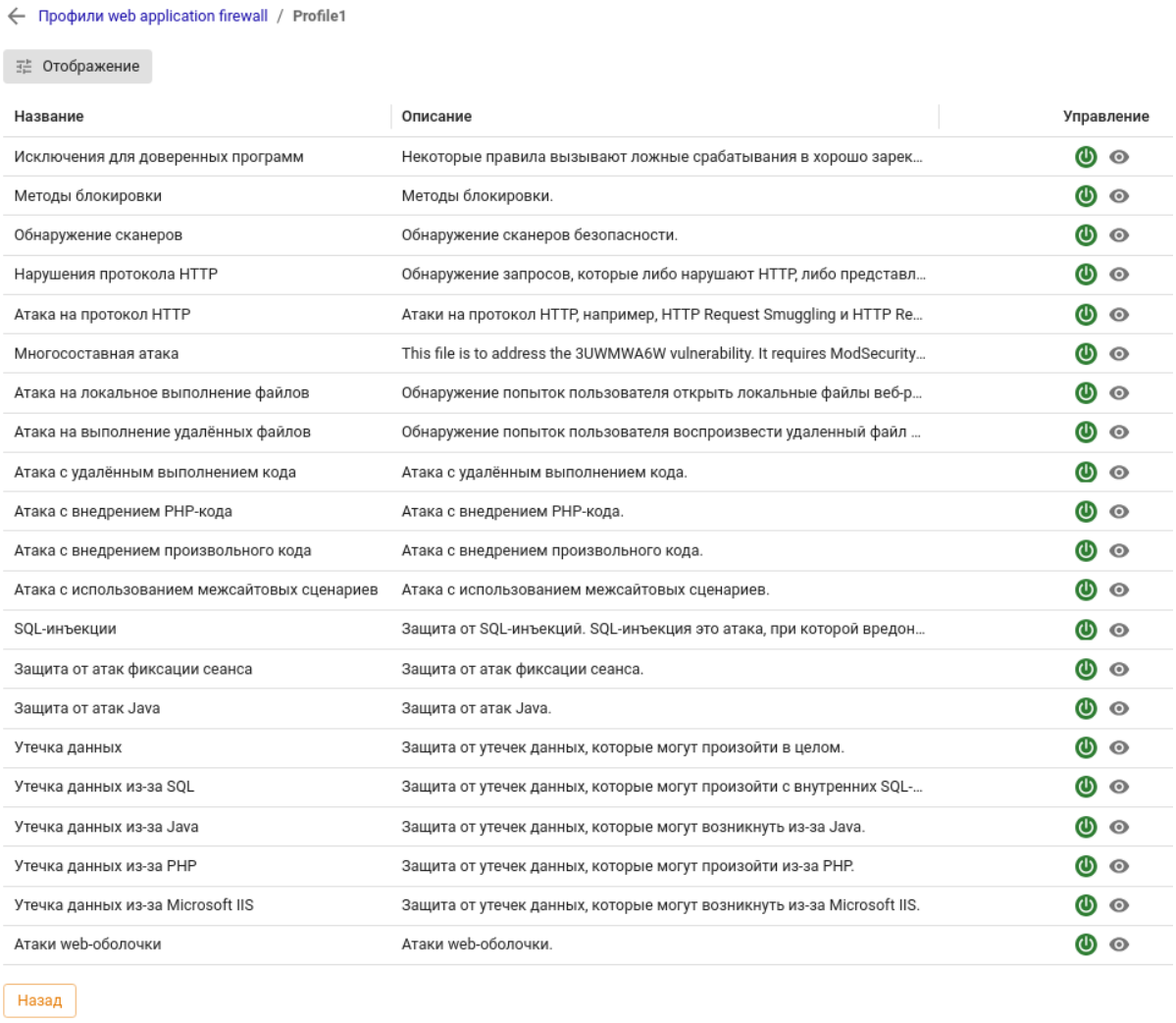
1. Нажмите **Добавить** и заполните поля:



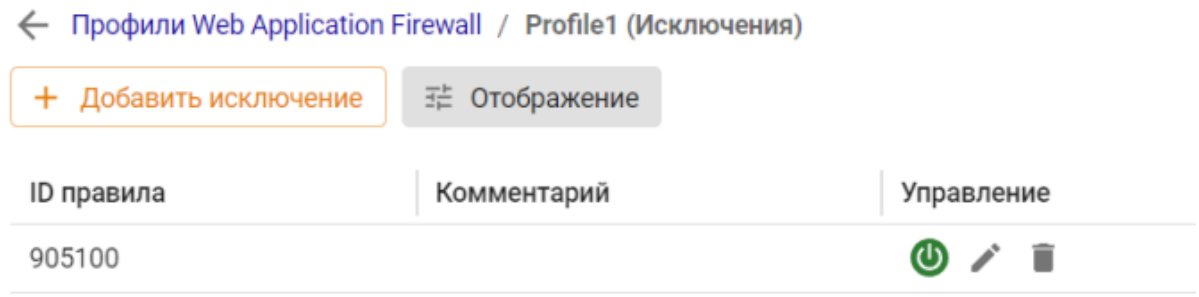
- **Название** - введите название профиля;
- **Комментарий** - введите пояснение для профиля;
- **Режим работы**:
  - **Обнаружение и блокировка** - подозрительные запросы будут блокироваться и логироваться WAF;
  - **Только обнаружение** - подозрительные запросы будут логироваться WAF, но не будут блокироваться;
- **Дополнительные настройки**:
  - **Скрывать HTTP-заголовок Server** - позволяет скрыть данные, идентифицирующие сервер.

2. Нажмите **Добавить профиль**.

3. Нажмите на , выберите **Категории** и включите/отключите правила:



4. Чтобы добавить определенное правило в исключения, нажмите на , выберите **Исключения** и нажмите **Добавить исключение**. Укажите ID правила (его можно найти в журнале в разделе **Отчеты и журналы -> События безопасности -> *Web Application Firewall*:

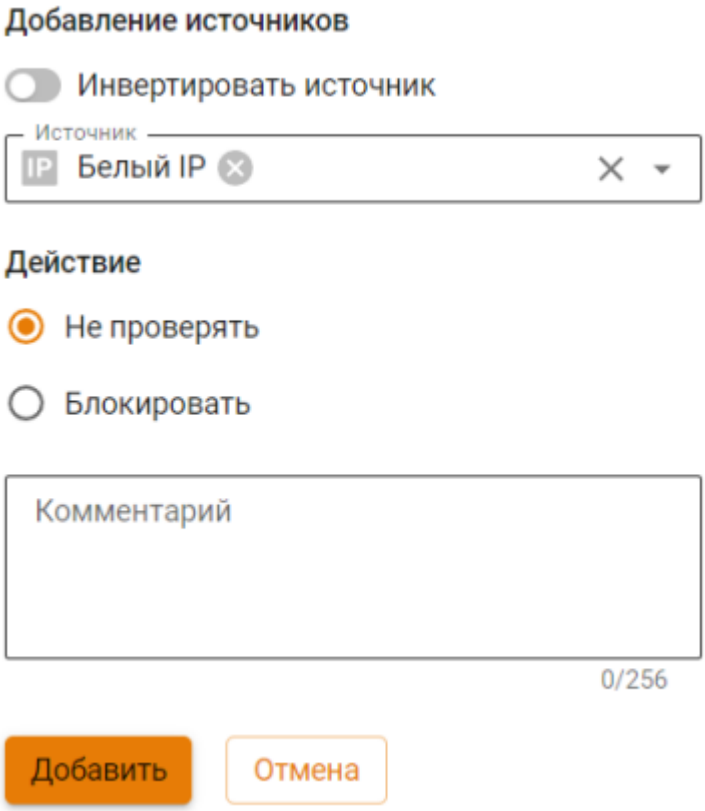


5. Чтобы настроить белый и черный список подсетей профиля, нажмите на , выберите **Белый и черный списки**:

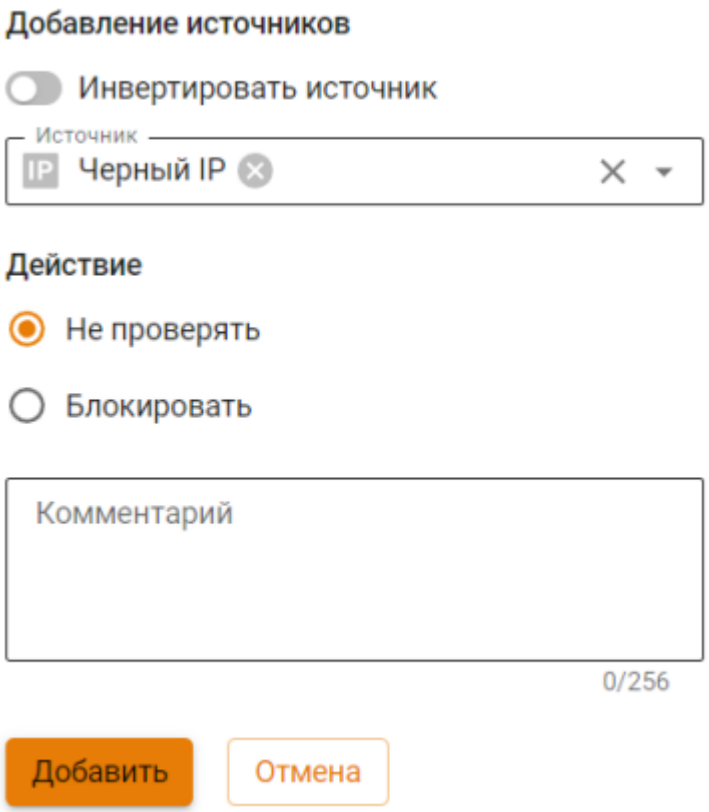
Подсказка: В каждый профиль WAF можно добавить не более двух тысяч источников в белых и черных списках. Если лимит будет превышен, появится соответствующее сообщение в уведомлениях.

- Для добавления в белый список нажмите **Добавить источник**. Укажите необходимые IP-адреса и

подсети, а затем выберите действие **Не проверять**:



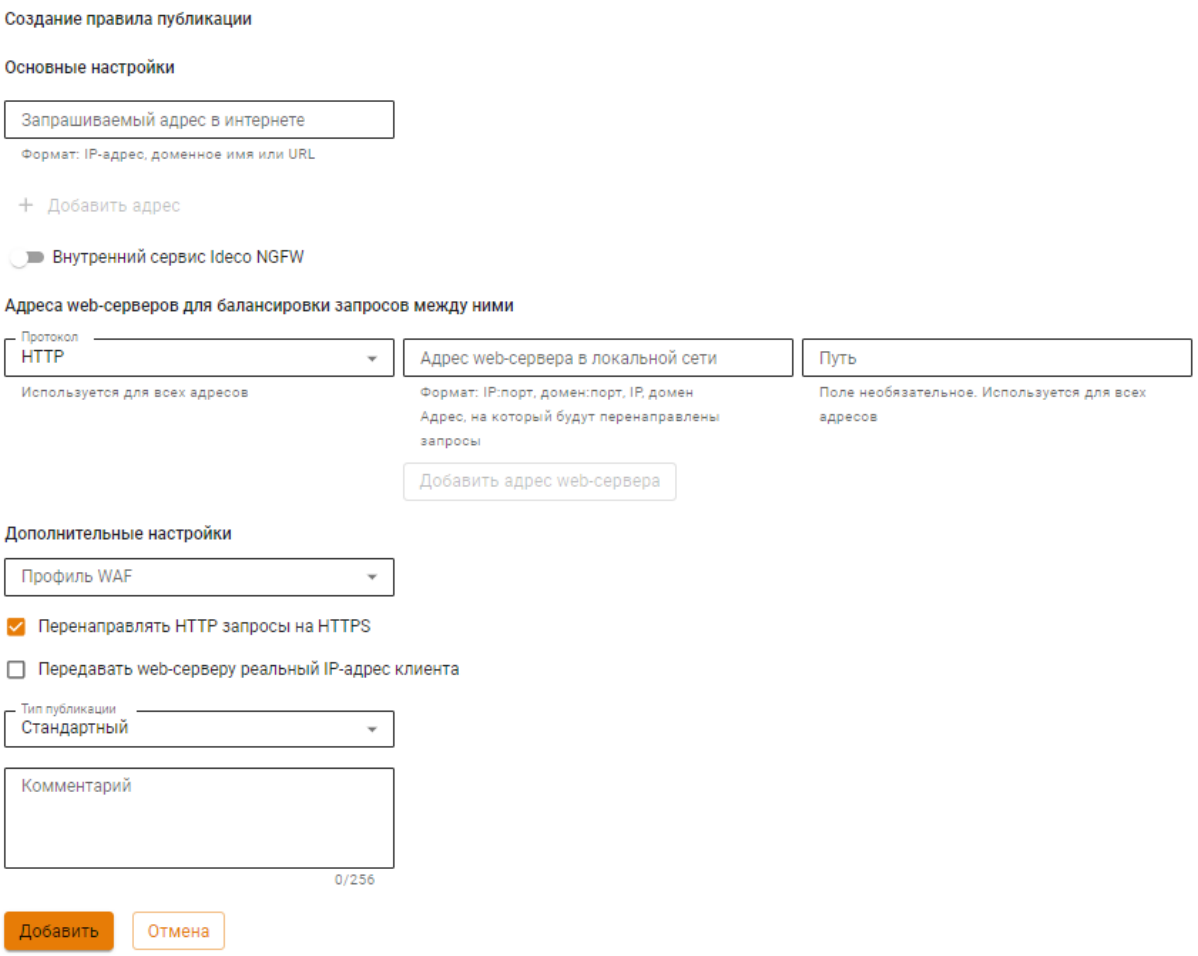
- Для добавления в черный список нажмите **Добавить источник**. Укажите необходимые IP-адреса и подсети, а затем выберите действие **Блокировать**:



17.2.2 Использование профиля WAF в правиле Обратного прокси

1. Перейдите в раздел **Сервисы -> Обратный прокси** и нажмите **Добавить**.

2. Заполните поля:



- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных адресов нажмите кнопку **Добавить адрес**;
- **Адрес web-сервера в локальной сети** - введите IP-адрес из локальной сети, на который будут перенаправляться пользователи;
- **Протокол** - выбранный протокол используется для всех адресов в правиле;
- **Адрес web-сервера в локальной сети** - адрес, на который будут перенаправлены запросы;
- **Путь** - поле необязательное и используется для всех адресов;
- **Перенаправлять HTTP-запросы на HTTPS** - включите настройку, если ваш сайт работает только по протоколу HTTPS, но при этом вы не хотите терять посетителей, обратившихся к вашему сайту по HTTP;
- **Профиль WAF** - выберите созданный ранее профиль WAF;
- **Передавать web-серверу реальный IP-адрес клиента** - включите настройку, если нужно, чтобы публичный IP-адрес клиента при обратном проксировании не заменялся на адрес NGFW.

3. Нажмите **Добавить**.

17.3 Контроль приложений

В разделе **Профили безопасности -> Контроль приложений** создаются профили, разрешающие или запрещающие доступ пользователя к заданному администратором набору приложений и протоколов. Для выявления протоколов приложений осуществляется глубокий анализ трафика (Deep Packet Inspection - DPI).

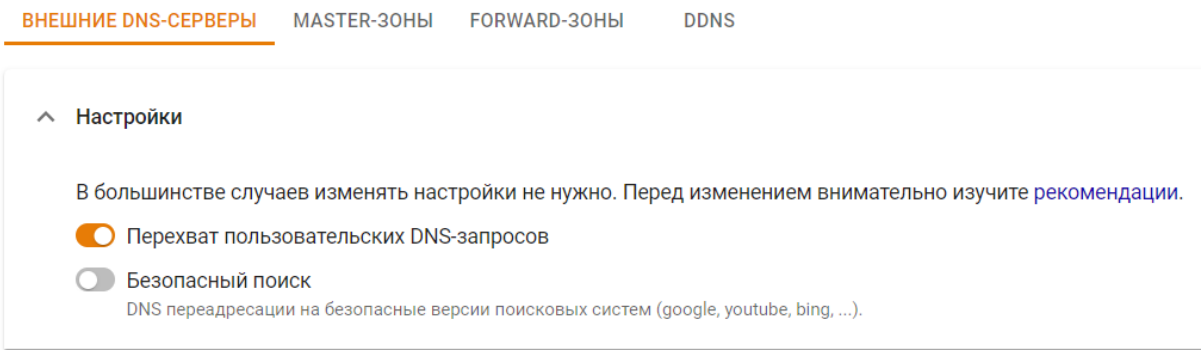
При наличии большого количества профилей в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Названия служб раздела *Контроль приложений*: `ideco-app-backend` и `ideco-app-control-nfq`.\

Список имен служб для других разделов доступен по *ссылке*.

В 18 версии Ideco NGFW созданные в разделе **Профили безопасности -> Контроль приложений** профили применяются при создании/редактировании и включении правил в разделе **Правила трафика -> Файрвол**.

Чтобы трафик фильтровался модулем **Контроль приложений**, создайте для всех локальных интерфейсов правило FORWARD, содержащее нужный профиль безопасности. Если в разделе **Сервисы -> DNS -> Внешние DNS-серверы** включена опция **Перехват пользовательских DNS-запросов** (по умолчанию включена), нужно также создать аналогичное правило INPUT:



Внимание: Если профиль не добавлен в правила таблицы FORWARD или INPUT раздела **Правила трафика -> Файрвол**, трафик не будет фильтроваться модулем **Контроль приложений**.

17.3.1 Особенности обработки трафика с помощью профиля Контроля приложений

С 18 версии изменили последовательность обработки трафика. В предыдущих версиях FORWARD- и INPUT-трафик сначала проходит модуль **Контроль приложений**, а затем **Файрвол**. В 18 версии в модуль **Контроль приложений** отправляется трафик, соответствующий только разрешающему правилу **Файрвола** с включенной проверкой через профиль **Контроля приложений**.

Файрвол Ideco NGFW анализирует трафик, чтобы найти подходящее правило, и применяет его. Если в списке есть несколько правил с одними и теми же условиями, применяется правило, стоящее выше по списку. Запрещающие правила **Файрвола** сразу блокируют соответствующий трафик и не проходит дополнительную проверку в модуле **Контроль приложений**.

Чтобы через модуль **Контроль приложений** проходил трафик, для которого нет разрешающего правила в таблицах FORWARD или INPUT, рекомендуем создать и включить в **Файрволе** правило с источником **Локальные интерфейсы** и назначением **Любой**, разместив его в конец таблицы. В этом случае трафик, который не был найден в правилах **Файрвола**, пройдет проверку **Контролем приложений**. Трафик, не учтенный правилами **Файрвола**, но запрещенный профилями **Контроля приложений**, будет заблокирован.

Подсказка: Принцип создания профилей **Контроля приложений** в 18 версии NGFW: все протоколы и

приложения, которые не были запрещены, остаются разрешены.

17.3.2 Особенности работы с Ideco Center

В Ideco Center 17.6 были добавлены профили **Контроля приложений**. Принцип создания профилей и их применения в правилах **Файрвола** был такой же, как и в Ideco NGFW версии 17. Но синхронизация профилей между Ideco NGFW и Ideco Center не осуществлялась. Поэтому рекомендуем начать обновление на 18 версию с Ideco Center и далее приступить к обновлению синхронизированного Ideco NGFW.

После обновления Ideco Center на 18 версию правила, синхронизированные из Ideco Center в **Правила трафика -> Контроль приложений**, будут доступны только для просмотра и не будут влиять на обработку трафика в подключенных NGFW.

Перечень доступных на вкладке Доступ к приложениям групп приложений и протоколов:

- Стриминговые сервисы
- Веб-ресурсы
- Компьютерные игры
- Видео-контент
- Реклама
- Контент для взрослых
- Передача данных
- Облачные сервисы
- Виртуальные ассистенты
- RPC
- IoT-Scada
- Удаленный доступ
- Обновления ПО
- Сети
- Социальные сети
- Криптовалюты
- Обмен файлами
- Системные
- Базы данных
- VoIP
- VPN
- Кибербезопасность
- Музыка
- Командная работа
- Магазины
- Чаты и мессенджеры
- Почта
- Медиа-контент
- Майнинг

Описание приложений и протоколов, доступных для создания профилей:

1kxun
Китайский видеосервис. На нем представлены различные анимационные фильмы, телевидение, спорт и кино.

AccuWeather
Частная американская медиа-компания, предоставляющая коммерческие услуги по прогнозированию погоды по всему миру.

Activision
Американская компания по изданию и разработке компьютерных игр, разработчик Call of Duty.

AdobeConnect
Платформа веб-конференций, которая позволяет пользователям проводить онлайн-встречи, вебинары.

ADS_Analytic_Track
Отслеживание и аналитика рекламы (mobile marketing analytics and attribution platform).

AFP
Протокол представительского и прикладного уровней сетевой модели OSI, предоставляющий доступ к файлам в MacOS X.

AJP
Протокол, который может проводить входящие запросы с веб-сервера до сервера приложений.

Alibaba
Китайская публичная компания, работающая в сфере интернет-коммерции, владелец веб-порталов Taobao.com, Tmall, Alibaba.com и ряда других.

AliCloud
Компания, предоставляющая ресурсы для облачных вычислений, дочерняя компания Alibaba Group.

Amazon
Американская компания-разработчик платформ электронной коммерции и публично-облачных вычислений.

AmazonAlexa
Облачная голосовая служба Amazon.

AmazonAWS
Коммерческое публичное облако, поддерживаемое и развиваемое компанией Amazon.

AmazonVideo
Стриминговый сервис компании Amazon.

AmongUs
Многопользовательская компьютерная игра.

AMQP
Открытый протокол прикладного уровня для передачи сообщений между компонентами системы.

ANSI_C1222
Протокол прикладного уровня, предназначенный для использования в сетях электросчетчиков Smart Grid.

AnyDesk
Приложение для удаленного рабочего стола, распространяемое AnyDesk Software GmbH.

Apple
Компания-производитель смартфонов и компьютерной техники.

AppleiCloud
Облачное хранилище от компании Apple, которое предоставляет пользователям доступ к их музыке, фотографиям, документам и другим файлам с любого устройства.

AppleiTunes
Медиаплеер для организации и воспроизведения музыки и фильмов, разработанный компанией Apple и бесплатно распространявшийся для платформ MacOS и Windows.

ApplePush
Сервис, созданный Apple для отправки уведомлений от сторонних приложений на устройства Apple.

AppleSiri
Облачный персональный помощник и вопросно-ответная система компании Apple.

AppleStore
Онлайн-магазин техники Apple и аксессуаров к ней.

AppleTVPlus
Американский стриминговый сервис, принадлежащий и управляемый компанией Apple.

Armagetron
Свободная компьютерная игра для операционных систем Linux, Windows, MacOS, FreeBSD и AmigaOS 4.

AVAST
Семейство антивирусных программ, разработанных компанией Avast для операционных систем Windows, MacOS, Android и iOS.

AVASTSecureDNS
Сервис защищенных DNS-серверов от компании Avast.

Azure
Облачная платформа компании Microsoft. Предоставляет возможность разработки, выполнения приложений и хранения данных на серверах, расположенных в распределенных дата-центрах.

BACnet
Сетевой протокол, применяемый в системах автоматизации зданий и сетях управления.

Badoo
Приложение для онлайн-знакомств.

BeckhoffADS
Открытый протокол обмена данными ADS на базе TCP/IP для общения с контроллером, разработанный BECKHOFF.

BFCP
Протокол предназначен для обмена презентациями и демонстрации рабочего стола в рамках видеоконференции.

BFD
Протокол обнаружения двунаправленной пересылки, который используется для обнаружения неисправностей между двумя маршрутизаторами или коммутаторами.

BGP
Протокол динамической маршрутизации.

BITCOIN
Криптовалюта, использующая децентрализованную систему для записи транзакций в блокчейне.

BitTorrent
Пиринговый протокол для кооперативного обмена файлами через интернет.

BJNP
Протокол обнаружения служб локальной сети, используемый принтерами и сканерами Canon. Компьютерные системы используют этот протокол для автоматического обнаружения устройств Canon в сети.

Bloomberg
Американская компания, информационное агентство, один из двух ведущих американских поставщиков финансовой информации для профессиональных участников финансовых рынков.

Bluesky
Bluesky Socialg представляет собой децентрализованную социальную платформу для микроблогов.

Cachefly
Поставщик сети доставки контента.

CAPWAP
Сетевой протокол с возможностью взаимодействия, который позволяет центральному контроллеру доступа к беспроводной локальной сети управлять набором беспроводных оконечных точек.

Cassandra
Распределенная система управления базами данных, относящаяся к классу NoSQL-систем и рассчитанная на создание масштабируемых хранилищ данных, представленных в виде хеша.

Ceph
Свободная программная объектная сеть хранения, обеспечивающая как файловый, так и блочный интерфейсы доступа.

CHECKMK
Протокол используется для мониторинга серверных и контейнерных систем в ИТ-инфраструктуре.

CIP
Информационно-управляющий протокол, который обеспечивает обмен сообщениями ввода/вывода в реальном времени и прямой обмен информационными сообщениями.

CiscoSkinny
Корпоративный (проприетарный) VoIP-протокол для управления взаимодействием между оконечными телефонными устройствами и сервером телефонной системы (IP-АТС).

CiscoVPN
Протокол VPN, разработанный компанией Cisco Systems.

Citrix
Программа, предоставляющая доступ к приложениям и рабочим столам с удаленного клиентского устройства с помощью ресурсов Citrix Virtual Apps and Desktops и Citrix DaaS.

ClickHouse
Система управления базами данных с открытым исходным кодом, построенная на основе колонок.

Cloudflare
Американская компания, предоставляющая услуги CDN, защиту от DDoS-атак, безопасный доступ к ресурсам и серверы DNS.

CloudflareWarp
Бесплатный VPN от CloudFlare, который проксирует все сетевые запросы в системе (включая обновления Windows и др. ПО, трафик многопользовательских игр, торренты).

CNN
Американский круглосуточный кабельный телеканал новостей.

COAP
Протокол для взаимодействия простых устройств, например, датчиков малой мощности, выключателей, клапанов, которые управляются или контролируются удаленно через интернет.

CoD_Mobile
Бесплатный шутер для устройств iOS и Android.

Collectd
Демон Unix, который собирает, передает и хранит данные о производительности компьютеров и сетевого оборудования.

Controller_Area_Network
Стандарт протокола связи, используемый для обмена данными между устройствами в автомобильной промышленности и других промышленных приложениях.

Corba
Технологический стандарт написания распределенных приложений, продвигаемый консорциумом OMG, и соответствующая ему информационная технология.

CPHA
Алгоритм хеширования, который может использоваться для безопасного хранения паролей в РТС.

Crashlytics
Инструмент отчетности о сбоях, который помогает выявлять ошибки.

Crossfire
Южнокорейский тактический сетевой шутер от первого лица, разработанный компанией SmileGate.

CryNetwork
Составной модуль для создания многопользовательских игр.

Cybersec
Компании сферы кибербезопасности: checkpoint.com norton.com, kaspersky.com, fortinet.com.

Dailymotion
Французский видеохостинг.

DataSaver
Функция для Chrome, которая позволяет значительно сократить использование мобильных данных.

Dazn
Спортивный стриминговый сервис.

DCERPC
Система удаленного вызова процедур, разработанная для Distributed Computing Environment.

Deezer
Французский интернет-сервис потоковой передачи музыки.

DHCP
Протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети.

DHCPV6
Протокол динамического конфигурирования хостов для межсетевого протокола версии 6.

Diameter
Сеансовый протокол, созданный, отчасти, для преодоления некоторых ограничений протокола RADIUS.

DirecTV
Компания прямого теле-радиовещания в США, сигналы цифрового спутникового телевидения и радио передаются на территорию США и Латинской Америки.

Discord
Кроссплатформенная проприетарная система мгновенного обмена сообщениями с поддержкой VoIP и видеоконференций, предназначенная для использования различными сообществами по интересам.

DisneyPlus
Американский сервис потокового вещания типа OTT на основе подписки.

DLEP
Протокол маршрутизации с учетом радиосвязи (RAR).

DNP3
Протокол передачи данных, используемый для связи между компонентами АСУ ТП.

DNS
Протокол, используемый для получения IP адреса хоста по его доменному имени.

DNScrypt
Протокол шифрования DNS-трафика.

Dofus
Массовая многопользовательская ролевая онлайн-игра (MMORPG), использующая Flash-графику и фэнтезийный сеттинг.

DoH_DoT
Протокол защиты DNS-трафика (запросов и ответов) от перехвата и подмены. В том числе включает в себя обычные DNS-запросы адресов DoT/DoH-серверов.

Dota2
Многопользовательская командная компьютерная игра в жанре MOBA, разработанная и изданная корпорацией Valve.

DRDA
Набор протоколов, обеспечивающих возможность связи между программами и системами баз данных на разных платформах и позволяющих распределять реляционные данные по нескольким платформам.

Dropbox
Файловый хостинг компании Dropbox Inc, включающий персональное облачное хранилище, синхронизацию файлов и программу-клиент.

DTLS
Протокол передачи данных, обеспечивающий защищенность соединений для протоколов, использующих датаграммы.

EAQ
Entitade Aferidora da Qualidade de Banda Larga - эксцентричный протокол VoIP/конференц-связи, который редко встречается в реальной жизни.

eBay
Американская компания, предоставляющая услуги в областях интернет-аукционов и интернет-магазинов.

Edgecast
Децентрализованное приложение для потоковой передачи видео, построенное на собственной технологии блокчейн THETA со смарт-контрактами.

eDonkey
Файлообменная сеть, построенная по принципу P2P на основе сетевого протокола прикладного уровня MFTP.

EGP
Устаревший протокол обмена информации между маршрутизаторами нескольких автономных систем.

Elasticsearch
Тиражируемая программная поисковая система.

ElectronicArts
Американская публичная транснациональная корпорация, занимающаяся распространением и изданием компьютерных игр (FIFA, Battlefield).

EpicGames
Американская компания, занимающаяся разработкой компьютерных игр и программного обеспечения, в частности - Fortnite.

ETHEREUM
Криптовалюта и платформа для создания децентрализованных онлайн-сервисов на базе блокчейна.

EthernetGlobalData
Протокол связи, разработанный GE Fanuc Automation для обмена данными в реальном времени между устройствами автоматизации и системами управления с использованием стандартной технологии Ethernet.

EthernetIP
Промышленный сетевой стандарт, который поддерживает неявный обмен сообщениями (обмен сообщениями ввода/вывода в реальном времени), явный обмен (обмен сообщениями) или оба и использует широко распространенные коммерческие чипы связи Ethernet и физические носители.

Ether-S-Bus
Промышленный протокол управления, используемый компанией SAIA Burgess.

EtherSIO
Протокол используется для передачи данных между программируемыми логическими контроллерами и удаленными устройствами ввода/вывода производства компании Saia-Burgess Controls Ltd.

Facebook
Крупнейшая социальная сеть в мире, которой владеет компания Meta Platforms.

FacebookMessenger
Приложение для обмена мгновенными сообщениями и видео, созданное Meta.

FacebookVoip
Голосовые и видеозвонки в FaceBook.

FastCGI
Клиент-серверный протокол взаимодействия веб-сервера и приложения, дальнейшее развитие технологии CGI.

FbookReelStory
Короткие видеоролики на Facebook.

FINS
Открытый протокол связи поддерживаемый большинством контроллеров и сетей разработки компании Omron.

FIX
Протокол передачи данных, являющийся международным стандартом для обмена данными между участниками биржевых торгов в режиме реального времени.

FLUTE
Доставка файлов по однонаправленному транспорту.

FortiClient
Комплексное решение безопасности, предназначенное для защиты компьютеров и ноутбуков. Также имеет версии для планшетов и мобильных устройств под управлением Android и Apple iOS.

FTP_CONTROL
Протокол, предназначенный для передачи файлов в компьютерных сетях.

FTP_DATA
Протокол доступа, предназначенный для удаленной передачи файлов в компьютерных сетях.

FTPS
Расширение широко используемого протокола передачи файлов FTP, которое добавляет поддержку для криптографических протоколов уровней транспортной безопасности и защищенных сокетов.

Fuze
Файловая система в пользовательском пространстве для Unix-подобных операционных систем, позволяющая непривилегированным пользователям создавать собственные файловые системы без редактирования кода ядра.

GaijinEntertainment
Частная компания, разработчик и издатель компьютерных игр, в частности - War Thunder.

Gearman
Платформа приложений с открытым исходным кодом, предназначенная для распределения соответствующих компьютерных задач на несколько компьютеров.

GeForceNow
Облачный игровой сервис компании Nvidia.

GenshinImpact
Компьютерная игра в жанре action-adventure с открытым миром и элементами RPG, разработанная китайской компанией miHoYo Limited.

Git
Распределенная система управления версиями.

GitHub
Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки.

GitLab
Веб-инструмент жизненного цикла DevOps с открытым исходным кодом, представляющий систему управления репозиториями кода для Git с собственной вики, системой отслеживания ошибок, CI/CD пайплайном и другими функциями.

GMail
Бесплатная почтовая служба от компании Google. Предоставляет доступ к почтовым ящикам через веб-интерфейс и по протоколам POP3, SMTP и IMAP, а также в приложении Gmail на Android.

Gnutella
Протокол для распределенного обмена файлами, в основном, музыкальными.

Google
Американская технологическая компания, которая специализируется на поисковых технологиях, искусственном интеллекте, онлайн-рекламе, программном обеспечении, бытовой электронике.

GoogleCall
Аудио- и видеозвонки, совершаемые с помощью (любых) приложений Google (например, Google Meet).

GoogleChat
Коммуникационный сервис, разработанный компанией Google.

GoogleClassroom
Облачная платформа для организации образовательного процесса.

GoogleCloud
Предоставляемый компанией Google набор облачных служб, которые выполняются на той же самой инфраструктуре, которую Google использует для своих продуктов, предназначенных для конечных потребителей.

GoogleDocs
Текстовый онлайн-процессор, входящий в состав бесплатного веб-пакета редакторов GoogleDocs.

GoogleDrive
Сервис хранения, редактирования и синхронизации файлов, разработанный компанией Google. Его функции включают хранение файлов в интернете, общий доступ к ним и совместное редактирование.

GoogleMaps
Набор приложений, построенных на основе бесплатного картографического сервиса и технологии, предоставляемых компанией Google.

GoogleMeet
Сервис видео-телефонной связи и видеоконференций, разработанный компанией Google.

GoogleServices
Набор приложений и API, которые реализуют дополнительные возможности на устройствах Android. Сервисы Google для мобильных устройств включают основные приложения: Google Play, Gmail, Google Map, YouTube и Chrome.

GoTo
Американская компания, предоставляющая услуги телефонных систем для бизнеса, контакт-центров и продукты для ИТ-поддержки.

GRE
Протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems.

GTP_C
Группа протоколов соединения на основе IP, используемая в сетях GSM, UMTS и LTE.

GTP_PRIME
Группа протоколов связи на основе IP, используемых для передачи услуг пакетной радиосвязи общего пользования (GPRS) в сетях GSM, UMTS, LTE.

GTP_U
Протокол используется для транспортировки пользовательских данных между пакетной сетью и радиосетью.

GTP
Протокол туннелирования GPRS.

Guildwars
Фэнтезийная массовая многопользовательская ролевая онлайн-игра, разработанная компанией ArenaNet и выпущенная компанией NCsoft в 2005 году.

H323
Набор стандартов для передачи мультимедиа-данных по сетям с пакетной передачей.

HalfLife2
Компьютерная игра, научно-фантастический шутер от первого лица.

HAProxy
Программное обеспечение для балансировки нагрузки для TCP и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов.

HART-IP
Адресуемый по магистрали удаленный преобразователь по IP, в основном используется для обмена данными в качестве стандартного глобального протокола между интеллектуальными устройствами и системой управления и некоторой интеллектуальной системой.

HBO
Американский телеканал, принадлежащий компании WarnerMedia.

Heroes_of_the_Storm
Онлайн-игра, разработанная Blizzard Entertainment для Microsoft Windows и MacOS.

HiSLIP
Коммуникационный протокол для измерительного и тестового оборудования с использованием технологии VISA.

HL7
Стандарт обмена, управления и интеграции электронной медицинской информации.

HLS
Протокол для потоковой передачи медиа на основе HTTP, разработанный компанией Apple.

HotspotShield
Условно-бесплатное программное обеспечение для организации виртуальной частной сети, обеспечивающей безопасную передачу данных по шифрованному соединению, защищенному от прослушивания.

HP_VIRTGRP
Протокол HP Virtual Machine Group Management - часть пакета виртуализации, используемого в серверных средах HP.

HSRP
Протокол маршрутизации семейства FHRP (англ. First-hop redundancy protocols), разработанный компанией Cisco и стандартизованный в RFC 2281.

HTTP_Connect
Метод HTTP, который запускает двустороннюю связь с запрошенным ресурсом. Метод можно использовать для открытия туннеля.

HTTP_Proxy
Тип прокси-сервера, который действует как сервер-посредник между клиентом и веб-сервером.

HTTP
Протокол для получения с серверов гипертекстовых документов в формате HTML.

HTTP2
Вторая крупная версия сетевого протокола HTTP, используемая для доступа к World Wide Web.

Huawei
Трафик устройств Huawei.

HuaweiCloud
Мобильное облако Huawei.

Hulu
Стриминговый сервис по подписке, принадлежащий The Walt Disney Company.

i3D
Протокол с низкой задержкой, используемый в основном игровыми серверами.

IAX
Протокол обмена VoIP-данными между IP-ATC Asterisk и другим аналогичным софтсвичом или VoIP-телефоном.

IceCast
Протокол для организации потокового цифрового аудиовещания и видеовещания.

iCloudPrivateRelay
Сервис для маскировки IP-адреса пользователя с целью сохранения его конфиденциальности.

ICMP
Протокол третьего уровня модели OSI, который используется для диагностики проблем со связностью в сети.

ICMPV6
Протокол управляющих сообщений для межсетевого протокола версии 6.

IEC60870
Набор протоколов для контроля и управления с использованием постоянного соединения.

IEC62056
Набор стандартов Международной электротехнической комиссии для обмена данными учета электроэнергии.

IEEE-C37118
Потоковый протокол для обмена и передачи данных синхрофазоров (или PMU), которые фиксируют устойчивое состояние или динамический отклик энергосистемы. Обеспечивает высокоскоростную передачу большого количества данных в режиме реального времени.

IFLIX
Малайзийский бесплатный видеосервис.

IGMP
Протокол управления групповой передачей данных в сетях, основанных на протоколе IP. Используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы.

iHeartRadio
Американская платформа бесплатного вещания, подкастов и потокового радио, принадлежащая iHeartMedia.

IMAP
Протокол для доступа к электронной почте.

IMAPS
Протокол для осуществления доступа к электронной почте, включающий в себя обязательное шифрование.

IMO
Веб-сервис и кроссплатформенное приложение для мгновенного обмена сообщениями и VoIP-звонков.

Instagram
Американская социальная сеть для обмена фотографиями и видео.

IP_in_IP
Протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет.

IP_PIM
Семейство многоадресных протоколов маршрутизации для IP сетей, созданное для решения проблем групповой маршрутизации.

IPP
Протокол, используемый для передачи документов на печать.

IPSec
Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

iQIYI
Китайская онлайн-видеоплатформа, предлагающая широкий спектр оригинального и лицензионного контента, включая фильмы, драмы, развлекательные шоу и аниме.

IRC
Протокол прикладного уровня для обмена сообщениями в режиме реального времени.

ISO9506-1-MMS
Протокол передачи данных реального времени и команд диспетчерского управления между сетевыми устройствами и/или программными приложениями.

Jabber
Протокол, основанный на XML, свободный для использования протокол для мгновенного обмена сообщениями и информацией о присутствии в режиме, близком к режиму реального времени.

JRMI
Протокол удаленного вызова методов Java.

JSON-RPC
Протокол удаленного вызова процедур, использующий JSON для кодирования сообщений.

Kafka
Распределенный программный брокер сообщений с открытым исходным кодом.

KakaoTalk_Voice
Популярный в Южной Корее мессенджер, который поддерживает мгновенную передачу сообщений, позволяет отправлять файлы, а также совершать аудиозвонки и видеозвонки.

KakaoTalk
Бесплатное мобильное приложение для мгновенного обмена сообщениями для смартфонов.

KCP
Протокол связи, который максимально использует полосу пропускания для надежной связи с низкой задержкой.

Kerberos
Протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.

Kismet
Сетевой детектор, анализатор пакетов и система обнаружения вторжений для беспроводных локальных сетей стандарта 802.11.

KNXnet_IP
Протокол автоматизации зданий, который обеспечивает обмен данными и управляющей информацией через IP-сети, расширяя стандарт KNX для автоматизации дома и зданий.

LastFM
Сервис для прослушивания музыки онлайн.

LDAP
Протокол для доступа к службе каталогов X.500.

LDP
Протокол маршрутизации, используемый для установления и поддержания путей с коммутацией меток в сети с многопротокольной коммутацией меток (MPLS).

Likee
Социальная сеть, пользователи которой могут создавать и распространять короткие музыкальные видео.

Line
Приложение для смартфонов и ПК, средство моментального обмена сообщениями.

LineCall
Система звонков/видеоконференций, используемая в популярном мобильном приложении для обмена сообщениями LINE.

Linkedin
Американская социальная сеть для поиска и установления деловых контактов.

LISP
Протокол маршрутизации, построенный на идее разделения топологического расположения точки присоединения к сети и идентификации узла.

Livestream
Платная стриминговая платформа, которая позволяет клиентам загружать живое видео со своих мобильных устройств и компьютерных камер через интернет.

LLMNR
Протокол, основанный на формате пакета данных DNS, который позволяет компьютерам выполнять разрешение имен хостов в локальной сети.

LoLWildRift
League of Legends: Wild Rift — мобильная игра в жанре MOBA.

LotusNotes
Программный продукт, платформа для автоматизации совместной деятельности рабочих групп, содержащий в себе средства электронной почты, персональных и групповых электронных календарей, службы мгновенных сообщений и среду исполнения приложений делового взаимодействия.

MapleStory
Бесплатная многопользовательская ролевая онлайн-игра, разработанная южнокорейской компанией Wizet.

Mastodon
Бесплатное программное обеспечение с открытым исходным кодом для запуска самостоятельных служб социальных сетей. Он имеет функции микроблогов, аналогичные Twitter.

MDNS
Многоадресный протокол DNS, используемый для преобразования имени хостов в IP-адреса в небольших сетях, не включающих локальный сервер имен.

Megaco
Протокол для управления функциями шлюза на границе пакетной сети.

Memcached
Протокол кеширования, используемый для ускорения динамических веб-приложений путем кеширования данных в памяти.

MerakiCloud
Сервис компании Cisco, предоставляющий доступ к облачным технологиям.

MGCP
Протокол управления медиашлюзами.

Microsoft
Американская корпорация-разработчик в сфере проприетарного программного обеспечения для различного рода вычислительной техники: персональных компьютеров, игровых приставок, КПК, мобильных телефонов и прочего.

Microsoft365
Набор веб-сервисов на основе платформы Microsoft Office, электронная почта, функции для общения и управления документами, которые распространяются на основе подписки по схеме программное обеспечение как услуга.

Mining
Протоколы, использующиеся программами-майнерами.

Modbus
Протокол, основанный на архитектуре ведущий - ведомый, применяется в промышленности для организации связи между электронными устройствами.

Monero
Криптовалюта на основе протокола CryptoNote, ориентированная на повышенную конфиденциальность транзакций.

MongoDB
Протокол, используемый для взаимодействия клиентов и серверов MongoDB.

MPEG_TS
Протокол для передачи аудиоданных и видеоданных, описанных в MPEG2.

MpegDash
Протокол потоковой передачи данных, предоставляющий возможность доставки потокового мультимедиа-контента через интернет по протоколу HTTP.

MQTT
Упрощенный сетевой протокол, работающий поверх, ориентированный на обмен сообщениями между устройствами по принципу «издатель - подписчик».

MS_OneDrive
Облачное хранилище компании Microsoft. Является частью спектра онлайновых услуг Windows Live.

MS-RPCH
Microsoft RPC-over-HTTP (RPC через HTTP) позволяет клиентам RPC подключаться через интернет к программам сервера RPC и выполнять удаленные вызовы процедур.

MsSQL-TDS
Протокол прикладного уровня, используемый для передачи данных между сервером базы данных и клиентом.

Mullvad
Сервис по поставке услуг виртуальной частной сети (VPN) с открытым исходным кодом, работает с использованием протоколов WireGuard и OpenVPN.

Mumble
Свободное кроссплатформенное VoIP-приложение с открытым кодом, включающее особую технологию «позиционирования звука», как основную отличительную особенность.

Munin
Бесплатное программное приложение для мониторинга компьютерных систем, сети и инфраструктуры с открытым исходным кодом.

MySQL
Протокол, используемый для взаимодействия клиентов и серверов MySQL.

Nano
Консольный текстовый редактор для UNIX и Unix-подобных операционных систем.

NAT-PMP
Сетевой протокол для автоматической установки параметров преобразования сетевых адресов и конфигураций переадресации портов без участия пользователя.

Nats
Система обмена сообщениями с открытым исходным кодом.

NestLogSink
Система логирования для домашней системы пожарной безопасности от Google.

NetBIOS
Протокол, используемый для обнаружения компьютеров в сети.

NetEaseGames
Трафик различных игр NetEase.

Netflix
Стриминговый сервис фильмов и сериалов.

NetFlow
Протокол, предназначенный для учета сетевого трафика, разработанный компанией Cisco Systems.

NFS
Протокол сетевого доступа к файловым системам.

Nintendo
Японская компания, специализирующаяся на создании видеоигр и игровых систем.

NOE
New Office Environment - протокол VoIP, используемый совместимыми телефонными системами Alcatel-Lucent.

NoMachine
Проект итальянской компании Medialogic S.p.A. для дистанционной работы.

Ntop
Программное обеспечение, которое исследует компьютерную сеть.

NTP
Протокол для синхронизации внутренних часов компьютера.

Nvidia
Американская технологическая компания, разработчик графических процессоров и систем на чипе (SoC).

OCS
Спецификация программных интерфейсов класса REST для интеграции социальных интернет-коммуникаций в среды рабочего стола.

OCSP
Протокол, используемый для получения статуса отзыва цифрового сертификата X.509.

OICQ
Распространенный в Китае сервис мгновенного обмена сообщениями.

Ookla
Американская компания, которая владеет сервисом по измерению скорости интернета Speedtest.

OPC-UA
Программный интерфейс для промышленного протокола связи и модели данных. Используется для связи между конечными устройствами различных производителей по принципу клиент/сервер.

OpenDNS
Протокол, предоставляющий общедоступные DNS-серверы.

OpenFlow
Протокол управления процессом обработки данных, передающихся по сети маршрутизаторами и коммутаторами.

OpenVPN
Протокол VPN с открытым исходным кодом.

OpenWire
Библиотека программирования потоков данных с открытым исходным кодом.

OperaVPN
VPN-клиент, встроенный в браузер Opera.

Oracle
Американская компания, специализируется на выпуске систем управления базами данных, связующего программного обеспечения, бизнес-приложений.

OSPF
Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала.

Outlook
Персональный информационный менеджер с функциями почтового клиента, входящий в пакет офисных программ Microsoft Office.

Pandora
Тип цифровой криптовалюты.

Pastebin
Веб-приложение, которое позволяет загружать отрывки текста, обычно фрагменты исходного кода, для возможности просмотра окружающими.

PathofExile
Бесплатная онлайн-ролевая игра в жанре экшен.

PFCP
Протокол, используемый для связи между функциями управления (CP) и пользователя (UP) в сетях 4G и 5G.

PGM
Протокол надежной многоадресной передачи данных.

Pinterest
Социальный интернет-сервис, фотохостинг, позволяющий пользователям добавлять в режиме онлайн-изображения.

Playstation
Игровая приставка пятого поколения, разработанная компанией Sony Computer Entertainment.

PlayStore
Онлайн-магазин приложений для Android.

Pluralsight
Платформа для онлайн-обучения.

POP3
Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP.

POPS
Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP, включающий в себя обязательное шифрование.

PostgreSQL
Протокол, используемый для взаимодействия клиентов и серверов PostgreSQL.

PPTP
Туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищенное соединение с сервером за счет создания специального туннеля в стандартной, незащищенной сети.

PrivateInternetAccess
Персональная служба VPN.

PROFINET_IO
Протокол для связи реального времени (RT) и изохронного реального времени (IRT) с децентрализованной периферией.

Protobuf
Протокол сериализации (передачи) структурированных данных, предложенный Google как эффективная бинарная альтернатива текстовому формату XML.

ProtonVPN
Сервис по поставке услуг виртуальной частной сети (VPN), управляемый швейцарской компанией Proton AG.

Psiphon
Бесплатный инструмент для обхода цензуры в интернете с открытым исходным кодом, в котором используется сочетание технологий защищенной связи и обфускации.

PTPv2
Протокол синхронизации для промышленных сетей.

QQ
Протокол мгновенного обмена сообщениями.

QUIC
Экспериментальный интернет-протокол, позволяющий мультиплексировать несколько потоков данных между двумя компьютерами. Протокол работает поверх протокола UDP и содержит возможности шифрования, эквивалентные TLS и SSL.

RADIUS
Протокол удаленной аутентификации пользователей, представляет собой ключевой элемент в обеспечении безопасности и управлении доступом в сетях.

Radmin
Условно бесплатная программа удаленного администрирования ПК для платформы Windows, которая позволяет полноценно работать на нескольких удаленных компьютерах с помощью графического интерфейса.

Raft
Компьютерная игра в жанре симулятор выживания в открытом мире, разработанная шведской компанией Redbeet Interactive и изданная Axolot Games.

RakNet
Кроссплатформенный сетевой сервис, разработанный Oculus VR для использования в игровой индустрии.

RDP
Протокол удаленного рабочего стола.

Reddit
Сайт, сочетающий черты социальной сети и форума, где зарегистрированные пользователи могут размещать ссылки на понравившуюся информацию в интернете и обсуждать ее.

RESP
Двоичный протокол, в котором используются управляющие последовательности, закодированные в стандартном ASCII.

RiotGames
Американская компания, разработчик видеоигр, издатель и организатор киберспортивных турниров (League of Legends).

RipeAtlas
Протокол зонда RIPE Atlas используется для крупнейшей в мире активной сети измерения Интернета.

RMCP
Протокол многоадресной передачи с ретрансляцией для предоставления услуг сквозной многоадресной передачи данных по сетям на базе IP-протокола.

Roblox
Игровая онлайн-платформа и система создания игр, позволяющая любому пользователю создавать свои собственные и играть в созданные другими игры.

Roughtime
Протокол с криптографической защитой на базе UDP, который используется для синхронизации времени серверов.

RSH
Протокол, позволяющий подключаться удаленно к устройству и выполнять на нем команды.

RSYNC
Утилита для удаленной синхронизации и копирования файлов.

RTCP
Протокол управления передачей в реальном времени.

RTMP
Проприетарный протокол потоковой передачи данных, в основном используемый для передачи потокового видео и аудиопотоков с веб-камер через интернет.

RTP
Протокол, используемый при передаче трафика реального времени.

RTPS
Real Time Streaming Protocol - потоковый протокол реального времени - позволяет управлять вещанием: выполнять несколько команд, такие как «старт», «стоп», «переход на определенное время».

RTSP
Протокол реального времени, предназначенный для использования в системах, работающих с мультимедийными данными. Позволяет удаленно управлять потоком данных с сервера.

RX
Клиент-серверный RPC-протокол, расширенная и объединенная версия старых протоколов R и RFTP.

S7Comm
Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400.

S7CommPlus
Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400. Сложнее протокола S7Comm и использует двухбайтовое поле под названием ID сессии для защиты от атак воспроизведения.

Salesforce
Американская компания, разработчик одноименной CRM-системы, предоставляемой по модели SaaS.

SAP
Протокол позволяет сетевым устройствам постоянно корректировать данные о том, какие сервисные услуги имеются сейчас в сети.

SCTP
Протокол управления потоком передачи с установлением соединения, как TCP, но передающий данные сообщениями, как UDP.

SD-RTN
Software Defined Real-time Network - собственный протокол компании Agora, предназначен для потоковой передачи данных с низкой задержкой.

Service_Location_Protocol
Протокол обнаружения сервисов, который позволяет компьютерам и иным устройствам находить сервисы в локальной сети без предварительной конфигурации.

sFlow
Протокол, используемый для сбора, отправки и анализа информации о сетевом трафике в целях мониторинга.

Showtime
Американский кабельный телевизионный канал.

Signal
Криптографический протокол, созданный для обеспечения сквозного шифрования голосовых вызовов, видеозвонков и мгновенных сообщений.

SignalVoip
Протокол голосовой связи в мессенджере Signal.

Sina
Китайская интернет-компания, владеет аналогом Twitter - сервисом Sina Weibo.

SinaWeibo
Китайский сервис микроблогов, запущенный компанией Sina Corp.

SIP
Протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения, онлайн-игры).

SiriusXMRadio
Американская радиовещательная компания в сфере спутникового радио и онлайн-радио.

Skype_Teams
Сервис Microsoft, предназначенный для командной работы и обмена информацией между участниками проекта или команды.

Skype_TeamsCall
Бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее видеосвязь через интернет. Опционально использует технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны.

Slack
Корпоративный мессенджер.

SMBv1
Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети.

SMBv23
Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети.

SMPP
Протокол одноранговой передачи коротких сообщений.

SMTP
Протокол, предназначенный для передачи электронной почты.

SMTPS
Протокол для передачи электронной почты, включающий в себя обязательное шифрование.

Snapchat
Мобильное приложение обмена сообщениями с прикрепленными фото и видео.

SnapchatCall
Протокол голосовой передачи, основанный на VoIP, в мессенджере Snapchat.

SNMP
Протокол для управления устройствами в IP-сетях.

SOAP
Протокол обмена структурированными сообщениями в распределенной вычислительной среде.

SOCKS
Протокол сеансового уровня модели OSI, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно для них) и таким образом использовать сервисы за межсетевыми экранами (файрволами).

Softether
Бесплатное кроссплатформенное многопротокольное программное обеспечение VPN-клиента и VPN-сервера с открытым исходным кодом.

SOMEIP
Автомобильное программное обеспечение, которое может использоваться для передачи управляющих сообщений.

SoundCloud
Онлайн-платформа для распространения оцифрованной звуковой информации (например, музыкальных произведений).

Source_Engine
Игровой сервис, разработанный Valve Corporation для собственного использования и лицензирования другими разработчиками.

Spotify
Стриминговый сервис, позволяющий легально прослушивать музыкальные композиции, аудиокниги и подкасты, не скачивая их на устройство.

SRTP
Определяет профиль протокола RTP и предназначен для шифрования, установления подлинности сообщения, целостности, защиты от подмены данных RTP в однонаправленных и multicast-передачах медиа и приложениях.

SSDP
Протокол, служащий для объявления и обнаружения сетевых сервисов.

SSH
Протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.

StarCraft
Серия компьютерных игр в жанре стратегии в реальном времени, разработанная компанией Blizzard Entertainment.

Steam
Онлайн-сервис цифрового распространения компьютерных игр и программ.

SteamDatagramRelay
Закрытая виртуальная игровая сеть Valve. Используя функции API, позволяет перенести игровой трафик на сетевые магистрали Valve.

STOMP
Simple Text Oriented Messaging Protocol, протокол обмена сообщениями.

STUN
Протокол, который позволяет клиенту, находящемуся за сервером трансляции адресов (или за несколькими такими серверами), определить свой внешний IP-адрес, способ трансляции адреса и порта во внешней сети, связанный с определенным внутренним номером порта.

Syncthing
Приложение, позволяющее синхронизировать файлы между несколькими устройствами.

Syslog
Протокол отправки и регистрации сообщений о происходящих в системе событиях.

Tailscale
VPN-сервис, который работает поверх WireGuard и позволяет получить доступ к контроллеру даже, если у вас нет своего VPN-сервера.

TargusDataspeed
Проприетарный протокол, используемый для тестирования пропускной способности. Был разработан компанией TARGUSinfo.

Teams
Корпоративная платформа, объединяющая в рабочем пространстве чат, встречи, заметки и вложения.

TeamSpeak
Компьютерная программа, предназначенная для голосового общения в сети посредством технологии VoIP.

TeamViewer
Программное обеспечение для удаленного доступа, удаленного управления и удаленного обслуживания компьютеров и других конечных устройств.

Telegram
Кроссплатформенная система мгновенного обмена сообщениями с функциями обмена текстовыми, голосовыми и видеосообщениями, а также стикерами, фотографиями и файлами многих форматов.

TelegramVoip
Голосовые и видеозвонки в мессенджере Telegram.

Telnet
Протокол для реализации текстового терминального интерфейса по сети.

Tencent
Китайский конгломерат, создавший китайский клон ICQ, собственную валюту, отдельную соцсеть, множество игр, торговую площадку и WeChat.

TencentGames
Подразделение Tencent Interactive Entertainment, выпускающее видеоигры, разработчик PUPG MOBILE.

TencentVideo
Китайская стриминговая платформа, принадлежащая Tencent.

Teredo
Сетевой протокол, предназначенный для передачи IPv6-пакетов через сети IPv4, в частности, через устройства, работающие по технологии NAT, путем их инкапсуляции в UDP-дейтаграммы.

TES_Online
The Elder Scrolls Online — это MMORPG, действие которой разворачивается в фэнтезийном мире Тамриэля.

TeslaServices
Портал с сервисной и диагностической информацией для компаний и частных лиц, занимающихся профессиональным обслуживанием и ремонтом автомобилей Tesla.

TFTP
Простой протокол передачи файлов, как правило, используется при загрузке бездисковых систем.

Threads
Онлайн-сервис социальных сетей и социальных сетей, управляемый Meta Platforms.

Threema
Кроссплатформенное зашифрованное приложение для обмена мгновенными сообщениями.

Thrift
Программный фреймворк Apache Thrift, предназначенный для масштабируемой разработки межъязыковых сервисов.

Tidal
Интернет-сервис подписки на музыку, подкасты и потоковое видео, сочетающий в себе звук без потерь и музыкальные видеоролики высокой четкости с эксклюзивным контентом и специальными функциями для музыки.

TikTok
Сервис для создания и просмотра коротких видео, принадлежащий пекинской компании ByteDance.

TINC
Открытый, самомаршрутизирующийся сетевой протокол и программная реализация, используемая для сжатых и зашифрованных виртуальных частных сетей.

TiVoConnect
Протокол TivoConnect обеспечивает автоматическое обнаружение оборудования для двух или более систем медиаплееров Tivo, работающих в одной сети.

TLS
Протокол защиты транспортного уровня.

TocaBoca
Интерактивная мобильная игра.

Tor
Протокол анонимной сети виртуальных туннелей, предоставляющий передачу данных в зашифрованном виде.

TPLINK_SHP
Протокол TP-Link Smart Home Protocol используется для подключения устройств «Умного дома» с помощью приложения-компаньона.

TruPhone
Глобальная мобильная сеть, которая занимается разработкой технологии eSim, позволяющей подключаться к разным провайдерам без замены сим-карты.

Tumblr
Протокол микроблогов, включающий в себя множество картинок, статей, видео и gif-изображений по разным тематикам и позволяющий пользователям публиковать посты в их тамблелог.

TuneIn
Американский аудиопотоковый сервис, транслирующий новости, эфиры радиостанций, спортивные мероприятия, музыку и подкасты.

TunnelBear
Кроссплатформенный VPN-клиент.

TuyaLP
Протокол Tuya LAN используется для взаимодействия многих IoT-устройств, включая светодиодные лампы, лампочки, умные розетки и другое.

Twitch
Видеостриминговый сервис, специализирующийся на тематике компьютерных игр, в том числе на трансляциях геймплея и киберспортивных турниров.

Twitter
Американский сервис микроблогов и социальная сеть, в которой пользователи публикуют сообщения и взаимодействуют с ними.

UBNTAC2
Утилита управления оборудованием Ubiquiti airControl, версия 2.

UbuntuONE
Онлайн-хранилище для обмена файлами и синхронизации между компьютерами и мобильными устройствами.

UFTP
Протокол передачи файлов на основе UDP.

UltraSurf
Бесплатная утилита для обхода цензурных ограничений в интернете.

UMAS
Unified Messaging Application Services - проприетарный протокол Schneider Electric, который используется для конфигурации, мониторинга сбора данных и управления промышленными контроллерами Schneider Electric.

Unknown
Не распознанные модулем протоколы и приложения.

Usenet
Протокол, используемый для общения и публикации файлов.

VHUA
Протокол, который использовался для Skype-подобных сервисов в Китае.

Viber
Приложение-мессенджер, которое позволяет отправлять сообщения, совершать видео- и голосовые VoIP-звонки через интернет.

ViberVoip
Аудио/видеозвонки, совершаемые с помощью приложения Viber.

Vimeo
Американский сервис для публикации и просмотра видео.

VK
Приложение для взаимодействия с социальной сетью ВКонтакте.

VMware
Американская компания-разработчик программного обеспечения для виртуализации.

VNC
Протокол удаленного доступа к рабочему столу.

VRRP
Протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию.

Vudu
Потоковый сервис цифрового видео.

VXLAN
Протокол инкапсуляции, который обеспечивает подключение центров обработки данных с использованием туннелирования для расширения соединений канального уровня в используемой сети сетевого уровня.

Warcraft3
Компьютерная игра в жанре стратегии в реальном времени с элементами RPG.

Waze
Бесплатное социальное навигационное приложение для мобильных устройств, позволяющее отслеживать ситуацию на дорогах в режиме реального времени, прокладывать оптимальные маршруты, узнавать о расположении радаров скорости.

WebDAV
Набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах.

Webex
Американская компания, которая разрабатывает и продает приложения для веб-конференций, видеоконференцсвязи и контакт-центра как сервиса.

WebSocket
Протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером, используя постоянное соединение.

WeChat
Мобильная коммуникационная система для передачи текстовых и голосовых сообщений, разработана китайской компанией Tencent.

WhatsApp
Американский бесплатный сервис обмена мгновенными сообщениями и голосовой связи по IP, принадлежащий компании Meta.

WhatsAppCall
Протокол голосовой передачи, основанный на VoIP.

WhatsAppFiles
Протокол загрузки медиафайлов (изображений, видео, музыки, документов) мессенджера WhatsApp.

Whois-DAS
Сетевой протокол прикладного уровня, базирующийся на протоколе TCP, применяется для получения регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем.

Wikipedia
Самая крупная в мире онлайн-энциклопедия.

WindowsUpdate
Сервис обновления операционной системы Windows.

WireGuard
Высокоскоростной и безопасный VPN-протокол.

WorldOfKungFu
3D MMORPG с боевыми искусствами, основанная на традиционной китайской культуре.

WorldOfWarcraft
Массовая многопользовательская ролевая онлайн-игра.

WSD
Протокол многоадресного обнаружения для поиска сервисов в локальной сети. Работает через TCP- и UDP-порт 3702 и использует IP-адрес многоадресной рассылки 239.255.255.250 или ff02::c.

Xbox
Домашняя игровая консоль, разработанная и выпущенная американской корпорацией Microsoft.

XDMCP
Протокол аутентификации между X-сервером и X-клиентом.

Xiaomi
Китайская корпорация-производитель смартфонов, компьютерной и бытовой техники.

Yahoo
Американская компания, специализирующаяся на проектах и услугах в интернете. Владеет поисковой системой с одноименным названием.

Yandex
Российская транснациональная компания в отрасли информационных технологий, владеющая одноименной системой поиска в интернете, интернет-порталом и веб-службами.

YandexCloud
Публичная облачная платформа, разработанная российской интернет-компанией Яндекс.

YandexDirect
Сервис для размещения объявлений контекстной рекламы на Яндексе и на сайтах-партнерах его рекламной сети.

YandexDisk
Сервис для хранения данных в облаке.

YandexMail
Почтовый сервис от компании Яндекс.

YandexMarket
Сервис заказа товаров онлайн.

YandexMetrika
Бесплатный сервис веб-аналитики, предлагаемый Яндексом, который отслеживает и сообщает о трафике веб-сайта.

YandexMusic
Стриминговый сервис компании Яндекс, позволяющий слушать музыкальные композиции, их подборки, альбомы.

Yojimbo
Менеджер личной информации для MacOS от Bare Bones Software. Позволяет хранить заметки, изображения и медиафайлы, URL-адреса, веб-страницы и пароли.

YouTube
Видеохостинг, предоставляющий пользователям услуги хранения, доставки и показа видео.

YouTubeUpload
Загрузка файлов на видеохостинг YouTube.

Z3950
Клиент-серверный протокол для поиска и получения информации с удаленных компьютерных баз данных.

Zabbix
Свободная система мониторинга статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

Zattoo
Телевизионная платформа, которая предлагает прямые телетрансляции и контент по запросу для компьютеров, мобильных телефонов, планшетов и других сетевых устройств.

ZeroMQ
Высокопроизводительная асинхронная библиотека обмена сообщениями, ориентированная на использование в распределенных и параллельных вычислениях.

Zoom
Проприетарная программа для организации видеоконференций, разработанная компанией Zoom Video Communications.

ZUG
Протокол ZUG является частью консенсусной модели Casper 2.0.

17.3.3 Особенности создания профилей

Принцип создания профилей **Контроля приложений** в 18 версии Ideco NGFW аналогичен принципу создания правил **Контроля приложений** в более ранних версиях: все протоколы и приложения, которые не были запрещены, остаются разрешены.

Подсказка: С 18 версии NGFW правила Файрвола, которые блокировали трафик за счет перехвата DNS в предыдущих версиях, не смогут его блокировать. Чтобы это исправить, создайте и включите правила с профилями IPS и DPI в разделе **Правила трафика -> Файрвол -> INPUT**.

Для удобства настройки модуля фильтрации рекомендуем объединить пользователей в несколько групп/подгрупп (например, в соответствии с организационной структурой компании) и настроить профиль **Контроля приложений** отдельно для каждой группы.

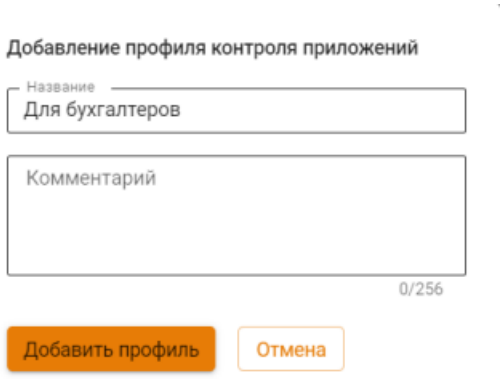
Создание профилей и добавление в правила Файрвола

Пример. Необходимо ограничить доступ к социальным сетям пользователям группы «Бухгалтерия».

Создание профиля Контроля приложений

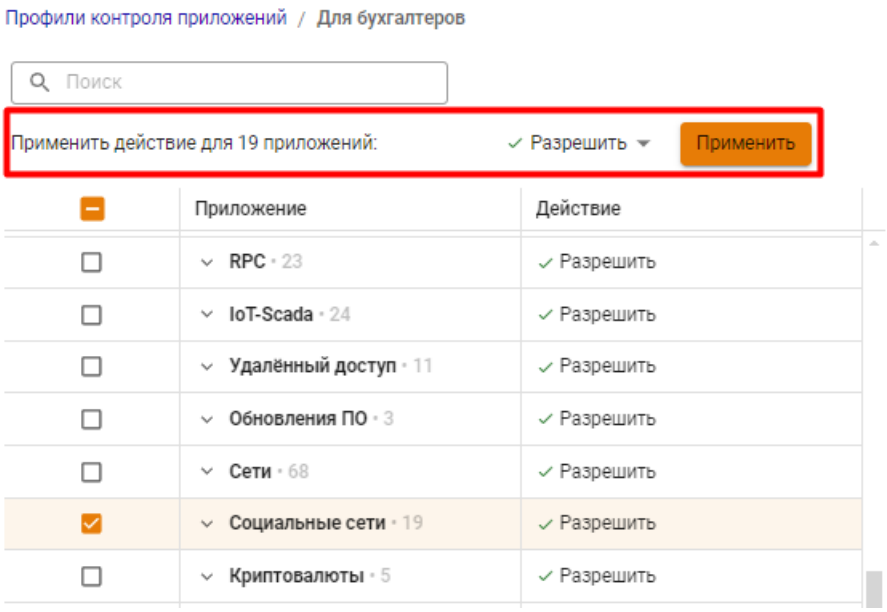
1. Перейдите в раздел **Профили безопасности -> Контроль приложений** и нажмите **Добавить**.

2. Заполните **Название**, **Комментарий** (необязательно) и добавьте профиль:

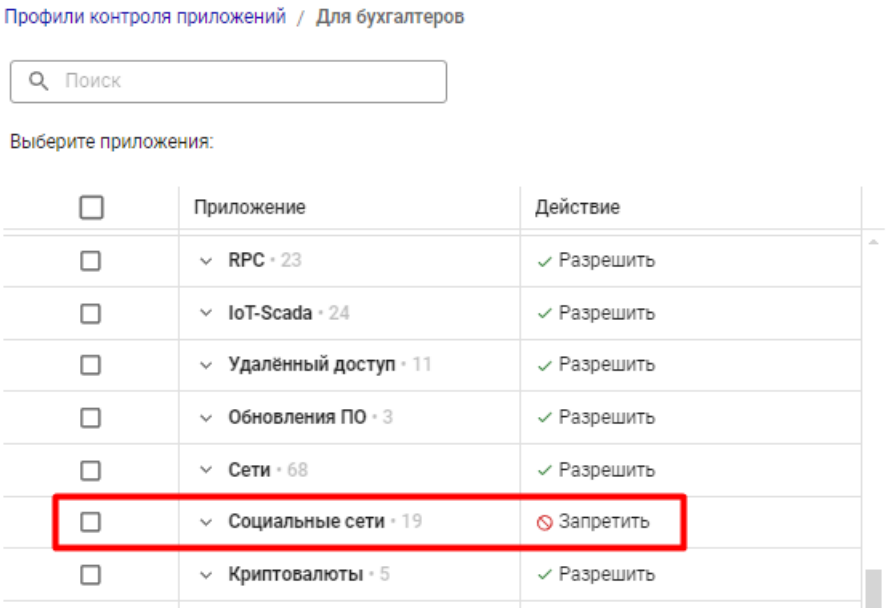


3. Нажмите в столбце **Управление** на , затем **Доступ к приложениям**.

4. Выберите **Социальные сети** (при необходимости используйте поиск). Появится строка с выбором действия:



5. Примените действие **Запретить** рядом со строкой поиска и нажмите **Применить**. Действие применится к выбранным приложениям:



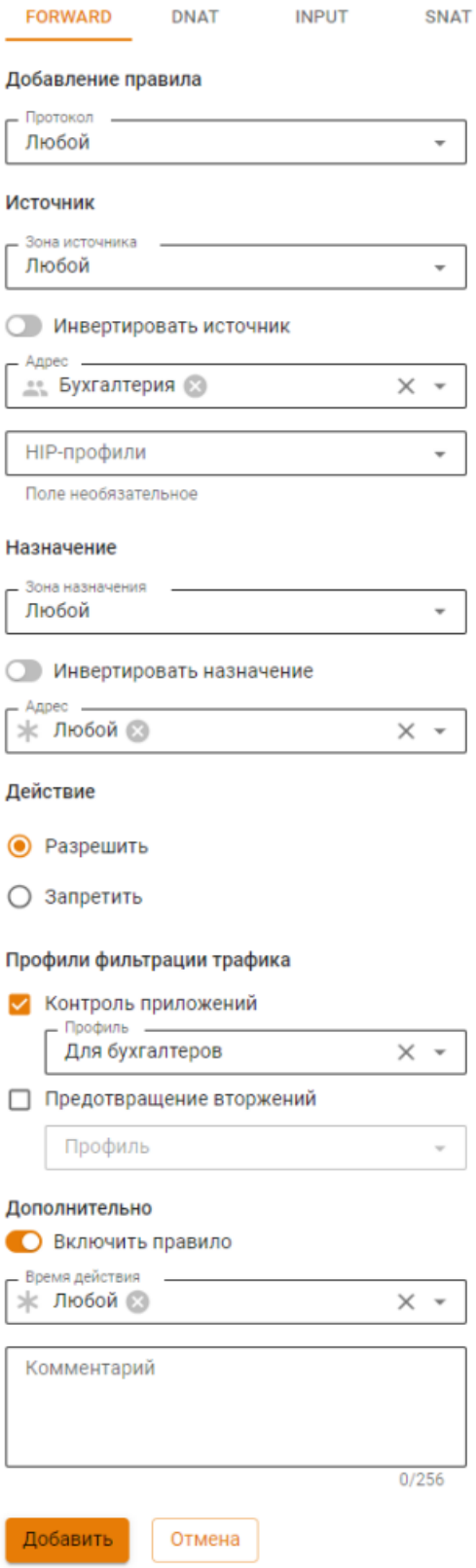
Подсказка: К неизвестным источникам по умолчанию применяется действие **Разрешить** (доступно для редактирования).

6. Нажмите **Сохранить**.

Добавление профиля в правила Файрвола

1. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать с помо-

щью профиля **Контроля приложений**;

- **Источник** - выберите **Адрес**, **Зону** и **HIP-профиль** источника трафика;
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика;
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** и в разделе **Профили для фильтрации** из раскрывающегося списка выберите профиль, запрещающий социальные сети сотрудникам бухгалтерии.

4. Включите правило или оставьте его выключенным.

5. Нажмите **Добавить**.

6. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичное правило INPUT.

Иерархическая структура Профилей контроля приложений

Один из вариантов корректного применения политик безопасности к вложенной структуре пользователей - построение иерархической структуры профилей **Контроля приложений**:

- Профили для самой большой группы пользователей запрещают наибольшее количество протоколов и приложений;
- Профили для более мелких групп пользователей повторяют запрет для самой большой группы пользователей, но точечно разрешают определенные приложения и протоколы для конкретных подгрупп;
- Профили для конкретных пользователей разрешают определенные протоколы и приложения, необходимые этим конкретным пользователям. В этих профилях также остаются запреты, которые должны сохраниться для этих пользователей.

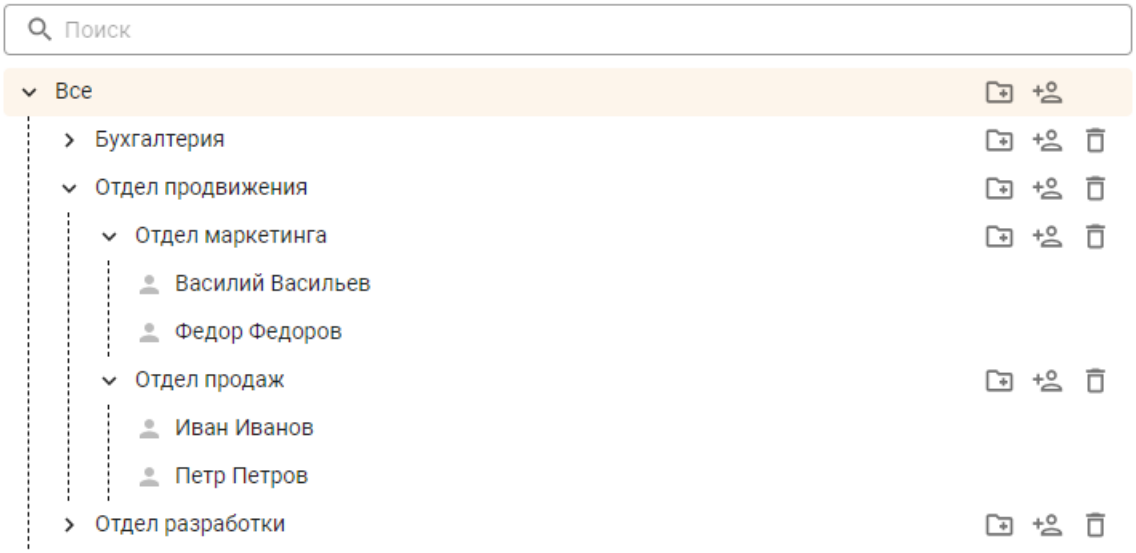
Чтобы настроить фильтрацию трафика, для которого в таблице FORWARD нет правил, воспользуйтесь инструкцией:

17.3.4 Пример создания иерархической структуры

Пример. Необходимо настроить профили **Контроля приложений** в соответствии с требованиями:

- Всем пользователям запрещены компьютерные игры, контент для взрослых, майнинг и криптовалюты;
- Доступ к социальным сетям разрешен только Отделу продвижения;
- Доступ к стриминговым сервисам разрешен только Отделу маркетинга;
- Доступ к музыкальным приложениям разрешен только Федору Федорову из Отдела маркетинга.

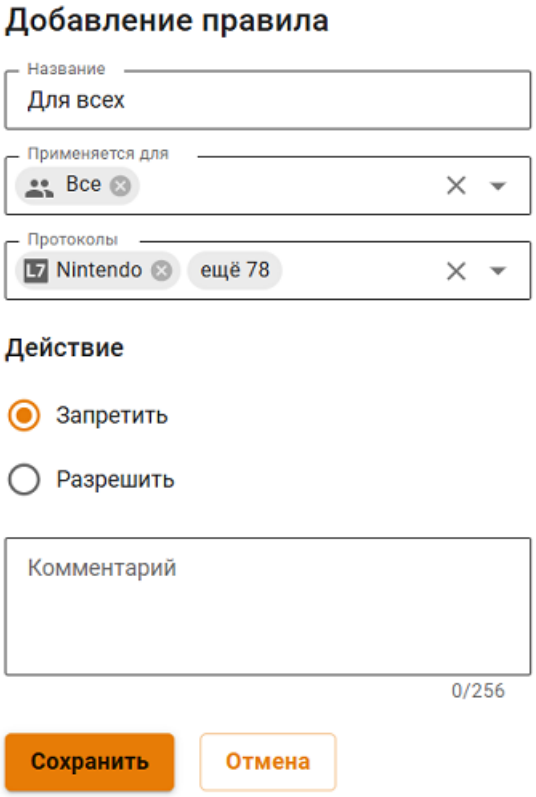
В описанном примере Федор Федоров - сотрудник Отдела маркетинга, а Отдел маркетинга - структурное подразделение Отдела продвижения:



Настройка в версии 17 (правила)

1. Создайте правило, запрещающее всем сотрудникам социальные сети, стриминговые сервисы, музыкальные приложения, компьютерные игры, контент для взрослых, майнинг и криптовалюты. Для этого:

- Перейдите в раздел **Правила трафика -> Контроль приложений** и нажмите **Добавить**;
- Настройте правило с действием **Запретить** для всех пользователей, выбрав протоколы и приложения, соответствующие условиям примера:

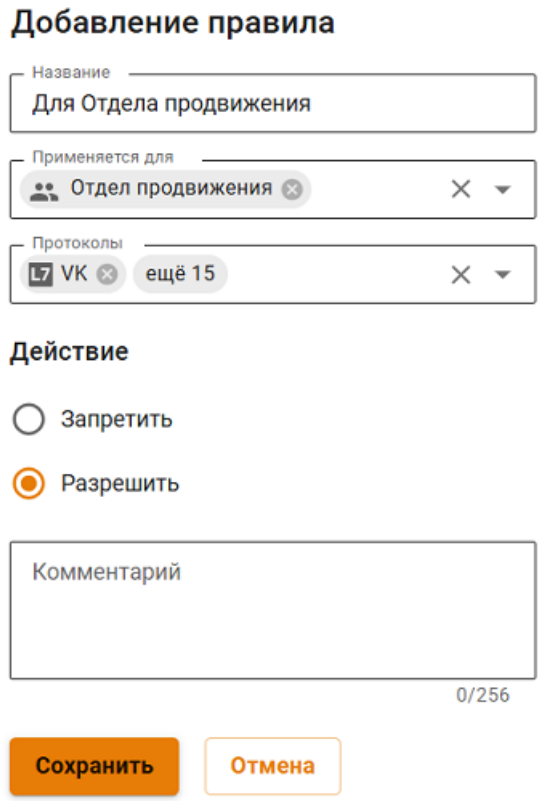


2. Аналогично создайте ряд правил, соответствующих условиям примера:

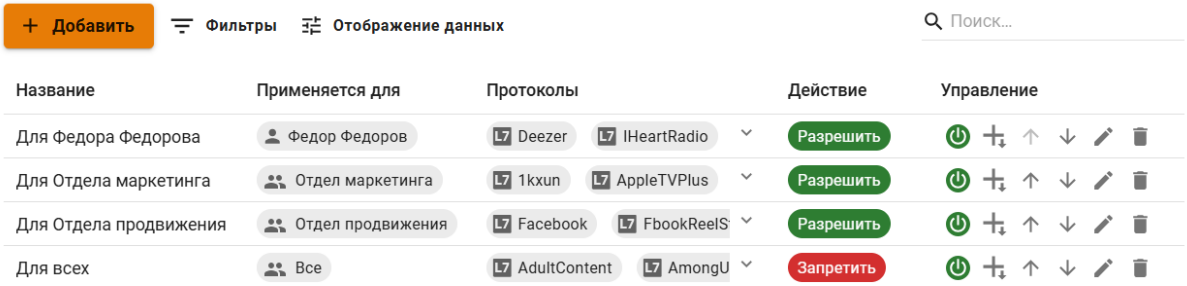
- Сотрудникам Отдела продвижения разрешен доступ к социальным сетям;

- Сотрудникам Отдела маркетинга разрешен доступ к стриминговым сервисам;
- Федору Федорову из Отдела маркетинга разрешен доступ к музыкальным приложениям.

Пример:



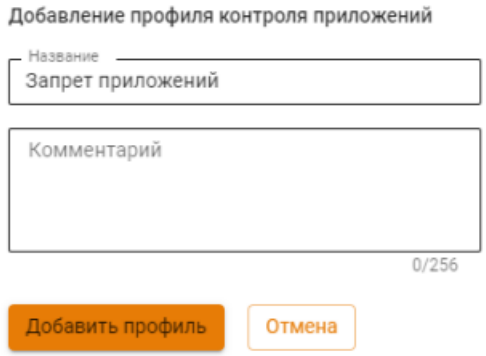
3. Поместите созданные в пункте 2 правила с действием **Разрешить** выше правила, созданного в пункте 1:



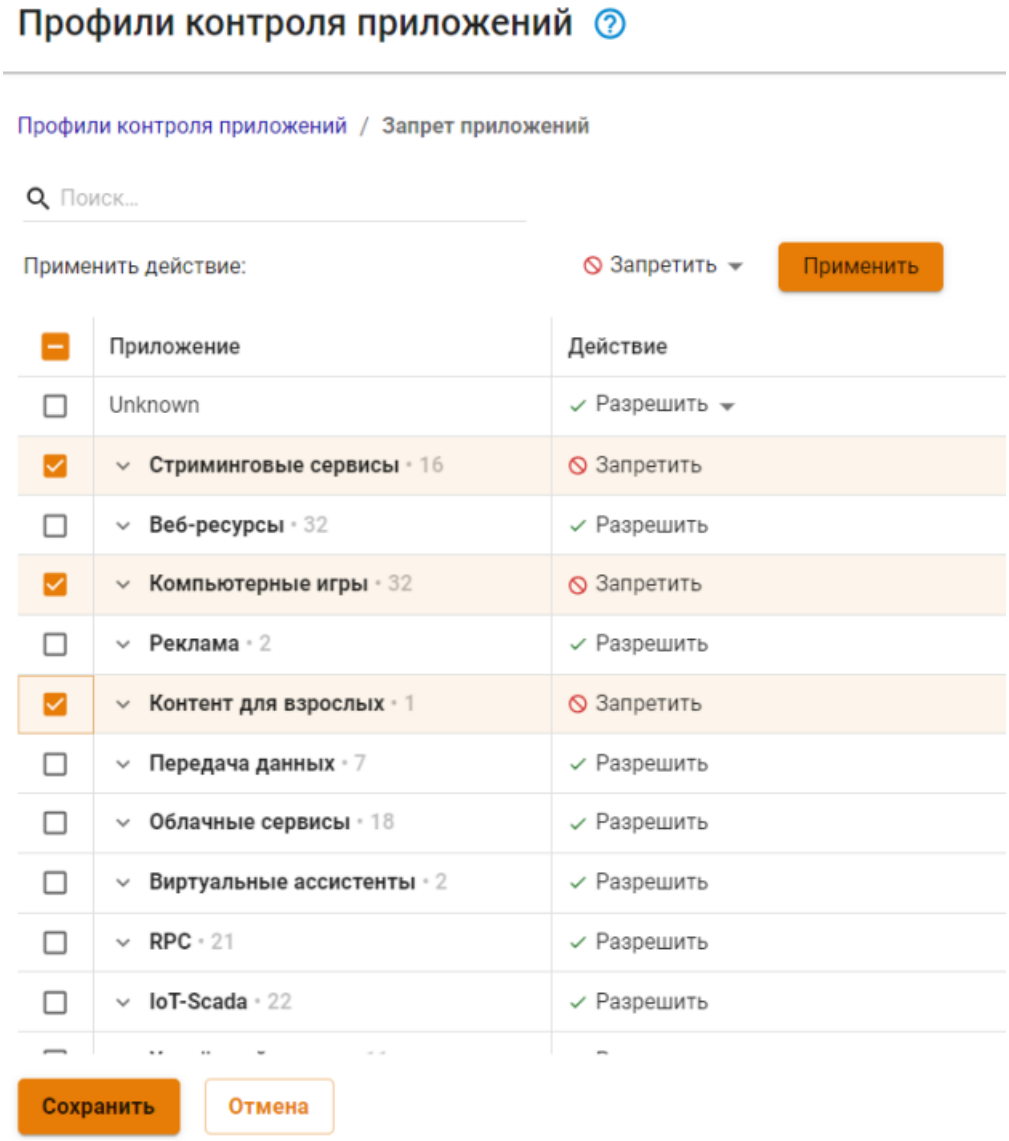
Настройка в версии 18 (профили)

Создайте профили в соответствии с условиями примера:

1. Перейдите в раздел **Профили безопасности -> Контроль приложений**, чтобы создать профиль, запрещающий доступ к социальным сетям, стриминговым сервисам, музыкальным приложениям, компьютерным играм, контенту для взрослых, майнингу и криптовалютам. Нажмите **Добавить** и введите название профиля:



2. Настройте добавленный профиль:



- Нажмите в столбце **Управление** на , а затем **Доступ к приложениям**;
- Выберите группы приложений, которые необходимо запретить (перечислены в описании примера);
- Установите настройку **Запретить** и нажмите **Применить** в правом верхнем углу;
- После применения действия нажмите **Сохранить** в левом нижнем углу.

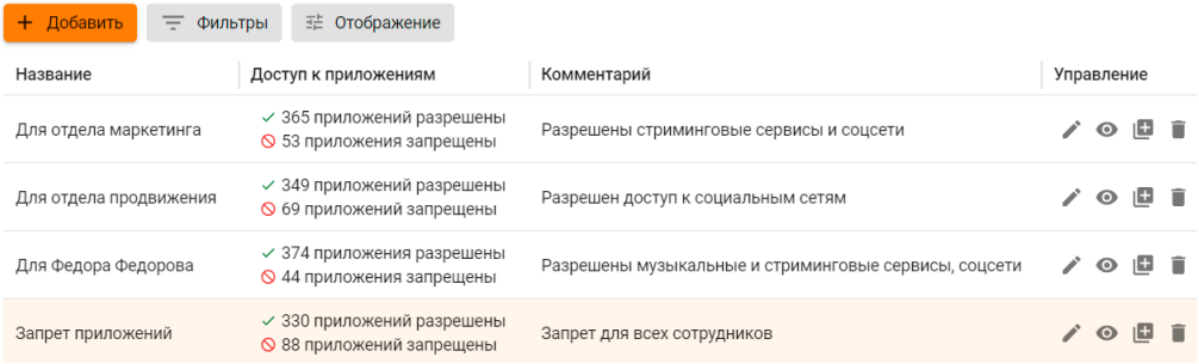
3. Создайте профиль для Отдела продвижения, разрешающий доступ к социальным сетям. Для этого:

- Клонируйте созданный профиль, нажав на  в столбце **Управление**;
- Отредактируйте клонированный профиль: поменяйте название (например, на **Для Отдела продвижения**) и настройки доступа к приложениям (разрешите доступ к социальным сетям).

4. Аналогично создайте профиль для Отдела маркетинга, разрешающий доступ к стриминговым сервисам. Для этого клонируйте профиль **Для Отдела продвижения**, введите название (например, **Для Отдела маркетинга**) и разрешите в нем доступ к стриминговым сервисам.

5. Создайте профиль для Федора Федорова, разрешающий доступ к музыкальным сервисам. Для этого клонируйте профиль **Для Отдела маркетинга** и установите необходимые настройки.

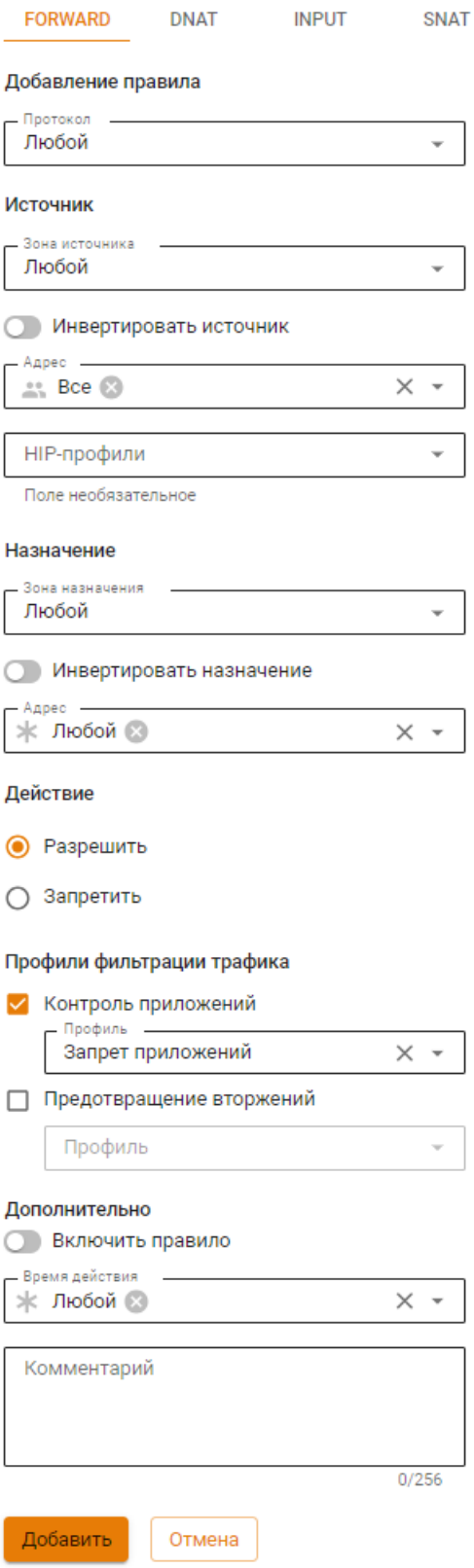
В итоге должен получиться набор профилей, учитывающий настройки, описанные в примере:



Теперь необходимо создать и включить правила в **Файрволе**, чтобы применить настройки для конкретных групп пользователей и установить приоритет прохождения трафика:

1. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD** и нажмите **Добавить**.

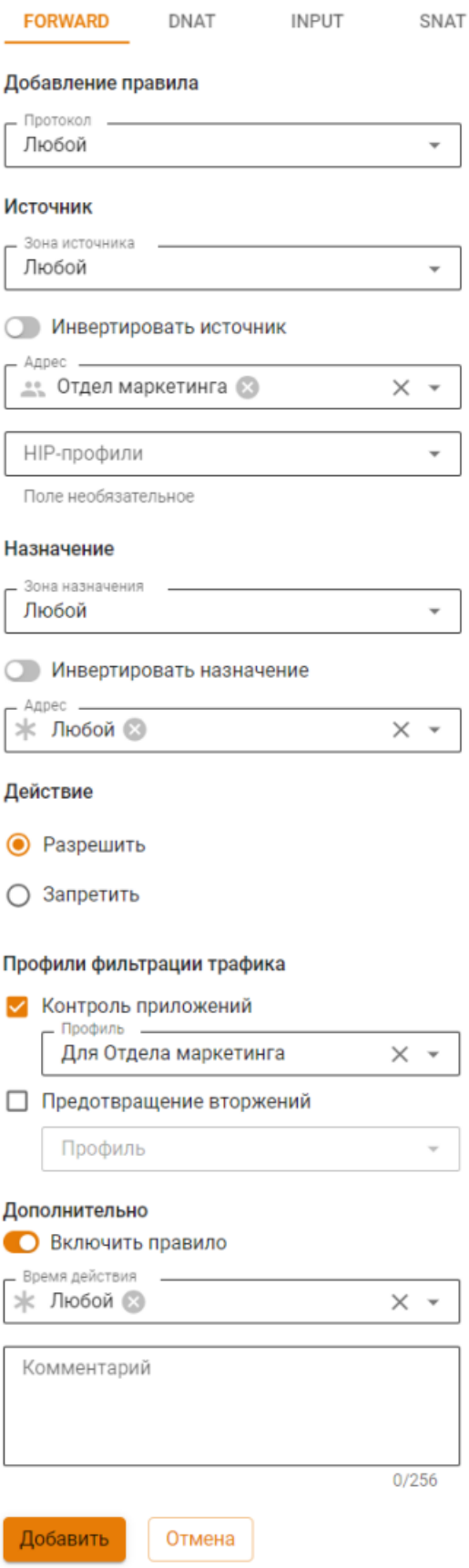
2. Заполните поля:



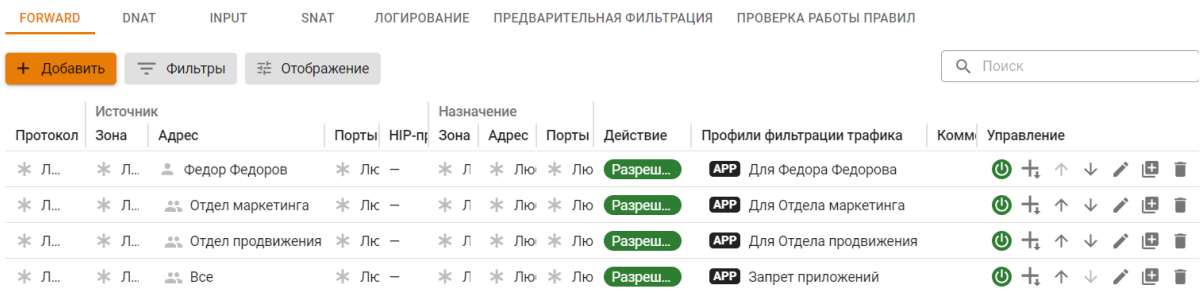
- В поле **Адрес** раздела **Источник** выберите группу **Все**;
- Выберите действие **Разрешить**;
- В профилях фильтрации трафика включите опцию **Контроль приложений** и выберите профиль **Запрет приложений**;
- Включите правило.

3. Нажмите **Добавить**.

4. Аналогично создайте правила для каждого профиля. При создании правила **Файрвола** укажите соответствующий профилю адрес источника. Например, при создании правила с профилем фильтрации **Для Отдела маркетинга** выберите в поле **Адрес** раздела **Источник** группу **Отдел маркетинга**:



5. Чтобы трафик проходил в соответствии с условиями примера, установите в **Файрволе** следующую последовательность правил:



Чем выше в таблице стоит правило, тем выше его приоритет.
Разрешающее правило для сотрудника не сработает, если выше в таблице **Файрвола** находится правило, запрещающее трафик для отдела, в котором работает этот сотрудник.

6. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичные правила INPUT.

17.3.5 Настройка фильтрации трафика, для которого в таблице FORWARD нет правил

Основное

Создайте профиль **Контроля приложений**, соответствующий нужным правилам:

1. Перейдите в раздел **Профили безопасности -> Контроль приложений** и нажмите **Добавить**.

2. Введите **Название** профиля, **Комментарий** и добавьте профиль.

3. Нажмите в столбце **Управление** на , затем **Доступ к приложениям**.

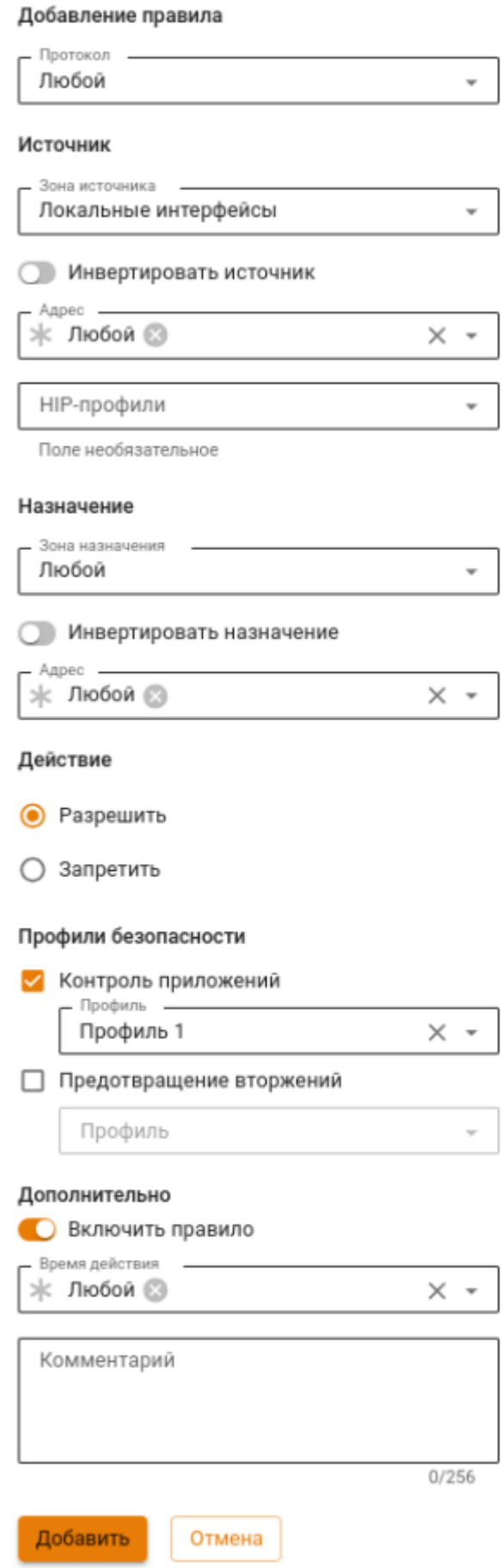
4. Выберите протоколы или группы протоколов и действия (**Запретить** или **Разрешить**), которые будут к ним применяться, затем нажмите **Применить**.

5. Нажмите **Сохранить** в левом нижнем углу.

Далее создайте правило **Файрвола** с созданным профилем **Контроля приложений**:

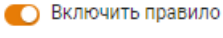
1. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD** и нажмите **Добавить**.

2. Заполните поля:


Добавление правила
Протокол
Любой
Источник
Зона источника
Локальные интерфейсы
Инвертировать источник
Адрес
Любой
HIP-профили
Поле необязательное
Назначение
Зона назначения
Любой
Инвертировать назначение
Адрес
Любой
Действие
Разрешить
Запретить
Профили безопасности
Контроль приложений
Профиль
Профиль 1
Предотвращение вторжений
Профиль
Дополнительно
Включить правило
Время действия
Любой
Комментарий
0/256
Добавить
Отмена

- **Протокол** - выберите **Любой**;
- **Источник**:
  - **Зона источника** - выберите **Локальные интерфейсы**;
  - При необходимости укажите **Адрес** и **HIP-профиль** источника трафика.
- **Назначение**:
  - **Зона назначения** - выберите **Любой**;
  - При необходимости укажите **Адрес** назначения трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** в профилях безопасности и из раскрывающегося списка выберите созданный ранее профиль.

4. Включите правило, нажав 

.

5. Нажмите **Добавить**.

6. Поместите правило в конец таблицы **Файрвола**. Если в таблице есть правило, запрещающее все, поместите правило с профилем **Контроля приложений** над ним.

7. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичное правило **INPUT**.

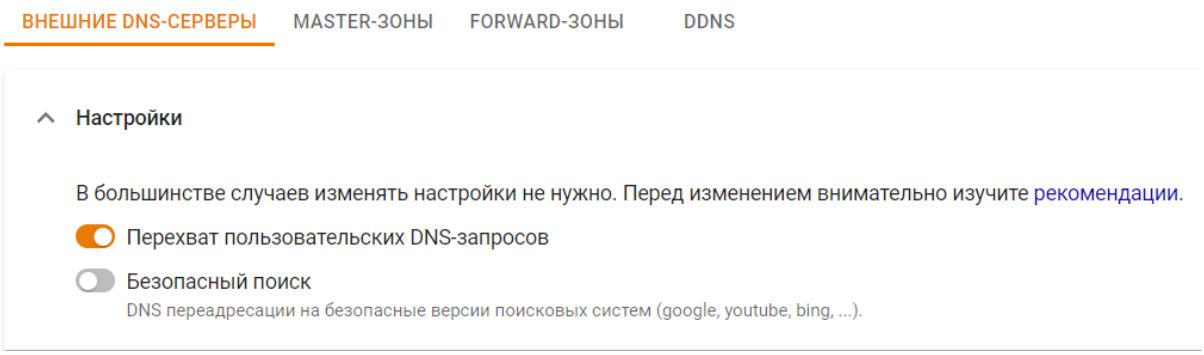
17.4 Предотвращение вторжений

Подсказка: Название службы раздела *Предотвращение вторжений*: `ideco-suricata-backend`; `ideco-suricata`; `ideco-suricata-event-syncer`; `ideco-suricata-profiles-syncer`.
Список имен служб для других разделов доступен по *ссылке*.

В разделе **Профили безопасности -> Предотвращение вторжений** создаются профили с правилами выбора сигнатур и действиями, которые NGFW будет применять к трафику, соответствующему этим сигнатурам.

В 18 версии Ideco NGFW созданные в разделе **Профили безопасности -> Предотвращение вторжений** профили применяются при создании правил в разделе **Правила трафика -> Файрвол**.

Чтобы трафик фильтровался системой **Предотвращения вторжений**, необходимо для всех локальных интерфейсов создать правило FORWARD, содержащее необходимый профиль безопасности. Если в разделе **Сервисы -> DNS -> Внешние DNS-серверы** включена опция **Перехват пользовательских DNS-запросов** (по умолчанию включена), нужно также создать аналогичное правило INPUT:



Внимание: Если профиль не добавлен в правила таблицы FORWARD или INPUT раздела **Правила трафика -> Файрвол**, трафик не будет фильтроваться системой **Предотвращения вторжений**.

Сигнатуры, не используемые в профилях, и профили, не используемые в правилах **Файрвола**, не участвуют в обработке трафика!

17.4.1 Особенности обработки трафика системой Предотвращения вторжений

В предыдущих версиях FORWARD- и INPUT-трафик сначала проходит модуль **Предотвращение вторжений**, а затем **Файрвол**. В 18 версии IPS обрабатывает только трафик, соответствующий разрешающему правилу **Файрвола** с включенной проверкой через **Предотвращение вторжений**.

Файрвол Ideco NGFW анализирует трафик для поиска подходящего правила и применяет его. Если в списке есть несколько правил с одними и теми же условиями, применяется правило, стоящее выше по списку. Запрещающие правила **Файрвола** сразу блокируют соответствующий трафик, он не проходит дополнительную проверку в модуле **Предотвращение вторжений**.

Чтобы через модуль **Предотвращение вторжений** проходил трафик, для которого нет разрешающего правила в таблице FORWARD или INPUT, рекомендуем создать и включить в **Файрволе** правило с источником **Любой** и назначением **Любой**, разместив его в конец таблицы. В этом случае трафик, который не был найден в правилах **Файрвола**, но соответствует профилям IPS, пройдет проверку системой **Предотвращения вторжений**.

Подсказка: Если в одном правиле **Файрвола** включены проверки и **Контролем приложений**, и системой **Предотвращения вторжений**, трафик сначала попадет в обработку DPI, затем - IPS.

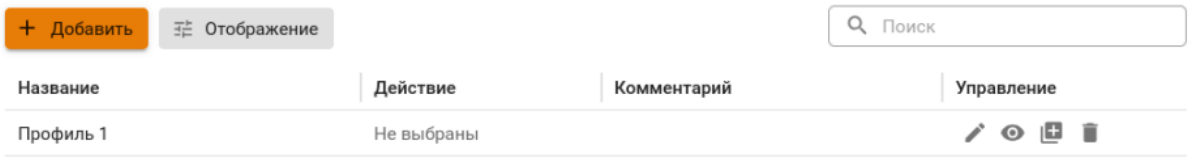
17.4.2 Создание профилей и добавление в правила Файрвола

Основное

Чтобы создать профиль **Предотвращения вторжений**, выполните действия:

1. Перейдите в раздел **Профили безопасности -> Предотвращение вторжений** и нажмите **Добавить профиль**.

2. Введите название профиля, комментарий и нажмите **Добавить**. Профиль появится в таблице:



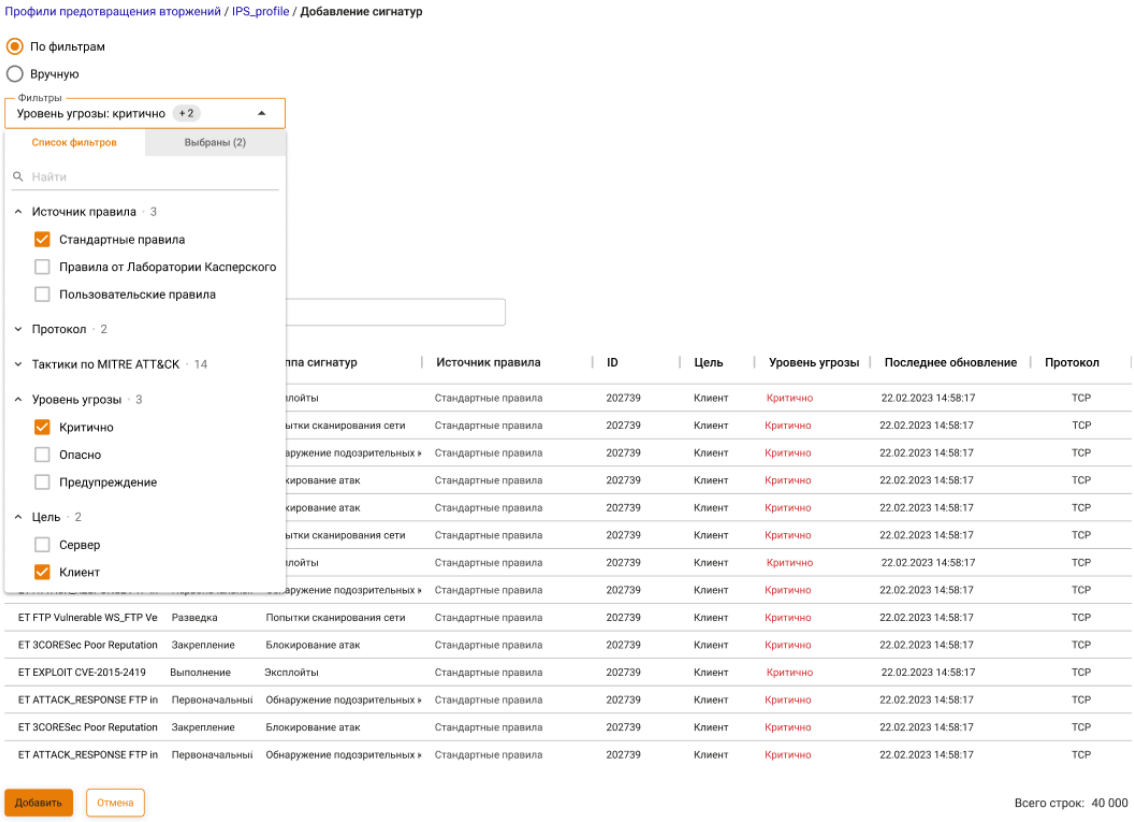
3. Нажмите на  напротив только что созданного профиля и выберите **Сигнатуры**.

4. Нажмите **Добавить**.

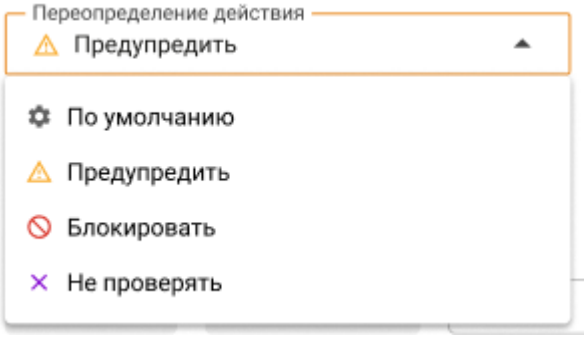
5. Выберите способ добавления сигнатур в профиль: **Вручную** или **По фильтрам**.

6. Если выбран способ добавления **По фильтрам**:

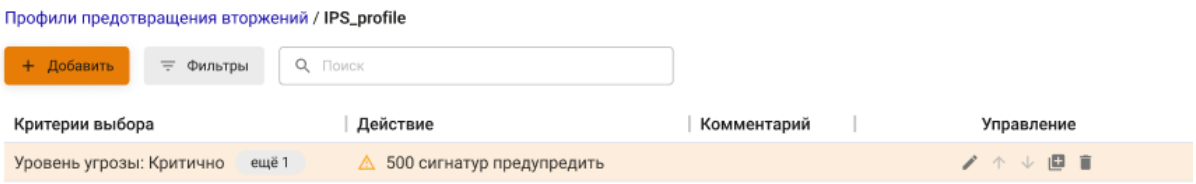
- Выберите **Фильтры**:
  - Источник правила (доступные варианты: *Стандартные правила*, *Правила от Лаборатории Касперского*, *Пользовательские правила*);
  - Протокол (доступные варианты: *TCP*, *UDP*, *ICMP*, *IP*);
  - Уровень угрозы (доступные варианты: *Критично*, *Опасно*, *Предупреждение*);
  - Цель (доступные варианты: *Клиент*, *Сервер*):



- Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие *По умолчанию*:

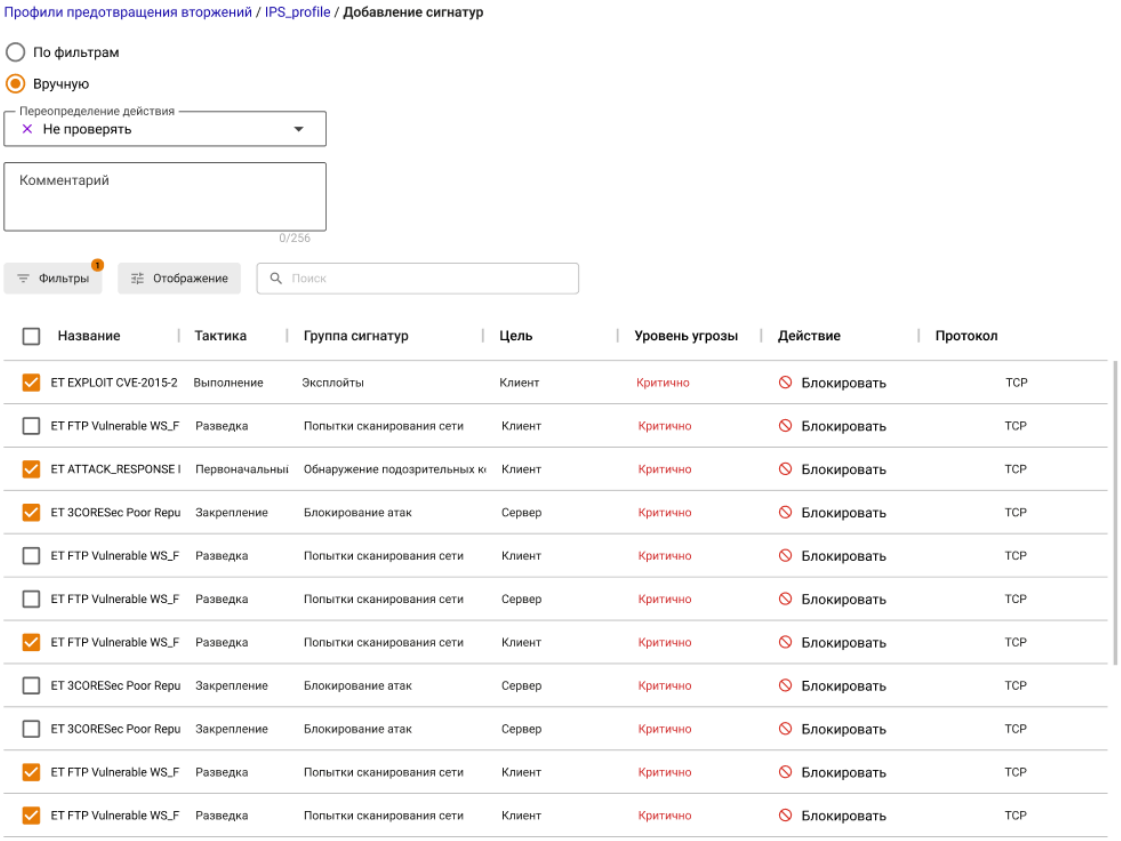


- Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

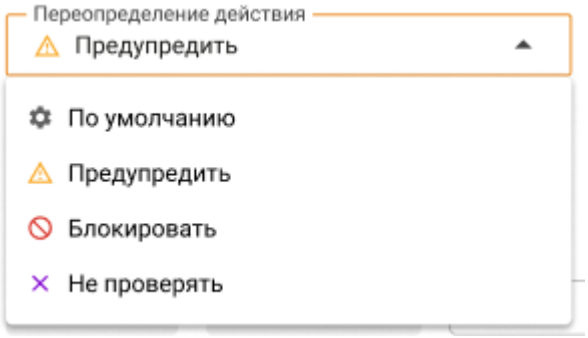


7. Если выбран способ добавления **Вручную**:

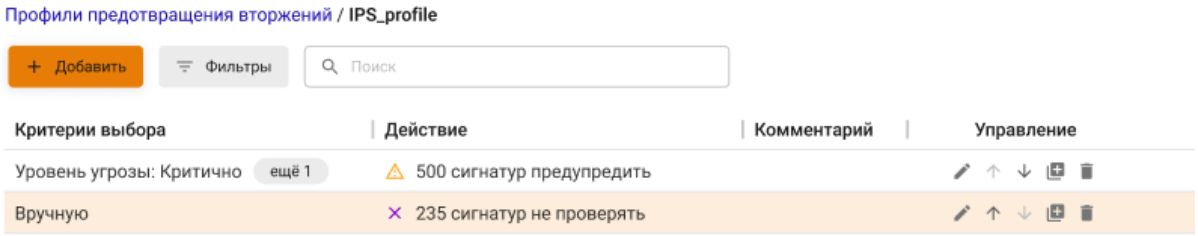
- В таблице отметьте сигнатуры, которые хотите добавить в профиль (при необходимости воспользуйтесь **Фильтром** отображения):



- Переопределите действие для выбранных сигнатур, выбрав необходимое в соответствующем поле, или оставьте действие *По умолчанию*:



- Нажмите **Добавить**. Правило выбора сигнатур появится в таблице профиля:

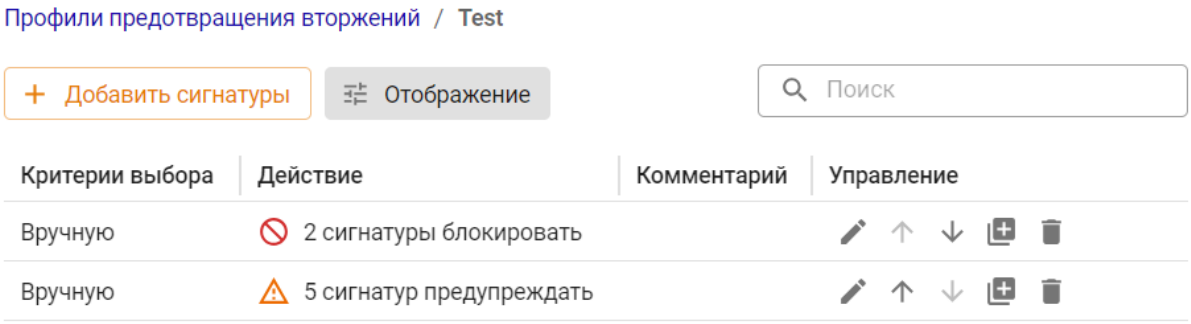


Подсказка: В один профиль **Предотвращения вторжений** можно добавить несколько правил выбора сигнатур. Их приоритет можно менять в таблице профиля кнопками ↑ и ↓.

Внимание: Количество сигнатур, отображаемых в таблице профилей, не всегда соответствует количеству сигнатур, добавленных при создании профиля. Это связано с тем, что для каждой сигнатуры может быть настроено несколько действий, но применяется только приоритетное. Приоритет определяется порядком правил внутри профиля.

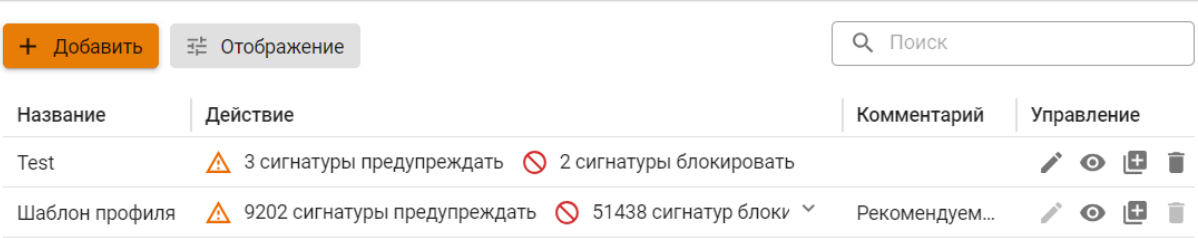
Пример отображения профиля при выборе нескольких действий сигнатур:

Настройки профиля Test:

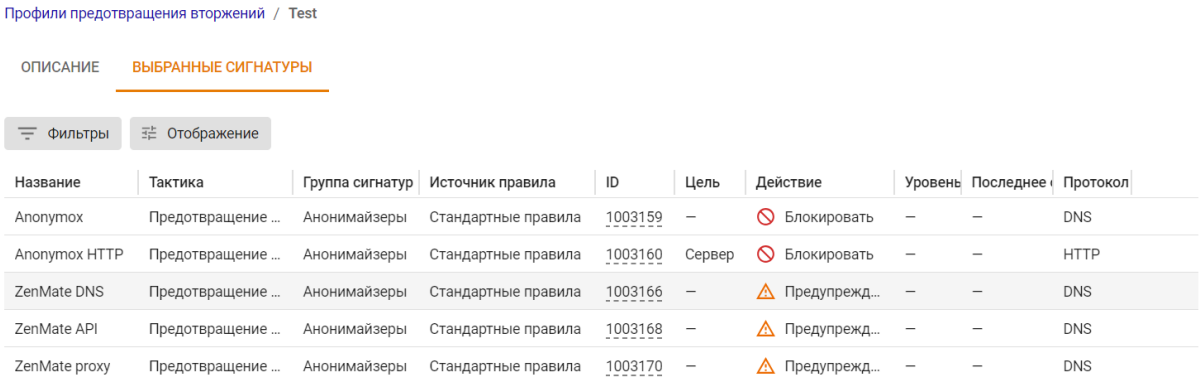


- Действие **Блокировать** применяется для сигнатур Anonymox и Anonymox HTTP (2 сигнатуры);
- Действие **Предупреждать** применяется для сигнатур Anonymox, Anonymox HTTP, ZenMate DNS, ZenMate API и ZenMate proxy (5 сигнатур);
- Блокирующее правило приоритетнее предупреждающего.

При переходе в раздел **Профили безопасности -> Предотвращение вторжений** в профиле Test отображаются 2 сигнатуры с действием **Блокировать** и 3 сигнатуры с действием **Предупреждать**, потому что фактически для дублирующихся сигнатур применяется более приоритетное правило:



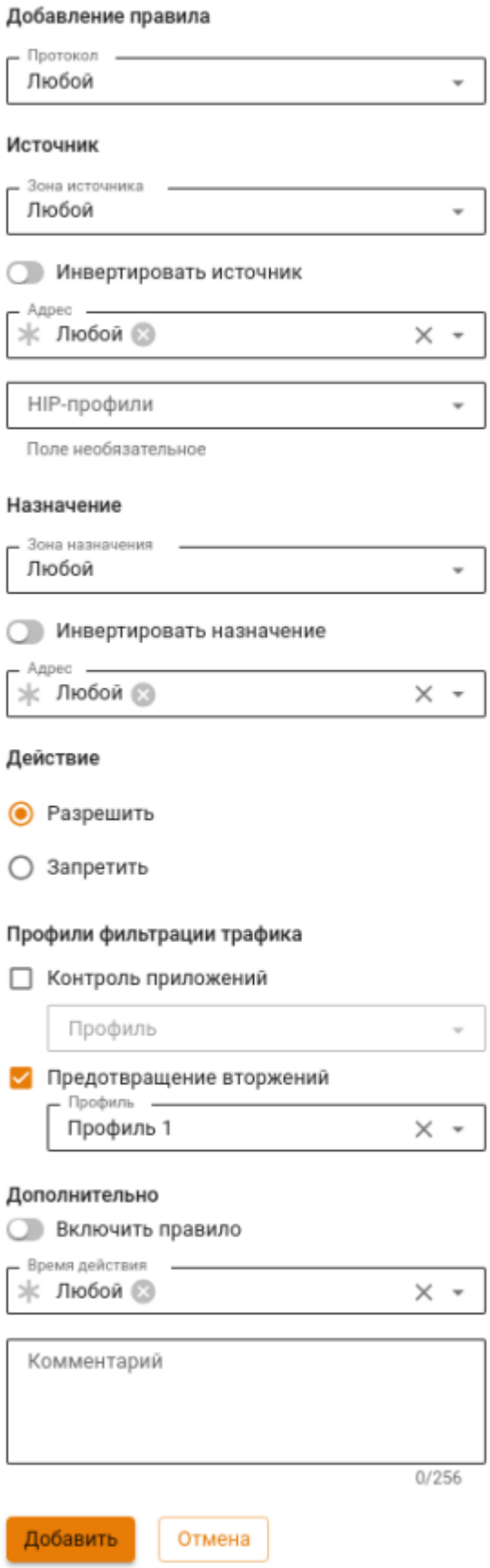
Чтобы просмотреть созданный профиль (описание и правила выбора сигнатур), нажмите на . На вкладке **Выбранные сигнатуры** представлены все сигнатуры, для которых настроено одно или несколько действий.



Для добавления правила **Файрвола** с профилем **Предотвращения вторжений** выполните действия:

1. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD** и нажмите **Добавить**.

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать системой **Предотвращения вторжений**;

- **Источник** - выберите **Адрес**, **Зону** и **HIP-профиль** источника трафика;
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика;
- **Действие** - выберите **Разрешить**;

3. Включите опцию **Предотвращение вторжений** и в разделе **Профили для фильтрации** из раскрывающегося списка выберите необходимый профиль.

4. Включите правило или оставьте его выключенным.

5. Нажмите **Добавить**.

6. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичное правило INPUT.

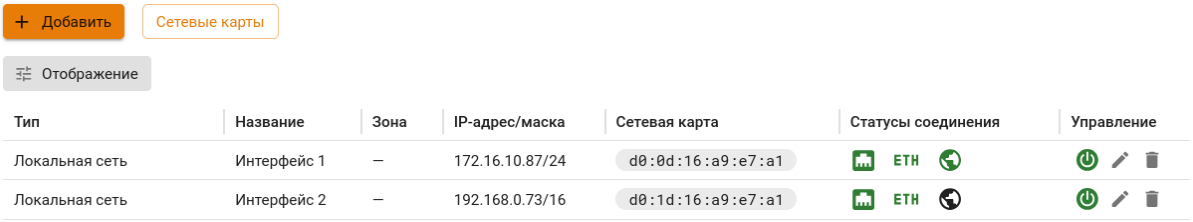
18. Сервисы

18.1 Сетевые интерфейсы

Подсказка: Название службы раздела *Сетевые интерфейсы*: `ideco-network-backend`; `ideco-network-nic`.
Список имен служб для других разделов доступен по *ссылке*.

Сетевой порт становится активным только после создания сетевого интерфейса (внешнего или локального). До этого момента индикаторы на подключенных сетевых портах не горят и Ethernet-кадры не передаются.

Все созданные интерфейсы представлены в виде таблицы:



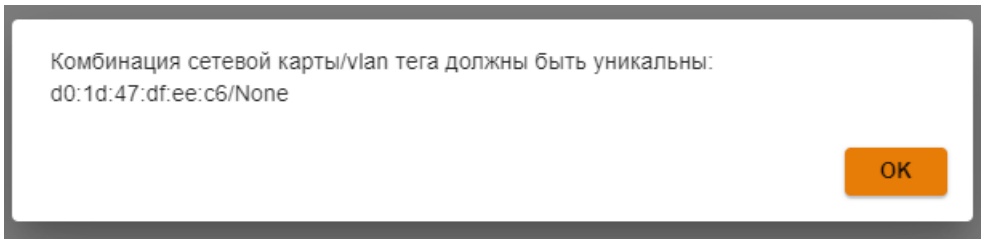
Статусы соединения:

-  - сигнал есть;
-  - статус сигнала не определен;
-  - сигнала нет;
-  - IP-адрес назначен;
-  - соединение с интернетом установлено;
-  - соединение с интернетом отсутствует.

В режиме редактирования доступно изменение названия, сетевой карты (по кнопке ), зоны, индекса интерфейса для Netflow и настроек конфигурации (вручную или автоматически):

Для перехода к редактированию интерфейса нажмите на  в столбце редактирования.

Если сетевая карта уже используется каким-либо интерфейсом, то NGFW выведет окно с ошибкой:



Подсказка: При миграции NGFW с одной физической машины на другую (перенос диска или восстановление бэкапа на новом оборудовании), будут восстановлены настройки всех сетевых интерфейсов, указанные до миграции. Для удаления ненужных интерфейсов воспользуйтесь кнопкой 20250219090034/docsUTM/.gitbook/assets.

Например: исходная версия NGFW 16.X -> провели миграцию NGFW на новое оборудование -> настроили новое оборудование -> провели обновление -> в разделе **Сетевые интерфейсы** будут отображаться старые (до миграции) и новые (после миграции и настройки) сетевые интерфейсы.

В зависимости от объема оперативной памяти на сервере в Ideco NGFW есть ограничения на количество сетевых интерфейсов:

- на количество сетевых VLAN-интерфейсов:
  - до 8 ГБ - 14 VLAN-интерфейсов;
  - от 8 до 16 ГБ - 33 VLAN-интерфейса;
  - 16 ГБ и более - 66 VLAN-интерфейсов.
    При создании большего количества VLAN-интерфейсов могут возникнуть проблемы в работе Контроля приложений и Ограничения скорости.
- на количество сетевых интерфейсов (не VLAN):
  - до 16 ГБ - 40 сетевых интерфейсов.

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

Подсказка: В Ideco NGFW нет подразделения локальных интерфейсов на VPN-интерфейсы и Ethernet, поскольку Ideco NGFW не содержит локальных VPN-интерфейсов.

18.1.1 Агрегированные интерфейсы

Подсказка:

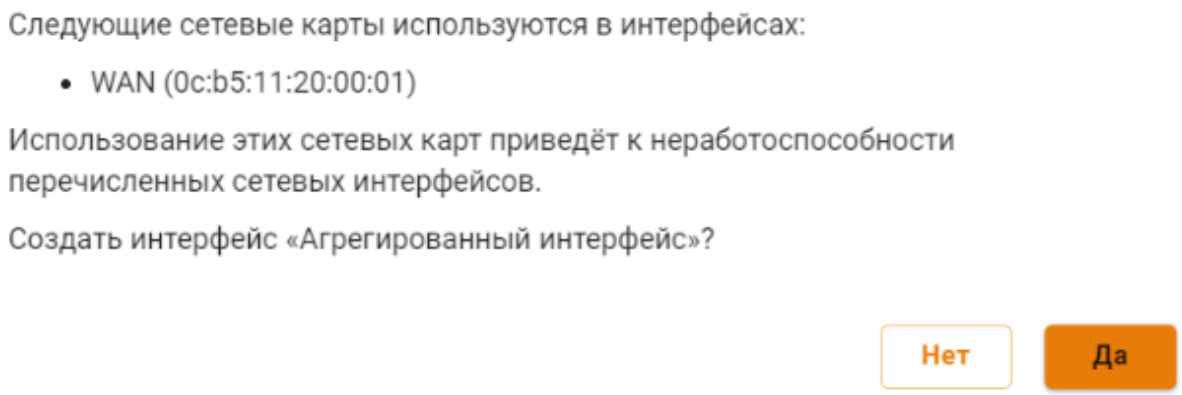
- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active** режим - постоянная рассылка LACP пакетов.
- Проверка соседства осуществляется в режиме **slow** - раз в 30 секунд.
- Количество сетевых карт, объединяемых в агрегированный интерфейс, не ограничено.
- Нельзя добавлять LACP-интерфейсы в VCE.

Чтобы объединить несколько сетевых интерфейсов в один агрегированный, перейдите в раздел **Сервисы -> Сетевые интерфейсы** и в таблице **Агрегированные интерфейсы (LACP)** нажмите **Добавить**. Укажите название, выберите сетевые карты и нажмите **Добавить**.

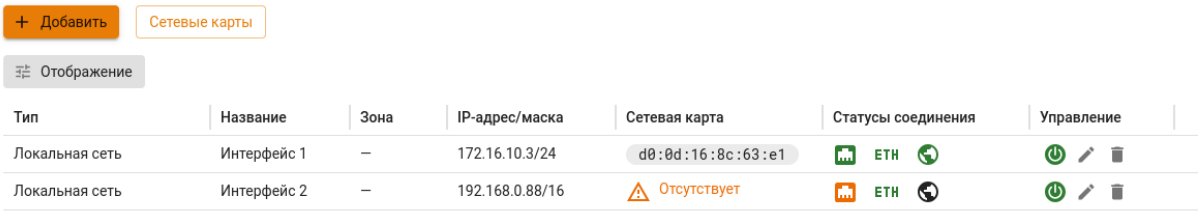
При выборе сетевой карты обращайте внимание на пиктограммы:

-  - сетевая карта уже используется другим интерфейсом;
-  - сетевая карта не используется.

Если были выбраны уже использующиеся сетевые интерфейсы, то при нажатии на кнопку **Добавить** появится сообщение:



При выборе **Да** сетевая карта будет использоваться агрегированным интерфейсом и станет недоступна для ранее созданного сетевого интерфейса:



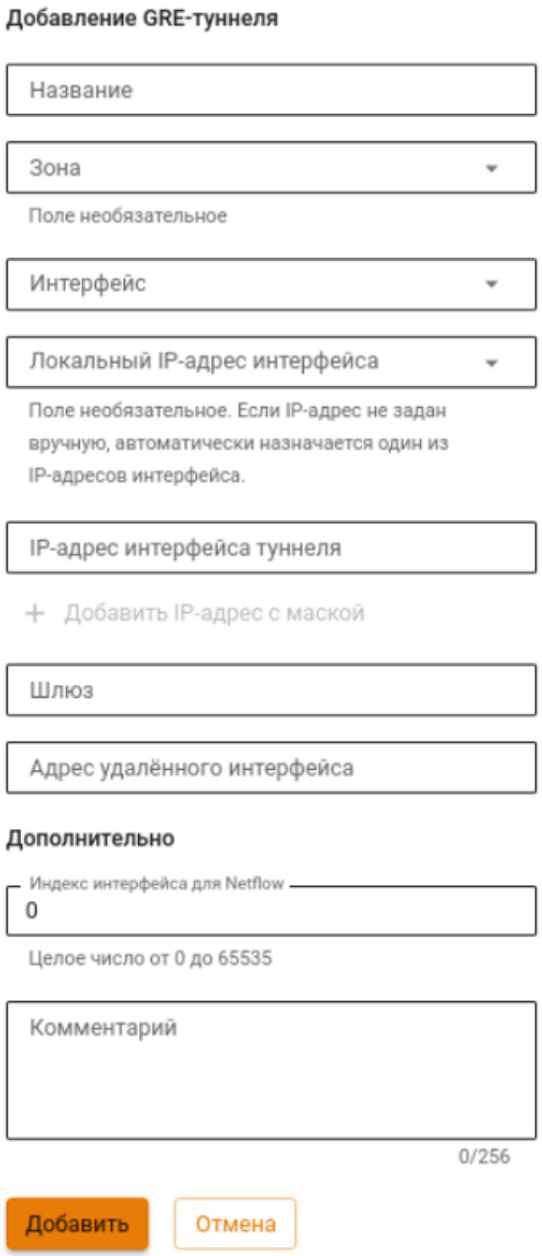
На основе созданного агрегированного интерфейса можно создавать любой логический интерфейс, в том числе с указанием VLAN.

18.1.2 Туннельные интерфейсы

На вкладке настраиваются GRE-туннели.

GRE-туннель - это соединение точка-точка с возможностью передавать широковещательный трафик. На таких интерфейсах может работать протокол динамической маршрутизации OSPF. Пакеты, проходящие внутри GRE, не шифруются.

Для добавления GRE-туннеля нажмите **Добавить**, заполните поля и нажмите **Добавить**:



- **Название** - введите название туннельного интерфейса;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый туннельный интерфейс;
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение;
- **Локальный IP-адрес интерфейса** - укажите IP-адрес родительского интерфейса запущенного туннеля;

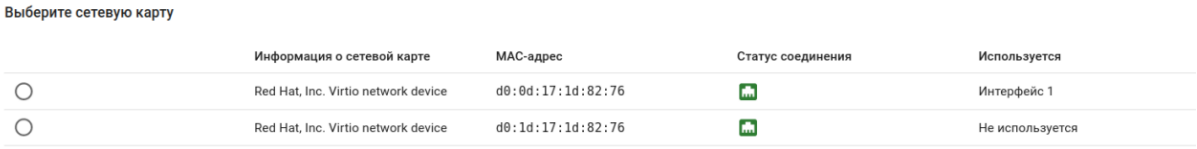
- **Адрес удаленного интерфейса** - укажите IP-адрес интерфейса, с которым будет производиться соединение;
- **IP-адрес/маска** - укажите данные создаваемого туннеля;
- **Шлюз** - шлюз для направления трафика по умолчанию;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса, если используете Netflow;
- **Комментарий** - поле может быть пустым.

18.1.3 VCE-интерфейсы

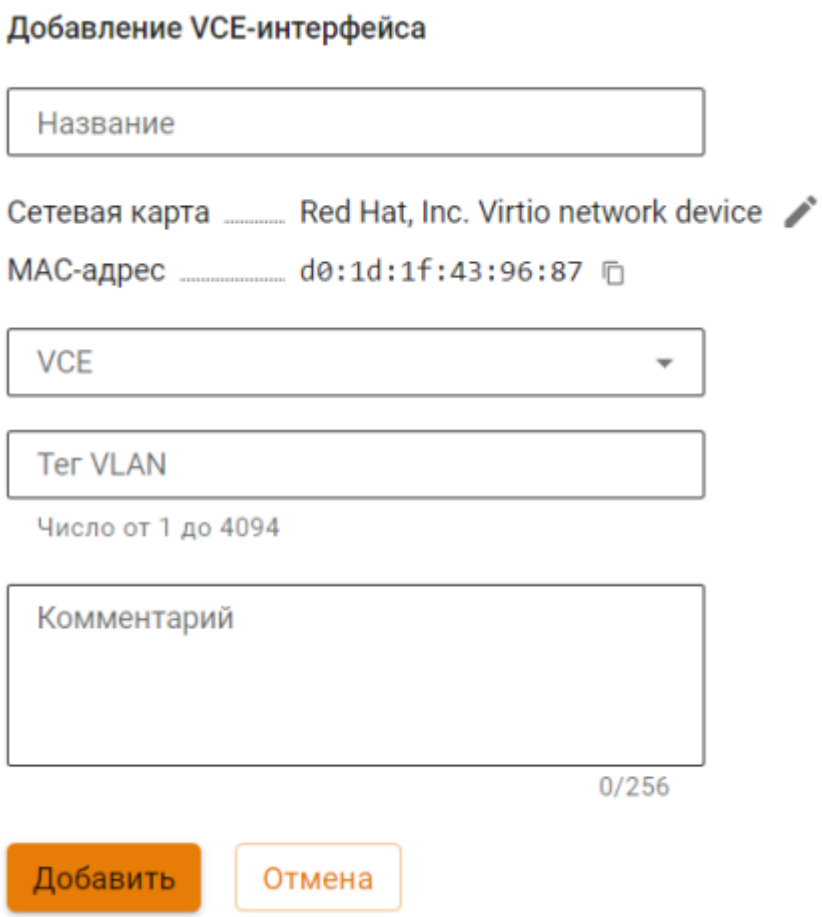
На этой вкладке пробрасываются сетевые карты и VLAN-интерфейсы Ideco NGFW в виртуальные серверы, созданные в разделе **Управление сервером -> *VCE***.

Чтобы назначить сетевую карту или VLAN-интерфейс VCE, нажмите **Добавить** и выполните действия:

1. Выберите сетевую карту:



2. Заполните следующие поля:



- **Название** - введите название VCE-интерфейса;

- **VCE** - выберите из списка VCE, созданный в разделе **Управление сервером -> VCE**;
- **Тег VLAN** - если нужно пробросить в VCE порт сетевой карты, оставьте поле пустым. Если нужно пробросить только VLAN, укажите тег VLAN - число от 1 до 4094;
- **Комментарий** - поле может быть пустым.

3. Нажмите **Добавить**.

При наличии большого количества VCE-интерфейсов в таблице воспользуйтесь кнопкой **Фильтры**.

По кнопке **Сетевые карты** доступны все сетевые карты корневого VCE, еще не проброшенные в дочерние VCE.

Подсказка: Переданная VCE сетевая карта будет недоступна для использования корневым NGFW. Также невозможно будет назначить эту карту другому VCE без указания тега VLAN.

Предупреждение: Не присваивайте VCE сетевые карты, которые используются корневым NGFW, без указания тега VLAN. В противном случае доступ к веб-интерфейсу NGFW будет потерян.

18.1.4 SPAN-интерфейсы

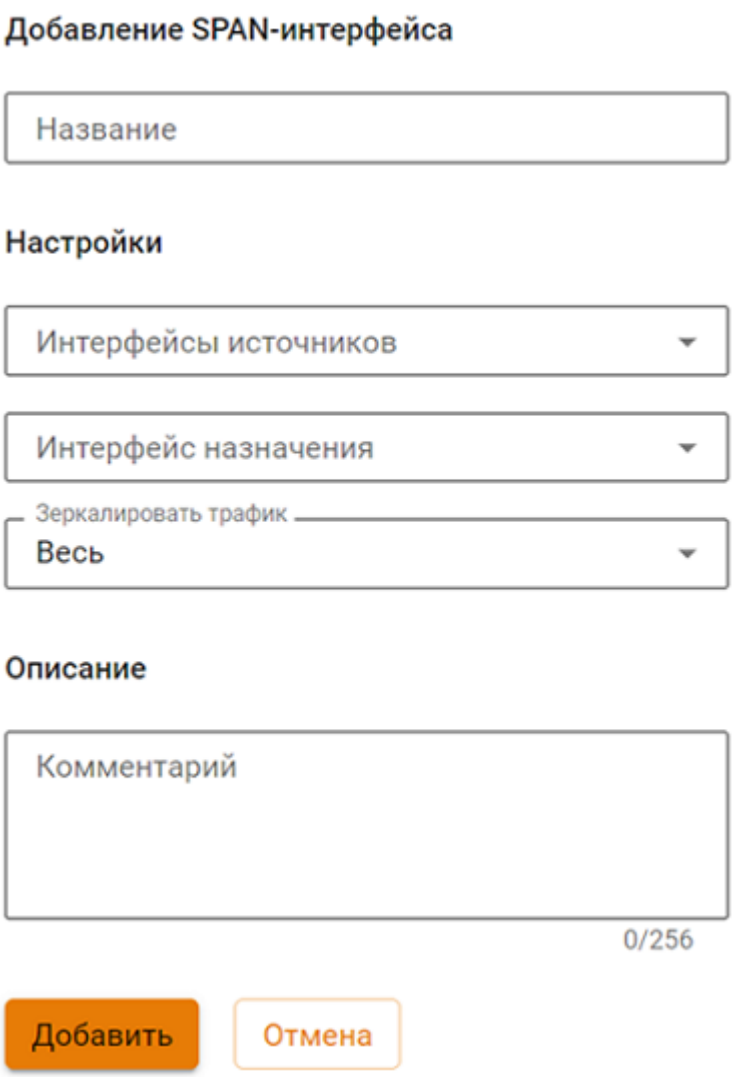
SPAN (Switch Port ANalyzer) - функция, которая позволяет копировать пакеты с порта или группы портов коммутатора или маршрутизатора (порт зеркалирования) и отправлять на выбранный порт (порт мониторинга). В Ideco NGFW SPAN-интерфейс позволяет дублировать трафик локальных и внешних интерфейсов на отдельное внешнее устройство для его мониторинга, анализа и выявления угроз.

Подсказка: SPAN-интерфейс должен быть свободным Ethernet-интерфейсом, не используемым для других целей.

Чтобы создать SPAN-интерфейс, выполните действия:

1. Перейдите в раздел **Сервисы -> Сетевые интерфейсы -> SPAN** и нажмите **Добавить**.

2. Заполните поля:



- **Название** - введите название SPAN-интерфейса;
- **Интерфейсы источников** - выберите интерфейсы, трафик которых хотите дублировать. Доступные варианты: Ethernet (как внешние, так и локальные, за исключением PPPoE, L2TP и PPTP), VLAN, а также клиентский VPN-трафик;
- **Интерфейс назначения** - выберите интерфейс, на который будет дублироваться трафик;
- **Зеркалировать трафик** - выберите тип трафика, который хотите дублировать. Доступные варианты: Весь, Только входящий или Исходящий;
- **Комментарий** - поле может быть пустым.

Предупреждение: Не указывайте в полях **Интерфейс источника** и **Интерфейс назначения** интерфейсы Ethernet + L2TP/PPTP/PPPoE. Этот тип интерфейсов не поддерживается в настройках SPAN.

3. Нажмите **Добавить**.

Внимание: SPAN-интерфейс может быть перегружен при большом количестве наблюдаемых интерфейсов.

18.1.5 Настройка Локального Ethernet

Внимание: Будьте внимательны!

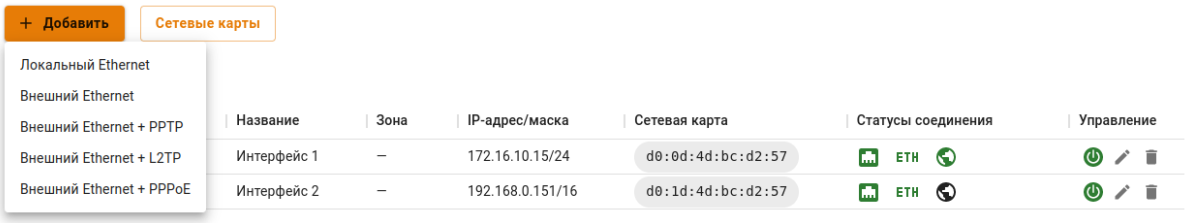
При выборе пункта **Локальный Ethernet** и заполнении поля **Шлюз** доступ в интернет будет отсутствовать. Шлюз указывается для маршрутизации внутри локальной сети или в режиме прямого прокси.

Ручная настройка

Для настройки подключения в веб-интерфейсе необходимо выполнить следующие действия:

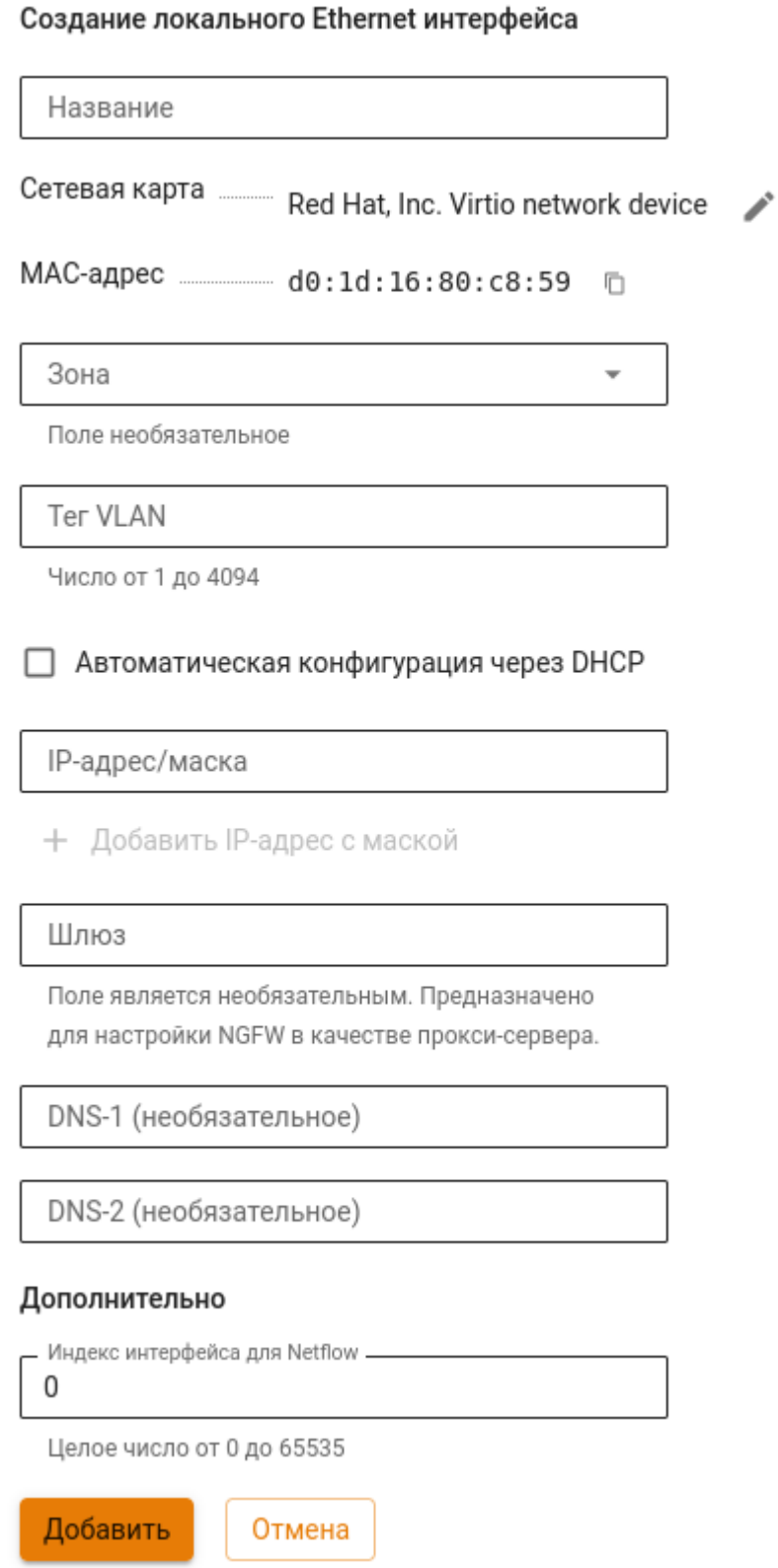
1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Локальный Ethernet**.



3. Выберите сетевую карту.

4. Заполните поля:



- **Название интерфейса** - имя для идентификации интерфейса;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;

- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется в том случае, если сетевая карта уже используется;
- **Автоматическая настройка через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Как минимум, должен быть указан хотя бы один IP-адрес;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS сервера (необязательно);
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Внимание: Поле **Шлюз** в Локальном интерфейсе задается только, если:

- Нет Внешнего интерфейса NGFW;
- NGFW используется как прокси-сервер.

Автоматическая настройка

Используется, если ваш интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Локальный Ethernet**.

3. Выберите сетевую карту.

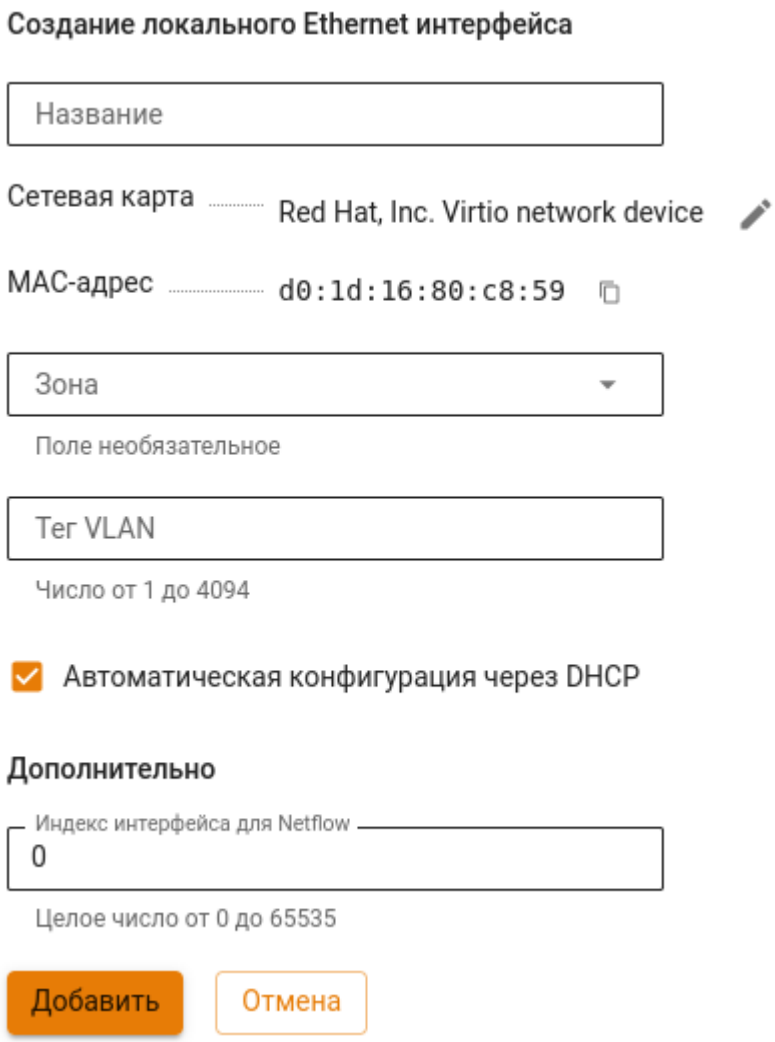
4. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется.

5. При необходимости выберите объект типа **Зона** в одноименном поле.

6. Включите настройку **Автоматическая конфигурация через DHCP**.

7. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Пример настройки:

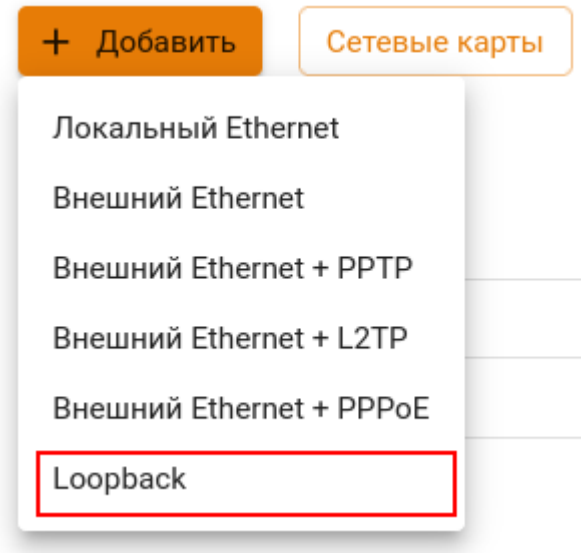


18.1.6 Настройка Loopback-интерфейса

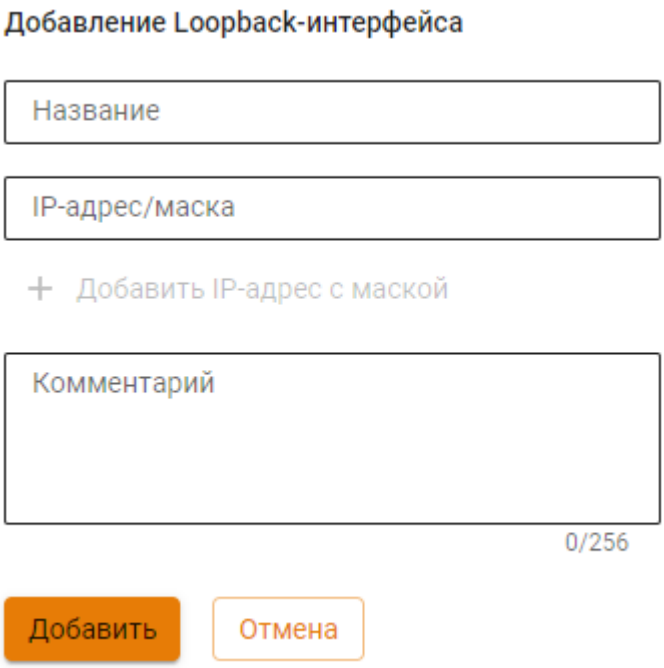
Loopback - это виртуальный интерфейс, который может использоваться для динамической маршрутизации (BGP и OSPF), удаленного администрирования и подключения пользователей по VPN. Преимущество Loopback-интерфейса в том, что он никогда не будет в состоянии Down - не перестанет работать, пока его не отключат административно.

Чтобы создать Loopback-интерфейс на Ideco NGFW, выполните действия:

1. Перейдите в раздел **Сервисы -> Сетевые интерфейсы -> Внешние и локальные** и нажмите **Добавить**. Выберите **Loopback**:



2. Заполните поля:



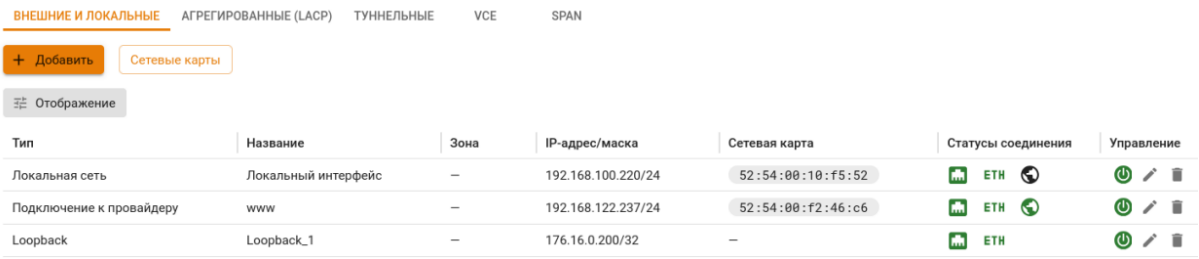
- **Название** - введите название интерфейса;
- **IP-адрес/маска** - введите IP-адрес, который требуется назначить на Loopback-интерфейс, с маской в формате `x.x.x.x/x`;
- **Комментарий** - поле не обязательное.

Предупреждение: Чтобы избежать проблем с подключением пользователей к Loopback-интерфейсу по VPN, IP-адрес Loopback-интерфейса **не должен** входить в диапазоны адресов, используемые для *SNAT*. Если включен автоматический SNAT локальных сетей, IP-адрес Loopback-интерфейса не должен входить в диапазоны:

- `10.0.0.0/8`
- `192.168.0.0/16`

- `172.16.0.0/12`

4. Нажмите **Добавить**. Loopback-интерфейс появится в таблице внешних и локальных интерфейсов:



Использование Loopback-интерфейса

Loopback-интерфейс можно использовать:

1. Для доступа к веб-интерфейсу Ideco NGFW укажите в адресной строке браузера `<IP-адрес Loopback-интерфейса>:8443`.

2. Для доступа к серверу по SSH:

   - *Разрешите доступ по SSH*;
   - Введите в терминале `ssh login@<IP-адрес Loopback-интерфейса>`.

3. Для подключения пользователей по VPN на устройстве пользователя при *создании VPN-подключения* в качестве шлюза укажите домен или IP-адрес Loopback-интерфейса.

4. В разделе ***BGP*** при добавлении **BGP-соседей** укажите в поле **Исходящий интерфейс** Loopback-интерфейс.

5. При настройке ***OSPF*** укажите в поле **Интерфейс** Loopback-интерфейс.

6. При создании *маршрута Null route* укажите Loopback-интерфейс в качестве шлюза для подсети/IP-адресов. В этом случае весь входящий на NGFW трафик, предназначенный для этих адресов, будет отбрасываться.

7. При создании *DNAT-правила* **Файрвола** в поле **Адрес назначения** укажите IP-адрес, назначенный на Loopback-интерфейс. Опубликованные ресурсы будут доступны по IP-адресу Loopback-интерфейса.

8. При создании *SNAT-правила* **Файрвола** в поле **Сменить IP-адрес источника** укажите IP-адрес, назначенный на Loopback-интерфейс. Исходный адрес, указанный в поле **Адрес источника**, будет заменен на адрес Loopback-интерфейса.

Предупреждение: Для подключения к Loopback-интерфейсу настройте маршрутизацию до IP-адреса, назначенного на этот Loopback-интерфейс.

18.1.7 Настройка Внешнего Ethernet

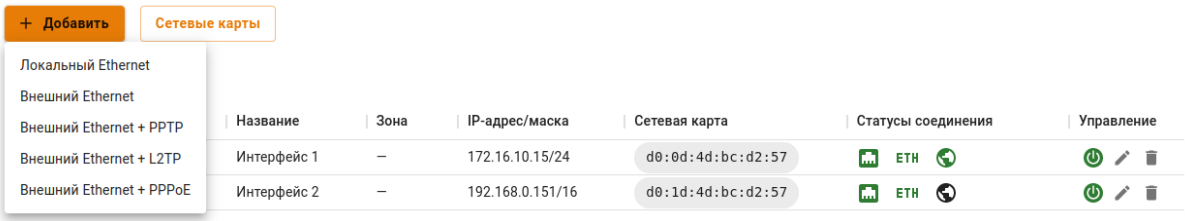
Как правило, вся необходимая информация для настройки содержится в договоре с интернет-провайдером.

Ручная настройка

Для настройки подключения в веб-интерфейсе необходимо выполнить следующие действия:

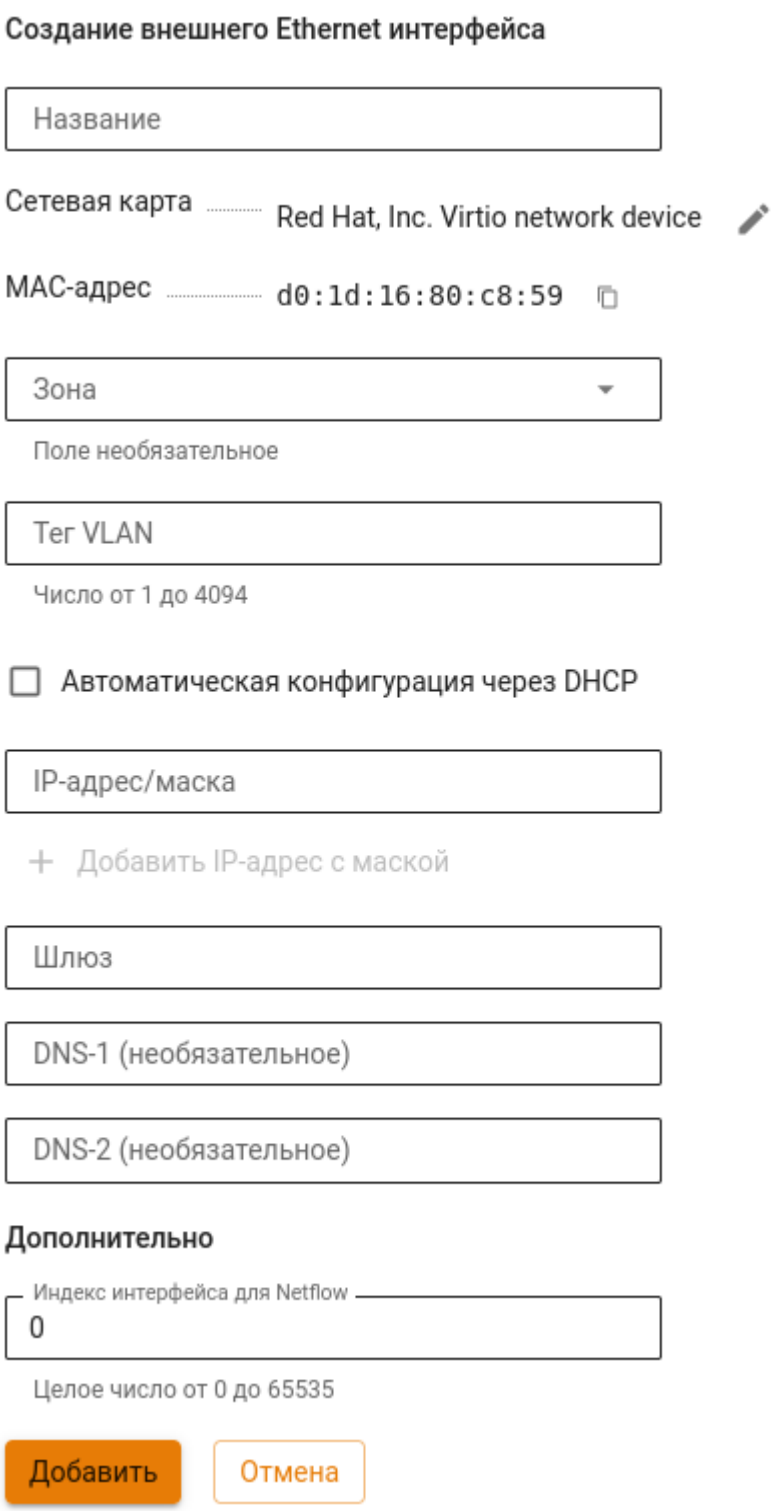
1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Внешний Ethernet**:



3. Выберите сетевую карту.

4. Заполните поля:



- **Название интерфейса** - имя, с помощью которого возможно в дальнейшем идентифицировать интерфейс;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который

будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется только в том случае, если сетевая карта уже используется;

- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес;
- **Шлюз** - укажите IP-адрес шлюза интернет-провайдера, через который будет осуществляться подключение к сети интернет;
- **DNS** - доступно два поля для указания DNS-сервера (необязательно);
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.............................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

Автоматическая настройка

Используется, если интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Внешний Ethernet**.

3. Выберите сетевую карту.

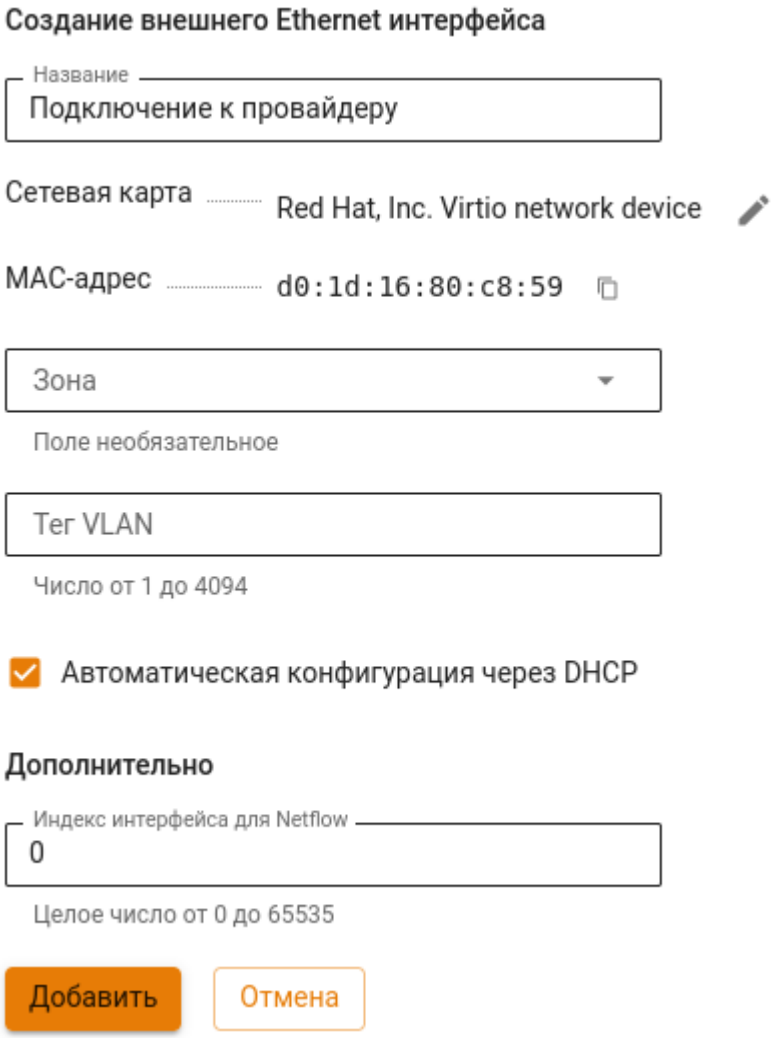
4. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется.

5. При необходимости выберите объект типа **Зона** в одноименном поле.

6. Включите настройку **Автоматическая конфигурация через DHCP**.

7. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Пример настройки:



18.1.8 Настройка подключения по PPTP

Основное

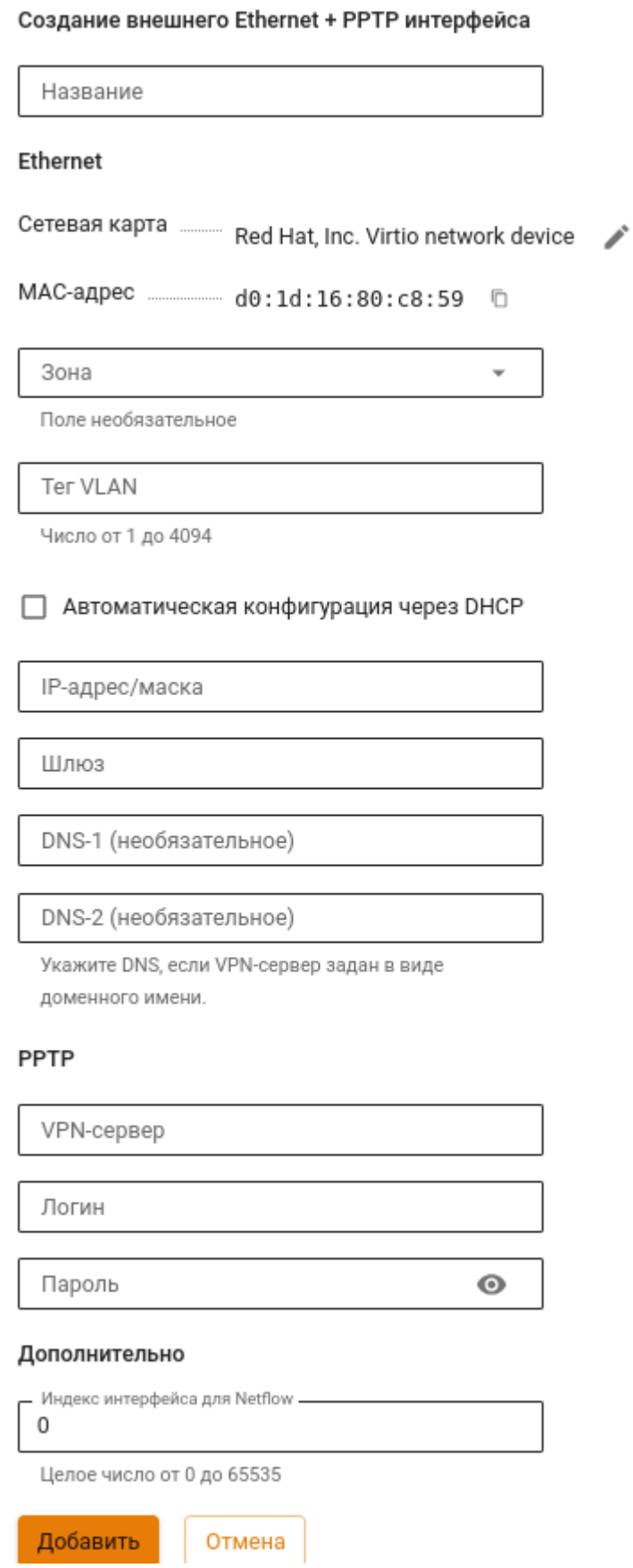
Для настройки такого подключения в веб-интерфейсе необходимо выполнить следующие действия:

1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите **Ethernet + PPTP**.

3. Выберите сетевую карту.

4. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-

провайдеру;

- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q;
- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS-сервера (необязательно);
- **VPN-сервер** - IP-адрес или доменное имя PPTP-сервера;
- **Логин** - имя пользователя для подключения по PPTP;
- **Пароль** - пароль для подключения по PPTP;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.............................
Download: 3887.98 Mbit/s
Testing upload speed..................................
................................................
Upload: 2235.66 Mbit/s
```

18.1.9 Настройка подключения по L2TP

Основное

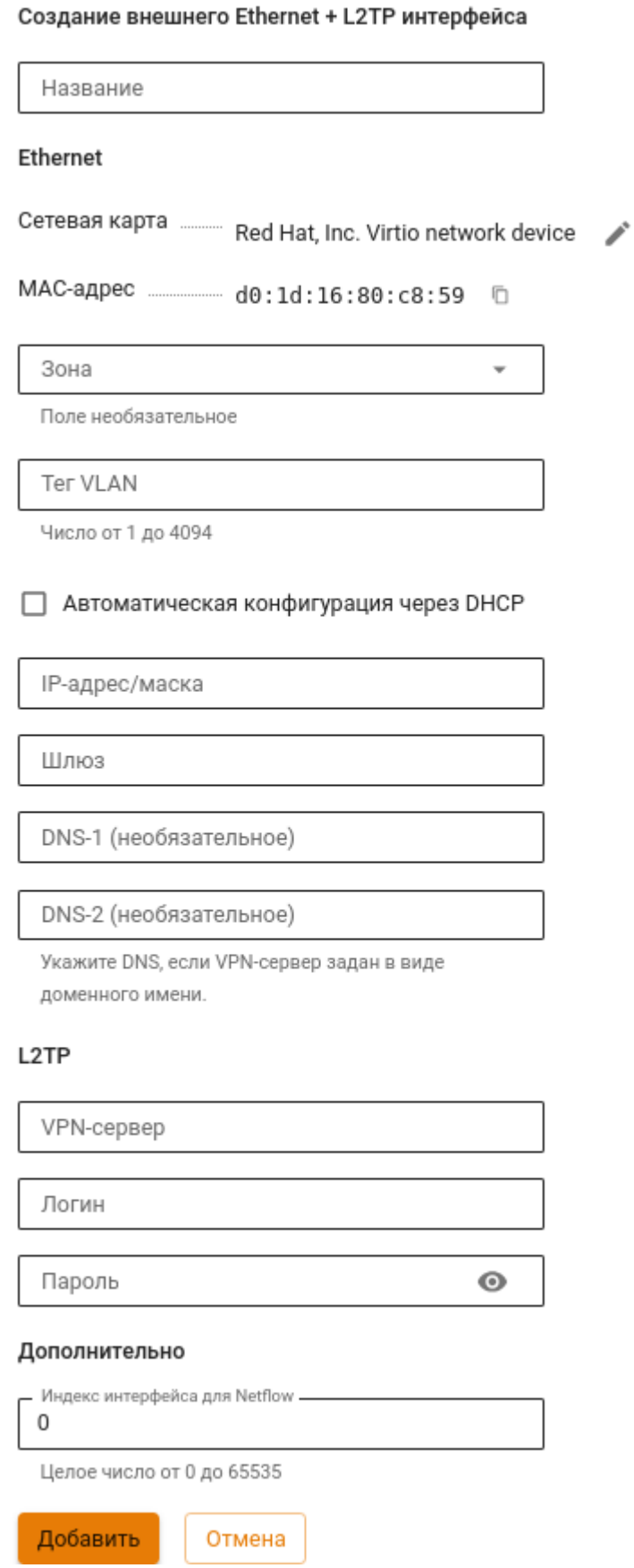
Для настройки такого подключения в веб-интерфейсе необходимо выполнить следующие действия:

1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Ethernet + L2TP**.

3. Выберите сетевую карту.

4. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-

провайдеру;

- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае если сетевая карта уже используется. Стандарт VLAN 802.3q;
- **Автоматическая конфигурация через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS-сервера (необязательно);
- **VPN-сервер** - IP-адрес или доменное имя L2TP-сервера;
- **Логин** - имя пользователя для подключения по L2TP;
- **Пароль** - пароль для подключения по L2TP;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.............................
Download: 3887.98 Mbit/s
Testing upload speed..................................
................................................
Upload: 2235.66 Mbit/s
```

18.1.10 Настройка подключения по PPPoE

Основное

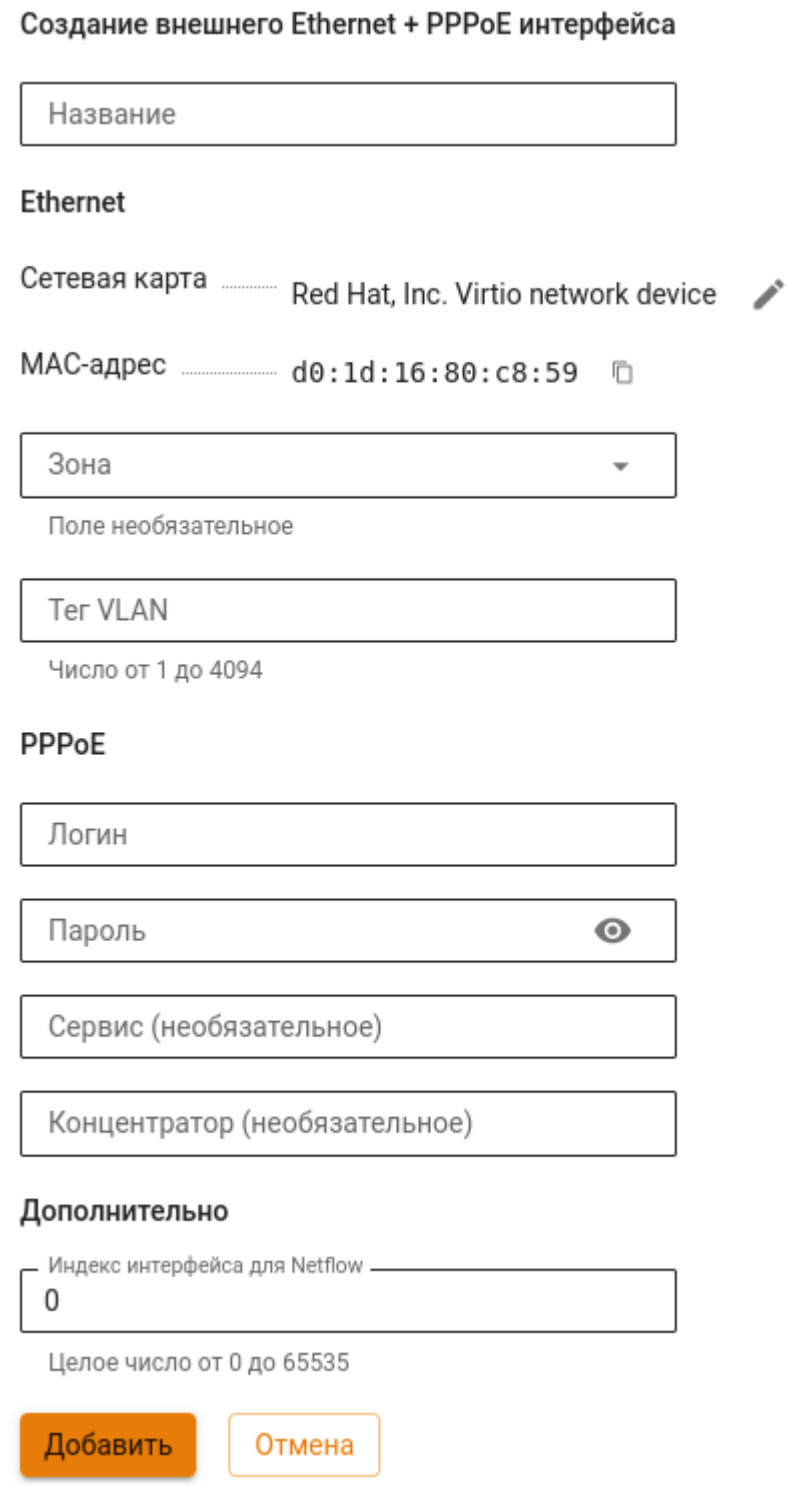
Для настройки подключения в веб-интерфейсе необходимо выполнить следующие действия:

1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Ethernet + PPPoE**.

3. Выберите сетевую карту.

4. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q;

- **Логин** - имя пользователя для подключения по PPPoE;
- **Пароль** - пароль для подключения по PPPoE;
- **Сервис** - идентификатор сервиса. Необязательное поле;
- **Концентратор** - идентификатор концентратора. Необязательное поле;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Добавить**.

Подсказка: При подключении к провайдеру с использованием протокола PPPoE настройте DNS-сервер вручную, воспользовавшись *статьей*.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.............................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

18.1.11 Подключение по 3G и 4G

Основное

Сервер Ideco NGFW поддерживает некоторые модели USB-модемов, например, Huawei E8372. При подключении USB-модем будет отображаться в Ideco NGFW как новый ethernet-интерфейс.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.............................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

18.2 Балансировка и резервирование

Подсказка: Название службы раздела **Балансировка и резервирование**: `ideco-routing-backend`. Список служб для других разделов доступен по *ссылке*.

При наличии нескольких подключений к интернет-провайдерам балансировку и резервирование можно осуществлять следующими способами:

- Резервирование одного из подключений, при отключении которого трафик пойдет через другие доступные подключения;
- Статическая балансировка трафика между несколькими подключениями. При этом часть пользователей локальной сети будет выходить в интернет через одного провайдера, часть - через другого;
- Динамическая балансировка трафика между несколькими подключениями. При этом подключения будут поочередно переключаться в зависимости от нагрузки, а сессии от всех пользователей будут равномерно распределяться между ними.

Перед настройкой убедитесь, что на сервере уже созданы минимум два подключения к сети интернет. Если нет, то создайте дополнительное подключение. Подробнее о создании подключения в статье *Настройка Внешнего Ethernet*

Для работы с трафиком в Ideco NGFW важно учитывать 2 момента: маршрутизация и NAT. Это касается как балансировки, так и резервирования.

Видеоинструкция по Балансировке и резервированию:

Ссылка на видеоинструкцию по балансировке и резервированию

18.2.1 Основное

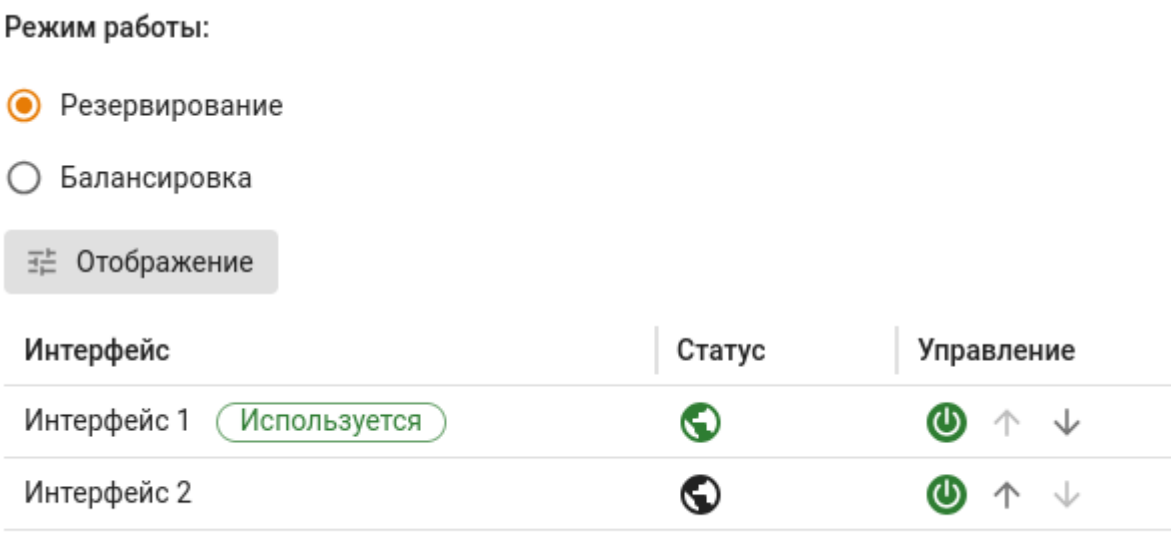
На вкладке доступен выбор одного из двух режимов - **Балансировка** или **Резервирование**.

При **Резервировании** Ideco NGFW использует каналы в соответствии с их приоритетом. Приоритет задается порядком подключений в таблице, сверху вниз. Если интернет стал недоступен через используемое подключение, то NGFW будет перебирать подключения сверху вниз (до первого рабочего подключения).

При **Балансировке** сервер балансирует трафик в зависимости от загрузки подключений.

Резервирование каналов

Перейдите в раздел **Сервисы -> Балансировка и резервирование** и выберите режим **Резервирование**.

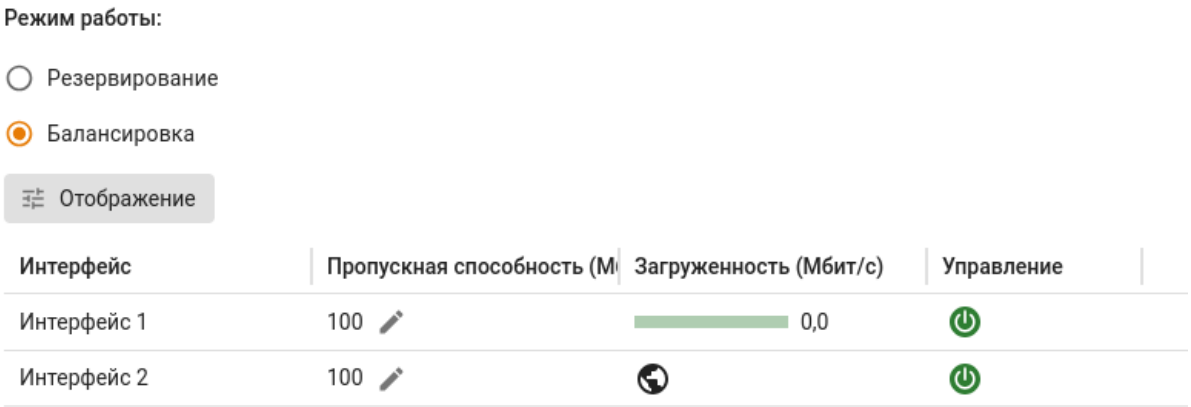


Подключение, которое используется в данный момент, отмечено тегом **Используется**. Для смены приоритета используйте соответствующие элементы управления (↑ ↓).

Динамическая балансировка. Распределение нагрузки по нескольким подключениям

Действия для настройки:

1. Перейдите в раздел **Сервисы -> Балансировка и резервирование**.
2. Выберите режим работы **Балансировка**.

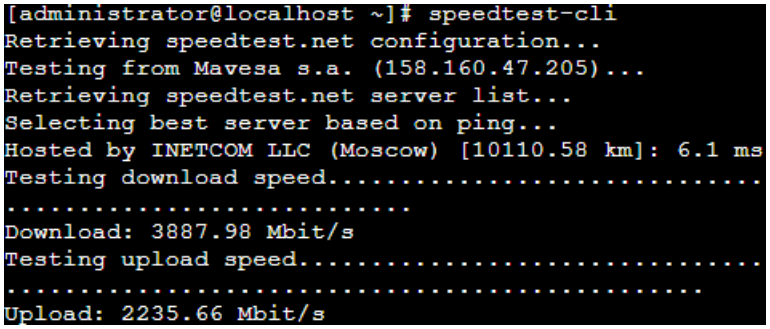


Для равномерного распределения сессий между подключениями необходимо указать значение **Пропускной способности** - максимальной скорости интернета по тарифам провайдеров. Ideco NGFW будет автоматически балансировать трафик в зависимости от загрузки подключений.

Подсказка: Создавать маршруты или выполнять еще какие-либо настройки для динамической балансировки трафика не требуется. Трафик прокси-сервера также будет балансироваться автоматически.

Подсказка: Для проверки скорости подключения перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:



Статическая балансировка. Доступ к сети интернет через определенное подключение к провайдеру

Способы применения:

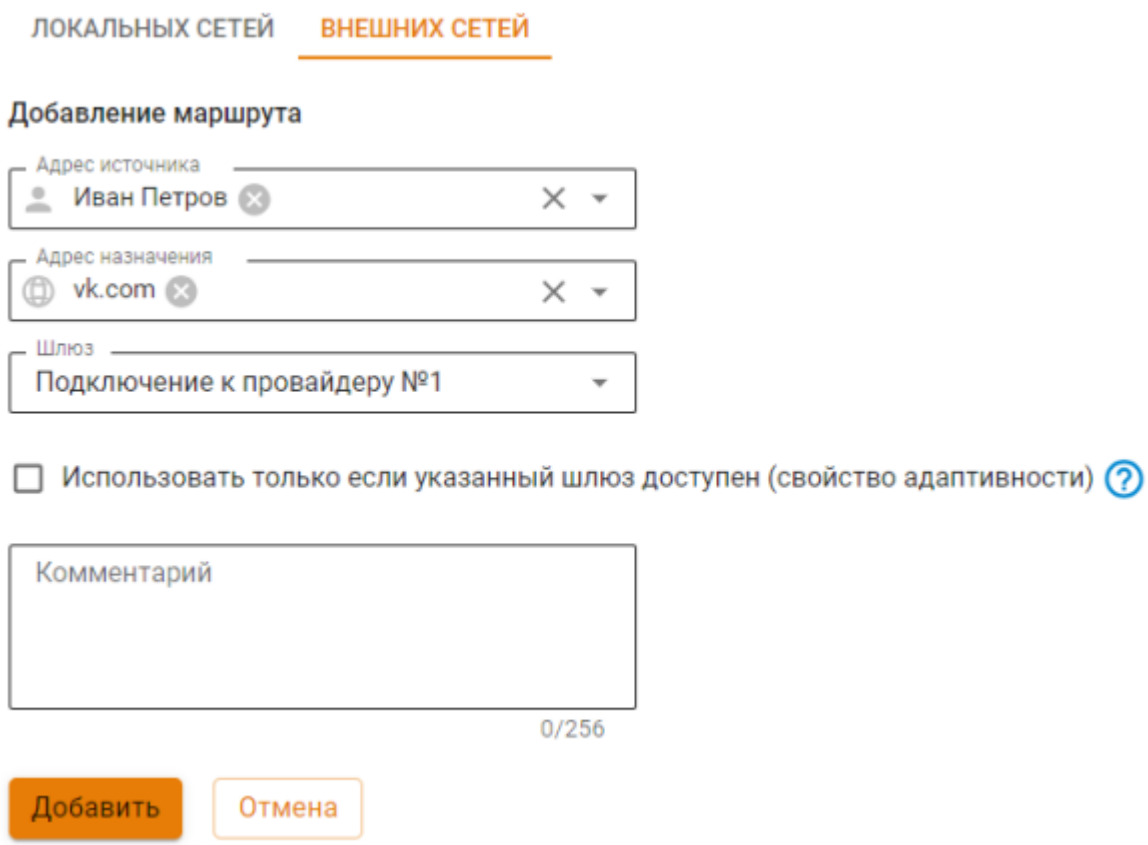
- Направление части трафика через интернет-провайдера, чья тарификация для этого трафика дешевле.
- Предоставление доступа к внутренним сетям одного из провайдеров для определенных пользователей/групп пользователей.

Действия для настройки:

1. Перейдите в раздел меню **Сервисы -> Маршрутизация -> Внешних сетей**.

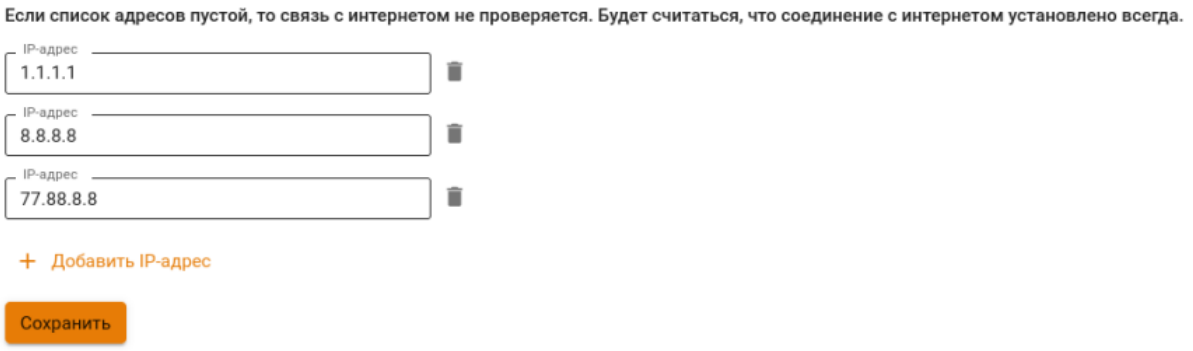
2. Добавьте правила маршрутизации для определенного списка ресурсов, трафик к которым необходимо направить через нужное подключение к провайдеру, нажав кнопку **Добавить**.

Пример направления трафика к ресурсу **vk.com** от пользователя **Иван Петров** через подключение к провайдеру **Подключение к провайдеру №1**:



18.2.2 Адреса для проверки связи

На вкладке задаются IP-адреса, которые Ideco NGFW будет использовать для проверки связи с интернетом. По умолчанию заданы три IP-адреса - DNS-серверы Cloudflare, Google и Яндекс:



Сервер посылает на эти адреса ping-запросы. Соединение с инернетом считается установленным, если проходит пинг хотя бы до одного адреса из списка. Если этого не происходит, NGFW считает, что соединение с интернетом у интерфейса отсутствует - статус интерфейса меняется с  на  .

Подсказка: Если список адресов будет пустым, то связь с интернетом проверяться не будет. Будет считаться, что соединение с интернетом установлено всегда.

18.3 Маршрутизация

Подсказка: Название службы раздела **Маршрутизация**: `ideco-routing-backend`.
Список служб для других разделов доступен по *ссылке*.

Преимущества маршрутизации Ideco NGFW:

- Возможность указывать сеть источника при маршрутизации внешних сетей;
- Функция адаптивности (в случае недоступности шлюза или интерфейса поиск маршрута продолжится по следующим правилам в таблице маршрутизации).

Подсказка: Доступность шлюза проверяется с помощью отправки ARP-запроса на получение MAC-адреса для IP, указанного в качестве шлюза.

В веб-интерфейсе Ideco NGFW есть возможность маршрутизировать локальные и внешние сети. Создавать и редактировать маршруты можно в разделе **Сервисы -> Маршрутизация**.

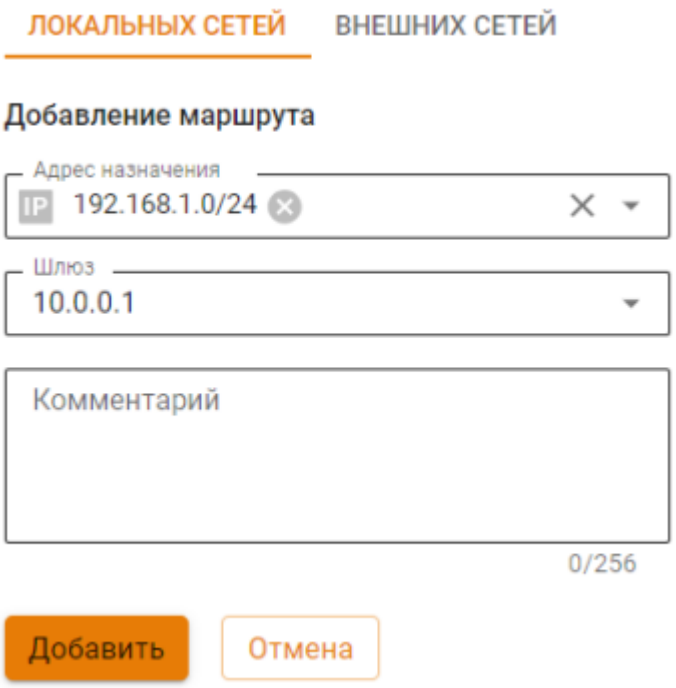
Для организации доступа в удаленные сети через роутер в локальной сети читайте статью по *ссылке*.

Подсказка: При маршрутизации локальных и внешних сетей доступны GRE-интерфейсы в качестве шлюза.

Видеоинструкция по настройке Маршрутизации Ideco NGFW: Ссылка на видеоинструкцию по маршрутизации Ideco NGFW

18.3.1 Маршрутизация локальных сетей

Маршрутизация локальных сетей действует внутри локальных сетей. Поэтому при добавлении маршрута отсутствует поле **Адрес источника**. Для добавления нового маршрута перейдите в раздел **Сервисы -> Маршрутизация -> Локальных сетей** и нажмите **Добавить**:



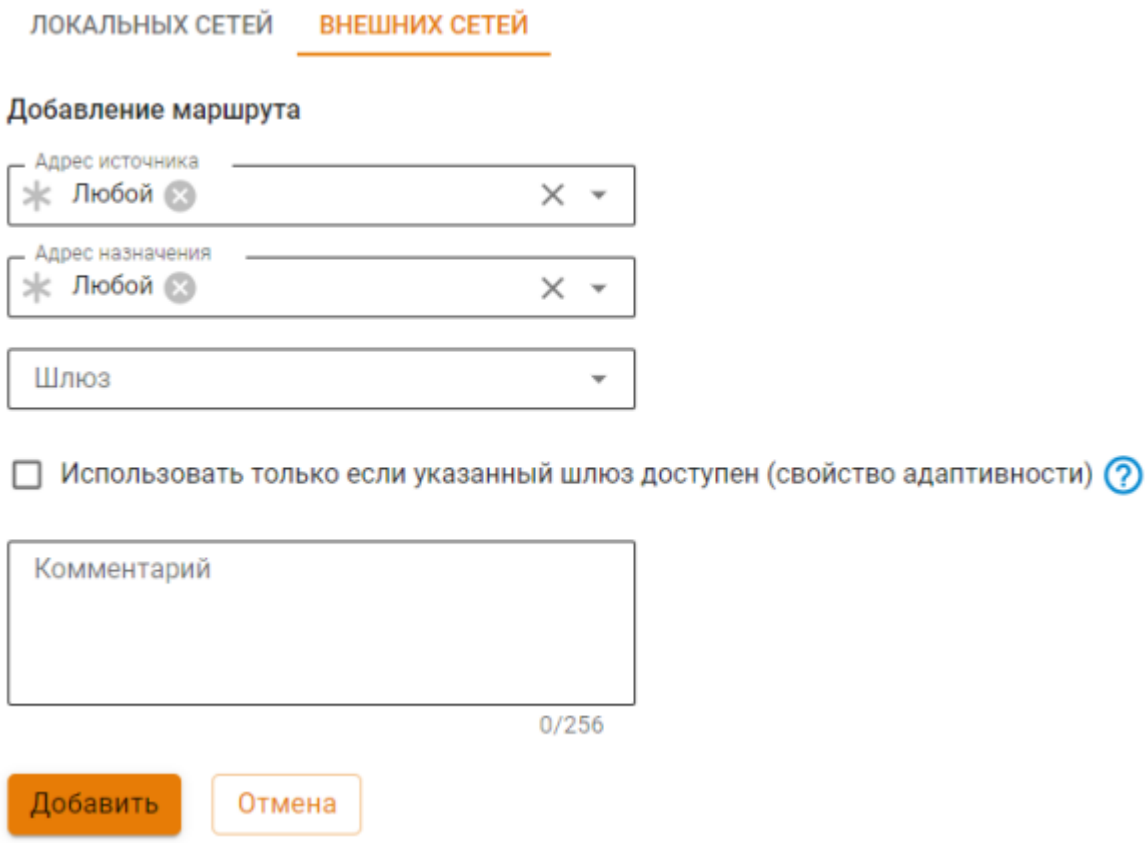
- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться это правило. Возможные типы объектов: IP-адрес, подсеть, домен, список IP-объектов, диапазон IP-адресов;
- **Шлюз** - выберите объект, через который направляется трафик. Возможные типы объектов: IP-адрес, пользователь;
- **Комментарий** - необязательное поле описания маршрута. Значение - не длиннее 128 символов.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: При создании IPSec-подключения в разделе **Сервисы -> IPsec** с включенной опцией **Автоматическое создание маршрутов** будут добавляться маршруты до локальных сетей NGFW в таблицу **Маршрутизации локальных сетей**.

18.3.2 Маршрутизация внешних сетей

Для добавления нового маршрута перейдите в раздел **Сервисы -> Маршрутизация -> Внешних сетей** и нажмите кнопку **Добавить**. На странице откроется форма создания маршрута:

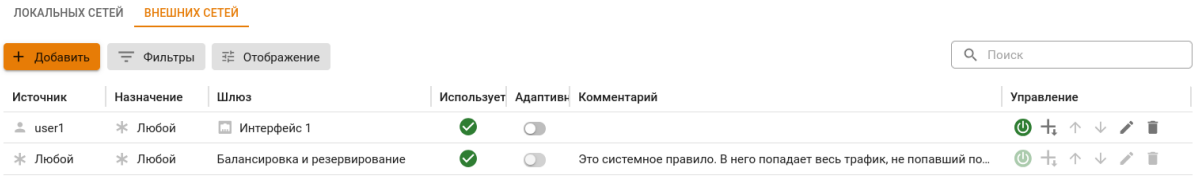


Опишем назначение каждой опции:

- **Адрес источника** - выберите объекты, для которых будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен;
- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен;
- **Шлюз** - выберите объект, через который будет направлен трафик. Возможные типы объектов: сетевой интерфейс, IP-адрес;

- **Использовать только если шлюз доступен (адаптивность)** - если свойство включено, то при недоступности шлюза или интерфейса поиск маршрута продолжится по следующим правилам маршрутизации. Если свойство отключено (по умолчанию), то трафик отправляется в выбранный шлюз или интерфейс. Если шлюз недоступен или интерфейс не работает, то трафик будет отброшен (destination unreachable);
- **Комментарий** - необязательное поле описания маршрута. Значение не должно быть длиннее 128 символов.

После сохранения маршрута страница выглядит так:



Кнопки и повышают или понижают приоритет правила.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

Статусы в столбце **Используется**:

- - маршрут активен и трафик, попадающий под условия маршрута, будет перенаправлен в указанный Шлюз;
- - маршрут не активен и трафик, попадающий под условия маршрута, не будет обработан правилом.

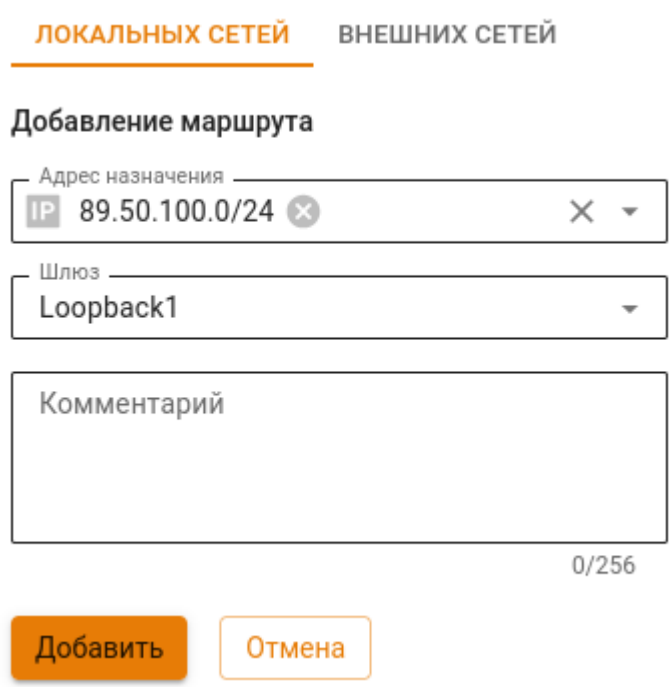
Подсказка: Трафик, не попавший под условия правил маршрутизации, или с объектом **Любой** в качестве шлюза, будет отправлен в *Балансировку и резервирование*.

Примеры популярных маршрутов

При маршрутизации трафика через подключения к провайдеру важно понимать, что чаще всего одного маршрута недостаточно. Понадобится также переопределить адрес с помощью SNAT, иначе такой маршрут не будет работать. SNAT можно настроить с помощью *Файрвола*.

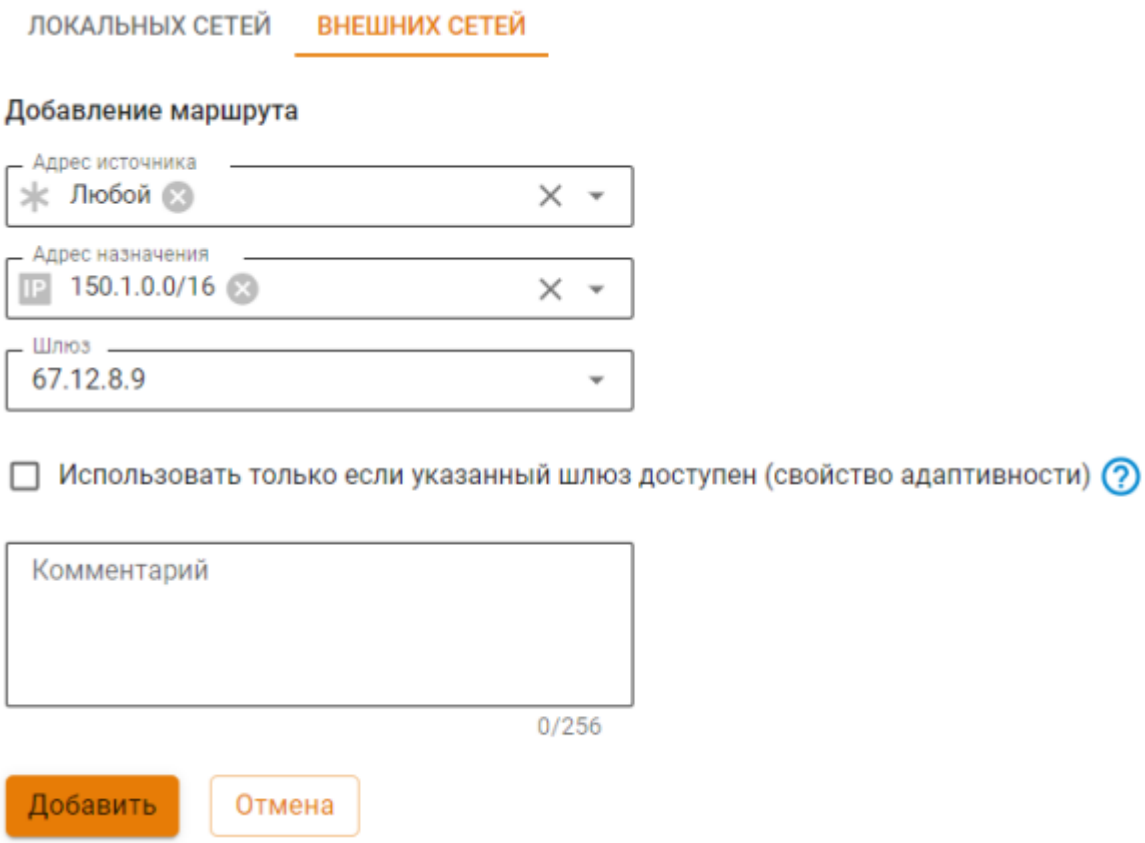
Задача: отбрасывать весь трафик до подсети `89.50.100.0/24`:

На вкладке **Маршрутизация локальных сетей** создайте правило Null route:

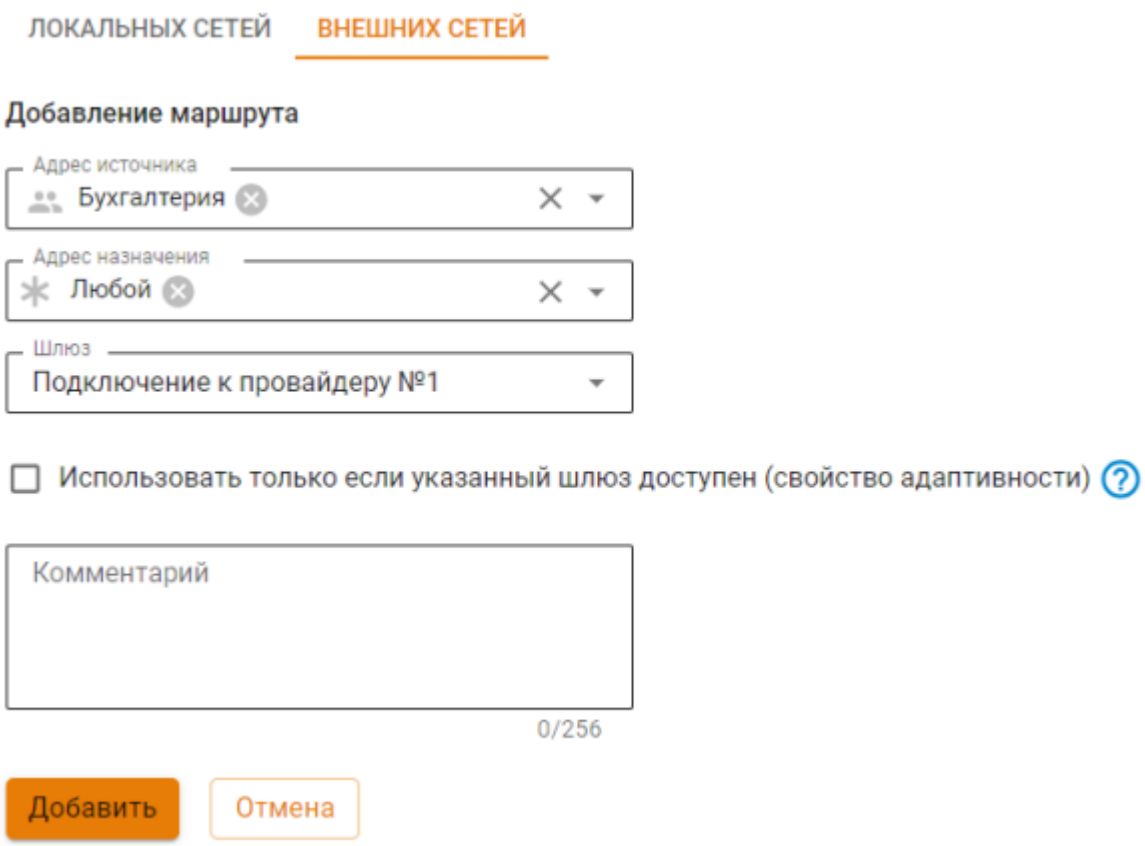


Укажите Loopback-интерфейс в качестве шлюза. В этом случае весь входящий на NGFW трафик, предназначенный для подсети `89.50.100.0/24`, будет отбрасываться.

Задача: любой трафик в подсеть `150.1.0.0/16` **направлять на шлюз** `67.12.8.9`**:**



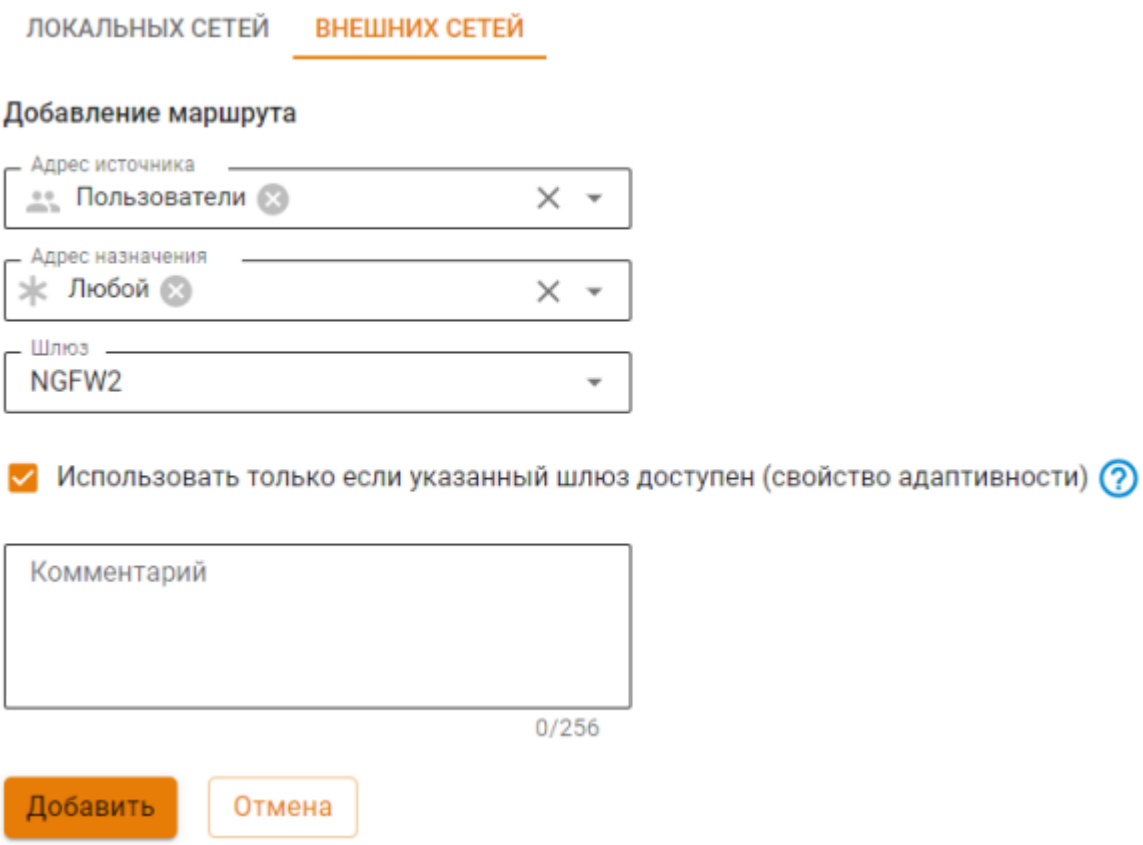
Задача: весь трафик пользователей из группы Бухгалтерия направить через шлюз выбранного сетевого интерфейса:



Если настраивается маршрут в удаленную сеть через дополнительный роутер, расположенный в одной локальной сети с клиентами, то убедитесь, что нет «асимметричной маршрутизации» и роутер вынесен в DMZ. Подробнее в статье *Доступ в удаленные сети через роутер в локальной сети*

Задача: предоставить доступ в интернет пользователям NGFW1, подключенного по IPsec к NGFW2, через внешний интерфейс NGFW2:

Для доступа в интернет пользователям NGFW1 укажите в качестве шлюза IPsec-подключение к NGFW2:



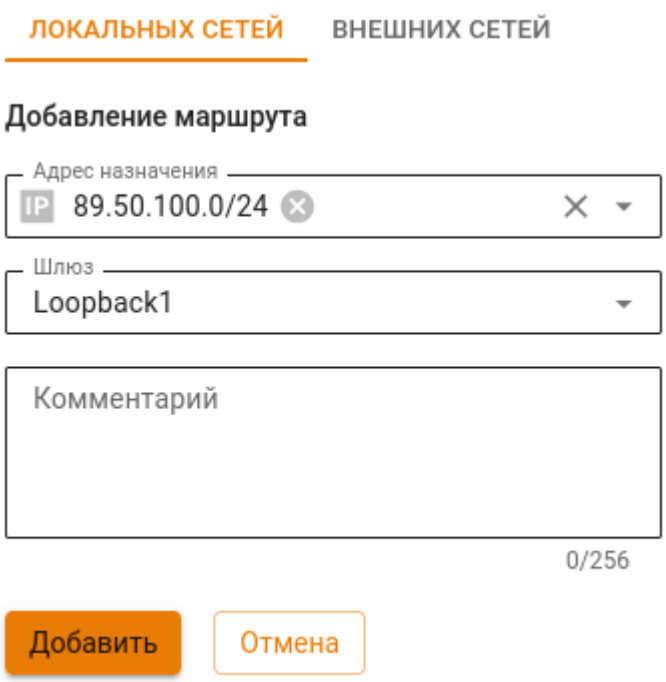
Задача: создать правило маршрутизации до сетей филиала через подключение client-to-site:

Если установка подключения site-to-site до сетей филиала недоступна, в Ideco NGFW можно настроить подключение роутера client-to-site. В этом случае при добавлении маршрута локальных сетей в качестве шлюза используется роутер, который подключается по VPN.

Для настройки подключения выполните действия:

1. В разделе **Пользователи -> Учетные записи** создайте учетную запись для роутера с разрешенным доступом к VPN.

2. При добавлении маршрута в разделе **Сервисы -> Маршрутизация -> Локальных сетей** выберите созданного пользователя в поле **Шлюз**:



Сети за роутером станут доступны после установки VPN-подключения через Ideco NGFW.

Информация об особенностях маршрутизации и организации доступа при настроенном VPN-подключении представлена в *статье*.

18.4 BGP

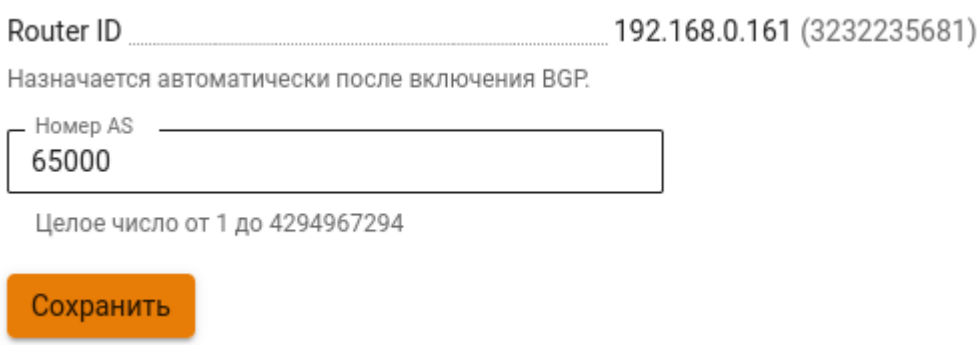
Подсказка: Название службы раздела **BGP**: `frr`; `ideco-routing-backend`.
Список служб для других разделов доступен по *ссылке*.

BGP (Border Gateway Protocol) — это основной протокол динамической маршрутизации, который используется в интернете.

Для запуска сервиса он должен быть не только включен, но и корректно настроен: должен быть указан номер автономной системы, а также создан и включен хотя бы один BGP-сосед.

18.4.1 Настройка своей автономной системы

1. Введите номер автономной системы в строку **Номер AS** и нажмите **Сохранить**:



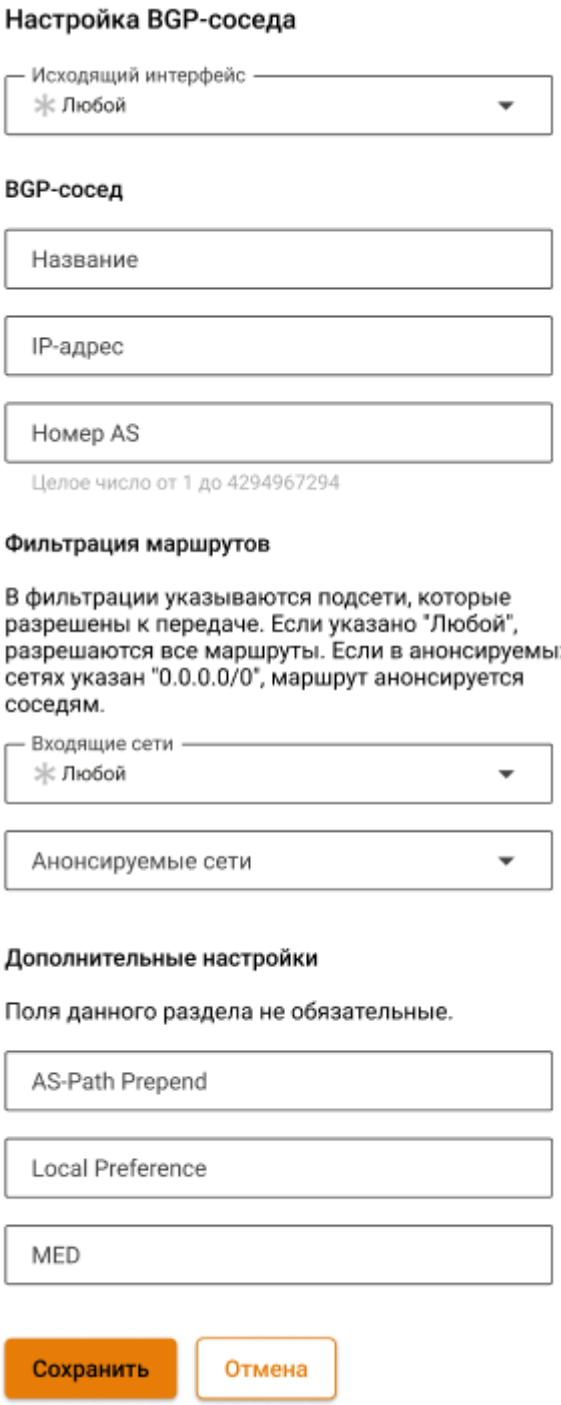
2. Переведите опцию раздела **BGP** в положение **включен**;

3. Ideco NGFW заполнит поле **Router ID** автоматически.

18.4.2 Настройка BGP-соседей

1. Для добавления BGP-соседа нажмите **Добавить** в правом верхнем углу;

2. Заполните поля:



- **Исходящий интерфейс** - интерфейс Ideco NGFW, IP-адрес которого будет использован для обмена маршрутами. Для надежности и стабильности работы службы рекомендуем выбрать *Loopback-интерфейс*. Если выбран **Любой**, будет использоваться ближайший к соседу интерфейс;

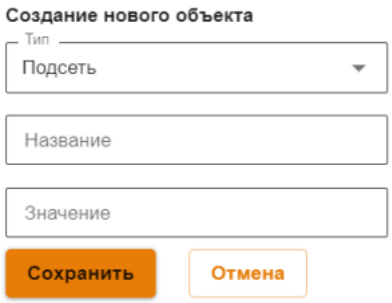
- **Название** - любое значение;
- **IP-адрес** - IP-адрес BGP-соседа. Рекомендуем указать адрес Loopback-интерфейса соседа;
- **Номер AS** - номер AS BGP-соседа;
- **Входящие сети** - сети, информацию от которых хотите получать. Если выбран объект **Любой**, то фильтрация будет отключена и будут приниматься все сети от BGP-соседа. Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру **0.0.0.0/0**;
- **Анонсируемые сети** - сети, информацию о которых хотите отправлять. Если выбран объект **Любой**, то фильтрация будет отключена и будет передаваться информация обо всех маршрутах, известных NGFW (redistribute static, connected, ospf). Предустановленный объект фильтров **Маршрут по умолчанию** соответствует фильтру **0.0.0.0/0**;
- **AS-Path Prepend** - чем больше значение, тем менее приоритетным становится канал;
- **Local Preference** - определяет приоритет пути для выхода трафика. Чем больше значение, тем более приоритетным становится канал;
- **MED** - определяет приоритет пути для входа трафика. Чем меньше значение, тем приоритетнее путь.

Подсказка: Для динамической маршрутизации сетей двух NGFW, соединенных по IPSec, воспользуйтесь BGP. Подробнее про настройку подключения двух NGFW по IPSec - в статье *Подключение по IPsec между двумя Ideco NGFW*

Для **Входящих сетей** и **Анонсируемых сетей** объект **Любой** не может быть установлен одновременно с другими фильтрами.

Подсказка: На Ideco NGFW по умолчанию включен **BGP Multipath**. Этот механизм позволяет устанавливать несколько путей BGP к одному месту назначения в таблице IP-маршрутизации. BGP Multipath не влияет на процесс выбора лучшего пути.

Если нужного объекта для фильтрации нет, то создать его можно, выбрав **Создать новый объект** в поле **Входящие сети** или **Анонсируемые сети**:



- **Название** - любое значение;
- **Значение** - значение подсети в формате: `подсеть/маска подсети`, например, `192.168.100.0/24`.

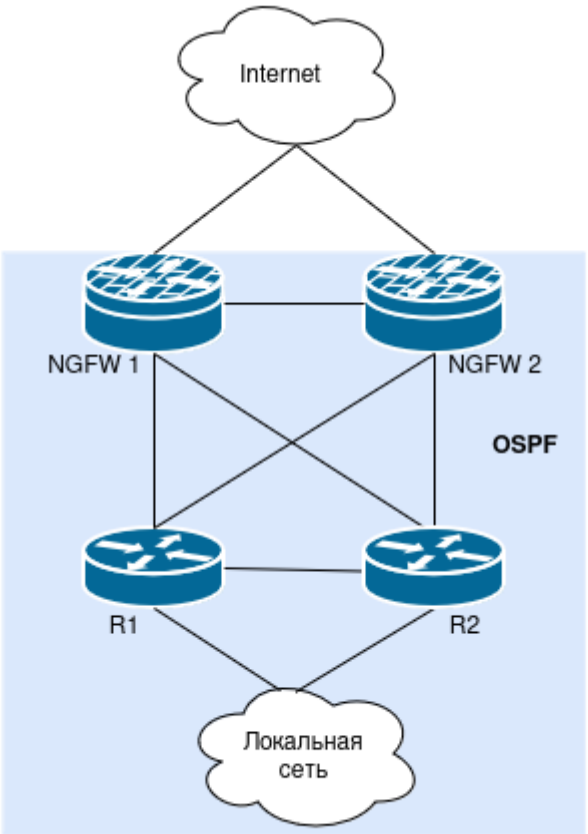
18.5 OSPF

Подсказка: Название службы раздела **OSPF**: `frr; ideco-routing-backend`.
Список служб для других разделов доступен по *ссылке*.

В Ideco NGFW реализована поддержка OSPF (Open Shortest Path First) - протокола маршрутизации по состоянию каналов. Канал - это интерфейс маршрутизатора или сегмент сети, который соединяет два маршрутизатора.

Использовать модуль лучше всего в сетях, где применяется балансировка нагрузки на сеть и резервирование каналов.

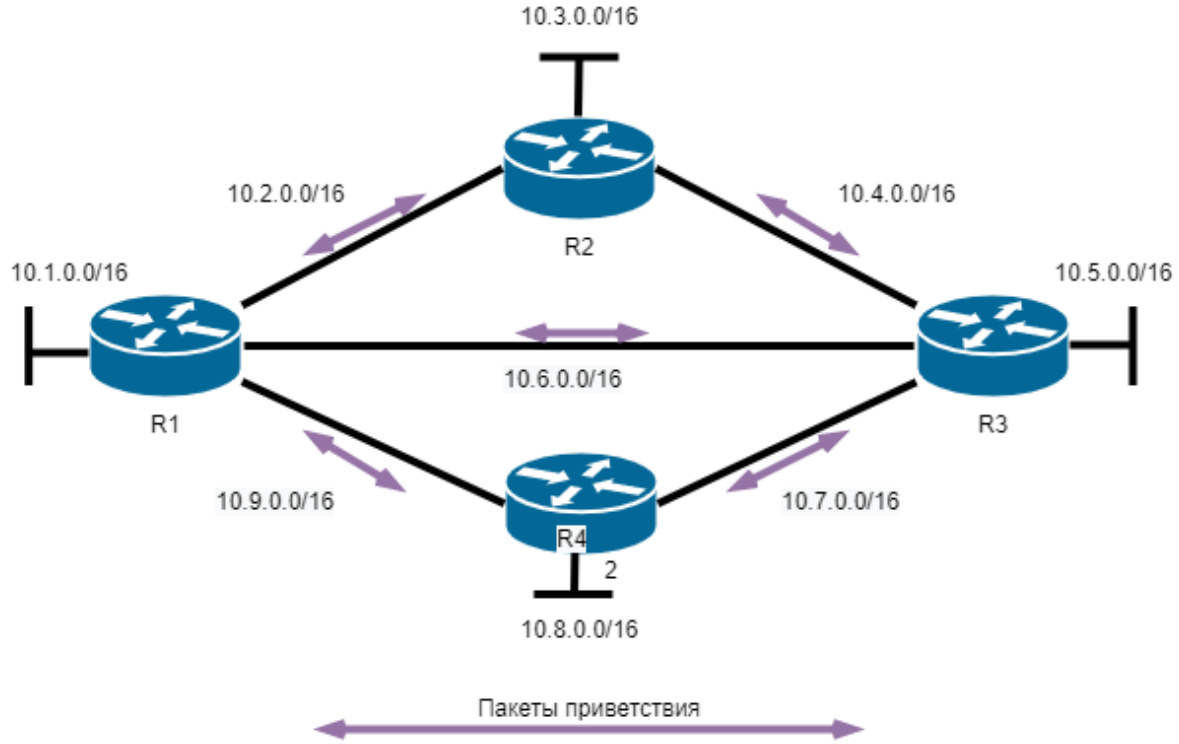
Пример топологии с использованием OSPF представлен на схеме ниже:



Принцип работы маршрутизации по состоянию канала:

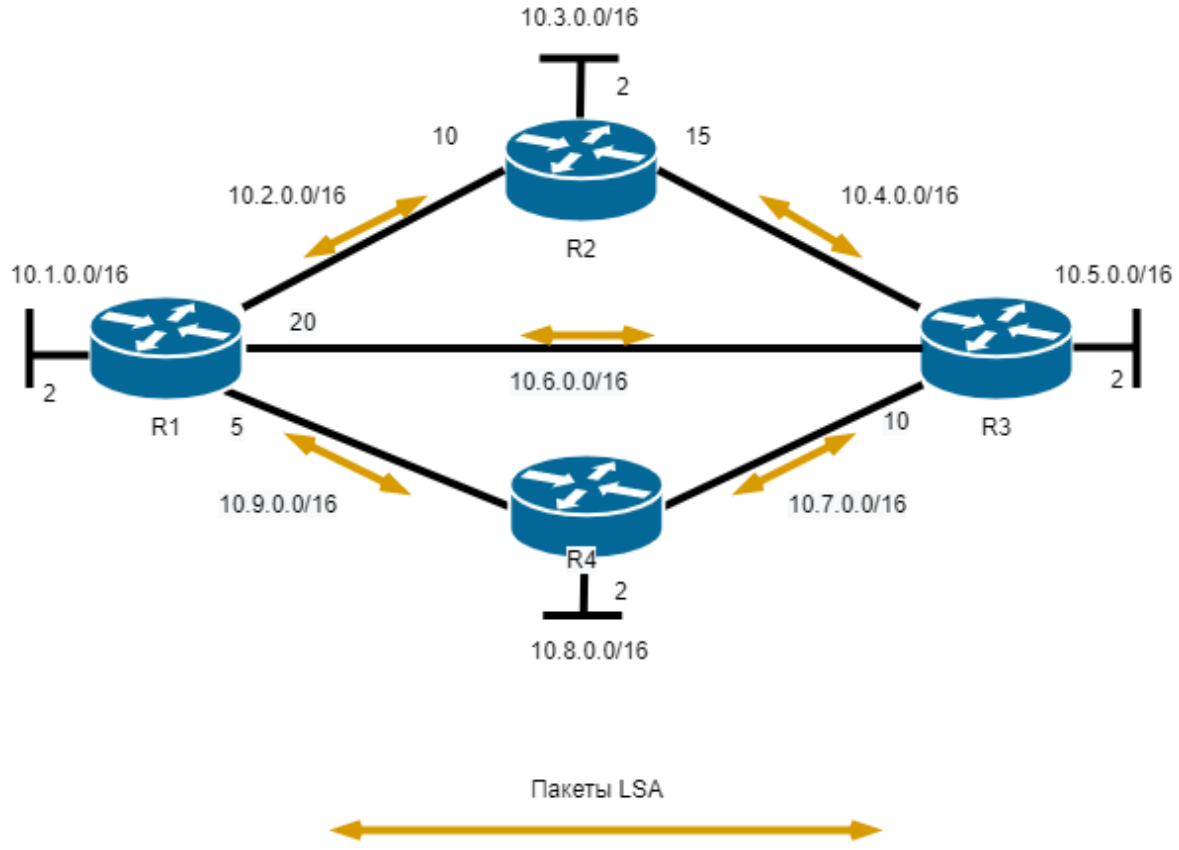
1. Установление отношений смежности с соседними устройствами

Маршрутизатор, использующий OSPF, отправляет hello-пакеты на мультикастовый адрес 224.0.0.5 со всех интерфейсов, где запущен OSPF. При наличии соседнего устройства маршрутизатор пытается установить с ним отношения смежности.



2. Обмен объявлениями о состоянии каналов

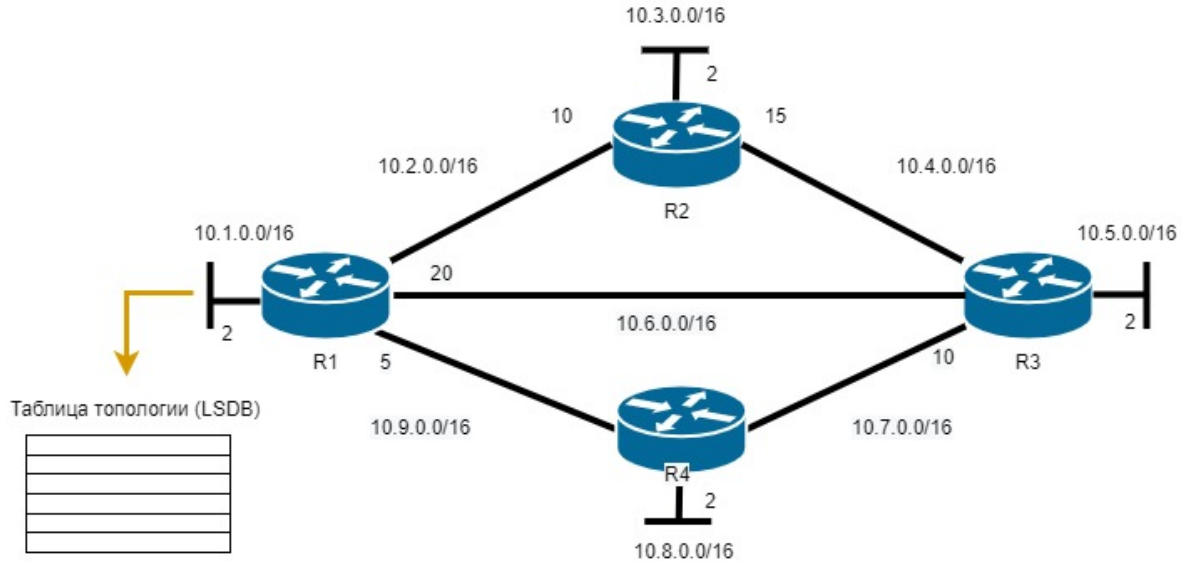
После установления смежности устройства выполняют обмен LSA. LSA содержат информацию о состоянии и стоимости каждого канала с прямым подключением.



3. Создание базы данных состояния связи

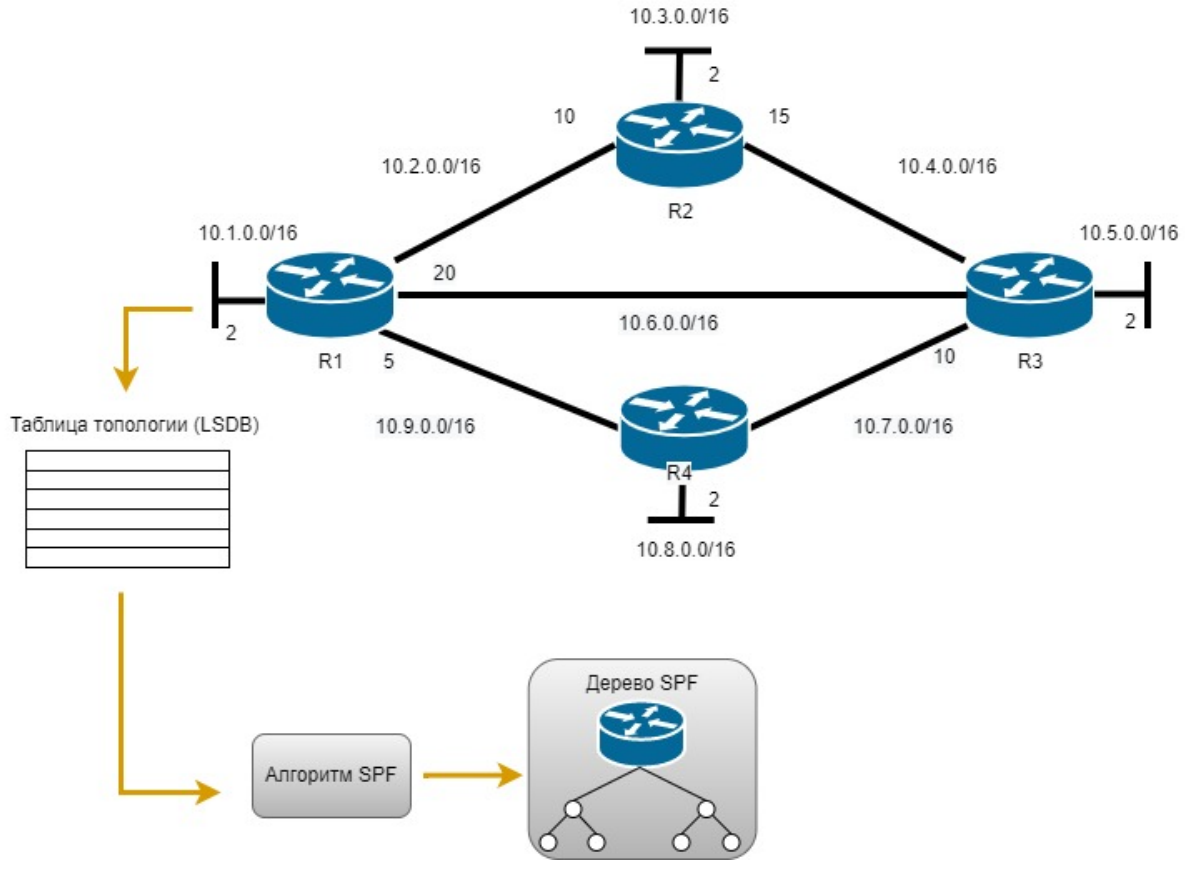
На основе объявления LSA маршрутизаторы собирают базу данных, в которой содержатся данные о топо-

логии сети в области.



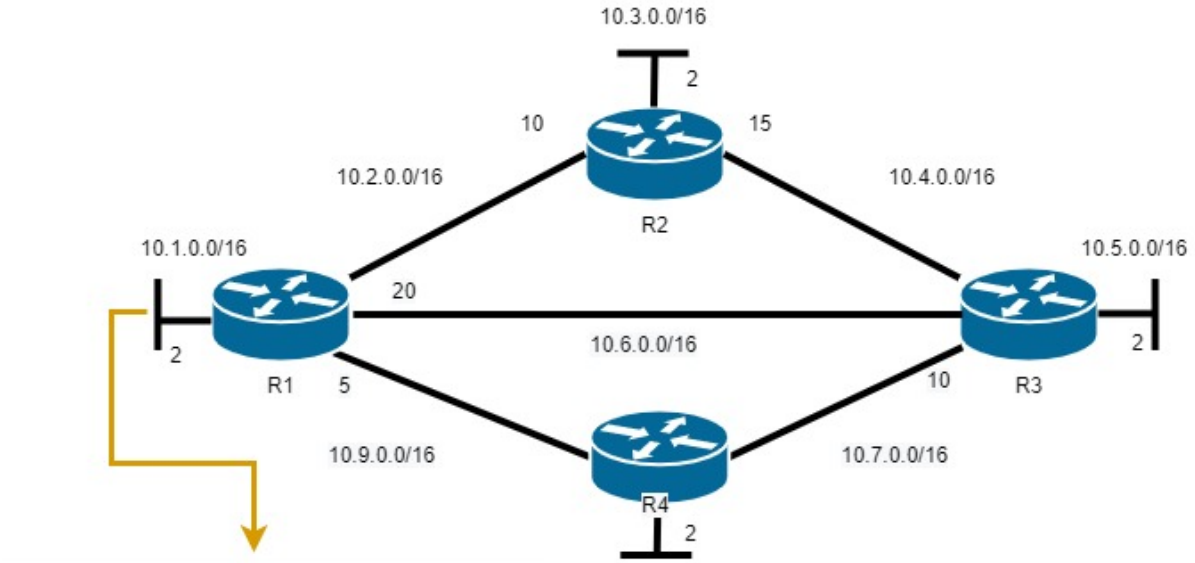
4. Исполнение алгоритма SPF

На устройствах выполняется алгоритм SPF, результатом которого является создание дерева кратчайших путей.



5. Выбор лучшего маршрута

На основании данных дерева SPF обновляются данные в таблице IP-маршрутизации. Маршрут добавляется в таблицу маршрутизации, если отсутствует источник маршрута к той же сети с меньшим административным расстоянием, например, статический маршрут.
Решения по маршрутизации пакетов принимаются на основе записей в таблице маршрутизации.



Название	Кратчайший путь	Стоимость
10.3.0.0/16	R1 -> R2	12
10.4.0.0/16	R1 -> R2	25
10.5.0.0/16	R1 -> R3	22
10.7.0.0/16	R1 -> R4	17
10.8.0.0/16	R1 -> R4	7

18.5.1 Особенности работы OSPF в Ideco NGFW

- Ideco NGFW всегда будет являться шлюзом по умолчанию для других устройств. Считать другие устройства шлюзом по умолчанию NGFW не сможет;
- OSPF работает только на локальных интерфейсах. Локальными считаются локальные *Ethernet-интерфейсы*, *GRE*;
- Значение *Типа сети* (*Network Type*) в Ideco NGFW устанавливается автоматически в зависимости от типа интерфейса, используемого для OSPF: для GRE-интерфейсов - значение p2p, для Ethernet-интерфейсов - значение broadcast.

18.5.2 Основное

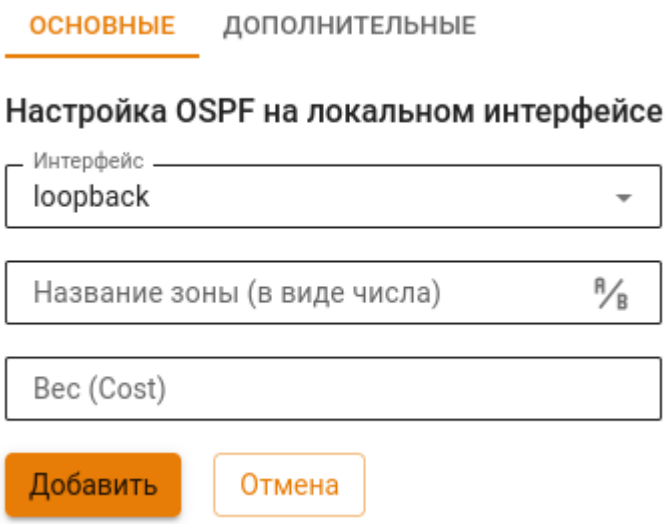
Настройка Ideco NGFW

Router ID - IP-адрес маршрутизатора. Присваивается автоматически в виде самого большого IP-адреса локальной сети, заданной в разделе *Сетевые интерфейсы*.

Для того чтобы настроить OSPF на NGFW, выполните действия:

1. В веб-интерфейсе NGFW перейдите в раздел **Сервисы –> OSPF –> Основные** и нажмите кнопку **Добавить**.

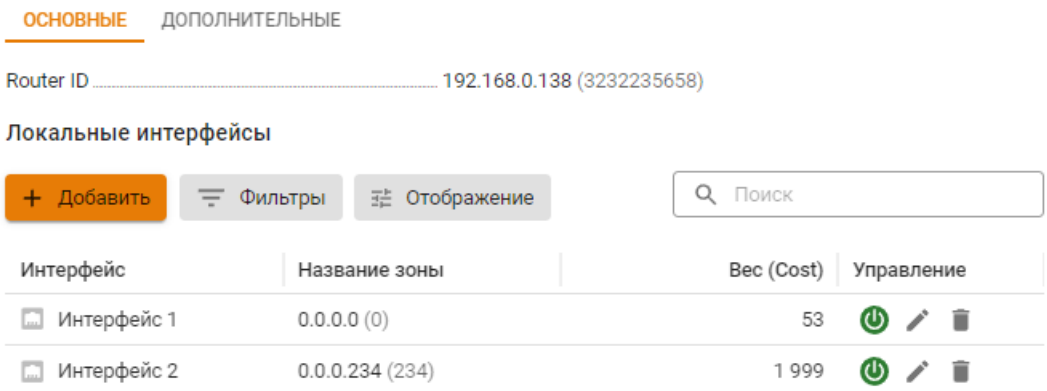
2. Заполните поля:



- **Интерфейс** - выберите локальный или *Loopback-интерфейс* Ideco NGFW, IP-адрес которого будет использован для обмена маршрутами;
- **Название зоны** - введите номер зоны (значение `area`, для небольших сетей введите 0). Можно ввести в виде числа или IP-адреса, нажав иконку A/B ;
- **Вес** - введите стоимость маршрута.

3. Нажмите **Добавить.**

Пример готовой таблицы:



При наличии большого количества настроек OSPF в таблице воспользуйтесь кнопкой **Фильтры**.

Настройка MikroTik:

1. Авторизуйтесь на MikroTik и выполните команду:

```
routing ospf area add area-id=x.x.x.x default-cost=1 disabled=no inject-summary-lsa=no
name=area1 type=default
```

- `x.x.x.x` - **название зоны, которое указали при настройке Ideco NGFW**. ID должен быть уникален для каждого роутера;

2. Для передачи любых других сетей соседним устройствам по динамической маршрутизации введите команду:

```
routing ospf network add network=(другая подсеть)/24 area=area1
```

3. Повторите команду из п. 1 для добавления каждой подсети;

4. Для вывода таблицы маршрутизации введите команду:

`ip route print`

Настройка Cisco:

1. Настройте локальный интерфейс Cisco:

```
enable
conf t
interface GigabitEthernet0/1
ip address <локальный IP Cisco> <маска подсети>
no shutdown
exit
```

2. Настройте внешний интерфейс Cisco:

```
enable
conf t
interface GigabitEthernet0/0
ip address <внешний IP Cisco> <маска подсети>
no shutdown
exit
```

3. Проверьте наличие связи между Ideco NGFW и Cisco. Для этого в консоли Cisco используйте команду `ping <внешний IP NGFW>`. Результат вывода команды - наличие ICMP-ответов.

4. Сохраните настройки конфигурации:

```
write memory
```

5. Запустите на Cisco процесс OSPF:

```
enable
conf t
router ospf 1
```

6. По умолчанию отключите отправку hello-пакетов на всех интерфейсах и включите на нужных интерфейсах:

```
passive-interface default
no passive-interface GigabitEthernet0/0
```

- `GigabitEthernet0/0` - название интерфейса.

7. Укажите сети, маршруты до которых хотите анонсировать:

```
network <IP-адрес подсети> <wildcart-маска подсети> area <номер зоны, указанный при␣
↪настройке Ideco NGFW>
```

Пример команды:

```
network 192.168.100.0 0.0.255.255 area 0
```

8. Если Cisco получил уведомление вида `*Dec 18 10:02:03.628: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.122.73 on GigabitEthernet0/0 from LOADING to FULL, Loading Done`, соседские отношения установлены.

9. Для просмотра списка соседей воспользуйтесь командой `show ip ospf neighbor`:

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.122.73    1   FULL/DR         00:00:38    192.168.102.11  GigabitEthernet0/0
Router#
```

10. Для вывода таблицы маршрутизации введите команду `show ip route` (в таблице должны появиться маршруты до сетей NGFW):

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.102.11 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      10.0.0.0/16 is subnetted, 1 subnets
O E2     10.128.0.0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.100.0/32 is subnetted, 1 subnets
O E2     192.168.100.100
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.102.0/24 is directly connected, GigabitEthernet0/0
L        192.168.102.79/32 is directly connected, GigabitEthernet0/0
      192.168.103.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.103.0/24 is directly connected, GigabitEthernet0/1
L        192.168.103.130/32 is directly connected, GigabitEthernet0/1
O E2  192.168.122.0/24
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
```

18.5.3 Дополнительное

На вкладке доступны к установке следующие флаги:

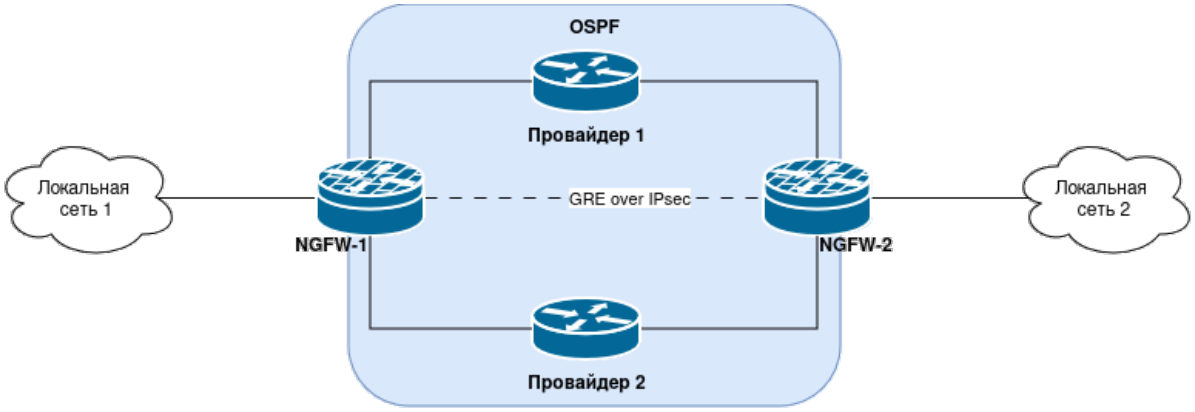
- **Redistribute default** - будут анонсироваться маршруты по умолчанию. Устройство, принявшее эту информацию, будет отправлять на NGFW весь трафик;
- **Redistribute static** - будут анонсироваться статические маршруты, указанные на вкладке **Сервисы -> Маршрутизация -> Локальных сетей**;
- **Redistribute connected** - будут анонсироваться маршруты подсетей, подключенных напрямую, в том числе и *Loopback-интерфейсов*. Если настройку отключить, сети Loopback-интерфейсов будут анонсироваться при добавлении в конфигурацию OSPF Loopback-интерфейса.

Подробнее о значении поля **Метрика** - в статье.

Подсказка: Для передачи маршрутов до VPN-сети через OSPF необходимо в разделе **OSPF -> Дополнительные** включить чек-бокс **Redistribute static (передача статических маршрутов)**.

18.5.4 Примеры использования

1. Объединение филиальной сети с резервированием и/или балансировкой

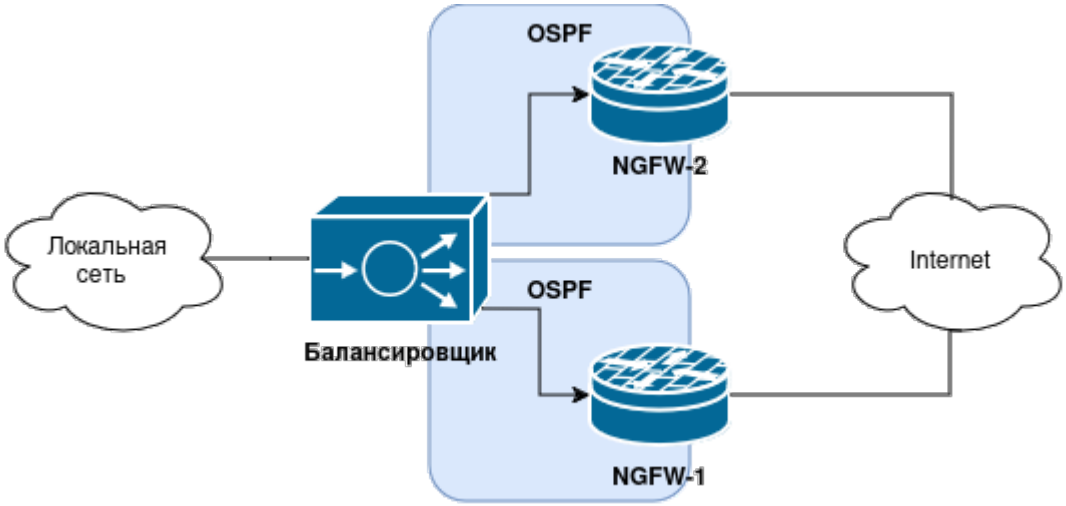


- Между **NGFW-1** в Филиале 1 и **NGFW-2** в Филиале 2 настраивается GRE-over-IPsec и OSPF;
- Каждый NGFW подключен к двум провайдерам (**Провайдер-1** и **Провайдер-2**).

Преимущества настройки:

- Трафик будет автоматически балансироваться между **Провайдером-1** и **Провайдером-2**;
- При неисправности одного из провайдеров трафик автоматически смаршрутизируется через другое соединение;
- Отсутствует необходимость вручную настраивать маршруты до локальных сетей филиалов.

2. Схема с балансировкой доступа из локальной сети в интернет или другую сеть



- И **NGFW-1**, и **NGFW-2** используются в качестве шлюза по умолчанию;
- Между балансировщиком и каждым из NGFW настроена OSPF.

Преимущества настройки:

- Трафик балансируется между **NGFW-1** и **NGFW-2**: часть пользователей из Локальной сети выходят в интернет через **NGFW-1**, часть - через **NGFW-2**;

- При неисправности одного из NGFW трафик автоматически смаршрутизируется через другое соединение;
- Отсутствует необходимость вручную настраивать маршруты для хостов в Локальной сети.

18.6 IGMP Proxy

Подсказка: Название службы раздела **IGMP Proxy**: `ideco-igmpproxy-backend`, `ideco-igmpproxy`. Список служб для других разделов доступен по *ссылке*.

Подсказка: IGMP Proxy работает только с Ethernet-интерфейсами и не работает на интерфейсах VLAN, PPPoE или VPN (L2TP, PPTP).

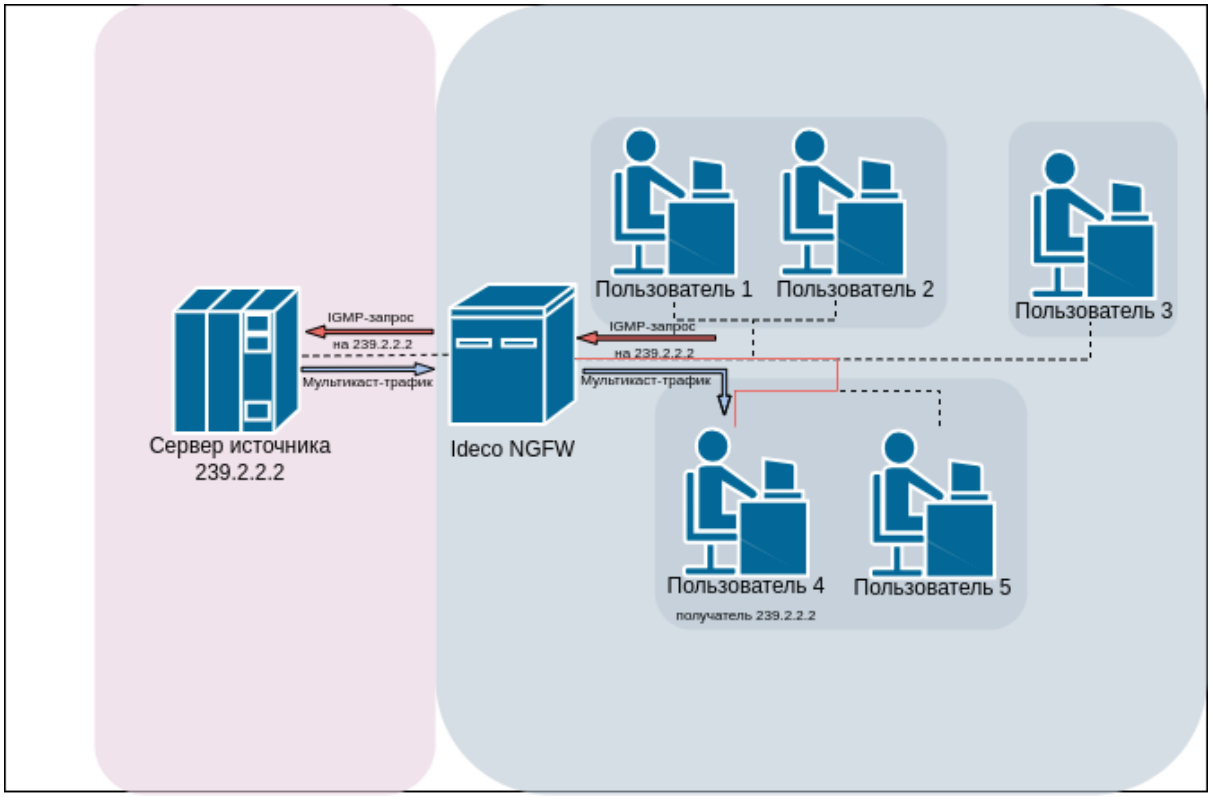
IGMP Proxy - служба, которая проксирует (передает) мультакаст-трафик сквозь роутер. Это сокращает объем трафика, что влияет на скорость работы и нагрузку сети.

18.6.1 Принцип работы

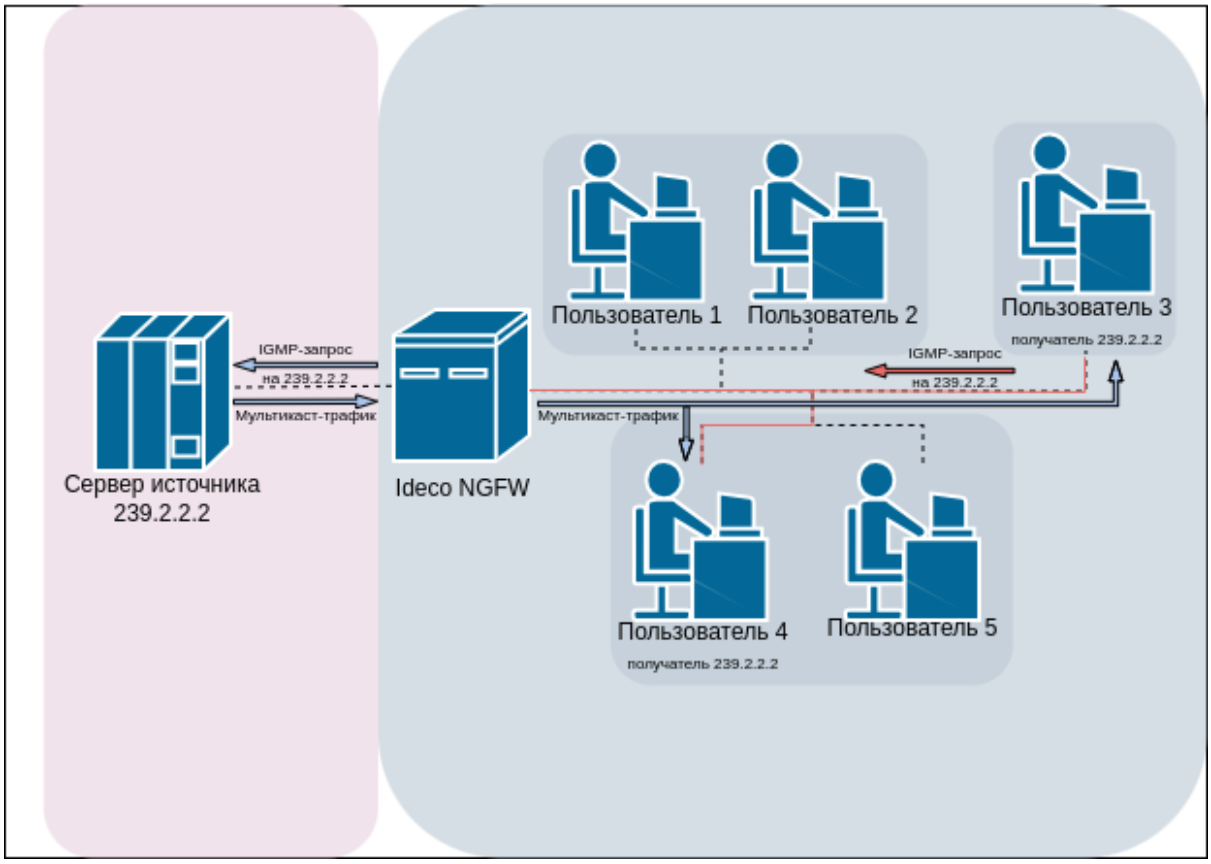
Со стороны клиентов IGMP Proxy поддерживает версии IGMPv1 и IGMPv2.

Принцип работы на примере подключения двух пользователей к мультикаст-потоку одного источника:

- *Сервер источника* начинает трансляцию мультикаст-трафика с адреса из диапазона 224.0.0.0/4.
- *Пользователь 4* хочет подключиться к трафику и генерирует IGMP-запрос (Join) на *Ideco NGFW* для получения мультикаст-трафика от сервера источника.
- *Ideco NGFW* получает IGMP-запрос и отправляет аналогичный запрос к серверу источника;
- Сервер источника получает запрос и начинает транслировать мультикаст-трафик на *Ideco NGFW*;
- *Ideco NGFW* пропускает трафик с адреса 239.2.2.2 в подсеть с *Пользователем 4*, и *Пользователь 4* становится его получателем.



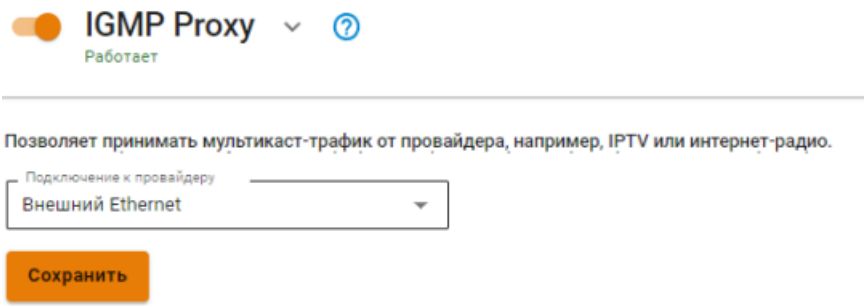
- *Пользователь 3*, находящийся в другой подсети, также решает подключиться к этой трансляции и генерирует IGMP-запрос (Join) на Ideco NGFW;
- *Ideco NGFW* получает этот запрос и дублирует *Пользователю 3* трафик, поступающий *Пользователю 4*;



Ideco NGFW периодически проверяет, есть ли получатели, отправляя пользователям IGMP-запрос (Query). Пользователи в ответ отправляют Join, как при подключении.
Если на Ideco NGFW приходит хотя бы один Join, то мультикаст-трафик продолжает транслироваться получателям.

18.6.2 Настройка в Ideco NGFW

Для настройки перейдите в раздел **Сервисы -> IGMP Proxy**. Переведите опцию **IGMP Proxy** в положение **Включен**. В строке **Подключение к провайдеру** выберите Ethernet-подключение.



18.7 Прокси

Подсказка: Название службы раздела **Прокси**: `ideco-proxy-backend`; `squid`.
Список служб для других разделов доступен по *ссылке*.

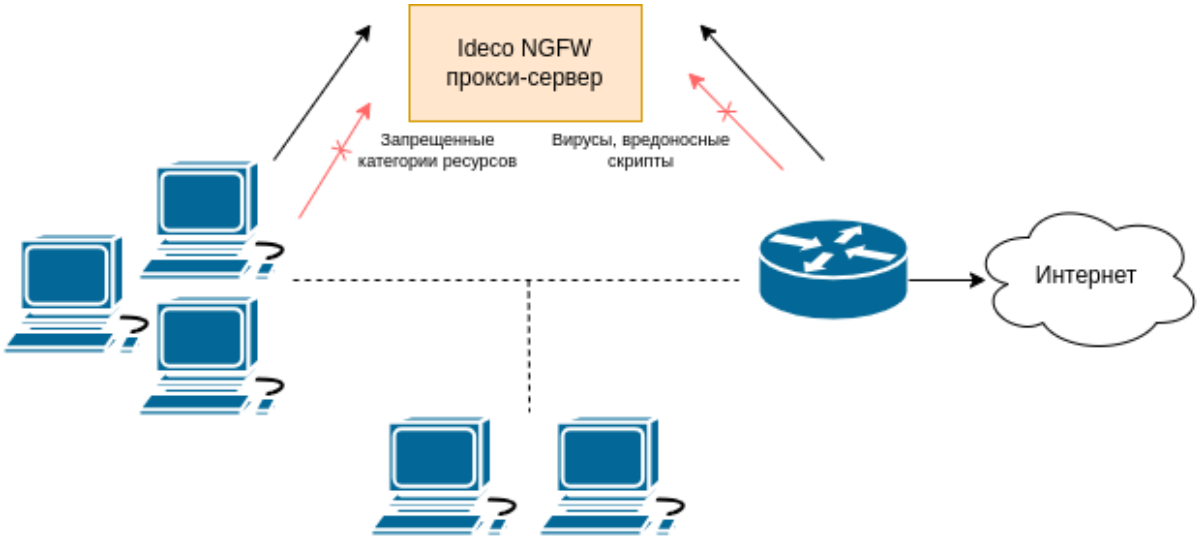
Прокси-сервер, помимо проксирования веб-трафика, используется для передачи трафика сервисам:

- Антивирус для веб-трафика (Антивирус Касперского);
- Сервис отчетности по веб-трафику пользователей;
- Контент-фильтр.

Порядок обработки веб-трафика подробнее описан в *статье*.

Подсказка: Не указывайте на хостах локальной сети настройки прокси. Достаточно указания NGFW в качестве шлюза по умолчанию для устройств в сети.

Для настройки фильтрации HTTPS-трафика нужно добавить корневой сертификат NGFW на компьютеры пользователей. Подробнее в статье *Настройка фильтрации HTTPS*.



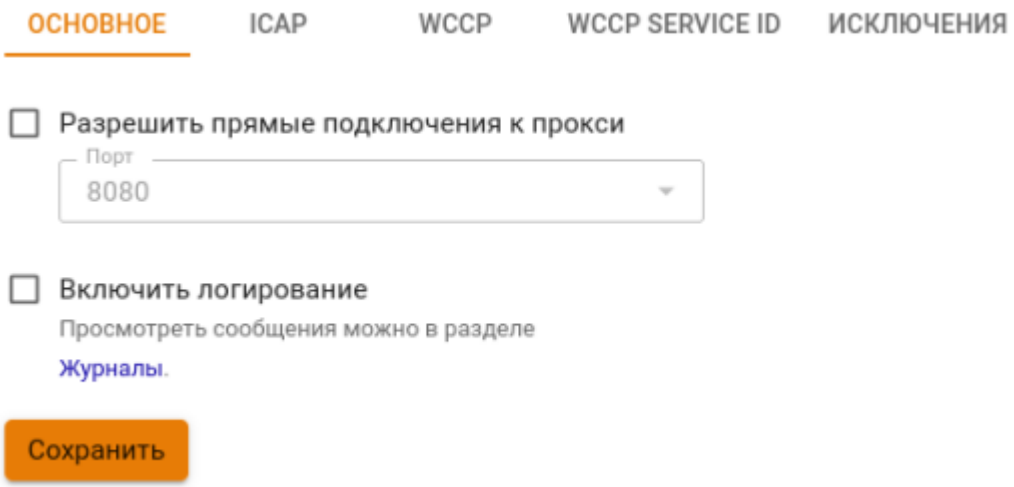
При использовании Ideco NGFW в качестве прокси-сервера с прямыми подключениями к прокси большинство функций будет работать с некоторыми особенностями:

- В правилах **Файрвола** для пользователей необходимо указывать цепочки INPUT вместо FORWARD;
- Глубокий анализ трафика системой предотвращения вторжений и модулем контроля приложений будет осуществляться только для трафика, проходящего через прокси-сервер (часть правил работать не будет);
- Исключения из прокси-сервера необходимо делать средствами браузера или правилами маршрутизации на конечных устройствах. Настройки в разделе **Сервисы -> Прокси -> Исключения** применяются только для прозрачного режима работы прокси-сервера.

18.7.1 Основное

На вкладке **Основное** предоставлены возможности:

- **Разрешить прямые подключения к прокси**
  Этот режим применяется, когда Ideco NGFW не является шлюзом по умолчанию для клиентов сети. Порт, указанный на стороне NGFW, следует указать на сетевых устройствах локальной сети, веб-трафик которых нужно пропускать через прокси.
- **Включить журналирование**
  Включает запись логов Контент-фильтра и Антивирусов веб-трафика.



О настройке прямого подключения к прокси и прокси с одним интерфейсом читайте в *статье*.

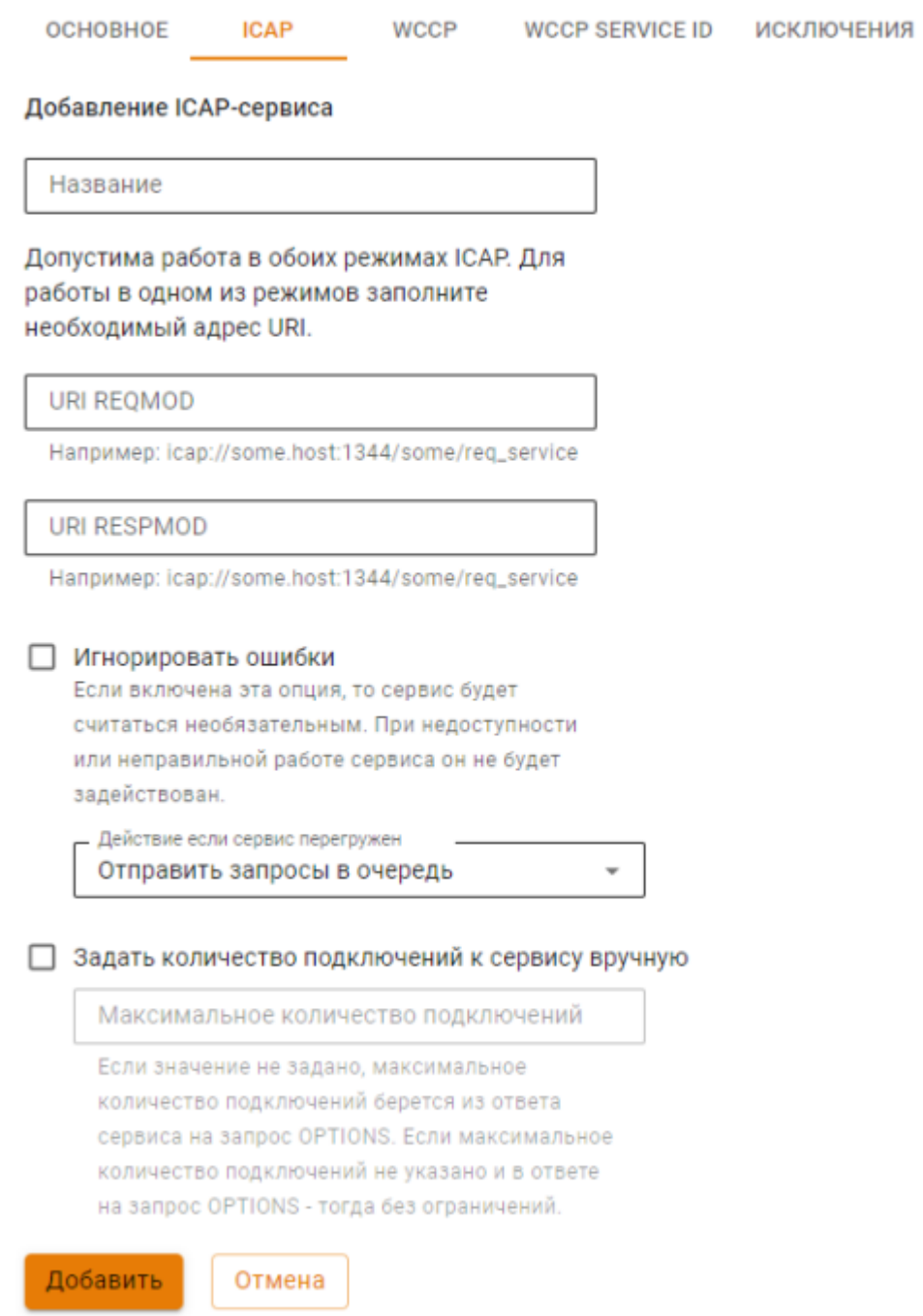
18.7.2 ICAP

Протокол ICAP используется для отправки HTTP(S)-трафика в расшифрованном виде сторонним серверам. ICAP-сервисы будут обрабатывать трафик после антивирусов и контент-фильтра.

При добавлении ICAP-сервиса доступны следующие настройки:

- **Игнорировать ошибки** - если включена эта опция, то сервис будет считаться необязательным. При недоступности или неправильной работе сервиса он не будет задействован.
- **Задать количество подключений к сервису вручную** - если значение не задано, максимальное количество подключений берется из ответа сервиса на запрос OPTIONS. Если максимальное количество подключений не указано в ответе на запрос OPTIONS, тогда - без ограничений.

Предупреждение: Если указать в опции **Задать количество подключений к сервису вручную** значение меньше четырех, то клиентские подключения могут быть нестабильными.



Подсказка: Для корректной работы ICAP-сервиса должна быть настроена расшифровка HTTPS-трафика в **Контент-фильтре**.

18.7.3 WCCP

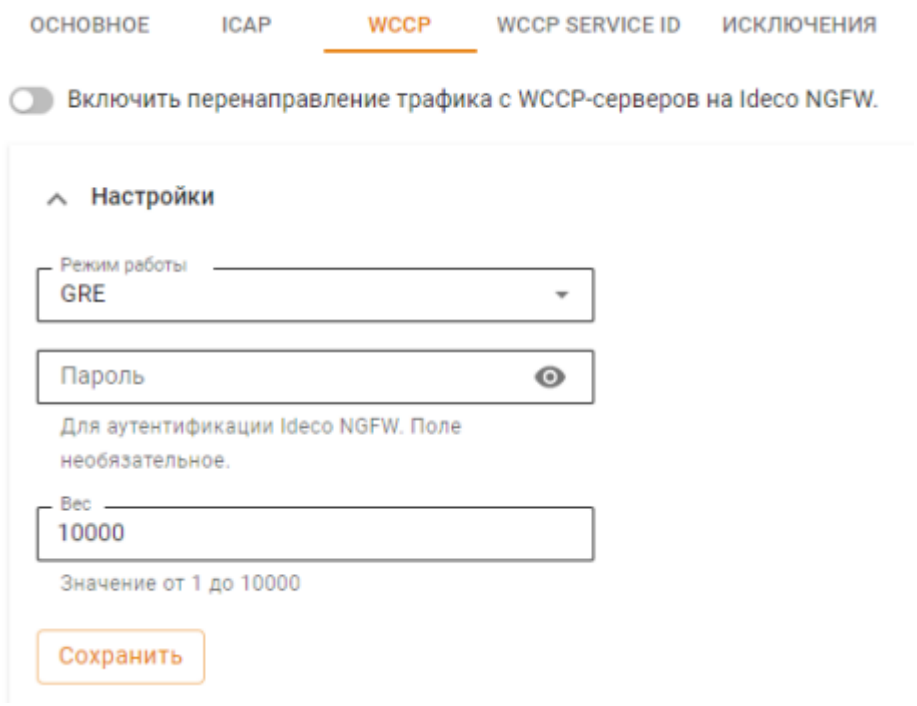
Протокол WCCP используется для перенаправления трафика на Ideco NGFW.

По умолчанию перенаправляется только HTTP/HTTPS-трафик.

Для активации WCCP переведите опцию **Включить перенаправление трафика с WCCP-серверов на Ideco NGFW** в положение **Включен**. Ideco NGFW запустит процесс согласования параметров с WCCP-сервером.

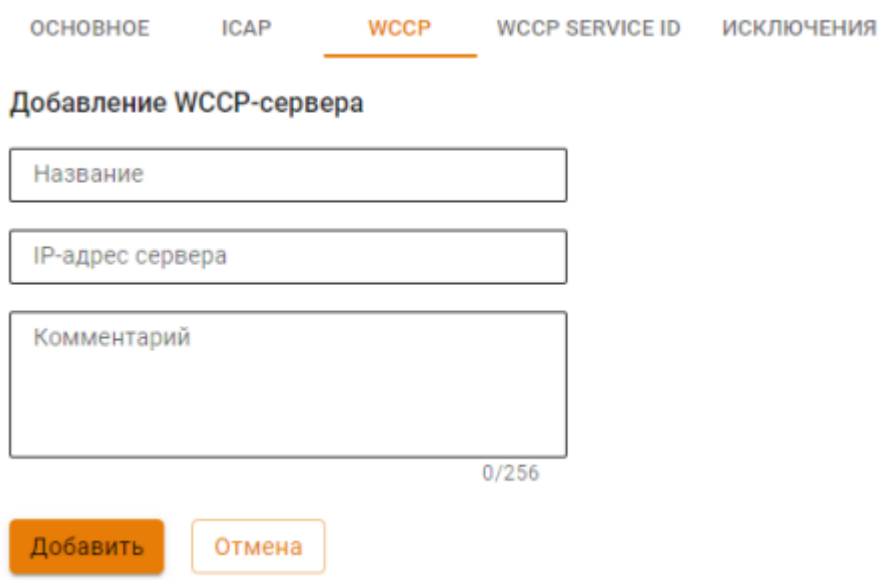
В NGFW предусмотрено два режима работы WCCP - L2 и GRE. Для выбора режима раскройте блок **Настройки**. Для работы WCCP в GRE-режиме необходимо также создать на Ideco NGFW *GRE-интерфейс*, указав в поле **Адрес удаленного интерфейса** IP-адрес WCCP-сервера.

Если на WCCP-сервере задан пароль, сохраните его в соответствующем поле:



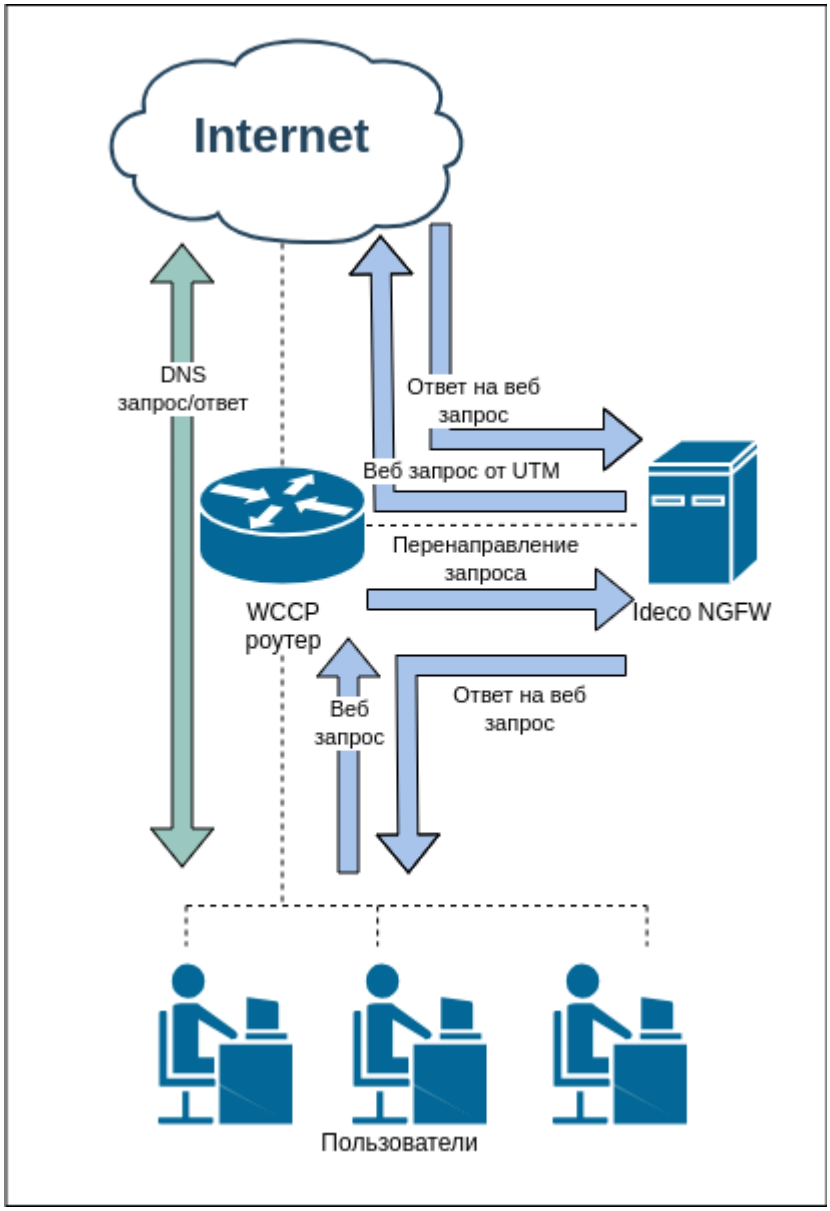
Если роутер использует несколько Ideco NGFW, настройте распределение трафика с помощью указания приоритета в поле **Вес**. Допустимые значения - от 1 до 10000.

Для добавления WCCP-сервера нажмите кнопку **Добавить** и укажите IP-адрес сервера:



L2:

Режим L2 используется, если роутер и Ideco NGFW находятся в одном сетевом сегменте.



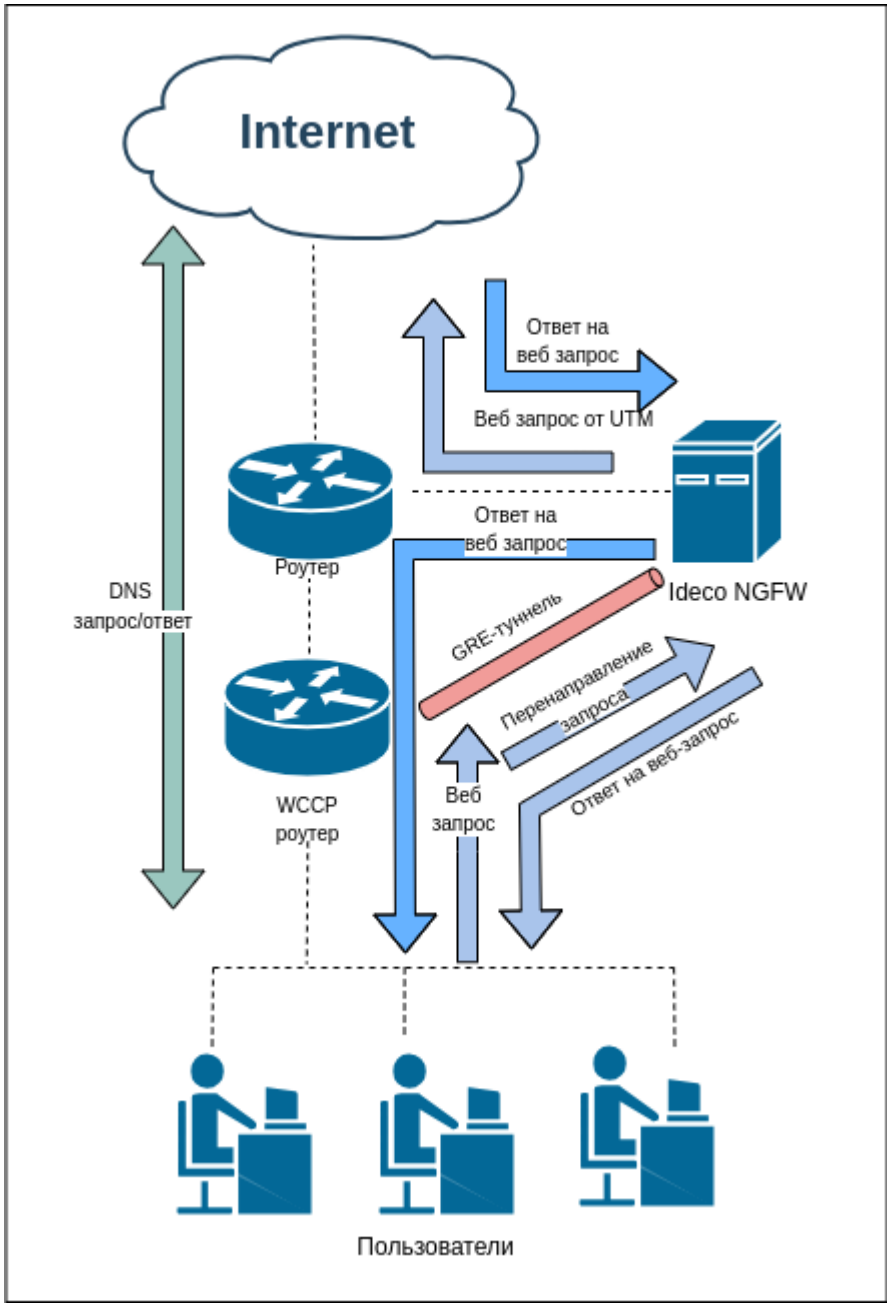
Последовательность обработки веб-запросов на уровне L2:

- Пользователь отправляет веб-запрос;
- Запрос перенаправляется роутером на Ideco NGFW;
- Ideco NGFW обрабатывает запрос;
- Если запрос заблокирован, информация о блокировке отправляется обратно пользователю;
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается обратно по тому же пути, по которому уходил на внешний сервер.

GRE:

Режим GRE используется, если роутер и Ideco NGFW находятся в разных сетевых сегментах.



Последовательность обработки веб-запросов на уровне GRE:

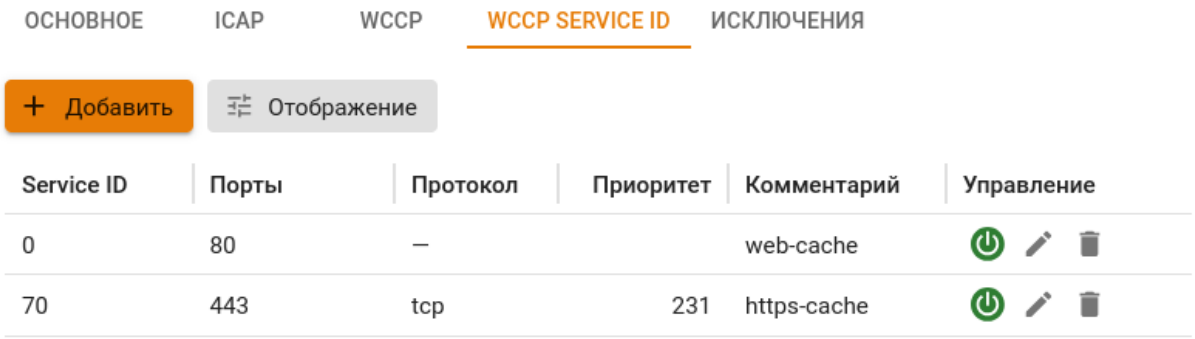
- Пользователь отправляет веб-запрос;
- Запрос перенаправляется по GRE-туннелю на Ideco NGFW;
- Ideco NGFW обрабатывает запрос.
- Если запрос заблокирован, то информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается напрямую от Ideco NGFW пользователю, минуя GRE-туннель.

18.7.4 WCCP Service ID

Service ID - идентификаторы сервисной группы. Настройки на этой вкладке позволяют выбрать службы, трафик которых маршрутизатор WCCP будет перенаправлять на Ideco NGFW.

По умолчанию настроены сервисы для HTTP/HTTPS-трафика:



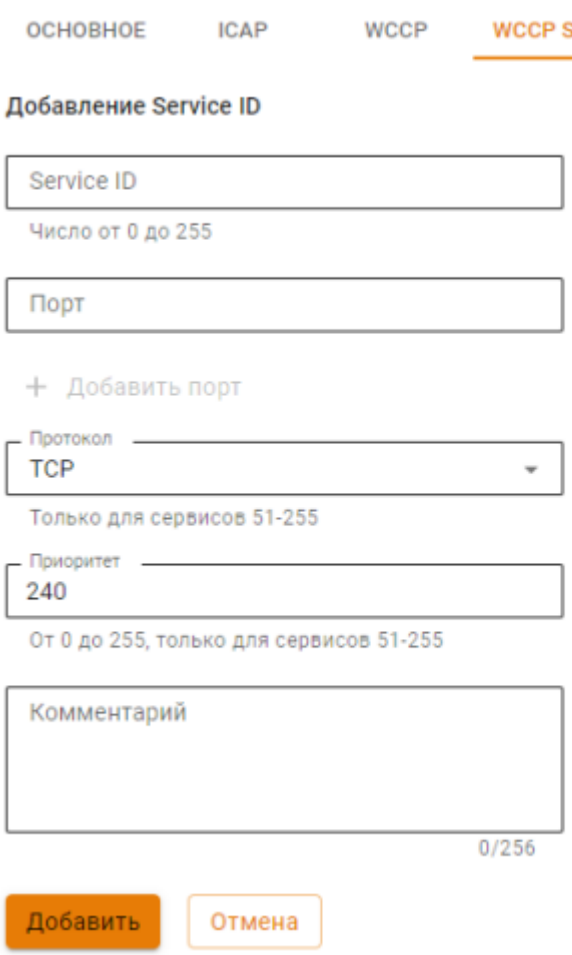
Предупреждение: Service ID с 0 по 50 зарезервированы под фиксированные сервисы. Для них выбирать порты и протоколы нельзя.

Service ID 70 - общепринятое значение для HTTPS-трафика на 443 TCP-порт.

Чтобы настроить Service ID, выполните действия:

1. На вкладке **WCCP Service ID** нажмите кнопку **Добавить**.

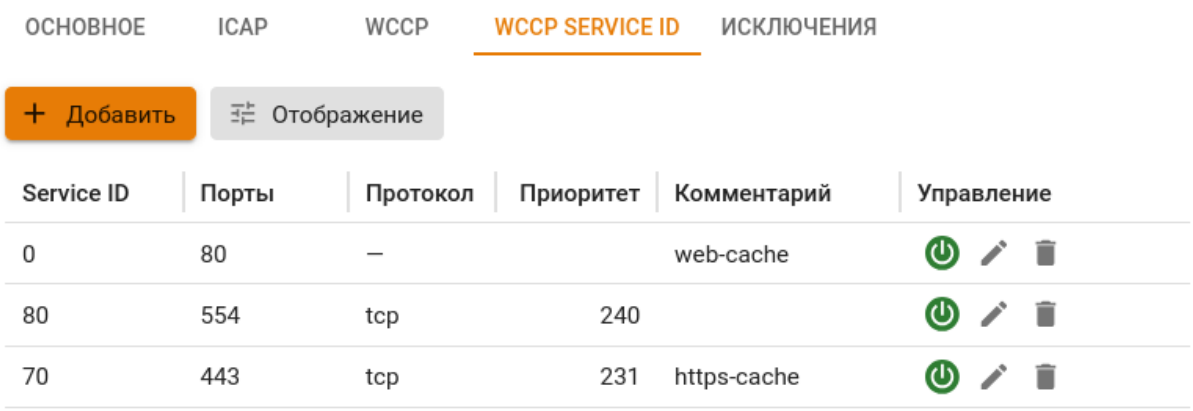
2. В открывшейся форме укажите следующие значения:



- **Service ID** - идентификатор сервисной группы, трафик которой планируется перенаправлять на прокси-сервер. Выбирайте значения от 51 до 255, чтобы избежать проблем со старыми маршрутизаторами WCCP.
- **Порты** - укажите порты назначения. Максимум 8 значений.
- **Протокол** - укажите протокол для перенаправляемого трафика (TCP, UDP).
- **Приоритет** - укажите приоритет Service ID от 0 до 255. Чем больше число, тем выше приоритет.

Внимание: Service ID должен должен соответствовать идентификатору группы, определенному на маршрутизаторе WCCP.

3. Нажмите **Добавить**. Созданный Service ID появится в таблице:



18.7.5 Исключения

Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

Подробнее о типах исключений в статье *Исключения*.

18.7.6 Исключения

Подсказка: Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

На вкладке **Исключения** можно исключить ресурсы из обработки прокси-сервером и всеми связанными службами (контент-фильтр, веб-отчетность, антивирусы):

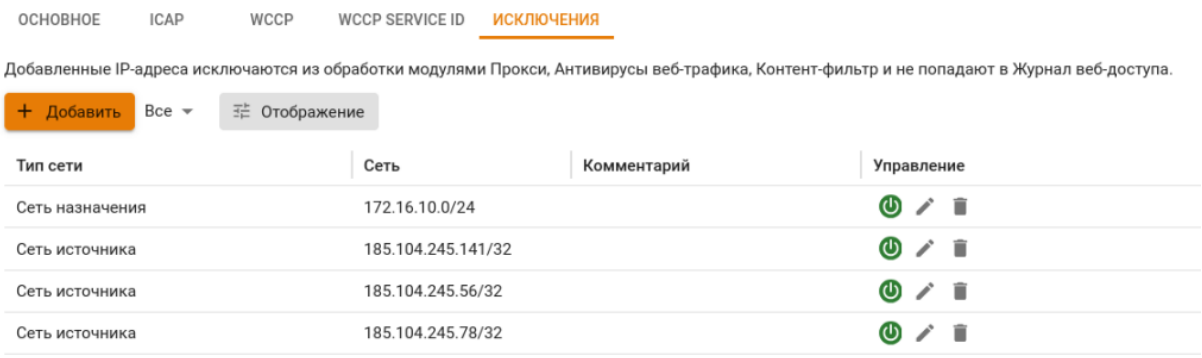
- **Сети источника** - указываются сети, трафик из которых исключается из обработки прокси-сервером;
- **Сети назначения** - указываются внешние сети или IP-адреса (как правило, адреса веб-сайтов или веб-сервисов), трафик до которых из всех локальных сетей NGFW исключается из обработки прокси-сервером.

Внимание: Настоятельно не рекомендуем исключать из обработки прокси-сервером ВСЮ локальную сеть.

Подсказка: При прямом подключении к прокси-серверу нельзя исключить трафик из обработки прокси. Исключать трафик нужно в настройках прокси-сервера на устройстве (в веб-браузере или системных настройках прокси-сервера).

При создании исключений можно указывать только IP-адреса или IP-сети.

Трафик, исключенный из обработки прокси, не будет участвовать в **Отчетах**, проверяться на вирусы и обрабатываться модулем **Контент-фильтра**. В то же время такой трафик будет проверен **Файрволом**, модулями **Предотвращение вторжений** и **Контроль приложений**.



Поиск по таблице исключений

Над таблицей исключений расположена строка поиска. Она позволяет искать среди исключений определенные IP-адреса и сети. Для поиска начните вводить требуемый IP-адрес:

Таблица будет динамически изменяться, отфильтруются только строки, содержащие значение, введенное в строку поиска.

Программы, работающие по отличным от HTTP(S) протоколам через веб-прокси

Некоторые программы, отправляющие трафик на свои серверы по портам 80 и 443, но при этом работающие по протоколам, отличным от HTTP(S), не могут быть обработаны веб-прокси-сервером на NGFW с включенной фильтрацией HTTPS-трафика. Трафик таких программ следует исключать из обработки прокси в поле **Сети назначения**.

1С Коннект:

- 185.104.248.141/32
- 185.151.243.218/32
- 185.99.140.108/32
- 185.99.140.101/32
- 185.99.140.102/32
- 185.99.140.103/32
- 185.99.140.104/32
- 185.99.140.105/32
- 185.99.140.106/32
- 185.99.140.107/32
- 185.99.140.108/32
- 185.99.140.114/32
- 185.99.140.115/32
- 193.107.238.195/32
- 77.223.98.83/32
- 77.244.213.204/32
- 78.155.206.40/32
- 78.155.218.78/32
- 80.249.148.135/32

- 88.198.27.15/32
- 88.198.27.27/32
- 88.221.132.128/32
- 92.242.35.35/32
- 46.4.207.211/32
- 2.16.154.81/32
- 185.188.183.87/32
- 185.24.93.122/32
- 185.244.173.25/32
- 185.143.172.61/32

ВЭД-Декларант:

- 46.48.116.196/32
- 94.213.21.144/32
- 194.213.21.144/32
- 91.220.57.3/32
- 212.49.126.110/32

Webinar.ru:

- 185.45.80.0/22
- 37.130.192.0/22

vks.samregion.ru:

- 195.248.236.141/32

Магазин DNS:

- 185.165.123.176
- 5.8.69.70/32

СДЭК:

- 185.165.123.40

Сбербанк Бизнес Онлайн:

- 194.54.14.137
- 194.186.207.182
- 195.8.62.178
- 194.54.15.90
- 10.21.132.124/32
- 92.38.2.37

Яндекс.Телемост:

- 37.140.128.0/18
- 37.9.64.0/18
- 5.255.192.0/18
- 5.45.192.0/18
- 37.9.127.0/25

- 5.255.192.0/25
- 5.255.252.0/25
- 37.9.123.192/31
- 5.255.192.176/31
- 5.255.230.32/31

Более подробная информация по настройке Телемоста в корпоративной сети представлена по ссылке.

18.7.7 Настройка прямого подключения к прокси

Настройка прямого подключения к прокси

Для настройки выполните действия:

1. Укажите IP-адрес локального интерфейса Ideco NGFW в качестве веб-прокси в локальной сети на клиентских устройствах;

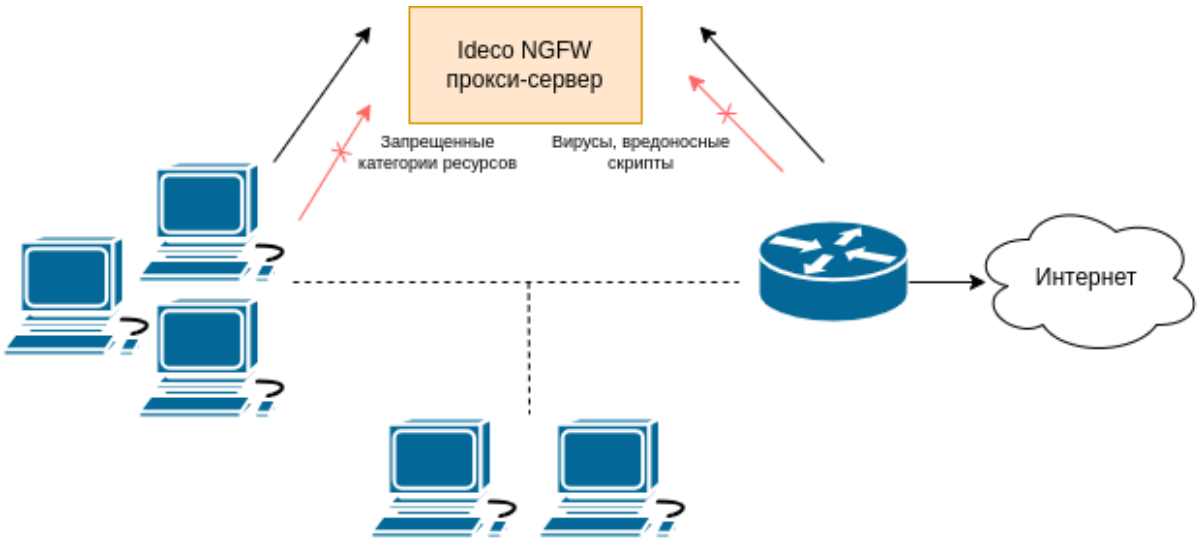
2. В настройках прокси на Ideco NGFW укажите порт для прямых подключений к прокси (возможен выбор портов из списка: 3128, 1080, 8000, 8080, 8888, 8081, 8088, 10080).

В таком режиме NGFW сможет предоставлять клиентским устройствам веб-трафик по другим портам (по умолчанию - по всем, при необходимости можно закрыть порты файрволом).

Подсказка: Если прямое подключение к прокси требуется только части клиентских устройств или части локальных интерфейсов, то создайте INPUT-правило файрвола.

Для учета, контроля и проверки веб-трафика на вирусы, требуется соблюдение следующих условий:

- Локальная подсеть не пересекается с внешним интерфейсом NGFW;
- У сервера Ideco NGFW есть доступ в интернет;
- На клиентских устройствах указан адрес веб-прокси (в настройках прокси-сервера в браузерах).



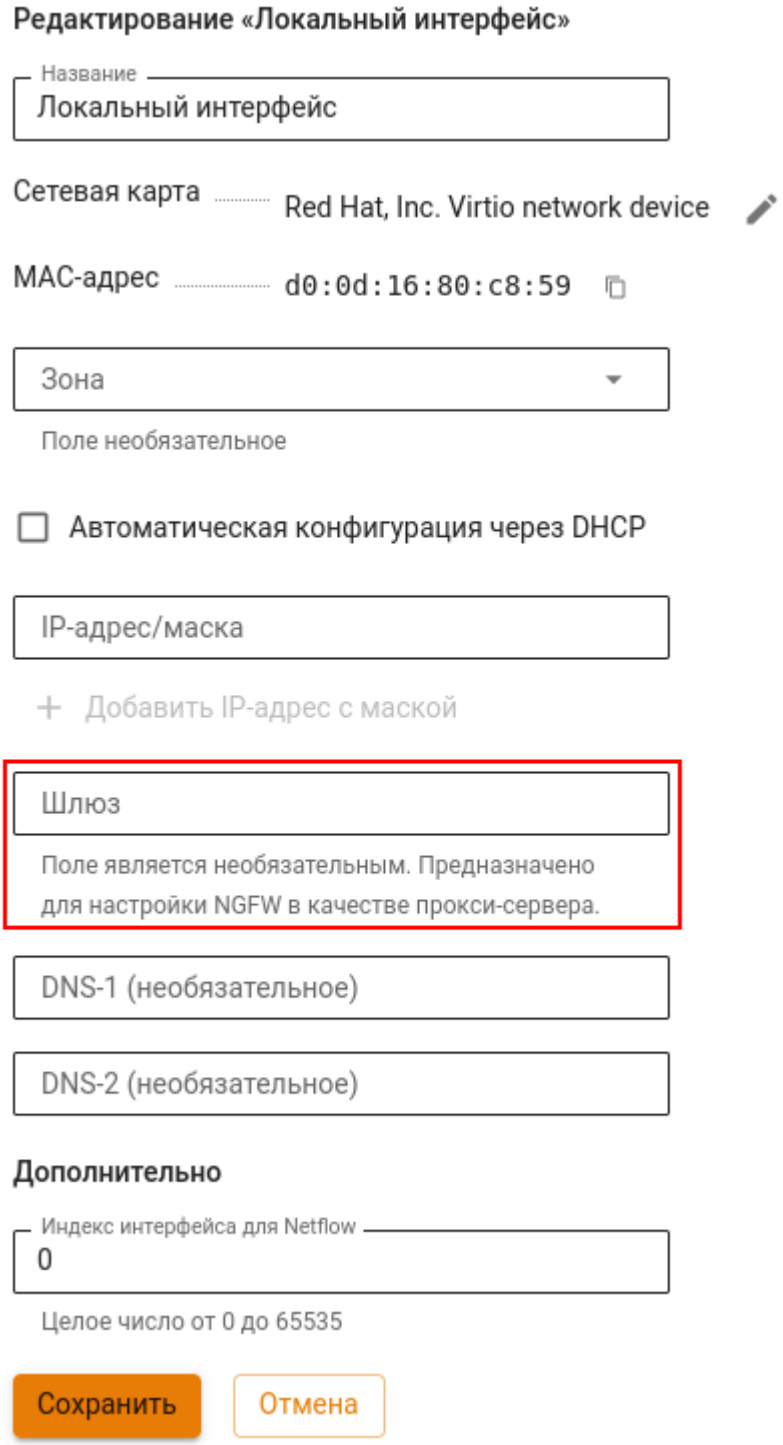
Если в настройках программы под ОС Windows или MacOS X нет возможности указать прокси-сервер, воспользуйтесь сторонним ПО для маршрутизации всего трафика рабочей станции на прокси-сервер. Такую возможность предоставляет программа **Proxifier**, которую можно настроить для прямых подключений к прокси, воспользовавшись *статьей*.

18.7.8 Настройка прокси с одним интерфейсом

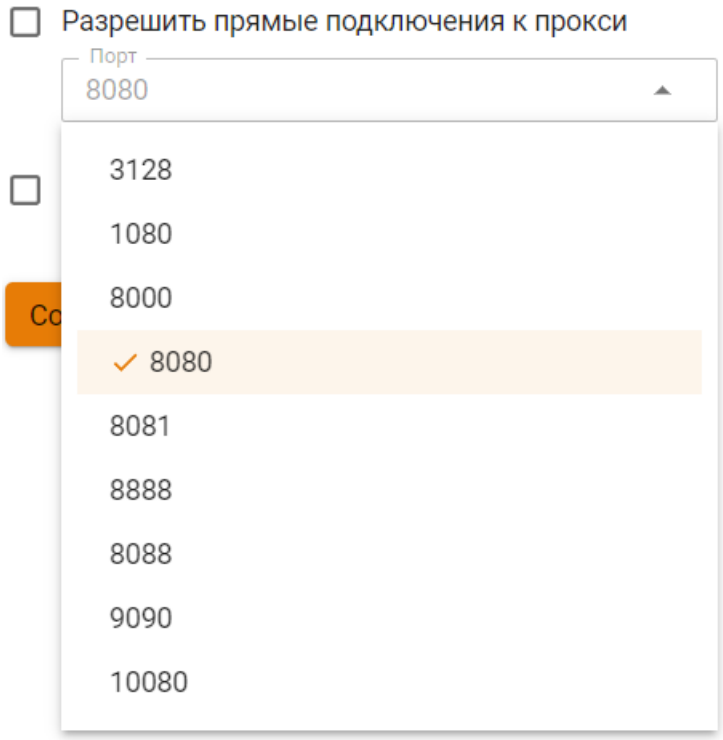
Настройка прокси с одним интерфейсом

При необходимости можно использовать Ideco NGFW в качестве прокси-сервера с прямыми подключениями клиентов к прокси, с одним интерфейсом. Для этого выполните действия:

1. При создании локального интерфейса в разделе **Сервисы -> Сетевые интерфейсы** укажите **Шлюз**:



2. Разрешите прямые подключения к прокси-серверу в разделе **Сервисы -> Прокси**, выбрав нужный порт из списка:



18.8 Обратный прокси

Подсказка: Название службы раздела **Обратный прокси**: `ideco-reverse-backend`.
Список служб для других разделов доступен по *ссылке*.

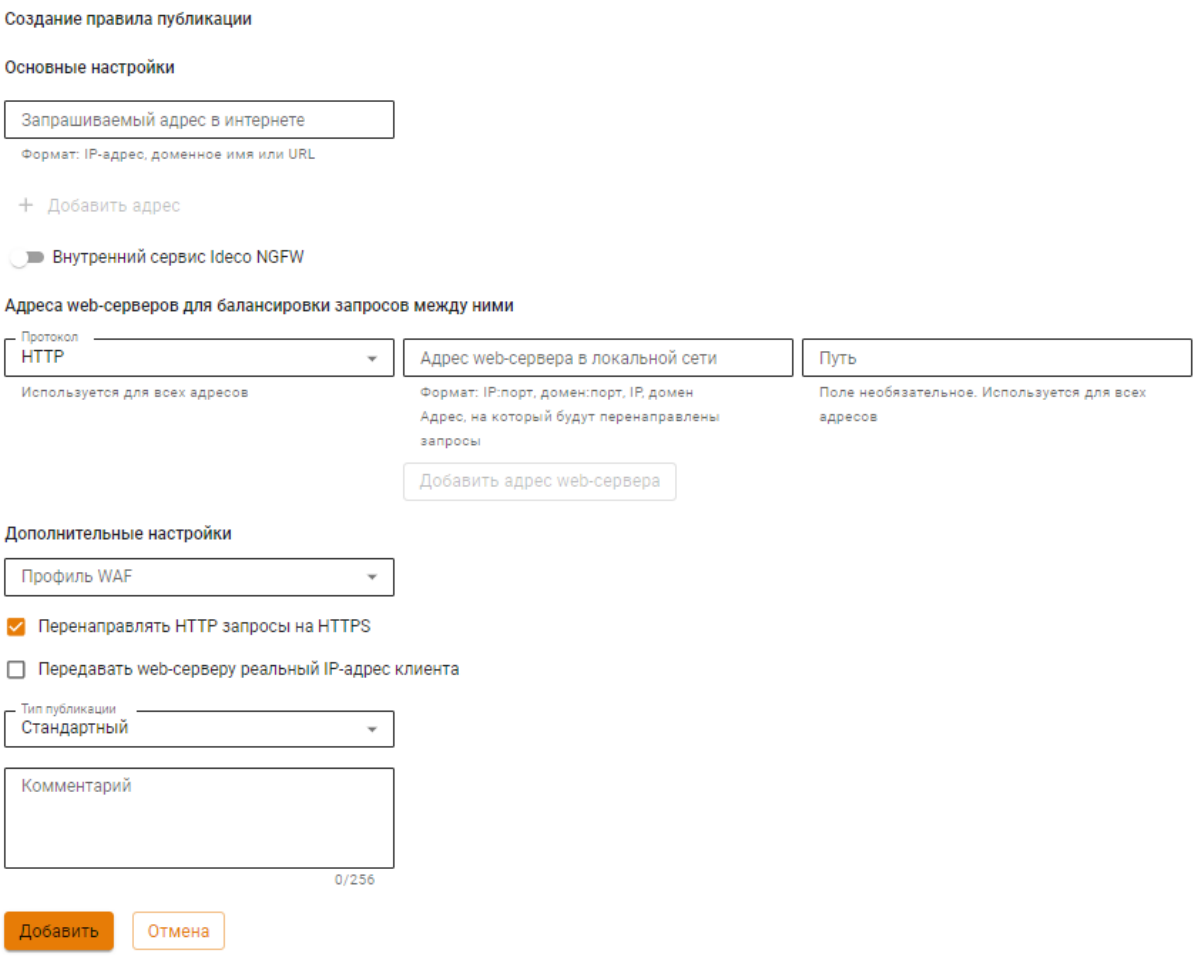
Технология обратного прокси позволяет проксировать веб-трафик из сети интернет в локальную сеть. Отличается от DNAT тем, что работает на более высоком уровне (прикладной протокол HTTP вместо сетевого протокола IP) и позволяет более гибко реализовать публикацию ресурсов.

Обратный прокси позволяет смаршрутизировать запрос на HTTP-сервер в локальной сети из внешней сети. Таким образом, имея одну ресурсную A-запись для внешнего сетевого интерфейса NGFW, можно опубликовать несколько ресурсов в локальной сети, распределив их по нескольким входящим URL.

18.8.1 Создание и настройка правила

Настройка сертификатов для публикуемых ресурсов не требует их ручной загрузки. Ideco NGFW сам отправляет запрос на выпуск сертификата Let's Encrypt. Выпуск сертификата может занять до 20 минут. Выпущенные сертификаты будут доступны в разделе *Сертификаты*.

Для создания правила перейдите в раздел **Сервисы -> Обратный прокси** и нажмите на кнопку **Добавить**. Форма добавления правила разделена на два подраздела: **Основные настройки**, **Адреса web-серверов для балансировки запросов между ними** и **Дополнительные настройки**.



Основные настройки

- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных адресов нажмите кнопку **Добавить адрес**;
- **Адрес web-сервера в локальной сети** - введите IP-адрес из локальной сети, на который будут перенаправляться пользователи.

Подсказка: Если указать в строке **Запрашиваемый адрес в интернете** *0.0.0.0*, перенаправление будет работать со всех внешних IP-адресов Ideco NGFW на адрес из строки **Адрес web-сервера в локальной сети**.

Чтобы перенаправление работало с доменов Ideco NGFW на адрес из строки **Адрес web-сервера в локальной сети**, необходимо явно указать домены в строке **Запрашиваемый адрес в интернете**.

Адреса web-серверов для балансировки запросов между ними

- **Протокол** - выбранный протокол используется для всех адресов в правиле;
- **Адрес web-сервера в локальной сети** - адрес, на который будут перенаправлены запросы;
- **Путь** - поле необязательное и используется для всех адресов.

Дополнительные настройки

- Функция **Перенаправлять HTTP-запросы на HTTPS** используется в случае, если ваш сайт работает только по протоколу HTTPS, но при этом вы не хотите терять посетителей, обратившихся к вашему сайту по HTTP;
- **Профиль WAF** - позволяет задать параметры защиты веб-ресурса при указании WAF-профиля.
- При включении функции **Передавать web-серверу реальный IP-адрес клиента** публичный IP-адрес клиента при обратном проксировании не заменяется на адрес NGFW.

Подсказка: Web Application Firewall (WAF) анализирует запросы к сайту и блокирует атаки на уязвимые компоненты веб-приложения (в частности, типы атак, входящие в OWASP TOP-10). При активации этого модуля также будут блокироваться злоумышленники, ведущие сканирование сайта на уязвимости, с помощью модуля защиты от brute force атак.

Не рекомендуем использовать проброс веб-интерфейса NGFW через WAF, так как при попытке входа пользователь может быть заблокирован средствами WAF.

- Поле **Тип публикации** позволяет выбрать один из типов: **Стандартный** и **Outlook Web Access**. Тип **Outlook Web Access** используется для публикации Microsoft Exchange.

В полях **Запрашиваемый адрес в интернете** и **Адрес в локальной сети** для типа **Outlook Web Access** укажите только домены `https://youdomain/` без остальной части URL (она не используется при публикации этим способом).

Внимание: При публикации Outlook Web Access не включайте Web Application Firewall. Их совместная работа будет возможна в следующих версиях.

Если у вас имеется доверенный SSL-сертификат для домена, по которому будет идти обращение извне на публикуемый ресурс, то его можно загрузить в раздел **Сервисы -> Сертификаты** с помощью кнопки **Добавить**.

Доменные имена, указываемые в поле **Запрашиваемый адрес в интернете**, должны резолвиться во внешний IP-адрес сервера NGFW. Доменные имена, указываемые в поле **Адрес в локальной сети**, должны резолвиться в IP-адреса публикуемых ресурсов самим сервером NGFW.

Публикация CMS

Нами протестирована и официально поддерживается публикация сайтов на двух популярных CMS: **Joomla** и **Wordpress**. Подробности публикации каждой CMS описаны ниже.

Joomla:

Joomla в текущей реализации публикуется, если настроить перенаправление с внешнего домена на локальный домен без префикса:

- Ассоциировать с внешним адресом NGFW дополнительное доменное имя специально для публикации Joomla: `joomla.mydomain.ru`;
- Настроить правило публикации `joomla.mydomain.ru` -> `joomla.local:port` (порт не обязателен).

WordPress:

WordPress в текущей реализации публикуется только в конфигурации, когда в WordPress и в обратном прокси настроен один и тот же домен:

- Для домена компании добавить A-запись `wordpress.mydomain.ru`, указывающую на внешний IP-адрес NGFW;
- На локальном сервере, в админ-панели WordPress должен быть настроен домен `wordpress.mydomain.ru` на стандартном порту HTTP;
- Добавить в обратный прокси правило публикации `wordpress.mydomain.ru -> wordpress.mydomain.ru`.

18.8.2 Защита от DoS-атак

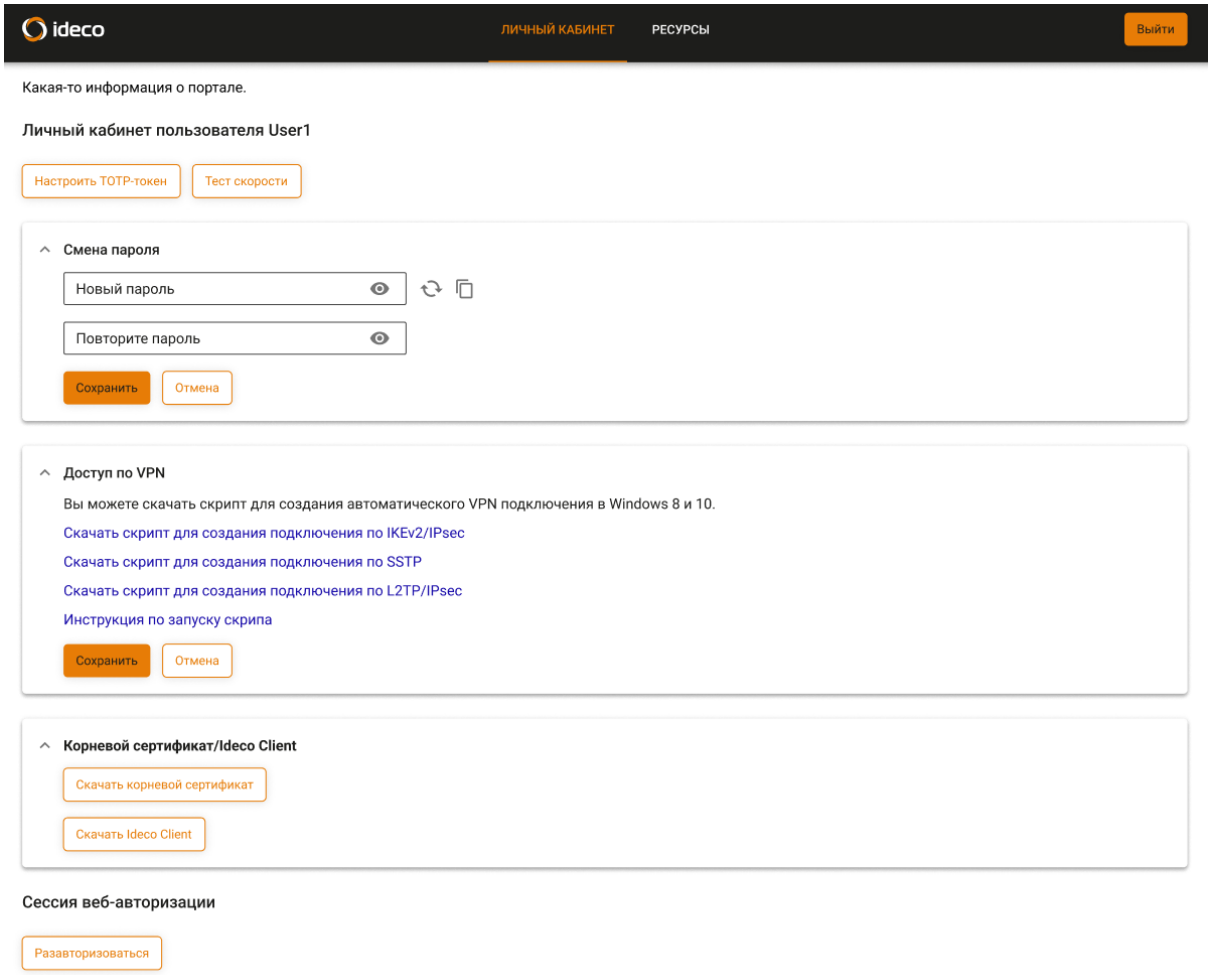
Включение опции **Защита от DoS-атак** ограничивает трафик, если:

- скорость - более 200 запросов в секунду с одного IP-адреса;
- количество подключений с одного IP-адреса - более 1000;
- размер запроса - более 50 Мб;
- время ожидания на чтение заголовка и тела запроса - более 5 секунд.

18.9 ЛК/Портал SSL VPN

Возможности личного кабинета Ideco NGFW:

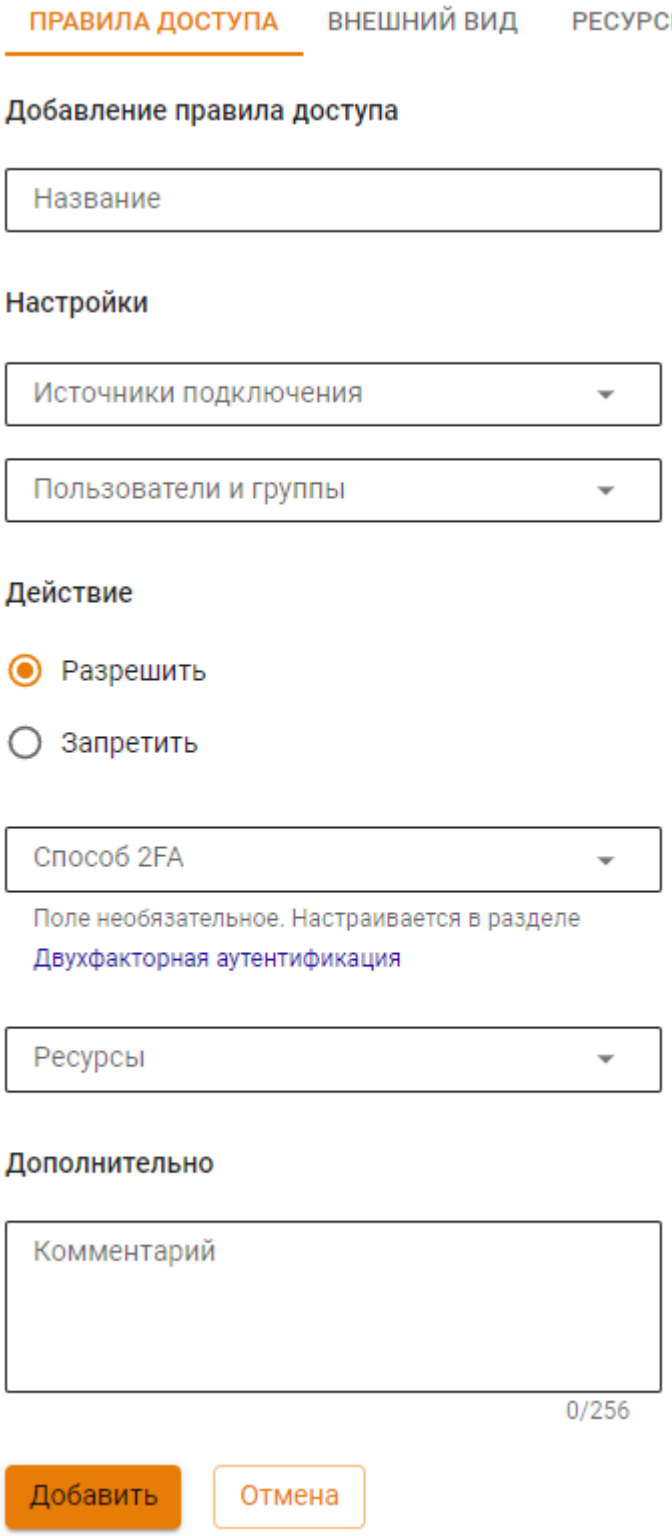
- **Смена пароля**;
- **Скачивание корневого сертификата**;
- **Скачивание скриптов для создания автоматического VPN-подключения в Windows 8 и 10**. Будут доступны скрипты настройки только тех типов подключения, которые указаны для пользователя в таблице **Доступ по VPN** в разделе **Пользователи -> VPN-подключения**;
- **Информация о квоте**;
- **Генерация TOTP-токена**. Для настройки двухфакторной аутентификации воспользуйтесь *статьей*;
- **Скачивание Ideco Client**. Подробнее о работе в Ideco Client - в *статье*;
- **Тестирование скорости**. При нажатии на соответствующую кнопку в веб-интерфейсе личного кабинета откроется меню тестирования скорости между хостом и NGFW;
- **Разавторизация**. Разавторизация пользователя в сети NGFW, если он был авторизован через Web/SSO.



Настроить доступ пользователей в личный кабинет можно в разделе **Пользователи -> Личный кабинет пользователя**. Для этого необходимо создать **Правило доступа**, а затем опубликовать личный кабинет через обратный прокси, чтобы пользователи получили к нему доступ.

18.9.1 Правила доступа

Чтобы создать правила доступа, нажмите **Добавить** и заполните необходимые поля:



- **Название** - название правила доступа;
- **Источники подключения** - укажите IP-адреса, подсети, страны или домены;
- **Пользователи и группы** - выберите пользователей, группы пользователей, группы безопасности из AD, которым хотите предоставить доступ в личный кабинет;
- **Способ 2FA** - выберите метод двухфакторной аутентификации. Поле может быть пустым;

- **Ресурсы** - укажите необходимые ресурсы, созданные в разделе **ЛК/Портал SSL VPN -> Ресурсы**. Поле может быть пустым;
- **Комментарий** - поле может быть пустым.

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

Подсказка: По умолчанию в таблице правил раздела настроено правило доступа к личному кабинету для всех пользователей:

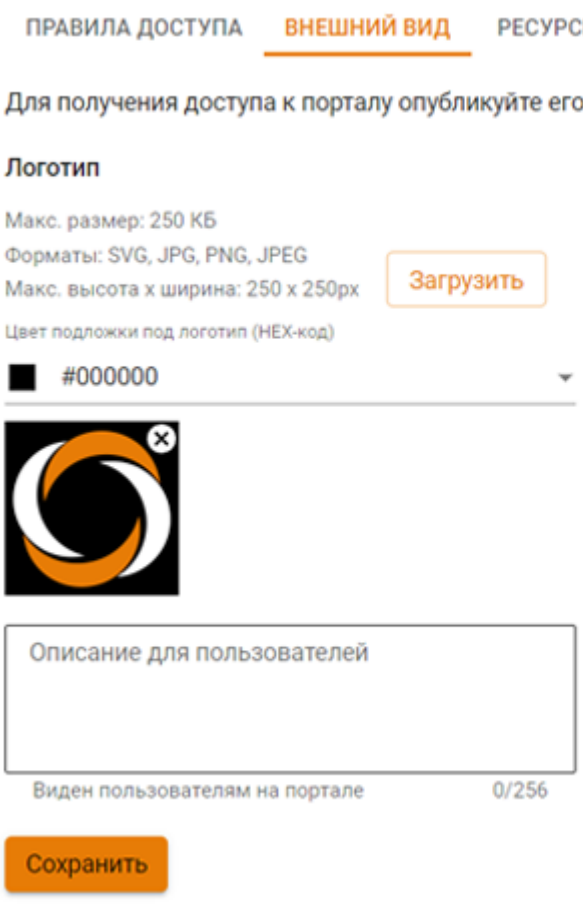
Название	Источник	Пользователи и группы	Доступ в ЛК	Ресурсы SSL VPN	Способ 2FA	Комментарий
Создано автоматически	Любой	Любой	Разрешить	–	–	Доступ всем пользователям к личному кабинету.
Запрет всем	Любой	Любой	Запретить	–	–	Это системное правило. В него попадают пользователи, не попавшие под условия остальных правил.

Обработка правил происходит следующим образом:

1. При входе пользователя в ЛК правила проверяются сверху вниз до первого совпадения по полям **Источник** и **Пользователи и группы**;
2. Если правило разрешающее, то доступные пользователю в ЛК ресурсы определяются этим правилом. Последующие правила с такими же полями учитываться не будут;
3. При изменении таблицы, пользователя, участия пользователя в группах определение доступа пользователя или группы пользователей к ресурсу происходит снова как в пункте 1.

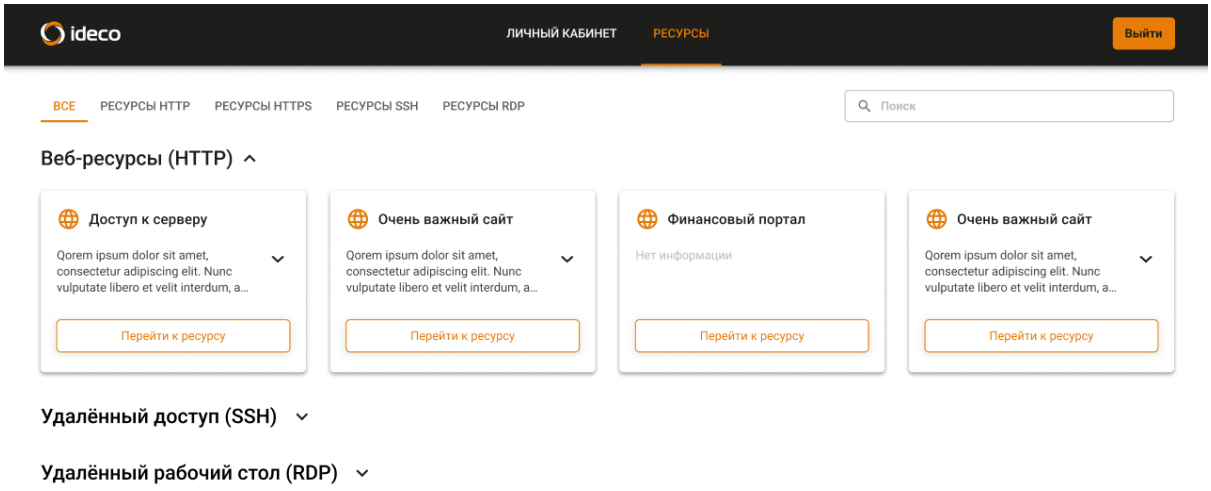
18.9.2 Внешний вид

На вкладке можно изменить логотип и добавить описание для пользователей, которое будет отображаться рядом с логотипом в личном кабинете и на портале:

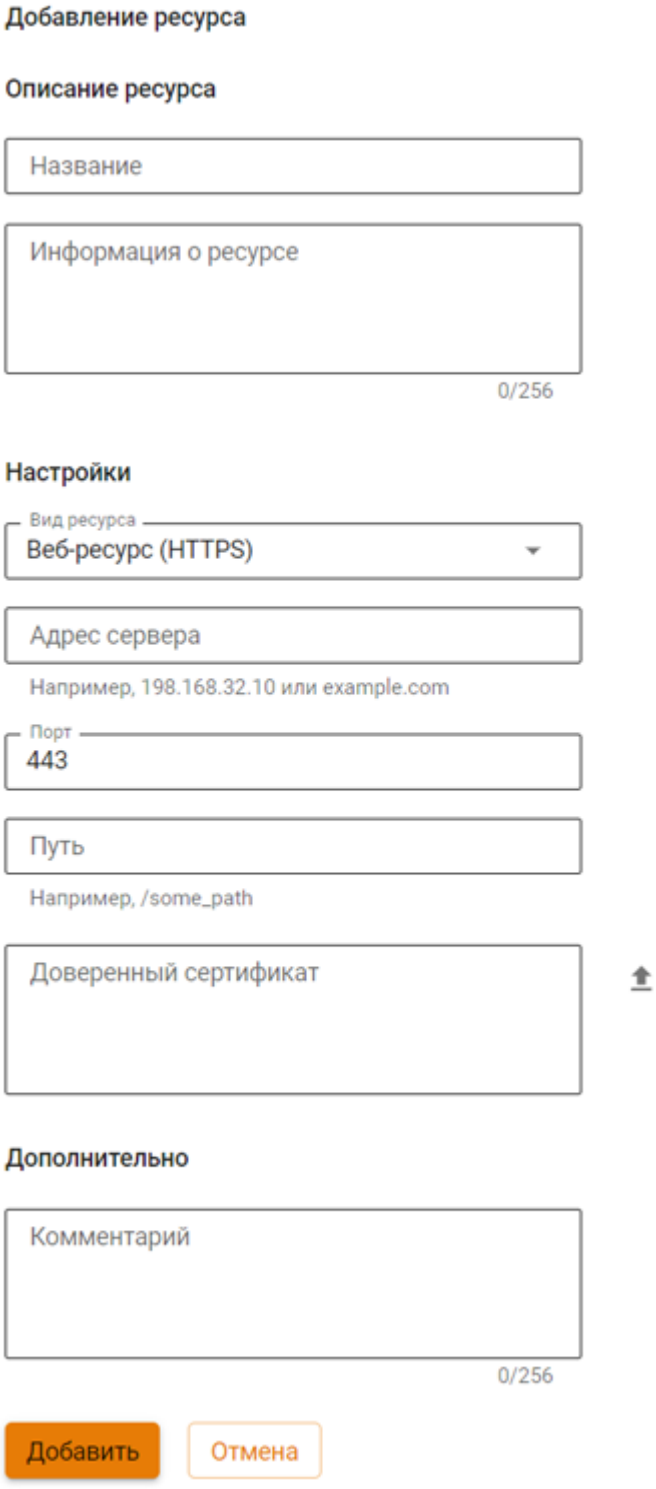


18.9.3 Ресурсы

В личном кабинете Ideco NGFW можно разместить информацию о любых ресурсах для пользователей:



Чтобы добавить ресурс, перейдите в раздел **Пользователи -> ЛК/Портал SSL VPN -> Ресурсы**, нажмите **Добавить** и заполните поля:



Описание ресурса:

- **Название** - имя ресурса, может содержать до 42 символов;
- **Информация о ресурсе** - укажите текстовое описание, которое будет отображаться в личном кабинете, или оставьте поле пустым.

Настройки:

- **Вид ресурса** - **Веб-ресурс (HTTPS)**:
  - **Адрес сервера** - укажите доменное имя или IP-адрес сервера;

  - **Порт** - по умолчанию значение 443;
  - **Путь** - укажите путь. чего куда. Поле не является обязательным;
  - **Доверенный сертификат** - загрузите доверенный сертификат. Поле не является обязательным.
- **Вид ресурса** - **Веб-ресурс (HTTP)**:
  - **Адрес сервера** - укажите доменное имя или IP-адрес сервера;
  - **Порт** - по умолчанию значение 80;
  - **Путь** - укажите путь. чего куда. Поле не является обязательным.
- **Вид ресурса** - **Удаленный доступ (SSH)**:
  - **Адрес сервера** - укажите доменное имя или IP-адрес сервера;
  - **Порт** - по умолчанию значение 22;
  - **Отпечаток ключа** - загрузите отпечаток ключа.
- **Вид ресурса** - **Удаленный рабочий стол (RDP)**:
  - **Адрес сервера** - укажите доменное имя или IP-адрес сервера;
  - **Порт** - по умолчанию значение 3389. **Дополнительно:**
  - **Комментарий** - поле может быть пустым.

Подсказка: Адреса, на которые ссылается HTTP/HTTPS-ресурс, должны быть относительными во избежание нарушения CORS. Подробнее про CORS.

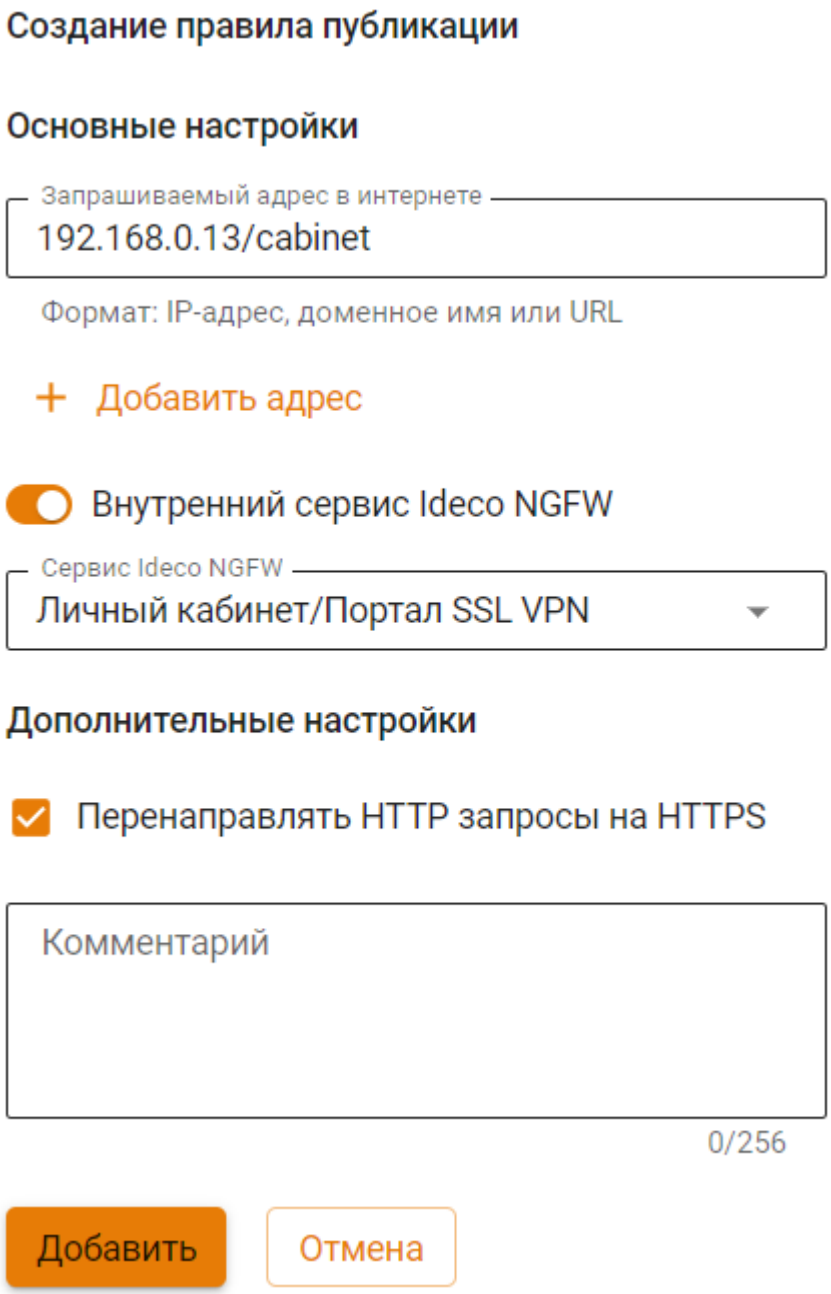
18.9.4 Публикация личного кабинета

Чтобы пользователи получили доступ в личный кабинет, он должен быть опубликован. Для публикации ЛК перейдите в раздел **Сервисы -> Обратный прокси** и выполните действия:

1. Нажмите **Добавить**.

2. Включите опцию **Внутренний сервис Ideco NGFW**.

3. В поле **Запрашиваемый адрес в интернете** введите адрес, по которому хотите опубликовать личный кабинет:



4. Нажмите **Добавить**.

После этого пользователь сможет зайти в личный кабинет по логину и паролю либо через авторизацию в сети NGFW.

18.9.5 Настройка доступа пользователя в личный кабинет Ideco NGFW

Подсказка: Личный кабинет пользователя будет доступен по ссылке, указанной при публикации через обратный прокси.

Чтобы зайти в личный кабинет, выполните действия:

1. Перейдите по ссылке, указанной в правиле публикации личного кабинета.

2. В открывшейся форме авторизации введите логин и пароль пользователя.

Если пользователь уже авторизован в сети NGFW, то логин и пароль вводить не потребуется, личный кабинет откроется сразу.

18.10 DNS

18.10.1 Основное

Подсказка: Название службы раздела **DNS**: `ideco-unbound`; `ideco-dns-backend; nsd`.
Список служб для других разделов доступен по *ссылке*.

Настройка производится в разделе **Сервер -> DNS** на следующих вкладках:

Внешние DNS-серверы - позволяют указать DNS-серверы во внешних сетях, через которые будут разрешаться доменные имена, запрашиваемые из локальных сетей.

Forward-зоны - позволяют указать сторонние DNS-серверы (в локальных или внешних сетях относительно NGFW) с указанием конкретных DNS-зон, которые эти серверы обслуживают. Перечисленные возможности DNS-сервера могут использоваться одновременно.

Master-зоны - позволяют настроить полнофункциональный DNS-сервер, разрешающий имена в IP-адреса сетевых устройств в локальной сети.

При наличии большого количества Forward- и Master-зон в таблицах воспользуйтесь кнопкой **Фильтры**.

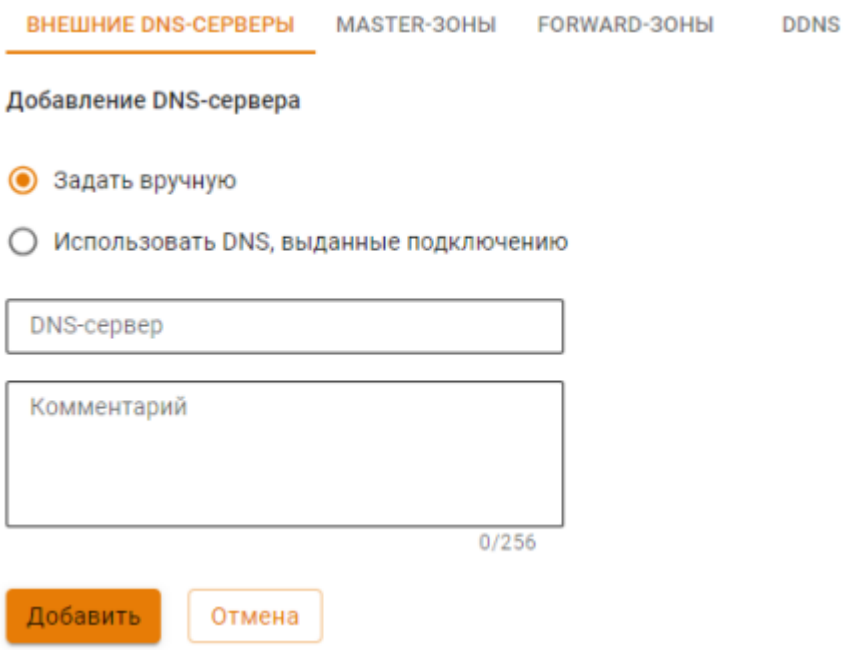
18.10.2 Внешние DNS-серверы

Для корректной работы резолвинга имен через Ideco NGFW указывать DNS-серверы в этом разделе не требуется.

Если DNS-серверы не указаны, то сервер будет разрешать имена в сети интернет, используя корневые DNS-серверы в интернете.

Данная конфигурация не будет работать, если вышестоящий роутер перехватывает DNS-запросы. В этом случае рекомендуем:

- Укажите DNS-серверы вручную (нажмите **Добавить**):
  - Выберите **Задать вручную** и укажите IP-адрес DNS-сервера;
  - Используйте опцию **Использовать DNS, выданные подключению**, указав нужное подключение.



Рекомендации:

1. В Ideco NGFW встроен кеширующий DNS-сервер. Рекомендуется использовать его в качестве DNS-сервера для локальной сети.

2. Не указывайте `8.8.8.8`, `1.1.1.1` или подобные без особой необходимости. Ideco NGFW справится с резолвингом самостоятельно.

3. Не указывайте DNS-серверы от внутреннего сервера Active Directory, даже если он может самостоятельно резолвить доменные имена в интернете. При интеграции с AD Ideco NGFW автоматически настроит все необходимое (Forward-зону) для работы AD и резолвинга внутренних имен домена. Для резолвинга каких-то особых зон, не связанных с AD, создавайте Forward-зону.

4. Не рекомендуем использовать DNS, выданные интернет-провайдером, так как они превышают TTL и долго отвечают. Ideco NGFW настроит автоматически все необходимое для подключения к PPTP/L2TP через доменное имя. Если нужна особая внутренняя доменная зона провайдера, то создавайте Forward-зону.

5. Можно указывать DNS-серверы занимающиеся фильтрацией, если это необходимо (SkyDNS или Яндекс-DNS).

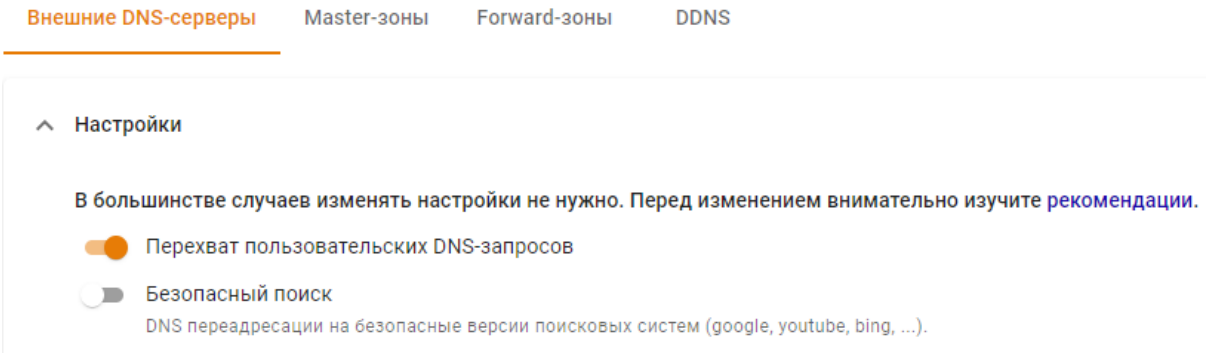
6. Если все DNS-серверы отключены или удалены, то DNS будет работать нормально (Ideco NGFW резолвит имена самостоятельно).

7. 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 подключению.

Перехват DNS-запросов

Подсказка: Включение перехвата пользовательских DNS-запросов блокирует использование DNS-over-TLS (DoT), DNS-over-QUIC (DoQ) и DNS-over-HTTPS (DoH).

Если на рабочей станции пользователя указаны сторонние DNS-серверы (например, с целью обхода блокировок), включите опцию **Перехват пользовательских DNS-запросов** в разделе **Внешние DNS-серверы**.



Опция включается глобально для всех хостов в локальной сети для избежания возможной подмены адреса ресурса при резолвинге его домена.
Также перехват позволит контролировать процесс резолвинга доменных имен в интернете исключительно средствами NGFW. Запрос будет перенаправлен на DNS-сервер NGFW, и он же сформирует ответ (вместо исходного DNS-сервера).

Перехват DNS-запросов также блокирует возможность туннелирования через DNS (DNS-tunneling) и блокирует использование DNS-over-TLS.

Сторонние DNS-серверы для дополнительной фильтрации трафика:

- SkyDNS `193.58.251.251`;
- Yandex DNS `77.88.8.88`, `77.88.8.2`;
- Google DNS `8.8.8.8`, `8.8.4.4`;
- Open DNS `208.67.222.222`, `208.67.220.220`, `208.67.222.220`, `208.67.220.222`;
- Cloudflare DNS `1.1.1.1`, `1.0.0.1`.

Безопасный поиск

При резолвинге через DNS-сервер NGFW будет возвращать адреса поисковых систем с включенной фильтрацией неподобающего контента.

18.10.3 Master-зоны

Master-зоны позволят использовать NGFW как сервер имен внутри сетевой инфраструктуры для обращения к IP-адресам хостов в сети по доменным именам. При настройке Master-зон в NGFW не предусмотрено автозаполнение.

Подсказка: DNS-сервер в Ideco NGFW недоступен извне по соображениям безопасности. Для поддержки внешних DNS-зон, рекомендуем использовать сторонние DNS-хостинги.

Для корректной работы Master-зон с IDN-доменами выполните действия:

1. Преобразуйте IDN-домены в формат **Punnycode**. Подробнее в RFC.

2. При создании содержимого Master-зоны используйте преобразованное в формат **Punnycode** доменное имя.

IDN-домен - домен, составленный из национальных символов алфавита. Например, **дневник.ру**.

Не используйте Master-зоны для блокировки доступа к сайтам, для этого есть другие *средства*.
Блокировка таким способом работает неэффективно и не позволяет выборочно запрещать доступ по пользователям или подсетям. Также приводит к проблемам с излишним кешированием.

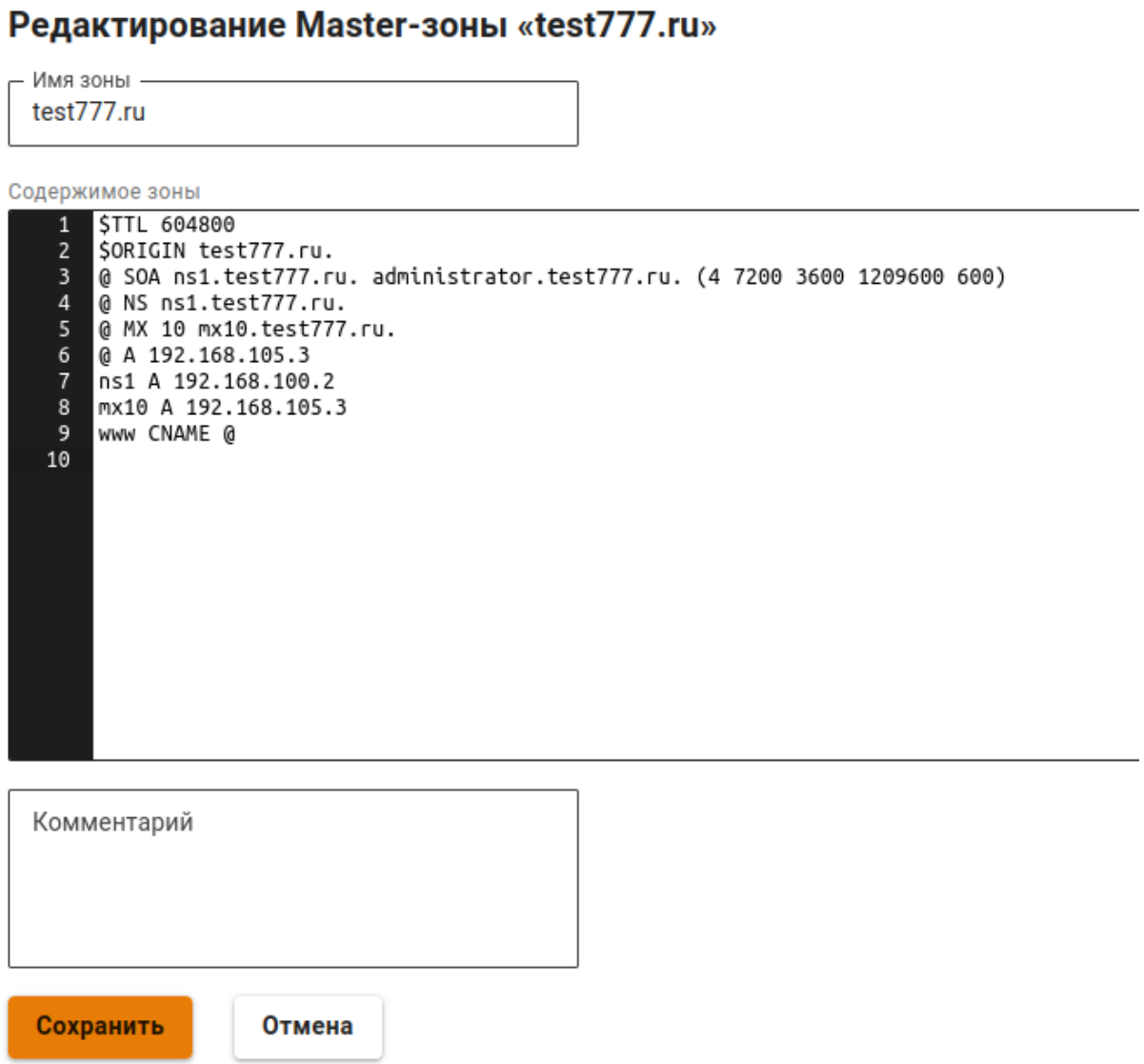
Формат записей для настройки Master-зоны соответствует формату записей DNS-сервера BIND.

Описание параметров записи:

- **$TTL** - определяет время кеширования положительных ответов (ответ в виде найденного IP-адреса). Время задается в секундах или с помощью сокращений: m — минуты, h — часы, d — дни, w — недели;
- **$ORIGIN** - определяет текущее имя домена. Текущее значение $ORIGIN заменяет символ @ в записи. Текущее значение $ORIGIN добавляется к любому имени, которое не заканчивается на «точку»;
- **$SOA** - описывает основные/начальные настройки зоны, или *определяет зону ответственности данного сервера*. Для каждой зоны должна существовать только одна запись SOA и она должна быть первая. В записи $SOA указывается primary NS для домена и e-mail контактного лица и далее в скобках:
  1. **Serial** - Серийный номер файла зоны. При изменении данных нужно менять серийный номер, при этом зона обновляется на всех серверах. Используйте формат: ГГГГММДДнн (год, месяц, день, нн — порядковый номер изменения за день). Если второй раз за день вносите изменения в файл зоны, укажите «нн» равным 01, если третий - 02, и т. д.;
  2. **Refresh** - указывает, как часто вторичные серверы должны опрашивать первичный, чтобы узнать, не увеличился ли серийный номер зоны;
  3. **Retry** - время ожидания после неудачной попытки опроса;
  4. **Expiry** - максимальное время, в течение которого вторичный сервер может использовать информацию о полученной зоне;
  5. **TTL** - минимальное время, в течение которого данные остаются в кеше вторичного сервера.
- **$SRV** - указывают на сервера, обеспечивающие работу тех или иных служб в этом домене (например, Jabber и Active Directory);
- **$NS** - DNS-сервер, обслуживающий этот домен. Минимально их необходимо два, причем они должны находится в разных подсетях, а лучше - в географически разных местах. Первым указывайте primary сервер;
- **$PTR** - отображает IP-адрес в доменное имя;
- **$MX** - описывает почтовые шлюзы (обычно один), на которые будет доставляться вся почта этого домена. Для каждого шлюза устанавливается приоритет (по умолчанию - 10). Обычно имя домена почтового шлюза выглядит так: *mx.example.com*. Для MX хостов должны быть соответствующие A-записи;
- **$A** - отображают имя хоста (доменное имя) на адрес IPv4. Для каждого сетевого интерфейса машины должна быть сделана одна **A-запись**;
- **$AAAA** - аналогична записи A, но для IPv6;
- **$CNAME** - отображает алиас на реальное имя (для перенаправления на другое имя).

Со всеми ресурсными записями можно ознакомиться по ссылке.

Пример записи приведен на скриншоте ниже:



Несколько примеров записей в Master-зону:

1. Имя зоны: ms

```
$ORIGIN ms.
$TTL 600
@ SOA ns1.ms. administrator.ms. ( 4 7200 3600 1209600 600 )
@ NS ns1.ms.
@ MX 10 mx10.ms.
@ A 192.168.0.250
ns1 A 192.168.0.250
mx10 A 192.168.0.250
www CNAME @
```

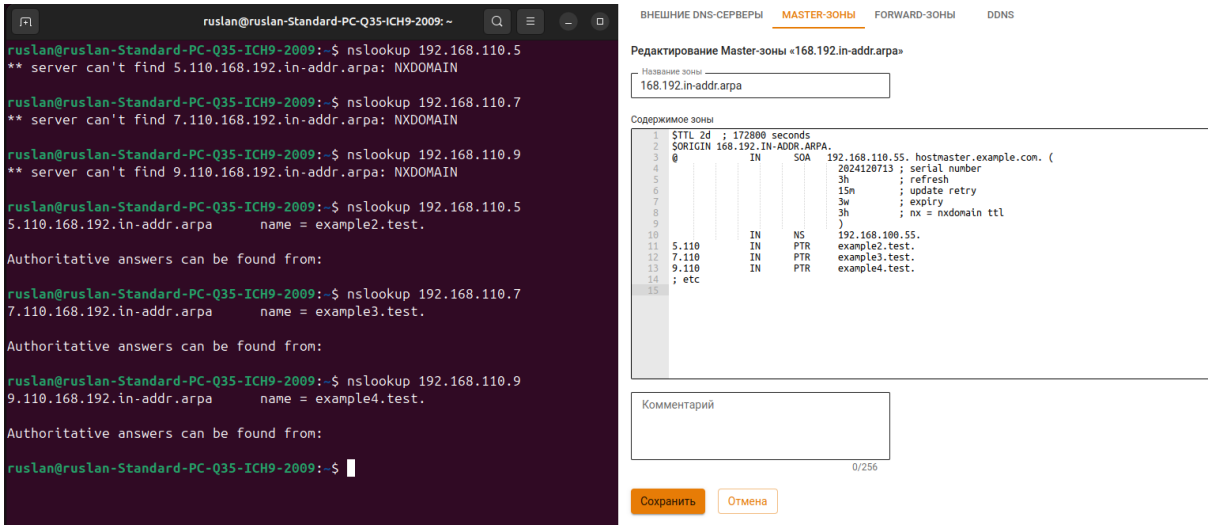
2. Имя зоны: example.com

```
$TTL 86400
@ SOA localhost. root.localhost. ( 991079290 28800 14400 3600000 86400 )
@ NS my-dns-server.example.com.
my-dns-server A 1.2.3.4
```

Обратная Master-зона

Обратная Master-зона используется для распознавания домена по IP-адресу.

При создании Master-зоны необходимо указать хотя бы одну PTR-запись. Пример обратной Master-зоны:



Имя зоны: 168.192.in-addr.arpa

Доменная зона соответствует IP-адресу 192.168.0.0/16. В содержимом зоны указаны 3 PTR-записи:

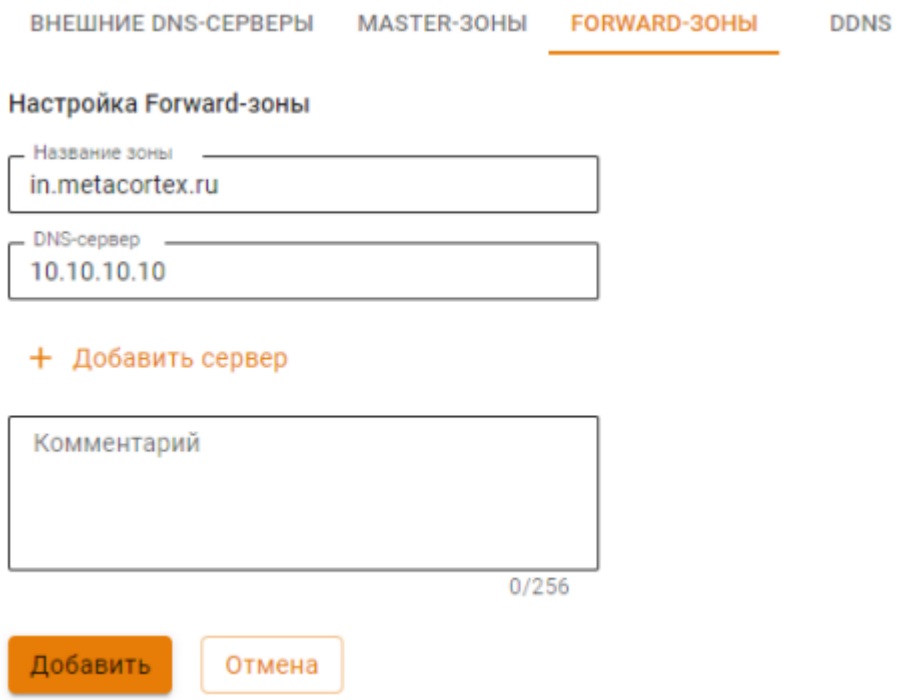
```
$TTL 2d  ; 172800 seconds
$ORIGIN 168.192.IN-ADDR.ARPA.
@             IN      SOA   192.168.100.6. hostmaster.example.com. (
                              2024120713 ; serial number
                              3h         ; refresh
                              15m        ; update retry
                              3w         ; expiry
                              3h         ; nx = nxdomain ttl
                              )
              IN      NS      192.168.100.6.
5.100         IN      PTR     example2.test
7.100         IN      PTR     example3.test.
8.100         IN      PTR     example4.test.
; etc
```

18.10.4 Forward-зоны

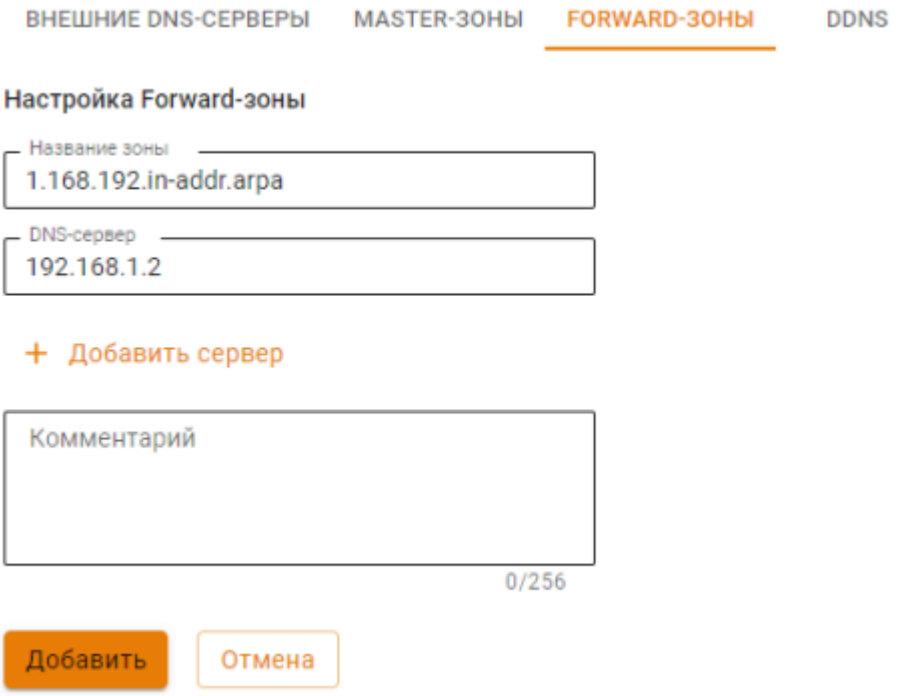
Основное

Позволяет задать DNS-сервер для разрешения имен конкретной DNS-зоны. Указав доступный в сети DNS-сервер и обслуживаемую зону, клиенты сети Ideco NGFW получают возможность обращаться к ресурсам этой зоны по именам домена.

Например, IT-отдел предприятия предоставляет ресурсы для сотрудников в зоне `in.metacortex.ru` под именами `realm1.in.metacortex.ru`, `sandbox.in.metacortex.ru` и использует для этого DNS-сервер 10.10.10.10.
Для возможности доступа к этим ресурсам по доменным именам укажите Forward-зону провайдера как isp и далее задайте DNS-сервер 10.10.10.10:



Подсказка: Для резолвинга PTR при интеграции с Active Directory пропишите обратную Forward-зону. Например, для подсети **192.168.1.0/24** в названии зоны нужно прописать **1.168.192.in-addr.arpa**:



18.10.5 DDNS

Подсказка: Название службы раздела **DDNS**: `ideco-dns-backend`.
Список служб для других разделов доступен по *ссылке*.

DDNS в Ideco NGFW реализован через интеграцию с хостингом RU-CENTER. Перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.
Для решения вопросов по работе с хостингом воспользуйтесь страницей помощи.

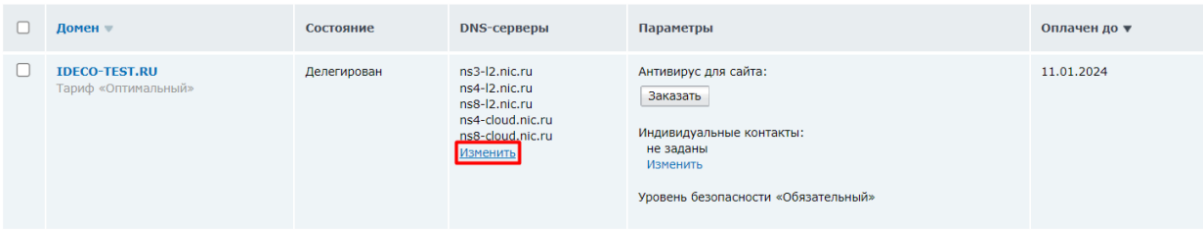
Настройка DDNS

Подсказка: DDNS не будет работать:

- если NGFW находится за NAT;
- если включена балансировка трафика.

1. После входа в личный кабинет RU-CENTER откроется страница Для клиентов. Для дальнейшей работы откройте два раздела - **Мои домены** и **DNS-хостинг**:

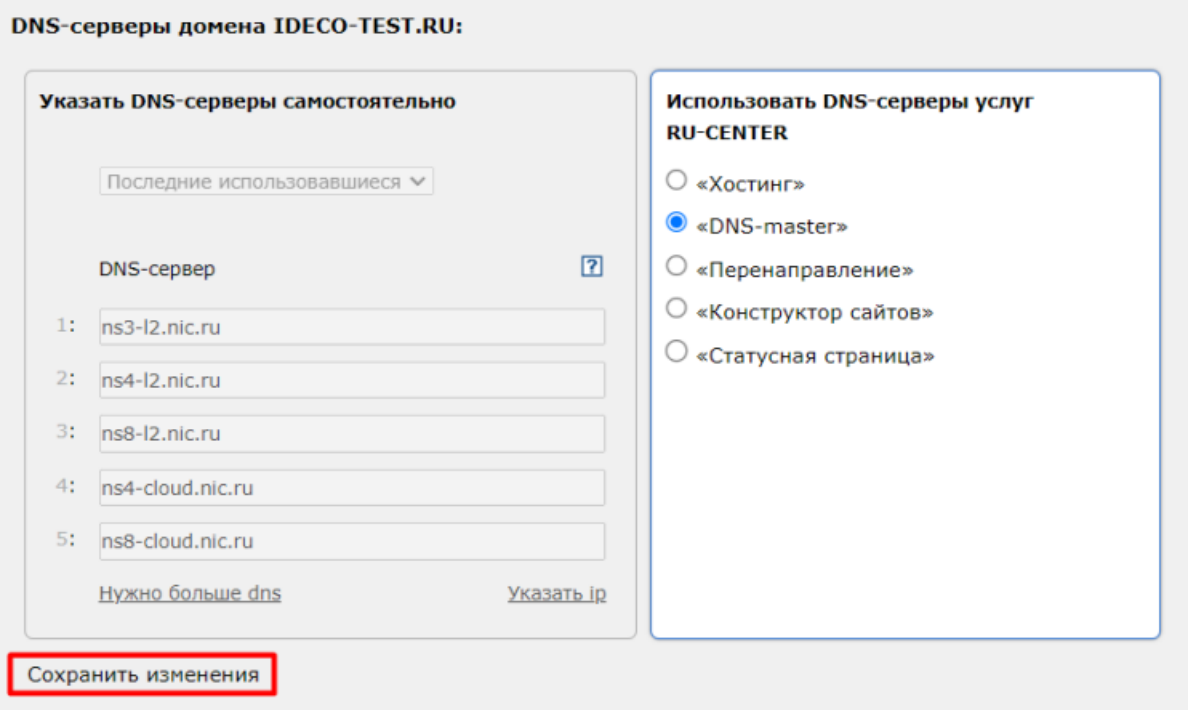
2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:



3. Делегируйте домен, отредактировав настройки DNS-серверов:

- **Указать DNS-серверы самостоятельно** - укажите DNS-серверы. Если домен был приобретен на хостинге RU-CENTER, поля заполнятся автоматически;
- **Использовать DNS-серверы услуг RU-CENTER** - выберите **DNS-master**.

Сохраните изменения:



Домен будет делегирован с заданным списком DNS-серверов. Это может занять несколько часов.

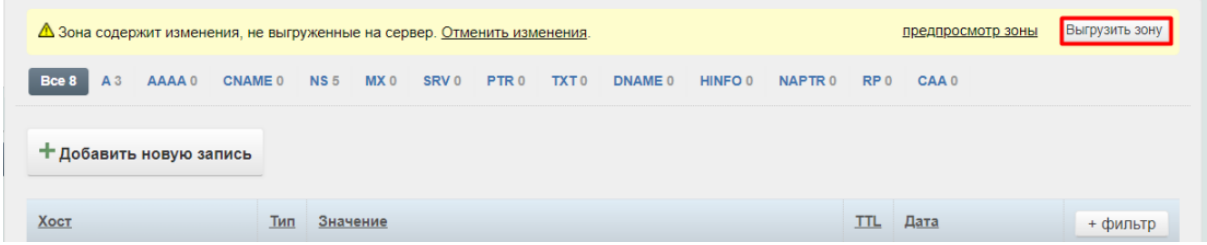
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

5. Выберите нужный домен или добавьте (если домен был приобретен на стороннем ресурсе), нажав соответствующую кнопку.

6. Добавьте две записи по кнопке **Добавить новую запись**:

- Первая запись:
  - Name - укажите знак `@`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco NGFW (указывается в разделе *Техническая поддержка -> Информация для технической поддержки*);
  - TTL - оставьте не заполненным.
- Вторая запись:
  - Name - укажите `www`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco NGFW;
  - TTL - оставьте не заполненным.

7. Нажмите кнопку **Выгрузить зону**:



8. Перейдите в раздел **DDNS** в Ideco NGFW и заполните поля:

- **Домен на DNS-хостинге nic.ru** - укажите приобретенный домен;
- **Логин от API** и **Пароль от API** - для получения логина и пароля перейдите по ссылке Динамический DNS и нажмите **Получить**:

9. Сохраните настройки в Ideco NGFW, нажав соответствующую кнопку.

18.11 DHCP-сервер

Подсказка: Название службы раздела **DHCP**: `ideco-dnsmasq`.
Список служб для других разделов доступен по *ссылке*.

18.11.1 Интерфейс Ideco NGFW:

- Вкладка **Настройки** - позволяет настроить диапазон IP-адресов для автоматического назначения
- Вкладка **Привязка IP к MAC** - позволяет сформировать статические привязки IP-адресов к MAC-адресам
- Вкладка **Мониторинг аренды** - позволяет получить сведения об аренде IP-адреса для устройства

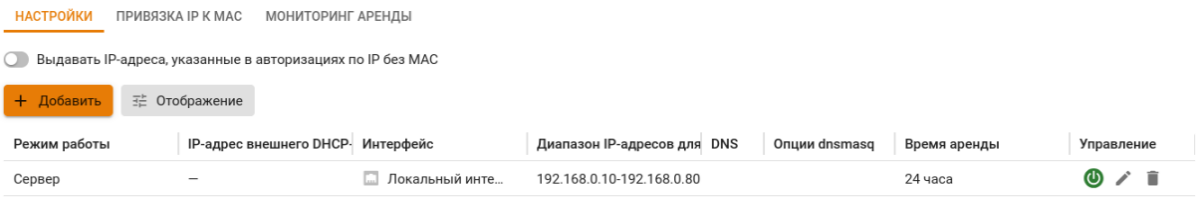
Сетевые устройства в локальной сети должны быть настроены на автоматическое получение сетевых реквизитов от DHCP-сервера. Таким образом, клиенты отправляют широковещательный запрос в сегмент локальной сети, а сервер перехватывает и отправляет на эти запросы ответы, содержащие необходимые настройки для клиента.

Подсказка: Для сортировки строк таблицы по определенному столбцу нажмите на этот столбец в заголовке таблицы.

Для управления настройками DHCP-сервера перейдите в раздел **Сервисы -> DHCP-сервер**.

> **Предупреждение:** На локальном интерфейсе Ideco NGFW, участвующем в раздаче адресов, должен быть настроен статический IP адрес.

При использовании DHCP-сервера переключите ползунок в левом верхнем углу в положение **Включен**:



18.11.2 Настройки

Если сервер Ideco NGFW является шлюзом и DNS-сервером для всех сетевых устройств локальной сети, настройка службы ограничивается определением диапазона IP-адресов.

Подсказка: При включении опции **Выдавать IP-адреса, указанные в авторизациях по IP без MAC**, будут выдаваться IP-адреса (исключение - правило с IP+MAC), использованные в качестве фактора авторизации пользователя (раздел *Авторизация*).

Если на Ideco NGFW настроен *перехват DNS*, то резолвинг имен будет производиться при помощи сервера, указанного в настройках перехвата DNS.

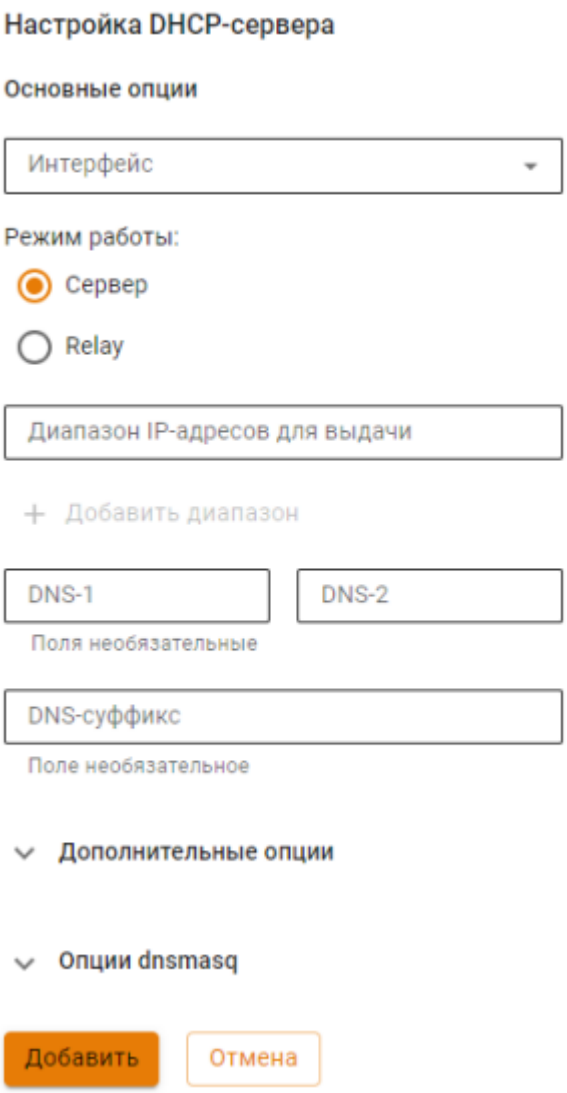
Настройка DHCP-сервера делится на три блока:

- **Основные опции** - задаются диапазоны IP-адресов и DNS-серверы;
- **Дополнительные опции** - статические маршруты, адреса WINS-серверов, время аренды, PXE Boot и WPAD;
- **Опции dnsmasq** - предназначены для ручного задания опций DHCP, передаваемых сервером клиенту при получении сетевых реквизитов от DHCP-сервера.

Основные опции

Режим работы Сервер:

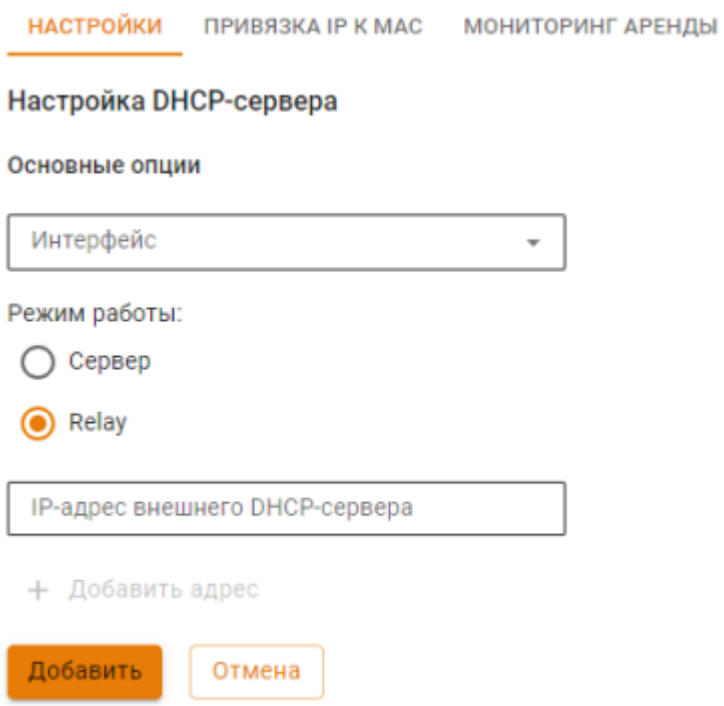
Выберите режим работы **Сервер**, чтобы настроить выдачу IP-адресов на Ideco NGFW. Заполните следующие поля:



- **Интерфейс** - выберите интерфейс, который будет участвовать в раздаче адресов;
- **Диапазон IP-адресов для выдачи** - укажите диапазон IP-адресов, которые будут выданы устройствам в локальной сети, должен входить в одну из подсетей выбранного интерфейса. Размер диапазона не должен превышать 256 адресов;
- **DNS-1** и **DNS-2** - укажите IP-адреса DNS-серверов для устройств локальной сети. Если ни одно из полей не заполнено, то DNS-сервером для всех сетевых устройств локальной сети будет являться Ideco NGFW;
- **DNS-суффикс** - введите домен, прибавляющийся к запрашиваемому имени устройства в локальной сети. Поле не обязательное. Нужен, для того, чтобы в локальной сети вводить не полное имя компьютера вместе с доменом, а только само имя.

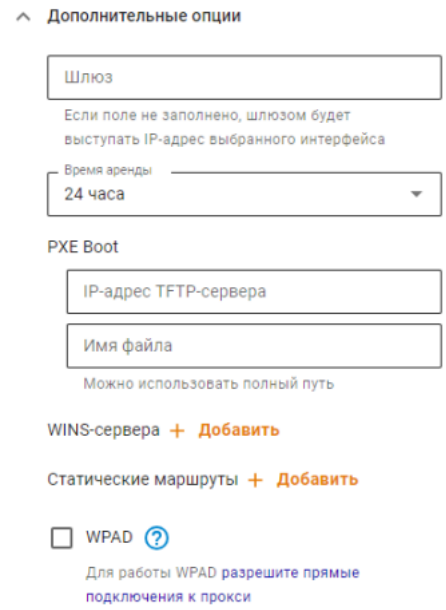
Режим работы Relay:

Выберите режим работы **Relay**, если IP-адреса будет выдавать внешний DHCP-сервер. Выберите интерфейс, который будет участвовать в раздаче IP-адресов, и введите IP-адрес внешнего DHCP-сервера:



Включить/выключить, редактировать или удалить правила для выдачи IP-адресов можно кнопками управления в колонке **Управление**.

Дополнительные опции



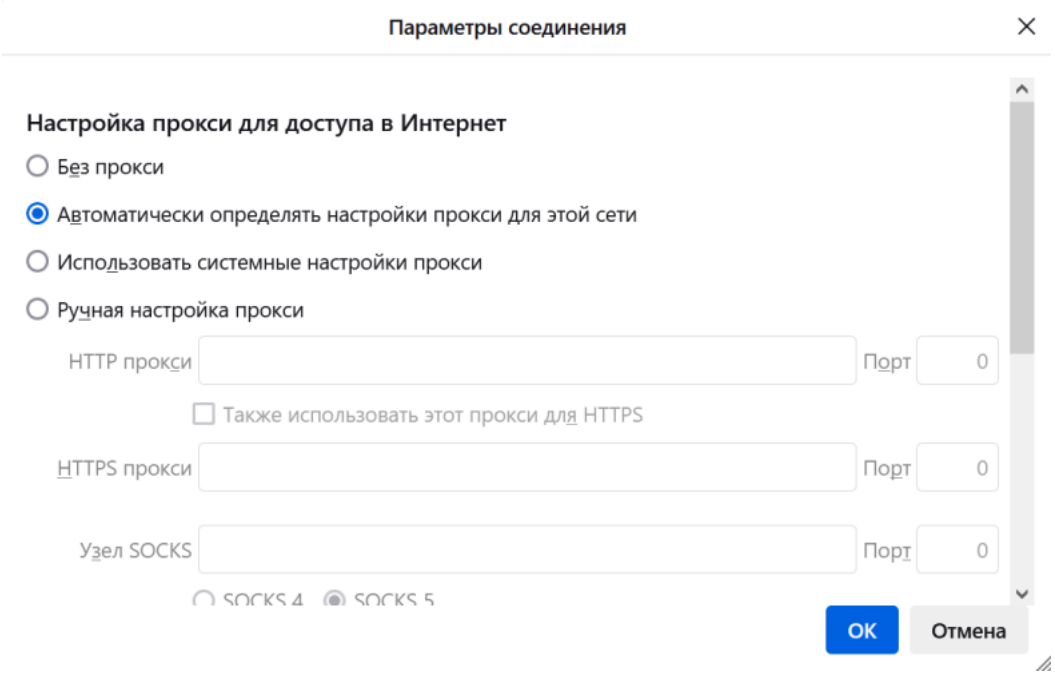
- **Шлюз** - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса;
- **Время аренды** - время, на которое выдается IP-адрес;
- **PXE Boot** - IP-адрес TFTP-сервера для настройки загрузки образа по сети;
- **WINS-сервера** - IP-адрес WINS-сервера;

- **Статические маршруты** - подсеть и шлюз для указания статического маршрута;
- **WPAD** - протокол автоматической настройки прокси.

При включении опции WPAD Ideco NGFW будет автоматически генерировать файл с настройками подключения к прокси и передавать его хостам в локальной сети, на которых настроено получение IP по DHCP. Локальные сети в файле конфигураций будут добавлены в исключения из прокси.

Подсказка: Для работы WPAD необходимо разрешить прямые подключения к прокси в разделе **Сервисы -> Прокси**.

Подсказка: Браузеры Google Chrome и Microsoft Edge автоматически примут настройки прокси, переданные хостам по DHCP. В Mozilla Firefox необходимо будет дополнительно зайти в **Настройки браузера -> Настройки прокси** и выбрать пункт **Автоматически определять настройки прокси для этой сети**:



Опции dnsmasq

Подсказка: Опция dnsmasq имеет больший приоритет чем опция, внесенная в блок **Основные опции** или **Дополнительные опции**.

Строка **Значение** может содержать только одну опцию.

Формат записи опции соответствует части записи опции в конфигурации dnsmasq - `[vendor:[<vendor-class>],][<opt>|option:<opt-name>],[<value>[,<value>]]`, где:

- `[vendor:[<vendor-class>],]` - вендор, необязательно:
- `[<opt>|option:<opt-name>]` - числовое или строковое (напр. option:nis-server) обозначение опции;
- `[<value>[,<value>]]` - одно или несколько значений опции через запятую.

Установите флаг **Force** если требуется отправлять опцию DHCP-клиенту, даже если он ее не запрашивал.

Предупреждение: **Важно**: некорректно заданные dnsmasq-опции могут привести к остановке работы раздела **DHCP-сервер**. Статус раздела сменится на `Модуль "dnsmasq" не смог запуститься` и `Служба 'ideco-dnsmasq' остановлена`.

Для поиска некорректно заданной опции выполните действия:

- Перейдите в раздел **Отчеты и журналы -> Системный журнал**;
- В столбце **Сообщение** найдите запись формата `bad option at line 15 of /run/ideco-dhcp-server-backend/dnsmasq.conf`. В записи указано, на какую строку в конфиге нужно обратить внимание;
- Перейдите в раздел **Управление сервером -> Терминал**;
- Откройте конфиг `/run/ideco-dhcp-server-backend/dnsmasq.conf` и найдите нужную строку.

Расширение базовых опций, отсылаемых DHCP-сервером для конфигурирования IP-телефонов Avaya:

Для IP-телефонов Avaya может потребоваться передать оборудованию опции 176 и 242. Для ознакомления со списком опций для конкретной модели обратитесь к документации нужной модели Avaya.

1. Перейдите к созданию настройки DHCP-сервера (**Сервисы -> DHCP-сервер -> Настройки -> Добавить**).

2. Заполните **Основные** и **Дополнительные** опции.

3. Нажмите **Добавить опцию** и заполните 176 опцию. Она используется для указания голосового сервера:

```
176,"MCIPADD=1.2.3.4,MCPORT=1719"
```

4. После добавления 176 опции добавьте 242. Она используется для серверов передачи данных:

```
242,"MCIPADD=1.1.1.2,MCPORT=1719"
```

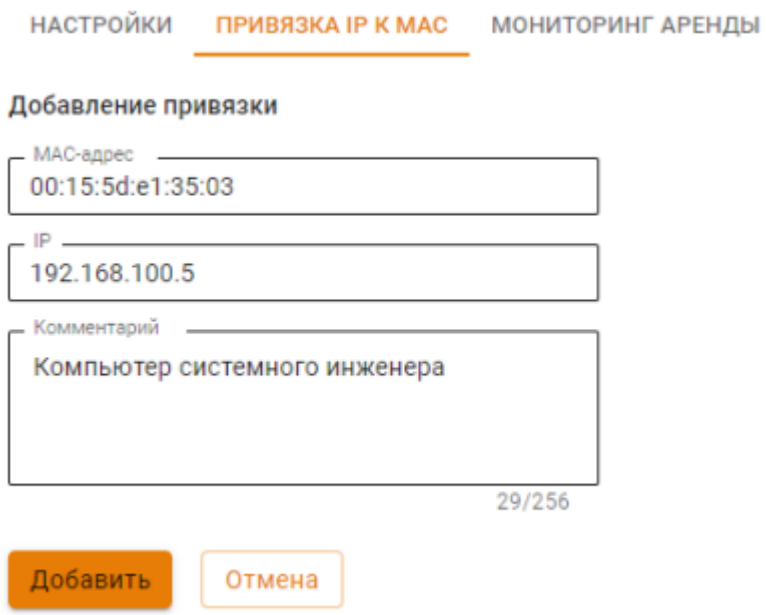
После сохранения настроек IP-телефония Avaya будет получать от DHCP-сервера расширенный список опций.

18.11.3 Привязка IP к MAC

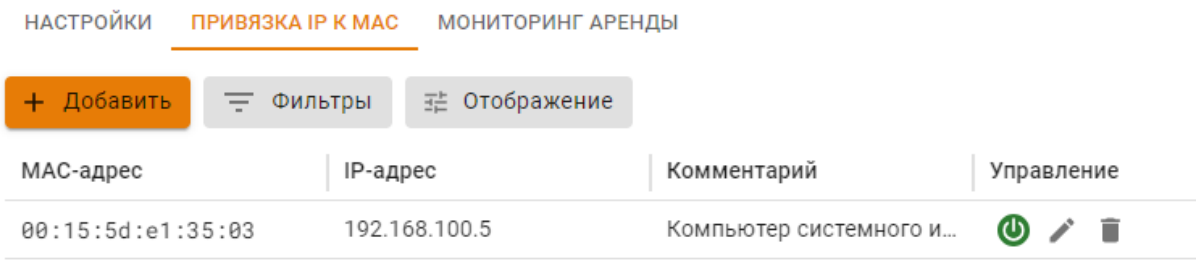
Для настройки в DHCP-сервере привязки IP-адреса к MAC-адресу необходимо:

1. В разделе **Сервисы -> DHCP** выберите вкладку **Привязка IP к MAC**.

2. Создайте правило привязки **IP к MAC**:



Пример созданного правила привязки показан ниже на скриншоте:



Для проверки созданного правила на компьютере с указанным в правиле MAC-адресом получите IP-адрес по DHCP и проверьте результат с помощью команды `ipconfig /all` (для операционной системы Windows):

```
C:\Windows\system32>ipconfig /all | findstr адрес
   Физический адрес. . . . . . . . . . . : 00-15-5D-E1-35-03
   Локальный IPv6-адрес канала . . . : fe80::85df:8421:a811:c8be%4(Основной)
   IPv4-адрес. . . . . . . . . . . . . . : 192.168.100.5(Основной)

C:\Windows\system32>
```

При наличии большого количества привязок в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW.

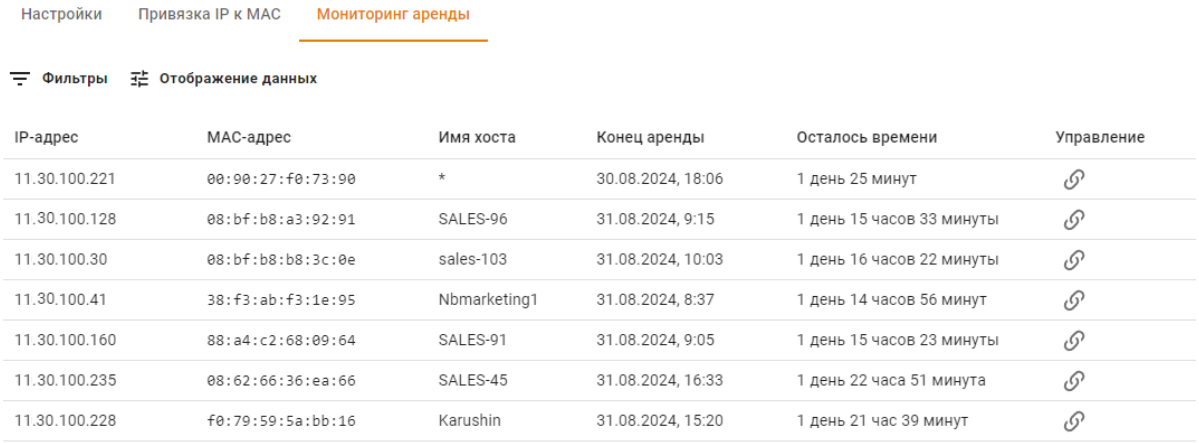
Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (`01-02-03-04-05-06`). В настройках Ideco NGFW октеты MAC-адреса разделяются только двоеточиями (`01:02:03:04:05:06`).

Настройка DHCP-сервера для Wi-Fi сетей:

При настройке Wi-Fi сетей может понадобиться настройка DHCP-сервера. Для получения подробной информации перейдите в раздел *Wi-Fi-сети*.

18.11.4 Мониторинг аренды

Содержит информацию об аренде IP-адресов для устройств. Для поиска воспользуйтесь кнопкой **Фильтры**:



IP-адрес	MAC-адрес	Имя хоста	Конец аренды	Осталось времени	Управление
11.30.100.221	00:90:27:f0:73:90	*	30.08.2024, 18:06	1 день 25 минут	
11.30.100.128	08:bf:b8:a3:92:91	SALES-96	31.08.2024, 9:15	1 день 15 часов 33 минуты	
11.30.100.30	08:bf:b8:b8:3c:0e	sales-103	31.08.2024, 10:03	1 день 16 часов 22 минуты	
11.30.100.41	38:f3:ab:f3:1e:95	Nbmarketing1	31.08.2024, 8:37	1 день 14 часов 56 минут	
11.30.100.160	88:a4:c2:68:09:64	SALES-91	31.08.2024, 9:05	1 день 15 часов 23 минуты	
11.30.100.235	08:62:66:36:ea:66	SALES-45	31.08.2024, 16:33	1 день 22 часа 51 минута	
11.30.100.228	f0:79:59:5a:bb:16	Karushin	31.08.2024, 15:20	1 день 21 час 39 минут	

Для привязки IP к MAC нажмите на кнопку в столбце **Управление**.

18.12 NTP-сервер

Подсказка: Название службы раздела **NTP**: `chronyd`.
Список служб для других разделов доступен по *ссылке*.

NTP - протокол для синхронизации времени. Он позволяет установить точное время на компьютере, используя информацию от специальных серверов времени. По умолчанию работает на 123/UDP-порту.

18.12.1 Принцип работы

Серверы времени, используемые в NTP, имеют свою иерархию:

- Верхний уровень иерархии занимают официальные источники времени.
- На следующем уровне находятся сервера времени, которые синхронизируют свои часы с официальными источниками времени.
- На последнем уровне находятся клиенты NTP, которые получают информацию от серверов времени.

Ideco NGFW может выступать в роли сервера времени.

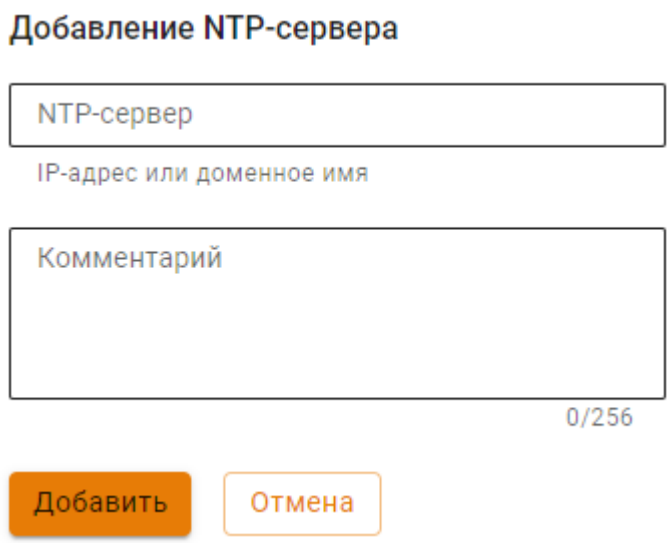
18.12.2 Настройка Ideco NGFW

Для настройки перейдите в раздел **Сервисы -> NTP-сервер**.

При включении опции **NTP-сервер на всех локальных интерфейсах (порт 123/UDP)**, Ideco NGFW будет доступен в качестве NTP-сервера для локальных клиентов.

При активации **Перехвата NTP-запросов** все запросы локальных клиентов будут обрабатываться NGFW, даже если были отправлены на другой NTP-сервер.

Для добавления NTP-сервера, с которым NGFW будет синхронизировать время, нажмите **Добавить** в левом верхнем углу. Заполните поле **NTP-сервер**, указав IP-адрес или доменное имя:



При наличии большого количества NTP-серверов в таблице воспользуйтесь кнопкой **Фильтры**.

18.13 IPsec

Подсказка: Название службы раздела **IPsec**: `ideco-ipsec-backend`; `strongswan`.
Список служб для других разделов доступен по *ссылке*.

Особенность работы некоторых Cisco: Если в подключении site2site активную сторону представляет Cisco и Child_SA закрывается, то пассивная сторона не сможет отправить пакет в сторону Cisco, пока Cisco не создаст новый Child_SA.

Подсказка: В **Туннельном** режиме работы для создания туннелей используются все внешние интерфейсы со шлюзом по умолчанию и все **Адреса удаленного устройства**, указанные при создании IPsec-подключений.

Выбор конкретного туннеля для обмена трафиком зависит от приоритета внешнего интерфейса в таблице раздела **Балансировка и резервирование**. Приоритет интерфейса определяется местом в таблице: чем выше интерфейс, тем больше у него приоритет.

Интерфейсы без выхода в интернет имеют меньший приоритет по сравнению с интерфейсами с доступом в интернет.

18.13.1 Устройства

Подключение устройств по IPsec позволит обеспечить безопасность сетевых соединений и защитить данные, передаваемые между устройствами.

Воспользуйтесь конфигураторами подключений для MikroTik или Cisco. Они позволяют сгенерировать конфиг, запуск которого на удаленном устройстве установит заранее подготовленные настройки IPsec.

18.13.2 Исходящие подключения

Настройте исходящее подключение, если Ideco NGFW является инициатором подключения, а удаленное устройство - принимающей стороной.

Для настройки исходящего подключения подготовьте:

Тип аутентификации	Требуемые параметры
Сертификат	- Подписанный удаленным устройством **Запрос на подпись сертификата**. Файл запроса скачивается из веб-интерфейса NGFW при создании подключения (), отправляется удаленному устройству и подписанный возвращается для настройки NGFW;- Корневой сертификат удаленного устройства;- Список домашних локальных сетей NGFW, которые будут видны противоположной стороне;- Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	- PSK-ключ. Генерируется на NGFW при создании подключения;- Идентификатор ключа, который потребуется удаленному устройству для идентификации подключения;- Список локальных сетей NGFW, которые будут видны противоположной стороне;- Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

18.13.3 Входящие подключения

Настройте входящее подключение, если удаленное устройство является инициатором подключения, а Ideco NGFW - принимающей стороной.

Для настройки входящего подключения подготовьте:

Тип аутентификации	Требуемые параметры
Сертификат	- Запрос на подпись сертификата (`.csr`), полученный от удаленного устройства;- Список домашних локальных сетей NGFW, которые будут видны противоположной стороне;- Список всех локальных сетей удаленного устройства, которые будут видны противоположной стороне.
PSK	- PSK-ключ, сгенерированный на удаленном устройстве;- Идентификатор удаленной стороны для идентификации входящего подключения;- Список локальных сетей NGFW, которые будут видны противоположной стороне;- Список локальных сетей удаленного устройства, которые будут видны противоположной стороне.

18.13.4 Выбор алгоритмов шифрования на удаленных устройствах

При настройке сторонних устройств необходимо явно указать алгоритмы шифрования, используемые для подключения.
Ideco NGFW не поддерживает устаревшие и небезопасные алгоритмы (MD5, SHA1, AES128, DES, 3DES, blowfish и др.).
При конфигурировании сторонних устройств можно указать несколько поддерживаемых алгоритмов одновременно, так как не все устройства поддерживают современные алгоритмы.

Список алгоритмов и пример использования:

- **Phase 1 (IKE):**
  - encryption (шифрование):
    - **AES256-GCM**;
    - **AES256 (AES256-CBC)**.
  - integrity (hash, целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы;
    - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA256**.
  - prf (функция генерации случайных значений):
    - как правило, настраивается автоматически в зависимости от выбора алгоритмов integrity (поэтому в примере *ниже* значение prf: PRF-HMAC-SHA512);
    - для AES-GCM может потребоваться указать явно. В этом случае по приоритету: **AESXCBC, SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman):
    - **Curve25519 (group 31)**;
    - **ECP256 (group 19)**;
    - **modp4096 (group 16)**;
    - **modp2048 (group 14)**;
    - **modp1024 (group 2)**.
  - Таймауты:
    - **Lifetime**: 14400 сек;

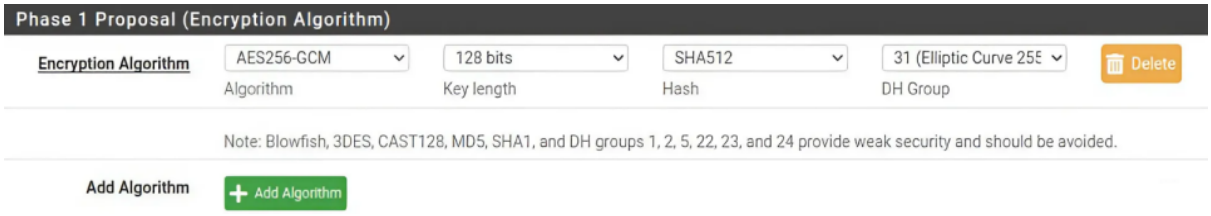
        * **DPD Timeout** (для L2TP/IPsec): 40 сек;
        * **DPD Delay**: 30 сек.

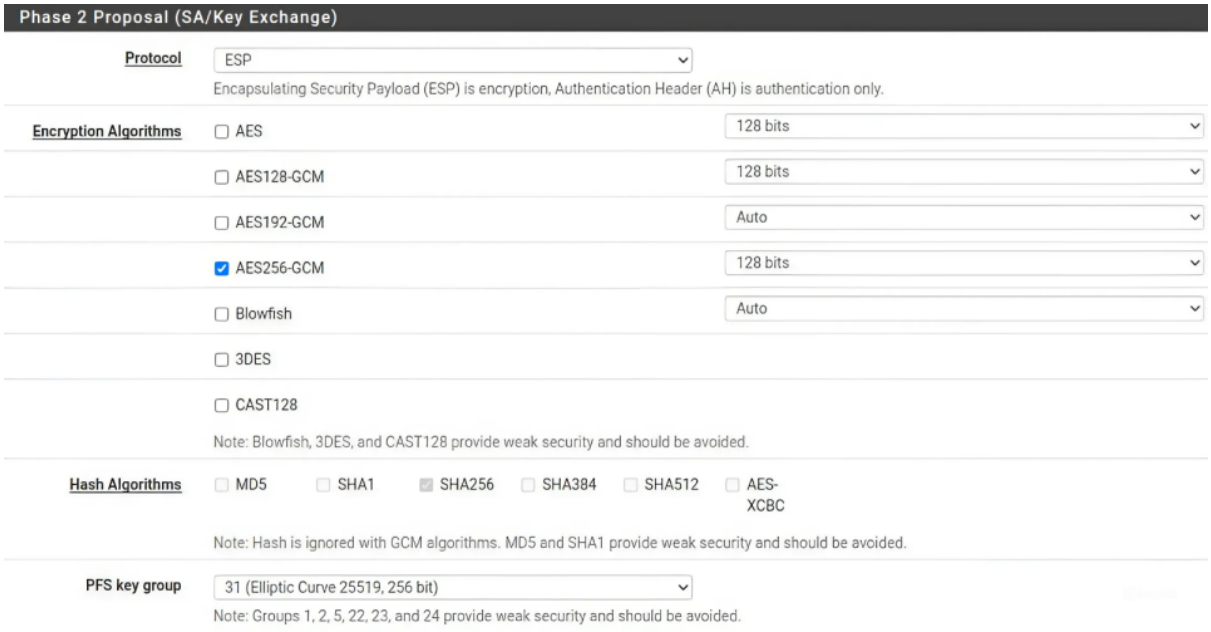
- **Phase 2 (ESP):**
  - encryption (шифрование):
    * **AES256-GCM**;
    * **AES256 (AES256-CBC)**.
  - integrity (целостность):
    * для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы;
    * для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman, PFS). **ВНИМАНИЕ! Если не указать группу, то подключение будет установлено, но через некоторое время не сработает параметр rekey**:
    * **Curve25519 (group 31)**;
    * **ECP256 (group 19)**;
    * **modp4096 (group 16)**;
    * **modp2048 (group 14)**;
    * **modp1024 (group 2)**.
  - Таймаут:
    * **Lifetime**: 3600 сек.

Пример:

- **Phase 1 (IKE)** (нужна одна из строк)**:**
  - AES256-GCM\PRF-HMAC-SHA512\Curve25519;
  - AES256(AES256-CBC)\SHA512\PRF-HMAC-SHA512\ECP384;
  - AES256(AES256-CBC)\SHA256\PRF-HMAC-SHA256\MODP2048.
- **Phase 2 (ESP)** (нужна одна из строк)**:**
  - AES256-GCM\ECP384;
  - AES256(AES256-CBC)\SHA256\MODP2048.

Пример настройки подключения pfSense к Ideco NGFW по IPsec:



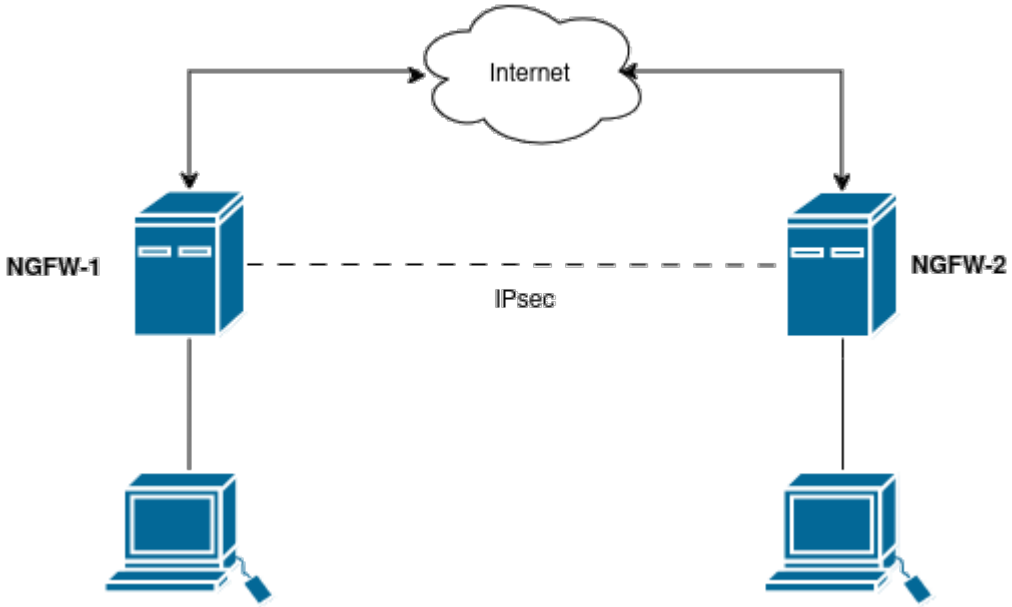


18.13.5 Изменение настроек созданных IPsec-подключений

Начиная с 16 версии в Ideco NGFW появилась возможность изменять настройки **Домашних локальных сетей** и **Удаленных локальных сетей** для IPsec-подключений. После редактирования подсетей произойдет перезапуск всех IPsec-соединений, в которых использовались измененные подсети:

Подсказка: Изменить настройки подсетей можно в настройках IPsec-подключения и в разделе **Правила трафика -> Объекты -> Подсеть**.

18.13.6 Подключение между двумя Ideco NGFW в туннельном режиме работы



Для создания IPsec-подключения между Ideco NGFW нужно настроить на одном NGFW входящее подключение, а на другом NGFW - исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключе-

ние, а на **NGFW-2** - входящее подключение.

Шаг 1. Проверка условий подключения

Перед созданием подключения убедитесь, что:

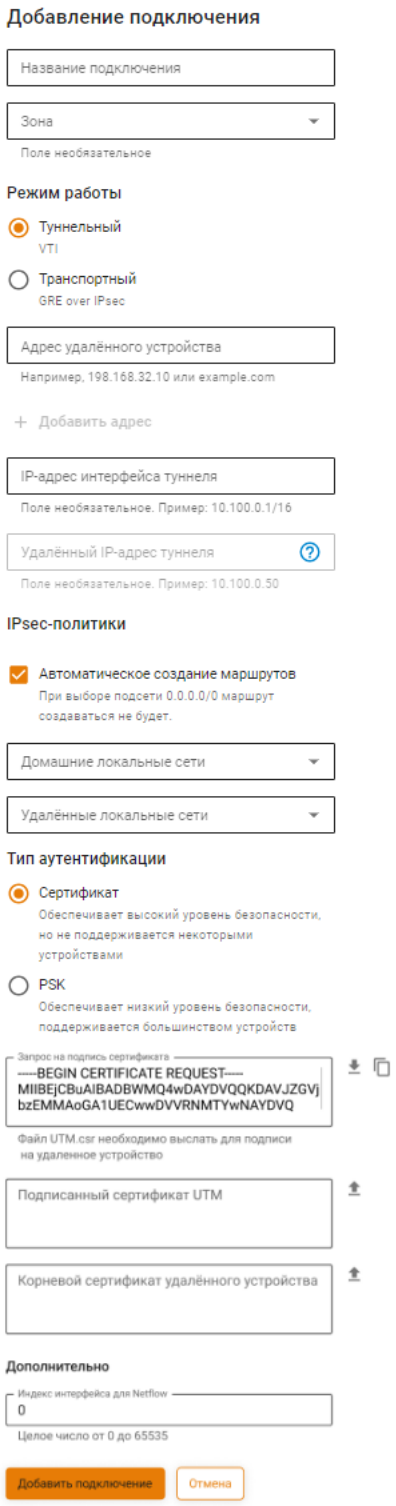
- На **NGFW-1** и **NGFW-2 правильно настроены временные зоны**. Без этого подключение не установится;
- Для работы IPsec все подсети, участвующие в соединениях, не пересекаются;
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. **Входящее подключение должно настраиваться на сервере с белым IP-адресом**;
- Пользовательские правила из раздела **Правила трафика -> Файрвол -> INPUT** не блокируют входящий трафик для протоколов ESP и UDP (порты 500 и 4500), поступающий на внешние интерфейсы **NGFW-2**;
- Сети для VPN-подключений у **NGFW-1** и **NGFW-2** не пересекаются.

Шаг 2. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Название подключения** - максимальное количество символов - 42;
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым;
- **Режим работы** - выберите **Туннельный**;
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес. Адресов может быть несколько;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, запол-

няется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;

- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**. Поле необязательное, заполняется для получения статистики обмена пакетами;
- **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW;
- **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW;
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните его для настройки входящего подключения;
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните его для настройки входящего подключения. Заполните поле **Идентификатор UTM**.

Подсказка: Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

---

3. Выполните действие для нужного типа аутентификации:

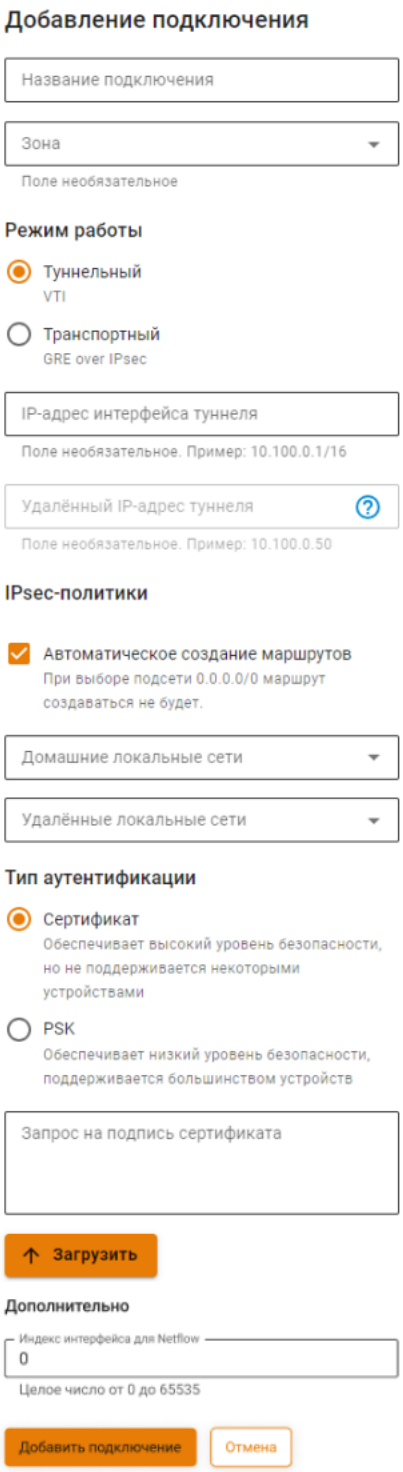
- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 3**;
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 3** для настройки входящего подключения на **NGFW-2**.

Шаг 3. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Название подключения** - максимальное количество символов - 42;
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-1**. Поле необязатель-

ное, заполняется для получения статистики обмена пакетами;

- **Домашние локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с другого NGFW;
- **Удаленные локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с текущего NGFW;
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - **Сертификат** - заполните поле **Запрос на подпись сертификата**, вставив значение сохраненное при первоначальной настройке исходящего подключения;
  - **PSK** - заполните поле **PSK ключ**, вставив значение сохраненное при первоначальной настройке исходящего подключения. Заполните поле **Идентификатор удаленной стороны**.

3. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Действия для доступа к удаленным локальным сетям NGFW:

- Укажите сеть в поле **Удаленные локальные сети**;
- Добавьте статический маршрут до этой сети.

Для автоматического создания статического маршрута до удаленных локальных сетей NGFW активируйте опцию **Автоматическое создание маршрутов**.

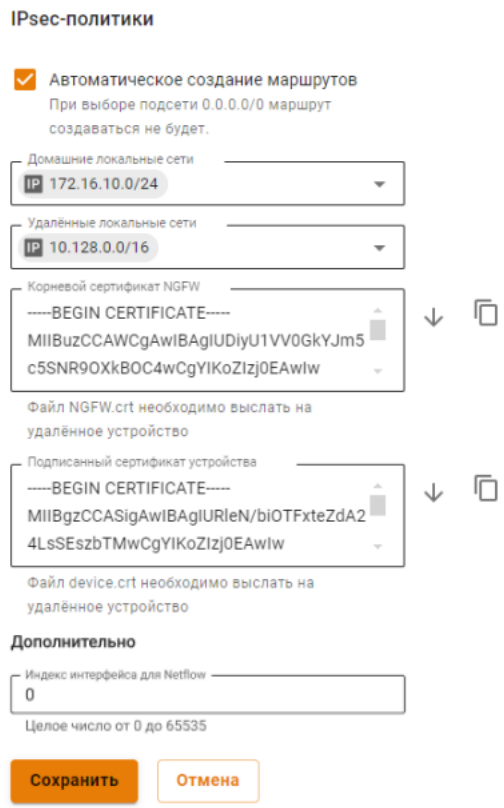
Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно вручную добавить маршруты в разделе **Сервисы -> Маршрутизация**.

Если был выбран тип аутентификации **PSK**, то настройка завершена.
Если был выбран тип аутентификации **Сертификат**, то выполните **Шаг 4**.

Шаг 4. Донастройка исходящего подключения с типом аутентификации Сертификат

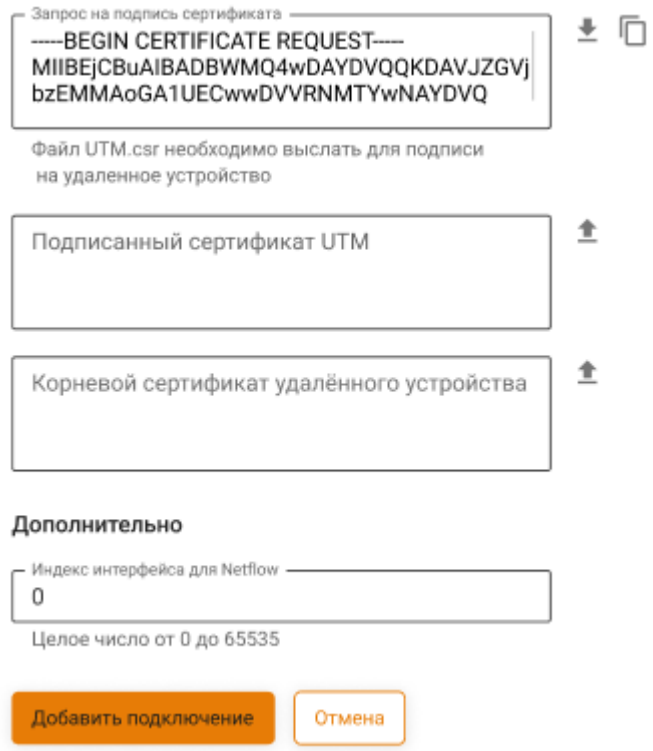
1. В **NGFW-2** перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите  по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** значениями, ранее скопированными из **NGFW-2**:



5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Действия для доступа к удаленным локальным сетям NGFW:

- Укажите сеть в поле **Удаленные локальные сети**;
- Добавьте статический маршрут до этой сети.

Для автоматического создания статического маршрута до удаленных локальных сетей NGFW активируйте опцию **Автоматическое создание маршрутов**.

Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно вручную добавить маршруты в разделе **Сервисы -> Маршрутизация**.

Подсказка: Если соединение по IPsec не устанавливается, воспользуйтесь *статьей*.

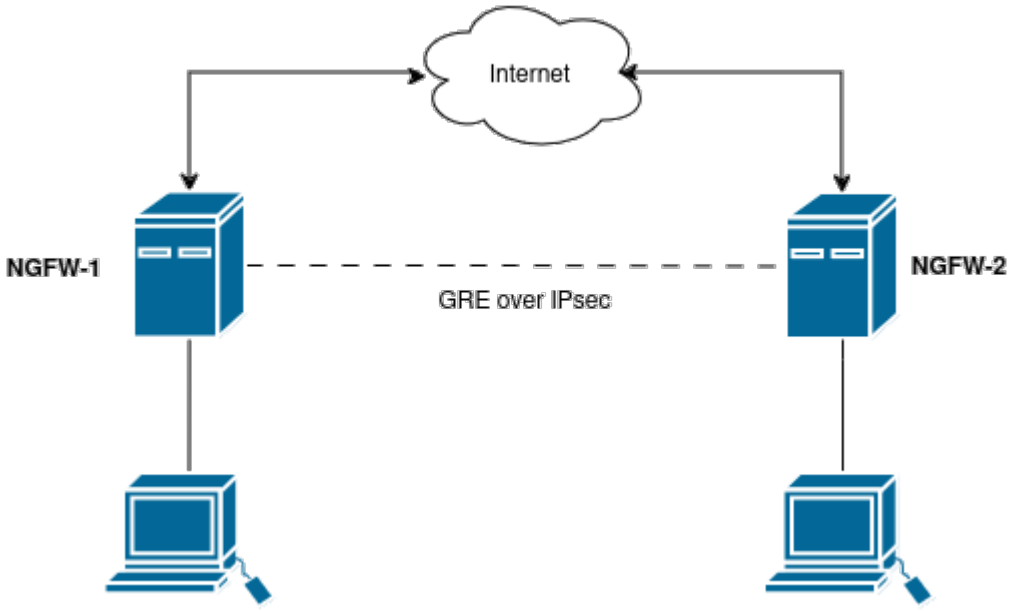
Настройка доступа к локальным сетям по VPN из NGFW-1 к NGFW-2

Для доступа к локальным сетям по VPN из **NGFW-1** к **NGFW-2** выполните действия:

1. Перейдите к редактированию настроенного IPsec-подключения на **NGFW-2**.

2. Укажите в поле **Домашние локальные сети** сеть, используемую для VPN в **NGFW-2**.

18.13.7 Подключение между двумя Ideco NGFW в транспортном режиме работы



Подсказка: GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

При замене/перевыпуске корневого сертификата в разделе *Сертификаты*, IPsec-подключения перестанут работать и их необходимо будет пересоздать;

Предупреждение: Перед настройкой убедитесь, что:

- В каждой из подключаемых сторон **правильно настроена временная зона**. Без этого установить подключение невозможно;
- Пользовательские правила из раздела **Правила трафика -> Файрвол -> INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протоколов ESP и UDP (порты 500 и 4500);
- Пользовательские правила из раздела **Правила трафика -> Файрвол -> INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протокола GRE;
- Ни один Ideco NGFW не находится за NAT, так как в таком случае подключение двух Ideco NGFW в транспортном режиме недоступно;
- Все IP-подсети, участвующие в соединениях не должны пересекаться и, тем более, не должны совпадать;
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. Входящее подключение должно настраиваться на сервере с белым IP-адресом;
- Сети для VPN-подключений у двух NGFW не пересекаются.

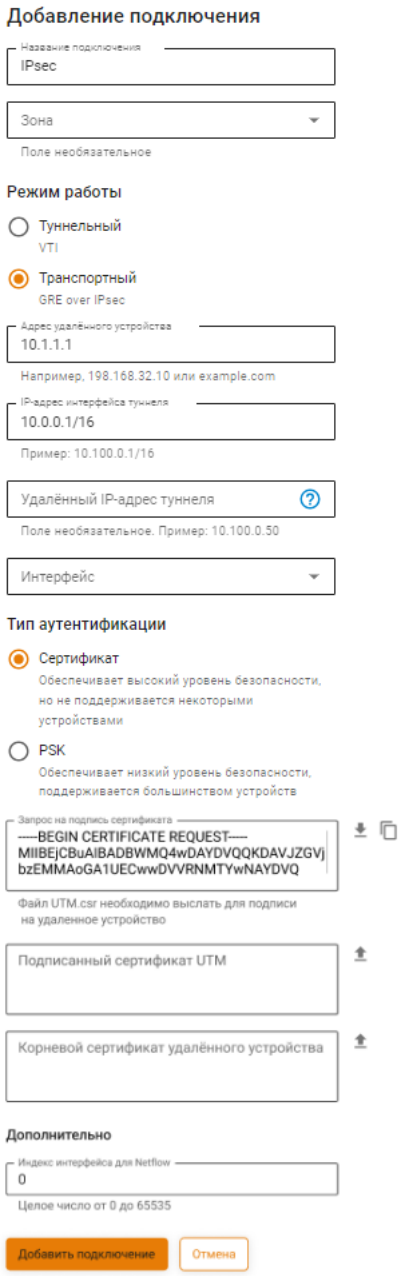
Для создания IPsec подключения между Ideco NGFW нужно настроить на одном NGFW входящее подключение, а на другом NGFW исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключение, а на **NGFW-2** входящее подключение.

Шаг 1. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - максимальное количество символов 42;
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым;
- **Режим работы** - выберите **Транспортный**;
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение;
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его IP-адрес, доступный с сетевого интерфейса, указанного в поле выше;
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:

– При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните его для настройки входящего подключения;

– При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните его для настройки входящего подключения. Заполните поле **Идентификатор NGFW**.

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

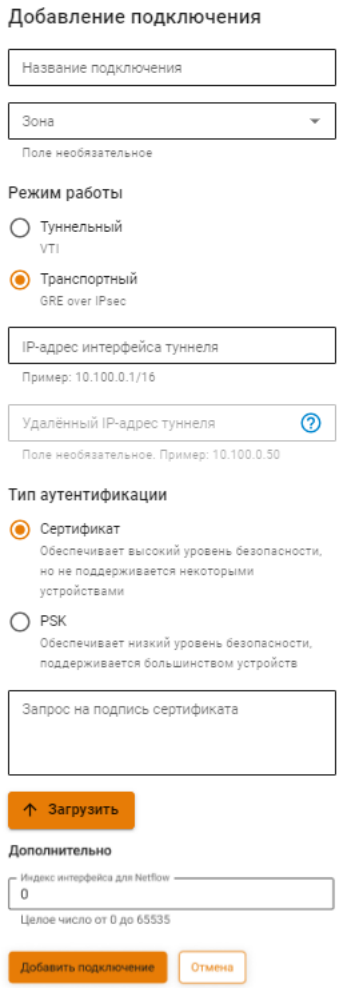
4. Если тип аутентификации - **PSK**, проверьте правильность заполнения полей и нажмите **Добавить подключение** и перейдите к **Шагу 2**. Если тип аутентификации - **Сертификат**, **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 2** для настройки входящего подключения на другом NGFW.

Шаг 2. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - максимальное количество символов - 42;
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым:
- **Режим работы** - выберите **Транспортный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;

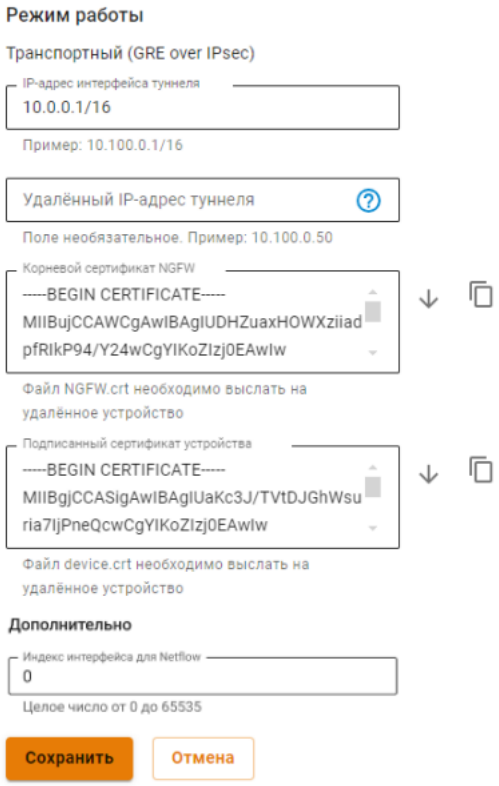
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интрефейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - **Сертификат** - заполните поле **Запрос на подпись сертификата**, вставив значение сохраненное при первоначальной настройке исходящего подключения;
  - **PSK** - заполните поле **PSK ключ**, вставив значение сохраненное при первоначальной настройке исходящего подключения.Заполните поле **Идентификатор удаленной стороны**.
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Шаг 3. Донастройка исходящего подключения с типом аутентификации Сертификат

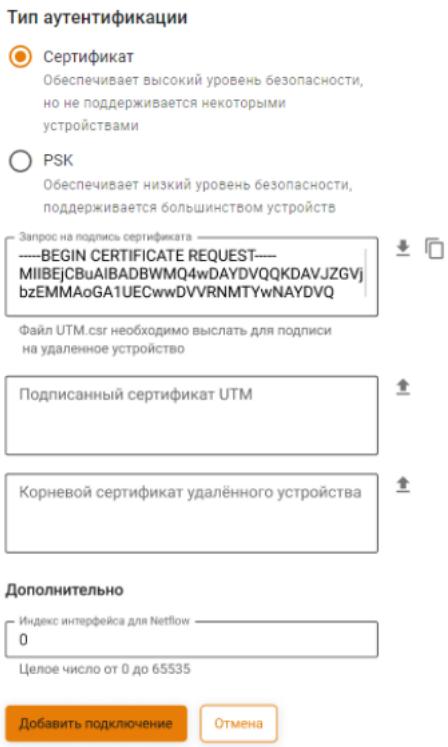
1. В **NGFW-2** перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** ранее скопированным значением при редактировании входящего подключения:



5. Нажмите **Сохранить**.

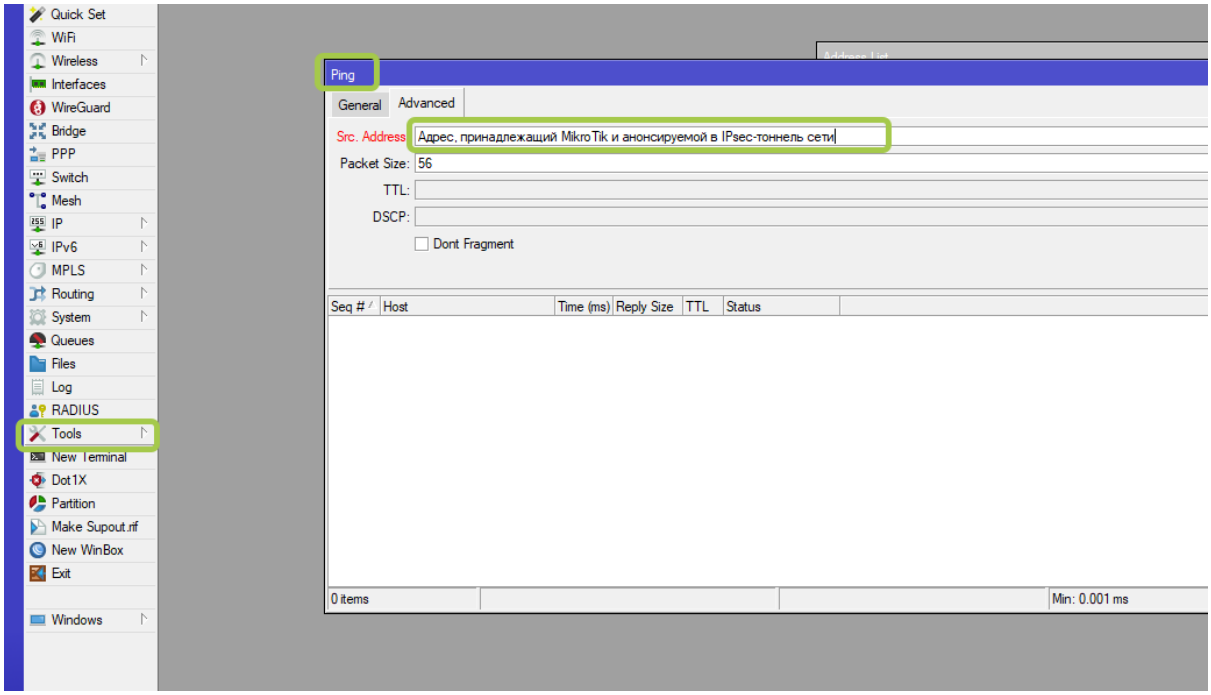
18.13.8 Подключение Ideco NGFW и Mikrotik

Подсказка: При объединении сетей с помощью VPN локальные сети в разных офисах не должны пересекаться.

Для корректной работы подключений по сертификатам синхронизируйте время на MikroTik по NTP (например, предоставьте доступ в интернет).

Исходящие IPsec-подключения по сертификатам к MikroTik ниже версии 6.45 не работают из-за невозможности использования современных криптоалгоритмов.

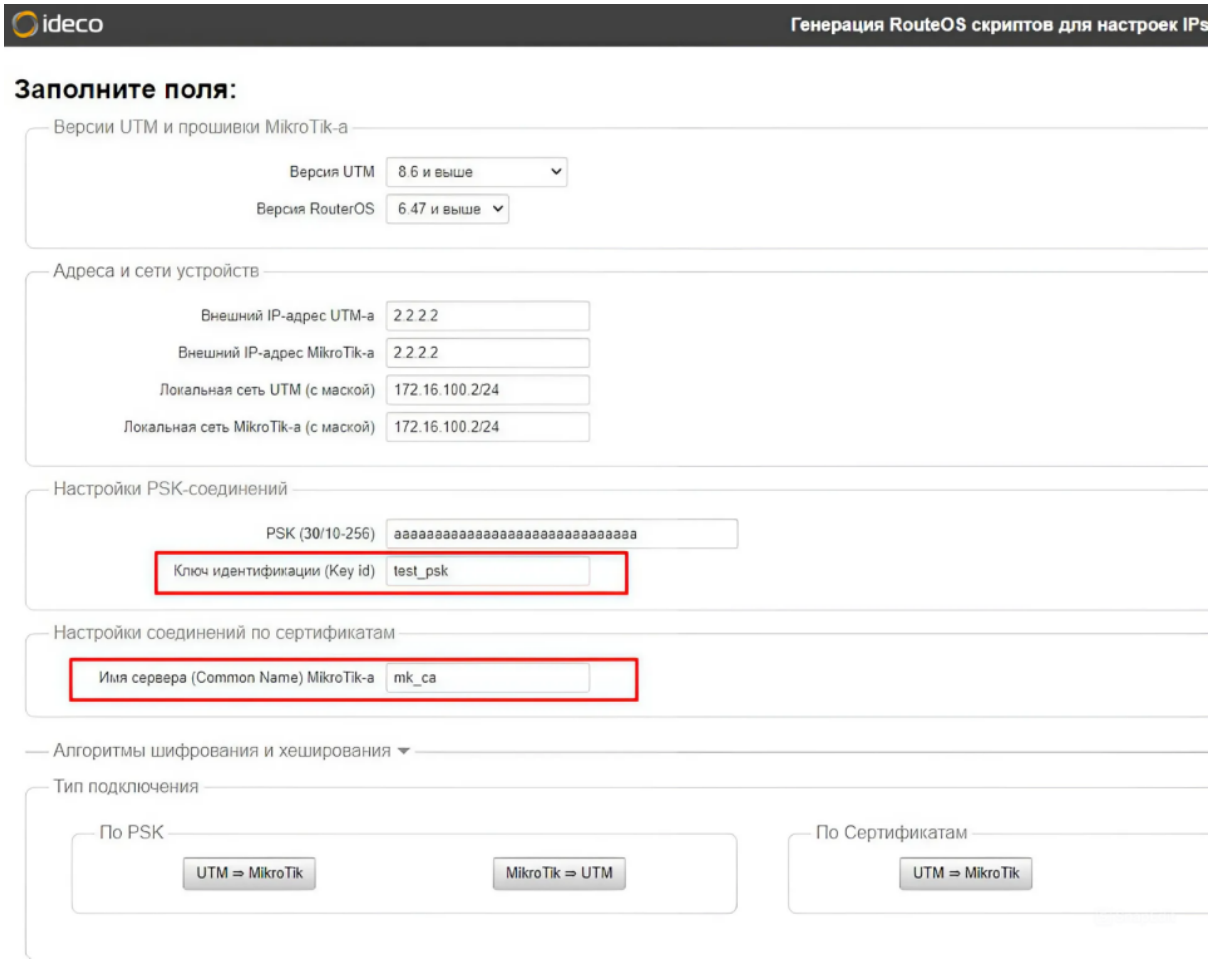
Подсказка: Для проверки доступности анонсируемых сетей Ideco NGFW с MikroTik указывайте IP-адрес источника:



Подключение в Туннельном режиме

При использовании нашего конфигуратора скриптов настроек MikroTik есть несколько особенностей:

- При подключении нескольких устройств MikroTik к одному Ideco NGFW по PSK указывайте разные **Идентификаторы ключа (key-id)** для каждого устройства;
- При подключении нескольких устройств MikroTik к одному Ideco NGFW по сертификатам указывайте разные **Имена сервера** (Common Name) для каждого устройства:



Подключение от Ideco NGFW к MikroTik

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на Ideco NGFW:

1. Откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**, нажмите **Добавить** и заполните поля:

Добавление подключения

Название подключения
Тестовое подключение

Зона

Поле необязательное

Режим работы

- (•) Туннельный
  VTI
- ( ) Транспортный
  GRE over IPsec

Адрес удалённого устройства
172.16.10.3

Например, 198.168.32.10 или example.com

+ Добавить адрес

IP-адрес интерфейса туннеля

Поле необязательное. Пример: 10.100.0.1/16

Удалённый IP-адрес туннеля

Формат: 10.100.0.50
Заполните «IP-адрес интерфейса туннеля» и «Удалённый IP-адрес туннеля» для получения статистики о потере пакетов, средней задержке и джиттере. Они должны находиться в одной подсети.

IPsec-политики

- [x] Автоматическое создание маршрутов
  При выборе подсети 0.0.0.0/0 маршрут создаваться не будет.

Домашние локальные сети
IP 192.168.105.0/24

Удалённые локальные сети
IP 192.168.100.0/24

Тип аутентификации

- ( ) Сертификат
  Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
- (•) PSK
  Обеспечивает низкий уровень безопасности, поддерживается большинством устройств

PSK ключ
••••••••••••••••••••••••••••••

Тип идентификатора
auto

NGFW идентификатор
test_psk

Зависит от настроек удалённого устройства

Дополнительно

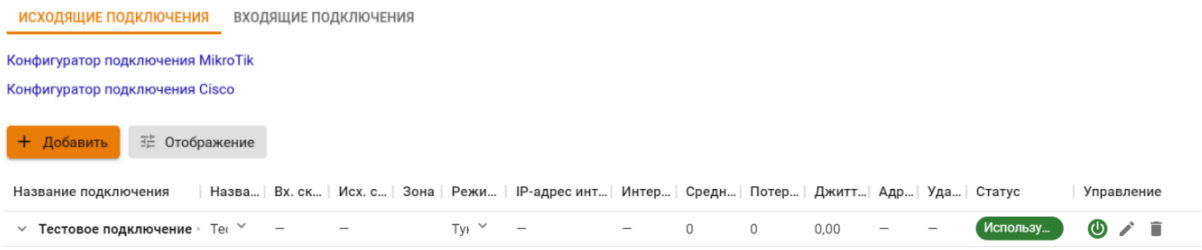
Индекс интерфейса для Netflow
0

Целое число от 0 до 65535

Добавить подключение Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Туннельный**;
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне;
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне;
- **Тип аунтификации** - выберите **PSK**. В поле **PSK-ключ** будет сгенерирован случайный PSK-ключ. Он потребуется для настройки подключения в MikroTik;
- **Тип идентификатора** - выберите **auto**;
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего IPsec-подключения в MikroTik;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. После заполнения всех полей нажмите **Добавить подключение**. В списке подключений появится созданное подключение:



Настройка входящего IPsec-подключения на MikroTik:

Настройку устройства MikroTik можно осуществить несколькими способами:

- GUI;
- Консоль устройства;
- Конфигурационными скриптами (https://mikrotik.ideco.ru/).

После генерации скрипта необходимо открыть раздел **System -> Scripts**, создать скрипт, вставить в него код, сгенерированный конфигуратором, и запустить.

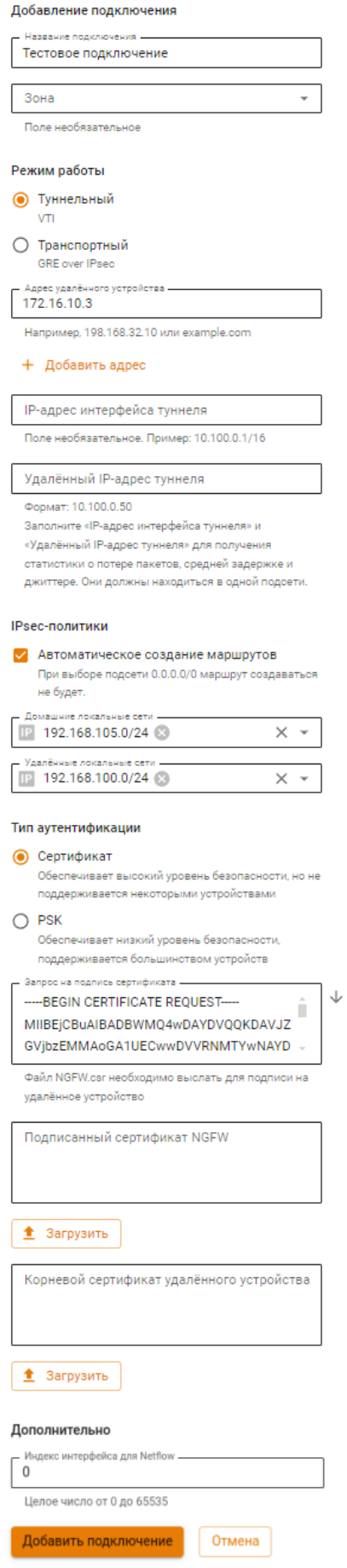
Тип аутентификации Сертификат

Подключение по сертификатам является более безопасным по сравнению с PSK.

Настройка исходящего IPsec-подключения на Ideco NGFW:

Сгенерируйте запрос на подпись сертификата:

1. В Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**, нажмите **Добавить** и заполните поля:


Добавление подключения
Название подключения
Тестовое подключение
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
Адрес удалённого устройства
172.16.10.3
Например, 198.168.32.10 или example.com
Добавить адрес
IP-адрес интерфейса туннеля
Поле необязательное. Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
Формат: 10.100.0.50
Заполните «IP-адрес интерфейса туннеля» и «Удалённый IP-адрес туннеля» для получения статистики о потере пакетов, средней задержке и джиттере. Они должны находиться в одной подсети.
IPsec-политики
Автоматическое создание маршрутов
При выборе подсети 0.0.0.0/0 маршрут создаваться не будет.
Домашние локальные сети
192.168.105.0/24
Удалённые локальные сети
192.168.100.0/24
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
Запрос на подпись сертификата
-----BEGIN CERTIFICATE REQUEST-----
MIIBEjCBuAIBADBWMQ4wDAYDVQQKDAVJZ
GVjbzEMMAoGA1UECwwDVVRNMTYwNAYD
Файл NGFW.csr необходимо выслать для подписи на удалённое устройство
Подписанный сертификат NGFW
Загрузить
Корневой сертификат удалённого устройства
Загрузить
Дополнительно
Индекс интерфейса для Netflow
0
Целое число от 0 до 65535
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPsec-подключения;
- **Режим работы** - выберите **Туннельный**;
- **Адрес удаленного устройства** - укажите внешний IP-адрес MikroTik;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне;
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне;
- **Тип аунтификации** - выберите **Сертификат**;
- **Запрос на подпись сертификата** - будет сгенерирован **запрос, который необходимо выслать для подписи на MikroTik**;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. После подписания запроса необходимо продолжить настройку подключения в Ideco NGFW.

Не закрывайте вкладку с настройками! При закрытии вкладки с настройками *Запрос на подпись сертификата* изменит значение и процесс подписания файла NGFW.csr потребуется повторить.

Настройка входящего IPsec-подключения на MikroTik:

На этом этапе следует настроить MikroTik, чтобы продолжить настройку NGFW.

Файл **NGFW.csr**, полученный из Ideco NGFW, необходимо загрузить в файловое хранилище MikroTik:

1. Откройте раздел **File**.

2. Нажмите кнопку **Browse**.

3. Выберите файл и загрузите его.

Настроить MikroTik можно:

- Через GUI;
- Через консоль устройства;
- Через конфигурационные скрипты, сгенерированные по адресу https://mikrotik.ideco.ru/.

После генерации скрипта откройте раздел **System -> Scripts**, создайте скрипт и вставьте в него код, сгенерированный конфигуратором, затем запустите.

В файловой системе MikroTik появятся два файла, которые необходимо скачать, чтобы впоследствии загрузить на NGFW:

Файл `cert_export_device_<случайный набор символов>.ipsec.crt` - подписанный сертификат NGFW.
Файл `cert_export_mk_ca.crt` - корневой сертификат MikroTik.

Донастройка исходящего IPsec-подключение на Ideco NGFW:

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW.

1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

Подключение от MikroTik к Ideco NGFW

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на MikroTik:

Настроить устройство MikroTik можно:

- Через GUI;
- Через консоль устройства;
- Через конфигурационные скрипты, сгенерированные по адресу https://mikrotik.ideco.ru/.

После генерации скрипта необходимо открыть раздел **System -> Scripts**, создать скрипт, вставить в него код, сгенерированный конфигуратором, и запустить.

Настройка входящего IPsec-подключения на Ideco NGFW:

1. В Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**, нажмите **Добавить** и заполните поля:

Добавление подключения

Название подключения
Тестовое подключение

Зона

Поле необязательное

Режим работы

- (•) Туннельный
  VTI
- ( ) Транспортный
  GRE over IPsec

IP-адрес интерфейса туннеля

Поле необязательное. Пример: 10.100.0.1/16

Удалённый IP-адрес туннеля

Формат: 10.100.0.50
Заполните «IP-адрес интерфейса туннеля» и «Удалённый IP-адрес туннеля» для получения статистики о потере пакетов, средней задержке и джиттере. Они должны находиться в одной подсети.

IPsec-политики

- [x] Автоматическое создание маршрутов
  При выборе подсети 0.0.0.0/0 маршрут создаваться не будет.

Домашние локальные сети
IP 192.168.105.0/24

Удалённые локальные сети
IP 192.168.100.0/24

Тип аутентификации

- ( ) Сертификат
  Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
- (•) PSK
  Обеспечивает низкий уровень безопасности, поддерживается большинством устройств

PSK ключ
QWERqwer1234@1

Тип идентификатора
auto

Идентификатор удалённой стороны
test_psk

Для идентификации входящего соединения

Дополнительно

Индекс интерфейса для Netflow
0

Целое число от 0 до 65535

Добавить подключение Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPsec-подключения;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне;
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне;
- **Тип аунтификации** - выберите **PSK**;
- **PSK-ключ** - вставьте PSK-ключ, полученный от MikroTik;
- **Тип идентификатора** - выберите **auto**;
- **Идентификатор удаленной стороны** - вставьте идентификатор MikroTik (параметр key-id в `/ip ipsec peers`);
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Нажмите кнопку **Добавить подключение**.

Тип аутентификации Сертификат

Подключение по сертификатам является более безопасным, чем подключение по PSK.

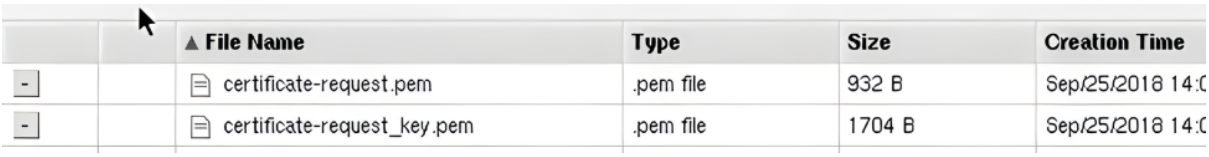
Предварительная настройка MikroTik:

Настроить MikroTik можно:

- Через GUI;
- Через консоль устройства;
- Через конфигурационные скрипты, сгенерированные по адресу https://mikrotik.ideco.ru/.

После генерации скрипта необходимо открыть раздел **System -> Scripts**, создать скрипт для генерации запроса на подпись сертификата, вставить в него сгенерированный конфигуратором код и запустить. Конфигуратором генерируется два скрипта, поэтому в MikroTik также создайте два скрипта.

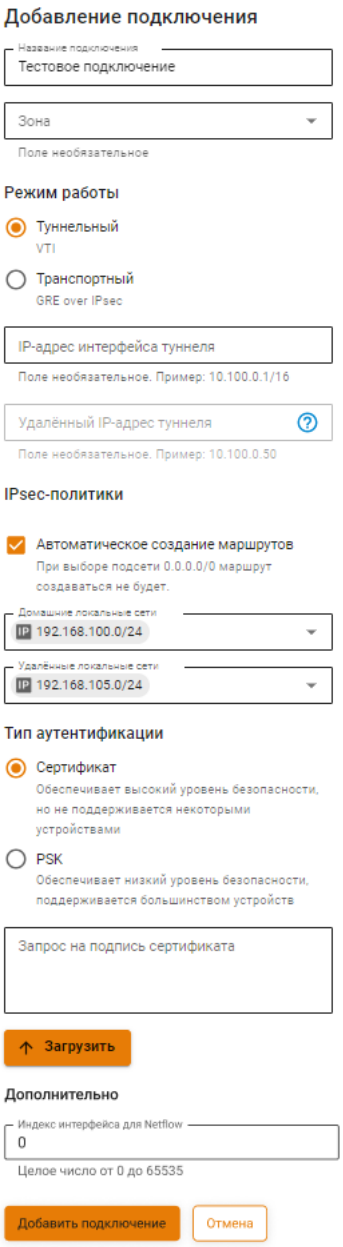
Перед настройкой необходимо запустить первый скрипт для запроса на подпись сертификата. После чего в файловом хранилище MikroTik появятся два файла, которые необходимо скачать, они требуются для дальнейшей настройки:



- Файл `certificate-request.pem` - **запрос на подпись сертификата**;
- Файл `certificate-request_key.pem` - **приватный ключ**.

Настройка входящего IPsec-подключения на Ideco NGFW:

1. В Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**, нажмите **Добавить** и заполните поля:

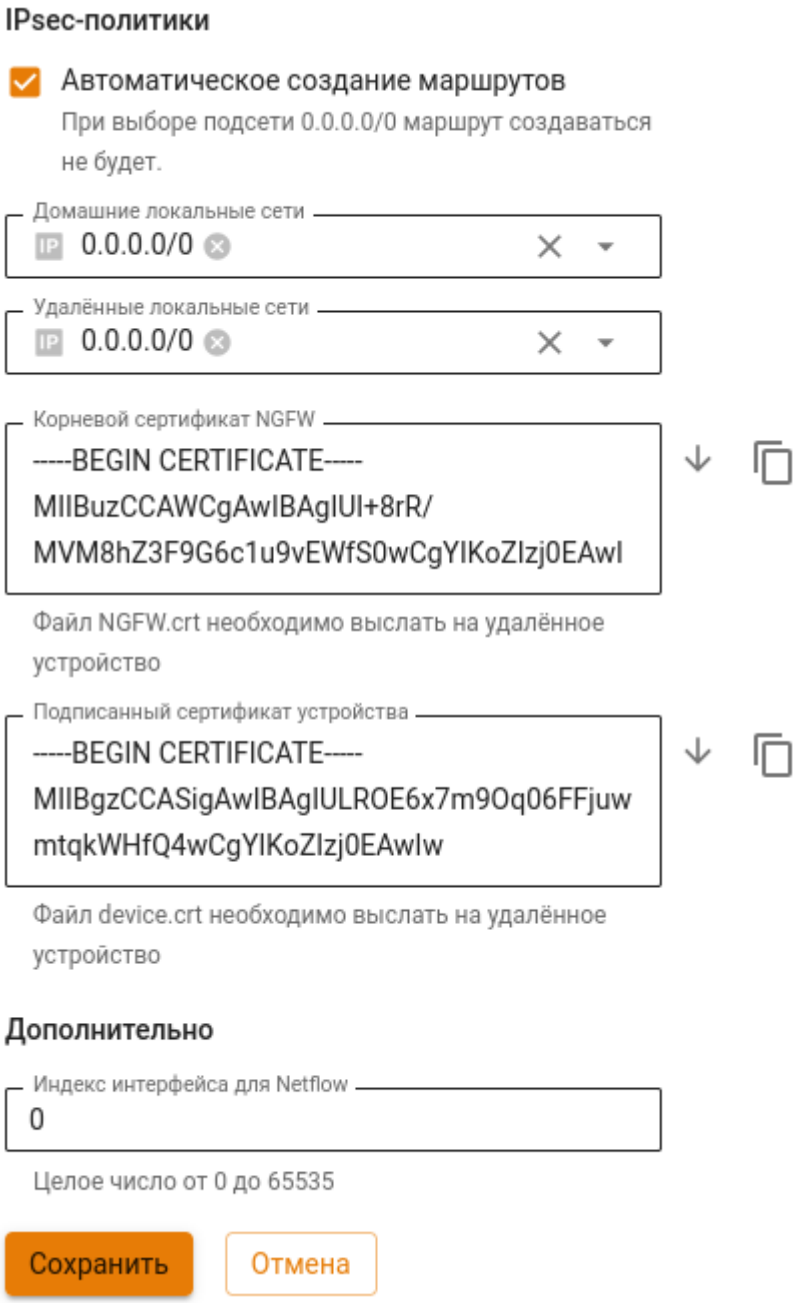


- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону, в которую требуется добавить IPsec-подключение;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное;
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне;

- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне;
- **Тип аунтификации** - выберите **Сертификат**;
- **Запрос на подпись сертификата** - загрузите запрос на подпись, **полученный от MikroTik**;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

2. Нажмите кнопку **Добавить подключение**. Нажмите на кнопку редактирования соединения ( ), чтобы продолжить настройку.

3. Откройте созданное IPsec-соединение, нажав на , и загрузите файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`).



Настройка исходящего IPsec-подключение на MikroTik:

1. Загрузите на MikroTik скачанные ранее файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`) через WinBox или по SSH.

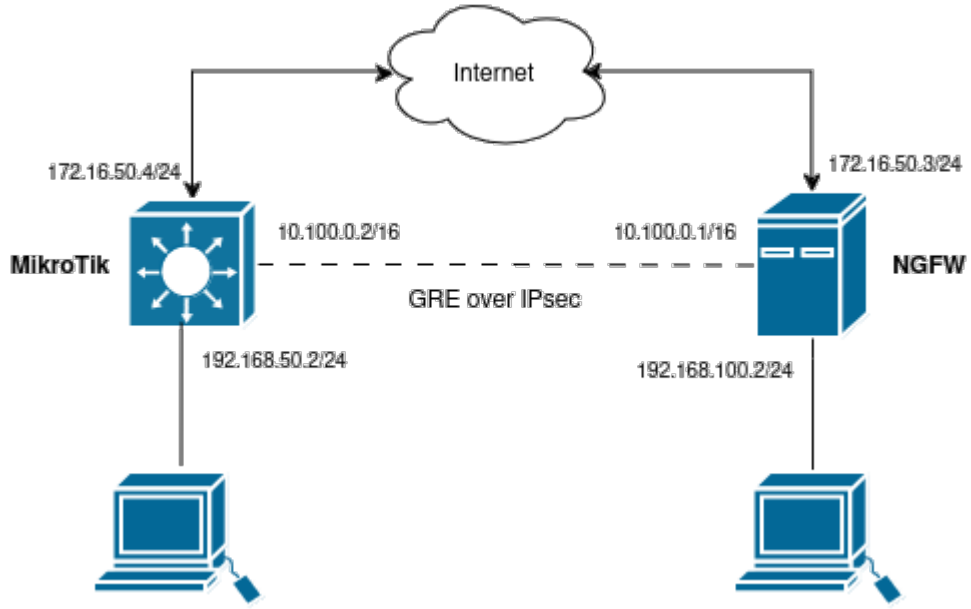
2. Запустите второй сгенерированный конфигуратором скрипт.

Подключение в Транспортном режиме (GRE over IPsec)

Подсказка: GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

Рассмотрим настройку подключения по схеме:



- `172.16.50.3/24` - внешний IP-адрес NGFW;
- `192.168.100.2/24` - локальный IP-адрес NGFW;
- `10.100.0.1/16` - IP-адрес GRE-тунеля NGFW;
- `172.16.50.4/24` - внешний IP-адрес MikroTik;
- `192.168.50.2/24` - локальный IP-адрес MikroTik;
- `10.100.0.2/16` - IP-адрес GRE-тунеля MikroTik.

Для настройки подключения MikroTik и Ideco NGFW следуйте инструкции в каждом из пунктов.

Подключение от Ideco NGFW к MikroTik

Предварительная настройка MikroTik:

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

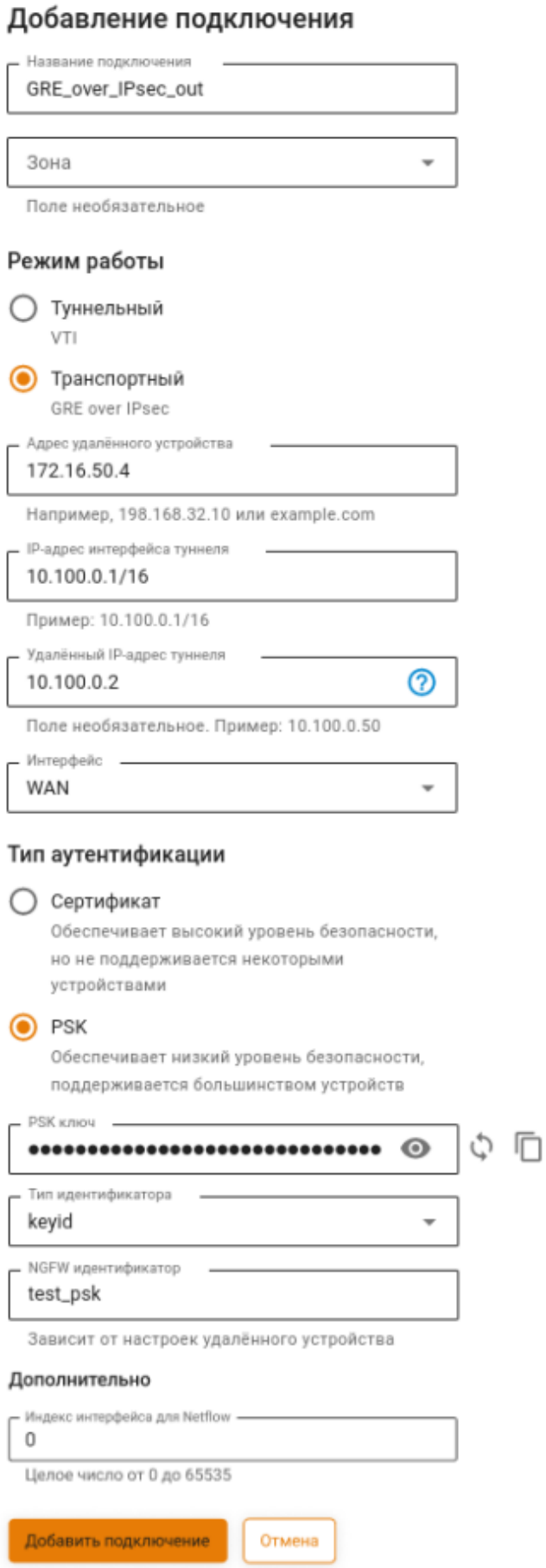
2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1␣
↪remote-address=172.16.50.3
/ip address add address=10.100.0.2/16 interface=gre-tunnel1 network=10.100.0.0
```

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на Ideco NGFW:

Заполните поля:


Добавление подключения
Название подключения
GRE_over_IPsec_out
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
Адрес удалённого устройства
172.16.50.4
Например, 198.168.32.10 или example.com
IP-адрес интерфейса туннеля
10.100.0.1/16
Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
10.100.0.2
Поле необязательное. Пример: 10.100.0.50
Интерфейс
WAN
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
PSK ключ
Тип идентификатора
keyid
NGFW идентификатор
test_psk
Зависит от настроек удалённого устройства
Дополнительно
Индекс интерфейса для Netflow
0
Целое число от 0 до 65535
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Транспортный** режим;
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Интерфейс** - выберите внешний интерфейс NGFW;
- **Тип аутентификации** - выберите **PSK**;
- **PSK-ключ** - будет сгенерирован случайный PSK-ключ. Он потребуется для настройки подключения в MikroTik;
- **Тип идентификатора** - выберите **keyid**;
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего подключения в MikroTik;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Настройка входящего IPsec-подключения на MikroTik:

Настройте IPsec-подключение со стороны MikroTik:

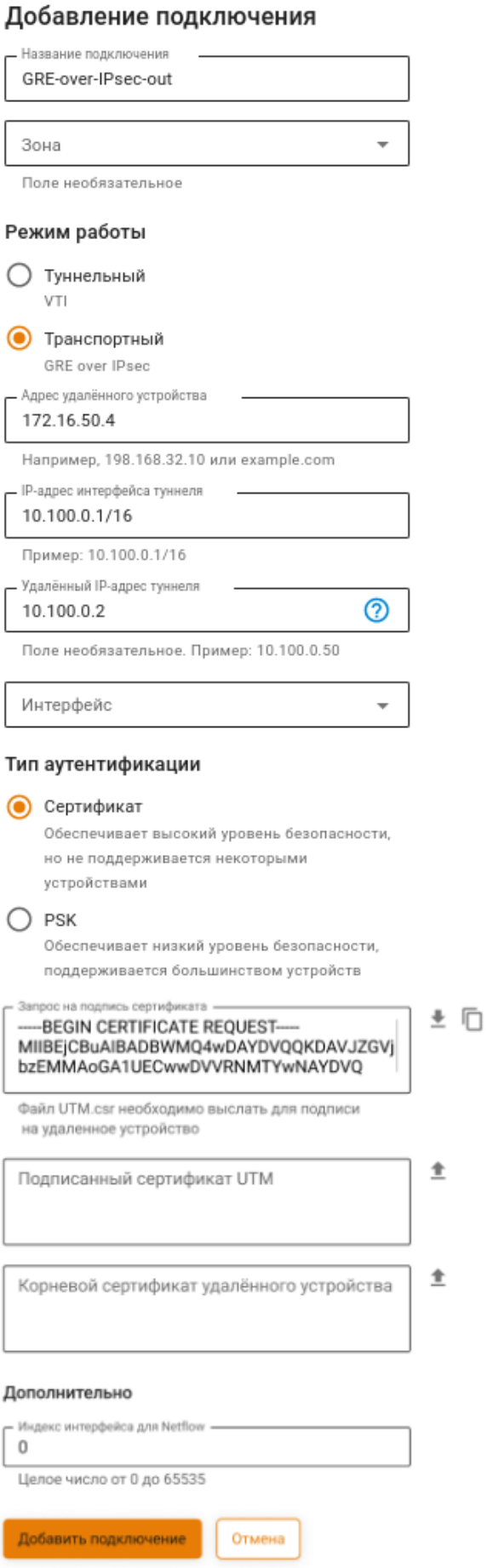
```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256␣
↪name=from_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=from_192.168.100.0/24 enc-
↪algorithms=aes-256-cbc name=172.16.50.3 pfs-group=modp4096

/ip ipsec peer add address=172.16.50.3/32 comment=from_192.168.100.0/24 exchange-
↪mode=ike2 name=from_192.168.100.0/24 passive=yes profile=from_192.168.100.0/24

/ip ipsec identity add comment=from_192.168.100.0/24 peer=from_192.168.100.0/24␣
↪secret="<Сгенерированный NGFW PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24␣
↪proposal=172.16.50.3 protocol=gre src-address=172.16.50.4/32
```

Тип аутентификации Сертификат

Настройка исходящего IPsec-подключения на Ideco NGFW:

1. Перейдите в раздел **IPsec -> Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:


Добавление подключения
Название подключения
GRE-over-IPsec-out
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
Адрес удалённого устройства
172.16.50.4
Например, 198.168.32.10 или example.com
IP-адрес интерфейса туннеля
10.100.0.1/16
Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
10.100.0.2
Поле необязательное. Пример: 10.100.0.50
Интерфейс
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
Запрос на подпись сертификата
-----BEGIN CERTIFICATE REQUEST-----
MIIBEjCBuAIBADBWMQ4wDAYDVQQKDAVJZGVj
bzEMMAoGA1UECwwDVVRNMTYwNAYDVQ
Файл UTM.csr необходимо выслать для подписи на удаленное устройство
Подписанный сертификат UTM
Корневой сертификат удалённого устройства
Дополнительно
Индекс интерфейса для Netflow
0
Целое число от 0 до 65535
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Транспортный** режим;
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Интерфейс** - выберите интерфейс NGFW;
- **Тип аутентификации** - выберите **Сертификат**;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Скачайте **Запрос на подпись сертификата**.

4. Не закрывая форму создания исходящего подключения NGFW, перейдите к настройке Mikrotik.

Настройка входящего IPsec-подключения на MikroTik:

1. Загрузите скачанный ранее файл с **Запросом на подпись сертификата** (`NGFW.crt`) на MikroTik через WinBox или по SSH.

2. Создайте корневой сертификат MikroTik:

```
/certificate add common-name=mk_ca name=mk_ca_template key-usage=key-cert-sign,crl-
↪sign,digital-signature,content-commitment
/certificate sign mk_ca_template ca-crl-host=172.16.50.4 name=mk_ca
```

3. Подпишите сертификат Ideco NGFW и сделайте его доверенным:

```
/certificate sign-certificate-request file-name=NGFW.csr ca=mk_ca
/certificate set [find name~"^device_.+\\.ipsec\$"] trusted=yes
```

4. Экспортируйте корневой сертификат MikroTik и подписанный сертификат NGFW в формат `.pem`:

```
/certificate export-certificate mk_ca type=pem
/certificate export-certificate [find name~"^device_.+\\.ipsec\$"] type=pem
```

5. Загрузите с MikroTik корневой сертификат MikroTik и подписанный сертификат NGFW через WinBox или по SSH. Названия файлов содержат `cert_export`.

6. Настройте входящее IPsec-соединение на MikroTik:

```
/ip ipsec profile add name=from_192.168.100.0/24 hash-algorithm=sha256 enc-
↪algorithm=aes-256 dh-group=modp4096 dpd-interval=120s dpd-maximum-failures=5

/ip ipsec peer add name=from_192.168.100.0/24 address=172.16.50.3/32 profile=from_192.
↪168.100.0/24 exchange-mode=ike2 passive=yes comment=from_192.168.100.0/24

/ip ipsec identity add peer=from_192.168.100.0/24 auth-method=digital-signature␣
↪certificate=mk_ca remote-certificate=[: put [/certificate get [/certificate find␣
↪name~"^device_.+\\.ipsec\$"] name]] comment=from_192.168.100.0/24

/ip ipsec proposal add name=172.16.50.3 enc-algorithms=aes-256-cbc auth-
↪algorithms=sha256 pfs-group=modp4096 comment=from_192.168.100.0/24
```

(continues on next page)

(продолжение с предыдущей страницы)

```
/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24␣
↪proposal=172.16.50.3 protocol=gre src-address=172.16.50.4/32
```

Донастройка исходящего IPsec-подключение на Ideco NGFW:

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW.

1. Загрузите скачанные ранее **Корневой сертификат MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_<случайный набор символов>.ipsec.crt`) в соответствующие поля.

2. Нажмите **Добавить подключение**.

Подключение от MikroTik к Ideco NGFW

Тип аутентификации PSK

Настройка исходящего IPsec-подключения на MikroTik:

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

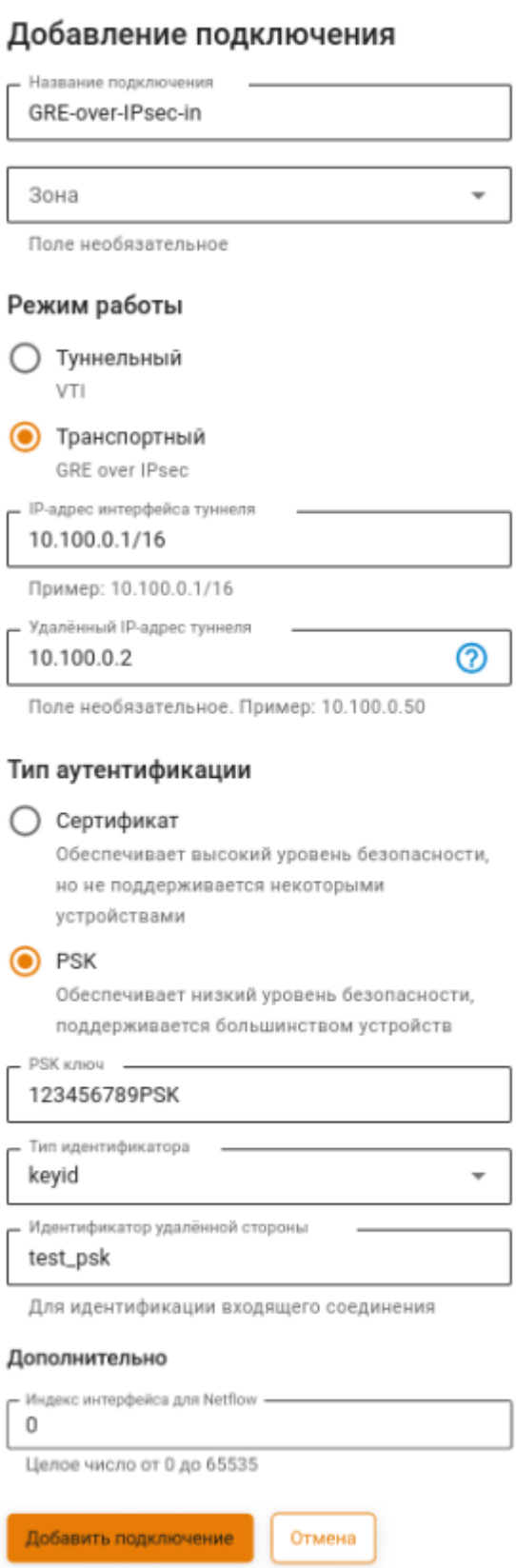
```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1␣
↪remote-address=172.16.50.3
/ip address add address=10.100.0.2/16 interface=gre-tunnel1 network=10.100.0.0
```

3. Настройте IPsec-подключение со стороны MikroTik:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256␣
↪name=to_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-
↪algorithms=aes-256-cbc name=172.16.50.3 pfs-group=modp4096

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-
↪mode=ike2 name=to_192.168.100.0/24 profile=to_192.168.100.0/24

/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 my-id=key-
↪id:"test_psk" secret="<PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.
↪16.50.3 protocol=gre src-address=172.16.50.4/32
```

Настройка входящего IPsec-подключения на Ideco NGFW:

Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Транспортный** режим;

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Тип аутентификации** - выберите **PSK**;
- **PSK-ключ** - введите PSK-ключ, указанный при настройке исходящего IPsec-подключения в MikroTik;
- **Тип идентификатора** - выберите **keyid**;
- **NGFW идентификатор** - введите **key-id**, использованный при настройке исходящего IPsec-подключения в MikroTik;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Тип аутентификации Сертификат

Предварительная настройка MikroTik:

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1␣
↪remote-address=172.16.50.3
/ip address add address=10.100.0.2/16 interface=gre-tunnel1 network=10.100.0.0
```

3. Сгенерируйте запрос на подпись сертификата:

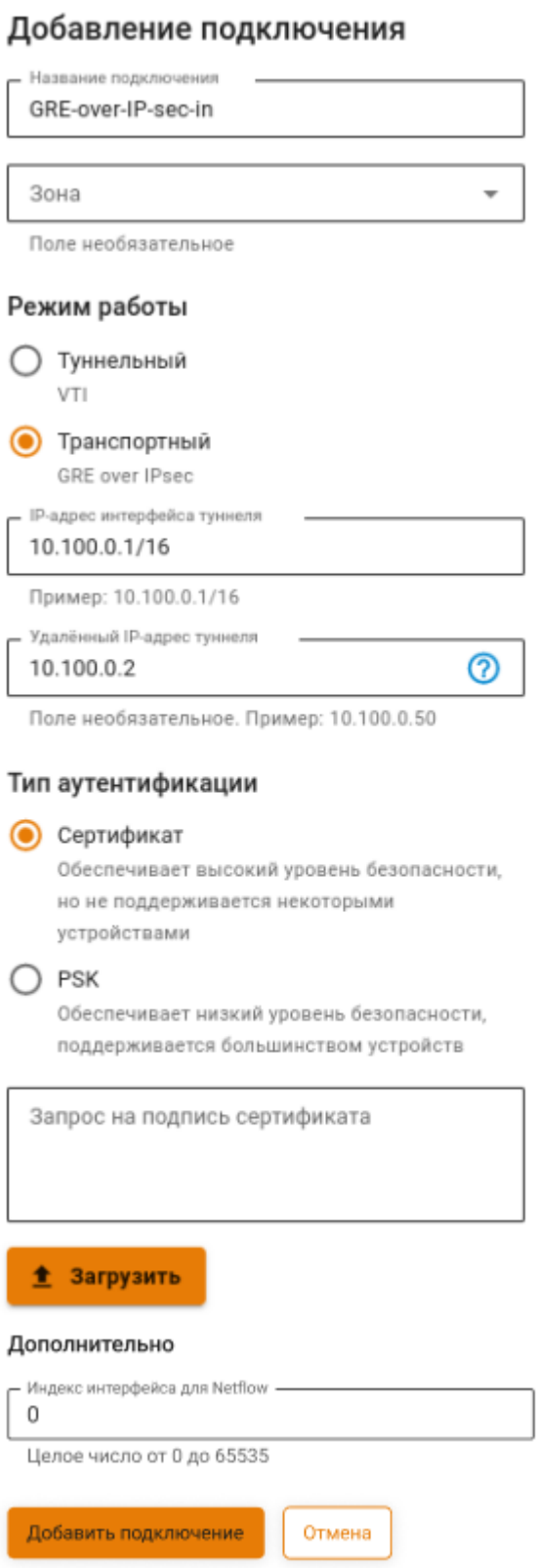
```
/certificate add name=mk_ca common-name=mk_ca key-usage=digital-signature,content-
↪commitment
/certificate create-certificate-request key-passphrase="" template=mk_ca
```

4. Загрузите файл `certificate-request.pem` с MikroTik через WinBox или по SHH.

Настройка входящего IPsec-подключения на Ideco NGFW:

1. Перейдите в раздел **IPsec -> Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Транспортный** режим;

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети;
- **Тип аутентификации** - выберите **Сертификат**;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

3. Загрузите скачанный ранее с MikroTik файл `certificate-request.pem` в поле **Запрос на подпись сертификата**.

4. Нажмите **Добавить подключение**.

5. Откройте созданное IPsec-соединение, нажав на  , и загрузите файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`).

Настройка исходящего IPsec-подключение на MikroTik:

1. Загрузите на MikroTik скачанные ранее файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанного сертификата устройства** (`device.crt`) через WinBox или по SSH.

2. Импортируйте сертификаты:

```
/certificate import file-name=NGFW.crt passphrase=""
/certificate import file-name=device.crt passphrase=""
/certificate import file-name=certificate-request_key.pem passphrase=""
```

3. Настройте IPsec-соединение:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256␣
↪name=to_192.168.100.0/24 dpd-interval=120s dpd-maximum-failures=5

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-
↪mode=ike2 name=to_192.168.100.0/24 profile=to_192.168.100.0/24

/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 auth-
↪method=digital-signature certificate=device.crt_0 remote-certificate=NGFW.crt_0

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-
↪algorithms=aes-256-cbc name=172.16.50.3 pfs-group=modp4096

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.
↪16.50.3 protocol=gre src-address=172.16.50.4/32
```

Проблемы при повторной активации входящего IPsec-подключения к Ideco NGFW

Если подключение было отключено и при попытке включения соединение не установилось, удаленное устройство попало в fail2ban. Для установки соединения сбросьте блокировки по IP на Ideco NGFW. О сбросе блокировки читайте в статье *Защита от брутфорс-атак*.

Fail2ban отслеживает в log-файлах попытки обратиться к сервисам, и, если находит повторяющиеся неудачные попытки авторизации с одного и того же IP-адреса или хоста, блокирует IP-адрес.

18.13.9 Подключение MikroTik и Ideco NGFW по L2TP/IPsec

Подключение MikroTik к Ideco NGFW по L2TP/IPsec

- Настройте VPN-сервер на Ideco NGFW в разделе **Пользователи -> VPN-подключения**. Подробная инструкция по настройке - в статье *Подключение по L2TP/IPsec*;
- Настройте подключение на MikroTik, выполнив команды:

1. Отредактируйте IPsec profile:

```
ip ipsec profile set default hash-algorithm=sha1 enc-algorithm=aes-256 dh-
↪group=modp2048
```

2. Отредактируйте IPsec proposals:

```
ip ipsec proposal set default auth-algorithms=sha1 enc-algorithms=aes-256-cbc,aes-192-
↪cbc,aes-128-cbc pfs-group=modp2048
```

3. Создайте подключение к Ideco NGFW:

```
interface l2tp-client add connect-to=<server> profile=default disabled=no name=
↪<interface_name> password="<password>" user="<login>" use-ipsec="yes" ipsec-secret="
↪<psk>"
```

4. Добавьте маршрут до первого адреса VPN-сети NGFW (remote VPN subnet):

```
ip route add dst-address=<remote VPN subnet> gateway=l2tp-out1
```

Подсказка: Для работы удаленных сетей на NGFW и на MikroTik нужно создавать маршруты на обоих устройствах.

Подсказка: Если у вас в разделе **Правила трафика -> Файрвол -> SNAT** отключен **Автоматический SNAT локальных сетей**, то может понадобиться прописать маршрут до сети VPN, где шлюзом является NGFW.

Пример:

- Адрес NGFW = `169.254.1.5`
- Первый адрес VPN = `10.128.0.1`

```
ip route add dst-address=169.254.1.5 gateway==10.128.0.1
```

18.13.10 Подключение pfSense к Ideco NGFW по IPsec

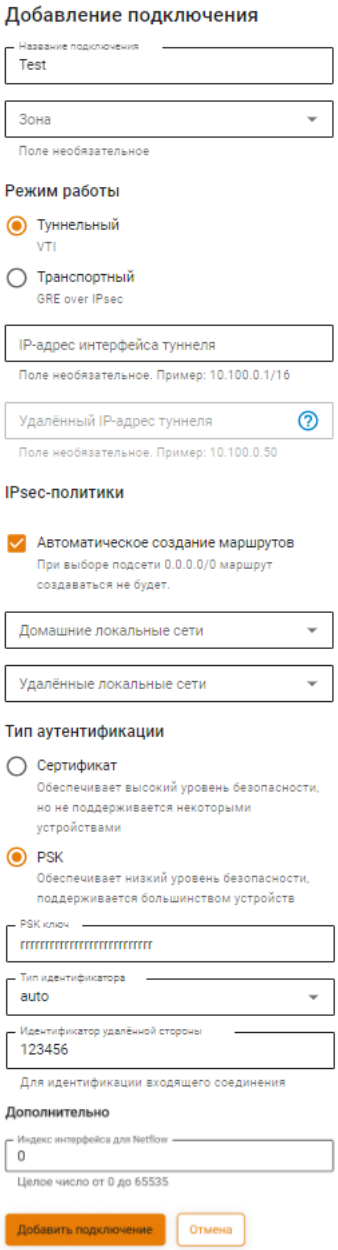
Подсказка: Объединяемые локальные сети не должны пересекаться!

Настройка входящего подключения

Для настройки Ideco NGFW следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**.

2. Добавьте новое подключение:



- **Название подключения** - любое;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами;

- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения;
- **Идентификатор удаленной стороны** - любой;
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense;
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Подсказка: Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

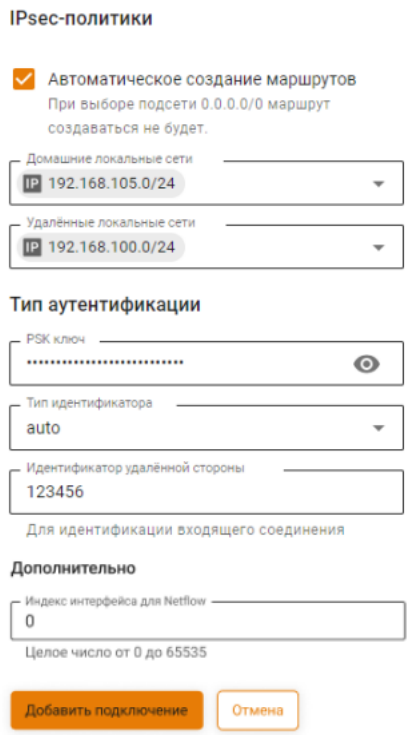
---

3. Сохраните созданное подключение, нажмите на кнопку **Включить**.

4. Скопируйте значение идентификатора удаленной стороны одним из способов:

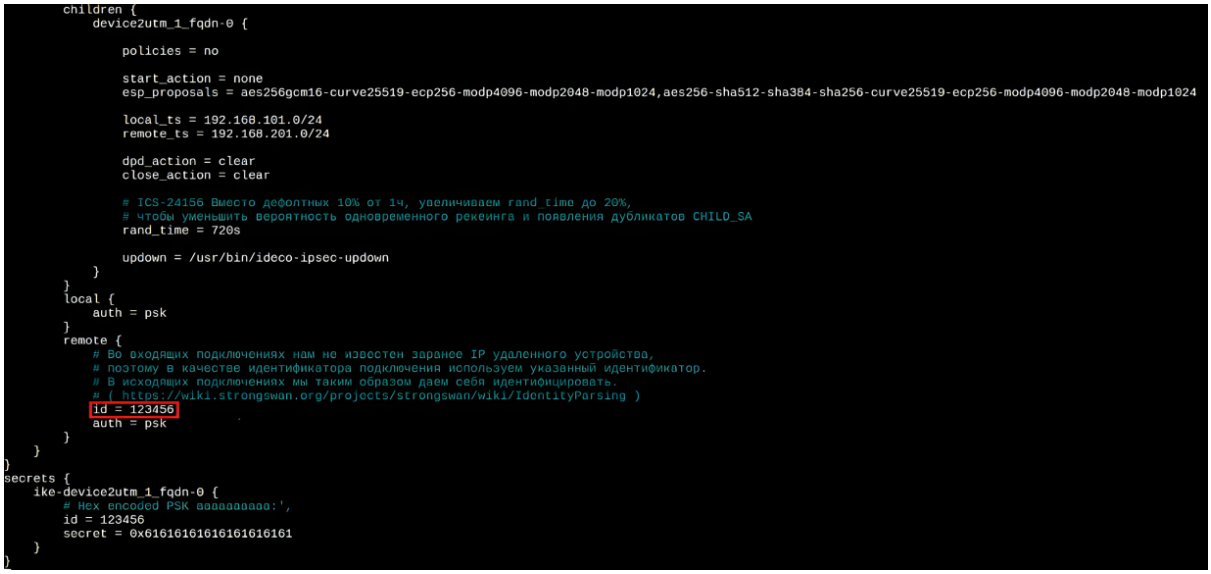
В интерфейсе NGFW:

На вкладке **Сервисы -> IPsec -> Входящие подключения** в строке **Идентификатор удаленной стороны**:



Через терминал:

На Ideco NGFW в папке `/run/ideco-ipsec-backend/strongswan/swanctl/conf.d/` будет сгенерирован конфигурационный файл. Необходимо перейти в консоль и открыть на редактирование файл вида `device_<номер>.conf`. Из этого файла необходимо скопировать значение строки `id`(идентификатор удаленной стороны):



5. Перейдите к настройке pfSense, предварительно записав значение строки `id` (идентификатор удаленной стороны).

Настройка pfSense:

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите на вкладку **VPN –> IPsec –> Tunnels**.

2. Добавьте новое подключение:

- **Description** - любое;
- **Key Exchange version** - IKEv2;
- **Internet Protocol** - IPv4;
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW;
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;
- **Authentication Method** - Mutual PSK;
- **My identifier и Peer identifier** - сюда вставьте значение строки `id` на Ideco NGFW (см. шаг 4 в настройке Ideco NGFW);
- **Pre-Shared Key** - вставьте PSK-ключ, который ранее прописывали на Ideco NGFW;
- **Encryption Algorithm** - используйте следующие параметры: \
  - **Algorithm** - AES256-GCM; \
  - **Key length** - 128 bit; \
  - **Hash** - SHA256; \
  - **DH Group** - Elliptic Curve 25519-256.

Все остальные значения можно оставить по умолчанию.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2. Здесь укажите:

- **Encryption Algorithm** - используйте следующие параметры: \
  - **Algorithm** - AES256-GCM; \
  - **Key length** - 128 bit; \
  - **Hash** - SHA256; \

  - **DH Group** - Elliptic Curve 25519-256.

- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW;
- **Remote Network** - локальную сеть Ideco NGFW, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. Разрешите хождение трафика между локальными сетями pfSense и Ideco NGFW в настройках файрвола pfSense (переходим на вкладку **Firewall -> Rules -> IPsec** и создаем два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense).

Обращаем внимание на раздел файрвола WAN - в нем по умолчанию запрещен входящий трафик из «серых» подсетей, который требуется разрешить.

7. Теперь переходим на вкладку **Status -> IPsec** (там должно появится созданное подключение), нажимаем на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы указали в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

Настройка исходящего подключения

Для настройки Ideco NGFW следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Адрес удаленного устройства** - укажите адрес удаленного устройства;
- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения;
- **NGFW идентификатор** - любой;
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense;
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Настройка pfSense:

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите на вкладку **VPN > IPsec > Advanced Options** и в поле **Child SA Start Action** выберите параметр **None (Responder Only)**.

2. Добавьте новое подключение:

- **Key Exchange version** - IKEv2;
- **Internet Protocol** - IPv4;
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW;

- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;
- **Description** - любое;
- **Authentication Method** - Mutual PSK;
- **My identifier** - My ip address;
- **Peer identifier** - KeyID tag. Введите идентификатор удаленной стороны, т. е. Ideco NGFW;
- **Pre-Shared Key** - введите PSK-ключ;
- **Encryption Algorithm**:
  - Для **Ideco UTM версии 10.0 и Ideco NGFW версии 16.0 и новее** используйте следующие параметры: \
    * **Algorithm** - AES256-GCM;
    * **Key length** - 128 bit;
    * **Hash** - SHA256;
    * **DH Group** - Elliptic Curve 25519-256.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2 и укажите следующие значения:

- **Encryption Algorithm**:
  - **Для Ideco UTM версии 10.0 и Ideco NGFW версии 16.0 и новее** используйте следующие параметры: \
    * **Algorithm** - AES256-GCM;
    * **Key length** - 128 bit;
    * **Hash** - SHA256;
    * **DH Group** - Elliptic Curve 25519-256.
- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW;
- **Remote Network** - локальную сеть Ideco NGFW, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. В настройках файрвола pfSense перейдите на вкладку **Firewall -> Rules -> IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense.

7. Обратите внимание на раздел файрвола **WAN** - в нем по умолчанию запрещен входящий трафик из «серых» подсетей, который требуется разрешить.

8. Перейдите на вкладку **Status -> IPsec** (там должно появится созданное подключение), нажмите на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы указали в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

18.13.11 Подключение Kerio Control и Ideco NGFW по IPsec

Подсказка: Объединяемые локальные сети не должны пересекаться!

Предварительная настройка Kerio Control:

1. По умолчанию Kerio Control использует IKEv1 для создания подключений к сторонним устройствам. Включить IKEv2 можно через консоль, выполнив действия:

- Подключиться к Kerio Control по SSH;
- Перейти в папку `/var/winroute`;
- Открыть на редактирование файл `winroute.cfg`;
- В нем найти раздел, начинающийся с текста `<table name="Firewall">`;
- В этом разделе найти строку `<variable name="IKEVersion">ikev1</variable>` и изменить в ней `ikev1` на `ikev2`;
- После этого требуется перезагрузить сервер и убедиться, что изменения в настройках сохранились.

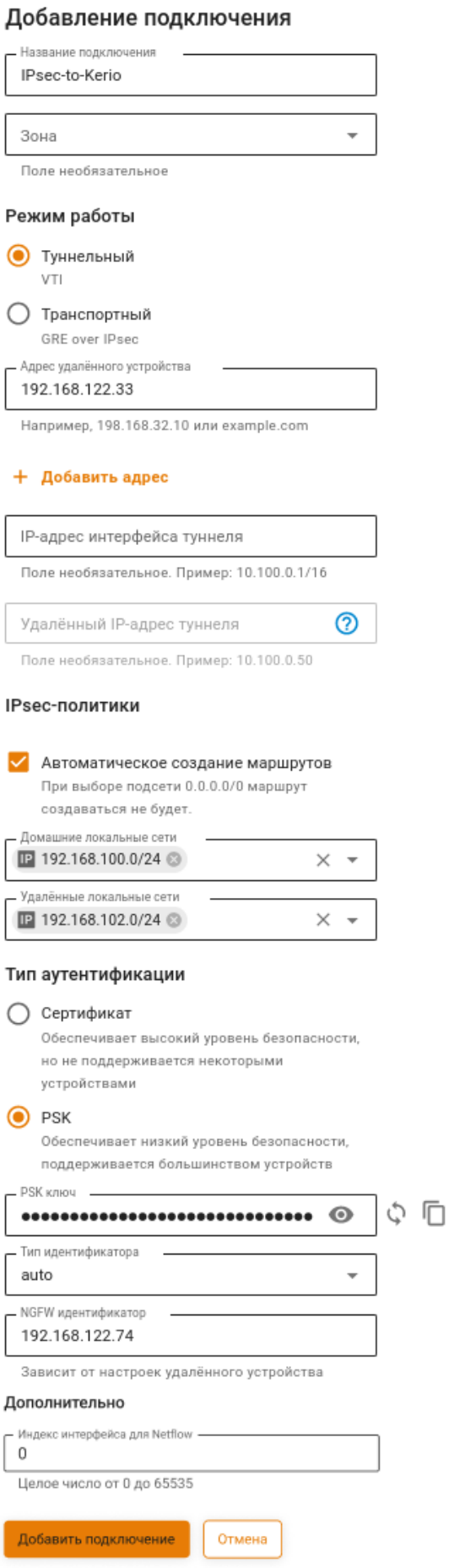
2. В разделе **Правила трафика** разрешите трафик VPN-служб.

Подключение от Ideco NGFW к Kerio Control

Настройка исходящего подключения на Ideco NGFW:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**.

2. Добавьте новое подключение и заполните поля:


Добавление подключения
Название подключения
IPsec-to-Kerio
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
Адрес удалённого устройства
192.168.122.33
Например, 198.168.32.10 или example.com
Добавить адрес
IP-адрес интерфейса туннеля
Поле необязательное. Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
Поле необязательное. Пример: 10.100.0.50
IPsec-политики
Автоматическое создание маршрутов
При выборе подсети 0.0.0.0/0 маршрут создаваться не будет.
Домашние локальные сети
192.168.100.0/24
Удалённые локальные сети
192.168.102.0/24
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
PSK ключ
Тип идентификатора
auto
NGFW идентификатор
192.168.122.74
Зависит от настроек удалённого устройства
Дополнительно
Индекс интерфейса для Netflow
0
Целое число от 0 до 65535
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Режим работы** - выберите **Туннельный**;
- **Адрес удаленного устройства** - укажите внешний IP-адрес Kerio Control;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами;
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW, которая будет видна из подсети Kerio Control;
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW;
- **Тип аутентификации** - выберите тип PSK;
- **PSK-ключ** - укажите PSK-ключ, который будет использоваться для подключения;
- **Тип идентификатора** - выберите auto;
- **Идентификатор NGFW** - укажите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

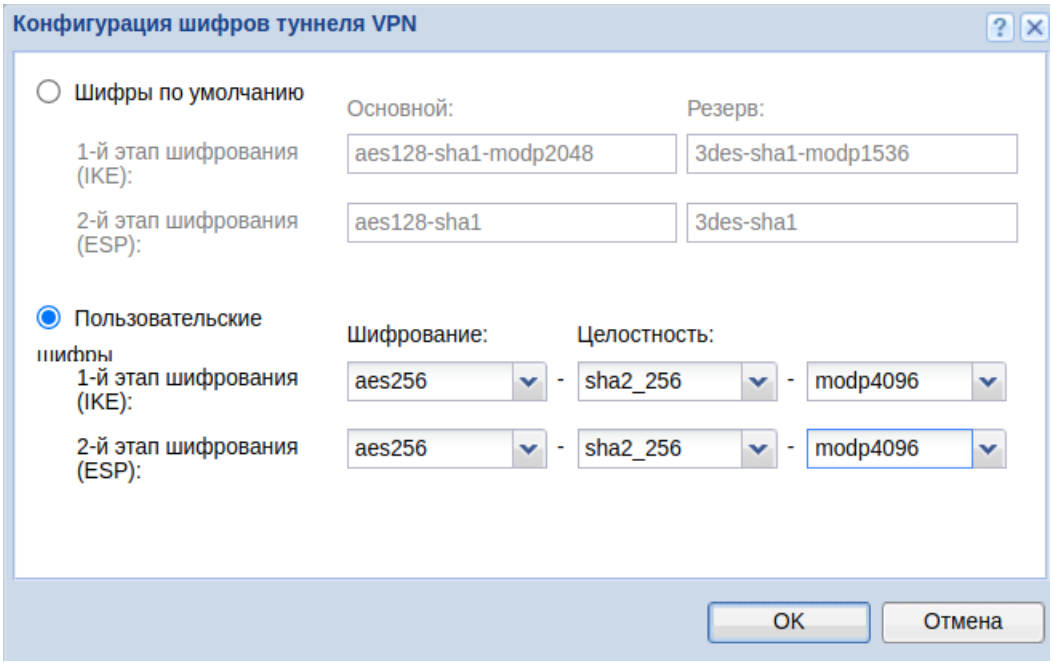
Настройка завершена, теперь переходим к настройке Kerio Control.

Настройка входящего подключения на Kerio Control:

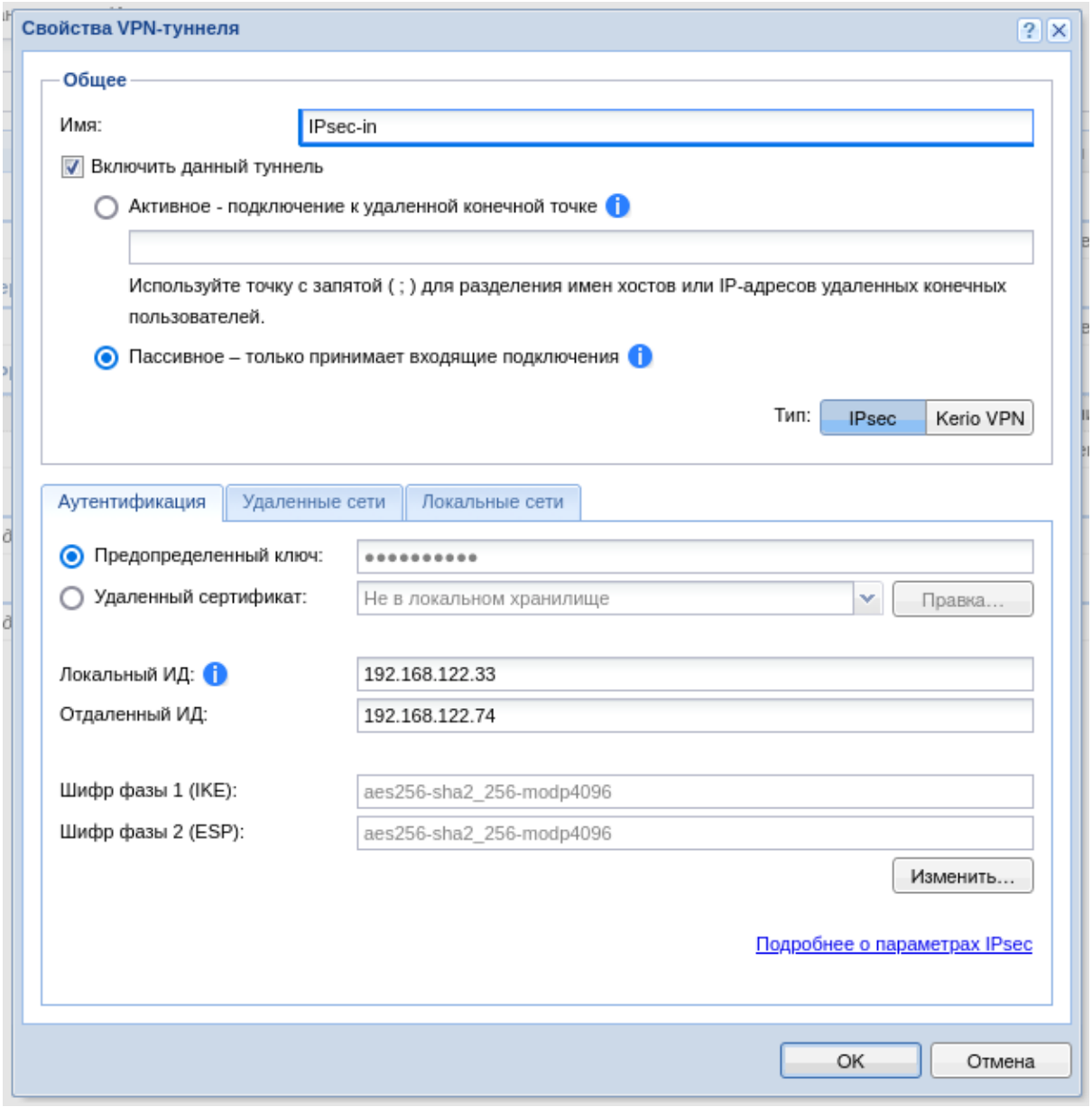
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель...**.

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec;
- **Имя** - произвольное;
- **Включить данный туннель**;
- Тип **Пассивное**;
- **Предопределенный ключ** - введите PSK-ключ, который был указан при создании подключения на Ideco NGFW;
- **Локальный ИД** - укажите IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения;
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW;
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



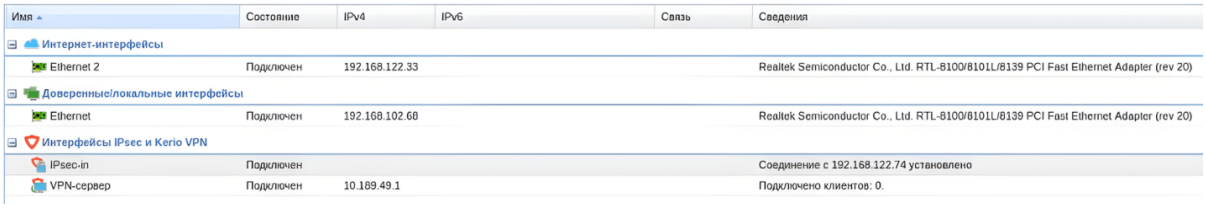
Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW, которая будет видна из подсети Kerio Control.

4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице:



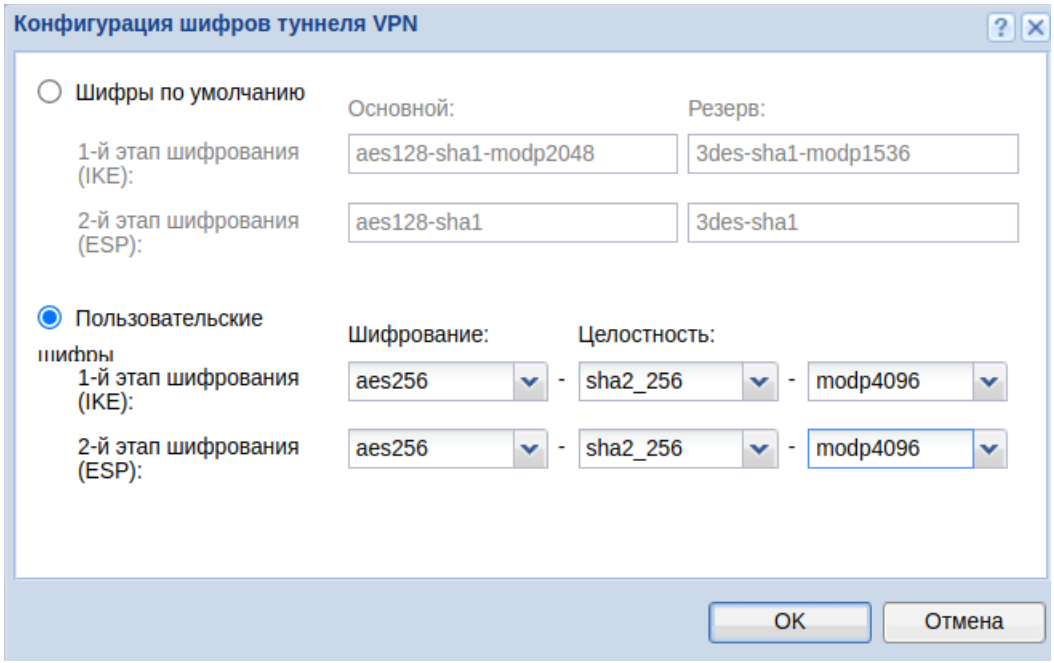
Подключение от Kerio Control к Ideco NGFW

Настройка исходящего подключения на Kerio Control:

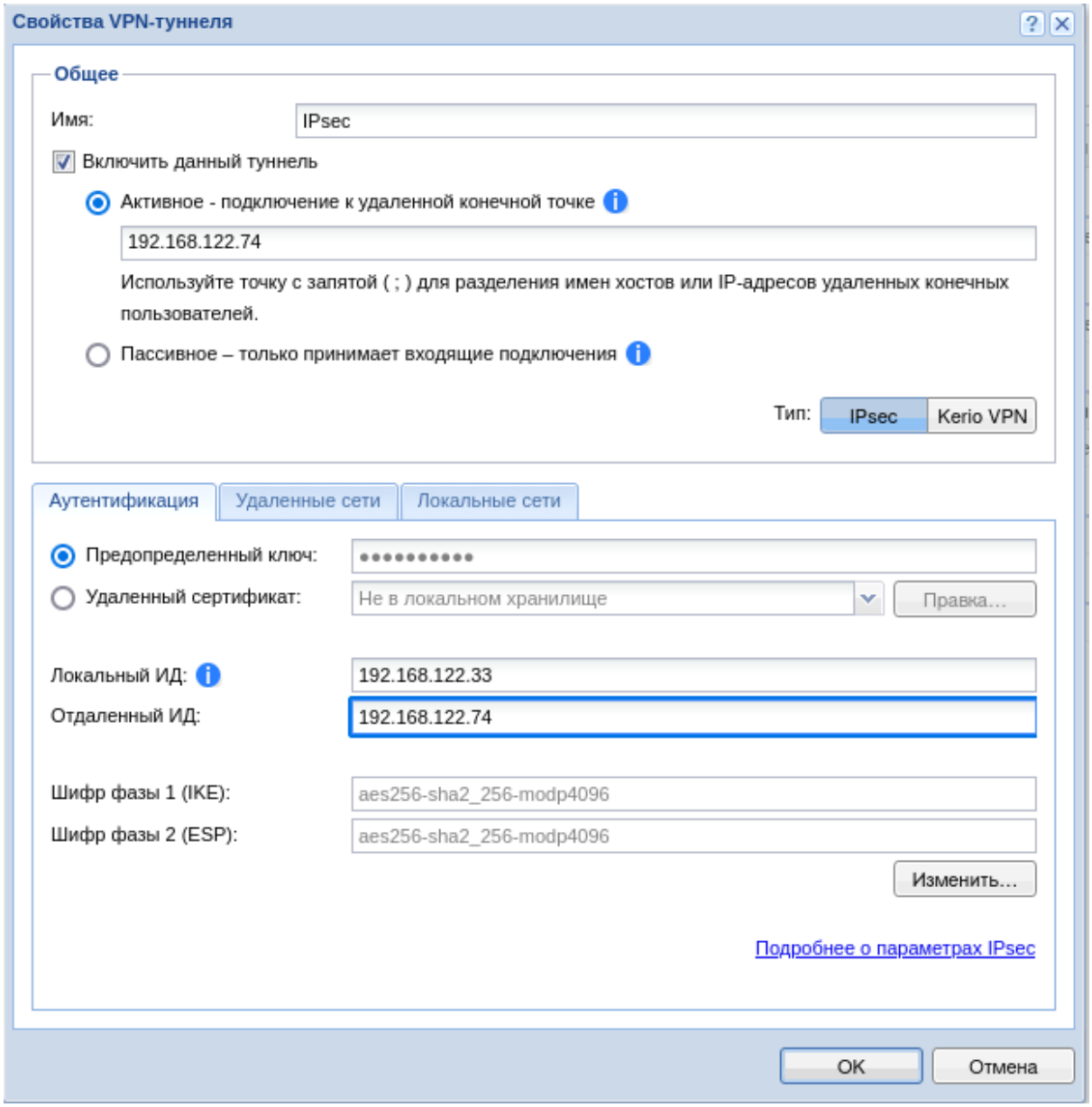
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель. . .** .

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec;
- **Имя** - произвольное;
- **Включить данный туннель**;
- Выберите тип **Активное** и в поле под ним пропишите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- **Предопределенный ключ** - введите PSK-ключ, который будет использоваться для подключения;
- **Локальный ИД** - укажите ключ, который будет задан в поле **Идентификатор NGFW** при настройке входящего подключения на Ideco NGFW, или IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения. **Предпочтительное значение - имя хоста Kerio**;
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW, которая будет видна из подсети Kerio Control.

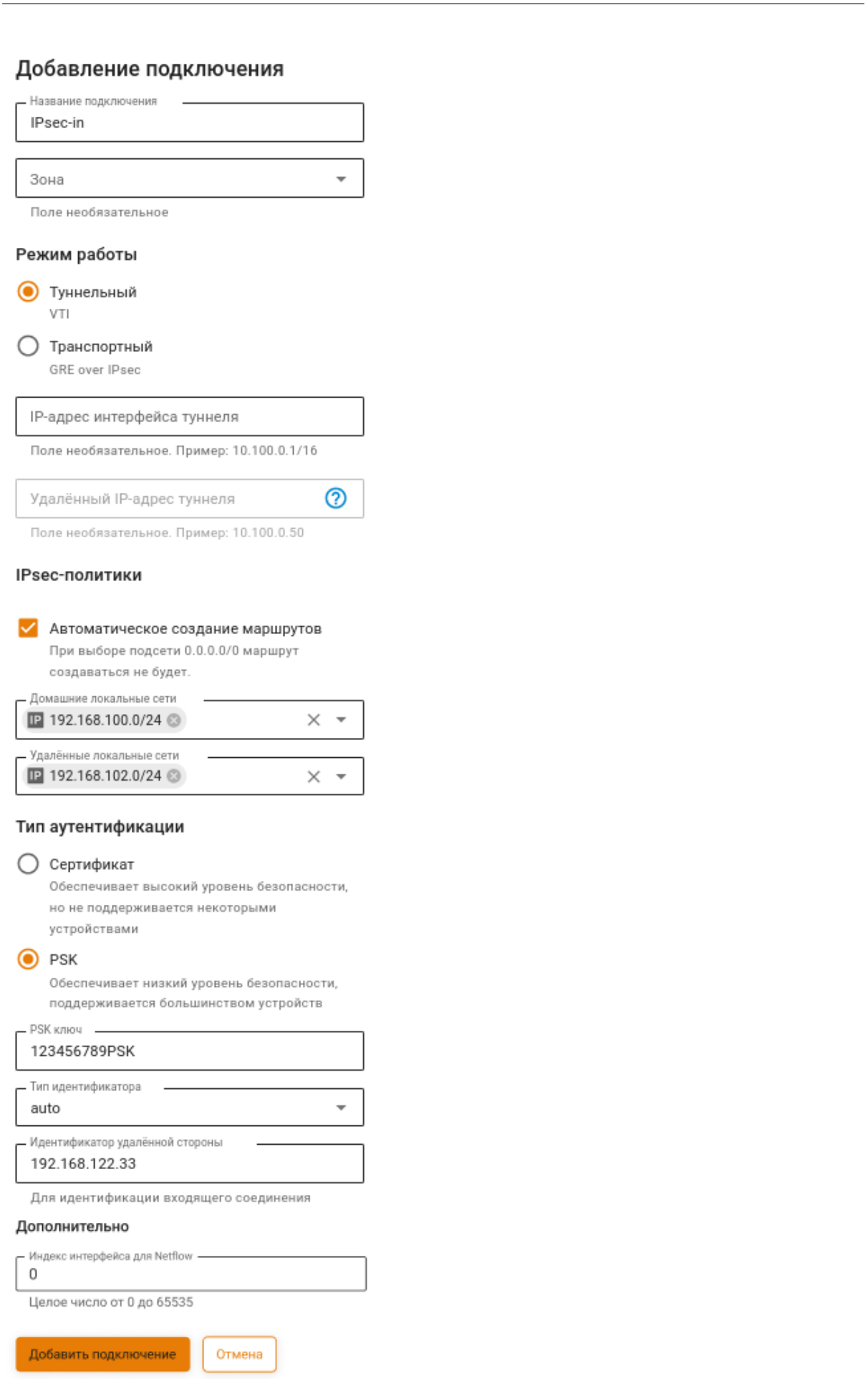
4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице.

Настройка входящего подключения на Ideco NGFW:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**.

2. Добавьте новое подключение и заполните поля:


Добавление подключения
Название подключения
IPsec-in
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
IP-адрес интерфейса туннеля
Поле необязательное. Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
Поле необязательное. Пример: 10.100.0.50
IPsec-политики
Автоматическое создание маршрутов
При выборе подсети 0.0.0.0/0 маршрут создаваться не будет.
Домашние локальные сети
192.168.100.0/24
Удалённые локальные сети
192.168.102.0/24
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
PSK ключ
123456789PSK
Тип идентификатора
auto
Идентификатор удалённой стороны
192.168.122.33
Для идентификации входящего соединения
Дополнительно
Индекс интерфейса для Netflow
0
Целое число от 0 до 65535
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами;
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW, которая будет видна из подсети Kerio Control;
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW;
- **Тип аутентификации** - выберите тип PSK;
- **PSK-ключ** - введите PSK-ключ, который был указан при создании подключения в Kerio;
- **Тип идентификатора** - выберите auto;
- **Идентификатор удаленной стороны** - укажите **Локальный ИД**, указанный при настройке исходящего подключения на Kerio;
- **Индекс интерфейса для Netflow** - введите индекс для идентификации интерфейса (целое число от 0 до 65535), если используете Netflow.

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

Настройка завершена.

Подсказка: При возникновении проблем обратите внимание на настройки файрвола Kerio Control.

18.13.12 Подключение Keenetic по SSTP или IPsec

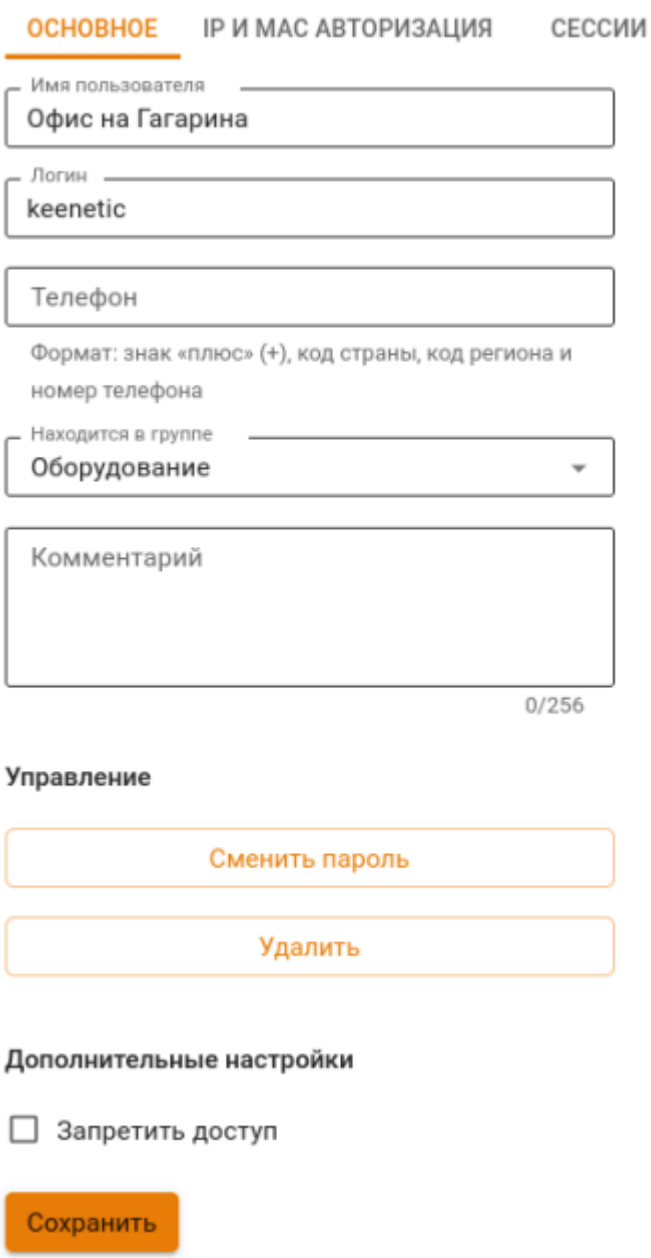
Основное

Если доступ из центрального офиса в сеть за Keenetic не нужен, то воспользуйтесь статьей *Подключение по SSTP Wi-Fi роутеров Keenetic* по client-to-site подключению.

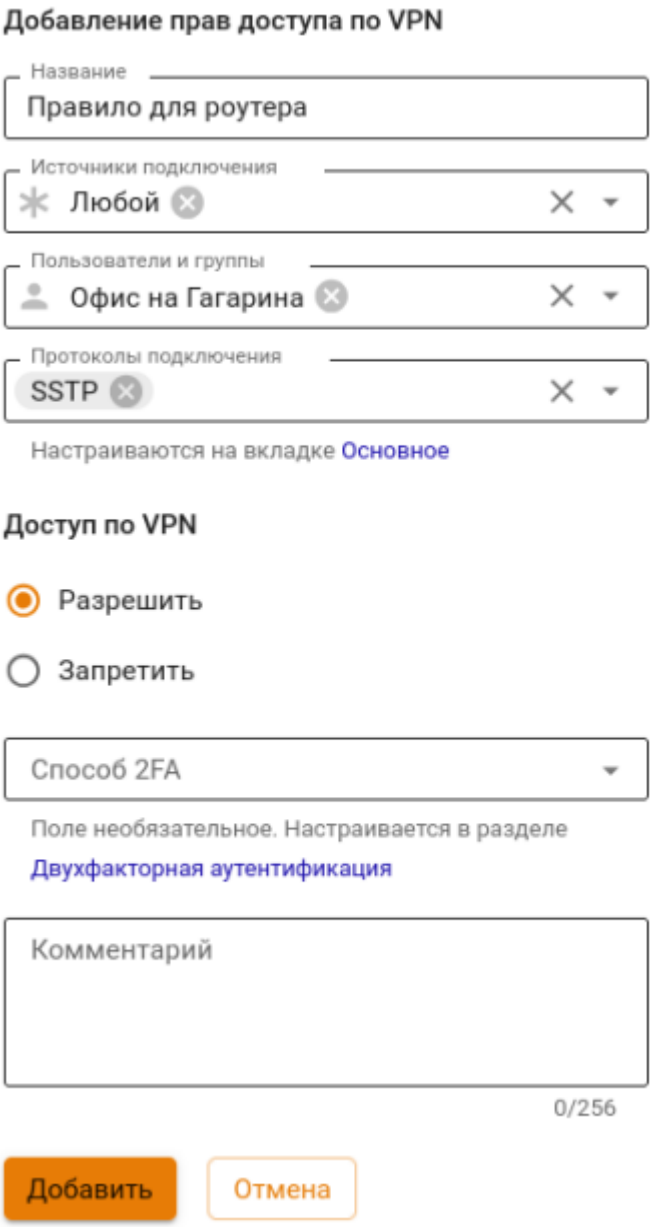
Настройка Ideco NGFW:

1. Включите и настройте порт и домен для SSTP в разделе **Пользователи -> VPN-подключения**.

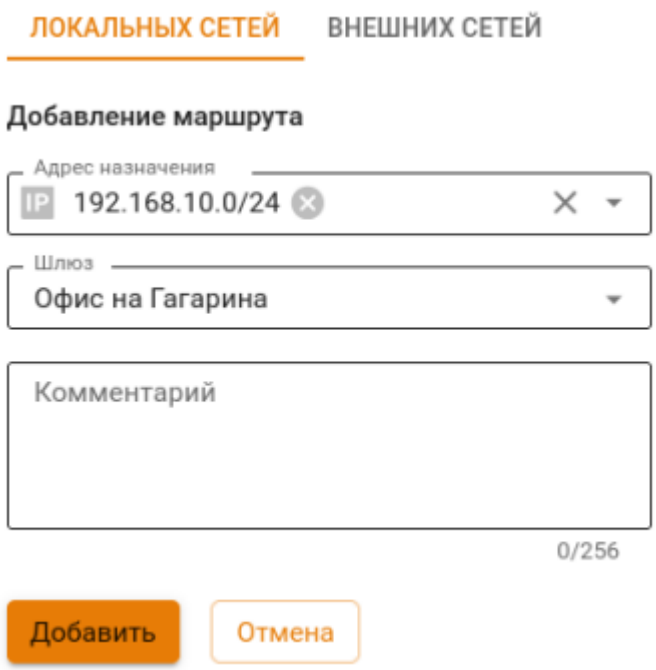
2. В разделе **Пользователи -> Учетные записи** создайте специального пользователя для удаленного роутера. **Логин и пароль пользователя будут использоваться на роутере, сохраните или запишите их:**



3. Перейдите в раздел **VPN-подключения -> Доступ по VPN** и создайте правило доступа по VPN для этого пользователя:



4. Пропишите маршруты в удаленную сеть. Например, если сеть за роутером `192.168.10.0/24`, необходимо добавить маршрут в раздел **Сервисы -> Маршрутизация -> Локальные сети**:



Настройка роутера Keenetic:

Настройте VPN-подключение роутера Keenetic по инструкции для client-to-site подключений.

Не забудьте выполнить все три пункта:

1. Настроить VPN-подключение;

2. Настроить маршруты;

3. Настроить DNS для резолвинга локального домена (если используете Active Directory).

Подсказка: Для проверки связи используйте утилиты ping и traceroute.

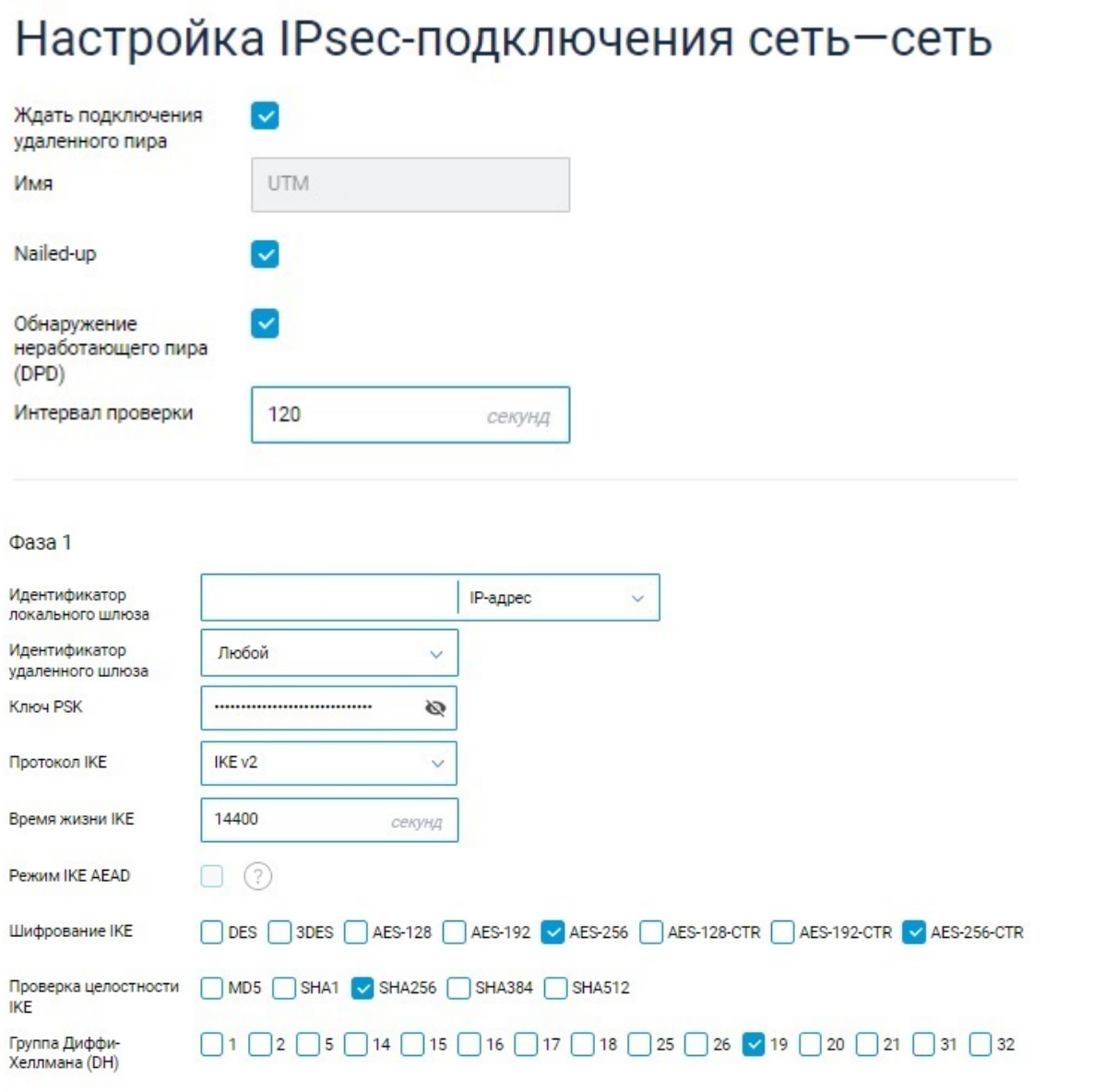
Доступ часто блокируется в Windows из-за настроек сетевых профилей.

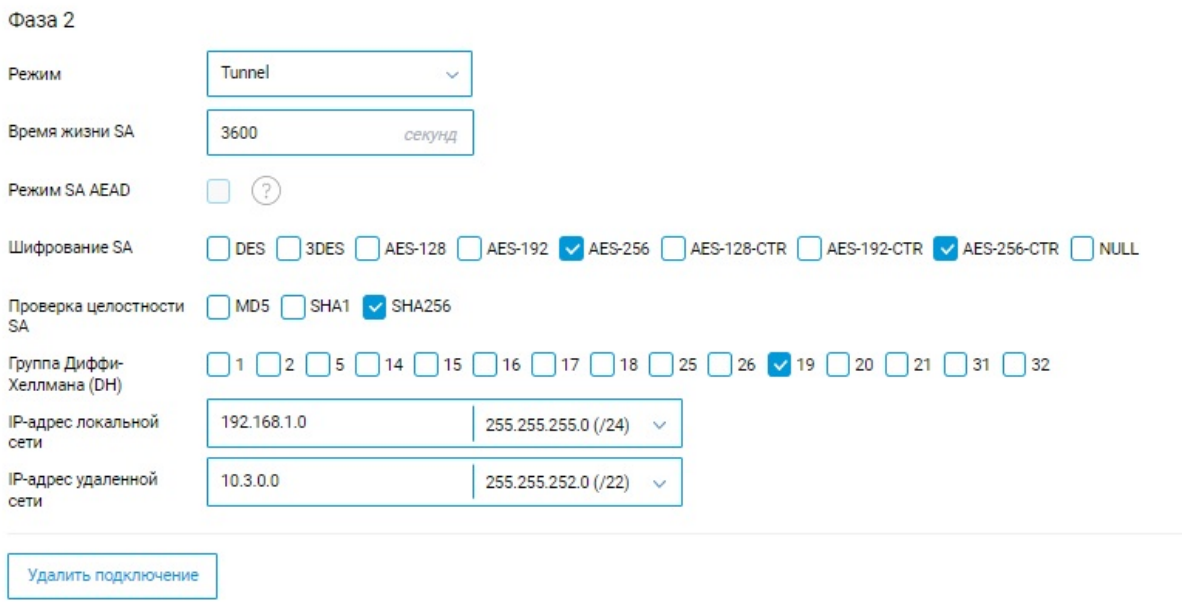
Разрешите доступ до «не локальных» сетей во всех профилях, выполнив команду в PowerShell (запущенного с повышением прав до администратора): `Enable-NetFirewallRule -Group "@FirewallAPI.dll, -28502"`

Основное

На стороне Ideco NGFW произведите настройки подключения в разделе **Сервисы -> IPsec -> Исходящие подключения** или в разделе **Сервисы -> IPsec -> Входящие подключения**.

На стороне устройства Keenetic используйте следующие настройки протоколов шифрования:





18.14 ГОСТ VPN

ГОСТ VPN - это протокол для соединения двух устройств NGFW с использованием технологии виртуальной частной сети. Соединение шифруется с применением российского сертифицированного решения от компании Рутокен. Использование **ГОСТ VPN** в Ideco NGFW не делает его сертифицированным ФСТЭК. Если вам требуется сертифицированная ФСТЭК версия межсетевого экрана, используйте Ideco UTM ФСТЭК.

Используются алгоритмы шифрования:

- **ГОСТ Р 34.10-2012** - для создания ключевой пары;
- **ГОСТ Р 34.12-2015** (*Кузнечик* и *Магма*) - для симметричного шифрования;
- **VKO ГОСТ Р 34.10-2012** - для выработки сессионных ключей.

Туннельное соединение можно использовать в *маршрутизации* локальных сетей, динамической маршрутизации *OSPF* и в *Файрволе*.

В разделе *График загруженности -> ГОСТ VPN* представлена информация о входящих и исходящих соединениях ГОСТ VPN, а также данные мониторинга трафика.

Подсказка: В случае извлечения USB-токена или истечения срока действия сертификатов, хранящихся на USB-токене, VPN-соединение будет разорвано.

18.14.1 Настройка ГОСТ VPN

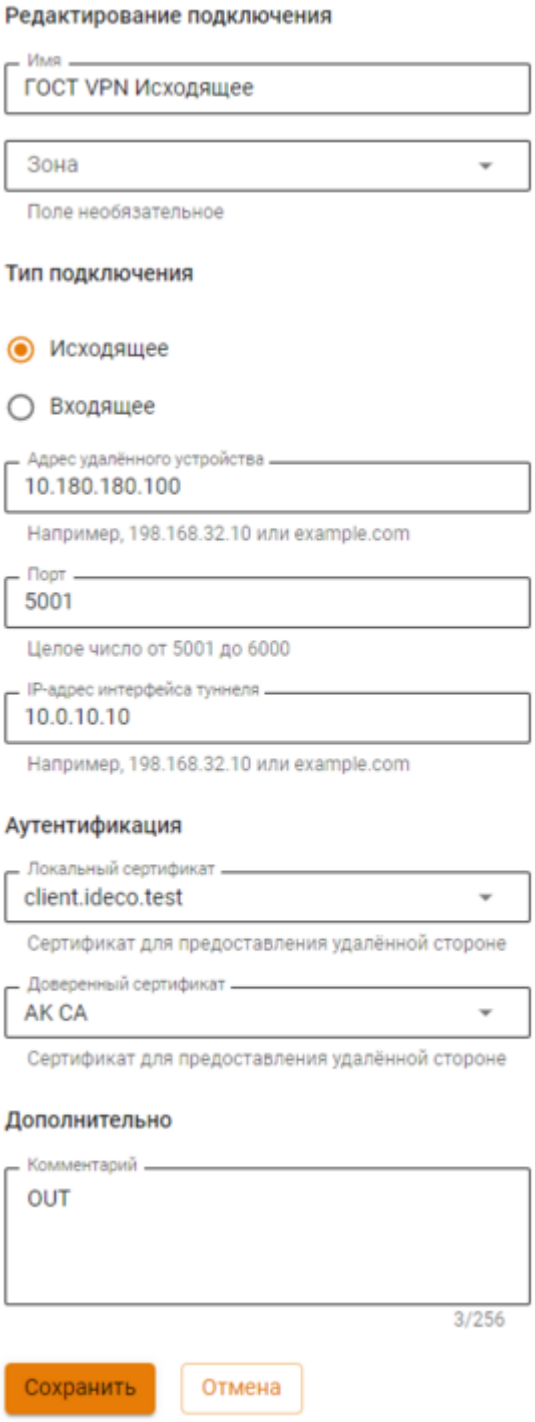
Для настройки ГОСТ VPN необходимо подготовить USB-токен в соответствии с инструкцией, представленной в *статье*, и подключить его к USB-порту сервера.

Для создания соединения между двумя Ideco NGFW необходимо настроить входящее соединение на одном NGFW и исходящее соединение на другом NGFW.

Настройка исходящего подключения

1. Перейдите в раздел **Сервисы -> ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Имя** - максимальное количество символов - 42;
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым;
- **Тип подключения** - выберите **Исходящее**;
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес;

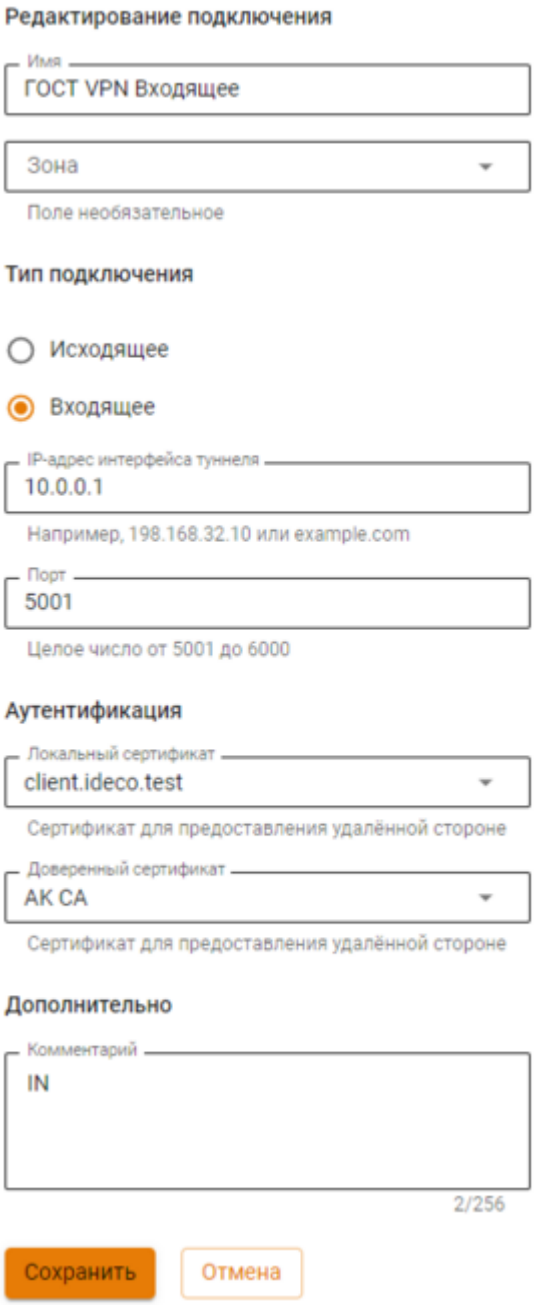
- **Порт** - введите порт в диапазоне от 5001 до 6000;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля, который будет использоваться для маршрутизации данных на сетевом уровне;
- **Локальный сертификат** - выберите локальный сертификат настраиваемого устройства, который содержит приватный ключ и хранится на USB-токене;
- **Доверенный сертификат** - выберите доверенный сертификат, который хранится на том же USB-токене, где находится локальный сертификат.

Как подготовить сертификаты и настроить USB-токен - в *статье*.

Настройка входящего подключения

1. Перейдите в раздел **Сервисы -> ГОСТ VPN** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Имя** - максимальное количество символов - 42;
- **Зона** - выберите зону, в которую нужно добавить подключение, или оставьте поле пустым;
- **Тип подключения** - выберите **Входящее**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля, который будет использоваться для маршрутизации данных на сетевом уровне;
- **Порт** - введите порт в диапазоне от 5001 до 6000;
- **Локальный сертификат** - выберите локальный сертификат настраиваемого устройства, который содержит приватный ключ и хранится на USB-токене;
- **Доверенный сертификат** - выберите доверенный сертификат, который хранится на том же USB-токене, где находится локальный сертификат.

Как подготовить сертификаты и настроить USB-токен - в *статье*.

Статусы подключения

После настройки в таблице **ГОСТ VPN** появится site-to-site соединение, в котором можно отслеживать статус подключения.

Статус подключения ГОСТ VPN	Описание
Подключено	ГОСТ VPN подключен и работает
Соединяется	Происходит установление соединения или ожидание ответа от другого устройства
Отключение	Происходит разъединение подключенных устройств
Не подключено	Отсутствует подключение
Ошибка	Возникла ошибка

18.15 Сертификаты

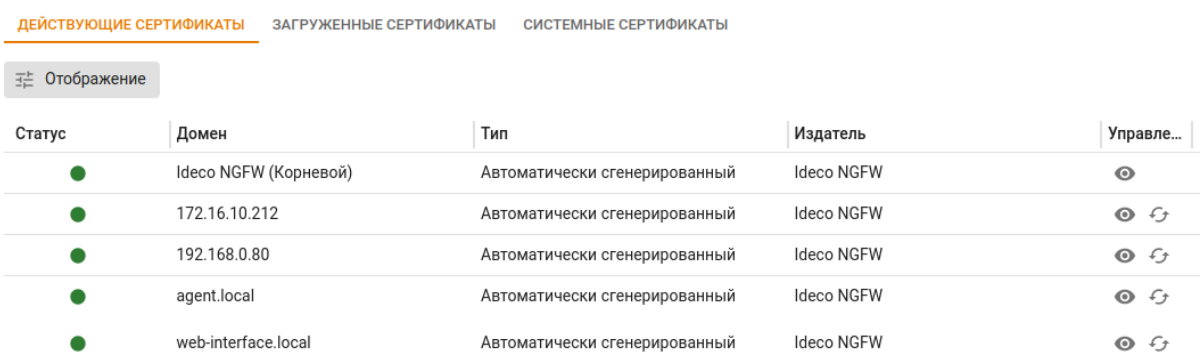
18.15.1 Общая информация

В этом разделе отображаются SSL-сертификаты или цепочки сертификатов, список которых формируется модулями:

- Модуль обратного проксирования;
- VPN-серверы IKEv2 и SSTP;
- Веб-интерфейс, веб-аутентификация;
- Почта.

Для просмотра основной информации о сертификате нажмите кнопку .

Действующие сертификаты

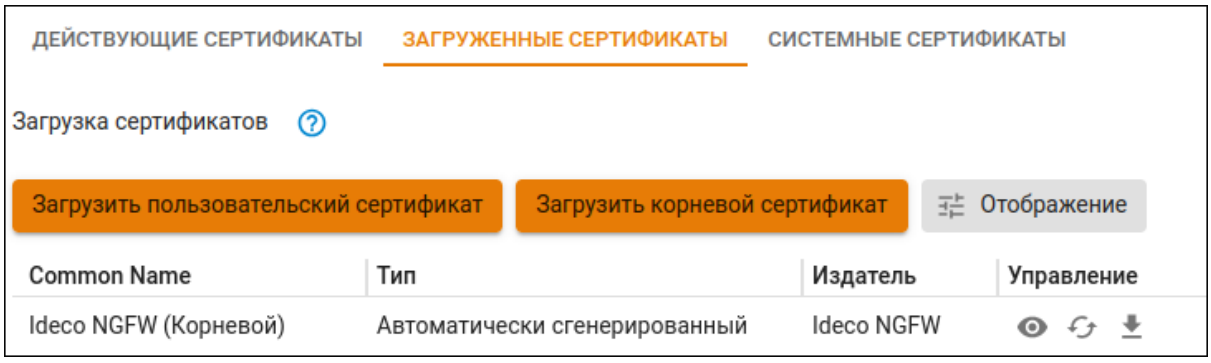


В таблице *Действующие сертификаты* отображаются:

- Автоматически сгенерированные цепочки сертификатов;
- Загруженные цепочки сертификатов, используемые модулями Ideco NGFW.

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

Загруженные сертификаты



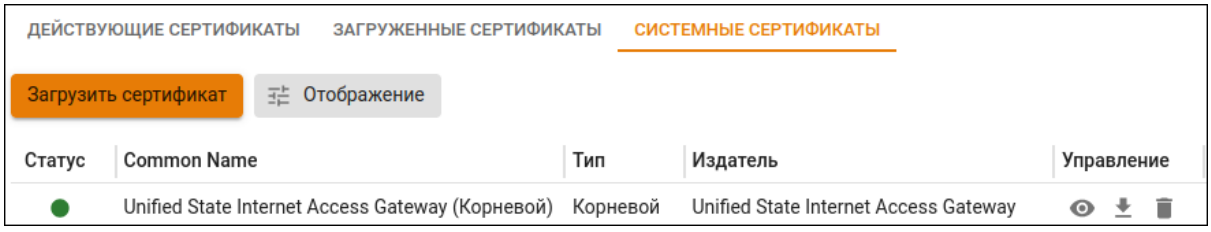
В таблице *Загруженные сертификаты* отображаются:

- Все загруженные цепочки сертификатов;
- Корневой сертификат Ideco NGFW.

Подсказка: Подробная инструкция по загрузке SSL-сертификата в *статье*.

Системные сертификаты

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



18.15.2 Логика работы

NGFW позволяет выпустить или загрузить корневые и не корневые (пользовательские) сертификаты.

Корневые сертификаты обязательно должны иметь разрешение выдавать дочерние сертификаты *X509v3 Basic Constraints: CA: TRUE*. При первоначальной установке и запуске NGFW корневой (самоподписанный) сертификат генерируется автоматически. Его можно скачать, нажав на соответствующую кнопку.

Пользовательские сертификаты - любые сертификаты на домен. Могут быть как подписанными корпоративным корневым сертификатом, так и выданными Certificate Authority (CA) или Центрами сертификации. NGFW автоматически генерирует и подписывает сертификаты на домены, которые вы указываете для модулей.

Процесс выпуска сертификата

Чтобы выпустить сертификат, NGFW выполняет следующие действия:

1. Создает локальную цепочку сертификатов, подписанную корневым (самоподписанным) сертификатом.

2. Параллельно с созданием локальной цепочки сертификатов отправляет запрос на выпуск цепочки в Let's Encrypt.

Условия автоматического выпуска сертификатов Let's Encrypt:

- Наличие доменного имени, зарегистрированного на статический белый IP-адрес, который назначен на внешний интерфейс Ideco NGFW;
- Открытый 80 TCP-порт на внешнем интерфейсе. После установки Ideco NGFW 80 TCP-порт по умолчанию открыт во внешнюю сеть.

Если при соблюдении перечисленных выше условий сертификат Let's Encrypt не выпускается автоматически, перейдите в раздел **Управление сервером -> Терминал** веб-интерфейса NGFW и воспользуйтесь командой:

```
systemctl restart ideco-cert-backend.service
```

Команда для просмотра логов:

```
journalctl -u ideco-cert-backend.service -f
```

3. При успешном выпуске цепочки сертификатов Let's Encrypt заменяет локальную цепочку.

4. Если выпуск цепочки сертификатов Let's Encrypt завершился неудачей, продолжает использовать локальную цепочку сертификатов.

Если требуется повторить попытку получения сертификата Let's Encrypt вместо самоподписанного, то нужно нажать на кнопку **Перевыпустить** в столбце **Управление**.

Подсказка: Сертификат Let's Encrypt **выпускается на 3 месяца** и будет **автоматически перевыпущен** по окончании срока действия.

С 17 версии Ideco NGFW автоматически сгенерированные NGFW пользовательские сертификаты выпускаются на **825 дней** и будут автоматически перевыпущены по окончании срока действия. В предыдущих версиях срок действия таких сертификатов составлял **10 лет**.

Процесс перевыпуска сертификата

Чтобы перевыпустить не корневую цепочку сертификатов, нажмите кнопку  в столбце **Управление** в таблице **Действующие сертификаты**. NGFW будет актуализировать цепочку следующим образом:

- Проверит загруженные сертификаты. Если сертификат найден, то заменит действующую цепочку сертификатов на домен на найденную;
- Если для данного домена новые сертификаты не загружались, Ideco NGFW обратится к Let's Encrypt для выпуска новой цепочки;
- Если цепочка от Let's Encrypt получена, она отобразится в таблице;
- Если получить цепочку сертификатов от Let's Encrypt не удалось, продолжит использовать локальную цепочку сертификатов.

Для перевыпуска корневого сертификата нажмите кнопку  напротив соответствующей цепочки в таблице **Загруженные сертификаты**. NGFW заменит ее на автоматически сгенерированный корневой сертификат.

Предупреждение: При замене/перевыпуске корневого сертификата в разделе *Сертификаты*, IPsec-подключения перестанут работать. Для восстановления соединения вам потребуется заменить сертификат в свойствах подключения. Для этого перейдите в раздел **Сервисы -> IPsec** и нажмите на  с нужным подключением.

Внимание: Для работы *Ideco Client под MacOS* необходимо, чтобы срок действия сертификата на домен или IP-адрес NGFW, введенный в разделе **Пользователи -> Ideco Client** не превышал 825 дней.

Проверить, что срок действия загруженного пользовательского или сгенерированного NGFW сертификата не превышает **825 дней**, можно в разделе **Сервисы -> Сертификаты -> Действующие сертификаты**, нажав на  .

Чтобы перевыпустить локальную цепочку сертификатов, выполните действия:

1. Перейдите в раздел **Управление сервером -> Терминал**.

2. Перейдите в директорию `/var/cache/ideco/cert-backend`, выполнив команду:

```
cd /var/cache/ideco/cert-backend
```

3. Выведите содержимое директории, выполнив команду `ls`.

4. Скопируйте название файла сертификата, который требуется перевыпустить. Названия файлов будут иметь вид:

`test.ideco.ru-self-sign_chain_833bcda78229059d2c2886548c75e9e3.pem`, где `test.ideco.ru` - доменное имя или IP-адрес, на который выпущен сертификат.

5. Удалите файл, выполнив команду:

```
rm test.ideco.ru-self-sign_chain_d1f73bf1fcc4d55ca31004ecb13d19b3.pem
```

6. Перейдите в раздел **Сервисы -> Сертификаты -> Действующие сертификаты** и перевыпустите сертификат на домен или IP-адрес NGFW, нажав на  .

Проверить, перевыпустился ли сертификат на новый срок, можно , нажав на  .

18.15.3 Загрузка SSL-сертификата на сервер

Подсказка: Видеоинструкция по загрузке пользовательского и корневого сертификата на Ideco NGFW:

Ссылка на видеоинструкцию по загрузке пользовательского и корневого сертификата на NGFW

Перед загрузкой корневого или пользовательского сертификата на NGFW убедитесь, что они отвечают требованиям:

- Сертификаты должны иметь расширения *.pem*. Если у вашего сертификата другое расширение, конвертируйте его. Как это сделать описано ниже в разделе **Конвертация сертификата из формата pkcs12 в формат pem с помощью openssl**;
- В составе сертификата **Издатель** и **Субъект** должны содержать поле **CN** (Common Name, общее имя). При загрузке собственной цепочки сертификатов **CN** (общее имя) последнего сертификата в цепочке должно соответствовать домену, для которого сертификат загружается;
- Цепочка сертификата должна быть валидной и соответствовать структуре:

```
Приватный ключ
Сертификат на домен (Common Name)
Сертификат из состава бандла vendor-сертификатов (промежуточный сертификат, если есть)
...
Основной (корневой) сертификат
```

Если сертификат самоподписанный, его структура может содержать всего 2 блока - **Приватный ключ** и **Сертификат на домен (Common Name)**. Если структура сертификата невалидна, переходите к разделу ниже **Подготовка SSL-сертификата для загрузки на NGFW**.

Предупреждение: Если вы хотите загрузить сертификат как корневой, удостоверьтесь, что он может выдавать дочерние сертификаты: *X509v3 Basic Constraints: CA: TRUE* (это можно проверить в открытом ключе сертификата).

Загрузка SSL-сертификата на NGFW

Если сертификат удовлетворяет всем перечисленным выше условиям, загрузите его на NGFW. Для этого:

1. Перейдите в раздел **Сервисы -> Сертификаты -> Загруженные сертификаты**.

2. Нажмите **Загрузить корневой сертификат**.

3. Выберите нужный сертификат.

Подсказка: Загруженный корневой сертификат автоматически переподпишет все пользовательские сертификаты на домены, которые ранее автоматически сгенерировал NGFW. Сертификаты Let's Encrypt и сертификаты, купленные у CA и Центров сертификации, переподписаны не будут.

Если в инфраструктуре компании есть свой корневой центр сертификации, выпустите сертификат с шаблоном **Subordinate Certification Authority** и загрузите его на Ideco NGFW в качестве корневого. Это позволит выстроить цепочку доверия для автоматически выданных сертификатов до корневого центра сертификации. Пользовательские компьютеры будут доверять сертификатам, выданным на стороне NGFW.

Подготовка SSL-сертификата для загрузки на NGFW:

При покупке доверенного SSL-сертификата на домен у Certificate Authority или Центра сертификации данные для его установки как правило высылаются электронным письмом в разрозненном виде. Для кор-

ректной загрузки сертификаты на домен, промежуточные и корневые сертификаты нужно собрать в один файл в правильном порядке.

Предупреждение: Некоторые данные (CSR-запрос и приватный ключ) генерируются только во время покупки SSL-сертификата и не высылаются в письме. Сразу сохраняйте такие данные на своем компьютере.

Корневые (самоподписанные) сертификаты также требуют построения цепочек. Структура таких сертификатов может содержать 2 блока - *Приватный ключ* и *Сертификат на домен (Comon Name)* - или более в зависимости от того, есть ли у вас промежуточные сертификаты (из состава бандла vendor-сертификатов).

Для создания корректной цепочки сертификатов выполните действия:

1. Создайте текстовый файл вида:

```
-----BEGIN PRIVATE KEY-----
.....
.....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
.....
-----END CERTIFICATE-----
```

2. Добавьте в блок (**BEGIN PRIVATE KEY**) *расшифрованный* приватный ключ.

Если Центр сертификации выдал приватный ключ в зашифрованном виде, расшифруйте его с помощью passphrase (фразы-пароля).

3. В каждый из блоков (**BEGIN CERTIFICATE**) добавьте сертификат. В начало - сертификат на домен, следом - сертификаты из бандла vendor-сертификатов (если они есть), в самый конец - корневой сертификат. Файл должен получить такую структуру:

```
Приватный ключ
Сертификат на домен
Сертификат из состава бандла vendor-сертификатов (при наличии)
...
Основной (корневой) сертификат
```

4. Сохраните файл с расширением **.pem** и загрузите его на NGFW.

Подсказка: С общепринятым стандартом создания файла-цепочки сертификатов можно также ознакомиться здесь: https://www.digicert.com/ssl-support/pem-ssl-creation.htm.

Конвертация сертификата из формата pkcs12 в формат pem с помощью openssl:

Подсказка: Для конвертации сертификата с помощью openssl на Windows воспользуйтесь ссылкой для загрузки openssl на компьютер.

Для конвертации сертификата из формата **pkcs12** в формат **pem** выполните действия:

1. Откройте командную строку.

2. Введите команду `openssl pkcs12 -in certificate.pkcs12 -out certificate.pem` (сконвертирует сертификат в нужный формат), где:

- **certificate.pkcs12** - исходный сертификат который был получен у центра сертификации;
- **certificate.pem** - результат конвертации.

3. Откройте полученный файл и убедитесь, что он имеет структуру:

```
-----BEGIN CERTIFICATE-----
..............
..............
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
..............
..............
-----END PRIVATE KEY-----
```

Если в сертификате написано `--BEGIN ENCRYPTED PRIVATE KEY--`, расшифруйте его, введя в openssl команду
`openssl rsa -in certificate.pem -out certificate_decoded.pem`, где:

- **certificate.pem** - файл который был получен после конвертации;
- **certificate_decode.pem** - результат расшифровки.

18.15.4 Создание самоподписанного сертификата с помощью PowerShell

Основное

Чтобы создать корневой (самоподписанный) сертификат с помощью PowerShell, выполните следующие действия:

1. Запустите PowerShell от имени администратора.

2. Сгенерируйте сертификат, выполнив команду:

```
New-SelfSignedCertificate -DnsName test.ideco.com -TextExtension @("2.5.29.19={text}
↪CA=true") -CertStoreLocation cert:\LocalMachine\My
```

Где `test.ideco.com` - домен.

```
Установите последнюю версию PowerShell для новых функций и улучшения! https://aka.ms/PSWindows

PS C:\Users\a.istomina> New-SelfSignedCertificate -DnsName test.ideco.com -TextExtension @("2.5.29.19={text}CA=true") -C
ertStoreLocation cert:\LocalMachine\My


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
2284919151C5C624341D7B75FE034B00DF6A44FA  CN=test.ideco.com
```

Для просмотра сгенерированного сертификата выполните команду `certlm.msc`.

3. Сформируйте пароль для сертификата:

```
$CertPassword = ConvertTo-SecureString -String ‘‘12345’’ -Force -AsPlainText
```

Где 12345 - пароль.

4. Экспортируйте сертификат выполнив команду:

```
Export-PfxCertificate -Cert cert:\LocalMachine\My\
↪2284919151C5C624341D7B75FE034B00DF6A44FA -FilePath C:\Users\pende\ssl\test.ideco.
↪pfx -Password $CertPassword
```

- `2284919151C5C624341D7B75FE034B00DF6A44FA` - идентификатор сертификата полученный на шаге 2;
- `C:\Users\pende\ssl\test.ideco.pfx` - путь до папки, в которую требуется сохранить сертификат (проверьте его корректность во избежание ошибок).

5. Конвертируйте сертификат в расширение .pem (пример конвертора).

Подсказка: Для загрузки сертификата на сервер воспользуйтесь статьей *Загрузка SSL-сертификата на сервер*

18.15.5 Создание сертификата с помощью openssl

Основное

Подсказка: Видеоинструкция по созданию пользовательских и корневых сертификатов:

Ссылка на видеоинструкцию по созданию пользовательских и корневых сертификатов

Подсказка: Используйте эту статью, если вы пользуетесь операционной системой с ядром Linux. При использовании операционной системы Windows воспользуйтесь статьей *Создание самоподписанного сертификата с помощью PowerShell*.

Для создания самоподписанного сертификата выполните действия:

1. Создайте закрытый ключ для сертификата:

```
openssl genrsa -out ca.key 2048
```

Где `ca.key` - файл с приватным ключом.

2. Создайте запрос на подпись сертификата:

```
openssl req -key ca.key -new -out cert.csr
```

- `ca.key` - файл с приватным ключом;
- `cert.csr` - файл с запросом на подпись.

3. Создайте файл с именем test.txt:

```
cat >> ./test.txt << EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:TRUE
keyUsage = digitalSignature, keyCertSign, cRLSign
subjectAltName=DNS:test.com
EOF
```

- `test.txt` - файл с расширениями сертификата;
- `test.com` - доменное имя сервера.

4. Сгенерируйте самоподписанный сертификат:

```
openssl x509 -extfile ./test.txt -signkey ca.key -in cert.csr -req -days 365 -out ca.
↪crt
```

- `test.txt` - файл, созданный в 3 пункте;
- `ca.key` - файл с приватным ключом;
- `cert.csr` - файл с запросом на подпись сертификата;
- `ca.crt` - файл со сгенерированным сертификатом.

5. Добавьте к сертификату приватный ключ:

```
cat ca.key ca.crt > server.pem
```

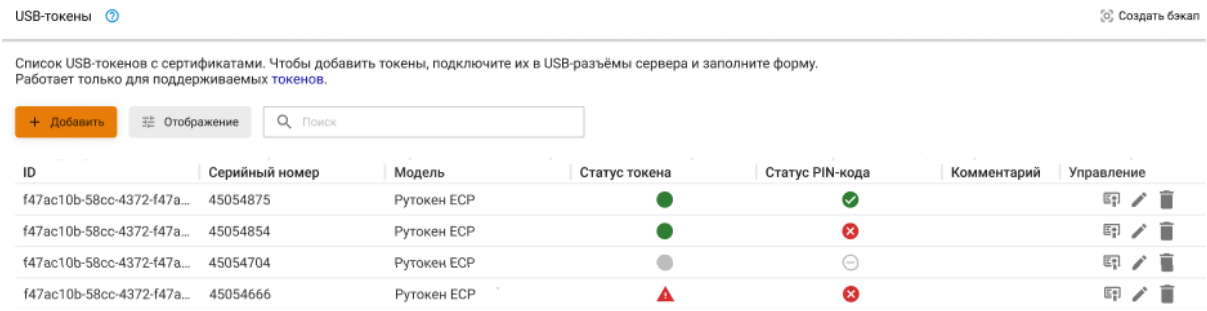
Где `server.pem` - самоподписанный сертификат для загрузки на сервер.

Подсказка: Для загрузки сертификата на сервер воспользуйтесь статьей *Загрузка SSL-сертификата на сервер*

18.16 USB-токены

Подсказка: **Ideco NGFW** поддерживает только USB-токен модели **Рутокен ЭЦП 3.0**. USB-токены других моделей могут не отображаться в веб-интерфейсе **Ideco NGFW**.

В таблице USB-токенов представлена информация о серийном номере, модели, метке ключа и корректности настройки USB-токена:



Статус USB-токена	Описание
	Токен подключен в USB-разъем сервера
	Токен не подключен в USB-разъем сервера
	Возникла ошибка или токен заблокирован

Статус PIN-кода	Описание
	Верный PIN-код
	Неизвестеный статус PIN-кода. PIN-код был введен, но USB-токен не был установлен в USB-разъем сервера. USB-токен с верным PIN-кодом был извлечен из USB-разъема сервера
	Неверный PIN-код

Чтобы проверить содержимое USB-токенов и убедиться, что на них загружены все необходимые сертификаты, нажмите на  у соответствующего USB-токена. Откроется список всех загруженных сертификатов с подробной информацией.

18.16.1 Подготовка USB-токена

Процесс подготовки USB-токена ЭЦП версии 3.0 от компании **Рутокен** подробно описан в документации производителя. В помощь предлагаются статьи, которые помогут разобраться в этом вопросе:

- Начало работы с Рутокеном;
- Рутокен и OpenSSL;
- Рутокен для Windows;
- Рутокен для отечественных ОС Линукс;
- Рутокен для КриптоПро.

18.16.2 Настройка USB-токена на Ideco NGFW

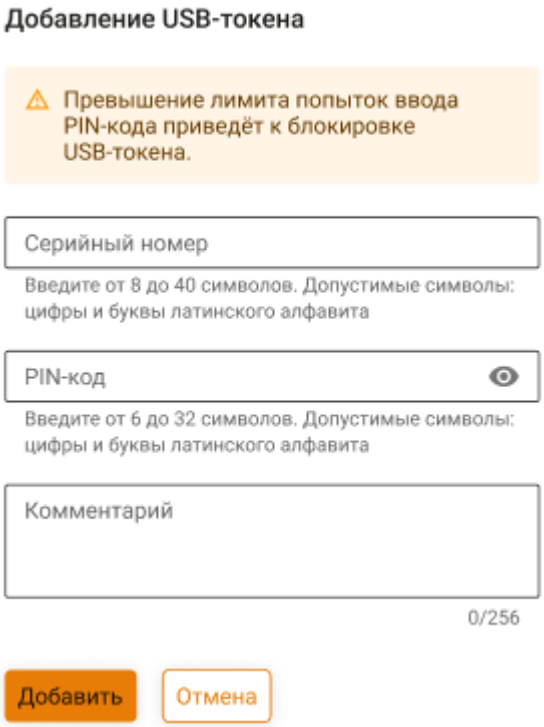
Для работы Ideco NGFW с USB-токеном необходимо ввести корректный PIN-код. После этого сервисы NGFW смогут использовать токен для выполнения криптографических операций.

> **Предупреждение: Важно!** При превышении лимита попыток неправильного ввода PIN-кода устройство будет заблокировано. Лимит устанавливается производителем и считается до правильного ввода PIN-кода.

Чтобы добавить новый USB-токен, выполните действия:

1. Подготовьте USB-токен в соответствии с инструкциями производителя, представленными выше.

2. Подключите его к USB-разъему вашего сервера. Нажмите **Добавить** и заполните необходимые поля:



Расшифровка полей:

- **Серийный номер** - укажите серийный номер USB-токена;
- **PIN-код** - введите PIN-код;
- **Комментарий** - необязательное поле.

3. Нажмите **Добавить**.

19. Отчеты и журналы

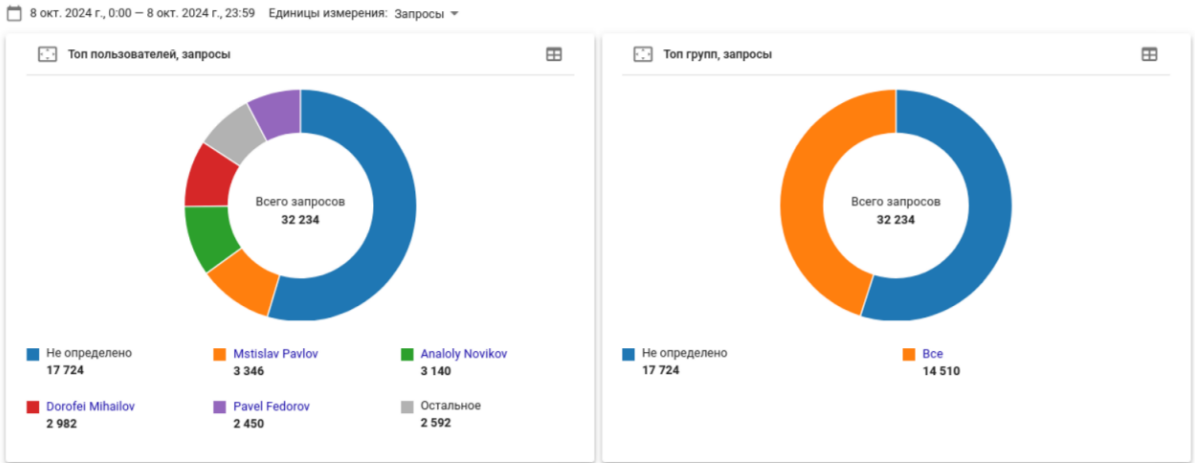
19.1 Трафик

При переводе ползунка **Трафик** в левом верхнем углу в положение **Включен** раздел начинает собирать статистику из *Контент-фильтра* (категории и сайты) и *Контроля приложений* (протоколы) и отображает в виде виджетов.

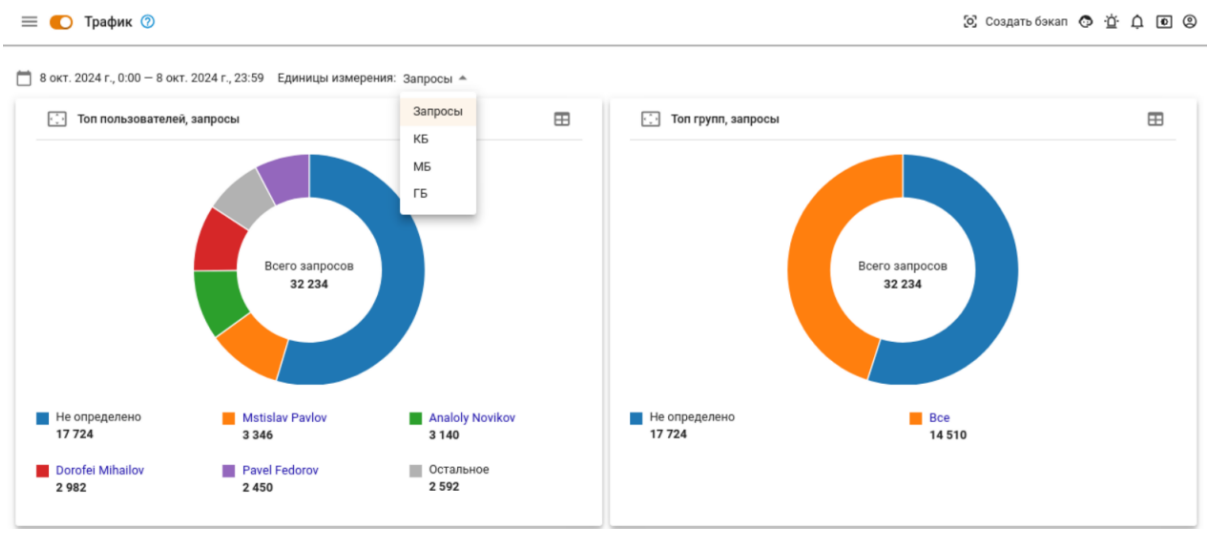
19.1.1 Способ отображения информации:

Круговая диаграмма ( ) и таблица ( )

Содержит топ-6 объектов. Каждый объект кликабелен и ведет на страницу с виджетами, в которых статистика фильтруется по этому объекту:

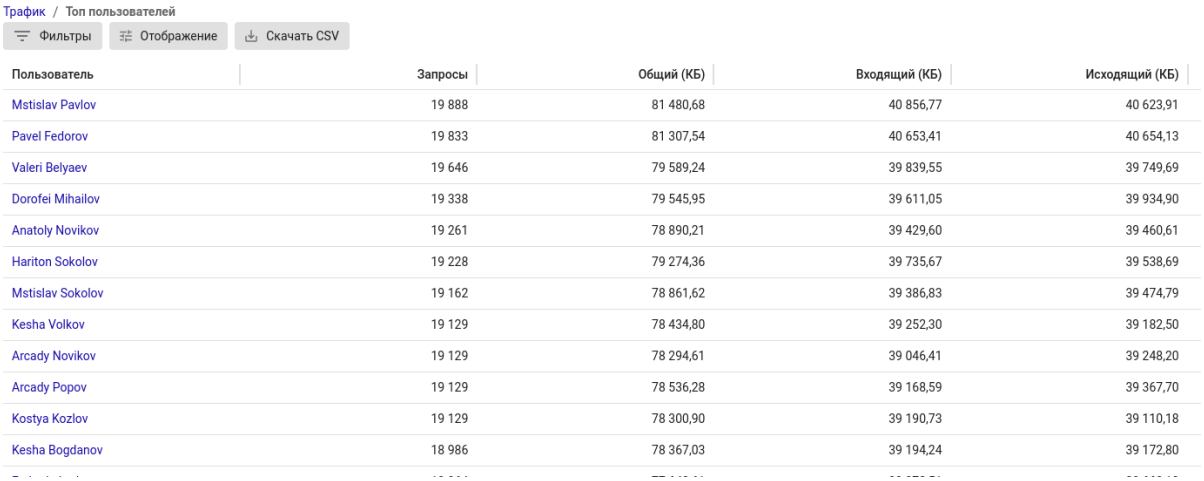


Единицу измерения можно изменить по кнопке над виджетами:



Развернутый режим ( )

Содержит данные по всем объектам из топа. Для поиска по объектам воспользуйтесь **Фильтром** (Фильтры).



Пользователь	Запросы	Общий (КБ)	Входящий (КБ)	Исходящий (КБ)
Mstislav Pavlov	19 888	81 480,68	40 856,77	40 623,91
Pavel Fedorov	19 833	81 307,54	40 653,41	40 654,13
Valeri Belyaev	19 646	79 589,24	39 839,55	39 749,69
Dorofei Mihailov	19 338	79 545,95	39 611,05	39 934,90
Anatoly Novikov	19 261	78 890,21	39 429,60	39 460,61
Hariton Sokolov	19 228	79 274,36	39 735,67	39 538,69
Mstislav Sokolov	19 162	78 861,62	39 386,83	39 474,79
Kesha Volkov	19 129	78 434,80	39 252,30	39 182,50
Arcady Novikov	19 129	78 294,61	39 046,41	39 248,20
Arcady Popov	19 129	78 536,28	39 168,59	39 367,70
Kostya Kozlov	19 129	78 300,90	39 190,73	39 110,18
Kesha Bogdanov	18 986	78 367,03	39 194,24	39 172,80

Если в левом верхнем углу установлен флаг в строке **Запросы**, то объекты отфильтруются по убыванию по колонке **Запросы**. Если **Трафик**, - по убыванию в колонке **Входящий**.

Подсказка: Время и дата в виджете отображается в часовом поясе сервера.

Примеры использования:

На какие запрещенные сайты переходил определенный пользователь:

- Откройте раздел **Отчеты и журналы -> Трафик**;
- В виджете **Топ пользователей** найдите нужного пользователя и кликните по нему.

  Если пользователя нет в списке, то нажмите **Развернуть** () в левом верхнем углу виджета (откроется список всех пользователей);
- В виджете **Топ заблокированных сайтов** NGFW покажет топ-5 блокировок. Для просмотра полного списка блокировок нажмите **Развернуть** ().

Каким пользователям заблокировали определенное приложение:

- Откройте раздел **Отчеты и журналы -> Трафик**;
- В виджете **Топ заблокированных протоколов** найдите требуемый протокол и кликните по нему. Если его нет в списке, то нажмите **Развернуть** ();
- Чтобы увидеть список всех пользователей, у которых был заблокирован этот протокол, на открывшейся странице найдите виджет **Топ пользователей**

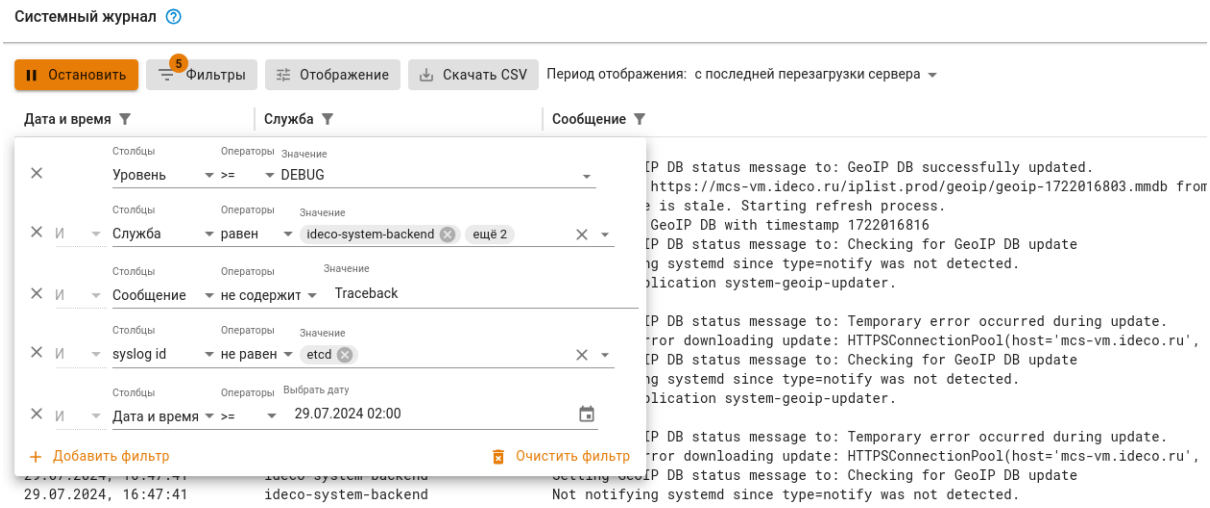
  и нажмите **Развернуть** ().

Подробнее о создании собственных шаблонов со статистикой - в статье *Конструктор отчетов*.

Подсказка: Время хранения логов в разделе **Журналы** - три месяца. После этого логи доступны в разделе **Управление сервером -> Терминал**.

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:



Подсказка: По кнопке **Скачать CSV** сохраняются те строки логов, которые заданы фильтрацией.

Список служб, доступных в разделе:

- **Учетные записи** - `ideco-user-backend`;
- **Личный кабинет пользователя** - `ideco-user-cabinet-backend`;
- **Файрвол** - `ideco-firewall-backend`;
- **Контроль приложений** - `ideco-app-backend`;
- **Контент-фильтр** - `ideco-content-filter-backend`;
- **Ограничение скорости** - `ideco-shaper-backend`;
- **Антивирус** - `ideco-av-backend`;
- **Предотвращение вторжений** - `ideco-suricata-event-syncer`, `ideco-suricata-backend`;
- **Объекты** - `ideco-alias-backend`;
- **Сетевые интерфейсы** - `ideco-network-backend`, `ideco-network-nic`;
- **Маршрутизация** - `ideco-routing-backend`, `ideco-routing-rest`;
- **Прокси** - `ideco-proxy-backend`, `squid`;
- **Обратный прокси** - `ideco-reverse-backend`;
- **DNS** - `ideco-dns-backend`, `unbound`, `nsd`, `unbound-anchor`, `unbound-keygen`;
- **DDNS** - `ideco-dns-backend`;
- **DHCP** - `ideco-dhclient`, `ideco-dhcp-server-backend`;

- **NTP** - `chronyd`;
- **IPsec** - `ideco-ipsec-backend`;
- **Ideco Center** - `ideco-central-console-backend`;
- **VCE** - `ideco-vce-backend`;
- **Кластеризация** - `ideco-cluster-backend`;
- **Обновления** - `ideco-sysupdate-backend`;
- **Бэкапы** - `ideco-backup-backend`;
- **Лицензия** - `ideco-license-backend`;
- **VPN-подключения** - `ideco-vpn-authd`, `ideco-vpn-dhcp-backend`, `ideco-vpn-dhcp-server`, `ideco-vpn-servers-backend`, `ideco-vpn-netns`, `ideco-vpn-sessions-sync`;
- **Авторизация** - `ideco-auth-backend`;
- **Веб-аутентификация, Двухфакторная аутентификация** - `ideco-web-authd`;
- **Active Directory** - `ideco-ad-backend`;
- **ALD Pro** - `ideco-ald-rest`, `ideco-ald-backend`;
- **Ideco Client** - `ideco-agent-websocket`, `ideco-agent-backend`, `ideco-app-stats`;
- **Syslog** - `ideco-logs-backend`;
- **Отчеты и журналы** - `ideco-logs-backend`, `ideco-reports-backend`, `ideco-logs-syncer`;
- **Действия администраторов** - `ideco-audit-backend`;
- **Обнаружение устройств** - `ideco-netscan-backend`;
- **Web Application Firewall** - `ideco-waf-backend`, `ideco-waf-event-syncer`;
- **IGMP Proxy** - `ideco-igmpproxy-backend`;
- **Сертификаты** - `ideco-cert-backend`;
- **Почтовый релей** - `ideco-mail-backend`;
- **Сбор анонимной статистики о работе сервера** - `ideco-gatherstat-backend`;
- **Локальное меню** - `ideco-local-menu`;
- **Отправка оповещений через телеграм-бота** - `ideco-mir-alerts`;
- **Проверка скорости** - `ideco-speedtest`;
- **Дополнительно (язык, часовой пояс, включение особых режимов работы)** - `ideco-system-backend`;
- **Защита от повторяющихся зловредных или подозрительных действия, в т.ч. от брутфорс-атак (brute force - атака полным перебором)** - `fail2ban`;
- **Доступ по SSH** - `sshd`.

Служебное:

- `clickhouse-server` - сервер базы данных;
- `ideco-etcd-runtime`, `ideco-etcd-permanent` - локальная база данных;
- `prometheus`, `prometheus-node-exporter` - сбор метрик и статистики.

19.2.1 Защита от брутфорс-атак

Подсказка: Защита от брутфорс-атак (brute force - атака полным перебором) работает только для NGFW.

После 6 неудачных попыток ввода пароля в течение 15 минут IP-адрес подбирающего блокируется на 45 минут.

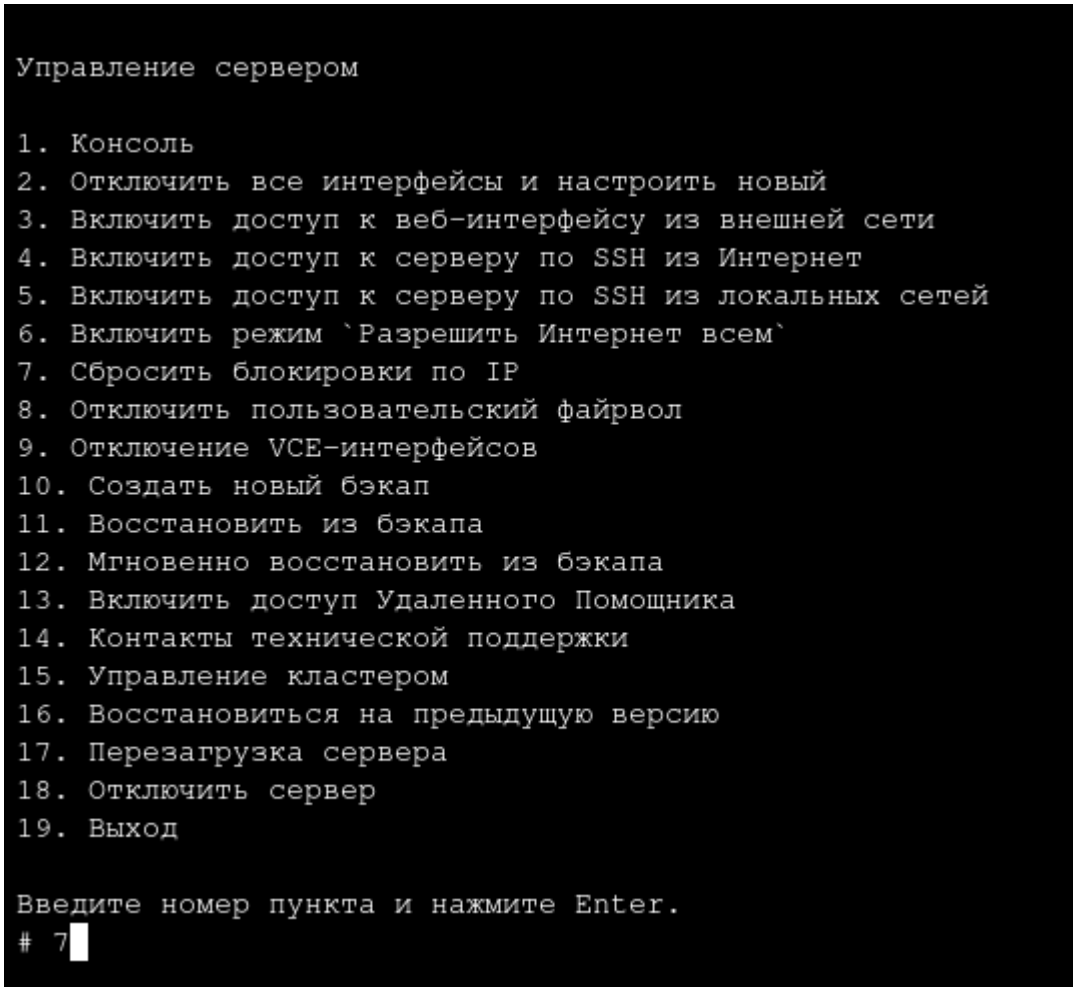
Логи службы `fail2ban` можно увидеть:

- В веб-интерфейсе в разделе **Отчеты и журналы -> Системный журнал**, задав фильтр `fail2ban`.
- В разделе **Управление сервером -> Терминал**, введя команду `journalctl -u fail2ban`.

Для разблокировки через терминал используйте команды:

- `fail2ban-client unban --all` - команда используется для снятия всех блокировок;
- `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса, указав нужный IP-адрес в качестве аргумента.

Также можно сбросить блокировки из локального меню шлюза, выбрав опцию **Сбросить блокировки по IP**:



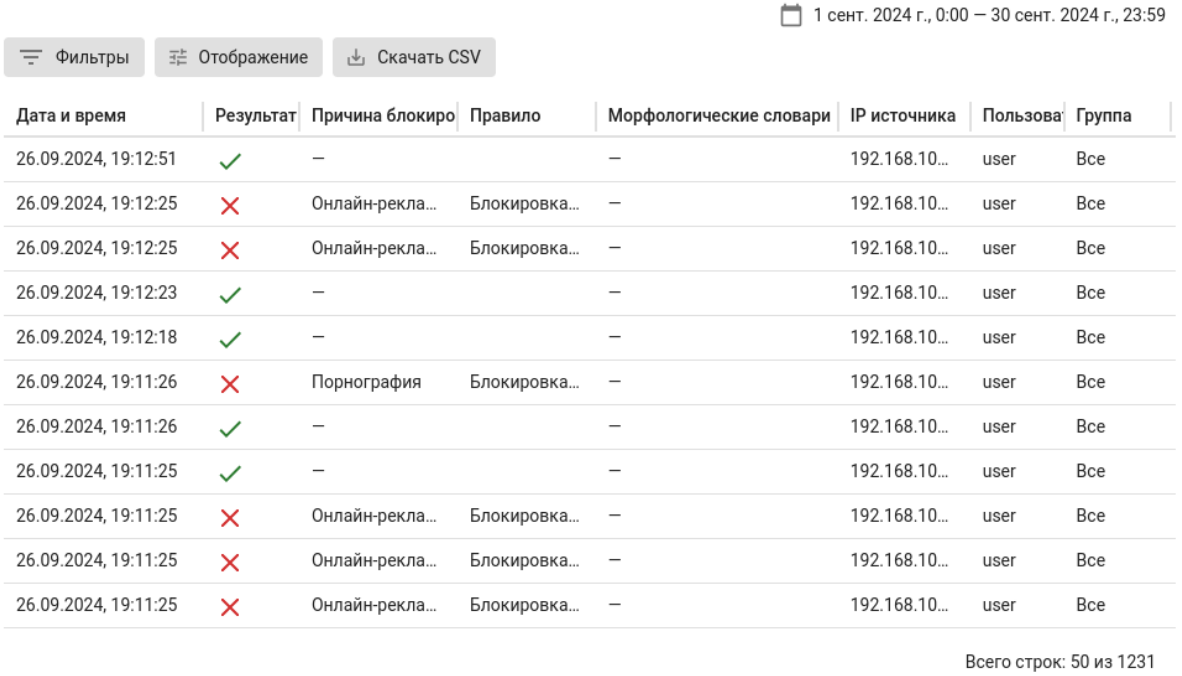
19.3 Журнал веб-трафика

19.3.1 Основное

Раздел позволяет посмотреть результат обработки пользовательского запроса службой **Контент-фильтра**. Для просмотра **Журнала веб-трафика** перейдите в раздел **Отчеты и Журналы -> Журнал веб-трафика**.

Результаты обработки службы:

- - **Разрешено**
- - **Расшифровано**
- - **Запрещено**
- - **Перенаправлено на**



Подсказка: Если нет доступа к какому-либо интернет-ресурсу, воспользуйтесь разделом **Журнал веб-трафика** для поиска правила, блокирующего этот ресурс.

Подсказка: Для просмотра блокировок по конкретному правилу воспользуйтесь кнопкой **Фильтры**, указав в форме наименование правила и оператор.

19.4 Журнал трафика

19.4.1 Основное

На вкладке отображается информация о срабатывании правил **Файрвола** (таблицы FORWARD, DNAT, SNAT и INPUT), в том числе - о профилях **Предотвращения вторжений** и **Контроля приложений**.

Раздел позволяет быстро выявить модуль фильтрации, который блокирует трафик, а также выявить DDoS-атаки.

В таблицу попадают соединения, которые подошли под правила в таблице *Логирования*. Фильтрация наиболее быстро работает с полями **Пользователь источника**.

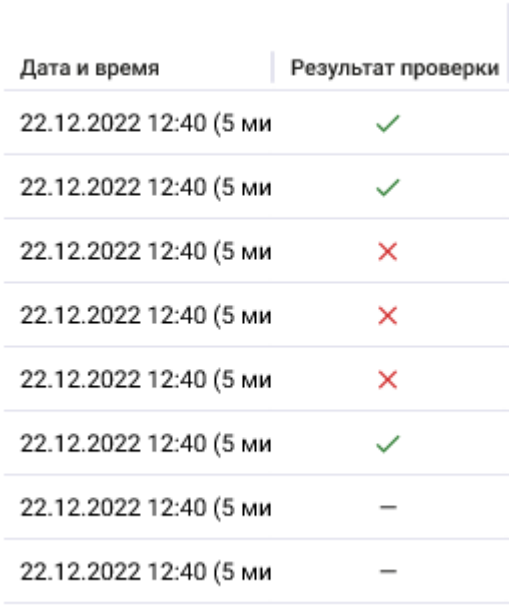
> **Предупреждение:** Соединения, которые были установлены до включения правил в таблице Логирование или не попали ранее под эти правила, не будут отображены в журнале.

> **Внимание:** Будьте внимательны: объем данных в **Журнале трафика** может кратно превысить объем данных любого другого журнала. Журнал хранит данные за три месяца, но при превышении размера журнала 15 ГБ старые записи будут удалены.
>
> При включении логирования убедитесь, что на Ideco NGFW достаточно свободного места.

Чтобы отрегулировать столбцы, отображаемые в таблице, воспользуйтесь кнопкой **Отображение**. Чтобы скачать CSV-файл с отчетом, нажмите на соответствующую кнопку.

В таблице отображается:

Общее



- **Дата и время** - дата и время срабатывания правила;
- **Результат проверки** - совокупный результат проверки трафика тремя модулями фильтрации: **Файрвол**, **IPS**, **DPI**.

Файрвол

Файрвол			
ID правила	Таблица правил	Действие правила	Протокол
17	Предправило/F	Разрешить	TCP
17	Input	Разрешить	TCP
52	Forward	Перенаправить в профиль	TCP
78	Forward	Перенаправить в профиль	TCP
77	Forward	Запретить	TCP
–	System/Fowrwai	Запретить	TCP
–	–	–	ICMP
–	–	–	ICMP

- **ID правила** - идентификатор правила **Файрвола** в таблице;
- **Таблица правил** - таблица **Файрвола**, правило котрой сработало (правила DNAT и SNAT отображаются в отдельных столбцах):
  - **FORWARD** - таблица FORWARD **Файрвола** Ideco NGFW;
  - **FORWARD BEFORE** - предправило FORWARD Ideco Center;
  - **FORWARD AFTER** - постправило FORWARD Ideco Center;
  - **FORWARD SYSTEM** - системное правило FORWARD;
  - **INPUT** - таблица INPUT **Файрвола** Ideco NGFW;
  - **INPUT BEFORE** - предправило INPUT Ideco Center;
  - **INPUT AFTER** - постправило INPUT Ideco Center;
  - **INPUT SYSTEM** - системное правило INPUT.
- **Действие правила** - действие, определенное для трафика, подпадающего под сработавшее правило. Возможные действия: Разрешить, Запретить, Перенаправить в профиль. Для правил DNAT и SNAT действие отсутствует;
- **Протокол** - протокол соединения.

Предотвращение вторжений

Предотвращение вторжений

Профиль	Действие	ID соединения	ID сигнатуры
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
Для сетевиков	Блокировать	15NPWWGAWPW4GMFAC2S	10085
Для сетевиков	Блокировать	15NPWWGAWPW4GMFAC2S	10085
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–
–	–	15NPWWGAWPW4GMFAC2S	–

- **Профиль** - название профиля **Предотвращения вторжений**, использованного в правиле **Файрвола**;
- **Действие** - действие для трафика, определенное профилем (*Разрешить*, *Запретить*, -);
- **ID соединения** - идентификатор соединения, трафик которого был обработан **Предотвращением вторжений**. Нажмите на значение, чтобы перейти к разделу **События безопасности ->** ***Журнал IPS*** ;
- **ID сигнатуры** - идентификатор сигнатуры, которой соответствует трафик.

Контроль приложений

Контроль приложений

Профиль	Действие	Приложение	Протокол прикладного уровня
–	–	–	–
–	–	–	–
Профиль 1	Блокировать	SSL	SSL
–	–	–	–
–	–	–	–
–	–	–	–
–	–	–	–
–	–	–	–

- **Профиль** - название профиля **Контроля приложений**, использованного в правиле **Файрвола**;
- **Действие** - действие для трафика, определенное профилем;
- **Приложение** - приложение, действие для которого определено профилем;

- **Протокол прикладного уровня** - протокол, к которому применяется действие, определенное профилем.

Источник

Источник

IP-адрес	Порт	Зона	Логин	Пользователь	Группа	Местоположение
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	Англия
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.1.50	50084	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.136	43612	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.136	43612	Любой	a.qwertyy	Имя Фамилия	Разработка	–

- **IP-адрес** - IP-адрес источника трафика;
- **Порт** - порт источника трафика;
- **Зона** - интерфейс или группа интерфейсов, из которых пришел трафик;
- **Логин** - логин пользователя источника;
- **Пользователь** - имя пользователя источника;
- **Группа** - группа, в которую входит пользователь;
- **Местоположение** - страна источника трафика (GeoIP).

Назначение

Назначение

IP-адрес	Порт	Зона	Логин	Пользователь	Группа	Местоположение
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	Англия
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
217.65.3.21	443	Любой	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.201	2222	–	a.qwertyy	Имя Фамилия	Разработка	–
192.168.122.201	2222	–	a.qwertyy	Имя Фамилия	Разработка	–

- **IP-адрес** - IP-адрес назначения трафика;
- **Порт** - порт назначения трафика;
- **Зона** интерфейс или группа интерфейсов, в которые вошел трафик;
- **Логин** - логин пользователя назначения;
- **Пользователь** - имя пользователя назначения;
- **Группа** - группа, в которую входит пользователь;
- **Местоположение** - страна назначения трафика (GeoIP).

DNAT/SNAT

DNAT			SNAT	
ID правила	Новый IP назначения	Новый порт назначения	ID правила	Новый IP источника
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
17	217.65.3.21	443	–	–
–	–	–	2	217.65.3.21

DNAT:

- **ID правила** - идентификатор сработавшего правила таблицы DNAT;
- **Новый IP назначения** - IP-адрес, на который **Файрвол** поменял **IP-адрес назначения**;
- **Новый порт назначения** - порт, на который **Файрвол** поменял **Порт назначения**.

SNAT:

- **ID правила** - идентификатор сработавшего правила таблицы SNAT;
- **Новый IP источника** - IP-адрес, на который **Файрвол** поменял **IP-адрес источника**.

Кластер/VCE

Кластер		VCE	
ID	Название	ID	Название
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1
–	–	656	вдом_1

Кластер:

- **ID** - идентификатор кластера (если он настроен на NGFW);

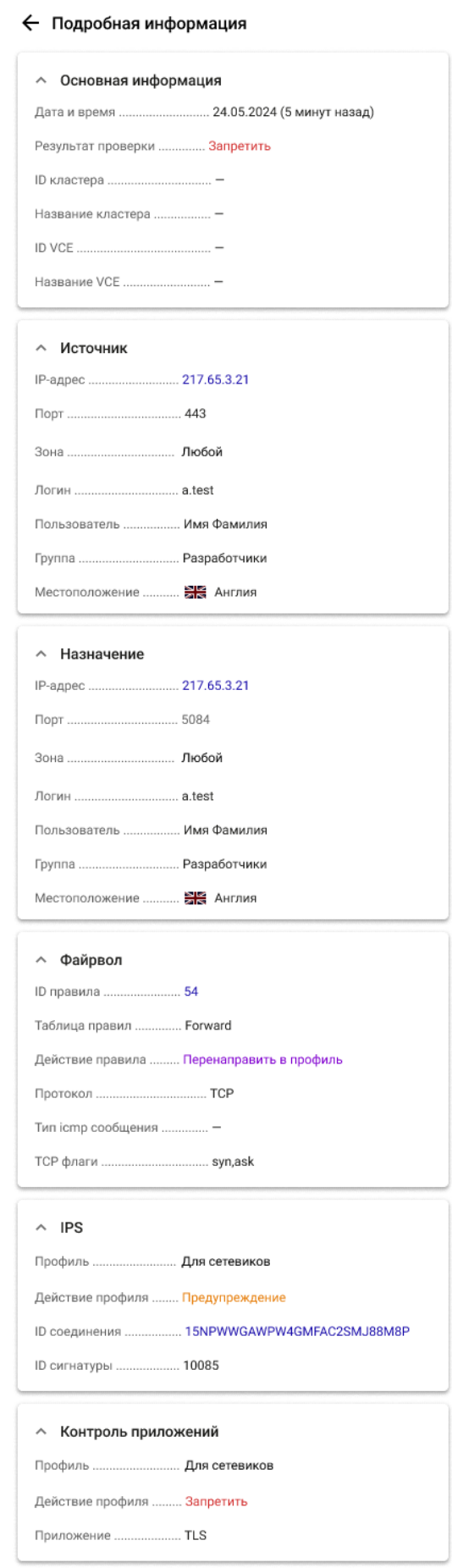
- **Название** - название кластера (если он настроен на NGFW).

VCE:

- **ID** - идентификатор *VCE*;
- **Название** - название VCE.

Чтобы перейти к сработавшему правилу **Файрвола**, нажмите на ID правила в таблице **Журнала трафика**. Чтобы увидеть подробную информацию о конкретном правиле, выделите строку таблицы и нажмите 

:

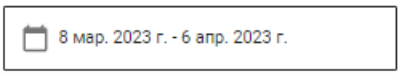

Подробная информация
Основная информация
Дата и время ..... 24.05.2024 (5 минут назад)
Результат проверки ..... Запретить
ID кластера ..... –
Название кластера ..... –
ID VCE ..... –
Название VCE ..... –
Источник
IP-адрес 217.65.3.21
Порт 443
Зона ..... Любой
Логин ..... a.test
Пользователь ..... Имя Фамилия
Группа ..... Разработчики
Местоположение ..... Англия
Назначение
IP-адрес 217.65.3.21
Порт 5084
Зона ..... Любой
Логин ..... a.test
Пользователь ..... Имя Фамилия
Группа ..... Разработчики
Местоположение ..... Англия
Файрвол
ID правила 54
Таблица правил ..... Forward
Действие правила ..... Перенаправить в профиль
Протокол ..... TCP
Тип icmp сообщения ..... –
TCP флаги ..... syn,ask
IPS
Профиль ..... Для сетевиков
Действие профиля ..... Предупреждение
ID соединения 15NPWWGAWPW4GMFAC2SMJ88M8P
ID сигнатуры 10085
Контроль приложений
Профиль ..... Для сетевиков
Действие профиля ..... Запретить
Приложение ..... TLS

19.5 События безопасности

Подсказка: Все графики формируются в часовом поясе сервера.

В разделе **События безопасности** представлены события модулей WAF и IPS, а также графики событий IPS.

19.5.1 Выбор периода

Все отображаемые данные фильтруются по дате и времени. Например, выберите определенный временной период (по кнопке 

) или воспользуйтесь одним из предустановленных фильтров:

Доступные варианты: сегодня, вчера, текущая неделя, прошлая неделя, текущий месяц, прошлый месяц.

Если не выбран ни один фильтр по дате и времени, то по умолчанию устанавливается интервал **Сегодня** в часовом поясе сервера.

19.5.2 Графики IPS

В этом разделе представлены графики, содержащие краткую информацию раздела **Предотвращение вторжений**. Подробные сведения обо всех срабатываниях правил **Предотвращение вторжений** можно найти на вкладке **Журнал IPS** в виде таблицы.

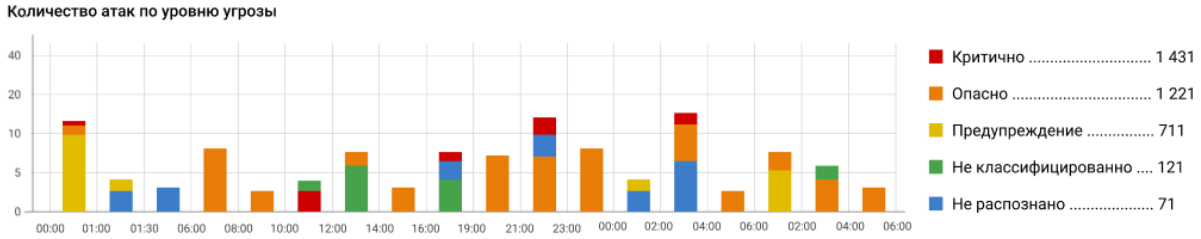
График Количество атак по уровню угрозы

Информация представлена в виде графика с пятью значениями угрозы безопасности:

- **Критично** - уровень угрозы 1;
- **Важно** - уровень угрозы 2;
- **Предупреждение** - уровень угрозы 3;
- **Не классифицировано** - уровень угрозы 4;
- **Не распознано** - уровень угрозы 255.

Если нажать на уровень угрозы в правом списке, все графики будут отфильтрованы в соответствии с этим уровнем. Чтобы отменить фильтрацию, нажмите еще раз на выбранный уровень.

Пример графика *Количество атак по уровню угрозы*:



Описание дополнительных графиков

Топ атакованных адресов:

В топ атакованных попадают как внешние, так и внутренние адреса. Один из примеров, когда атакованный адрес является внешним, - работа трояна изнутри защищаемой сети.

Топ заблокированных типов атак:

График подсчитывает статистику типов атак (например, типы атак *Черный список IP-адресов* или *Попытки получения привилегий администратора*) по количеству срабатываний с этим типом атаки.

Топ внешних узлов по количеству блокировок:

График содержит информацию о внешних адресах и количестве блокировок по ним.

Топ атакующих стран:

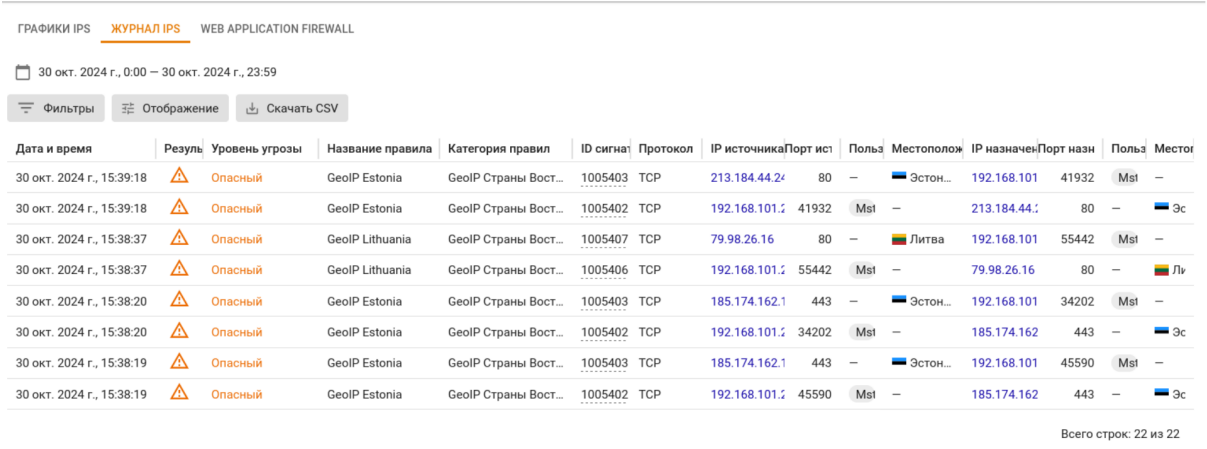
Топ атакующих стран строится по IP-адресам, полученным при срабатывании правил в разделе **Предотвращение вторжений**. Если IP-адрес не геокодируется в наименование страны, такой адрес не отображается в виджете.
По этой причине локальные IP-адреса не отображаются в виджете.

Топ подозрительных локальных узлов:

В топ попадают как авторизованные, так и не авторизованные пользователи, запросы которых блокировались.

19.5.3 Журнал IPS

В разделе **Отчеты и журналы -> События безопасности -> Журнал IPS** можно просмотреть логи системы **Предотвращения вторжений**:



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

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

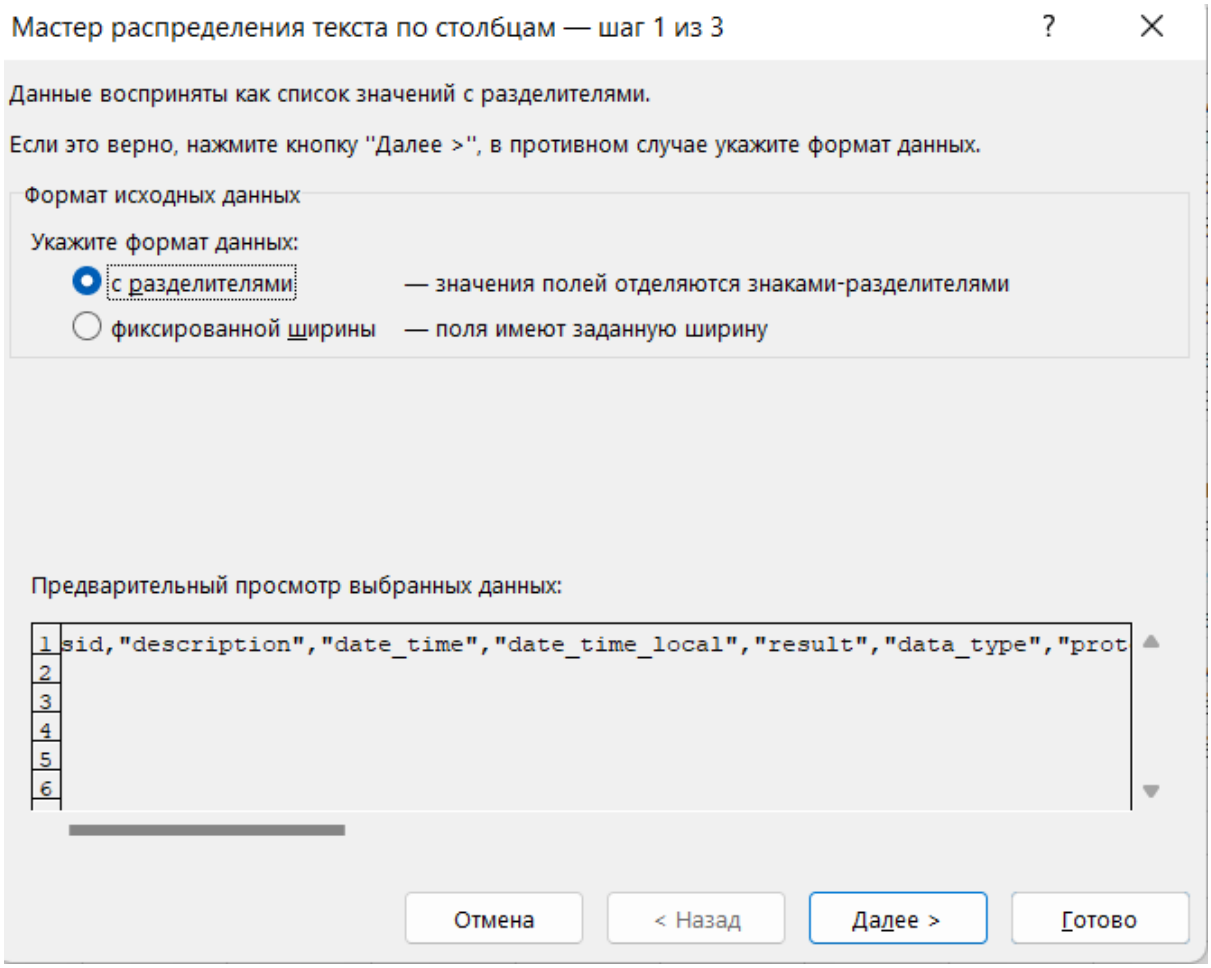
Для корректного отображения информации из CSV-файла выполните действия::

1. Скачайте CSV-файл с логами системы **Предотвращения вторжений** за определенный период по соответствующей кнопке.

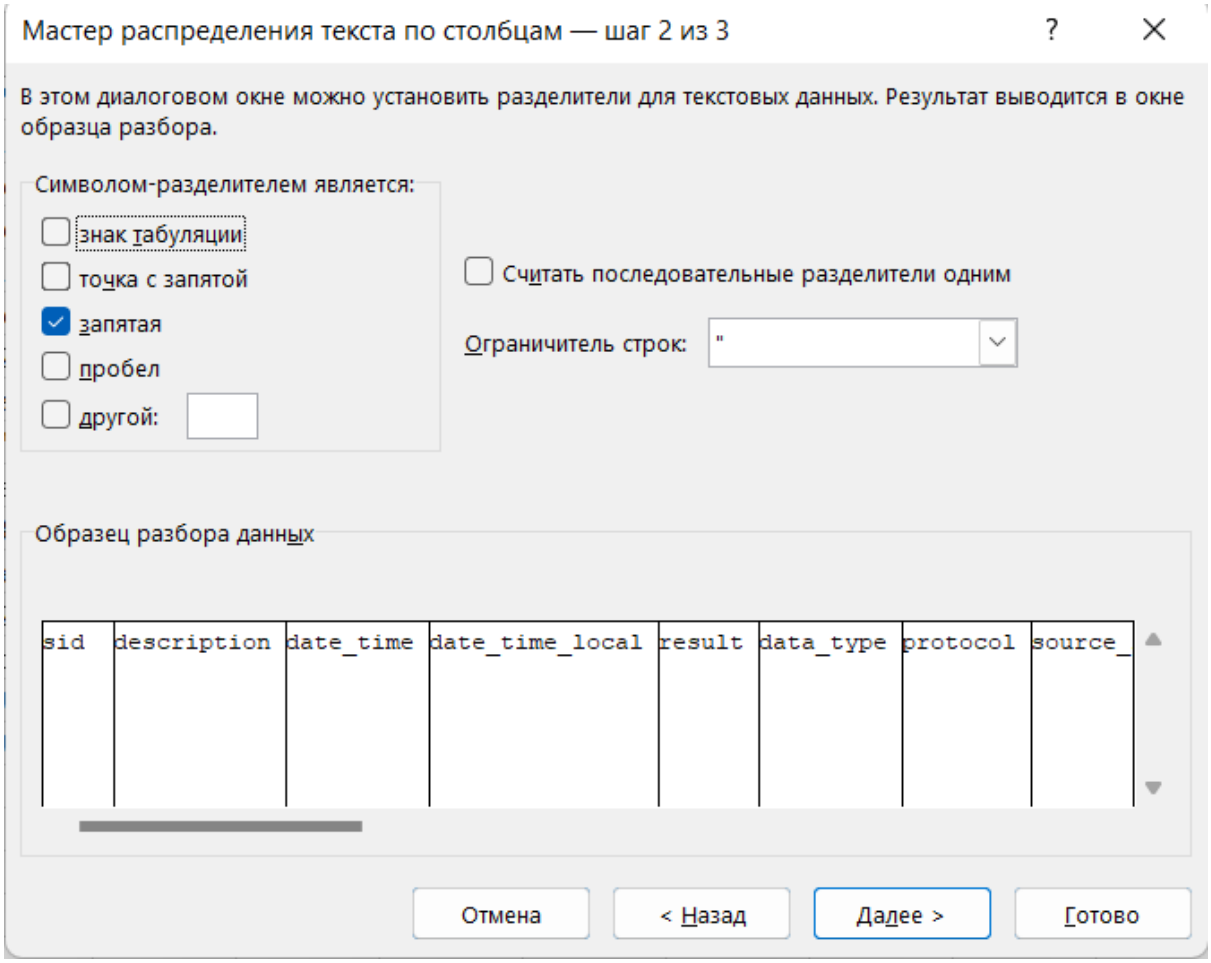
2. Откройте CSV-файл в MS Excel и выделите весь первый столбец.

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

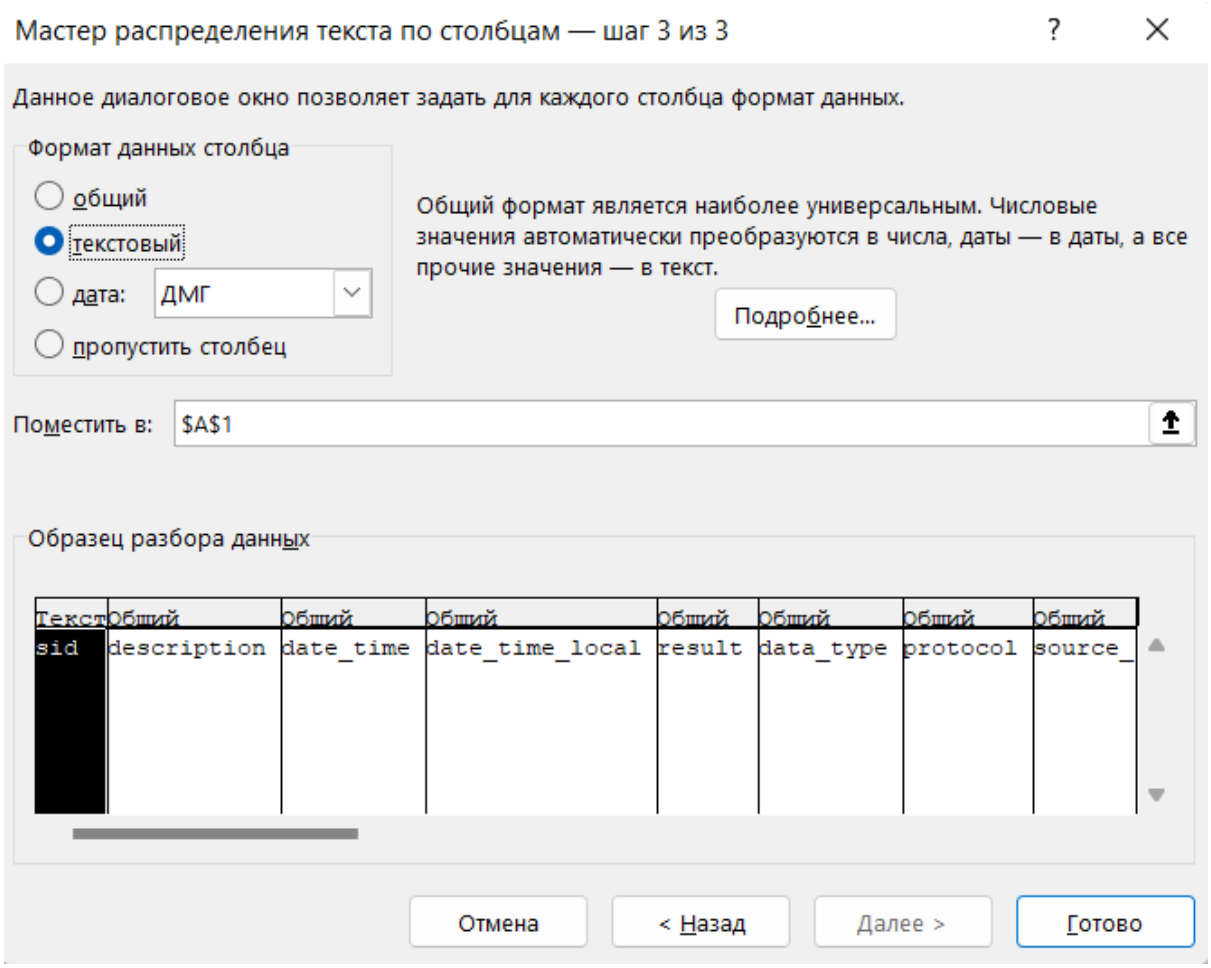
4. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:



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

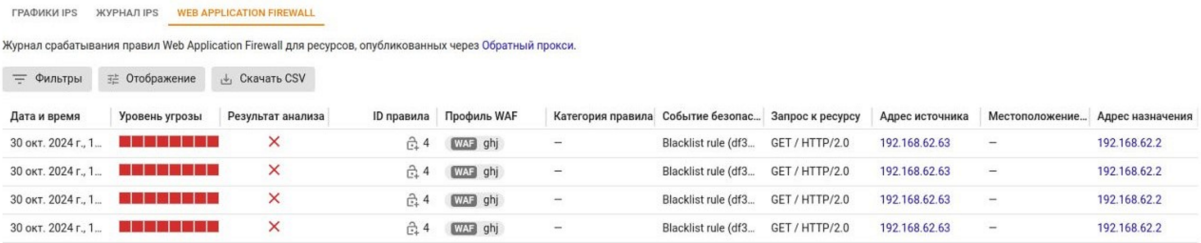


6. В блоке **Формат данных столбца** выберите **Текстовый** и нажмите **Готово**:



19.5.4 Web Application Firewall

Раздел **Отчеты и журналы -> События безопасности -> Web Application Firewall** содержит информацию о срабатывании правил Web Application Firewall в виде таблицы:



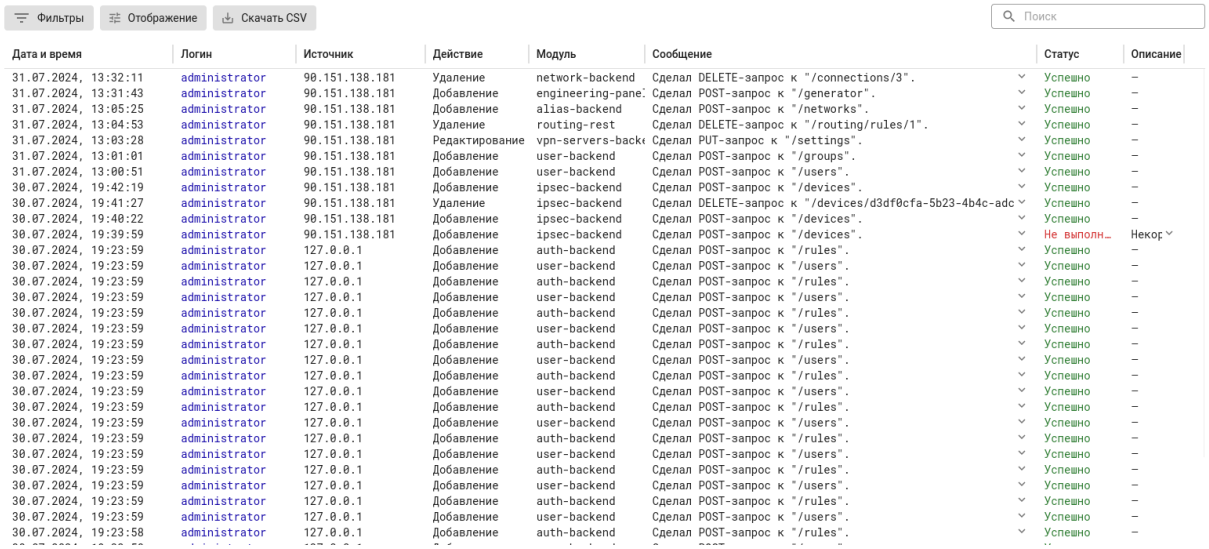
IP-адреса в столбцах **Адрес источника** и **Адрес назначения** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.

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

19.6 Действия администраторов

19.6.1 Основное

Ideco NGFW логирует действия администраторов, которые вносят изменения в конфигурацию NGFW из веб-интерфейса, локального интерфейса и терминала. Действия, осуществляемые через локальное меню NGFW, отображаются в журнале действий администраторов с источником 127.0.0.1:



Дата и время	Логин	Источник	Действие	Модуль	Сообщение	Статус	Описание
31.07.2024, 13:32:11	administrator	90.151.138.181	Удаление	network-backend	Сделал DELETE-запрос к "/connections/3".	Успешно	–
31.07.2024, 13:31:43	administrator	90.151.138.181	Добавление	engineering-pane	Сделал POST-запрос к "/generator".	Успешно	–
31.07.2024, 13:05:25	administrator	90.151.138.181	Добавление	alias-backend	Сделал POST-запрос к "/networks".	Успешно	–
31.07.2024, 13:04:53	administrator	90.151.138.181	Удаление	routing-rest	Сделал DELETE-запрос к "/routing/rules/1".	Успешно	–
31.07.2024, 13:03:28	administrator	90.151.138.181	Редактирование	vpn-servers-backe	Сделал PUT-запрос к "/settings".	Успешно	–
31.07.2024, 13:01:01	administrator	90.151.138.181	Добавление	user-backend	Сделал POST-запрос к "/groups".	Успешно	–
31.07.2024, 13:00:51	administrator	90.151.138.181	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:42:19	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Успешно	–
30.07.2024, 19:41:27	administrator	90.151.138.181	Удаление	ipsec-backend	Сделал DELETE-запрос к "/devices/d3df0cfa-5b23-4b4c-adc	Успешно	–
30.07.2024, 19:40:22	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Успешно	–
30.07.2024, 19:39:59	administrator	90.151.138.181	Добавление	ipsec-backend	Сделал POST-запрос к "/devices".	Не выполн…	Некор
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–
30.07.2024, 19:23:59	administrator	127.0.0.1	Добавление	user-backend	Сделал POST-запрос к "/users".	Успешно	–
30.07.2024, 19:23:58	administrator	127.0.0.1	Добавление	auth-backend	Сделал POST-запрос к "/rules".	Успешно	–

Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

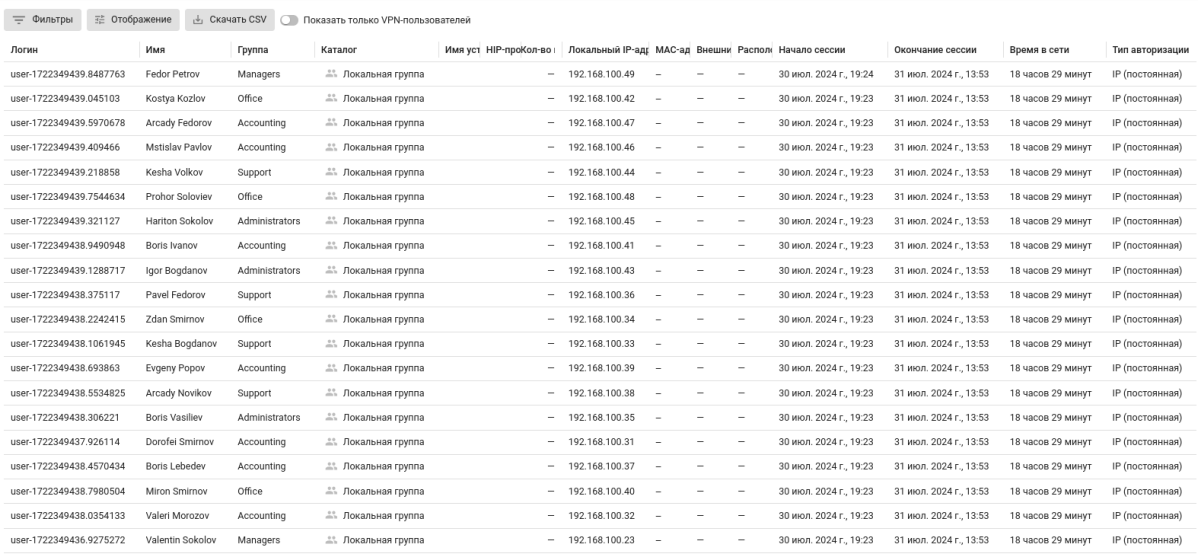
При работе Ideco NGFW в режиме *кластера* логи действия администраторов не передаются резервной ноде.

Подсказка: При бездействии в течение 15 минут администратор будет автоматически разавторизован.

19.7 Журнал аутентификации

19.7.1 Основное

Подсказка: Время хранения данных в **Журнале аутентификации** составляет 180 дней.



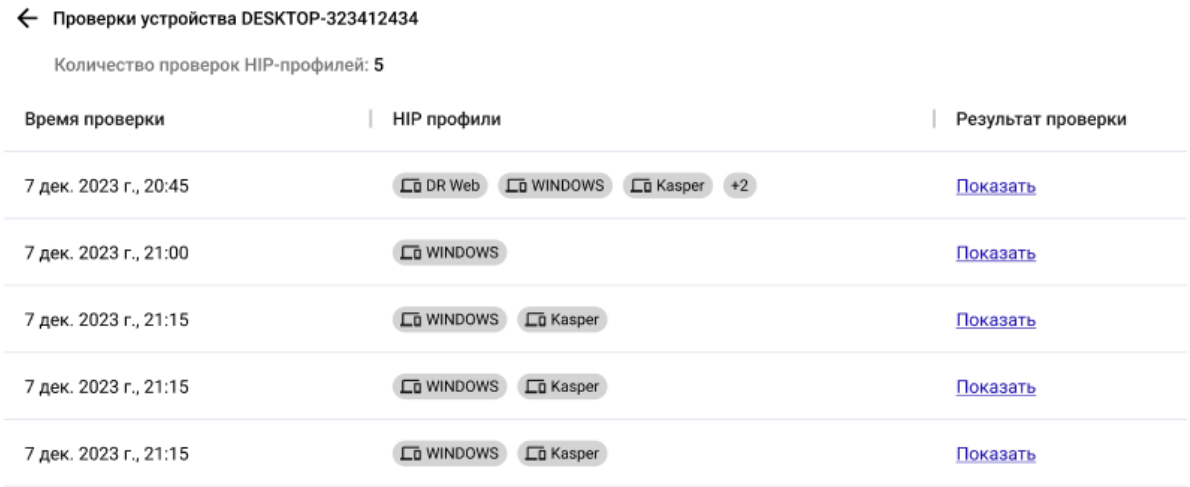
Логин	Имя	Группа	Каталог	Имя уст	HIP-про	Кол-во	Локальный IP-адр	MAC-ад	Внешни	Распол	Начало сессии	Окончание сессии	Время в сети	Тип авторизации
user-1722349439.8487763	Fedor Petrov	Managers	Локальная группа			–	192.168.100.49	–	–	–	30 июл. 2024 г., 19:24	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.045103	Kostya Kozlov	Office	Локальная группа			–	192.168.100.42	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.5970678	Arcady Fedorov	Accounting	Локальная группа			–	192.168.100.47	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.409466	Mstislav Pavlov	Accounting	Локальная группа			–	192.168.100.46	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.218858	Kesha Volkov	Support	Локальная группа			–	192.168.100.44	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.7544634	Prohor Soloviev	Office	Локальная группа			–	192.168.100.48	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.321127	Hariton Sokolov	Administrators	Локальная группа			–	192.168.100.45	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.9490948	Boris Ivanov	Accounting	Локальная группа			–	192.168.100.41	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349439.1288717	Igor Bogdanov	Administrators	Локальная группа			–	192.168.100.43	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.375117	Pavel Fedorov	Support	Локальная группа			–	192.168.100.36	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.2242415	Zdan Smirnov	Office	Локальная группа			–	192.168.100.34	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.1061945	Kesha Bogdanov	Support	Локальная группа			–	192.168.100.33	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.693863	Evgeny Popov	Accounting	Локальная группа			–	192.168.100.39	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.5534825	Arcady Novikov	Support	Локальная группа			–	192.168.100.38	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.306221	Boris Vasiliev	Administrators	Локальная группа			–	192.168.100.35	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349437.926114	Dorofei Smirnov	Accounting	Локальная группа			–	192.168.100.31	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.4570434	Boris Lebedev	Accounting	Локальная группа			–	192.168.100.37	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.7980504	Miron Smirnov	Office	Локальная группа			–	192.168.100.40	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349438.0354133	Valeri Morozov	Accounting	Локальная группа			–	192.168.100.32	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)
user-1722349436.9275272	Valentin Sokolov	Managers	Локальная группа			–	192.168.100.23	–	–	–	30 июл. 2024 г., 19:23	31 июл. 2024 г., 13:53	18 часов 29 минут	IP (постоянная)

Для поиска авторизованных пользователей нажмите на **Фильтры**, укажите в поле **Столбец** требуемый параметр поиска и в последнем поле - его значение.

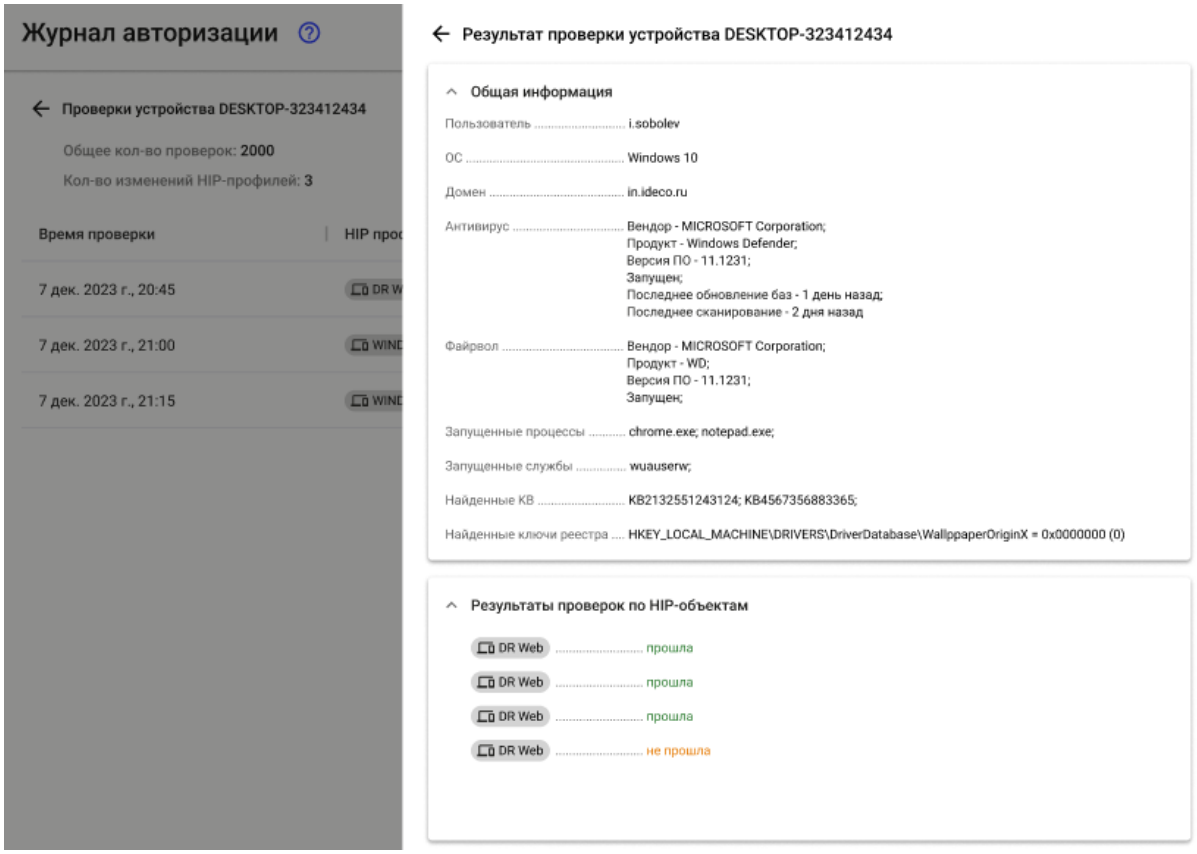
В столбце **Кол-во изменений профилей** указано количество изменений HIP-профилей, зафиксированных в результате проверок устройств, подключенных через Ideco Client. Изменения фиксируются при редактировании HIP-профиля в веб-интерфейсе или изменении соответствия устройств настроенным профилям.

Для просмотра результатов проверок устройств, подключенных через Ideco Client, выполните действия:

1. Кликните на число в столбце **Кол-во изменений профилей**. Откроется список проверок:



2. Кликните **Показать** в столбце **Результат**, чтобы увидеть общую информацию и результат проверки по *HIP-объектам*:



Особенности работы Журнала аутентификации:

- Время окончания открытой сессии пользователя меняется каждые 5 минут, поскольку происходит запись текущего времени в поле **Окончание сессии**. Если запрос на поиск будет отправлен до момента синхронизации буфера, то время окончания будет одно, в ином случае - другое.
- Для завершенной сессии информация о времени закрытия не меняется.

Включение опции **Показать VPN-пользователей** отфильтрует в таблице журнала информацию обо всех VPN-сессиях по всем протоколам.

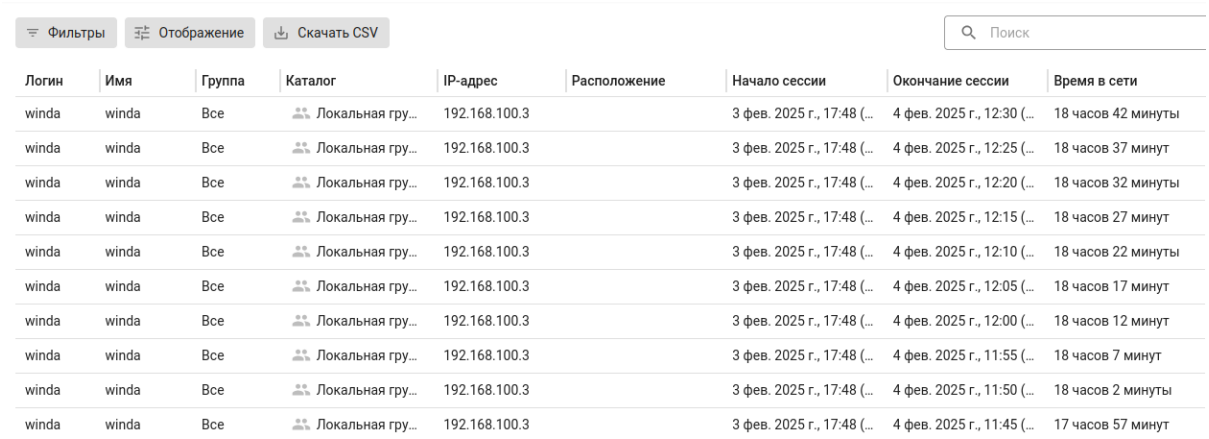
19.8 Журнал авторизации ЛК

19.8.1 Основное

Журнал аутентификации ЛК представляет собой историю сессий пользователей, авторизованных в личном кабинете пользователя Ideco NGFW.

Записи в журнале отображаются после настройки *Обратного прокси* и сработки правил в разделе **Сервисы -> *ЛК/Портале SSL VPN***. Технология SSL VPN используется пользователями для получения доступа к ресурсам в локальной сети через веб-браузер по HTTPS. При этом не устанавливается отдельное туннельное соединение.

Таблицу сессий можно скачать в формате CSV, воспользовавшись соответствующей кнопкой:



Помимо общих сведений об учетной записи пользователя (логин, имя, группа и каталог), список сессий включает столбцы:

- **IP-адрес** - IP-адрес, с которого произведена аутентификация;
- **Расположение** - страна IP-адреса, с которого произведена аутентификация. Значение пустое, если:
  - Отсутствует лицензия;
  - Невозможно получить базу GeoIP;
  - IP-адрес локальный.
- **Начало сессии** - момент запуска сессии с указанием даты в формате день/месяц/год и времени в формате час/минута;
- **Окончание сессии** - момент завершения сессии с указанием даты в формате день/месяц/год и времени в формате час/минута. Пустое значение, если сессия активна;
- **Время в сети** - продолжительность сессии с момента запуска.

Наличие столбцов в таблице регулируется кнопкой **Отображение**. По каждому столбцу доступна фильтрация и сортировка.

Для поиска нужной сессии воспользуйтесь одним из способов:

- Нажмите кнопку **Фильтры**, установите параметр поиска (все наименования доступных столбцов) и его значение;
- Введите ключевое слово в поле **Поиск** в правом верхнем углу.

19.9 Конструктор отчетов

NGFW предоставляет возможность создать шаблоны отчетов и настроить их рассылку в форматах .pdf и/или .csv на электронную почту.

19.9.1 Мои шаблоны

На этой вкладке создаются шаблоны со статистикой, которую можно просмотреть в браузере, сохранить или отправить на электронную почту.

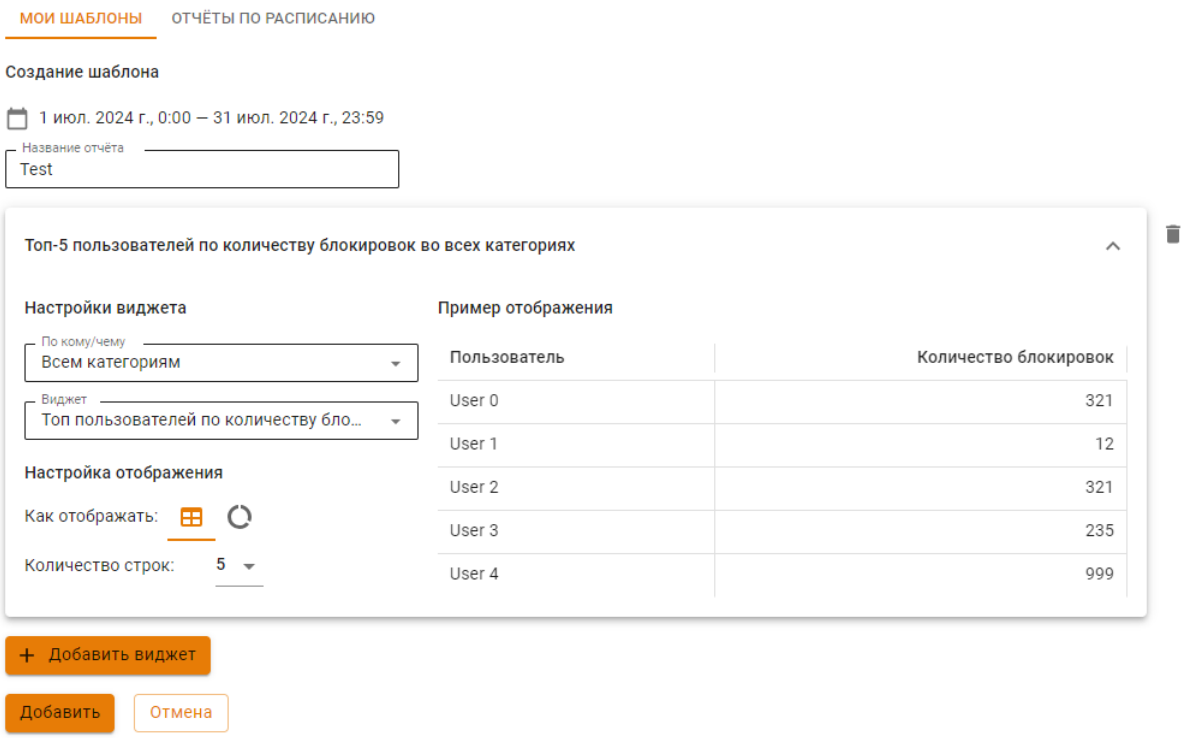
При нажатии на кнопку **Добавить** откроется меню настройки шаблона.

Задайте временной промежуток, название отчета и нажмите **Добавить виджет**. Один шаблон может содержать несколько виджетов.

Настройка виджетов:

- В строке **По кому/чему** выберите объект, по которому будет собираться статистика. Если выбираете **Определенный** объект (например, *Определенный пользователь* или *Определенная группа*), то появится дополнительная строка **Объекты**, где можно выбрать несколько объектов;
- В строке **Виджет** укажите, какую информацию хотите видеть по выбранному объекту;
- Задайте **Настройки отображения**.

После окончания настройки шаблона нажмите **Добавить**.



Подсказка: Будьте внимательны при задании временного промежутка для шаблона отчетов. Ideco NGFW хранит данные в течение определенного времени (TTL), по прошествии которого они безвозвратно удаляются и не могут быть включены в отчеты:

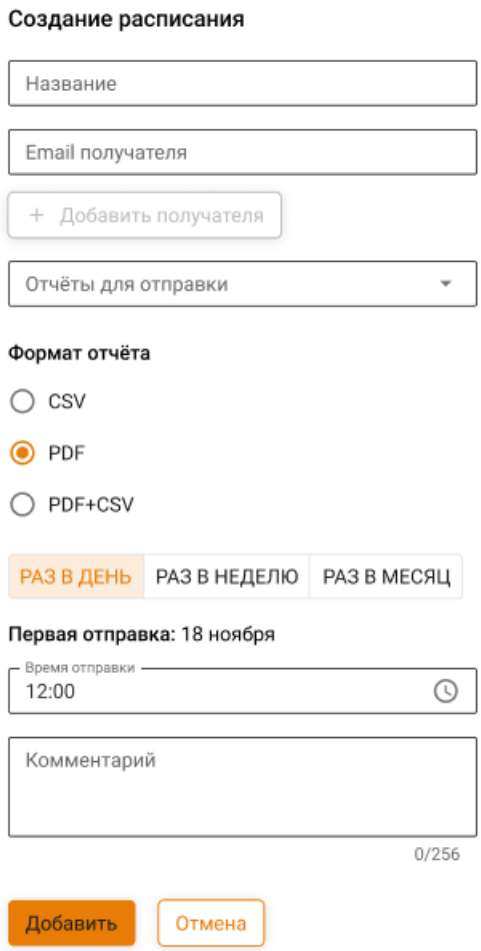
Сроки хранения данных по разделам:

- *Системный журнал* (кроме логов служб `strongswan`, `squid`, `ideco-app-control`, `fail2ban`) - 90 дней;
- Логи *служб* `strongswan`, `squid`, `ideco-app-control`, `fail2ban` (Системный журнал) - 14 дней;
- Данные веб-трафика (Журнал веб-трафика, а также посещенные сайты) - 1 месяц;
- События безопасности (Журнал IPS и Web application firewall) - 3 месяца;
- Действия администраторов и Авторизация администраторов - 1 год;
- Журнал аутентификации - 180 дней.

19.9.2 Отчеты по расписанию

На этой вкладке предоставлена возможность создания/редактирования настроек для отправки рассылки на электронную почту, доступна фильтрация по всем столбцам с помощью кнопки **Фильтры**.

Для создания настройки нажмите **Отчеты по расписанию -> Добавить** в левом верхнем углу. В одной настройке можно указать несколько e-mail-получателей (кнопка **Добавить получателя**) и несколько отчетов (поле **Отчеты для отправки**):



Допустимые форматы отчетов: CSV, PDF и PDF+CSV. Генерация отчетов в PDF требует значительных ресурсов ЦПУ и ОЗУ.

Отчеты будут отправляться:

- **Раз в день** - отправка произойдет на следующий день после сохранения, если время отправки меньше текущего на сервере;
- **Раз в неделю** - укажите день и время отправки;
- **Раз в месяц** - укажите определенный по счету день и время или каждое 1-е число месяца. Если выбрано 31-е число, но в месяце меньше дней, то выбирается последнее число месяца.

После нажатия на кнопку **Добавить** NGFW сохранит все пользовательские настройки времени отправки во всех фильтрах (раз в день, раз в неделю и раз в месяц), но отправляться шаблон будет только в период, выбранный пользователем.
Например:

1. Задайте временной период:

- Раз в неделю;
- День недели - четверг;

- Нажмите **Добавить**.

2. Перейдите к редактированию отчета по кнопке **Редактировать** и измените настройки временного периода:

- Раз в месяц;
- Каждую вторую среду;
- Нажмите **Сохранить**.

3. Перейдите к редактированию отчета и выберите **Раз в месяц**. Откроются настройки, созданные в пункте 1.

Пример настройки ежемесячного отчета в формате CSV:

Пример. Требуется настроить отправку отчета в формате CSV с информацией о заблокированных сайтах по всем пользователям. Периодичность - ежемесячно, каждое первое число месяца.

Создайте шаблон отчета, на основании которого будет собрана статистика для отправки:

1. Нажмите **Добавить** на вкладке **Мои шаблоны**.

2. Выберите временной период, за который следует сформировать отчет, из предложенных фильтров или укажите даты нажав **Выберите дату**.

3. Укажите название отчета (строка *Название отчета*).

4. Кликните по кнопке **Добавить виджет**.

5. Заполните строки:

- **По кому/чему** - выберите **Всем пользователям**;
- **Виджет** - выберите **Топ заблокированных сайтов**;

6. Укажите **Настройки отображения**:

7. Сохраните шаблон по кнопке **Добавить**.

Создайте правило, по которому шаблон отчета будет отправляться на электронную почту:

1. Нажмите **Добавить** на вкладке **Отчеты по расписанию**.

2. Заполните строки:

- **Название** - любое название, которое поможет идентифицировать правило расписания;
- **Email получателя** - электронная почта получателя отчета. Если нужно отправлять отчет нескольким получателям, укажите дополнительные адреса по кнопке **Добавить получателя**.

3. Выберите нужный шаблон в поле **Отчеты для отправки**.

4. Выберите формат отчета (CSV).

5. Укажите настройки даты/дня и времени отправки отчета получателю (раз в месяц, каждый 1-й день месяца).

19.10 Syslog

Подсказка: Название службы раздела **Syslog**: `ideco-logs-backend`.

Список служб для других разделов доступен по *ссылке*.

19.10.1 Пересылка системных сообщений

Чтобы настроить пересылку системных сообщений, перейдите в раздел **Отчеты и журналы -> Syslog** и выполните действия:

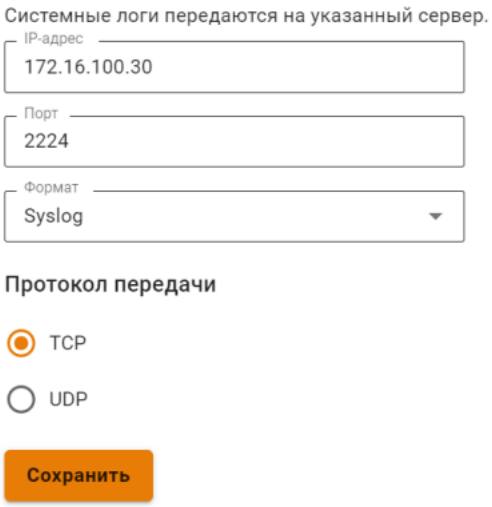
1. Укажите IP-адрес сервера-коллектора (любой локальный или публичный IP-адрес).

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

3. Выберите формат передаваемых системных сообщений (Syslog или CEF).

4. Выберите протокол передачи системных логов - TCP или UDP.

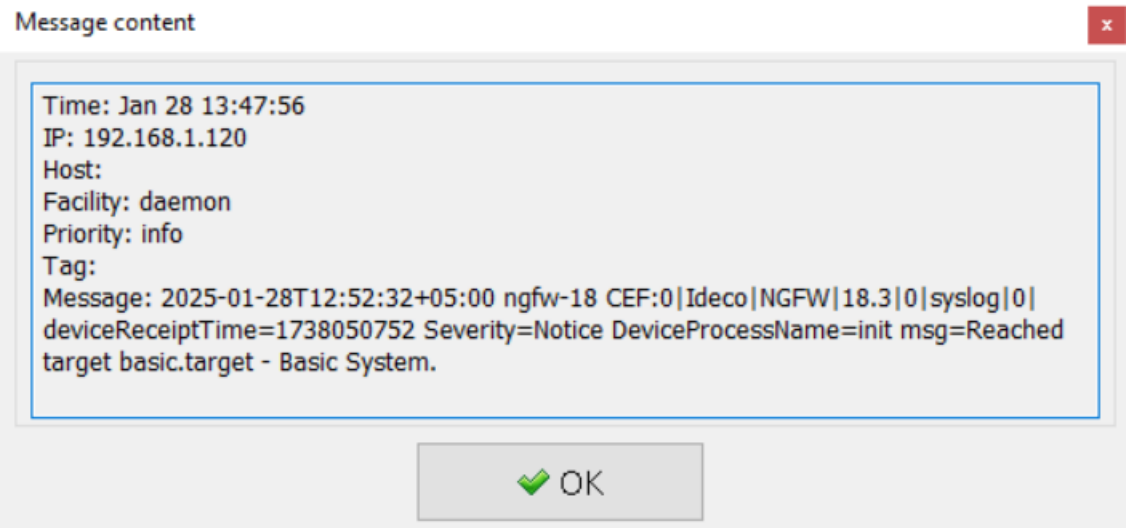
5. Нажмите **Сохранить** и включите опцию Syslog:



Подсказка: Рекомендуется передавать логи по протоколу TCP, так как он гарантирует доставку и соблюдает последовательность сообщений.

19.10.2 Расшифровка передаваемых логов

В статье представлены примеры сообщений (message) в форматах CEF и Syslog (скриншот из Visual Syslog server):



Формат CEF

Message в CEF-формате начинается со строки вида:

```
2024-11-18T15:38:54+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.0|0|syslog|0|
```

где:

- `2024-11-18T15:38:54+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `CEF:0` - версия формата CEF;
- `Ideco` - вендор;
- `NGFW` - название продукта;
- `18.0` - версия продукта;
- `0|syslog|0` - идентификатор лога, постоянный для NGFW. Состоит из трех полей: идентификатор типа события, описание события, важность события.

Предотвращение вторжений:

```
2024-11-18T15:38:54+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731926334 Severity=Warning DeviceProcessName=web-
↪proxy DeviceCustomString1=1881087344384816 DeviceInboundInterface=␣
↪DeviceProcessName=ideco-ips DeviceCustomString5=alert SourceAddress=192.168.101.25␣
↪DeviceCustomString1=local DeviceCustomString1Label=Src IP Type SourcePort=55644␣
↪SourceCountry= DeviceCustomString2= DeviceCustomString2Label=Src Country Code␣
↪DeviceCustomString3=34fbd7c6-716b-4858-bb68-313729b1cad4␣
↪DeviceCustomString3Label=Src session UUID SourceUserID=9 SourceUserName=user␣
↪DestinationAddress=212.70.163.70 DeviceCustomString4=external␣
↪DeviceCustomString4Label=Dst IP Type DestinationPort=443 DestinationCountry=Латвия␣
↪DeviceCustomString5=LV DeviceCustomString5Label=Dst Country Code␣
↪DeviceCustomString6= DeviceCustomString6Label=Dst session UUID DestinationUserID=-1␣
↪DestinationUserName= TransportProtocol=TCP DeviceEventClassID=1005404 Message=GeoIP␣
↪Latvia DeviceEventCategory=GeoIP Страны Восточной Европы Severity=2␣
↪DeviceCustomString8=1 DeviceCustomString8Label=Alert GID␣
↪DeviceCustomString9=blocked DeviceCustomString9Label=Alert action␣
↪DestinationHostName= RequestUrl= RequestClientApplication= FlexNumber1=1␣
↪FlexNumber1Label=Flow packets to server FlexNumber2=0 FlexNumber2Label=Flow packets␣
↪to client BytesIn=60 BytesOut=0 StartTime=2024-11-18 10:38:54.110294 EndTime=2024-
↪11-18 10:38:54.110969 FlexNumber3=0 FlexNumber3Label=flow DeviceCustomString11=␣
↪DeviceCustomString11Label=flow.state DeviceCustomString12=␣
↪DeviceCustomString12Label=flow.reason FlexNumber4=0 FlexNumber4Label=flow.alerted␣
↪DeviceCustomString14= DeviceCustomString14Label=tcp.tcp_flags DeviceCustomString15=␣
↪DeviceCustomString15Label=tcp.tcp_flags_ts DeviceCustomString16=␣
↪DeviceCustomString16Label=tcp.tcp_flags_tc FlexNumber5=0 FlexNumber5Label=tcp.cwr␣
↪FlexNumber6=0 FlexNumber6Label=tcp.ecn FlexNumber7=0 FlexNumber7Label=tcp.urg␣
↪FlexNumber8=0 FlexNumber8Label=tcp.ack FlexNumber9=0 FlexNumber9Label=tcp.psh␣
↪FlexNumber10=0 FlexNumber10Label=tcp.rst FlexNumber11=0 FlexNumber11Label=tcp.syn␣
↪FlexNumber12=0 FlexNumber12Label=tcp.fin DeviceCustomString17=␣
↪DeviceCustomString17Label=tcp.state
```

где:

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;

- `DeviceCustomString1=1881087344384816` - внутренний идентификатор системы предотвращения вторжений flow (сессии);
- `DeviceInboundInterface` - идентификатор входящего интерфейса;
- `DeviceProcessName=ideco-ips` - имя экземпляра системы предотвращения вторжений;
- `DeviceCustomString5=alert` - тип события;
- `SourceAddress=192.168.101.25` - IP-адрес источника;
- `DeviceCustomString1=local DeviceCustomString1Label=Src IP Type` - тип IP-адреса источника (`local` - локальный, `external` - внешний);
- `SourcePort=55644` - порт источника;
- `SourceCountry` - название местоположения источника;
- `DeviceCustomString2= DeviceCustomString2Label=Src Country Code` - ISO-код страны источника;
- `DeviceCustomString3=34fbd7c6-716b-4858-bb68-313729b1cad4 DeviceCustomString3Label=Src session UUID` - внутренний идентификатор сессии Ideco NGFW источника;
- `SourceUserID=9` - идентификатор пользователя источника;
- `SourceUserName=user` - имя пользователя источника;
- `DestinationAddress=212.70.163.70` - IP-адрес назначения;
- `DeviceCustomString4=external DeviceCustomString4Label=Dst IP Type` - тип IP-адреса назначения (`local` - локальный, `external` - внешний);
- `DestinationPort=443` - порт назначения;
- `DestinationCountry=Латвия` - название местоположения назначения;
- `DeviceCustomString5=LV DeviceCustomString5Label=Dst Country Code` - ISO-код страны назначения;
- `DeviceCustomString6= DeviceCustomString6Label=Dst session UUID` - внутренний идентификатор сессии Ideco NGFW назначения;
- `DestinationUserID=-1` - идентификатор пользователя назначения;
- `DestinationUserName` - имя пользователя назначения;
- `TransportProtocol=TCP` - протокол;
- `DeviceEventClassID=1005404` - ID правила системы предотвращения вторжений;
- `Message=GeoIP Latvia` - сообщение из сработавшего правила;
- `DeviceEventCategory=GeoIP Страны Восточной Европы` - описание колонки в веб-интерфейсе События безопасности;
  Соответствие *alert.category: -> alert.signature* описаны в файле;
- `Severity=2` - уровень угрозы, может принимать значения 1, 2, 3 и 256, где 1 - самый высокий уровень угрозы;
- `DeviceCustomString8=1 DeviceCustomString8Label=Alert GID` - GID угрозы;
- `DeviceCustomString9=blocked DeviceCustomString9Label=Alert action` - действие по отношению к угрозе (блокировать).

Служебные поля результата анализа HTTP-трафика. Заполняются, если в процессе анализа трафика был определен HTTP-протокол:

- `DestinationHostName` - идентификатор хоста;
- `RequestUrl` - URL, на который велось обращение;
- `RequestClientApplication=` - информация, идентифицирующая HTTP-клиента.

Служебные поля flow (сессии):

- `FlexNumber1=1 FlexNumber1Label=Flow packets to server` - количество пакетов, переданное от клиента к серверу;
- `FlexNumber2=0 FlexNumber2Label=Flow packets to client` - количество пакетов, переданное от сервера к клиенту;
- `BytesIn=60` - количество байт, переданное от клиента к серверу;
- `BytesOut=0` - количество байт, переданное от сервера к клиенту;
- `StartTime=2024-11-18 10:38:54.110294` - начало;
- `EndTime=2024-11-18 10:38:54.110969` - окончание;
- `FlexNumber3=0 FlexNumber3Label=flow` - возраст;
- `DeviceCustomString11= DeviceCustomString11Label=flow.state` - текущее состояние;
- `DeviceCustomString12= DeviceCustomString12Label=flow.reason` - запущен ли IPsec в режиме отладки;
- `FlexNumber4=0 FlexNumber4Label=flow.alerted` - сгенерировался ли поток alert.

Состояние флага TCP flow (сессии):

- `DeviceCustomString14= DeviceCustomString14Label=tcp.tcp_flags` - значение поля flags в заголовке TCP;
- `DeviceCustomString15= DeviceCustomString15Label=tcp.tcp_flags_ts` - timestamp флаги;
- `DeviceCustomString16= DeviceCustomString16Label=tcp.tcp_flags_tc` - флаг Truncated response;
- `FlexNumber5=0 FlexNumber5Label=tcp.cwr` - флаг TCP-пакета, информирующий отправителя, что получен пакет с установленным флагом ECE (Подробнее в RFC-3186);
- `FlexNumber6=0 FlexNumber6Label=tcp.ecn` - флаг TCP-пакета, информирующий получателя, что узел способен на явное уведомление о перегрузке сети;
- `FlexNumber7=0 FlexNumber7Label=tcp.urg` - флаг TCP-пакета, указывающий важность пакета;
- `FlexNumber8=0 FlexNumber8Label=tcp.ack` - флаг TCP-пакета, указывающий, что пакет получен;
- `FlexNumber9=0 FlexNumber9Label=tcp.psh` - флаг TCP-пакета, информирующий получателя, что все данные переданы и можно передать их приложению;
- `FlexNumber10=0 FlexNumber10Label=tcp.rst` - флаг TCP-пакета, указывающий, что соединение завершено в аварийном режиме;
- `FlexNumber11=0 FlexNumber11Label=tcp.syn` - флаг TCP-пакета, отвечающий за установку соединения;
- `FlexNumber12=0 FlexNumber12Label=tcp.fin` - флаг TCP-пакета, указывающий на завершение соединения в штатном порядке;
- `DeviceCustomString17= DeviceCustomString17Label=tcp.state` - состояния сеанса TCP.

Файрвол:

Логирование включается в разделе **Правила трафика -> Файрвол -> Логирование**. Включите опцию **Логировать срабатывания правил**.

```
2025-01-27T13:28:14+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪3|0|syslog|0|deviceReceiptTime=1737966494 Severity=Warning DeviceProcessName=ideco-
↪nflog msg=TCP src 192.168.101.25 sport 41528 dst 74.125.131.105 dport 443 table FWD␣
↪rule 2 action drop
```

где:

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `TCP` - протокол. Это поле принимает значения: UDP, TCP, ICMP, GRE, ESP и AH;
- `src` - IP-адрес источника;
- `sport` - порт источника для UDP и TCP;
- `dst` - IP-адрес назначения;
- `dport` - порт назначения для UDP и TCP;
- `table` - таблица правил, в которой произошло логирование;
- `rule` - ID правила из таблицы;
- `action` - действие, которое произошло.

Контроль приложений:

```
2024-12-02T20:40:13+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪2|0|syslog|0|deviceReceiptTime=1733154013 Severity=Notice DeviceProcessName=ideco-
↪app-stats msg=192.168.101.25:37030 -> 192.168.101.10:53 [eBay] \= DROP
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `192.168.101.25:37030` - IP-адрес и порт источника;
- `192.168.101.10:53` - IP-адрес и порт назначения;
- `DROP` - результат анализа трафика;
- `[eBay]` - название приложения, к которому применен результат. Список всех приложений.

Контент-фильтр:

Логирование включается в разделе **Сервисы -> Прокси -> Основное**. Просмотр логов доступен в веб-интерфейсе в разделе **Отчеты и журналы -> Системный журнал**. Название служб для фильтрации: `ideco-content-filter-backend` и `squid`.

Пример блокировки ресурса:

```
2024-11-18T19:56:41+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731941801 Severity=Notice DeviceProcessName=squid␣
↪msg={10.128.0.5 - - [18/Nov/2024:19:56:41 +0500] "GET http://counter.yadro.ru/hit;
↪argon? HTTP/1.1" 403 7594 "http://argon.pro/" "Mozilla/5.0 (Windows NT 10.0; Win64;␣
↪x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.
↪0.0.0" TCP_MISS:ORIGINAL_DST "-","av_name": "-","av_object_infected": "-","av_
↪object_size": "7250","av_virus_name": "-","x_infection_found": "-","x_virus_id": "-
↪","x_av_verifed": "-","morph-action": "CheckedOK","morph-dict-id": "-"}
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `10.128.0.5` - IP-адрес пользователя;

- `[18/Nov/2024:19:56:41 +0500]` - дата/время события блокировки;
- `GET` - метод;
- `http://counter.yadro.ru/hit;argon?` - URL заблокированного ресурса;
- `HTTP/1.1` - протокол;
- `403` - код состояния HTTP;
- `7594` - передано байт (в ответ, включая HTTP-заголовок);
- `http://argon.pro/` - HTTP referer;
- `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0` - цифровой отпечаток браузера;
- `TCP_MISS:ORIGINAL_DST` - техническое сообщение от squid;
- `"av_name": "-"` - название антивируса, если он включен, в примере антивирус отключен;
- `"av_object_infected": "-"` - результат проверки антивирусом, пустое поле - вирус не обнаружен;
- `"av_object_size": "7250"` - размер проверяемого объекта;
- `"av_virus_name": "-"` - название обнаруженного вируса;
- `"x_infection_found": "-"` - подтверждение, что запрос был обработан ICAP-оберткой для антивируса (Касперский);
- `"morph-action": "CheckedOK"` - результат проверки **Морфологическим анализом**;
- `"morph-dict-id": "-"` - название морфологического словаря, указывается в случае запрета **Морфологическим анализом**.

SSO-аутентификация:

```
2024-07-18T17:11:40+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721304700 Severity=Notice DeviceProcessName=ideco-
↪web-authd msg=Subnet 192.168.205.254/32 is authorized as user 'Sanek'. Connection␣
↪made from None, type 'web'.
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `192.168.205.254/32` - IP-адрес пользователя;
- `Sanek` - логин пользователя;
- `type 'web'` - тип авторизации (веб).

Авторизация через журнал безопасности AD:

```
2024-07-18T17:20:22+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721305222 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.205.254/32 is authorized as user 'Sanek'.␣
↪Connection made from None, type 'log'.
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `192.168.205.254/32` - IP-адрес пользователя;

- Sanek - логин пользователя;
- type 'log' - тип авторизации (через журнал безопасности AD).

Веб-авторизация:

```
2024-11-18T14:54:21+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731923661 Severity=Notice DeviceProcessName=ideco-
↪web-authd msg=Subnet 192.168.101.25/32 is authorized as user 'user'. Connection␣
↪made from None, type 'web'.
```

- deviceReceiptTime - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- Severity - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- DeviceProcessName - название службы NGFW;
- user - логин пользователя;
- 192.168.101.25/32 - IP-адрес пользователя;
- type 'web' - тип авторизации (веб).

Авторизация по IP:

```
2024-11-18T18:51:43+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731937903 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.101.25/32 is authorized as user 'user'. Connection␣
↪made from None, type 'ip'.
```

- deviceReceiptTime - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- Severity - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- DeviceProcessName - название службы NGFW;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'ip' - тип авторизации (IP).

Авторизация по MAC:

```
2024-11-18T18:54:21+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731938061 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.101.25/32 is authorized as user 'user'. Connection␣
↪made from None, type 'mac'.
```

- deviceReceiptTime - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- Severity - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- DeviceProcessName - название службы NGFW;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'mac' - тип авторизации (MAC).

Авторизация по подсетям:

```
2024-11-18T19:07:54+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731938874 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.101.0/24 is authorized as user 'user'. Connection␣
↪made from None, type 'net'.
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `192.168.101.0/24` - подсеть, по которой происходит авторизация;
- `user` - логин пользователя;
- `type 'net'` - тип авторизации (подсеть).

Подключение по VPN:

```
2024-11-18T19:16:18+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731939378 Severity=Notice DeviceProcessName=ideco-
↪vpn-authd msg=Start vpn authorization ('user', '192.168.1.25', 'pptp').
2024-11-18T19:16:18+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731939378 Severity=Notice DeviceProcessName=ideco-
↪vpn-authd msg=Subnet 10.128.0.6/32 is authorized as user 'user'. Connection made␣
↪from '192.168.1.25', type 'pptp'.
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `10.128.0.6/32` - сеть для VPN-подключений;
- `user` - логин пользователя;
- `192.168.1.25` - IP-адрес, откуда установлено подключение;
- `pptp` - протокол.

Служба fail2ban:

```
2024-11-18T19:26:57+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Notice␣
↪DeviceProcessName=fail2ban msg=INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-18␣
↪19:26:57
2024-11-18T19:26:57+05:00 ngfw-18 CEF:0|Ideco|NGFW|18.
↪0|0|syslog|0|deviceReceiptTime=1731940017 Severity=Warning␣
↪DeviceProcessName=fail2ban msg=NOTICE [utm-vpn-authd] Ban 192.168.1.25
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `INFO` или `NOTICE` - приоритет сообщения в логах в виде информационного сообщения или уведомления;
- `INFO [utm-web-interface] Found 192.168.1.25 - 2024-11-18 19:26:57` - факт обнаружения правил безопасности с указанием группы правил ([utm-web-interface]), IP-адреса и даты/времени. Список групп правил:

- `utm-dovecot` - авторизация на почтовом сервере через почтовые клиенты;
- `utm-postfix-connrate` - превышение лимита подключения к почтовому серверу;
- `utm-postscreen-prgrt` - отслеживание нежелательных подключений (PREGREET) к почтовому серверу;
- `utm-reverse-proxy-conn` - защита от DoS (лимит подключений);
- `utm-reverse-proxy-req` - защита от DoS (лимит запросов в секунду);
- `utm-reverse-proxy` - Web Application Firewall (WAF);
- `utm-roundcube` - авторизация в веб-интерфейсы почтового сервера;
- `utm-smtp` - авторизация по smtp;
- `utm-ssh` - авторизация по ssh;
- `utm-two-factor-codes` - прохождение двухфакторной аутентификации;
- `utm-vpn-authd` - авторизация по VPN;
- `utm-vpn-pppoe-authd` - авторизация по VPN PPPoE;
- `utm-web-interface` - авторизация в административном веб-интерфейсе;
- `utm-user-cabinet` - авторизация в пользовательском веб-интерфейсе.

- `NOTICE [utm-vpn-authd] Ban 192.168.1.25` - факт блокировки или разблокировки IP-адреса, где:
  - `Ban` - факт блокировки;
  - `Unban` - факт разблокировки.

Формат Syslog

Message в Syslog-формате:

Предотвращение вторжений:

```
2024-11-18T15:40:12+05:00 ngfw-18 suricata - - - flow_id:1344232018329395, in_iface:,␣
↪sensor_name:ideco-ips, event_type:alert, src_ip:192.168.101.25, src_ip_type:local,␣
↪src_port:40632, src_country:, src_country_code:, src_session_uuid:34fbd7c6-716b-
↪4858-bb68-313729b1cad4, src_user_id:9, src_user_name:user, dest_ip:212.70.163.70,␣
↪dest_ip_type:external, dest_port:443, dest_country:Латвия, dest_country_code:LV,␣
↪dest_session_uuid:, dest_user_id:-1, dest_user_name:, proto:TCP, alert.signature_
↪id:1005404, alert.signature:GeoIP Latvia, alert.category:GeoIP Страны Восточной␣
↪Европы, alert.severity:2, alert.gid:1, alert.action:blocked, http.hostname:, http.
↪url:, http.http_user_agent:, flow.pkts_toserver:1, flow.pkts_toclient:0, flow.bytes_
↪toserver:60, flow.bytes_toclient:0, flow.start:2024-11-18 10:40:12.378514, flow.
↪end:2024-11-18 10:40:12.379198, flow.age:0, flow.state:, flow.reason:, flow.
↪alerted:0, tcp.tcp_flags:, tcp.tcp_flags_ts:, tcp.tcp_flags_tc:, tcp.cwr:0, tcp.
↪ecn:0, tcp.urg:0, tcp.ack:0, tcp.psh:0, tcp.rst:0, tcp.syn:0, tcp.fin:0, tcp.state:
```

где:

- `2024-11-18T15:40:12+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `suricata` - название службы;
- `flow_id:1344232018329395` - внутренний идентификатор системы предотвращения вторжений flow (сессии);
- `in_iface` - идентификатор входящего интерфейса;
- `sensor_name:ideco-ips` - имя экземпляра системы предотвращения вторжений;

- `event_type:alert` - тип события;
- `src_ip:192.168.101.25` - IP-адрес источника;
- `src_port:40632` - порт источника;
- `src_country` - название местоположения источника;
- `src_country_code` - ISO-код страны источника;
- `src_session_uuid:34fbd7c6-716b-4858-bb68-313729b1cad4` - внутренний идентификатор сессии Ideco NGFW источника;
- `src_user_id:9` - идентификатор пользователя источника;
- `src_user_name:user`- имя пользователя источника;
- `dest_ip:212.70.163.70` - IP-адрес назначения;
- `dest_port:443` - порт назначения;
- `dest_country:Латвия` - название местоположения назначения;
- `dest_country_code:LV` - ISO-код страны назначения;
- `dest_session_uuid` - внутренний идентификатор сессии Ideco NGFW назначения;
- `dest_user_id:-1` - идентификатор пользователя назначения;
- `dest_user_name` - имя пользователя назначения;
- `proto:TCP` - протокол;
- `alert.signature_id:1005404` - идентификатор правила системы предотвращения вторжений;
- `alert.signature:GeoIP Latvia` - сообщение из сработавшего правила;
- `alert.category:GeoIP Страны Восточной Европы` - описание колонки в веб-интерфейсе События безопасности;
  Соответствие *alert.category: -> alert.signature* описаны в файле.
- `alert.severity:2` - уровень угрозы, может принимать значения 1, 2, 3 и 256, где 1 - самый высокий уровень угрозы;
- `alert.gid:1` - GID угрозы;
- `alert.action:blocked` - действие по отношению к угрозе (блокировать).

Служебные поля результата анализа HTTP-трафика. Заполняются, если в процессе анализа трафика был определен HTTP-протокол:

- `http.hostname` - идентификатор хоста;
- `http.url` - URL, на который велось обращение;
- `http.http_user_agent` - информация, идентифицирующая HTTP-клиента.

Служебные поля flow (сессии):

- `flow.pkts_toserver:1` - количество пакетов, переданное от клиента к серверу;
- `flow.pkts_toclient:0` - количество пакетов, переданное от сервера к клиенту;
- `flow.bytes_toserver:60` - количество байт, переданное от клиента к серверу;
- `flow.bytes_toclient:0` - количество байт, переданное от сервера к клиенту;
- `flow.start:2024-11-18 10:40:12.378514` - начало;
- `flow.end:2024-11-18 10:40:12.379198` - окончание;
- `flow.age:0` - возраст;
- `flow.state` - текущее состояние;
- `flow.reason` - запущена ли IPsec в режиме отладки;

- `flow.alerted:0` - сгенерировался ли поток alert.

Состояние флага TCP flow(сессии):

- `tcp.tcp_flags` - значение поля flags в заголовке TCP;
- `tcp.tcp_flags_ts` - timestamp флаги;
- `tcp.tcp_flags_tc` - флаг Truncated response;
- `tcp.cwr: 0` - флаг TCP-пакета, информирующий отправителя, что получен пакет с установленным флагом ECE (Подробнее в RFC-3186);
- `tcp.ecn:0` - флаг TCP-пакета, информирующий получателя, что узел способен на явное уведомление о перегрузке сети;
- `tcp.urg:0` - флаг TCP-пакета, указывающий важность пакета;
- `tcp.ack:0` - флаг TCP-пакета, указывающий, что пакет получен;
- `tcp.psh:0` - флаг TCP-пакета, информирующий получателя, что все данные переданы и можно передать их приложению;
- `tcp.rst:0` - флаг TCP-пакета, указывающий, что соединение завершено в аварийном режиме;
- `tcp.syn:0` - флаг TCP-пакета, отвечающий за установку соединения;
- `tcp.fin:0` - флаг TCP-пакета, указывающий на завершение соединения в штатном порядке;
- `tcp.state` - состояния сеанса TCP.

Файрвол:

Логирование включается в разделе **Правила трафика -> Файрвол -> Логирование**. Включите опцию **Логировать срабатывания правил**.

```
2025-01-27T13:33:19+05:00 ngfw-18 ideco-nflog - - - TCP src 192.168.101.25 sport␣
↪54186 dst 64.233.164.105 dport 443 table FWD rule 2 action drop
```

- `2025-01-27T13:33:19+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-nflog` - название службы;
- `TCP` - протокол. Это поле принимает значения: UDP, TCP, ICMP, GRE, ESP и AH;
- `src` - IP-адрес источника;
- `sport` - порт источника для UDP и TCP;
- `dst` - IP-адрес назначения;
- `dport` - порт назначения для UDP и TCP;
- `table` - таблица правил, в которой произошло логирование;
- `rule` - ID правила из таблицы;
- `action` - действие, которое произошло.

Контроль приложений:

```
2024-12-02T20:38:38+05:00 ngfw-18 ideco-app-stats - - - 192.168.101.25:56854 -> 192.
↪168.101.10:53 [eBay] = DROP
```

- `2024-12-02T20:38:38+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-app-stats` - название службы;
- `192.168.101.25:56854` - IP-адрес и порт источника;

- `192.168.101.10:53` - IP-адрес и порт назначения;
- `DROP` - результат анализа трафика;
- `[eBay]` - название приложения, к которому применен результат. Список всех приложений.

Контент-фильтр:

Логирование включается в разделе **Сервисы -> Прокси -> Основное**. Просмотр логов доступен в веб-интерфейсе в разделе **Отчеты и журналы -> Системный журнал**. Название служб для фильтрации: `ideco-content-filter-backend` и `squid`.

Пример блокировки ресурса:

```
2024-11-18T19:49:58+05:00 ngfw-18 squid - - - {10.128.0.6 - - [18/Nov/2024:19:49:58␣
↪+0500] "GET http://counter.yadro.ru/hit;argon? HTTP/1.1" 403 7594 "http://argon.pro/
↪" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)␣
↪Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0" TCP_MISS:ORIGINAL_DST "-","av_name":
↪"-","av_object_infected": "-","av_object_size": "7250","av_virus_name": "-","x_
↪infection_found": "-","x_virus_id": "-","x_av_verifed": "-","morph-action":
↪"CheckedOK","morph-dict-id": "-"}
```

- `2024-11-18T19:49:58+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `squid` - название службы;
- `10.128.0.6` - IP-адрес пользователя;
- `[18/Nov/2024:19:49:58 +0500]` - дата/время события блокировки;
- `GET` - метод;
- `http://counter.yadro.ru/hit;argon?` - URL заблокированного ресурса;
- `HTTP/1.1` - протокол;
- `403` - код состояния HTTP;
- `7594` - передано байт (в ответ, включая HTTP-заголовок);
- `http://argon.pro/` - HTTP referer;
- `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0` - цифровой отпечаток браузера;
- `TCP_MISS:ORIGINAL_DST` - техническое сообщение от squid;
- `"av_name": "-"` - название антивируса, если он включен, в примере антивирус отключен;
- `"av_object_infected": "-"` - результат проверки антивирусом, пустое поле - вирус не обнаружен;
- `"av_object_size": "7250"` - размер проверяемого объекта;
- `"av_virus_name": "-"` - название обнаруженного вируса;
- `"x_infection_found": "-"` - подтверждение, что запрос был обработан ICAP-оберткой для антивируса (Касперский);
- `"morph-action": "CheckedOK"` - результат проверки **Морфологическим анализом**;
- `"morph-dict-id": "-"` - название морфологического словаря, указывается в случае запрета **Морфологическим анализом**.

SSO-аутентификация:

```
2024-07-18T16:59:55+05:00 Ideco-NGFW ideco-web-authd - - - Subnet 192.168.205.254/32␣
↪is authorized as user 'Sanek'. Connection made from None, type 'web'.
```

- `2024-07-18T16:59:55+05:00` - время события в Ideco NGFW;

- `Ideco-NGFW` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-web-authd` - название службы;
- `192.168.205.254/32` - IP-адрес пользователя;
- `Sanek` - логин пользователя;
- `type 'web'` - тип авторизации (веб).

Авторизация через журнал безопасности AD:

```
2024-07-18T16:19:39+05:00 Ideco-NGFW ideco-auth-backend - - - Subnet 192.168.205.254/
↪32 is authorized as user 'Sanek'. Connection made from None, type 'log'.
```

- `2024-07-18T16:19:39+05:00` - время события в Ideco NGFW;
- `Ideco-NGFW` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-auth-backend` - название службы;
- `192.168.205.254/32` - IP-адрес пользователя;
- `Sanek` - логин пользователя;
- `type 'log'` - тип авторизации (через журнал безопасности AD).

Веб-авторизация:

```
2024-11-18T14:47:11+05:00 ngfw-18 ideco-web-authd - - - Subnet 192.168.101.25/32 is␣
↪authorized as user 'user'. Connection made from None, type 'web'.
```

- `2024-11-18T14:47:11+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-web-authd` - название службы;
- `192.168.101.25/32` - IP-адрес пользователя;
- `user` - логин пользователя;
- `type 'web'` - тип авторизации (веб).

Авторизация по IP:

```
2024-11-18T18:42:45+05:00 ngfw-18 ideco-auth-backend - - - Subnet 192.168.101.25/32␣
↪is authorized as user 'user'. Connection made from None, type 'ip'.
```

- `2024-11-18T18:42:45+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-web-authd` - название службы;
- `192.168.101.25/32` - IP-адрес пользователя;
- `user` - логин пользователя;
- `type 'ip'` - тип авторизации (IP).

Авторизация по MAC:

```
2024-11-18T19:01:14+05:00 ngfw-18 ideco-auth-backend - - - Subnet 192.168.101.25/32␣
↪is authorized as user 'user'. Connection made from None, type 'mac'.
```

- `2024-11-18T19:01:14+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-auth-backend` - название службы;

- `192.168.101.25/32` - IP-адрес пользователя;
- `user` - логин пользователя;
- `type 'mac'` - тип авторизации (MAC).

Авторизация по подсетям:

```
2024-11-18T19:06:08+05:00 ngfw-18 ideco-auth-backend - - - Subnet 192.168.101.0/24 is␣
↪authorized as user 'user'. Connection made from None, type 'net'.
```

- `2024-11-18T19:06:08+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-auth-backend` - название службы;
- `192.168.101.0/24` - подсеть пользователя;
- `user` - логин пользователя;
- `type 'net'` - тип авторизации (подсеть).

Подключение по VPN:

```
2024-11-18T19:17:56+05:00 ngfw-18 ideco-vpn-authd - - - Start vpn authorization ('user
↪', '192.168.1.25', 'pptp').
2024-11-18T19:17:56+05:00 ngfw-18 ideco-vpn-authd - - - Subnet 10.128.0.5/32 is␣
↪authorized as user 'user'. Connection made from '192.168.1.25', type 'pptp'.
```

- `2024-11-18T19:17:56+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-vpn-authd` - название службы;
- `10.128.0.5/32` - сеть для VPN-подключений;
- `user` - логин пользователя;
- `192.168.1.25` - IP-адрес, с которого установлено подключение;
- `pptp` - протокол.

Служба fail2ban:

```
2024-11-18T19:21:54+05:00 ngfw-18 fail2ban - - - INFO [utm-vpn-authd] Found 192.168.1.
↪25 - 2024-11-18 19:21:54
```

- `2024-11-18T19:21:54+05:00` - время события в Ideco NGFW;
- `ngfw-18` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `fail2ban` - название службы;
- `info` или `notice` - приоритет сообщения в логах в виде информационного сообщения или уведомления;
- `INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-18 19:21:54` - факт обнаружения правил безопасности с указанием группы правил (`[utm-web-interface]`), IP-адреса и даты/времени. Список групп правил:
  - `utm-dovecot` - авторизация на почтовом сервере через почтовые клиенты;
  - `utm-postfix-connrate` - превышение лимита подключения к почтовому серверу;
  - `utm-postscreen-prgrt` - отслеживание нежелательных подключений (PREGREET) к почтовому серверу;
  - `utm-reverse-proxy-conn` - защита от DoS (лимит подключений);

- `utm-reverse-proxy-req` - защита от DoS (лимит запросов в секунду);
- `utm-reverse-proxy` - Web Application Firewall (WAF);
- `utm-roundcube` - авторизация в веб-интерфейсы почтового сервера;
- `utm-smtp` - авторизация по smtp;
- `utm-ssh` - авторизация по ssh;
- `utm-two-factor-codes` - прохождение двухфакторной аутентификации;
- `utm-vpn-authd` - авторизация по VPN;
- `utm-vpn-pppoe-authd` - авторизация по VPN PPPoE;
- `utm-web-interface` - авторизация в административном веб-интерфейсе;
- `utm-user-cabinet` - авторизация в пользовательском веб-интерфейсе.

20. Управление сервером

20.1 Администраторы

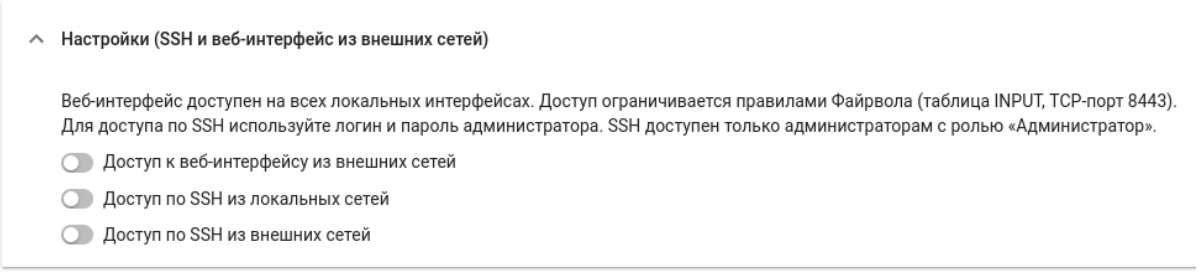
В Ideco NGFW вы можете создать локальных администраторов или интегрировать администраторов из сервисов Active Directory, ALD PRO, RADIUS.

Сведения об авторизованных администраторах представлены в разделах **Авторизация администраторов** и *Сессии администраторов*.

Подсказка: При бездействии в течение 15 минут администратор будет автоматически разавторизован.

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

- Для получения доступа к Ideco NGFW из внешней сети включите опцию **Доступ к веб-интерфейсу из внешней сети**. Эта функция помогает заниматься администрированием Ideco NGFW удаленно. Попытки подбора паролей блокируются автоматически.
- Для получения доступа к Ideco NGFW по SSH из локальной или внешних сетей включите соответствующие опции. Доступ осуществляется по 22 TCP-порту. Попытки подбора паролей также будут автоматически блокироваться:



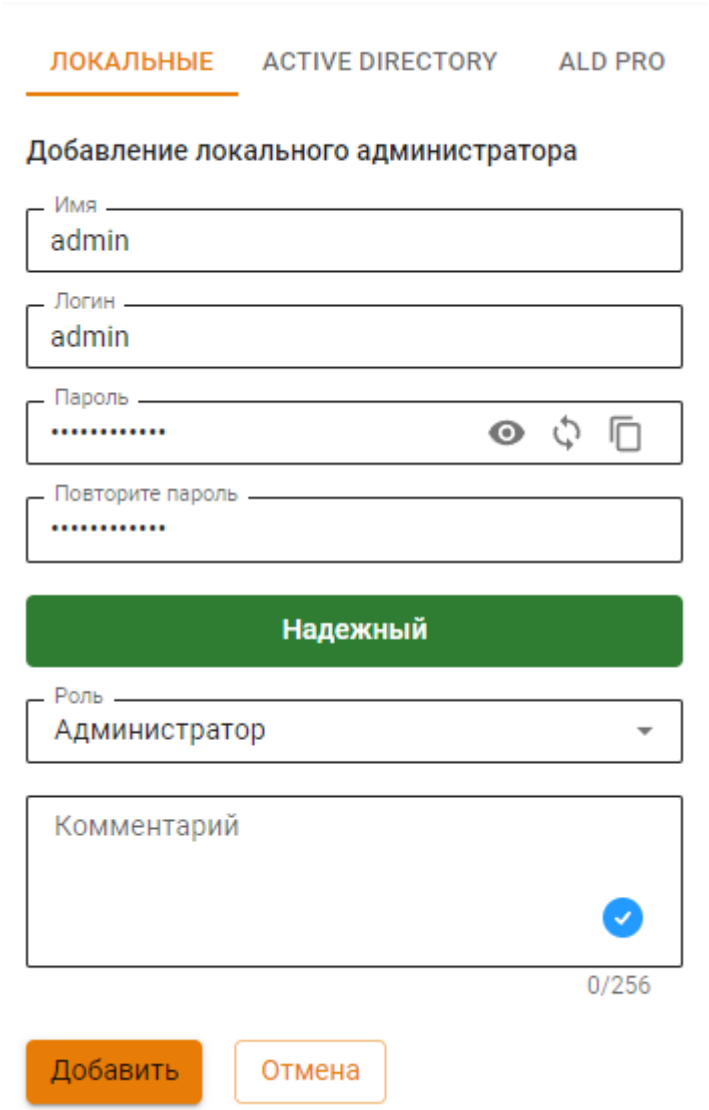
Подробнее о настройке подключения к веб-интерфейсу при удаленном доступе смотрите в статье *Удаленный доступ для управления сервером*.

20.1.2 Управление локальными администраторами

Чтобы добавить нового локального администратора выполните действия:

1. Перейдите в раздел **Управление сервером -> Администраторы**, на вкладку **Локальные** и нажмите кнопку **Добавить**.

2. Заполните поля:



- **Имя** - введите имя нового администратора. Значение не должно быть длиннее 42 символов;
- **Логин** - введите логин нового администратора. Значение не должно превышать 42 символа и не должно состоять только из цифр;
- **Пароль/повторите пароль** - введите пароль нового администратора. Рекомендуем использовать сложные пароли, содержащие латинские строчные и заглавные буквы, цифры и специальные символы;
- **Роль** - выберите роль:
  - **Администратор** - полный доступ к настройке Ideco NGFW;
  - **Только просмотр** - доступ к просмотру настроек Ideco NGFW;
  - **Администратор ИБ** - доступ к работе с событиями безопасности;
  - **Администратор файрвола** - доступ к созданию учетных записей, работа с правилами фильтрации, управление режимами работы Файрвола;

– **Администратор настройки доступов** - доступ к настройкам сетевого взаимодействия пользователей Файрвола, субъектов доступа, информационных систем;

– **Просмотр отчетов** - доступ к части раздела *Отчеты и журналы*, а именно: **Трафик**, **Журнал событий**, **Журнал веб-трафика**, **События безопасности** и **Журнал аутентификации**;

– **Создание отчетов** - доступ к части раздела *Отчеты и журналы*, а именно: **Трафик**, **Журнал событий**, **Журнал веб-трафика**, **События безопасности**, **Журнал аутентификации** и **Конструктор отчетов**.

3. Нажмите **Добавить**.

Чтобы изменить имя и пароль администратора, нажмите на  в столбце **Управление**. Подробнее о восстановлении пароля администратора смотрите в статье по *ссылке*.

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

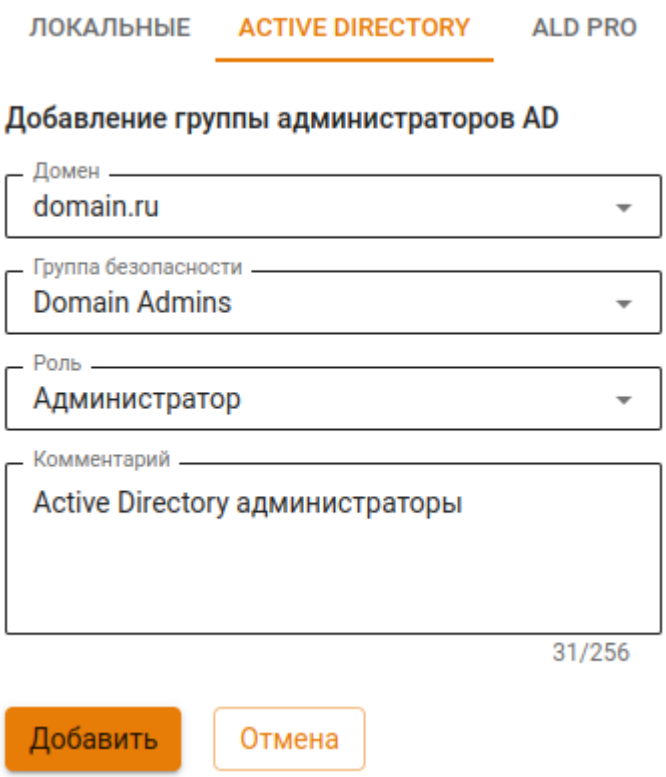
20.1.3 Управление AD/ALD администраторами

Подсказка: Чтобы добавить администраторов, необходимо ввести NGFW в домен *Active Directory* или *ALD Pro*. При удалении домена AD/ALD из Ideco NGFW будут удалены сессии администраторов.

Чтобы интегрировать администраторов Active Directory или ALD Pro с Ideco NGFW выполните действия:

1. Перейдите в раздел **Управление сервером -> Администраторы**, выберите нужную вкладку и нажмите кнопку **Добавить**.

2. Заполните поля:



- **Домен** - выберите доменное имя;
- **Группа безопасности** - выберите созданную *группу безопасности*;
- **Роль** - выберите роль. Роли AD/ALD администраторов идентичны ролям локальных администраторов.

3. Нажмите **Добавить**.

Особенности работы:

- Если администратор был авторизован по правилу или группе безопасности, которые были удалены, его сессия будет удалена. Это произойдет только после синхронизации групп безопасности на Ideco NGFW, которая выполняется каждые 5 минут;
- Если администратора исключить из группы безопасности, он не будет удален сразу. Его сессия завершится через некоторое время, и при следующей попытке авторизации он не сможет войти в систему;
- Если администратор соответствует нескольким правилам при авторизации, например, входит в несколько выбранных групп безопасности, ему будет отказано в доступе. Это необходимо, чтобы избежать проблем в определении прав доступа для администратора.

20.1.4 Управление RADIUS-администраторами

Особенности настройки RADIUS-сервера

В Ideco NGFW используется **Vendor Code** 39410. Для авторизации через RADIUS укажите атрибуты:

```
ATTRIBUTE   Ideco-Administrator-Role            30  string
ATTRIBUTE   Ideco-Administrator-Name            31  string
```

`Ideco-Administrator-Role` обязателен для авторизации, а `Ideco-Administrator-Name` опционален. Атрибуты передают ID роли и ФИО администратора соответственно.

Чтобы узнать ID роли RADIUS-администратора:

1. Перейдите в раздел **Управление сервером -> Администраторы -> Роли**;

2. Нажмите на **Отображение** и включите столбец ID. ID роли появится в левом столбце таблицы.

ID роли администраторов:

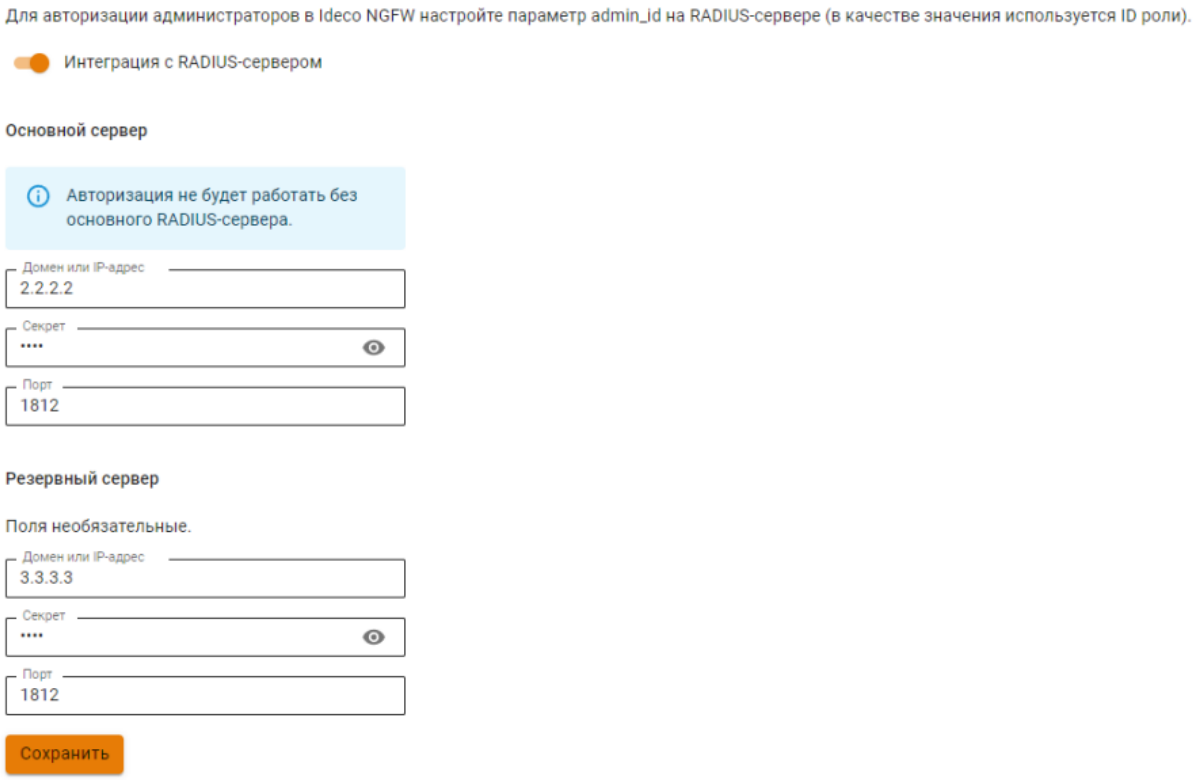
- `predefined_admin_write` - Администратор;
- `predefined_admin_readonly` - Только просмотр;
- `predefined_security_admin` - Администратор информационной безопасности;
- `predefined_firewall_admin` - Администратор файрвола;
- `predefined_access_settings_admin` - Администратор настройки доступов;
- `predefined_reports_view` - Просмотр отчетов;
- `predefined_reports_change` - Создание отчетов.

Интеграция администраторов RADIUS с Ideco NGFW

Выполните действия:

1. Перейдите в раздел **Управление сервером -> Администраторы**, на вкладку **RADIUS** и включите опцию **Интеграция с RADIUS-сервером**.

2. Укажите доменное имя или IP-адрес внутреннего RADIUS-сервера и секрет (пароль доступа). Если требуется, поменяйте порт, по которому будет происходить подключение к серверу:



При наличии в сети двух RADIUS-серверов настройте один как резервный с указанием порта подключения. При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.

3. Нажмите **Сохранить**.

20.1.5 Особенности удаления администраторов

- Если администратора удалить из раздела **Администраторы**, его сессия будет автоматически завершена, и он потеряет доступ к веб-интерфейсу;
- Если администратора удалить из группы безопасности, то сессия будет автоматически завершена через 24 часа после авторизации.

Чтобы удалить администратора, нажмите на  напротив нужной учетной записи. Можно удалить и собственный аккаунт.

Предупреждение: Не рекомендуем удалять или отключать всех администраторов с ролью **Администратор**, это приведет к тому, что доступ к настройке Ideco NGFW будет потерян. Если подобное произошло, обратитесь в *Техническую поддержку*.

20.1.6 Аутентификация администраторов

Подсказка: Ideco NGFW не только блокирует попытки авторизации с неправильными логином или паролем, но и обнаруживает случаи, когда не удается получить информацию об администраторе из контроллера домена. Если администратор не соответствует ни одному из правил авторизации, Ideco NGFW считает попытку авторизации неудачной и блокирует доступ, если количество неудачных попыток превышает допустимое.

Чтобы получить доступ к веб-интерфейсу Ideco NGFW, администратору нужно выполнить процедуру аутентификации, указав логин и пароль.

Для разных групп администраторов предусмотрены разные логины:

- **Локальный администратор** - логин в формат `User`;
- **AD/ALD администратор** - логин в формате `User@test.com`, где `test.com` домен;
- **RADIUS администратор** - логин в формате `User@radius`, где `@radius` обязательная часть логина.

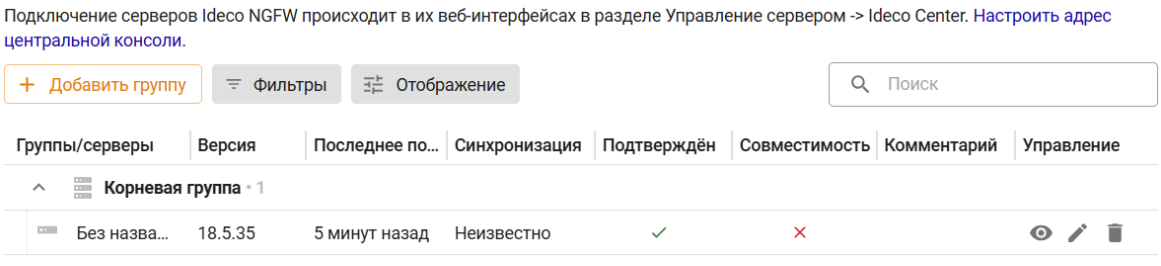
20.2 Ideco Center

Подсказка: Название службы раздела **Ideco Center**: `ideco-central-console-backend`.
Список служб для других разделов доступен по *ссылке*.

Ideco Center - это центральная консоль, которая поможет в администрировании нескольких серверов Ideco NGFW. На данный момент не требует лицензирования и не имеет ограничений к использованию. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW, даже если они были подключены после того, как политики были настроены.

20.2.1 Подключение Ideco NGFW к Ideco Center

Внимание: При синхронизации Ideco Center и Ideco NGFW с разными мажорными версиями передача правил с Ideco Center происходить не будет. При этом в разделе **Серверы** будет информация о том, что Ideco Center и Ideco NGFW несовместимы:

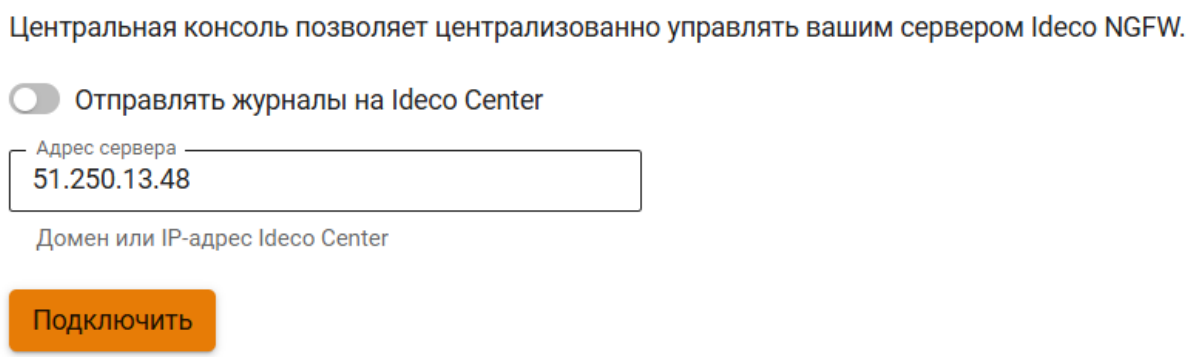


Предупреждение: Особенности работы:

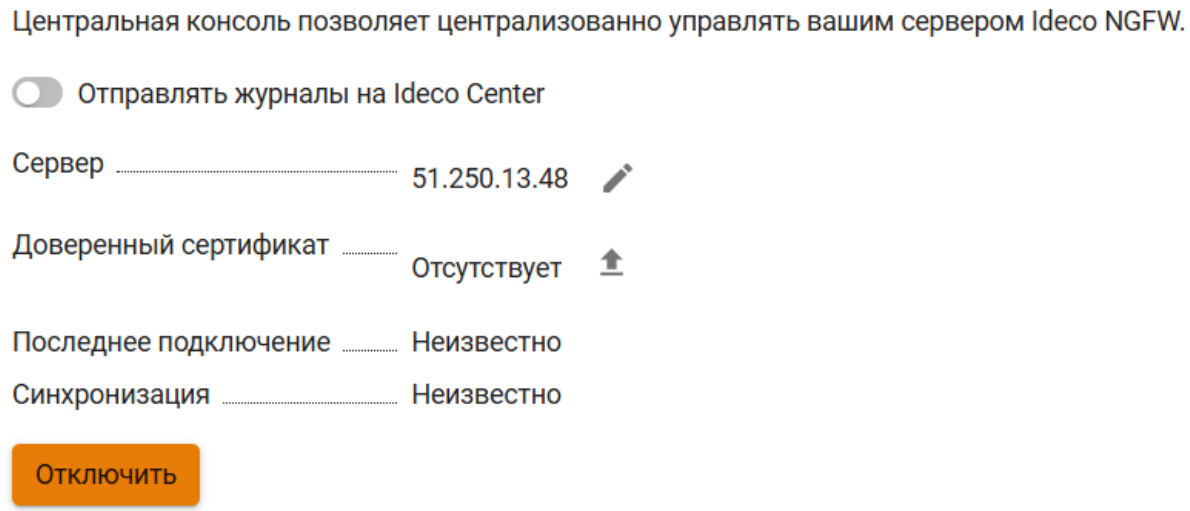
- Если в подключаемом Ideco NGFW используется кластер, достаточно подключить только активную ноду, пассивная автоматически примет эту настройку;
- Сетевое подключение производится в направлении от Ideco NGFW к Ideco Center, т. е. возможна связь и когда Ideco NGFW за NAT;
- Если сервер Ideco Center находится за NAT, укажите IP-адрес NAT-устройства или доменное имя, перейдя в Ideco Center в раздел **Управление сервером -> Дополнительно -> Адрес Ideco Center**.

1. Перейдите в раздел **Управление сервером -> Ideco Center**.

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

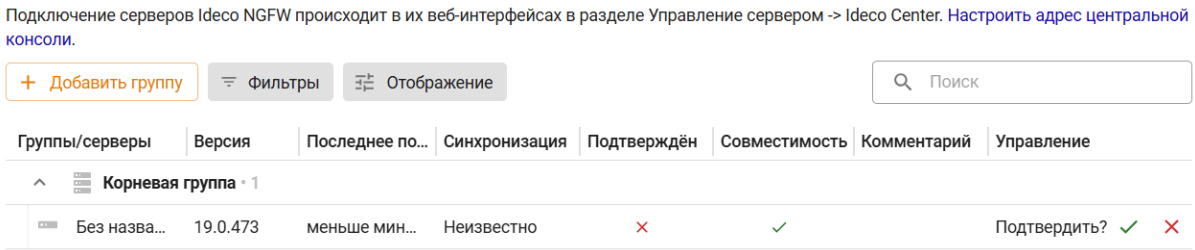


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW:



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

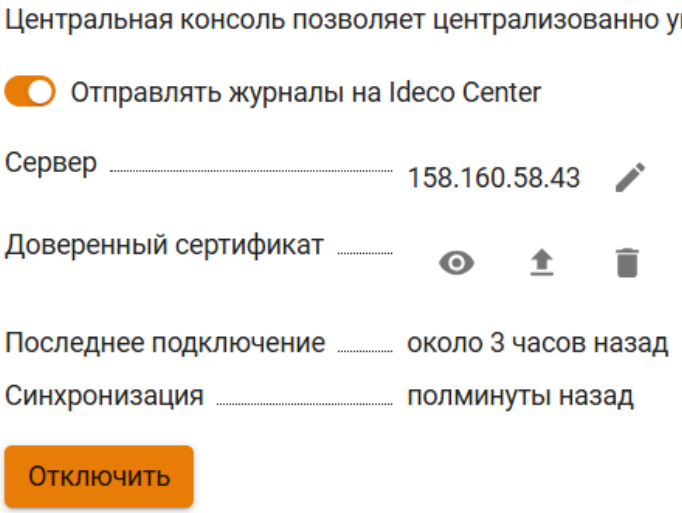
3. В интерфейсе Ideco Center перейдите в раздел **Серверы** и подтвердите подключение кнопкой ✓ :



Для удаления сервера Ideco NGFW из Ideco Center разорвите привязку в интерфейсе Ideco Center:

20.2.2 Настройка просмотра логов

Для отображения логов Ideco NGFW в разделе ***Отчеты и журналы*** Ideco Center необходимо включить опцию **Отправлять журналы на Ideco Center**:



Для этого в таблице **Серверы** в столбце **Управление** напротив нужного сервера выберите  и подтвердите выбор.

20.3 VCE

Подсказка: Название службы раздела **VCE**: `ideco-vce-backend`.
Список служб для других разделов доступен по *ссылке*.

VCE (virtual context engine) - это функция Ideco NGFW, которая позволяет создавать виртуальные серверы на одном корневом NGFW. Это дает возможность разбить одну локальную сеть на несколько независимых подсетей, индивидуально создавать для каждой из этих сетей политики безопасности и объекты, а также разграничивать доступ и независимо управлять дочерними VCE. При этом нет необходимости устанавливать и настраивать для этого отдельные физические серверы.

Предупреждение: Не предоставляйте доступ к VCE сторонним организациям, поскольку полная изоляция VCE не реализована и не предусмотрена. Предоставление доступа сторонним организациям может привести к угрозе безопасности сервера.

Подсказка: Сейчас для каждого созданного VCE загружается файл лицензии корневой системы. Это значит, что на Ideco NGFW с лицензией на 100 пользователей можно создать неограниченное количество VCE, каждый из которых также будет поддерживать по 100 пользователей.

Функциональность созданных внутри NGFW виртуальных VCE почти не отличается от функциональности NGFW.

Возможности VCE:

- Создание виртуальных серверов Ideco NGFW и настройка независимых сетевых интерфейсов;
- Независимая настройка политик безопасности и прав доступа различным виртуальным NGFW;
- Связь с Ideco Center;

- Запуск и остановка виртуальных серверов с одного корневого NGFW.

В интерфейсе VCE недоступно:

- Создание *кластера*;
- Полное восстановление из бэкапов (как в локальном меню, так и в веб-интерфейсе Ideco NGFW). Доступно только быстрое восстановление;
- Изменение статуса **Разрешить интернет всем** (настраивается в корневой системе);
- Переход в **Профиль** через иконку ☺ в шапке веб-интерфейса (настраивается в корневой системе);
- Возможность выключения и перезагрузки (настраивается в корневой системе);
- Энергосберегающий режим (настраивается в корневой системе);
- Изменение настроек часового пояса и языка (настраивается в корневой системе).

Подсказка: В *бэкап* корневого VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте бэкапы корневого NGFW и каждого из дочерних VCE.

Нельзя добавлять LACP-интерфейсы в VCE.

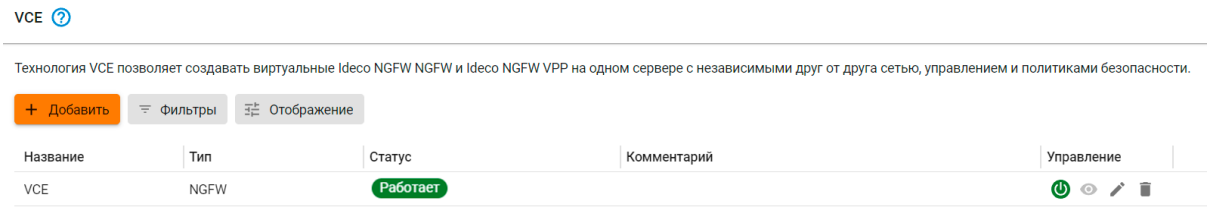
20.3.1 Создание VCE

Подсказка: Для работы VCE требуется минимум 8 ГБ оперативной памяти, а максимум можно выделить 16 ГБ.

Чтобы создать виртуальный сервер в рамках VCE, перейдите в раздел **Управление сервером -> VCE** и выполните действия:

1. Нажмите кнопку **Добавить**.

2. Введите название сервера и нажмите **Добавить**. Виртуальный сервер появится в таблице:



3. Перейдите в раздел **Сервисы -> Сетевые интерфейсы** и на вкладке **VCE** создайте интерфейс для виртуального сервера. Для работы VCE нужна минимум одна сетевая карта, их максимальное количество не ограничено. Подробнее о создании VCE-интерфейсов в *статье*.

Подсказка: Сетевая карта без тега VLAN, подключенная к VCE, будет недоступна для использования корневым NGFW.

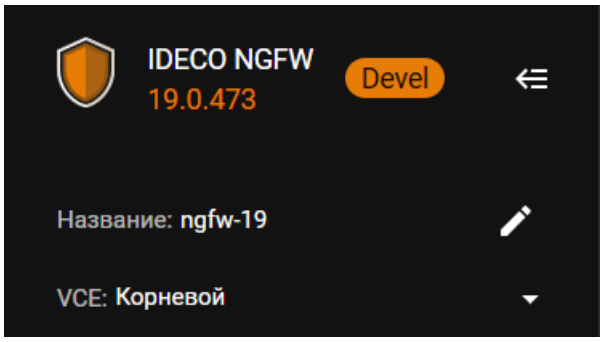
Если VCE выключен, переданные ему сетевые карты становятся вновь доступны корневому NGFW, их можно использовать для создания нового виртуального сервера. При этом VCE, которому они принадлежали ранее, станет недоступен после включения.

Чтобы отредактировать VCE, нажмите на . При редактировании можно менять название виртуального сервера. Редактирование доступно в том числе для работающего VCE.

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

20.3.2 Переход в веб-интерфейс VCE

После создания VCE текущий сервер NGFW, в котором VCE был создан, будет обозначен как корневой:



Перейти в веб-интерфейс созданного VCE из веб-интерфейса NGFW можно двумя способами:

1. Перейдите в **Управление сервером -> VCE** и нажмите на :

После этого веб-интерфейс VCE откроется в новой вкладке браузера.

В новой вкладке откроется веб-интерфейс VCE.

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

После этого веб-интерфейс VCE откроется в текущей вкладке браузера. Меню интерфейса корневого NGFW будет свернуто, вернуться к нему можно, кликнув на панель слева.

Также перейти в веб-интерфейс VCE можно из веб-интерфейса Ideco Center. Для этого сначала перейдите из интерфейса Ideco Center в интерфейс корневого NGFW одним из способов, указанных в *статье*.

Пример перехода:

В интерфейсе Ideco Center нажмите на в левом верхнем углу и выберите нужный NGFW. В открывшемся веб-интерфейсе NGFW нажмите на в левом верхнем углу и выберите нужный VCE.

20.3.3 Удаление VCE

Удалить VCE можно, нажав на 20250219090034/docsUTM/.gitbook/assets/delete-icon.png в корневом VCE.

Предупреждение: После удаления VCE все его настройки, журналы и внутренние данные будут безвозвратно утеряны. Восстановить их будет невозможно.

20.4 Кластеризация

Подсказка: Название службы раздела **Кластеризация**: `ideco-cluster-backend`; `ideco-cluster-backup-pusher`.
Список служб для других разделов доступен по *ссылке*.

Подсказка: Для настройки кластеризации требуется активная лицензия с модулем кластеризации. Подробную информацию о лицензировании кластера можете найти в *статье*.

Каждое из двух устройств Ideco NGFW, объединенных в кластер, называется нодой.

Кластер работает в режиме active-passive:

- **Активной** является нода, обрабатывающая трафик в данный момент.
- **Резервная** нода находится в предзагруженном состоянии и непрерывно мониторит состояние активной ноды, а при отсутствии связи с ней переводит текущие задачи обработки трафика на себя.

Предупреждение: В любой момент обрабатывать трафик может только одна из нод.

Сетевое взаимодействие между нодами осуществляется по *Кластерной сети*. Это физический канал, под который на каждой из нод резервируется по одному физическому порту. Веб-сервер активной ноды управляет кластером, а резервная нода постоянно готова принимать данные. При переключении нод пассивная нода полностью прогружается и становится активной.

Если IP-адреса кластера настроены вручную, то он имеет один общий IP на внутреннем интерфейсе и другой общий IP на внешнем интерфейсе. В случае автоматической конфигурации по DHCP адреса будут отличаться в зависимости от ноды.

20.4.1 Процесс синхронизации нод в кластере

- При синхронизации двух NGFW данные активной ноды копируются в резервную ноду. Вся информация на резервной ноде перезаписывается;
- Синхронизация данных происходит автоматически в фоновом режиме;
- Автоматические бэкапы отключены на резервной ноде. Все бэкапы с активной ноды передаются на резервную в момент обмена данными и заменяют те бэкапы, которые там присутствовали ранее.

Внимание: Для корректной работы кластера необходимо постоянное наличие связи между нодами. Для моментального переключения ноды следует соединять прямым линком, не используя мост или коммутатор.

Обмен данными между нодами кластера происходит раз в три минуты. Все несинхронизированные пользовательские изменения настроек и бэкапы **могут быть потеряны, если с момента внесения изменений на активной ноде до переключения нод не было обмена данными**.

20.4.2 Особенности работы кластера

Особенности работы кластера с синхронизацией сессий:

- При переключении на резервную ноду изменения с активной ноды применяются к etcd, бэкапам, ClickHouse на резервной ноде. Изменения не применяются к логам journald и мониторинга, а также аппаратным данным;
- Время переключения нод - 15 сек. В 18 версии при пропадании линка между нодами переключение происходит моментально;
- При переключении происходит синхронизация данных приложений с активной ноды на резервную;
- Нода, на которой есть внесенные администратором изменения, будет оставаться активной до синхронизации данных с резервной нодой;
- При отключении линка локальной/внешней сети активная нода становится резервной, резервная становится активной;
- При отключении линка локальной/внешней сети активной становится нода, у которой больше активных линков. Резервной - нода, у которой меньше активных линков;
- При одинаковом количестве отключенных линков на обеих нодах активной становится нода, у которой было меньше всего деградации сети (разрывов). Резервной - нода, у которой было больше всего разрывов;
- При одинаковом количестве отключенных/включенных линков на обеих нодах и одинаковом количестве разрывов сети активной становится нода, у которой больше uptime (запущена раньше). Резервной - нода, у которой uptime меньше (запущена позднее);
- При офлайн-обновлении кластера с синхронизацией сессий обновления баз **Предотвращения вторжений**, **Контент-фильтра** и **Антивирусов веб-трафика** не синхронизируются, каждая нода обновляется отдельно. Вторая нода обновится после того, как станет активной.

Особенности работы кластера без синхронизации сессий:

- При переключении на резервную ноду синхронизируются все данные с диска активной ноды (синхронизация осуществляется за счет копирования файлов в файловой системе);
- Время переключения нод - 15 сек + загрузка резервной ноды;
- При переключении нод не синхронизируются логи мониторинга и journald, а также аппаратные данные.

Особенности работы с бэкапами при кластеризации:

- Невозможно полное восстановление из бэкапов. При этом можно создать резервную копию и после разрушения кластера восстановить копию на ноде, которая была активной;
- На активной ноде доступно **Мгновенное восстановление из бэкапа**. Восстанавливаются все настройки, кроме изменений в списке пользователей и отчетах. Данные на второй ноде также придут в соответствие с восстановленными настройками после синхронизации нод.

20.4.3 Возможные проблемы при работе двух Ideco NGFW в кластере

- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено;
- Два NGFW с разными версиями не синхронизируются;
- При обновлении Ideco NGFW в кластере сначала обновится активная нода, затем резервная нода с младшей версией принудительно станет активной для обновления до версии активной ноды.
- При различных размерах жестких дисков могут возникнуть проблемы синхронизации из-за нехватки места;
- Если у провайдера имеется привязка по MAC-адресу, то при переключении нод будет отсутствовать доступ в интернет;

- Если с момента создания бэкапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения этот бэкап будет потерян;
- Если с момента мгновенного восстановления из бэкапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения вторая нода окажется в состоянии до восстановления.

Внимание: Не рекомендуем создавать VCE на нодах кластера. Если в кластере на одной из нод был создан *VCE*, со второй нодой будут синхронизироваться только данные таблицы раздела **Управление сервером -> VCE**. После переключения на пассивной ноде будет создан VCE с тем же именем и комментарием, но внутренние настройки созданных на первой ноде VCE (администраторы, сетевые интерфейсы, политики безопасности и т. д.) не перенесутся.

20.4.4 Настройка кластера

Если на момент создания кластера у вас уже есть настроенный Ideco NGFW, рекомендуем выбрать его в качестве активной ноды. Все настройки резервной ноды в процессе создания кластера будут удалены.

Требования

Для создания кластера необходимо соблюдение следующих требований:

- В кластере может быть только две ноды Ideco NGFW;
- Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки;
- Количество **используемых** физических сетевых карт на обоих серверах должно совпадать. В ином случае создать кластер нельзя. При этом само наличие дополнительных физических сетевых карт на нодах на создание кластера никак не влияет;
- Сетевые карты для использования в кластере желательно соединять напрямую, т.к. на основе линка происходит ускоренное переключение нод, поэтому не рекомендуется использовать коммутаторы для кластерной сети. Как минимум сеть должна быть изолирована;
- Не рекомендуется объединять в кластер георазпределенные ноды;
- При работе NGFW на гипервизорах используйте средства отказоустойчивости гипервизора.

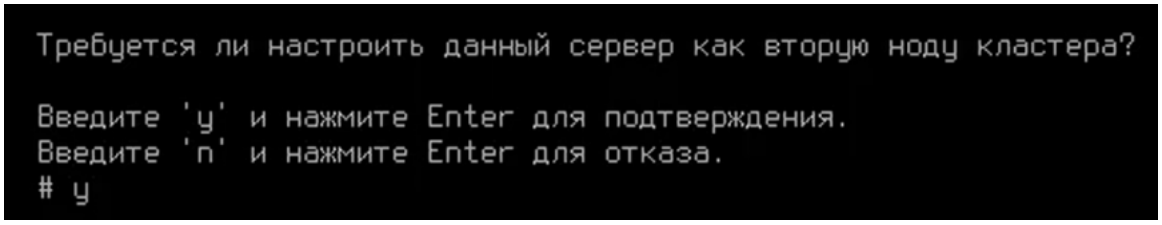
Предупреждение:

- Интерфейсы для создания кластерной сети на каждом Ideco NGFW должны быть в одном сегменте локальной сети, в котором нет других устройств. Не используйте в качестве кластерной сети общедоступную сеть, используемую для передачи стороннего трафика. Обмен данными между нодами не защищен от подмены и прослушивания.
- При настройке кластеризации с использованием гипервизора убедитесь, что сетевая карта, предназначенная для связи между нодами, подключена к изолированной IPv6 сети.
- Запрещено добавлять сетевые интерфейсы, но РАЗРЕШЕНО отключать и редактировать. Удаление сетевого интерфейса, использующегося для связи между нодами, разрушит кластер.

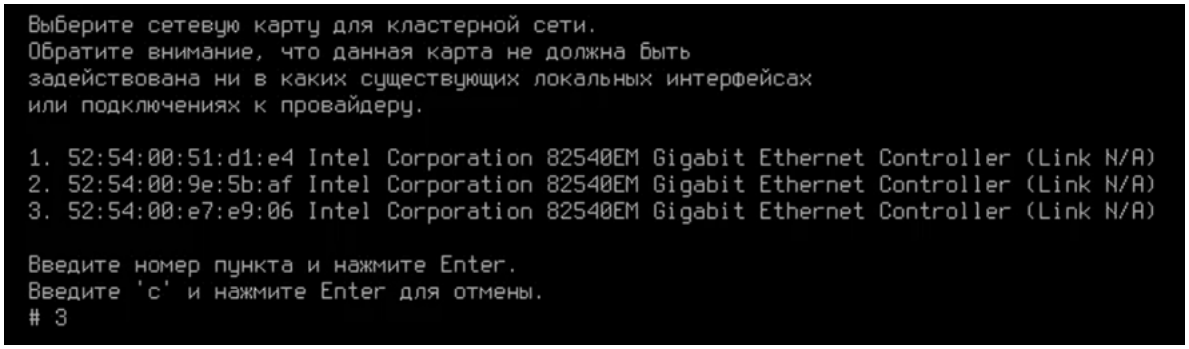
Шаг 1 - Конфигурация резервной ноды

Если только установили сервер Ideco NGFW:

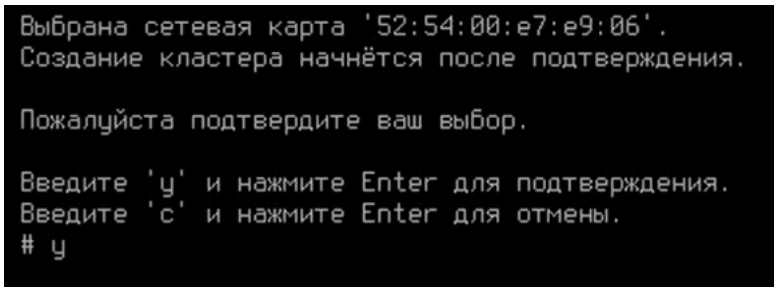
1. При входе в локальное меню резервной ноды, увидев следующее сообщение, введите **y** и нажмите **Enter**:



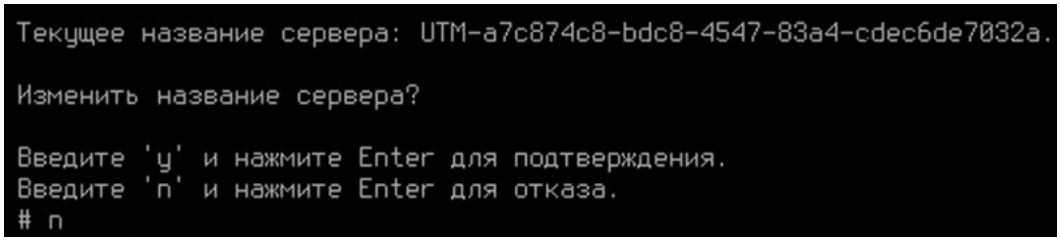
2. Выберите сетевую карту:



3. Подтвердите создание кластера, введя **y** и нажав **Enter**:



4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *Изменить название сервера?*, появится надпись с предложением ввести новое название.
Допустимое количество символов в названии - от 2 до 62:



После ввода нового названия нажмите **Enter** для продолжения.

5. Появится сообщение, что процесс создания кластера запущен:

```
Процесс создания кластера запущен.
Зайдите в web-интерфейс первой ноды и запустите настройку кластера.
Для этого выделяется 3600 секунд. После того, как настройка кластера на
первой ноде будет завершена, данная нода будет перезагружена автоматически.
Для отмены процесса создания кластера нажмите Ctrl+C.

Ожидание завершения настройки кластера, 3599 секунд до отмены.
```

Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Если создаете резервную ноду из уже установленного сервера Ideco NGFW с лицензией и доступом в интернет:

1. Перейдите в локальное меню;

2. Выберите пункт **Управление кластером**. Подтвердите создание кластера, введя **y** и нажав **Enter**:

```
Управление сервером

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

Введите номер пункта и нажмите Enter.
# 15

Кластер не настроен. Создать его?

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

Если на ноде нет свободных сетевых карт, создание кластера будет недоступно.
Если кластер на ноде уже настроен, при выборе пункта *Управление кластером* будет доступно только его разрушение.

3. Выберите свободную физическую сетевую карту для создания кластерной сети и подтвердите выбор:

```
Выберите сетевую карту для кластерной сети.
Обратите внимание, что данная карта не должна быть
задействована ни в каких существующих локальных интерфейсах
или подключениях к провайдеру.

1. 52:54:00:39:8e:e8 Intel Corporation 82540EM Gigabit Ethernet Controller (Link N/A)
2. 52:54:00:b3:01:ea Intel Corporation 82540EM Gigabit Ethernet Controller (Link N/A)

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

4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *«Изменить название сервера?»* появится надпись с предложением ввести новое название.
Допустимое количество символов в названии - от 2 до 42:

```
Текущее название сервера: UTM-7a8af3d1-ffec-470b-b30f-a97f7985aee7.

Изменить название сервера?

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

После ввода нового названия нажмите **Enter** для продолжения.

5. Появится сообщение, что процесс создания кластера запущен:

```
Процесс создания кластера запущен.
Зайдите в web-интерфейс первой ноды и запустите настройку кластера.
Для этого выделяется 3600 секунд. После того, как настройка кластера на
первой ноде будет завершена, данная нода будет перезагружена автоматически.
Для отмены процесса создания кластера нажмите Ctrl+C.

Ожидание завершения настройки кластера, 3599 секунд до отмены.
```

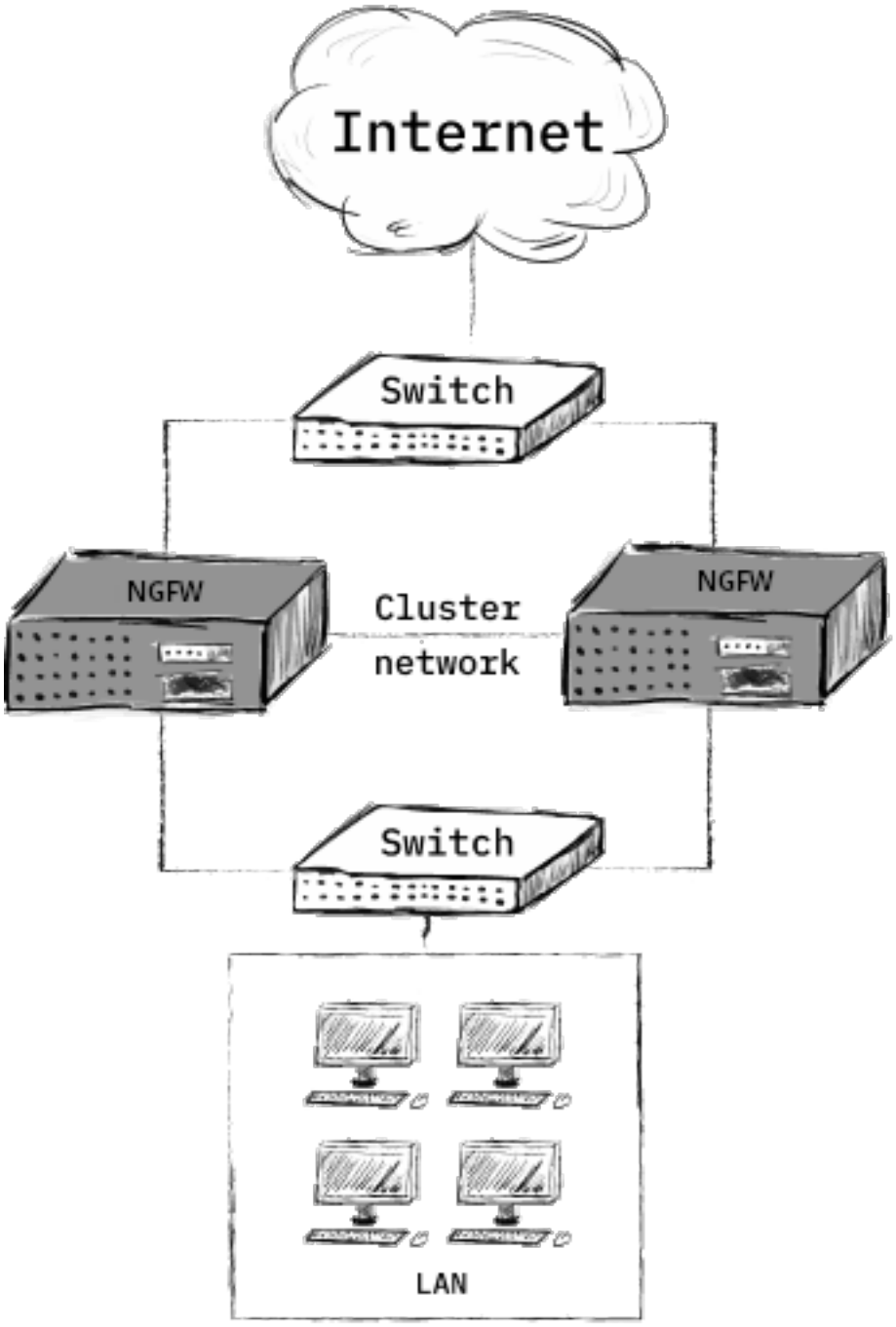
Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Шаг 2 - Конфигурация активной ноды

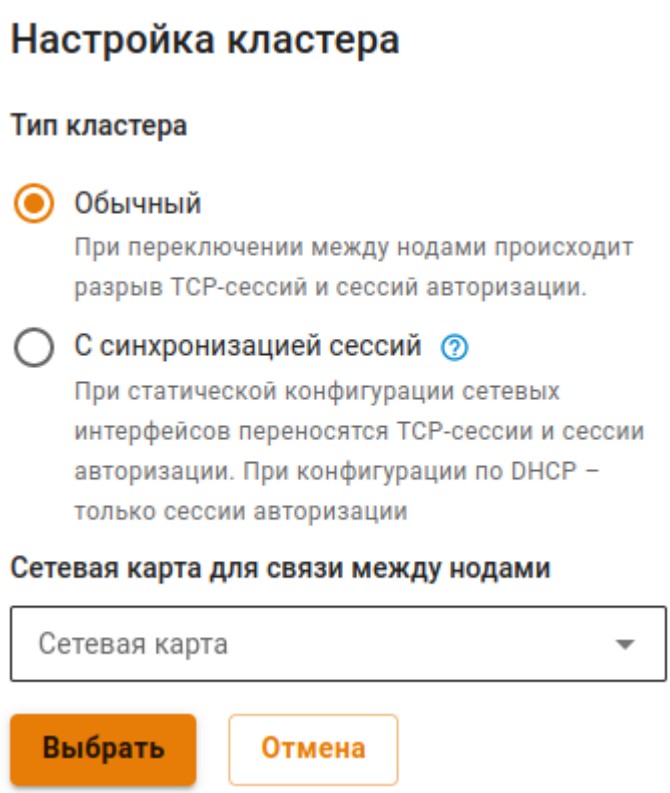
Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW выполните следующие действия:

1. Перейдите в раздел **Управление сервером -> Кластеризация** и нажмите кнопку **Настроить кластер отказоустойчивости**.

2. Подтвердите, что топология сети соответствует схеме:



3. Выберите тип кластера и сетевую карту для соединения между нодами:

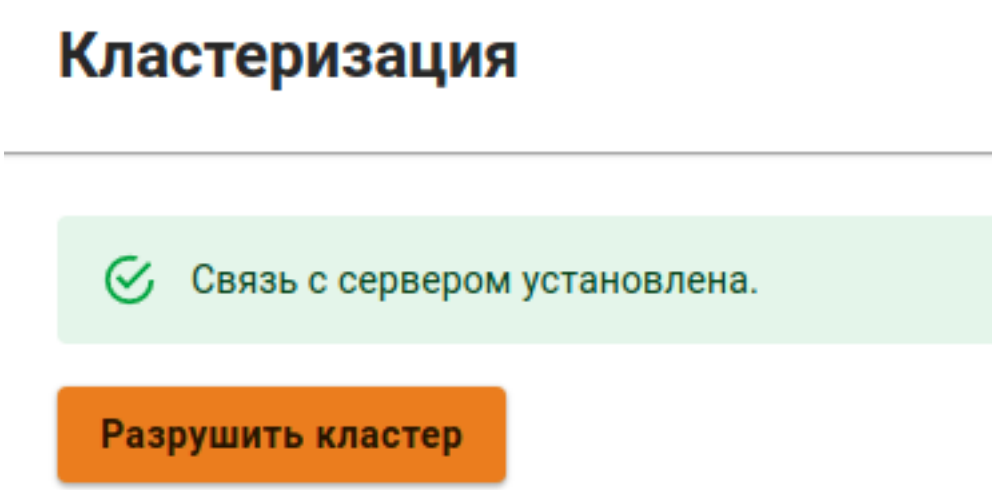


Подсказка: Если был настроен **Обычный** тип кластера, то при переключении между нодами происходит разрыв TCP-сессий пользователей и сессий авторизации.

Если был настроен тип кластера **С синхронизацией сессий**, то при статической конфигурации сетевых интерфейсов все TCP-сессии пользователей и сессии авторизации перенесутся на резервную ноду. При конфигурации по DHCP - перенесутся только сессии авторизации.

4. Сопоставьте сетевые карты. Для этого выберите в каждом столбце по одной сетевой карте и нажмите **Сопоставить**:

5. После применения настроек резервная нода перезагрузится, и в веб-интерфейсе активной ноды отобразится информация о том, что связь с сервером установлена.



Предупреждение: Локальное меню резервной ноды недоступно в NGFW, начиная с версии 16.0.

Изменение названия кластера

Изменить название кластера можно в веб-интерфейсе активной ноды, нажав на кнопку **Редактировать** рядом с названием кластера в левом верхнем углу экрана:

После ввода нового названия нажмите ✓.

Изменение названия сервера

Изменить название сервера можно у активной ноды из веб-интерфейса, нажав кнопку **Редактировать** рядом с названием сервера в левом верхнем углу экрана:

После ввода нового названия нажмите ✓.

Разрушение кластера

Разрушить кластер можно только из локального меню или веб-интерфейса *активной* ноды. При этом она продолжит работать, а вторая нода (резервная) сбросит настройки до состояния только что установленного Ideco NGFW.

Разрушение кластера из локального меню:

1. Выберите пункт локального меню **Управление кластером**, введите **y** и нажмите **Enter**;

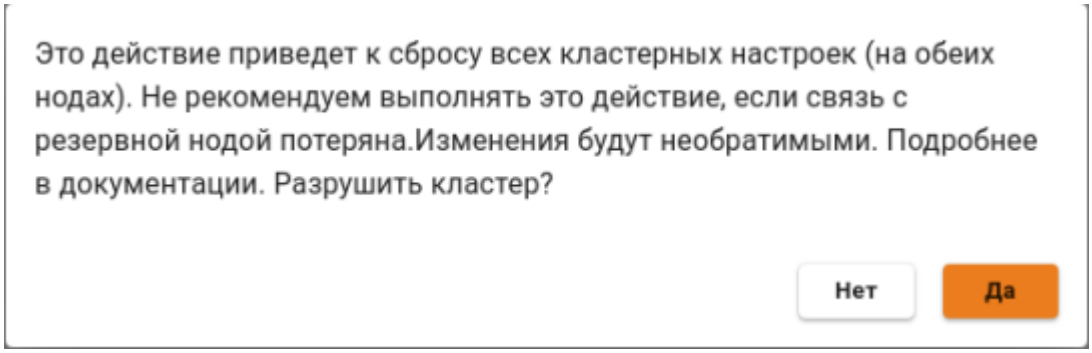
```
Управление сервером

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

Введите номер пункта и нажмите Enter.
# 15

Кластер настроен. Разрушить его?

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

2. Подтвердите выбор.

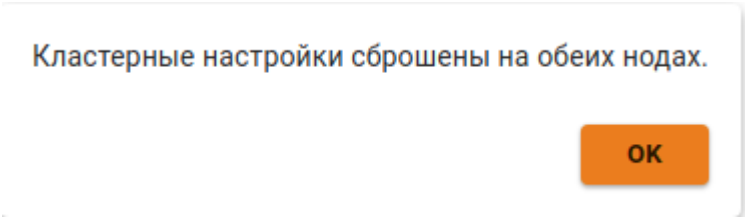
Разрушение кластера из веб-интерфейса:

1. Перейдите в раздел **Управление сервером -> Кластеризация** и нажмите кнопку **Разрушить кластер**.

2. Появится окно с предупреждением:



3. Нажмите **ОК**:



Процедура обновления нод

Чтобы обновить NGFW до последней версии в режиме кластера, выполните действия:

1. Запустите обновление активной ноды - в разделе **Управление сервером -> Автоматическое обновление** нажмите соответствующую кнопку. В процессе обновления произойдет перезагрузка ноды. Резервная нода станет активной, переведя текущие задачи обработки трафика на себя.
Обмен данными между нодами будет остановлен, как только первая нода обновилась и перезагрузилась. Для синхронизации оба устройства должны иметь одну версию системы, идентичную вплоть до номера сборки.

Предупреждение: При офлайн-обновлении кластера с синхронизацией сессий обновления баз **Предотвращения вторжений**, **Контент-фильтра** и **Антивирусов веб-трафика** не синхронизируются, каждая нода обновляется отдельно. Вторая нода обновится после того, как станет активной.

2. Дождитесь, когда активная нода скачает обновление, и запустите его. После завершения обновления кластер вновь будет работоспособен.

Подсказка: Обновление активной ноды кластера будет заблокировано, если она не синхронизирована с резервной нодой или с момента последней синхронизации прошло более 30 минут. В случае блокировки обновлений произойдет переключение нод кластера. Нода с младшей версией сможет обновиться без синхронизации.

20.5 Обновления

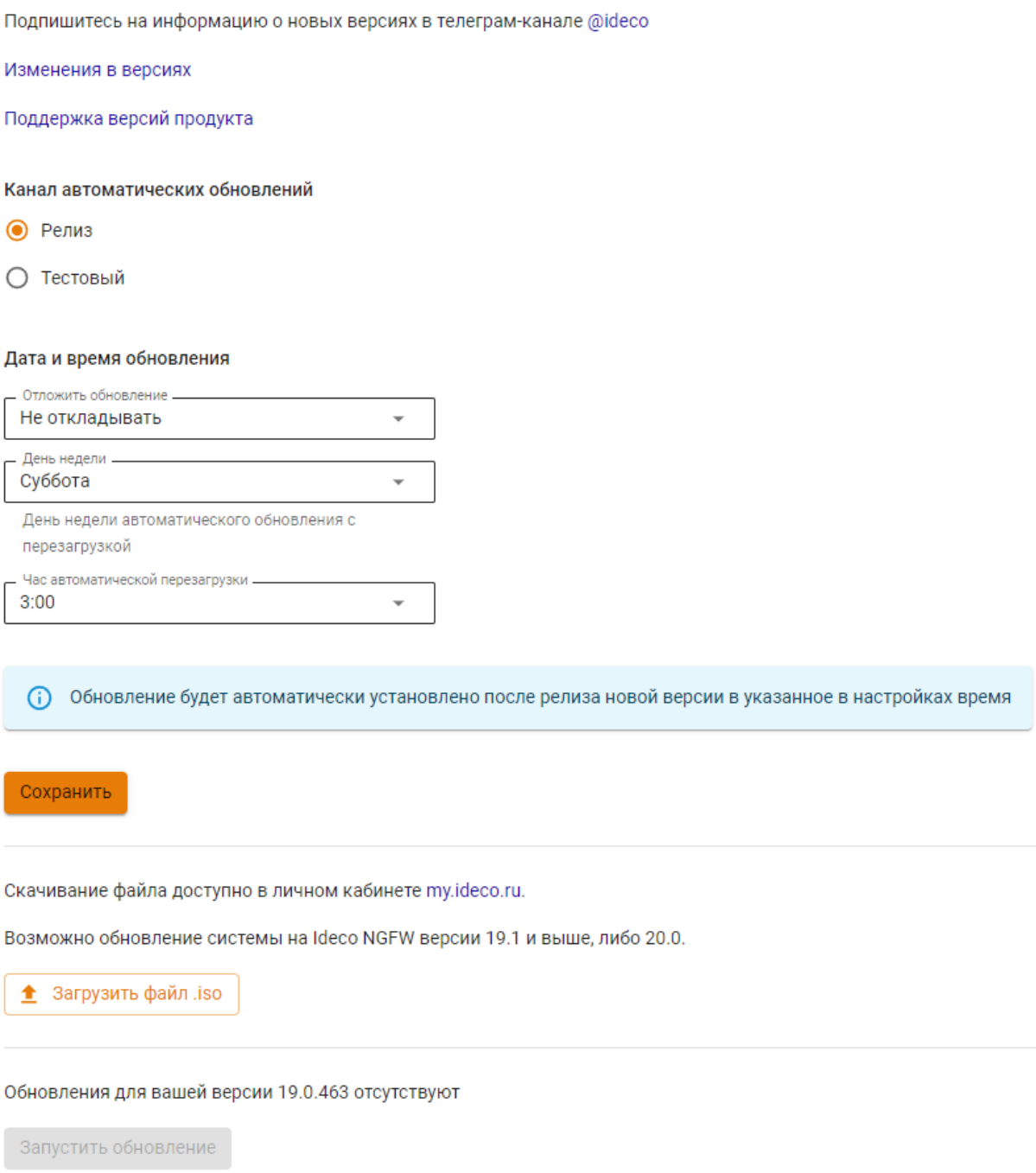
Подсказка: Название службы раздела **Обновления**: `ideco-sysupdate-backend`.
Список служб для других разделов доступен по *ссылке*.

Предупреждение: Для отключения автоматического обновления Ideco NGFW в строке **Отложить обновление** выберите **Навсегда**.

20.5.1 Система

Обновить систему Ideco NGFW можно как в офлайн-режиме, так и по сети. Отрегулировать режим обновления можно в разделе **Управление сервером -> Лицензия**.

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

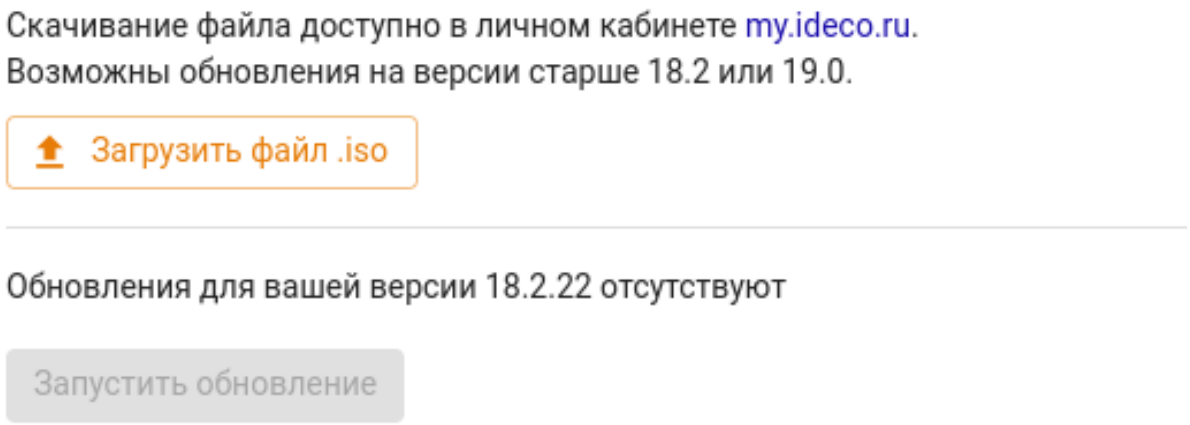


Расшифровка полей:

- **Канал обновлений** - пункт **Релиз** позволяет обновляться на стабильно работающие версии. Пункт **Тестовый** позволяет быстрее обновляться как на релизные версии, так и на последние бета-версии продукта во время коротких периодов бета-тестирования новых мажорных версий. По умолчанию выбран пункт **Релиз**;
- **Отложить обновления** - время, на которое будет отложено обновление (Максимальный срок - шесть месяцев с даты релиза последней версии, до которой доступно обновление);
- **День недели** - день недели запуска автоматического обновления;
- **Час автоматической перезагрузки** - час запуска автоматического обновления;
- **Загрузить файл .iso** - позволяет обновить Ideco NGFW путем загрузки ISO-образа необходимой версии;

- **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

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



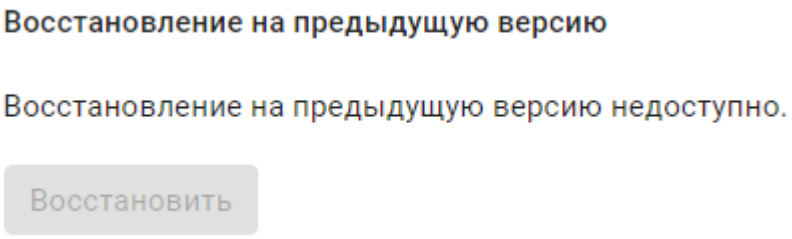
Подсказка: Кнопка принудительного обновления активна, когда обновление уже скачано, и только применяет его, инициировать скачивание нельзя.

После принудительного обновления потребуется полная перезагрузка сервера.

После проведения процедуры обновления новая версия будет отображаться в верхнем левом углу веб-интерфейса NGFW.

Обновить серверы Ideco NGFW, подключенные к центральной консоли, можно через Ideco Center. Для этого нужно перейти в интерфейс NGFW одним из способов, указанных в разделе *Ideco Center*.

Восстановление на предыдущую версию



Кнопка **Восстановить** позволяет вернуться к предыдущей версии NGFW. Система будет перезагружена, при этом текущие настройки будут потеряны. После восстановления отложите автоматическое обновление.

Если в **Ideco NGFW** настроен кластер, то в веб-интерфейсе будет отсутствовать пункт **Восстановление на предыдущую версию**.

Предупреждение: При восстановлении на предыдущую версию данные перенесены не будут. Сохраните информацию на внешнем носителе.

Процесс выхода релизов в каналы обновлений

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

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

Особенности обновления NGFW

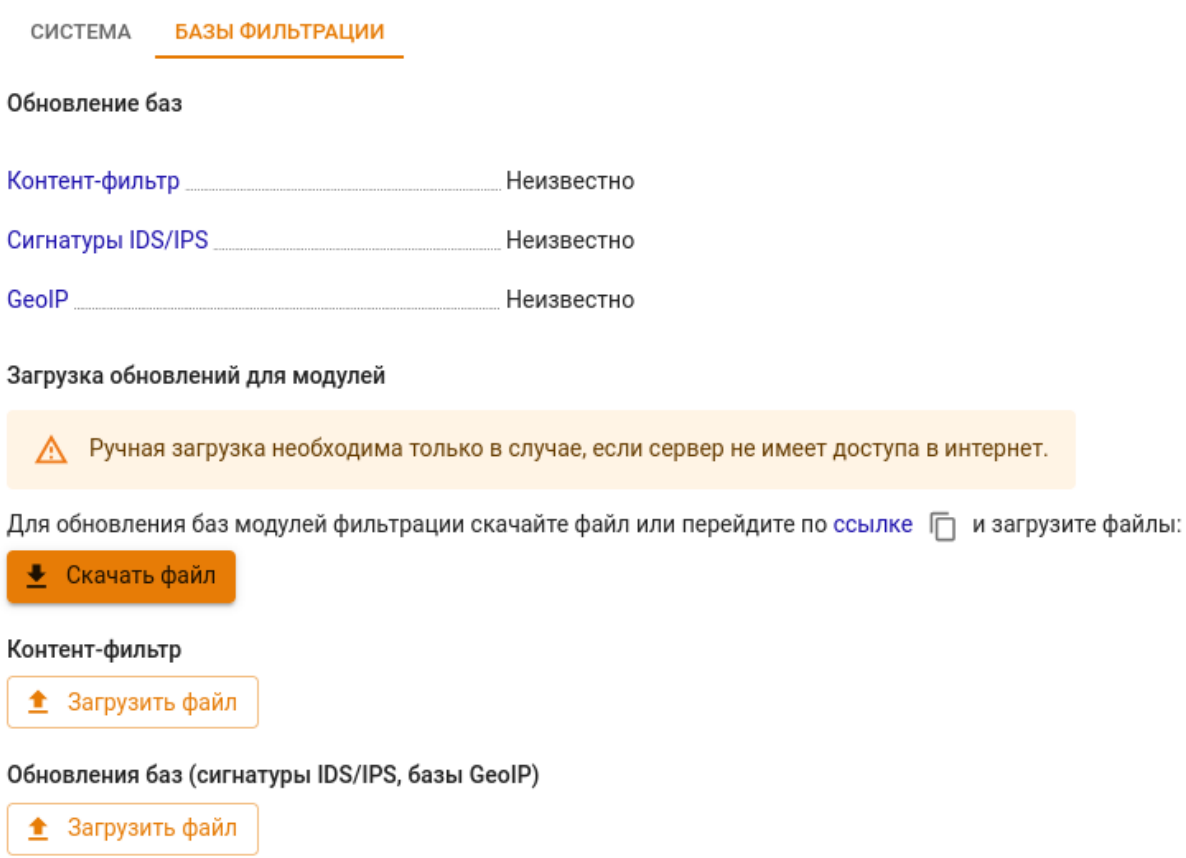
- Обновление будет автоматически установлено в указанное в настройках время после релиза новой версии;
- Обновления можно отложить на срок до шести месяцев или навсегда. Если отложить обновление на определенный срок, то период будет отсчитываться от **даты релиза** последнего доступного обновления и корректироваться в соответствии с указанным для обновления днем недели;
- Даты релизов можно посмотреть на сайте или в документации в разделе Changelog;
- Номер мажорной версии NGFW - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7);
- Автоматическое обновление Ideco NGFW на следующую мажорную версию возможно только после обновления до последней выпущенной в релиз минорной версии. Например, UTM 14.2 можно обновить до версии 14.10, а затем - до версии 15.7.

Подсказка: 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.

Особенности обновления кластера

- Если активная нода кластера не синхронизирована с резервной или с момента последней синхронизации прошло более 30 минут, ее обновления будут заблокированы. Произойдет переключение нод кластера. Нода с младшей версией сможет обновиться без синхронизации;
- При офлайн-обновлении кластера с синхронизацией сессий обновления баз **Предотвращения вторжений**, **Контент-фильтра** и **Антивирусов веб-трафика** не синхронизируются, каждая нода обновляется отдельно. Вторая нода обновится после того, как станет активной.

20.5.2 Базы фильтрации



На вкладке доступны обновления баз модулей фильтрации Ideco NGFW - баз **Контент-фильтра** и модуля **Предотвращения вторжений**, а также баз соответствия подсетей и стран (GeoIP).

Подсказка: Ручная загрузка необходима только в случае, если сервер не имеет доступа в интернет, а в разделе **Управление сервером -> Лицензия** выбран способ обновления **Ручная загрузка**.

Чтобы загрузить на Ideco NGFW файлы обновления баз, скачайте их в личном кабинете MY.IDECO одним из способов:

1. В интерфейсе Ideco NGFW в разделе **Управление сервером -> Обновления** скачайте файл или перейдите по ссылке и загрузите файлы:

2. В интерфейсе MY.IDECO напротив названия сервера нажмите и вставьте ссылку, скопированную в разделе **Обновления -> Базы фильтрации**, в открывшуюся форму. Скачайте файлы.

В веб-интерфейс Ideco NGFW перейдите в раздел **Управление сервером -> Обновления -> Базы фильтрации** и загрузите скачанные файлы, нажав на соответствующие кнопки.

Внимание: Базы фильтрации Ideco NGFW могут меняться ежедневно, поэтому при ручной загрузке обновляйте их как можно чаще.

20.6 Бэкапы

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

Подсказка: Название служб раздела **Бэкапы**: `ideco-backup-backend`; `ideco-backup-create`; `ideco-backup-restore`; `ideco-backup-rotate`.
Список служб для других разделов доступен по *ссылке*.

В NGFW создается только полный бэкап, который включают в себя все настройки, созданные администратором в веб-интерфейсе.

Бэкапы не включают:

- Системный журнал;
- Почту;
- Статистику web-трафика и другие отчеты;
- Любые кешируемые данные, базы антивирусов, правила IPS и т. п.;
- Настройки созданных *VCE*;
- Любые данные, генерируемые в процессе работы системы автоматически.

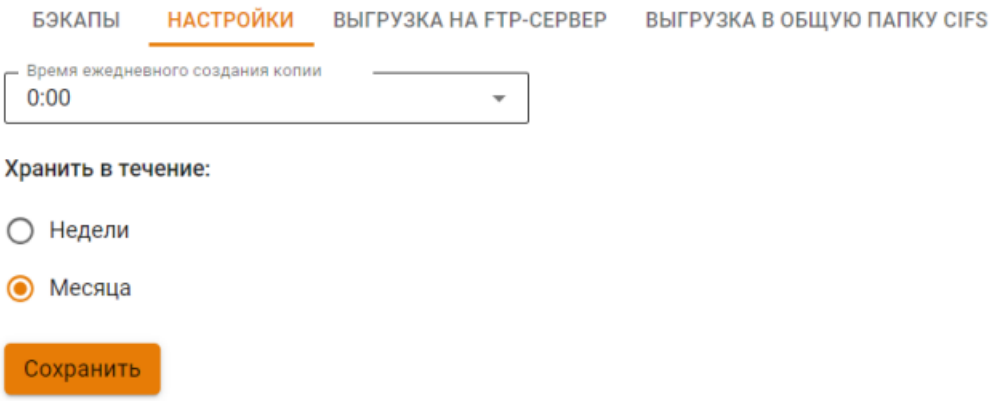
Подсказка: В бэкап корневого VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте бэкап отдельно по корневому VCE и по каждому

из дочерних VCE.

В NGFW бэкап создается как автоматически, так и вручную.

20.6.1 Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в раздел **Управление сервером -> Бэкапы -> Настройки**:



Установите время ежедневного создания и продолжительность хранения бэкапа на локальном жестком диске. При настройке выгрузки на сетевое файловое хранилище автоматический бэкап будет также дублироваться туда.

- **Время ежедневного создания копии** - укажите в настройках час (рекомендуется выбирать ночное время для создания бэкапа);
- **Хранить в течение** - хранить бэкапы на локальном жестком диске можно в течение недели или месяца.

Подсказка: Рекомендуется хранить бэкапы не только на локальном жестком диске, но и на внешних носителях. NGFW предоставляет возможность выгружать бэкапы:

- на сетевое файловое хранилище по протоколу FTP;
- на сетевое файловое хранилище по протоколу NetBIOS (CIFS);
- на ПК через кнопку **Скачать** в таблице бэкапов ( ) для переноса с сервера на иной внешний носитель вручную.

Бэкапы на удаленное файловое хранилище по протоколу FTP

Ключевые параметры, необходимые для настройки бэкапа на FTP-сервер, описаны в таблице:

Параметр	Описание
Адрес сервера	IP-адрес удаленного FTP-сервера, на котором будут размещаться бэкапы
Логин	Имя пользователя для авторизации на FTP-сервере
Пароль	Пароль для авторизации на FTP-сервере
Путь к каталогу	Каталог, в который будут записываться бэкапы

Бэкапы на сетевое файловое хранилище по протоколу NetBIOS (CIFS)

Ключевые параметры, необходимые для настройки бэкапа на NetBIOS-сервер, описаны в таблице:

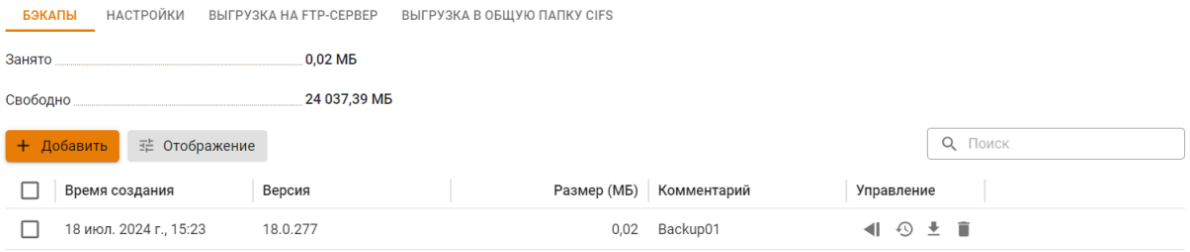
Параметр	Описание
Адрес сервера	IP-адрес удаленного NetBIOS-сервера, на котором будут размещаться бэкапы
Логин	Имя пользователя для авторизации на сетевом ресурсе Windows
Пароль	Пароль для авторизации на сетевом ресурсе Windows
Путь к каталогу	Каталог, в который будут записываться бэкапы

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

20.6.2 Ручное создание бэкапа

Через веб-интерфейс

Для создания бэкапа через интерфейс Ideco NGFW перейдите в **Управление сервером -> Бэкапы -> Бэкапы** и нажмите **Добавить -> Создать**. Введите комментарий и нажмите **Добавить** или нажмите **Создать бэкап** в правом верхнем углу веб-интерфейса. Новый бэкап появится в таблице:



Через локальное меню

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

1. Выберите пункт **10** и нажмите **Enter**.

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

Пример создания бэкапа через локальное меню приведен на скриншоте ниже:

```
Управление сервером

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

Введите номер пункта и нажмите Enter.
# 10

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

Введите 'c' и нажмите Enter для отмены.
# Backup1
Создание бэкапа, пожалуйста подождите...
Бэкап создан успешно.
```

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

20.6.3 Восстановление конфигурации из бэкапа

В NGFW восстановление из бэкапа возможно полное и мгновенное.

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

При выполнении мгновенного восстановления бэкап применятся без перезагрузки. При этом не сохраняются:

- Счетчики квот;
- Системный журнал.

Предупреждение: При восстановлении системы из резервной копии информация о лицензии не будет восстановлена, поскольку это может привести к использованию устаревшей лицензии.

После завершения процесса восстановления Ideco NGFW автоматически отправит запрос в личный кабинет для обновления лицензии. Если используется офлайн-лицензия, ее необходимо загрузить самостоятельно.

Если резервное копирование используется для переноса настроек с одного сервера на другой, выполните «перепривязку» лицензии. Подробную информацию можно найти в статье *Перенос данных и настроек на другой сервер*.

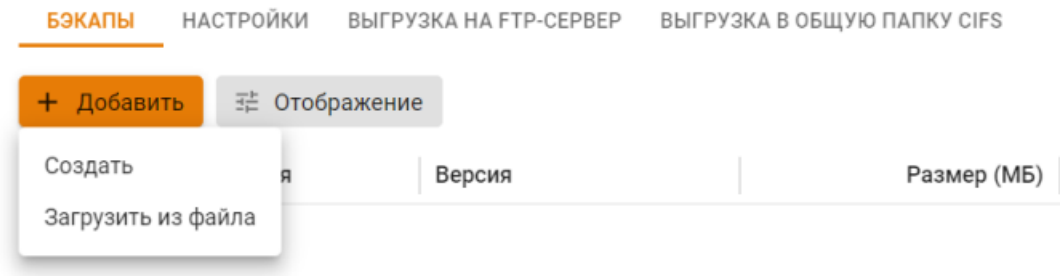
Подсказка: Полное восстановление возможно либо на текущую версию, либо на предыдущую мажорную версию. Например, на версии 17 возможно полное восстановление бэкапа версии 16 или версии 17.

Мгновенное восстановление возможно только для бэкапа версии, полностью совпадающей с установленной на сервере.

Через веб-интерфейс

Перейдите в раздел **Управление сервером -> Бэкапы -> Бэкапы** и нажмите кнопку **Полное восстановление** ( ) или **Мгновенное восстановление** ( ) в столбце **Управление**.

Также можно загрузить бэкап из файла. Например, в случае переноса с другого сервера. Для восстановления конфигураций бэкапа, который находится на внешнем носителе, перейдите на **Управление сервером -> Бэкапы -> вкладка Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

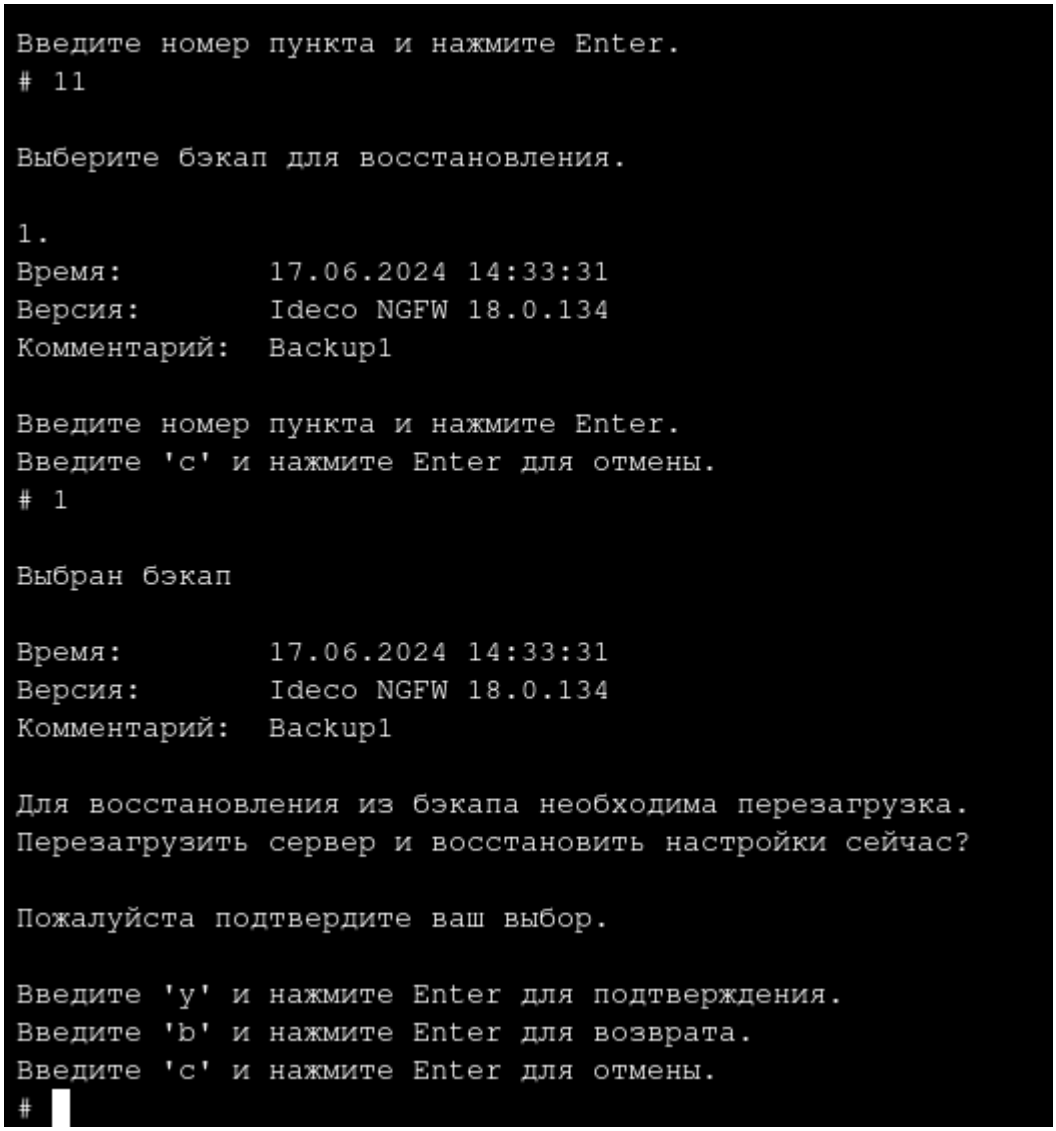
   - **11** - восстановятся все настройки и перезагрузится сервер;
   - **12** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

     Нажмите **Enter**.

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

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

Пример восстановления из бэкапа через локальное меню:



Подсказка: Чтобы перенести установленный Ideco NGFW с одного сервера на другой с сохранением всех настроек, воспользуйтесь статьей *Перенос данных и настроек на другой сервер*.

Предупреждение: Если на Ideco NGFW настроен кластер, то перед работой с бэкапами нужно ознакомиться с особенностями работы бэкапов:

- Невозможно полное восстановление из бэкапов. При этом можно создать резервную копию и после разрушения кластера восстановить копию на ноде, которая была активной;
- На активной ноде доступно **Мгновенное восстановление из бэкапа**. Восстанавливаются все настройки, кроме изменений в списке пользователей и отчетах. Данные на второй ноде также придут в соответствие с восстановленными настройками после синхронизации нод.

20.7 Терминал

Предупреждение: Используйте терминал только для диагностики. Воздержитесь от команд, изменяющих файлы. Система рассчитана на настройку только через веб-интерфейс. Компания «Айдеко» не несет ответственности за негативные последствия работы с Ideco NGFW из терминала. Техническая поддержка вправе отказать в обслуживании, если окажется, что работа системы была нарушена из-за действий пользователя в терминале.

20.7.1 Основные команды

- **Утилиты сетевой диагностики:** `ping`, `host`, `nslookup`, `tracepath`, `tcpdump`, `arping`, `ss` (аналог `netstat`);
- **Файловый редактор:** `nano`;
- **Просмотр логов:** `journalctl -u <название службы>` (например, `journalctl -u ideco-routing-backend`);
- **Проверка скорости интернета:** `speedtest-cli`;
- **Просмотр ARP-таблицы:** `ip neigh show`;
- **Разблокировка в случае срабатывания защиты от брутфорс-атак:**
  - `fail2ban-client unban --all` - команда используется для снятия всех блокировок;
  - `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса. Укажите нужный IP-адрес в качестве аргумента.
- **Просмотр конфигурации FRR:** `vtysh`.

20.7.2 Таблица служб

Раздел	Имя службы
Файрвол	ideco-nflog;ideco-firewall-backend
Профили контроля приложений	ideco-app-backend; ideco-app-control-nfq
Контент-фильтр	ideco-content-filter-backend
Ограничение скорости	ideco-shaper-backend
Антивирус	ideco-av-backend
Предотвращение вторжений	ideco-suricata-backend; ideco-suricata; ideco-suricata-event-syncer; ideco-suricata-profiles-syncer
Объекты	ideco-alias-backend
Сетевые интерфейсы	ideco-network-backend; ideco-network-nic
Балансировка и резервирование, Маршрутизация	ideco-routing-backend
BGP, OSPF	frr; ideco-routing-backend
Прокси	ideco-proxy-backend; squid
Обратный прокси	ideco-reverse-backend
DNS	ideco-dns-backend; unbound; nsd
DDNS	ideco-dns-backend
DHCP	ideco-dnsmasq
NTP	chronyd
IPsec	ideco-ipsec-backend; strongswan
Ideco Center	ideco-central-console-backend
VCE	ideco-vce-backend
Кластеризация	ideco-cluster-backend; ideco-cluster-backup-pusher
Обновления	ideco-sysupdate-backend

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Раздел	Имя службы
Бэкапы	ideco-backup-backend; ideco-backup-create; ideco-backup-restore; ideco-backup-rotate
Лицензия	ideco-license-backend
VPN-подключения	ideco-accel-l2tp; ideco-accel-pptp; ideco-accel-sstp; ideco-vpn-servers-backend; ideco-vpn-authd; ideco-vpn-dhcp-backend
Авторизация	ideco-auth-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-authd
Active Directory	ideco-ad-backend; ideco-ad-log-collector@<имя домена>
ALD Pro	ideco-ald-rest; ideco-ald-backend
Ideco Client	ideco-agent-backend; ideco-agent-websocket
Syslog	ideco-logs-backend
Обнаружение устройств	ideco-netscan-backend
Web Application Firewall	ideco-waf-backend; ideco-waf-event-syncer
IGMP Proxy	ideco-igmpproxy-backend; ideco-igmpproxy

20.7.3 Примеры использования утилит

Примеры использования утилиты vtysh

Просмотр таблицы маршрутизации:

1. Перейдите в раздел **Управление сервером -> Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра таблицы маршрутизации введите:

```
show ip route
```

Пример вывода утилиты:

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 1.1.1.1/32 [1/0] via 10.10.10.1, Leth1, weight 1, 00:02:32
O   10.10.10.0/24 [110/1] is directly connected, Leth1, weight 1, 00:02:28
C>* 10.10.10.0/24 is directly connected, Leth1, 00:02:33
C>* 10.11.12.0/25 is directly connected, Eeth2, 00:02:33
O>* 10.20.40.0/24 [110/21] via 10.10.10.201, Leth1, weight 1, 00:02:18
S>* 10.128.0.0/16 [1/0] is directly connected, Lvpn0, weight 1, 00:02:32
C>* 169.254.1.0/29 is directly connected, lb_local_in, 00:02:33
C>* 169.254.1.0/29 is directly connected, lb_local_out, 00:02:33
C>* 169.254.1.4/32 is directly connected, Lvpn0, 00:02:33
C>* 169.254.254.254/32 is directly connected, lo, 00:02:33
```

Полезная информация:

- Не все маршруты могут быть выгружены в ядро, поэтому при просмотре таблицы маршрутизации без утилиты `vtsyh` некоторые маршруты могут не отображаться.

Просмотр конфигурации FRR:

1. Перейдите в раздел **Управление сервером -> Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра конфигурации введите:

```
show running-config
```

Пример вывода утилиты:

```
Building configuration...

Current configuration:
!
frr version 8.5.3
frr defaults traditional
hostname bez-nazvaniya-23000007-c6d8-01c2-a572-d68497c66441
no ipv6 forwarding
service integrated-vtysh-config
!
ip route 10.128.0.0/16 Lvpn0
!
interface Leth1
 ip ospf cost 125
exit
!
interface lo
 ip ospf passive
exit
!
router ospf
 ospf router-id 192.168.0.200
 redistribute connected
 redistribute static
 network 172.16.10.0/24 area 0.0.0.200
 default-information originate always
exit
!
ip prefix-list DEFAULT seq 5 deny 0.0.0.0/0
ip prefix-list DEFAULT seq 10 permit 0.0.0.0/0 le 32
!
route-map DEFMAP permit 10
 match ip address prefix-list DEFAULT
exit
!
ip protocol ospf route-map DEFMAP
!
end
```

Просмотр OSPF соседства:

1. Перейдите в раздел **Управление сервером -> Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей OSPF введите:

```
show ip ospf neighbor
```

Пример вывода утилиты:

```
Neighbor ID     Pri State           Up Time         Dead Time Address         ␣
↪Interface                         RXmtL RqstL DBsmL
10.10.10.201      1 Full/DR         6m35s             34.709s 10.10.10.201    ␣
↪Leth1:10.10.10.126                    0     0     0
```

Просмотр BGP соседства:

1. Перейдите в раздел **Управление сервером -> Терминал**.

2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей BGP введите:

```
show ip bgp neighbors
```

Пример вывода утилиты:

```
BGP neighbor is 10.10.10.2, remote AS 123, local AS 123, internal link
  Local Role: undefined
  Remote Role: undefined
 Member of peer-group V4_AS123_10_10_10_2 for session parameters
  BGP version 4, remote router ID 10.11.12.2, local router ID 10.11.12.71
  BGP state = Established, up for 00:00:10
  Last read 00:00:10, Last write 00:00:09
  Hold time is 180 seconds, keepalive interval is 60 seconds
  Configured hold time is 180 seconds, keepalive interval is 60 seconds
  Configured conditional advertisements interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Extended Message: advertised
    AddPath:
      IPv4 Unicast: RX advertised
    Long-lived Graceful Restart: advertised
    Route refresh: advertised and received(new)
    Enhanced Route Refresh: advertised
    Address Family IPv4 Unicast: advertised and received
    Hostname Capability: advertised (name: bez-nazvaniya-5f3323c3-6462-4981-b8a0-
↪2b4397e3448a,domain name: n/a) not received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 0 seconds
      Address families by peer:
        none
  Graceful restart information:
    End-of-RIB send: IPv4 Unicast
    End-of-RIB received:
    Local GR Mode: Helper*

    Remote GR Mode: Helper
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    R bit: False
    N bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
    IPv4 Unicast:
      F bit: False
      End-of-RIB sent: Yes
      End-of-RIB sent after update: Yes
      End-of-RIB received: No
      Timers:
        Configured Stale Path Time(sec): 360
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          3
    Keepalives:             1          2
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  3          6
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  V4_AS123_10_10_10_2 peer-group member
  Update group 1, subgroup 1
  Packet Queue length 0
  NEXT_HOP is always this router
  Community attribute sent to this neighbor(all)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *IMPORT_V4_AS123_10_10_10_2
  Route map for outgoing advertisements is *EXPORT_V4_AS123_10_10_10_2
  12 accepted prefixes

  Connections established 1; dropped 0
  Last reset 00:05:26,  No AFI/SAFI activated for peer
  Internal BGP neighbor may be up to 255 hops away.
Local host: 10.10.10.126, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 38445
Nexthop: 10.10.10.126
Nexthop global: ::
Nexthop local: ::
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Estimated round trip time: 1 ms
Read thread: on  Write thread: on  FD used: 25
```

20.8 Лицензия

Подсказка: Название службы раздела **Лицензия**: `ideco-license-backend`.
Список служб для других разделов доступен по *ссылке*.

В разделе **NGFW** личного кабинета MY.IDECO находится информация о зарегистрированных серверах и имеющихся лицензиях.

Подсказка: Подробнее о видах лицензий в статье *Лицензирование*.

Доступные действия для управления лицензиями:

- регистрация сервера;
- добавление коммерческой или бесплатной лицензии;
- привязка лицензии к серверу;
- просмотр информации об имеющихся лицензиях;
- офлайн-обновление лицензии и баз модулей фильтрации.

20.8.1 Добавление коммерческой (Enterprise) лицензии

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

2. Перейдите в личный кабинет MY.IDECO в раздел **NGFW -> Лицензирование** и нажмите **Добавить коммерческую лицензию**.

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

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

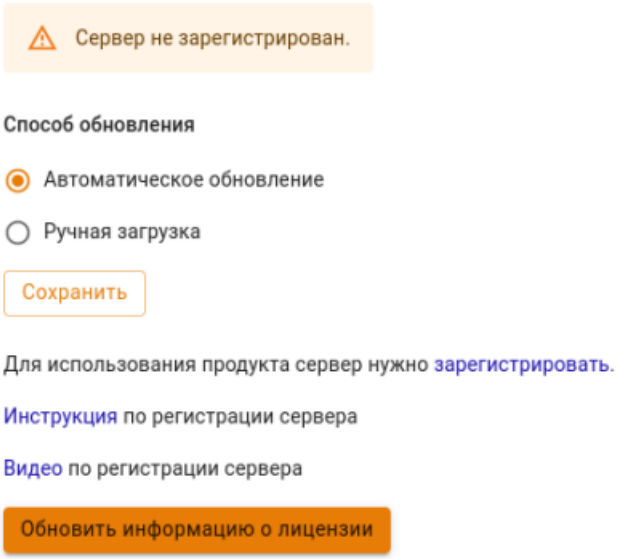
20.8.2 Добавление FREE (бесплатной) лицензии

Для добавления FREE-лицензии нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Свободные лицензии**.

20.8.3 Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн. Онлайн проводится только в MY.IDECO. Офлайн потребует доступ к веб-интерфейсу сервера.

Чтобы выбрать онлайн-привязку, в веб-интерфейсе Ideco NGFW в разделе **Управление сервером -> Лицензия** выберите способ обновления **Автоматическое обновление**, для офлайн-привязки выберите **Ручную загрузку**:



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

- Одна лицензия может быть привязана только к одному серверу;
- Демо-лицензию нельзя привязать к другому серверу;
- Демо-лицензию нельзя повторно получить на одну и ту же инсталляцию сервера;
- При удалении сервера с демо-лицензией также удаляется и лицензия.

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

Онлайн-привязка лицензии

Выберите удобный вариант привязки:

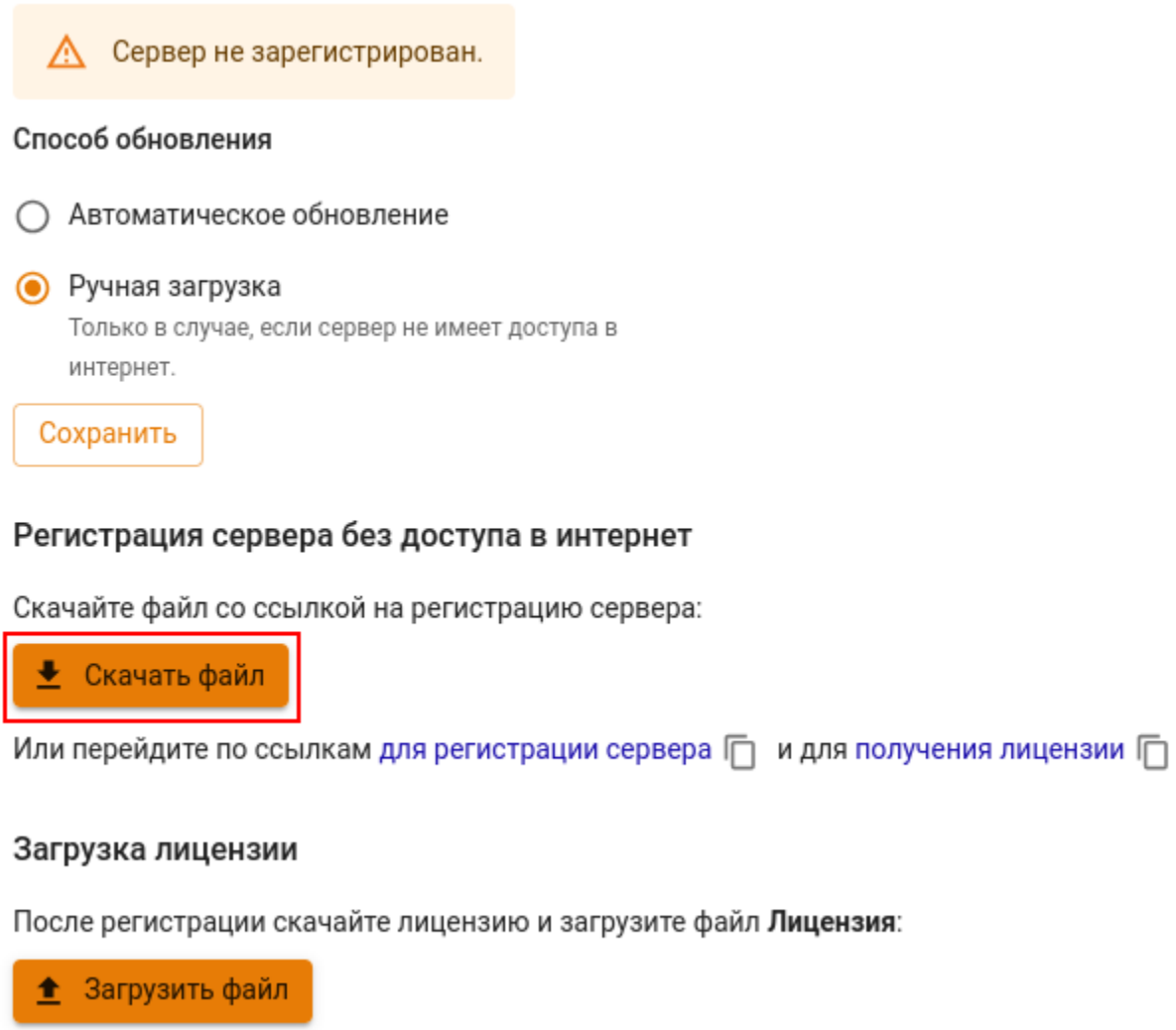
- В MY.IDECO на вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ . Далее в открывшемся окне выберите нужную лицензию и сохраните изменения, нажав **Привязать лицензию**;
- В MY.IDECO на вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

Офлайн-привязка лицензии

Шаги офлайн-регистрации сервера и привязки лицензии:

1. В веб-интерфейсе Ideco NGFW перейдите в раздел **Управление сервером -> Лицензия**, выберите **Ручная загрузка** в качестве способа обновления и нажмите **Сохранить**.

2. Скачайте файл со ссылками на регистрацию сервера и скачивание баз и лицензии, нажав на кнопку, или скопируйте эти ссылки из веб-интерфейса:

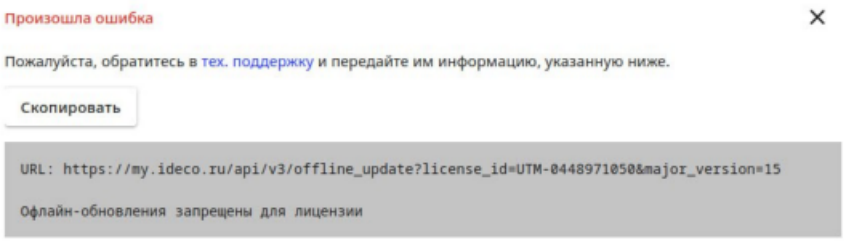


3. На устройстве с доступом к интернету перейдите по ссылке для регистрации сервера, полученной в пункте 2. Сервер автоматически появится в списке серверов в MY.IDECO.

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

5. В личном кабинете MY.IDECO перейдите в раздел **NGFW -> Лицензирование** и нажмите **Привязать лицензию** рядом с нужным сервером.

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

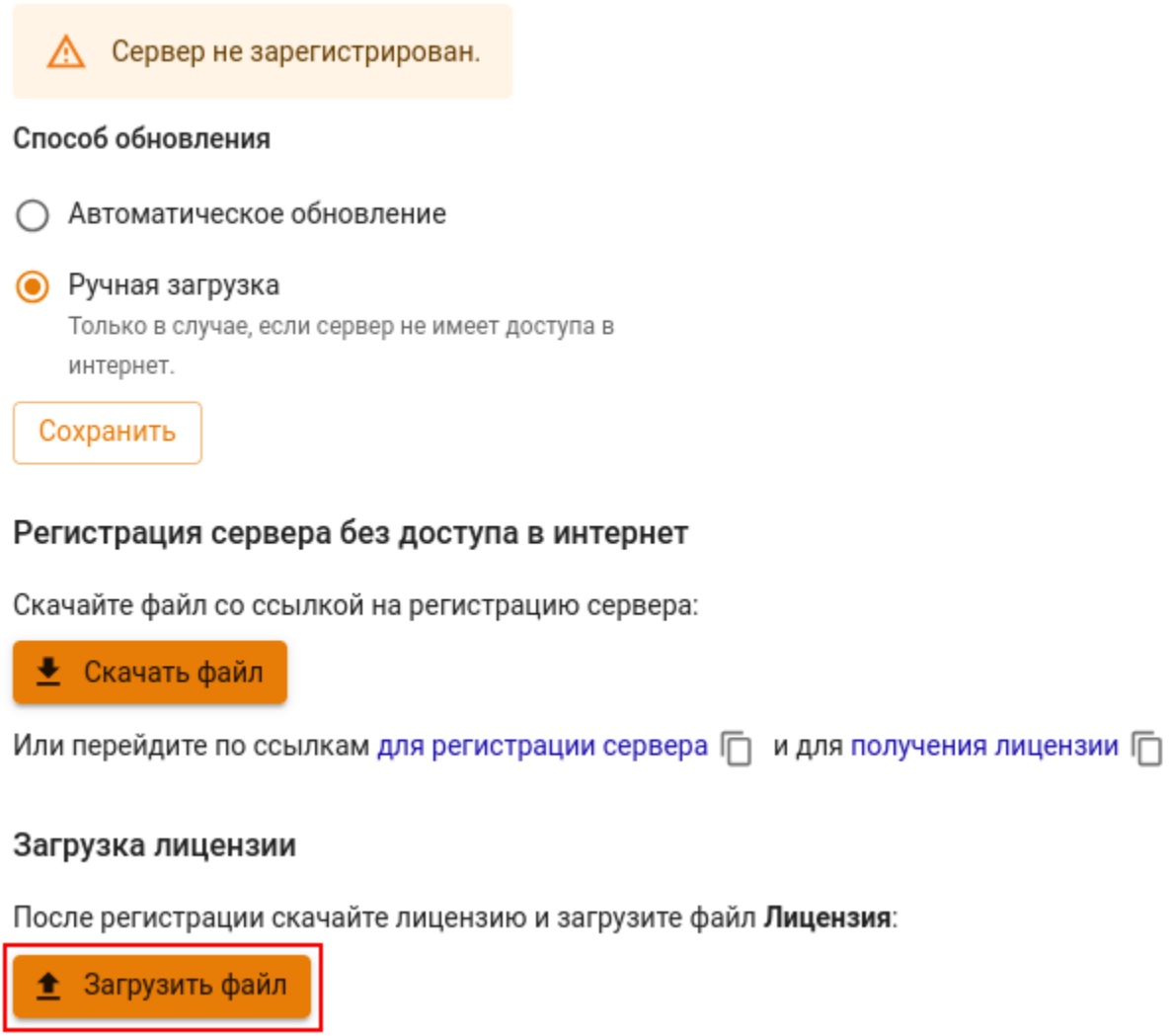


6. Получите файлы лицензии и баз фильтрации одним из способов:

- Перейдите по ссылке для скачивания баз и лицензии из пункта 2 и скачайте файлы, нажав на соответствующие ссылки в открывшейся форме:

- В интерфейсе MY.IDECO напротив названия сервера нажмите и вставьте ссылку, скопированную в разделе **Обновления -> Базы фильтрации**, в открывшуюся форму. Скачайте файлы.

7. В веб-интерфейсе Ideco NGFW перейдите в раздел **Управление сервером -> Лицензия** и загрузите файл с лицензией, скачанный в пункте 6:



20.8.4 Просмотр информации о лицензиях

Посмотреть информацию о модулях и лицензии можно:

- В личном кабинете *MY.IDECO* в разделе **NGFW -> Лицензирование**, нажав на иконку напротив нужного сервера;
- В веб-интерфейсе Ideco NGFW, в разделе **Управление сервером -> Лицензия**.

Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др.

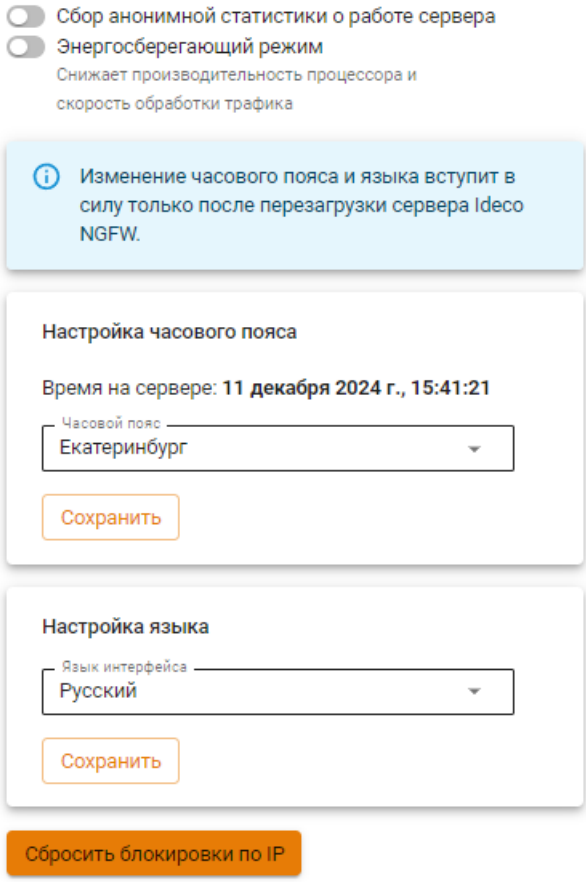
20.9 Дополнительно

20.9.1 Основное

Предупреждение: Изменение часового пояса вступит в силу только после перезагрузки сервера Ideco NGFW.

Подсказка: В интерфейсе *VCE* изменение настроек часового пояса и языка недоступно.

Настройка осуществляется через веб-интерфейс в разделе **Управление сервером -> Дополнительно**.



- **Настройка часового пояса** - установите часовой пояс для корректного сбора логов и статистики;
- **Сбор анонимной статистики о работе сервера** - включение этого параметра разрешает серверу отправлять информацию об используемых модулях. При этом не отправляется информация о пользователях, проходящем через сервер трафике, сетевых интерфейсах и идентификаторах сервера и лицензии;
- **Энергосберегающий режим** - включение этого режима снижает производительность процессора и обработки трафика;
- **Настройка часового пояса** - установите часовой пояс для корректного сбора логов и статистики;
- **Настройка языка** - укажите язык, удобный для работы в веб-интерфейсе;
- **Сбросить блокировки по IP** - используйте для сброса всех заблокированных IP-адресов. Если требуется разблокировать какой-то конкретный IP-адрес, воспользуйтесь командой `fail2ban-client unban <IP-адрес>` в терминале.

21. Почтовый релей

21.1 Основное

Подсказка: Все возможности по фильтрации почтового трафика можно также применить к внутреннему почтовому серверу, опубликовав его через почтовый релей.

Для фильтрации почтового трафика от вирусов, спама и фишинга рекомендуется покупка лицензии на антиспам Касперского.

Для настройки почтового сервера в веб-интерфейсе Ideco NGFW необходимо перейти в меню **Почтовый релей**. В этом разделе находятся все ключевые параметры, влияющие на работу почтовой службы. Все настраиваемые параметры разделены по нескольким категориям. Ниже описан каждый раздел почтового сервера.

Если используется почтовый сервер Ideco NGFW как полноценный сервер с хранением почты, обязательным является хранение почты на дополнительном HDD/SSD-диске. Подключите дополнительный жесткий диск к серверу перед использованием почты.

В настройках почтового сервера можно указать максимальный размер почтового ящика и максимальный размер письма. Подробнее в *статье*.

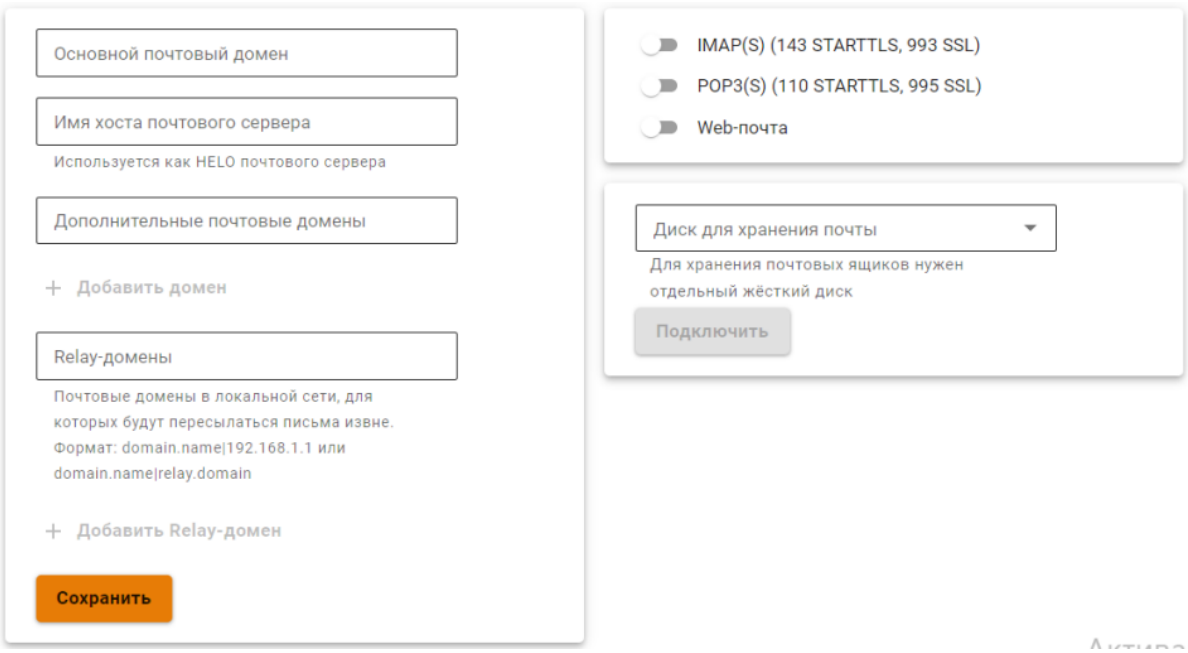
Предупреждение: При настройке *кластера* почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.

21.2 Основные настройки

21.2.1 Основное

Предупреждение: NGFW не поддерживает кириллические почтовые домены.

В разделе **Основные настройки** представлены базовые параметры, необходимые для настройки почтового сервера, почтового релея и веб-почты.



Ideco NGFW можно настроить, как почтовый сервер, почтовый релей или воспользоваться почтовым клиентом NGFW. В зависимости от необходимой функциональности, следуйте соответствующим инструкциям:

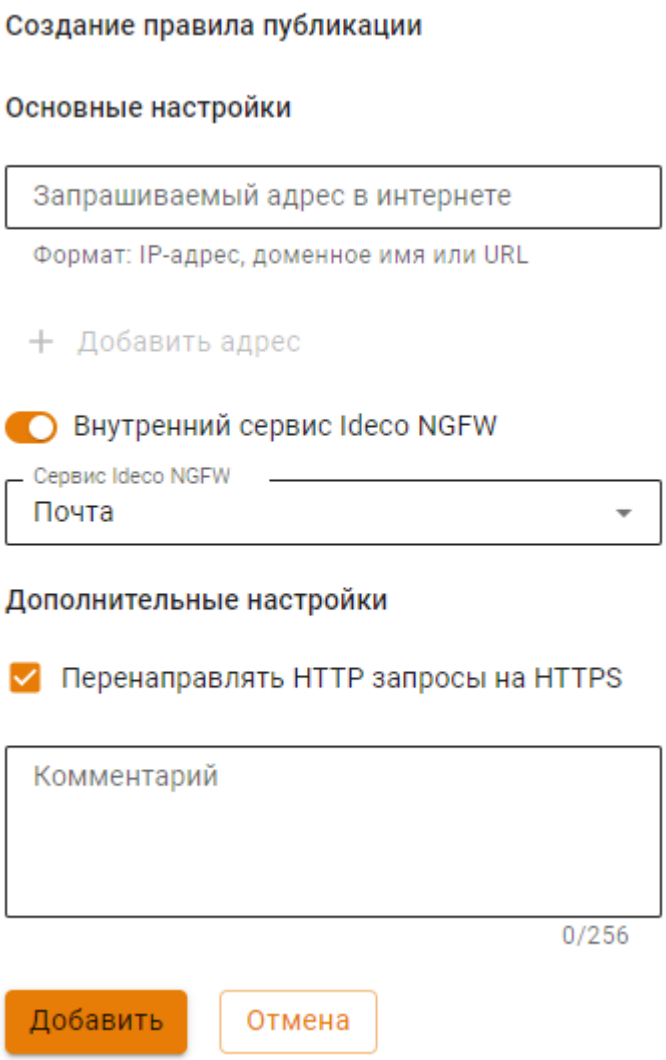
21.2.2 Web-почта

Основное

Подсказка: Перед настройкой веб-почты настройте на Ideco NGFW почтовый сервер.

Для работы веб-почты необходимо активировать опцию **Web-почта** в разделе **Почтовый релей -> Основные настройки** и создать правило публикации в разделе **Сервисы -> Обратный прокси**.

При добавлении правила:



- Включите опцию **Внутренний сервис Ideco NGFW**;
- В качестве сервиса выберите почту;
- В поле **Запрашиваемый адрес в интернете** введите домен, IP-адрес или URL, по которому должна быть доступна веб-почта (например, `webmail.example.com`, `192.168.100.40` или `192.168.100.20/webmail`);
- Нажмите **Добавить**.

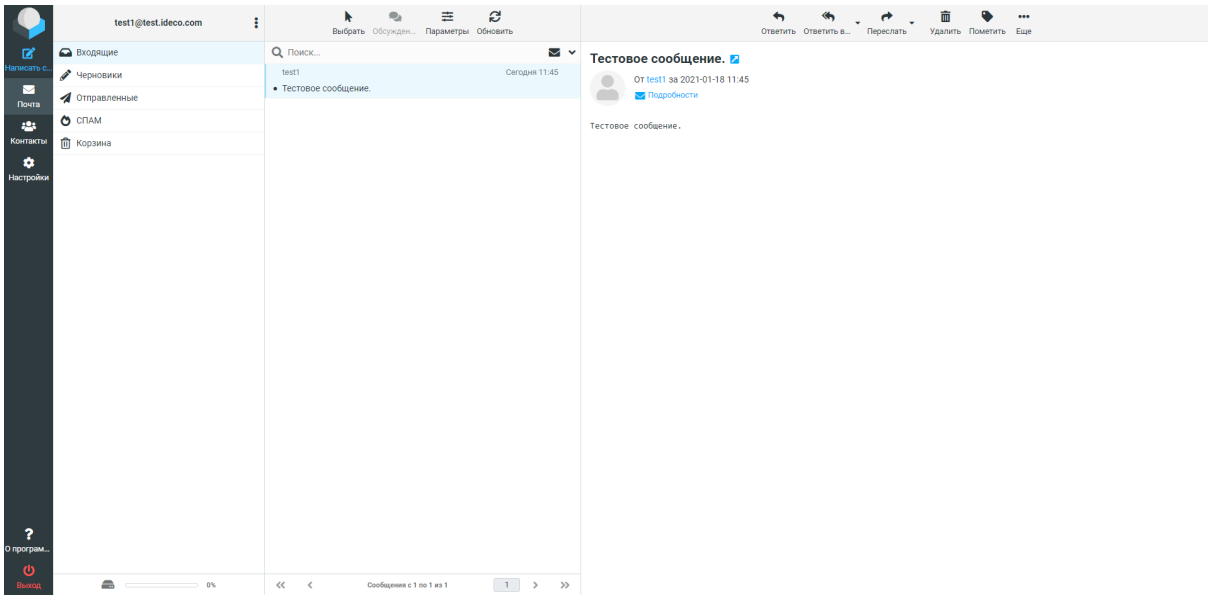
После создания правила из локальной или внешней сети в браузере наберите: `https://<IP-адрес>`, `https://<домен>` или `https://<URL>`.

Предупреждение: Важно:

- Чтобы пользователи имели доступ к веб-почте из внешней сети, в правиле публикации в поле **Запрашиваемый адрес в интернете** необходимо указывать белый IP-адрес или зарегистрированный домен.
- Для подключения обязательно использовать HTTPS.
- С 17 версии Ideco NGFW веб-почта не доступна через `IP-адрес_или_домен_веб-интерфейса:8443/webmail`, т. к. не связана с административным веб-интерфейсом NGFW.

- В открывшейся форме входа в почтовый ящик в качестве логина укажите логин от учетной записи пользователя;
- В качестве пароля всегда прописывается пароль от учетной записи пользователя. **Установить отдельный пароль на почту нельзя.**

При успешном входе в браузере откроется веб-интерфейс почтового ящика пользователя:



Веб-интерфейс встроенного почтового клиента работает с почтовым сервером по протоколу IMAP и обладает возможностями:

- Создание и отправка писем. Поддерживается загрузка множественных вложений;
- Просмотр, удаление, перемещение письма. Управление IMAP-папками ящика;
- Персональная (для конкретного ящика) адресная книга, работающая только в рамках веб-приложения;
- Адресная книга поддерживает формат контактов VCARD и может быть экспортирована или сохранена на вашем компьютере;

- Календарь с возможностью создавать события и уведомлять о них сотрудников по почте;
- Цветные метки писем, как это принято в почтовом клиенте Thunderbird. Проставляются клавишами от 1 до 5. Изменения сохраняются на сервере, поэтому в другом почтовом клиенте метки будут видны;
- Расширенный поиск по всем письмам ящика находится в разделе **Еще...** панели инструментов ящика.

21.2.3 Настройка почтового релея

Основное

Подсказка: Видеоинструкция по настройке почтового релея в Ideco NGFW:

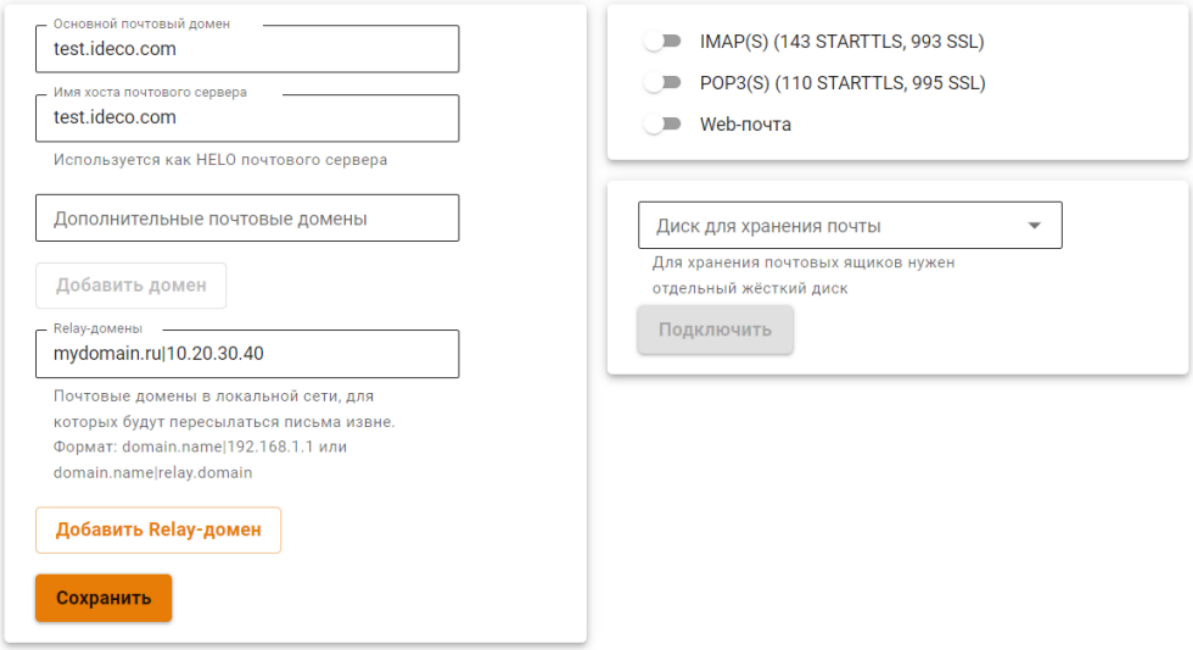
Ссылка на видеоинструкцию по настройке почтового релея в Ideco NGFW

Предупреждение: NGFW не поддерживает кириллические почтовые домены.

Перед настройкой почтового релея убедитесь, что на Ideco NGFW включен почтовый сервер.

Для настройки почтового релея:

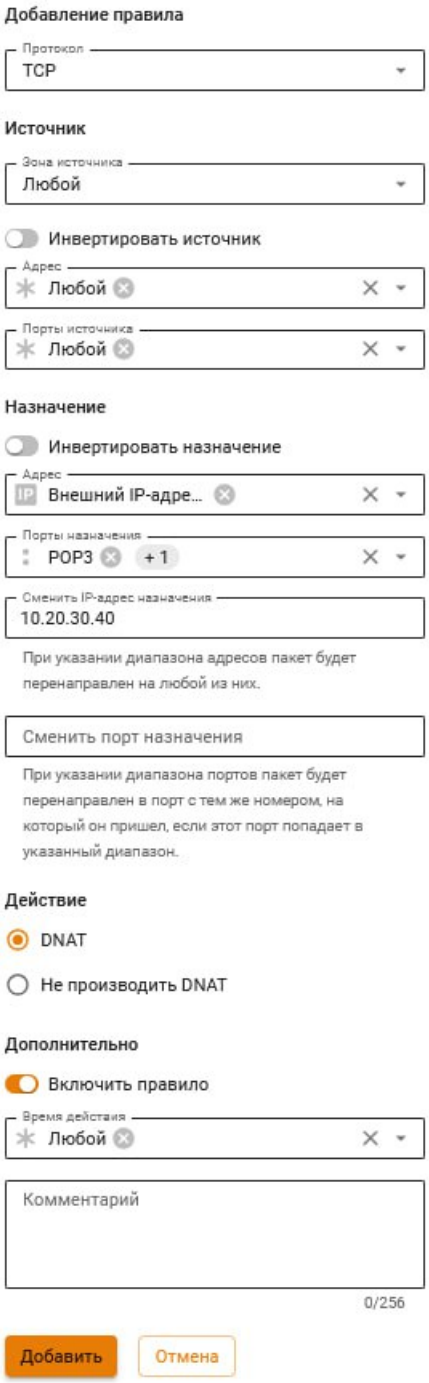
1. Добавьте в поле **Relay-домены** (почтовые домены в локальной сети, для которых будут пересылаться письма извне) запись вида: `mydomain.ru|10.20.30.40`, где:



- `mydomain.ru` - почтовый домен, зарегистрированный в интернете на публичный адрес Ideco NGFW;
- `10.20.30.40` - адрес почтового сервера в локальной сети.

Подсказка: Основной почтовый домен Ideco и имя хоста почтового сервера должны отличаться от Relay-домена. Для этого в поля **Основной почтовый домен** и **Имя хоста почтового сервера** в настройках почтового сервера нужно прописать вымышленный домен, не совпадающий с зарегистрированным.

2. Перейдите в раздел **Правила трафика -> Файрвол -> DNAT**, создайте и включите правило проброса портов POP3 и IMAP:



Все почтовые домены должны быть ассоциированы с внешним адресом сервера Ideco NGFW (A- и MX-записи в DNS-зоне).

Работа в режиме открытого почтового релея невозможна, поэтому Ideco NGFW в режиме Relay может принимать почту только в следующих случаях:

- Когда почта адресована исключительно для указанного Relay-домена;
- Из сетей, которые входят в список доверенных в разделе **Расширенные настройки -> Безопасность**.

Вся остальная почта будут отвергнута сервером.

21.2.4 Настройка почтового сервера

Подсказка: Видеоинструкция по настройке почтового сервера в Ideco NGFW:

Ссылка на видеоинструкцию по настройке почтового сервера в Ideco NGFW

1. Перейдите в раздел **Почтовый релей -> Основные настройки**, заполните поля **Основной почтовый домен** и **Имя хоста почтового сервера**.

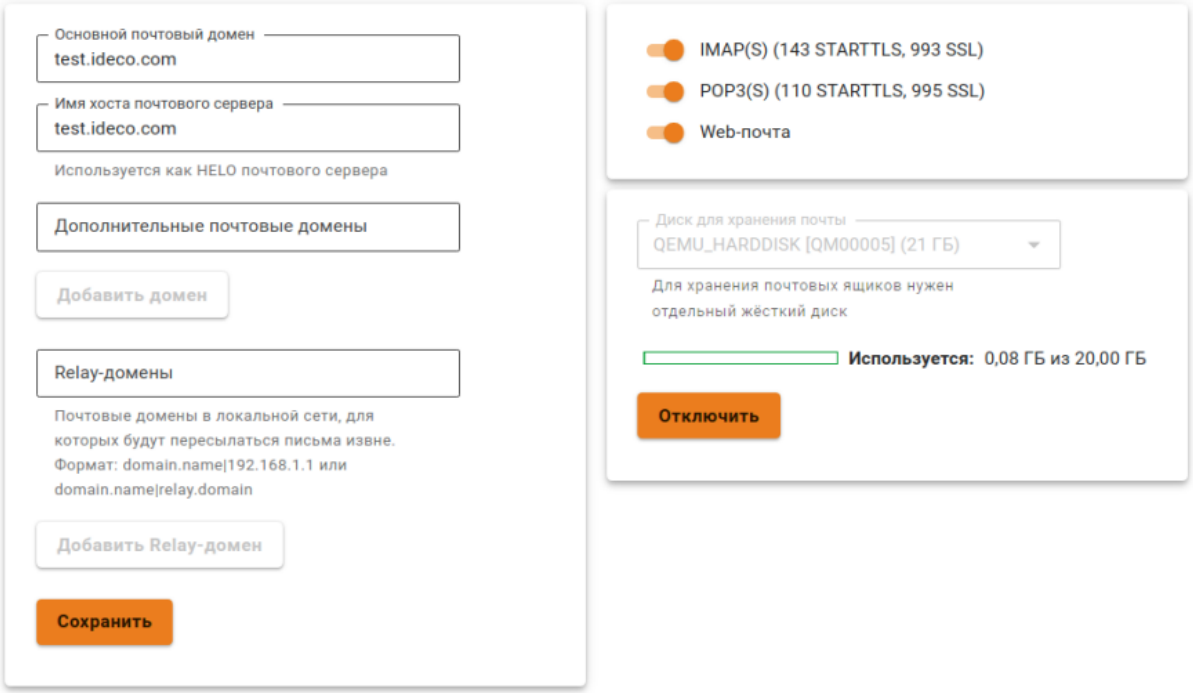
- **Основной почтовый домен** указывает серверу на его почтовый домен, для которого он должен принимать и обрабатывать письма. Все ящики пользователей будут принадлежать этому домену. От имени этого домена будет вестись переписка с корреспондентами.
- **Имя хоста почтового сервера** должно разрешаться из сети интернет во внешний IP-адрес NGFW. Почтовый сервер использует это имя как идентификатор при транспорте почты между другими почтовыми серверами. Необходимо для корректной работы почтового сервера в интернете.

Подсказка: Имя хоста почтового сервера как правило, совпадает с MX-записью для вашего домена.

2. Заполните дополнительные почтовые домены, которые почтовый сервер будет считать своими. Корреспонденция, отправляемая с ящиков в этих почтовых доменах, будет обрабатываться сервером при условии правильной установки MX-записей.

3. Включите опции IMAP(S) и POP(S).

4. Подключите дополнительный жесткий диск к серверу, если Ideco NGFW планируется использовать, как полноценный сервер с хранением почты. Перед подключением диска включите почту:



Предупреждение: Хранение почты на дополнительном HDD/SSD-диске обязательно, начиная с версии Ideco UTM 7.9.0. Рекомендуем использовать SSD-диск. Поддерживаются SATA/SAS- и NVMe-накопители. Дополнительное устройство используется только для работы почтового сервера, другие данные на нем храниться не будут.

Если диск после подключения не отображается:

- Проверьте, стерты ли с диска все данные, в том числе таблица разделов;
- Обратитесь в *техническую поддержку*, если проблему не удалось решить самостоятельно.

SSL-сертификат для почтового домена

После сохранения настроек основного почтового домена и имени хоста почтового сервера Ideco NGFW создает локальный сертификат, подписанный корневым (самоподписанным) сертификатом. Параллельно с созданием локального сертификата отправляется запрос на выпуск сертификата Let's Encrypt.

- Если сертификат Let's Encrypt успешно выпущен, то он заменит собой локальный сертификат.
- Если выпуск сертификата Let's Encrypt завершился неудачей, то будет использоваться локальный сертификат.

Подсказка: Для замены автоматически выпущенного сертификата перейдите в раздел **Сервисы -> Сертификаты -> Загруженные сертификаты** и загрузите собственную цепочку сертификатов. **CN (Общее имя)** последнего сертификата в цепочке должно соответствовать домену, для которого сертификат загружается. Подробнее в *инструкции*.

Проверка настроек почтового сервера

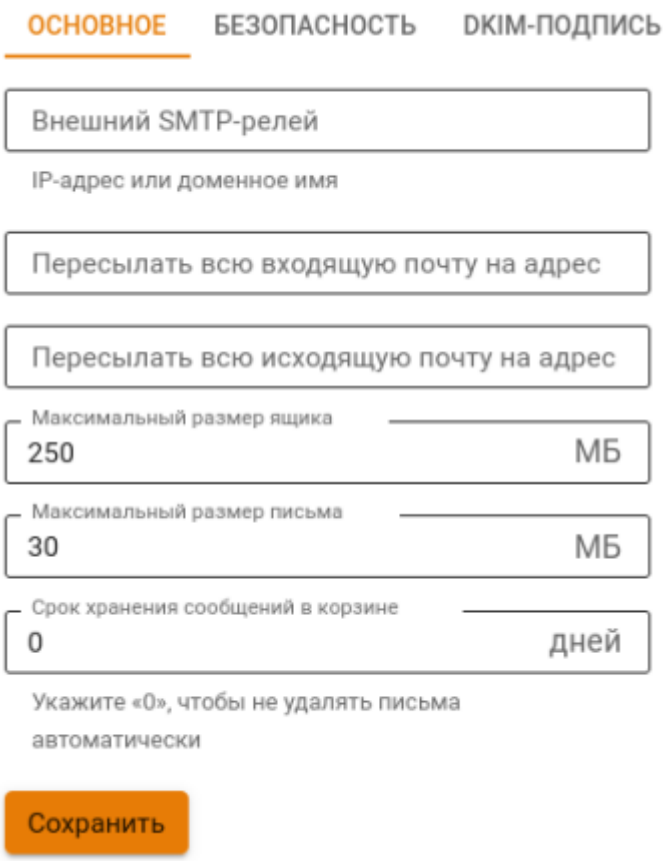
Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса mail-tester.com.

При правильной настройке почтовый сервер на Ideco NGFW должен получить 10 баллов из 10.

21.3 Расширенные настройки

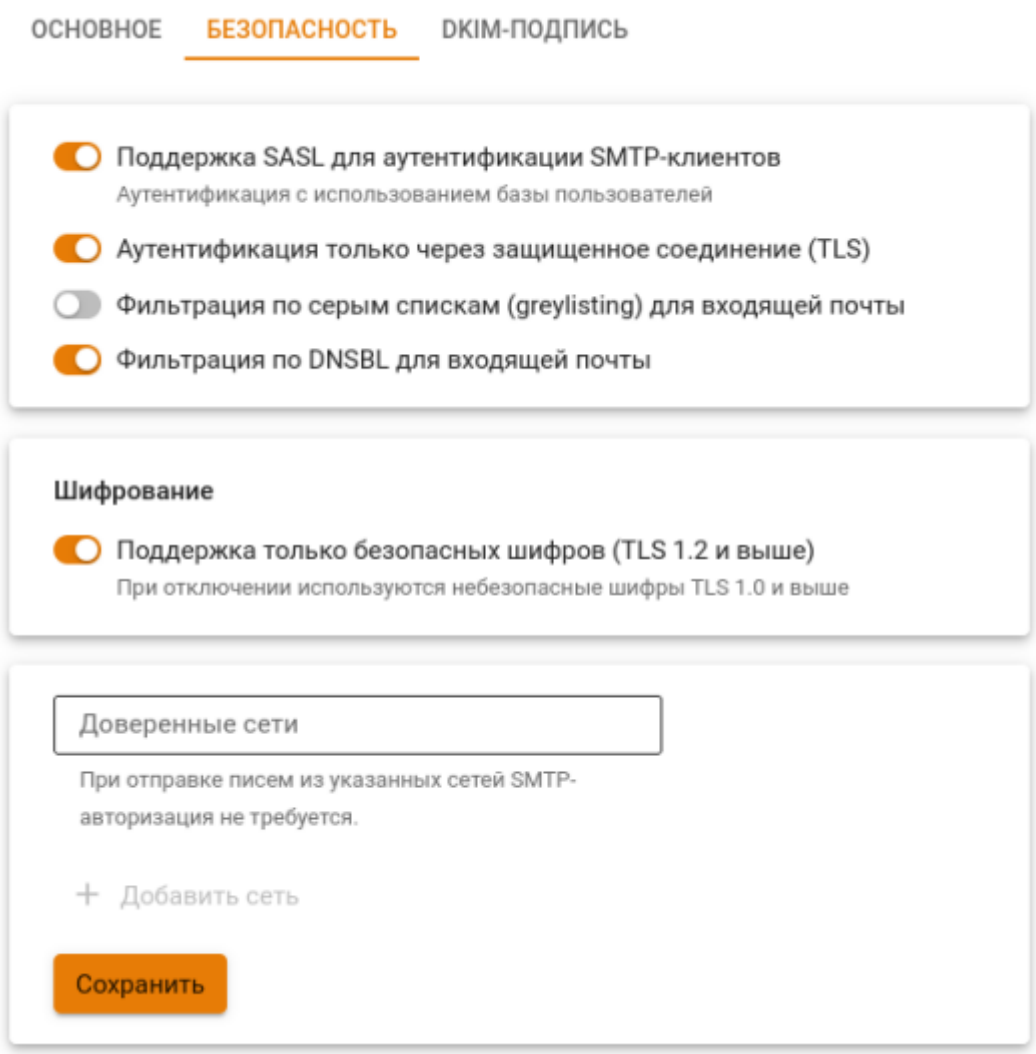
Раздел **Расширенные настройки** состоит из трех подразделов: **Основное, Безопасность, DKIM-подпись**.

21.3.1 Основное



- **Внешний SMTP-релей.** Вся исходящая почта будет отправляться на указанный адрес. Используется, например, если почта должна проходить через вышестоящий сервер провайдера перед отправкой в интернет;
- **Пересылать всю исходящую почту на адрес.** Вся исходящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости;
- **Пересылать всю входящую почту на адрес.** Вся входящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости;
- **Максимальный размер ящика.** Ограничение на максимальный размер почтового ящика в мегабайтах (**100ГБ - максимальное значение**);
- **Максимальный размер письма.** Ограничение на максимальный размер формируемого сервером письма в мегабайтах (**150МБ - максимальное значение**);
- **Срок хранения сообщений в корзине.** Количество дней, в течение которых почта хранится в корзине перед удалением. Максимальный срок хранения - 60 дней.

21.3.2 Безопасность

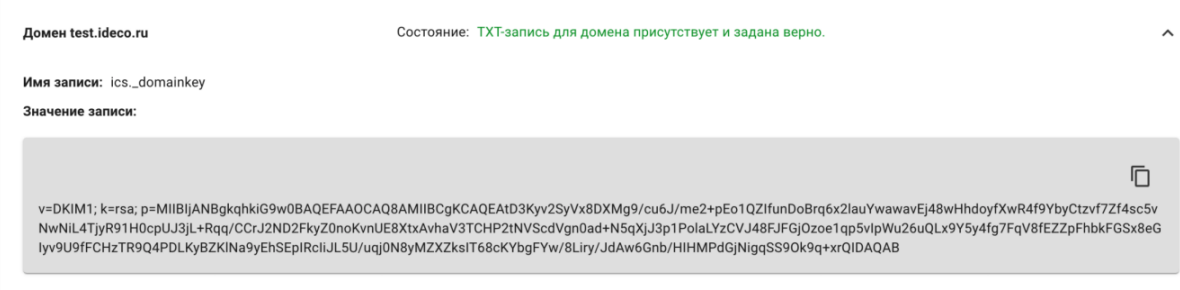


- **Поддержка SASL для аутентификации SMTP-клиентов.** Подключиться к почтовому ящику из интернета и отправить письмо, используя SMTP сервер Ideco, можно будет только, пройдя авторизацию по логину и паролю, заданному для этой учетной записи пользователя на сервере. **Не включайте этот параметр, если используете NGFW в качестве почтового релея**;
- **Разрешить аутентификацию только через защищенное соединение (TLS).** Запрещает незащищенную передачу учетных данных клиента при аутентификации на SMTP сервере;
- **Фильтрация по серым спискам (greylisting) для входящей почты.** Включает фильтрацию по серым спискам (greylisting) для входящей почты. При этом почта от неизвестных доменов отправителей может приходить с небольшой задержкой;
- **Фильтрация по DNSBL для входящей почты.** Включает фильтрацию по DNSBL для входящей почты;
- **Поддержка только безопасных шифров (TLS 1.2 и выше)**. При отключении используются небезопасные шифры TLS 1.0 и выше;
- **Доверенные сети.** Авторизация на сервере для доступа к почтовому ящику не требуется при попытке доступа из этих сетей. Указываются IP-сети и хосты в нотации CIDR или с префиксом сети, например, `10.0.0.5/255.255.255.255` или `192.168.0.0/16`.

21.3.3 DKIM-подпись

Настраивается в разделе **Почтовый релей -> Расширенные настройки -> DKIM-подпись.** Подписывает исходящую с сервера корреспонденцию уникальной для почтового домена подписью так, что другие почтовые серверы в сети интернет могут убедиться, что почта легитимна и заслуживает доверия.

Для функционирования технологии потребуется создать TXT-запись для домена у держателя зоны со значением, которое сформирует для этого почтового домена наш сервер. TXT-записи будут сформированы для основного почтового домена, настроенного на Ideco NGFW, и дополнительных почтовых доменов (если указаны). Сервер также проверит, правильно ли была указана запись и резолвится ли она в интернет.



Подсказка: Объем TXT-записи достаточно велик и многие регистраторы/держатели зон испытывают сложности с предоставлением интерфейса клиентам для указания TXT-записей длиннее 255 символов. Зачастую они предоставляют возможность указания TXT-записей длиной до 256 символов, согласно стандарту RFC1035. Но другой стандарт, RFC4408, предполагает объединение строк в случаях, когда нужно использовать длинные TXT-записи при настройке SPF и DKIM. Оперируйте этой информацией в диалоге с держателем доменной зоны. Как правило, держатели зон находят способ создания длинных TXT-записей.

Подсказка: Подпись содержит сочетание кавычек (кавычка-пробел-кавычка: « «).
Если хостинг не воспринимает такой формат записи, удалите эти символы.

21.3.4 Настройка домена у регистратора/держателя зоны

Основное

Для создания почтового сервера потребуется доменное имя. Зарегистрируйте его у интернет-провайдера или напрямую у регистратора, например, в RUcenter.

После того как было зарегистрировано доменное имя, потребуется внести изменения в описание зоны на DNS-сервере (у держателя доменной зоны, которой зачастую является регистратор).

1. Создайте ресурсную запись типа A с именем для почтового сервера в домене, указывающую на внешний IP-адрес Ideco NGFW. **Убедитесь, что на внешнем интерфейсе NGFW назначен публичный адрес, доступный из сети интернет.**

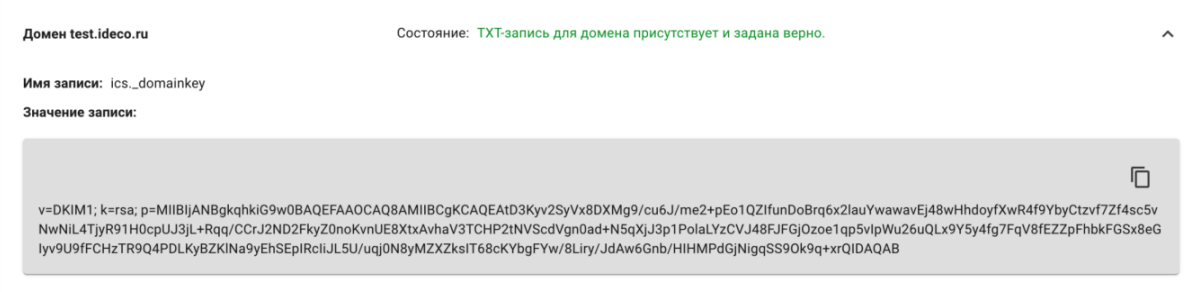
2. Добавьте ресурсную запись типа MX, указывающую на A-запись, которая была создана на предыдущем шаге. Запись типа MX указывает на сетевой узел, который занимается обработкой почтовых сообщений для домена. Она должна ссылаться на доменное имя почтового сервера, а не на IP-адрес.

Рекомендуем:

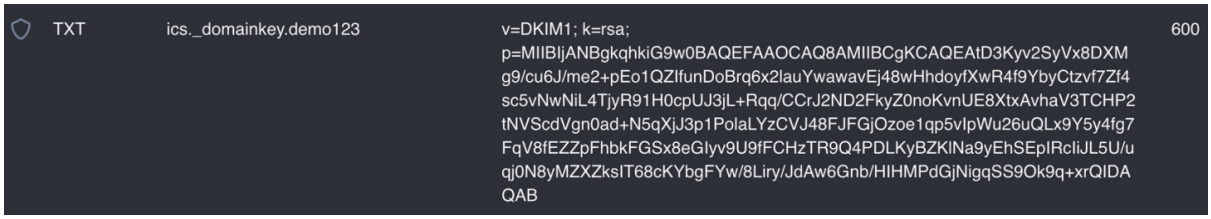
3. Добавить обратную ресурсную запись типа PTR. Эта запись должна быть прописана в файле обратной зоны. Эти изменения должны быть сделаны на стороне интернет-провайдера. Обратитесь к нему с просьбой прописать обратную ресурсную запись для IP-адреса, которая должна ссылаться на запись типа MX.

4. Настроить SPF-запись для почтового сервера.

5. После настройки почтового сервера настроить также DKIM-подпись почтовых сообщений. Для этого перейдите в раздел **Почтовый релей -> Расширенные настройки -> DKIM-подпись** и активируйте пункт **Подписывать исходящую почту с помощью DKIM**.



Также создайте TXT-запись для домена у держателя зоны с именем из строки *Имя записи* и с содержимым, которое было сформировано Ideco NGFW в **Значение записи**:



Рассмотрим набор необходимых записей на примере вымышленного домена `example.net`:

- A-запись вида: `mail.example.net. IN A 23.45.67.89`, где 23.45.67.89 - это внешний IP-адрес Ideco NGFW;
- MX-запись вида: `example.net. MX 10 mx.example.net`;
- Обратитесь на свой хостинг для регистрации PTR-записи для нужного IP-адреса вида: `89.67.45.23.in-addr.arpa IN PTR mail.example.net`;
- SPF-запись, объявляющая другим почтовым серверам в интернет, что отправка писем с домена разрешена только с хоста почтового сервера, указанного в MX-записи: `example.net. IN TXT "v=spf1 a mx -all"`.

Подсказка: Синтаксис SPF:

- «v=spf1» — версия SPF, обязательный параметр, всегда spf1, никакие другие версии не работают;
- «+» — принимать письма (по умолчанию);
- «-» — отклонить;
- «~» — «мягкое» отклонение (письмо будет принято, но будет помечено как спам);
- «?» — нейтральное отношение;
- «mx» — включает в себя все адреса серверов, указанные в MX-записях домена;

При использовании почтового сервера на NGFW в качестве почтового релея ресурсные записи будут выглядеть так же, так как в интернете почтовый сервер в локальной сети будет представлен SMTP-релеем на NGFW.

21.4 Антиспам и антивирус

Подсказка: Видеоинструкция по настройке антиспама в Ideco NGFW:

Ссылка на видеоинструкцию по настройке антиспама в Ideco NGFW

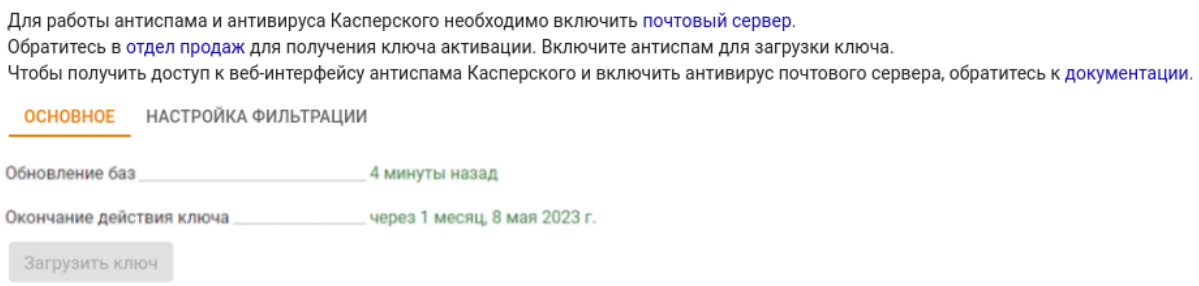
Раздел **Антиспам и антивирус** состоит из двух подразделов: **Основное** и **Настройки фильтрации**.

21.4.1 Основное

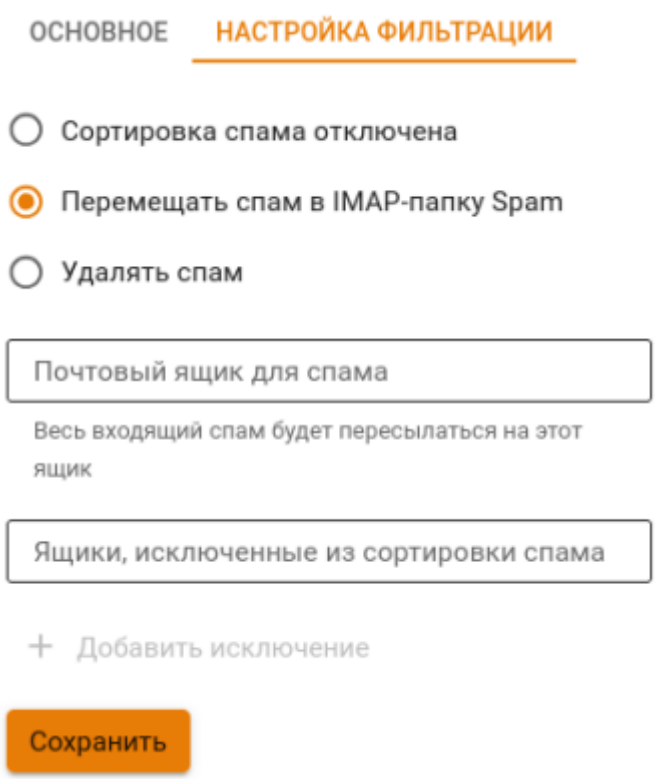
Позволяет управлять работой службы антиспама и антивируса почтового сервера на основе технологий Лаборатории Касперского с функцией машинного обучения и искусственного интеллекта. Также на этой вкладке предоставлена возможность добавления лицензионного ключа антиспама. Ключ поставляется в файле, имеющем расширение `.key`.

Если приобретена лицензия на антиспам, но нет в распоряжении лицензионного ключа, проверьте переписку с отделом продаж нашей компании (sales@ideco.ru) на наличие вложений. Если не удалось найти таких вложений, запросите ключ заново, выслав письмо на sales@ideco.ru с указанием наименования организации или номера лицензии.

Подсказка: Для работы антиспама и антивируса Касперского необходимо включить *почтовый сервер*. Перед загрузкой ключа обязательно включите модуль антиспама и антивируса.



21.4.2 Настройки фильтрации



- **Сортировка спама.** Задание логики сортировки нежелательной корреспонденции (спама). На выбор предоставляются следующие опции: отключение сортировки, перемещение нежелательных отправлений в папку Spam, удаление таких писем с сервера;
- **Почтовый ящик для спама.** Весь входящий спам будет пересылаться на указанный ящик (не используйте ящик Spam);
- **Ящики, исключенные из сортировки спама.** Позволяет задать почтовые адреса, которые не будут проверяться на спам.

Веб-интерфейс для Антиспама

Подсказка: Для включения веб-интерфейса Антиспама требуется, чтобы сам модуль **Антиспам и антивирус** был включен.

Веб-интерфейс имеет следующие преимущества:

- Отображает статистику по категориям Антиспама Касперского в удобном и понятном виде;
- Генерирует отчеты по работе за определенный период;
- Отображает очередь обрабатываемых сообщений;
- Позволяет задавать правила *Запрещенных и Разрешенных адресов*;
- Ведет аудит всех действий, производимых с Антиспамом.

Чтобы включить веб-интерфейс для Антиспама:

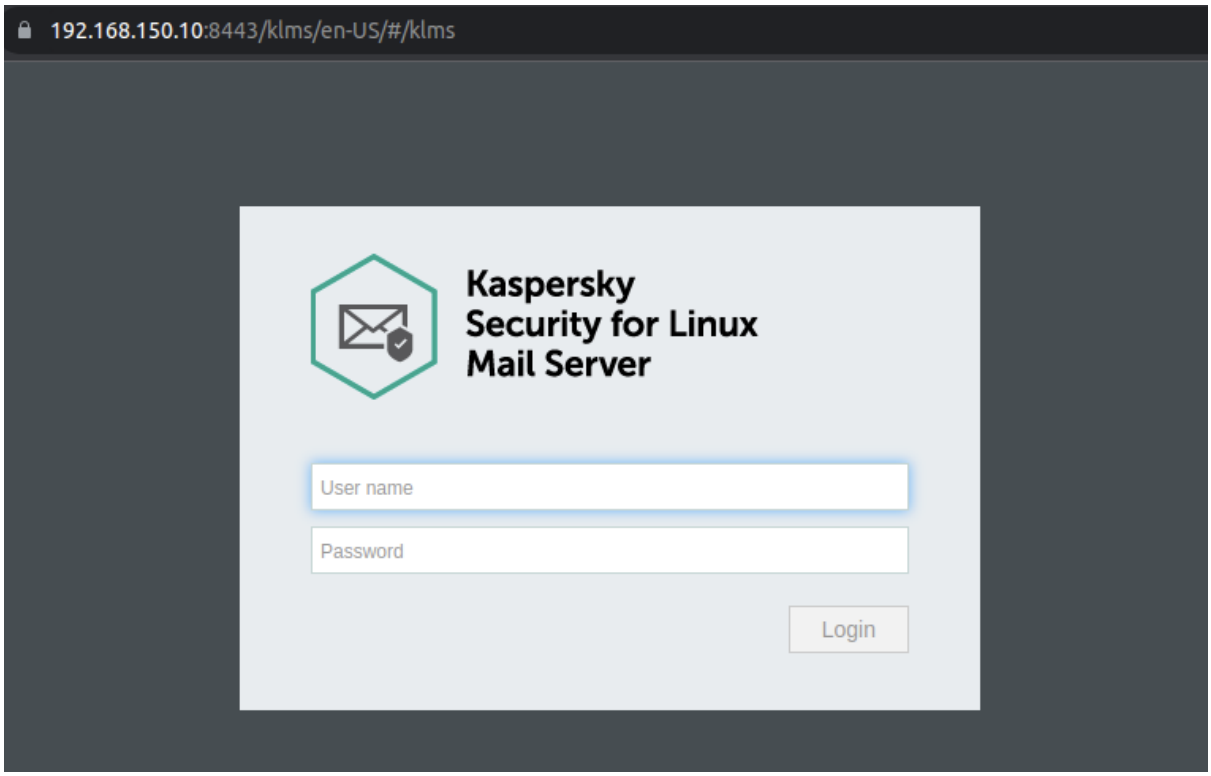
1. Перейдите в раздел **Управление сервером -> Терминал** и выполните команду `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`

2. Задайте пароль для стандартного аккаунта **Administrator**, состоящий минимум из 8 символов:

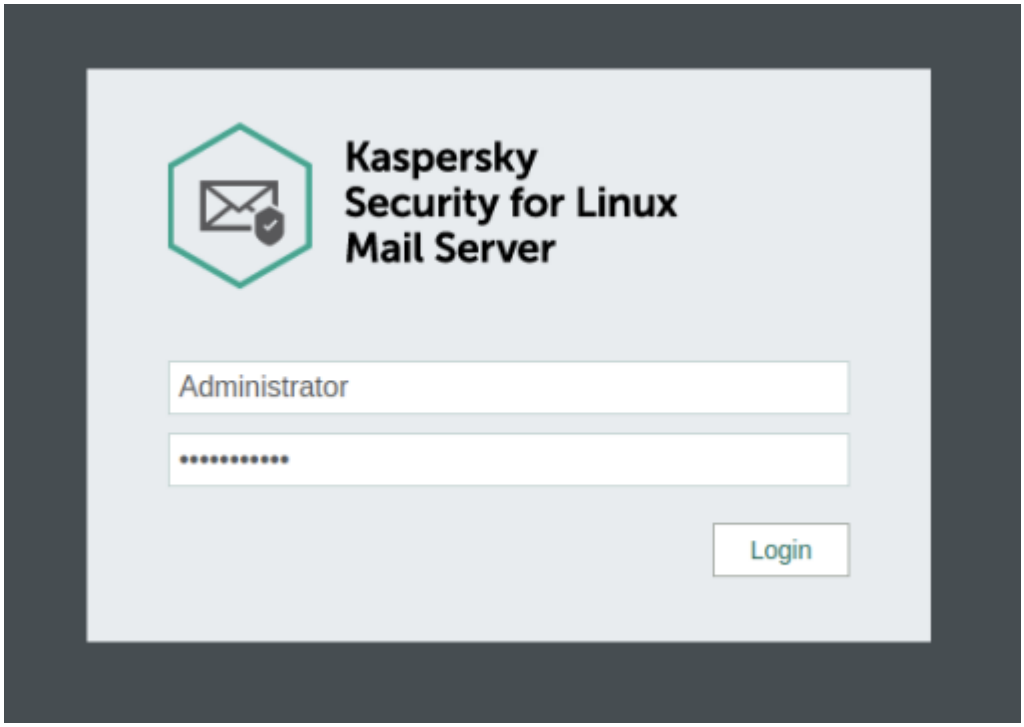
- Строчных букв;
- Заглавных букв;
- Специальных символов;
- Чисел.

```
[admin@localhost ~]# /opt/kaspersky/klms/bin/klms-control --set-web-admin-password
Password must satisfy three of four requirements:
        (1) Contains an uppercase letter;
        (2) Contains a lowercase letter;
        (3) Contains a special symbol;
        (4) Contains a number.
        And it must at least contain 8 characters

Enter new WEB console password for Administrator:
Retype new WEB console password for Administrator:
[admin@localhost ~]#
```

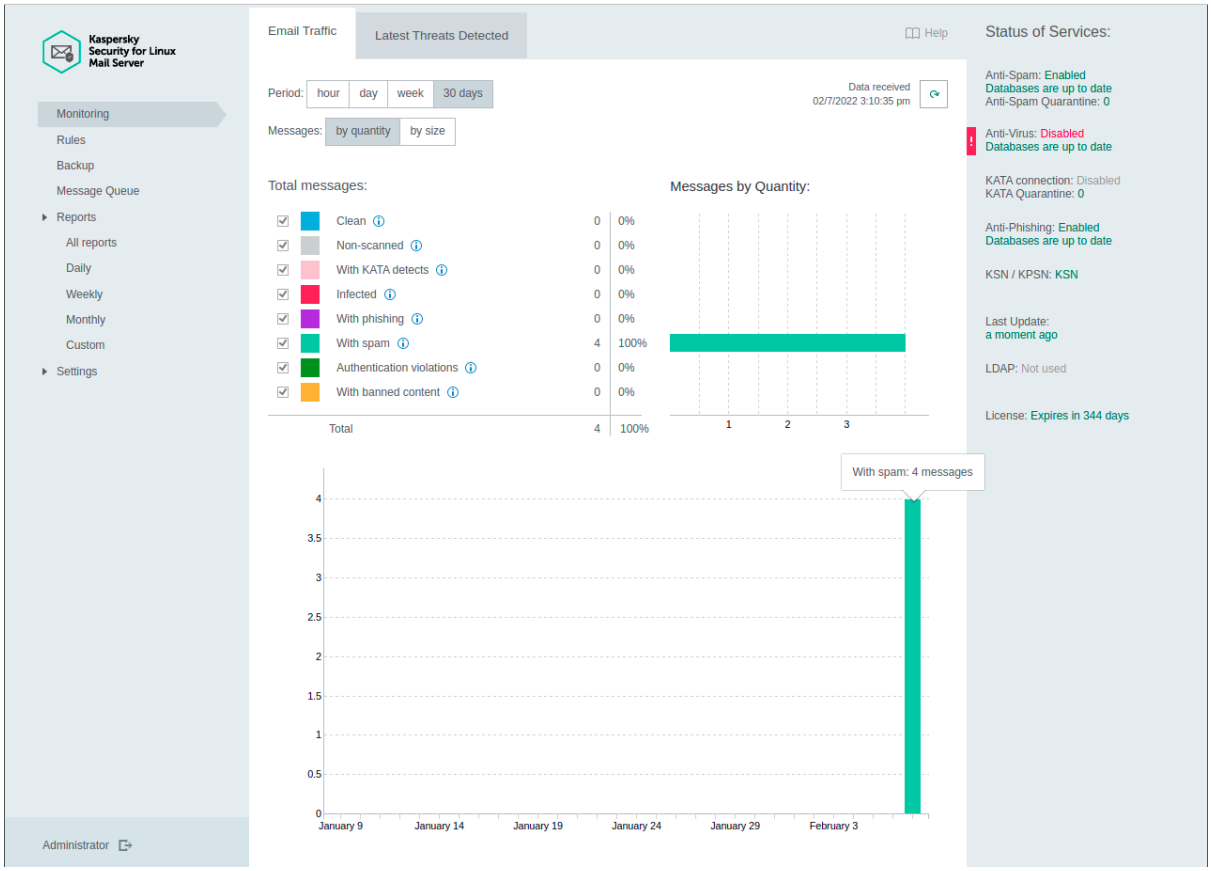
3. Для доступа к веб-интерфейсу перейдите в адресной строке по пути `ngfw_ip_address:8443/klms/`:



4. Войдите в веб-интерфейс с учетной записью **Administrator** и ранее заданным в терминале паролем:



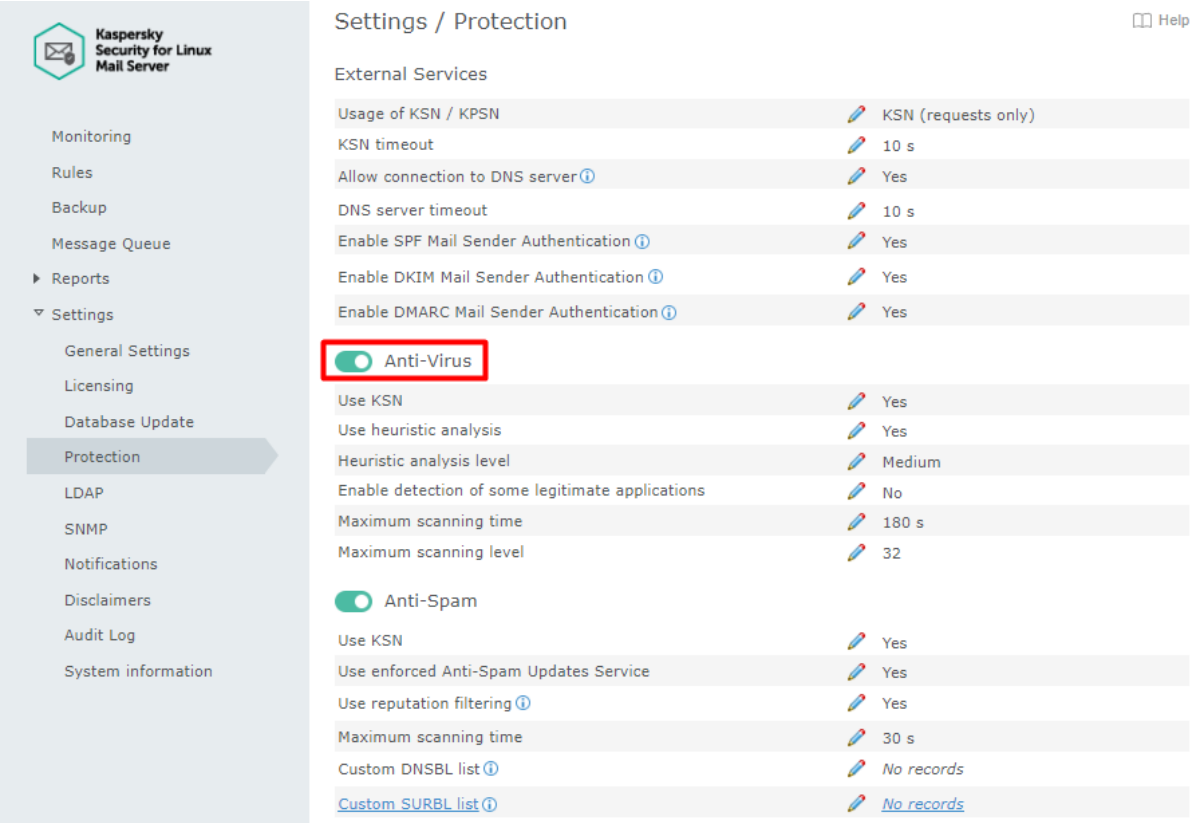
После успешного входа будет отображен дашборд со статистикой работы Антиспама:



Включение Антивируса почтового сервера

1. Перейдите в веб-интерфейс Антиспама. Подробные шаги настройки и входа в веб-интерфейс описаны в статье *Веб-интерфейс для Антиспама*;

2. Включите антивирус почтового сервера, перейдите в раздел **Settings -> Protection** и активируйте опцию **Anti-Virus**:



Предупреждение: Не рекомендуем вносить какие-либо изменения в разделе `Settings`, кроме указанных выше, потому как не можем гарантировать функциональность работы Антиспама в таких случаях.

21.5 Правила

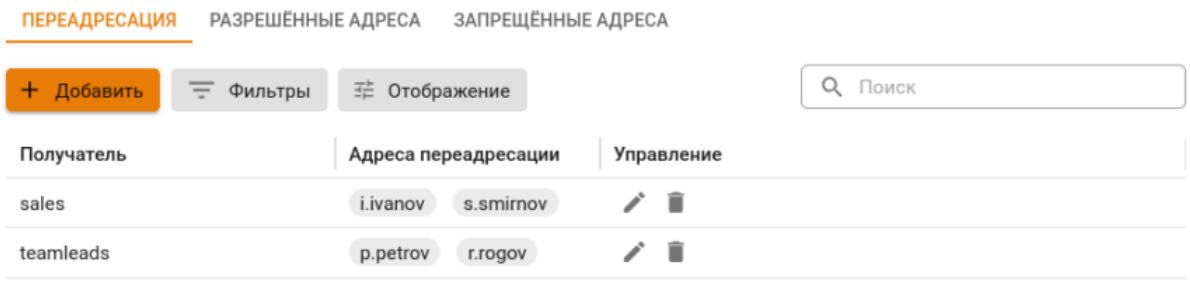
Раздел **Правила** состоит из трех вкладок: **Переадресация, Разрешенные адреса, Запрещенные адреса**. На каждой вкладке доступна фильтрация по кнопке **Фильтры**.

21.5.1 Переадресация

Позволяет настроить переадресацию почты на сервере с помощью почтовых алиасов.

Алиасы, в отличие от почтовых ящиков, не требуют логинов и паролей, они закрепляются за ящиком и служат его копией с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, может служить группой рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в графе **Получатель**, должен реально существовать.

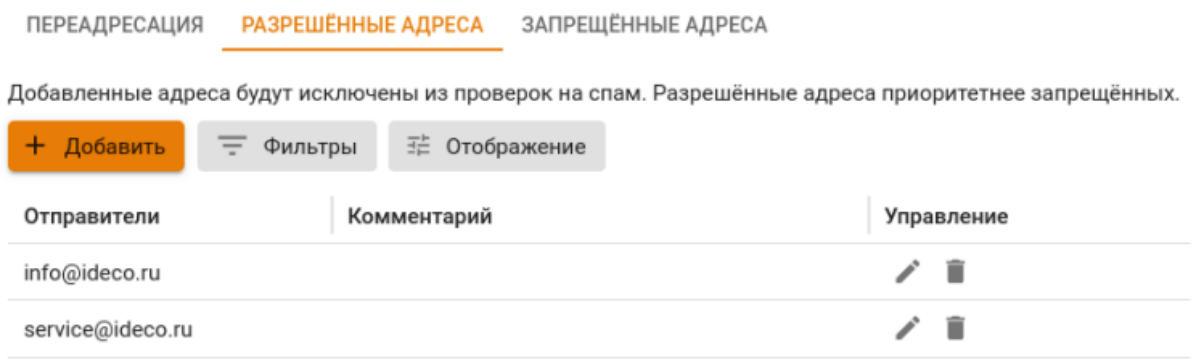
Подробнее с документацией по настройке почтовых алиасов на Ideco NGFW ознакомьтесь в статье *Переадресация почты*.



21.5.2 Разрешенные адреса

Позволяет указывать почтовые домены, IP-адреса почтовых серверов и почтовые ящики, отправления с которых не будут проверяться на спам.

Предупреждение: Если ящик одновременно указан в **Запрещенном адресе** и в **Разрешенном адресе**, то наивысший приоритет имеет **Разрешенный адрес**.



Подсказка: При занесении пересекающихся источников в оба списка корреляции между источниками не происходит. Приоритет будет отдан сначала IP-адресам, затем ящикам и затем доменам. То есть, если запрещен IP-адрес почтового сервера и разрешен домен, который он обслуживает, то письма от него будут блокироваться (блокировка по IP-адресу имеет приоритет). Обратный пример: разрешен IP-адрес, но запрещен домен. Письма блокируются, просто на более поздней стадии, при проверке почтового домена.

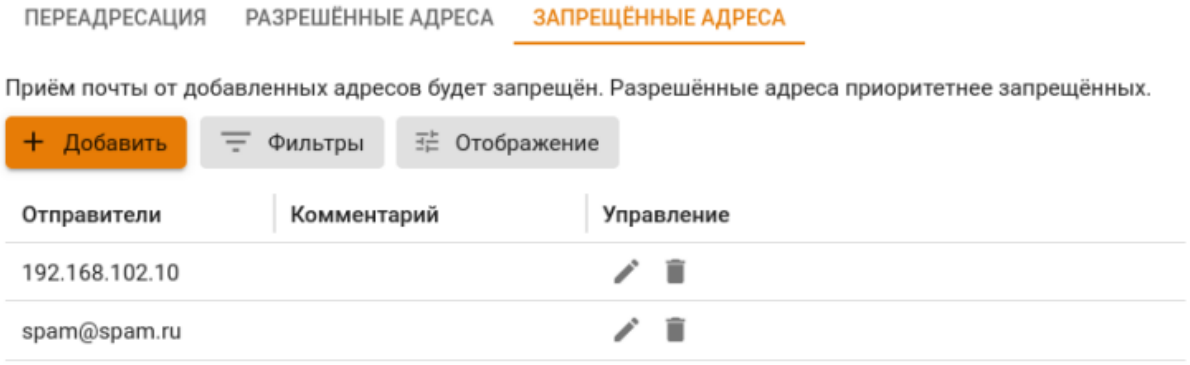
Еще один пример: в **Разрешенные адреса** внесен домен, в **Запрещенные адреса** - ящик из этого домена. Тогда письма с ящика будут заблокированы.

Обратный пример: письма от ящика, занесенного в **Разрешенные адреса**, будут разрешены, даже если домен, которому принадлежит ящик, занесен в **Запрещенные адреса**.

Подсказка: Схема обработки писем в почтовом сервере представлена в статье *Схема фильтрации почтового трафика*. Обратите внимание, что Разрешенные и Запрещенные адреса срабатывают после нескольких предварительных этапов фильтрации.

21.5.3 Запрещенные адреса

Позволяет указывать почтовые домены и ящики, отправления с которых не будут приниматься сервером.



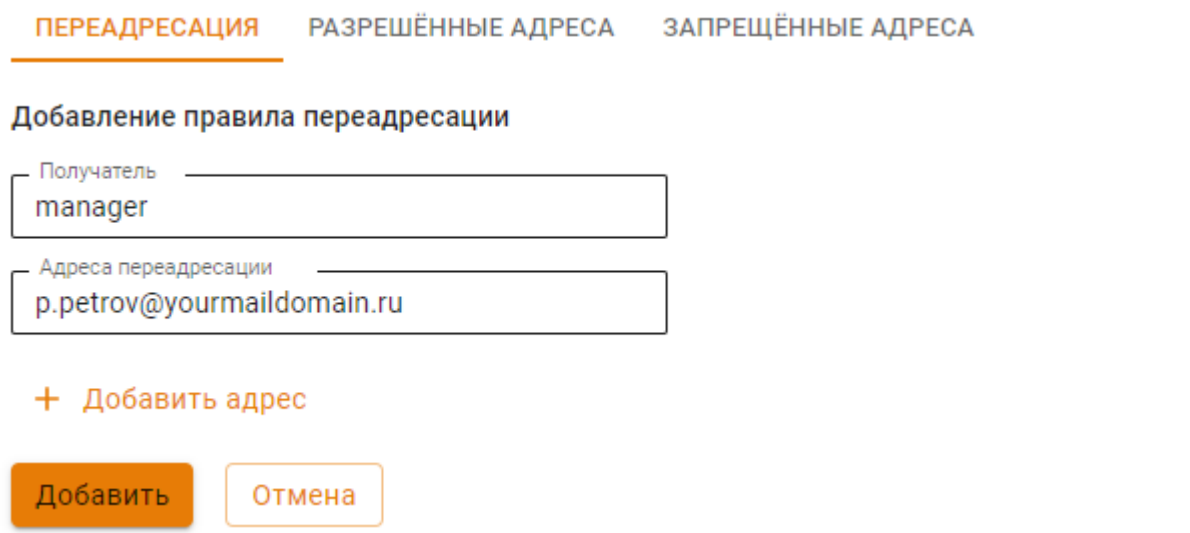
21.5.4 Переадресация почты

Чтобы создавать и редактировать почтовые правила переадресации (алиасы), перейдите в раздел **Почтовый релей -> Правила -> Переадресация**.

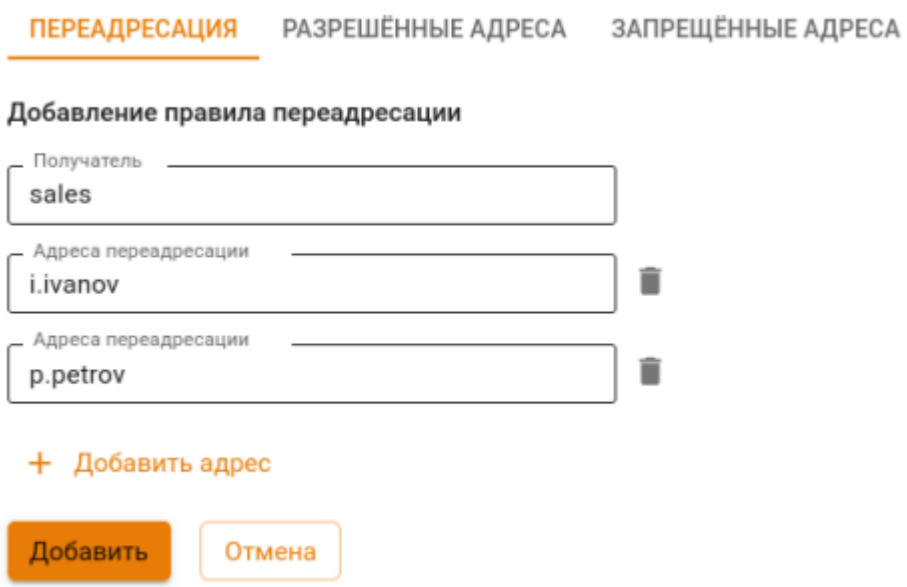
Почтовые алиасы отличаются от почтовых ящиков тем, что не требуют логинов и паролей. Они закрепляются за ящиком и служат его копией с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, можно сказать что алиас - это группа почтовых ящиков или группа рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Часть адреса `@yourdomain.com` можно не указывать при создании правил, если ящик расположен на почтовом сервере Ideco NGFW. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в поле **Получатель**, должен реально существовать.

Примеры:

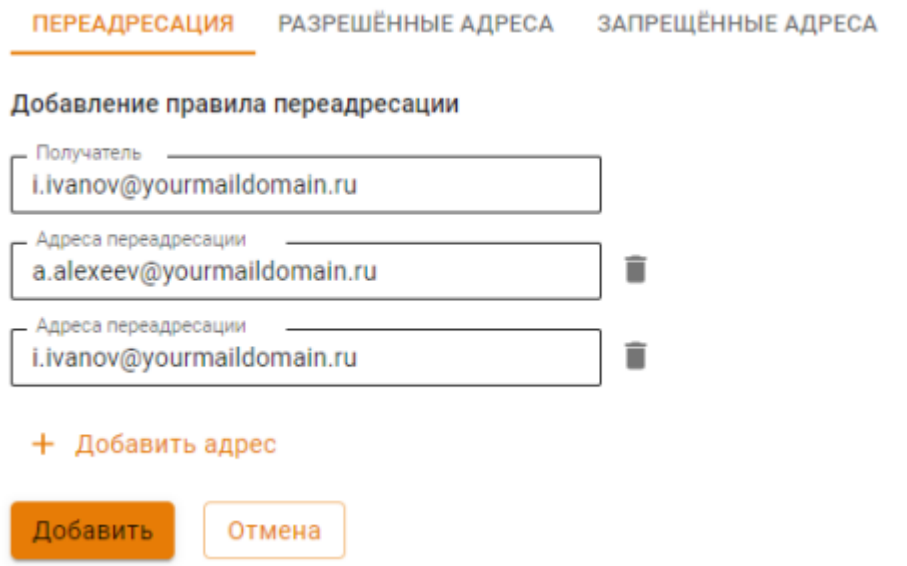
- Создать алиас `manager@yourdomain.ru` для ящика менеджера компании для связи с клиентами и партнерами, у которого реальный почтовый ящик имеет имя `p.petrov@yourmaildomain.ru`:



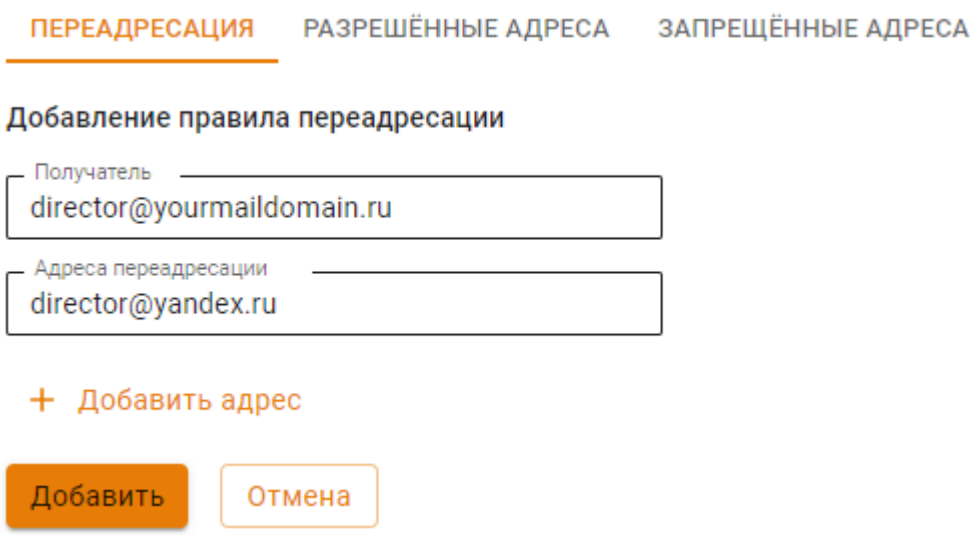
- Создать корпоративный алиас для отдела продаж `sales@yourmaildomail.ru`, чтобы почта пересылалась на всех сотрудников этого отдела:



- Создать временный алиас для переадресации почты сотрудника, который находится в отпуске `i.ivanov@yourmaildomail.ru`, на ящик его коллеги `a.alexeev@yourmaildomain.ru` с сохранением почты на ящике `i.ivanov@yourmaildomail.ru`:



- Создать алиас `director@yourmaildomain.ru`, который будет перенаправлять почту на реальный ящик `director@yandex.ru`:



Работа почты при настроенных правилах переадресации:

Письма, приходящие на несуществующий ящик (алиас) `manager@yourdomain.ru`, будут попадать на реальный `p.petrov@yourmaildomain.ru`. Также есть алиас для отдела продаж `sales@yourmaildomail.ru`, который, по сути, служит алиасом для рассылки почты и сам писем не хранит. Это удобно, если есть информация для отдела продаж, которую надо распространить на каждого сотрудника. Все то же самое можно сделать, если просто указать в письме всех получателей, но использовать алиас намного удобнее. Также сотрудник с почтой `i.ivanov@yourmaildomail.ru` сейчас находится в отпуске, вся приходящая к нему почта попадает на его ящик и дублируется на `a.alexeev@yourmaildomain.ru`. Последнее правило позволяет директору получать почту не на корпоративный ящик, а на его личную почту на Яндексе.

Подсказка: Алиас не является действительным почтовым ящиком. К нему нельзя подключиться почтовым клиентом, используя логин и пароль, как в обычном почтовом аккаунте. Таким образом, создание алиасов не увеличивает максимально возможное количество реальных почтовых аккаунтов на Ideco NGFW.

21.6 Почтовая очередь

Модуль позволяет управлять входящей и исходящей отложенной корреспонденцией. Для анализа возможных причин задержки корреспонденции в очереди можно использовать информацию из соответствующего столбца таблицы для каждого письма. По кнопке **Фильтры** доступна фильтрация по каждому столбцу.

Почтовая очередь позволяет выполнять следующие выборочные и групповые действия с отправлениями:

- Очистка очереди
- Повторная отправка отдельного письма
- Удаление отдельных писем из очереди
- Повторная отправка всей корреспонденции из очереди

Подсказка: Значение в столбце **Время доставки** соответствует времени поступления письма в очередь. Если письмо не будет отправлено в течение 7 дней, то оно будет удалено из почтовой очереди и не будет доставлено получателю.

Предупреждение: При обновлении Ideco NGFW почтовая очередь очищается.

21.6.1 Проверка настроек почтового сервера

Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса mail-tester.com.

При правильной настройке почтовый сервер на Ideco NGFW должен получить 10 баллов из 10.

21.7 Настройка почтовых клиентов

Предупреждение: Начиная с версии UTM 7.0.0, подключиться из сети интернет программой Outlook (любой версии) по протоколу POP3 можно только с типом шифрования SSL. Подключение без шифрования извне запрещено на почтовом сервере.

Остается возможность подключаться по протоколу IMAP с использованием STARTTLS или SSL. Для этого выберите соответствующий тип шифрования в Outlook.

Подсказка: В Ideco NGFW нет ограничений по количеству почтовых клиентов для одного почтового адреса по протоколу imap.

21.7.1 Настройка почтового клиента при работе из локальной сети

1. Сервер входящей почты работает на 995 TCP-порту (POP3) и на 143 TCP-порту (IMAP) с шифрованием STARTTLS/SSL:

- В качестве логина прописывается логин от учетной записи пользователя.
- В качестве пароля всегда прописывается пароль от учетной записи пользователя (в том числе для пользователей, импортированных из Active Directory), задать отдельный пароль на почтовый ящик нельзя.

2. Сервер исходящей почты работает на 587 порту TCP с шифрованием STARTTLS/SSL. Без авторизации возможна отправка почты только из доверенных сетей (их можно настроить в разделе **Почтовый релей -> Расширенные настройки -> Безопасность**).

21.7.2 Настройка почтового клиента при работе из сети интернет

1. Сервер входящей почты работает на 995 TCP-порту (POP3S) и на 143 TCP-порту (IMAP-STARTTLS/SSL), шифрование обязательно:

- В качестве логина прописывается логин от учетной записи пользователя;
- В качестве пароля всегда прописывается пароль от учетной записи пользователя, сделать отдельный пароль на почту нельзя.

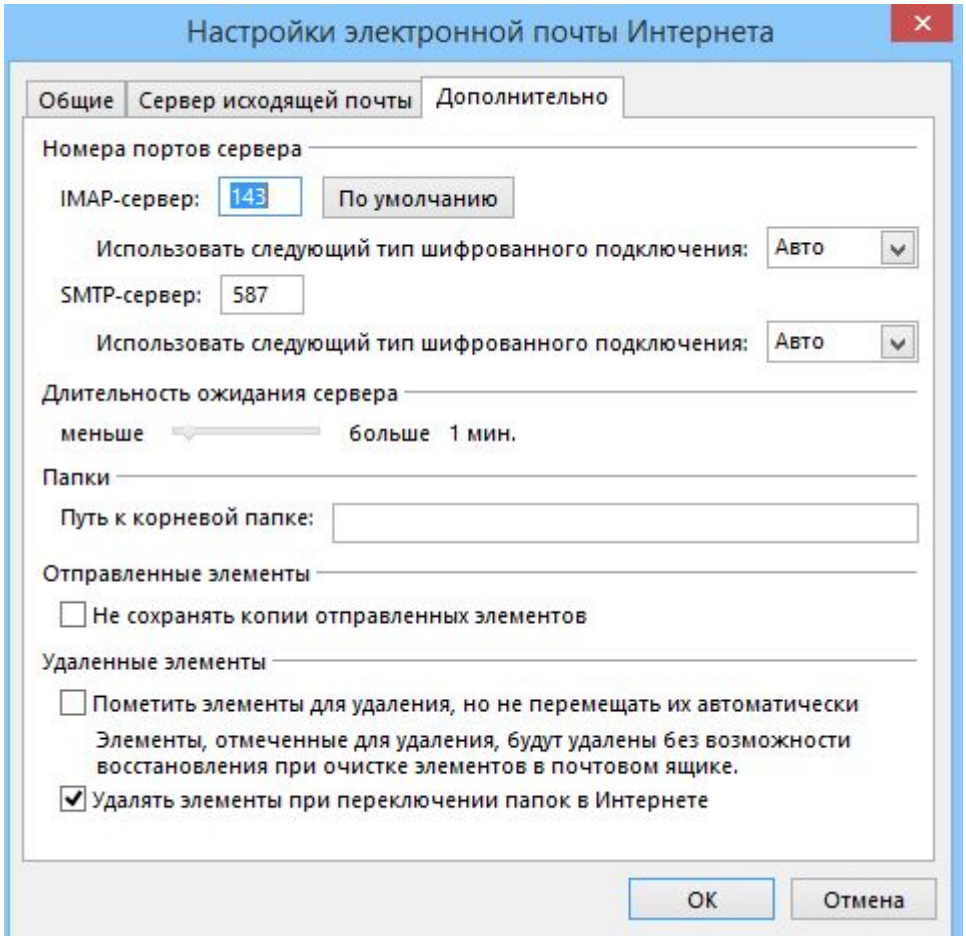
2. Сервер исходящей почты работает только с авторизацией и шифрованием. Необходимо обязательно использовать 587 порт для подключения (а не 25). Тип шифрования, логин и пароль указываются аналогично серверу входящей почты.

Для любого почтового клиента, кроме веб-интерфейса почты в составе NGFW, установите корневой сертификат сервера NGFW, его можно скачать в разделе **Сервисы -> Сертификаты**.

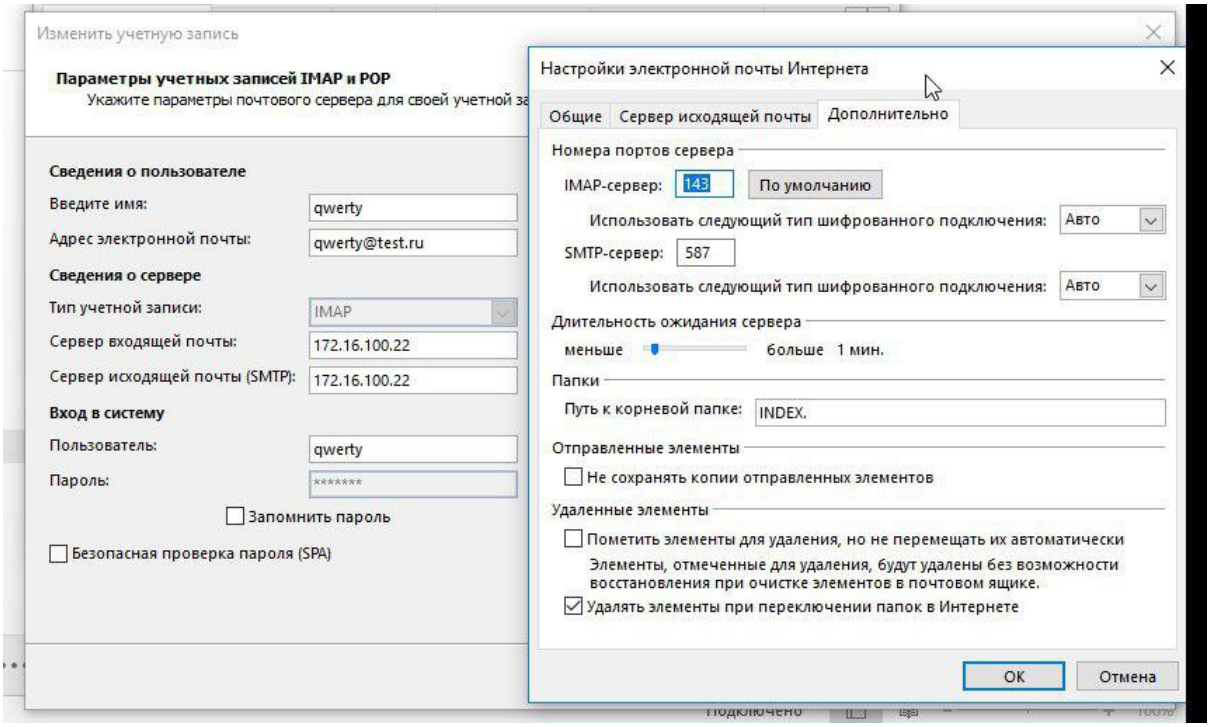
21.7.3 Примеры настроек популярных почтовых клиентов

Настройка почтового клиента Outlook 2013 и 2016:

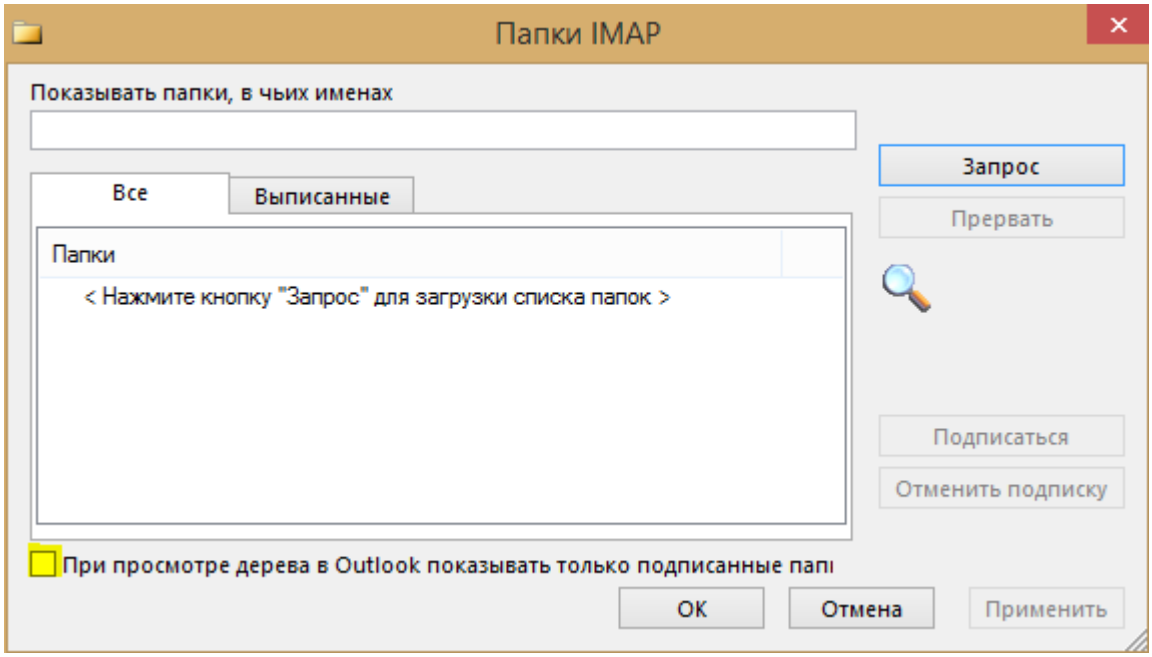
Пример настроек клиента Microsoft Outlook 2013 по протоколу IMAP:



Пример настроек клиента Microsoft Outlook 2016 по протоколу IMAP:



Для отображения IMAP-папок отключите опцию **При просмотре дерева в Outlook показывать только подписанные папки** в свойствах IMAP-папок:



Настройка почтового клиента iPhone:

Процесс настройки делится на два этапа:

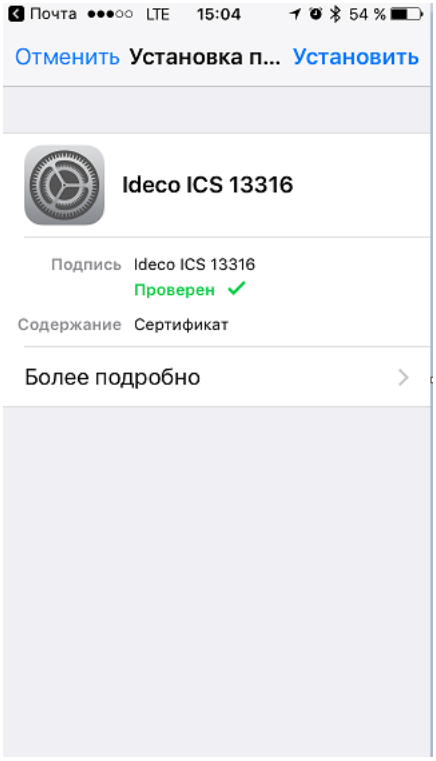
- Установка корневого SSL-сертификат NGFW;
- Настройка почтового ящика.

Установка корневого SSL-сертификат NGFW:

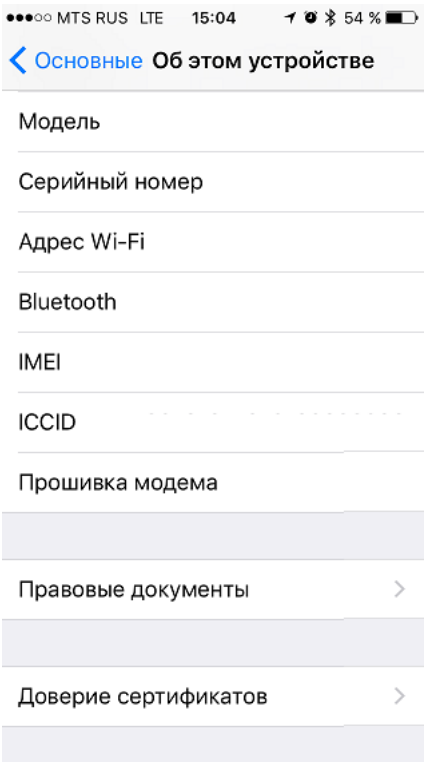
1. Скачайте сертификат в разделе **Сервисы -> Сертификаты** и перенесите на настраиваемое устройство (например, отправив по почте).

2. Нажмите кнопку **Установить**.

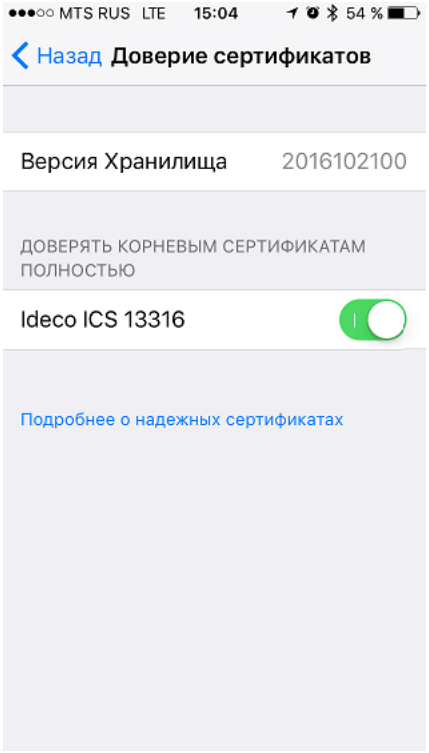
3. Зайдите в раздел **Настройки -> Основные**.



4. Выберите **Об этом устройстве -> Доверие сертификатов**:

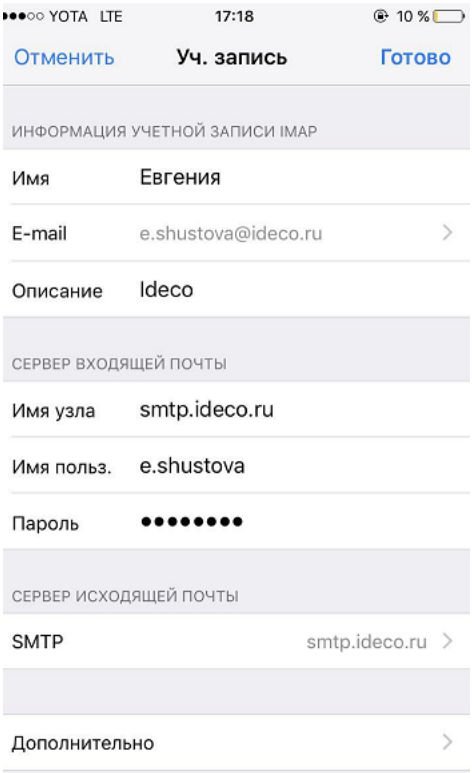


5. Включите настройку **Доверять корневым сертификатам полностью**

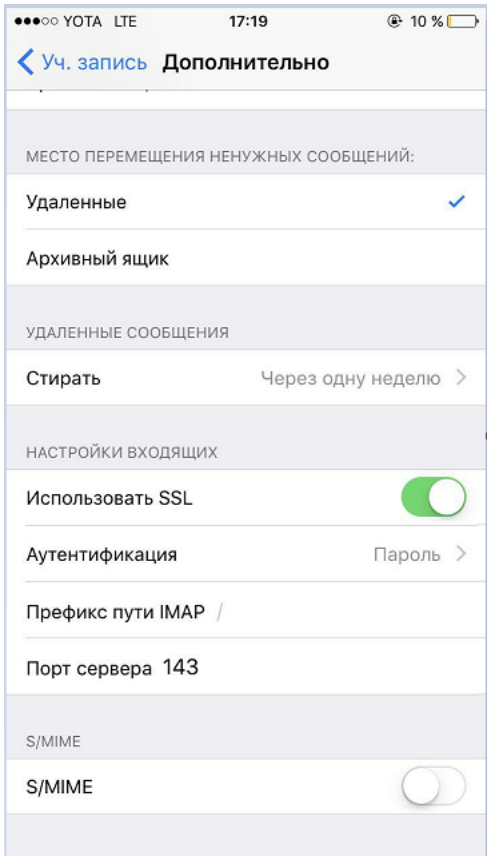


Настройка почтового ящика:

1. Перейдите в Учетную запись почты и нажмите **Дополнительно**:



2. Скорректируйте настройки:



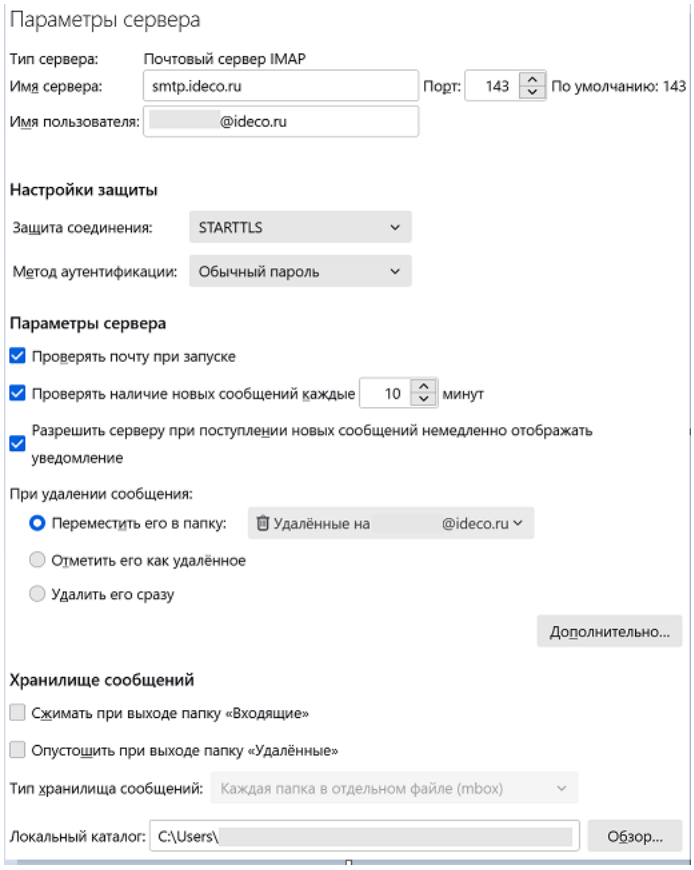
Настройка почтового клиента Thunderbird:

1. Перейдите в **Настройки -> Параметры ученой записи**.

2. Заполните обязательные поля:

- Имя сервера;
- Порт;
- Имя пользователя;
- Защита соединения;
- Метод аутентификации (рекомендуем указать **Обычный пароль**).

При необходимости заполните *Параметры сервера* и *Хранилище сообщений*.



21.8 Схема фильтрации почтового трафика

21.8.1 Основное

Полная схема и последовательность фильтрации:

Модуль Антиспама и антивируса Касперского использует собственный набор методик для фильтрации спама и обеспечивает высокий уровень детектирования спама при низких значениях ложных срабатываний (0,003-0,005% от общего количества сообщений).

Для защиты пользователей используется набор технологий распознавания спама с использованием внешних облачных сервисов (DNSBL, SPF и SURBL) и собственных алгоритмов: сигнатурный анализ текста и графики, лингвистический эвристик, использование UDS-запросов в режиме реального времени. Также проверяются все ссылки в почтовых сообщениях, письма со ссылками на фишинговые ресурсы блокируются.

Белый список в настройках почты обеспечивает прохождение писем без фильтрации, начиная с уровня **Фильтрации по серым спискам и проверки DKIM/SPF**. Предварительные спам-фильтры срабатывают для любых адресатов.

22. Публикация ресурсов

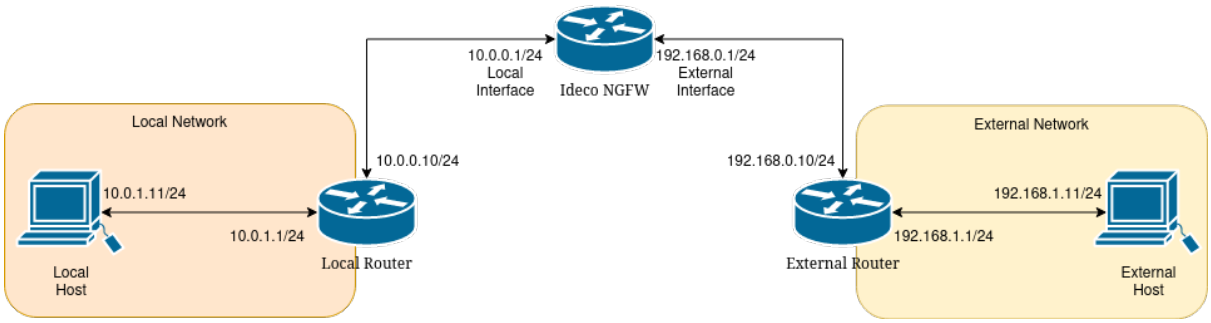
22.1 Доступ из внешней сети без NAT

22.1.1 Основное

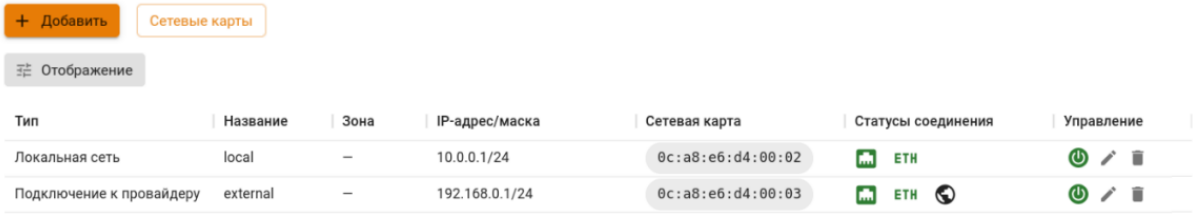
При необходимости (как правило, когда Ideco NGFW расположен внутри локальной сети, а не на границе с интернетом) возможно:

- Организовать прямой доступ к ресурсам внешних по отношению к Ideco NGFW сетей без использования NAT;
- Разрешить доступ из внешних относительно Ideco NGFW сетей в локальную сеть с прямым обращением к локальным IP-адресам.

Для примера разберем настройку Ideco NGFW для доступа без NAT в следующей конфигурации сети:



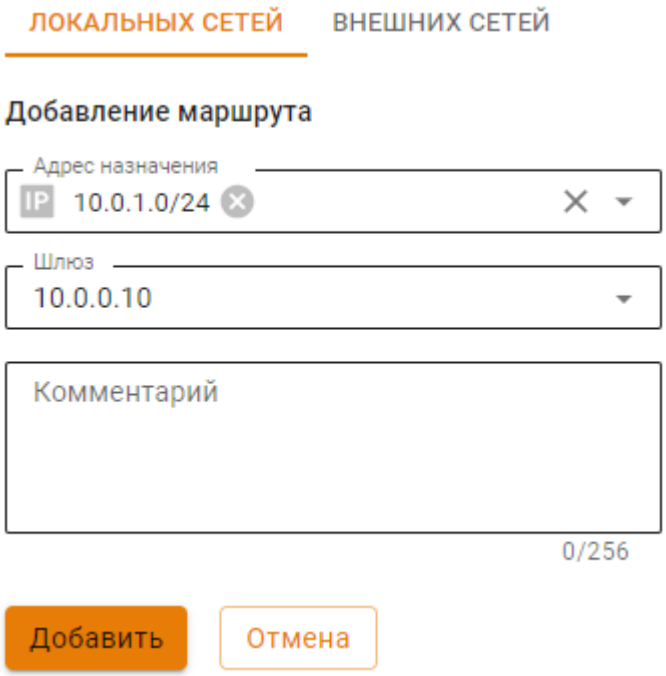
1. Настройте сетевые интерфейсы в разделе **Сервисы -> Сетевые интерфейсы** на Ideco NGFW:



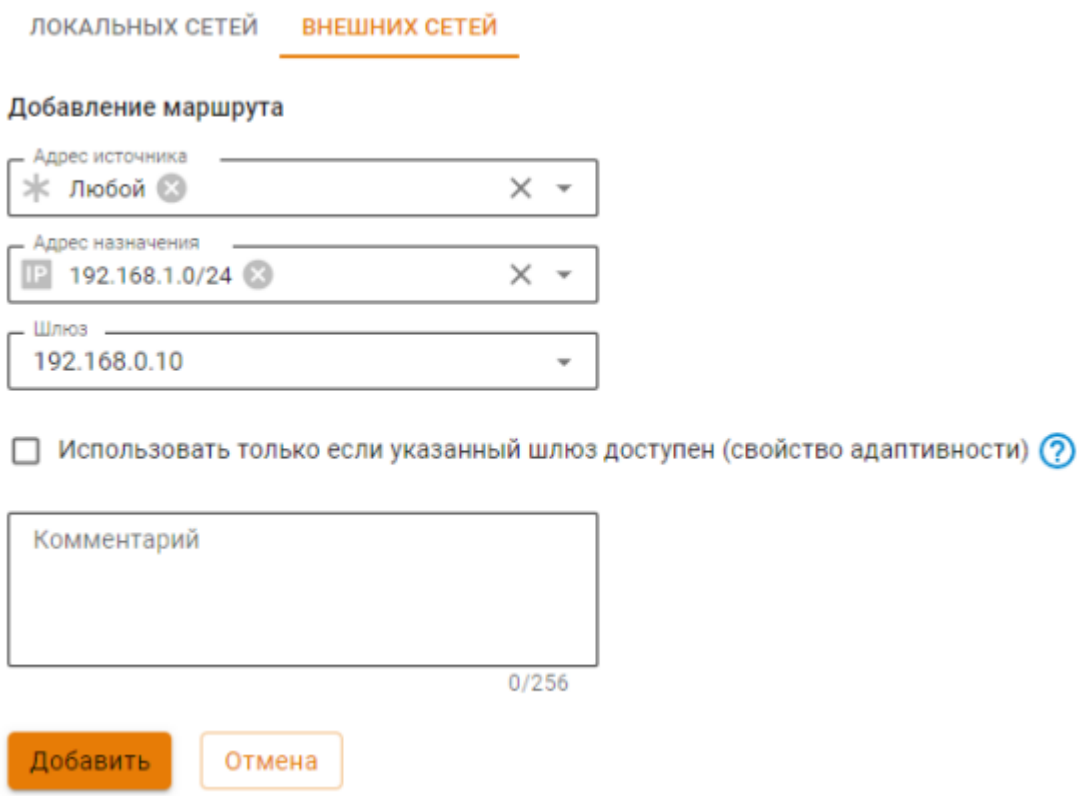
- **local** - интерфейс для доступа в пользовательскую локальную сеть;
- **external** - интерфейс для доступа в пользовательскую внешнюю сеть пользователей.

2. Перейдите в раздел **Сервисы -> Маршрутизация** и создайте правила для доступа к IP-адресам пользователей, которые находятся за маршрутизаторами:

- Для **Локальных сетей**:

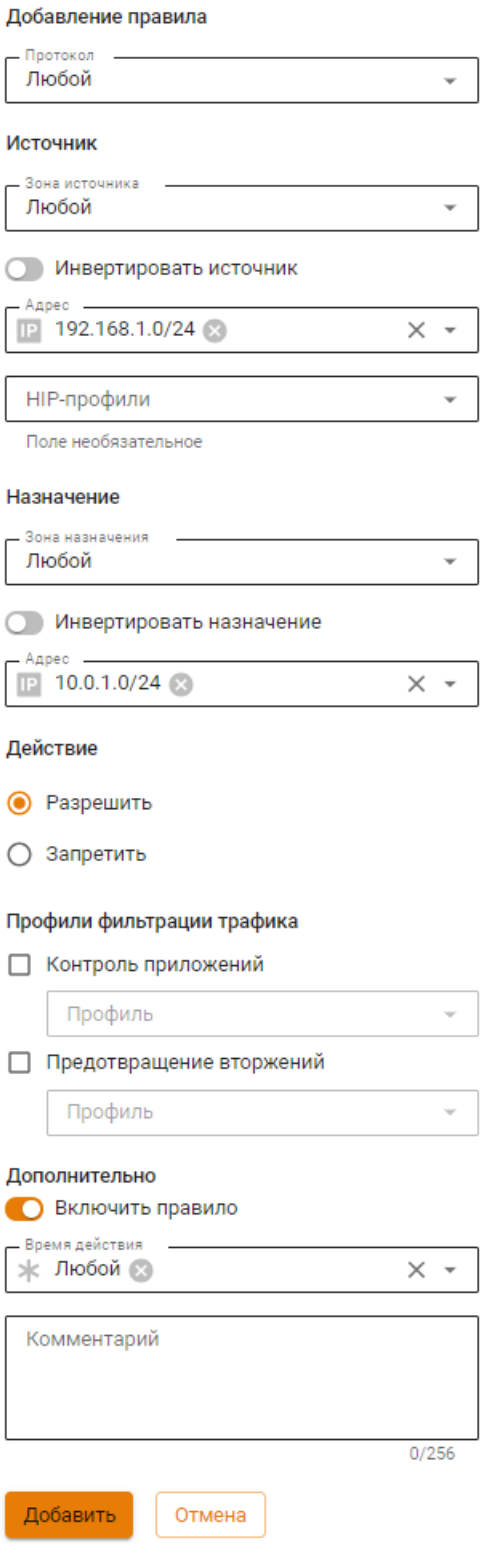


- **Адрес назначения** - адрес локальной сети за маршрутизатором (`10.0.1.0/24`);
- **Шлюз** - адрес машрутизатора (`10.0.0.10`).
- Для **Внешних сетей**:



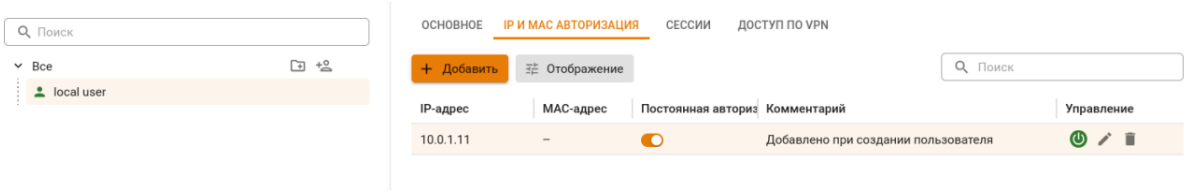
- **Источник** - Любой;
- **Адрес назначения** - адрес внешней сети за маршрутизатором (`192.168.1.0/24`);
- **Шлюз** - адрес машрутизатора (`192.168.0.10`).

3. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD**, создайте и включите правило для доступа хостов из внешней сети `192.168.1.0/24` до IP-адресов пользователей локальной сети `10.0.1.0/24`:



4. Перейдите в раздел **Правила трафика -> Файрвол -> SNAT** и отключите опцию **Автоматический SNAT локальных сетей**.

5. Перейдите в раздел **Пользователи -> Учетные записи** и включите опцию **Постоянная авторизация** для пользователей локальной сети `10.0.1.0/24`. Устройства локальной сети должны быть авторизованы на NGFW:



Внимание: Учитывайте риски подобного доступа с точки зрения информационной безопасности. Не предоставляйте доступ для внешних сетей и хостов, в безопасности которых не уверены.

Предупреждение: Правила трафика Ideco NGFW будут работать только для трафика, приходящего из внешней сети в локальную сеть.

22.2 Публикация веб-приложений (обратный прокси-сервер)

22.2.1 Основное

Публикация веб-серверов возможна через *обратный прокси сервер*.

22.3 Настройка публичного IP-адреса на компьютере в локальной сети

22.3.1 Основное

Для версии Ideco UTM 7.9.0 и старше настройка публичного IP-адреса для компьютеров, находящихся в локальной сети, невозможна.

Используйте *портмаппинг*, чтобы пробросить весь их диапазон от 0 до 65535 для получения эффекта присутствия локального сервера на внешнем IP-адресе.

22.4 Портмаппинг (проброс портов, DNAT)

22.4.1 Основное

Сервер предоставляет доступ к опубликованному в интернете веб-ресурсу (сервису, сетевой службе) на устройстве в локальной сети с серым IP-адресом. Ресурс публикуется путем трансляции (проброса) любого неиспользуемого сетевого порта на публичном IP-адресе сервера Ideco NGFW на порт ресурса, работающего на устройстве в локальной сети. При этом все обращения из внешних сетей на публичный адрес сервера Ideco по транслируемому порту перенаправляются на публикуемый порт данного ресурса. Эта технология называется DNAT, portmapper или port forwarding.

Для настройки портмаппинга в Ideco NGFW добавьте правило в разделе **Правила трафика -> Файрвол -> DNAT**. При создании правила укажите адреса сервера, публикуемой машины и сетевого порта, с которого и на который осуществляется трансляция сетевых запросов извне.

Создайте разрешающее FORWARD-правило, если:

- В таблице FORWARD есть запрещающее прохождение трафика правило. В этом случае поместите созданное правило выше запрещающего;
- Нужна проверка трафика профилями безопасности. В этом случае укажите в правиле нужные профили **Контроля приложений** или **Предотвращения вторжений**. Укажите при создании правила назначение (адрес устройства в локальной сети) и порт назначения.

Подсказка: Не рекомендуется использовать проброс портов для публикации веб- и почтовых серверов (80, 443 порты). Для их публикации воспользуйтесь *обратным прокси-сервером*.

Особенности создания правил DNAT в версии 18:

- В предыдущих версиях профили безопасности настраивались в отдельных разделах. В версии 18 ***Контроль приложений*** и система ***Предотвращения вторжений*** настраиваются в правилах **Файрвола**;
- Для проверки трафика модулем **Контроль приложений** и системой **Предотвращения вторжений** необходимо создать FORWARD-правило с включенными настройками профилей безопасности;
- В случае проблем с доступом до публикуемой службы проверьте **Отчеты и журналы -> События безопасности -> Журнал IPS** и при необходимости отредактируйте правила нужного профиля ***Предотвращения вторжений***.

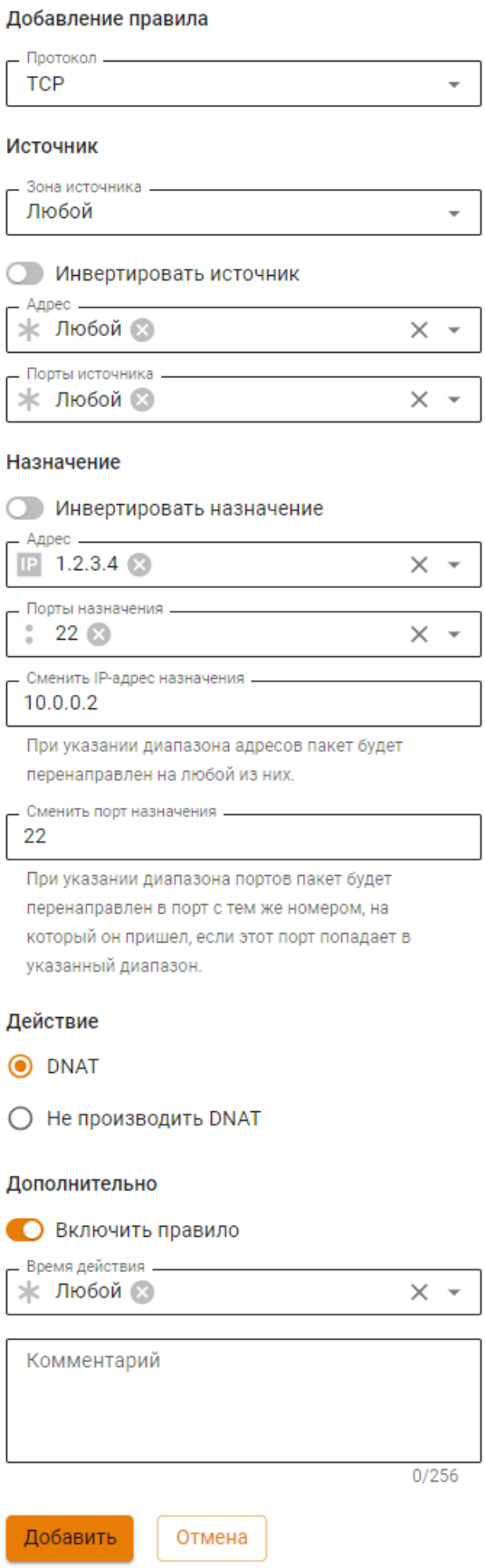
Создание правил DNAT и FORWARD в Файрволе Ideco NGFW:

Пример:

- Публичный адрес сервера Ideco - 1.2.3.4;
- Публикуемая служба - SSH, работающая на 22 TCP-порте;
- Адрес компьютера в локальной сети, где запущена служба, к которой нужен доступ извне - 10.0.0.2.

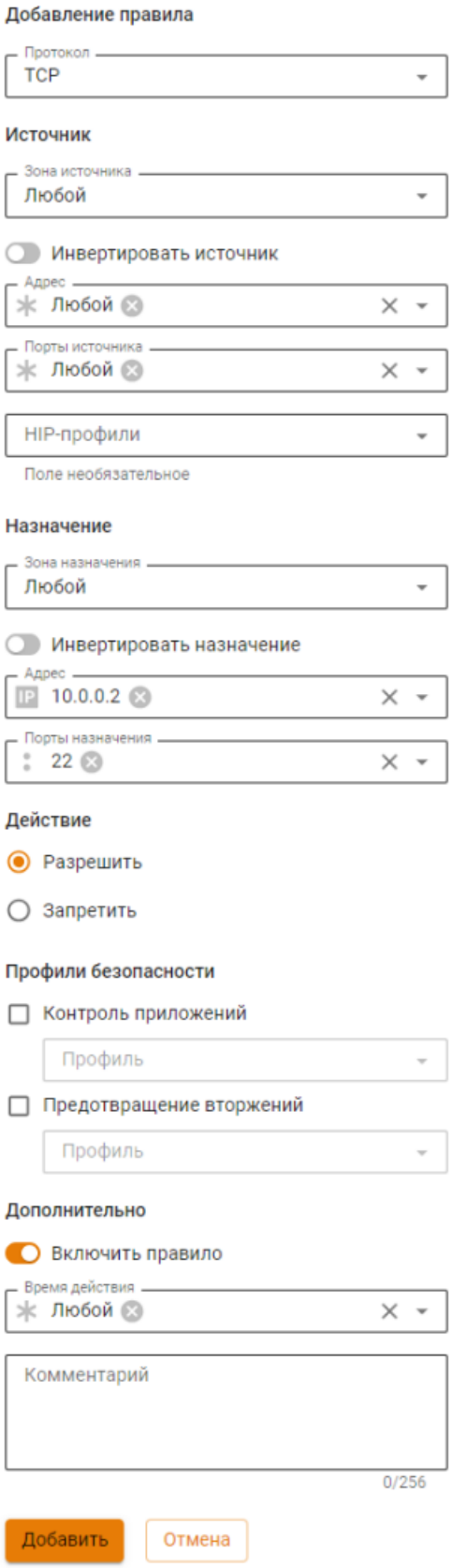
Для настройки трансляции запросов к службе извне через сервер Ideco NGFW на устройство в локальной сети перейдите в раздел **Правила трафика -> Файрвол -> DNAT** и нажмите **Добавить**.

Заполните поля в соответствии с характеристиками, указанными в примере:

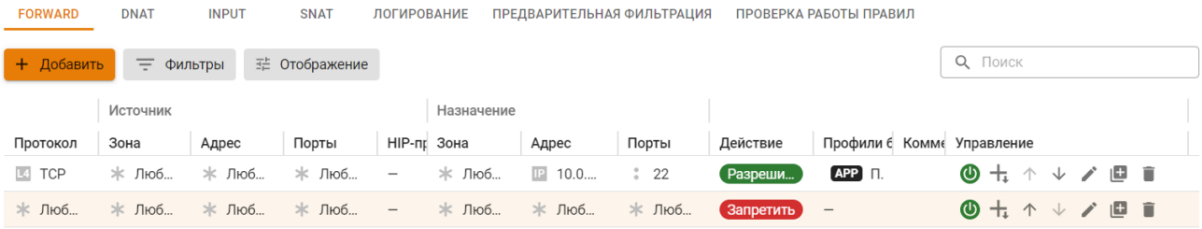


Вид правила в таблице после сохранения:

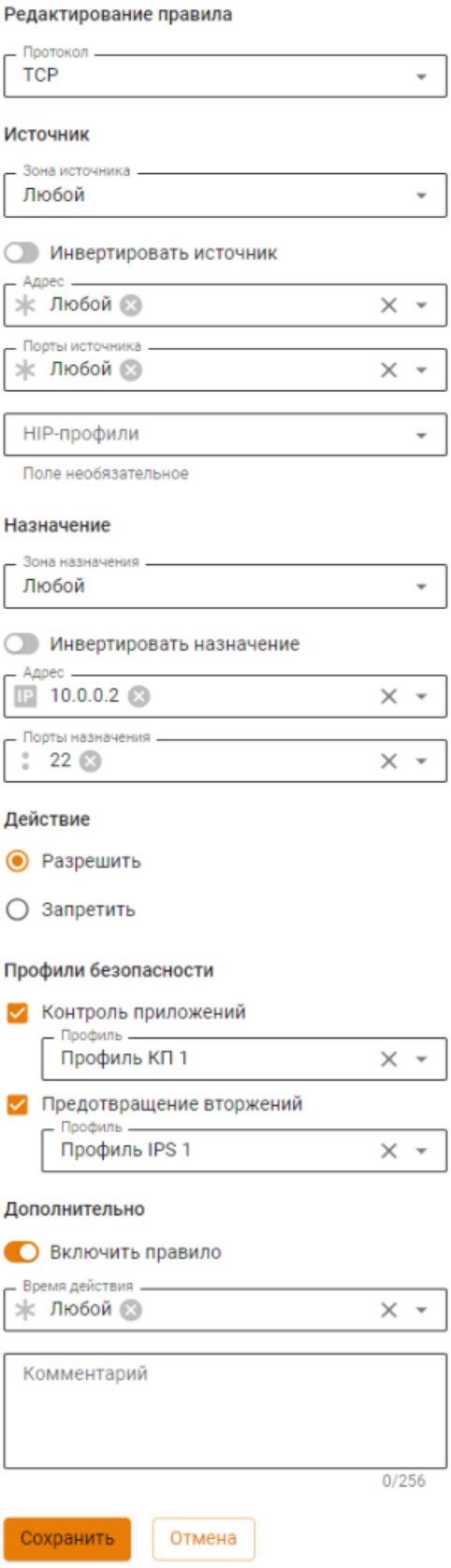
Проверьте наличие запрещающих правил в таблице FORWARD. При необходимости создайте правило, разрешающее трафик:



Поместите созданное правило выше запрещающего трафик:



Если вы хотите, чтобы трафик проверялся профилями безопасности, включите в созданном правиле соответствующие настройки:



Настройки **Файрвола** применяются сразу при создании правил.

Частые ошибки:

- Если включен режим **Разрешить интернет всем**, правила **Файрвола**, включая таблицу DNAT, не работают;

- Если в одной локальной сети находятся пользователи и сервер с опубликованным при помощи DNAT-правила ресурсом, вероятна асимметричная маршрутизация. Информация о способах устранения асимметричной маршрутизации трафика представлена в *статье*.

Рекомендации:

- Проверять работу правила DNAT следует из внешней сети. Если необходим доступ из локальной сети, используйте обратный прокси-сервер для публикации веб-ресурсов;
- Порт на внешнем интерфейсе сервера, с которого транслируются запросы, не всегда совпадает с публикуемым портом самой службы. Например, для предотвращения автоматических попыток подключения вредоносного ПО на популярный сервис внешние запросы транслируются на порт 4489, а в локальную сеть - на порт 3389;
- Для защиты от нежелательных подключений к публикуемой службе при создании правила укажите в поле **Источник** IP-адрес или подсеть, с которой разрешено подключаться к этой службе;
- Если осуществляется трансляция на один и тот же номер порта локального сервера, заполнять поле **Сменить порт назначения** не обязательно. Система автоматически переадресует запрос на соответствующий порт устройства в локальной сети.

Устранение неполадок:

- Убедитесь, что клиент, на которого осуществляется проброс портов, отвечает на эхо-запросы ping к внешним ресурсам. Основным шлюзом на данном устройстве следует указать локальный IP-адрес Ideco NGFW, либо прописать маршрут;
- При правильной настройке публикуемая служба отвечает клиенту во внешней сети через тот же внешний интерфейс сервера, с которого изначально пришел запрос. Настройте правильный адрес SNAT для опубликованного сервиса с помощью создания правил в таблице SNAT, если в созданном правиле в поле **Назначение** указан публичный IP-адрес сервера для приема подключений извне, а также в случае переопределения автоматических правил NAT;
- Правило трансляции запросов на сервере не работает, если брандмауэр Windows или другие программы защиты блокируют соединения с внешних адресов в интернете. Для диагностики убедитесь, что настройки встроенного брандмауэра Windows или сторонних файрволов и антивирусов разрешают целевое соединение. Например, для проверки настроек брандмауэра на устройстве Windows перейдите в **Панель управления -> Брандмауэр Защитника Windows -> Дополнительные параметры -> Правила для входящих подключений / Правила для исходящих подключений**;
- Правило портмаппинга пробрасывает трафик из внешней сети на хост в локальной сети. Трафик запроса ресурса из этой же локальной сети при обращении на внешний адрес не будет проброшен правильно. Во избежание асимметричной маршрутизации при диагностике сетевыми утилитами подключайтесь из внешних для NGFW сетей, а внутри локальной сети обращайтесь к сервису по его IP-адресу в локальной сети. Альтернативный вариант - вынесите ресурс в отдельную локальную сеть, DMZ и обращайтесь к ресурсу из локальной сети клиентов по внешнему IP-адресу.

23. Интеграция NGFW и SkyDNS

Подсказка: Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

23.1 Чем может быть полезна интеграция:

- **Защита от зараженных сайтов**. Вредоносные скрипты могут содержать сайты, как взломанные злоумышленниками, так и созданные специально для распространения вредоносного ПО.
- **Защита от бот-сетей**. Созданные из зараженных вредоносными программами компьютеров сети используются в DDoS-атаках на серверы, рассылках спама, похищениях паролей от интернет-банков и сервисов и в других целях. DNS-фильтрация ограничивает доступ к выявленным серверам для управления бот-сетями. В результате злоумышленники не смогут управлять компьютером, даже если он заражен вредоносной программой.
- **Защита от нежелательных сайтов**. SkyDNS фильтрует интернет-ресурсы по более чем 50 категориям, что повышает качество фильтрации нежелательного контента.
- **Соблюдение 436-ФЗ О защите детей от информации, причиняющей вред их здоровью и развитию**. Сервис SkyDNS полностью соответствует требованиям Правил подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети интернет Минобрнауки РФ.

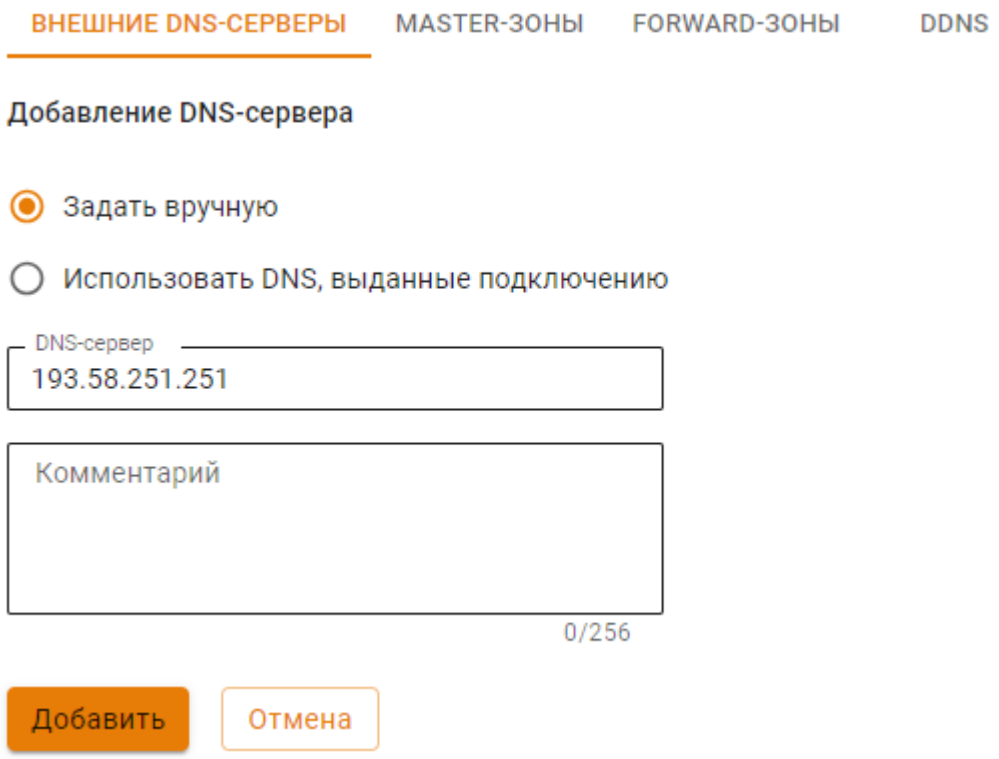
Подсказка: Специально для школ и колледжей можно приобрести комплект Шлюз безопасности Ideco NGFW + контент-фильтр SkyDNS.

23.2 Настройка интеграции Ideco NGFW и SkyDNS

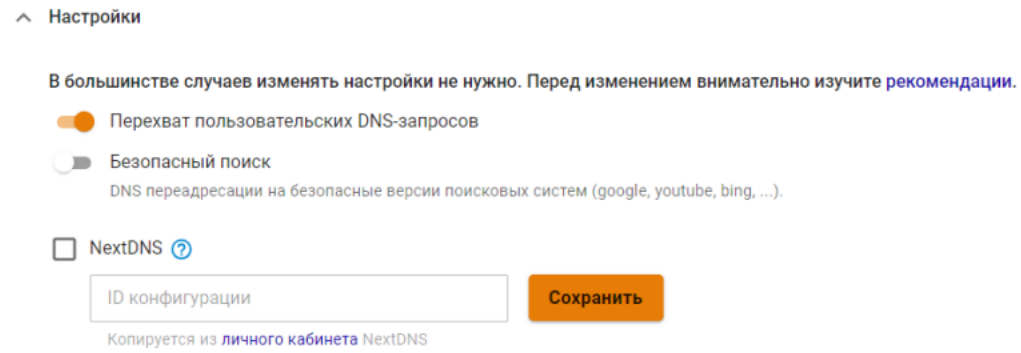
Чтобы настроить интеграцию со SkyDNS, выполните действия:

1. Перейдите в раздел **Сервисы -> DNS -> Внешние DNS-серверы** и нажмите **Добавить**.

2. Выберите пункт **Задать вручную** и в поле **DNS-сервер** введите IP-адрес DNS-сервера SkyDNS (`193.58.251.251`) и нажмите **Добавить**:

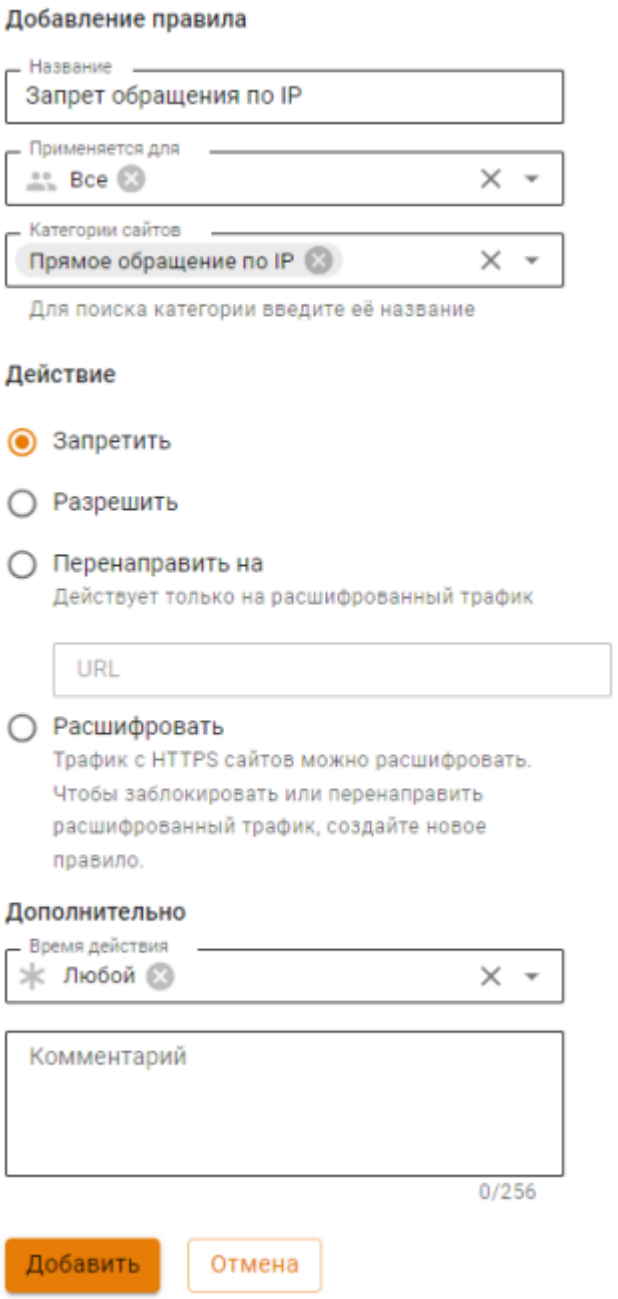


3. В настройках DNS включите опцию **Перехват пользовательских DNS-запросов** для запрета обращения к другим DNS-серверам (если фильтрация через SkyDNS обязательна для всей сети):



4. Если внутри локальной сети или внутри сети провайдера есть внутренняя DNS-зона, не обслуживаемая внешними DNS-серверами (например, домен Active Directory), укажите ее в разделе **DNS -> FORWARD-ЗОНЫ**.

5. Перейдите в раздел **Правила трафика -> Контент-фильтр** и создайте правило запрета прямого обращения к сайтам по IP-адресу:



6. Пропишите IP-адрес локального интерфейса Ideco NGFW в качестве единственного DNS-сервера в сетевых настройках на всех устройствах, которые требуется защитить.

Подсказка: Пользователи, получающие адреса автоматически через DHCP-сервер Ideco NGFW или подключающиеся по VPN, получают нужные настройки автоматически.

Чтобы исключить некоторые компьютеры из фильтрации, пропишите на них другой внешний DNS-сервер (например, 8.8.8.8) и не включайте **Перехват пользовательских DNS-запросов**.

---

7. При наличии у Ideco NGFW статического белого IP-адреса привяжите этот адрес к аккаунту SkyDNS в личном кабинете на сайте SkyDNS (в разделе **Настройки -> Сети**).

8. Настройте запрет доступа к сайтам по категориям безопасного поиска и другие сервисы в личном кабинете на сайте SkyDNS.

23.3 Документация по настройке и активации сервиса SkyDNS

Документация доступна на сайте сервиса.

По вопросам настройки сервиса обращайтесь в техническую поддержку SkyDNS.

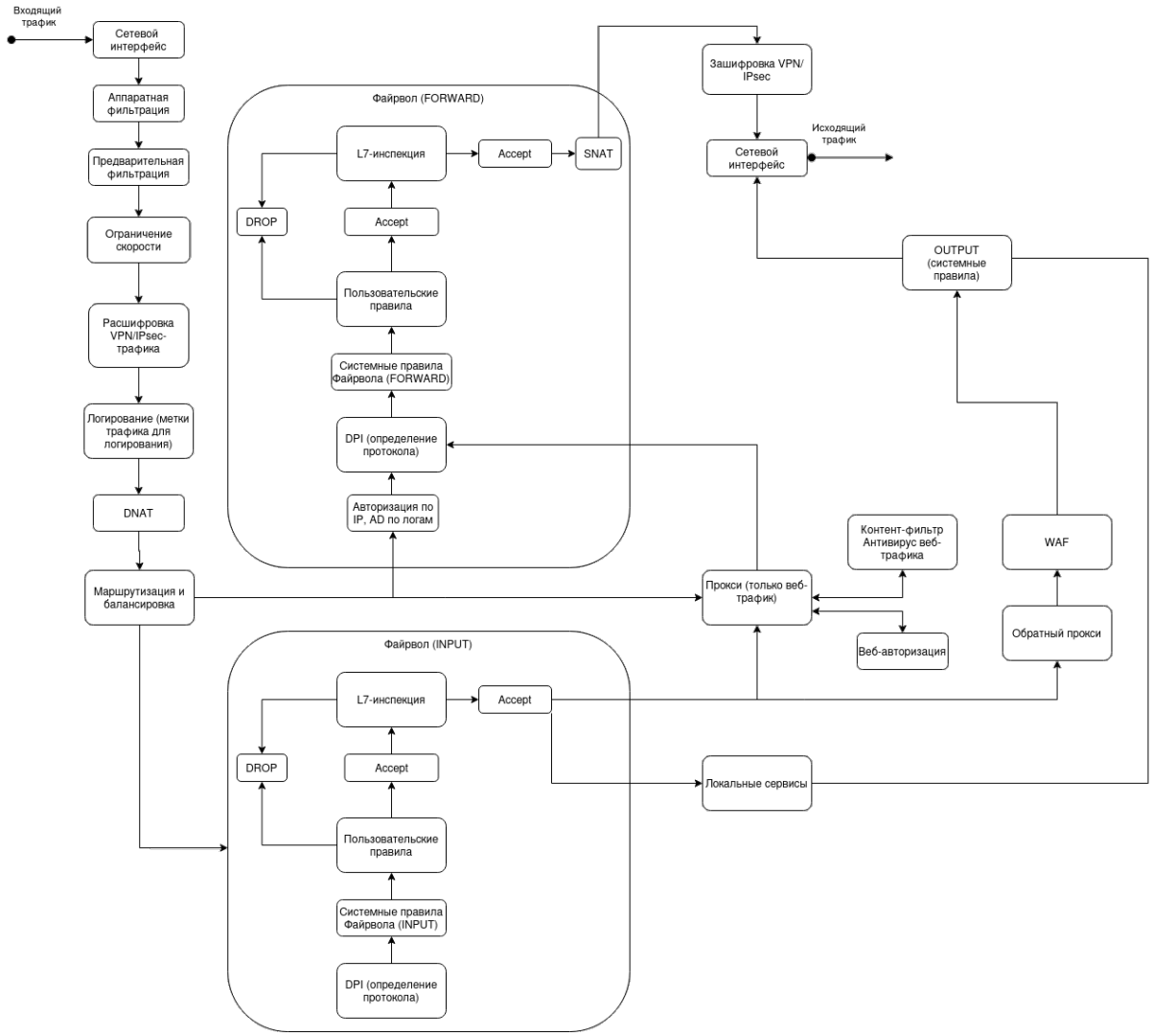
23.4 Схема фильтрации веб-трафика при использовании SkyDNS

24. Полный цикл обработки трафика в Ideco NGFW

Статья описывает цикл, который проходят пакеты трафика в Ideco NGFW, в зависимости от сценария.

Обработку трафика условно можно разделить на три стадии:

- Предварительная;
- Файрвол;
- Завершающая.



К **Предварительной стадии** можно отнести *Аппаратную* и *Предварительную* фильтрацию, *Ограничение скорости*, расшифровку VPN/IPsec-трафика. Также на этой стадии трафик помечается для логирования, если он подпадает под правило в разделе **Файрвол -> *Логирование***. После этого при необходимости у пакета подменяется IP-адрес назначения (DNAT), он проходит маршрутизацию и балансировку.

На второй стадии трафик проходит либо таблицу **INPUT**, либо таблицу **FORWARD** ***Файрвола***:

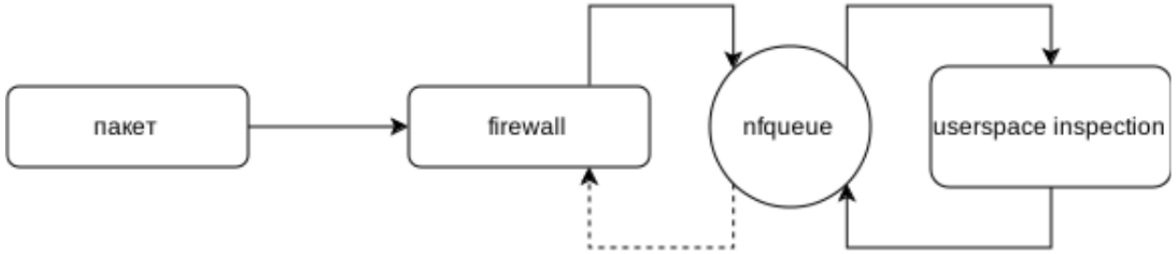
- В первом случае - одно из двух:
  - Трафик проходит таблицу **INPUT** (системные и пользовательские правила, L7-фильтрацию) и направляется в локальные сервисы NGFW (например, DNS, NTP);
  - Трафик направляется в **Прокси** или **Обратный прокси**, обрабатывается соответствующими модулями и направляется в таблицу **FORWARD** (от **Прокси**) или в **OUTPUT** (от **Обратного прокси**).
- Во втором случае трафик проходит таблицу **FORWARD** (системные и пользовательские правила, L7-фильтрацию).

На **Завершающей стадии** трафик после обработки зашифровывается (при необходимости) и направляется получателю.

24.1 Принцип работы L7-инспекций

Трафик на обработку *Предотвращением вторжений* и *Контролем приложений* из Файрвола передается через NFQUEUE.

NFQUEUE - это технология интеграции файрвола linux с userspace-процессами, выполняющими инспекцию. Она позволяет выполнять L7-инспекции после L3-правил **Файрвола**:



24.2 Примеры прохождения трафика

24.2.1 Транзит трафика с фильтрацией и прозрачным прокси

1. Трафик пользователя попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию, Ограничение скорости (если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет).

2. Если пользователь подключился через VPN, трафик будет расшифрован.

3. Будет проверена DNAT-талица **Файрвола**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

4. Веб-трафик направляется в **Прокси** для веб-авторизации, проверки **Контент-фильтром** и **Антивирусом веб-трафика**.

5. Трафик направляется в **FORWARD**-таблицу **Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, Контроль приложений).

6. Трафик проверяется на соответствие правилам таблицы **SNAT**. При необходимости подменяется IP-адрес источника.

7. Если пользователь подключился через VPN, трафик будет зашифрован.

24.2.2 Прямое подключение к прокси

1. Трафик пользователя попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию, Ограничение скорости (если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет).

2. Будет проверена DNAT-талица **Файрвола**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT**, веб-трафик оттуда захватывается **Прокси**, где обрабатывается **Контент-фильтром** и **Антивирусом веб-трафика**. Пользователь проходит веб-авторизацию (если она настроена).

4. Трафик направляется в **FORWARD**-таблицу **Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, Контроль приложений).

5. Запрос направляется ресурсу, на который обратился пользователь, ответ направляется пользователю (трафик вновь проходит п. 1 - п. 4).

24.2.3 Публикация ресурсов через обратный прокси

1. Трафик из внешней сети попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию (если трафик подпадает под их правила, то он может быть заблокирован и дальше не пойдет).

2. Будет проверена DNAT-талица **Файрвола**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

3. Трафик направляется в таблицу **INPUT Файрвола**:

- Если трафик подпадает под запрещающее правило, он блокируется;
- Если трафик подпадает под разрешающее правило, он направляется на L7-инспекцию (Предотвращение вторжений, Контроль приложений).

3. Трафик попадает в **Обратный прокси**, где проходит через **Web Application Firewall**. Если трафик подпадает под правила WAF, он может быть отброшен.

4. Трафик направляется ресурсу в локальной сети, который был опубликован через **Обратный прокси**, и возвращает ответ.

24.2.4 Разрешить интернет всем

1. Трафик пользователя попадает на Ideco NGFW, проходит Аппаратную и Предварительную фильтрацию, Ограничение скорости (если трафик подпадает под их правила - он может быть заблокирован и дальше не пойдет).

2. Если пользователь подключился через VPN, трафик будет расшифрован.

3. Будет проверена DNAT-талица **Файрвола**: если трафик подпадет под правила - IP-адрес или порт назначения будет заменен.

4. Трафик, минуя стадию авторизации, пройдет таблицу **FORWARD** и не будет отброшен вне зависимости от созданных там правил фильтрации.

25. О личном кабинете MY.IDECO

MY.IDECO - это личный кабинет, где вы можете использовать все возможности Ideco NGFW: скачать дистрибутив, добавить лицензию, привязать телеграм-аккаунт к мониторинг-боту и получать мгновенные уведомления о работе Ideco NGFW и многое другое.

25.1 Возможности Ideco NGFW:

- Управлять лицензированием серверов
- Скачивать дистрибутивы
- Привязывать телеграм-аккаунт для получения уведомлений о состоянии работы серверов
- Добавлять компании в учетную запись для управления лицензированием
- Добавлять пользователей в компанию для управления лицензированием
- Настраивать авторизацию в MY.IDECO через социальные сети

26. NGFW

26.1 Лицензирование

Подсказка: Подробнее о видах лицензий в статье *Лицензирование*.

Посмотреть информации о сервере и лицензии можно в разделе **NGFW -> Лицензирование**, нажав на иконку 👁 напротив нужного сервера.

Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др.

26.1.1 Добавление коммерческой (Enterprise) лицензии

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

2. Перейдите в личный кабинет MY.IDECO в раздел **NGFW -> Лицензирование** и нажмите **Добавить коммерческую лицензию**.

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

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

26.1.2 Добавление FREE (бесплатной) лицензии

Для добавления FREE-лицензии нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Свободные лицензии**.

26.1.3 Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн. Онлайн проводится только в MY.IDECO. Офлайн потребует доступ к веб-интерфейсу сервера.

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

- Одна лицензия может быть привязана только к одному серверу;
- Демо-лицензию нельзя привязать к другому серверу;
- Демо-лицензию нельзя повторно получить на одну и ту же инсталляцию сервера;
- При удалении сервера с демо-лицензией также удаляется и лицензия.

Онлайн

Выберите удобный вариант привязки:

- На вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения, нажав **Привязать лицензию**.
- На вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

Офлайн

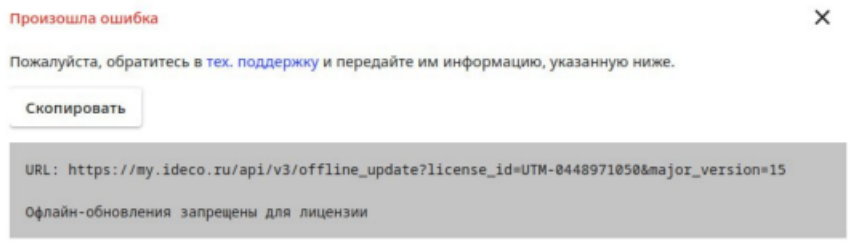
1. Для предоставления офлайн-лицензии обратитесь к менеджеру.

2. Привяжите предоставленную лицензию к серверу:

- На вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения, нажав **Привязать лицензию**.
- На вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

Пример наименования сервера для **офлайн**-регистрации: `UTM (UTM Unknown)`

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

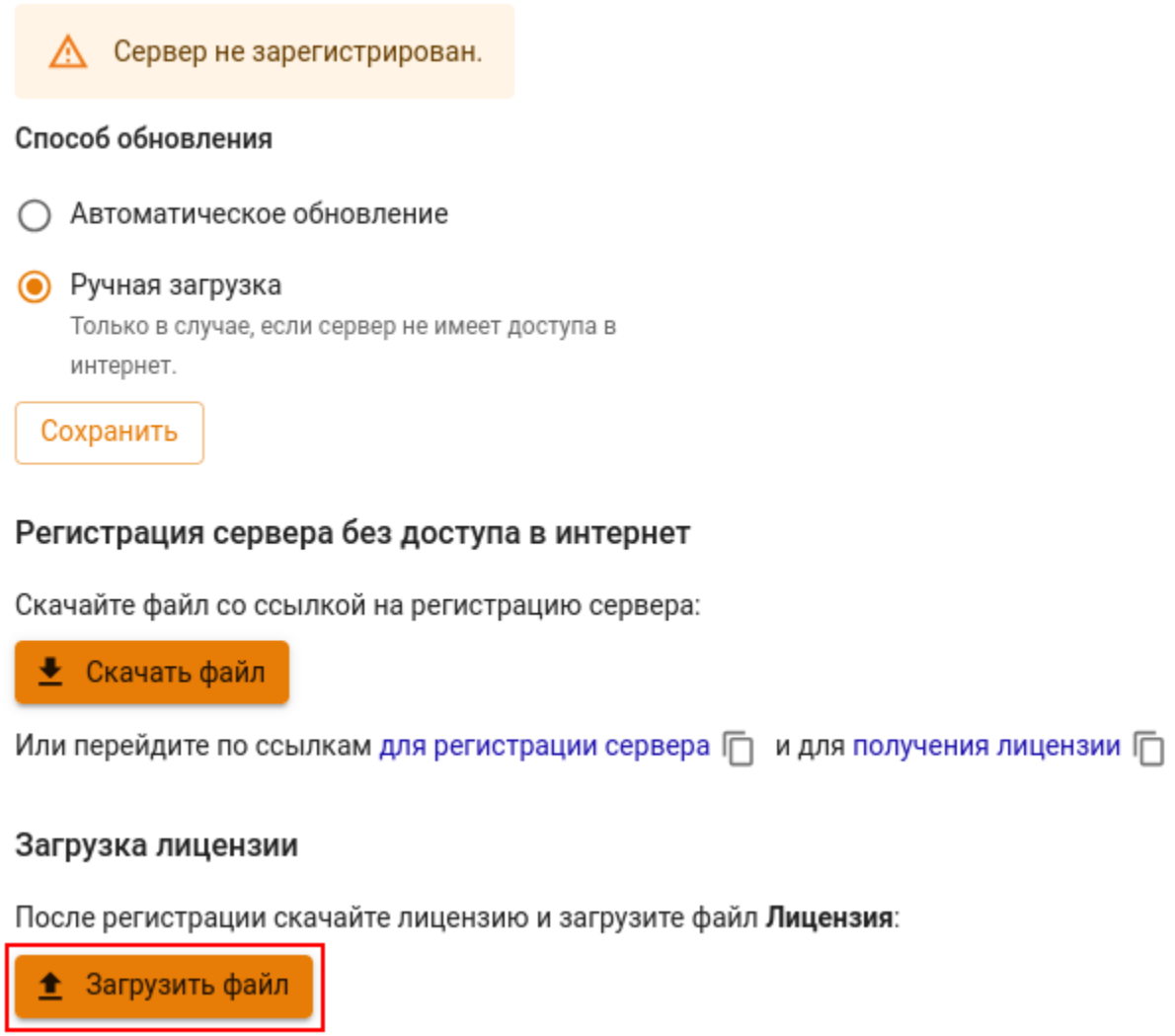


3. Напротив названия сервера нажмите , вставьте ссылку, скопированную в веб-интерфейсе Ideco NGFW в разделе **Управление сервером -> Лицензия**.

4. Скачайте файлы, нажав на соответствующие ссылки в открывшейся форме.

Помимо информации о лицензии в личном кабинете представлены файлы для обновления баз модулей безопасности. Подробнее о процессе обновления в статье *Регистрация сервера*.

5. В веб-интерфейсе Ideco NGFW перейдите в раздел **Управление сервером -> Лицензия** и загрузите файл с лицензией, скачанный в пункте 4:



26.2 Скачать

Вкладка содержит установочные файлы последних версий разработанных компанией «Айдеко» программных продуктов и их краткое описание.

26.3 Online-демо

Чтобы ознакомиться с демоверсией Ideco NGFW, перейдите в раздел **NGFW -> Online-демо** личного кабинета MY.IDECO. Перейдите по ссылке **Реквизиты для доступа на демо-сайт** и введите логин `administrator` и пароль `servicemode`.

Демоверсия Ideco NGFW всегда равна последней реализованной версии. Учетная запись, доступная по логину и паролю выше, имеет права только на просмотр интерфейса. Если необходима учетная запись с правами на редактирование, обратитесь в отдел продаж.

27. Monitoring Bot и Security

27.1 Monitoring Bot

Ideco Monitoring Bot присылает уведомления о событиях в Ideco NGFW (уведомления из колокольчика).

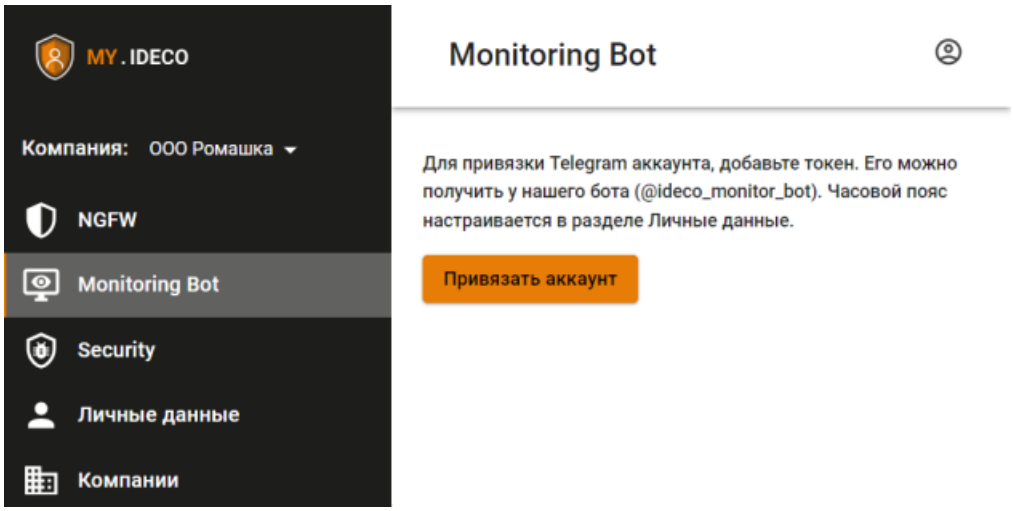
Бот может отправлять оповещения:

- в личные сообщения;
- в беседы, где 2 и более пользователей (groups).

27.1.1 Привязка Ideco Monitoring Bot

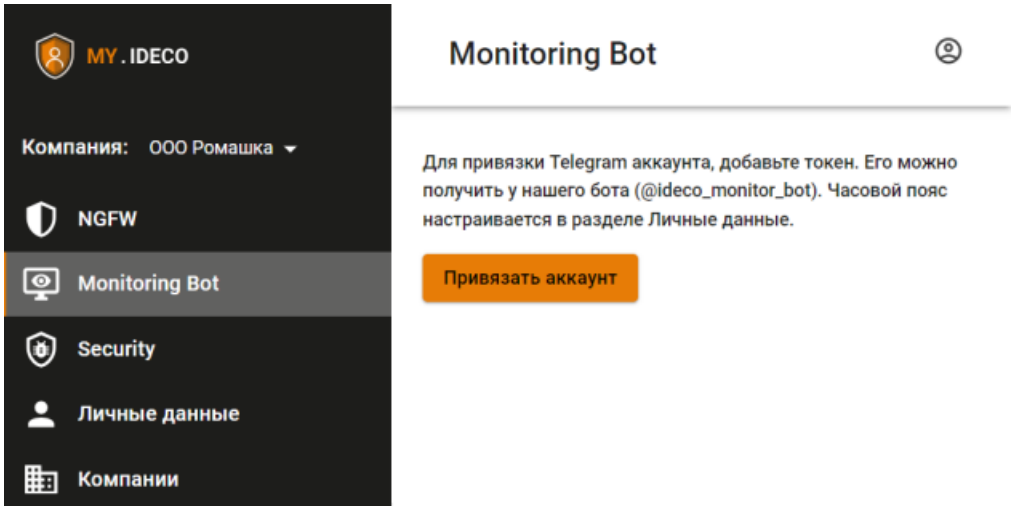
Настройка привязки Ideco Monitoring Bot к одному пользователю:

1. Настроить интернет на Ideco NGFW.
2. *Привязать лицензию* к серверу.
3. Перейти к диалогу с ботом: @ideco_monitor_bot.
4. Написать боту `/start`.
5. Скопировать код привязки к аккаунту.
6. Перейти в раздел **Ideco Monitoring Bot** в личном кабинете.
7. Нажать на кнопку **Привязать аккаунт**.
8. Ввести код в соответствующее поле и нажать на кнопку **Привязать**.



Настройка привязки Ideco Monitoring Bot к беседе:

1. Настроить интернет на Ideco NGFW.
2. *Привязать лицензию* к серверу.
3. Перейти в группу и добавить пользователя @ideco_monitoring_bot.
4. Написать `/start` в группе.
5. Скопировать код привязки к аккаунту.
6. Перейти в раздел **Ideco Monitoring Bot**.
7. Нажать на кнопку **Привязать аккаунт**.
8. Ввести код в соответствующее поле и нажать на кнопку **Привязать**.



Подсказка: При настройке подключения Ideco Monitoring Bot к беседе нельзя использовать подсказки для команд, поскольку требуется ввод команды `/start` вручную.

Подсказка: Уведомления начнут приходить в сообщения привязанного аккаунта.

27.1.2 Настройка оповещений Ideco Monitoring Bot

Настройте оповещения, которые приходят от Ideco Monitoring Bot, для каждой отдельной беседы.

Для настройки оповещений:

1. Перейдите в раздел Ideco Monitoring Bot в личном кабинете и нажмите на иконку .

2. Выберите уведомления, которые хотели бы получать в выбранной беседе.

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

27.2 Security

Онлайн-сервис для проверки защиты сетевого периметра, оценки текущего уровня защиты и возможности повышения уровня защиты.

Сервис проверит:

- Есть ли доступ через используемый браузер к сайтам из 15 потенциально опасных категорий;
- Возможность проникновения тестовых образцов вирусов и эксплойтов;
- Открытые порты и ответы сервисов на внешнем интерфейсе вашего интернет-шлюза;
- Торренты, скачанные из сети за последний месяц;
- Есть ли ваш IP-адрес в черных списках зараженных хостов;
- Наличие пароля к почте в известных базах данных хакеров.

Подсказка: Чтобы оценить эффективность работы служб фильтрации и повысить уровень безопасности, рекомендуем ознакомиться с нашей статьей о сервисе *Security Ideco*.

28. Личные данные и Компании

В разделах меняются данные учетной записи, добавляются компании для управления в них лицензиями и пользователи для управления компаниями

28.1 Личные данные

Информация о профиле:

- E-mail - почта, используемая для авторизации;
- Телефон - телефон для звонков по вопросам продления лицензии;
- Временная зона - временная зона региона, в котором находится пользователь. Monitoring Bot будет указывать время в уведомлениях у учетом этой временной зоны.

Авторизация через социальные сети:
При добавлении авторизации через аккаунт социальной сети система получит доступ к имени, адресу электронной почты, языковым настройкам и фото профиля аккаунта.

Смена пароля:
Для смены пароля укажите старый и новый пароль.

28.2 Компании

Раздел содержит информацию о пользователях, добавленных в компанию, и настройки компании.

28.2.1 Добавление компании

Для добавления компании нажмите **Добавить компанию**, заполните название компании, выберите количество пользователей и нажмите **Создать**.

Способы переключения между компаниями:

- В разделе **Компании** в раскрывающемся списке;
- В левом верхнем углу по кнопке ▼.

Чтобы изменить название и количество пользователей, перейдите в **Настройки компании**:

В правой части экрана измените необходимые параметры и нажмите **Сохранить**.

28.2.2 Добавление пользователей

Для добавления пользователя в компанию нажмите **Добавить пользователя**, укажите e-mail и нажмите **Добавить**.

Если у добавляемого пользователя нет учетной записи в MY.IDECO, то на указанную при добавлении электронную почту отправится письмо со ссылкой-приглашением. При переходе по ссылке откроется страница входа в MY.IDECO.

Для задания пароля потребуется нажать **Забыли пароль?** и пройти процедуру восстановления пароля, перейдя по ссылке из отправленного письма.

29. Об Ideco Center

29.1 Основное

Подсказка: Название службы раздела **Ideco Center**: `ideco-central-console-backend`.
Список служб для других разделов доступен по *ссылке*.

Ideco Center - это центральная консоль, которая поможет в администрировании нескольких серверов Ideco NGFW. На данный момент не требует лицензирования и не имеет ограничений к использованию. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW, даже если они были подключены после того, как политики были настроены.

Возможности Ideco Center:

- Централизованное управление серверами, подключенными к Ideco Center, с возможностью группировки Ideco NGFW и формирования иерархии из этих групп для совместного управления;
- Создание правил политик безопасности и объектов, которые одновременно переносятся в серверы Ideco NGFW определенной группы. В частности - создание пользовательских категорий контент-фильтра;
- Переход из Ideco Center в веб-интерфейс подключенных Ideco NGFW. Администраторы Ideco Center имеют доступ к подключенными NGFW, но администраторы подключенных NGFW не имеют доступ к Ideco Center.
- Обновление подключенных к Ideco Center NGFW;
- Управление правами доступа администраторов серверов NGFW.

Подсказка: Подробнее о работе политик безопасности и объектов - в статье *Политики и объекты*.

Источники обновления данных для Ideco Center:

Ideco Center получает обновления из следующих источников:

- Отсылка уведомлений в личный кабинет/телеграм-бот: alerts.v17.ideco.dev;
- Обновление баз **Контент-фильтра**: content-filter.v17.ideco.dev;
- Отсылка анонимной статистики: gatherstat.v17.ideco.dev;
- Обновления баз GeoIP: ip-list.v17.ideco.dev;
- Отправка отчетов по почте: send-reports.v17.ideco.dev;
- Обновления системы: sysupdate.v17.ideco.dev;
- Синхронизация времени: ntp.ideco.ru.

Кроме того, часть запросов к указанным выше серверам может быть перенаправлена на mcs-vm.ideco.ru, update.ideco.ru, storage.yandexcloud.net.

Подсказка: Для корректной работы всех модулей фильтрации Ideco Center необходимо, чтобы доступ к вышеуказанным ресурсам, был разрешен настройками фильтрации.

---

30. Установка Ideco Center

Технические требования для серверов и виртуальных машин:

Комплектующие	Минимальные системные требования
Процессор	Intel i3/i5/i7/i9/Xeon с поддержкой SSE 4.2
Объем оперативной памяти	16 ГБ (16-64 ГБ в зависимости от количества пользователей)
Дисковая подсистема	SSD объемом 150 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe
Сеть	Одна сетевая карта. Рекомендуется использовать карты на чипах Intel
Гипервизоры	VMware, Microsoft Hyper-V (виртуальные машины 2-го поколения), VirtualBox, KVM, Citrix XenServer, Proxmox VE
Дополнительно	Монитор и клавиатура
Замечания	Обязательна поддержка UEFI. Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет). Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти

Подсказка: Обязательные условия для работы с Ideco Center:

1. Обязательная поддержка UEFI;
2. Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти;
3. Отключить режим Legacy загрузки, он может называться CSM (Compatability Support Module);
4. Отключить опцию Secure Boot в UEFI.

Файл для установки центральной консоли доступен для скачивания в личном кабинете. Процесс установки Ideco Center аналогичен *процессу установки Ideco NGFW*.

30.1 Процесс установки

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

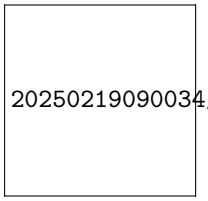
Для установки Ideco Center выполните действия:

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

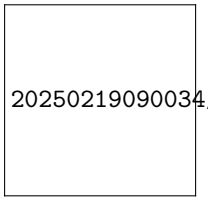
2. Выберите диск для установки и ознакомьтесь с **предупреждением об уничтожении данных на диске**:

```
Установка Ideco CC 16.0 сборка 647
----------------------------------

Для установки выбран диск '161 ГБ - Noname (Unknown)'.
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 вы находитесь:



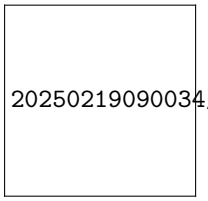
4. Настройте дату и время в соответствии с вашей временной зоной. **Обязательно проверьте правильность даты и времени**:



Подсказка: Не забудьте извлечь USB диск после установки Ideco Center, чтобы загрузка с USB диска не началась заново.

30.2 Создание учетной записи администратора

Для входа в веб-интерфейс Ideco Center нужно создать учетную запись администратора с соблюдением требований к паролю:



Требования к паролю:

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

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

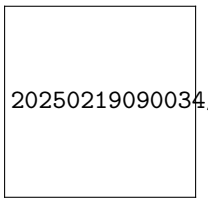
Не используйте Numpad при введении пароля, поскольку в будущем это может привести к проблемам при авторизации администратора.

30.3 Настройка локального интерфейса

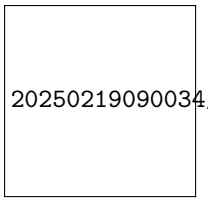
Подсказка: При использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса. Для корректной идентификации сетевой карты используйте ее MAC-адрес.

Для настройки Ideco Center через веб-интерфейс нужно настроить локальный интерфейс в локальном меню:

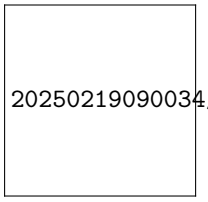
1. Введите номер сетевого адаптера, который будет использоваться в качестве локального сетевого интерфейса:



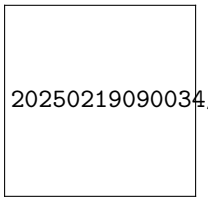
2. Настройте локальную сеть автоматически через DHCP, введя **y**, или настройте вручную, введя **n**:



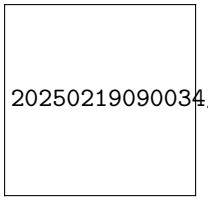
3. Введите локальный IP-адрес и маску подсети в формате `ip/маска` и нажмите **Enter**:



4. Введите адрес шлюза или оставьте поле пустым:



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



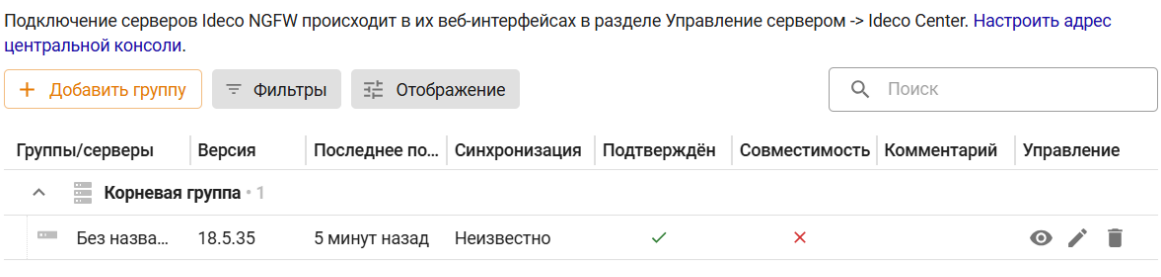
20250219090034/docsUTM/.gitbook/assets/installation-process11.png

После создания локального интерфейса откроется локальное меню управления:

```
Управление сервером

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

31. Серверы

Внимание: При синхронизации Ideco Center и Ideco NGFW с разными мажорными версиями передача правил с Ideco Center происходить не будет. При этом в разделе **Серверы** будет информация о том, что Ideco Center и Ideco NGFW несовместимы:



В разделе **Серверы** можно группировать синхронизированные с ней серверы NGFW и формировать из них древовидную структуру. Это позволит управлять сразу несколькими серверами, применять правила и политики безопасности ко всем серверам определенной группы.

Предупреждение: Особенности работы:

- Если в подключаемом Ideco NGFW используется кластер, достаточно подключить только активную ноду, пассивная автоматически примет эту настройку;
- Сетевое подключение производится в направлении от Ideco NGFW к Ideco Center, т. е. возможна связь и когда Ideco NGFW за NAT;
- Если сервер Ideco Center находится за NAT, укажите IP-адрес NAT-устройства или доменное имя в разделе **Управление сервером -> Дополнительно -> Адрес Ideco Center**;
- Для обновления серверов, подключенных к Ideco Center, перейдите в интерфейс NGFW одним из указанных выше способов и воспользуйтесь статьей *Обновления*;
- Для подключения нескольких Ideco NGFW к Ideco Center рекомендуем настроить VPN-подключение через IPsec. Альтернативный способ - создать правило DNAT в веб-интерфейсе Ideco NGFW.

Портмаппинг при подключении Ideco NGFW к Ideco Center:

Если между офисами отсутствует VPN-подключение, для подключения нескольких Ideco NGFW к Ideco Center можно настроить проброс портов. Вместо подключения по IPsec в этом случае настраивается перенаправление портов.

Чтобы выполнить настройку, необходимо создать два одинаковых правила для протоколов **UDP** и **TCP** в разделе **Правила трафика -> Файрвол -> DNAT**:

Добавление правила

Протокол
UDP

Источник

Зона источника
Любой

Инвертировать источник

Адрес
Любой

Порты источника
Любой

Назначение

Инвертировать назначение

Адрес
Внешний IP NGFW

Порты назначения
3151

Сменить IP-адрес назначения
192.168.10.10

При указании диапазона адресов пакет будет перенаправлен на любой из них.

Сменить порт назначения

При указании диапазона портов пакет будет перенаправлен в порт с тем же номером, на который он пришел, если этот порт попадает в указанный диапазон.

Действие

DNAT

Не производить DNAT

Дополнительно

Включить правило

Время действия
Любой

Комментарий

0/256

Добавить Отмена

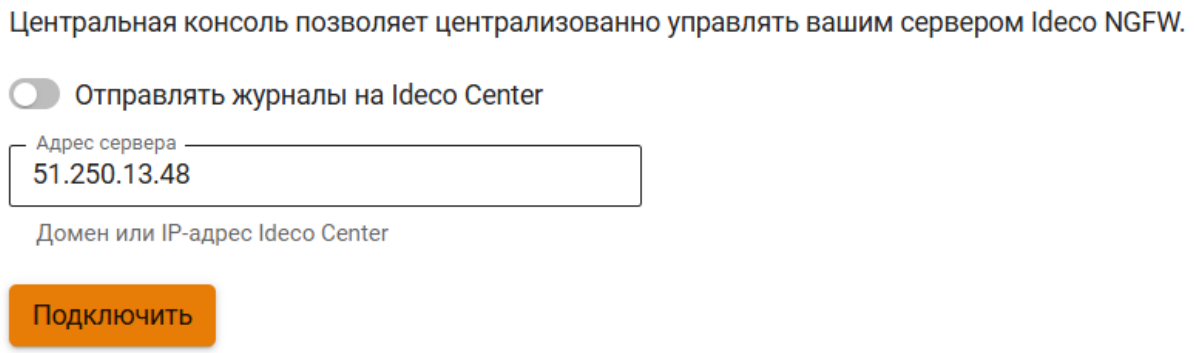
- **Назначение источника** - внешний IP-адрес Ideco NGFW;
- **Сменить IP-адрес назначения** - внутренний IP-адрес Ideco Center;
- **Порт** - только порт 3151.

При применении настроенного правила трафик проходит в локальную сеть через внешний интерфейс и перенаправляется в Ideco Center. При получении трафика Ideco Center отправляет подтверждение.

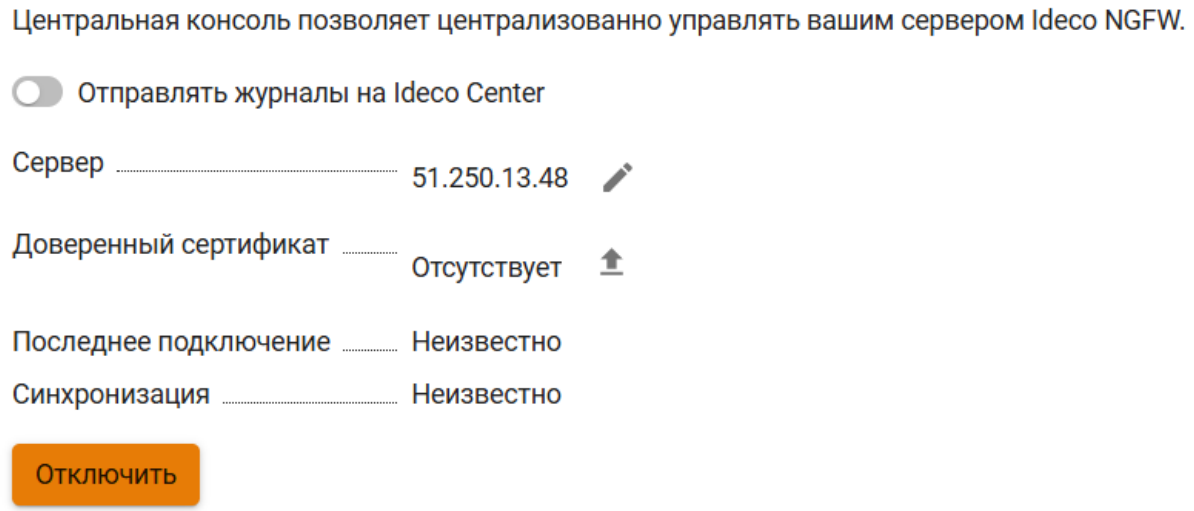
Подключение Ideco NGFW к Ideco Center:

1. Перейдите в раздел **Управление сервером -> Ideco Center**;

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

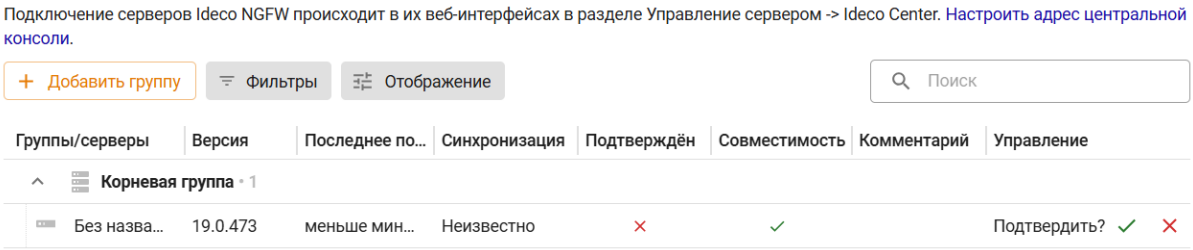


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW:



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

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



Для удаления сервера Ideco NGFW из Ideco Center разорвите привязку в интерфейсе Ideco Center:

Для этого в таблице **Серверы** в столбце **Управление** напротив нужного сервера выберите  и подтвердите выбор.

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

В Ideco Center предусмотрено два способа перехода в Ideco NGFW:

1. Перейдите в раздел **Серверы** и нажмите на  . В новой вкладке откроется веб-интерфейс Ideco NGFW:

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

Подсказка: При переходе из Ideco Center в веб-интерфейс Ideco NGFW внутри иконки ⊛ в шапке блокируются кнопки **Профиль** и **Выход**.

Подсказка: Чтобы перейти к веб-интерфейсу VCE подключенных серверов в Ideco Center, выполните следующие действия:

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

2. Затем следуйте инструкциям из *статьи*.

31.2 Группировка серверов Ideco NGFW

Структура групп серверов в Ideco Center предполагает три уровня вложенности. Первый - Корневая группа. В нее по умолчанию попадают все серверы NGFW, впервые синхронизированные с Ideco Center, а также все группы, созданные администратором.

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

Подсказка: Серверы NGFW, подключенные к Ideco Center, и группы по умолчанию, созданные в центральной консоли, являются частью **корневой группы** и не могут быть вынесены оттуда.

31.2.1 Создание, редактирование и удаление групп серверов

Создание группы серверов:

1. Перейдите в раздел **Серверы** и нажмите **Добавить группу**.

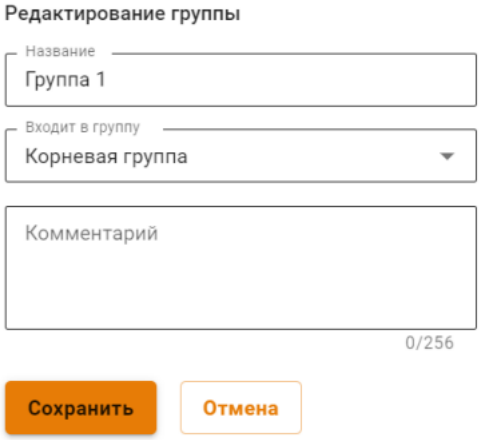
2. В открывшемся окне заполните **Название группы** и выберите родительскую группу из раскрывающегося списка (если это первая создаваемая группа, в нем будет только Корневая группа):

3. Нажмите **Сохранить**.

Редактирование группы серверов:

1. Нажмите на  напротив ее названия.

2. В открывшемся окне можно изменить 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):

31.2.2 Перемещение серверов Ideco NGFW между группами

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

1. Нажмите на напротив ее названия.

2. В открывшемся окне из раскрывающегося списка выберите группу, в которую хотите переместить сервер:

> **Предупреждение:** При подключении к Ideco Center сервера, настройки которого *восстановлены* из бэкапа другого сервера, такой клон не появится в таблице серверов Ideco Center. Возникает конфликт с донором бэкапа из-за одинакового claster_id.
>
> В случае возникновения такой проблемы обратитесь в *Техническую поддержку*.

32. Мониторинг

В этом разделе можно настроить интеграцию с системами SNMP или Zabbix для мониторинга устройств и систем.

32.1 SNMP

Подсказка: Для перевода раздела в рабочий режим переключите опцию в положение **Включен**.

Протокол SNMP позволяет осуществлять мониторинг устройств и систем. С помощью протокола SNMP передается информация:

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

Подсказка: На сервере, с которым будет осуществляться соединение по SNMPv3, укажите алгоритмы Auth Algorithm MD5 и Crypto Algorithm AES.

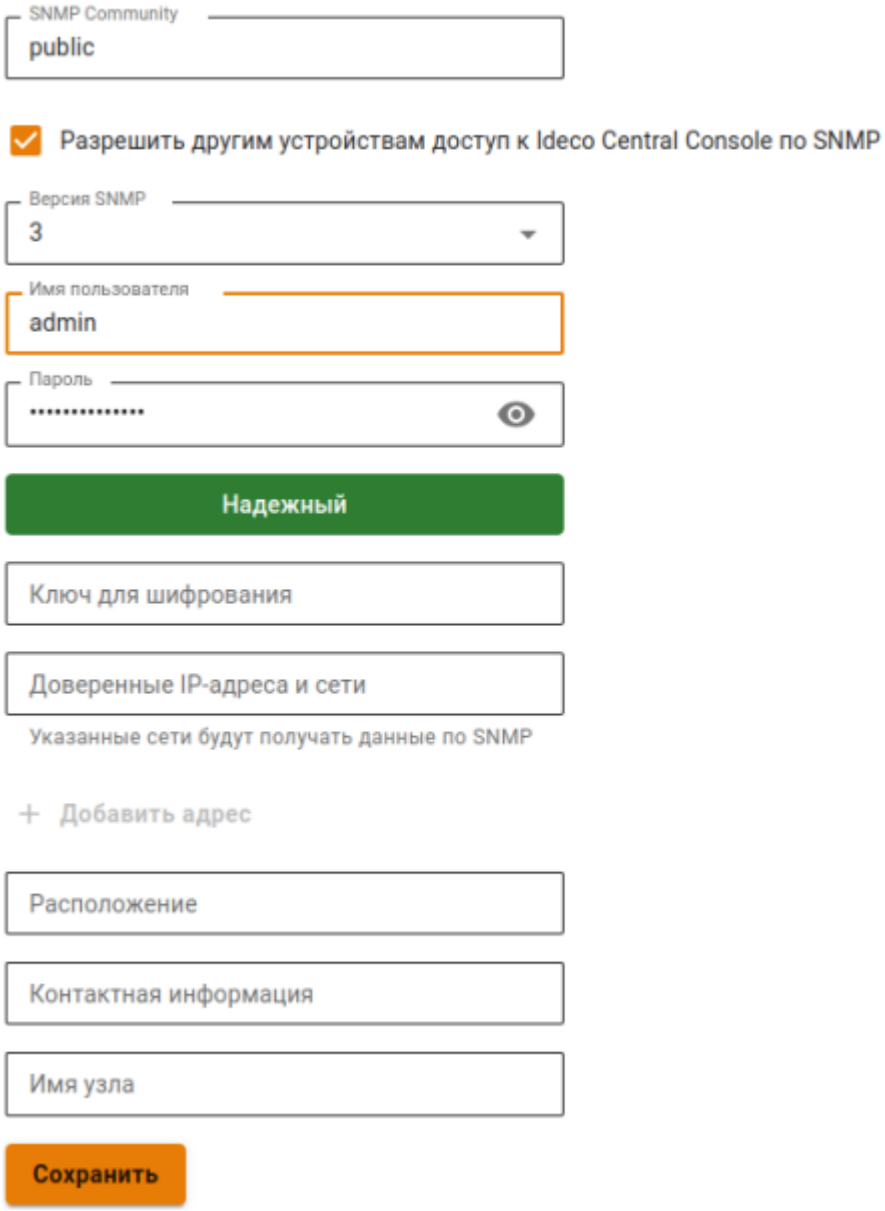
Для версии SNMPv1/v2 необязательно указывать поля **Имя**, **Пароль**, **Ключ шифрования**.

Поле SNMP community для SNMPv3 необязательно для заполнения.

Настройка SNMP:

1. Перейдите в раздел **Мониторинг -> SNMP**.

2. Активируйте опцию **Разрешить другим устройствам доступ к Ideco Central Console по SNMP** и заполните поля:



- **Версия SNMP** - версия протокола SNMP;
- **Имя пользователя** - имя пользователя для подключения по SNMP;
- **Пароль** - пароль для прохождения аутентификации;
- **Ключ для шифрования** - ключ, с помощью которого будет выполняться шифрование информации;

- **Доверенные IP-адреса и сети** - сети, в которые будут передаваться данные по SNMP;
- Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и являются необязательными:

3. Нажмите **Сохранить** для завершения настройки.

32.2 Zabbix-агент

Zabbix - это решение распределенного мониторинга корпоративного класса с открытыми исходными кодами.

Ознакомиться с Zabbix можно на официальной странице Zabbix.

Опробуйте Zabbix в виде готового решения или установить его, воспользовавшись документацией Zabbix.

> **Предупреждение:** Для работы системы мониторинга Zabbix активируйте опцию **Zabbix-агент** после настройки интеграции с сервером.

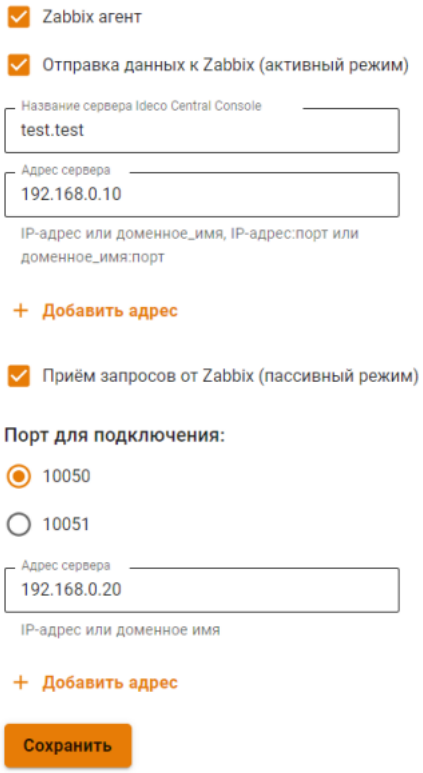
Настройка Zabbix-агент:

Интеграция с системой мониторинга Zabbix возможна в двух режимах:

1. **Активный режим** - соединение с Zabbix-сервером происходит со стороны Ideco Center. Для настройки этого режима заполните следующие поля:

- **Название сервера Ideco Central Console** - имя, которое будет отображаться на сервере мониторинга;
- **Адрес сервера** - IP-адрес, доменное имя, либо `IP-адрес:порт`, `доменное имя:порт`, если используется не стандартный для Zabbix входящий порт. Для добавления еще одного адреса нажмите на кнопку **Добавить адрес**.

2. **Пассивный режим** - подключение происходит со стороны Zabbix-сервера. Для настройки этого режима заполните следующие поля:



- **Порт для подключения** - выберите 10050 или 10051 порт;

- **Адрес сервера** - IP-адрес или доменное имя Zabbix-серверов. Для добавления еще одного адреса нажмите на кнопку **Добавить адрес**.

Zabbix-сервер может находиться как внутри локальной сети Ideco Center, так и за ее пределами. Подключение мониторинга возможно как к локальным, так и к внешним интерфейсам. В качестве шаблонов данных можно использовать стандартные шаблоны для Linux-серверов.

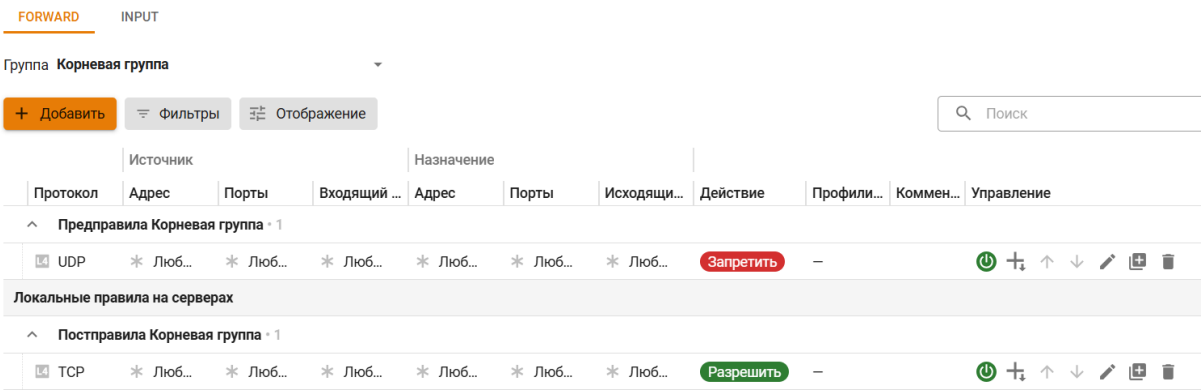
33. Политики и объекты

В Ideco NGFW из Ideco Center переносятся только те настройки, которые присутствуют в центральной консоли. Принципы работы разделов **Файрвол**, **Контент-фильтр** и **Ограничение скорости** с подключенными NGFW идентичен. Рассмотрим на примере раздела **Файрвол**.

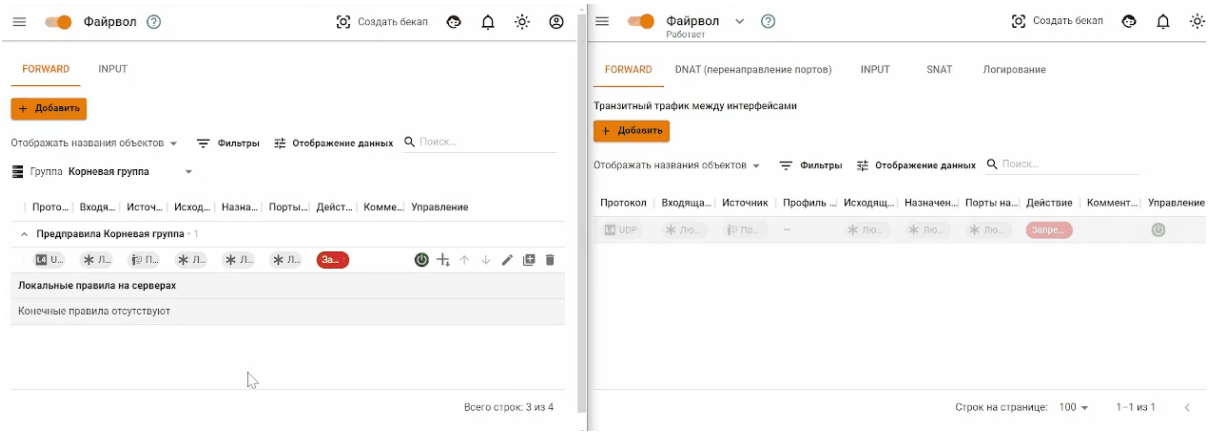
> **Предупреждение:** На Ideco NGFW будут распространяться правила и политики безопасности всех вышестоящих групп в соответствии с вложенностью. Правила **Корневой группы** распространяются на все подключенные NGFW.

33.1 Файрвол

Файрвол 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 Ideco NGFW:



В Ideco Center:

Созданные в Ideco Center правила FORWARD отображаются в виде двух таблиц: **Начальные правила** и **Конечные правила**. Правила применяются на подключенных Ideco NGFW в следующем порядке: сначала

- **Начальные правила** Ideco Center, затем - **Локальные правила** NGFW, затем - **Конечные правила** Ideco Center.

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

Правила можно включать и редактировать только в Ideco Center. В Ideco NGFW они доступны только для просмотра. Перемещать правила между таблицами **Начальные правила** и **Конечные правила** нельзя.

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

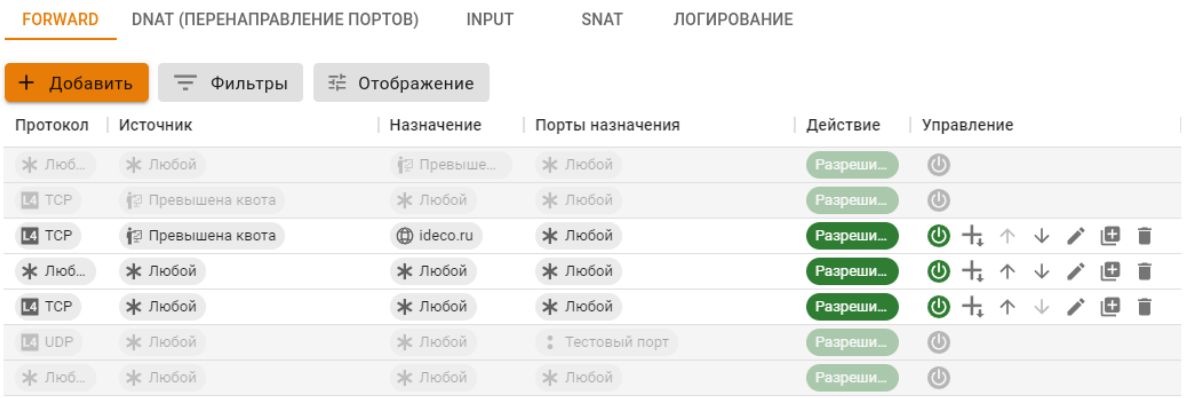
Чтобы увидеть все правила, распространяющиеся на группу серверов, выберите название группы над таблицей:

В таблице отобразятся все правила, распространяющиеся на выбранную группу, с учетом вложенности групп.

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

В Ideco NGFW:

Таблица в Ideco NGFW визуально делится на три части: верхняя, средняя и нижняя.



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

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

Подсказка: Локальные правила на серверах Ideco NGFW не видны в интерфейсе Ideco Center.

Для просмотра перейдите в раздел **Серверы**, нажмите на  в строке с нужным Ideco NGFW и перейдите в раздел **Файрвол**.

33.2 Контроль приложений

Механизм работы правил **Контроля приложений** изменился, создайте профили безопасности ***Контроля приложений***.

В Ideco Center все правила, которые создаются в разделе **Политики и объекты**, работают по одному и тому же принципу. Рассмотрим это на примере раздела *Файрвол*.

33.3 Контент-фильтр

Контент-фильтр проверяет наличие сайта, который хочет открыть пользователь, в списках ресурсов Ideco NGFW. Если адрес находится в этих списках, то применяются настроенные правила фильтрации.

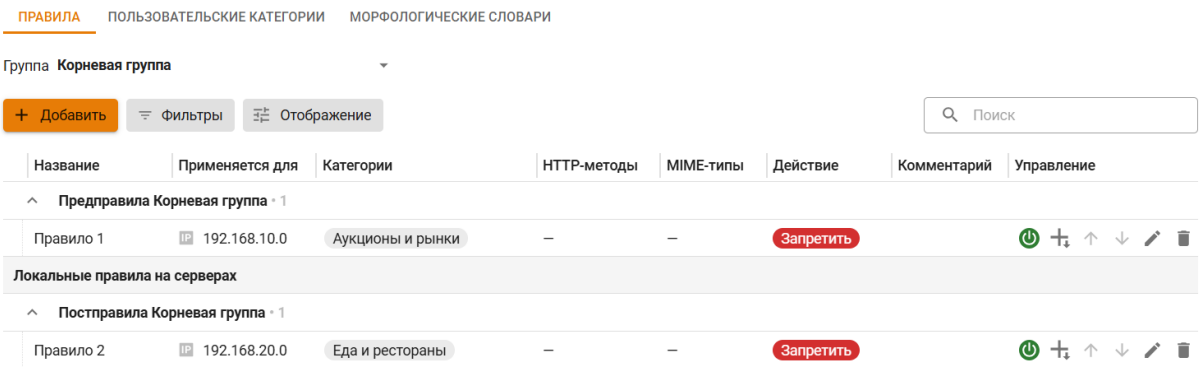
Процессы создания правил в Ideco Center и в *Ideco NGFW* аналогичны. Созданные в Ideco Center правила **Контент-фильтра** переносятся в подключенные Ideco NGFW в соответствии с группами серверов.

Созданные в Ideco Center правила **Контент-фильтра** можно включать и редактировать только в Ideco Center. В Ideco NGFW они доступны только для просмотра.

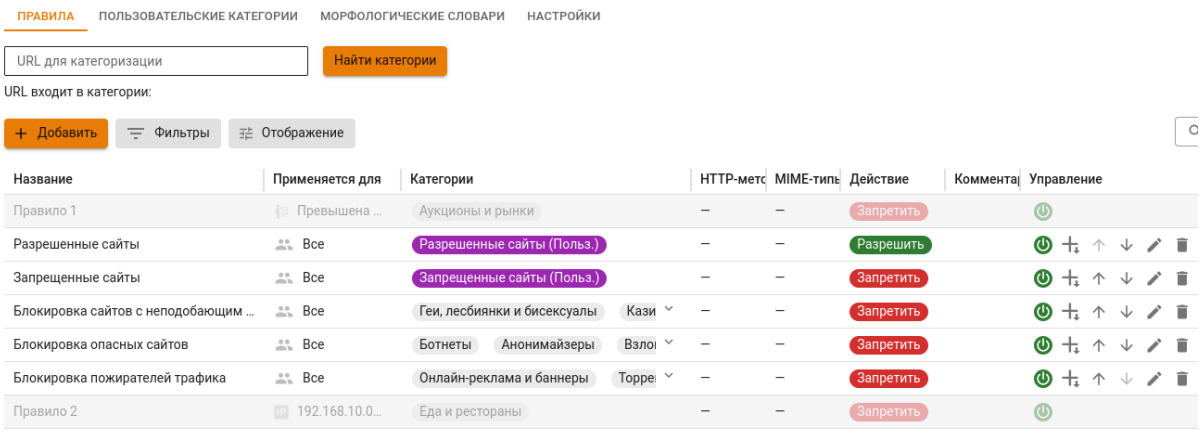
В Ideco Center все правила, которые создаются в разделе **Политики и объекты**, работают по одному и тому же принципу. Рассмотрим это на примере раздела *Файрвол*.

Правила **Контент-фильтра**:

- В Ideco Center:



- В подключенном Ideco NGFW:

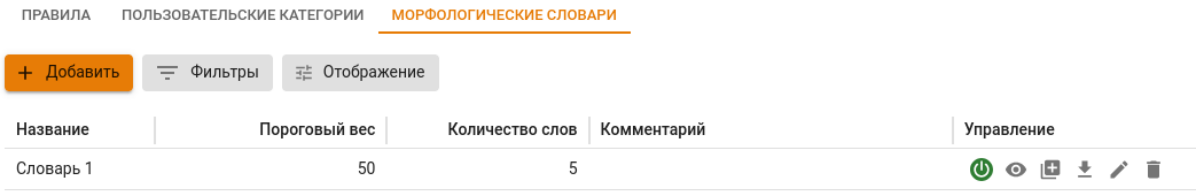


На вкладке **Морфологические словари** создаются и редактируются словари, которые можно использовать для проведения морфологического анализа сайтов в подключенных Ideco NGFW. В Ideco Center включить морфологический анализ нельзя. Процессы создания **Морфологических словарей** в Ideco Center и в *Ideco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

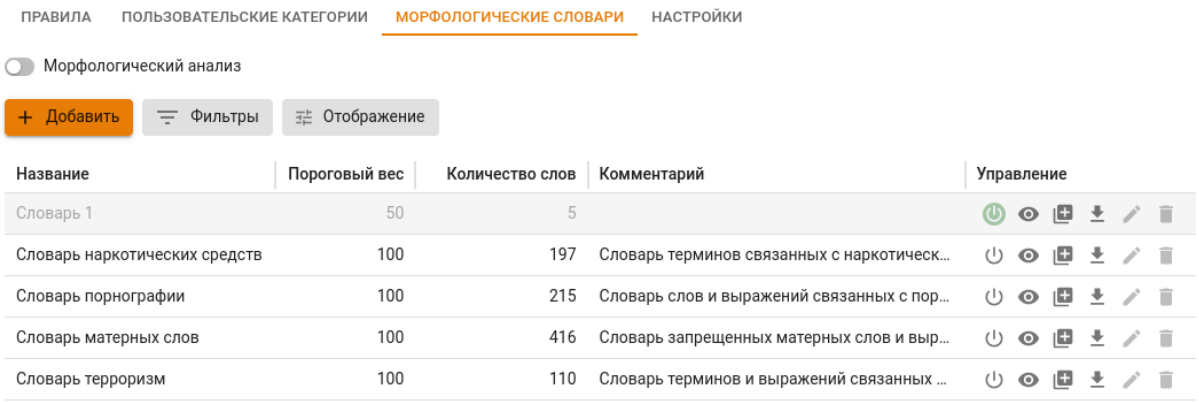
Созданные в Ideco Center **Морфологические словари** можно включать и редактировать только в Ideco Center. В Ideco NGFW они доступны только для просмотра.

Морфологические словари:

- В Ideco Center:



- В подключенном Ideco NGFW:



33.4 Объекты

Объекты, созданные в Ideco Center, переносятся в подключенные Ideco NGFW. Администратор Ideco NGFW может использовать эти объекты для создания правил.

При удалении объекта из Ideco Center, объект удаляется и из Ideco NGFW. Если в Ideco NGFW было создано правило с удаленным объектом, то этот объект будет отмечен иконкой 

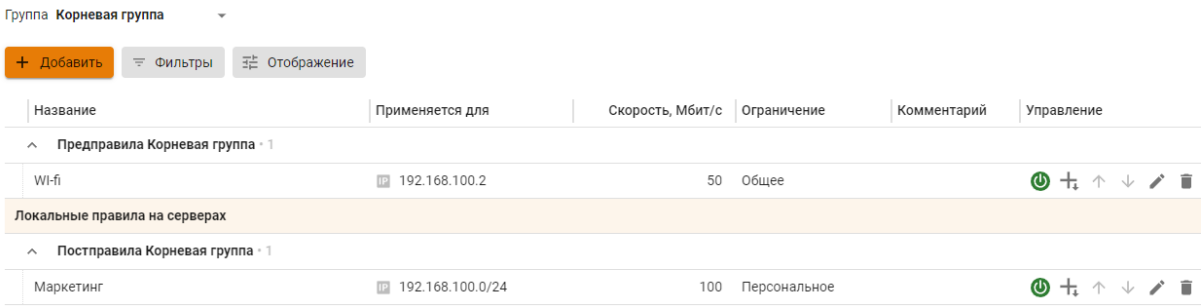
.

Подсказка: Принцип создания и удаления объектов в Ideco Center соответствуют принципам Ideco NGFW. Подробное описание в статье *Объекты*.

33.5 Ограничение скорости

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

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



В Ideco Center все правила, которые создаются в разделе **Политики и объекты**, работают по одному и тому же принципу. Рассмотрим это на примере раздела *Файрвол*.

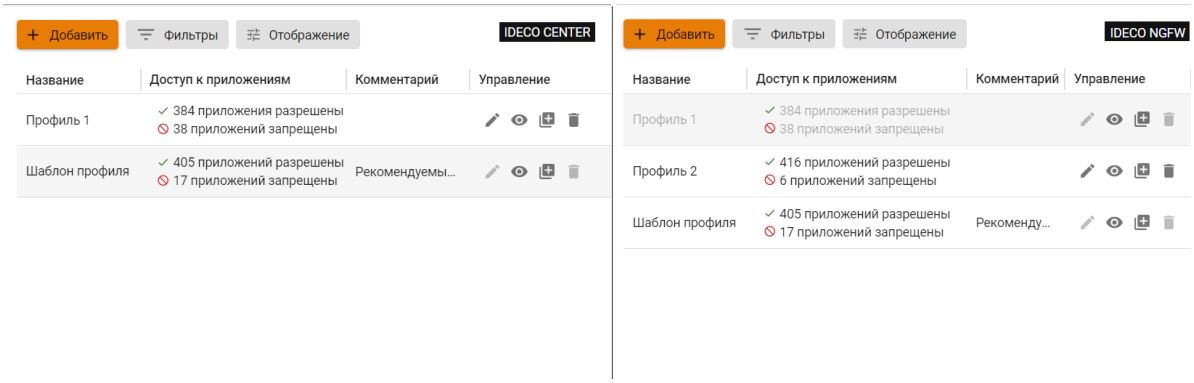
34. Профили безопасности

Профили безопасности представляют собой наборы параметров, которые используются для фильтрации трафика различными модулями. Это позволяет настраивать разные политики безопасности независимо друг от друга.

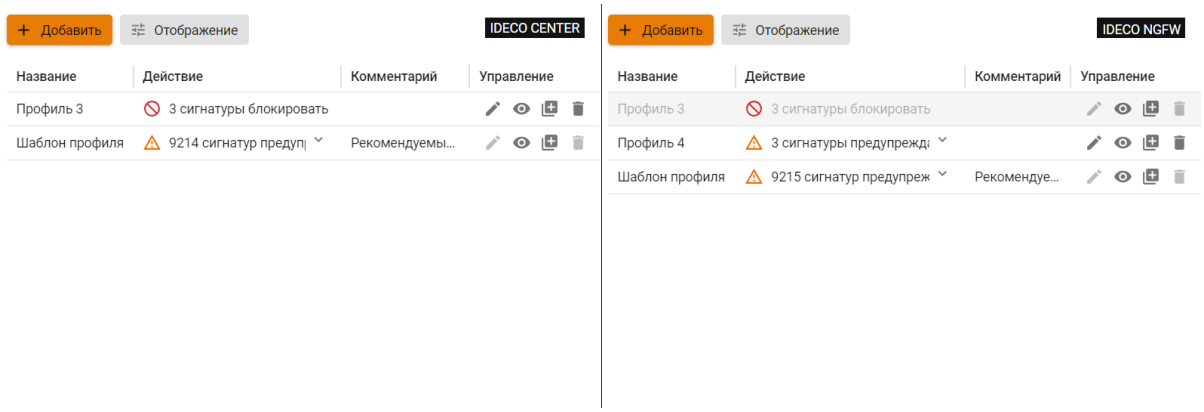
В Ideco Center можно управлять профилями безопасности для всех подключенных Ideco NGFW одновременно.

Созданные в Ideco Center профили безопасности можно редактировать только в Ideco Center, в интерфейсе Ideco NGFW они доступны только для просмотра:

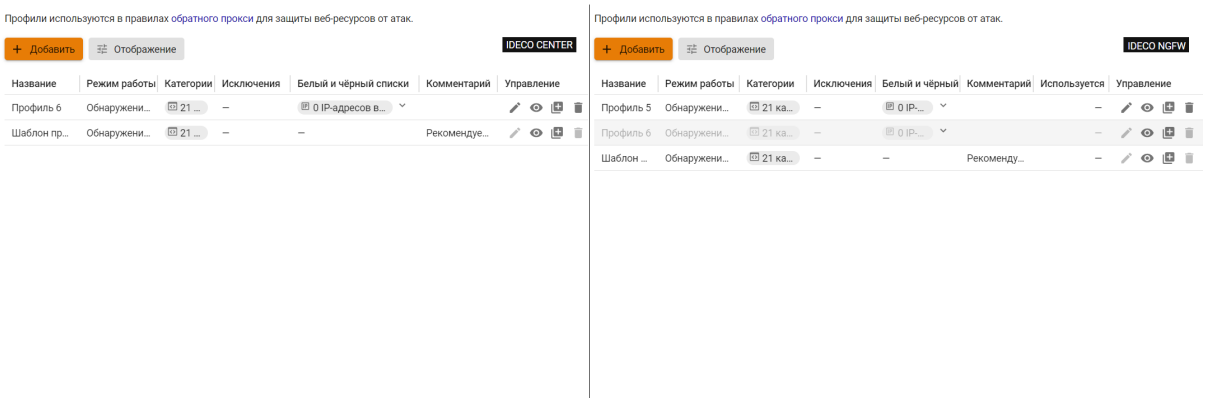
- Таблица профилей **Контроля приложений**:



- Таблица профилей **Предотвращения вторжений**:



- Таблица профилей **Web Application Firewall**:



Созданные в Ideco Center профили **Контроля приложений** и **Предовращения вторжений** доступны для добавления при создании правил *Файрвола* в NGFW:

FORWARD INPUT

Добавление правила

Вид правила
Предправило

Группа серверов
Корневая группа

Протокол
Любой

Источник

Инвертировать источник

Адрес
Любой

Входящий интерфейс
Любой

Назначение

Инвертировать назначение

Адрес
Любой

Исходящий интерфейс
Любой

Действие

Разрешить

Запретить

Профили безопасности

Контроль приложений

Профиль
Профиль 1

Предотвращение вторжений

Профиль

Дополнительно

Включить правило

Время действия
Любой

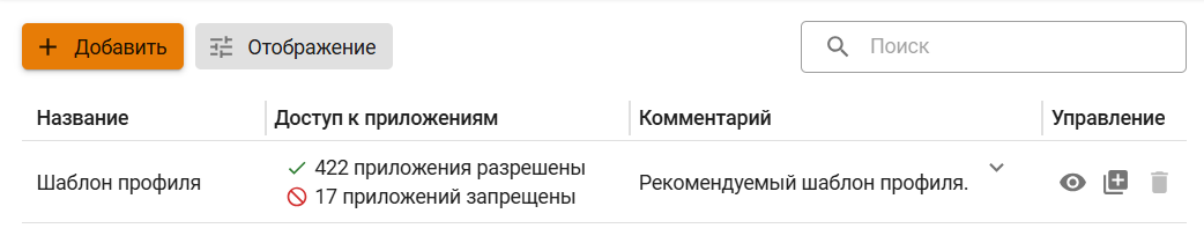
Комментарий

0/256

Добавить Отмена

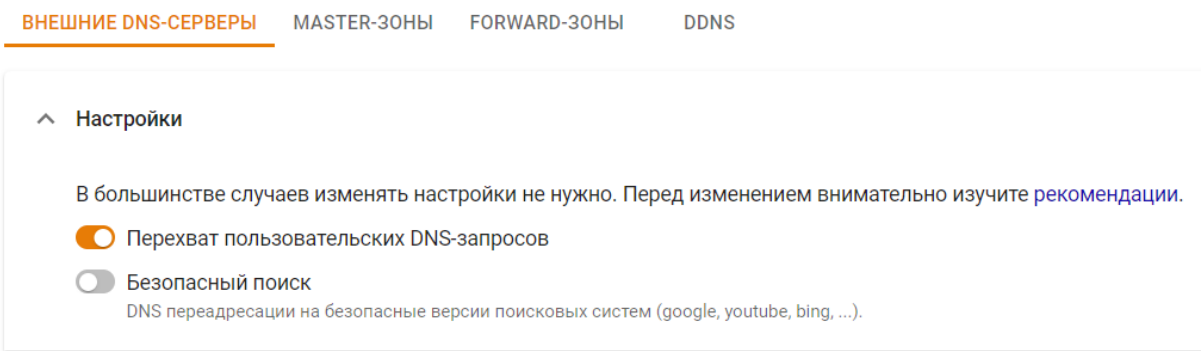
34.1 Контроль приложений

В разделе **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).



Подсказка: Принцип создания и настройки профилей в Ideco Center соответствуют принципам Ideco NGFW. Подробное описание в статье *Контроль приложений*.

Чтобы трафик фильтровался модулем **Контроль приложений**, необходимо для всех локальных интерфейсов создать правило FORWARD, содержащее необходимый профиль безопасности. Если в разделе **Сервисы -> DNS -> Внешние DNS-серверы** включена опция **Перехват пользовательских DNS-запросов** (по умолчанию включена), нужно также создать аналогичное правило INPUT:



В Ideco Center 17.6 были добавлены профили **Контроля приложений**. Но синхронизация профилей между Ideco NGFW и Ideco Center не осуществлялась.
В 18 версии синхронизацию добавили. Поэтому рекомендуем начать обновление на 18 версию с Ideco Center и далее приступить к обновлению синхронизированного Ideco NGFW.

После обновления Ideco Center на 18 версию правила, синхронизированные из Ideco Center в **Правила трафика -> Контроль приложений**, будут доступны только для просмотра и не будут влиять на обработку трафика в подключенных NGFW.

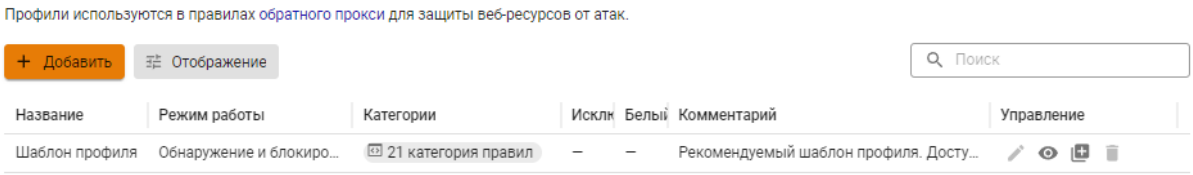
34.2 Предотвращение вторжений

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

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

34.3 Web Application Firewall

Использование WAF-профилей позволит настроить параметры защиты для опубликованных веб-ресурсов. Профиль создается в разделе **Профили безопасности -> Web Application Firewall**.



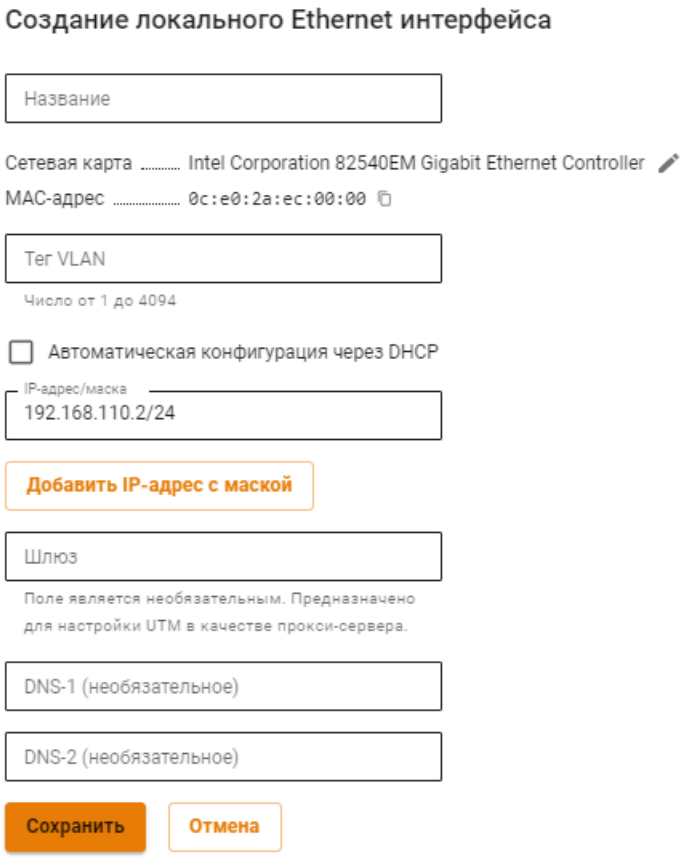
Подсказка: Для удобной настройки **Web Application Firewall** на Ideco NGFW, соединенных с Ideco Center, создайте профиль WAF на Ideco Center и используйте его в Ideco NGFW. Подробное описание в статье *Web Application Firewall*.

---

35. Сервисы

35.1 Сетевые интерфейсы

В отличие от Ideco NGFW, в Ideco Center создается только локальный Ethernet-интерфейс. Для этого нажмите **Добавить**, выберите сетевую карту и заполните нужные поля:



- **Название интерфейса** - имя для идентификации интерфейса;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется в том случае если сетевая карта уже используется;
- **Автоматическая настройка через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - назначьте на интерфейс минимум один IP-адрес. Если нужно, настройте интерфейс с несколькими IP-адресами;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS сервера (необязательно).

Внимание: 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.

35.2 Маршрутизация

Маршрутизация работает аналогично маршрутизации Ideco NGFW. Подробное описание по *ссылке*.

35.3 DNS

Принцип работы DNS в Ideco Center аналогичен принципу работы *Внешних DNS-серверов* в Ideco NGFW. Если вышестоящий роутер перехватывает DNS-запросы Ideco Center, то добавьте внешние DNS-серверы.

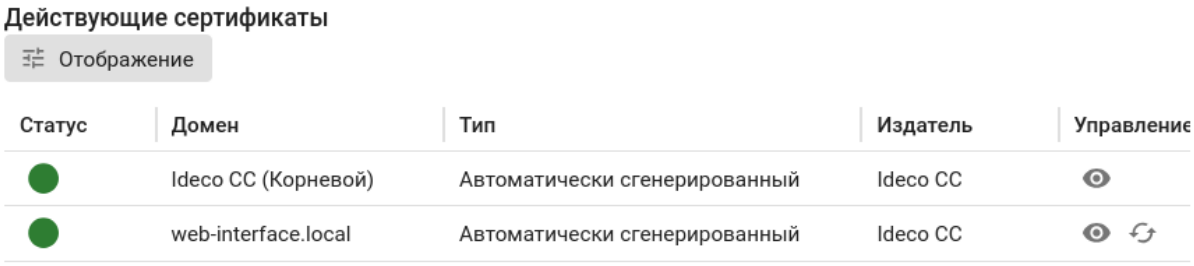
35.4 Сертификаты

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

Для просмотра основной информации о сертификате нажмите кнопку .

Процесс выпуска и перевыпуска сертификата одинаков с Ideco NGFW и описан в *статье*

35.4.1 Действующие сертификаты

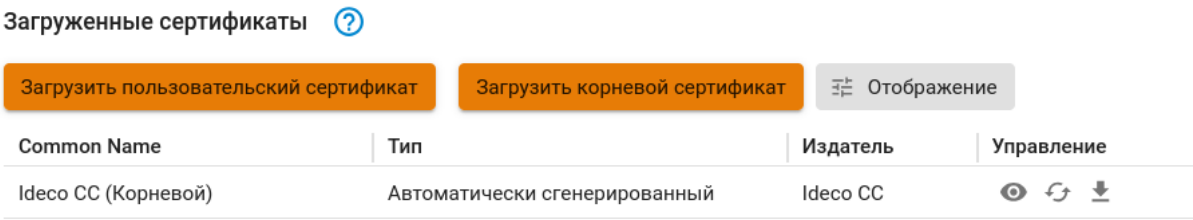


В таблице *Действующие сертификаты* отображаются:

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

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

35.4.2 Загруженные сертификаты



В таблице *Загруженные сертификаты* отображаются:

- Все загруженные цепочки сертификатов;

- Корневой сертификат Ideco Center.

Подсказка: Загрузка SSL-сертификата на Ideco Center аналогична загрузке на Ideco NGFW. Подробная инструкция - в *статье*.

Подсказка: На Ideco Center можно загрузить самоподписанные сертификаты, созданные в *PowerShell* или *OpenSSL*.

35.4.3 Системные сертификаты

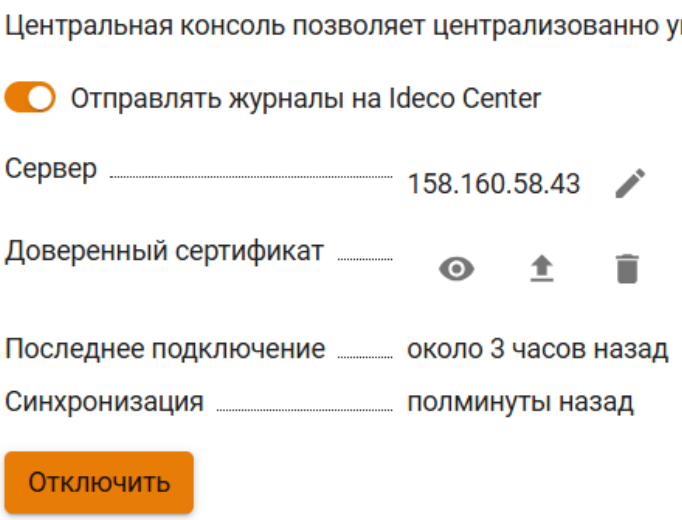
Раздел позволяет загружать свои сертификаты в хранилище доверенных сертификатов ОС Fedora на Ideco Center. Подробнее о системных сертификатах - по ссылке. После добавления сертификата в таблицу **Системные сертификаты** Ideco Center будет доверять загруженному сертификату и всем сертификатам, подписанным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

36. Отчеты и журналы

36.1 Системный журнал

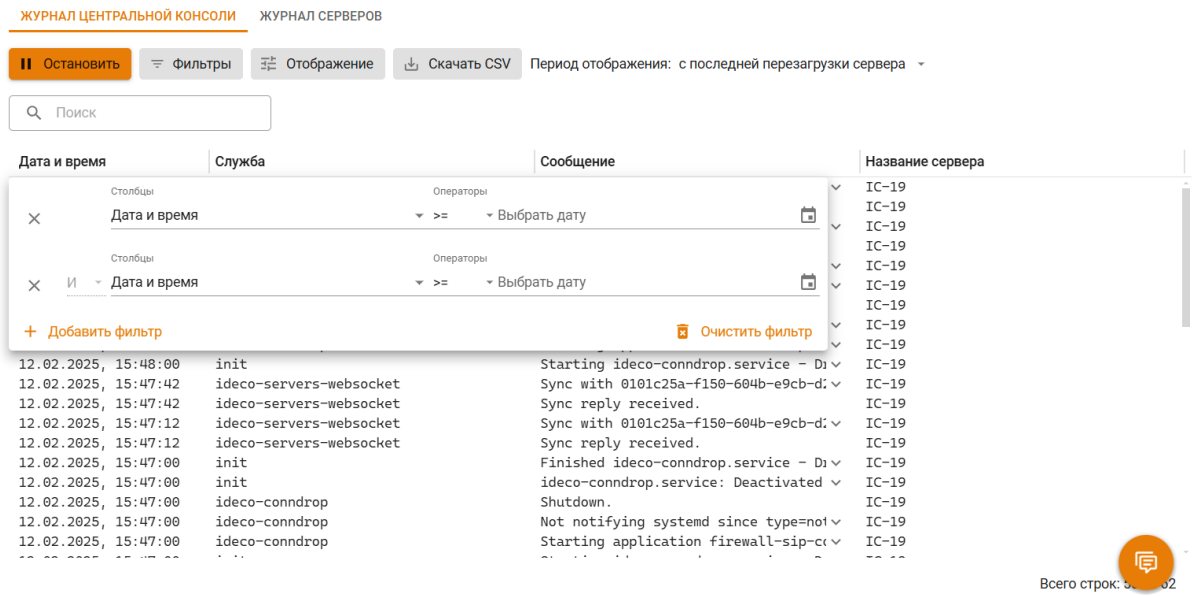
Подсказка: Время хранения логов в разделе **Журналы** - три месяца. После этого логи доступны в разделе **Управление сервером -> Терминал**.

В разделе доступен просмотр логов Ideco Center и подключенных к центральной консоли Ideco NGFW. Для отображения в таблице логов серверов необходимо в разделе **Управление сервером -> *Ideco Center*** каждого Ideco NGFW включить опцию **Отправлять журналы на Ideco Center**:

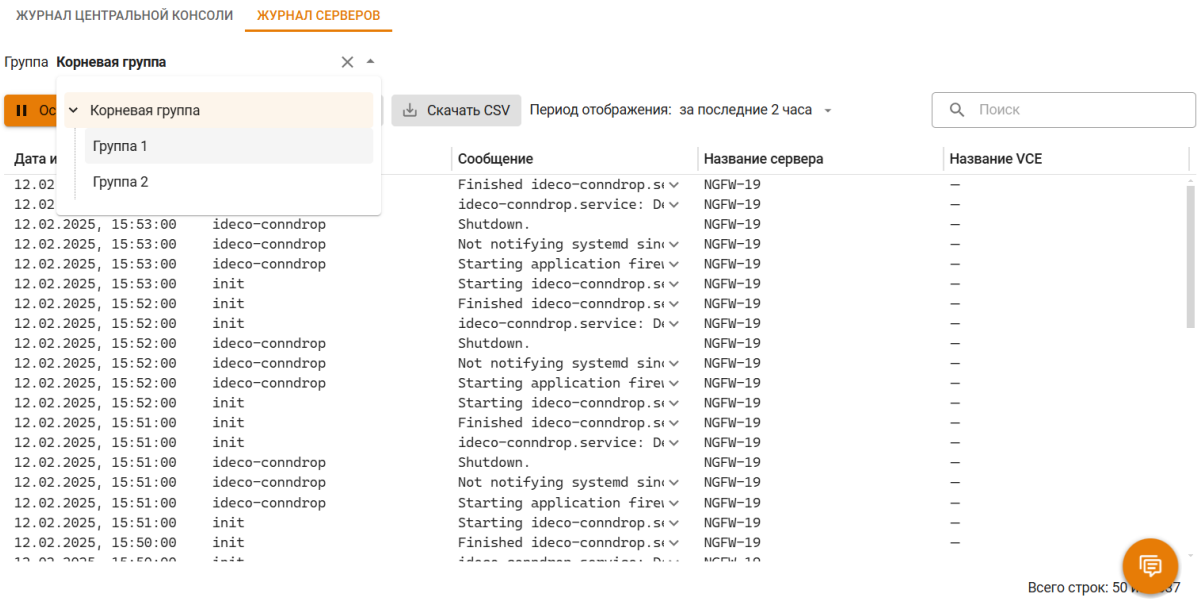


Чтобы просмотреть логи определенной службы, воспользуйтесь строкой поиска или фильтром. Для филь-

трации логов по нескольким параметрам нажмите **Добавить фильтр** и выберите соответствующий критерий, значение и оператор в форме:



На вкладке **Журнал серверов** можно выбрать группу серверов для просмотра логов Ideco NGFW из веб-интерфейса Ideco Center:



Подсказка: По кнопке **Скачать CSV** сохраняются те строки логов, которые заданы фильтрацией.

Список служб, доступных в разделе:

- **Серверы** - `ideco-servers-backend`, `ideco-servers-websocket`;
- **Файрвол** - `ideco-firewall-backend`;
- **Контроль приложений** - `ideco-app-backend`;
- **Контент-фильтр** - `ideco-content-filter-backend`;
- **Предотвращение вторжений** - `ideco-suricata-event-syncer`, `ideco-suricata-backend`;

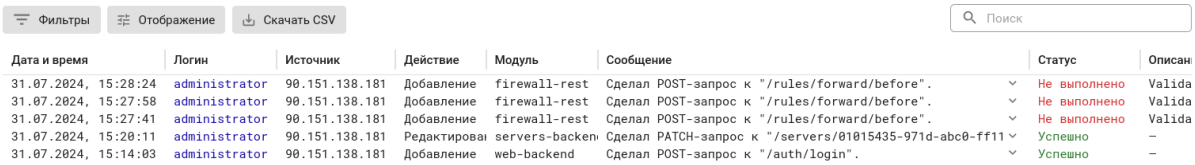
- **Объекты** - `ideco-alias-backend`;
- **Сетевые интерфейсы** - `ideco-network-backend`, `ideco-network-nic`;
- **Маршрутизация** - `ideco-routing-backend`, `ideco-routing-rest`;
- **Обратный прокси** - `ideco-reverse-backend`;
- **DNS** - `ideco-dns-backend`, `unbound`, `nsd`, `unbound-anchor`, `unbound-keygen`;
- **NTP** - `chronyd`;
- **Кластеризация** - `ideco-cluster-backend`;
- **Обновления** - `ideco-sysupdate-backend`;
- **Бэкапы** - `ideco-backup-backend`;
- **Лицензия** - `ideco-license-backend`;
- **Syslog** - `ideco-logs-backend`;
- **Отчеты и журналы** - `ideco-logs-backend`, `ideco-logs-syncer`;
- **Действия администраторов** - `ideco-audit-backend`;
- **Сертификаты** - `ideco-cert-backend`;
- **Сбор анонимной статистики о работе сервера** - `ideco-gatherstat-backend`;
- **Локальное меню** - `ideco-local-menu`;
- **Дополнительно (язык, часовой пояс, включение особых режимов работы)** - `ideco-system-backend`;
- **Защита от повторяющихся зловредных или подозрительных действия, в т.ч. от брутфорс-атак (brute force - атака полным перебором)** - `fail2ban`;
- **Доступ по SSH** - `sshd`.

Служебное:

- `clickhouse-server` - сервер базы данных;
- `ideco-etcd-runtime`, `ideco-etcd-permanent` - локальная база данных;
- `prometheus`, `prometheus-node-exporter` - сбор метрик и статистики.

36.2 Действия администраторов

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



37. Управление сервером

37.1 Администраторы

В Ideco Center можно создать несколько администраторов с разными ролями:

- **Администратор** - администратор с этой ролью имеет доступ ко всем функциональностям Ideco Center;
- **Только просмотр** - администратор с этой ролью не имеет возможности управлять правилами в Ideco Center (создавать, менять приоритет и др.).

Подсказка: Удалять подключенный Ideco NGFW из Ideco Center могут только администраторы с ролью **Администратор**.

Войти в подключенный Ideco NGFW с логином и паролем администратора Ideco Center **невозможно**.

37.2 Обновления

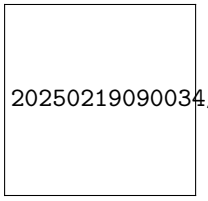
Подсказка: Название службы раздела **Обновления**: `ideco-sysupdate-backend`.

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

37.3 Система

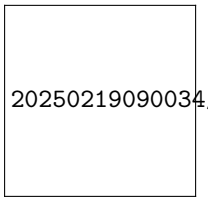
Обновить систему Ideco Center можно как в офлайн-режиме, так и по сети. Отрегулировать режим обновления можно в разделе **Управление сервером -> Лицензия**.

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



- **Канал 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 6 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.

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

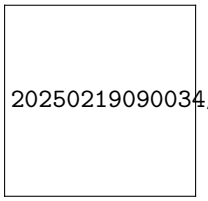


Подсказка: Кнопка принудительного обновления активна, когда обновление уже скачано, и только применяет его, инициировать скачивание нельзя.

После принудительного обновления потребуется полная перезагрузка сервера.

После проведения процедуры обновления новая версия будет отображаться в верхнем левом углу локальной консоли и веб-интерфейса администратора.

37.3.1 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.

Если в **Ideco Center** настроен кластер, то в веб-интерфейсе будет отсутствовать пункт **Восстановление на предыдущую версию**.

Предупреждение: При восстановлении на предыдущую версию данные перенесены не будут. Сохраните информацию на внешнем носителе.

37.3.2 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. Обратная связь позволяет выявить недочеты и уязвимости в продукте. После их исправления происходит выкладка в канал **Релиз**.

Подсказка: 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.

37.3.3 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).

Предупреждение: 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.

37.4 Бэкапы

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

Подсказка: Название служб раздела **Бэкапы**: `ideco-backup-backend`; `ideco-backup-create`; `ideco-backup-restore`; `ideco-backup-rotate`.

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

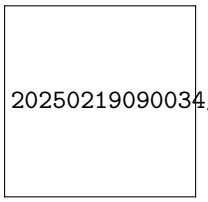
Бэкапы не включают:

- Системный журнал;
- Любые данные, генерируемые в процессе работы системы автоматически.

В Ideco Center бэкап создается как автоматически, так и вручную.

37.5 Автоматическое создание бэкапа

Для настройки автоматического бэкапа перейдите в раздел **Управление сервером -> Бэкапы -> Настройки**:


20250219090034/docsUTM/20250219090034/docsUTM/.gitbook/assets/backup.png

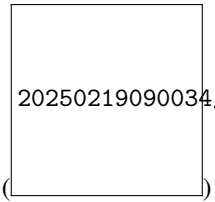
Установите время ежедневного создания и продолжительность хранения бэкапа на локальном жестком диске. При настройке выгрузки на сетевое файловое хранилище автоматический бэкап будет также дублироваться туда.

- **Время ежедневного создания копии** - укажите в настройках час (рекомендуется выбирать ночное время для создания бэкапа);
- **Хранить в течение** - хранить бэкапы на локальном жестком диске можно в течение недели или месяца.

Подсказка: 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.

Бэкапы на сетевое файловое хранилище Ключевые параметры, необходимые для настройки бэкапа на NetBIOS-сервер:

- 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:

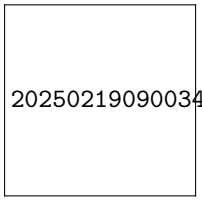
- Адрес сервера - IP-адрес удаленного FTP-сервера, на котором будут размещаться бэкапы;
- Логин - Имя пользователя для авторизации на FTP-сервере;
- Пароль - Пароль для авторизации на FTP-сервере;
- Путь к каталогу - Каталог, в который будут записываться бэкапы.

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

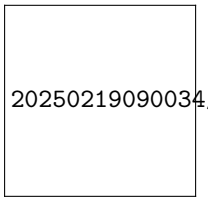
37.6 Ручное создание бэкапа

Через веб-интерфейс:

Для создания бэкапа через интерфейс Ideco Center перейдите в **Управление сервером -> Бэкапы -> Бэкапы** и нажмите **Добавить -> Создать**. Введите комментарий и нажмите **Добавить** или нажмите



Создать бэкап в правом верхнем углу веб-интерфейса. Новый бэкап появится в таблице:



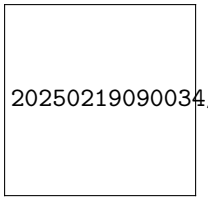
Через локальное меню:

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

1. Выберите пункт **10** и нажмите **Enter**.

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

Пример создания бэкапа через локальное меню приведен на скриншоте ниже:



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

37.6.1 Восстановление конфигурации из бэкапа

В Ideco Center восстановление из бэкапа возможно полное и мгновенное.

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

При выполнении мгновенного восстановления бэкап применятся без перезагрузки. При этом не сохраняются:

- Счетчики квот;
- Системный журнал.

Предупреждение: При восстановлении системы из резервной копии информация о лицензии не будет восстановлена, поскольку это может привести к использованию устаревшей лицензии.

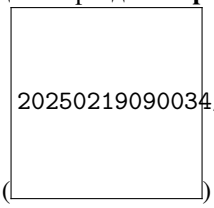
После завершения процесса восстановления Ideco Center автоматически отправит запрос в личный кабинет для обновления лицензии. Если используется офлайн-лицензия, ее необходимо загрузить самостоятельно.

Если резервное копирование используется для переноса настроек с одного сервера на другой, выполните «перепривязку» лицензии. Подробную информацию можно найти в статье *Перенос данных и настроек на другой сервер*.

Подсказка: 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.

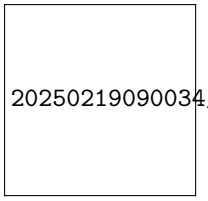
Через веб-интерфейс:

Перейдите в раздел **Управление сервером -> Бэкапы -> Бэкапы** и нажмите кнопку **Полное восстановление** (

) или **Мгновенное восстановление** (

) в столбце **Управление**.

Также можно загрузить бэкап из файла. Например, в случае переноса с другого сервера. Для восстановления конфигураций бэкапа, который находится на внешнем носителе, перейдите на **Управление сервером -> Бэкапы -> вкладка Бэкапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню:

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

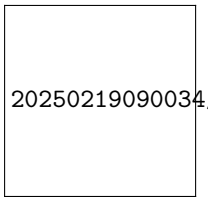
- **11** - восстановятся все настройки и перезагрузится сервер;
- **12** - восстановятся все настройки без перезагрузки сервера, кроме изменений в списке пользователей и отчетах.

  Нажмите **Enter**.

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

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

Пример восстановления из бэкапа через локальное меню:



Чтобы перенести установленный Ideco Center с одного сервера на другой с сохранением всех настроек, воспользуйтесь статьей *Перенос данных и настроек на другой сервер*.

37.7 Терминал

Предупреждение: 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.

37.8 Основные команды

- **Утилиты сетевой диагностики:** `ping`, `host`, `nslookup`, `tracepath`, `tcpdump`, `arping`, `ss` (аналог `netstat`);
- **Файловый редактор:** `nano`;
- **Просмотр логов:** `journalctl -u <название службы>` (например, `journalctl -u ideco-routing-backend`);
- **Проверка скорости интернета:** `speedtest-cli`;
- **Просмотр ARP-таблицы:** `ip neigh show`;
- **Разблокировка в случае срабатывания защиты от брутфорс-атак:**
  - `fail2ban-client unban --all` - команда используется для снятия всех блокировок;

- `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса. Укажите нужный IP-адрес в качестве аргумента.

- **Просмотр конфигурации FRR:** `vtysh`.

37.9 Таблица служб

Раздел	Имя службы
Файрвол	ideco-nflog;ideco-firewall-backend
Профили контроля приложений	ideco-app-backend; ideco-app-control-nfq
Контент-фильтр	ideco-content-filter-backend
Ограничение скорости	ideco-shaper-backend
Антивирус	ideco-av-backend
Предотвращение вторжений	ideco-suricata-backend; ideco-suricata; ideco-suricata-event-syncer; ideco-suricata-profiles-syncer
Объекты	ideco-alias-backend
Сетевые интерфейсы	ideco-network-backend; ideco-network-nic
Балансировка и резервирование, Маршрутизация	ideco-routing-backend
BGP, OSPF	frr; ideco-routing-backend
Прокси	ideco-proxy-backend; squid
Обратный прокси	ideco-reverse-backend
DNS	ideco-dns-backend; unbound; nsd
DDNS	ideco-dns-backend
DHCP	ideco-dnsmasq
NTP	chronyd
IPsec	ideco-ipsec-backend; strongswan
Центральная консоль	ideco-central-console-backend
VCE	ideco-vce-backend
Кластеризация	ideco-cluster-backend; ideco-cluster-backup-pusher
Обновления	ideco-sysupdate-backend
Бэкапы	ideco-backup-backend; ideco-backup-create; ideco-backup-restore; ideco-backup-rotate
Лицензия	ideco-license-backend
VPN-подключения	ideco-accel-l2tp; ideco-accel-pptp; ideco-accel-sstp; ideco-vpn-servers-backend; ideco-vpn-authd; ideco-vpn-dhcp-backend
Авторизация	ideco-auth-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-authd
Active Directory	ideco-ad-backend; ideco-ad-log-collector@<имя домена>
ALD Pro	ideco-ald-rest; ideco-ald-backend
Ideco Client	ideco-agent-backend; ideco-agent-websocket
Syslog	ideco-logs-backend
Обнаружение устройств	ideco-netscan-backend
Web Application Firewall	ideco-waf-backend; ideco-waf-event-syncer
IGMP Proxy	ideco-igmpproxy-backend; ideco-igmpproxy

37.10 Дополнительно

В разделе доступны настройки:

- **Адрес Ideco Center** - поле заполняется, если сервер Ideco Center находится за NAT;
- **Настройка часового пояса** - изменения вступают в силу только после перезагрузки Ideco Center;
- **Настройки языка** - изменения вступают в силу только после перезагрузки Ideco Center.
- **Сбор анонимной статистики о работе сервера** - включение этого параметра разрешает серверу отправлять информацию об используемых модулях. При этом не отправляется информация о пользователях, проходящем dчерез сервер трафике, сетевых интерфейсах и идентификаторах сервера и лицензии.

38. FAQ

38.1 Как заблокировать чат-боты?

Заблокировать чат-боты можно, создав правило в Контент-фильтре. О том, как это сделать, написано в статье *Блокировка чат-ботов*.

38.2 Как настроить совместную работу ViPNet-Координатора с Ideco NGFW ?

Процесс настройки подробно описан в *статье*.

38.3 Как настроить автоматическую аутентификацию на Linux через веб-интерфейс ?

Процесс настройки подробно описан в статье *Настройка автоматической аутентификации на NGFW на Linux*. Скрипт подходит для всех Linux-систем с Python 3.5 и выше.

38.4 Есть ли возможность добавлять сигнатуры IPS?

Да, добавьте сигнатуру вручную в файл `/var/opt/ideco/suricata-backend/custom.rules`. Важно: sid правила не должен совпадать с существующими.
Подробнее о добавлении в статье *Как исключить узел из обработки системой IDS/IPS через терминал*.

38.5 Как настроить кластеризацию Active/Active?

Для настройки кластеризации Active/Active воспользуйтесь решением наших партнеров АО «НПП «Цифровые решения». Инструкция по интеграции Ideco NGFW и брокера сетевых пакетов DS Integrity NG - по *ссылке*.

38.6 Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW?

Порядок обработки веб-трафика и примеры проверки работоспособности модулей описаны в *статье*.

38.7 Хочу работать из дома, подключившись по RDP к своем компьютеру в офисе. Можно ли опубликовать RDP, чтобы он был доступен из интернета?

Не рекомендуем так делать. В такой ситуации существуют риски успешного взлома с помощью RDP. Даже сложный пароль и актуальные обновления не гарантируют того, что злоумышленники не смогут проникнуть внутрь сети через опубликованный RDP. Не рекомендуем публиковать RDP и подобные сервисы “наружу” (SSH, FTP и т.д.), так как это увеличивает количество потенциальных точек входа для злоумышленников. Рекомендуем использовать подключение по VPN к своей сети.

38.8 Как создать VPN-подключение?

В зависимости от операционной системы выберите подходящую инструкцию из *Инструкций по созданию VPN-подключений*.

38.9 Что делать, если сети за роутером, находящимся после NGFW, не доступны по VPN?

Для решения вопроса воспользуйтесь статьей *Доступ в удаленные сети через роутер в локальной сети*.

38.10 Что делать, если ваш IP попал в черные списки DNSBL?

Если вы используете белый статический IP-адрес, то попадание IP-адреса в черные списки может означать, что в сети зафиксирована бот-активность, участие в DDoS-атаках, либо рассылка спама.

Наличие в черных списках динамического IP-адреса из «домашних» диапазонов IP-адресов провайдеров в целом нормальное явление, т. к. вредоносная активность в таком случае может исходить не из вашей сети. Порядок действий при попадании в черный список описан в *статье*.

38.11 Утрачен пароль администратора, как его восстановить?

При утере пароля администратора можно его восстановить, имея физический доступ к серверу. Подробнее о процессе восстановления в статье *Как восстановить доступ к Ideco NGFW*.

38.12 После обновления потребовалось вернуть предыдущую версию со всеми настройками. Как это сделать?

Возможность восстановиться на предыдущую версию после обновления Ideco NGFW доступна с 12.X версий. Подробнее о процессе восстановления в статье *Как восстановиться на прошлую версию после обновления Ideco NGFW*.

38.13 Как понять, что контент-фильтр настроен эффективно?

Эффективность настроек контент-фильтра вы можете проверить с помощью сервиса security.ideco.ru. При правильной настройке общий уровень защиты должен показывать «зеленый» цвет. Если это не так, проверьте с помощью *статьи* настройки контент-фильтра и других служб фильтрации трафика.

38.14 Как подобрать аппаратную платформу для Ideco NGFW?

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 40 и содержит ядро Linux с набором драйверов от этой ОС с небольшими изменениями с нашей стороны. Таким образом, Ideco NGFW можно установить на большую часть оборудования, поддерживающего Fedora 40. Подробнее в статье *Выбор аппаратной платформы для Ideco NGFW*.

38.15 Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW?

Для настройки Ideco NGFW воспользуйтесь рекомендациями из статьи *Поддержка устаревших алгоритмов шифрования*.

38.16 Как настроить прямое подключение к прокси-серверу, если ПО его не поддерживает?

При использовании прямых подключений к прокси-серверу выход в интернет будет поддерживаться всеми программами, имеющими настройки прокси-сервера, либо программами, применяющими системные настройки прокси.

Некоторое ПО не имеет настроек прокси-сервера, поэтому необходимо использовать специализированное ПО на конечных рабочих станциях для вывода в интернет таких программ. Одно из таких ПО - Proxifier.

Инструкция по настройке программы Proxifier для прямых подключений к прокси-серверу доступна по *ссылке*.

38.17 Как эффективно заблокировать Ammyy Admin, Анонимайзеры, BitTorrent и т. д.?

Примеры блокировки программ удаленного доступа, анонимайзеров, торрентов и др. описаны в статье *Блокировка популярных ресурсов*.

38.18 Как настроить SSO-авторизацию для Astra Linux в домене AD?

Описание процесса настройки можно найти в статье *Настройка прозрачной авторизации на Astra linux*. Это решение подходит для браузеров Chromium и Firefox.

38.19 Как перенести данные и настройки с одного сервера на другой?

Чтобы перенести установленный Ideco NGFW с одного сервера на другой с сохранением всех настроек, следуйте *инструкции*.

38.20 Инструкции по созданию VPN-подключений

38.20.1 Создание VPN-подключения в Alt Linux

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

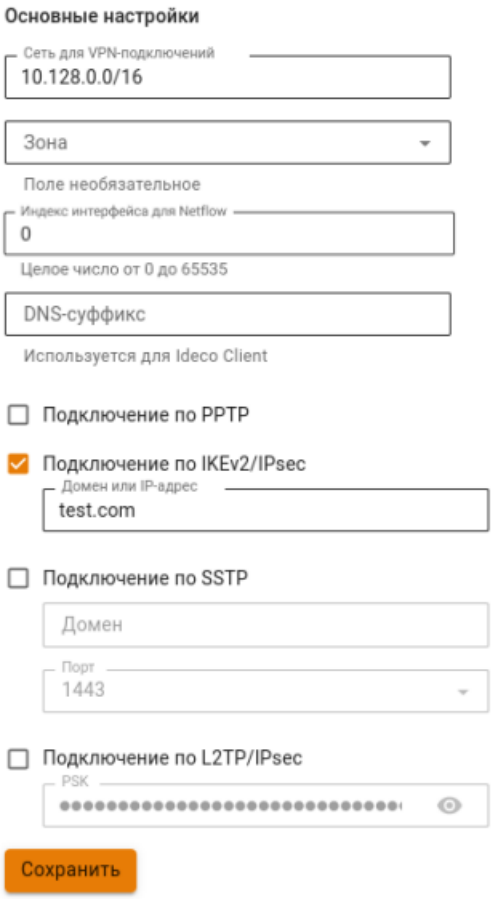
> **Предупреждение:** Не рекомендуем использовать для VPN-подключений кириллические логины.

Протокол IKEv2/IPsec

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите опцию **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения Alt Linux:

1. Откройте терминал сочетанием клавиш Ctrl+Alt+T и установите необходимые пакеты:

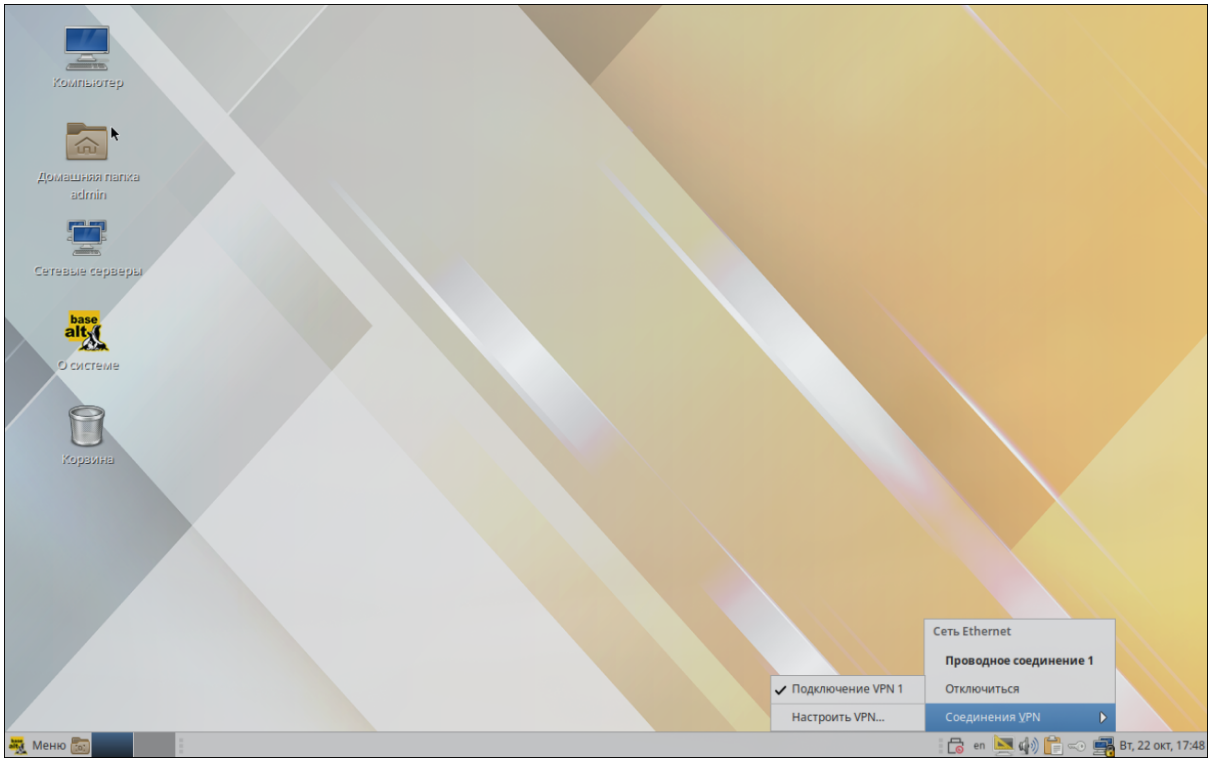
```
apt-get update && apt-get dist-upgrade && apt-get install NetworkManager-strongswan␣
↪NetworkManager-strongswan-gnome strongswan strongswan-charon-nm strongswan-testing
```

2. Установите корневой сертификат на рабочую станцию:

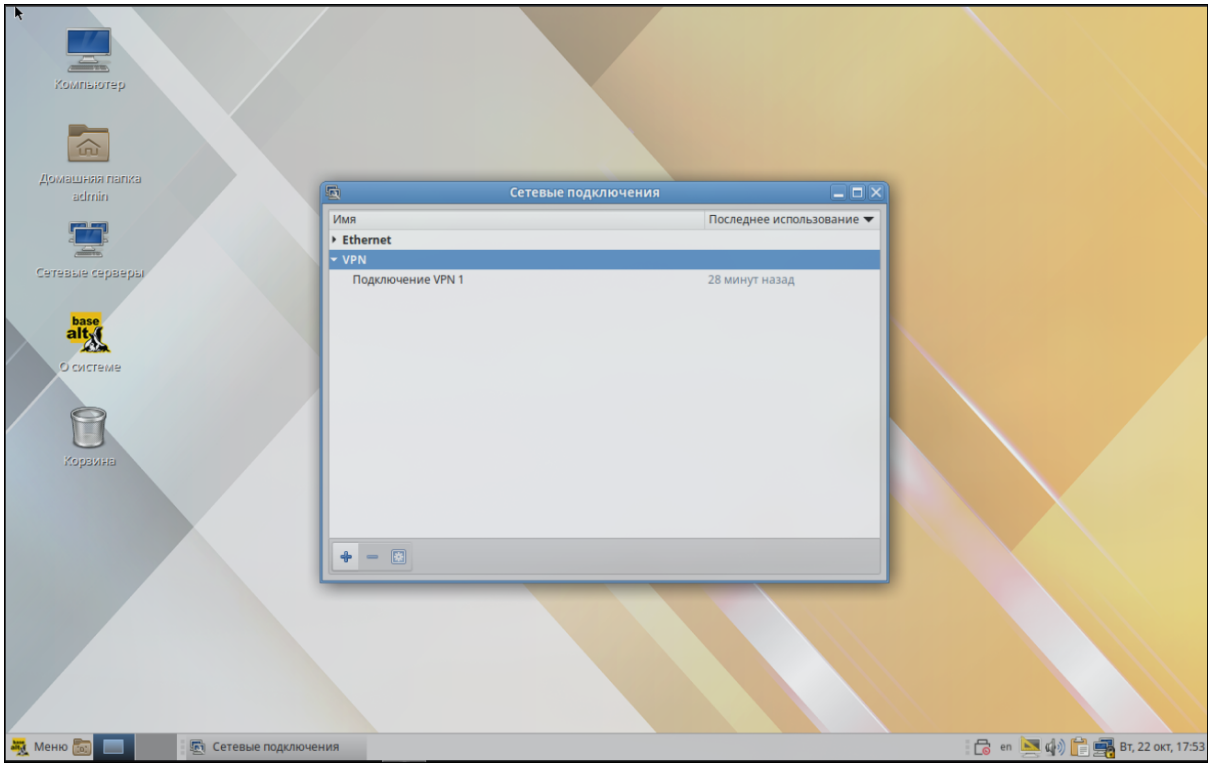
```
cp root-ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

- `root-ca.crt` - путь к сертификату.

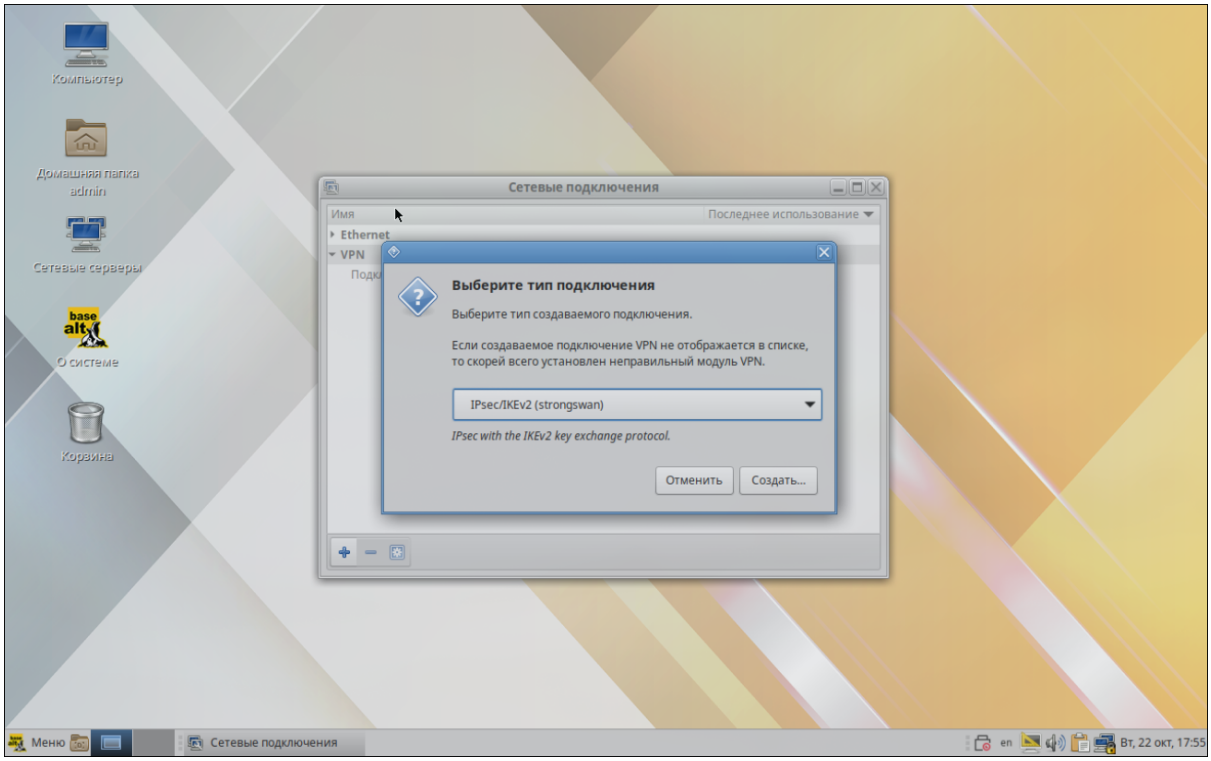
3. Перейдите в **Соединения VPN** и нажмите **Настроить VPN**:



4. Добавьте новое VPN-подключение:

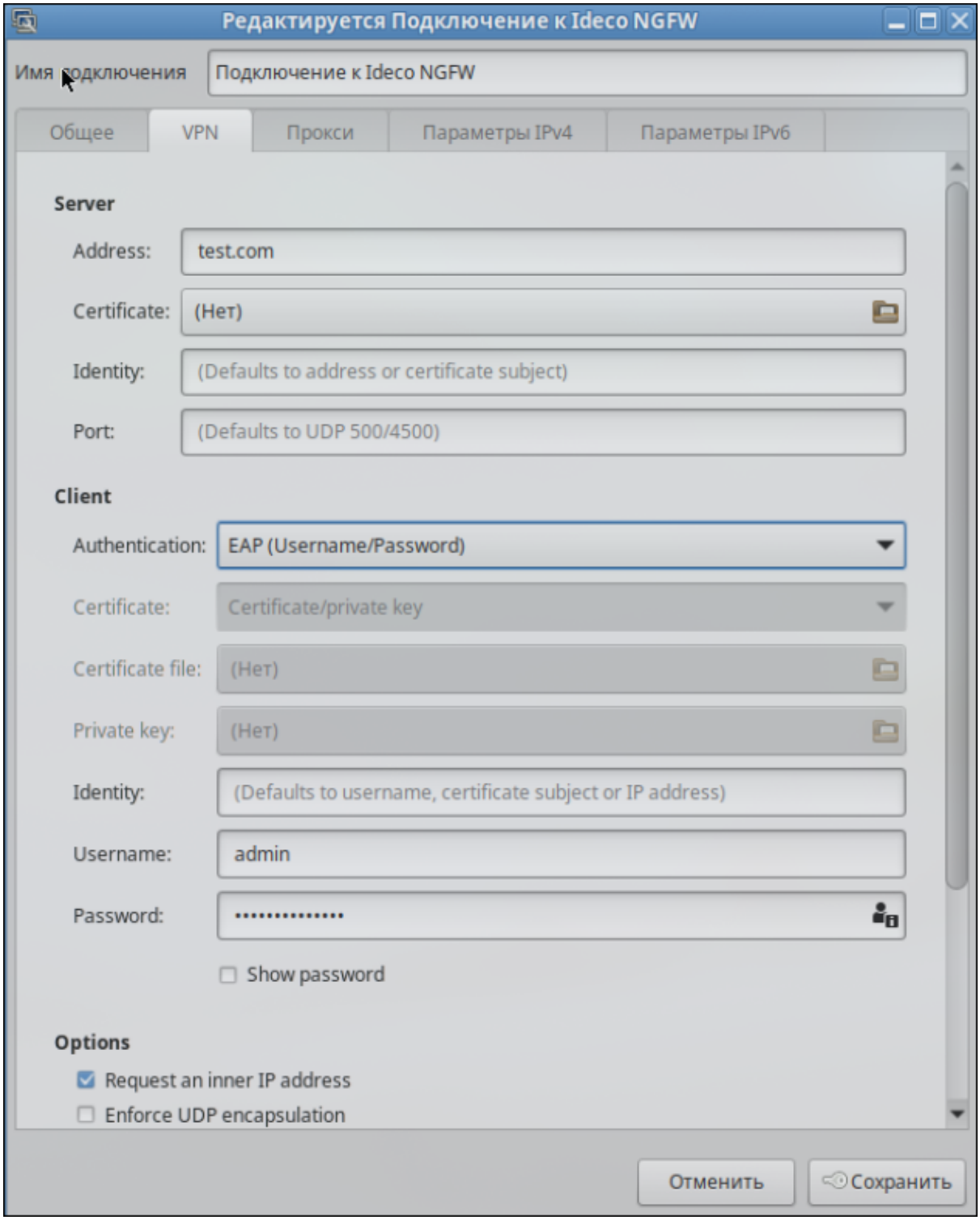


5. Выберите тип VPN-подключения `IPsec/IKEv2 (strongswan)` и нажмите **Создать**:

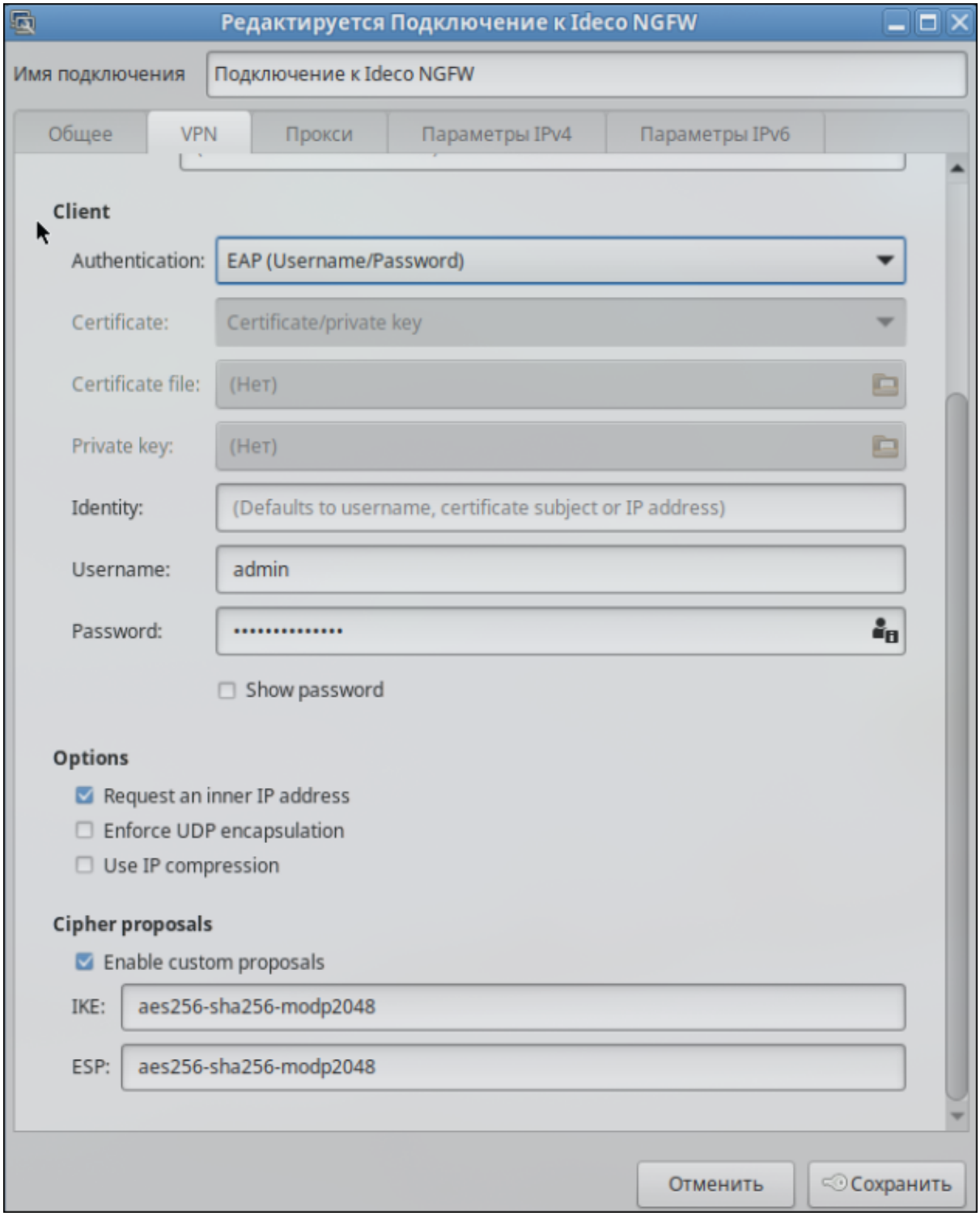


6. Заполните необходимые поля для создания VPN-подключения, как на скриншоте:

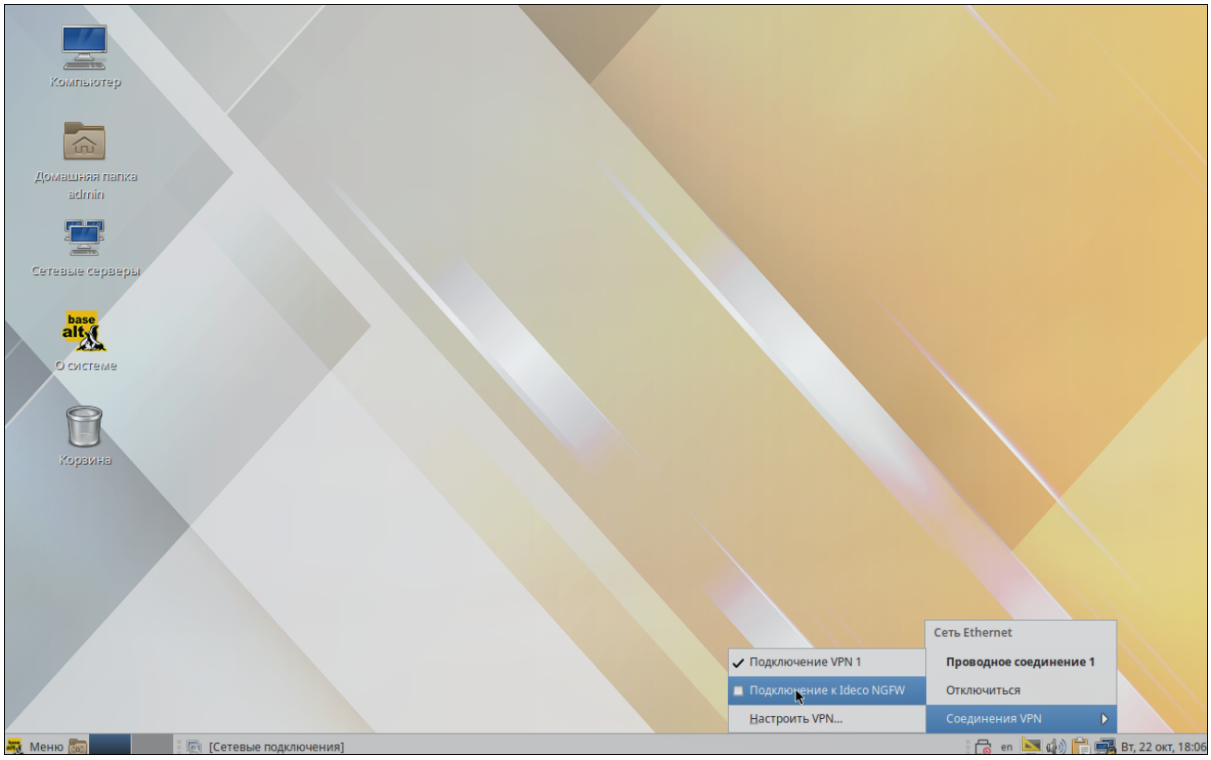
- Address - адрес шлюза;
- Authentication - тип аутентификации;
- Username - логин пользователя на Ideco NGFW;
- Password - пароль пользователя на Ideco NGFW.



7. Заполните параметры шифрования, как на скриншоте, и нажмите **Сохранить**:



8. Включите созданное VPN-подключение:



38.20.2 Создание VPN-подключения в Ubuntu

Основное

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

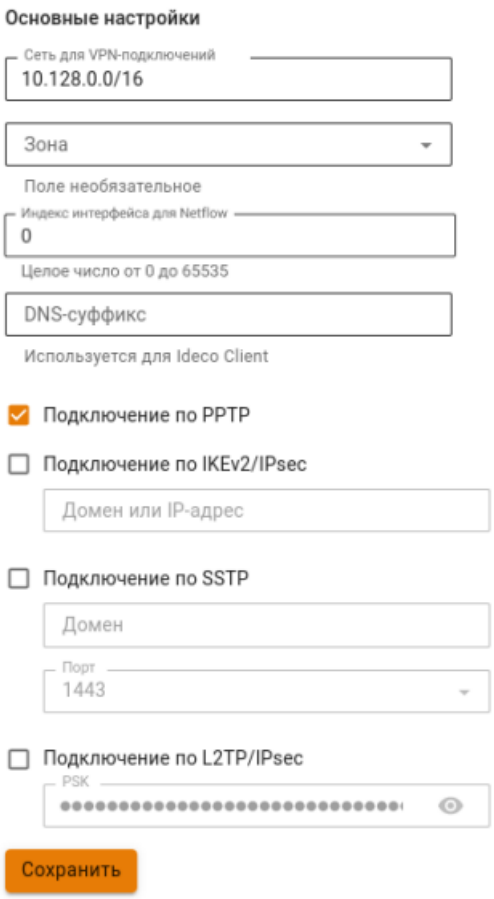
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Предупреждение: Инструкция актуальна для версии Ubuntu 24.04 LTS.

Протокол PPTP:

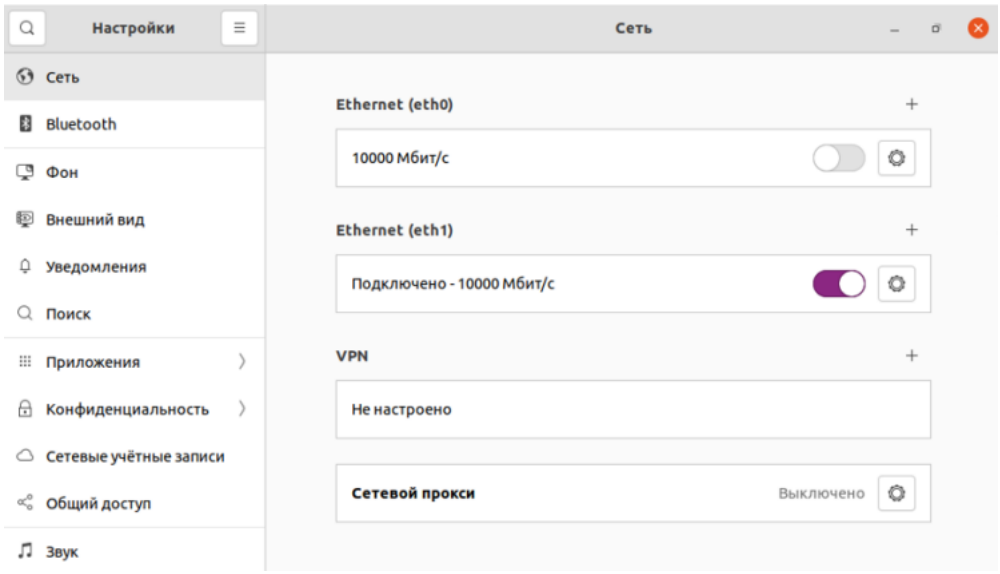
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное** и установите флаг **Подключение по PPTP**:

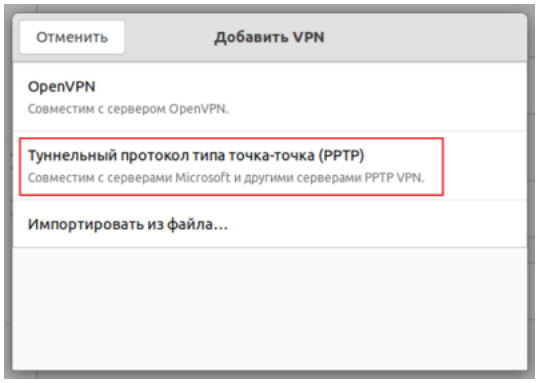


Создание подключения в Ubuntu:

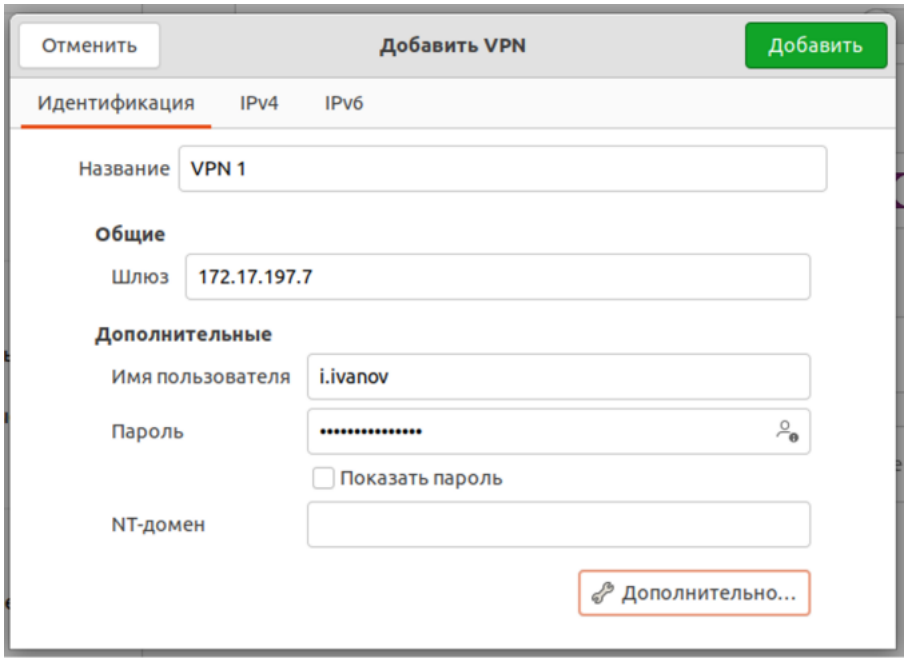
1. Перейдите **Настройки -> Сети** и в строке **VPN** нажмите + :



2. В окне создания подключений выберите пункт **Туннельный протокол типа точка-точка (PPTP)**:

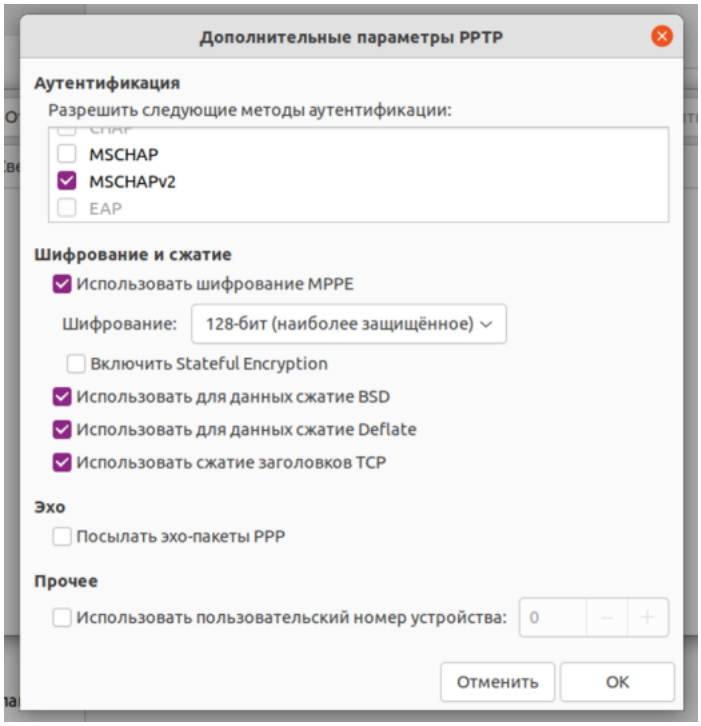


3. В разделе **Идентификация** заполните следующие поля:



- **Название** - имя подключения;
- **Шлюз** - доменное имя или IP-адрес интерфейса NGFW;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

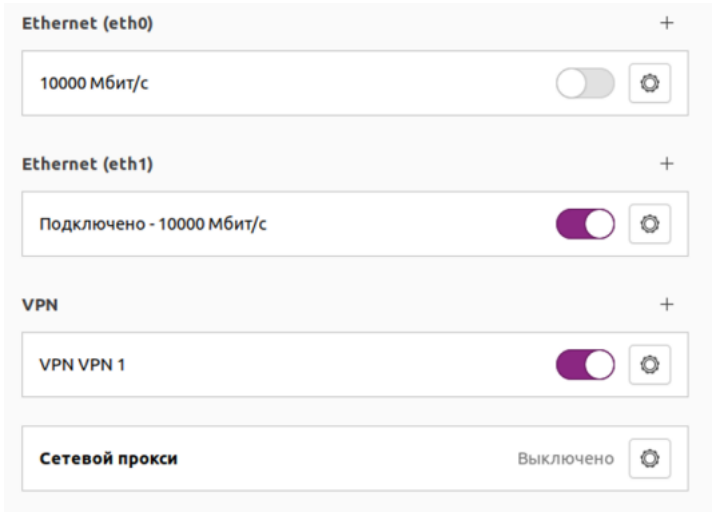
Рекомендуем нажать **Дополнительно** и установить флаги на пунктах:



- **Разрешить следующие методы аутентификации** - установите флаг на *MSCHAPv2*;
- **Использовать шифрование MPPE** - в строке *Шифрование* выберите 128-бит (наиболее защищенное);
- **Использовать для данных сжатие BSD** - использование алгоритма BSD-compress;
- **Использовать для данных сжатие Deflate** - использование алгоритма Deflate;
- **Использовать сжатие заголовков TCP** - использование метода сжатия заголовков TCP/IP Вана Якобсона.

4. Нажмите **ОК** и **Добавить**.

5. Включите созданное VPN-подключение:

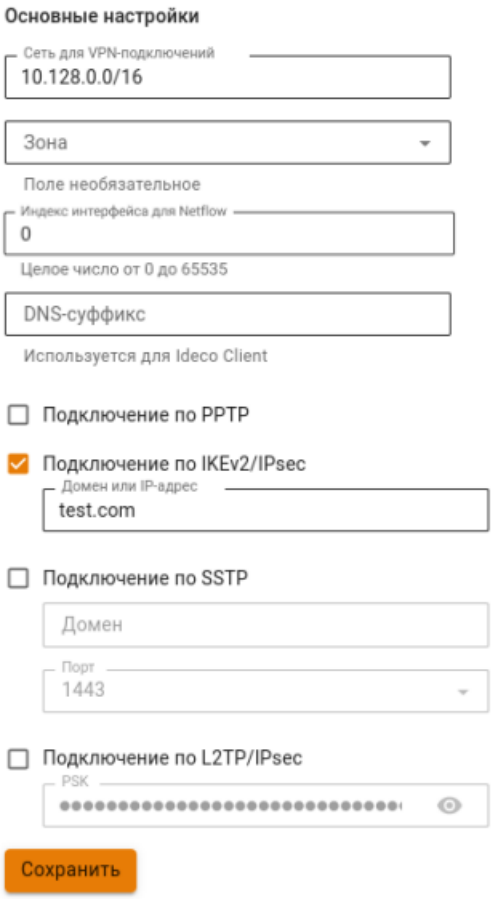


Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в Ubuntu:

1. Откройте терминал сочетанием клавиш Ctrl+Alt+F1 и выполните команду:

```
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-
↪extra-plugins
```

2. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

3. Перейдите в терминале в директорию с загруженным корневым сертификатом (если на доменное имя NGFW выпущен Let`s Encrypt сертификат, сразу перейдите к пункту 6).

4. Установите корневой сертификат NGFW в доверенные сертификаты Ubuntu:

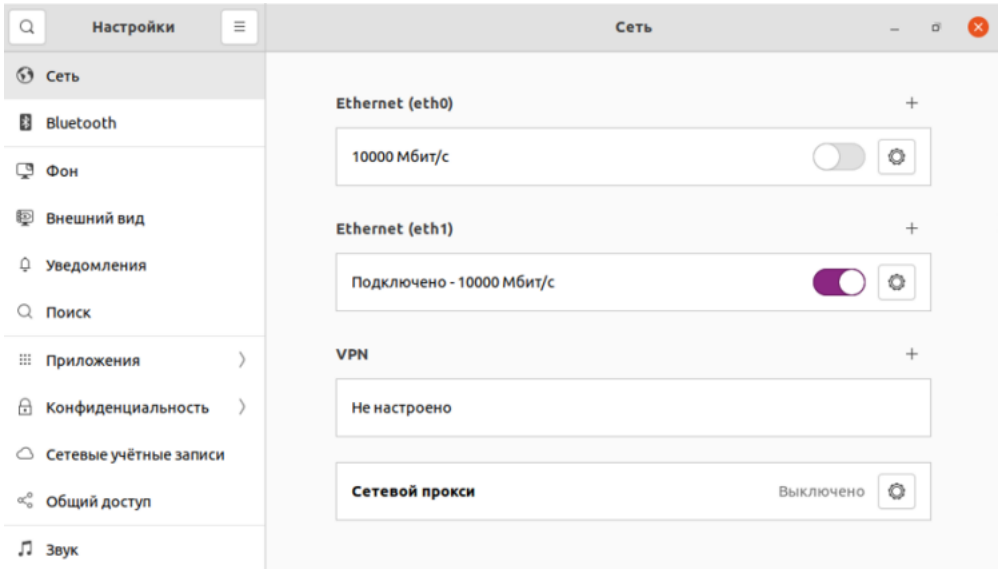
```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

- `ca.crt` - имя скачанного сертификата.

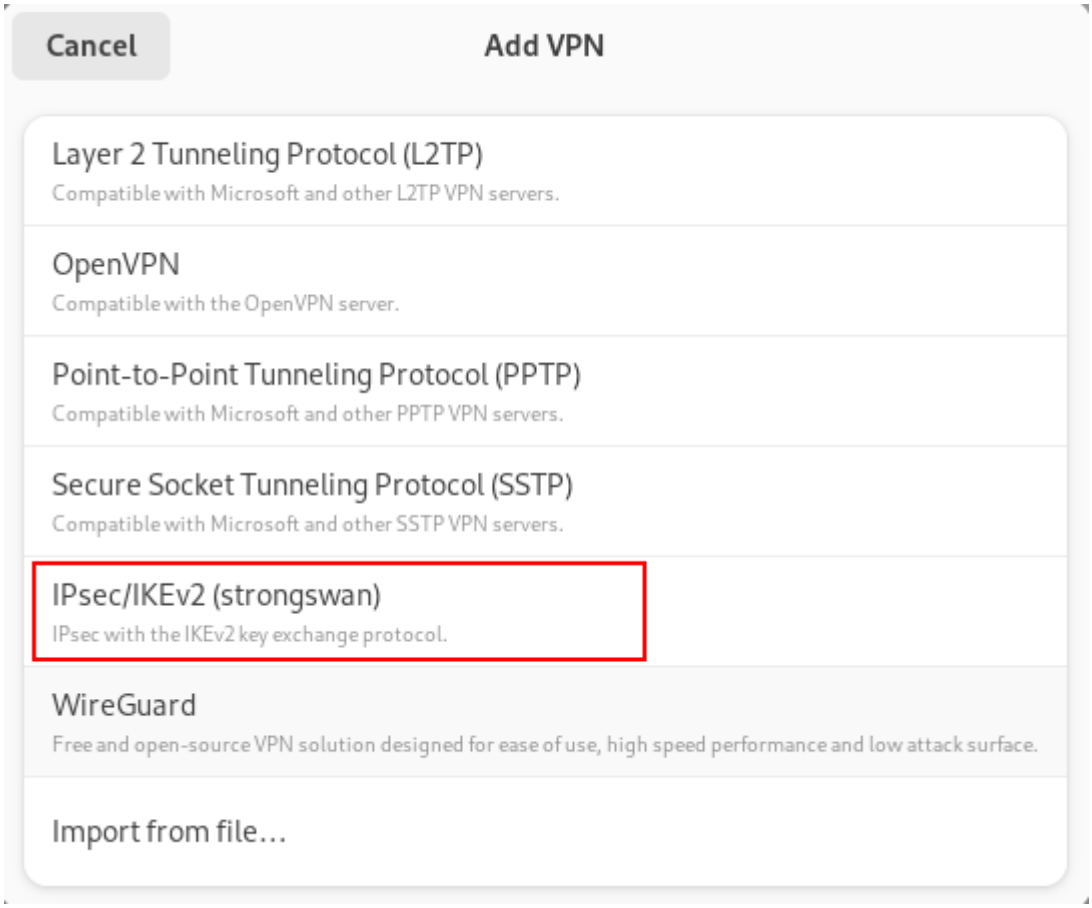
5. Для обновления сертификатов устройства выполните команду:

```
sudo update-ca-certificates
```

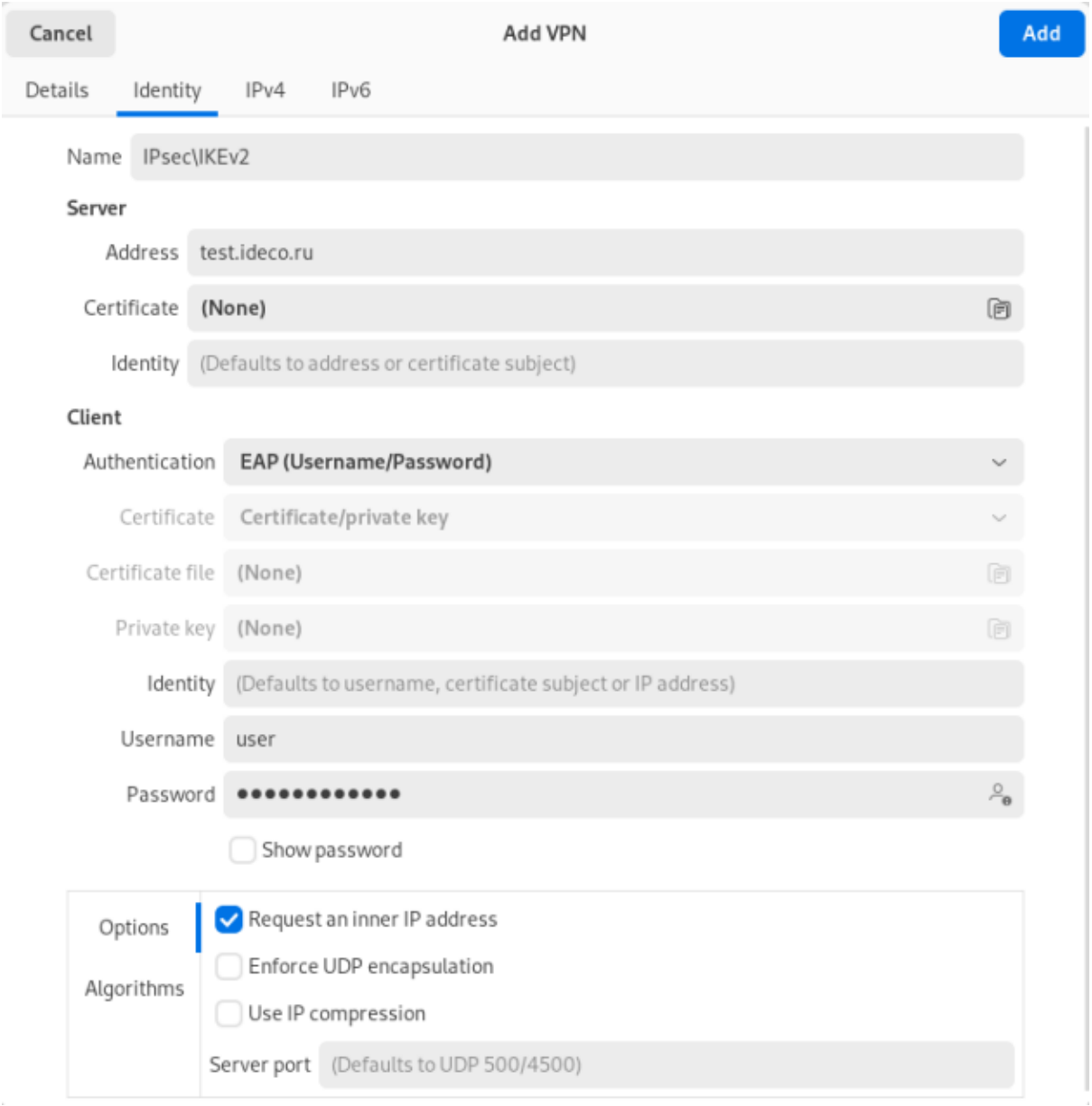
6. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + :



7. В появившемся окне выберите **IPsec\IKEv2 (strongswan)**:



8. В разделе **Идентификация** и заполните следующие поля:



- **Название** - имя подключения;
- **Address** - введите домен, который указан в настройках **Пользователи -> VPN-подключения -> Основное -> Подключение по IKEv2/IPsec**;
- **Authentication** - рекомендуем выбрать EAP;
- **Username** - имя пользователя, которому разрешено подключение по VPN;
- **Password** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения.

Установите флаг **Request an inner IP address** и нажмите **Добавить**.

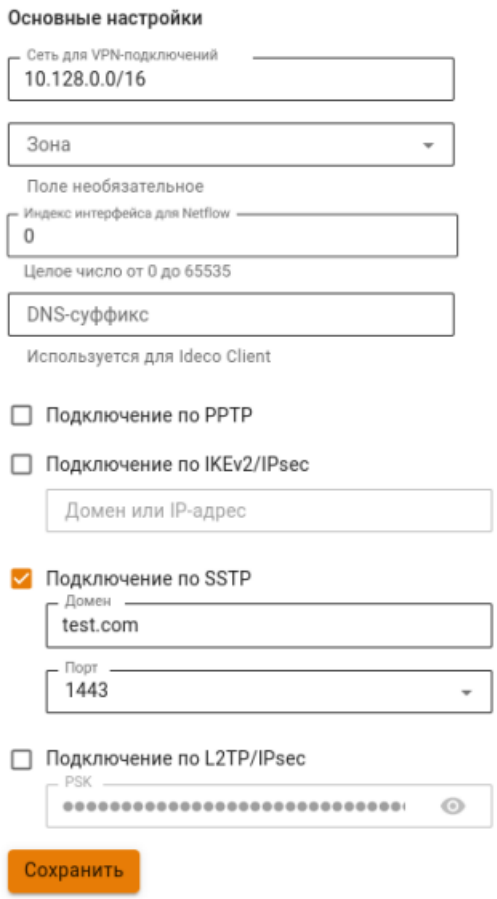
9. Включите созданное VPN-подключение.

Протокол SSTP:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в Ubuntu:

1. Откройте терминал и выполните две команды:

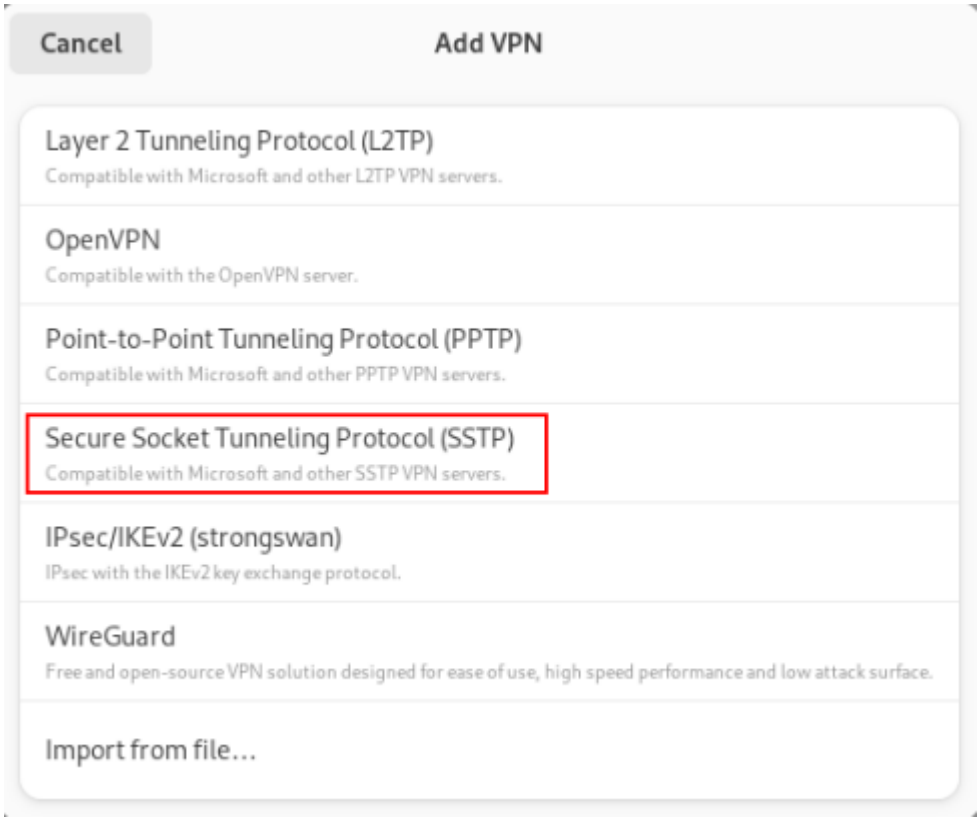
```
sudo apt-add-repository ppa:eivnaes/network-manager-sstp
sudo apt install -y network-manager-sstp sstp-client
```

2. По окончании установки перезагрузите компьютер:

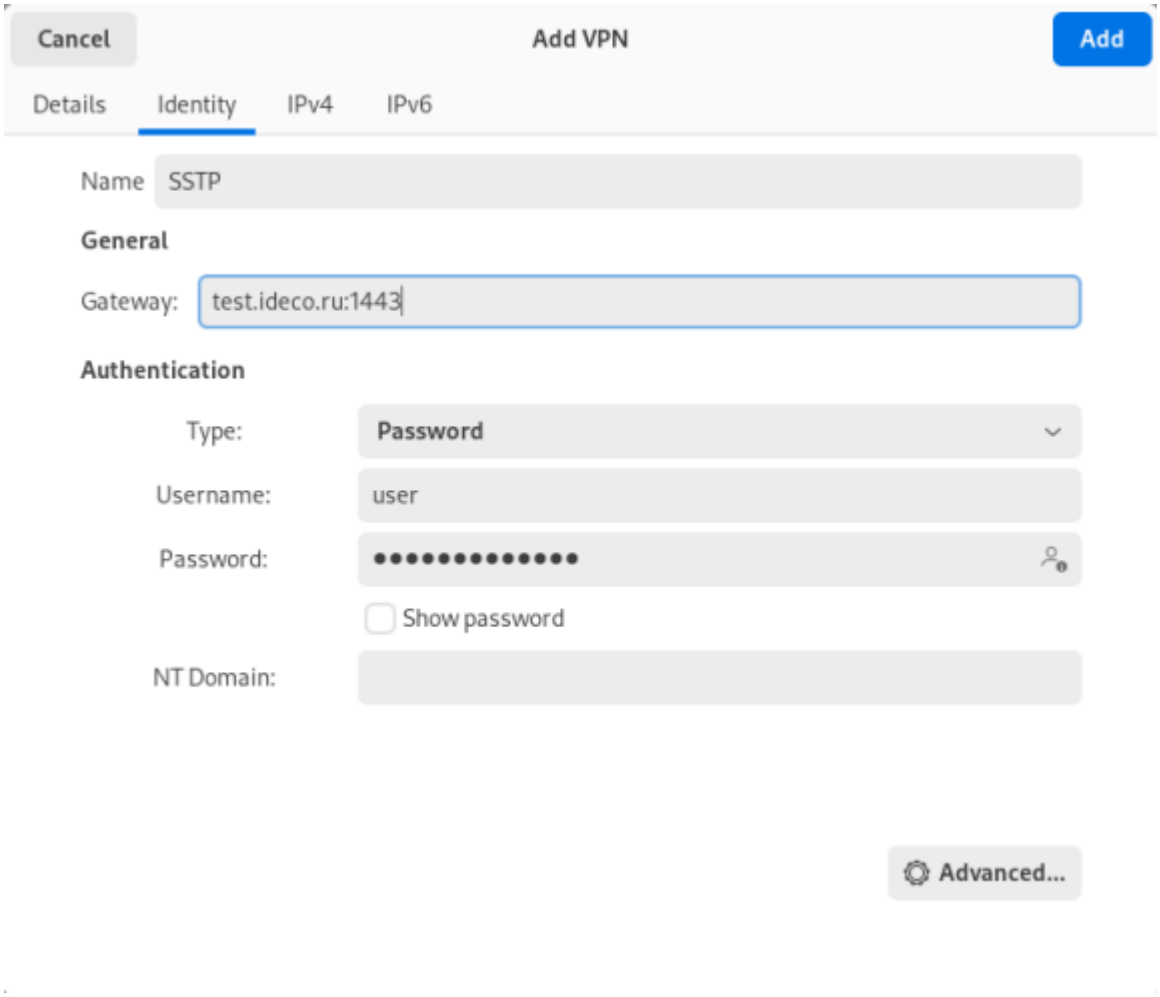
```
sudo reboot
```

3. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + .

4. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)** (**Туннельный протокол типа точка-точка (SSTP)**):



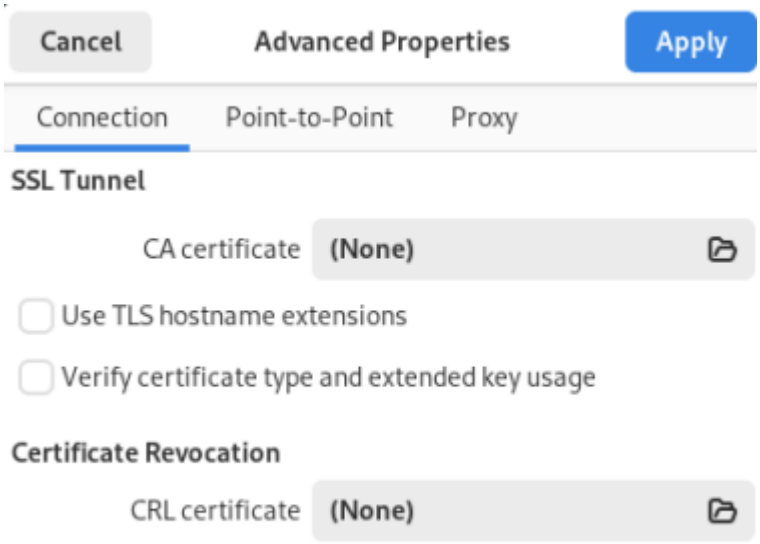
5. В разделе **Identity (Идентификация)** заполните следующие поля:



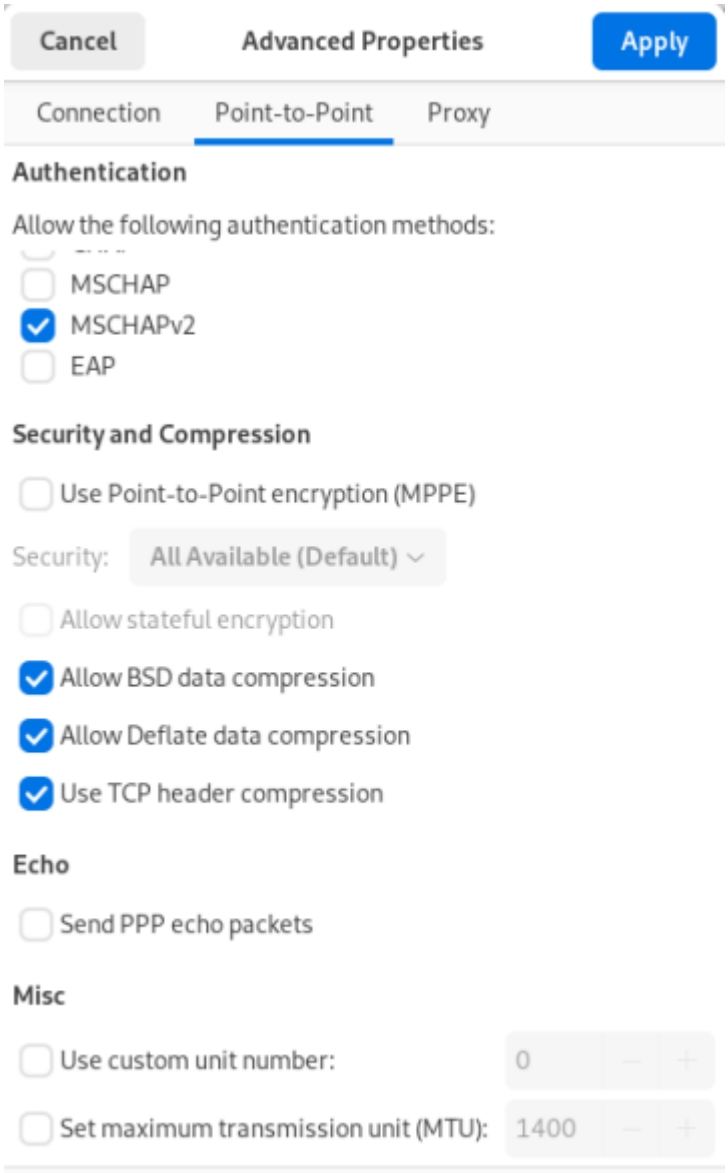
- **Название** - имя подключения;
- **Шлюз** - укажите в формате *домен:[порт, выбранный на NGFW]*;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

6. Нажмите **Advanced**:

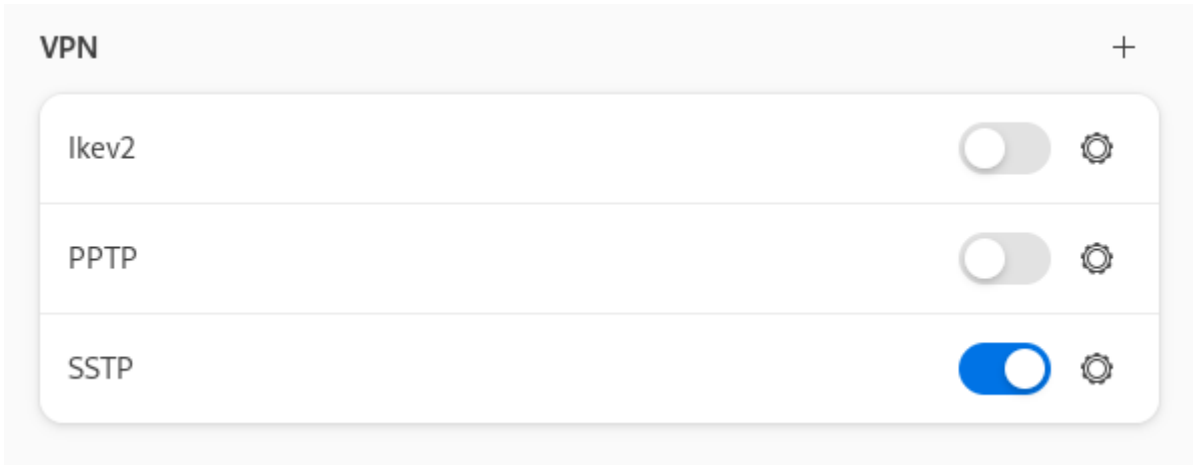
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**;
  - **Verify certificate type and extended key usage**:



- На вкладке **Point-to-Point**:
  - **Разрешить следующие методы аутентификации** - установите флаг только на *MSCHAPv2*;
  - **Использовать для данных сжатие BSD** - включите использование алгоритма BSD-compress;
  - **Использовать для данных сжатие Deflate** - включите использование алгоритма Deflate;
  - **Использовать сжатие заголовков TCP** - включите использование метода сжатия заголовков TCP/IP Вана Якобсона:



6. Нажмите **Добавить** и включите созданное VPN-подключение:



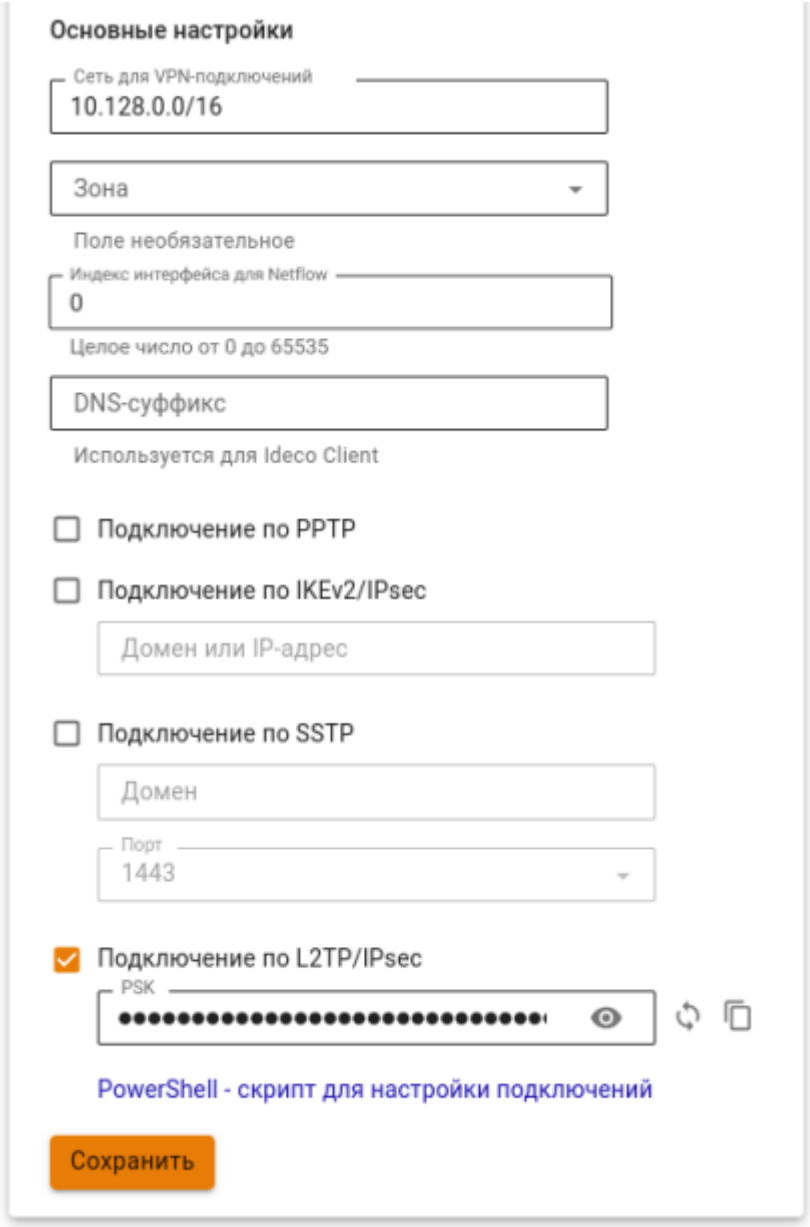
Протокол L2TP/IPsec:

Важно: L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их более одного. Рекомендуем вместо L2TP IPsec использовать IKEv2 IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Ubuntu:

1. Подключите репозиторий, в котором находятся необходимые пакеты для создания L2TP VPN-соединения, а затем обновите информацию о репозиториях. Для этого выполните следующие команды:

```
sudo add-apt-repository ppa:nm-l2tp/network-manager-l2tp
sudo apt update
```

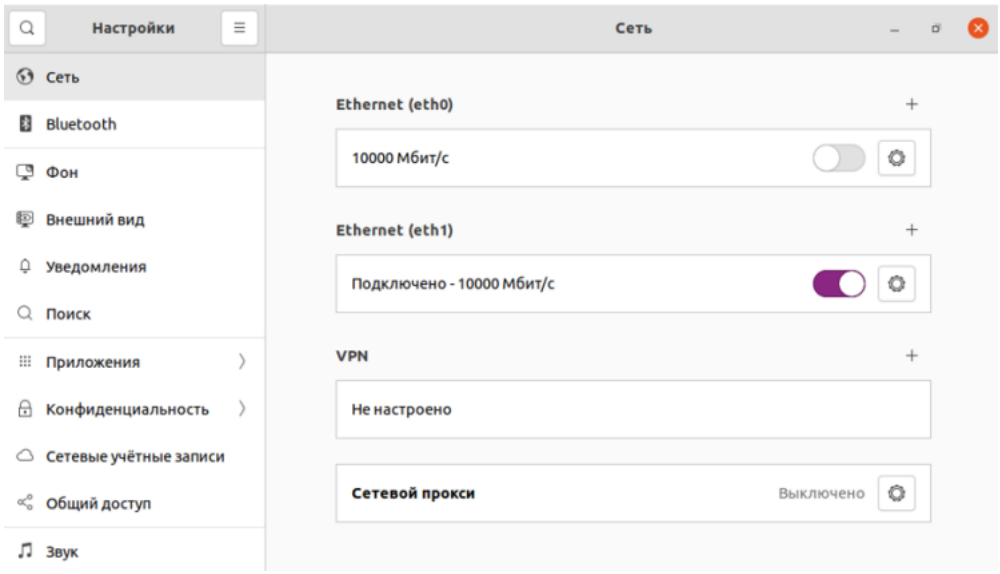
2. Установите дополнение к стандартному NetworkManager с помощью двух пакетов:

```
sudo apt install -y network-manager-l2tp network-manager-l2tp-gnome
```

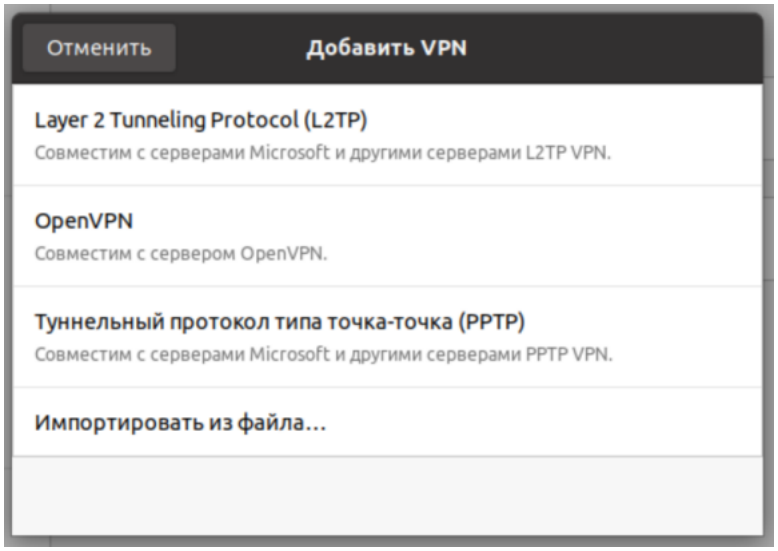
3. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

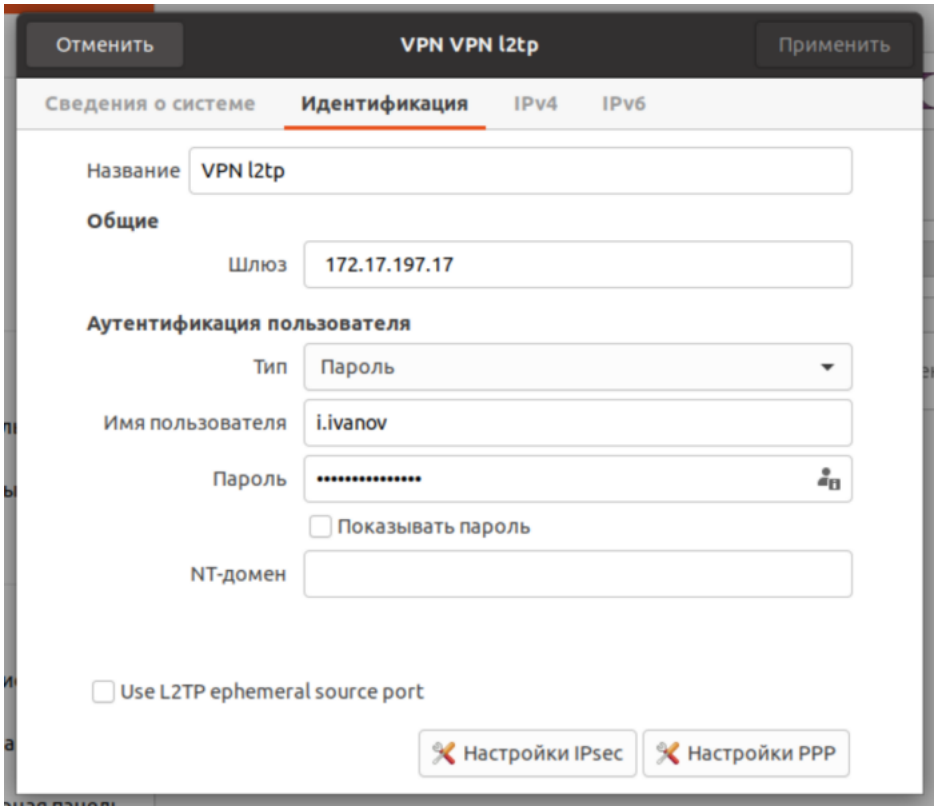
4. После окончания установки пакетов перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + :



5. В окне создания подключений по VPN выберите пункт **Layer 2 Tunneling Protocol (L2TP)**:

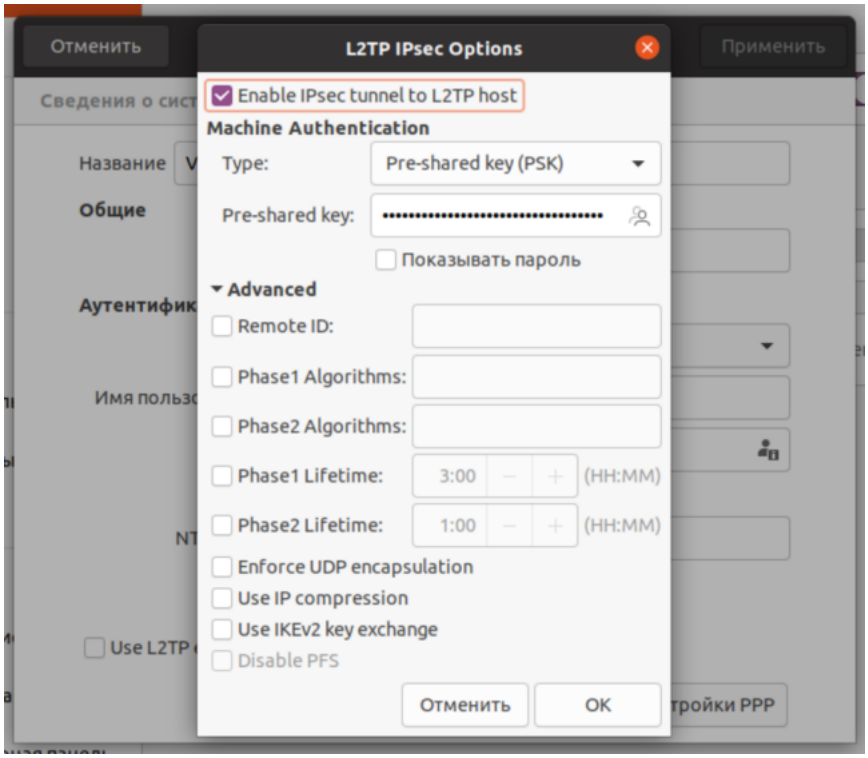


6. На вкладке **Идентификация** заполните следующие поля:



- **Название** - имя подключения;
- **Шлюз** - доменное имя или IP-адрес интерфейса NGFW;
- **Тип** - Password (аутентификация по имени пользователя и паролю);
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

7. Перейдите в **Настройки IPsec** и включите настройку **Enable IPsec tunnel to L2TP host**, чтобы активировалась возможность настраивать остальные параметры:

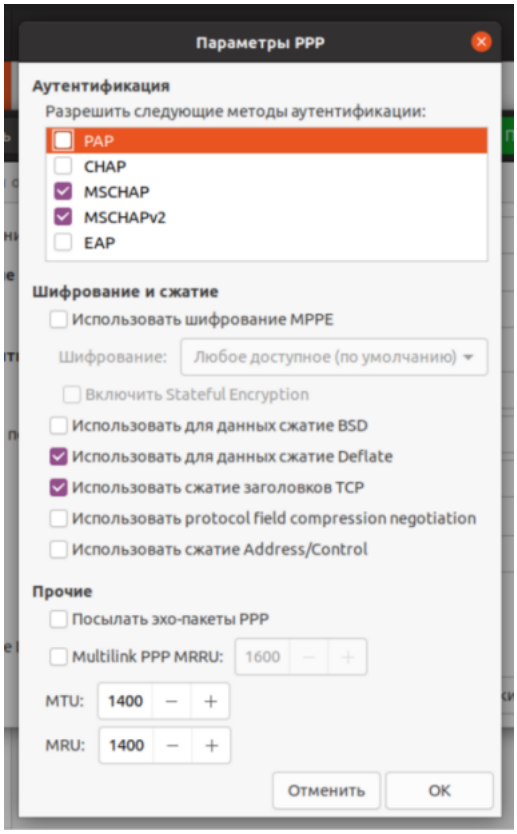


- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу;
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи -> VPN-подключения -> Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения.

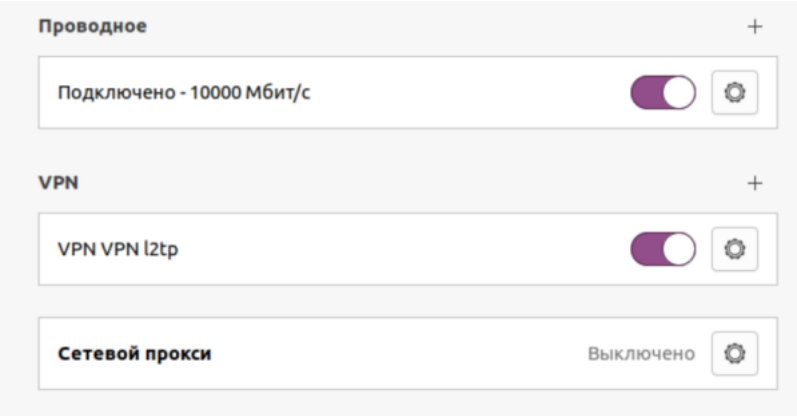
После окончания настройки **L2TP IPsec Options** нажмите **ОК**.

8. При необходимости перейдите в **Настройки PPP** и настройте раздел **Аутентификация**, **Шифрование и сжатие** и **Прочие**:



После настройки **Параметры PPP** нажмите **ОК** и **Применить**.

9. Включите созданное VPN-подключение:



38.20.3 Создание VPN-подключения в Fedora

Основное

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Перед настройкой подключения загрузите на устройство корневой сертификат Ideco NGFW (включая всю цепочку доверия) или **ISRG_ROOT_X1** сертификат при использовании сертификата Let`s encrypt.

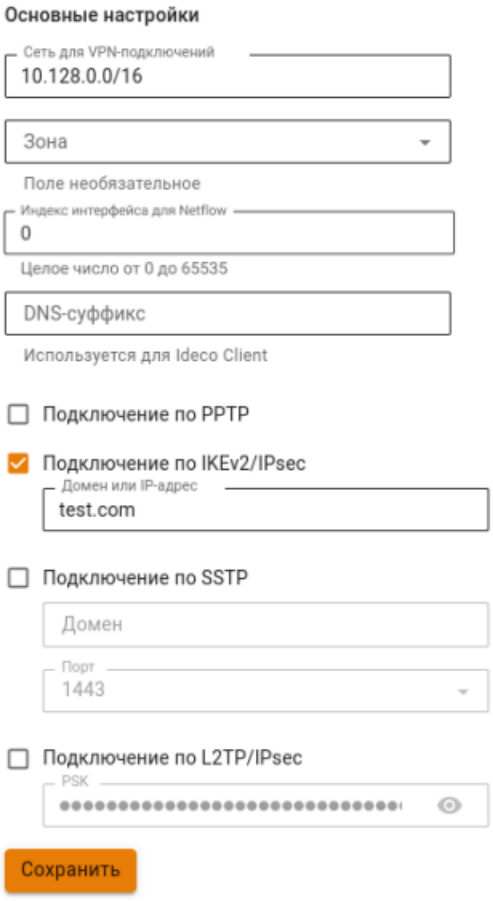
> **Предупреждение:** Файл сертификата должен находится в общедоступном каталоге.
>
> Если загрузить корневой сертификата NGFW (включая всю цепочку доверия) в каталог `/etc/strongswan/ipsec.d/cacerts`, то не потребуется указывать сертификат при настройке подключения.
>
> Если в системе уже имеется сертификат **ISRG_ROOT_X1**, то загружать его отдельно не требуется.
>
> При настройке подключения в Fedora 40 **не требуется** загружать сертификат **ISRG_ROOT_X1**, поскольку он уже есть в системе. Сертификат находится в каталоге `/etc/ssl/certs`

Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Создание подключения в Fedora

1. Для поддержки подключения по IPsec для NetworkManager установите пакет **NetworkManager-strongswan**:

```
sudo dnf -y install NetworkManager-strongswan
```

2. Установите пакет для настройки IPsec-подключения через графический интерфейс:

- Окружение рабочего стола GNOME:

```
sudo dnf -y install NetworkManager-strongswan-gnome
```

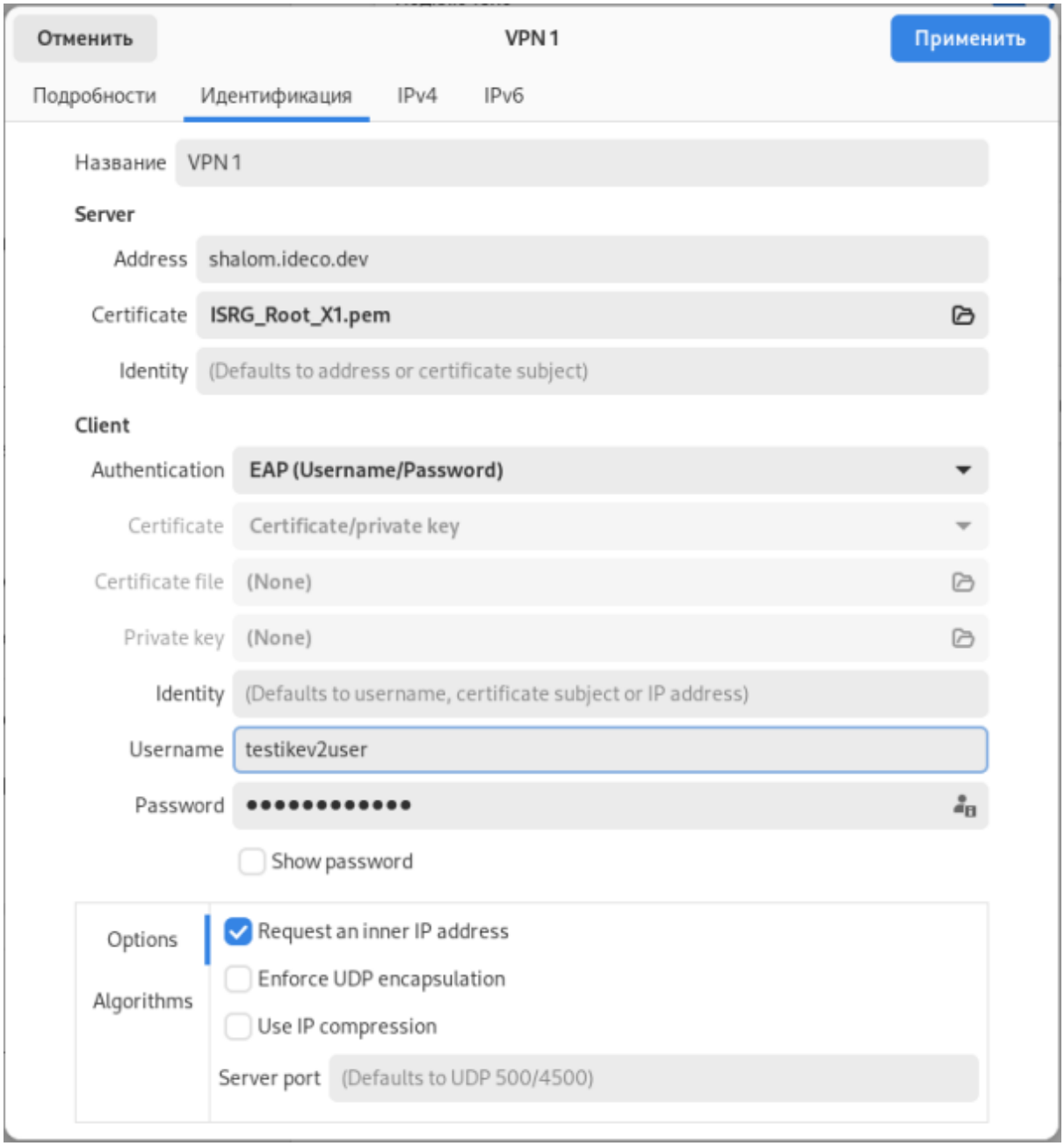
- Окружение рабочего стола KDE:

```
sudo dnf -y install plasma-nm-strongswan
```

Создание подключения в Fedora:

1. Перейдите в настройки VPN-подключений на компьютере и выберите тип **IKEV2**.

2. Заполните поля:



- **Название** - название VPN-подключения;

- **Address** - доменное имя шлюза для VPN-подключения;
- **Certificate** - сертификат, загруженный на шаге 1;
- **Authentication** - EAP;
- **Username** - имя пользователя на Ideco NGFW;
- **Password** - пароль пользователя на Ideco NGFW.

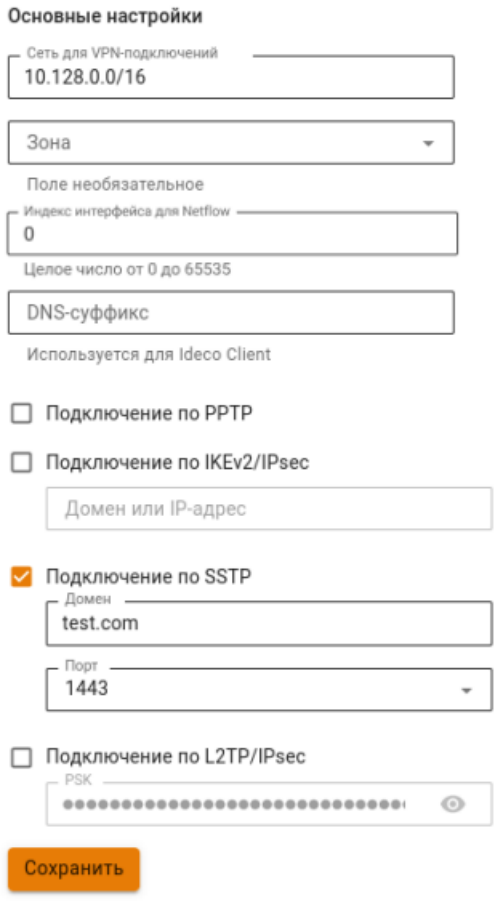
3. Нажмите **Применить** и подключитесь к Ideco NGFW.

Протокол SSTP:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Создание подключения в Fedora:

1. Откройте терминал и установите необходимые пакеты, выполнив команду:

- Окружение рабочего стола GNOME:

```
sudo dnf install NetworkManager-sstp.x86_64 NetworkManager-sstp-gnome.x86_64 sstp-
↪client.x86_64
```

- Окружение рабочего стола KDE:

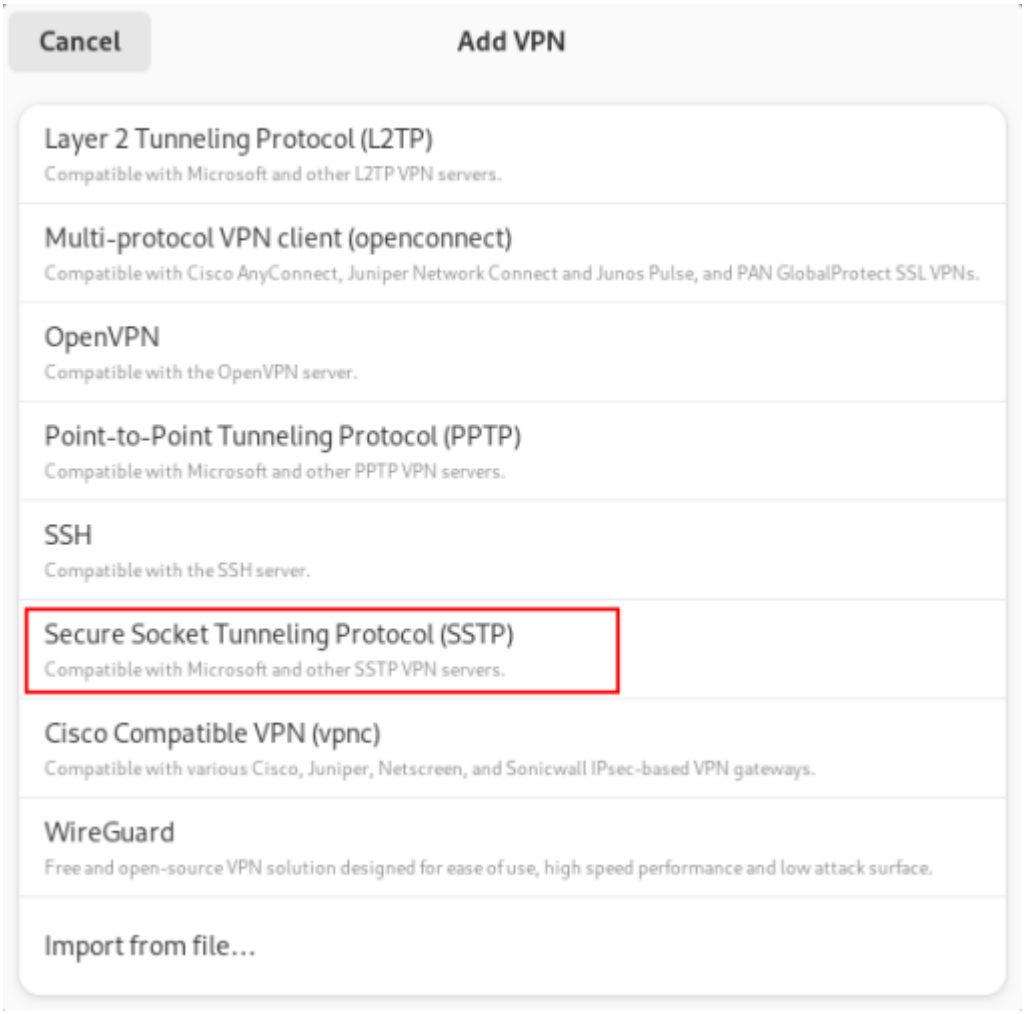
```
sudo dnf install NetworkManager-sstp.x86_64 plasma-nm-sstp.x86_64 sstp-client.x86_64
```

2. По окончании установки перезагрузите компьютер:

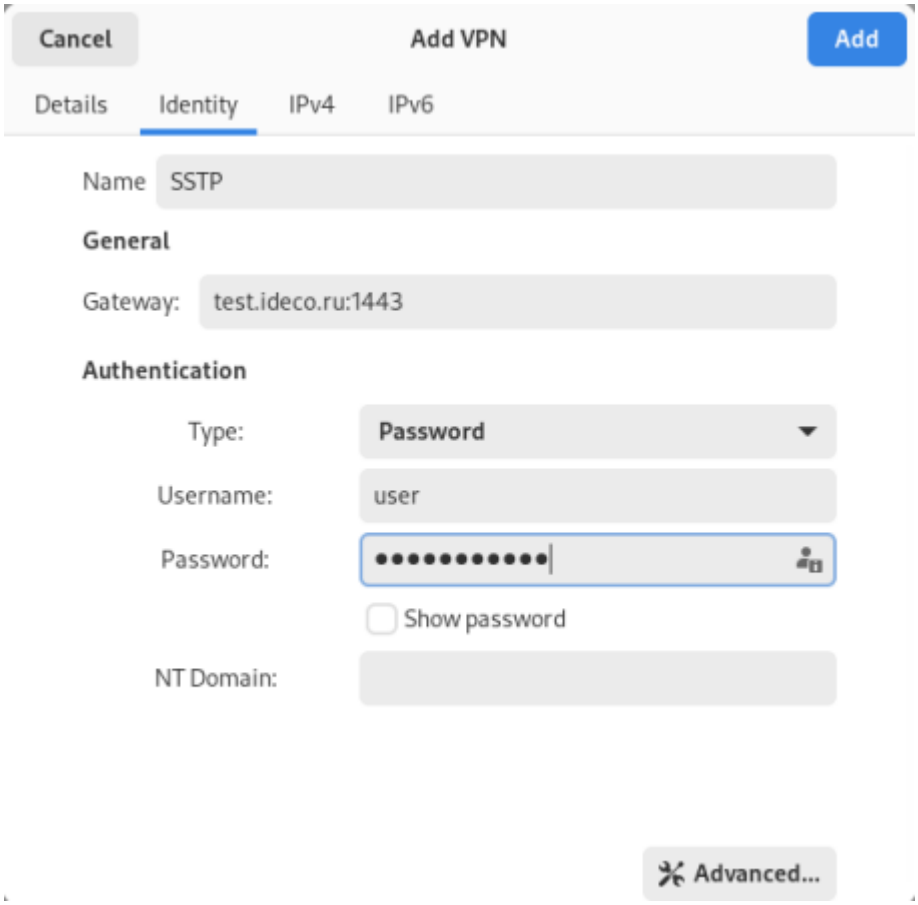
```
sudo reboot
```

3. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + .

4. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)** или **Туннельный протокол типа точка-точка (SSTP)**:



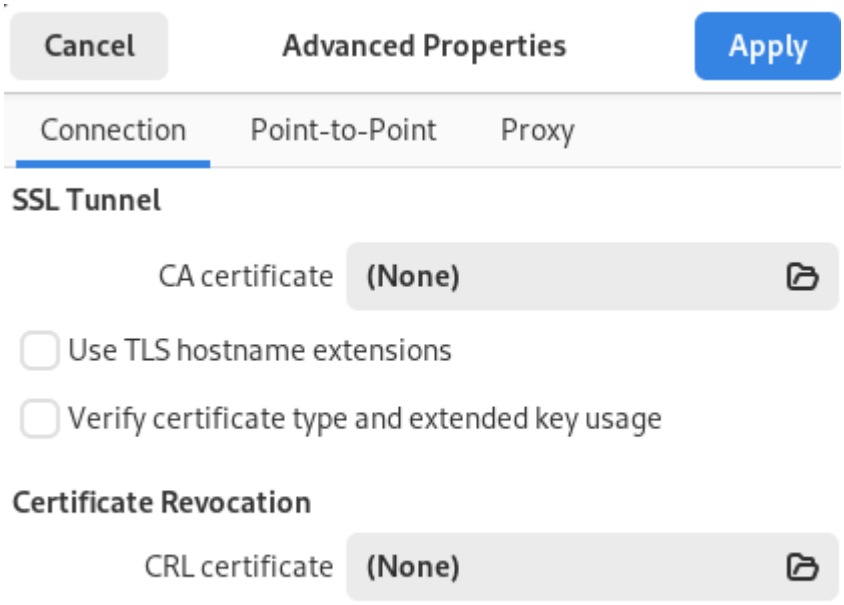
5. В разделе **Identity (Идентификация)** заполните следующие поля:



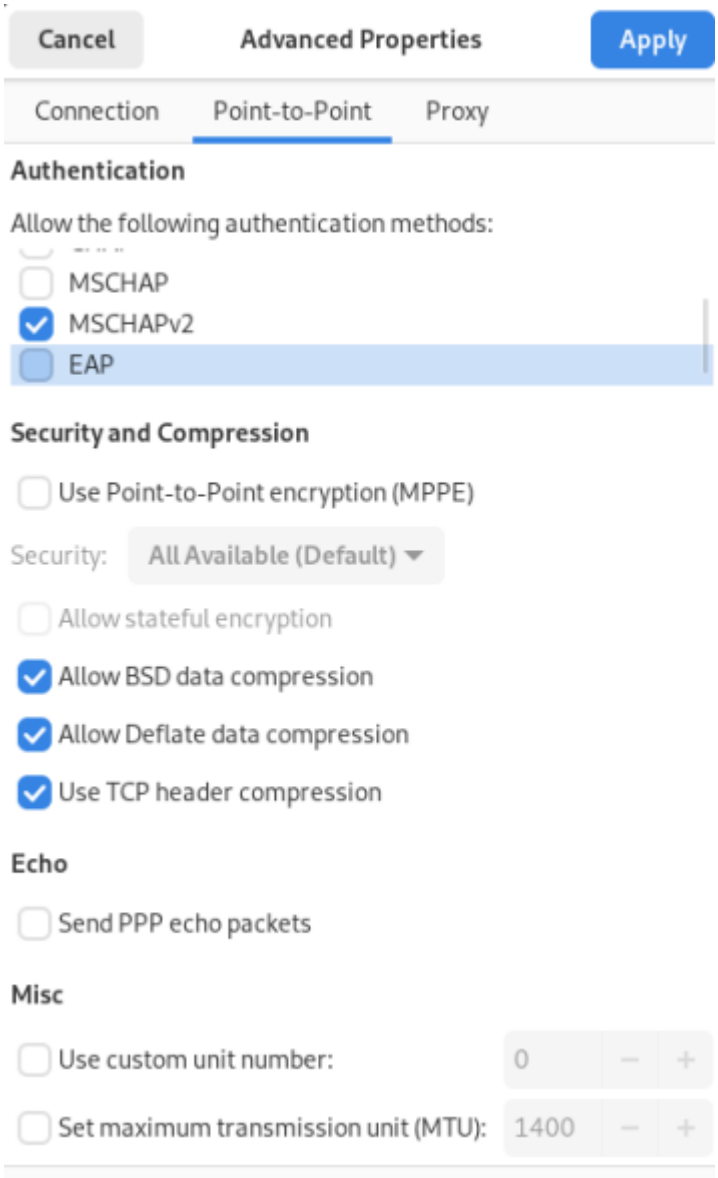
- **Название** - имя подключения;
- **Шлюз** - укажите в формате `домен:<порт, выбранный на NGFW>`;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

6. Нажмите **Advanced**:

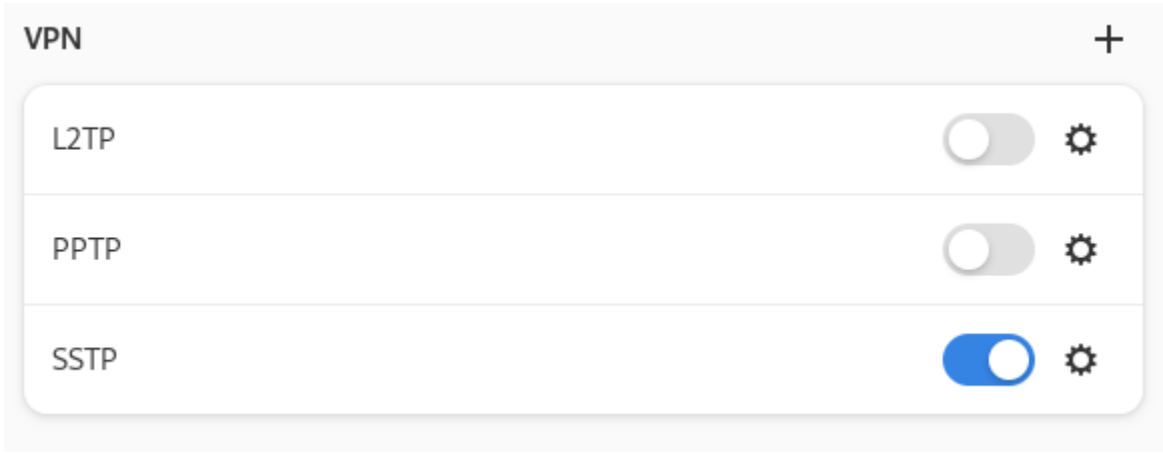
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**;
  - **Verify certificate type and extended key usage**:



- На вкладке **Point-to-Point**:
  - **Разрешить следующие методы аутентификации** - установите флаг только на *MSCHAPv2*;
  - **Использовать для данных сжатие BSD** - включите использование алгоритма BSD-compress;
  - **Использовать для данных сжатие Deflate** - включите использование алгоритма Deflate;
  - **Использовать сжатие заголовков TCP** - включите использование метода сжатия заголовков TCP/IP Вана Якобсона:



7. Нажмите **Добавить** и включите созданное VPN-подключение:



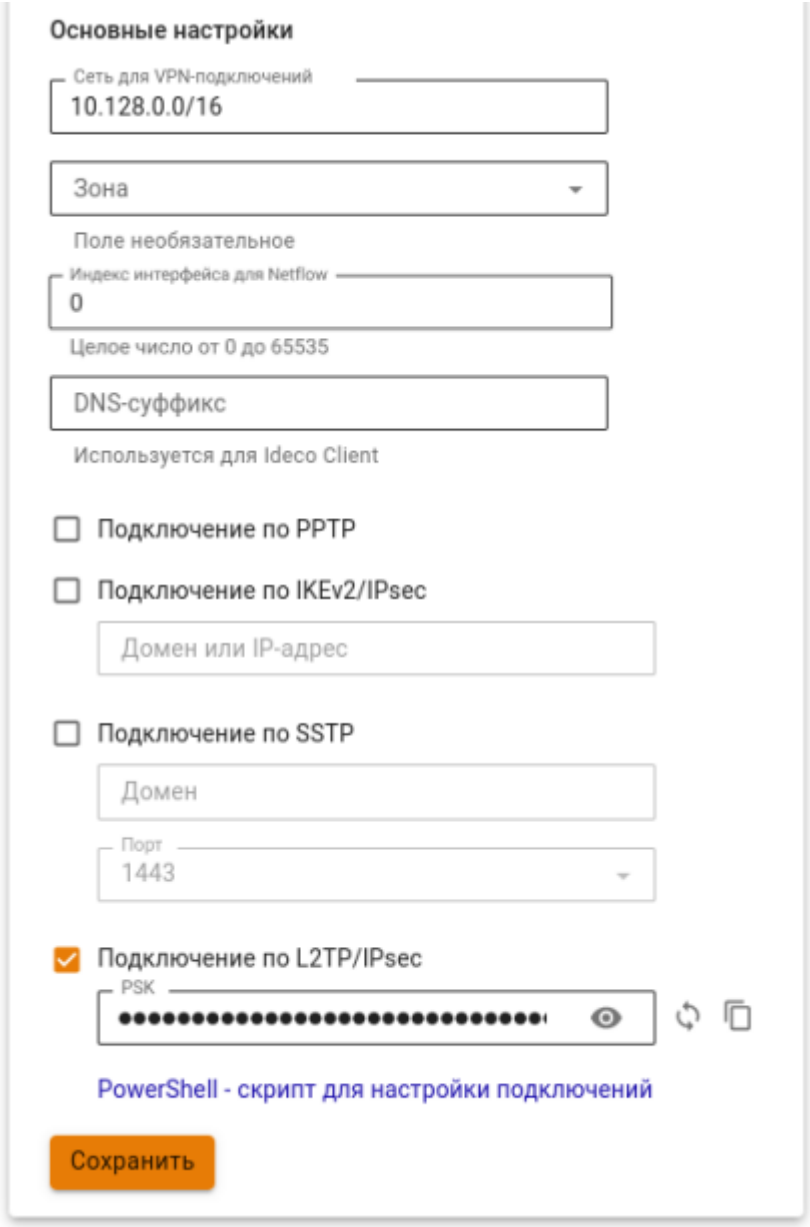
Протокол L2TP/IPsec:

Важно: L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их более одного. Рекомендуем вместо L2TP IPsec использовать IKEv2 IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Fedora:

1. Установите необходимые пакеты для создания L2TP VPN-соединения, выполнив следующую команду:

- Окружение рабочего стола GNOME:

```
sudo dnf install NetworkManager-l2tp.x86_64 NetworkManager-l2tp-gnome.x86_64 xl2tpd.
↪x86_64
```

- Окружение рабочего стола KDE:

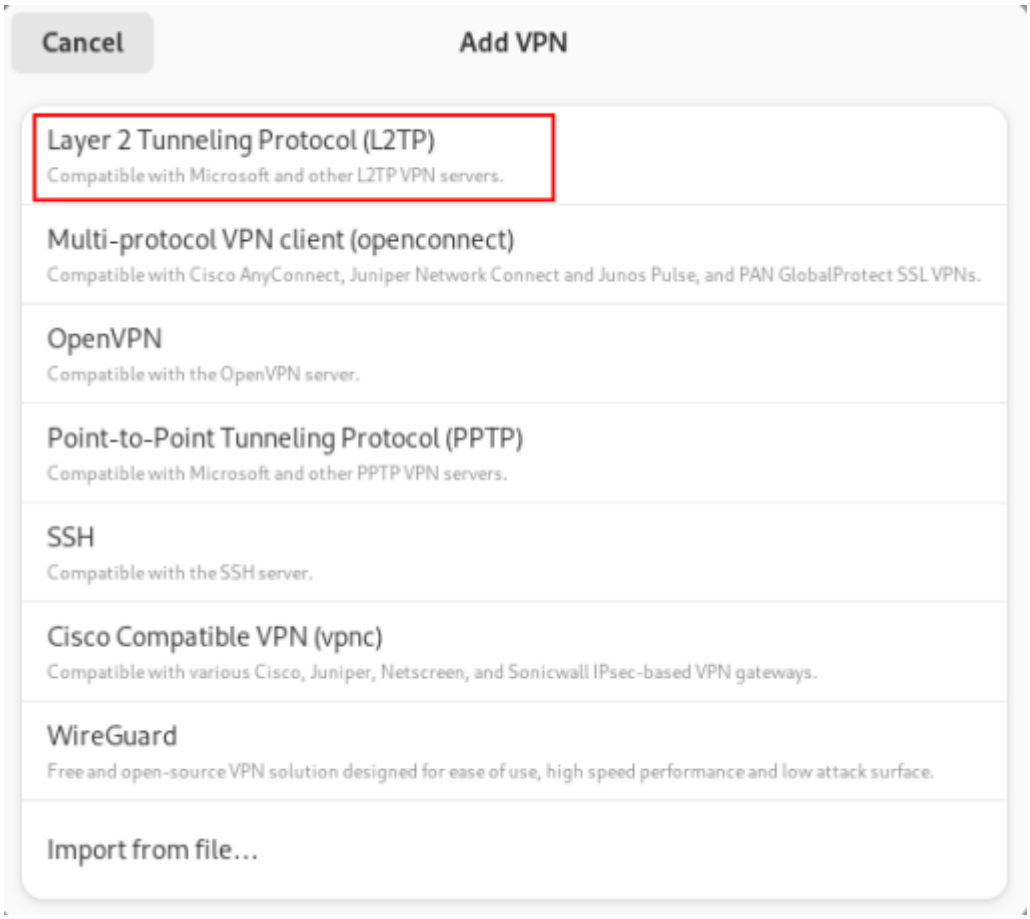
```
sudo dnf install NetworkManager-l2tp.x86_64 plasma-nm-l2tp.x86_64 xl2tpd.x86_64
```

2. После окончания установки перезагрузите компьютер:

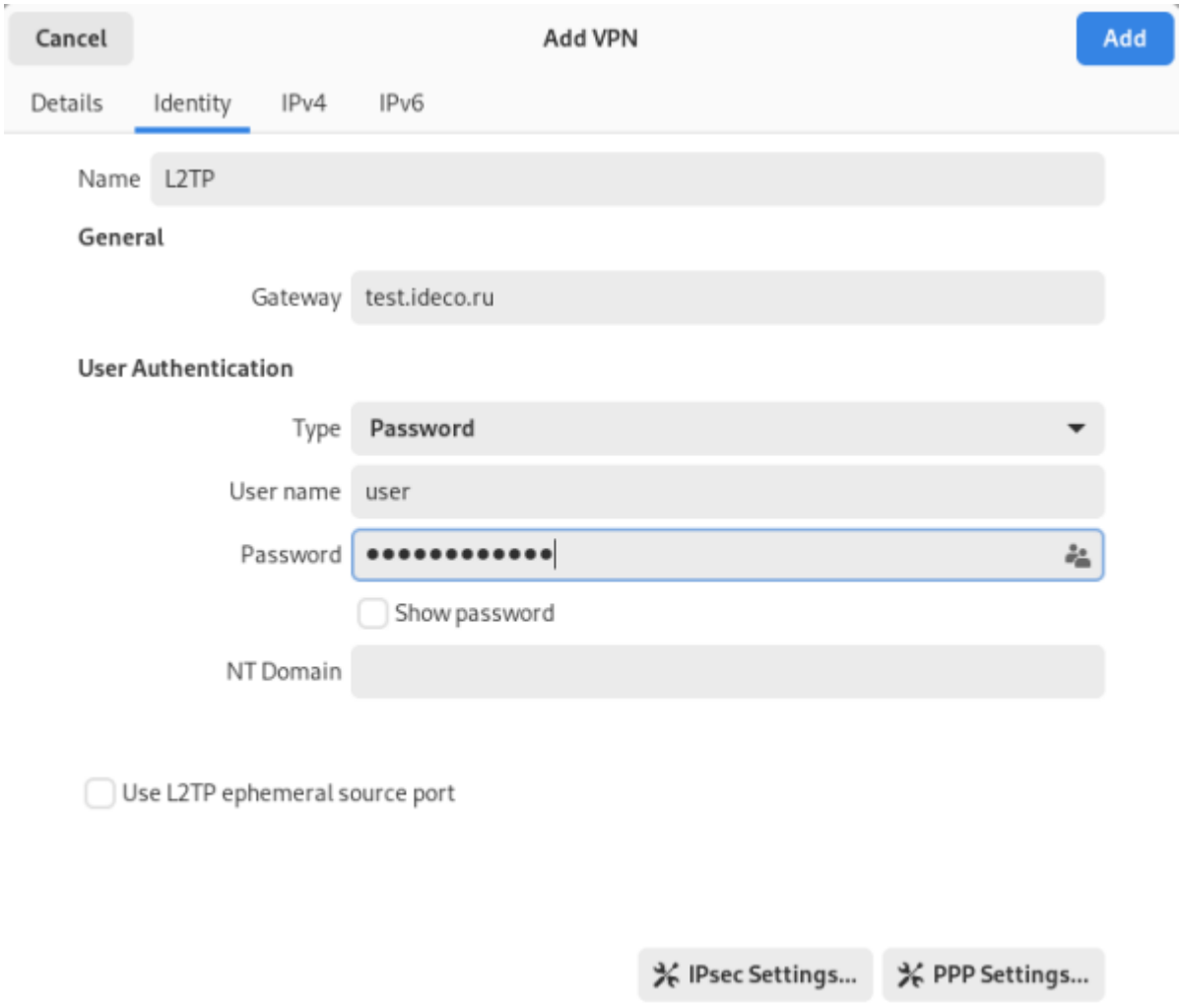
```
sudo reboot
```

4. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + .

5. В окне создания подключений по VPN выберите пункт **Layer 2 Tunneling Protocol (L2TP)**:

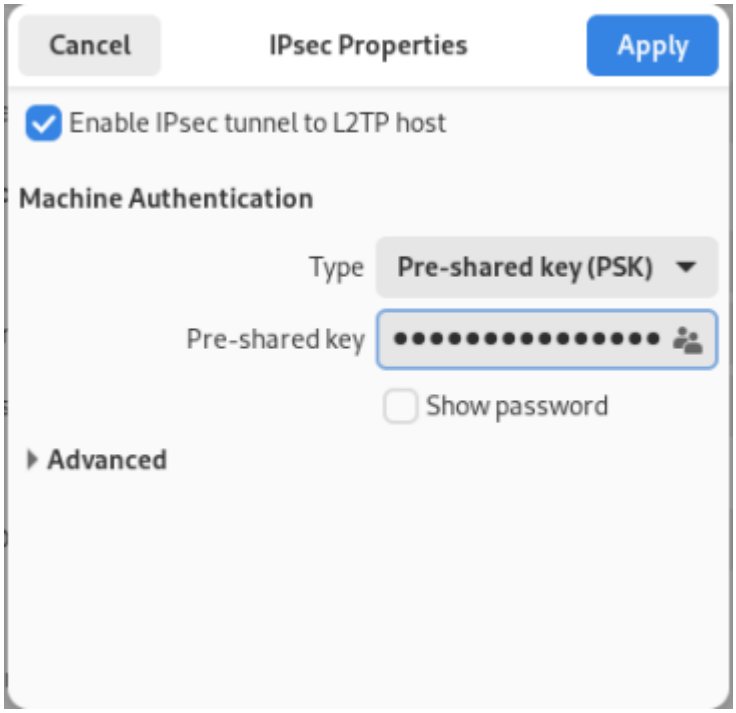


6. На вкладке **Идентификация** заполните следующие поля:



- **Название** - имя подключения;
- **Шлюз** - доменное имя или IP-адрес интерфейса NGFW;
- **Тип** - Password (аутентификация по имени пользователя и паролю);
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

7. Перейдите в **Настройки IPsec** и включите настройку **Enable IPsec tunnel to L2TP host**, чтобы активировалась возможность настраивать остальные параметры:

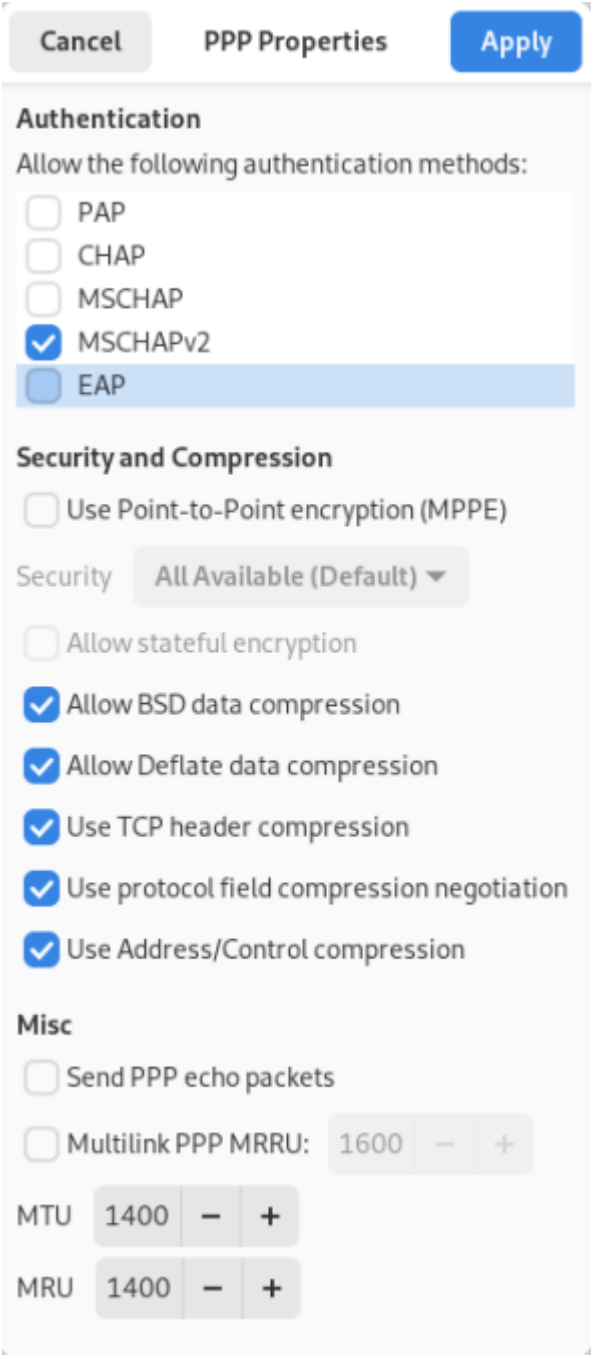


- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу;
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи -> VPN-подключения -> Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения.

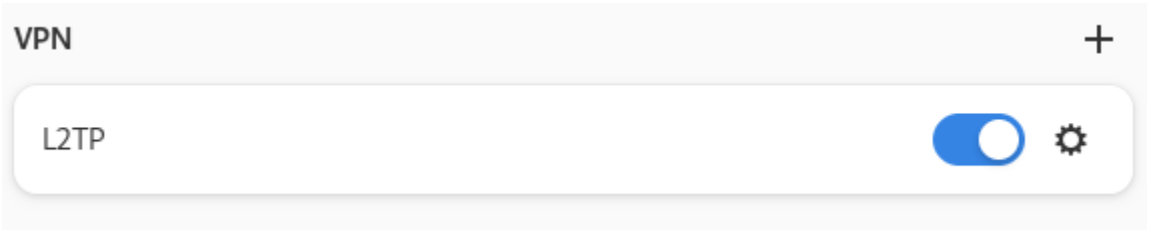
После окончания настройки **L2TP IPsec Options** нажмите **ОК**.

8. При необходимости перейдите в **Настройки PPP** и настройте раздел **Аутентификация**, **Шифрование и сжатие** и **Прочие**:



После настройки **Параметров PPP** нажмите **ОК** и **Применить**.

9. Включите созданное VPN-подключение:



38.20.4 Создание подключения в Astra Linux

Основное

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

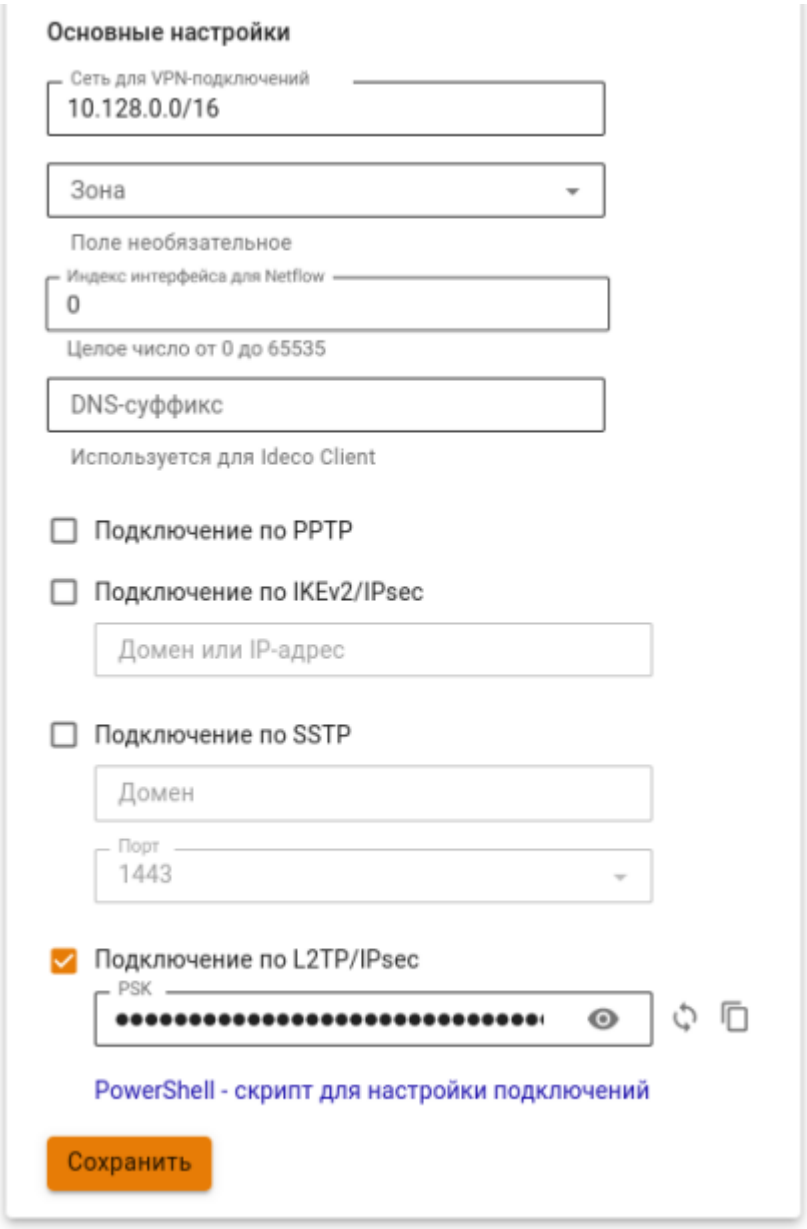
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Протокол L2TP/IPsec:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

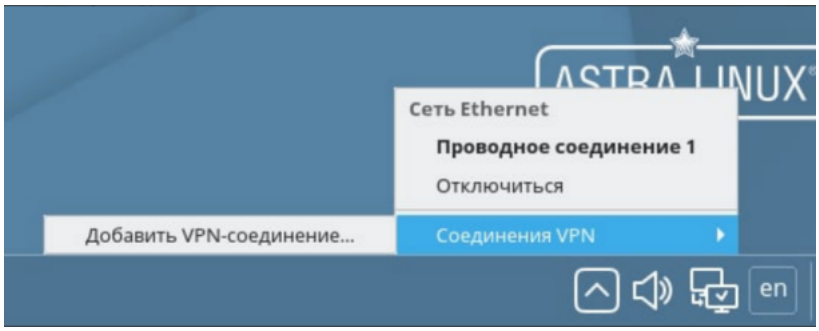


Создание подключения в Astra Linux:

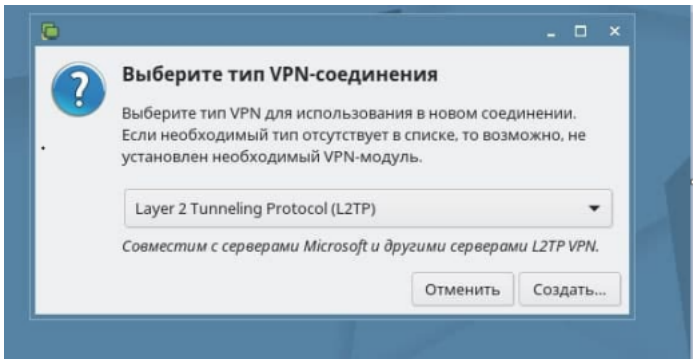
1. Откройте терминал сочетанием клавиш Ctrl+Alt+F1 или через путь **Пуск -> Системные -> Терминал Fly** и выполните три команды:

```
sudo apt update
sudo apt install network-manager-l2tp-gnome
sudo reboot
```

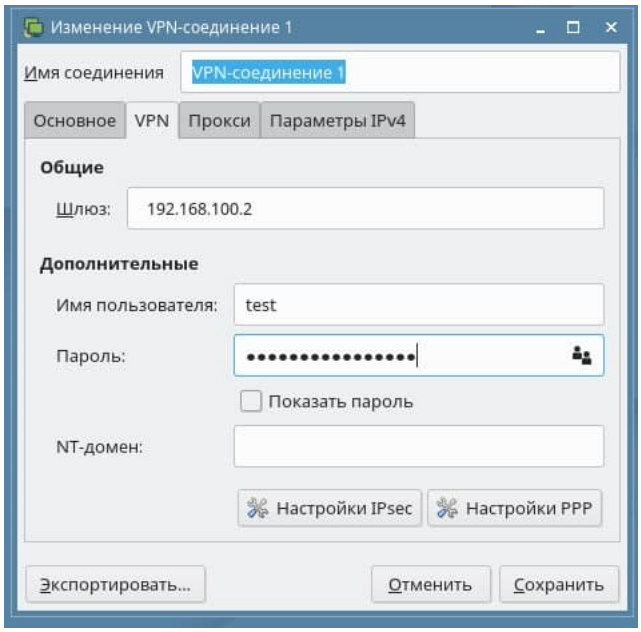
2. В трее (в настройках сети) выберите **Соединение VPN -> Добавить VPN-соединение**:



3. Выберите тип соединения **Layer 2 Tunneling Protocol (L2TP)** и нажмите **Создать**:



4. На вкладке **VPN** заполните поля:

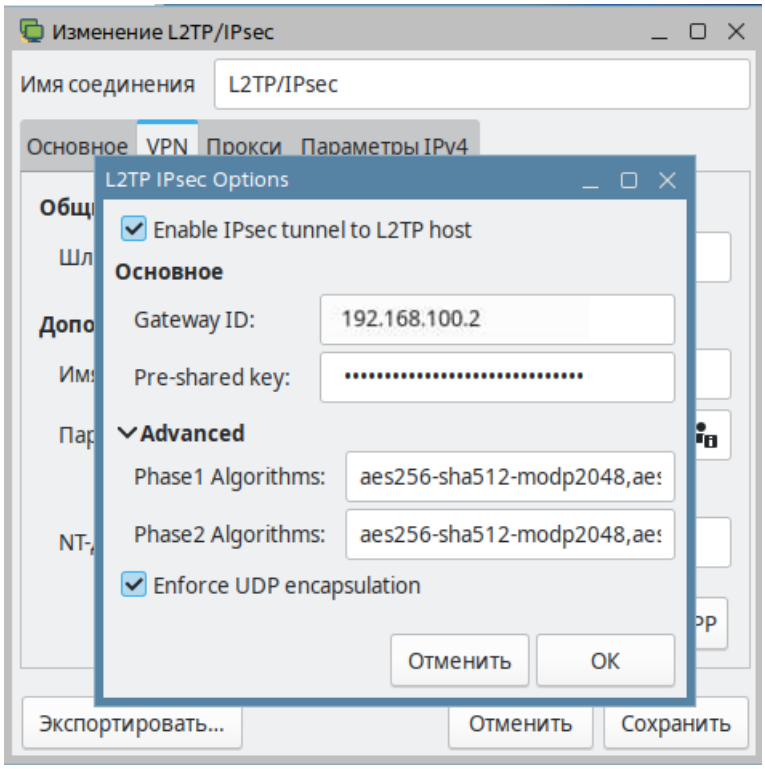


- **Шлюз** - IP-адрес внешнего интерфейса Ideco NGFW или домен;
- **Имя пользователя**;

- **Пароль**.

5. Нажмите **Настройки IPsec**.

6. Заполните поля:

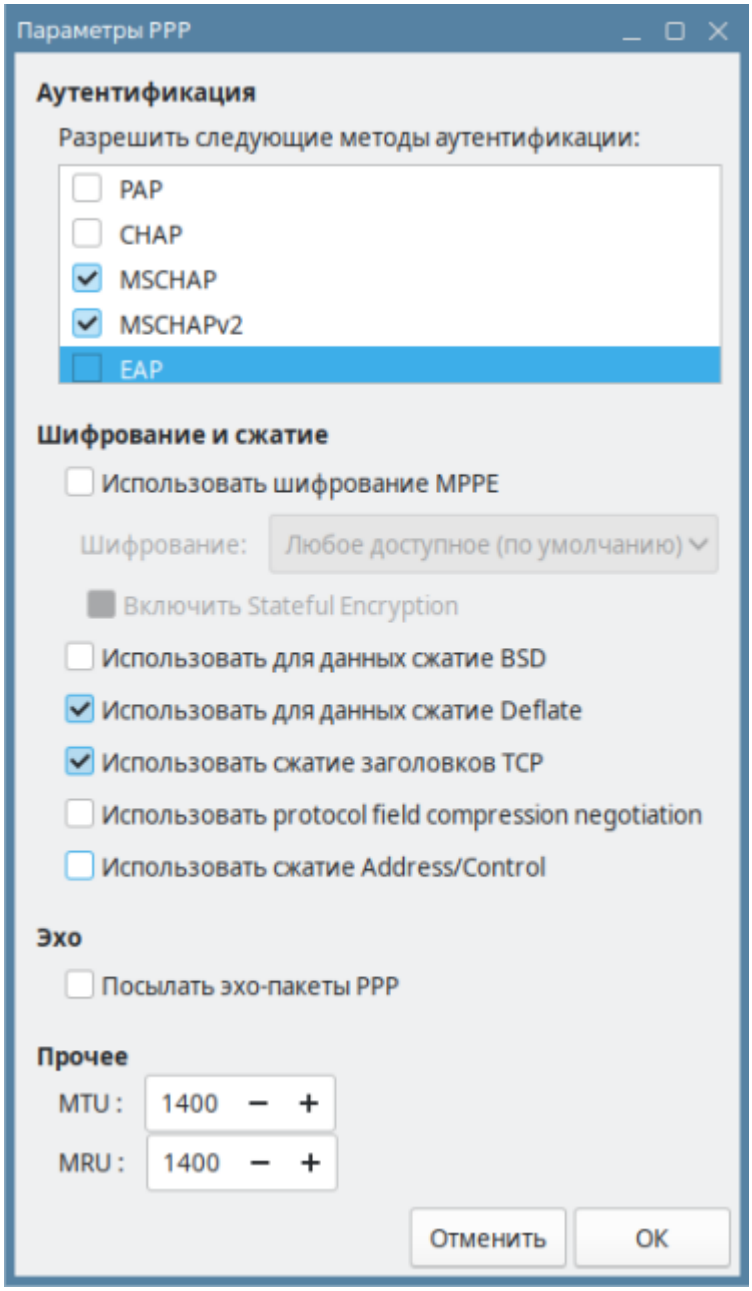


- **Gateway ID** - IP-адрес интерфейса, к которому осуществляется подключение;
- **Pre-shared key** - PSK-ключ из настроек Ideco NGFW (**Пользователи -> VPN-подключение -> Основное**);
- **Phase1 Algorithm** - `aes256-sha512-modp2048,aes256-sha512-modp1024,aes256-sha1-ecp256,aes256-sha1-modp2048,aes256-sha1-modp1024!`; *
- **Phase2 Algorithms** - `aes256-sha512-modp2048,aes256-sha256-modp2048,aes256-sha1-modp2048,aes128-sha1-modp2048,aes256-sha512-modp1024,aes256-sha256-modp1024,aes256-sha1-modp1024,aes128-sha1-modp1024,aes256-sha512,aes256-sha256,aes256-sha1,aes128-sha1!`.*

* Обязательно поставьте восклицательный знак в конце строки.

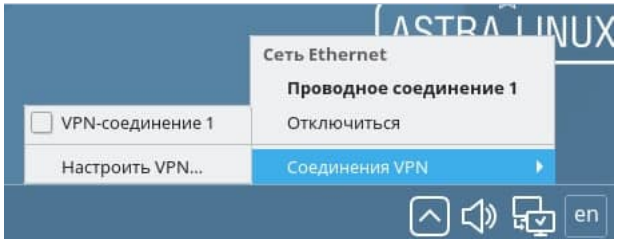
Так как Astra Linux по умолчанию запрашивает не самые защищенные алгоритмы, рекомендуем заполнить их самостоятельно.

7. При необходимости перейдите в Настройки PPP и настройте разделы **Аутентификация**, **Шифрование и сжатие**, **Прочее**:



8. Нажмите **ОК**, затем **Сохранить**.

Далее в трее (в настройках сети) **Соединение VPN** появится VPN-подключение. Для активации включите опцию **VPN-соединение**:



Подсказка: Проверить способы шифрования можно в конфигурации NGFW. Для этого включите в настройках VPN «Подключение по IKEv2/IPsec», откройте терминал NGFW и введите команду:
`cat /run/ideco-ipsec-backend/strongswan/swanctl/conf.d/rw_ikev2.conf`

- дляPhase1 Algorithm ищите значения “proposals=”;

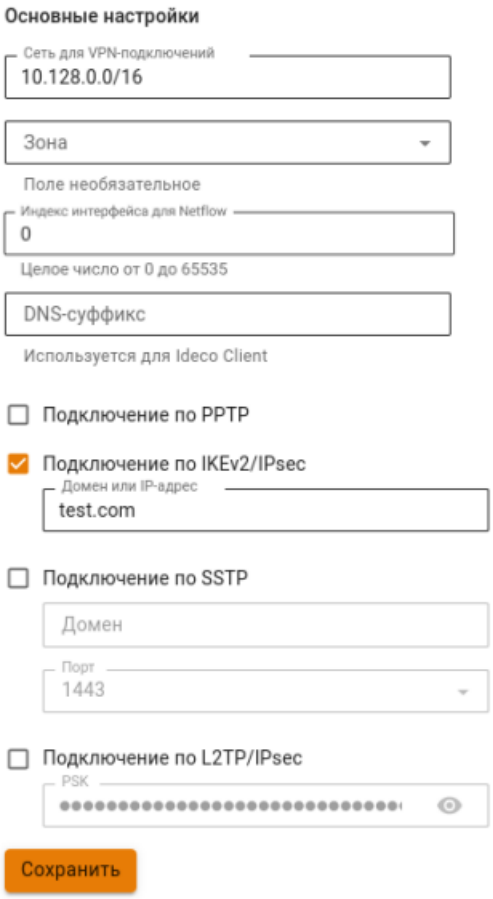
- для Phase2 Algorithms ищите значения “esp_proposals=”.

Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

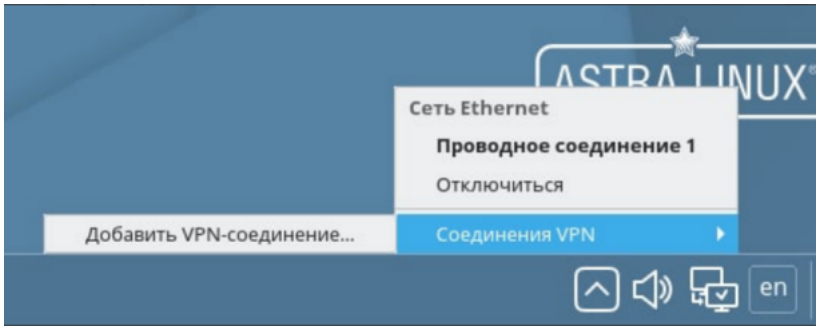
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в Astra Linux:

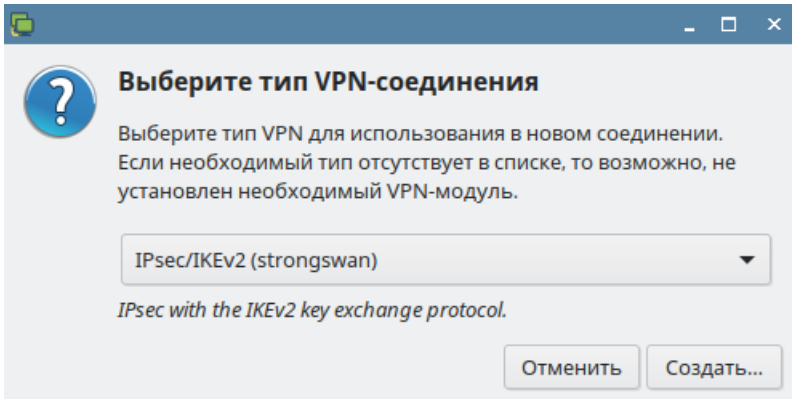
1. Откройте терминал сочетанием клавиш Ctrl+Alt+F1 или через путь **Пуск -> Системные -> Терминал Fly** и выполните три команды:

```
sudo apt install libcharon-extra-plugins
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-
↪extra-plugins
sudo reboot
```

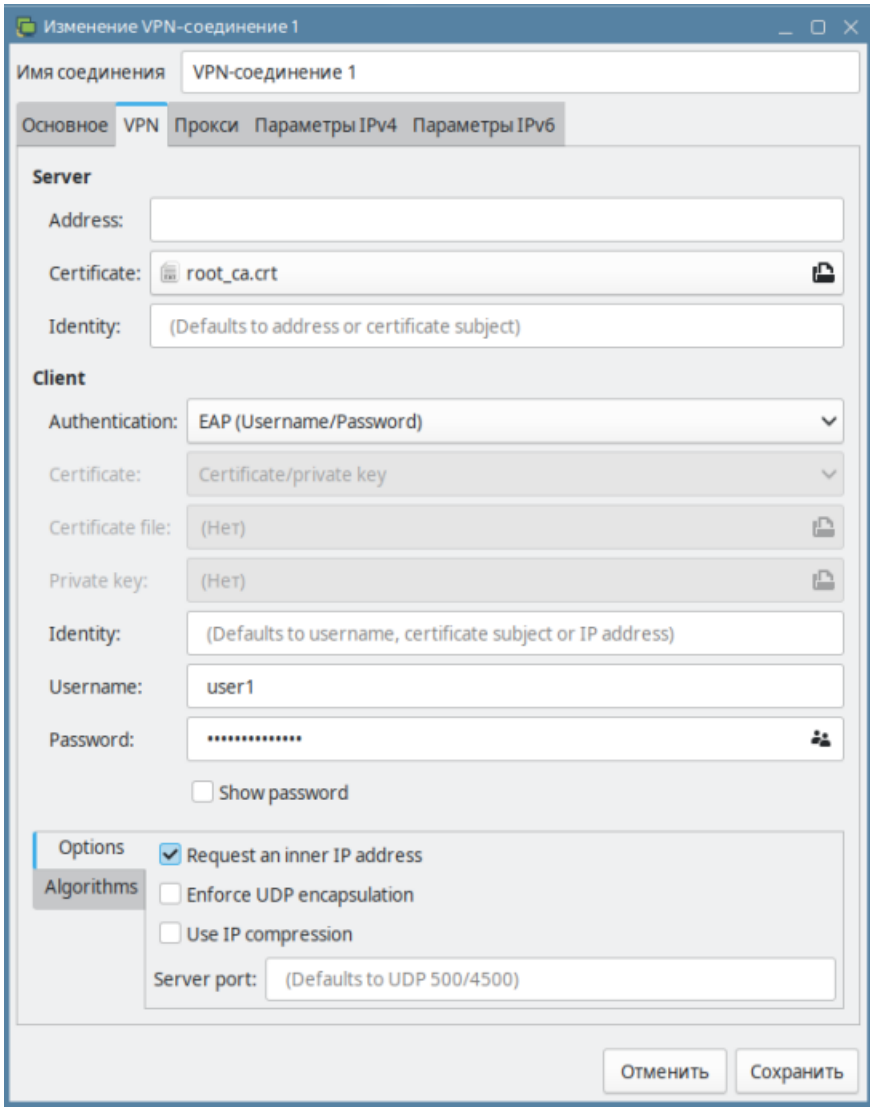
2. В трее (в настройках сети) выберите **Соединение VPN -> Добавить VPN-соединение**:



3. Выберите тип соединения **IPsec/IKEv2 (strongswan)** и нажмите **Создать**:



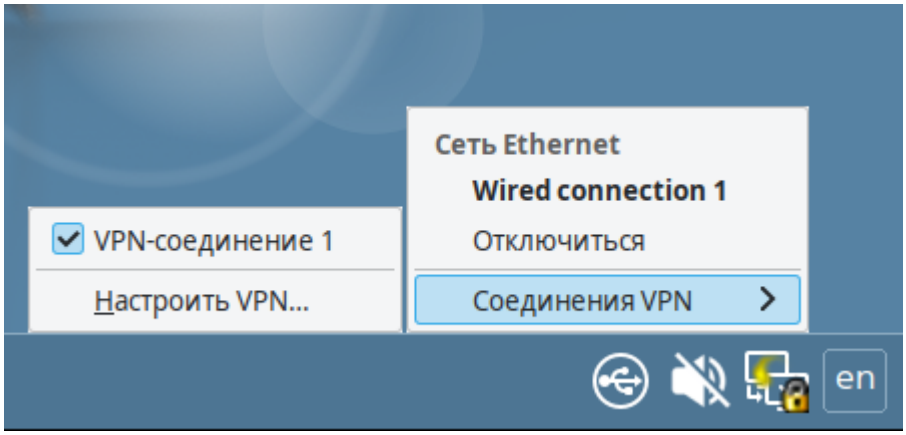
4. На вкладке **VPN** заполните следующие поля:



- **Имя соединения** - имя подключения;
- **Address** - введите домен, который указан в настройках **Пользователи -> VPN-подключения -> Основное -> Подключение по IKEv2/IPsec**;
- **Certificate** - выберите ранее сохраненный корневой сертификат (если он не был выдан Let`s Encrypt);
- **Authentication** - рекомендуем выбрать EAP (Username/Password);
- **Username** - имя пользователя, которому разрешено подключение по VPN;
- **Password** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения.

Установите флаг **Request an inner IP address** и нажмите **Добавить**.

5. В трее (в настройках сети) выберите **Соединение VPN** и установите флаг в строке с созданным соединением.



38.20.5 Создание подключения в Windows

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

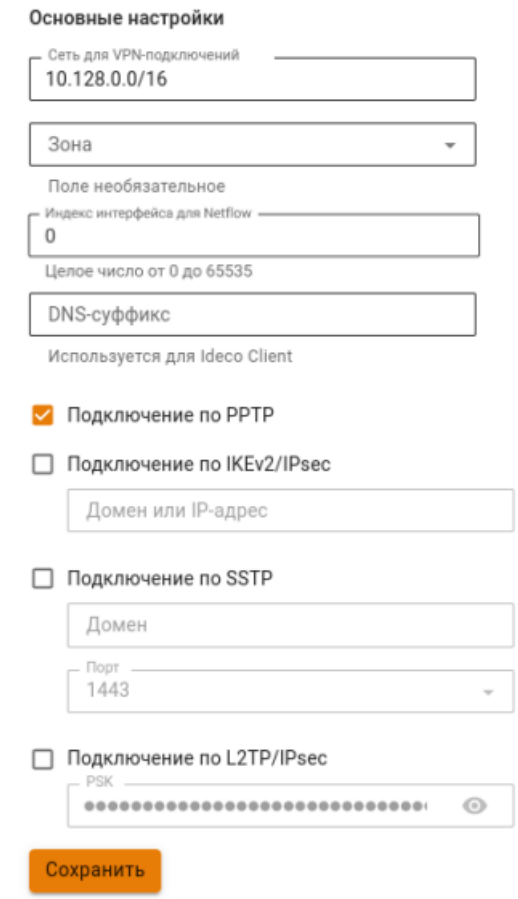
Создание VPN-подключения в Windows

Подсказка: Для корректной передачи маршрутов клиенту убедитесь, что опция **Использовать основной шлюз удаленной сети** выключена. Для отключения опции перейдите в **Панель управления -> Сеть и интернет -> Центр управления сетями и общим доступом -> Изменение параметров адаптера -> Свойства**. После этого перейдите на вкладку **Сеть -> IP версии 4 (TCP/IPv4) -> Дополнительно**.

Протокол PPTP:

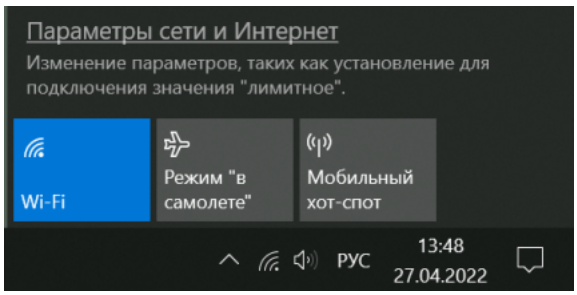
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное** и установите флаг **Подключение по PPTP**:

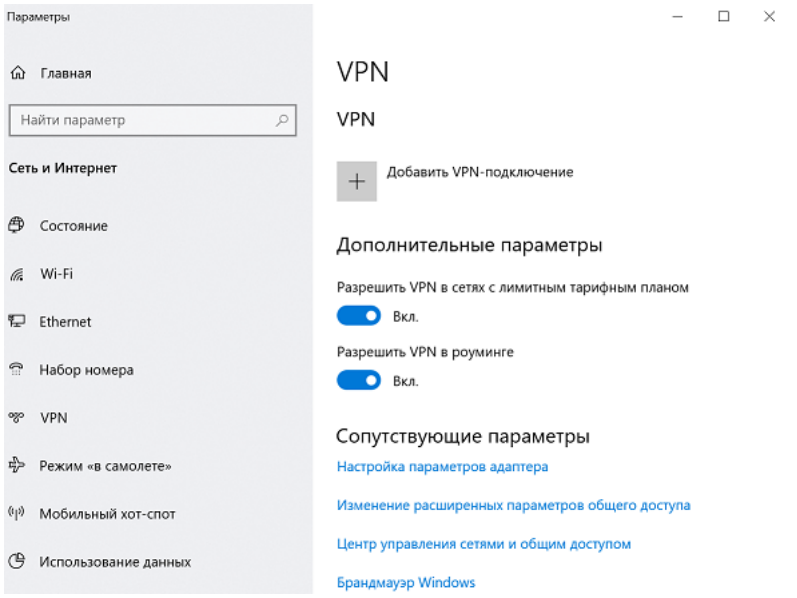


Создание подключения в Windows:

1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:

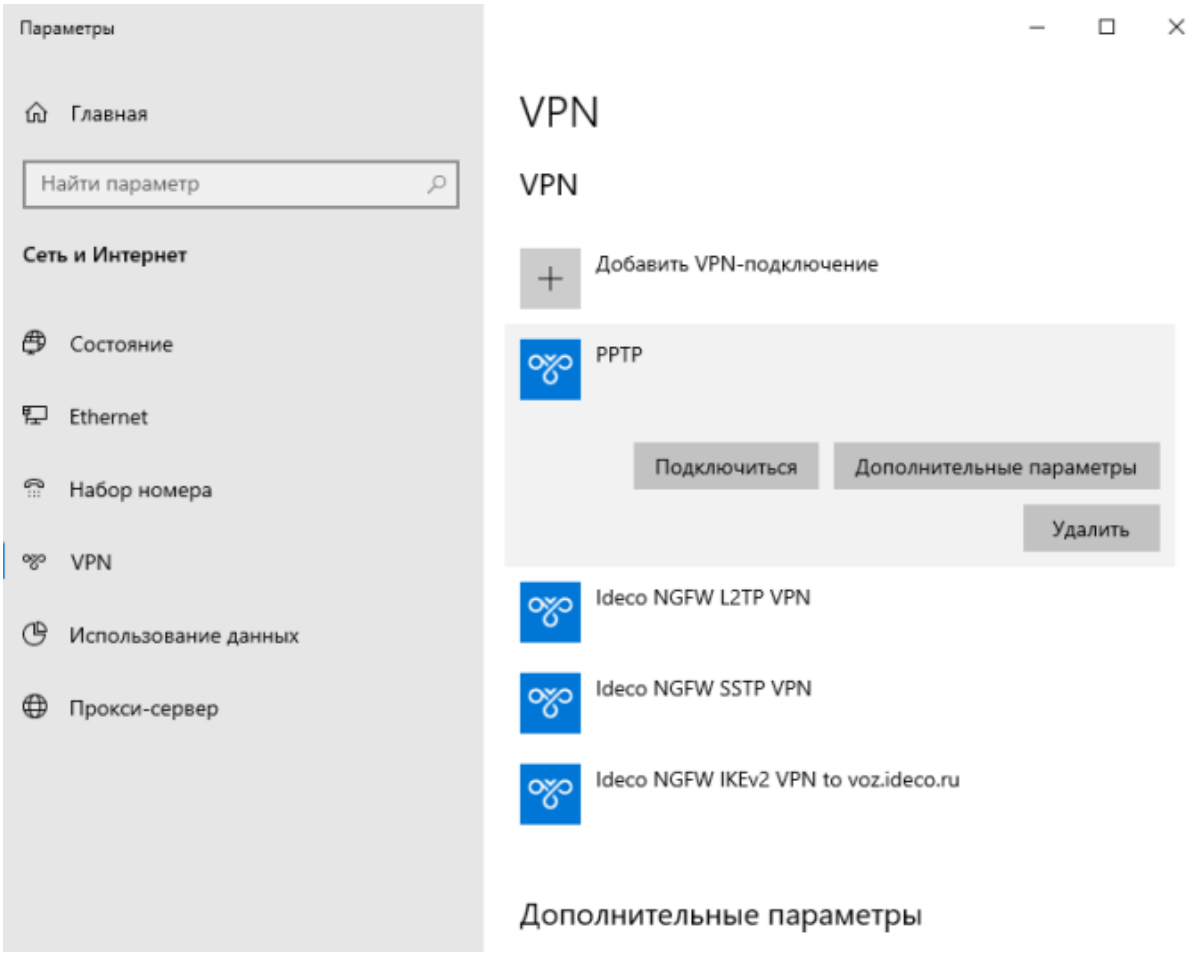
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол PPTP;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования);
- **Разрешить следующие протоколы** - протокол Microsoft CHAP версии 2 (MS-CHAP v2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры -> Изменить**.

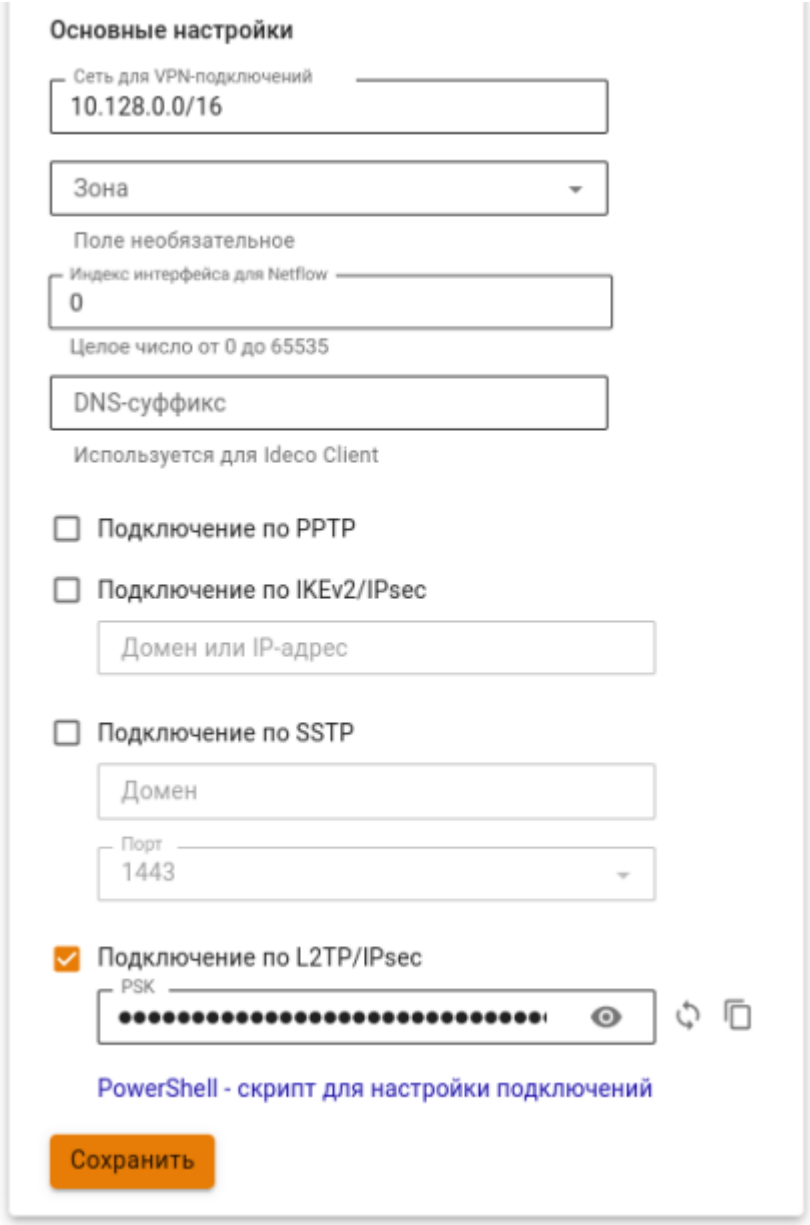
Протокол L2TP/IPsec с общим ключом:

Важно: L2TP IPsec клиенты, находящиеся за одним NAT, могут испытывать проблемы подключения, если их более одного. В решении проблемы поможет инструкция. Рекомендуем вместо L2TP IPsec использовать IKEv2 IPsec.

Настройка Ideco NGFW:

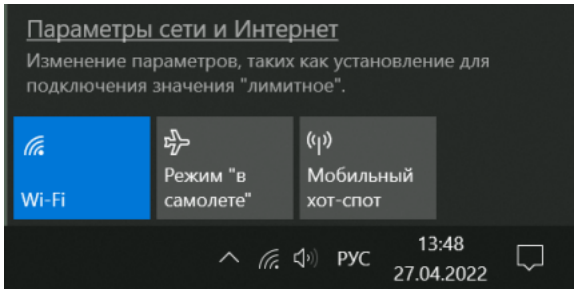
1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

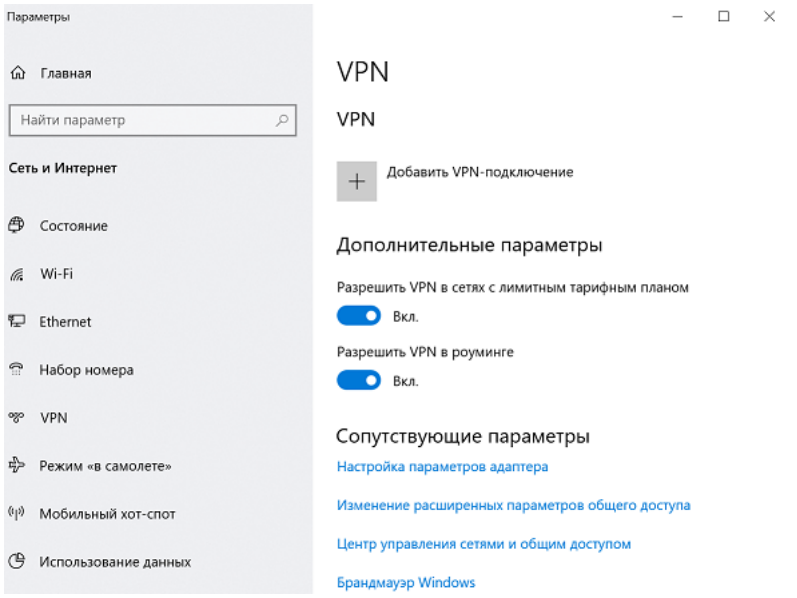


Создание подключения в Windows:

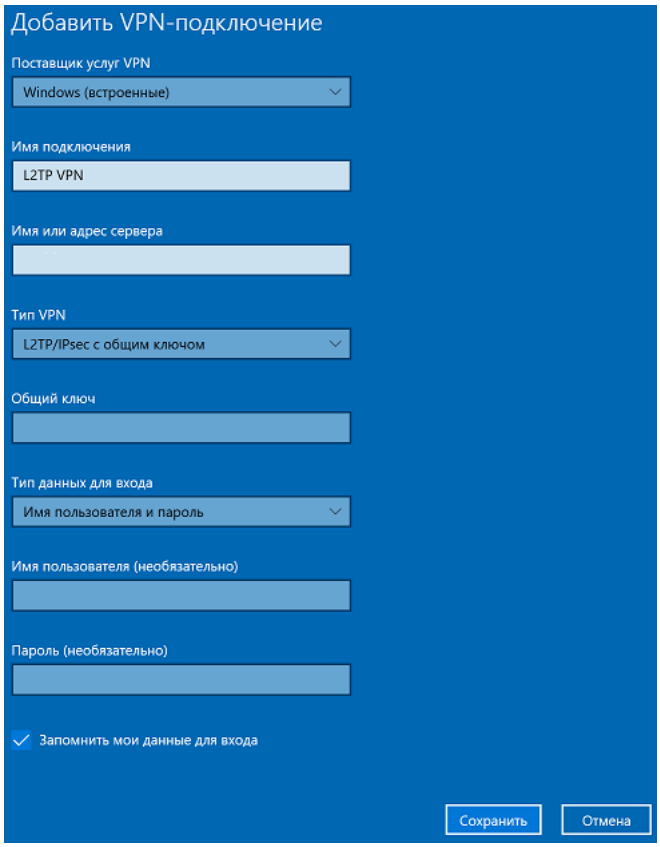
1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол L2TP/IPsec с общим ключом;
- **Общий ключ** - значение строки **PSK** в разделе **Пользователи -> VPN-подключения -> Основное -> Подключение по L2TP/IPsec**;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;

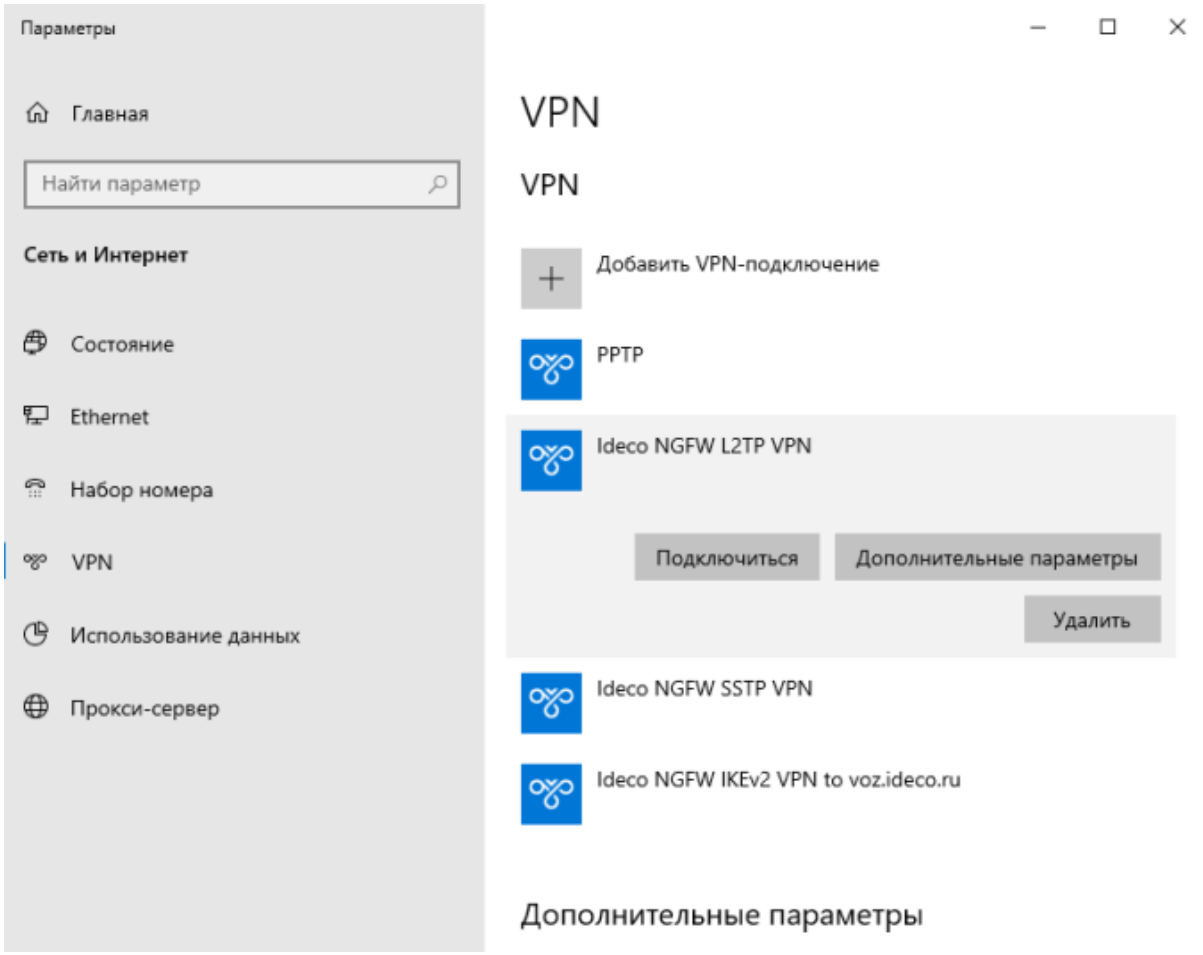
- **Пароль** - пароль пользователя.

4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования);
- **Разрешить следующие протоколы** - протокол Microsoft CHAP версии 2 (MS-CHAP v2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры -> Изменить**.

Если создается VPN-подключение к NGFW через проброс портов:

1. Откройте **Редактор реестра**.

2. Перейдите в `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent` и создайте DWORD-параметр с именем AssumeUDPEncapsulationContextOnSendRule и значением 2.

3. Перезагрузите Windows.

Возможные неполадки

1. Неправильно указан логин или пароль пользователя. Часто при повторном соединении предлагается указать домен. Старайтесь создавать для учетных записей цифро-буквенные пароли, желательно на латинице. Если есть сомнения в этом пункте, то временно установите логин и пароль пользователю `user` и `123456`.

2. Чтобы пакеты пошли через VPN-туннель, надо убедиться, что в настройках этого подключения стоит чекбокс **Использовать основной шлюз в удаленной сети** в разделе **Настройка параметров адаптера ->**

Правой кнопкой мыши по подключению -> Свойства -> Сеть -> Свойства опции «Протокол интернета версии 4 (TCP/IPv4)» -> Дополнительно. Если же маршрутизировать все пакеты в этот интерфейс не обязательно, то маршрут надо прописать вручную.

3. Подключение происходит через DNAT, т.е. внешний интерфейс Ideco NGFW не имеет «белого» IP-адреса, а необходимые для работы порты (500 и 4500) «проброшены» на внешний интерфейс устройства, расположенного перед Ideco NGFW и имеющего «белый» IP-адрес. В данном случае VPN-подключение либо вообще не будет устанавливаться, либо будут периодические обрывы. Решение - исключить устройство перед Ideco NGFW и указать на внешнем интерфейсе Ideco NGFW «белый» IP-адрес, к которому в итоге и будут осуществляться L2TP/IPsec-подключения. Либо используйте протокол SSTP - его проще опубликовать с помощью проброса портов.

4. Если в ОС Windows 10 повторно подключиться по L2TP, но при этом использовать **невалидный** ключ PSK (введя его в дополнительных параметрах), подключение все равно будет установлено успешно. Это связано с особенностями работы ОС.

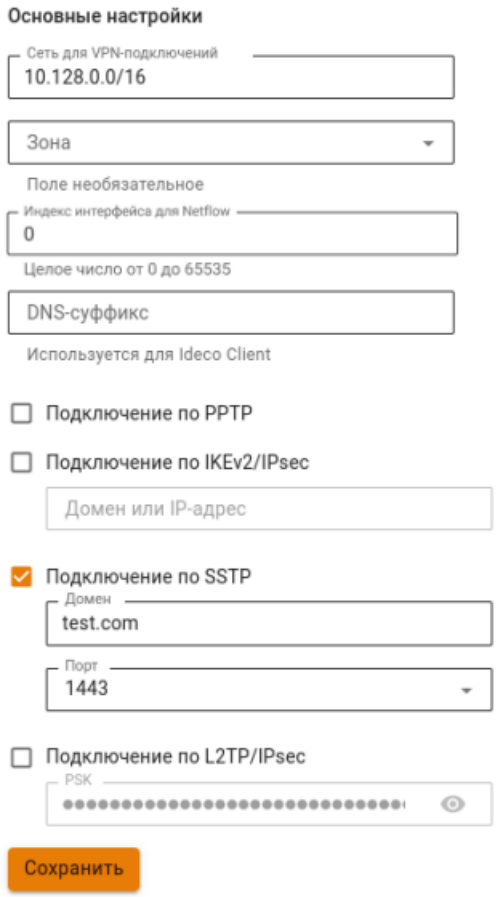
Убедитесь, что локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. Если пересекается, то доступа к сети организации не будет (трафик по таблице маршрутизации пойдет в физический интерфейс, а не в VPN). Адресацию необходимо менять.

Протокол SSTP:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



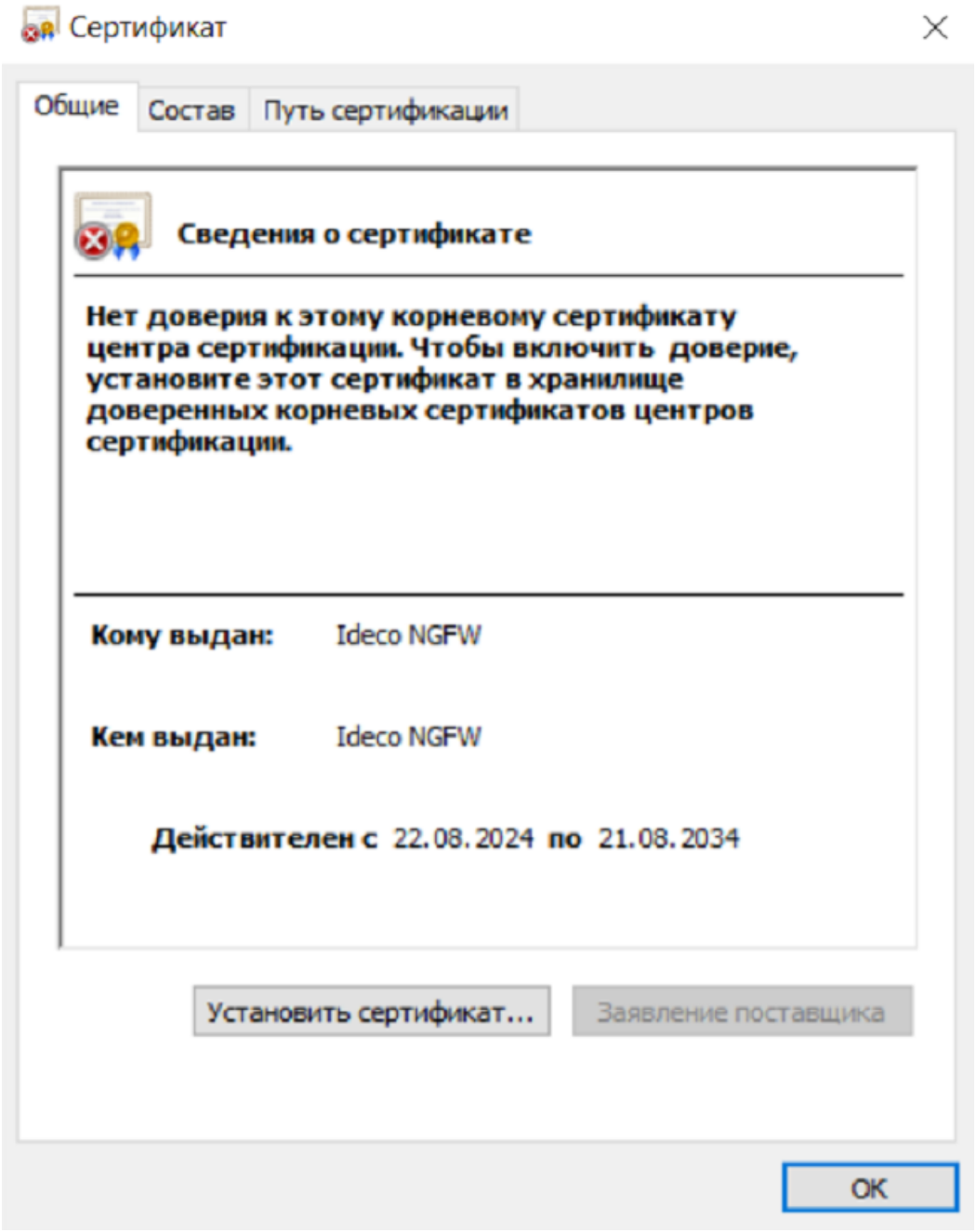
3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был

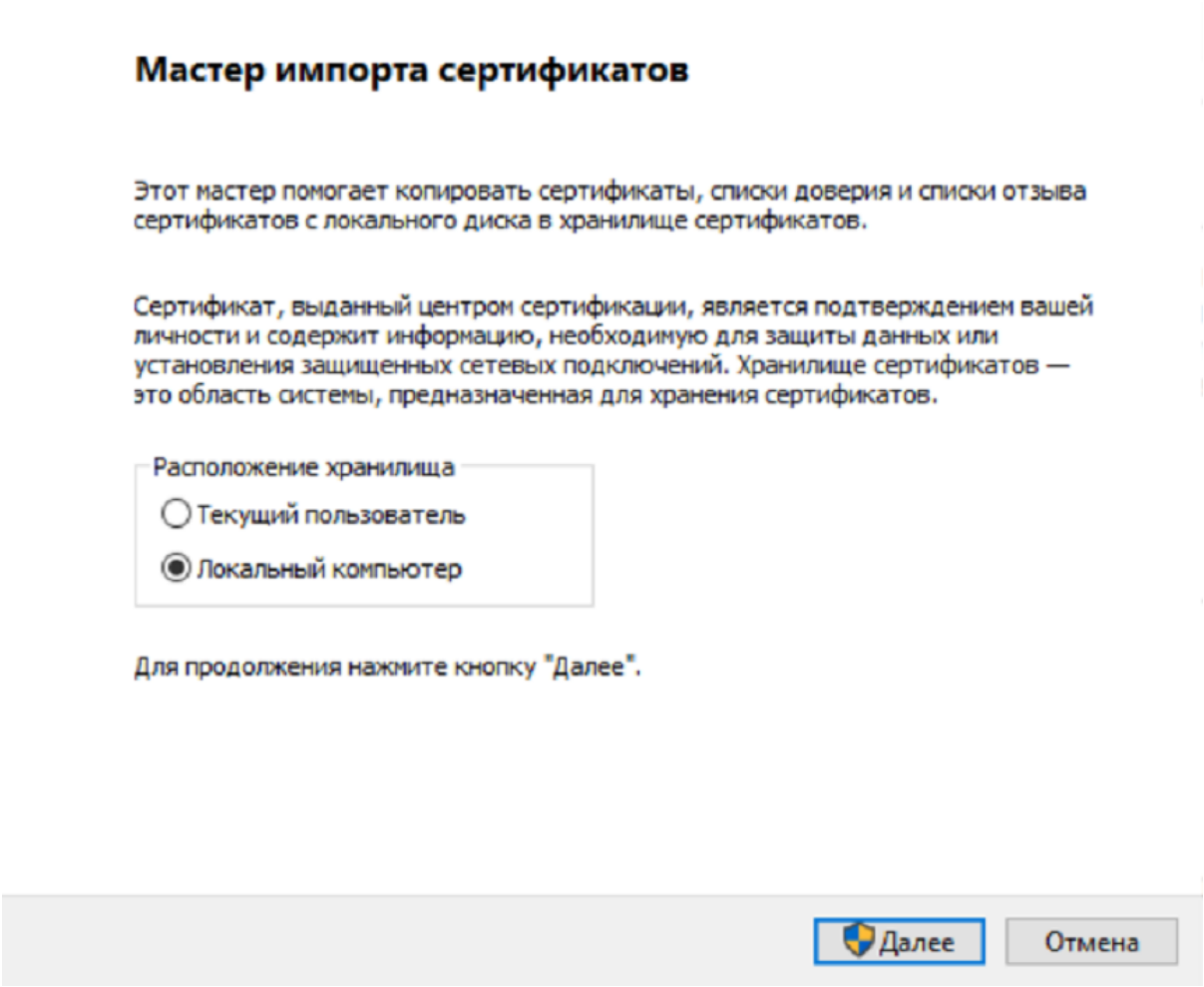
получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

4. Импортируйте сертификат Ideco NGFW в Windows. Для этого выполните действия:

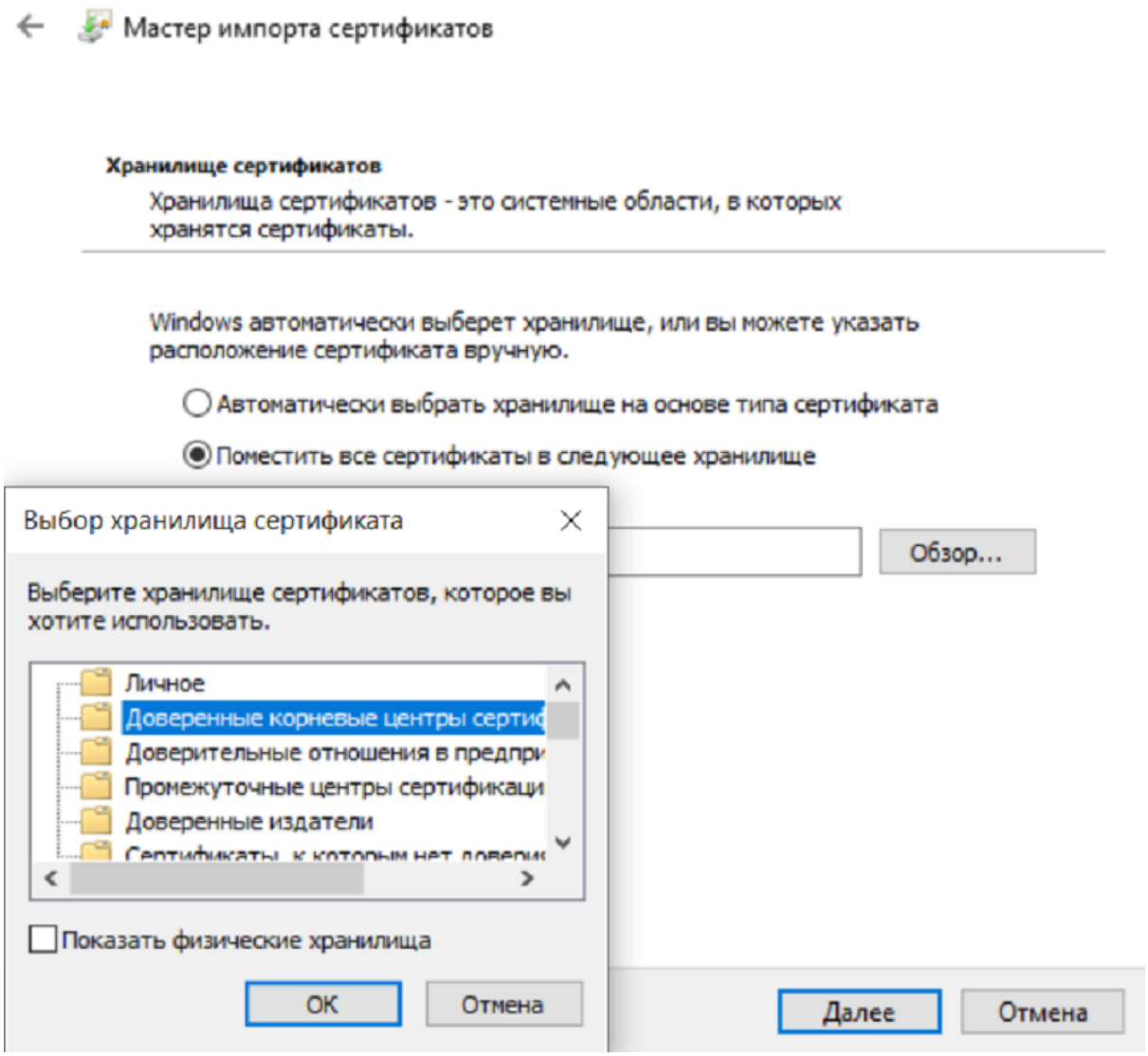
- Откройте скачанный сертификат и нажмите **Установить сертификат**:



- Для корректной настройки выберите расположение хранилища **Локальный компьютер**:

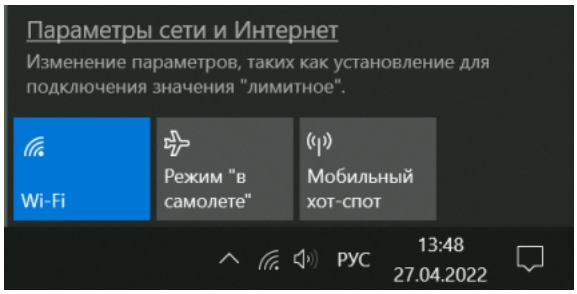


- Установите сертификат в **Доверенные корневые центры сертификации**:

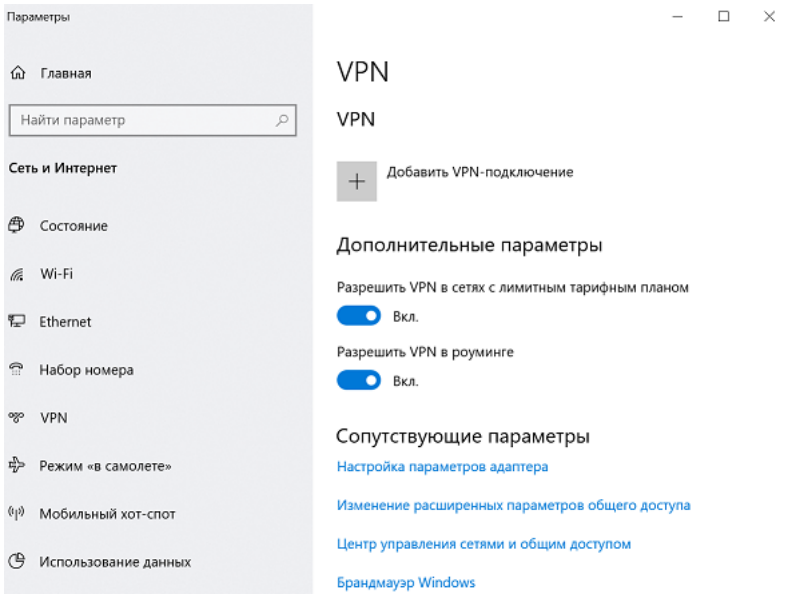


Создание подключения в Windows:

1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:

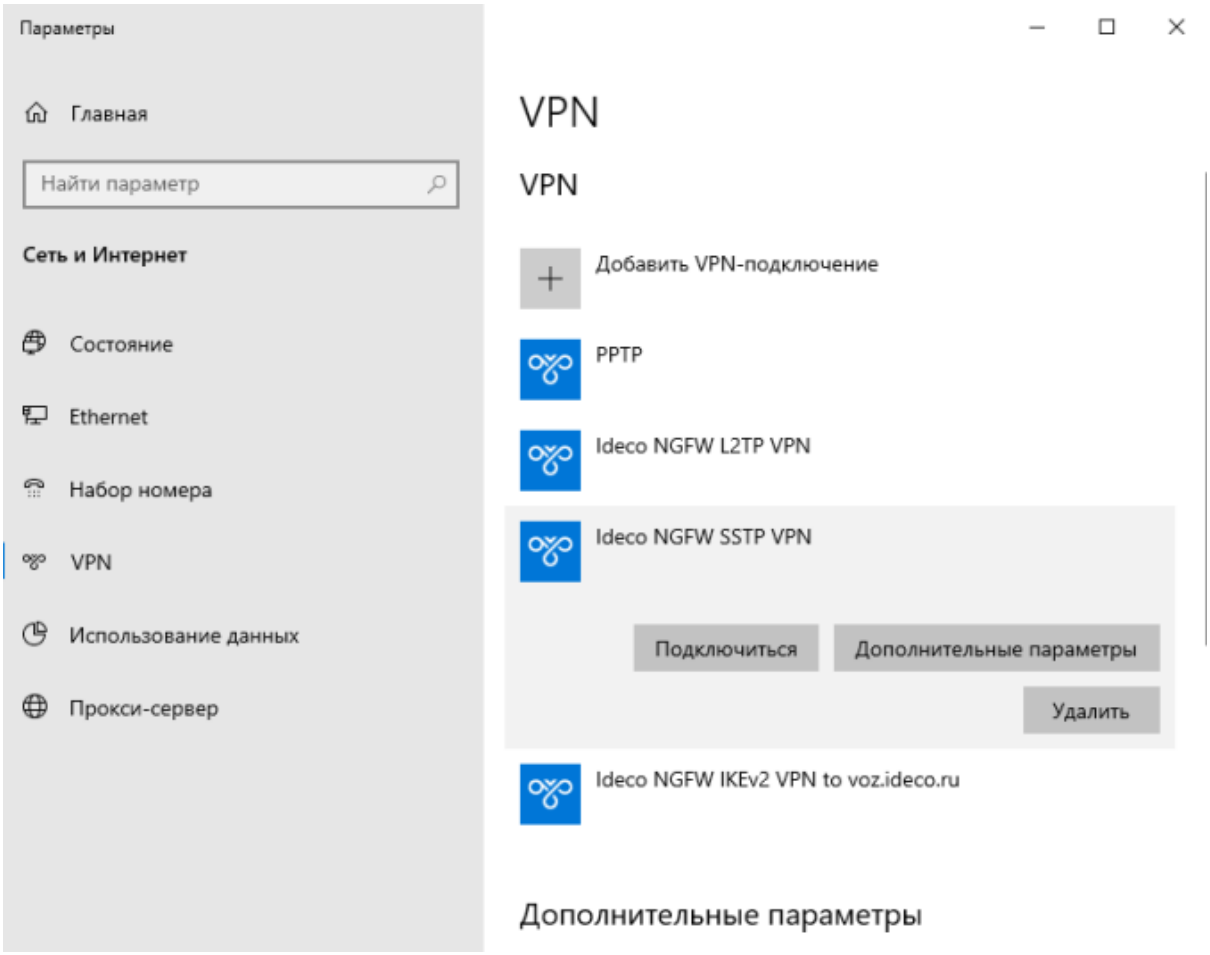
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера в формате *адрес_VPN_сервера:порт*;
- **Тип VPN** - протокол SSTP;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования);
- **Разрешить следующие протоколы** - протокол Microsoft CHAP версии 2 (MS-CHAP v2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



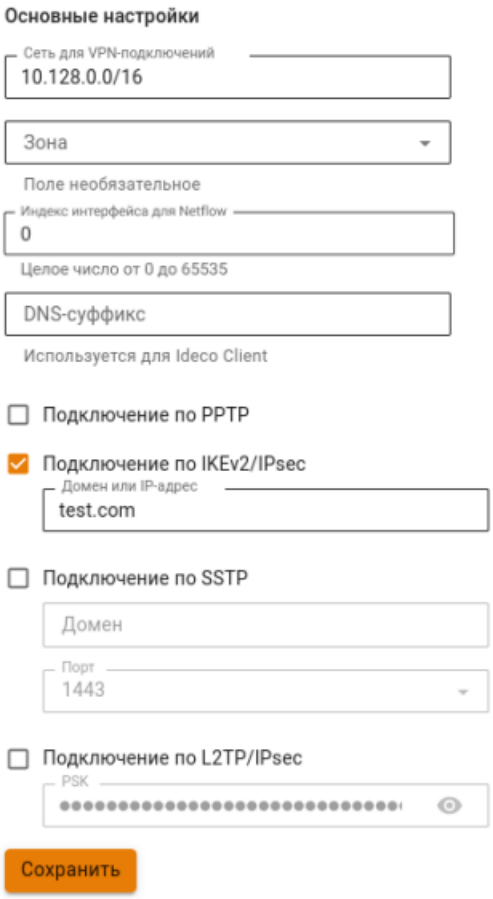
7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры -> Изменить**.

Протокол IKEv2:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:

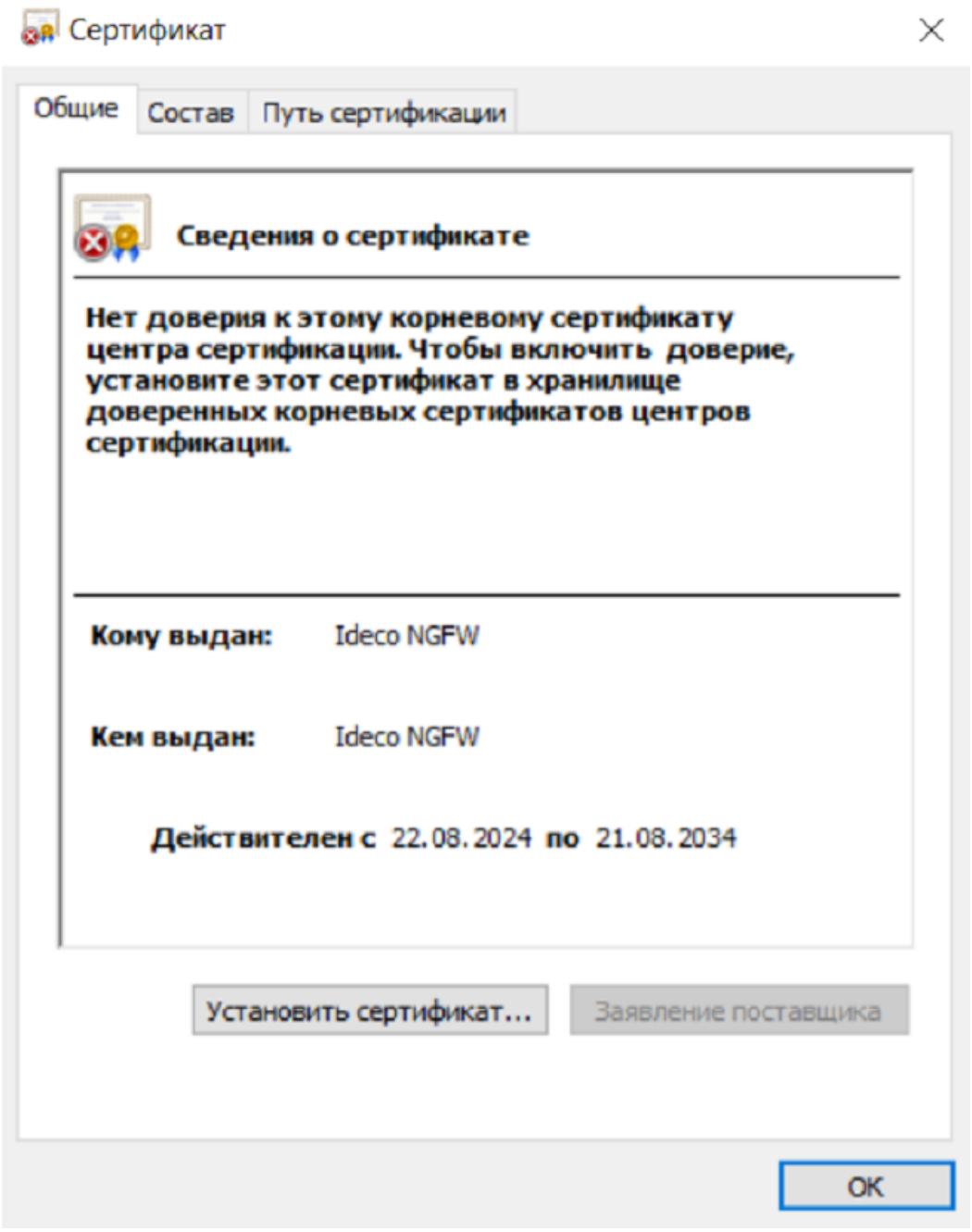


3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

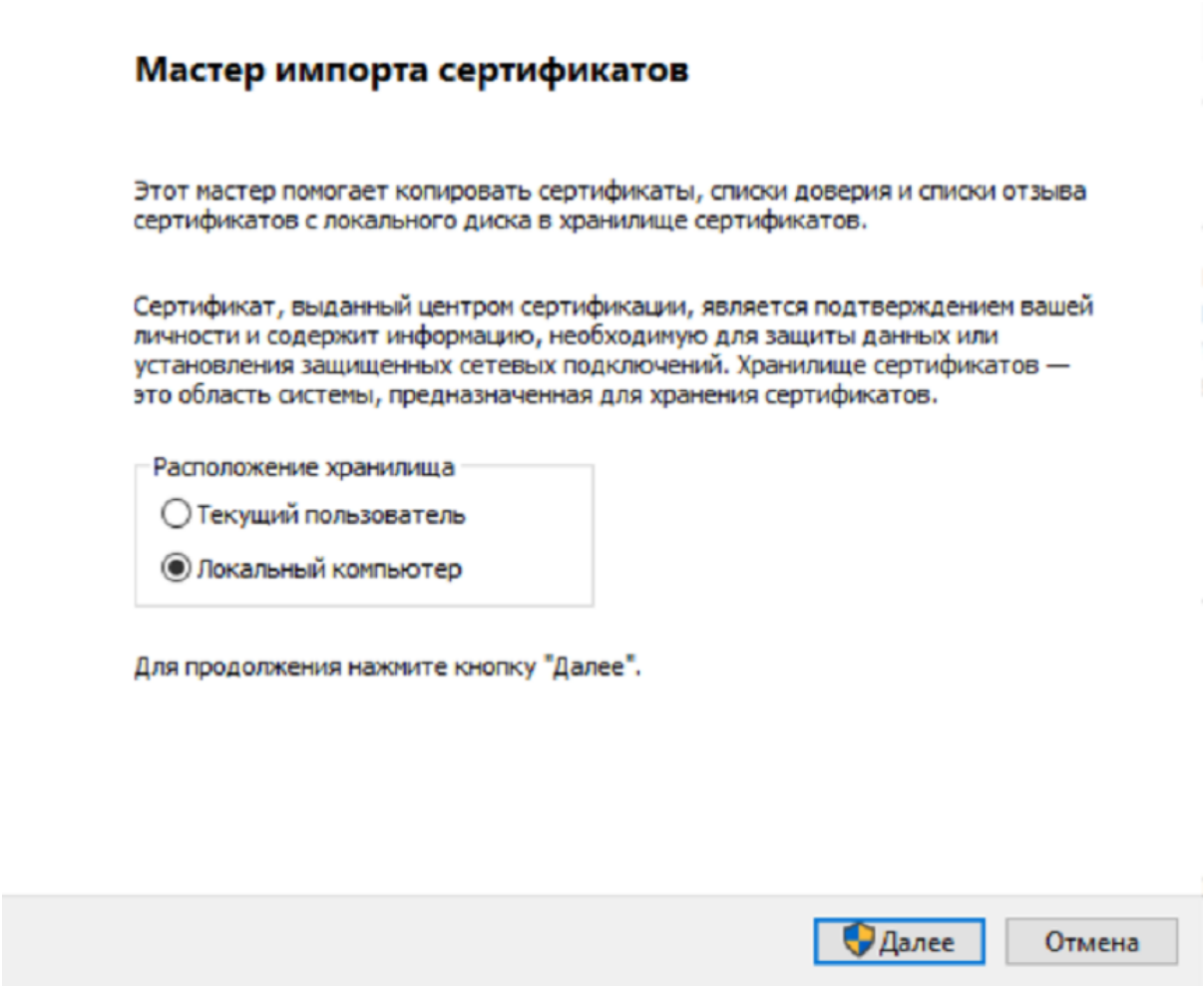
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

4. Импортируйте сертификат Ideco NGFW в Windows. Для этого выполните действия:

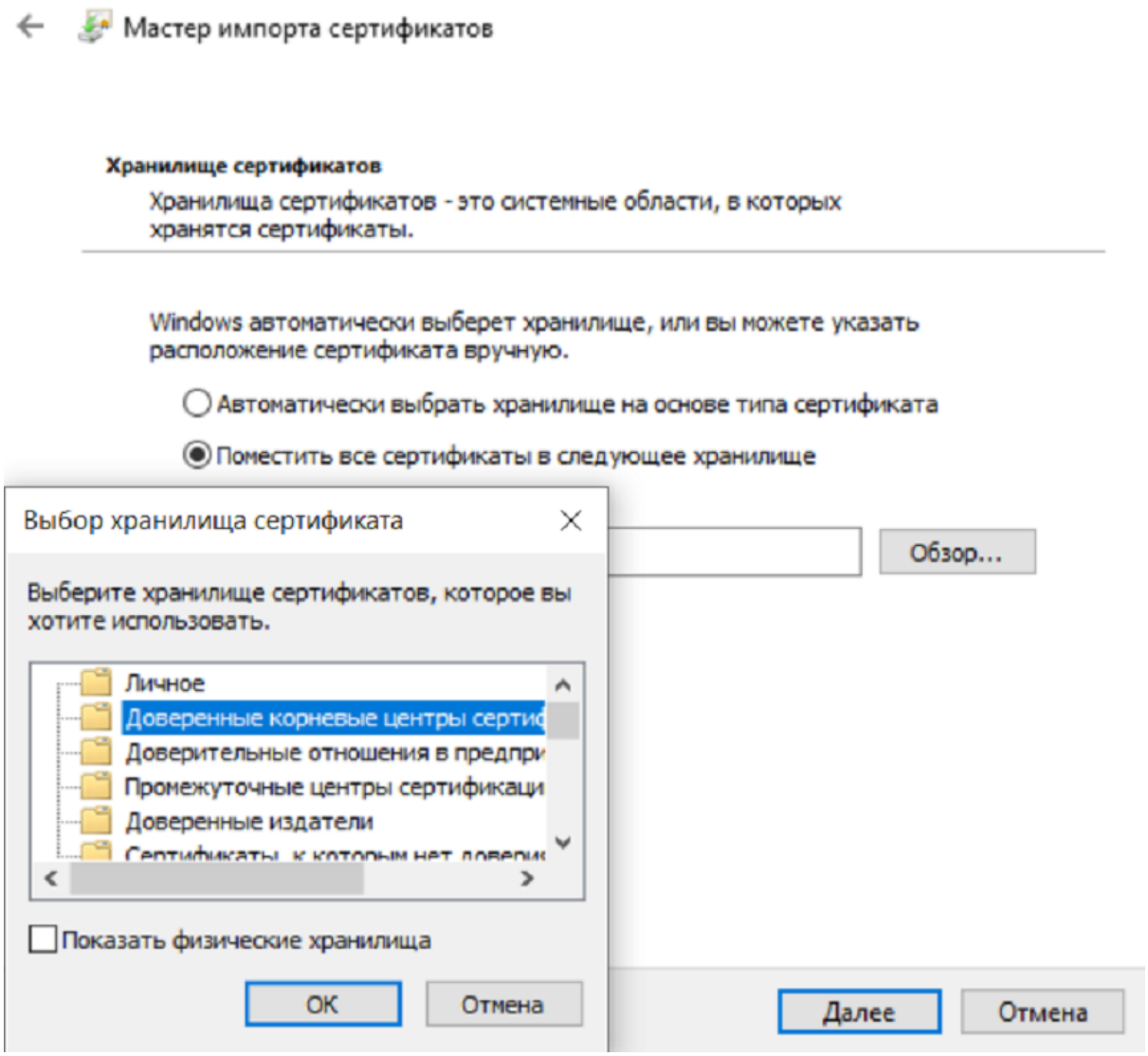
- Откройте скачанный сертификат и нажмите **Установить сертификат**:



- Для корректной настройки выберите расположение хранилища **Локальный компьютер**:

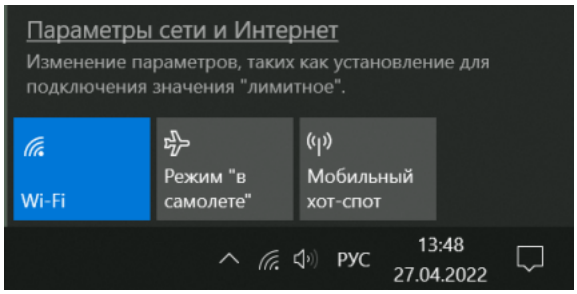


- Установите сертификат в **Доверенные корневые центры сертификации**:

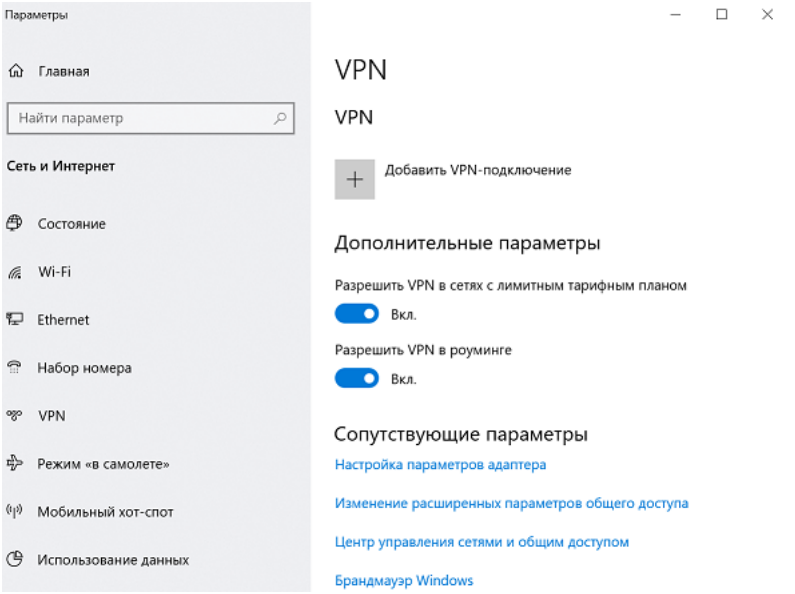


Создание подключения в Windows:

1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:

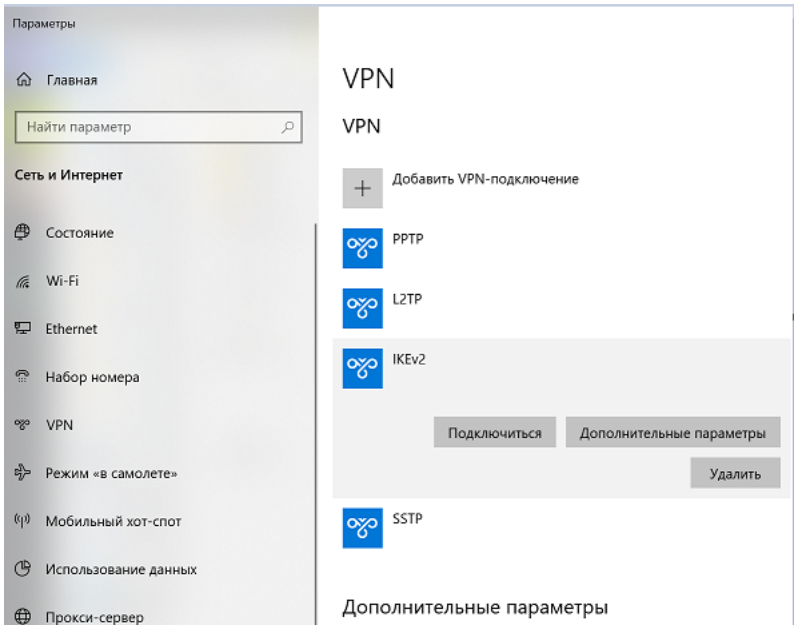
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол IKEv2;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

4. Перейдите в **Настройки параметров адаптера**, нажмите на созданное подключение правой кнопкой мыши и выберите **Свойства**.

5. Перейдите на вкладку **Безопасность** и установите:

- **Шифрование данных** - обязательное (отключиться, если нет шифрования);
- **Протокол расширенной проверки подлинности (EAP)** - Microsoft защищенный пароль (EAP MSCHAPV2).

6. Активируйте подключение, нажав правой кнопкой мыши по созданному подключению и выбрав **Подключиться**:



7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры -> Изменить**.

Ошибки работы VPN-подключений

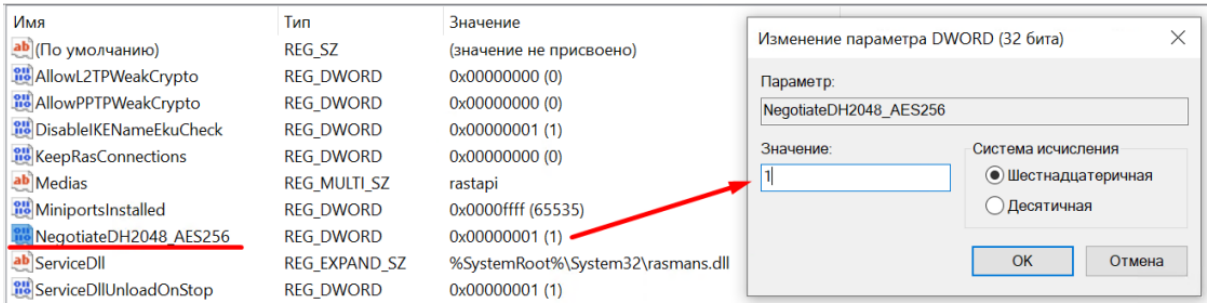
Если при подключении по IKEv2 возникает «Ошибка сопоставления групповой политики» или ошибка с кодом «13868»:

Если VPN-подключение по протоколам IPSec в Windows автоматически разрывается через 7 часов 45 минут, для восстановления связи подойдут следующие действия:

1. Переподключите соединение. Оно восстановится, но через 7 часов 45 минут вновь будет автоматически разорвано. Если требуется, чтобы подключение не разрывалось автоматически, то выполните действия из следующего пункта.

2. Внесите изменения в реестр:

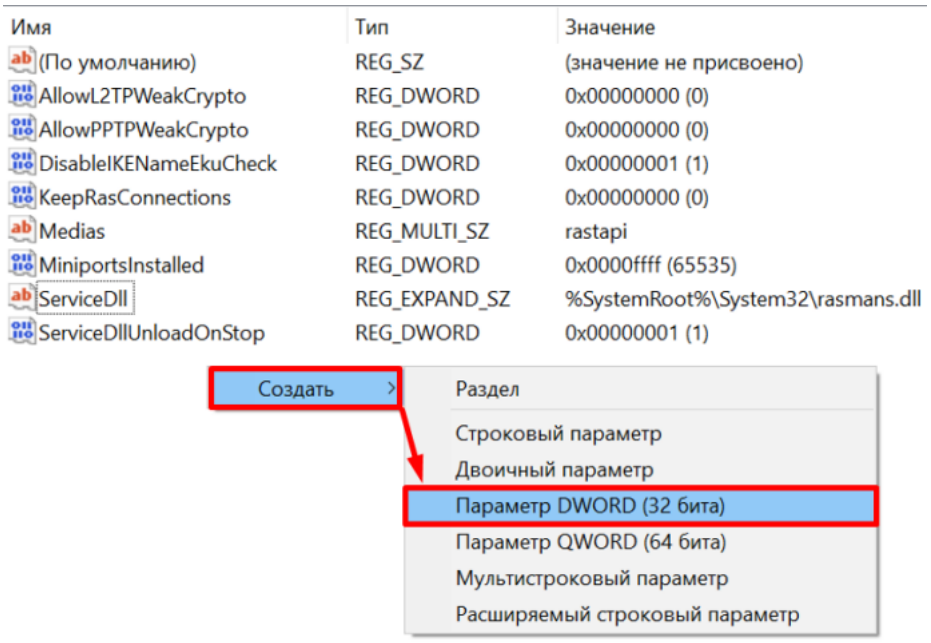
- Откройте **Редактор реестра**;
- Перейдите по пути `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters`;
- Нажмите правой кнопкой мыши по параметру с именем **NegotiateDH2048_AES256** и нажмите **Изменить**;
- В строке **Значение** укажите значение `1`:



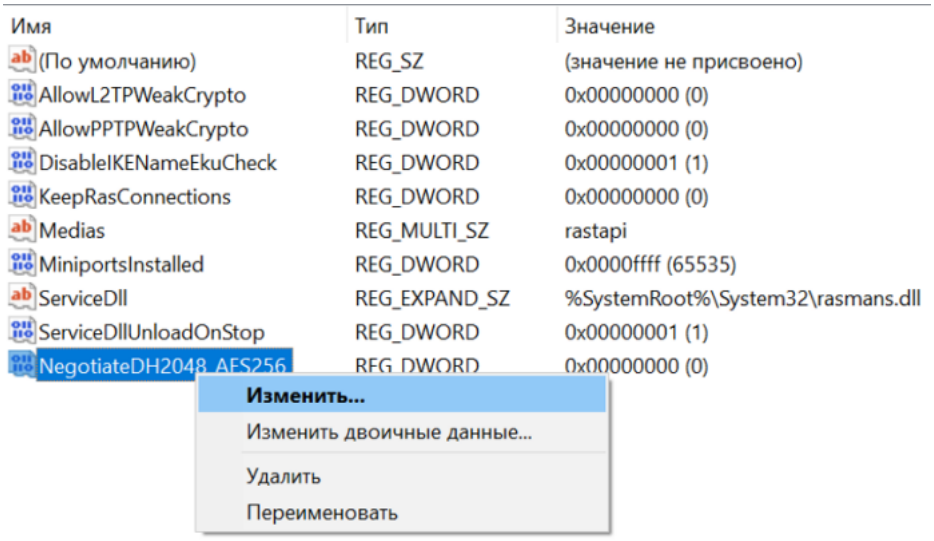
- Нажмите **OK**;
- Перезагрузите Windows.

  Если параметра с именем **NegotiateDH2048_AES256** нет, то создайте его. Для этого:

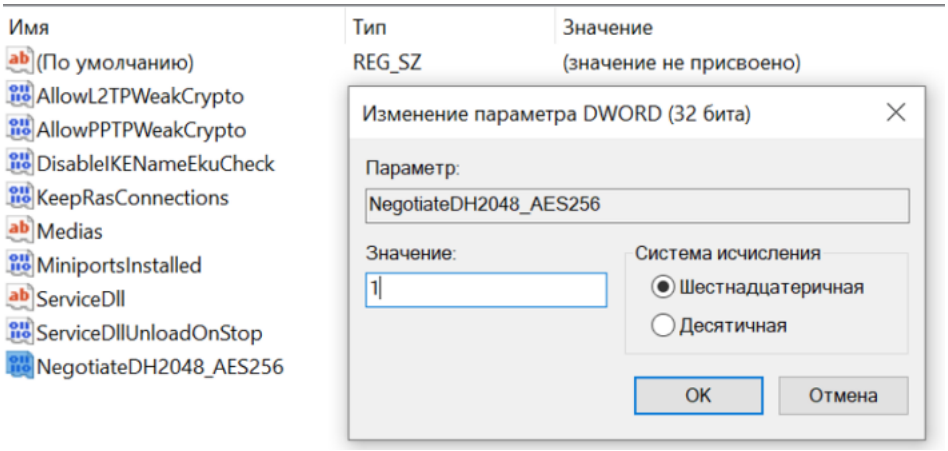
- Нажмите правой кнопкой мыши по свободному месту реестра в **Parameters** и выберите **Создать -> DWORD**:



- Задайте имя **NegotiateDH2048_AES256**;
- Нажмите правой кнопкой мыши по созданному файлу и выберите **Изменить**:



- В строке **Значение** укажите значение 1:



- Нажмите **OK**.

3. Перезагрузите Windows.

Подсказка: В Ideco NGFW также есть возможность загрузить с сервера готовые скрипты для создания VPN-подключения в ОС Windows версий 8.1 и 10. Для загрузки и запуска скриптов воспользуйтесь *инструкцией*.

38.20.6 Создание VPN-подключения на мобильных устройствах

Основное

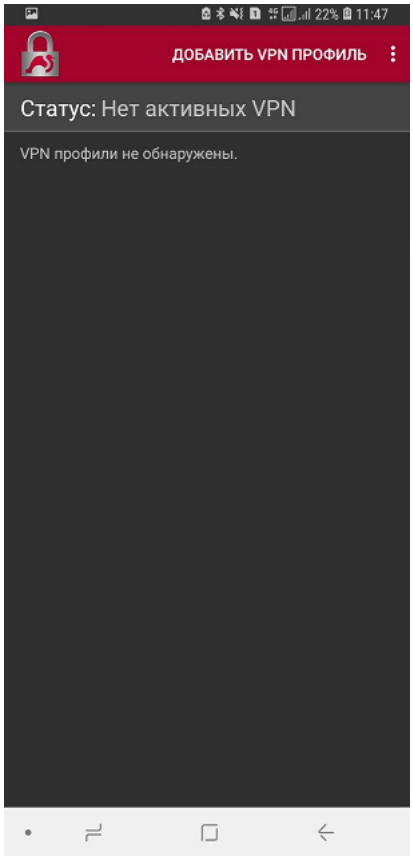
Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Также установите корневой сертификат NGFW на устройство пользователя. Скачать сертификат можно в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

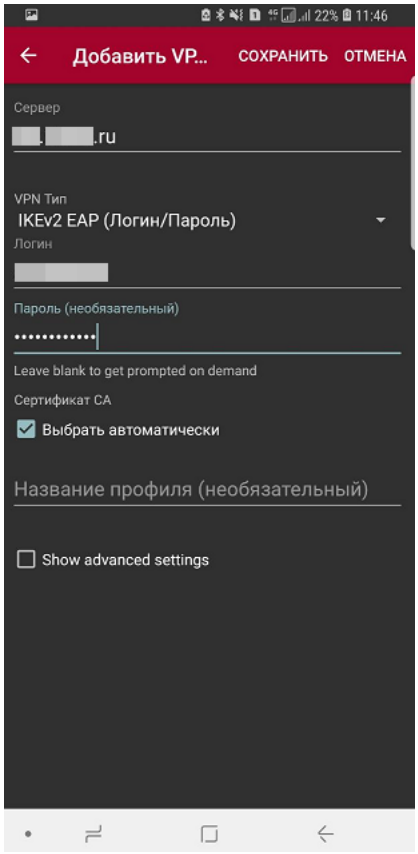
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Подключение через приложение StrongSwan:

1. Нажмите **Добавить VPN профиль**:



2. Заполните поля:



- **Сервер** - домен, указанный в Ideco NGFW в разделе **Пользователи -> VPN-подключения -> Основное -> Подключение по IKEv2/IPsec**;

- **VPN тип** - IKEv2 EAP (Логин/Пароль);
- **Логин** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

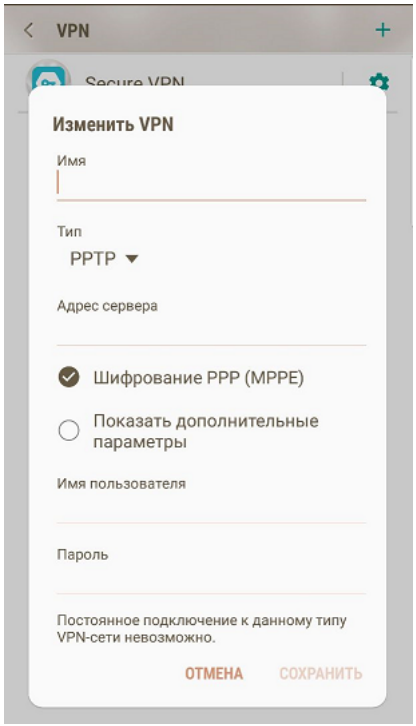
3. Нажмите **Сохранить** и кликните по созданному подключению:

Подключение на Android:

1. Перейдите в **VPN** в раздел **Настройки -> Подключения -> Другие настройки**. При необходимости воспользуйтесь строкой поиска по настройкам.

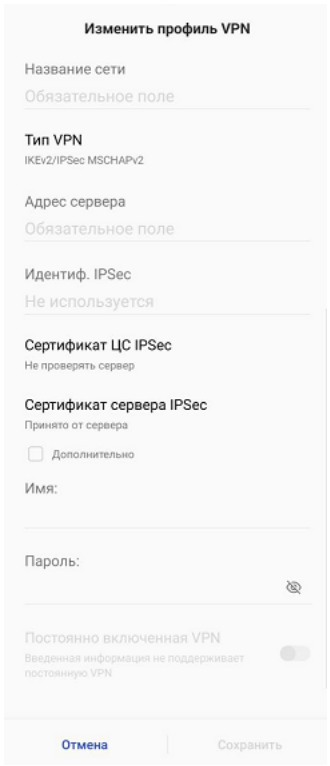
2. Выберите тип подключения и заполните следующие поля:

Для PPTP:



- **Имя** - имя подключения;
- **Адрес сервера** - адрес VPN-сервера;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

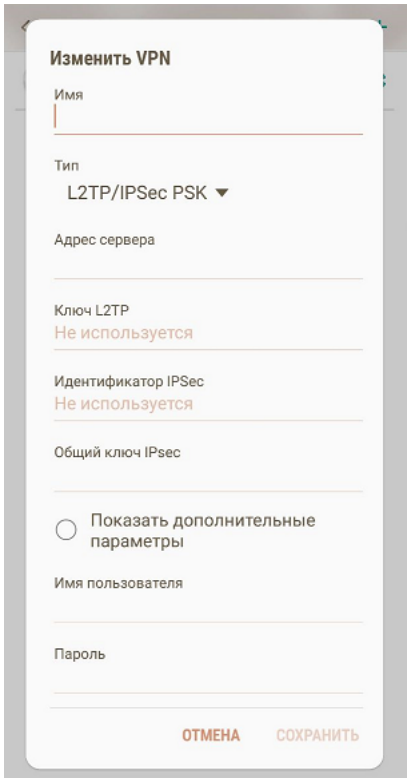
Для IKEv2/IPsec MSCHAPv2:



- **Имя** - имя подключения;
- **Адрес сервера** - адрес VPN-сервера;

- **Идентификатор IPsec** - логин пользователя;
- **Сертификат сервера** - «Принято от сервера»;
- **Сертификат ЦС IPsec** - «Не проверять сервер»;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

Для L2TP/IPsec PSK:

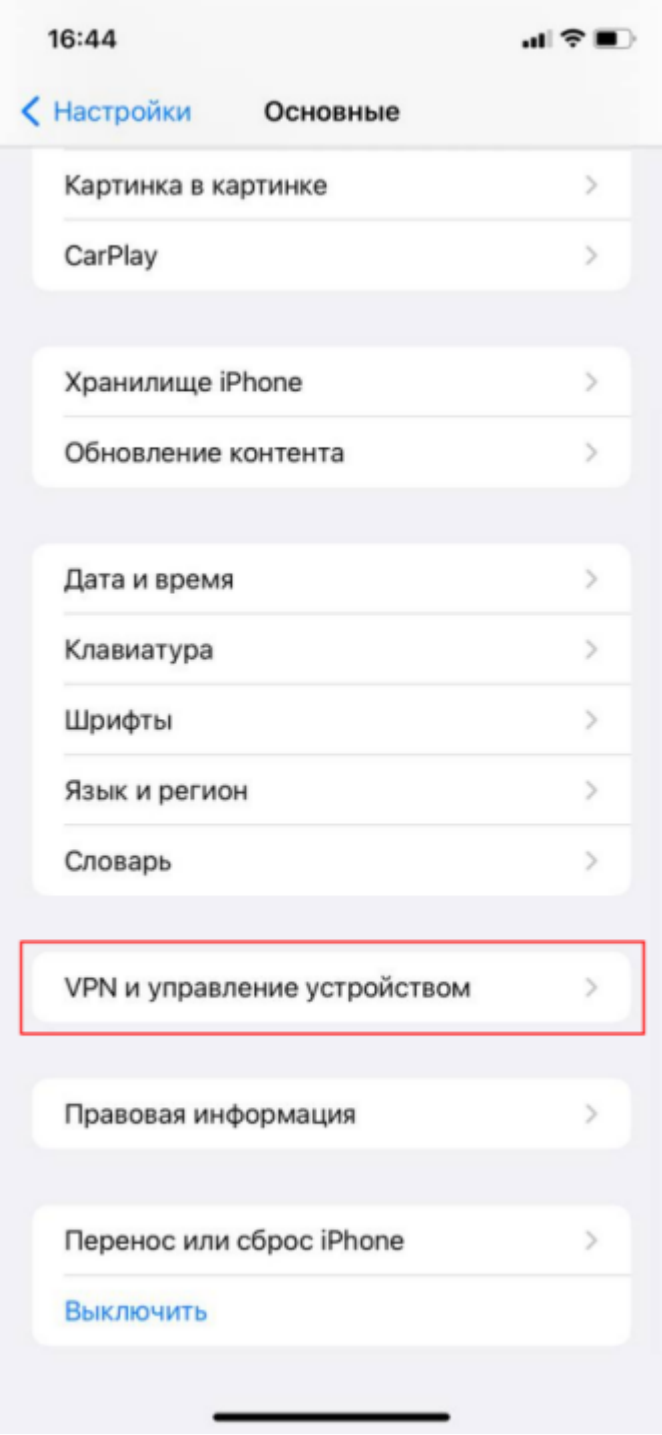


- **Имя** - имя подключения;
- **Адрес сервера** - адрес VPN-сервера;
- **Общий ключ IPsec** - значение строки **PSK** в разделе **Пользователи -> VPN-подключения -> Основное -> Подключение по L2TP/IPsec**.

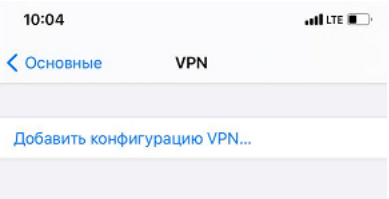
4. Нажмите **Сохранить** и активируйте подключение.

Подключение на iOS:

1. Перейдите в раздел **Настройки -> Основные -> VPN и управление устройством -> VPN**:



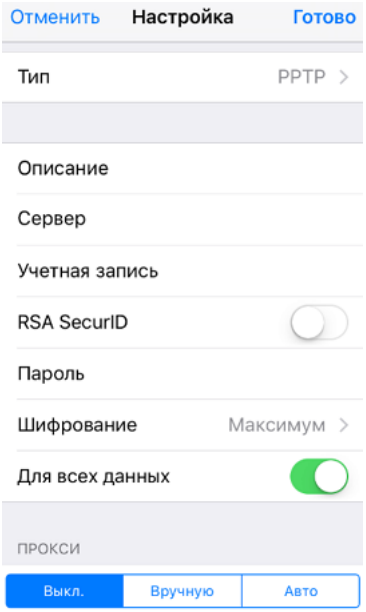
2. Нажмите **Добавить конфигурацию VPN**:



3. Выберите **Тип** подключения и заполните соответствующие поля:

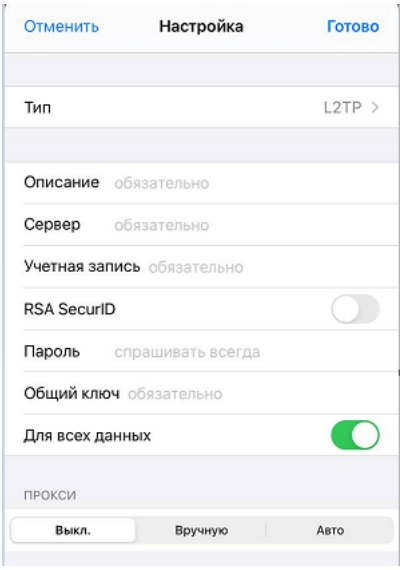
Для PPTP:

Начиная с версии iOS-10 компания Apple убрала поддержку протокола PPTP.



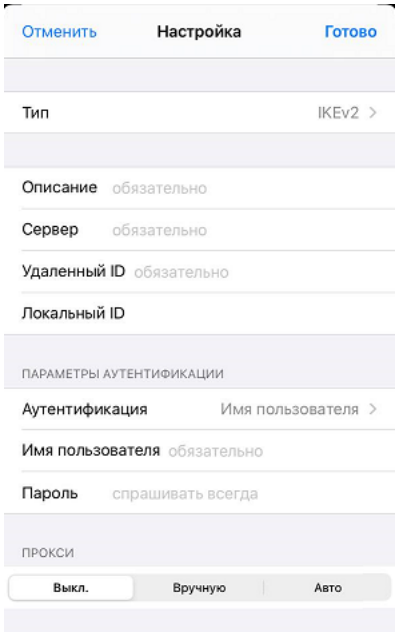
- **Описание** - название соединения;
- **Сервер** - адрес VPN-сервера;
- **Учетная запись** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

Для L2TP:



- **Описание** - название соединения;
- **Сервер** - адрес VPN-сервера;
- **Учетная запись** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя;
- **Общий ключ** - значение строки **PSK** в разделе **Пользователи -> VPN-подключения -> Основное -> Подключение по L2TP/IPsec**.

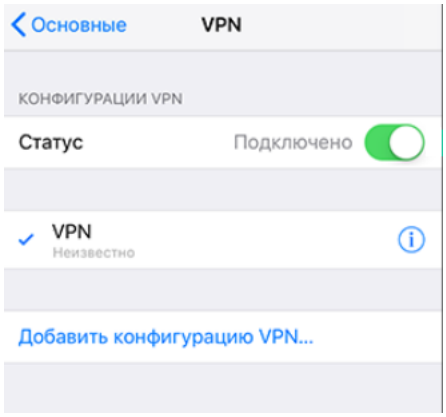
Для IKEv2:



- **Описание** - название соединения;
- **Сервер** - адрес VPN-сервера;
- **Удаленный ID** - адрес VPN-сервера;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

4. Нажмите **Готово**;

5. Переведите опцию **Статус** вправо:



38.20.7 Создание подключения в Mac OS

Основное

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Подсказка: При проблемах с подключением на IOS требуется:

1. Проверить, что в качестве VPN-сервера указано его доменное имя в разделе **Пользователи -> VPN-подключения**.

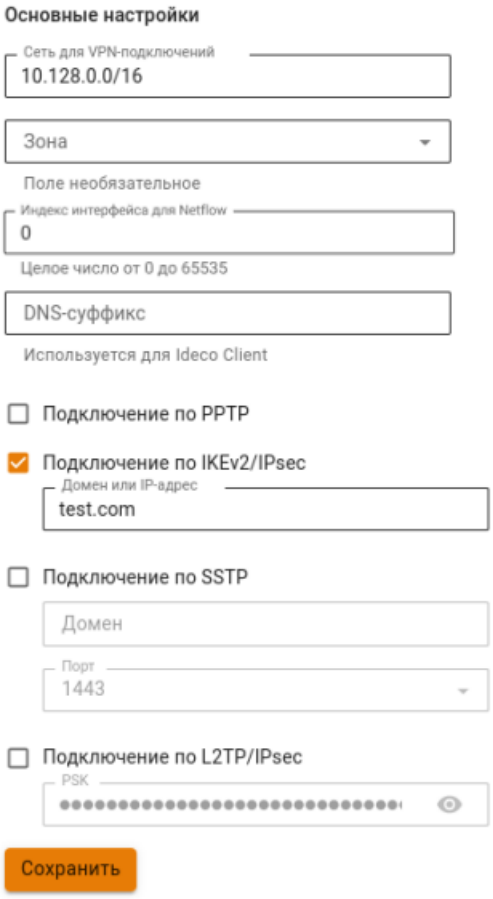
2. Проверить, что на доменное имя VPN-сервера выдан сертификат Let's Encrypt.

Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен или IP-адрес**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

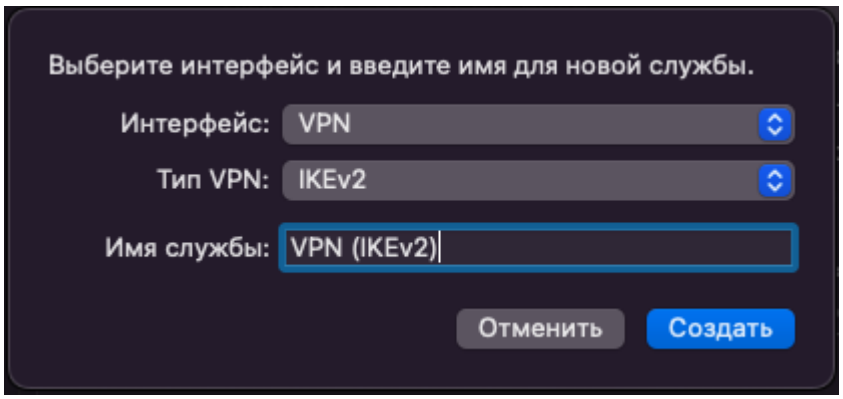
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки -> Сеть**.

2. Нажмите **Добавить** в левом нижнем углу (иконка +).

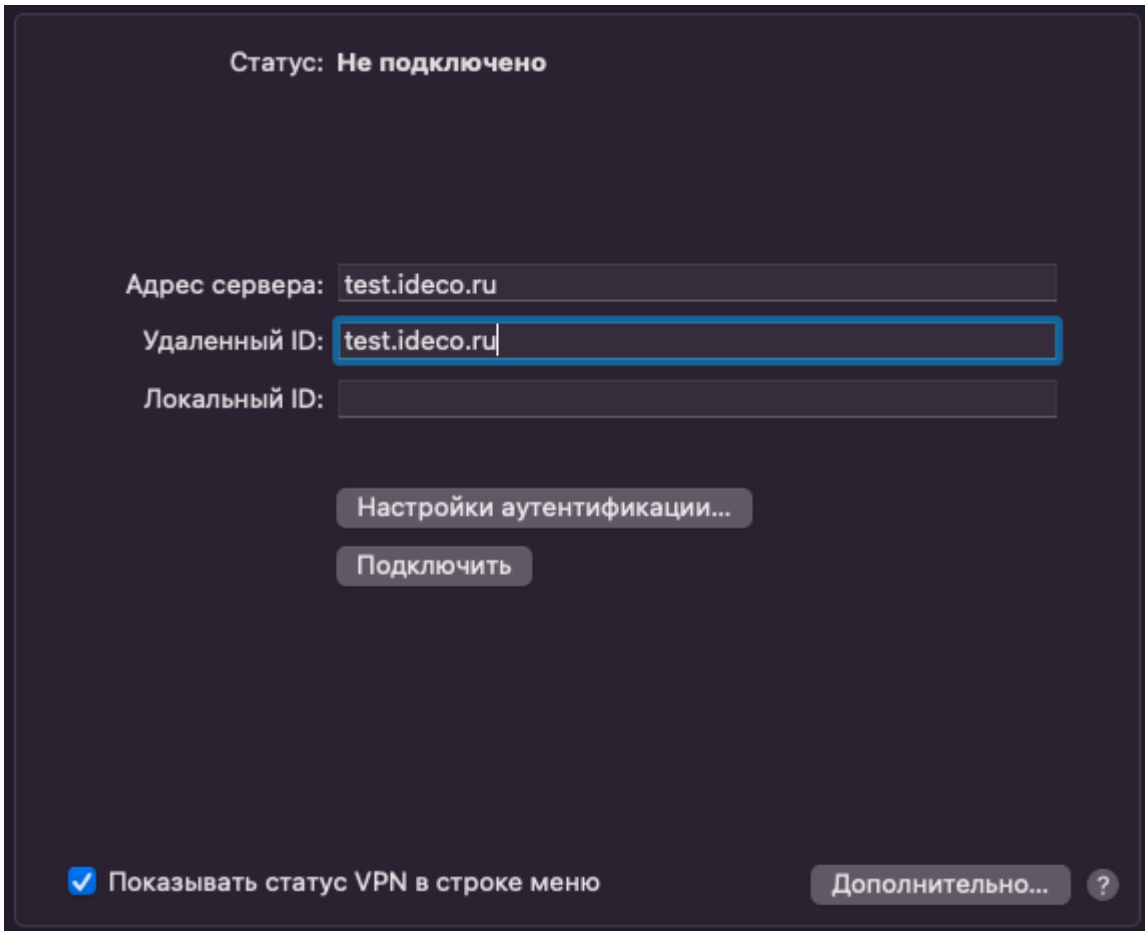
3. Заполните поля:



- **Интерфейс** - VPN;
- **Тип VPN** - IKEv2;
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

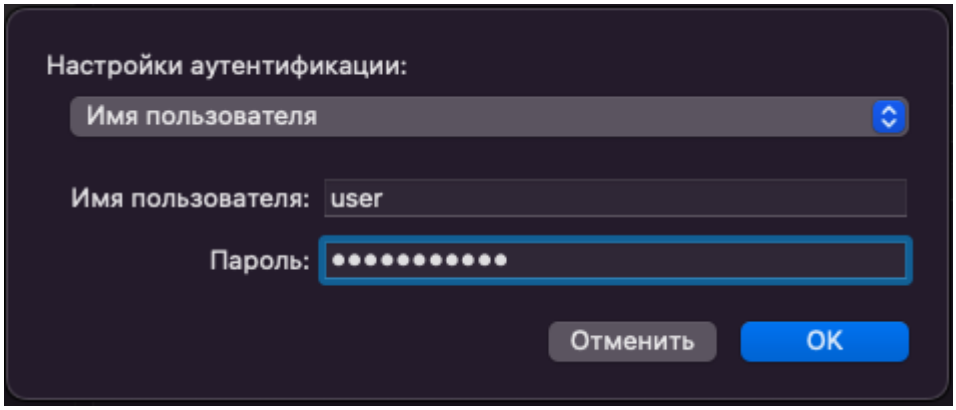
5. Установите параметры подключения:



- **Адрес сервера** - адрес VPN-сервера;
- **Удаленный ID** - продублируйте адрес VPN-сервера.

6. Выберите **Настройки аутентификации**.

7. Укажите идентификационные данные и нажмите **OK**:



- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

8. Нажмите **OK**.

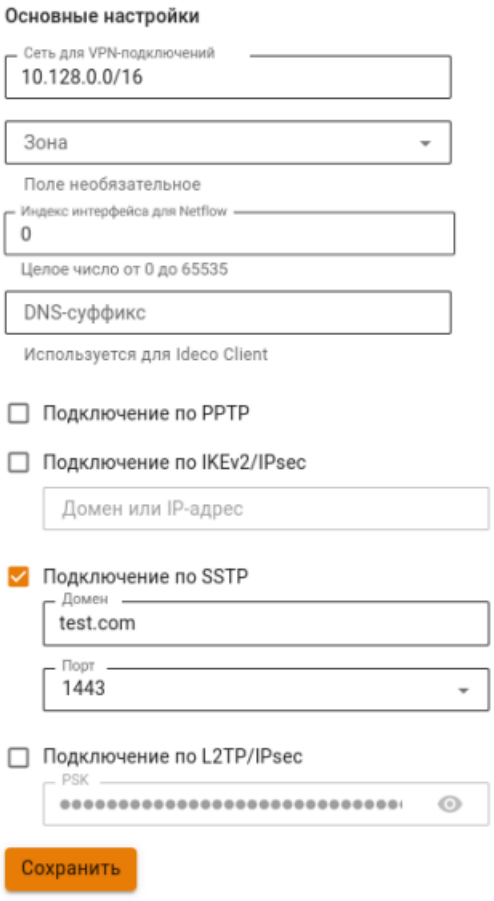
9. Поставьте флаг в пункте **Показывать статус VPN в строке меню**, нажмите **Применить** и включите соединение.

Протокол SSTP:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные**

сертификаты в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в MacOS:

1. Откройте терминал и установите `sstp-client`, выполнив команды:

```
brew update
brew install sstp-client
```

2. Создайте и включите SSTP-подключение командой:

```
sudo /usr/local/sbin/sstpc --cert-warn --tls-ext --user <логин пользователя Ideco␣
↪NGFW> --password <Пароль пользователя Ideco NGFW> <домен:порт> usepeerdns require-
↪mschap-v2 noauth noipdefault noccp refuse-eap refuse-pap refuse-mschap defaultroute
```

- Если указан параметр `defaultroute`, в VPN-туннель будет заворачиваться весь трафик.
- Чтобы через VPN-туннель проходил только трафик до определенных сетей, используйте параметр `nodefaultroute` и добавьте маршруты в таблицу маршрутизация вручную, например: `sudo route add -net "172.16.0.0/12" -interface ppp0`.

3. Для проверки подключения откройте новую вкладку или окно терминала и введите команду `ifconfig -a`. Если в выводе присутствует строка вида `ppp0: flags=8051 mtu 1500 inet 10.128.0.0 -> 10.128.0.1 netmask 0xff000000`, подключение установлено.

4. Чтобы отключить соединение, перейдите в терминал, из которого оно было установлено, и нажмите **Ctrl+C**.

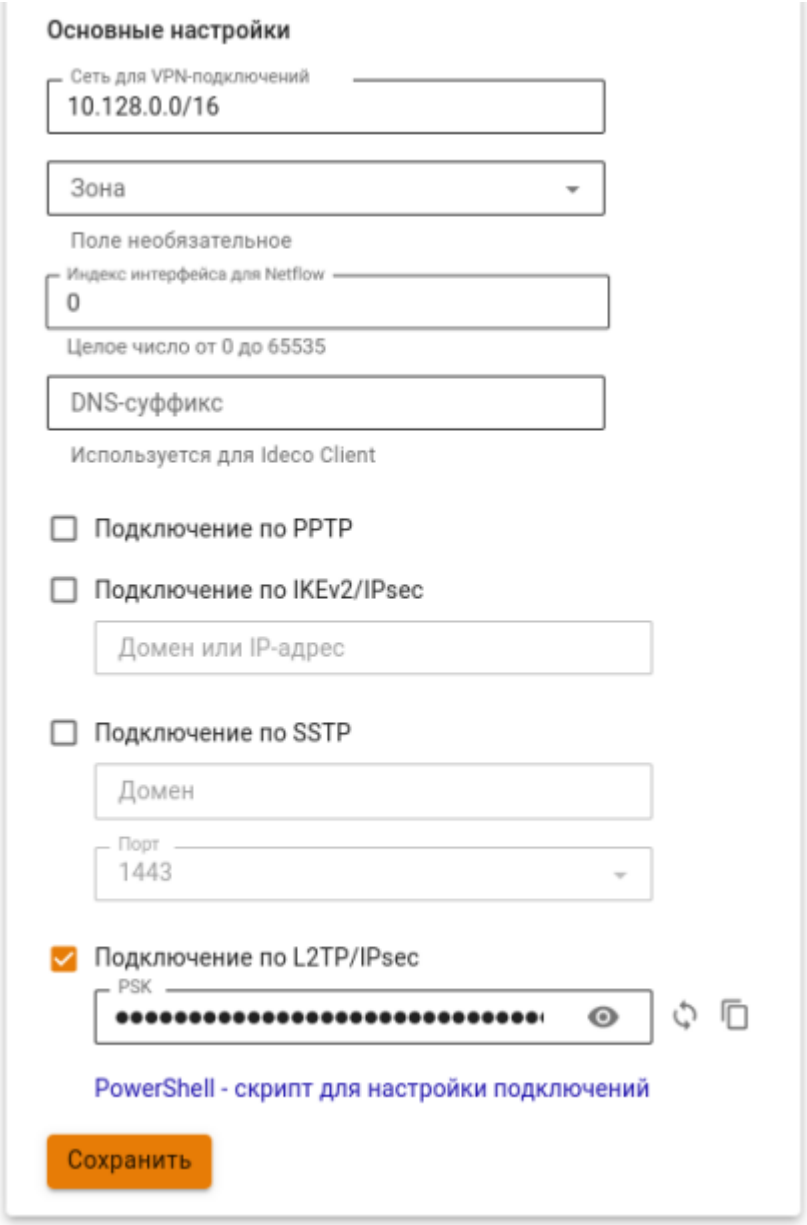
Протокол L2TP/IPsec:

Важно: L2TP IPsec-клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их более одного. Рекомендуем вместо L2TP IPsec использовать IKEv2 IPsec.

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

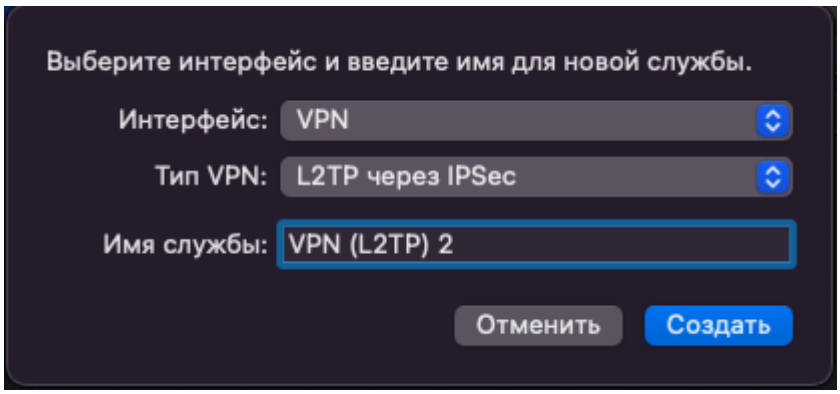
2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки -> Сеть** и нажмите **Добавить** в левом нижнем углу (иконка +).

3. Заполните поля:

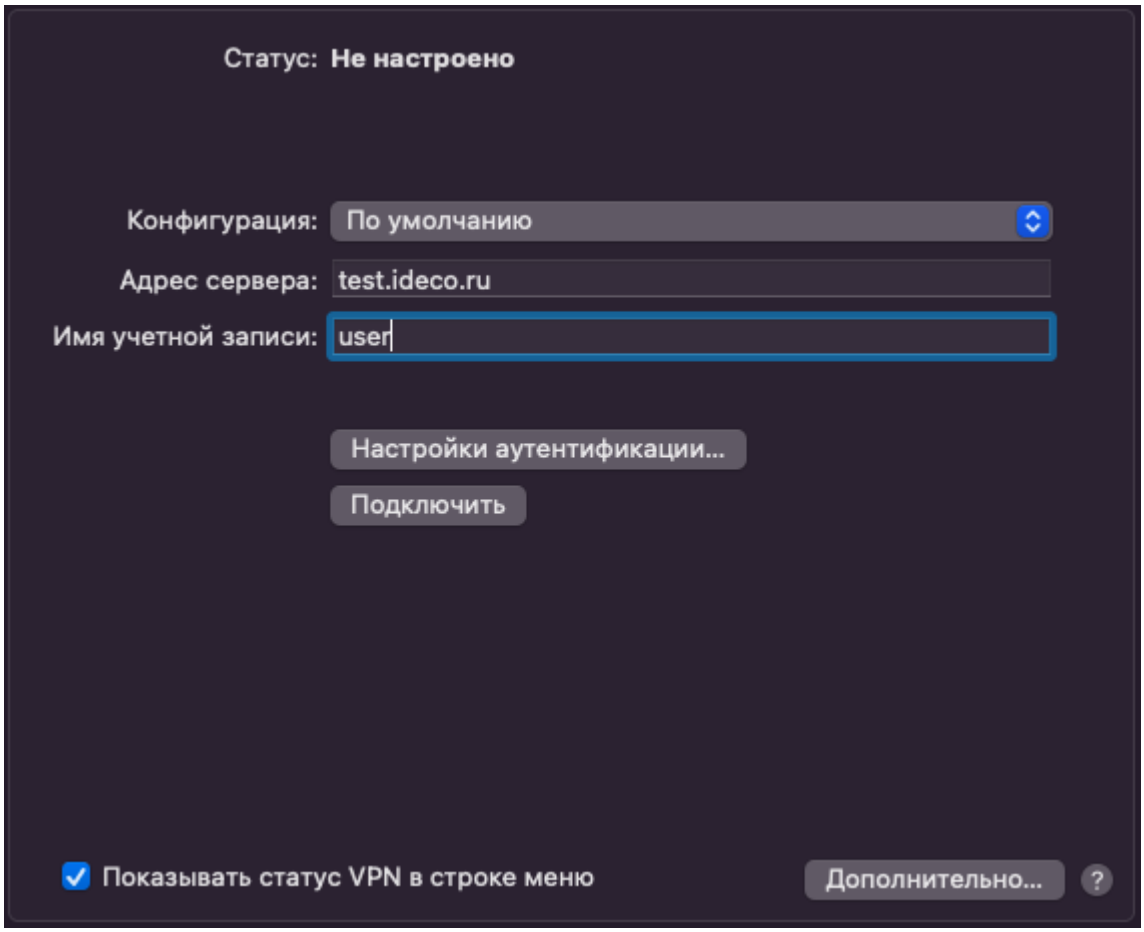


- **Интерфейс** - VPN;

- **Тип VPN** - L2TP через IPsec;
- **Имя службы** - имя подключения.

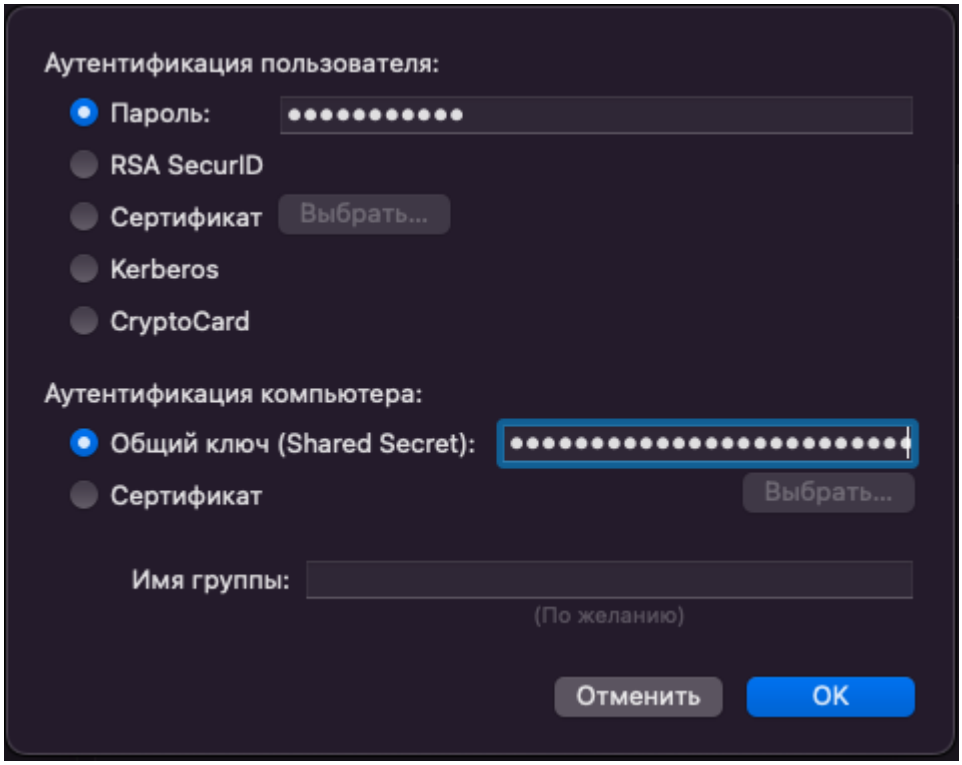
4. Нажмите **Создать**.

5. Заполните **Адрес сервера** и **Имя учетной записи**:



6. Поставьте флаг на пункте **Показывать статус VPN в строке меню** и выберите **Настройки аутентификации**.

7. В **Аутентификации пользователя** заполните **Пароль**, в **Аутентификации компьютера** - **Общий ключ (Shared Secret)**:



8. Нажмите **ОК -> Применить** и включите соединение.

38.20.8 Подключение по SSTP Wi-Fi роутеров Keenetic

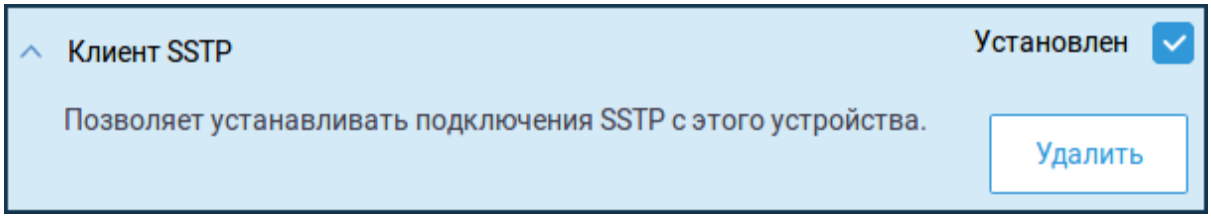
Основное

Поддерживаются все роутеры на базе KeeneticOS 3.x.x.

1. Выполните настройку пользователей в Ideco NGFW и включите SSTP в разделе **Пользователи -> VPN-подключения -> Основное**.

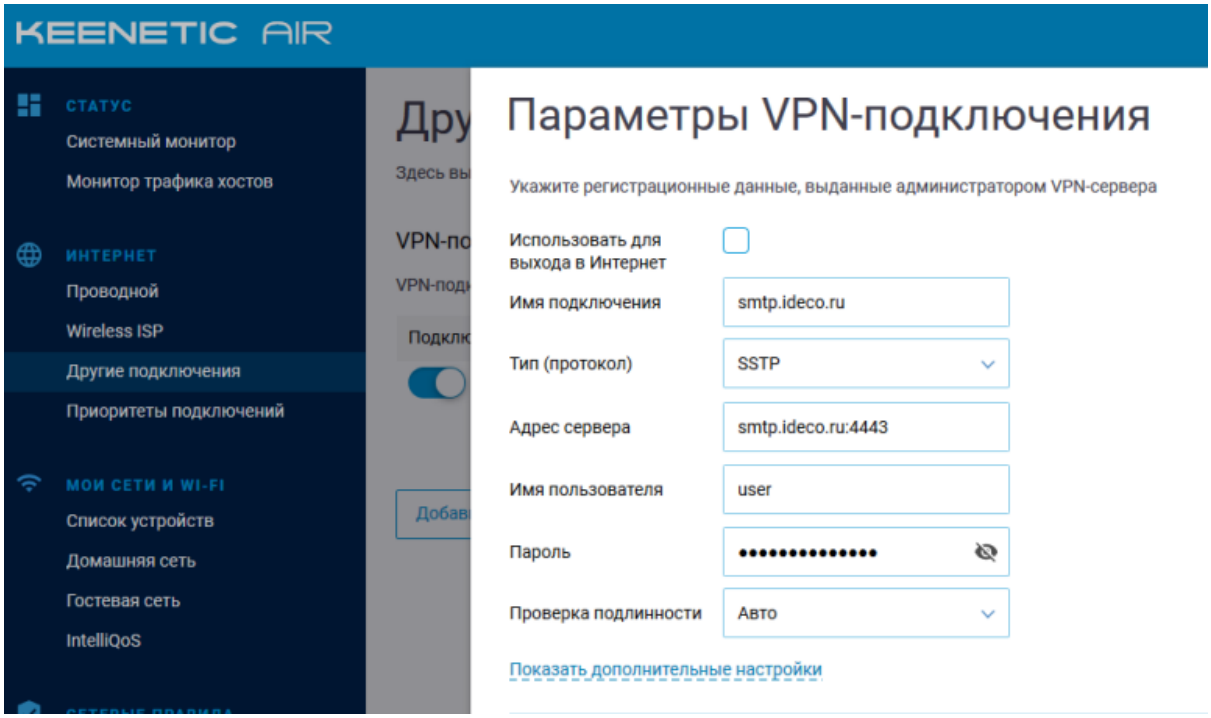
2. Зайдите в веб-интерфейс управления Keenetic: `http://my.keenetic.net`.

3. Установите компонент системы **Клиент SSTP** на странице **Общие настройки** в разделе **Обновления и компоненты**, нажмите **Изменить набор компонентов**.



Подробнее о настройках в документации Keenetic.

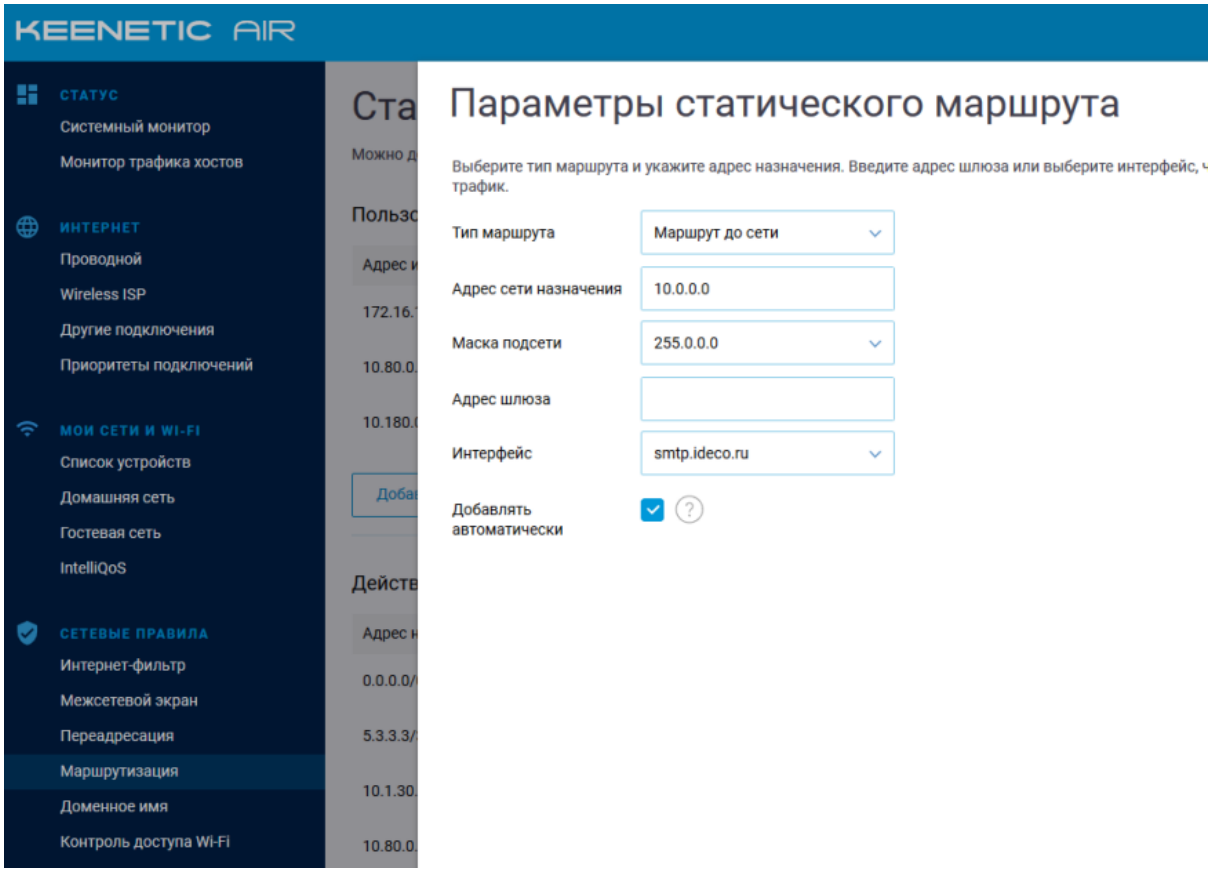
4. Создайте подключение в разделе **Интернет -> Другие подключения** нажмите кнопку **Добавить подключение**



Не устанавливайте флаг **Использовать для выхода в интернет**.

Введите имя подключения, протокол SSTP, адрес сервера (**обязательно укажите в адресе порт через двоеточие**), имя пользователя и пароль.

5. В разделе **Сетевые правила -> Маршруты** добавьте маршруты в рабочую сеть. Например, если сеть офиса `10.0.0.0/8`, добавьте маршрут:

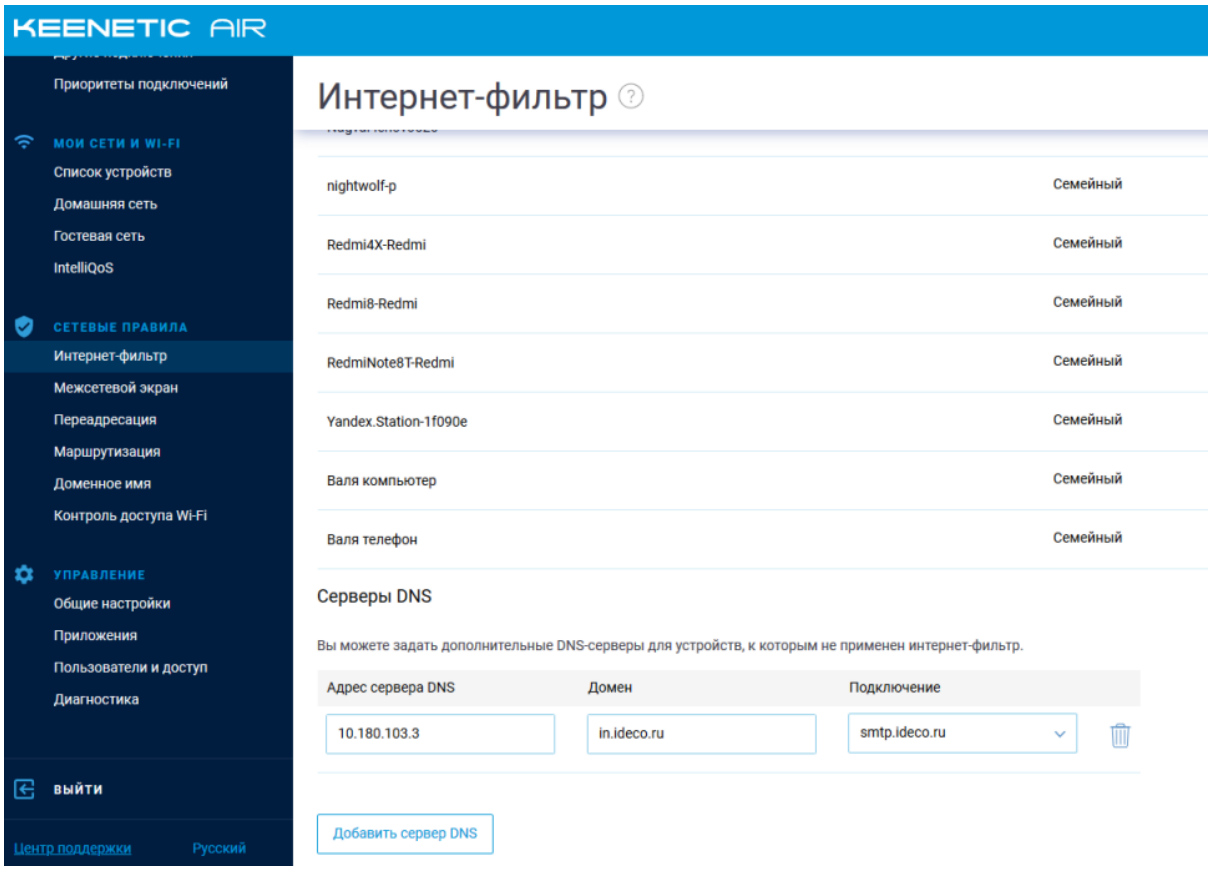


Выберите в качестве **Интерфейса** созданное VPN-подключение и установите флаг **Добавлять автомати-**

чески, чтобы маршрут действовал только при активном VPN-подключении.

6. Настройте DNS для локального домена (например, Active Directory), чтобы обращаться к ресурсам (файловым и иным серверам) по DNS-именам.

В разделе **Сетевые правила -> Интернет-фильтр -> Серверы DNS** укажите DNS-сервер контроллера домена и имя домена.



Настройка закончена.

7. Используйте утилиту ping в командной строке для проверки связи и маршрутизации.

`nslookup` - для проверки резолвинга локальных имен рабочей сети.

Если VPN работает, но с некоторыми ресурсами (например, файловыми или RDP) нет связи, воспользуйтесь инструкцией для диагностики проблем.

38.21 Подключение к сертифицированным Ideco EX и настройка Ideco NGFW

38.21.1 Подготовка к настройке

1. Подключите питание к серверу Ideco EX.

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

3. Убедитесь, что на ПК установлены утилиты по типу *tio* и *putty* для подключения к консольному порту.

38.21.2 Процесс подключения

Пример процесса подключения рассмотрим через утилиту *tio*.

1. Откройте терминал на ПК.

2. Подключитесь к серверу через консольный порт с помощью утилиты с правами суперпользователя:

```
sudo tio /dev/ttyUSB0
```

- `tio` - вызов утилиты;
- `/dev/ttyUSB0` - абсолютный путь до устройства.

Для вывода списка доступных устройств используйте команду `ls /dev/tty`.

3. На начальном экране загрузки NGFW нажмите **E**.

4. Переместите курсор в конец строки и проверьте наличие параметра `console=ttyS0,115200n8`. Если параметра нет, добавьте:

5. Нажмите **Enter** для начала загрузки NGFW.

Откроется локальное меню NGFW. Если нет учетной записи администратора, настройте ее по инструкции.

38.22 Анализ трафика

Для анализа трафика на компьютерах или NGFW используйте утилиту `tcpdump`. На Ideco NGFW утилита используется в разделе **Управление сервером -> Терминал**.

Подсказка: Утилита `tcpdump` предустановлена в продукт Ideco NGFW.

38.22.1 Описание использования утилиты и ключи tcpdump

Подсказка: Для работы `tcpdump` требует прав суперпользователя.

При запуске `tcpdump` без каких-либо ключей/параметров произойдет перехват всех пакетов через интерфейс по умолчанию.

Для просмотра всех ключей утилиты введите `tcpdump -h`.

Для более гибкого использования утилиты используйте комбинацию ключей.

Например:

Для вывода и разбора только 5 захваченных пакетов с интерфейса `eth1` введите:

```
tcpdump -i eth1 -c 5
```

Использование tcpdump с применением ключей

Просмотр списка сетевых интерфейсов:

Для просмотра введите в терминале:

```
tcpdump -D
```

Пример вывода утилиты:

```
1.eth0
2.nflog (Linux netfilter log (NFLOG) interface)
3.nfqueue (Linux netfilter queue (NFQUEUE) interface)
4.eth1
5.any (Pseudo-device that captures on all interfaces)
6.lo [Loopback]
```

Захват пакетов, проходящих через определенный интерфейс:

Для захвата пакетов с интерфейса `eth1` введите:

```
tcpdump -i eth1
```

Пример вывода утилиты:

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
01:06:09.278817 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761,␣
↪seq 1, length 64
01:06:09.279374 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 4761,␣
↪seq 1, length 64
01:06:10.281142 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761,␣
↪seq 2, length 6
```

Полезная информация:

- Ключ `-v` увеличивает количество отображаемой информации о пакетах (добавляется протокол, флаги пакета)
- Ключ `-vv` дает еще более подробную информацию (полный разбора пакета и вывод в терминал).

Пример использования с ключами:

```
tcpdump -i eth1 -v
```

```
tcpdump -i eth1 -vv
```

Вывод и захват только определенного числа пакетов:

Для захвата и разбора 5 пакетов с интерфейса по-умолчанию введите:

```
tcpdump -c 5
```

Пример вывода утилиты:

```
04:19:07.675216 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq␣
↪2186733178:2186733278, ack 204106815, win 37232, length 100
04:19:07.675497 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 100, win 65535,␣
↪length 0
04:19:07.675747 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 100:136, ack 1, win␣
↪37232, length 36
```

(continues on next page)

(продолжение с предыдущей страницы)

```
04:19:07.675902 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 136, win 65535,␣
↪length 0
04:19:07.676142 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 136:236, ack 1, win␣
↪37232, length 100
5 packets captured
```

Использование tcpdump с применением фильтров

Список часто используемых фильтров `tcpdump`:

- `port` - фильтрация пакетов по номеру порта;
- `host` - фильтрация исходящих и входящих пакетов по IP-адресу;
- `src` - фильтрация пакетов по IP-адресу источника;
- `dst` - фильтрация пакетов по IP-адресу назначения.

Для фильтрации по определенному протоколу укажите его в качестве фильтра:

- `tcp` - фильтрация пакетов с протоколом `TCP`;
- `udp` - фильтрация пакетов с протоколом `UDP`;
- `icmp` - фильтрация пакетов с протоколом `ICMP`;
- `arp` - фильтрация пакетов с протоколом `ARP`.

Для комбинирования фильтров используйте логические операторы:

- `and` - пакет выведется при совпадении условий у всех указанных фильтров;
- `or` - пакет выведется при совпадении условий у одного указанного фильтра;
- `not` - инвертирует условие фильтра.

Фильтрация пакетов по 80 порту:

Для фильтрации введите:

```
tcpdump port 80
```

Пример вывода утилиты:

```
23:54:24.978612 IP 10.0.0.1.53971 > 10.0.0.50.80: Flags [SEW], seq 53967733, win␣
↪65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 256360128 ecr 0,sackOK,eol],␣
↪length 0
23:54:24.978650 IP 10.0.0.50.80 > 10.0.0.1.53971: Flags [S.E], seq 996967790, ack␣
↪53967734, win 28960, options [mss 1460,sackOK,TS val 5625522 ecr 256360128,nop,
↪wscale 6], length 0
23:54:24.978699 IP 10.0.0.1.53972 > 10.0.0.50.80: Flags [SEW], seq 226341105, win␣
↪65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 256360128 ecr 0,sackOK,eol],␣
↪length 0
23:54:24.978711 IP 10.0.0.50.80 > 10.0.0.1.53972: Flags [S.E], seq 1363851389, ack␣
↪226341106, win 28960, options [mss 1460,sackOK,TS val 5625522 ecr 256360128,nop,
↪wscale 6], length 0
```

Фильтрация пакетов по хосту с IP-адресом 10.0.2.15:

Для фильтрации введите:

```
tcpdump host 10.0.2.15
```

Пример вывода утилиты:

```
03:48:06.087509 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq␣
↪3862934963:3862934999, ack 65355639, win 37232, length 36
03:48:06.087806 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 36, win 65535,␣
↪length 0
03:48:06.088087 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 36:72, ack 1, win␣
↪37232, length 36
03:48:06.088274 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 72, win 65535,␣
↪length 0
03:48:06.088440 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 72:108, ack 1, win␣
↪37232, length 36
```

Фильтрация пакетов по IP-адресу назначения 8.8.8.8:

Для фильтрации введите:

```
tcpdump dst 8.8.8.8
```

Пример вывода утилиты:

```
17:32:19.642154 IP desktop > dns.google: ICMP echo request, id 1, seq 1, length 64
17:32:20.644231 IP desktop > dns.google: ICMP echo request, id 1, seq 2, length 64
17:32:21.645715 IP desktop > dns.google: ICMP echo request, id 1, seq 3, length 64
17:32:22.647387 IP desktop > dns.google: ICMP echo request, id 1, seq 4, length 64
17:32:23.648814 IP desktop > dns.google: ICMP echo request, id 1, seq 5, length 64
```

Фильтрация пакетов по протоколу ICMP:

Для фильтрации введите:

```
tcpdump icmp
```

Пример вывода утилиты:

```
04:03:47.408545 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812,␣
↪seq 75, length 64
04:03:47.408999 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812,␣
↪seq 75, length 64
04:03:48.408697 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812,␣
↪seq 76, length 64
04:03:48.409208 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812,␣
↪seq 76, length 64
04:03:49.411287 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812,␣
↪seq 77, length 64
```

Фильтрация пакетов с интерфеса eth1 с IP-адресом источника 10.0.0.1 и 80 портом назначения:

Для фильтрации введите:

```
tcpdump -i eth1 src 10.0.0.1 and dst port 80
```

Пример вывода утилиты:

```
00:18:17.155066 IP 10.0.0.1.54222 > 10.0.0.50.80: Flags [F.], seq 500773341, ack␣
↪2116767648, win 4117, options [nop,nop,TS val 257786173 ecr 5979014], length 0
00:18:17.155104 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [S], seq 904045691, win 65535,
↪ options [mss 1460,nop,wscale 5,nop,nop,TS val 257786173 ecr 0,sackOK,eol], length 0
00:18:17.157337 IP 10.0.0.1.54221 > 10.0.0.50.80: Flags [P.], seq␣
↪4282813257:4282813756, ack 1348066220, win 4111, options [nop,nop,TS val 257786174␣
↪ecr 5979015], length 499: HTTP: GET / HTTP/1.1
```

(continues on next page)

(продолжение с предыдущей страницы)

```
00:18:17.157366 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [.], ack 1306947508, win 4117,
↪ options [nop,nop,TS val 257786174 ecr 5983566], length 0
```

Фильтрация пакетов по всем доступным протоколам, кроме ICMP:

Для фильтрации введите:

```
tcpdump not icmp
```

Пример вывода утилиты:

```
17:45:34.847882 IP desktop.48552 > 149.154.167.41.https: Flags [P.], seq␣
↪3991504547:3991504748, ack 499514727, win 248, options [nop,nop,TS val 1585771305␣
↪ecr 4205201964], length 201
17:45:34.918383 IP 149.154.167.41.https > desktop.48552: Flags [.], ack 201, win 7509,
↪ options [nop,nop,TS val 4205203056 ecr 1585771305], length 0
17:45:34.919444 IP 149.154.167.41.https > desktop.48552: Flags [.], seq 1:1229, ack␣
↪201, win 7509, options [nop,nop,TS val 4205203056 ecr 1585771305], length 1228
17:45:34.919475 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 1229, win 239,
↪ options [nop,nop,TS val 1585771377 ecr 4205203056], length 0
17:45:34.919778 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 1229:2457,␣
↪ack 201, win 7509, options [nop,nop,TS val 4205203056 ecr 1585771305], length 1228
17:45:34.919804 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2457, win 239,
↪ options [nop,nop,TS val 1585771377 ecr 4205203056], length 0
17:45:34.923322 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 2457:2845,␣
↪ack 201, win 7509, options [nop,nop,TS val 4205203061 ecr 1585771305], length 388
17:45:34.923351 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2845, win 239,
↪ options [nop,nop,TS val 1585771381 ecr 4205203061], length 0
17:45:35.644804 IP desktop.49669 > _gateway.domain: 65295+ PTR? 41.167.154.149.in-
↪addr.arpa. (45)
```

Сохранение дампа захваченных пакетов в файл в формате .pcap:

Для сохранения дампа в файл `out.pcap` введите:

```
tcpdump -w out.pcap
```

Подсказка: Для анализа захваченных пакетов в формате `.pcap` используйте Wireshark.

Примеры использования с Ideco NGFW

Проверка работы IPsec-туннелей:

Позволяет понять причину неработоспособности IPsec-туннеля.

1. Для проверки прохождения трафика на всех интерфейсах головного офиса по порту 4500 введите:

```
tcpdump -i any port 4500 -ttttnnn
```

2. Для проверки прохождения трафика на всех интерфейсах филиала по порту 500 введите:

```
tcpdump -i any port 500 -tttnnn
```

38.23 Режим удаленного помощника

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

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

Предупреждение: Включение режима удаленного помощника изменяет таблицу правил файрвола. При этом становится доступно подключение по SSH из локальных и внешних сетей.

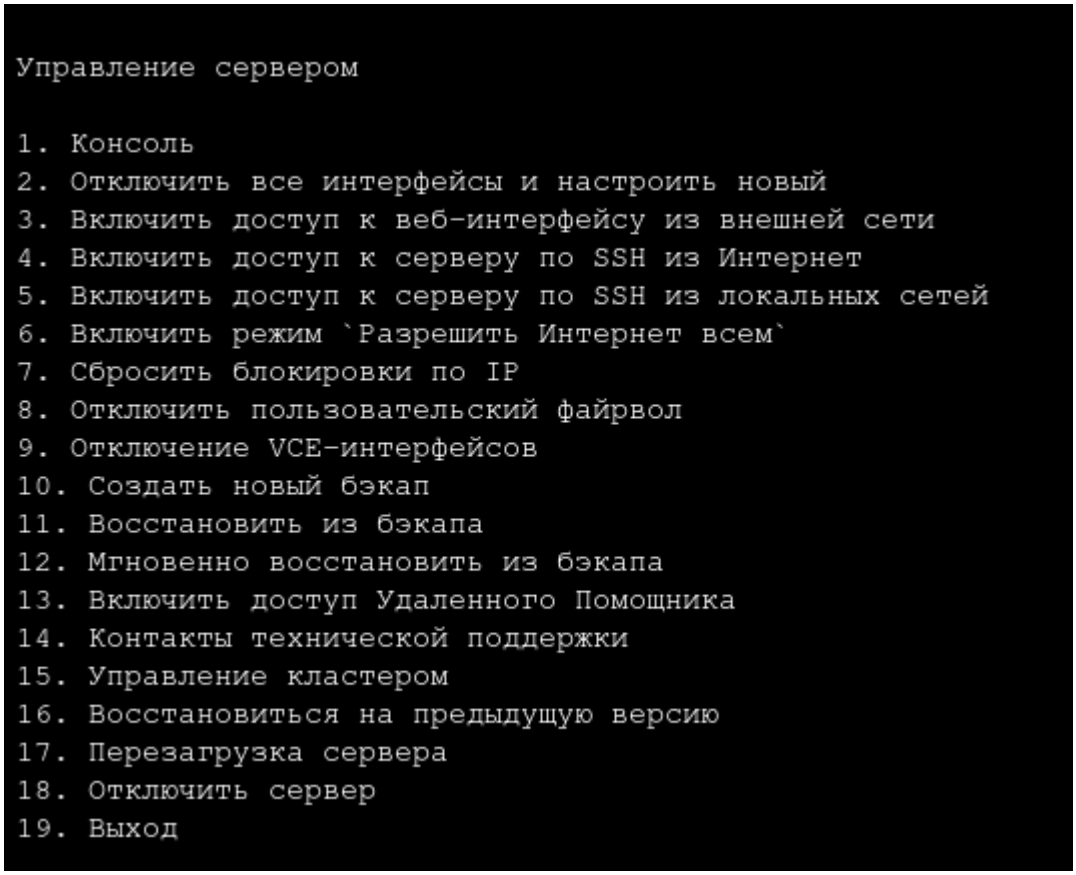
38.23.1 Включение режима удаленного помощника из веб-интерфейса

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

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

38.23.2 Включение режима удаленного помощника из локального меню сервера

Чтобы включить режим удаленного помощника, в локальном меню Ideco NGFW выберите пункт **Включить доступ Удаленного помощника**, введя пункт **13**, затем нажмите **Enter**.
Сгенерируется пароль, который необходимо сообщить технической поддержке для подключения по SSH.



38.23.3 Работа с сервером по протоколу SSH в режиме удаленного помощника

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

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

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

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

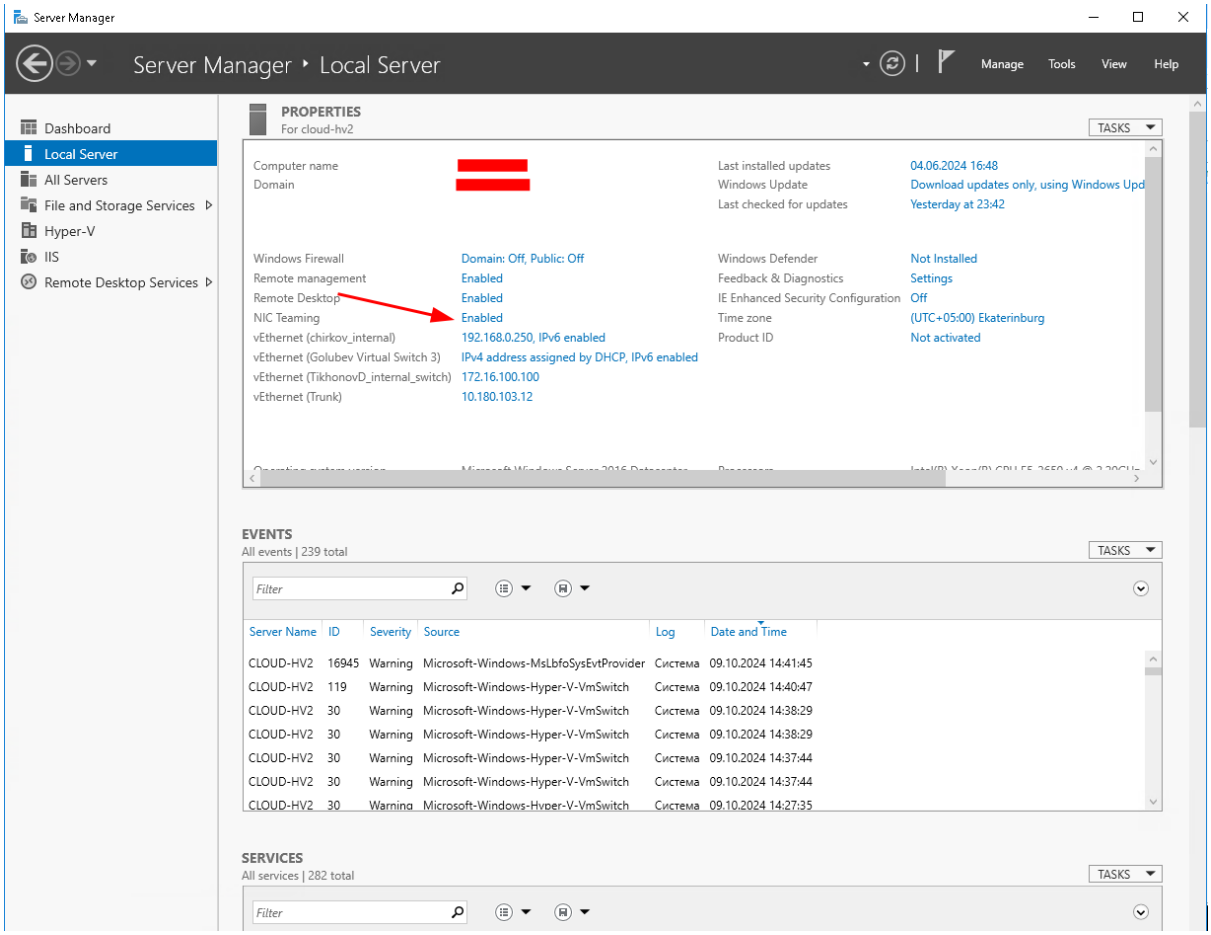
Символ «#» свидетельствует, что работа ведется от имени суперпользователя.

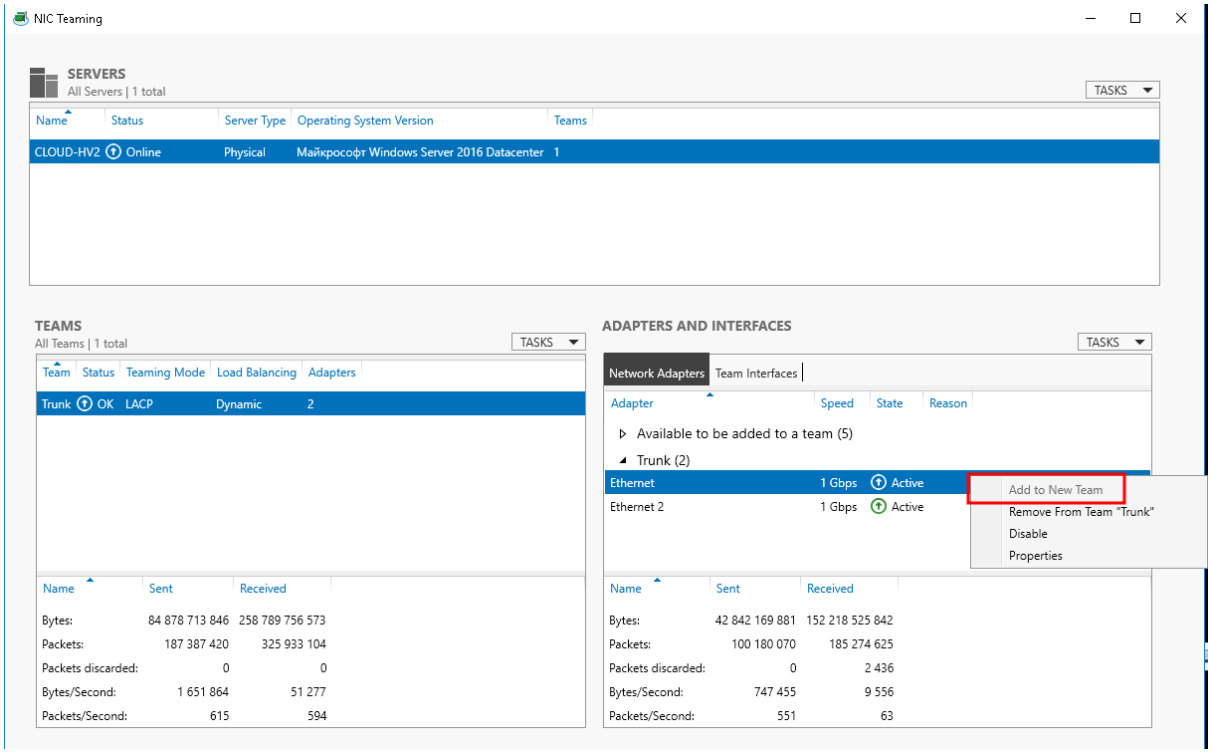
38.24 Настройка LACP на Hyper-V

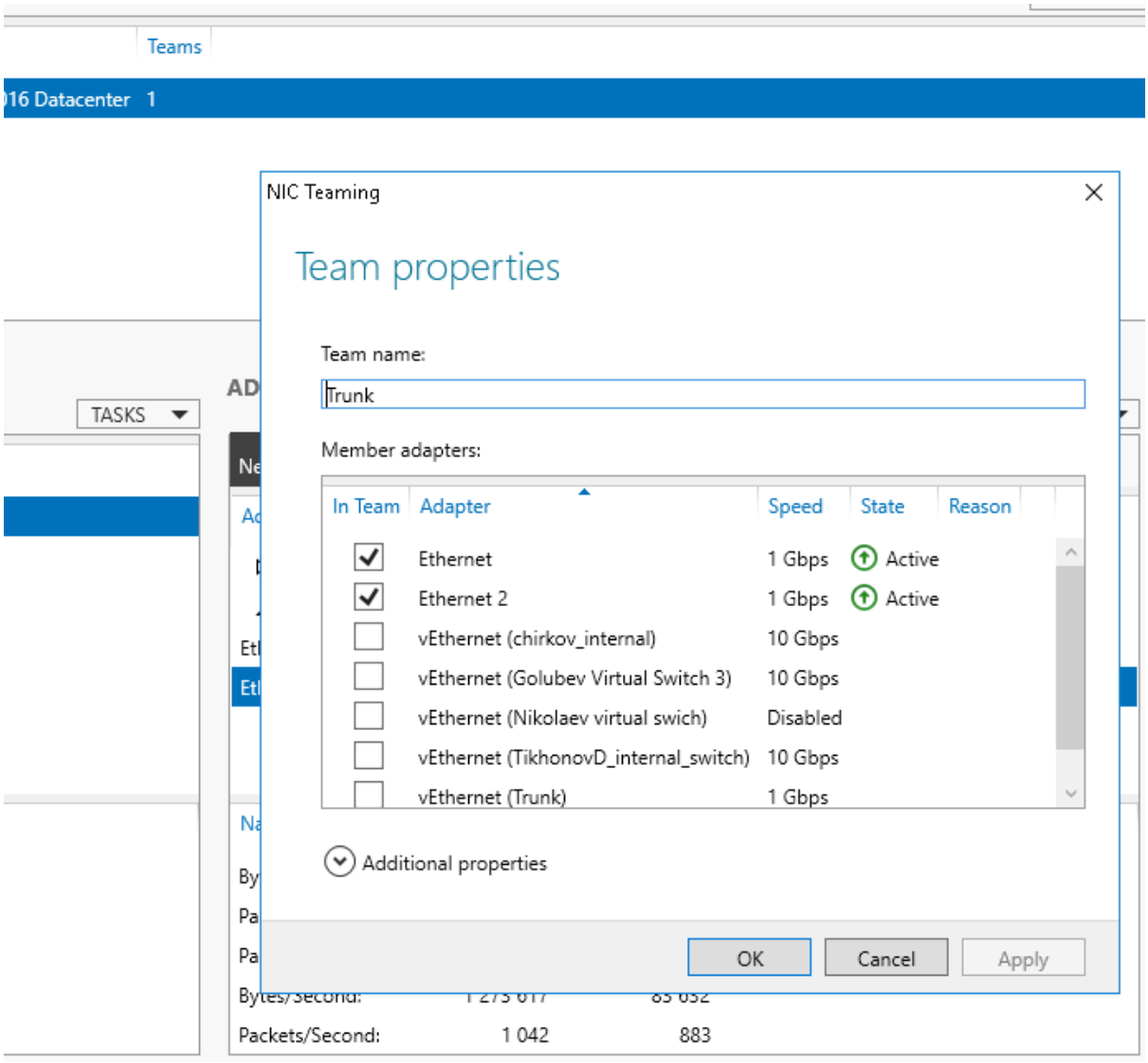
Для настройки LACP на гипервизоре Hyper-V существуют два способа:

38.24.1 Настройка на хост системе

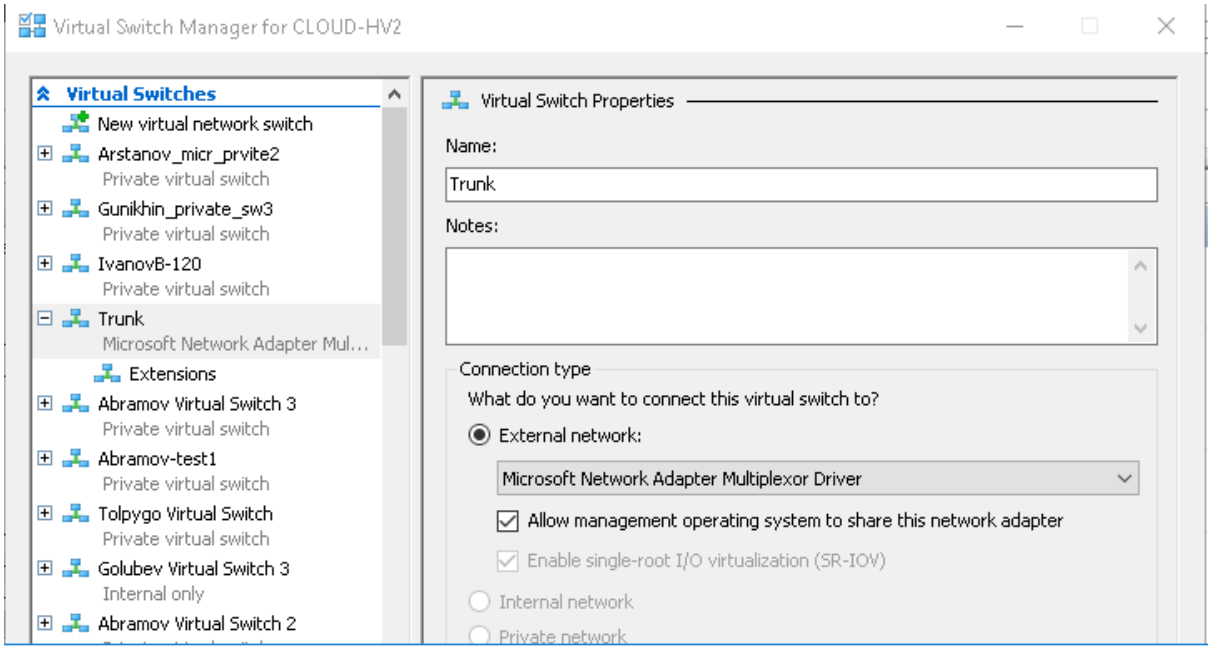
1. Объедините физические интерфейсы:

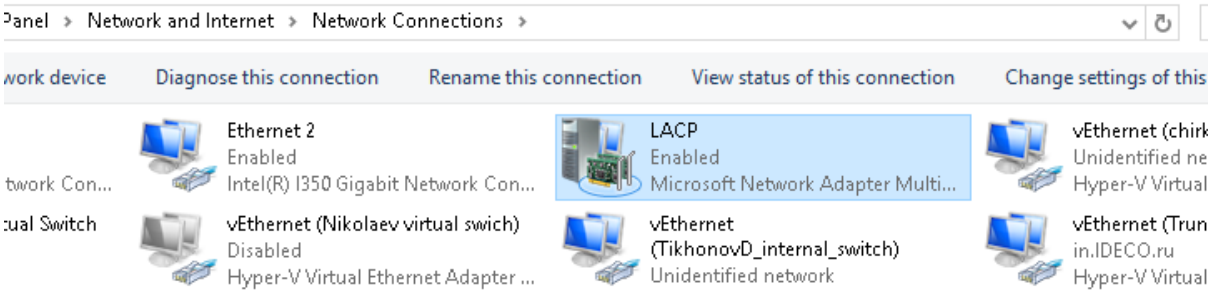



NIC Teaming
SERVERS
All Servers | 1 total
TASKS
Name
Status
Server Type
Operating System Version
Teams
CLOUD-HV2
Online
Physical
Майкрософт Windows Server 2016 Datacenter
1
TEAMS
All Teams | 1 total
TASKS
Team
Status
Teaming Mode
Load Balancing
Adapters
Trunk
OK
LACP
Dynamic
2
Name
Sent
Received
Bytes:
84 878 713 846
258 789 756 573
Packets:
187 387 420
325 933 104
Packets discarded:
0
0
Bytes/Second:
1 651 864
51 277
Packets/Second:
615
594
ADAPTERS AND INTERFACES
TASKS
Network Adapters
Team Interfaces
Adapter
Speed
State
Reason
Available to be added to a team (5)
Trunk (2)
Ethernet
1 Gbps
Active
Ethernet 2
1 Gbps
Active
Add to New Team
Remove From Team "Trunk"
Disable
Properties
Name
Sent
Received
Bytes:
42 842 169 881
152 218 525 842
Packets:
100 180 070
185 274 625
Packets discarded:
0
2 436
Bytes/Second:
747 455
9 556
Packets/Second:
551
63



2. Выберите созданный интерфейс при настройке виртуального свитча:





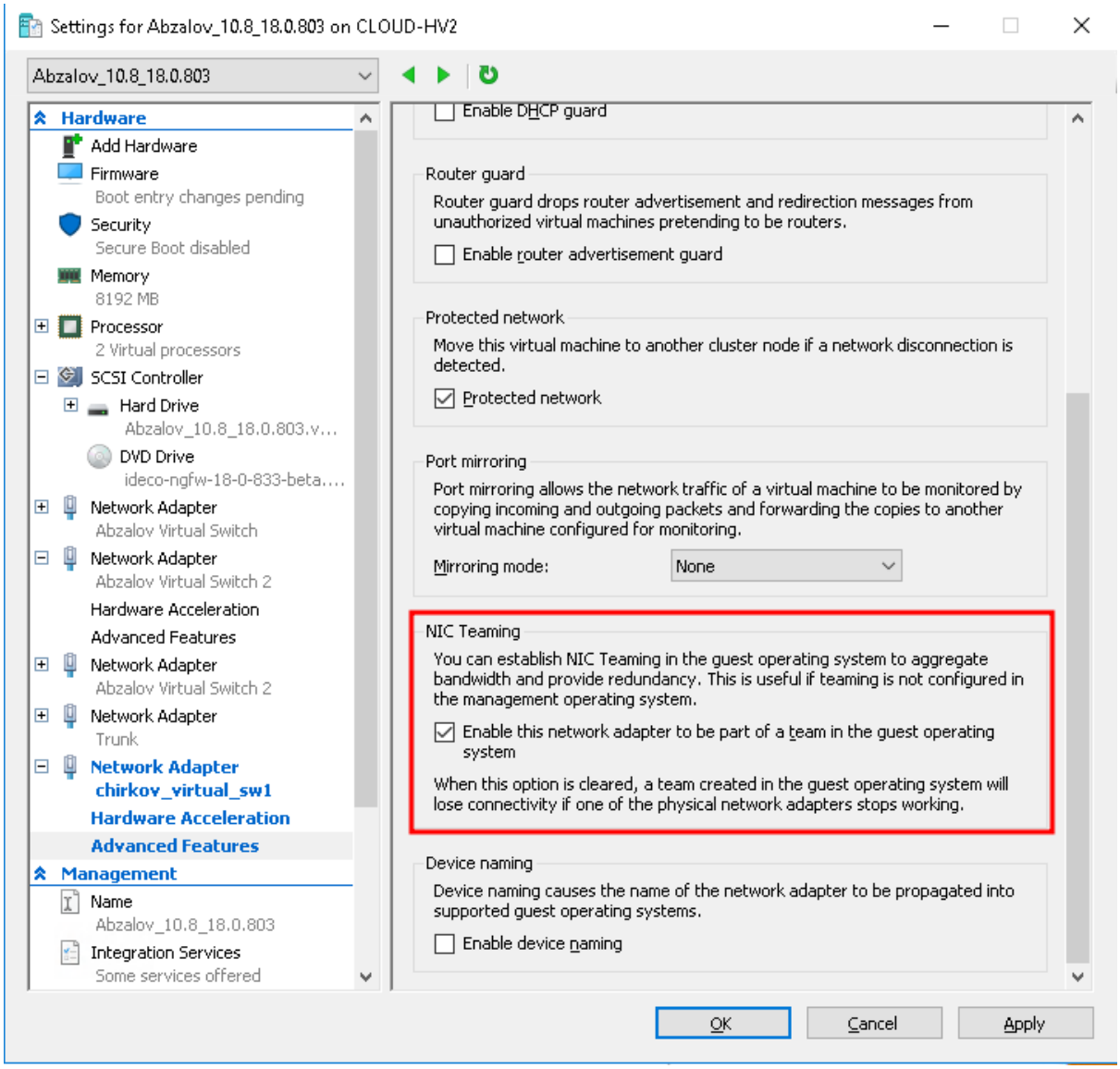
Получившийся виртуальный свитч можно использовать для добавления новых интерфейсов в LACP на гостевую систему.

3. Настройте подключение на вкладке **Сетевые интерфейсы -> Внешние и локальные** для вновь созданного LACP-интерфейса, как для обычного сетевого интерфейса NGFW.

38.24.2 Настройка на гостевой системе

1. Добавьте необходимое количество интерфейсов на гостевую систему, на основе виртуального свитча, например, с названием **Virtual Switch 1**.

2. На каждом добавляемом интерфейсе включите опцию NIC Teaming:



3. Добавьте вновь созданные интерфейсы в LACP-интерфейсы NGFW в разделе **Сетевые интерфейсы -> Агрегированные(LACP)**.

4. Настройте подключения на вкладке **Сетевые интерфейсы -> Внешние и локальные**.

38.25 Разрешить интернет всем: диагностика неполадок

38.25.1 Основное

Этот режим используется для диагностики неполадок.

Активный режим **Разрешить интернет всем** автоматически не отключается и работает, пока его не отключить.

При этом:

- не будут работать правила *файрвола*;
- не будет происходить фильтрация трафика;
- не будет производиться сбор веб-статистики;
- не будет доступа к серым IP-адресам за NGFW из внешней сети;

- пользователям будет разрешен доступ в интернет без авторизации.

Включить режим можно двумя способами:

1. Через веб-интерфейс.

Для этого нажмите на иконку технической поддержки в верхней правой части окна  и в открывшемся окне переведите ползунок активации режима в положение **Активно.**

2. Через локальное меню.
Для этого введите номер пункта **6. Включить режим Разрешить интернет всем** и нажмите **Enter** для применения настройки.

38.26 Удаленный доступ к серверу

38.26.1 Доступ по SSH к локальному меню сервера

Для подключения по SSH из внешних или локальных сетей выполните действия:

1. Перейдите в раздел **Управление сервером -> Администраторы**.

2. Уточните сеть, из которой планируется подключение:

- При подключении из внешних сетей активируйте **Доступ по SSH из внешних сетей**.
- При подключении из локальных сетей активируйте **Доступ по SSH из локальных сетей**.

3. Подключитесь к серверу с помощью любого SSH-клиента (например, PuTTY), используя 22 порт. Скачать SSH-клиент PuTTY можно на сайте https://www.putty.org/. Необходимо указать логин **Администратора** и его пароль.

4. Используйте `ideco-local-menu --debug` для доступа к локальному меню или `ls` для вывода каталогов текущей директории.

Пример подключения при помощи OpenSSH через консоль:

```
[test@My-PC home]$ ssh admin@192.168.100.183
admin@192.168.100.183's password:
Last login: Wed Sep  6 11:51:38 2023 from 192.168.100.1
[admin@localhost ~]#
```

38.26.2 Доступ к веб-интерфейсу сервера из сети интернет

Доступ из внешней сети:

- Включите функцию **Доступ к веб-интерфейсу из внешней сети** в разделе **Управление сервером -> Администраторы**. Для доступа введите внешний IP-адрес Ideco NGFW и порт 8443.

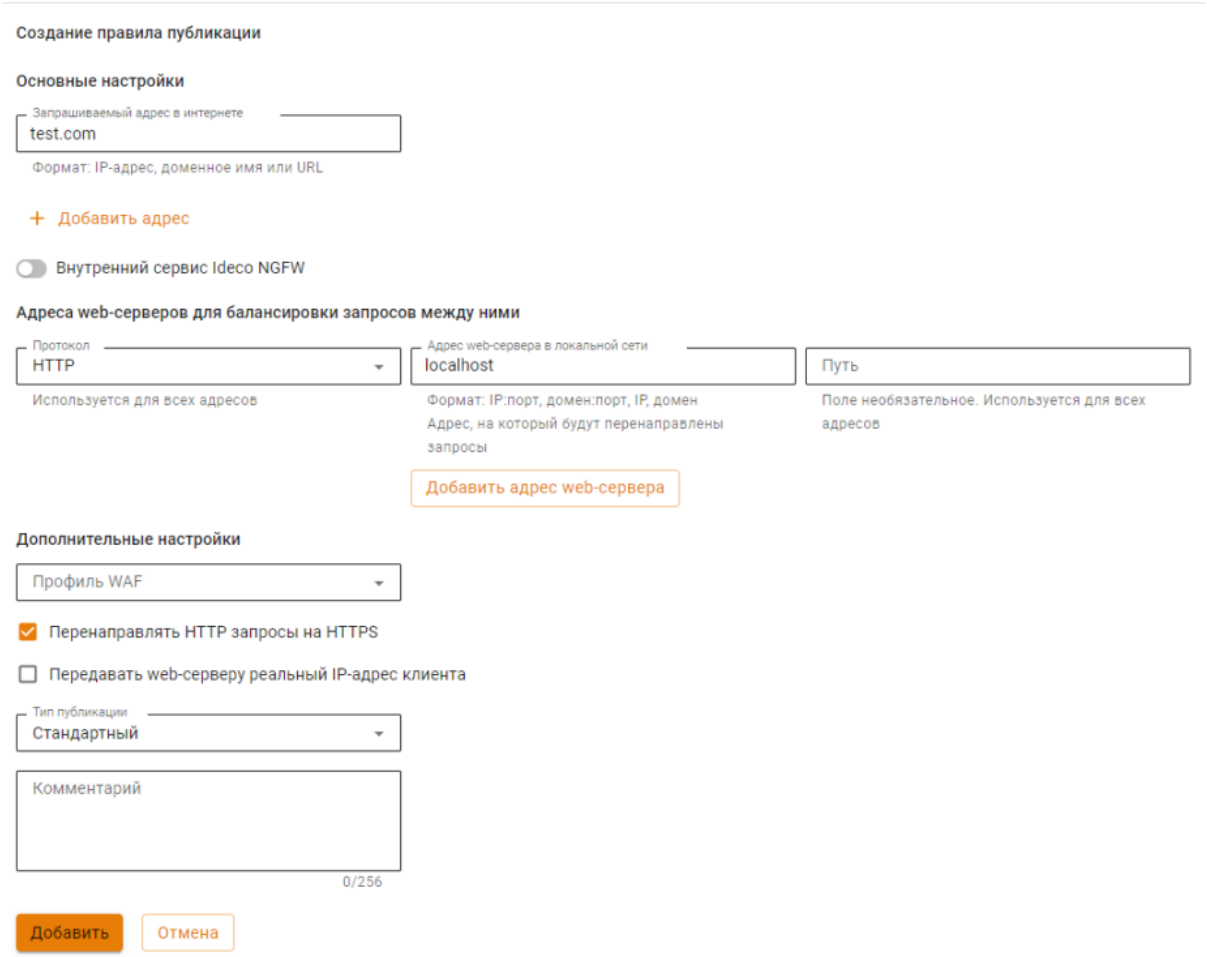
Доступ по VPN:

- Создайте VPN-подключение к серверу, например, по IPsec, IKEv2 или SSTP. После подключения можно перейти в веб-интерфейс по IP-адресу любого локального интерфейса (в том числе IP-адрес из диапазона для VPN-подключений. Адрес по умолчанию - 10.128.0.1).

Публикация через обратный прокси:

1. Перейдите в раздел **Сервисы -> Обратный прокси**.

2. Добавьте новое правило, заполнив поля:



3. Укажите в качестве запрашиваемого адреса IP-адрес или доменное имя внешнего интерфейса Ideco NGFW.

4. Нажмите на кнопку **Добавить** и зайдите по одному из адресов, которые были указаны в поле **Запрашиваемый адрес в интернете**.

38.27 Тестирование оперативной памяти сервера

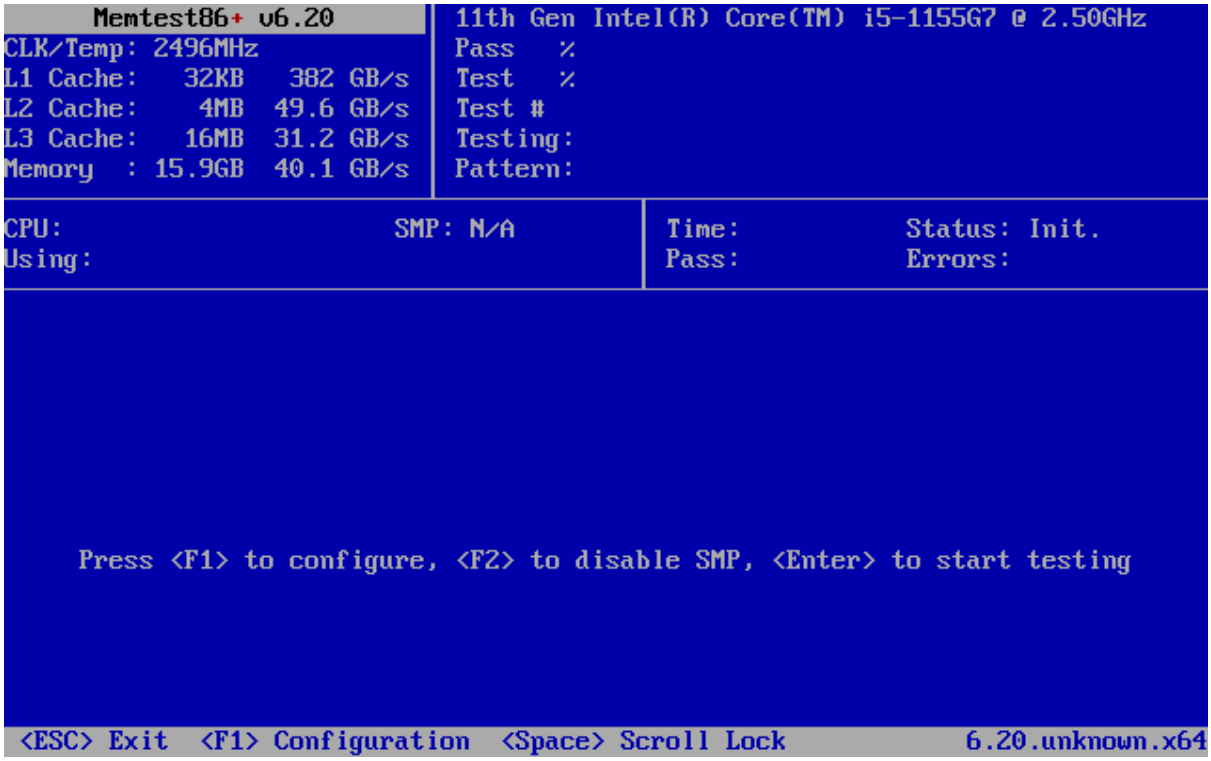
38.27.1 Основное

Для корректной работы сервера требуется, чтобы все его аппаратные составляюшие работали исправно. Тестирование памяти позволяет исключить из рассмотрения часть возможных проблем с памятью сервера при поиске неисправностей.

При загрузке GRUB для тестирования оперативной памяти используйте Memtest86+. Для запуска тестирования памяти выполните действия:

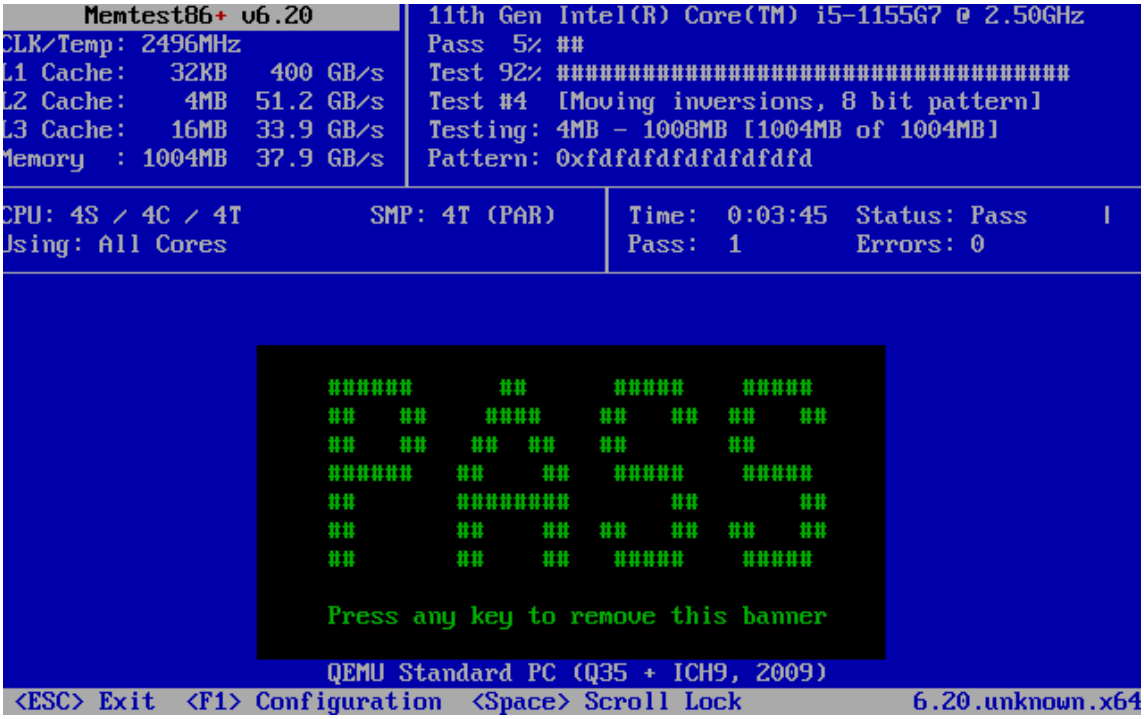
1. При загрузке сервера выберите **Memory test**:

2. Для начала тестов нажмите **Enter** или подождите 5 секунд до автоматического запуска тестирования:

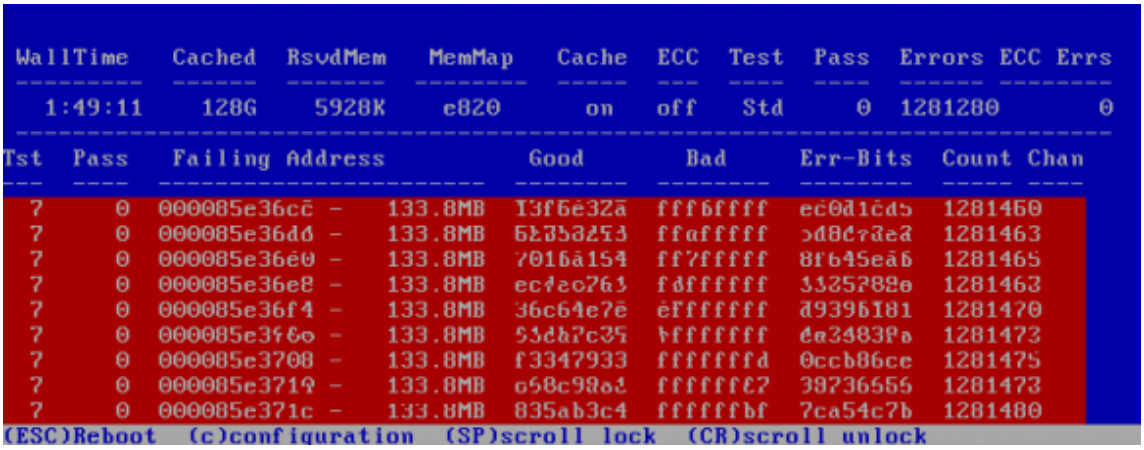


Подсказка: Для выбора режима диагностики **Fail-Safe Mode** нажмите **F1**.
Для выбора режима диагностики **Multi-Threading(SMP)** нажмите **F2**.

- Если появится запись **PASS**, тесты памяти пройдены успешно:



- При ошибке памяти появится запись вида:



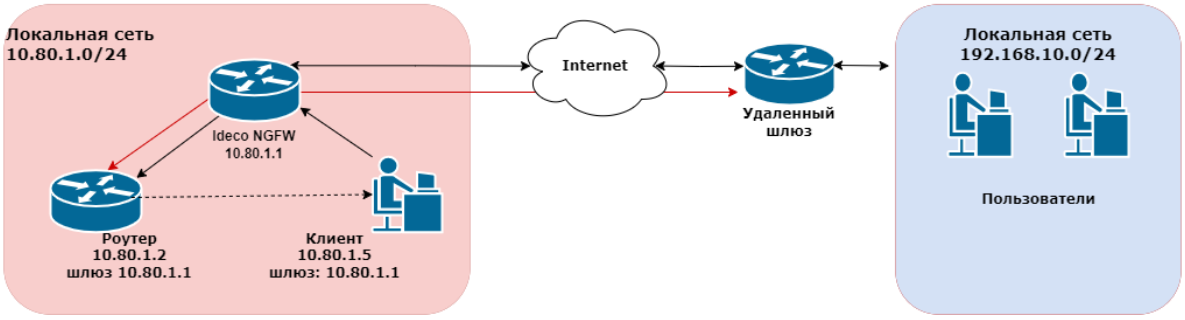
38.28 Как избавиться от асимметричной маршрутизации трафика

При попытке настроить доступ в удаленные сети через роутер в локальной сети может возникнуть асимметричная маршрутизация, препятствующая прохождению пакетов между двумя локальными сетями. В этой статье описаны случаи возникновения асимметричной маршрутизации и способы предотвращения.

Пример. В локальной сети NGFW используется роутер, устанавливающий связь с другими сетями. NGFW - шлюз по умолчанию для клиентов сети. Требуется настроить маршрутизацию на NGFW так, чтобы клиенты сети `10.80.1.0/24` получали доступ в удаленную сеть `192.168.10.0/24` и обратно через роутер.

38.28.1 Асимметричная маршрутизация при наличии роутера в локальной сети

Неправильная топология сети, способствующая асимметричной маршрутизации:

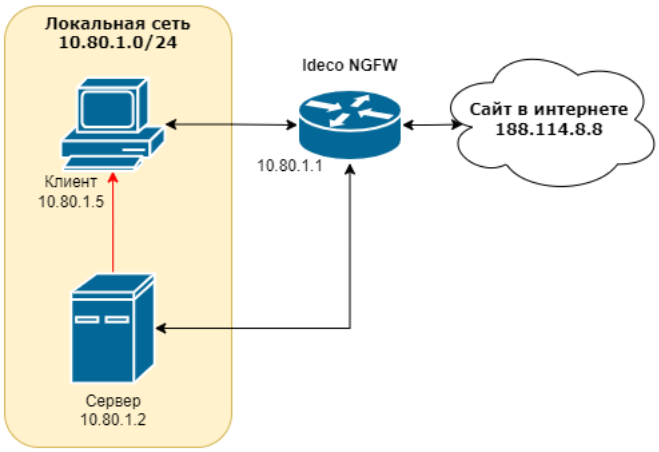


- `10.80.1.1` - шлюз для локальной сети `10.80.1.0/24`;
- `10.80.1.2` - роутер, имеющий доступ в удаленную сеть `192.168.10.0/24`;
- `10.80.1.5` - адрес хоста в локальной сети;
- **Красные стрелки** - двусторонняя связь роутера с удаленным шлюзом или роутером, обеспечивающая доступ к удаленной сети `192.168.10.0/24` (туннель к шлюзу, маршрут до роутера в соседнюю сеть предприятия);
- **Черные стрелки** - трафик от хостов локальной сети `10.80.1.0/24` до удаленной сети `192.168.10.0/24` через шлюз NGFW (`10.80.1.1`) и роутер (`10.80.1.2`);
- **Пунктирная стрелка** - трафик, который роутер возвращает хостам локальной сети в обход NGFW, поэтому хосты этот трафик обратно не принимают.

Предупреждение: Часть трафика от клиентов до роутера идет через шлюз, а часть - непосредственно от роутера до абонентов сети. Разная маршрутизация на разных участках делает прохождение пакетов между двумя локальными сетями невозможной.

38.28.2 Асимметричная маршрутизация при публикации сайтов через DNAT

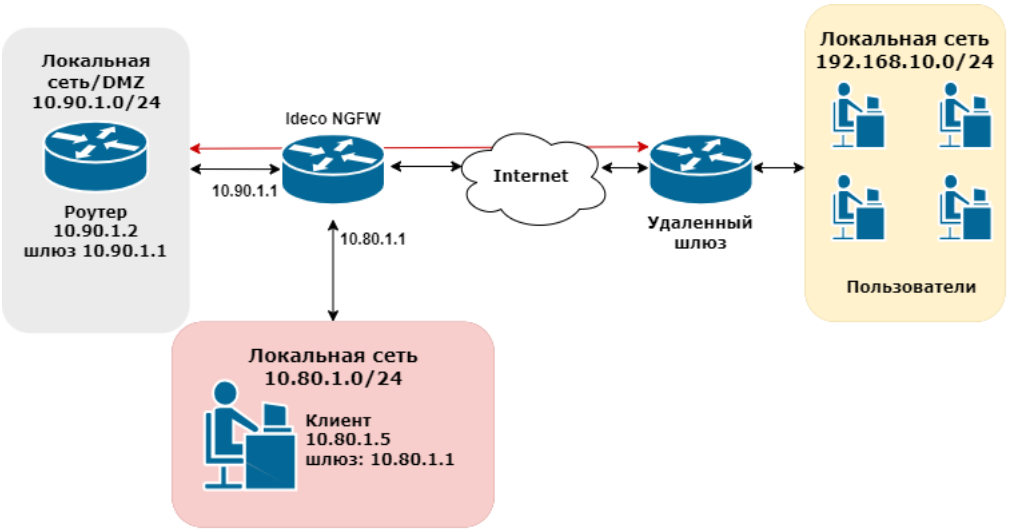
Асимметричная маршрутизация также возникает, когда в одной локальной сети находится хост и сервер, на котором расположен опубликованный при помощи DNAT-правила ресурс:



- `10.80.1.1` - адрес Ideco NGFW в локальной сети;
- `10.80.1.2` - адрес сервера в локальной сети;
- `10.80.1.5` - адрес хоста в локальной сети;
- `188.114.8.8` - адрес сайта в интернете;
- **Красная стрелка** - ответ напрямую от сервера хосту в локальной сети.

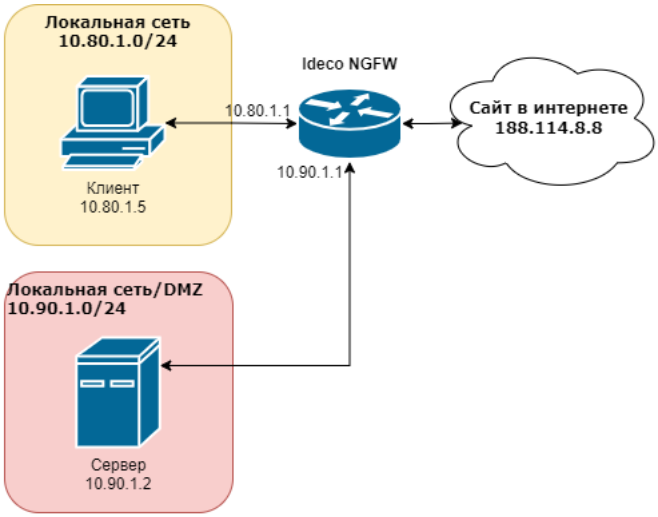
Когда хост `10.80.1.5` обращается на сайт по внешнему адресу `188.114.8.8` (например, в случае обращения по доменному имени, которое разрешено во внешнем IP), трафик проходит через NGFW. На NGFW срабатывает правило DNAT и перенаправляет трафик на сервер `10.80.1.2`, а сервер отвечает хосту, минуя NGFW.

38.28.3 Правильная топология сети:



Для правильной работы схемы потребуется:

1. Вынести роутер в отдельную локальную сеть (DMZ `10.90.1.0/24`), чтобы избежать асимметричной маршрутизации между роутером и клиентами локальной сети:



2. Настроить DMZ на NGFW, добавив на локальный интерфейс NGFW еще один IP-адрес (`10.90.1.0/24`), к локальной сети которого подключен роутер.

3. Настроить IP-адрес на роутере из адресного пространства новой сети `10.90.1.2`. Шлюзом указать дополнительный IP-адрес, настроенный на локальном интерфейсе NGFW из этой сети `10.90.1.1`.

Физически роутер и клиенты локальной сети будут находиться в одном сегменте сети, имея при этом разную IP-адресацию и шлюзы. Как правило, схемы с виртуальной изоляцией сетей на основе одного физического интерфейса достаточно.

Подсказка: Для физической изоляции локальной сети клиентов NGFW и роутера:

- Подключите к Ideco NGFW дополнительную сетевую карту;
- Настройте на сетевой карте дополнительный локальный интерфейс и отдельную IP-адресацию в этой сети;
- Укажите в качестве шлюза для роутера адрес, настроенный на дополнительном локальном интерфейсе.

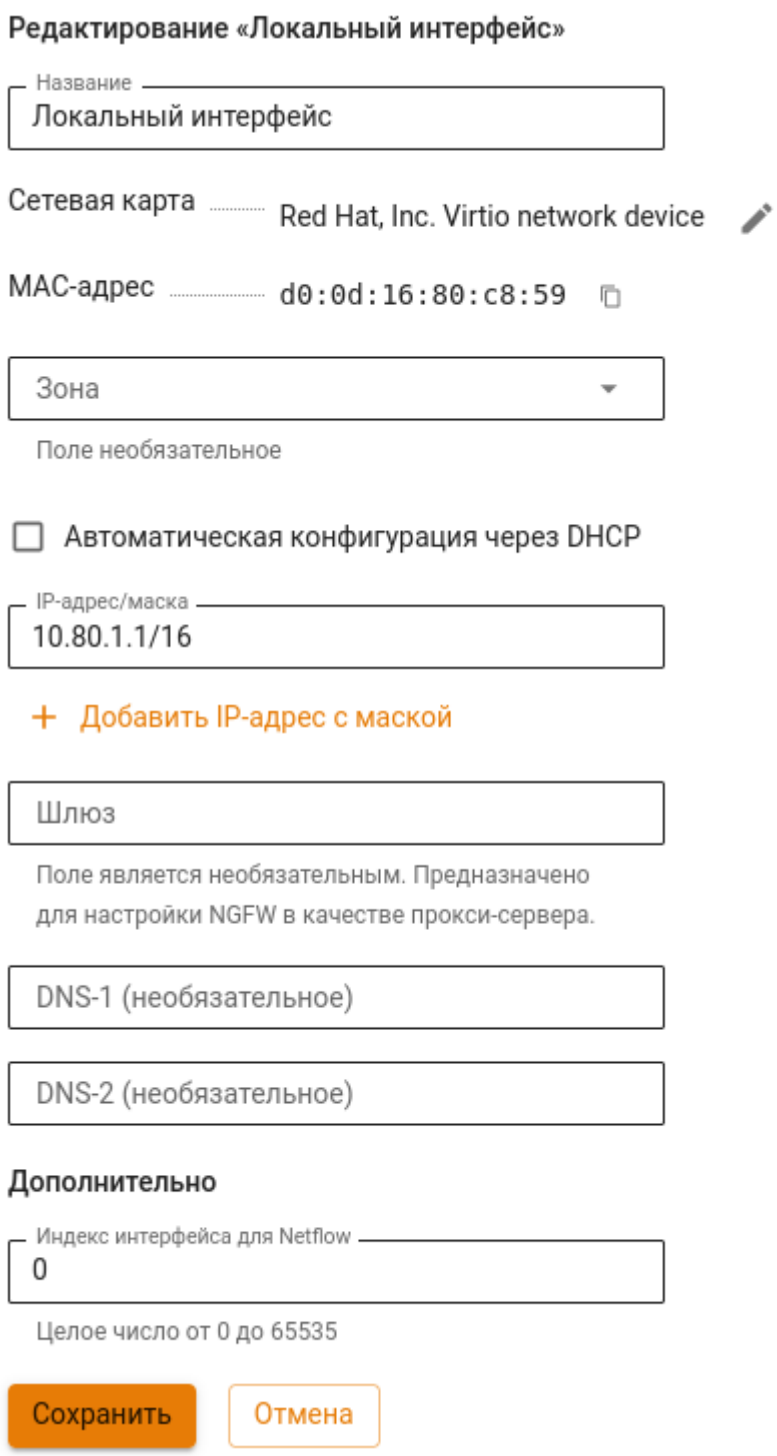
Физически роутер будет находиться в сегменте дополнительной сетевой карты.

Настройка NGFW:

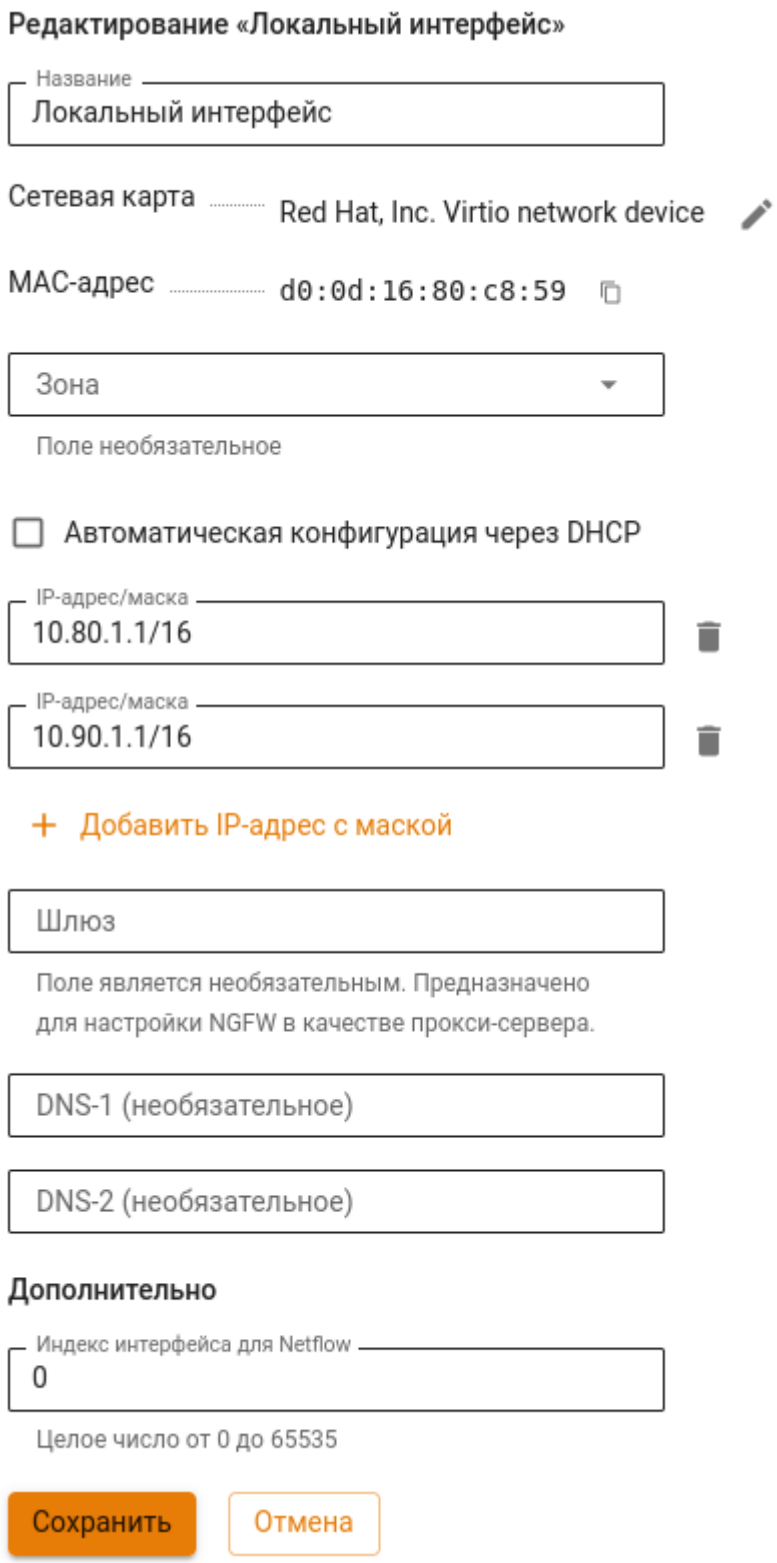
Для настройки нескольких виртуальных локальных сетей на одном физическом локальном интерфейсе NGFW перейдите в раздел **Сервисы -> Сетевые интерфейсы** и выполните действия:

1. Откройте в режиме редактирования **Локальный интерфейс**, к которому подключены пользователи нужной вам локальной сети (`10.80.1.1/24`), нажав на напротив его названия.

2. Если IP-адрес вашей локальной сети был автоматически сконфигурирован через DHCP, отключите опцию и введите его вручную:



3. Нажмите на + Добавить IP-адрес с маской и введите IP-адрес DMZ для изоляции роутера:

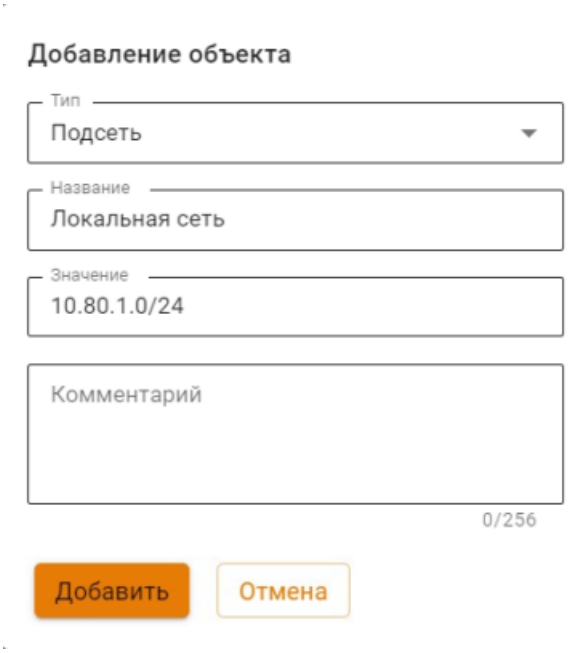


4. Нажмите **Сохранить**.

После изоляции роутера в DMZ нужно указать маршрут на NGFW до удаленной сети. Для этого перейдите в **Сервисы -> Маршрутизация** и выполните действия:

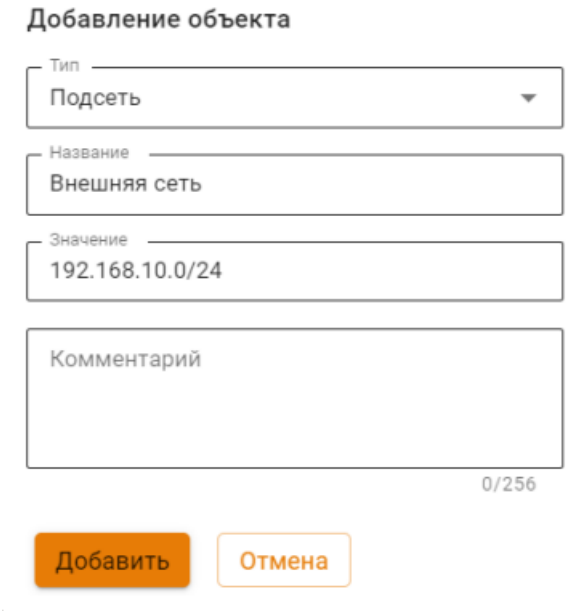
1. Перейдите на вкладку **Внешних сетей** нажмите кнопку **Добавить**.

2. В поле **Адрес источника** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес вашей локальной сети (`10.80.1.0/24`):



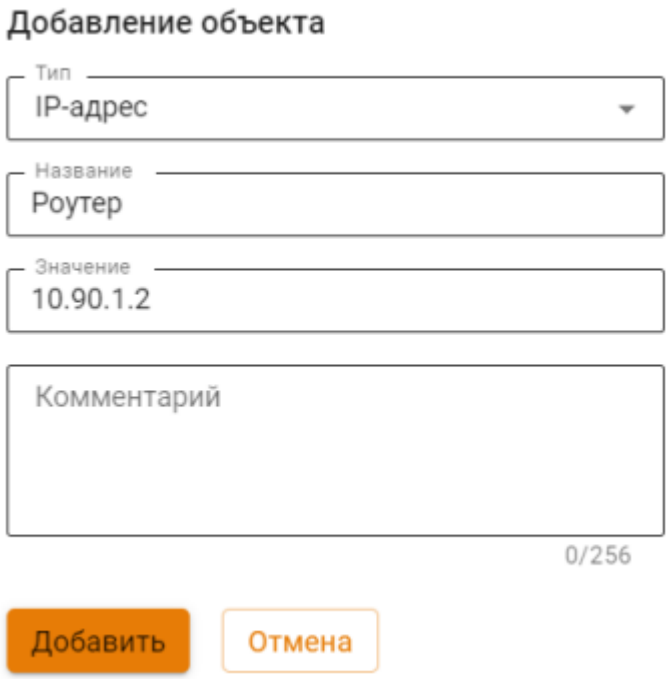
Выберите в качестве источника только что созданный объект.

3. В поле **Адрес назначения** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес внешней сети (`192.168.10.0/24`), в которую нужно настроить доступ:

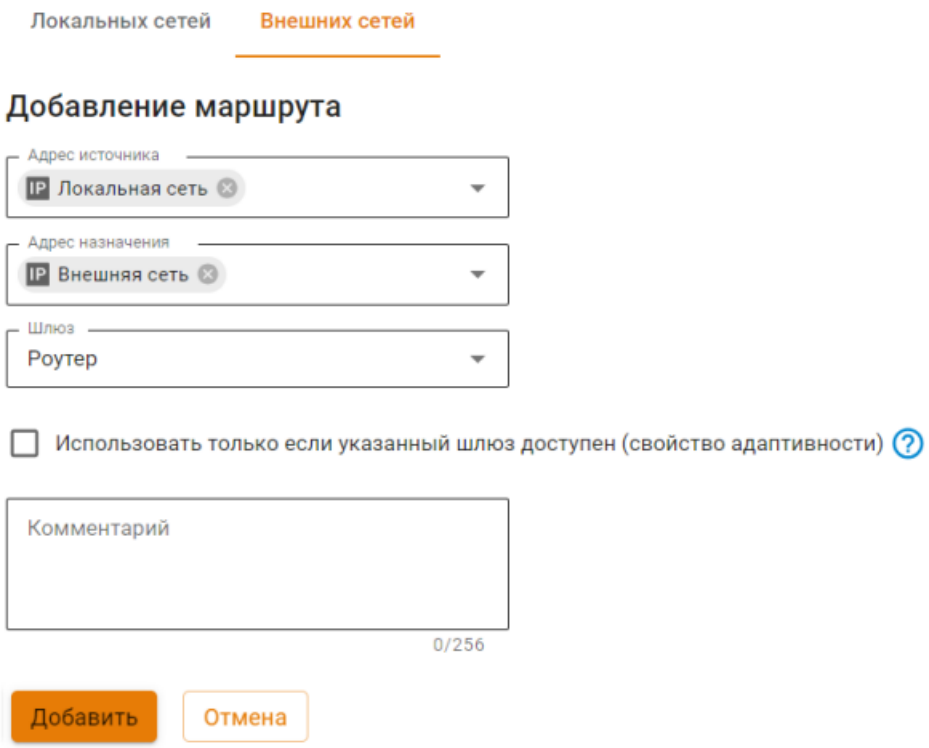


Выберите в качестве назначения только что созданный объект.

4. В поле **Шлюз** нажмите **Добавить объект**, выберите тип **IP-адрес** и введите адрес роутера в DMZ (`10.90.1.2`):



5. Сохраните маршрут вида:



Теперь трафик между сетями NGFW (`10.80.1.0/24` и `192.168.10.0/24`) во всех направлениях будет направляться через NGFW и роутер.

Настройка клиентских машин:

Хосты сетей, которые теперь обслуживает NGFW (`10.80.1.0/24` и `10.90.1.0/24`), физически включены в один Ethernet-сегмент. Чтобы шлюзом и DNS-сервером для хостов этих сетей был соответствующий адрес на локальном интерфейсе NGFW, укажите:

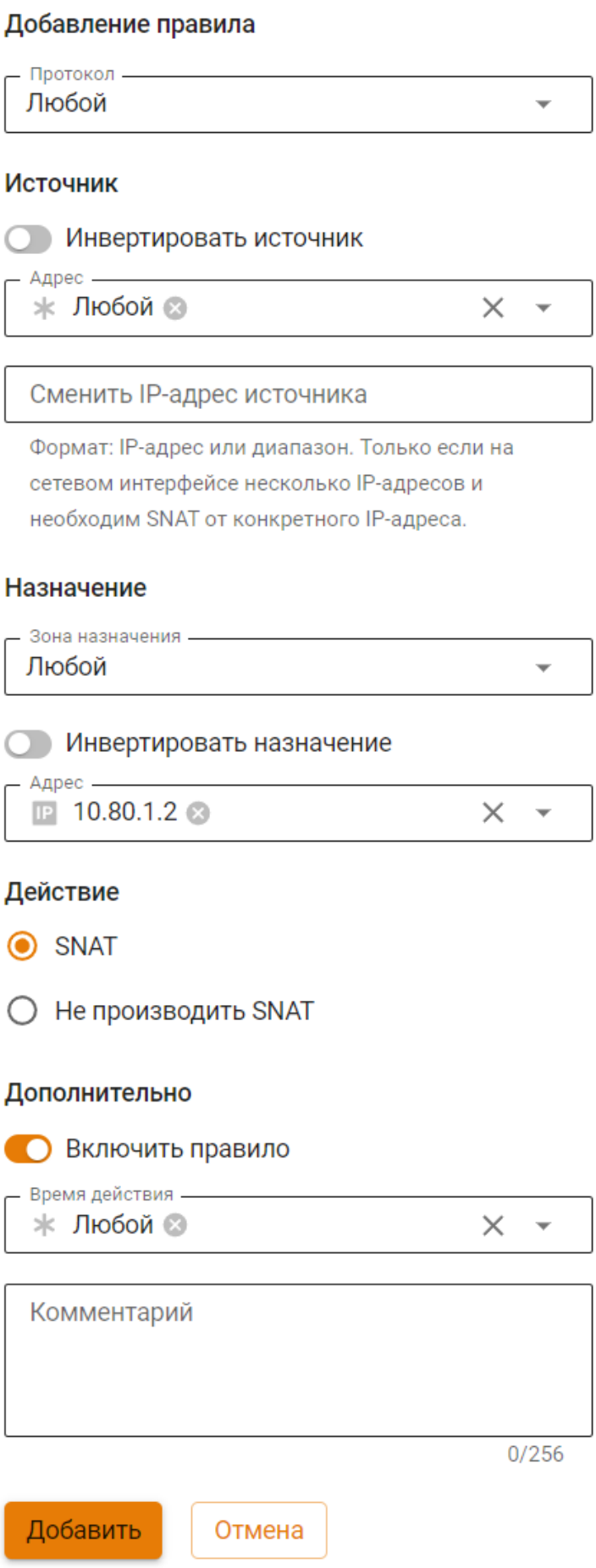
1. Для хостов из подсети `10.80.1.0/24` значение шлюза и DNS-сервера - `10.80.1.1`.

2. Для хостов из подсети `10.90.1.0/24` значение шлюза и DNS-сервера - `10.90.1.1`.

Предупреждение: Если по какой-то причине изолировать сервер в DMZ невозможно, создайте на NGFW специальное SNAT-правило.

Создание на NGFW SNAT-правила для избежания асимметричной маршрутизации:

Чтобы сервер `10.80.1.2` не отвечал напрямую на `10.80.1.5`, а посылал ответ на NGFW `10.80.1.1`, нужно в разделе **Правила трафика -> Файрвол -> SNAT** создать и включить правило вида:


Добавление правила
Протокол
Любой
Источник
Инвертировать источник
Адрес
Любой
Сменить IP-адрес источника
Формат: IP-адрес или диапазон. Только если на сетевом интерфейсе несколько IP-адресов и необходим SNAT от конкретного IP-адреса.
Назначение
Зона назначения
Любой
Инвертировать назначение
Адрес
IP
10.80.1.2
Действие
SNAT
Не производить SNAT
Дополнительно
Включить правило
Время действия
Любой
Комментарий
0/256
Добавить
Отмена

Заполните поля:

- Назначение - `10.80.1.2`;
- Зона назначения - Локальные интерфейсы.

В этом случае трафик хоста `10.80.1.5` на внешний адрес сайта `188.114.8.8` будет перенаправлен на адрес сервера `10.80.1.2` правилом DNAT. При этом созданное правило SNAT заменит адрес источника `10.80.1.5` на адрес NGFW - пакет приобретет вид: `scr 10.80.1.1 dst 10.80.1.2`. Ответ от сервера также пройдет через NGFW - пакет `scr 10.80.1.2 dst 10.80.1.1`.

38.29 Что делать если ваш IP попал в черные списки DNSBL

Если используется белый статический IP-адрес, то попадание IP-адреса в черные списки может означать, что в сети зафиксирована бот-активность, участие в DDoS-атаках либо рассылка спама.

Наличие в черных списках динамического IP-адреса из «домашних» диапазонов IP-адресов провайдеров в целом нормальное явление, т. к. вредоносная активность в таком случае может исходить не из вашей сети.

38.29.1 Порядок действий при попадании в черный список

1. Узнайте причину попадания в DNSBL-список. Часто сервис называет конкретный вирус или сетевой червь и его особенности - используемые порты, протоколы. Выполните рекомендации сервиса.

2. Активируйте систему предотвращения вторжений на шлюзе. Проанализируйте логи, наличие обращений к командным центрам ботнетов.

3. Проверьте все компьютеры сети антивирусом. Убедитесь, что антивирусная защита активирована, базы обновлены (как правило, вирусы мешают обновлению баз или работе антивирусного ПО).

4. После лечения зараженных компьютеров отправьте в DNSBL-сервис сообщение с просьбой исключить IP из черного списка.

38.29.2 Ideco NGFW

Наше решение обладает всей функциональностью, обеспечивающей максимальную защиту от спам-ботов, ботнет-клиентов и предотвращение вирусной активности в сети.

До 22 пользователей - решение предоставляется бесплатно. Для 10000 пользователей доступна 40-дневная пробная версия.

Скачать Ideco NGFW

38.30 Как восстановить доступ к Ideco NGFW

38.30.1 Основное

Для этого нужно выполнить следующие действия:

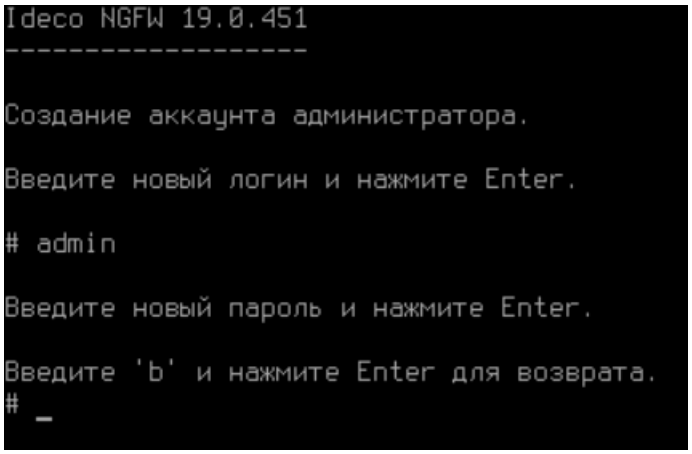
1. Перезагрузите сервер. При появлении меню загрузчика GRUB с выбором ядра Linux для загрузки системы нажмите англоязычную клавишу **E** на клавиатуре.

2. Откроется окно параметров ядра с возможностью редактирования. Переместите указатель стрелками на клавиатуре вправо до слова `quiet` и допишите текст `p=1`:

Строка с параметрами отображается внизу экрана.

3. Нажмите `Enter`.

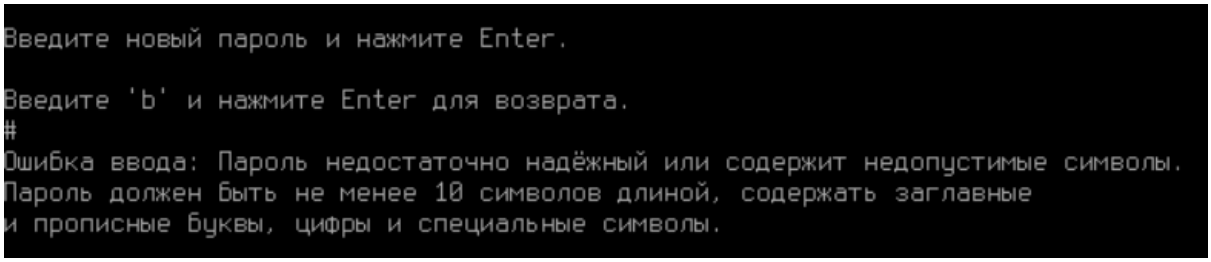
4. После повторной загрузки системы появится окно создания аккаунта администратора. Задайте новый логин и пароль администратора:



Требования к созданию пароля администратора:

- Минимальная длина пароля - 10 символов;
- Строчные и заглавные латинские символы;
- Цифры;
- Специальные символы (! # $ % & „ * + и т. д.).

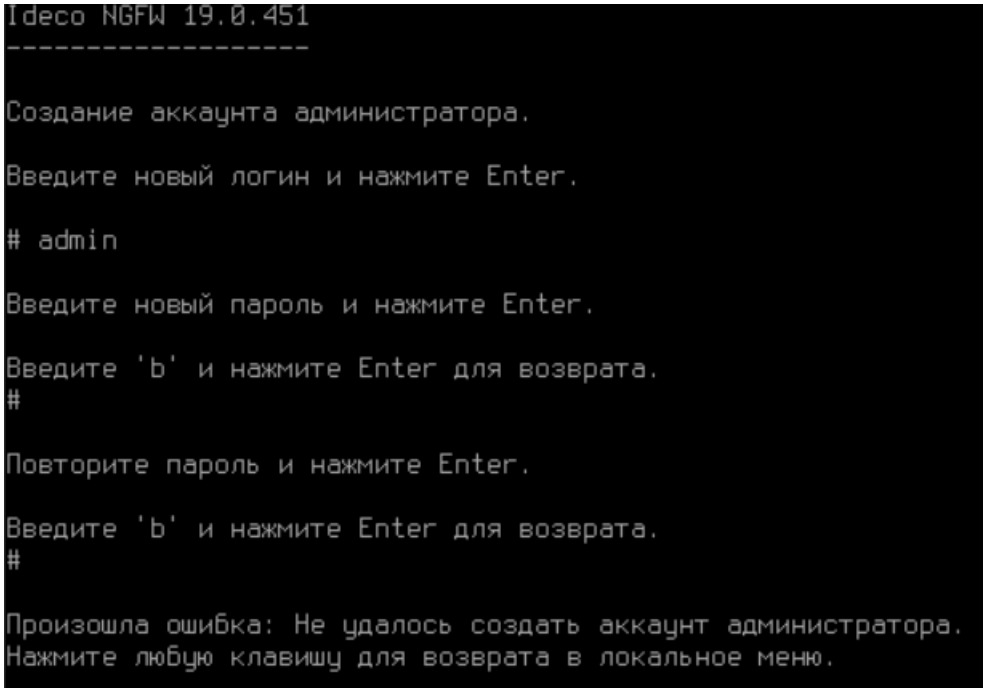
Если пароль не будет соответствовать требованиям политики безопасности, то появится ошибка:



Необходимо ввести новый пароль, учитывая требования к созданию паролей.

Предупреждение: Если при создании нового логина администратора он будет совпадать с предыдущим логином, то будет выведена ошибка. Создайте имя администратора, отличное от предыдущего.

Не используйте Numpad при введении нового пароля, поскольку в будущем это может привести к проблемам при авторизации администратора.



38.31 Как восстановиться на прошлую версию после обновления Ideco NGFW

38.31.1 Основное

Рекомендуем использовать эту возможность, если после обновления Ideco NGFW работает некорректно.

Подсказка: Возможность восстановиться на предыдущую версию после обновления Ideco NGFW доступна с 12.0.

При обновлении NGFW на версию 12.0 и выше вся информация версии, с которой обновляетесь, сохранится на диске NGFW.

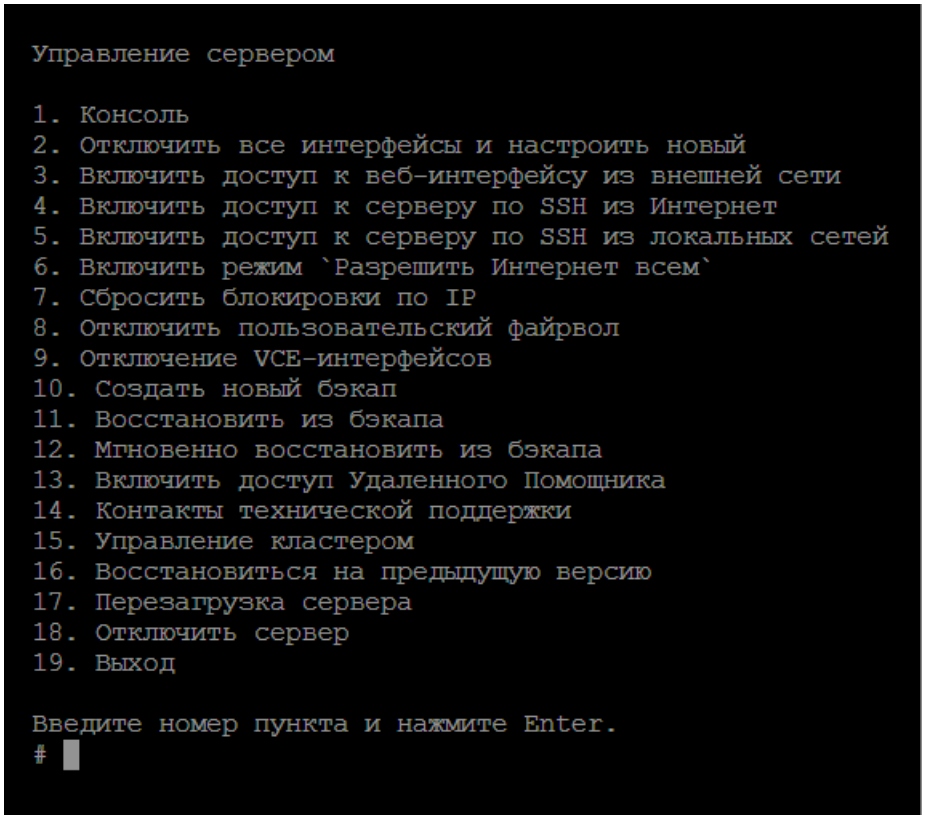
При восстановлении на предыдущую версию данные перенесены не будут. Сохраните бэкап на внешнем носителе. Информация о работе с API бэкапа описана в статье *Бэкапы и возврат к предыдущей версии*.

Для восстановления на предыдущую версию выполните действия:

1. Перейдите в локальное меню Ideco NGFW.

2. Введите логин и пароль администратора.

3. Укажите номер пункта 16 и нажмите **Enter**:

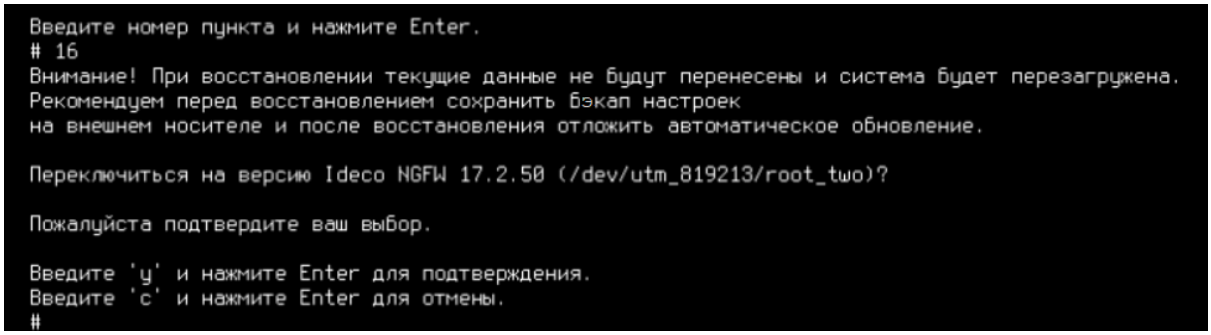


Появится окно с предупреждением и описанием версии, на которую произойдет переключение.

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

---

3. Подтвердите выбор, введя **y** и нажав **Enter**:



4. После перезагрузки Ideco NGFW переключится на предыдущую версию.

38.32 Проверка настроек фильтрации с помощью security ideco

При правильной настройке общий уровень защиты должен показывать зеленый цвет. Если это не так, проверьте с помощью этой статьи настройки **Контент-фильтра** и других служб фильтрации трафика.

38.32.1 Предварительная проверка

Перейдите в веб-интерфейс Ideco NGFW и убедитесь, что все описанные ниже службы включены и функционируют корректно.

Раздел Правила трафика

- *Контент-фильтр*;
- *Контроль приложений*;
- *Антивирус* (антивирус Касперского);
- *Предотвращение вторжений*.

Эти службы полноценно работают только при активной подписке на обновления Ideco NGFW. Для проверки статуса вашей лицензии и модулей, которые в нее входят, откройте раздел **Управление сервисом -> Лицензия**.

Раздел Сервисы

1. Откройте раздел **Сервисы -> Прокси -> Исключения**.

2. Убедитесь, что в типе **Сеть источника** нет сети, к которой относится IP-адрес вашего компьютера при входе на сайт security.ideco.ru.

3. В типе **Сеть назначения**:

- Не должно быть неизвестных сетей;
- Не используйте сеть с маской, которая включает в себя большое количество адресов.

Подсказка: Если ресурсы исключены в **Прокси-сервере**, они также не будут проверяться **Контент-фильтром**. Подробная информация о работе с исключениями представлена в *статье*.

38.32.2 Проверка настроек служб

Контент-фильтр

Категории сайтов, которые запрещают правила Контент-фильтра:

- Анонимайзеры;
- Ботнеты;
- Фишинг/мошенничество;
- Казино, лотереи, тотализаторы;
- Порнография;
- Список Минюста;
- Астрология и гороскопы;

- Знакомства;
- Компьютерные игры;
- Мультфильмы, аниме и комиксы;
- Развлекательные новости и сайты про знаменитостей;
- Онлайн-реклама и баннеры;
- Торрент-трекеры.

Чтобы антивирус проверял HTTPS-трафик, необходимо создать правило расшифровки всего HTTPS-трафика для пользователей. Это правило будет применяться, в том числе к тем, кто проверяет настройки на сайте security.ideco.ru.

Проверьте, что **Контент-фильтр** работает. Для этого перейдите с компьютера пользователя на сайт: `sex.com`. Если фильтр работает, то отобразится страница блокировки.

Контроль приложений

Для защиты от «пожирателей времени и трафика»:

1. В разделе **Профили безопасности -> Контроль приложений** создайте профиль, который будет блокировать доступ к протоколам:

- Bittorrent;
- Steam;
- Worldofwarcraft;
- Mining.

2. В разделе **Правила трафика -> Файрвол** в таблицу **FORWARD** добавьте и включите правило с профилем, созданным в пункте 1.

3. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичное правило INPUT.

Предотвращение вторжений

1. В разделе **Профили безопасности -> Предотвращение вторжений** создайте профиль, который будет блокировать следующие группы сигнатур:

- Анонимайзеры;
- Пулы криптомайнеров.

2. В разделе **Правила трафика -> Файрвол** в таблицу **FORWARD** добавьте и включите правило с профилем, созданным в пункте 1.

3. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичное правило INPUT.

Предупреждение: С 18 версии NGFW правила Файрвола, которые блокировали трафик за счет перехвата DNS в предыдущих версиях, не смогут его блокировать. Чтобы это исправить, создайте правила с профилями IPS и DPI в разделе **Правила трафика -> Файрвол -> INPUT**.

Подсказка: После изменений правил проведите повторное тестирование с помощью security.ideco.ru.

38.33 Выбор аппаратной платформы для Ideco NGFW

38.33.1 Сведения о программной платформе

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 40 и содержит ядро Linux с набором драйверов от этой ОС с небольшими изменениями с нашей стороны. Таким образом, Ideco NGFW можно установить на большую часть оборудования, поддерживающего Fedora 40.

38.33.2 Общие рекомендации по чипсетам и производителям

- Рекомендуем чипсеты и контроллеры фирм Intel и Broadcom. Особенно сетевые карты и наборы логики, используемые в материнских платах;
- Не рекомендуем использовать встроенные сетевые карты, особенно интерфейсы на бюджетных/редких/устаревших/noname чипсетах. NGFW работает с сетью, и зачастую бюджетные сетевые адаптеры для десктопов не справляются с задачами шлюза;
- Не рекомендуем использовать RAID-контроллеры в работе сетевого шлюза. Встроенные в материнские платы программные и полуаппаратные RAID-контроллеры официально не поддерживаются нашим продуктом;
- Материнские платы могут использоваться как серверные, так и десктопные. Желательно использование процессоров Intel;
- Бюджетные, энергоэкономичные платформы для десктопов, полутонких клиентов на базе Intel Atom не подходят для работы Ideco NGFW и не соответствуют минимальным *системным требованиям* продукта.

38.33.3 Подбор мощности аппаратной платформы

Количество ГГц процессора и объем ОЗУ сервера сильно зависят от нагрузки, возлагаемой на Ideco NGFW. При подсчете нагрузки нужно выделить три фактора:

- Количество одновременно авторизованных на NGFW пользователей;
- Задействованные компоненты NGFW (прокси с его сервисами, проверка трафика на спам/вирусы, обширность настройки модуля контентной фильтрации или файрвола);
- Система предотвращения вторжений - при высокоскоростном подключении к провайдеру эта служба может потребовать значительных ресурсов процессора и памяти. Рекомендуется использовать многоядерные процессоры (4 и более ядер с частотой более 3 ГГц) и от 16 ГБ оперативной памяти.

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

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

38.33.4 Дисковая подсистема

RAID-массивы не требуются при типичных схемах использования NGFW. Одного современного жесткого диска SATA от 200 ГБ хватает в большинстве конфигураций. В случае использования почтового сервера на Ideco NGFW требуется подключить отдельный винчестер для хранения почтовой корреспонденции. Рекомендуется использование SSD-дисков и устройств марки Micron.

38.34 Поддержка устаревших алгоритмов шифрования

38.34.1 Основное

Ideco NGFW основан на операционной системе Fedora. В Ideco NGFW используется Fedora 40. Подробнее об изменениях политики алгоритмов можно прочитать в статье.

Устаревшие алгоритмы, как (криптографическое) хеширование и шифрование, обычно имеют время жизни, по истечении которого они считаются либо слишком рискованными для использования, либо просто небезопасными.

Могут возникнуть неполадки, связанные с работой HTTPS, например, при пробросе OWA (веб-интерфейс для доступа к Microsoft Exchange). Столкнувшись с этим, выполните следующие действия для перехода в режим совместимости уровней политики шифрования:

1. Зайдите в консоль Ideco NGFW. Это можно сделать из локального меню, по ssh или через веб-интерфейс Ideco NGFW.

2. Введите в терминале команду `update-crypto-policies --set DEFAULT:FEDORA32`.

3. Перезагрузите Ideco NGFW.

> **Предупреждение:** Мы настоятельно не рекомендуем использовать данную настройку, так как при следующем обновлении Ideco NGFW настройки режима совместимости будут сброшены. В более новых версиях данная возможность будет отключена.

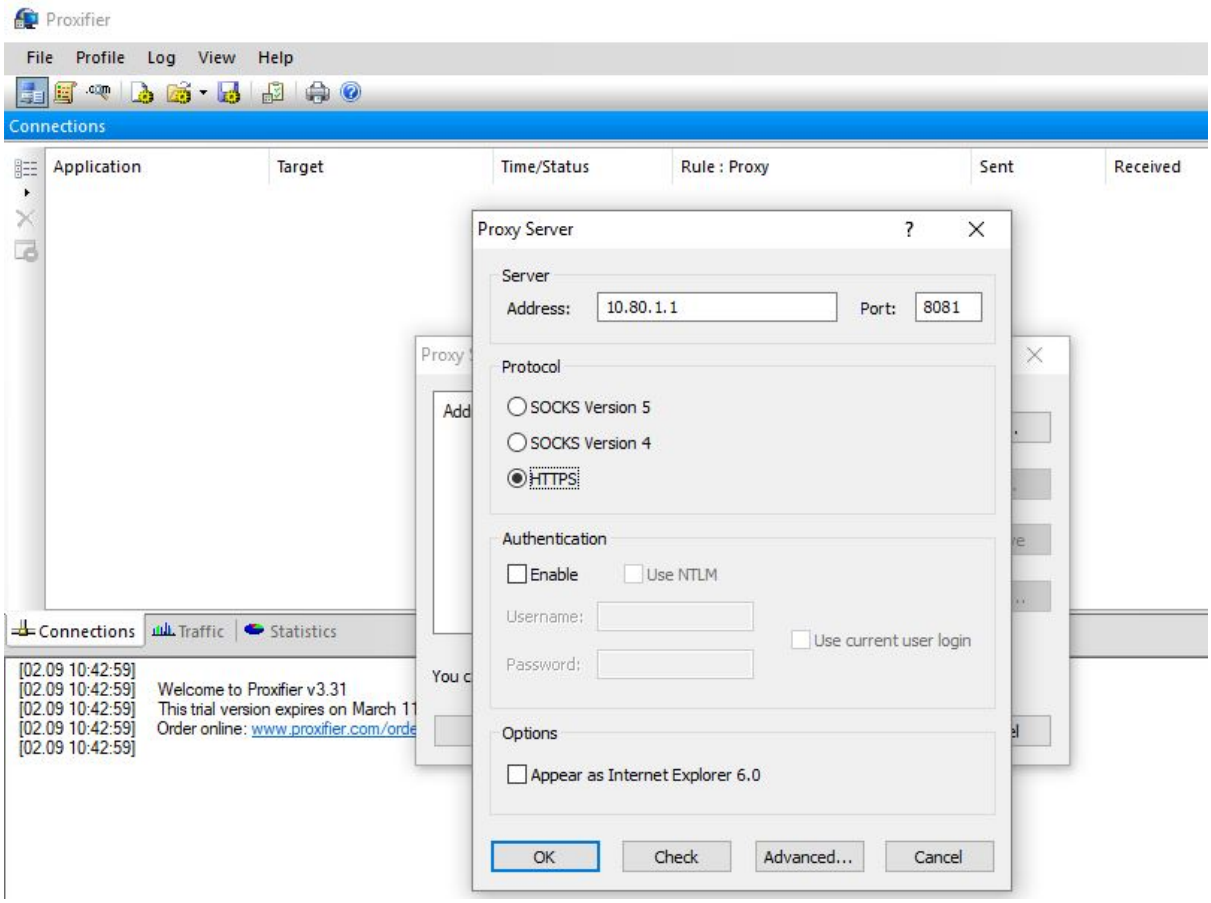
38.35 Настройка программы Proxifier для прямых подключений к прокси серверу

Скачать Proxifier можно с сайта разработчика.

38.35.1 Настройка

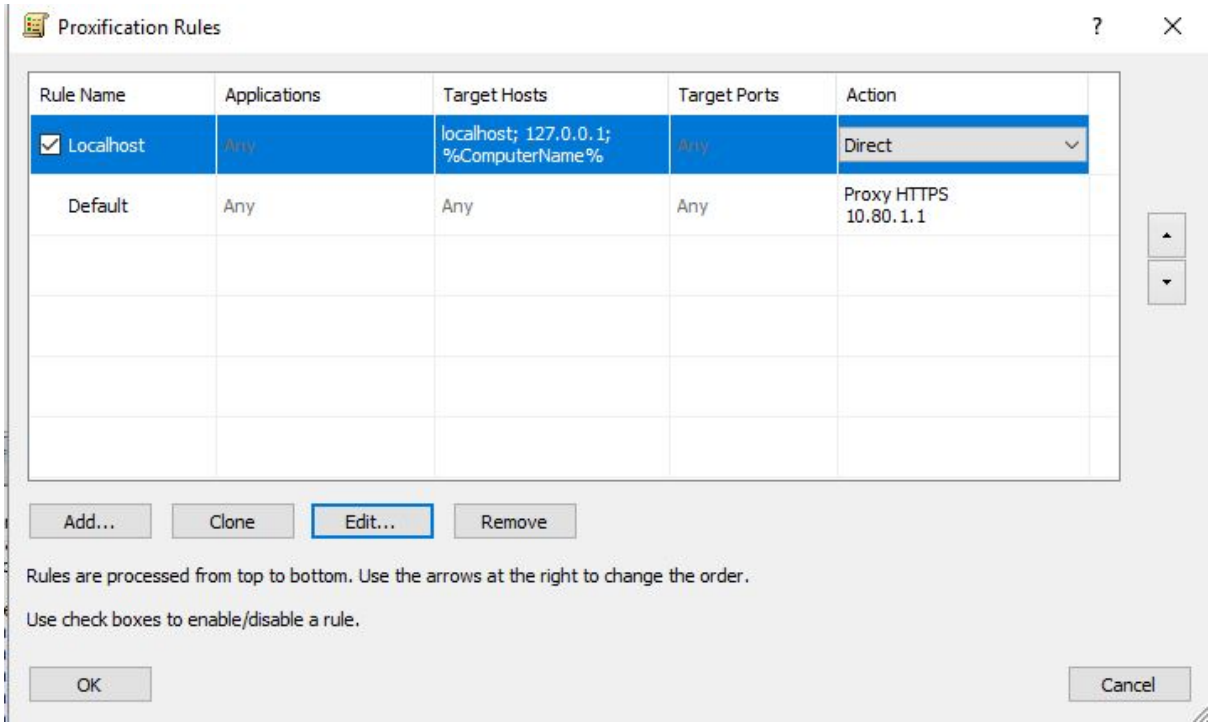
Выполните стандартные настройки браузера для прямых подключений к прокси-серверу, а затем настройте программу для перенаправления остального трафика на прокси-сервер.

Пропишите в настройках прокси-сервера в Proxyfier IP-адрес локального интерфейса Ideco NGFW и порт, указанный в настройке прокси для прямых подключений (см. документацию по *прокси-серверу*). Тип протокола: HTTPS. Настройки авторизации указывать необязательно.



После добавления прокси-сервера ответьте утвердительно на вопросы о создании правил перенаправления трафика на него.

Либо эти настройки можно отредактировать позже:



Настройка закончена, программы будут выходить в интернет через заданный прокси-сервер.

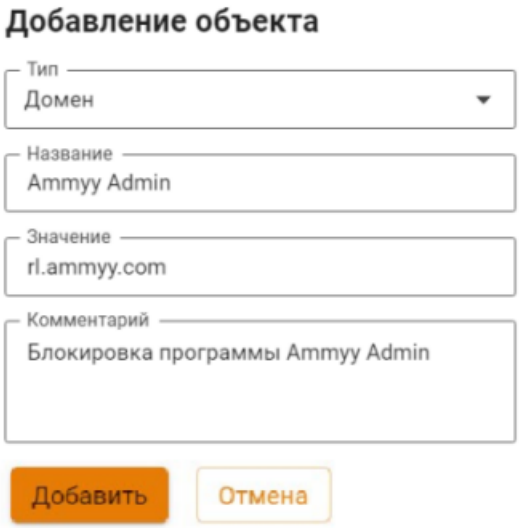
38.36 Блокировка популярных ресурсов

38.36.1 Основное

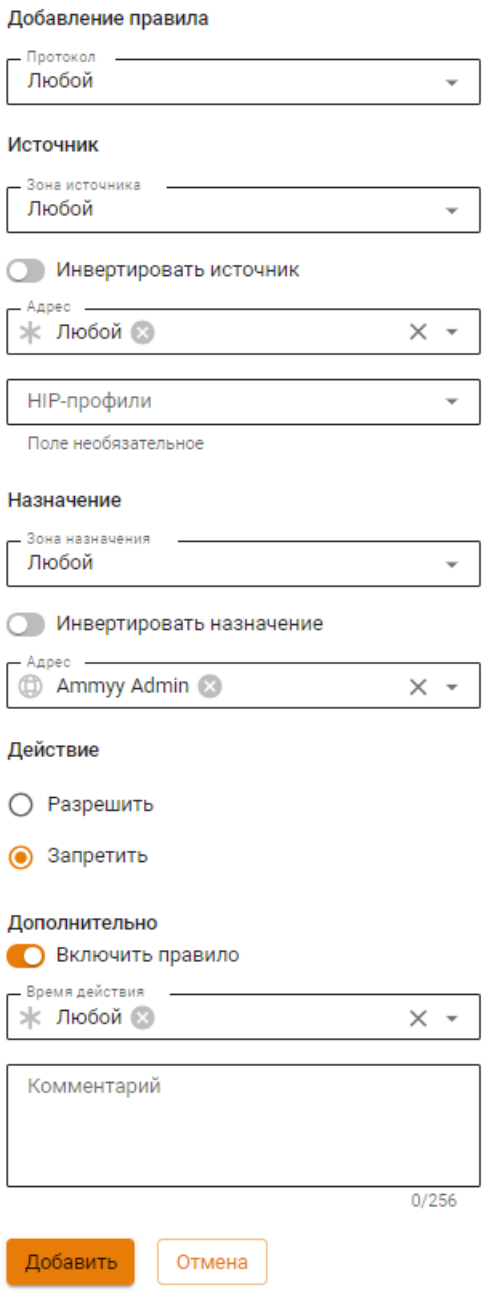
Блокировка Ammyy Admin:

Ammyy Admin - это система, удаленного доступа и администрирования. Чтобы заблокировать систему, выполните следующие настройки:

1. Откройте раздел **Правила трафика -> Объекты** и создайте объект типа **Домен** с доменным именем rl.ammyy.com:



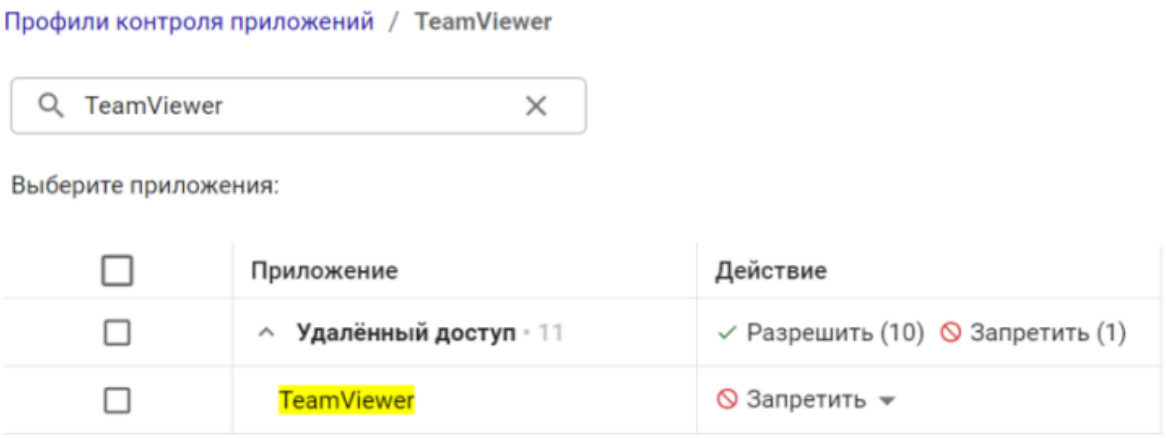
2. Перейдите на вкладку **Правила трафика -> Файрвол -> FORWARD**, создайте и включите правило запрета для нужных пользователей или групп. В поле **Назначение** выберите объект, созданный в пункте 1:



Блокировка TeamViewer:

TeamViewer - это программное обеспечение для удаленного доступа и управления компьютерами. Его можно заблокировать с помощью *Контроля приложений*.

1. Перейдите в раздел **Профили безопасности -> Контроль приложений**. Создайте новый профиль для TeamViewer с действием **Запретить**:

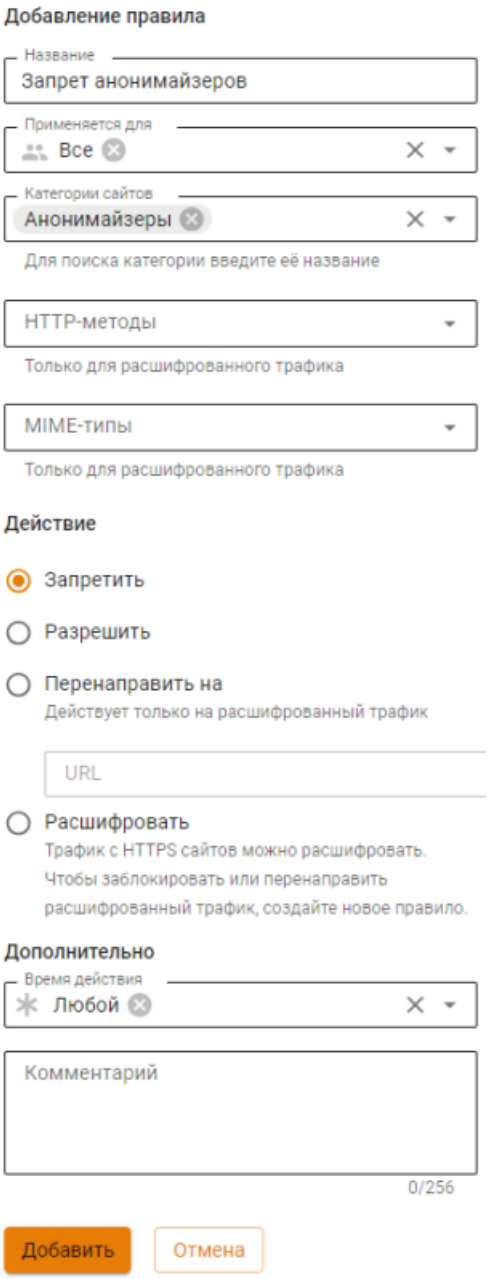


2. В разделе **Правила трафика -> Файрвол** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

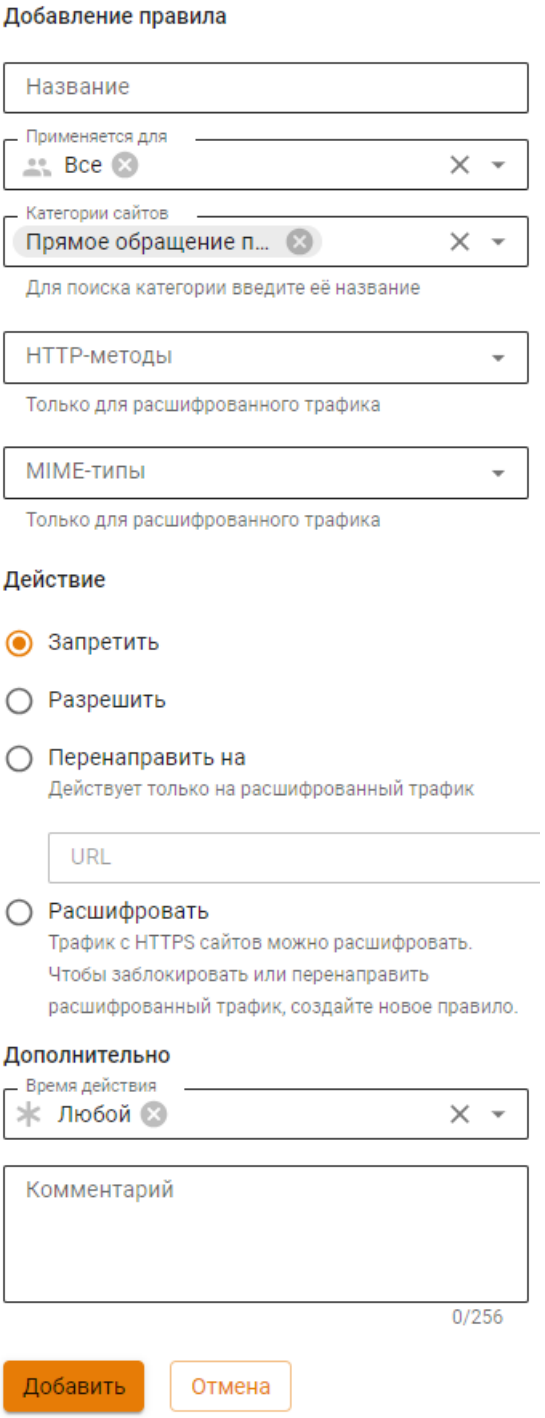
Блокировка анонимайзеров:

Заблокировать анонимайзеры можно в разделе **Правила трафика** тремя способами:

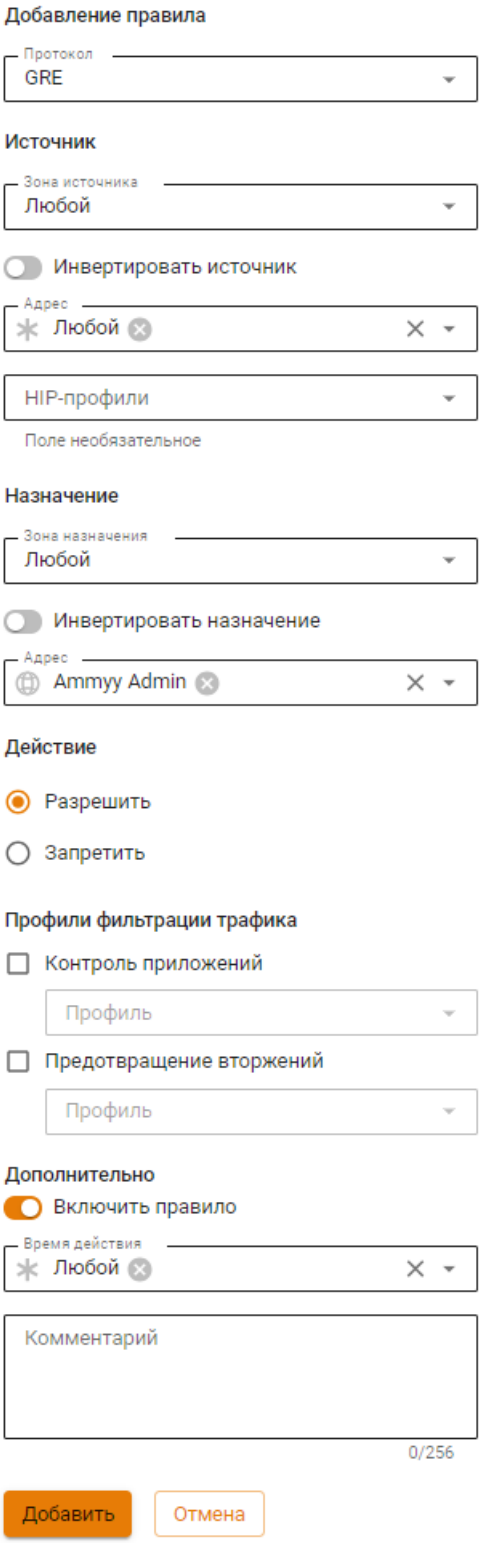
1. Анонимайзеры, работающие по протоколам HTTP(S), блокируются в разделе **Правила трафика -> *Контент-фильтр***. Для этого создайте правило, в котором запретите категорию сайтов **Анонимайзеры**:



2. Чтобы предотвратить обход **Контент-фильтра**, создайте правило, которое будет блокировать прямые обращения по IP-адресам в Контент-фильтре:



3. Для блокировки VPN-анонимайзеров, использующих протокол PPTP, достаточно заблокировать протокол GRE в правилах ***Файрвола***:

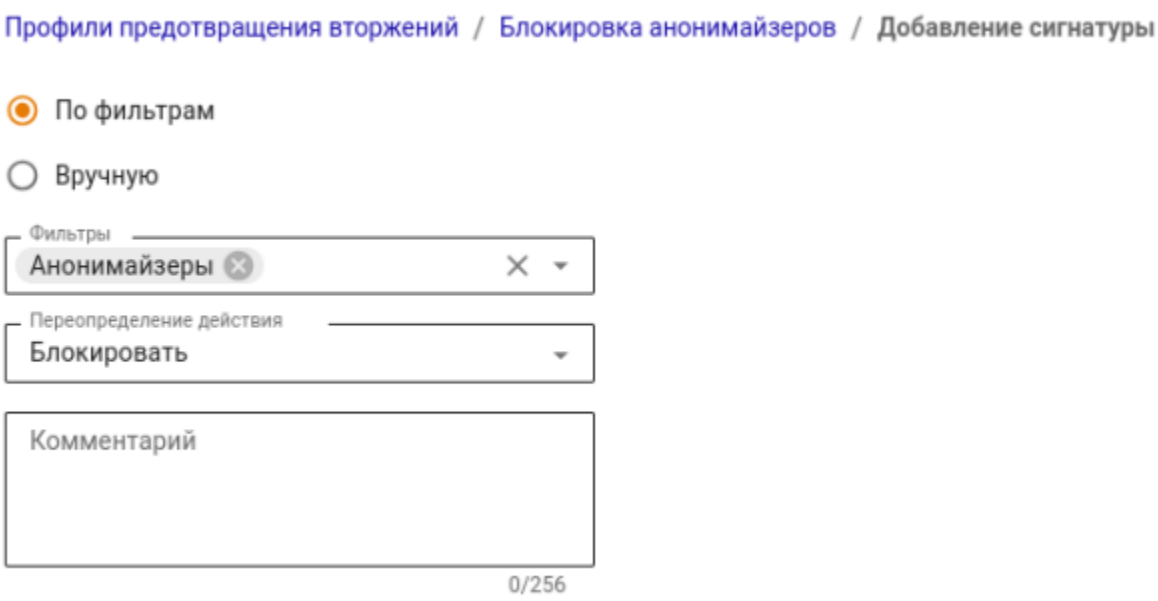


Блокировка Opera.Turbo, Opera VPN, Yandex.Turbo, friGate, Anonymox:

Чтобы заблокировать функции браузеров, которые используются для обхода контентной фильтрации, воспользуйтесь модулем *Предотвращение вторжений*.

1. Перейдите в раздел **Профили безопасности -> Предотвращение вторжений**. Создайте новый профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило, блокирующее группу сигнатур **Анонимайзеры**:



3. Нажмите **Добавить**.

4. В разделе **Правила трафика -> Файрвол** добавьте и включите разрешающее правило с профилем, созданным ранее.

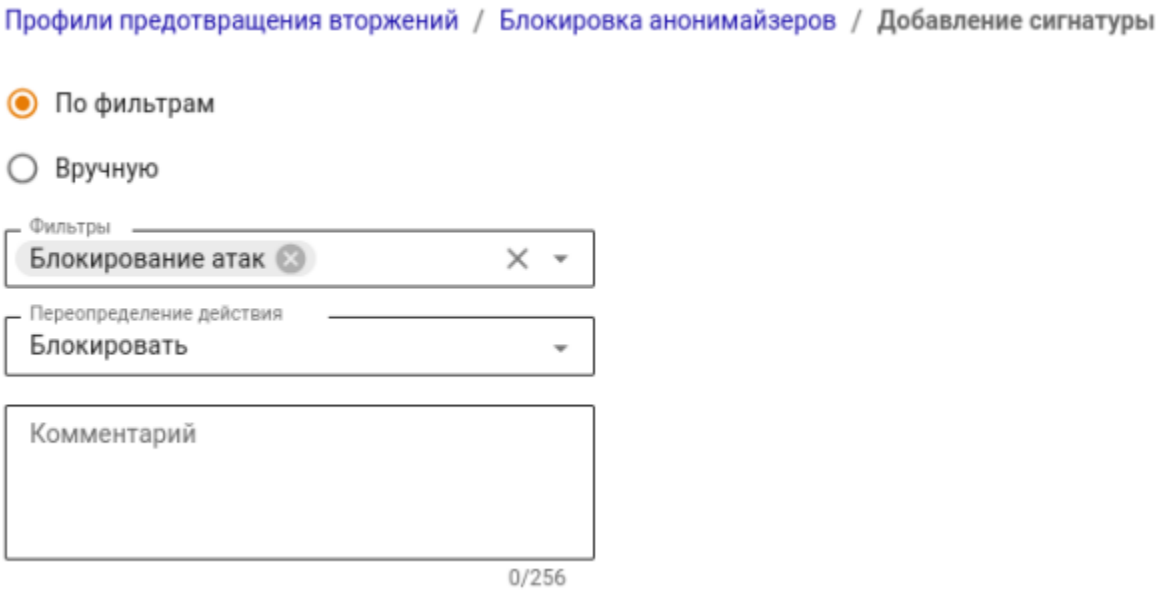
Блокировка Tor:

Tor - специально разработанное программное обеспечение и среда прокси-серверов, предназначенная для обхода различного рода блокировок, поэтому полностью заблокировать его сейчас невозможно.

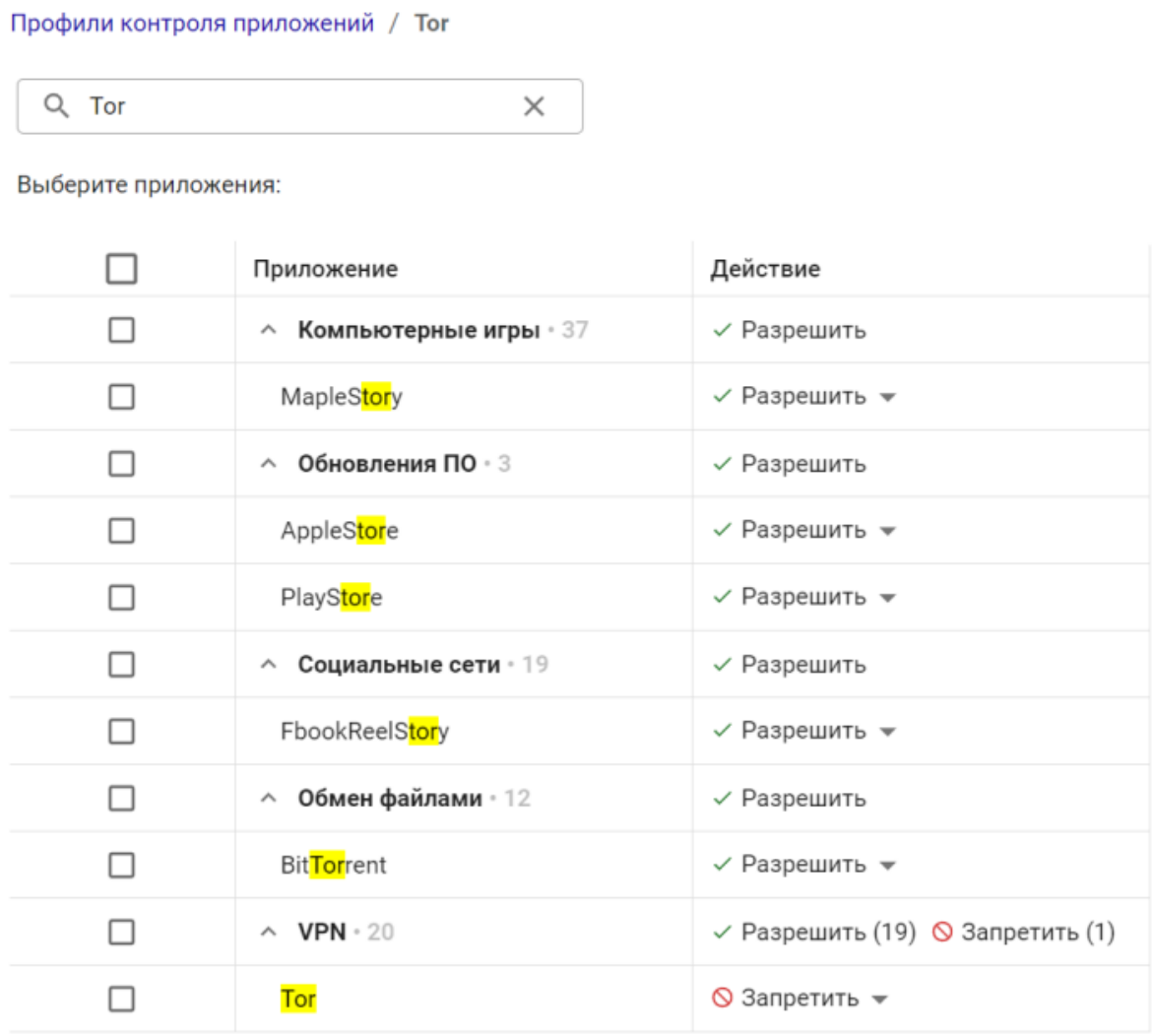
Для противодействия использованию сети Tor, а также для журналирования попыток подключения к ней и ее использования выполните следующие настройки:

1. В разделе **Профили безопасности ->** ***Предотвращение вторжений*** создайте профиль.

2. Нажмите **Добавить сигнатуру** и создайте правило для группы сигнатур **Блокирование атак**:



3. В разделе **Профили безопасности ->** ***Контроль приложений*** добавьте профиль, запрещающий приложение Tor:



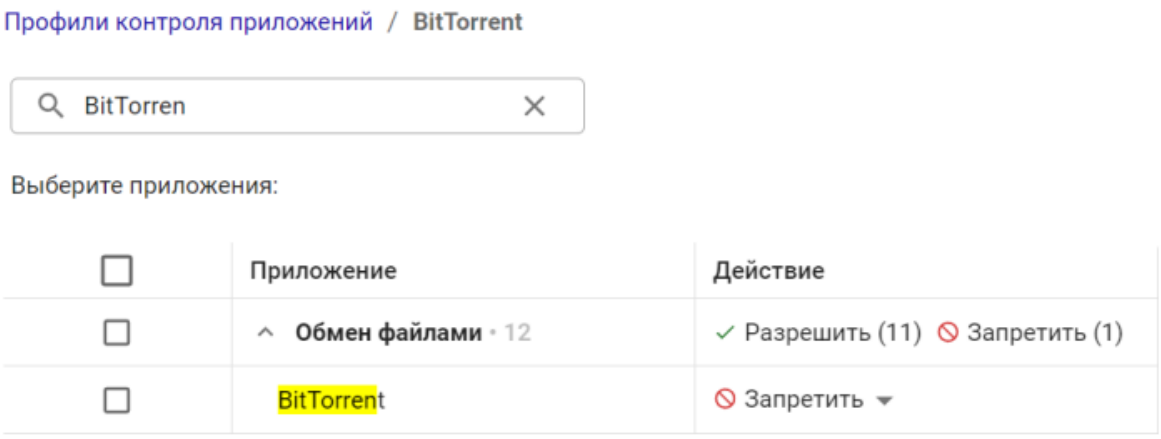
4. В разделе **Правила трафика -> Файрвол** добавьте и включите разрешающее правило с профилями **Предотвращения вторжений** и **Контроля приложений**, созданными ранее.

Блокировка торрентов:

BitTorrent - P2P-протокол, предназначенный для обмена файлами через интернет.

Для ограничения возможности использования торрентов выполните следующие настройки:

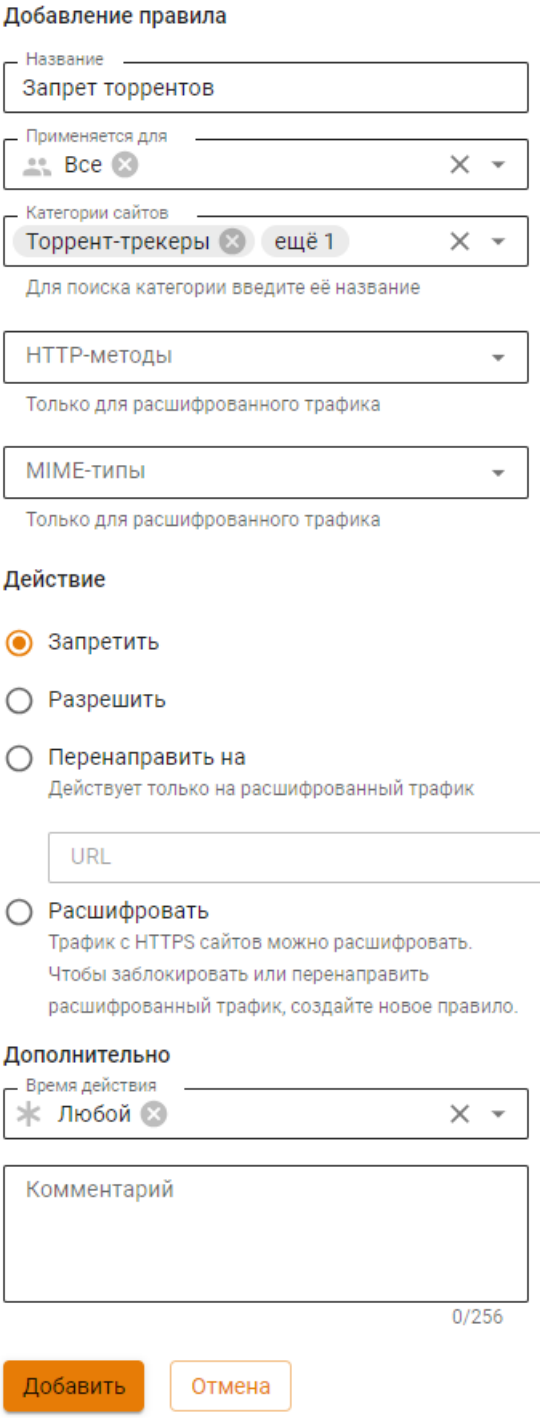
1. Запретите протокол BitTorrent с помощью правила в разделе **Профили безопасности ->** ***Контроль приложений***:



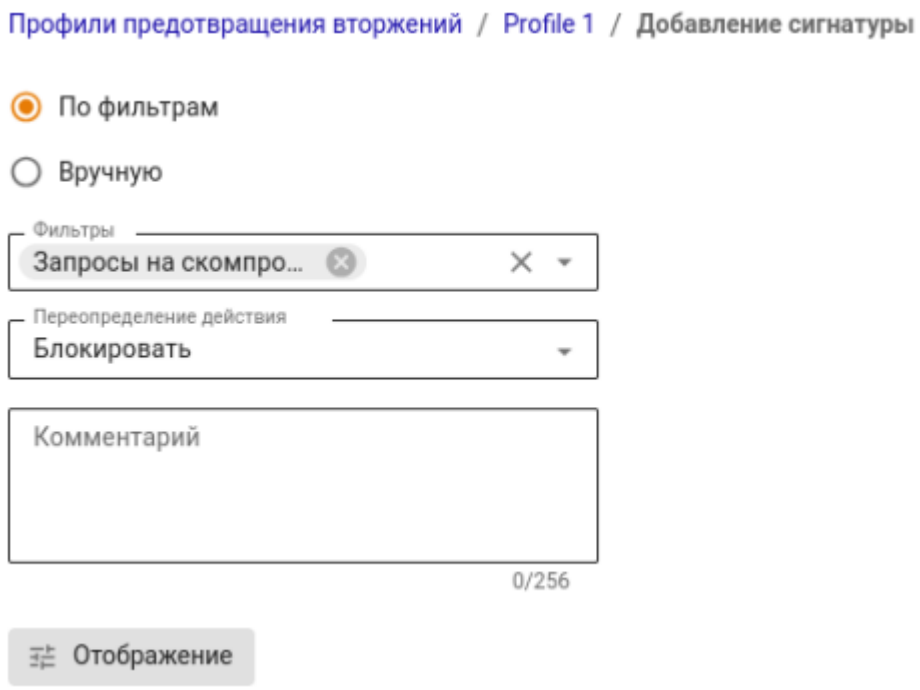
2. В разделе **Правила трафика -> Файрвол** добавьте и включите разрешающее правило с профилем, созданным в пункте 1.

3. Разрешите нужные TCP и UDP порты пользователям. Затем создайте и включите в разделе **Правила трафика -> Файрвол -> FORWARD** правило, которое запрещает все протоколы (правила действуют сверху вниз).

4. В разделе *Контент-фильтр* заблокируйте доступ к сайтам-каталогам и торрент-файлам. Для этого запретите категории **Торрент-трекеры** и **Torrent-файлы**:



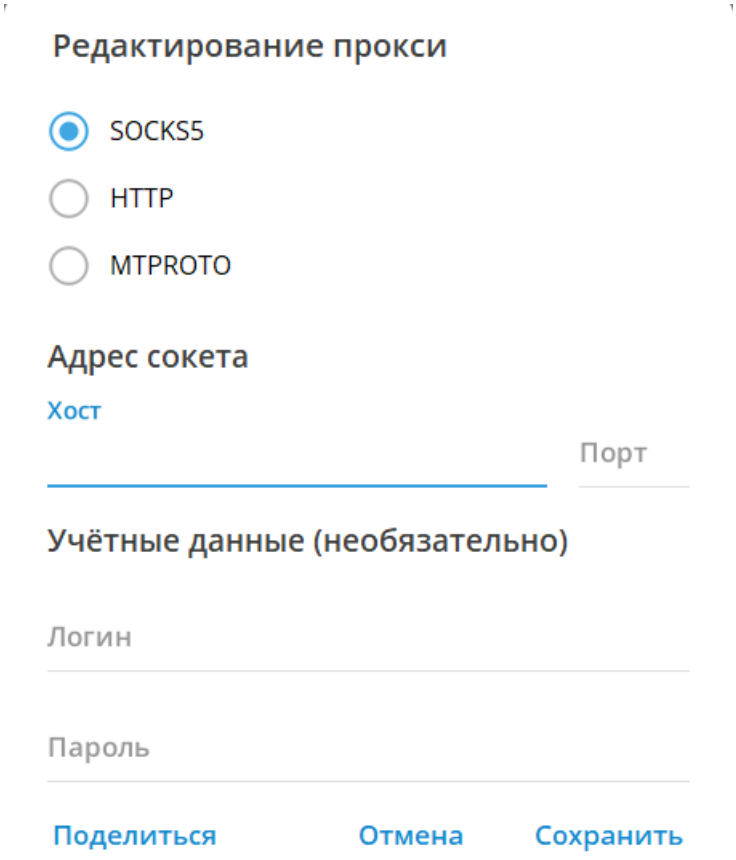
5. В разделе **Профили безопасности ->** ***Предотвращение вторжений*** создайте профиль, блокирующий группу сигнатур **Запросы на скомпрометированные ресурсы**, которая позволяет блокировать активность P2P-программ:



Блокировка Telegram:

Telegram - облачный мессенджер для мобильных устройств и компьютеров (приложение и веб-версия).

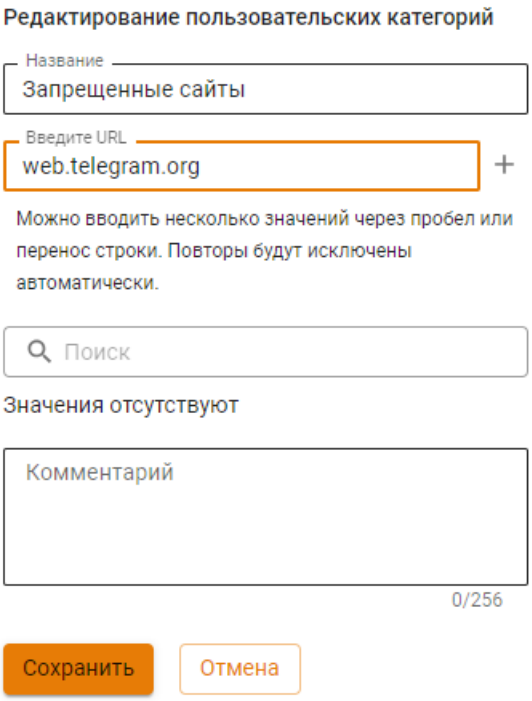
Telegram не блокируется **Контролем приложений**, если в приложении настроить опцию **Использовать собственный прокси** в разделе **Настройки -> Продвинутые настройки -> Тип соединения**:



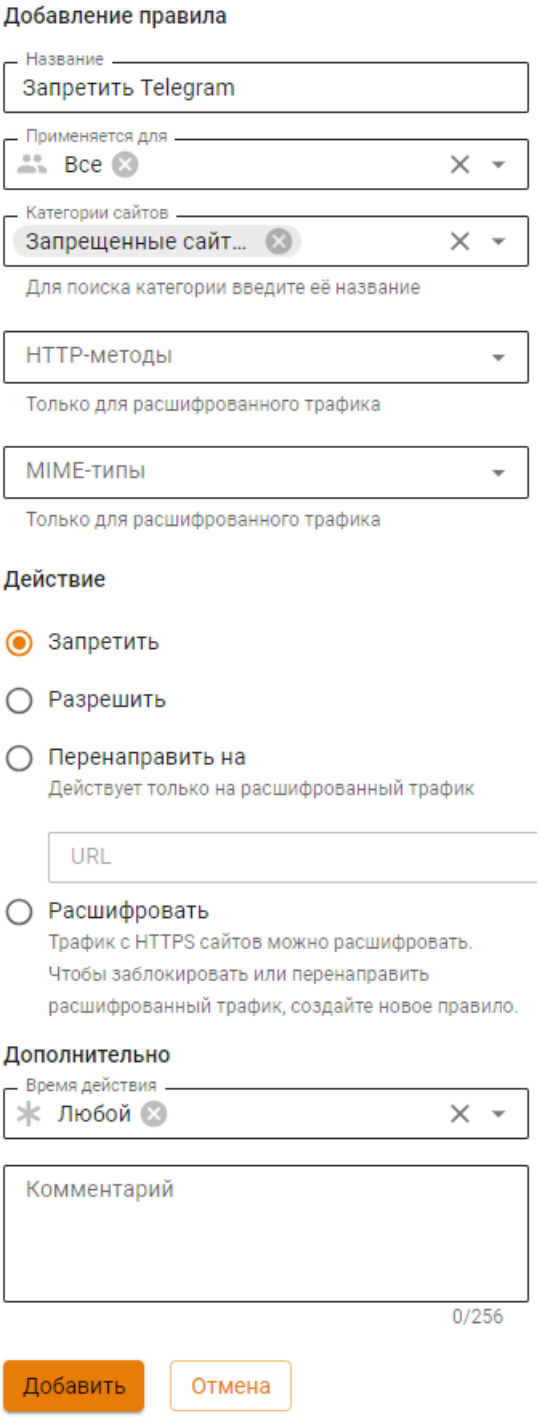
При необходимости рекомендуем блокировать доступ к приложению Telegram на рабочих станциях: запрещать установку и запуск приложения политиками безопасности или антивирусом.

Веб-версию Telegram можно заблокировать с помощью ***Контент-фильтра***. Для этого выполните следующие действия:

1. Создайте пользовательскую категорию, включающую значение `web.telegram.org`, или отредактируйте уже существующую:



2. Укажите созданную или отредактированную пользовательскую категорию при добавлении правила **Контент-фильтра** с действием **Запретить**:



38.37 Настройка прозрачной авторизации на Astra Linux

38.37.1 Основное

Предупреждение: Решение подходит для браузеров **Yandex**, **Chromium** и **Firefox.**

1. Установите и настройте NGFW на устройстве администратора, получите лицензию.

2. Введите Astra Linux в домен (например, через Active Directory).

3. Введите NGFW в тот же домен и импортируйте пользователей (в том числе Astra Linux) в группу.

4. Включите в NGFW **SSO-аутентификацию через Active Directory и ALD Pro** в разделе **Пользователи -> Авторизация -> Веб-аутентификация**.

5. Зайдите под доменной учетной записью на Astra Linux.

6. В зависимости от выбранного браузера, выполните действия:

**

Для браузера **Yandex**:**

1. Создайте файл **mydomain.json** в директории `/etc/opt/yandex/browser/policies/managed/` и впишите в него строку:

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

2. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.

**

Для браузера **Chromium**:**

1. Создайте файл **mydomain.json** в директории `/etc/chromium/policies/managed/` и впишите в него строку:

```
{
    "AuthServerWhitelist": "*.имя_домена"
}
```

2. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.

**

Для браузера **Firefox**:**

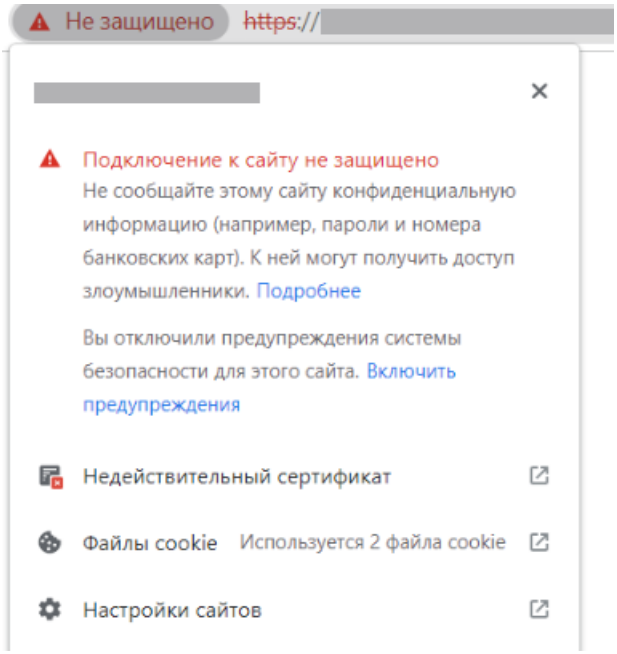
1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

2. Введите параметр `security.enterprise\_roots.enabled` и дважды кликните по блоку, чтобы значение изменилось на **True**.

3. В параметрах `network.automatic-ntlm-auth.trusted-uris` и `network.negotiate-auth.trusted-uris` впишите доменное имя NGFW через HTTP и HTTPS через запятую. Например, http://utm.domain.com, https://utm.domain.com.

4. Откройте страницу любого сайта в браузере. Появится окно с авторизацией, после чего произойдет перенаправление на начальную страницу.

7. При возникновении проблемы с доверенным сертификатом установите корневой сертификат NGFW. Пример проблемы:



**

Для браузера **Yandex**:**

1. Скачайте корневой *сертификат*.

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

**

Для браузера **Chromium**:**

1. Скачайте корневой *сертификат*.

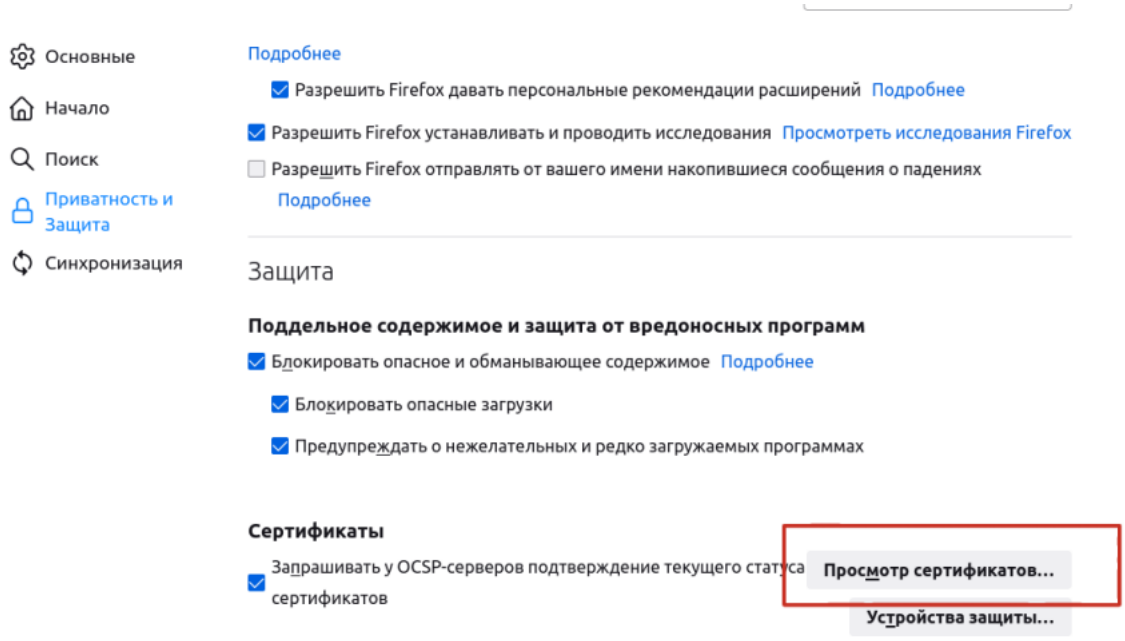
2. В браузере Chromium перейдите на вкладку **Безопасность -> Управление сертификатами -> Центры сертификации -> Импортировать** и добавьте сертификат в список доверенных.

**

Для браузера **Firefox**:**

1. Скачайте корневой *сертификат*.

2. В настройках браузера Firefox в пункте **Защита и приватность** в разделе **Защита** выберите **Просмотр сертификатов**:



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

4. Отметьте пункт **Доверять при идентификации веб-сайтов** и подтвердите.

38.38 Настройка автоматической веб-аутентификации на Ideco NGFW на Linux

38.38.1 Инструкция по настройке автоматической веб-аутентификации на Ideco NGFW

Для настройки автоматической аутентификации выполните действия:

1. Перейдите в домашнюю директорию пользователя (Home) и включите отображение скрытых файлов.

2. Перейдите в папку `.config` и создайте там каталог `ideco-utm`.

3. Скачайте корневой сертификат NGFW (подробнее в *статье*) и поместите его в каталог, созданный на предыдущем шаге.

4. Создайте в папке `ideco-utm` файл `auth.conf`. Откройте его, введите логин и пароль пользователя по образцу:

```
login=логин_пользователя
password=пароль_пользователя
```

5. Скачайте скрипт на компьютер пользователя и настройте автозагрузку в соответствии с описанным ниже алгоритмом:

Предупреждение: Для корректной работы скрипта имя корневого сертификата должно быть `root_ca.crt`.

38.38.2 Настройка автозагрузки скрипта

Для настройки выясните возможность добавления приложений в автозагрузку через графический интерфейс. При отсутствии такой возможности настройте автозагрузку через терминал.

Подсказка: Для настройки через терминал потребуются права администратора.

Настройка через терминал:

Подсказка: Если сделать скрипт исполняемым файлом с помощью команды `chmod +x <путь до скрипта>`, можно не указывать путь до python.

1. Откройте терминал и введите команду:

```
sudo nano /etc/systemd/system/auto-authorization.service
```

2. Заполните файл следующим образом:

```
[Unit]
Description=Auto-Authorization

[Service]
Type=simple
User=имя_пользователя_в_системе
ExecStart=полный_путь_до_python полный_путь_до_скрипта

[Install]
WantedBy=multi-user.target
```

Введите имя пользователя Linux и полный путь до скрипта.

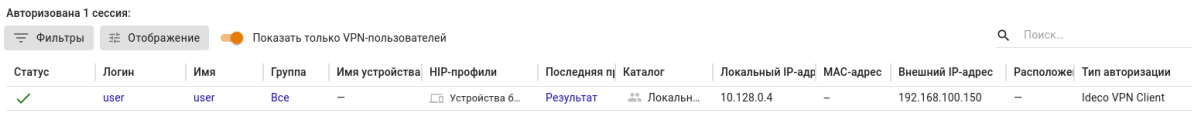
3. Сохраните файл и выйдите из редактора.

4. Добавьте службу в автозагрузку командой `systemctl enable auto-authorization`.

Подсказка: Скрипт поддерживает множество ключей, с помощью которых можно менять путь к файлам и другие параметры. Для вывода справки утилиты используйте ключ `-h`.

Подсказка: Для проверки статуса ранее настроенной службы введите `systemctl status auto-authorization.service`

Проверить работу настройки можно с помощью интерфейса Ideco NGFW. Зайдите в раздел **Мониторинг -> Авторизованные пользователи** и завершите сессию пользователя, для которого настраивалась автоматическая аутентификация. Чтобы удалить авторизованную сессию, нажмите на соответствующую пиктограмму и подтвердите свой выбор.



Если выйти из сессии на устройстве пользователя и повторно открыть браузер, то запрос на авторизацию появиться не должен.

38.39 Перенос данных и настроек на другой сервер

Чтобы перенести установленный Ideco NGFW с одного сервера на другой с сохранением всех настроек, выполните следующие действия:

38.39.1 Этап 1: Копирование бэкапа с сервера

В разделе веб-интерфейса **Управление сервером -> Бэкапы -> Бэкапы** создайте бэкап настроек сервера. Загрузите созданную копию на ваш компьютер, нажав на кнопку **Скачать** в столбце **Управление**.

38.39.2 Этап 2. Установка Ideco NGFW на новый сервер

Инструкция по установке: *Процесс установки*.

38.39.3 Этап 3: Перенос бэкапа на новый сервер

В разделе **Сервисы -> Сетевые интерфейсы** посмотрите и запишите MAC-адрес локальной сетевой карты, он потребуется для перенастройки локального интерфейса в дальнейшем.

В разделе веб-интерфейса **Управление сервером -> Бэкапы -> Бэкапы** нажмите кнопку добавления бэкапа -> **Загрузить из файла** и выберите выгруженный на первом этапе бэкап.

38.39.4 Этап 4: Восстановление БД из бэкапа

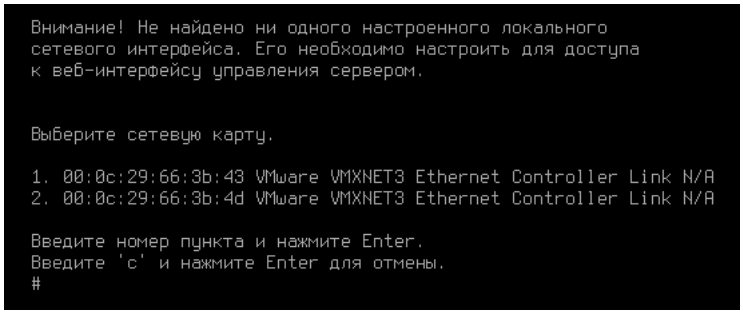
Нажмите кнопку **Применить** (иконка  в столбце **Управление**). Система будет перезагружена для применения настроек сервера.

38.39.5 Этап 5: Настройка восстановленного сервера

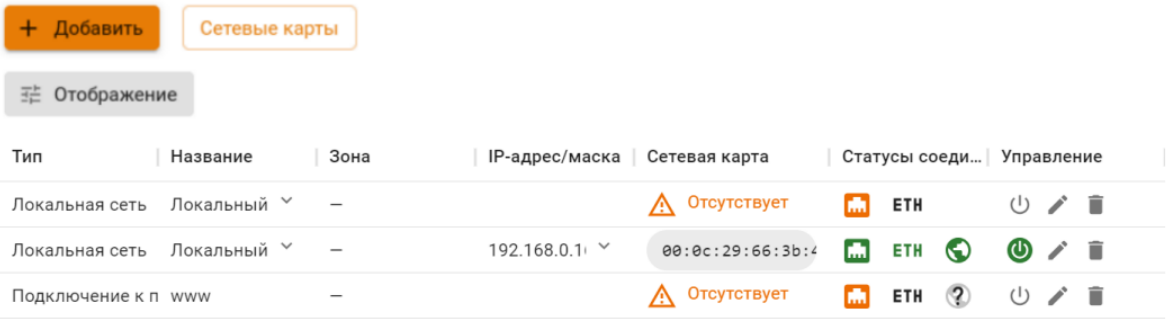
После перезагрузки Ideco NGFW, восстановленного из бэкапа, веб-интерфейс будет недоступен, поскольку ни один локальный интерфейс не будет настроен. Для настройки выполните действия:

1. Перейдите в **Локальное меню**, введите логин и пароль.

2. Выберите сетевую карту и настройте интерфейс.



3. Перейдите в веб-интерфейс в раздел **Сервисы -> Сетевые интерфейсы**. Настройте интерфейсы, восстановленные из бэкапа, привязав к ним сетевые карты:



4. Проверьте:

- В разделе **Сервисы -> DNS** - выданные подключению внешние DNS-серверы;
- В разделе **Сервисы -> DHCP** - опции DHCP-сервера;
- В разделе **Сервисы -> Маршрутизация -> Внешних сетей** - правила маршрутизации;
- В разделе **Сервисы -> OSPF** - настройки интерфейсов;
- В разделе **Правила трафика -> Файрвол** - зоны источника и зоны назначения в правилах;

38.39.6 Этап 6: Привязка лицензии к восстановленному из бэкапа серверу

Если вы переносите бэкап с одного сервера на другой в случае неисправности первого сервера, выполните «перепривязку» лицензии. Для этого перейдите в личный кабинет my.ideco.ru и выполните действия:

1. Отвяжите лицензию от неисправного сервера, нажав на  .

2. Отвяжите demo-лицензию от нового сервера, нажав на  .

3. Привяжите enterprise-лицензию к новому серверу, нажав на 

.

Предупреждение: При подключении к Ideco Center восстановленного из бэкапа клона сервера он не появится в таблице серверов Ideco Center, изменится только **Последнее подключение** в строке неисправного сервера. Это происходит из-за конфликта с донором бэкапа, если у них одинаковый cIUster_id. Сервер-клон подменяет собой уже подключенный Ideco NGFW.

В случае возникновения такой проблемы обратитесь в *Техническую поддержку*.

38.40 Порядок обработки веб-трафика в Ideco NGFW

Порядок обработки веб-трафика:

1. Ограничение скорости;

2. DNS;

3. Захват трафика для фильтрации (прокси-сервер):

- Контент-фильтр;
- Антивирус веб-трафика.

4. Файрвол;

5. Контроль приложений;

6. Система Предотвращения вторжений.

Подсказка: INPUT-правила Файрвола обрабатывают трафик раньше прокси-сервера.

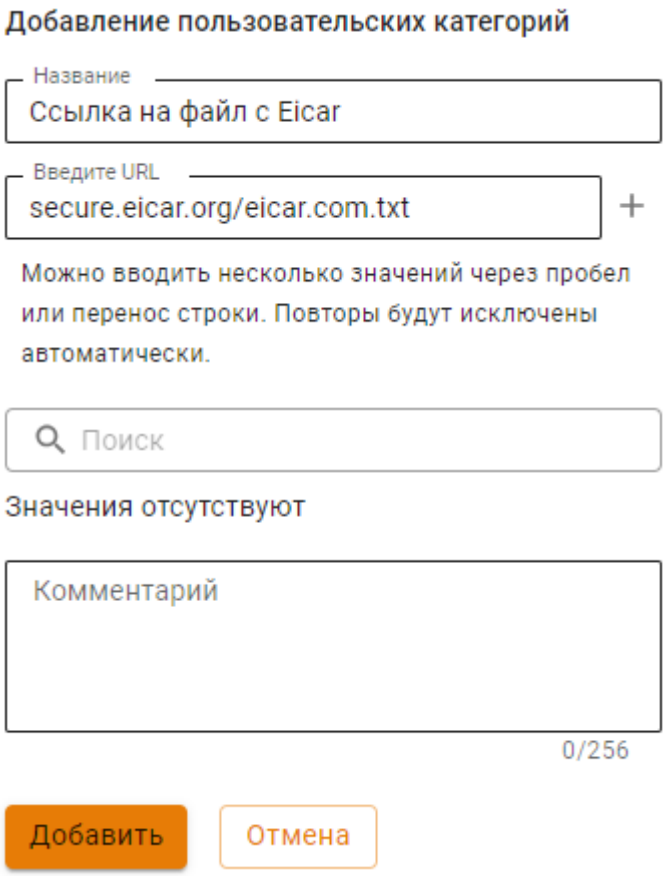
Предупреждение: В 18 версии в модули **Контроль приложений** и **Предотвращение вторжений** отправится только тот трафик, который попадает под разрешающее правило **Файрвола** с включенной проверкой через профиль контроля приложений и профиль предотвращения вторжений соответственно.

38.40.1 Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика?

Для примера использовался тестовый файл с Eicar, доступный для скачивания по ссылке.

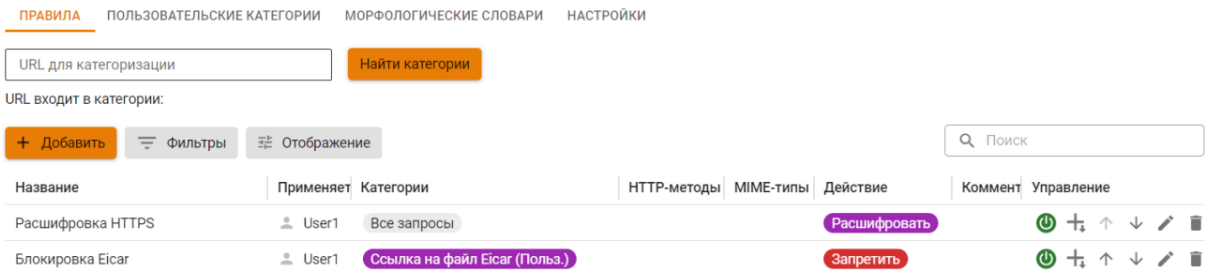
1. Перейдите в раздел **Правила трафика -> Контент-фильтр -> Пользовательские категории**. Нажмите **Добавить**.

2. Введите ссылку на ресурс и нажмите + :



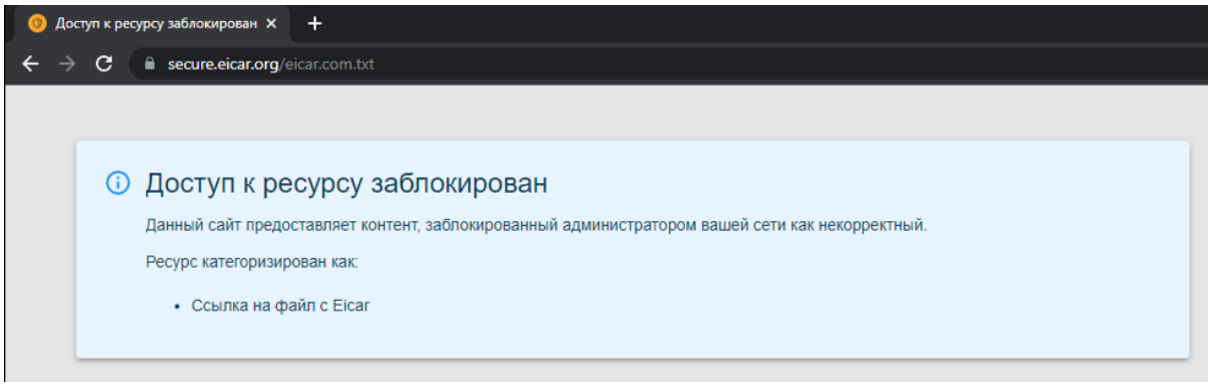
3. Перейдите на вкладку **Правила** и создайте два правила для **User1**:

- Правило расшифровки всех HTTPS-запросов, чтобы антивирус мог работать с HTTPS-трафиком;
- Правило блокировки созданной пользовательской категории:



4. Убедитесь, что опция **Антивирус** переведена в положение **Включен**.

5. Авторизуйте пользователя и перейдите по ссылке на скачивание Eicar.
Откроется страница блокировки **Контент-фильтра**:



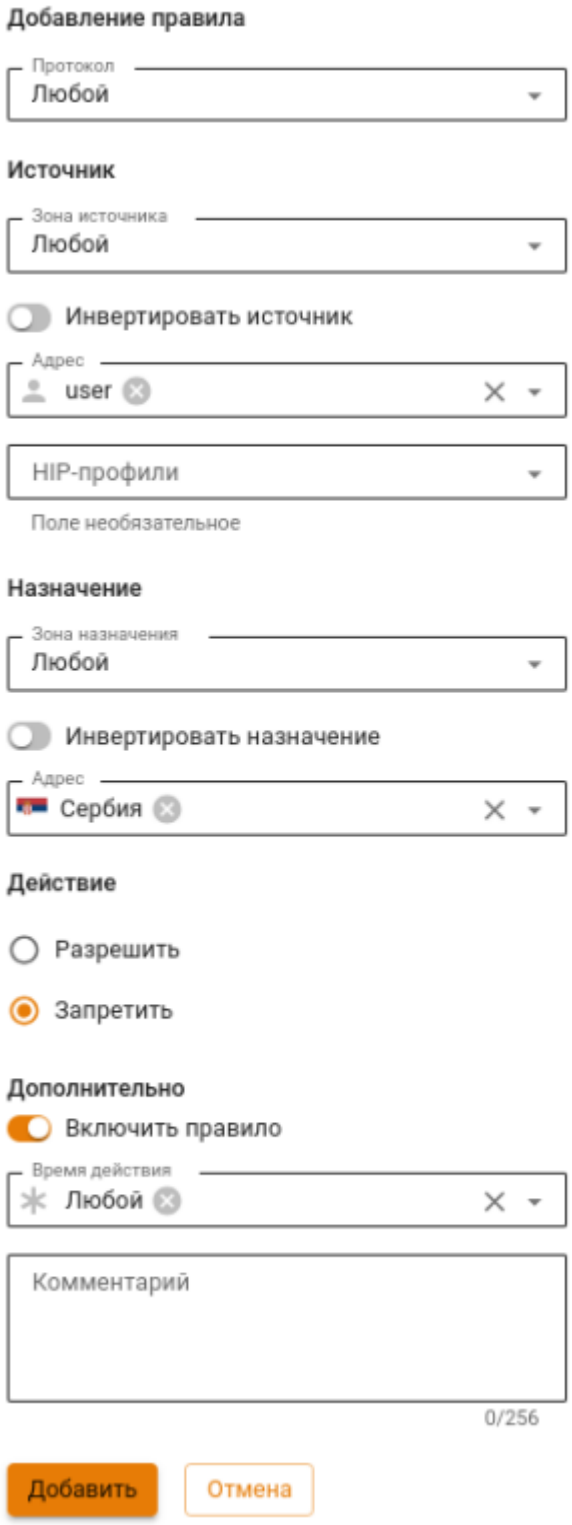
Контент-фильтр обрабатывает трафик приоритетнее, чем антивирусы. Просмотреть информацию о срабатывании правил **Контент-фильтра** можно в **Отчеты -> Трафик -> Топ сайтов**.

38.40.2 Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Файрвол?

Для примера заблокируем пользователю `user` сайт `rts.rs`.

1. Перейдите в раздел **Правила трафика -> Файрвол**, на вкладку **FORWARD** и нажмите **Добавить**.

2. Заполните поля:

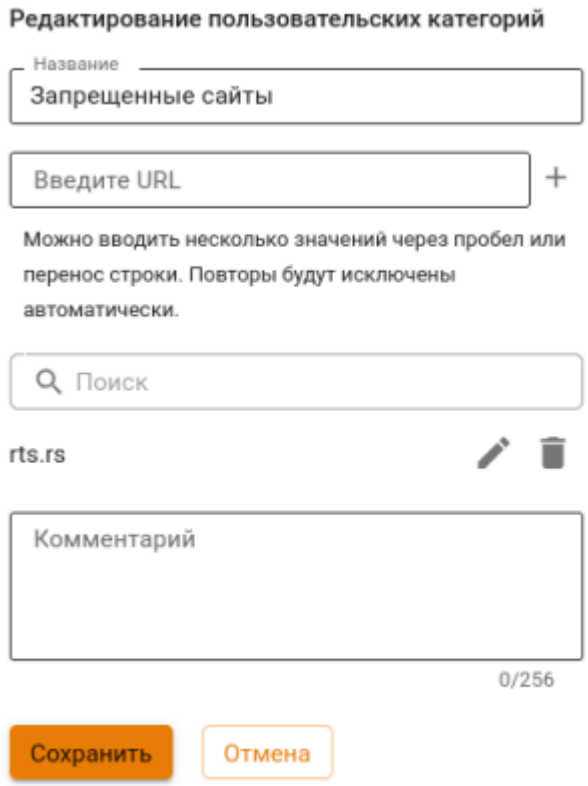


- **Протокол** - выберите **Любой**;
- **Адрес** источника - выберите пользователя `user`;
- **Адрес** назначения - выберите страну **Сербия**;
- **Действие** - выберите **Запретить**.

3. Нажимити **Добавить**.

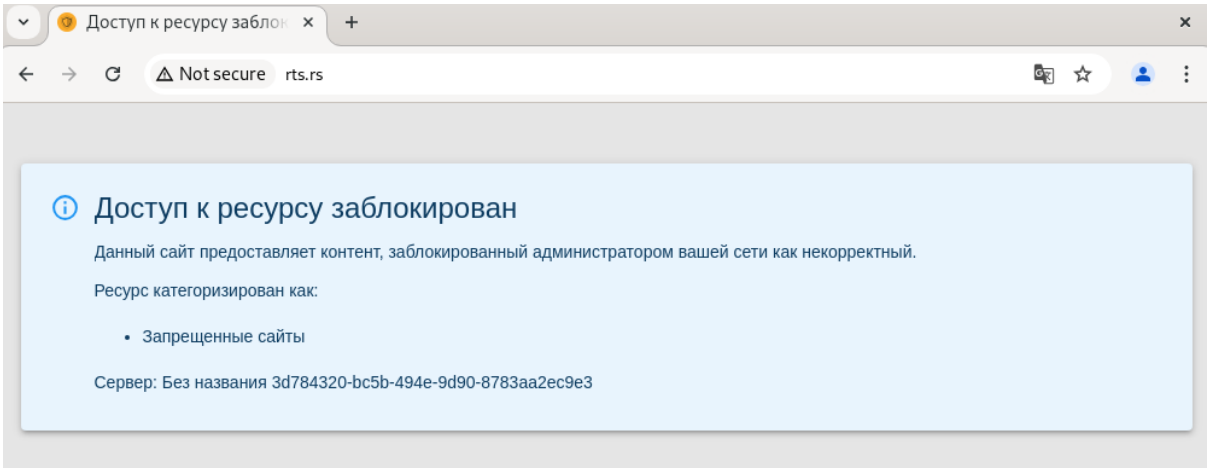
4. Перейдите в раздел **Контент-фильтр** на вкладку **Пользовательские категории** и нажмите на напротив категории **Запрещенные сайты**.

5. Добавьте ссылку на сайт `rts.rs` и нажмите **Сохранить**:



6. Убедитесь, что в таблице правил **Контент-фильтра** включено правило запрета для категории **Запрещенные сайты**.

7. Авторизуйте пользователя и перейдите на сайт `rts.rs`.
Откроется страница блокировки **Контент-фильтра**:



Контент-фильтр обрабатывает трафик приоритетнее, чем **Файрвол**.

38.41 Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG

В Ideco NGFW реализована кластеризации Active/Passive. Повысить отказоустойчивость можно, создав кластер Active/Active. Для этого воспользуйтесь решением наших партнеров АО «НПП «Цифровые решения» - брокером сетевых пакетов DS Integrity NG.

Расположите брокер сетевых пакетов перед Ideco NGFW. Брокер будет самостоятельно балансировать трафик устройств в локальной сети между нодами созданного кластера.
При падении одной ноды трафик перебалансируется между остальными Ideco NGFW без перерыва в связи.
Это реализует схему кластера Active/Active.

Предупреждение: Объединять в кластер устройства Ideco NGFW между собой не нужно.
Для корректной работы нод установите одинаковые настройки.

Подсказка: Для централизованного управления нодами Ideco NGFW воспользуйтесь Ideco Center.

Внимание: Особенности использования схемы:

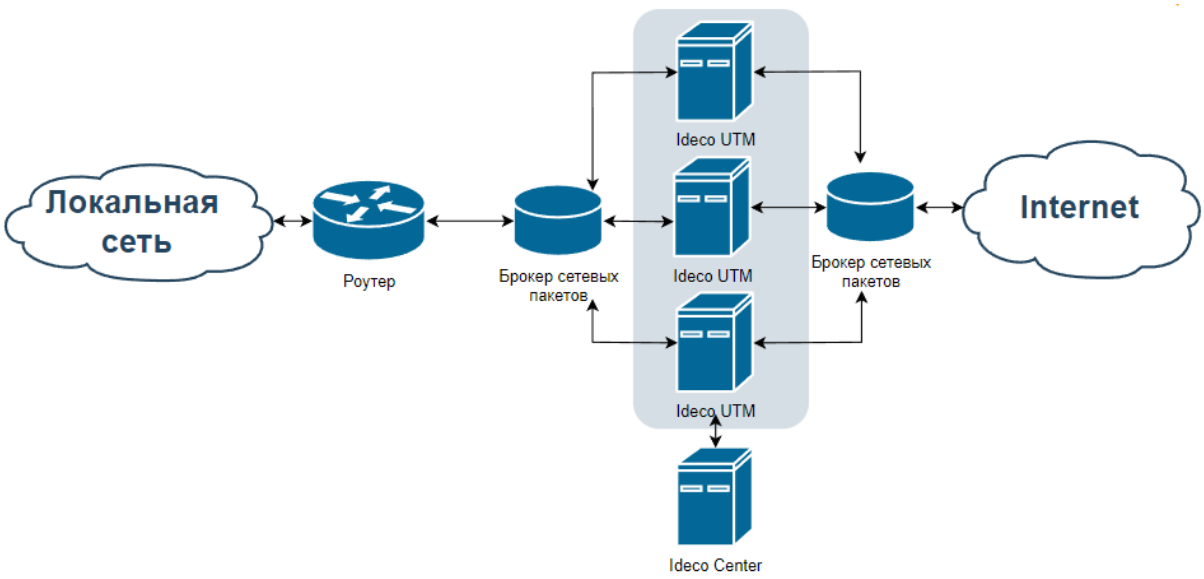
- Настройки, которые нельзя распространить через Ideco Center, придется вручную изменять на каждом Ideco NGFW;
- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено;
- Данные отчетности, логов и мониторинга не синхронизируются между нодами. В каждой ноде хранятся свои данные;
- Восстановление из бэкапа и обновление системы будет затрагивать только одну ноду. Каждую ноду потребуется обновлять отдельно;
- Между локальной сетью и брокером сетевых пакетов потребуется расположить роутер с настроенной динамической маршрутизацией (OSPF) для обмена маршрутами;
- На каждую ноду Ideco NGFW потребуется отдельная лицензия. По вопросам условий лицензирования при использовании такой конфигурации обратитесь к менеджерам.

Примеры трех типовых схем совместного использования брокера сетевых пакетов DS Integrity NG и Ideco NGFW ниже. На этой основе встройте оба решения в свою сеть.

На каждом Ideco NGFW для обмена маршрутами необходимо настроить OSPF для всех локальных интерфейсов. Название зоны и вес должны быть идентичными настроенным ранее на роутере. Информация о настройке OSPF описана в статье *OSPF*. Там же находятся инструкции для настройки OSPF для MikroTik, который можно использовать в качестве роутера.

Подсказка: По вопросам настройки брокера обращайтесь в техническую поддержку АО «НПП «Цифровые решения».

38.41.1 Пример 1 - Два брокера, по одному со стороны локальной и внешней сетей



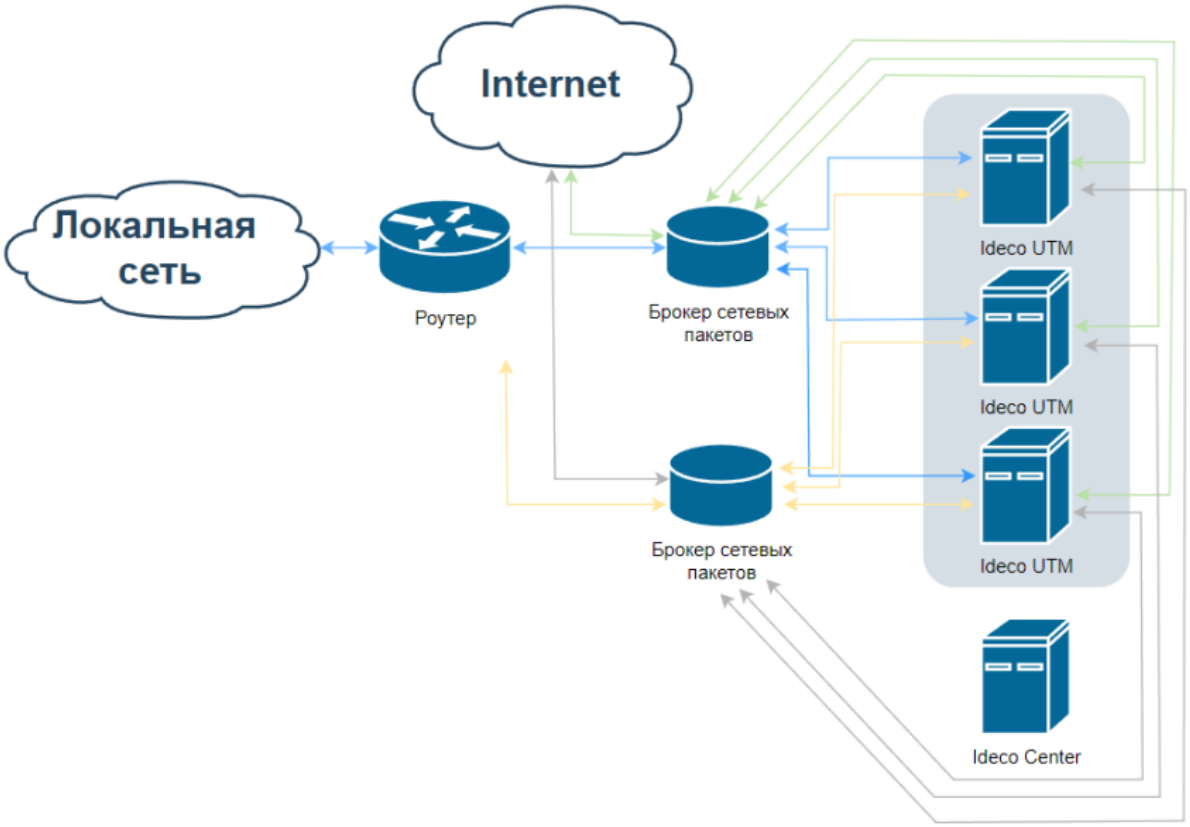
Настройка Ideco NGFW:

На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку *локального* и *внешнего* интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW.

На каждом Ideco NGFW в качестве шлюза внешнего интерфейса нужно использовать IP-адрес, полученный от провайдера.

38.41.2 Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW



Настройка Ideco NGFW

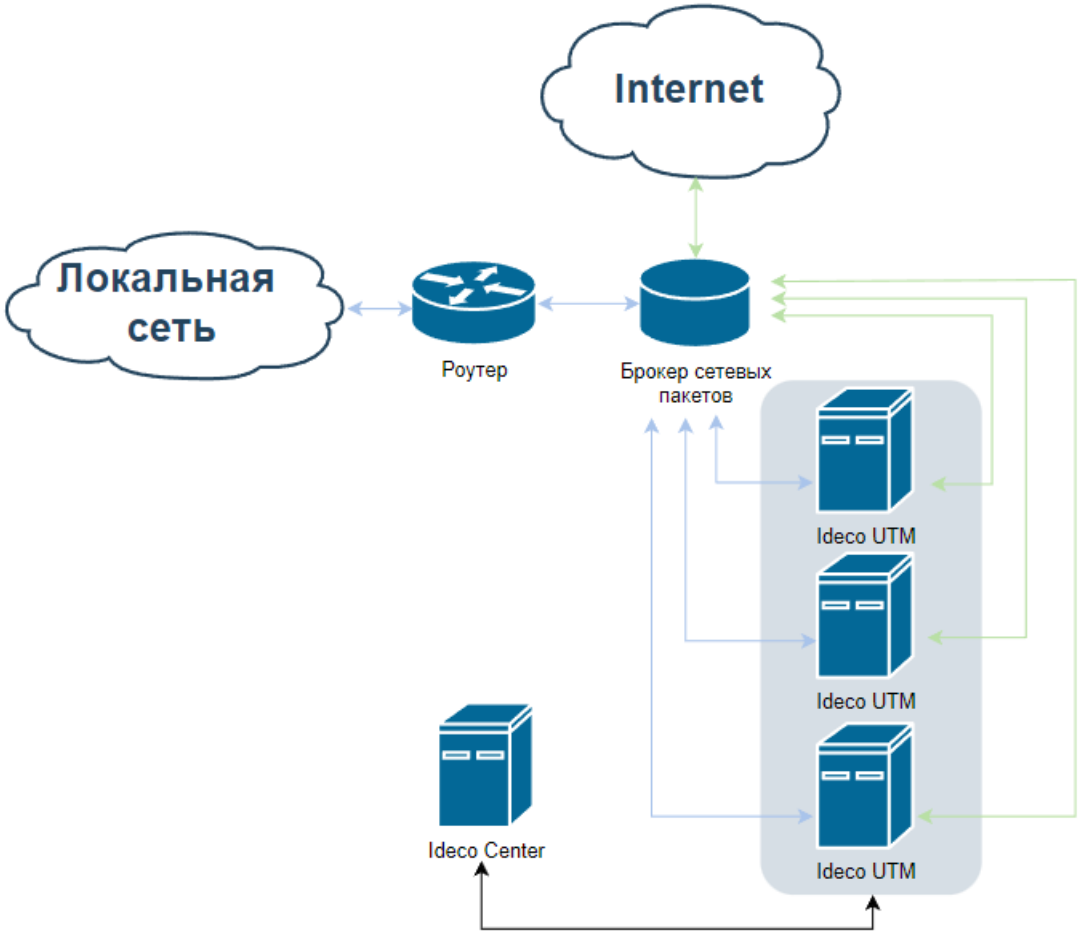
На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку *локального* и *внешнего* интерфейсов.

Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW;
- На каждом NGFW будет два локальных и два внешних интерфейса. Шлюзом внешних интерфейсов нужно указать IP-адрес, полученный от провайдера.

На Ideco NGFW в этой конфигурации в разделе Балансировка и резервирование должен быть активирован режим резервирования. Приоритетным внешним интерфейсом должен быть выбран тот, который идет к основному брокеру сетевых пакетов.

38.41.3 Пример 3 - Один брокер, расположенный перед Ideco NGFW



Настройка Ideco NGFW

На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку *локального* и *внешнего* интерфейсов.

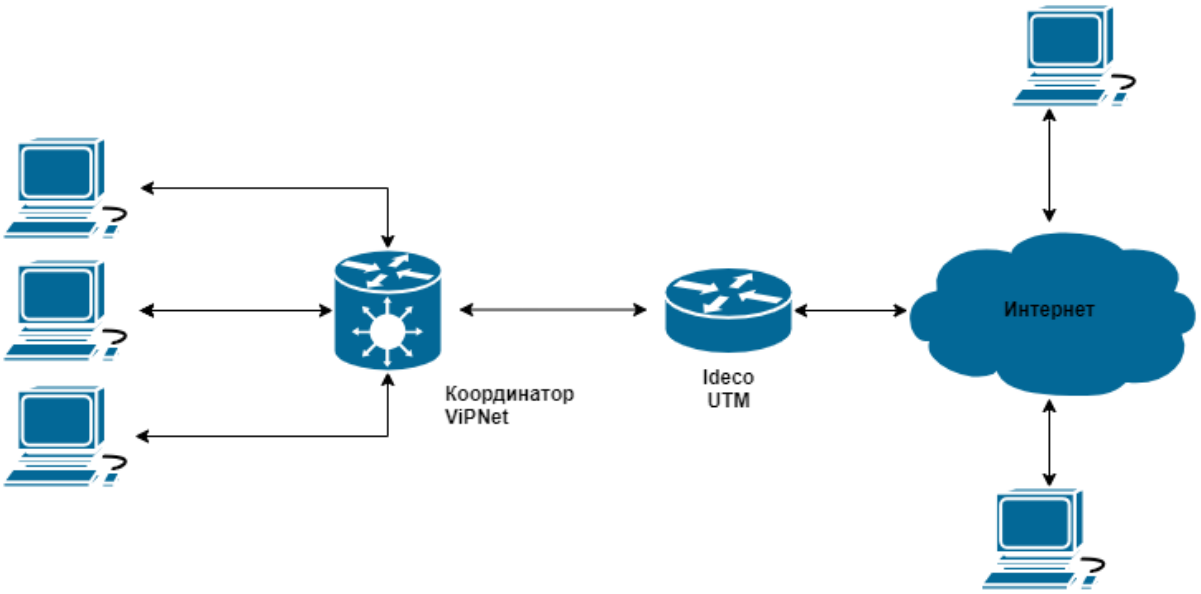
Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- Для устройств в локальной сети шлюзом нужно указать IP-адрес любого из имеющихся Ideco NGFW;
- Шлюзом внешнего интерфейса нужно указать IP-адрес, полученный от провайдера.

38.42 Настройка совместной работы ViPNet Координатор с Ideco NGFW

ViPNet-координатор используется для шифрования трафика подсети, в которой он является шлюзом. Шифрование позволяет обеспечить конфиденциальность информации, передаваемой по незащищенному каналу.

Схема совместной работы Ideco NGFW с ViPNet-координатором:



38.42.1 Настройка Ideco NGFW и ViPNet-координатора

Для корректной работы Координатора совместно с NGFW выполните действия:

1. Настройте проброс порта udp 55777 на IP адрес координатора в разделе **Файрвол -> DNAT (перенаправление портов)**.
2. Переведите Координатор в режим **Со статической трансляцией адресов**.

> **Предупреждение:** Работа Координатора в режиме динамической трансляции адресов совместно с Ideco NGFW не гарантируется.

Подсказка: Более подробно о настройке ViPNet можно узнать в статье.

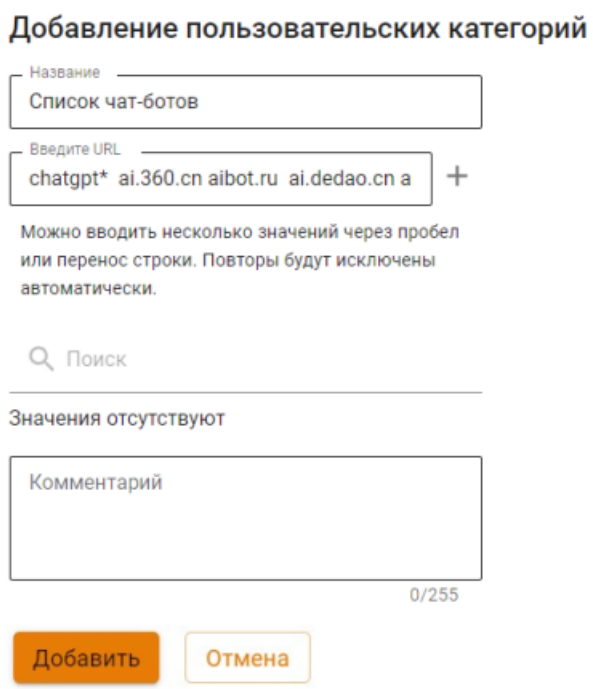
38.43 Блокировка чат-ботов

38.43.1 Основное

Для блокировки ресурсов, взаимодействующих с чат-ботами, потребуется создать правило в Контент-фильтре:

1. Перейдите в раздел **Правила трафика -> Контент-фильтр -> Пользовательские категории**.

2. Добавьте категорию, заполнив следующие поля:



- **Название** - введите любое название;
- **URL** - внесите список URL из блока ниже;
- **Комментарий** - заполнение не обязательно.

Список URL:

```
chatgpt*
ai.360.cn
aibot.ru
ai.dedao.cn
ai.ls
aiservice.vercel.app
aitianhu.com
anse.app
anthropic.com
b.ai-huan.xyz
bard.google.com
bard.google.com
bettergpt.chat
bing.com
bing.com
chadgpt.ru
character.ai
chat4gpt.ru
chat9.yqcloud.top
chat.acytoo.com
chataigpt.org
chat.ai-open.ru
chatboxai.app
chat.dfehub.com
chat.getgpt.world
chatglm.cn
chatgp.ru
chat.gpt4free.io
```

(continues on next page)

(продолжение с предыдущей страницы)

```
chatgpt4rus.ru
chatgpt.ai
chatgptbot.ru
chat-gpt.com
chatgptfree.ai
chat-gpt-free.ru
chatgptlogin.ac
chatgpt-me.ru
chat-gpt-na.ru
chat-gpt-na.ru
chatgptnarusskom.ru
chat-gpt.org
chatgpt.org
chatgpt.pro
chat-gpt.ru
chatgpt-telegram.com
chatgptweb.ru
chathub.gg
chatinfo.ru
chat.lmsys.org
chat.openai.com
chat.ramxn.dev
chat.su
claude.ai
crfm.stanford.edu
deepai.org
easychat-ai.app
itbabushka.com
forefront.com
freechatgpt.chat
free-chatgpt.ru
free.easychat.work
gpt2.ru
gpt4all.io
gpt-chatbot.ru
gptchatbot.ru
gptchatly.com
gpt-gm.h2o.ai
gptgo.ai
gpt-open.ru
gptschat.ru
gradio.app
h2o.ai
huggingface.co
iask.ai
liaobots.com
liftweb.ru
lmsys.org
macgpt.com
mashagpt.ru
moss.fastnlp.top
neice.tiangong.cn
openai.ru
openai-gpt.ru
openai-chat-gpt.ru
open-assistant.io
```

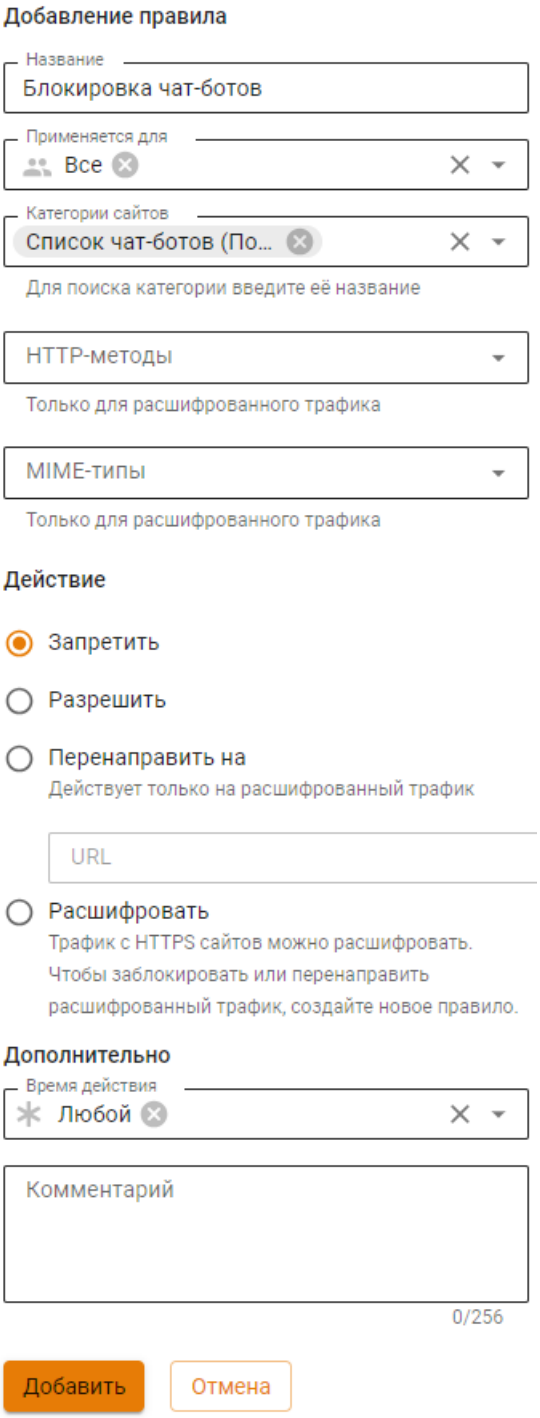
(continues on next page)

(продолжение с предыдущей страницы)

```
opencat.app
petals.ml
play.vercel.ai
poe.com
ru-chatgpt.ru
rugpt.chat
sdk.vercel.ai
supertest.lockchat.app
tenchat.ru
theb.ai
timeai.ru
tongyi.aliyun.com
tools.zmo.ai
trychatgpt.ru
wewordle.org
xinghuo.xfyun.cn
yandex-gpt.com
yandex-gpt.ru
yiyan.baidu.com
you.com
zhpt.tech
```

4. Сохраните категорию.

3. Перейдите на вкладку **Правила** и добавьте правило с действием **Запретить**:



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

В этой таблице приведен список портов, которые находятся в состоянии **Listen** после включения на Ideco NGFW различных служб.

38.44.1 Доступные из внешней сети

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

Подсказка: 80 и 443 TCP-порты открыты во внешнюю сеть сразу после установки Ideco NGFW и настройки интерфейсов и находятся в состоянии **Listen** постоянно.

38.44.2 Доступные из локальной сети

Включенная служба	Порты
Прокси	8080 (порт настраивается пользователем)
DNS	53 TCP, UDP
DHCP-сервер	67, 68 UDP
NTP-сервер	123 UDP
Тест скорости	18080 TCP
OSPF	-

Подсказка: 8443 TCP-порт предназначен для веб-интерфейса, открыт в локальную сеть сразу после установки Ideco NGFW и настройки интерфейсов и находится в состоянии **Listen** постоянно.

38.44.3 Как проверить, открыт ли порт

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

```
nmap -v 192.168.0.150
```

- 192.168.0.150 - адрес локального или внешнего интерфейса Ideco NGFW.

38.45 Как Ideco Client осуществляет обработку запросов с редиректом на сервер Ideco NGFW

38.45.1 Основное

Ideco Client может обрабатывать запросы с перенаправлением (код ответа 302). Получив ответ от сервера, **Ideco Client** выполняет шаги для подключения к **Ideco NGFW**:

1. Отправляет запрос на адрес https://host:14765/connect.
2. Если сервер отвечает статусом 302 с редиректом, **Ideco Client** использует информацию из этого ответа для установления соединения.
3. **Ideco Client** подключается к NGFW, используя имя сервера или IP-адрес, указанный в поле Location.

Предупреждение: Важно:

- Адрес обязательно должен включать порт `14765`;
- В заголовке Location в ответе 302 должен быть указан полный URL-адрес, из которого будет извлечено только имя сервера или IP-адрес;
- Полученное имя сервера или IP-адрес используются для создания адреса в формате `wss://host_from_location:14765/connect`, к которому будет подключаться **Ideco Client**;
- Если ответа со статусом 302 от адреса `https://host:14765/connect` нет, то **Ideco Client** подключится к NGFW по адресу `wss://host:14765/connect`.

Пример правильного редиректа, полученный с помощью утилиты **curl**:

1. **Запрос**: `curl -il https://host.dev:14765/connect`.

2. **Ответ**:

```
HTTP/1.1 302 Found
Server: SERVERNAME
Date: Fri, 15 Nov 2024 04:22:46 GMT
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=15
Location: https://ngfw-host.dev/
cache-control: no-cache
```

Из заголовка `Location: https://ngfw-host.dev/` будет извлечен новый хост `ngfw-host.dev`, и **Ideco Client** будет подключаться к NGFW по адресу `wss://ngfw-host.dev:14765/connect`.

3. Если при попытке доступа к URL-адресу `https://host.dev:14765/connect` не будет получен ответ с кодом 302, то **Ideco Client** подключится к NGFW по адресу `wss://host.dev:14765/connect`.

39. Диагностика проблем

39.1 Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Перед проверкой модулей фильтрации NGFW убедитесь, что на работу сайта не влияют:

- технические проблемы на самом ресурсе;
- блокировка со стороны провайдера;
- некорректная работа устройства пользователя и т.д.

Откройте сайт с устройства вне локальной сети NGFW. Например, со смартфона через мобильный интернет. Если сайт доступен, перейдите в веб-интерфейс NGFW.

Подсказка: Для определения модуля фильтрации, блокирующего сайт, можно проверить логи в разделах *Системный журнал* и *Syslog*. Это может помочь определить причину возникшей проблемы и более точно ее диагностировать.

39.1.1 Шаг 1. Проверьте, открывается ли сайт в режиме Разрешить интернет всем

1. Нажмите на в верхней правой части веб-интерфейса NGFW.

2. Переведите опцию **Разрешить интернет всем** в положение **Включен**:

3. Откройте сайт.

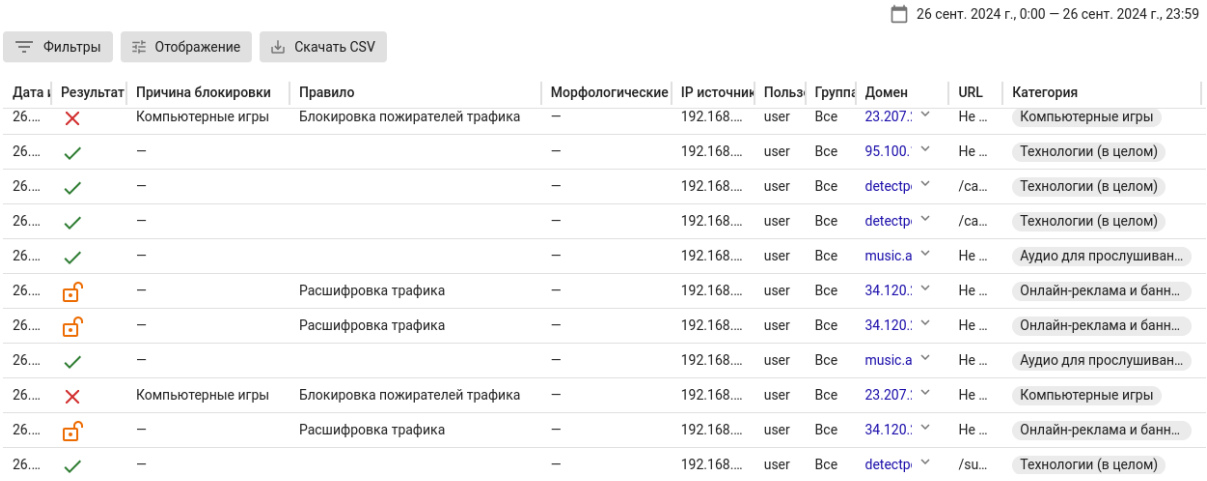
Если сайт не открывается, проверьте, откроется ли сайт на другом устройстве с того же IP-адреса:

- Если не открывается, рекомендуем обратиться к провайдеру. Скорее всего, провайдер блокирует IP-адрес или адрес сайта;
- Если сайт открывается, проверьте настройки устройства пользователя.

39.1.2 Шаг 2. Проверьте, не блокируется ли сайт правилом Контент-фильтра

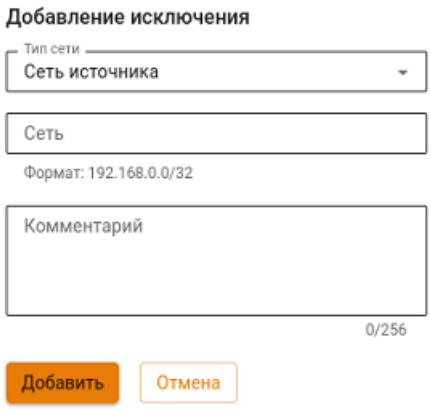
1. Откройте сайт с устройства пользователя.

2. В NGFW перейдите в раздел **Отчеты и журналы -> Журнал веб-трафика** и посмотрите, какое правило блокирует сайт:



3. Для поиска блокирующего правила также можно ввести URL сайта в строку поиска категорий **Контент-фильтра** на вкладке **Правила** в разделе **Правила трафика -> Контент-фильтр**:

4. Если сайт блокируется правилом **Контент-фильтра**, измените его настройки или добавьте сайт в исключения в разделе **Сервисы -> Прокси** на вкладке **Исключения**:



Подсказка: В раздел **Сервисы -> Прокси -> Исключения** рекомендуем добавлять заведомо надежные сервисы.

Добавлять в исключения адреса клиентов вашей сети не рекомендуется, так как в этом случае их веб-трафик не будет фильтроваться правилами **Контент-фильтра** и не будет попадать в отчеты.

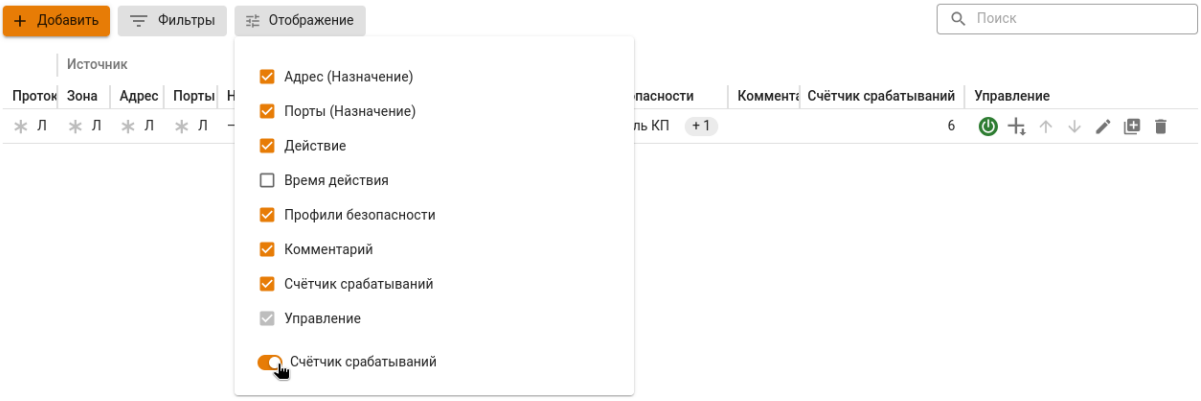
39.1.3 Шаг 3. Проверьте, не блокирует ли сайт правило Файрвола

Найдите блокирующее правило одним из способов:

Первый способ. Счетчик срабатываний:

1. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD**.

2. Нажмите на **Отображение** и включите **Счетчик срабатываний**:



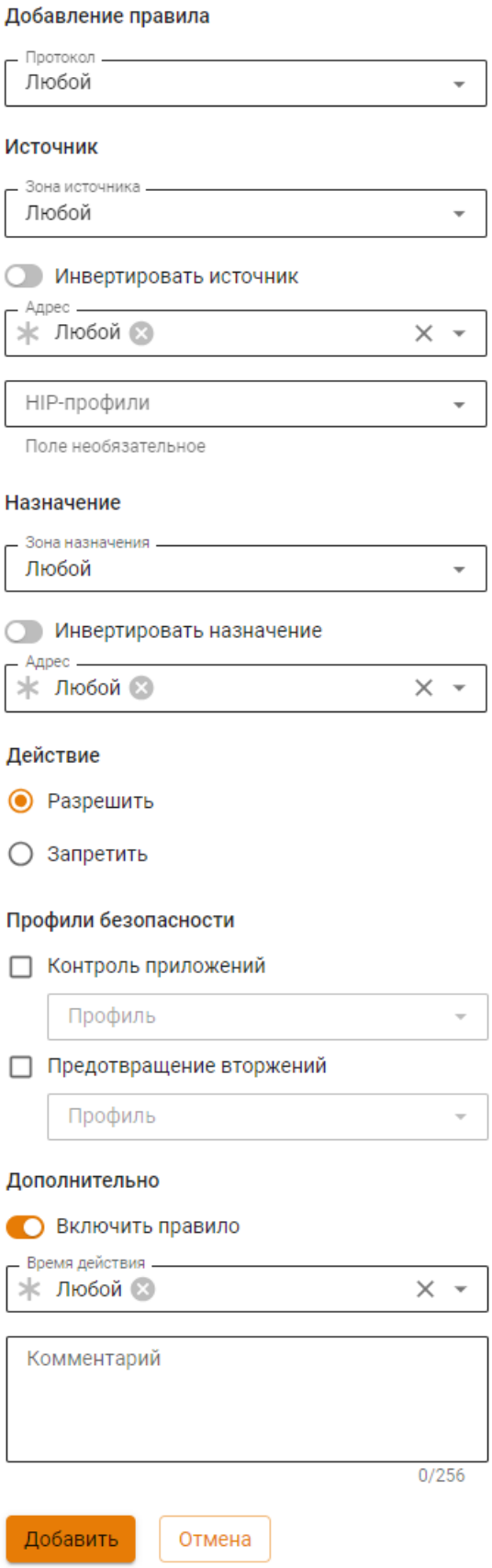
3. Откройте сайт с устройства пользователя.

4. Найдите в таблице FORWARD правило с заметным увеличением количества срабатываний.

Второй способ. Тестовое правило:

1. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD**.

2. Создайте тестовое правило, разрешающее любой трафик:



3. Правило добавится в конец таблицы. Поместите созданное правило на одну позицию вверх, нажав на кнопку ↑.

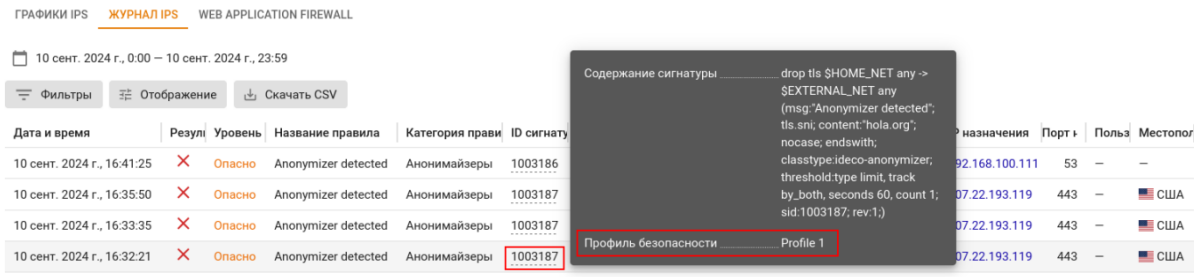
4. Откройте сайт с устройства пользователя.

5. Если сайт не открывается, поднимите тестовое правило на позицию выше и повторно откройте сайт с устройства пользователя. Повторяйте эти действия до тех пор, пока сайт не откроется.

6. Если сайт открывается, блокирующее правило расположено ниже тестового.

Если блокирующее правило направляет трафик через систему Предотвращения вторжений:

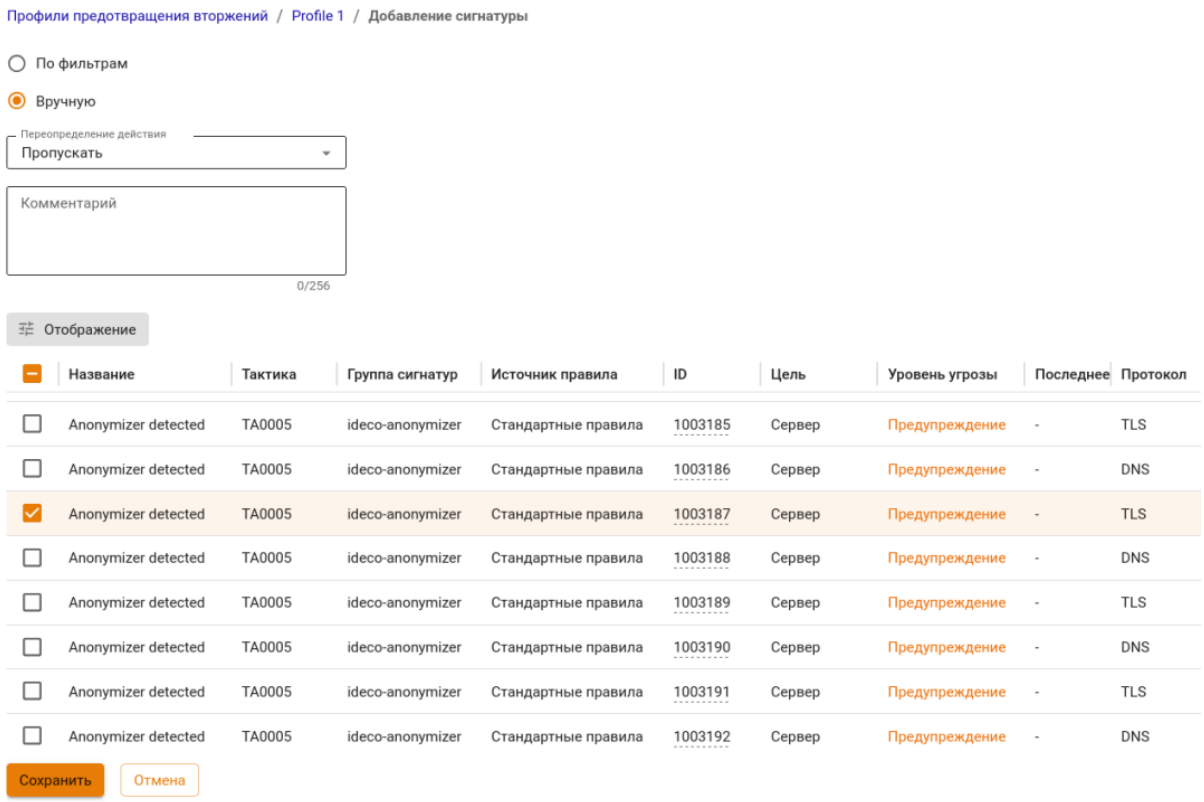
1. Перейдите в раздел **Отчеты и журналы -> События безопасности** на вкладку **Журнал IPS** и найдите в таблице ID сигнатуры, заблокировавшей сайт, и название профиля, к которому она относится:



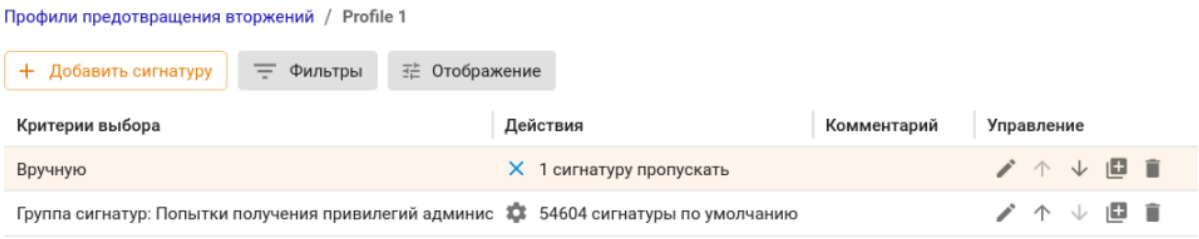
2. Перейдите в раздел **Профили безопасности -> Предотвращение вторжений**, нажмите на напротив профиля, заблокировавшего сайт, и выберите **Сигнатуры**.

3. Нажмите **Добавить сигнатуру** и выберите способ **Вручную**.

4. В таблице сигнатур по ID найдите сигнатуру (или сигнатуры), заблокировавшую сайт, и переопределите действие для нее:



5. Нажмите **Добавить** и переместите только что созданное правило на самый верх таблицы правил профиля:



Если блокирующее правило направляет трафик через Контроль приложений:

1. Перейдите в раздел **Отчеты и журналы -> Трафик**.

2. В виджете **Топ заблокированных протоколов** найдите протоколы, которые блокируются **Контролем приложений**.

3. Перейдите в раздел **Профили безопасности -> Контроль приложений** и отредактируйте профиль, разрешив заблокированные протоколы.

39.1.4 Шаг 4. Определите блокируемый домен или IP-адрес (рассмотрим на примере FireFox)

1. Откройте в браузере нужный сайт.

2. Откройте инструменты веб-разработчика одним из способов:

   - Нажмите Ctrl+Shift+I;
   - Нажмите на ☰ в правом верхнем углу браузера, перейдите в раздел **Другие инструменты -> Инструменты веб-разработчика**.

3. Выберите вкладку **Сеть**.

4. Обновите страницу.

5. Отсортируйте столбец **Статус** левой кнопкой мыши. Обратите внимание на коды состояния 4xx и 5xx. Часто именно эти запросы блокируются NGFW.

39.1.5 Если решить проблему не удалось

Отправьте в техподдержку:

1. Скриншот ошибки в браузере;

2. Скриншот отсортированных ошибок из браузера, чтобы было видно проблемные домены или IP-адреса.

39.2 Что делать если не работает интернет

39.2.1 Шаг 1. Проверить параметры пользователя

Убедитесь, что проверяемый пользователь авторизован на сервере. Возможные состояния пользователя описаны в главе *Дерево пользователей*.

39.2.2 Шаг 2. Проверка компьютера пользователя

Выполните команду `ping` с компьютера пользователя до адреса `8.8.8.8`: **Пуск -> Выполнить**, введите команду `cmd`, в появившемся окне введите `ping 8.8.8.8`.

1. Если адрес `8.8.8.8` отвечает на эхо-запросы, проверяем `ping ya.ru`;

2. Если адрес `8.8.8.8` не отвечает на эхо-запросы, перейдите к Шагу 3;

3. Если адрес `ya.ru` отвечает на эхо-запросы, перейдите к Шагу 5;

4.Если появилось сообщение **Не удалось обнаружить узел ya.ru**, то, возможно, не работает DNS-провайдер, проверьте командой `nslookup ya.ru 222.222.222.222`, вместо `222.222.222.222` укажите DNS адрес провайдера:

- Если ответа нет - обратитесь к провайдеру;
- Если ответ есть, проверьте адрес первичного DNS на вашем компьютере (должен быть указан локальный адрес Ideco NGFW). Проверьте также, что DNS-сервер работает на Ideco NGFW в разделе **Сервисы -> DNS**.

39.2.3 Шаг 3. Проверка доступа к интернету на сервере

Зайдите в раздел **Терминал** в веб-интерфейсе: выполните команду `ping 8.8.8.8`, для остановки `ctrl+c`.

Если ping не проходит:

1. Проверьте настройки сервера, адреса и маски интерфейсов;

2. Убедитесь, что используемое вами сетевое оборудование является исправным, сетевые кабели правильно обжаты, а также не имеют изломов и обрывов, проверьте индикатор сигнала на сетевой карте (его можно посмотреть в разделе **Сервисы -> Сетевые интерфейсы**), перезагрузите коммутатор и модем (если используется);

3. Если используется подключение по Ethernet, то необходимо выполнить команду `ip neigh | grep <адрес_шлюза_провайдера>`. Если MAC-адрес шлюза провайдера не определился, то имеет смысл попробовать перезагрузить Сервер, переподключив сетевой кабель. После этого проверить наличие MAC-адреса шлюза провайдера. Такое решение помогает, если «подвисает» порт коммутатора провайдера. Если после указанной меры MAC шлюза провайдера не появился в таблице MAC-адресов, обратитесь к провайдеру. Следует отметить, что при смене сетевого оборудования отсутствие доступа к интернету может быть обусловлено использованием вашим интернет-провайдером привязки по MAC-адресу.

Если ping проходит, перейдите к Шагу 4.

39.2.4 Шаг 4. Проверка файрвола

1. Отключите модуль **Файрвол** в разделе веб-интерфейса **Правила трафика -> Файрвол**. Если веб-интерфейс недоступен, то файрвол можно выключить с помощью локального меню;

2. Если доступ к интернету появился, найти правило, запрещающее доступ к сети, в файрволе, поочередно включая правила;

3. Если ничего не помогло, перейдите к следующему шагу.

39.2.5 Шаг 5. Проверка работы веб-трафика

Если пользователь получает ответы на эхо-запросы командой `ping` и по доменному имени, и по IP-адресу, но при этом веб-трафик отсутствует:

1. Проверьте, что в браузере отсутствуют все настройки прокси;

2. Выключите временно файрвол Windows и антивирусное ПО;

3. Если ничего не помогло, перейдите к Шагу 6.

39.2.6 Шаг 6. Если вам не удалось решить проблему

1. Сделайте скриншоты вкладки **Основное** у пользователя в развернутом виде и создайте обращение на портале поддержки или напишите письмо на support@ideco.ru.

2. Включите *режим удаленного помощника* и обратитесь в службу технической поддержки: https://ideco.ru/tekhnicheskaya-podderzhka.

39.3 Ошибка при авторизации «The browser is outdated»

39.3.1 Основное

Если используется браузер, который не поддерживает NGFW, при авторизации появится ошибка **Your browser is outdated. This version of browser is unsecure and unsupported by modern web-technologies. Please, install the latest version of one of the listed browsers**.

Поддерживаемые версии браузеров:

- Google Chrome версия >= 90;
- Firefox версия >= 78;
- Safari версия >= 14.

Рекомендуем обновить браузер до минимально поддерживаемой версии.

Для продолжения авторизации несмотря на риски потребуется нажать **I understand the risks and wish to continue**.

39.4 Если соединение по IPsec не устанавливается

39.4.1 Основное

1. Перезагрузите сервисы двух NGFW, выполнив команду `systemctl restart ideco-ipsec-backend.service && systemctl restart strongswan.service`.

2. Проверьте работоспособность перезагруженных сервисов:

- выполните команду `systemctl status strongswan.service`;
- перейдите в раздел **Сервисы -> IPsec**.

Если при переходе в раздел IPsec и выполнении команды возникли ошибки, то перейдите к пункту 3.

3. Пересоздайте соединение из веб-интерфейса по инструкции *Настройка подключения между Филиалом и Главным офисом*.

Если пересоздание соединения не помогло, перейдите к пункту 4.

4. Проверьте, ходит ли трафик по портам 500 и 4500, выполнив команды `tcpdump -i any port 4500 -ttttnnn` и `tcpdump -i any port 500 -ttttnnn` в головном офисе и филиале.

Если трафик уходит с одного NGFW и приходит на второй NGFW, то обратитесь в *техническую поддержку*.
Если трафик уходит с одного NGFW и не приходит на второй NGFW, обратитесь к провайдеру.

39.5 Ошибка 400 Bad Request Request Header Or Cookie Too Large при авторизации в браузерах

39.5.1 Основное

Ошибка возникает на Windows 7, 8, 11, Windows Server 2008 R2, 2012, 2022 из-за большого количества групп безопасности и неспособности токена Kerberos вместить все данные.

По умолчанию размер токена Kerberos:

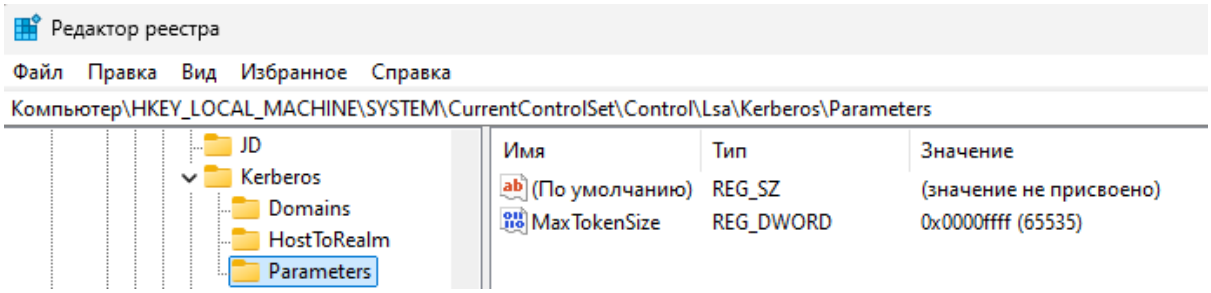
- **Windows 7 и Windows Server 2008R2** - 12000 байт;
- **Windows 8 и Windows Server 2012 (включая Windows Server 2022 и Windows 11)** - 48000 байт.

Для решения проблемы нужно увеличить размер токена на пользовательской ОС. Для этого:

1. Откройте редактор реестра и перейдите в раздел **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Ker**

2. Создайте новый параметр типа **DWORD (32-bit)** с именем **MaxTokenSize**.

3. Задайте максимальное значение размера буфера - 65535 байт в десятичной системе счисления:



4. Перезагрузите компьютер.

Подсказка: Чтобы узнать текущее значение параметра **MaxTokenSize**, выполните следующую команду в **PowerShell**:

```
Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\
↪Parameters|select MaxTokenSize
```

---

40. Описание основных хендлеров

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Авторизация администратора:

```
POST /web/auth/login
```

Json-тело запроса:

```
{
    "login": "string",
    "password": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "rest_path": "string",
}
```

- `login` - логин, каталог администратора указывается после `@`. Примеры:
  - `admin` - локальный админ, без `@`;
  - `admin@ad_domain.ru` - AD/ALD администратор;
  - `admin@radius` - для RADIUS-администраторов `@radius`.
- `password` - пароль;
- `rest_path` - префикс URL, на который выставлять cookie. Например, `/` или `/rest`.

Ответ на успешный запрос: 200 OK

После успешной авторизации сервер Ideco NGFW передает в заголовках куки. Пример значений:

```
set-cookie: insecure-ideco-session=02428c1c-fcd5-42ef-a533-5353da743806
set-cookie: __Secure-ideco-3ea57fca-65cb-439b-b764-d7337530f102=df164532-b916-4cda-
↪a19b-9422c2897663:1663839003
```

Эти куки нужно передавать при каждом запросе после авторизации в заголовке запроса Cookie.

Разавторизация администратора:

```
DELETE /web/admin/auth/login
```

Ответ на успешный запрос: 200 OK

После успешной разавторизации сервер Ideco NGFW передает в заголовках куки. Пример значений:

```
set-cookie: insecure-ideco-session=""; expires=Thu, 01 Jan 1970 00:00:00 GMT; Max-
↪Age=0; Path=/
set-cookie: __Secure-ideco-b7e3fb6f-7189-4f87-a4aa-1bdc02e18b34=""; HttpOnly; Max-
↪Age=0; Path=/; SameSite=Strict; Secure
```

Добавление правила авторизации:

```
POST /auth/rules
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "ip": "string" | "null",
    "mac": "string" | "null",
    "user_id":  "integer",
    "always_logged": "boolean",
    "comment": "string"
}
```

- `enabled` - `true` для включения правила, `false` для выключения;
- `ip` - IP-адрес, который нужно авторизовать;
- `mac` - MAC-адрес, который нужно авторизовать;
- `always_logged` - авторизован всегда. Может быть включено только при указанном IP;
- `user_id` - идентификатор пользователя, к которому будет применено правило;
- `comment` - комментарий к правилу, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного правила.

Изменение части правила авторизации:

```
PATCH /auth/rules/<id правила>
```

```
{
    "enabled": "boolean",
    "ip": "string" | "null",
    "mac": "string" | "null",
    "user_id":  "integer",
    "always_logged": "boolean",
    "comment": "string"
}
```

- `enabled` - `true` для включения правила, `false` для выключения;
- `ip` - IP-адрес, который нужно авторизовать;
- `mac` - MAC-адрес, который нужно авторизовать;
- `always_logged` - авторизован всегда. Может быть включено только при указанном IP;
- `user_id` - идентификатор пользователя, к которому будет применено правило;
- `comment` - комментарий к правилу, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление правила авторизации:

```
DELETE /auth/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

Сбор анонимной статистики о работе сервера:

40.1 Получение текущих настроек:

```
GET /gather_stat/settings
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - если `true`, то сбор анонимной статистики о работе сервера включен, `false` - выключен.

40.2 Изменение настроек

```
PATCH /gather_stat/settings
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

Ответ на успешный запрос: 200 OK

40.3 Лицензирование

Регистрация сервера:

```
POST /license/register
```

Json-тело запроса:

```
{
    "token": "string"
}
```

- `token` - получить токен лицензии можно в отделе продаж, он высылается в активационном письме;

Ответ на успешный запрос: 200 OK

Чтобы добавить enterprise-demo лицензию, необходимо сначала получить токен лицензии в личном кабинете. Для этого выполните действия:

1. Авторизуйтесь в личном кабинете MY.IDECO:

```
POST /20250219090034/docsUTM/api/v3/login
```

Json-тело запроса:

```
{
    "login": "string",
    "password": "string",
    "g_recaptcha_response": "string" | "null"
}
```

2. Выполните запрос на регистрацию сервера:

```
PUT /20250219090034/docsUTM/api/v3/<company_id>/go_to_product
```

- `company_id` - идентификатор компании пользователя, его можно получить по запросу `GET /20250219090034/docsUTM/api/v3/companies`.

Ответ на успешный запрос:

```
{
    "token": "string"
}
```

Используйте полученный токен в теле запроса при регистрации Ideco NGFW.

Получение информации о лицензии:

```
GET /license/info
```

Пример ответа на успешный запрос:


```
{
    "modules": {
        "active_directory": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "kaspersky_av_for_web": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "kaspersky_av_for_mail": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "application_control": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "suricata": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "advanced_content_filter": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "standard_content_filter": {
            "available": false,
            "expiration_date": 0
        },
        "ips_advanced_rules": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "cluster": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "icsd": {
            "available": true,
            "max_users_count": 10000
        }
    },
    "general": {
        "available": true,
        "reason": "",
        "not_upgrade_after": 1712400382.0,
        "tech_support_end": 1712400382.0,
        "start_date": 1708944382.2658572,
        "expiration_date": 1712400382.0
    },
    "license_type": "enterprise-demo",
    "license_id": "UTM-3883264353",
```


(continues on next page)

(продолжение с предыдущей страницы)

```
    "server_name": "UTM",
    "last_update_time": 1708944385.1747465,
    "company_id": "Ideco",
    "server_id": "OQHsviy10sEOOQXWs-8c7tnwJb4AaOvplT2iJc-im677",
    "registered": true,
    "unreliable": false,
    "has_connection": true,
    "license_server": "https://my.ideco.ru"
}
```

Если лицензия для данного сервера отсутствует:

```
{
    "registered": false,
    "has_connection": true,
    "license_server": "https://my.ideco.ru"
}
```

Получение информации о механизме обновления лицензии:

```
GET /license/update-type
```

Ответ на успешный запрос:

```
{
    "update_type": "auto" | "manual"
}
```

- `auto` - при автоматическом получении лицензии;
- `manual` - при ручной загрузке лицензии.

Изменение механизма обновления лицензии:

```
PATCH /license/update-type
```

Json-тело запроса:

```
{
    "update_type": "auto" | "manual"
}
```

Ответ на успешный запрос: 200 OK

Получение ссылки для офлайн-регистрации:

```
GET /license/license-get-offline-registration-url
```

Ответ на успешный запрос:

```
{
    "registration_url": "https://my.ideco.ru/ngfw?server_name=...hwid=...version=..."
}
```

- `server_name` - имя сервера Ideco NGFW;
- `hwid` - HWID сервера;
- `version` - версия сервера.

Получение ссылки для офлайн-регистрации сервера возможно только при ручном механизме обновления лицензии.

Загрузка файла с лицензией на NGFW:

```
PUT /license/license-upload
```

Тело запроса: файл с лицензией в формате jwt, который можно скачать в личном кабинете MY.IDECO. Более подробная информация представлена в *статье*.

Ответ на успешный запрос: 200 OK

40.4 Офлайн-обновления

Загрузить ISO-файл с офлайн-обновлением системы:

```
PUT /sysupdate/iso-upload
```

Тело запроса: ISO-файл с обновлением, который можно скачать в личном кабинете MY.IDECO по ссылке.

Ответ на успешный запрос: 200 OK

Получить версию загруженного офлайн-обновления системы:

```
GET /sysupdate/iso-upload
```

Ответ на успешный запрос:

```
{
    "uploaded_iso_version": "SystemVersion" | "null"
}
```

- `null` - если ISO-файл не был загружен;
- `SystemVersion` - объект с описанием версии для загруженного ISO-файла:

```
{
    "major": "integer",
    "minor": "integer",
    "build": "integer",
    "timestamp": "integer",
    "vendor": "string",
    "product": "UTM" | "CC",
    "kind": "FSTEK" | "VPP" | "STANDARD" | "BPF",
    "release_type": "release" | "beta" | "devel"
}
```

- `major` - мажорный номер версии (например, 18);
- `minor` - минорный номер версии (например, 1);
- `build` - номер сборки (например, 42);
- `timestamp` - время сборки версии в формате UNIX timestamp;
- `vendor` - вендор продукта, значения могут быть произвольными;
- `product` - название продукта;
- `kind` - вид продукта;
- `release_type` - тип редакции.

Запустить обновление из загруженного ISO-файла для офлайн-обновления системы:

```
POST /sysupdate/iso-install
```

Ответ на успешный запрос: 200 OK

Офлайн-обновление баз GeoIP, Iplist, Suricata:

```
PUT /20250219090034/docsUTM/api/offline-update
```

Тело запроса: архивный файл с обновлением, который можно скачать в личном кабинете MY.IDECO. Более подробная информация представлена в *статье*. Архивный файл содержит:

- `ideco-header.json` - json-файл, словарь, содержащий ключи:
  - `hwid` - должно совпадать с HWID NGFW, на который загружается обновление;
  - `pack-type` - значение должно быть равно `suricata-iplist-geoip` для архива с обновлением базы данных GeoIP, Iplist, Suricata;
  - `geoip-timestamp` - timestamp создания базы GeoIP;
  - `iplist-timestamp` - timestamp создания базы Iplist;
  - `version` - значения атрибутов версии.
- `license.jwt` - файл с лицензией для этого NGFW, содержит подписанную лицензию в формате jwt;
- `ideco-geoip.mmdb` - файл обновления базы GeoIP;
- `iplist.tar.gz` - файл обновления списка IP-адресов;
- `suricata-rules.tar.gz` - файл обновления правил Suricata.

Файлы должны быть представлены именно в такой последовательности, других файлов в архиве быть не должно.

Ответ на успешный запрос: 200 OK

Офлайн-обновление Контент-фильтра:

```
PUT /content-filter/update_archive_upload
```

Тело запроса: архивный файл с офлайн-обновлением для **Контент-фильтра**, который можно скачать в личном кабинете MY.IDECO. Более подробная информация представлена в *статье*.

Ответ на успешный запрос: 200 OK

40.5 Управление объектами

Получение идентификаторов объектов:

```
GET /aliases/<название объекта> | all
```

Ответ на успешный запрос:

```
[
    {
        "comment": "string",
        "title": "string",
        "type": "string",
        "values": [
            "string" | "integer",
            "string" | "integer"
        ],
        "id": "type.id.1"
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    },
{
        "comment": "string",
        "title": "string",
        "type": "string",
        "value": "string" | "integer",
        "id": "type.id.1"
    },
    ...
]
```

В качестве ответа будет возвращен список всех объектов, существующих в NGFW:

- `protocol.ah` - протокол AH;
- `protocol.esp` - протокол ESP;
- `protocol.gre` - протокол GRE;
- `protocol.icmp` - протокол ICMP;
- `protocol.tcp` - протокол TCP;
- `protocol.udp` - протокол UDP;
- `quota.exceeded`- IP-адреса пользователей, которые превысили квоту;
- `any` - допускается любое значение в этом поле;
- `interface.external_any` - все внешние интерфейсы (равно таблице *Подключение к провайдеру* в веб-интерфейсе и включает в себя подключения к провайдеру по Ethernet/VPN);
- `interface.external_eth` - внешние Ethernet-интерфейсы;
- `interface.external_vpn` - внешние VPN-интерфейсы;
- `interface.ipsec_any` - IPsec-интерфейсы;
- `interface.local_any` - все локальные интерфейсы;
- `interface.tunnel_any` - все туннельные интерфейсы;
- `group.id.` - идентификатор группы пользователей;
- `interface.id.`- идентификатор конкретного интерфейса;
- `interface.utm_outgoing` - исходящий трафик устройства;
- `interface.vpn_traffic` - клиентский VPN-трафик;
- `interface.wccp_gre_any` - все WCCP GRE интерфейсы;
- `hip_profile.id.` - устройства без профиля;
- `security_group.guid.` - идентификатор группы безопасности AD;
- `user.id.` - идентификатор пользователя;
- `domain.id.` - идентификатор домена;
- `ip.id.` - идентификатор IP-адреса;
- `ip_range.id.` - идентификатор объекта *Диапазон адресов*;
- `address_list.id.` - идентификатор объекта *Список IP-объектов*;
- `list_of_iplists.id.` - идентификатор объекта *Список стран*;
- `port_list.id.` - идентификатор объекта *Порты*;
- `time_list.id.` - идентификатор объекта *Расписание*;

- `subnet.id.` - идентификатор объекта *Подсеть*;
- `port_range.id.` - идентификатор объекта *Диапазон портов*;
- `port.id.` - идентификатор объекта *Порт*;
- `time_range.id.` - идентификатор объекта *Время*.

40.5.1 Создание объектов

Создание объекта IP-адрес:

```
POST /aliases/ip_addresses
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;
- `value` - IP-адрес в формате `192.168.0.0`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта IP-адрес.

Создание объекта Диапазон IP-адресов:

```
POST /aliases/ip_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "string",
    "end": "string"
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;
- `start` - первый IP-адрес в диапазоне, например, `192.168.100.2`;
- `end` - последний IP-адрес в диапазоне, например, `192.168.100.15`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Диапазон IP-адресов.

Создание объекта Подсеть:

```
POST /aliases/networks
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - адрес подсети в формате `192.168.0.0/24` либо `192.168.0.0/255.255.255.0`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Подсеть.

Создание объекта Домен:

```
POST /aliases/domains
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - домен в формате mydomain.com.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Домен.

Создание объекта Порт:

```
POST /aliases/ports
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - номер порта в формате `8080`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Порт.

Создание объекта Диапазон портов:

```
POST /aliases/port_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "integer",
    "end": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `start` - первый порт в диапазоне, например, `8080`;
- `end` - последний порт в диапазоне, например, `8090`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Диапазон портов.

Создание объекта Время:

```
POST /aliases/time_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "weekdays": [ "integer" ],
    "start": "string",
    "end": "string",
    "period": {
            "first": "integer",
            "last": "integer"
        }
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;

- `weekdays` - список дней недели, где 1-пн, 2-вт . . . 7-вс;
- `start` - начало временного отрезка в формате `ЧЧ:ММ`;
- `end` - конец временного отрезка в формате `ЧЧ:ММ`;
- `first` - момент начала срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240215000000`;
- `last` - момент окончания срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240229235959`.

Если для `period` установить значение `null`, у объекта будет включена опция **Бессрочно**.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Время.

Создание объекта Список IP-объектов:

```
POST /aliases/lists/addresses
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - идентификаторы IP-объектов, через запятую.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Список IP-объектов.

Создание объекта Список IP-адресов:

```
POST /aliases/ip_address_lists
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список IP-адресов без указания маски, либо с указанием маски подсети в виде десятичного числа 0. . . 32 или четырех десятичных чисел от 0 до 255. Например: `192.168.0.0`, `192.168.0.0/24` или `192.168.0.0/255.255.255.0`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Список IP-адресов.

Создание объекта Порты:

```
POST /aliases/lists/ports
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список портов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Порты.

Создание объекта Расписание:

```
POST /aliases/lists/times
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список идентификаторов объектов Время.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Расписание.

40.5.2 Изменение объектов

Изменение объекта IP-адрес:

```
PUT /aliases/ip_addresses/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - IP-адрес в формате `192.168.0.0`.

Ответ на успешный запрос: 200 OK

Изменение объекта Диапазон IP-адресов:

```
PUT /aliases/ip_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "string",
    "end": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `start` - первый IP-адрес в диапазоне, например, `192.168.100.2`;
- `end` - последний IP-адрес в диапазоне, например, `192.168.100.15`.

Ответ на успешный запрос: 200 OK

Изменение объекта Подсеть:

```
PUT /aliases/networks/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - адрес подсети в формате `192.168.0.0/24` либо `192.168.0.0/255.255.255.0`.

Ответ на успешный запрос: 200 OK

Изменение объекта Домен:

```
PUT /aliases/domains/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - домен в формате mydomain.com.

Ответ на успешный запрос: 200 OK

Изменение объекта Порт:

```
PUT /aliases/ports/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - номер порта в формате 8080.

Ответ на успешный запрос: 200 OK

Изменение объекта Диапазон портов:

```
PUT /aliases/port_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "integer",
    "end": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `start` - первый порт в диапазоне, например, 8080;
- `end` - последний порт в диапазоне, например, 8090.

Ответ на успешный запрос: 200 OK

Изменение объекта Время:

```
PUT /aliases/time_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "weekdays": [ "integer" ],
    "start": "string",
    "end": "string",
    "period": {
            "first": "integer",
            "last": "integer"
        }
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `weekdays` - список дней недели, где 1-пн, 2-вт . . . 7-вс;
- `start` - начало временного отрезка в формате `ЧЧ:ММ`;
- `end` - конец временного отрезка в формате `ЧЧ:ММ`;
- `first` - момент начала срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240215000000`;
- `last` - момент окончания срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240229235959`.

Если для `period` установить значение `null`, у объекта будет включена опция **Бессрочно**.

Ответ на успешный запрос: 200 OK

Изменение объекта Список IP-объектов:

```
PUT /aliases/lists/addresses/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - идентификаторы IP-объектов, через запятую.

Ответ на успешный запрос: 200 OK

Изменение объекта Список IP-адресов:

```
PUT /aliases/ip_address_lists/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;

- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список IP-адресов без указания маски, либо с указанием маски подсети в виде десятичного числа 0. . . 32 или четырех десятичных чисел от 0 до 255. Например: `192.168.0.0`, `192.168.0.0/24` или `192.168.0.0/255.255.255.0`.

Ответ на успешный запрос: 200 OK

Изменение объекта Порты:

```
PUT /aliases/lists/ports/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список портов.

Ответ на успешный запрос: 200 OK

Изменение объекта Расписание:

```
PUT /aliases/lists/times/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список идентификаторов объектов Время.

Ответ на успешный запрос: 200 OK

40.5.3 Удаление объектов

Удаление объектов:

```
DELETE /aliases/<название объекта>/<id объекта>
```

Ответ на успешный запрос: 200 OK

Названия объектов:

- `ip_addresses` - IP-адрес;
- `ip_ranges` - Диапазон IP-адресов;
- `networks` - Подсеть;
- `domains` - Домен;

- `ports` - Порт;
- `port_ranges` - Диапазон портов;
- `time_ranges` - Время;
- `ip_address_lists` - Список IP-адресов.

Удаление списка объектов:

```
DELETE /aliases/lists/<название объекта>/<id объекта>
```

Ответ на успешный запрос: 200 OK

Названия объектов:

- `addresses` - Список IP-объектов;
- `ports` - Порты;
- `times` - Расписание.

40.6 Обнаружение устройств

Получение настроек:

```
GET /netscan_backend/settings
```

Ответ на успешный запрос:

```
{
   "enabled": "boolean",
   "group_id": "integer",
   "networks": [ "string" ]
}
```

- `group_id` - идентификатор группы, в которую будут добавлены обнаруженные устройства;
- `networks` - список локальных сетей, устройства из которых будут автоматически добавлены и авторизованы на Ideco NGFW.

Изменение настроек:

```
PUT /netscan_backend/settings
```

Json-тело запроса:

```
{
   "enabled": "boolean",
   "group_id": "integer",
   "networks": [ "string" ]
}
```

- `group_id` - идентификатор группы, в которую будут добавлены обнаруженные устройства;
- `networks` - список локальных сетей, устройства из которых будут автоматически добавлены и авторизованы на Ideco NGFW.

Ответ на успешный запрос: 200 OK

40.7 Распространенные статусы

- **200** OK - Операция успешно завершена;
- **302** Found - Запрашиваемая страница была найдена / временно перенесена на другой URL;
- **400** Bad Request - Сервер не смог понять запрос из-за недействительного синтаксиса;
- **401** Unauthorized - Запрещено. Сервер понял запрос, но он не выполняет его из-за ограничений прав доступа к указанному ресурсу;
- **404** Not Found - Запрашиваемая страница не найдена. Сервер понял запрос, но не нашел соответствующего ресурса по указанному URL;
- **405** Method Not Allowed - Метод не поддерживается. Запрос был сделан методом, который не поддерживается данным ресурсом;
- **502** Bad Gateway - Ошибка шлюза. Сервер, выступая в роли шлюза или прокси-сервера, получил недействительное ответное сообщение от вышестоящего сервера;
- **542** - Валидация не пропустила тело запроса.

41. Управление интеграцией с Active Directory

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

41.1 Управление интеграцией с доменами AD

Получение статуса работы службы ad_backend:

```
GET /ad_backend/status
```

Ответ на успешный запрос:

```
{
    "msg": [ "string" ]
}
```

- `msg` - список ошибок.

Возможные ошибки:

- **no_license** - Лицензия отсутствует | License is not available

Ввод NGFW в домен:

```
POST /ad_backend/domains
```

Json-тело запроса:

```
{
    "name": "string",
    "computer_name": "string",
    "dns_ips": [ "string" ],
    "user": "string",
    "password": "string",
    "ldap_paths": [ "string" ]
}
```

- name - имя домена;
- computer_name - имя компьютера (NGFW) в домене;
- dns_ips - список IP-адресов контроллеров домена;
- user - имя пользователя, имеющего права на ввод компьютера в домен;
- password - пароль пользователя user;
- ldap_paths - список LDAP-путей, по которым будет происходит поиск групп безопасности. Максимум 10 путей, максимальная длина строки - 1024 символа. Если при интеграции передать пустой список, то поиск групп безопасности будет производиться по всему лесу доменов. Если указаны конкретные LDAP-пути, импорт прочих пользователей и групп безопасности будет невозможен.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- id - идентификатор домена.

Получение списка присоединенных доменов:

```
GET /ad_backend/domains
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "computer_name": "string",
        "dns_ips": [ "string" ],
        "user": "string",
        "ldap_paths": [ "string" ],
    },
    ...
]
```

- name - имя домена;
- computer_name - имя компьютера (NGFW) в домене;
- dns_ips - список IP-адресов контроллеров домена;
- ldap_paths - список LDAP-путей, по которым будет происходит поиск групп безопасности. Максимум 10 путей, максимальная длина строки - 1024 символа. Если при интеграции передать пустой список, то поиск групп безопасности будет производиться по всему лесу доменов. Если указаны конкретные LDAP-пути, импорт прочих пользователей и групп безопасности будет невозможен.

Выполнение «переинтеграции» с AD:

```
PUT /ad_backend/domains/<id домена>
```

Json-тело запроса:

```
{
    "computer_name": "string",
    "user": "string",
    "password": "string",
    "ldap_paths": [ "string" ]
}
```

- `computer_name` - имя компьютера (NGFW) в домене;
- `user` - имя пользователя, имеющего права на ввод компьютера в домен;
- `password` - пароль пользователя `user`;
- `ldap_paths` - список LDAP-путей, по которым будет происходит поиск групп безопасности. Максимум 10 путей, максимальная длина строки - 1024 символа. Если при интеграции передать пустой список, то поиск групп безопасности будет производиться по всему лесу доменов. Если указаны конкретные LDAP-пути, импорт прочих пользователей и групп безопасности будет невозможен.

Ответ на успешный запрос: 200 OK

Удаление интеграции с доменом:

```
DELETE /ad_backend/domains/<id домена>
```

Ответ на успешный запрос: 200 OK

При выводе NGFW из домена удаляются все настройки интеграции с контроллером домена, а также все настройки синхронизируемых групп. При этом сами группы и пользователи в них становятся локальными.

В AD созданный для NGFW компьютер не удаляется.

41.2 Управление AD правилами авторизации

Получение списка AD правил авторизации:

```
GET /web/admins/ad?format_type=JSON|CSV&columns=["id","enabled",...]
```

Параметры запроса:

- `format_type` - поддерживается `CSV` и `JSON`, по умолчанию `JSON`;
- `columns` - список столбцов, которые попадут в `CSV` отчет, по умолчанию пустой список.

Список `columns` состоит из столбцов (значения столбцов описаны ниже):

- `id`;
- `enabled`;
- `role`;
- `group_alias`;
- `comment`.

Ответ на успешный запрос в формате JSON:

```
[
    {
        "id": "string",
        "enabled": "boolean",
        "role": "integer",
        "group_alias": "string",
        "comment": "string",
    },
    ...
]
```

- `id` - идентификатор правила;
- `enabled` - правило включено/выключено (можно/нельзя по нему зайти в систему);
- `role` - идентификатор уровня доступа правила;

- `group_alias` - алиас группы безопасности;
- `comment` - комментарий.

Добавление AD правил авторизации:

```
POST /web/admins/ad
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "role": "integer",
    "group_alias": "string",
    "comment": "string",
}
```

Ответ на успешный запрос:

```
{
    "id": "string",
}
```

- `enabled` - правило включено/выключено (можно/нельзя по нему зайти в систему);
- `role` - идентификатор уровня доступа правила;
- `group_alias` - алиас группы безопасности, тип алиаса должен соответствовать типу домена;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым.

Изменение AD правил авторизации:

```
PATCH /web/admins/ad/<id правила>
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "role": "integer",
    "group_alias": "string",
    "comment": "string",
}
```

- `enabled` - правило включено/выключено (можно/нельзя по нему зайти в систему);
- `role` - идентификатор уровня доступа правила;
- `group_alias` - алиас группы безопасности, тип алиаса должен соответствовать типу домена;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым.

Ответ на успешный запрос: 200 OK

При успехе веб-сессии удаляются.

Удаление AD правил авторизации:

```
DELETE /web/admins/ad/<id правила>
```

Ответ на успешный запрос: 200 OK

41.3 Управление настройками службы

Получение настроек авторизации:

```
GET /ad_backend/settings
```

Ответ на успешный запрос:

```
{
    "authorization_by_logs": "boolean"
}
```

Изменение настроек авторизации:

```
PATCH /ad_backend/settings
```

Json-тело запроса:

```
{
    "authorization_by_logs": "boolean"
}
```

Ответ на успешный запрос: 200 OK

41.4 Получение информации об объектах контроллера домена

Получение списка групп безопасности в заданном домене:

```
GET /ad_backend/domains/<имя домена>/security_groups
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "guid": "string"
    },
    ...
]
```

- `name` - отображаемое имя группы безопасности;
- `guid` - objectGUID группы безопасности.

Получение дерева OU в заданном домене:

```
GET /ad_backend/domains/<имя домена>/tree
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "guid": "string",
        "parent_guid": "string" | "null"
    }
    ...
]
```

- `name` - отображаемое имя группы;
- `guid` - objectGUID группы;
- `parent_guid` - objectGUID родительской группы.

Дерево представлено в виде линейного списка со всеми узлами. У каждого узла есть его `guid` и `parent_guid`.

Получение списка Forward-зон контроллера домена:

```
GET /ad_backend/forward_zones
```

Ответ на успешный запрос:

```
[
    {
        "id":  "string",
        "name": "string",
        "servers": [ "string" ],
        "enabled": "boolean",
        "comment": "string"
    },
    ...
]
```

- `id` - идентификатор зоны;
- `name` - название зоны;
- `servers` - список IP-адресов DNS-серверов;
- `enabled` - включена/выключена зона;
- `comment` - комментарий, может быть пустым.

41.5 Управление настройками синхронизации групп

Получение настройки синхронизации групп:

```
GET /ad_backend/group_settings
```

Ответ на успешный запрос:

```
[
  {
    "id": "integer",
    "group_alias_id": "string",
    "search_filter": "string",
    "object_guid": "string",
    "domain_name": "string",
    "sync_type": "ldap" | "security"
  },
  ...
]
```

- `id` - идентификатор записи синхронизации;
- `group_alias_id` - идентификатор алиаса группы NGFW;
- `search_filter` - фильтр поиска в домене;
- `object_guid` - objectGUID группы из AD, с которой выполняется синхронизация;

- `domain_name` - имя домена, с которым выполняется синхронизация;
- `sync_type` - `security`, если группа синхронизируется с группой безопасности, `ldap` - если группа синхронизируется с OU.

Добавление настроек синхронизации группы с контроллером домена:

Группа безопасности импортируется как плоский список пользователей без сохранения древовидной структуры AD. Синхронизация с OU сохраняет древовидную структуру пользователей.

Если группа была локальной, а после этого запроса - синхронизируемой, то все ее текущие потомки считаются импортированными из AD. Если в домене таких пользователей нет, то они при первой же синхронизации будут перемещены в корзину.

```
POST /ad_backend/group_settings
```

Json-тело запроса:

```
{
    "search_filter": "string",
    "object_guid": "string",
    "group_alias_id": "string",
    "domain_name": "string",
    "sync_type": "ldap" | "security"
  }
```

- `search_filter` - фильтр поиска в домене;
- `object_guid` - objectGUID группы из AD, с которой выполняется синхронизация;
- `group_alias_id` - идентификатор алиаса группы NGFW;
- `domain_name` - имя домена, с которым выполняется синхронизация;
- `sync_type` - `security`, если группа синхронизируется с группой безопасности, `ldap` - если группа синхронизируется с OU.

Ответ на успешный запрос:

```
{
    "id": "sync_record_id"
}
```

- `id` - идентификатор записи синхронизации.

Изменение настроек синхронизации группы с контроллером домена:

Группа безопасности импортируется как плоский список пользователей без сохранения древовидной структуры AD. Синхронизация с OU сохраняет древовидную структуру пользователей.

```
PUT /ad_backend/group_settings/<id записи синхронизации>
```

Json-тело запроса:

```
{
    "search_filter": "string",
    "object_guid": "string",
    "domain_name": "string",
    "group_alias_id": "string",
    "sync_type": "ldap" | "security"
  }
```

- `search_filter` - фильтр поиска в домене;
- `object_guid` - objectGUID группы из AD, с которой выполняется синхронизация;

- `group_alias_id` - идентификатор алиаса группы NGFW;
- `domain_name` - имя домена, с которым выполняется синхронизация;
- `sync_type` - `security`, если группа синхронизируется с группой безопасности, `ldap` - если группа синхронизируется с OU.

Ответ на успешный запрос: 200 OK

Отмена синхронизации группы с контроллером домена:

После отмены синхронизации группы с доменом все ее потомки считаются локальными. Для авторизации таких пользователей нужно либо ставить тип авторизации «по IP», либо менять всем пароли.

```
DELETE /ad_backend/group_settings/<id группы>
```

Ответ на успешный запрос: 200 OK

42. Управление интеграцией с ALD Pro

42.1 Управление интеграцией с доменами ALD

Получение списка присоединенных доменов:

```
GET /ald_backend/domains
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "computer_name": "string",
        "dns_ips": ["string"],
        "status": "string",
        "error": "string",
    }
    ...
]
```

- `id` - идентификатор домена;
- `name` - имя домена, должно быть уникальным;
- `computer_name` - имя компьютера (NGFW) в домене;
- `dns_ips` - список IP-адресов контроллеров домена;
- `status` - статус присоединения. Статус может быть `init`, `error`, `completed`;
- `error` - ошибка, возникшая при присоединении к домену.

Ввод NGFW в домен:

```
POST /ald_backend/domains
```

JSON-тело запроса:

```
{
    "name": "string",
    "computer_name": "string",
    "dns_ips": ["string"],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "user": "string",
    "password": "string"
}
```

- `name` - имя домена;
- `computer_name` - имя компьютера (NGFW) в домене;
- `dns_ips` - список IP-адресов контроллеров домена;
- `user` - имя пользователя, имеющего права на ввод компьютера в домен;
- `password` - пароль пользователя.

Ответ на успешный запрос: 200 OK

Удалении интеграции с доменом:

```
DELETE /ald_backend/domains/<имя домена>
```

Удалить можно только домены в состоянии *error* или *complete*.

Ответ на успешный запрос: 200 OK

42.2 Управление ALD-правилами авторизации

Получение списка ALD-правил авторизации:

```
GET /web/admins/ald?format_type=JSON|CSV&columns=["id","enabled",...]
```

Параметры запроса:

- `format_type` - поддерживается `CSV` и `JSON`, по умолчанию `JSON`;
- `columns` - список столбцов, которые попадут в `CSV` отчет, по умолчанию пустой список.

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "enabled": "boolean",
        "role": "integer",
        "group_alias": "string",
        "comment": "string"
    },
    ...
]
```

- `id` - идентификатор правила;
- `enabled` - правило включено/выключено (можно/нельзя по нему зайти в систему);
- `role` - идентификатор уровня доступа правила;
- `group_alias` - алиас группы безопасности;
- `comment` - комментарий.

Добавление ALD-правил авторизации:

```
POST /web/admins/ald
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "role": "integer",
    "group_alias": "string",
    "comment": "string"
}
```

- `enabled` - правило включено/выключено (можно/нельзя по нему зайти в систему);
- `role` - идентификатор уровня доступа правила;
- `group_alias` - алиас группы безопасности, тип алиаса должен соответствовать типу домена;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "string",
}
```

Изменение ALD-правил авторизации:

```
PATCH /web/admins/ald/<id правила>
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "role": "integer",
    "group_alias": "string",
    "comment": "string"
}
```

- `enabled` - правило включено/выключено (можно/нельзя по нему зайти в систему);
- `role` - идентификатор уровня доступа правила;
- `group_alias` - алиас группы безопасности, тип алиаса должен соответствовать типу домена;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым.

Ответ на успешный запрос: 200 OK

Удаление ALD-правил авторизации:

```
DELETE /web/admins/ald/<id правила>
```

Ответ на успешный запрос: 200 OK

43. Управление администраторами

43.1 Управление локальными администраторами

Получение списка локальных администраторов:

```
GET /web/admins/local?format_type=JSON|CSV&columns=["id","name", ...]
```

- `format_type` - поддерживается `CSV` и `JSON`, по умолчанию `JSON`;
- `columns` - список столбцов, которые попадут в `CSV` отчет, по умолчанию пустой список.

Список `columns` состоит из столбцов (значения столбцов описаны ниже):

- `id`
- `name`
- `enabled`
- `login`
- `role`
- `comment`
- `password_timestamp`

Ответ на успешный запрос в формате JSON:

```
[
    {
        "id": "string",
        "enabled": "boolean",
        "name": "string",
        "login": "string",
        "role": "string",
        "comment": "string",
        "password_timestamp": "integer"
    },
    ...
]
```

Ответ на успешный запрос в формате CSV:

```
id,name,enabled,login,role,comment,password_timestamp
8aa49b1f-5711-4e5e-ab66-4828c6785b84,Administrator,True,administrator,predefined_
↪admin_write,Создано через cloud-init.,1724047828
8aa49b1f-5711-4e5e-ab66-4828c6785b92,Admin,True,administrator,predefined_admin_write,
↪Главный администратор,1724047850
```

- `id` - идентификатор администратора;
- `enabled` - аккаунт включен/выключен (можно/нельзя под ним зайти в систему);
- `name` - имя администратора;
- `login` - логин администратора;
- `role` - идентификатор уровня доступа администратора;
- `comment` - комментарий;
- `password_timestamp` - время последнего успешного изменения пароля.

Добавление локального администратора:

```
POST /web/admins/local
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "name": "string",
    "login": "string",
    "password": "string",
    "role": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "comment": "string"
}
```

- `enabled` - аккаунт включен/выключен (можно/нельзя под ним зайти в систему);
- `name` - имя, ненулевое текстовое поле, длина от 1 до 42 символов;
- `login` - логин не должен содержать `.` (одну точку) или `..` (две точки), а также символов [\:/~$!\s@]. Длина поля от 1 до 42 символов включительно;
- `password` - пароль, ненулевое текстовое поле, длина от 10 до 42 символов;
- `role` - идентификатор уровня доступа аккаунта:
  - `predefined_admin_write` - администратор (полный доступ к настройке);
  - `predefined_admin_readonly` - только просмотр;
  - `predefined_reports_view` - просмотр отчетов;
  - `predefined_reports_change` - создание отчетов (доступно создание шаблонов, расписание отправки и просмотр отчетов);
  - `predefined_security_admin` - администратор ИБ (работа с событиями безопасности);
  - `predefined_firewall_admin` - администратор файрвола (создание учетный записей, работа с правилами фильтрации, управление режимами работы файрвола);
  - `predefined_access_settings_admin` - администратор настройки доступов (настройки сетевого взаимодействии пользователей файрвола, субъектов доступа, информационных систем).
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор администратора.

Изменение настроек и пароля локального администратора:

```
PATCH /web/admins/local/<id администратора>
```

Json-тело запроса:

Все поля необязательные

```
{
    "enabled": "boolean",
    "name": "string",
    "login": "string",
    "password": "string",
    "role": "string",
    "comment": "string"
}
```

Ответ на успешный запрос: 200 OK

- `enabled` - аккаунт включен/выключен (можно/нельзя под ним зайти в систему);
- `name` - имя администратора;
- `login` - логин администратора;
- `password` - пароль (если значение `null`, пароль останется прежним);

- role - идентификатор уровня доступа аккаунта;
- comment - комментарий, максимальная длина - 255 символов, может быть пустым.

При смене пароля или отключении аккаунта веб-сессии удаляются.

Удаление локального администратора:

Последнего локального администратора удалять нельзя!

```
DELETE /web/admins/local/<id администратора>
```

Ответ на успешный запрос: 200 OK

43.2 Управление сессиями

Получение списка сессий:

```
GET /monitor_backend/admin_sessions
```

Ответ на успешный запрос:

```
[
   {
    "id": "string",
    "login": "string",
    "name": "string",
    "competence": [ "string" ],
    "role_id": "string",
    "role_name": "string",
    "domain_name": "string",
    "ip": "string",
    "auth_type": "string",
    "auth_rule_id": "string",
    "admin_id": "string",
    "login_timestamp": "integer",
    "country_code": "string"
    }
]
```

- id - идентификатор сессии администратора;
- login - логин администратора;
- name - имя администратора;
- competence - список доступных администратору компетенций (admin_write - редактирование, admin_read - чтение, allow_terminal - доступ к терминалу, reports_view - просмотр отчетов, reports_change - изменение отчетов);
- role_id - идентификатор уровня доступа аккаунта;
- role_name - название уровня доступа аккаунта;
- domain_name - домен, в котором находится авторизованный администратор (пустое значение, если auth_type не равен ad или ald);
- ip - IP-адрес, с которого авторизовался администратор;
- auth_type - тип авторизации администратора (ad, ald, local, radius);
- auth_rule_id - идентификатор правила, по которому авторизовался администратор;
- admin_id - идентификатор администратора;

- `login_timestamp` - время момента успешной авторизации администратора (число в формате `YYYYMMDDhhmmss`).
- `country_code` - код страны источника подключения. Пустая строка, если страну не удалось определить.

Удаление сессии:

```
DELETE /monitor_backend/admin_sessions/<id сессии авторизации администратора>
```

Ответ на успешный запрос: 200 OK

44. Управление пользователями

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

44.1 Управление пользователями

Получение списка пользователей:

```
GET /user_backend/users
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "login": "string",
        "parent_id": "string",
        "enabled": "boolean",
        "domain_type": "local" | "ad" | "ald" | "radius" | "device",
        "domain_name": "string",
        "ldap_guid": "string",
        "phone_number": "string",
        "comment": "string"
    },
    ...
]
```

- `id` - идентификатор пользователя;
- `name` - имя пользователя;
- `login` - логин пользователя;
- `parent_id` - идентификатор группы;
- `enabled` - соответствует опции **Запретить доступ**: `true` - включена, `false` - выключена;
- `domain_type` - тип пользователя:
  - `local` - локальный пользователь Ideco NGFW;
  - `ad` - пользователь, импортированный из Active Directory;
  - `ald` - пользователь, импортированный из ALD Pro;
  - `radius` - пользователь RADIUS-сервера;
  - `device` - клиентское устройство, подключающееся через Ideco Client в режиме Device VPN.

- domain_name - имя домена, из которого импортирован пользователь;
- ldap_guid - идентификатор объекта AD;
- phone_number - номер телефона пользователя;
- comment - комментарий.

Создание пользователя:

```
POST /user_backend/users
```

Json-тело запроса:

```
{
    "name": "string",
    "login": "string",
    "psw": "string",
    "parent_id": "string",
    "phone_number": "string" | null,
    "comment": "string"
}
```

- name - имя пользователя;
- login - логин пользователя;
- psw - пароль пользователя;
- parent_id - идентификатор группы;
- phone_number - номер телефона пользователя, не обязательно;
- comment - комментарий, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- id - идентификатор добавленного пользователя.

Если пользователь с указанным логином или именем существует, то исключение с описанием ошибки.

Изменение одного пользователя:

```
PUT /user_backend/users/<id пользователя>
```

Json-тело запроса:

```
{
    "name": "string",
    "login": "string",
    "parent_id": "string",
    "enabled": "boolean",
    "domain_type": "string",
    "domain_name": "string",
    "ldap_guid": "string",
    "phone_number": "string" | null,
    "comment": "string"
}
```

- name - имя пользователя;
- login - логин пользователя;

- `parent_id` - идентификатор группы;
- `enabled` - соответствует опции **Запретить доступ**: `true` - включена, `false` - выключена;
- `domain_type` - тип пользователя:
  - `local` - локальный пользователь Ideco NGFW;
  - `ad` - пользователь, импортированный из Active Directory;
  - `ald` - пользователь, импортированный из ALD Pro;
  - `radius` - пользователь RADIUS-сервера;
  - `device` - клиентское устройство, подключающееся через Ideco Client в режиме Device VPN.
- `domain_name` - имя домена, из которого импортирован пользователь;
- `ldap_guid` - идентификатор объекта AD;
- `phone_number` - номер телефона пользователя;
- `comment` - комментарий, может быть пустым.

Важно! Для пользователя со значением `domain_type`: `radius` можно изменить только значения полей `enabled`, `comment` и `name`. Для пользователя со значением `domain_type`: `device` нельзя изменить никакие значения.

Ответ на успешный запрос: 200 OK

Удаление пользователя:

```
DELETE /user_backend/users/<id пользователя>
```

Ответ на успешный запрос: 200 OK

Смена пароля пользователя:

```
PUT /user_backend/change_password/<id пользователя>
```

Json-тело запроса:

```
{
    "password": "string"
}
```

- `password` - новый пароль пользователя, не может быть пустым.

Ответ на успешный запрос: 200 OK

44.2 Управление группами пользователей

Получение групп пользователей:

```
GET /user_backend/groups
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "parent_id": "string",
        "domain_type": "string",
        "domain_name": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "ldap_guid": "string"
    }
]
```

- `id` - идентификатор группы;
- `name` - имя группы;
- `parent_id` - идентификатор родительской группы;
- `domain_type` - тип группы пользователей:
  - `local` - локальная группа Ideco NGFW;
  - `ad` - группа, импортированная из Active Directory;
  - `ald` - группа, импортированная из ALD Pro;
  - `radius` - группа RADIUS-сервера;
  - `device` - группа Device VPN.
- `domain_name` - имя домена, из которого импортирована группа;
- `ldap_guid` - идентификатор объекта AD.

Создание группы пользователей:

```
POST /user_backend/groups
```

Json-тело запроса:

```
{
    "name": "string",
    "parent_id": "string"
}
```

- `name` - имя группы;
- `parent_id` - идентификатор группы.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор добавленной группы.

Если группа с указанным именем у указанного предка существует, то код ответа 542 с описанием ошибки.

Изменение группы:

```
PUT /user_backend/groups/<id группы>
```

Json-тело запроса:

```
{
    "name": "string",
    "parent_id": "string",
    "domain_type": "string",
    "domain_name": "string",
    "ldap_guid": "string"
}
```

- `name` - имя группы;
- `parent_id` - идентификатор родительской группы;
- `domain_type` - тип группы пользователей:
  - `local` - локальная группа Ideco NGFW;
  - `ad` - группа, импортированная из Active Directory;
  - `ald` - группа, импортированная из ALD Pro;
  - `radius` - группа RADIUS-сервера;
  - `device` - группа Device VPN.
- `domain_name` - имя домена, из которого импортирована группа;
- `ldap_guid` - идентификатор объекта AD.

Ответ на успешный запрос: 200 OK

Удаление группы:

```
DELETE /user_backend/groups/<id группы>
```

Ответ на успешный запрос: 200 OK

44.3 Настройки RADIUS-авторизации администраторов

Получение статуса RADIUS-авторизации:

```
GET /admins-radius-auth/state
```

Ответ на успешный запрос:

```
{
  "enabled": "boolean"
}
```

- `enabled` - если `true`, то RADIUS-авторизация включена, `false` - выключена.

Изменение статуса RADIUS-авторизации:

```
PATCH /admins-radius-auth/state
```

Json-тело запроса:

```
{
  "enabled": "boolean"
}
```

- `enabled` - включить (`true`) или выключить (`false`) RADIUS-авторизацию.

Ответ на успешный запрос: 200 OK

Получение настроек RADIUS-авторизации:

```
GET /admins-radius-auth/settings
```

Ответ на успешный запрос:

```
{
    "primary": {
      "server": "string",
      "port": "integer",
      "secret": "string"
    },
    "secondary": {
      "server": "string",
      "port": "integer",
      "secret": "string"
    }
}
```

- `primary` - основной сервер RADIUS-авторизации:
  - `server` - IP-адрес или домен основного RADIUS-сервера, может быть пустой строкой;
  - `port` - порт основного RADIUS-сервера. Целое число от 1 до 65535, по умолчанию `1812`, может быть null;
  - `secret` - секрет основного RADIUS-сервера. Строка с максимальной длиной 128 символов, может быть пустой.
- `allow_external` - резервный сервер RADIUS-авторизации, нельзя настроить без основного:
  - `server` - IP-адрес или домен основного RADIUS-сервера, может быть пустой строкой;
  - `port` - порт резервного RADIUS-сервера. Целое число от 1 до 65535, может быть null;
  - `secret` - секрет основного RADIUS-сервера. Строка с максимальной длиной 128 символов, может быть пустой.

Интеграция с RADIUS-сервером считается настроенной, если заполнены поля `server` и `secret`.

Изменение настроек RADIUS-авторизации:

```
PATCH /admins-radius-auth/settings
```

Json-тело запроса:

```
{
    "primary": {
      "server": "string",
      "port": "integer",
      "secret": "string"
    },
    "secondary": {
      "server": "string",
      "port": "integer",
      "secret": "string"
    }
}
```

- `primary` - основной сервер RADIUS-авторизации:
  - `server` - IP-адрес или домен основного RADIUS-сервера, может быть пустой строкой;
  - `port` - порт основного RADIUS-сервера. Целое число от 1 до 65535, по умолчанию `1812`, может быть null;
  - `secret` - секрет основного RADIUS-сервера. Строка с максимальной длиной 128 символов, может быть пустой.
- `allow_external` - резервный сервер RADIUS-авторизации, нельзя настроить без основного:

- `server` - IP-адрес или домен основного RADIUS-сервера, может быть пустой строкой;
- `port` - порт резервного RADIUS-сервера. Целое число от 1 до 65535, может быть null;
- `secret` - секрет основного RADIUS-сервера. Строка с максимальной длиной 128 символов, может быть пустой.

Интеграция с RADIUS-сервером считается настроенной, если заполнены поля `server` и `secret`.

Ответ на успешный запрос: 200 OK

45. Управление Ideco Client

45.1 Настройка авторизации через Ideco Client

Получение настроек авторизации:

```
GET /agent_backend/wireguard/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

`enabled` - если `true`, то авторизация через Ideco Client включена, `false` - выключена.

Изменение настроек авторизации:

```
PUT /agent_backend/wireguard/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

`enabled` - `true` для включения авторизации через Ideco Client, `false` для выключения.

Ответ на успешный запрос: 200 OK

45.2 Настройки авторизации Ideco Client

Получение настроек авторизации Ideco Client:

```
GET /agent_backend/wireguard/setting
```

Ответ на успешный запрос:

```
{
    "auth_domain": "string" | "null",
    "local_tunnel": "boolean",
    "device_vpn": "boolean",
    "trusted_ca_cert": "string" | "null"
}
```

- `auth_domain` - домен/IP-адрес, в котором будет происходить аутентификация;
- `local_tunnel` - включено или выключено построение туннеля WireGuard для подключений из локальных сетей;

- `device_vpn` - включено или выключено подключение в режиме **Device VPN**;
- `trusted_ca_cert` - доверенный сертификат в формате `.pem` для проверки подлинности устройства, подключаемого в режиме **Device VPN**.

Изменение настроек авторизации Ideco Client:

```
PUT /agent_backend/wireguard/setting
```

Json-тело запроса:

```
{
    "auth_domain": "string" | "null",
    "local_tunnel": "boolean",
    "device_vpn": "boolean",
    "trusted_ca_cert": "string" | "null"
}
```

- `auth_domain` - домен/IP-адрес, в котором будет происходить аутентификация;
- `local_tunnel` - включено или выключено построение туннеля WireGuard для подключений из локальных сетей;
- `device_vpn` - включено или выключено подключение в режиме **Device VPN**;
- `trusted_ca_cert` - доверенный сертификат в формате `.pem` для проверки подлинности устройства, подключаемого в режиме **Device VPN**. Обязательно для заполнения, если разрешены подключения в режиме **Device VPN**.

Ответ на успешный запрос: 200 OK

45.3 Протокол подключения и авторизации Ideco Client

Сообщения WebSocket с типом TEXT от Ideco Client принимаются бэкендом и после обработки посылается ответное сообщение с типом TEXT, за исключением обмена информацией для ZTNA. Принимаемые и ответные сообщения содержат информацию в формате JSON.

Процесс подключения и авторизации должен проходить в несколько этапов обмена сообщениями:

45.3.1 1. Подключение и запрос соответствия версии Ideco Client

После установления соединения через WebSocket Ideco Client должен сделать запрос со своей версией и типом операционной системы, чтобы Ideco NGFW удостоверился в соответствии версии Ideco Client и при необходимости обновления передал ссылку на скачивание новой версии.

Если версия Ideco Client не совпадает с той, что требует NGFW, нужно скачать дистрибутив, разорвать соединение и установить уже с актуальной версии.

Json-тело запроса:

```
{
    "type": "version",
    "major": "integer",
    "minor": "integer",
    "build": "integer",
    "os": "windows" | "macos" | "linux"
}
```

- `type` - команда;
- `major` - мажорная версия;

- `minor` - минорная версия;
- `build` - версия сборки;
- `os` - тип ОС Ideco Client.

Ответ на успешный запрос:

```
{
    "type": "update",
    "need_update": "boolean",
    "download_url": "string"| "null",
    "version": {
        "major": "integer",
        "minor": "integer",
        "build": "integer",
        "os": "windows" | "macos" | "linux"
    }
}
```

- `need_update` - требование обновления: `true` - необходимо, `false` - не требуется;
- `download_url` - путь для скачивания дистрибутива актуальной версии Ideco Client для требуемой ОС (пример: `:14765/IdecoAgent_x64.msi`). Если обновление не требуется, то значение поля будет `null`;
- `version` - версия дистрибутива Ideco Client на Ideco NGFW. Значения полей аналогичны описанным в запросе. Если обновление не требуется, поле будет отсутствовать.

45.3.2 2. Авторизация

Если версия Ideco Client совпадает с требуемой Ideco NGFW, то Ideco Client будет разрешено инициировать авторизацию на NGFW и при необходмости установить туннельное соединение WireGuard, если подключение идет из внешних сетей. Доступно два варианта авторизации: по логину и паролю или через SSO.

Авторизация по логину и паролю:

Json-тело запроса:

```
{
    "type": "authorize",
    "login": "string",
    "password": "string"
}
```

- `login` - логин пользователя, может также содержать домен;
- `password` - пароль.

Ответ на успешный запрос:

```
{
    "type": "auth_state",
    "authorized": "boolean",
    "need_tunnel": "boolean",
    "timeout": "integer",
    "message": "string"
}
```

- `authorized` - состояние авторизации: `true` - авторизован, `false` - не авторизован;
- `need_tunnel` - требуется ли установить туннель WireGuard;

- `timeout` - время до повторной попытки авторизации в секундах в случае возникновения ошибок в процессе авторизации. Если повторная попытка авторизации не требуется, то значение будет равно 0;
- `message` - сообщение о состоянии авторизации.

Авторизация с использованием SSO:

Авторизация SSO возможна только с локальных сетей Ideco NGFW. При попытке авторизации с внешних сетей сразу произойдет отказ.

Авторизация проходит в несколько обменов пакетами:

1. Запрос на доступность SSO:

Json-тело запроса:

```
{
    "type": "sso",
    "token": "null",
    "session_token": "null",
    "domain": "string"
}
```

- `token` - SSO токен Kerberos или NTLM, для данного запроса должен быть `null`;
- `session_token` - идентификатор сессии авторизации, для данного запроса должен быть `null`;
- `domain` - домен ActiveDirectory.

Ответ на успешный запрос:

```
{
    "type": "sso",
    "status": "not_authorized" | "challenge",
    "session_token": "null",
    "access_token": "null",
    "computer_name": "string",
    "error": "string" | "null"
}
```

- `status` - статус авторизации для домена: `not_authorized` - недоступна; `challenge` - доступна, необходимо передать токен для авторизации;
- `session_token` - токен сессии авторизации;
- `access_token` - ответный токен доступа SSO;
- `computer_name` - имя сервера контроллера домена. Если `status = "not_authorized"`, поле будет отсутствовать;
- `error` - сообщение об ошибке/причине недоступности SSO авторизации для домена: `null, status = "challenge"`.

2. Запрос на авторизацию SSO:

Json-тело запроса:

```
{
    "type": "sso",
    "token": "string",
    "session_token": "string" | "null",
    "domain": "string"
}
```

- `token` - должнен содержать соответствующий токен;

- `session_token` - идентификатор сессии, если это вторая или более итерация запроса на авторизацию;
- `domain` - домен ActiveDirectory.

Если авторизация SSO еще выполняется и нужно отправить еще один запрос на авторизацию SSO (повторить этот же этап обмена пакетами), ответ на успешный запрос:

```
{
    "type": "sso",
    "status": "in_progress",
    "session_token": "string",
    "access_token": "string",
    "error": "null"
}
```

Назначение полей аналогично первому ответу (см. выше), только session_token и access_token содержат соответствующие значения.

Если авторизациая завершилась, то в ответ NGFW отправит:

```
{
    "type": "auth_state",
    "authorized": "boolean",
    "need_tunnel": "boolean",
    "timeout": "integer",
    "message": "string"
}
```

- `authorized` - состояние авторизации: `true` - авторизован, `false` - не авторизован;
- `need_tunnel` - требуется ли установить туннель WireGuard;
- `timeout` - время до повторной попытки авторизации в секундах в случае возникновения ошибок в процессе авторизации. Если повторная попытка авторизации не требуется, то значение будет равно 0;
- `message` - сообщение о состоянии авторизации.

45.4 Протокол обмена информацией для ZTNA

Запрос Ideco NGFW на получение информации от Ideco Client:

Ideco NGFW отправляет запрос на сбор информации при подключении Ideco Client. В этом запросе указаны списки параметров, которые необходимо собрать, а также интервал, с которым Client должен собирать данные.

Json-тело запроса о сборе информации:

```
{
    "type": "ztna",
    "period": "integer",
    "test_list": [
      "os_type" | "os_version" | "domain" | "kb_list" | "av_active" | "av_name" | "av_
↪version" |" av_update" | "av_scan" | "fw_active" | "fw_name" | "fw_version" |
↪"processes" | "services" | "registry"
    ],
    "kb_list": [ "string"] ,
    "proc_list": [ "string" ],
    "service_list": [ "string" ],
    "reg_key_list": [ "string" ]
}
```

- `type` - тип запроса (`ztna`);
- `period` - интервал в минутах, через который Ideco Client должен собирать и передавать информацию. Если указан интервал, равный 0, проверка и передача собранных параметров выполняется однократно;
- `test_list` - список ключевых слов, определяющий необходимость выполнения проверок заданного типа:
  - `os_type` - проверка типа операционной системы;
  - `os_version` - проверка версии операционной системы;
  - `domain` - проверка включенности в домен;
  - `kb_list` - проверка обновлений операционной системы (в объеме списка, указанного в параметре `kb_list`);
  - `av_active` - проверка, запущен ли антивирус;
  - `av_name` - проверка типа установленного антивируса;
  - `av_version` - проверка версии установленного антивируса;
  - `av_update` - проверка даты последнего обновления баз антивируса;
  - `av_scan` - проверка даты последнего антивирусного сканирования на наличие угроз;
  - `fw_active` - проверка, запущен ли межсетевой экран;
  - `fw_name` - проверка типа установленного межсетевого экрана;
  - `fw_version` - проверка версии установленного межсетевого экрана;
  - `processes` - проверка запущенных процессов (в объеме списка, указанного в параметре `proc_list`);
  - `services` - проверка списка запущенных служб (в объеме списка, указанного в параметре `service_list`);
  - `registry` - проверка наличия и значения ключей реестра Windows (в объеме списка, указанного в параметре `key_list`).
- `kb_list` - список обновлений для выполнения проверки, может быть пустым, если проверка не требуется;
- `proc_list` - список процессов для выполнения проверки, может быть пустым, если проверка не требуется;
- `service_list` - список служб для выполнения проверки, может быть пустым, если проверка не требуется;
- `reg_key_list`: - список ключей реестра для выполнения проверки: путь/имя, может быть пустым, если проверка не требуется.

Ответ Ideco Client с информацией о выполнении проверок:

Ideco Client отправляет ответ с собранной информацией об устройстве в ответ на запрос проверок. Через определенный промежуток времени Ideco Client снова собирает информацию. Если с момента последней проверки ни один из параметров не изменился, то на NGFW ничего не отправляется.

Если хотя бы один из параметров изменился с момента последнего сбора информации, то Ideco Client отправляет обновленный ответ с собранной информацией об устройстве (полный набор запрошенных сведений) и повторяет проверку через указанный интервал времени.

Формат ответа с собранной в результате проверок информацией:

```
{
    "type": "ztna",
    "node_name": "string",
    "operation_system": {
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      "type": "string",
      "version": "string",
      "domain": "string"
    },
    "kb_list": [ "string" ],
    "antivirus": [
      {
        "active": "boolean",
        "name": "string",
        "version": "string",
        "last_update": "integer" | "null",
        "last_scan": "integer" | "null",
      },
    ],
    "firewall": [
      {
        "active": "boolean",
        "name": "string",
        "version": "string",
      },
    ],
    "proc_list": [ "string" ],
    "service_list": [ "string" ],
    "reg_key_list": [
      {
        "key": "string",
        "value": "string",
      }
    ],
}
```

- `type` - тип сообщения (`ztna`);
- `node_name` - имя узла (собирается для отчетности, но не проходит никаких проверок);
- `operation_system` - результаты проверки ОС. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствуют ключевые слова `os_type`, `os_version`, `domain`:
  - `type` - тип операционной системы: `Windows`, `Linux`, `MacOS` (пустая строка, если проверка не выполнялась);
  - `version` - редакция и версия операционной системы (пустая строка, если проверка не выполнялась);
  - `domain` - имя домена (если проверка не выполнялась и в случае отсутствия домена - пустая строка).
- `kb_list` - результаты проверки установленных обновлений KB для Windows. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `kb_list`;
- `antivirus` - результаты проверок Антивируса. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`);
- `antivirus` - список результатов проверок Антивирусов (по числу установленных антивирусных пакетов). Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствуют ключевые слова `av_active`, `av_name`, `av_version`, `av_update`, `av_scan`:
  - `active` - если `true` - запущен, `false` - не запущен;
  - `name` - наименование продукта (пустая строка, если проверка не выполнялась);
  - `version` - версия продукта (пустая строка, если проверка не выполнялась);

  - `last_update` - количество полных дней, прошедших с последнего обновления баз (`null`, если проверка не выполнялась);
  - `last_scan` - количество полных дней, прошедших с последнего сканирования (`null`, если проверка не выполнялась или не проводилось сканирование).
- `firewall` - список результатов проверок межсетевых экранов (по числу установленных продуктов). Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствуют ключевые слова `fw_active`, `fw_name`, `fw_version`:
  - `active` - если `true` - активен, `false` - не активен;
  - `name` - наименование продукта (пустая строка, если проверка не выполнялась);
  - `version` - версия продукта (пустая строка, если проверка не выполнялась).
- `proc_list` - список найденных процессов. Может отсутствовать или быть пустым списком, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `processes`;
- `service_list` - список найденных служб Windows. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `services`;
- `reg_key_list` - список найденных ключей реестра. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `registry`;
  - `key` - ключ реестра (путь/имя);
  - `value` - значение параметра.

46. Мониторинг и журналы

46.1 Монитор трафика

Получение списка сессий:

```
GET /reports/traffic/sessions?<GET-параметры, разделенные знаком &>
```

Перечень необязательных GET-параметров:

- `limit: integer` - ограничение на количество срабатываний (строк). Минимальное значение `1`;
- `offset: integer` - количество строк, которые необходимо пропустить, прежде чем начать выводить записи. Минимальное значение `0`;
- `sort: [{"field": "string", "direction": "asc | desc"}]` - список параметров сортировки:
  - `field` - столбец, по которому производится сортировка;
  - `direction` - направление сортировки: `asc` - по возрастанию, `desc` - по убыванию. Сортировка производится в прямом порядке следования в массиве. По умолчанию сортируется по убыванию столбец `duration`.

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "source_ip": "string",
        "src_aliases": ["string"],
        "destination_ip": "string",
        "dst_aliases": ["string"],
        "source_proto": "string",
        "destination_proto": "string",
        "application": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "duration": "integer",
        "bps_in": "integer",
        "bps_out": "integer",
        "pps_in": "integer",
        "pps_out": "integer",
        "in_iface_alias": "string",
        "out_iface_alias": "string"
    },
    ...
]
```

- `id` - идентификатор сессии, в формате ULID;
- `source_ip` - IP-адрес источника;
- `src_aliases` - список всех id алиасов, связанных с IP-адресом источника;
- `destination_ip` - IP-адрес назначения;
- `dst_aliases` - список всех id алиасов, связанных с IP-адресом назначения;
- `source_proto` - протокол источника (если TCP или UDP, также указывается порт);
- `destination_proto` - протокол назначения (если TCP или UDP, также указывается порт);
- `application` - приложение;
- `duration` - продолжительность сессии в секундах;
- `bps_in` - входящая скорость трафика (байты в секунду);
- `bps_out` - исходящая скорость трафика (байты в секунду);
- `pps_in` - скорость обработки входящих пакетов (пакеты в секунду);
- `pps_out` - скорость обработки исходящих пакетов (пакеты в секунду);
- `in_iface_alias` - алиас сетевого интерфейса (входящий);
- `out_iface_alias` - алиас сетевого интерфейса (исходящий).

Получение списка сессий, сгруппированных по узлам локальной сети:

```
GET /reports/traffic/top/sources?<GET-параметры, разделенные знаком &>
```

Перечень необязательных GET-параметров:

- `limit: integer` - ограничение на количество срабатываний (строк). Минимальное значение `1`;
- `offset: integer` - количество строк, которые необходимо пропустить, прежде чем начать выводить записи. Минимальное значение `0`;
- `sort: [{"field": "string", "direction": "asc | desc"}]` - список параметров сортировки:
  - `field` - столбец, по которому производится сортировка;
  - `direction` - направление сортировки: `asc` - по возрастанию, `desc` - по убыванию. Сортировка производится в прямом порядке следования в массиве. По умолчанию сортируется по убыванию столбец `sessions`.

Ответ на успешный запрос:

```
[
    {
        "source_ip": "string",
        "src_aliases": ["string"],
        "bps_in": "integer",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "bps_out": "integer",
        "pps_in": "integer",
        "pps_out": "integer",
        "sessions": "integer"
    },
    ...
]
```

- `source_ip` - IP-адрес источника подключения;
- `src_aliases` - список всех идентификаторов алиасов, связанных с IP-адресом источника;
- `bps_in` - входящая скорость трафика (байты в секунду);
- `bps_out` - исходящая скорость трафика (байты в секунду);
- `pps_in` - скорость обработки входящих пакетов (пакеты в секунду);
- `pps_out` - скорость обработки исходящих пакетов (пакеты в секунду);
- `sessions` - количество сессий.

Получение списка сессий, сгруппированных по приложению:

```
GET /reports/traffic/top/applications?<GET-параметры, разделенные знаком &>
```

Перечень необязательных GET-параметров:

- `limit: integer` - ограничение на количество срабатываний (строк). Минимальное значение `1`;
- `offset: integer` - количество строк, которые необходимо пропустить, прежде чем начать выводить записи. Минимальное значение `0`;
- `sort: [{"field": "string", "direction": "asc | desc"}]` - список параметров сортировки:
  - `field` - столбец, по которому производится сортировка;
  - `direction` - направление сортировки: `asc` - по возрастанию, `desc` - по убыванию. Сортировка производится в прямом порядке следования в массиве. По умолчанию сортируется по убыванию столбец `sessions`.

Ответ на успешный запрос:

```
[
    {
        "application": "string",
        "bps_in": "integer",
        "bps_out": "integer",
        "pps_in": "integer",
        "pps_out": "integer",
        "sessions": "integer"
    },
    ...
]
```

- `application` - приложение;
- `bps_in` - входящая скорость трафика (байты в секунду);
- `bps_out` - исходящая скорость трафика (байты в секунду);
- `pps_in` - скорость обработки входящих пакетов (пакеты в секунду);
- `pps_out` - скорость обработки исходящих пакетов (пакеты в секунду);
- `sessions` - количество сессий.

46.2 Netflow

Получение состояния экспорта Netflow:

```
GET /20250219090034/docsUTM/api/netflow-export/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true`, если экспорт через Netflow включен; `false` - если выключен.

Изменение состояния экспорта Netflow:

```
PATCH /20250219090034/docsUTM/api/netflow-export/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true`, чтобы включить экспорт через Netflow; `false` - чтобы выключить.

Ответ на успешный запрос: 200 OK

Получение настроек экспорта NetFlow:

```
GET /20250219090034/docsUTM/api/netflow-export/settings
```

Ответ на успешный запрос:

```
{
    "version": "integer",
    "exported_interfaces": ["string"],
    "destination_ip": "string",
    "destination_port": "integer",
    "active_flow_interval": "integer",
    "template_tx_counter": "integer" | "null",
    "template_tx_interval": "integer" | "null"
}
```

- `version` - версия протокола NetFlow:
  - `5` - для NetFlow 5;
  - `9` - для NetFlow 9;
  - `10` - для NetFlow 10 (IPFIX).
- `exported_interfaces` - алиасы интерфейсов учета трафика в NetFlow. Допустимы алиасы Ethernet-интерфейсов, Ethernet + PPTP/L2TP/PPPoE, GRE, локального VPN-трафика, IPsec, GRE over IPsec;
- `destination_ip` - IP-адрес коллектора NetFlow. Не может иметь значение `0.0.0.0`. Если пустая строка, статистика не будет экспортироваться;
- `destination_port` - UDP-порт коллектора NetFlow. Целое число от `1` до `65535`;
- `active_flow_interval` - интервал отправки статистики NetFlow для активного потока (от `60` до `3600` секунд), через который NGFW будет отправлять на коллектор отчеты (информация о завершенных потоках отправляется по завершении);

- `template_tx_counter` - количество пакетов, через которое на коллектор будет послан шаблон. Минимум 10, максимум 6000. Должно быть `null` при значении 5 в поле `version`;
- `template_tx_interval` - количество секунд, через которое на коллектор будет послан шаблон. Минимум 60, максимум 86400. Должно быть `null` при значении 5 в поле `version`.

Изменение настроек экспорта NetFlow:

```
PATCH /20250219090034/docsUTM/api/netflow-export/settings
```

Json-тело запроса:

```
{
    "version": "integer",
    "exported_interfaces": ["string"],
    "destination_ip": "string",
    "destination_port": "integer",
    "active_flow_interval": "integer",
    "template_tx_counter": "integer" | "null",
    "template_tx_interval": "integer" | "null"
}
```

- `version` - версия протокола NetFlow:
  - 5 - для NetFlow 5;
  - 9 - для NetFlow 9;
  - 10 - для NetFlow 10 (IPFIX).
- `exported_interfaces` - алиасы интерфейсов учета трафика в NetFlow. Допустимы алиасы Ethernet-интерфейсов, Ethernet + PPTP/L2TP/PPPoE, GRE, локального VPN-трафика, IPsec, GRE over IPsec;
- `destination_ip` - IP-адрес коллектора NetFlow. Не может иметь значение `0.0.0.0`. Если пустая строка, статистика не будет экспортироваться;
- `destination_port` - UDP-порт коллектора NetFlow. Целое число от 1 до 65535;
- `active_flow_interval` - интервал отправки статистики NetFlow для активного потока (от 60 до 3600 секунд), через который NGFW будет отправлять на коллектор отчеты (информация о завершенных потоках отправляется по завершении);
- `template_tx_counter` - количество пакетов, через которое на коллектор будет послан шаблон. Минимум 10, максимум 6000. Должно быть `null` при значении 5 в поле `version`;
- `template_tx_interval` - количество секунд, через которое на коллектор будет послан шаблон. Минимум 60, максимум 86400. Должно быть `null` при значении 5 в поле `version`.

Ответ на успешный запрос: 200 OK

46.3 SNMP

Получение настройки включенности модуля:

```
GET /monitor_backend/snmp/state
```

Ответ на успешный запрос:

```
{
  "enabled": "boolean"
}
```

- `enabled` - если `true`, то модуль включен, `false` - выключен.

Включение/выключение модуля:

```
PATCH /monitor_backend/snmp/state
```

Json-тело запроса:

```
{
  "enabled": "boolean"
}
```

- `enabled` - включить (`true`) или выключить (`false`) модуль.

Ответ на успешный запрос: 200 OK

Получение состояния работы модуля:

```
GET /monitor_backend/snmp/status
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
        "msg": [ "string" ]
    }
]
```

- `name` - название модуля;
- `status` - статус модуля;
- `msg` - список сообщений, объясняющий текущее состояние.

Получение настроек SNMP:

```
GET /monitor_backend/snmp/settings
```

Ответ на успешный запрос:

```
{
    "community": "string",
    "allow_external": "boolean",
    "version": "2 | 3",
    "user": "string",
    "password": "string",
    "private_key": "string",
    "hosts": [
        "string",
        ...
    ],
    "location": "string",
    "contact": "string",
    "name": "string"
}
```

- `community` - назначение поля, может быть пустой строкой;
- `allow_external` - разрешить запросы к серверу SNMP;
- `version` - версия протокола, может принимать только значение 2 или 3;

- `user` - логин, может быть пустой строкой;
- `password` - пароль, может быть пустой строкой;
- `private_key` - приватный ключ, может быть пустой строкой;
- `hosts` - список доверенных адресов и сетей, может быть пустой строкой;
- `location` - расположение, может быть пустой строкой;
- `contact` - контактная информация, может быть пустой строкой;
- `name` - имя узла, может быть пустой строкой.

Изменение настроек SNMP:

```
PATCH /monitor_backend/snmp/settings
```

Json-тело запроса:

```
{
    "community": "string",
    "allow_external": "boolean",
    "version": "2 | 3",
    "user": "string",
    "password": "string",
    "private_key": "string",
    "hosts": [
        "string",
        ...
    ],
    "location": "string",
    "contact": "string",
    "name": "string"
}
```

- `community` - назначение поля, может быть пустой строкой;
- `allow_external` - разрешить запросы к серверу SNMP;
- `version` - версия протокола, может принимать только значение 2 или 3;
- `user` - логин, может быть пустой строкой;
- `password` - пароль, может быть пустой строкой;
- `private_key` - приватный ключ, может быть пустой строкой;
- `hosts` - список доверенных адресов и сетей, может быть пустой строкой;
- `location` - расположение, может быть пустой строкой;
- `contact` - контактная информация, может быть пустой строкой;
- `name` - имя узла, может быть пустой строкой.

Ответ на успешный запрос: 200 OK

46.4 Zabbix-агент

Получение статуса Zabbix-агента:

```
GET /monitor_backend/zabbix_agent/status
```

Ответ на успешный запрос:

```
{
  "enabled": "boolean"
}
```

- `enabled` - если `true`, то Zabbix-агент включен, `false` - выключен.

Получение настроек Zabbix-агента:

```
GET /monitor_backend/zabbix_agent
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean",
    "active_mode_enabled": "boolean",
    "passive_mode_enabled": "boolean",
    "active_mode_servers": [ "string" ],
    "passive_mode_servers": [ "string" ],
    "hostname": "string",
    "listen_port": "integer"
}
```

- `enabled` - если `true`, то Zabbix-агент включен, `false` - выключен;
- `active_mode_enabled` - если `true`, то активный режим включен, `false` - выключен;
- `passive_mode_enabled` - если `true`, то пассивный режим включен, `false` - выключен;
- `active_mode_servers` - список адресов Zabbix-серверов для активного режима. Допустимые форматы: IP-адрес, имя домена, IP-адрес:порт, домен:порт (можно указать интернационализированные доменные имена). Пустой список допустим, если активный режим выключен;
- `passive_mode_servers` - список адресов Zabbix-серверов для пассивного режима. Допустимые форматы: IP-адрес, имя домена, IP-адрес:порт, домен:порт (можно указать интернационализированные доменные имена). Пустой список допустим, если пассивный режим выключен;
- `hostname` - имя сервера Ideco NGFW, допустимые значения: английские буквы, цифры, символы `.`, `_`, `-` и `'` (пробелы в начале и конце запрещены). Максимальная длина - 64 символа, может быть пустой строкой, если активный режим выключен.
- `listen_port` - порт для подключения в пассивном режиме, разрешены только порты `10050` и `10051`.

Изменение настроек Zabbix-агента:

```
PATCH /monitor_backend/zabbix_agent
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "active_mode_enabled": "boolean",
    "passive_mode_enabled": "boolean",
    "active_mode_servers": [ "string" ],
    "passive_mode_servers": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "hostname": "string",
    "listen_port": "integer"
}
```

- `enabled` - если `true`, то Zabbix-агент включен, `false` - выключен;
- `active_mode_enabled` - если `true`, то активный режим включен, `false` - выключен;
- `passive_mode_enabled` - если `true`, то пассивный режим включен, `false` - выключен;
- `active_mode_servers` - список адресов Zabbix-серверов для активного режима. Допустимые форматы: IP-адрес, имя домена, IP-адрес:порт, домен:порт (можно указать интернационализированные доменные имена). Пустой список допустим, если активный режим выключен;
- `passive_mode_servers` - список адресов Zabbix-серверов для пассивного режима. Допустимые форматы: IP-адрес, имя домена, IP-адрес:порт, домен:порт (можно указать интернационализированные доменные имена). Пустой список допустим, если пассивный режим выключен;
- `hostname` - имя сервера Ideco NGFW, допустимые значения: английские буквы, цифры, символы `.`, `_`, `-` и `'` (пробелы в начале и конце запрещены). Максимальная длина - 64 символа, может быть пустой строкой, если активный режим выключен.
- `listen_port` - порт для подключения в пассивном режиме, разрешены только порты `10050` и `10051`.

Ответ на успешный запрос: 200 OK

46.5 Журнал трафика

Получение таблицы Журнал трафика:

```
GET /reports/report/firewall/journal?<GET-параметры, разделенные знаком &>
```

Перечень необязательных GET-параметров:

- `limit: integer` - ограничение на количество срабатываний (строк). Минимальное значение `1`;
- `offset: integer` - количество строк, которые необходимо пропустить, прежде чем начать выводить записи. Минимальное значение `0`;
- `format_type` - формат данных, поддерживает `CSV` и `JSON`, по умолчанию `JSON`;
- `sort: [{"field": "string", "direction": "asc | desc"}]` - список параметров сортировки:
  - `field` - столбец, по которому производится сортировка;
  - `direction` - направление сортировки: `asc` - по возрастанию, `desc` - по убыванию. Сортировка производится в прямом порядке следования в массиве. По умолчанию сортируется по убыванию столбец `duration`.

Ответ на успешный запрос:

```
{
    "data": [
        {
            "date_time": "integer",
            "result": "string",
            "rule_id": "integer",
            "table": "string",
            "action": "string",
            "protocol": "string",
            "ips_profile": "string",
            "ips_action": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)


```
            "ips_signature_id": "integer",
            "dpi_profile": "string",
            "dpi_action": "string",
            "dpi_app": "string",
            "dpi_protocol": "string",
            "src_ip": "string",
            "src_port": "integer",
            "src_zone": "string",
            "src_user_login": "string",
            "src_user_name": "string",
            "src_group": "string",
            "src_location_name": "string",
            "src_location_code": "string",
            "dst_ip": "string",
            "dst_port": "integer",
            "dst_zone": "string",
            "dst_user_login": "string",
            "dst_user_name": "string",
            "dst_group": "string",
            "dst_location_name": "string",
            "dst_location_code": "string",
            "dnat_rule_id": "integer",
            "dnat_ip": "string",
            "dnat_port": "integer",
            "snat_rule_id": "integer",
            "snat_ip": "string",
            "cluster_id": "string",
            "cluster_name": "string",
            "vce_id": "string",
            "vce_name": "string",
            "flow_id": "string"
        }
    ],
    "rows": "integer",
    "rows_before_limit_at_least": "integer"
}
```


- `date_time` - дата и время срабатывания правила в формате `YYYYMMDDHHMMSS`;
- `result` - общий результат проверки трафика тремя модулями фильтрации: **Файрвол**, **Предотвращение вторжений**, **Контроль приложений**:
  - `absent` - значение отсутствует;
  - `accept` - разрешить;
  - `drop` - запретить.
- `rule_id` - идентификатор правила **Файрвола**. `0` указывает на отсутствие значения;
- `table` - таблица **Файрвола**, правило котрой сработало:
  - `absent` - значение отсутствует;
  - `fwd` - таблица FORWARD **Файрвола** Ideco NGFW;
  - `fwd_a` - постправило FORWARD Ideco Center;
  - `fwd_b` - предправило FORWARD Ideco Center;
  - `fwd_s` - системное правило FORWARD;
  - `inp` - таблица INPUT **Файрвола** Ideco NGFW;

  - `inp_a` - постправило INPUT Ideco Center;
  - `inp_b` - предправило INPUT Ideco Center;
  - `inp_s` - системное правило INPUT.
- `action` - действие, определенное для трафика, подпадающего под сработавшее правило:
  - `absent` - значение отсутствует;
  - `accept` - разрешить;
  - `drop` - запретить;
  - `l7_inspection` - перенаправить в профиль.
- `protocol` - протокол соединения;
- `ips_profile` - название профиля **Предотвращения вторжений**, использованного в правиле **Файрвола**;
- `ips_action` - действие для трафика, определенное профилем:
  - `absent` - значение отсутствует;
  - `accept` - разрешить;
  - `drop` - запретить.
- `ips_signature_id` - идентификатор сигнатуры, сработавшей в профиле;
- `dpi_profile` - название профиля **Контроля приложений**, использованного в правиле **Файрвола**;
- `dpi_action` - действие для трафика, определенное профилем:
  - `absent` - значение отсутствует;
  - `accept` - разрешить;
  - `drop` - запретить.
- `dpi_app` - приложение, действие для которого определено профилем;
- `dpi_protocol` - протокол, к которому применяется действие, определенное профилем;
- `src_ip` - IP-адрес источника трафика;
- `src_port` - порт источника трафика. `0` указывает на отсутствие значения;
- `src_zone` - интерфейс или группа интерфейсов, из которых пришел трафик;
- `src_user_login` - логин пользователя источника;
- `src_user_name` - имя пользователя источника;
- `src_group` - группа, в которую входит пользователь;
- `src_location_name` - страна источника трафика (GeoIP);
- `src_location_code` - код страны источника трафика (GeoIP);
- `dst_ip` - IP-адрес назначения трафика;
- `dst_port` - порт назначения трафика. `0` указывает на отсутствие значения;
- `dst_zone` - интерфейс или группа интерфейсов, в которые вошел трафик;
- `dst_user_login` - логин пользователя назначения;
- `dst_user_name` - имя пользователя назначения;
- `dst_group` - группа, в которую входит пользователь;
- `dst_location_name` - страна назначения трафика (GeoIP);
- `dst_location_code` - код страны назначения трафика (GeoIP);

- `dnat_rule_id` - идентификатор сработавшего **DNAT** правила. `0` указывает на отсутствие значения;
- `dnat_ip` - IP-адрес, на который **Файрвол** поменял `dst_ip`;
- `dnat_port` - порт, на который **Файрвол** поменял `dst_port`;
- `snat_rule_id` - идентификатор сработавшего **SNAT** правила. `0` указывает на отсутствие значения;
- `snat_ip` - IP-адрес, на который **Файрвол** поменял `src_ip`;
- `cluster_id` - идентификатор кластера (если он настроен на NGFW);
- `cluster_name` - название кластера (если он настроен на NGFW);
- `vce_id` - идентификатор **VCE**;
- `vce_name` - название **VCE**;
- `flow_id` - идентификатор соединения. Уникален для каждой записи.
- `rows` - количество записей в `data`;
- `rows_before_limit_at_least` - абсолютное количество записей в таблице.

47. Управление правилами трафика

47.1 Основное

Подсказка: API правил трафика Ideco Center описано в статье *Управление Ideco Center*.

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

47.2 Файрвол

Получение статуса службы:

```
GET /firewall/status
```

Ответ на успешный запрос:

```
[
   {
      "name": "rules-in-kernel",
      "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
      "msg": [ "string" ]
  },
  {
        "msg": [ "string" ],
        "status": "active",
        "name": "auto-snat"
    }
]
```

- `msg` - список строк, поясняющих текущее состояние.

Получение настроек Файрвола:

47.2.1 Включенность пользовательских правил

```
GET /firewall/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - опция раздела **Файрвол**: `true` - включена, `false` - выключена.

47.2.2 Логирование правил

```
GET /firewall/settings
```

Ответ на успешный запрос:

```
{
    "automatic_snat_enabled": "boolean",
    "log_mode": "nothing" | "all" | "selected",
    "log_actions": [ "accept" | "drop" | "dnat" | "snat" | "mark_log" | "mark_not_log
↪" ]
}
```

- `automatic_snat_enabled` - включение автоматического SNAT: `true` - включен, `false`- выключен;
- `log_mode` - режим логирования;
- `log_actions` - события, которые будут логироваться.

Изменение настроек:

```
PUT /firewall/settings
```

Json-тело запроса:

```
{
    "automatic_snat_enabled": "boolean",
    "log_mode": "nothing" | "all" | "selected",
    "log_actions": [ "accept" | "drop" | "dnat" | "snat" | "mark_log" | "mark_not_log
↪" ]
}
```

- `automatic_snat_enabled` - включение автоматического SNAT: `true` - включен, `false`- выключен;
- `log_mode` - режим логирования;
- `log_actions` - события, которые будут логироваться.

Ответ на успешный запрос: 200 OK

47.2.3 Управление правилами

Получение списка правил:

- `GET /firewall/rules/forward` - раздел FORWARD;
- `GET /firewall/rules/input` - раздел INPUT;
- `GET /firewall/rules/dnat` - раздел DNAT;
- `GET /firewall/rules/snat` - раздел SNAT;
- `GET /firewall/rules/log` - раздел Логирование.

Ответ на успешный запрос: объекты FilterRuleObject, DnatRuleObject, SnatRuleObject

Объект FilterRuleObject (разделы FORWARD и INPUT)

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "hip_profiles": [ "string" ],
    "dpi_profile": "string",
    "dpi_enabled": "boolean",
    "ips_profile": "string",
    "ips_enabled": "boolean",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "drop"
}
```

- `id` - идентификатор правила.
- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;

- `dpi_profile` - строка в формате UUID, идентификатор профиля DPI. Не может быть пустой строкой, если `dpi_enabled` = `true`;
- `dpi_enabled` - если `true`, то обработка с помощью модуля **Контроль приложений** включена, `false` - выключена;
- `ips_profile` - строка в формате UUID, идентификатор профиля IPS. Не может быть пустой строкой, если `ips_enabled` = `true`;
- `ips_enabled` - если `true`, то обработка с помощью модуля **Предотвращение вторжений** включена, `false` - выключена;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

Объект DnatRuleObject (раздел DNAT)

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "dnat",
    "change_destination_address": "null" | "string",
    "change_destination_port": "null" | "string"
}
```

- `id` - идентификатор правила.
- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;

- `action` - действие:
  - `accept` - разрешить;
  - `dnat` - производить DNAT.
- `change_destination_address` - IP-адрес или диапазон IP-адресов для замены назначения, или `null`, если `action` = `accept`;
- `change_destination_port` - порт или диапазон портов для замены значения, или `null`, если `action` = `accept`.

Объект SnatRuleObject (раздел SNAT)

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "snat",
    "change_source_address": "null" | "string"
}
```

- `id` - идентификатор правила.
- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `timetable` - время действия;
- `action` - действие:
  - `accept` - разрешить;
  - `snat` - производить SNAT.
- `change_destination_address` - IP-адрес для замены источника, или `null`, если `action` = `accept`.

Добавление правила:

- `POST /firewall/rules/forward?anchor_item_id=<id правила>&insert_after={true|false}` - раздел FORWARD;

- `POST /firewall/rules/input?anchor_item_id=<id правила>&insert_after={true|false}` - раздел INPUT;
- `POST /firewall/rules/dnat?anchor_item_id=<id правила>&insert_after={true|false}` - раздел DNAT;
- `POST /firewall/rules/snat?anchor_item_id=<id правила>&insert_after={true|false}` - раздел SNAT;
- `POST /firewall/rules/log?anchor_item_id=<id правила>&insert_after={true|false}` - раздел Логирование.
  - `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое. Если отсутствует, то новое правило будет добавлено в конец таблицы;
  - `insert_after` - вставка до или после. Если значение `true` или отсутствует, то новое правило будет добавлено сразу после указанного в `anchor_item_id`. Если `false` - на месте указанного в `anchor_item_id`.

Json-тело запроса: один из объектов FilterRuleObject (разделы FORWARD и INPUT) | DnatRuleObject (раздел DNAT) | SnatRuleObject (раздел SNAT), описанных в раскрывающемся блоке ***Получение списка правил***

- В запросе не должно быть `id`, так как правило еще не создано и не имеет идентификатора.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Редактирование правила:

- `PUT /firewall/rules/forward/<id правила>` - раздел FORWARD;
- `PUT /firewall/rules/input/<id правила>` - раздел INPUT;
- `PUT /firewall/rules/dnat/<id правила>` - раздел DNAT;
- `PUT /firewall/rules/snat/<id правила>` - раздел SNAT;
- `PUT /firewall/rules/log/<id правила>` - раздел Логирование.

Json-тело запроса: один из объектов FilterRuleObject (разделы FORWARD и INPUT) | DnatRuleObject (раздел DNAT) | SnatRuleObject (раздел SNAT), которые описаны в раскрывающемся блоке ***Получение списка правил***, без поля `id`

Ответ на успешный запрос: 200 OK

Перемещение правила:

- `PATCH /firewall/rules/forward/move` - раздел FORWARD;
- `PATCH /firewall/rules/input/move` - раздел INPUT;
- `PATCH /firewall/rules/dnat/move` - раздел DNAT;
- `PATCH /firewall/rules/snat/move` - раздел SNAT;
- `PATCH /firewall/rules/log/move` - раздел Логирование.

Json-тело запроса:

```
{
    "params": {
      "id": "integer",
      "anchor_item_id": "integer",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      "insert_after": "boolean"
    }
}
```

- `id` - идентификатор перемещаемого правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно поместить перемещаемое правило;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Удаление правила:

- `DELETE /firewall/rules/forward/<id правила>` - раздел FORWARD;
- `DELETE /firewall/rules/input/<id правила>` - раздел INPUT;
- `DELETE /firewall/rules/dnat/<id правила>` - раздел DNAT;
- `DELETE /firewall/rules/snat/<id правила>` - раздел SNAT;
- `DELETE /firewall/rules/log/<id правила>` - раздел Логирование.

Ответ на успешный запрос: 200 OK

47.2.4 Счетчик срабатывания правил

Проверка включенности счетчика срабатываний правил:

```
GET /firewall/watch
```

Ответ на успешный запрос:

```
{
   "enabled": "boolean"
}
```

- `enabled` - если `true`, то счетчик включен, `false` - выключен.

Включение/выключение счетчика срабатывания правил:

```
PUT /firewall/watch
```

Json-тело запроса:

```
{
   "enabled": "boolean"
}
```

- `enabled` - `true` для включения, `false` для выключения.

Ответ на успешный запрос: 200 OK

Получение счетчиков по правилам:

- `GET /firewall/counters/forward` - раздел FORWARD;
- `GET /firewall/counters/input` - раздел INPUT;
- `GET /firewall/counters/dnat` - раздел DNAT;
- `GET /firewall/counters/snat` - раздел SNAT;
- `GET /firewall/rules/log` - раздел Логирование.

Ответ на успешный запрос:

```
[
   {
      "id": "integer",
      "packets": "integer"
   },
   ...
]
```

- `id` - идентификатор правила;
- `packets` - сумма сработанных правил.

47.2.5 Проверка прохождения трафика

Получение списка проверок:

```
GET /firewall/checks_packets
```

Ответ на успешный запрос:

```
{
    "id": "string",
    "enabled": "boolean",
    "protocol": "tcp" | "udp",
    "src_ip": "string",
    "src_port": "integer",
    "dst_ip": "string",
    "dst_port": "integer",
    "incoming_interface": "string",
    "expected_result": "drop" | "accept",
    "comment": "string"
}
```

- `id` - идентификатор проверки;
- `enabled` - включена ли данная проверка;
- `protocol` - протокол, используемый в данной проверке. Может быть `tcp` или `udp`;
- `src_ip` - адрес источника тестовых пакетов;
- `src_port` - порт источника тестовых пакетов;
- `dst_ip` - адрес назначения тестовых пакетов;
- `dst_port` - порт назначения тестовых пакетов;
- `incoming_interface` - идентификатор алиаса сетевого интерфейса, на который приходят тестовые пакеты;
- `expected_result` - ожидаемый результат выполнения проверки. Может быть `drop` или `accept`;
- `comment` - комментарий, может быть пустым.

Добавление новых проверок:

```
POST /firewall/checks_packets
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "protocol": "tcp" | "udp",
    "src_ip": "string",
    "src_port": "integer",
    "dst_ip": "string",
    "dst_port": "integer",
    "incoming_interface": "string",
    "expected_result": "drop" | "accept",
    "comment": "string"
}
```

- `enabled` - включена ли данная проверка;
- `protocol` - протокол, используемый в данной проверке. Может быть `tcp` или `udp`;
- `src_ip` - адрес источника тестовых пакетов;
- `src_port` - порт источника тестовых пакетов;
- `dst_ip` - адрес назначения тестовых пакетов;
- `dst_port` - порт назначения тестовых пакетов;
- `incoming_interface` - идентификатор алиаса сетевого интерфейса, на который приходят тестовые пакеты;
- `expected_result` - ожидаемый результат выполнения проверки. Может быть `drop` или `accept`;
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданной проверки.

Добавление новой проверки путем копирования существующей:

```
POST /firewall/checks_packets/<id проверки>/copy
```

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор созданной проверки.

Редактирование проверок:

```
PATCH /firewall/checks_packets/<id проверки>
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "protocol": "tcp" | "udp",
    "src_ip": "string",
    "src_port": "integer",
    "dst_ip": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "dst_port": "integer",
    "incoming_interface": "string",
    "expected_result": "drop" | "accept",
    "comment": "string"
}
```

- `enabled` - включена ли данная проверка;
- `protocol` - протокол, используемый в данной проверке. Может быть `tcp` или `udp`;
- `src_ip` - адрес источника тестовых пакетов;
- `src_port` - порт источника тестовых пакетов;
- `dst_ip` - адрес назначения тестовых пакетов;
- `dst_port` - порт назначения тестовых пакетов;
- `incoming_interface` - идентификатор алиаса сетевого интерфейса, на который приходят тестовые пакеты;
- `expected_result` - ожидаемый результат выполнения проверки. Может быть `drop` или `accept`;
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос: 200 OK

Удаление проверок:

```
PATCH /firewall/checks_packets/<id проверки>
```

Ответ на успешный запрос: 200 OK

Запуск проверок:

```
POST /firewall/checks_start
```

Ответ на успешный запрос: 200 OK

Получение результатов проверок:

```
GET /firewall/checks_result
```

Ответ на успешный запрос:

```
{
    "block_status": "boolean",
    "in_progress": "boolean",
    "check_datetime": "integer",
    "data": {
        "check_id": {
                "result": "drop" | "accept",
                "rule_id": "string",
                "verdict": "boolean"
                }
    }
}
```

- `block_status` - текущий статус блокировки трафика, вызванный провалом проверок;
- `in_progress` - выполняются ли проверки в данный момент;
- `check_datetime` - время выполнения последних проверок в формате `YYYYMMDDHMS`;
- `data` - словарь результатов проверок, ключ - uuid проверки;

- `result` - результат выполнения проверки, может быть `drop` или `accept`;
- `rule_id` - номер отработавшего правила. Например, `fwd.ngfw.2`;
- `verdict` - совпал ли фактический результат с ожидаемым.

Номер правила в поле `rule_id` будет отсутствовать, если пакет был заблокирован пользовательским правилом INPUT. В этом случае поле `rule_id` будет иметь вид `inp.ngfw`.

Получение настроек блокировки трафика в случае неудачных проверок:

```
GET /firewall/checks_settings
```

Ответ на успешный запрос:

```
{
    "block_traffic": "boolean"
}
```

- `block_traffic` - настройка блокировки прохождения трафика при провале какой-либо проверки.

Изменение настроек блокировки трафика в случае неудачных проверок:

```
PUT /firewall/checks_settings
```

Json-тело запроса:

```
{
    "block_traffic": "boolean"
}
```

- `block_traffic` - настройка блокировки прохождения трафика при провале какой-либо проверки.

Ответ на успешный запрос: 200 OK

47.2.6 Аппаратная фильтрация

Список поддерживаемых сетевых карт доступен в *статье*.

Получение выбранного режима фильтрации:

```
GET /firewall/hw_settings
```

Ответ на успешный запрос:

```
{
    "mode": "string"
}
```

- `mode` - режим фильтрации; допустимые значения:
  - `mac` - по MAC-адресу источника;
  - `src-ip` - по IP-адресу источника;
  - `dst-ip` - по IP-адресу назначения;
  - `src-and-dst-ip` - по IP-адресу источника и назначения.

Изменение выбранного режима фильтрации:

```
PATCH /firewall/hw_settings
```

Json-тело запроса:

```
{
    "mode": "string"
}
```

- `mode` - режим фильтрации; допустимые значения:
  - `mac` - по MAC-адресу источника;
  - `src-ip` - по IP-адресу источника;
  - `dst-ip` - по IP-адресу назначения;
  - `src-and-dst-ip` - по IP-адресу источника и назначения.

Ответ на успешный запрос: 200 OK

Управление правилами аппаратной фильтрации

Получение правил фильтрации по MAC-адресу источника:

```
GET /firewall/hw_rules_mac
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "mac": "string",
        "protocol": "integer",
        "comment": "string",
        "enabled": "boolean"

    },
    ...
]
```

- `id` - уникальный идентификатор правила;
- `mac` - MAC-адрес в формате `11:22:33:aa:bb:CC`;
- `protocol` - номер протокола сетевого уровня. Диапазон 1-65535;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов;
- `enabled` - `true`, если правило включено; `false` - если выключено.

Создание правил фильтрации по MAC-адресу источника:

```
POST /firewall/hw_rules_mac
```

Json-тело запроса:

```
{
    "mac": "string",
    "protocol": "integer",
    "comment": "string",
    "enabled": "boolean"
}
```

- `mac` - MAC-адрес в формате `11:22:33:aa:bb:CC`;

- `protocol` - номер протокола сетевого уровня. Диапазон 1-65535. **Не указывайте протокол IPv4** (значение 2048), для фильтрации на сетевом уровне используйте правила *По IP-адресу источника*, *По IP-адресу назначения*, *По IP-адресу источника и назначения*;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов;
- `enabled` - `true`, если правило включено; `false` - если выключено.

Ответ на успешный запрос:

```
{
  "id": "string",
}
```

Редактирование правил фильтрации по MAC-адресу источника:

```
PATCH /firewall/hw_rules_mac/<id правила>
```

Json-тело запроса (любые поля):

```
{
    "mac": "string",
    "protocol": "integer",
    "comment": "string",
    "enabled": "boolean"
}
```

- `mac` - MAC-адрес в формате `11:22:33:aa:bb:CC`;
- `protocol` - номер протокола сетевого уровня. Диапазон 1-65535. **Не указывайте протокол IPv4** (значение 2048), для фильтрации на сетевом уровне используйте правила *По IP-адресу источника*, *По IP-адресу назначения*, *По IP-адресу источника и назначения*;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов;
- `enabled` - `true`, если правило включено; `false` - если выключено.

Ответ на успешный запрос: 200 OK

Удаление правил фильтрации по MAC-адресу источника:

```
DELETE /firewall/hw_rules_mac/<id правила>
```

Ответ на успешный запрос: 200 OK

Получение правил фильтрации по IP-адресу источника:

```
GET /firewall/hw_rules_src_ip
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "enabled": "boolean",
    "source_ip": "string",
    "comment": "string"
    },
    ...
]
```

- `id` - уникальный идентификатор правила;

- `enabled` - `true`, если правило включено; `false` - если выключено;
- `source_ip` - IP-адрес источника без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Создание правил фильтрации по IP-адресу источника:

```
POST /firewall/hw_rules_src_ip
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "source_ip": "string",
    "comment": "string"
}
```

- `enabled` - `true`, если правило включено; `false` - если выключено;
- `source_ip` - IP-адрес источника без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

Редактирование правил фильтрации по IP-адресу источника:

```
PATCH /firewall/hw_rules_src_ip
```

Json-тело запроса (любые поля):

```
{
    "enabled": "boolean",
    "source_ip": "string",
    "comment": "string"
}
```

- `enabled` - `true`, если правило включено; `false` - если выключено;
- `source_ip` - IP-адрес источника без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Ответ на успешный запрос: 200 OK

Удаление правил фильтрации по IP-адресу источника:

```
DELETE /firewall/hw_rules_src_ip/<id правила>
```

Ответ на успешный запрос: 200 OK

Получение правил фильтрации по IP-адресу назначения:

```
GET /firewall/hw_rules_dst_ip
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "enabled": "boolean",
    "destination_ip": "string",
    "comment": "string"
    },
    ...
]
```

- `id` - уникальный идентификатор правила;
- `enabled` - `true`, если правило включено; `false` - если выключено;
- `destination_ip` - IP-адрес назначения без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Создание правил фильтрации по IP-адресу назначения:

```
POST /firewall/hw_rules_dst_ip
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "destination_ip": "string",
    "comment": "string"
}
```

- `enabled` - `true`, если правило включено; `false` - если выключено;
- `destination_ip` - IP-адрес назначения без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

Редактирование правил фильтрации по IP-адресу назначения:

```
PATCH /firewall/hw_rules_dst_ip
```

Json-тело запроса (любые поля):

```
{
    "enabled": "boolean",
    "destination_ip": "string",
    "comment": "string"
}
```

- `enabled` - `true`, если правило включено; `false` - если выключено;
- `destination_ip` - IP-адрес назначения без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Ответ на успешный запрос: 200 OK

Удаление правил фильтрации по IP-адресу назначения:

```
DELETE /firewall/hw_rules_dst_ip/<id правила>
```

Ответ на успешный запрос: 200 OK

Получение правил фильтрации по IP-адресу источника и назначения:

```
GET /firewall/hw_rules_src_dst_ip
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "enabled": "boolean",
    "source_ip": "string",
    "destination_ip": "string",
    "comment": "string"
    },
    ...
]
```

- `id` - уникальный идентификатор правила;
- `enabled` - `true`, если правило включено; `false` - если выключено;
- `source_ip` - IP-адрес источника без маски в формате `192.168.1.2`
- `destination_ip` - IP-адрес назначения без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Создание правил фильтрации по IP-адресу назначения:

```
POST /firewall/hw_rules_dst_ip
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "source_ip": "string",
    "destination_ip": "string",
    "comment": "string"
}
```

- `enabled` - `true`, если правило включено; `false` - если выключено;
- `source_ip` - IP-адрес источника без маски в формате `192.168.1.2`
- `destination_ip` - IP-адрес назначения без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

Редактирование правил фильтрации по IP-адресу назначения:

```
PATCH /firewall/hw_rules_src_dst_ip/<id правила>
```

Json-тело запроса (любые поля):

```
{
    "enabled": "boolean",
    "source_ip": "string",
    "destination_ip": "string",
    "comment": "string"
}
```

- `enabled` - `true`, если правило включено; `false` - если выключено;
- `source_ip` - IP-адрес источника без маски в формате `192.168.1.2`
- `destination_ip` - IP-адрес назначения без маски в формате `192.168.1.1`;
- `comment` - комментарий к правилу, может быть пустым. Не длиннее 256 символов.

Ответ на успешный запрос: 200 OK

Удаление правил фильтрации по IP-адресу назначения:

```
DELETE /firewall/hw_rules_src_dst_ip/<id правила>
```

Ответ на успешный запрос: 200 OK

47.2.7 Управление списками ACL

Получение списка ACL правил:

```
GET /acl/rules
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "value": [
            {
                "saddr": "string",
                "daddr": "string",
                "proto": "tcp|udp|ip|icmp",
                "sport_min": "integer",
                "sport_max": "integer",
                "dport_min": "integer",
                "dport_max": "integer",
                "action": "allow|deny"
            }
        ],
        "id": "string"
    },
    ...
]
```

Создание ACL правил:

```
POST /acl/rules
```

Json-тело запроса:

```
{
    "name": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "value": [
        {
            "saddr": "string",
            "daddr": "string",
            "proto": "tcp|udp|ip|icmp",
            "sport_min": "integer",
            "sport_max": "integer",
            "dport_min": "integer",
            "dport_max": "integer",
            "action": "allow|deny"
        }
    ]
}
```

- `name` - название правила;
- `saddr` - сеть источника, указанная в формате CIDR (адрес сети и префикс маски), пример: `10.11.12.0/24`, допустимо `0.0.0.0/0`;
- `daddr` - сеть назначения, указанная в формате CIDR (адрес сети и префикс маски), пример: `8.8.8.8/32`, допустимо `0.0.0.0/0`;
- `proto` - тип потокола;
- `sport_min` - порт источника начальный (0-65535), для протоколов без порта - оставить `0`;
- `sport_max` - порт источника конечный (0-65535), для протоколов без порта - оставить `0`;
- `dport_min` - порт назначения начальный (0-65535), для протоколов без порта - оставить `0`;
- `dport_max` - порт назначения конечный (0-65535), для протоколов без порта - оставить `0`;
- `action` - блокировать (`deny`) или пропускать (`allow`) сетевые пакеты, если для них нет подходящего правила.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

Изменение ACL правил:

```
PATCH /acl/rules/<id правила>
```

Json-тело запроса:

```
{
    "name": "string",
    "value": [
        {
            "saddr": "string",
            "daddr": "string",
            "proto": "tcp|udp|ip|icmp",
            "sport_min": "integer",
            "sport_max": "integer",
            "dport_min": "integer",
            "dport_max": "integer",
            "action": "allow|deny"
        }
    ]
}
```

- `name` - название правила;
- `saddr` - сеть источника, указанная в формате CIDR (адрес сети и префикс маски), пример: `10.11.12.0/24`, допустимо `0.0.0.0/0`;
- `daddr` - сеть назначения, указанная в формате CIDR (адрес сети и префикс маски), пример: `8.8.8.8/32`, допустимо `0.0.0.0/0`;
- `proto` - тип потокола;
- `sport_min` - порт источника начальный (0-65535), для протоколов без порта - оставить `0`;
- `sport_max` - порт источника конечный (0-65535), для протоколов без порта - оставить `0`;
- `dport_min` - порт назначения начальный (0-65535), для протоколов без порта - оставить `0`;
- `dport_max` - порт назначения конечный (0-65535), для протоколов без порта - оставить `0`;
- `action` - блокировать `deny` или пропускать `allow` сетевые пакеты, если для них нет подходящего правила.

Ответ на успешный запрос: 200 OK

Удаление ACL правил:

```
DELETE /acl/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

Получение упорядочного списка ACL правил:

```
GET /acl/acl-order
```

Ответ на успешный запрос:

```
{
    "acl_ordered_list":
    [
        {
            "src": ["string"],
            "hip": ["string"],
            "acl": "string"
        }
    ],
  ...
}
```

- `src` - источник содержит список алиасов групп пользователей или групп безопасности, таких как AD;
- `hip` - HIP-профили;
- `acl` - идентификатор правил ACL.

Изменение упорядочного списка ACL правил:

```
PATCH /acl/acl-order
```

Json-тело запроса:

```
{
    "acl_ordered_list":
    [
        {
            "src": ["string"],
            "hip": ["string"],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
            "acl": "string"
        }
    ]
}
```

- `src` - источник содержит список алиасов групп пользователей или групп безопасности, таких как AD;
- `hip` - HIP-профили;
- `acl` - идентификатор правил ACL.

Ответ на успешный запрос: 200 OK

Получение настроек ACL:

```
GET /acl/acl-state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean",
    "default_action": "deny|allow",
    "logging_enabled": "boolean"
}
```

- `enabled` - разрешить `true`, либо запретить `false` обработку трафика (при значении `false` - для всего трафика allow);
- `default_action` - блокировать `deny`, либо пропустить `allow` сетевые пакеты, если нет подходящего правила;
- `logging_enabled` - разрешить `true`, либо запретить `false` логирование действий по обработке трафика.

Изменение настроек ACL:

```
PATCH /acl/acl-state
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "default_action": "deny|allow",
    "logging_enabled": "boolean"
}
```

- `enabled` - разрешить `true`, либо запретить `false` обработку трафика (при значении `false` - для всего трафика allow);
- `default_action` - блокировать `deny`, либо пропустить `allow` сетевые пакеты, если нет подходящего правила;
- `logging_enabled` - разрешить `true`, либо запретить `false` логирование действий по обработке трафика.

Ответ на успешный запрос: 200 OK

47.3 Контроль приложений

47.3.1 Основное

Получение списка правил:

```
GET /application_control_backend/rules
```

Ответ на успешный запрос:

```
[
    {
        "action": "drop" | "accept",
        "aliases": [ "string" ],
        "comment": "string",
        "enabled": "boolean",
        "name": "string",
        "parent_id": "string",
        "protocols": [ "string" ],
        "id": "integer"
    },
    ...
 ]
```

- `action` - действие, применяемое к правилу;
- `aliases` - объекты, которые используются в правиле (например, any. Список объектов доступен по *ссылке*;
- `comment` - комментарий правила;
- `enabled` - статус правила: `true` - включено, `false` - выключено;
- `name` - имя правила;
- `parent_id` - идентификатор родительской группы серверов;
- `protocols` - список протоколов;
- `id` - идентификатор правила.

Создание нового правила:

```
POST /application_control_backend/rules
```

Json-тело запроса:

```
{
    "parent_id": "string",
    "name": "string",
    "action": "drop" | "accept",
    "comment": "string",
    "aliases": [ "string" ],
    "protocols": [ "string" ],
    "enabled": "boolean"
}
```

- `parent_id` - идентификатор родительской группы серверов;
- `name` - имя правила;
- `action` - действие, применяемое к правилу;

- `comment` - комментарий правила;
- `aliases` - объекты, которые используются в правиле (например, any. Список объектов доступен по *ссылке*;
- `protocols` - список протоколов;
- `enabled` - статус правила: `true` - включено, `false` - выключено.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Изменение правила:

```
PUT /application_control_backend/rules/<id правила>
```

Json-тело запроса:

```
{
    "parent_id": "string",
    "name": "string",
    "comment": "string",
    "aliases": [ "string" ],
    "protocols": [ "string" ],
    "action": "drop" | "accept",
    "enabled": "boolean"
}
```

- `parent_id` - идентификатор родительской группы серверов;
- `name` - имя правила;
- `comment` - комментарий правила;
- `aliases` - объекты, которые используются в правиле (например, any. Список объектов доступен по *ссылке*;
- `protocols` - список протоколов;
- `action` - действие, применяемое к правилу;
- `enabled` - статус правила: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Изменение приоритета правила:

```
PATCH /application_control_backend/rules/move
```

Json-тело запроса:

```
{
    "params": {
      "id": "integer",
      "anchor_item_id": "integer",
      "insert_after": "boolean"
    }
}
```

- `id` - идентификатор правила;

- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false`, то на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление правила:

```
DELETE /application_control_backend/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

47.4 Контент-фильтр

Включение/выключение Контент-фильтра:

47.4.1 Проверить включенность

```
GET /content-filter/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние **Контент-фильтра**: `true` - включен, `false` - выключен.

47.4.2 Включить/выключить Контент-фильтр

```
PUT /content-filter/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения **Контент-фильтра**, `false` для выключения.

Ответ на успешный запрос: 200 OK

47.4.3 Настройки

Получение настроек:

```
GET /content-filter/settings
```

Ответ на успешный запрос:

```
{
    "enabled_extended_categorizer": "boolean",
    "quic_reject_enabled": "boolean"
}
```

- `enabled_extended_categorizer` - расширенная категоризация (SkyDNS): `true` - включена, `false` - выключена;
- `quic_reject_enabled` - запрет трафика по протоколу QUIC: `true` - включен, `false` - выключен.

Изменение настроек:

```
PATCH /content-filter/settings
```

Json-тело запроса:

```
{
    "enabled_extended_categorizer": "boolean",
    "quic_reject_enabled": "boolean"
}
```

- `enabled_extended_categorizer` - расширенная категоризация (SkyDNS): `true` - включена, `false` - выключена;
- `quic_reject_enabled` - запрет трафика по протоколу QUIC: `true` - включен, `false` - выключен.

Ответ на успешный запрос: 200 OK

Получение настройки безопасного поиска:

```
GET /proxy_backend/safe_search
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние безопасного поиска: `true` - включен, `false` - выключен.

Изменение настройки безопасного поиска:

```
PUT /proxy_backend/safe_search
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения, `false` для выключения.

Ответ на успешный запрос: 200 OK

47.4.4 Категории Контент-фильтра

Получение списка категорий (предустановленных и пользовательских):

```
GET /content-filter/categories
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "type": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "name": "string",
        "comment": "string"
    },
    ...
]
```

- `id` - номер категории в формате `users.id.1` или `extended.id.1`;
- `type` - тип категории:
  - `users` - пользовательские категории;
  - `extended` - расширенные категории (SkyDNS);
  - `files` - категории для файлов;
  - `special` - специальные предопределенные категории (Прямое обращение по IP, Все категоризированные запросы, Все некатегоризированные запросы, Все запросы);
  - `other` - остальные категории.
- `name` - имя категории;
- `comment` - описание категории.

Получение списка пользовательских категорий:

```
GET /content-filter/users_categories
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "comment": "string",
        "urls": [ "string" ]
    },
    ...
]
```

- `id` - идентификатор категории в формате `users.id.1`;
- `name` - название категории, не пустая строка;
- `comment` - комментарий;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Создание пользовательской категории:

```
POST /content-filter/users_categories
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий;

- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор пользовательской категории.

Редактирование пользовательских категорий:

```
PUT /content-filter/users_categories/<id категории>
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string",
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `id` - идентификатор пользовательской категории.

47.4.5 Правила Контент-фильтра

Получение списка правил:

```
GET /content-filter/rules
```

Ответ на успешный запрос:

```
[
    {
        "id": "integer",
        "parent_id": "string",
        "name": "string",
        "comment": "string",
        "aliases": [ "string" ],
        "categories": [ "string" ],
        "http_methods": [ "string" ],
        "content_types": [ "string" ],
        "access": "allow" | "deny" | "bump" | "redirect",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "redirect_url": "string | null",
        "enabled": "boolean",
        "timetable": [ "string" ]
    },
    ...
]
```

- `id` - идентификатор правила;
- `parent_id` - идентификатор группы в Ideco Center, в которую входит Ideco NGFW, или константа «f3ffde22-a562-4f43-ac04-c40fcec6a88c» (соответствует Корневой группе);
- `name` - название правила, не пустая строка;
- `comment` - комментарий, может быть пустым (максимальная длина - 255 символов);
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `http_methods` - список методов HTTP. Доступен выбор из списка: GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE, CONNECT;
- `content_types` - список mime types;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия, список идентификаторов алиасов.

Создание правила:

```
POST /content-filter/rules?anchor_item_id=<id правила>&insert_after={true|false}
```

- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое. Если отсутствует, то новое правило будет добавлено в конец таблицы;
- `insert_after` - вставка до или после. Если значение `true` или отсутствует, то новое правило будет добавлено сразу после указанного в `anchor_item_id`. Если `false` - на месте указанного в `anchor_item_id`.

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "parent_id": "string",
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "http_methods": [ "string" ],
    "content_types": [ "string" ],
    "access": "allow" | "deny" | "bump" | "redirect",
    "redirect_url": "string" | "null",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `name` - название правила, не пустая строка;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `parent_id` - идентификатор группы в Ideco Center, в которую входит Ideco NGFW, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `http_methods` - список методов HTTP. Доступен выбор из списка: GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE, CONNECT;
- `content_types` - список mime types;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия.

Редактирование правила:

```
PUT /content-filter/rules/<id правила>
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "parent_id": "string",
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "http_methods": [ "string" ],
    "content_types": [ "string" ],
    "access": "allow | deny | bump | redirect",
    "redirect_url": "string" | "null",
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `name` - название правила, не пустая строка;
- `comment` - комментарий, может быть пустым (максимальная длина - 255 символов);
- `parent_id` - идентификатор группы в Ideco Center, в которую входит Ideco NGFW, или константа «f3ffde22-a562-4f43-ac04-c40fcec6a88c» (соответствует Корневой группе);
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;

- `http_methods` - список методов HTTP. Доступен выбор из списка: GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE, CONNECT;
- `content_types` - список mime types;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия.

Ответ на успешный запрос: 200 OK

Перемещение правила:

```
PATCH /content-filter/rules/move
```

Json-тело запроса:

```
{
    "params": {
      "id": "integer",
      "anchor_item_id": "integer",
      "insert_after": "boolean"
    }
}
```

- `id` - идентификатор правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно вставить правило, которое перемещаем;
- `insert_after` - вставка до или после. Если `true`, то правило будет вставлено сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление правила:

```
DELETE /content-filter/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

47.4.6 Морфологический анализ

Получение текущего состояние модуля морфологического анализа:

```
GET /content-filter/morph_analysis/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние: `true` - включен, `false` - выключен.

Изменение состояния модуля морфологического анализа:

```
PUT /content-filter/morph_analysis/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние: `true` - включен, `false` - выключен.

Ответ на успешный запрос: 200 OK

Получение списка словарей:

```
GET /content-filter/morph_analysis_dicts
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "title": "string",
        "comment": "string",
        "enabled": "boolean",
        "read_only": "boolean",
        "threshold": "integer",
        "words": [
            {
            "value":  "string",
            "weight": "integer"
            },
            ...
        ],
        "from_central_console": "boolean"
    },
    ...
]
```

- `id` - идентификатор словаря, формируется автоматически при добавлении правила;
- `title` - название словаря, максимальная длина - 42 символа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включен, `false` - выключен. Предустановленные словари по умолчанию выключены, дополнительные - включены;
- `read_only` - тип словаря: `true` - предустановленный, `false` - дополнительный;
- `threshold` - пороговый вес словаря, целое неотрицательное число. Может быть равен нулю, но не должен быть пустым. Если пороговый вес равен нулю, страница блокируется при наличии любого слова из словаря весом больше нуля;
- `words` - массив словарей:
  - `value` - слово/словосочетание. Длина - не больше 50 символов. Количество слов в словаре - не больше 1000;
  - `weight` - вес в словаре, целое неотрицательное число, может быть равен нулю.
- `from_central_console` - `true`, если словарь сформирован в Ideco Center, только для чтения.

Создание дополнительного словаря:

```
POST /content-filter/morph_analysis_dicts
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "enabled": "boolean",
    "read_only": "boolean",
    "threshold": "integer",
    "words": [
        {
          "value":  "string",
          "weight": "integer",
        },
        ...
    ]
}
```

- `title` - название словаря, максимальная длина - 42 символа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включен, `false` - выключен;
- `read_only` - тип словаря: `true` - предустановленный, `false` - дополнительный;
- `threshold` - пороговый вес словаря, целое неотрицательное число. Может быть равен нулю, но не должен быть пустым. Если пороговый вес равен нулю, страница блокируется при наличии любого слова из словаря весом больше нуля;
- `words` - массив словарей:
  - `value` - слово/словосочетание. Длина - не больше 50 символов. Количество слов в словаре - не больше 1000;
  - `weight` - вес в словаре, целое неотрицательное число, может быть равен нулю.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного словаря.

Редактирование дополнительного словаря:

```
PATCH /content-filter/morph_analysis_dicts/<id словаря>
```

Json-тело запроса:

```
{
    "title": "string",
    "enabled": "boolean",
    "comment": "string",
    "threshold": "integer",
    "words": [
        {
          "value":  "string",
          "weight": "integer",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        },
        ...
    ]
}
```

- `title` - название словаря, максимальная длина - 42 символа;
- `enabled` - статус: `true` - включен, `false` - выключен;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `threshold` - пороговый вес словаря, целое неотрицательное число. Может быть равен нулю, но не должен быть пустым. Если пороговый вес равен нулю, страница блокируется при наличии любого слова из словаря весом больше нуля;
- `words` - массив словарей:
  - `value` - слово/словосочетание. Длина - не больше 50 символов. Количество слов в словаре - не больше 1000;
  - `weight` - вес в словаре, целое неотрицательное число, может быть равен нулю.

Ответ на успешный запрос: 200 OK

Удаление дополнительного словаря:

```
DELETE /content-filter/morph_analysis_dicts/<id словаря>
```

Ответ на успешный запрос: 200 OK

Скачивание словаря:

```
GET /content-filter/morph_analysis_dicts/download/<id словаря>
```

Ответ на успешный запрос: файл в формате CSV. В первой строке записан пороговый вес словаря;название словаря;комментарий. В последующих строках представлены слова и их вес. Пример:

```
100;Словарь;Комментарий
слово;20
словосочетание;20
```

47.5 Предотвращение вторжений

Путь в веб-интерфейсе NGFW: **Правила трафика -> Предотвращение вторжений**

Получение статуса работы службы:

```
GET /ips/status
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
        "msg": [ "string" ]
    }
]
```

- `name` - название демона;

- `status` - статус;
- `msg` - список сообщений, объясняющий текущее состояние.

Управление статусом работы службы:

Получение текущей настройки включенности модуля

```
GET /ips/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` если модуль включен, `false` - если выключен.

Изменение настройки включенности модуля

```
PUT /ips/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

Ответ на успешный запрос: 200 OK

47.5.1 Группы сигнатур

Получение представления групп сигнатур в табличном виде:

```
GET /ips/signature_groups/table
```

Ответ на успешный запрос:

```
{
    "signature_groups": [
        {
            "classtype": "string",
            "classtype_name": "string",
            "mitre_tactics": [
                {
                    "mitre_tactic_id": "string",
                    "mitre_tactic_name": "string"
                },
                ...
            ],
            "count": "integer"
        },
        ...
    ]
}
```

- `classtype` - группа сигнатур;
- `classtype_name` - название группы сигнатур (отображается в интерфейсе Ideco NGFW);
- `mitre_tactics` - тактика согласно матрице MITRE ATT&CK, которой соответствует группа сигнатур:

- mitre_tactic_id - идентификатор тактики;
- mitre_tactic_name - название тактики.

- count - количество сигнатур в группе.

Получение представления групп сигнатур в матричном виде MITRE ATT&CK:

```
GET /ips/signature_groups/mitre
```

Ответ на успешный запрос:

```
{
    "signature_groups": [
        {
            "mitre_tactic_id": "string",
            "mitre_tactic_name": "string",
            "classtypes": [
                {
                    "classtype": "string-admin",
                    "classtype_name": "string",
                    "count": "integer"
                },
                ...
            ]
        },
        ...
    ]
}
```

- mitre_tactic_id - идентификатор тактики согласно матрице MITRE ATT&CK;
- mitre_tactic_name - название тактики;
- classtypes - группы сигнатур, соответствующие тактике:
  - classtype - группа сигнатур;
  - classtype_name - название группы сигнатур (отображается в интерфейсе Ideco NGFW);
  - count - количество сигнатур в группе.

Получение списка сигнатур определенной группы:

```
GET /ips/signatures?filter=[ { "items": [ {"column_name":"classtype","operator":
↪"equals","value":[<classtype нужной группы сигнатур (может быть несколько значений␣
↪через запятую)>]} ], "link_operator":"or" } ]
```

- "column_name":"classtype","operator":"equals","value":[<classtype нужной группы сигнатур (может быть несколько значений через запятую)>] - фильтр. Отбирает из таблицы групп сигнатур только те группы, у которых значение classtype соответствует указанным в value.

Ответ на успешный запрос:

```
{
    "signatures": [
        {
            "action": "string",
            "protocol": "string",
            "flow": "string",
            "classtype": "string-admin",
            "sid": "integer",
            "signature_severity": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
            "mitre_tactic_id": "string",
            "signature_source": "string",
            "msg": "string",
            "source": "string",
            "source_ports": "string",
            "destination": "string",
            "destination_ports": "string",
            "updated_at": "string"
        },
        ...
    ]
}
```

- `action` - действие для трафика, соответствующего сигнатуре:
  - `pass` - **Пропускать**;
  - `alert` - **Предупреждать**;
  - `drop` - **Блокировать**;
  - `rejectsrc` - **Отправлять RST узлу источника**;
  - `rejectdst` - **Отправлять RST узлу назначения**;
  - `rejectboth` - **Отправлять RST обоим**.
- `protocol` - протокол (`tcp`, `udp`, `icmp`, `ip`). Возможные значения представлены по ссылке;
- `flow` - направление трафика (`client2server`, `server2client`, `-`);
- `classtype` - группа, к которой относится сигнатура;
- `sid` - идентификатор сигнатуры;
- `signature_severity` - уровень угрозы;
- `mitre_tactic_id` - тактика согласно матрице MITRE ATT&CK;
- `signature_source` - источник сигнатуры:
  - `standard` - стандартные правила;
  - `advanced` - правила IPS от Лаборатории Касперского;
  - `custom` - пользовательские правила.
- `msg` - название сигнатуры;
- `source` - источник подключения;
- `source_ports` - порты источника;
- `destination` - назначение;
- `destination_ports` - порты назначения;
- `updated_at` - дата в формате `YYYY-MM-DD` или строка со значением `-`.

Получение оригинального содержания сигнатуры:

```
GET /ips/signatures/<sid>
```

- `sid` - идентификатор сигнатуры.

Ответ на успешный запрос:

```
{
    "signature": "string"
}
```

- `signature` - содержание сигнатуры.

47.5.2 Пользовательские сигнатуры

Получение списка пользовательских сигнатур:

```
GET /ips/custom
```

Ответ на успешный запрос:

```
{
    "signatures": [
        {
            "action": "string",
            "protocol": "string",
            "flow": "string",
            "classtype": "string-admin",
            "sid": "integer",
            "signature_severity": "string",
            "mitre_tactic_id": "string",
            "signature_source": "string",
            "msg": "string",
            "source": "string",
            "source_ports": "string",
            "destination": "string",
            "destination_ports": "string",
            "updated_at": "string"
        },
        ...
    ]
}
```

- `action` - действие для трафика, соответствующего сигнатуре:
  - `pass` - **Пропускать**;
  - `alert` - **Предупреждать**;
  - `drop` - **Блокировать**;
  - `rejectsrc` - **Отправлять RST узлу источника**;
  - `rejectdst` - **Отправлять RST узлу назначения**;
  - `rejectboth` - **Отправлять RST обоим**.
- `protocol` - протокол (`tcp`, `udp`, `icmp`, `ip`). Возможные значения представлены по ссылке;
- `flow` - направление трафика (`client2server`, `server2client`, `-`);
- `classtype` - группа, к которой относится сигнатура;
- `sid` - идентификатор сигнатуры;
- `signature_severity` - уровень угрозы;
- `mitre_tactic_id` - тактика согласно матрице MITRE ATT&CK;
- `signature_source` - источник сигнатуры:

  - `standard` - стандартные правила;
  - `advanced` - правила IPS от Лаборатории Касперского;
  - `custom` - пользовательские правила.
- `msg` - название сигнатуры;
- `source` - источник подключения;
- `source_ports` - порты источника;
- `destination` - назначение;
- `destination_ports` - порты назначения;
- `updated_at` - дата в формате `YYYY-MM-DD` или строка со значением `-`.

Создание пользовательской сигнатуры вручную:

```
POST /ips/custom
```

Json-тело запроса:

```
{
    "comment": "string",
    "rule": "string"
}
```

- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `rule` - строка с правилом, не более 8196 символов, переводы строк в ней запрещены.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданной сигнатуры.

Загрузка пользовательских сигнатур из файла:

```
POST /ips/custom_rules_file
```

Файл загружается как тело запроса, он должен иметь текстовый формат text/plain, максимальный размер файла - 32 MB.

Ответ на успешный запрос:

```
{
    "count": "integer"
}
```

- `count` - количество загруженных правил.

Редактирование пользовательской сигнатуры:

```
PATCH /ips/custom/<sid>
```

- `sid` - идентификатор сигнатуры

Json-тело запроса (все или некоторые поля):

```
{
    "comment": "string",
    "rule": "string"
}
```

- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `rule` - строка с правилом, не более 8196 символов, переводы строк в ней запрещены.

Ответ на успешный запрос: 200 OK

Удаление пользовательской сигнатуры:

```
DELETE /ips/custom/<sid>
```

- `sid` - идентификатор сигнатуры

Ответ на успешный запрос: 200 OK

47.5.3 Обновление баз

Получение статуса обновления баз правил Suricata и GeoIP:

```
GET /ips/update
```

Ответ на успешный запрос:

```
{
    "status": "up_to_date" | "updating" | "failed_to_update|disabled",
    "msg": "i18n_string",
    "last_update": "float" | "null"
}
```

- `status` - текущий статус обновления баз:
  - `up_to_date` - базы успешно обновлены;
  - `updating` - скачиваются новые базы;
  - `failed_to_update` - последняя попытка обновления баз завершилась неудачно;
  - `disabled` - обновление баз выключено.
- `msg` - текстовое описание статуса обновления баз;
- `last_update` - время последнего успешного обновления баз.

Получение статуса обновления расширенных баз правил Suricata и GeoIP:

```
GET /ips/update_advanced
```

Ответ на успешный запрос:

```
{
    "status": "up_to_date" | "updating" | "failed_to_update|disabled",
    "msg": "i18n_string",
    "last_update": "float" | "null"
}
```

- `status` - текущий статус обновления баз:
  - `up_to_date` - базы успешно обновлены;
  - `updating` - скачиваются новые базы;

- `failed_to_update` - последняя попытка обновления баз завершилась неудачно;
- `disabled` - обновление баз выключено.

- `msg` - текстовое описание статуса обновления баз;
- `last_update` - время последнего успешного обновления баз.

Запуск принудительного обновления баз:

```
POST /ips/update
```

Ответ на успешный запрос: 200 OK

47.5.4 Сети, защищенные от вторжений

Получение списка локальных подсетей:

```
GET /ips/nets
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "address": "string"
  },
  ...
]
```

- `id` - идентификатор подсети;
- `address` - адрес подсети (например, `192.168.0.0/16`).

Добавление новой локальной подсети:

```
POST /ips/nets
```

Json-тело запроса:

```
{
    "address": "string"
  }
```

- `address` - адрес подсети (например, `192.168.0.0/16`).

Удаление локальной подсети:

```
DELETE /ips/nets/<id локальной подсети>
```

Ответ на успешный запрос: 200 OK

47.6 Исключения

47.6.1 Основное

Получение списка исключений объектов:

```
GET /ips/bypass
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "aliases": [ "string" ],
        "comment": "string",
        "enabled": "boolean"
    },
    ...
]
```

- `id` - идентификатор исключения;
- `aliases` - список идентификаторов объектов. Допустимые типы: IP-адрес, Диапазон IP-адресов, Список IP-объектов, Список IP-адресов, Подсеть, Домен, Пользователь, Группа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - состояние исключения: `true` - включено, `false` - выключено.

Добавление исключения объектов:

```
POST /ips/bypass
```

Json-тело запроса:

```
{
    "aliases": [ "string" ],
    "comment": "string",
    "enabled": "boolean"
}
```

- `aliases` - список идентификаторов объектов. Допустимые типы: IP-адрес, Диапазон IP-адресов, Список IP-объектов, Список IP-адресов, Подсеть, Домен, Пользователь, Группа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - состояние исключения: `true` - включено, `false` - выключено.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного исключения.

Изменение исключения объектов:

```
PATCH /ips/bypass/<id исключения>
```

Json-тело запроса:

```
{
    "aliases": [ "string" ],
    "comment": "string",
    "enabled": "boolean"
}
```

- `aliases` - список идентификаторов объектов. Допустимые типы: IP-адрес, Диапазон IP-адресов, Список IP-объектов, Список IP-адресов, Подсеть, Домен, Пользователь, Группа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - состояние исключения: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Удаление существующего исключения объектов:

```
DELETE /ips/bypass/<id исключения>
```

Ответ на успешный запрос: 200 OK

48. Управление профилями безопасности

48.1 Предотвращение вторжений

Путь в веб-интерфейсе NGFW: **Профили безопасности -> Предотвращение вторжений**

Получение списка профилей:

```
GET /ips/profiles
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "name": "string",
    "comment": "string"
  },
  ...
]
```

- `id` - идентификатор профиля или фиксированная строка `__DEFAULT_IPS_PROFILE_ID__` (шаблонный профиль);
- `name` - название профиля, максимальная длина - 42 символа;
- `comment` - комментарий, максимальная длина - 255 символов.

Шаблонный профиль отображается в режиме **Только для чтения**. Идентификатор шаблонного профиля не может быть использован в запросах на изменение/удаление профиля и на создание/изменение/перемещение/удаление правил профиля.

Создание профиля:

```
POST /ips/profiles
```

Json-тело запроса::

```
{
    "name": "string",
    "comment": "string"
}
```

- `name` - название профиля, максимальная длина - 42 символа;
- `comment` - комментарий, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор профиля.

Изменение профиля:

```
PATCH /ips/profiles/<id профиля>
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string"
}
```

- `name` - название профиля, максимальная длина - 42 символа;
- `comment` - комментарий, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление профиля:

```
DELETE /ips/profiles/<id профиля>
```

Ответ на успешный запрос: 200 OK

Получение списка правил профиля:

```
GET /ips/profiles/<profile_id>/rules
```

- `profile_id` - идентификатор профиля, список правил которого запрашивается (без скобок и кавычек).

Ответ на успешный запрос:

```
[
  {
    "id": "integer",
    "filters": [
      {
        "key": "sid" | "mitre_tactic_id" | "protocol" | "signature_severity" | "flow"␣
↪| "classtype",
        "operator": "equals",
        "values": [ "string" | "integer" ],
     },
    ...
    ]
    "action": "default" | "alert" | "drop" | "pass",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "comment": "string"
  },
  ...
]
```

- `id` - номер правила выбора сигнатур;
- `filters` - список фильтров правила (список не может быть пустым):
  - `key` - поле фильтра (`sid` - идентификатор, `mitre_tactic_id` - тактика MITRE, `protocol` - протокол, `signature_severity` - уровень серьезности, `flow` - направление, `classtype` - класс);
  - `operator` - оператор, только `equals`;
  - `values` - список значений, которые должны принимать поля `key` (если `key` - `sid`, то `values` - число).
- `action` - строка с действием при срабатывании правила;
- `comment` - комментарий, максимальная длина 255 символов.

Создание правила в профиле:

```
POST /ips/profiles/<profile_id>/rules?anchor_item_id=<integer>&insert_after=
↪<true|false>
```

- `profile_id` - идентификатор профиля, в котором создается правило (без скобок и кавычек);
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое;
- `insert_after` - вставка до или после. Если `true` или отсутствует, то вставить правило сразу после указанного в `anchor_item_id`. Если `false`, то на месте указанного в `anchor_item_id`.

Json-тело запроса:

```
{
    "filters": [
       {
        "key": "sid" | "mitre_tactic_id" | "protocol" | "signature_severity" | "flow"␣
↪| "classtype",
        "operator": "equals",
        "values": [ "string" | "integer" ]
      },
      ...
    ],
    "action": "default" | "alert" | "drop" | "pass",
    "comment": "string"
}
```

- `filters` - список фильтров правила (список не может быть пустым):
  - `key` - поле фильтра (`sid` - идентификатор, `mitre_tactic_id` - тактика MITRE, `protocol` - протокол, `signature_severity` - уровень серьезности, `flow` - направление, `classtype` - класс);
  - `operator` - оператор, только `equals`;
  - `values` - список значений, которые должны принимать поля `key` (если `key` - `sid`, то `values` - число).
- `action` - строка с действием при срабатывании правила;
- `comment` - комментарий, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
  "id": "integer"
}
```

- `id` - номер правила выбора сигнатур.

Изменение правила в профиле:

```
PATCH /ips/profiles/<profile_id>/rules/<rule_id>
```

- `profile_id` - идентификатор профиля, в котором изменяется правило;
- `rule_id` - идентификатор правила в профиле.

Json-тело запроса: (некоторые или все поля объекта)

```
{
    "filters": [
      {
        "key": "sid" | "mitre_tactic_id" | "protocol" | "signature_severity" | "flow"␣
↪| "classtype",
        "operator": "equals",
        "values": [ "string" | "integer" ]
       },
      ...
    ],
    "action": "default" | "alert" | "drop" | "pass",
    "comment": "string"
}
```

- `filters` - список фильтров правила (список не может быть пустым):
  - `key` - поле фильтра (`sid` - идентификатор, `mitre_tactic_id` - тактика MITRE, `protocol` - протокол, `signature_severity` - уровень серьезности, `flow` - направление, `classtype` - класс);
  - `operator` - оператор, только `equals`;
  - `values` - список значений, которые должны принимать поля `key` (если `key` - `sid`, то `values` - число).
- `action` - строка с действием при срабатывании правила;
- `comment` - комментарий, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Перемещение правила в профиле:

```
PATCH /ips/profiles/rules/move
```

Json-тело запроса::

```
{
    "params": {
        "profile_id": "string",
        "rule_id": "integer",
        "anchor_item_id": "integer",
        "insert_after": "boolean"
    }
}
```

- `profile_id` - идентификатор профиля, в котором перемещается правило;
- `rule_id` - идентификатор правила в профиле;

- anchor_item_id - идентификатор правила, выше или ниже которого нужно разместить rule_id;
- insert_after - вставить до (false) или после (true) правила anchor_item_id.

Ответ на успешный запрос: 200 OK

Удаление правила в профиле:

```
DELETE /ips/profiles/<profile_id>/rules/<rule_id>
```

- profile_id - идентификатор профиля, в котором удаляется правило;
- rule_id - идентификатор правила в профиле.

Ответ на успешный запрос: 200 OK

Создание профиля с правилами:

```
POST /ips/profiles-create-with-rules
```

Json-тело запроса::

```
{
    "name": "string",
    "comment": "string",
    "rules": [
          {
          "filters": [
                {
                "key": "sid" | "mitre_tactic_id" | "protocol" | "signature_severity"␣
↪| "flow" | "classtype",
                "operator": "equals",
                "values": [ "string" | "integer" ]
                  },
                  ...
                ],
          "action": "default" | "alert" | "drop" | "pass",
          "comment": "string"
          },
          ...
       ]
    }
```

- name - название профиля, максимальная длина - 42 символа;
- comment - комментарий, максимальная длина - 255 символов;
- rules - список правил профиля:
  - filters - список фильтров правила (список не может быть пустым):
    - key - поле фильтра (sid - идентификатор, mitre_tactic_id - тактика MITRE, protocol - протокол, signature_severity - уровень серьезности, flow - направление, classtype - класс);
    - operator - оператор, только equals;
    - values - список значений, которые должны принимать поля key (если key - sid, то values - число).
  - action - строка с действием при срабатывании правила;
  - comment - комментарий, максимальная длина 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- id - идентификатор созданного профиля с правилами.

Копирование профиля с правилами:

```
POST /ips/profiles/<id профиля>/copy
```

В качестве id профиля может быть указана фиксированная строка __DEFAULT_IPS_PROFILE_ID__ для создания копии шаблонного профиля. Поле **Комментарий** будет заменено на пустую строку.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- id - идентификатор созданного профиля.

Получение списка сигнатур в определенном профиле:

```
GET /ips/profiles/<id профиля>/signatures
```

В качестве id профиля может быть указана фиксированная строка __DEFAULT_IPS_PROFILE_ID__ для получения списка сигнатур шаблонного профиля.

Ответ на успешный запрос:

```
{
    "signatures": [
        {
            "action": "string",
            "protocol": "string",
            "flow": "string",
            "classtype": "string-admin",
            "sid": "integer",
            "signature_severity": "string",
            "mitre_tactic_id": "string",
            "signature_source": "string",
            "msg": "string",
            "source": "string",
            "source_ports": "string",
            "destination": "string",
            "destination_ports": "string",
            "updated_at": "string"
        },
        ...
    ]
}
```

- action - действие для трафика, соответствующего сигнатуре:
  - pass - **Пропускать**;
  - alert - **Предупреждать**;
  - drop - **Блокировать**;
  - rejectsrc - **Отправлять RST узлу источника**;
  - rejectdst - **Отправлять RST узлу назначения**;

  - `rejectboth` - **Отправлять RST обоим**.
- `protocol` - протокол (`tcp`, `udp`, `icmp`, `ip`). Возможные значения представлены по ссылке;
- `flow` - направление трафика (`client2server`, `server2client`, `-`);
- `classtype` - группа, к которой относится сигнатура;
- `sid` - идентификатор сигнатуры;
- `signature_severity` - уровень угрозы;
- `mitre_tactic_id` - тактика согласно матрице MITRE ATT&CK;
- `signature_source` - источник сигнатуры:
  - `standard` - стандартные правила;
  - `advanced` - правила IPS от Лаборатории Касперского;
  - `custom` - пользовательские правила.
- `msg` - название сигнатуры;
- `source` - источник подключения;
- `source_ports` - порты источника;
- `destination` - назначение;
- `destination_ports` - порты назначения;
- `updated_at` - дата в формате `YYYY-MM-DD` или строка со значением `-`.

Получение количества сигнатур профиля по действиям для всех профилей:

```
GET /ips/profiles/actions-counts
```

Ответ на успешный запрос:

```
{
    "profile_id": {
      "pass": "integer",
      "alert": "integer",
      "drop": "integer",
      "rejectsrc": "integer",
      "rejectdst": "integer",
      "rejectboth": "integer"
    },
    ...
}
```

- `profile_id` - идентификатор профиля или фиксированная строка `__DEFAULT_IPS_PROFILE_ID__` (шаблонный профиль):
  - `pass` - **Пропускать**;
  - `alert` - **Предупреждать**;
  - `drop` - **Блокировать**;
  - `rejectsrc` - **Отправлять RST узлу источника**;
  - `rejectdst` - **Отправлять RST узлу назначения**;
  - `rejectboth` - **Отправлять RST обоим**.

Получение количества сигнатур профиля по действиям для конкретного профиля:

```
GET /ips/profiles/<id профиля>/actions-counts
```

Ответ на успешный запрос:

```
{
    "rule_id": {
      "pass": "integer",
      "alert": "integer",
      "drop": "integer",
      "rejectsrc": "integer",
      "rejectdst": "integer",
      "rejectboth": "integer"
    },
    ...
}
```

- `rule_id` - идентификатор правила в профиле:
  - `pass` - **Пропускать**;
  - `alert` - **Предупреждать**;
  - `drop` - **Блокировать**;
  - `rejectsrc` - **Отправлять RST узлу источника**;
  - `rejectdst` - **Отправлять RST узлу назначения**;
  - `rejectboth` - **Отправлять RST обоим**.

Получение профилей Предотвращения вторжений, которые содержат определенную сигнатуру:

```
GET /ips/signatures/<sid>/profiles
```

- `sid` - идентификатор сигнатуры.

Ответ на успешный запрос:

```
{
    "id": "string",
    "name": "string"
}
```

- `id` - идентификатор профиля;
- `name` - название профиля.

48.2 Профили Web Application Control (WAF)

Получение списка профилей:

```
GET /reverse_proxy_backend/waf/profiles
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "name": "string",
    "detection_only": "boolean",
    "disabled_categories": ["string"],
    "exceptions": [
      {
        "id": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "rule_id": "integer",
        "comment": "string",
        "enabled": "boolean"
      },
      ...
    ],
    "server_tokens": "boolean",
    "comment": "string",
    "from_central_console": "boolean"
  },
  ...
]
```

- `id` - идентификатор профиля;
- `name` - название профиля, максимальная длина - 42 символа;
- `detection_only` - режим работы: `true` - только обнаружение, `false` - обнаружение и блокировка;
- `disabled_categories` - список идентификаторов категорий для исключения, максимальная длина - 128 символов;
- `exceptions` - исключенные правила:
  - `id` - идентификатор исключенного правила;
  - `rule_id` - идентификатор исключенного правила в профиле;
  - `comment` - комментарий, максимальная длина - 255 символов;
  - `enabled` - статус: `true` - включено, `false` - выключено.
- `server_tokens` - статус HTTP-заголовка Server: `true` - показывать, `false` - скрывать;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `from_central_console` - `true`, если профиль создан в Ideco Center, только для чтения.

Создание профиля:

```
POST /reverse_proxy_backend/waf/profiles
```

Json-тело запроса:

```
{
    "name": "string",
    "detection_only": "boolean",
    "disabled_categories": ["string"],
    "server_tokens": "boolean",
    "comment": "string",
    "from_central_console": "boolean"
}
```

- `name` - название профиля, максимальная длина - 42 символа;
- `detection_only` - режим работы: `true` - только обнаружение, `false` - обнаружение и блокировка;
- `disabled_categories` - список идентификаторов категорий для исключения, максимальная длина - 128 символов, при создании профиля может быть пустым;
- `server_tokens` - статус HTTP-заголовка Server: `true` - показывать, `false` - скрывать;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `from_central_console` - `true`, если профиль создан в Ideco Center, только для чтения.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

Изменение профиля:

```
PATCH /reverse_proxy_backend/waf/profiles/<id профиля>
```

Json-тело запроса:

```
{
    "name": "string",
    "detection_only": "boolean",
    "disabled_categories": ["string"],
    "server_tokens": "boolean",
    "comment": "string",
    "from_central_console": "boolean"
}
```

- `name` - название профиля, максимальная длина - 42 символа;
- `detection_only` - режим работы: `true` - только обнаружение, `false` - обнаружение и блокировка;
- `disabled_categories` - список идентификаторов категорий правил, которые были отключены, максимальная длина - 128 символов;
- `server_tokens` - статус HTTP-заголовка Server: `true` - показывать, `false` - скрывать;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `from_central_console` - `true`, если профиль создан в Ideco Center, только для чтения.

Ответ на успешный запрос: 200 OK

Удаление профиля:

```
DELETE /reverse_proxy_backend/waf/profiles/<id профиля>
```

Ответ на успешный запрос: 200 OK

Получение списка категорий правил:

```
GET /reverse_proxy_backend/waf/categories
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string",
    "required": "boolean",
    "description": "string"
  },
  ...
]
```

- `id` - идентификатор категории, максимальная длина - 42 символа;
- `title` - название категории, максимальная длина - 42 символа;
- `required` - является ли категория необходимой, т.е. ее нельзя будет выключать;
- `description` - описание категории, максимальная длина - 255 символов.

Получение списка категорий правил в профиле:

```
GET /reverse_proxy_backend/waf/profiles/<id профиля>/categories
```

Ответ на успешный запрос:

- Список категорий правил, которые включены в профиле.

```
[
  {
    "id": "string",
    "title": "string",
    "required": "boolean",
    "description": "string"
  },
  ...
]
```

- `id` - идентификатор категории, максимальная длина - 42 символа;
- `title` - название категории, максимальная длина - 42 символа;
- `required` - является ли категория необходимой, т.е. ее нельзя будет выключать;
- `description` - описание категории, максимальная длина - 255 символов.

Добавление или удаление категории правил в профиле:

```
PATCH /reverse_proxy_backend/waf/profiles/<id профиля>/categories/<id категории>
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

Ответ на успешный запрос:

- Если профиль или категория не найдены по идентификатору, то код ответа - 542;
- Если enabled - `true`, то категория, идентификатор которой указан в запросе, будет удалена из списка `disabled_categories` профиля. Ответ - 200 OK;
- Если enabled - `false`, то категория, идентификатор которой указан в запросе, будет добавлена в список `disabled_categories` профиля. Ответ - 200 OK.

Получение белых и черных списков в профиле:

```
GET /reverse_proxy_backend/waf/profiles/<id профиля>/rules
```

Ответ на успешный запрос:

```
[
  {
    "aliases": ["string"],
    "aliases_negate": "boolean",
    "action": "block" | "pass",
    "comment": "string",
    "enabled": "boolean",
    "id": "integer"
  },
  ...
]
```

- `aliases` - список алиасов IP-адресов, подсетей, стран, списков стран и континентов;
- `aliases_negate` - инверсия правила;
- `action` - действие:
  - `block` - блокировать запросы;
  - `pass` - пропускать запросы.
- `comment` - комментарий, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включено, `false` - выключено;
- `id` - номер правила.

Создание белых и черных списков в профиле:

```
POST /reverse_proxy_backend/waf/profiles/<id профиля>/rules?anchor_item_id=<integer>&
↪insert_after=<true|false>
```

- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое;
- `insert_after` - вставка до или после. Если `true` или отсутствует, то вставить правило сразу после указанного в `anchor_item_id`. Если `false`, то на месте указанного в `anchor_item_id`.

Json-тело запроса:

```
{
    "aliases": ["string"],
    "aliases_negate": "boolean",
    "action": "block" | "pass",
    "comment": "string",
    "enabled": "boolean"
}
```

- `aliases` - список алиасов IP-адресов, подсетей, стран, списков стран и континентов;
- `aliases_negate` - инверсия правила;
- `action` - действие:
  - `block` - блокировать запросы;
  - `pass` - пропускать запросы.
- `comment` - комментарий, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включено, `false` - выключено.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

Изменение белых и черных списков в профиле:

```
PATCH /reverse_proxy_backend/waf/profiles/<id профиля>/rules/<id правила в профиле>
```

Json-тело запроса:

```
{
    "aliases": ["string"],
    "aliases_negate": "boolean",
    "action": "block" | "pass",
    "comment": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "enabled": "boolean"
}
```

- `aliases` - список алиасов IP-адресов, подсетей, стран, списков стран и континентов;
- `aliases_negate` - инверсия правила;
- `action` - действие:
  - `block` - блокировать запросы;
  - `pass` - пропускать запросы.
- `comment` - комментарий, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Перемещение белых и черных списков в профиле:

```
PATCH /reverse_proxy_backend/waf/profiles/rules/move
```

Json-тело запроса:

```
{
  "params": {
    "profile_id": "string",
    "rule_id": "integer",
    "anchor_item_id": "integer",
    "insert_after": "boolean",
  },
}
```

- `profile_id` - идентификатор профиля, в котором перемещается правило;
- `rule_id` - идентификатор перемещаемого правила;
- `anchor_item_id` - идентификатор правила, относительно которого будет перемещено правило;
- `insert_after` - вставить правило до или после `anchor_item_id`. Если `true` или отсутствует, то вставить правило сразу после указанного в `anchor_item_id`. Если `false`, то на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление белых и черных списков в профиле:

```
DELETE /reverse_proxy_backend/waf/profiles/<id профиля>/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

Получение списка исключенных правил профиля:

```
GET /reverse_proxy_backend/waf/profiles/<id профиля>/exceptions
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "rule_id": "integer",
    "comment": "string",
    "enabled": "boolean"
```

(continues on next page)

(продолжение с предыдущей страницы)

```
  },
  ...
]
```

- `id` - идентификатор исключенного правила;
- `rule_id` - идентификатор правила;
- `comment` - комментарий, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включено, `false` - выключено.

Создание исключенного правила в профиле:

```
POST /reverse_proxy_backend/waf/profiles/<id профиля>/exceptions
```

Json-тело запроса:

```
{
    "rule_id": "integer",
    "comment": "string",
    "enabled": "boolean"
}
```

- `rule_id` - идентификатор правила. Можно найти в журнале в разделе **Отчеты и журналы -> События безопасности ->** ***Web Application Firewall***;
- `comment` - комментарий, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включено, `false` - выключено.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

Изменение исключенного правила в профиле:

```
PATCH /reverse_proxy_backend/waf/profiles/<id профиля>/exceptions/<id исключенного␣
↪правила>
```

Json-тело запроса:

```
{
    "rule_id": "integer",
    "comment": "string",
    "enabled": "boolean"
}
```

- `rule_id` - идентификатор правила. Можно найти в журнале в разделе **Отчеты и журналы -> События безопасности ->** ***Web Application Firewall***;
- `comment` - комментарий, максимальная длина - 255 символов;
- `enabled` - статус: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Удаление исключенного правила в профиле:

```
DELETE /reverse_proxy_backend/waf/profiles/<id профиля>/exceptions/<id исключенного␣
↪правила>
```

Ответ на успешный запрос: 200 OK

48.3 Контроль приложений

Получение списка профилей:

```
GET /20250219090034/docsUTM/api/application_control/profiles
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "name": "string",
    "comment": "string",
    "protocols": [
      {
        "id": "string",
        "action": "deny" | "allow"
      },
      ...
    ],
  }
]
```

- `id` - идентификатор профиля;
- `name` - название профиля;
- `comment` - комментарий к профилю;
- `protocols` - список протоколов, выбранных для профиля:
  - `id` - строковый идентификатор алиаса протокола с префиксом `id.l7`. Например, `id.l7.ftp_protocol`;
  - `action` - действие, применяемое к протоколу (`deny` - запретить, `allow` - разрешить).

Создание профиля:

```
POST /20250219090034/docsUTM/api/application_control/profiles
```

Json-тело запроса:

```
{
  "name": "string",
  "comment": "string",
  "protocols": [
    {
      "id": "string",
      "action": "deny" | "allow"
    },
    ...
    ],
}
```

- `name` - название профиля;
- `comment` - комментарий к профилю;
- `protocols` - список протоколов, выбранных для профиля:

  - id - строковый идентификатор алиаса протокола с префиксом id.l7. Например, id.l7.ftp_protocol;
  - action - действие, применяемое к протоколу (deny - запретить, allow - разрешить).

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "name": "string",
    "comment": "string",
    "protocols": [
      {
        "id": "string",
        "action": "deny" | "allow"
      },
      ...
      ],
  }
]
```

- id - идентификатор профиля;
- name - название профиля;
- comment - комментарий к профилю;
- protocols - список протоколов, выбранных для профиля:
  - id - строковый идентификатор алиаса протокола с префиксом id.l7. Например, id.l7.ftp_protocol;
  - action - действие, применяемое к протоколу (deny - запретить, allow - разрешить).

Копирование профиля:

```
POST /20250219090034/docsUTM/api/application_control/profiles/<id профиля>/copy
```

Ответ на успешный запрос:

```
{
  "id": "integer"
}
```

- id - идентификатор копии профиля.

Редактирование профиля:

```
PATCH /20250219090034/docsUTM/api/application_control/profiles/<id профиля>
```

Json-тело запроса:

```
[
  {
    "name": "string",
    "comment": "string",
    "protocols": [
      {
        "id": "string",
        "action": "deny" | "allow"
      },
      ...
```

(continues on next page)

```
      ],
  }
]
```

- `name` - название профиля;
- `comment` - комментарий к профилю;
- `protocols` - список протоколов, выбранных для профиля:
  - `id` - строковый идентификатор алиаса протокола с префиксом `id.l7`. Например, `id.l7.ftp_protocol`;
  - `action` - действие, применяемое к протоколу (`deny` - запретить, `allow` - разрешить).

Ответ на успешный запрос: 200 OK

Удаление профиля:

```
DELETE /20250219090034/docsUTM/api/application_control/profiles/<id профиля>
```

Ответ на успешный запрос: 200 OK

49. Управление сетевыми интерфейсами

49.1 Внешние и локальные интерфейсы

Получение списка всех внешних и локальных интерфейсов:

```
GET /network/connections
```

Ответ на успешный запрос: объекты LAN, WAN, PPTP, L2TP, PPPoE

LAN (Локальный Ethernet-интерфейс):

```
{
    "id": "integer",
    "type": "lan",
    "title": "string",
    "enabled": "boolean",
    "mac": "string",
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean",
    "netflow_index": "integer"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;

- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP;
- `dns` - список IP-адресов DNS. Может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть равен `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*.

WAN (Подключение к провайдеру по Ethernet):

```
{
    "id": "integer",
    "type": "wan",
    "title": "string",
    "enabled": "boolean",
    "mac": "string",
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean",
    "netflow_index": "integer"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `enable_dhcp` - получать ли адрес интерфейса и адрес шлюза от провайдера по DHCP;
- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP;
- `dns` - список IP-адресов DNS, может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно), `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*.

PPTP (Подключение к провайдеру по PPTP):

```
{
    "id": "integer",
    "type": "pptp",
    "title": "string",
    "enabled": "boolean",
    "server": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "login": "string",
    "password": "string",
    "mac": "string",
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean",
    "netflow_index": "integer"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `server` - IP-адрес или доменное имя PPTP-сервера, к которому осуществляется подключение;
- `login` - логин на сервере PPTP, не может быть пустым;
- `password` - пароль на сервере PPTP, не может быть пустым;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `enable_dhcp` - получать ли адрес интерфейса и адрес шлюза от провайдера по DHCP;
- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP или PPTP-сервер находится в той же подсети, что назначена на интерфейс;
- `dns` - список IP-адресов DNS, может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть `null` если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*.

L2TP (Подключение к провайдеру по L2TP):

```
{
    "id": "integer",
    "type": "l2tp",
    "title": "string",
    "enabled": "boolean",
    "server": "string",
    "login": "string",
    "password": "string",
    "mac": "string",
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "netflow_index": "integer"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `server` - IP-адрес или доменное имя L2TP-сервера, к которому осуществляется подключение;
- `login` - логин на сервере L2TP, не может быть пустым;
- `password` - пароль на сервере L2TP, не может быть пустым;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `enable_dhcp` - получать ли адрес интерфейса и адрес шлюза от провайдера по DHCP;
- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP или L2TP-сервер находится в той же подсети, что назначена на интерфейс;
- `dns` - список IP-адресов DNS, может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно), `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*.

PPPoE (Подключение к провайдеру по PPPoE):

```
{
    "id": "integer",
    "type": "pppoe",
    "title": "string",
    "enabled": "boolean",
    "login": "string",
    "password": "string",
    "service": "string",
    "concentrator": "string",
    "mac": "string",
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean",
    "netflow_index": "integer"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `login` - логин на сервере PPPoE, не может быть пустым;
- `password` - пароль на сервере PPPoE, не может быть пустым;
- `service` - название сервиса, может быть пустым;
- `concentrator` - название концентратора, может быть пустым;

- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно), `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*.

Получение состояния локальных интерфейсов и подключений:

```
GET /network/states
```

Ответ на успешный запрос:

```
[
  {
    "id": "integer",
    "type": "lan" | "wan" | "pptp" | "l2tp" | "pppoe",
    "ether": {
        "device": "null" | "string",
        "vlan_tag": "null" | "integer",
        "addresses": [ "string" ],
        "gateway": "null" | "string",
        "dns": [ "string" ],
        "status": "down" | "going-up" | "up",
        "errors": [ "string" ]
    },
    "ppp": {
        "device": "null" | "string",
        "remote_address": "null" | "string",
        "local_address": "null" | "string",
        "dns": [ "string" ],
        "status": "down" | "going-up" | "up",
        "errors": [ "string" ]
    },
    "summary": {
        "device": "null" | "string",
        "addresses": [ "string" ],
        "dns": [ "string" ],
        "gateway": "null" | "string",
        "zone": "null" | "string",
        "ifindex": "null" | "integer",
        "scope": "kernel" | "vpp"
    }
  },
...
]
```

- `id` - идентификатор интерфейса;
- `type` - тип подключения;
- `ether` - состояние Ethernet или VLAN:
  - `device` - название устройства в системе, например, `Leth1`;
  - `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно) или `null`, если не назначен;
  - `addresses` - список адресов, может быть пустым. Адреса в формате `IP/prefix`;
  - `gateway` - IP-адрес шлюза, может быть равен `null`, если шлюза нет;

  - `dns` - адреса DNS, выданные по DHCP или назначенные пользователем;
  - `status` - текущее состояние интерфейса;
  - `errors` - список ошибок.
- `ppp` - состояние PPP-подключения. Поле определено только для интерфейсов с полем `type` равным `pptp | l2tp | pppoe`, для всех остальных типов `lan | wan` равно `null`:
  - `device` - название устройства в системе, например `Eppp4`;
  - `remote_address` - туннельный IP-адрес сервера;
  - `local_address` - туннельный IP-адрес клиента (IP-адрес NGFW);
  - `dns` - адреса DNS, выданные из PPP;
  - `status` - текущее состояние интерфейса;
  - `errors` - список ошибок.
- `summary` - общее состояние подключение:
  - `device` - итоговое активное устройство, например, `Eppp4` или `Eeth3`;
  - `addresses` - список адресов интерфейса или подключения к провайдеру;
  - `dns` - адреса DNS, пригодные к использованию для сервера DNS и других целей;
  - `gateway` - IP-адрес шлюза, может быть равен `null`, если шлюза нет;
  - `zone` - алиас зоны. Может быть равен `null`, если не назначен;
  - `ifindex` - числовой идентификатор интерфейса;
  - `scope` - принадлежность интерфейса сетевому стеку: kernel - ядро.

Создание внешнего или локального интерфейса:

```
POST /network/connections
```

Json-тело запроса: один из объектов LAN | WAN | PPTP | L2TP | PPPoE, которые описаны в раскрывающемся блоке *Получение списка всех внешних и локальных интерфейсов*, без поля «id»

Ответ на успешный запрос:

```
{
    "id": "number"
}
```

- `id` - идентификатор созданного интерфейса.

Редактирование внешнего или локального интерфейса:

```
PATCH /network/connections/<id интерфейса>
```

Json-тело запроса: некоторые поля одного из объектов LAN | WAN | PPTP | L2TP | PPPoE, которые описаны в раскрывающемся блоке *Получение списка всех внешних и локальных интерфейсов*

Ответ на успешный запрос: 200 OK

Удаление внешнего или локального интерфейса:

```
DELETE /network/connections/<id интерфейса>
```

Ответ на успешный запрос: 200 OK

49.2 Агрегированные интерфейсы

Получение списка агрегированных интерфейсов:

```
GET /network/aggregated
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "enabled": "boolean",
    "title": "string",
    "comment": "string",
    "nics": [ "string" ]
  },
...
]
```

- `id` - идентификатор агрегированного интерфейса;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `title` - название, не может быть пустым;
- `comment` - комментарий, может быть пустым;
- `nics` - список MAC-адресов в формате `11:22:33:44:55:66`, все буквы в нижнем регистре, может быть пустым.

Получение состояния агрегированных интерфейсов:

```
GET /network/aggregated_states
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "link": "up" | "down"
  },
...
]
```

- `id` - идентификатор агрегированного интерфейса;
- `link` - состояние соединения на агрегированном интерфейсе.

Создание нового агрегированного интерфейса:

```
POST /network/aggregated
```

Json-тело запроса:

```
{
  "enabled": "boolean",
  "title": "string",
  "comment": "string",
  "nics": [ "string" ]
  }
```

- `enabled` - если `true`, то интерфейс включен, `false` - выключен;

- `title` - название, не может быть пустым;
- `comment` - комментарий, может быть пустым;
- `nics` - список MAC-адресов в формате `11:22:33:44:55:66`, все буквы в нижнем регистре, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного агрегированного интерфейса.

Редактирование агрегированного интерфейса:

```
PUT /network/aggregated/<id интерфейса>
```

Json-тело запроса:

```
{
  "enabled": "boolean",
  "title": "string",
  "comment": "string",
  "nics": [ "string" ]
  }
```

- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `title` - название, не может быть пустым;
- `comment` - комментарий, может быть пустым;
- `nics` - список MAC-адресов в формате `11:22:33:44:55:66`, все буквы в нижнем регистре, может быть пустым.

Ответ на успешный запрос: 200 OK

Удаление агрегированного интерфейса:

```
DELETE /network/aggregated/<id интерфейса>
```

Ответ на успешный запрос: 200 OK

49.3 Туннельные интерфейсы

Получение списка всех туннельных интерфейсов:

```
GET /network/tunnels
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string",
    "enabled": "boolean",
    "comment": "string",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "parent_interface": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "osdevname": "string",
    "server": "string",
    "zone": "null" | "string",
    "netflow_index": "integer",
    "local_ip": "null" | "string"
  },
...
]
```

- `id` - идентификатор интерфейса, строка в формате UUID;
- `title` - название интерфейса, не может быть пустым, максимальная длина - 42 символа;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `comment` - комментарий, может быть пустым;
- `addresses` - список адресов в формате `IP/prefix`;
- `gateway` - IP-адрес шлюза, может быть равен `null`;
- `parent_interface` - алиас родительского интерфейса, его IP-адрес будет источником туннеля;
- `osdevname` - название существующего или планируемого сетевого интерфейса в ядре (например, `Gre00000001`). Значение создается автоматически, является уникальным и **доступно только для чтения**;
- `server` - IP-адрес или доменное имя устройства, к которому осуществляется подключение;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*;
- `local_ip` - IP-адрес родительского интерфейса запущенного туннеля.

Получение состояния туннельных интерфейсов:

```
GET /network/tunnel_states
```

Ответ на успешный запрос:

```
{
  "id": "string",
  "link": "up" | "down" | "inactive",
  "local_ip": "string"
}
```

- `id` - идентификатор интерфейса;
- `link` - состояние туннельного интерфейса, `inactive` при недоступности родительского интерфейса;
- `local_ip` - IP-адрес родительского интерфейса запущенного туннеля.

Создание нового туннельного интерфейса:

```
POST /network/tunnels
```

Json-тело запроса:

```
{
    "title": "string",
    "enabled": "boolean",
    "comment": "string",
    "addresses": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "gateway": "null" | "string",
    "parent_interface": "string",
    "osdevname": "string",
    "server": "string",
    "zone": "null" | "string",
    "netflow_index": "integer",
    "local_ip": "null" | "string"
}
```

- `title` - название интерфейса, не может быть пустым, максимальная длина - 42 символа;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `comment` - комментарий, может быть пустым;
- `addresses` - список адресов в формате `IP/prefix`;
- `gateway` - IP-адрес шлюза, может быть равен `null`;
- `parent_interface` - алиас родительского интерфейса, его IP-адрес будет источником туннеля;
- `osdevname` - название существующего или планируемого сетевого интерфейса в ядре (например, `Gre00000001`). Значение создается автоматически, является уникальным и **доступно только для чтения**;
- `server` - IP-адрес или доменное имя устройства, к которому осуществляется подключение;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*;
- `local_ip` - IP-адрес родительского интерфейса запущенного туннеля. Если не задавать, берется с родительского интерфейса.

Важно: Для каждого родительского интерфейса все настроенные туннели должны иметь уникальные значения в поле `server`. Не допускается создание туннельных интерфейсов с повторяющимися значениями в полях `parent_interface` и `server`!

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного туннельного интерфейса.

Редактирование туннельного интерфейса:

```
PUT /network/tunnels/<id интерфейса>
```

Json-тело запроса:

```
{
    "title": "string",
    "enabled": "boolean",
    "comment": "string",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "parent_interface": "string",
    "osdevname": "string",
    "server": "string",
    "zone": "null" | "string",
    "netflow_index": "integer",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "local_ip": "null" | "string"
}
```

- `title` - название интерфейса, не может быть пустым, максимальная длина - 42 символа;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `comment` - комментарий, может быть пустым;
- `addresses` - список адресов в формате `IP/prefix`;
- `gateway` - IP-адрес шлюза, может быть равен `null`;
- `parent_interface` - алиас родительского интерфейса, его IP-адрес будет источником туннеля;
- `osdevname` - название существующего или планируемого сетевого интерфейса в ядре (например, `Gre00000001`). Значение создается автоматически, является уникальным и **доступно только для чтения**;
- `server` - IP-адрес или доменное имя устройства, к которому осуществляется подключение;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*;
- `local_ip` - IP-адрес родительского интерфейса запущенного туннеля. Если не задавать, берется с родительского интерфейса.

Ответ на успешный запрос: 200 OK

Удаление туннельного интерфейса:

```
DELETE /network/tunnels/<id интерфейса>
```

Ответ на успешный запрос: 200 OK

49.4 VCE-интерфейсы

Получение списка всех сетевых интерфейсов, пробрасываемых в VCE:

```
GET /network/vce_conns
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string",
    "vce_id": "string",
    "mac": "string",
    "vlan_tag": "null" | "integer",
    "comment": "string"
  },
  ...
]
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `vce_id` - идентификатор VCE, для которого создан интерфейс;
- `mac` - MAC-адрес сетевой карты в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;

- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть `null`, если пробрасывается сетевой интерфейс целиком;
- `comment` - комментарий, может быть пустым.

Важно: Изменяемыми являются только поля `title` и `comment`.

Создание пробрасываемого в VCE интерфейса:

```
POST /network/vce_conns
```

Json-тело запроса:

```
{
    "title": "string",
    "vce_id": "string",
    "mac": "string",
    "vlan_tag": "null" | "integer",
    "comment": "string"
}
```

- `title` - название интерфейса, не может быть пустым;
- `vce_id` - идентификатор VCE, для которого создан интерфейс;
- `mac` - MAC-адрес сетевой карты в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть `null`, если пробрасывается сетевой интерфейс целиком;
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор созданного интерфейса.

Редактирование пробрасываемого в VCE интерфейса:

```
PATCH /network/vce_conns/<id интерфейса>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string"
}
```

- `title` - название интерфейса, не может быть пустым;
- `comment` - комментарий, может быть пустым.

Поля опциональны, можно передавать любое из них отдельно или оба сразу.

Ответ на успешный запрос: 200 OK

Удаление пробрасываемого в VCE интерфейса:

```
DELETE /network/vce_conns/<id интерфейса>
```

Ответ на успешный запрос: 200 OK

49.5 SPAN-интерфейсы

Получение списка SPAN-интерфейсов:

```
GET /network/span
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string",
    "comment": "string",
    "enabled": "boolean",
    "mac": "string",
    "monitor_interfaces": [ "string" ],
    "direction": "string",
    "osdevindex": "integer"
  },
...
]
```

- `id` - идентификатор интерфейса (строка в формате UUID);
- `title` - название интерфейса, не может быть пустым;
- `comment` - комментарий. Может быть пустым.
- `enabled` - включен или выключен интерфейс;
- `mac` - MAC-адрес сетевой карты;
- `monitor_interfaces` - список идентификаторов алиасов интерфейсов, трафик с которых надо зеркалировать. Допустимые типы алиасов: `isp`, `lan`, `interface.vpn_traffic`;
- `direction` - тип трафика, который требуется дублировать на SPAN-интерфейс. Может принимать значения `rx` - входящий, `tx` - исходящий и `both` - оба;
- `osdevindex` - суффикс (числовой индекс) названия существующего или планируемого сетевого интерфейса в ядре (например, число 43818 соответствует интерфейсу с системным именем `Span43818`). Значение создается автоматически. Является уникальным и доступно только для чтения.

Создание нового SPAN-интерфейса:

```
POST /network/span
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "enabled": "boolean",
    "mac": "string",
    "monitor_interfaces": [ "string" ],
    "direction": "string"
}
```

- `title` - название интерфейса, не может быть пустым;
- `comment` - комментарий. Может быть пустым.
- `enabled` - включен или выключен интерфейс;
- `mac` - MAC-адрес сетевой карты;

- `monitor_interfaces` - список идентификаторов алиасов интерфейсов, трафик с которых надо зеркалировать. Допустимые типы алиасов: `isp`, `lan`, `ipsec`, `ipsec_gre`, `tunnel`;
- `direction` - тип трафика, который требуется дублировать на SPAN-интерфейс. Может принимать значения `rx` - входящий, `tx` - исходящий и `both` - оба.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного SPAN-интерфейса.

Редактирование SPAN-интерфейса:

```
PATCH /network/span/<id SPAN-интерфейса>
```

Json-тело запроса (любые поля интерфейса, кроме id и osdevindex):

```
{
    "title": "string",
    "comment": "string",
    "enabled": "boolean",
    "mac": "string",
    "monitor_interfaces": [ "string" ],
    "direction": "string"
}
```

- `title` - название интерфейса, не может быть пустым;
- `comment` - комментарий. Может быть пустым.
- `enabled` - включен или выключен интерфейс;
- `mac` - MAC-адрес сетевой карты;
- `monitor_interfaces` - список идентификаторов алиасов интерфейсов, трафик с которых надо зеркалировать. Допустимые типы алиасов: `isp`, `lan`, `ipsec`, `ipsec_gre`, `tunnel`;
- `direction` - тип трафика, который требуется дублировать на SPAN-интерфейс. Может принимать значения `rx` - входящий, `tx` - исходящий и `both` - оба.

Ответ на успешный запрос: 200 OK

Удаление SPAN-интерфейса:

```
DELETE /network/span/<id SPAN-интерфейса>
```

Ответ на успешный запрос: 200 OK

50. Управление VPN

Статус VPN-сервера:

```
GET /vpn_servers/status
```

Ответ на успешный запрос:

```
{
    "name": "string",
    "status": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "msg": [ "string" ]
}
```

- `name` - доменное имя;
- `status` - статус домена;
- `msg` - список сообщений, объясняющий текущее состояние.

50.1 Настройка VPN-подключения по PPTP, SSTP

Получение настроек:

```
GET /vpn_servers/settings
```

Ответ на успешный запрос:

```
{
  "pptp_enabled": "boolean",
  "sstp": {
      "enabled": "boolean",
      "domain": "string",
      "port": "integer"
  },
  "network": "string",
  "zone": "string" | "null",
  "dns_suffix": "string",
  "netflow_index": "integer"
}
```

- `pptp_enabled` - если `true`, то сервер PPTP включен, `false` - выключен;
- `sstp` - настройки сервера SSTP:
  - `enabled` - если `true`, то сервер SSTP включен, `false` - выключен;
  - `domain` - доменное имя, присвоенное внешнему интерфейсу. Если домен еще не задан, то `null`;
  - `port` - порт для подключения, одно из предустановленных значений (`1443`, `2443`, `3443`, `4443`).
- `network` - сеть, из которой VPN-серверы раздают адреса. Первый адрес в этой сети - всегда адрес самого сервера;
- `zone` - зона для Lvpn0-интерфейса. Если зона не назначена, то `null`;
- `dns_suffix` - DNS-суффикс, передаваемый в Ideco Client. Если не назначен, то может быть пустой строкой;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*.

Изменение настроек:

```
PUT /vpn_servers/settings
```

Json-тело запроса:

```
{
  "pptp_enabled": "boolean",
  "sstp": {
      "enabled": "boolean",
      "domain": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      "port": "integer"
  },
  "network": "string",
  "zone": "string" | "null",
  "dns_suffix": "string",
  "netflow_index": "integer"
}
```

- `pptp_enabled` - если `true`, то сервер PPTP включен, `false` - выключен;
- `sstp` - настройки сервера SSTP:
  - `enabled` - если `true`, то сервер SSTP включен, `false` - выключен;
  - `domain` - доменное имя, присвоенное внешнему интерфейсу. Если домен еще не задан, то `null`;
  - `port` - порт для подключения, одно из предустановленных значений (`1443`, `2443`, `3443`, `4443`).
- `network` - сеть, из которой VPN-серверы раздают адреса. Первый адрес в этой сети - всегда адрес самого сервера;
- `zone` - зона для Lvpn0-интерфейса. Если зона не назначена, то `null`;
- `dns_suffix` - DNS-суффикс, передаваемый в Ideco Client. Если не назначен, то может быть пустой строкой;
- `netflow_index` - целое число от 0 до 65535, индекс сетевого подключения для *NetFlow*.

Ответ на успешный запрос: 200 OK

50.2 Скрипт для подключения пользователей по SSTP

Проверка возможности сгенерировать скрипт:

```
GET /vpn_servers/powershell/status
```

Ответ на успешный запрос:

```
{
    "sstp_available": "boolean",
}
```

Создание скрипта:

```
GET /vpn_servers/powershell/sstp
```

Ответ на успешный запрос: создается скрипт для подключения пользователей по SSTP. В ответе отображается заголовок `Content-Disposition: attachment; filename=\"Ideco_NGFW_VPN_SSTP.ps1`

50.3 Управление правилами доступа к VPN

Получение списка правил:

```
GET /vpn_servers/access_rules
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "enabled": "boolean",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "title": "string",
    "sources": [ "string" ],
    "objects": [ "string" ],
    "vpns": [ "string" ],
    "action": "allow" | "deny",
    "two_factor": "smsaero" | "totp" | "multifactor" | "not_required",
    "comment": "string"
}
```

- `id` - идентификатор правила;
- `enabled` - статус правила: `true` - включено, `false` - выключено;
- `title` - название правила, может быть пустым, но не должно превышать 42 символов;
- `sources` - список источников подключения, не может быть пустым, допустимые типы:
  - `any` - любой источник подключения (если указан алиас `any`, то других алиасов в списке быть не должно);
  - `ip.id` - IP-адрес;
  - `ip_range.id` - диапазон IP-адресов;
  - `subnet.id` - подсеть;
  - `ip_address_list.id` - список IP-адресов;
  - `list_of_iplists.id` - список стран;
  - `domain.id` - домен.
- `objects` - список объектов, для которых будут назначены адреса, не может быть пустым. Объекты могут быть:
  - `any` - для любых объектов (если указан объект `any`, то других объектов в списке быть не должно);
  - `user.id` - для пользователей;
  - `group.id` - для групп;
  - `security_group.guid` - для групп безопасности AD.
- `vpns` - список типов VPN (протоколов подключения), не может быть пустым. Допустимые варианты:
  - `any` - любой тип подключения (если указан `any`, то других типов VPN в списке быть не должно);
  - `pptp` - подключение по PPTP;
  - `l2tp` - подключение по L2TP;
  - `sstp` - подключение по SSTP;
  - `ikev2`- подключение по IKEv2;
  - `agent-vpn-ng` - подключение по Wireguard (Ideco Client).
- `action` - действие при совпадении источника, объекта и типа VPN, не может быть пустым, допустимые варианты:
  - `allow` - разрешить;
  - `deny` - запретить.
- `two_factor` - тип требуемой двухфакторной авторизации, не может быть пустым. Должен быть `not_required`, если в поле `action` выбран `deny`. Допустимые варианты:
  - `smsaero` - аутентификация при помощи вода кода из СМС;
  - `totp` - аутентификация сканированием QR-кода или использованием токена;

- `multifactor` - аутентификация подтверждением личности в стороннем приложении;
- `not_required` - означает, что двухфакторная авторизация не требуется.

- `comment` - комментарий, может быть пустым, но не должен превышать 255 символов.

Добавление правил:

```
POST /vpn_servers/access_rules?anchor_item_id={int}&insert_after={true|false}
```

Параметры запроса:

- `anchor_item_id` - идентификатор правила, ниже или выше которого необходимо создать новое правило. Если параметр не указан, то правило будет создано в конце списка;
- `insert_after` - указывает, куда необходимо вставить новое правило. Если параметр не указан или равен `true`, то новое правило будет добавлено сразу после правила с указанным идентификатором. Если параметр равен `false`, то новое правило заменит правило с указанным идентификатором.

Json-тело запроса:

```
{
    "enabled": "boolean",
    "title": "string",
    "sources": [ "string" ],
    "objects": [ "string" ],
    "vpns": [ "string" ],
    "action": "allow" | "deny",
    "two_factor": "smsaero" | "totp" | "multifactor" | "not_required",
    "comment": "string"
}
```

- `enabled` - статус правила: `true` - включено, `false` - выключено;
- `title` - название правила, может быть пустым, но не должно превышать 42 символов;
- `sources` - список источников подключения, не может быть пустым, допустимые типы:
  - `any` - любой источник подключения (если указан алиас `any`, то других алиасов в списке быть не должно);
  - `ip.id` - IP-адрес;
  - `ip_range.id` - диапазон IP-адресов;
  - `subnet.id` - подсеть;
  - `ip_address_list.id` - список IP-адресов;
  - `list_of_iplists.id` - список стран;
  - `domain.id` - домен.
- `objects` - список объектов, для которых будут назначены адреса, не может быть пустым. Объекты могут быть следующими:
  - `any` - для любых объектов (если указан объект `any`, то других объектов в списке быть не должно);
  - `user.id` - для пользователей;
  - `group.id` - для групп;
  - `security_group.guid` - для групп безопасности AD.
- `vpns` - список типов VPN (протоколов подключения), не может быть пустым. Допустимые варианты:
  - `any` - любой тип подключения (если указан `any`, то других типов VPN в списке быть не должно);
  - `pptp` - подключение по PPTP;

  - `l2tp` - подключение по L2TP;
  - `sstp` - подключение по SSTP;
  - `ikev2`- подключение по IKEv2;
  - `agent-vpn-ng` - подключение по Wireguard (Ideco Client).
- `action` - действие при совпадении источника, объекта и типа VPN, не может быть пустым, допустимые варианты:
  - `allow` - разрешить;
  - `deny` - запретить.
- `two_factor` - тип требуемой двухфакторной авторизации, не может быть пустым. Должен быть `not_required`, если в поле `action` выбран `deny`. Допустимые варианты:
  - `smsaero` - аутентификация при помощи вода кода из СМС;
  - `totp` - аутентификация сканированием QR-кода или использованием токена;
  - `multifactor` - аутентификация подтверждением личности в стороннем приложении;
  - `not_required` - означает, что двухфакторная авторизация не требуется.
- `comment` - комментарий, может быть пустым, но не должен превышать 255 символов.

Ответ на успешный запрос:

```
{
   "id": "integer"
}
```

- `id` - идентификатор добавленного правила.

Редактирование правил:

```
PATCH /vpn_servers/access_rules/<id правила>
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "title": "string",
    "sources": [ "string" ],
    "objects": [ "string" ],
    "vpns": [ "string" ],
    "action": "allow" | "deny",
    "two_factor": "smsaero" | "totp" | "multifactor" | "not_required",
    "comment": "string"
}
```

- `enabled` - статус правила: `true` - включено, `false` - выключено;
- `title` - название правила, может быть пустым, но не должно превышать 42 символов;
- `sources` - список источников подключения, не может быть пустым, допустимые типы:
  - `any` - любой источник подключения (если указан алиас `any`, то других алиасов в списке быть не должно);
  - `ip.id` - IP-адрес;
  - `ip_range.id` - диапазон IP-адресов;
  - `subnet.id` - подсеть;
  - `ip_address_list.id` - список IP-адресов;

  - `list_of_iplists.id` - список стран;
  - `domain.id` - домен.
- `objects` - список объектов, для которых будут назначены адреса, не может быть пустым. Объекты могут быть следующими:
  - `any` - для любых объектов (если указан объект `any`, то других объектов в списке быть не должно);
  - `user.id` - для пользователей;
  - `group.id` - для групп;
  - `security_group.guid` - для групп безопасности AD.
- `vpns` - список типов VPN (протоколов подключения), не может быть пустым. Допустимые варианты:
  - `any` - любой тип подключения (если указан `any`, то других типов VPN в списке быть не должно);
  - `pptp` - подключение по PPTP;
  - `l2tp` - подключение по L2TP;
  - `sstp` - подключение по SSTP;
  - `ikev2`- подключение по IKEv2;
  - `agent-vpn-ng` - подключение по Wireguard (Ideco Client).
- `action` - действие при совпадении источника, объекта и типа VPN, не может быть пустым, допустимые варианты:
  - `allow` - разрешить;
  - `deny` - запретить.
- `two_factor` - тип требуемой двухфакторной авторизации, не может быть пустым. Должен быть `not_required`, если в поле `action` выбран `deny`. Допустимые варианты:
  - `smsaero` - аутентификация при помощи вода кода из СМС;
  - `totp` - аутентификация сканированием QR-кода или использованием токена;
  - `multifactor` - аутентификация подтверждением личности в стороннем приложении;
  - `not_required` - означает, что двухфакторная авторизация не требуется.
- `comment` - комментарий, может быть пустым, но не должен превышать 255 символов.

Ответ на успешный запрос: 200 OK

Удаление правил:

```
DELETE /vpn_servers/access_rules/<id правила>
```

Ответ на успешный запрос: 200 OK

Изменение порядка правил:

```
PATCH /vpn_servers/access_rules/<id правила>/position
```

Json-тело запроса:

```
{
   "direction": "up" | "down"
}
```

- `direction` - направление сдвига строки с правилом в таблице:
  - `up` - правило поднимается на одну позицию вверх;
  - `down` - правило опускается на одну позицию вниз.

Ответ на успешный запрос: 200 OK

50.4 Управление правилами выдачи IP-адресов

Получение списка правил:

```
GET /vpn_servers/lease_rules
```

Ответ на успешный запрос:

```
{
  "id": "integer",
  "title": "string",
  "objects": [ "string" ],
  "address": "string",
  "comment": "string",
  "enabled": "boolean"
}
```

- `id` - идентификатор правила получения адресов;
- `title` - название правила, может быть пустым, но не должно превышать 42 символов;
- `objects` - список объектов, для которых будут назначены адреса, не может быть пустым. Объекты могут быть следующими:
  - `any` - для любых объектов (если указан объект `any`, то других объектов в списке быть не должно);
  - `user.id` - для пользователей;
  - `group.id` - для групп;
  - `security_group.guid` - для групп безопасности AD.
- `address` - IP-адрес, который будет назначен пользователю, или адрес сети, в которой ему будет выделен IP-адрес, если пользователь соответствует списку объектов. В строке может быть указан IP-адрес без маски или подсеть (значение не может быть пустым и не должно повторяться);
- `comment` - комментарий, может быть пустым, но не должен превышать 255 символов;
- `enabled` - статус правила: `true` - включено, `false` - выключено.

Добавление правил:

```
POST /vpn_servers/lease_rules?anchor_item_id=<integer>&insert_after=<true|false>
```

Параметры запроса:

- `anchor_item_id` - идентификатор правила, ниже или выше которого необходимо создать новое правило. Если параметр не указан, то правило будет создано в конце списка;
- `insert_after` - указывает, куда необходимо вставить новое правило. Если параметр не указан или равен `true`, то новое правило будет добавлено сразу после правила с указанным идентификатором. Если параметр равен `false`, то новое правило заменит правило с указанным идентификатором.

Json-тело запроса:

```
{
  "title": "string",
  "objects": [ "string" ],
  "address": "string",
  "comment": "string",
  "enabled": "boolean"
}
```

- `title` - название правила, может быть пустым, но не должно превышать 42 символов;
- `objects` - список объектов, для которых будут назначены адреса, не может быть пустым. Объекты могут быть следующими:
  - `any` - для любых объектов (если указан объект `any`, то других объектов в списке быть не должно);
  - `user.id` - для пользователей;
  - `group.id` - для групп;
  - `security_group.guid` - для групп безопасности AD.
- `address` - IP-адрес, который будет назначен пользователю, или адрес сети, в которой ему будет выделен IP-адрес, если пользователь соответствует списку объектов. В строке может быть указан IP-адрес без маски или подсеть (значение не может быть пустым и не должно повторяться);
- `comment` - комментарий, может быть пустым, но не должен превышать 255 символов;
- `enabled` - статус правила: `true` - включено, `false` - выключено.

Ответ на успешный запрос:

```
{
   "id": "integer"
}
```

- `id` - идентификатор добавленного правила.

Редактирование правил:

```
PATCH /vpn_servers/lease_rules/<id правила>
```

Json-тело запроса:

```
{
  "title": "string",
  "objects": [ "string" ],
  "address": "string",
  "comment": "string",
  "enabled": "boolean"
}
```

- `title` - название правила, может быть пустым, но не должно превышать 42 символов;
- `objects` - список объектов, для которых будут назначены адреса, не может быть пустым. Объекты могут быть следующими:
  - `any` - для любых объектов (если указан объект `any`, то других объектов в списке быть не должно);
  - `user.id` - для пользователей;
  - `group.id` - для групп;
  - `security_group.guid` - для групп безопасности AD.
- `address` - IP-адрес, который будет назначен пользователю, или адрес сети, в которой ему будет выделен IP-адрес, если пользователь соответствует списку объектов. В строке может быть указан IP-адрес без маски или подсеть (значение не может быть пустым и не должно повторяться);
- `comment` - комментарий, может быть пустым, но не должен превышать 255 символов;
- `enabled` - статус правила: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Удаление правил:

```
DELETE /vpn_servers/lease_rules/<id правила>
```

Ответ на успешный запрос: 200 OK

Изменение порядка правил:

```
PATCH /vpn_servers/lease_rules/<id правила>/position
```

Json-тело запроса:

```
{
   "direction": "up" | "down"
}
```

- `direction` - направление сдвига строки с правилом в таблице:
  - `up` - правило поднимается на одну позицию вверх;
  - `down` - правило опускается на одну позицию вниз.

Ответ на успешный запрос: 200 OK

50.5 Работа с таблицей VPN

Получение типов VPN, используемых в таблице Доступ по VPN:

```
GET /vpn_servers/vpns_in_access_rules
```

Ответ на успешный запрос:

```
{
   "pptp": "boolean",
   "l2tp": "boolean",
   "sstp": "boolean",
   "ikev2": "boolean",
   "agent-vpn-ng": "boolean"
}
```

Значение по ключу `boolean` указывает, используется ли этот тип в таблице VPN.

Получение типов двуфакторной авторизации, используемых в таблице Доступ по VPN:

```
GET /vpn_servers/two_factor_in_access_rules
```

Ответ на успешный запрос:

```
{
   "smsaero": "boolean",
   "totp": "boolean",
   "multifactor": "boolean"
}
```

Значение по ключу `boolean` указывает, используется ли этот тип в таблице VPN.

Получение списка правил доступа к VPN для конкретного пользователя:

```
GET /vpn_servers/user_access_rules/<id пользователя>
```

Ответ на успешный запрос:

```
{
  "id": "integer",
  "enabled": "boolean",
  "title": "string",
  "sources": [ "string" ],
  "objects": [ "string" ],
  "vpns": [ "string" ],
  "action": "allow" | "deny",
  "two_factor": "smsaero" | "totp" | "multifactor" | "not_required",
  "comment": "string"
}
```

Для несуществующего пользователя или пользователя, для которого нельзя получить полный список групп, возвращается пустой список правил.

50.6 DHCP-сервер

Получение настроек:

```
GET /vpn_servers/dhcp
```

Ответ на успешный запрос:

```
{
  "mode": "all" | "utm" | "local" | "none" | "custom",
  "networks": [ "string" ],
  "excluded_networks": [ "string" ]
}
```

- `mode` - режим раздачи маршрутов:
  - `all` - направляем весь трафик на NGFW (маршрут 0.0.0.0/0);
  - `utm` - раздаем маршруты до локальных и внутренних сетей NGFW;
  - `local` - раздаем маршруты только до локальных сетей NGFW;
  - `none` - не раздаем маршруты;
  - `custom` - раздаем только маршруты до указанных подсетей.
- `networks` - список подсетей, маршруты до которых передаются в режиме custom. Допустимы алиасы подсетей, IP-адресов, доменов;
- `excluded_networks` - список подсетей, маршруты до которых исключаются в любом режиме. Допустимы алиасы подсетей, IP-адресов, доменов.

Изменение настроек:

```
PUT /vpn_servers/dhcp
```

Json-тело запроса:

```
{
  "mode": "all" | "utm" | "local" | "none" | "custom",
  "networks": [ "string" ],
  "excluded_networks": [ "string" ]
}
```

Ответ на успешный запрос: 200 OK

51. DHCP-сервер

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Получение статуса службы DHCP-сервера:

```
GET /dhcp_server/status
```

Ответ на успешный запрос:

```
[
  {
      "name": "string",
      "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
      "msg": [ "string" ]
  }
]
```

- `name` - название службы;
- `status` - текущее состояние службы;
- `msg` - список строк, подробно описывающих состояние службы.

51.1 Настройки

Получение настроек:

```
GET /dhcp_server/settings
```

Пример ответа на успешный запрос:

```
[
  {
      "enabled": "boolean",
      "interface": "string",
      "relay": {
          "external_servers": [
              "string"
          ]
      },
      "server": null,
      "id": "string"
    },
  {
      "enabled": "boolean",
      "interface": "string",
      "relay": null,
      "server": {
          "dns": [ "string" ],
          "domain": "string",
          "gateway": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
          "lease_time": "integer",
          "options": [
              {
                  "comment": "string",
                  "enabled": "boolean",
                  "forced": "boolean",
                  "option": "string"
                }
            ],
          "ranges": [ "string" ],
          "routes": [ {
                  "destination": "string",
                  "gateway": "string"
                } ],
          "tftp_filename": "string",
          "tftp_server": "string",
          "wins": [ "string" ],
          "wpad_enabled": "boolean"
        },
      "id": "string"
    },
    ...
]
```

- `id` - идентификатор настройки;
- `enabled` - если `true`, то настройка включена, `false` - выключена;
- `interface` - интерфейс Ideco NGFW;
- `relay` - режим работы (если активен `server`, должен быть `null`):
  - `external_servers` - IP-адрес внешнего DHCP-сервера.
- `server` - режим работы (если активен `relay`, должен быть `null`):
  - `dns` - поля DNS-1 и DNS-2 в веб-интерфейсе. Если не задано значение в поле DNS-1 или DNS-2, то DNS-сервером для всех сетевых устройств локальной сети будет являться Ideco NGFW;
  - `domain` - DNS-суффикс;
  - `gateway` - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса;
  - `lease_time` - время аренды (в минутах);
  - `options` - опции dnsmasq (`comment` - комментарий, может быть пустым; `enabled` - включена или отключена опция; `forced` - принудительная отправка опции клиенту; `option` - значение опции);
  - `ranges` - диапазон IP-адресов для выдачи;
  - `routes` - статические маршруты (`destination` - хост, `gateway` - шлюз);
  - `tftp_filename` - имя файла для загрузки по TFTP;
  - `tftp_server` - IP-адрес TFTP-сервера для настройки загрузки образа по сети;
  - `wins` - IP-адрес WINS-сервера;
  - `wpad_enabled` - включение протокола автоматической настройки прокси. Для работы WPAD необходимо разрешить прямые подключения к прокси.

Создание настроек:

```
POST /dhcp_server/settings
```

Json-тело запроса для режима сервера:

```
{
      "enabled": "boolean",
      "interface": "string",
      "relay": null,
      "server": {
          "dns": [ "string" ],
          "domain": "string",
          "gateway": "string",
          "lease_time": "integer",
          "options": [
              {
                  "comment": "string",
                  "enabled": "boolean",
                  "forced": "boolean",
                  "option": "string"
              }
          ],
          "ranges": [ "string" ],
          "routes": [ {
                  "destination": "string",
                  "gateway": "string"
              } ],
          "tftp_filename": "string",
          "tftp_server": "string",
          "wins": [ "string" ],
          "wpad_enabled": "boolean"
      }
  }
```

- `enabled` - если `true`, то настройка включена, `false` - выключена;
- `interface` - интерфейс Ideco NGFW;
- `relay` - режим работы (если активен `server`, должен быть `null`):
  - `external_servers` - IP-адрес внешнего DHCP-сервера.
- `server` - режим работы (если активен `relay`, должен быть `null`):
  - `dns` - поля DNS-1 и DNS-2 в веб-интерфейсе. Если не задано значение в поле DNS-1 или DNS-2, то DNS-сервером для всех сетевых устройств локальной сети будет являться Ideco NGFW;
  - `domain` - DNS-суффикс;
  - `gateway` - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса;
  - `lease_time` - время аренды (в минутах);
  - `options` - опции dnsmasq (`comment` - комментарий, может быть пустым; `enabled` - включена или отключена опция; `forced` - принудительная отправка опции клиенту; `option` - значение опции);
  - `ranges` - диапазон IP-адресов для выдачи;
  - `routes` - статические маршруты (`destination` - хост, `gateway` - шлюз);
  - `tftp_filename` - имя файла для загрузки по TFTP;
  - `tftp_server` - IP-адрес TFTP-сервера для настройки загрузки образа по сети;
  - `wins` - IP-адрес WINS-сервера;

- wpad_enabled - включение протокола автоматической настройки прокси. Для работы WPAD необходимо разрешить прямые подключения к прокси.

Json-тело запроса для режима релея:

```
{
    "enabled": "boolean",
    "interface": "string",
    "relay": {
        "external_servers": [
            "string"
        ]
    },
    "server": null
  }
```

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- id - идентификатор настройки.

Изменение настроек:

```
PATCH /dhcp_server/20250219090034/docsUTM/settings/<id настройки>
```

Json-тело запроса - все или некоторые поля для создания настроек, например:

```
{
    "relay": {
        "external_servers": [
            "string"
        ]
    }
  }
```

- relay - режим работы (если активен server, должен быть null):
  - external_servers - IP-адрес внешнего DHCP-сервера.

Ответ на успешный запрос: 200 OK

Удаление настроек:

```
DELETE /dhcp_server/20250219090034/docsUTM/settings/<id настройки>
```

Ответ на успешный запрос: 200 OK

51.2 Привязка IP к MAC

Получение статических привязок:

```
GET /dhcp_server/static_leases
```

Пример ответа на успешный запрос:

```
[
  {
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      "comment": "",
      "enabled": true,
      "ip_address": "192.168.0.40",
      "mac": "50:46:5d:6e:8c:20",
      "id": "3e4827dd-5e0c-4932-98b1-fa2d9826b0ce"
  },
  ...
]
```

- `ip_address` - IP-адрес;
- `mac` - MAC-адрес;
- `enabled` - если `true`, то запись включена, `false` - выключена;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `id` - идентификатор статической привязки.

Создание статической привязки:

```
POST /dhcp_server/static_leases
```

Json-тело запроса:

```
{
    "comment": "string",
    "enabled": "boolean",
    "ip_address": "string",
    "mac": "string"
  }
```

- `ip_address` - IP-адрес;
- `mac` - MAC-адрес;
- `enabled` - если `true`, то запись включена, `false` - выключена;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW. Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (01-02-03-04-05-06). В настройках Ideco NGFW октеты MAC-адреса разделяются только двоеточиями (01:02:03:04:05:06).

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор статической привязки.

Редактирование статической привязки:

```
PATCH /dhcp_server/static_leases/<id статической привязки>
```

Json-тело запроса (все или некоторые поля):

```
{
    "comment": "string",
    "enabled": "boolean",
    "ip_address": "string",
```

(continues on next page)

```
    "mac": "string"
  }
```

- `ip_address` - IP-адрес;
- `mac` - MAC-адрес;
- `enabled` - если `true`, то запись включена, `false` - выключена;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление статической привязки:

```
DELETE /dhcp_server/static_leases/<id статической привязки>
```

Ответ на успешный запрос: 200 OK

52. DNS-сервер

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Получение статуса службы DNS:

```
GET /dns/status
```

Ответ на успешный запрос:

```
[
  {
    "name": "string",
    "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
    "msg": [ "string" ]
  },
  ...
]
```

- `name` - название службы;
- `status` - состояние службы;
- `msg` - список ошибок, может быть пустым.

52.1 Настройки

Получение настроек DNS-сервера:

```
GET /dns/settings
```

Ответ на успешный запрос:

```
{
        "intercept_enabled": "boolean"
}
```

- `intercept_enabled` - перехватывать DNS-запросы на серверы в интернет.

Включение/выключение DNS-сервера:

```
PUT /dns/settings
```

Json-тело запроса:

```
{
    "intercept_enabled": "boolean"
}
```

- `intercept_enabled` - перехватывать DNS-запросы на серверы в интернет.

Ответ на успешный запрос: 200 OK

Включение/выключение переадресации DNS для безопасного поиска:

52.1.1 Получение настроек:

```
GET /dns/safesearch
```

Ответ на успешный запрос:

```
{
        "enabled": "boolean"
}
```

- `enabled` - переадресовывать DNS-запросы на безопасные домены поиска Google, Yandex, YouTube, Bing, DuckDuckGo, Qwant и Pixabay.

52.1.2 Изменение настроек:

```
PUT /dns/safesearch
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - переадресовывать DNS-запросы на безопасные домены поиска Google, Yandex, YouTube, Bing, DuckDuckGo, Qwant и Pixabay.

Ответ на успешный запрос: 200 OK

52.2 Управление внешними DNS-серверами

Получение списка:

```
GET /dns/zones/root
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "enabled": "boolean",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "type": "ip" | "interface",
    "object": "string",
    "comment": "string"
},
...
]
```

- `id` - идентификатор объекта;
- `enabled` - если `true`, то элемент включен, `false` - выключен;
- `type` - принимает два значения:
  - `ip` - IP-адрес DNS-сервера, заданного вручную;
  - `interface` - идентификатор алиаса подключения к провайдеру (DNS-серверы, выданные подключению). Тип алиаса - `isp`.
- `object` - IP-адрес, если тип `ip`, или идентификатор алиаса подключения к провайдеру, если тип `interface`;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Добавление корневого DNS-сервера:

```
POST /dns/zones/root
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "type": "ip" | "interface",
    "object": "string",
    "comment": "string"
}
```

- `enabled` - если `true`, то элемент включен, `false` - выключен;
- `type` - принимает два значения:
  - `ip` - IP-адрес DNS-сервера, заданного вручную;
  - `interface` - идентификатор алиаса подключения к провайдеру (DNS-серверы, выданные подключению). Тип алиаса - `isp`.
- `object` - IP-адрес, если тип `ip`, или идентификатор алиаса подключения к провайдеру, если тип `interface`;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор DNS-сервера.

Редактирование корневого DNS-сервера:

```
PATCH /dns/zones/root/<id DNS-сервера>
```

Json-тело запроса (все или некоторые поля):

```
{
    "enabled": "boolean",
    "type": "ip" | "interface",
    "object": "string",
    "comment": "string"
}
```

- `enabled` - если `true`, то элемент включен, `false` - выключен;
- `type` - принимает два значения:
  - `ip` - IP-адрес DNS-сервера, заданного вручную;
  - `interface` - идентификатор алиаса подключения к провайдеру (DNS-серверы, выданные подключению). Тип алиаса - `isp`.
- `object` - IP-адрес, если тип `ip`, или идентификатор алиаса подключения к провайдеру, если тип `interface`;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление корневого DNS-сервера:

```
DELETE /dns/zones/root/<id DNS-сервера>
```

Ответ на успешный запрос: 200 OK

52.3 Управление Forward-зонами

Получение списка:

```
GET /dns/zones/forward
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "name": "string",
    "enabled": "boolean",
    "servers": [ "string" ],
    "comment": "string",
},
    ...
]
```

- `id` - идентификатор объекта;
- `name` - название зоны;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `servers` - список IP-адресов DNS-серверов, заданных вручную;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Добавление Forward-зоны:

```
POST /dns/zones/forward
```

Json-тело запроса:

```
{
    "name": "string",
    "enabled": "boolean",
    "servers": [ "string" ],
    "comment": "string"
}
```

- `name` - название зоны;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `servers` - список IP-адресов DNS-серверов, заданных вручную;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор Forward-зоны.

Редактирование Forward-зоны:

```
PATCH /dns/zones/forward/<id Forward-зоны>
```

Json-тело запроса (все или некоторые поля):

```
{
    "name": "string",
    "enabled": "boolean",
    "servers": [ "string" ],
    "comment": "string"
}
```

- `name` - название зоны;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `servers` - список IP-адресов DNS-серверов, заданных вручную;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление Forward-зоны:

```
DELETE /dns/zones/forward/<id Forward-зоны>
```

Ответ на успешный запрос: 200 OK

52.4 Управление Master-зонами

Получение списка:

```
GET /dns/zones/master
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "name": "string",
    "enabled": "boolean",
    "config": "string",
    "comment": "string",
},
    ...
]
```

- `id` - идентификатор объекта;
- `name` - уникальное название зоны, имеет вид домена example.com;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `config` - текст с параметрами зоны, не может быть пустым. Максимальная длина - 10000 символов;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Подробнее о формате записей для настройки Master-зоны - в статье *Master-зоны*.

Добавление Master-зоны:

```
POST /dns/zones/master
```

Json-тело запроса:

```
{
    "name": "string",
    "enabled": "boolean",
    "config": "string",
    "comment": "string",
}
```

- `name` - уникальное название зоны, имеет вид домена example.com;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `config` - текст с параметрами зоны, не может быть пустым. Максимальная длина - 10000 символов;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор Master-зоны.

Редактирование Master-зоны:

```
PATCH /dns/zones/master/<id Master-зоны>
```

Json-тело запроса (все или некоторые поля):

```
{
    "name": "string",
    "enabled": "boolean",
    "config": "string",
    "comment": "string",
}
```

- `name` - уникальное название зоны, имеет вид домена example.com;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `config` - текст с параметрами зоны, не может быть пустым. Максимальная длина - 10000 символов;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление Master-зоны:

```
DELETE /dns/zones/master/<id Master-зоны>
```

Ответ на успешный запрос: 200 OK

52.5 DDNS

Подсказка: DDNS в Ideco NGFW реализован через интеграцию с хостингом RU-CENTER. Перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.

Подробнее о DDNS - в *статье*.

Получение состояния:

```
GET /dns/ddns/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние DDNS: `true` - включено, `false` - выключено.

Включение/выключение DDNS:

```
PUT /dns/ddns/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние DDNS: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Получение настроек:

```
GET /dns/ddns
```

Ответ на успешный запрос:

```
{
    "domain": "string",
    "service_login": "string",
    "service_password": "string"
}
```

- `domain` - домен, который администратор хочет видеть в адресной строке. Формат: `domain.com` (без `https://` и `www`);
- `service_login` - логин для доступа к API сервиса DDNS;
- `service_password` - пароль для доступа к API сервиса DDNS, до 42 символов.

Изменение настроек:

```
PUT /dns/ddns
```

Json-тело запроса:

```
{
    "domain": "string",
    "service_login": "string",
    "service_password": "string"
}
```

- `domain` - домен, который администратор хочет видеть в адресной строке. Формат: `domain.com` (без `https://` и `www`);
- `service_login` - логин для доступа к API сервиса DDNS;
- `service_password` - пароль для доступа к API сервиса DDNS, до 42 символов.

Ответ на успешный запрос: 200 OK

53. Настройка удаленной передачи системных логов

Получение статуса работы службы:

```
GET /logs_backend/remote_syslog/status
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
        "msg": [ "string" ]
    },
    ...
]
```

- `name` - название модуля;
- `status` - статус;
- `msg` - список сообщений, объясняющий текущее состояние.

53.1 Общие настройки

Включение/выключение службы:

Проверка состояния:

```
GET /logs_backend/remote_syslog/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `msg` - `true` для включения, `false` для выключения.

Включение/выключение

```
PUT /logs_backend/remote_syslog/state
```

Json-тело запроса:

```
{
  "enabled": "boolean"
}
```

Ответ на успешный запрос: 200 OK

Получение настроек удаленной передачи системных логов:

```
GET /logs_backend/remote_syslog
```

Ответ на успешный запрос:

```
{
  "host": "string",
  "port": "integer",
  "protocol": "tcp" | "udp",
  "format": "syslog" | "cef"
}
```

- `host` - IP-адрес сервера;
- `port` - порт;
- `protocol` - протокол, допустимые значения: `tcp` или `udp`;
- `format` - формат, допустимые значения: `syslog` или `cef`.

Изменение настроек удаленной передачи системных логов:

```
PATCH /logs_backend/remote_syslog
```

Json-тело запроса:

```
{
  "host": "string" | "null",
  "port": "integer" | "null",
  "protocol": "tcp" | "udp",
  "format": "syslog" | "cef",
}
```

- `host` - IP-адрес сервера;

- `port` - порт;
- `protocol` - протокол, допустимые значения: `tcp` или `udp`;
- `format` - формат, допустимые значения: `syslog` или `cef`.

Пустые значения «» не допускаются.

Ответ на успешный запрос: 200 OK

Получение данных о логировании для таблицы:

```
GET /logs_backend/logs?<GET-параметры, разделенные знаком &>
```

Список GET-параметров, которые не являются обязательными:

- `limit: integer` - ограничение на количество записей, выбираемых из базы данных;
- `offset: integer` - количество строк, которые необходимо пропустить перед выводом записей, указанных в `limit`;
- `sort: [Sort]` - список параметров для сортировки данных. Сортировка производится в прямом порядке следования в массиве;
- `filter: [Filter]` - список параметров для фильтрации данных. Фильтры применяются в прямом порядке следования в массиве, с логикой `and` между объектами `Filter`;
- `search: Search` - объект с параметрами поиска подстроки в данных;
- `last_reboot_only: boolean` - параметр типа `boolean` со значениями: `false` - выводить все записи лога, `true` - только записи после последней загрузки;
- `format_type:` - формат возвращаемых данных:
  - `CSV` - CSV-файл;
  - `JSON` - тип по умолчанию.

Обьект Sort:

```
{
  "field": "string",
  "direction": "asc | desc"
}
```

- `field` - столбец, по которому производится сортировка;
- `direction` - направление сортировки: `asc` - по возрастанию, `desc` - по убыванию.

Обьект Filter:

```
{
  "items": [
      {
        "column_name": "string",
        "operator": "contains | not_contains | equals | not_equals | greater |␣
↪greater_equal | less | less_equal",
        "value": ["string | integer | boolean"]
      },
      ...
    ],
  "link_operator": "and | or"
}
```

- `items` - массив фильтров `FilterItem`:
  - `column_name` - поле для фильтрации;

- operator - одно из значений:
  - contains - содержит подстроку (без учета регистра);
  - not_contains - не содержит подстроку (без учета регистра);
  - equals - равно;
  - not_equals - не равно;
  - greater - больше, в values передается массив, содержащий только одно значение;
  - greater_equal - больше или равно, в values передается массив, содержащий только одно значение;
  - less - меньше, в values передается массив, содержащий только одно значение;
  - less_equal - меньше или равно, в values передается массив, содержащий только одно значение.
- value - массив значений фильтра. Максимальное количество передаваемых в массиве значений - 255. Данные отбираются по логике or.

- link_operator - логика наложения фильтров items.

Обьект Search:

```
{
  "text": "string",
  "columns": ["string"]
}
```

- text - искомая строка;
- columns - набор полей, по которым ведется поиск.

Ответ на успешный запрос:

```
{
  "meta": [
    {
      "name": "string",
      "type": "string"
    },
    ...
  ],
  "data": [
    {
      "id": "string",
      "date_time": "integer",
      "microseconds": "integer",
      "priority": "integer",
      "message": "string",
      "syslog_id": "string",
      "unit": "string"
    },
    ...
  ],
  "rows": "integer",
  "rows_before_limit_at_least": "integer"
}
```

- meta - массив метаданных, описывающих поля запроса:
  - name - имя поля данных;

  - `type` - тип данных.
- `data` - массив, содержащий `Log` - объект, представляющий собой данные, соответствующие одной строке таблицы:
  - `id` - уникальный идентификатор строки;
  - `date_time` - время возникновения события в формате YYYYMMDDhhmmss;
  - `microseconds` - микросекунды во времени возникновения события (0. . . 999999);
  - `priority` - число от 0 до 7:
    * `0` - LOG_EMERG;
    * `1` - LOG_ALERT;
    * `2` - LOG_CRIT;
    * `3` - LOG_ERR;
    * `4` - LOG_WARNING;
    * `5` - LOG_NOTICE;
    * `6` - LOG_INFO;
    * `7` - LOG_DEBUG.
  - `message` - сообщение логирования;
  - `syslog_id` - название исполняемой программы;
  - `unit` - название сервиса, сообщение которого было сохранено в журнале.
- `rows` - количество строк `Log`;
- `rows_before_limit_at_least` - количество строк `Log`, которое вернет запрос, если использовать ограничение на количество записей из базы данных (GET-параметры `limit` или `offset`).

54. Управление Ideco Center

54.1 Управление Ideco Center

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

54.1.1 Настройки Ideco Center в Ideco NGFW

Получение настроек Ideco Center:

```
GET /central_console/settings
```

Ответ на успешный запрос:

```
{
    "cc_server": "string" | "null",
    "last_connect": "integer" | "null",
    "last_sync": "integer" | "null",
    "root_ca": "string" | "null"
}
```

- `cc_server` - доменное имя или IP-адрес Ideco Center;

- `last_connect` - timestamp последней успешной синхронизации данных;
- `last_sync` - timestamp;
- `root_ca` - корневой сертификат в формате PEM.

Изменение настроек Ideco Center:

```
PATCH /central_console/settings
```

Json-тело запроса:

```
{
    "cc_server": "string" | "null"
}
```

- `cc_server` - доменное имя или IP-адрес Ideco Center.

Загрузка корневого сертификата Ideco Center на NGFW:

```
POST /central_console/root_ca
```

В тело запроса поместите содержимое корневого сертификата, скачанного в Ideco Center. Для этого откройте сертификат в текстовом редакторе и скопируйте текст.

Удаление корневого сертификата Ideco Center:

```
DELETE /central_console/root_ca
```

Ответ на успешный запрос: 200 OK

Отключение NGFW от Ideco Center:

```
DELETE /central_console/settings
```

Ответ на успешный запрос: 200 OK

54.1.2 API Ideco Center

Получение статуса службы:

```
GET /servers/status
```

Ответ на успешный запрос:

```
{
    "name": "string",
    "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
    "msg": [ "string" ]
}
```

- `name` - название службы;
- `status` - текущее состояние службы;
- `msg` - список строк, описывающих состояние службы.

Общие настройки

Получение общих настроек:

```
GET /servers/setting
```

Ответ на успешный запрос:

```
{
    "domain": "string" | "null"
}
```

- `domain` - внешний адрес Ideco Center (IP-адрес или доменное имя).

Изменение общих настроек:

```
PUT /servers/setting
```

Json-тело запроса:

```
{
    "domain": "string" | "null"
}
```

- `domain` - внешний адрес Ideco Center (IP-адрес или доменное имя).

Ответ на успешный запрос: 200 OK

Получение настройки включенности синхронизации правил:

```
GET /servers/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - если `true`, то синхронизация правил включена, `false` - выключена.

Включение/выключение синхронизации правил:

```
PUT /servers/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения синхронизации правил, `false` для выключения.

Ответ на успешный запрос: 200 OK

Группировка серверов

Получение списка групп серверов в Ideco Center:

```
GET /servers/groups
```

Пример ответа на успешный запрос:

```
[
    {
        "comment": "",
        "name": "Группа 1",
        "parent_id": "f3ffde22-a562-4f43-ac04-c40fcec6a88c",
        "id": "e37ec0bb-fc27-406f-bd24-d0e89200561d"
    },
    {
        "comment": "",
        "name": "Корневая группа",
        "parent_id": null,
        "id": "f3ffde22-a562-4f43-ac04-c40fcec6a88c"
    },
    ...
]
```

- `id` - идентификатор группы;
- `comment` - комментарий, может быть пустым;
- `name` - название группы серверов;
- `parent_id` - идентификатор родительской группы серверов.

Создание группы серверов:

```
POST /servers/groups
```

Json-тело запроса:

```
{
    "comment": "string",
    "name": "string",
    "parent_id": "string"
}
```

- `name` - название группы;
- `parent_id` - идентификатор родительской группы (если группа входит в Корневую группу, идентификатор Корневой группы);
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданной группы.

Редактирование группы серверов:

```
PATCH /servers/groups/<id группы серверов>
```

Json-тело запроса:

```
{
    "comment": "string",
    "name": "string",
    "parent_id": "string"
}
```

- `name` - название группы;
- `parent_id` - идентификатор родительской группы (если группа входит в Корневую группу, идентификатор Корневой группы);
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос: 200 OK

Удаление группы серверов:

```
DELETE /servers/groups/<id группы серверов>
```

Ответ на успешный запрос: 200 OK

Управление подключенными серверами

Получение списка подключенных серверов:

```
GET /servers/servers
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "parent_id": "string",
        "version": {
          "major": "integer",
          "minor": "integer",
          "build": "integer",
          "timestamp": "integer",
          "vendor": "Ideco",
          "product": "UTM",
          "kind": "FSTEK" | "VPP" | "STANDARD" | "BPF",
          "release_type": "release" | "beta" | "devel"
    },
        "cl_tunnel_addr": "string",
        "title": "string",
        "approved": "boolean",
        "last_sync": "integer" | "null",
        "last_connect": "integer",
        "utm_login_secret": "string",
        "comment": "string"
    },
    ...
]
```

- `id` - идентификатор сервера;
- `parent_id` - идентификатор группы, в которую входит сервер;
- `version` - версия сервера:

  - `major` - мажорный номер версии;
  - `minor` - минорный номер версии;
  - `build` - номер сборки;
  - `timestamp` - время выхода версии;
  - `vendor` - вендор («Ideco»);
  - `product` - код продукта;
  - `kind` - вид продукта;
  - `release_type` - тип релиза.
- `cl_tunnel_addr` - IPv6-адрес сервера внутри WireGuard-туннеля;
- `title` - название сервера;
- `approved` - флаг, означающий, подтверждено ли подключение сервера в Ideco Center;
- `last_sync` - timestamp последней успешной синхронизации данных;
- `last_connect` - timestamp последнего успешного подключения;
- `utm_login_secret` - секретное значение для отправки в URL авторизации Ideco Center в Ideco NGFW;
- `version_diff` - разница мажорных версий Ideco Center и NGFW. Если значение равно нулю - мажор одинаковый, больше нуля - версия Ideco Center выше, меньше нуля - версия NGFW выше.
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым.

Перемещение подключенных серверов между группами/подтверждение подключения сервера к Ideco Center:

```
PATCH /servers/servers/<id сервера>
```

Json-тело запроса:

```
{
    "parent_id": "string",
    "approved": "boolean"
}
```

- `parent_id` - идентификатор группы, в которую входит сервер;
- `approved` - флаг, означающий, подтверждено ли подключение сервера в Ideco Center.

Ответ на успешный запрос: 200 OK

При добавлении нового сервера ему автоматически присваивается parent_id Корневой группы.

После подтверждения подключения сервера (установки approved=true) менять это свойство нельзя (для удаления сервера вызывается метод DELETE)

Удаление сервера из Ideco Center:

```
DELETE /servers/servers/<id сервера>
```

Ответ на успешный запрос: 200 OK

Управление правилами трафика Ideco Center

Контент-фильтр

Получение списка категорий (предустановленных и пользовательских):

```
GET /content-filter/categories
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "type": "string",
        "name": "string",
        "comment": "string"
    },
    ...
]
```

- `id` - номер категории в формате `users.id.1` или `extended.id.1`;
- `type` - тип категории:
  - `users` - пользовательские категории;
  - `extended` - расширенные категории (SkyDNS);
  - `files` - категории для файлов;
  - `special` - специальные предопределенные категории (Прямое обращение по IP, Все категоризированные запросы, Все некатегоризированные запросы, Все запросы).
  - `other` - остальные категории.
- `name` - имя категории;
- `comment` - описание категории.

Получение списка пользовательских категорий:

```
GET /content-filter/users_categories
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "comment": "string",
        "urls": [ "string" ]
    },
    ...
]
```

- `id` - номер категории в формате `users.id.1`;
- `name` - название категории, не пустая строка;
- `comment` - комментарий, может быть пустым;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Создание пользовательской категории:

```
POST /content-filter/users_categories
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий, может быть пустым;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

Редактирование пользовательских категорий:

```
PUT /content-filter/users_categories/<id категории>
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий, может быть пустым;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string",
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

Получение списка правил:

- `GET /content-filter/rules/before?groups=[UUID1,UUID2]` - начальные правила;
- `GET /content-filter/rules/after?groups=[UUID1,UUID2]` - конечные правила.
  - `UUID1` - идентификатор группы серверов в Ideco Center (`id`).

Ответ на успешный запрос:

```
[
    {
        "id": "integer",
        "parent_id": "string",
        "name": "string",
        "comment": "string",
        "aliases": [ "string" ],
        "categories": [ "string" ],
        "http_methods": [ "string" ],
        "content_types": [ "string" ],
        "access": "allow" | "deny" | "bump" | "redirect",
        "redirect_url": "string" | "null",
        "enabled": "boolean",
        "timetable": [ "string" ]
    },
    ...
]
```

- `id` - идентификатор правила;
- `parent_id` - идентификатор группы серверов, к которой применяется правило;
- `name` - название правила, не пустая строка;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым;
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `http_methods` - список методов HTTP. Доступен выбор из списка: GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE, CONNECT;
- `content_types` - список mime types;
- `access` - действие, которое необходимо выполнить в правиле, строка, может принимать три значения:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump`- расшифровать запрос;
  - `redirect`: перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled`: правило включено (true) или выключено (false);
- `timetable` - время действия.

Создание правила:

- `POST /content-filter/rules/before?anchor_item_id=123&insert_after={true|false}` - создание начального правила;
- `POST /content-filter/rules/after?anchor_item_id=123&insert_after={true|false}` - создание конечного правила.

Json-тело запроса:

```
{
    "parent_id": "string",
    "name": "string",
    "comment": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "http_methods": [ "string" ],
    "content_types": [ "string" ],
    "access": "allow" | "deny" | "bump" | "redirect",
    "redirect_url": "string" | "null",
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `parent_id` - идентификатор родительской группы;
- `name` - название правила, не может быть пустым;
- `comment` - комментарий, может быть пустым (максимальная длина - 255 символов);
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий;
- `http_methods` - список методов HTTP. Доступен выбор из списка: GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE, CONNECT;
- `content_types` - список mime types;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Редактирование правила:

- `PATCH /content-filter/rules/before/<id правила>` - изменение начального правила;
- `PATCH /content-filter/rules/after/<id правила>` - изменение конечного правила.

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "parent_id": "string",
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "http_methods": [ "string" ],
    "content_types": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "access": "allow" | "deny" | "bump" | "redirect",
    "redirect_url": "string" | "null",
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `parent_id` - идентификатор родительской группы;
- `name` - название правила, не может быть пустым;
- `comment` - комментарий, может быть пустым (максимальная длина - 255 символов);
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий;
- `http_methods` - список методов HTTP. Доступен выбор из списка: GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE, CONNECT;
- `content_types` - список mime types;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия.

Ответ на успешный запрос: 200 OK

Важно! Чтобы переместить правило между группами серверов, измените его `parent_id`.

Перемещение правила:

- `PATCH /content-filter/rules/before/move` - перемещение начального правила;
- `PATCH /content-filter/rules/after/move` - перемещение конечного правила.

Json-тело запроса:

```
{
    "params": {
      "id": "integer",
      "anchor_item_id": "integer",
      "insert_after": "boolean"
  }
}
```

- `id` - идентификатор перемещаемого правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно поместить перемещаемое правило;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление правила:

- `DELETE /content-filter/rules/before/move` - перемещение начального правила;
- `DELETE /content-filter/rules/after/move` - перемещение конечного правила.

Ответ на успешный запрос: 200 OK

API для управления морфологическим анализом представлен в *статье*.

Файрвол

Получение настроек Файрвола:

```
GET /firewall/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - опция раздела **Файрвол**: `true` - включена, `false` - выключена.

Изменение настроек:

```
PUT /firewall/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения, `false` для выключения.

Ответ на успешный запрос: 200 OK

Получение списка правил:

- `GET /firewall/rules/forward/before?groups=[UUID1, UUID2]` - начальные правила раздела FORWARD;
- `GET /firewall/rules/forward/after?groups=[UUID1, UUID2]` - конечные правила раздела FORWARD;
- `GET /firewall/rules/input/before?groups=[UUID1, UUID2]` - начальные правила раздела INPUT;
- `GET /firewall/rules/input/after?groups=[UUID1, UUID2]` - конечные правила раздела INPUT.

Ответ на успешный запрос:

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "outgoing_interface": "string",
    "hip_profiles": [ "string" ],
    "dpi_profile": "string",
    "dpi_enabled": "boolean",
    "ips_profile": "string",
    "ips_enabled": "boolean",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "drop"
}
```

- `id` - идентификатор правила.
- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;
- `dpi_profile` - строка в формате UUID, идентификатор профиля DPI. Не может быть пустой строкой, если `dpi_enabled = true`;
- `dpi_enabled` - если `true`, то обработка с помощью модуля **Контроль приложений** включена, `false` - выключена;
- `ips_profile` - строка в формате UUID, идентификатор профиля IPS. Не может быть пустой строкой, если `ips_enabled = true`;
- `ips_enabled` - если `true`, то обработка с помощью модуля **Предотвращение вторжений** включена, `false` - выключена;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

Добавление правила:

- `POST /firewall/rules/forward/before?anchor_item_id=123&insert_after={true|false}` - начальное правило в раздел FORWARD;
- `POST /firewall/rules/forward/after?anchor_item_id=123&insert_after={true|false}` - конечное правило в раздел FORWARD;

- `POST /firewall/rules/input/before?anchor_item_id=123&insert_after={true|false}` - начальное правило в раздел INPUT;
- `POST /firewall/rules/input/after?anchor_item_id=123&insert_after={true|false}` - конечное правило в раздел INPUT.
  - `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое. Если отсутствует, то новое правило будет добавлено в конец таблицы;
  - `insert_after` - вставка до или после. Если значение `true` или отсутствует, то новое правило будет добавлено сразу после указанного в `anchor_item_id`. Если `false` - на месте указанного в `anchor_item_id`.

Json-тело запроса:

```
{
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "hip_profiles": [ "string" ],
    "dpi_profile": "string",
    "dpi_enabled": "boolean",
    "ips_profile": "string",
    "ips_enabled": "boolean",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "drop"
}
```

- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;
- `dpi_profile` - строка в формате UUID, идентификатор профиля DPI. Не может быть пустой строкой, если `dpi_enabled = true`;
- `dpi_enabled` - если `true`, то обработка с помощью модуля **Контроль приложений** включена, `false` - выключена;

- `ips_profile` - строка в формате UUID, идентификатор профиля IPS. Не может быть пустой строкой, если `ips_enabled` = `true`;
- `ips_enabled` - если `true`, то обработка с помощью модуля **Предотвращение вторжений** включена, `false` - выключена;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Редактирование правила:

- `PUT /firewall/rules/forward/before/<id правила>` - раздел FORWARD, начальное правило;
- `PUT /firewall/rules/forward/after/<id правила>` - раздел FORWARD, конечное правило;
- `PUT /firewall/rules/input/before/<id правила>` - раздел INPUT, начальное правило;
- `PUT /firewall/rules/input/after/<id правила>` - раздел INPUT, конечное правило.

Json-тело запроса:

```
{
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "hip_profiles": [ "string" ],
    "dpi_profile": "string",
    "dpi_enabled": "boolean",
    "ips_profile": "string",
    "ips_enabled": "boolean",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "drop"
}
```

- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;

- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;
- `dpi_profile` - строка в формате UUID, идентификатор профиля DPI. Не может быть пустой строкой, если `dpi_enabled` = `true`;
- `dpi_enabled` - если `true`, то обработка с помощью модуля **Контроль приложений** включена, `false` - выключена;
- `ips_profile` - строка в формате UUID, идентификатор профиля IPS. Не может быть пустой строкой, если `ips_enabled` = `true`;
- `ips_enabled` - если `true`, то обработка с помощью модуля **Предотвращение вторжений** включена, `false` - выключена;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

Ответ на успешный запрос: 200 OK

Важно! Чтобы переместить правило между группами серверов, измените его `parent_id`.

Перемещение правила:

- `PATCH /firewall/rules/forward/before/move` - раздел FORWARD, начальное правило;
- `PATCH /firewall/rules/forward/after/move` - раздел FORWARD, конечное правило;
- `PATCH /firewall/rules/input/before/move` - раздел INPUT, начальное правило;
- `PATCH /firewall/rules/input/after/move` - раздел INPUT, конечное правило.

Json-тело запроса:

```
{
    "params": {
      "id": "integer",
      "anchor_item_id": "integer",
      "insert_after": "boolean"
  }
}
```

- `id` - идентификатор перемещаемого правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно поместить перемещаемое правило;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление правила:

- `DELETE /firewall/rules/forward/before/<id правила>` - раздел FORWARD, начальное правило;
- `DELETE /firewall/rules/forward/after/<id правила>` - раздел FORWARD, конечное правило;
- `DELETE /firewall/rules/input/before/<id правила>` - раздел INPUT, начальное правило;
- `DELETE /firewall/rules/input/after/<id правила>` - раздел INPUT, конечное правило.

Ответ на успешный запрос: 200 OK

55. Бэкапы и возврат к предыдущей версии

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Получение настроек бэкапов:

```
GET /backup/settings
```

Ответ на успешный запрос:

```
{
   "common": {
      "hour": "integer",
      "rotate": "weekly" | "monthly"
   },
   "ftp": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
   },
   "cifs": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
   }
}
```

- `common` - общие настройки бэкапов;
  - `hour` - час, в который делается автоматический бэкап, число от 0 до 23;
  - `rotate` - удалять бэкапы старше недели (`weekly`) или месяца (`monthly`).
- `ftp` - настройки выгрузки бэкапов на FTP:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.

- `cifs` - настройки выгрузки бэкапов в общую папку CIFS:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.

Изменение настроек бэкапов и настройка выгрузки на FTP-сервер или в общую папку CIFS:

```
PUT /backup/settings
```

Json-тело запроса:

```
{
   "common": {
      "hour": "integer",
      "rotate": "weekly | monthly"
   },
   "ftp": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
   },
   "cifs": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
   }
}
```

- `common` - общие настройки бекапов:
  - `hour` - час, в который делается автоматический бекап, число от 0 до 23;
  - `rotate` - удалять бекапы старше недели (`weekly`) или месяца (`monthly`).
- `ftp` - настройки выгрузки бекапов на FTP:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.
- `cifs` - настройки выгрузки бекапов в общую папку CIFS:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.

Ответ на успешный запрос: 200 OK

55.1 Управление бэкапами

Создание бэкапа:

```
POST /backup/backups
```

Json-тело запроса:

```
{
   "comment": "string"
}
```

- `comment` - комментарий, произвольный текст.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор бэкапа.

Получение списка бэкапов:

```
GET /backup/backups
```

Ответ на успешный запрос:

```
[
   {
      "id": "string",
      "version": {
         "major": "integer",
         "minor": "integer",
         "build": "integer",
         "timestamp": "integer",
         "vendor": "Ideco",
         "product": "UTM" | "CC",
         "kind": "FSTEK" | "VPP" | "STANDARD" | "BPF",
         "release_type": "release" | "beta" | "devel"
      },
      "timestamp": "float",
      "comment": "string",
      "md5": "string",
      "size": "integer",
      "fast_restore_allowed": "boolean"
   }
...
]
```

- `id` - идентификатор бэкапа;
- `version` - версия системы:
  - `major` - мажорный номер версии;
  - `minor` - минорный номер версии;
  - `build` - номер сборки;

  - `timestamp` - время выхода версии;
  - `vendor` - вендор («Ideco»);
  - `product` - код продукта;
  - `kind` - вид продукта;
  - `release_type` - тип релиза;
- `timestamp` - дата/время создания бэкапа в формате UNIX timestamp;
- `comment` - комментарий, произвольный текст;
- `md5` - контрольная сумма файла бэкапа (`data.tar`);
- `size` - размер бэкапа, байт;
- `fast_restore_allowed` - можно ли выполнить быстрое восстановление из данного бэкапа (версия идентична системной).

Скачивание бэкапа:

```
GET /backup/download/<id бэкапа>
```

Ответ на успешный запрос: тело бэкапа.

Загрузка бэкапа на Ideco NGFW из файла:

```
POST /backup/upload
```

Используйте стандартный POST-запрос на загрузку файла. Название поля в форме должно быть `backup_file`.

Ответ на успешный запрос:

```
{
   "id": "string"
}
```

- `id` - идентификатор бэкапа.

Восстановление из бэкапа:

```
POST /backup/backups/<id бэкапа>/apply
```

Ответ на успешный запрос: 200 OK

Быстрое восстановление из бэкапа:

```
POST /backup/backups/<id бэкапа>/apply/fast
```

Ответ на успешный запрос: 200 OK

Удаление бэкапа:

```
DELETE /backup/backups/<id бэкапа>
```

Ответ на успешный запрос: 200 OK

55.2 Возврат к предыдущей версии Ideco NGFW

Получение информации о наличии предыдущей версии:

```
GET /system_management/change_sys_root
```

Ответ на успешный запрос:

```
{
   "previous_version": {
      "major": "integer",
      "minor": "integer",
      "build": "integer",
      "timestamp": "integer",
      "vendor": "string",
      "product": "UTM" | "CC",
      "kind": "FSTEK" | "NGFW-FSTEK" | "VPP" | "STANDARD" | "BPF",
      "release_type": "release" | "beta" | "devel"
   }
}
```

- `major` - мажорный номер версии;
- `minor` - минорный номер версии;
- `build` - номер сборки;
- `timestamp` - время сборки версии в формате UNIX timestamp;
- `vendor` - вендор продукта. Значения могут быть произвольными;
- `product` - название продукта;
- `kind` - вид продукта;
- `release_type` - тип редакции.

Если предыдущей версии не было, то значение поля `previous_version` будет `null`.

Возврат к предыдущей версии:

```
POST /system_management/change_sys_root
```

Json-тело запроса:

```
{
   "version": {
      "major": "integer",
      "minor": "integer",
      "build": "integer",
      "timestamp": "integer",
      "vendor": "string",
      "product": "UTM" | "CC",
      "kind": "FSTEK" | "NGFW-FSTEK" | "VPP" | "STANDARD" | "BPF",
      "release_type": "release" | "beta" | "devel"
   }
}
```

- `major` - мажорный номер версии;
- `minor` - минорный номер версии;
- `build` - номер сборки;

- `timestamp` - время сборки версии в формате UNIX timestamp;
- `vendor` - вендор продукта. Значения могут быть произвольными;
- `product` - название продукта;
- `kind` - вид продукта;
- `release_type` - тип редакции.

Ответ на успешный запрос: 200 OK

56. Почтовый релей

Получение статуса почтовых служб:

`GET /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/status`

Ответ на успешный запрос:

```
[
  {
    "name": "string",
    "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
    "msg": [
      "string",
      ...
    ]
  },
  ...
]
```

- `name` - имя демона;
- `status` - одна из строк, означающих состояние демона;
- `msg` - массив строк с сообщениями об ошибках, если ошибки есть.

56.1 Основные настройки

Получение настроек почтового сервера:

`GET /mail/20250219090034/docsUTM/settings/general`

Ответ на успешный запрос:

```
{
  "mail_domain": "string" | "null",
  "mail_hostname": "string",
  "mail_additional_domains": [
    "string",
    ...
  ],
  "mail_relay_domains": [
    "string",
    ...
  ]
}
```

- `mail_domain` - основной почтовый домен. Если не настроен - `null`;

- `mail_hostname` - имя хоста почтового сервера. Если не настроено - `null`;
- `mail_additional_domains` - массив дополнительных почтовых доменов. Если не настроены - пустой массив;
- `mail_relay_domains` - массив relay-доменов. Если не настроены - пустой массив. Каждый элемент массива имеет вид `from_domain|to_domain`, где:
  - `from_domain` - валидное доменное имя;
  - `to_domain` - валидное доменное имя или IP-адрес.

Сохранение настроек почтового сервера:

`PUT /mail/20250219090034/docsUTM/settings/general`

Json-тело запроса:

```
{
  "mail_domain": "string",
  "mail_hostname": "string",
  "mail_additional_domains": [
    "string",
    ...
  ],
  "mail_relay_domains": [
    "string",
    ...
  ]
}
```

- `mail_domain` - основной почтовый домен. Если не настроен - `null`. Не может быть пустым;
- `mail_hostname` - имя хоста почтового сервера. Если не настроено - `null`. Не может быть пустым;
- `mail_additional_domains` - массив дополнительных почтовых доменов. Каждый элемент массива должен быть валидным доменным именем и не может быть пустой строкой или `null`. Может быть пустым;
- `mail_relay_domains` - массив relay-доменов. Может быть пустым. Каждый элемент массива должен иметь вид `from_domain|to_domain`, где:
  - `from_domain` - валидное доменное имя, не может быть пустой строкой или `null`;
  - `to_domain` - валидное доменное имя или IP-адрес, не может быть пустой строкой или `null`.

Ответ на успешный запрос: 200 OK

56.2 Настройки IMAP(S), POP3(S), Web-почты

Получение настроек:

`GET /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/server_access`

Ответ на успешный запрос:

```
{
  "imap_enabled": "boolean",
  "pop3_enabled": "boolean",
  "webmail_enabled": "boolean"
}
```

- `imap_enabled` - `true`, когда IMAP включен, и `false`, когда выключен;
- `pop3_enabled` - `true`, когда POP3 включен, и `false`, когда выключен;

- `webmail_enabled` - `true`, когда интерфейс веб-почты включен, и `false`, когда выключен.

Изменение настроек:

`PATCH /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/server_access`

Json-тело запроса (все или некоторые поля):

```
{
  "imap_enabled": "boolean",
  "pop3_enabled": "boolean",
  "webmail_enabled": "boolean"
}
```

- `imap_enabled` - `true`, когда IMAP включен, и `false`, когда выключен;
- `pop3_enabled` - `true`, когда POP3 включен, и `false`, когда выключен;
- `webmail_enabled` - `true`, когда интерфейс веб-почты включен, и `false`, когда выключен.

Ответ на успешный запрос: 200 OK

56.3 Внешний диск для хранения почты

Получение списка доступных дисков:

`GET /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/ext_hdd/list`

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string"
  },
  ...
]
```

- `id` - идентификатор диска;
- `title` - название.

Подключение диска:

`POST /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/ext_hdd`

Json-тело запроса:

```
{
  "id": "string"
}
```

- `id` - идентификатор диска.

Ответ на успешный запрос: 200 OK

Получение текущего состояния диска для хранения почты:

`GET /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/ext_hdd`

Ответ на успешный запрос:

```
{
  "disk_id": "string" | "null",
  "title": "string" | "null",
  "status": "connecting" | "connected" | "disconnected" | "error" | "check",
  "fs_uuid": "string" | "null",
  "free_size": "integer" | "null",
  "total_size": "integer" | "null",
  "error": "string" | "null"
}
```

- `disk_id` - идентификатор диска. Может быть `null`, если диск не подключен;
- `title` - название диска. Может быть `null`, если диск не подключен;
- `fs_uuid` - идентификатор файловой системы. Может быть `null`, если диск не подключен;
- `status` - текущее состояние диска:
  - `connecting`- диск в процессе монтирования;
  - `connected`- диск подключен и работает нормально;
  - `disconnected`: диск не подключен;
  - `error`- при подключении диска произошла ошибка;
  - `check`- проверка формата почтовых ящиков.
- `free_size` - количество свободного места, байт. Может быть `null`, если диск не подключен;
- `total_size` - размер диска, байт. Может быть `null`, если диск не подключен;
- `error` - текст ошибки, если текущее состояние диска - `error`, иначе - `null`.

Отключение диска:

`DELETE /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/ext_hdd`

Ответ на успешный запрос: 200 OK

56.4 Включенность почтового сервера

Получение настроек:

`GET /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/state`

Ответ на успешный запрос:

```
{
  "enabled": "boolean"
}
```

- `enabled` - опция раздела **Основные настройки**: `true` - включена, `false` - выключена.

Включение/отключение почтового сервера:

`PUT /mail/20250219090034/docsUTM/settings/20250219090034/docsUTM/general/state`

Json-тело запроса:

```
{
  "enabled": "boolean"
}
```

- `enabled` - опция раздела **Основные настройки**: `true` - включена, `false` - выключена.

Ответ на успешный запрос: 200 OK

56.5 Расширенные настройки

Получение настроек:

`GET /mail/20250219090034/docsUTM/settings/advanced/general`

Ответ на успешный запрос:

```
{
  "mail_relay": "string",
  "sender_bcc": "string",
  "recipient_bcc": "string",
  "max_mailbox_size": "integer",
  "max_message_size": "integer",
  "autoexpunge_days": "integer"
}
```

- `mail_relay` - внешний SMTP-релей. Если не настроен - `null`. Не может быть пустой строкой;
- `sender_bcc` - копировать исходящую почту на электронный адрес. Если не настроен - `null`;
- `recipient_bcc` - копировать входящую почту на электронный адрес. Если не настроен - `null`;
- `max_mailbox_size` - максимальный размер почтового ящика в байтах, минимум - 1 000 000;
- `max_message_size` - максимальный размер письма в байтах, минимум - 1 000 000;
- `autoexpunge_days` - количество дней (возраст письма), после которого автоматически удалять из корзины письма. Значения от 0 до 60 (0 - не удалять).

Изменение настроек:

`PUT /mail/20250219090034/docsUTM/settings/advanced/general`

Json-тело запроса:

```
{
  "mail_relay": "string",
  "sender_bcc": "string",
  "recipient_bcc": "string",
  "max_mailbox_size": "integer",
  "max_message_size": "integer",
  "autoexpunge_days": "integer"
}
```

- `mail_relay` - внешний SMTP-релей. Если не настроен - `null`. Не может быть пустой строкой;
- `sender_bcc` - копировать исходящую почту на электронный адрес. Если не настроен - `null`. Не может быть пустой строкой;
- `recipient_bcc` - копировать входящую почту на электронный адрес. Если не настроен - `null`. Не может быть пустой строкой;
- `max_mailbox_size` - максимальный размер почтового ящика в байтах, минимум - 1 000 000;
- `max_message_size` - максимальный размер письма в байтах, минимум - 1 000 000;
- `autoexpunge_days` - количество дней (возраст письма), после которого автоматически удалять из корзины письма. Возможно указать значения от 0 до 60 (0 - не удалять).

Ответ на успешный запрос: 200 OK

56.5.1 Безопасность

Получение состояния переключателей:

`GET /mail/20250219090034/docsUTM/settings/advanced/security/state`

Ответ на успешный запрос:

```
{
  "smtpd_sasl_enabled": "boolean",
  "smtpd_tls_only_auth": "boolean",
  "dnsbl_enabled": "boolean",
  "greylisting_enabled": "boolean",
  "secure_encryption": "boolean"
}
```

- `smtpd_sasl_enabled` - поддержка SASL для аутентификации SMTP-клиентов;
- `smtpd_tls_only_auth` - аутентификация только через защищенное соединение (TLS);
- `dnsbl_enabled` - фильтрация по DNSBL для входящей почты;
- `greylisting_enabled` - фильтрация по серым спискам (greylisting) для входящей почты;
- `secure_encryption` - поддержка только безопасных шифров (TLSv1.2 и выше).

Изменение состояния переключателей:

`PATCH /mail/20250219090034/docsUTM/settings/advanced/security/state`

Json-тело запроса (все или некоторые поля):

```
{
  "smtpd_sasl_enabled": "boolean",
  "smtpd_tls_only_auth": "boolean",
  "dnsbl_enabled": "boolean",
  "greylisting_enabled": "boolean",
  "secure_encryption": "boolean"
}
```

- `smtpd_sasl_enabled` - поддержка SASL для аутентификации SMTP-клиентов;
- `smtpd_tls_only_auth` - аутентификация только через защищенное соединение (TLS);
- `dnsbl_enabled` - фильтрация по DNSBL для входящей почты;
- `greylisting_enabled` - фильтрация по серым спискам (greylisting) для входящей почты;
- `secure_encryption` - поддержка только безопасных шифров (TLSv1.2 и выше).

Ответ на успешный запрос: 200 OK

Получение списка доверенных сетей:

`GET /mail/20250219090034/docsUTM/settings/advanced/security/network`

Ответ на успешный запрос:

```
{
  "postfix_mynetworks": [
    "string"
  ]
}
```

- `postfix_mynetworks` - список доверенных сетей. Если не настроен - пустой массив.

Установка списка доверенных сетей:

`PUT /mail/20250219090034/docsUTM/settings/advanced/security/network`

Json-тело запроса:

```
{
  "postfix_mynetworks": [
    "string"
  ]
}
```

- `postfix_mynetworks` - список доверенных сетей. Если не настроен - пустой массив. Ни один элемент массива не может быть пустой строкой или `null`.

Ответ на успешный запрос: 200 OK

56.5.2 DKIM-подпись

Получение состояния DKIM:

`GET /mail/20250219090034/docsUTM/settings/advanced/dkim/state`

Ответ на успешный запрос:

```
{
  "opendkim_enabled": "boolean"
}
```

- `opendkim_enabled` - `true`, когда DKIM-подпись включена, `false` - когда выключена.

Установка состояния DKIM:

`PUT /mail/20250219090034/docsUTM/settings/advanced/dkim/state`

Json-тело запроса:

```
{
  "opendkim_enabled": "boolean"
}
```

- `opendkim_enabled` - `true`, когда DKIM-подпись включена, `false` - когда выключена.

Ответ на успешный запрос: 200 OK

Получение ключей:

`GET /mail/20250219090034/docsUTM/settings/advanced/dkim`

Ответ на успешный запрос:

```
[
  {
    "public_key": "string",
    "selector": "string",
    "dkim_domain_status": "mismatch" | "error" | "missing" | "set",
    "domain": "string"
  }
]
```

- `public_key` - публичный ключ;
- `selector` - строка вида `ics._domainkey.<домен>.`;
- `dkim_domain_status` - статус наличия публичного ключа в DNS-записи;

- `domain` - домен.

56.6 Антиспам и антивирус

Получение настроек Антиспама и антивируса:

`GET /mail/klms/state`

Ответ на успешный запрос:

```
{
  "enabled": "boolean"
}
```

- `enabled` - `true`, когда KLMS включен, и `false`, когда выключен.

Изменение настроек Антиспама и антивируса:

`PUT /mail/klms/state`

Json-тело запроса:

```
{
  "enabled": "boolean"
}
```

- `enabled` - `true`, когда KLMS требуется включить, и `false`, когда выключить.

Ответ на успешный запрос: 200 OK

Загрузка ключа лицензии:

ВАЖНО! Загрузить ключ лицензии можно только в том случае, когда KLMS включен. Если KLMS выключен, то загрузка ключа недоступна.

`POST /mail/klms/license`

Тело запроса: двоичные данные файла лицензии.

Получение даты/времени обновления баз:

`GET /mail/klms/last_update`

Ответ на успешный запрос:

```
{
  "last_update": "null" | "float"
}
```

- `last_update` - дата/время последнего обновления баз в формате UNIX timestamp; `null`, если невозможно определить статус; 0, если базы не установлены.

Получение даты/времени окончания ключа лицензии:

`GET /mail/klms/license`

Ответ на успешный запрос:

```
{
  "is_active": "null" | "boolean",
  "expiration_date": "null" | "float"
}
```

- `is_active` - `true`, когда ключ лицензии активирован, и `false`, когда не активирован; `null`, если невозможно определить статус активированности.

- `expiration_date` - дата/время окончания действия ключа лицензии в формате UNIX timestamp; `null`, когда ключ отсутствует или невозможно определить статус.

56.7 Правила

56.7.1 Переадресация

Получение правил переадресации:

`GET /mail/rules/alias`

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "recipient": "string",
    "map": [
      "string",
      ...
    ]
  },
  ...
]
```

- `id` - идентификатор правила;
- `recipient` - получатель. Не может быть пустой строкой, максимальная длина - 255 символов;
- `map` - массив адресов для пересылки. Если не настроен - пустой массив. Каждый элемент массива не может быть пустой строкой, максимальная длина - 255 символов.

Добавление правил переадресации:

`POST /mail/rules/alias`

Json-тело запроса:

```
{
  "recipient": "string",
  "map": [
    "string"
  ]
}
```

- `id` - идентификатор правила;
- `recipient` - получатель. Не может быть пустой строкой, максимальная длина - 255 символов;
- `map` - массив адресов для пересылки. Если не настроен - пустой массив. Каждый элемент массива не может быть пустой строкой, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор созданного правила.

Изменение правил переадресации:

`PUT /mail/rules/alias/<id правила>`

Json-тело запроса:

```
{
  "recipient": "string",
  "map": [
    "string",
    ...
  ]
}
```

- `id` - идентификатор правила;
- `recipient` - получатель. Не может быть пустой строкой, максимальная длина - 255 символов;
- `map` - массив адресов для пересылки. Если не настроен - пустой массив. Каждый элемент массива не может быть пустой строкой, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление правил переадресации:

`DELETE /mail/rules/alias/<id правила>`

Ответ на успешный запрос: 200 OK

56.7.2 Разрешенные адреса

Получение списка:

`GET /mail/rules/whitelist`

Ответ:

```
[
  {
    "id": "string",
    "address": "string",
    "comment": "string",
    "type": "integer"
  },
  ...
]
```

- `id` - идентификатор правила;
- `address` - домен/IP-адрес/адрес почты, который будет исключен из проверок на спам. Не может быть пустой строкой, максимальная длина - 255 символов;
- `comment` - комментарий. Может быть пустой строкой, максимальная длина - 255 символов;
- `type` - тип поля `address` (1 - домен, 2 - IP-адрес, 3 - адрес почты).

Создание разрешенного адреса:

`POST /mail/rules/whitelist`

Json-тело запроса:

```
{
  "address": "string",
  "comment": "string"
}
```

- `address` - домен/IP-адрес/адрес почты, который будет исключен из проверок на спам. Не может быть пустой строкой, максимальная длина - 255 символов;

- `comment` - комментарий. Может быть пустой строкой, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор созданного правила.

Изменение разрешенного адреса:

`PUT /mail/rules/whitelist/<id правила>`

Json-тело запроса:

```
{
  "address": "string",
  "comment": "string"
}
```

- `address` - домен/IP-адрес/адрес почты, который будет исключен из проверок на спам. Не может быть пустой строкой, максимальная длина - 255 символов;
- `comment` - комментарий. Может быть пустой строкой, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление разрешенного адреса:

`DELETE /mail/rules/whitelist/<id правила>`

Ответ на успешный запрос: 200 OK

56.7.3 Запрещенные адреса

Получение списка:

`GET /mail/rules/blacklist`

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "address": "string",
    "comment": "string",
    "type": "integer"
  },
  ...
]
```

- `id` - идентификатор правила;
- `address` - домен/IP-адрес/адрес почты, который будет отфильтрован. Не может быть пустой строкой, максимальная длина - 255 символов;
- `comment` - комментарий. Может быть пустой строкой, максимальная длина - 255 символов;
- `type` - тип поля `address` (1 - домен, 2 - IP-адрес, 3 - адрес почты).

Создание запрещенного адреса:

`POST /mail/rules/blacklist`

Json-тело запроса:

```
{
  "address": "string",
  "comment": "string"
}
```

- address - домен/IP-адрес/адрес почты, который будет отфильтрован. Не может быть пустой строкой, максимальная длина - 255 символов;
- comment - комментарий. Может быть пустой строкой, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- id - идентификатор созданного правила.

Изменение запрещенного адреса:

`PUT /mail/rules/blacklist/<id правила>`

Json-тело запроса:

```
{
  "address": "string",
  "comment": "string"
}
```

- address - домен/IP-адрес/адрес почты, который будет отфильтрован. Не может быть пустой строкой, максимальная длина - 255 символов;
- comment - комментарий. Может быть пустой строкой, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление запрещенного адреса:

`DELETE /mail/rules/blacklist/<id правила>`

Ответ на успешный запрос: 200 OK

56.8 Почтовая очередь

56.8.1 Почтовая очередь

Получение очереди:

`GET /mail/mail_queue`

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "arrival_time": "integer",
    "sender": "string",
    "recipient": "string",
    "delay_reason": "string"
  },
  ...
]
```

- `id` - идентификатор письма;
- `arrival_time` - время отправки;
- `sender` - отправитель;
- `recipient` - получатель;
- `delay_reason` - причина задержки. Может быть пустой строкой.

Повторная отправка:

`POST /mail/mail_queue_retry`

Json-тело запроса:

```
{
  "ids": ["string", "string", ...]
}
```

- `ids` - список идентификаторов писем.

Ответ на успешный запрос: 200 OK

Удаление писем из очереди:

`DELETE /mail/mail_queue/ID1,ID2,...`

- `ID1,ID2,...` - список идентификаторов писем.

Ответ на успешный запрос: 200 OK

57. Примеры использования

57.1 Редактирование пользовательской категории контент-фильтра

57.1.1 Основное

Предполагается, что уже созданы и настроены:

- пользователи;
- пользовательская категория **Контент-фильтра** (`users.id.3`);
- правило **Контент-фильтра**, в котором используются созданные пользователи и категория.

Через API требуется редактировать список URL в пользовательской категории (добавить `https://wrong-url.com`), в правила **Контент-фильтра** и пользователей изменения не вносим.

Все приведенные ниже команды выполняются в bash-терминале.

При использовании curl в командной строке Windows замените все одинарные кавычки двойными, при этом кавычки внутри кавычек необходимо экранировать. Пример:

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

1. Авторизуйте администратора:

```
curl -k -c /tmp/cookie -b /tmp/cookie -X POST https://x.x.x.x:8443/web/auth/login --
↪data '{"login": "логин", "password": "пароль", "rest_path": "/"}'
```

- `x.x.x.x` - IP-адрес веб-интерфейса Ideco NGFW.

Ответ на успешный запрос: 200 OK

2. Получите текущий список URL из пользовательских категории:

```
curl -k -b /tmp/cookie https://x.x.x.x:8443/content-filter/users_categories/users.id.3
```

Ответ на успешный запрос: 200 OK

Ответ будет содержать описание всех пользовательских категорий. Среди них требуется найти `users.id.3`:

```
{"id": "users.id.1", "name": "Разрешенный сайты", "comment": "Созданы по умолчанию",
↪"urls": ["translate.google.ru", "translate.google.com", "translate.yandex.ru"]}, {
↪"id": "users.id.2", "name": "Запрещенные сайты", "comment": "Созданы по умолчанию",
↪"urls": []}, {"id": "users.id.3", "name": "Запрещенные для бухгалтеров", "comment":
↪"комментарий", "urls": ["https://yandex.ru"]}
```

3. Отредактируйте список URL:

```
curl -k -b /tmp/cookie -X PUT https://x.x.x.x:8443/content-filter/users_categories/
↪users.id.3 --data '{"name": "Запрещенные для бухгалтеров", "description":
↪"комментарий", "urls": ["https://yandex.ru", "https://wrong-url.com"]}'
```

Ответ на успешный запрос: 200 OK

Результат: Правило **Контент-фильтра**, которое использует эту пользовательскую категорию, будет запрещать пользователям переходить на сайты `https://yandex.ru` и `https://wrong-url.com`.

> **Предупреждение:** Запрос перезапишет ранее созданную пользовательскую категорию. Поэтому при выполнении запроса следует указать все URL (старые и новые - указанные при создании категории и те, которые хотите добавить).

57.2 Создание правила FORWARD

57.2.1 Основное

Задача: создать правило FORWARD для протокола TCP и отредактировать, указав время действия.
Для правила нужно создать:

- Диапазон IP-адресов (`192.168.0.1-192.168.0.20`);
- Список адресов в качестве источника (`9.9.9.9`, `9.9.9.10`);
- Время действия (с 09:00 по 18:00, с понедельника по пятницу).

Все приведенные ниже команды выполняются в bash-терминале.

При использовании curl в командной строке Windows замените все одинарные кавычки двойными, при этом кавычки внутри кавычек необходимо экранировать. Пример:

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

1. Авторизуйте администратора:

```
curl -k -c /tmp/cookie -b /tmp/cookie -X POST https://x.x.x.x:8443/web/auth/login --
↪data '{"login": "логин", "password": "пароль", "rest_path": "/"}'
```

- `x.x.x.x` - IP-адрес веб-интерфейса Ideco NGFW.

Ответ на успешный запрос: 200 OK

2. Создайте объект **Диапазон IP-адресов** с `192.168.0.1` по `192.168.0.20`:

```
curl -k -b /tmp/cookie -X POST https://x.x.x.x:8443/aliases/ip_ranges --data '{"title
↪": "test ip range", "comment": "test ip range", "start": "192.168.0.1", "end": "192.
↪168.0.20"}'
```

Ответ на успешный запрос:

```
{
    "id": "ip_range.id.2"
}
```

3. Создайте объект **Список IP-объектов**:

- Создайте объекты **IP-адрес** для IP `9.9.9.9` и повторите действие для IP `9.9.9.10`. Пример:

  ```
  curl -k -b /tmp/cookie -X POST https://x.x.x.x:8443/aliases/ip_addresses --data '
  ↪{"comment": "комментарий", "title": "название", "value": "9.9.9.9"}'
  ```

  Ответ на успешный запрос:

  ```
  {
      "id": "ip.id.3"
  }
  ```

- Создайте объект типа Список IP-объектов, указав в `values` полученные в прошлом шаге `id` (например: `ip.id.2` и `ip.id.3`):

  ```
  curl -k -b /tmp/cookie -X POST https://x.x.x.x:8443/aliases/lists/addresses --
  ↪data '{"title": "название", "comment": "комментарий", "values": ["ip.id.2",
  ↪"ip.id.3"]}'
  ```

  Ответ на успешный запрос:

  ```
  {
      "id": "address_list.id.2"
  }
  ```

4. Создайте объект **Время**:

```
curl -k -b /tmp/cookie -X POST https://x.x.x.x:8443/aliases/time_ranges --data '{
↪"title":"Рабочее время","comment":"пн-пт 09:00-18:00","weekdays":[1,2,3,4,5],"start
↪":"09:00","end":"18:00", "period": null}'
```

Ответ на успешный запрос: 200 OK

```
{
    "id": "time_range.id.3"
}
```

5. Создайте правило файрвола, используя *id* из пунктов 2 и 3:

```
curl -k -b /tmp/cookie -X POST https://x.x.x.x:8443/firewall/rules/forward --data '{
↪"action": "drop", "comment": "", "destination_addresses": ["ip_range.id.2"],
↪"destination_addresses_negate": false, "destination_ports": ["any"], "enabled":␣
↪true, "hip_profiles": [], "incoming_interface": "any", "outgoing_interface": "any",
↪"protocol": "protocol.tcp", "source_addresses": ["address_list.id.2"], "source_
↪addresses_negate": false, "timetable": ["any"], "parent_id": "f3ffde22-a562-4f43-
↪ac04-c40fcec6a88c"}'
```

Значение `action`:

- `accept` - принять пакет;
- `drop` - отклонить пакет.

Ответ на успешный запрос:

```
{
    "id": 2
}
```

6. Отредактируйте созданное правило, указав время действия:

```
curl -k -b /tmp/cookie -X PUT https://x.x.x.x:8443/firewall/rules/forward/<id␣
↪созданного в пункте 5 правила> --data '{"action": "drop", "comment": "",
↪"destination_addresses": ["ip_range.id.2"], "destination_addresses_negate": false,
↪"destination_ports": ["any"], "enabled": true, "hip_profiles": [], "incoming_
↪interface": "any", "outgoing_interface": "any", "protocol": "protocol.tcp", "source_
↪addresses": ["address_list.id.2"], "source_addresses_negate": false, "timetable": [
↪"time_range.id.1"], "parent_id": "f3ffde22-a562-4f43-ac04-c40fcec6a88c"}'
```

Ответ на успешный запрос: 200 OK