Пользовательская документация

Ideco NGFW

нояб. 09, 2024

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 и client-to-site (с 2FA), протоколы IKEv2/IPSec, L2TP/IPSec, SSTP, Wireguard)
- Логирование действий администратора
- Управление через Центральную консоль
- 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

В разделе **NGFW** личного кабинета находится информация о зарегистрированных вами серверах и имеющихся лицензиях.

2.1 Схема лицензирования

У лицензии Ideco NGFW есть три основные характеристики.

Количество пользователей Ideco NGFW: максимальное количество авторизованных (подключенных к интернету) пользователей локальной сети клиента или VPN-подключения пользователей, трафик которых проверяется и контролируется шлюзом.

Редакция Ideco NGFW (FREE и Enterprise): набор доступных к использованию модулей в системе и особенности их работы.

Срок действия лицензии: в редакциях FREE 5 лет, Enterprise бессрочно и Enterprise-demo 40 дней.

Различия между редакциями Ideco NGFW опубликованы на сайте: https://ideco.ru/sravnenie-versiy

2.2 Виды лицензий

2.2.1 Enterprise-demo - 40-дневная пробная версия

- Авторизация до 10 000 пользователей
- Срок действия лицензии (включены все модули, кроме технологий Касперского для фильтрации почтового трафика) 40 дней
- Техническая поддержка на 40 дней

Эту лицензию нельзя переназначить на другой сервер или переместить в свободные. **Выдается автоматически один раз при регистрации сервера.**

2.2.2 Enterprise - коммерческая

- Количество авторизованных пользователей ограничено лицензией
- Включены модули интеграции с **Active Directory**, **Контроль приложений**, **Предотвращение вторжений**, расширенный **Контент-фильтр**
- Доступ к технической поддержке на период активности подписки

Право на использование лицензии действует 5 лет с момента приобретения (согласно п.4, статья 1235 ГК РФ).

Модуль *Антивируса Kaspersky* и *Расширенная база правил (от Лаборатории Касперского)* приобретаются отдельно (для покупки вы можете обратиться в отдел продаж).

После окончания действия подписки:

- **Предотвращение вторжений** - остается доступ к старой отчетности, но защита периметра отключается;
- **Расширенный Контент-фильтр** - остаются доступны только пользовательские категории;
- **Техническая поддержка** - перестает оказываться техническая поддержка сервера по этой лицензии.

На остальную функциональность сервера ограничения подписки не распространяются.
Стандартная стоимость лицензии включает годовую подписку. Иные сроки подписки и результирующая стоимость лицензии обсуждаются в отделе продаж компании «Айдеко».

2.2.3 FREE - бесплатная лицензия, действует 5 лет

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

Техническая поддержка не оказывается. Недоступны модули: расширенная база правил **Предотвращения вторжений** (от Лаборатории Касперского), антивирусы **Kaspersky** и **Kaspersky Anti-Spam**.

Как добавить бесплатную лицензию в личный кабинет MY.IDECO:

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

Подсказка: Более подробная таблица сравнения видов лицензий доступна на сайте https://ideco.ru/sravnenie-versiy.

Подсказка: Если у сервера Ideco NGFW нет лицензии или срок действия лицензии (не подписки) закончился, будет отключена авторизация пользователей и фильтрация трафика. При отсутствии лицензии доступен перехват DNS-запросов и подключение по SSH при включении удаленного помощника.

2.3 Привязка лицензии к серверу

Подсказка: При изменении 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** и нажмите **Обновить информацию о лицензии**.

Привязать лицензию можно двумя способами:

1. Во вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ . Далее в выберите нужную лицензию и сохраните изменения нажав **Привязать лицензию**.

2. Во вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите  . Далее укажите нужный сервер и сохраните изменения нажав **Привязать**.

Предупреждение: Назначьте имеющиеся коммерческие лицензии на любой зарегистрированный вами 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 лицензия будет также удалена.

2.4 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.

2.5 Контроль и учет сетевых устройств на NGFW

- Для доступа сетевого устройства (хоста) в интернет через NGFW с возможностью контроля его трафика, это устройство должно быть авторизовано на NGFW под учетной записью пользователя;
- 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;
- Сессия авторизации учетной записи привязана к IP-адресам хостов на протяжении действия сессии;
- Учетная запись может быть авторизована несколькими способами. Подробнее в статье ***Авторизация пользователей***;
- Неавторизованный на NGFW хост не имеет доступа во внешние сети;
- Сессии авторизации пользователя, не проявляющего активность, завершаются по тайм-ауту (подробнее об установке тайм-аута в *статье*) и могут быть заняты новыми сессиями пользователей. Таким образом обеспечивается конкурентность процесса авторизации пользователей на NGFW.

3. Системные требования и источники обновления данных Ideco NGFW

3.1 Системные требования

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. Дополнительный SSD при использовании почтового сервера.
Сеть	Две сетевые карты (или два сетевых порта) 100/1000 Mbps. Рекомендуется использовать карты на чипах Intel. Поддерживаются Realtek, D-Link и другие.
Гипервизоры	VMware, Microsoft Hyper-V (виртуальные машины 2-го поколения), VirtualBox, KVM, Citrix XenServer.
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 NGFW:

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.

Подсказка: 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.

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

3.2 Примеры конфигураций

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

Количество пользователей	Модель процессора	Объем оперативной памяти	Дисковая подсистема	Сетевые адаптеры
до 80	Intel Core i3, i5 или совместимый	16 ГБ	150 ГБ	2 шт.
до 350	Intel Xeon-D 1537, Atom C-3758 или совместимый	16 ГБ	240 ГБ	2 шт.
от 300 до 2000	Intel Xeon E-22, Xeon-D 1577 или совместимый	32 ГБ	480 ГБ	2 шт.
от 2000 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.v16.ideco.dev;
- Обновление баз **Контент-фильтра**: content-filter.v16.ideco.dev;
- Отсылка анонимной статистики: gatherstat.v16.ideco.dev;
- Обновления баз GeoIP: ip-list.v16.ideco.dev;
- Обмен информации о лицензии: license.v16.ideco.dev;
- Отправка отчетов по почте: send-reports.v16.ideco.dev;
- Обновления suricata: suricata.v16.ideco.dev;
- Обновления системы: sysupdate.v16.ideco.dev;
- Синхронизация времени: ntp.ideco.ru;
- Антивирус Касперского для обновления баз использует список серверов, указанный на официальном сайте «Лаборатории Касперского».

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

Описание линейки программно-аппаратных комплексов доступно по ссылке.

Внимание: 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	01.01.2023
8	08.09.2020	01.01.2023	01.01.2023	01.01.2023
9	28.12.2020	01.01.2023	01.01.2023	01.01.2023
10	30.07.2021	01.01.2023	01.01.2023	01.01.2023
11	03.11.2021	01.01.2024	01.01.2024	01.01.2024
12	04.05.2022	01.01.2024	01.01.2024	01.01.2024
13	01.09.2022	01.01.2024	01.01.2024	01.01.2024
14	27.01.2023	01.01.2024	01.01.2024	01.01.2024
15	29.08.2023	01.07.2024	01.07.2024	01.07.2024
16	28.12.2023	01.10.2024	01.01.2025	01.01.2026
17	07.05.2024	01.01.2025	01.06.2025	01.01.2027
18	11.10.2024	01.05.2025	01.10.2025	01.05.2027

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. Личный кабинет my.ideco

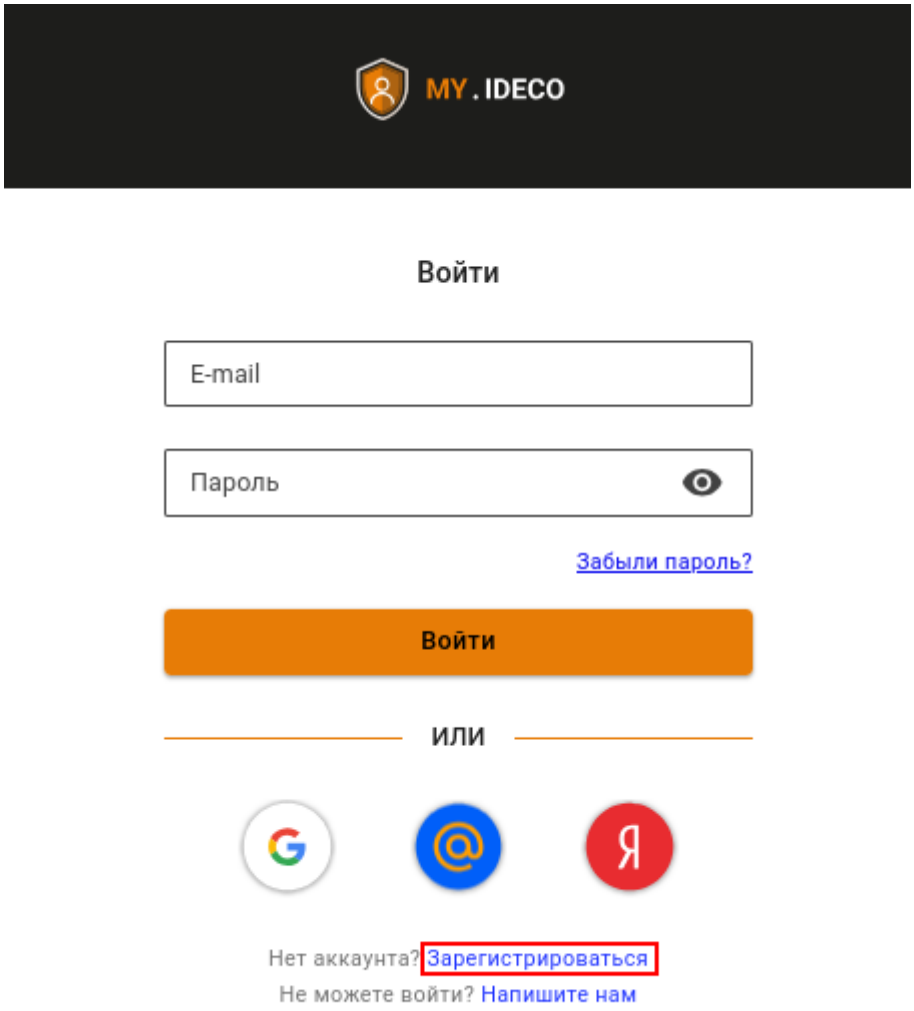
Подсказка: Личный кабинет my.ideco.ru позволяет пользователю получить информацию:

- об имеющихся лицензиях;
- о сроке окончания подписки на обновления модулей и технической поддержки.

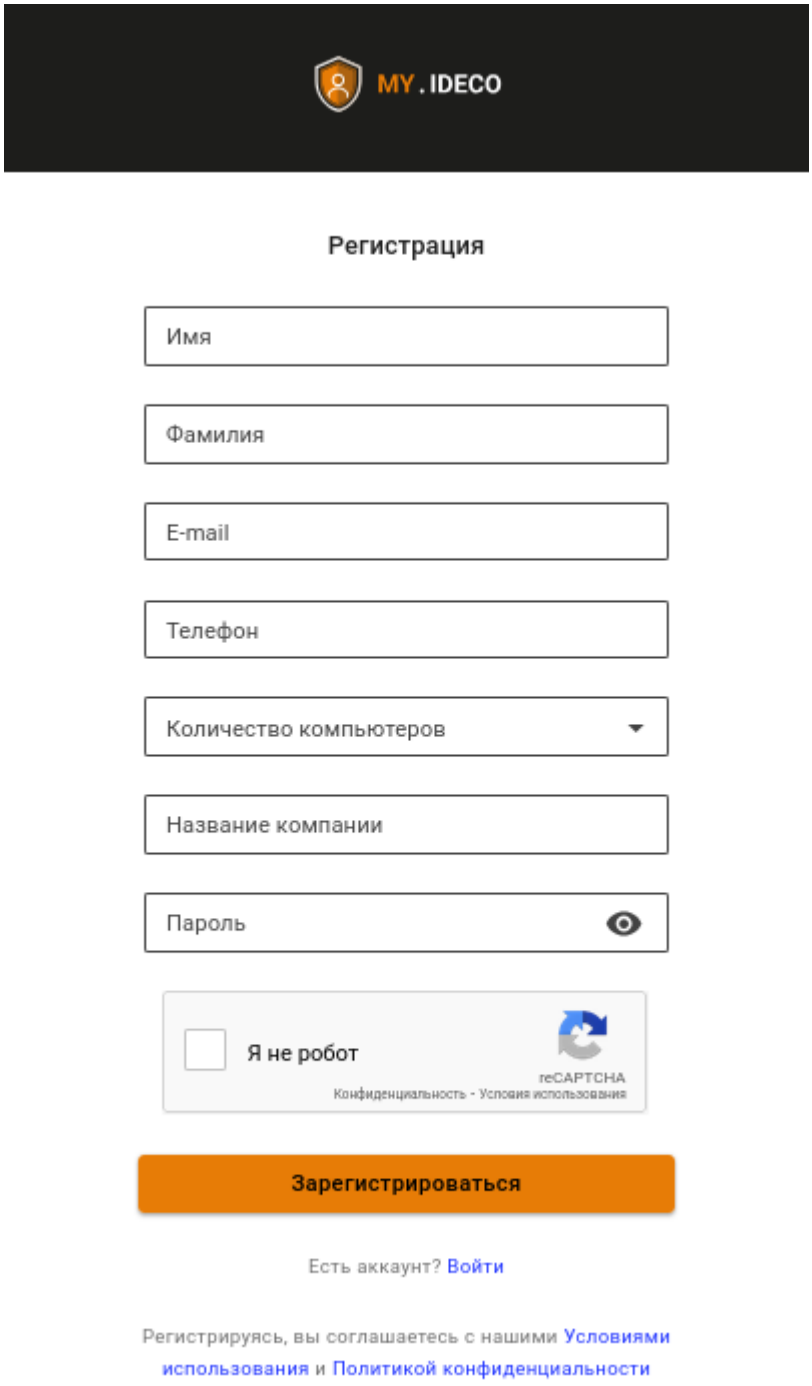
6.1 Регистрация на my.ideco

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.

6.2 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. Подготовка к установке на устройство

7.1 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*.

7.2 Настройка гипервизора

Предупреждение: Для установки Ideco NGFW нужно включить режим UEFI в настройках виртуальной машины.

Подсказка: Обязательные условия для работы Ideco NGFW:

- Поддержка UEFI;
- Отключить режим Legacy загрузки (он также может называться CSM);
- Отключить опцию Secure Boot в UEFI.

Ideco NGFW поддерживает работу на следующих гипервизорах:

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

7.2.1 Общие рекомендации

- Тип ОС для создания виртуальной машины: **Linux Fedora 64 bit**;
- Минимальный размер жесткого диска: **150 ГБ**;
- Минимальное количество оперативной памяти: **16 ГБ**;
- Внутренние часы ВМ должны быть настроены на хранение времени во временной зоне UTC.

Предупреждение: Если при установке Ideco NGFW появилась ошибка с текстом **Требуется не менее 16 ГБ оперативной памяти** и при этом указан рекомендуемый размер оперативной памяти, то уменьшите размер ресурсов, выделенных под видеопамять, до минимального.

Подсказка: Если при установке Ideco NGFW появилось окно с надписью **Installation in BIOS mode is not supported**, проверьте включение режима UEFI в настройках виртуальной машины.

7.2.2 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).

Видеоинструкция по настройке виртуальной машины:

https://www.youtube.com/watch?v=238bs_4ObPY

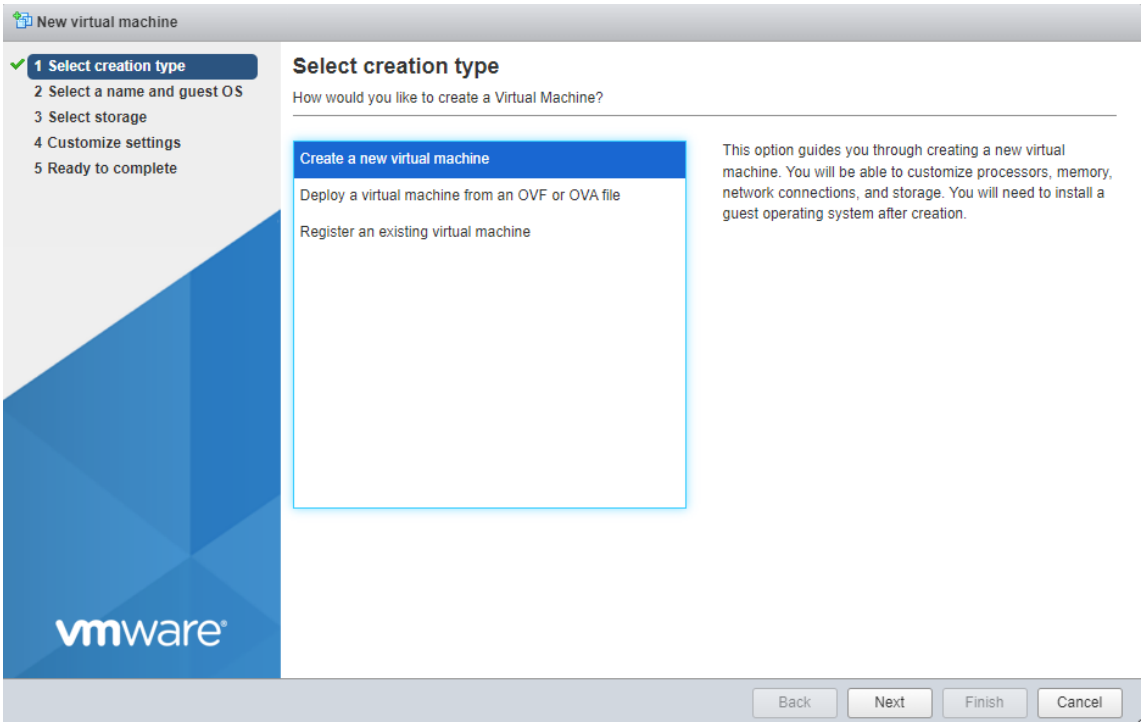
7.2.3 VMware ESXi 6.7

- Перед установкой Ideco NGFW увеличьте размер видеопамяти для виртуальной машины до 16 МБ;
- Используйте виртуальные сетевые адаптеры **vmxnet3**.

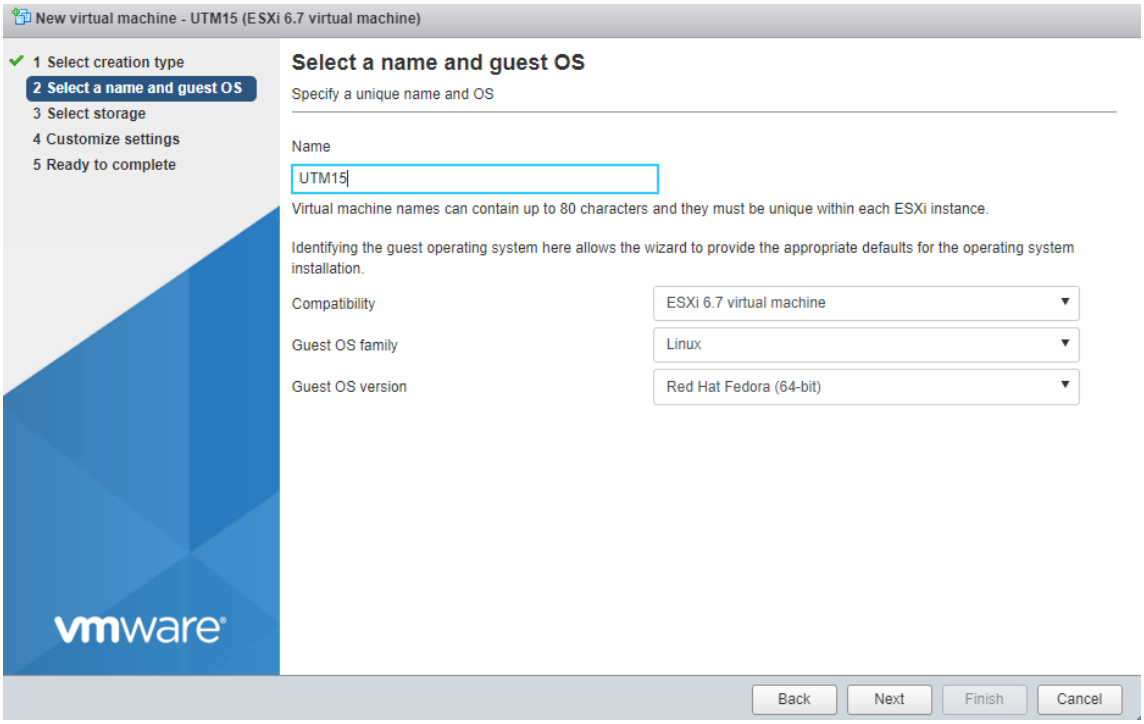
Настройка:

Перед установкой Ideco NGFW загрузите образ, скачанный с MY.IDECO, на VMware ESXi. При настройке виртуальной машины потребуется указать его путь.

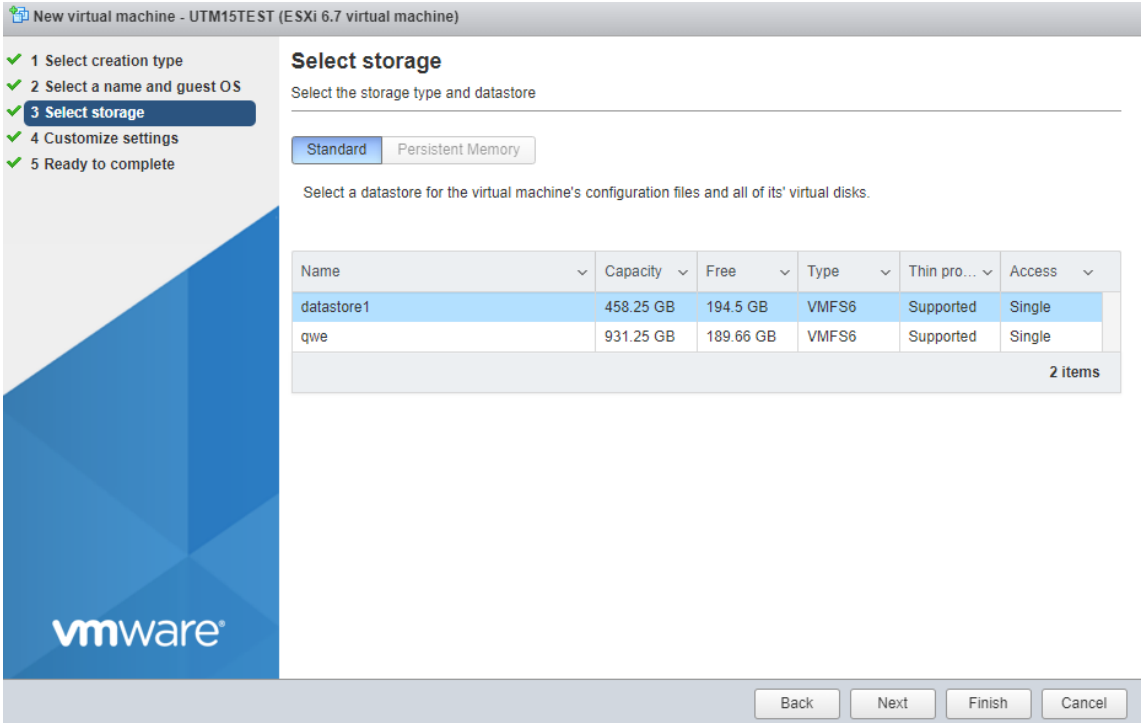
1. Создайте виртуальную машину:



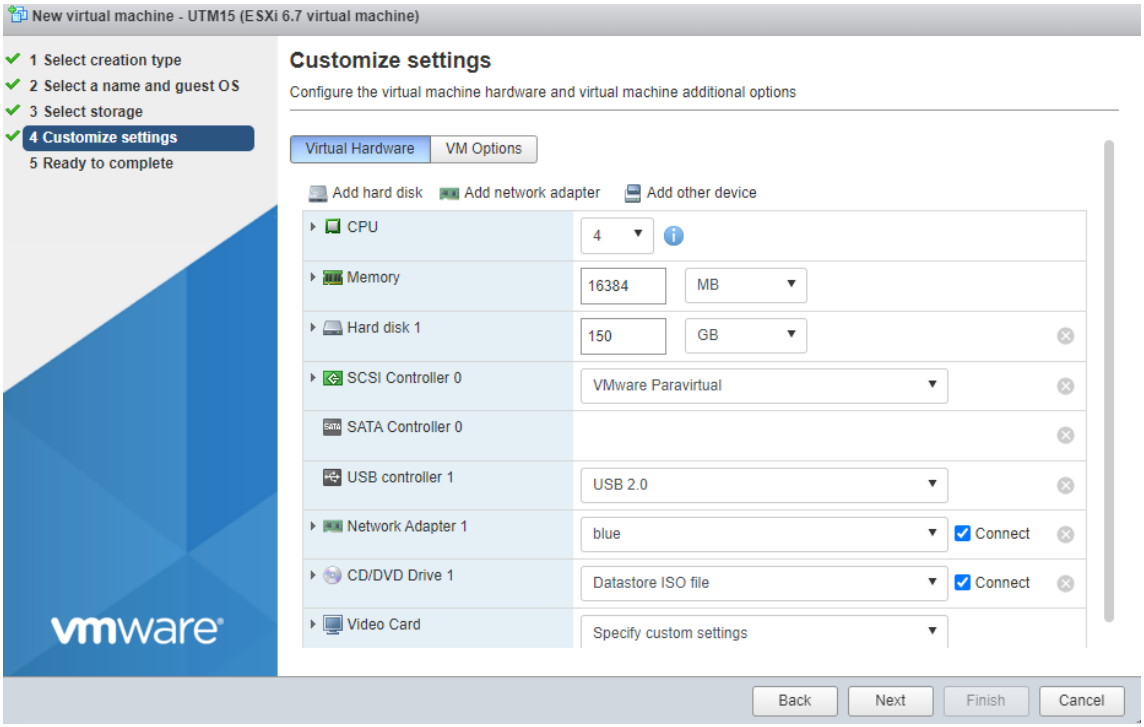
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



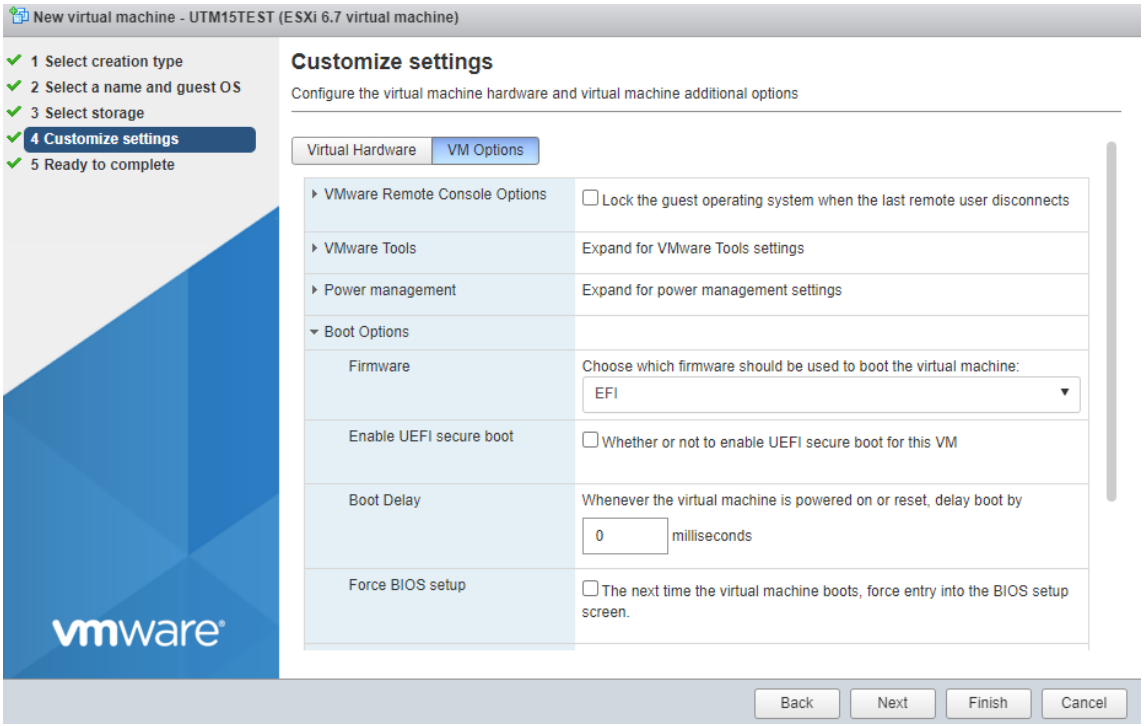
3. Выберите хранилище для виртуальной машины:



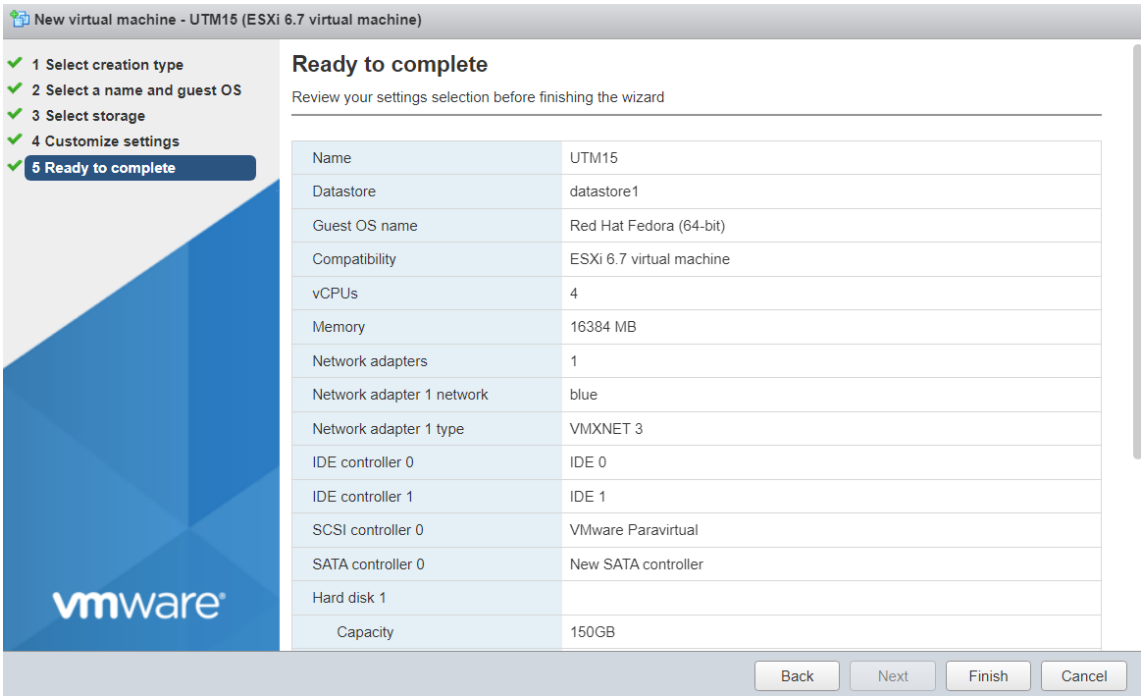
4. Установите размер оперативной памяти **16ГБ** и размер диска **150ГБ**. После выберите в поле **CD/DVD Drive** Datastore ISO file и укажите путь к загрузочному образу:



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



6. Нажмите **Finish**:



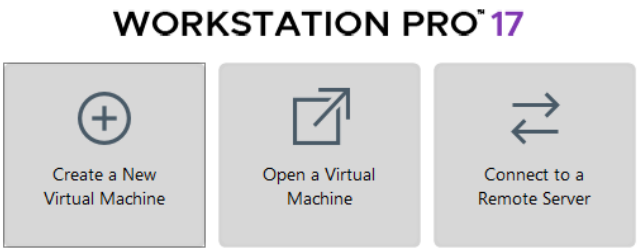
Подсказка: При установке Ideco NGFW на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

7.2.4 VMware Workstation 17.0

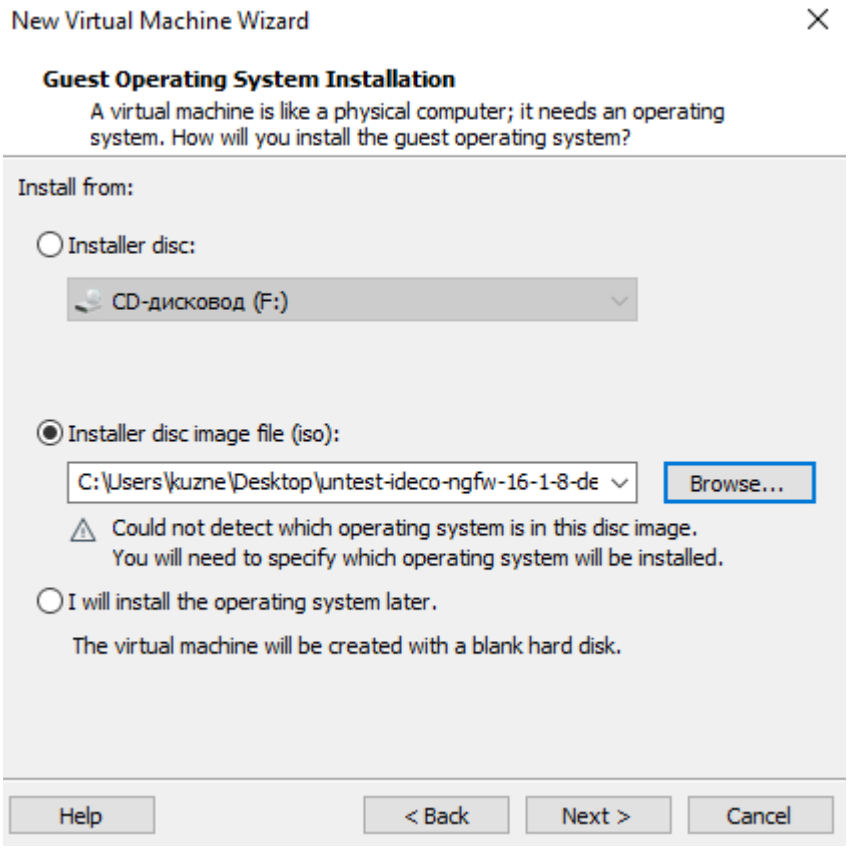
- Перед установкой Ideco NGFW увеличьте размер видеопамяти для виртуальной машины до 16 МБ;
- Используйте виртуальные сетевые адаптеры **vmxnet3**.

Настройка:

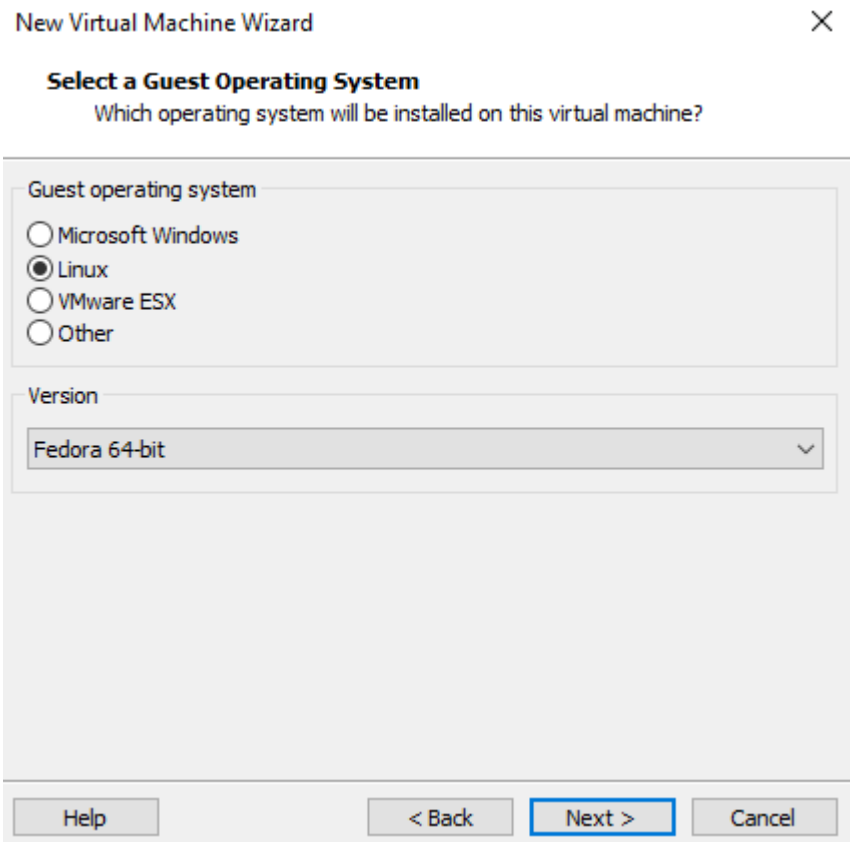
1. Создайте виртуальную машину, нажав **Create a New Virtual Machine**:



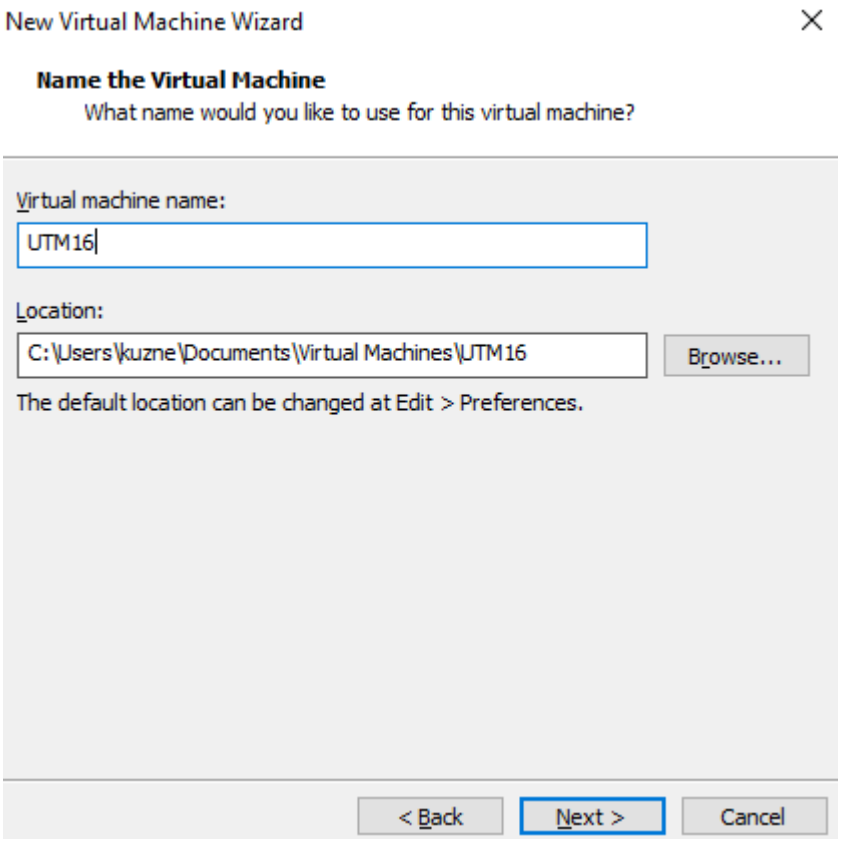
2. Укажите загрузочный ISO-образ:



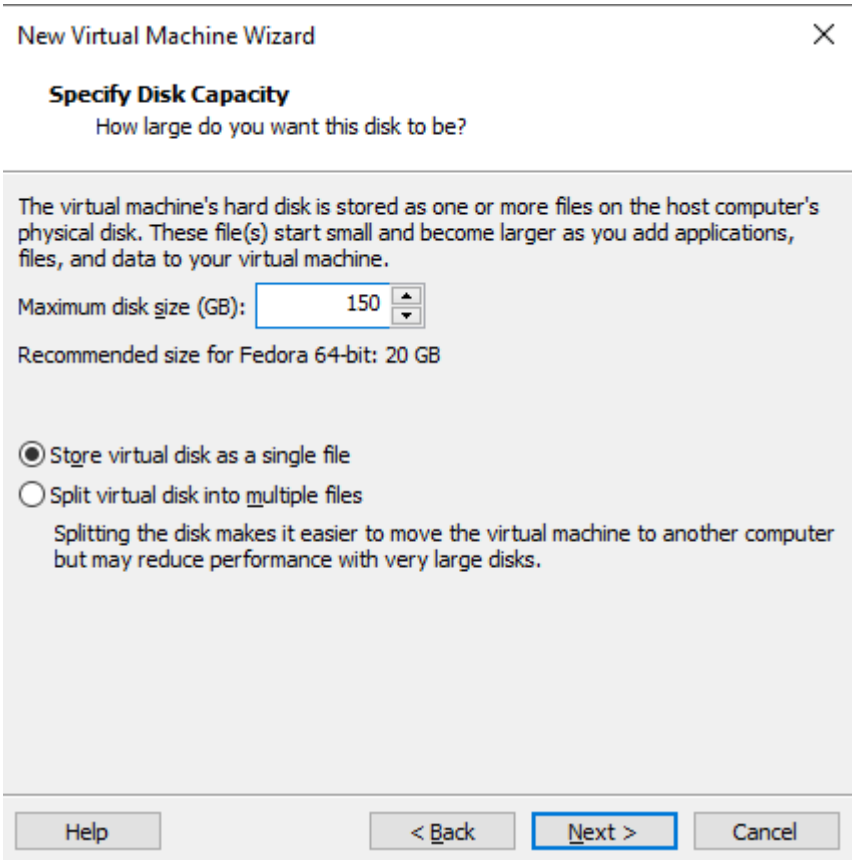
3. Выберите гостевую операционную систему **Linux** и в раскрывающемся списке укажите тип **Fedora 64-bit**:



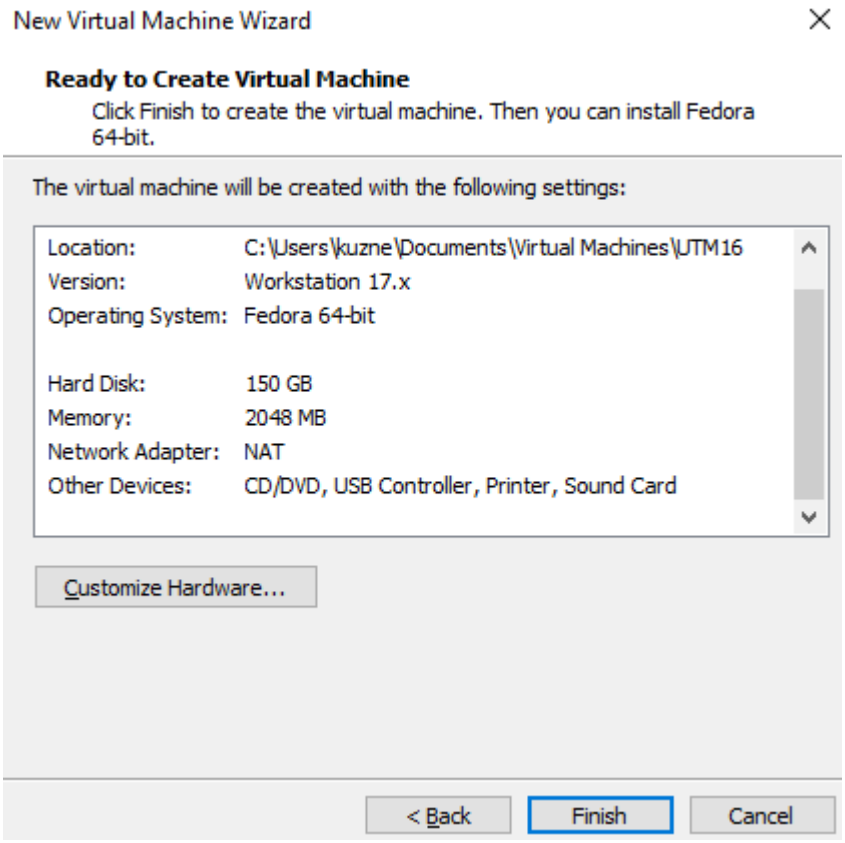
4. Укажите имя виртуальной машины и директорию для создания виртуального диска:



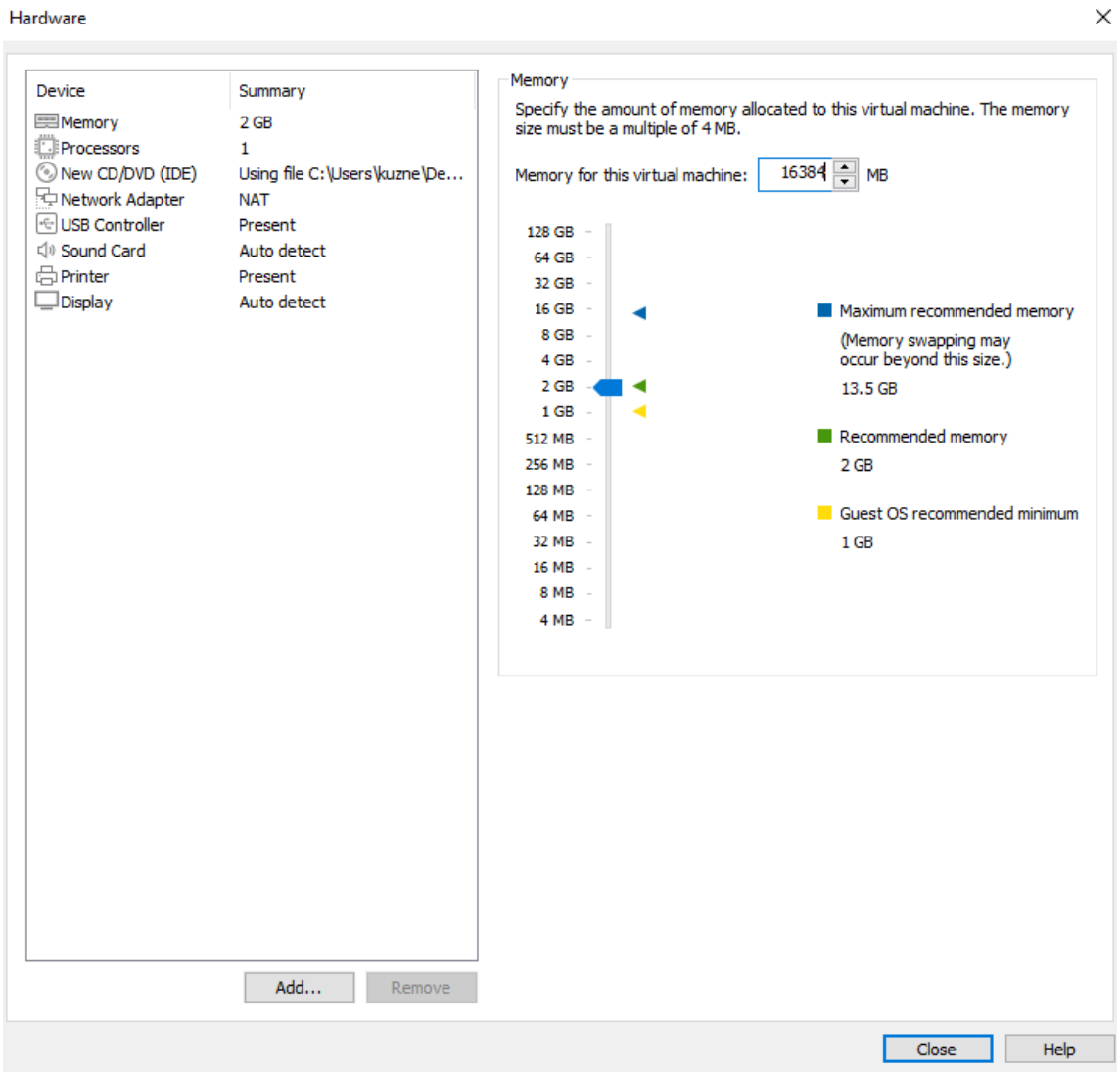
5. Укажите размер вирутального жесткого диска **150ГБ**:



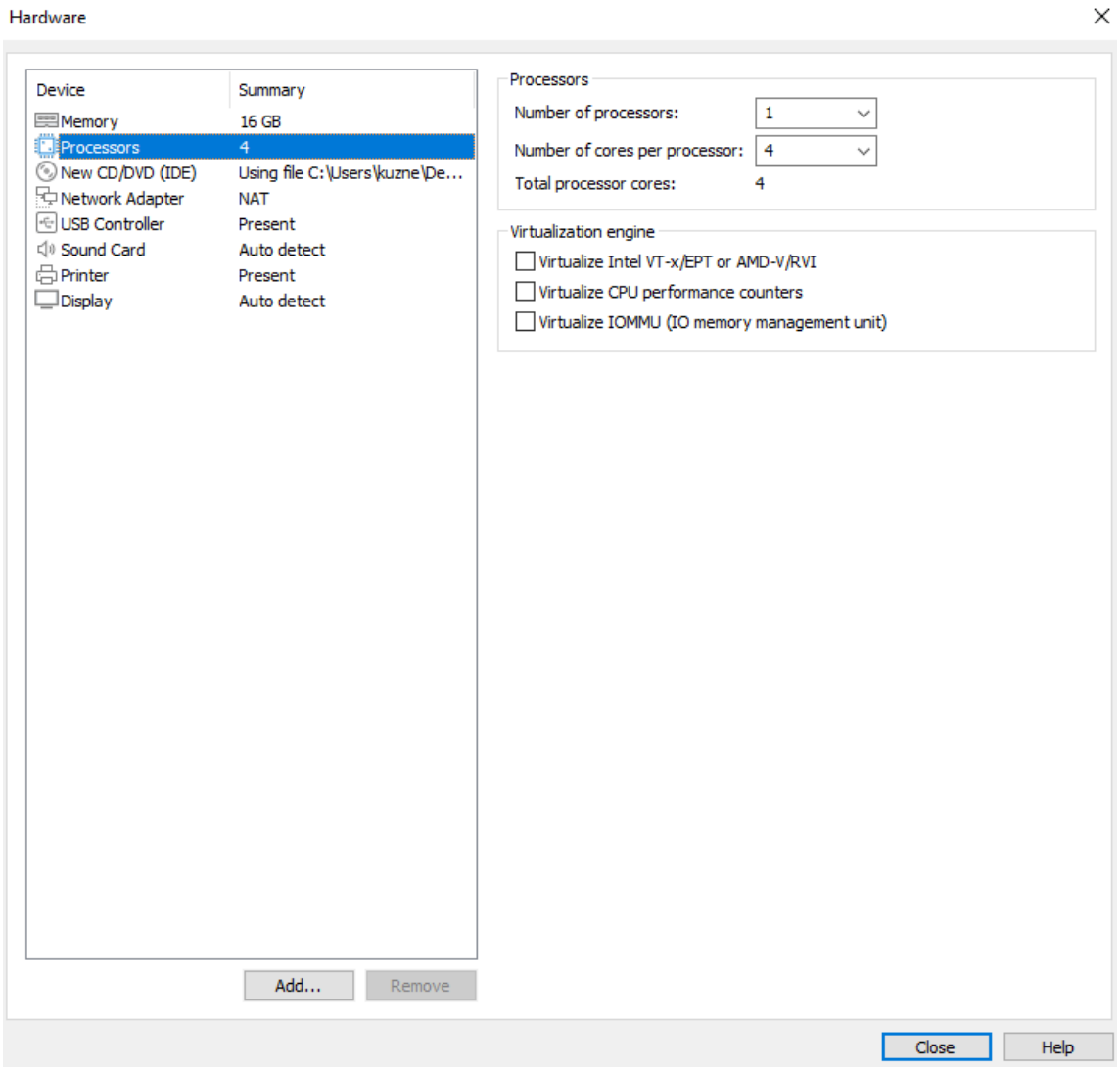
6. Выберите **Customize Hardware** для изменения настроек виртуальной машины:



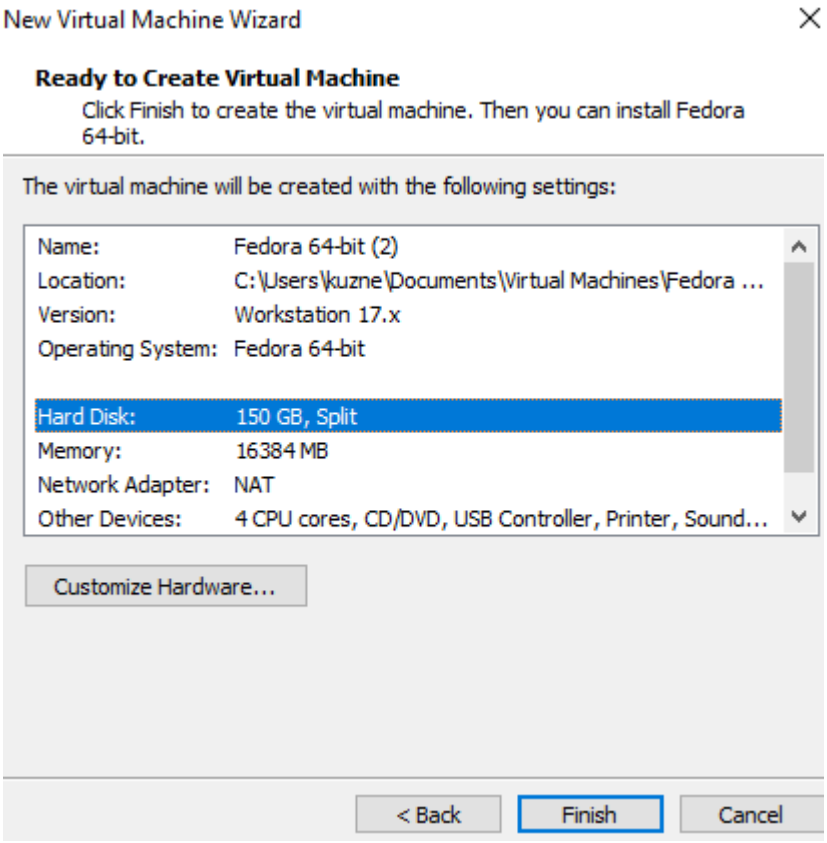
7. Укажите размер виртуальной оперативной памяти **16384МБ**:



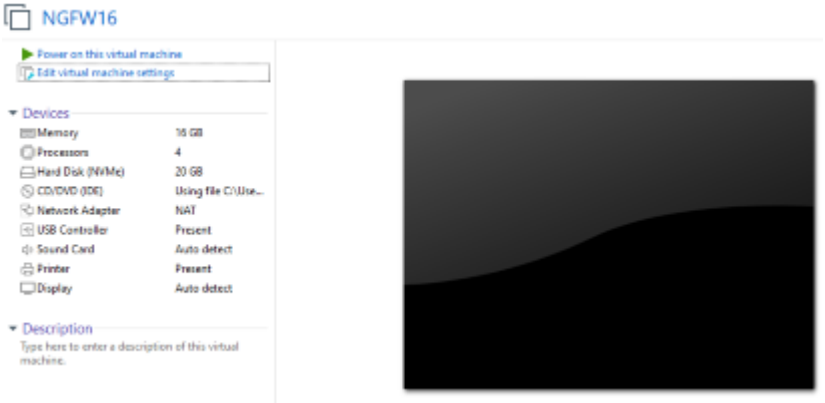
8. Укажите количество ядер процесса равное 4:



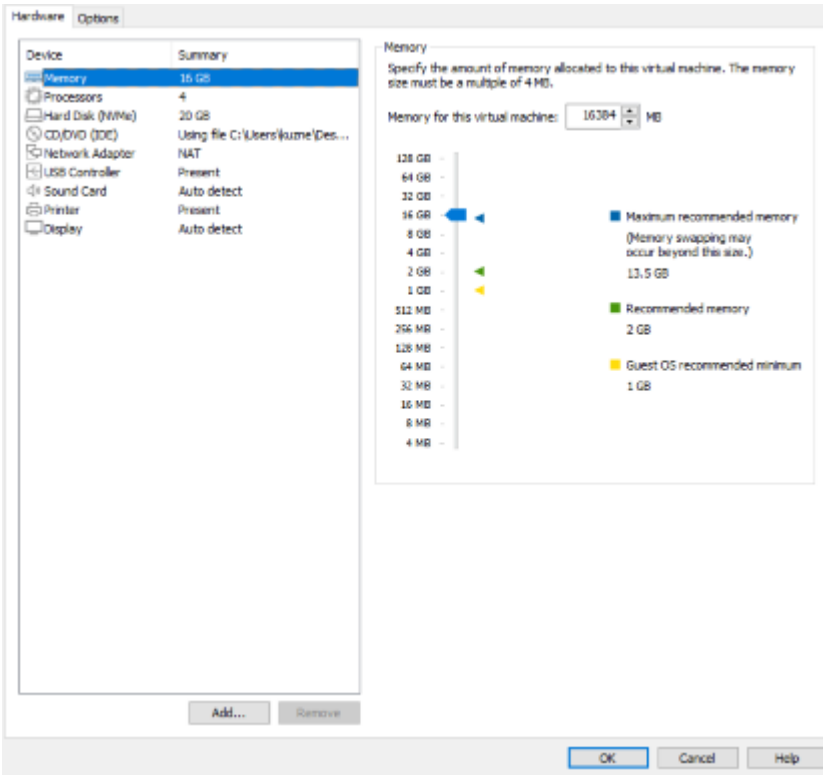
9. Выйдите из меню и нажмите **Finish** для окончания настройки:



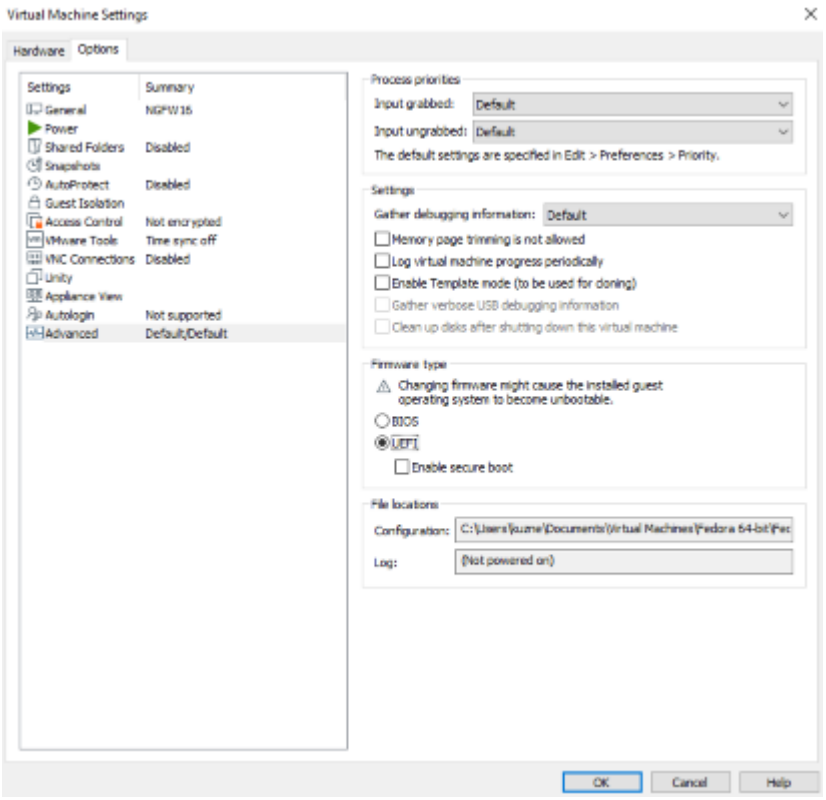
10. Перейдите в окно виртуальной машины и нажмите **Edit virtual machine settings**:



11. Перейдите во вкладку **Options**:



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



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

7.2.5 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:

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

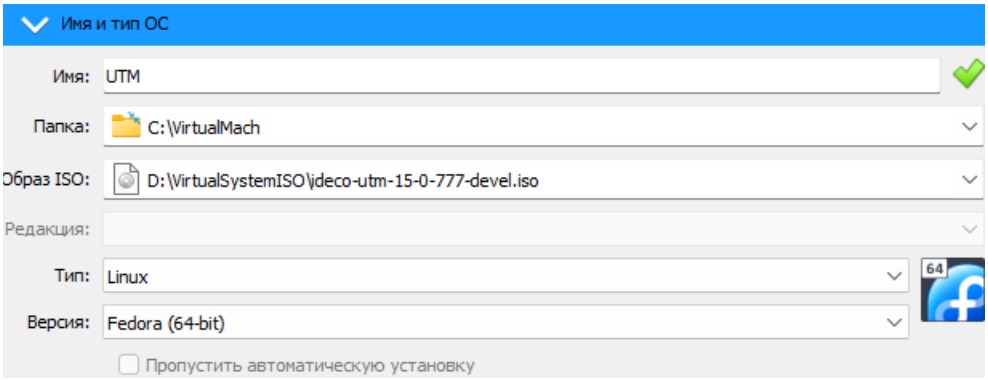
После 3 шага начнется загрузка с установочного носителя.

7.2.6 VirtualBox 7.0.12

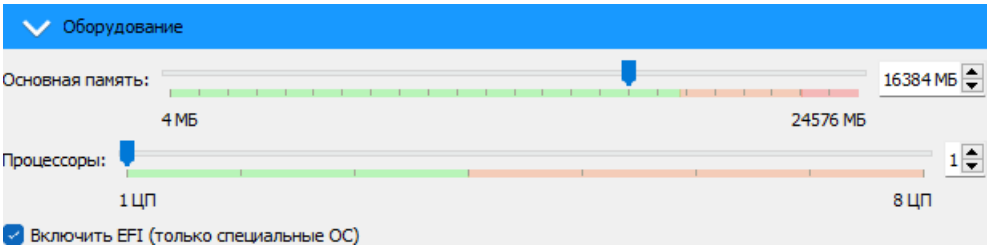
- По умолчанию при создании виртуальной машины создается 1 сетевая карта с типом подключения **NAT**.

Настройка:

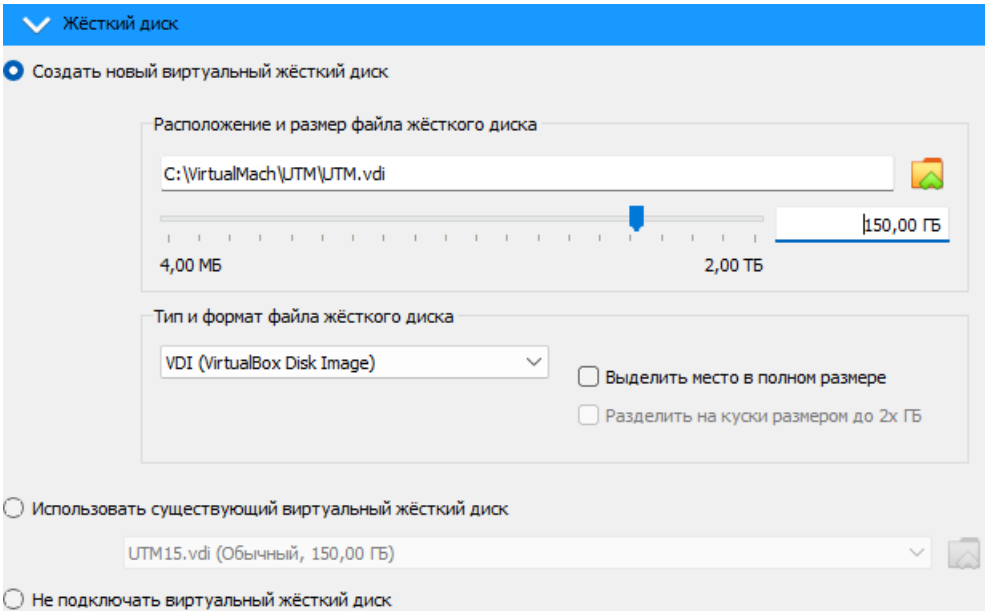
1. Укажите **Имя** виртуальной машины (ВМ), выберите директорию для ВМ и установите путь до загрузочного образа NGFW. Остальные параметры установите как на скриншоте:



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



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

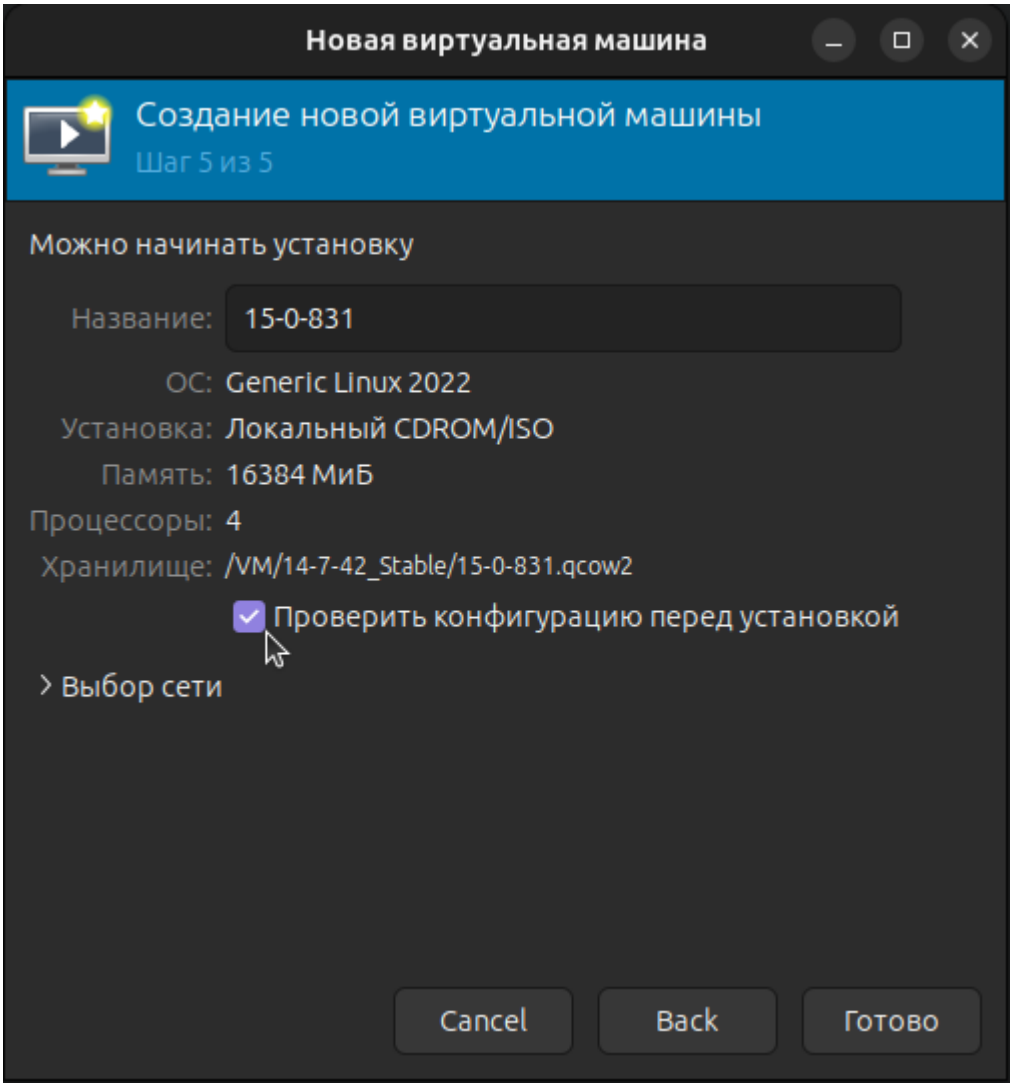


4. Нажмите **Готово**

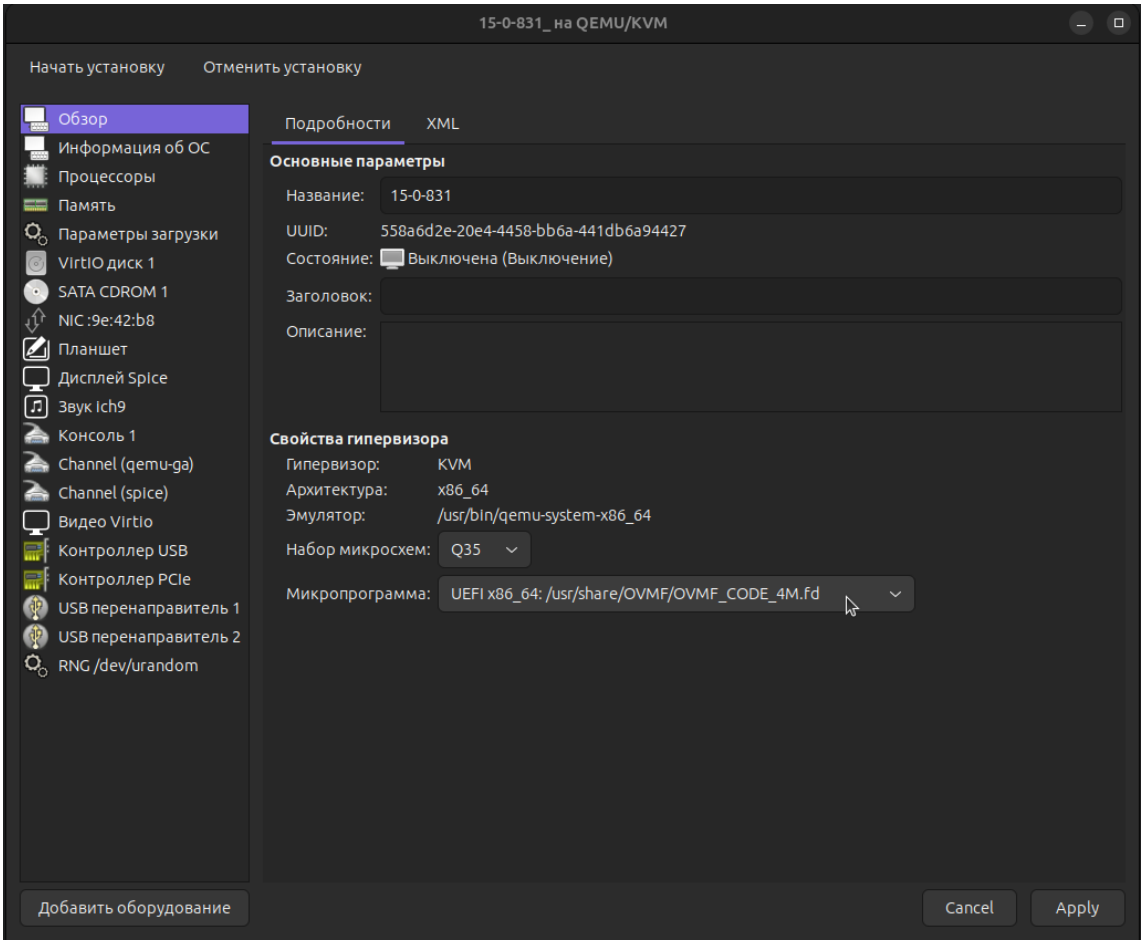
7.2.7 KVM

Настройка:

1. При установке Ideco NGFW выберите тип операционной системы - **Fedora**
2. На пятом шаге (virtm-manager) установки обязательно поставьте галочку **Проверить конфигурацию перед установкой** и нажмите кнопку **Готово**.



3. Для дисков и сетевых карт измените интерфейс на **virtio.**
4. Для дисков используйте режим кеширования **writeback**, если диски хранятся в qcow2 или raw-файлах. Если нет - проконсультируйтесь у администратора хранилища или нашей технической поддержки относительно 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`.

Далее начнется установка Ideco NGFW на виртуальную машину. Подробнее об установке в статье *Установка*

Подсказка: При возможных проблемах проверьте соответствие параметров виртуальной машины *общим рекомендациям*.

7.3 Подготовка загрузочного диска

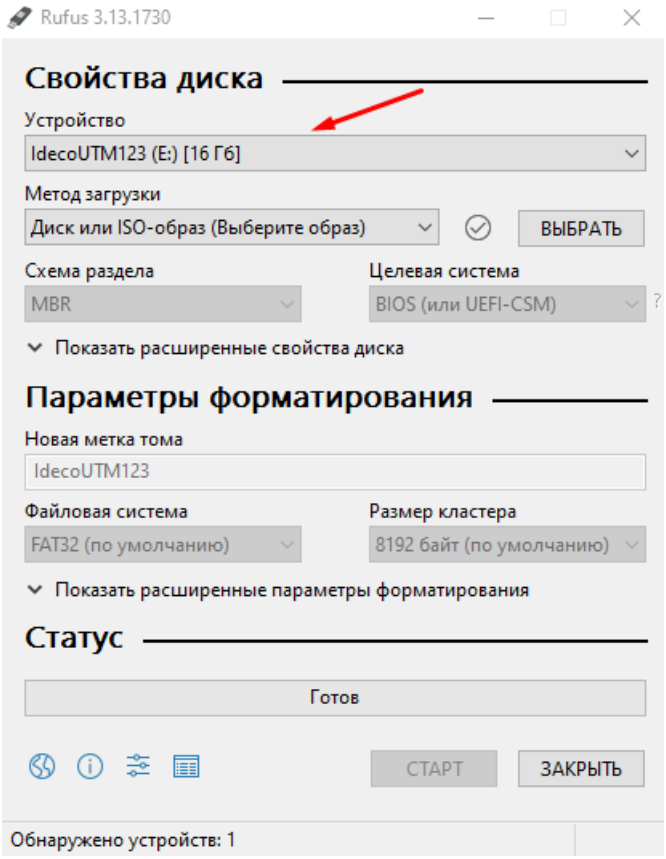
Подсказка: При записи ISO образа вся информация с USB-накопителя будет удалена.

Подсказка: Подробнее об установке Ideco NGFW после создания загрузочного диска можно прочитать в статье *Установка*.

Для установки на отдельный сервер нужно подготовить загрузочный USB-диск.

7.3.1 В среде Windows

1. Скачайте программу Rufus и запустите скачанный файл.
2. Выберите нужный USB-диск в пункте **Устройство**:



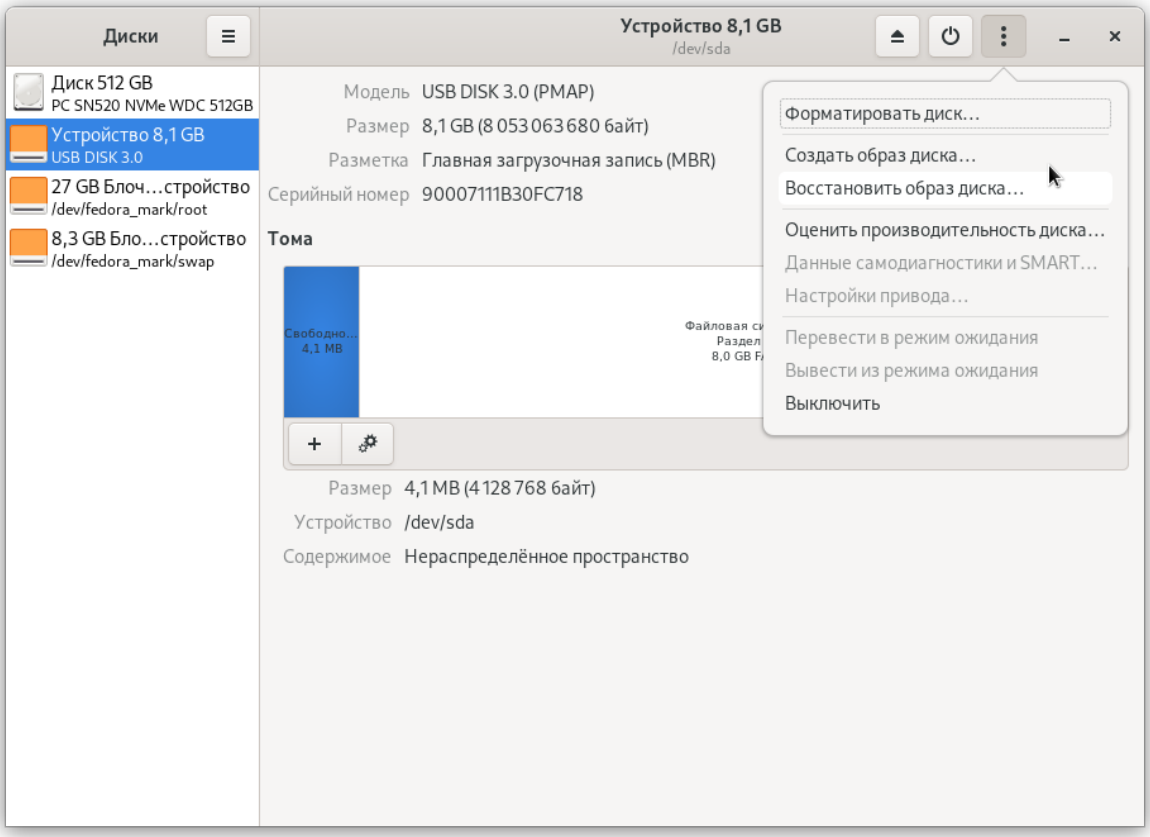
3. Выберите метод загрузки **Диск или ISO-образ**.
4. Нажмите на кнопку **Выбрать** и откройте скачанный образ Ideco NGFW.
5. Нажмите **Старт** и в появившемся окне выберите пункт **Запись в режиме DD-образ**.
6. В диалоговом окне подтвердите запись на USB-диск.

Шаги по установке Ideco NGFW описаны в статье *Процесс установки*.

7.3.2 В среде Linux

Создать загрузочный USB-диск в Linux можно двумя способами:

С помощью программы gnome-disks:



Вручную в терминале:

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
```

8. Установка

8.1 Процесс установки

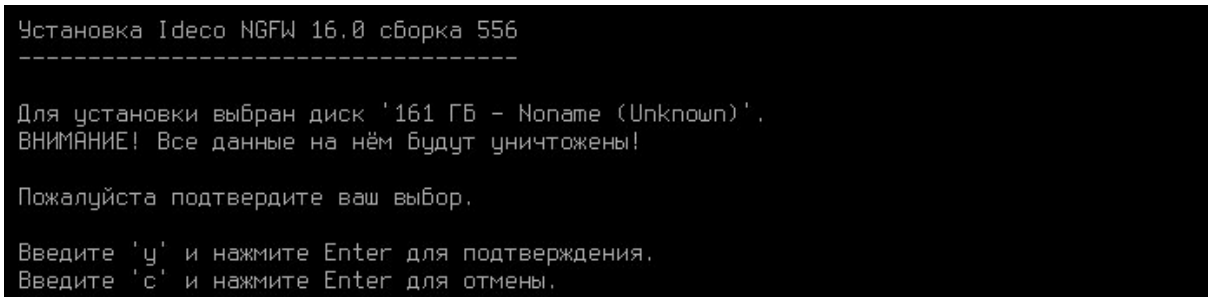
Подсказка: При установке Ideco NGFW с загрузочного USB-диска выберите загрузку с USB-диска в настройках UEFI компьютера.

Ссылка на видеоинструкцию по установке Ideco NGFW

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 вы находитесь:

```
Выберите временную зону.

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

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

4. Настройте дату и время в соответствии с вашей временной зоной. **Обязательно проверьте правильность даты и времени**:

```
Текущая дата и время: 15 августа 2023, 12:58.

Данные указаны правильно?

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

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

8.2 Создание учетной записи администратора

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

```
Внимание! Аккаунт администратора отсутствует.
Требуется предварительно его создать.

Создание аккаунта администратора.

Введите новый логин и нажмите Enter.

# admin

Введите новый пароль и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
#

Повторите пароль и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
#
Аккаунт администратора создан успешно.

Нажмите любую клавишу для перехода к локальному меню.
```

Требования к паролю:

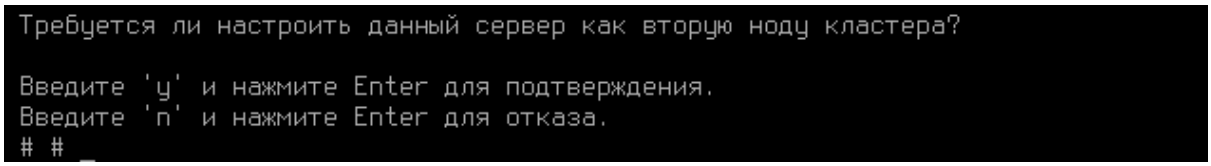
- **Минимальная длина пароля** - 12 символов;
- **Содержит только строчные и заглавные латинские буквы**;
- **Содержит цифры**;
- **Содержит специальные символы** (! # $ % & „ * + и другие).

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 введении пароля, поскольку в будущем это может привести к проблемам при авторизации администратора.

8.3 Настройка второй ноды кластера

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



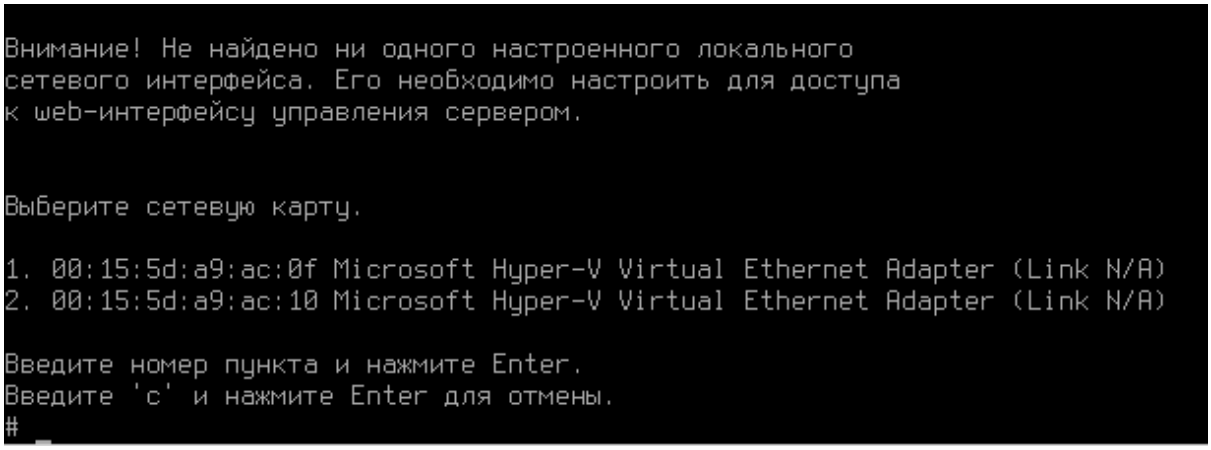
2. Для продолжения настройки воспользуйтесь статьей *Кластеризация*.

8.4 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 нужно настроить локальный интерфейс в локальном меню шлюза:

1. Введите номер сетевого адаптера под локальный интерфейс:



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

```
Настроить локальную сеть автоматически через DHCP?

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

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

```
Введите IP/префикс и нажмите Enter.

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

4. Введите адрес шлюза или оставьте поле пустым:

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

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

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

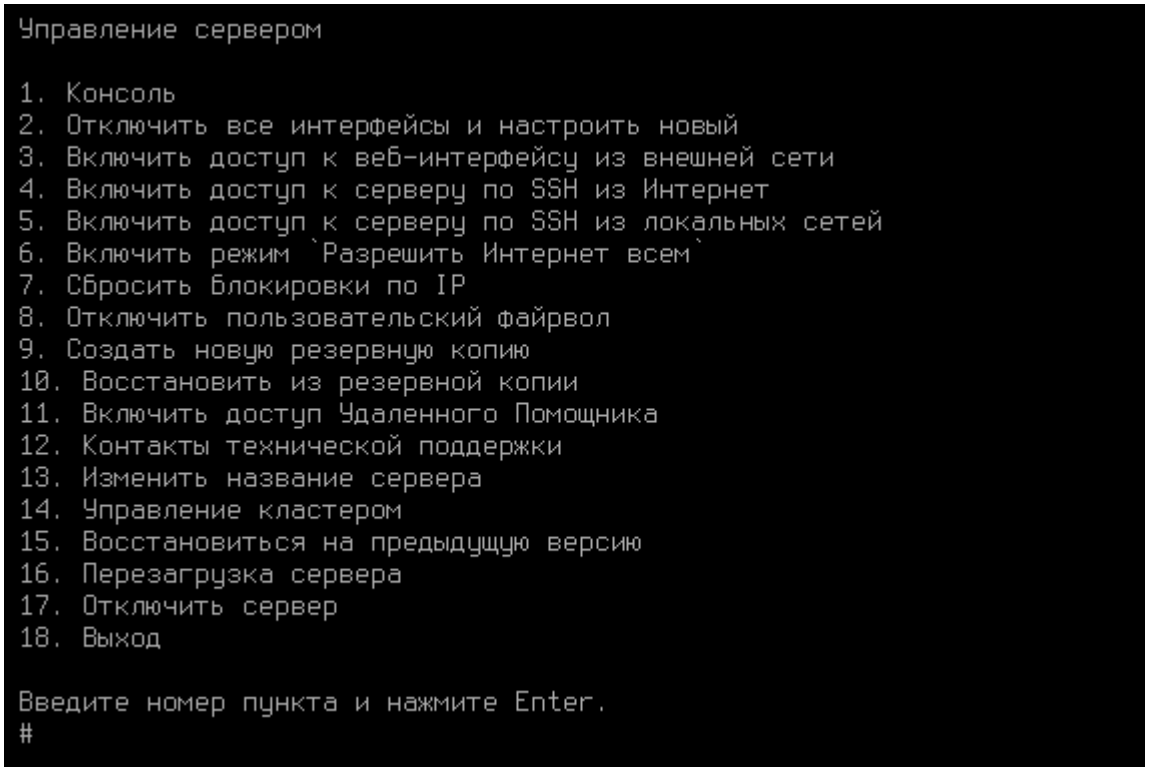
- При настройке **Ideco NGFW в качестве прокси** введите шлюз с доступом в интернет:

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

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

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

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

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

После создания локального интерфейса откроется локальное меню управления сервером:



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

9. Первоначальная настройка

Подсказка: Поддерживаются современные версии браузеров Firefox, Chrome и браузеров, основанных на Chromium, для администрирования сервера через веб-интерфейс.

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.

9.1 Подключение к веб-интерфейсу Ideco NGFW

1. Запустите на любом компьютере в локальной сети поддерживаемый интернет-браузер.
2. Введите в адресной строке IP-адрес, указанный при настройке локального интерфейса, и порт 8443.
   Пример: `192.168.100.2:8443`
3. Браузер выдаст предупреждение о том, что сертификат безопасности не был выпущен доверенным центром сертификации. Продолжите соединение, нажав на соответствующую кнопку в нижней части окна:

Появится предупреждение о незащищенном подключении. Перейдите по ссылке - откроется форма авторизации.

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

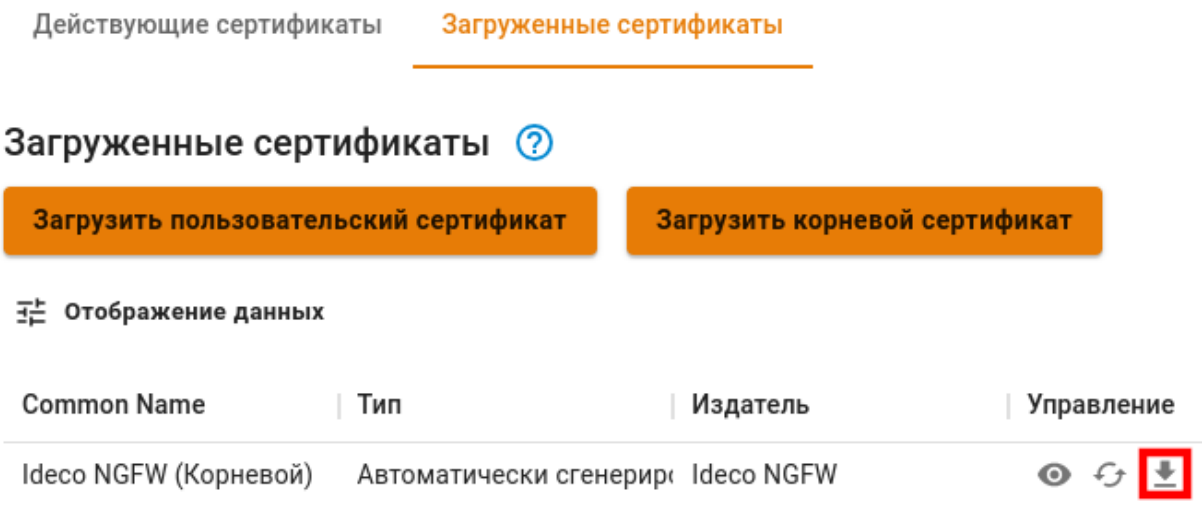
9.2 Импорт корневого сертификата NGFW в браузер

Для устранения предупреждения в браузере при входе в веб-интерфейс нужно импортировать корневой сертификат NGFW или добавить сертификат в **доверенные корневые центры сертификации** устройства.

**

Из раздела **Сервисы**:**

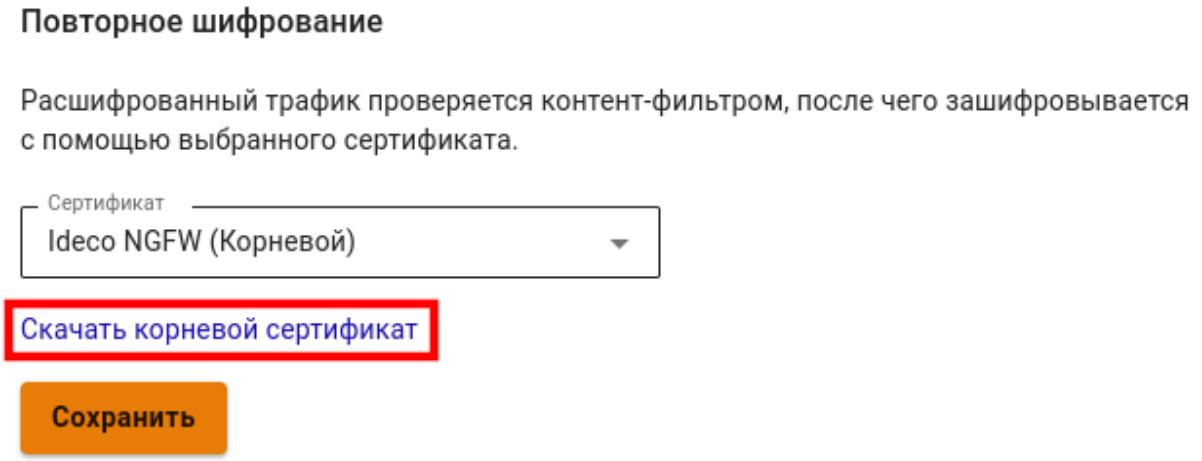
В разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** нажмите на стрелку для скачивания:



**

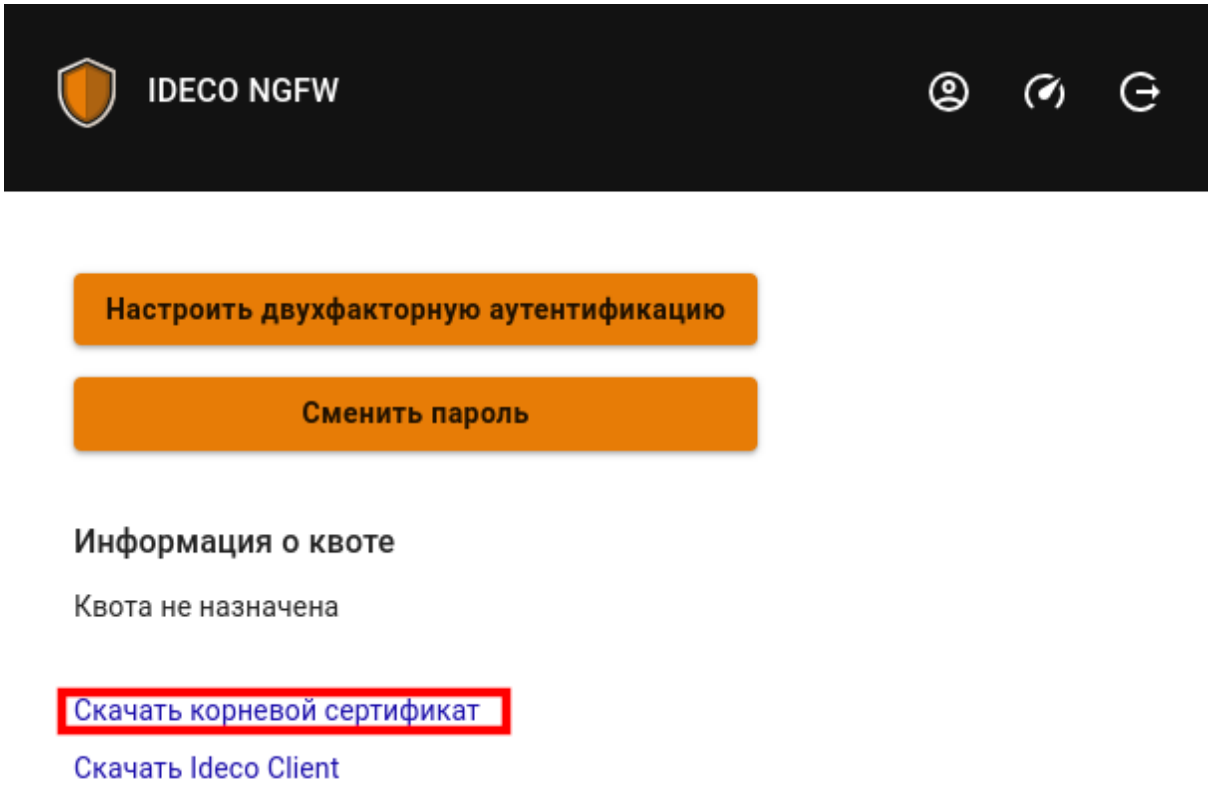
Из раздела **Правила трафика**:**

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



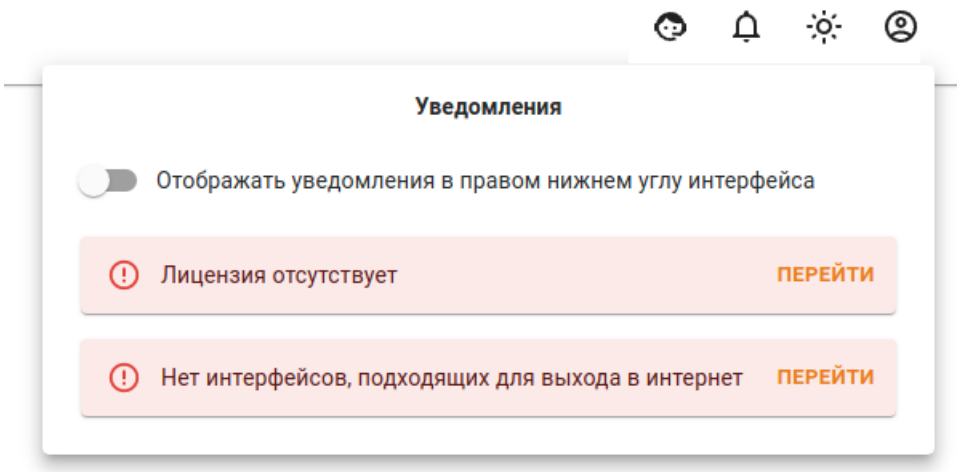
Из личного кабинета пользователя:

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



После первого входа в веб-интерфейс появится несколько уведомлений, которые подскажут, что для корректной работы Ideco NGFW необходимо настроить подключение к провайдеру и зарегистрировать сервер.

После первого входа в веб-интерфейс появится несколько уведомлений, которые подскажут, что для корректной работы Ideco NGFW необходимо настроить подключение к провайдеру и зарегистрировать сервер:



9.3 Настройка Ethernet-подключения

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

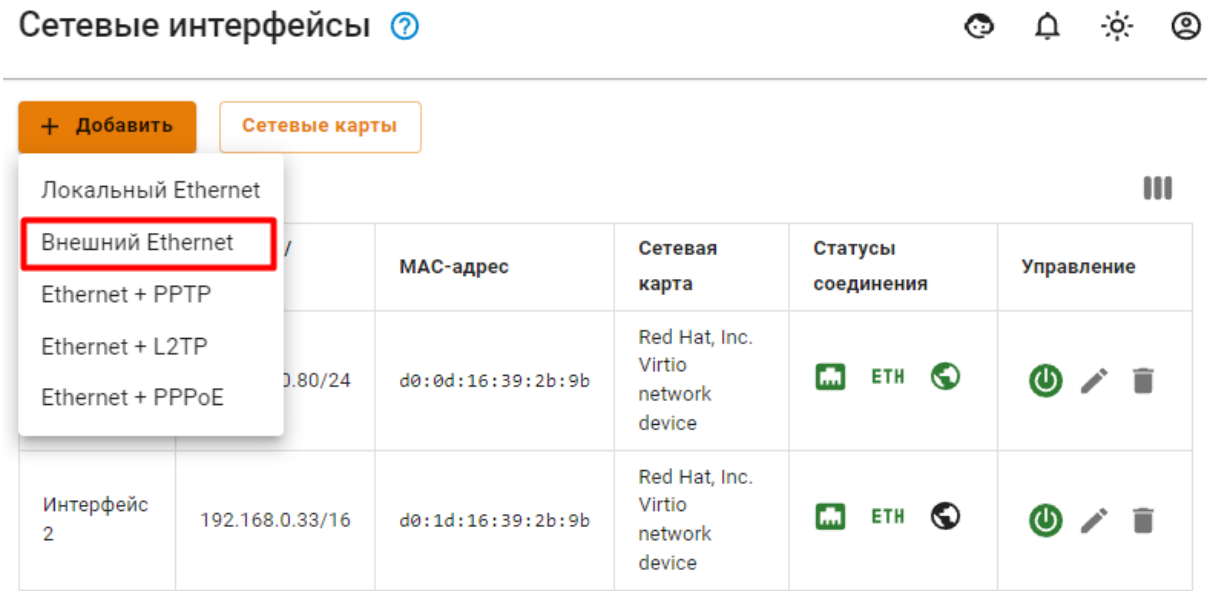
Параметр	Примечание
Сетевая карта	Необходимо указать сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру. Для идентификации адаптера ориентируйтесь на наименование производителя или MAC-адрес
IP-адрес и маска	Сетевые реквизиты, которые были назначены провайдером. Укажите 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

Подсказка: Если провайдер поддерживает автоматическое конфигурирование внешнего сетевого интерфейса с помощью протокола DHCP, то отметьте пункт **Автоматическая конфигурация через DHCP**.

Для настройки Ethernet-подключения выполните следующие шаги:

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

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



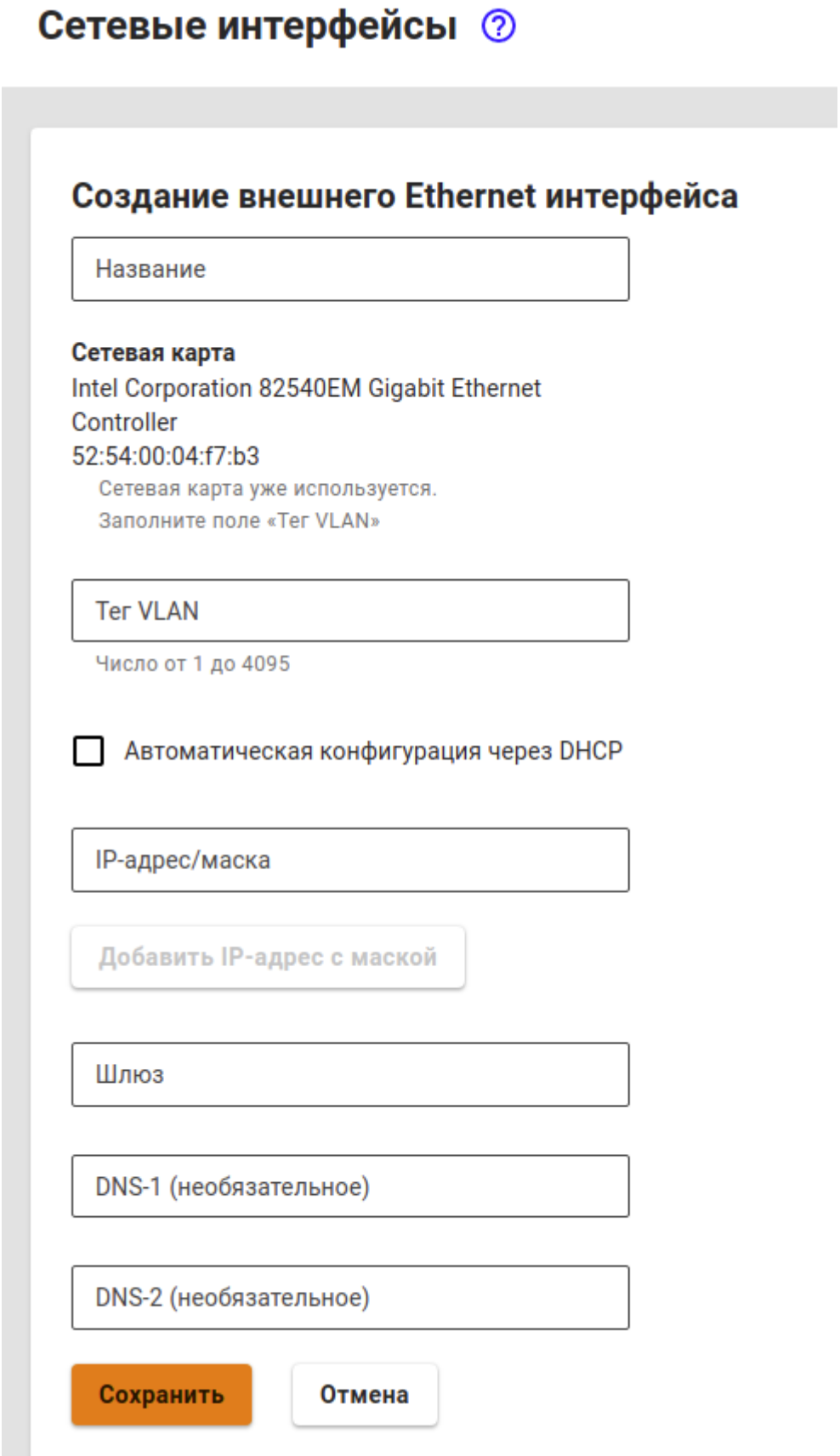
Внимание: Будьте внимательны!

При выборе пункта **Локальный Ethernet** и настройке его как **Внешний Ethernet доступ в интернет будет отсутствовать.**

1. Выберите подходящую сетевую карту.
2. Заполните следующие поля, они являются обязательными:

- Название;

- IP-адрес/маска;
- Шлюз (или установите флаг в строке *Автоматическая конфигурация через DHCP*);



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.

5. Проверьте правильность введенных данных и нажмите кнопку **Сохранить**.

9.3.1 Настройка других типов подключений

Если провайдер использует другой тип подключения, ознакомиться с остальными инструкциями по настройке можно по следующим 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*.

10. Регистрация сервера

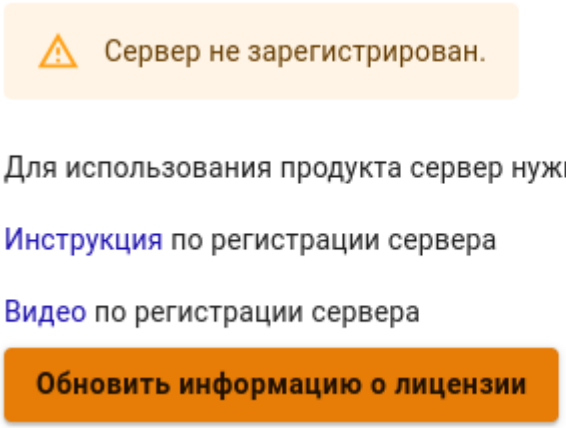
Подсказка: Для активации лицензии необходима обязательная регистрация сервера в личном кабинете.

10.1 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** и нажмите **Зарегистрировать**:



2. В открывшемся окне перейдите по ссылке **Зарегистрировать новый сервер**, 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.

10.2 Офлайн-регистрация

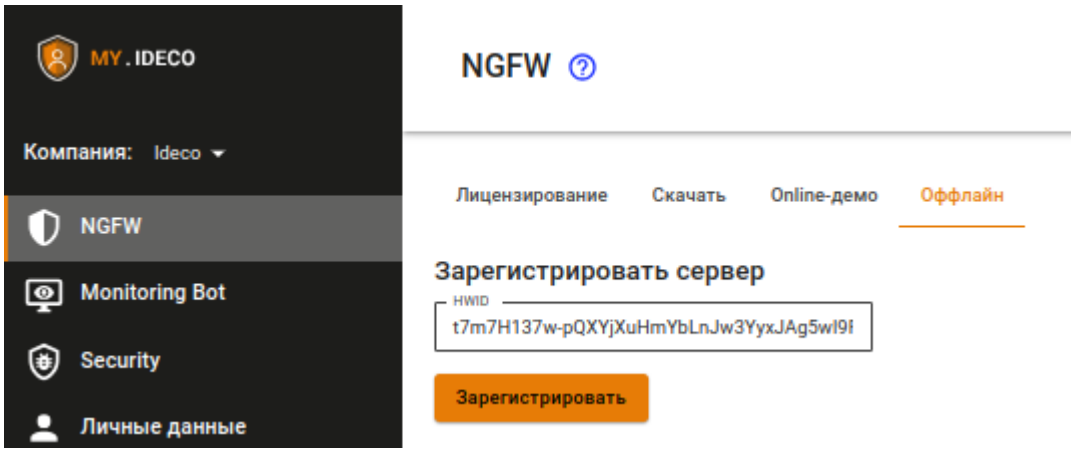
Шаги офлайн-регистрации сервера и привязки лицензии:

1. Привяжите сервер к личному кабинету в MY.IDECO:

   - Перейдите в веб-интерфейс Ideco NGFW в раздел **Управление сервером -> Терминал**;
   - Выполните команду `cat /usr/share/ideco/license-backend/hwid`;
   - Скопируйте hwid сервера. Пример: `t7m7H137w-pQXYjXuHmYbLnJw3YyxJAg5wl9FfARlh`;

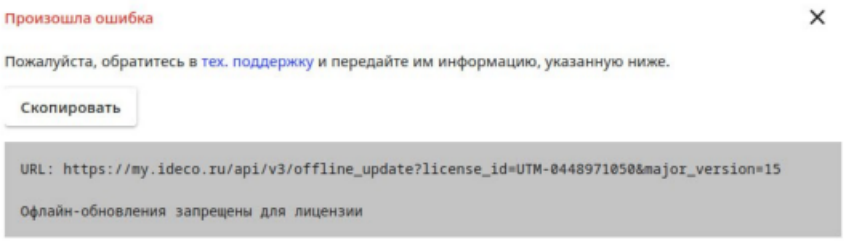
2. Обратитесь к вашему менеджеру для предоставления лицензии.

3. Перейдите в личный кабинет MY.IDECO в раздел **NGFW -> Офлайн** и заполните поле **HWID** скопированными на шаге 1 данными:

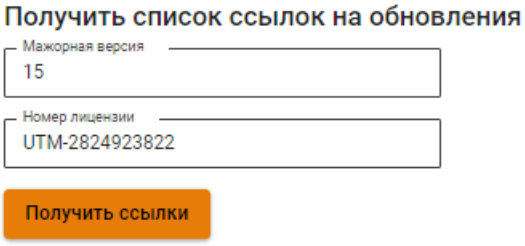


4. Перейдите в раздел **NGFW -> Лицензирование** и нажмите **Привязать лицензию** рядом с нужным сервером. Пример наименования сервера для офлайн-регистрации: `UTM (UTM Unknown)`.

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



5. Перейдите в раздел **NGFW -> Офлайн** и введите в соответствующие поля цифрами мажорный номер версии и номер лицензии:



6. Нажмите **Получить ссылки** и сохраните файлы конфигураций, нажав на появившиеся ссылки:

   - `license.json` - информация о лицензии;

- `geoip-<timestamp>.mmdb` - база для работы модуля **Предотвращение вторжений**;
- `iplist-<timestamp>.tar.gz` - база соответствия подсетей и стран, в которые они входят;
- `simple.tgz` - правила фильтрации для модуля **Предотвращение вторжений**;
- `sky-from-0-to-<timestamp>.sst` - база для работы модуля **Контент-фильтр**.

7. Добавьте конфигурационный файл с информацией о лицензии в Ideco NGFW:

- Перейдите в раздел **Управление сервером -> Терминал**;
- Загрузите полученный файл `license.json` на сервер Ideco NGFW в директорию `/var/cache/ideco/license-backend/`;
- Перезапустите сервис лицензий командой `systemctl restart ideco-license-backend.service`;
- Перейдите в раздел **Управление сервером - Лицензия** и убедитесь, что лицензия установлена.

10.3 Офлайн-обновление баз модулей безопасности

Для обновления баз модулей безопасности при офлайн-регистрации сервера выполните действия:

1. Сохраните скрипты запуска обновления баз модулей безопасности в папку с файлами, скачанными на шаге 6:

2. Обновите базы модулей безопасности:

- Перейдите в директорию `scp -r <путь до папки со скачанными файлами> administrator@<IP-адрес NGFW>:~/`;
- Подключитесь к серверу по SSH `ssh administrator@<IP-адрес NGFW>`;
- Перед обновлением модулей перейдите в директорию `cd ~/<название папки со скачанными файлами>`;
- Обновите базы модулей безопасности, выполнив команды:
  - Базы модуля **Предотвращения вторжений** - `python3 geoip.py <geoip-<timestamp>.mmdb>`;
  - Базы соответствия подсетей и стран - `python3 iplist.py <iplist-<timestamp>.tar.gz>`;
  - Правила фильтрации модуля **Предотвращение вторжений** - `python3 suricata.py simple.tgz`;
  - Базы модуля **Контент-фильтр** - `python3 content_filter.py <sky-from-0-to-<timestamp>.sst>`.

11. Получение доступа в интернет

11.1 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.

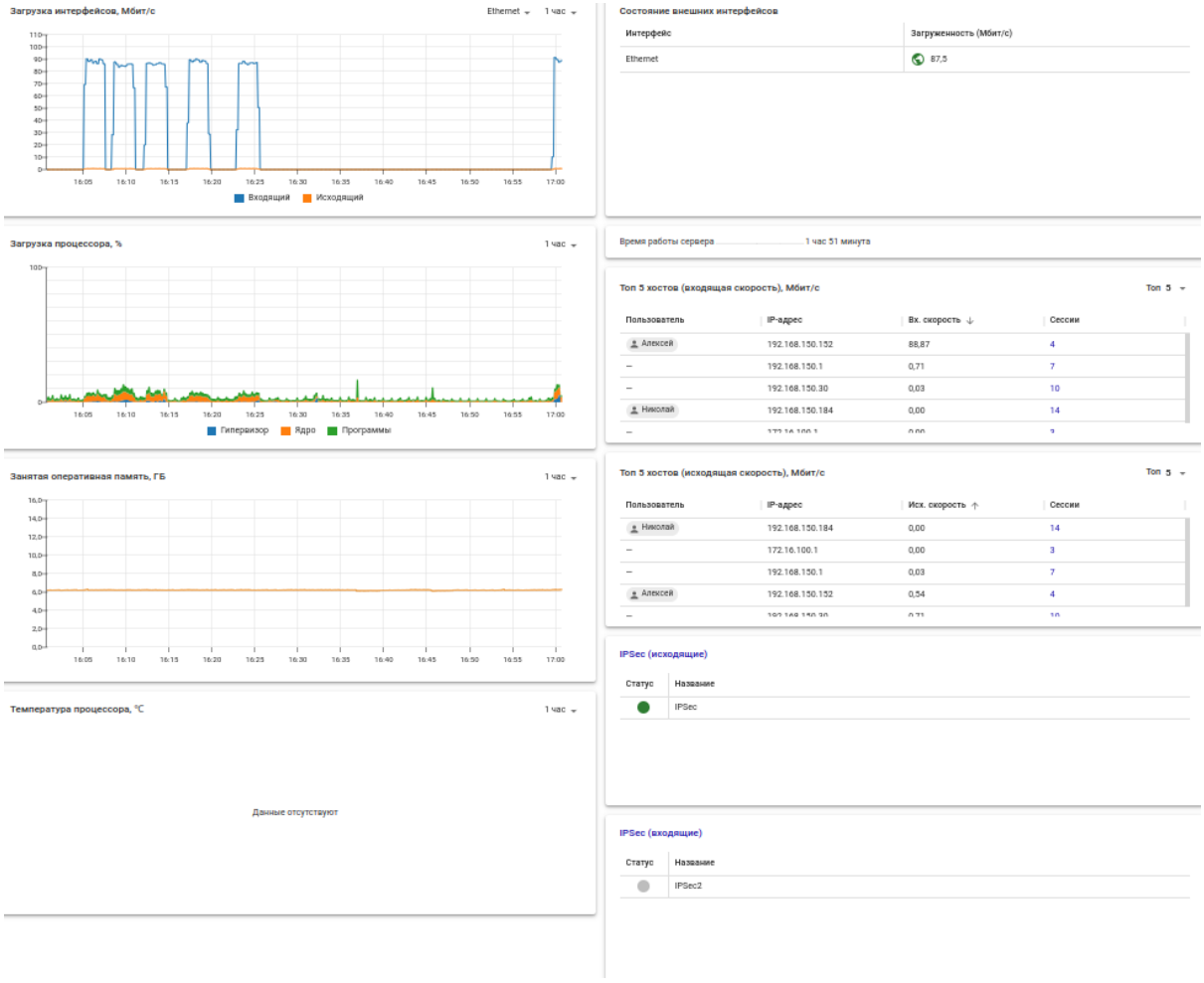
- ***Авторизация по подсетям*** - способ автоматической авторизации большого количества устройств из требуемой подсети без привязки к MAC и/или конкретному IP.

12. Панель мониторинга

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

- 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:



12.1 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.

13. Пользователи

13.1 Учетные записи

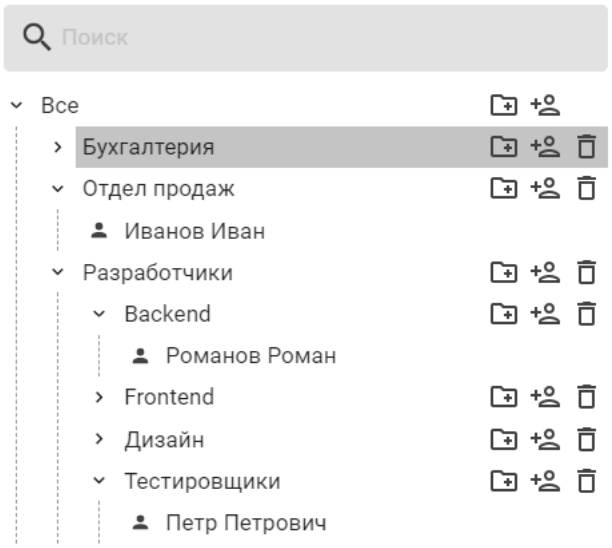
13.1.1 Основное

Пользователи в веб-интерфейсе Ideco NGFW отображаются в виде дерева и могут быть организованы в группы. Уровень вложенности групп не ограничен. Дерево учетных записей пользователей доступно в разделе **Пользователи -> Учетные записи**.

В Ideco NGFW реализован принцип наследования, что позволяет легко задавать и изменять общие для пользователей параметры, определяя их для родительской группы. Принцип наследования очень удобен

для выполнения операций управления, осуществляемых по отношению ко всем пользователям группы.

Пример дерева пользователей представлен ниже:



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

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 распросстраняться на всех пользователей NGFW.

13.1.2 Управление пользователями

Общее

В дереве пользователей есть соответствующие кнопки, чтобы управлять группами и учетными записями:

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

Создание учетной записи пользователя

Создать учетную запись пользователя можно в определенной группе или вне групп:

- **В определенной группе** - выберите группу, нажмите кнопку **Создать пользователя** во вкладке **Основное** или  рядом с названием группы в дереве: Логин необходимо вводить латинскими символами в нижнем регистре, например, i.ivanov.

При заполнении **Дополнительных настроек** будет создано соответствующее правило в карточке пользователя во вкладке **IP и MAC авторизация** и в разделе **Авторизация -> IP и MAC-авторизация**.
Но если этот IP- или MAC-адрес будет использоваться в правилах *DHCP-сервера*, то правило DHCP-сервера будет выполняться в приоритете.

Рекомендации к созданию сложности паролей (можно автоматически сгенерировать пароль):

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

Предупреждение: Не используйте Numpad при введении пароля, поскольку в будущем это может привести к проблемам при авторизации пользователя.

Подсказка: **Телефон** указывается для *Двухфакторной аутентификации*.

Кнопка **Получить MAC по IP** будет активна, если IP пользователя и IP Ideco NGFW в одной подсети.

Для учетных записей, импортированных из MS Active Directory (AD), проверка пароля осуществляется средствами AD. Настройка авторизации пользователей Active Directory производится в соответствующем *разделе*.

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.

Предупреждение: Посмотреть или восстановить пароль учетной записи пользователя нельзя, допускается только его изменение.

После определения всех параметров нажмите кнопку **Сохранить**. Создастся учетная запись, для которой автоматически будут установлены значения некоторых параметров группы (в зависимости от того, в какой группе она была создана).

Создание группы:

Для создания группы нужно нажать на соответствующий элемент управления, который находится справа от названия группы (можно создать как группу в корне дерева, так и дочернюю).

Откроется окно, в котором нужно указать название новой группы и нажать кнопку **Сохранить**:

Удаление учетной записи пользователя или группы

Для удаления учетной записи пользователя необходимо навести курсор на пользователя и нажать на соответствующий элемент управления. Также можно выбрать нужного пользователя и нажать на кнопку **Удалить** на вкладке **Основное**:

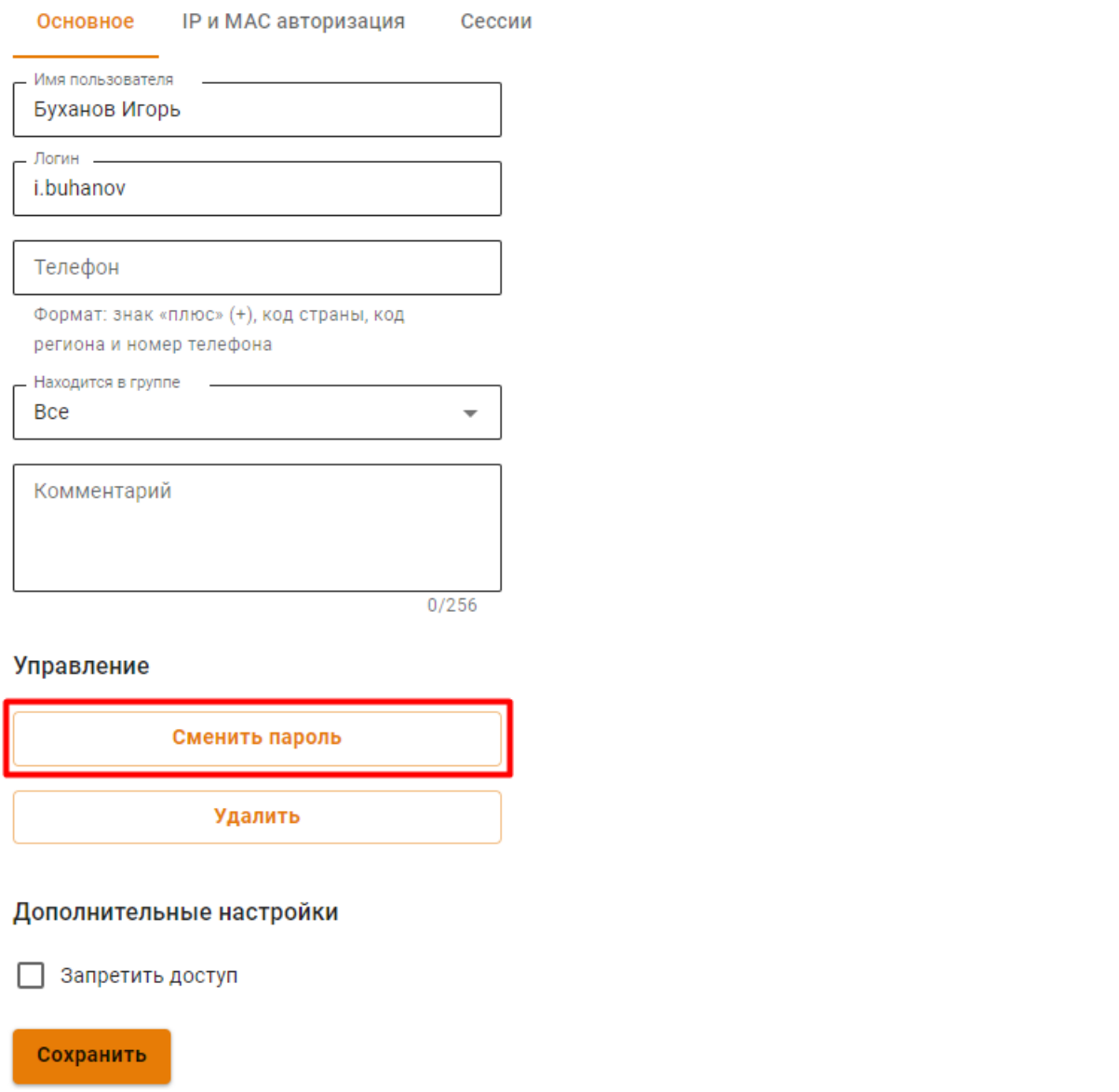
Удаление группы осуществляется аналогичным образом.

Перемещение учетной записи пользователя

Чтобы переместить учетную запись пользователя в другую группу, выделите этого пользователя и на вкладке **Основное** найдите поле **Находится в группе**. Из выпадающего списка выберите группу, в которую надо переместить пользователя, и нажмите на кнопку **Сохранить**:

Редактирование учетной записи пользователя

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



13.1.3 Настройка пользователей

Общее

Настройка пользователей осуществляется в разделе **Пользователи -> Учетные записи**.

Для редактирования параметров УЗ пользователя или групп пользователей выберите нужный объект в дереве пользователей. В правой части экрана появятся параметры выделенного объекта и будут отличаться списком категорий:

- Категории для **УЗ пользователя**:
  - Основное;
  - IP и MAC авторизация;
  - Сессии
  - Доступ по VPN
  - Квота;
- Категории для **Группы пользователей**:
  - Основное;
  - Active Directory/Samba DC;
  - ALD Pro
  - Квота.

Группы пользователей

Основное

В категории представлена возможность:

- **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 УЗ пользователей группы и привязки по IP- и MAC-адресам;
- **Запретить доступ**. При активации опции всем пользователям группы будет запрещен доступ в интернет;

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*.

Квота

Категория позволяет распространить квоту на всех пользователей этой группы, у которых в персональной квоте включена опция **Наследовать квоту от группы**.
Для каждой группы пользователей есть аналогичная опция. Группы наследуют квоту, установленную в вышестоящей группе.

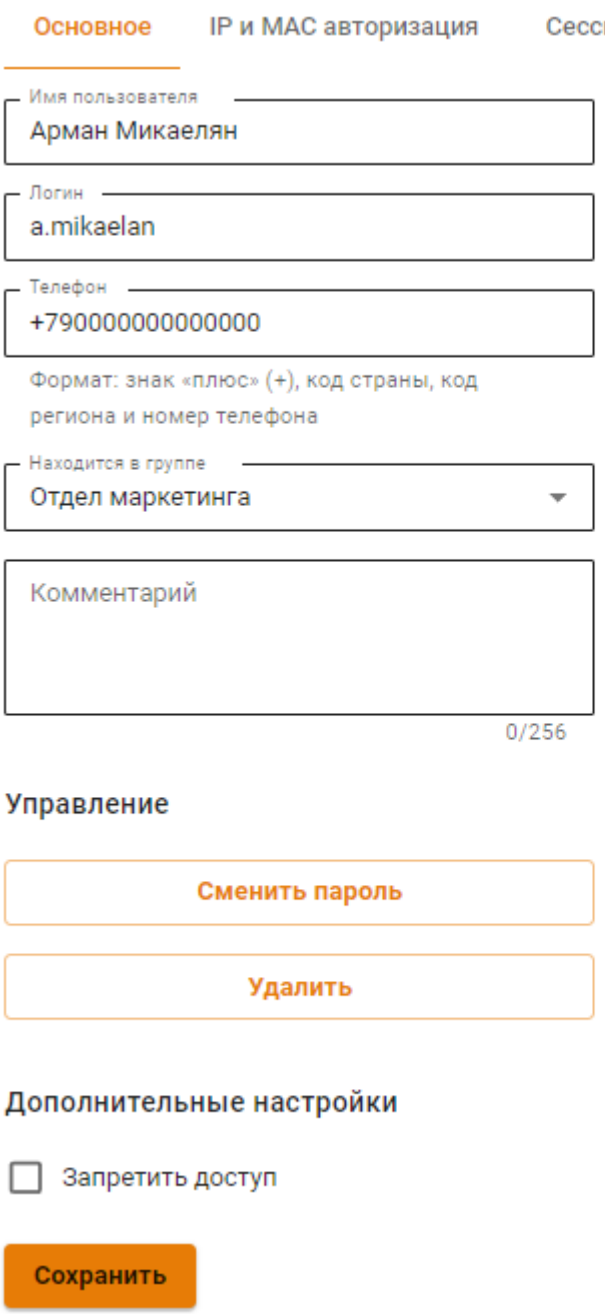
Подсказка: Настройка квот трафика описана в разделе *Квоты*.

УЗ пользователей

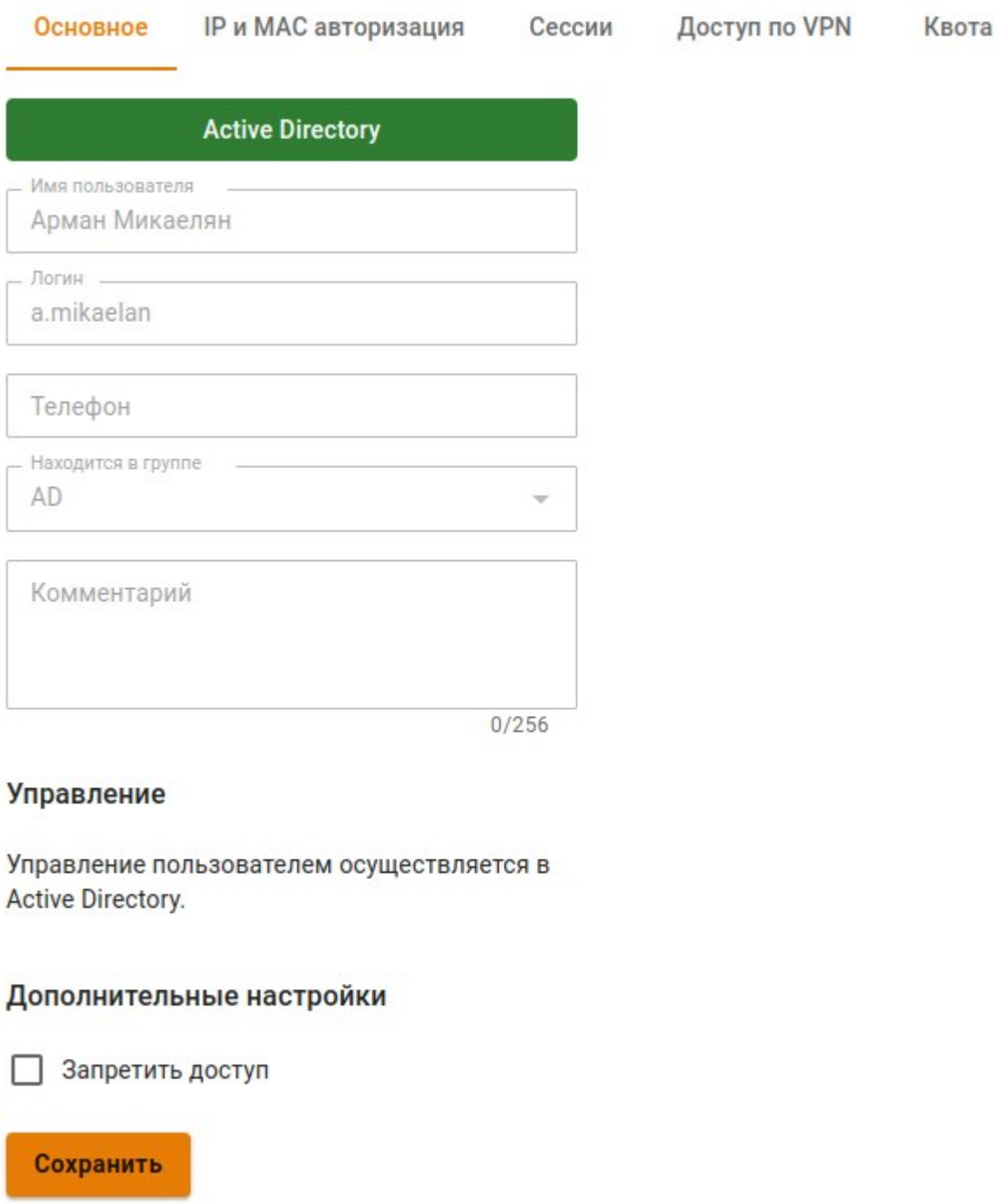
Основное

Раздел основных настроек включает множество параметров, определяющих статус учетной записи 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. Максимальное количество символов - 32;
- **Телефон** - телефон для *двухфакторной аутентификации*. Формат: знак «плюс» (+), 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 сети интернет, почтой и личным кабинетом;



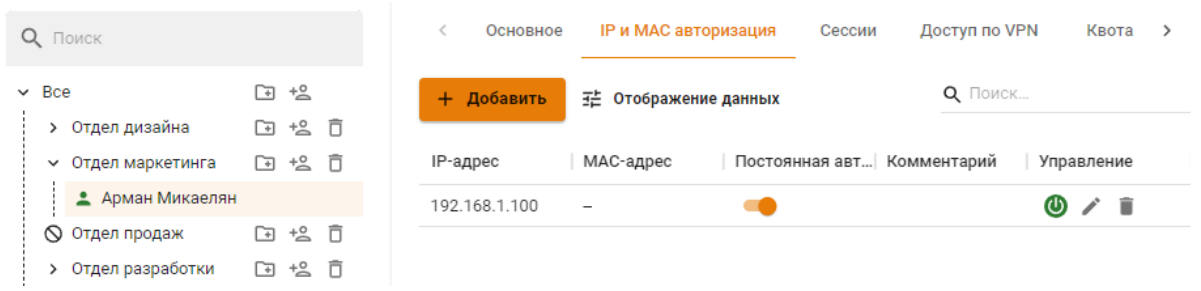
Для пользователей, экспортированных из *Active Directory* и *ALD Pro*, во вкладке **Основное** нельзя редактировать имя, логин, телефон, перемещать в другую группу и менять пароль. Пример импортированного из AD пользователя представлен на скриншоте:



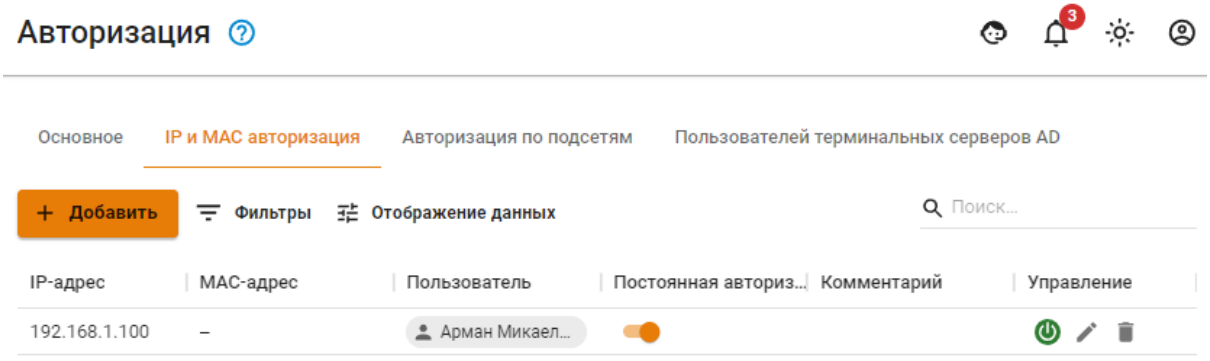
IP и MAC авторизация

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

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



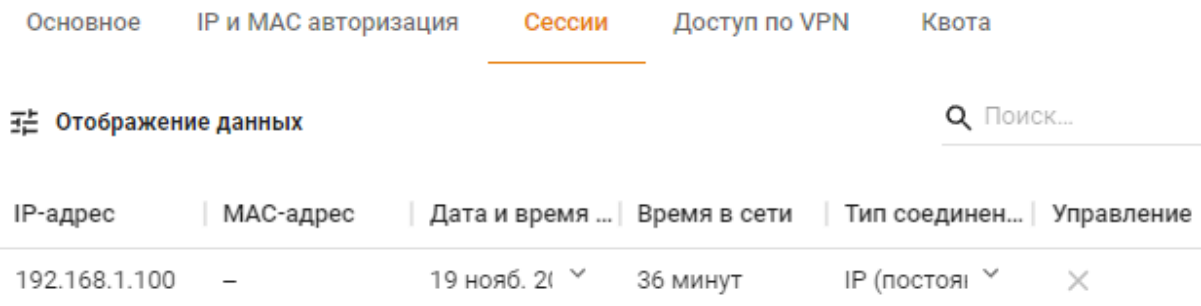
- Пользователи -> *Авторизации* -> *IP и MAC авторизация*:



Подсказка: Правила **IP и MAC авторизации** также 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.

Сессии

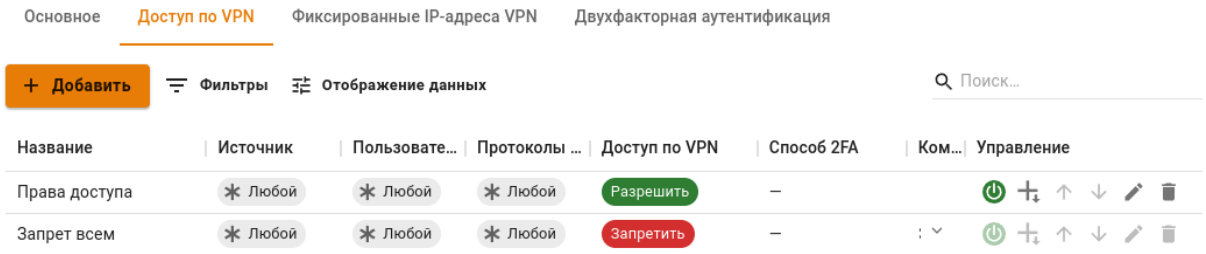
Содержит таблицу с информацией обо всех активных сессиях пользователях:



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

Доступ по VPN

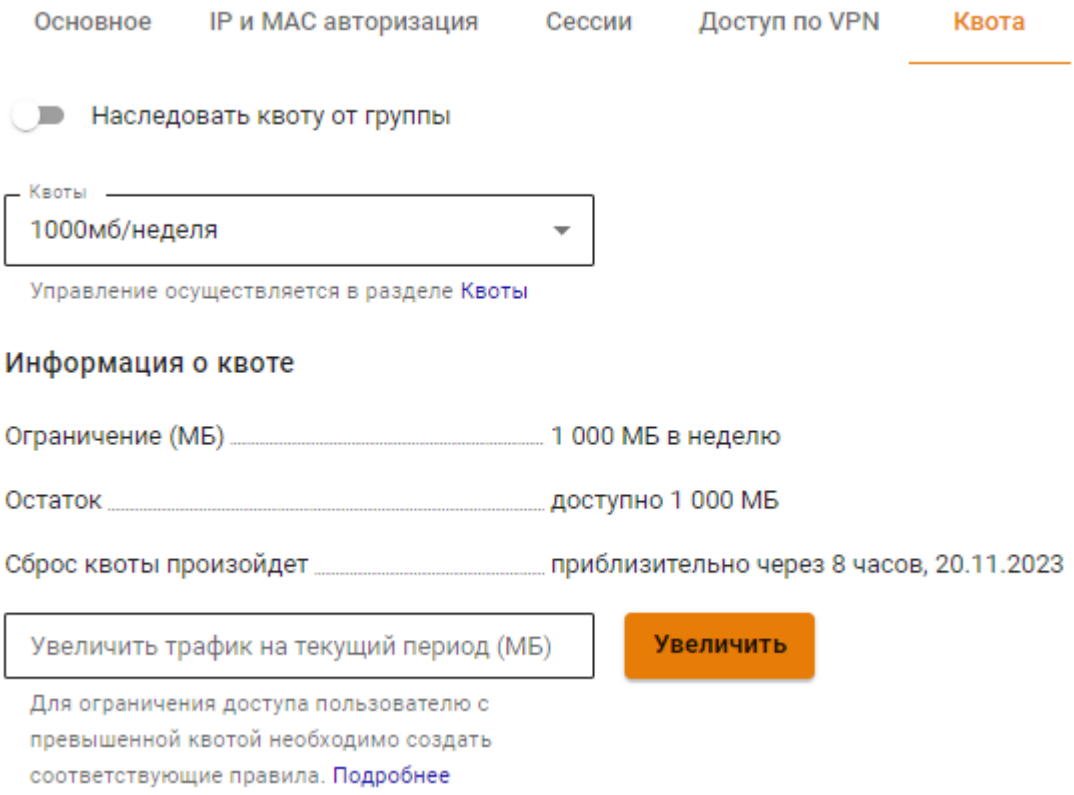
Категория позволяет просматривать правила доступа VPN, которые настраиваются в разделе **VPN-подключения -> Доступ по VPN**.



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

Квота

Категория позволяет просматривать и увеличивать квоту пользователя в случае использования лимитов трафика:



Для увеличения квоты воспользуйтесь полем **Увеличить трафик на текущий период**.

Пример использования квоты:

Пользователю назначена квота на 1000 МБ на неделю (с понедельника по воскресенье). К четвергу количество трафика превысило значение, заданное квотой. Требуется единоразово предоставить пользователю дополнительный трафик.
Для этого введите требуемое значение в поле **Увеличить трафик на текущий период** и нажмите **Увеличить**. В строке **Остаток** будет отражен весь доступный трафик с учетом добавленного.

Подсказка: Настройка квот трафика описана в разделе *Квоты*.

13.1.4 Личный кабинет пользователя

Основное

Для входа в личный кабинет пользователя перейдите на адрес NGFW и введите логин и пароль.

Возможности:

- **Настройка двухфакторной аутентификации**. Подробнее об этом способе аутентификации в статье *Двухфакторная аутентификация*.
- **Смена пароля**.
- **Скачать корневой сертификат**.
- **Скачать Ideco Client**. Подробнее о работе в Ideco Client в *статье*.
- **Тестирование скорости**. При нажатии на кнопку  в правом верхнем углу откроется меню тестирования скорости между хостом и NGFW.

13.2 Авторизация пользователей

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

13.2.1 Общая информация

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

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 Agent, 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  , сигнализирующей, 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 (пример: телеметрия Windows). Из-за этого таймаут для пользователя будет постоянно сбрасываться и не сможет отрабатывать.

Измените время автоматической разавторизации с помощью настройки **Тайм-аут отключения**, перейдя в раздел **Пользователи -> Авторизация**:

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

Подсказка: 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*, и *инструкцией по запуску PowerShell скриптов*.

13.2.2 Веб-аутентификация

Основное

Подсказка: Поддерживаемые браузеры:

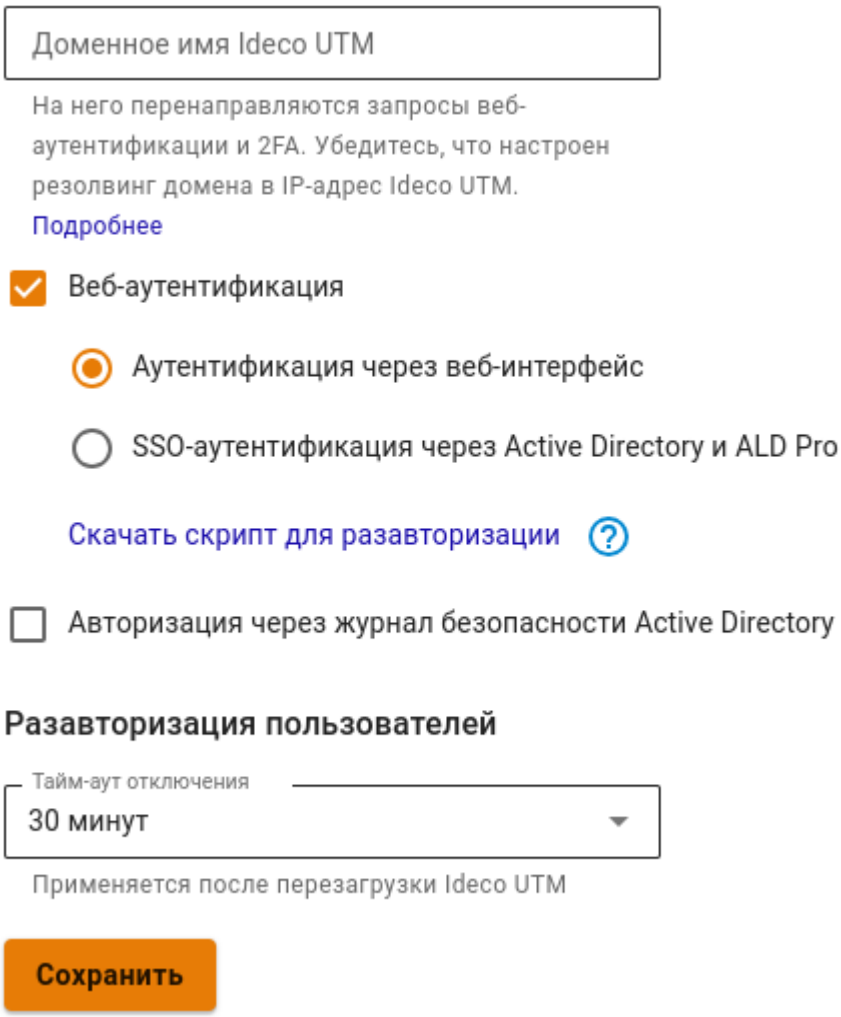
- Google Chrome, версия >= 90;
- Firefox, версия >= 78;
- Safari, версия >= 14.

Этот тип авторизации предполагает, что запрос неавторизованного пользователя, отправленный через веб-браузер, будет переадресован на страницу авторизации Ideco NGFW. После успешной авторизации произойдет переход по указанному запросу.

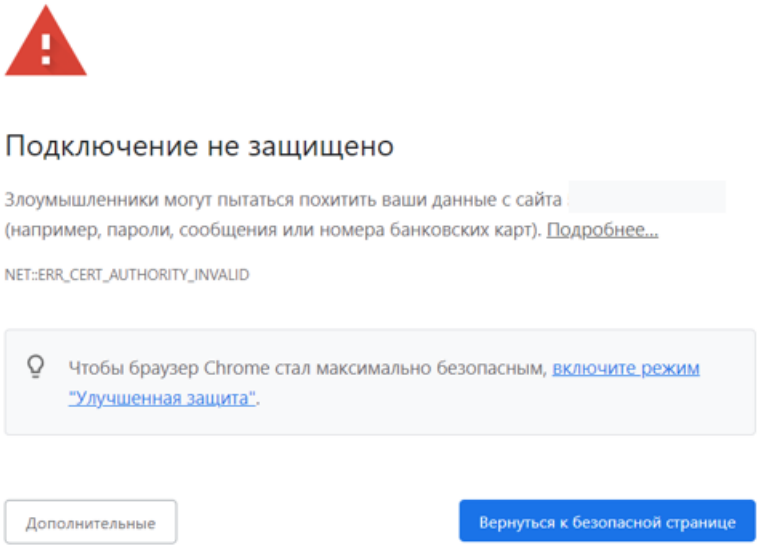
Для этого типа авторизации у пользователя на сетевой карте в качестве шлюза (объединенных в цепочку нескольких шлюзов) или при прямых подключениях к прокси по умолчанию должен быть указан IP-адрес локального сетевого интерфейса Ideco NGFW. Также до подключения к интернету должен работать **DNS-резолвинг 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.

Чтобы настроить авторизацию через веб-интерфейс, в разделе **Пользователи -> Авторизация** выберите пункты **Веб-аутентификация -> Аутентификация через веб-интерфейс**:



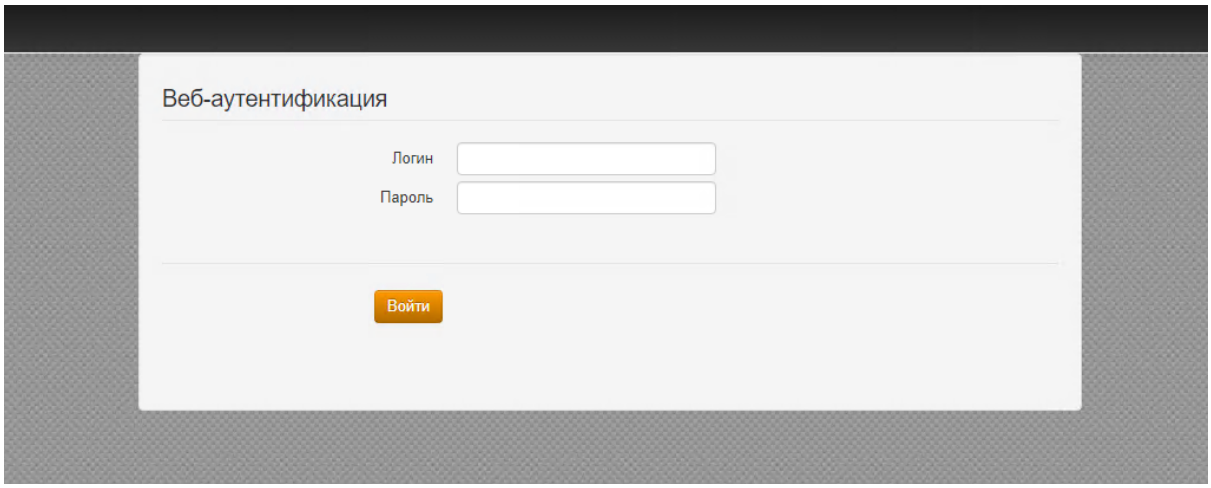
После заполнения поля **Имя домена** и сохранения настроек будет выдан Let's Encrypt сертификат, пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



Подсказка: Если NGFW не подключен к интернету или доменное имя не соответствует внешнему IP-адресу NGFW, то 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.

Далее попробуйте выйти в интернет через веб-браузер. Должно появиться окно авторизации, где необходимо ввести логин и пароль от учетной записи пользователя, созданного на Ideco NGFW. Окно авторизации представлено на скриншоте ниже:



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

Подсказка: 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).

Подсказка: Рекомендуется указывать в качестве DNS-сервера на компьютерах и устройствах локальной сети IP-адрес локального интерфейса Ideco NGFW.

Подробнее об авторизации пользователей **Active Directory** в статье *Аутентификация пользователей AD/Samba DC*.

Подробнее об авторизации пользователей **ALD Pro** в статье *ALD Pro*.

13.2.3 IP и MAC авторизация

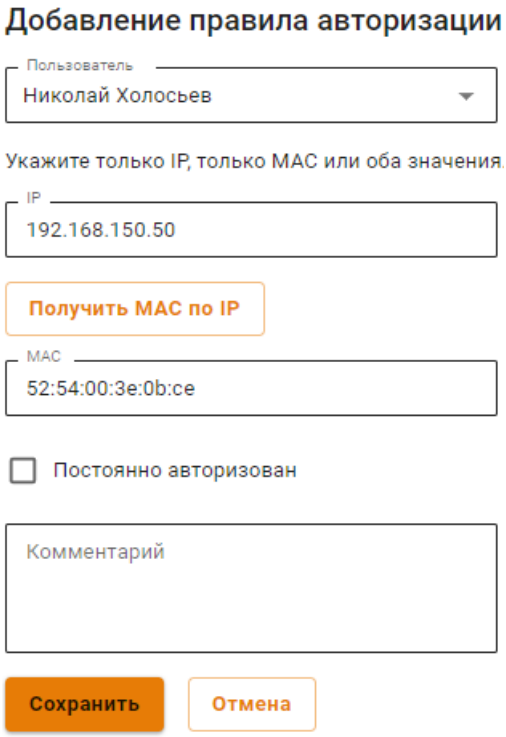
Общая информация

Подсказка: Правила **IP и MAC авторизации** также 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.

Для настройки IP и MAC авторизации, необходимо:

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

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



Подсказка: Установите флаг **Постоянно авторизован**, чтобы обеспечить непрерывный доступ в интернет, даже если пользователь не активен.

Созданные в этом разделе правила отражаются в *карточке пользователя*.

Подробнее об авторизации пользователей только по IP- или MAC-адресу - в статьях *Авторизация по IP-адресу* и *Авторизация по MAC-адресу*.

Авторизация по IP-адресу

При авторизации по IP пользователь получит доступ до интернет-ресурсов после инициации подключения. Без ввода логина и пароля.

Также можно авторизовать сетевые устройства (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 и в нем включен SNAT, то 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 связке IP-адрес - MAC-адрес, так как маршрутизатор не обрабатывает трафик уровня L2.

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

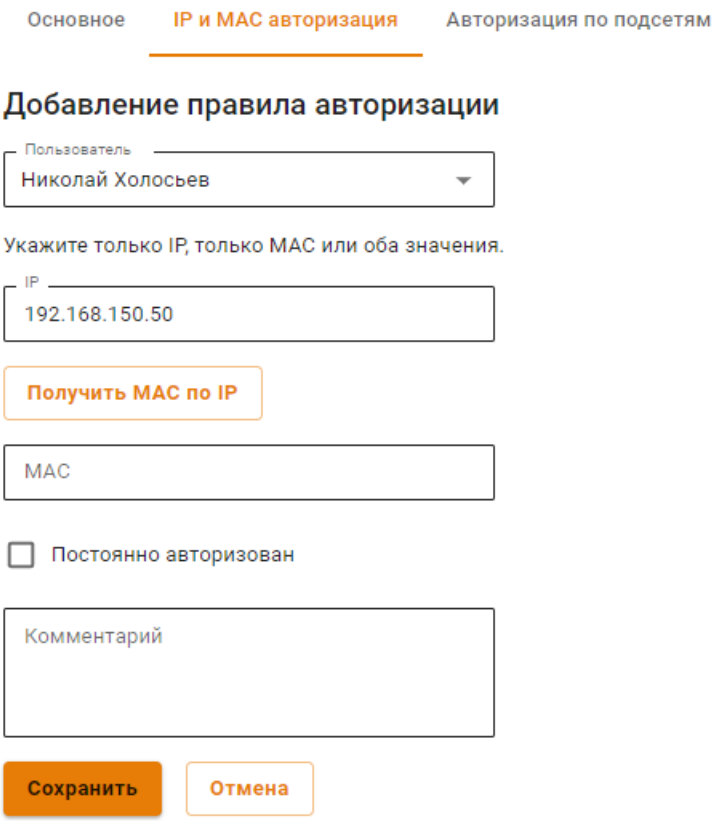
Настройка авторизации по IP

Чтобы авторизовать пользователя по IP-адресу:

1. *Создайте* пользователя в Ideco NGFW или *импортируйте* его из Active Directory, который будет авторизован по IP.

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**:



Подсказка: IP-адрес на компьютере/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.

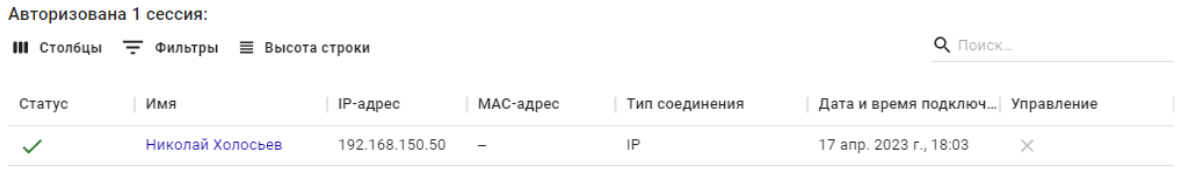
Для пользователя, которым является сетевое оборудование, рекомендуем настроить **Постоянную авторизацию**. Это позволит NGFW создать сессию, а сетевому оборудованию не потребуется делать запрос в интернет.
Так же рекомендуем настроить статический IP-адрес или DHCP с привязкой по IP-адресу. Это требуется, например, для ресурсов, *опубликованных через DNAT*.

Подсказка: Воспользуйтесь поиском устройств для автоматического создания пользователей при попытке выхода в интернет. Подробнее о настройке читайте в статье *Обнаружение устройств*.

Предупреждение: Если используется авторизация по IP со статической привязкой в DHCP, то рекомендуем перенести такие правила на *авторизацию по MAC-адресу*.

Просмотр сессии

После того как пользователь делает запрос в интернет, на NGFW будет автоматически создана сессия с типом авторизации `IP` в разделе **Мониторинг -> Авторизованные пользователи**:



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

Под одним пользователем можно авторизовать только одно устройство по IP-адресу. Но одновременно с данным типом авторизации под одним пользователем можно авторизовать еще четыре устройства любым другим методом авторизации.

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.

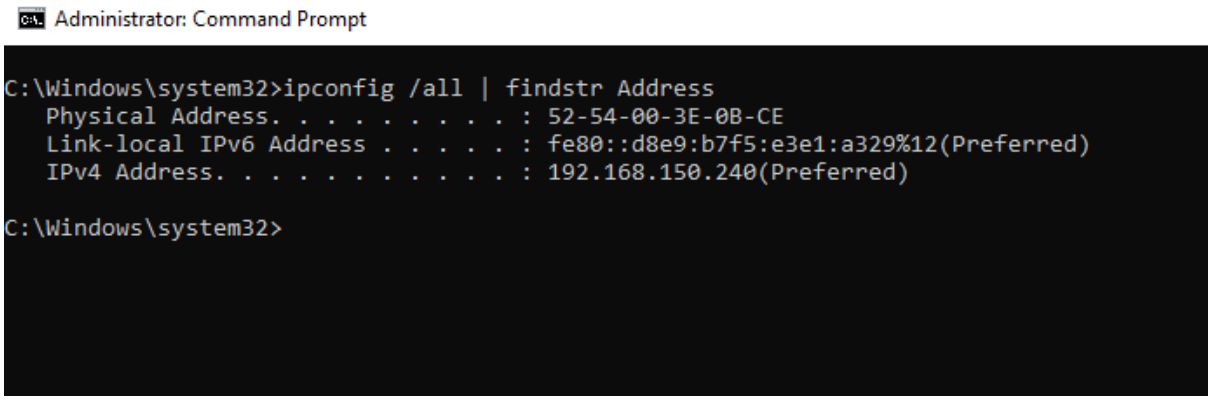
Предупреждение: Чтобы устройство могло авторизоваться на NGFW по MAC-адресу, они оба должны находиться в одном широковещательном домене и NGFW должен выступать шлюзом для устройств.

Подсказка: Пользователи, находящиеся за роутером в локальной сети NGFW, не могут авторизоваться 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.

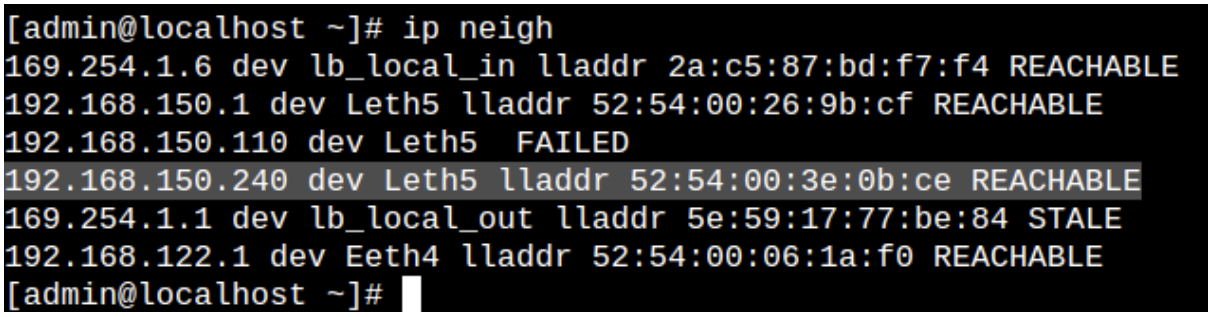
Настройка авторизации по MAC

Чтобы авторизовать пользователя по MAC-адресу, необходимо выполнить следующие действия:

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



2. Удостоверьтесь что компьютер и NGFW находятся в одном широковещательном домене.
Для этого на NGFW в разделе **Управление сервером -> Терминал** введите команду: `ip neigh`

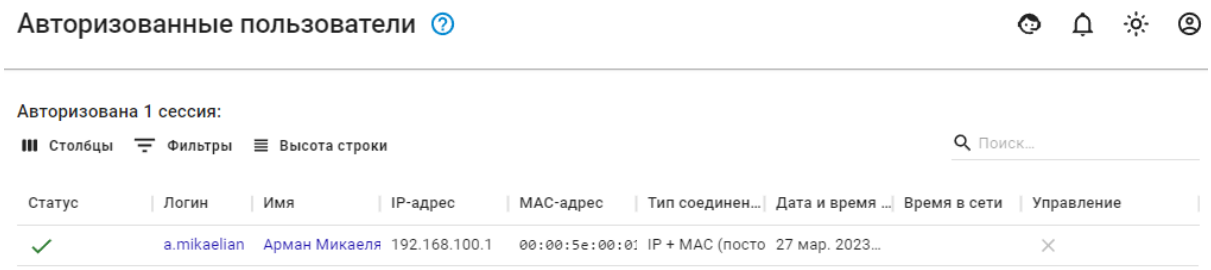


Подсказка: Эта команда выводит ARP-таблицу NGFW. Наличие записи с MAC-адресом устройства и статусом REACHEBLE говорит об имеющейся L2-доступности между NGFW и устройством.

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

Предупреждение: Для MAC-авторизации невозможно настроить постоянную авторизацию.
Это технически невозможно, т. к. для создания авторизованной сессии необходим
IP-адрес. Поэтому рекомендуется использовать MAC-авторизацию в комбинации с *DHCP-сервером*.

Результат можно будет посмотреть в разделе: **Мониторинг -> Авторизованные пользователи**, там отобразится сессия с типом авторизации MAC.



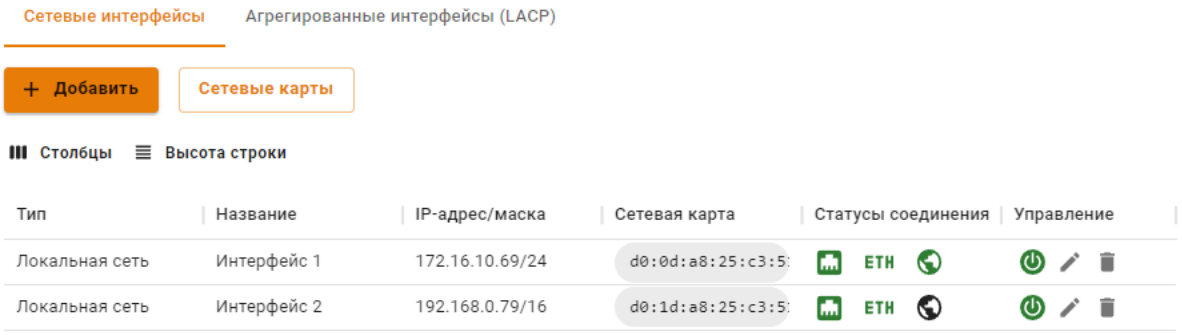
Поведение MAC-авторизации при перемещении устройства между локальными сетями

В организациях часто возникает ситуация, когда необходимо перемещаться между локальными сетями с ноутбуком на руках и при этом оставаться всегда в сети. В таких случаях авторизация по MAC-адресу прекрасно себя показывает.

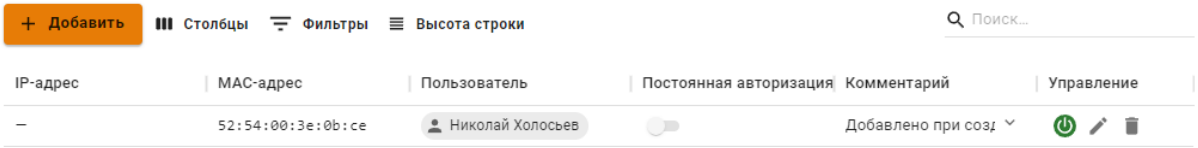
Подсказка: У Вас должен быть настроен собственный DHCP-сервер или на Ideco NGFW.
В раздаваемых реквизитах шлюзом должен выступать локальный интерфейс
Ideco NGFW.

Возьмем за пример ситуацию, когда пользователю `Николай Холосьев` понадобилось переместиться с ноутбуком между локальными сетями:

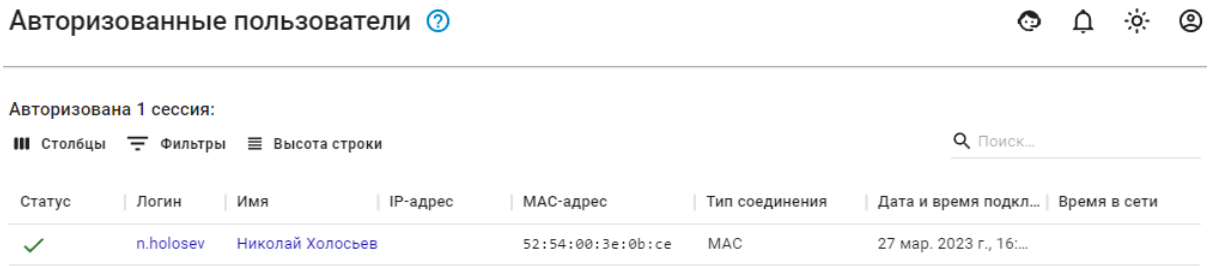
- На NGFW имеются настроенные следующим образом локальные интерфейсы:



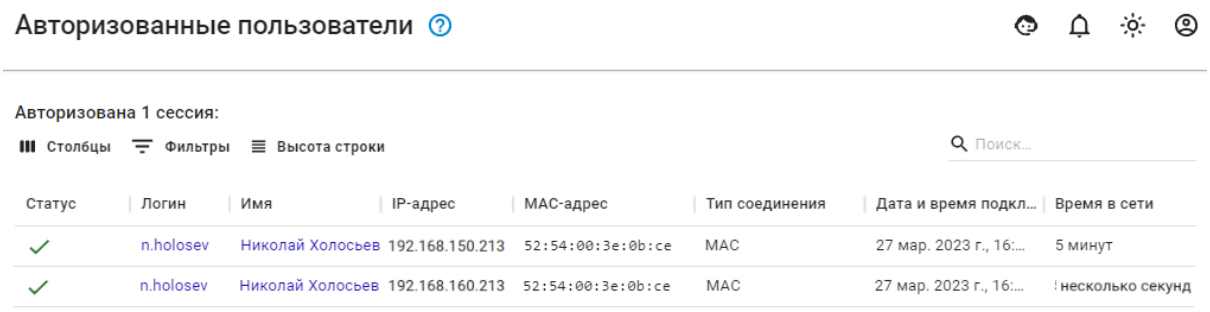
- У пользователя настроено правило авторизации по MAC-адресу:



- Также у него есть одна активная сессия в разделе **Авторизованные пользователи**:



- Далее пользователь переходит из одной локальной сети в другую. Ему выдаются другие сетевые реквизиты от DHCP-сервера, в которых шлюзом указан NGFW, и при обнаружении любой активности со стороны пользователя у него появится вторая сессия с авторизацией по MAC-адресу:



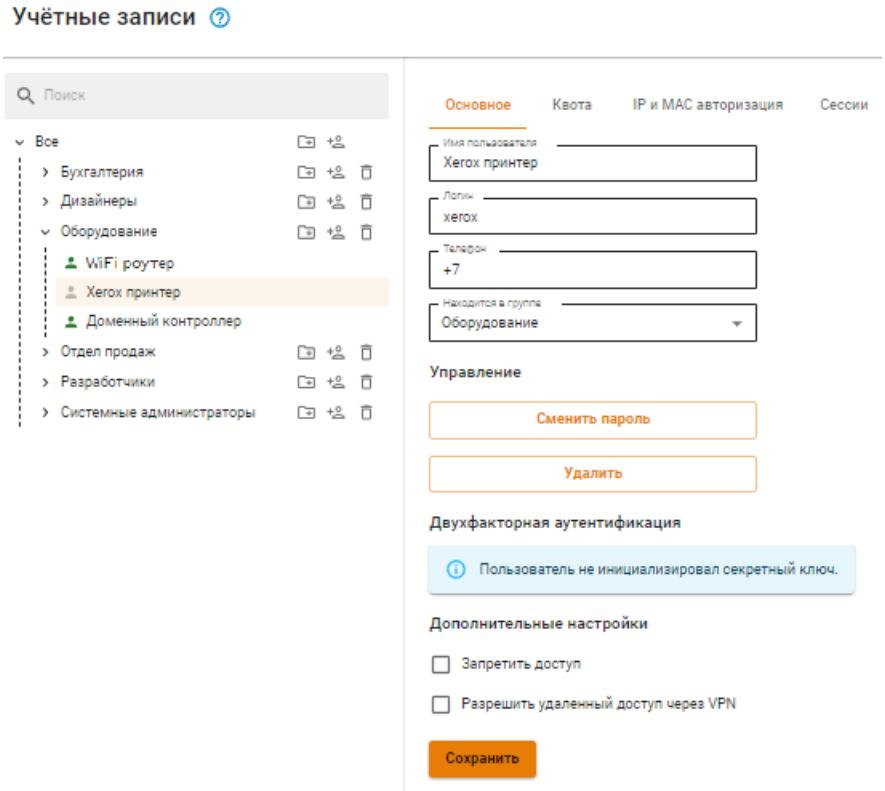
Подсказка: Если у пользователя не появляется доступ и вторая сессия с авторизацией по MAC-адресу, то у пользователя не обновились сетевые реквизиты.

Сбросьте старые сетевые реквизиты от DHCP-сервера и получите новые с помощью команды: `ipconfig /release && ipconfig /renew`.

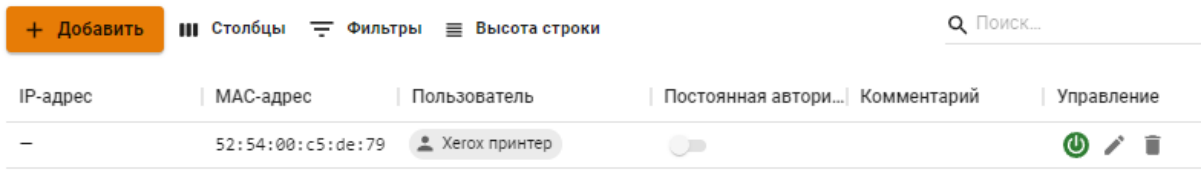
Настройка авторизации по MAC-адресу для сетевого принтера и других сетевых устройств

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

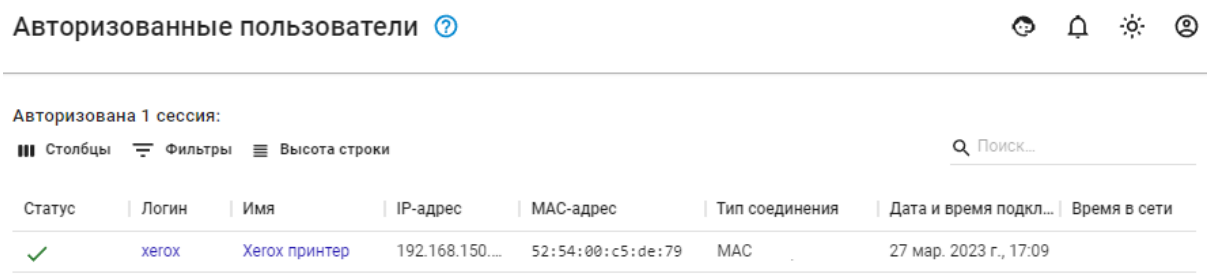
Для авторизации сетевого принтера необходимо создать пользователя для этого принтера вручную или через *Обнаружение устройств*.



Для сетевого принтера в разделе **Пользователи -> Авторизация -> IP и MAC авторизация** необходимо создать правило **Пользователь < MAC-адрес**



При обнаружении активности от сетевого принтера или другого устройства его пользователь сразу появится в **Мониторинг -> Авторизованные пользователи**



Подсказка: В современных телефонах имеется опция **Рандомизация MAC-адреса**. Эта опция будет мешать при авторизации телефона по MAC-адресу. Рекомендуется эту опцию отключать, либо использовать другие типы авторизации (например: *Веб-аутентификации*)

13.2.4 Авторизация по подсетям

Основное

Чтобы не регистрировать каждое устройство в виде отдельного NGFW-пользователя и не фиксировать для него факторы авторизации, можно воспользоваться **Авторизацией по подсети**.

Эта функция позволит пользователю NGFW из требуемой подсети авторизоваться автоматически без привязки к MAC и/или конкретному IP и будет полезна, если требуется автоматически авторизовать большое количество устройств.

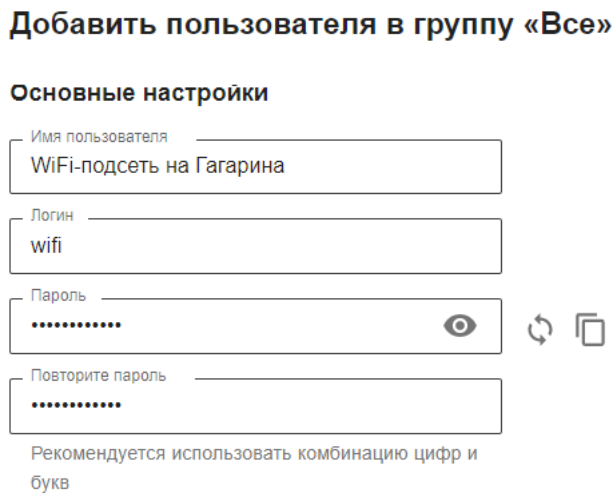
Подсказка: Трафик по всей подсети будет фиксироваться на одного пользователя.

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

Например, в подсети 192.168.10.0/24 есть Wi-Fi-подсеть, устройствам из которой нужно позволить авторизоваться. Создайте правило авторизации:

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

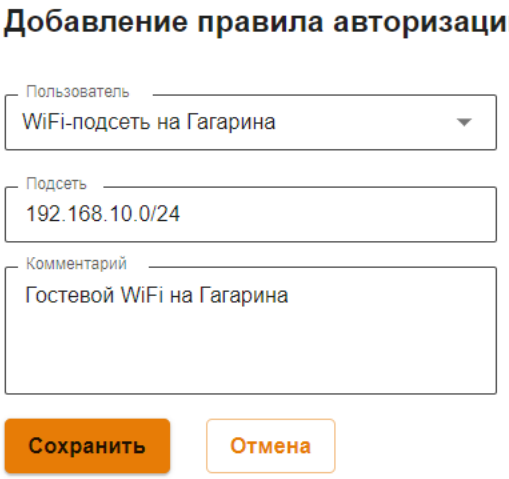
2. Заполните поля *Имя подсети*, *Логин* и нажмите **Сохранить**:



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

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

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



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

Предупреждение: Будьте внимательны при создании правил Авторизации по подсетям
Будут проблемы с авторизацией, если:

- Для разных пользователей создать пересекающиеся сети;
- Есть правила авторизаций пользователей по IP-адресам из подсети в правиле *Авторизации по подсетям*;
- Созданы правила в подразделе **Фиксированные IP-адреса VPN** с привязкой к IP-адресу из подсети правила *Авторизации по подсетям*.

13.2.5 Авторизация пользователей терминальных серверов

Подсказка: 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. Пользователи, отправляющие запросы с этих IP-адресов, 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 авторизовать 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)*.

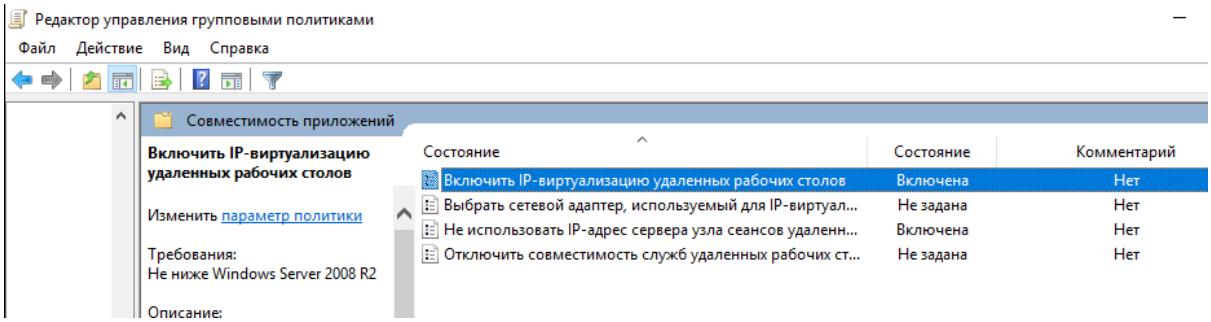
Подсказка: Авторизация пользователей терминального сервера по логам контроллера домена AD пока не реализована.

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 также 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, что настройки изменились, командой в PowerShell:

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

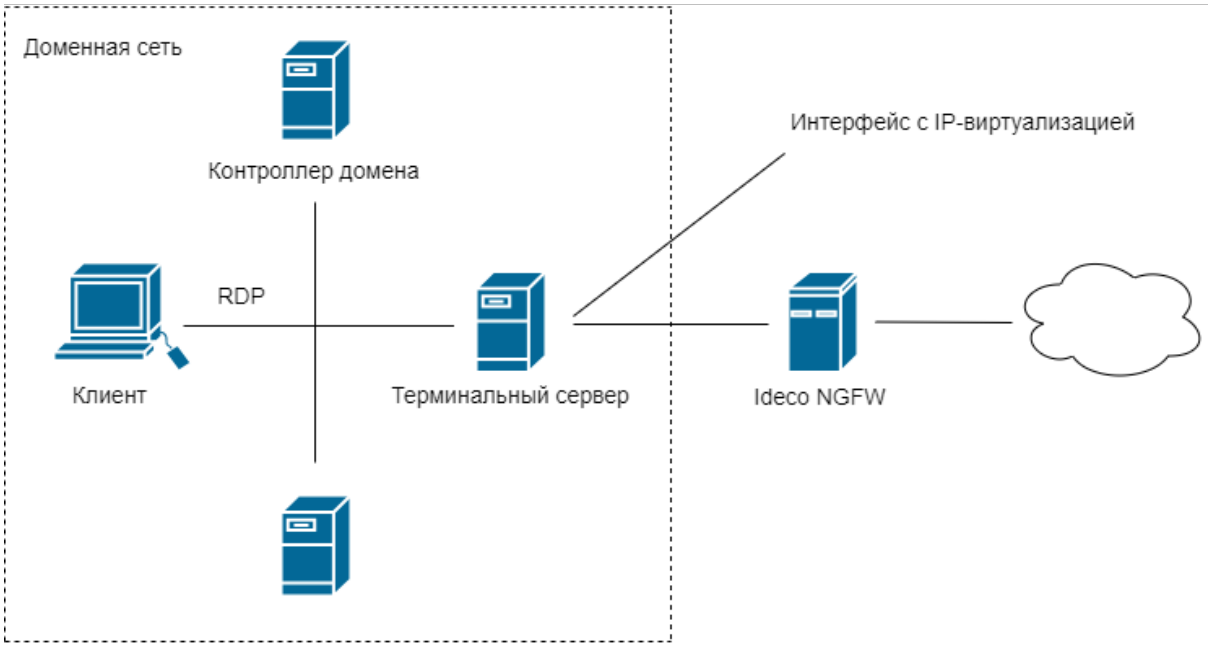
Значения:

- `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 подойдёт.

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 удалённых рабочих столов на сервере с ролью терминального сервера;

Подсказка: Далее описана настройка для режима **Для сеансов**, который выдаёт 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')
```

(continues on next page)

(продолжение с предыдущей страницы)

```
$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 удалённых рабочих столов –> Узел сеансов удалённых 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**;

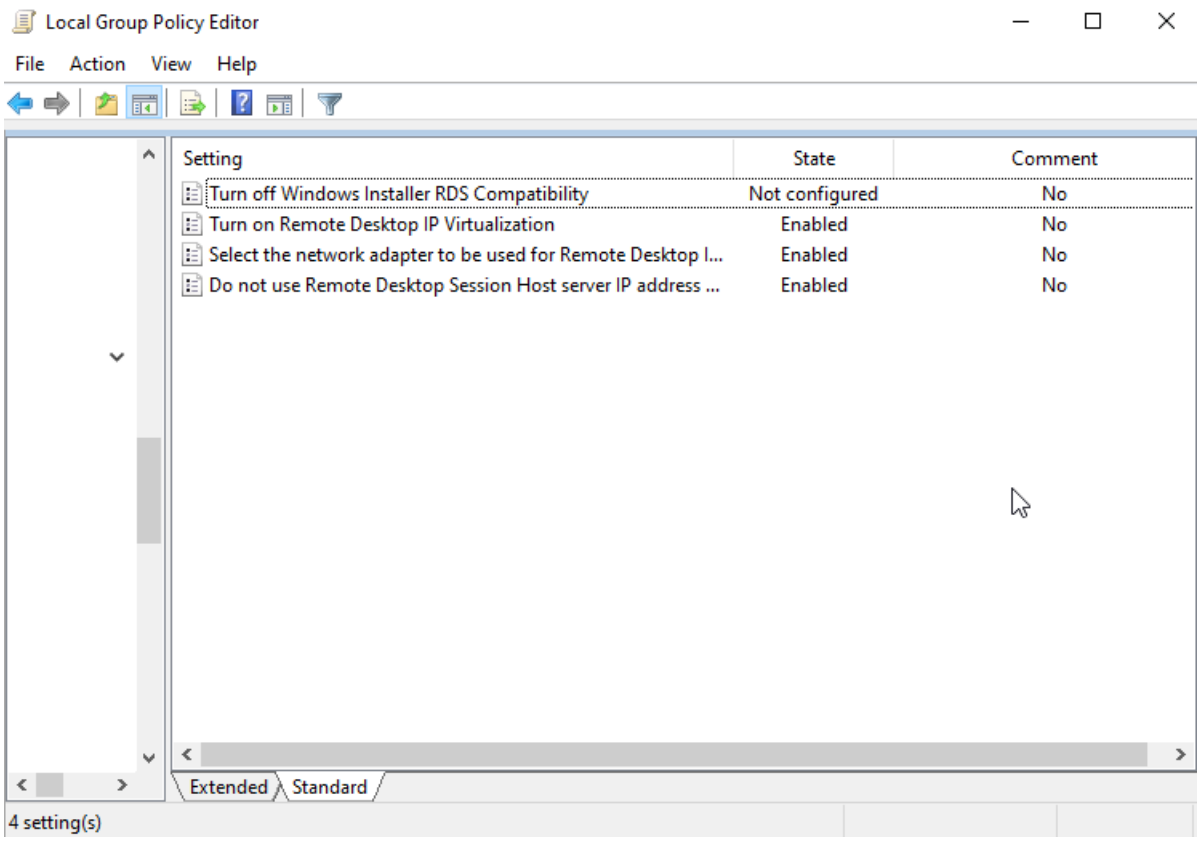
2. Включите параметр политики **Включить IP-виртуализацию удаленных рабочих столов** с параметром **Для сеансов**.

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

3. Включите параметр политики **Выбрать сетевой адаптер, используемый для IP-виртуализации удалённых 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

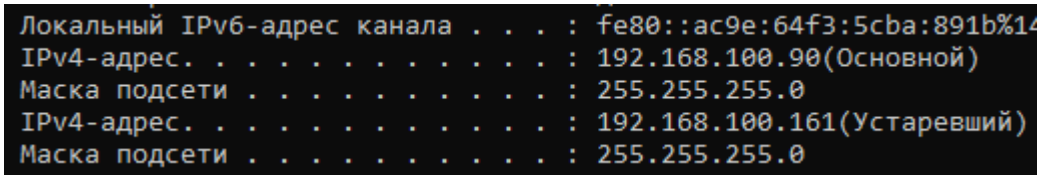
Тип: REG_MULTI_SZ (многострочный параметр)

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.



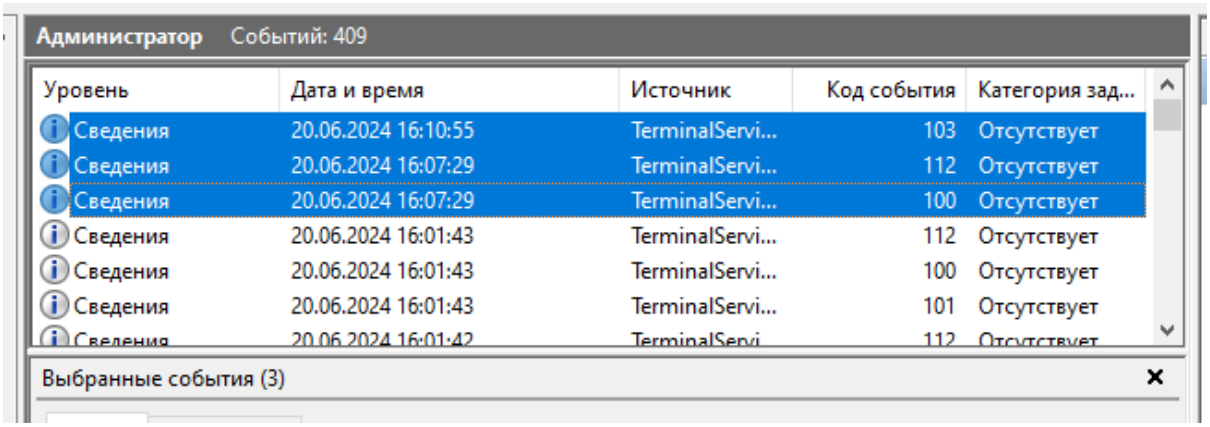
Диагностика

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 произведёт 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, подключённых к терминальному серверу через службу mstsc (**Подключение к удалённому рабочему столу**).

13.3 VPN-подключение

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

Инструкция по настройке VPN-подключения через *Ideco Client*.

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

Для получения доступа извне (из дома, отеля, другого офиса) к локальной сети предприятия, которая находится за Ideco NGFW, можно подключиться по VPN с этой машины (компьютера или мобильного устройства) к серверу Ideco NGFW.

Для client-to-site VPN наш сервер поддерживает четыре протокола туннельных соединений: *IKEv2*, *SSTP*, *L2TP/IPsec*, *PPTP*. Также поддерживается туннелирующий протокол *PPPoE*.

Подсказка: В целях безопасности не рекомендуется использовать протокол PPTP (он оставлен для совместимости с устаревшими операционными системами и оборудованием, а также для авторизации в локальной сети, где нет требований к строгому шифрованию трафика).

Рекомендуемым в плане скорости и безопасности является протокол IKEv2.

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.

Можно использовать *личный кабинет пользователя* для раздачи инструкций по созданию пользовательских VPN-подключений.

13.3.1 Основное

В поле **Сеть для VPN-подключений** указывается подсеть, в рамках которой будут динамически присваиваться IP-адреса. Маска подсети должна быть в диапазоне от 16 до 30.

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

Чтобы VPN-подключение работало на устройствах пользователей, необходимо загрузить корневой сертификат. Корневые сертификаты Ideco NGFW действительны в течение 10 лет.

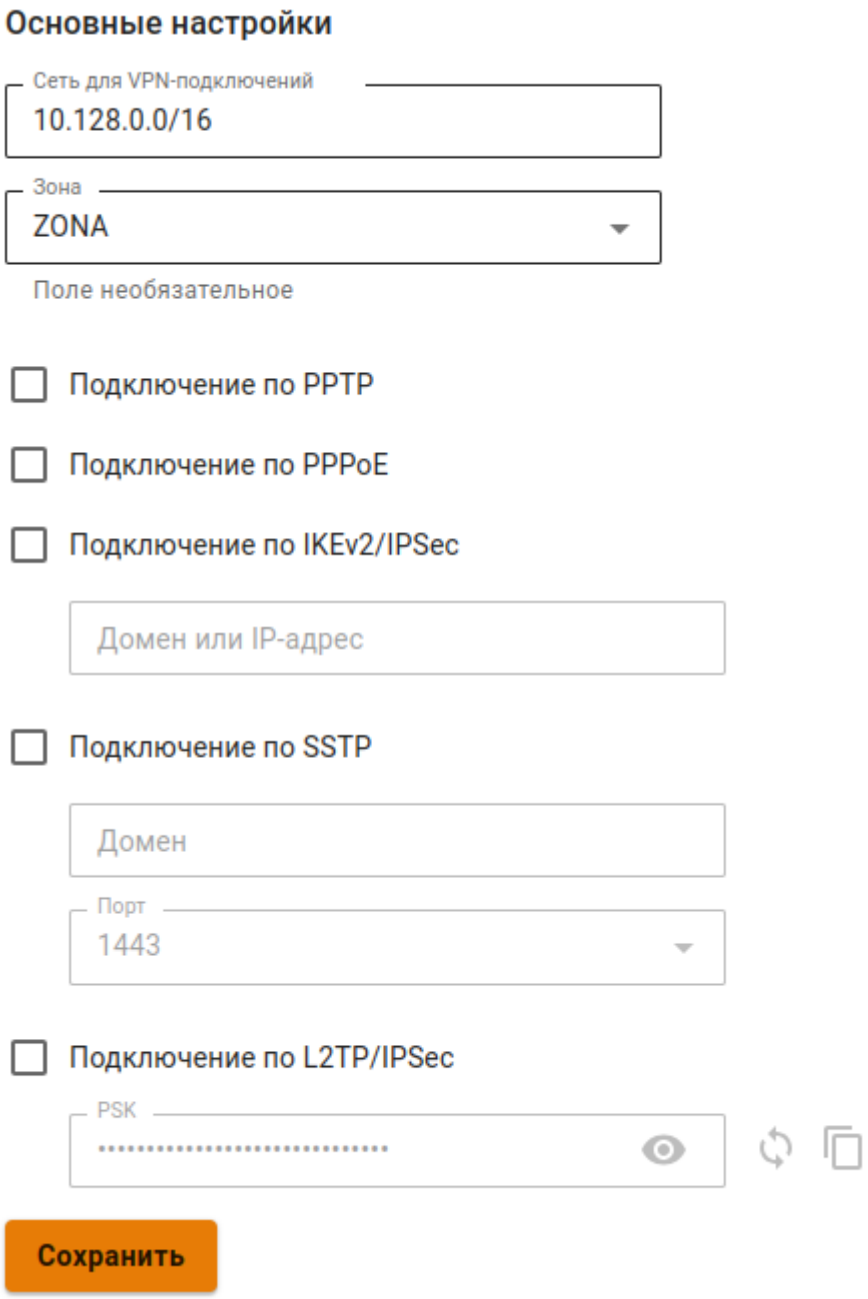
Если используется сертификат Let's Encrypt, обновление будет происходить автоматически. Подробнее о сертификатах можно узнать из соответствующей *статьи*.

Основные настройки

В основных настройках выберите протоколы, по которым смогут подключаться пользователи. Подробнее о настройках протоколов туннельных соединений - в статьях: *PPTP*, *IKEv2/IPsec*, *SSTP* и *L2TP/IPsec*, о настройке туннелирующего протокола PPPoE - в *статье*.

Для настройки конфигурации VPN-подключения сразу на несколько сетевых интерфейсов:

1. Создайте зону и добавьте сетевые интерфейсы для подключения по VPN в эту зону;
2. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное** и укажите зону, созданную на первом шаге.



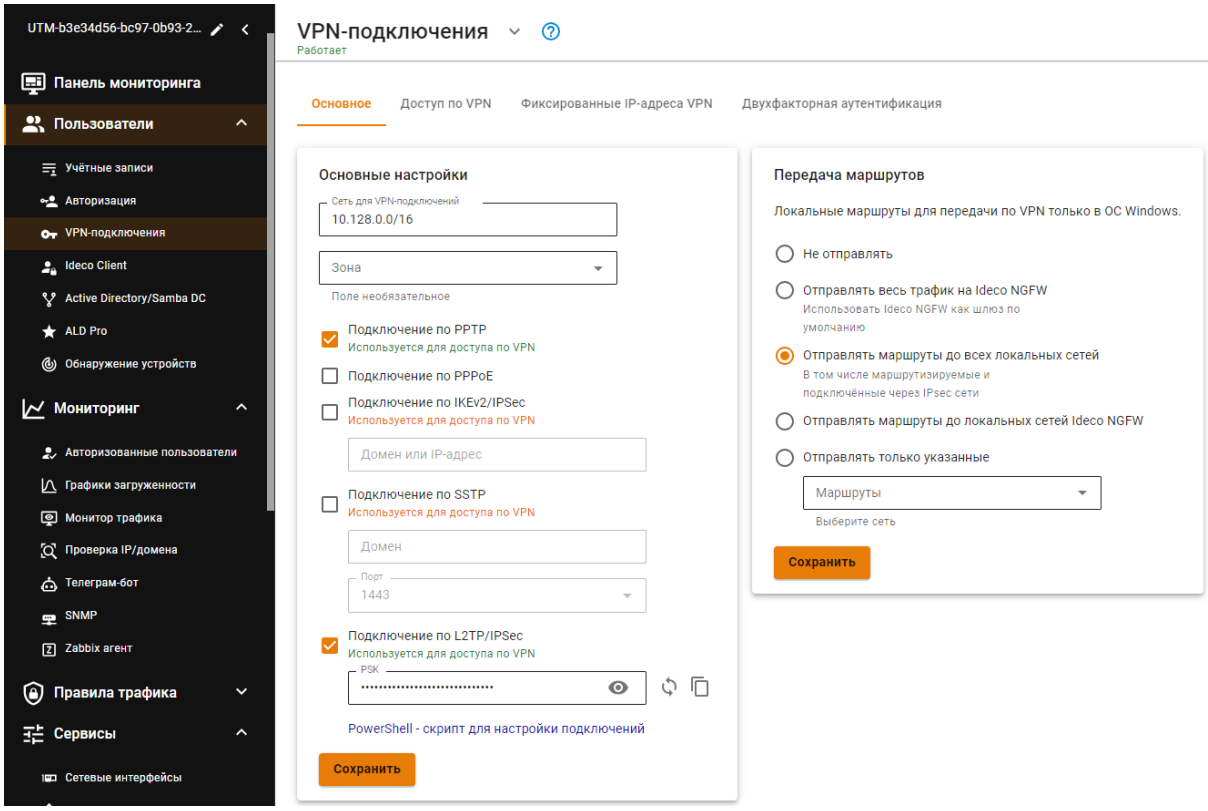
Подсказка: Используйте зоны для настройки конфигурации VPN-подключения сразу нескольких сетевых интерфейсов.

Внимание: Не рекомендуем использовать тип подключения PPTP. Этот способ подключения КРАЙНЕ небезопасен, оставлен исключительно для совместимости со старыми решениями. Используйте IPsec-IKEv2.

Статусы подключения

Начиная с 16.0 версии Ideco NGFW, у каждого протокола VPN-подключения появился статус использования. Статусы отображаются в виде подсказок под названиями протоколов, когда протокол используется в правилах таблицы **Доступ по VPN**.

Если включена опция рядом с названием протокола в разделе **Пользователи -> VPN-подключения -> Основное** и есть подключение, цвет статуса - зеленый, если протокол выключен - оранжевый.

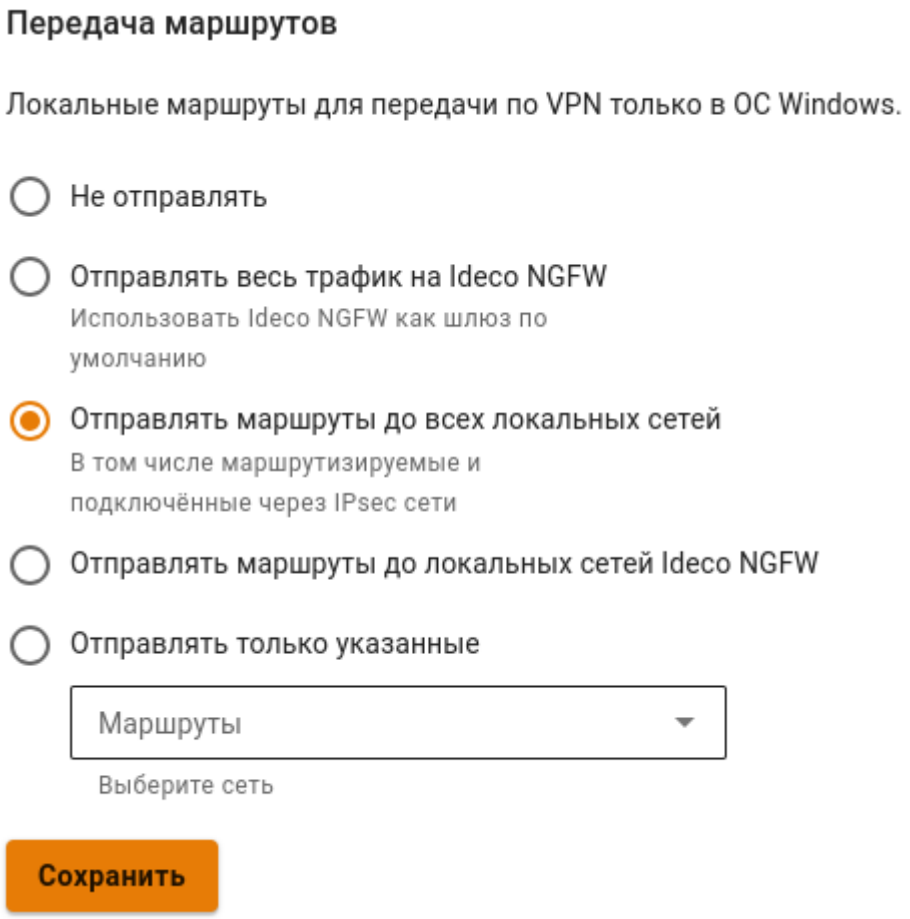


Передача маршрутов

Маршруты, переданные Ideco NGFW для VPN-клиента, имеют меньшую метрику (т. е. высокий приоритет). В меню передача маршрутов существует 5 опций для настройки передачи маршрутов клиентам:

1. **Не отправлять**. При включении данной опции клиентам не будут передаваться никакие маршруты, то есть никакой трафик не будет проходить через NGFW.
2. **Отправлять весь трафик на Ideco NGFW**. При включении этой опции клиентам будет передаваться маршрут 0.0.0.0/0, то есть весь трафик будет проходить через NGFW.
3. **Отправлять маршруты до всех локальных сетей**. При включении опции клиентам будут передаваться маршруты до всех локальных сетей NGFW, в том числе подключенных через IPSec и маршрутизируемых.
4. **Отправлять маршруты до локальных сетей Ideco NGFW**. При включении опции клиентам будут переданы маршруты только до локальных сетей NGFW, без учета IPSec и маршрутизируемых.

5. **Отправлять только указанные**. При включении опции предоставляется возможность выбрать, какие маршруты нужно отправлять клиентам.



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

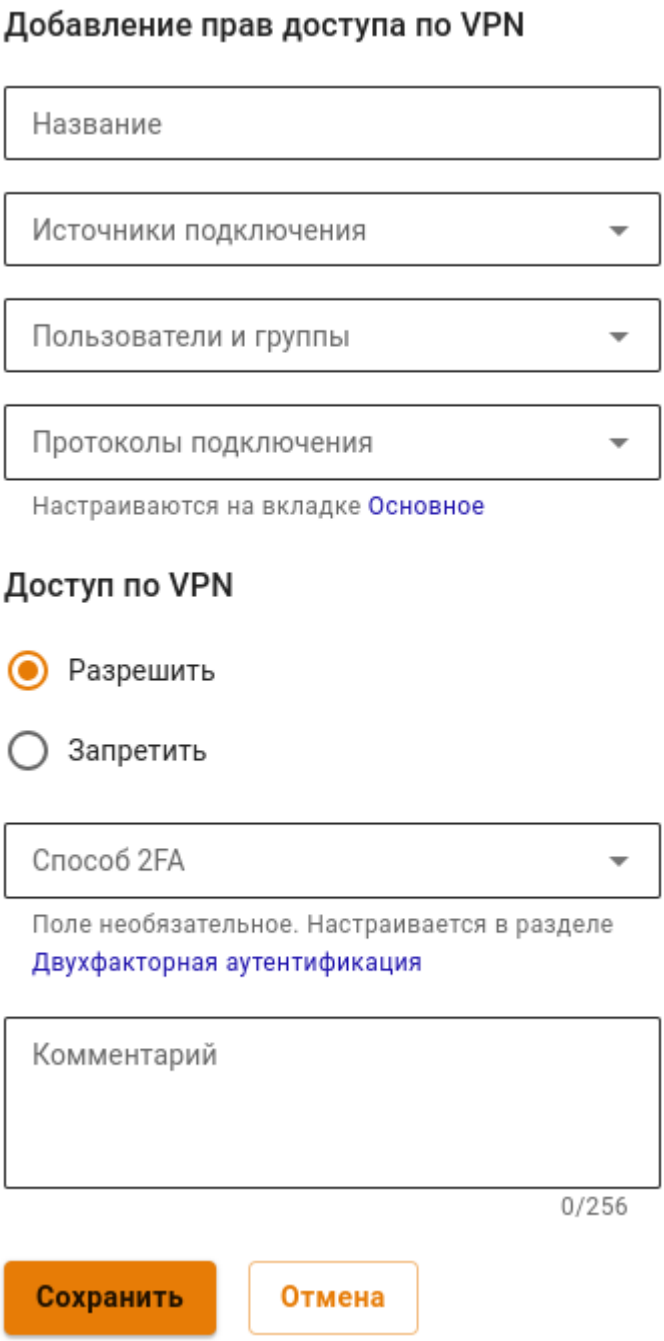
13.3.2 Доступ по VPN

Вкладка содержит таблицу правил, которые действуют сверху вниз. Как только в правиле происходит совпадение полей **Источник подключения**, **Пользователи и группы**, **Протокол подключения** производится действие, выбранное при создании правила. В случае указания **Способа 2FA** будет происходить аутентификация по второму фактору. В правилах можно использовать как группы пользователей Ideco NGFW, так и группы безопасности AD.

Подсказка: Для добавления группы безопасности AD для VPN не требуется импорт в дерево пользователей. Введите Ideco NGFW в домен и выберите на вкладке **Доступ по VPN** требуемую группу безопасности.

Для включения доступа по VPN у группы пользователей выполните действия:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN**.
2. Заполните необходимые поля формы:



3. Нажмите **Сохранить**.

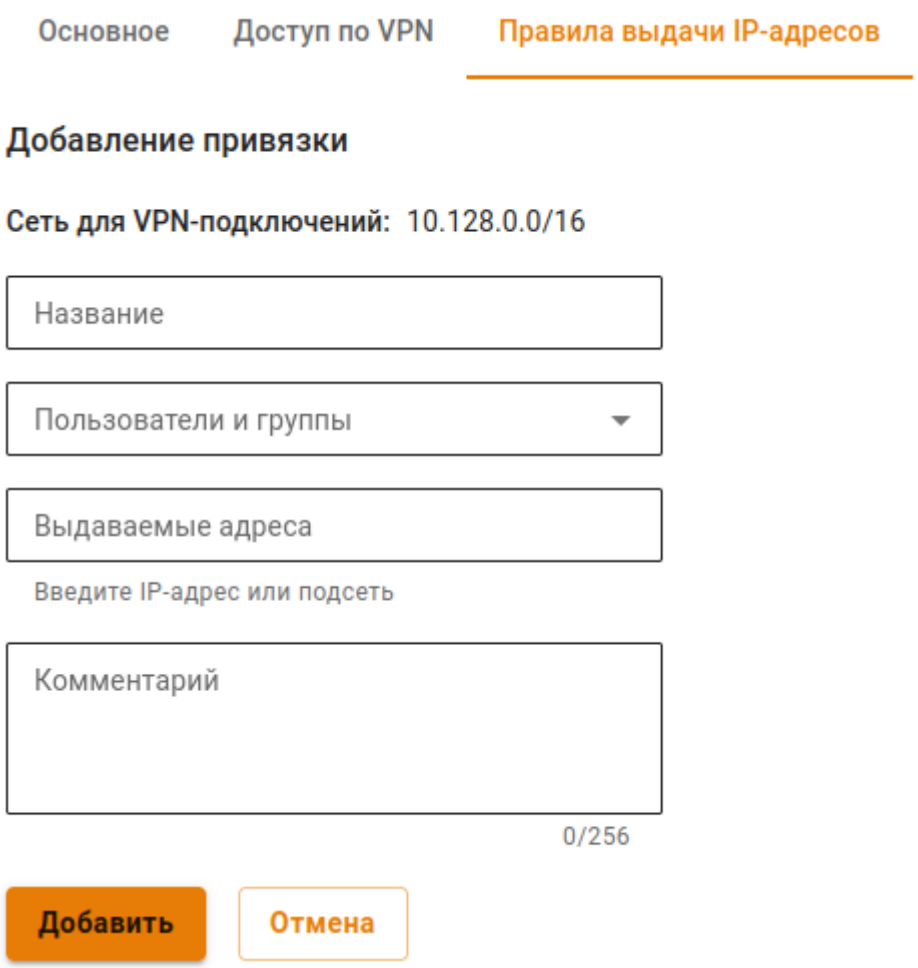
Подсказка: Для работы VPN-подключений по выбранному протоколу настройте Ideco NGFW соответствующим образом в разделе **VPN-подключения -> Основное**.

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

13.3.3 Фиксированные IP-адреса VPN

Подсказка: Если создать фиксированную привязку для какого-либо пользователя, то для него будет возможна только одна активная VPN-сессия.

Например: хост в локальной сети, к которому могут подключиться пользователи только с определенными IP-адресами. Для предоставления прямого доступа по VPN-подключению к этому хосту перейдите в раздел **Пользователи -> VPN-подключения -> Фиксированные IP-адреса VPN**, нажмите **Добавить**, заполните поля **Пользователь** и **IP-адрес** и нажмите **Применить**.



- **Название** - введите название правила;
- **Пользователи и группы** - выберите пользователей или группы пользователей, на которых будет распространяться правило;
- **Выдаваемые адреса** - введите IP-адрес или подсеть;
- **Комментарий** - поле может быть пустым.

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.

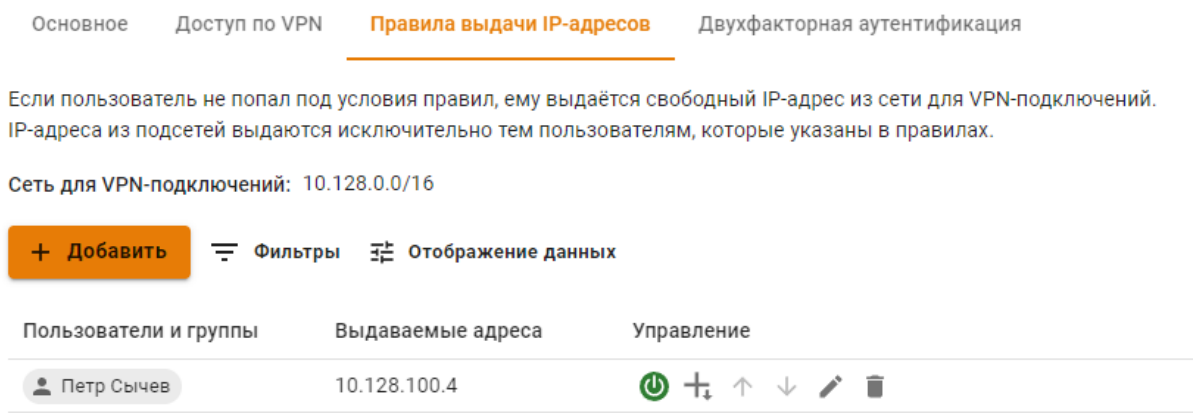
- Если в разных правилах указаны пересекающиеся сети (например, сеть `10.128.1.0/24` является подсетью сети `10.128.0.0/20`), то:
  - адреса из сети `10.128.1.0/24` никогда не будут выдаваться;
  - при выдаче адресов сети `10.128.0.0/20` из нее будут исключаться адреса подсети `10.128.1.0/24`.
- Если 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 пользоавтеля 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.

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:



13.3.4 Двухфакторная аутентификация

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

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.

В Ideco NGFW реализовано три типа двухфакторной аутентификации:

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

Подсказка: Для двухфакторной аутентификации SMS Aero и Мультифактор требуется указать номер телефона в карточке пользователя. С версии 17.4 и выше при использовании Мультифактора указывать номер телефона не обязательно.

Для корректной работы двухфакторной аутентификации с использованием TOTP-токена необходимо, чтобы совпадало время на Ideco NGFW и устройстве пользователя с приложением для второго фактора.

Предупреждение: Двухфакторная аутентификация не работает для пользователей RADIUS-сервера.

При добавлении прав доступа по VPN для группы пользователей RADIUS-сервера появится предупреждение, что для этой группы пользователей двухфакторная аутентификация отключена.

Настройки Ideco NGFW с разными типами аутентификации

Для работы двухфакторной аутентификации выполните действия:

1. Укажите домен в Ideco NGFW для перенаправления запроса двухфакторной аутентификации с IP-адреса Ideco NGFW:

- 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 -> VPN-подключения -> 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.

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**.

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**.

4. Разрешите доступ по VPN нужным группам пользователей в таблице **Доступ по VPN**, воспользовавшись *инструкцией*.

Настройка аутентификации на пользовательских устройствах

Для настройки определенного типа аутентификации на устройстве пользователя воспользуйтесь инструкциями ниже:

TOTP-токен:

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

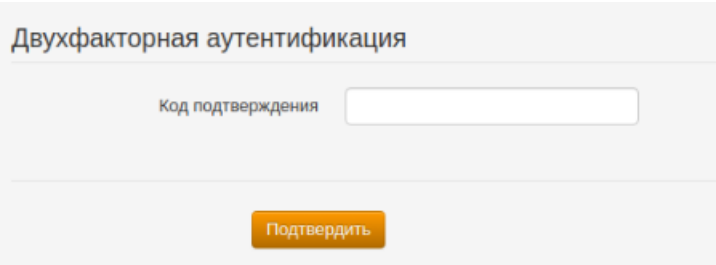
2. Войдите в личный кабинет NGFW, указав логин и пароль пользователя.

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

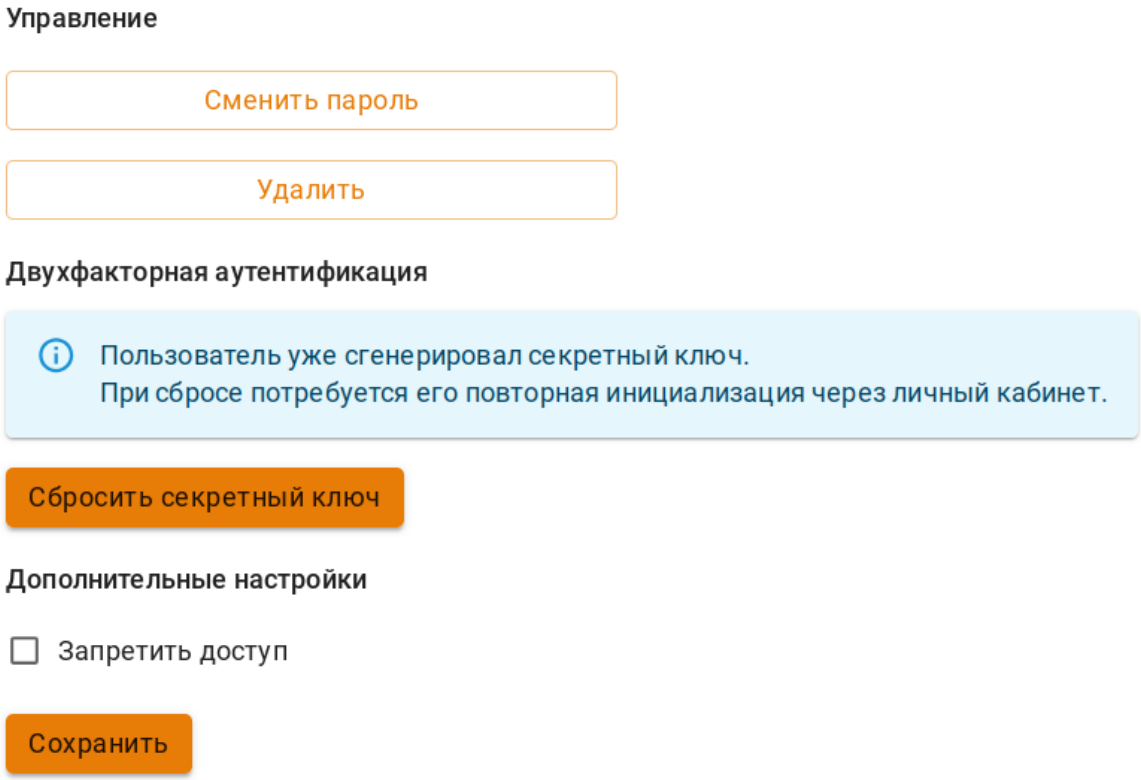
4. Войдите в приложение для аутентификации (Яндекс Ключ, Google Authenticator или Microsoft Authenticator и т.п.), отсканируйте код или введите секретный ключ, который находится под QR-кодом. При вводе ключа выберите тип ключа **По времени**. Если выбрать тип **По счетчику**, то пользователь не сможет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

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

5. Подключитесь к VPN и откройте любой сайт, кроме личного кабинета пользователя. В появившемся поле введите код, который вы получили в приложении:



Подсказка: Чтобы сбросить секретный ключ TOTP-токена, который сгенерировал пользователь, перейдите в раздел **Пользователи -> Учетные записи**. Выберите нужного пользователя и нажмите **Сбросить секретный ключ**:



SMS Aero:

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

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

Для Windows 10:

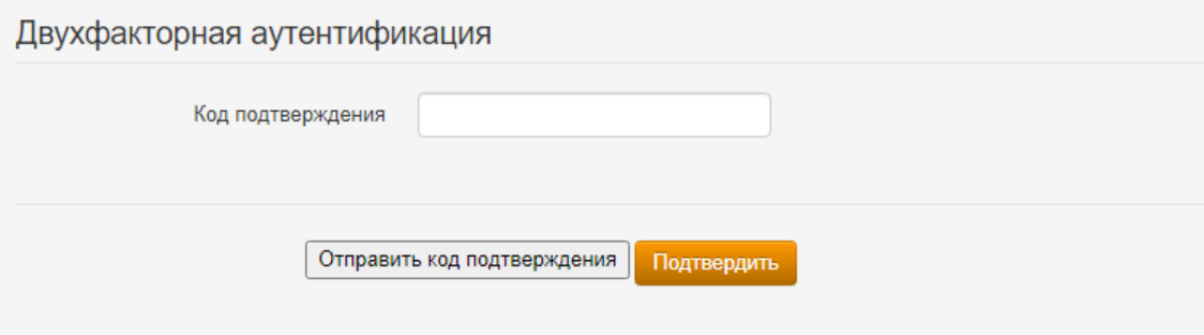
- Откройте параметры и перейдите в раздел **Сеть и Интернет -> VPN -> Настройка параметров адаптера**;
- Нажмите правой кнопкой мыши по созданному подключению и выберите **Свойства**;
- Перейдите во вкладку **Сеть**;
- Нажмите на **IP версии 4 (TCP/IPv4) -> Свойства -> Дополнительно**;
- Снимите флаг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

Для Ubuntu:

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

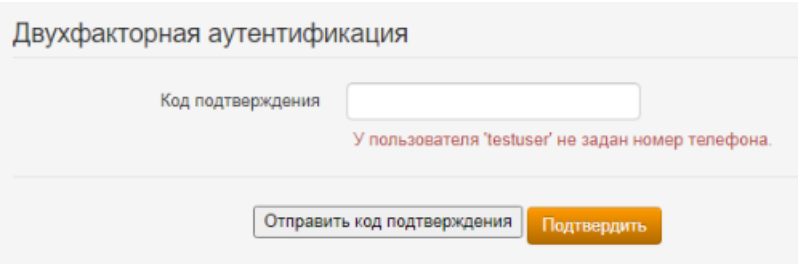
3. Включите созданное VPN-подключение.

4. Перейдете в браузер, откроется страница аутентификации:

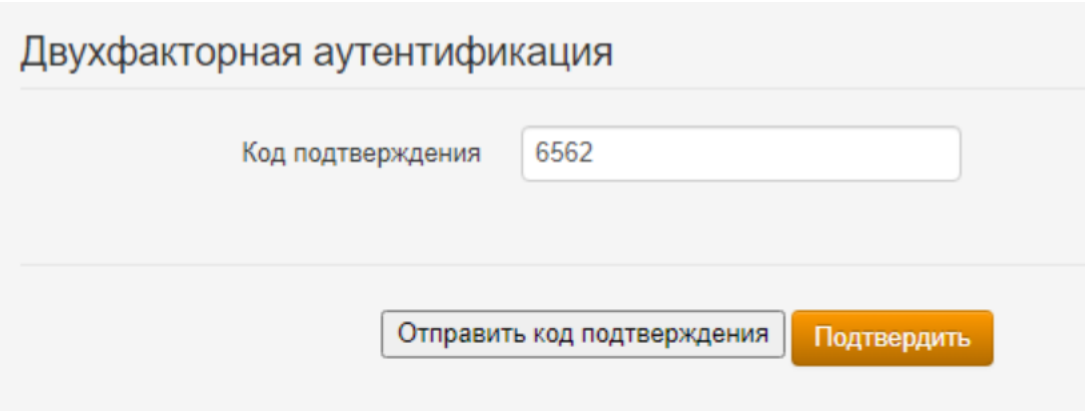


5. Нажмите **Отправить код подтверждения**. На номер телефона, указанный в учетной записи, придет SMS с кодом:

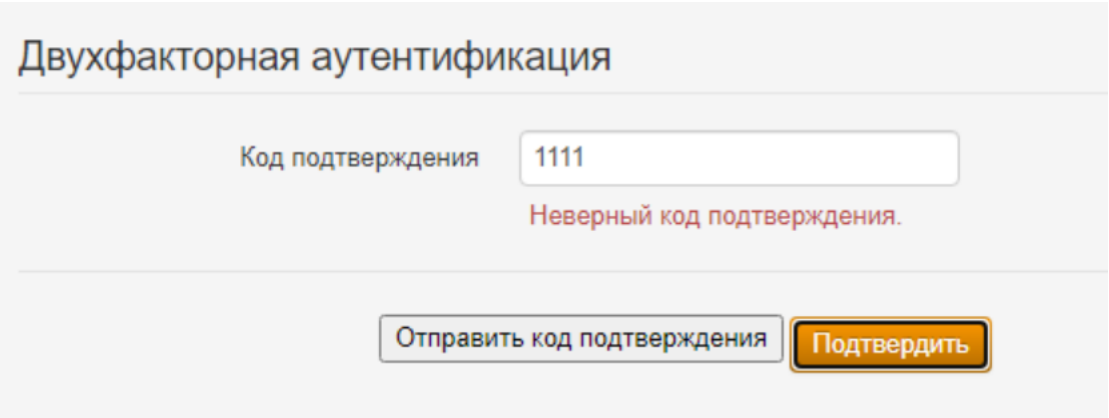
- Если номер телефона в карточке пользователя отсутствует, то на странице аутентификации появится предупреждение:



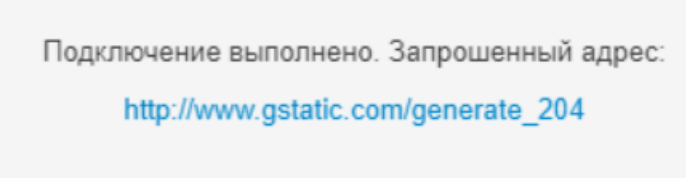
- Если номер телефона сохранен, то на указанный номер телефона поступит SMS. Введите код из SMS и нажмите **Подтвердить**:



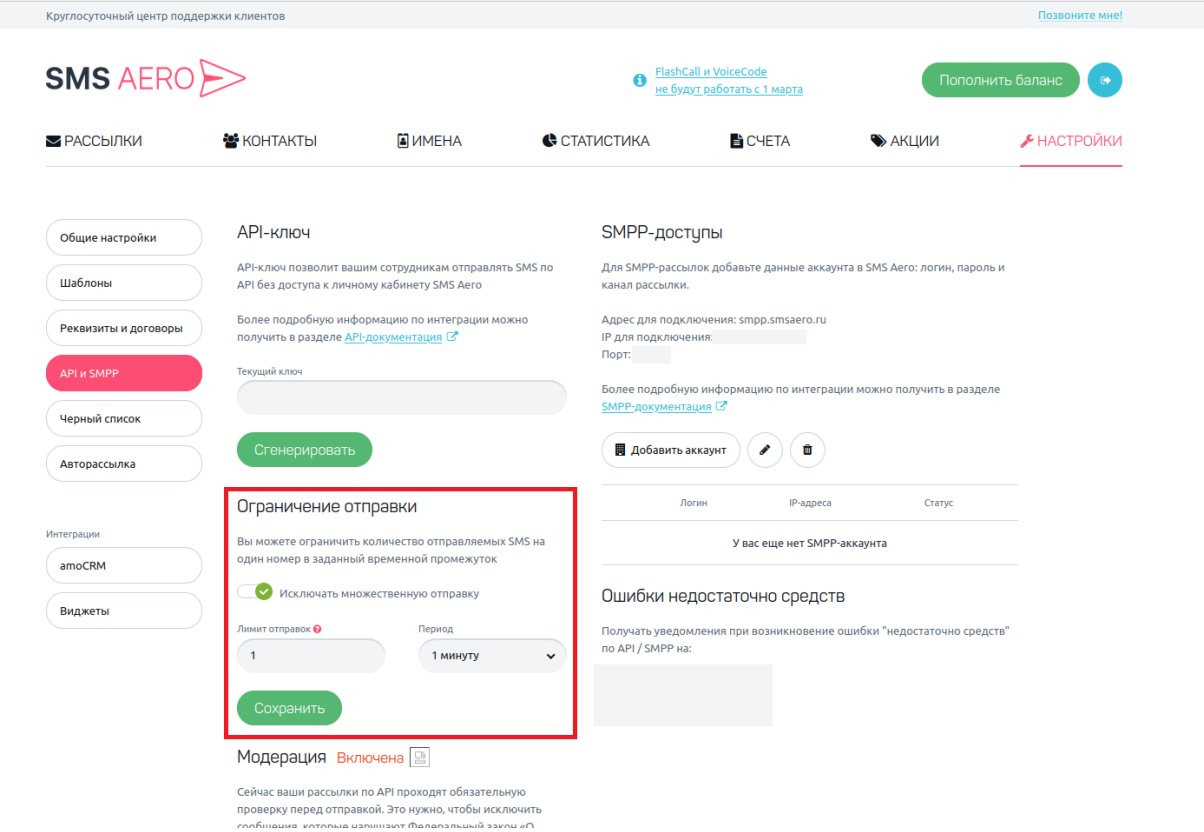
- Если код введен неверно, то появится соответствующее предупреждение:



- Если код введен верно, то появится следующее окно:



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

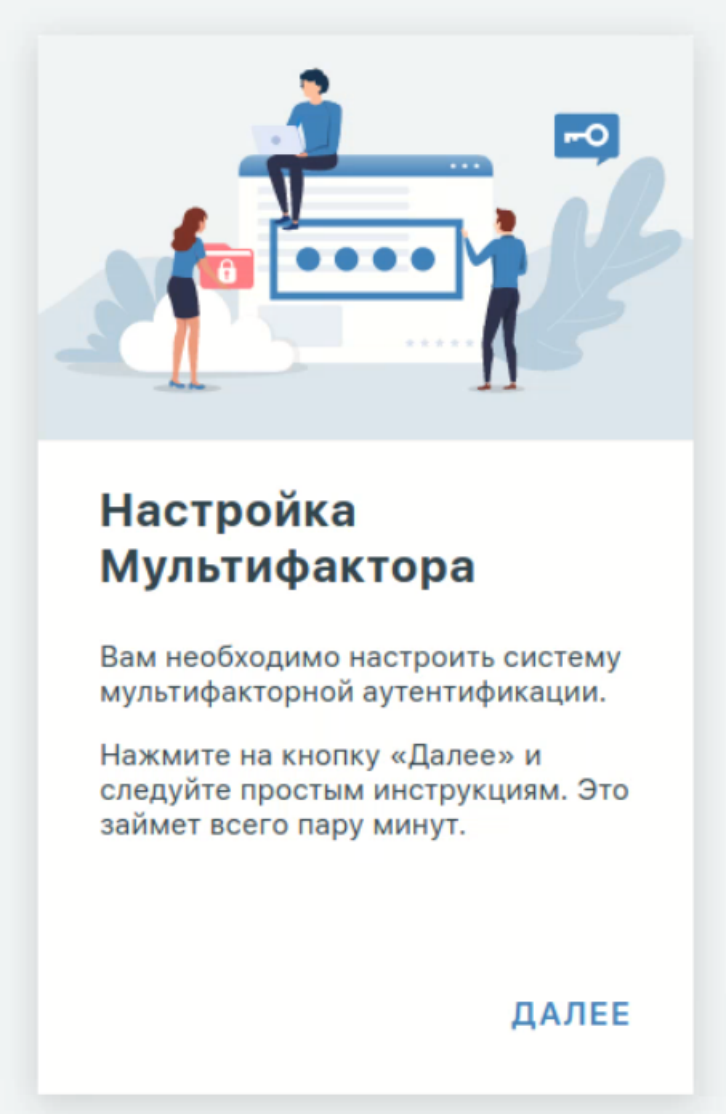


Мультифактор:

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

2. Включите созданное VPN-подключение.

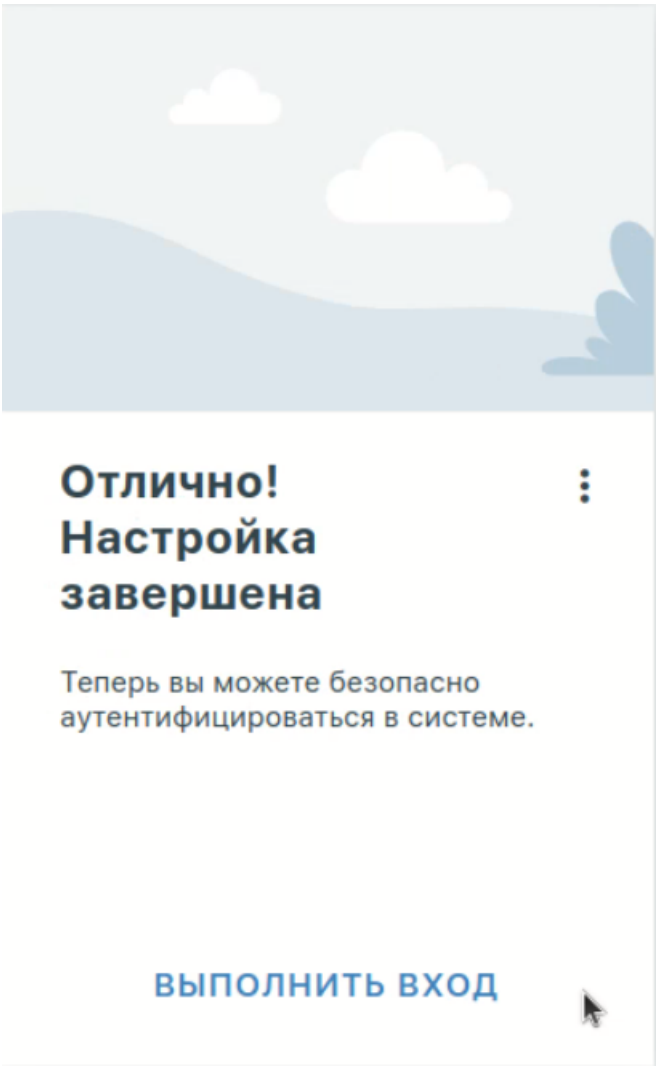
3. При переходе в браузер откроется страница аутентификации:



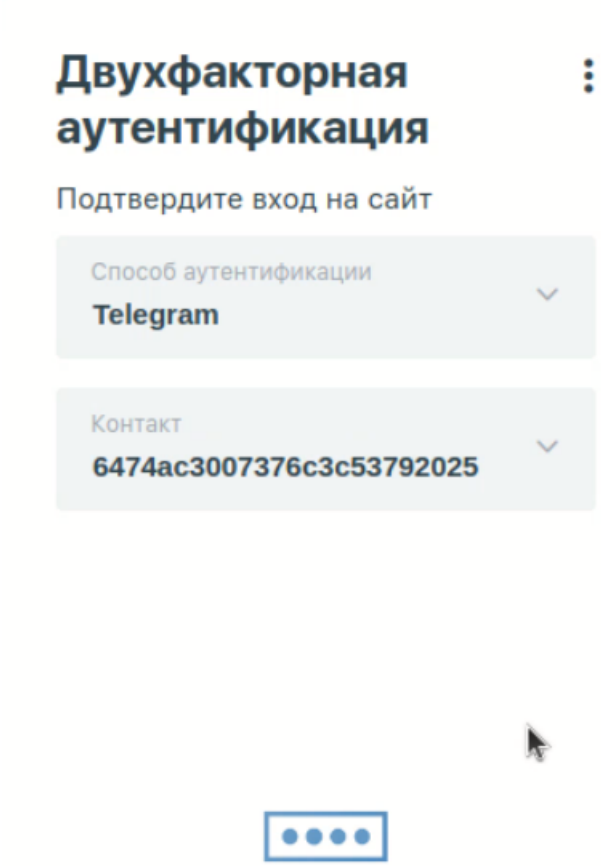
4. После нажатия **Далее** появится страница с предложением установить приложение на устройство пользователя. Если приложение установлено, нажмите **Далее**.

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.

13.3.5 Подключение по PPTP

> **Внимание:** Не используйте этот тип подключения, он КРАЙНЕ небезопасен, оставлен исключительно для совместимости со старыми решениями. Используйте IPsec-IKEv2.
>
> Инструкции по настройке VPN-подключений на разных ОС доступны по *ссылке*.

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.

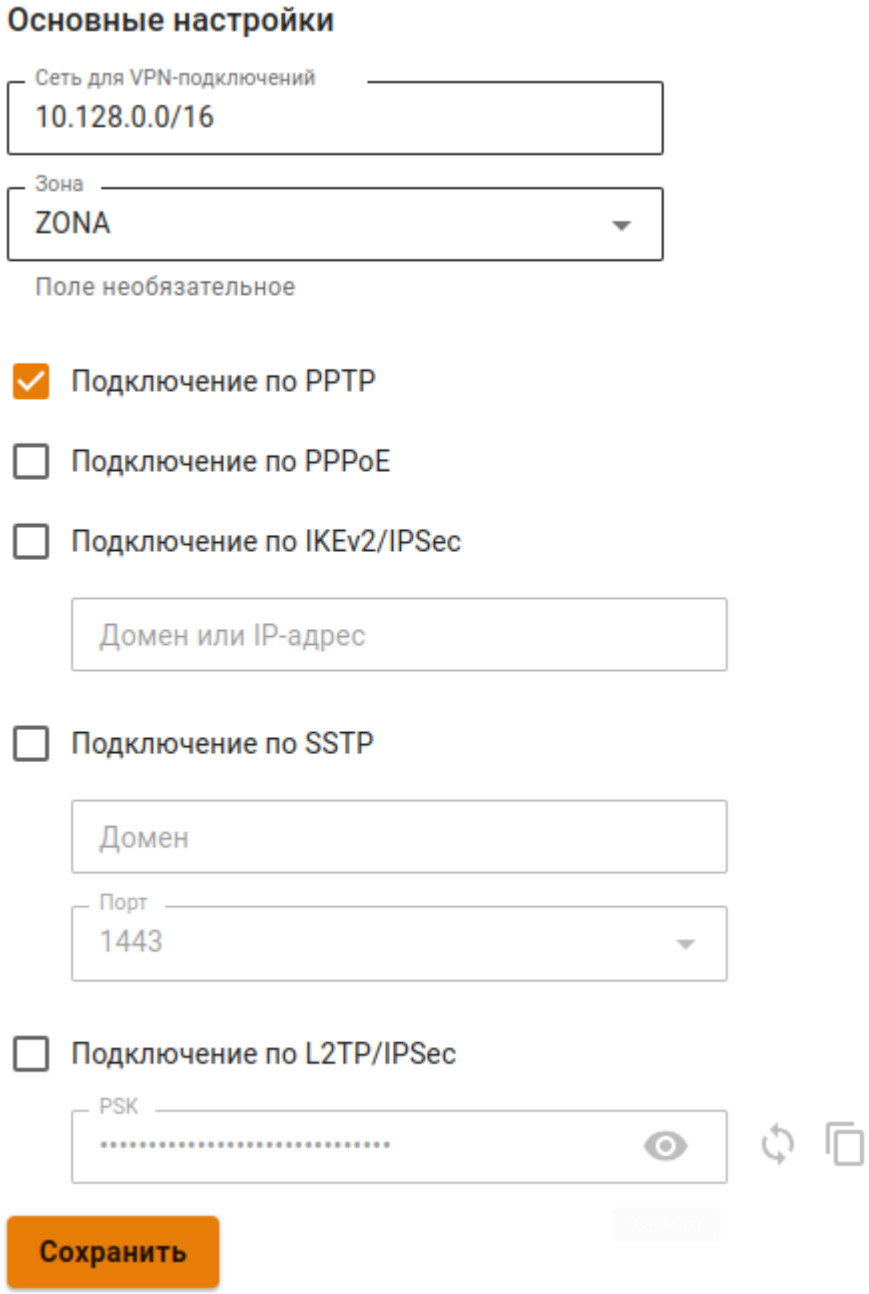
При успешной аутентификации и установлении PPTP-туннеля сетевому устройству будет автоматически назначен дополнительный IP-адрес для получения доступа к ресурсам сети интернет. Использование авторизации по PPTP никак не отражается на возможности доступа сетевого устройства к ресурсам локальной сети.

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

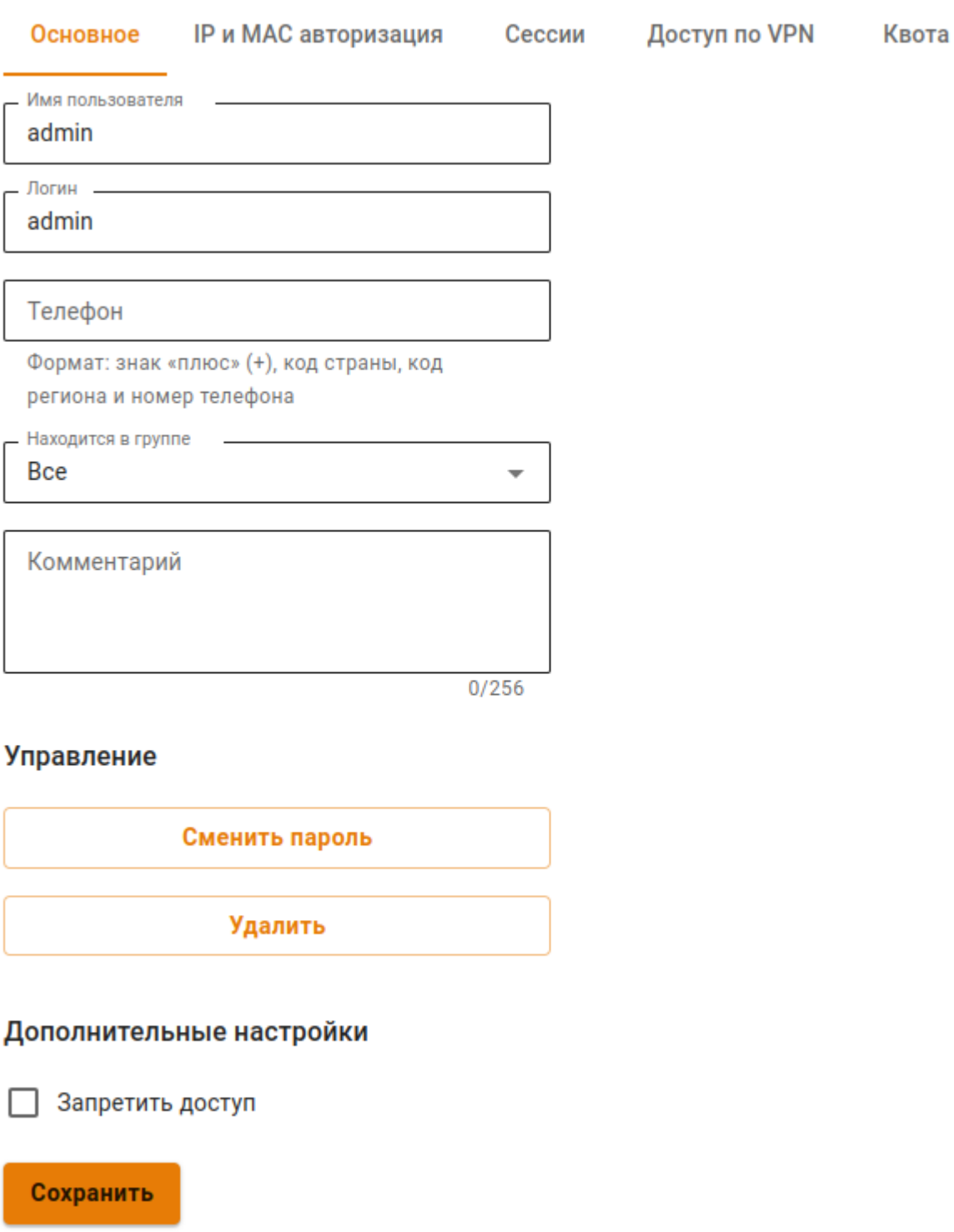
Настройка глобальных параметров Ideco NGFW

Для настройки авторизации по протоколу PPTP необходимо выполнить следующие действия:

1. Перейти в раздел **Пользователи -> VPN-подключение -> Основное**.
2. Включить флаг **Подключение по PPTP**.
3. Нажать на кнопку **Сохранить**.



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



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

Чтобы настроить **статическую** привязку адресов, выдаваемых по VPN определенным пользователям, необходимо перейти в раздел **Пользователи -> VPN-подключения -> Фиксированные IP-адреса VPN**, нажать **Добавить** и указать нужного пользователя и IP-адрес:

При подключении из сети интернет рекомендуем использовать IPsec IKEv2, L2TP IPsec или SSTP для более надежного шифрования трафика.

Настройка пользователей в Ideco NGFW

Разрешите пользователю подключения по VPN из сети интернет, создав в разделе **Пользователи -> VPN-подключения -> Доступ по VPN** разрешающее правило.

Возможные неполадки

- Провайдер со стороны шлюза или со стороны подключаемого клиента не пропускает GRE-протокол, с помощью которого происходит PPTP-соединение. В таком случае при попытке подключиться на внешний адрес Ideco NGFW будет получена ошибка 619. Можно определить, с какой стороны проблема, подключаясь с разных мест и от разных провайдеров. Если из некоторых мест удастся подключиться, значит, проблема со стороны тех клиентов, которые подключиться не могут. Когда провайдер будет определен, то нужно попытаться решить проблему с ним, либо использовать *IPsec-IKEv2* или *SSTP*;
- Заблокирован порт 1723 TCP. Проверить доступность порта можно с помощью стандартных сетевых утилит, таких как telnet. Если соединения на этот порт нет, то туннель не может быть установлен;
- Неправильно указан логин или пароль пользователя. Если такое происходит, то часто при повторном соединении предлагается указать домен. Старайтесь создавать для ваших учетных записей цифро-буквенные пароли, желательно, на латинице. При неправильном вводе пароля более 6 раз произойдет блокировка IP-адреса пользователя *службой защиты от подбора паролей*;
- Если подключение осуществляется с ОС Windows, для того чтобы пакеты пошли через него, надо убедиться, что в настройках этого подключения стоит чекбокс **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 отмечать только MSCHAPV2.

Если VPN-соединение установлено, но не получается получить доступ к ресурсам локальной сети

Выполните рекомендации статьи *Особенности маршрутизации и организации доступа*.

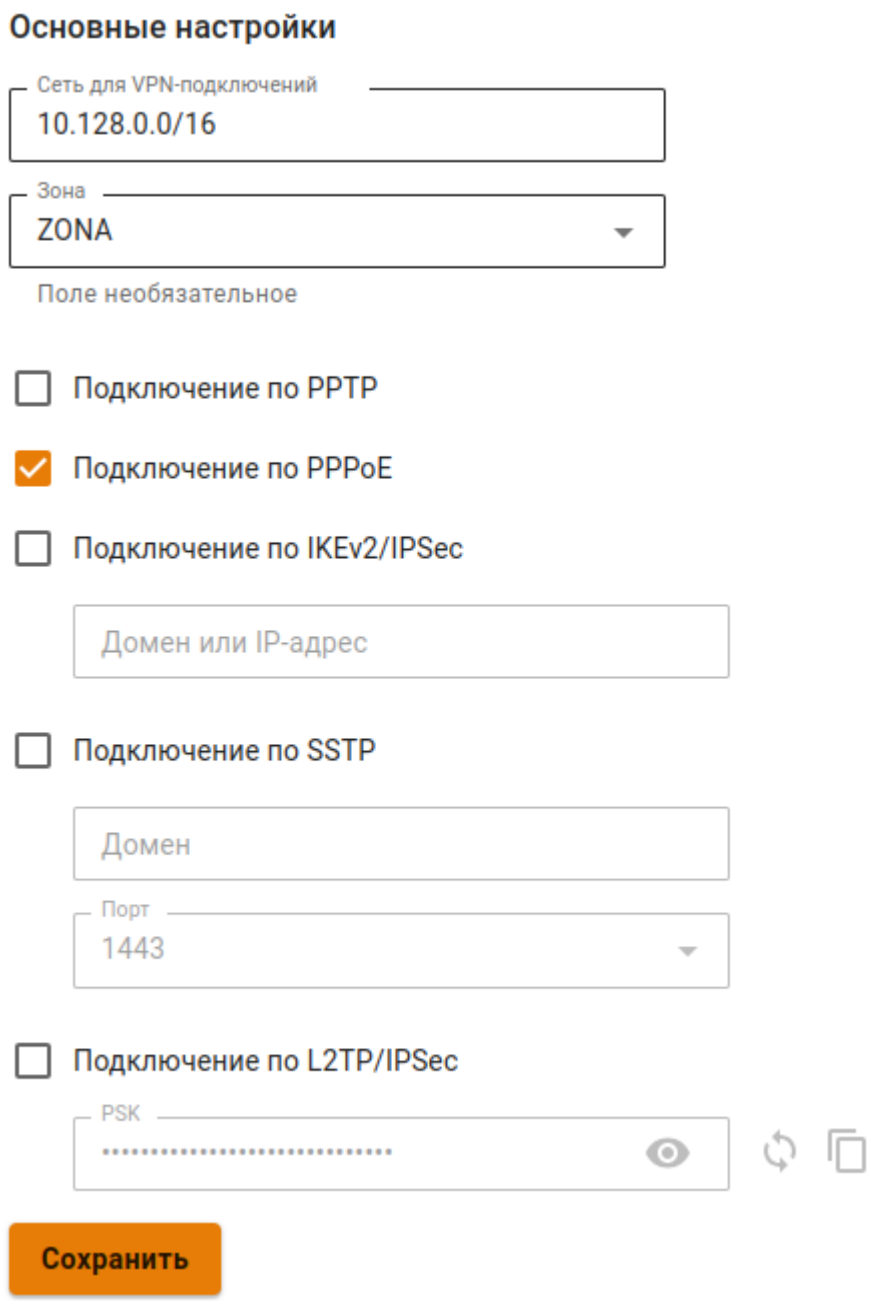
13.3.6 Подключение по PPPoE

Основное

Авторизация по протоколу PPPoE предполагает авторизацию по защищенному сетевому туннелю между сетевым устройством пользователя и сервером Ideco NGFW. Аутентификация пользователя осуществляется по связке Логин/Пароль. При этом типе авторизации не требуется назначение IP-адреса рабочей станции, так как IP-адрес будет автоматически назначен в случае успешной аутентификации и создания защищенного сетевого туннеля.

Для настройки авторизации по протоколу PPPoE необходимо выполнить следующие действия:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.
2. Установите флаг у пункта **Подключение по PPPoE** и нажмите кнопку **Сохранить**.



Подсказка: Подключение по PPPoE возможно только в одном ethernet-сегменте с локальными интерфейсами Ideco NGFW.

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

13.3.7 Подключение по IKEv2/IPsec

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

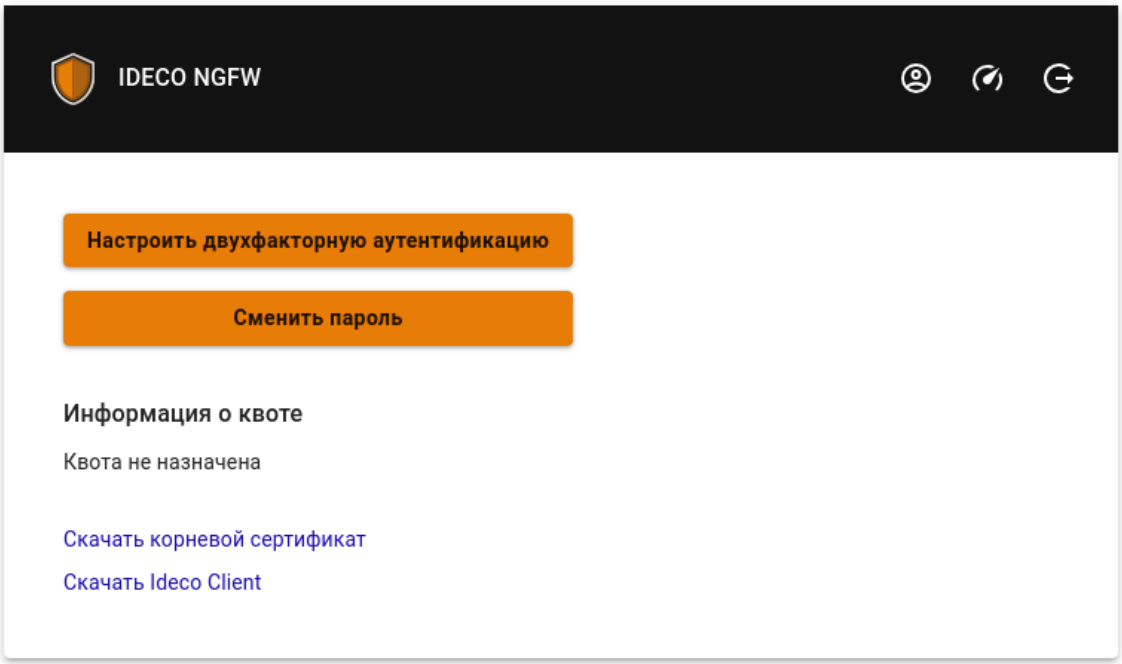
Инструкции по настройке VPN-подключений на разных ОС доступны по *ссылке*.

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

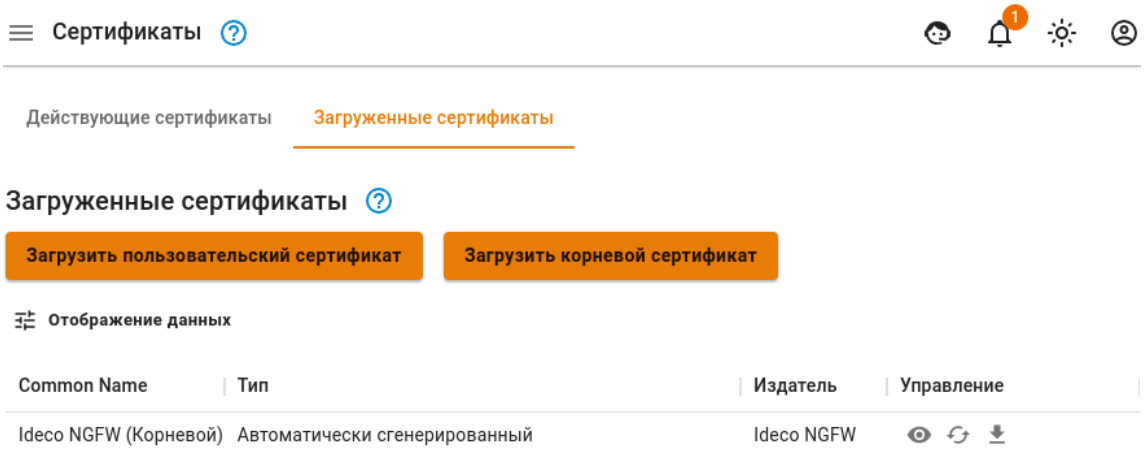
Настройка VPN-сервера в Ideco NGFW

Если корневой сертификат NGFW не находится в доверенных, то скачайте и установите его на компьютер пользователя. Скачать сертификат можно одним из способов:

- В личном кабинете, введя логин/пароль пользователя:

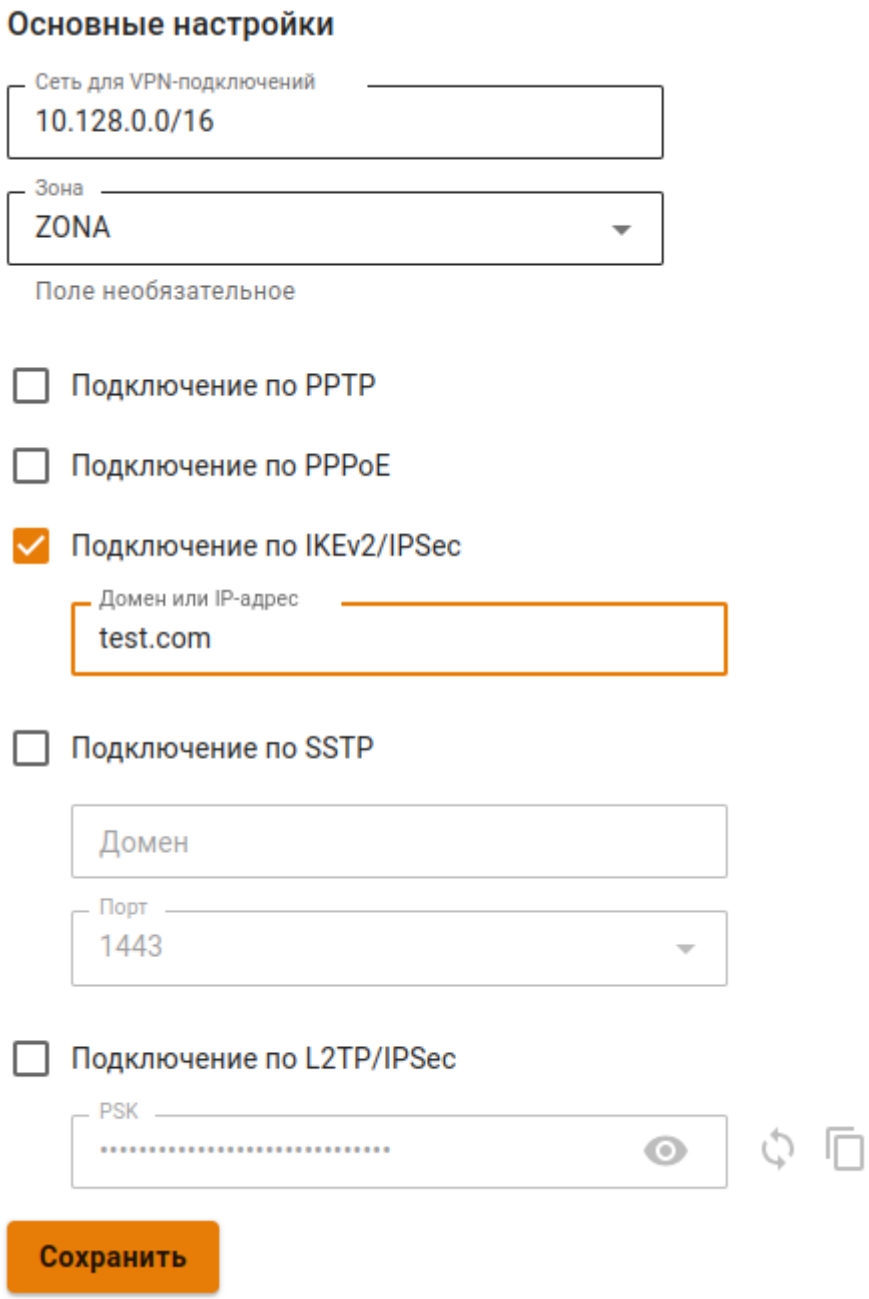


- В разделе **Сервисы -> Сертификаты -> Загруженные сертификаты**:



1. Для включения авторизации по IKEv2 установите соответствующий флаг **Подключение по IKEv2/IPsec** в разделе веб-интерфейса **Пользователи -> VPN-подключение -> Основное**.

2. 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. Wildcard-сертификат не может быть использован.



3. Создайте в разделе **Пользователи -> VPN-подключения -> Доступ по VPN** правило, разрешающее пользователю VPN-подключение для пользователей, которым необходимо подключаться извне по VPN. Указанный в карточке пользователя логин и пароль будут использоваться для подключения.

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

Поддержка IPsec IKEv2 в клиентских ОС

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

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.

13.3.8 Подключение по SSTP

Подсказка: 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 IPsec-IKEv2 вместо SSTP.

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

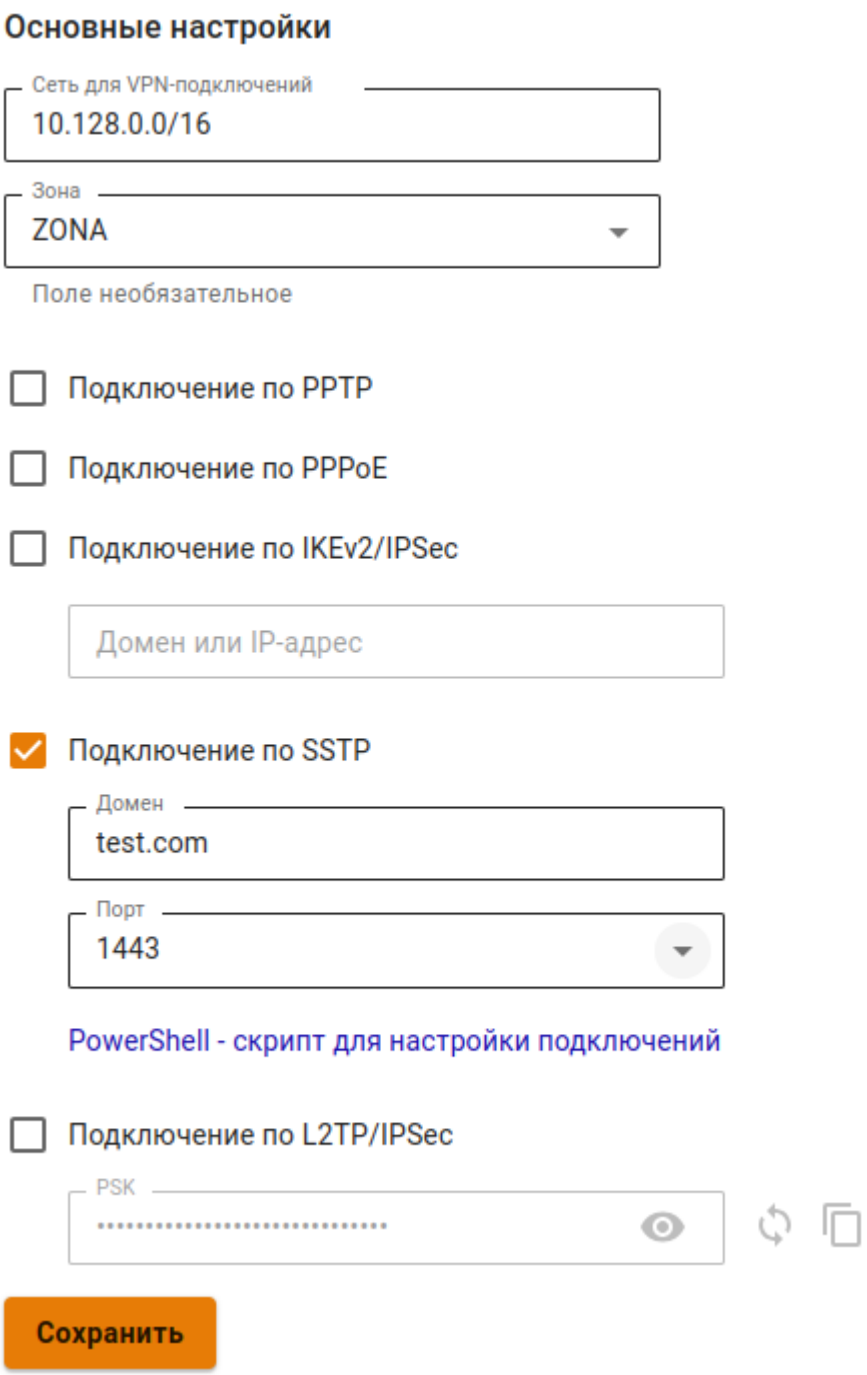
Настройка Ideco NGFW

Предупреждение: Запрещено использовать домен `.local`. Подключение по SSTP поддерживается только из внешних сетей.

1. Для включения авторизации по SSTP установите флаг **Подключение SSTP** в веб-интерфейсе в разделе **Пользователи -> VPN-подключение -> Основное**.

2. 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** необходимо указать данное DNS-имя (используйте реальное имя с правильной A-записью, т. к. оно необходимо для выписки сертификата Let's Encrypt).

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



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

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

Если VPN-соединение установлено, но не получается получить доступ к ресурсам локальной сети

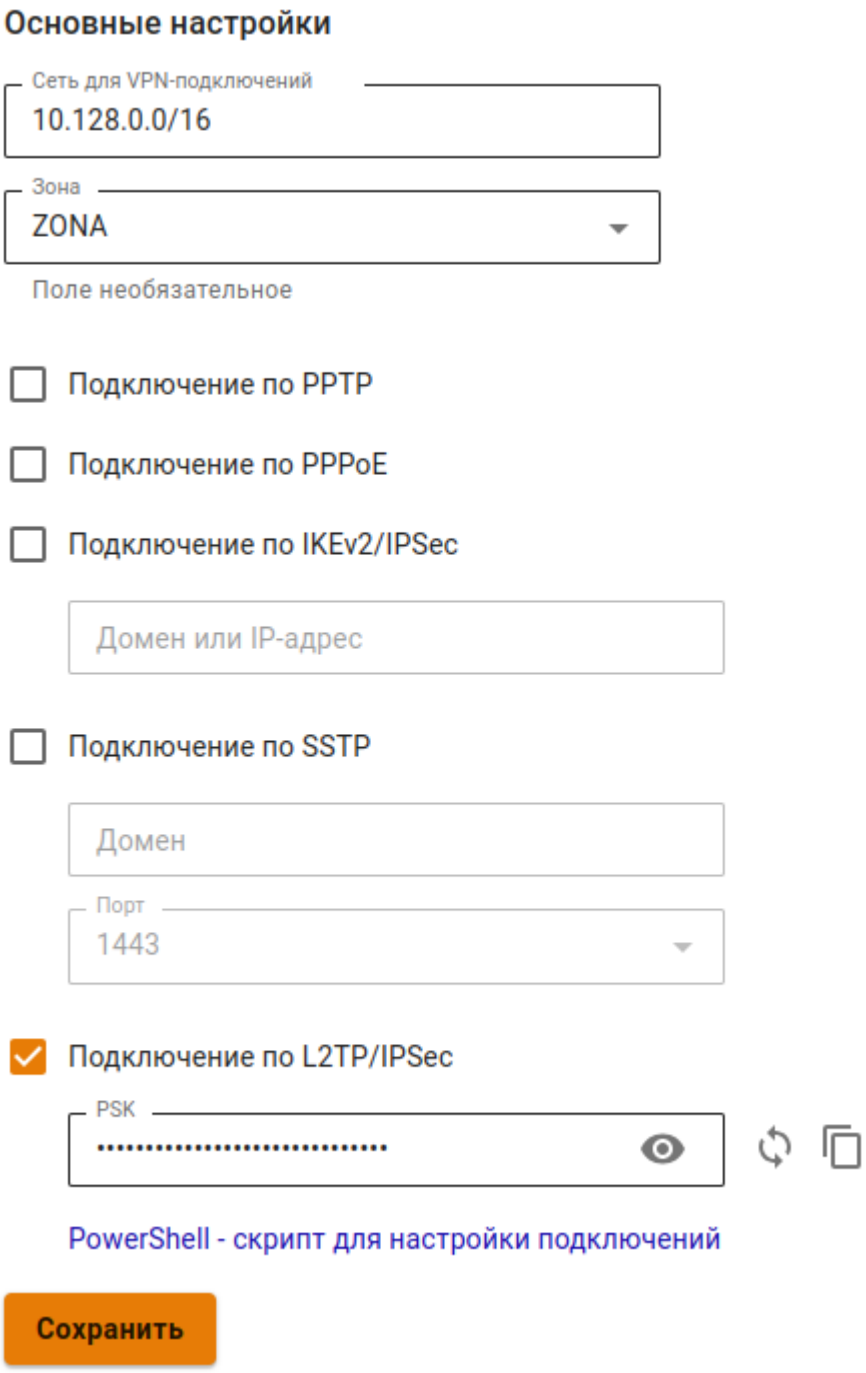
Выполните рекомендации статьи *Особенности маршрутизации и организации доступа*.

13.3.9 Подключение по L2TP/IPsec

Предупреждение: 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 IPsec-IKEv2. Все современные ОС поддерживают IKEv2, либо для них есть приложения.

Настройка глобальных параметров Ideco NGFW

1. Перейдите в раздел **Пользователи -> VPN-подключение -> Основное**.
2. Включите флаг **Подключение по L2TP/IPsec**.
3. Укажите секретную фразу (PSK-ключ).
4. Нажмите на кнопку **Сохранить**.



Настройка пользователей в Ideco NGFW

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

Разрешите пользователю подключения по VPN из сети интернет, создав в разделе **Пользователи -> VPN-подключения -> Доступ по VPN** правило, разрешающее пользователю VPN-подключение.

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

Предупреждение: L2TP IPsec клиенты, находящиеся за одним NAT'ом, могут испытывать проблемы подключения, если их больше одного. Решить проблему может помочь инструкция. Рекомендуем вместо L2TP IPsec использовать *IKEv2 IPsec*.

Если VPN-соединение установлено, но не получается получить доступ к ресурсам локальной сети

Выполните рекомендации статьи *Особенности маршрутизации и организации доступа*.

13.3.10 Личный кабинет пользователя

Основное

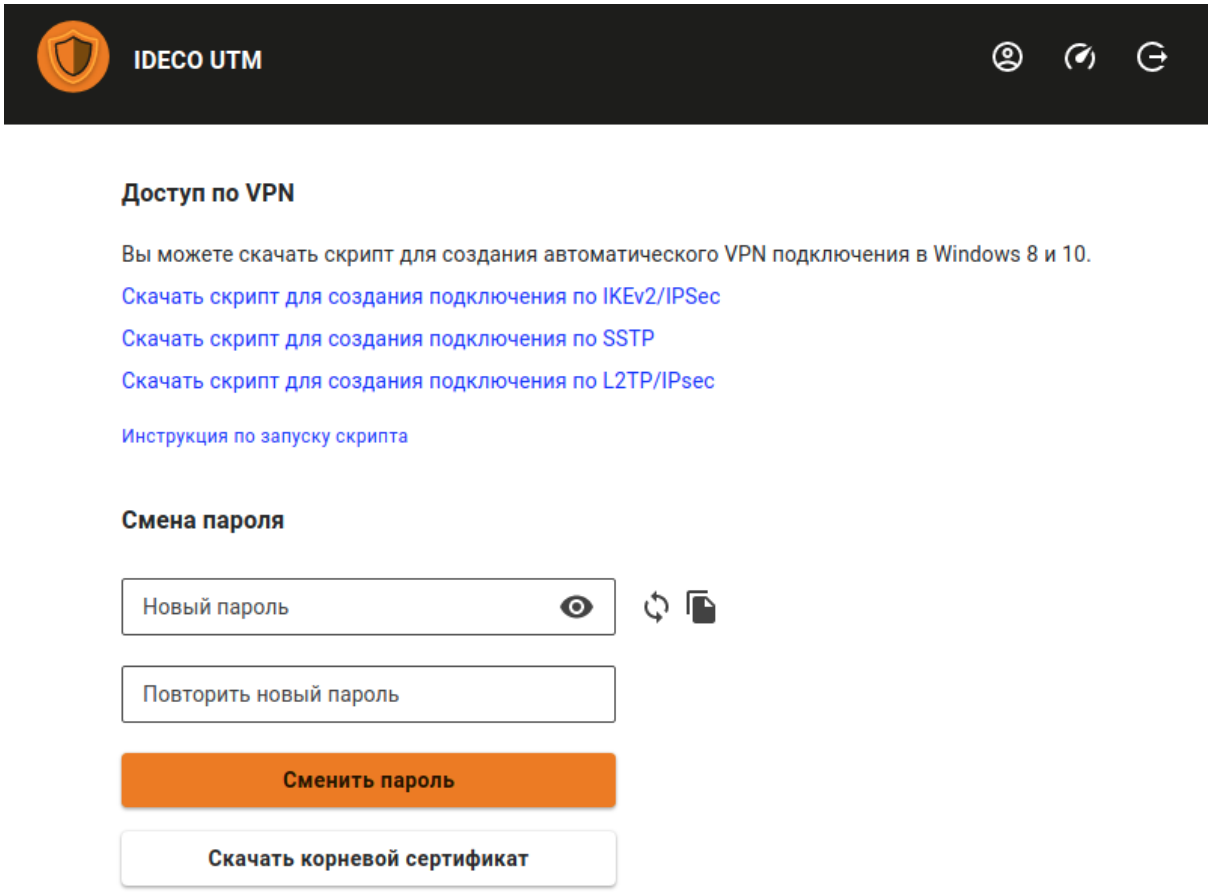
Для быстрой настройки пользовательских подключений включите доступ к веб-интерфейсу Ideco NGFW.

В личном кабинете, доступном по реквизитам учетных записей Ideco NGFW (локальных или доменных в случае *интеграции с Active Directory*) пользователи смогут скачать готовые PowerShell-скрипты для создания пользовательских подключений и ссылку на инструкцию по настройке VPN и запуску скриптов.

Включить доступ из сети интернет к личному кабинету и веб-интерфейсу администрирования Ideco NGFW можно в разделе **Управление сервером -> Администраторы**, включив настройку **Доступ к веб-интерфейсу из внешней сети**. После включения параметра личный кабинет и веб-интерфейс администрирования будут доступны по IP-адресу внешнего интерфейса Ideco NGFW.

Подсказка: Если внешний IP-адрес Ideco NGFW не входит в «белые» сети, то нужно пробросить порт 8443 на вышестоящем устройстве.

При входе под учетной записью пользователей (в том числе импортированных из Active Directory) они получат возможность скачать скрипты создания VPN-подключений и ссылку на инструкцию по их выполнению.



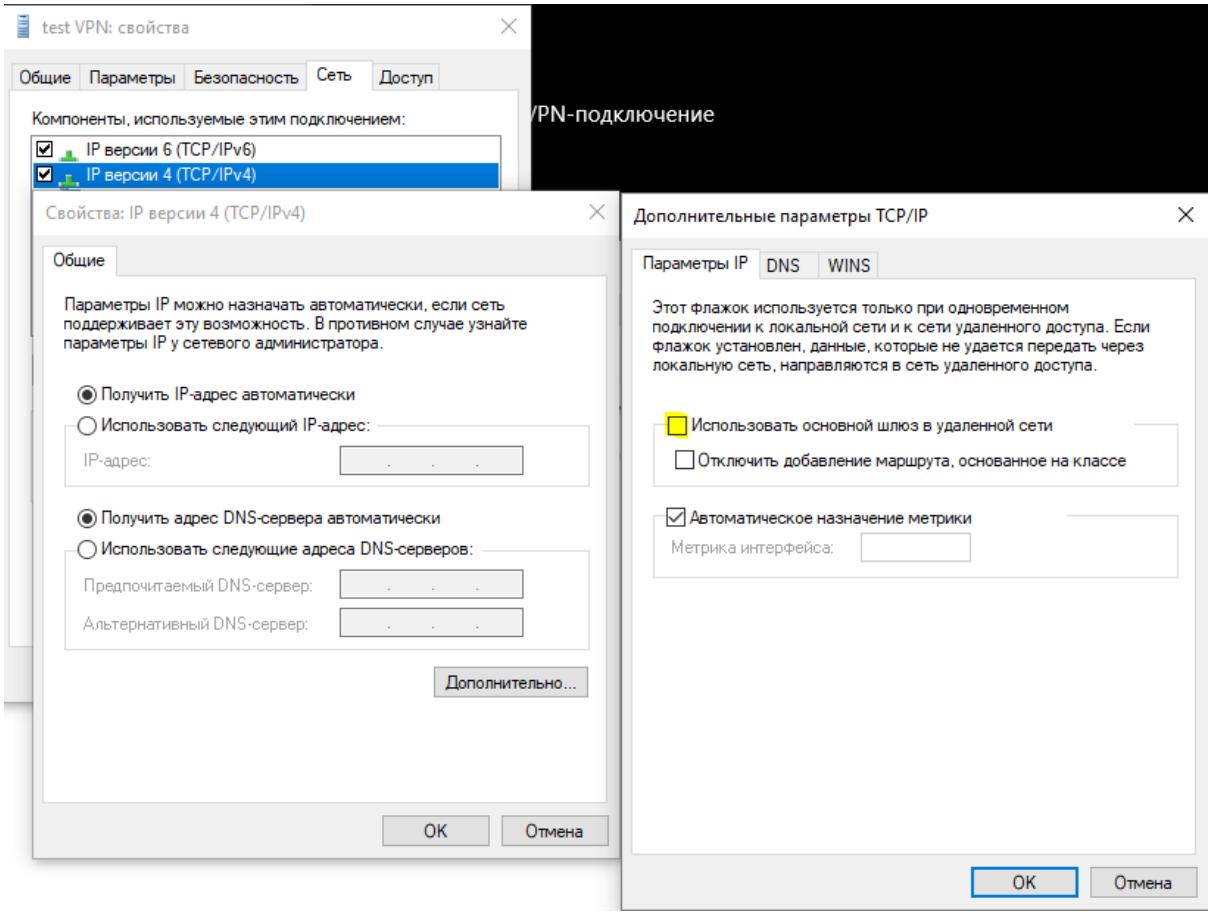
Также они получат возможность удаленного администрирования сервера Ideco NGFW.

13.3.11 Особенности маршрутизации и организации доступа

Если по VPN необходим доступ только к ресурсам локальной сети

В случае, если в интернет необходимо выходить напрямую через своего провайдера, а через VPN получать доступ только к ресурсам корпоративной сети на компьютерах, подключающихся по VPN, необходимо выполнить следующие настройки:

- В свойствах VPN-подключения убрать флаг **Использовать основной шлюз в удаленной сети**. Вкладка **Сеть -> IP версии 4 -> Дополнительно -> Параметры IP**:



- Прописать маршрут до корпоративной сети (**в Windows 8, 8.1, 10 автоматически будет создан маршрут, основанный на классе, в зависимости от адреса, который получит подключение по VPN. Например, маршрут будет добавлен для сети 10.0.0.0/8, если по VPN сервер получит адрес из сети 10.128.0.0/16**). Для IPsec-IKEv2 можно настроить автоматическое получение маршрута;

  Пример маршрута, если корпоративная сеть - `172.16.0.0/16`, а сеть для VPN-подключений, настроенная на Ideco NGFW, - `10.128.0.0/16` (и из этой же сети выдается IP-адрес VPN-подключению), то маршрут будет таким: `route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1`

- В некоторых случаях маршрут может не работать, тогда есть пинг до защищенного 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. Итоговый маршрут будет таким:

  `route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn`,
  где **nn**-номер интерфейса VPN-подключения, посмотреть который можно при активном VPN-подключении в выводе в консоли команды route print раздел «Список интерфейсов».

Если не удается получить доступ к компьютерам в локальной сети Ideco NGFW

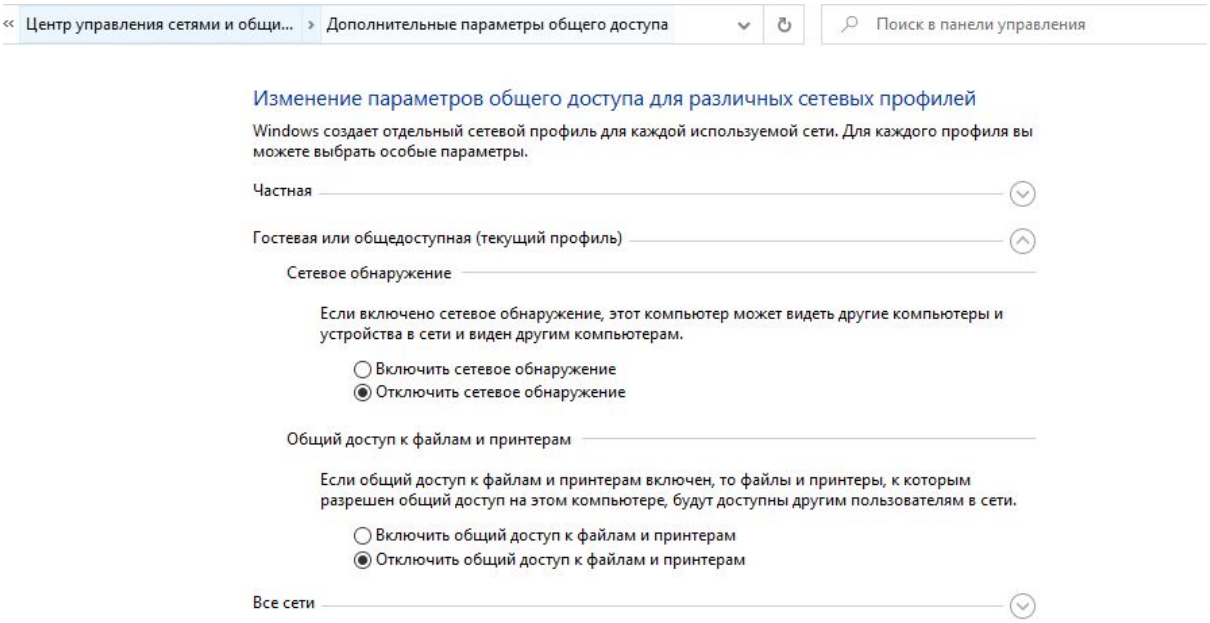
- Убедитесь, что локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. Если пересекается, то доступа к сети организации не будет (трафик по таблице маршрутизации пойдет в физический интерфейс, а не в VPN); **Адресацию необходимо менять.**

- На компьютерах локальной сети в качестве основного шлюза должен быть прописан Ideco NGFW. Если это не так, то необходимо прописать соответствующий маршрут на устройствах вручную, 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`
  где: `10.128.0.0/16` - адрес VPN-сети Ideco NGFW (настраивается в разделе **Пользователи -> VPN-**

подключения), а `10.1.1.1` - IP-адрес локального интерфейса Ideco NGFW.

- Проверьте настройки файрвола (**таблица FORWARD**) в Ideco NGFW на предмет запрещающих правил;
- Компьютеры и серверы на ОС Windows могут ограничивать доступ к сетевым папкам с помощью правил настроек профилей сети (причем как на стороне подключающегося по VPN компьютера, так и на стороне компьютеров и серверов локальной сети):

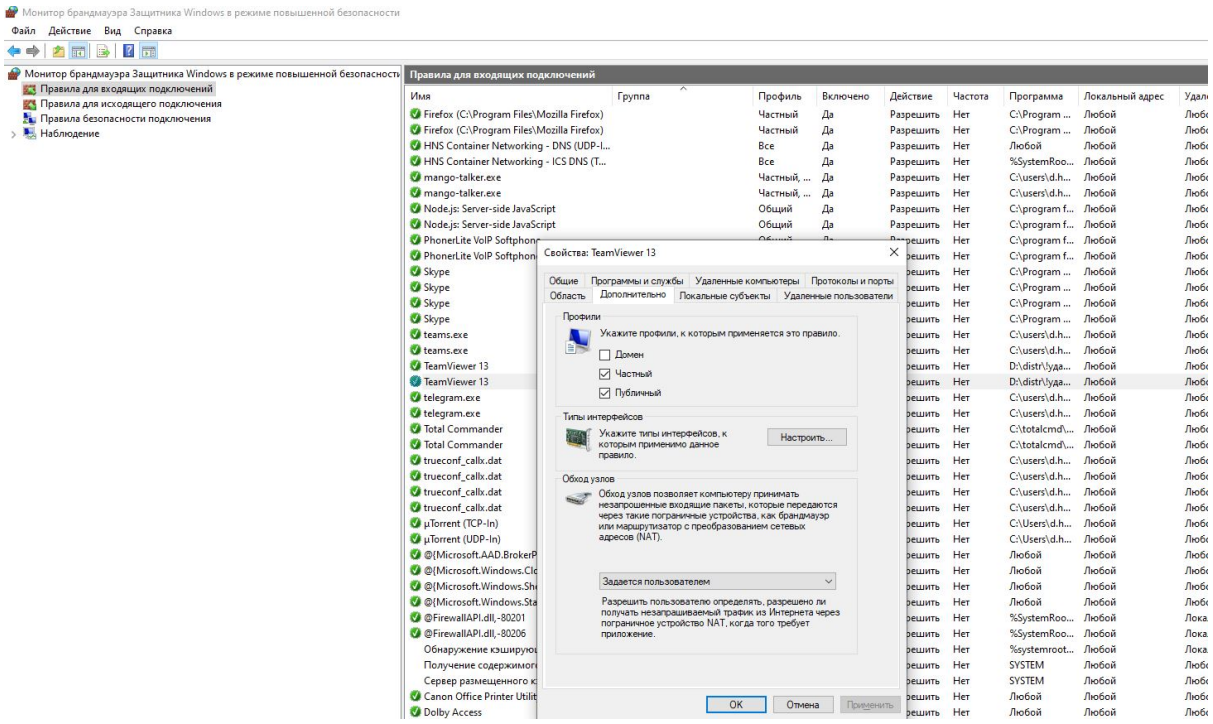


Включите доступ к файлам и принтерам для профиля «Все сети» и «Частных сетей».

Сделайте это с помощью PowerShell (запущенного с повышением прав до администратора), выполнив команду: `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`.

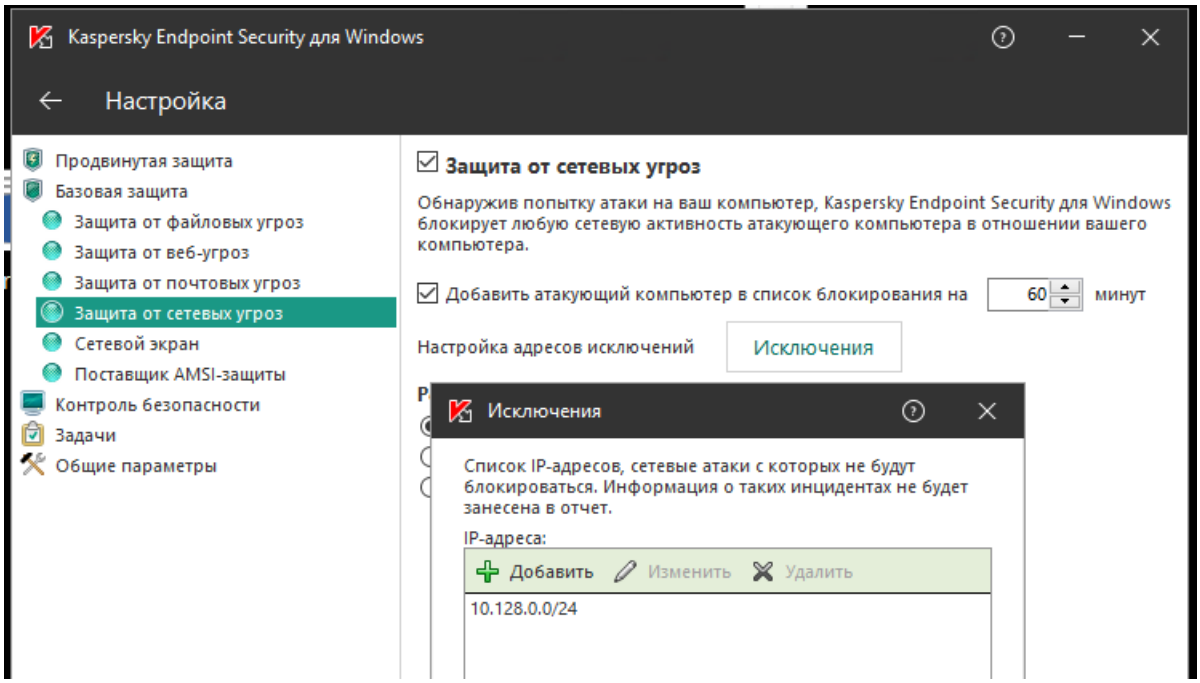
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей;

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



- Антивирусное ПО на компьютере может блокировать доступ к нему из не локальных 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:

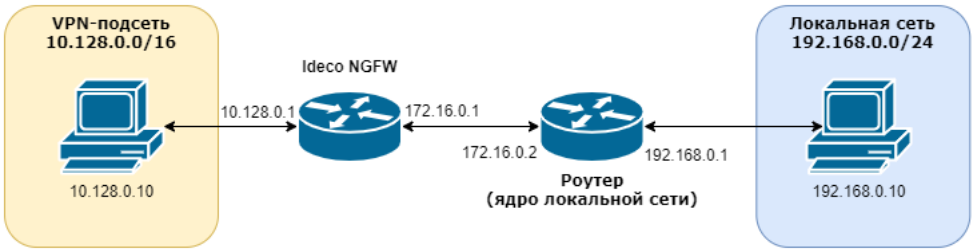


Если нет доступа к локальной сети Филиала

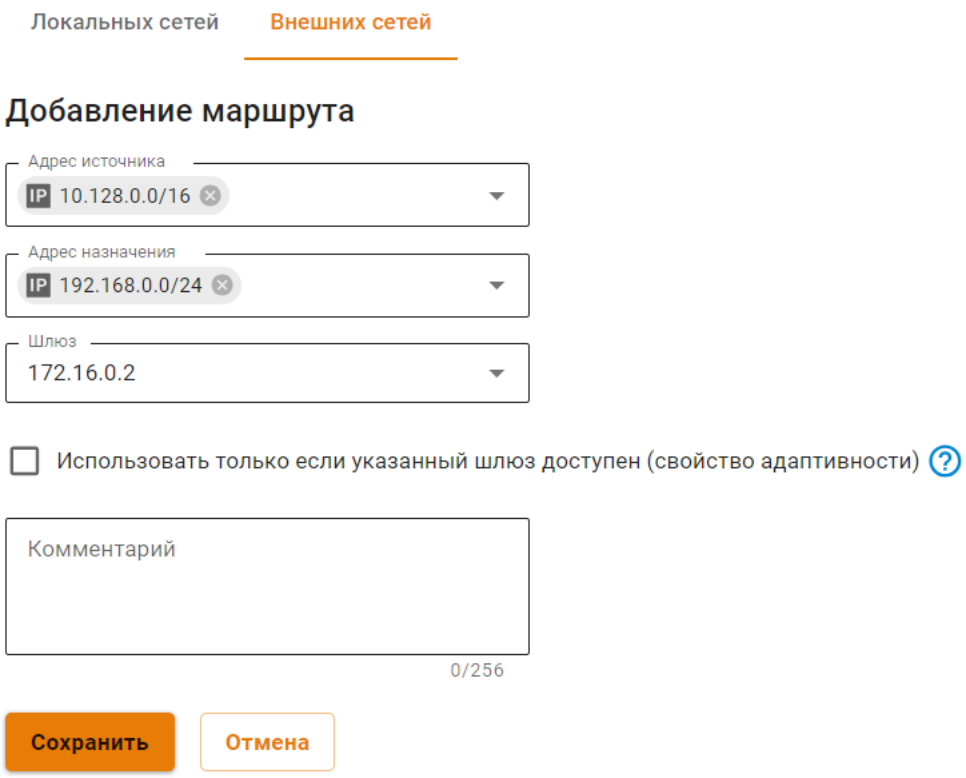
Если нет доступа к локальным сетям другого NGFW при подключении по VPN с основого NGFW (при подключении между двумя NGFW по IPSec):

- Убедитесь, что VPN-сети двух NGFW не пересекаются;
- Проверьте настройки основного NGFW, обратившись к *статье*.

Если за NGFW есть маршрутизатор, выступающий в качестве ядра локальной сети



Если между NGFW и хостами локальной сети в качестве ядра сети присутствует роутер, клиенты из VPN-сети не смогут получить доступ к хостам этой локальной сети, даже если на NGFW создано правило маршрутизации:



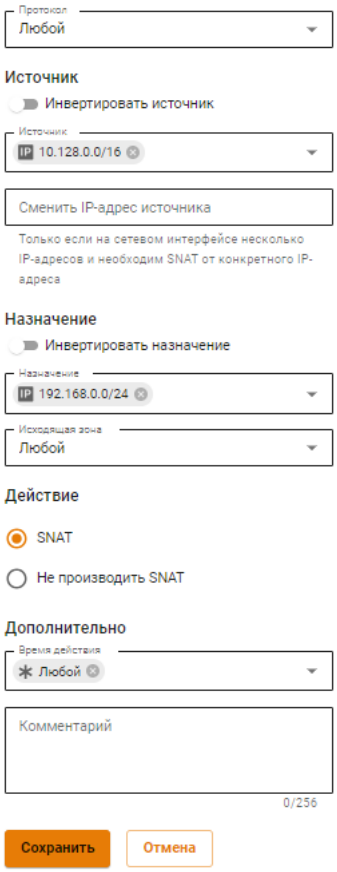
- `192.168.0.0/24` - сеть за роутером, к которой требуется получить доступ из VPN-сети;
- `172.16.0.2` - адрес роутера в локальной сети NGFW.

Причина в том, что хост (`192.168.0.10`) получает пакеты из VPN-сети с адресом источника `src 10.128.0.1`. Ответ с адресом назначения `dst 10.128.0.1` попадает на роутер, но у роутера отсутствует маршрут до указанной сети и трафик не проходит.

Чтобы обеспечить доступ, нужно настроить на роутере маршрут от нужной локальной сети до VPN-сети.

Для этого 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 вида:



Для этого:

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 **Сохранить**.

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.

Предупреждение: При этом у хостов из локальной сети `192.168.0.0/24` не будет доступа к VPN-сети `10.128.0.0\16`.

13.3.12 Инструкция по запуску PowerShell скриптов

Какой протокол VPN выбрать?

При нескольких вариантах подключений по VPN выбирайте протоколы по следующим критериям:

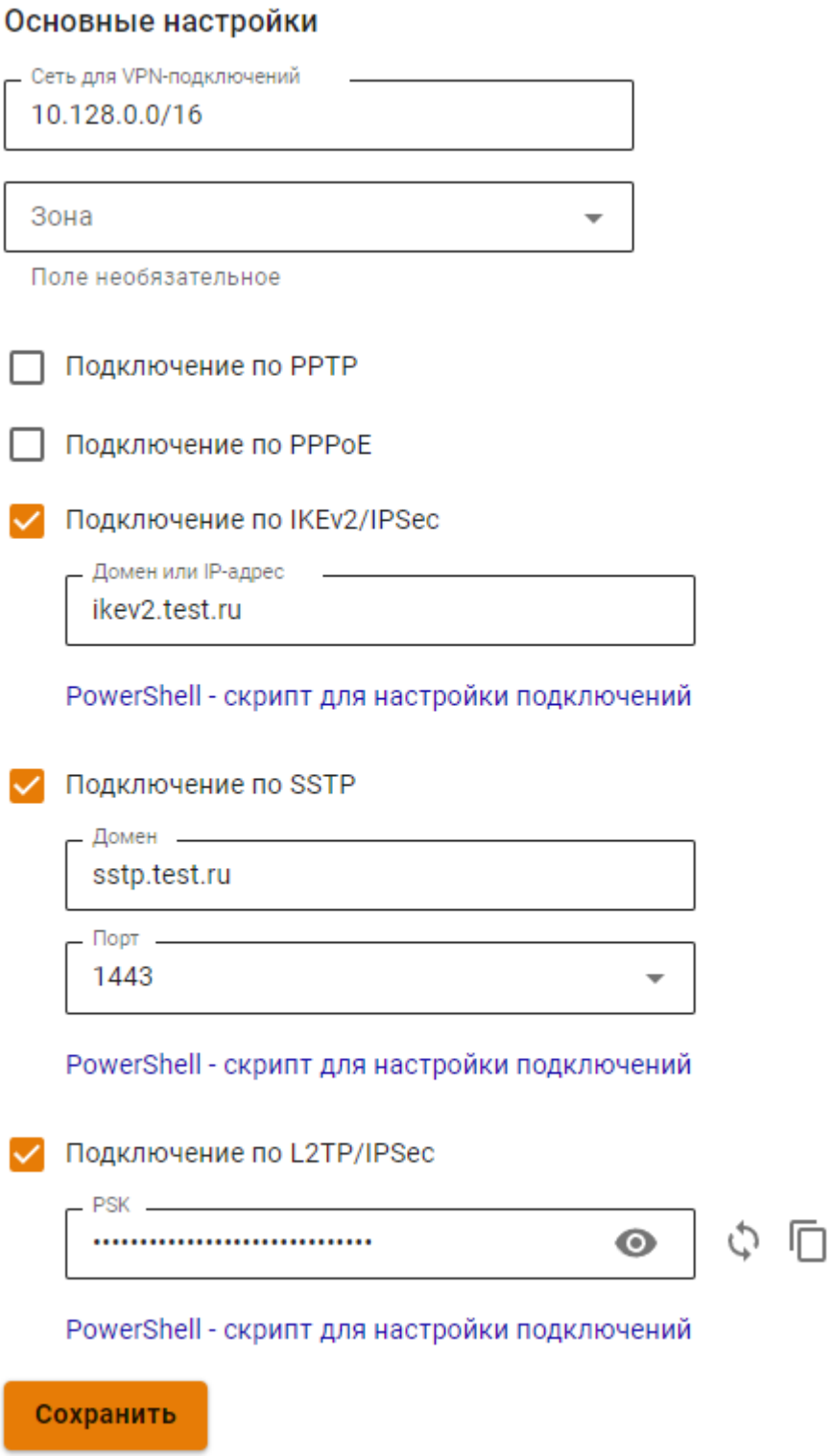
1. **IKEv2/IPsec** - лучший в плане производительности и надежности подключения протокол;
2. **SSTP** - протокол, основанный на TCP и SSL. Выберите его, если подключение по IKEv2 не проходит через провайдера;
3. **L2TP/IPsec** - надежный в плане шифрования, но не самый оптимальный в плане скорости и производительности протокол.

Как запустить PowerShell-скрипт?

1. Скачайте скрипт одним из вариантов:

Из Ideco NGFW:

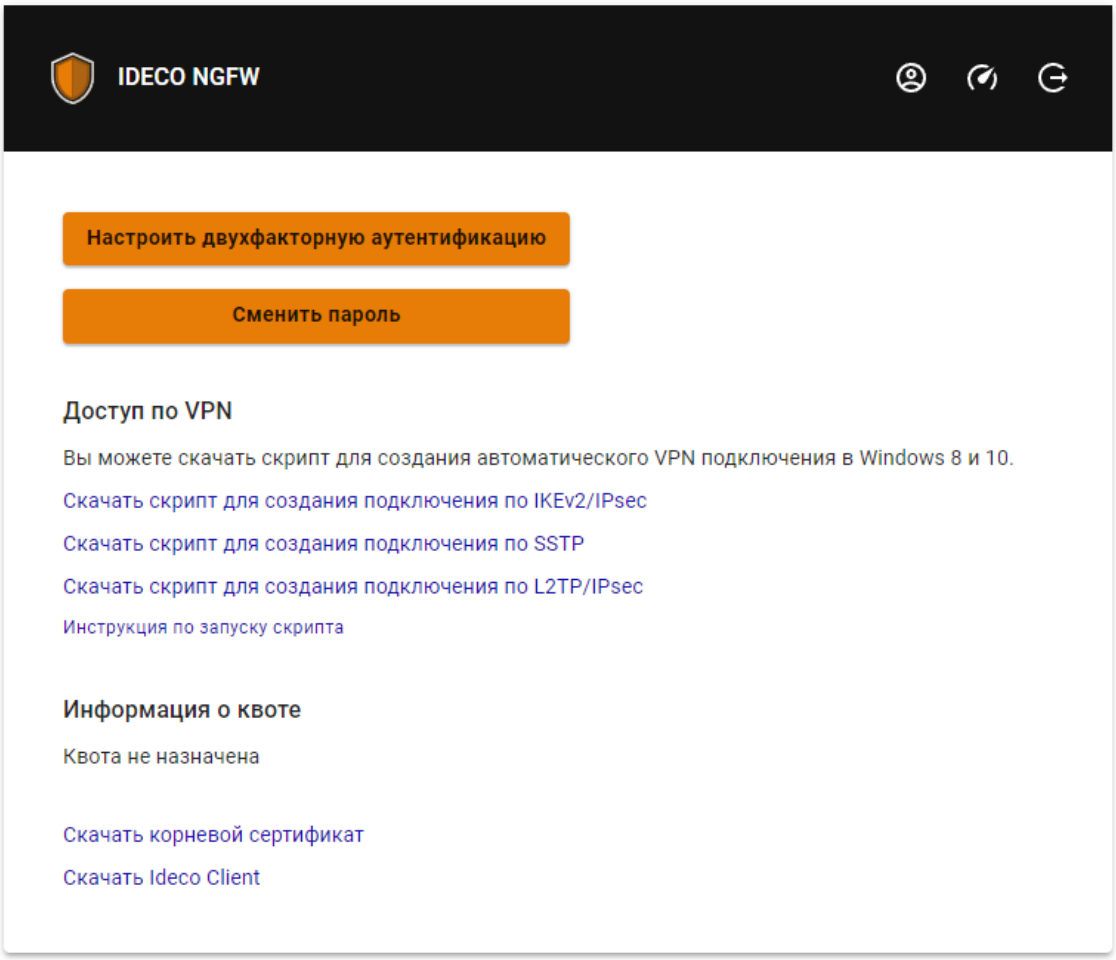
- Перейдите в раздел **Пользователи -> VPN-подключение -> Основное**;
- Установите флаг у требуемого протокола подключения, если требуется, заполните поля и нажмите **Сохранить**;
- Кликните по ссылке **PowerShell - скрипт для настройки подключений**:



- Перенесите скачанный файл на устройство, на котором требуется создать VPN-подключение.

В личном кабинете пользователя:

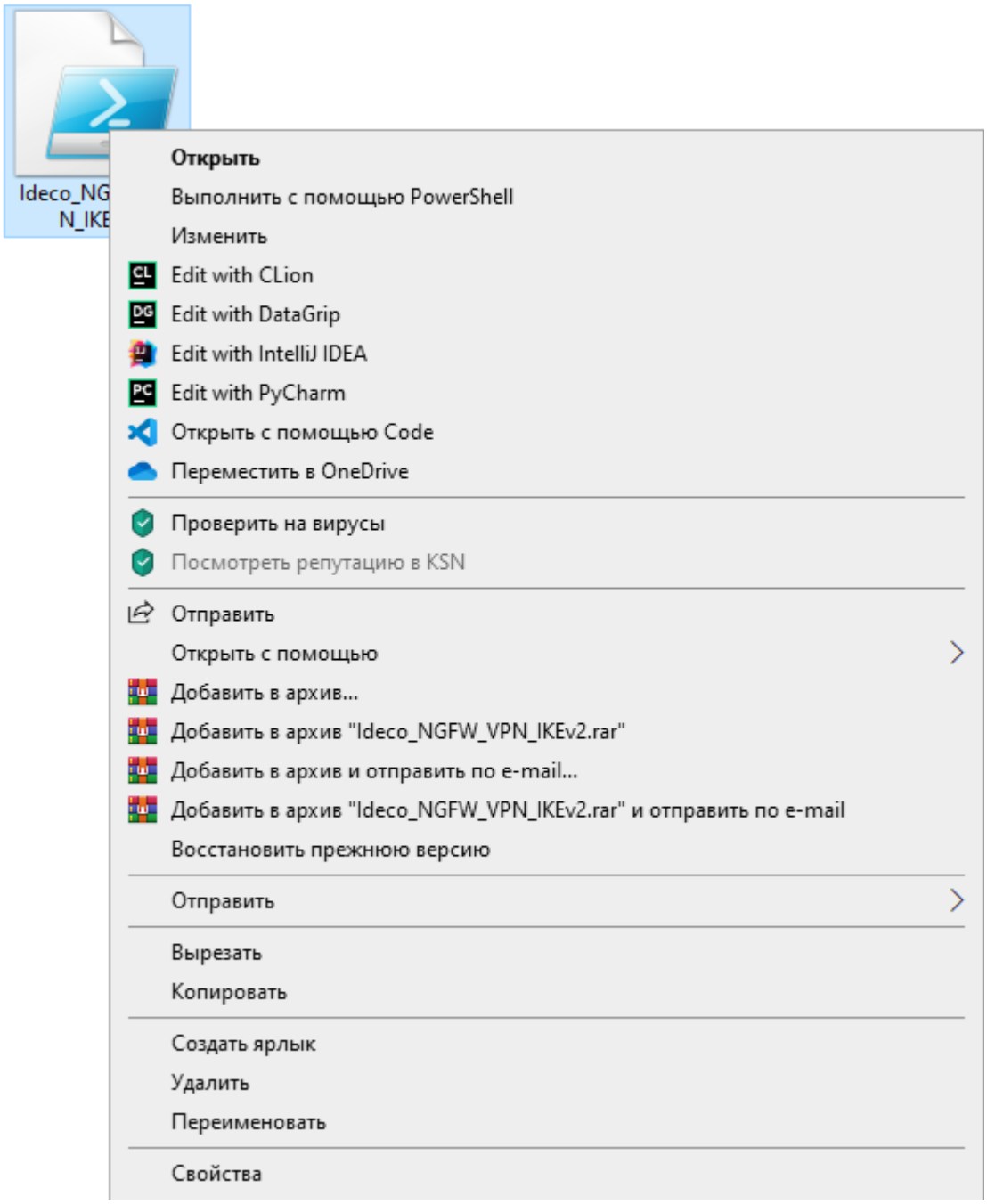
- Скачайте скрипт, кликнув по ссылке **Скачать скрипт для создания подключения**:



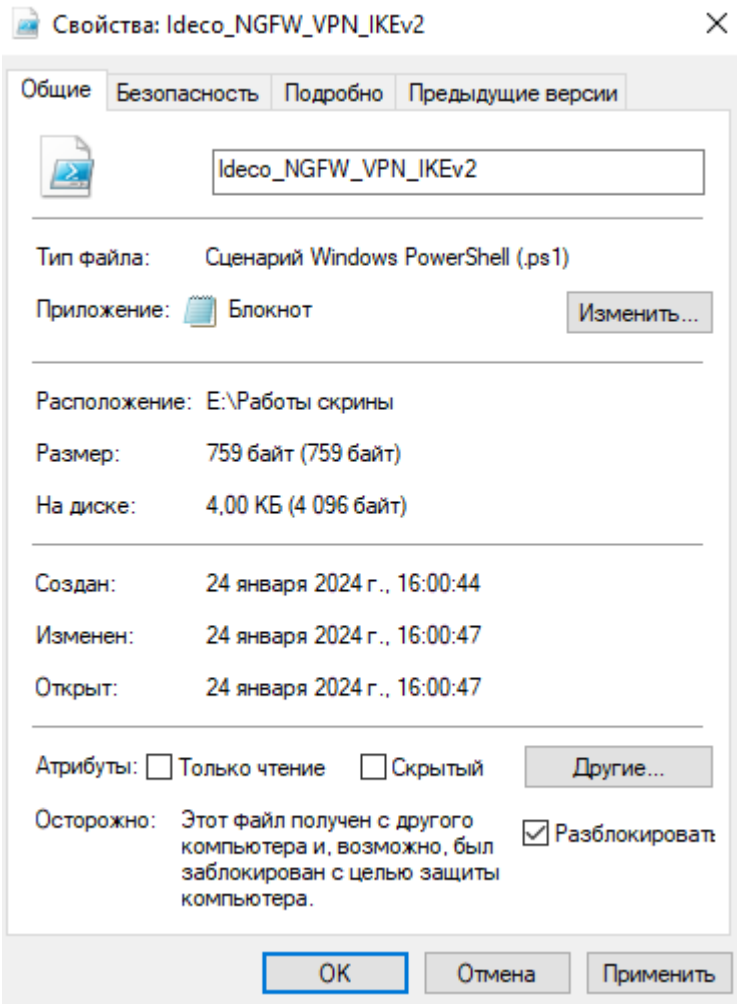
- Перейдите к выполнению пункта 2.

Предупреждение: 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*.

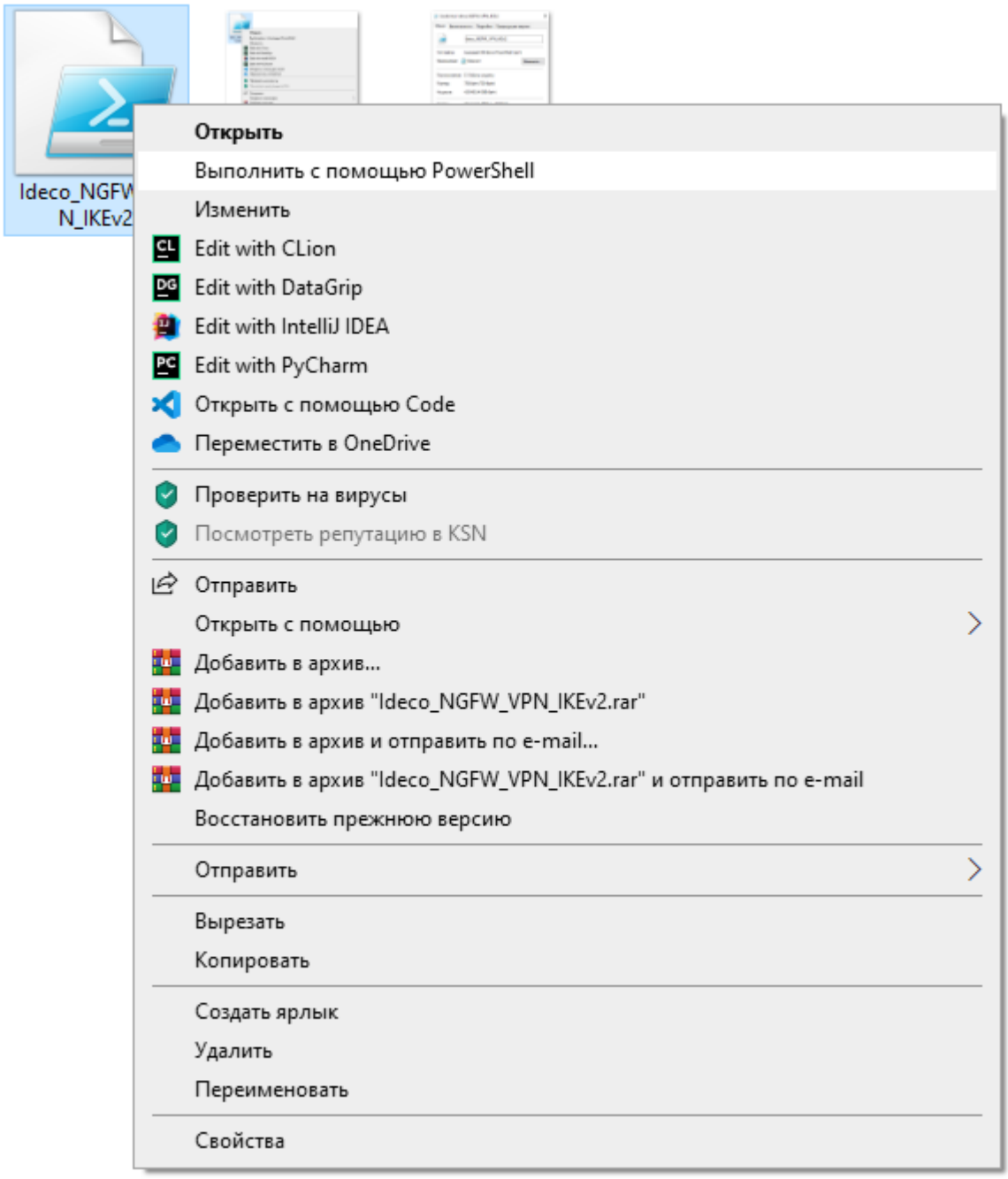
2. Щелкните правой кнопкой мыши по скачанному файлу и в контекстном меню выберите **Свойства**.



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



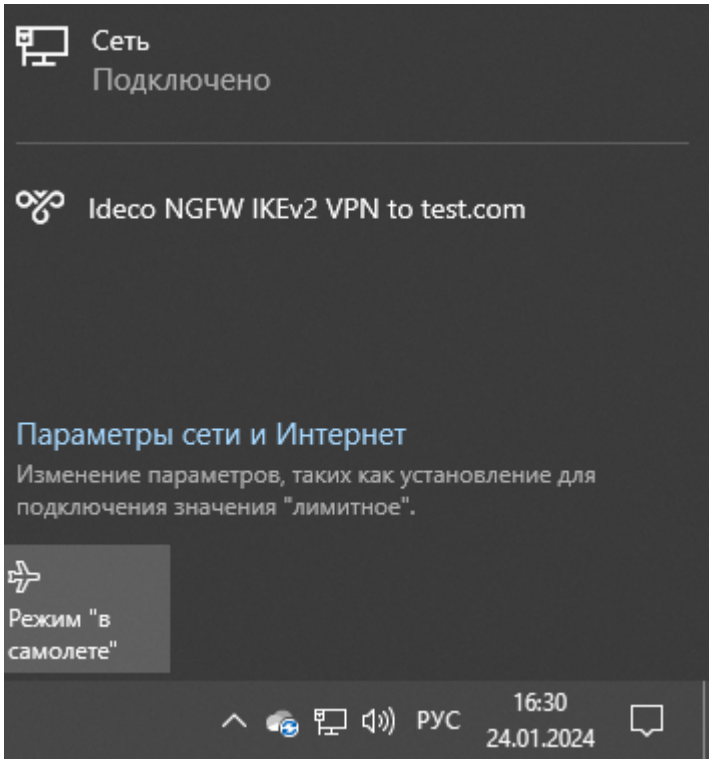
4. Нажмите правой кнопкой мыши на файл и выберите **Выполнить в PowerShell** в контекстном меню:



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. Ответьте **Да** на вопрос о внесении изменений в компьютер;

6. Подключение создано. Нажмите **Подключиться** в списке сетей.



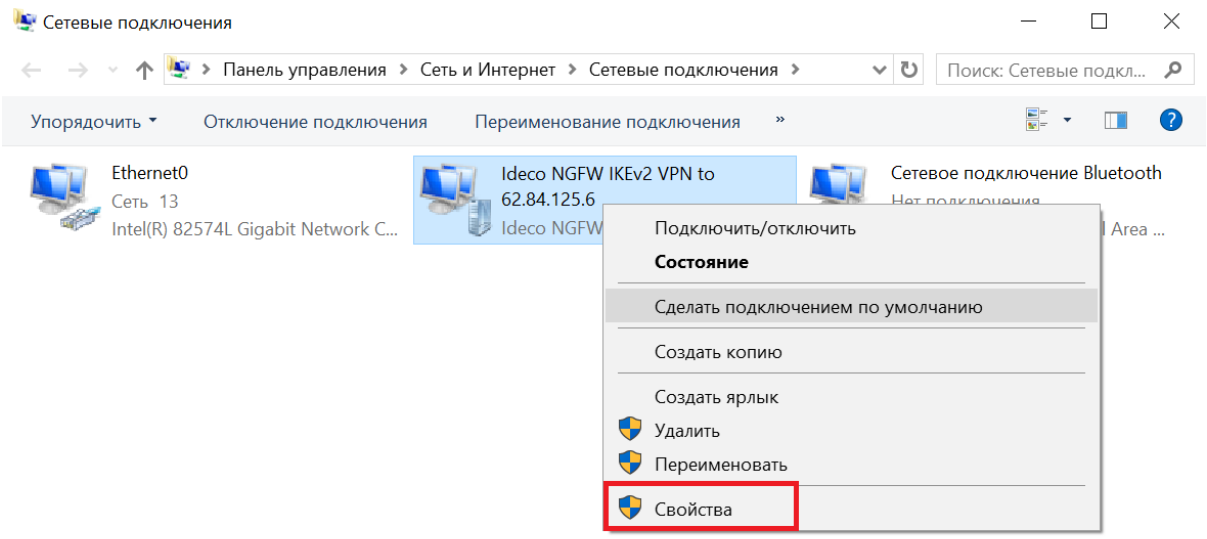
DNS-суффиксы для VPN-подключений

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.

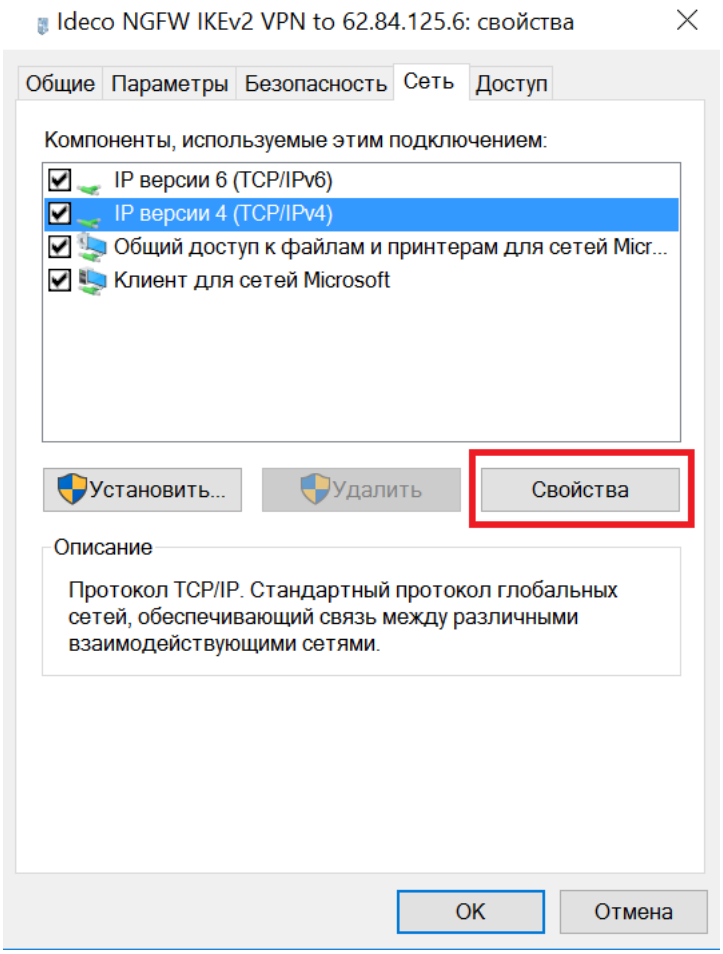
Предупреждение: Если Ideco NGFW введен в несколько доменов, то DNS-суффиксы в Powershell-скриптах не прописываются, их необходимо настраивать вручную на подключенном по VPN устройстве.

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

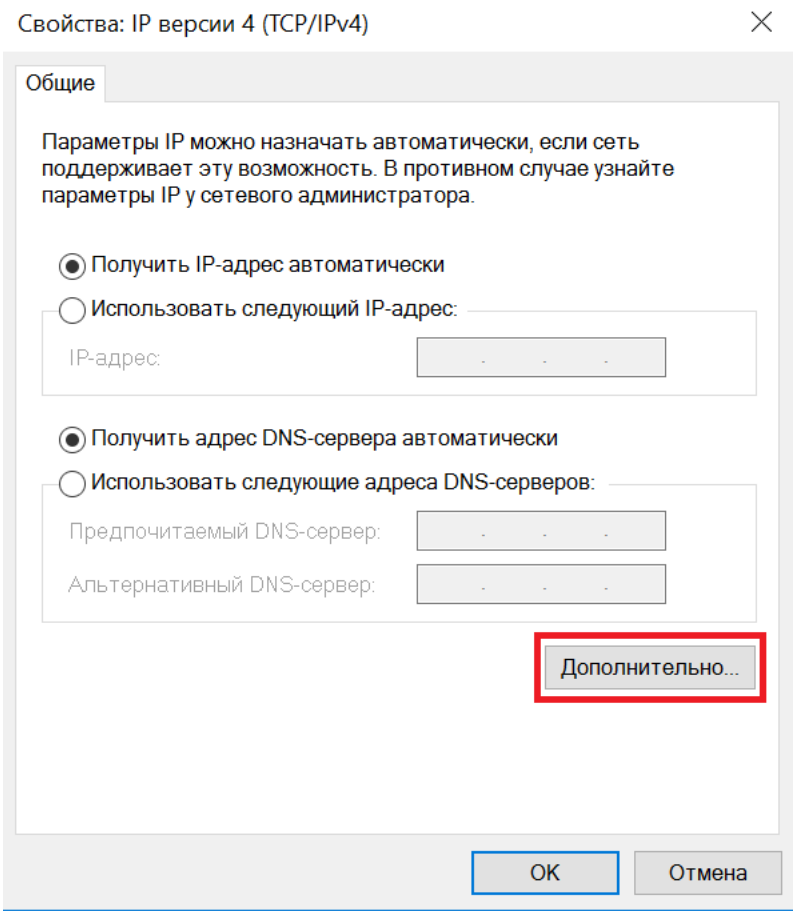
1. Перейдите в **Сетевые подключения**, нажмите правой кнопкой мыши по нужному VPN-подключению и выберите **Свойства**:



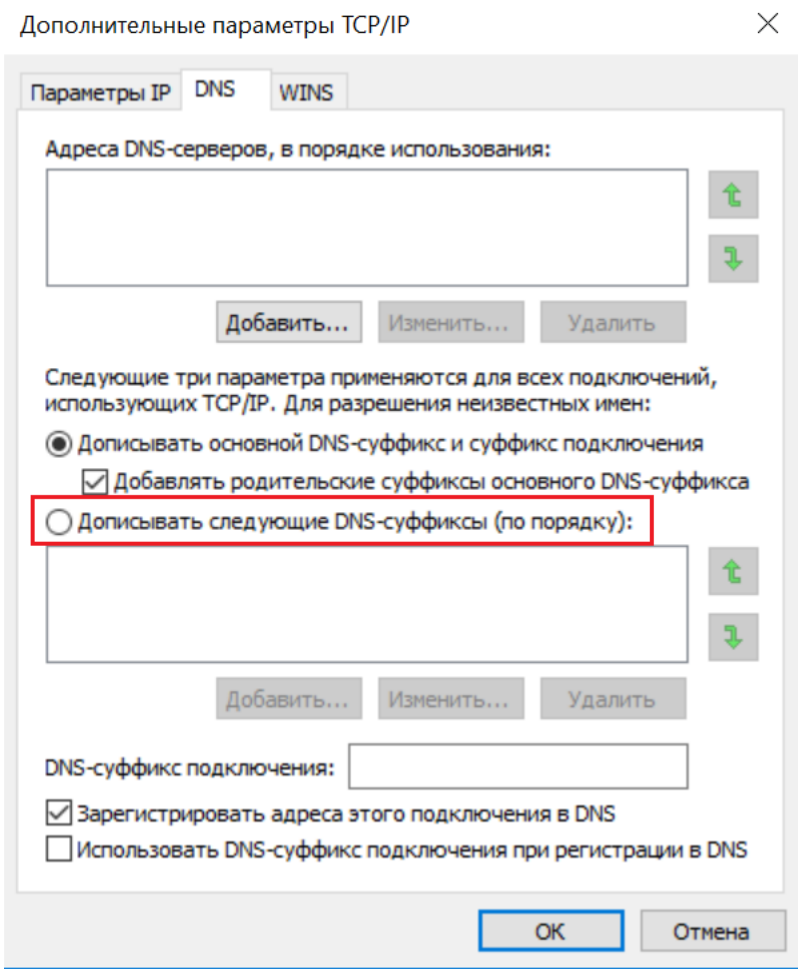
2. В открывшемся окне перейдите на вкладку **Сеть**, выберите компонент **IP версии 4 (TCP/IPv4)** и нажмите кнопку **Свойства**:



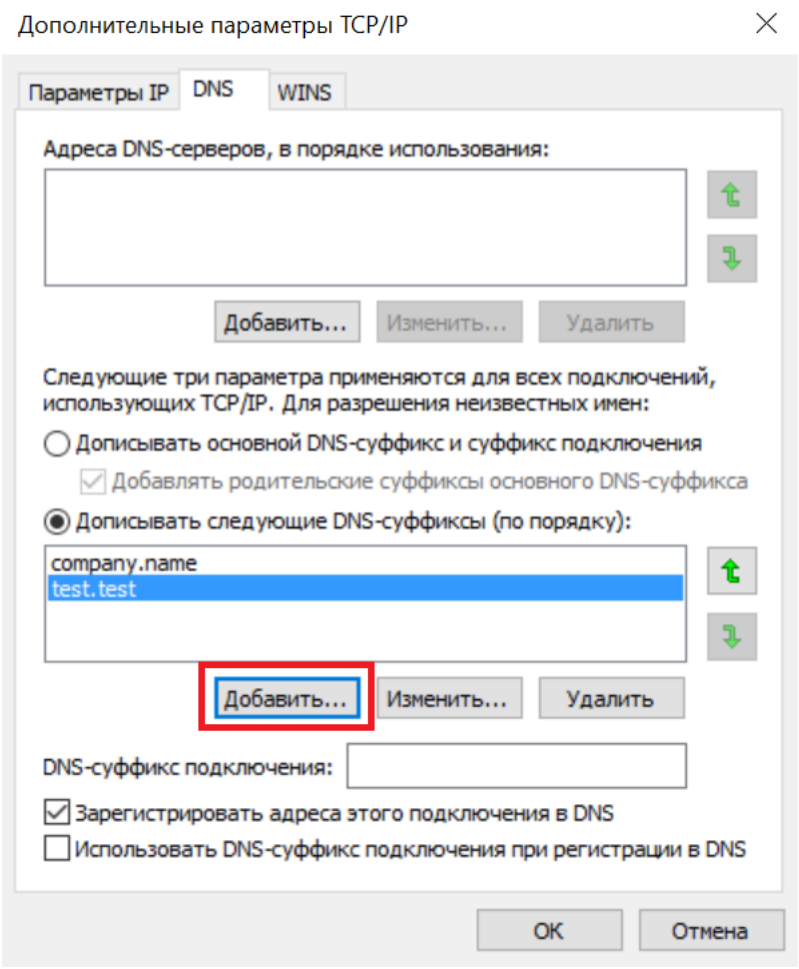
3. В открывшемся окне нажмите на кнопку **Дополнительно**:



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 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 *Как запустить Powershell скрипт*.
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.

1. После выполнения действий следуйте инструкции *Как запустить Powershell-скрипт* с 4 пункта.

Что делать, если запустить скрипт не получается?

Возможно не хватает прав на запуск скриптов или PowerShell не установлен в системе.

Воспользуйтесь инструкцией для создания подключения в *Windows 10* вручную.

13.4 Ideco Client

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

Использует протокол Wireguard.

> **Предупреждение:** Установить программу Ideco Client можно только на ОС семейства Windows с 10 версии и новее.

Ideco Client управляет авторизацией пользователей при подключении к Ideco NGFW в локальной сети и по VPN из внешних сетей.

Подсказка: Программа должна быть установлена на рабочей станции пользователя.

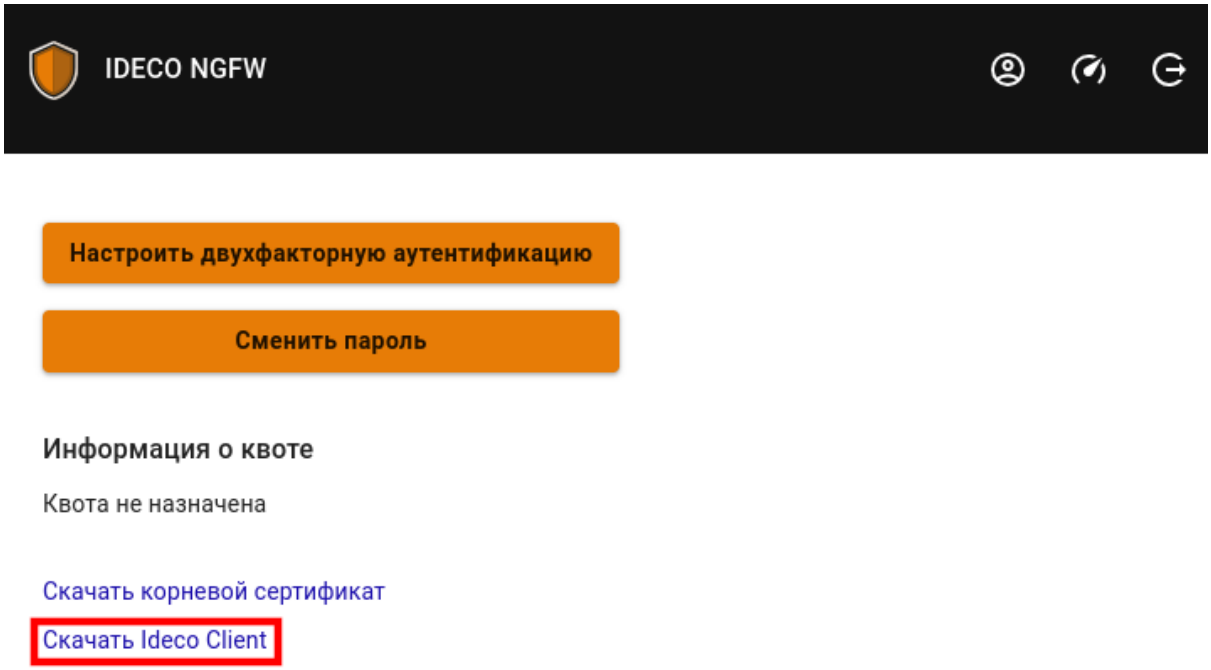
Порты для подключения, если NGFW за NAT:

- 80 TCP - для работы сертификатов let's encrypt;
- 14765 TCP и 3051 UDP - для работы Ideco Client.

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

13.4.1 Установка Ideco Client

- Перейдите в раздел **Пользователи –> Ideco-Client**, переведите опцию **Ideco Client** в положение включен, введите доменное имя в соответствующей строке и нажмите **Сохранить**. Появится кнопка **Скачать Ideco Client**:
- В личном кабинете пользователя по кнопке **Скачать Ideco VPN-клиент для Windows** или **Скачать Ideco Client** для пользователя Active Directory:



Сохраните и запустите двойным кликом файл установки программы *IdecoAgent.msi*.

Если требуется заранее установить адрес подключения, запустите файл из командной строки с ключом `utm_address=имя_домена` (перейдите в директорию с файлом `cd [путь до файла]` и вызовите файл с ключом `IdecoAgent.msi utm_address=имя_домена`);

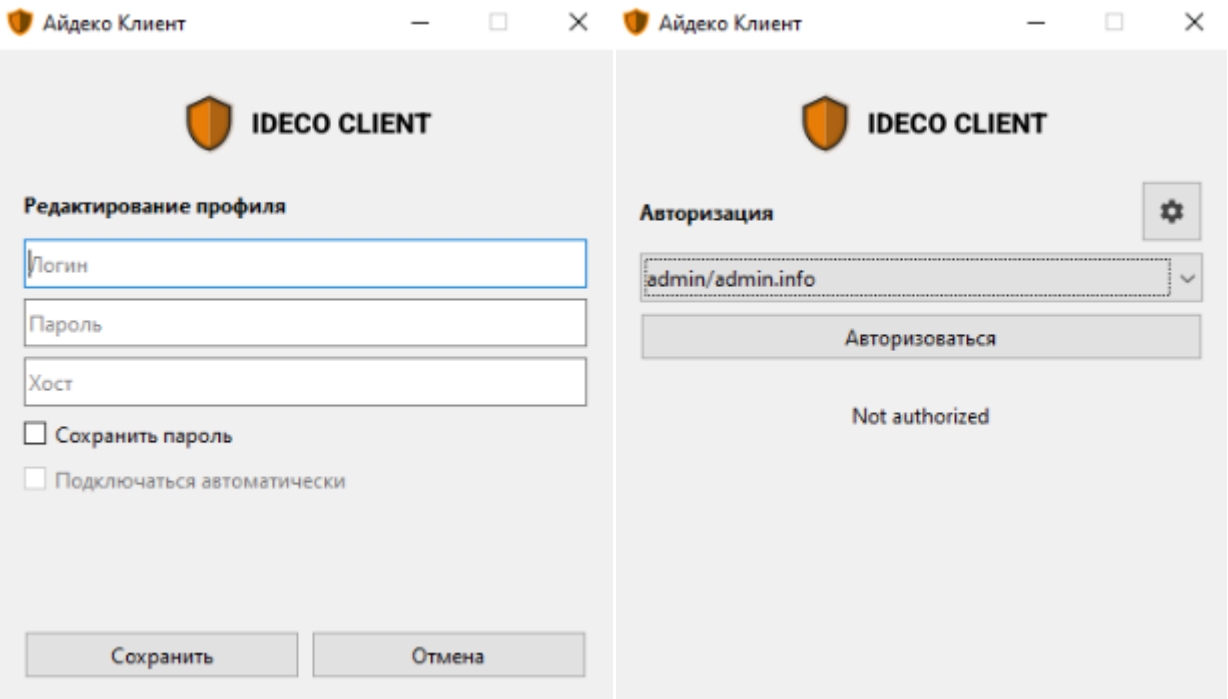
13.4.2 Настройка профиля для первого запуска

Предупреждение: 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:

- Дважды кликните на скачанный файл сертификата;
- В открывшемся окне выберите **Установить сертификат**;
- Откроется **Мастер импорта сертификатов. В качестве **Расположения хранилища** выберите **Локальный компьютер**;
- Выберите пункт **Поместить все сертификаты в следующее хранилище**, нажмите **Обзор** и выберите папку **Доверенные корневые центры сертификации**;
- Нажмите **Ок -> Далее -> Готово**.

1. После установки запустите Ideco Client. Программа установит связь с сервером и предложит ввести данные. Дальнейший формат ввода логина и хоста зависит от количества доменов, в которые введен NGFW:
2. Введите **логин** в домене, в качестве **хоста** укажите домен или IP-адрес.



3. Нажмите **Сохранить**, чтобы создать новый профиль пользователя для авторизации;
4. Для авторизации выберите профиль пользователя из выпадающего списка и нажмите **Авторизоваться**.

13.4.3 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**.

13.4.4 Особенности работы Ideco Client

- Опцией автоматического подключения может обладать только один профиль. При активации опции автоподключения другому профилю у предыдущего автоподключение будет отключено.
- Если компьютер уже находится в домене, то Client создаст для текущего пользователя SSO-профиль с включенным автоподключением. В ином случае нужно будет добавить стандартный профиль, воспользовавшись *инструкцией*;
- Ошибка с текстом **Неизвестная ошибка** возникает при попытке повторной авторизации уже авторизованного по IP пользователя;
- При обновлении запуск приложения Ideco Client необходимо выполнять вручную. С 18-й версии запуск осуществляется автоматически.

Подсказка: Чтобы исключить взаимодействие пользователя с приложением, нужно установить Client на доменный компьютер с ключом хоста NGFW. В этом случае авторизация для пользователей этого компьютера будет происходить через их SSO-профиль по умолчанию в «тихом» режиме автоподключения.

При подключении из локальной и внешней сети пользователи появятся в разделе *Авторизованные пользователи*.

13.5 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.

13.5.1 Поддерживаемые контроллеры домена:

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

Подсказка: При выходе из домена удаляются все пользователи и группы, импортированные из него.

Внимание: Приостанавливается синхронизация с контроллером домена, если локальные пользователи Ideco NGFW находятся в группах AD.
Для возобновления синхронизации вынесите локальных пользователей из групп AD. Автоматическая синхронизация произойдет через 15 минут.

Если на контроллере домена отключить пользователя, который уже импортирован в группу AD, то после включения ему присвоится новый ID и ранее настроенные правила фильтрации перестанут работать.

13.5.2 Особенности использования интеграции с несколькими контроллерами домена

Ограничения при интеграции Ideco NGFW с несколькими контроллерами доменами:

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

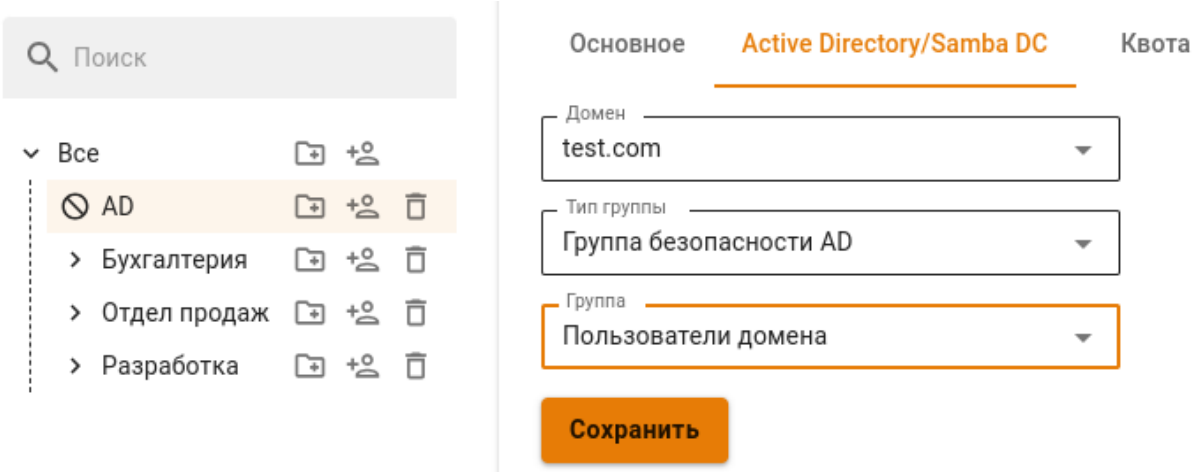
13.5.3 Настройка учетных записей и групп безопасности в качестве объектов правил фильтрации

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

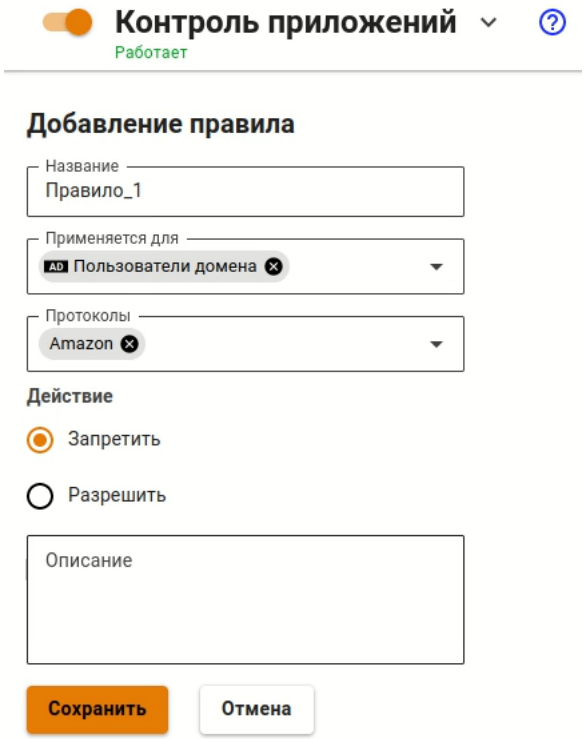
- *Файрвол*;
- *Контроль приложений*;
- *Ограничение скорости*;
- *Контент-фильтр*.

Пример настройки фильтрации при импорте из AD:

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 *Контроль приложений*:



3. Заполните требуемые поля и нажмите **Сохранить**.

13.5.4 Ввод сервера в домен

Подсказка: Перед вводом в домен убедитесь, что время на контроллере домена и Ideco NGFW совпадает.

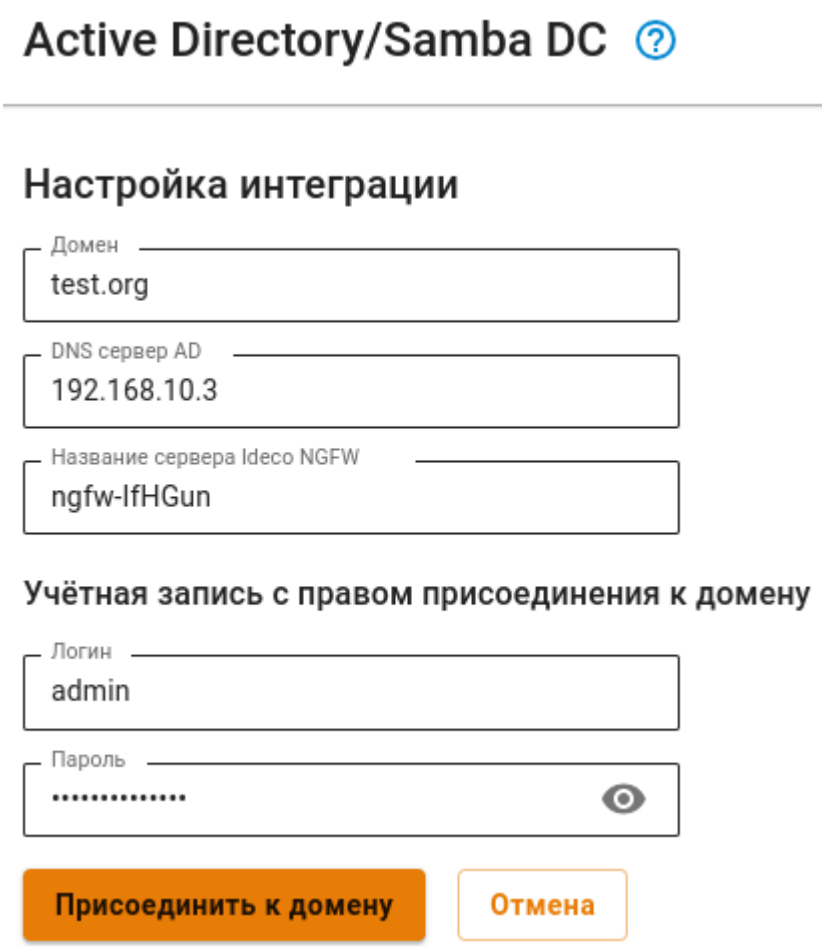
Для ввода сервера в домен следуйте пунктам:

1. Перейдите на вкладку **Пользователи -> Active Directory/Samba DC**.
2. Нажмите кнопку **Добавить**.
3. Заполните следующие поля:
    - **Имя домена**: введите полное наименование домена, длина которого не должна превышать 64 символа. Например: `mydomain.example`;
    - **DNS-сервер AD/Samba**: введите адрес сервера, обладающий ролью DNS-сервера в контроллере домена, доступный с локального интерфейса Ideco NGFW;
    - **Имя сервера Ideco NGFW**: введите имя компьютера, под которым Ideco NGFW будет введен в контроллер домена;
    - **Учетная запись с правом присоединения к домену**: введите учетную запись AD с правами присоединения к домену.

Подсказка: Данные учетной записи с правом присоединения к домену не сохраняются на сервере и используются один раз при вводе в домен.

Предупреждение: Хотя бы один контроллер домена должен находиться в локальной сети Ideco NGFW или быть доступен через локальный интерфейс с помощью настроенной маршрутизации.

Пример настройки интеграции:



Процесс присоединения к домену после нажатия одноименной кнопки может занять до одной минуты. Возможно присоединение сервера к нескольким доменам с некоторыми особенностями работы, описанными в *статье*.

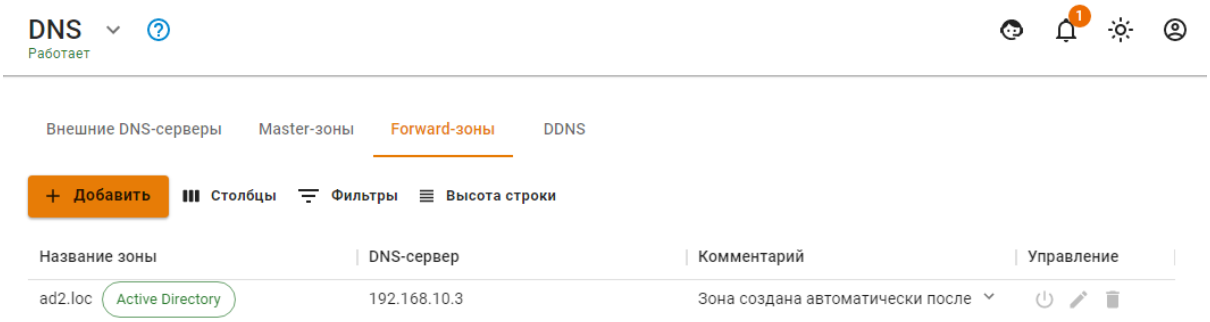
Подсказка: При выходе из домена удаляются все пользователи и группы, импортированные из него.

Настройка DNS для разрешения имен локального домена

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).

Подсказка: В Ideco NGFW Forward-зона DNS создается автоматически при вводе сервера в домен, и настраивать ее вручную нет необходимости. Создавайте ее вручную только, если по ошибке удалили данную зону из настроек DNS-сервера или если не получилось присоединить сервер к домену.



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.

13.5.5 Аутентификация пользователей AD/Samba DC

Внимание: Синхронизация с контроллером домена приостанавливается, если локальные пользователи Ideco NGFW находятся в группах AD.
Для возобновления синхронизации вынесите локальных пользователей из групп AD. Автоматическая синхронизация произойдет через 15 минут.

Настройка авторизации пользователей

Для пользователей, импортированных из Active Directory, доступны все типы авторизации.

Подсказка: Рекомендуется одновременно использовать оба типа авторизации.

Для пользователей, импортированных из Samba, доступны **все типы авторизации**, кроме **авторизации через журнал безопасности**.

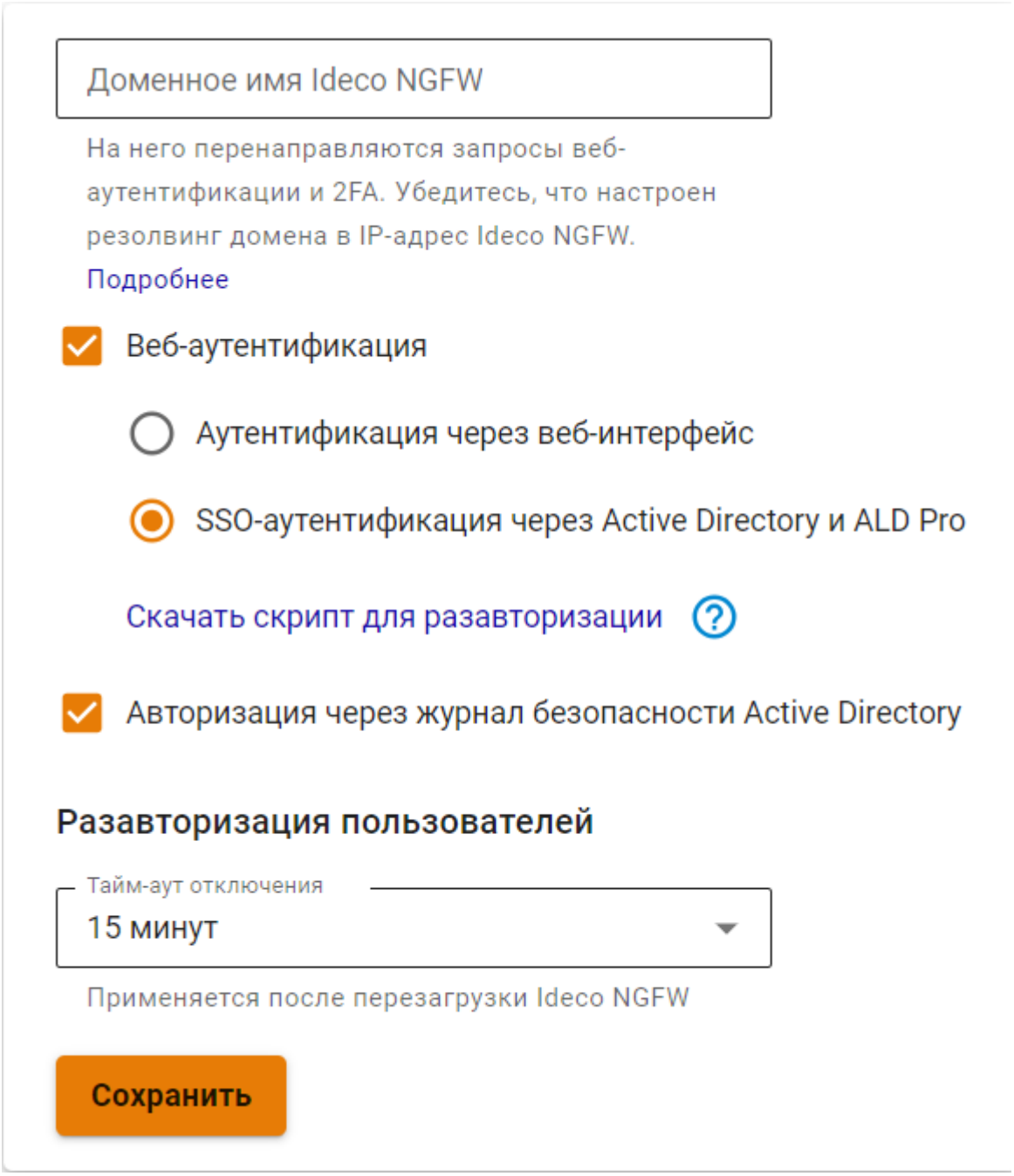
Подсказка: Если у домена, в который введен **NGFW**, настроено доверие с другим доменом, то пользователи доверенного домена смогут авторизоваться на **NGFW** при выполнении условий:

- 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

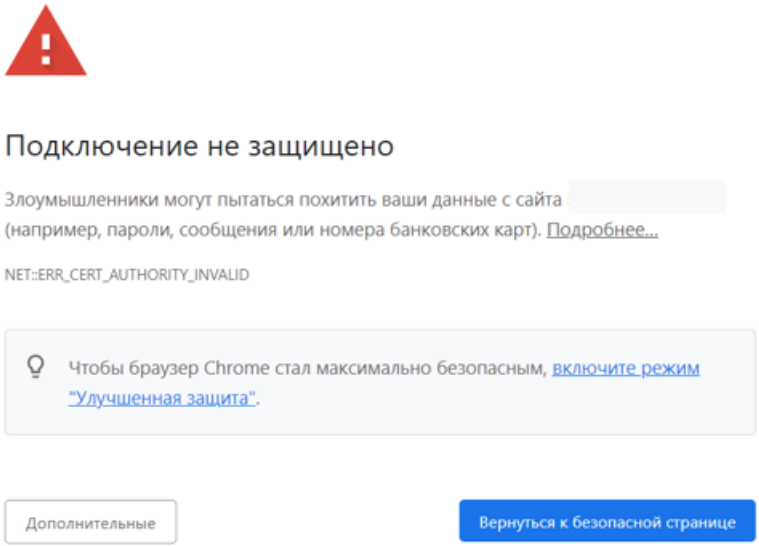
Для включения **SSO-аутентификации** и **Авторизации через журнал безопасности Active Directory** перейдите на вкладку **Пользователи -> Авторизация -> Основное** и заполните поля:



- 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

Авторизация через журнал безопасности 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.

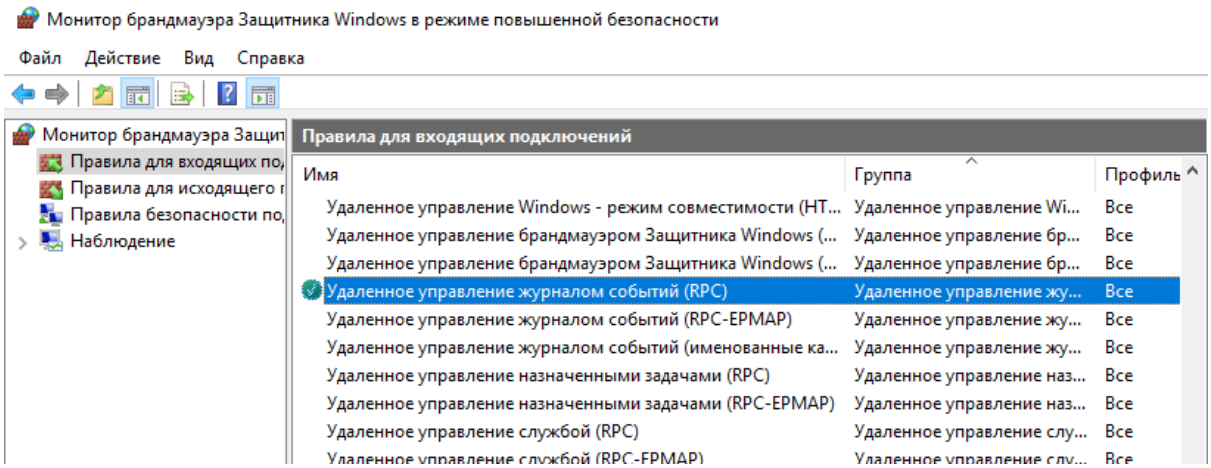
Подсказка: Особенности работы авторизации через журнал безопасности Active Directory:

- 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 аутентификациии пользователя перезагрузите службу `ideco-auth-backend`.

Используйте Ideco Client совместно с SSO-аутентификацией на Ideco NGFW.

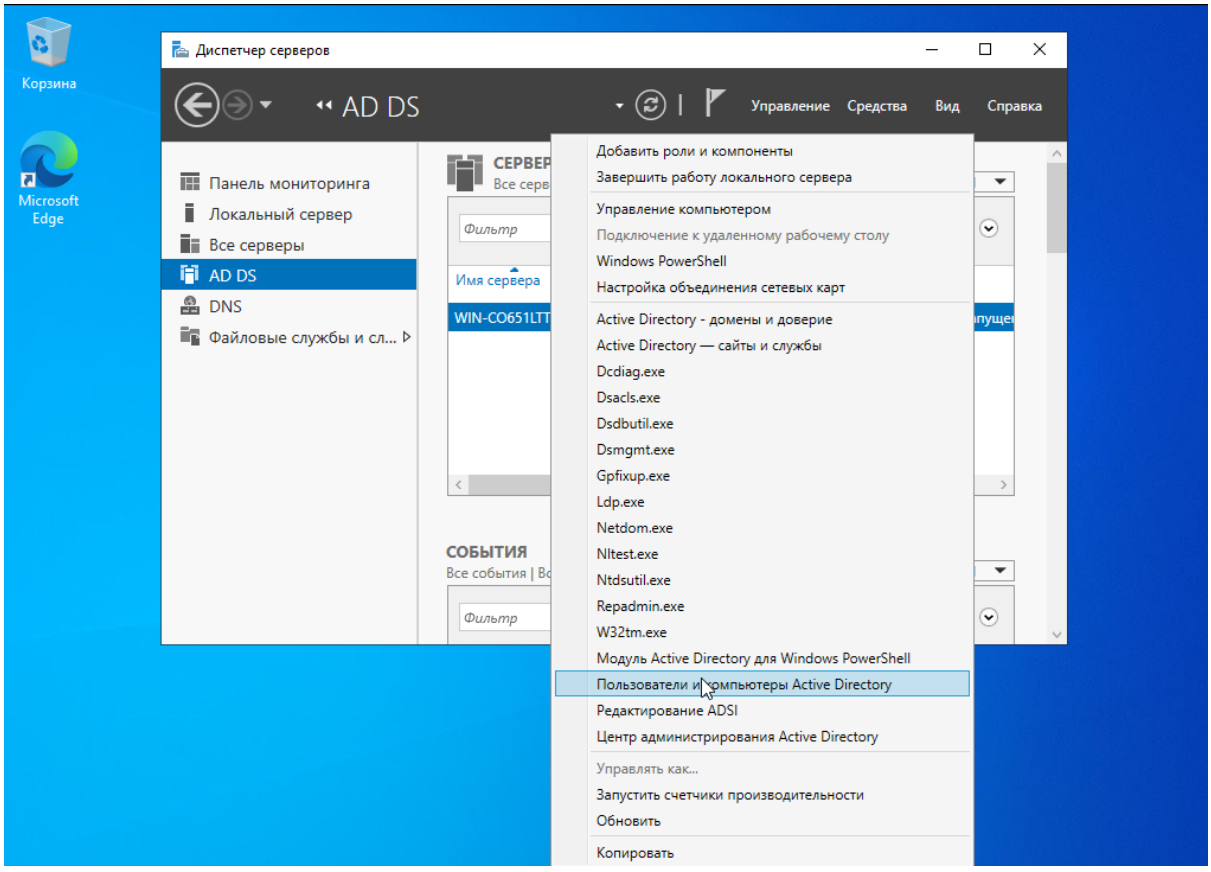
Для работы авторизации через журнал безопасности выполните настройку контроллера домена:

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

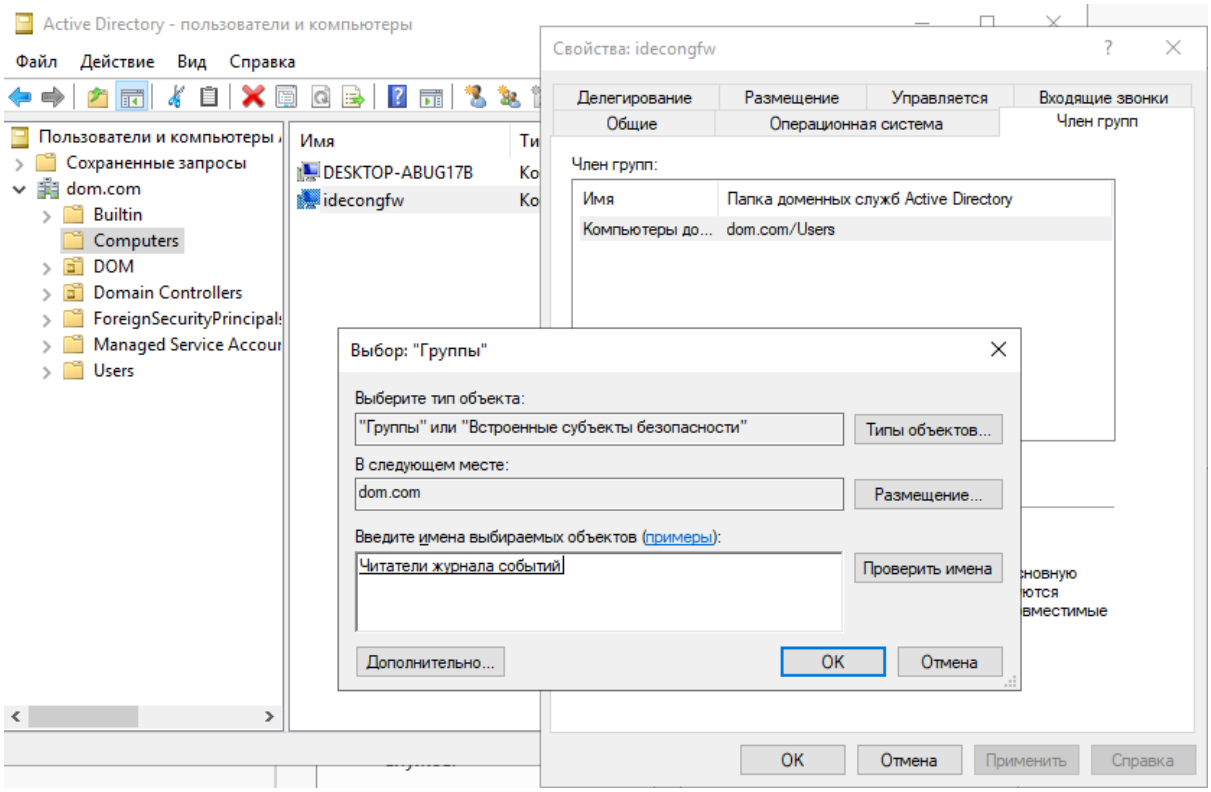


2. Добавьте Ideco NGFW в группу безопасности **Читатели журнала событий (Event Log Readers)**.

Для этого 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**:



Зайдите в **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. Отключите эту настройку и заново включите.

При изменении стандартной политики безопасности контроллеров домена выполните действия:

Англоязычная версия:

1. Откройте **Group policy management**.

2. Выберите **Forest: test.org -> Domains -> test.org**.

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: test.org -> Домены -> test.org**.

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 контроллеров доменов выполните `gpupdate /force`;
Если авторизация пользователей при логине не происходит, нужно проверить в журнале безопасности наличие событий 4768, 4769, 4624.

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.

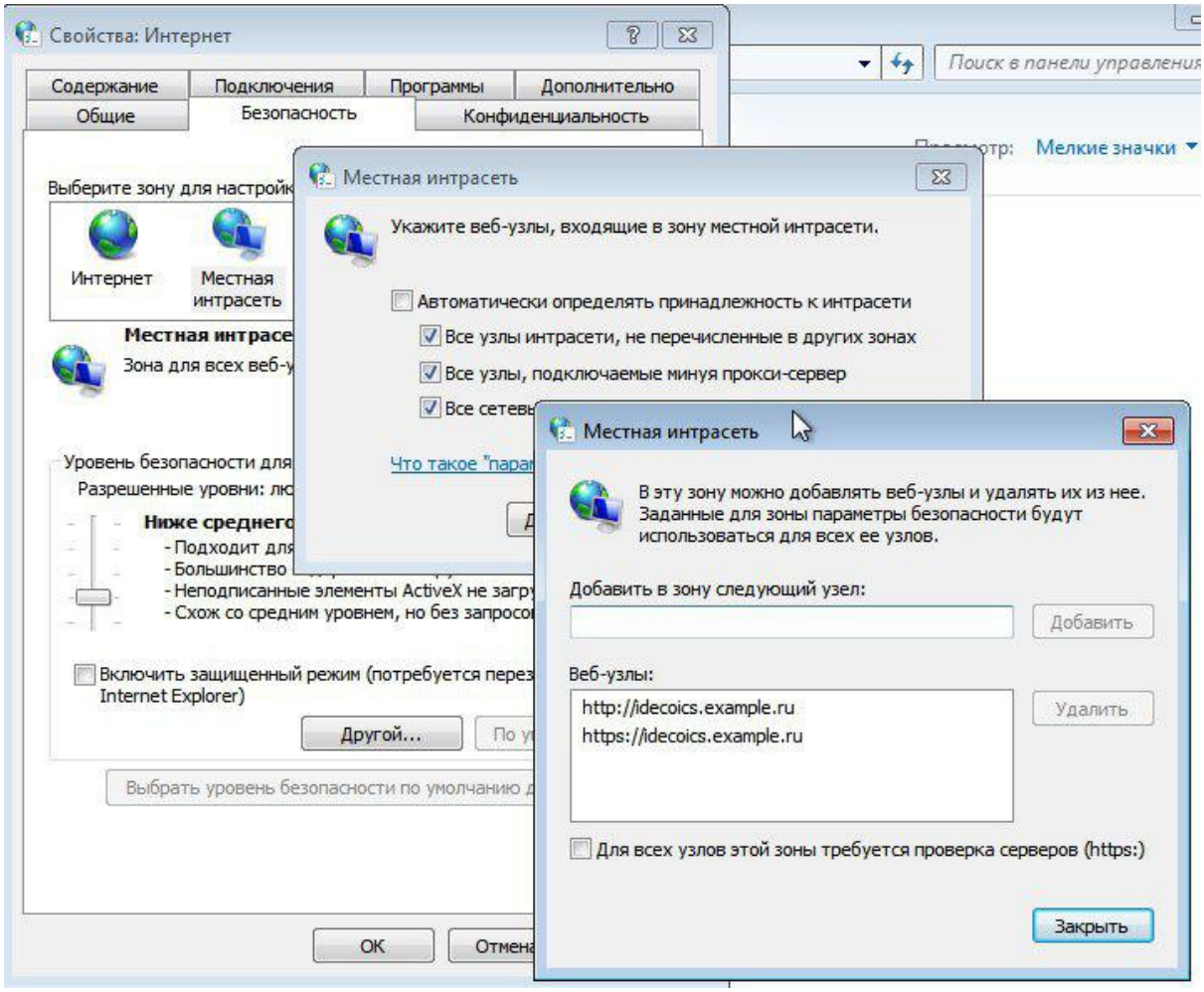
Для настройки аутентификации через веб-браузер выполните следующие действия:

1. Зайдите в свойства браузера на вкладку **Безопасность**.

2. Выберите **Местная интрасеть -> Сайты -> Дополнительно**.

3. 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. Перейдите по пути:

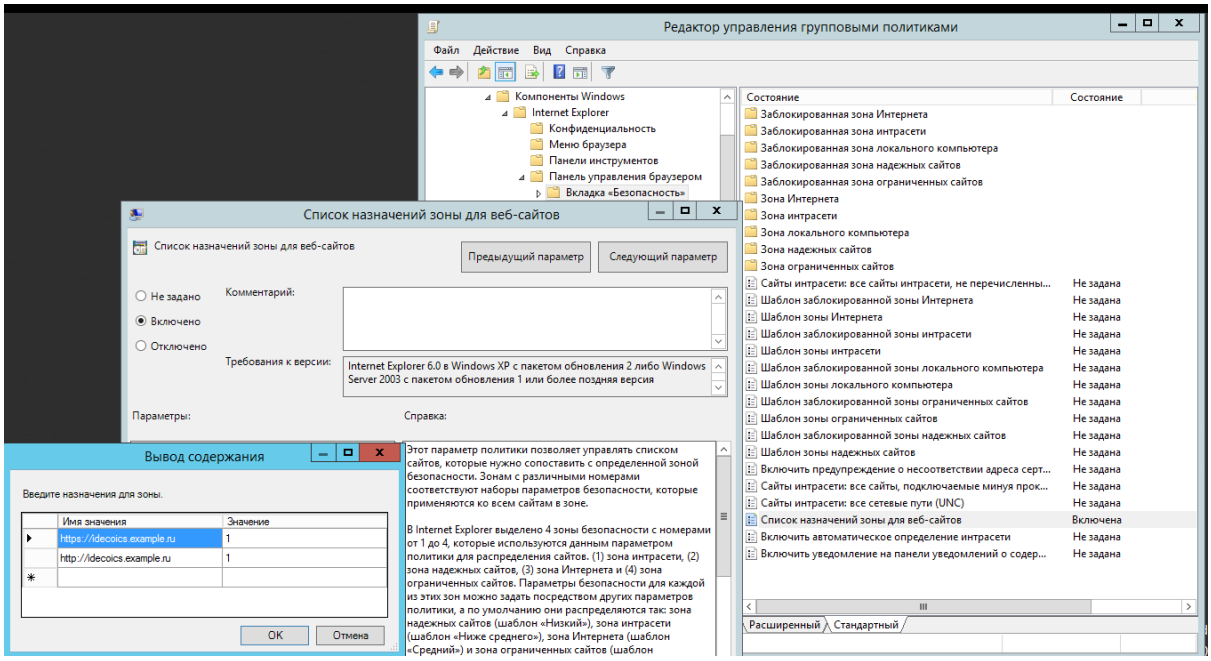
Англоязычная версия:

Edit group policy -> Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Site to Zone Assignment List

Русскоязычная версия:

Изменение локальной групповой политики -> Политика «Локальный компьютер» -> Административные шаблоны -> Компоненты Windows -> Internet Explorer -> Панель управления браузером -> Вкладка безопасность -> Список назначений зоны для веб-сайтов

2. Введите назначение зоны для DNS-имени Ideco NGFW (в примере idecoics.example.ru) со значением, равным 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.

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, `idecoUTM.example.ru`);
- **security.enterprise_roots.enabled** в значении `true` позволит Firefox доверять системным сертификатом и авторизовать пользователей при переходе на HTTPS-сайты.

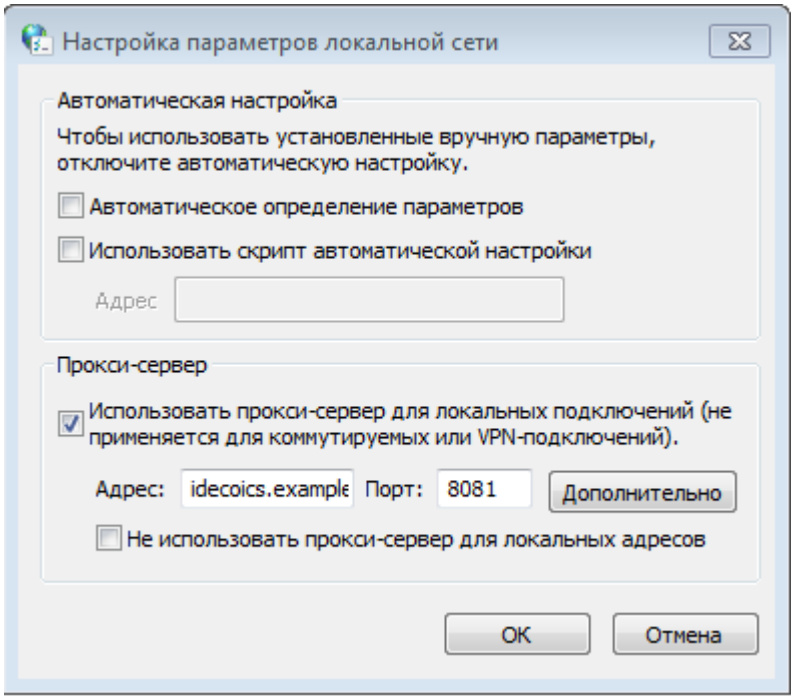
Способы аутентификации импортированных пользователей:

- **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:

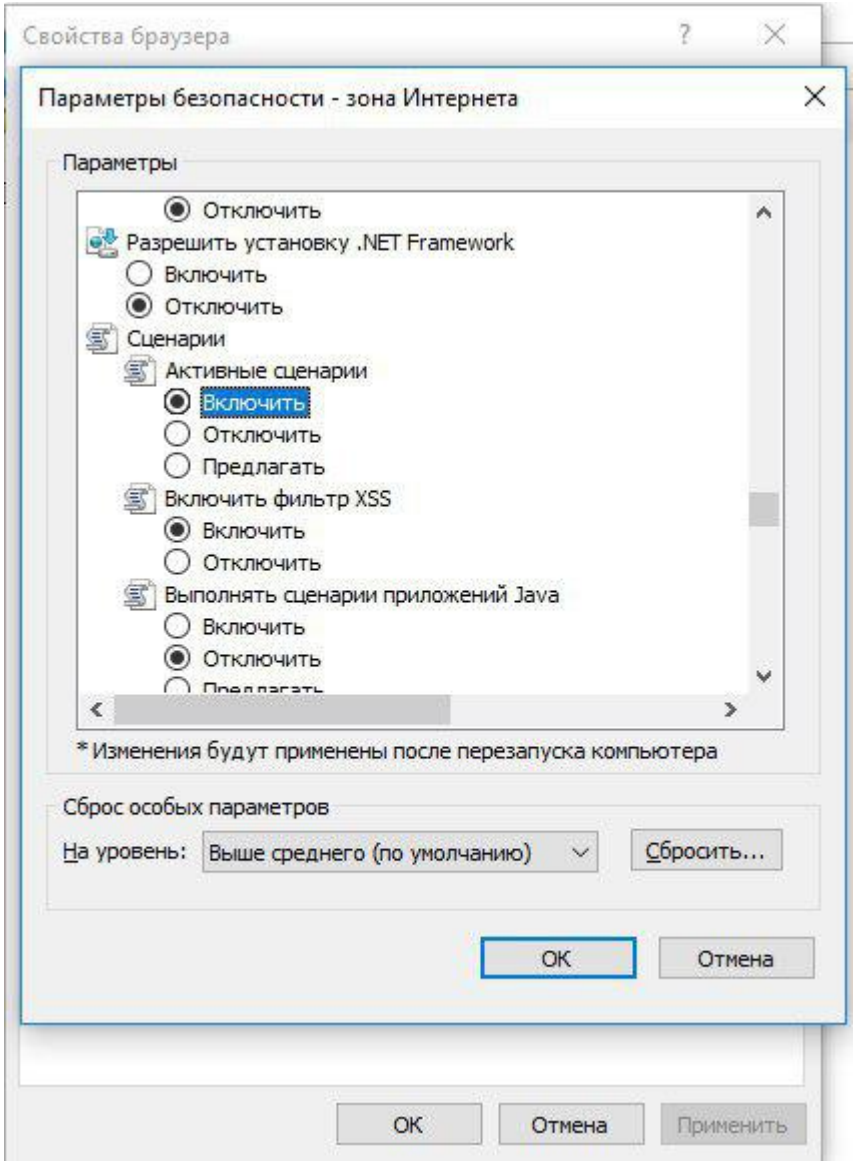
Для аутентификации компьютеров, которые **не находятся в домене**, под доменным пользовательским аккаунтом на странице настроек браузера **Mozilla Firefox** (about:config в адресной строке) укажите следующие параметры:

- **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.

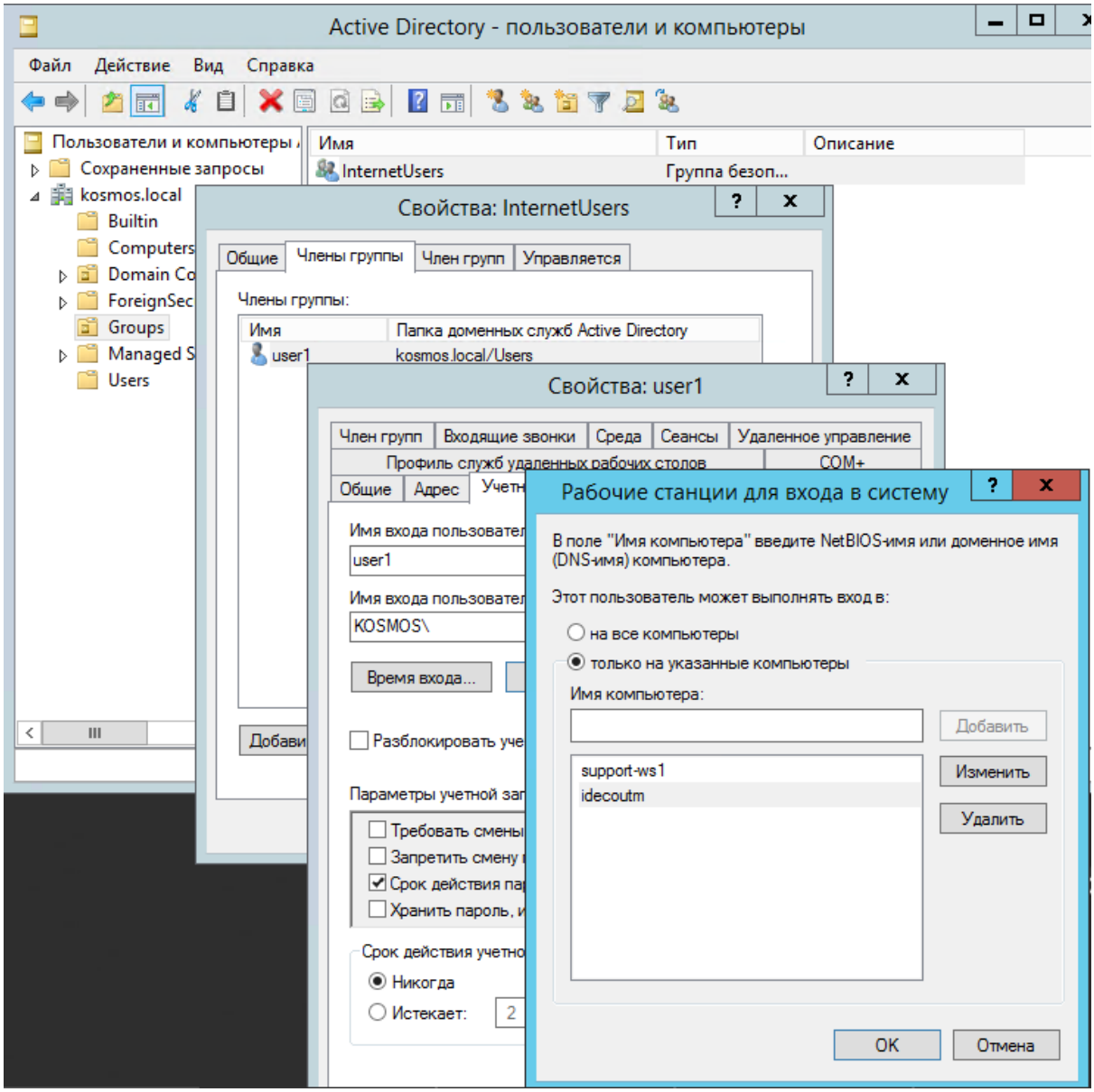
Возможные проблемы:

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 во 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:



13.5.6 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*.

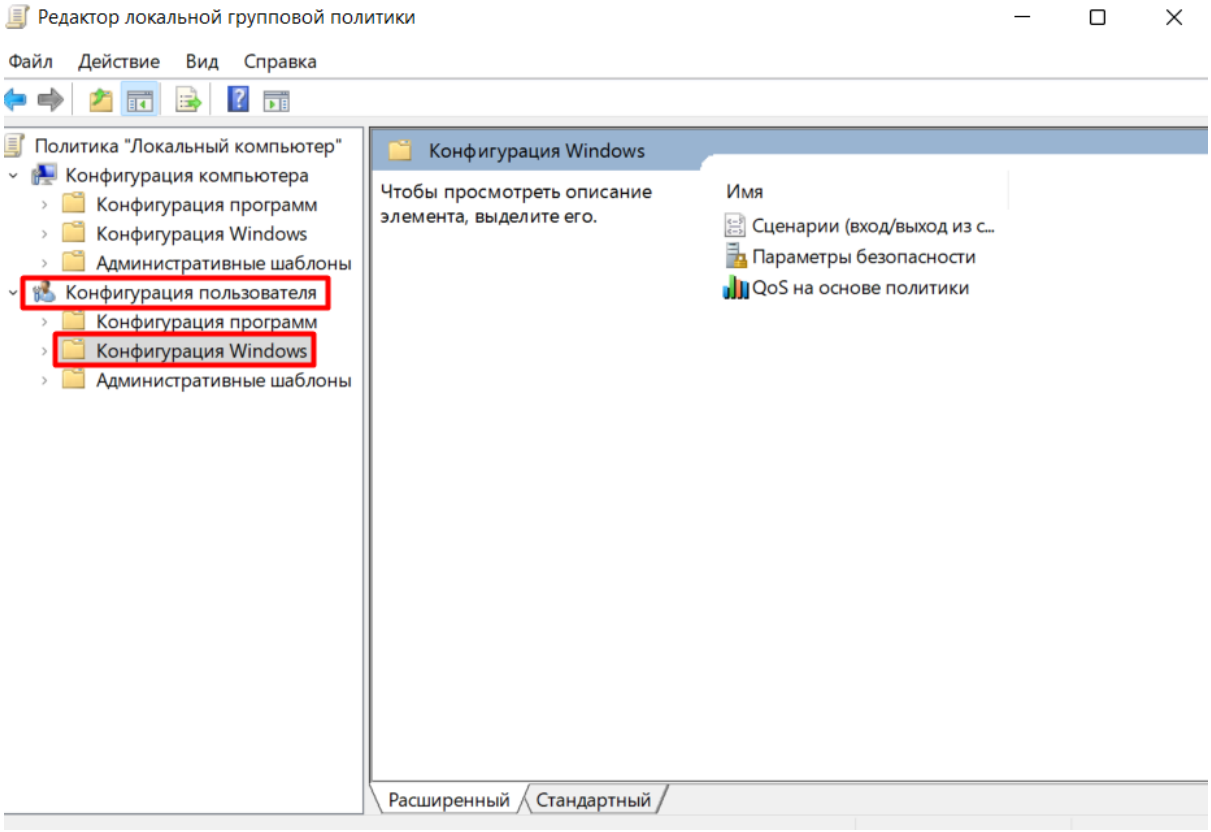
Разавторизация пользователя

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**. Переключите опцию **Веб-аутентификация**, после чего появится кнопка **Скачать скрипт для разавторизации**:

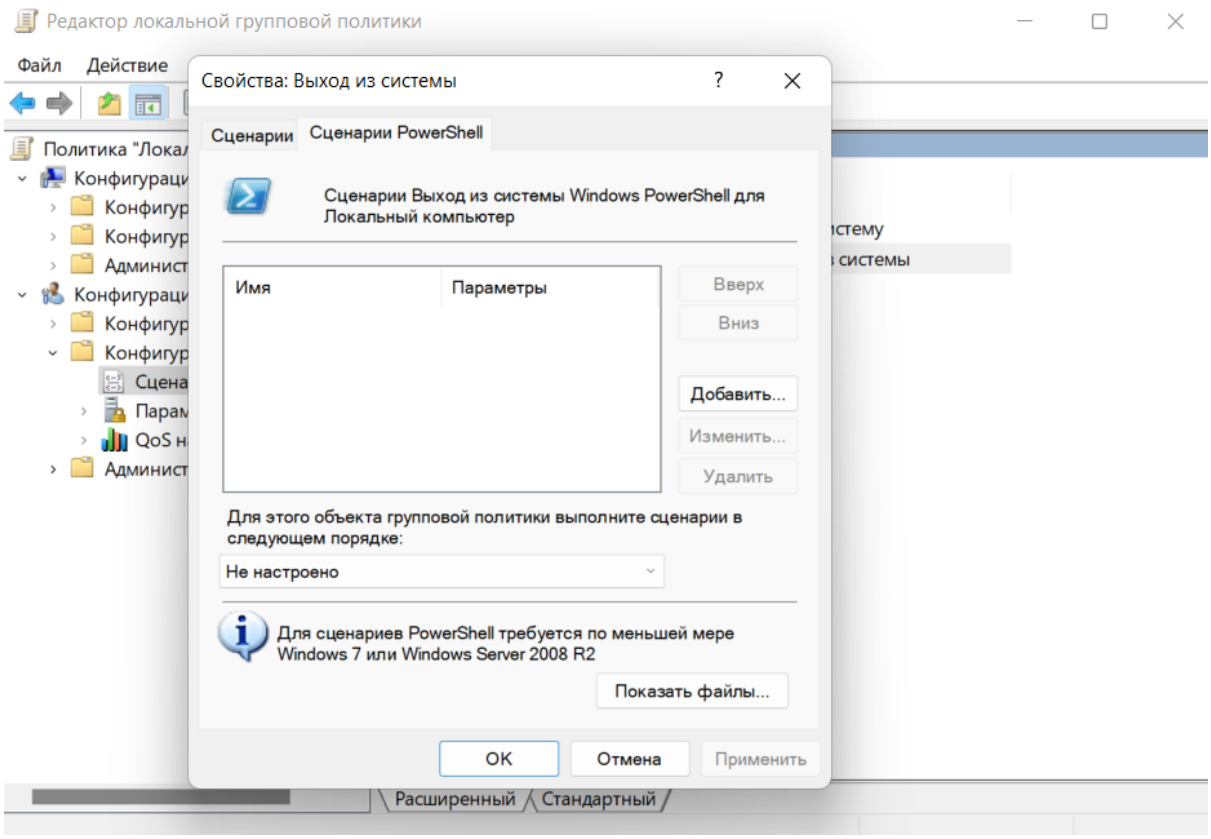
2. Откройте групповые политики (gpedit.msc) от имени администратора на устройстве пользователя.

3. Перейдите в **Конфигурации пользователя**, далее в **Конфигурации Windows**:

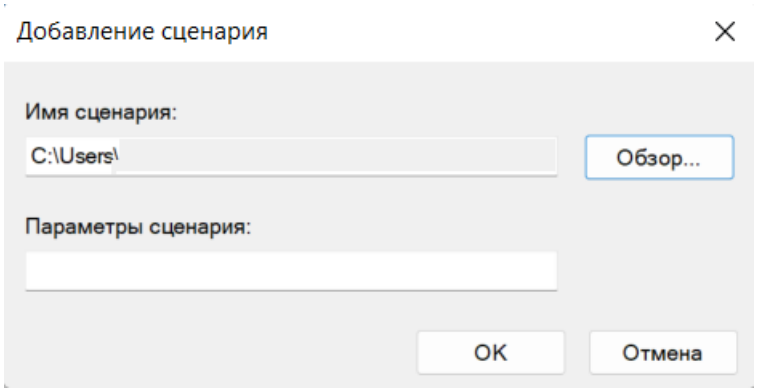


4. Нажмите **Сценарии (вход/выход из системы)**.

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

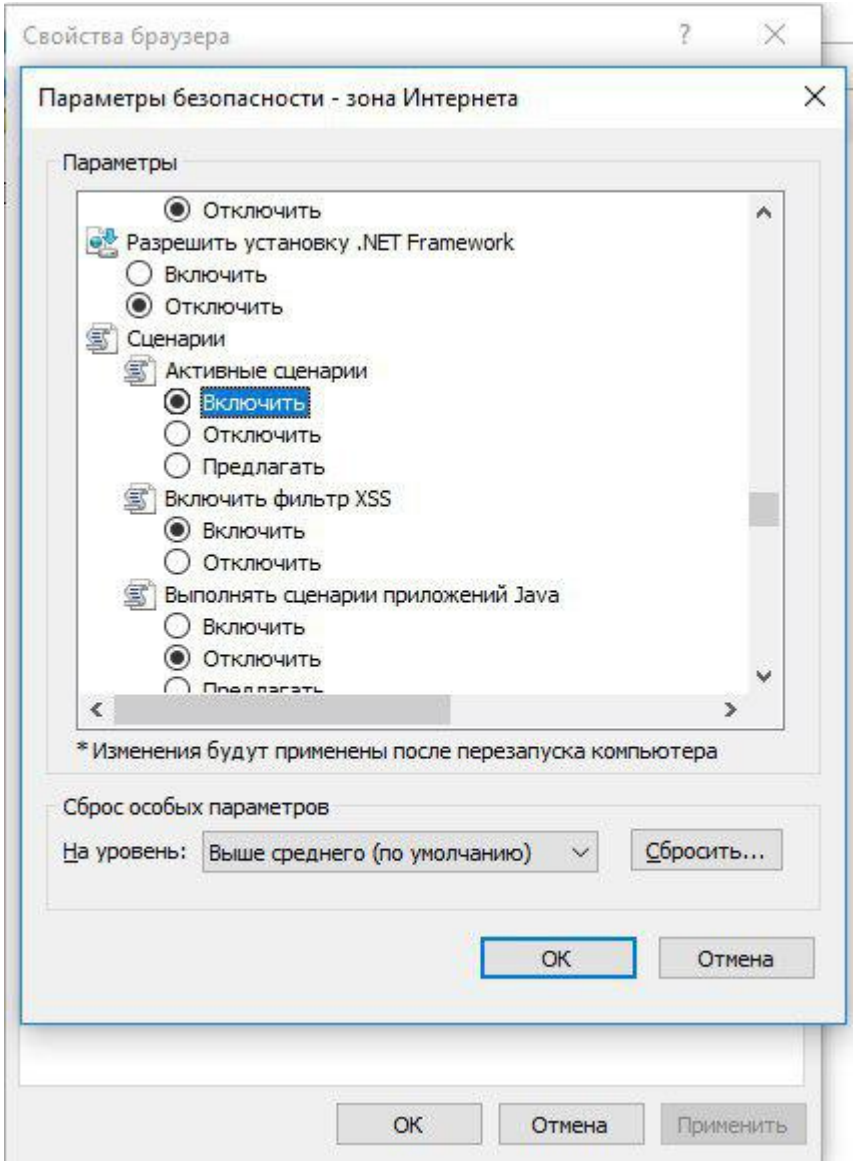


6. Нажмите **Добавить** и выберите скачанный файл **Ideco_NGFW_logout.ps1**, нажав на кнопку **Обзор**:



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

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



13.5.7 Импорт пользователей

Внимание: Приостанавливается синхронизация с контроллером домена, если локальные пользователи Ideco NGFW находятся в группах AD.
Для возобновления синхронизации вынесите локальных пользователей из групп AD. Автоматическая синхронизация произойдет через 15 минут.

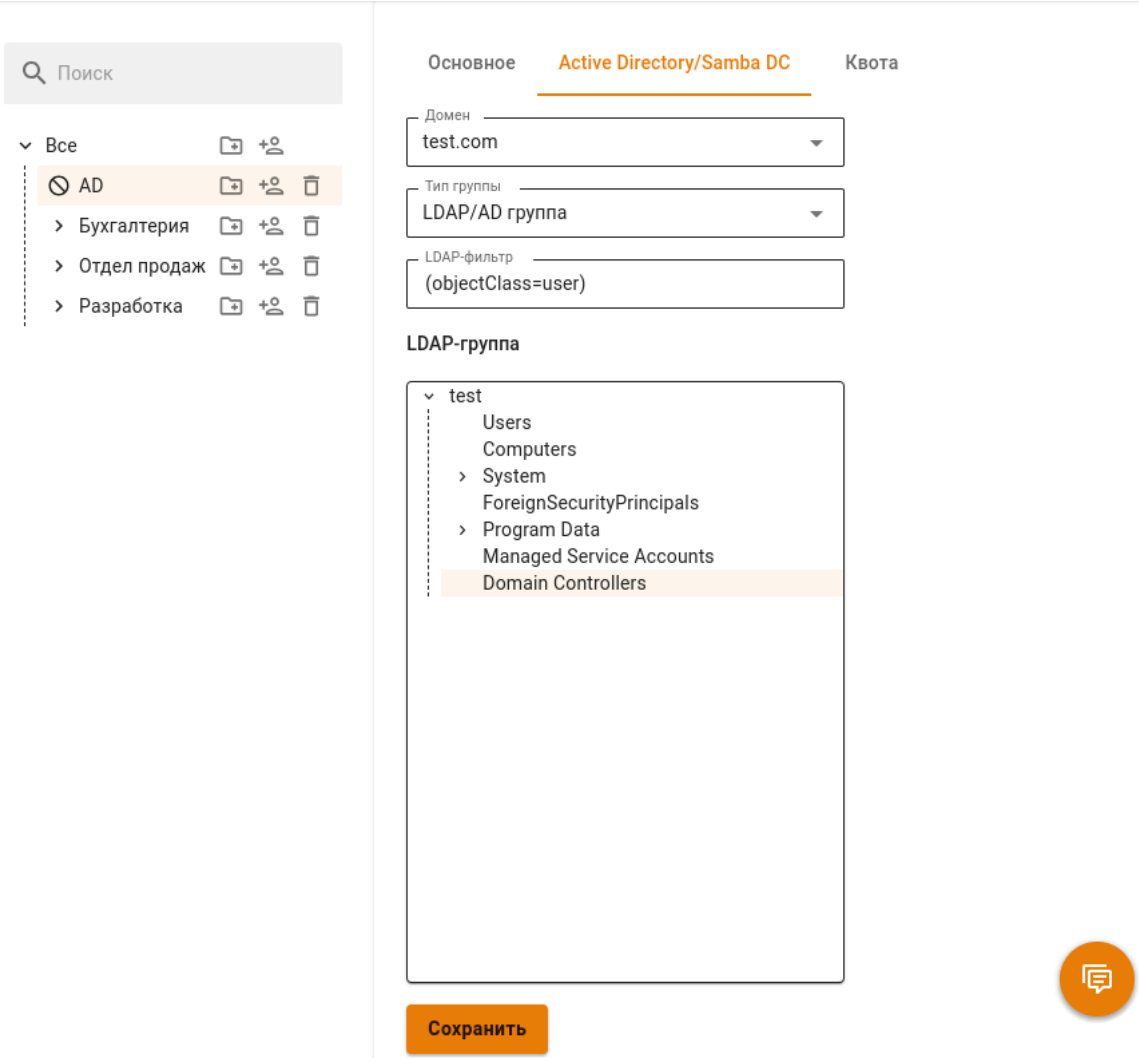
Импорт учетных записей из LDAP

В Ideco NGFW реализована возможность импорта учетных записей из LDAP-каталога. Импорт осуществляется по протоколам LDAP/LDAPS (протокол LDAPS не требует дополнительных настроек со стороны NGFW и будет использоваться автоматически в случае использования его на контроллере домена).

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

Для импорта пользователей выполните следующие 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 (если Ideco NGFW является членом нескольких доменов).
4. В поле **Тип группы** выберите LDAP/AD группа.
5. При нажатии на поле **LDAP группа** откроется дерево пользователей. Выберите из него необходимую группу для импорта (также можно выбрать корневую группу для импорта всего дерева).
6. Нажмите **Сохранить** (будет произведен импорт пользователей).



Подсказка: В дальнейшем пользователи будут автоматически синхронизироваться с контроллером домена каждые 15 минут.

При импорте пользователей также импортируются и номера телефонов для использования *двухфакторной аутентификации*.

При необходимости можно воспользоваться 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 следующий текст:

```
(&(objectCategory=person)(objectClass=user))
```

Можно импортировать разные группы пользователей контроллера домена в различные группы Ideco NGFW для удобства назначения на них правил файрвола, контентной фильтрации, контроля приложений, ограничения полосы пропускания и других модулей.

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

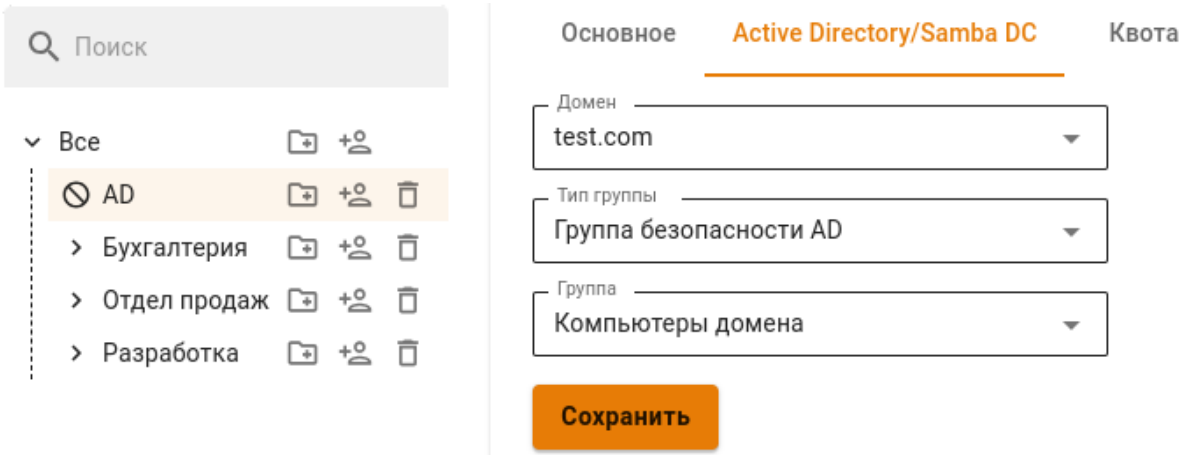
Импорт учетных записей из групп безопасности

Подсказка: Пользователь контроллера домена может быть импортирован только в одну группу Ideco NGFW. Если он находится в нескольких группах безопасности, он попадет только в одну группу, которая была импортирована самой последней.

Можно импортировать любое количество групп безопасности AD в разные папки в дереве пользователей Ideco NGFW.

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**.

Пример настройки импорта пользователей из групп безопасности представлен на скриншоте ниже:



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 PUT 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 во вкладку **Сеть** и нажмите на любой запрос;

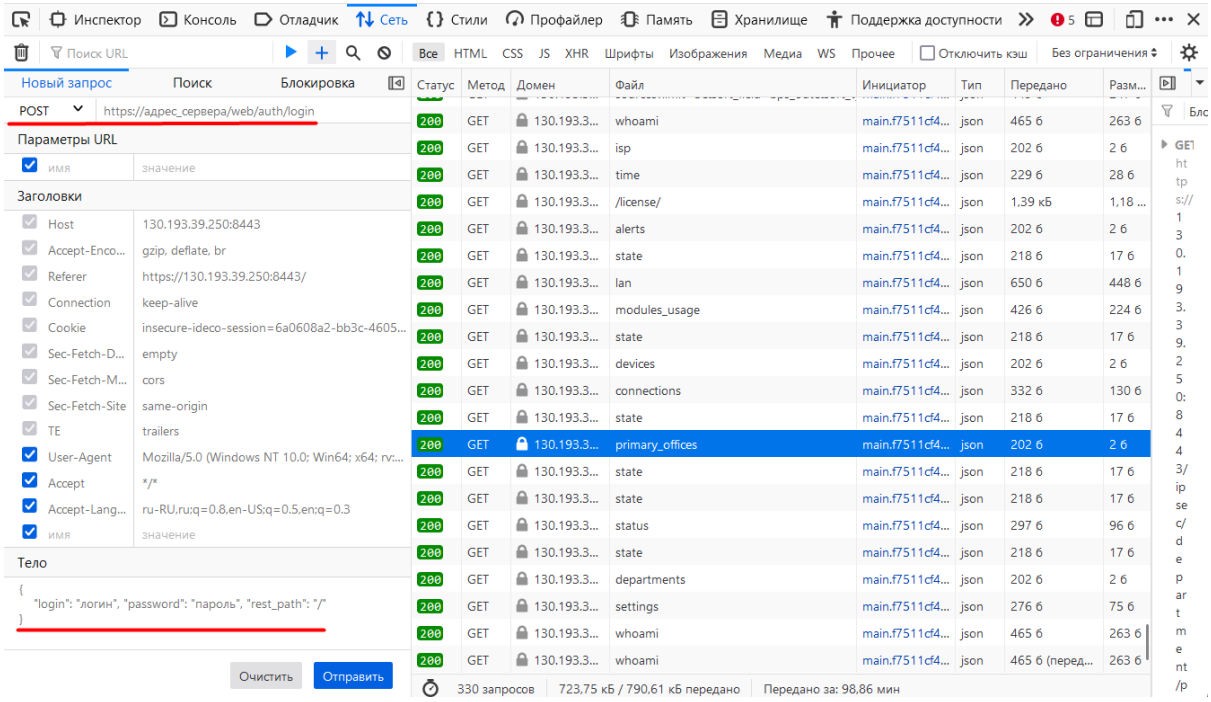
3. В появившемся окне перейдите на вкладку **Новый запрос**;

4. Отправьте запрос авторизации:

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

Тело запроса:

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

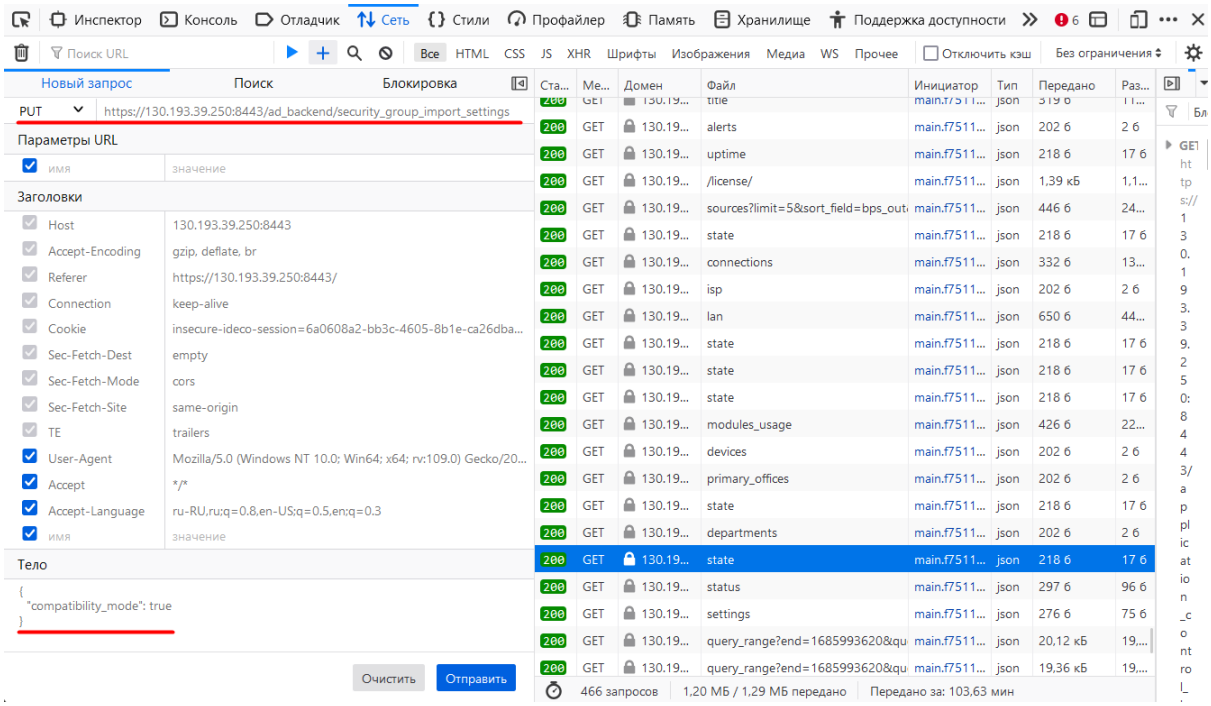


5. Отправьте запрос на включение режима:

```
PUT /ad_backend/security_group_import_settings
```

Тело запроса:

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



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

13.6 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 и выше.

ALD Pro предназначен для централизованного управления ресурсами под управлением ОС Astra Linux и может использоваться в организациях различного масштаба.

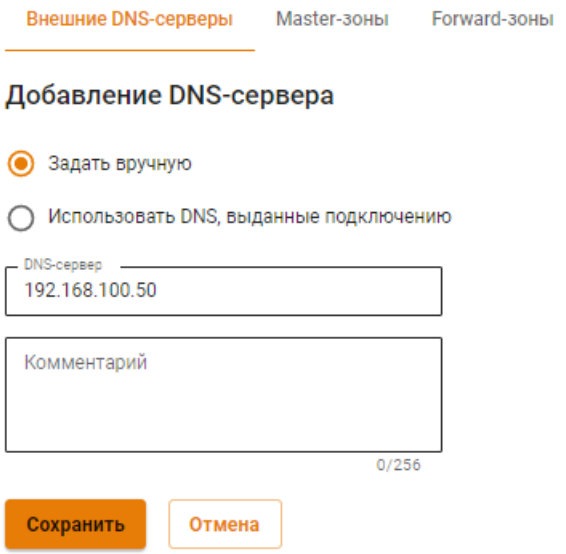
Руководства по эксплуатации ALD Pro доступны на официальном сайте.

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.

Предупреждение: Если после обновлении с 15 версии Ideco UTM на 16 версию Ideco NGFW отображается пустой список пользователей (OU), удалите интеграцию с доменом ALD и заново введите NGFW в домен ALD.

13.6.1 Ввод сервера в домен

1. Перейдите в раздел **Сервисы -> DNS -> Внешние DNS-серверы** и добавьте IP-адрес DNS-сервера ALD:

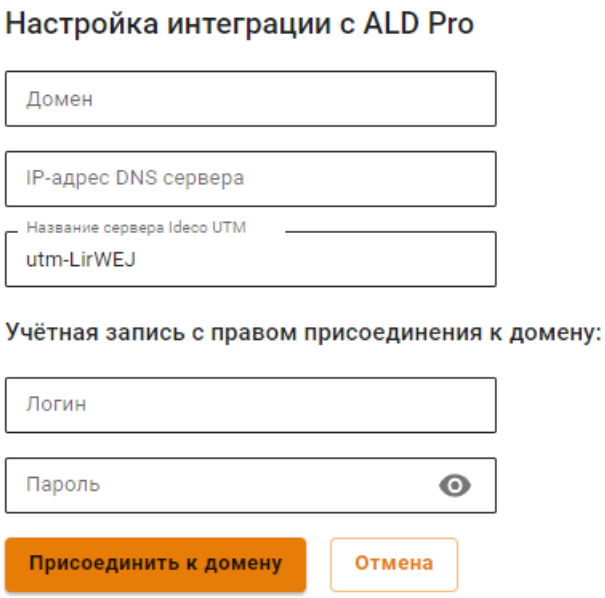


2. Перейдите на вкладку **Пользователи -> ALD Pro**.

2. Нажмите на кнопку **Добавить**.

3. Заполните следующие поля:

- **Домен**: введите полное имя домена (не контроллера домена). Например: `mydomain.example`. Домен может содержать только латинские символы, цифры, подчеркивание, дефис и точку;
- **IP-адрес DNS-сервера**: добавьте IP адрес DNS-сервера ALD;
- **Имя сервера Ideco NGFW**: введите имя сервера. Оно может содержать только 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 используется 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.

13.6.2 Импорт пользователей

ALD Pro поддерживает импорт двух типов групп:

- Группа пользователей - содержит несколько пользователей ALD.
- Подразделение - содержит дерево пользователей ALD, 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**, выберите домен, тип группы и нажмите **Сохранить**.

Импортированных пользователей можно использовать в качестве объектов для авторизации, настройки VPN-подключений, создания правил (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 одну группу, которая была импортирована последней.

13.6.3 Аутентификация пользователей

При аутентификации пользователей проверка осуществляется средствами Kerberos.

ALD Pro поддерживает два типа входа в систему:

- вход по логину/паролю;
- вход через SSO.

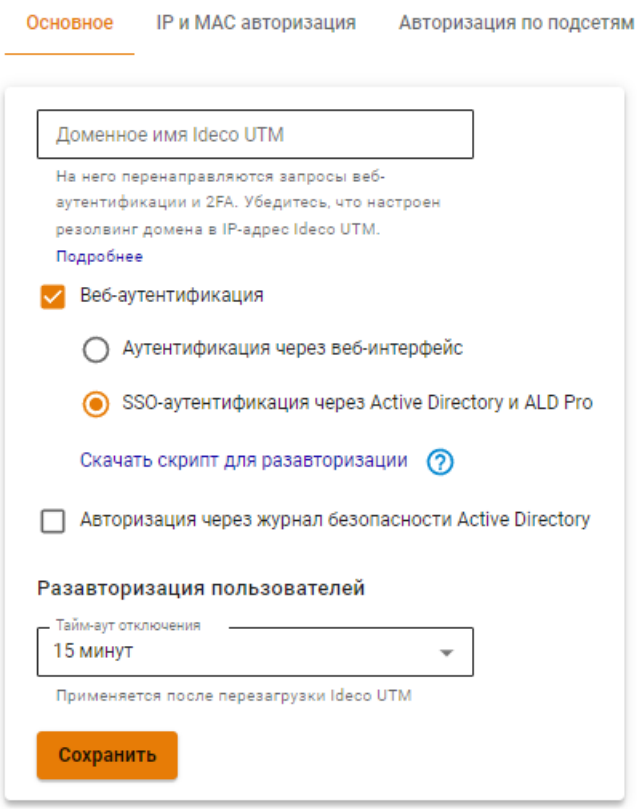
Настройка Ideco NGFW

Для настройки аутентификации выполните действия:

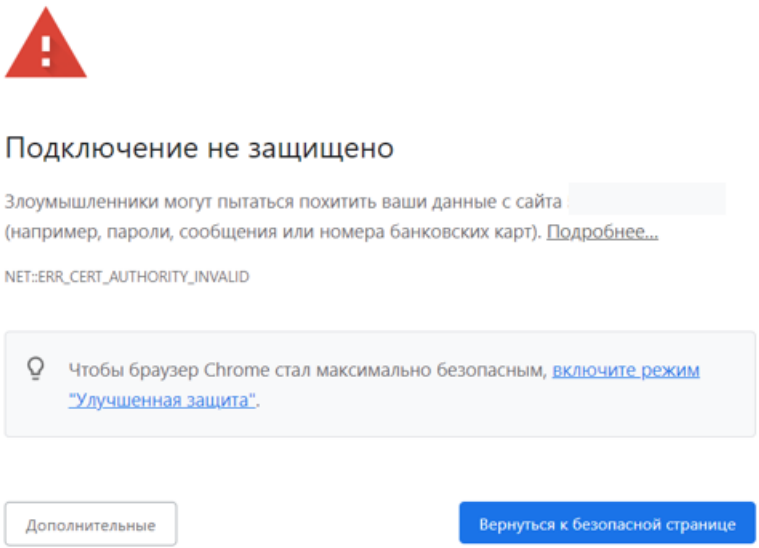
1. Перейдите в раздел **Пользователи -> Авторизация -> Основное**.

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

3. Выберите тип входа в систему:
3.1 Для входа по логину/паролю активируйте опцию **Аутентификация через веб-интерфейс**.
3.2 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.

Настройка клиентских машин для SSO-авторизации

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 авторизовать пользователей при переходе на HTTPS-сайты.

Способы аутентификации импортированных пользователей:

- 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.

Подсказка: Для настройки авторизации по VPN воспользуйтесь статьей *VPN-подключение*.

13.7 Обнаружение устройств

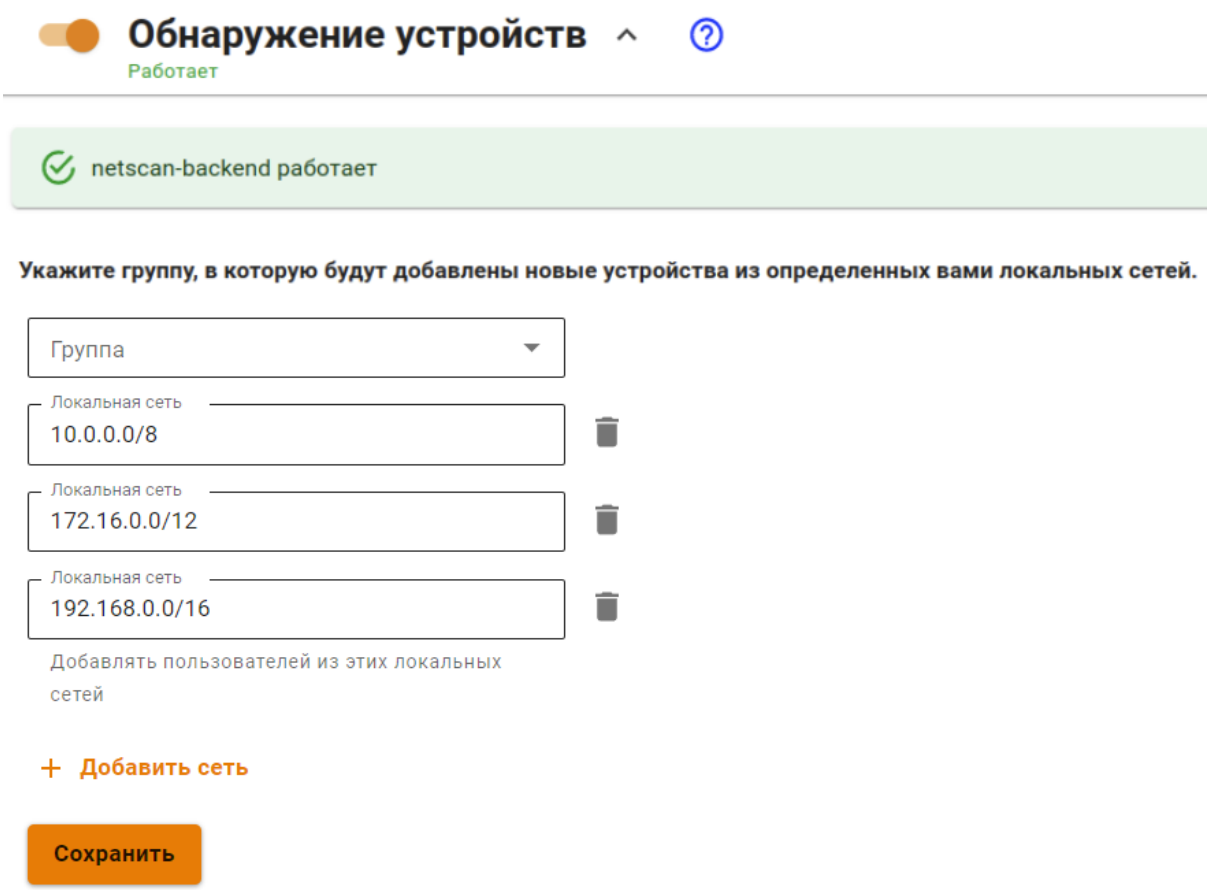
13.7.1 Основное

Подсказка: Название службы раздела **Обнаружение устройств**: `ideco-netscan-backend`.
Список служб для других разделов доступен по *ссылке*.

Подсказка: **Обнаружение устройств** создает авторизацию по MAC для локальных адресов в одном Ethernet-сегменте. Если устройство находится в локальной сети за роутером, то **Обнаружение устройств** создаст авторизацию по IP-адресу.

Данный модуль не осуществляет сканирования сети в поисках устройств, а работает в пассивном режиме.

При попытке выхода в интернет будет создан пользователь в указанной группе с именем, соответствующим NetBIOS-имени компьютера. Если NetBIOS-имя определить не удалось, то IP-адресу.



При необходимости можно ограничить локальные сети, пользователи из которых будут автоматически добавлены и авторизованы на Ideco NGFW. Например, таким образом 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.

13.8 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:

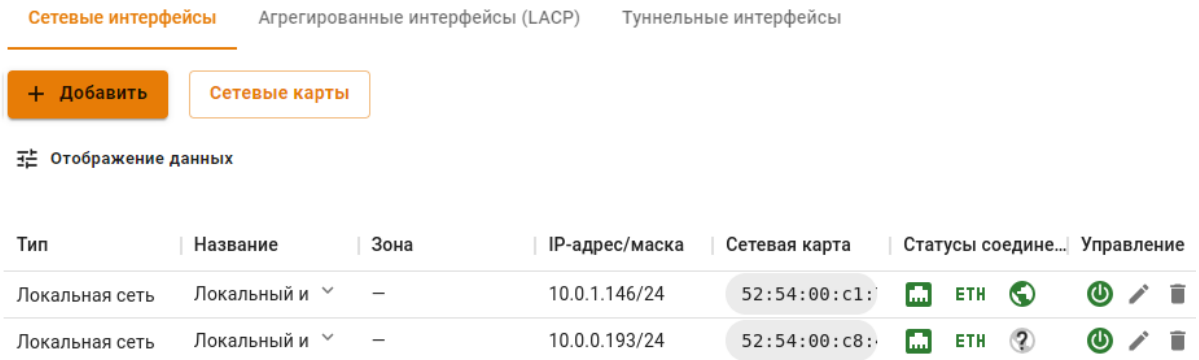
В режиме точки доступа или bridge устройство Wi-Fi предоставляет возможность беспроводным клиентам подключаться к локальной сети.

Для этого индивидуально авторизуйте всех беспроводных клиентов на Ideco NGFW с помощью IP-авторизации. Воспользуйтесь следующими 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:



- **10.0.1.146/24** - шлюз для беспроводной Wi-Fi-сети;
- **10.0.0.193/24** - шлюз для локальной Ethernet-сети.

13.8.1 Настройка DHCP:

1. Добавьте отдельную логическую сеть для клиентов Wi-Fi;

2. Добавьте в сетевые интерфейсы шлюз созданной сети;

3. Перейдите в раздел 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.

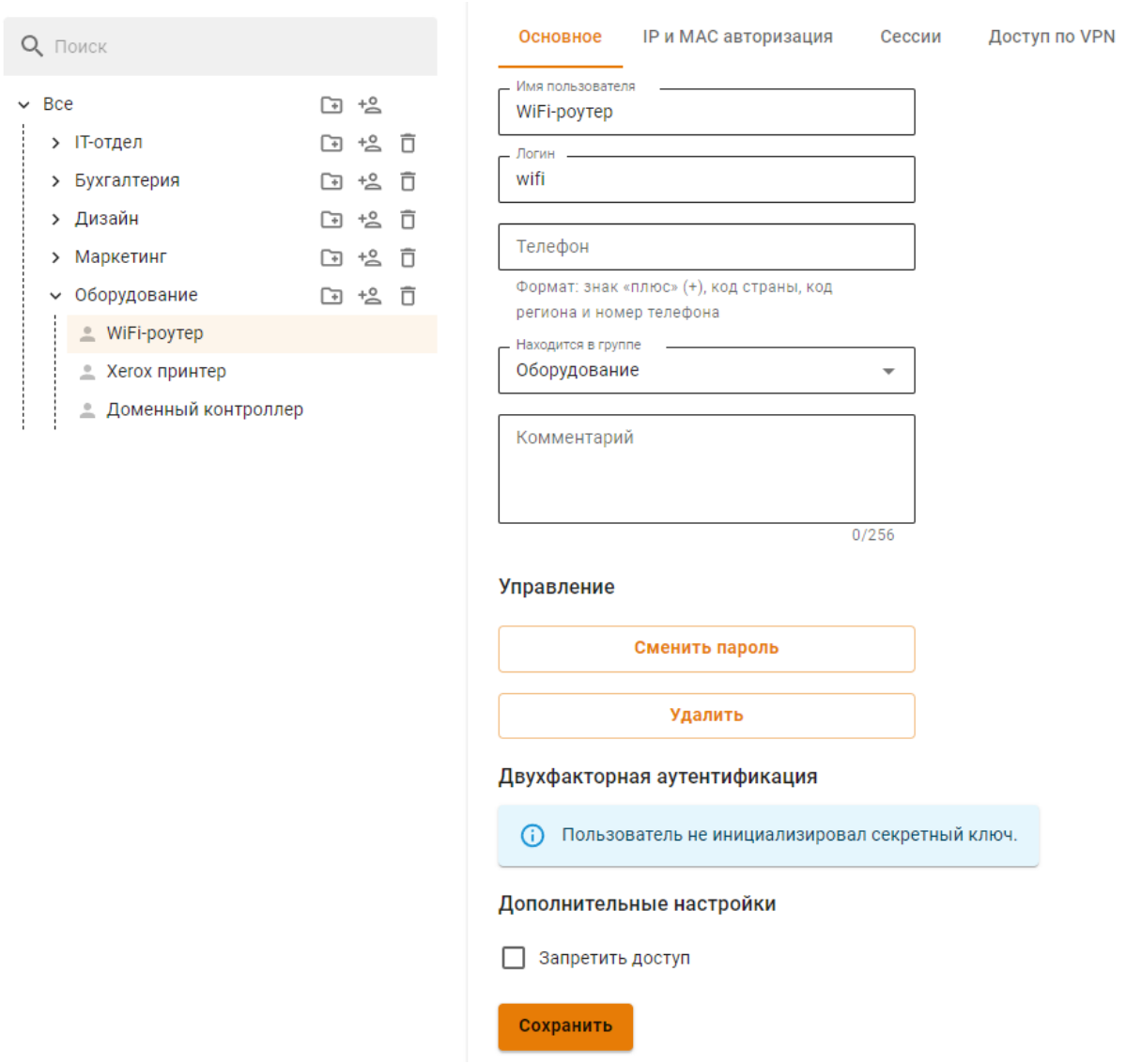
Режим роутера:

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.

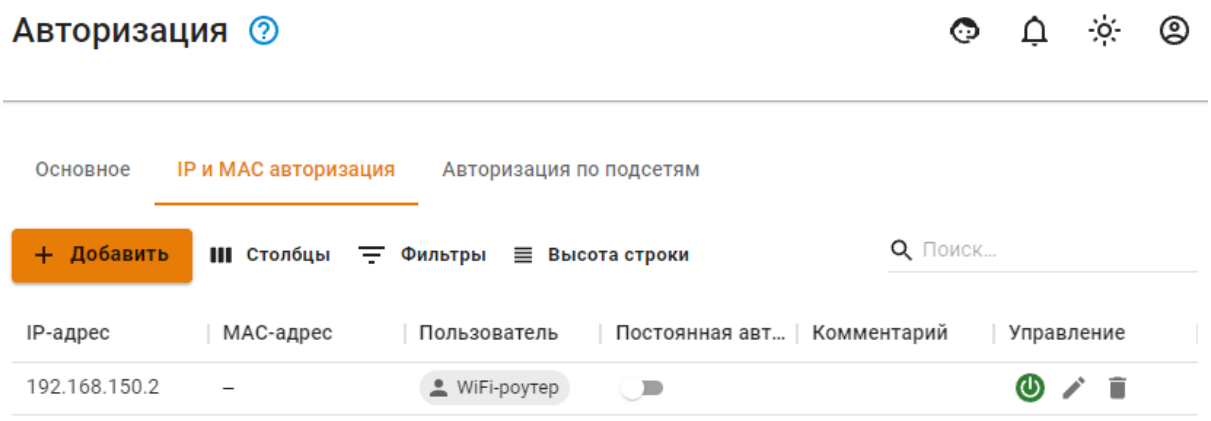
Пример настройки пользователя в режиме роутера представлен на скриншотах ниже:

1. Создайте пользователя для Wi-Fi-роутера.

Пароль у пользователя может быть любой.



2. В разделе **Пользователи -> Авторизация -> IP и MAC авторизация** создайте правило следующего вида:



К пользователю необходимо применить общие ограничения *контент-фильтра* и *файрвола* для Wi-Fi-сети.

13.8.2 Настройка DHCP:

В большинстве случаев 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.

14. Мониторинг

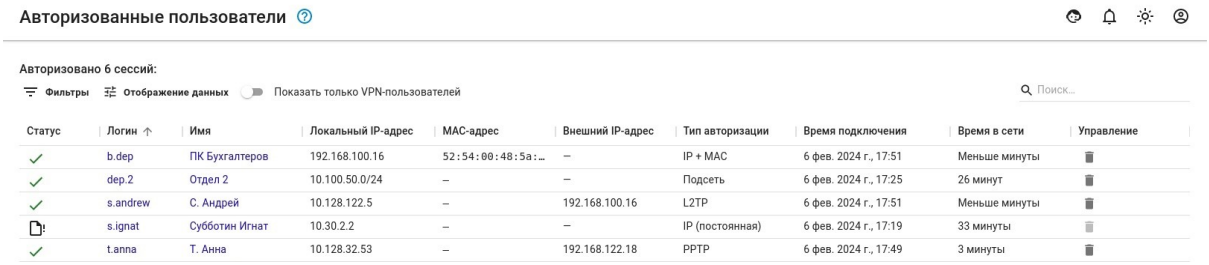
14.1 Авторизованные пользователи

14.1.1 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 таблицы с авторизованными разными способами пользователями представлен на скриншоте ниже:



В столбце **Управление** можно разавторизовать пользователя при необходимости.

Включение опции **Показать только VPN-пользователей** отфильтрует в таблице журнала информацию о всех VPN-сессиях по всем протоколам.

14.2 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.

14.2.1 Ядро

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.

14.2.2 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:

```
[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
```

14.2.3 Диски

Содержит статистику об объеме записанной и прочитанной информации (график *Диск*) в определенный промежуток времени 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 *Резервное копирование*.

14.2.4 VPN

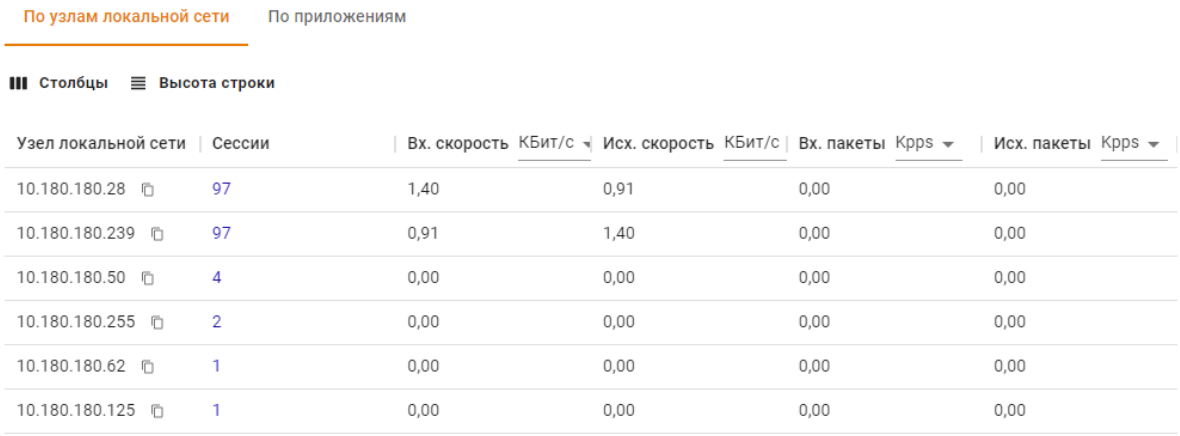
Содержит информацию о количестве подключений пользователей по протоколам L2TP/IPsec, PPTP и IKEv2. Инструкция по VPN-подключению пользователей доступна по *ссылке*.

14.3 Монитор трафика

Подсказка: Для включения мониторинга трафика необходимо запустить модуль *Контроля приложений*.

14.3.1 По узлам локальной сети

Вкладка **По узлам локальной сети** позволяет отслеживать активность пользователей сети и выявлять тех, кто нагружает канал трафиком.



Узел локальной сети	Сессии	Вх. скорость КБит/с	Исх. скорость КБит/с	Вх. пакеты Kpps	Исх. пакеты Kpps
10.180.180.28	97	1,40	0,91	0,00	0,00
10.180.180.239	97	0,91	1,40	0,00	0,00
10.180.180.50	4	0,00	0,00	0,00	0,00
10.180.180.255	2	0,00	0,00	0,00	0,00
10.180.180.62	1	0,00	0,00	0,00	0,00
10.180.180.125	1	0,00	0,00	0,00	0,00

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

По узлам локальной сети | По приложениям

← Сессии10.180.180.28 | Столбцы | Высота строки

Протокол/порт лок...	Внешний хост	Приложение	Протокол/Порт при...	Вх. скорость	Исх. скорость КБ	Вх. пакеты Kpps
TCP/43236	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60556	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60570	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60572	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60582	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60594	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60610	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60622	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00

14.3.2 По приложениям

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

Например, если пользователь не загружает канал трафиком, но в таблице **По узлам локальной сети** присутствует большое количество пакетов данных, то на вкладке **По приложениям** можно выявить приложение с подозрительной активностью.

По узлам локальной сети | По приложениям

Столбцы | Высота строки

Приложение	Сессии	Вх. скорость КБит/с	Исх. скорость КБит/с	Вх. пакеты Kpps	Исх. пакеты Kpps
Неизвестно	2	0,00	0,32	0,00	0,00
TLS	104	0,00	0,00	0,00	0,00
DHCP	1	0,00	0,00	0,00	0,00
NetBIOS	1	0,00	0,00	0,00	0,00
BJNP	2	0,00	0,00	0,00	0,00

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

По узлам локальной сети | По приложениям

← Сессии TLS | Столбцы | Высота строки

Узел локал...	Протокол/...	Внешний х...	Протокол/...	Вх. скорость	Исх. скорост	Вх. пакеты К	Исх. пакеты	Длительно...	Интерфейс
10.180.180.2	TCP/43236	10.180.180.2	TCP/8443	0,00	0,00	0,00	0,00	1 час 19 мин	Лока...
10.180.180.2	TCP/8443	10.180.180.2	TCP/43236	0,00	0,00	0,00	0,00	1 час 19 мин	Лока...
10.180.180.2	TCP/33566	10.180.180.2	TCP/8443	0,00	0,00	0,00	0,00	1 минута	Лока...
10.180.180.2	TCP/8443	10.180.180.2	TCP/33566	0,00	0,00	0,00	0,00	1 минута	Лока...
10.180.180.2	TCP/33586	10.180.180.2	TCP/8443	0,00	0,00	0,00	0,00	1 минута	Лока...
10.180.180.2	TCP/8443	10.180.180.2	TCP/33586	0,00	0,00	0,00	0,00	1 минута	Лока...

14.4 Telegram-бот

Бот может отправлять оповещения:

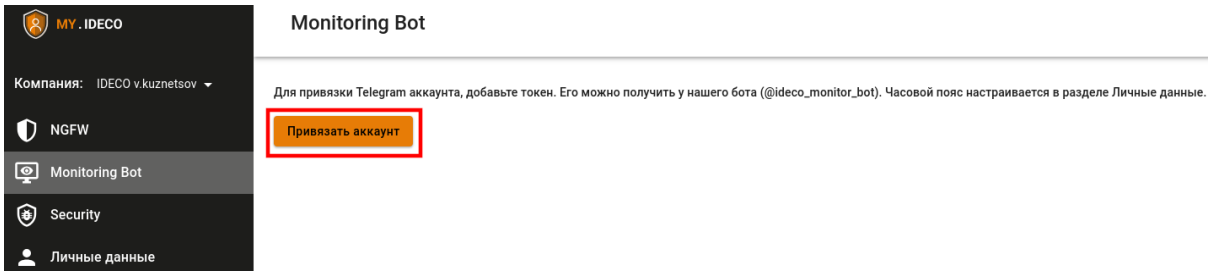
- в личные сообщения;
- в беседы, где 2 и более пользователей (groups).

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

14.4.1 Привязка Ideco Monitoring Bot

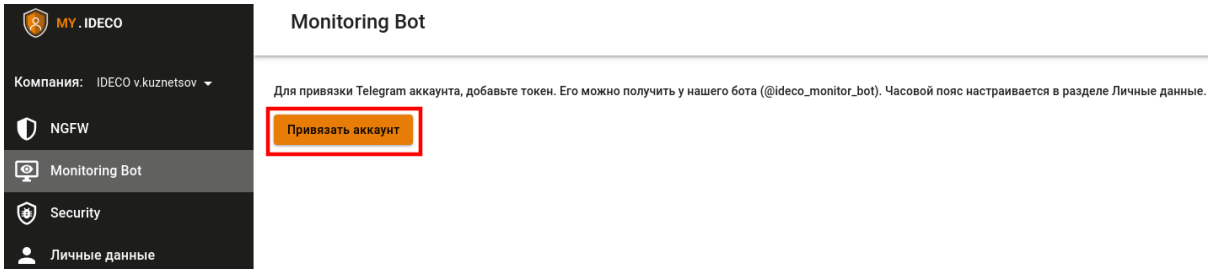
Настройка привязки Ideco Monitoring Bot к одному пользователю:

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.

14.4.2 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. Проставьте галочки напротив тех уведомлений, 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.

14.5 SNMP

14.5.1 Основное

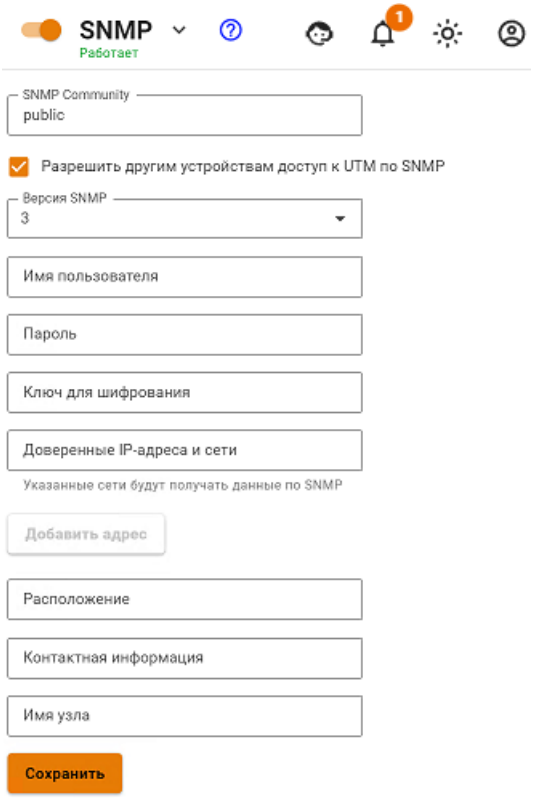
Подсказка: Для перевода раздела в рабочий режим переключите ползунок в положение **Включен**.

Этот модуль позволяет осуществлять мониторинг работы Ideco NGFW по протоколу SNMP версий 1/2c и 3. Для этого необходимо настроить имя пользователя, пароль (минимальное количество символов - 8) и ключ шифрования.

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.

Также можно внести IP-адреса и сети в доверенные, чтобы они получили доступ к данным с Ideco NGFW. Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и являются необязательными.



14.6 Zabbix-агент

Zabbix - это решение распределенного мониторинга корпоративного класса с открытыми исходными кодами.

Ознакомиться с Zabbix можно на официальной странице Zabbix.

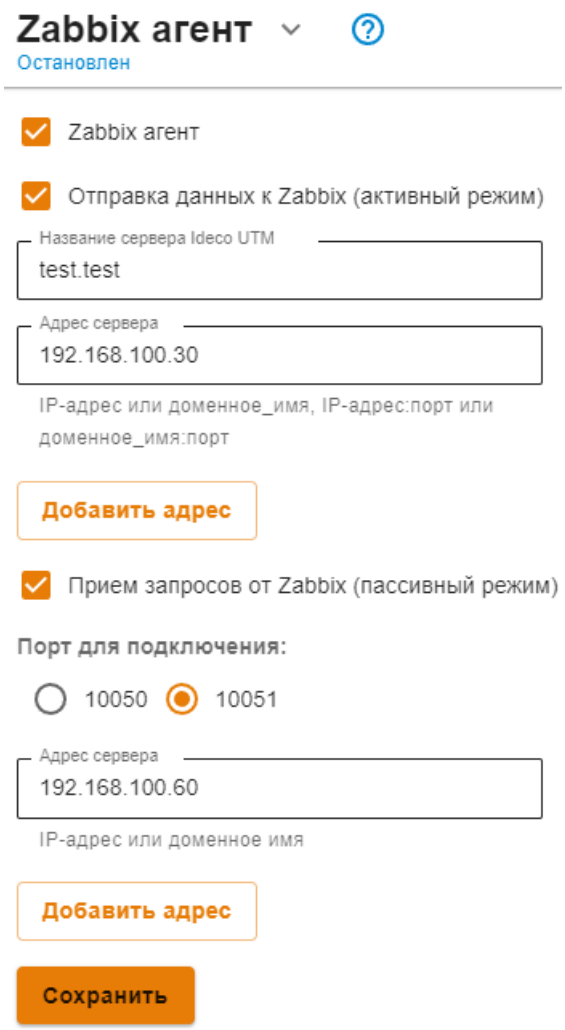
Опробуйте Zabbix в виде готового решения или установить его, воспользовавшись документацией Zabbix.

14.6.1 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. Правила трафика

15.1 Файрвол

Подсказка: Название службы раздела *Файрвол*: `ideco-firewall-backend`.
Список имен служб для других разделов доступен по *ссылке*.

Принцип работы файрвола заключается в проведении анализа заголовков пакетов, проходящих через интерфейсы сервера.

Эта низкоуровневая задача решается шлюзом на основе стека протоколов TCP/IP. Поэтому файрвол хорошо подходит для определения глобальных правил управления трафиком по сетевым протоколам, портам и другим критериям, основанным на значениях полей в заголовках сетевых пакетов.

Настройка файрвола производится в разделе веб-интерфейса **Правила трафика -> Файрвол**.

Файрвол Ideco NGFW использует для фильтрации трафика как отдельные интерфейсы, так и зоны - логические объединения сетевый 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 - “Разработчики“, “Гости“ и т. д., что сделает правила файрвола более читаемыми.

Для обеспечения защиты в NGFW есть преднастроенные и автоматически включаемые системные правила. Используйте пользовательские правила для фильтрации трафика локальной сети и публикации ресурсов.

Предупреждение: Сетевой экран не предназначен для решения задач, связанных с контролем доступа к ресурсам сети интернет исходя из адреса URL, доменного имени или типа контента на веб-сайтах. Эти задачи, обычно касающиеся веб-трафика, решаются с помощью модуля *Контент фильтр*.

Для блокировки веб-трафика **используйте** модуль *Контент фильтра*.

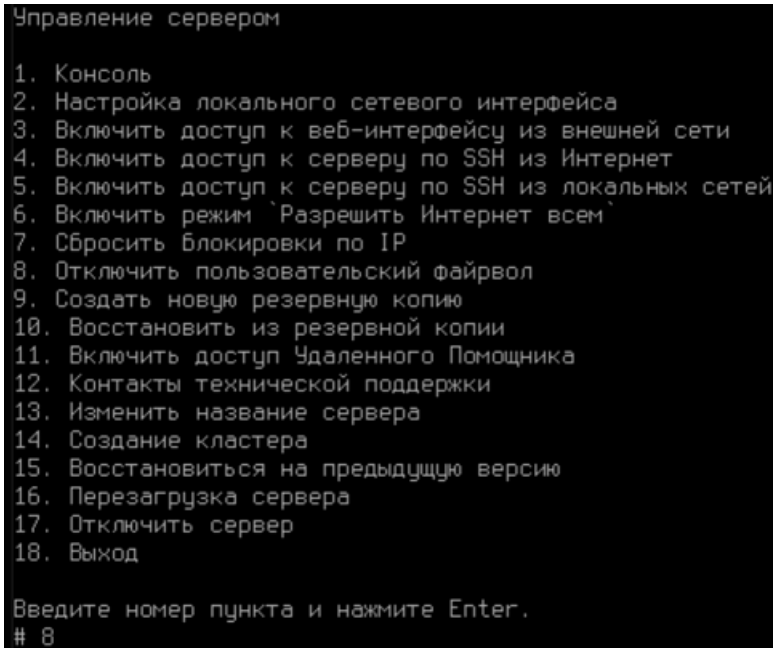
Предупреждение: Включение режима удаленного помощника изменяет таблицу правил файрвола. При этом становится доступно подключение по SSH из локальных и внешних сетей.

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 учтите, 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.**



15.1.1 Автоматический SNAT локальных сетей и счетчик срабатываний

Включите опцию **Автоматический SNAT локальных сетей** для автоматического преобразования адреса трафика, уходящего во внешнюю зону, если источник равен `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`, и адресов, которые прописаны во вкладке **SNAT**, если выбрано действие **SNAT**. Таким образом, не нужно создавать правила вручную и изменять их при добавлении или изменении локальных сетей.

Можно создать правила SNAT вручную для тех, кому он необходим, и отключить (правилом «не SNAT») для тех, кого необходимо допустить в сеть без сетевой трансляции адресов.

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**.

15.1.2 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, которые запрещают весь трафик, поскольку в дальнейшем могут возникнуть проблемы при настройке разрешающих правил.

Если такие правила все же создаются, необходимо:

- Создать правило, разрешающее трафик от пользователя;
- Создать правило, разрешающее трафик для специальной зоны источника **Исходящий трафик устройства**.

В противном случае клиентский HTTP/HTTPS-трафик будет блокироваться.

Для удобства управления правилами в интерфейсе они разбиты на четыре таблицы: FORWARD, DNAT,

INPUT и SNAT.

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, portmapper).

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. Для включения автоматического SNAT локальных сетей, переведите соответствующую опцию в положение включен.
Пользовательские правила SNAT приоритетнее автоматического SNAT 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 **Сохранить**. 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: 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.

Описание параметров и действий при создании правил:

- **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**;
- **Источник** - 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);

- **Зона источника** - интерфейс или группа интерфейсов, из которой 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.

Назначение

- **Инвертировать назначение** - позволяет использовать в правиле все объекты, кроме выбранных в строке **Назначение**;
- **Назначение** - 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);
- **Зона назначения** - интерфейс или группа интерфейсов, в которую входит трафик. Можно выбрать отдельные **Сетевые интерфейсы**, созданные пользователем зоны или **Специальные** типы;
- **Порт назначения** - указывается при создании правила с протоколами TCP/UDP. Это может быть отдельный порт, список портов или диапазон портов, определенных в *Объектах*;
- **Сменить IP-адрес назначения** - при указании диапазона адресов пакет будет перенаправлен на любой из них.

Действия

- **Запретить** - запрещает трафик;
- **Разрешить** - разрешает трафик;
- **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;
- **SNAT** - транслирует адреса источника;
- **Не производить SNAT** - отменяет действие SNAT для трафика, удовлетворяющего критериям правила.

Дополнительно

- **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.

Примеры

Настройка правил файрвола для IPsec-подключений:

Чтобы настроить правило файровола 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:

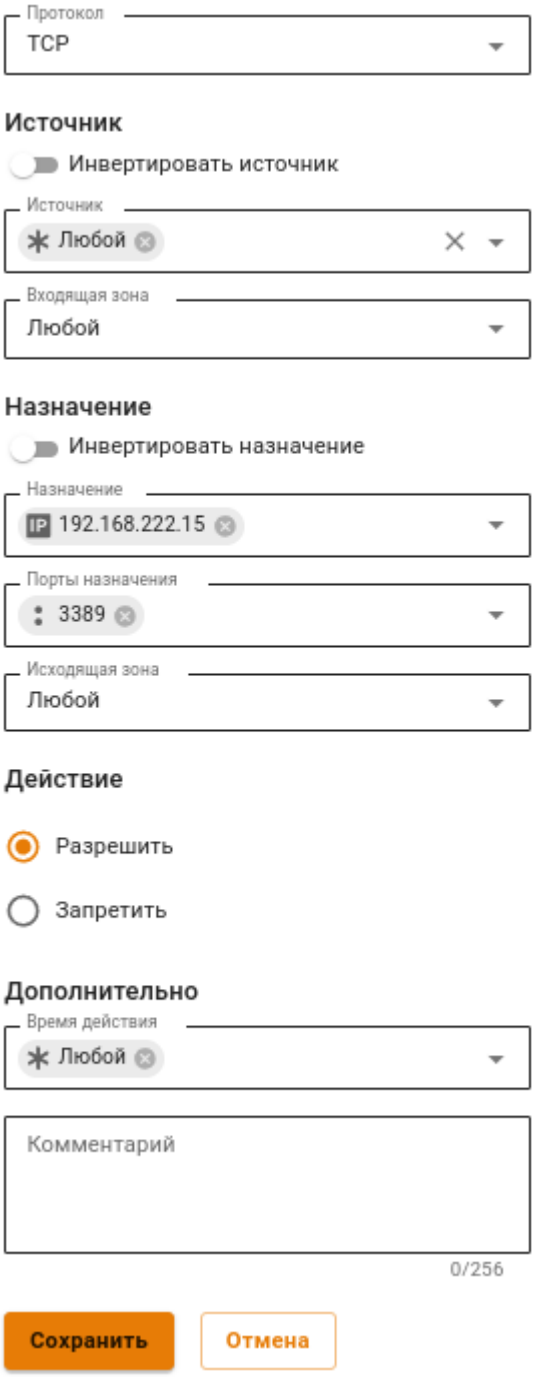
Вопросы блокировки различных ресурсов: программ удаленного управления (AmmyAdmin и TeamViewer), мессенджеров и другого ПО описаны в разделе *Блокировка популярных ресурсов*.

Доступ к терминальному серверу для определенного пользователя:

1. Во вкладке **Forward** нажмите **Добавить**;

2. Заполните следующие поля:

- **Протокол** - выберите TCP;
- **Источник** - выберите пользователя или группу пользователей;
- **Назначения** - укажите адрес терминального сервера;
- **Порты назначения** - укажите порт 3389 ;
- **Действие** - Разрешить.



3. Нажмите **Сохранить**.

15.1.3 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.

Также необходимо, чтобы действие в сработавшем правиле файрвола было среди **Действий для логирования** во вкладке **Логирование**. Иначе срабатывание логироваться не будет.

Далее трафик проходит через правила в *таблицах файрвола*. Если при срабатывании правила на трафике

стояла метка логирования и действие соответствовало выборке **Действий для логирования**, то в логи попадают:

- стандартные поля логирования;
- атрибуты пакета, с которым произошло событие (протокол, порты и IP-адреса);
- название таблицы файрвола;
- идентификатор правила файрвола;
- действие, которое произошло.

Логи записываются в системный журнал. В том числе эти сообщения могут отправляться через *syslog*.

Подсказка: Включите опцию **Логировать срабатывания правил** для начала логирования.

Такая система ограничений нужна для исключения неподходящих правил файрвола из логирования. Логирование всех срабатываний правил файрвола требует дополнительных ресурсов на сервере и затрудняет отладку правил. Если для нормальной работы логирование не требуется, рекомендуем его отключить.

Действия для логирования

Выберите действия правил **Файрвола**, которые требуется логировать, нажав на  .

> **Внимание:** Если ни одно действие во вкладке **Логирование** не выбрано, срабатывания правил логироваться не будут.

Трафик для логирования

Создайте 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**.

Применение правил для отметки трафика, подлежащего проверке, проходит всегда по всем правилам до конца этой таблицы.

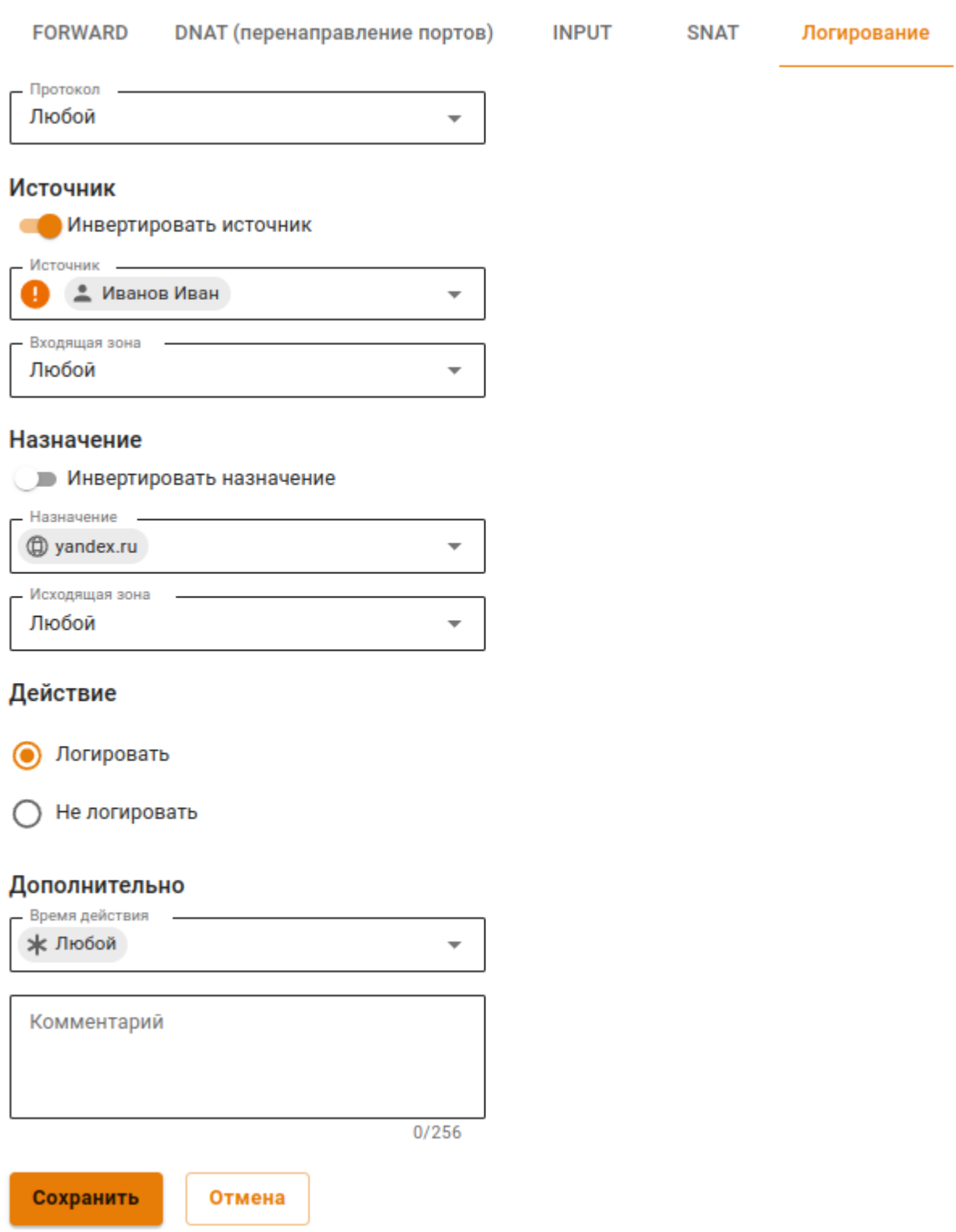
Таким образом, предоставляется возможность гибкой выборки трафика, который подлежит логированию.

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**:


FORWARD
DNAT (перенаправление портов)
INPUT
SNAT
Логирование
Протокол
Любой
Источник
Инвертировать источник
Источник
Иванов Иван
Входящая зона
Любой
Назначение
Инвертировать назначение
Назначение
yandex.ru
Исходящая зона
Любой
Действие
Логировать
Не логировать
Дополнительно
Время действия
Любой
Комментарий
0/256
Сохранить
Отмена

15.2 Контроль приложений

Подсказка: Название службы раздела *Контроля приложений*: `ideco-app-backend` и `ideco-app-control@Leth<номер локального интерфейса>`.
Список имен служб для других разделов доступен по *ссылке*.

Подсказка: Правила разделов *Предотвращения вторжений*, *Контроля приложений* и *Ограничение скорости* не обрабатывают трафик между локальными сетями и сетями филиалов.

Для исключения пользователя или групп пользователей из обработки этих разделов добавьте соответствующее правило в
Правила трафика -> Исключения.

Установленные во время отключения раздела **Контроля приложений** сессии не будут разорваны при включении модуля.

Статус модуля можно посмотреть, нажав на стрелку в верхней части экрана около надписи **Контроль приложений**:

При нажатии раскроется список модулей с их статусами.

Раздел работает только в редакции Enterprise у пользователей с активной подпиской на обновления и техническую поддержку, а также в редакции Ideco SMB с приобретенным модулем.

Принцип действия набора правил:
Ideco NGFW анализирует трафик, ищет правило, которое подходит к этому трафику из списка, и применяет его. Если в списке есть несколько правил с одними и теми же условиями (колонки **Применяются для** и **Протоколы**), но разными действиями (колонка **Действие**), то будет применено правило, стоящее выше по списку.

Внимание: При отключении раздела **Контроль приложений** в правом верхнем углу:

- Статистика по трафику, предоставляемая этим разделом, перестанет появляться в разделе **Отчеты и журналы ->Трафик**;
- Перестанет работать раздел **Монитор трафика**.

Подсказка: Рекомендуем указывать на устройствах пользователя в качестве DNS-сервера Ideco NGFW, а не иной DNS-сервер в локальной сети (например, контроллер домена). Иначе Контроль приложений может некорректно определять тип протокола приложений, использующих HTTPS как транспортный протокол.
Причина в том, что Ideco NGFW будет получать DNS-запрос от DNS-сервера, а не от устройства пользователя.

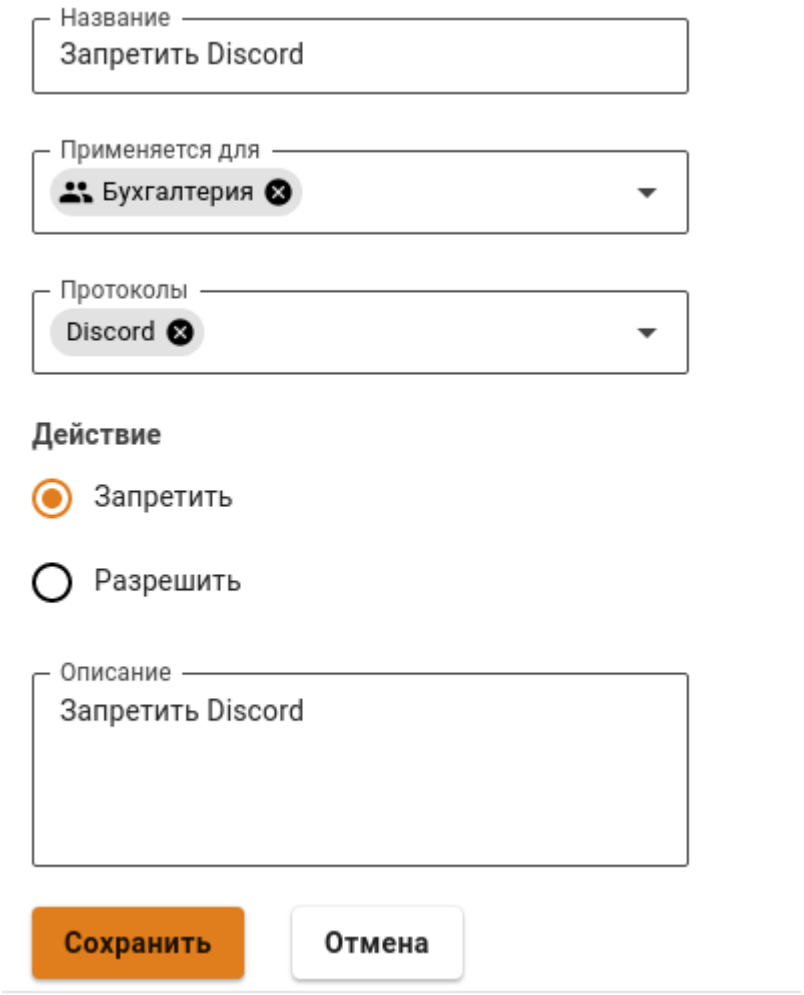
15.2.1 Создание правил

Предупреждение: Не рекомендуем создавать в **Контроле приложений** наиболее приоритетное запрещающее правило со значениями **Любой** в полях **Применяется для** и **Протокол**. Это приведет к тому, что веб-интерфейс NGFW и доступ к серверу по SSH станут недоступны.

Правила настраиваются в разделе **Правила трафика -> Контроль приложений**.

Чтобы создать новое правило, выполните действия:

1. Нажмите **Добавить** в левом верхнем углу экрана:



2. Укажите значения следующих параметров:

- **Название** - введите название правила для удобства администрирования;
- **Применяется для** - можно выбрать объекты следующих типов: пользователь, группа пользователей, IP-адрес, диапазон IP-адресов, подсеть, список IP-адресов или специальный объект **Превышена квота** (в этот объект попадают пользователи превысившие квоту по трафику);
- **Протоколы** - выберите протокол(ы) 7-го уровня (приложения) из списка;
- **Действие** - разрешить или запретить выбранный протокол.

3. Нажмите **Сохранить**.

Подсказка: О блокировке программ удаленного доступа, анонимайзеров, торрентов и других популярных ресурсов смотрите в статье *Блокировка популярных ресурсов*.

Описание протоколов, распознаваемых модулем:

FTP_CONTROL
Протокол, предназначенный для передачи файлов в компьютерных сетях.

POP3
Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP.

SMTP
Протокол, предназначенный для передачи электронной почты.

IMAP
Протокол для доступа к электронной почте.

DNS
Протокол, используемый для получения IP адреса хоста по его доменному имени.

IPP
Протокол, используемый для передачи документов на печать.

HTTP
Протокол для получения с серверов гипертекстовых документов в формате HTML.

MDNS
Многоадресный протокол DNS, используемый для преобразования имени хостов в IP-адреса в небольших сетях, не включающих локальный сервер имен.

NTP
Протокол для синхронизации внутренних часов компьютера.

NetBIOS
Протокол, используемый для обнаружения компьютеров в сети.

NFS
Протокол сетевого доступа к файловым системам.

SSDP
Протокол, служащий для объявления и обнаружения сетевых сервисов.

BGP
Протокол динамической маршрутизации.

SNMP
Протокол для управления устройствами в IP-сетях.

XDMCP
Протокол аутентификации между X-сервером и X-клиентом.

SMBv1
Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети.

Syslog
Протокол отправки и регистрации сообщений о происходящих в системе событиях.

DHCP
Протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети.

PostgreSQL
Протокол, используемый для взаимодействия клиентов и серверов PostgreSQL.

MySQL
Протокол, используемый для взаимодействия клиентов и серверов MySQL.

COAP
Протокол для взаимодействия простых устройств, например, датчиков малой мощности, выключателей, клапанов, которые управляются или контролируются удаленно через интернет.

SMTPS
Протокол для передачи электронной почты, включающий в себя обязательное шифрование.

POPS
Протокол, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP, включающий в себя обязательное шифрование.

DTLS
Протокол передачи данных, обеспечивающий защищенность соединений для протоколов, использующих датаграммы.

Gnutella
Протокол для распределенного обмена файлами, в основном, музыкальными.

BitTorrent
Пиринговый протокол для кооперативного обмена файлами через интернет.

Signal
Криптографический протокол, созданный для обеспечения сквозного шифрования голосовых вызовов, видеозвонков и мгновенных сообщений.

Memcached
Протокол кэширования, используемый для ускорения динамических веб-приложений путем кэширования данных в памяти.

SMBv23
Протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети.

Mining
Протоколы, использующиеся программами-майнерами.

Modbus
Протокол, основанный на архитектуре ведущий - ведомый, применяется в промышленности для организации связи между электронными устройствами.

WhatsAppCall
Протокол голосовой передачи, основанный на VoIP.

QQ
Протокол мгновенного обмена сообщениями.

IMAPS
Протокол для осуществления доступа к электронной почте, включающий в себя обязательное шифрование.

IceCast
Протокол для организации потокового цифрового аудио и видеовещания.

Zattoo
Телевизионная платформа, которая предлагает прямые телетрансляции и контент по запросу для компьютеров, мобильных телефонов, планшетов и других сетевых устройств.

TVUplayer
Протокол, используемый для просмотра телевидения через интернет.

MongoDB
Протокол, используемый для взаимодействия клиентов и серверов MongoDB.

OCSP
Протокол, используемый для получения статуса отзыва цифрового сертификата X.509.

VXLAN
Протокол инкапсуляции, который обеспечивает подключение центров обработки данных с использованием туннелирования для расширения соединений канального уровня в используемой сети сетевого уровня.

IRC
Протокол прикладного уровня для обмена сообщениями в режиме реального времени.

Jabber
Протокол, основанный на XML, свободный для использования протокол для мгновенного обмена сообщениями и информацией о присутствии в режиме, близком к режиму реального времени.

Nats
Протокол обмена сообщениями.

VRRP
Протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию.

Telnet
Протокол для реализации текстового терминального интерфейса по сети.

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.

IPSec
Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

GRE
Протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems.

EGP
Устаревший протокол обмена информации между маршрутизаторами нескольких автономных систем.

IP_in_IP
Протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет.

RTP
Протокол, используемый при передаче трафика реального времени.

RDP
Протокол удаленного рабочего стола.

VNC
Протокол удаленного доступа к рабочему столу.

Tumblr
Протокол микроблогов, включающий в себя множество картинок, статей, видео и gif-изображений по разным тематикам и позволяющий пользователям публиковать посты в их тамблелог.

TLS
Протокол защиты транспортного уровня.

SSH
Протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.

Usenet
Протокол, используемый для общения и публикации файлов.

MGCP
Протокол управления медиашлюзами.

IAX
Протокол обмена VoIP-данными между IP-АТС Asterisk и другим аналогичным софтсвичом или VoIP-телефоном.

AFP
Протокол представительского и прикладного уровней сетевой модели OSI, предоставляющий доступ к файлам в MacOS X.

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).

ICMPV6
Протокол управляющих сообщений для межсетевого протокола версии 6.

DHCPV6
Протокол динамического конфигурирования хостов для межсетевого протокола версии 6.

Kerberos
Протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.

LDAP
Протокол для доступа к службе каталогов X.500.

PPTP
Туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищенное соединение с сервером за счет создания специального туннеля в стандартной, незащищенной сети.

NetFlow
Протокол, предназначенный для учета сетевого трафика, разработанный компанией Cisco Systems.

sFlow
Протокол, используемый для сбора, отправки и анализа информации о сетевом трафике в целях мониторинга.

CHECKMK
Протокол используется для мониторинга серверных и контейнерных систем в ИТ-инфраструктуре.

AJP
Протокол, который может проводить входящие запросы с веб-сервера до сервера приложений, который находится позади веб-сервера.

RADIUS
Протокол удаленной аутентификации пользователей, представляет собой ключевой элемент в обеспечении безопасности и управлении доступом в сетях.

SAP
Протокол позволяет сетевым устройствам постоянно корректировать данные о том, какие сервисные услуги имеются сейчас в сети.

GTP
Протокол туннелирования GPRS.

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..

LLMNR
Протокол, основанный на формате пакета данных DNS, который позволяет компьютерам выполнять разрешение имен хостов в локальной сети.

H323
Набор стандартов для передачи мультимедиа-данных по сетям с пакетной передачей.

OpenVPN
Протокол VPN с открытым исходным кодом.

CiscoVPN
Протокол VPN, разработанный компанией Cisco Systems.

Tor
Протокол анонимной сети виртуальных туннелей, предоставляющий передачу данных в зашифрованном виде.

RTCP
Протокол управления передачей в реальном времени.

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).

RTMP
Проприетарный протокол потоковой передачи данных, в основном используемый для передачи потокового видео и аудиопотоков с веб-камер через интернет.

QUIC
Экспериментальный интернет-протокол, позволяющий мультиплексировать несколько потоков данных меж-

ду двумя компьютерами, работая поверх протокола UDP, и содержит возможности шифрования, эквивалентные TLS и SSL.

AMQP
Открытый протокол прикладного уровня для передачи сообщений между компонентами системы.

MPEG_TS
Протокол для передачи аудио и видеоданных, описанным в MPEG2.

SMPP
Протокол одноранговой передачи коротких сообщений.

DNScrypt
Протокол шифрования DNS-трафика.

TINC
Открытый, самомаршрутизирующийся сетевой протокол и программная реализация, используемая для сжатых и зашифрованных виртуальных частных сетей.

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.

MQTT
Упрощенный сетевой протокол, работающий поверх, ориентированный на обмен сообщениями между устройствами по принципу «издатель - подписчик».

OpenDNS
Протокол, предоставляющий общедоступные DNS-серверы.

DRDA
Набор протоколов, обеспечивающих возможность связи между программами и системами баз данных на разных платформах и позволяющих распределять реляционные данные по нескольким платформам.

FIX
Протокол передачи данных, являющийся международным стандартом для обмена данными между участниками биржевых торгов в режиме реального времени.

Diameter
Сеансовый протокол, созданный, отчасти, для преодоления некоторых ограничений протокола RADIUS.

DNP3
Протокол передачи данных, используемый для связи между компонентами АСУ ТП.

IEC60870
Набор протоколов для контроля и управления с использованием постоянного соединения.

CAPWAP
Сетевой протокол с возможностью взаимодействия, который позволяет центральному контроллеру доступа к беспроводной локальной сети управлять набором беспроводных оконечных точек.

WebSocket
Протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером, используя постоянное соединение.

SOAP
Протокол обмена структурированными сообщениями в распределенной вычислительной среде.

Z3950
Клиент-серверный протокол для поиска и получения информации с удаленных компьютерных баз данных.

GTP_U
Протокол используется для транспортировки пользовательских данных между пакетной сетью и радиосетью.

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.

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.

HSRP
Протокол маршрутизации семейства FHRP (англ. First-hop redundancy protocols), разработанный компанией Cisco и стандартизованный в RFC 2281.

MpegDash
Протокол потоковой передачи данных, предоставляющая возможность доставки потокового мультимедиаконтента через интернет по протоколу HTTP.

PGM
Протокол надежной многоадресной передачи данных.

IP_PIM
Семейство многоадресных протоколов маршрутизации для IP сетей, созданное для решения проблем групповой маршрутизации.

FastCGI
Клиент-серверный протокол взаимодействия веб-сервера и приложения, дальнейшее развитие технологии CGI.

FTPS
Расширение широко используемого протокола передачи файлов FTP, которое добавляет поддержку для криптографических протоколов уровней транспортной безопасности и защищенных сокетов.

NAT-PMP
Сетевой протокол для автоматической установки параметров преобразования сетевых адресов и конфигураций переадресации портов без участия пользователя.

BACnet
Сетевой протокол, применяемый в системах автоматизации зданий и сетях управления.

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.

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.

Outlook
Персональный информационный менеджер с функциями почтового клиента, входящий в пакет офисных программ Microsoft Office.

VK
Приложение для взаимодействия с социальной сетью ВКонтакте.

Tailscale
VPN-сервис, который работает поверх WireGuard и позволяет получить доступ к контроллеру даже, если у вас нет своего VPN-сервера.

Ntop
Программное обеспечение, которое исследует компьютерную сеть.

PPStream
Китайское программное обеспечение для одноранговой потоковой передачи видео.

YandexMarket
Сервис заказа товаров онлайн.

YandexDisk
Сервис для хранения данных в облаке.

Discord
Кроссплатформенная проприетарная система мгновенного обмена сообщениями с поддержкой VoIP и видеоконференций, предназначенная для использования различными сообществами по интересам.

YandexCloud
Публичная облачная платформа, разработанная российской интернет-компанией Яндекс.

Nats
Система обмена сообщениями с открытым исходным кодом.

AmongUs
Многопользовательская компьютерная игра.

DisneyPlus
Американский сервис потокового вещания типа OTT на основе подписки.

Steam
Онлайн-сервис цифрового распространения компьютерных игр и программ.

HalfLife2
Компьютерная игра, научно-фантастический шутер от первого лица.

WorldOfWarcraft
Массовая многопользовательская ролевая онлайн-игра.

YandexMetrika
Бесплатный сервис веб-аналитики, предлагаемый Яндексом, который отслеживает и сообщает о трафике веб-сайта.

YandexDirect
Сервис для размещения объявлений контекстной рекламы на Яндексе и на сайтах-партнерах его рекламной сети.

Armagetron
Свободная компьютерная игра для операционных систем Linux, Windows, MacOS, FreeBSD и AmigaOS 4.

Warcraft3
Компьютерная игра в жанре стратегии в реальном времени с элементами RPG.

Facebook
Крупнейшая социальная сеть в мире, которой владеет компания Meta Platforms.

Twitter
Американский сервис микроблогов и социальная сеть, в которой пользователи публикуют сообщения и взаимодействуют с ними.

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.

GoogleMaps
Набор приложений, построенных на основе бесплатного картографического сервиса и технологии, предоставляемых компанией Google.

YouTube
Видеохостинг, предоставляющий пользователям услуги хранения, доставки и показа видео.

Citrix
Программа, предоставляющая доступ к приложениям и рабочим столам с удаленного клиентского устройства с помощью ресурсов Citrix Virtual Apps and Desktops и Citrix DaaS.

Netflix
Стриминговый сервис фильмов и сериалов.

LastFM
Сервис для прослушивания музыки онлайн.

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.

Hulu
Стриминговый сервис по подписке, принадлежащий The Walt Disney Company.

WhatsApp
Американский бесплатный сервис обмена мгновенными сообщениями и голосовой связи по IP, принадлежащий компании Meta.

Viber
Приложение-мессенджер, которое позволяет отправлять сообщения, совершать видео- и голосовые VoIP-звонки через интернет.

AppleiTunes
Медиаплеер для организации и воспроизведения музыки и фильмов, разработанный компанией Apple и бесплатно распространявшийся для платформ MacOS и Windows.

WindowsUpdate
Сервис обновления операционной системы Windows.

Skype_TeamsCall
Бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее текстовую, голосовую и видеосвязь через интернет между компьютерами, опционально используя технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны.

Teams
Корпоративная платформа, объединяющая в рабочем пространстве чат, встречи, заметки и вложения.

Slack
Корпоративный мессенджер.

TeamViewer
Программное обеспечение для удаленного доступа, удаленного управления и удаленного обслуживания компьютеров и других конечных устройств.

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.

TocaBoca
Интерактивная мобильная игра.

Spotify
Стриминговый сервис, позволяющий легально прослушивать музыкальные композиции, аудиокниги и подкасты, не скачивая их на устройство.

Messenger
Приложение для обмена мгновенными сообщениями и видео, созданное Meta.

Telegram
Кроссплатформенная система мгновенного обмена сообщениями с функциями обмена текстовыми, голосовыми и видеосообщениями, а также стикерами, фотографиями и файлами многих форматов.

Vevo
Музыкальный видеосайт и видеохостинг.

Zoom
Проприетарная программа для организации видеоконференций, разработанная компанией Zoom Video Communications.

KakaoTalk
Бесплатное мобильное приложение для мгновенного обмена сообщениями для смартфонов.

Twitch
Видеостриминговый сервис, специализирующийся на тематике компьютерных игр, в том числе на трансляциях геймплея и киберспортивных турниров.

WeChat
Мобильная коммуникационная система для передачи текстовых и голосовых сообщений, разработана китайской компанией Tencent.

Snapchat
Мобильное приложение обмена сообщениями с прикрепленными фото и видео.

GitHub
Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки.

IFLIX
Малайзийский бесплатный видеосервис.

Deezer
Французский интернет-сервис потоковой передачи музыки.

Instagram
Американская социальная сеть для обмена фотографиями и видео.

StarCraft
Серия компьютерных игр в жанре стратегии в реальном времени, разработанная компанией Blizzard Entertainment.

HotspotShield
Условно-бесплатное программное обеспечение для организации виртуальной частной сети, обеспечивающей безопасную передачу данных по шифрованному соединению, защищенному от прослушивания.

IMO
Веб-сервис и кроссплатформенное приложение для мгновенного обмена сообщениями и VoIP-звонков.

GoogleDrive
Сервис хранения, редактирования и синхронизации файлов, разработанный компанией Google. Его функции включают хранение файлов в интернете, общий доступ к ним и совместное редактирование.

MS_OneDrive
Облачное хранилище компании Microsoft. Является частью спектра онлайновых услуг Windows Live.

Pastebin
Веб-приложение, которое позволяет загружать отрывки текста, обычно фрагменты исходного кода, для возможности просмотра окружающими.

Linkedin
Американская социальная сеть для поиска и установления деловых контактов.

ApplePush
Сервис, созданный Apple для отправки уведомлений от сторонних приложений на устройства Apple.

AmazonVideo
Стриминговый сервис компании Amazon.

GoogleDocs
Текстовый онлайн-процессор, входящий в состав бесплатного веб-пакета редакторов GoogleDocs.

Zabbix
Свободная система мониторинга статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

FortiClient
Комплексное решение безопасности, предназначенное для защиты компьютеров и ноутбуков. Также имеет версии для планшетов и мобильных устройств под управлением Android и Apple iOS.

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.

AmazonAWS
Коммерческое публичное облако, поддерживаемое и развиваемое компанией Amazon.

Azure
Облачная платформа компании Microsoft. Предоставляет возможность разработки, выполнения приложений и хранения данных на серверах, расположенных в распределенных дата-центрах.

GoogleCloud
Предоставляемый компанией Google набор облачных служб, которые выполняются на той же самой инфраструктуре, которую Google использует для своих продуктов, предназначенных для конечных потребителей.

RakNet
Кроссплатформенный сетевой сервис, разработанный Oculus VR для использования в игровой индустрии.

Dazn
Спортивный стриминговый сервис.

Psiphon
Бесплатный инструмент для обхода цензуры в интернете с открытым исходным кодом, в котором используется сочетание технологий защищенной связи и обфускации.

UltraSurf
Бесплатная утилита для обхода цензурных ограничений в интернете.

Threema
Кроссплатформенное зашифрованное приложение для обмена мгновенными сообщениями.

AVAST
Семейство антивирусных программ, разработанных компанией Avast для операционных систем Windows, MacOS, Android и iOS.

Syncthing
Приложение, позволяющее синхронизировать файлы между несколькими устройствами.

Line
Приложение для смартфонов и ПК, средство моментального обмена сообщениями.

AppleTVPlus
Американский стриминговый сервис, принадлежащий и управляемый компанией Apple.

Vudu
Потоковый сервис цифрового видео.

Dailymotion
Французский видеохостинг.

TencentVideo
Китайская стриминговая платформа, принадлежащая Tencent.

iHeartRadio
Американская платформа бесплатного вещания, подкастов и потокового радио, принадлежащая iHeartMedia.

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.

TuneIn
Американский аудиопотоковый сервис, транслирующий новости, эфиры радиостанций, спортивные мероприятия, музыку и подкасты.

Munin
Бесплатное программное приложение для мониторинга компьютерных систем, сети и инфраструктуры с открытым исходным кодом.

Elasticsearch
Тиражируемая программная поисковая система.

Heroes_of_the_Storm
Онлайн-игра, разработанная Blizzard Entertainment для Microsoft Windows и MacOS.

Activision
Американская компания по изданию и разработке компьютерных игр, разработчик Call of Duty.

TeslaServices
Портал с сервисной и диагностической информацией для компаний и частных лиц, занимающихся профессиональным обслуживанием и ремонтом автомобилей Tesla.

AppleStore
Онлайн-магазин техники Apple и аксесуаров к ней.

MapleStory
Бесплатная многопользовательская ролевая онлайн-игра, разработанная южнокорейской компанией Wizet.

Kontiki
Платформа доставки видео и контента.

PlayStore
Онлайн-магазин приложений для Android.

1kxun
Китайский видеосервис. На нем представлены различные анимационные фильмы, телевидение, спорт и кино.

Bloomberg
Американская компания, информационное агентство, один из двух ведущих американских поставщиков финансовой информации для профессиональных участников финансовых рынков.

WireGuard
Высокоскоростной и безопасный VPN-протокол.

AccuWeather
Частная американская медиа-компания, предоставляющая коммерческие услуги по прогнозированию погоды по всему миру.

GeForceNow
Облачный игровой сервис компании Nvidia.

TikTok
Сервис для создания и просмотра коротких видео, принадлежащий пекинской компании ByteDance.

Likee
Социальная сеть, пользователи которой могут создавать и распространять короткие музыкальные видео.

Alibaba
Китайская публичная компания, работающая в сфере интернет-коммерции, владелец веб-порталов Taobao.com, Tmall, Alibaba.com и ряда других.

Badoo
Приложение для онлайн-знакомств.

MsSQL-TDS
Протокол прикладного уровня, используемый для передачи данных между сервером базы данных и клиентом.

ETHEREUM
Криптовалюта и платформа для создания децентрализованных онлайн-сервисов на базе блокчейна.

Cachefly
Поставщик сети доставки контента.

eDonkey
Файлообменная сеть, построенная по принципу P2P на основе сетевого протокола прикладного уровня MFTP.

VHUA
Протокол, который использовался для Skype-подобных сервисов в Китае.

GenshinImpact
Компьютерная игра в жанре action-adventure с открытым миром и элементами RPG, разработанная китайской компанией miHoYo Limited.

Thrift
Программный фреймворк Apache Thrift, предназначенный для масштабируемой разработки межъязыковых сервисов.

Dropbox
Файловый хостинг компании Dropbox Inc., включающий персональное облачное хранилище, синхронизацию файлов и программу-клиент.

EpicGames
Американская компания, занимающаяся разработкой компьютерных игр и программного обеспечения, в частности - Fortnite.

TeamSpeak
Компьютерная программа, предназначенная для голосового общения в сети посредством технологии VoIP.

SOMEIP
Автомобильное программное обеспечение, которое может использоваться для передачи управляющих сообщений.

RSYNC
Утилита для удаленной синхронизации и копирования файлов.

OperaVPN
VPN-клиент, встроенный в браузер Opera.

Source_Engine
Игровой сервис, разработанный Valve Corporation для собственного использования и лицензирования другими разработчиками.

Service_Location_Protocol
Протокол обнаружения сервисов, который позволяет компьютерам и иным устройствам находить сервисы в локальной сети без предварительной конфигурации.

AVASTSecureDNS
Сервис защищенных DNS-серверов от компании Avast.

iCloudPrivateRelay
Сервис для маскировки IP-адреса пользователя с целью сохранения его конфиденциальности.

Salesforce
Американская компания, разработчик одноименной CRM-системы, предоставляемой по модели SaaS.

PTPv2
Протокол синхронизации для промышленных сетей.

RTSP
Потоковый протокол реального времени, предназначенный для использования в системах, работающих с мультимедийными данными и позволяющий удаленно управлять потоком данных с сервера.

ZeroMQ
Высокопроизводительная асинхронная библиотека обмена сообщениями, ориентированная на использование в распределенных и параллельных вычислениях.

TFTP
Простой протокол передачи файлов, как правило, используется при загрузке бездисковых систем.

OPC-UA
Программный интерфейс для промышленного протокола связи и модели данных. Используется для связи между конечными устройствами различных производителей по принципу клиент/сервер.

HTTP2
Вторая крупная версия сетевого протокола HTTP, используемая для доступа к World Wide Web.

SCTP
Протокол управления потоком передачи с установлением соединения, как TCP, но передающий данные сообщениями, как UDP.

Crashlytics
Инструмент отчетности о сбоях, который помогает выявлять ошибки.

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.

Fuze
Файловая система в пользовательском пространстве для Unix-подобных операционных систем, позволяющая непривилегированным пользователям создавать собственные файловые системы без редактирования кода ядра.

YandexMail
Почтовый сервис от компании Яндекс.

MerakiCloud
Сервис компании Cisco, предоставляющий доступ к облачным технологиям.

HAProxy
Программное обеспечение для обеспечения высокой доступности и балансировки нагрузки для TCP и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов.

Amazon
Американская компания-разработчик платформ электронной коммерции и публично-облачных вычислений.

FbookReelStory
Короткие видеоролики на Facebook.

Microsoft
Американская корпорация-разработчик в сфере проприетарного программного обеспечения для различного рода вычислительной техники - персональных компьютеров, игровых приставок, КПК, мобильных телефонов и прочего.

SiriusXMRadio
Американская радиовещательная компания в сфере спутникового радио и онлайн-радио.

Corba
Технологический стандарт написания распределенных приложений, продвигаемый консорциумом OMG, и соответствующая ему информационная технология.

OCS
Спецификация программных интерфейсов класса REST для интеграции социальных интернет-коммуникаций в среды рабочего стола.

AnyDesk
Приложение для удаленного рабочего стола, распространяемое AnyDesk Software GmbH.

OICQ
Распространенный в Китае сервис мгновенного обмена сообщениями.

LineCall
Система звонков/видеоконференций, используемая в популярном мобильном приложении для обмена сообщениями LINE.

Sina
Китайская интернет-компания, владеет аналогом Twitter - сервисом Sina Weibo.

Livestream
Платная стриминговая платформа, которая позволяет клиентам загружать живое видео со своих мобильных устройств и компьютерных камер через интернет.

YandexMusic
Стриминговый сервис компании Яндекс, позволяющий слушать музыкальные композиции, их подборки, альбомы.

Pinterest
Социальный интернет-сервис, фотохостинг, позволяющий пользователям добавлять в режиме онлайн-изображения.

KakaoTalk_Voice
Популярный в Южной Корее мессенджер, который поддерживает мгновенную передачу сообщений, позволяет отправлять файлы, а также совершать аудио и видео-звонки.

OSPF
Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала.

Controller_Area_Network
Стандарт протокола связи, используемый для обмена данными между устройствами в автомобильной промышленности и других промышленных приложениях.

Skype_Teams
Сервис Microsoft, предназначенный для командной работы и обмена информацией между участниками проекта или команды.

Crossfire
Южнокорейский тактический сетевой шутер от первого лица, разработанный компанией SmileGate.

WhatsAppFiles
Протокол загрузки медиафайлов (изображений, видео, музыки, документов) мессенджера WhatsApp.

GoogleServices
Набор приложений и API, которые реализуют дополнительные возможности на устройствах Android. Сервисы Google для мобильных устройств включают основные приложения, такие как Google Play, Gmail, Google Map, YouTube и Chrome.

Vimeo
Американский сервис для публикации и просмотра видео.

Edgecast
Децентрализованное приложение для потоковой передачи видео, построенное на собственной технологии блокчейн THETA со смарт-контрактами.

TuyaLP
Протокол Tuya LAN используется для взаимодействия многих IoT-устройств, включая светодиодные лампы, лампочки, умные розетки и другое.

S7Comm
Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400.

Webex
Американская компания, которая разрабатывает и продает приложения для веб-конференций, видеоконференцсвязи и контакт-центра как сервиса.

i3D
Протокол с низкой задержкой, используемый в основном игровыми серверами.

RiotGames
Американская компания, разработчик видеоигр, издатель и организатор киберспортивных турниров (League of Legends).

SignalVoip
Протокол голосовой связи в мессенджере Signal.

Roblox
Игровая онлайн-платформа и система создания игр, позволяющая любому пользователю создавать свои собственные и играть в созданные другими игры.

TPLINK_SHP
Протокол TP-Link Smart Home Protocol используется для подключения устройств «Умного дома» с помощью приложения-компаньона.

Apple
Компания-производитель смартфонов и компьютерной техники.

Cassandra
Распределенная система управления базами данных, относящаяся к классу NoSQL-систем и рассчитанная на создание масштабируемых хранилищ данных, представленных в виде хеша.

Cloudflare
Американская компания, предоставляющая услуги CDN, защиту от DDoS-атак, безопасный доступ к ресурсам и серверы DNS.

TruPhone
Глобальная мобильная сеть, которая занимается разработкой технологии eSim, позволяющей подключаться к разным провайдерам без замены сим-карты.

BJNP
Протокол обнаружения служб локальной сети, используемый принтерами и сканерами Canon. Компьютерные системы используют этот протокол для автоматического обнаружения устройств Canon в сети.

HTTP_Connect
Метод HTTP, который запускает двустороннюю связь с запрошенным ресурсом. Метод можно использовать для открытия туннеля.

UMAS
Unified Messaging Application Services - проприетарный протокол Schneider Electric, который используется для конфигурации, мониторинга сбора данных и управления промышленными контроллерами Schneider Electric.

IGMP
Протокол управления групповой передачей данных в сетях, основанных на протоколе IP. Используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы.

Whois-DAS
Сетевой протокол прикладного уровня, базирующийся на протоколе TCP, применяется для получения регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем.

Yahoo
Американская компания, специализирующаяся на проектах и услугах в интернете. Владеет поисковой системой с одноименным названием.

DirecTV
Компания прямого теле-радиовещания в США, сигналы цифрового спутникового телевидения и радио передаются на территорию США и Латинской Америки.

eBay
Американская компания, предоставляющая услуги в областях интернет-аукционов и интернет-магазинов.

Mullvad
Сервис по поставке услуг виртуальной частной сети (VPN) с открытым исходным кодом, работает с использованием протоколов WireGuard и OpenVPN.

Tencent
Китайский конгломерат, создавший китайский клон ICQ, собственную валюту, отдельную соцсеть, множество игр, торговую площадку и WeChat.

HBO
Американский телеканал, принадлежащий компании WarnerMedia.

WorldOfKungFu
3D MMORPG с боевыми искусствами, основанная на традиционной китайской культуре.

Oracle
Американская компания, специализируется на выпуске систем управления базами данных, связующего программного обеспечения, бизнес-приложений.

BITCOIN
Криптовалюта, использующая децентрализованную систему для записи транзакций в блокчейне.

ICMP
Протокол третьего уровня модели OSI, который используется для диагностики проблем со связностью в сети.

EtherSIO
Протокол используется для передачи данных между программируемыми логическими контроллерами и удаленными устройствами ввода/вывода производства компании Saia-Burgess Controls Ltd.

RMCP
Протокол многоадресной передачи с ретрансляцией для предоставления услуг сквозной многоадресной передачи данных по сетям на базе IP-протокола.

Tuenti
Испанская закрытая социальная сеть, в которую можно попасть только по приглашению частного характера.

CloudflareWarp
Бесплатный VPN от CloudFlare, который проксирует все сетевые запросы в системе (включая обновления Windows и др. ПО, трафик многопользовательских игр, торренты).

SnapchatCall
Протокол голосовой передачи, основанный на VoIP, в мессенджере Snapchat.

Playstation
Игровая приставка пятого поколения, разработанная компанией Sony Computer Entertainment.

CPHA
Алгоритм хеширования, который может использоваться для безопасного хранения паролей в PTC.

Ookla
Американская компания, которая владеет сервисом по измерению скорости интернета Speedtest.

HTTP_Proxy
Тип прокси-сервера, который действует как сервер-посредник между клиентом и веб-сервером.

Megaco
Протокол для управления функциями шлюза на границе пакетной сети.

Reddit
Сайт, сочетающий черты социальной сети и форума, где зарегистрированные пользователи могут размещать ссылки на понравившуюся информацию в интернете и обсуждать ее.

RTPS
Real Time Streaming Protocol - потоковый протокол реального времени - позволяет управлять вещанием: выполнять несколько команд, такие как «старт», «стоп», «переход на определенное время».

Nvidia
Американская технологическая компания, разработчик графических процессоров и систем на чипе (SoC).

Nintendo
Японская компания, специализирующаяся на создании видеоигр и игровых систем.

FTP_DATA Протокол доступа, предназначенный для удаленной передачи файлов в компьютерных сетях.

GoogleClassroom
Облачная платформа для организации образовательного процесса.

RX
Клиент-серверный RPC-протокол, расширенная и объединенная версия старых протоколов R и RFTP.

SD-RTN
Software Defined Real-time Network - собственный протокол компании Agora, предназначен для потоковой передачи данных с низкой задержкой.

FINS
Открытый протокол связи поддерживаемый большинством контроллеров и сетей разработки компании Omron.

TelegramVoip
Голосовые и видеозвонки в мессенджере Telegram.

AliCloud
Компания, предоставляющая ресурсы для облачных вычислений, дочерняя компания Alibaba Group.

Microsoft365
Программный продукт от компании Microsoft. Набор веб-сервисов на основе платформы Microsoft Office, электронная почта, функции для общения и управления документами, которые распространяется на основе подписки по схеме «программное обеспечение как услуга».

Guildwars
Фэнтезийная массовая многопользовательская ролевая онлайн-игра, разработанная компанией ArenaNet и выпущенная компанией NCsoft в 2005 году.

FacebookVoip
Голосовые и видеозвонки в FaceBook.

AppleSiri
Облачный персональный помощник и вопросно-ответная система компании Apple.

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.

Wikipedia
Самая крупная в мире онлайн-энциклопедия.

Softether
Бесплатное кроссплатформенное многопротокольное программное обеспечение VPN-клиента и VPN-сервера с открытым исходным кодом.

Google
Американская технологическая компания, которая специализируется на поисковых технологиях, искусственном интеллекте, онлайн-рекламе, программном обеспечении, бытовой электронике.

YouTubeUpload
Загрузка файлов на видеохостинг YouTube.

Unknown
Не распознанные модулем протоколы и приложения.

Git
Распределенная система управления версиями.

SinaWeibo
Китайский сервис микроблогов, запущенный компанией Sina Corp.

CNN
Американский круглосуточный кабельный телеканал новостей.

Dofus
Массовая многопользовательская ролевая онлайн-игра (MMORPG), использующая Flash-графику и фэнтезийный сеттинг.

DataSaver
Функция для Chrome, которая позволяет значительно сократить использование мобильных данных.

Xiaomi
Китайская корпорация-производитель смартфонов, компьютерной и бытовой техники.

VMware
Американская компания-разработчик программного обеспечения для виртуализации.

LISP
Протокол маршрутизации, построенный на идее разделения топологического расположения точки присоединения к сети и идентификации узла.

CryNetwork
Составной модуль для создания многопользовательских игр.

AppleiCloud
Облачное хранилище от компании Apple, которое предоставляет пользователям доступ к их музыке, фотографиям, документам и другим файлам с любого устройства.

SoundCloud
Онлайн-платформа и сайт для распространения оцифрованной звуковой информации (например, музыкальных произведений).

UbuntuONE
Онлайн-хранилище, разрабатываемое компанией Canonical, предназначавшееся для обмена файлами и синхронизации между компьютерами и мобильными устройствами.

Pluralsight
Платформа для онлайн-обучения.

GoTo
Американская компания, предоставляющая услуги телефонных систем для бизнеса, контакт-центров и продукты для ИТ-поддержки.

TunnelBear
Кроссплатформенный VPN-клиент.

collectd
Демон Unix, который собирает, передает и хранит данные о производительности компьютеров и сетевого оборудования.

CiscoSkinny
Корпоративный (проприетарный) VoIP-протокол для управления взаимодействием между оконечными телефонными устройствами и сервером телефонной системы (IP-АТС).

ProtonVPN
Сервис по поставке услуг виртуальной частной сети (VPN), управляемый швейцарской компанией Proton AG.

Protobuf
Протокол сериализации (передачи) структурированных данных, предложенный Google как эффективная бинарная альтернатива текстовому формату XML.

Kismet
Сетевой детектор, анализатор пакетов и система обнаружения вторжений для беспроводных локальных сетей стандарта 802.11.

Showtime
Американский кабельный телевизионный канал.

Xbox
Домашняя игровая консоль, разработанная и выпущенная американской корпорацией Microsoft.

Yandex
Российская транснациональная компания в отрасли информационных технологий, владеющая одноименной системой поиска в интернете, интернет-порталом и веб-службами.

AmazonAlexa
Облачная голосовая служба Amazon.

RSH
Протокол, позволяющий подключаться удаленно к устройству и выполнять на нем команды.

NOE
New Office Environment - протокол VoIP, используемый совместимыми телефонными системами Alcatel-Lucent.

Pandora
Тип цифровой криптовалюты.

HP_VIRTGRP
Протокол HP Virtual Machine Group Management - часть пакета виртуализации, используемого в серверных средах HP.

TiVoConnect
Протокол TivoConnect обеспечивает автоматическое обнаружение оборудования для двух или более систем медиаплееров Tivo, работающих в одной сети.

EAQ
Entitade Aferidora da Qualidade de Banda Larga - эксцентричный протокол VoIP/конференц-связи, который редко встречается в реальной жизни.

NestLogSink
Система логирования для домашней системы пожарной безопасности от Google.

Cybersec
Компании сферы кибербезопасности: checkpoint.com norton.com, kaspersky.com, fortinet.com.

ADS_Analytic_Track
Отслеживание и аналитика рекламы (mobile marketing analytics and attribution platform).

TargusDataspeed
проприетарный протокол, используемый для тестирования пропускной способности. Был разработан компанией TARGUSinfo.

UBNTAC2
Утилита управления оборудованием Ubiquiti airControl, версия 2.

GoogleHangoutDuo
Программное обеспечение для мгновенного обмена сообщениями и видеоконференций.

RPC
Протокол, позволяющий программам вызывать функции или процедуры в другом адресном пространстве (на удаленных узлах, либо в независимой сторонней системе на том же узле).

CSGO
Серия компьютерных игр в жанре командного шутера от первого лица, основанная на движке GoldSrc и выросшая из одноименной модификации игры Half-Life.

Redis
Резидентная система управления базами данных класса NoSQL с открытым исходным кодом, работающая со структурами данных типа «ключ - значение».

AdultContent
Сайты и приложения, связанные с контентом «для взрослых».

15.3 Контент-фильтр

Подсказка: Имя юнита контент-фильтра: ideco-content-filter-backend.service.
Список имен юнитов для других разделов доступен по *ссылке*.

Для записи логов поставьте флаг строке **Включить журналирование** в разделе **Сервисы -> Прокси -> Основное**.

Механизм контентной фильтрации работает по принципу проверки принадлежности адреса, запрашиваемого пользователем сайта или отдельной страницы сайта, на наличие его в списках ресурсов. Списки поделены на категории для удобства администрирования.

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.

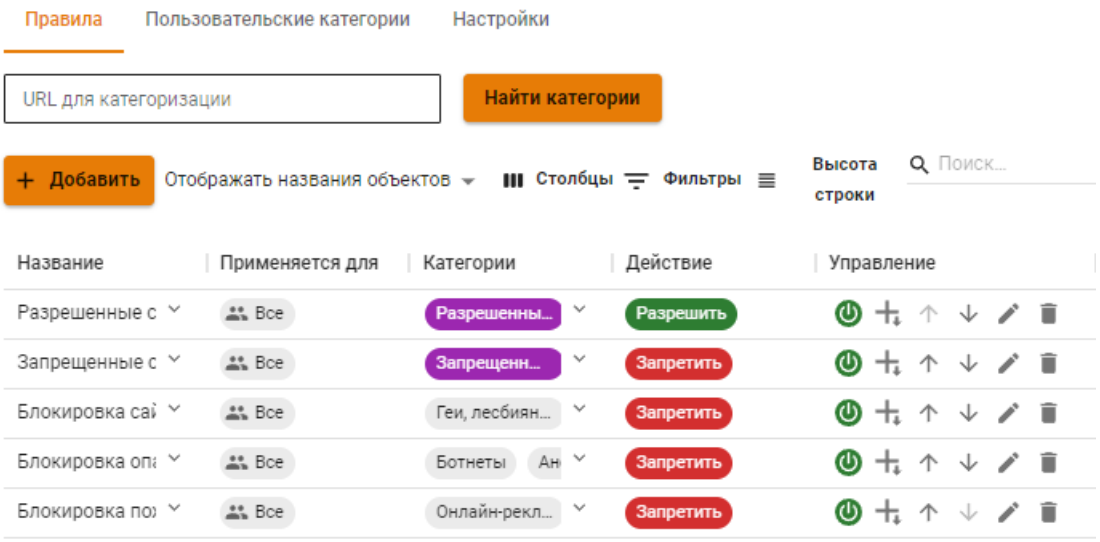
Файрвол анализирует пакет на сетевом уровне (L3), а **Контент-фильтр** - на прикладном уровне (L7). Информация об IP-адресах на прикладном уровне (L7) неточная, поэтому для блокировки IP-адресов нужно использовать **Файрвол**.

Контент-фильтр состоит из трех вкладок: правила, пользовательские категории и настройки.

15.3.1 Правила

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, то будет работать только верхнее правило. Для перемещения правил используйте стрелки ↑ и ↓;
- **Возможность добавления правил в Контент-фильтр.** При добавлении правила требуется заполнить название правила, указать, для кого оно будет применено, и выбрать категорию сайтов. Далее указать, какое действие будет выполняться. Если выбрать действие **Перенаправить на**, то нужно создать аналогичное правило с действием **Расшифровать** и поместить его выше перенаправляющего правила.



Категории сайтов делятся на четыре вида:

1. **Пользовательские**. Включают в себя категории, созданные во вкладке **Пользовательские категории**;

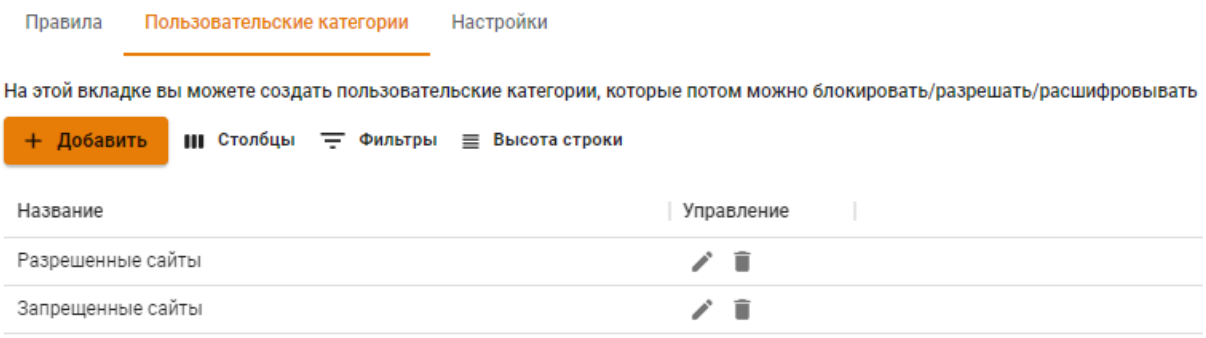
2. **Специальные**. Включает 4 категории: все запросы, все категоризированные запросы, все некатегоризированные запросы и запросы с прямыми обращениями по IP-адресам;

3. **Расширенные**. Правила, включающие в себя расширенные категории, работают только с включенной опцией **Расширенная база категорий** в левом верхнем углу;

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.

15.3.2 Пользовательские категории

На одноименной вкладке создаются собственные категории правил.



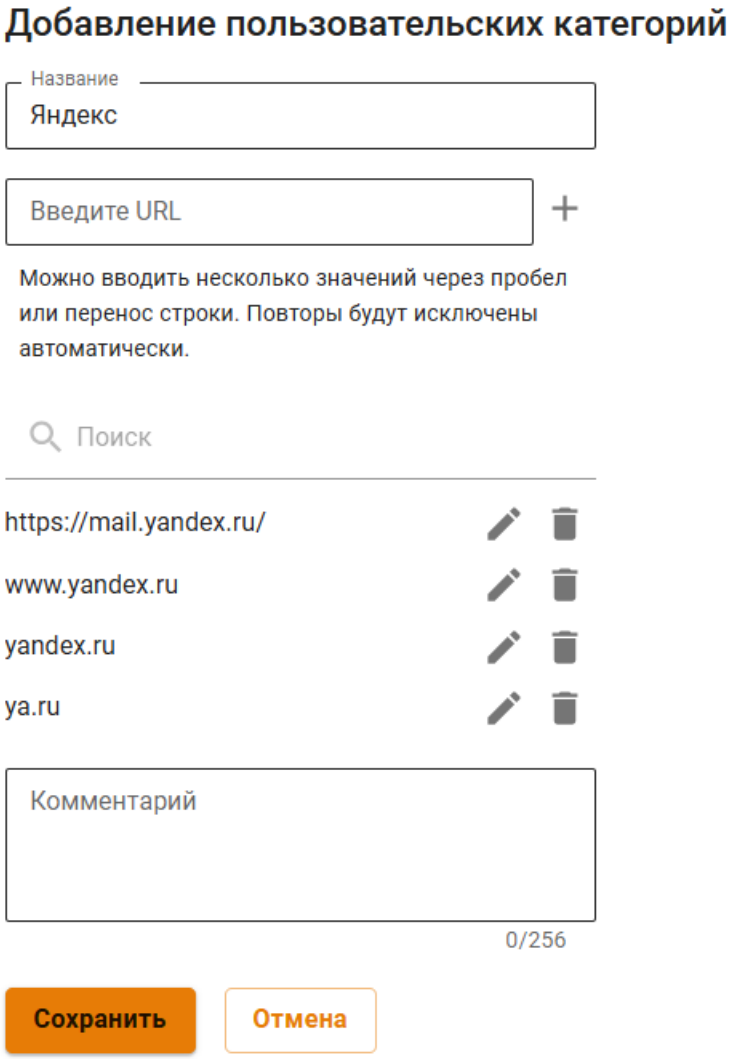
Подробное описание **расширенных** и **специальных** категорий читайте в статье *Описание категорий контент фильтра*.

При создании собственной 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.

Подсказка: Если URL или домен содержит специальные символы (или •), оставьте их в исходном виде. Адрес будут автоматически закодирован в формат punycode.

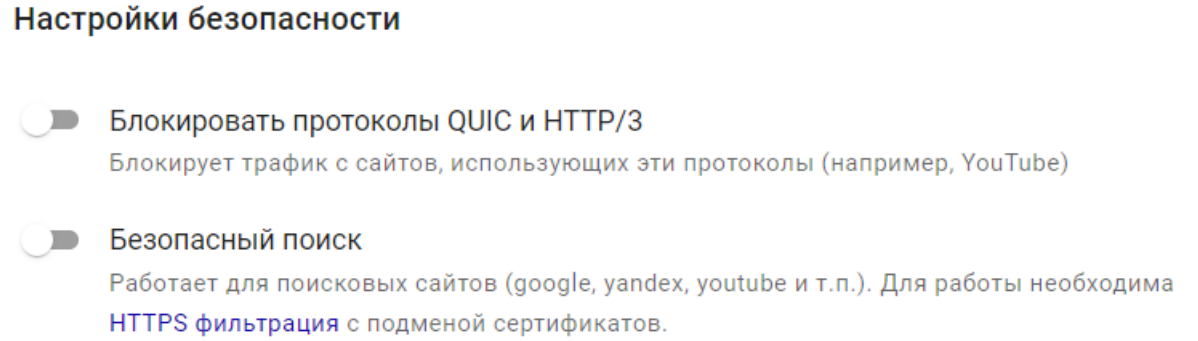
15.3.3 Настройки

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.

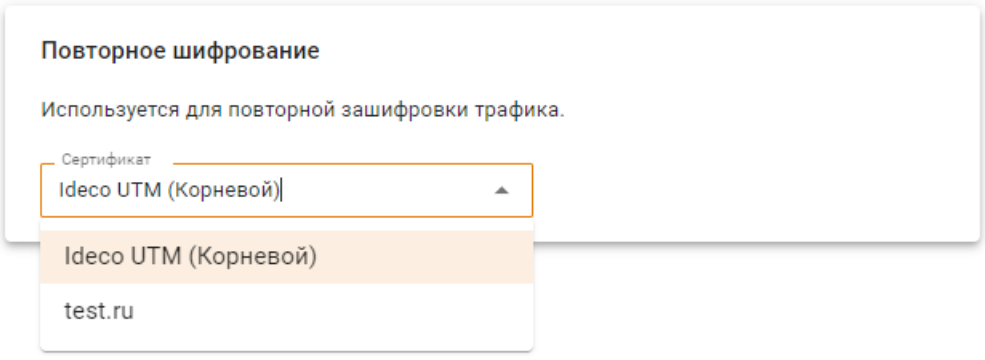
Подсказка: Если отключить опцию **Расширенная база категорий**, то все правила, включающие в себя расширенные категории, перестанут срабатывать.

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;
- **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:



15.3.4 Применение правил

Подсказка: Процесс блокировки ресурсов, взаимодействующих с чат-ботами, описан в *статье*.

Применение правил фильтрации для пользователей:

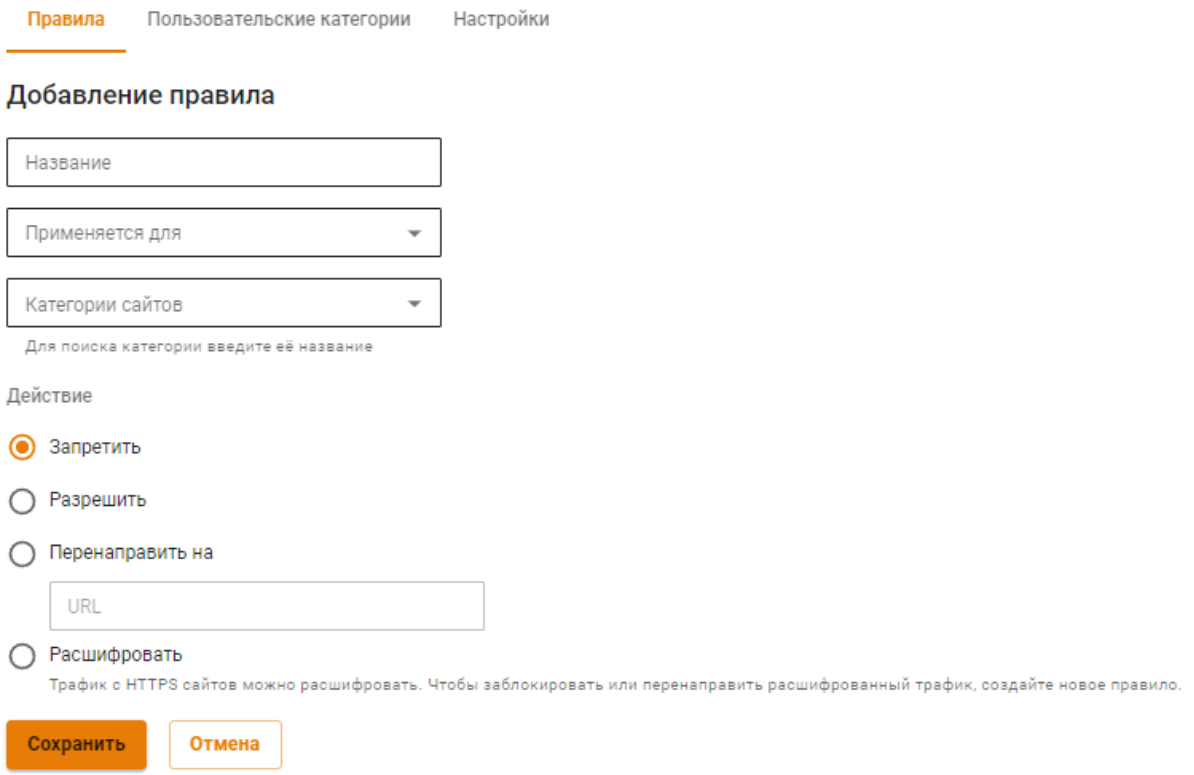
Правила применяются сверху вниз в порядке следования в таблице до первого совпадения. Таким образом, если вышестоящим правилом будет разрешен какой-то ресурс для определенной группы пользователей, то правила ниже применяться не будут. Так можно создавать гибкие настройки фильтрации, исключая нужных пользователей вышестоящими правилами из правил блокировки. Аналогичным образом действуют правила расшифровки HTTPS.

В столбце **Управление** можно активировать или деактивировать правило, менять его приоритет, редактировать и удалить. 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 или специальный объект **Превышена квота** (в этот объект попадают пользователи, превысившие квоту по трафику).
- **Категории сайтов** - пользовательские, специальные и расширенные категории веб-ресурсов;
- **Действие** - действие данного правила на веб-запросы. Можно запретить, разрешить или расшифровать HTTPS-трафик.



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, отобразятся 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.

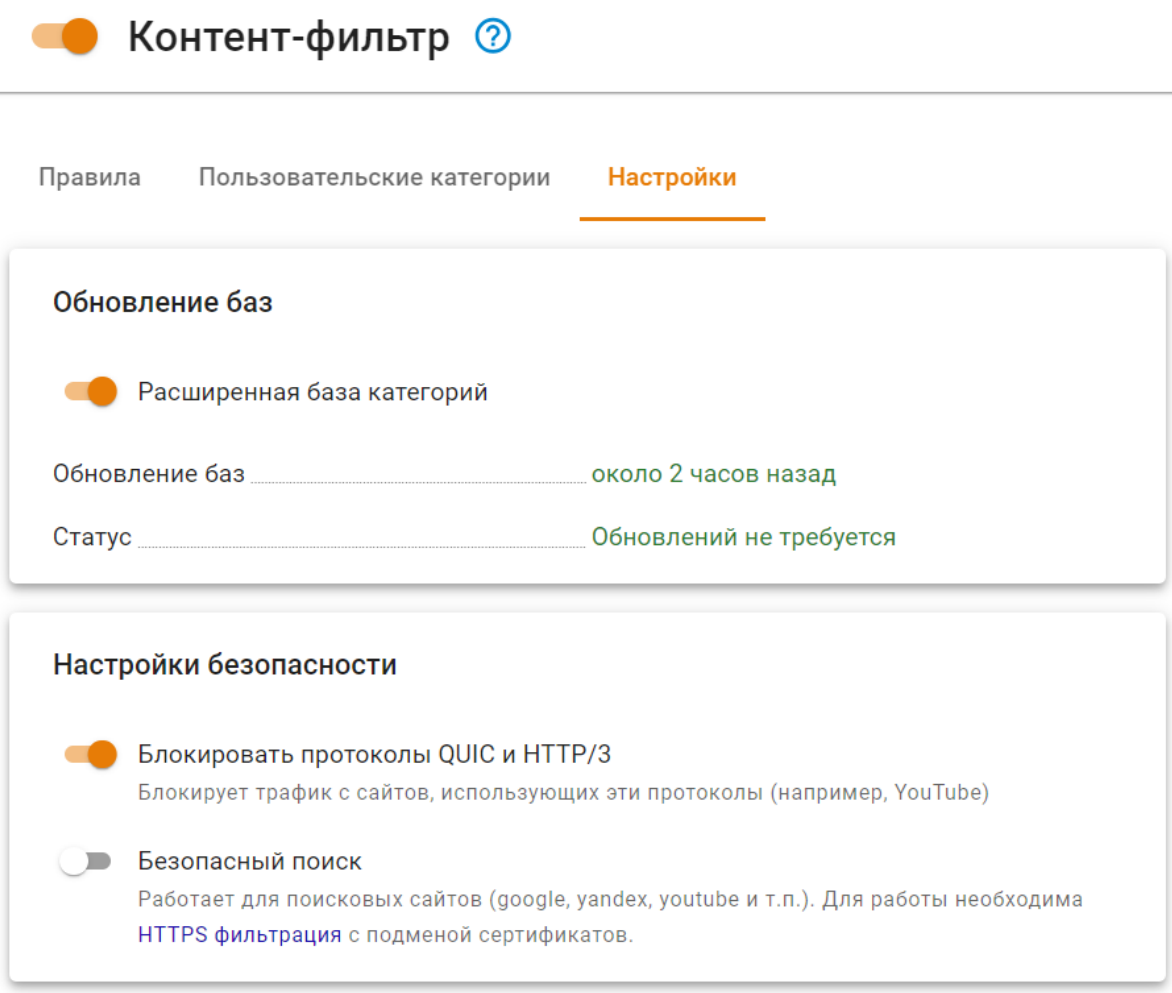
5. Проверить настройки контентной фильтрации по блокировке опасных и потенциально опасных файлов можно с помощью сервиса security.ideco.ru.

Блокировка загрузки файлов в файлообменники:

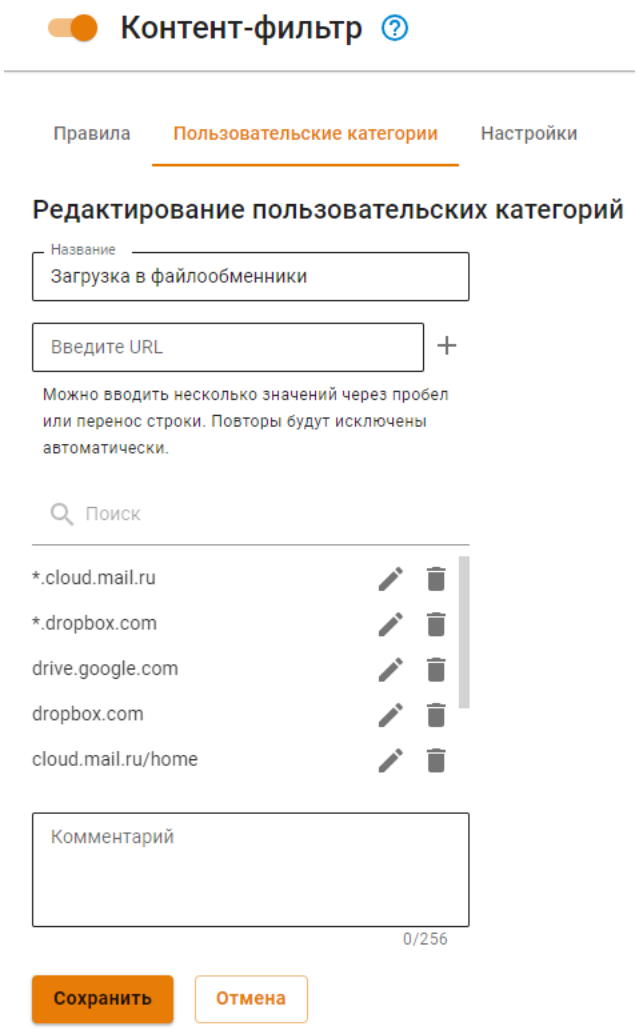
Блокирование этой категории требует особой настройки правил Контент-фильтра. В случае с файлообменниками (Google Drive, Яндекс.Диск, облако Mail.ru, Dropbox.com) расшифровки трафика категорий *Файлообменники*, *Файловые хранилища*, *Файловые архивы* и *Загрузка файлов в файлообменники* может быть недостаточно.

Чтобы заблокировать загрузку файлов в облака через браузер, выполните действия:

1. Включите **Блокировку протоколов Quic/HTTP3** на вкладке **Контент-фильтр -> Настройки**:

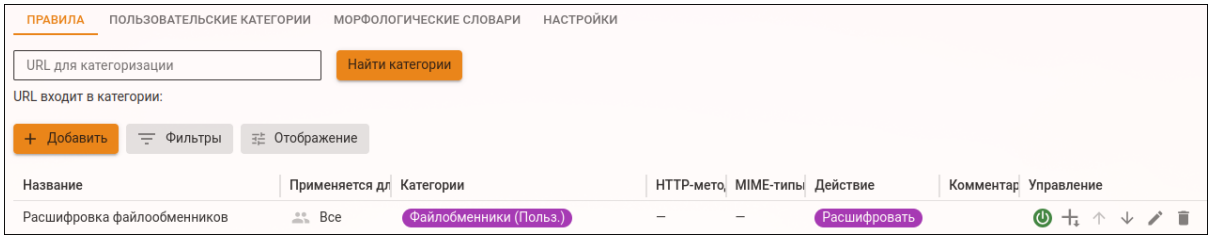


2. Создайте пользовательскую категорию для расшифровки трафика, указав домены нужных файлообменников:

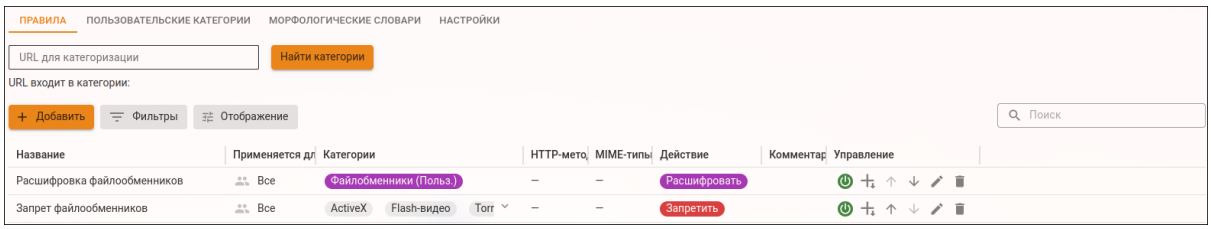


Для указания доменов используйте маски: `*.cloud.mail.ru`, `cloud.mail.ru/home`, `*.mail.ru`, `cloud.mail.ru`.

3. Создайте правило, расшифровывающее трафик созданной в п. 2 категории:

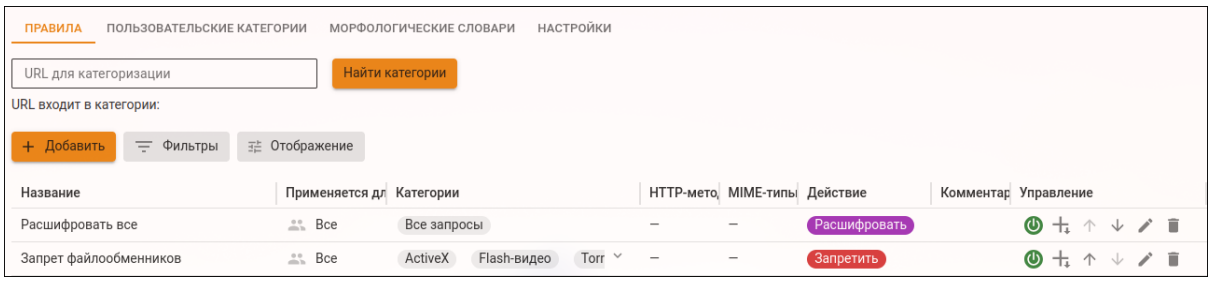


4. Ниже создайте правило, запрещающее загрузку файлов:



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:



15.3.5 Описание категорий Контент-фильтра

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
«Запаркованные»	Веб-сайты, которые используются в качестве «заглушек» для приобретенных, но не используемых доменных имен
Веб-почта	Службы, предоставляющие пользователям веб-доступ к почтовым ящикам. Как правило, речь идет о бесплатных ящиках
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
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
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-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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
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
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
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
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
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
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.
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.
Плата за серфинг	Сайты компаний, предлагающих оплату за просмотр рекламы в их специализированных приложениях
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
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
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
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Религия	Категория не содержит адресов и будет удалена в будущем
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

15.3.6 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 и ClamAV, внешним ICAP-сервисам и контент-фильтру (можно категоризировать полный URL запроса и MIME-type контента).

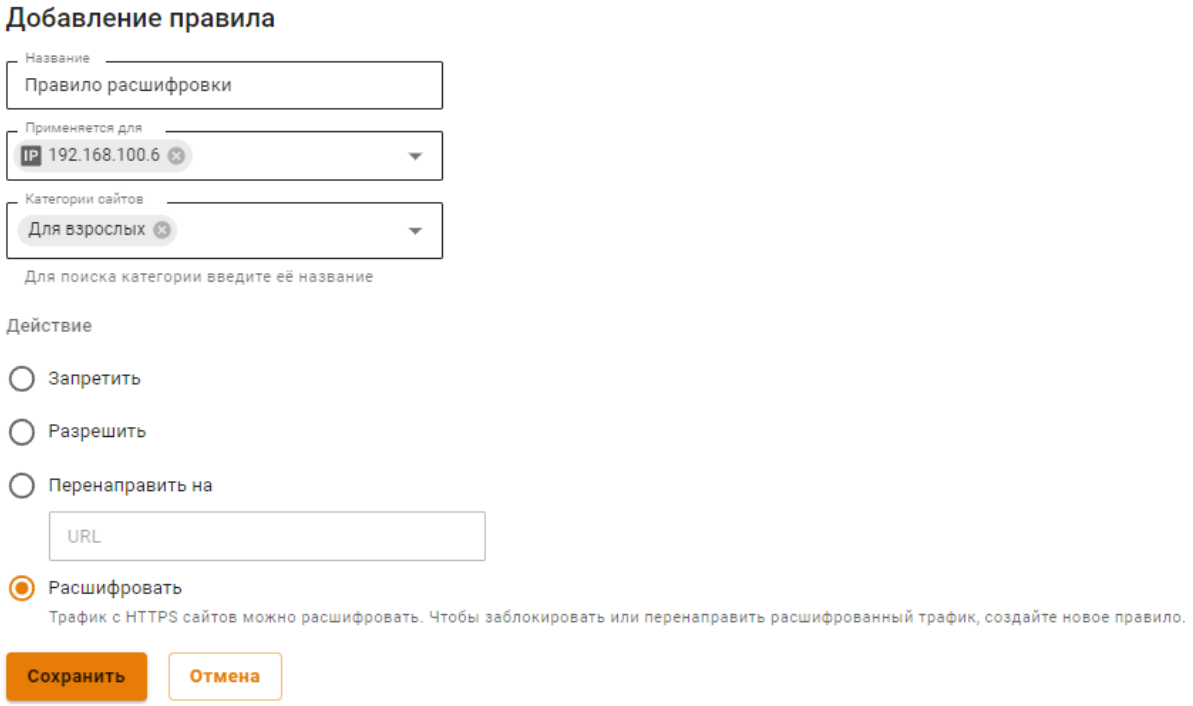
Подсказка: Специфика фильтрации HTTPS-трафика с подменой сертификата требует настройки обеих сторон подключения: сервера Ideco NGFW и рабочей станции каждого пользователя в локальной сети.

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**.

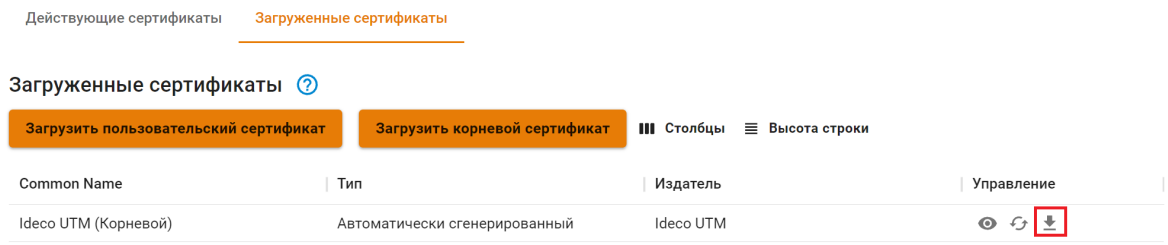
Пример правила для расшифровки:



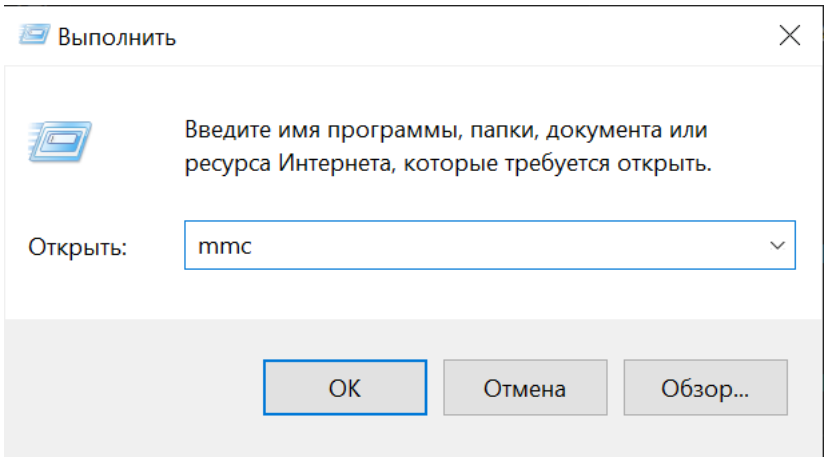
Настройка рабочей станции пользователя

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**:

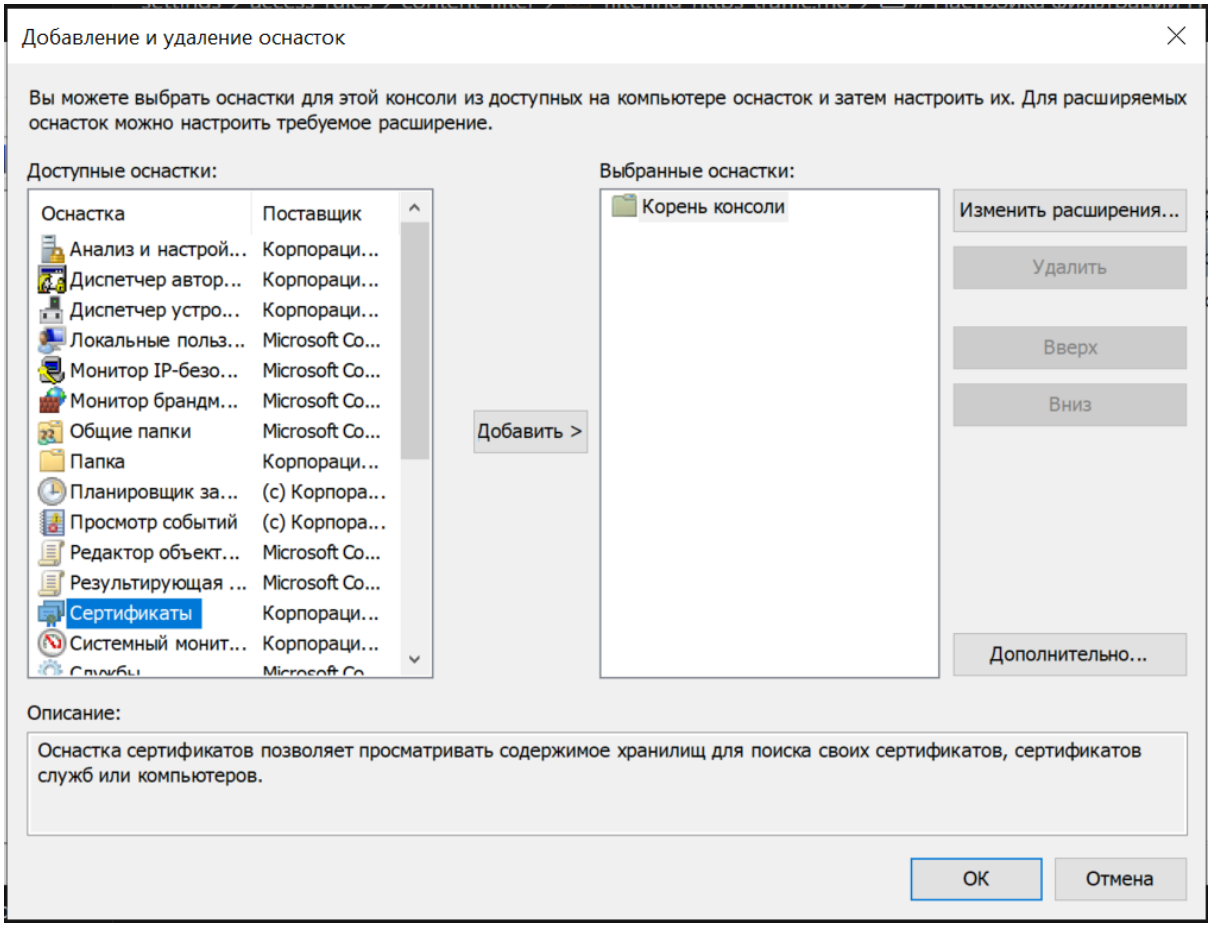


2. Откройте на рабочей станции центр управления сертификатами: **Пуск -> Выполнить**, выполнив в диалоге команду **mmc**:

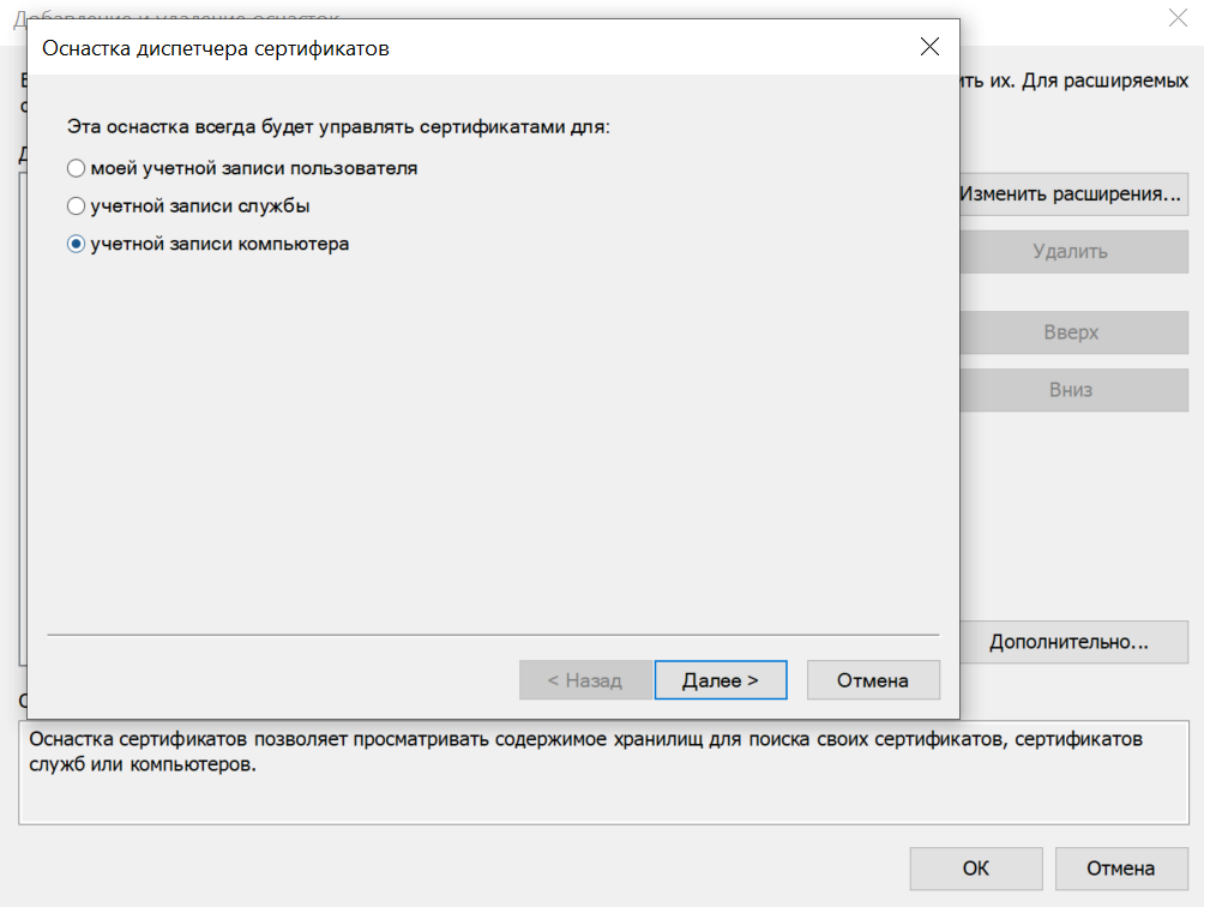


3. В меню **Файл** выберите **Добавить или удалить оснастку**:

4. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите кнопку **Добавить**:

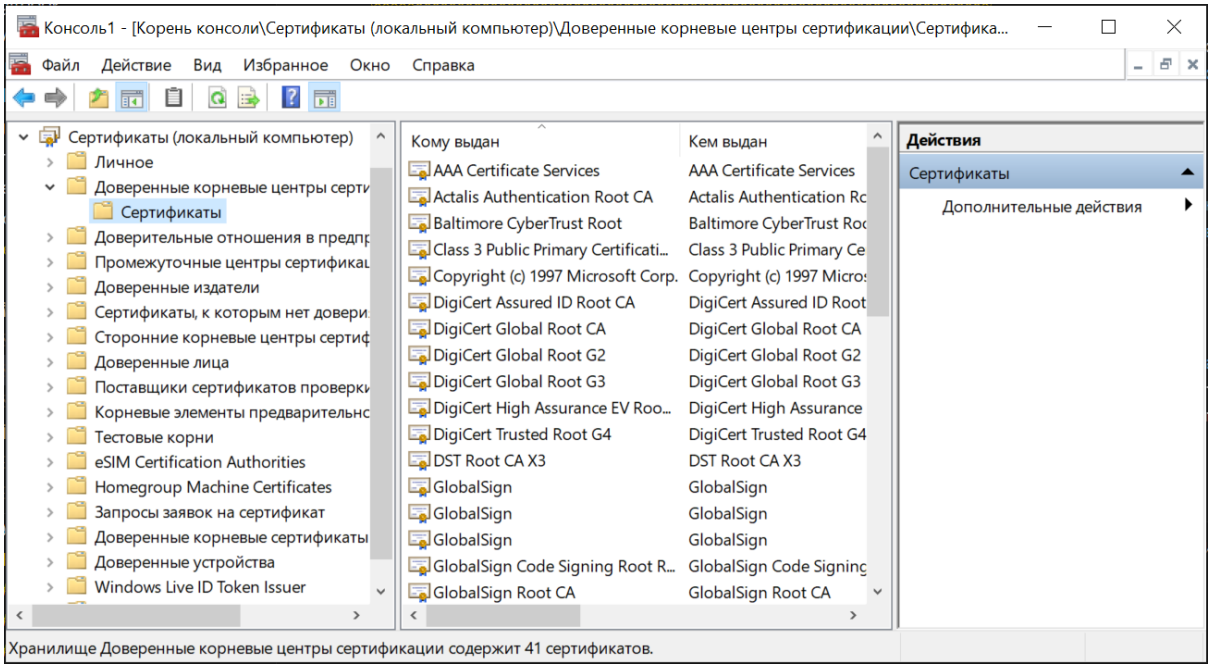


5. В открывшемся окне выберите пункт **Учетная запись компьютера** и нажмите кнопку **Далее**:



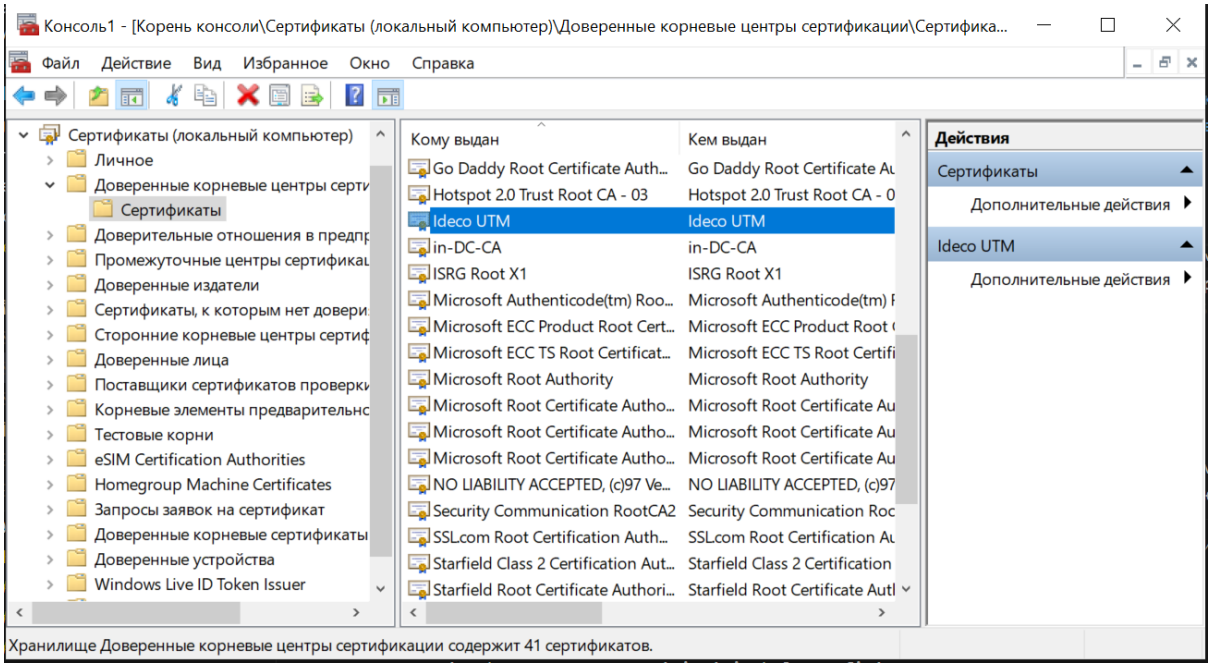
6. В окне **Выбор компьютера** оставьте флаг **Локальный компьютер** и нажмите кнопку **Готово**.

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**:

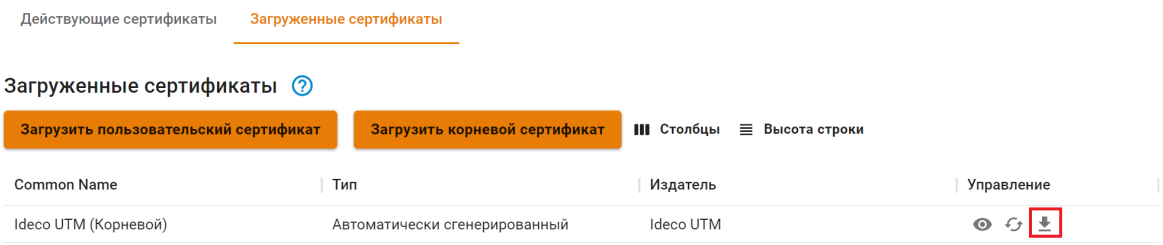
9. Следуя инструкциям Мастера импорта сертификатов, импортируйте корневой сертификат сервера Ideco NGFW. Импортированный сертификат появится в списке в правой части окна:



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**:



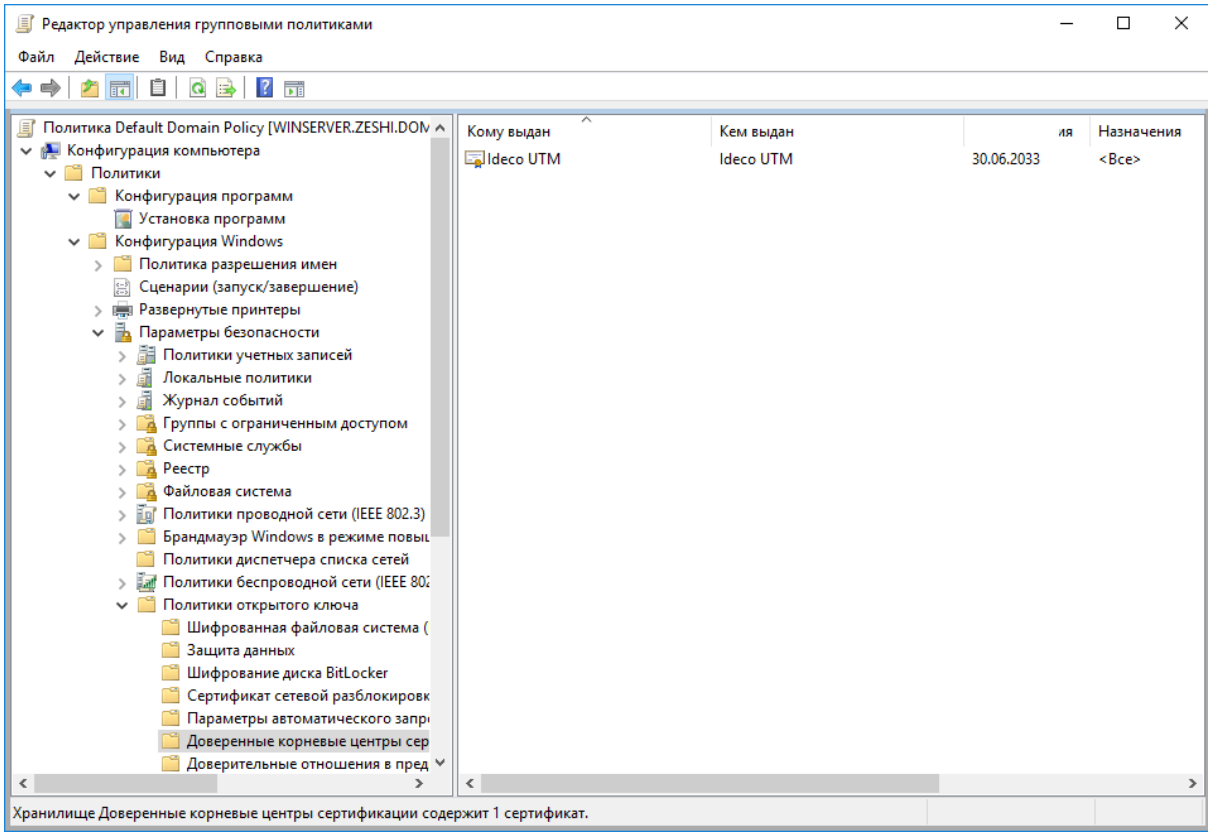
2. Зайдите на контроллер домена с правами администратора.

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

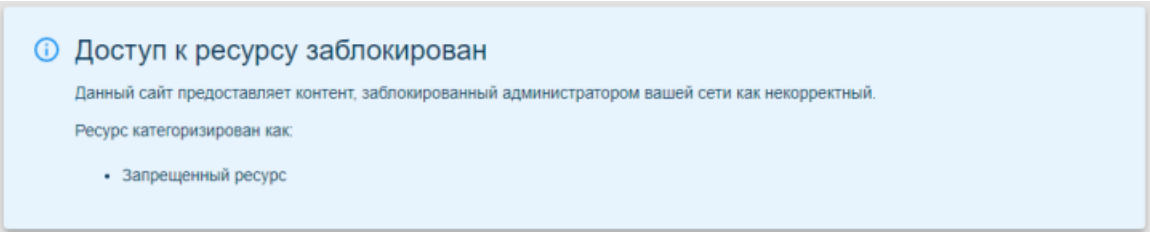
- Включения расшифровки трафика может быть недостаточно для подмены сертификата некоторых сайтов (например, `ya.ru`, `google.com`). В этом случае необходимо включить опцию **Блокировать протоколы QUIC и HTTP/3** на вкладке **Настройки** раздела **Контент-фильтр**.
- Если браузер не использует системное 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.

15.3.7 Изменение страницы блокировки Контент-фильтра

Основное

Страница блокировки Контент-фильтра по умолчанию содержит уведомление о блокировке доступа к ресурсу и категоризацию:



Для создания персонализированного шаблона страницы выполните действия:

1. Удалите директорию, в которой хранятся файлы кэша 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;
```

(continues on next page)

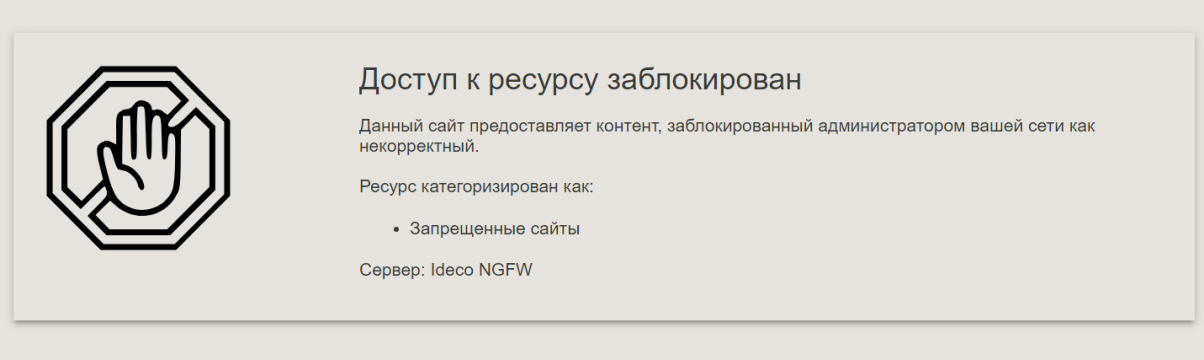
(продолжение с предыдущей страницы)

```
  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:

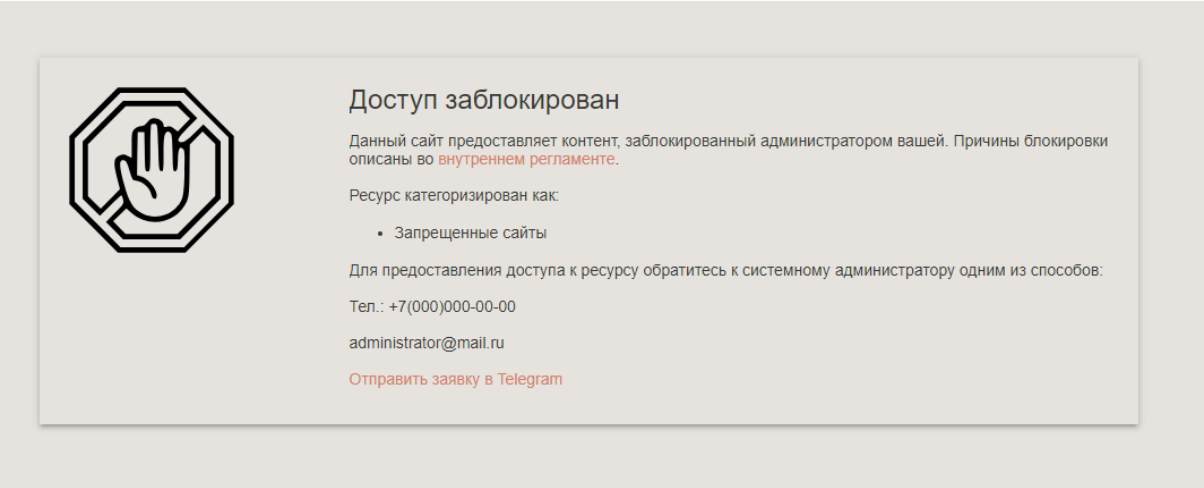
```
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width" />
  <link rel="icon" type="image/x-icon" href="IDECO_ICON_FAVICON">
  <link rel="apple-touch-icon" href="IDECO_ICON_FAVICON">
  <title>Доступ заблокирован</title>
  <style type="text/css">%l</style>
</head>

<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␣
↪одним из способов:</p>
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      <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.

15.4 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**.

15.4.1 Настройка ограничения скорости

Для создания правила необходимо перейти в раздел **Правила трафика -> Ограничение скорости** и нажать кнопку **Добавить**.

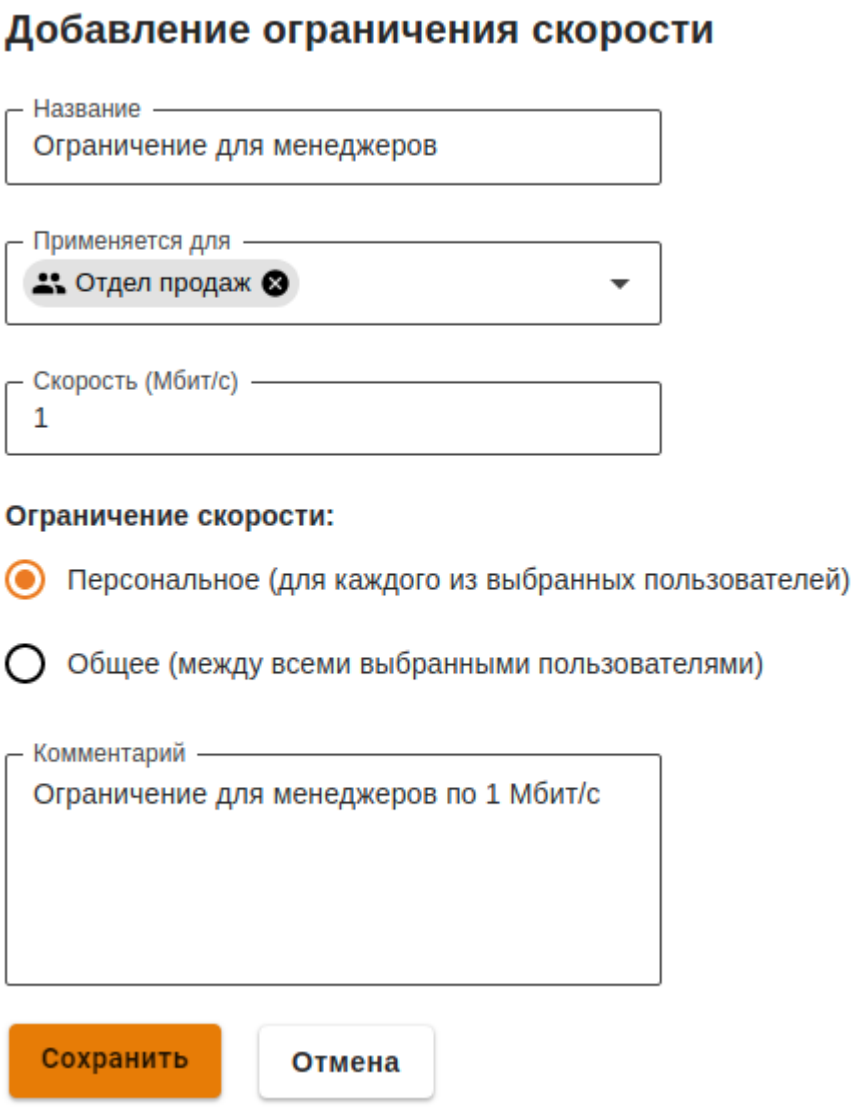
Далее заполните следующие поля:

- **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.

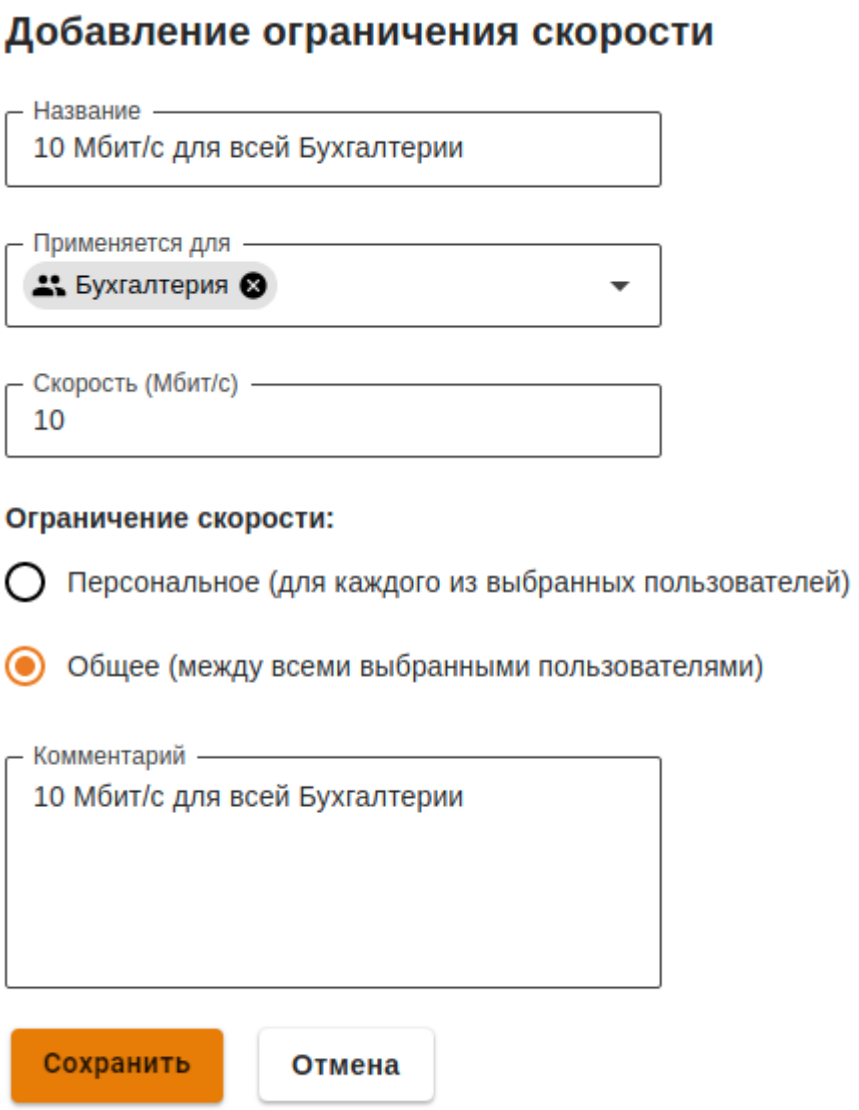
Для удобства настройки существует два типа ограничения скорости. Они могут быть применены для пользователей, групп, IP-адресов и объекта **Превышена квота** (в этот объект попадают пользователи, которые превысили квоту по трафику).

- **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.

Также не забывайте перевести ползунок в верхней части экрана около надписи **Ограничение скорости** в положение **Включен**, чтобы этот модуль работал.

Подсказка: Если не нажать кнопку **Применить** 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 следующий 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**.

15.4.2 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.

15.4.3 Особенности

При подключениях пользователей по VPN к Ideco NGFW из сети интернет скорость трафика в локальную сеть за Ideco NGFW 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.

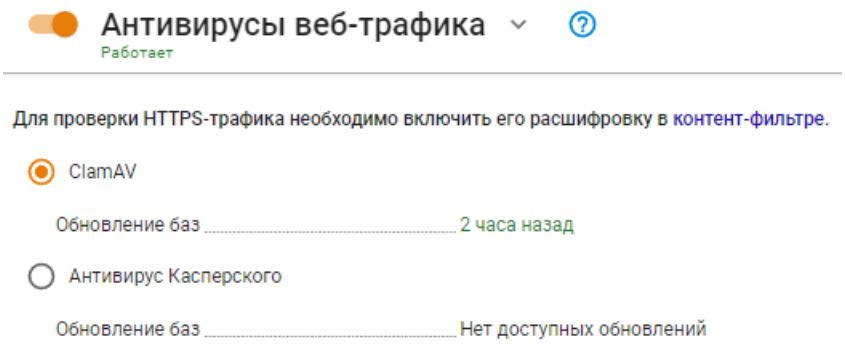
15.5 Антивирусы веб-трафика

15.5.1 Основное

Подсказка: Название службы раздела *Антивирусы веб-трафика*: `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 настройках можно выбрать между антивирусной фильтрацией модулями ClamAV (OpenSource-антивирус) или антивирусом от Лаборатории Касперского (лицензируется отдельно и может быть не доступен по условиям лицензии).



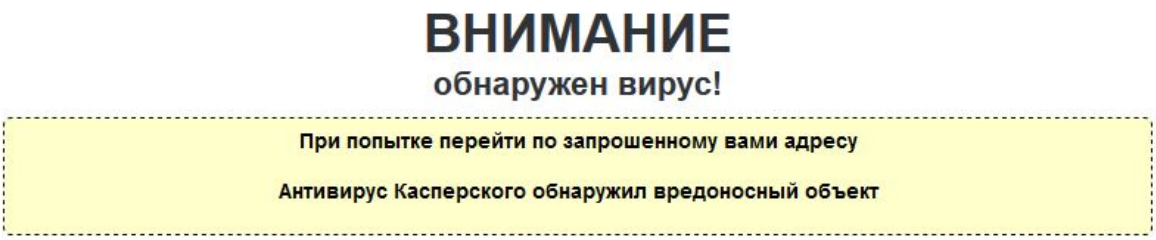
Модуль антивируса связан с прокси-сервером и контент-фильтром, поэтому фильтрует веб-трафик при выполнении следующих условий:

- Веб-ресурс не находится в списках исключений прокси-сервера по назначению;
- Пользователь, к которому поступает трафик, не включен в исключения прокси-сервера по источнику;
- HTTPS-сайт проверяется только в случае расшифровки HTTPS-трафика контент-фильтром.

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:



Лицензирование антивируса Касперского:

Данный модуль в нашем продукте создан на базе Kaspersky Anti-Virus Software Development Kit и лицензируется совместно с Ideco NGFW компании **Айдеко**.

Корпоративные ключи для других продуктов Лаборатории Касперского не могут быть использованы для его активации.

Добавление сигнатур в список исключений ClamAV:

Просмотреть логи CalmAV и определить сработавшую сигнатуру можно, введя в терминале Ideco NGFW команду:

```
journalctl -u ideco-clamd.service
```

Пример вывода команды:

```
Dec 20 13:40:40.083733 info clamd[12443]: /tmp/CI_TMP_1qlsy5: Html.Exploit.
CVE_2016_0228-6327291-2(00000000000000000000000000000000:888502) FOUND Dec
20 13:40:40.083750 info clamd[12443]: /tmp/CI_TMP_1qlsy5: Html.Exploit.
CVE_2016_0228-6327291-2 FOUND
```

```
Dec 20 14:11:24.375281 info clamd[12443]: /tmp/CI_TMP_DPpHnS: Win.Trojan.
LOLBins-7360503-2(00000000000000000000000000000000:388262) FOUND Dec 20 14:11:24.
375293 info clamd[12443]: /tmp/CI_TMP_DPpHnS: Win.Trojan.LOLBins-7360503-2 FOUND
```

```
Dec 20 15:28:11.031128 info clamd[5165]: /tmp/CI_TMP_g7aPdY: Html.Exploit.
CVE_2017_0011-5752098-0(00000000000000000000000000000000:354192) FOUND Dec
20 15:28:11.031144 info clamd[5165]: /tmp/CI_TMP_g7aPdY: Html.Exploit.
CVE_2017_0011-5752098-0 FOUND
```

Допустим, в 13:40 открывали сайт, на котором произошло ложное срабатывание ClamAV. Исходя из логов в исключения нужно добавить сигнатуру **Html.Exploit.CVE_2016_0228-6327291-2**.

Далее создайте файл белого списка `whitelist.ign2`, введя следующую команду:

```
touch /var/cache/ideco/av-backend/clamav_bases/whitelist.ign2
```

Добавьте в созданный файл следующий текст (не забудьте заменить сигнатуру из команды ниже на ту, которую хотите добавить):

```
echo 'Html.Exploit.CVE_2016_0228-6327291-2' >> /var/cache/ideco/av-backend/clamav_
↪bases/whitelist.ign2
```

Для применения изменений перезагрузите ideco-clamd.service.

```
systemctl restart ideco-clamd.service
```

15.6 Предотвращение вторжений

Подсказка: Название службы раздела *Предотвращение вторжений*: `ideco-suricata-backend`; `ideco-suricata`; `ideco-suricata-event-syncer`; `ideco-suricata-event-to-syslog`.
Список имен служб для других разделов доступен по *ссылке*.

Подсказка: Служба предотвращения вторжений доступна только в **Enterprise-версии Ideco NGFW** для пользователей с активной подпиской на обновления.

Правила **Предотвращения вторжений**, *Контроля приложений* и *Ограничения скорости* не обрабатывают трафик между локальными сетями и сетями филиалов.

Для исключения пользователя или групп пользователей из обработки служб **Предотвращения вторжений** добавьте соответствующее правило в **Правила трафика -> Исключения из правил**.

Служба предотвращения вторжений (IDS/IPS, Intrusion detection system / Intrusion prevention system) предназначена для:

- Обнаружения;
- Журналирования;
- Предотвращения атак злоумышленников на сервер, интегрированные службы и локальную сеть.

Правила блокировки трафика включают в себя блокирование активности троянских программ, spyware, бот-сетей, клиентов p2p и **торрент-трекеров**, вирусов, сети **TOR** (используемой для обхода правил фильтрации), анонимайзеров и т. д.

Для настройки службы перейдите на вкладку **Правила трафика -> Предотвращение вторжений**. Включите или выключите службу, переведя выключатель в соответствующее положение:

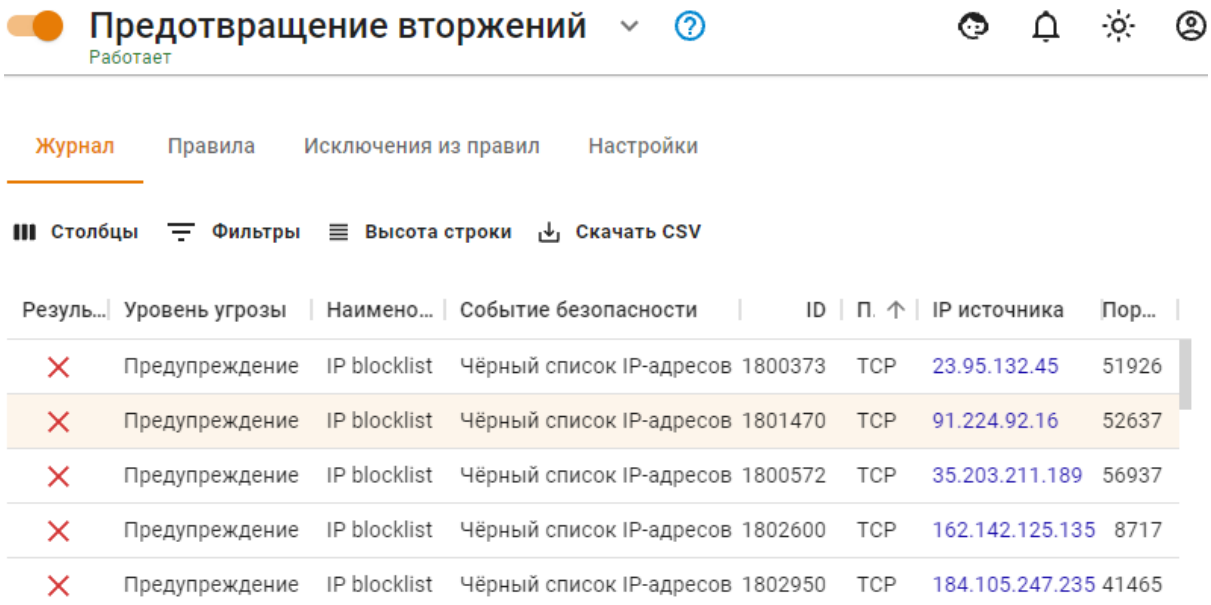
Раздел состоит из четырех вкладок:

- *Журнал* - фиксирует логи срабатывания правил службы;
- *Правила* - содержит список предустановленных правил;
- *Исключения из правил* - фиксирует в таблицу список отключенных правил службы предотвращения вторжений;
- *Настройки* - во вкладке создаются правила для службы предотвращения вторжений.

15.6.1 Примеры использования

Пример анализа логов:

Предупреждение службы предотвращения вторжений:



На вкладке **Правила** можно открыть найденную группу по **Событию безопасности**, нажать на и в ней найти сработавшее правило по его ID:

```
alert http $EXTERNAL_NET any -> any any (msg:"ET SCAN Zmap User-Agent (Inbound)";
flow:established,to_server; http.user_agent; content:"Mozilla/5.0 zgrab/0.x";
depth:21; endswith; classtype:network-scan; sid:2029054; rev:2; metadata:created_at
2019_11_26, former_category SCAN, updated_at 2020_10_23;)
```

Можно проанализировать IP-адрес, с которым была попытка подозрительного соединения, через whois.

Как исключить узел из обработки системой IDS/IPS через терминал:

Можно исключить узел из обработки в веб-интерфейсе в разделе
Правила трафика -> Исключения из правил.

Задача: Необходимо исключить из обработки узел `192.168.154.7`.

Решение:

1. В файл `/var/opt/ideco/suricata-backend/custom.rules` добавьте следующую строку: `pass ip 192.168.154.7 any <> any any (sid:1;)`.
2. Затем в разделе **Терминал** выполните команду `systemctl restart ideco-suricata-backend.service`.

Предупреждение: При создании нескольких ручных правил **обязательно** изменяйте ID-правила (sid:2;), иначе служба предотвращения вторжений прекратит работу из-за наличия нескольких правил с одним sid.

Технические требования:

Для работы службы 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.

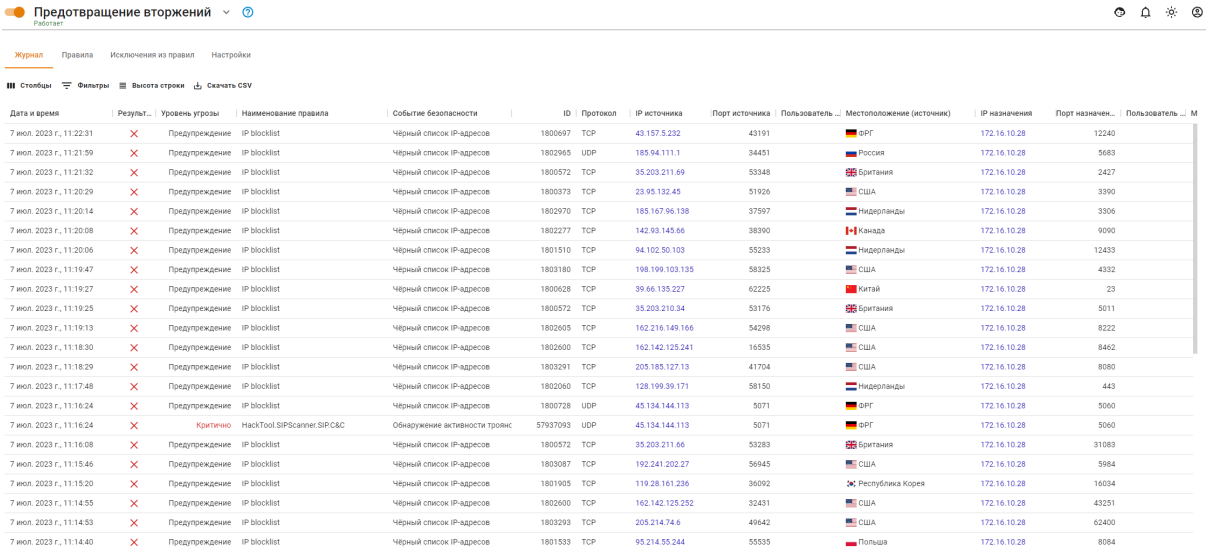
В разделе **Мониторинг -> Графики загруженности** выберите параметр средняя загрузка (за 1, 5 и 15 минут).

Подробнее о Load Average.

15.6.2 Журнал

Основное

В подразделе **Журнал** можно просмотреть логи службы предотвращения вторжений.



Дата и время	Результ...	Уровень угрозы	Наименование правила	Событие безопасности	ID	Протокол	IP источника	Порт источника	Пользователь ...	Местоположение (источник)	IP назначения	Порт назначен...	Пользователь ...	М
7 июл. 2023 г., 11:22:31	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800697	TCP	43.157.5.232	43191		ФРГ	172.16.10.28	12240		
7 июл. 2023 г., 11:21:59	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802965	UDP	185.94.111.1	34451		Россия	172.16.10.28	5683		
7 июл. 2023 г., 11:21:32	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800572	TCP	35.203.211.69	53348		Британия	172.16.10.28	2427		
7 июл. 2023 г., 11:20:29	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800373	TCP	23.95.132.45	51926		США	172.16.10.28	3390		
7 июл. 2023 г., 11:20:14	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802970	TCP	185.167.96.138	37597		Нидерланды	172.16.10.28	3306		
7 июл. 2023 г., 11:20:08	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802277	TCP	142.93.145.66	38390		Канада	172.16.10.28	9090		
7 июл. 2023 г., 11:20:06	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801510	TCP	94.102.50.103	55233		Нидерланды	172.16.10.28	12433		
7 июл. 2023 г., 11:19:47	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1803180	TCP	198.199.103.135	58325		США	172.16.10.28	4332		
7 июл. 2023 г., 11:19:27	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800628	TCP	39.66.135.227	62225		Китай	172.16.10.28	23		
7 июл. 2023 г., 11:19:25	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800572	TCP	35.203.210.34	53176		Британия	172.16.10.28	5011		
7 июл. 2023 г., 11:19:13	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802605	TCP	162.216.149.166	54298		США	172.16.10.28	8222		
7 июл. 2023 г., 11:18:30	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802600	TCP	162.142.125.241	16535		США	172.16.10.28	8462		
7 июл. 2023 г., 11:18:29	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1803291	TCP	205.185.127.13	41704		США	172.16.10.28	8080		
7 июл. 2023 г., 11:17:48	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802060	TCP	128.199.39.171	58150		Нидерланды	172.16.10.28	443		
7 июл. 2023 г., 11:16:24	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800728	UDP	45.134.144.113	5071		ФРГ	172.16.10.28	5060		
7 июл. 2023 г., 11:16:24	✕	Критично	HackTool.SIPScanner.SIP.C&C	Обнаружение активности троянс	57937093	UDP	45.134.144.113	5071		ФРГ	172.16.10.28	5060		
7 июл. 2023 г., 11:16:08	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800572	TCP	35.203.211.66	53283		Британия	172.16.10.28	31083		
7 июл. 2023 г., 11:15:46	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1803087	TCP	192.241.202.27	56945		США	172.16.10.28	5984		
7 июл. 2023 г., 11:15:20	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801905	TCP	119.28.161.236	36092		Республика Корея	172.16.10.28	16034		
7 июл. 2023 г., 11:14:55	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802600	TCP	162.142.125.252	32431		США	172.16.10.28	43251		
7 июл. 2023 г., 11:14:53	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1803293	TCP	205.214.74.6	49642		США	172.16.10.28	62400		
7 июл. 2023 г., 11:14:40	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801533	TCP	95.214.55.244	55535		Польша	172.16.10.28	8084		

- Поле **Результат анализа** отображает действие службы:
  - `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

При наведении на колонку **ID** в строке с правилом появится кнопка **Добавить в исключения** (), при нажатии на которую сигнатура будет добавлена в исключения из правил:

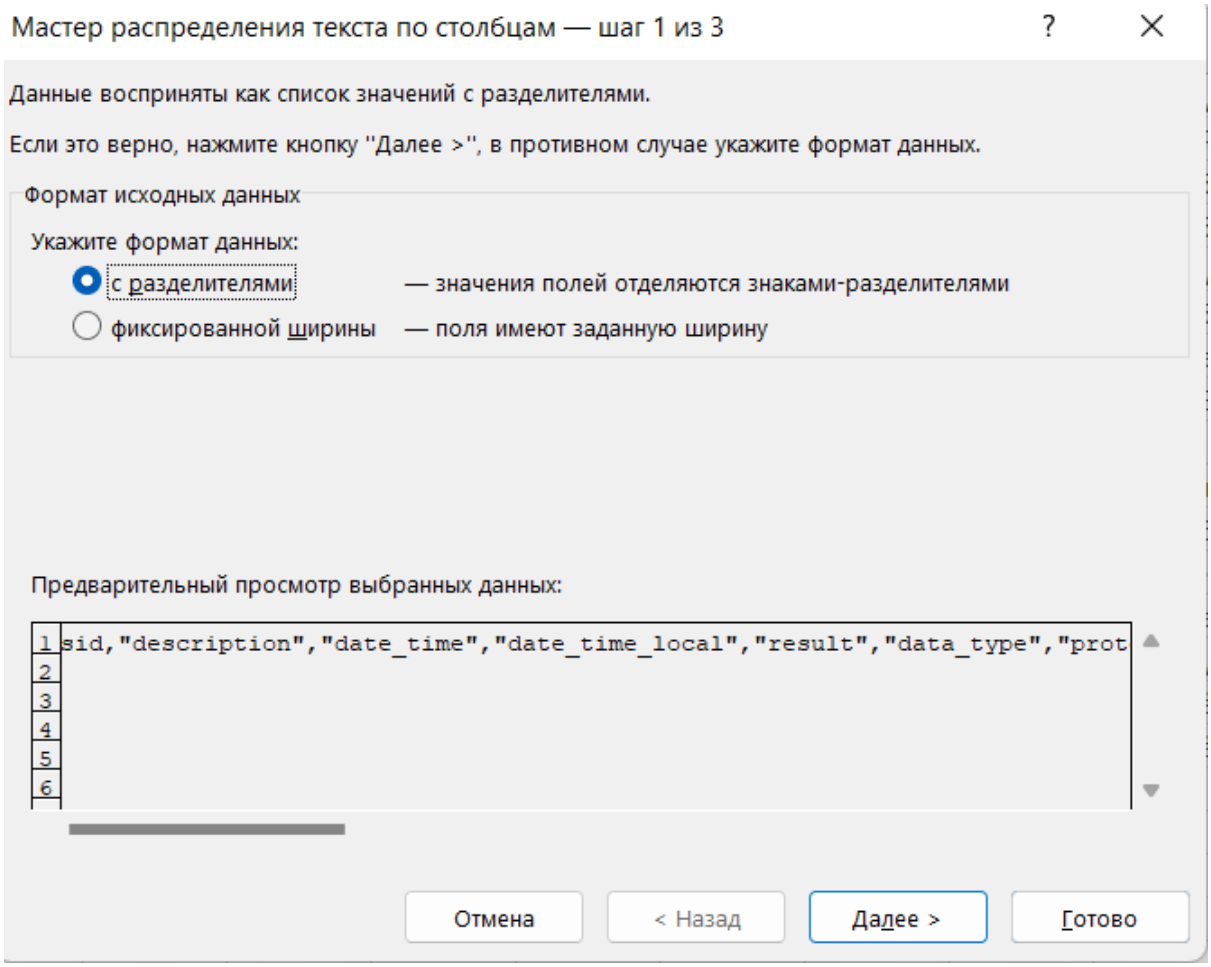
Скачайте CSV-файл с логами службы предотвращения вторжений за определенный период по соответствующей кнопке.

Для корректного отображения информации из CSV-файла в MS Excel повторите действия::

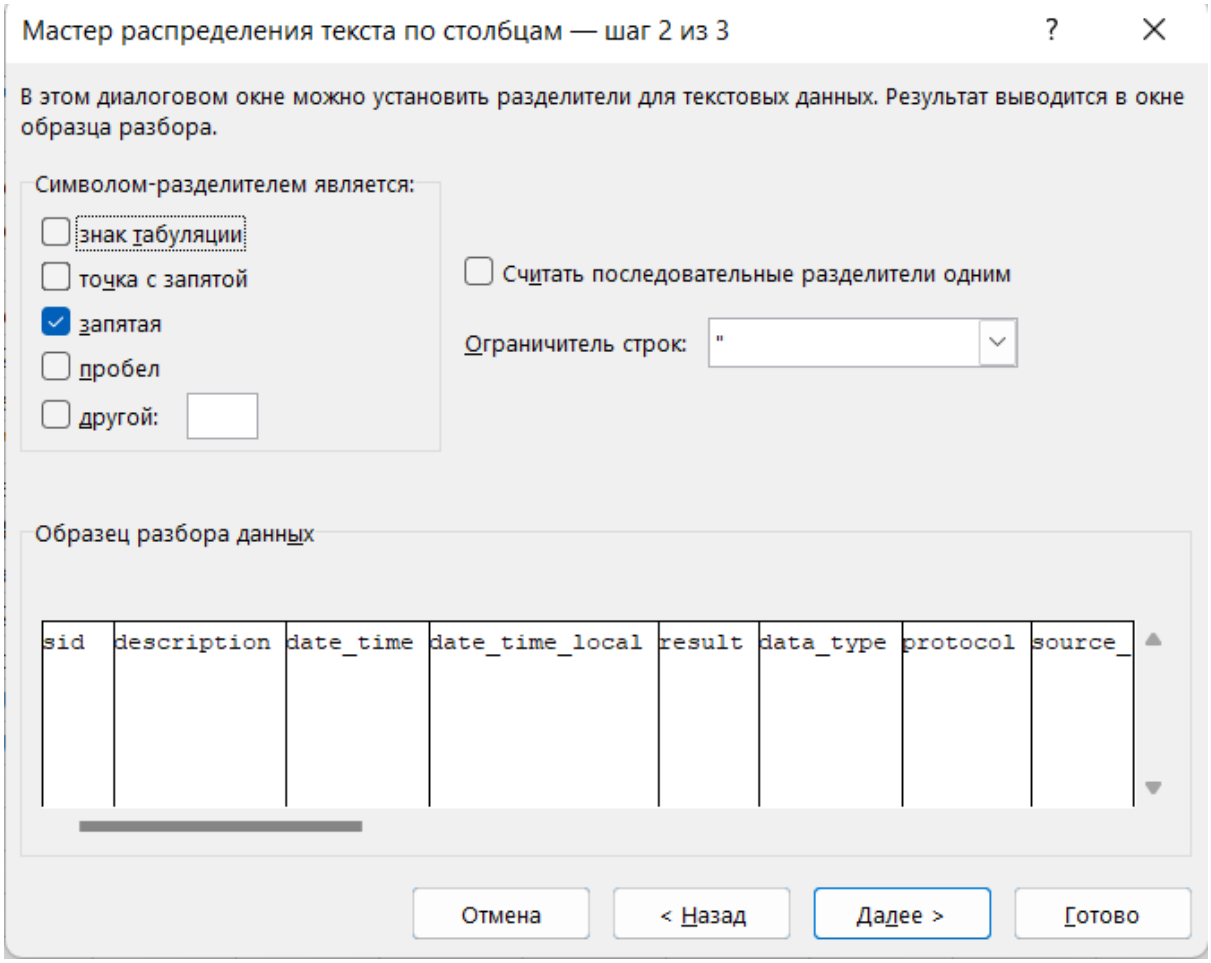
1. Откройте CSV-файл в MS Excel и выделите весь первый столбец.

2. Перейдите во вкладку **Данные** и нажмите кнопку **Текст по столбцам**.

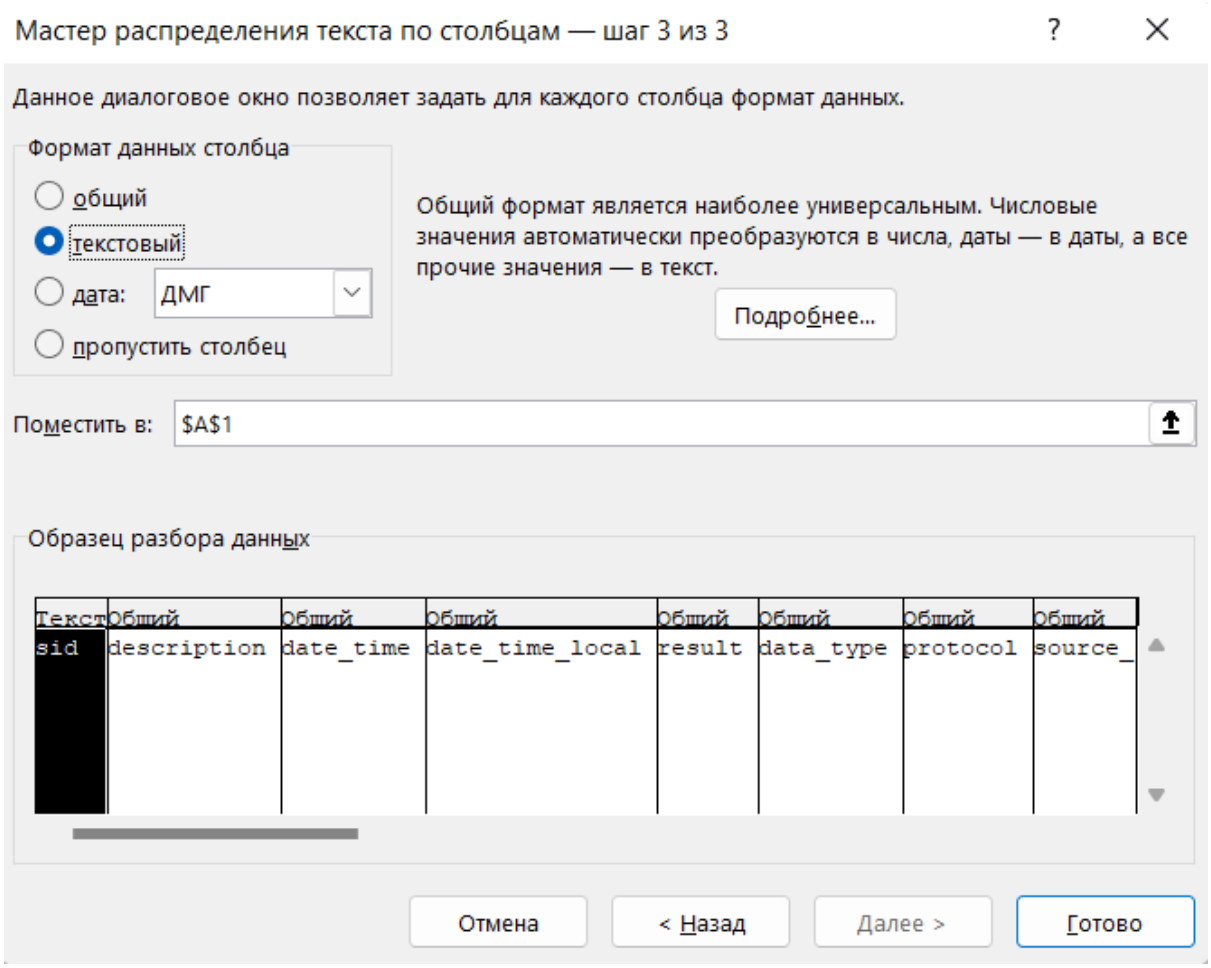
3. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:



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



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



15.6.3 Правила

Основное

На вкладке **Правила** доступны для просмотра, включения и отключения группы правил службы предотвращения вторжений. При включении/отключении группы правил настройки применяются мгновенно без необходимости перезапускать службу.

Описание правил:

- **Блокирование утечек информации** - обнаруживает/блокирует попытки получить данные и информацию.
- **Атаки на получение прав пользователя** - обнаруживает/блокирует попытки получить учетные данные пользователя.
- **Попытки получения привилегий администратора** - обнаруживает/блокирует попытки повысить привилегии до администратора и полученить учетные данные администратора.
- **Попытки проведения DoS-атак** - обнаруживает/блокирует попытки провести атаки типа «отказ в обслуживании» (denial-of-service attack).
- **Попытки получения системных файлов** - обнаруживает/блокирует системные конфигурации.
- **Попытки получения привилегий пользователя** - обнаруживает/блокирует попытки повысить привилегии и получить учетные данные пользователей.
- **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.
- **Блокирование крупных утечек информации** - обнаруживает/блокирует попытки получить данные и информацию.
- **Управление вредоносным ПО** - обнаруживает/блокирует связь с инфраструктурой управления и контроля (C2), которую злоумышленники используют для управления зараженными устройствами и кражи конфиденциальных данных.
- **Обнаружение успешных краж учетных данных** - обнаруживает/блокирует кражи учетных данных.
- **Попытки авторизации с логином и паролем по-умолчанию** - обнаруживает/блокирует попытки зайти под учетными данными с простыми паролями (аналогично Bruteforce).
- **Использование DNS-трафика для управления вредоносным ПО** - обнаруживает/блокирует связь с инфраструктурой управления и контроля (C2).
- **Эксплойты** - обнаруживает/блокирует использование уязвимостей систем (с индификатором CVE-XXXX-XXXXX).
- **Определение внешнего IP-адреса** - обнаруживает/блокирует попытки взаимодействия с инфраструктурой из внешних сетей.
- **Расширенная база правил (от Лаборатории Касперского)** - набор правил по обнаружению/блокировке от Лаборатории Касперского.
- **Анонимайзеры** - обнаруживает/блокирует анонимайзеры.
- **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.
- **Чёрный список IP-адресов** - обнаруживает/блокирует трафик к IP-адресам из баз safe-surf.ru и cinsarmy.com.
- **SSL-сертификаты, используемые вредоносным ПО и ботнетами** - обнаруживает/блокирует связь с командными цетрами злоумышленников (C2).
- **Телеметрия Windows** - обнаруживает/блокирует Телеметрию Windows.
- **Обнаружение подозрительной сетевой активности** - обнаруживает/блокирует аномалии или нестандартные действия легитимных пользователей в сети.
- **Блокирование атак** - обнаруживает/блокирует подозрительные IP-адреса (IP Reputation).
- **Попытки сканирования сети** - обнаруживает/блокирует сканирование сети.
- **Обнаружение нарушений стандартов сетевых протоколов** - обнаруживает/блокирует обращения по нестандартным/прошитым протоколам.
- **Трафик устаревшего уязвимого ПО** - обнаруживает/блокирует связи с командными цетрами злоумышленников (C2).
- **Запросы на скомпрометированные ресурсы** - обнаруживает/блокирует связи с командными цетрами злоумышленников (C2).
- **Ошибки в сетевых протоколах** - обнаруживает/блокирует ошибки сетевых протоколов.
- **Нежелательное программное обеспечение** - обнаруживает/блокирует вредоносное ПО.
- **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).
- **Попытки использования социальной инженерии** - обнаруживает/блокирует «атаку на человека».

- **Обнаружение подозрительных команд** - обнаруживает/блокирует нестандартные команды, не характерные системам.
- **Атаки на получение привилегий администратора** - обнаруживает/блокирует попытки получить привилегии администратора.
- **Подозрительное обращение к файлам** - обнаруживает/блокирует нестандартное обращение к файлам системы.
- **Авторизация с подозрительным логином**
- **Целевое использование вредоносного ПО** - обнаруживает/блокирует вредоносное программное обеспечение.
- **Блокирование активности троянских программ** - обнаруживает/блокирует вредоносные трояны.
- **Неизвестный тип трафика** - обнаруживает/блокирует неопознаный/вредоносный трафик.
- **Блокирование некорректных попыток получения привилегий пользователя** - обнаруживает/блокирует попытки получить привелегии пользователя.
- **Нецелевое использование стандартных портов** - обнаруживает/блокирует использование стандартных портов в нелегетимных целях.

История изменений правил:

14.12.2023

- Оптимизированы правила блокировки анонимайзеров

31.01.2024

- Улучшена блокировка Hola VPN и Browsec VPN

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 некоректности 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 эксплоита 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:

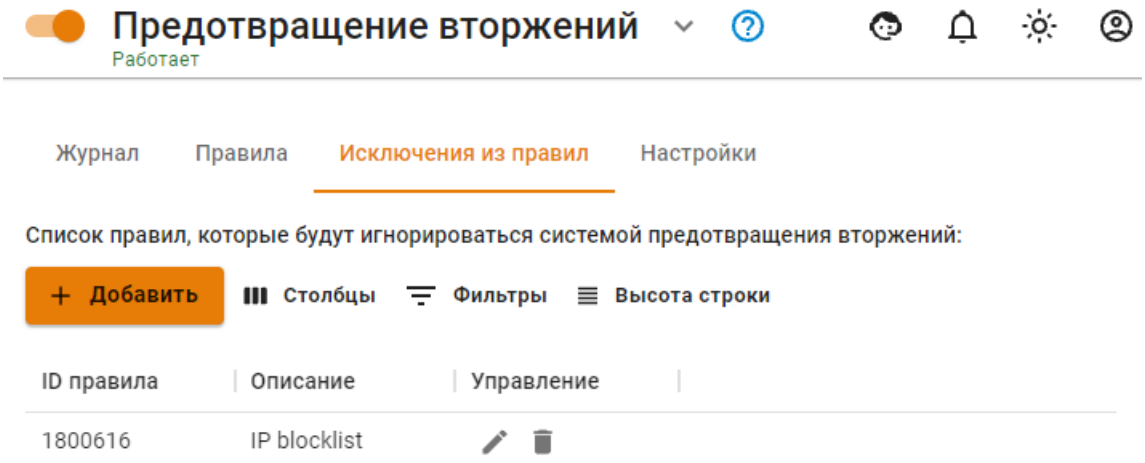
- Удалена группа **Активные ботнеты**
  Актуальные угрозы блокируются с помощью «Черных списков IP-адресов»

15.6.4 Исключения из правил

Основное

Таблица содержит список отключенных правил службы предотвращения вторжений в случае их ложных срабатываний или по другим причинам.

Отключить правила можно по кнопке **Добавить**, указав в соответствующем поле ID правила, или на вкладке **Журнал**, нажав **Добавить в исключения**.



Подсказка: Со временем при обновлении баз службы предотвращения вторжений ID правил могут меняться.

15.6.5 Настройки

Основное

Для добавления правила нажмите **Добавить** и в поле **Подсеть** укажите локальные сети, обслуживаемые NGFW (сети локальных интерфейсов NGFW, маршрутизируемые на них сети удаленных сегментов локальной сети предприятия).

Предупреждение: **Не указывайте** сети, принадлежащие внешним сетевым интерфейсам NGFW и внешним сетям. Указанные здесь сети участвуют в правилах службы предотвращения вторжения как локальные. Локальный межсегментный трафик не исключается из проверок системы.

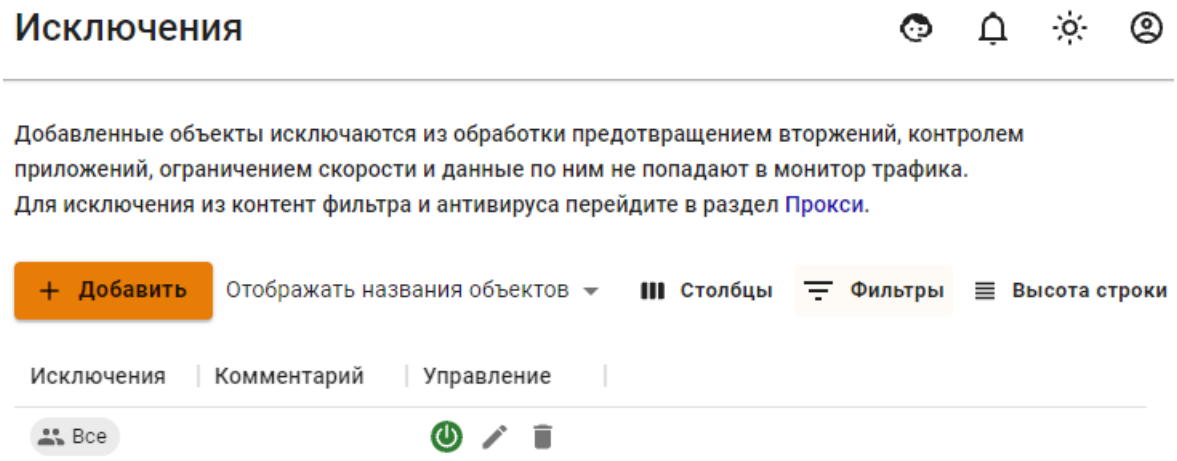
Предупреждение: При работе службы предотвращения вторжений **не используйте** сторонние DNS-серверы для компьютеров, т.к служба определяет зараженные устройства по DNS-запросам, проходящим через нее.
При использовании внутреннего домена AD рекомендуется:

- В компьютерах указать DNS-сервер Ideco NGFW в качестве единственного DNS-сервера;
- В настройках DNS-сервера на NGFW указать Forward-зону для локального домена.

15.7 Исключения

15.7.1 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.



Созданные исключения удалят объект из обработки правил на вкладке **Правила**.

Если после исключения объекта из обработки доступ к ресурсу не появился, проверьте, не блокируется ли DNS запрос. Для этого перейдите в раздел **Предотвращение вторжений -> Журнал**. Если запрос блокируется, то в журнале срабатываний наведите на строку и нажмите .

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.

15.8 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

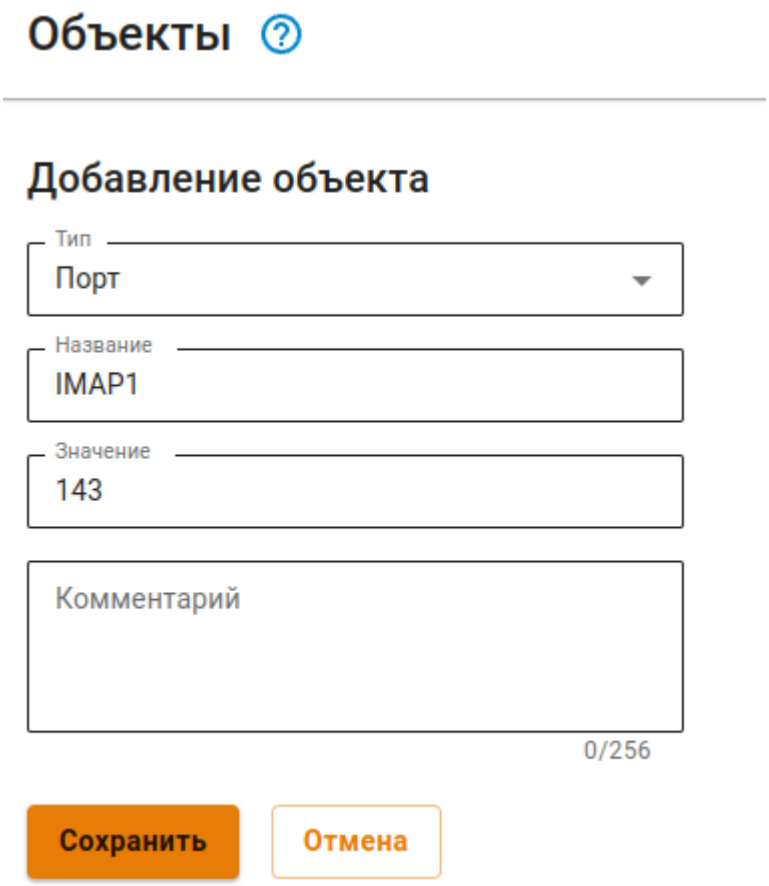
- **Зона** - логическое объединение сетевых интерфейсов. Используется для настройки правила файрвола на несколько интерфейсов.

- **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.

15.8.1 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 **Сохранить**.

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.

15.9 Квоты

Подсказка: Название службы раздела *Квоты*: `ideco-quotas-backend`; `systemd-quotacheck`.
Список имен служб для других разделов доступен по *ссылке*.

Для каждой квоты можно определить ее период действия (час, день, неделя, месяц, квартал). Она может быть назначена пользователям или группам в дереве пользователей на отдельной вкладке **Квота**. Также на этой вкладке можно увеличить и посмотреть доступный трафик на текущий период времени и узнать, когда произойдет сброс квоты.

Если квота назначена на группу, то по умолчанию она назначается на всех пользователей данной группы, а также на вложенные группы. Наследуемую от группы квоту можно изменить в свойствах вложенного пользователя или группы.

Подсказка: При превышении квоты пользователи попадают в объект **Превышена квота**, по умолчанию для таких пользователей никакие ограничения не действуют. Поэтому необходимо создать ограничивающее правило для объекта **Превышена квота** в одном или нескольких модулях Ideco NGFW (файрвол, контент-фильтр, контроль приложений, ограничение скорости).

15.9.1 Настройка квоты

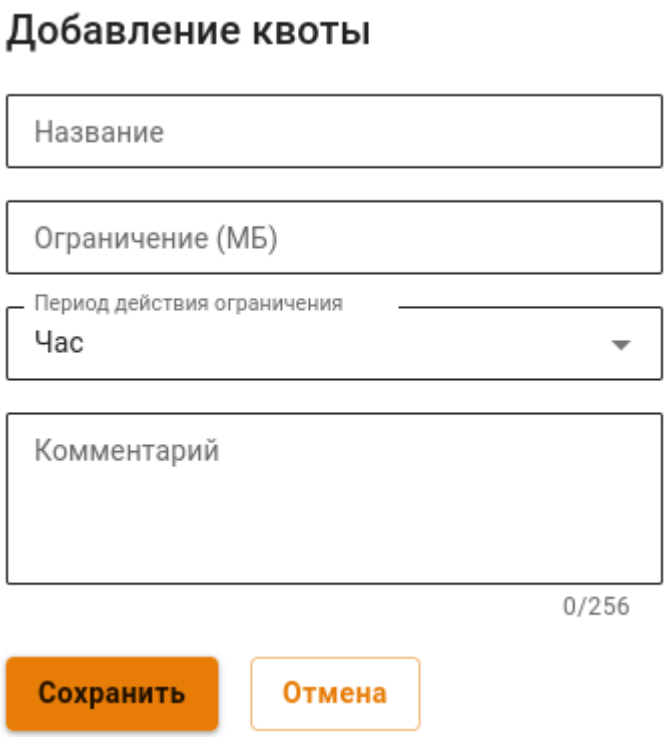
Предупреждение: Для работы всех квот активируйте опцию напротив раздела **Квоты**. При отключении этой опции все квоты, назначенные пользователем сохраняются за ними, но перестают действовать.

Для настройки квоты выполните следующие действия:

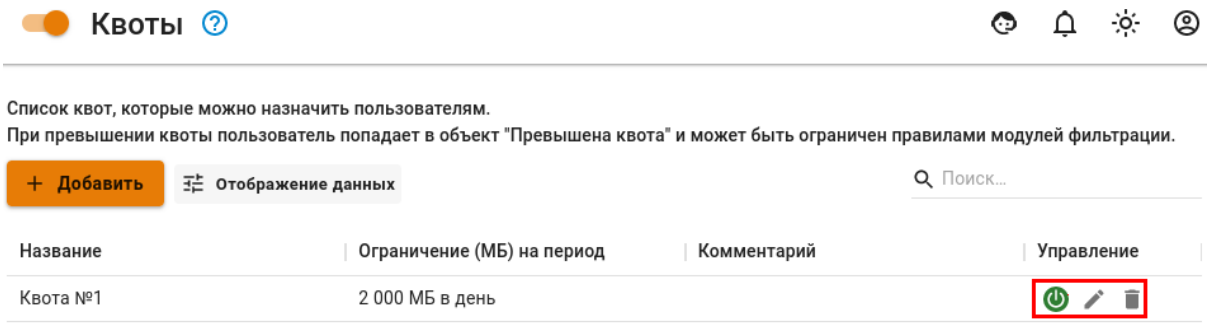
1. Перейдите в раздел **Правила трафика -> Квоты** и нажмите на кнопку **Добавить**.

2. В форме добавления квоты заполните обязательные поля:

- **Название** - введите произвольное название для квоты;
- **Ограничение (МБ)** - задайте ограничение по количеству мегабайт трафика за выбранный период;
- **Период действия ограничения** - выберите период действия, на который будет выделена квота. Время определяется часовым поясом сервера:
  - **День** - с 00:00 по 23:59;
  - **Неделя** - с 00:00 понедельника по 23:59 воскресенье;
  - **Месяц** - с 00:00 1 числа по 23:59 последнего дня месяца;
  - **Квартал** - начало кварталов: 1 января, 1 апреля, 1 июля, 1 октября. 3. Проверьте правильность введенных данных и нажмите на кнопку **Добавить**.



Управление квотами осуществляется с помощью кнопок в столбце **Управление**. Можно отключить или включить квоту, отредактировать или удалить:



15.9.2 Настройка пользователя и группы

Настройка группы:

Созданные квоты можно применить для групп пользователей на вкладке **Квота**.

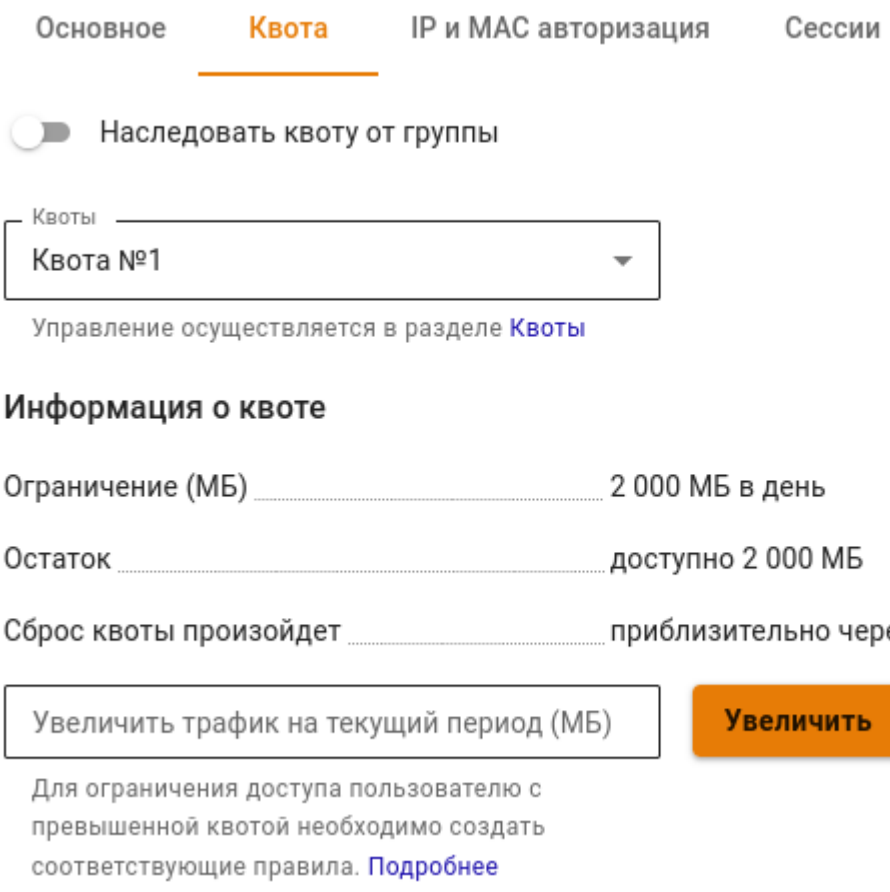
Можно наследовать квоту от вышестоящей группы или выбрать другую квоту, для этого потребуется деактивировать переключатель **Наследовать квоту от группы** и выбрать нужную квоту:

Для этого выберите нужную группу, перейдите на вкладку **Квота**, отключите опцию **Наследовать квоту от группы** и из раскрывающегося списка выберите нужную квоту.

У группы **Все** имеется отдельная опция **Использовать квоты**. Этот параметр позволяет распространить использование квот для всех пользователей:

Настройка пользователей:

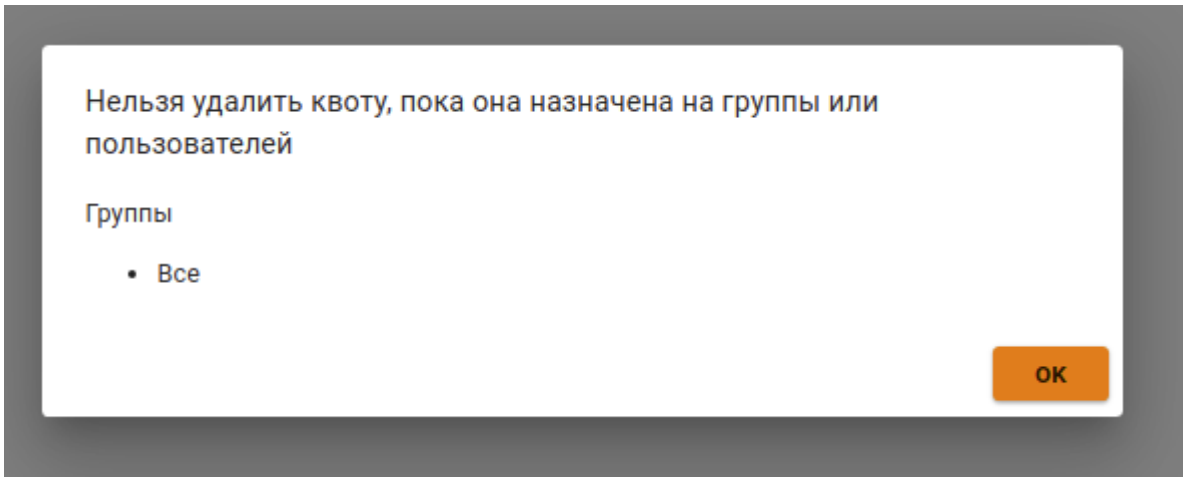
Созданные квоты можно применять для пользователей. Управление квотами происходит на вкладке **Квота** у выбранного пользователя:



На этой вкладке можно настроить наследование квоты у группы, в которой состоит пользователь, или назначить ему персональную квоту.

Если квота назначена на пользователя, то можно посмотреть информацию о ней - период действия, доступный трафик и дату сброса квоты. Здесь же можно ее увеличить, указав нужное количество мегабайт и нажав на кнопку **Увеличить**.

Чтобы удалить квоту, необходимо снять ее со всех пользователей и групп. Иначе при попытке удаления квоты появится окно, запрещающее это действие. Это окно представлено на скриншоте ниже:



Пример настройки действий при превышении квоты

Рассмотрим случай, когда пользователям, превысившим квоту (попавшим в объект **Превышена квота**), будет запрещен доступ ко всем социальным сетям и видеохостингам, а также ограничена скорость до 4 Мбит/с. Но одному пользователю доступ будет разрешен, даже в случае превышения квоты, так как этот сотрудник является маркетологом.

1. Для начала необходимо создать квоту с ограничением, равным 2000 МБ в день.

2. Во всех группах и у всех пользователей на вкладке **Квота** поставить переключатель **Наследовать квоту от группы** в положение включен. Это нужно сделать только в том случае, если его положение менялось, так как по умолчанию все группы и пользователи создаются с включенным переключателем.

3. На группу **Все** назначить созданную квоту (все остальные группы и пользователи унаследуют назначение этой квоты).

4. Создать правило в *контент-фильтре* для ограничения доступа к социальным сетям и видеохостингам для пользователей, превысивших квоту.

5. Создать правило, которое разрешает одному из пользователей социальные сети, даже если он превысил квоту.

6. Создать правило, ограничивающее скорость всем пользователям в разделе *Ограничение скорости*, которые попали в объект **Превышена квота**, до 4 Мбит/с.

16. Сервисы

16.1 Сетевые интерфейсы

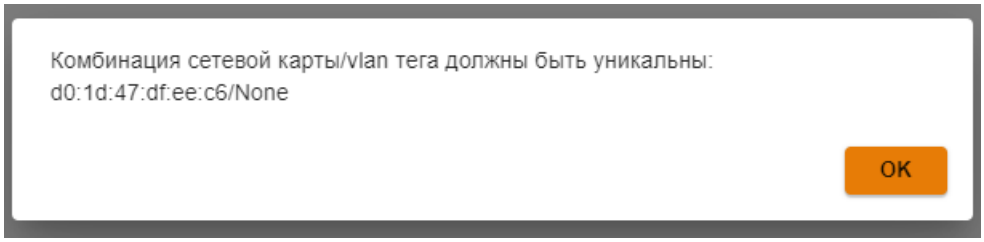
Подсказка: Название службы раздела *Сетевые интерфейсы*: `ideco-network-backend`; `ideco-network-nic`.
Список имен служб для других разделов доступен по *ссылке*.

Все созданные интерфейсы представлены в виде таблицы:

В режиме редактирования появляется возможность смены названия, сетевой карты (по кнопке), зоны 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 **Комбинации сетевой карты/vlan тега должны быть уникальны**:



Подсказка: При миграции NGFW с одной физической машины на другую (перенос диска или восстановление резервной копии на новом оборудовании), будут восстановлены настройки всех сетевых интерфейсов, указанные до миграции. Для удаления ненужных интерфейсов воспользуйтесь кнопкой  .

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.

16.1.1 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.

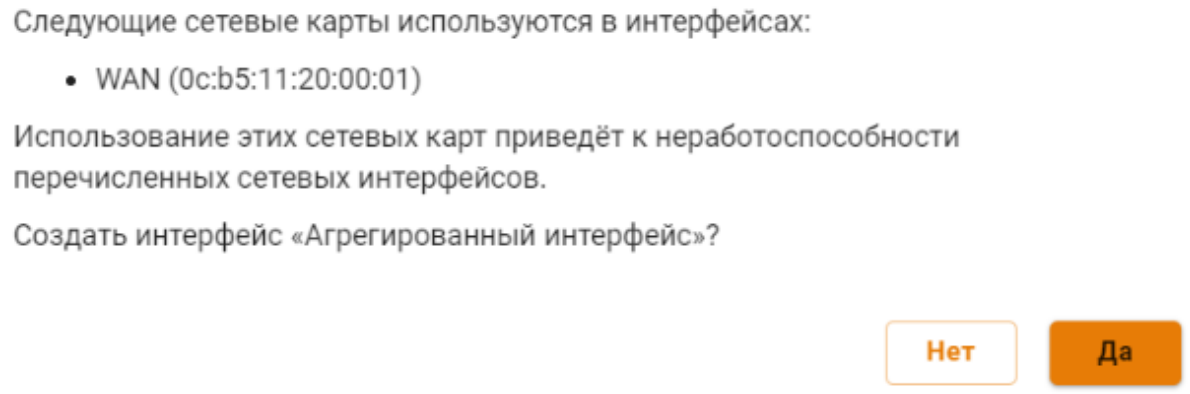
Количество сетевых карт, объединяемых в агрегированный интерфейс, не ограничено.

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 **Сохранить**.

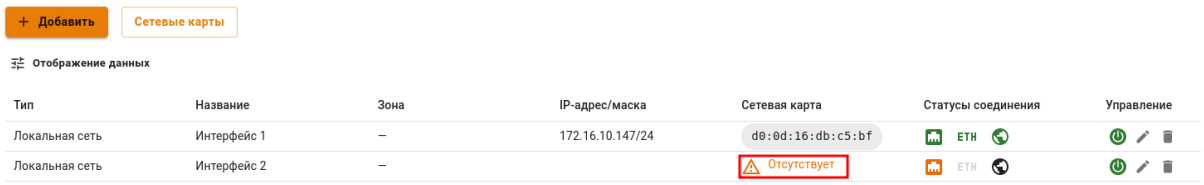
При выборе сетевой карты обращайте внимание на пиктограммы:

-  - сетевая карта уже используется другим интерфейсом;
-  - сетевая карта не используется.

Если были выбраны уже использующиеся сетевые интерфейсы, то при нажатии на кнопку **Сохранить** появится сообщение:



При нажатии на **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.

16.1.2 Настройка Локального Ethernet

Внимание: Будьте внимательны!

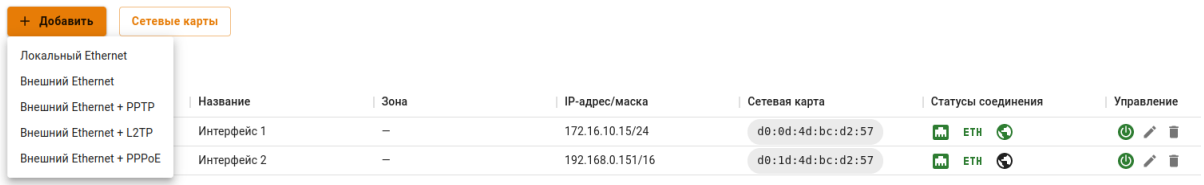
При выборе пункта **Локальный Ethernet** и настройке его как **Внешний Ethernet, доступ в интернет будет отсутствовать.**

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, указанные в таблице ниже:

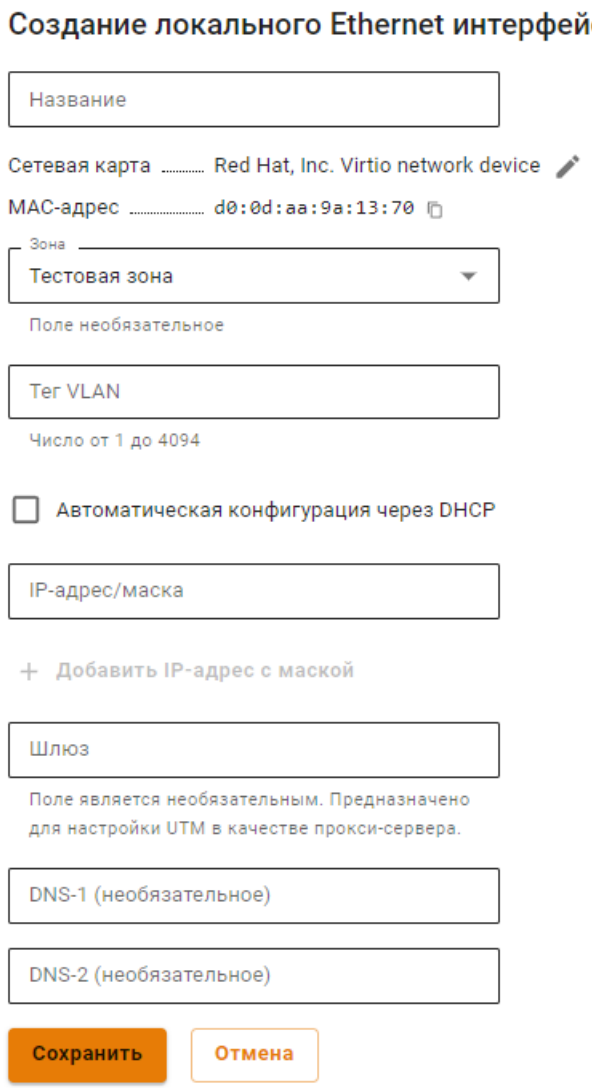
- **Название интерфейса** - имя для идентификации интерфейса;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения 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).

Внимание: Поле **Шлюз** в Локальном интерфейсе задается только, если:

- Нет Внешнего интерфейса NGFW;
- NGFW используется как прокси-сервер.

Пример настройки:

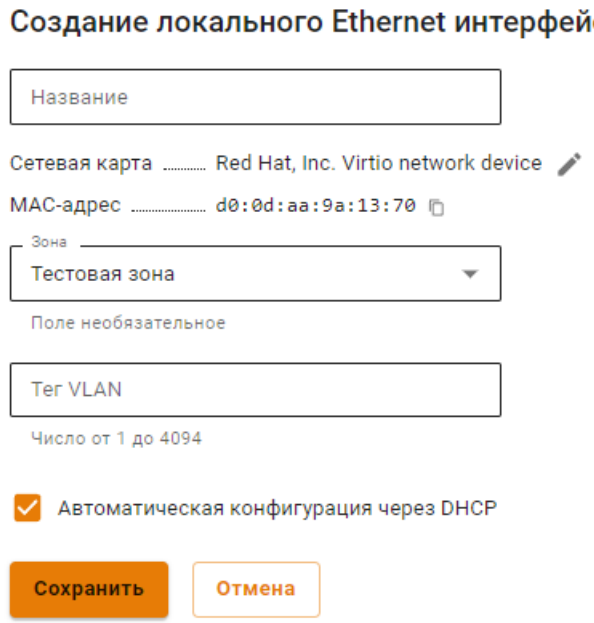


Автоматическая настройка

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 **Сохранить**.

Пример настройки:



16.1.3 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, указанные в таблице ниже:

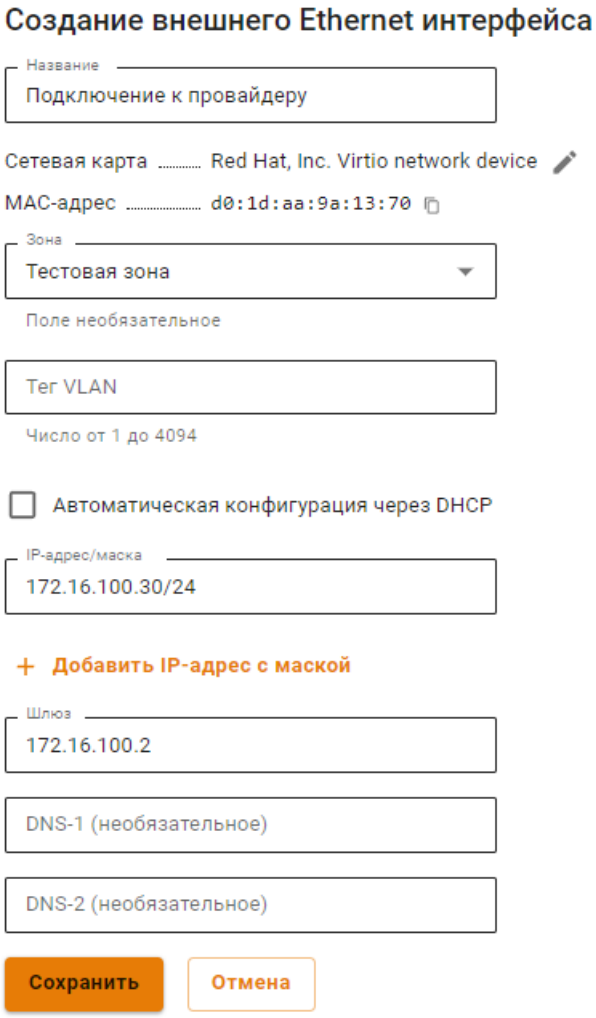
- **Название интерфейса** - имя, с помощью которого возможно в дальнейшем идентифицировать интерфейс;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой 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).

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
```

Пример настройки:

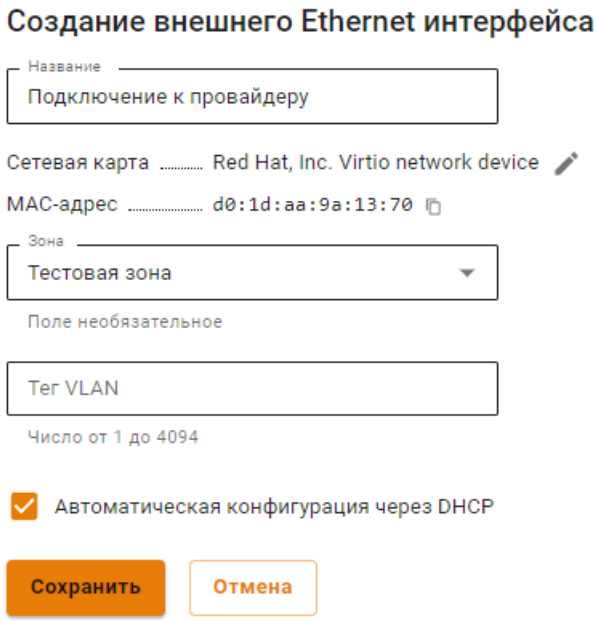


Автоматическая настройка

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 **Сохранить**.

Пример настройки:



16.1.4 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**.

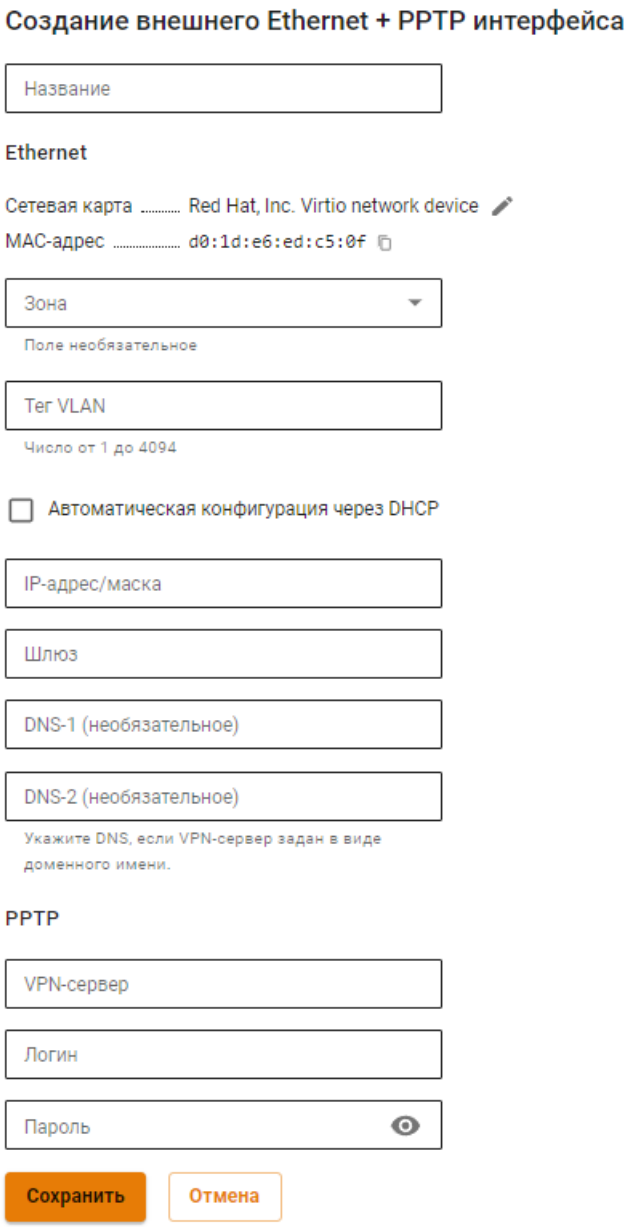
3. Выберите сетевую карту.

4. Заполните поля, указанные в таблице ниже:

- **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.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Пример настройки подключения по PPTP:



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
```

16.1.5 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**.

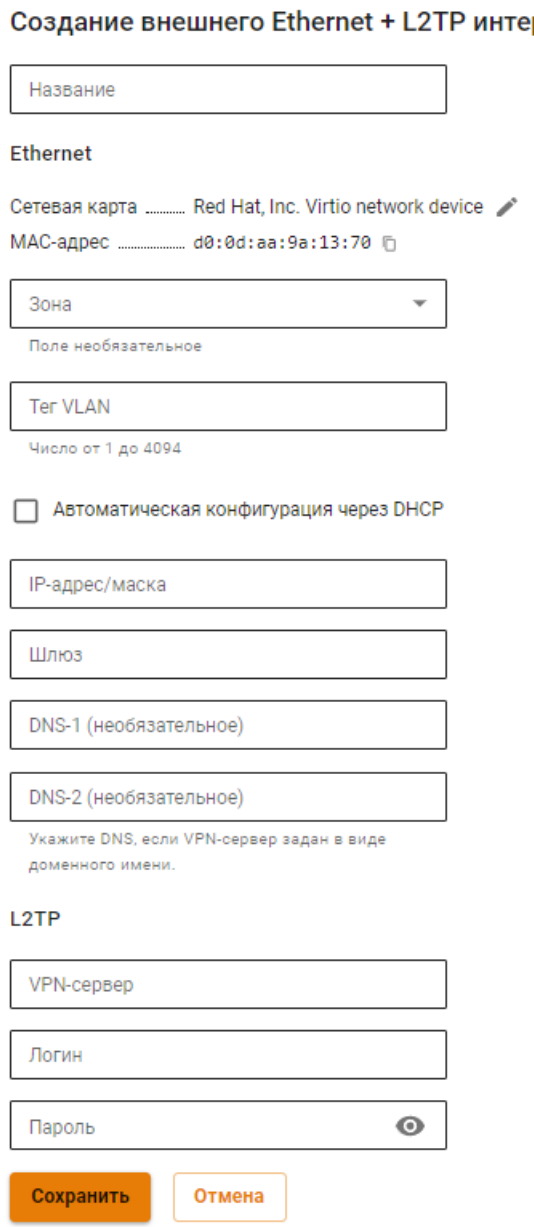
3. Выберите сетевую карту.

4. Заполните поля, указанные в таблице ниже:

- **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.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Пример настройки:



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
```

16.1.6 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**.

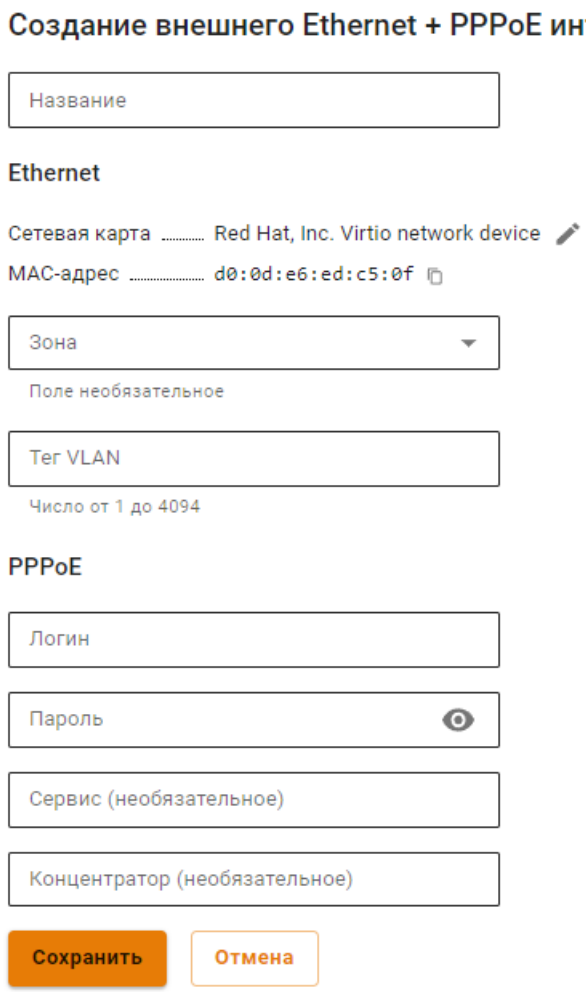
3. Выберите сетевую карту.

4. Заполните поля, указанные в таблице ниже:

- **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.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Пример настройки:



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
```

16.1.7 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
```

16.2 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.

16.2.1 Основное

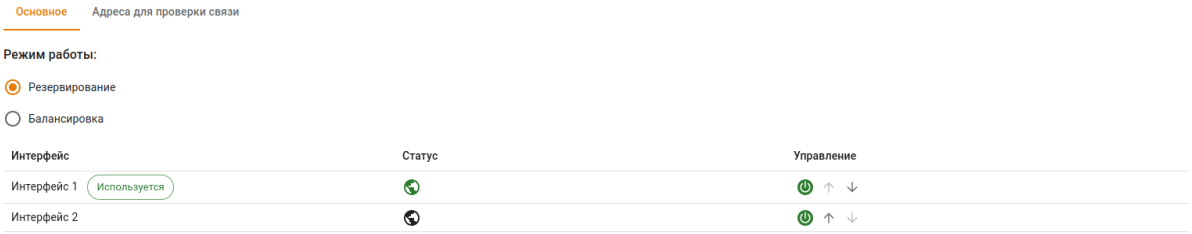
На вкладке доступен выбор одного из двух режимов - **Балансировка** или **Резервирование**.

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**.



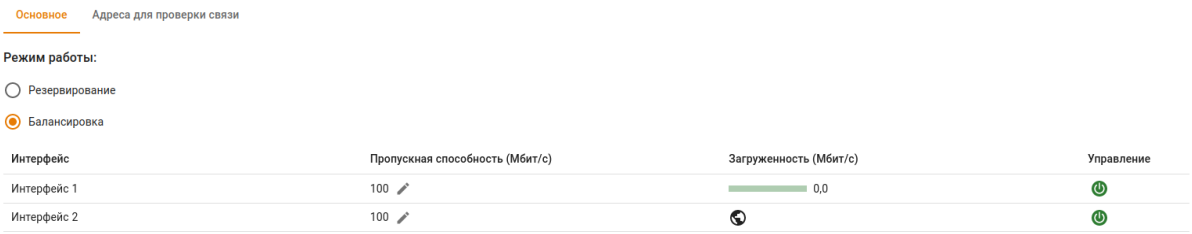
Подключение, которое используется в данный момент, отмечено тегом **Используется**. Для смены приоритета используйте соответствующие элементы управления (↑ ↓).

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 UTM 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:

```
[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
```

Статическая балансировка. Доступ к сети интернет через определенное подключение к провайдеру

Способы применения:

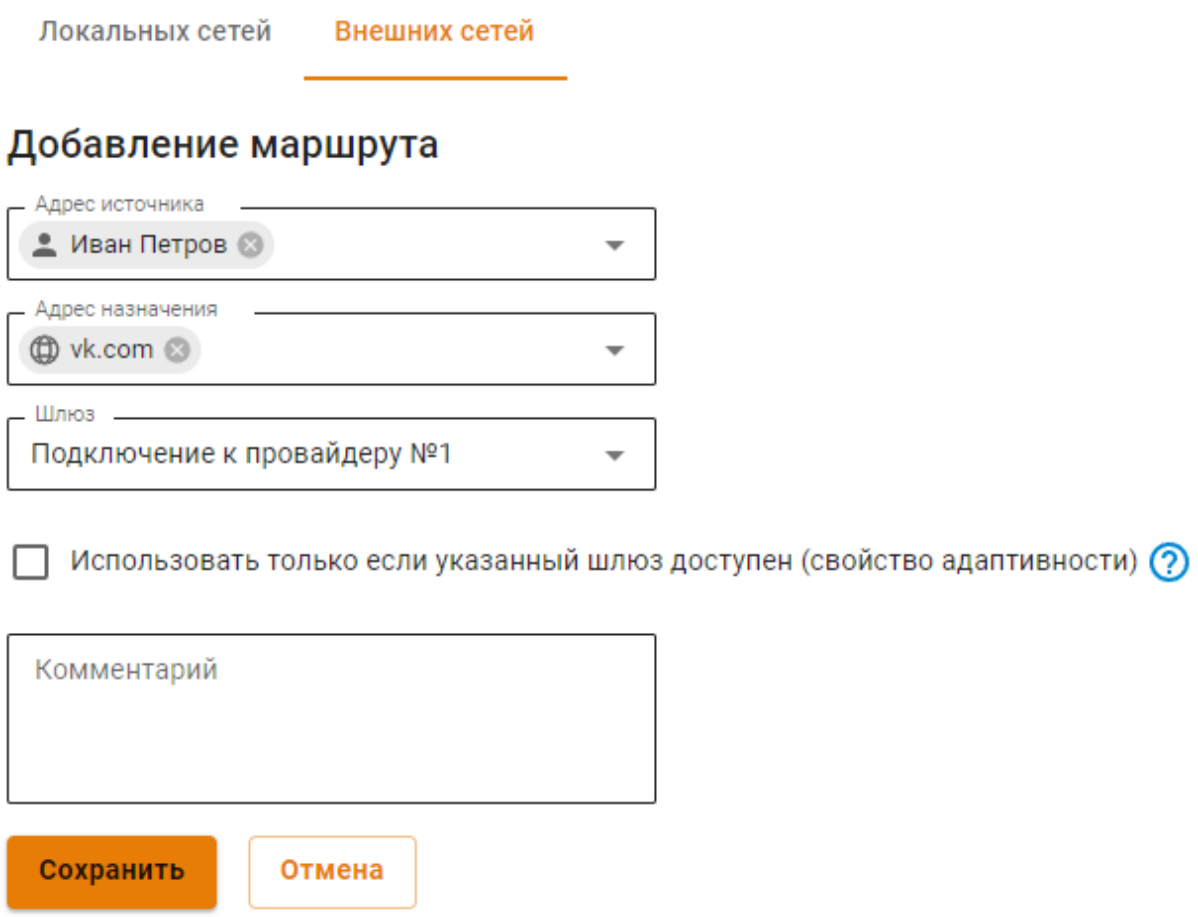
- Направление части трафика через интернет-провайдера, чья тарификация для этого трафика дешевле.
- Предоставление доступа к внутренним сетям одного из провайдеров для определенных пользователей/групп пользователей.

Действия для настройки:

1. Перейдите в раздел меню **Сервисы -> Маршрутизация -> Внешних сетей**.

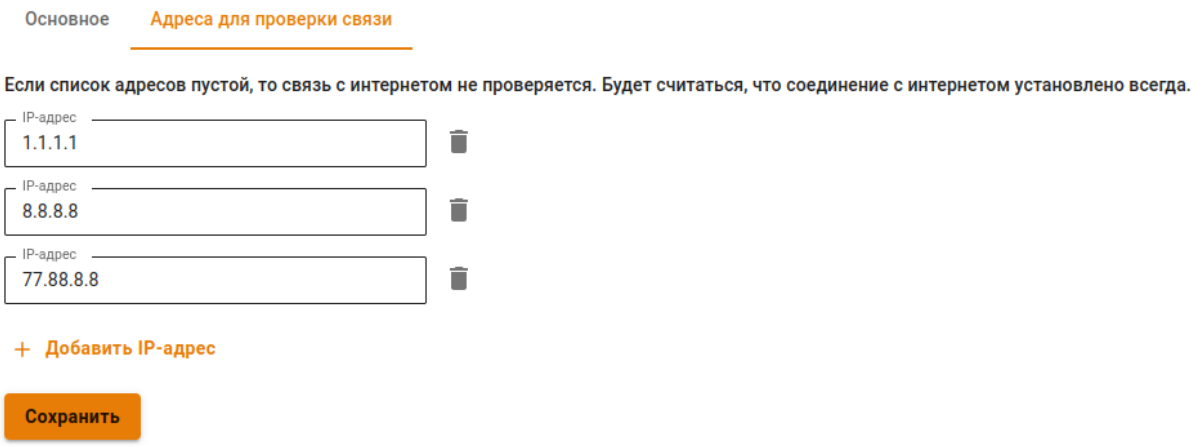
2. Добавьте правила маршрутизации для определенного списка ресурсов, трафик к которым необходимо направить через нужное подключение к провайдеру, нажав кнопку **Добавить**.

Пример направления трафика к ресурсу **vk.com** от пользователя **Иван Петров** через подключение к провайдеру **Подключение к провайдеру №1**:



16.2.2 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.

16.3 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).

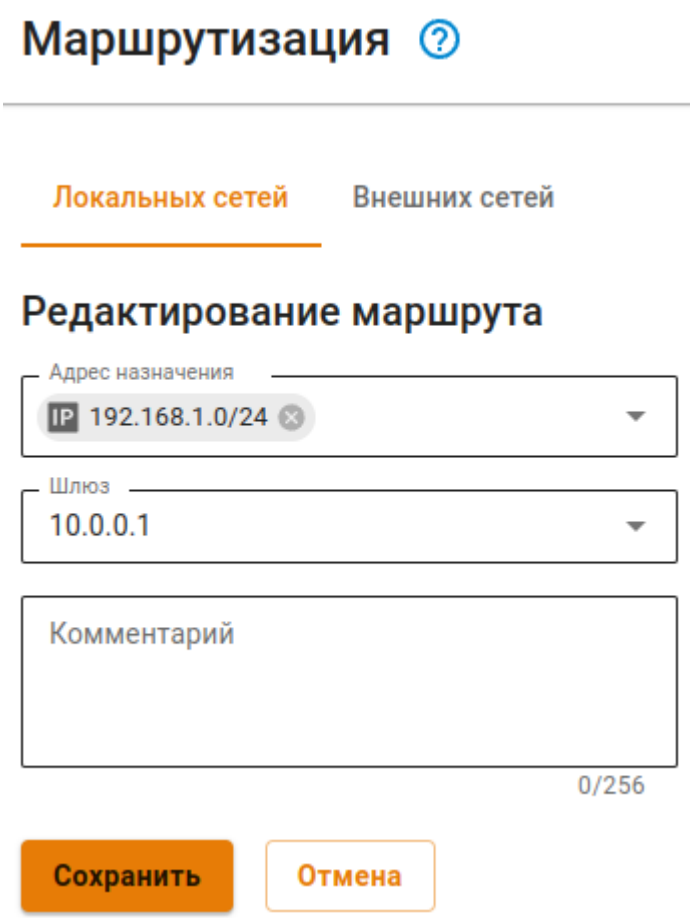
Подсказка: Доступность шлюза проверяется с помощью ICMP-запросов к набору IP-адресов, который определяется производителем сетевой карты.

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*.

16.3.1 Маршрутизация локальных сетей

Маршрутизация локальных сетей действует внутри локальных сетей. Поэтому при добавлении маршрута отсутствует поле **Адрес источника**. Для добавления нового маршрута перейдите на вкладку маршрутизации **Локальных сетей** и нажмите **Добавить**:

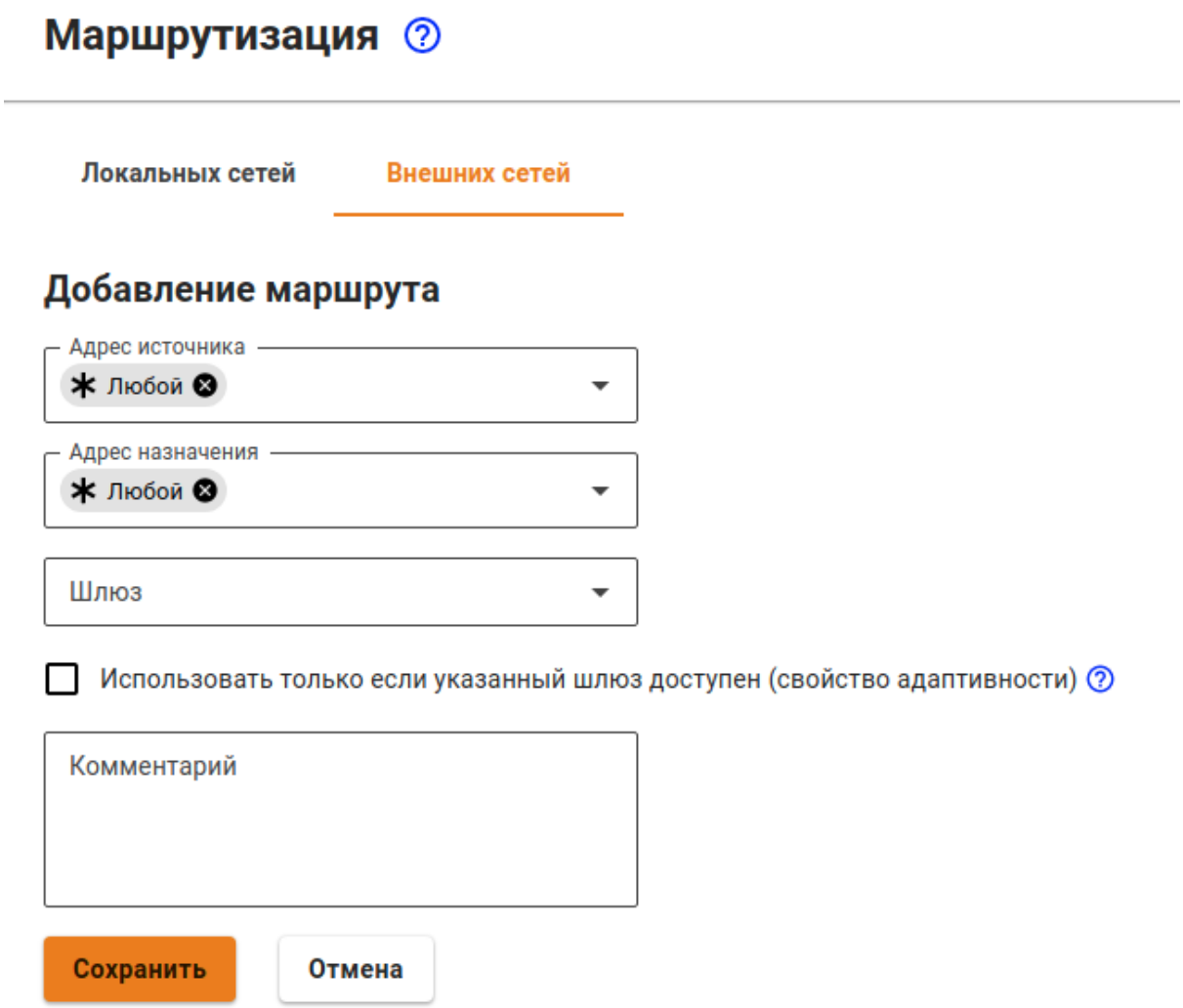


- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться это правило. Возможные типы объектов: IP-адрес, подсеть;
- **Шлюз** - выберите объект, через который направляется трафик. Возможный тип объекта: IP-адрес
- **Комментарий** - необязательное поле для описания маршрута. Значение - не длиннее 128 символов.

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**.

16.3.2 Маршрутизация внешних сетей

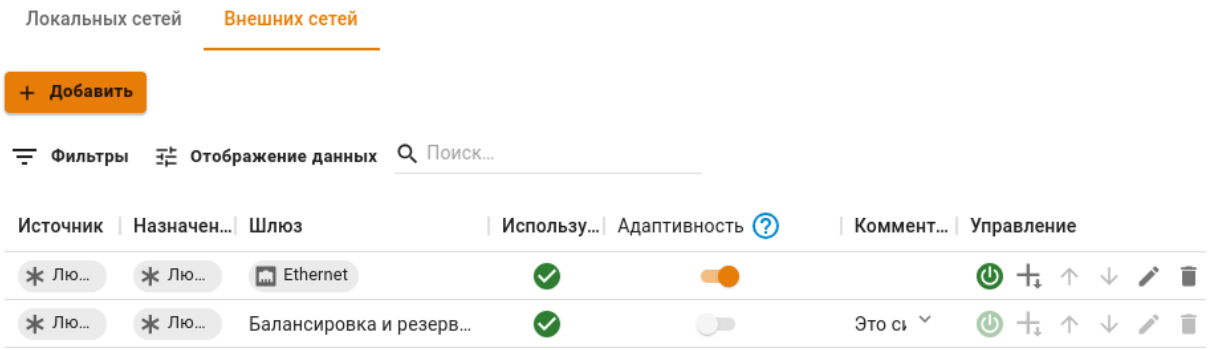
Для добавления нового маршрута перейдите на вкладку маршрутизации **Внешних сетей** и нажмите кнопку **Добавить**. На странице откроется форма создания маршрута:



Опишем назначение каждой опции:

- **Адрес источника** - выберите объекты, для которых будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, домен, диапазон IP-адресов, подсеть, список адресов;
- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, домен, диапазон IP-адресов, подсеть, список адресов;
- **Шлюз** - выберите объект, через который будет направлен трафик. Возможный тип объекта: 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, а 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 для описания маршрута. Значение не должно быть длиннее 128 символов.

После сохранения маршрута страница выглядит так:



Кнопки ↓ и ↑ повышают или понижают приоритет правила.

Статусы в столбце **Используется**:

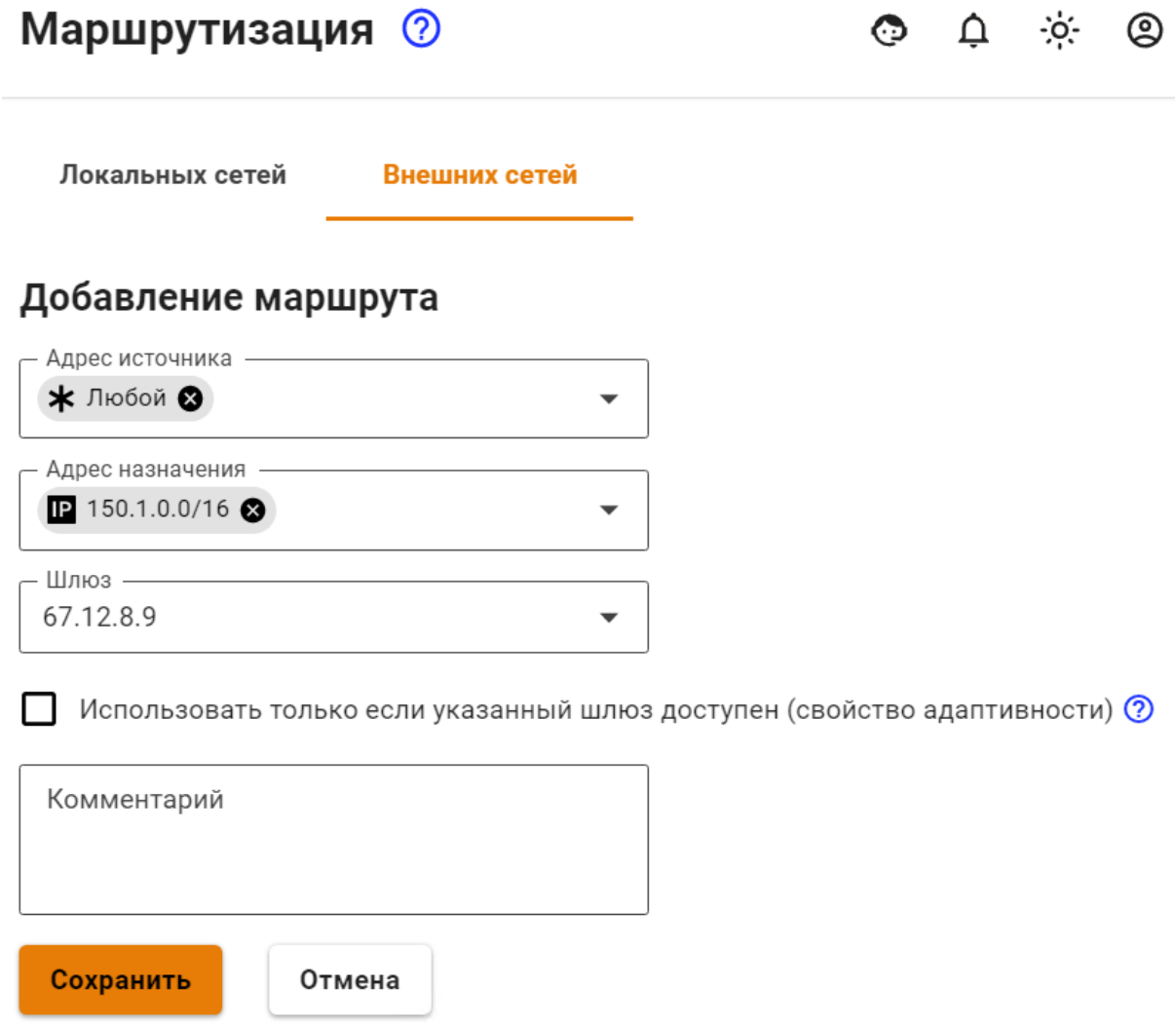
- ✓ - маршрут активен и трафик, попадающий под условия маршрута, будет перенаправлен в указанный Шлюз;
- ⊖ - маршрут не активен и трафик, попадающий под условия маршрута, не будет обработан правилом.

Подсказка: Трафик, не попавший под условия правил маршрутизации, или с объектом **Любой** в качестве шлюза, будет отправлен в *Балансировку и резервирование*.

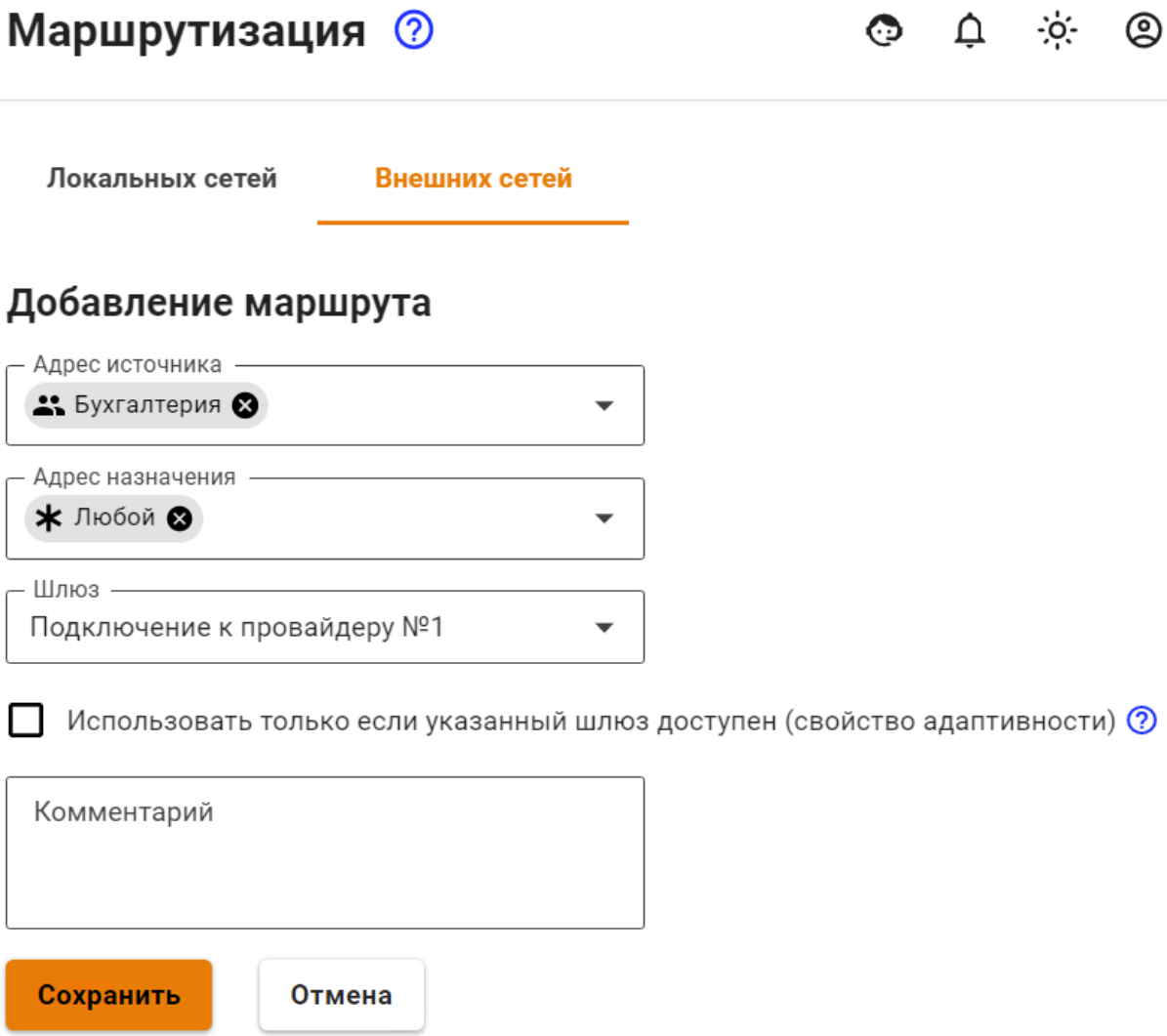
Примеры популярных маршрутов

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 просто не будет работать. SNAT можно настроить с помощью *файрвола*.

Задача: любой трафик в подсеть `150.1.0.0/16` **направлять на шлюз** `67.12.8.9`**:**



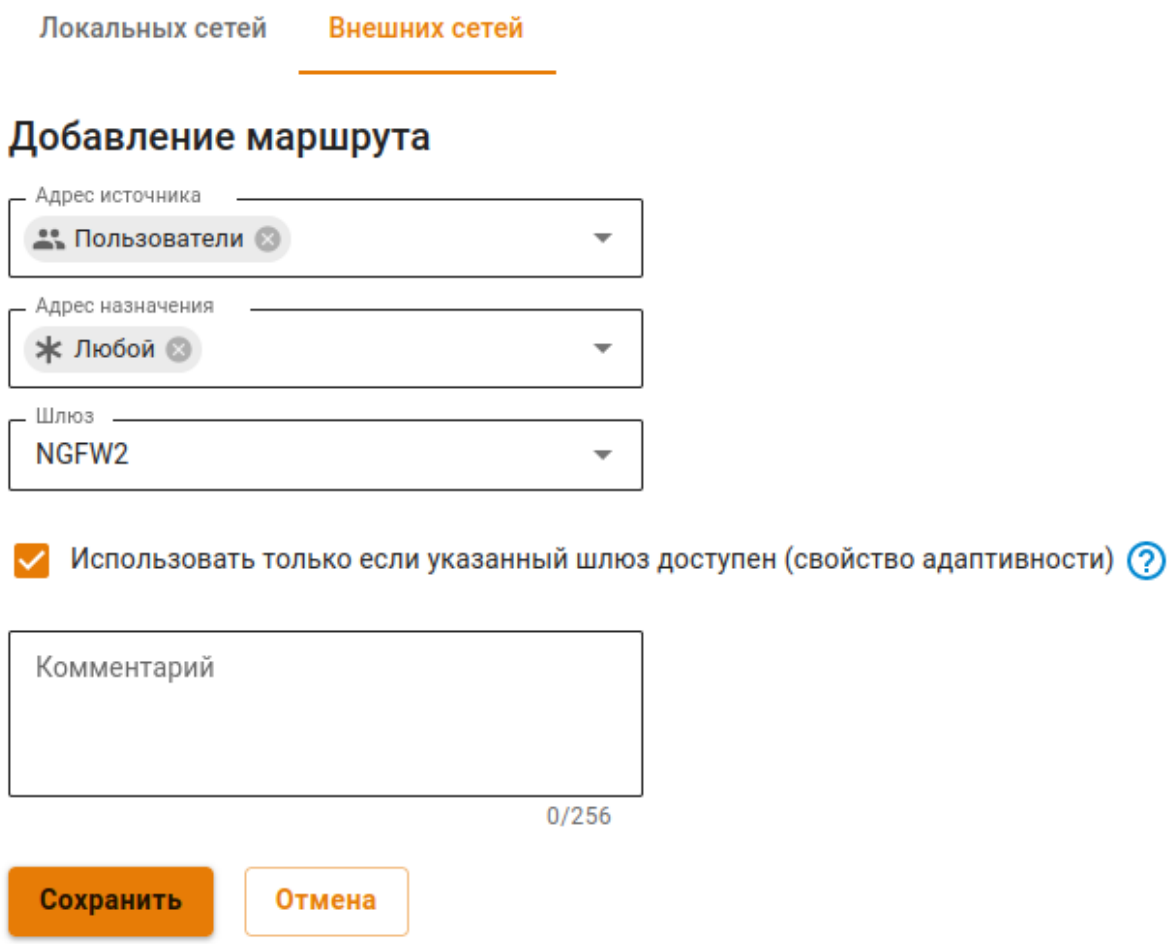
Задача: весь трафик пользователей из группы Бухгалтерия направить через шлюз выбранного сетевого интерфейса:



Если настраивается маршрут в удаленную сеть через дополнительный роутер, расположенный в одной локальной сети с клиентами, то убедитесь, что нет «асимметричной маршрутизации» и роутер вынесен в DMZ. Подробнее в статье *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:



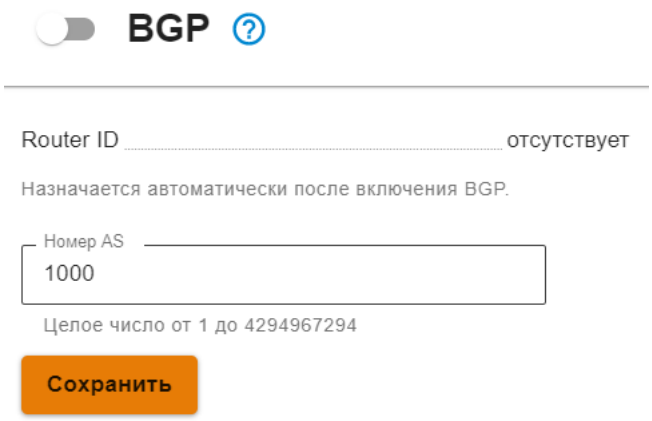
16.4 BGP

Подсказка: Название службы раздела **BGP**: `frr.service`; `ideco-routing-backend`.
Список служб для других разделов доступен по *ссылке*.

BGP (Border Gateway Protocol) — это основной протокол динамической маршрутизации, который используется в интернете.

16.4.1 Настройка своей автономной системы

1. Введите номер автономной системы в строку **Номер AS** и нажмите **Сохранить**:



2. Переведите опцию раздела **BGP** в положение **включен**;

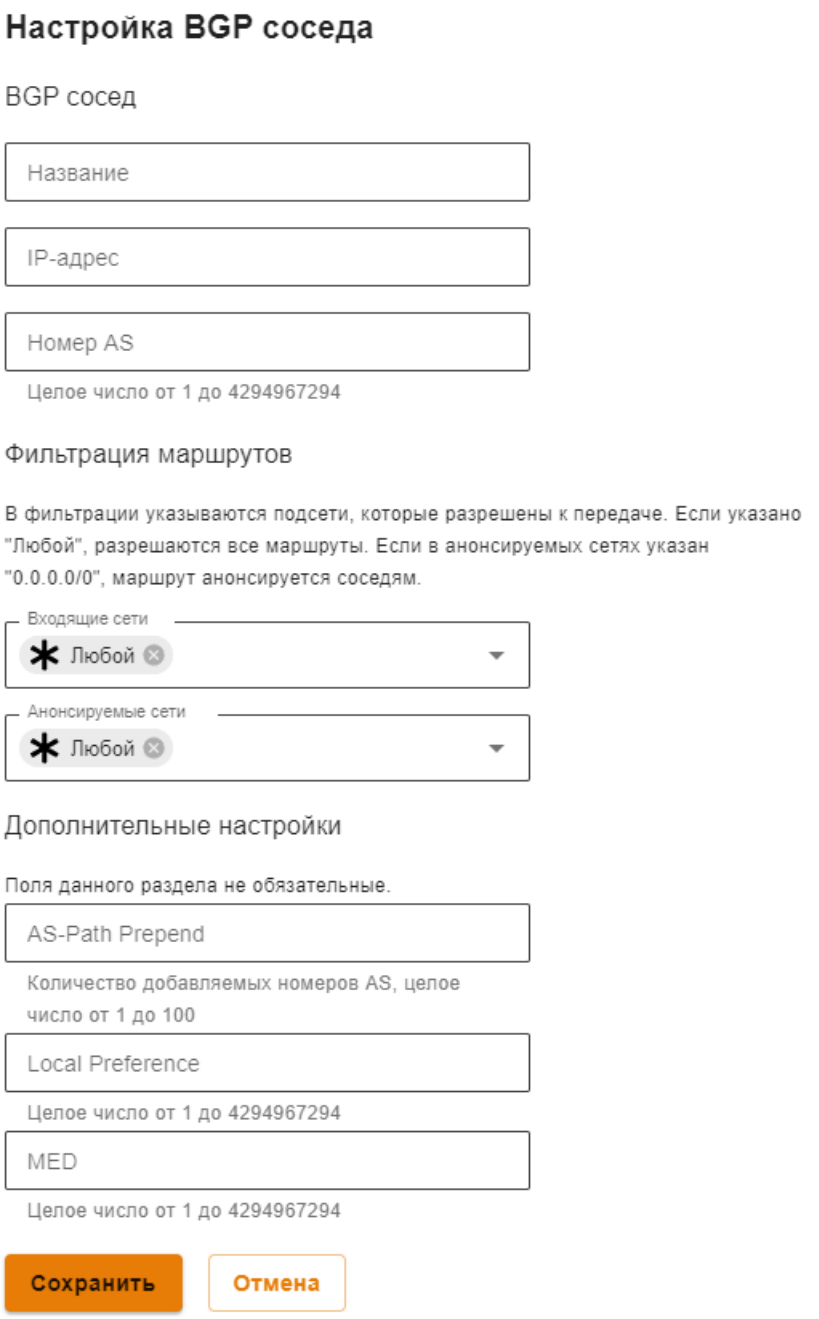
3. Ideco NGFW заполнит поле **Router ID** автоматически, если опция раздела **BGP** в положении **включен**.

16.4.2 Настройка BGP-соседей

1. Для добавления BGP-соседа нажмите **Добавить** в правом верхнем углу;

2. Заполните следующие поля:

- **Название** - любое значение;
- **IP-адрес** - IP-адрес BGP-соседа;
- **Номер AS** - номер AS BGP-соседа;
- **Входящие сети** - фильтр, в котором нужно выбрать 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** - фильтр, в котором нужно выбрать 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.

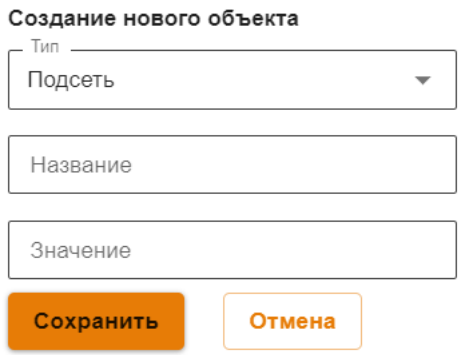


Подсказка: Для динамической маршрутизации сетей двух NGFW, соединенных по IPSec, воспользуйтесь BGP. Подробнее про настройку подключения двух NGFW по IPSec - в статье *Подключение по IPsec между двумя Ideco NGFW*

Подсказка: Для **Входящих сетей** и **Анонсируемых сетей** объект **Любой** не может быть установлен одновременно с другими фильтрами.

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*.



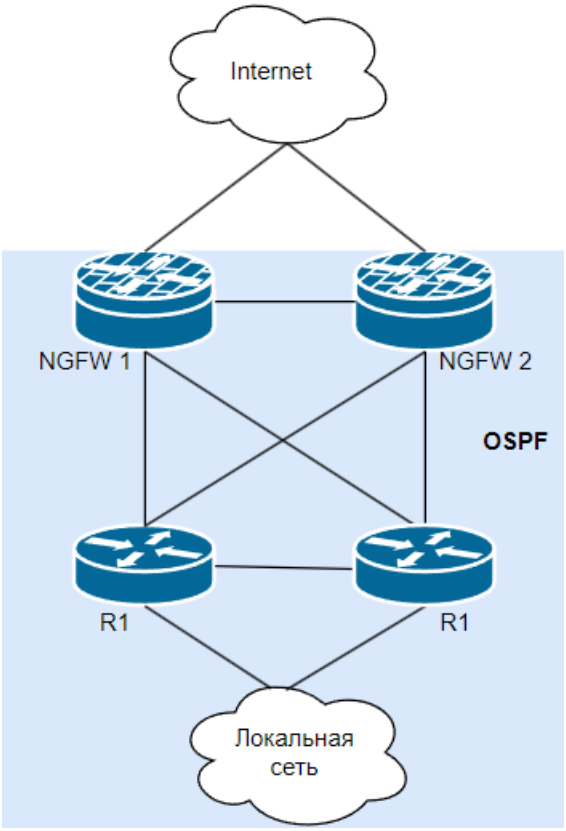
16.5 OSPF

Подсказка: Название службы раздела **OSPF**: `frr.service; 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.

Использование модуля лучше всего в сетях, использующих балансировку нагрузки на сеть и резервирование каналов.

Пример топологии с использованием OSPF представлен на схеме ниже:

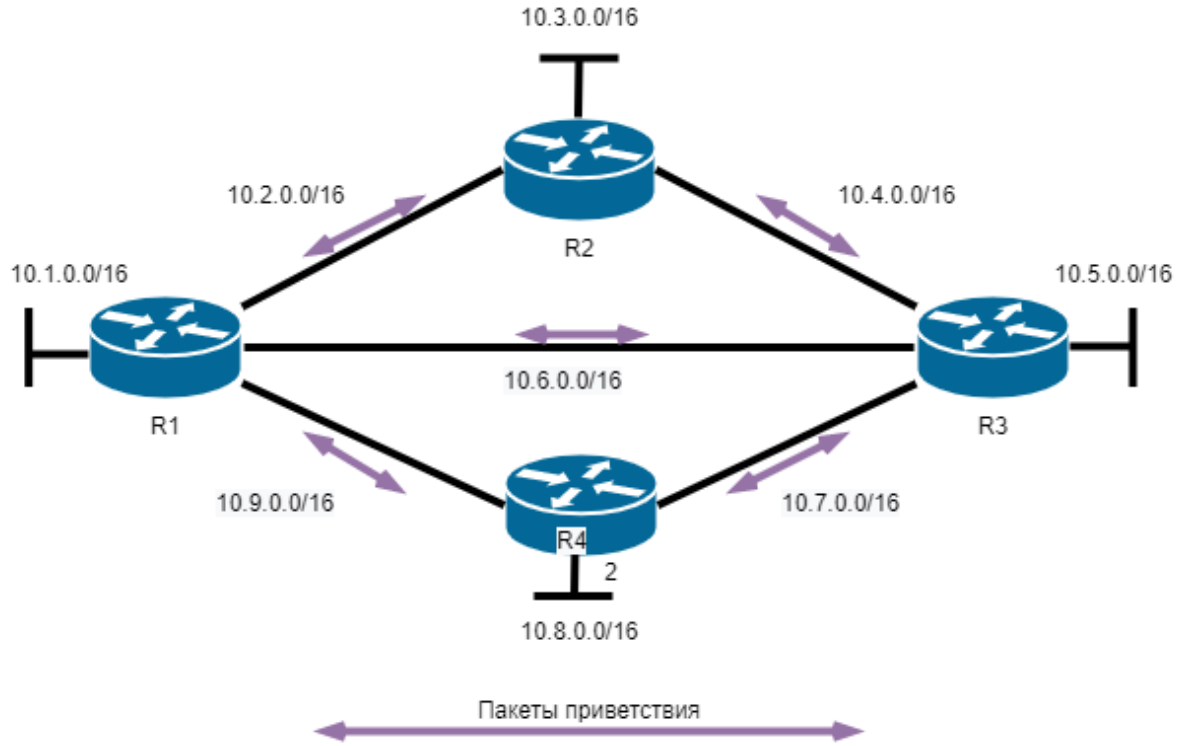


Принцип работы маршрутизации по состоянию канала:

1. Установление отношений смежности с соседними устройствами

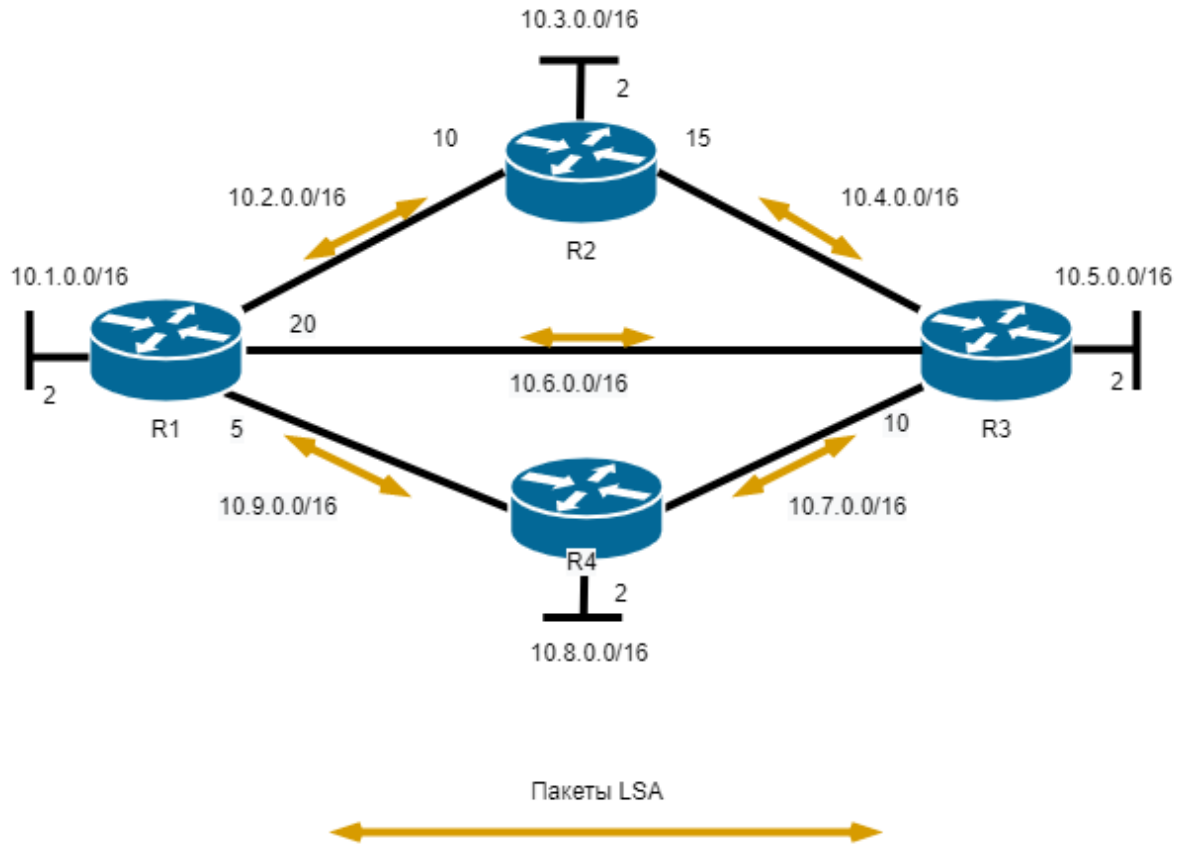
Маршрутизатор, использующий OSPF, отправляет Hello-пакеты на мультикастовый адрес 224.0.0.5 со всех

интерфейсов, где запущен OSPF. При наличии соседнего устройства маршрутизатор пытается установить с ним отношения смежности.



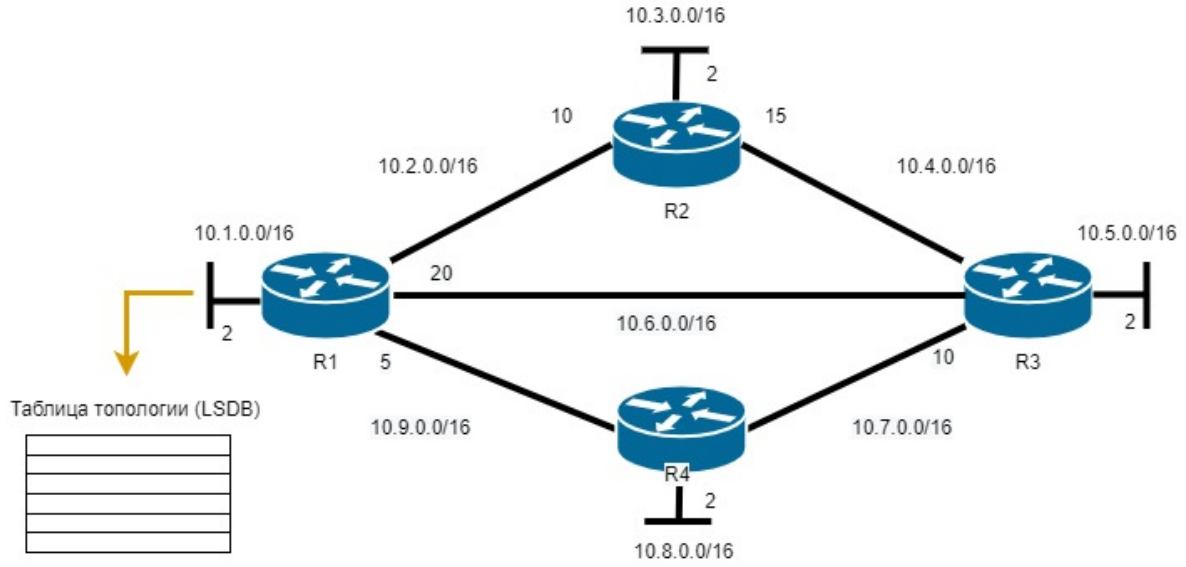
2. Обмен объявлениями о состоянии каналов

После установления смежности устройства выполняют обмен LSA. LSA содержат информацию о состоянии и стоимости каждого канала с прямым подключением.



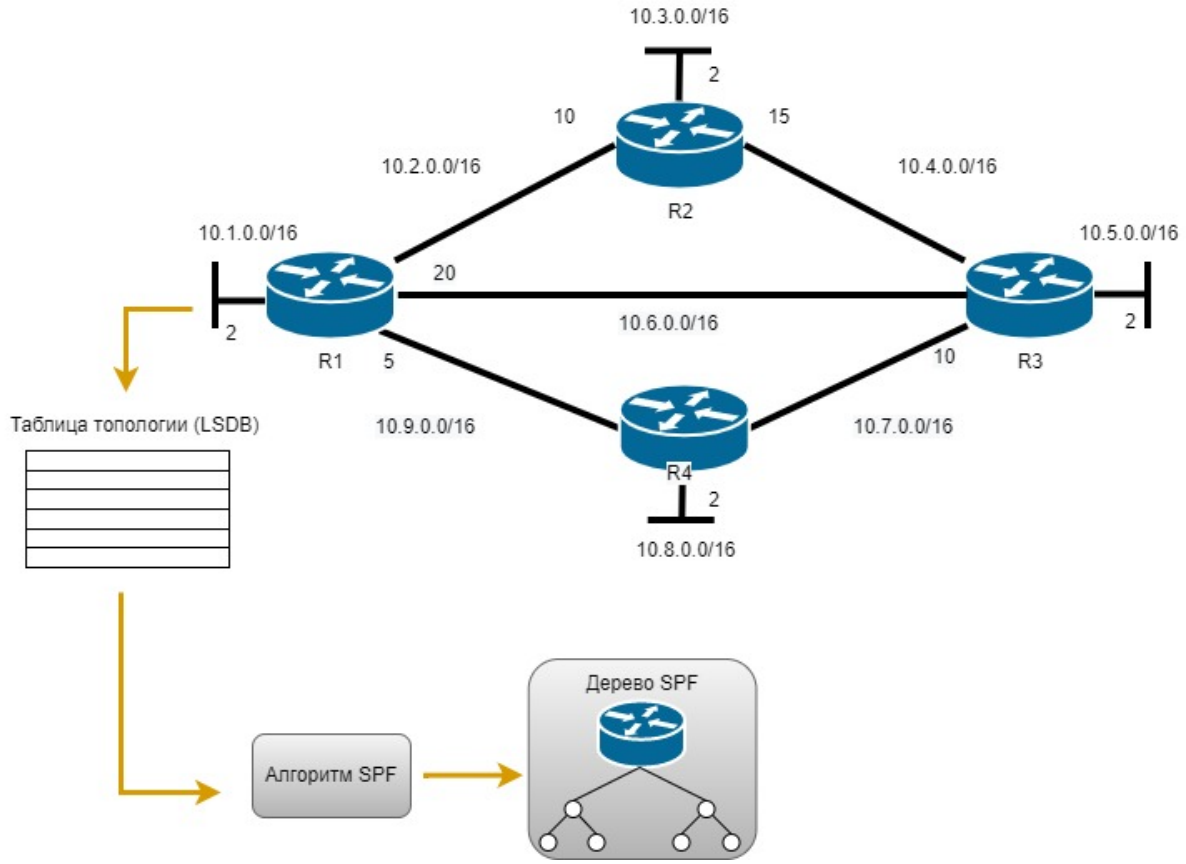
3. Создание базы данных состояния связи

На основе объявления LSA маршрутизаторы собирают базу данных, в которой содержатся данные о топологии сети в области.



4. Исполнение алгоритма SPF

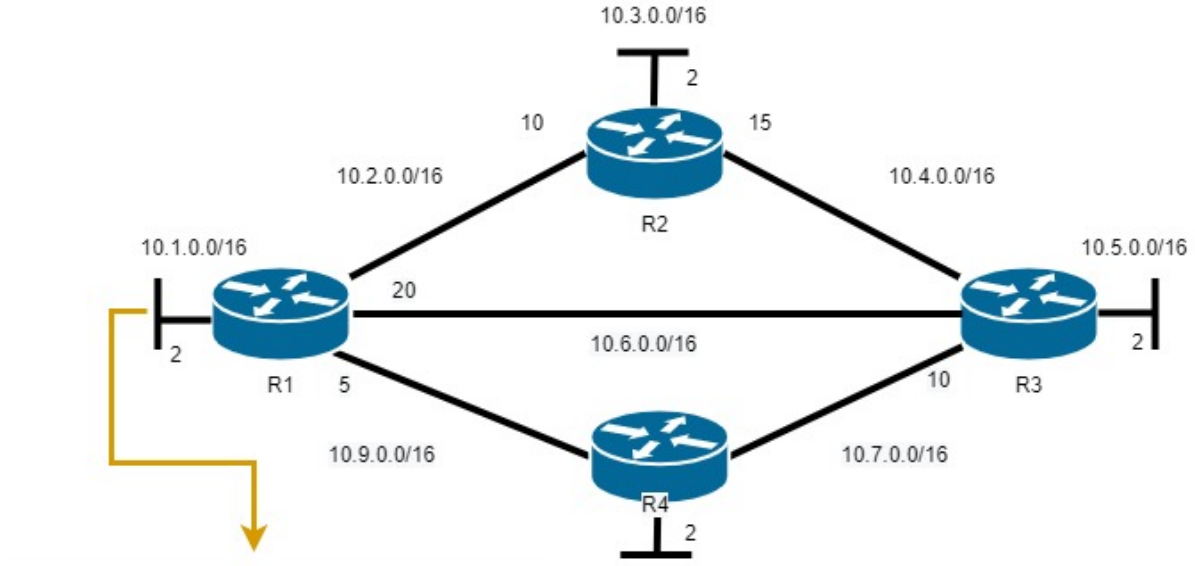
На устройствах выполняется алгоритм SPF, результатом которого является создание дерева кратчайших путей.



5. Выбор лучшего маршрута

На основании данных дерева SPF обновляются данные в таблице IP-маршрутизации. Маршрут добавляется в таблицу маршрутизации, если отсутствует источник маршрута к той же сети с меньшим административным

расстоянием, например, статический маршрут.
Решения по маршрутизации пакетов принимаются на основе записей в таблице маршрутизации.



Название	Кратчайший путь	Стоимость
10.3.0.0/16	R1 -> R2	12
10.4.0.0/16	R1 -> R2	25
10.5.0.0/16	R1 -> R3	22
10.7.0.0/16	R1 -> R4	17
10.8.0.0/16	R1 -> R4	7

16.5.1 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 следующие действия:

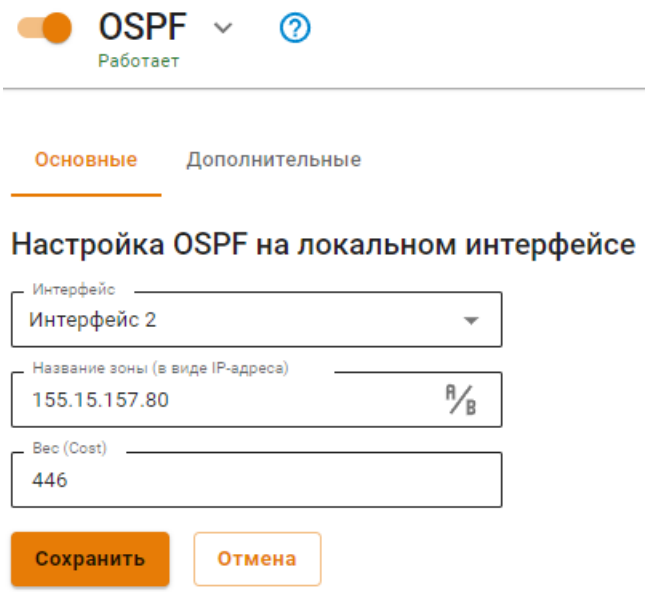
1. В веб-интерфейсе NGFW перейдите в раздел **Сервисы –> OSPF –> Основные** и нажмите кнопку **Добавить**.

2. Заполните следующие поля:

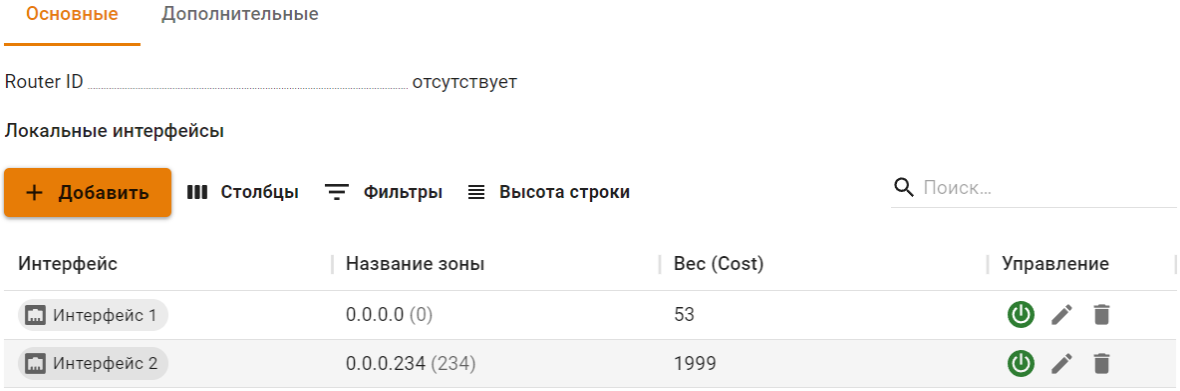
- **Интерфейс** - выберите локальный интерфейс, подключенный к роутеру;
- **Название зоны** - введите номер зоны (для небольших сетей введите зону 0). Наименование зоны можно ввести в виде числа или IP-адреса, нажав иконку A/B ;
- **Вес** - введите стоимость маршрута.

3. Нажмите **Сохранить.**

Пример настройки:



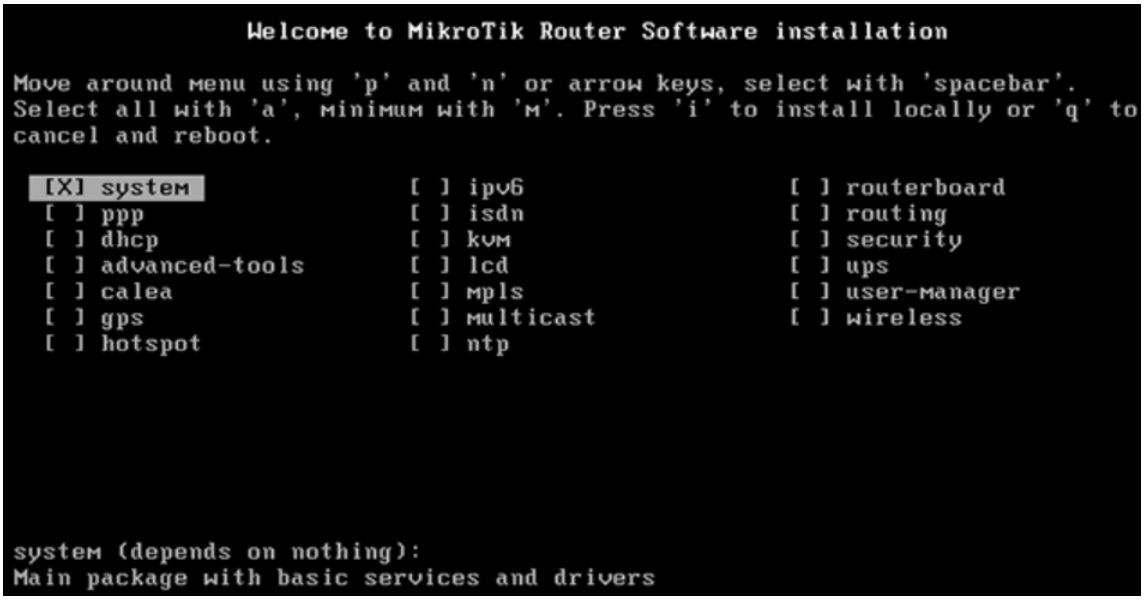
Пример готовой таблицы:



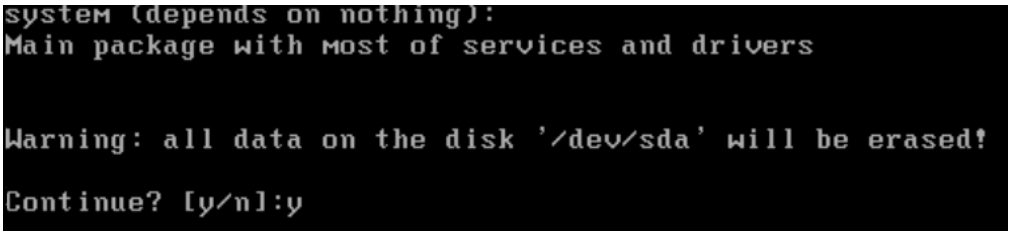
Настройка MikroTik:

1. Установите и запустите RouterOS:

   - Поставьте крестик на модуле **Routing**;
   - Укажите необходимые интерфейсы, но БЕЗ статических маршрутов:



- Для начала установки введите **i** и нажмите **Enter**;
- Появится сообщение «All data on the disk will be erased. Continue?», ведите **y** и нажмите **Enter**:



2. После установки RouterOS требуется его перезагрузить, нажав **Enter**:

3. По умолчанию *логин* - `admin`, а *пароль* - пустое значение;

4. Установите логин/пароль администратора;

5. Выполните следующую команду:

`routing ospf area add area-id=x.x.x.x default-cost=1 disabled=no inject-summary-lsa=no name=area1 type=default`,
где `x.x.x.x` - **название зоны, которое указали при настройке Ideco NGFW**. ID должен быть уникален для каждого роутера;

6. Для передачи любых других сетей соседним устройствам по динамической маршрутизации введите следующую команду:

`routing ospf network add network=(другая подсеть)/24 area=area1`

7. Повторите команду из п. 6 для добавления каждой подсети;

8. Для вывода таблицы маршрутизации введите команду:

`ip route print`

16.5.2 Дополнительное

Во вкладке Дополнительное 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 во вкладке **Сервисы -> Маршрутизация -> Локальных сетей**;
- **Redistribute connected** - будут анонсироваться маршруты напрямую подключенных подсетей.

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)**.

16.6 IGMP Proxy

Подсказка: Название службы раздела **IGMP Proxy**: `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).

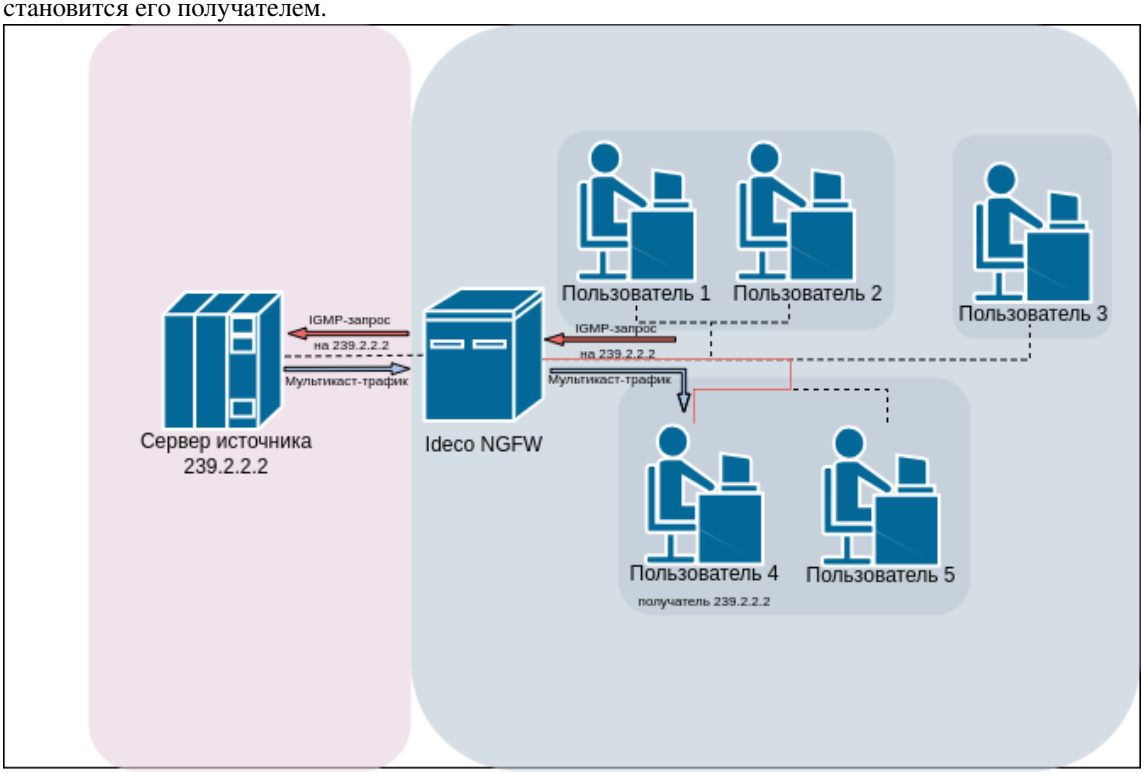
IGMP Proxy - служба, которая проксирует (передает) мультакаст-трафик сквозь роутер. Это сокращает объем трафика, что влияет на скорость работы и нагрузку сети.

16.6.1 Принцип работы

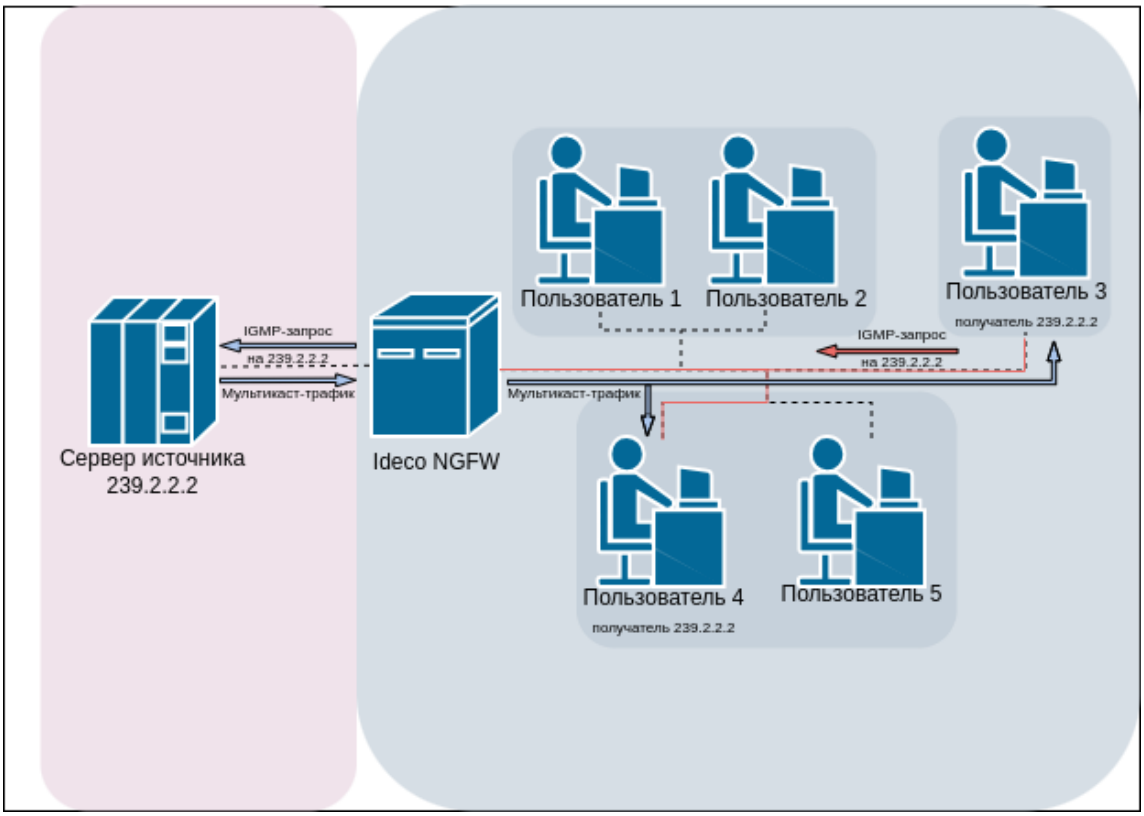
Со стороны клиентов IGMP Proxy поддерживает версии IGMPv1 и IGMPv2.

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.



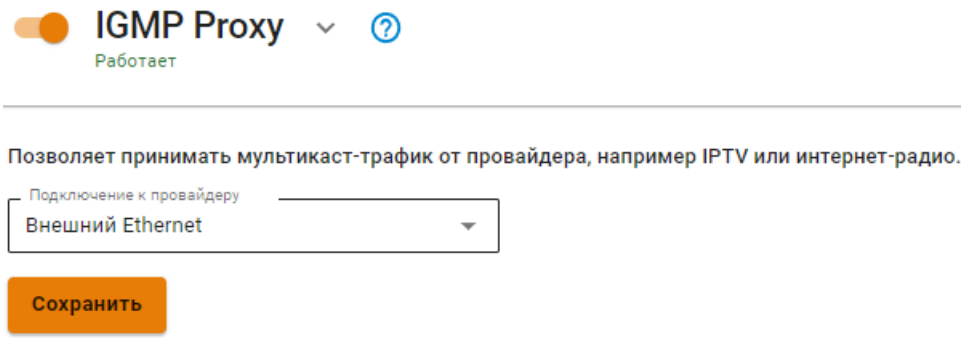
- *Пользователь 3*, находящийся в другой подсети, также решает подключиться к этой трансляции и генерирует IGMP-запрос (Join) на Ideco NGFW;
- *Ideco NGFW* получает этот запрос и дублирует *Пользователю 3* трафик, поступающий *Пользователю 4*;



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.

16.6.2 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.



16.7 Прокси

Подсказка: Название службы раздела **Прокси**: `ideco-proxy-backend`; `squid`.
Список служб для других разделов доступен по *ссылке*.

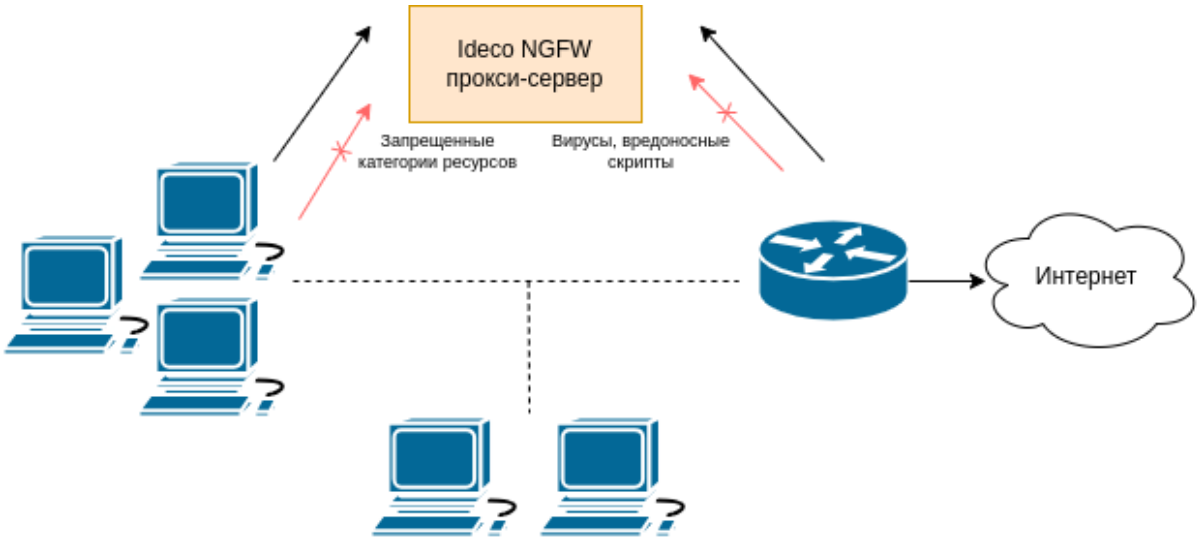
Прокси-сервер, помимо проксирования веб-трафика, используется для передачи трафика следующим сервисам:

- Антивирус для веб-трафика (Антивирус Касперского или ClamAV);
- 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*.



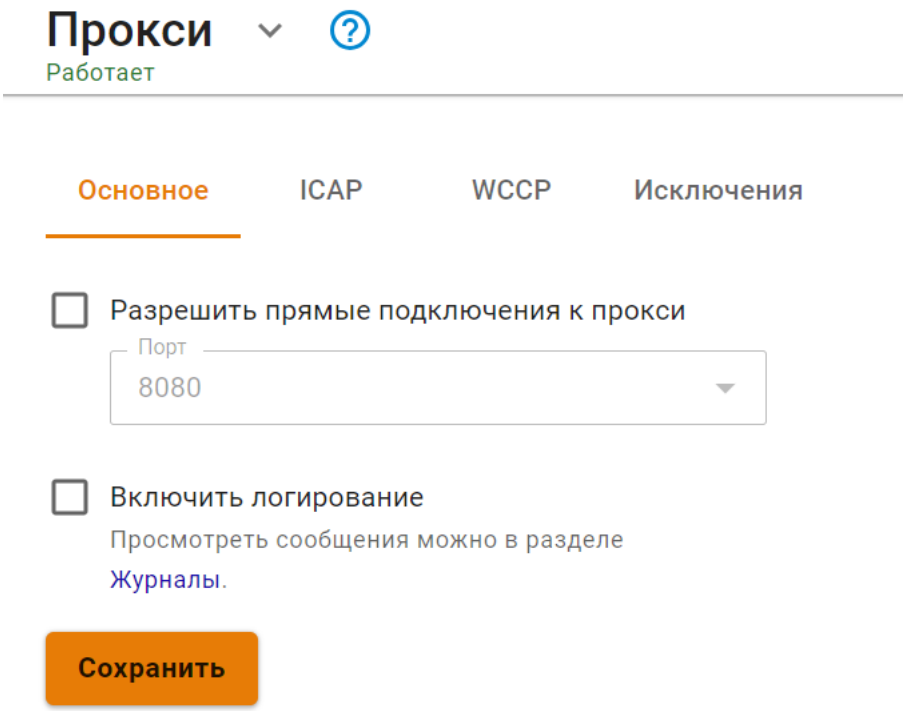
При использовании Ideco NGFW в качестве прокси-сервера с прямыми подключениями к прокси большинство функций будет работать с некоторыми особенностями:

- 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.

16.7.1 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*.

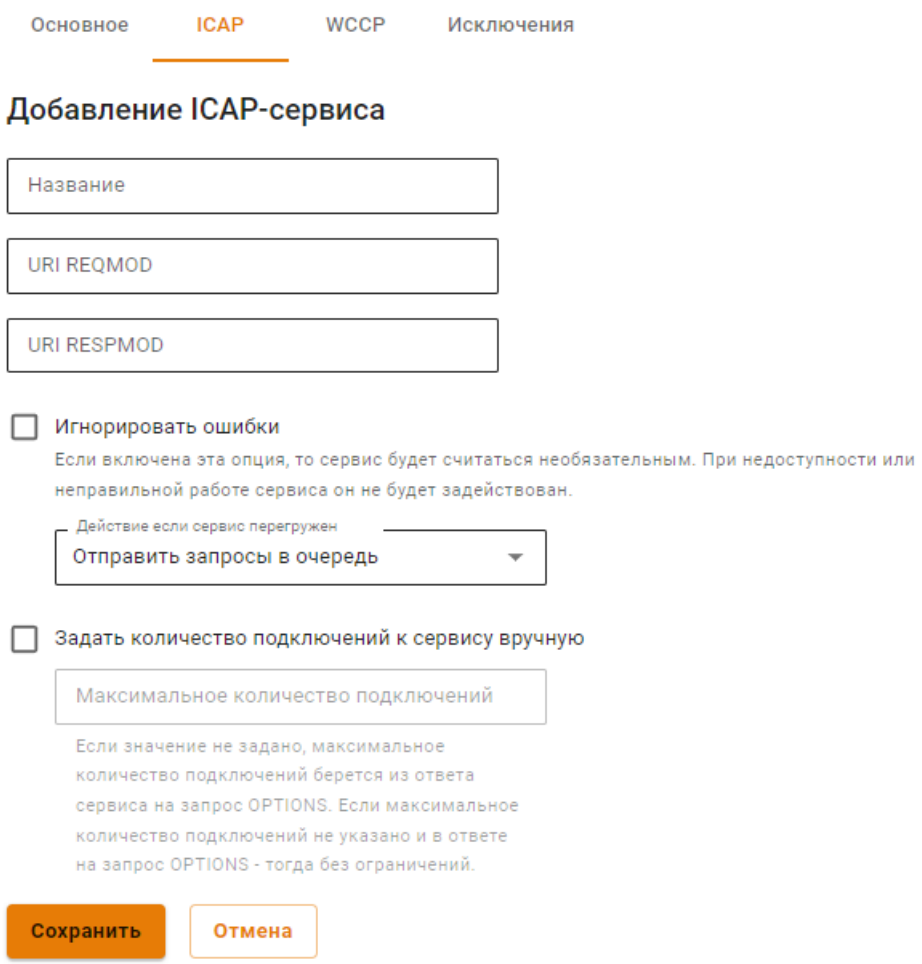
16.7.2 ICAP

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**.

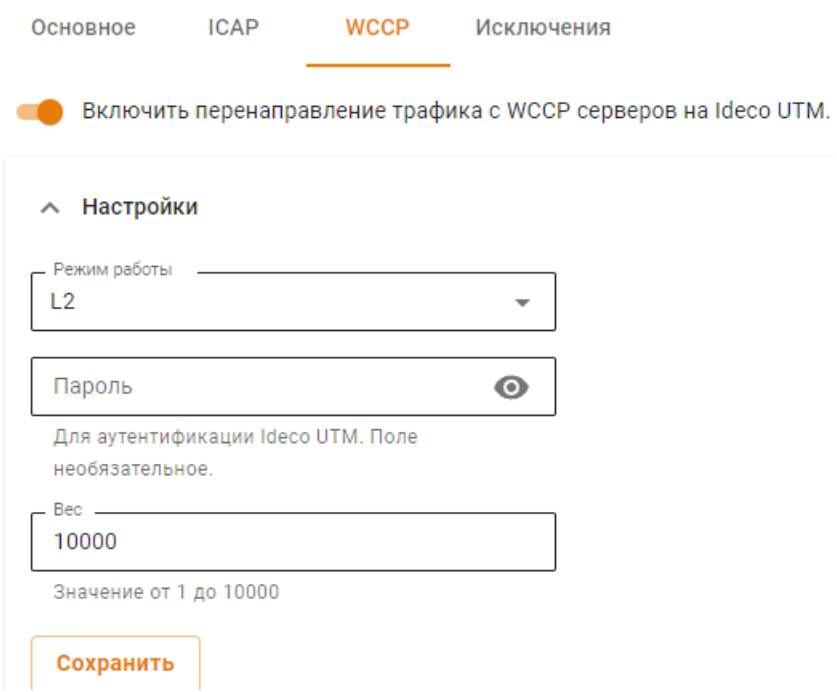
16.7.3 WCCP

Протокол WCCP используется для перенаправление веб-трафика на прокси-серверы.

Трафик, отличающийся от HTTP/HTTPS, не перенаправляется на Ideco NGFW. Веб-запросы обрабатываются роутером в соответствии с уровнем WCCP.

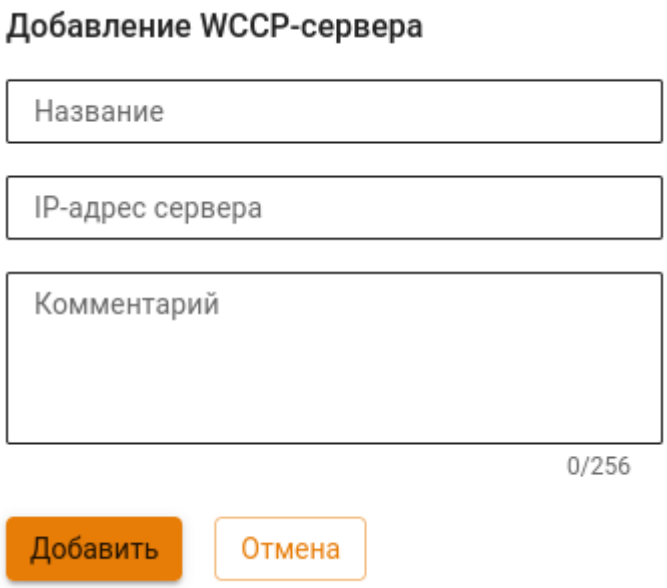
Для активации WCCP переведите опцию **Включить перенаправление трафика с WCCP-серверов на Ideco NGFW** в положение **Включен**. Ideco NGFW запустит процесс согласования параметров с WCCP-сервером.

В NGFW предусмотрено два режима работы WCCP - L2 и GRE. Для выбора режима раскройте блок **Настройки**.
Если на WCCP-сервере задан пароль, сохраните его в соответствующем поле:



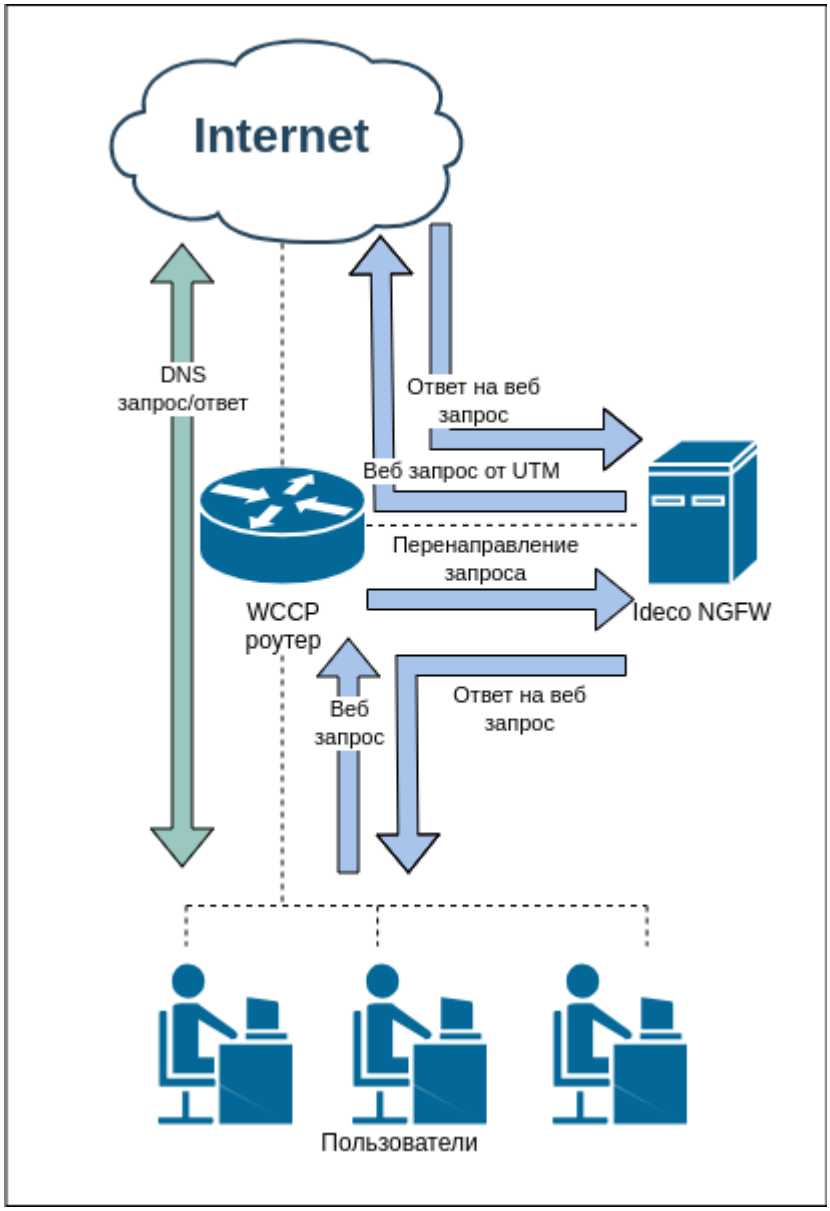
Если роутер использует несколько Ideco NGFW, настройте распределение трафика с помощью указания приоритета в поле **Вес**. Допустимые значения - от 1 до 10000.

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.



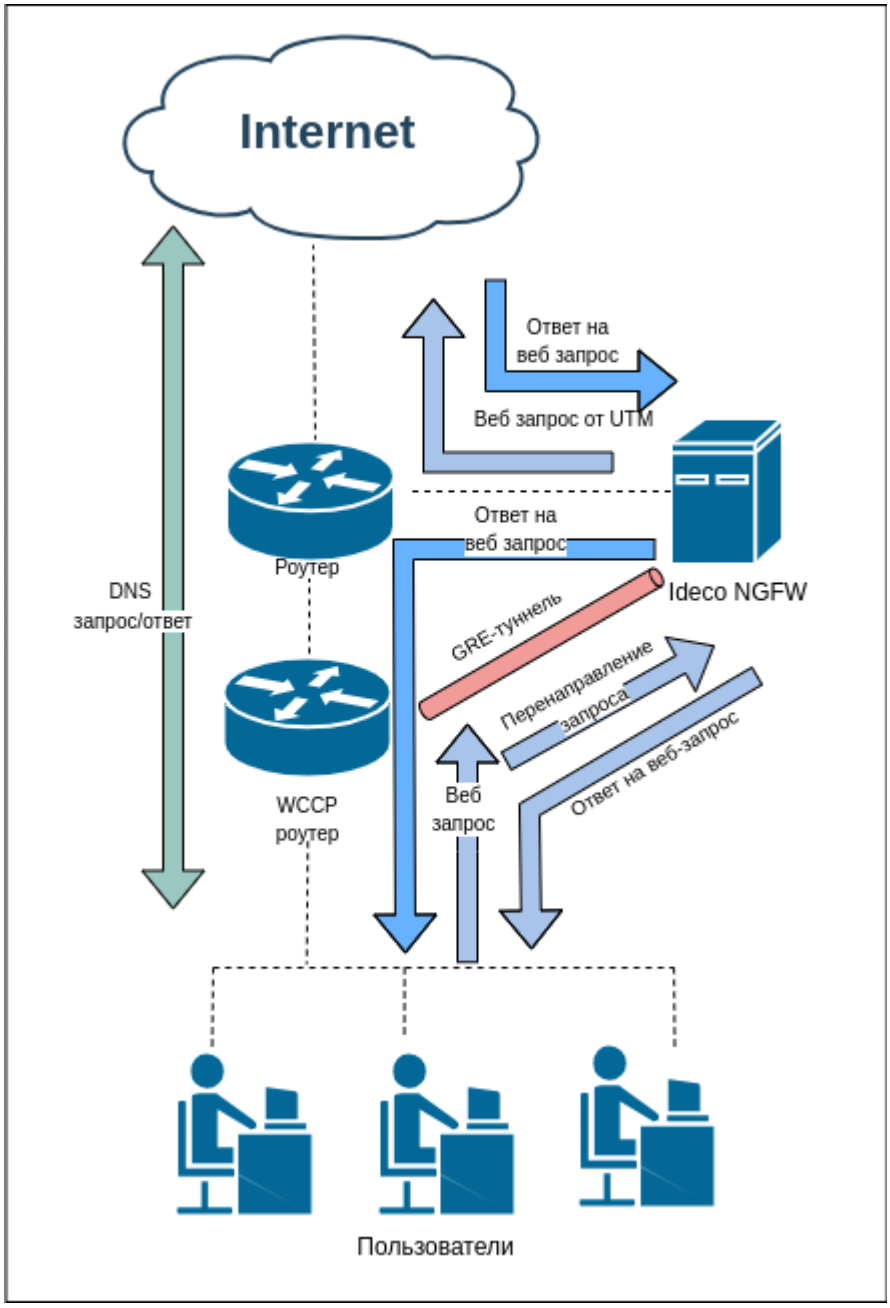
Последовательность обработки веб-запросов на уровне L2:

- 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 через WCCP-роутер, минуя Ideco NGFW и GRE-туннель.

16.7.4 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*.

16.7.5 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):

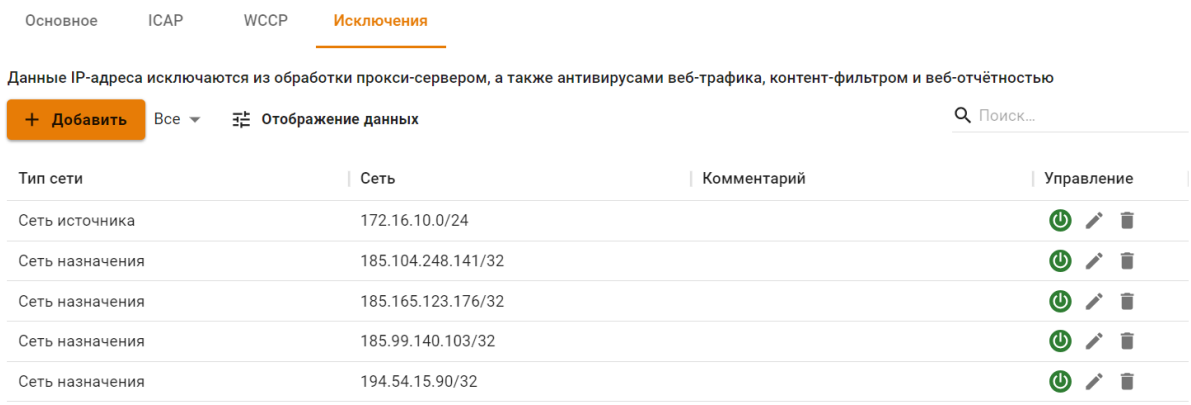
- **Сети источника:** указываются сети, трафик из которых исключается из обработки прокси-сервером;
- **Сети назначения:** указываются внешние сети или IP-адреса (как правило, адреса веб-сайтов или веб-сервисов), трафик до которых из всех локальных сетей NGFW исключается из обработки прокси-сервером.

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, соодержащие 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.

16.7.6 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;

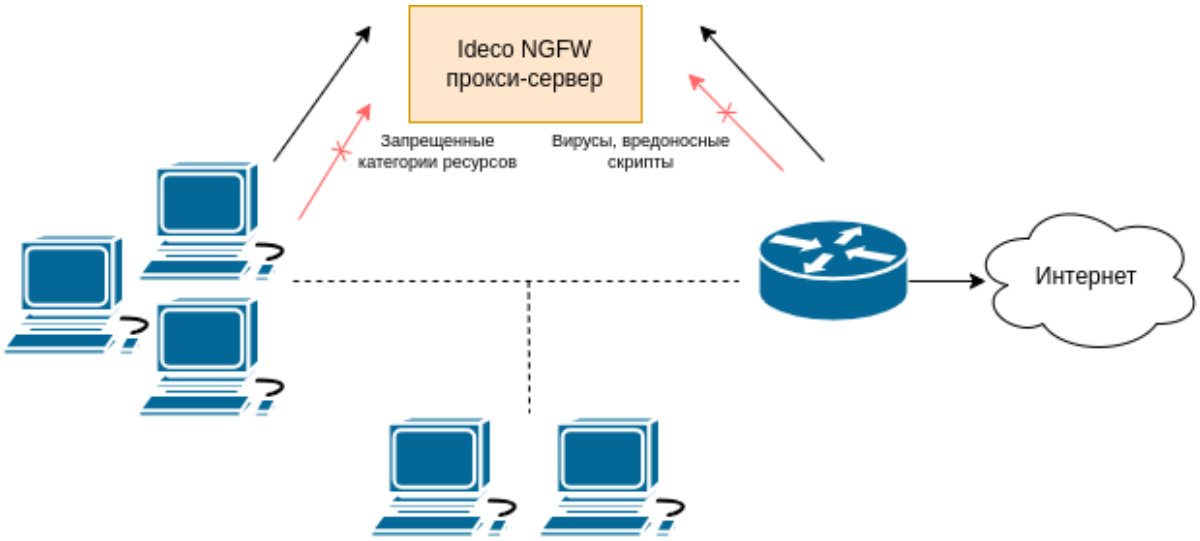
2. В настройках прокси на Ideco NGFW укажите порт для прямых подключений к прокси (возможен выбор портов из списка: 3128, 1080, 8000, 8080, 8888, 8081, 8088, 10080).

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);
- При *Single Sign-On* авторизации через Active Directory IP-адрес Ideco NGFW указан в качестве шлюза в настройках сетевого интерфейса клиентских машин.



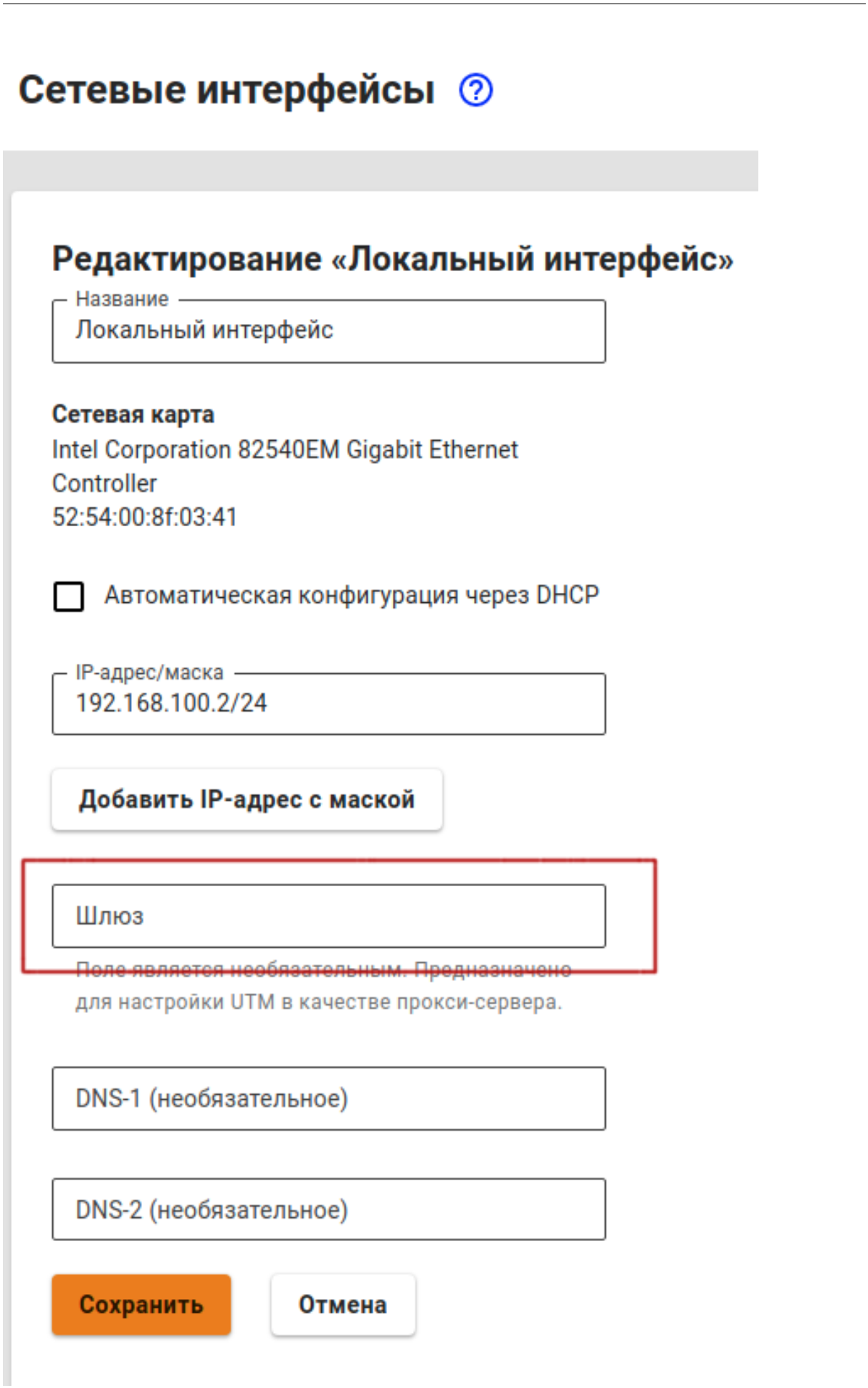
Если в настройках программы под ОС Windows или MacOS X нет возможности указать прокси-сервер, воспользуйтесь сторонним ПО для маршрутизации всего трафика рабочей станции на прокси-сервер. Такую возможность предоставляет программа **Proxifier**, которую можно настроить для прямых подключений к прокси, воспользовавшись *статьей*.

16.7.7 Настройка прокси с одним интерфейсом

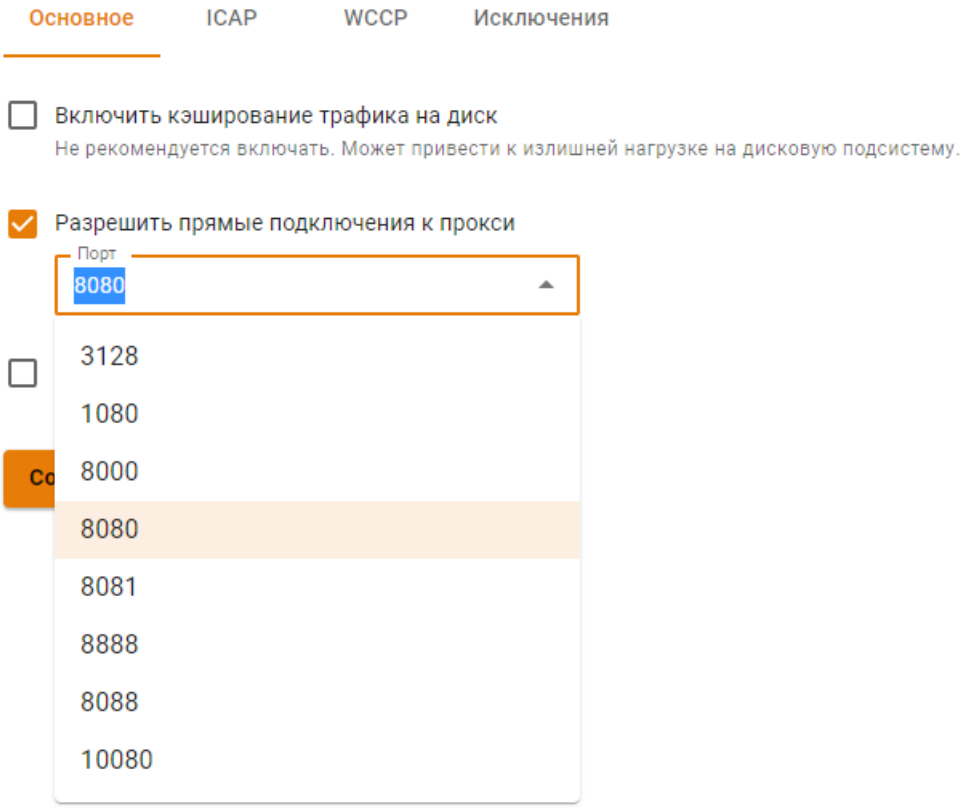
Настройка прокси с одним интерфейсом

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**:


Сетевые интерфейсы
Редактирование «Локальный интерфейс»
Название
Локальный интерфейс
Сетевая карта
Intel Corporation 82540EM Gigabit Ethernet Controller
52:54:00:8f:03:41
Автоматическая конфигурация через DHCP
IP-адрес/маска
192.168.100.2/24
Добавить IP-адрес с маской
Шлюз
Поле является необязательным. Предназначено для настройки UTM в качестве прокси-сервера.
DNS-1 (необязательное)
DNS-2 (необязательное)
Сохранить
Отмена

2. Разрешите прямые подключения к прокси-серверу в разделе **Сервисы -> Прокси**, выбрав нужный порт из списка:



16.8 Обратный прокси

Подсказка: Название службы раздела **Обратный прокси**: `ideco-reverse-backend`.
Список служб для других разделов доступен по *ссылке*.

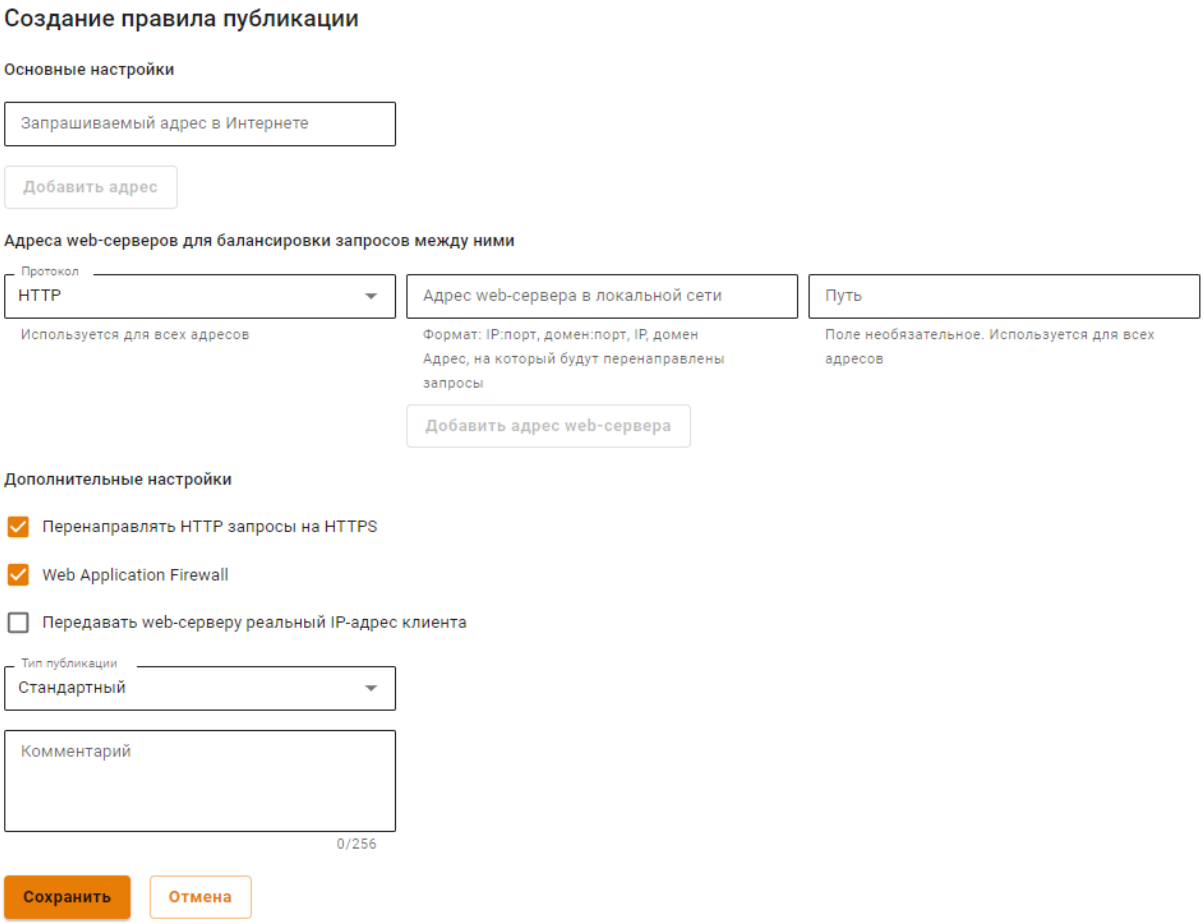
Технология обратного прокси позволяет проксировать веб-трафик из сети интернет в локальную сеть. Отличается от DNAT тем, что работает на более высоком уровне (прикладной протокол HTTP вместо сетевого протокола IP) и позволяет более гибко реализовать публикацию ресурсов.

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.

16.8.1 Создание и настройка правила

Настройка сертификатов для публикуемых ресурсов не требует их ручной загрузки. Сейчас 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 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 локальной сети**.

Чтобы перенаправление работало с доменов Ideco NGFW на адрес из строки **Адрес 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;
- Функция **Web Application Firewall** позволяет защитить опубликованные ресурсы с помощью Ideco NGFW от различного вида атак (включая атаки SQLi, XSS, DoS и другие);
- 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

На данный момент 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`.

16.8.2 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.

16.9 DNS

16.9.1 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** в 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.

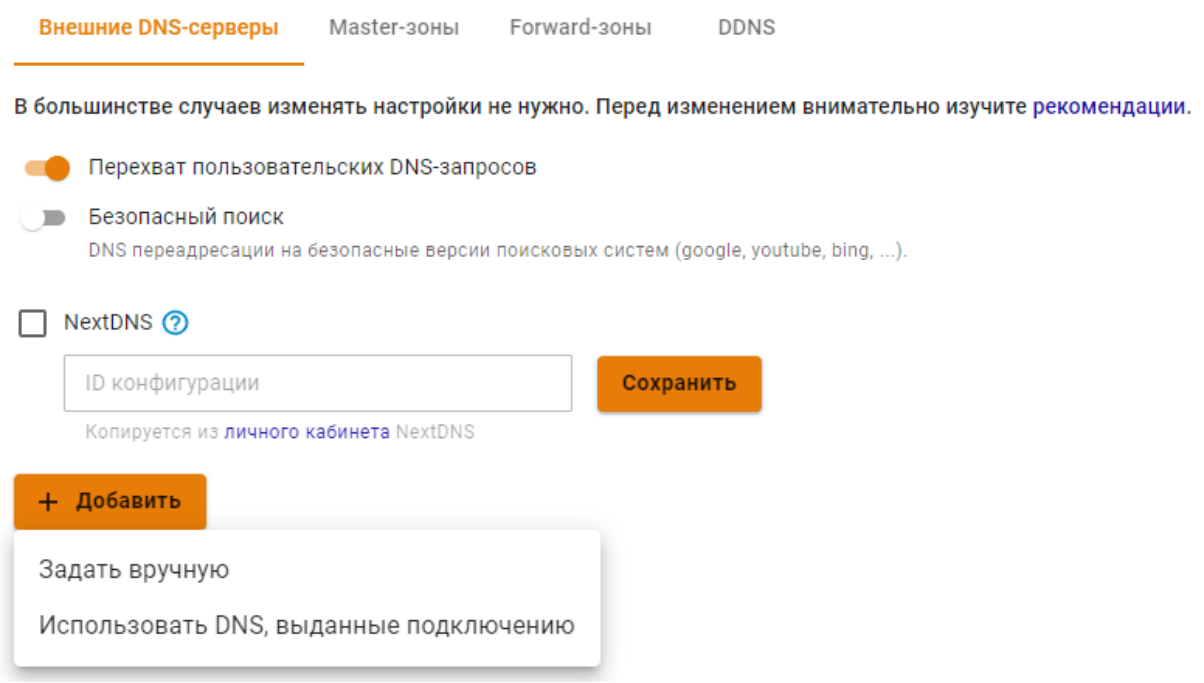
16.9.2 Внешние DNS-серверы

Для корректной работы резолвинга имен через Ideco NGFW указывать DNS-серверы в этом разделе не требуется.

Если DNS-сервера 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:

- указать DNS-серверы вручную (нажмите **Добавить -> Задать вручную** и укажите IP-адрес DNS-сервера);
- использовать опцию **Использовать DNS, выданные подключению**, указав нужное подключение;
- использовать NextDNS.



Рекомендации:

1. DNS-сервер, встроенный в Ideco NGFW, — кеширующий. 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-сервера 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-сервера занимающиеся фильтрацией, если это необходимо (SkyDNS или Яндекс-DNS).

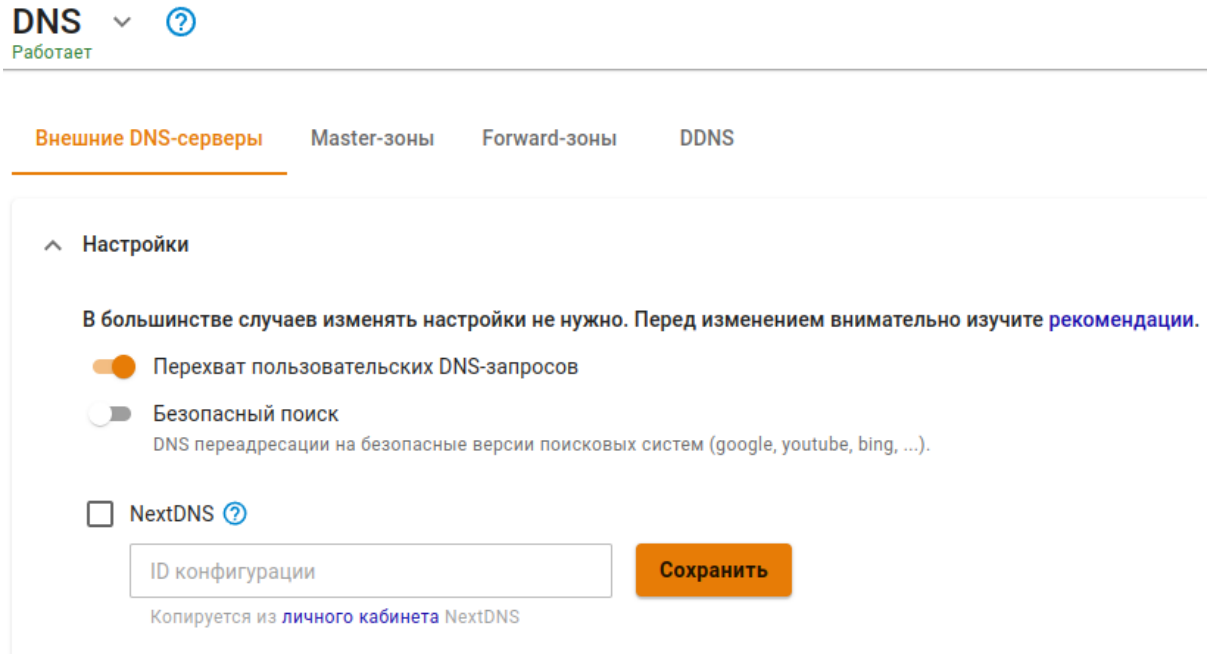
6. Если все DNS-сервера отключены или удалены, то DNS будет работать нормально (Ideco NGFW резолвит имена самостоятельно).

7. Если интернет-провайдер или вышестоящее устройство перехватывает DNS запросы, то использование стандартной конфигурации с корневыми серверами невозможно. Рекомендуем задать сервера вручную или использовать DNS-сервера, 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-сервера (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.

16.9.3 Master-зоны

Основное

Master-зоны позволят использовать NGFW как сервер имен внутри сетевой инфраструктуры для обращения к IP-адресам хостов в сети по доменным именам.

Подсказка: DNS-сервер в Ideco NGFW не доступен извне по соображениям безопасности. Для поддержки внешних DNS-зон, рекомендуем использовать сторонние DNS-хостинги.

Предупреждение: 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.

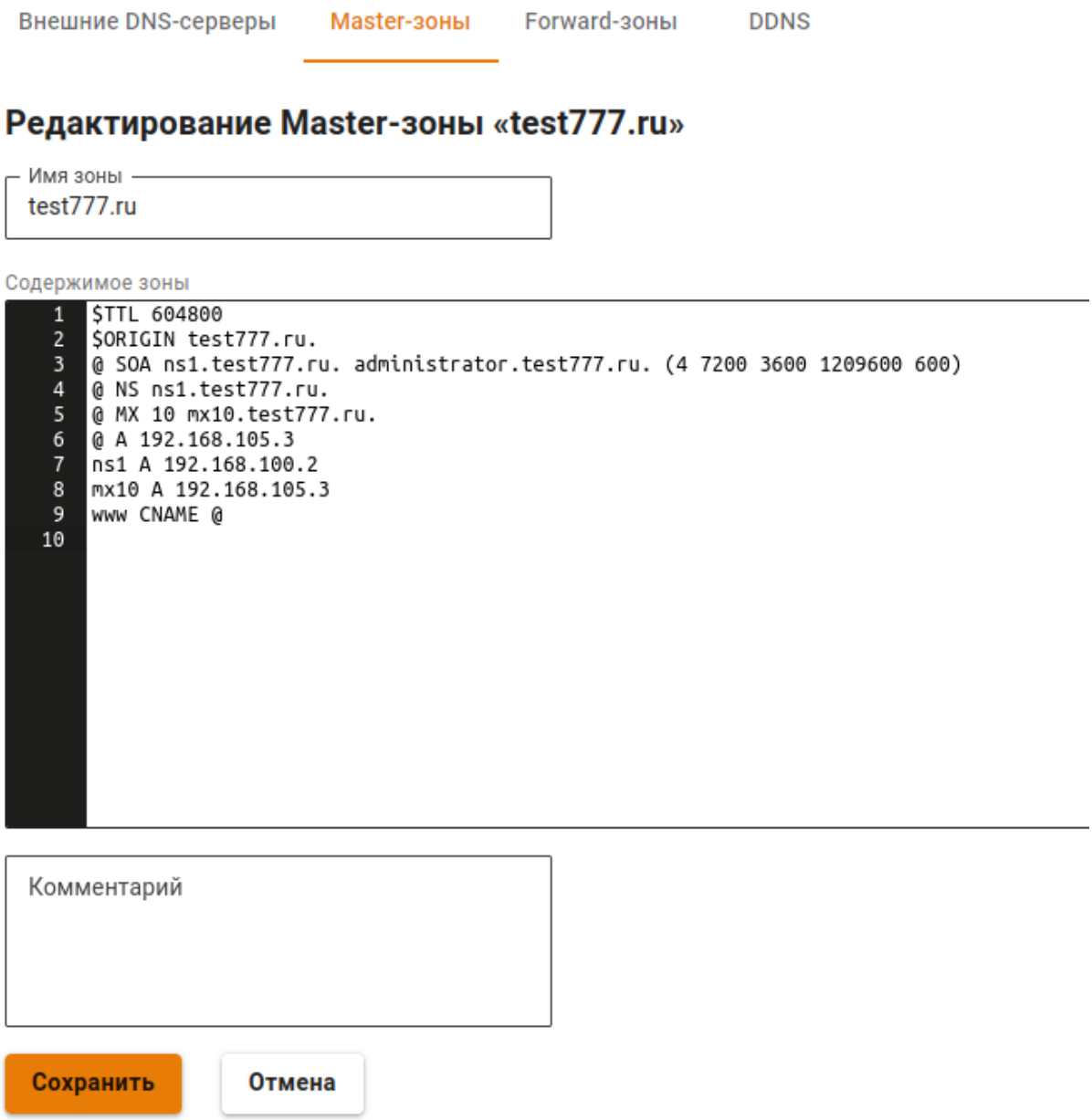
Описание параметров записи:

- **$TTL** - определяет время кеширования положительных ответов (ответ в виде найденного IP-адреса). Время задается в секундах или с помощью сокращений: m — минуты, h — часы, d — дни, w — недели;
- **$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 следующий 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 кэше 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 )
```

(continues on next page)

(продолжение с предыдущей страницы)

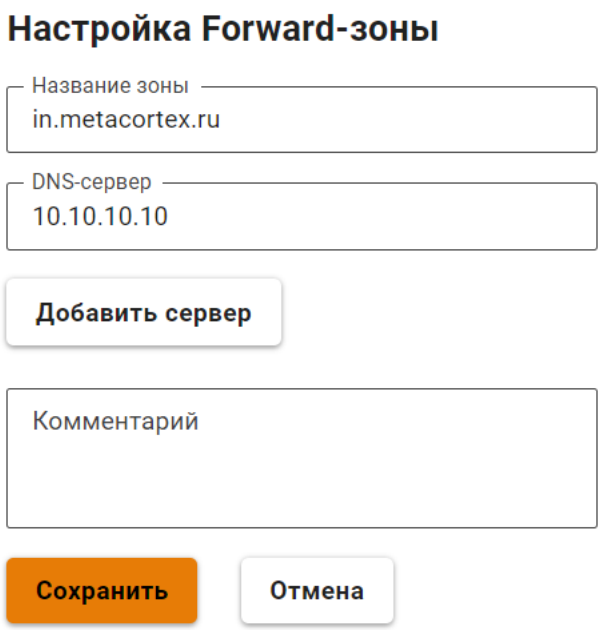
```
 @ NS my-dns-server.example.com.
my-dns-server A 1.2.3.4
```

16.9.4 Forward-зоны

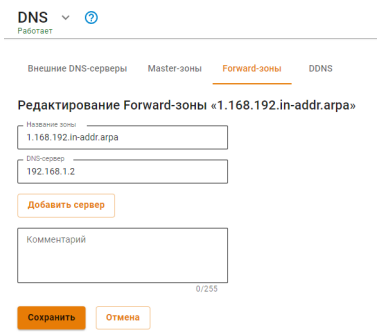
Основное

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.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**:



16.9.5 DDNS

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

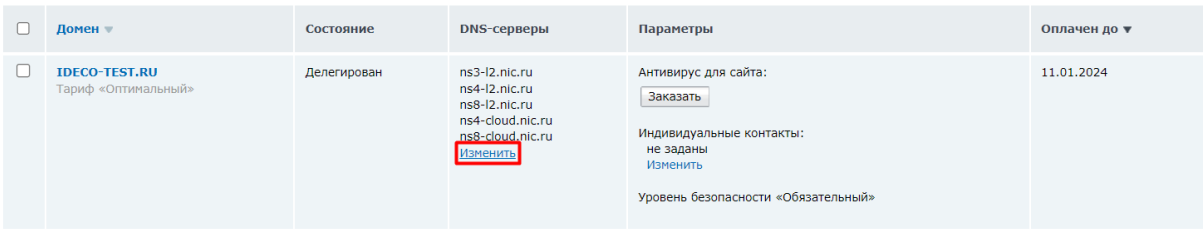
Подсказка: DDNS не будет работать:

- 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**:

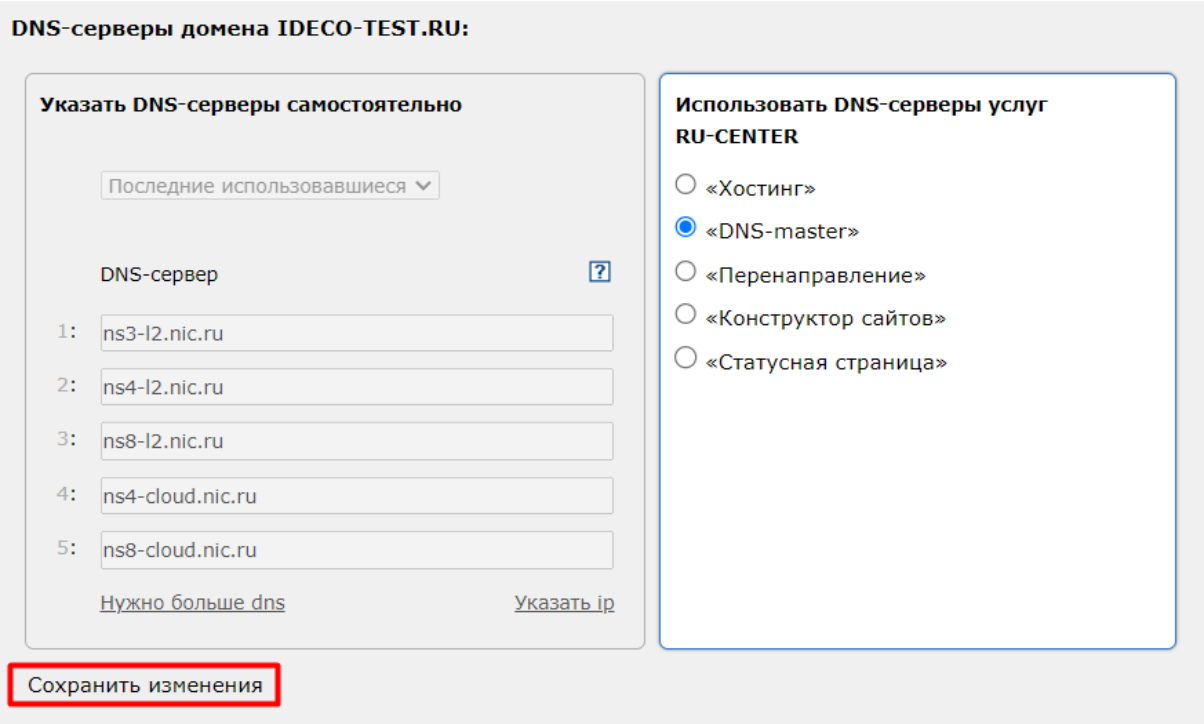
2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:



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.

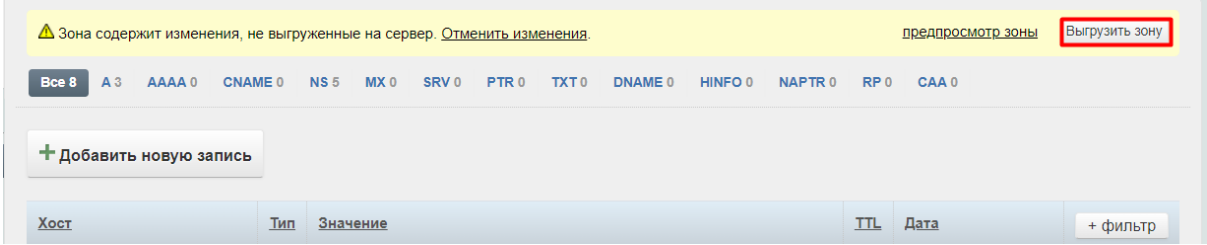
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

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.

16.9.6 NextDNS

NextDNS является облачным поставщиком услуг DNS в интернете. Используется для блокировки онлайн-трекеров, фильтрации баннеров и прочей рекламы, а также для ограничения доступа к нежелательным сайтам по доменным именам через черные и белые списки.

У NextDNS имеются различные тарифы, среди которых есть и бесплатный. Этот тариф подойдет для предприятий малого бизнеса или школ.

Предупреждение: Этот тариф имеет ограничение по количеству запросов в месяц, после превышения этого количества фильтрация со стороны NextDNS будет прекращена, но резолвинг имен продолжит работать.

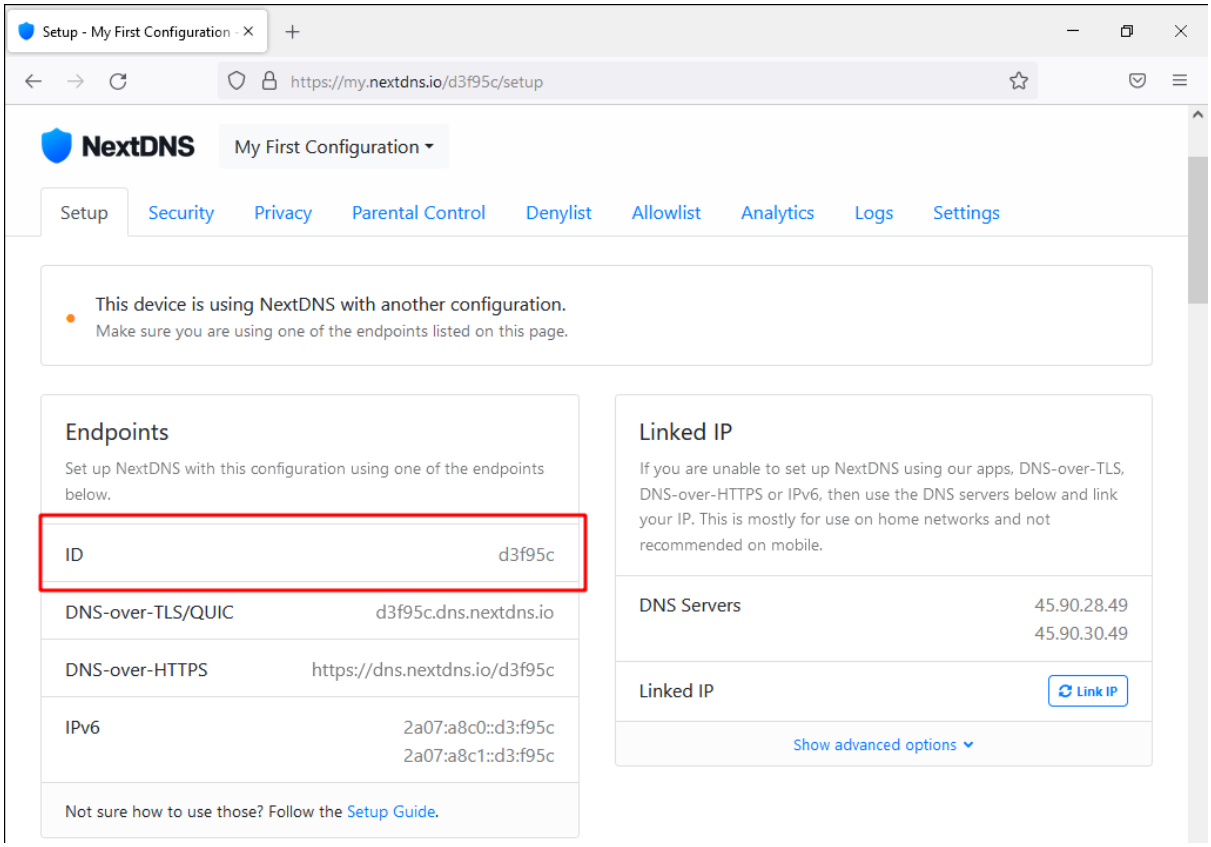
Подсказка: Эта интеграция была внедрена в Ideco NGFW для предоставления возможности использовать сервис NextDNS всем пользователям, находящимся в локальных сетях Ideco NGFW.

Настройка NextDNS на Ideco NGFW

Подсказка: Для использования сервиса NextDNS необходимо предварительно в нем зарегистрироваться. Без регистрации можно использовать пробный аккаунт, действующий в течение 7 дней, с последующим удалением.

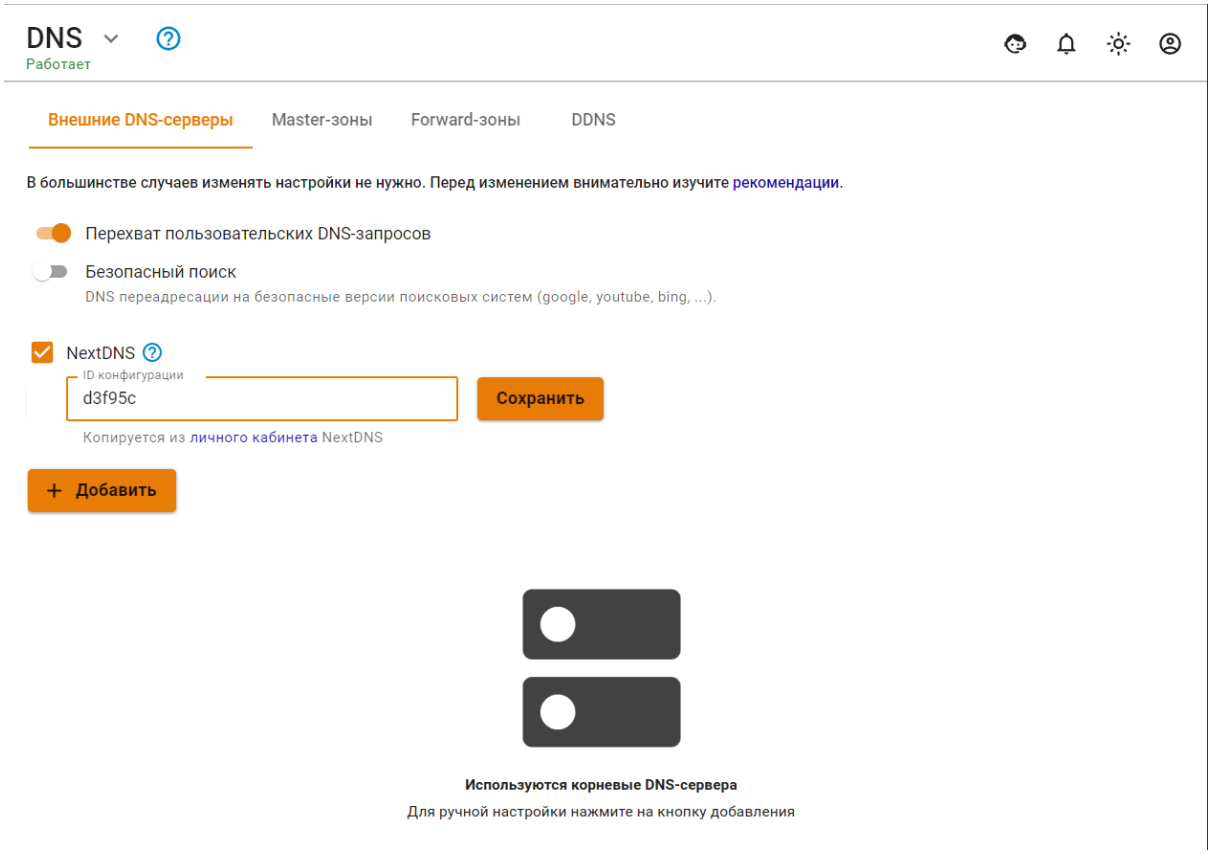
Для интеграции Ideco NGFW с NextDNS необходимо:

1. Зайти на сайт https://my.nextdns.io/`nextDNS-id`/setup



2. Перейти в раздел **Сервисы -> DNS**.

3. Нажать на флаг с **NextDNS** и вставить в поле ID из личного кабинета, как показано на скриншоте:



4. Нажать на кнопку **Сохранить**.

После сохранения настроек все имеющиеся в вашем личном кабинете NextDNS правила фильтрации начнут действовать на исходящие DNS-запросы от пользователей
из локальных сетей Ideco NGFW.

Подсказка: При возникновении проблем с интеграцией NextDNS обратитесь
в *техническую поддержку* Ideco NGFW.

При возникновении трудностей с настройкой или проблем с работой
самого NextDNS обратитесь в техническую поддержку NextDNS.

16.10 DHCP-сервер

Подсказка: Название службы раздела **DHCP**: `ideco-dnsmasq`.
Список служб для других разделов доступен по *ссылке*.

16.10.1 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.

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**.

16.10.2 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:

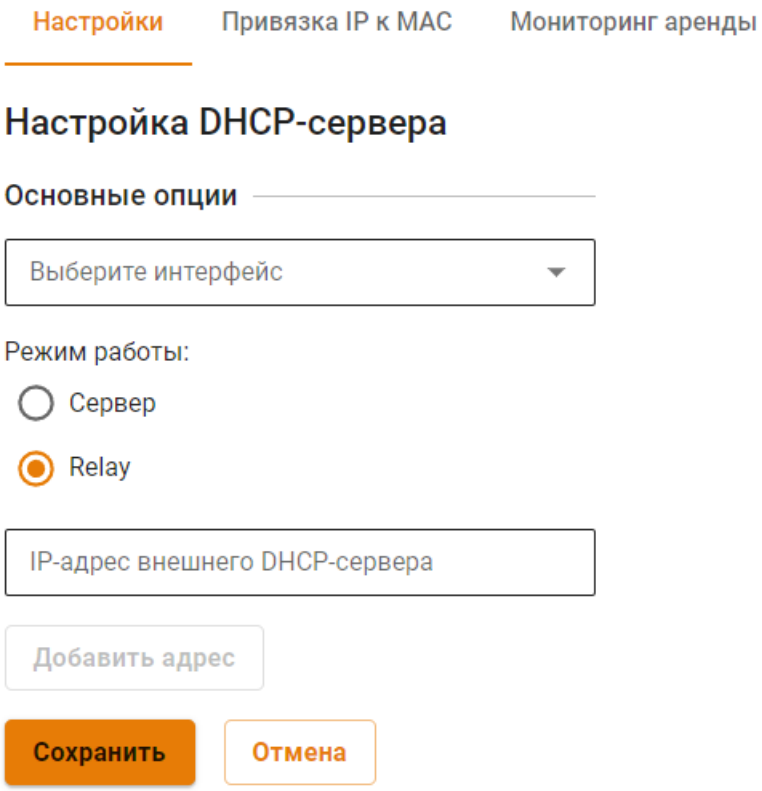
- **Основные опции** - задаются диапазоны IP-адресов и DNS-сервера;

- **Дополнительные опции** - статические маршруты, адреса WINS-серверов, время аренды и PXE Boot;
- **Опции dnsmasq** - предназначены для ручного задания опций DHCP, передаваемых сервером клиенту при получении сетевых реквизитов от DHCP-сервера.

Основные опции

Подсказка: Если не задано значение в поле DNS-1 или DNS-2, то DNS-сервером будет являться Ideco NGFW для всех сетевых устройств локальной сети.

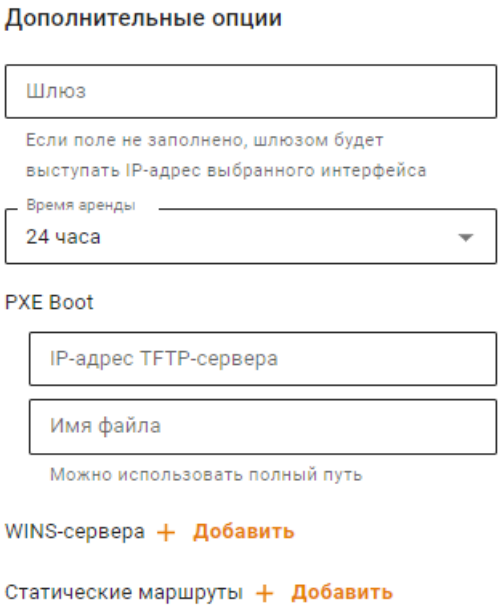
Выберите режим работы **Relay**, если IP-адреса будет выдавать внешний DHCP-сервер:



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.



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 -> Журнал событий**;
- 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"
```

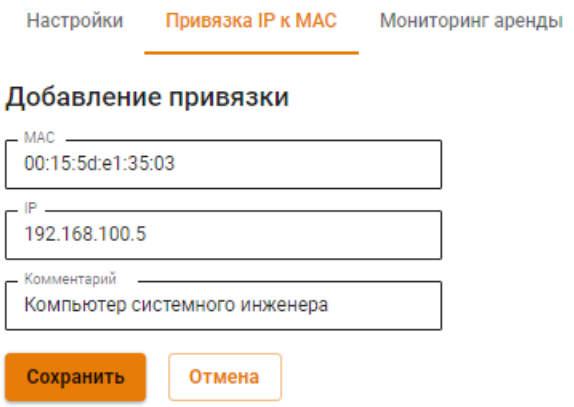
После сохранения настроек IP-телефония Avaya будет получать от DHCP-сервера расширенный список опций.

16.10.3 Привязка IP к MAC

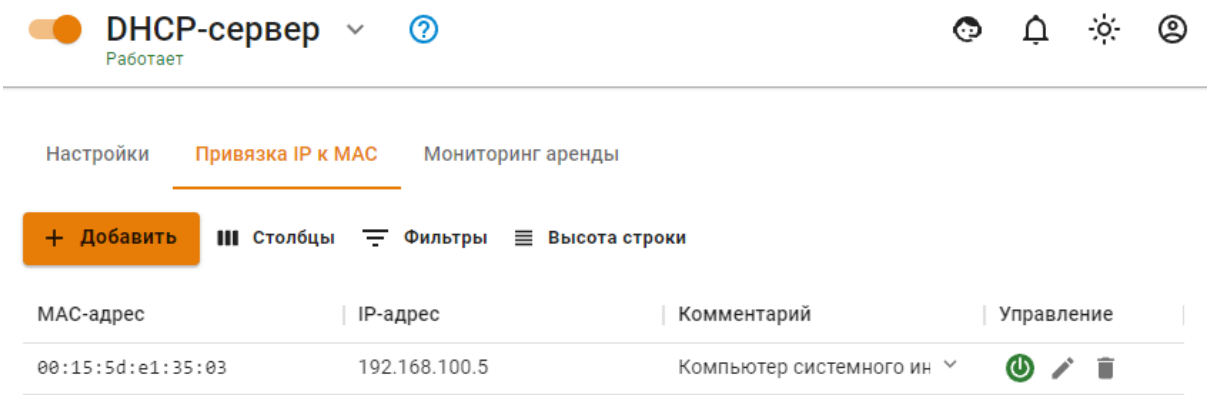
Для настройки в DHCP-сервере привязки IP-адреса к MAC-адресу необходимо:

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`.

```
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>
```

Подсказка: Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW.

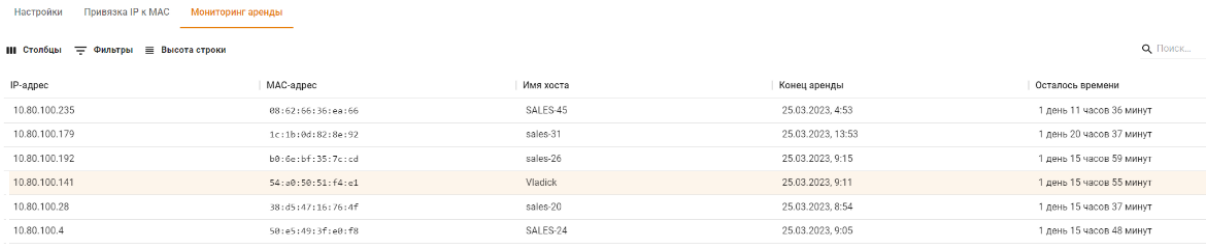
Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (`01-02-03-04-05-06`). В настройках Ideco NGFW октеты MAC-адреса разделяются только двоеточиями (`01:02:03:04:05:06`).

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-cemu*.

16.10.4 Мониторинг аренды

Содержит информацию об аренде IP-адресов для устройств.



Для привязки IP к MAC нажмите на кнопку  в столбце **Управление**.

16.11 NTP-сервер

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.

16.11.1 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.

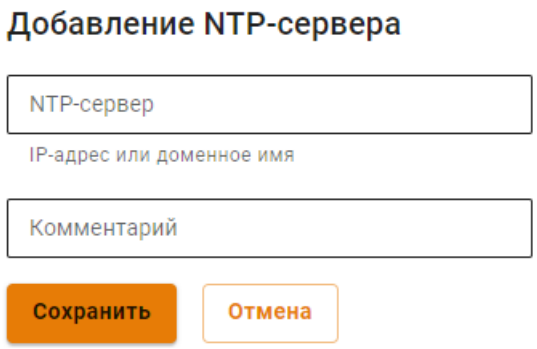
16.11.2 Настройка Ideco NGFW

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:



16.12 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: Выбор внешних интерфейсов для IPsec-подключений зависит от приоритета 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.

Туннели создаются на всех интерфейсах со шлюзом по умолчанию.

16.12.1 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.

16.12.2 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.

16.12.3 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.

16.12.4 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:

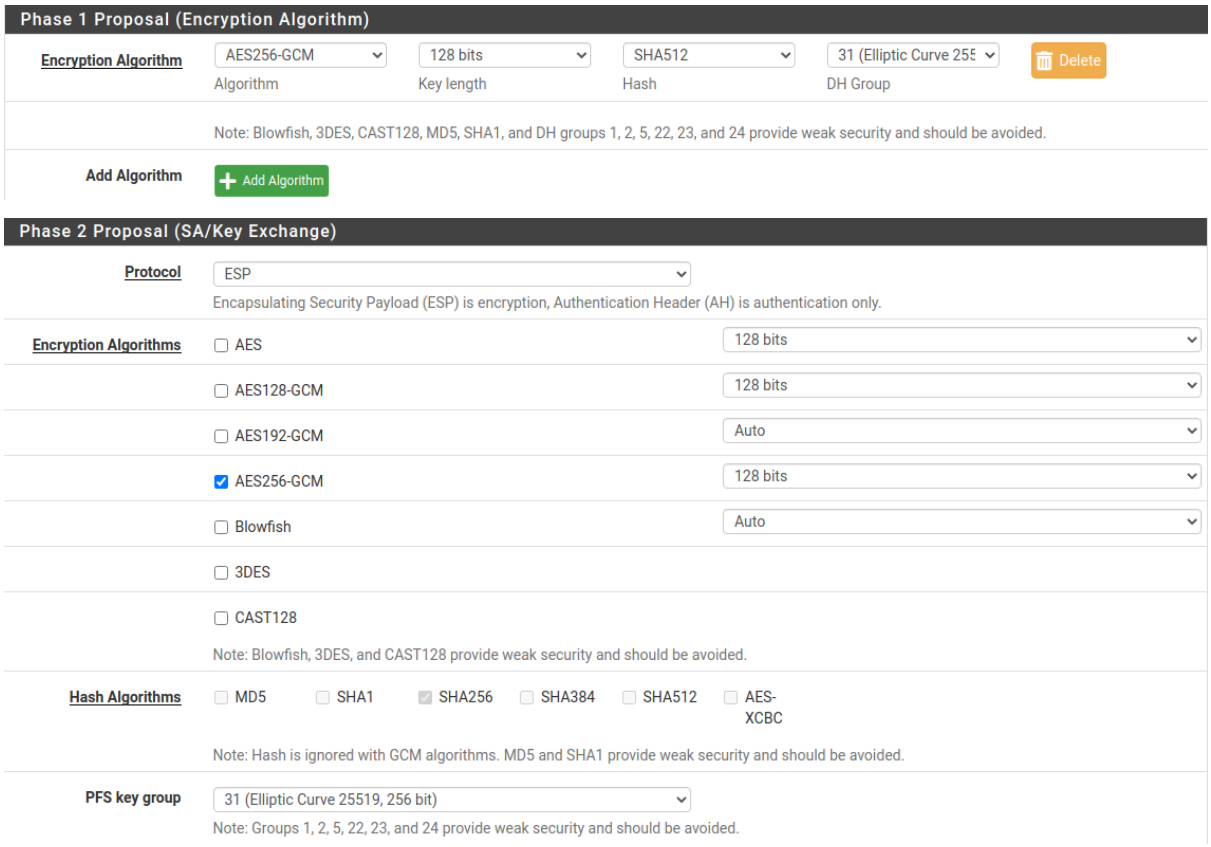
- **Phase 1 (IKE):**
  - encryption (шифрование):
    - **AES256-GCM**;
    - **AES256**.
  - integrity (hash, целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы;
    - для **AES256** - по приоритету: **SHA512, SHA256**.
  - prf (функция генерации 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**.
  - integrity (целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы;
    - для **AES-256** - по приоритету: **SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman, PFS). **ВНИМАНИЕ! Если не указать, подключаться будет, но не сработает rekey через некоторое время**:
    - **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\SHA512\PRF-HMAC-SHA512\ECP384;
    - AES256\SHA256\PRF-HMAC-SHA256\MODP2048.
- **Phase 2 (ESP)** (нужна одна из строк)**:**
    - AES256-GCM\ECP384;
    - AES256\SHA256\MODP2048.

Пример настройки подключения pfSense к Ideco NGFW по IPsec:

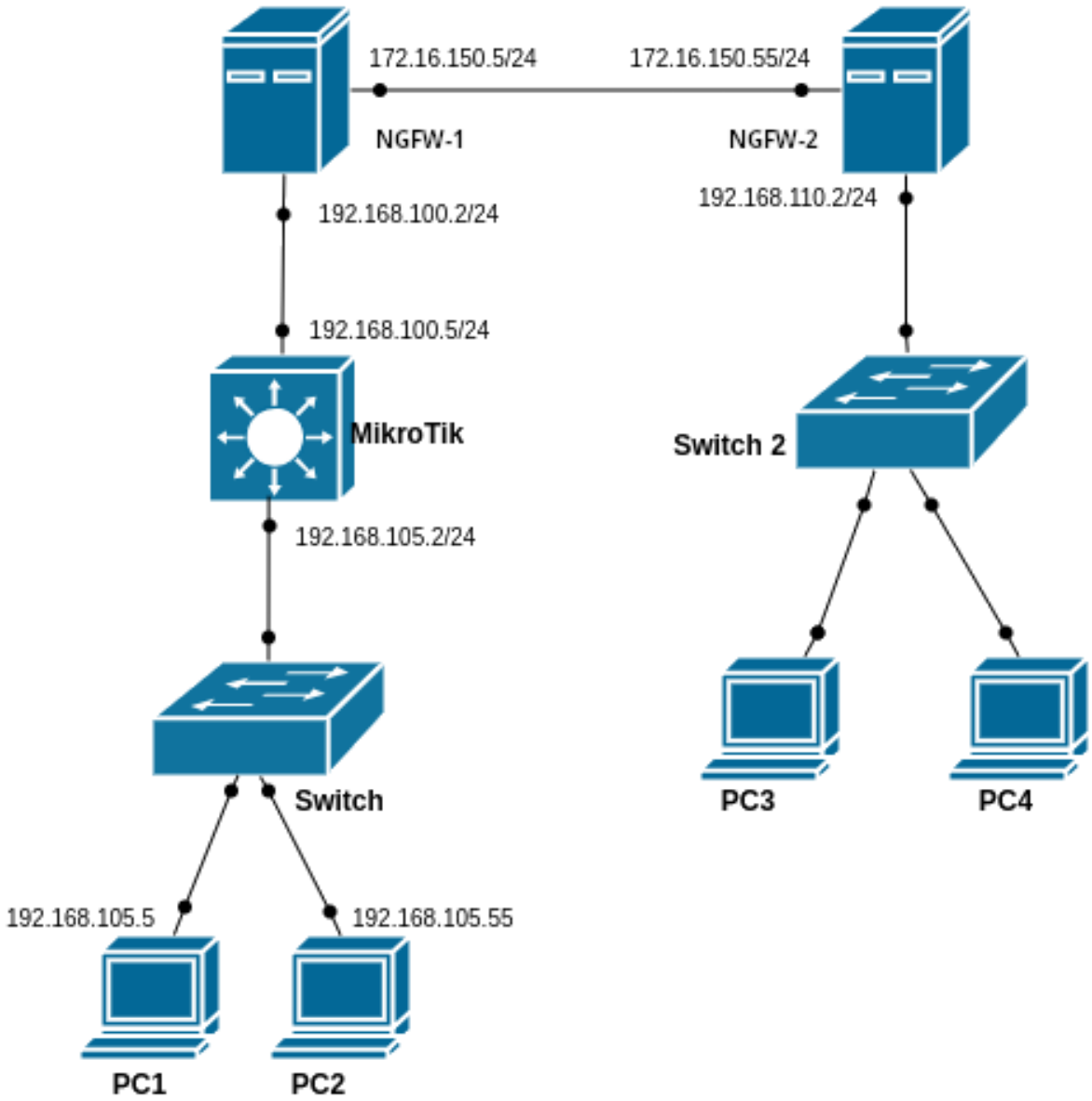


16.12.5 Изменение настроек созданных IPsec-подключений

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**.

16.12.6 Подключение по IPsec между двумя Ideco NGFW



Предупреждение:

- Перед тем как создать подключение между двумя NGFW, убедитесь, что в каждой из подключаемых сторон **правильно настроена временная зона**. Без этого установить подключение невоз-

можно;

- Убедитесь, что 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);
- Перед настройкой IPsec нужно учесть, что для его работы все IP-подсети, участвующие в соединениях не должны пересекаться и, тем более, не должны совпадать;
- Сети локальных интерфейсов, до которых требуется дать доступ, должны быть заданы статически;
- Перед настройкой соединения нужно убедиться в том, что один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. Входящее подключение должно настраиваться на сервере с белым IP-адресом.
- При замене/перевыпуске корневого сертификата в разделе *Сертификаты*, IPsec-подключения перестанут работать и их необходимо будет пересоздать.
- Сети для VPN-подключений у двух NGFW не должны пересекаться.

Подсказка: Для доступа к локальным сетям **NGFW-1** с **NGFW-2** при подключении по VPN к **NGFW-2** выполните действия:

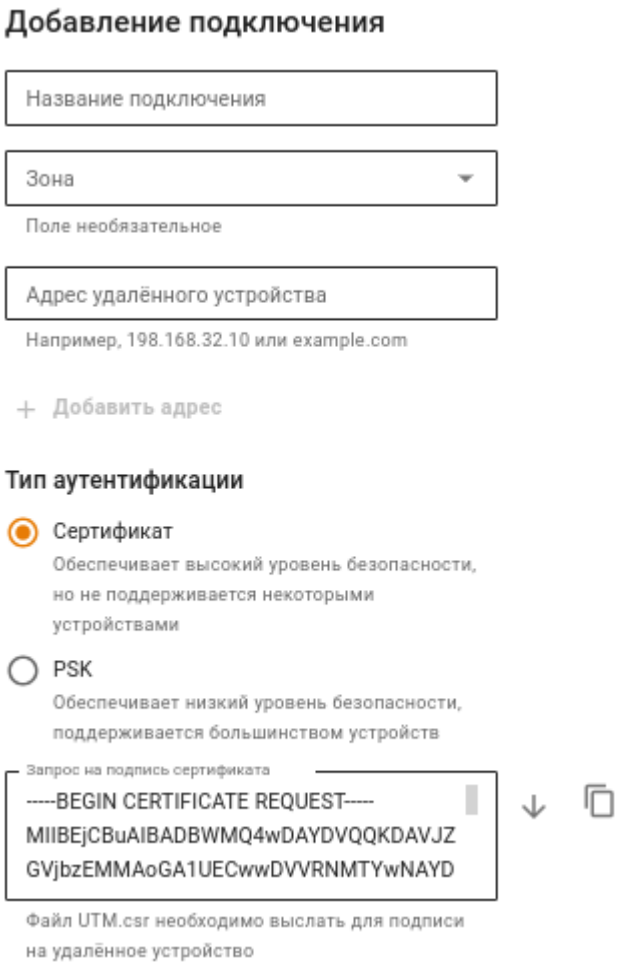
1. Перейдите к редактированию настроенного IPsec подключения на **NGFW-2**.
2. Укажите в поле **Домашние локальные сети** сеть, используемую для VPN, в **NGFW-2**.

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**:

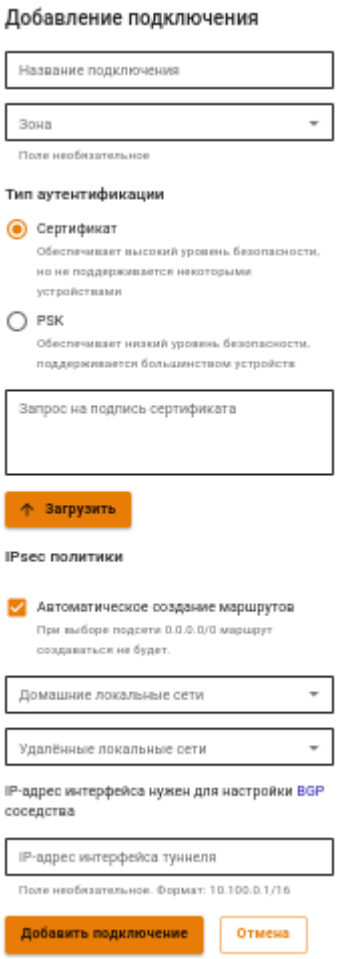
1. Перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения** и нажмите **Добавить**.
2. Выберите **Туннельный** режим работы.
3. Заполните поля:
   - **Название подключения** - максимальное количество символов - 42;
   - **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым;
   - **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес.
   - **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**.
4. Перед завершением настройки исходящего подключения настройте входящее подключение на другом NGFW. **Не закрывайте форму создания исходящего подключения**. 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;
   - **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. Добавьте **Домашние локальные сети**, к которым должен быть доступ с другого NGFW.
4. Добавьте **Удаленные локальные сети**, к которым должен быть доступ с текущего NGFW.
5. Укажите IP-адрес интерфейса туннеля в одноименное поле при настройке BGP соседства для динамической маршрутизации.
6. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.



Предупреждение: Для доступа к удаленным локальным сетям NGFW:

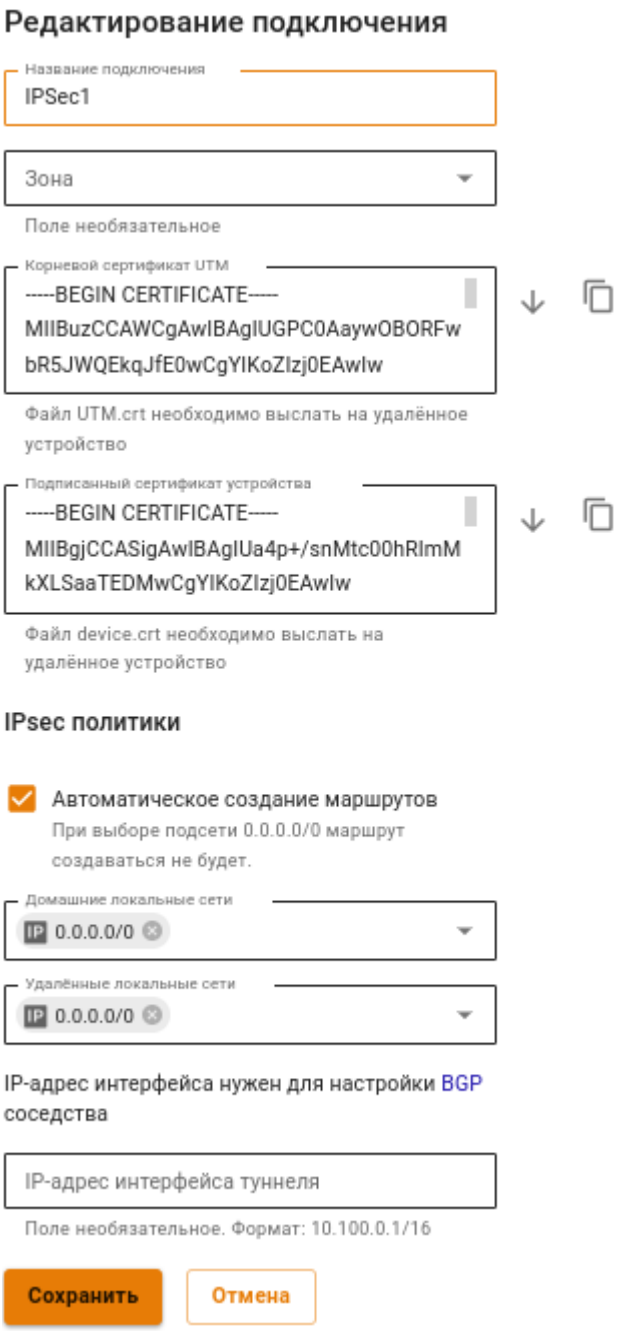
- Укажите сеть в поле **Удаленные локальные сети**,
- Добавьте статический маршрут до этой сети.

Для автоматического создания статического маршрута до удаленных локальных сетей NGFW активируйте опцию **Автоматическое создание маршрутов**.

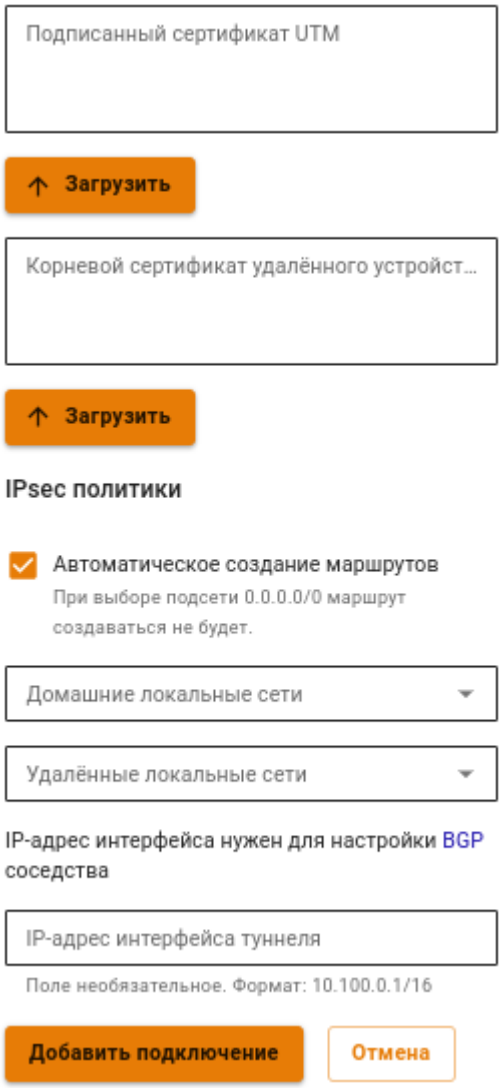
Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата 0.0.0.0/0, то для доступа к удаленному NGFW нужно указать его IP-адрес в поле **IP-адрес интерфейса туннеля**.

Шаг 3. Настройка исходящего подключения

1. В **NGFW-2** перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите по ранее созданному входящему подключению.
2. В зависимости от типа аутентификации выберите пункт:
   - **PSK** - перейдите к настройке исходящего подключения на **NGFW-1**.
   - **Сертификат** - скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения**.
4. В зависимости от типа аутентификации выберите пункт:
   - **Сертификат** - заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** ранее скопированным значением при редактировании входящего подключения.
   - **PSK** - перейдите к добавлению домашних и удаленных сетей.



5. Добавьте **Домашние локальные сети**, к которым должен быть доступ с другого NGFW.
6. Добавьте **Удаленные локальные сети**, к которым должен быть доступ с текущего NGFW.
7. Укажите IP-адрес интерфейса туннеля в одноименное поле при настройке BGP соседства для динамической маршрутизации.
8. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Предупреждение: Для доступа к удаленным локальным сетям NGFW при туннельном режиме работы:

- 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 для доступа к удаленному NGFW нужно указать IP-адрес удаленного NGFW в поле **IP-адрес интерфейса туннеля**.

Подсказка: Если соединение по IPsec не устанавливается, воспользуйтесь *статьей*.

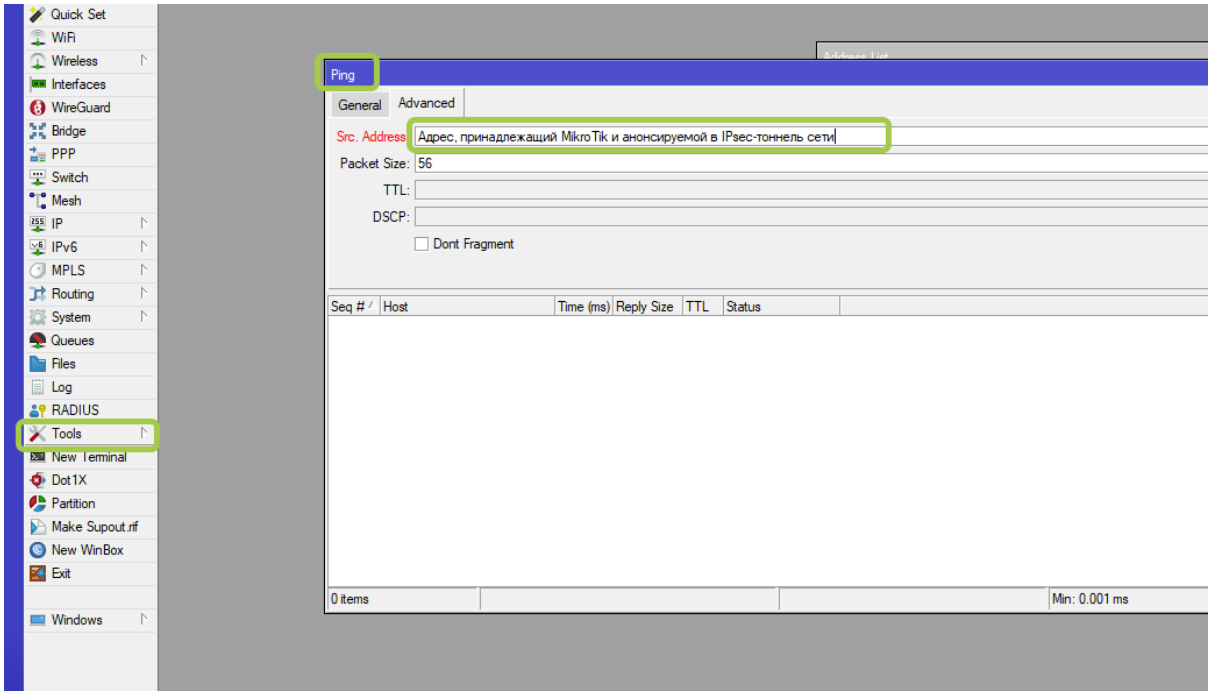
Подключение Ideco NGFW и Mikrotik

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).

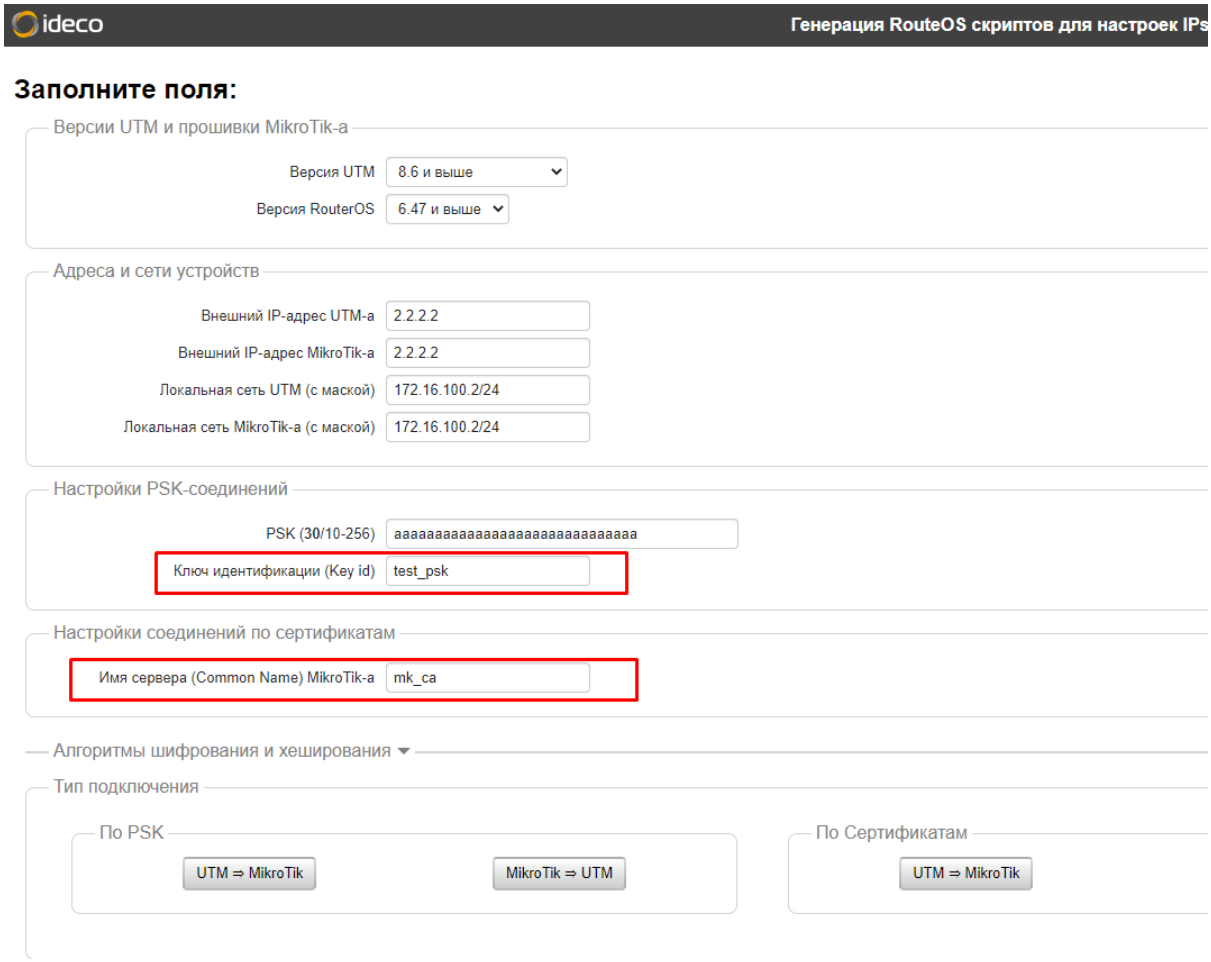
Исходящие IPsec-подключения по сертификатам к MikroTik ниже версии 6.45 не работают из-за невозможности использования современных криптоалгоритмов.

Подсказка: Для проверки доступности анонсируемых сетей Ideco NGFW с MikroTik указывайте IP-адрес источника:



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:



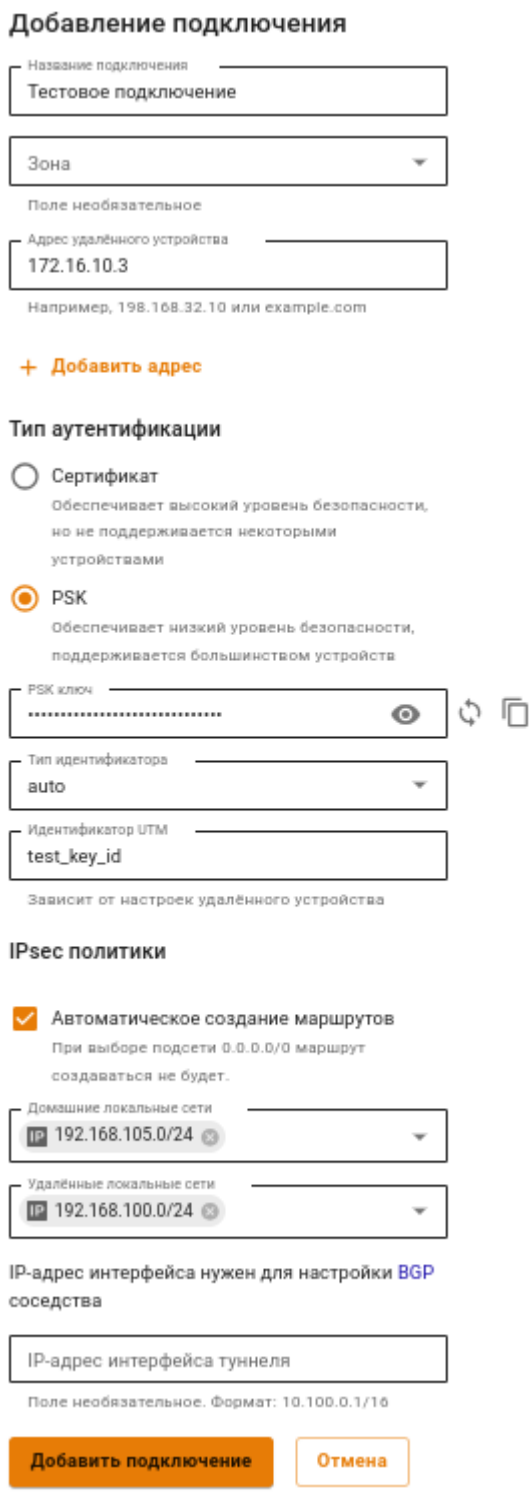
Исходящее подключение

Тип аутентификации PSK

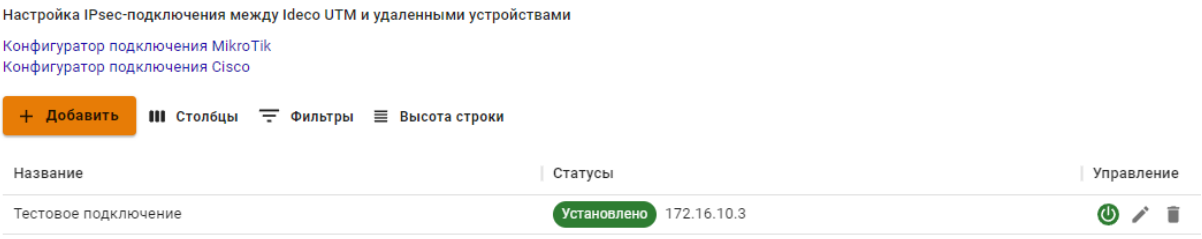
Настройка Ideco NGFW:

1. Откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**, нажмите **Добавить** и заполните поля:

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik;
- **PSK** - будет сгенерирован случайный PSK-ключ. Он потребуется для настройки подключения в MikroTik;
- **Идентификатор UTM** - введенный ключ будет использоваться для идентификации исходящего подключения;
- **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;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP.



2. После заполнения всех полей нажмите **Добавить подключение**. В списке подключений появится созданное подключение:



Настройка 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

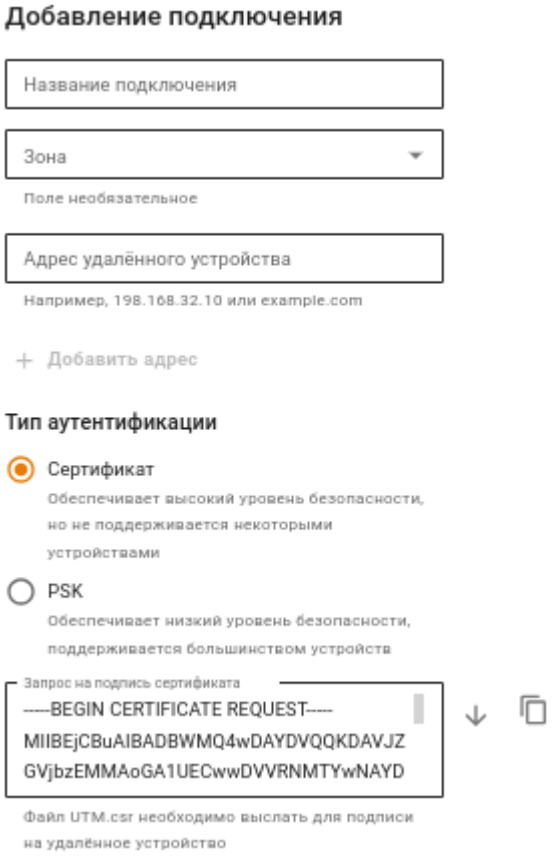
Подключение по сертификатам является более безопасным по сравнению с PSK.

Настройка Ideco NGFW:

Сгенерируйте запрос на подпись сертификата:

1. В Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**, нажмите **Добавить** и заполните поля:

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Адрес удаленного устройства** - укажите внешний IP-адрес MikroTik;
- **Запрос на подпись сертификата** - будет сгенерирован **запрос, который необходимо выслать для подписи на MikroTik**.



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 MikroTik:

На этом этапе следует настроить MikroTik, чтобы продолжить настройку NGFW.

Файл **NGFW.csr**, полученный из Ideco NGFW, необходимо загрузить в файловое хранилище MikroTik:

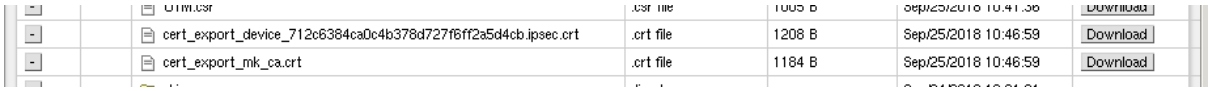
1. Откройте раздел **File**.
2. Нажмите кнопку **Browse**.
3. Выберите файл и загрузите его.

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.

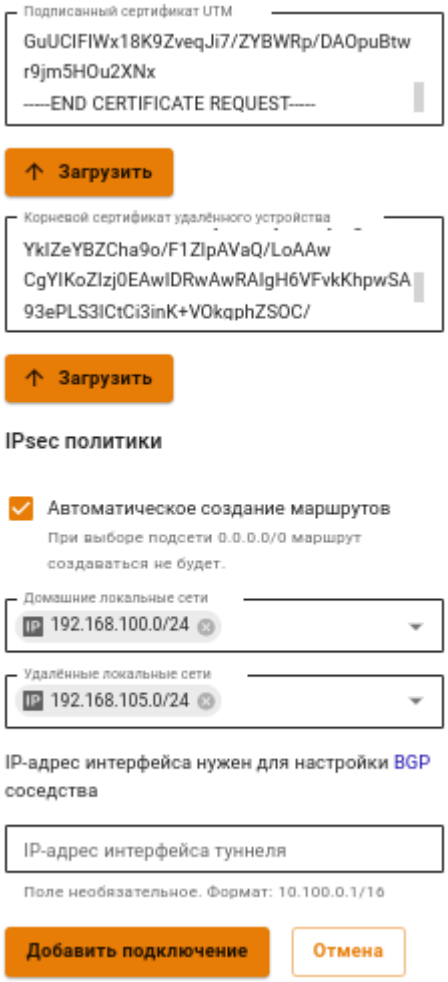


Файл вида `cert_export_device_<случайный набор символов>.ipsec.crt` - **это подписанный сертификат NGFW**.
Файл вида `cert_export_mk_ca.crt` - **это корневой сертификат MikroTik.**

Завершение настройки Ideco NGFW:

Перейдите обратно на Ideco NGFW во вкладку с настройками подключения устройства и продолжите заполнять поля:

- **Подписанный сертификат NGFW** - загрузите подписанный в MikroTik сертификат NGFW;
- **Корневой сертификат удаленного устройства** - загрузите корневой сертификат MikroTik;
- **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.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при использовании динамической маршрутизации BGP.



Нажмите кнопку **Добавить подключение**.

Входящее подключение

Тип аутентификации PSK

Настройка MikroTik:

Настроить устройство MikroTik можно:

- Через GUI
- Через консоль устройства
- Через конфигурационные скрипты, сгенерированные по адресу https://mikrotik.ideco.ru/.

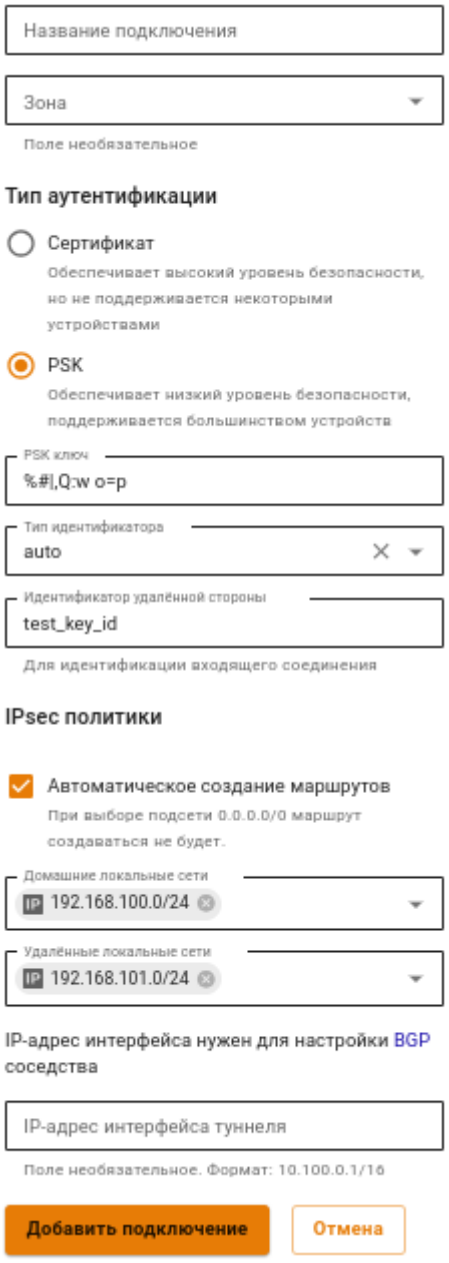
После генерации скрипта необходимо открыть раздел **System -> Scripts**, создать скрипт, вставить в него код, сгенерированный конфигуратором, и запустить.

Настройка Ideco NGFW:

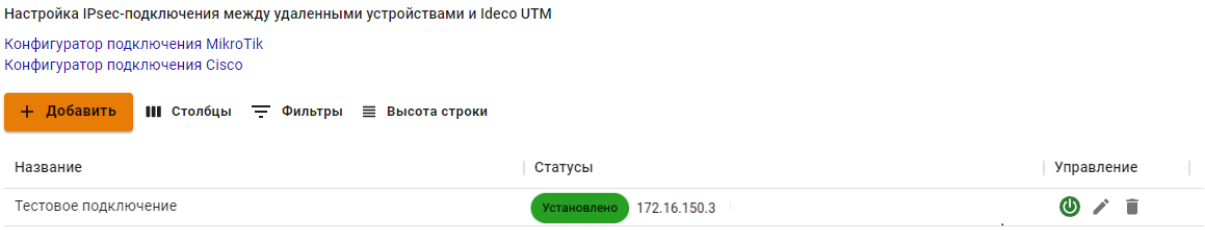
1. В Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**, нажмите **Добавить** и заполните поля:

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **PSK** - вставьте PSK-ключ, полученный от MikroTik;

- **Идентификатор удаленной стороны** - вставьте идентификатор MikroTik (параметр Key ID в `/ip ipsec peers`);
- **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;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP.



2. Нажмите кнопку **Добавить подключение**.



Тип аутентификации Сертификат

Подключение по сертификатам является более безопасным, чем подключение по PSK.

Настройка MikroTik:

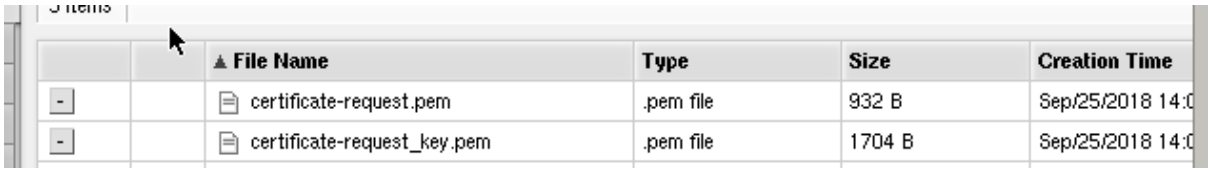
Настроить MikroTik можно:

- 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, вставить в него код, сгенерированный конфигуратором, и запустить его.

Конфигуратором генерируется два скрипта, потому в MikroTik также создайте два скрипта.

Перед настройкой необходимо запустить первый скрипт. В файловом хранилище MikroTik появятся два файла, которые необходимо скачать, они требуются для дальнейшей настройки:



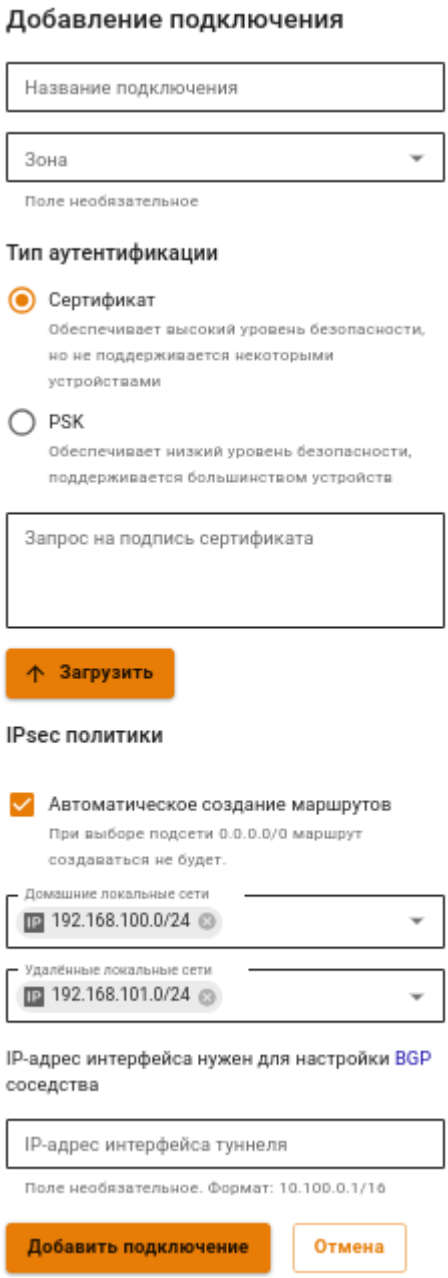
- Файл `certificate-request.pem` - **запрос на подпись сертификата**;
- Файл `certificate-request_key.pem` - **приватный ключ**.

Далее переходим к настройке Ideco NGFW.

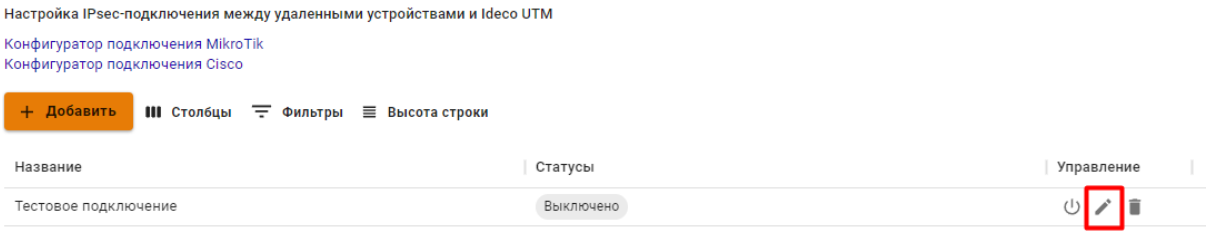
Настройка Ideco NGFW:

1. В Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**, нажмите **Добавить** и заполните поля:

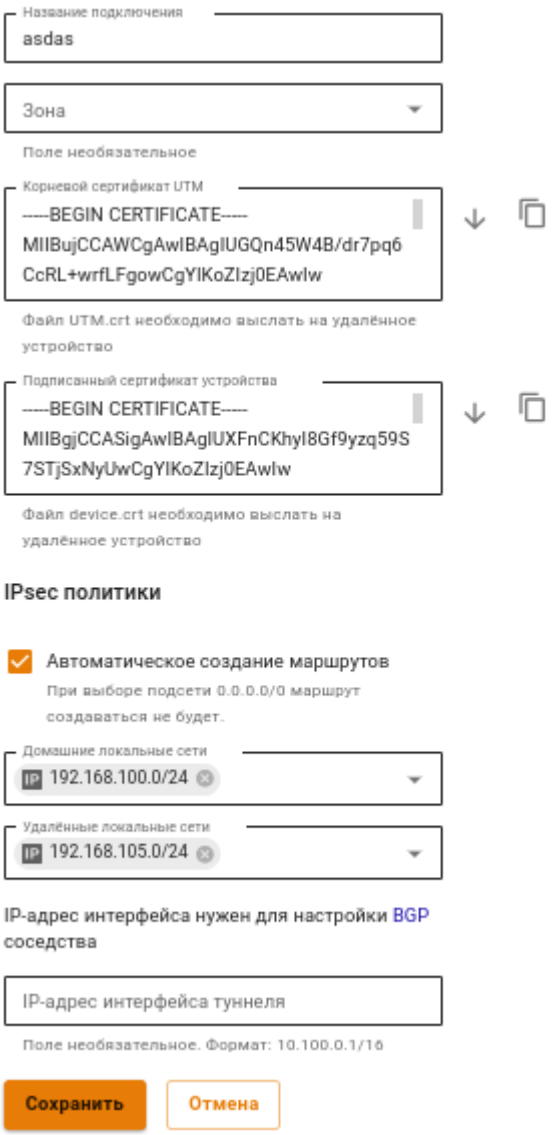
- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону, в которую требуется добавить IPSec-подключение;
- **Запрос на подпись сертификата** - загрузите запрос на подпись, **полученный от MikroTik**;
- **Домашние локальные сети** - необходимо перечислить все локальные сети NGFW, которые будут доступны в IPsec-подключении, т. е. будут видны противоположной стороне.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP.



2. Нажмите кнопку **Добавить подключение**. Нажмите на кнопку редактирования соединения, чтобы продолжить настройку.



3. Скачайте файлы, которые находятся в полях **Корневой сертификат NGFW** и **Подписанный сертификат устройства**, для их последующего использования в MikroTik.



Проблемы при повторной активации входящего 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 brute-force 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.

Подключение MikroTik к Ideco NGFW 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.

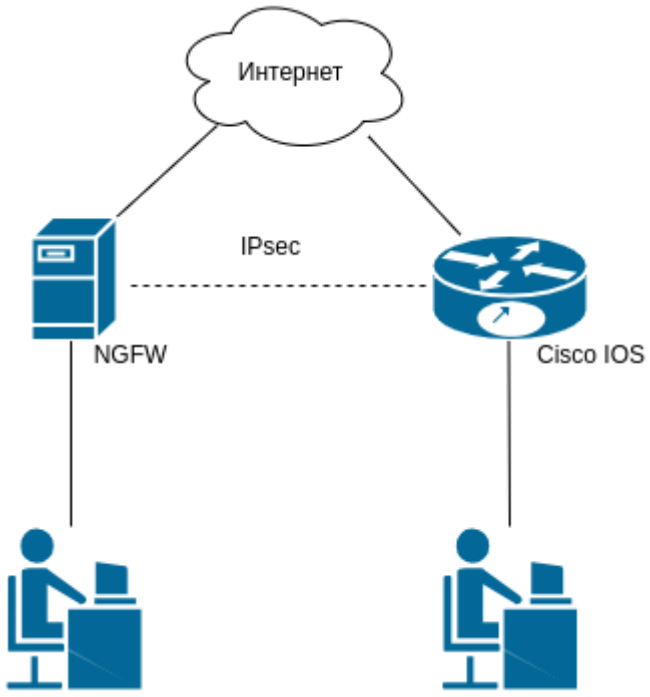
Пример:

- 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
```

16.12.7 Подключение Cisco IOS к Ideco NGFW по IPsec

Рассмотрим настройку подключения по схеме, представленной на рисунке ниже:



Для настройки подключения Cisco IOS к Ideco NGFW нужно следовать инструкции в каждом из пунктов.

Первоначальная настройка Ideco NGFW и Cisco IOS:

Настройка Ideco NGFW

Настройте на Ideco NGFW локальный и внешний интерфейсы. Подробная информация находится в статье *Первоначальная настройка*.

Настройка Cisco IOS EX

Настройку Cisco можно осуществить через консоль устройства или, воспользовавшись нашими конфигурационными скриптами, сгенерированными по адресу https://cisco.ideco.ru/.

Настройка Cisco через консоль:

1. Настройка локального интерфейса:

```
enable
conf t
interface GigabitEthernet2
ip address <локальный IP Cisco> <маска подсети>
no shutdown
ip nat inside
exit
```

2. Настройка внешнего интерфейса:

```
interface GigabitEthernet1
ip address <внешний IP Cisco> <маска подсети>
no shutdown
ip nat outside
exit
```

3. Проверьте наличие связи между внешними интерфейсами Ideco NGFW и Cisco. Для этого в консоли Cisco используйте команду `ping <внешний IP NGFW>`. Результат вывода команды - наличие ICMP-ответов.

4. Создание access-list с адресацией локальной сети:

```
ip access-list extended NAT
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit
```

5. Настройка NAT:

```
ip nat inside source list NAT interface GigabitEthernet1 overload
exit
```

6. Сохранение настроек конфигурации:

```
write memory
```

7. **После сохранения настроек проверьте, что из локальной сети Cisco присутствует доступ в сеть интернет.**
Для этого перейдите на какой-нибудь сайт (например: https://www.cisco.com/) с устройства в локальной сети Cisco.

Настройка IKEv2+IPsec на Cisco:

1. Создание proposal:

```
conf t
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha256
group 19
exit
```

2. Создание policy:

```
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
exit
```

3. Создание peer (key_id - идентификатор удаленной стороны, т. е. Ideco NGFW):

```
crypto ikev2 keyring key
peer strongswan
address <внешний IP NGFW>
identity key-id <key_id>
pre-shared-key local <psk>
pre-shared-key remote <psk>
exit
exit
```

4. Создание IKEv2 profile:

```
crypto ikev2 profile ikev2profile
match identity remote address <внешний IP NGFW> 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local key
exit
```

5. Настройка шифрования в esp:

```
crypto ipsec transform-set TS esp-gcm 256
mode tunnel
exit
```

6. Создание ipsec-isakmp:

```
crypto map cmap 10 ipsec-isakmp
set peer <внешний IP NGFW>
set transform-set TS
set ikev2-profile ikev2profile
match address cryptoacl
exit
```

7. Настройка crypto map на внешнем интерфейсе:

```
interface GigabitEthernet1
crypto map cmap
exit
```

8. Создание access-list для трафика между локальными сетями Cisco и NGFW:

```
ip access-list extended cryptoacl
permit ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW>
↪<обратная маска подсети>
exit
```

9. Добавление в access-list NAT исключения трафика между локальными сетями Cisco и NGFW (правило `deny` должно оказаться выше чем `permit`):

```
ip access-list extended NAT
no permit ip <локальная подсеть Cisco> <обратная маска подсети> any
deny ip <локальная подсеть Cisco> <обратная маска подсети> <локальная подсеть NGFW>
↪<обратная маска подсети>
permit ip <локальная подсеть Cisco> <обратная маска подсети> any
exit

end
```

10. Сохранение настроек конфигурации:

```
write memory
```

Настройка исходящего подключения Ideco NGFW к Cisco IOS:

Для настройки исходящего IPsec подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Адрес удаленного устройства** - введите IP-адрес удаленного устройства;
- **Тип аутентификации** - PSK;
- **PSK** - будет сгенерирован случайный PSK-ключ. Он потребуется, чтобы настроить подключение в Cisco;
- **Идентификатор NGFW** - введенный вами ключ будет использоваться для идентификации исходящего подключения. Введите также этот идентификатор в Cisco;
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW;
- **Удаленные локальные сети** - укажите локальную сеть Cisco;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP;

3. Проверьте, что подключение установилось (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

4. Проверьте наличие трафика между локальными сетями (TCP и web).

Подсказка: Если Cisco передает внешний IP-адрес вместо **KeyID** (проверьте, включив расширенный лог IPsec на Cisco), укажите в качестве **Идентификатора удаленной стороны** внешний IP-адрес Cisco.

Настройка входящего подключения Ideco NGFW к Cisco IOS:

Для настройки входящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Устройства(входящие подключения)**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ;
- **Идентификатор удаленной стороны** - вставьте идентификатор Cisco (параметр Key ID);
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW;
- **Удаленные локальные сети** - укажите локальную сеть Cisco;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации.

3. Сохраните созданное подключение, затем нажмите на кнопку **Включить**.

4. Проверьте, что подключение установлено (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

5. Проверьте наличие трафика между локальными сетями (TCP и web).

Итоговая конфигурация IKEv2 IPsec на Cisco IOS должна выглядеть следующим образом:

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy ikev2policy
 match fvrf any
 proposal ikev2proposal

crypto ikev2 keyring key
 peer strongswan
  address 5.5.5.5
  pre-shared-key local QWEqwe1234567890
  pre-shared-key remote QWEqwe1234567890

crypto ikev2 profile ikev2profile
 match identity remote key-id key-id
 authentication remote pre-share
 authentication local pre-share
 keyring local key

crypto ipsec transform-set TS esp-gcm 256
 mode tunnel

crypto map cmap 10 ipsec-isakmp
 set peer 5.5.5.5
 set transform-set TS
 set ikev2-profile ikev2profile
 match address cryptoacl

interface GigabitEthernet1
! внешний интерфейс
 ip address 1.1.1.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
```

(continues on next page)

(продолжение с предыдущей страницы)

```
 no mop sysid
 crypto map cmap

interface GigabitEthernet2
! локальный интерфейс
 ip address 2.2.2.2 255.255.255.0
 ip nat inside
 negotiation auto
 no mop enabled
 no mop sysid

ip nat inside source list NAT interface GigabitEthernet1 overload

ip access-list extended NAT
 deny   ip 2.2.2.0 0.0.0.255 3.3.3.0 0.0.0.255
 permit ip 2.2.2.0 0.0.0.255 any
ip access-list extended cryptoacl
 permit ip 2.2.2.0 0.0.0.255 3.3.3.0 0.0.0.255
```

16.12.8 Подключение pfSense к Ideco NGFW по IPsec

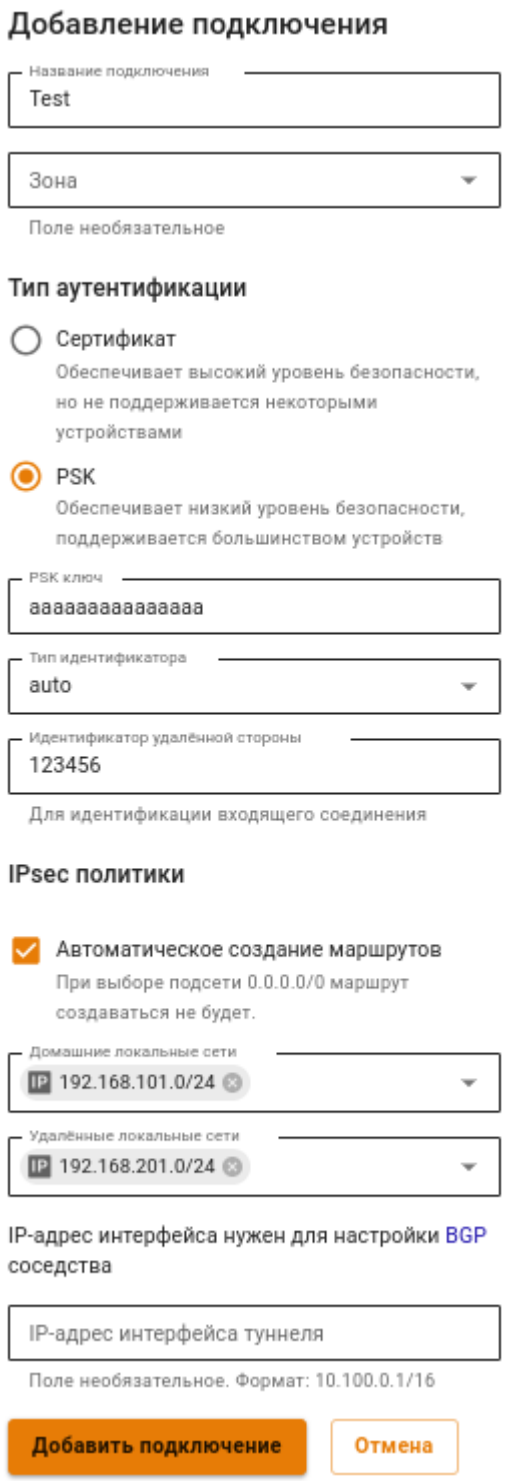
Подсказка: Объединяемые локальные сети не должны пересекаться!

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:

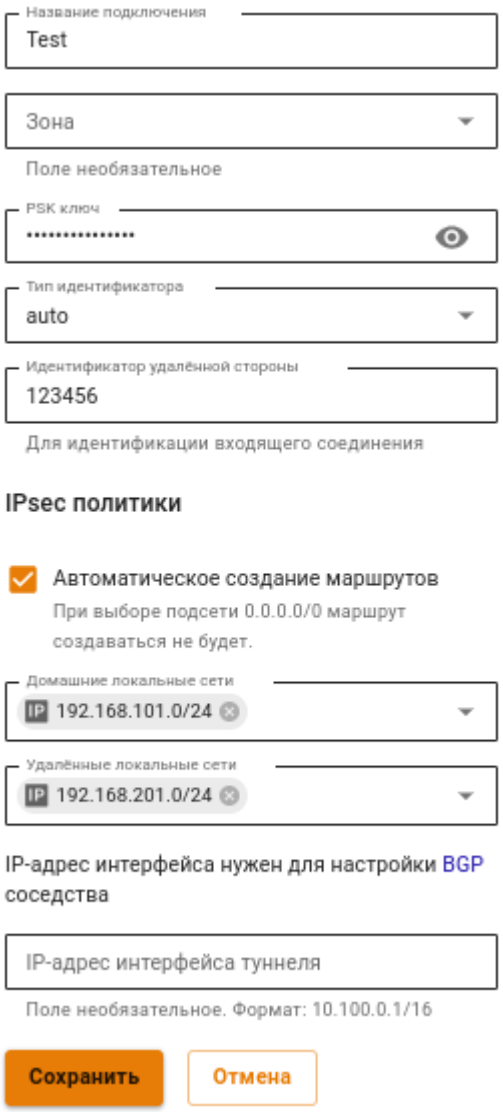
- **Название подключения** - любое;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения;
- **Идентификатор удаленной стороны** - любой;
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense;
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW.



3. Сохраните созданное подключение, нажмите на кнопку **Включить**. 4. Скопируйте значение идентификатора удаленной стороны одним из способов:

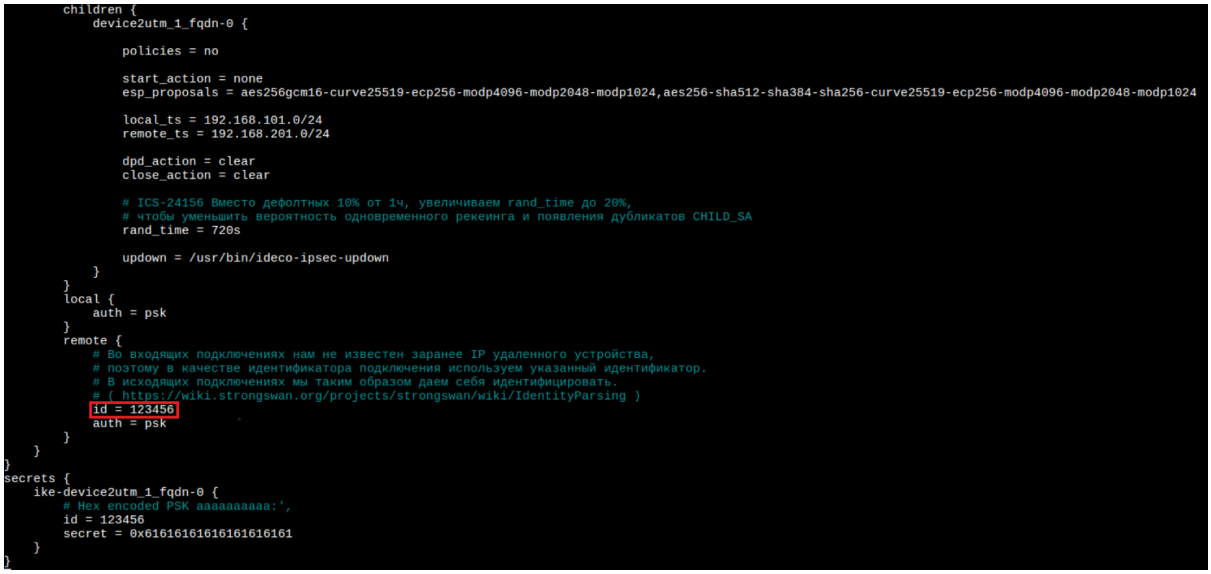
В интерфейсе NGFW:

Во 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.

1. **Algorithm** - AES256-GCM;
2. **Key length** - 128 bit;
3. **Hash** - SHA256;
4. **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.

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.
- **Для Ideco UTM версии 10.0 и Ideco NGFW версии 16.0 и новее** используйте следующие параметры: 1. **Algorithm** - AES256-GCM; 2. **Key length** - 128 bit; 3. **Hash** - SHA256; 4. **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. Затем нужно разрешить 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).

7. Обращаем внимание на раздел файрвола **WAN** - в нем по умолчанию запрещен входящий трафик из «серых» подсетей, который требуется разрешить.

8. 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.

16.12.9 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.

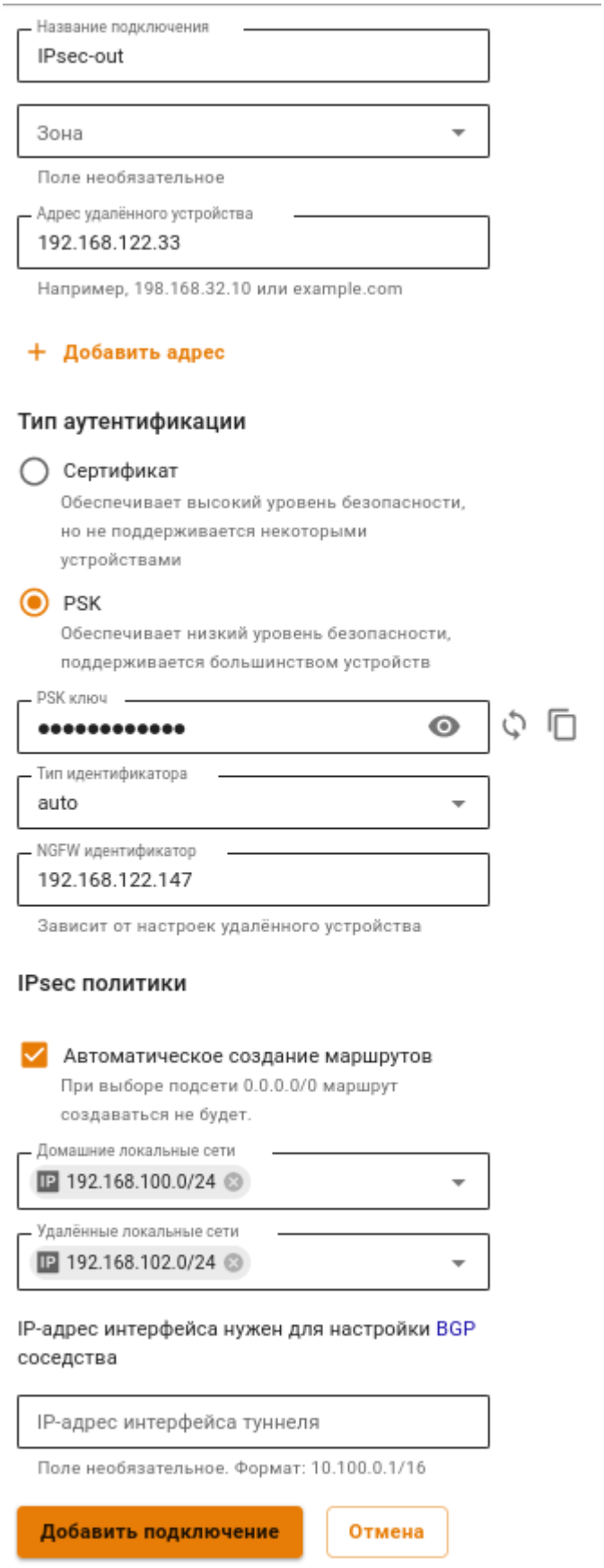
Подключение от Ideco NGFW к Kerio Control

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:

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Адрес удаленного устройства** - укажите внешний IP-адрес Kerio Control;
- **Тип аутентификации** - выберите тип PSK;
- **PSK-ключ** - укажите PSK-ключ, который будет использоваться для подключения;
- **Тип идентификатора** - выберите auto;
- **NGFW идентификатор** - укажите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- **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;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации:



3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

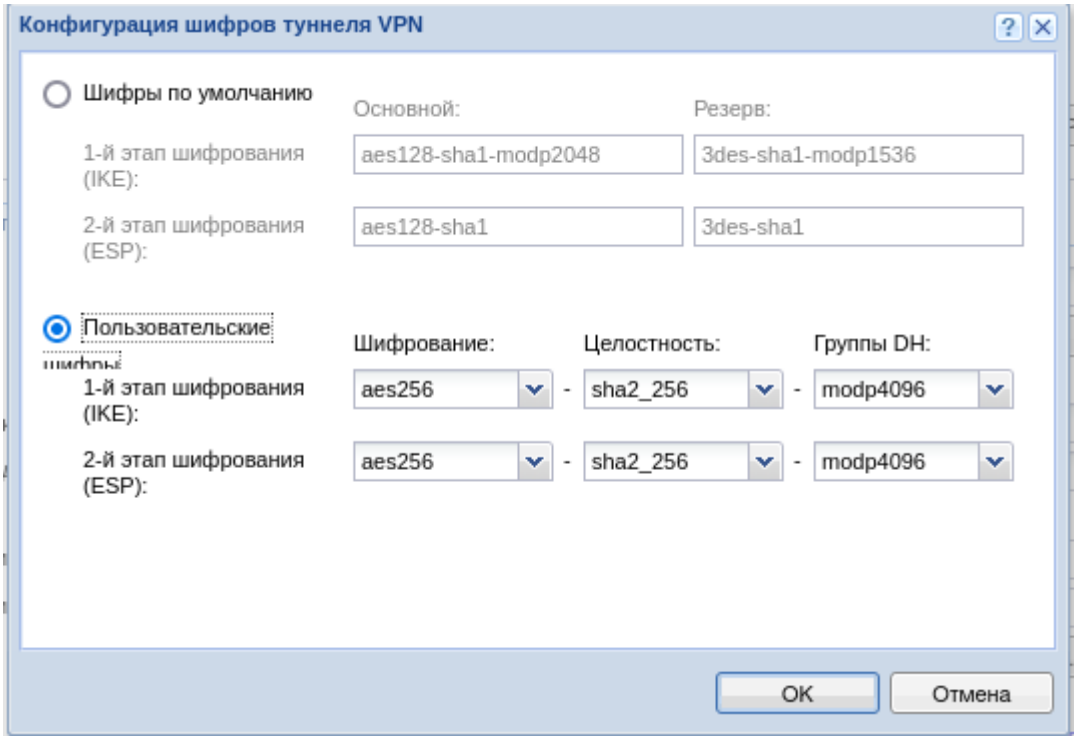
Настройка завершена, теперь переходим к настройке Kerio Control.

Настройка входящего подключения на Kerio Control:

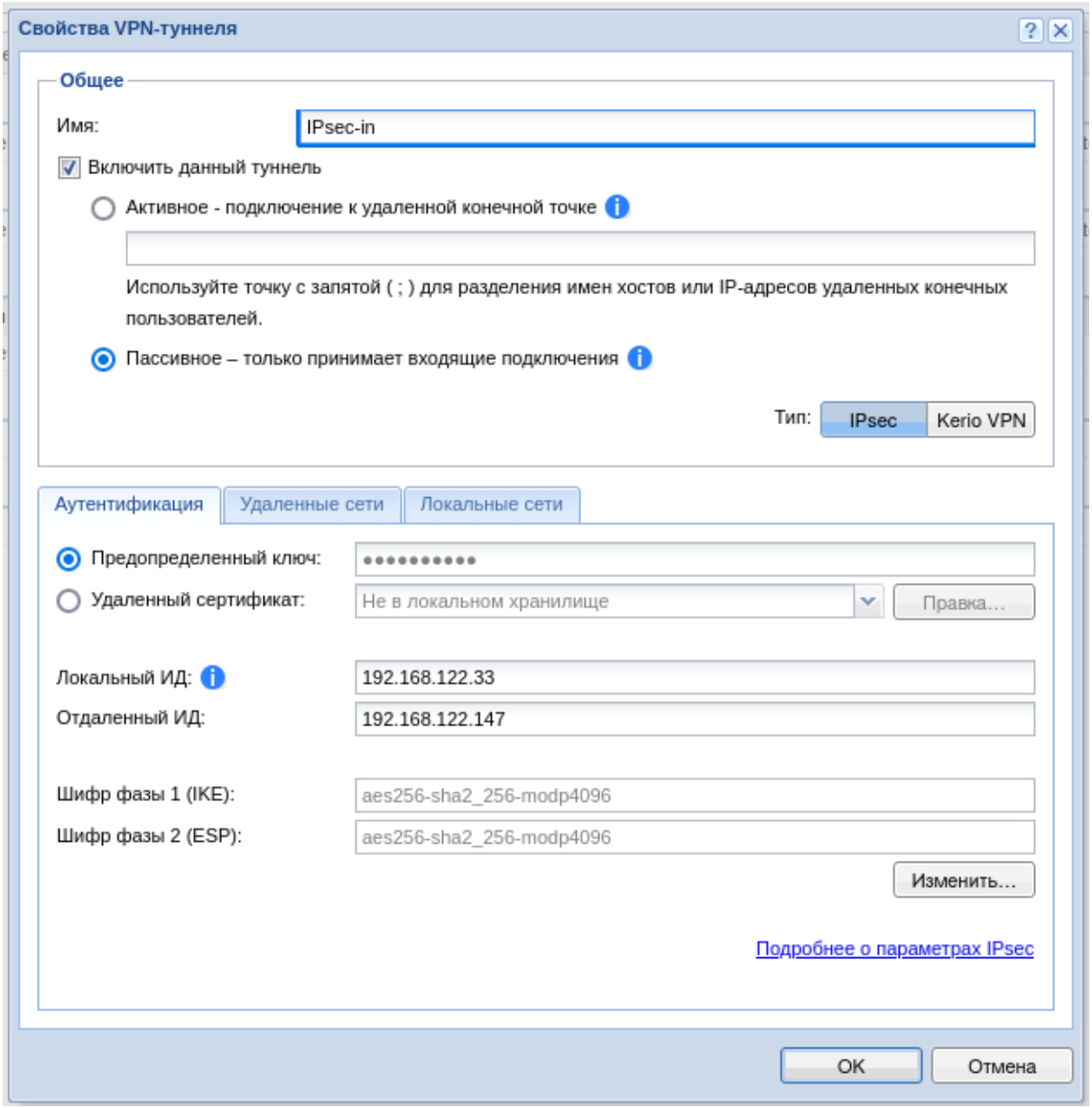
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель. . .** .

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec;
- **Имя** - произвольное;
- **Включить данный туннель**;
- Тип **Пассивное**;
- **Предопределенный ключ** - введите PSK-ключ, который был указан при создании подключения на Ideco NGFW;
- **Локальный ИД** - укажите IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения;
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW;
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



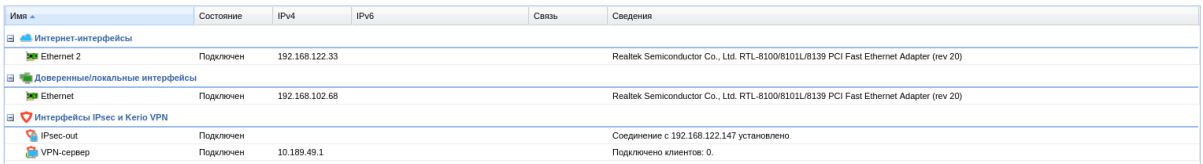
Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW, которая будет видна из подсети Kerio Control.

4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице:



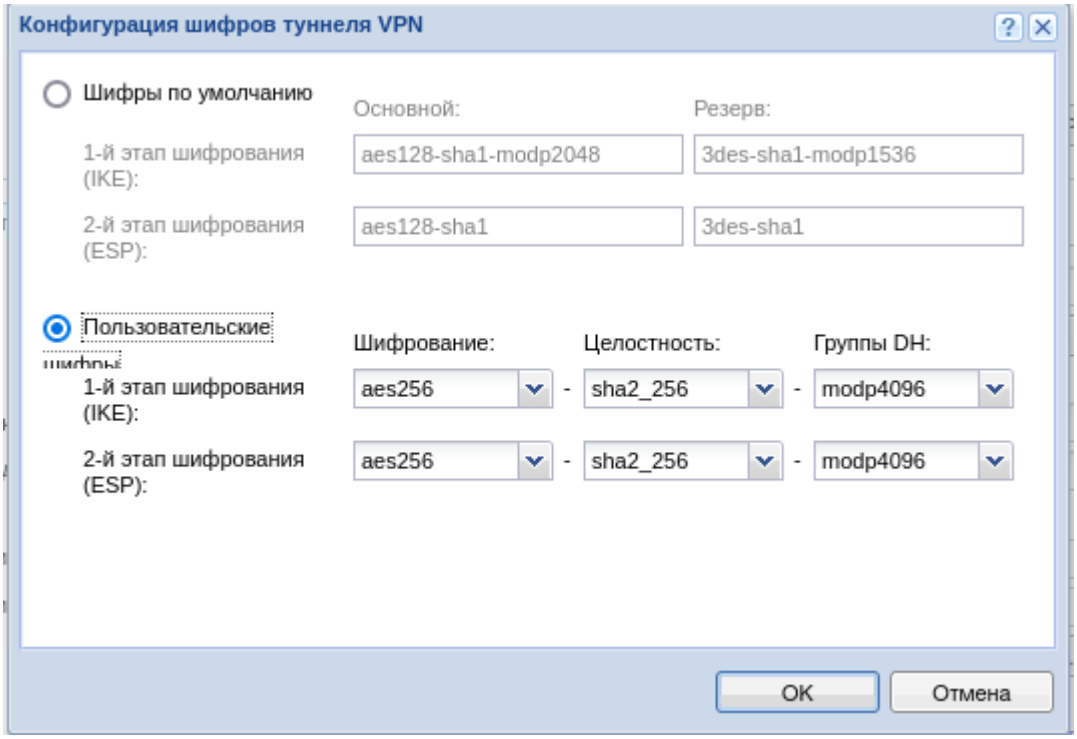
Подключение от Kerio Control к Ideco NGFW

Настройка исходящего подключения на Kerio Control:

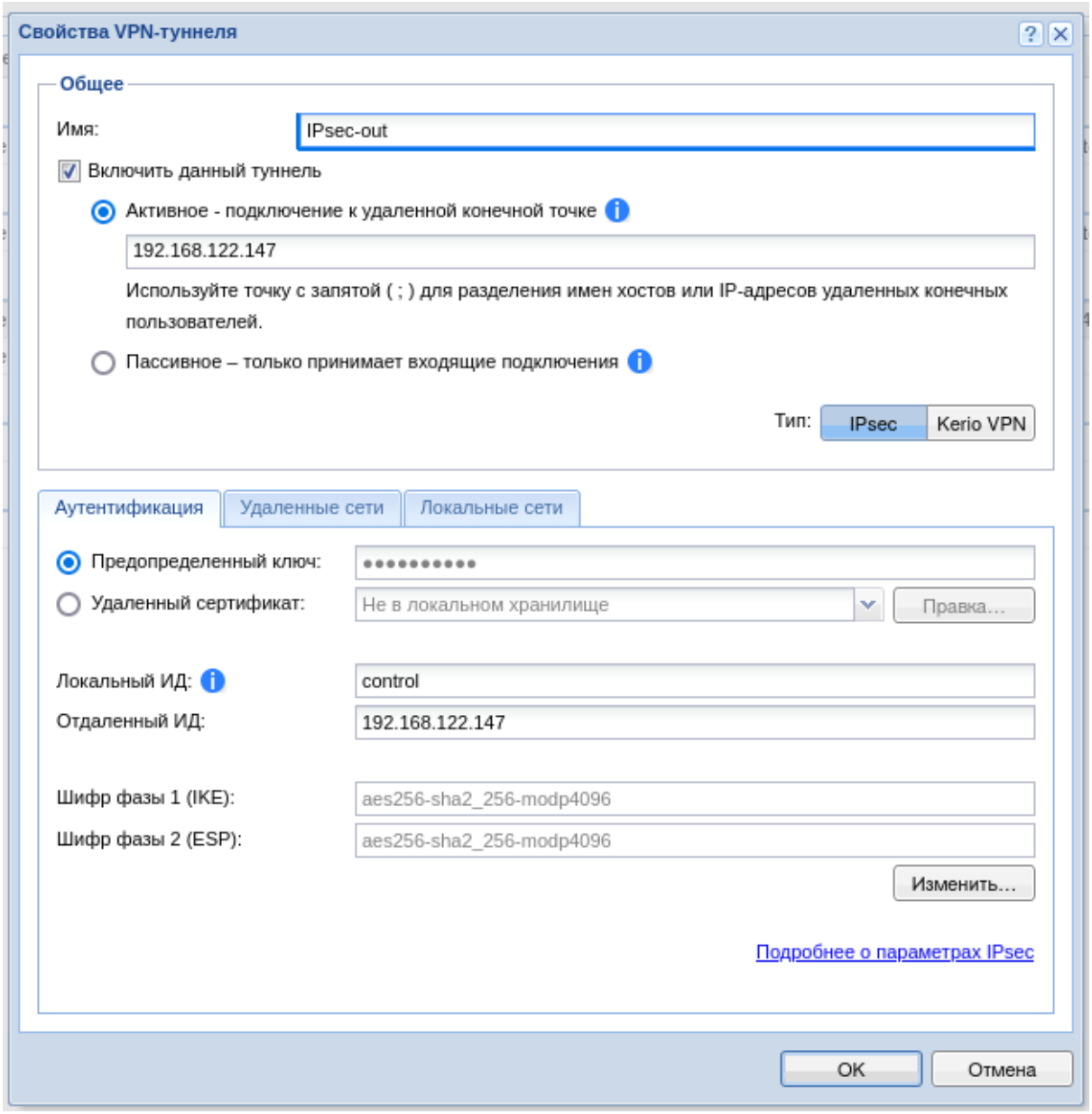
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель. . .** .

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec;
- **Имя** - произвольное;
- **Включить данный туннель**;
- Выберите тип **Активное** и в поле под ним пропишите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- **Предопределенный ключ** - введите PSK-ключ, который будет использоваться для подключения;
- **Локальный ИД** - укажите ключ, который будет задан в поле **Идентификатор NGFW** при настройке входящего подключения на Ideco NGFW, или IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения. **Предпочтительное значение - имя хоста Kerio**;
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW, которая будет видна из подсети Kerio Control.

4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице.

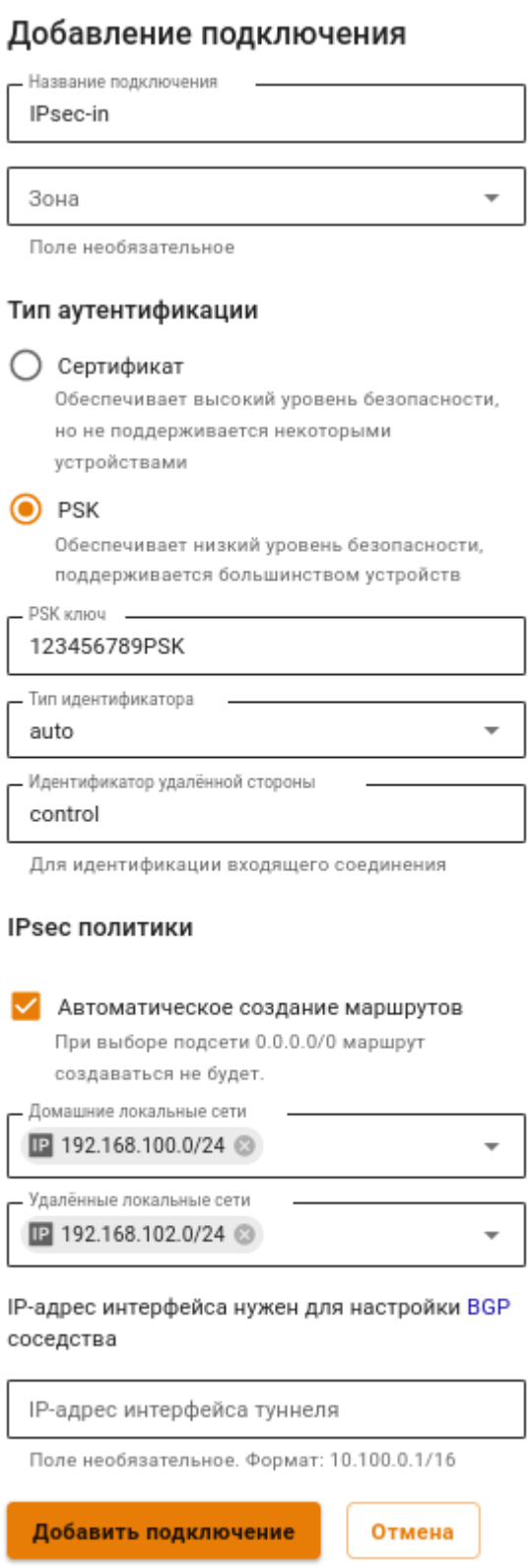
Настройка входящего подключения на Ideco NGFW:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**.

2. Добавьте новое подключение и заполните поля:

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec подключения;
- **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;
- **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;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации:



3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

Настройка завершена, теперь переходим к настройке Kerio Control.

Подсказка: При возникновении проблем обратите внимание на настройки файрвола Kerio Control.

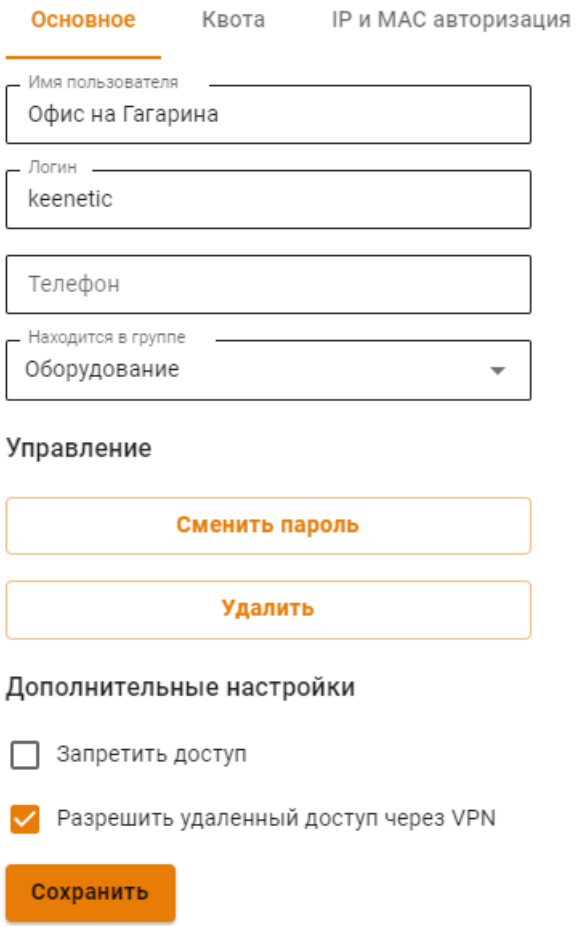
16.12.10 Подключение Keenetic по SSTP или IPsec

Основное

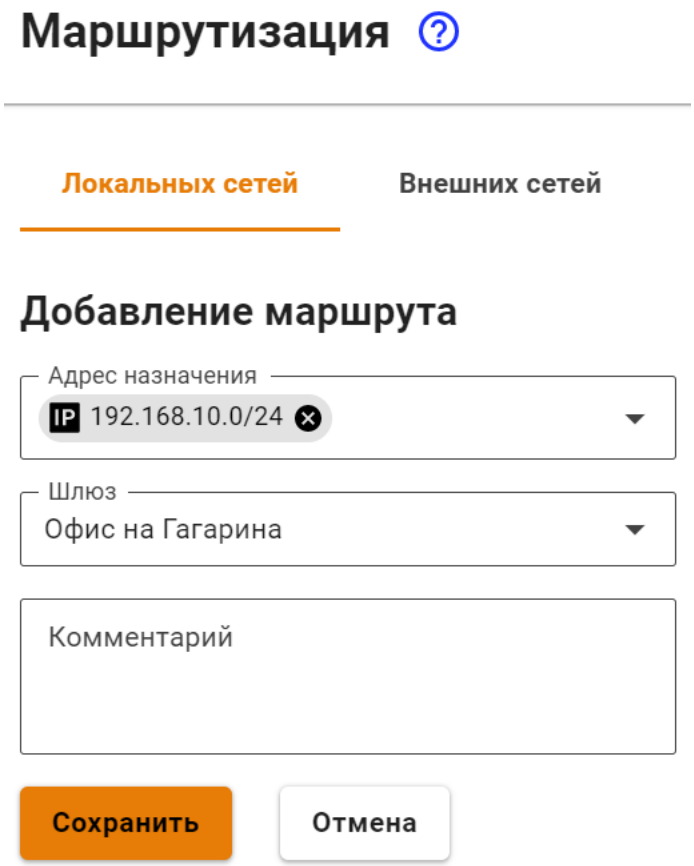
Если доступ из центрального офиса в сеть за Keenetic не нужен, то воспользуйтесь статьей *Подключение по SSTP Wi-Fi роутеров Keenetic* по client-to-site подключению.

Настройка Ideco NGFW:

1. Включите и настройте порт и домен для SSTP в разделе **Пользователи -> VPN-подключение**.
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 следующий 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.

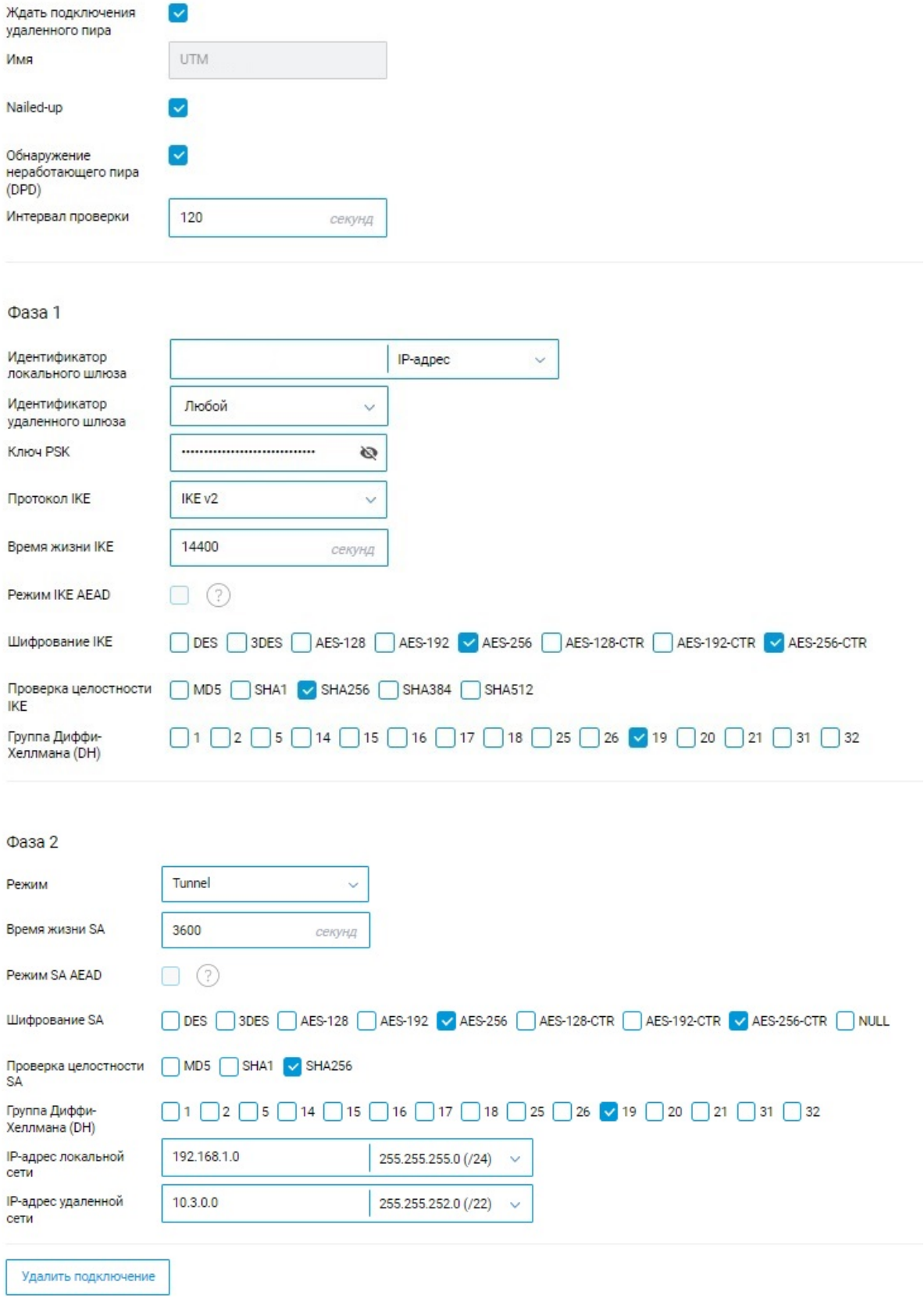
Разрешите доступ до «не локальных» сетей во всех профилях, выполнив команду в PowerShell (запущенного с повышением прав до администратора): `Enable-NetFirewallRule -Group "@FirewallAPI.dll, -28502"`

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:

Настройка IPsec-подключения сеть—сеть



16.13 Сертификаты

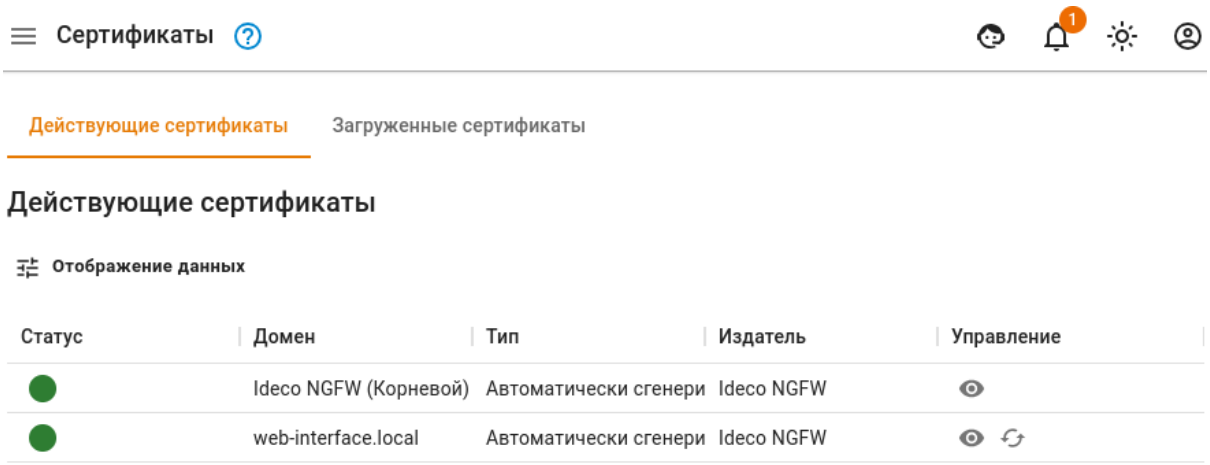
16.13.1 Общая информация

В этом разделе отображаются SSL-сертификаты или цепочки сертификатов, список которых формируется следующими модулями:

- Модуль обратного проксирования;
- VPN-серверы IKEv2 и SSTP;
- Веб-интерфейс, веб-аутентификация;
- Почта.

Для просмотра основной информации о сертификате нажмите кнопку .

Действующие сертификаты

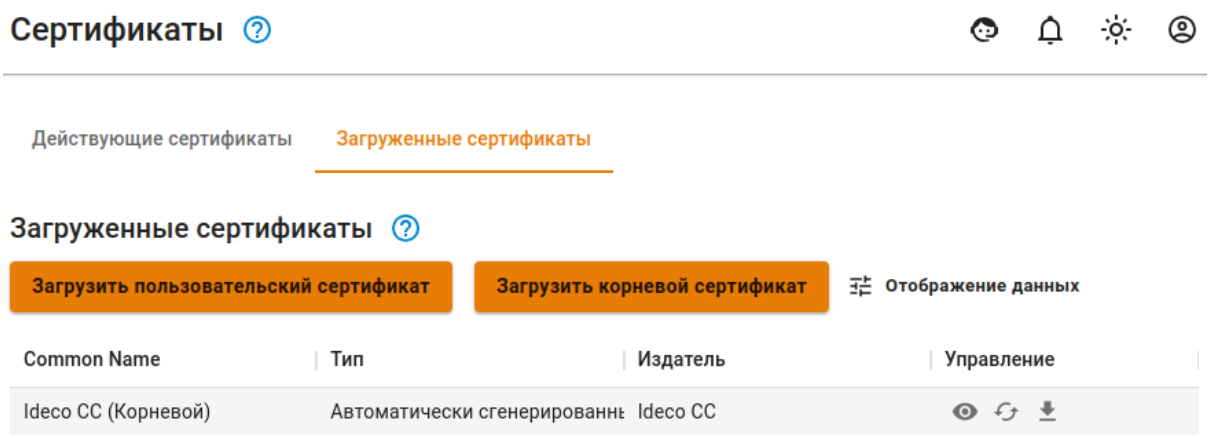


В таблице *Действующие сертификаты* отображаются:

- 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*.

16.13.2 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 отправляется запрос на выпуск цепочки в Let's Encrypt.

Подсказка: 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.

---

3. При успешном выпуске цепочки сертификатов Let's Encrypt заменяет локальную цепочку.

4. Если выпуск цепочки сертификатов Let's Encrypt завершился неудачей, продолжит использовать локальную цепочку сертификатов.

Если требуется повторить попытку получения сертификата Let's Encrypt вместо самоподписанного, то нужно нажать на кнопку **Перевыпустить** в столбце **Управление**.

Сертификат Let's Encrypt **выпускается на 3 месяца** и будет **автоматически перевыпущен** по окончании срока действия.

Процесс перевыпуска сертификата

Чтобы перевыпустить не корневую цепочку сертификатов, нажмите кнопку в столбце **Управление** в таблице **Действующие сертификаты**. NGFW попробует 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 или перевыпуске цепочки корневого сертификата, *IPsec-соединения* между NGFW перестанут работать (необходимо их пересоздать).

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 .

16.13.3 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 следующим требованиям:

- Сертификаты должны иметь расширения *.pem*. Если у вашего сертификата другое расширение, конвертируйте его, изучив статью *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).Если вы хотите заменить автоматически выпущенную цепочку сертификатов на свою, то 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 не валидна, переходите к статье *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.

Подготовка SSL-сертификата для загрузки на NGFW:

При покупке доверенного SSL-сертификата на домен у Certificate Authority или Центра сертификации данные для его установки как правило высылаются электронным письмом в разрозненном виде. Для корректной загрузки сертификаты на домен, промежуточные и корневые сертификаты нужно собрать в один файл в правильном порядке.

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.

Подсказка: 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 и для установки 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.

4. Для подготовки сертификата к загрузке воспользуйтесь статьей *Подготовка SSL-сертификата для загрузки на NGFW*.

5. Для загрузки сертификата на NGFW воспользуйтесь статьей *Загрузка SSL-сертификата на NGFW*.

16.13.4 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
```

- `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
```

- 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).
6. Воспользуйтесь *инструкцией по загрузке сертификата на NGFW*.

16.13.5 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
```

- 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
```

- server.pem - Самоподписанный сертификат для загрузки на сервер.

Подсказка: Для загрузки сертификата на сервер воспользуйтесь статьей *Загрузка SSL-сертификата на сервер*

---

17. Отчеты и журналы

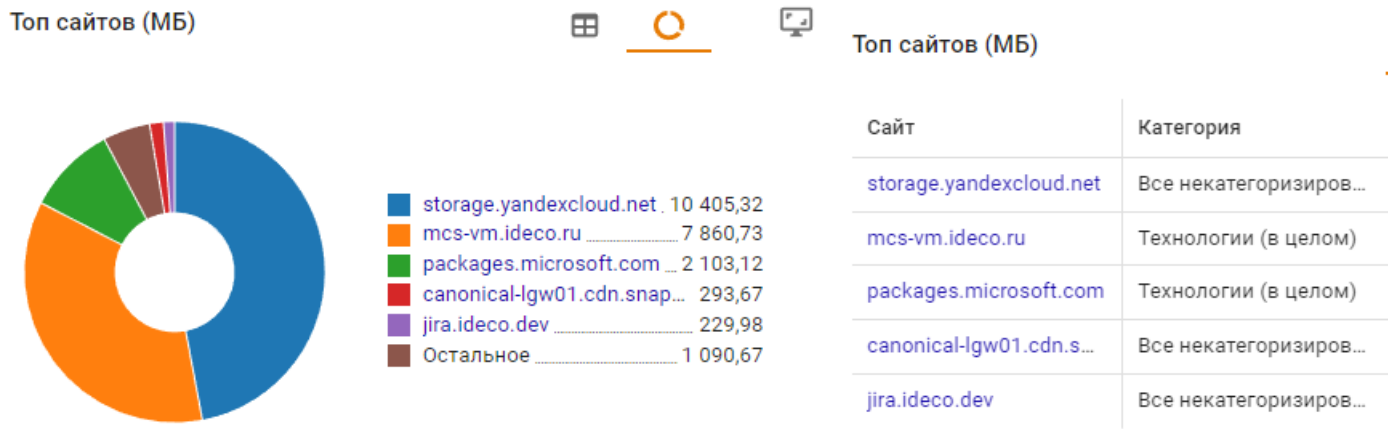
17.1 Трафик

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.

17.1.1 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.

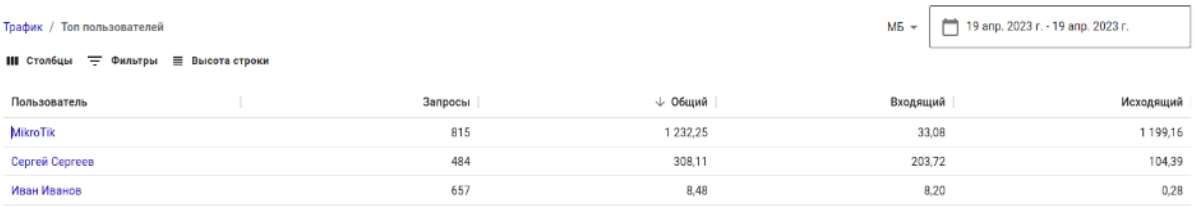


Единицу измерения можно изменить в левом верхнем углу:

Доступные варианты: Трафик в КБ, МБ, ГБ или Запросы.

Развернутый режим ( )

Содержит данные по всем объектам из топа. Для поиска по объектам воспользуйтесь **Фильтром**( ).



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 правом 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** ( ).

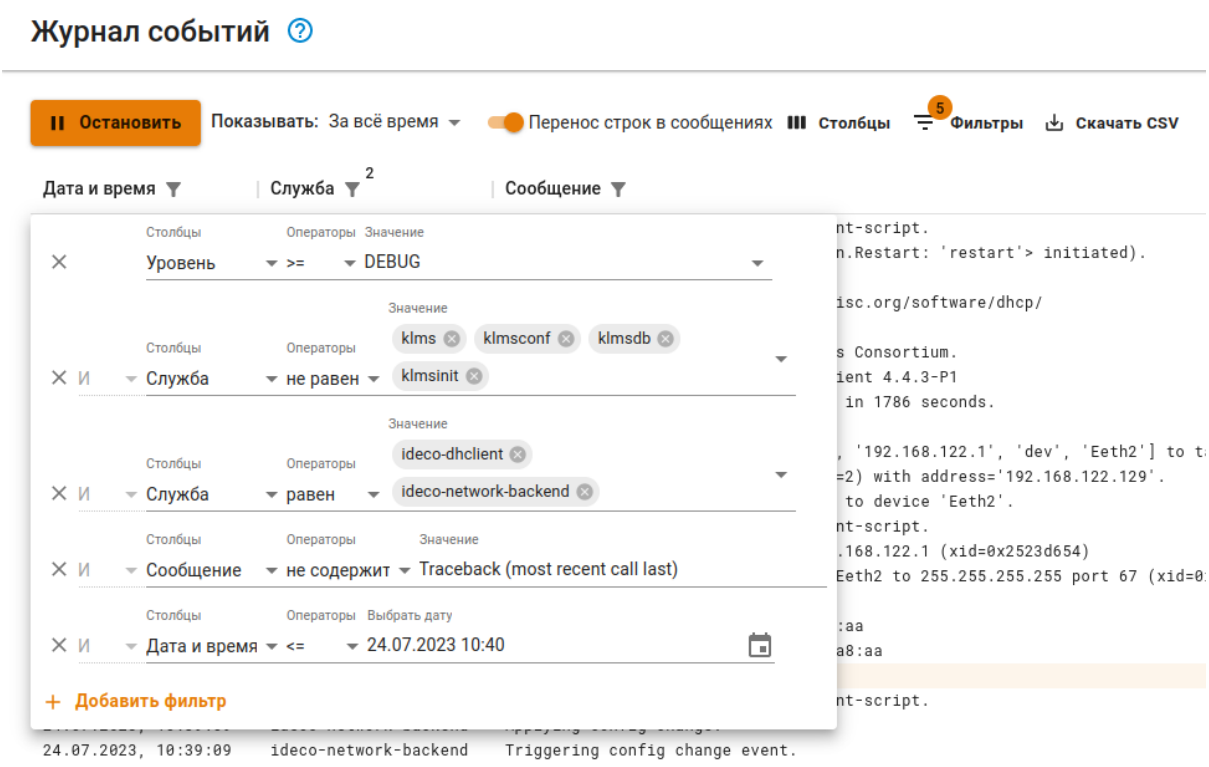
Подробнее о создании собственных шаблонов со статистикой - в статье *Конструктор отчетов*.

17.2 Журнал событий

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 заданны фильтрацией.

Список служб, доступных в разделе:

- **Файрвол** - ideco-firewall-backend, ideco-nflog;
- **Контроль приложений** - ideco-app-backend, ideco-app-control@Leth<номер локального интерфейса>;
- **Контент-фильтр** - ideco-content-filter-backend;
- **Ограничение скорости** - ideco-shaper-backend;
- **Антивирусы веб-трафика** - ideco-av-backend, ideco-clamd;
- **Предотвращение вторжений** - ideco-suricata-backend, ideco-suricata, ideco-suricata-event-syncer, ideco-suricata-event-to-syslog;
- **Объекты** - ideco-alias-backend;
- **Квоты** - ideco-quotas-backend, systemd-quotacheck;
- **Сетевые интерфейсы** - ideco-network-backend, ideco-network-nic;
- **Балансировка и резервирование**, **Маршрутизация** - ideco-routing-backend;
- **BGP**, **OSPF** - ideco-routing-backend;
- **Прокси** - ideco-proxy-backend, squid;
- **Обратный прокси** - ideco-reverse-backend;
- **DNS** - ideco-dns-backend, unbound;
- **DDNS** - ideco-dns-backend;
- **DHCP** - ideco-dnsmasq;
- **IPsec** - ideco-ipsec-backend, strongswan;
- **Центральная консоль** - ideco-central-console-backend;

- **Кластеризация** - ideco-cluster-backend, ideco-cluster-backup-pusher;
- **Автоматическое обновление** - ideco-sysupdate-backend;
- **Резервное копирование** - 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;
- **Авторизация** - ideco-auth-backend;
- **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-monitor-backend;
- **Обнаружение устройств** - ideco-netscan-backend;
- **Web Application Firewall** - ideco-waf-backend, ideco-waf-event-syncer;
- **IGMP Proxy** - igmpproxy.

17.2.1 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.

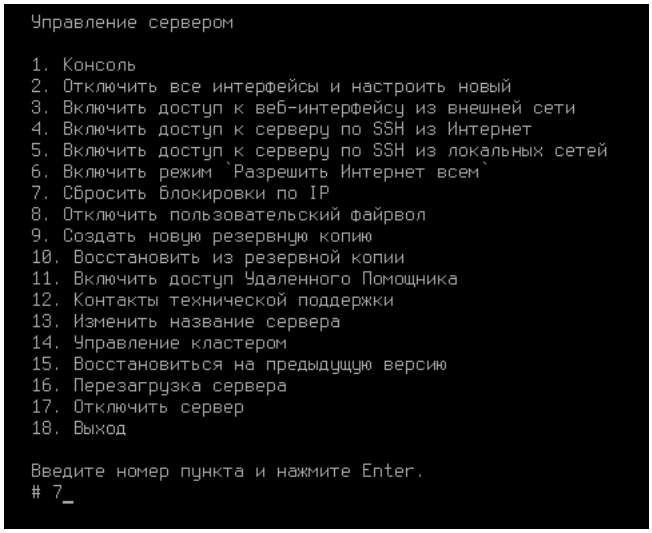
Логи службы `fail2ban` можно увидеть:

- В веб-интерфейсе в разделе **Отчеты и журналы -> Журнал Событий**, 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**:



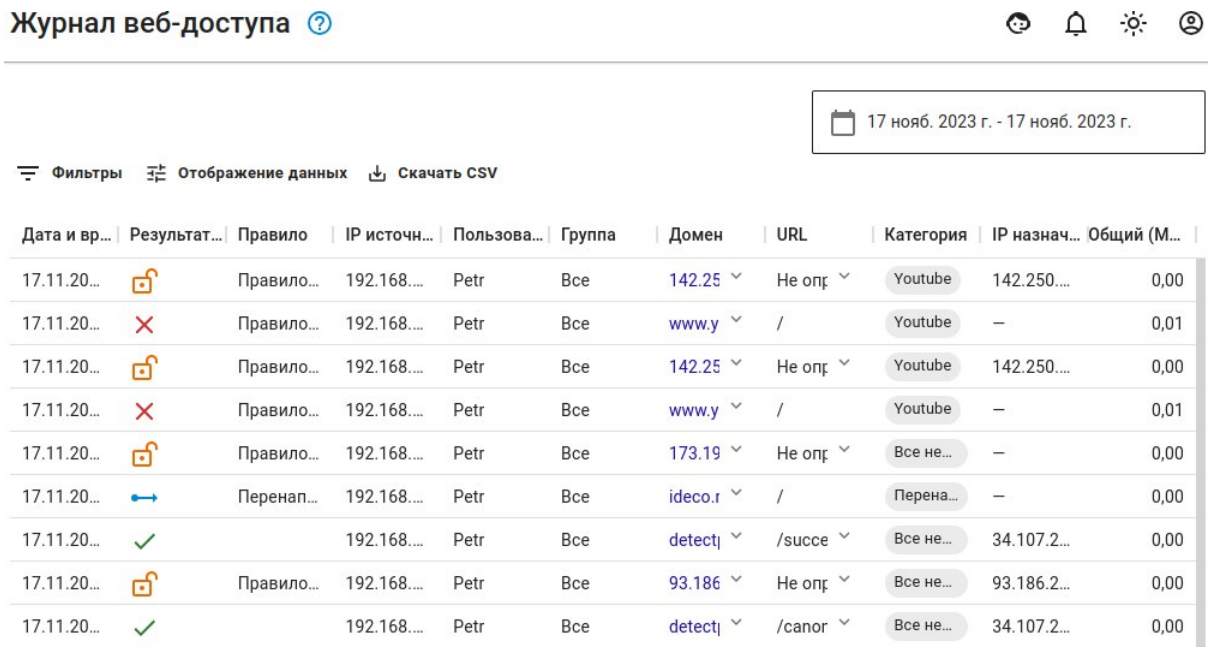
17.3 Журнал веб-доступа

17.3.1 Основное

Раздел позволяет посмотреть результат обработки пользовательского запроса службой **Контент-фильтра**. Для просмотра **Журнала веб-доступа** перейдите в раздел **Отчеты и Журналы -> Журнал веб-доступа**.

Результаты обработки службы:

- - **Разрешено**
- - **Расшифровано**
- - **Запрещено**
- - **Перенаправлено на**



Подсказка: Если нет доступа к какому-либо интернет-ресурсу, воспользуйтесь разделом **Журнал веб-**

доступа для поиска правила, блокирующего этот ресурс.

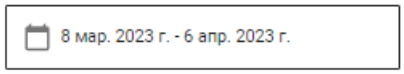
Подсказка: Для просмотра блокировок по конкретному правилу воспользуйтесь фильтром, указав в форме наименование правила и оператор.

17.4 События безопасности

Подсказка: Все виджеты формируются в часовом поясе сервера.

События безопасности структурируют информацию, полученную от раздела *Предотвращение вторжений*.

17.4.1 Выбор периода

Все отображаемые данные можно фильтровать по дате и времени. Например, установить какой-то временной период (по кнопке 

) или воспользоваться одним из предустановленных фильтров:

Доступные варианты: сегодня, вчера, текущая неделя, прошлая неделя, текущий месяц, прошлый месяц.

Если ни один фильтр по дате и времени не задан, то по умолчанию устанавливается интервал **Сегодня** в часовом поясе сервера.

17.4.2 Графики IDS/IPS

Виджеты содержат краткую информацию, собранную разделом **Предотвращение вторжений**. Подробная информация обо всех срабатываниях правил **Предотвращение вторжений** доступна на вкладке **Журнал IDS/IPS** в виде таблицы.

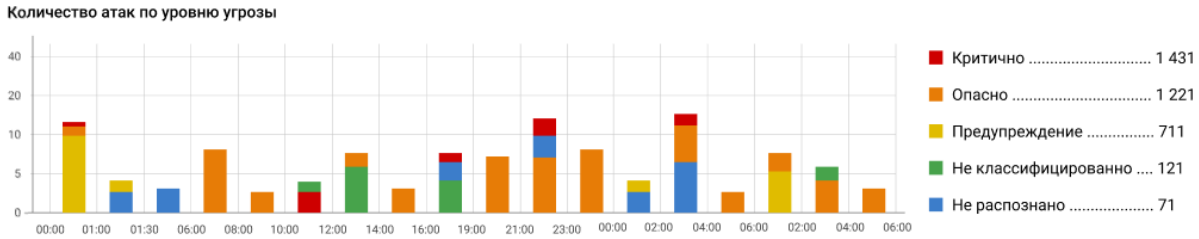
В таблице можно найти ID правила, которое сработало, и при необходимости создать исключение в разделе *Предотвращение вторжений*.

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.

Пример виджета *Количество атак по уровню угрозы*:



При нажатии на уровень угрозы все виджеты фильтруют содержание для этого уровня. Для перехода обратно к списку уровней угроз нажмите еще раз по выбранному уровню.

Описание виджетов

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:

Виджет подсчитывает статистику типов атак (например, типы атак *Черный список IP-адресов* или *Попытки получения привилегий администратора*, объединяющие в себе группу нескольких правил) по количеству срабатываний с данным типом атаки.
Тип атаки указан в столбце *Событие безопасности* в таблице внизу раздела.

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 внешних узлов по количеству блокировок:

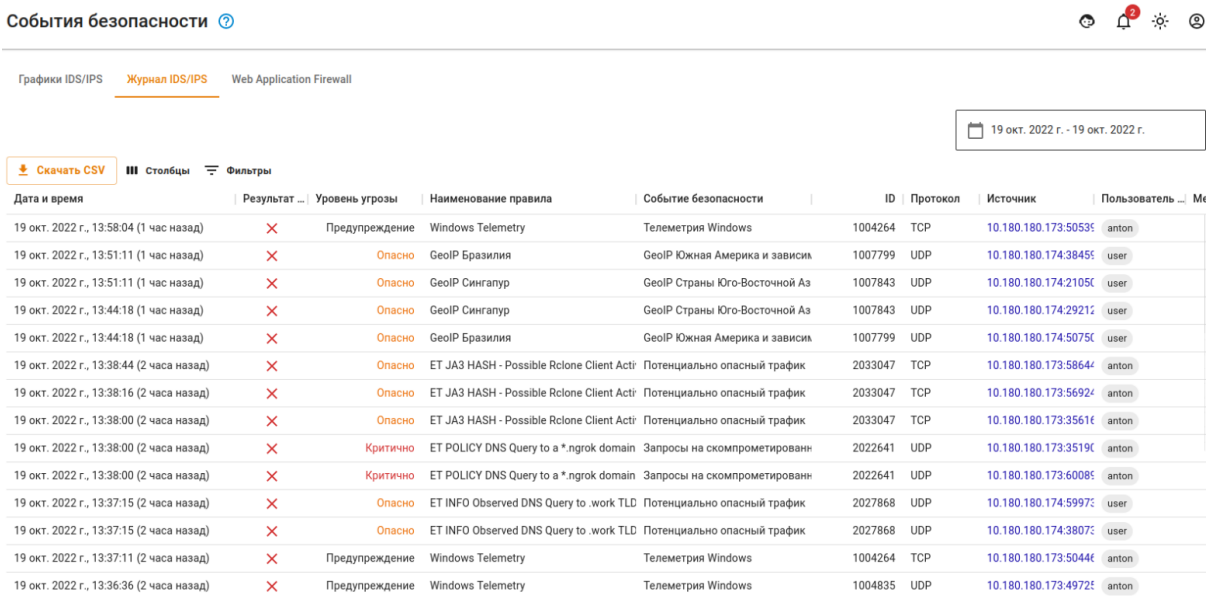
Представляет собой круговую диаграмму с внешними адресами и количеством блокировок по ним.

Топ подозрительных локальных узлов:

В топ попадают как авторизованные, так и не авторизованные пользователи, запросы которых блокировались.

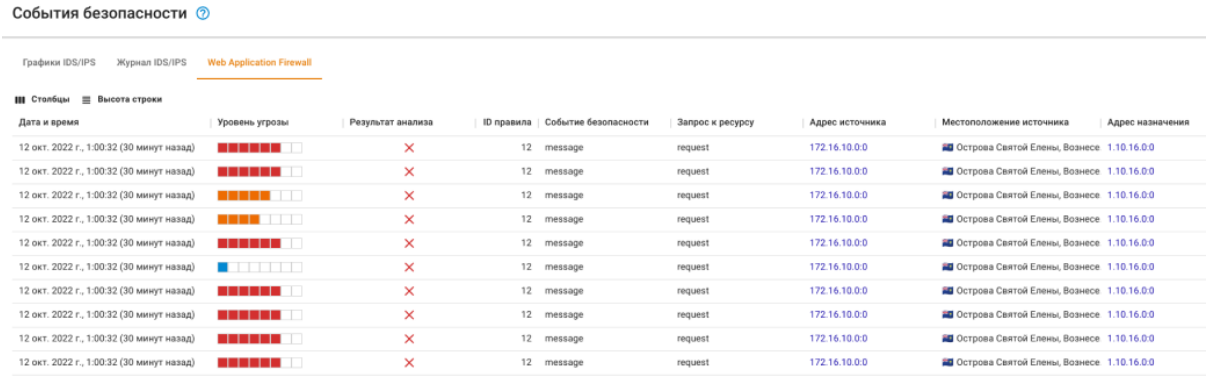
17.4.3 Журнал IDS/IPS

Содержит таблицу с информацией обо всех срабатываниях правил из раздела Предотвращение вторжений. IP-адреса в столбцах **Источник** и **Назначение** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.



17.4.4 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.

Добавление правила Web Application Firewall в исключения:

Чтобы добавить сработавшее правило WAF в исключения, выполните действия:

1. Перейдите в раздел **Управление сервером -> Терминал**.

2. В терминале перейдите в директорию `/var/opt/ideco/reverse-backend`, введя команду `cd /var/opt/ideco/reverse-backend`:

```
[admin@localhost ~]# cd /var/opt/ideco/reverse-backend
[admin@localhost reverse-backend]#
```

Если такой директории нет, создайте ее, выполнив команды:

```
mkdir /var/opt/ideco/reverse-backend
chown ideco-reverse-backend:ideco-reverse-backend /var/opt/ideco/reverse-backend
```

3. Проверьте наличие в директории `/var/opt/ideco/reverse-backend` файла `custom-waf.conf`. Для этого введите команду: `ls /var/opt/ideco/reverse-backend`. Если файл есть, он отобразится в выводе

терминала:

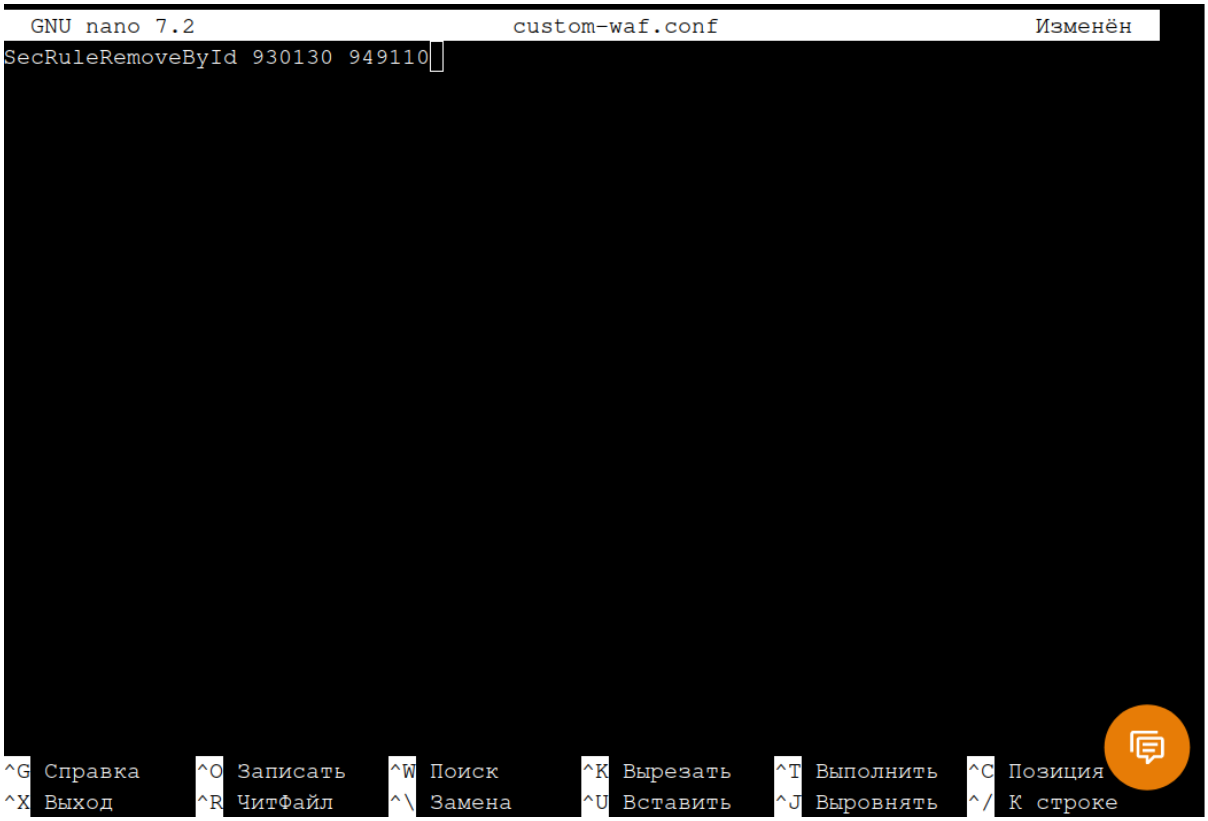
```
[admin@localhost ~]# ls /var/opt/ideco/reverse-backend
custom-waf.conf
[admin@localhost ~]#
```

Если файла нет, создайте его командами:

```
touch /var/opt/ideco/reverse-backend/custom-waf.conf
chown ideco-reverse-backend:ideco-reverse-backend /var/opt/ideco/reverse-backend/
↪custom-waf.conf
```

3. Откройте файл `custom-waf.conf` в режиме редактирования, введя команду `nano custom-waf.conf`.

4. В открывшемся файле введите `SecRuleRemoveById 930130 949110`, где `930130` и `949110` - ID сработавших правил WAF:



5. Сохраните файл, нажав **Ctrl + X**, а затем нажмите **Enter**.

6. Введите команду `sync --file-system /var/opt/ideco/reverse-backend/custom-waf.conf`, чтобы данные записались на диск.

7. Перезапустите службу, введя в терминале команду `systemctl restart ideco-reverse-backend.service`.

8. Введите в терминале команду `cat /run/ideco-reverse-backend/conf.d/modsec/main.conf`:

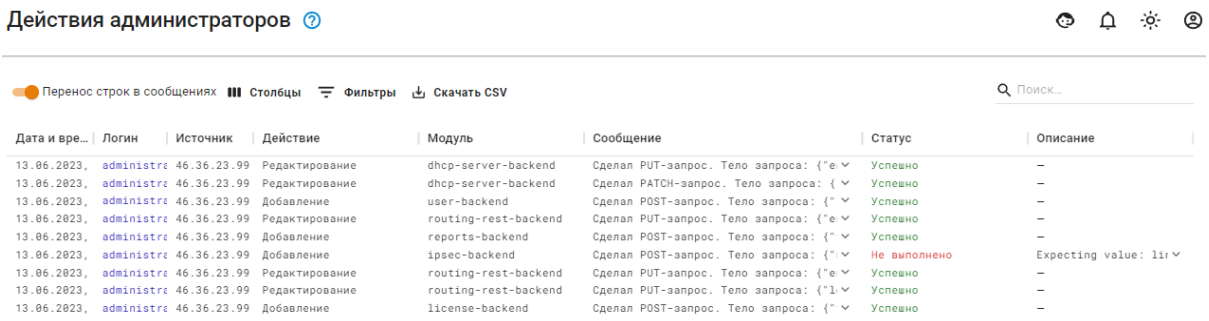
```
[admin@localhost ~]# cat /run/ideco-reverse-backend/conf.d/modsec/main.conf
# Конфиг для modsecurity объединяющий все файлы конфигураций modsecurity.
include /usr/share/modsecurity-rules/modsecurity.conf
include /usr/share/modsecurity-rules/crs-setup.conf
include /usr/share/modsecurity-rules/rules/*.conf
include /usr/share/modsecurity-rules/ideco-exclude-rules.conf
include /var/opt/ideco/reverse-backend/custom-waf.conf
[admin@localhost ~]#
```

Внесенные в файл `custom-waf.conf` исключения из правил WAF сохранятся при обновлении сервера Ideco NGFW. Создавать директорию и файл необходимо только один раз, новые исключения следует просто в него добавлять.

17.5 Действия администраторов

17.5.1 Основное

Ideco NGFW логирует действия администраторов, которые вносят изменения в конфигурацию NGFW из веб-интерфейса, локального интерфейса и терминала.

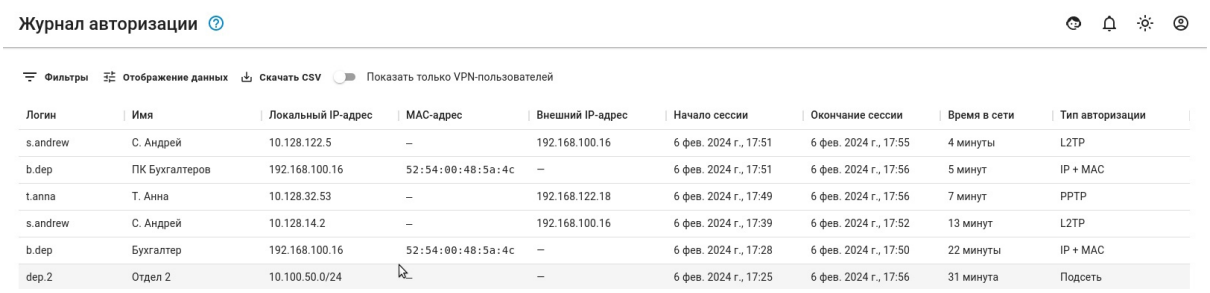


При работе Ideco NGFW в режиме *кластера* логи действия администраторов не передаются резервной ноде.

17.6 Журнал авторизации

17.6.1 Основное

Подсказка: Время хранения данных в **Журнале авторизации** составляет 180 дней.



Для поиска определенных авторизованных пользователей нажмите на **Фильтры**, укажите в поле **Столбец** требуемый параметр поиска и в последнем поле - его значение.

Особенность работы журнала авторизации:

- 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.

17.7 Конструктор отчетов

NGFW предоставляет возможность создать шаблоны отчетов и настроить их рассылку в формате .pdf на электронную почту.

17.7.1 Мои шаблоны

На этой вкладке создаются шаблоны со статистикой, которую можно просмотреть в браузере, сохранить в формате .pdf или отправить на электронную почту.

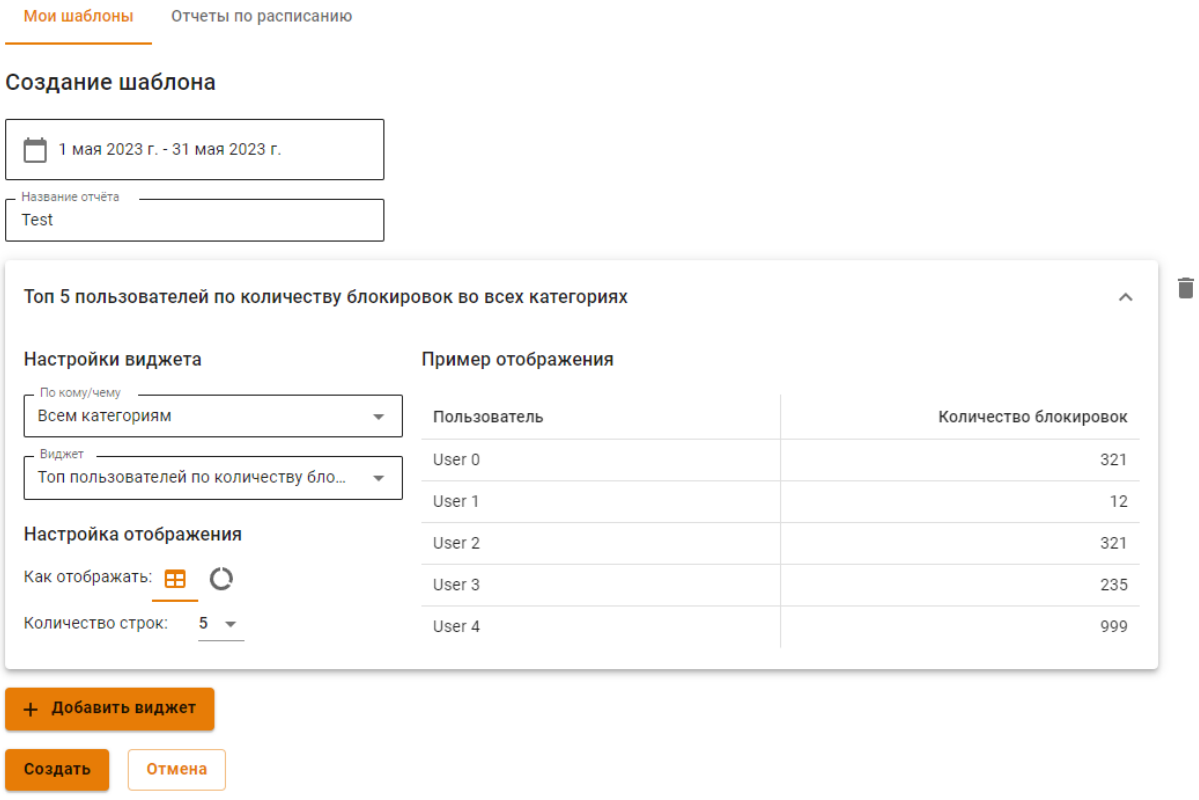
При нажатии на кнопку **Добавить** откроется меню настройки шаблона.

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 **Создать**.



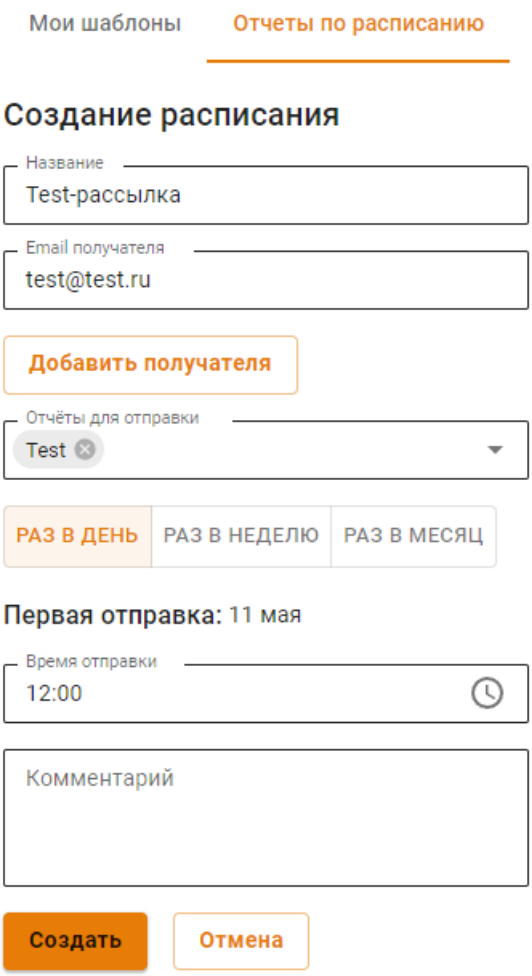
17.7.2 Отчеты по расписанию

На этой вкладке предоставлена возможность создания/редактирования настроек для отправки рассылки на электронную почту.

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 (кнопка **Добавить отчет**).

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 **Создать** 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 *Создать*.

2. Перейдите к редактированию отчета по кнопке **Редактировать** и измените настройки временного периода:

- Раз в месяц;
- Каждую вторую среду;
- Нажмите *Сохранить*.

3. ВПерейдите к редактированию отчета и выберите **Раз в месяц**. Откроются настройки, созданные в пункте 1.

Пример: Требуется настроить отправку отчета с информацией о заблокированных сайтах по всем пользователям каждое первое число месяца

Создайте шаблон отчета, на основании которого будет собрана статистика для отправки:

1. Нажмите **Добавить** во 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**

Выберите вид: таблицу или круговую диаграмму, а также количество отображаемых строк.

7. Сохраните шаблон по кнопке **Создать**.

Создайте правило, по которому будет отправляться шаблон отчета на электронную почту:

1. Нажмите **Добавить** во 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 в выпадающем списке в строке нужный шаблон.

4. Укажите настройки даты/дня и времени отправки отчета получателю.

17.8 Syslog

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

17.8.1 Пересылка системных сообщений

В качестве коллектора можно указывать любой локальный «серый» или публичный «белый» IP-адрес.

В поле **Порт** укажите любой порт из диапазона от 1 до 65535.

Подсказка: Передача системных сообщений происходит согласно RFC-5424 (транспорт UDP).

17.8.2 Расшифровка передаваемых логов

Предотвращение вторжений:

```
192.168.100.2        Dec 14␣
↪15:48:38               daemon        warning                 timestamp:2022-12-14␣
↪10:48:34.808465+00:00,flow_id:1189034483406353,in_iface:seq:Leth1:3:m,sensor_
↪name:suricata_debug,event_type:alert,src_ip:192.168.100.11,src_port:61790,src_
↪country:,src_country_code:,src_session_uuid:7100d1c8-017f-4cbf-8b78-482839300211,
↪src_user_id:2,src_user_name:a.istomina,dest_ip:192.168.100.2,dest_port:53,dest_
↪country:,dest_country_code:,dest_session_uuid:,dest_user_id:-1,dest_user_name:,
↪proto:UDP,alert.signature_id:1003892,alert.signature:Windows Telemetry,alert.
↪category:Telemetry Windows,alert.severity:3,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:73,flow.bytes_toclient:0,flow.start:2022-12-14 10:48:34.
↪808465+00:00,flow.end:2022-12-14 10:48:35.580143+00:00,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:

- **192.168.100.2** - ip-адрес NGFW отправителя;
- **Dec 14 15:48:38** - время получения события по Syslog;
- **timestamp:** 2022-12-14 10:48:34.808465+00:00 - время события в системе предотвращения вторжений, может не совпадать с временем получения события по Syslog;
- **flow_id:** 1189034483406353 - внутренний идентификатор системы предотвращения вторжений flow (сессии);
- **in_iface:** seq:Leth1:3:m - содержит идентификатор входящего интерфейса;
- **sensor_name:** suricata_debug - имя экземпляра системы предотвращения вторжений;
- **event_type:** alert - тип события;
- **src_ip:** 192.168.100.11 - IP-адрес источника;
- **src_port:** 61790 - порт источника;
- **src_country:** - название местоположения источника;
- **src_country_code:** - ISO-код страны источника;
- **src_session_uuid:** 7100d1c8-017f-4cbf-8b78-482839300211 - внутренний идентификатор сессии Ideco NGFW источника;
- **src_user_id:** 2 - идентификатор пользователя источника;
- **src_user_name:** a.istomina- имя пользователя источника;
- **dest_ip:** 192.168.100.2 - IP-адрес назначения;
- **dest_port:** 53 - порт назначения;

- **dest_country:** - название местоположения назначения;
- **dest_country_code:** - 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:** UDP - протокол;
- **alert.signature_id:** 1003892 - ID правила системы предотвращения вторжений;
- **alert.signature:** Windows Telemetry - сообщение из сработавшего правила;
- **alert.category:** Telemetry Windows - описание колонки в веб-интерфейсе События безопасности; Соответствие *alert.category:* -> *alert.signature* описаны в файле.
- **alert.severity:** 3 - уровень угрозы, может принимать значения 1, 2, 3 и 256, где 1 - самый высокий уровень угрозы;

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:** 73 - количество байт, переданное от клиента к серверу;
- **flow.bytes_toclient:** 0 - количество байт, переданное от сервера к клиенту;
- **flow.start:** 2022-12-14 10:48:34.808465+00:00 - начало;
- **flow.end:** 2022-12-14 10:48:35.580143+00:00 - 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;
- **tcp.ecn:** 0;
- **tcp.urg:** 0;
- **tcp.ack:** 0;
- **tcp.psh:** 0;
- **tcp.rst:** 0;
- **tcp.syn:** 0;
- **tcp.fin:** 0;

- **tcp.state:** - состояния сеанса TCP.

Файрвол:

```
ноя 24 09:36:27 localhost ideco-nflog[691]: UDP      src 192.168.100.12   sport 137  ␣
↪dst 40.125.122.151   dport 137   table FWD  rule  1    action accept
```

- **UDP** - протокол, принимает значения UDP, TCP, ICMP, GRE, ESP и AH;
- **src** - IP-адрес источника;
- **dst** - IP-адрес назначения;
- **sport** - порт источника для UDP и TCP;
- **dport** - порт назначения для UDP и TCP;
- **table** - таблица правил, в которой произошло логирование;
- **rule** - ID правила из таблицы *rule*;
- **action** - действие, которое произошло.

Контроль приложений:

```
192.168.100.2        Jan 12␣
↪11:00:15        1        user        err                2023-01-12T11:00:14+05:00␣
↪localhost app-control 2027 - - (flow_info_rules_was_checked) 192.168.100.11:52514 ->
↪ 192.168.100.2:53 [Amazon] = 'DROP'.
```

- **2027** - идентификатор процесса;
- **192.168.100.11:52514** - ip-адрес источника;
- **192.168.100.2:53 [Amazon]** = „DROP“ - результат анализа трафика, где *[Amazon]* название приложения, к которому был применен результат. Список всех приложений.

Контент-фильтр:

Просмотр логов доступен в веб-интерфейсе в разделе **Мониторинг -> Журналы**. Название служб для фильтрации: ideco-content-filter-backend и squid ().

Пример блокировки ресурса:

```
192.168.101.130    Mar 31 14:56:57    1    daemon    info        2023-03-
↪31T14:56:56+05:00 localhost squid 5950 - - 192.168.101.131 - - [31/Mar/
↪2023:14:56:56 +0500] "GET https://www.igromania.ru/? HTTP/1.1" 403 7455 "https://
↪yandex.ru/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101␣
↪Firefox/111.0" TCP_DENIED:HIER_NONE "Custom deny 8 Игры extended.id.21 group.id.1 "
```

- **5950** - идентификатор процесса;
- **192.168.101.131** - IP-адрес пользователя;
- **[31/Mar/2023:14:56:56 +0500] «GET https://www.igromania.ru/? HTTP/1.1**:
  - **[31/Mar/2023:14:56:56 +0500]** - дата/время события блокировки;
  - **GET** - метод;
  - **https://www.igromania.ru/?** - URL заблокированного ресурса;
  - **HTTP/1.1** - протокол;
- **403** - код состояния HTTP;
- **7455** - передано байт (в ответ, включая HTTP заголовок);
- **https://yandex.ru/** - HTTP referer;

- **Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0** - цифровой отпечаток браузера;
- **TCP_DENIED:HIER_NONE** - техническое сообщение от squid;
- **Custom deny 8 Игры extended.id.21 group.id.1**:
  - **Custom deny 8 Игры** - описание и номер правила блокировки;
  - **extended.id.21** - категория сайта;
  - **group.id.1** - значение поля **Применяется для** в сработавшем правиле.

Аутентификация через веб-интерфейс:

```
192.168.100.2        Jan 12␣
↪11:02:15        1        daemon        info                2023-01-
↪12T11:02:14+05:00 localhost fail2ban.filter 779 - - INFO [utm-web-interface] Found␣
↪192.168.100.1 - 2023-01-12 11:02:14
192.168.100.2        Jan 12␣
↪11:02:36        1        daemon        notice               2023-01-
↪12T11:02:35+05:00 localhost fail2ban.actions 779 - - NOTICE [utm-web-interface] Ban␣
↪192.168.100.1
```

- **info** или **notice** - приоритет сообщения в логах в виде информационного сообщения или уведомления;
- **779** - идентификатор процесса;
- **INFO [utm-web-interface] Found 192.168.100.1 - 2023-01-12 11:02:14** - факт обнаружения правил безопасности с указанием группы правил ([utm-web-interface]), ip-адреса и даты/времени. Список групп правил:
  - utm-dovecot;
  - utm-postfix-connrate.conf;
  - utm-postscreen-prgrt.conf;
  - utm-reverse-proxy.conf;
  - utm-roundcube.conf;
  - utm-smtp.conf;
  - utm-ssh.conf;
  - utm-two-factor-codes.conf;
  - utm-vpn-authd.conf;
  - utm-vpn-pppoe-authd.conf;
  - utm-web-interface.conf;
  - utm-wireguard-backend.conf.
- **NOTICE [utm-web-interface] Ban 192.168.100.1** - факт блокировки или разблокировки ip-адреса, где:
  - **Ban** - факт блокировки;
  - **Unban** - факт разблокировки.

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 (unit);
- `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 (unit);
- `192.168.205.254/32` - IP-адрес пользователя;
- `Sanek` - логин пользователя;
- `type 'log'` - тип авторизации через журнал безопасности AD.

Веб-авторизация:

```
2024-07-18T17:26:34+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721305594 Severity=Notice DeviceProcessName=ideco-
↪web-authd msg=User 'Sanek' has been successfully authorized in web interface from␣
↪IP '192.168.205.254'.
```

- `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 (unit);
- `Sanek` - логин пользователя;
- `192.168.205.254` - IP-адрес пользователя;

Авторизация по IP:

```
2024-07-18T17:29:18+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721305758 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.205.254/32 is authorized as user 'Sanek'.␣
↪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 (unit);
- `192.168.205.254/32` - IP-адрес пользователя;
- `Sanek` - логин пользователя;
- `type 'ip'` - тип авторизации по IP.

Авторизация по MAC:

```
2024-07-18T17:32:26+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721305946 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.205.254/32 is authorized as user 'Sanek'.␣
↪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 (unit);
- `192.168.205.254/32` - IP-адрес пользователя;
- `Sanek` - логин пользователя;
- `type 'mac'` - тип авторизации по MAC.

Авторизация по подсети:

```
2024-07-18T20:52:27+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721317947 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.205.0/24 is authorized as user 'Sanek'. 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 (unit);
- `192.168.205.0/24` - подсеть, по которой происходит авторизация;
- `Sanek` - логин пользователя;
- `type 'net'` - тип авторизации по подсети.

Подключение по VPN:

```
192.168.100.2        Jan 12␣
↪11:10:06        1        local0        info                2023-01-
↪12T11:10:05+05:00 localhost ideco-vpn-authd 1356 - - Start vpn authorization ('user_
↪1', '192.168.100.11', 'pptp').
192.168.100.2        Jan 12␣
↪11:10:06        1        local0        info                2023-01-
↪12T11:10:05+05:00 localhost ideco-vpn-authd 1356 - - Subnet 10.128.187.17/32 is␣
↪authorized as user 'user_1'. Connection made from '192.168.100.11', type 'pptp'.
```

- **1356** - идентификатор процесса;
- **Start vpn authorization**(„user_1“, „192.168.100.11“, „pptp“) - факт запроса на авторизацию с информацией о запрашиваемом подключении, где:
  - **user_1** - логин пользователя;
  - **192.168.100.11** - ip-адрес, откуда установлено подключение;
  - **pptp** - протокол.
- **Subnet 10.128.187.17/32** - факт успешной авторизации с локальным ip-адресом.

Веб-авторизация:

```
192.168.100.2        Jan 12␣
↪11:20:06        1        local0        info                2023-01-
↪12T11:20:05+05:00 ideco-ngfw ideco-web-authd 1665 - - Subnet 192.168.100.10/32 is␣
↪authorized as user 'user'. Connection made from None, type 'web'
```

- 1665 - идентификатор процесса;
- 192.168.100.10/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'web' - тип авторизации веб.

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'.
```

- Ideco-NGFW - название сервера;
- 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'.
```

- Ideco-NGFW - название сервера;
- 192.168.205.254/32 - IP-адрес пользователя;
- Sanek - логин пользователя;
- type 'log' - тип авторизации через журнал безопасности AD.

Авторизация по IP:

```
192.168.100.2        Jan 12␣
↪11:20:06        1        local0        info                2023-01-
↪12T11:20:05+05:00 ideco-ngfw ideco-web-authd 1665 - - Subnet 192.168.100.49/32 is␣
↪authorized as user 'user-1717140295.828113'. Connection made from None, type 'ip_
↪permanent'.
```

- 1665 - идентификатор процесса;
- 192.168.100.49/32 - IP-адрес пользователя;
- 'user-1717140295.828113' - логин пользователя;
- type 'ip_permanent' - тип авторизации IP с постоянной авторизацией.

Авторизация по MAC:

```
192.168.100.2        Jan 12␣
↪11:20:06        1        local0        info                2023-01-
↪12T11:20:05+05:00 ideco-ngfw ideco-auth-backend 3660 - - Subnet 192.168.100.10/32␣
↪is authorized as user 'user'. Connection made from None, type 'mac'.
```

- 3660 - идентификатор процесса;
- 192.168.100.10/32 - IP-адрес пользователя;
- user - логин пользователя;

- `type 'mac'` - тип авторизации MAC.

Авторизация по подсетям:

```
192.168.100.2        Jan 12␣
↪11:20:06        1        local0        info                2023-01-
↪12T11:20:05+05:00 ideco-ngfw ideco-auth-backend 3660 - - Subnet 192.168.100.0/24 is␣
↪authorized as user 'user'. Connection made from None, type 'net'.
```

- `3660` - идентификатор процесса;
- `192.168.100.0/24` - подсеть пользователя;
- `user` - логин пользователя;
- `type 'net'` - тип авторизации подсеть.

18. Управление сервером

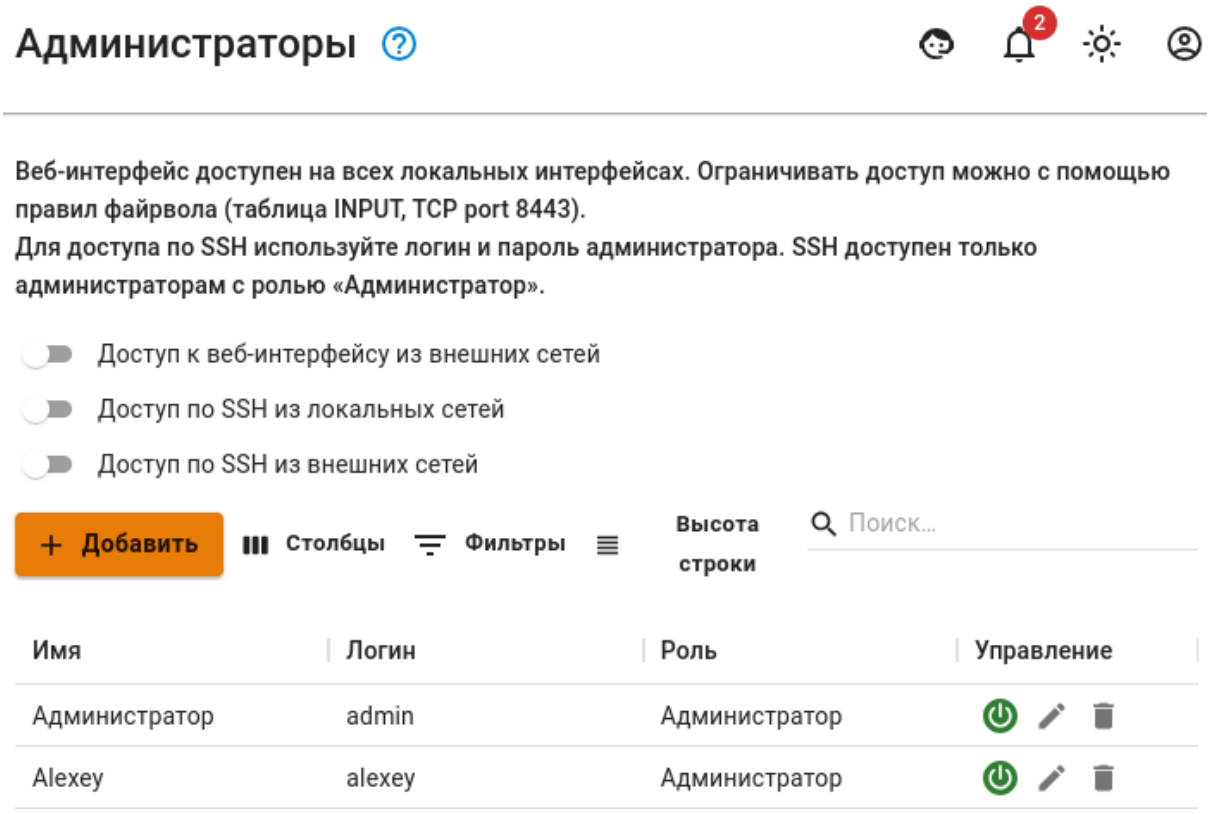
18.1 Администраторы

18.1.1 Управление администраторами

Существует возможность задать учетные данные нескольких администраторов сервера Ideco NGFW для доступа к веб-интерфейсам настроек.

Предустановленную запись администратора нельзя удалить, можно только сменить ее данные - имя и пароль - с помощью соответствующих элементов в столбце **Управление**.

Создать дополнительных администраторов сервера и управлять учетными записями можно в разделе **Управление сервером -> Администраторы**.



Чтобы добавить нового администратора, нажмите кнопку **Добавить** и заполните следующие поля:

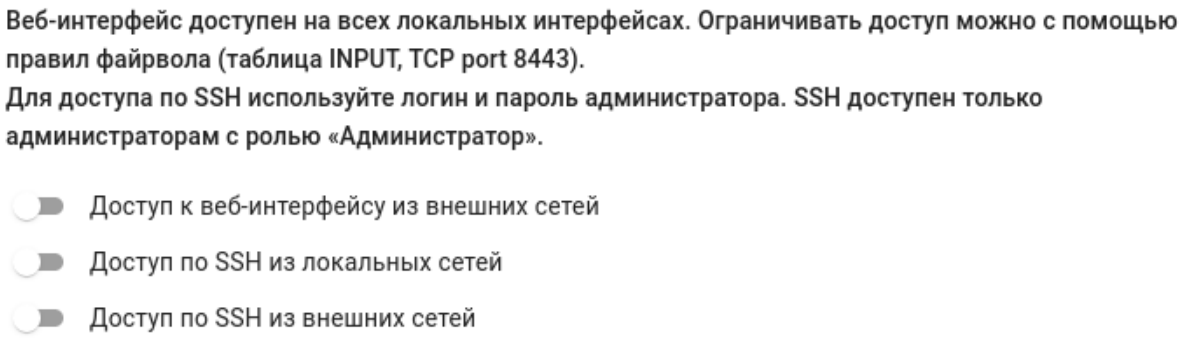
- **Имя** - введите имя нового администратора. Значение не должно быть длиннее 42 символов;
- **Логин** - введите логин нового администратора. Значение не должно быть длиннее 42 символов;
- **Пароль/повторите пароль** - введите пароль нового администратора. Значение не должно быть короче 10 символов. Рекомендуем использовать сложные пароли, содержащие латинские строчные и заглавные буквы, цифры и специальные символы;

Роль - выберите роль::

- **Администратор** - получает полный доступ к настройке NGFW;
- **Только просмотр** - администратор не сможет производить никаких настроек в веб-интерфейсе, так как при попытке внесения изменений будет появляться окно с ошибкой **Доступ запрещен**;
- **Просмотр отчетов** - администратору будет доступна часть раздела *Отчеты и журналы*, а именно Трафик, Журнал событий, Журнал веб-доступа, События безопасности и Журнал авторизации;
- **Создание отчетов** - администратору будет доступна часть раздела *Отчеты и журналы*, а именно Трафик, Журнал событий, Журнал веб-доступа, События безопасности, Журнал авторизации и Конструктор отчетов.

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

- Для включения доступа из внешней сети переключите ползунок в положение **Включен** около пункта **Доступ к веб-интерфейсу из внешней сети**. Эта функция помогает заниматься администрированием Ideco NGFW удаленно;
- Для включения доступа к серверу по SSH из локальной или внешних сетей переключите ползунок в положение **Включен** около соответствующих пунктов (не рекомендуется). Доступ осуществляется по 22 TCP-порту. Попытки подбора паролей блокируются автоматически. Используйте команду **ideco-local-menu –debug** для запуска меню.



Подробнее о настройке подключения к веб-интерфейсу при удаленном доступе смотрите в статье *Удаленный доступ для управления сервером*.

18.1.3 Восстановление пароля администратора

Подробнее о восстановлении пароля администратора смотрите в статье по *ссылке*.

18.2 Центральная консоль

Подсказка: Название службы раздела **Центральная консоль**: `ideco-central-console-backend`. Список служб для других разделов доступен по *ссылке*.

Ideco Center - это центральная консоль, которая поможет в администрировании сразу 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:

- Создание правил политик безопасности (файрвол, контроль приложений, контент-фильтр) и объектов, которые переносятся в подключенные сервера Ideco NGFW одновременно;
- Создание пользовательских категорий контент-фильтра;
- Переход из Ideco Center в веб-интерфейс подключенных Ideco NGFW;
- Обновление подключенных к Ideco Center NGFW;
- Управление правами доступа администраторов. При этом администраторы Ideco Center имеют доступ к подключенными NGFW, а администраторы подключенных NGFW не имеют доступ к Ideco Center.

Подробнее о работе политик безопасности и объектов в статье *Политики и объекты*.

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. Поддерживаются Realtek, D-Link и другие.
Гипервизоры	VMware, Microsoft Hyper-V (2-го поколения), VirtualBox, KVM, Citrix XenServer.
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.

Файл для установки центральной консоли доступен для скачивания в личном кабинете. Процесс установки Ideco Center аналогичен *процессу установки Ideco NGFW*.

Источники обновления данных для Ideco Center:

Ideco Center получает обновления из следующих источников:

- Отсылка уведомлений в личный кабинет/телеграм-бот: alerts.v16.ideco.dev;
- Обновление баз **Контент-фильтра**: content-filter.v16.ideco.dev;

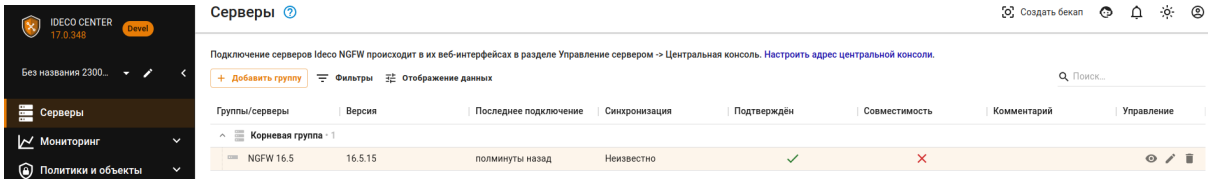
- Отсылка анонимной статистики: gatherstat.v16.ideco.dev;
- Обновления баз GeoIP: ip-list.v16.ideco.dev;
- Отправка отчетов по почте: send-reports.v16.ideco.dev;
- Обновления системы: sysupdate.v16.ideco.dev;
- Синхронизация времени: ntp.ideco.ru.

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.

18.2.1 Подключение Ideco NGFW к Ideco Center

Подсказка: 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:



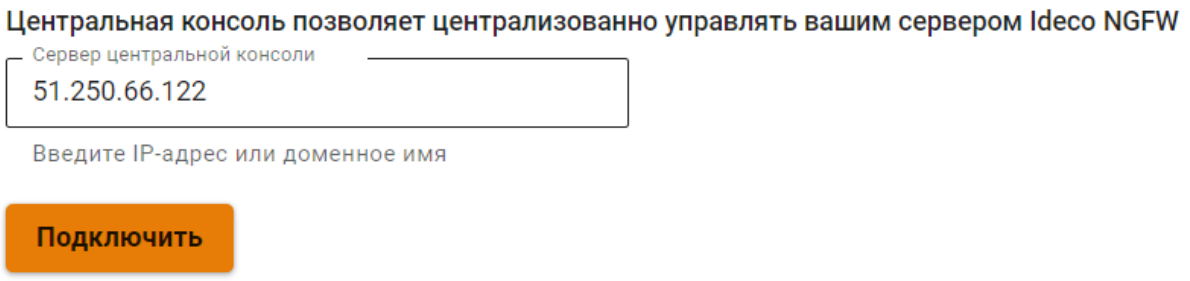
Подсказка: Если в подключаемом Ideco NGFW используется кластер, достаточно подключить только активную ноду, пассивная автоматически примет эту настройку.

Сетевое подключение производится в направлении от Ideco NGFW к Ideco Center, т. е. возможна связь и когда Ideco NGFW за NAT.

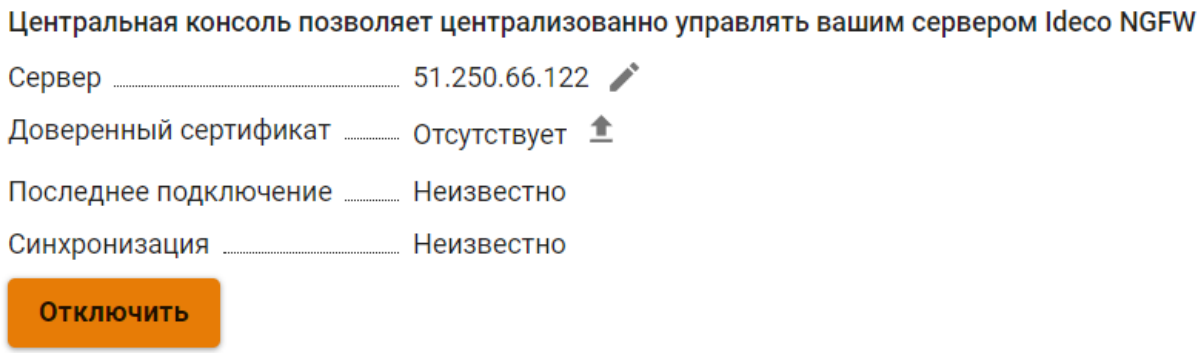
Для подключения Ideco NGFW к Ideco Center:

1. Перейдите в раздел **Управление сервером -> Центральная консоль**;

2. Введите IP-адрес или доменное имя в строке **Сервер центральной консоли** и нажмите **Подключить**:

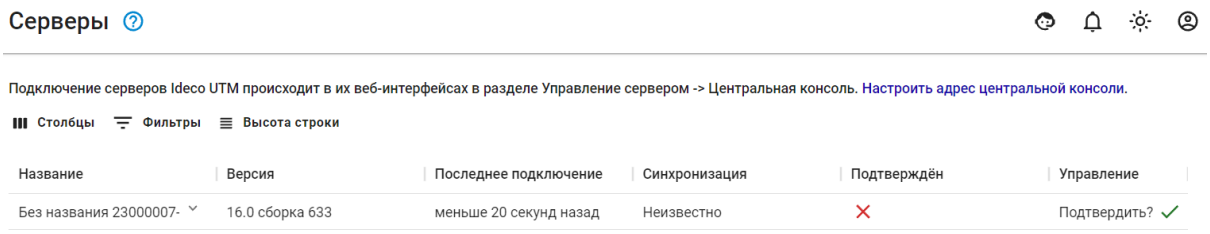


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW:



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

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



Подсказка: Если сервер Ideco Center находится за NAT, укажите IP-адрес или доменное имя в разделе **Управление сервером -> Дополнительно -> Адрес центральной консоли**.

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:

Проброс портов для подключения нескольких Ideco NGFW к Ideco Center осуществляется при отсутствии VPN-подключения между офисами. В этом случае вместо подключения по IPsec настраивается перенаправление портов. Для настройки нужно создать правило DNAT в веб-интерфейсе Ideco NGFW, через который Ideco Center выходит в интернет:

Протокол
UDP

Источник

Инвертировать источник

Источник
Любой

Зона источника
Любой

Назначение

Инвертировать назначение

Назначение
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

Время действия
Любой

Комментарий

0/256

Сохранить 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.

Удаление сервера Ideco NGFW из Ideco Center разорвет привязку в интерфейсе Ideco NGFW:

Для этого в таблице **Серверы** в столбце **Управление** напротив нужного сервера выберите  и подтвердите выбор.

Предупреждение: При подключении к Ideco Center сервера, настройки которого *восстановлены* из бекапа другого сервера, такой клон не появится в таблице серверов Ideco Center. Возникает конфликт с донором резервной копии из-за одинакового claster_id.

В случае возникновения такой проблемы обратитесь в *Техническую поддержку*.

18.2.2 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: Для обновления серверов, подключенных к центральной консоли, перейдите в интерфейс NGFW одним из указанных выше способов и воспользуйтесь статьей *Автоматическое обновление сервера*.

18.2.3 Установка

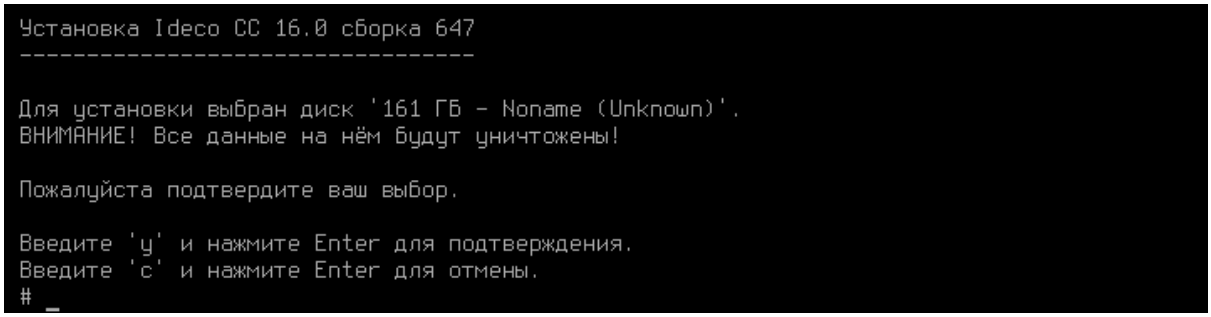
Процесс установки

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

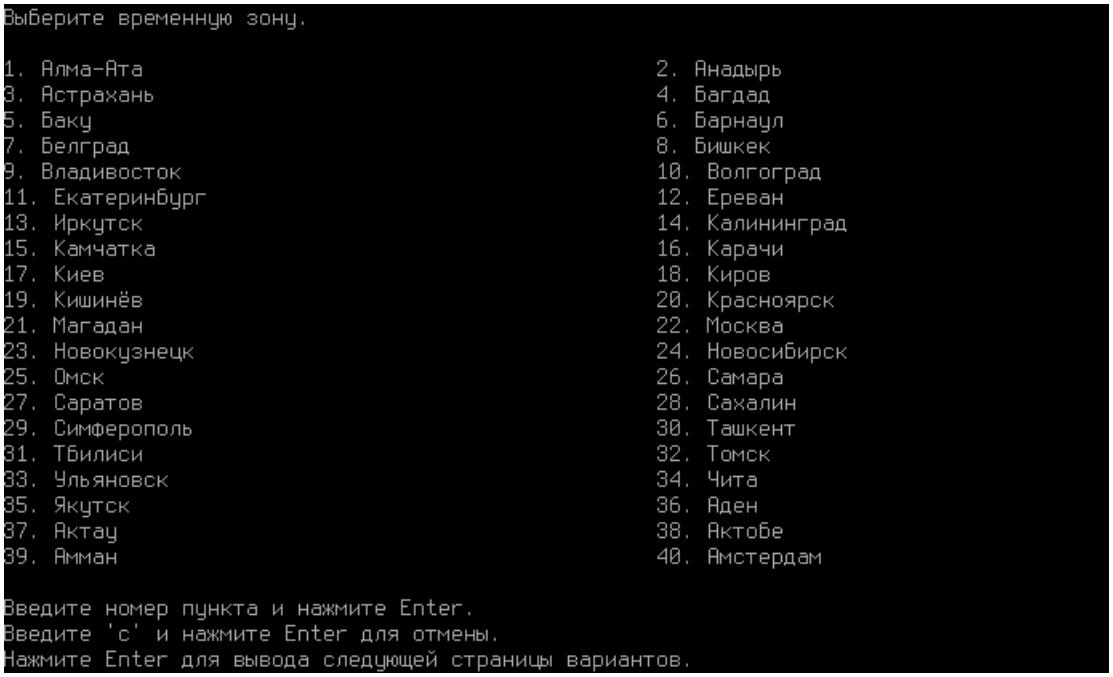
Для установки Ideco Center выполните действия:

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

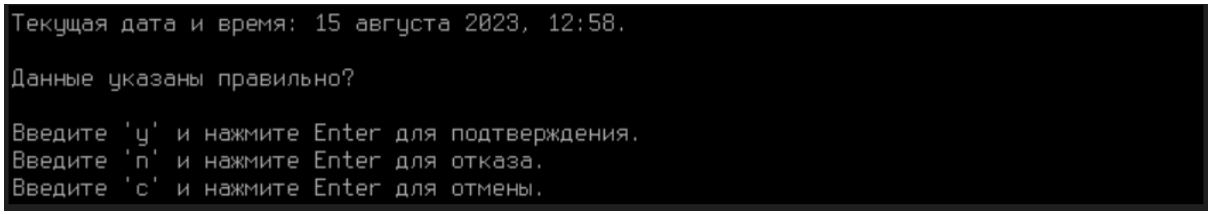
2. Выберите диск для установки и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой вы находитесь:



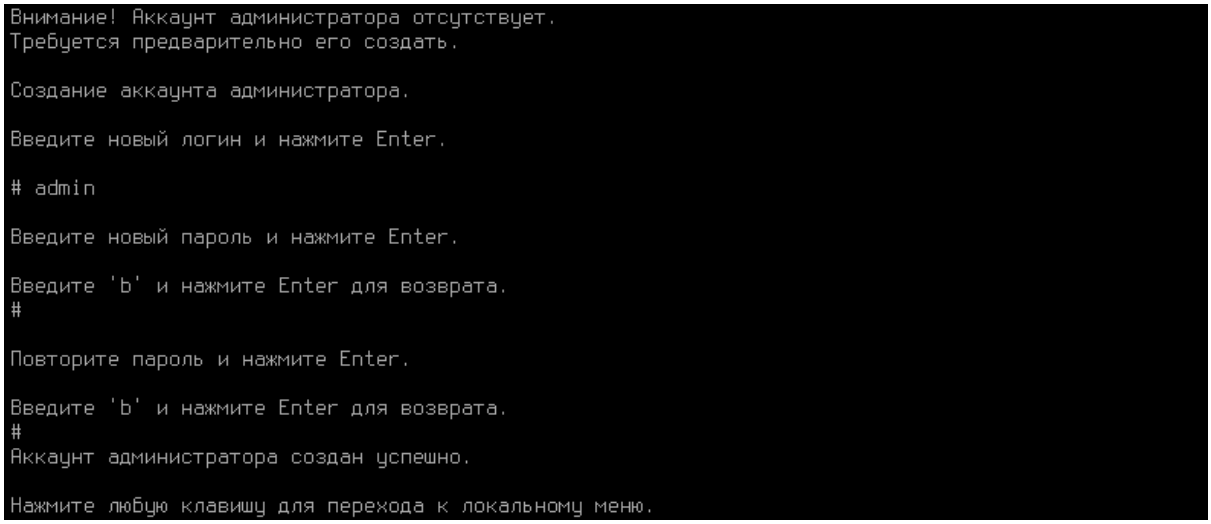
4. Настройте дату и время в соответствии с вашей временной зоной. **Обязательно проверьте правильность даты и времени**:



Подсказка: Не забудьте извлечь USB диск после установки Ideco Center, чтобы загрузка с USB диска не началась заново.

Создание учетной записи администратора

Для входа в веб-интерфейс Ideco CC нужно создать учетную запись администратора с соблюдением требований к паролю:



Требования к паролю:

- **Минимальная длина пароля** - 12 символов;
- **Содержит только 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.

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 под локальный интерфейс:

```
Внимание! Не найдено ни одного настроенного локального
сетевого интерфейса. Его необходимо настроить для доступа
к web-интерфейсу управления сервером.


Выберите сетевую карту.

1. 00:15:5d:a9:ac:0f Microsoft Hyper-V Virtual Ethernet Adapter (Link N/A)
2. 00:15:5d:a9:ac:10 Microsoft Hyper-V Virtual Ethernet Adapter (Link N/A)

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

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

```
 Настроить локальную сеть автоматически через DHCP?

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

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

```
Введите IP/префикс и нажмите Enter.

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

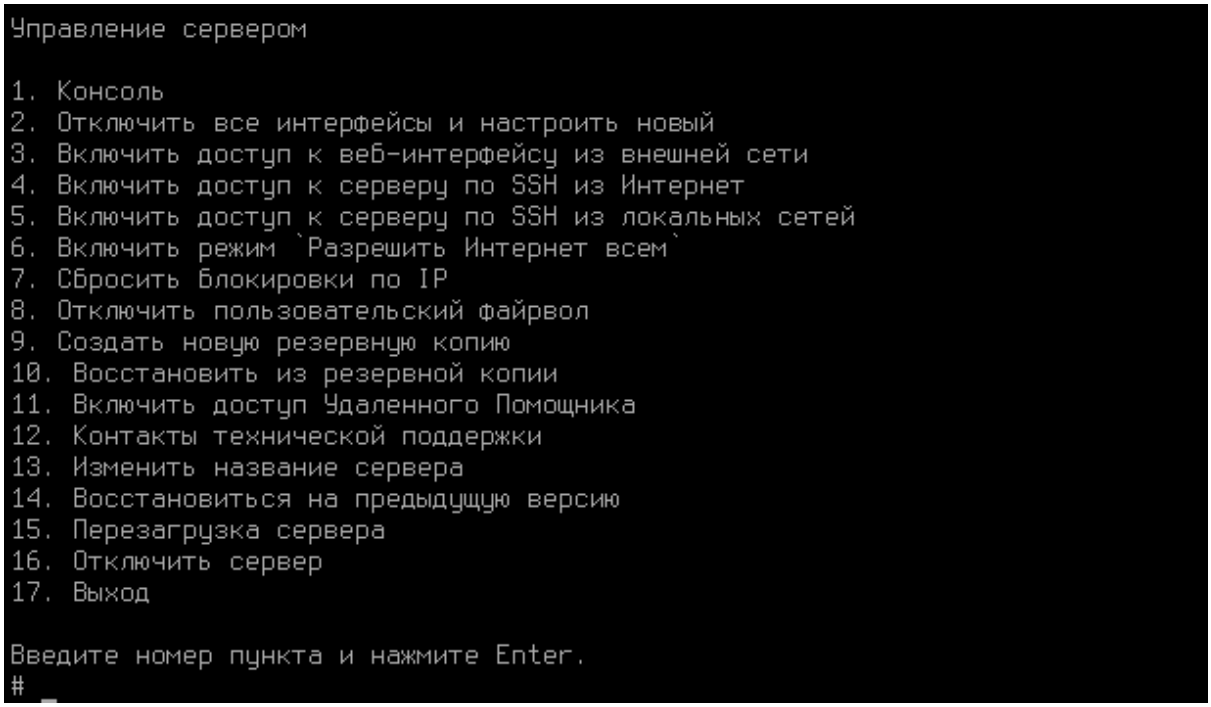
4. Введите адрес шлюза или оставьте поле пустым:

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

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

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:



18.2.4 Политики и объекты

Основное

Управляйте объектами и правилами на всех подключенных Ideco NGFW одновременно.

Принцип работы разделов **Файрвол**, **Контроль приложений**, **Контент-фильтр** и **Ограничение скорости** одинаков и описан в статье *Политики безопасности* на примере раздела **Файрвол**.

В разделе **Контент-фильтр** реализована возможность создать пользовательские категории на одноименной вкладке и использовать их для создания правил контентной фильтрации.

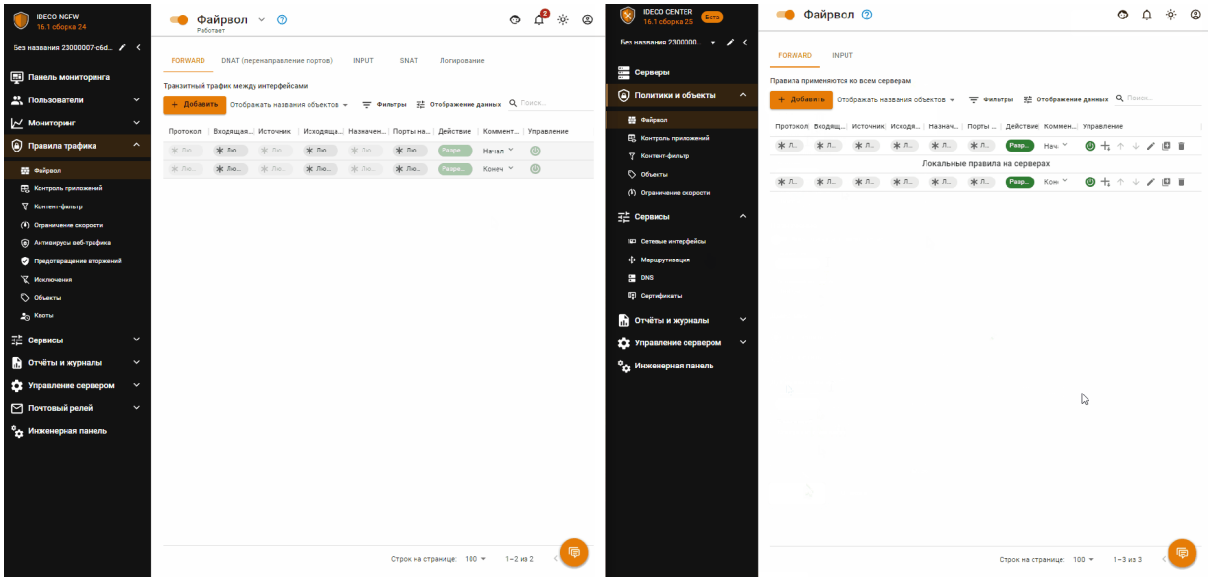
Политики безопасности

Принципы работы разделов **Файрвол**, **Контроль приложений**, **Контент-фильтр** и **Ограничение скорости** с подключенными NGFW идентичен. Рассмотрим его на примере раздела **Файрвол**.

Файрвол

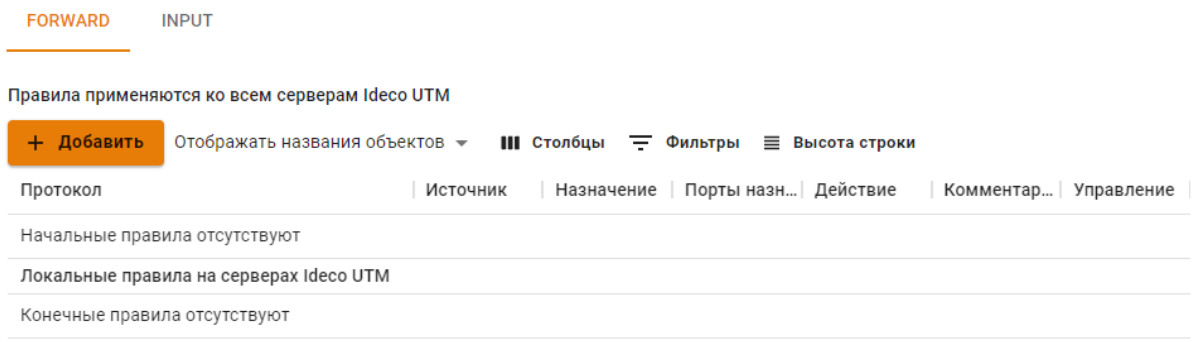
Файрвол Ideco Center содержит только таблицы FORWARD и INPUT.

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

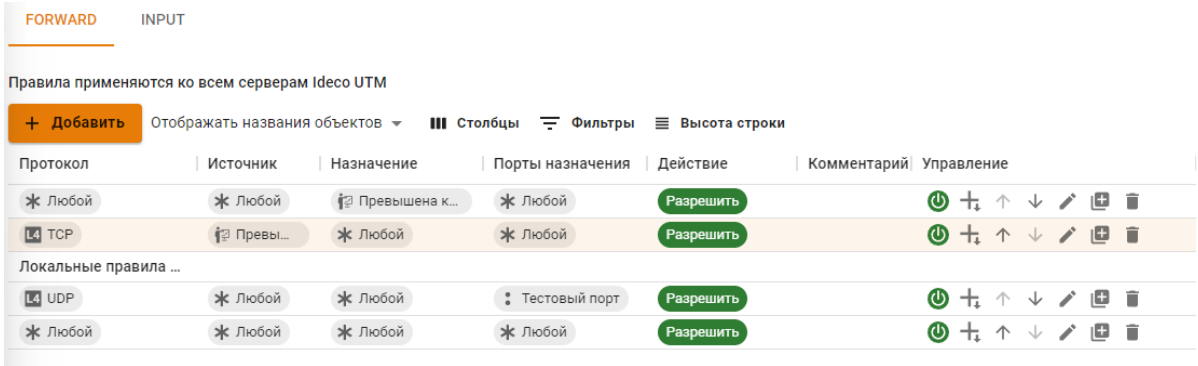


В Ideco Center Созданные в Ideco Center правила Forward отображаются в виде двух таблиц: **Начальные правила** и **Конечные правила**. Эти таблицы разделяют **Локальные правила на серверах Ideco NGFW**.

Пример незаполненной таблицы:



Пример заполненной таблицы:



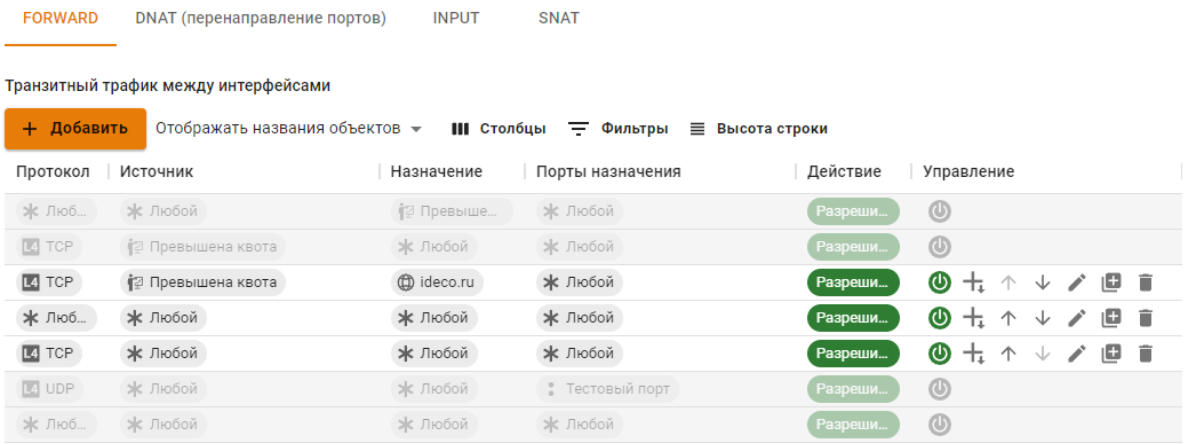
Подсказка: Локальные правила на серверах Ideco NGFW не видны в интерфейсе Ideco Center.

Для просмотра перейдите в раздел **Серверы**, нажмите на в строке с нужным Ideco NGFW и перейдите в раздел **Файрвол**.

Чтобы созданное правило попало в таблицу **Начальные правила**, укажите в строке **Вид правила** значение **Начальный**. Если правило требуется разместить в таблице **Конечные правила**, выберите значение **Конечный**.

Предупреждение: Перемещать правила между таблицами **Начальные правила** и **Конечные правила** нельзя.

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**.

Средняя часть создается администратором NGFW в самом NGFW и не видна в интерфейсе Ideco Center.

Объекты

Основное

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*.

18.2.5 Сервисы

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 несколько IP-адресов, если это требуется. Требуется указать минимум один IP-адрес;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS сервера (необязательно).

Маршрутизация

Маршрутизация работает аналогично маршрутизации Ideco NGFW. Подробное описание по *ссылке*.

DNS

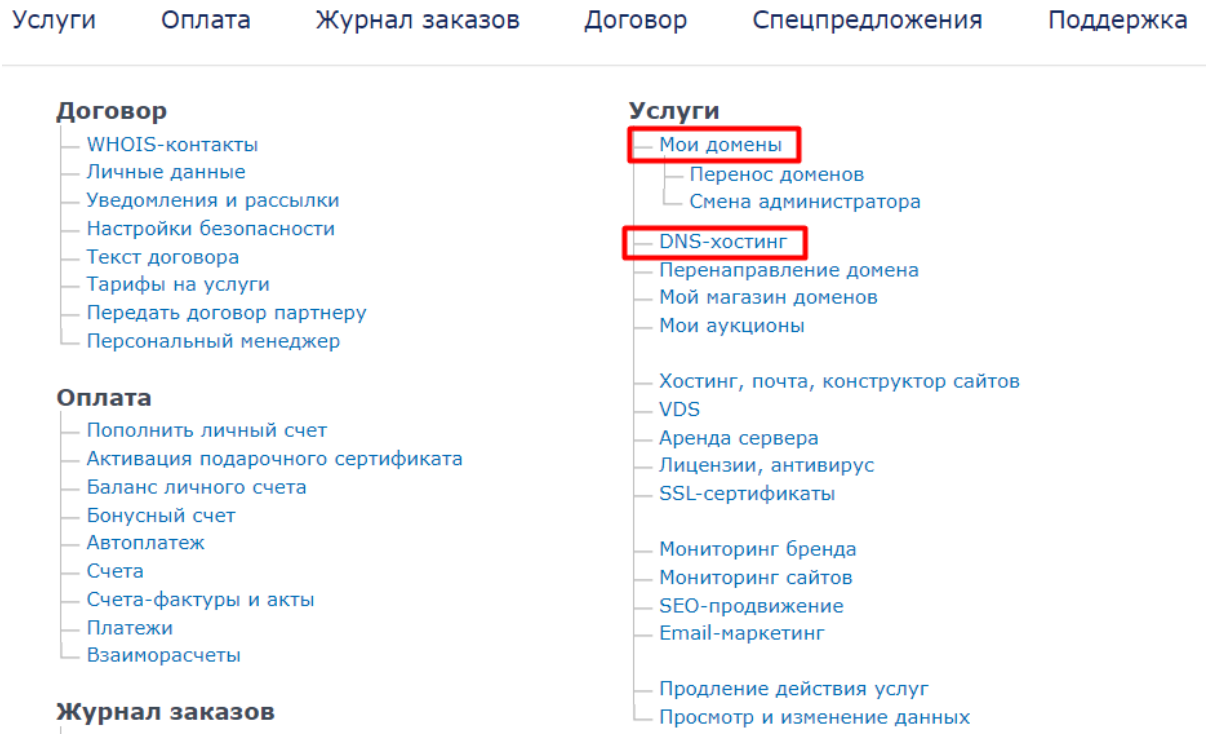
Принцип работы DNS в Ideco Center, аналогичный принципу работы *Внешних DNS-серверов* в Ideco NGFW. Если вышестоящий роутер перехватывает DNS-запросы Ideco Center, то добавьте внешние DNS-сервера.

DDNS

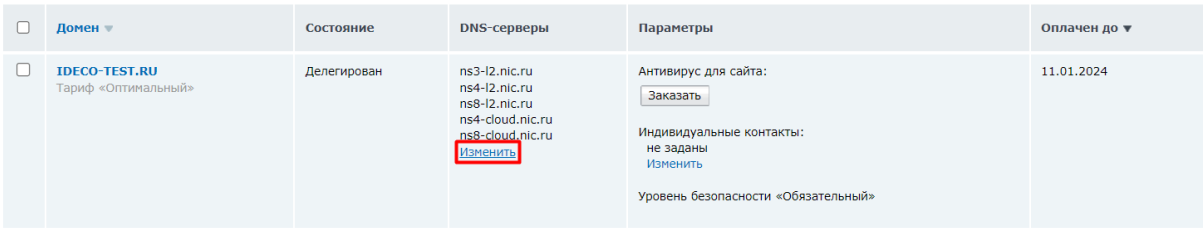
DDNS в Ideco NGFW реализован через интеграцию с хостингом RU-CENTER. Поэтому перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.
Для решения вопросов по работе с хостингом воспользуйтесь страницей помощи.

Настройка DDNS

1. После входа в личный кабинет RU-CENTER откроется страница Для клиентов. Для дальнейшей работы откройте два раздела - **Мои домены** и **DNS-хостинг**:



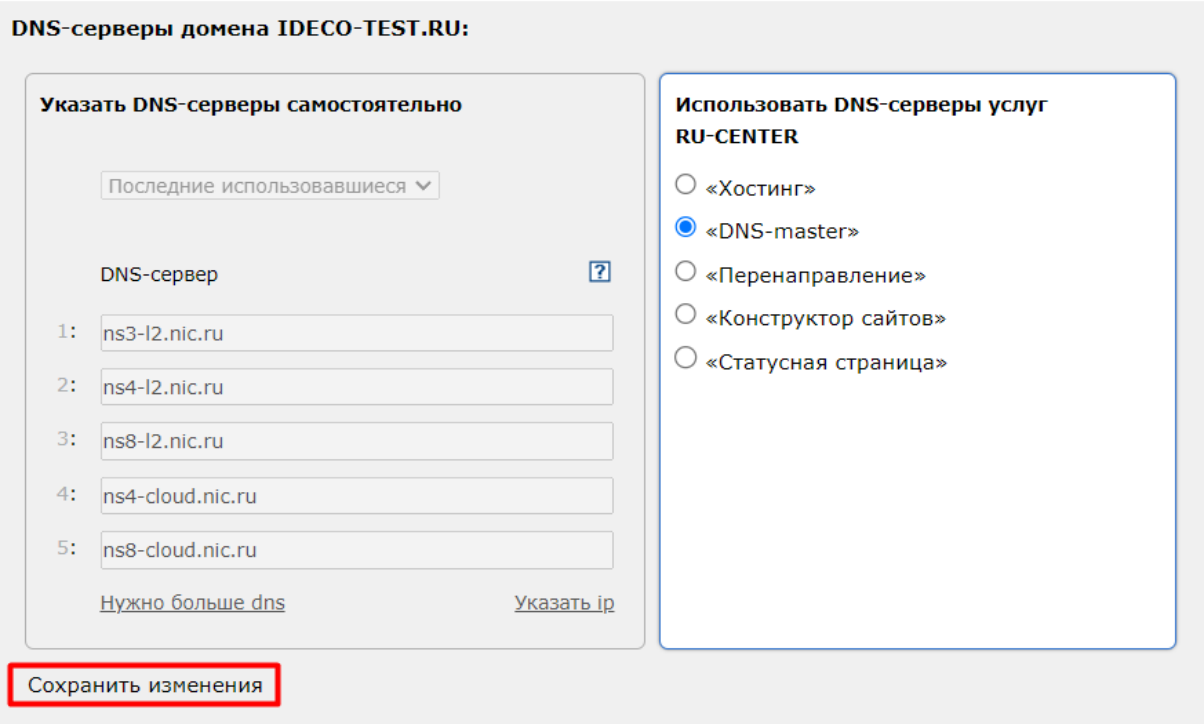
2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:



3. Делегируйте домен, настроив DNS-серверы:

- Если приобрели домен на RU-CENTER, выберите **DNS-master**;
- Если приобрели домен на сторонних ресурсах, откройте настройки домена и укажите DNS-серверы с nic.ru

Сохраните изменения:



Домен будет делегирован с заданным списком DNS-серверов. Это может занять нескольких часов.

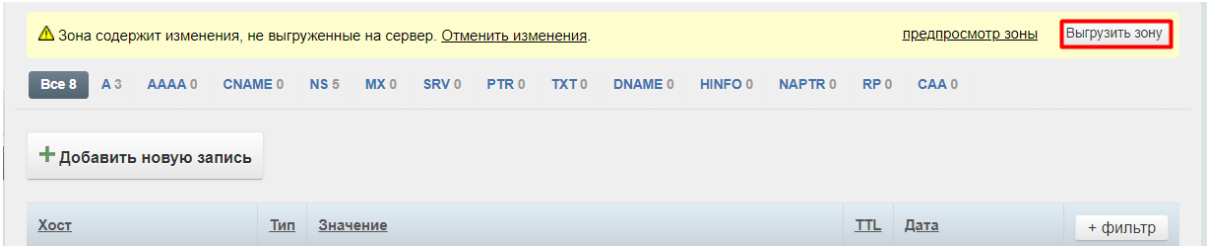
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

5. Выберите нужный домен или добавьте, нажав соответствующую кнопку.

6. Добавьте две записи по кнопке **Добавить новую запись**:

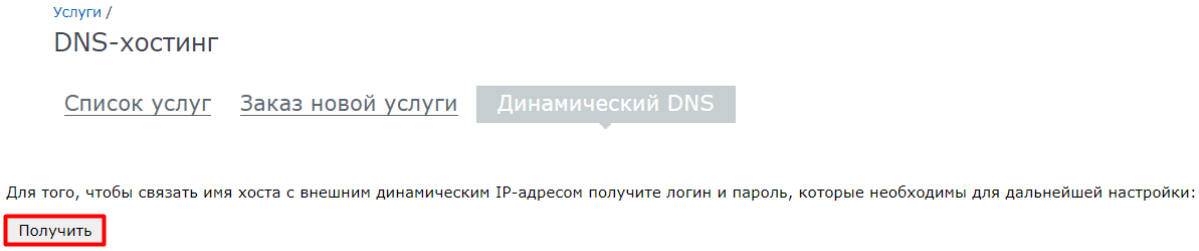
- Первая запись:
  - Name - укажите знак `@`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco Center (указывается в разделе *Техническая поддержка -> Информация для технической поддержки*);
  - TTL - оставьте не заполненным.
- Вторая запись:
  - Name - укажите `www`;
  - Type - выберите тип `A`;
  - IP address - текущий IP-адрес Ideco Center;
  - TTL - оставьте не заполненным.

7. Нажмите кнопку **Выгрузить зону**:



8. Перейдите в раздел **DDNS** в Ideco Center 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 над этими полями и нажмите **Получить**:



9. Сохраните настройки в Ideco Center, нажав **Сохранить**.

Сертификаты

Общая информация

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

Для просмотра основной информации о сертификате нажмите кнопку .

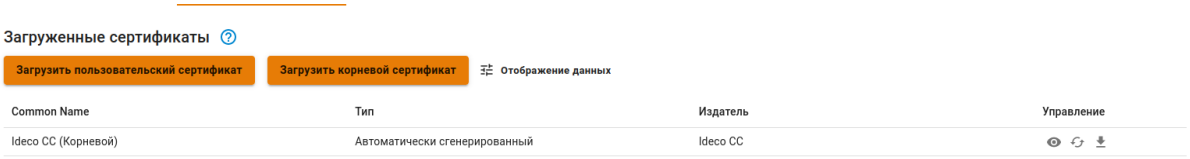
Действующие сертификаты

В таблице *Действующие сертификаты* отображаются:

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

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 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*.

Логика работы

Ideco Center 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 Ideco Center корневой (самоподписанный) сертификат генерируется автоматически. Скачать автоматически сгенерированный Ideco Center самоподписанный корневой сертификат можно, нажав на .

Пользовательские сертификаты - любые сертификаты на домен. Могут быть как подписанными корпоративным корневым сертификатом, так и выданными Certificate Authority (CA) или Центрами сертификации. Ideco Center автоматически генерирует и подписывает сертификаты на домены, которые вы указываете для модулей.

Процесс выпуска сертификата

Чтобы выпустить сертификат, Ideco Center выполняет 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;

3. При успешном выпуске цепочки сертификатов Let's Encrypt она заменит локальную цепочку;

4. Если выпуск цепочки сертификатов Let's Encrypt завершился неудачей, продолжит использовать локальную цепочку сертификатов.

Если требуется повторить попытку получения сертификата Let's Encrypt вместо самоподписанного, то нужно нажать на кнопку **Перевыпустить** в столбце **Управление**.

Сертификат Let's Encrypt **выпускается на 3 месяца** и будет **автоматически перевыпущен** по окончании срока действия.

С 17 версии Ideco Center автоматически сгенерированные Ideco Center 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**. Ideco Center попробует 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 Center 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**. Ideco Center заменит ее на автоматически сгенерированный корневой сертификат.

Внимание: Проверить, что срок действия загруженного пользовательского или сгенерированного Ideco Center 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 Ideco Center, нажав на .

Для проверки перевыпуска сертификата и нового срока его действия нажмите на .

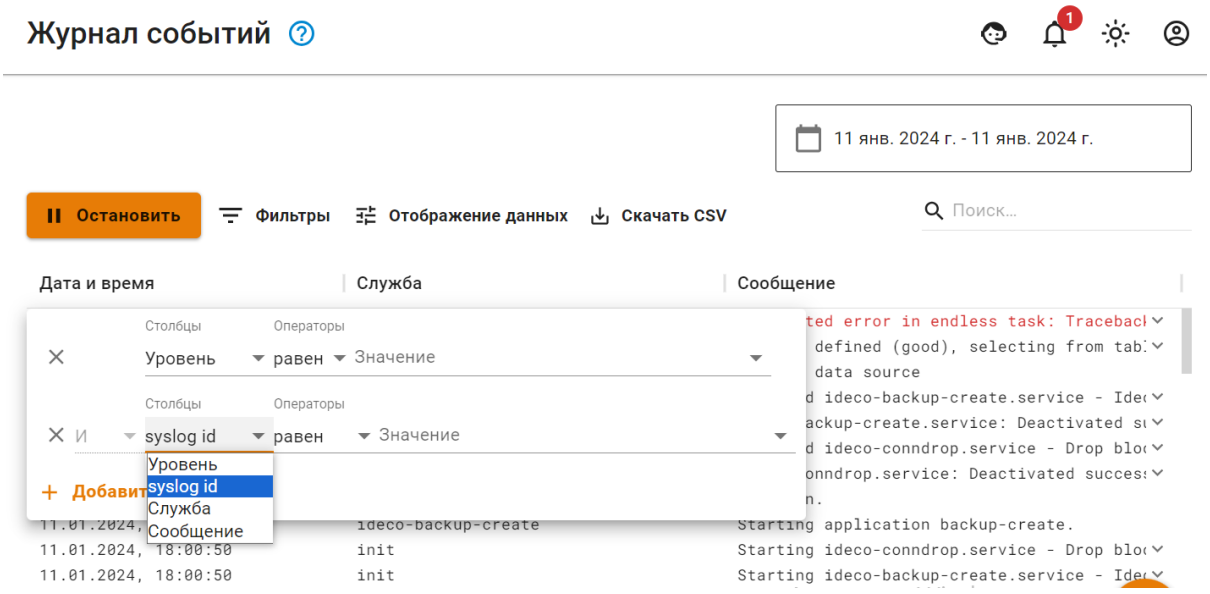
18.2.6 Отчеты и журналы

Основное

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:



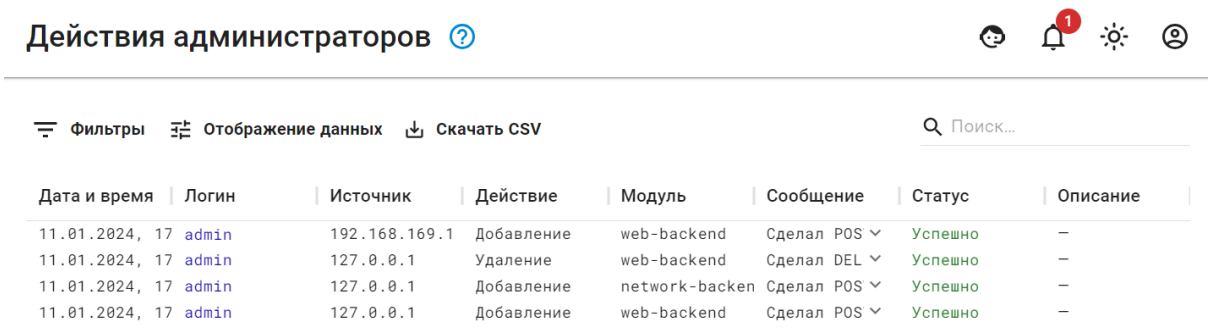
Подсказка: По кнопке **Скачать CSV** сохраняются те строки логов, которые заданы фильтрацией.

Список служб, доступных в разделе:

- **Файрвол** - ideco-firewall-backend, ideco-nflog;
- **Контроль приложений** - ideco-app-backend, ideco-app-control@Leth<номер локального интерфейса>;
- **Контент-фильтр** - ideco-content-filter-backend;
- **Ограничение скорости** - ideco-shaper-backend;
- **Объекты** - ideco-alias-backend;
- **Сетевые интерфейсы** - ideco-network-backend, ideco-network-nic;
- **Маршрутизация** - ideco-routing-backend;
- **DNS** - ideco-dns-backend, unbound;
- **DDNS** - ideco-dns-backend;
- **Автоматическое обновление** - ideco-sysupdate-backend;
- **Резервное копирование** - ideco-backup-backend, ideco-backup-create, ideco-backup-rotate;
- **Лицензия** - ideco-license-backend;
- **Syslog** - ideco-monitor-backend.

Основное

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



18.2.7 Управление сервером

В центральной консоли (далее Ideco Center) разделы *Автоматическое обновление*, *Резервное копирование* и *Терминал* аналогичны этим разделам в Ideco NGFW.

Администраторы

В Ideco Center можно создать несколько администраторов с разными ролями:

- **Администратор** - администратор с этой ролью имеет доступ ко всем функциональностям Ideco Center (*подробнее о возможностях*);
- **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**.

Есть два способа подключения к веб-интерфейсу Ideco NGFW из Ideco Center, которые находятся в Ideco Center:

- Из раздела *Серверы* (по нажатию на):
- При нажатии на стрелку в левом верхнем углу и выборе нужного NGFW:

Войти в подключенный Ideco NGFW с логином и паролем администратора Ideco Center **невозможно**.

Дополнительно

В разделе доступны настройки:

- **Адрес центральной консоли** - 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 данного 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.

18.3 Кластеризация

Подсказка: Название службы раздела **Кластеризация**: `ideco-cluster-backend`; `ideco-cluster-backup-pusher`.
Список служб для других разделов доступен по *ссылке*.

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. В свою очередь, 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 заниматься обработкой трафика может только одна из нод.

Сетевое взаимодействие между нодами осуществляется по *Кластерной сети*. Это физический канал, под который на каждой из нод резервируется по одной физической сетевой карте. Веб-сервер активной ноды управляет кластером, а резервная нода постоянно готова принимать данные.

Переключение нод происходит, когда пассивная нода перестает фиксировать работу активной - при отказе (полном зависании или перезагрузке) активной ноды, а также при потере связи между нодами по кластерной сети. В этом случае пассивная нода полностью прогружается и становится активной.

Если IP-адреса кластера настроены вручную, 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.

Подсказка: Для корректной работы кластера необходимо постоянное наличие связи между нодами.

Предупреждение: Особенности работы кластера:

- **Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено**;
- **Все данные, в том числе отчетность из ClickHouse, синхронизируются между двумя нодами. Исключение - логи из journald, мониторинг и аппаратные данные**;
- **При синхронизации двух NGFW происходит копирование данных активной ноды в резервную ноду с последующим перезаписыванием всей информации на резервной ноде**;
- **Синхронизация данных происходит автоматически в фоновом режиме**;
- **Синхронизация двух NGFW не производится при разных версиях**;
- **Не рекомендуется объединять в кластер георасределенные ноды**;
- **При работе NGFW на гипервизорах используйте средства отказоустойчивости гипервизора**;
- **При различных размерах жестких дисков могут возникнуть проблемы при синхронизации из-за нехватки места**;
- **Невозможно восстановление из бэкапов. При этом можно создать резервную копию и после разрушения кластера восстановить на нее ноду, которая была активной**;
- **Невозможно восстановиться на предыдущую версию**;
- **Запрещено добавлять сетевые интерфейсы, но РАЗРЕШЕНО отключать и редактировать. Удаление сетевого интерфейса кластера, использующегося для связи между нодами, сделает его недееспособным**;

- **Если у провайдера имеется привязка по MAC-адресу, то при переключении нод будет отсутствовать доступ в интернет**;
- **Для настройки кластеризации нужна только одна лицензия на Ideco NGFW.**

18.3.1 Требования

Для создания кластера необходимо соблюдение следующих требований:

- В кластере может быть только 2 ноды Ideco NGFW;
- Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки;
- Интерфейсы для создания кластерной сети на каждом Ideco NGFW должны быть в одном сегменте локальной сети, в котором нет других устройств;
- 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.

Предупреждение: Не используйте в качестве кластерной сети общедоступную сеть, используемую для передачи стороннего трафика. Обмен данными между нодами не защищен от подмены и прослушивания.

18.3.2 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.

Шаг 1 - Конфигурация резервной ноды

Если только установили сервер Ideco NGFW:

1. При входе в локальное меню резервной ноды увидите следующее сообщение:

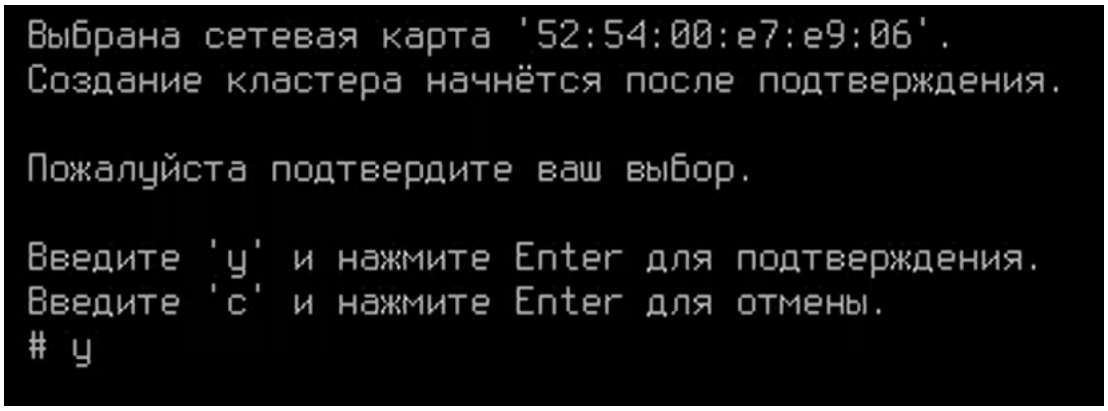
```
Требуется ли настроить данный сервер как вторую ноду кластера?

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

2. Введите **y** и нажмите **Enter**;

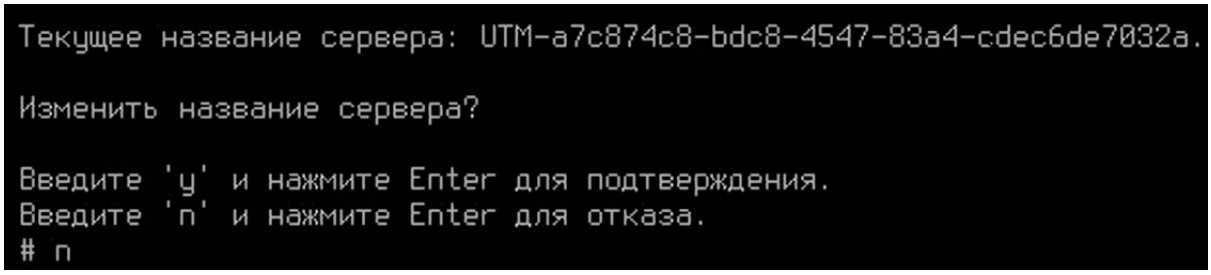
3. Выберите сетевую карту:

```
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. 52:54:00:51:d1:e4 Intel Corporation 82540EM Gigabit Ethernet Controller (Link N/A)
2. 52:54:00:9e:5b:af Intel Corporation 82540EM Gigabit Ethernet Controller (Link N/A)
3. 52:54:00:e7:e9:06 Intel Corporation 82540EM Gigabit Ethernet Controller (Link N/A)

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 3
```

4. Подтвердите создание кластера, введя **y** и нажав **Enter**:

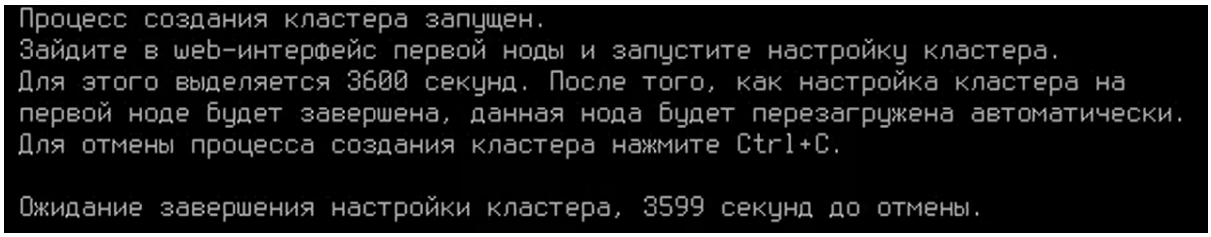


5. NGFW предложит изменить название сервера. При положительном ответите на вопрос *Изменить название сервера?*, появится надпись с предложением ввести новое название сервера.
Минимальное количество символов в названии - 2.
Максимальное количество символов в названии - 62.



После ввода нового названия нажмите **Enter** для продолжения диалога.

6. Появится сообщение, что процесс создания кластера запущен:

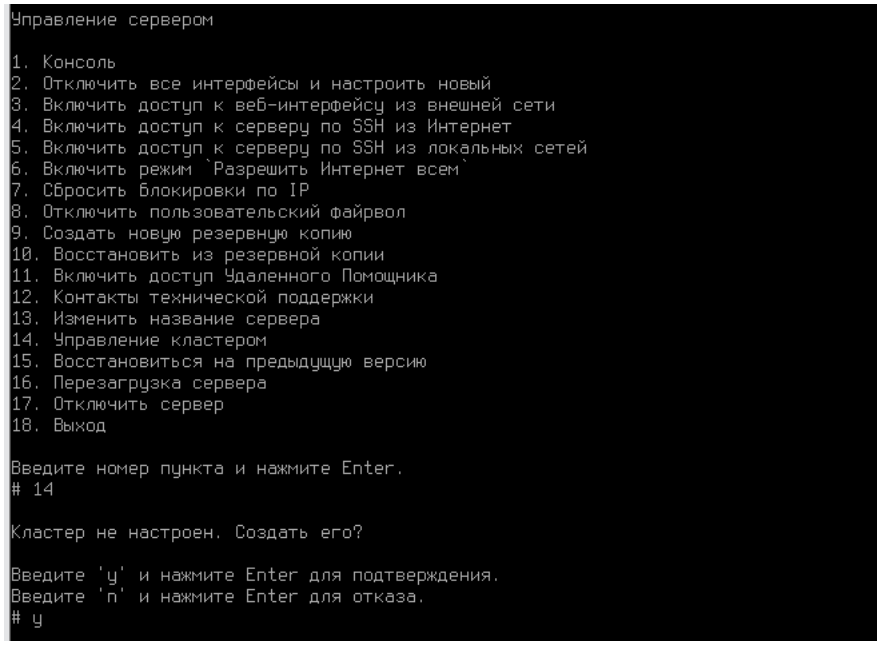


Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Если создаете резервную ноду из уже установленного сервера Ideco NGFW с лицензией и доступом в интернет:

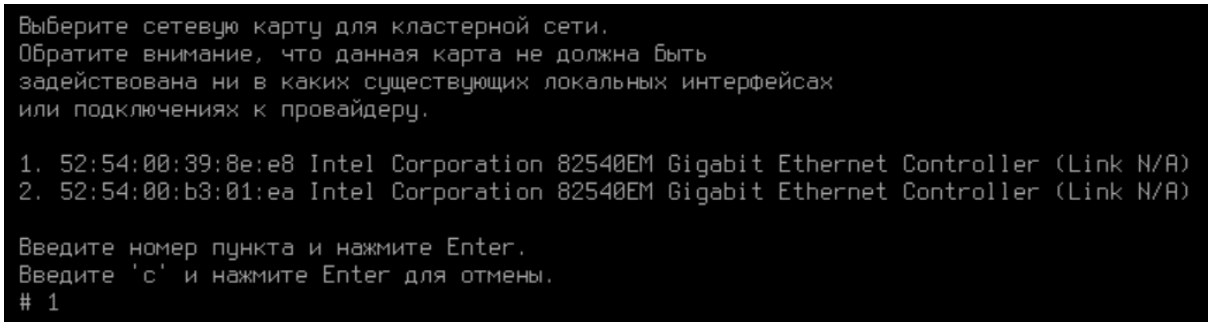
1. Перейдите в локальное меню;

2. Выберите пункт **Управление кластером**. Подтвердите создание кластера, введя **y** и нажав **Enter**:

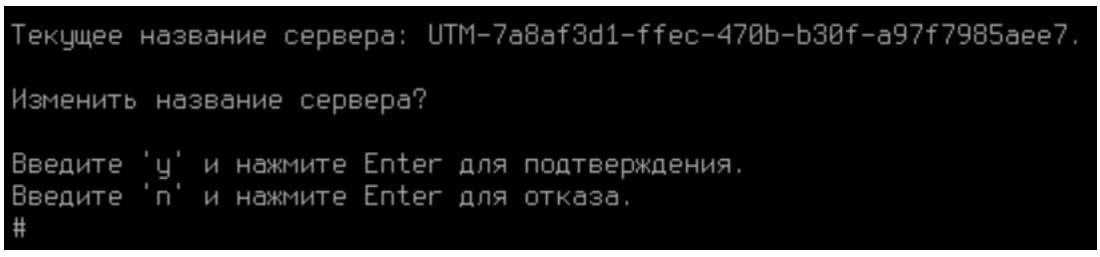


Если на ноде нет свободных сетевых карт, создание кластера будет недоступно.
Если кластер на ноде уже настроен, при выборе пункта *Управление кластером* будет доступно только его разрушение.

3. Выберите свободную физическую сетевую карту для создания кластерной сети и подтвердите выбор:



4. NGFW предложит изменить название сервера. При положительном ответите на вопрос *«Изменить название сервера?»* появится надпись с предложением ввести новое название сервера.
Минимальное количество символов в названии - 2.
Максимальное количество символов в названии - 42.



После ввода нового названия нажмите **Enter** для продолжения диалога.

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.
```

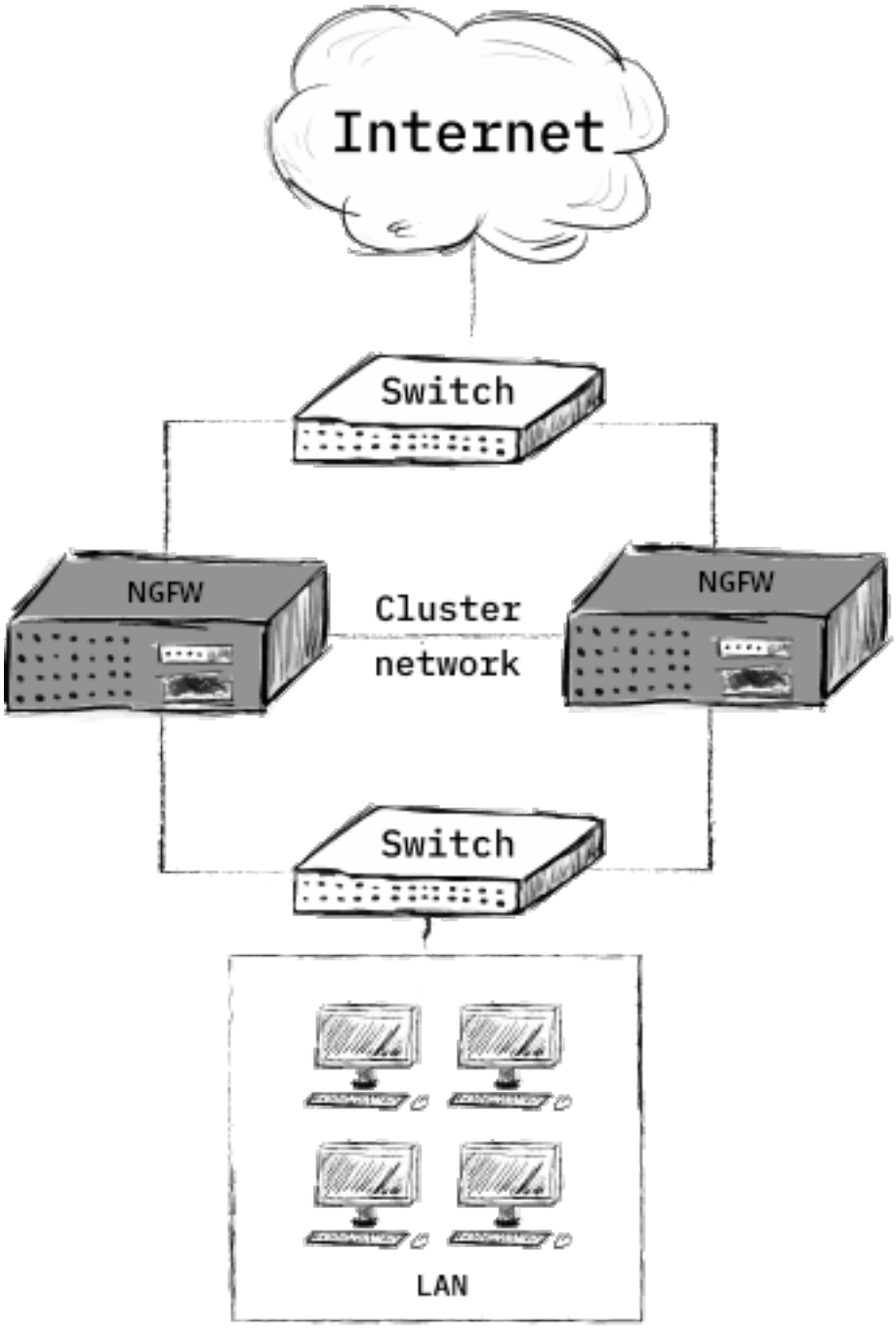
Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Шаг 2 - Конфигурация активной ноды

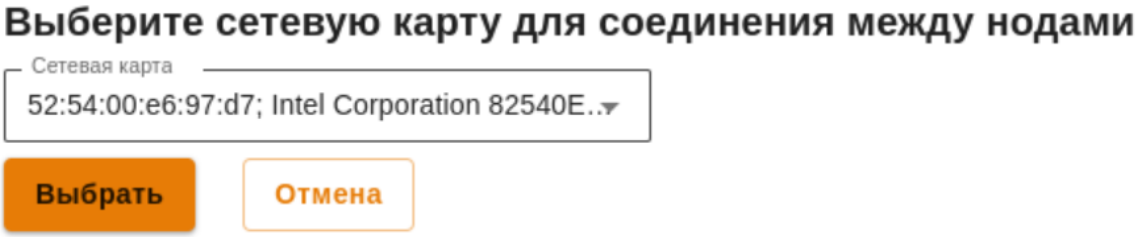
Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW выполните следующие действия:

1. Перейдите в раздел **Управление сервером -> Кластеризация** и нажмите кнопку **Настроить кластер отказоустойчивости**.

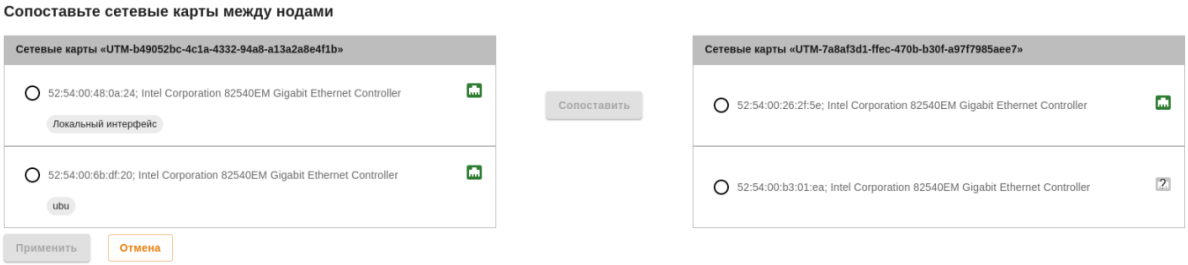
2. Подтвердите, что топология сети соответствует схеме ниже:



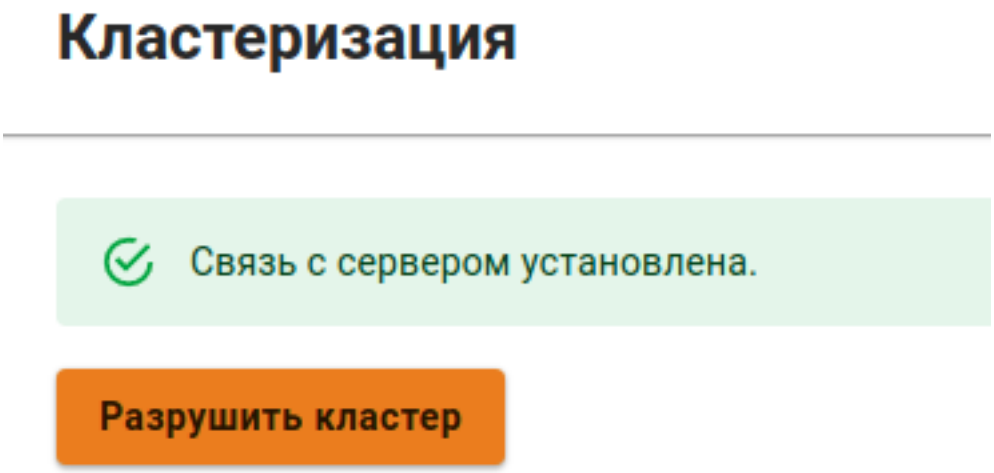
3. Выберите сетевую карту для соединения между нодами:



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.

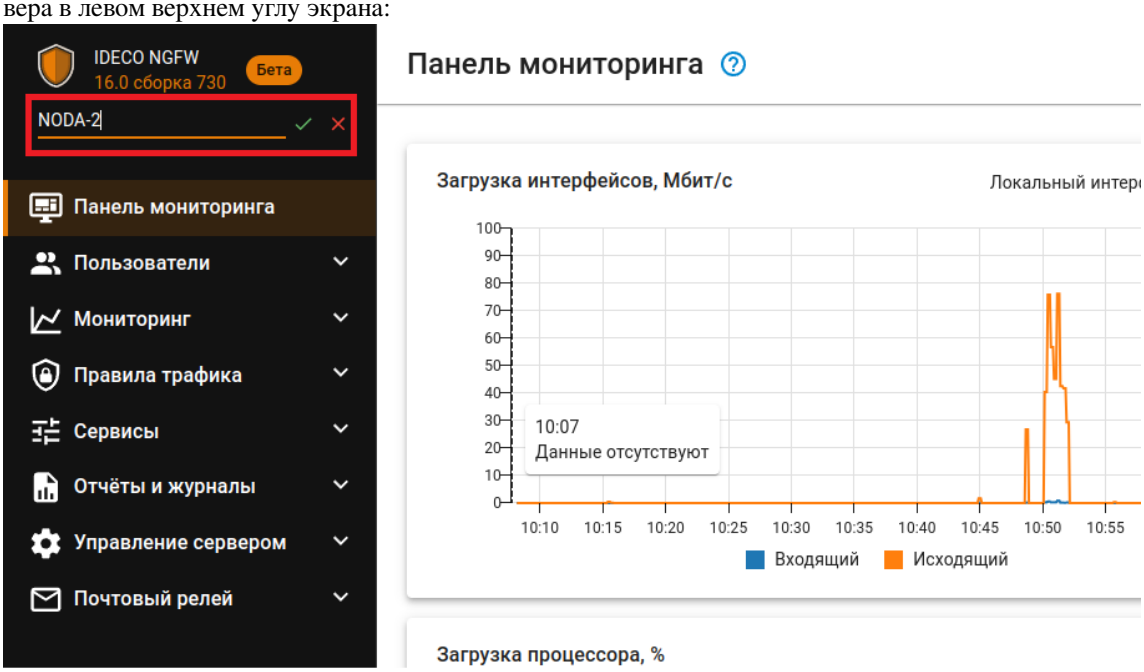
18.3.3 Изменение названия сервера

Изменить название сервера можно у той ноды, которая в данный момент является активной. Сделать это можно из локального меню или из веб-интерфейса.

- В локальном меню выберите соответствующий пункт и введите новое название:

```
Вход в локальное меню.

Введите логин и нажмите Enter.

# baryshev


Введите пароль и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
#

Управление сервером

1. Консоль
2. Включить доступ к веб-интерфейсу из внешней сети
3. Включить доступ к серверу по SSH из Интернет
4. Включить доступ к серверу по SSH из локальных сетей
5. Включить режим `Разрешить Интернет всем`
6. Сбросить блокировки по IP
7. Отключить пользовательский файрвол
8. Создать новую резервную копию
9. Восстановить из резервной копии
10. Включить доступ Удаленного Помощника
11. Контакты технической поддержки
12. Изменить название сервера
13. Управление кластером
14. Перезагрузка сервера
15. Отключить сервер
16. Выход

Введите номер пункта и нажмите Enter.
# 12
Текущее название сервера: NODA-2

Введите новое название сервера и нажмите Enter.

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

- В веб-интерфейсе поменять название можно, нажав кнопку **Редактировать** рядом с названием сервера в левом верхнем углу экрана:

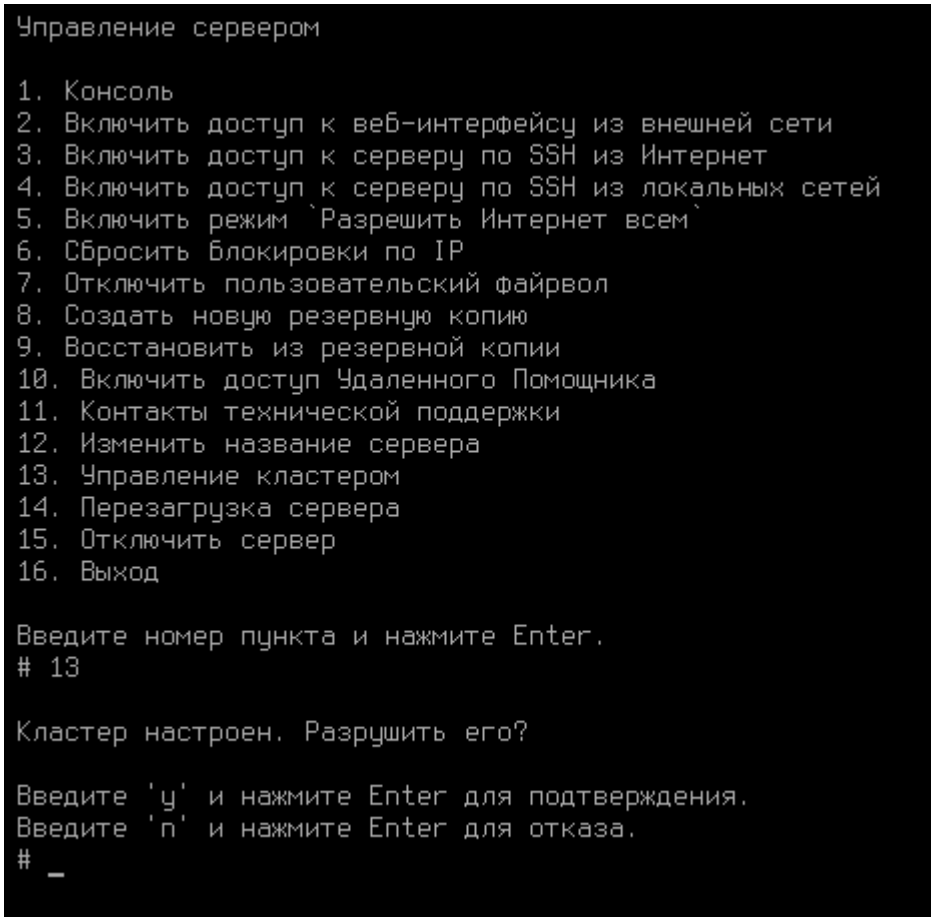


18.3.4 Разрушение кластера

Разрушить кластер можно только из локального меню или веб-интерфейса *активной* ноды. При этом она продолжит работать, а вторая нода (резервная) сбросит настройки до состояния только что установленного Ideco NGFW.

Разрушение кластера из локального меню:

1. Выберите пункт локального меню **Управление кластером**, введите **y** и нажмите **Enter**;

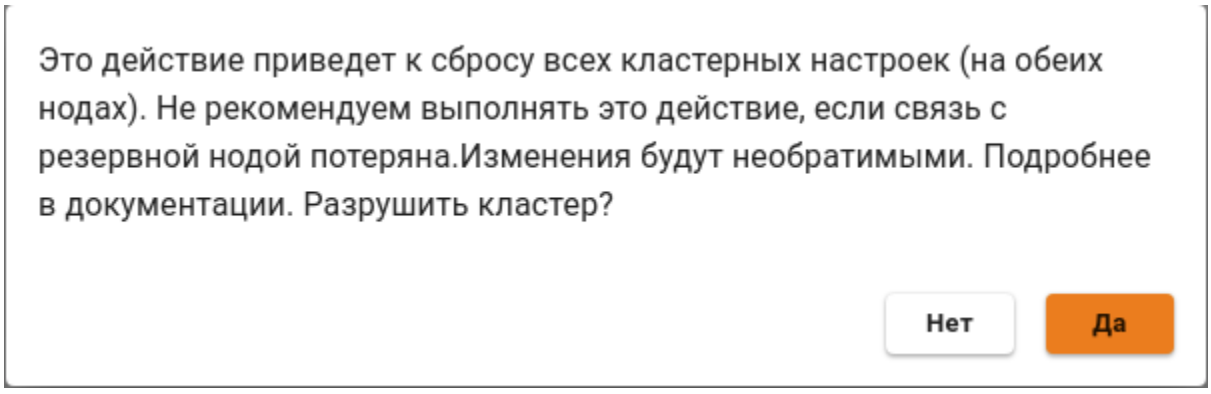


2. Подтвердите выбор.

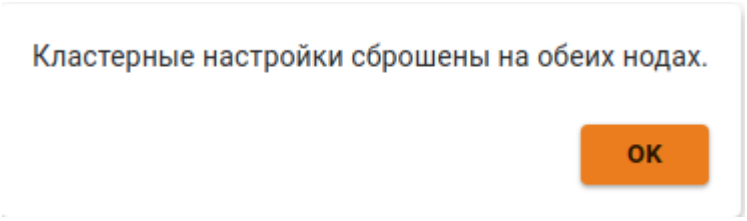
Разрушение кластера из веб-интерфейса:

1. Перейдите в раздел **Управление сервером -> Кластеризация** и нажмите кнопку **Разрушить кластер**.

2. Появится окно с предупреждением:



3. Нажмите **ОК**:



18.3.5 Процедура обновления нод

Чтобы обновить NGFW до последней версии в режиме кластера, необходимо выполнить следующие 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.

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.

18.4 Автоматическое обновление сервера

Подсказка: Название службы раздела **Автоматическое обновление сервера**: `ideco-sysupdate-backend`.
Список служб для других разделов доступен по *ссылке*.

> **Предупреждение:** Обновление сервера возможно исключительно по сети. Обновиться с помощью установочного диска или флешки невозможно.
>
> Отключить автоматическое обновление Ideco NGFW нельзя.

18.4.1 Автоматическое обновление

- Поле **Отложить обновления** - время, на которое будет отложено обновление (максимальный срок 6 месяцев с даты релиза последней версии, до которой доступно обновление);
- Поле **День недели** - день недели запуска автоматического обновления;
- Поле **Час автоматической перезагрузки** - позволяет выбрать час запуска автоматического обновления;
- Поле **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**;

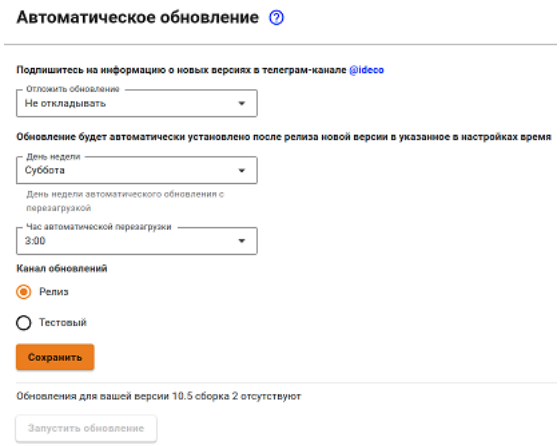
- Кнопка **Запустить обновление** - запускает механизм принудительного обновления. Если кнопка неактивна, обновления отсутствуют.

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 *Центральная консоль*.

Подсказка: Кнопка принудительного обновления активна, когда обновление уже скачано, и только применяет его, инициировать скачивание нельзя.

После принудительного обновления потребуется полная перезагрузка сервера.

Предупреждение: 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.



После проведения процедуры обновления новая версия будет отображаться в верхнем левом углу локальной консоли и веб-интерфейса администратора.

18.4.2 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 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.

18.4.3 Особенности обновления NGFW

Обновление будет автоматически установлено в указанное в настройках время после релиза новой версии.

Автоматическое обновление сервера можно отложить максимум на 6 месяцев. Этот 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.

Предупреждение: Если обновление было отложено на 6 месяцев, но за это время вышел новый минорный релиз, дата обновления сдвигается. 6 месяцев теперь отсчитываются с даты выхода последнего доступного минорного релиза.

Если сервер обновляется на последний минор и с момента релиза следующей мажорной версии прошло больше 6 месяцев, отложить обновление будет невозможно. NGFW начнет обновляться сразу (с учетом указанного дня недели и времени).

18.5 Резервное копирование

Подсказка: Название службы раздела **Резервное копирование**: `ideco-backup-backend`; `ideco-backup-create`; `ideco-backup-restore`; `ideco-backup-rotate`.
Список служб для других разделов доступен по *ссылке*.

Интернет-шлюз поддерживает следующие типы автоматического бекапа:

- на сетевое файловое хранилище по протоколу FTP;
- на сетевое файловое хранилище по протоколу NetBIOS;
- на локальный жесткий диск.

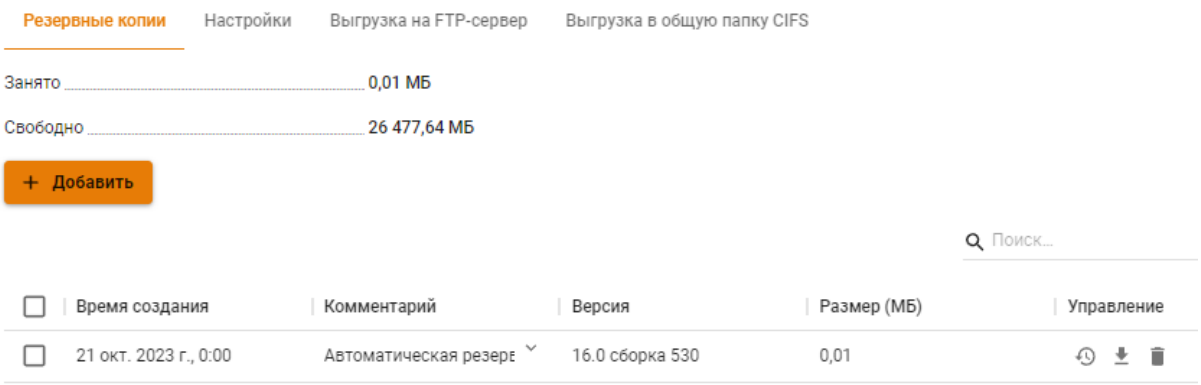
Для настройки автоматического резервного копирования перейдите в раздел **Управление сервером -> Резервное копирование -> Настройки**. Резервная копия создается каждый день в указанный в настройках час (рекомендуется выбирать ночное время для создания резервной копии).

Подсказка: Резервные копии включают в себя все настройки, которые администратор может создать в веб-интерфейсе.

Резервные копии не включают в себя:

- Логи;
- Почту;
- Статистику web-трафика и другие отчеты;
- Любые кешируемые данные - базы антивирусов, правила IPS и т. п.;
- Любые данные, генерируемые в процессе работы системы автоматически.

Хранить бекапы можно в течение недели или месяца.



18.5.1 Резервное копирование на удаленное файловое хранилище по протоколу FTP

Этот тип предусматривает запись резервных копий на FTP-сервер. Ключевые параметры, необходимые для настройки резервного копирования на FTP-сервер, описаны в таблице ниже.

Параметр	Описание
Адрес сервера	IP-адрес удаленного FTP-сервера, на котором будут размещаться копии базы данных
Логин	Имя пользователя для авторизации на FTP-сервере
Пароль	Пароль для авторизации на FTP-сервере
Путь к каталогу	Каталог, в который будут записываться копии базы данных

18.5.2 Резервное копирование на сетевое файловое хранилище по протоколу NetBIOS(CIFS)

Этот тип резервного копирования предусматривает запись копии на сервер по протоколу NetBIOS (CIFS). Ключевые параметры, необходимые для настройки резервного копирования на NetBIOS-сервер, описаны в таблице.

Параметр	Описание
Адрес сервера	IP-адрес удаленного NetBIOS-сервера, на котором будут размещаться копии базы данных
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 копии базы данных

Подсказка: Для доменной учетной записи формат поля **Логин** должен иметь вид: **Имя_пользователя**.

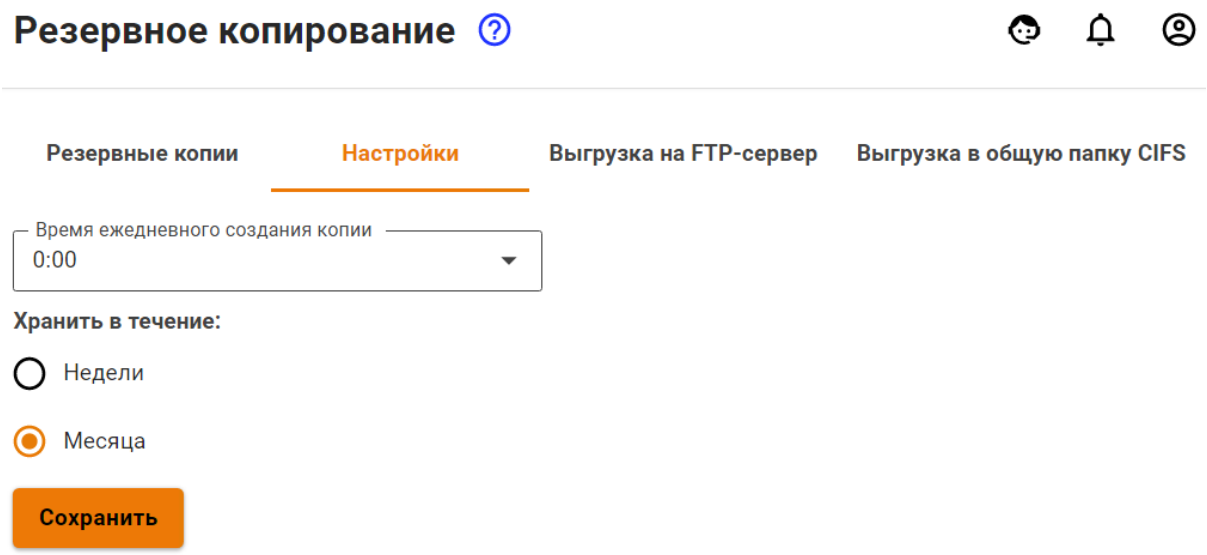
Путь к каталогу нужно указывать в UNIX-формате. К примеру, в ОС Windows каталог открывается по следующему пути `\\192.168.1.1\dir_1\dir_2\backup`, значит в поле **Путь к каталогу** нужно прописать `dir_1/dir_2/backup`.

18.5.3 Резервное копирование на локальный жесткий диск

Можно загрузить резервную копию с сервера или с компьютера на сервер с помощью веб-интерфейса либо локального меню.

- Кнопка **Добавить** позволяет создать резервную копию настроек сервера. Копии настроек создаются автоматически ежедневно;
- Кнопка **Применить** позволяет восстановить резервную копию настроек. Возможно восстановление настроек только для бэкапа версии, одинаковой с установленной на сервере;
- Кнопка **Скачать** позволяет скачать резервную копию с сервера на ваш компьютер;
- Кнопка **Удалить** удаляет резервную копию с сервера.

Интерфейс управления резервными копиями в веб-интерфейсе представлен на скриншоте ниже.



Управление резервными копиями через локальное меню

- Чтобы создать новую резервную копию через локальное меню Ideco NGFW, выберите пункт **9** и нажмите **Enter**. Далее введите комментарий для резервной копии и нажмите **Enter**.

Пример создания резервной копии через локальное меню приведен на скриншоте ниже:

- Чтобы восстановить конфигурацию из резервной копии, выберите пункт **10** и нажмите **Enter**. Выберите из списка резервную копию (если копий несколько), введя пункт нужной копии, и нажмите **Enter**. Для восстановления из резервной копии необходимо перезагрузить сервер. Введите **y**, а затем **Enter** для перезагрузки.

Пример восстановления из резервной копии через локальное меню приведен на скриншоте ниже:

```
Введите номер пункта и нажмите Enter.
# 10

Выберите резервную копию для восстановления.

1.
Время:         29.09.2021 11:33:22
Версия:        10.5 сборка 2
Комментарий:   Backup 3

2.
Время:         29.09.2021 11:32:32
Версия:        10.5 сборка 2
Комментарий:   Backup 2

3.
Время:         29.09.2021 11:18:07
Версия:        10.5 сборка 2
Комментарий:   Резервная копия 1

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 3

Выбрана резерная копия

Время:         29.09.2021 11:18:07
Версия:        10.5 сборка 2
Комментарий:   Резервная копия 1

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

Пожалуйста подтвердите ваш выбор.

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

Подсказка: Чтобы перенести установленный Ideco NGFW с одного сервера на другой с сохранением всех настроек, воспользуйтесь статьей *Перенос данных и настроек на другой сервер*.

18.6 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.

18.6.1 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`;
- **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 ARP-таблицы**: `ip neigh show`.

18.6.2 Таблица служб

Раздел	Имя службы
Файрвол	ideco-nflog; ideco-firewall-backend
Контроль приложений	ideco-app-backend; ideco-app-control@Leth<номер локального интерфейса>
Контент-фильтр	ideco-content-filter-backend
Ограничение скорости	ideco-shaper-backend
Антивирусы веб-трафика	ideco-av-backend;
Предотвращение вторжений	ideco-suricata-backend; ideco-suricata; ideco-suricata-event-syncer; ideco-suricata-event-to-syslog
Объекты	ideco-alias-backend
Квоты	ideco-quotas-backend; systemd-quotacheck
Сетевые интерфейсы	ideco-network-backend; ideco-network-nic
Балансировка и резервирование, Маршрутизация	ideco-routing-backend
BGP, OSPF	ideco-routing-backend
Прокси	ideco-proxy-backend; squid
Обратный прокси	ideco-reverse-backend
DNS	ideco-dns-backend; unbound
DDNS	ideco-dns-backend
DHCP	ideco-dnsmasq
IPsec	ideco-ipsec-backend; strongswan
Центральная консоль	ideco-central-console-backend
Кластеризация	ideco-cluster-backend; ideco-cluster-backup-pusher
Автоматическое обновление	ideco-sysupdate-backend

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Раздел	Имя службы
Резервное копирование	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
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-monitor-backend
Обнаружение устройств	ideco-netscan-backend
Web Application Firewall	ideco-waf-backend; ideco-waf-event-syncer
IGMP Proxy	ideco-igmpproxy-backend; ideco-igmpproxy

18.7 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.

18.7.1 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.

18.7.2 Добавление FREE (бесплатной) лицензии

Для добавления FREE-лицензии нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Свободные лицензии**.

18.7.3 Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн. Онлайн проводится только в MY.IDECO и ограничивается шагом 1 ниже. 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-привязка лицензии

Выберите удобный вариант привязки:

- Во вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ . Далее в открывшемся окне выберите нужную лицензию и сохраните изменения нажав **Привязать лицензию**.
- Во вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения нажав **Привязать**.

Офлайн-привязка лицензии

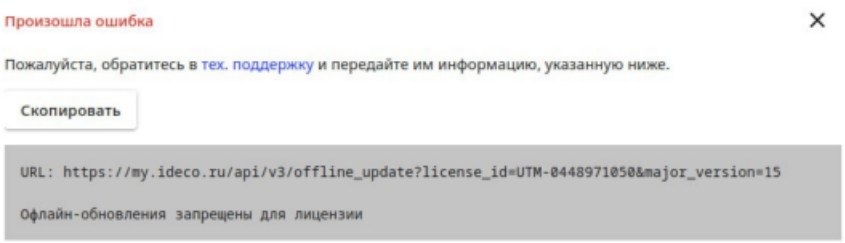
1. Для предоставления офлайн-лицензии обратитесь к менеджеру.

2. Привяжите предоставленную лицензию к серверу:

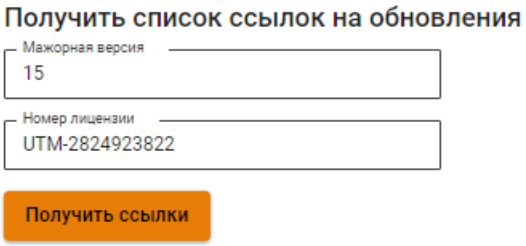
- Во вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ . Далее в открывшемся окне выберите нужную лицензию и сохраните изменения нажав **Привязать лицензию**.
- Во вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения нажав **Привязать**.

Пример наименования сервера для **офлайн**-регистрации: `UTM (UTM Unknown)`

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



3. Перейдите в раздел **NGFW -> Офлайн** и введите в соответствующие поля мажорный номер версии и номер лицензии:



4. Нажмите **Получить ссылки** и сохраните файл конфигураций, нажав на license:

Помимо информации о лицензии личный кабинет предоставит файлы для обновления баз модулей безопасности. Подробнее о процессе обновления в статье *Регистрация сервера* (шаги 8 и 9).

5. Добавьте конфигурационный файл с информацией о лицензии в Ideco NGFW:

- Перейдите в раздел **Управление сервером -> Терминал**;
- Загрузите полученный файл `license.json` на сервер Ideco NGFW в директорию `/var/cache/ideco/license-backend/`;
- Перезапустите сервис лицензий командой `systemctl restart ideco-license-backend.service`;
- Перейдите в раздел **Управление сервером - Лицензия** и убедитесь, что лицензия установлена.

18.7.4 Просмотр информации о лицензиях

Посмотреть информацию о модулях и лицензии можно:

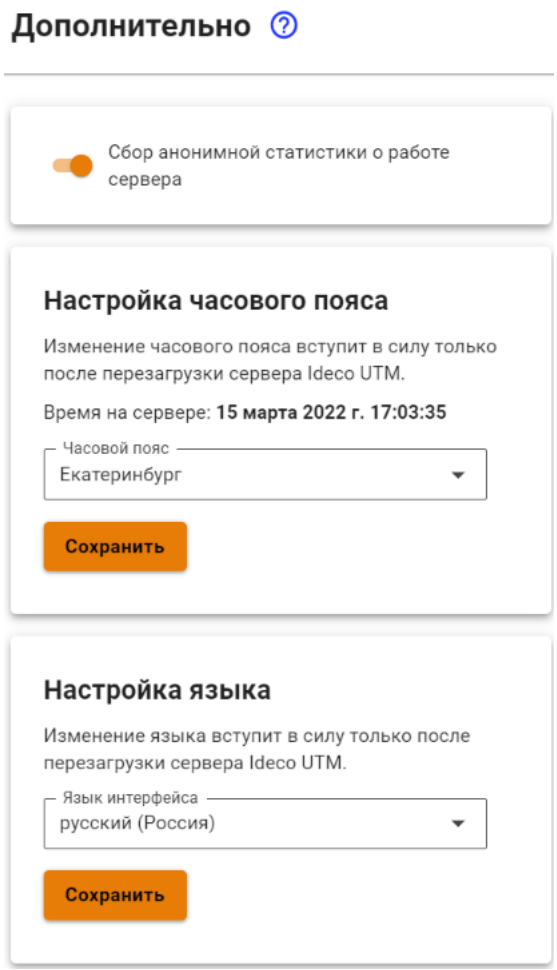
- В личном кабинете *MY.IDECO* в разделе **NGFW -> Лицензирование**, нажав на иконку напротив нужного сервера;
- В веб-интерфейсе Ideco NGFW, в разделе **Управление сервером -> Лицензия**.

Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др.

18.8 Дополнительно

18.8.1 Основное

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.

Предупреждение: Изменение часового пояса вступит в силу только после перезагрузки сервера Ideco NGFW.

19. Почтовый релей

19.1 Основное

Подсказка: Все возможности по фильтрации почтового трафика можно также применить к внутреннему почтовому серверу, опубликовав его через почтовый релей.

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*.

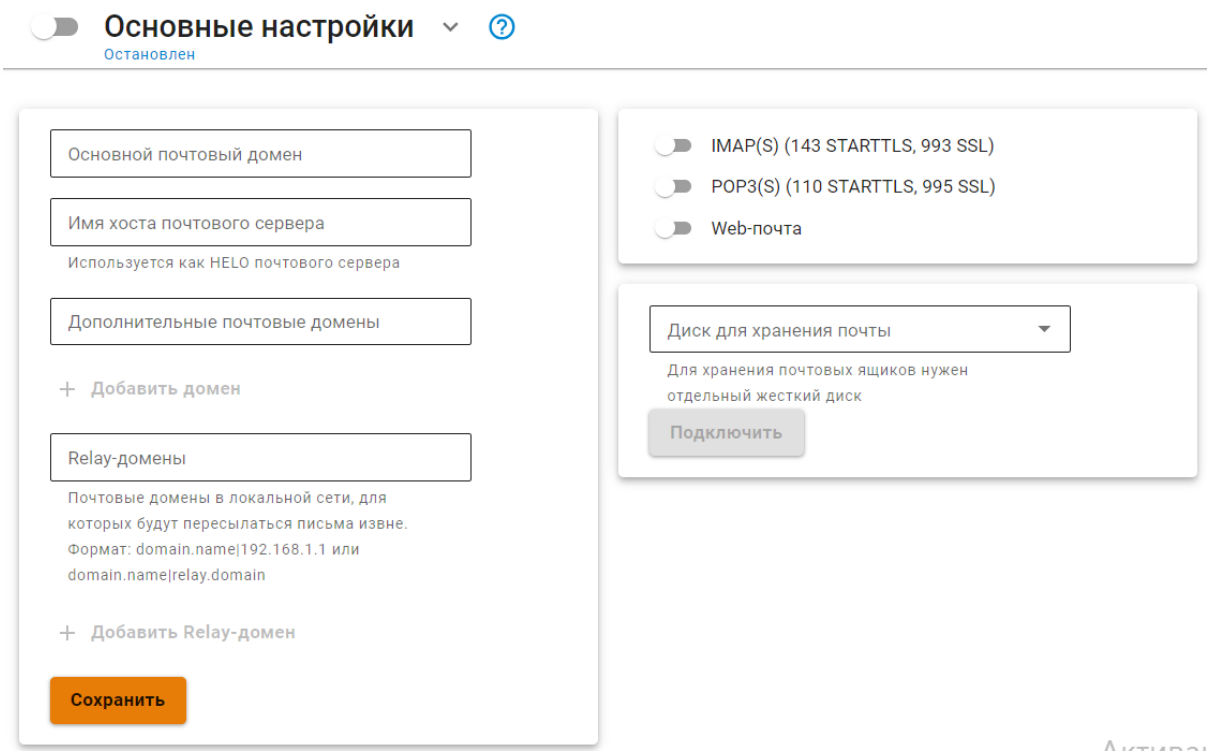
Предупреждение: При настройке *кластера* почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.

19.2 Основные настройки

19.2.1 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:

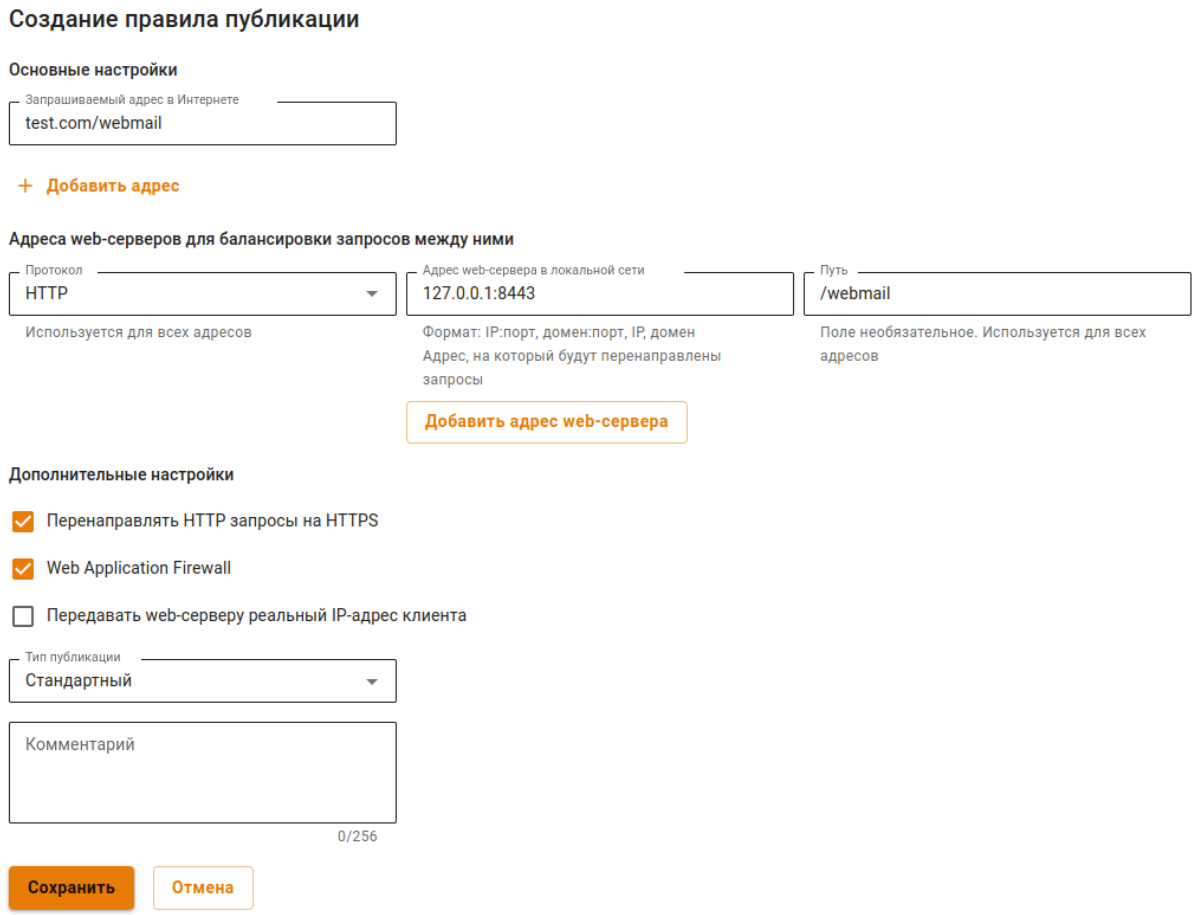
19.2.2 Web-почта

Основное

Подсказка: Перед настройкой веб-почты настройте на Ideco NGFW почтовый сервер.

1. Для работы веб-почты на локальном интерфейсе необходимо активировать настройку **Web-почта** в разделе **Почтовый релей -> Основные настройки**.

2. Для работы на внешнем интерфейсе нужно создать в разделе **Сервисы -> Обратный прокси** правило вида:



После создания правила из локальной сети в браузере наберите: `https://x.x.x.x:8443/webmail/`, где `x.x.x.x` - адрес локального интерфейса.

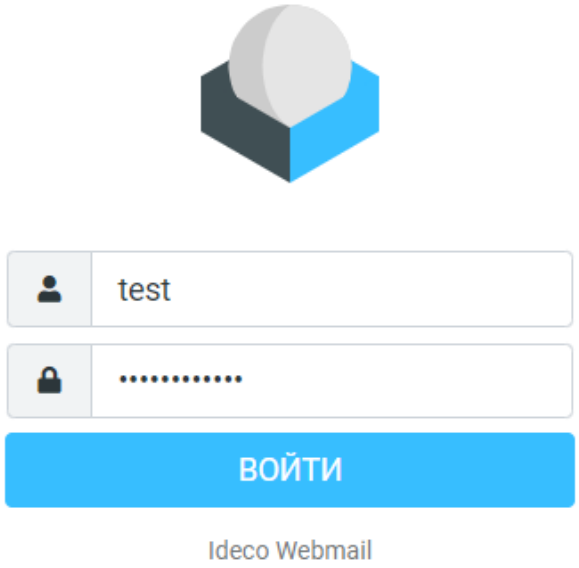
Из сети интернет наберите в браузере: `https://[доменное_имя]/webmail/`. Например: `https://test.com/webmail/`

Менее приоритетный альтернативный вариант: из сети интернет наберите в браузере: `https://x.x.x.x/webmail/`, где `x.x.x.x` - адрес внешнего интерфейса.
Например: `https://66.77.88.99/webmail/`

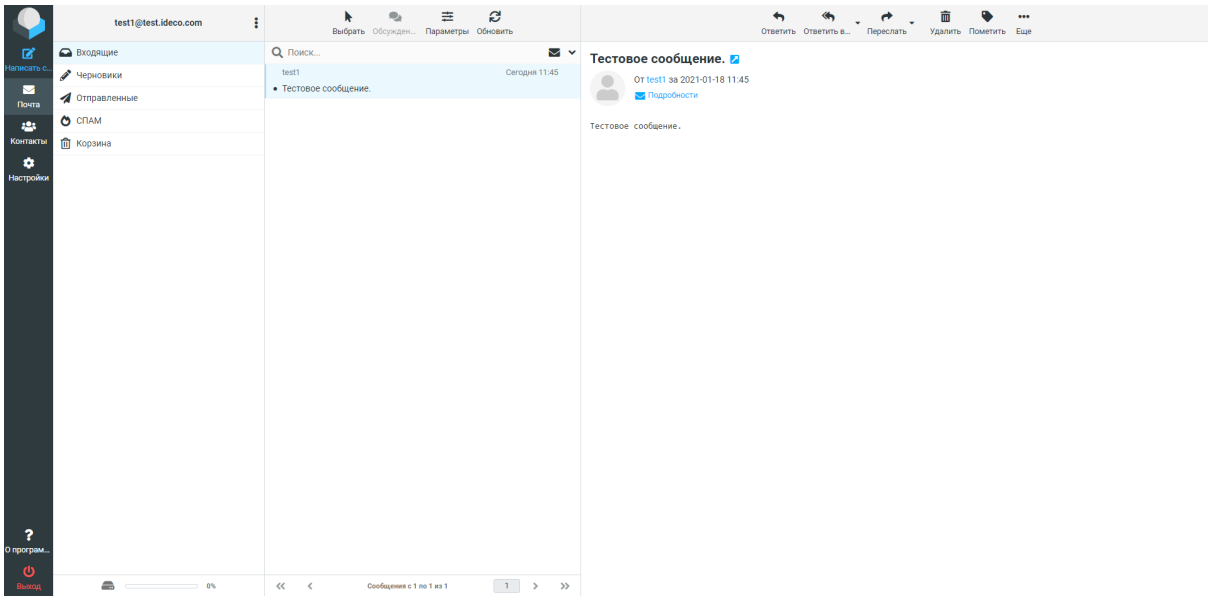
Подсказка: Для подключения обязательно использовать HTTPS.

- 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.

19.2.3 Настройка почтового релея

Основное

Подсказка: Видеоинструкция по настройке почтового релея в Ideco NGFW:

Ссылка на видеоинструкцию по настройке почтового релея в Ideco NGFW

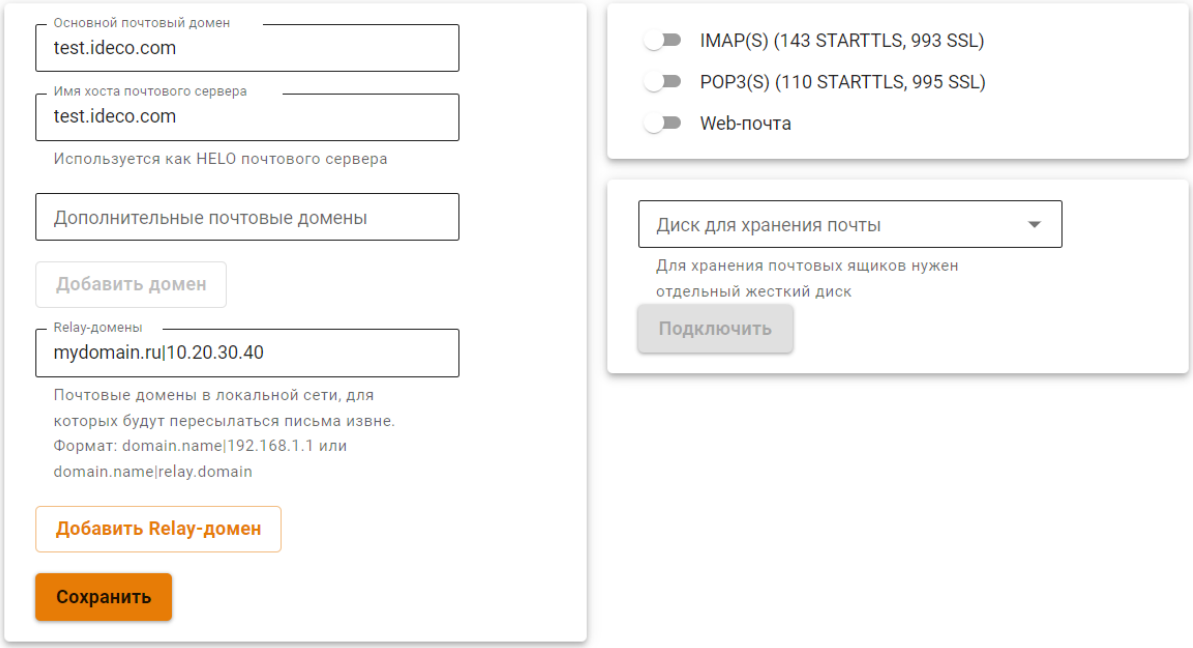
Предупреждение: NGFW не поддерживает кириллические почтовые домены.

Перед настройкой почтового релея убедитесь, что на Ideco NGFW включен почтовый сервер.

Для настройки почтового релея:

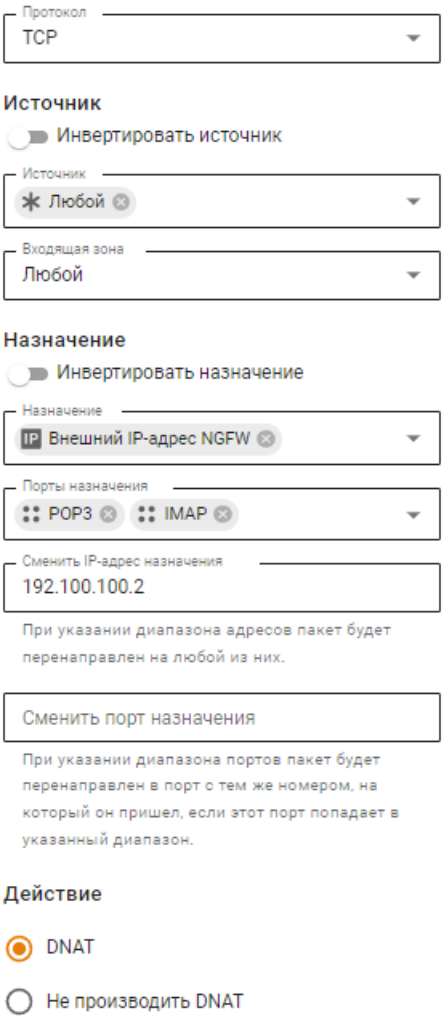
1. Добавьте в поле **Relay-домены** (почтовые домены в локальной сети, для которых будут пересылаться письма извне) запись вида: `mydomain.ru|10.20.30.40`, где:

- `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** и создайте 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.

19.2.4 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.

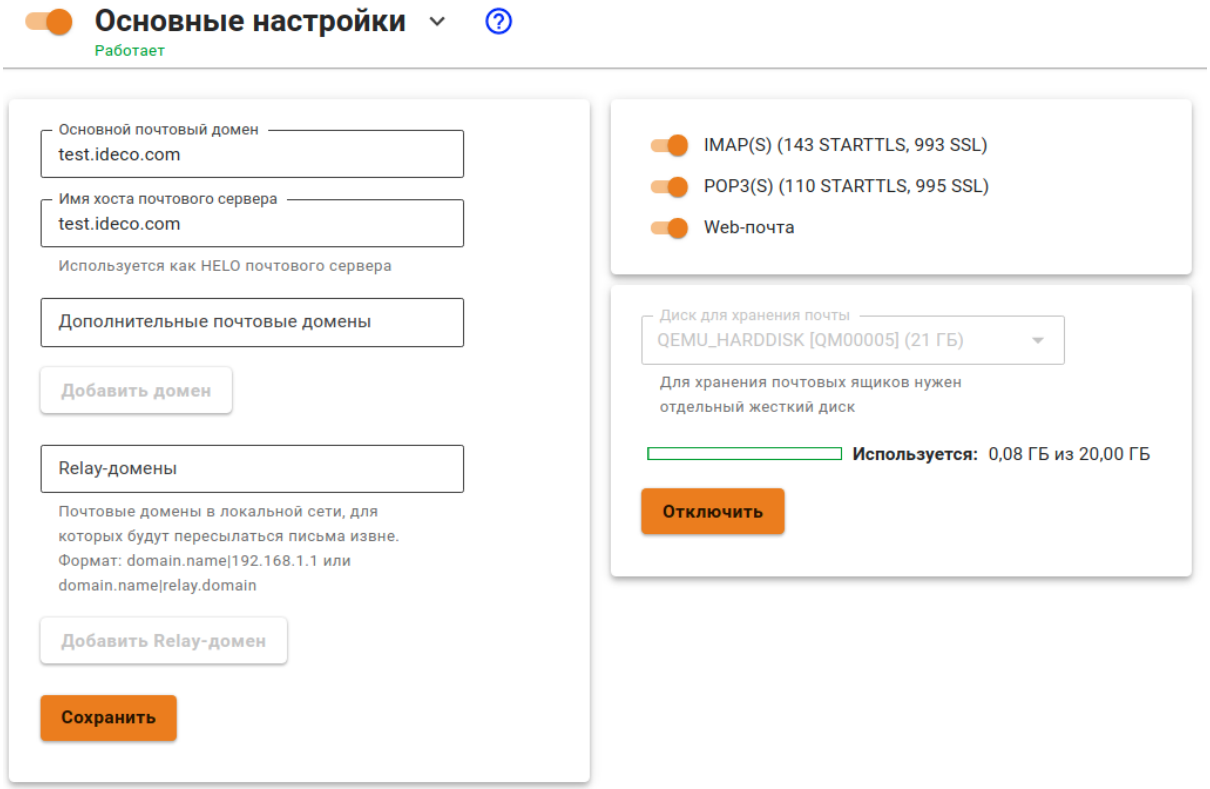
- **Имя хоста почтового сервера** должно разрешаться из сети интернет во внешний IP-адрес NGFW. Почтовый сервер использует это имя как уникальный идентификатор при транспорте почты между другими почтовыми серверами. Необходимо для корректной работы почтового сервера в интернете.

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.

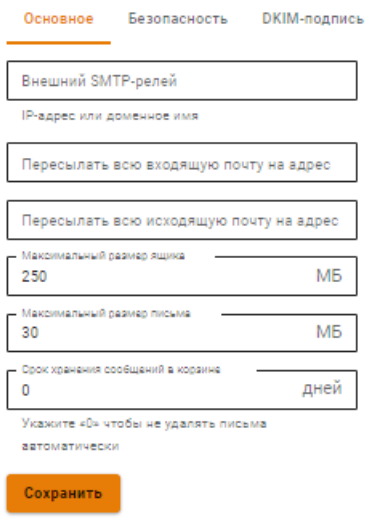
При правильной настройке почтовый сервер на Ideco NGFW должен получить 10 баллов из 10.

19.3 Расширенные настройки

Раздел **Расширенные настройки** состоит из трех подразделов: **Основное, Безопасность, DKIM-подпись**.

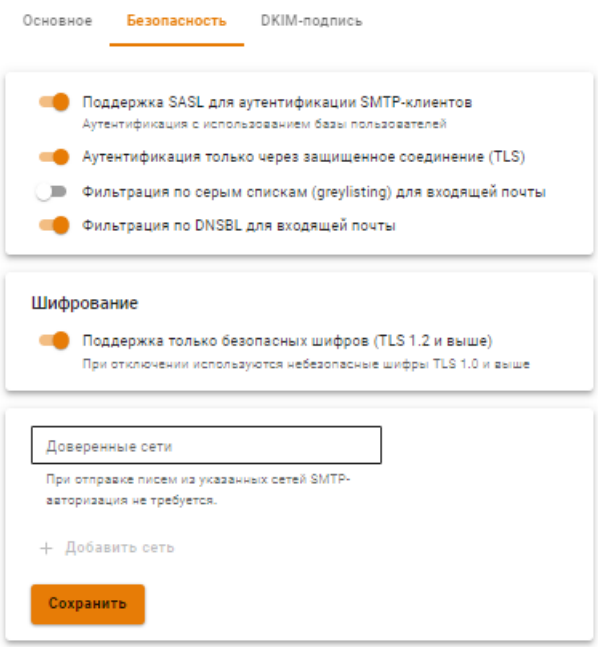
19.3.1 Основное

- **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.



19.3.2 Безопасность

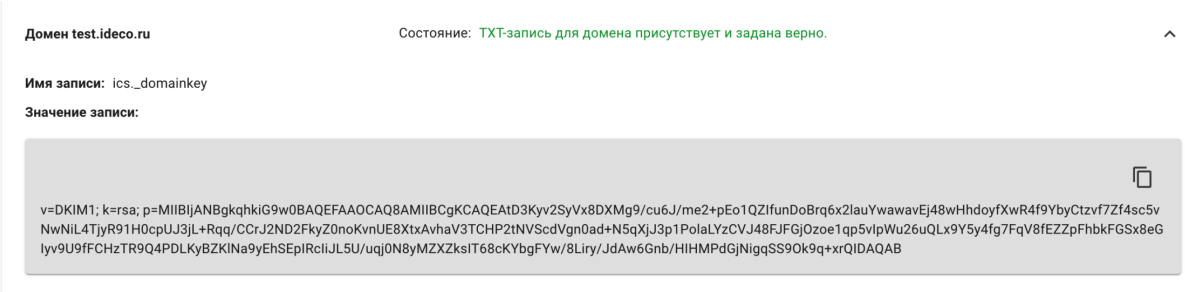
- **Поддержка SASL для аутентификации SMTP-клиентов.** Подключиться к почтовому ящику из интернета и отправить письмо, используя SMTP сервер Ideco, можно будет только, пройдя авторизацию по логину и паролю, заданному для этой учетной записи пользователя на сервере. **Не включайте данный параметр, если 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`.



19.3.3 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 256 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.

19.3.4 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.**

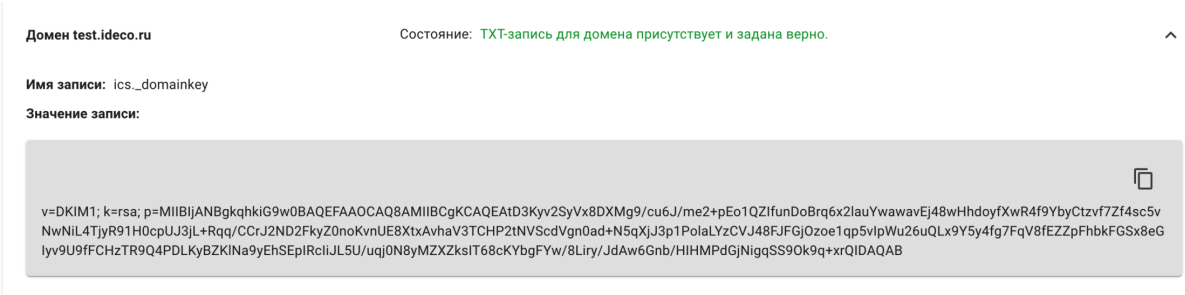
2. Добавьте ресурсную запись типа MX, указывающую на A-запись, которая была создана на предыдущем шаге. Запись типа MX указывает на сетевой узел, который занимается обработкой почтовых сообщений для домена. Она должна ссылаться на доменное имя почтового сервера, а не на IP-адрес.

Рекомендуем:

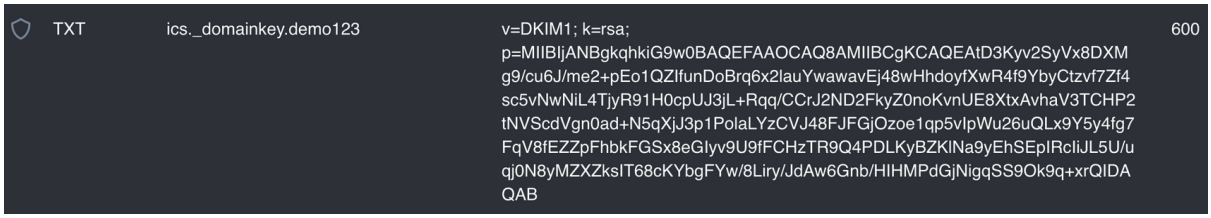
3. Добавить обратную ресурсную запись типа PTR. Эта запись должна быть прописана в файле обратной зоны. Эти изменения должны быть сделаны на стороне интернет-провайдера. Обратитесь к нему с просьбой прописать обратную ресурсную запись для IP-адреса, которая должна ссылаться на запись типа MX.

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.

19.4 Антиспам

Подсказка: Видеоинструкция по настройке антиспама в Ideco NGFW:

Ссылка на видеоинструкцию по настройке антиспама в Ideco NGFW

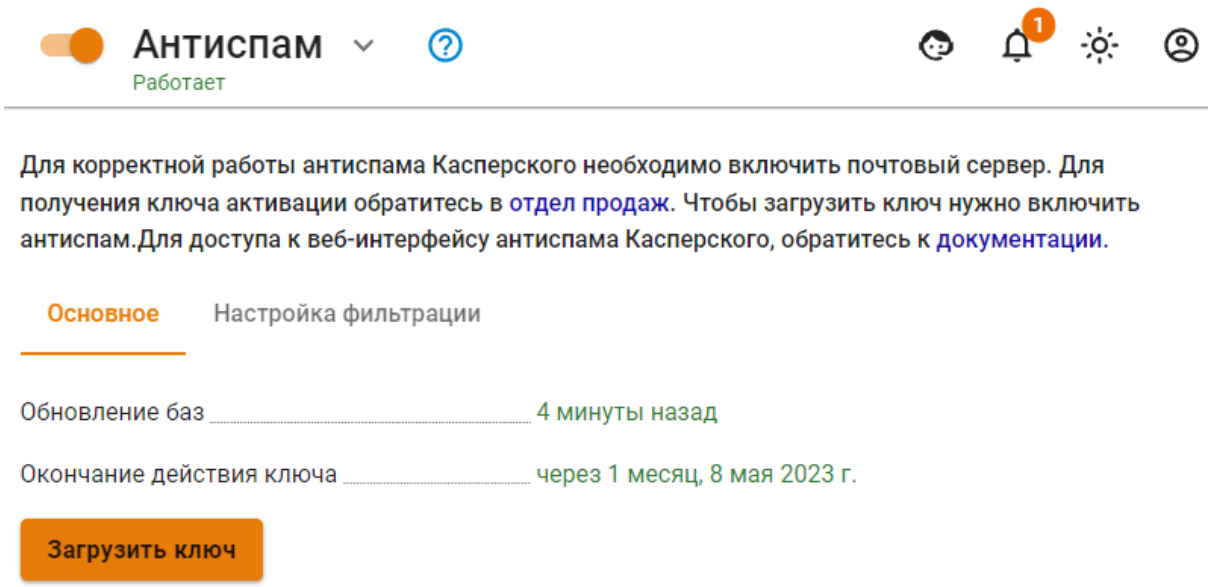
Раздел **Антиспам** состоит из двух подразделов: **Основное** и **Настройки фильтрации**.

19.4.1 Основное

Позволяет управлять работой службы антиспама 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`.

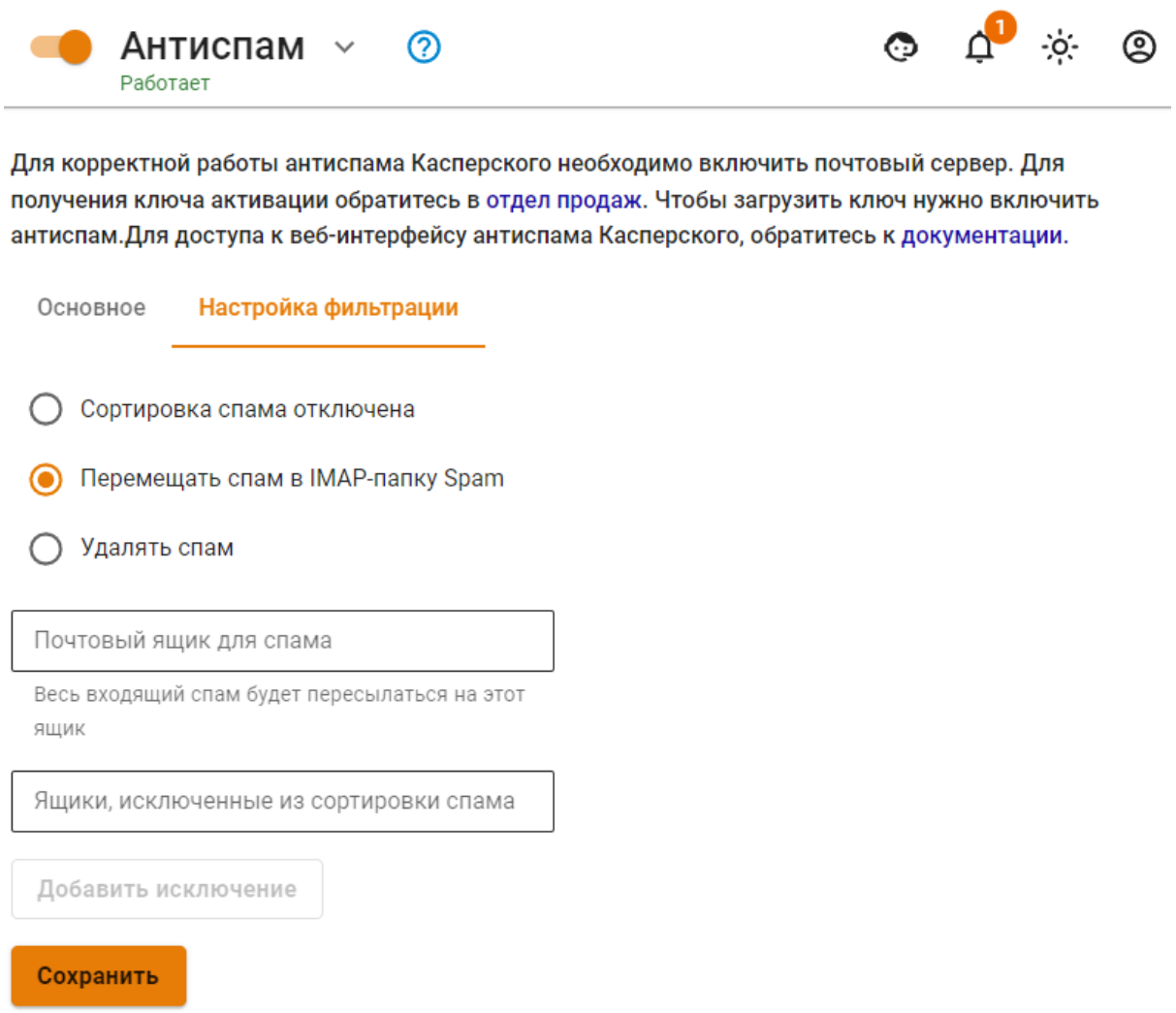
Если приобретена лицензия на антиспам, но нет в распоряжении лицензионного ключа, проверьте переписку с отделом продаж нашей компании (sales@ideco.ru) на наличие вложений. Если не удалось найти таких вложений, запросите ключ заново, выслав письмо на sales@ideco.ru с указанием наименования организации или номера лицензии.

Подсказка: Перед загрузкой ключа обязательно включите модуль антиспама.



19.4.2 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** 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 следующую команду `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`

2. Задайте пароль для стандартного аккаунта **Administrator**, состоящий минимум из 8 символов:

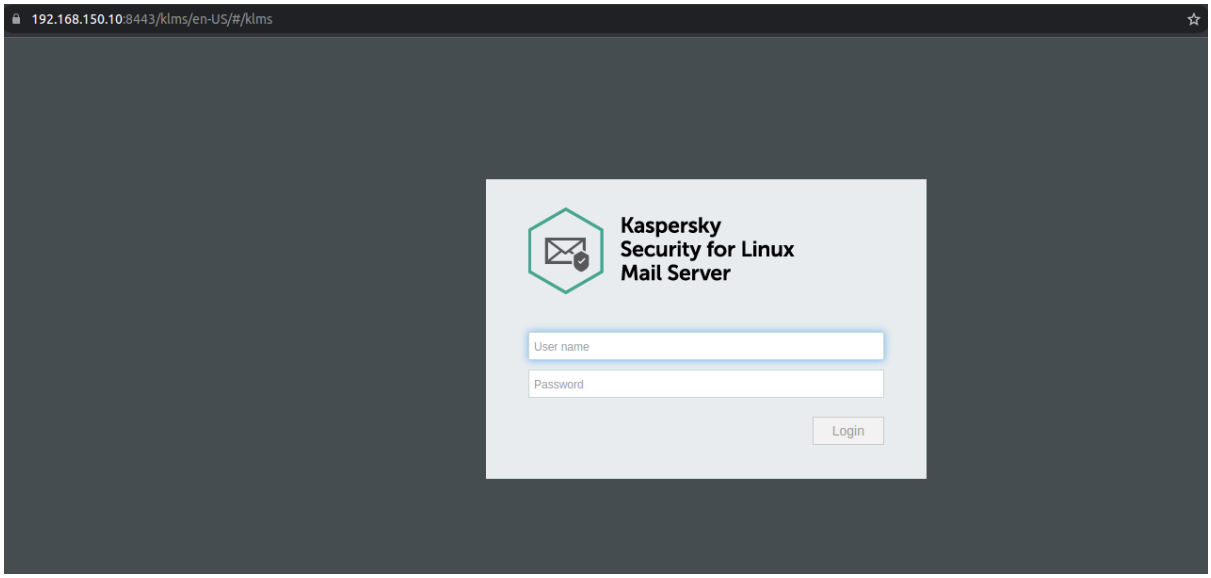
- Строчных букв;
- Заглавных букв;

- Специальных символов;
- Чисел.

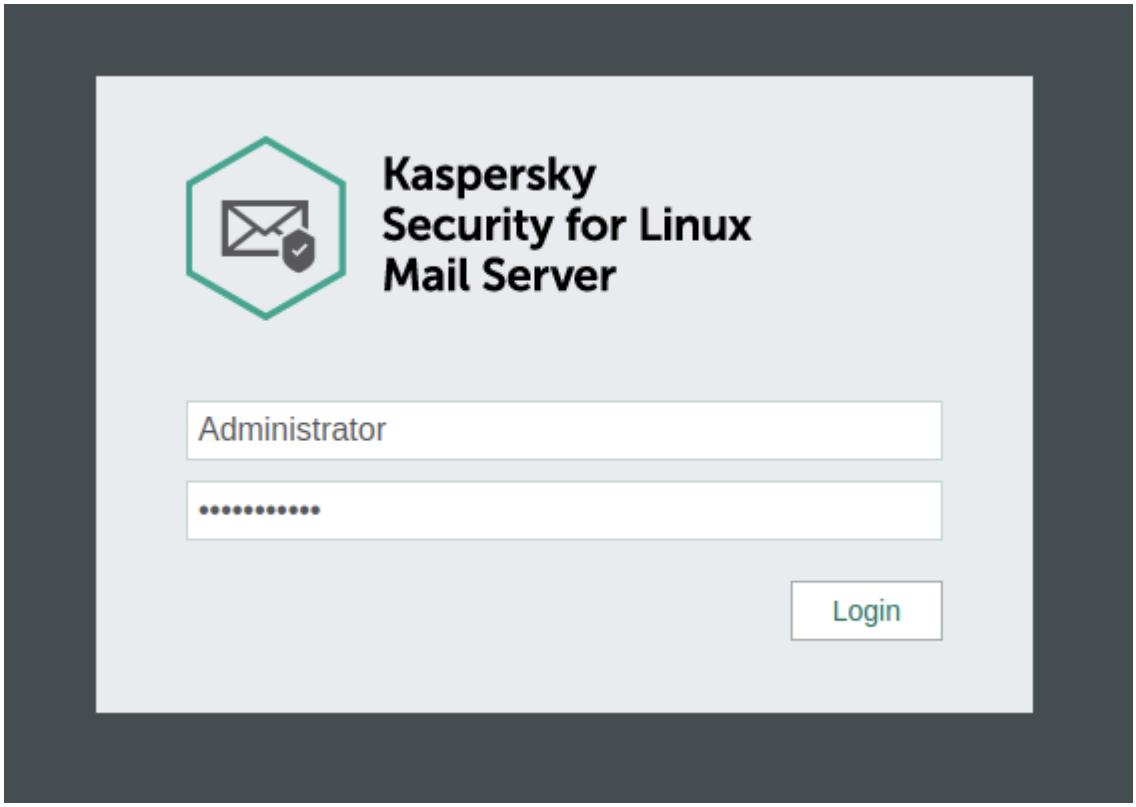
Терминал

```
[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 ~]#
```

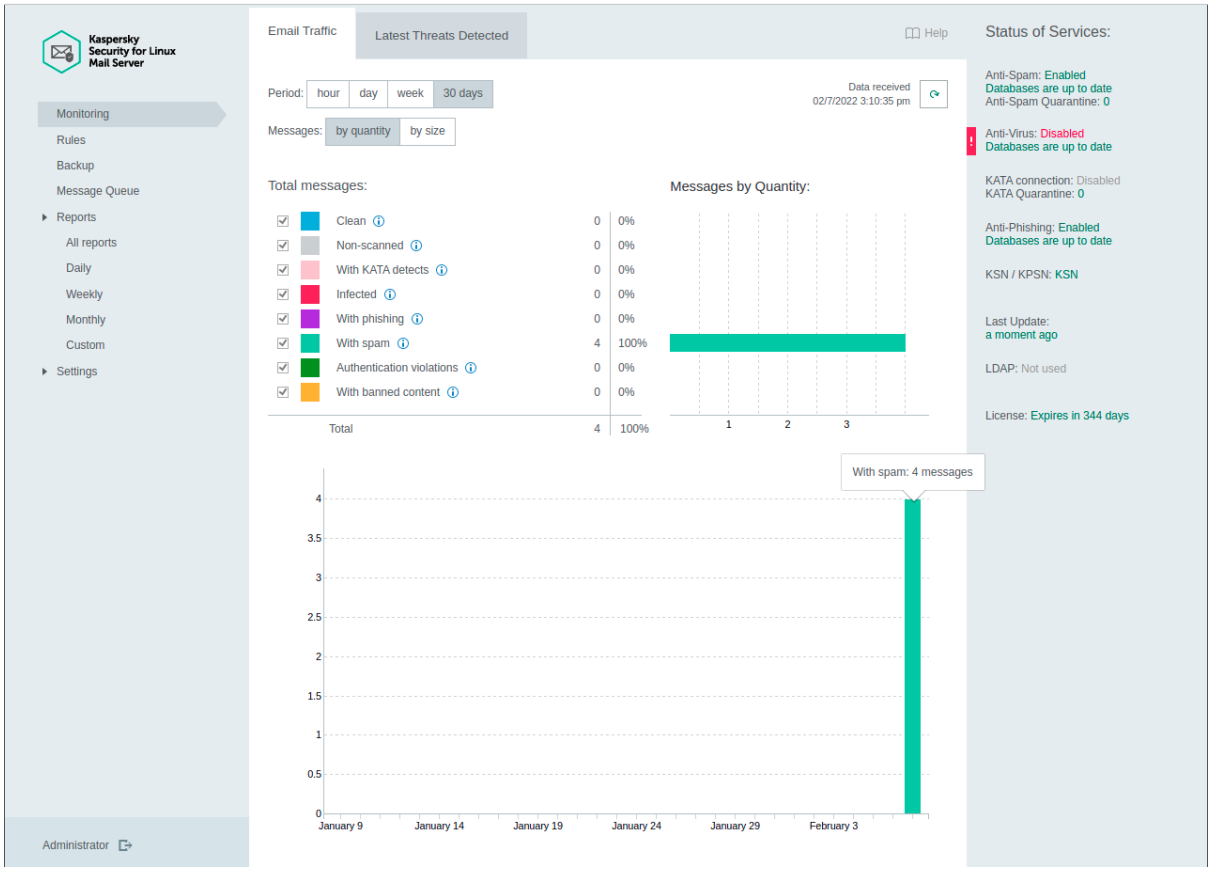
3. Для доступа к веб-интерфейсу перейдите в адресной строке по пути `ngfw_ip_address:8443/klms/`:



4. Войдите в веб-интерфейс с учетной записью **Administrator** и ранее заданным в терминале паролем:



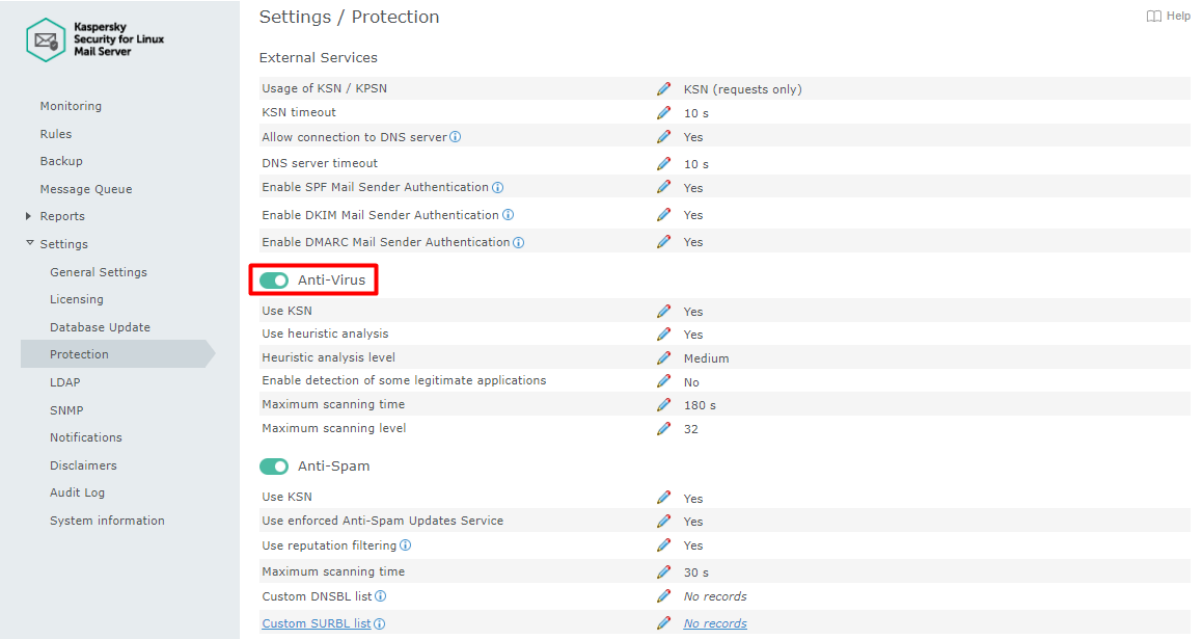
После успешного входа будет отображен дашборд со статистикой работы Антиспама:



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.

19.5 Правила

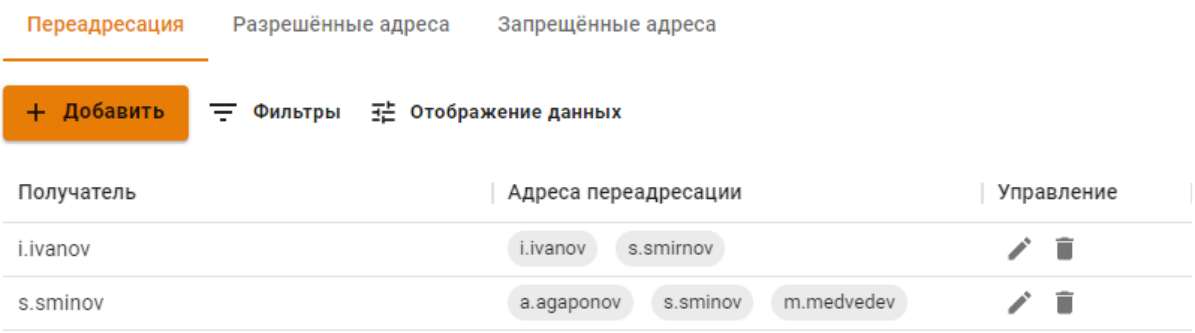
Раздел **Правила** состоит из трех вкладок: **Переадресация, Разрешенные адреса, Запрещенные адреса**.

19.5.1 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.

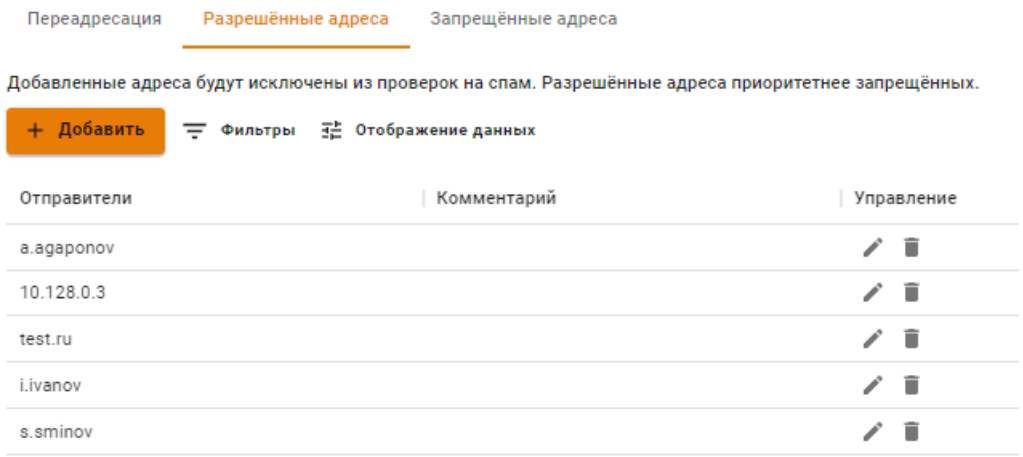
Подробнее с документацией по настройке почтовых алиасов на Ideco NGFW ознакомьтесь в статье *Переадресация почты*.



19.5.2 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.

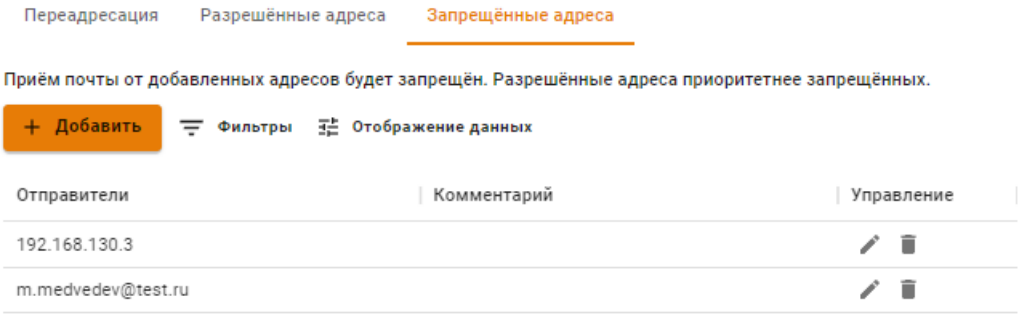
Еще один пример: в **Разрешенные адреса** внесен домен, в **Запрещенные адреса** - ящик из этого домена. Тогда письма с ящика будут заблокированы.

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.

19.5.3 Запрещенные адреса

Позволяет указывать почтовые домены и ящики, отправления с которых не будут приниматься сервером.



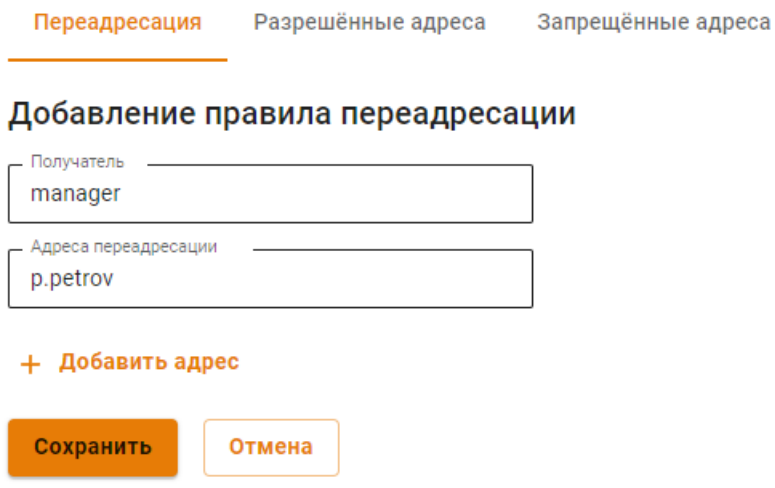
19.5.4 Переадресация почты

Чтобы создавать и редактировать почтовые правила переадресации (алиасы), перейдите в раздел **Почтовый релей -> Правила -> Переадресация**.

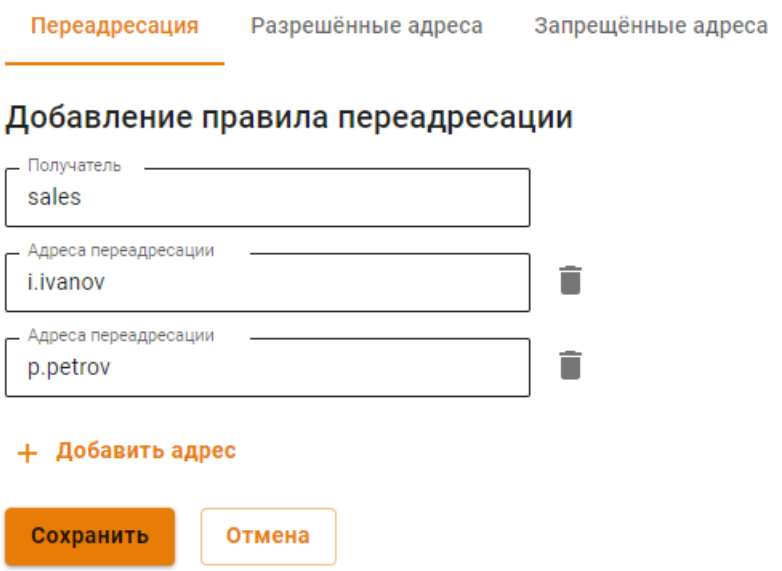
Почтовые алиасы отличаются от почтовых ящиков тем, что не требуют логинов и паролей. Они закрепляются за ящиком и служат его копией с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, можно сказать что алиас - это группа почтовых ящиков или группа рассылки. Поступающая на алиас 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:

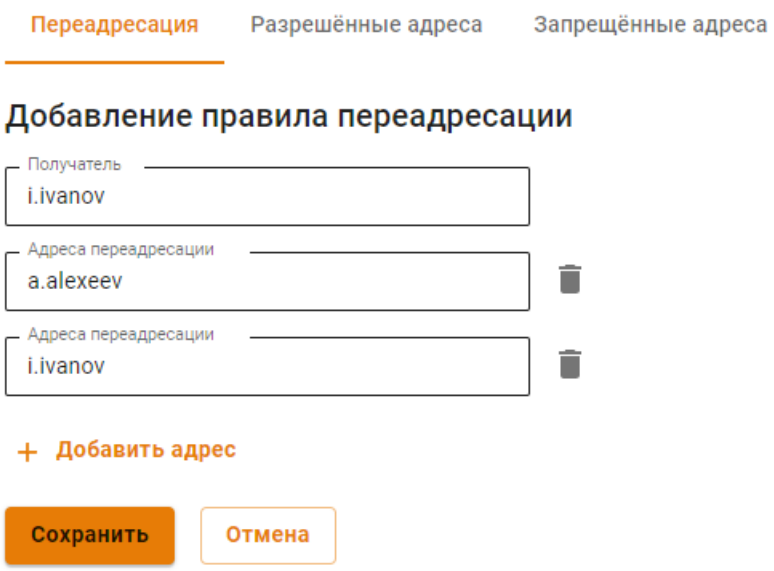
- Создать алиас `manager@yourdomain.ru` для ящика менеджера компании для связи с клиентами и партнерами, у которого реальный почтовый ящик имеет имя `p.petrov@yourmaildomain.ru`:



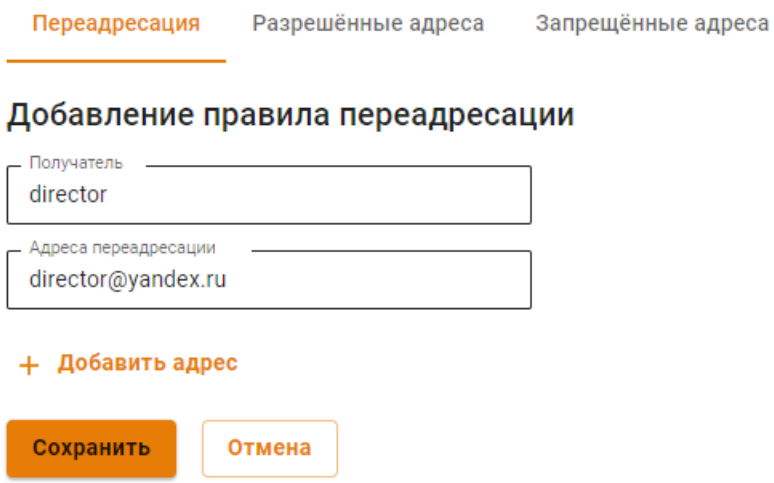
- Создать корпоративный алиас для отдела продаж `sales@yourmaildomail.ru`, чтобы почта пересылалась на всех сотрудников этого отдела:



- 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`:



Опишем, как будет работать почта при таких 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.

19.6 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.

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.

19.6.1 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.

19.7 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.

19.7.1 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**).

19.7.2 Настройка почтового клиента при работе из сети интернет

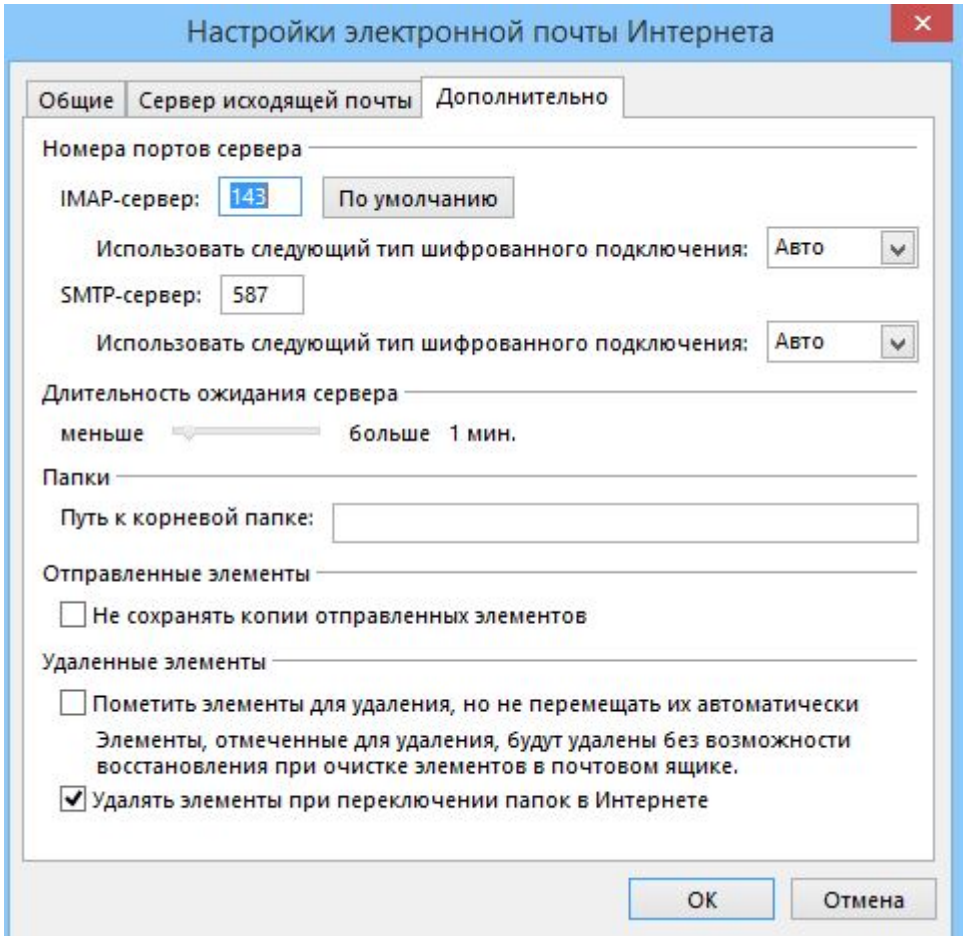
1. Сервер входящей почты работает на 995 TCP-порту (POP3S) и на 143 TCP-порту (IMAP-STARTTLS/SSL), шифрование обязательно:
   - В качестве логина прописывается логин от учетной записи пользователя;
   - В качестве пароля всегда прописывается пароль от учетной записи пользователя, сделать отдельный пароль 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**.

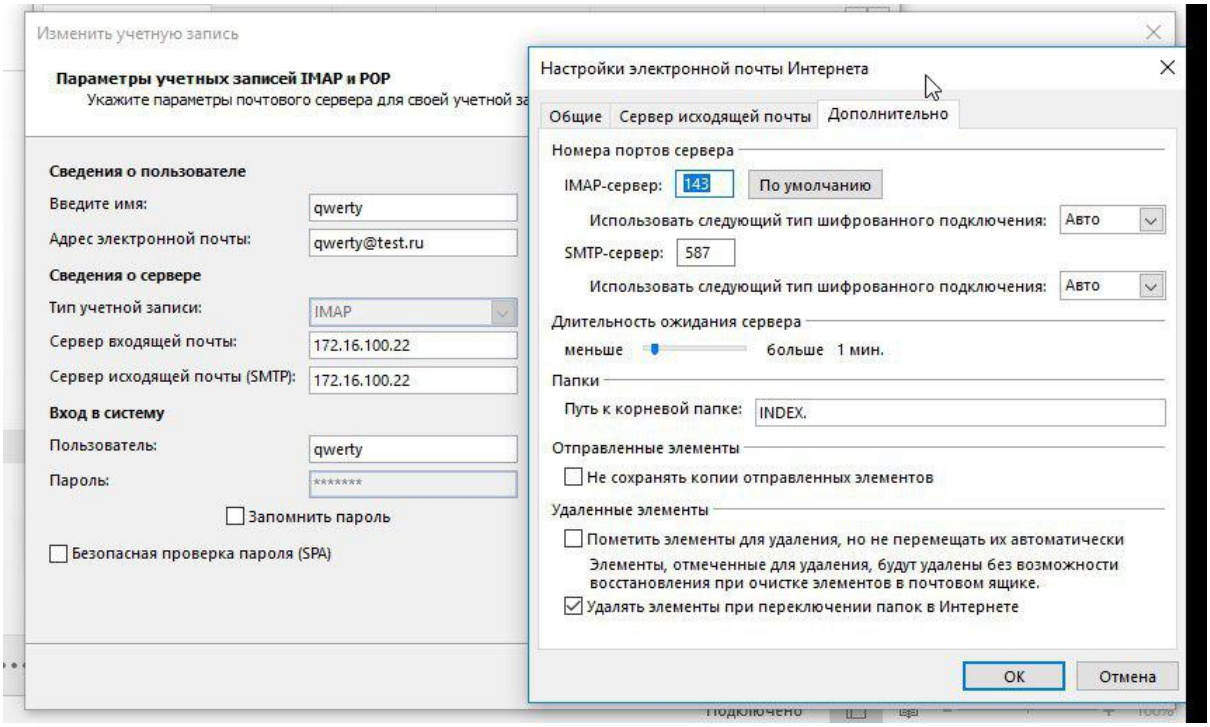
19.7.3 Примеры настроек популярных почтовых клиентов

Настройка почтового клиента Outlook 2013 и 2016:

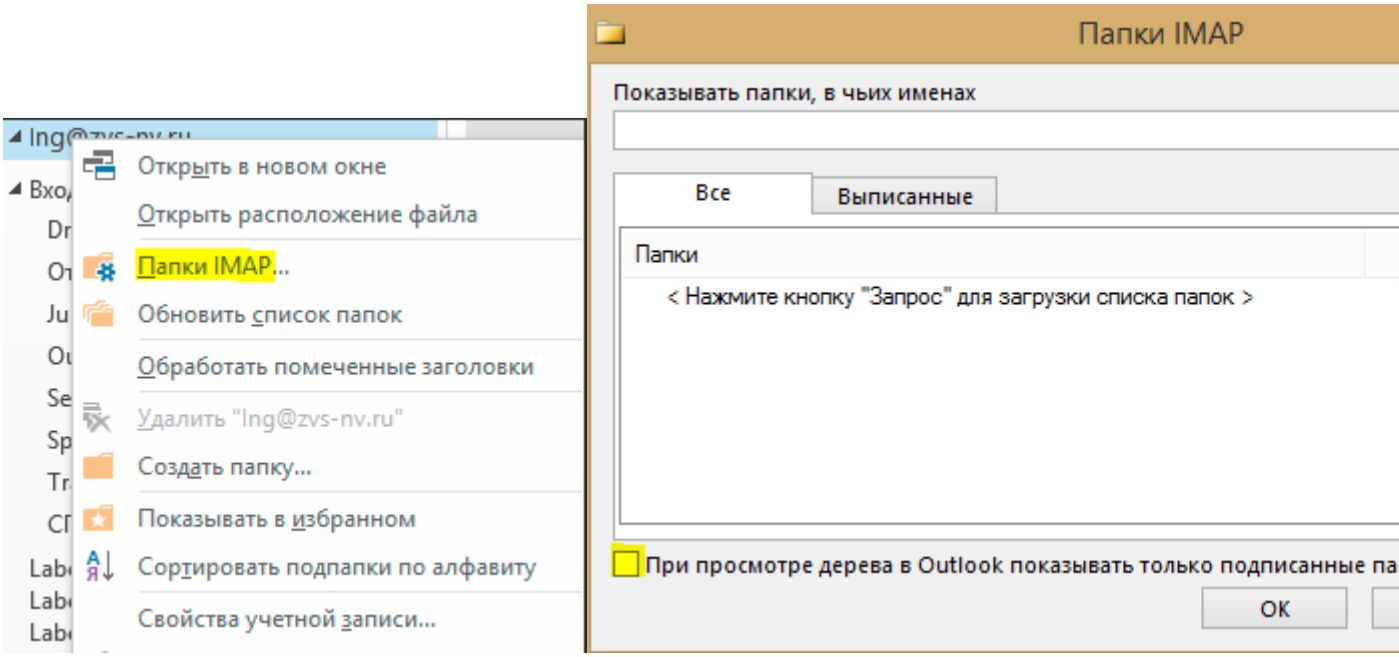
Пример настроек клиента Microsoft Outlook 2013 по протоколу IMAP:



Пример настроек клиента Microsoft Outlook 2016 по протоколу IMAP:



Для отображения IMAP-папок снимите галочку **При просмотре дерева в Outlook показывать только подписанные папки** в свойствах IMAP-папок:



Настройка почтового клиента iPhone:

Процесс настройки делится на два этапа:

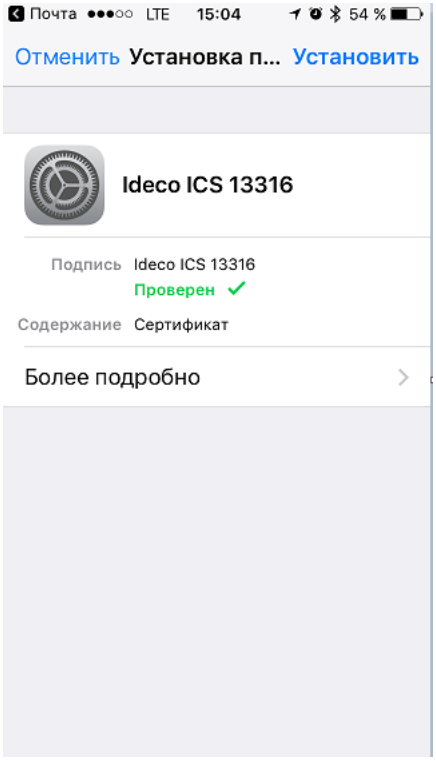
- Установка корневого SSL-сертификат NGFW;
- Настройка почтового ящика.

Установка корневого SSL-сертификат NGFW:

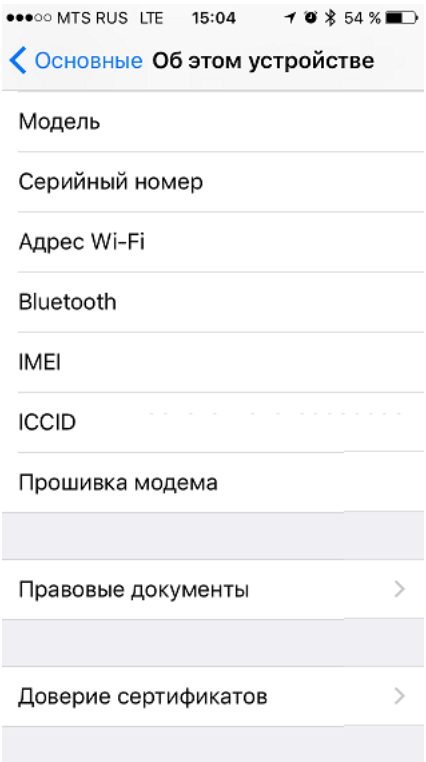
1. Скачайте сертификат в разделе **Сервисы -> Сертификаты** и перенесите на настраиваемое устройство (например, отправив по почте).

2. Нажмите кнопку **Установить**.

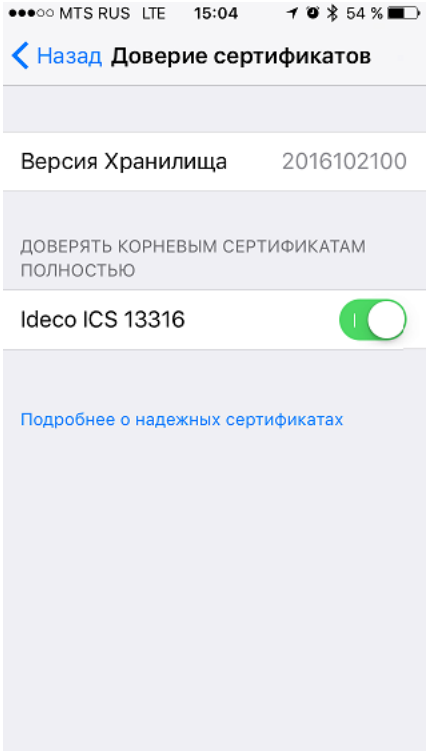
3. Зайдите в раздел **Настройки -> Основные**.



4. Выберите **Об этом устройстве -> Доверие сертификатов**:

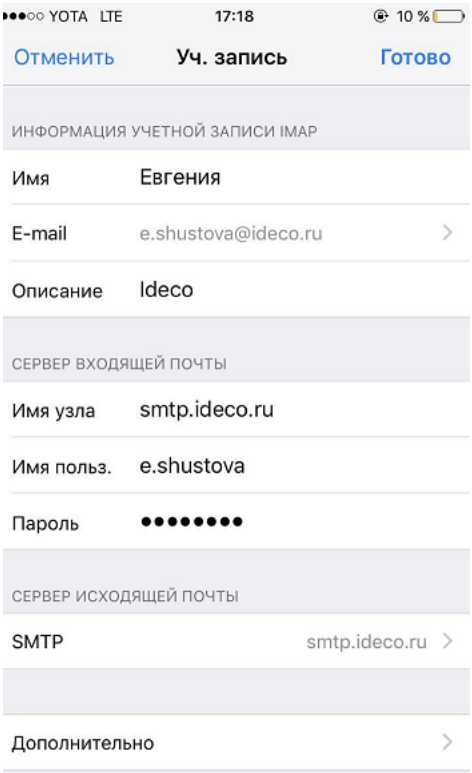


5. Включите настройку **Доверять корневым сертификатам полностью**

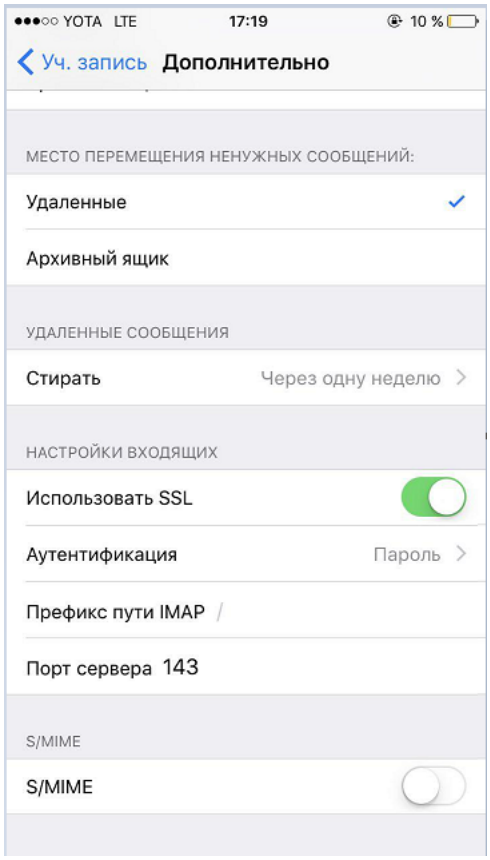


Настройка почтового ящика:

1. Перейдите в Учетную запись почты и нажмите **Дополнительно**:



2. Скорректируйте настройки:



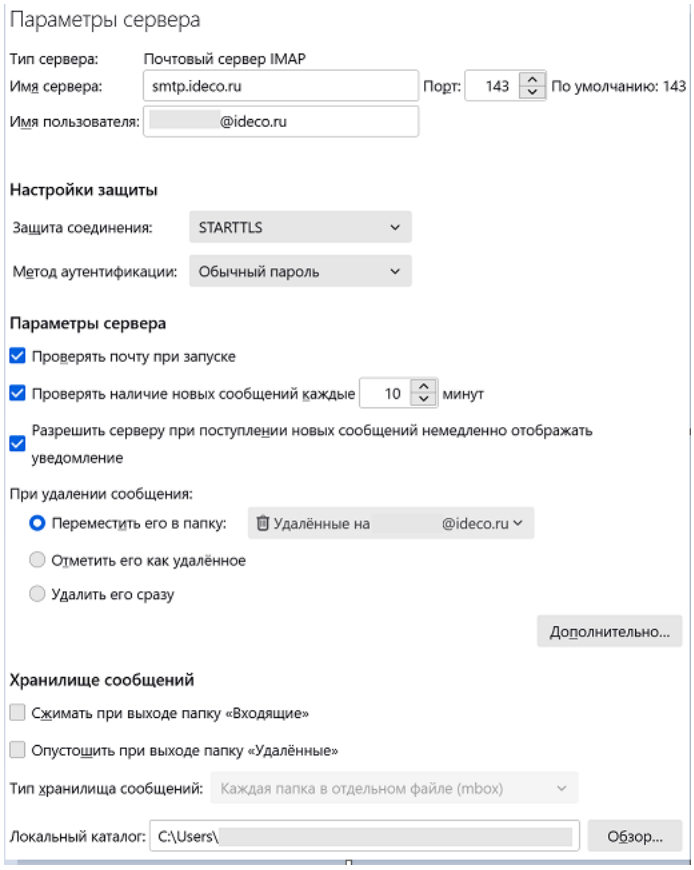
Настройка почтового клиента Thunderbird:

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*.

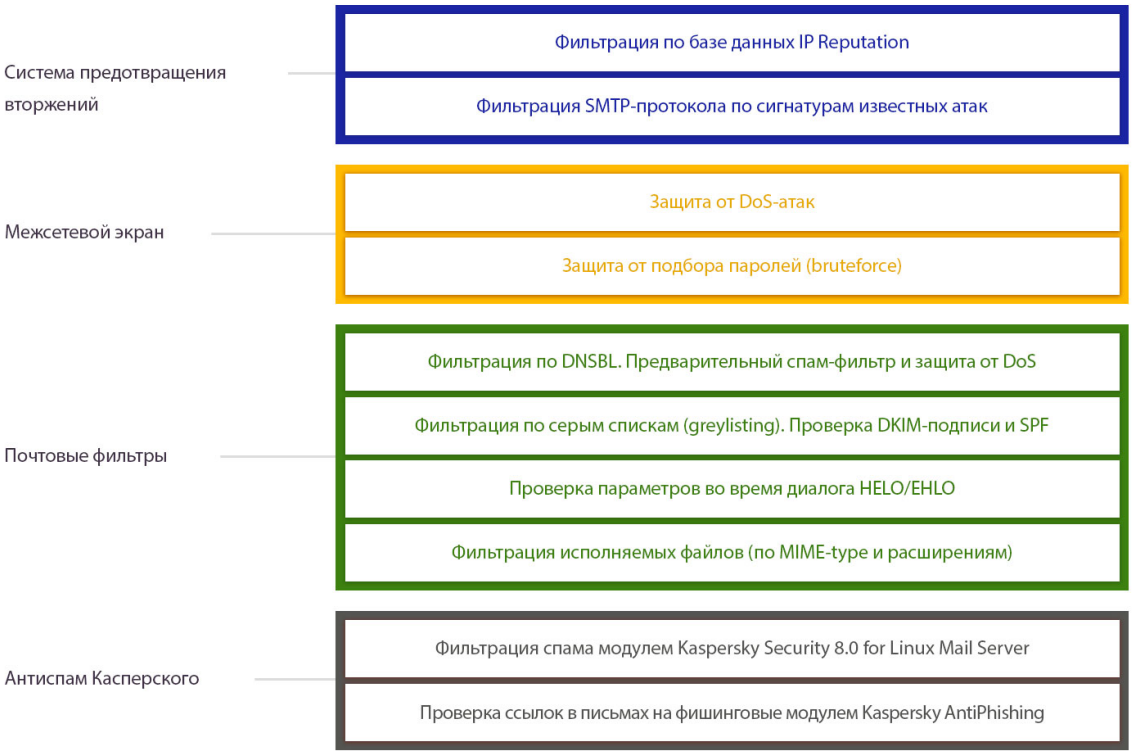


19.8 Схема фильтрации почтового трафика

19.8.1 Основное

Полная схема и последовательность фильтрации представлена на схеме.

IDECO UTM: СХЕМА ФИЛЬТРАЦИИ ЭЛЕКТРОННОЙ ПОЧТЫ



Модуль Антиспама Касперского использует собственный набор методик для фильтрации спама. Он обеспечивает высокий уровень детектирования спама при низких значениях ложных срабатываний (0,003-0,005% от общего количества сообщений). Для защиты пользователей используется большой 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.

20. Публикация ресурсов

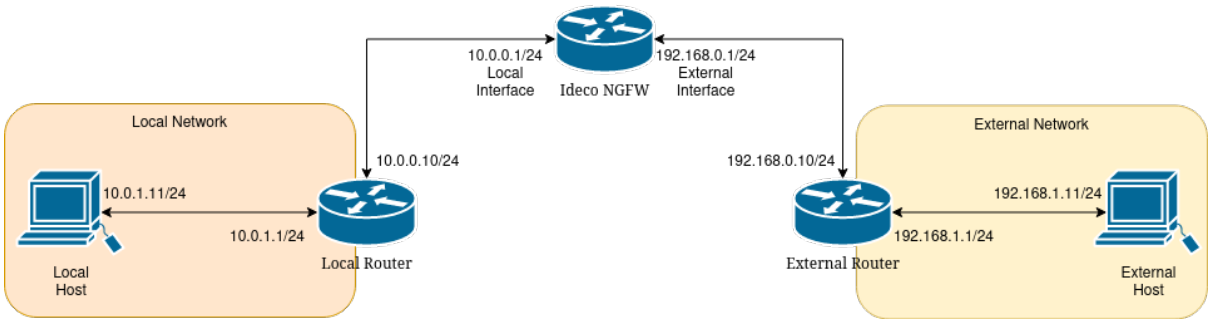
20.1 Доступ из внешней сети без NAT

20.1.1 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:

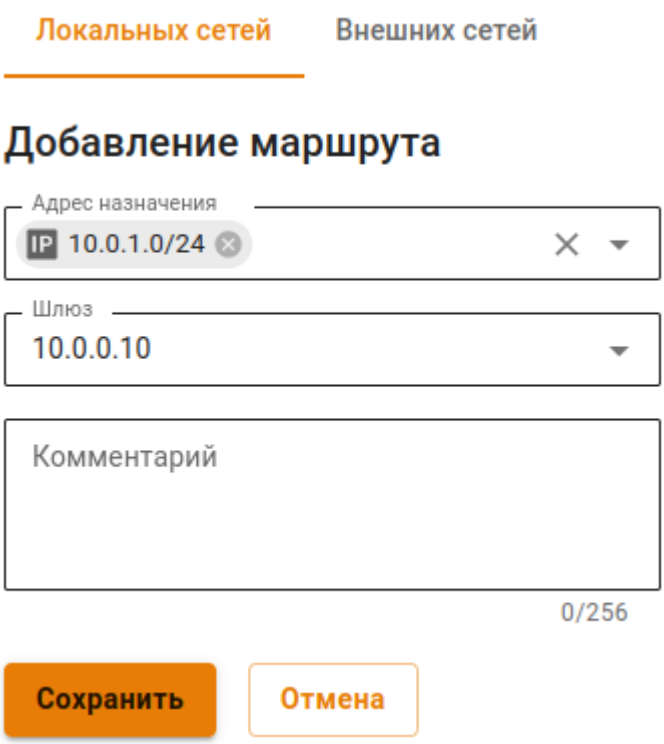


1. Настройте сетевые интерфейсы в разделе **Сервисы -> Сетевые интерфейсы** на Ideco NGFW:

- **local** - интерфейс для доступа в пользовательскую локальную сеть;
- **external** - интерфейс для доступа в пользовательскую внешнюю сеть пользователей.

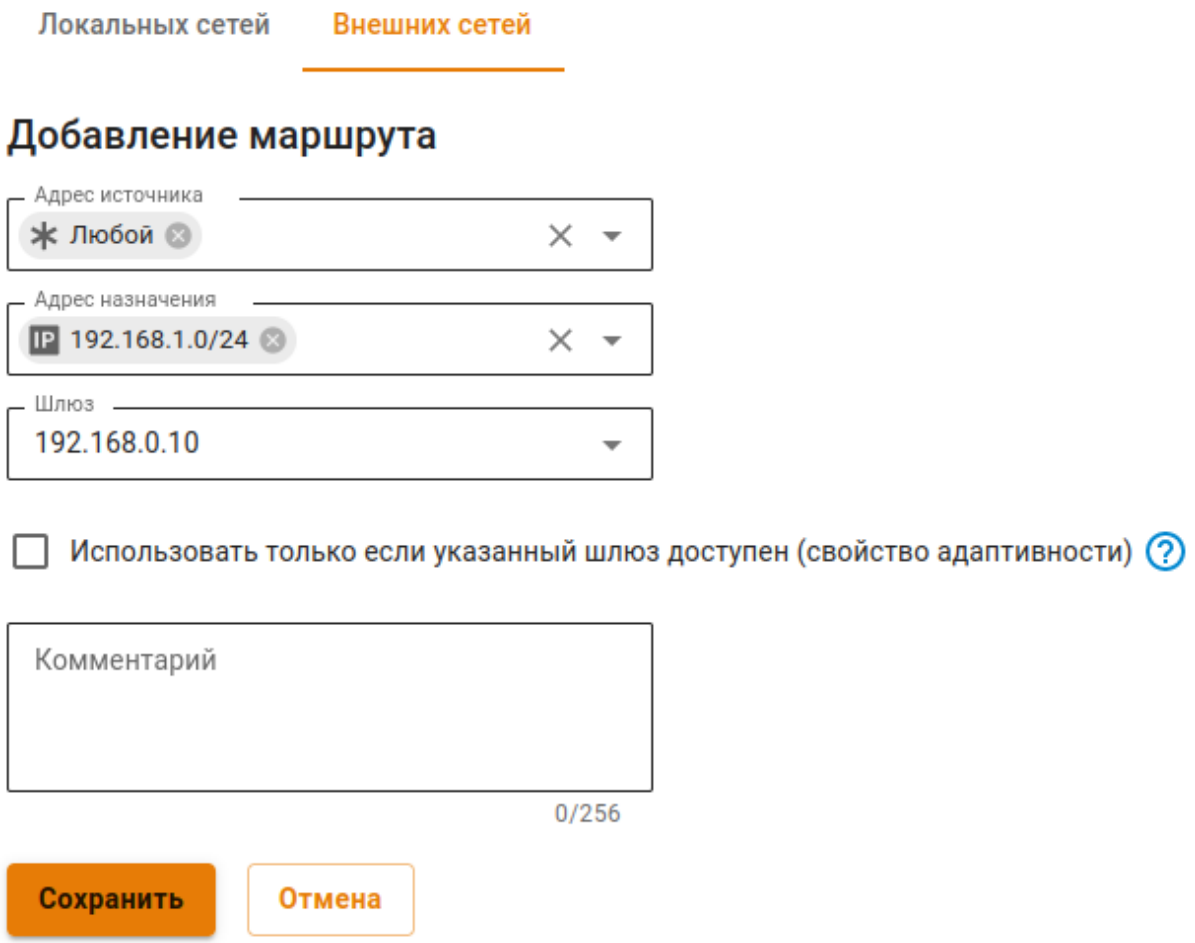
2. Перейдите в раздел **Сервисы -> Маршрутизация** и создайте правила для доступа к IP-адресам пользователей, которые находятся за маршрутизаторами:

- Для **Локальных сетей**:
  - **Адрес назначения** - адрес локальной сети за маршрутизатором (`10.0.1.0/24`);
  - **Шлюз** - адрес машрутизатора (`10.0.0.10`).

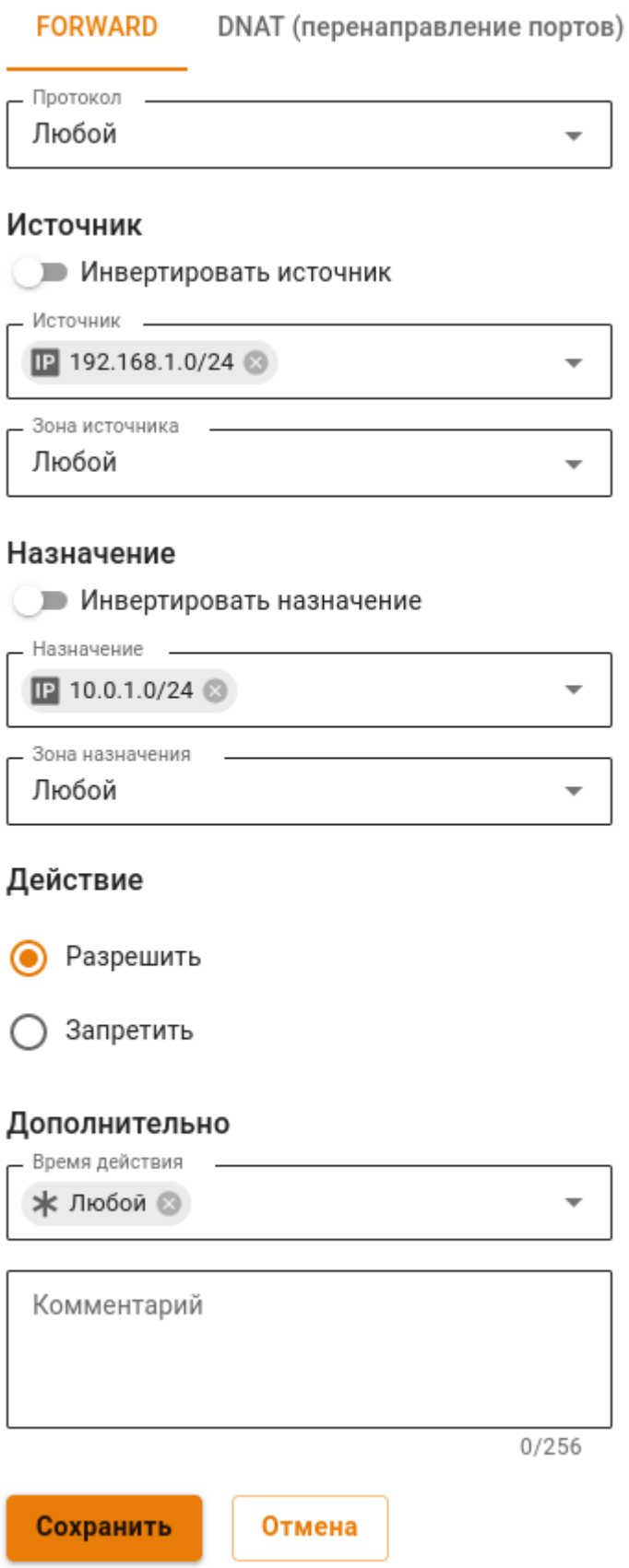


- Для **Внешних сетей**:
  - **Источник** - Любой;
  - **Адрес назначения** - адрес внешней сети за маршрутизатором (`192.168.1.0/24`);

– **Шлюз** - адрес машрутизатора (`192.168.0.10`).



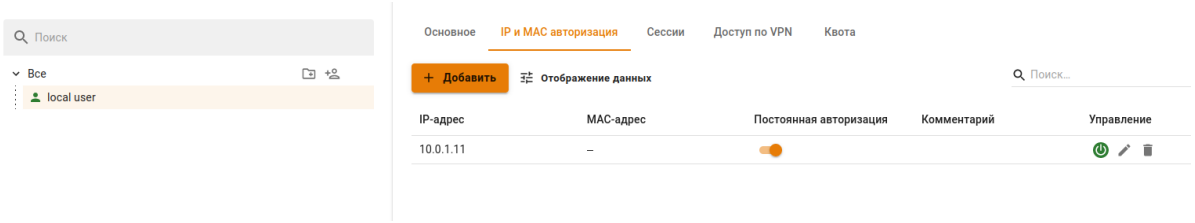
3. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD** и создайте правило для доступа хостов из внешней сети `192.168.1.0/24` до IP-адресов пользователей локальной сети `10.0.1.0/24`:



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.

20.2 Публикация веб-приложений (обратный прокси-сервер)

20.2.1 Основное

Публикация веб-серверов возможна через *обратный прокси сервер*.

20.3 Настройка публичного IP-адреса на компьютере в локальной сети

20.3.1 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.

20.4 Портмаппинг (проброс портов, DNAT)

20.4.1 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 на вкладке DNAT файрвола. При создании правила укажите адреса сервера, публикуемой машины и сетевого порта, с которого и на который осуществляется трансляция сетевых запросов извне.

Подсказка: Не рекомендуется использовать проброс портов для публикации веб- и почтовых серверов (80, 443 порты). Для их публикации воспользуйтесь *обратным прокси-сервером*.

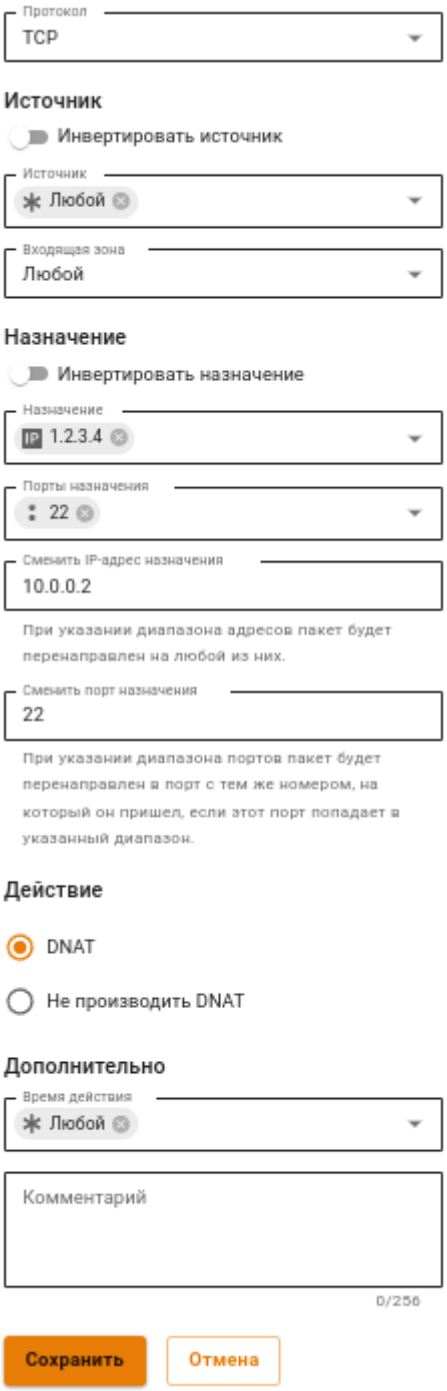
Создание правил DNAT в файрволе Ideco NGFW:

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 (перенаправление портов)** и нажмите **Добавить** в правом верхнем углу экрана, чтобы создать правило трансляции портов (DNAT).

Заполните поля в соответствии с характеристиками, указанными в примере:



После сохранения созданное правило будет выглядеть следующим образом:

Настройки файрвола применяются сразу при создании правила.

Частые ошибки:

- Если на хосте в локальной сети, куда осуществляется проброс порта, в качестве шлюза по умолчанию указан не Ideco NGFW, установить подключение не получится. Шлюзом по умолчанию устанавливается IP-адрес локального интерфейса Ideco NGFW. При подключении с определенного IP-адреса (сети) на устройстве прописывается маршрут, чтобы ответы для этого IP-адреса (сети) направлялись через IP-адрес локального интерфейса Ideco NGFW;
- 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 машрутизации 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;

- Трафик проброшенных портов проверяется модулем *Предотвращение вторжений*. Проверьте логи системы в случае неработоспособности правила и при необходимости добавьте в исключения сработавшее правило.

21. Интеграция NGFW и SkyDNS

Подсказка: Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

21.1 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.

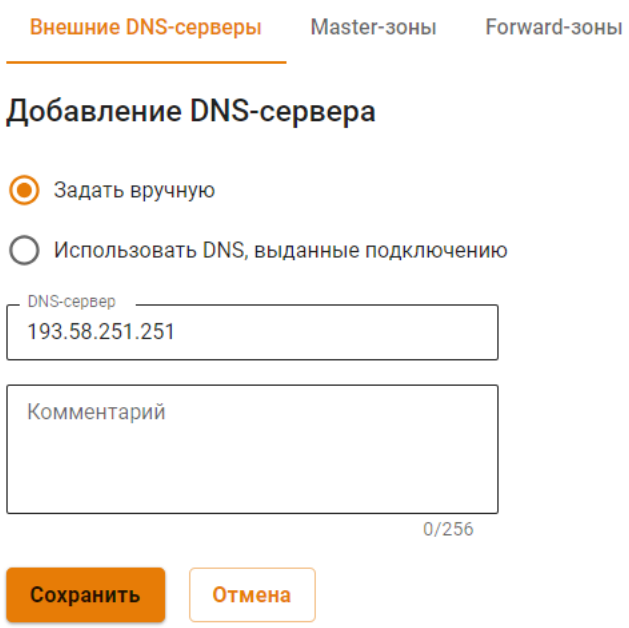
Подсказка: Специально для школ и колледжей можно приобрести комплект Шлюз безопасности Ideco NGFW + контент-фильтр SkyDNS.

21.2 Настройка интеграции Ideco NGFW и SkyDNS

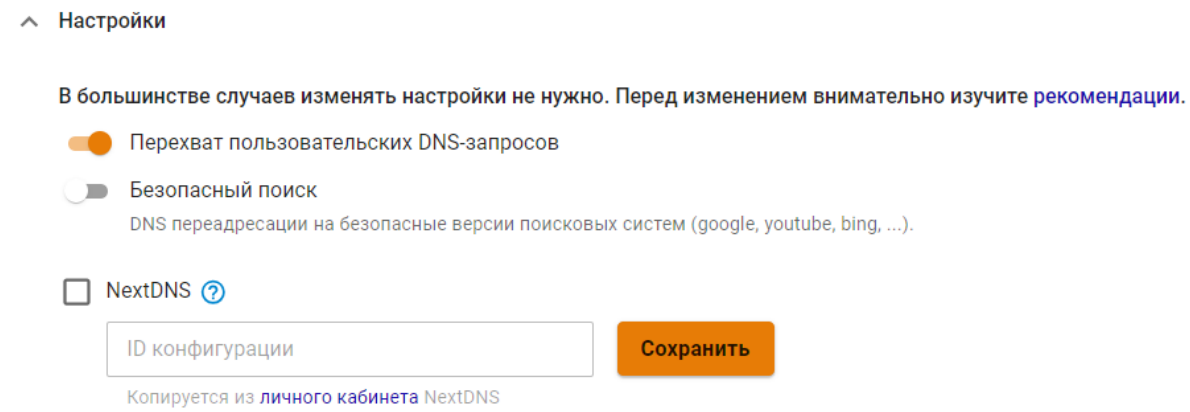
Чтобы настроить интеграцию со SkyDNS, выполните действия:

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 **Сохранить**:

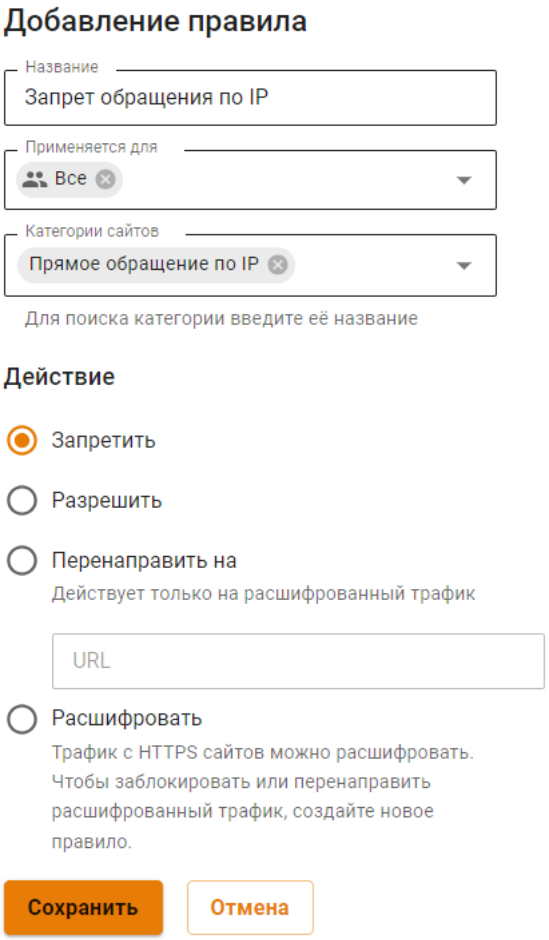


3. В настройках DNS включите опцию **Перехват пользовательских DNS-запросов** для запрета обращения к другим DNS-серверам (если фильтрация через SkyDNS обязательна для всей сети):



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.

21.3 Документация по настройке и активации сервиса SkyDNS

Документация доступна на сайте сервиса.

По вопросам настройки сервиса обращайтесь в техническую поддержку SkyDNS.

21.4 Схема фильтрации веб-трафика при использовании SkyDNS

22. FAQ

22.1 Как заблокировать чат-боты?

Заблокировать чат-боты можно, создав правило в Контент-фильтре. О том, как это сделать, написано в статье *Блокировка чат-ботов*.

22.2 Как настроить совместную работу ViPNet-Координатора с Ideco NGFW ?

Процесс настройки подробно описан в *статье*.

22.3 Как настроить автоматическую аутентификацию на Linux через веб-интерфейс ?

Процесс настройки подробно описан в статье *Настройка автоматической аутентификации на NGFW на Linux*. Данный скрипт подходит для всех Linux-систем с Python 3.5 и выше.

22.4 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*.

22.5 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*.

22.6 Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW?

Порядок обработки веб-трафика и примеры проверки работоспособности модулей описаны в *статье*.

22.7 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.

22.8 Как создать VPN-подключение?

В зависимости от операционной системы выберите подходящую инструкцию из *Инструкций по созданию VPN-подключений*.

22.9 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*.

22.10 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*.

22.11 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*.

22.12 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*.

22.13 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.

22.14 Как подобрать аппаратную платформу для Ideco NGFW?

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 37 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 37. Подробнее в статье *Выбор аппаратной платформы для Ideco NGFW*.

22.15 Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW?

Для настройки Ideco NGFW воспользуйтесь рекомендациями из статьи *Поддержка устаревших алгоритмов шифрования*.

22.16 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*.

22.17 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*.

22.18 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.

22.19 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*.

22.20 Инструкции по созданию VPN-подключений

22.20.1 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.

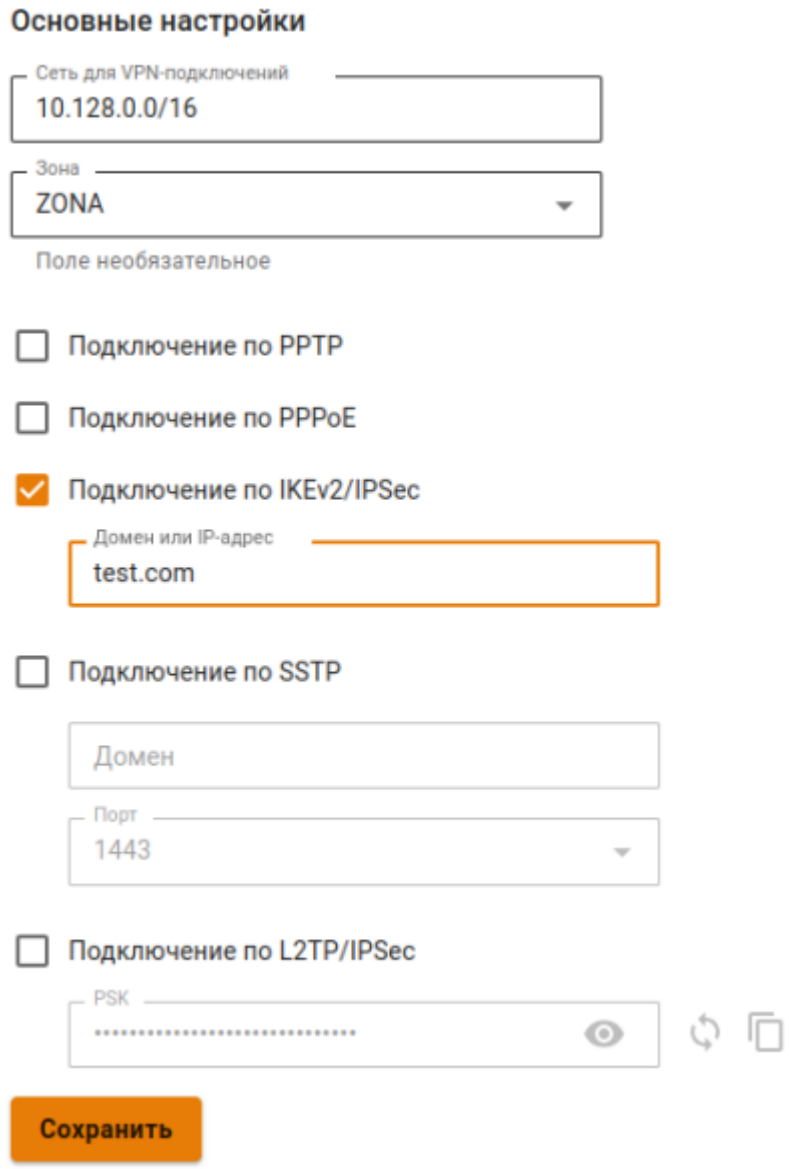
> **Предупреждение:** Не рекомендуем использовать для VPN-подключений кириллические логины.

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:

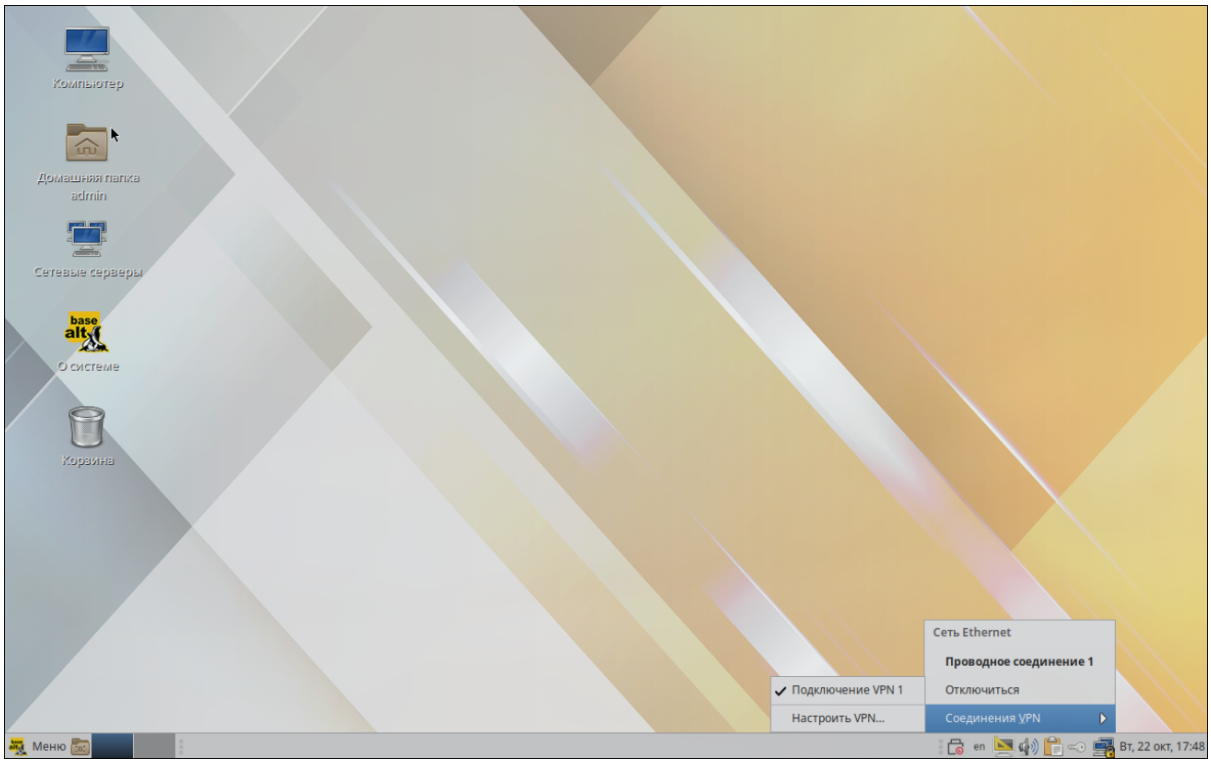
```
apt-get update && apt-get dist-upgrade && apt-get install NetworkManager-strongswan␣
↪NetworkManager-strongswan-gnome strongswan strongswan-charon-nm strongswan-testing
```

2. Установите корневой сертификат на рабочую станцию:

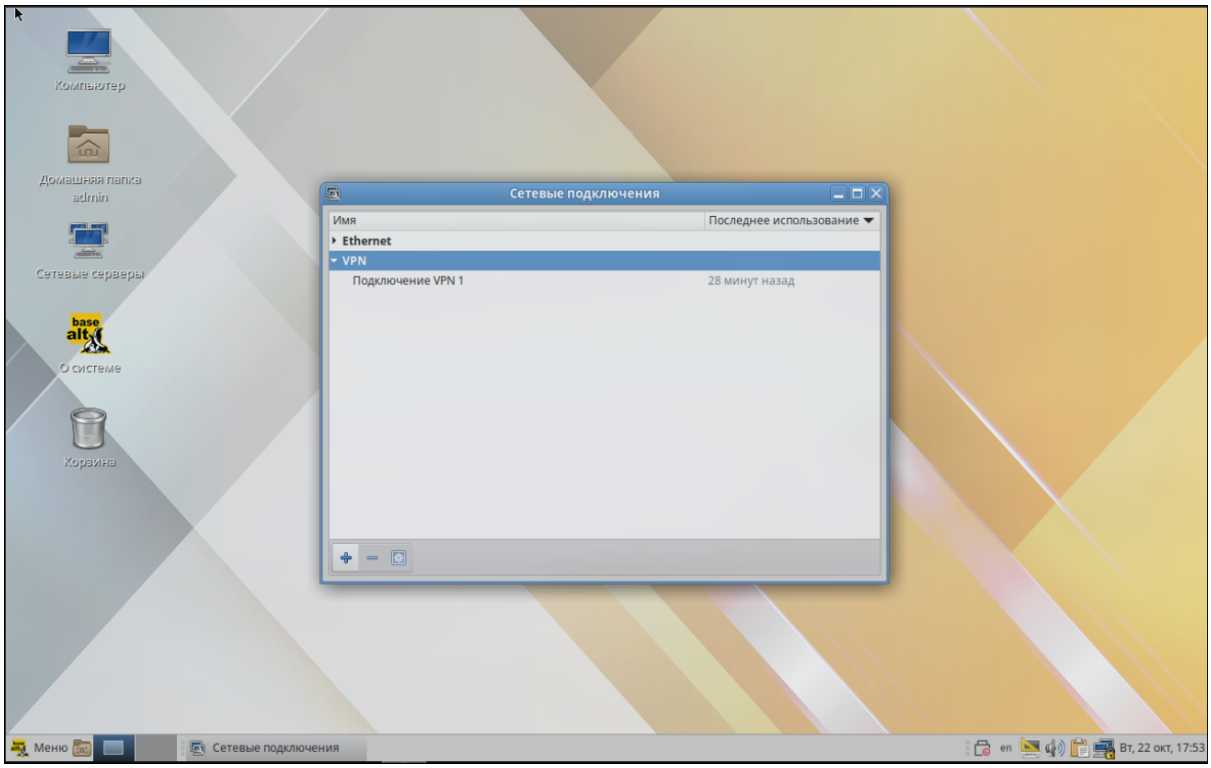
```
cp root-ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

- `root-ca.crt` - путь к сертификату.

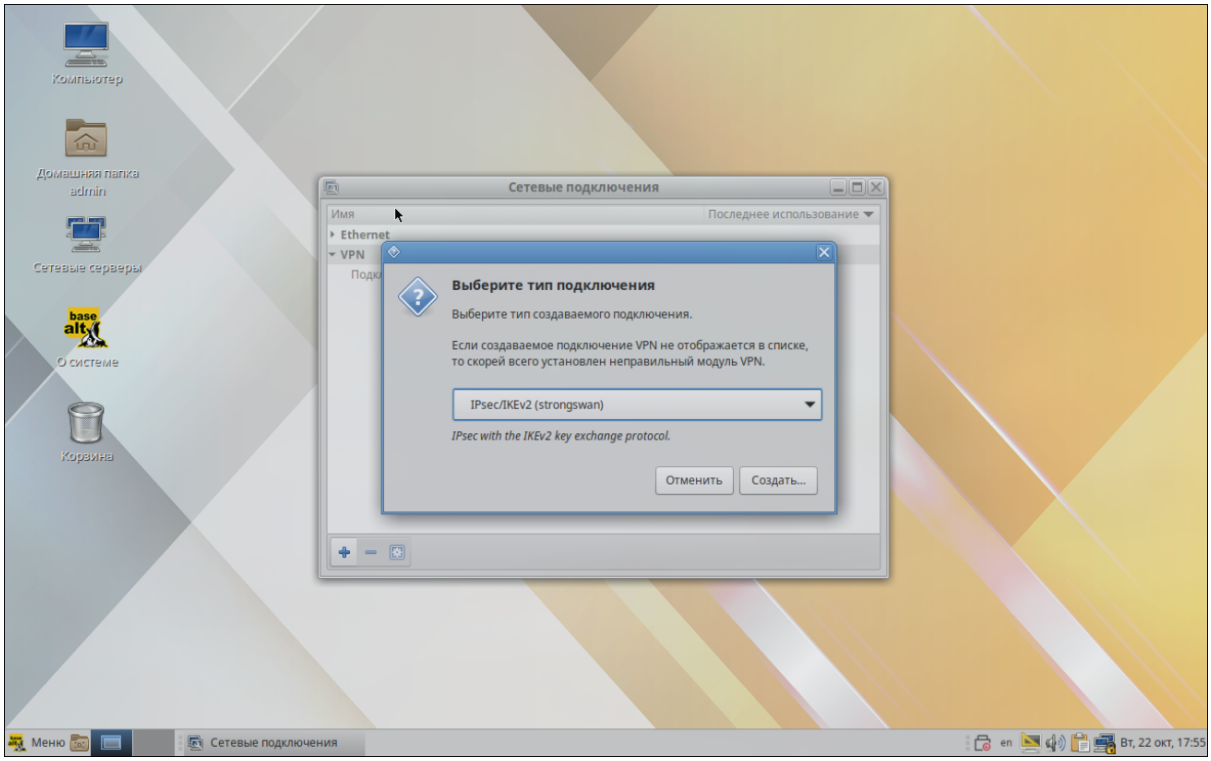
3. Перейдите в **Соединения VPN** и нажмите **Настроить VPN**:



4. Добавьте новое VPN-подключение:

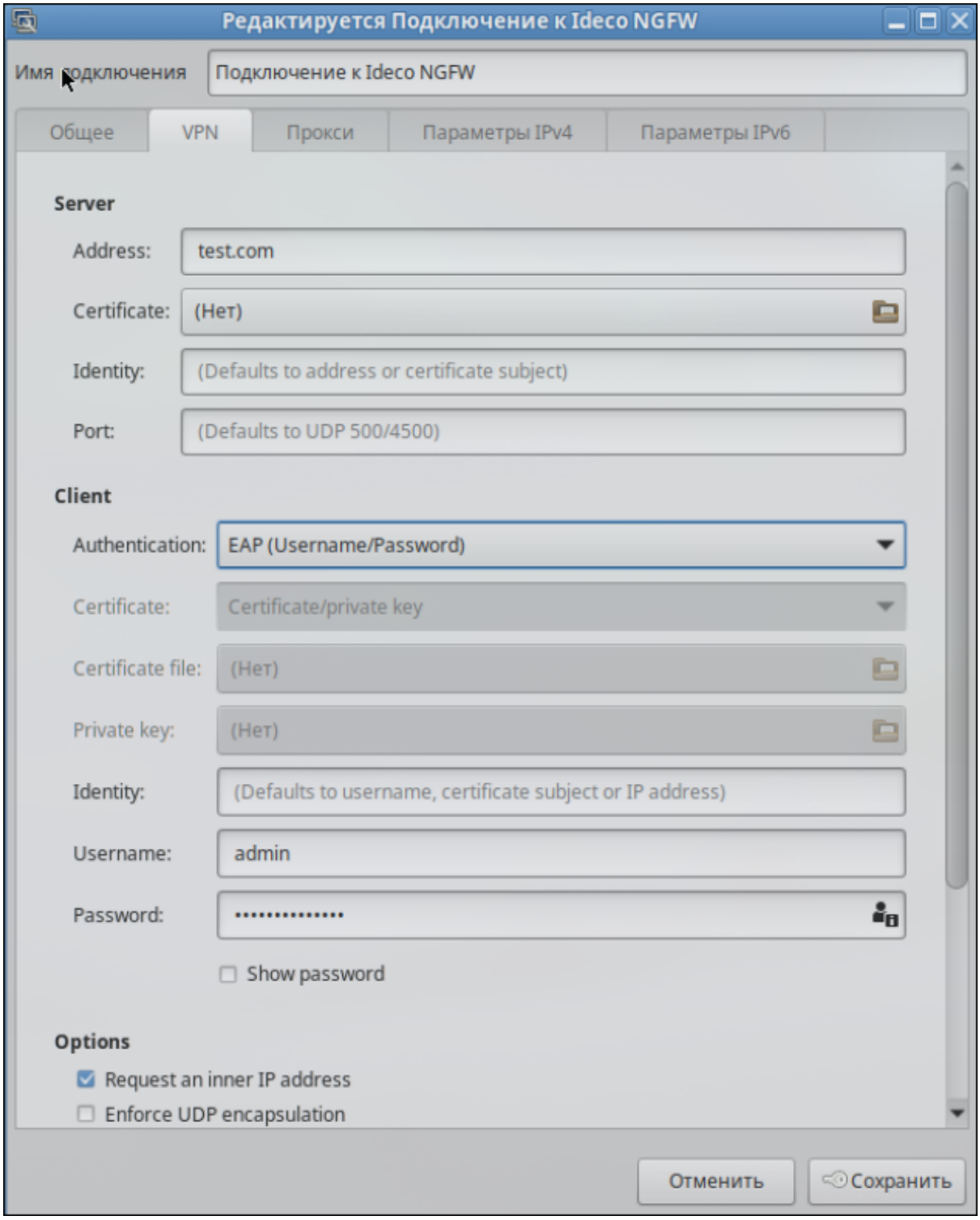


5. Выберите тип VPN-подключения `IPsec/IKEv2 (strongswan)` и нажмите **Создать**:

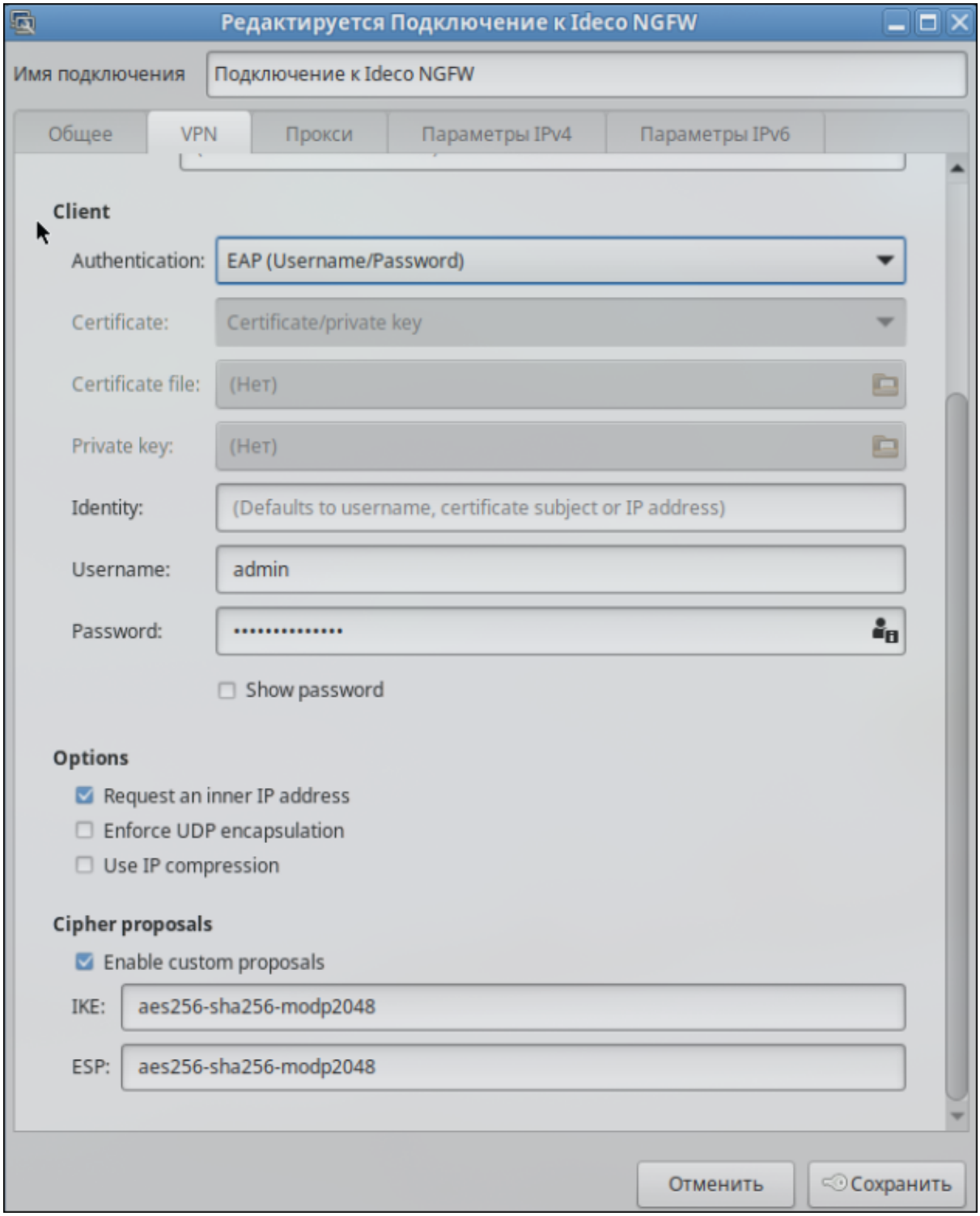


6. Заполните необходимые поля для создания VPN-подключения, как на скриншоте:

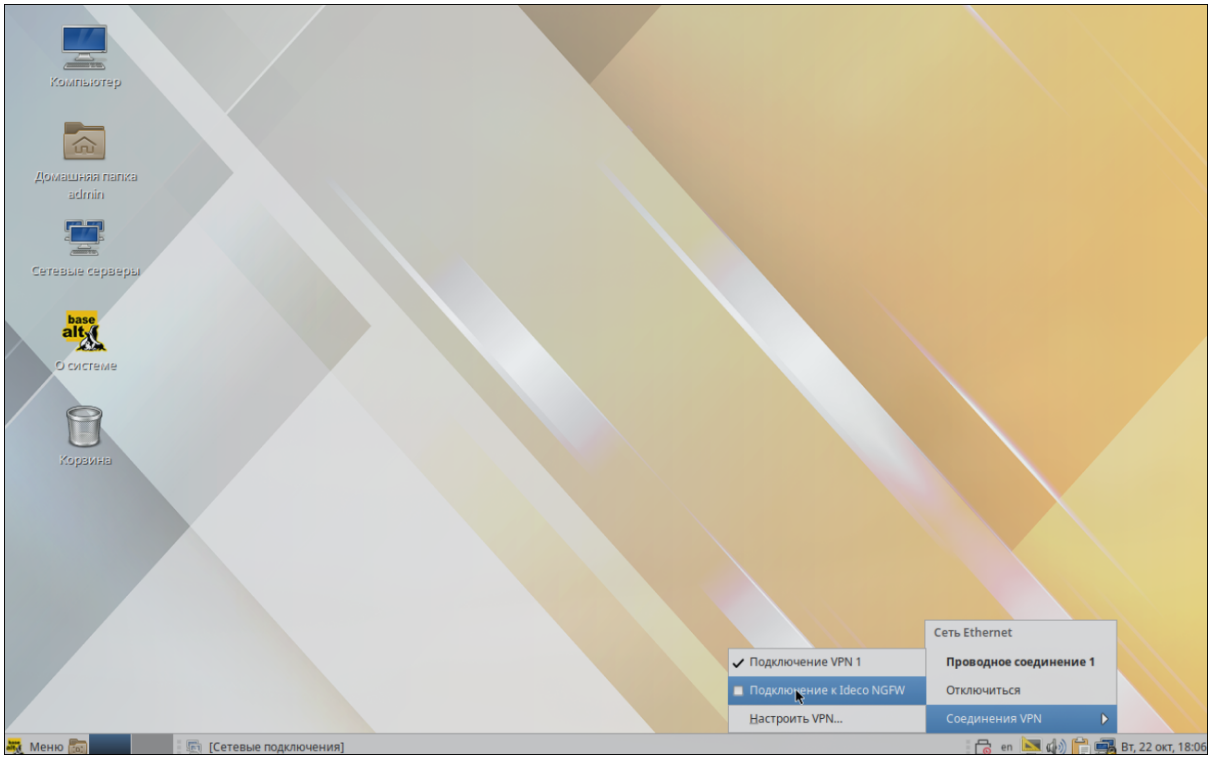
- Address - адрес шлюза;
- Authentication - тип аутентификации;
- Username - логин пользователя на Ideco NGFW;
- Password - пароль пользователя на Ideco NGFW.



7. Заполните параметры шифрования, как на скриншоте, и нажмите **Сохранить**:



8. Включите созданное VPN-подключение:



22.20.2 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.

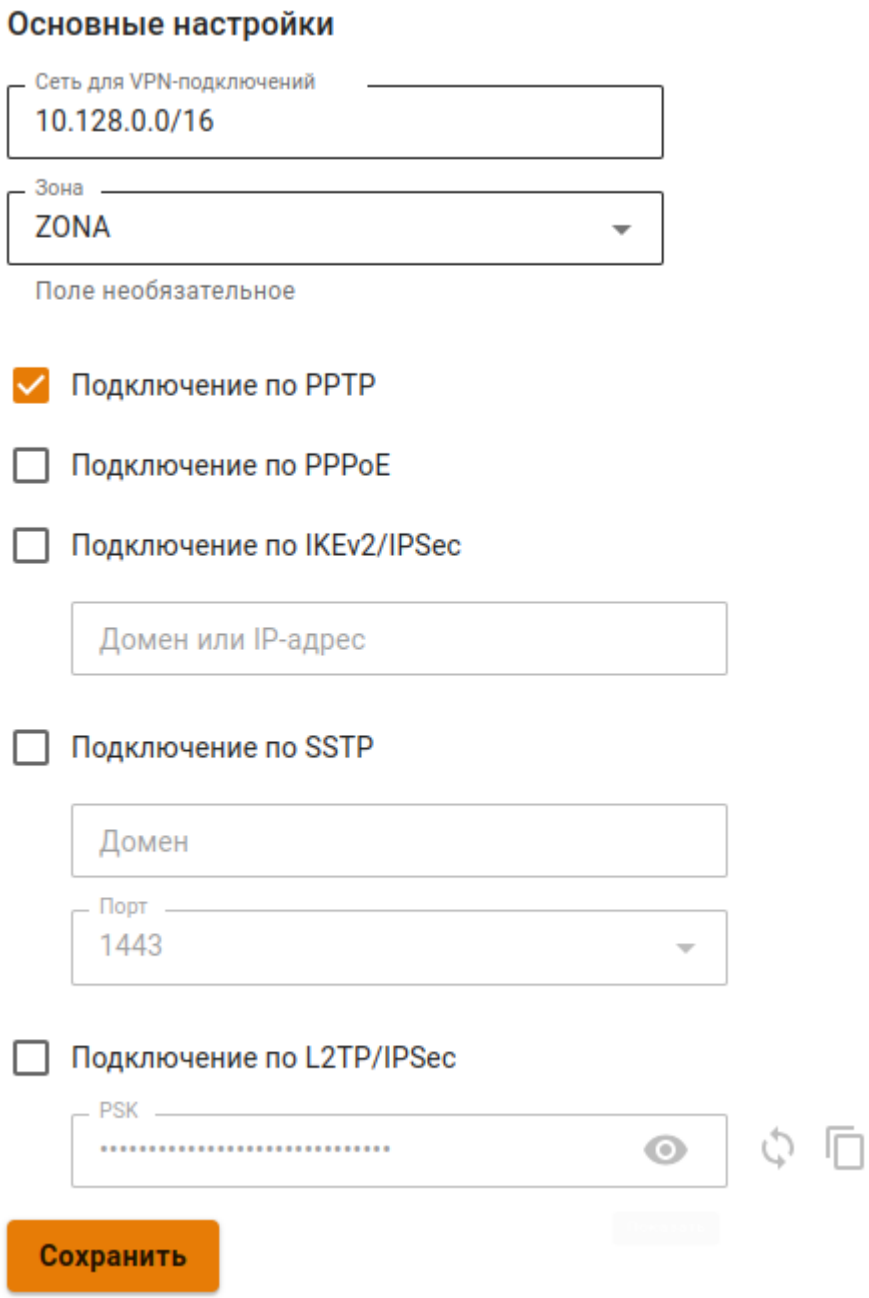
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Предупреждение: Инструкция актуальна для версии Ubuntu 24.04 LTS.

Протокол PPTP:

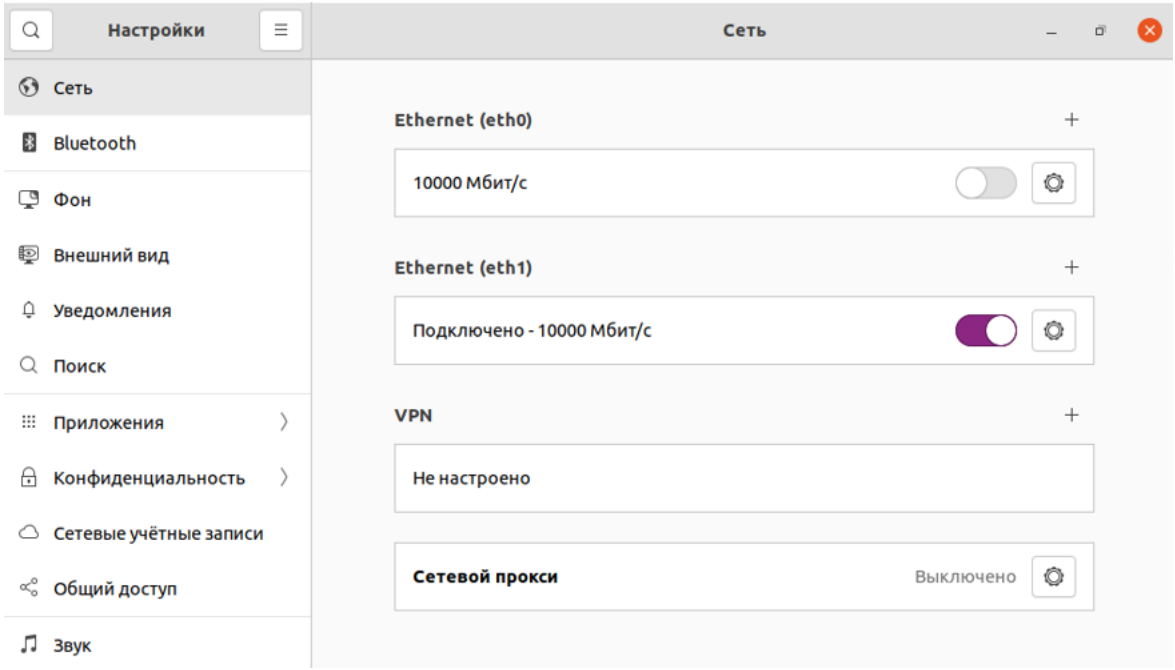
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное** и установите флаг **Подключение по PPTP**:

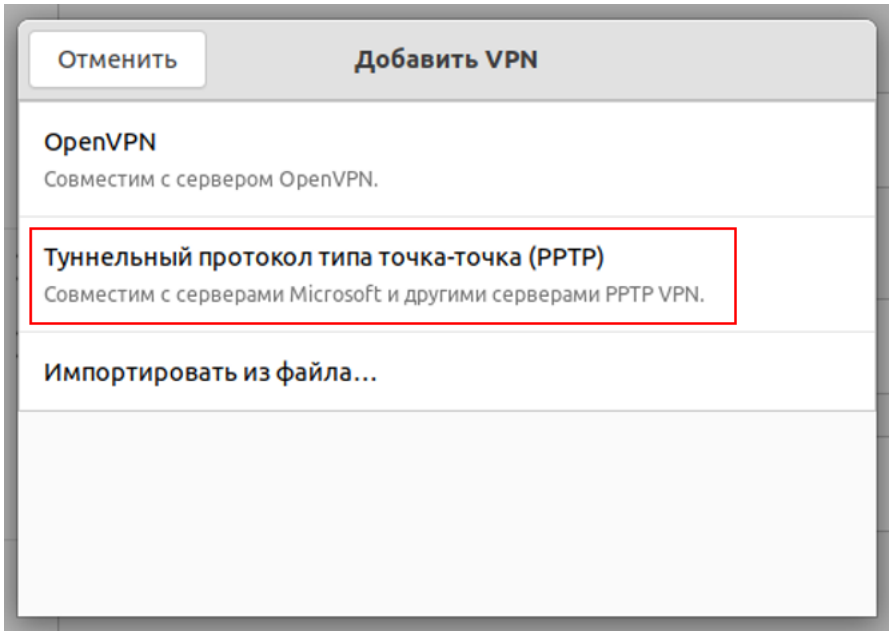


Создание подключения в Ubuntu:

1. Перейдите **Настройки -> Сети** и в строке **VPN** нажмите + :

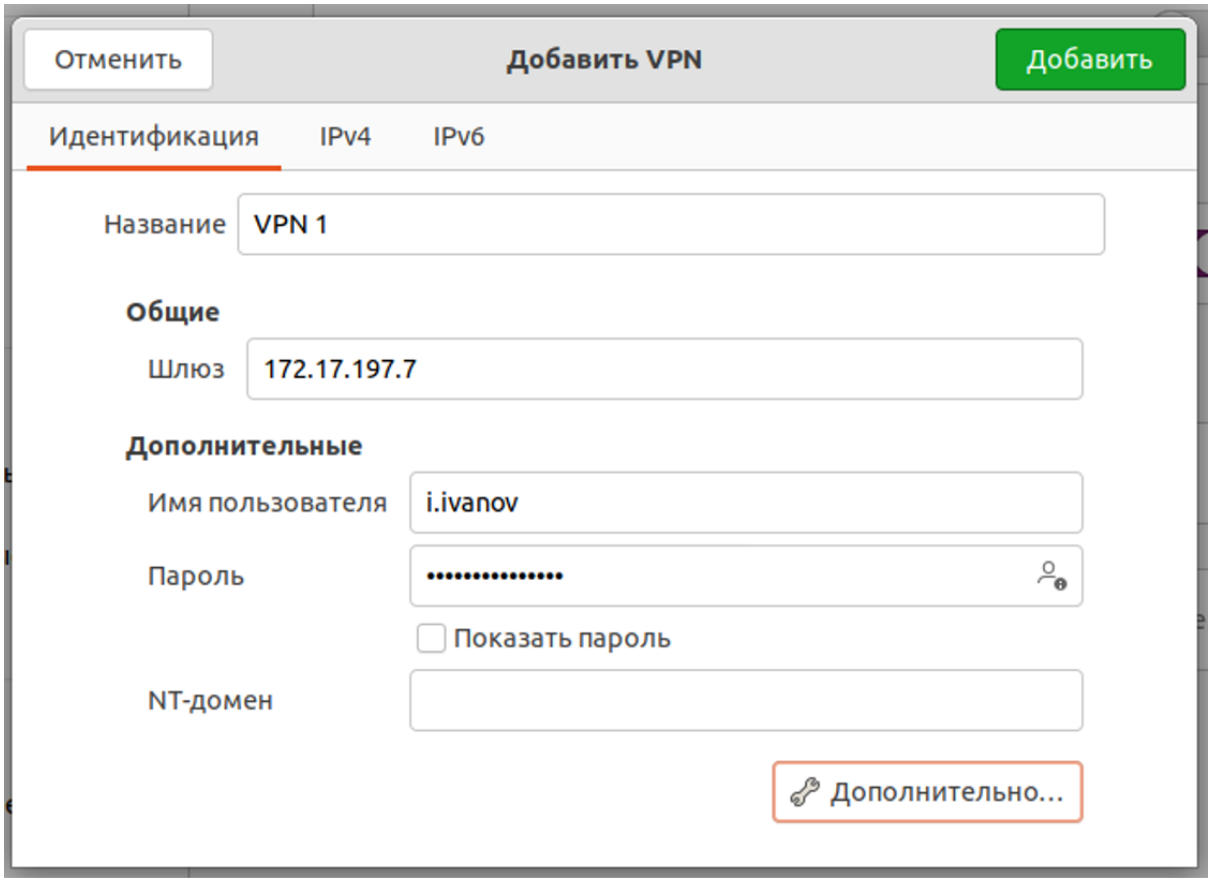


2. В окне создания подключений выберите пункт **Туннельный протокол типа точка-точка (PPTP)**:



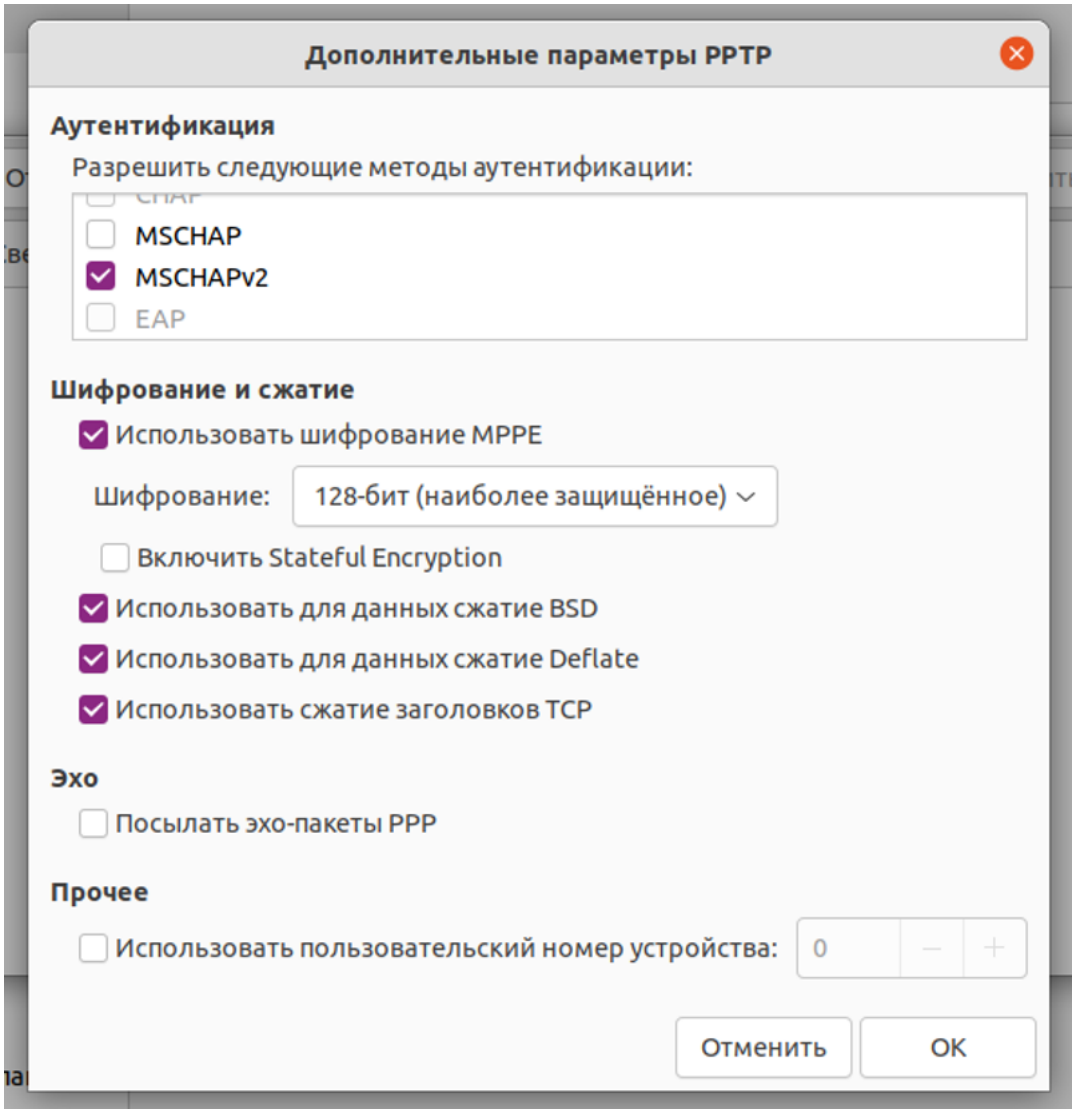
3. В разделе **Идентификация** заполните следующие поля:

- **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.



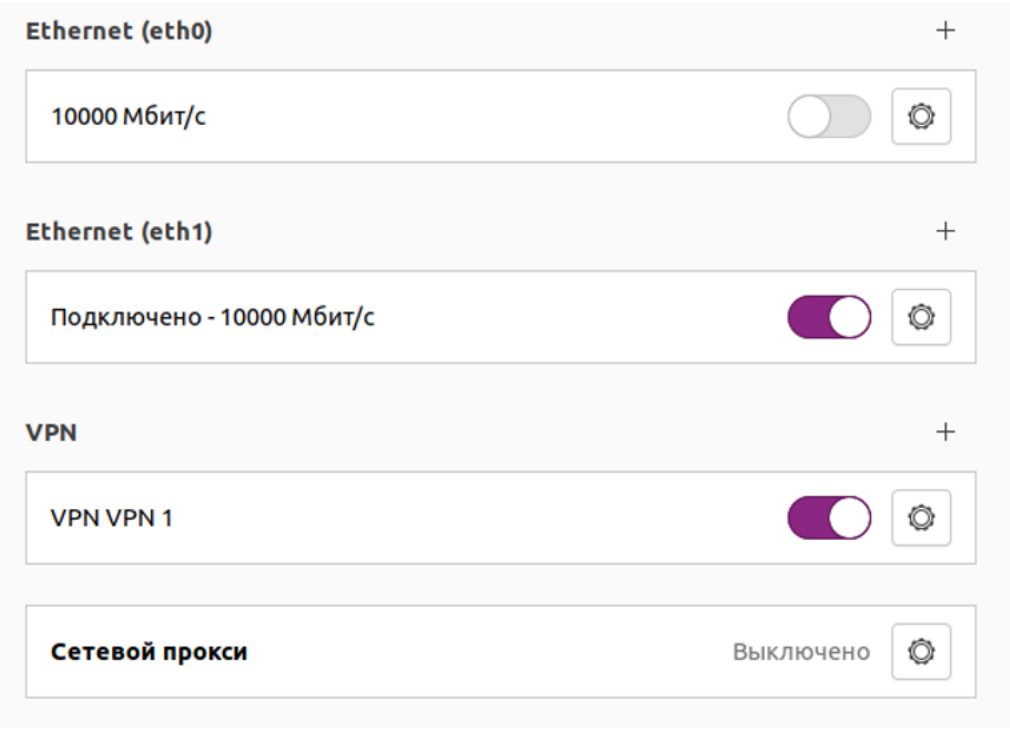
Рекомендуем нажать **Дополнительно** и установить флаги на пунктах:

- **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:

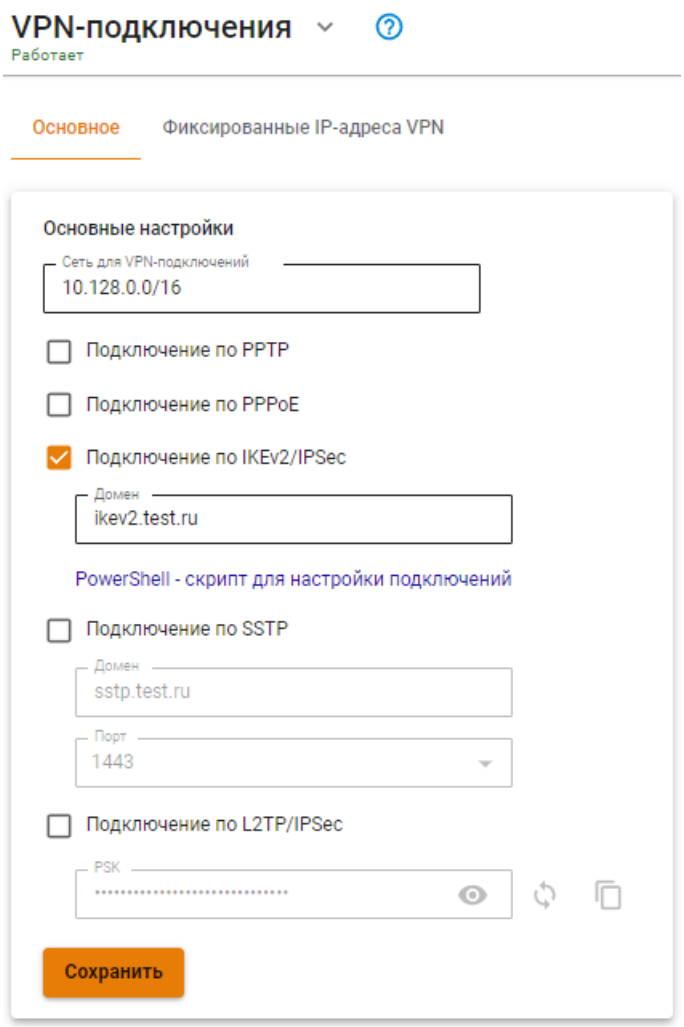


Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

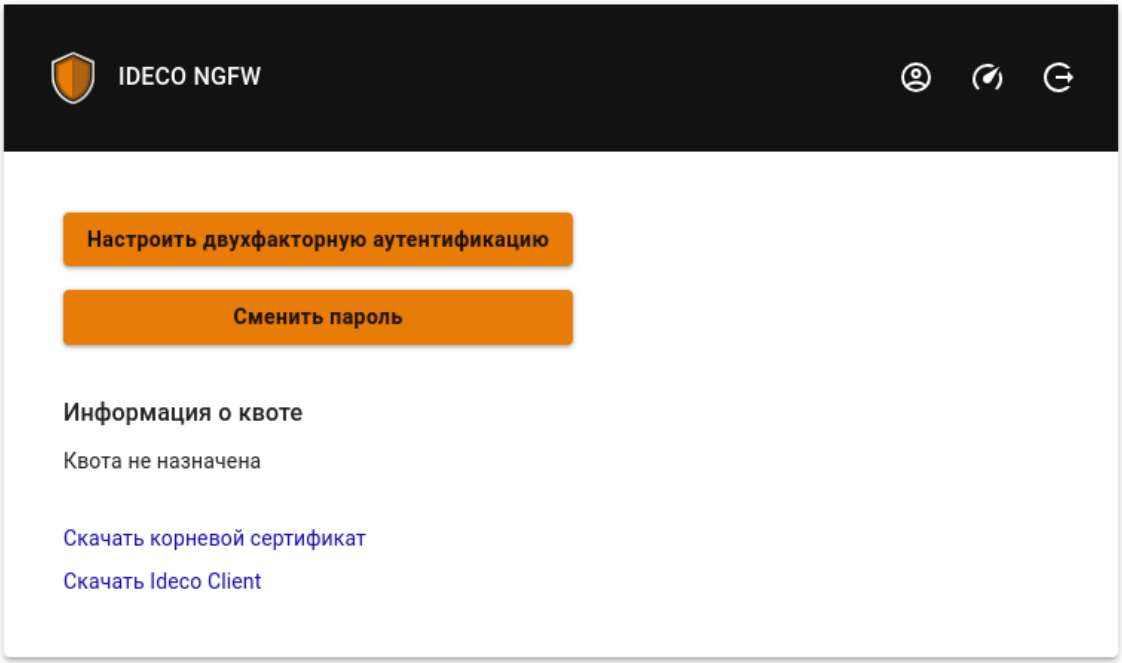
1. Перейдите в раздел **Пользователи -> VPN-подключение -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:

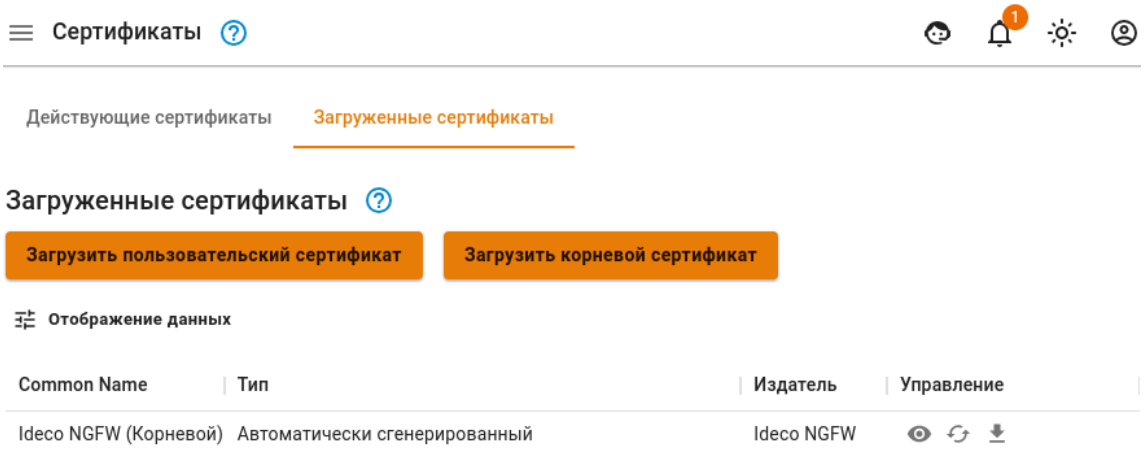


3. Скачайте корневой сертификат одним из способов:

- В личном кабинете, введя логин/пароль пользователя:



- В разделе **Сервисы -> Сертификаты -> Загруженные сертификаты**:



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:

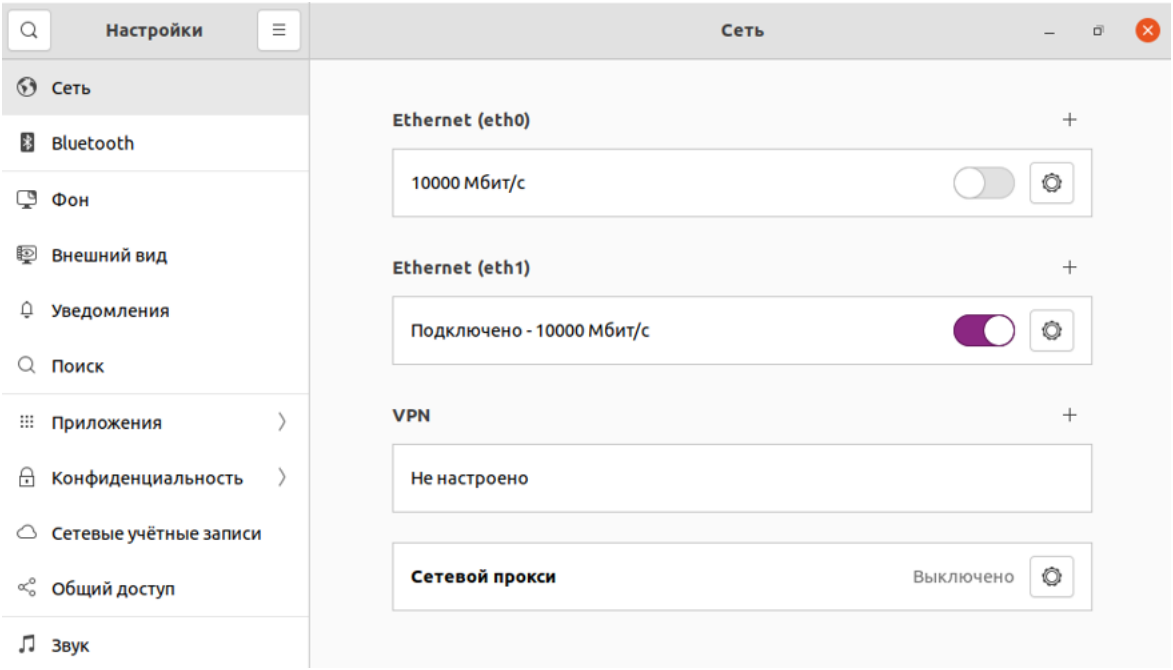
```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

- `ca.crt` - имя скачанного сертификата.

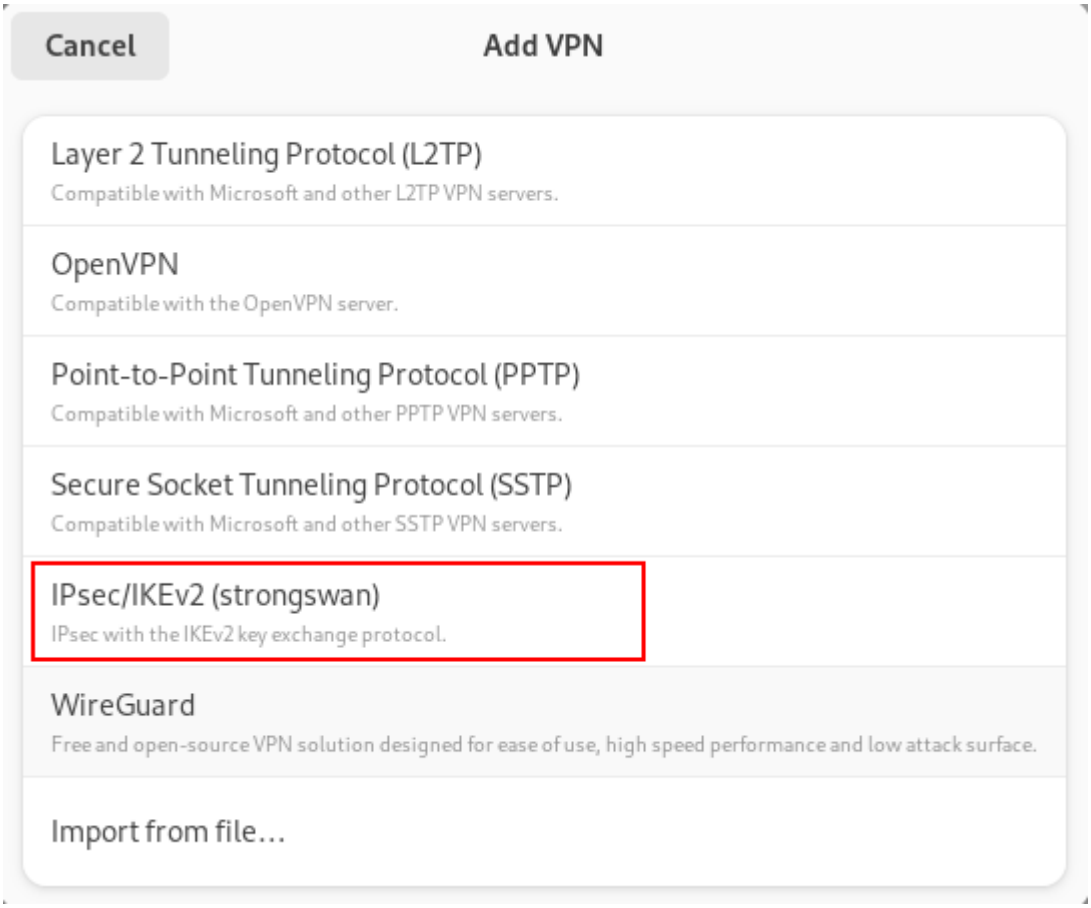
5. Для обновления сертификатов устройства выполните команду:

```
sudo update-ca-certificates
```

6. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + :



7. В появившемся окне выберите **IPsec\IKEv2 (strongswan)**:

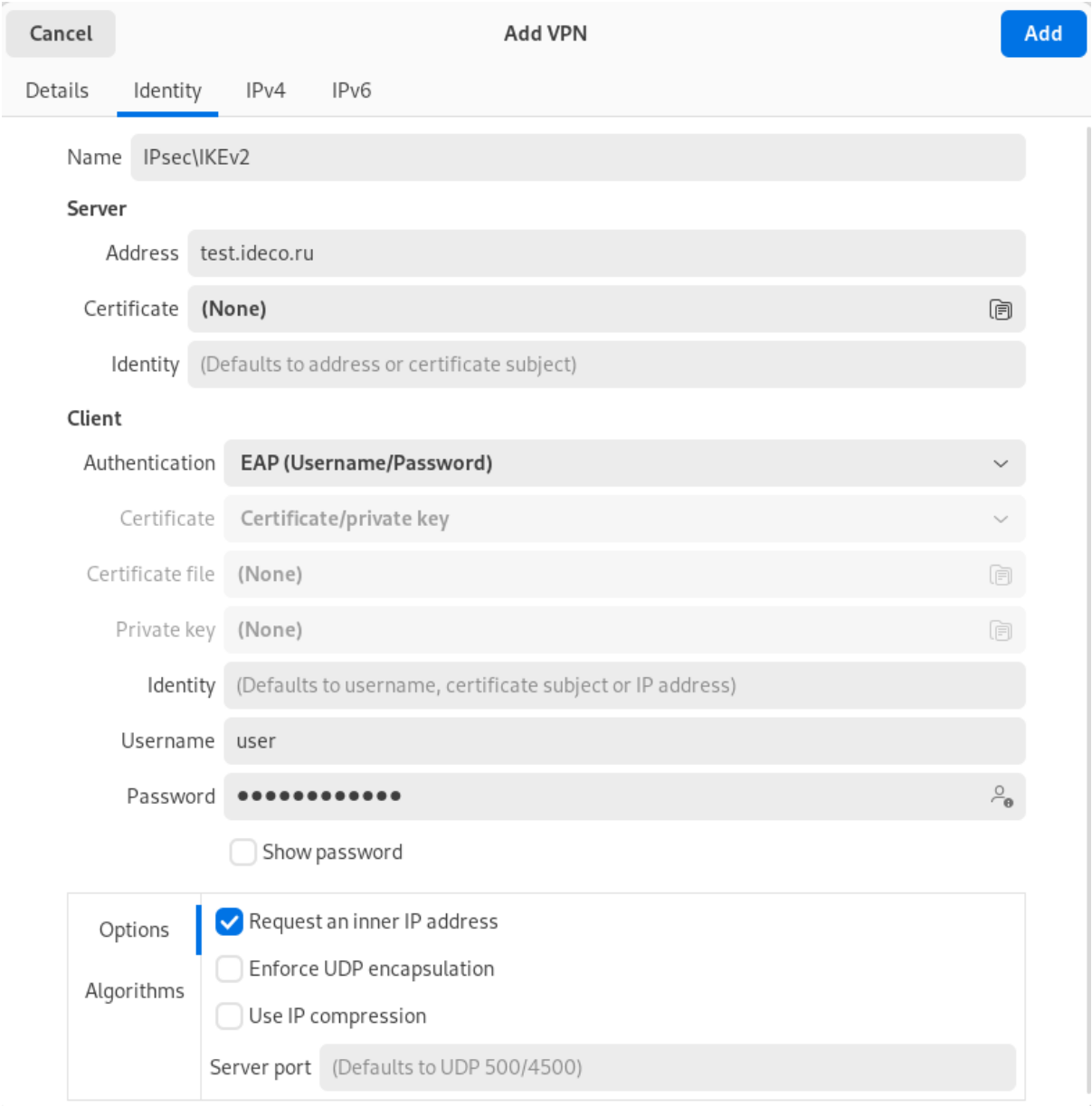


8. В разделе **Идентификация** и заполните следующие поля:

- **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:**



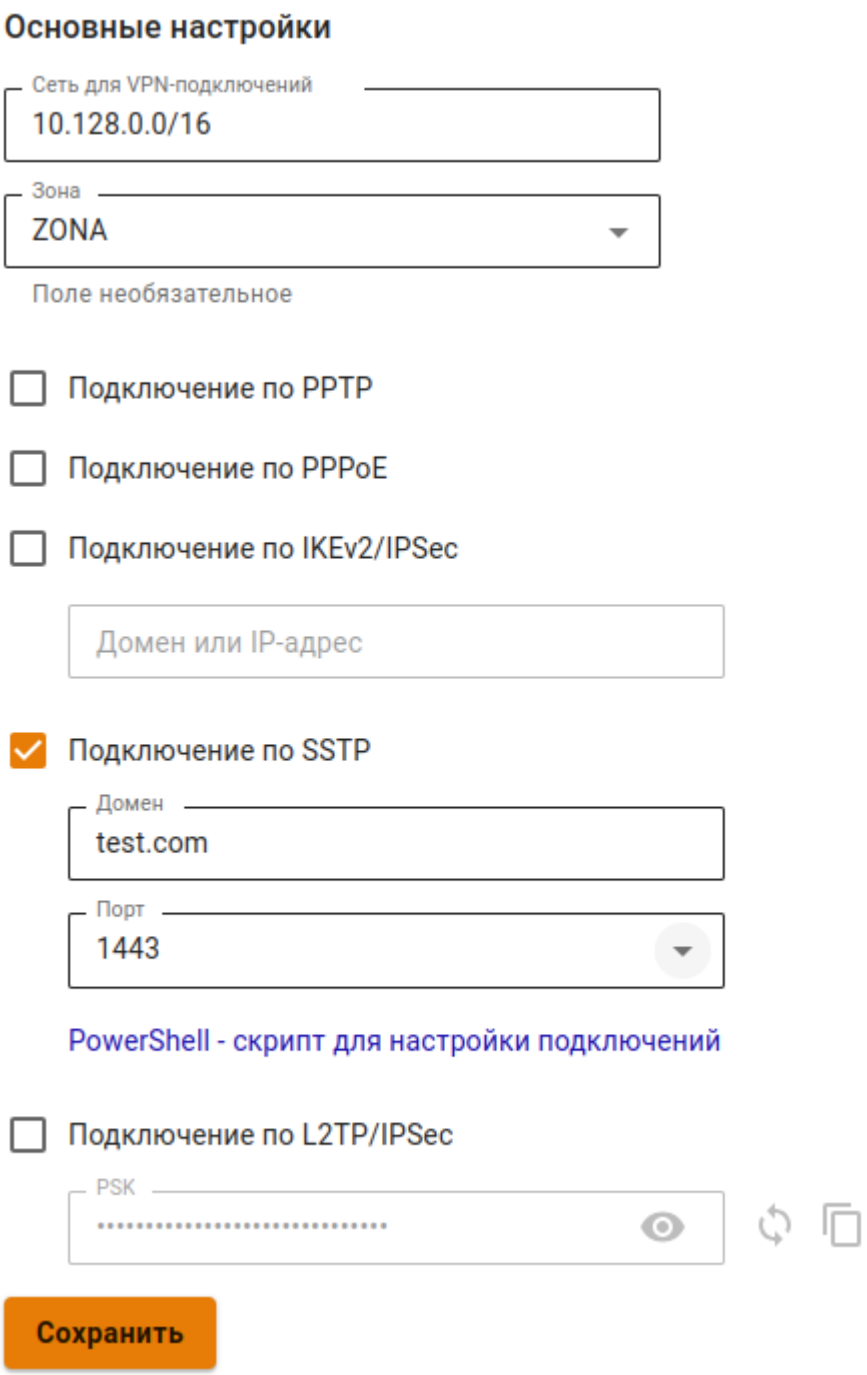
9. Включите созданное VPN-подключение.

Протокол SSTP:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключение -> 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:

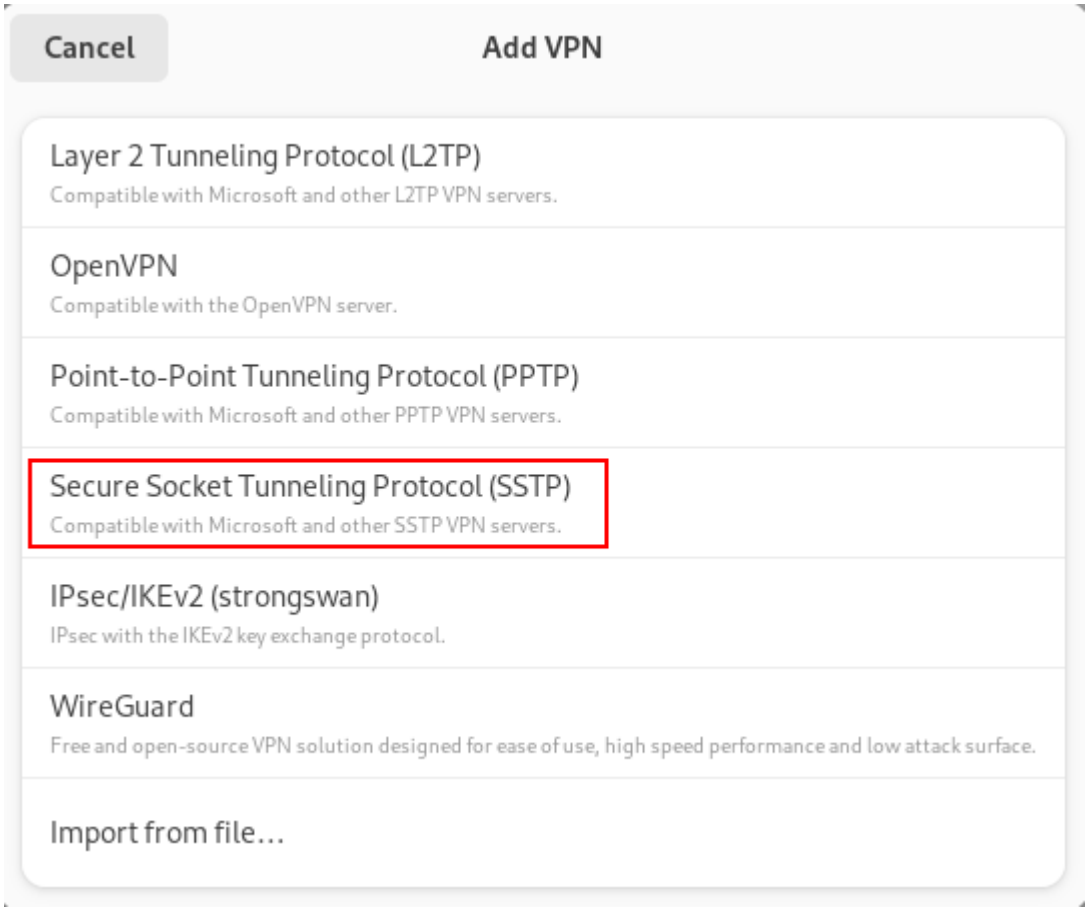
```
sudo apt-add-repository ppa:eivnaes/network-manager-sstp
sudo apt install -y network-manager-sstp sstp-client
```

2. По окончании установки перезагрузите компьютер:

```
sudo reboot
```

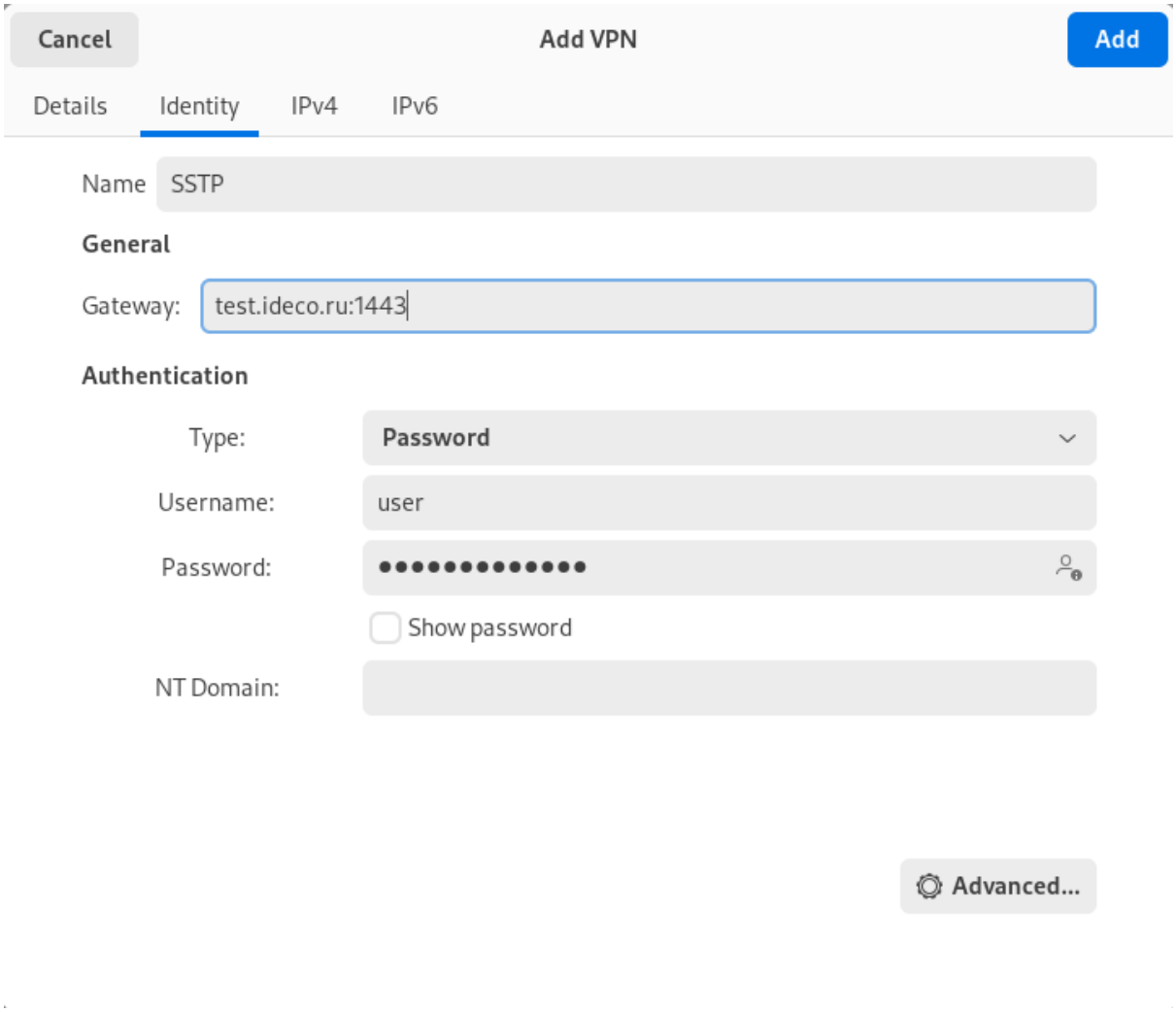
3. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + .

4. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)** или **Туннельный протокол типа точка-точка (SSTP)**:



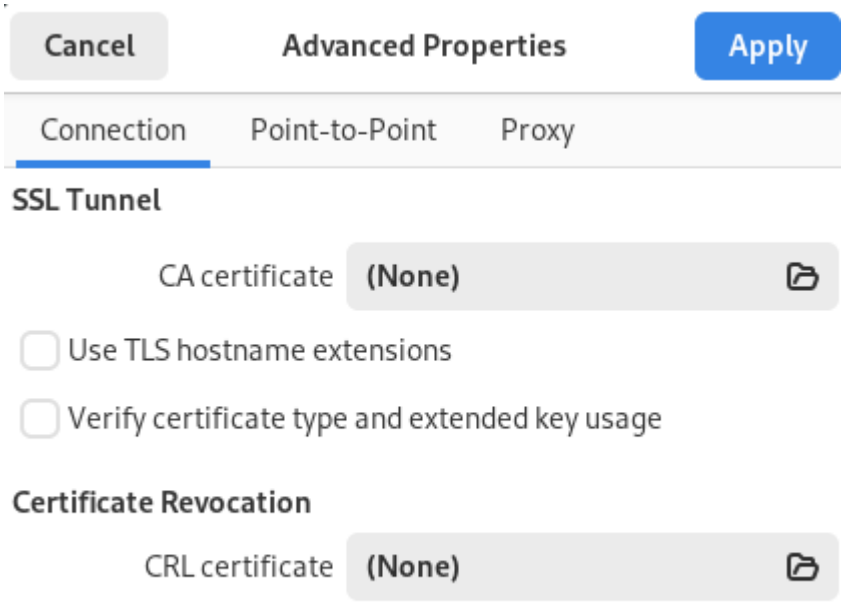
5. В разделе **Identity (Идентификация)** заполните следующие поля:

- **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.

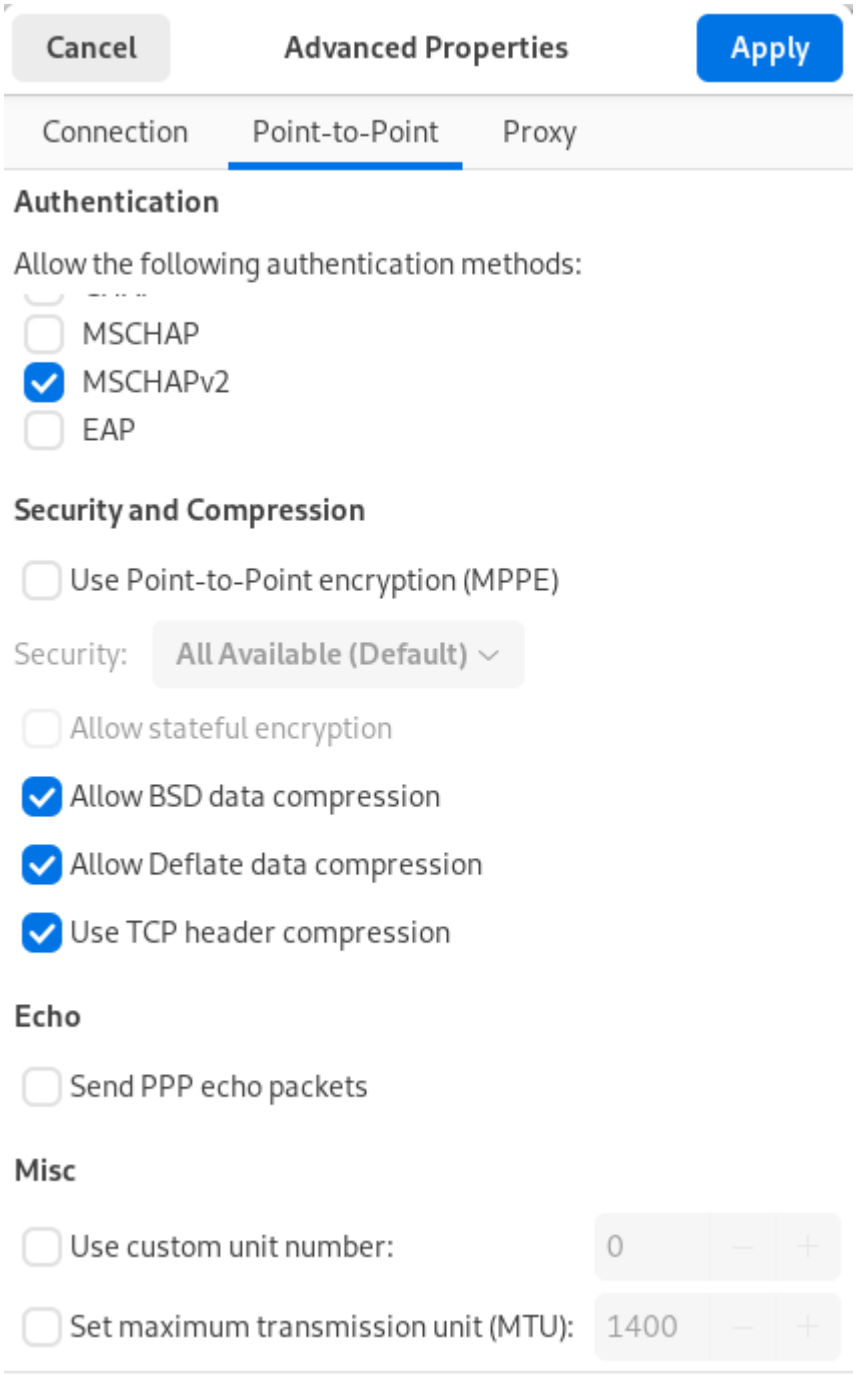


6. Нажмите **Advanced**:

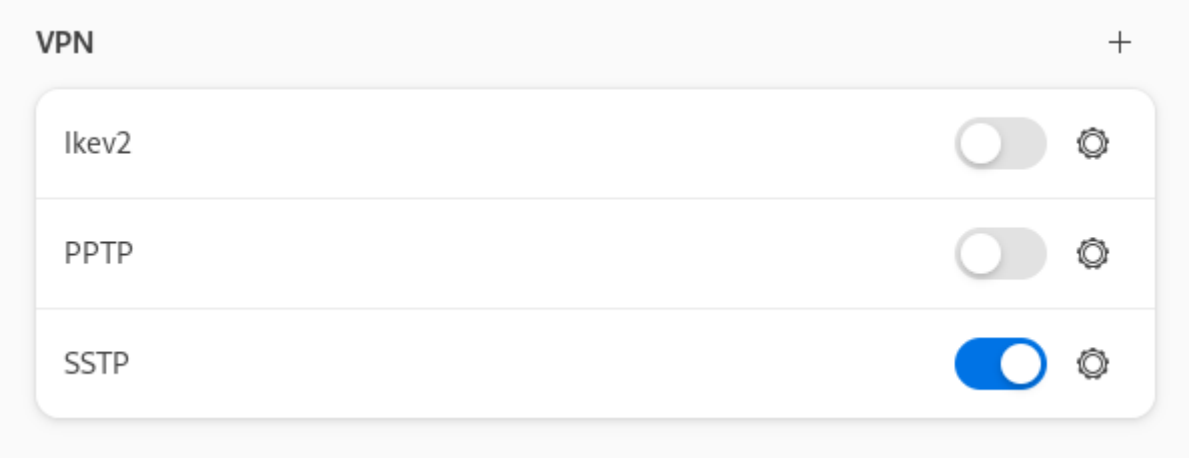
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**;
  - **Verify certificate type and extended key usage**:



- 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:



6. Нажмите **Добавить** и включите созданное VPN-подключение:



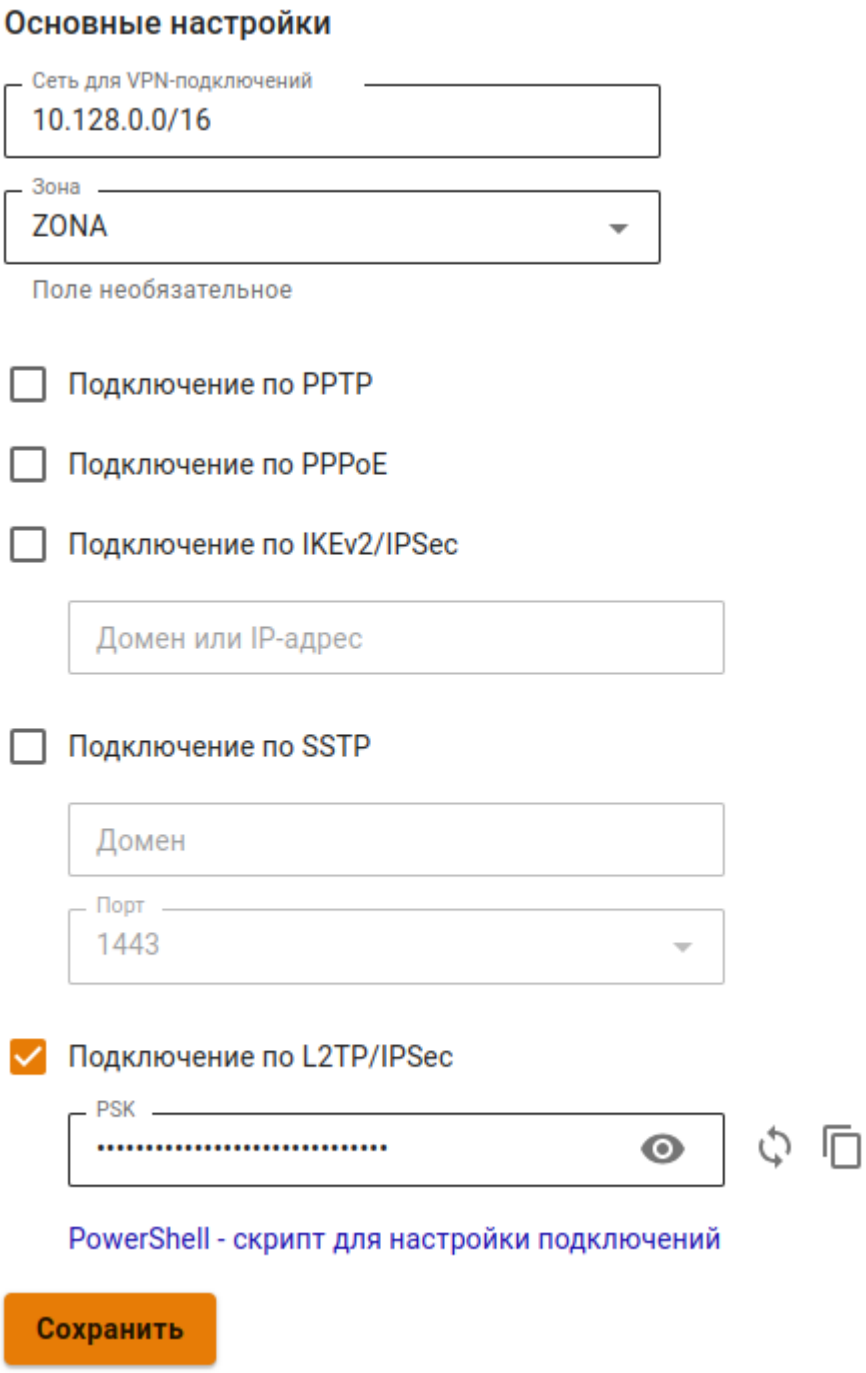
Протокол L2TP/IPsec:

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-подключение -> 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
```

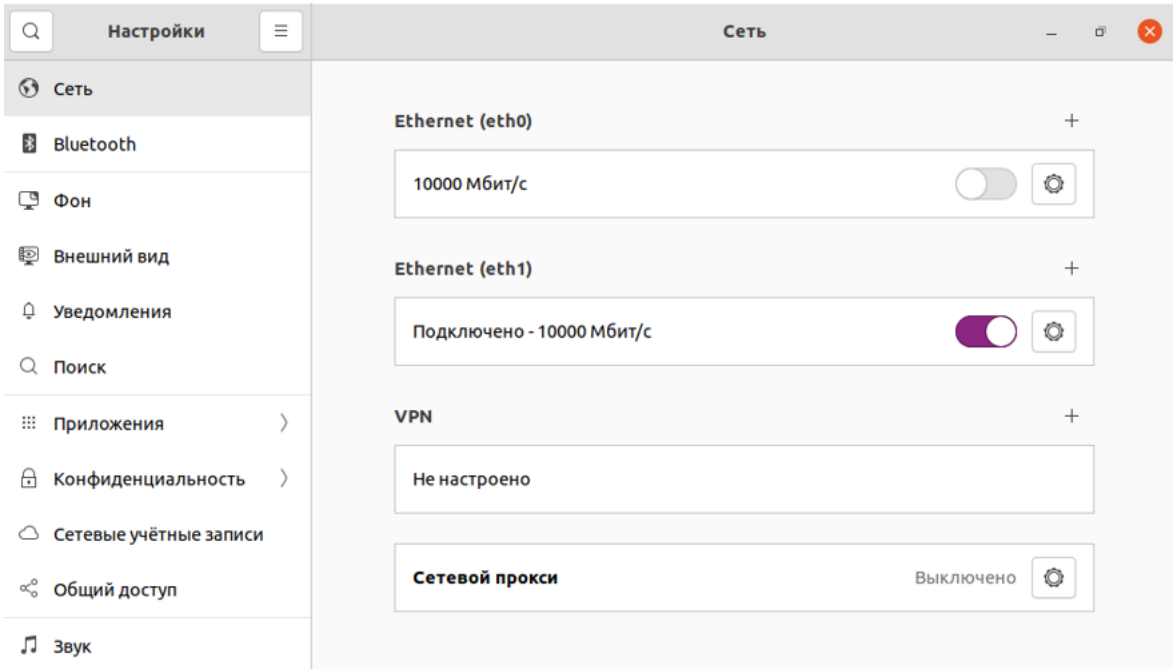
2. Установите дополнение к стандартному NetworkManager с помощью двух пакетов:

```
sudo apt install -y network-manager-l2tp network-manager-l2tp-gnome
```

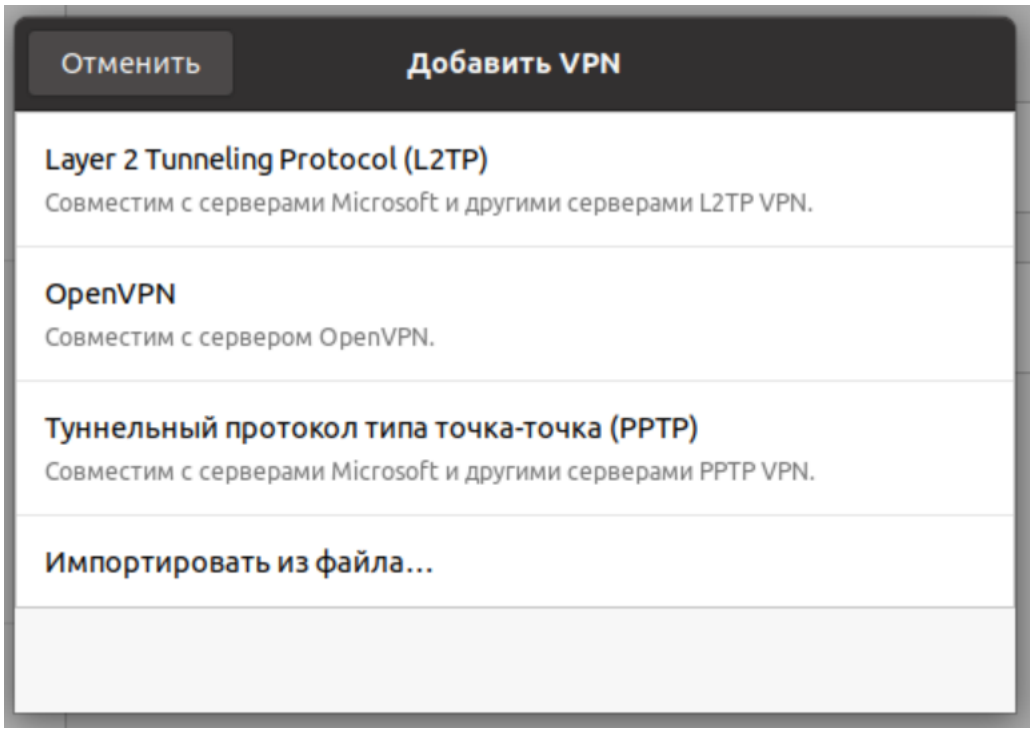
3. После окончания установки перезагрузите компьютер:

```
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. Во вкладке **Идентификация** заполните следующие поля:

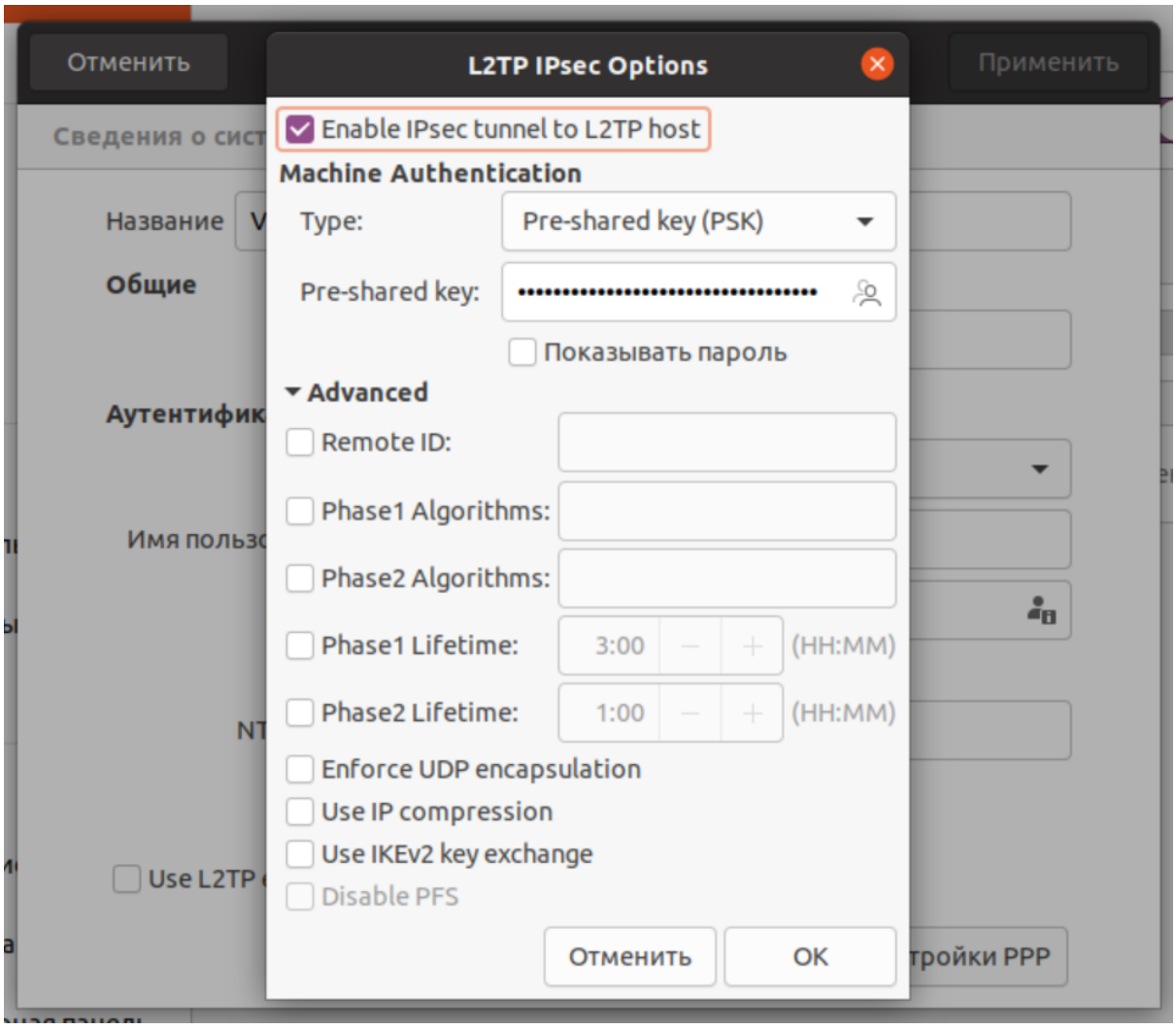
- **Название** - имя подключения;
- **Шлюз** - доменное имя или IP-адрес интерфейса NGFW;
- **Тип** - Password (аутентификация по имени пользователя и паролю);
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;

- **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:

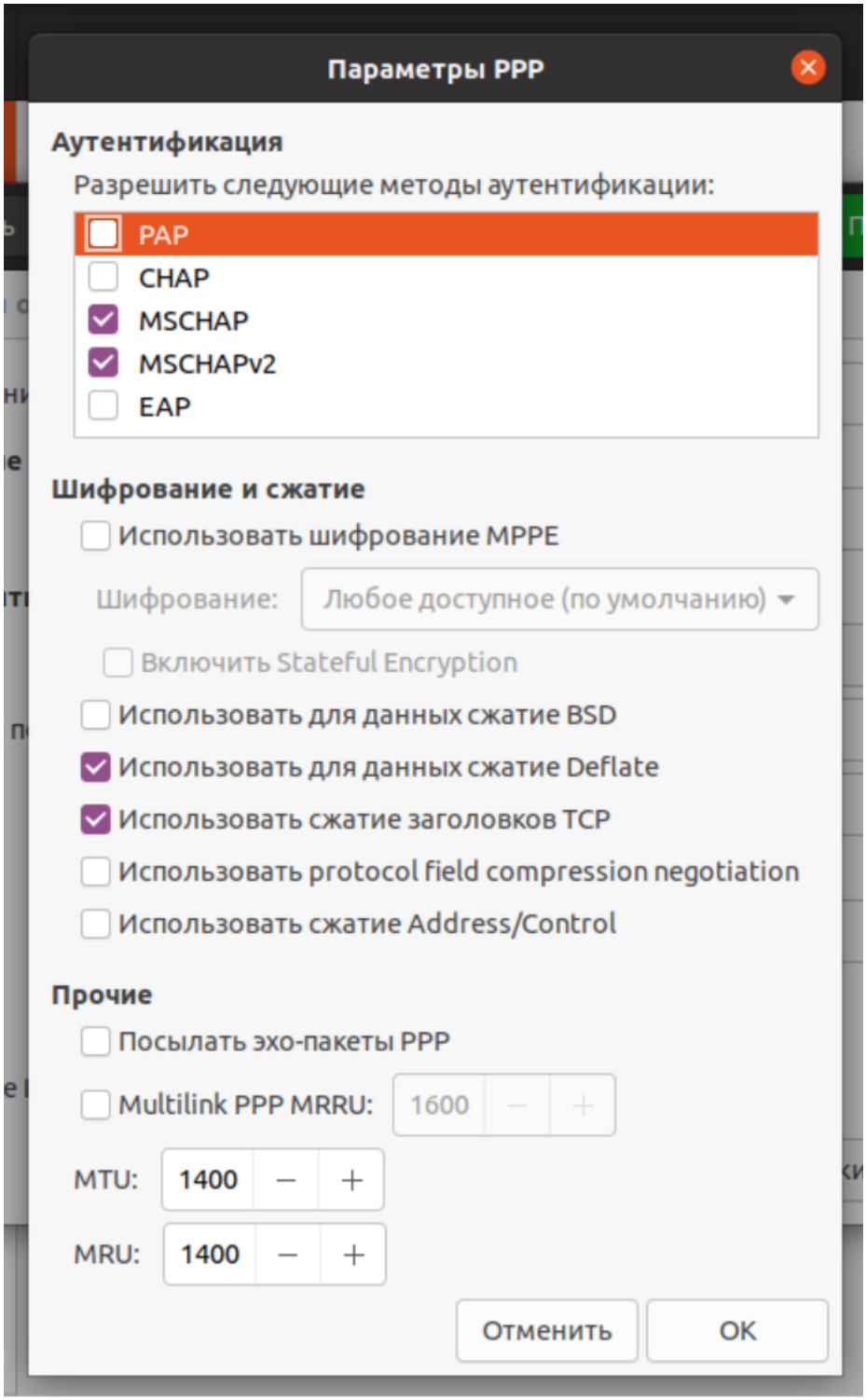
- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу;
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи -> VPN-подключение -> Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения:



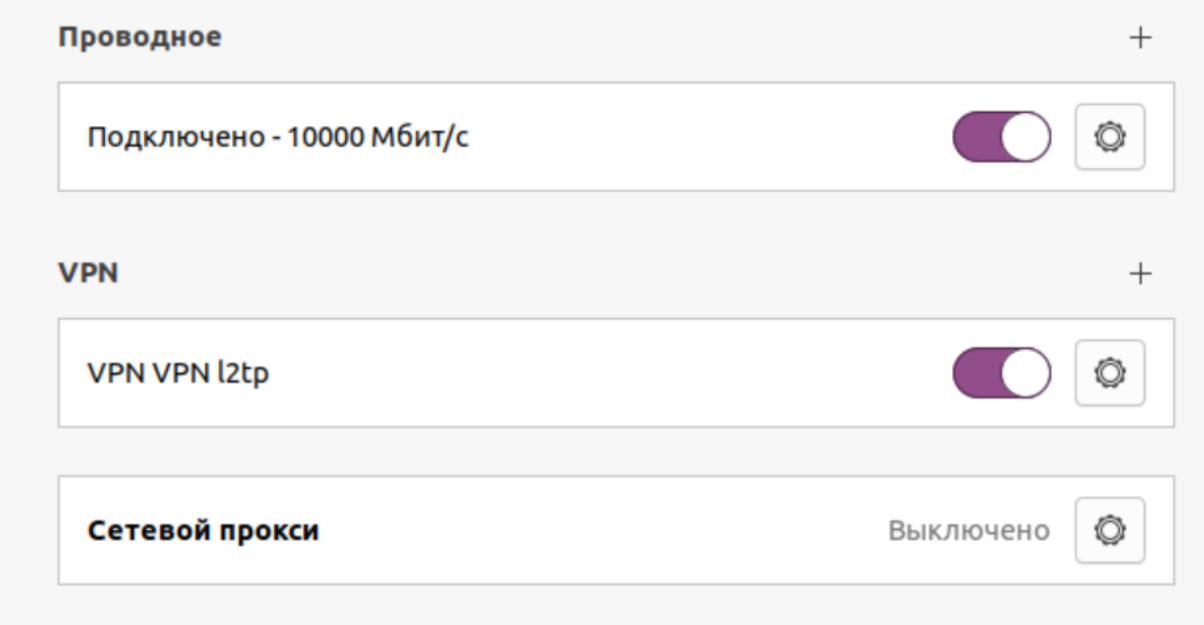
После окончания настройки **L2TP IPsec Options** нажмите **OK**.

8. При необходимости перейдите в **Настройки PPP** и настройте раздел **Аутентификация**, **Шифрование и сжатие** и **Прочие**:



После настройки **Параметры PPP** нажмите **ОК** и **Применить**.

9. Включите созданное VPN-подключение:



22.20.3 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.

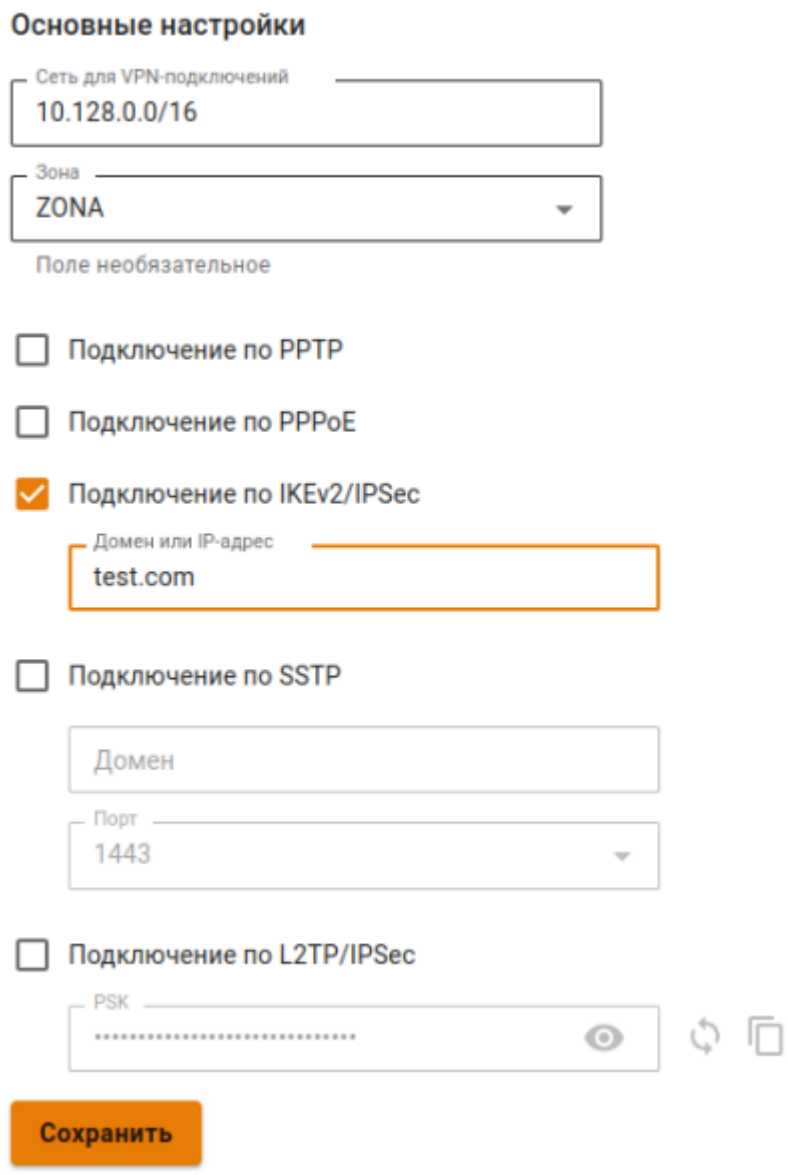
При настройке подключения в Fedora 40 **не требуется** загружать сертификат **ISRG_ROOT_X1**, поскольку он уже есть в системе. Сертификат находится в каталоге `/etc/ssl/certs`

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:

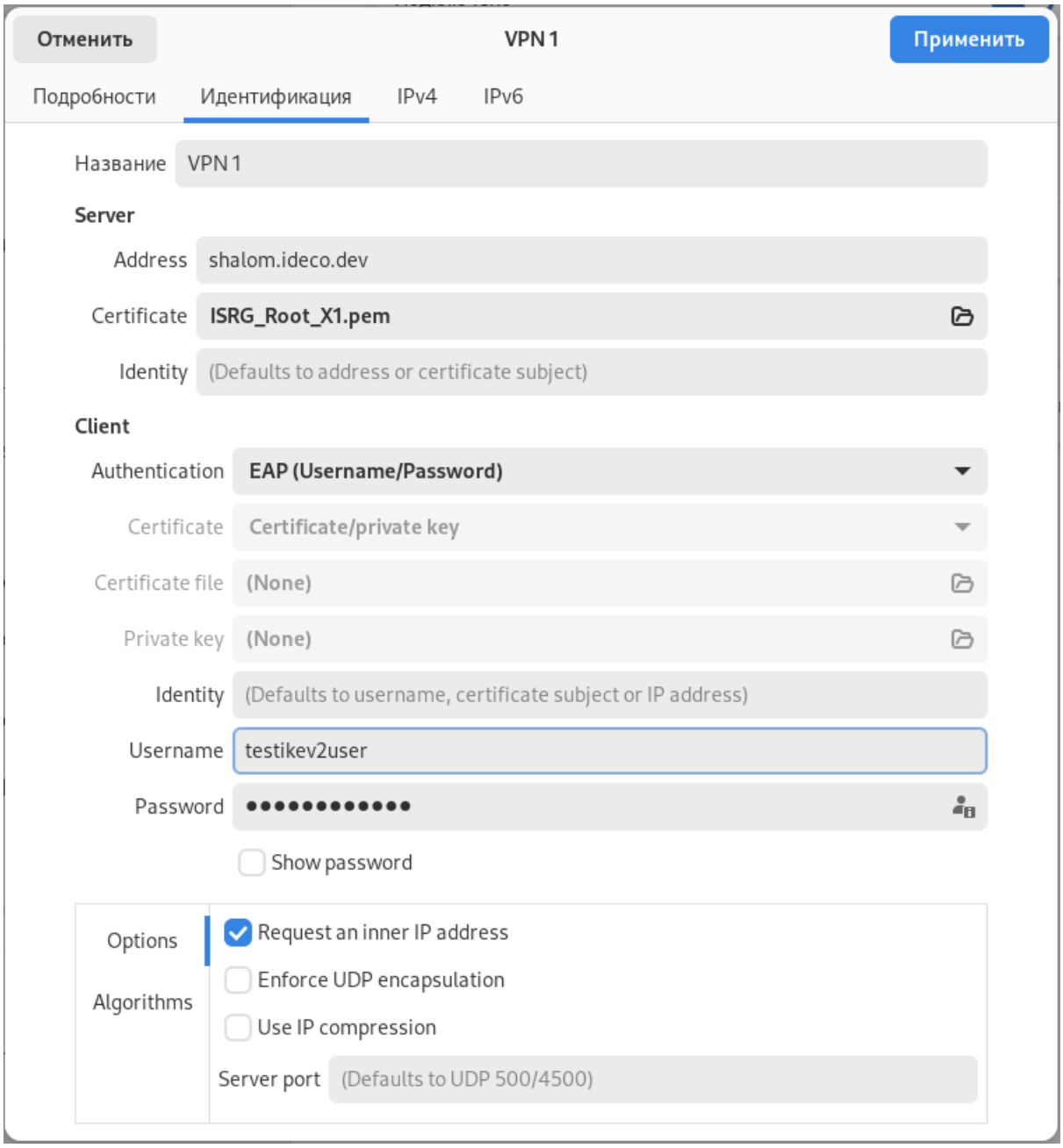
```
sudo dnf -y install plasma-nm-strongswan
```

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.



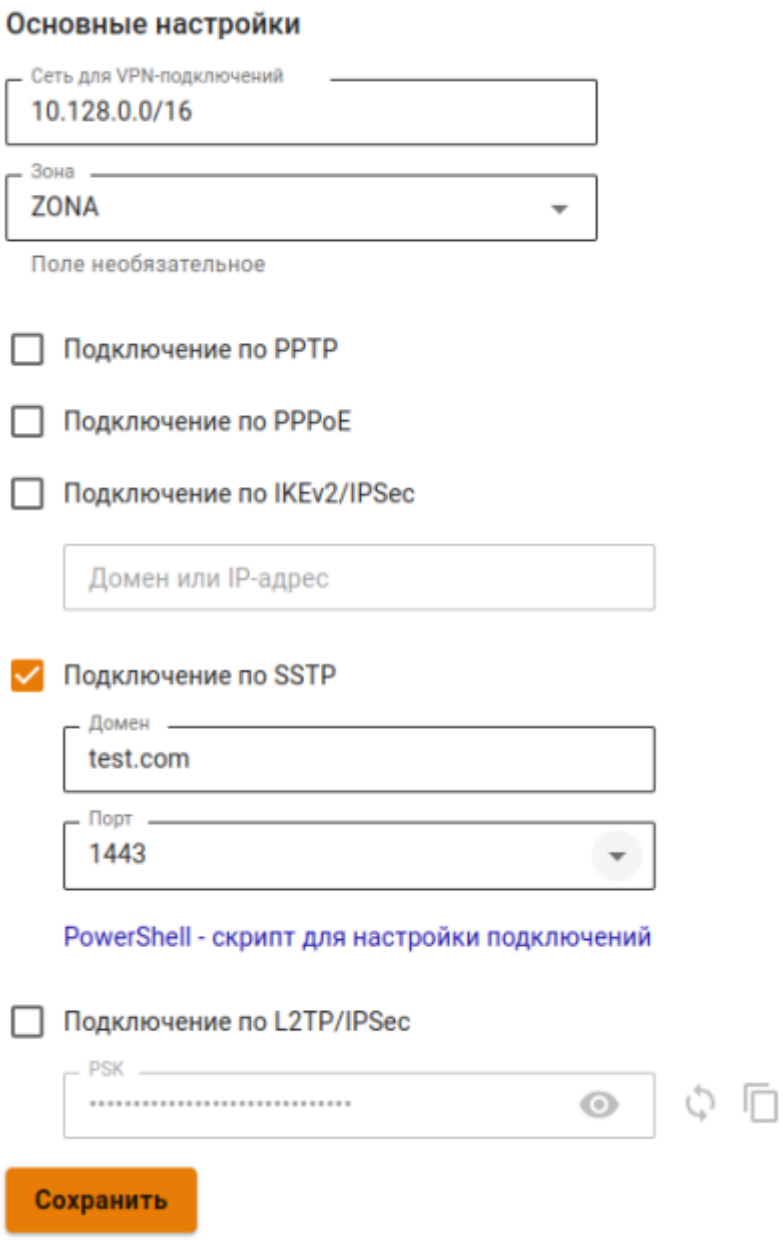
3. Нажмите **Применить** и подключитесь к Ideco NGFW.

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:

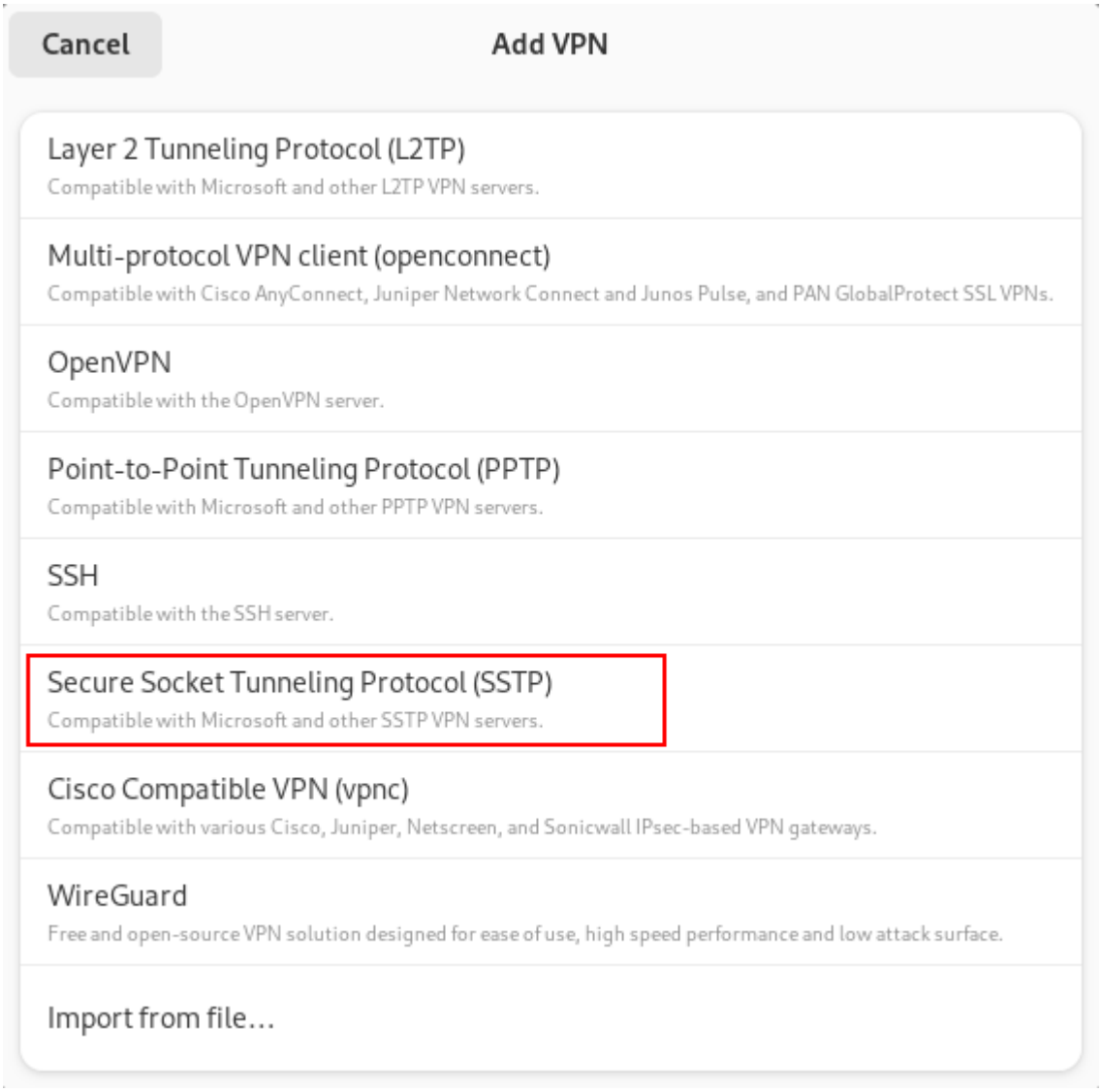
```
sudo dnf install NetworkManager-sstp.x86_64 plasma-nm-sstp.x86_64 sstp-client.x86_64
```

2. По окончании установки перезагрузите компьютер:

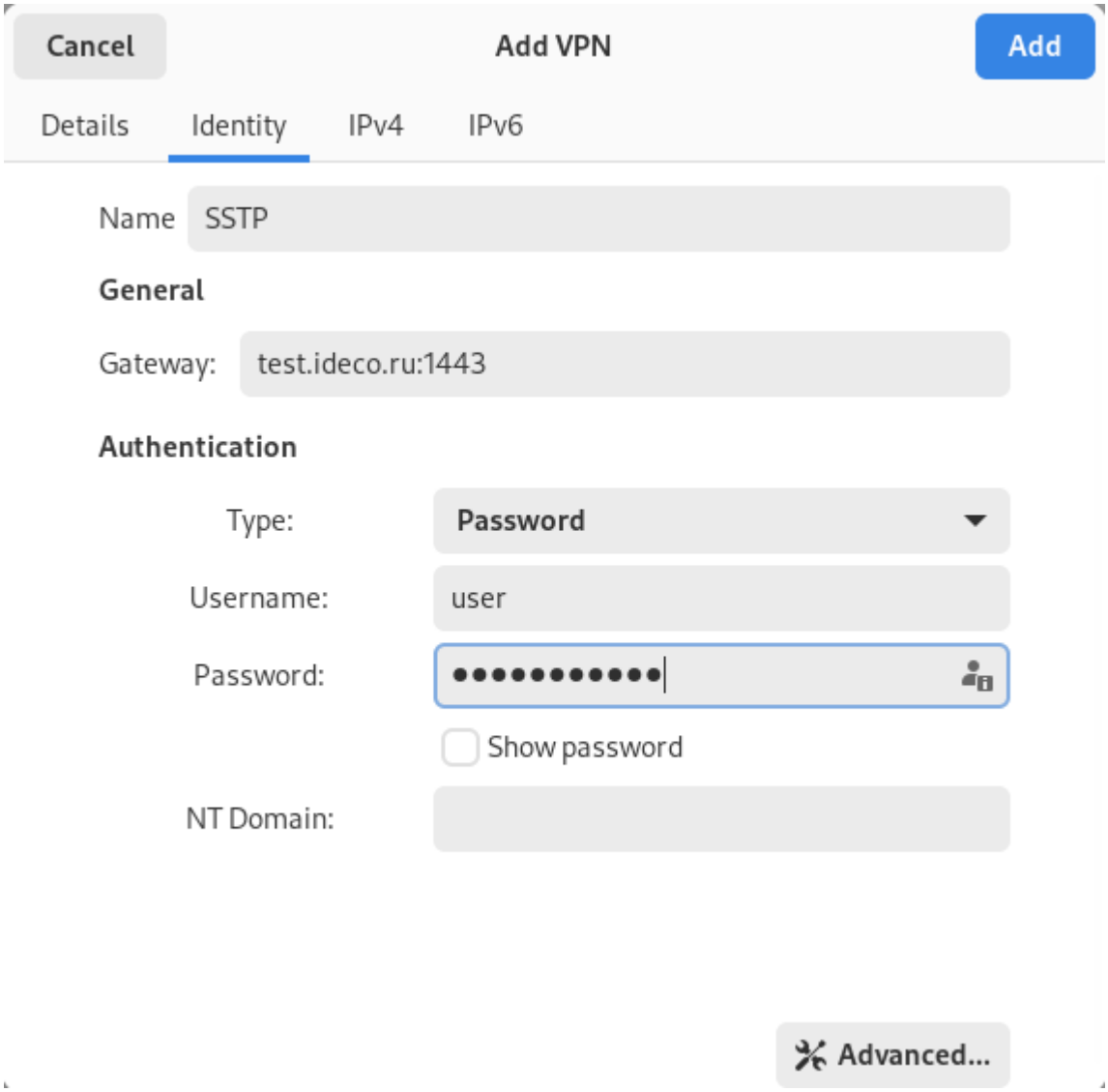
```
sudo reboot
```

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)**:



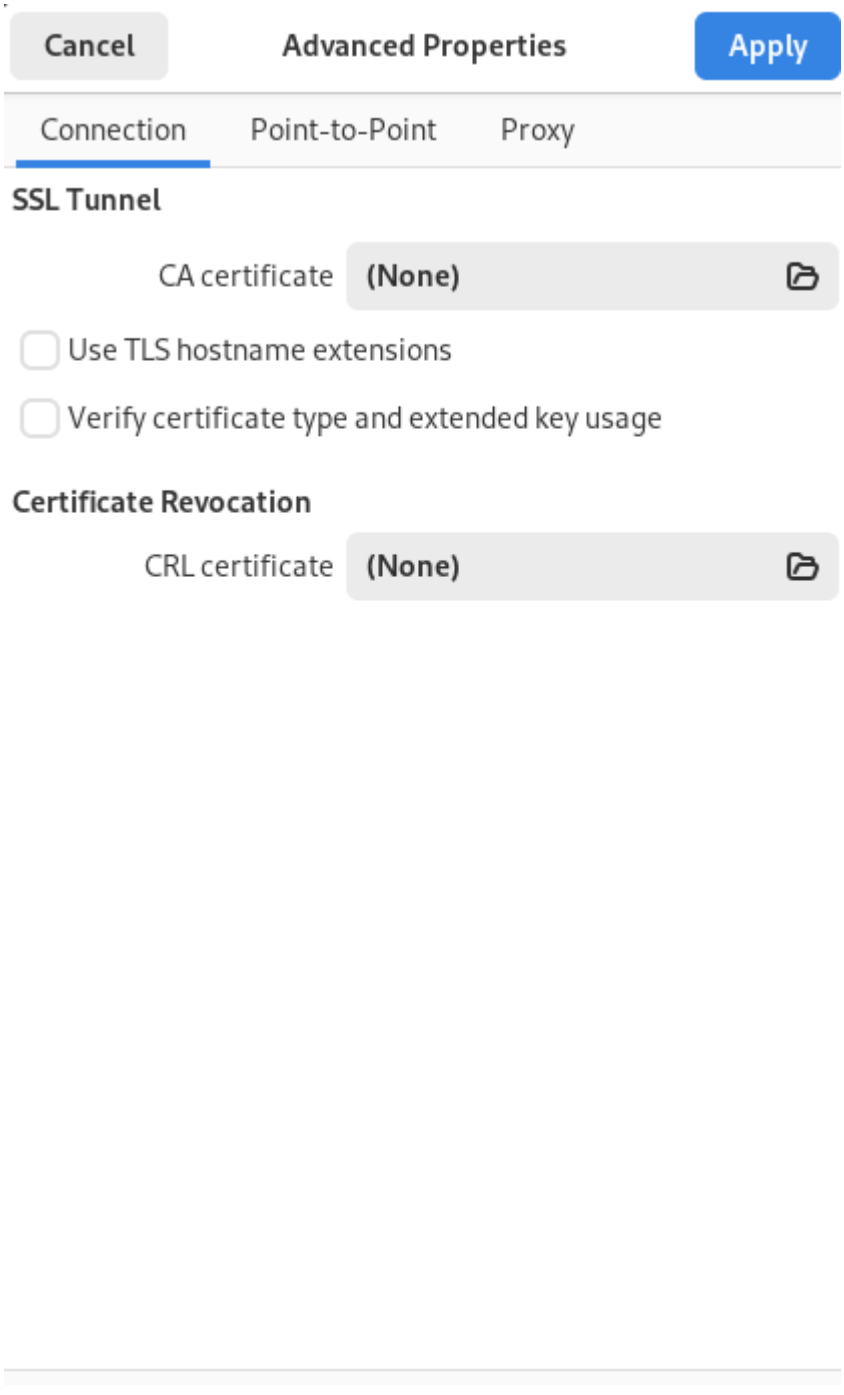
5. В разделе **Identity (Идентификация)** заполните следующие поля:



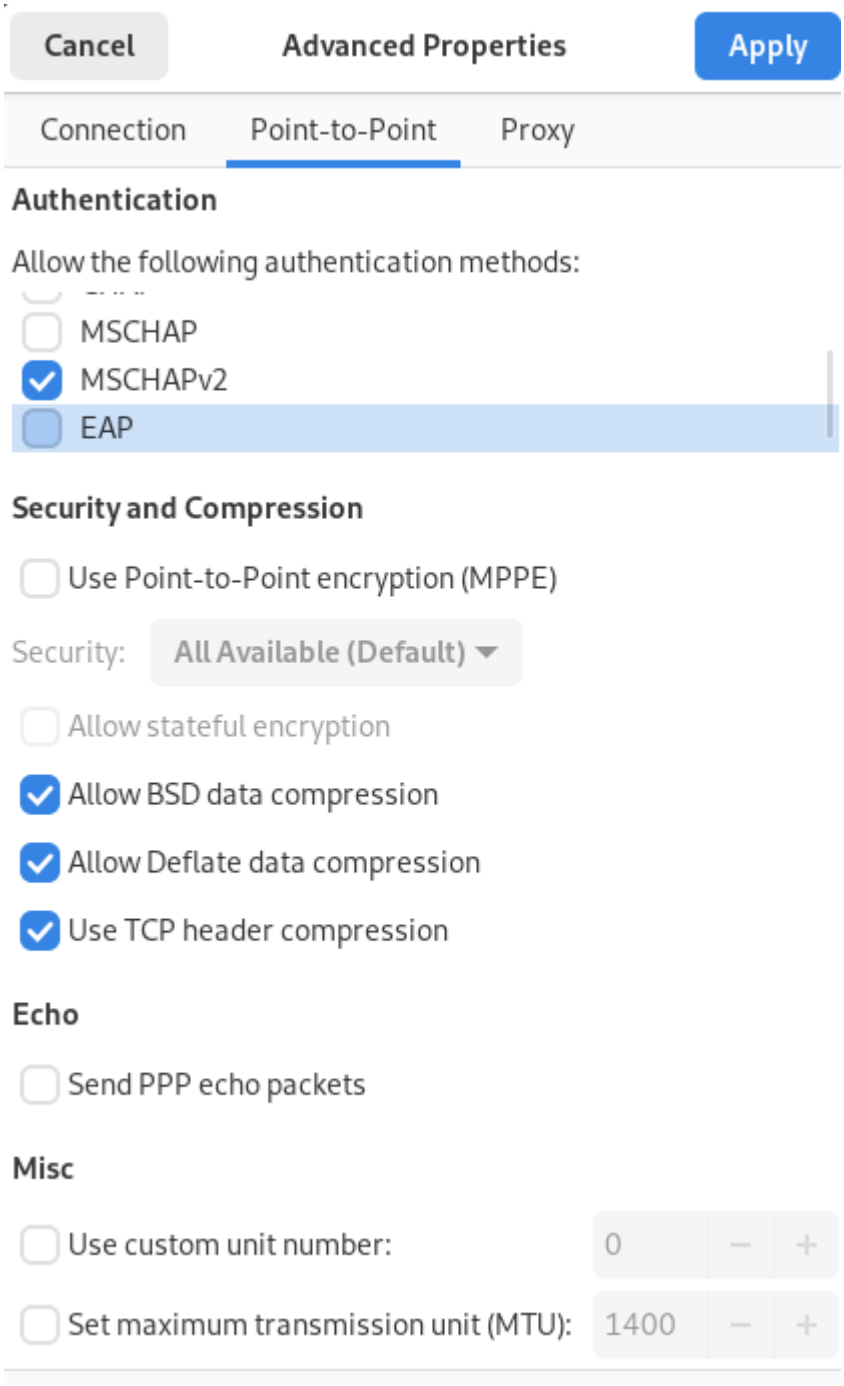
- **Название** - имя подключения;
- **Шлюз** - укажите в формате `домен:<порт, выбранный на NGFW>`;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

6. Нажмите **Advanced**:

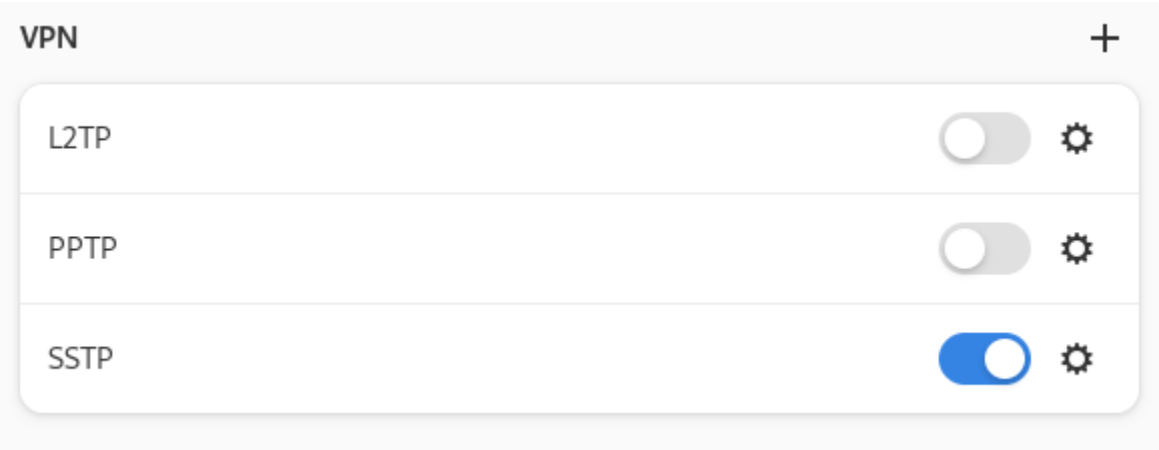
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**;
  - **Verify certificate type and extended key usage**:



- 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:



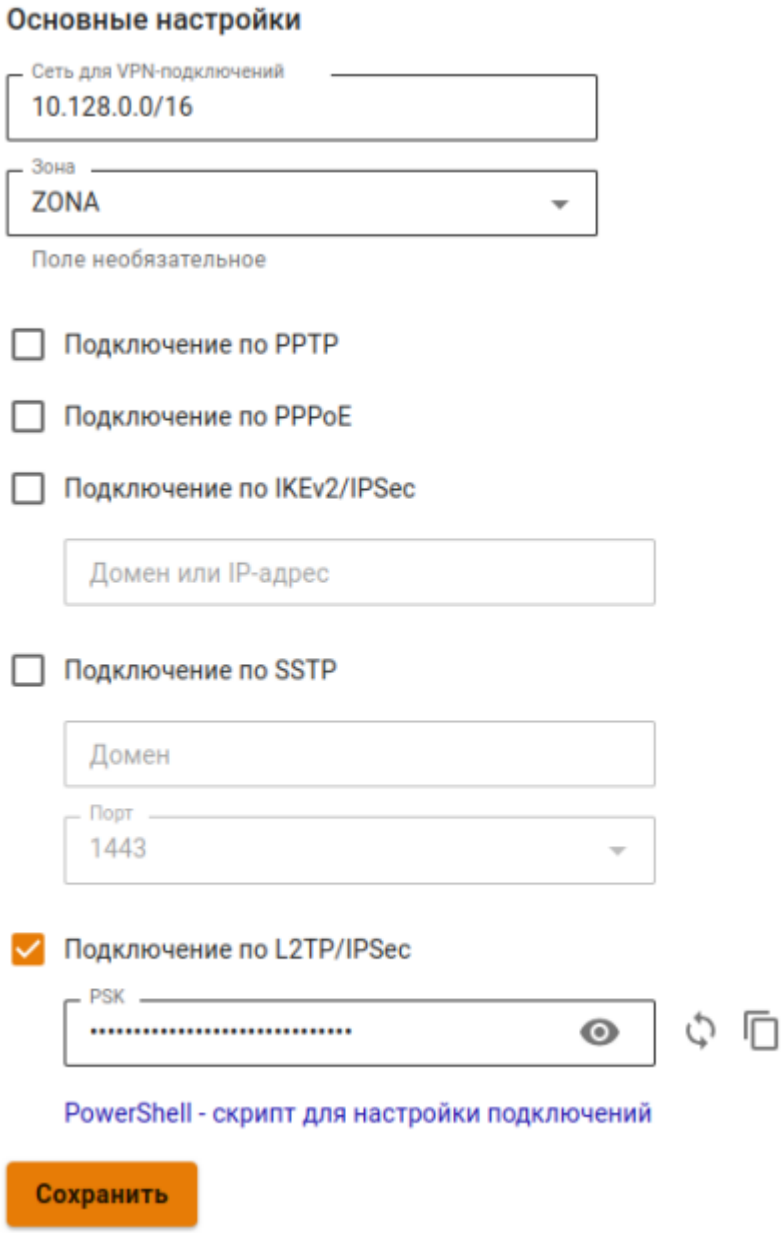
Протокол L2TP/IPsec:

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:

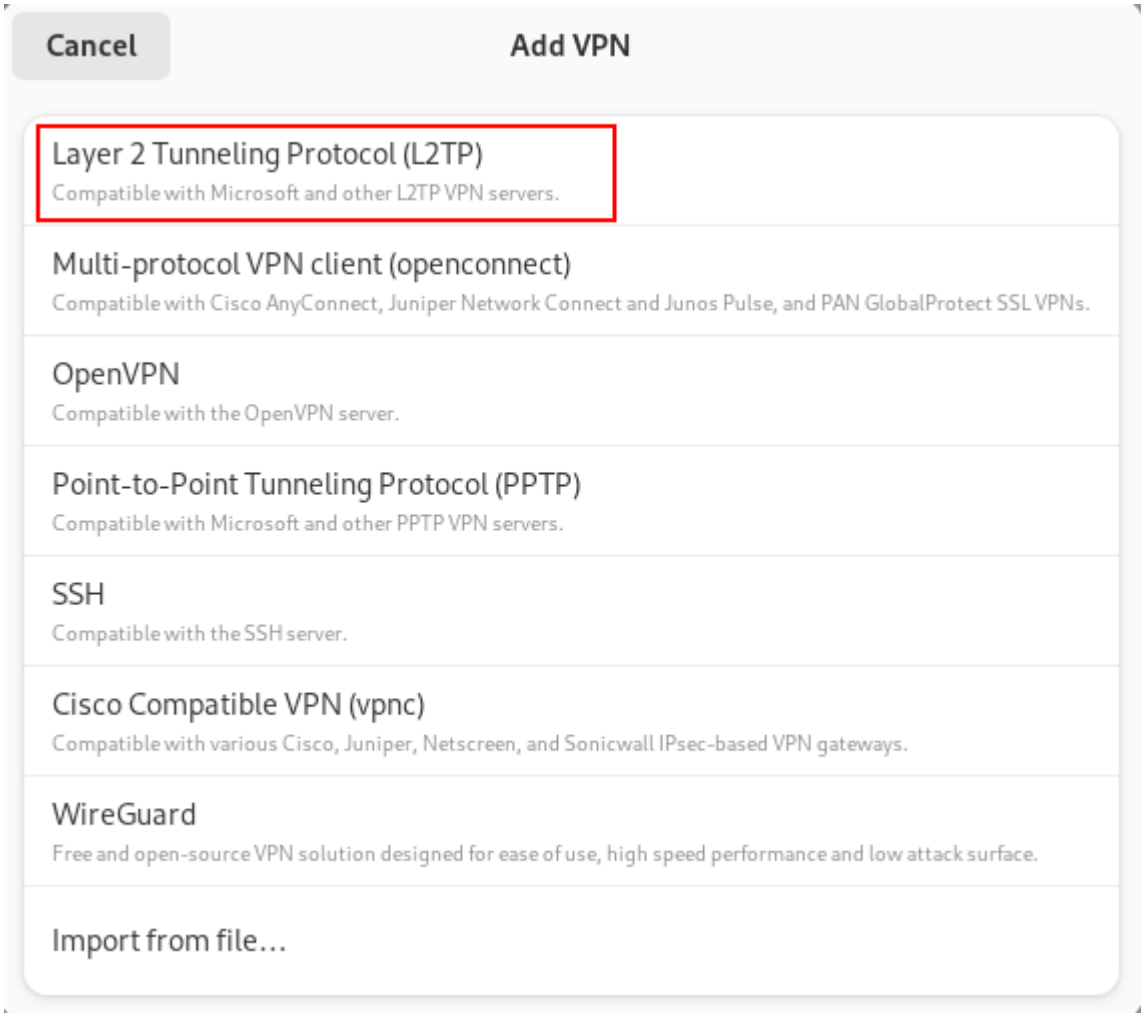
```
sudo dnf install NetworkManager-l2tp.x86_64 plasma-nm-l2tp.x86_64 xl2tpd.x86_64
```

2. После окончания установки перезагрузите компьютер:

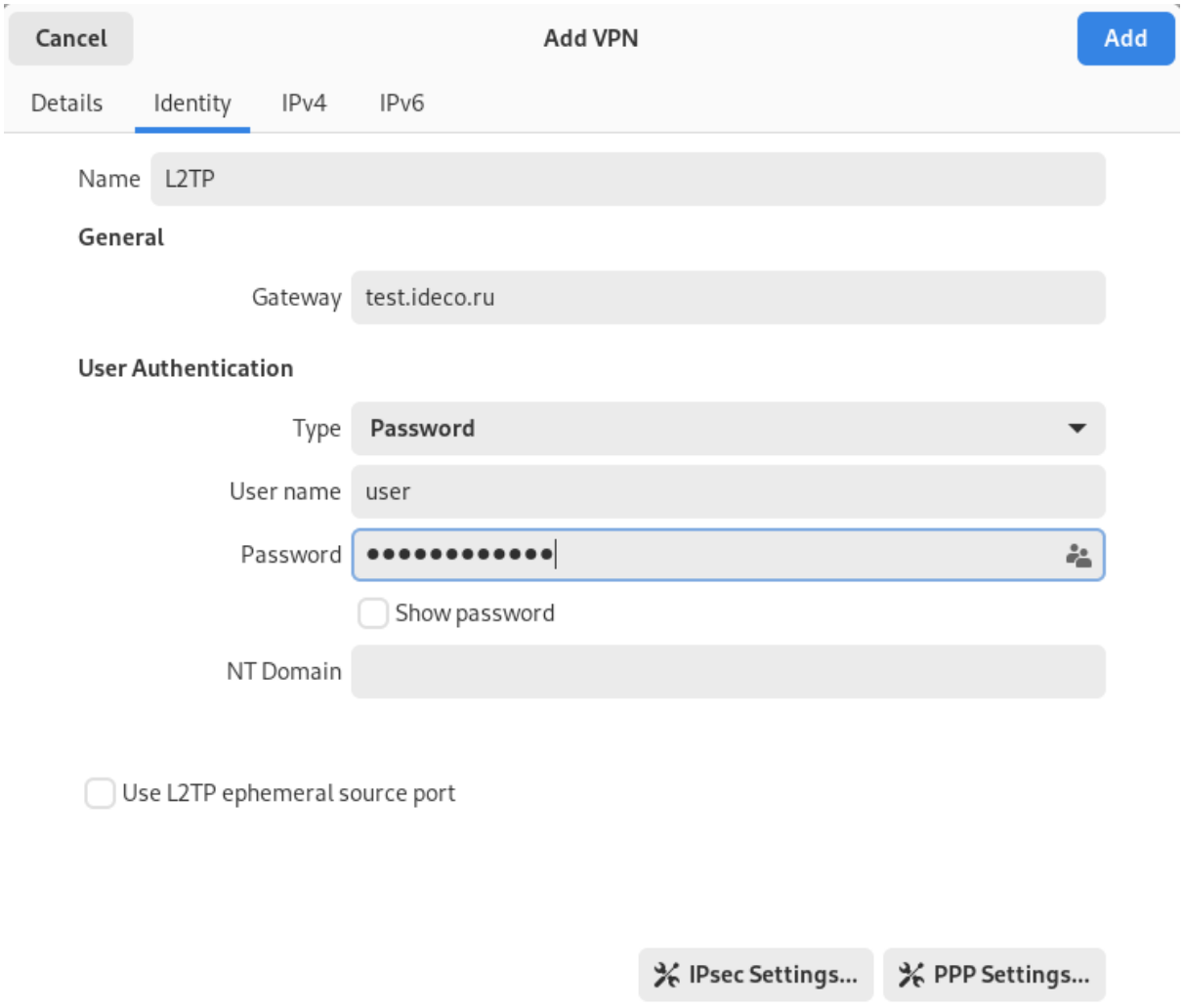
```
sudo reboot
```

4. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + .

5. В окне создания подключений по VPN выберите пункт **Layer 2 Tunneling Protocol (L2TP)**:

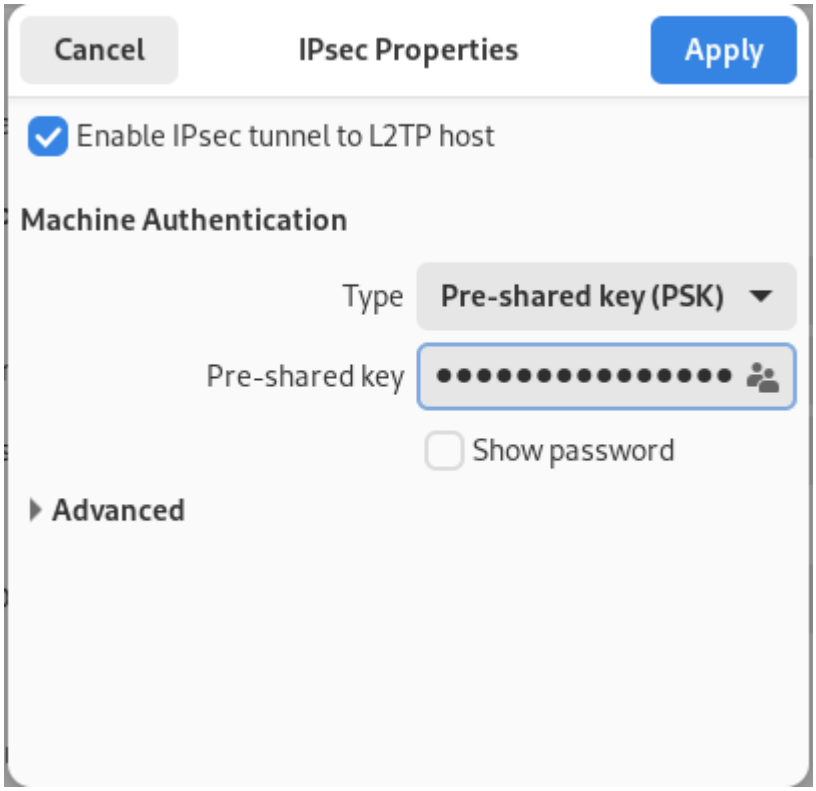


6. На вкладке **Идентификация** заполните следующие поля:



- **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:

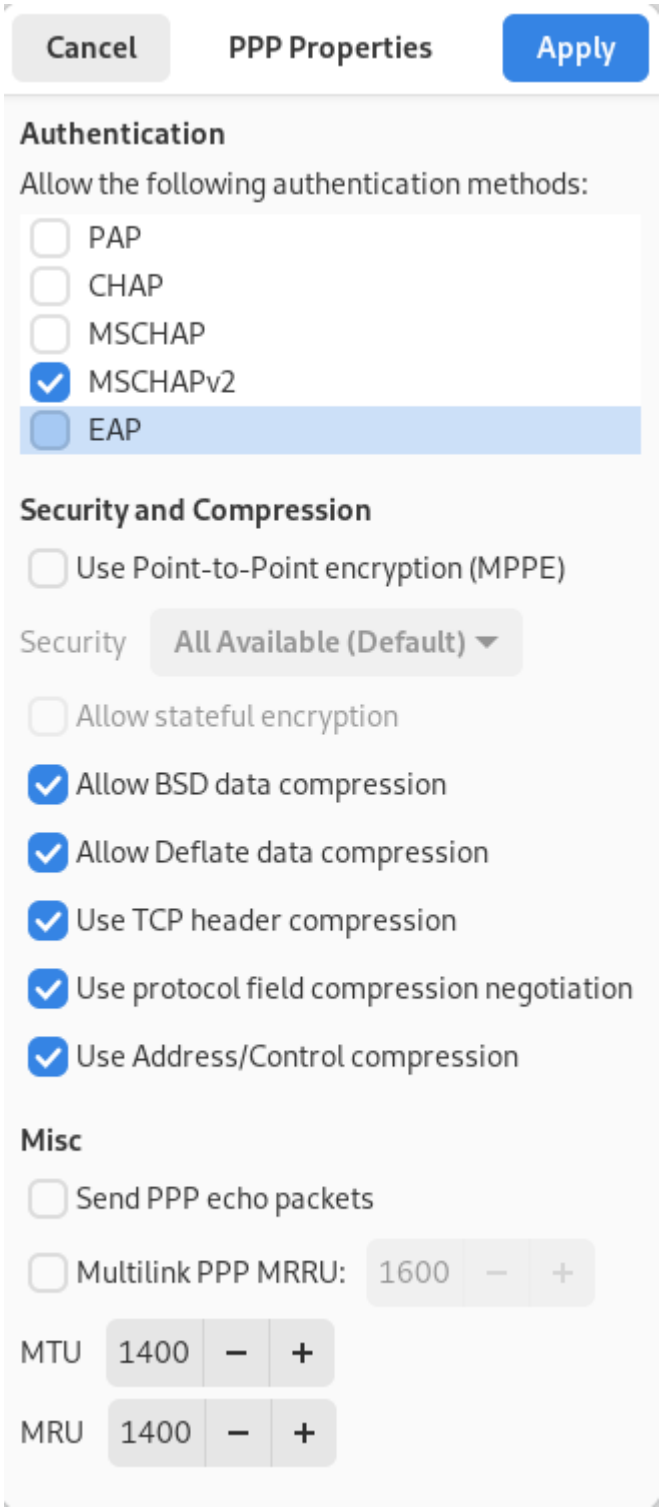


- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу;
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи -> VPN-подключения -> Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения.

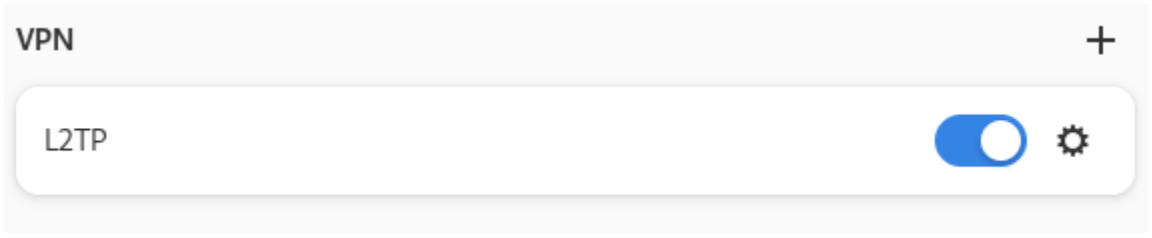
После окончания настройки **L2TP IPsec Options** нажмите **OK**.

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:



22.20.4 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.

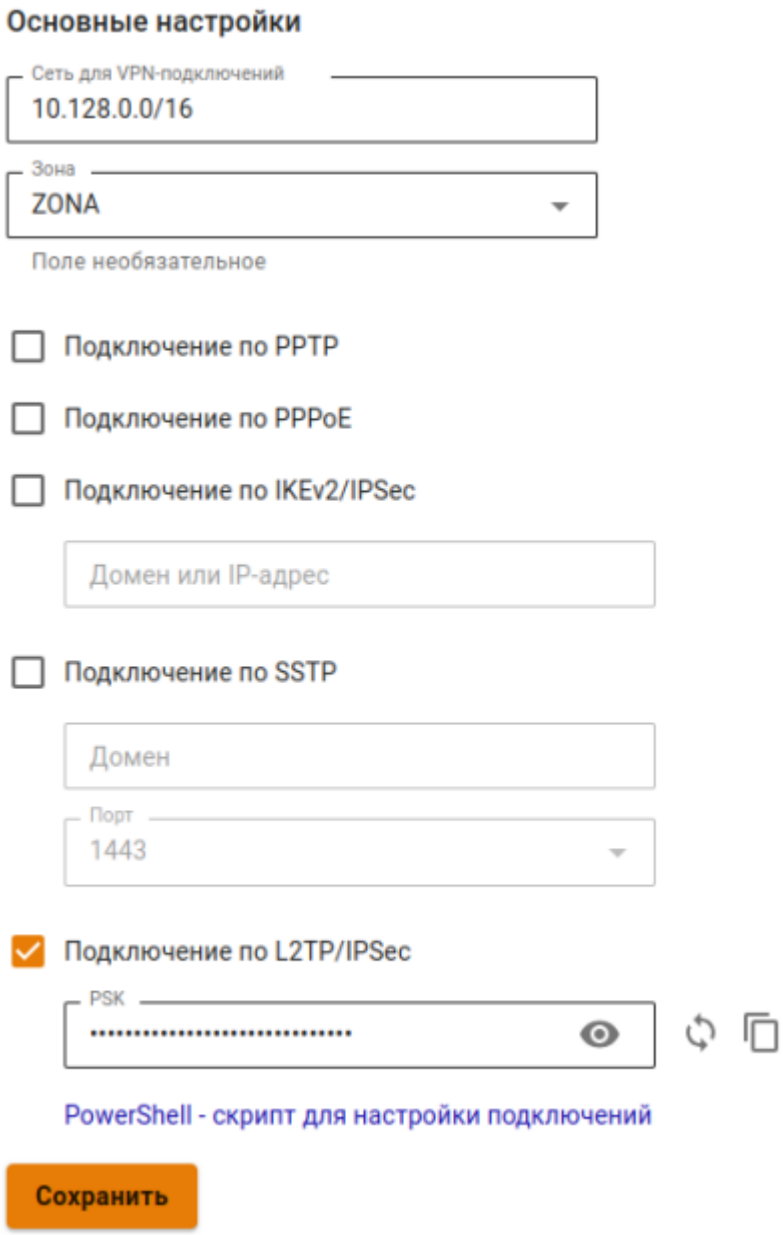
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

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:

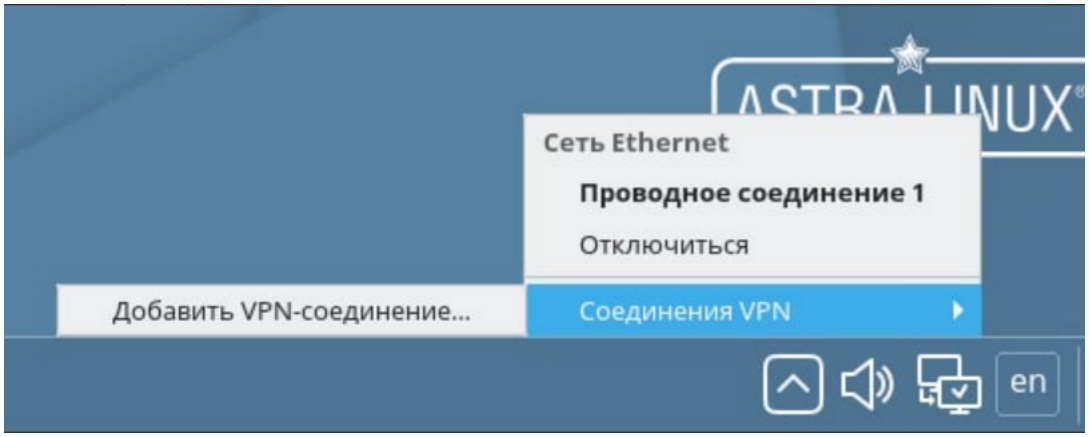


Создание подключения в Astra Linux:

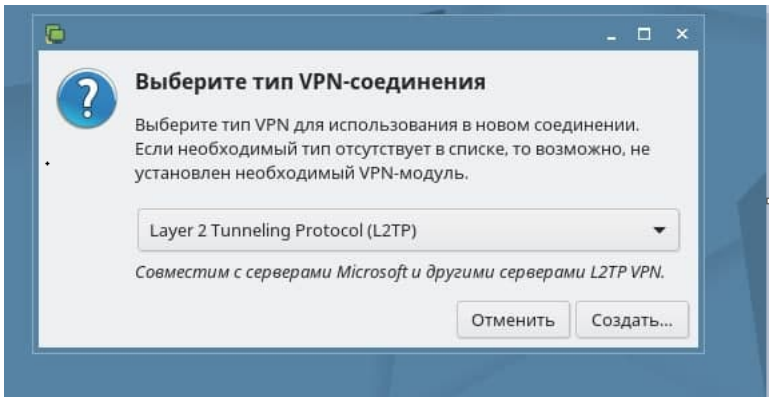
1. Откройте терминал сочетанием клавиш Ctrl+Alt+F1 или через путь **Пуск -> Системные -> Терминал Fly** и выполните три команды:

```
sudo apt update
sudo apt install network-manager-l2tp-gnome
sudo reboot
```

2. В трее (в настройках сети) выберите **Соединение VPN -> Добавить VPN-соединение**:

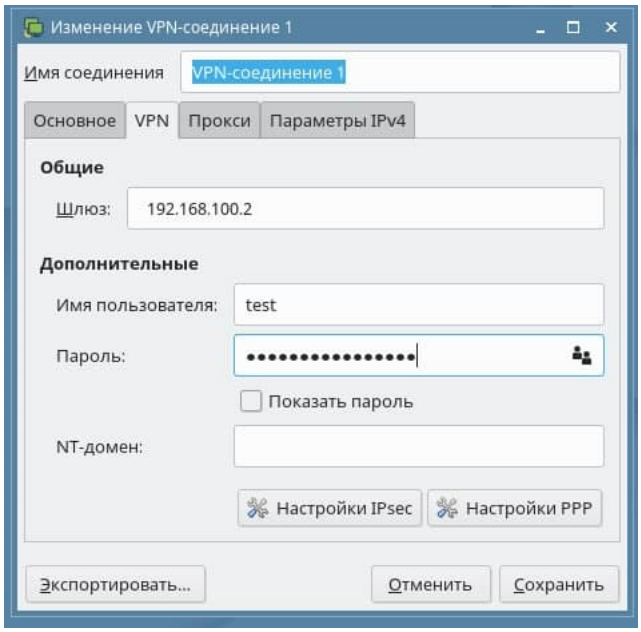


3. Выберите тип соединения **Layer 2 Tunneling Protocol (L2TP)** и нажмите **Создать**:



4. Во вкладке **VPN** заполните поля:

- **Шлюз** - IP-адрес внешнего интерфейса Ideco NGFW или домен;
- **Имя пользователя**;
- **Пароль**.

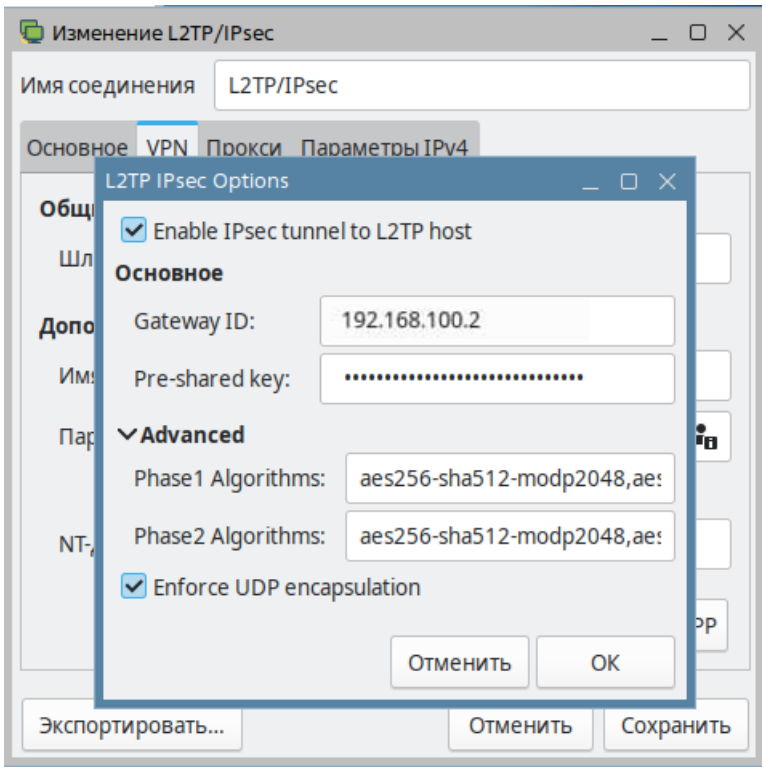


5. Нажмите **Настройки IPsec**.

6. Заполните поля:

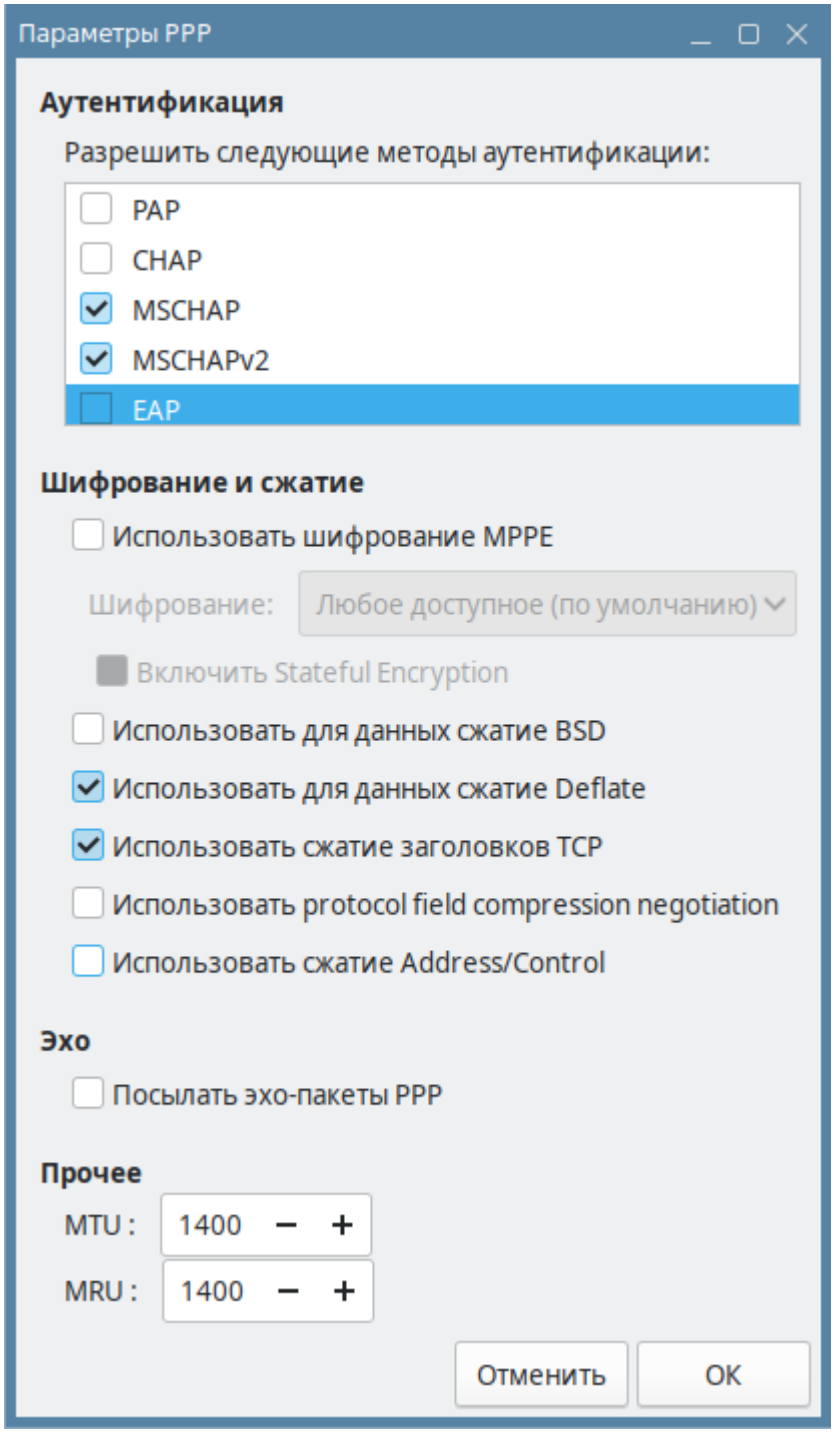
- **Gateway ID** - IP-адрес интерфейса, к которому осуществляется подключение;
- **Pre-shared key** - PSK-ключ из настроек Ideco NGFW (**Пользователи -> VPN-подключение -> Основное**);
- **Phase1 Algorithm** - `aes256-sha512-modp2048,aes256-sha512-modp1024,aes256-sha1-ecp256,aes256-sha1-modp2048,aes256-sha1-modp1024!`; *
- **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.



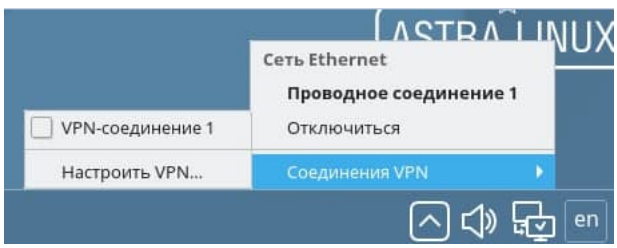
Так как Astra Linux по умолчанию запрашивает не самые защищенные алгоритмы, рекомендуем заполнить их самостоятельно.

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 установите галку **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`

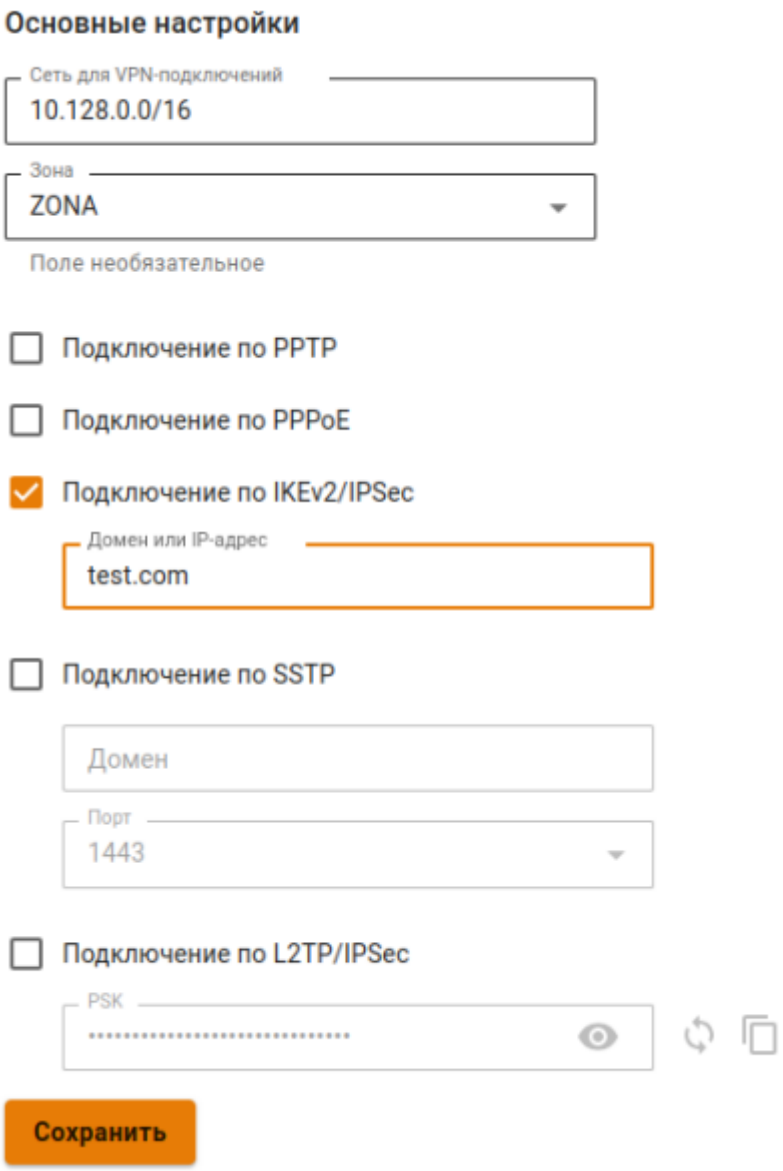
- дляPhase1 Algorithm ищите значения “proposals=”;
- для Phase2 Algorithms ищите значения “esp_proposals=”.

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

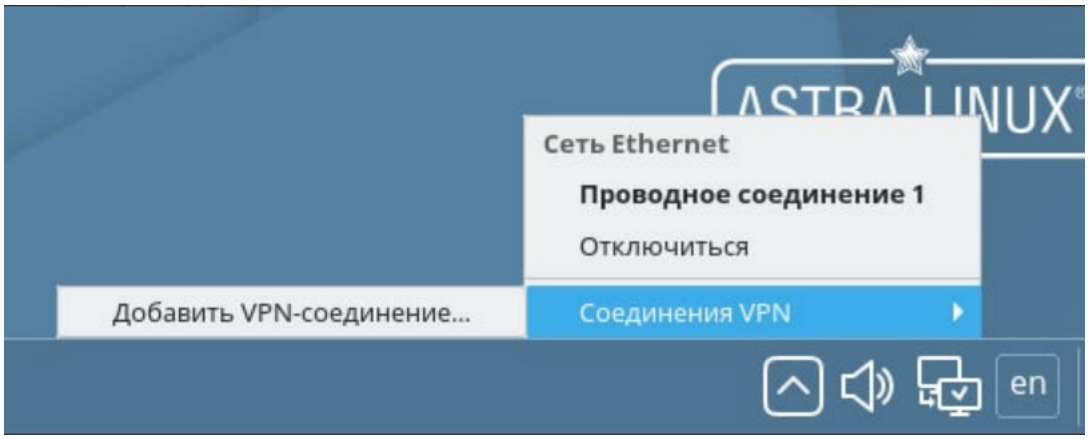
рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в Astra Linux:

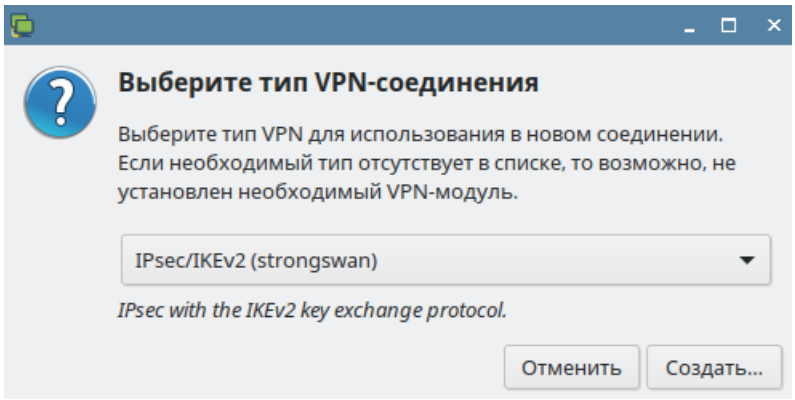
1. Откройте терминал сочетанием клавиш Ctrl+Alt+F1 или через путь **Пуск -> Системные -> Терминал Fly** и выполните три команды:

```
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**:



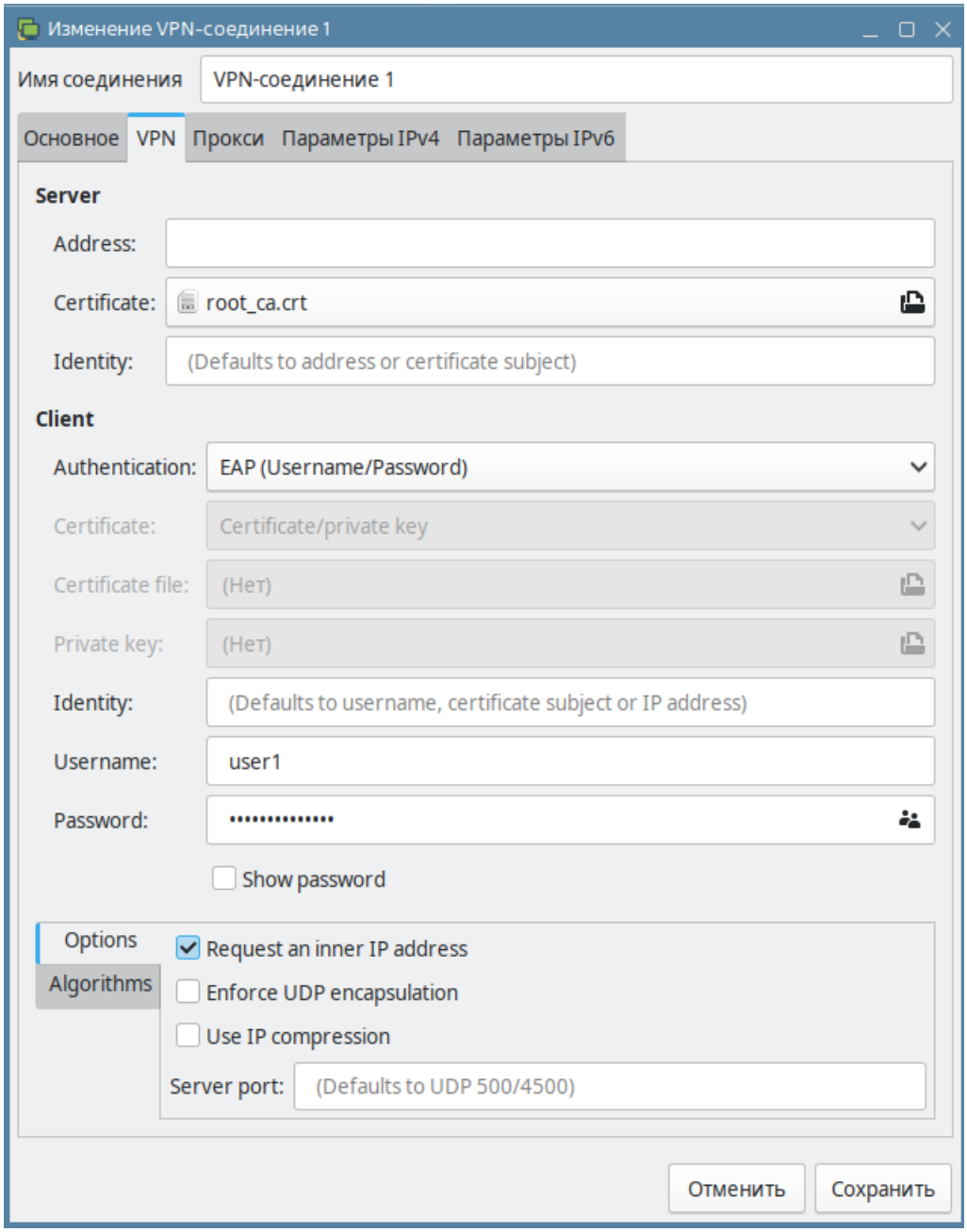
3. Выберите тип соединения **IPsec/IKEv2 (strongswan)** и нажмите **Создать**:



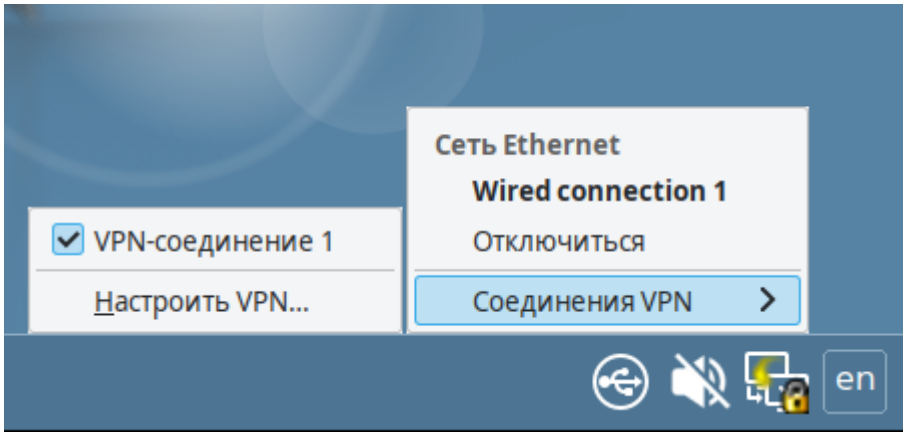
4. Во вкладке **VPN** заполните следующие поля:

- **Имя соединения** - имя подключения;
- **Address** - введите домен, который указан в настройках **Пользователи -> VPN-подключение -> 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.



22.20.5 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.

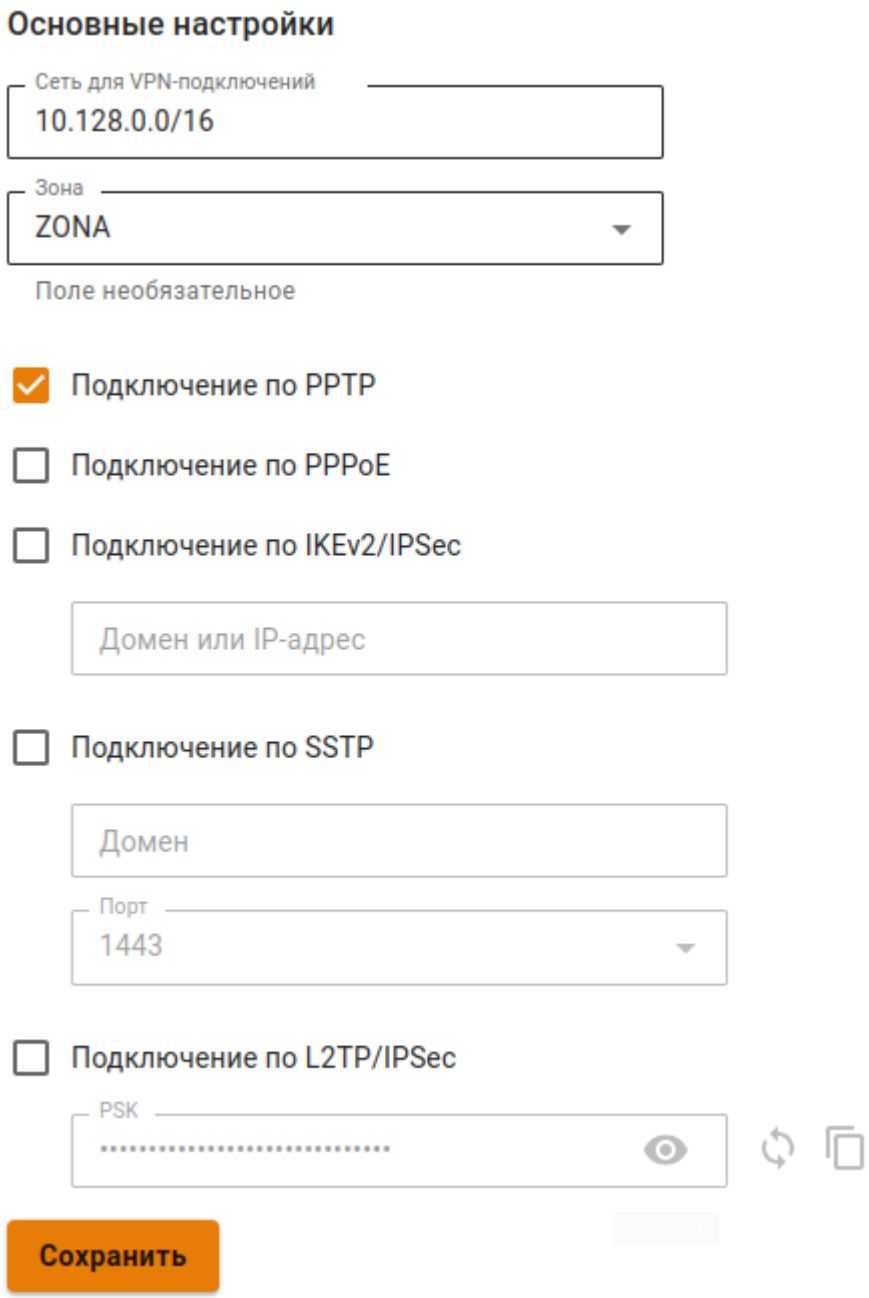
Создание VPN-подключения в Windows

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:

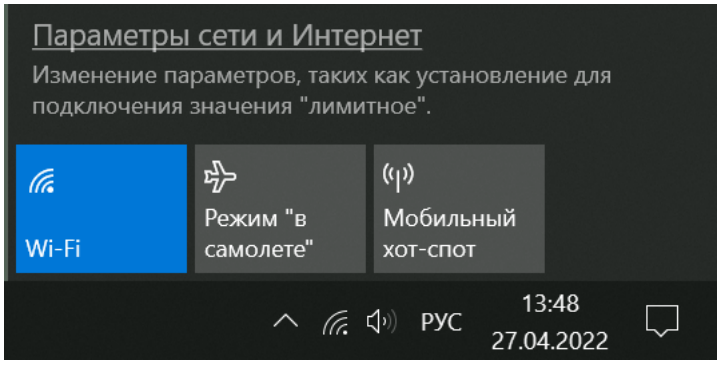
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное** и установите флаг **Подключение по PPTP**:

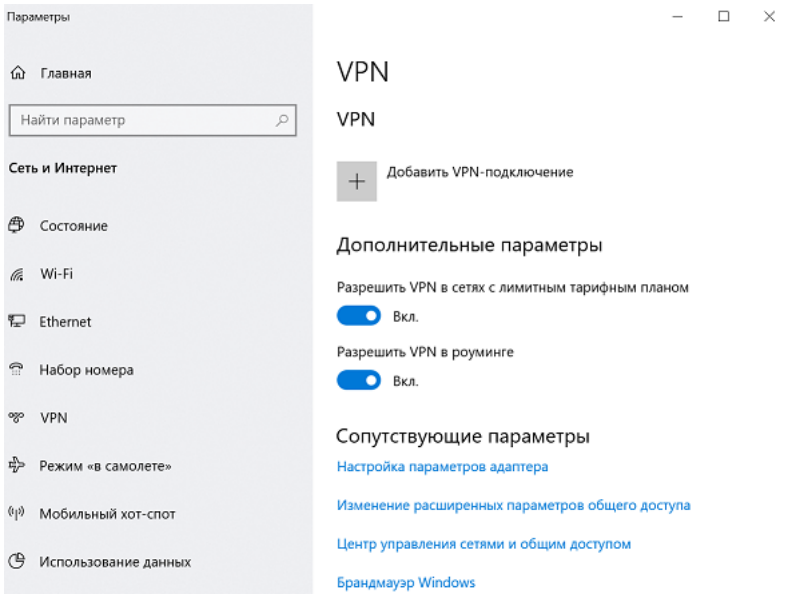


Создание подключения в Windows:

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**:

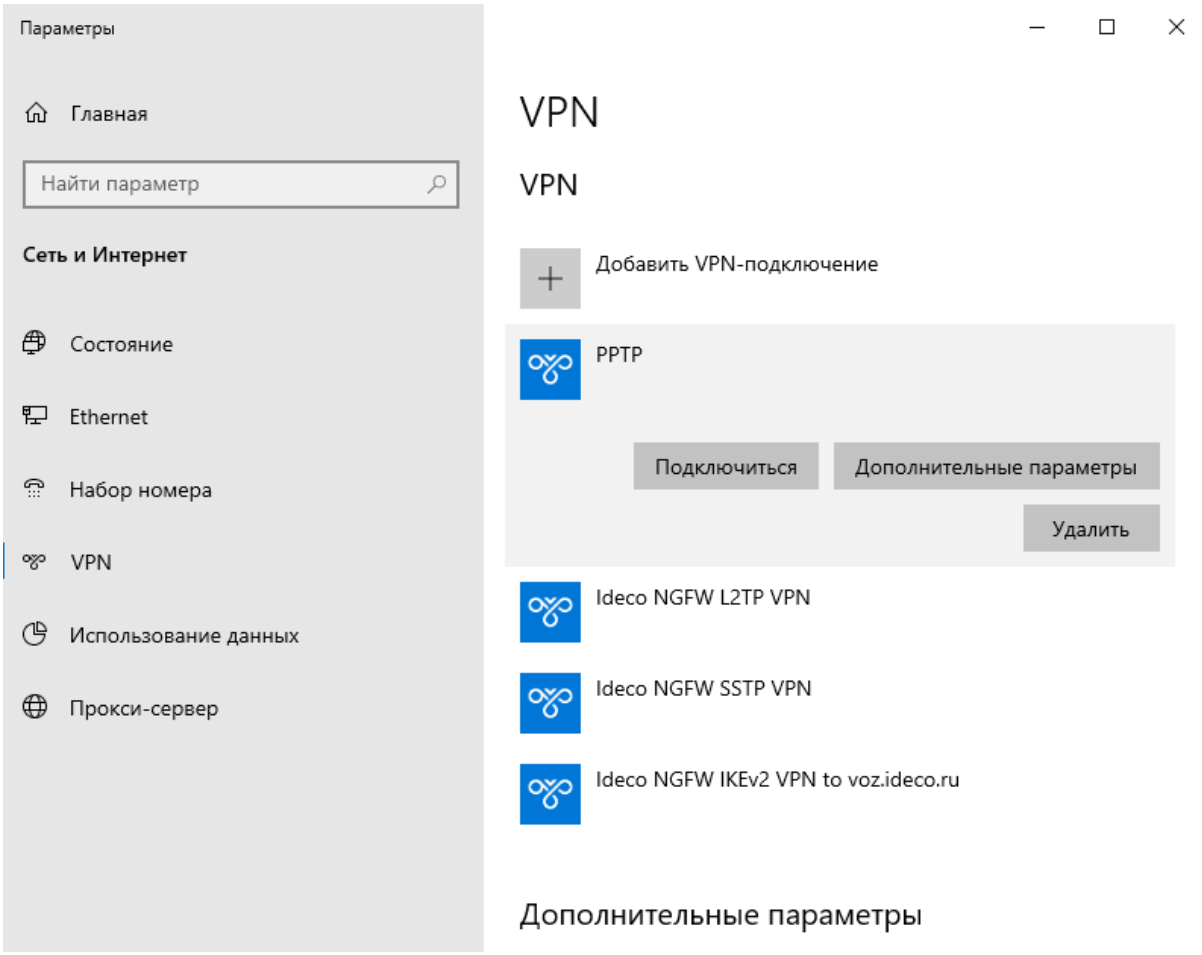
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол PPTP;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

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**.

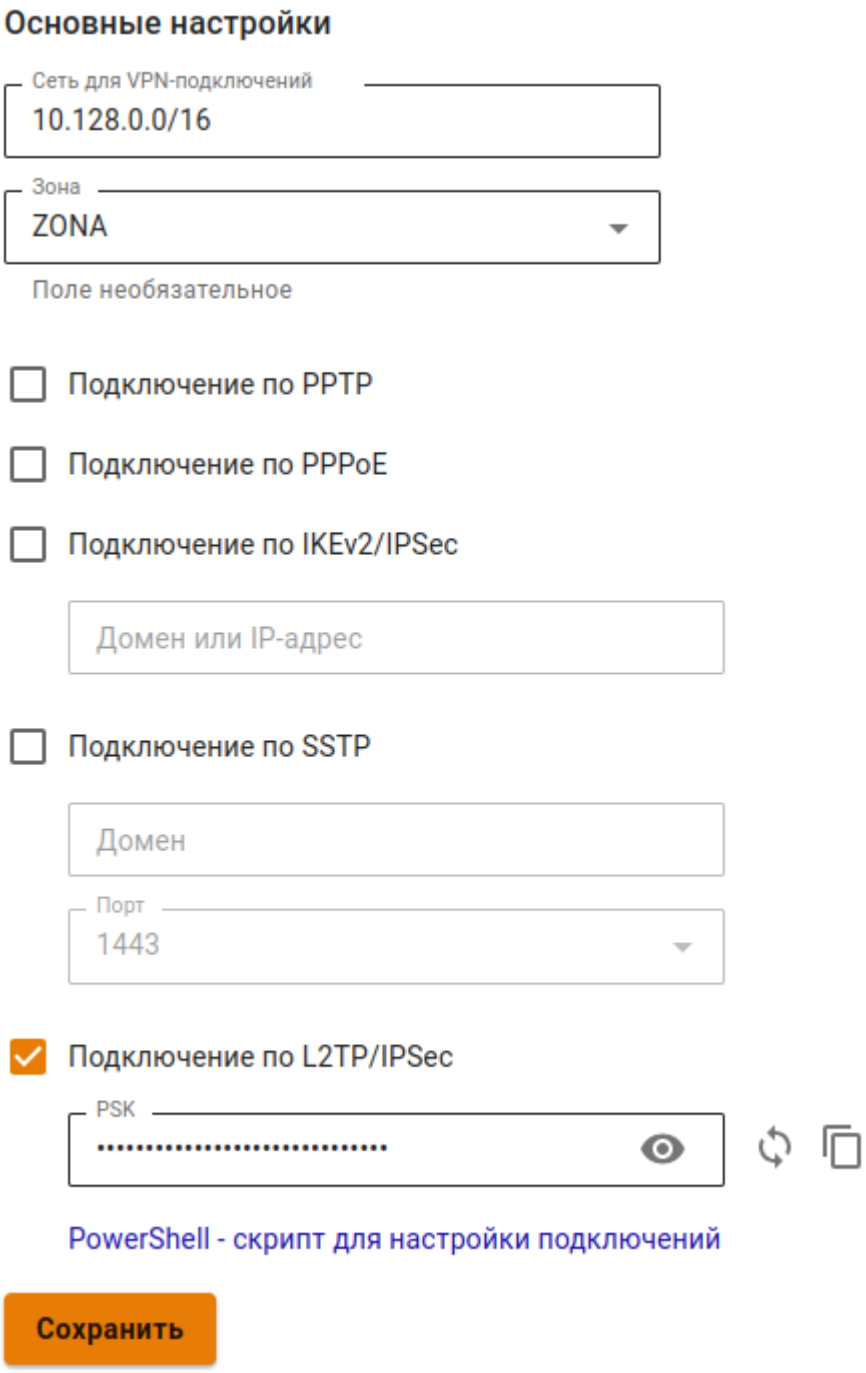
Протокол L2TP/IPsec с общим ключом:

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:

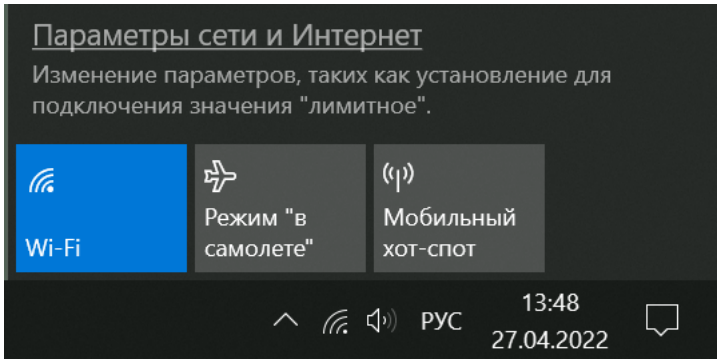
1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

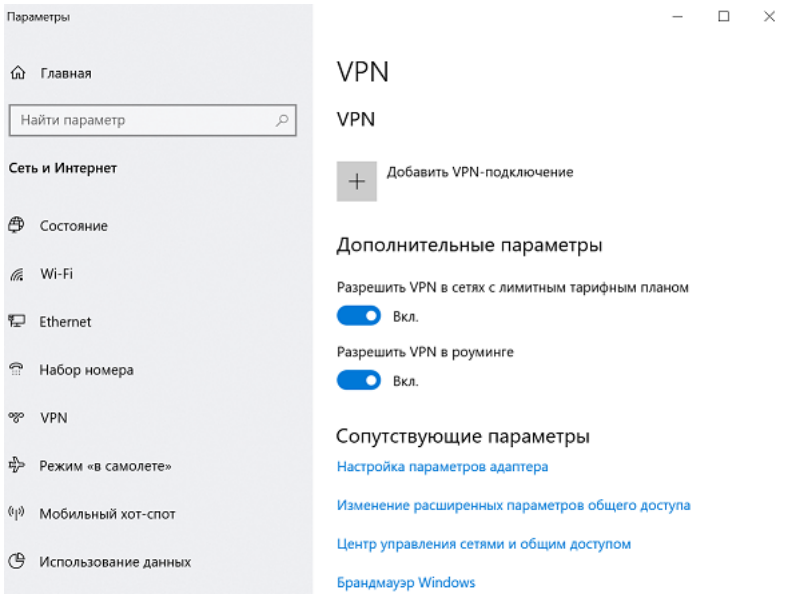


Создание подключения в Windows:

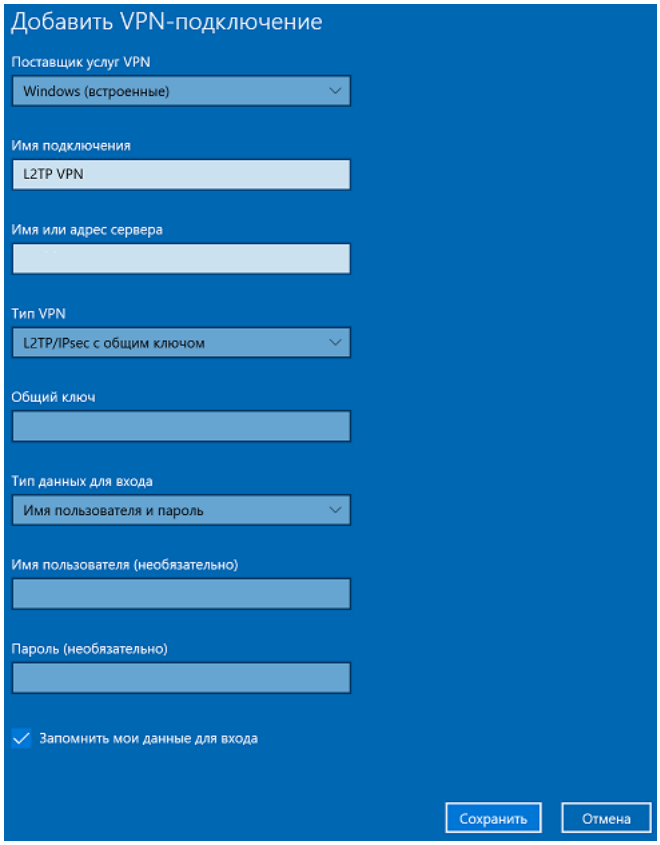
1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



2. Перейдите в раздел **VPN** и нажмите **Добавить VPN-подключение**:



3. Заполните соответствующие поля и нажмите **Сохранить**:



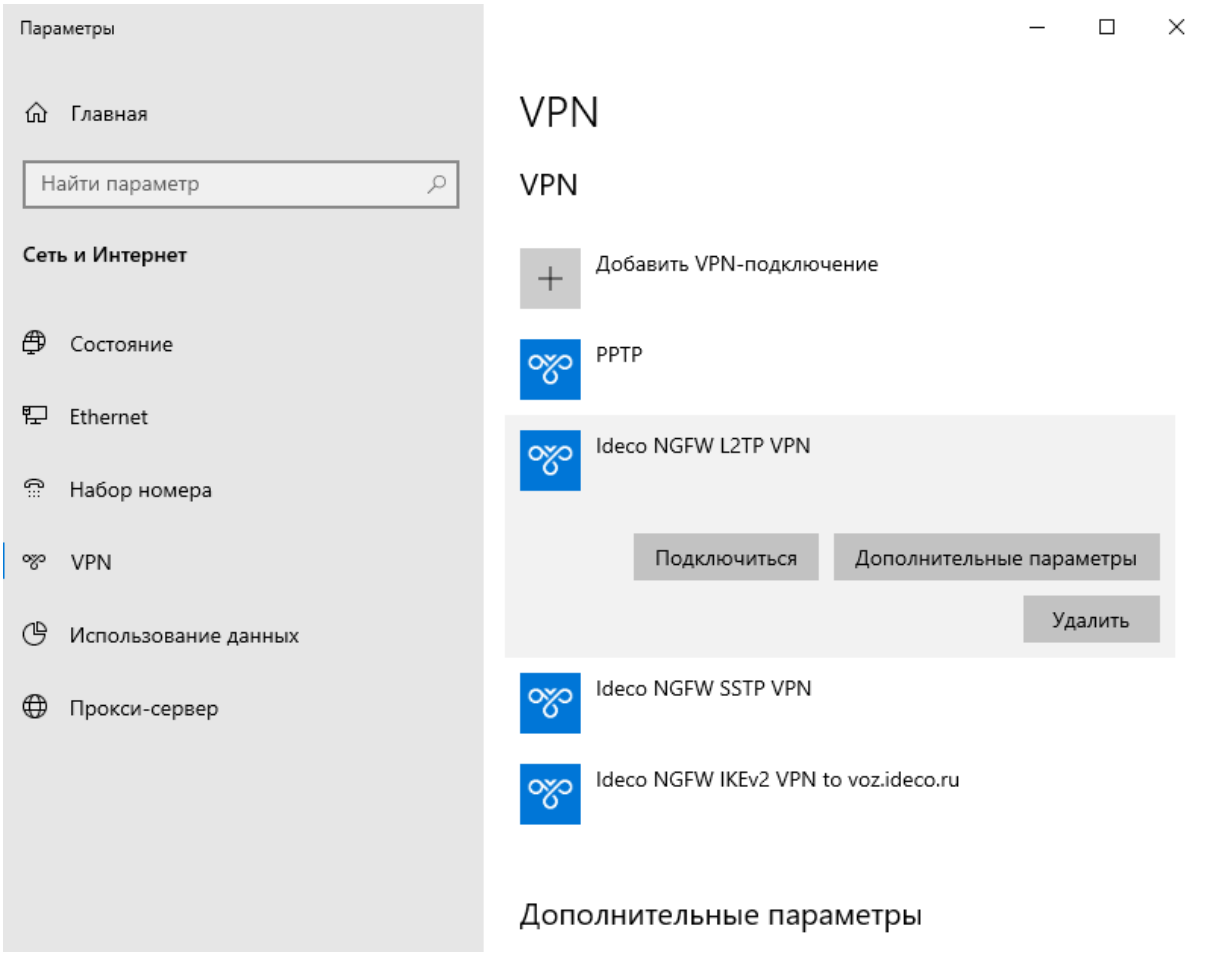
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол L2TP/IPsec с общим ключом;
- **Общий ключ** - значение строки **PSK** в разделе **Пользователи -> VPN-подключения -> Основное -> Подключение по L2TP/IPsec**;
- **Тип данных 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.

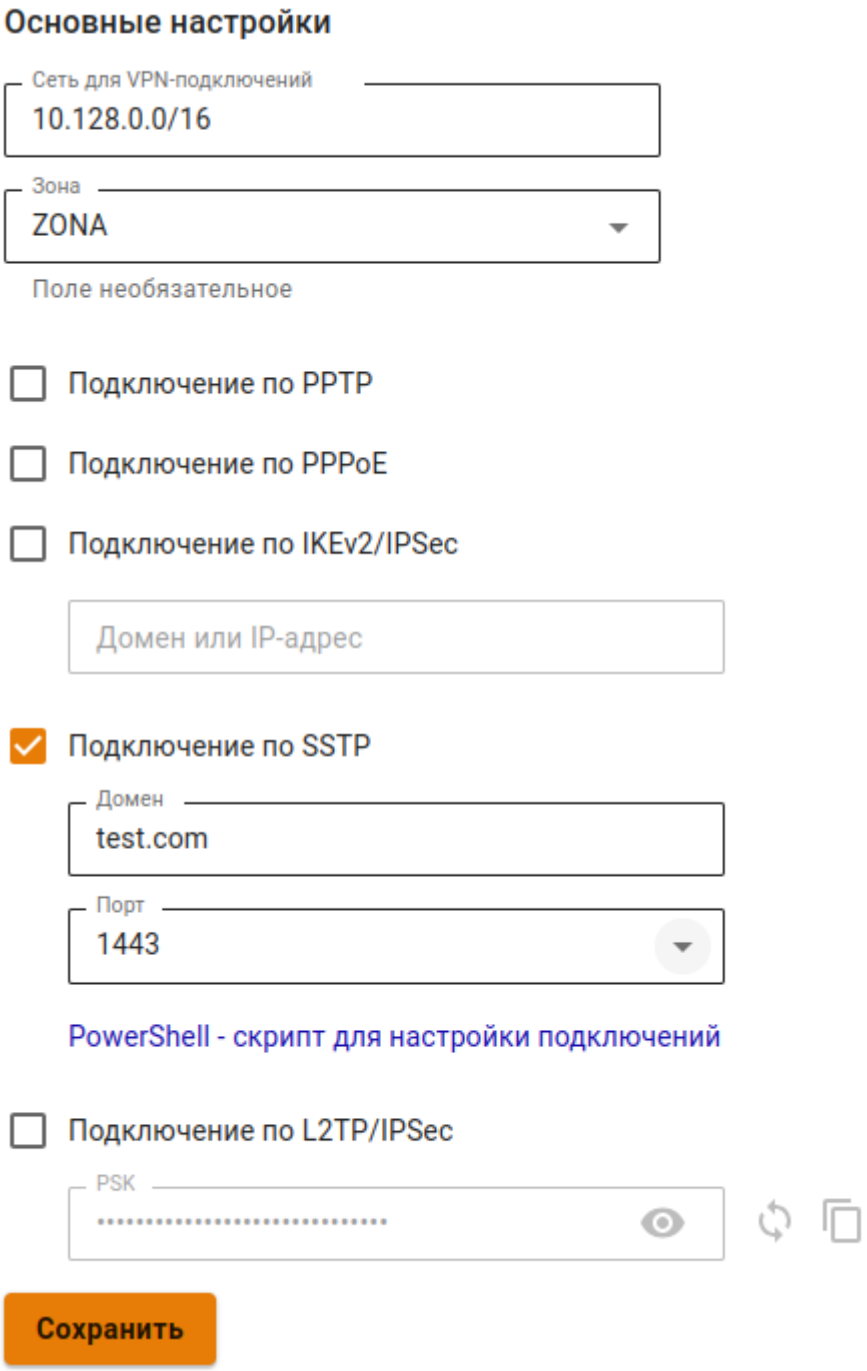
Убедитесь, что локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. Если пересекается, то доступа к сети организации не будет (трафик по таблице маршрутизации пойдет в физический интерфейс, а не в VPN). Адресацию необходимо менять.

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**:

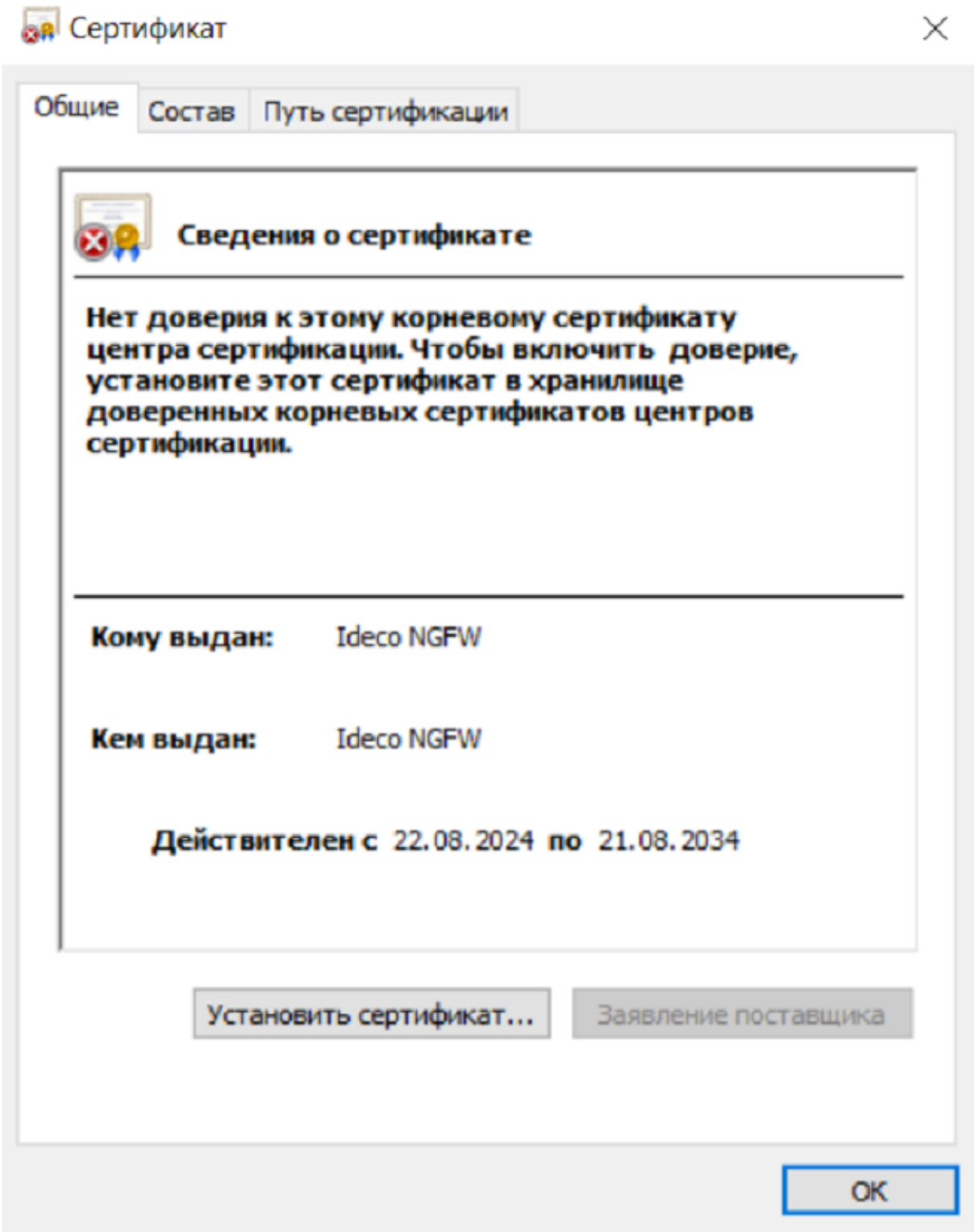


3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

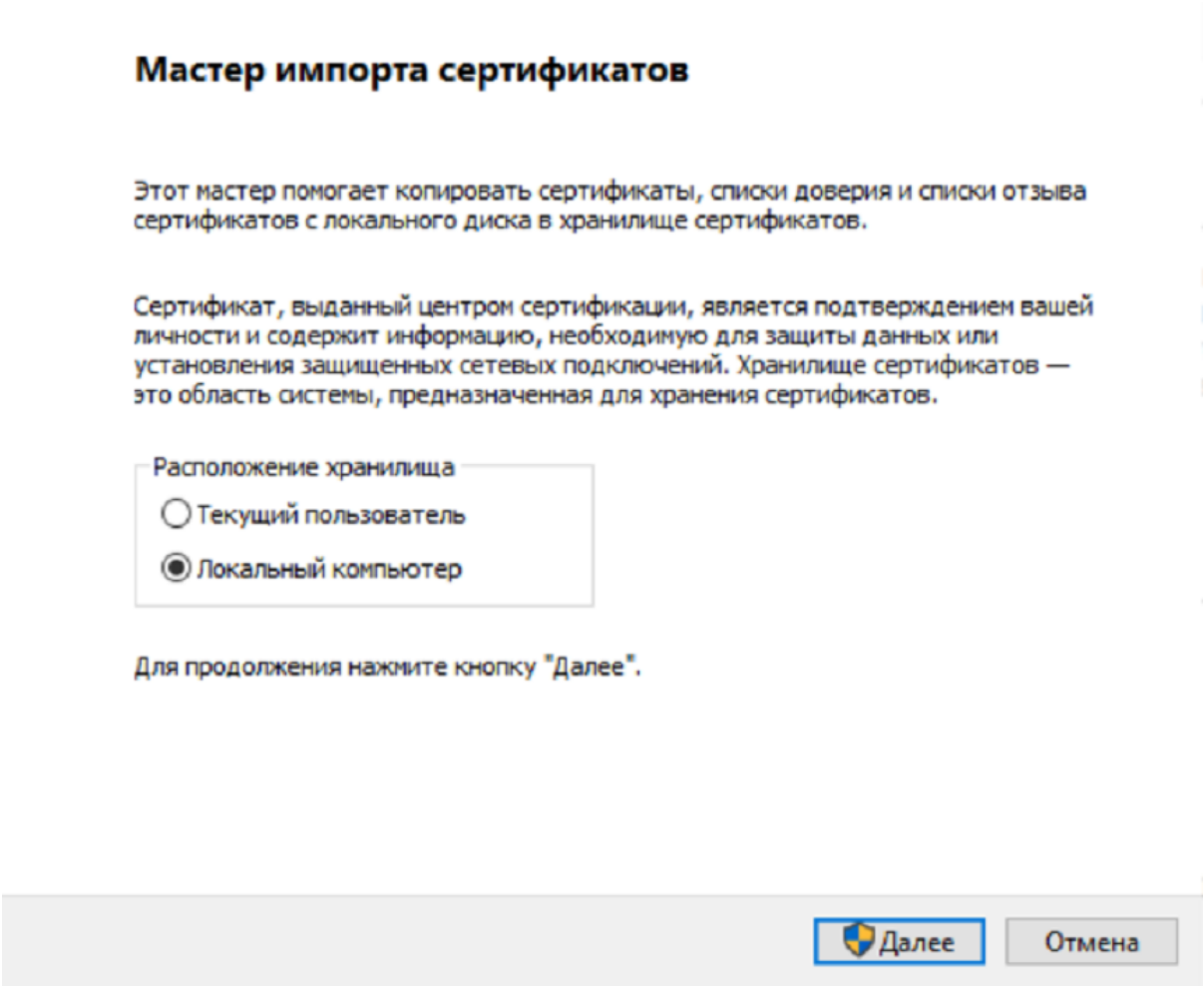
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

4. Импортируйте сертификат Ideco NGFW в Windows. Для этого выполните действия:

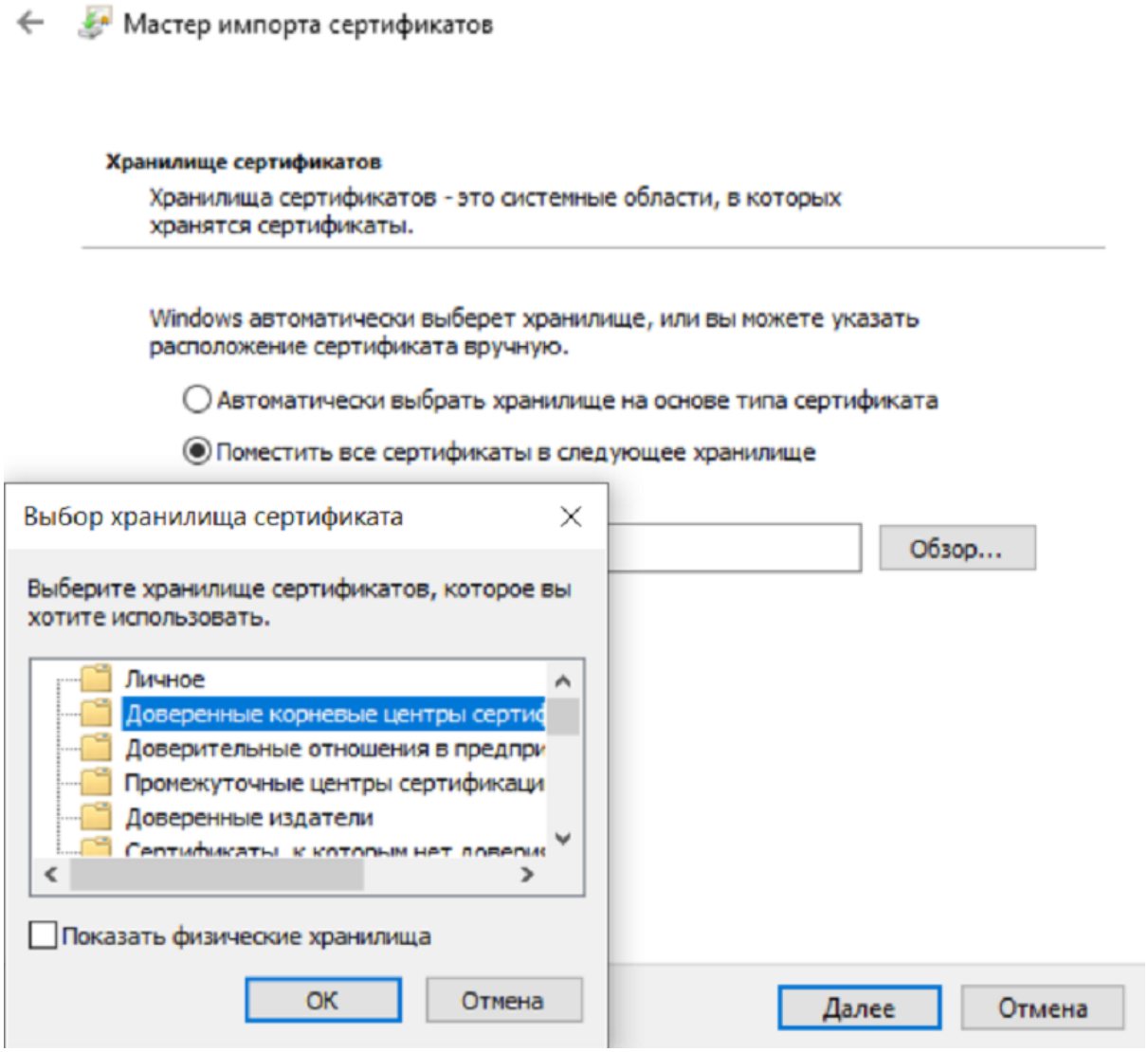
- Откройте скачанный сертификат и нажмите **Установить сертификат**:



- Для корректной настройки выберите расположение хранилища **Локальный компьютер**:

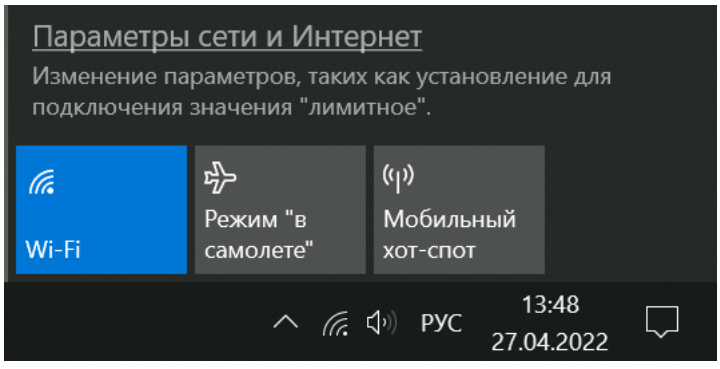


- Установите сертификат в **Доверенные корневые центры сертификации**:

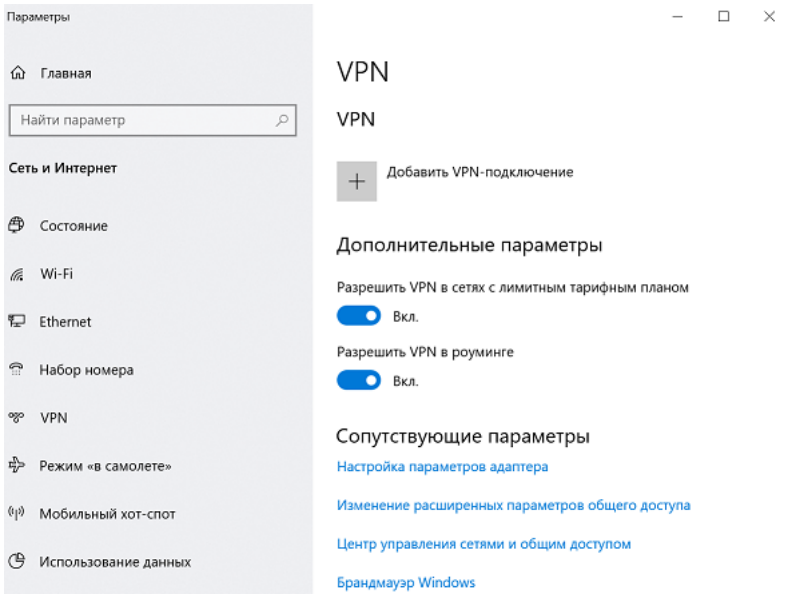


Создание подключения в Windows:

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**:

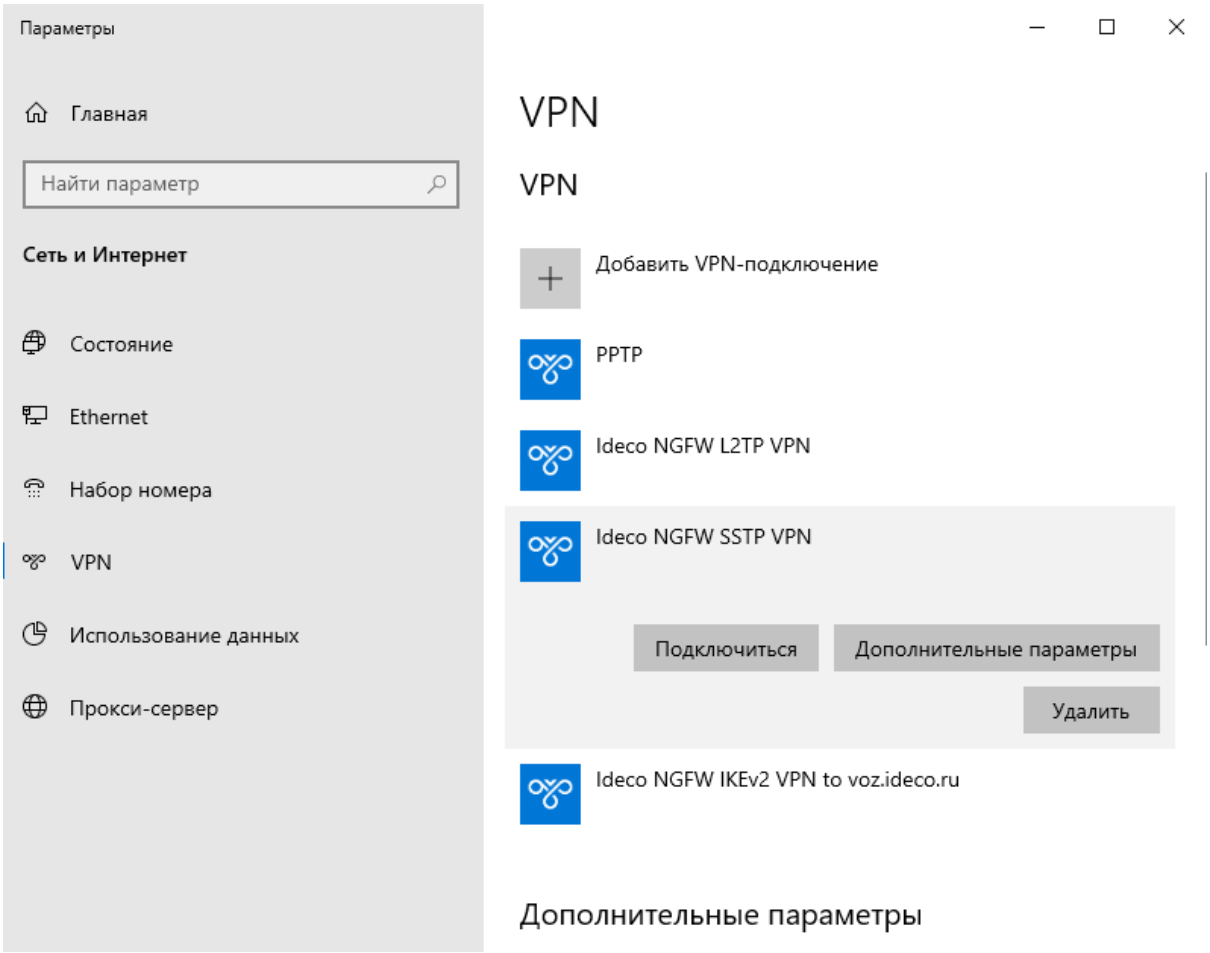
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера в формате *адрес_VPN_сервера:порт*;
- **Тип VPN** - протокол SSTP;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение 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**:



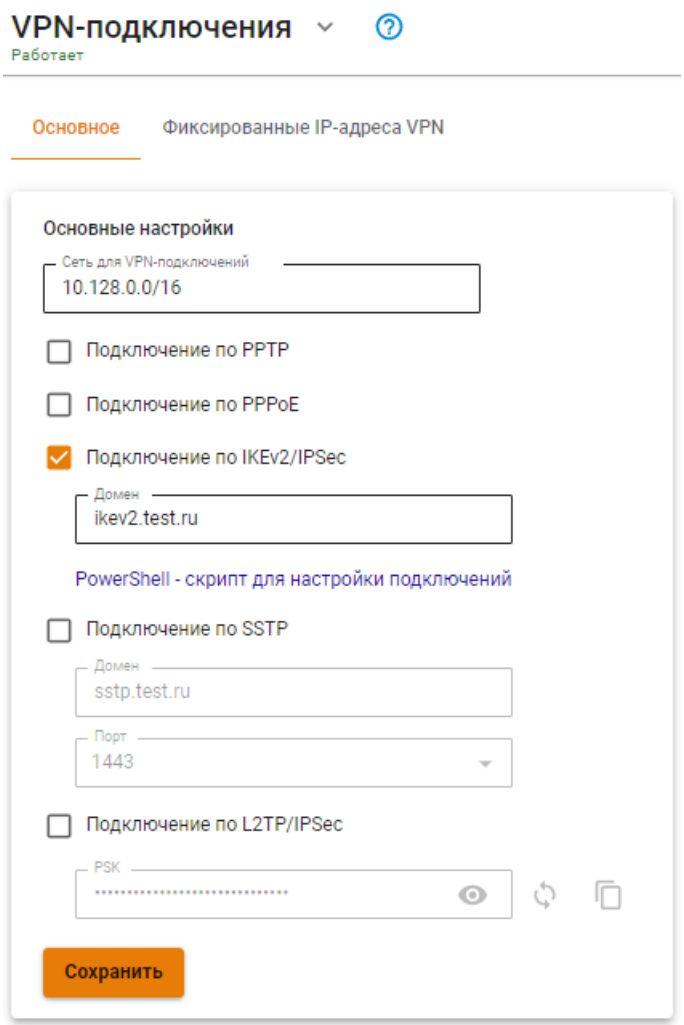
7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры -> Изменить**.

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**:

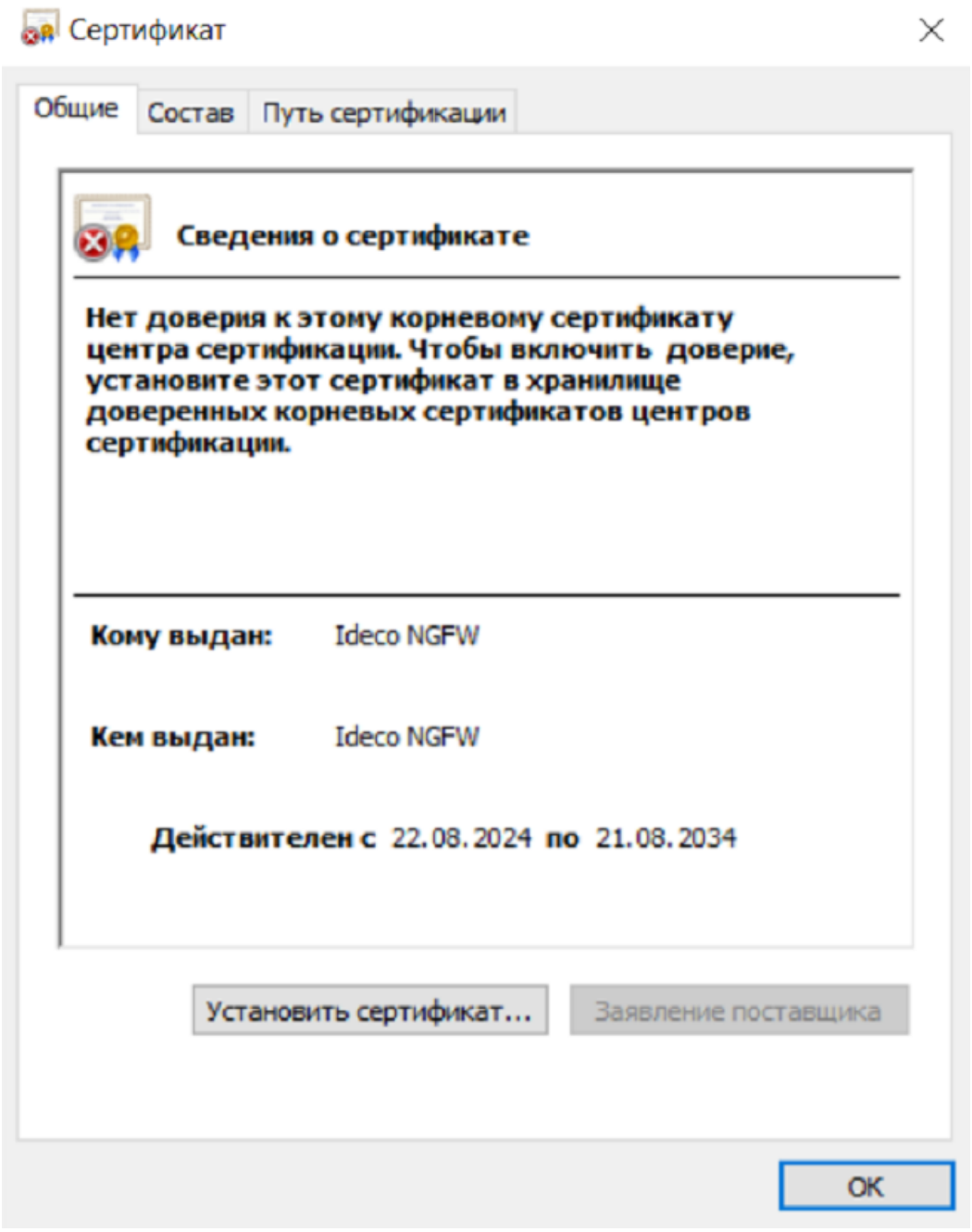


3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

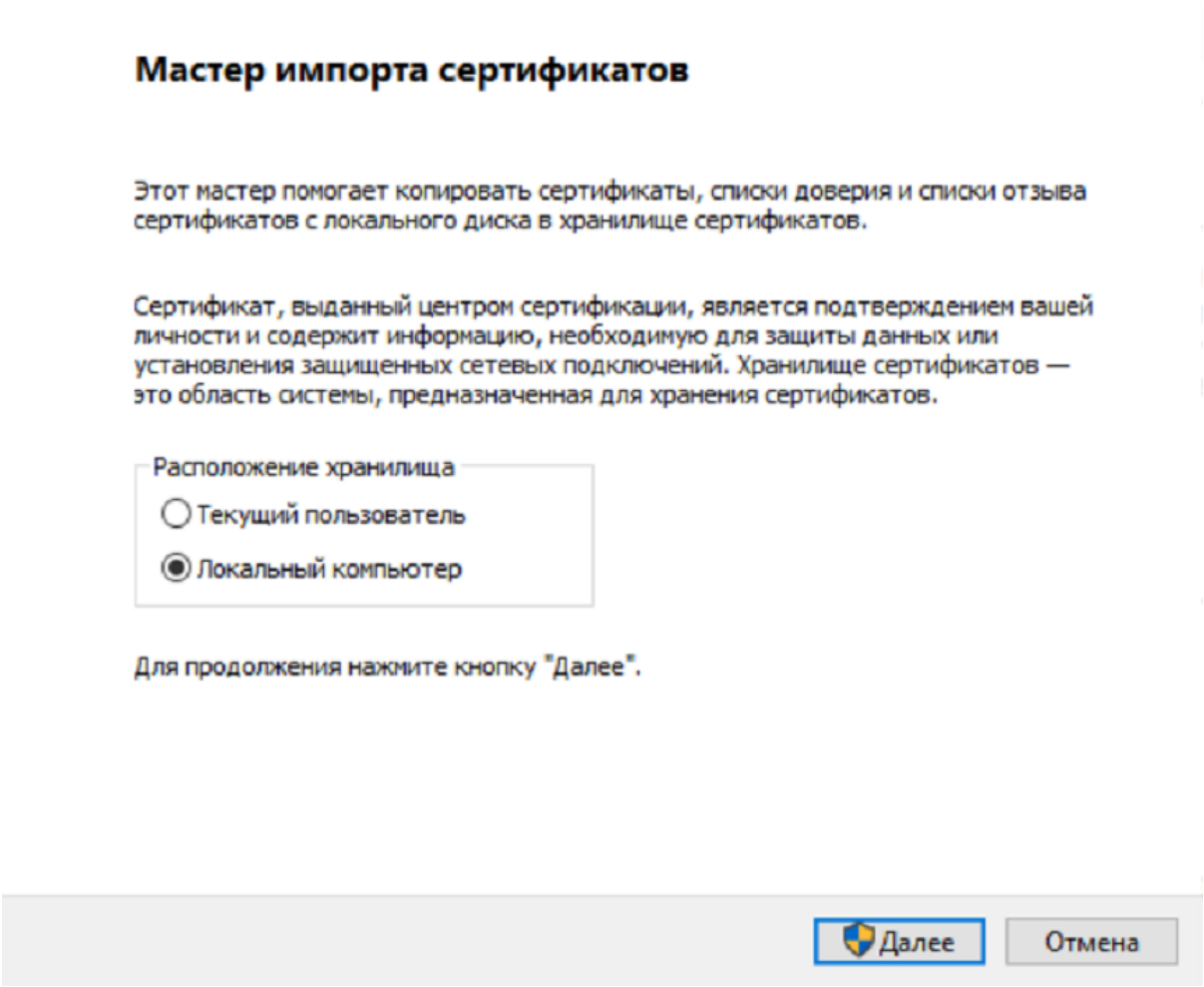
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

4. Импортируйте сертификат Ideco NGFW в Windows. Для этого выполните действия:

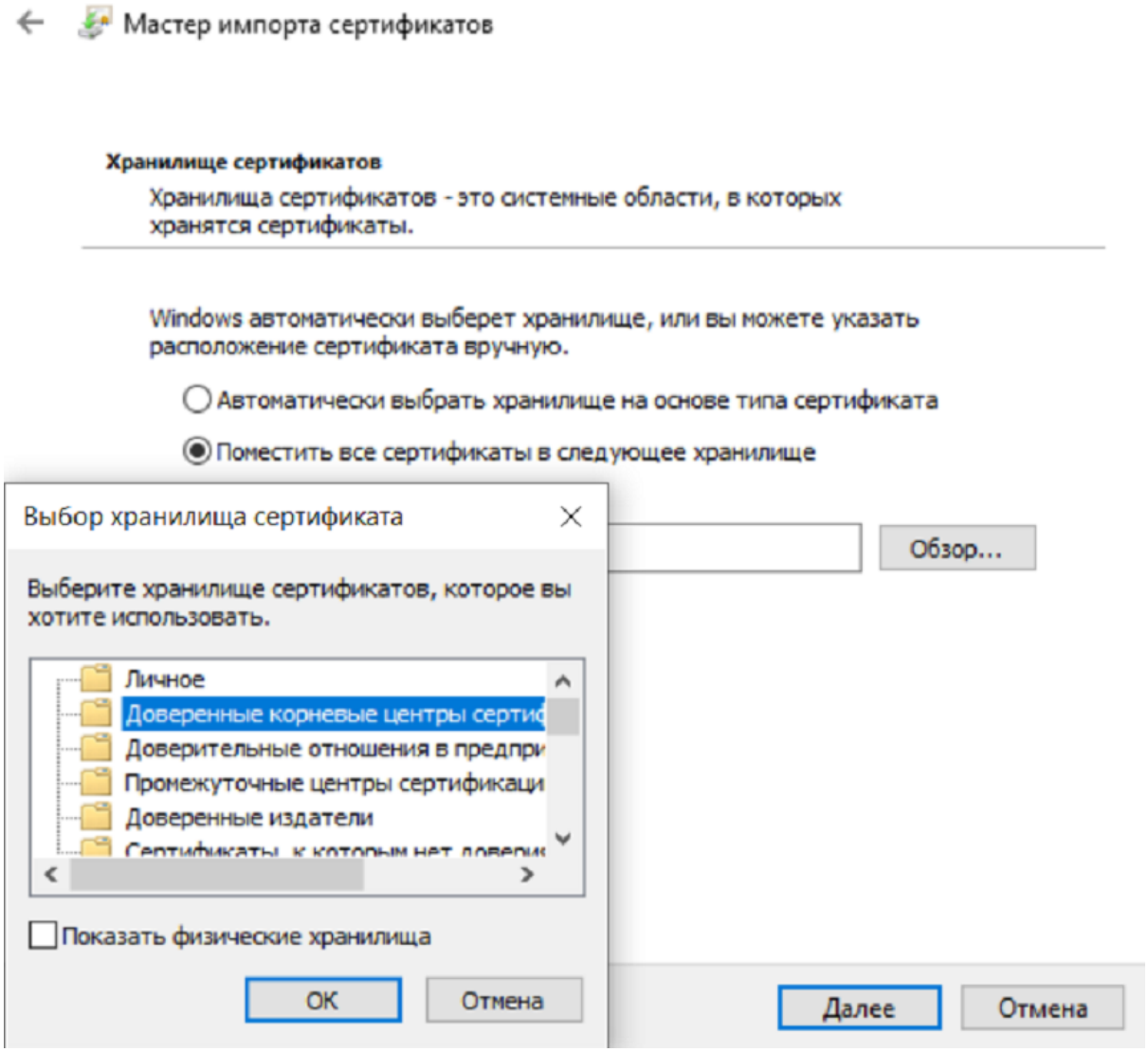
- Откройте скачанный сертификат и нажмите **Установить сертификат**:



- Для корректной настройки выберите расположение хранилища **Локальный компьютер**:

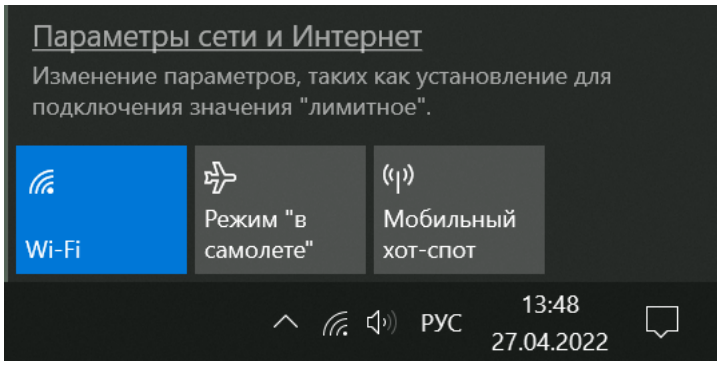


- Установите сертификат в **Доверенные корневые центры сертификации**:

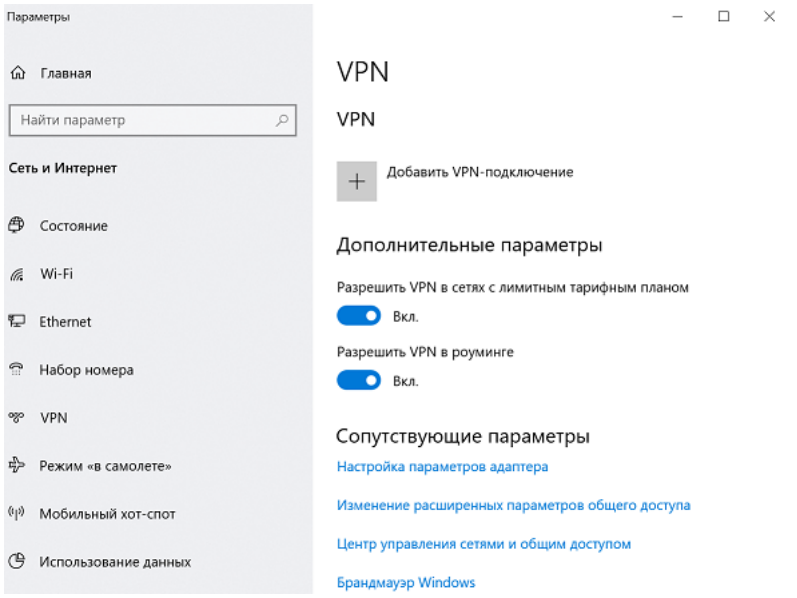


Создание подключения в Windows:

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**:

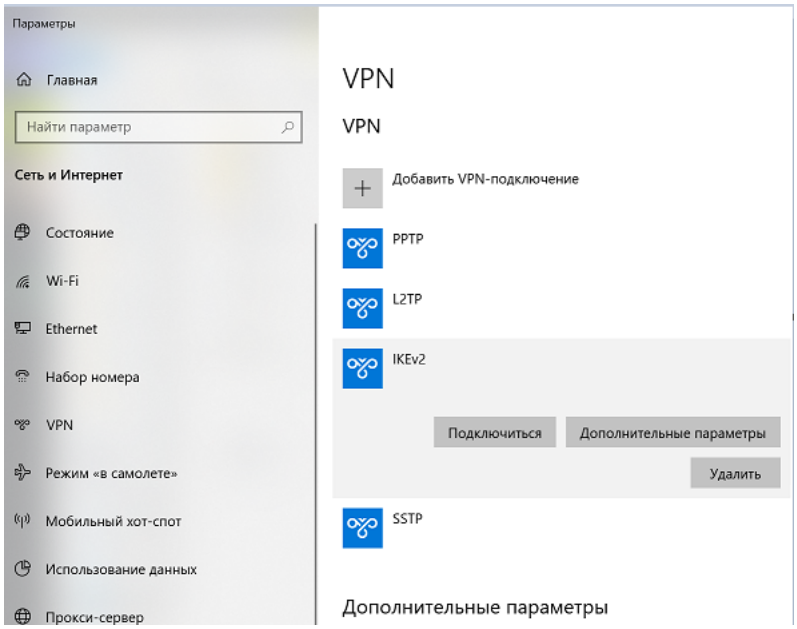
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол IKEv2;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

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

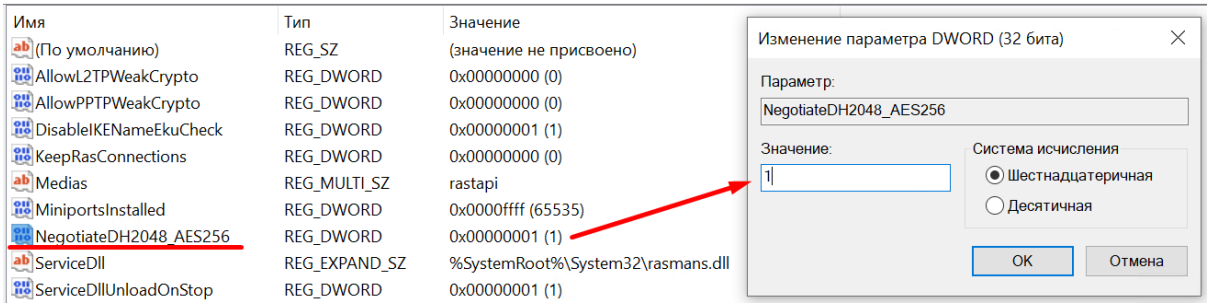
Если при подключении по IKEv2 возникает «Ошибка сопоставления групповой политики» или ошибка с кодом «13868»:

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:

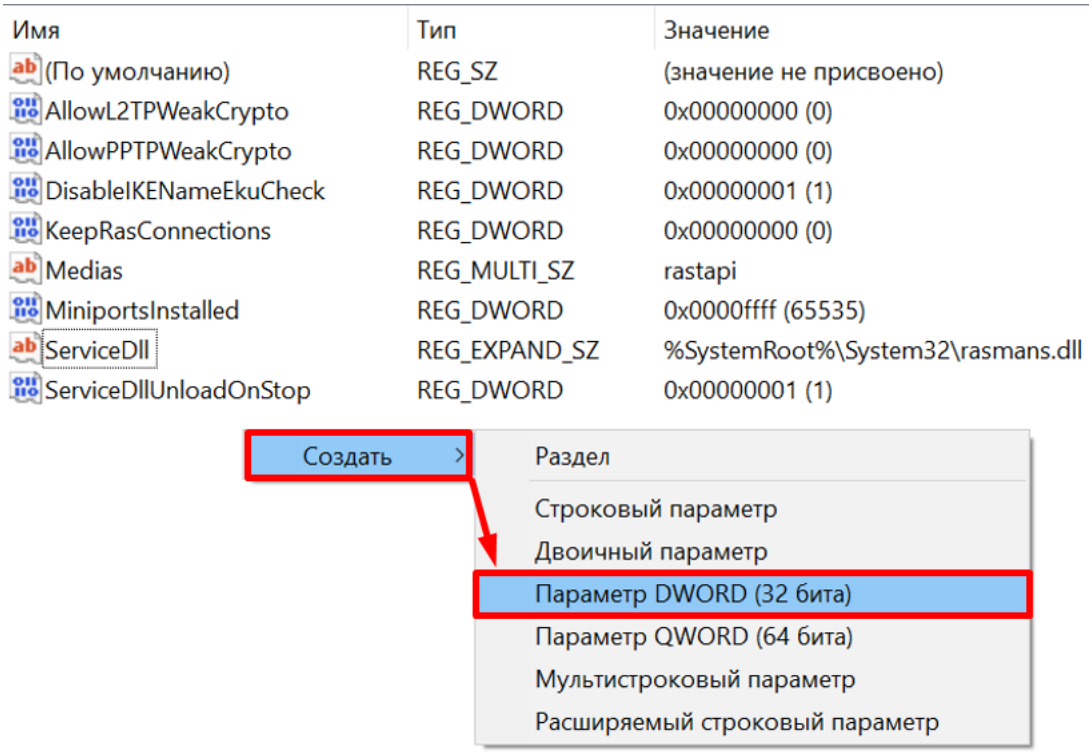
- Откройте **Редактор реестра**;
- Перейдите по пути `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters`;
- Нажмите правой кнопкой мыши по параметру с именем **NegotiateDH2048_AES256** и нажмите **Изменить**;
- В строке **Значение** укажите значение `1`:



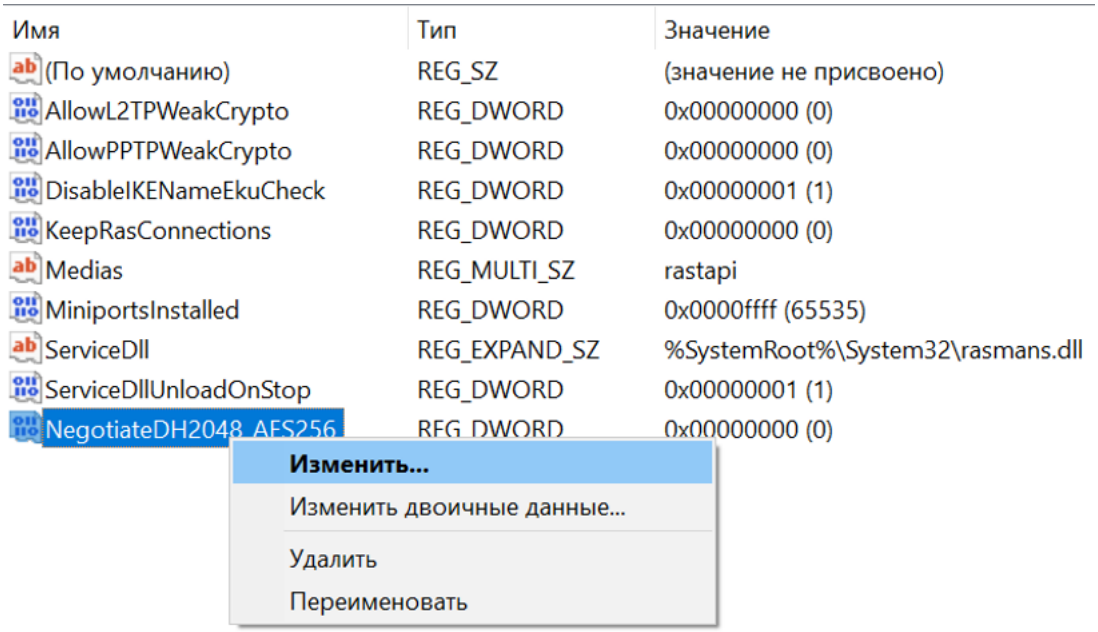
- Нажмите **OK**;
- Перезагрузите Windows.

  Если параметра с именем **NegotiateDH2048_AES256** нет, то создайте его. Для этого:

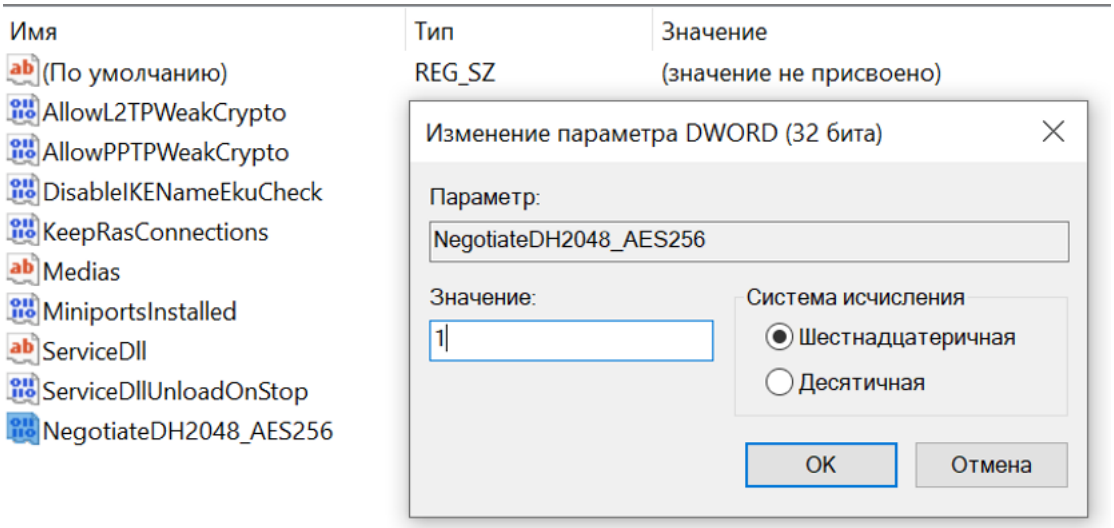
- Нажмите правой кнопкой мыши по свободному месту реестра в **Parameters** и выберите **Создать -> DWORD**:



- 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*.

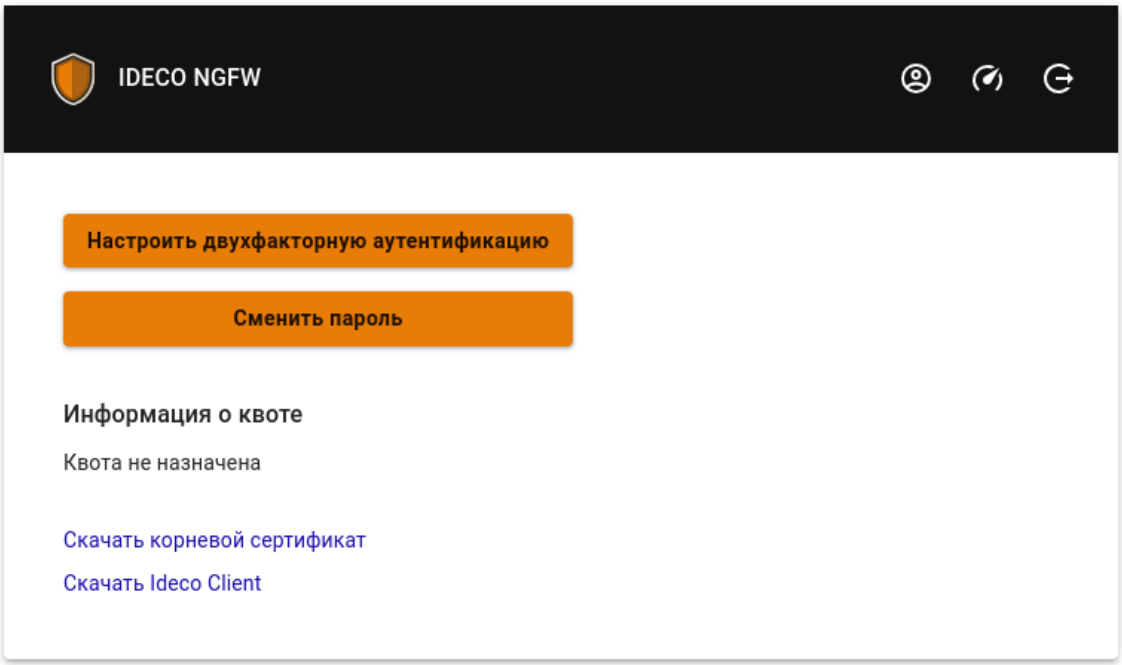
22.20.6 Создание VPN-подключения на мобильных устройствах

Основное

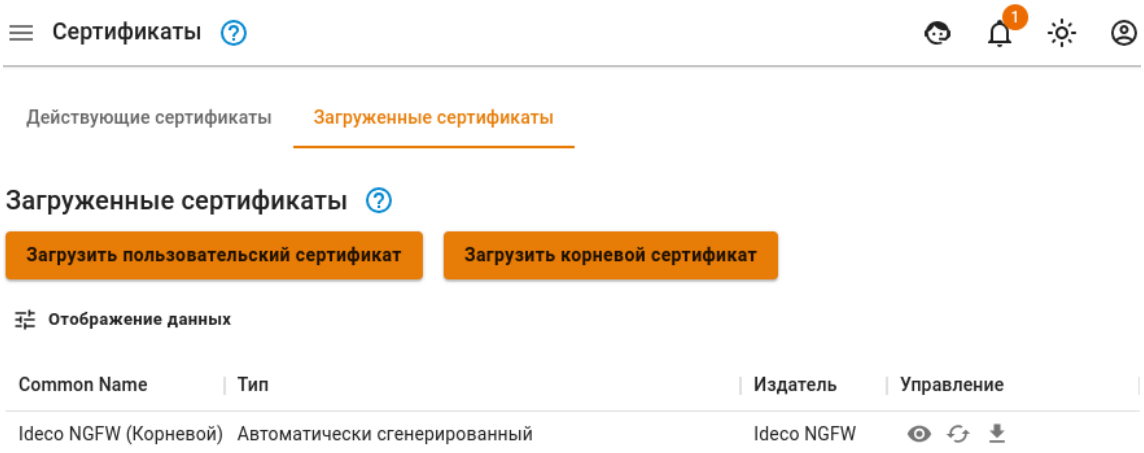
Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

Также установите корневой сертификат NGFW на устройство пользователя. Скачать сертификат можно одним из способов:

- В личном кабинете, введя логин/пароль пользователя:



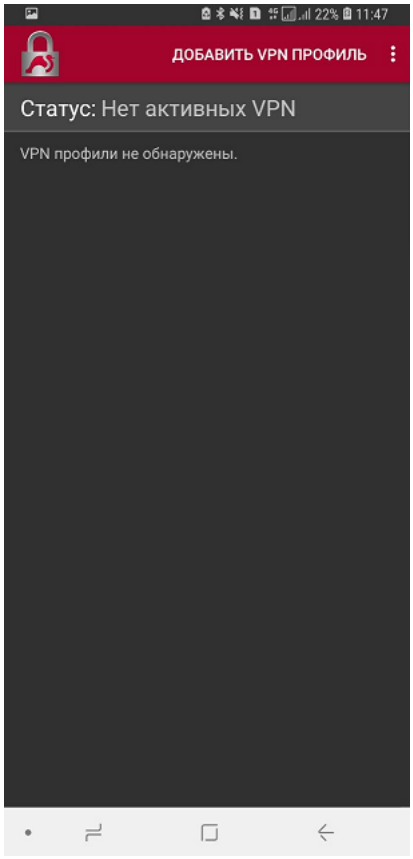
- В разделе **Сервисы -> Сертификаты**:



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

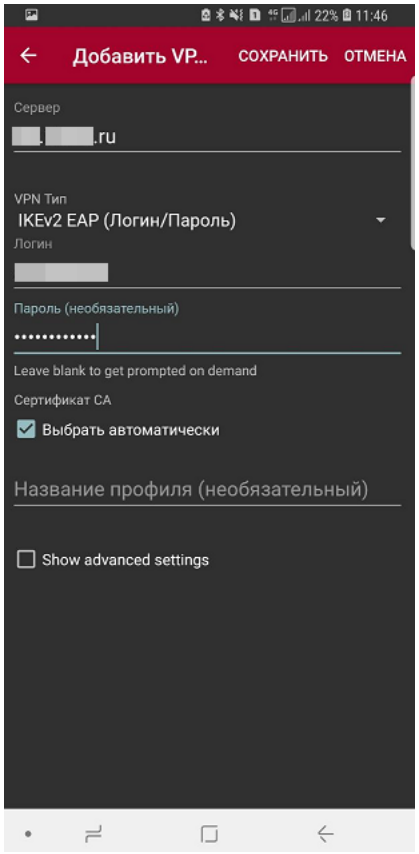
Подключение через приложение StrongSwan:

1. Нажмите **Добавить VPN профиль**:



2. Заполните поля:

- Сервер - домен, указанный в Ideco NGFW в разделе **Пользователи -> VPN-подключение -> 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:

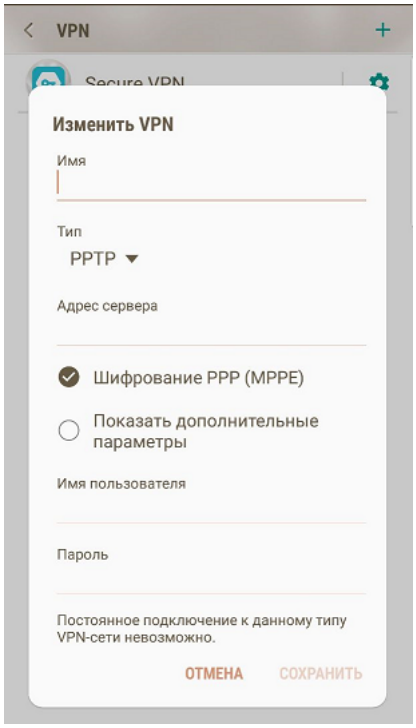
Подключение на Android:

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:

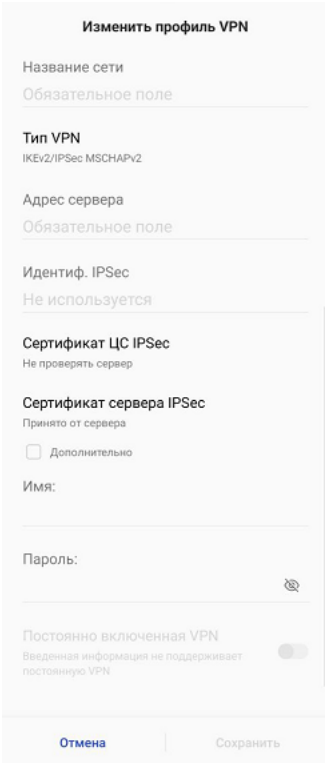
Для PPTP:

- Имя - имя подключения;
- Адрес сервера - адрес VPN-сервера;
- Имя пользователя - имя пользователя, которому разрешено подключение по VPN;
- Пароль - пароль пользователя.



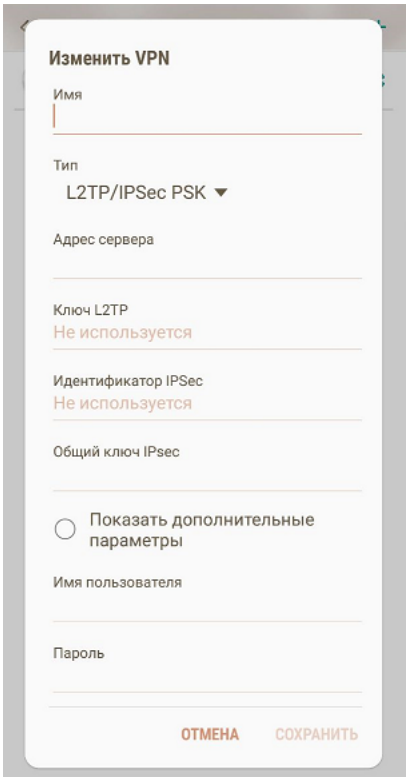
Для IKEv2/IPsec MSCHAPv2:

- 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:

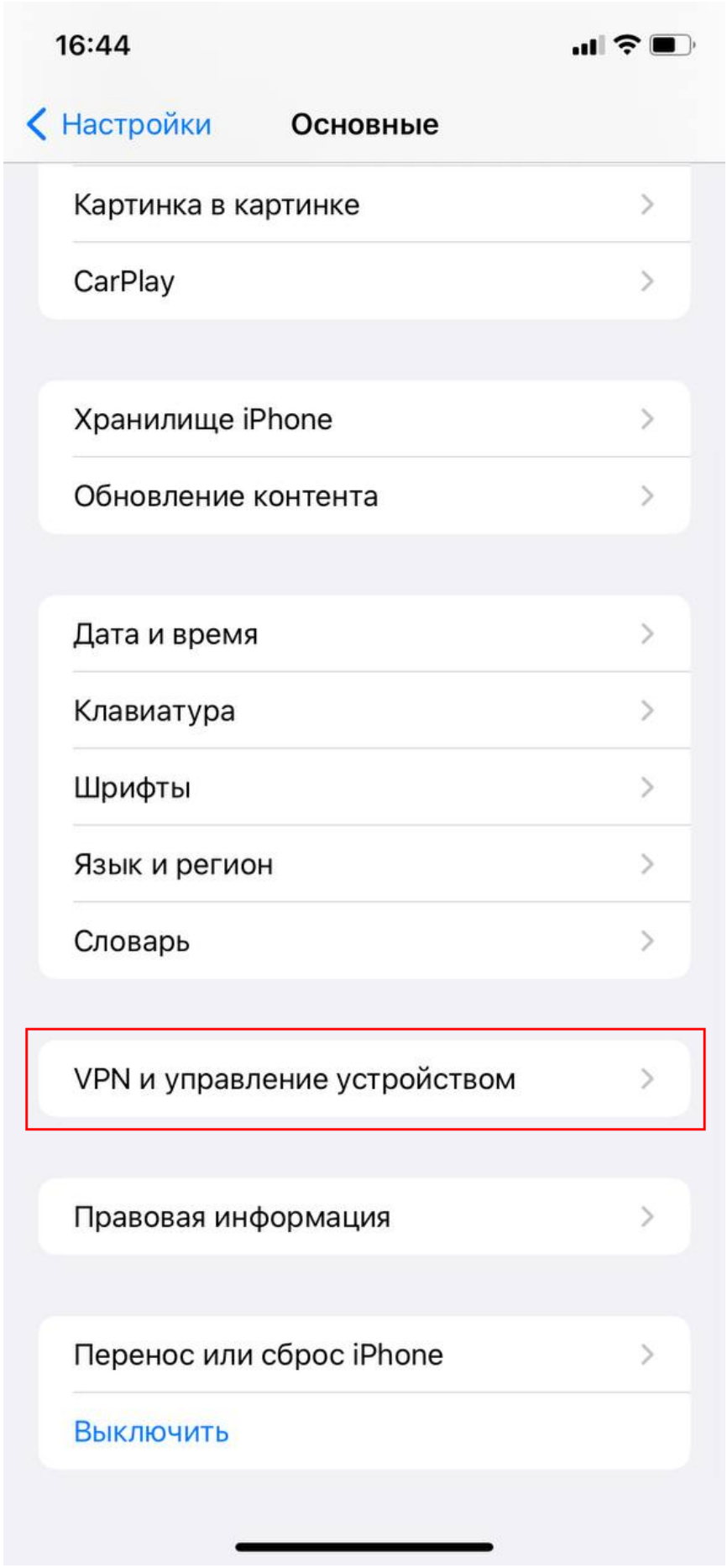
- Имя - имя подключения;
- Адрес сервера - адрес VPN-сервера;
- Общий ключ IPsec - значение строки **PSK** в разделе **Пользователи -> VPN-подключение -> Основное -> Подключение по L2TP/IPsec**.



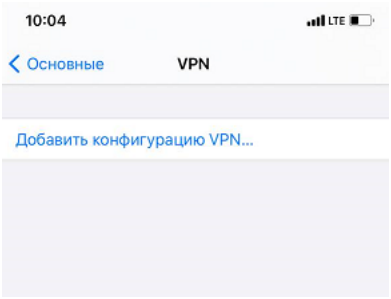
4. Нажмите **Сохранить** и активируйте подключение.

Подключение на iOS:

1. Перейдите в раздел **Настройки -> Основные -> VPN и управление устройством -> VPN**:


16:44
Настройки
Основные
Картинка в картинке
CarPlay
Хранилище iPhone
Обновление контента
Дата и время
Клавиатура
Шрифты
Язык и регион
Словарь
VPN и управление устройством
Правовая информация
Перенос или сброс iPhone
Выключить

2. Нажмите **Добавить конфигурацию VPN**:

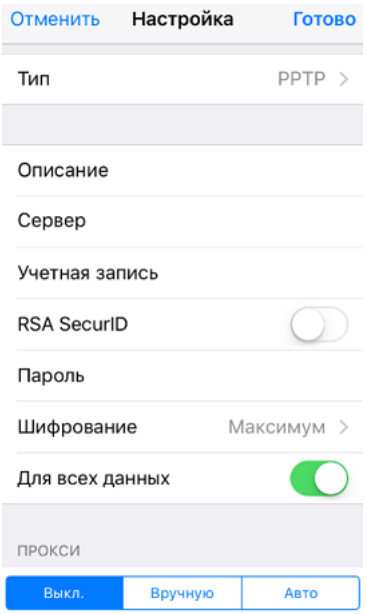


3. Выберите **Тип** подключения и заполните соответствующие поля:

Для PPTP:

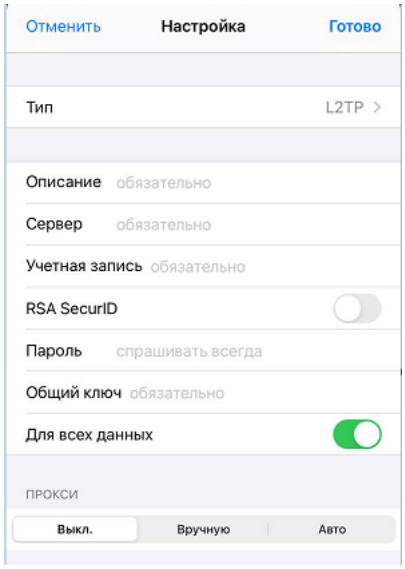
Начиная с версии iOS-10 компания Apple убрала поддержку протокола PPTP.

- Описание - название соединения;
- Сервер - адрес VPN-сервера;
- Учетная запись - имя пользователя, которому разрешено подключение по VPN;
- Пароль - пароль пользователя.



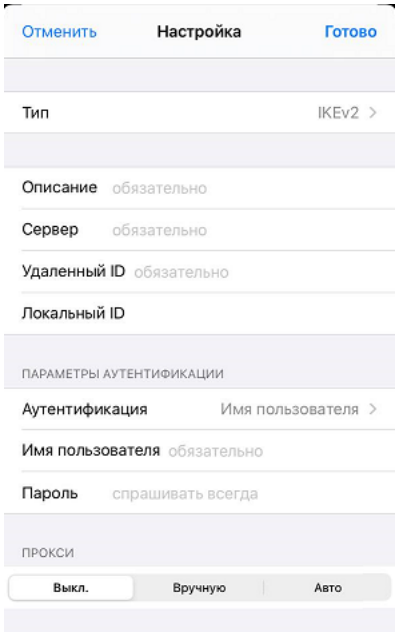
Для L2TP:

- 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-подключение -> Основное -> Подключение по L2TP/IPsec**.



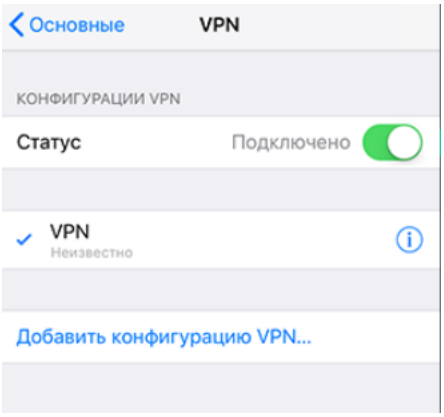
Для IKEv2:

- 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** в положение **включен**:



22.20.7 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.

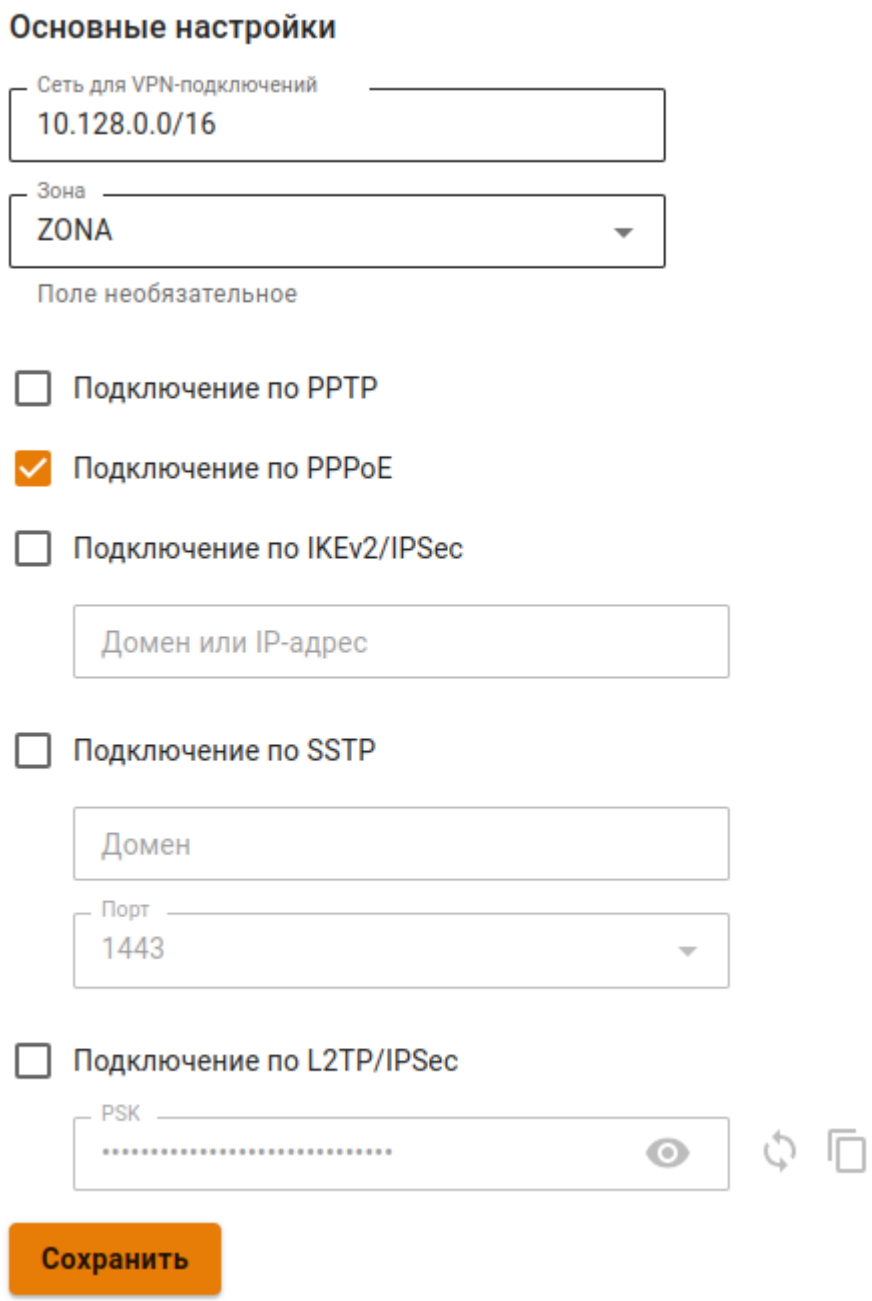
Подсказка: При проблемах с подключением на IOS требуется:

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 PPPoE:

Для настройки Ideco NGFW перейдите в раздел **Пользователи -> VPN-подключение -> Основное** и установите флаг **Подключение по PPPoE**:



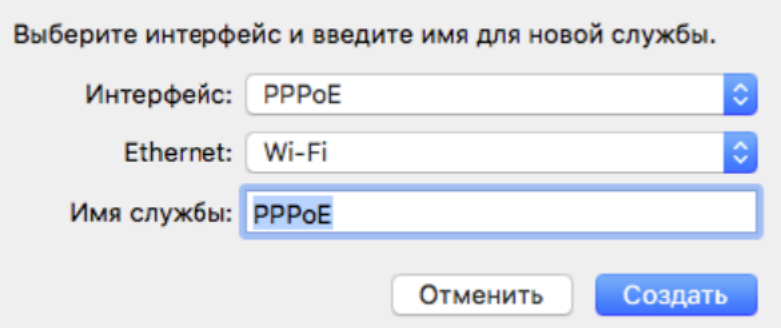
Создание подключения в MacOS

1. Перейдите в раздел **Системные настройки -> Сеть**;

2. Нажмите **Добавить** в левом нижнем углу (иконка +);

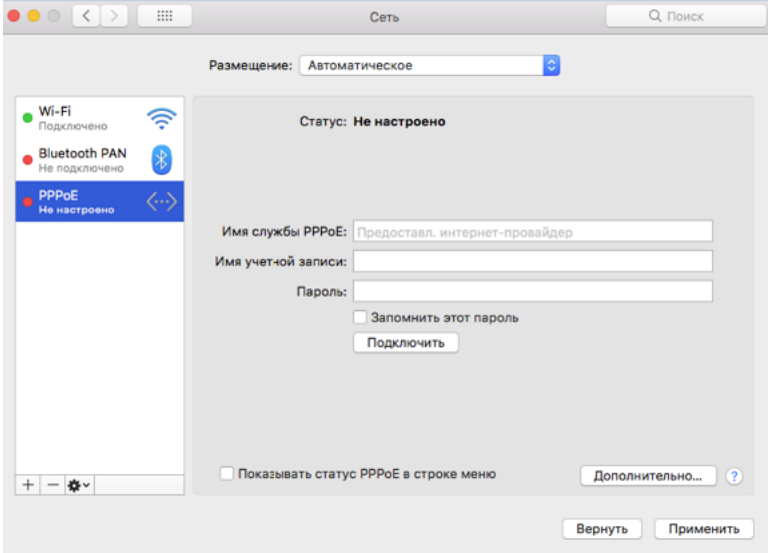
3. В появившемся окне заполните:

- **Интерфейс** - PPPoE;
- **Ethernet** - например, Wi-Fi;
- **Имя службы** - имя подключения.



4. Нажмите **Создать** и заполните:

- **Имя службы PPPoE** - имя службы;
- **Имя учетной записи** - логин;
- **Пароль** - пароль.



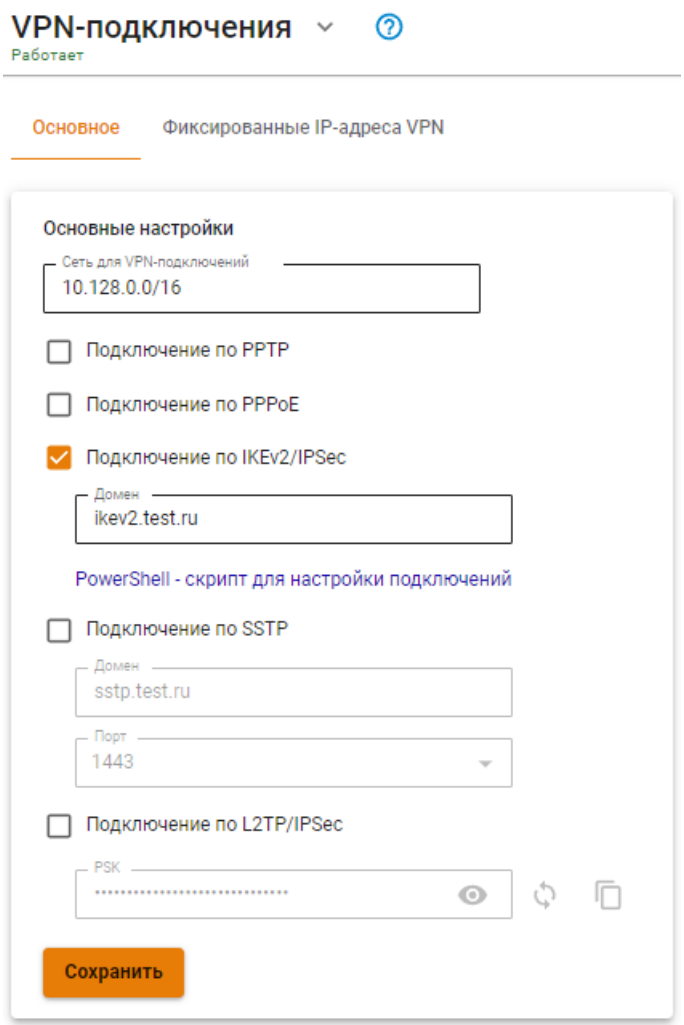
5. Нажмите **Подключить**.

Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключение -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поля **Домен**:



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.

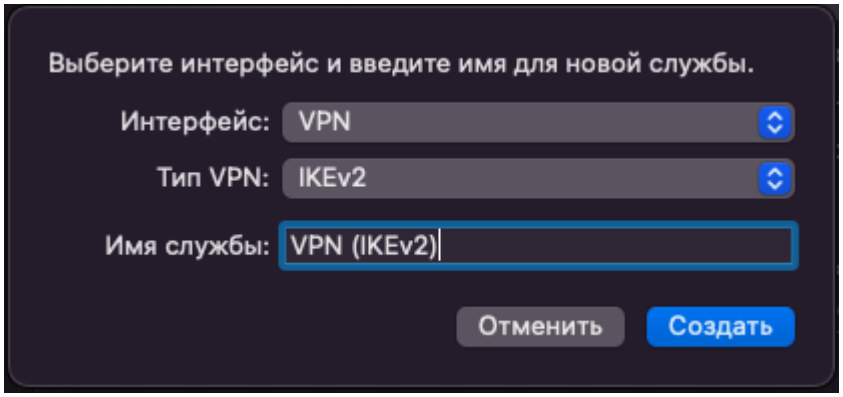
Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки -> Сеть**.

2. Нажмите **Добавить** в левом нижнем углу (иконка +).

3. Заполните поля:

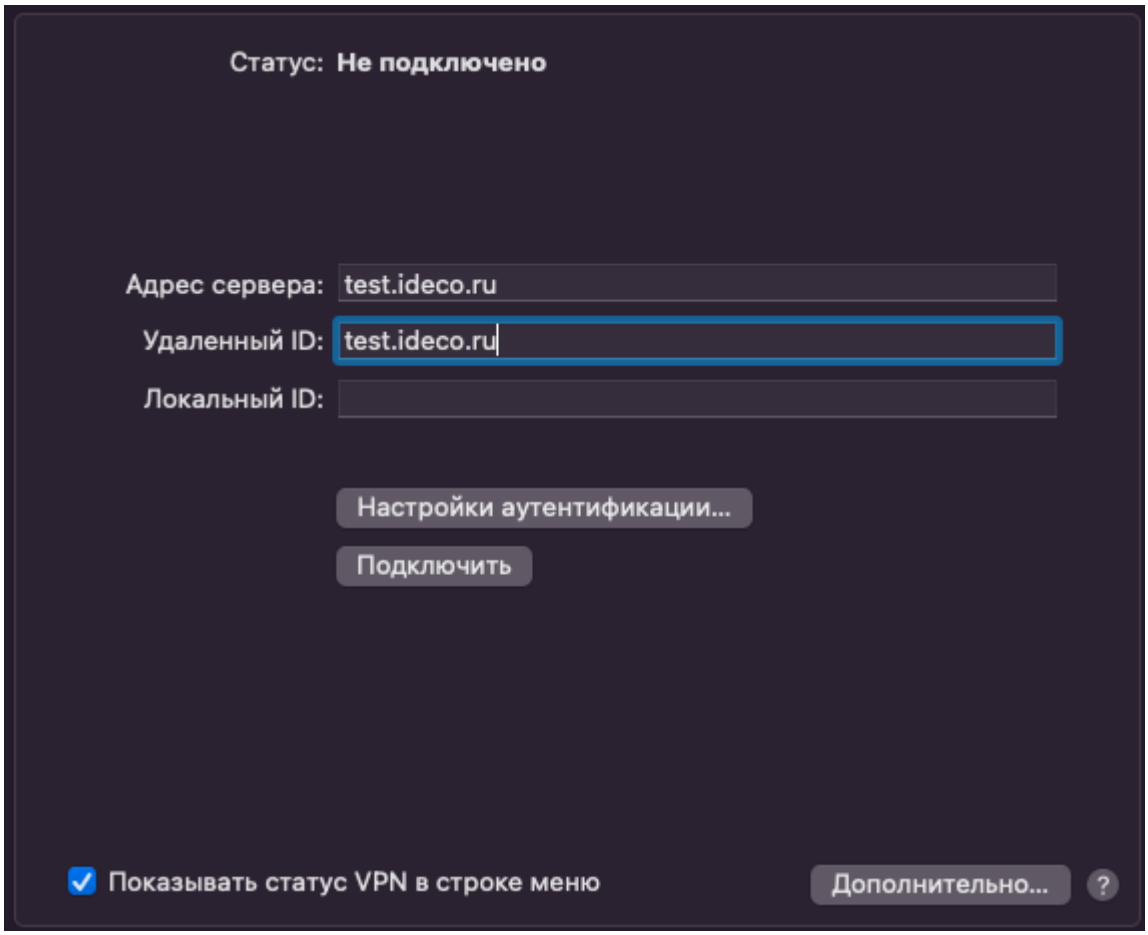
- **Интерфейс** - VPN;
- **Тип VPN** - IKEv2;
- **Имя службы** - имя подключения.



4. Нажмите **Создать**;

5. Установите параметры подключения:

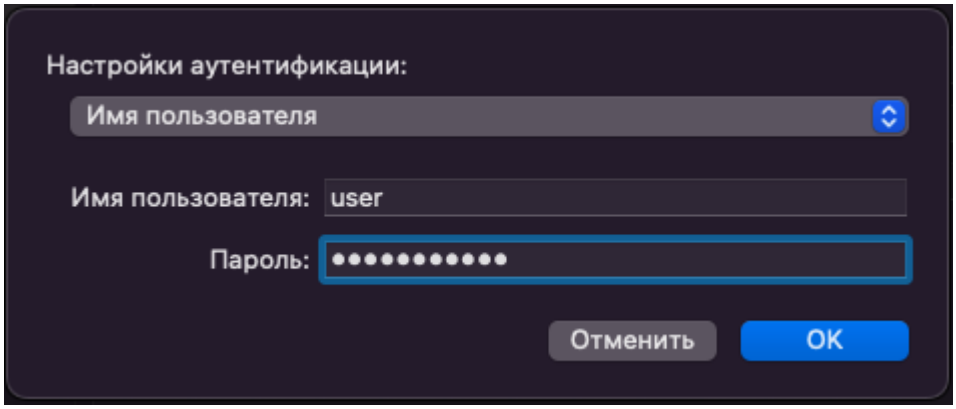
- **Адрес сервера** - адрес VPN-сервера;
- **Удаленный ID** - продублируйте адрес VPN-сервера.



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 **ОК**.

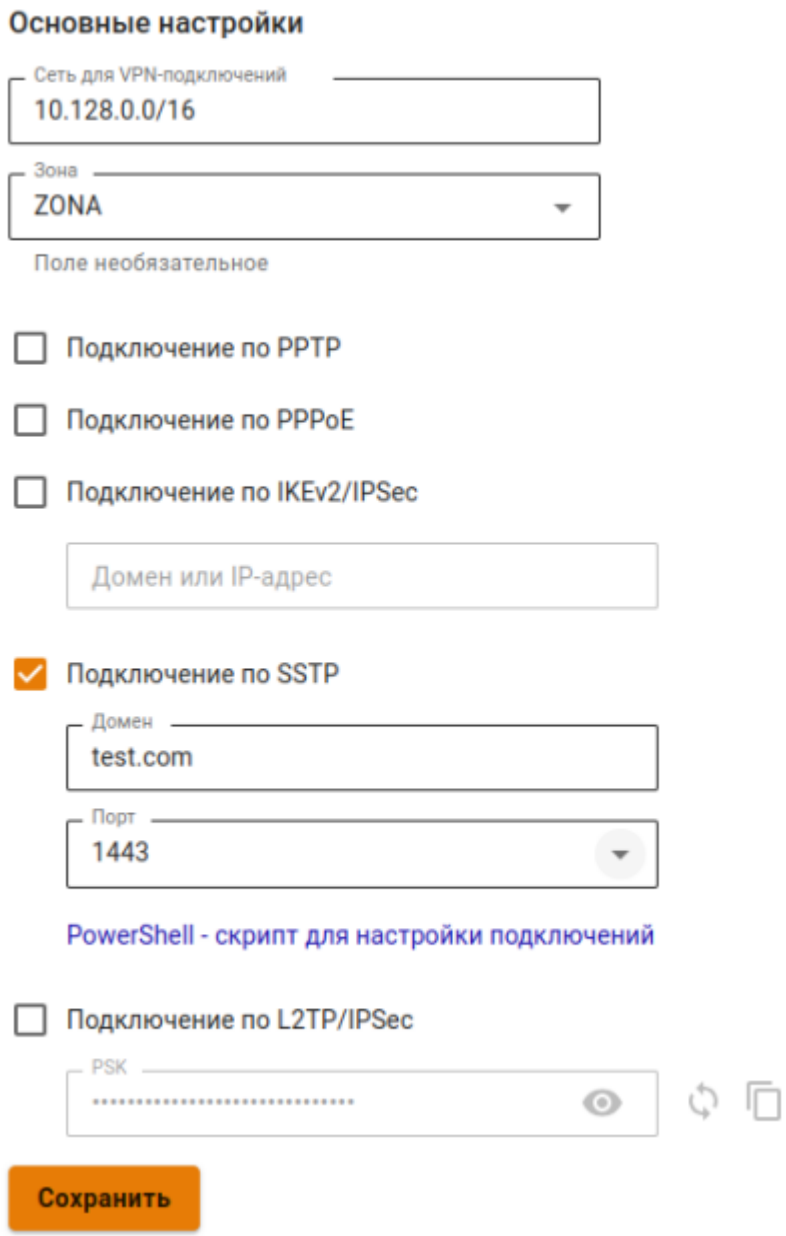
9. Поставьте флаг в пункте **Показывать статус VPN в строке меню**, нажмите **Применить** и включите соединение.

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 машрутизации вкручную, 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**.

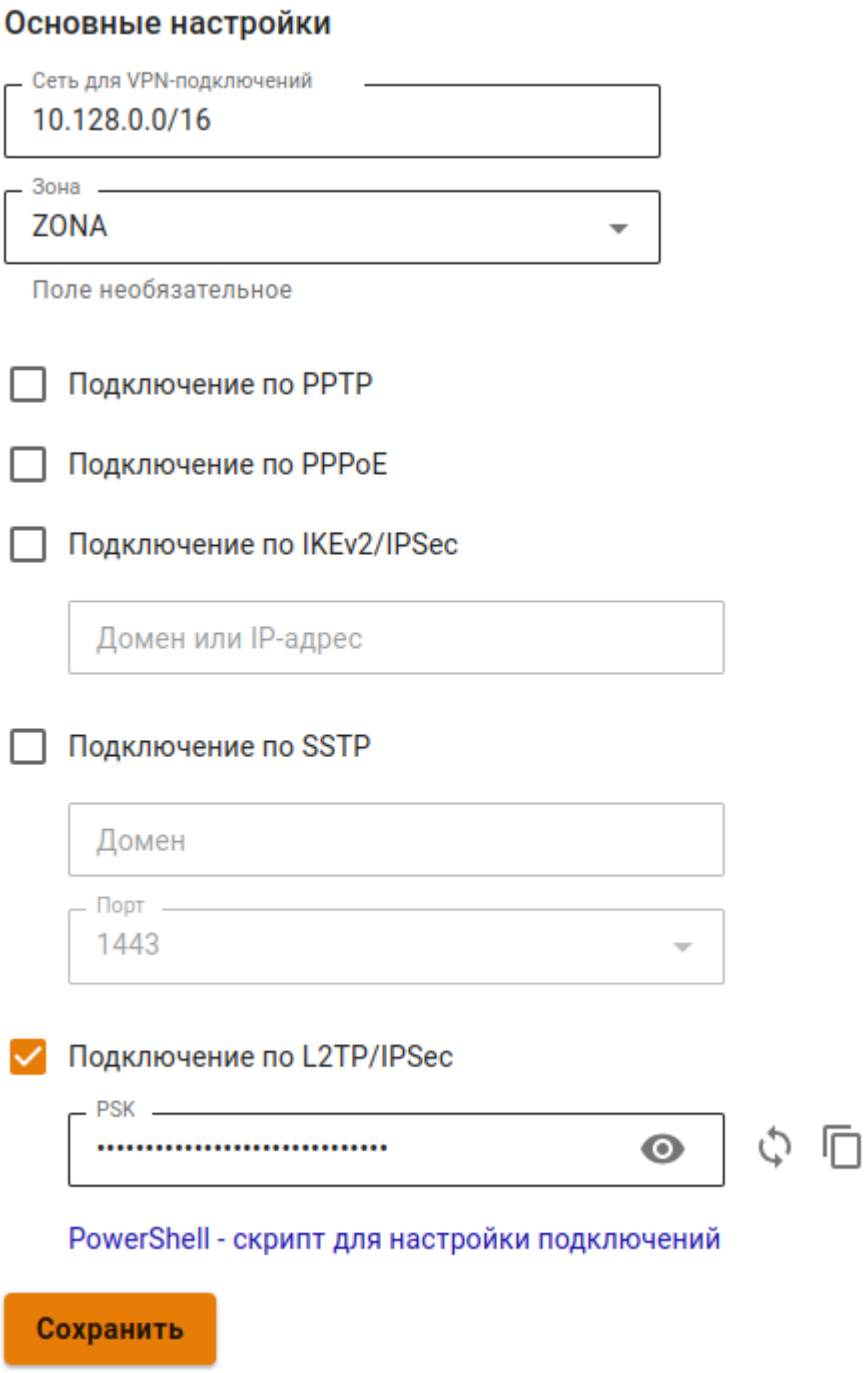
Протокол L2TP/IPsec:

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:

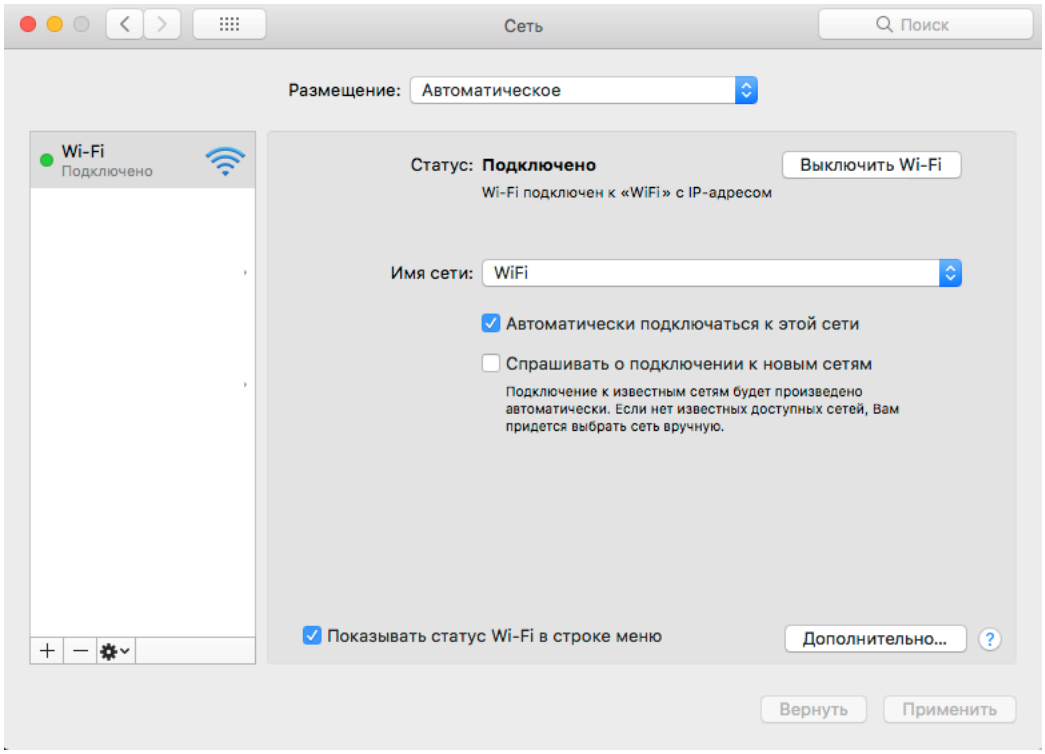
1. Перейдите в раздел **Пользователи -> VPN-подключение -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



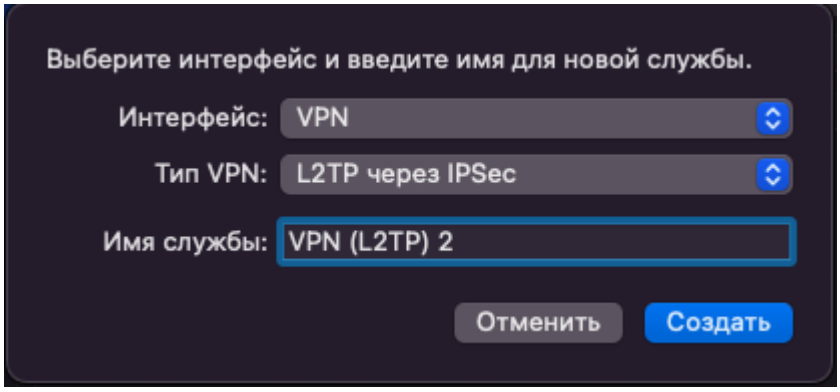
Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки -> Сеть** и нажмите **Добавить** в левом нижнем углу.



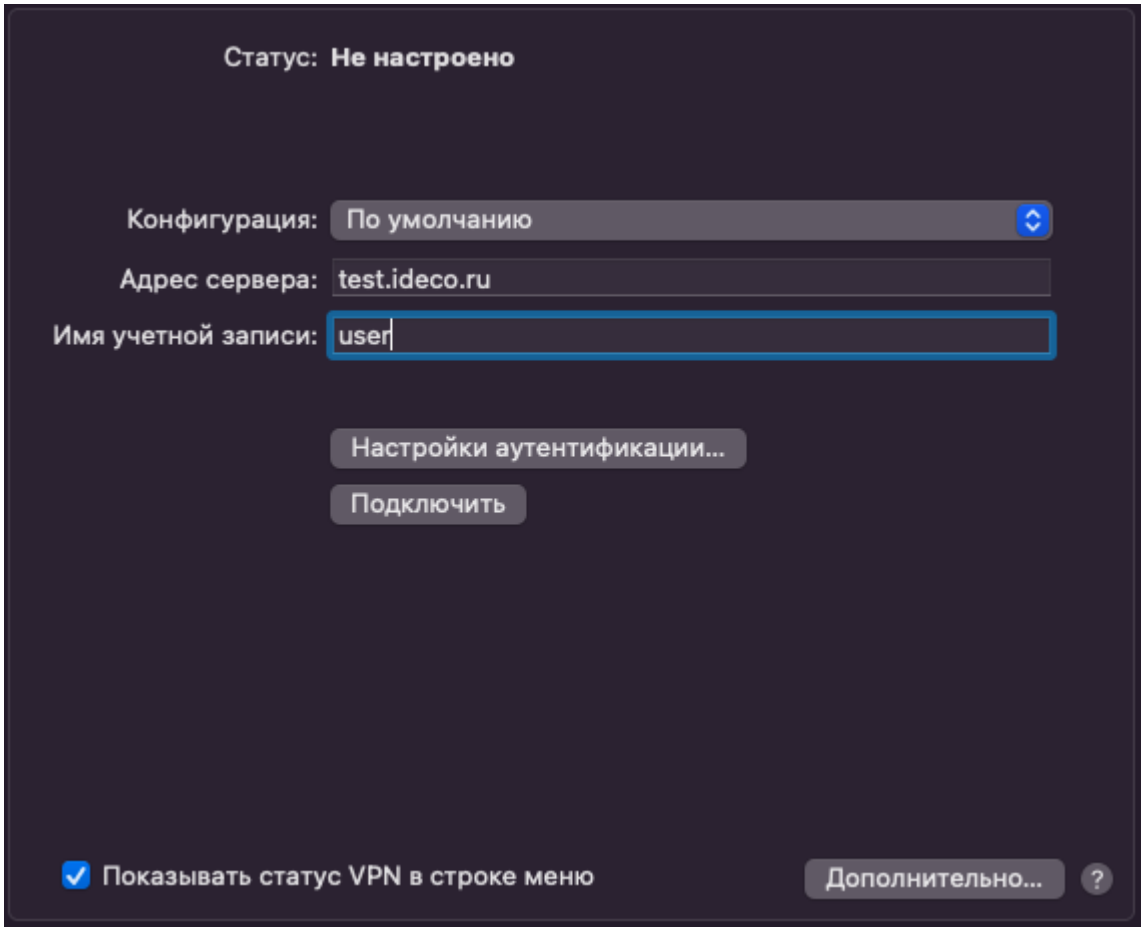
2. В появившемся окне заполните:

- **Интерфейс** - VPN;
- **Тип VPN** - L2TP через IPsec;
- **Имя службы** - имя подключения.



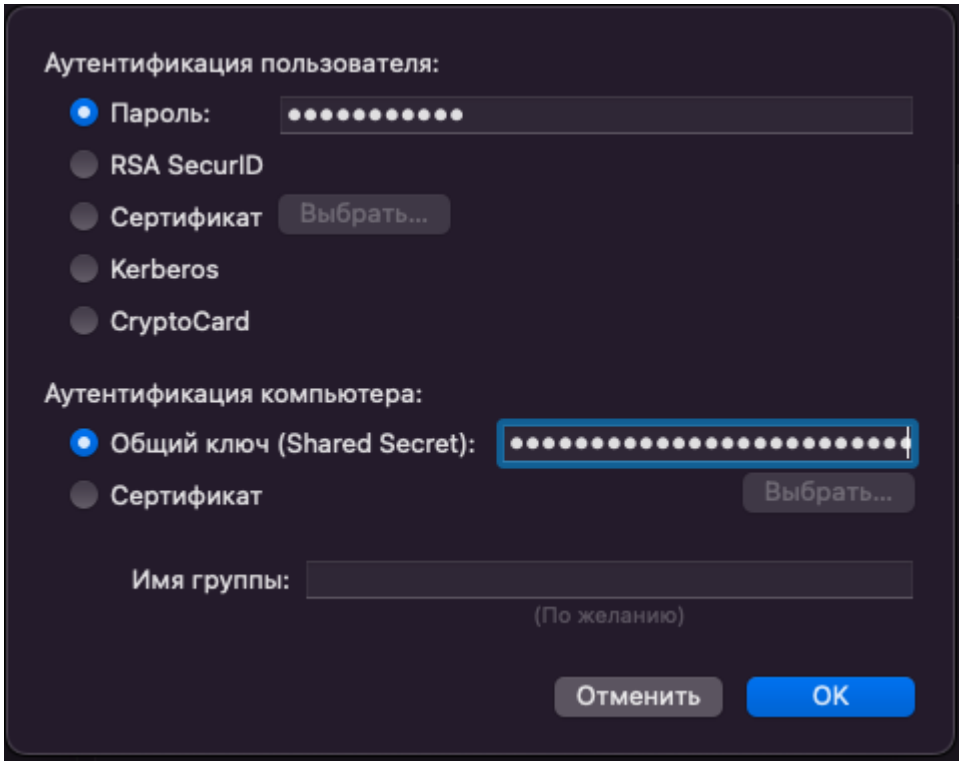
3. Нажмите **Создать**.

4. Заполните **Адрес сервера** и **Имя учетной записи**:



5. Поставьте флаг на пункте **Показывать статус VPN в строке меню** и выберите **Настройки аутентификации**.

6. В **Аутентификации пользователя** заполните **Пароль**, в **Аутентификации компьютера** - **Общий ключ (Shared Secret)**:



7. Нажмите **ОК -> Применить** и включите соединение.

22.20.8 Подключение по SSTP Wi-Fi роутеров Keenetic

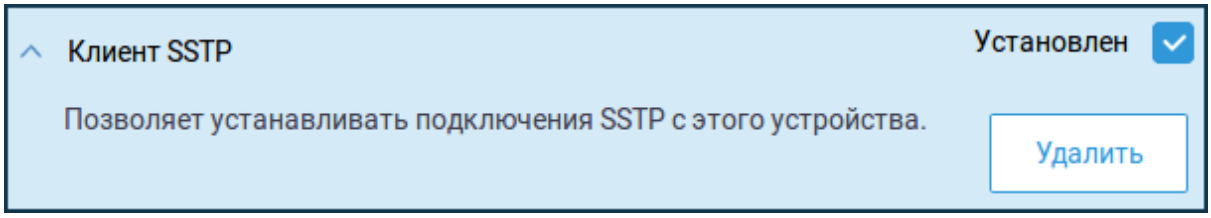
Основное

Поддерживаются все роутеры на базе KeeneticOS 3.x.x.

1. Выполните настройку пользователей в Ideco NGFW и включите SSTP в разделе **Пользователи -> VPN-подключение -> Основное**.

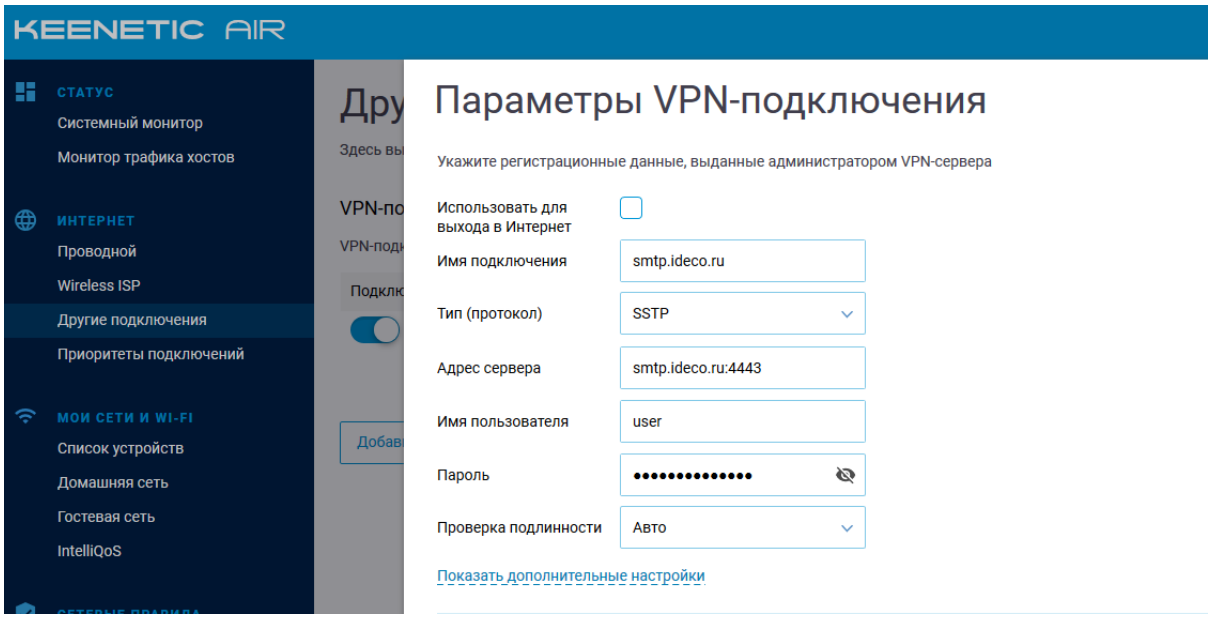
2. Зайдите в веб-интерфейс управления Keenetic: `http://my.keenetic.net`.

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.

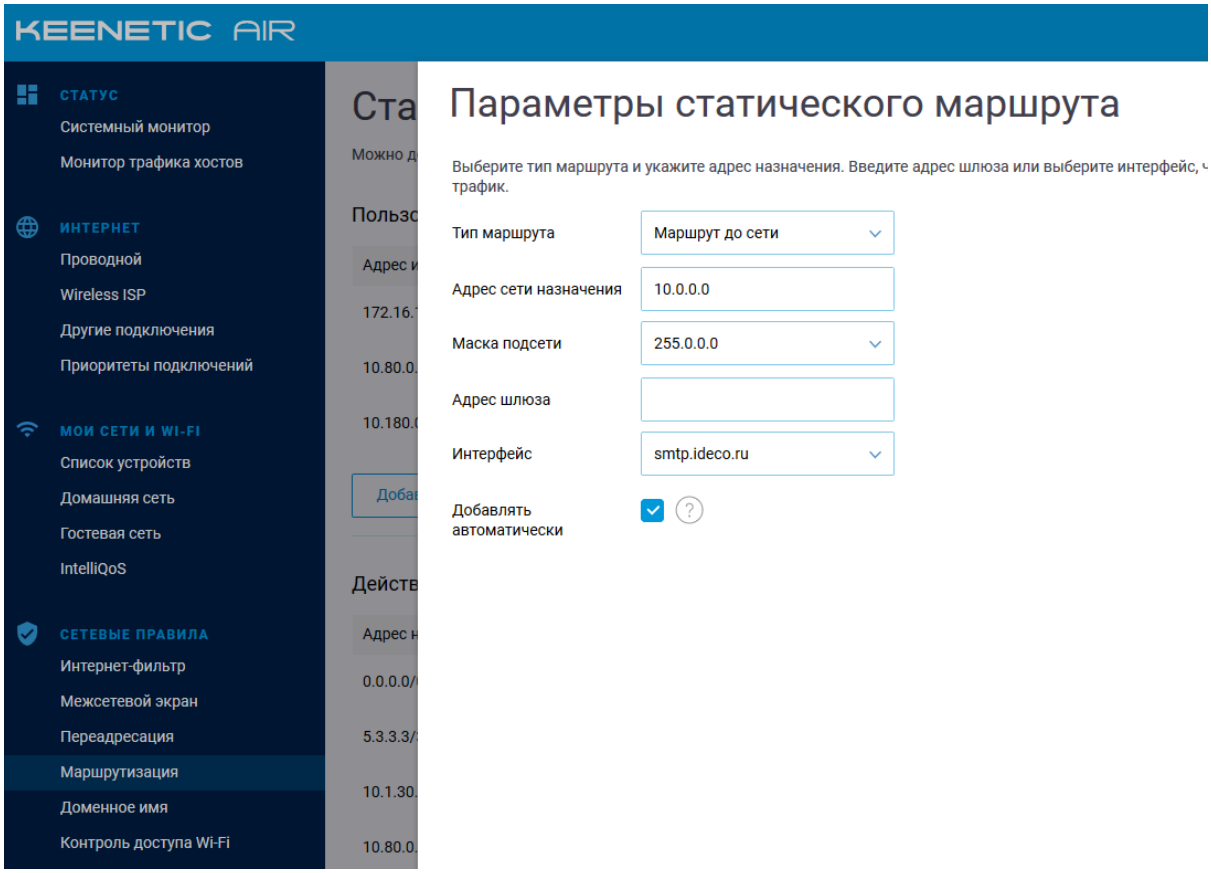
4. Создайте подключение в разделе **Интернет -> Другие подключения** нажмите кнопку **Добавить подключение**



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.

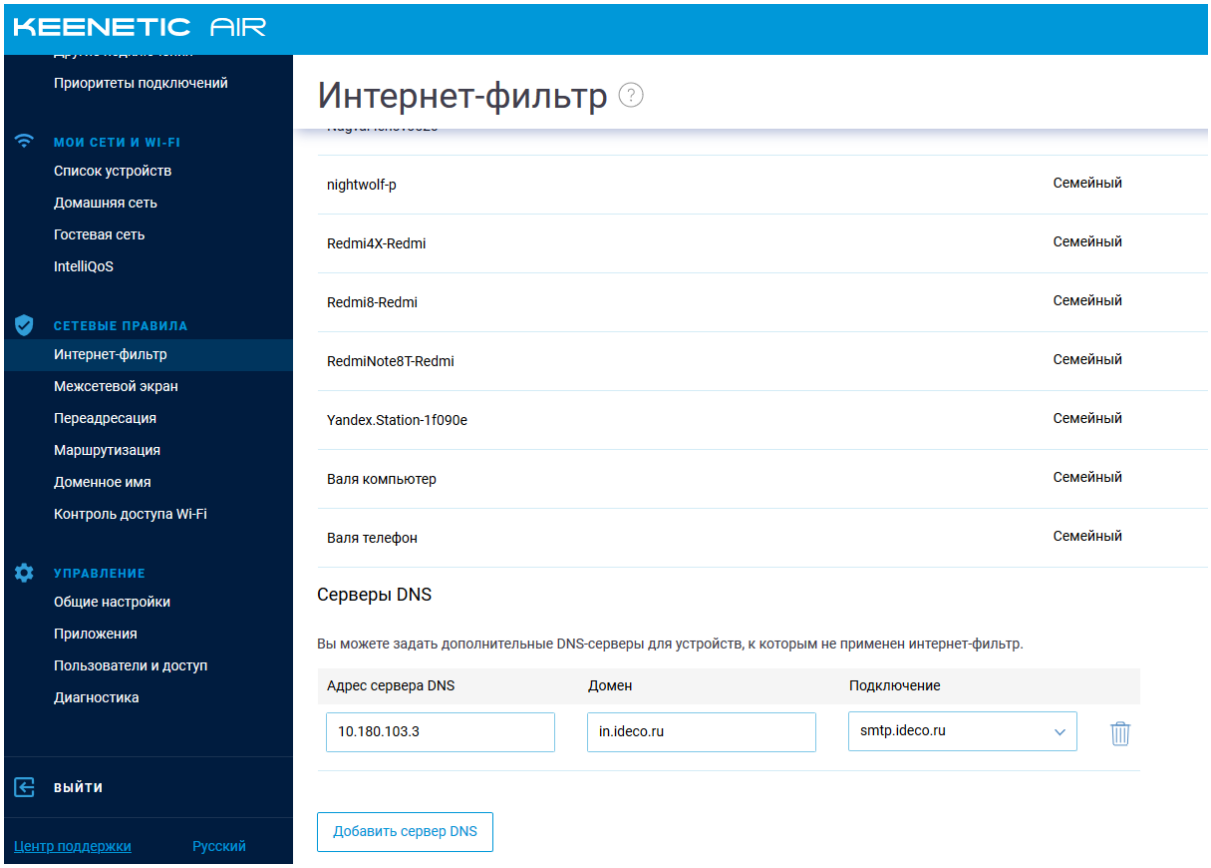
5. В разделе **Сетевые правила -> Маршруты** добавьте маршруты в рабочую сеть. Например, если сеть офиса `10.0.0.0/8`, добавьте следующий маршрут:



Выберите в качестве **Интерфейса** созданное VPN-подключение и установите флаг **Добавлять автоматически**, чтобы маршрут действовал только при активном VPN-подключении.

6. Настройте DNS для локального домена (например, Active Directory), чтобы обращаться к ресурсам (файловым и иным серверам) по DNS-именам.

В разделе **Сетевые правила -> Интернет-фильтр -> Серверы DNS** укажите DNS-сервер контроллера домена и имя домена.



Настройка закончена.

7. Используйте утилиту ping в командной строке для проверки связи и маршрутизации.

`nslookup` - для проверки резолвинга локальных имен рабочей сети.

Если VPN работает, но с некоторыми ресурсами (например, файловыми или RDP) нет связи, воспользуйтесь инструкцией для диагностики проблем.

22.21 Подключение к сертифицированным Ideco EX и настройка Ideco NGFW

22.21.1 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.

22.21.2 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.

22.22 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.

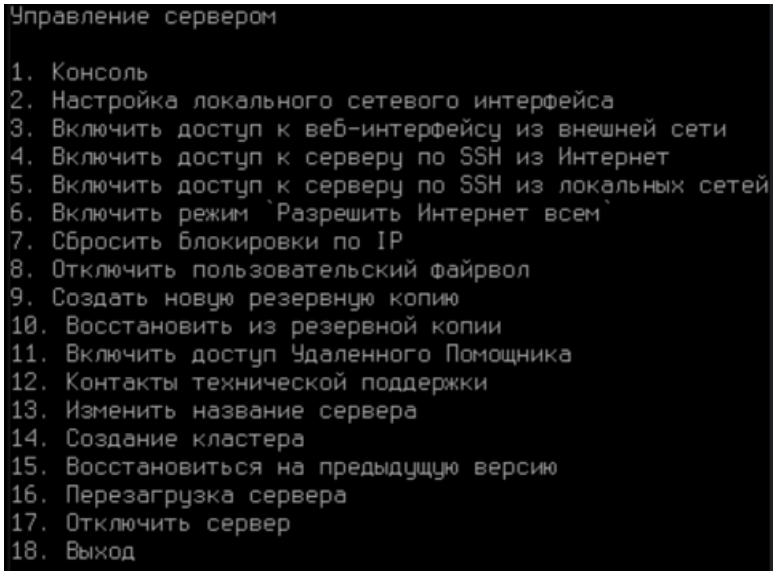
22.22.1 Включение режима удаленного помощника из веб-интерфейса

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.**

22.22.2 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 **11**, затем нажмите **Enter**.
Сгенерируется пароль, который необходимо сообщить технической поддержке для подключения по SSH.



22.22.3 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://putty.org.ru/;
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.**

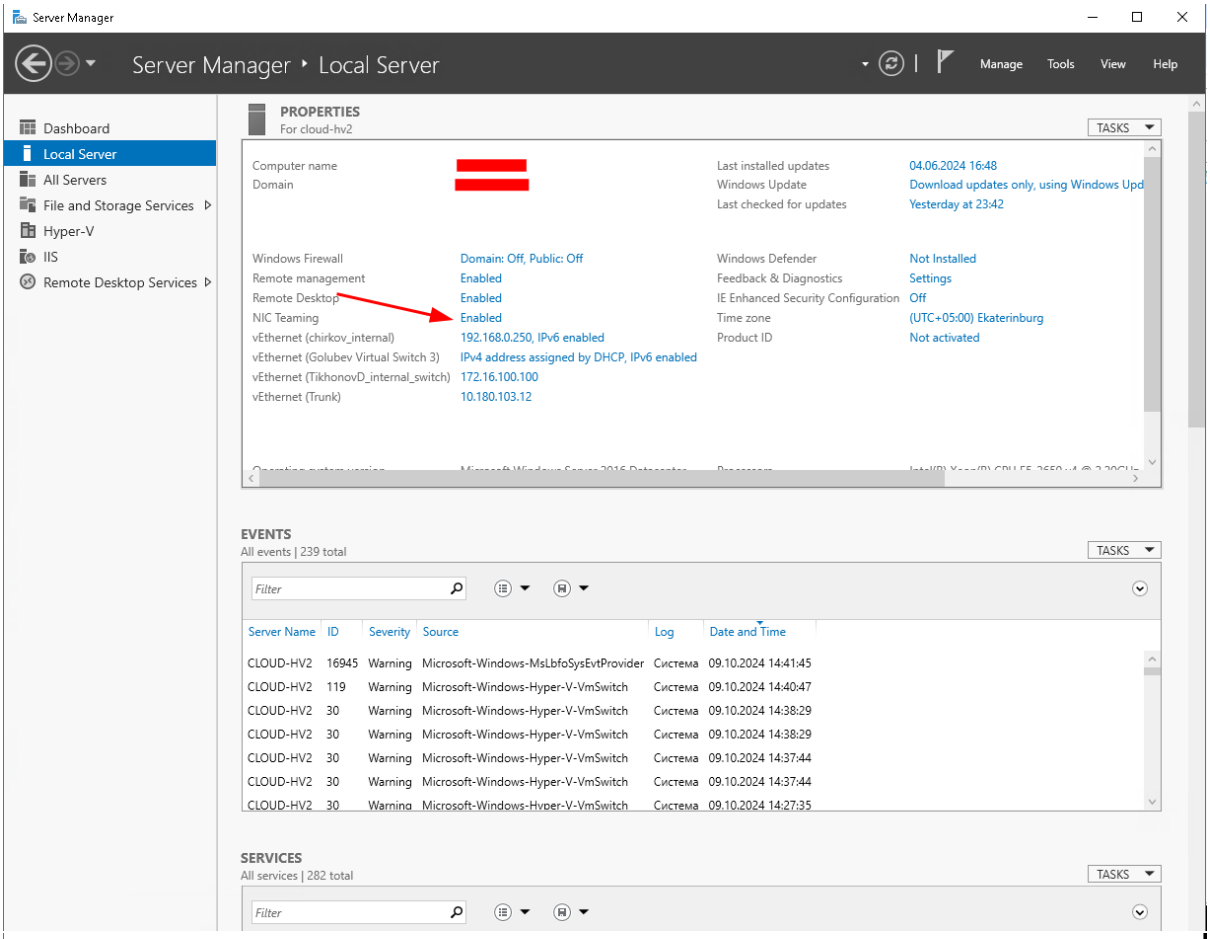
Символ «#» свидетельствует, что работа ведется от имени суперпользователя.

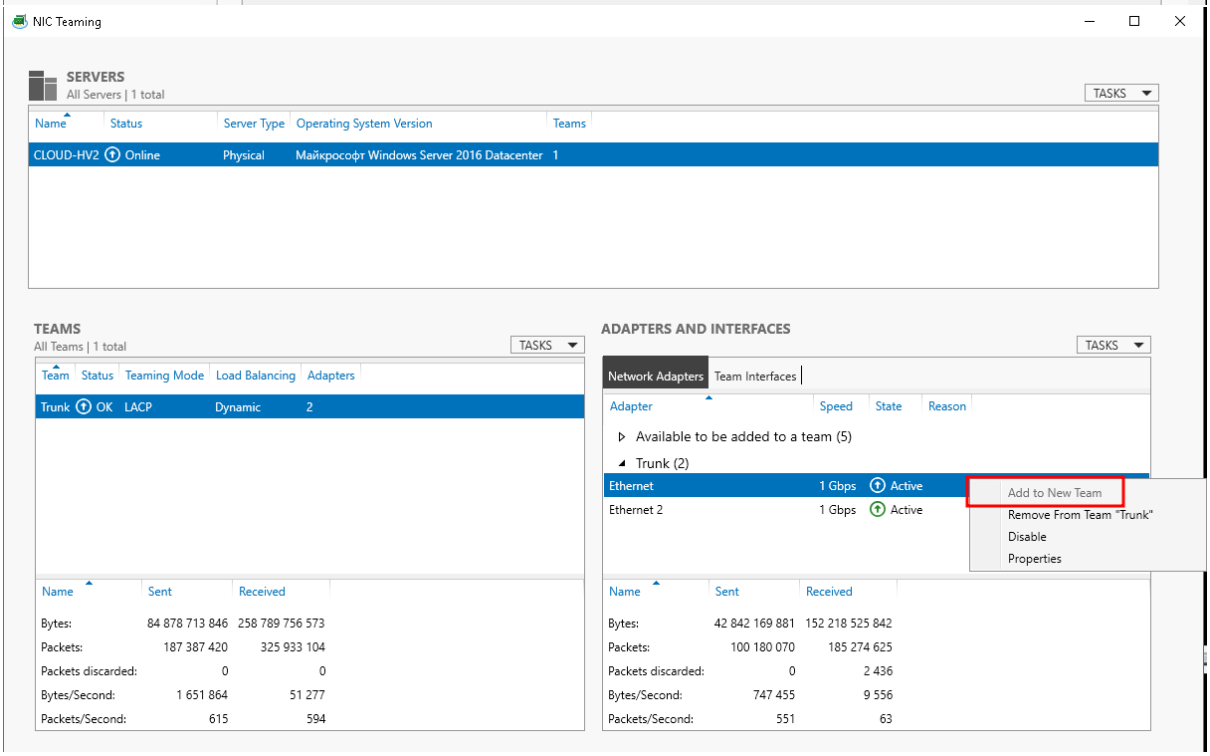
22.23 Настройка LACP на Hyper-V

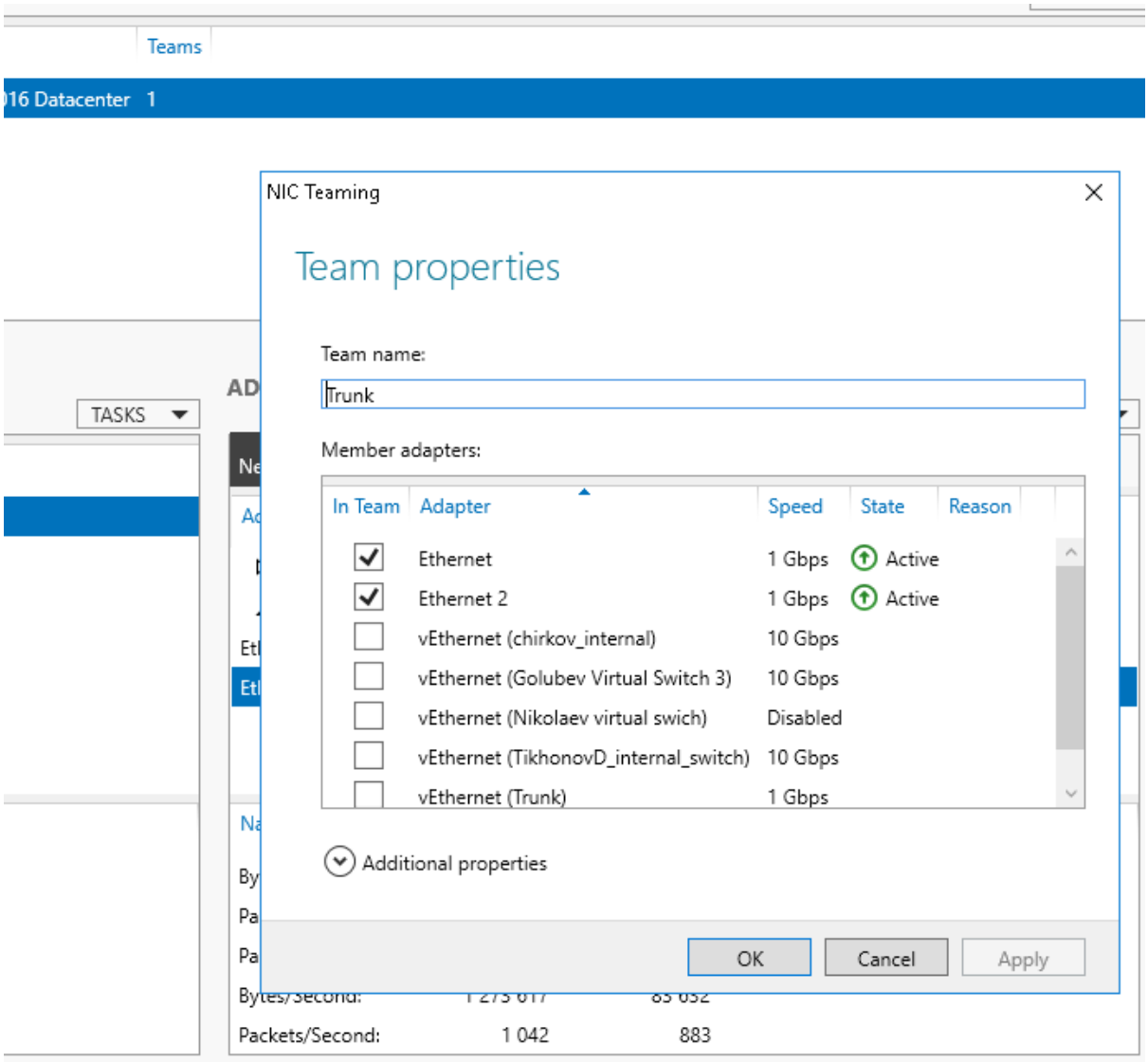
Для настройки LACP на гипервизоре Hyper-V существуют два способа:

22.23.1 Настройка на хост системе

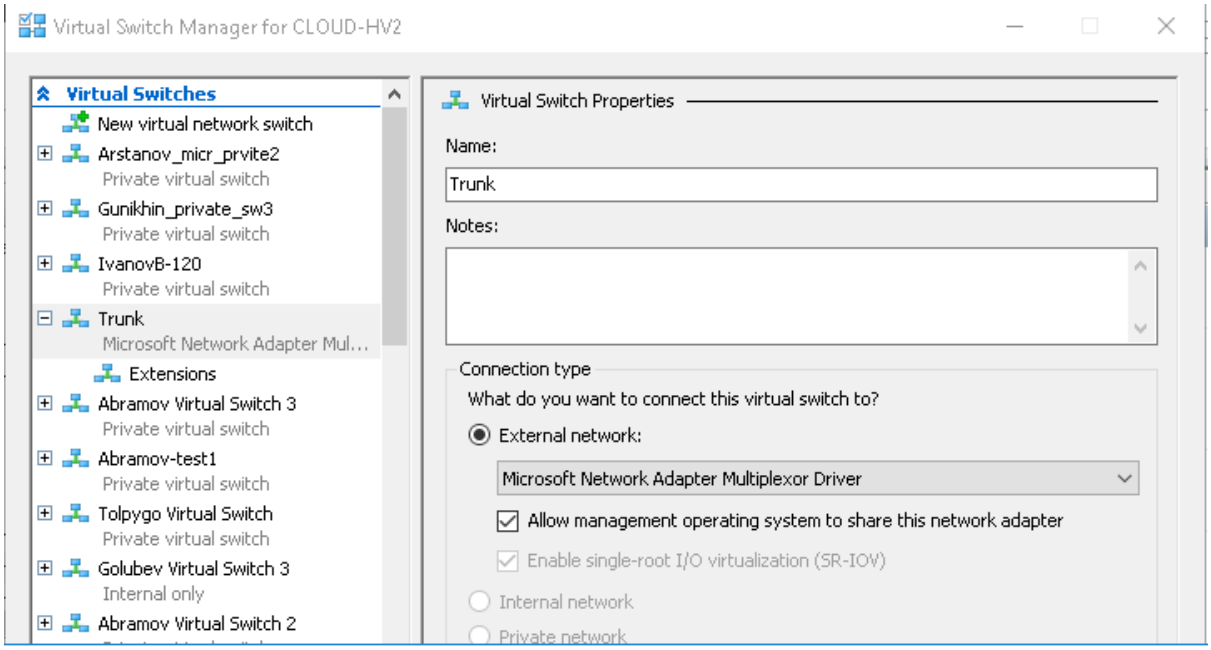
1. Объедините физические интерфейсы:

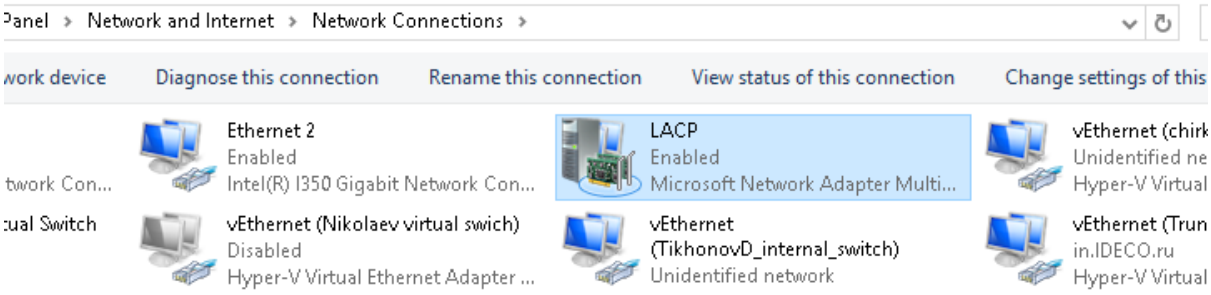






2. Выберите созданный интерфейс при настройке виртуального свитча:



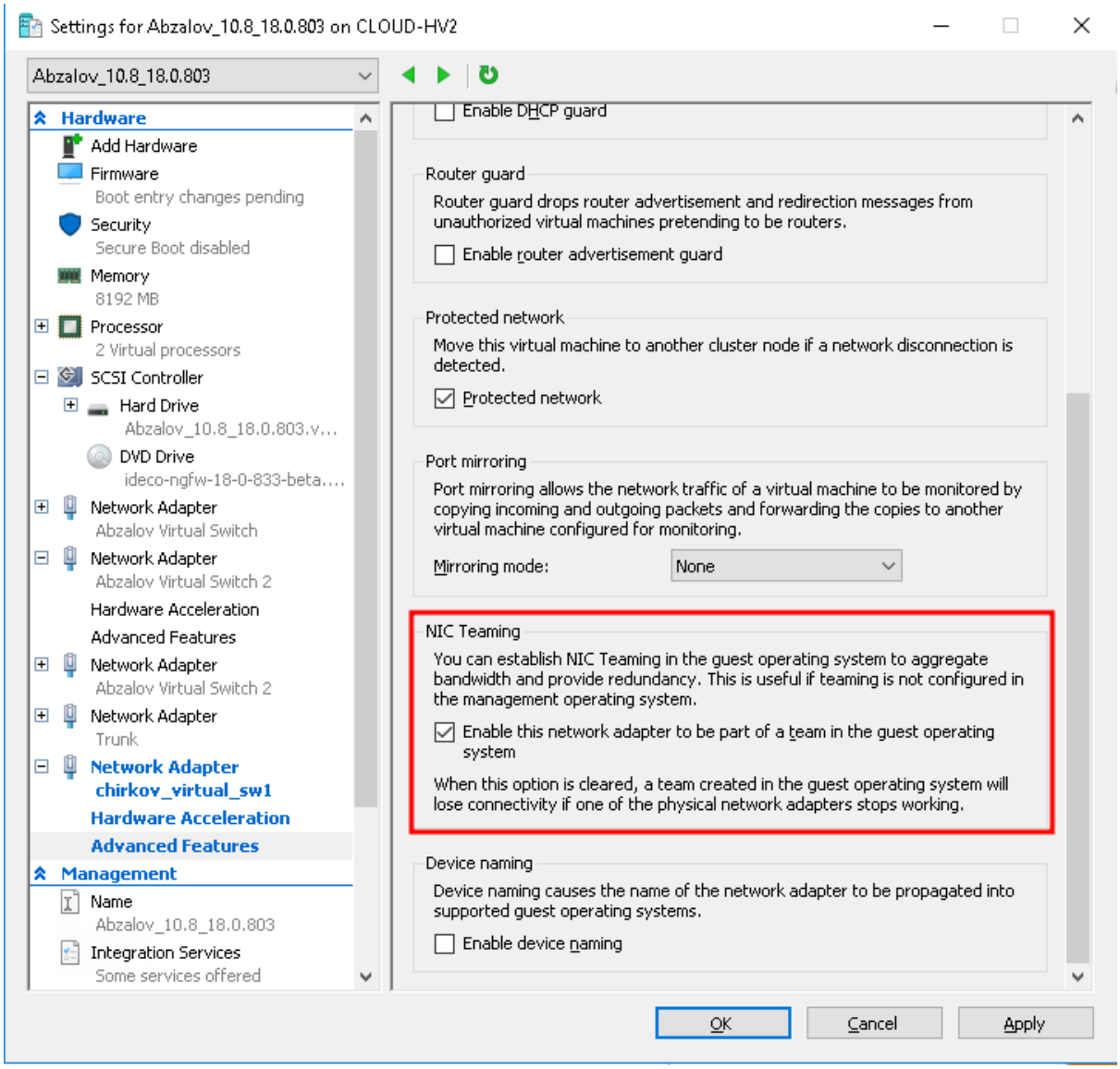


Получившийся виртуальный свитч можно использовать для добавления новых интерфейсов в LACP на гостевую систему.

3. Настройте подключение на вкладке **Сетевые интерфейсы -> Внешние и локальные** для вновь созданного LACP-интерфейса, как для обычного сетевого интерфейса NGFW.

22.23.2 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**.

22.24 Разрешить интернет всем: диагностика неполадок

22.24.1 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 данный 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.

22.25 Удаленный доступ к серверу

22.25.1 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.ru/. 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 ~]#
```

22.25.2 Доступ к веб-интерфейсу сервера из сети интернет

Доступ из внешней сети:

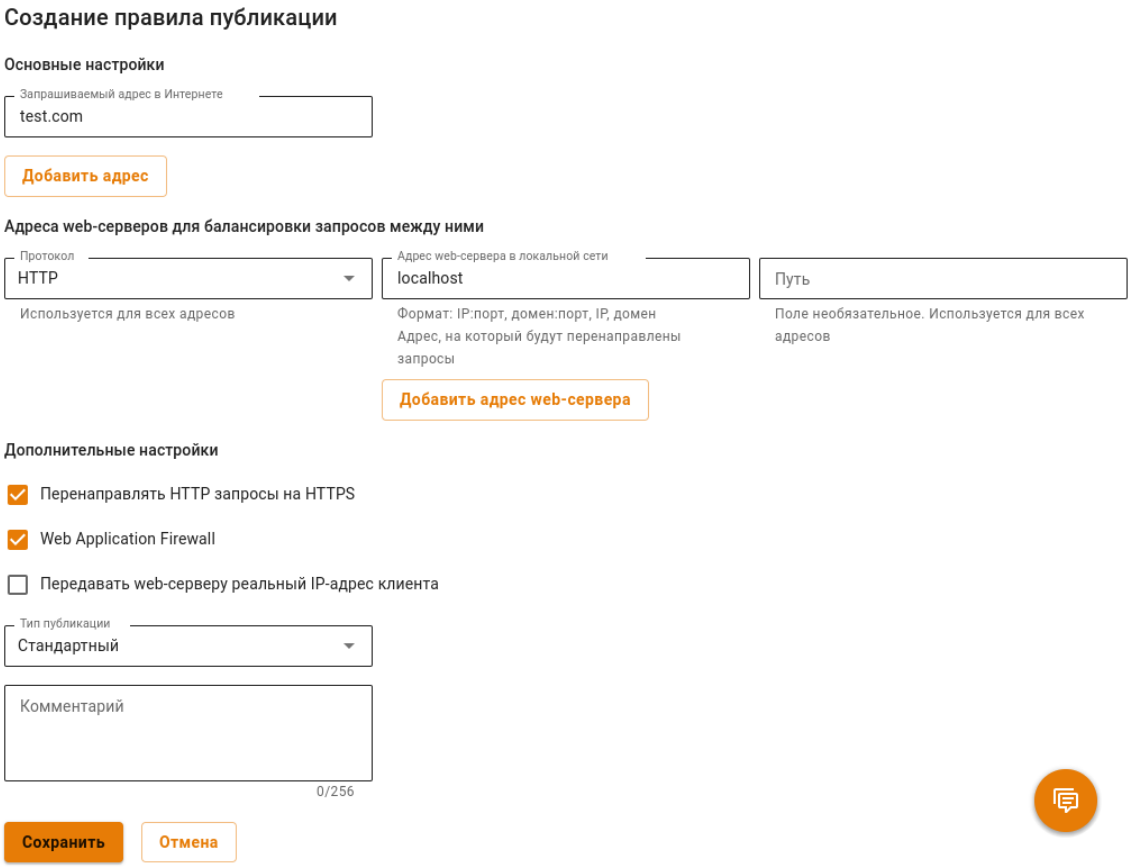
- Включите функцию **Доступ к веб-интерфейсу из внешней сети** в разделе **Управление сервером -> Администраторы**. Для доступа введите внешний IP-адрес Ideco NGFW и порт 8443.

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 следующим образом:



3. Укажите в качестве запрашиваемого адреса IP-адрес или доменное имя внешнего интерфейса Ideco NGFW.
4. Нажмите на кнопку **Сохранить** и зайдите по одному из адресов, которые были указаны в поле **Запрашиваемый адрес в интернете**.

22.26 Тестирование оперативной памяти сервера

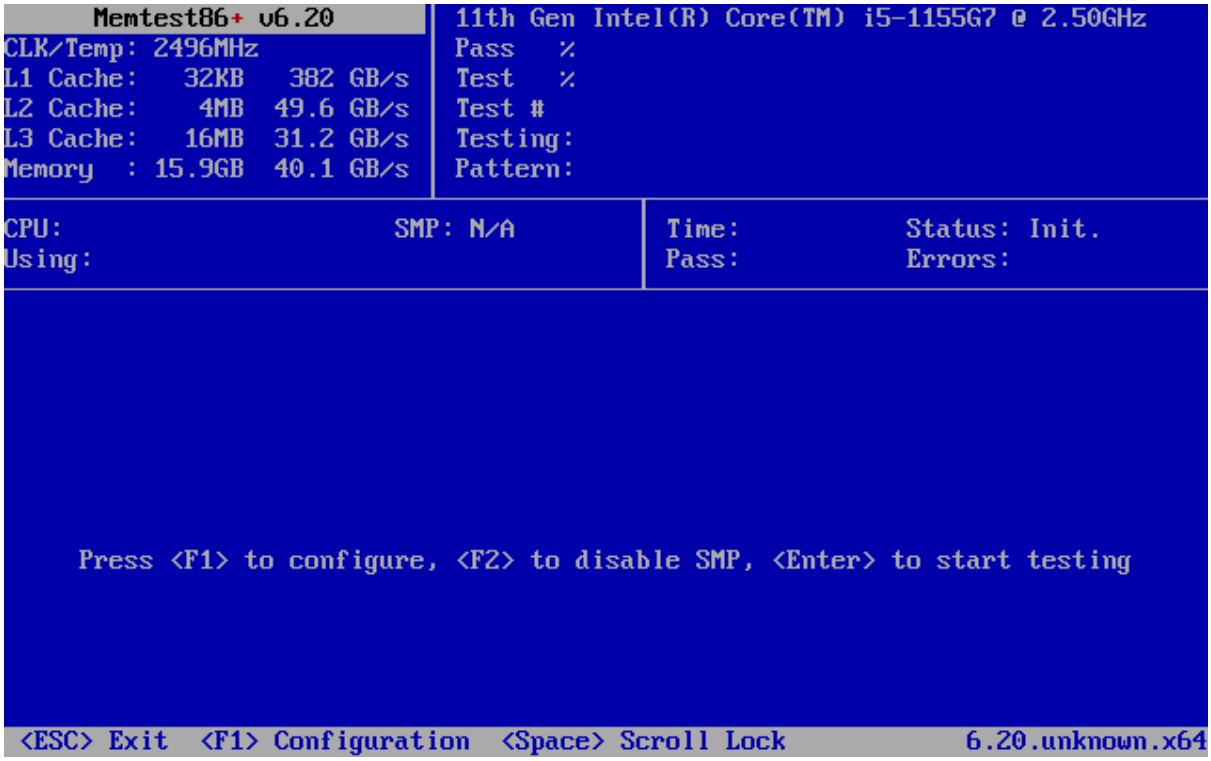
22.26.1 Основное

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:

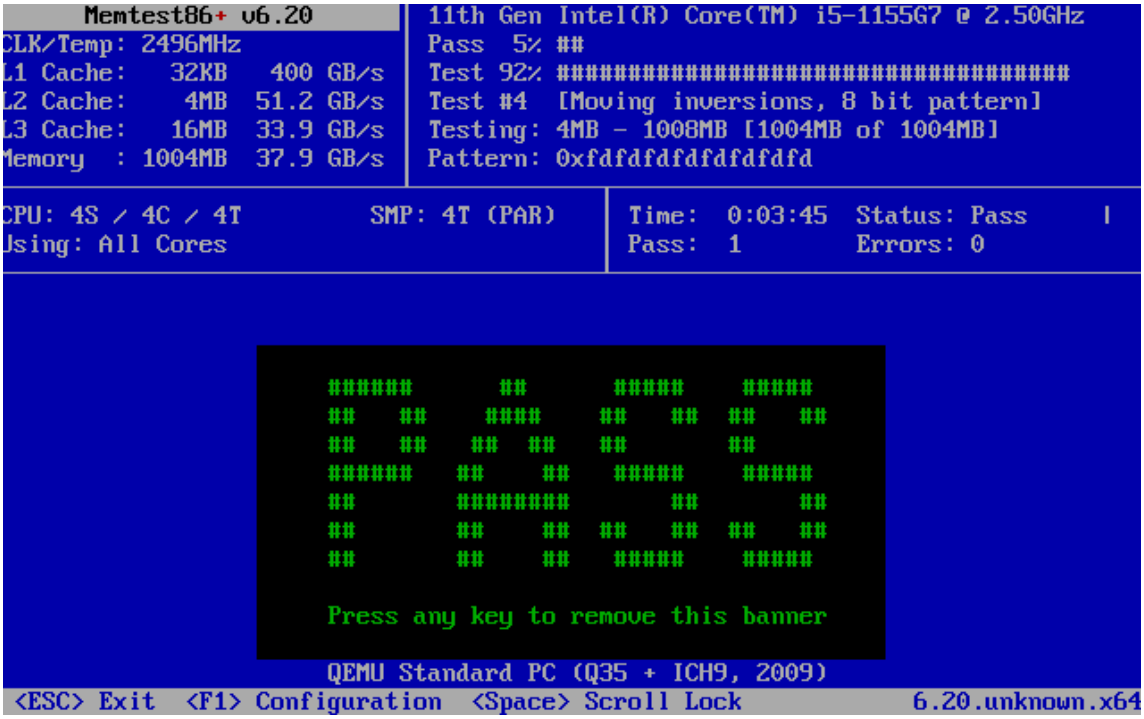
1. При загрузке сервера выберите **Memory test**:

2. Для начала тестов нажмите **Enter** или подождите 5 секунд до автоматического запуска тестирования:

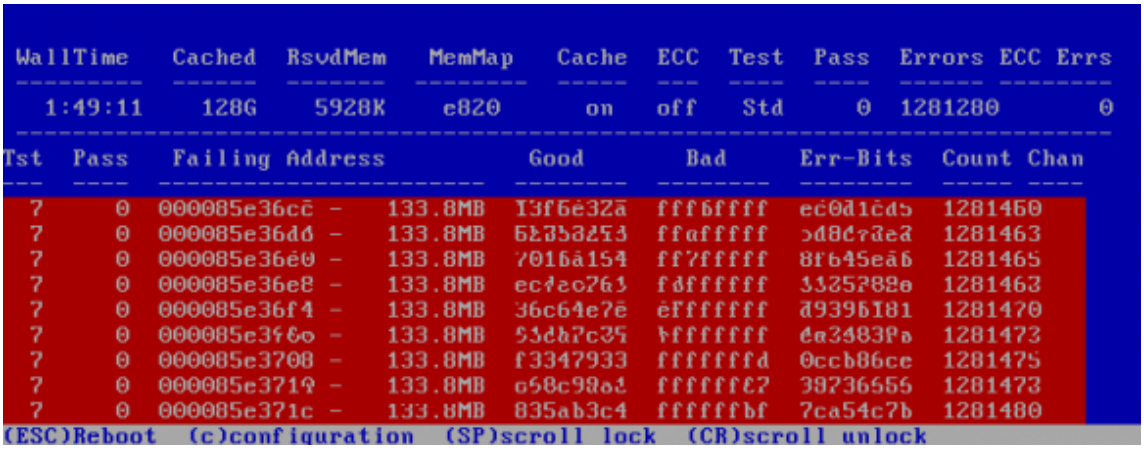


Подсказка: Для выбора режима диагностики **Fail-Safe Mode** нажмите **F1**.
Для выбора режима диагностики **Multi-Threading(SMP)** нажмите **F2**.

- Если появится запись **PASS**, тесты памяти пройдены успешно:



- При ошибке памяти появится запись вида:



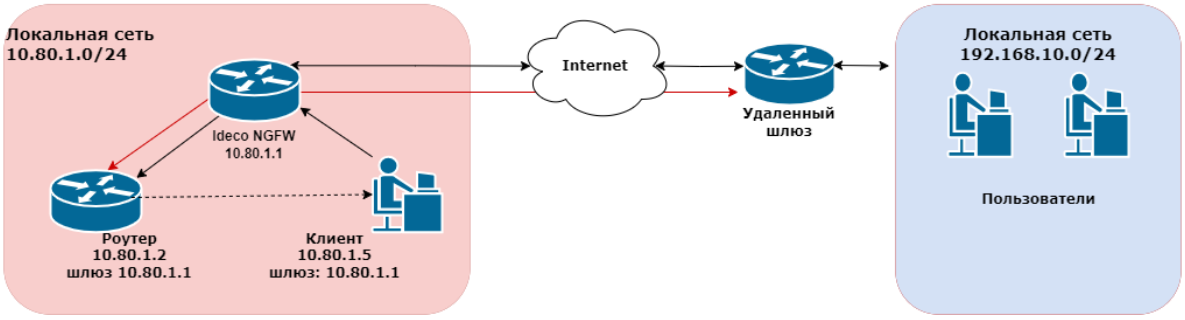
22.27 Как избавиться от асимметричной маршрутизации трафика

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.

22.27.1 Асимметричная маршрутизация при наличии роутера в локальной сети

Неправильная топология сети, способствующая асимметричной маршрутизации:

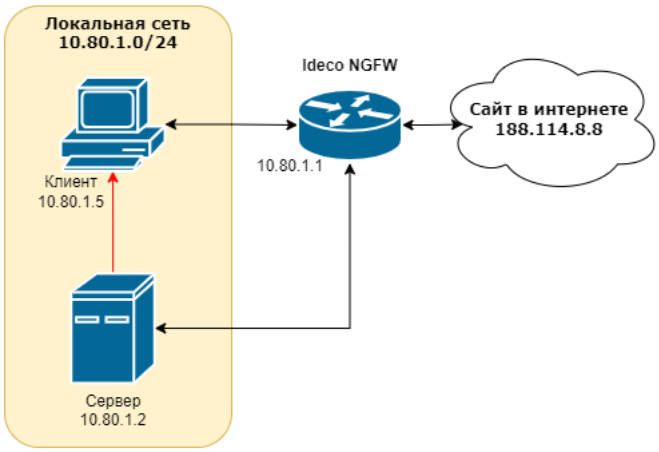


- `10.80.1.1` - шлюз для локальной сети `10.80.1.0/24`;
- `10.80.1.2` - роутер, имеющий доступ в удаленную сеть `192.168.10.0/24`;
- `10.80.1.5` - адрес хоста в локальной сети;
- **Красные стрелки** - двусторонняя связь роутера с удаленным шлюзом или роутером, обеспечивающая доступ к удаленной сети `192.168.10.0/24` (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.

22.27.2 Асимметричная маршрутизация при публикации сайтов через DNAT

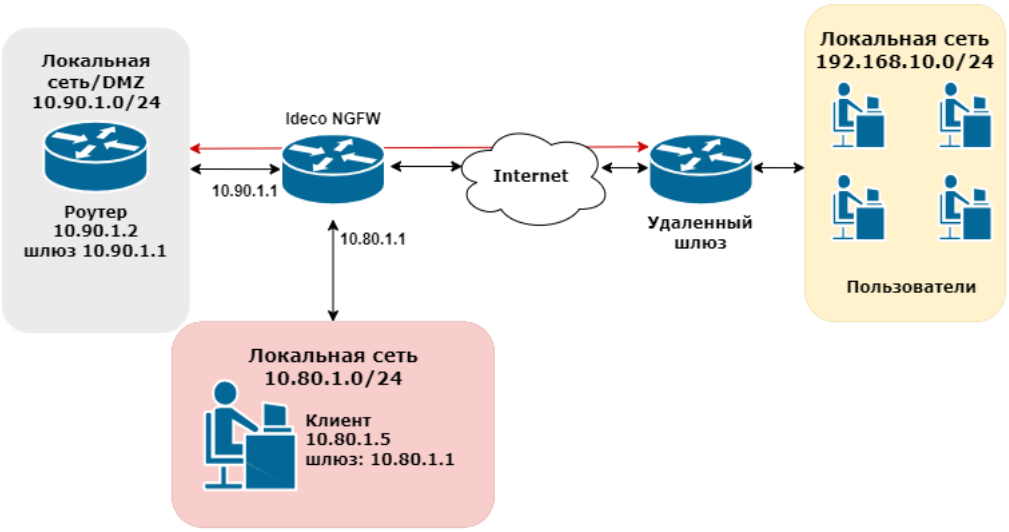
Асимметричная маршрутизация также возникает, когда в одной локальной сети находится хост и сервер, на котором расположен опубликованный при помощи DNAT-правила ресурс:



- `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.

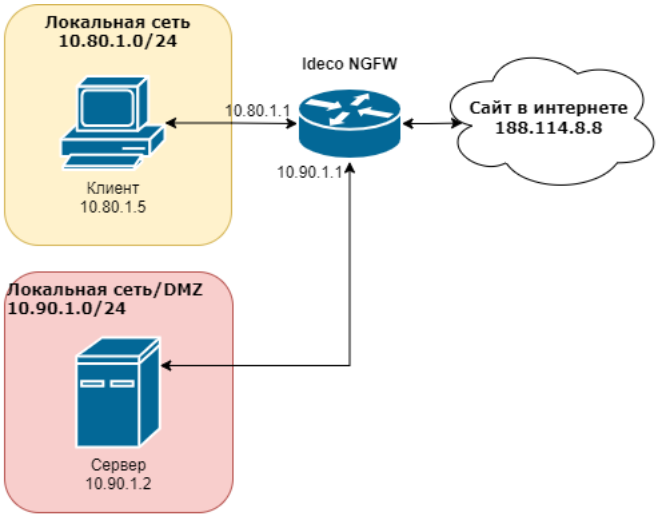
Когда хост `10.80.1.5` обращается на сайт по внешнему адресу `188.114.8.8` (например, в случае обращения по доменному имени, которое разрешено во внешнем IP), трафик проходит через NGFW. На NGFW срабатывает правило DNAT и перенаправляет трафик на сервер `10.80.1.2`, а сервер отвечает хосту, минуя NGFW.

22.27.3 Правильная топология сети:



Для правильной работы схемы нужно:

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. На роутере настроить IP-адрес 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.

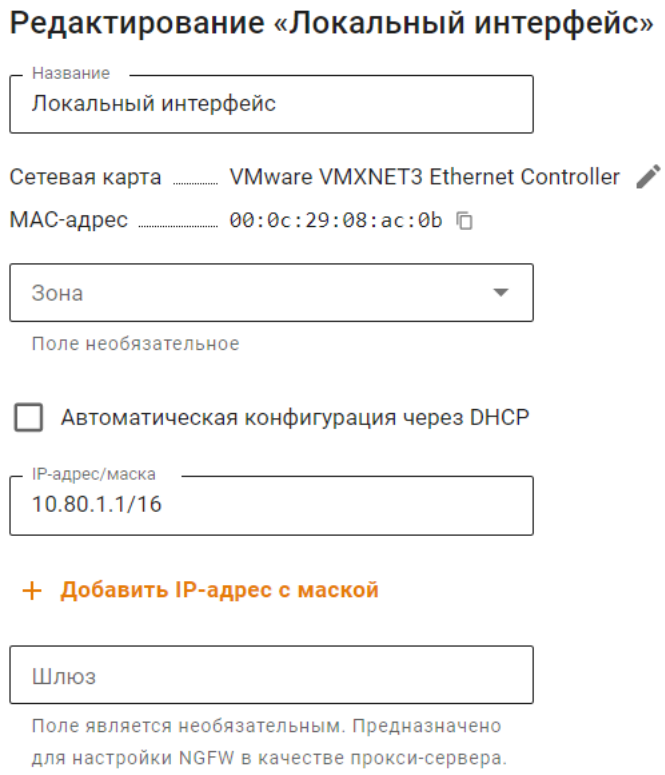
Физически роутер будет находиться в сегменте дополнительной сетевой карты.

Настройка NGFW:

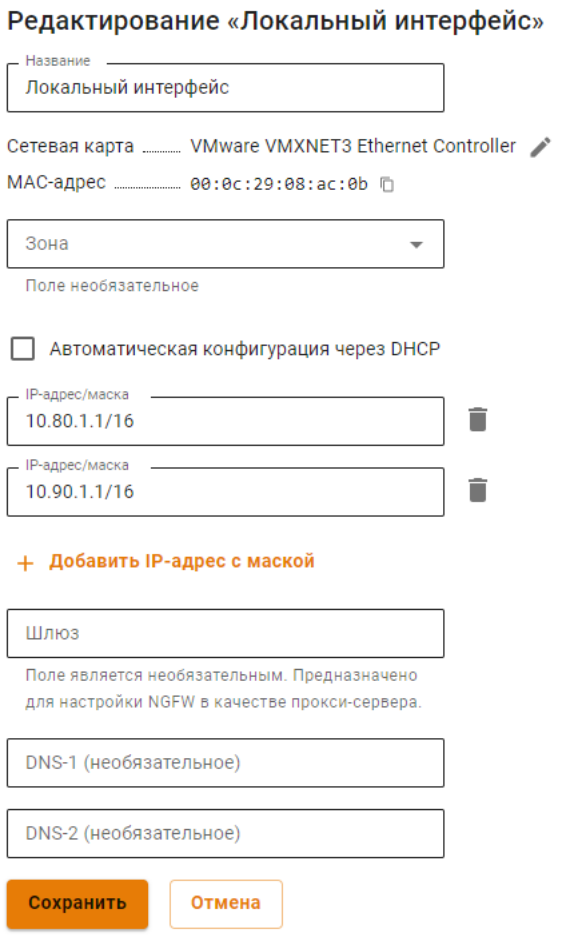
Для настройки нескольких виртуальных локальных сетей на одном физическом локальном интерфейсе NGFW перейдите в раздел **Сервисы -> Сетевые интерфейсы** и выполните действия:

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, снимите галку и введите его вручную:



3. Нажмите на + Добавить IP-адрес с маской и введите IP-адрес DMZ для изоляции роутера:

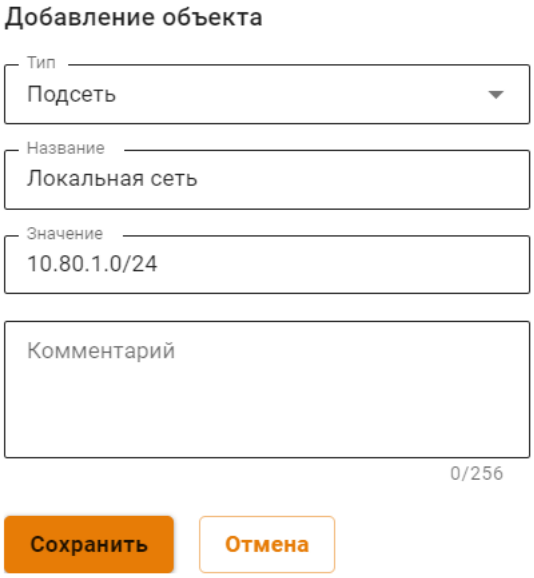


4. Нажмите **Сохранить**.

После изоляции роутера в DMZ нужно указать маршрут на NGFW до удаленной сети. Для этого перейдите в **Сервисы -> Маршрутизация** и выполните действия:

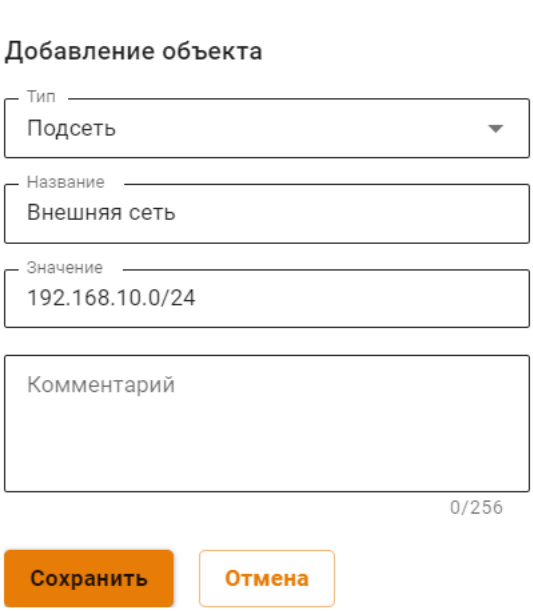
1. Перейдите на вкладку **Внешних сетей** нажмите кнопку **Добавить**.

2. В поле **Адрес источника** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес вашей локальной сети (`10.80.1.0/24`):



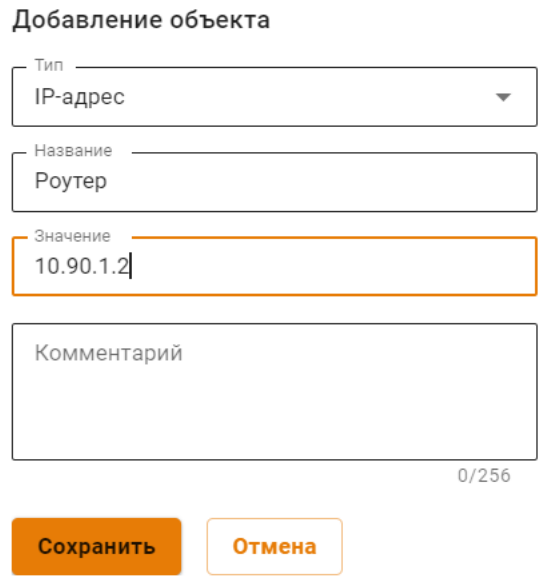
Выберите в качестве источника только что созданный объект.

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:

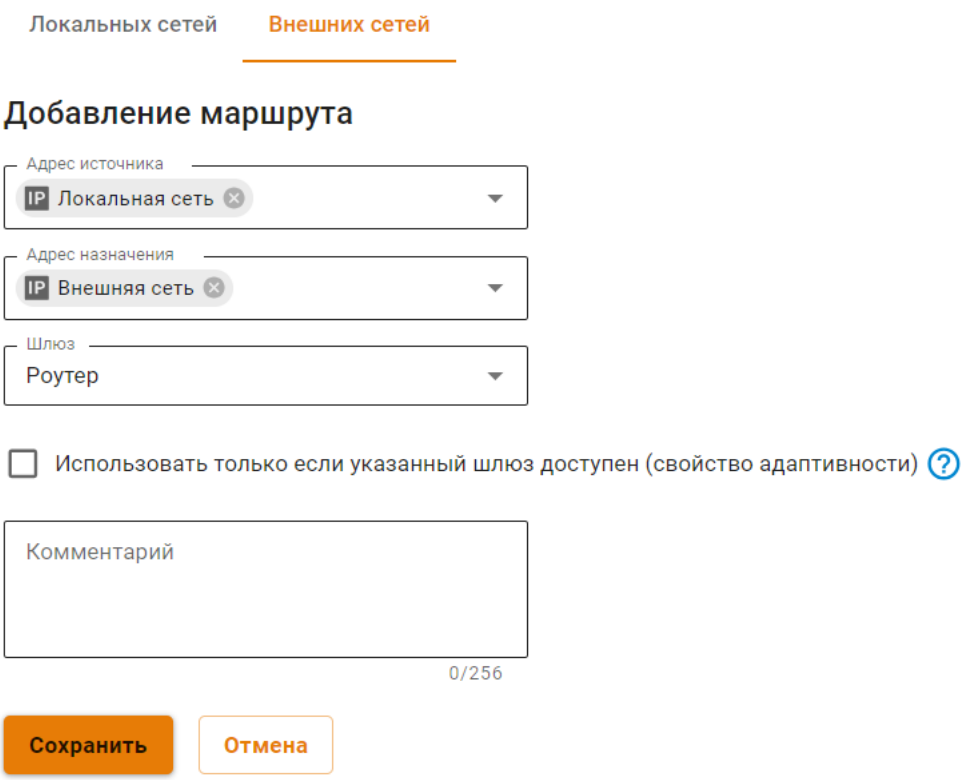


Выберите в качестве назначения только что созданный объект.

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:

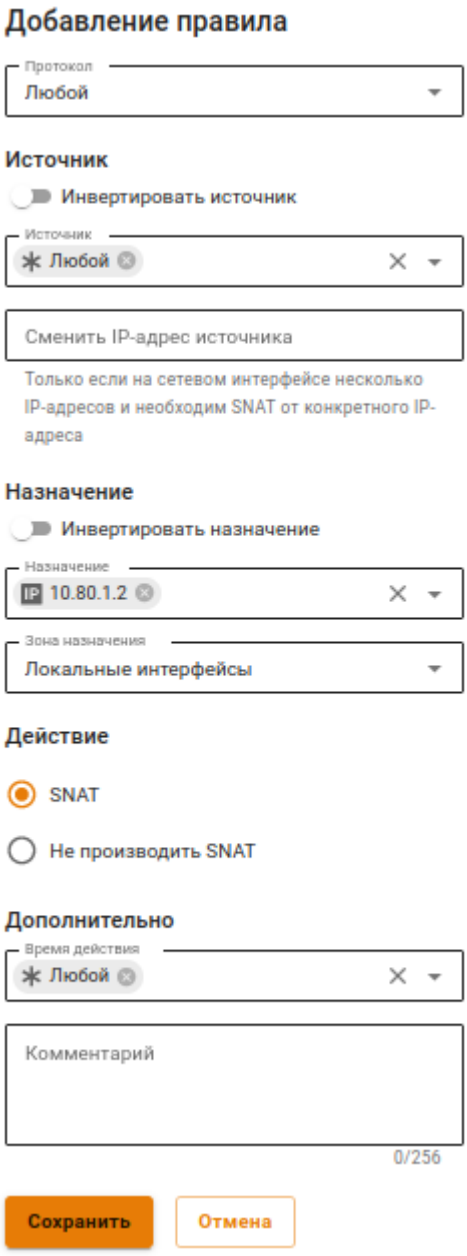
1. Для хостов из подсети `10.80.1.0/24` значение шлюза и DNS-сервера - `10.80.1.1`.

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 правило вида:



Заполните поля:

- Назначение - `10.80.1.2`;
- Зона назначения - Локальные интерфейсы.

В этом случае трафик хоста `10.80.1.5` на внешний адрес сайта `188.114.8.8` будет перенаправлен на адрес сервера `10.80.1.2` правилом DNAT. При этом созданное правило SNAT заменит адрес источника `10.80.1.5` на адрес NGFW - пакет приобретет вид: `scr 10.80.1.1 dst 10.80.1.2`. Ответ от сервера также пройдет через NGFW - пакет `scr 10.80.1.2 dst 10.80.1.1`.

22.28 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.

22.28.1 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.

22.28.2 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

22.29 Как восстановить доступ к Ideco NGFW

22.29.1 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 комбинацию кнопок `Ctrl - X`.

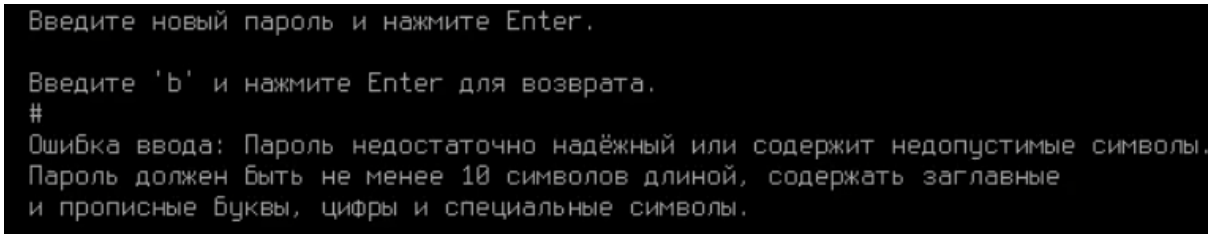
4. После повторной загрузки системы появится окно создания аккаунта администратора. Задайте новый логин и пароль администратора:

```
Ideco UTM 12.4 сборка 1
-----------------------

Создание аккаунта администратора.

Введите новый логин и нажмите Enter.

# testuser

Введите новый пароль и нажмите Enter.

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

Требования к созданию пароля администратора:

- Минимальная длина пароля - 12 символов;
- Строчные и заглавные латинские символы;
- Цифры;
- Специальные символы (! # $ % & „ * + и т. д.).

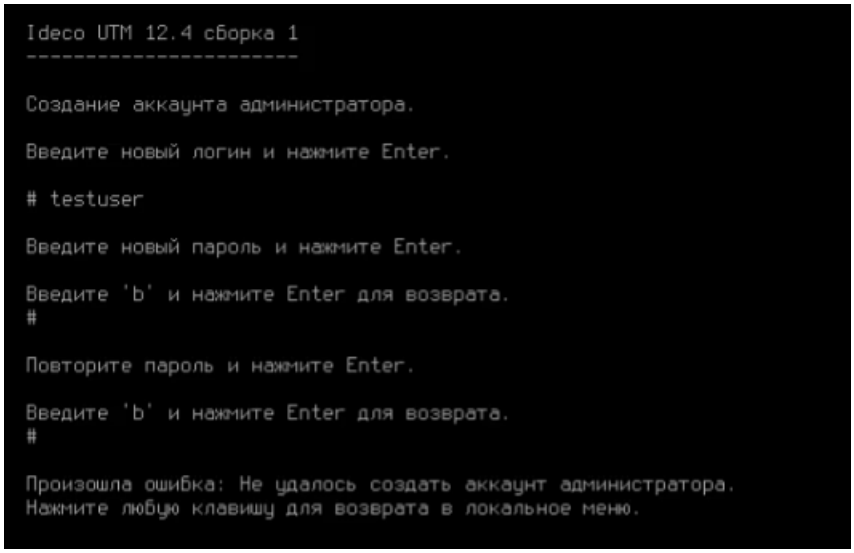
Если пароль не будет соответствовать требованиям политики безопасности, то появится ошибка:



Необходимо ввести новый пароль, учитывая требования к созданию паролей.

Предупреждение: Если при создании нового логина администратора он будет совпадать с предыдущим логином, то откроется окно с выводом ошибки. Создайте имя администратора, отличное от предыдущего.

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



22.30 Как восстановиться на прошлую версию после обновления Ideco NGFW

22.30.1 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.

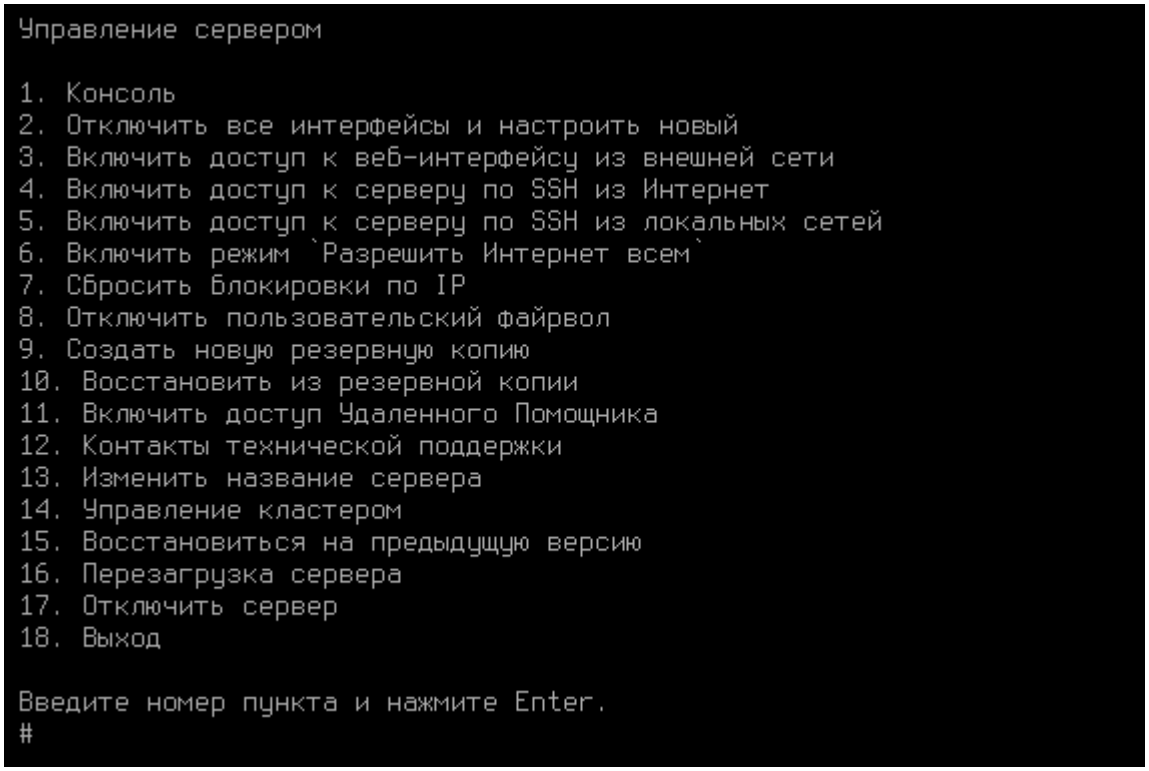
При восстановлении на предыдущую версию данные перенесены не будут. Сохраните бекап на внешнем носителе.

Для восстановления на предыдущую версию выполните действия:

1. Перейдите в локальное меню Ideco NGFW.

2. Введите логин и пароль администратора.

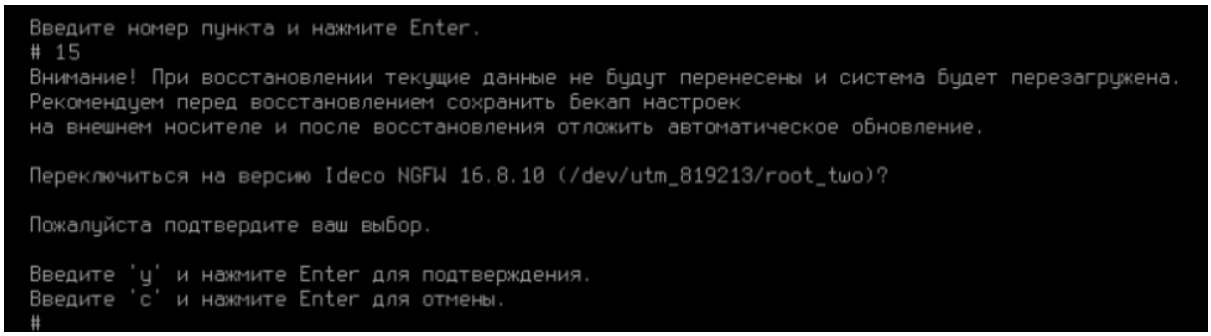
3. Укажите номер пункта 15 и нажмите **Enter**:



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.

22.31 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.

22.31.1 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*;
- *Антивирусы веб-трафика* (включен антивирус ClamAV или 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 неё 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*.

22.31.2 Проверка настроек служб

Контент-фильтр

Правила **Контент-фильтра** должны запрещать следующие категории сайтов:

- 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» создайте правила, которые будут блокировать доступ к следующим протоколам:

- Bittorrent;
- Steam;
- Worldofwarcraft;
- Mining.

Предотвращение вторжений

В этой службе должны быть активны следующие группы правил:

- Анонимайзеры;
- Пулы криптомайнеров.

Некоторые правила системы работают с помощью блокировки DNS-запросов пользователей, поэтому, если используете Ideco NGFW в качестве прокси-сервера, убедитесь, что DNS-запросы также проходят через него (например, сделайте так, чтобы контроллер домена Active Directory резолвил имена через Ideco NGFW).

Подсказка: После изменений правил проведите повторное тестирование с помощью security.ideco.ru.

22.32 Выбор аппаратной платформы для Ideco NGFW

22.32.1 Сведения о программной платформе

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 37 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 37.

22.32.2 Общие рекомендации по чипсетам и производителям

За годы работы с серверами клиентов мы можем выделить несколько закономерностей:

- Лучше остальных зарекомендовали себя 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. Лидирует по качеству тут также Intel;
- 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.

22.32.3 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.

Подсказка: Минимальные *системные требования* удовлетворяют низкой загруженности служб NGFW, обслуживающих небольшое количество авторизованных пользователей. Если обслуживается большее количество пользователей (от 50) и сервисов на Ideco NGFW, обратите внимание на рекомендуемые и максимальные системные требования сервера.

22.32.4 Дисковая подсистема

RAID-массивы не требуются при типичных схемах использования NGFW. Одного современного SATA жесткого диска от 200 ГБ хватает в большинстве конфигураций. В случае интенсивного использования почтового сервера на Ideco NGFW советуем подключать отдельный винчестер для хранения почтовой корреспонденции. Использование SSD-дисков также возможно и рекомендуется. Рекомендуем использовать устройства марки Micron.

22.33 Поддержка устаревших алгоритмов шифрования

22.33.1 Основное

Ideco NGFW основан на операционной системе Fedora. В Ideco NGFW используется Fedora 37. 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.

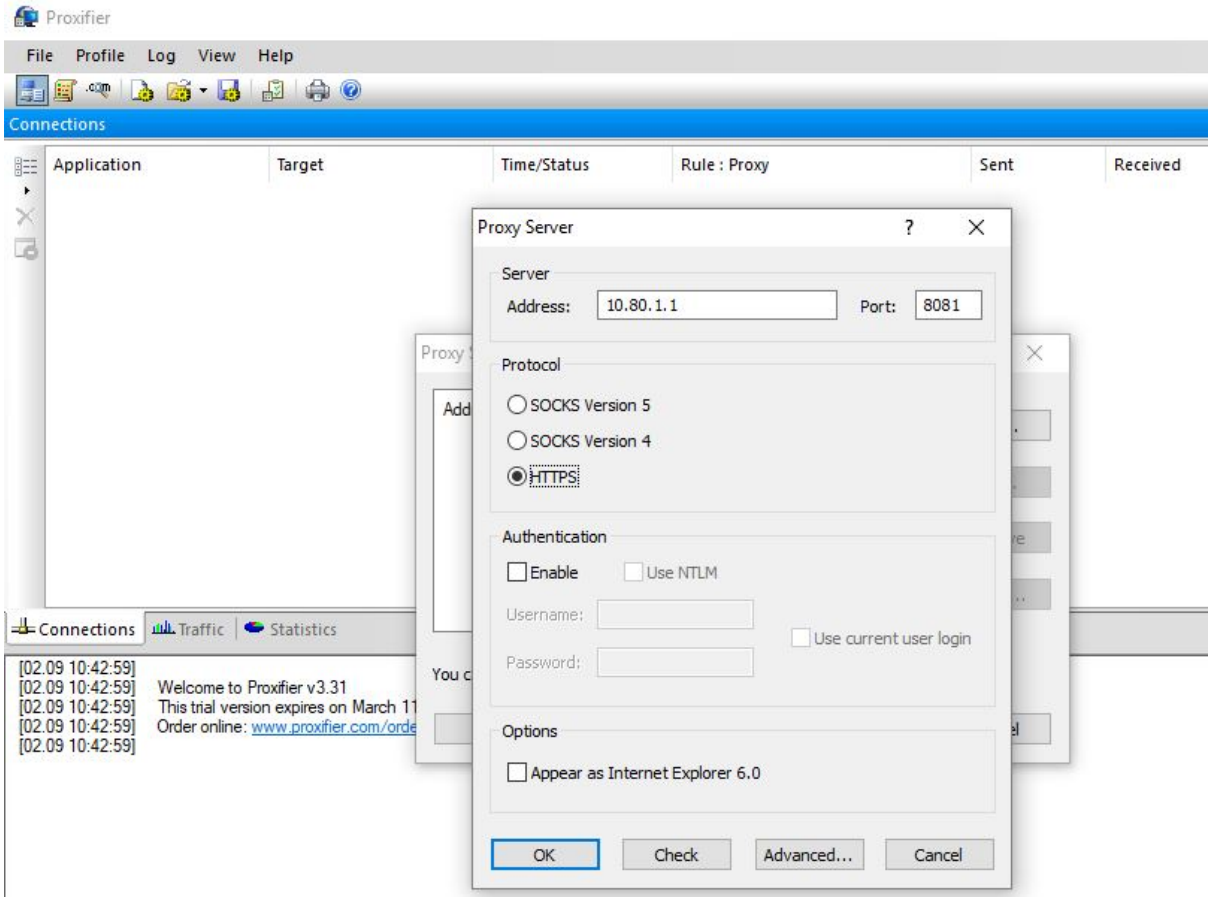
22.34 Настройка программы Proxifier для прямых подключений к прокси серверу

Скачать Proxifier можно с сайта разработчика.

22.34.1 Настройка

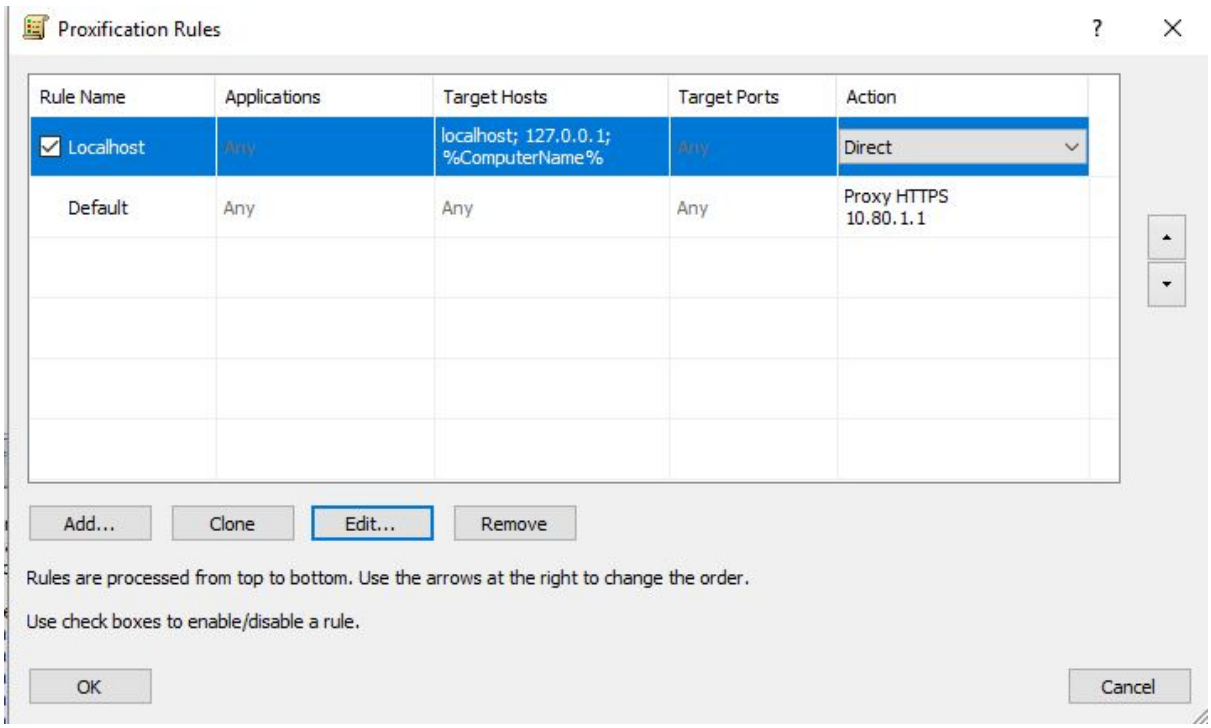
Выполните стандартные настройки браузера для прямых подключений к прокси-серверу, а затем настройте программу для перенаправления остального трафика на прокси-сервер.

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.

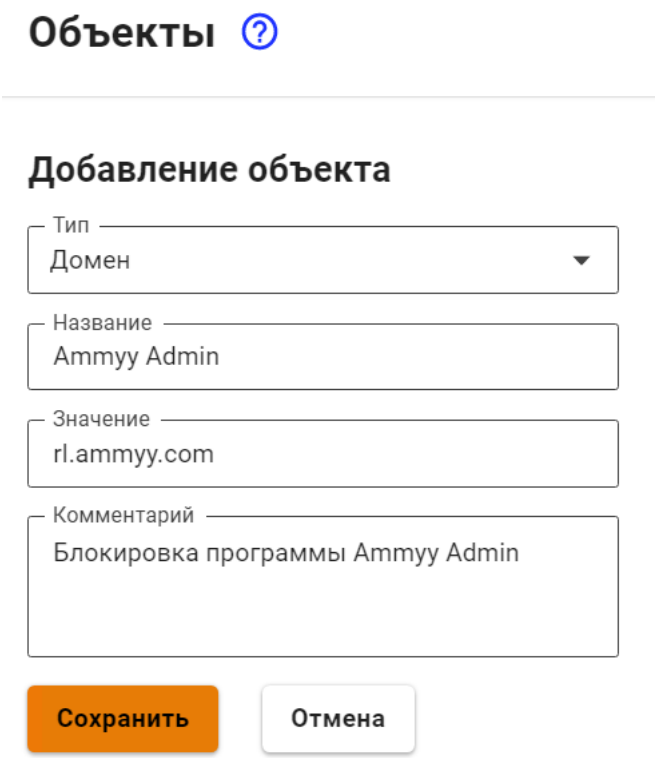
22.35 Блокировка популярных ресурсов

22.35.1 Основное

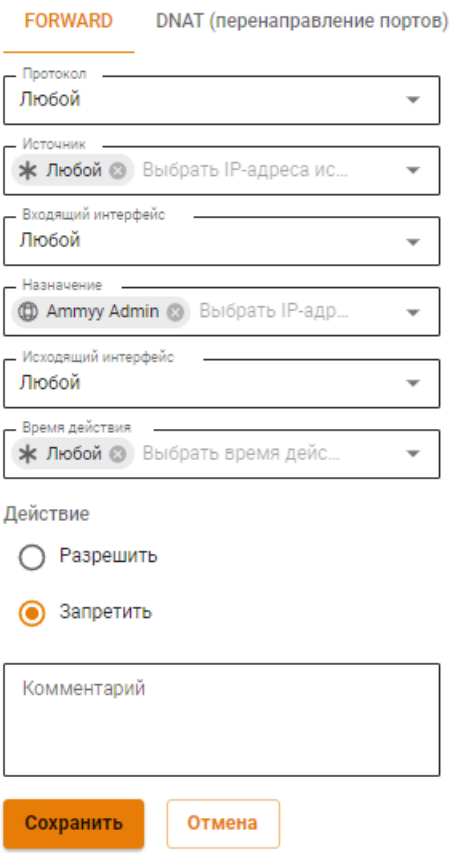
Блокировка Ammyy Admin:

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:



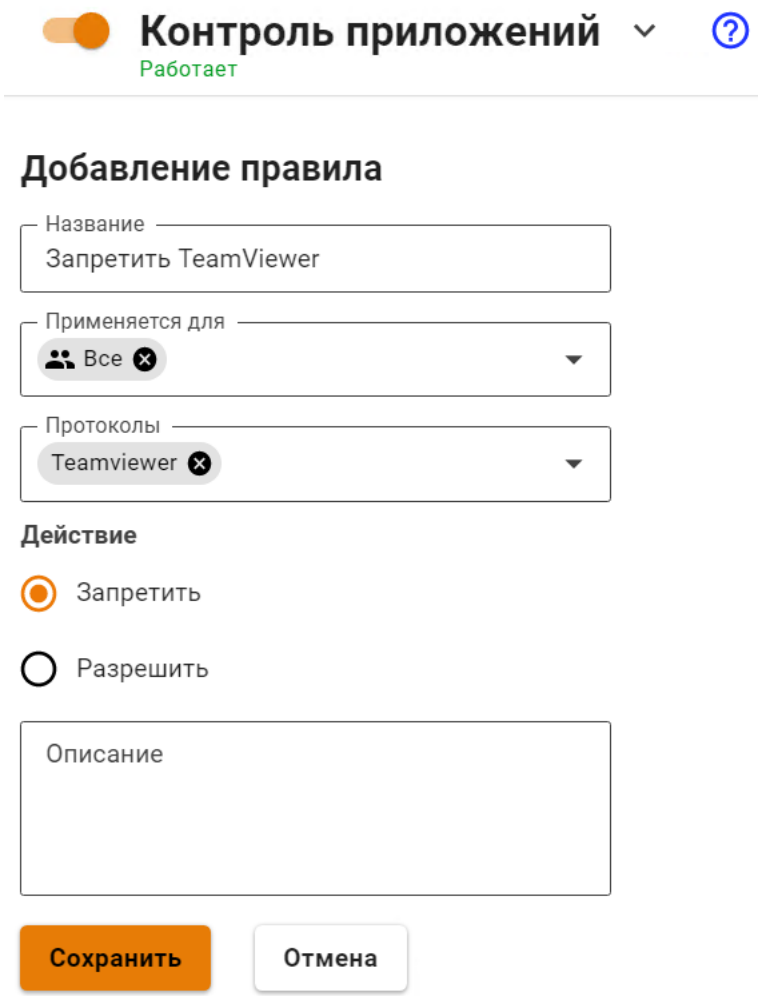
2. Перейдите на вкладку **Правила трафика -> Файрвол -> FORWARD** и создайте правило запрета для нужных пользователей или групп. В поле **Назначение** выберите объект, созданный в пункте 1:



Блокировка TeamViewer:

TeamViewer - это программное обеспечение для удаленного доступа и управления компьютерами. Его можно заблокировать с помощью *Контроль приложений*.

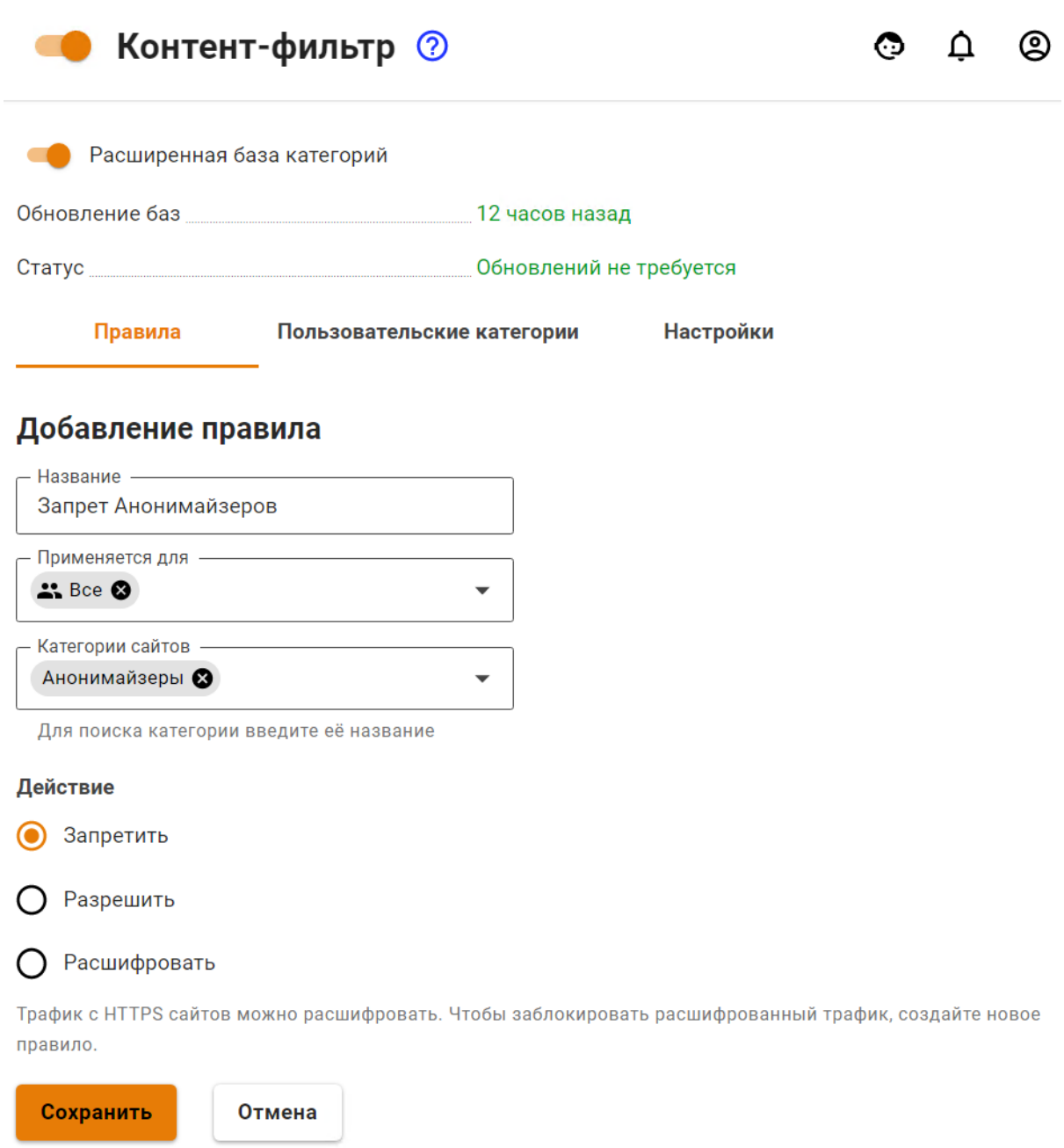
Перейдите в раздел **Правила трафика -> Контроль приложений**. Создайте новое правило, указав в поле **Протоколы** значение TeamViewer:



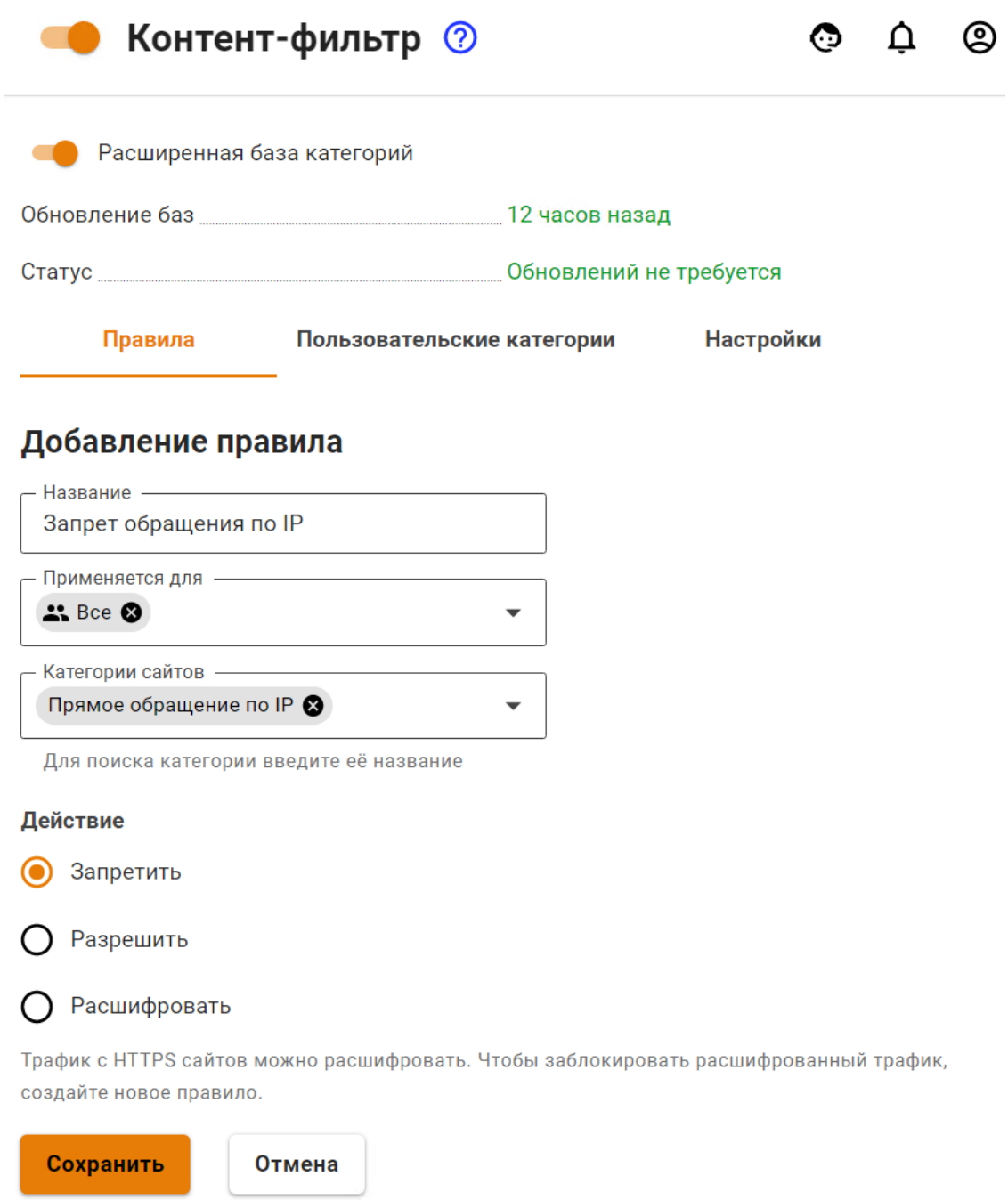
Блокировка анонимайзеров:

Заблокировать анонимайзеры можно в разделе **Правила трафика** тремя способами:

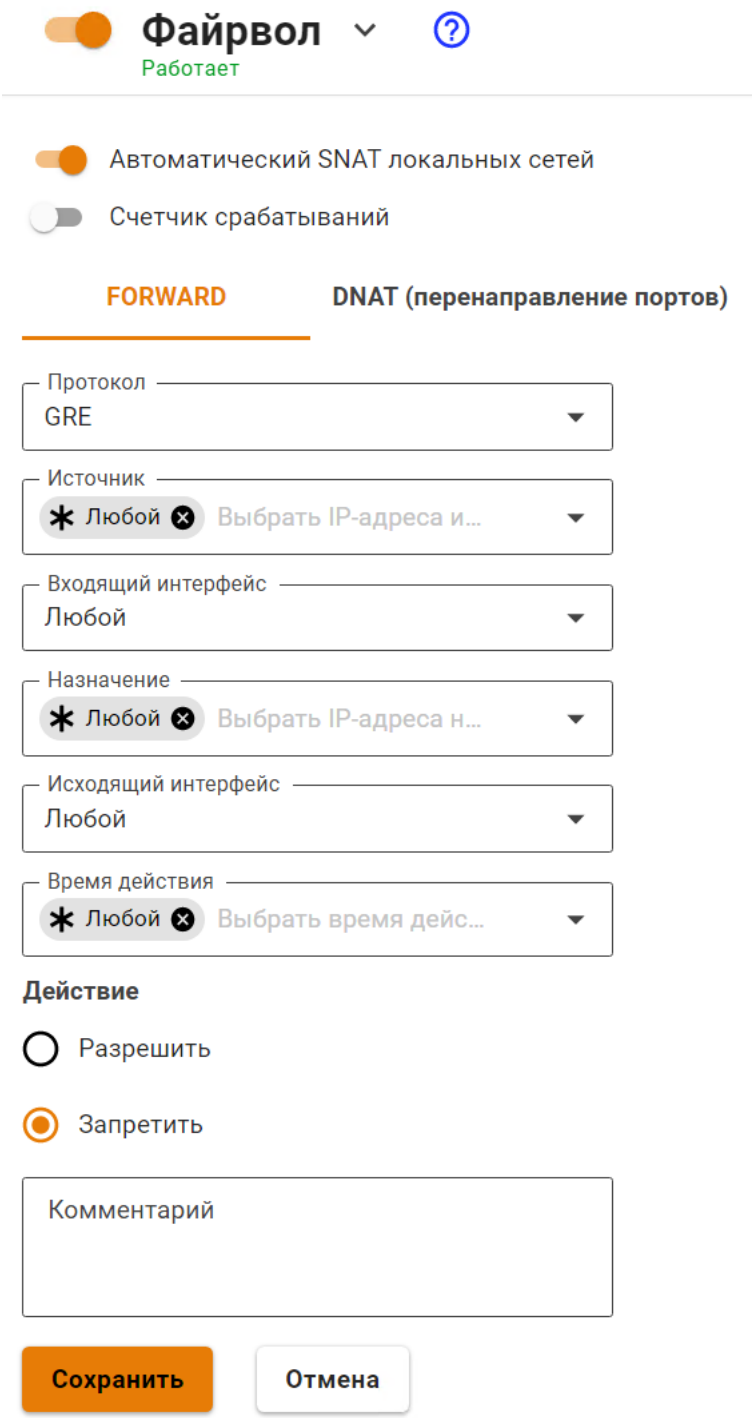
1. Анонимайзеры, работающие по протоколам HTTP(S), можно заблокировать в разделе *Контент-фильтр*. Для этого создайте правило, в котором запретите категорию сайтов **Анонимайзеры**:



2. Чтобы предотвратить обход Контент-фильтра, создайте правило, которое будет блокировать прямые обращения по IP-адресам в Контент-фильтре:



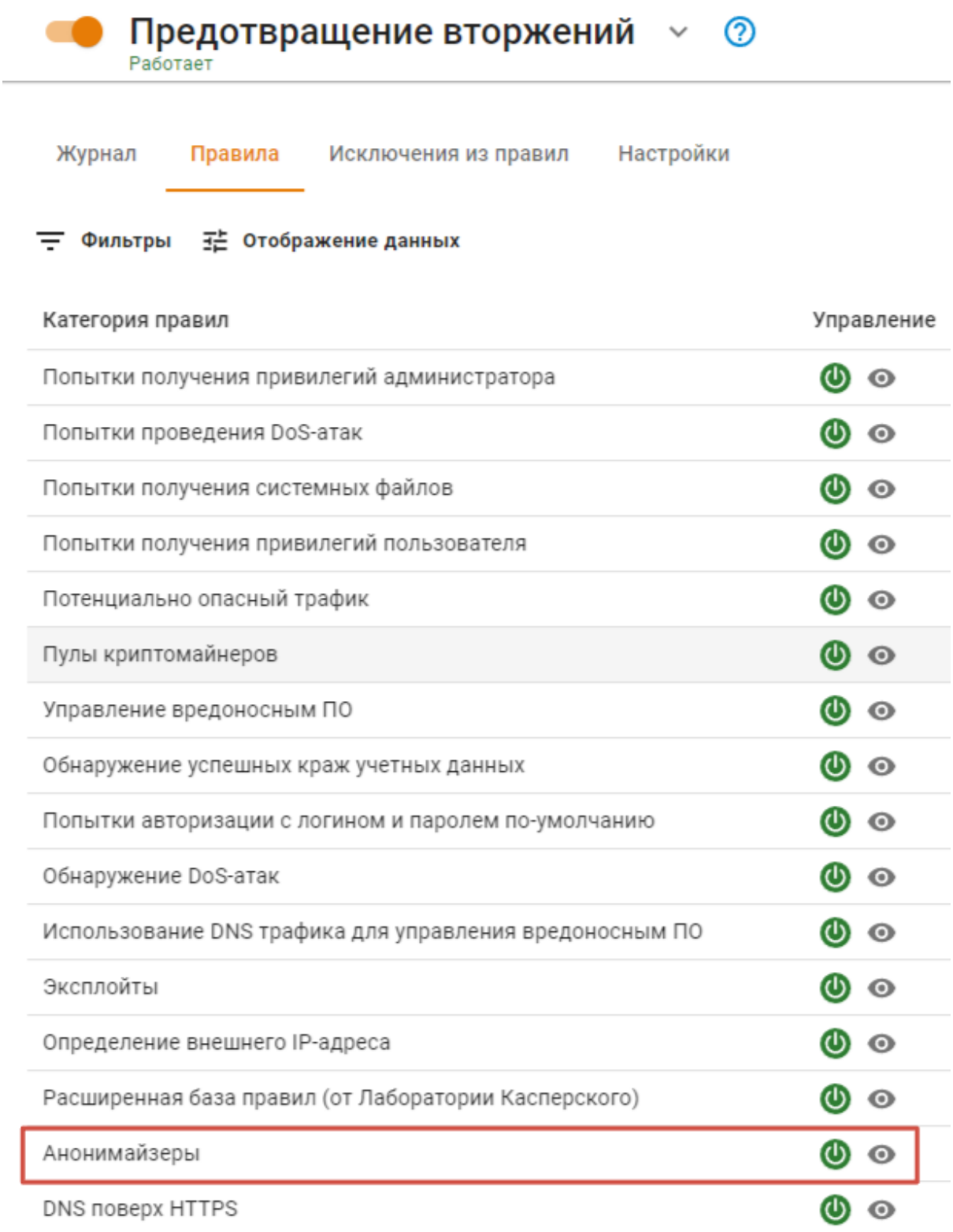
3. Для блокировки VPN-анонимайзеров, использующих протокол PPTP, достаточно заблокировать протокол GRE в правилах *Файрвола*:



Блокировка Opera.Turbo, Opera VPN, Yandex.Turbo, friGate, Anonymox:

Чтобы заблокировать функции браузеров, которые используются для обхода контентной фильтрации, можно воспользоваться разделом *Предотвращение вторжений*.

Перейдите на вкладку **Правила трафика -> Предотвращение вторжений -> Правила** и активируйте категорию **Анонимайзеры**:

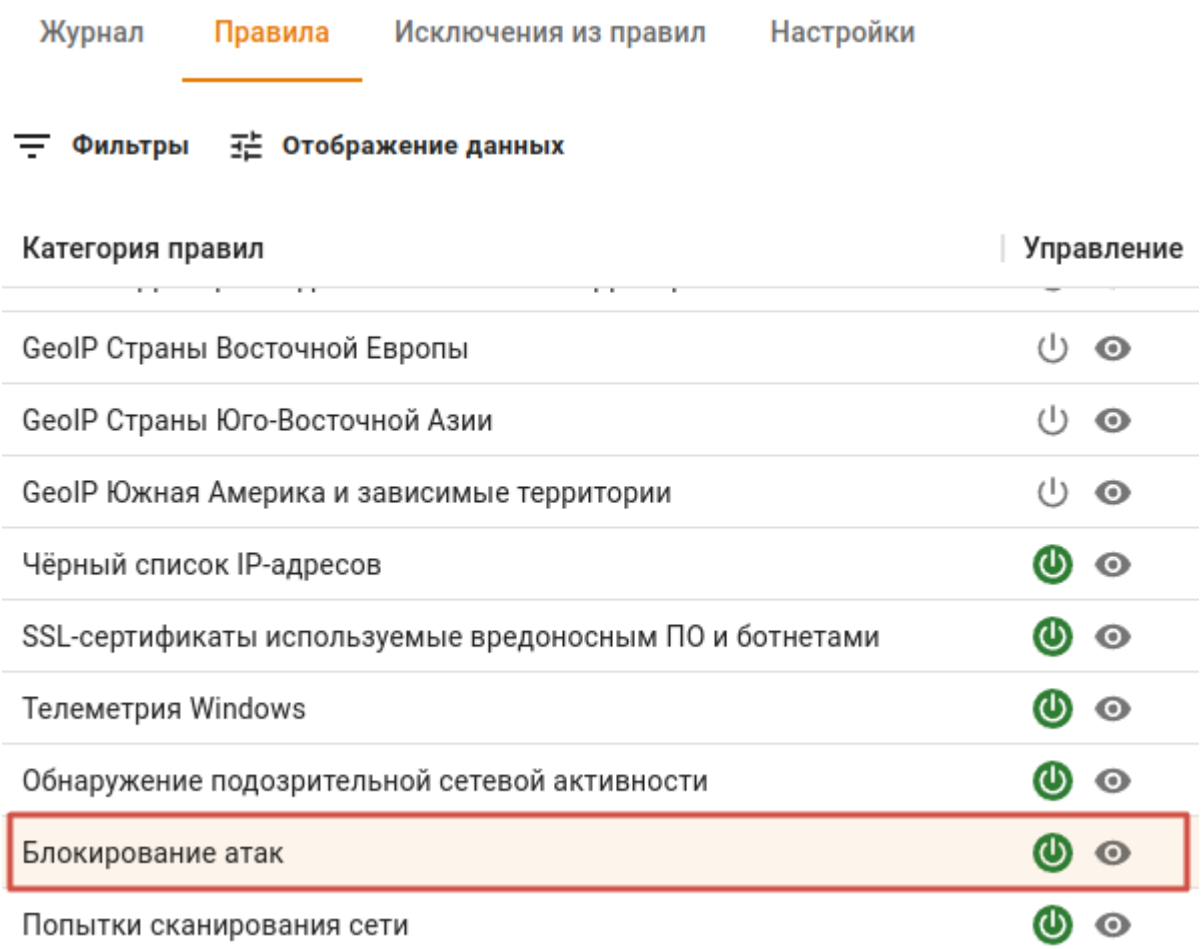


Блокировка Tor:

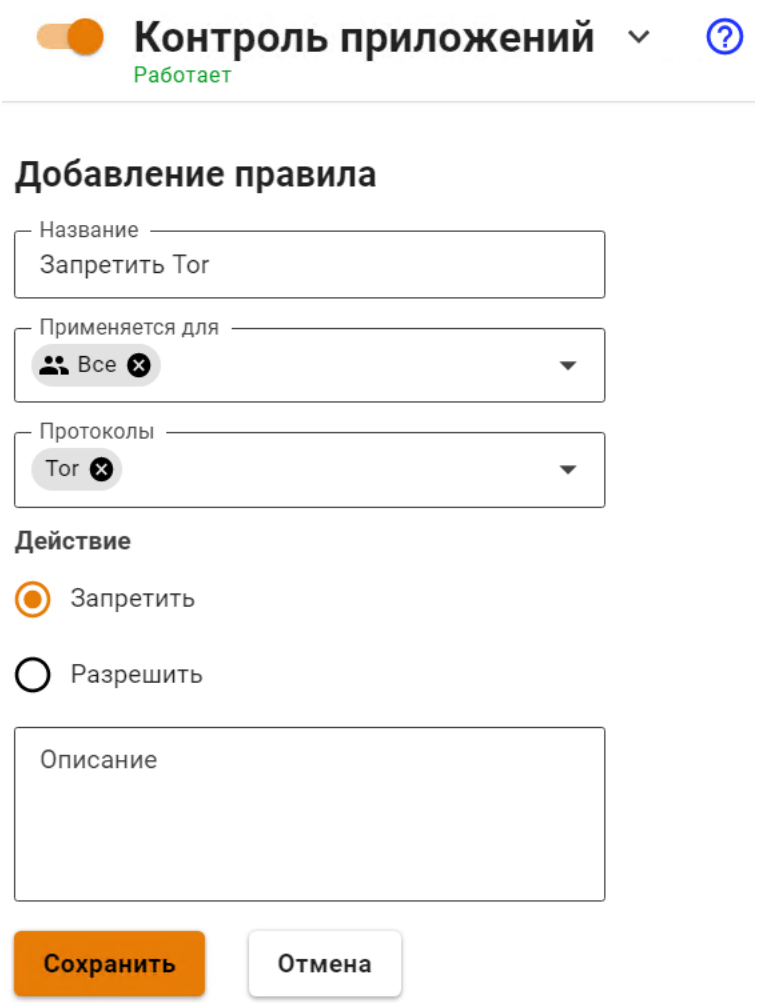
Tor - специально разработанное программное обеспечение и среда прокси-серверов, предназначенная для обхода различного рода блокировок, поэтому полностью заблокировать его сейчас невозможно.

Для противодействия использованию сети Tor, а также для журналирования попыток подключения к ней и ее использования выполните следующие настройки:

1. Включите систему *Предотвращение вторжений* и активируйте в ней категорию **Блокирование атак**:



2. Включите систему *Контроль приложений* и добавьте правила запрета приложения **Tor** определенной группе или всем пользователям:

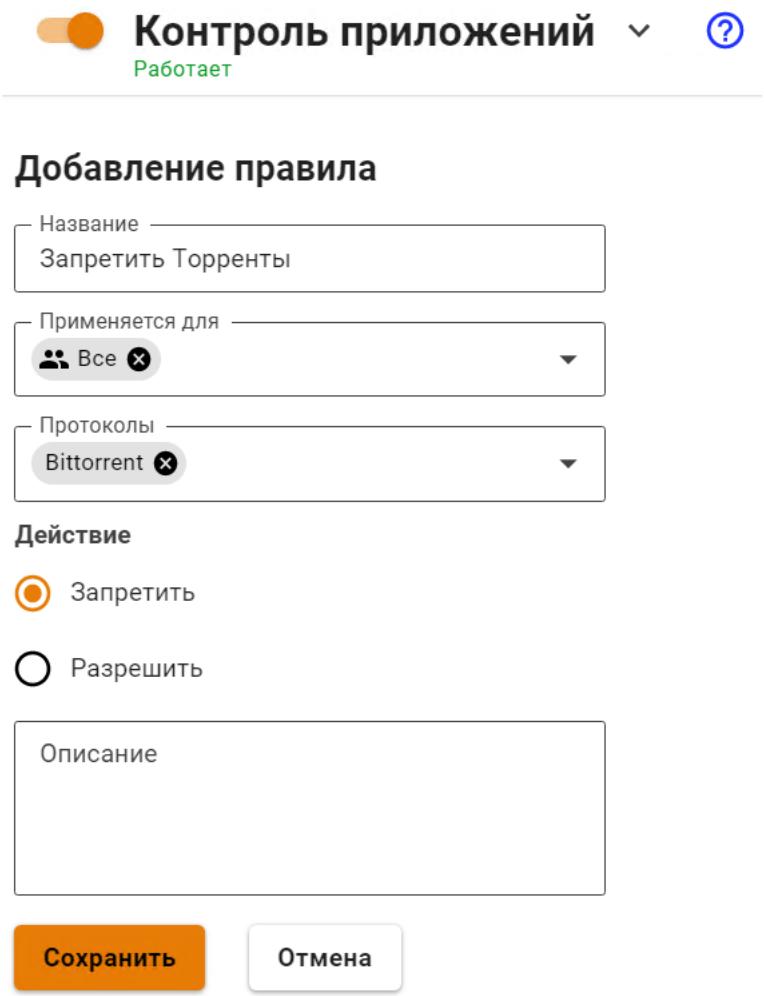


Блокировка торрентов:

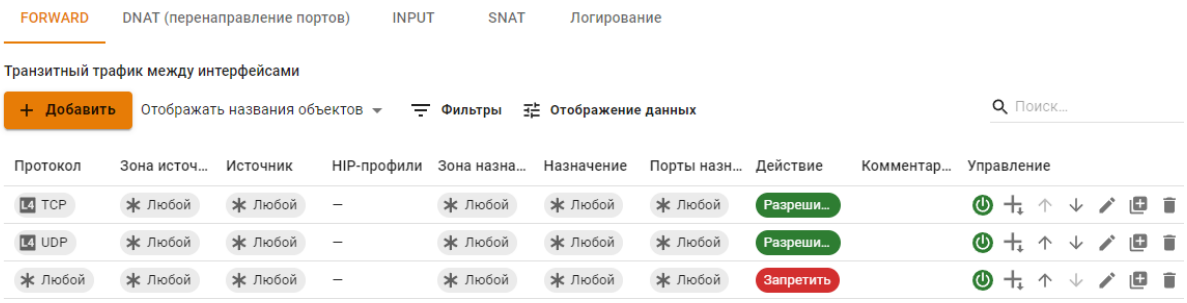
BitTorrent - P2P-протокол, предназначенный для обмена файлами через интернет.

Для ограничения возможности использования торрентов выполните следующие настройки:

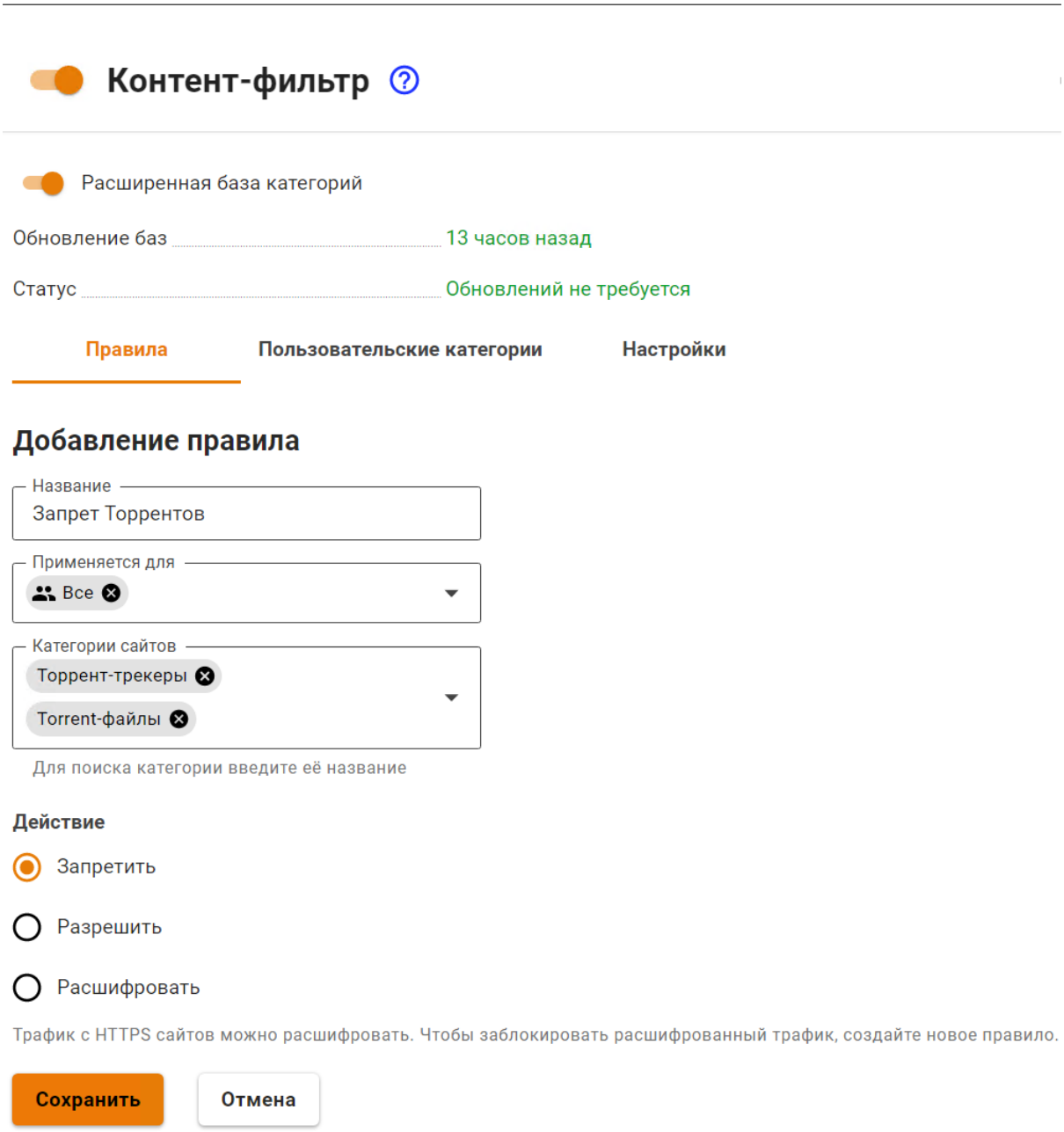
1. Запретите протокол BitTorrent с помощью правила в разделе *Контроль приложений*:



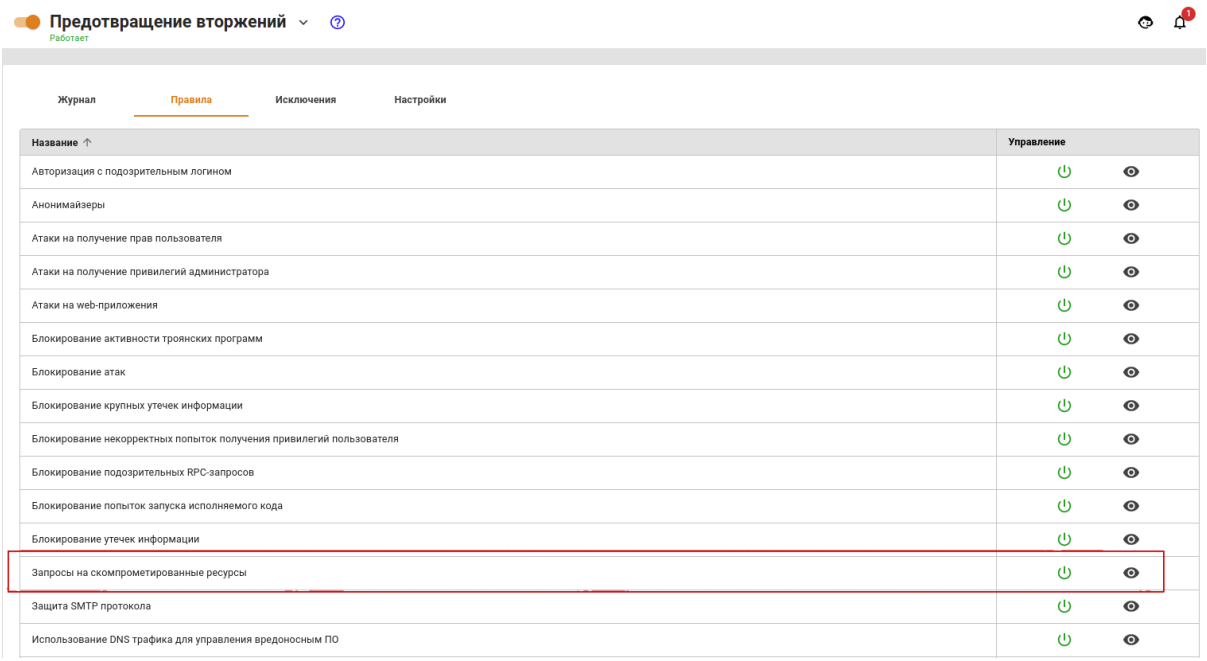
2. Перейдите на вкладку **Правила трафика -> Файрвол -> FORWARD** и разрешите нужные TCP и UDP порты пользователям. Затем создайте правило, которое запрещает все протоколы (правила действуют сверху вниз):



3. В разделе *Контент-фильтр* заблокируйте доступ к сайтам-каталогам и торрент-файлам. Для этого запретите категории **Торрент-трекеры** и **Torrent-файлы**:



4. В разделе *Предотвращение вторжений* активируйте категорию правил **Запросы на скомпрометированные ресурсы**, которая позволяет блокировать активность P2P-программ:



22.36 Настройка прозрачной авторизации на Astra Linux

22.36.1 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**:**

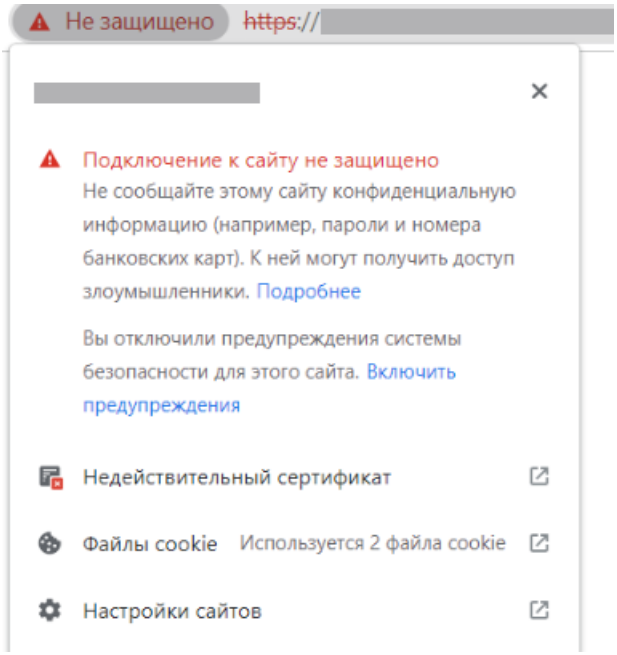
1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

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*.

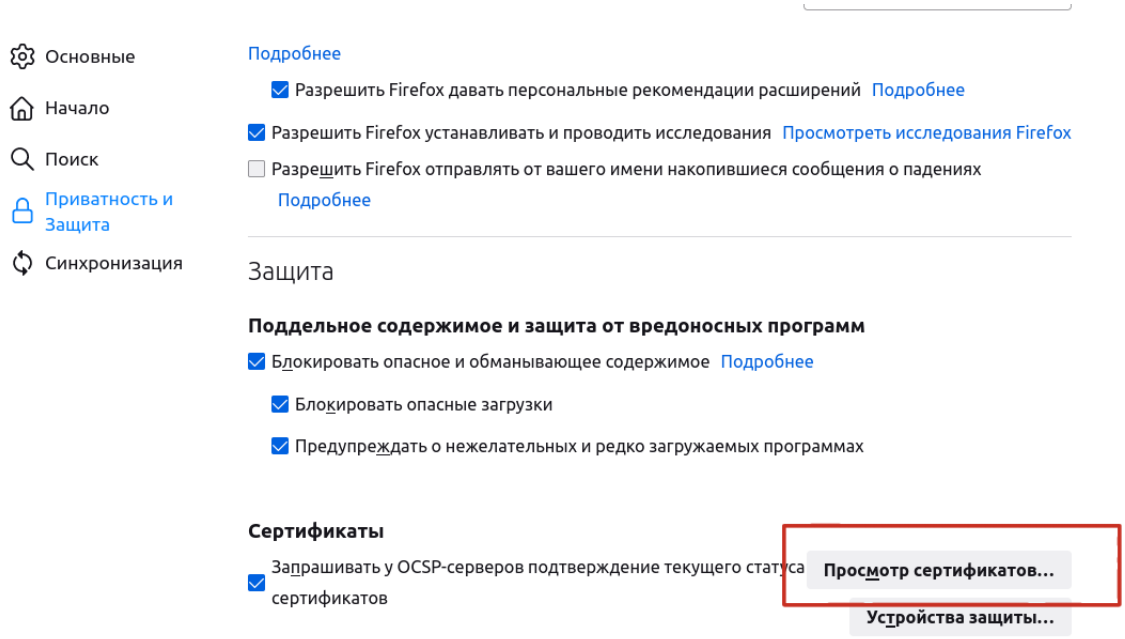
2. В браузере Chromium перейдите на вкладку **Безопасность -> Управление сертификатами -> Центры сертификации -> Импортировать** и добавьте сертификат в список доверенных.

**

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.

22.37 Настройка автоматической веб-аутентификации на Ideco NGFW на Linux

22.37.1 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`.

22.37.2 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
```

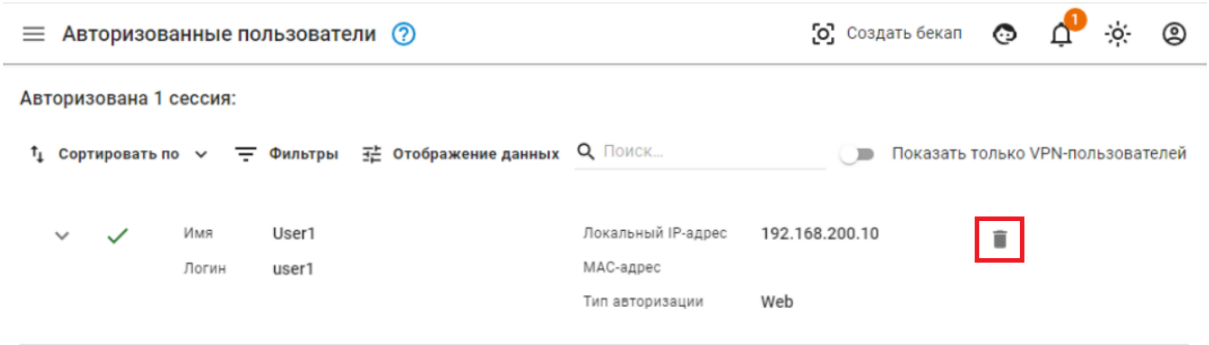
Введите имя пользователя Linux и полный путь до скрипта.

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.

22.38 Перенос данных и настроек на другой сервер

Подсказка: Восстановить бэкап настроек в Ideco UTM 9 из Ideco UTM 7 можно только с версии 7.9.9 Build 176.

Чтобы перенести установленный Ideco NGFW с одного сервера на другой с сохранением всех настроек, выполните следующие действия:

22.38.1 Этап 1: Копирование резервных копий с сервера

В разделе веб-интерфейса **Управление сервером -> Резервное копирование -> Резервные копии** создайте резервную копию настроек сервера. Загрузите созданную копию на ваш компьютер, нажав на кнопку **Скачать** в столбце **Управление**.

22.38.2 Этап 2. Установка Ideco NGFW на новый сервер

Инструкция по установке: *Процесс установки*.

22.38.3 Этап 3: Перенос резервных копий 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 -> Резервное копирование -> Резервные копии** нажмите кнопку добавления резервной копии -> **Загрузить из файла** и выберите выгруженный на первом этапе бекап.

22.38.4 Этап 4: Восстановление БД из резервной копии

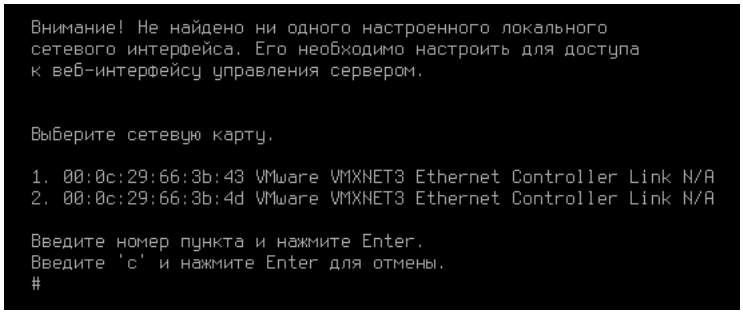
Нажмите кнопку **Применить** (иконка в столбце **Управление**). Система будет перезагружена для применения настроек сервера.

22.38.5 Этап 5: Настройка восстановленного сервера

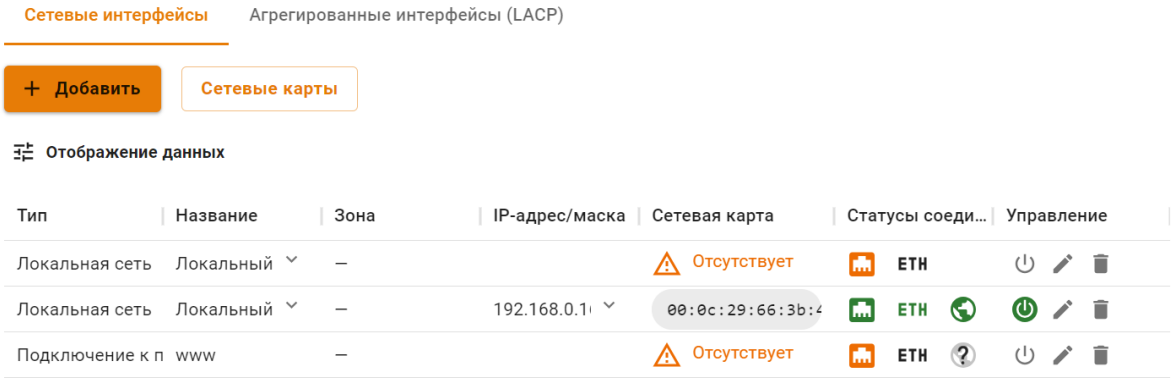
После перезагрузки Ideco NGFW, восстановленного из резервной копии, веб-интерфейс будет недоступен, поскольку ни один локальный интерфейс не будет настроен. Для настройки выполните действия:

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 бекапа, 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;

22.38.6 Этап 6: Привязка лицензии к восстановленному из резервной копии серверу

Если вы переносите резервную копию 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 демо-лицензию от нового сервера, нажав на  .

3. Привяжите энтерпрайз-лицензию к новому серверу, нажав на 

.

Предупреждение: При подключении к Ideco Center восстановленного из бекапа клона сервера он не появится в таблице серверов Ideco Center. Возникает конфликт с донором резервной копии из-за одинакового claster_id. Сервер-клон подменяет собой уже подключенный Ideco NGFW:

В случае возникновения такой проблемы обратитесь в *Техническую поддержку*.

22.38.7 Перенос данных почтового сервера

Чтобы перенести данные с UTM 7.9.9 на UTM 9.x с переносом почты на отдельный диск, выполните следующие действия:

1. Выкачайте всю почту из папки `/var/mail/` на внешнее хранилище. Это можно сделать с помощью различных программ для копирования файлов между локальным компьютером и удаленным сервером (например: rsync, WinSCP, scp от ssh и др.);
2. Установите с загрузочного образа последнюю версию Ideco NGFW на физический диск;
3. Подключите второй физический диск, который будет использоваться для хранения почты;
4. В веб-интерфейсе Ideco NGFW перейдите в раздел **Почтовый релей -> Основные настройки**, выберите диск для хранения почты и отформатируйте его;
5. Разрешите доступ по SSH из локальных сетей в разделе **Управление сервером -> Администраторы**;
6. Подключитесь к NGFW, например, с помощью программы WinSCP и скопируйте всю почту по пути `/var/mail/`;
7. По окончании копирования файлов почты, выполните команду `chown -R ideco-mail-backend:ideco-mail-backend /var/spool/mail/`. Она меняет владельца и группу для файлов почты, чтобы почтовый демон dovecot мог иметь доступ к этим файлам.

22.39 Порядок обработки веб-трафика в Ideco NGFW

Порядок обработки веб-трафика:

1. DNS.

2. Захват трафика для DPI:

   - Контроль приложений;
   - Ограничение скорости;
   - Система предотвращения вторжений.

3. Захват трафика для фильтрации (прокси-сервер):

   - Контент-фильтр;
   - Антивирус веб-трафика.

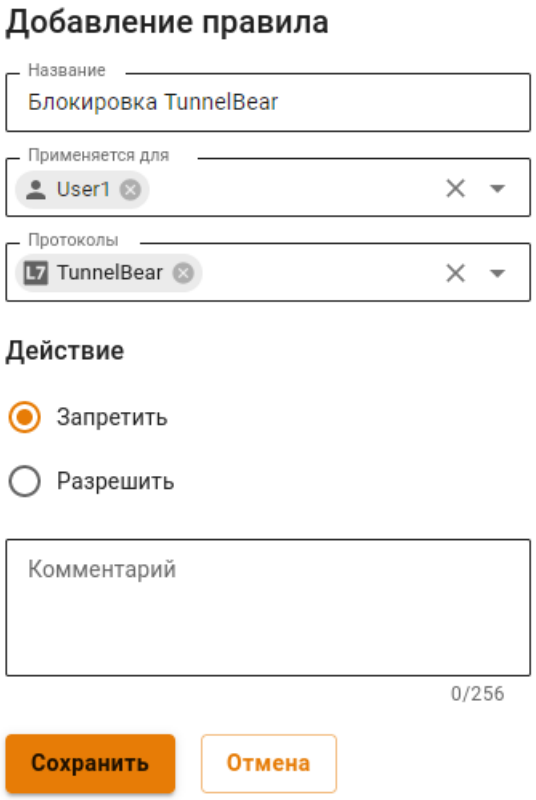
4. Файрвол.

Подсказка: INPUT-правила Файрвола обрабатывают трафик раньше прокси-сервера.

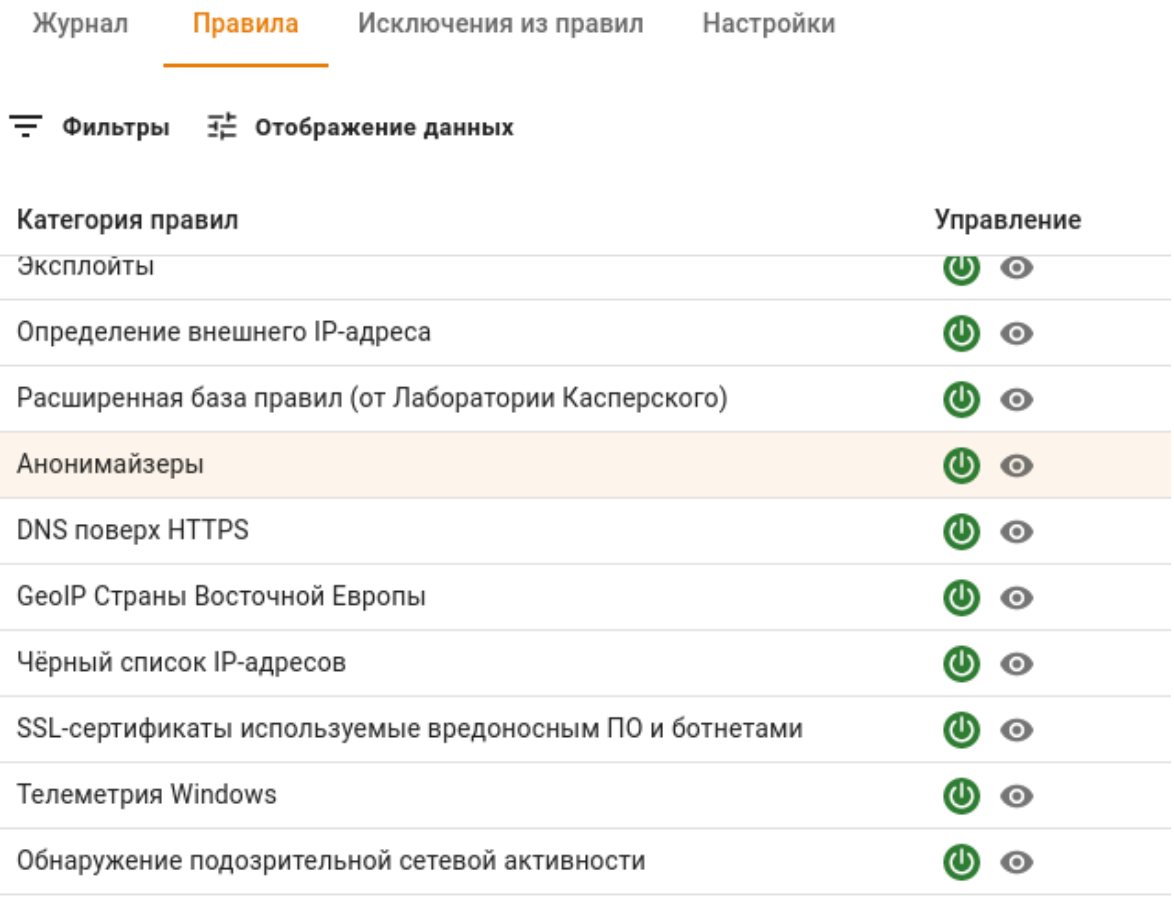
22.39.1 Как проверить, что заблокирует трафик первым: Контроль приложений или система Предотвращения вторжений?

Для примера заблокируем **TunnelBear** для **User1**.

1. Перейдите в раздел **Контроль приложений** и создайте правило, блокирующее протокол **TunnelBear** для **User1**:



2. Убедитесь, что в разделе **Предотвращение вторжений** активно правило блокировки **Анонимайзеры**:



3. Авторизуйте **User1** с устройства на Windows и попробуйте зайти на сайт `https://www.tunnelbear.com/`.

4. Перейдите в **Управление сервером -> Терминал** для просмотра логов **Контроля приложений**/системы **Предотвращение вторжений** и выполните команду:

```
journalctl -u ideco-app-control@Leth<номер локального интерфейса>.service -S today
```

Номер локального интерфейса можно узнать в Терминале, выполнив команду `ip a`.

В логах **Контроля приложений** появятся записи о блокировке протокола **TunnelBear**:

```
июн 26 16:11:45 localhost app-control[29554]: (flow_info_rules_was_checked) 192.168.
↪100.150:52168 -> 104.17.154.236:443 [TunnelBear] = 'DROP'.
июн 26 16:12:04 localhost app-control[29554]: (flow_info_rules_was_checked) 192.168.
↪100.150:52169 -> 104.17.155.236:443 [TunnelBear] = 'DROP'.
июн 26 16:12:23 localhost app-control[29554]: (flow_info_rules_was_checked) 192.168.
↪100.150:52170 -> 104.17.154.236:443 [TunnelBear] = 'DROP'.
```

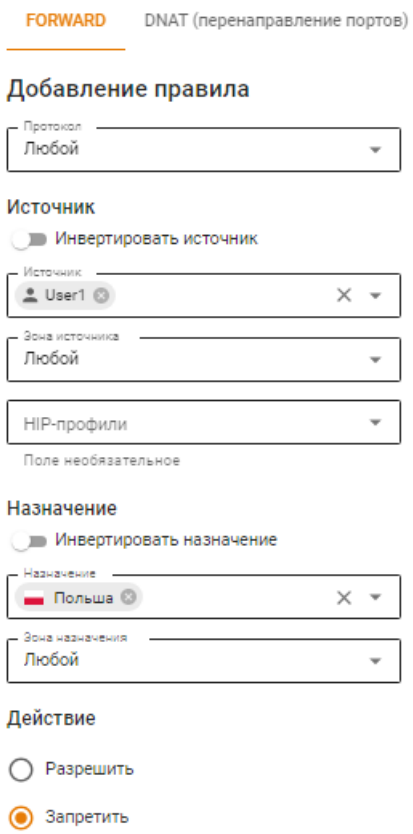
В **Правила трафика -> Предотвращение вторжений -> Журнал** записей о срабатывании правила **Анонимайзеры** нет. Значит, **Контроль приложений** обрабатывает трафик приоритетнее, чем система **Предотвращения вторжений**.

Подсказка: Подробнее о расшифровке передаваемых логов системы **Предотвращения вторжений** и **Контроля приложений** в статье *Syslog*.

22.39.2 Как проверить, что система Предотвращения вторжений обрабатывает трафик приоритетнее, чем Файрвол?

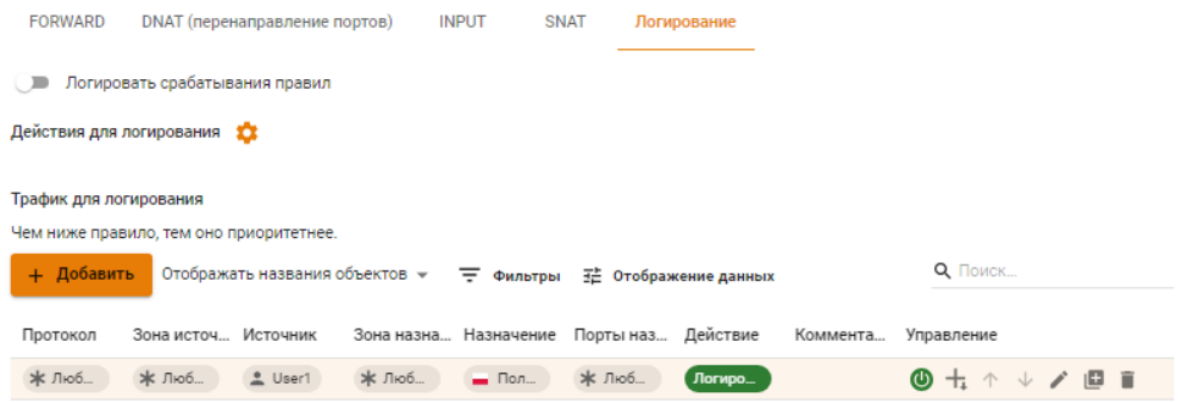
Для примера создайте GeoIP-правила для системы **Предотвращения вторжений** и **Файрвола**, блокирующие запросы к сайтам Польши.

1. В разделе **Правила трафика -> Файрвол** создайте правило, блокирующее запросы к сайтам Польши:

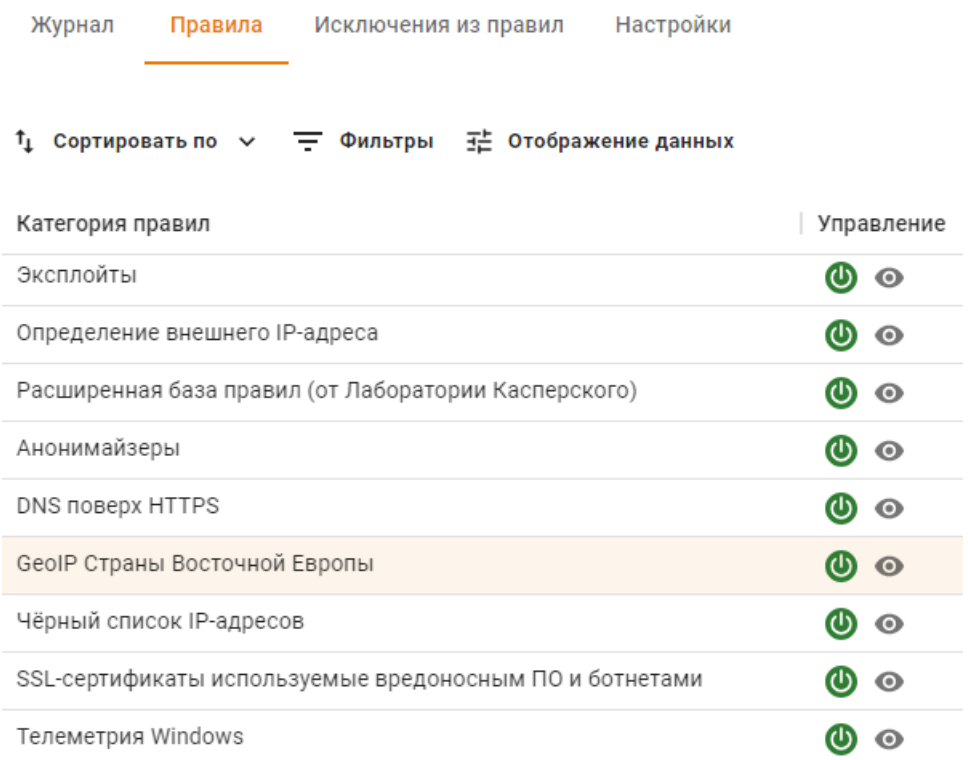


2. Переведите ползунок **Счетчик срабатываний** в **Отображении данных** в положение **Включен**, чтобы отследить, было ли срабатывание правила.

3. Перейдите на вкладку **Логирование**, создайте правило логирования:

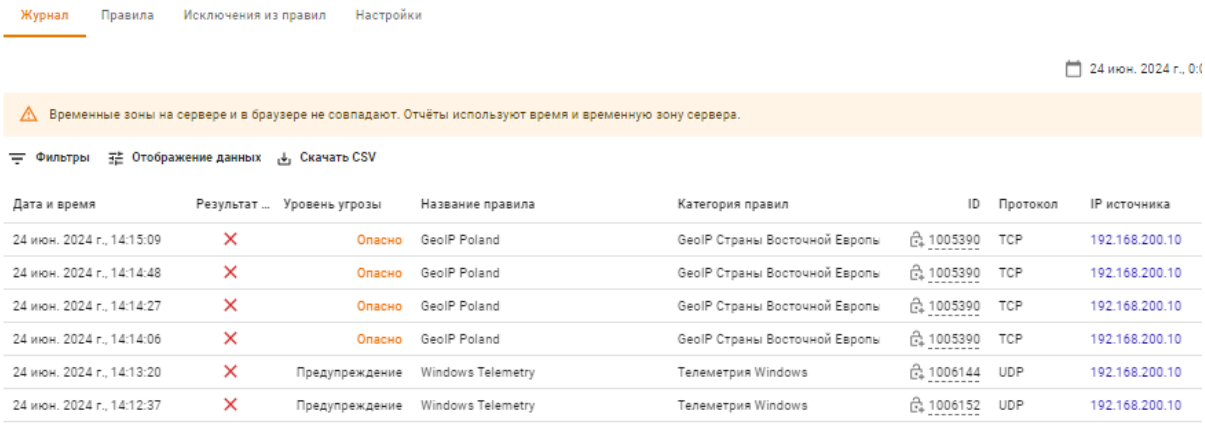


4. Проверьте, что в разделе **Предотвращения вторжений** включен блок правил блокировки стран Восточной Европы по GeoIP:



5. Авторизуйте пользователя и зайдите на любой польский сайт, например, `www.gov.pl`. Сайт не должен открыться.

6. В разделе **Правила трафика -> Предотвращение вторжений -> Журнал** появится запись о блокировке GeoIP Польши:



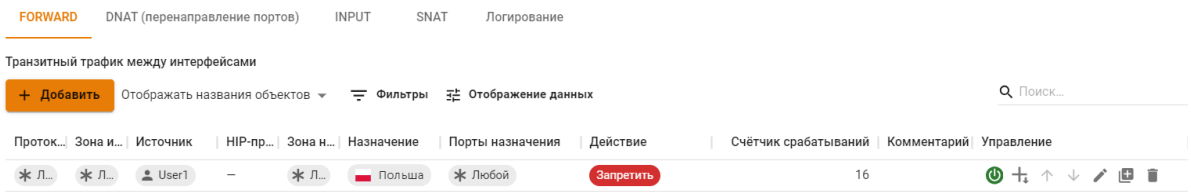
7. Перейдите в раздел **Файрвол** для просмотра счетчика срабатываний. Он должен быть равен нулю.

Если отключить систему **Предотвращения вторжений** и снова перейти на сайт `www.gov.pl`, то в логах срабатывания **Файрвола** начнут появляться записи о блокировке:

```
янв 19 17:44:13 localhost ideco-nflog[770]: TCP      src 192.168.105.3    sport 43431␣
↪dst 200.9.249.66     dport 443   table FWD  rule  4    action drop
янв 19 17:44:13 localhost ideco-nflog[770]: TCP      src 192.168.105.3    sport 35191␣
↪dst 200.9.249.66     dport 443   table FWD  rule  4    action drop
```

Информацию о том, как просмотреть логи срабатывания **Файрвола**, можно найти по *ссылке*.

Счетчик срабатываний запрещающего правила начал расти, так как трафик, будучи не заблокированным выключенной системой **Предотвращения вторжений**, пошел далее по приоритету и начал блокироваться **Файрволом**:



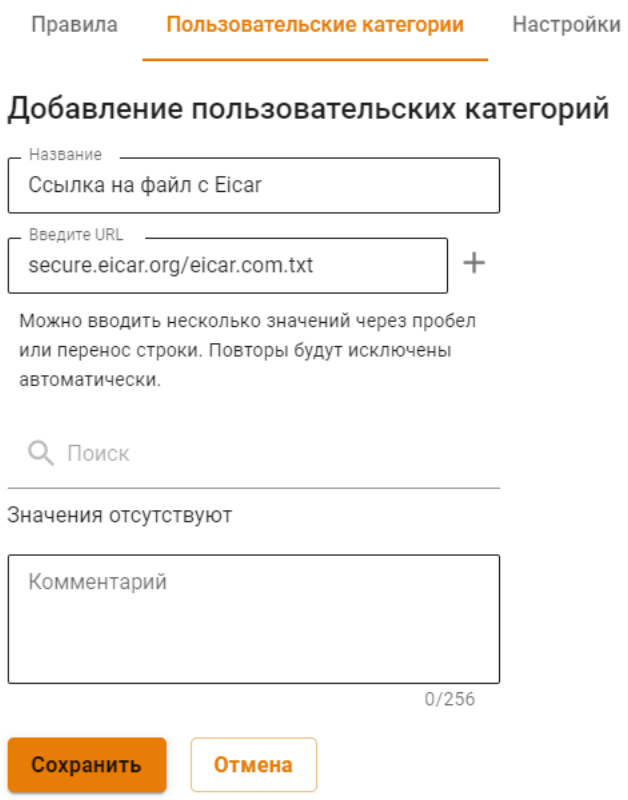
Система **Предотвращения вторжений** обрабатывает трафик приоритетнее, чем **Файрвол**.

22.39.3 Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика?

Для примера использовался тестовый файл с Eicar, доступный для скачивания по ссылке.

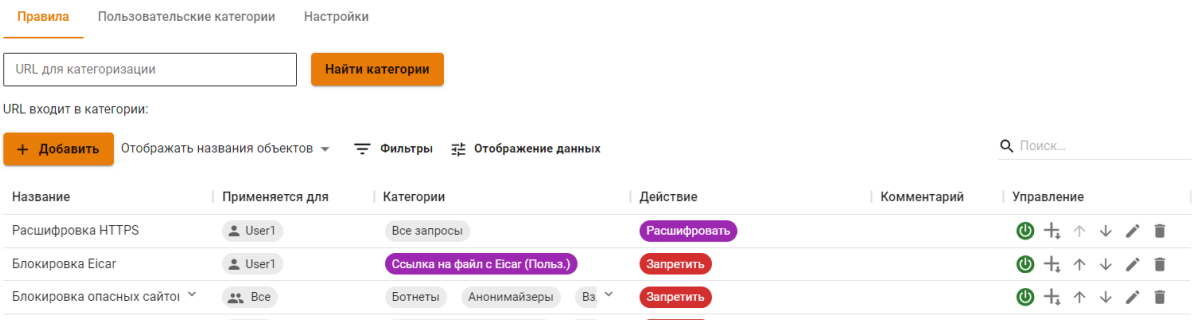
1. Перейдите в раздел **Правила трафика -> Контент фильтр -> Пользовательские категории**. Нажмите **Добавить**.

2. Введите ссылку на ресурс и нажмите + :



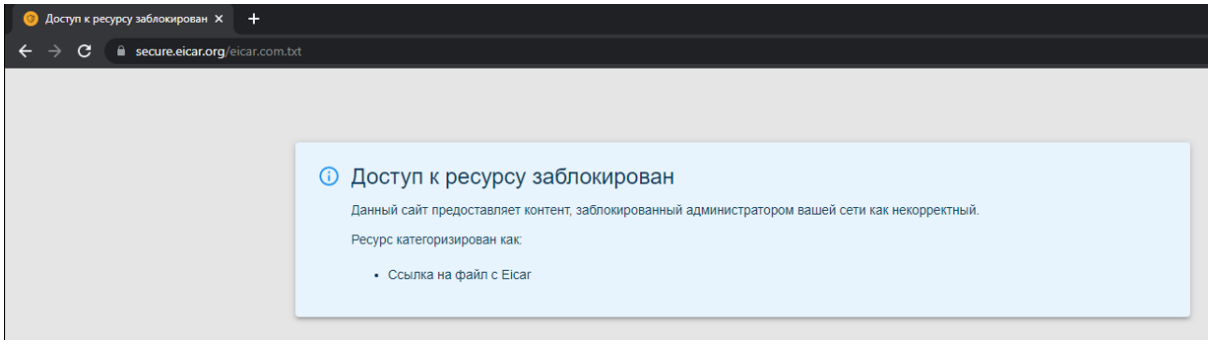
3. Перейдите на вкладку **Правила** и создайте два правила для **User1**:

- Правило расшифровки всех HTTPS-запросов, чтобы антивирус мог работать с HTTPS-трафиком;
- Правило блокировки созданной пользовательской категории:



4. Убедитесь, что опция **Антивирусы веб-трафика** 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**.

22.40 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 центральную консоль, придется вручную изменять на каждом Ideco NGFW;
- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено;

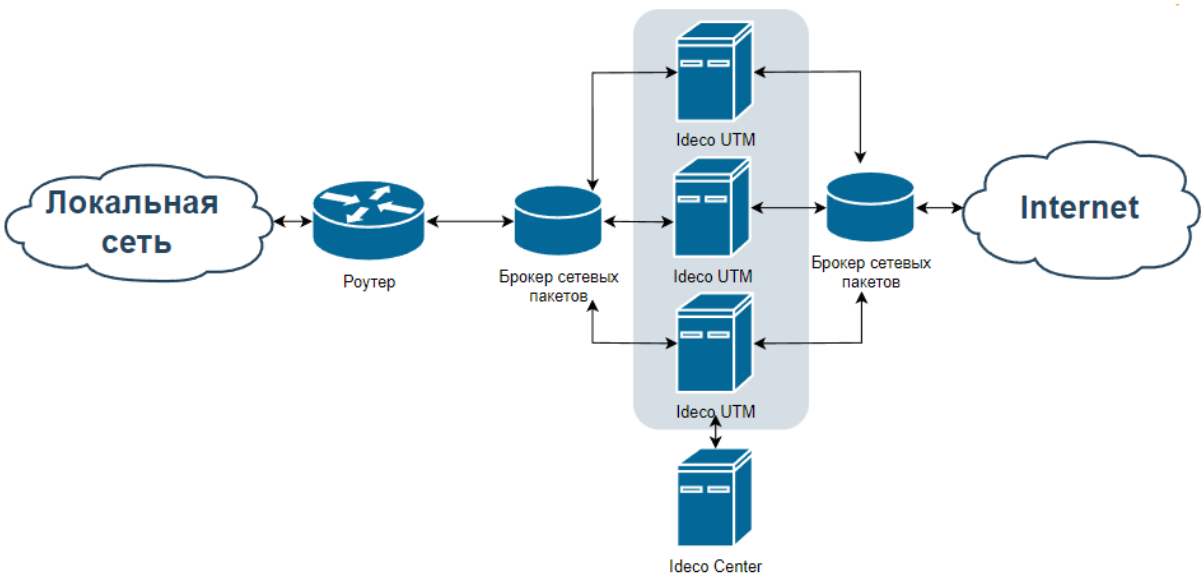
- Данные отчетности, логов и мониторинга не синхронизируются между нодами. В каждой ноде хранятся свои данные;
- Восстановление из резервной копии и обновление системы будет затрагивать только одну ноду. Каждую ноду потребуется обновлять отдельно;
- Между локальной сетью и брокером сетевых пакетов потребуется 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. Подробнее о настройке OSPF можно прочитать в соответствующей статье. 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».

22.40.1 Пример 1 - Два брокера, по одному со стороны локальной и внешней сетей



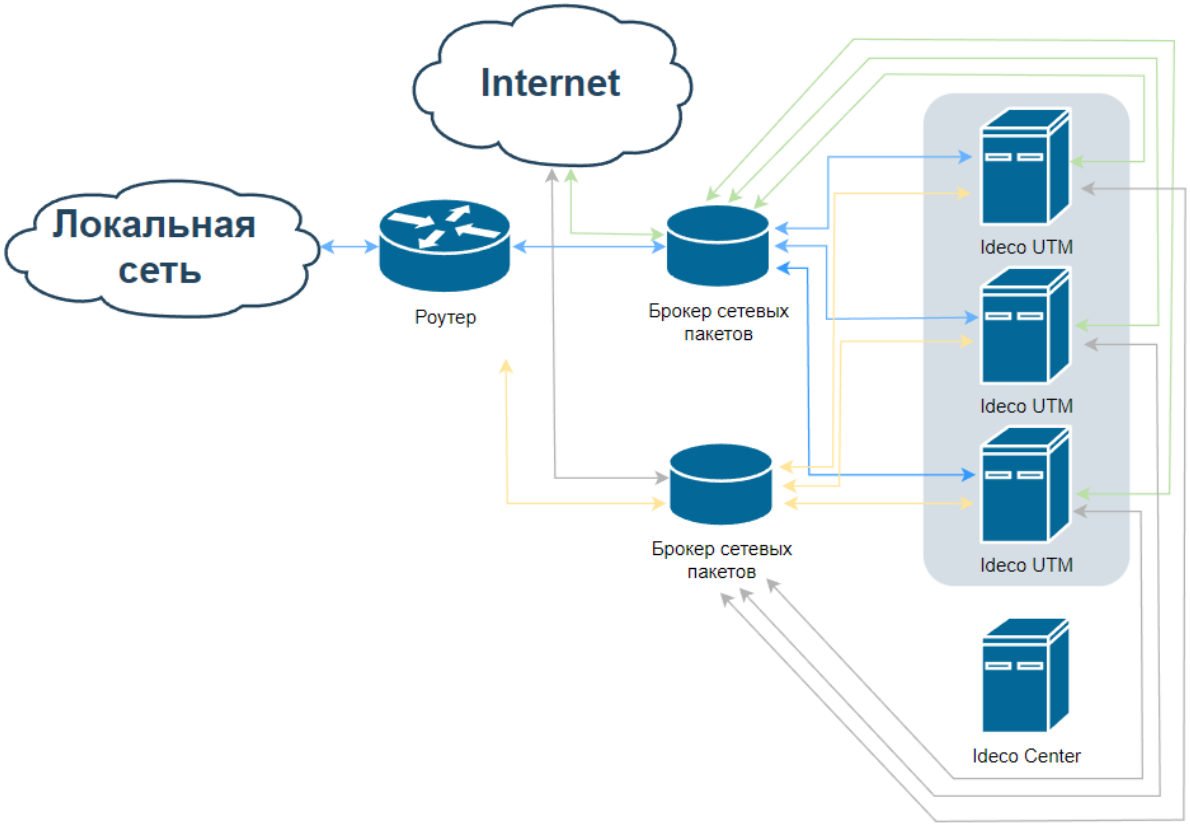
Настройка Ideco NGFW:

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.

22.40.2 Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW



Настройка Ideco NGFW

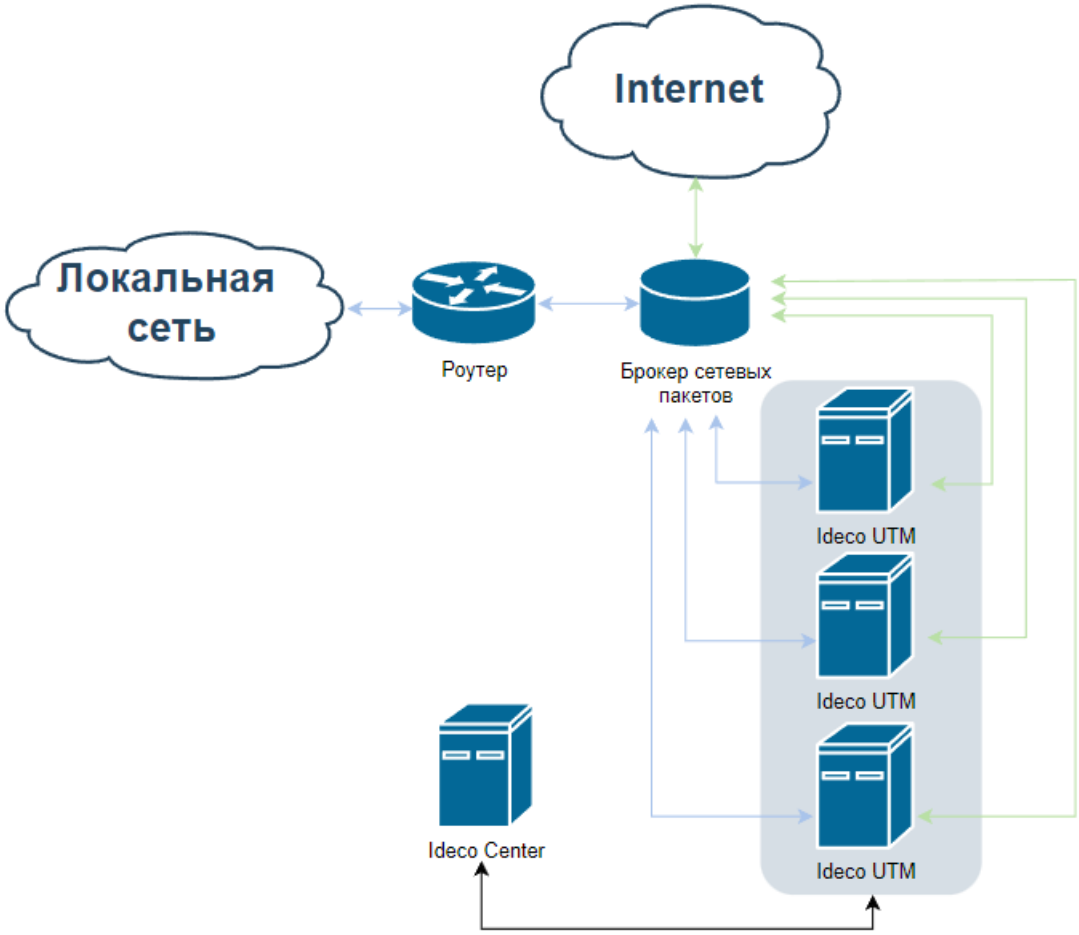
На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку *локального* и *внешнего* интерфейсов.

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.

22.40.3 Пример 3 - Один брокер, расположенный перед Ideco NGFW



Настройка Ideco NGFW

На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку *локального* и *внешнего* интерфейсов.

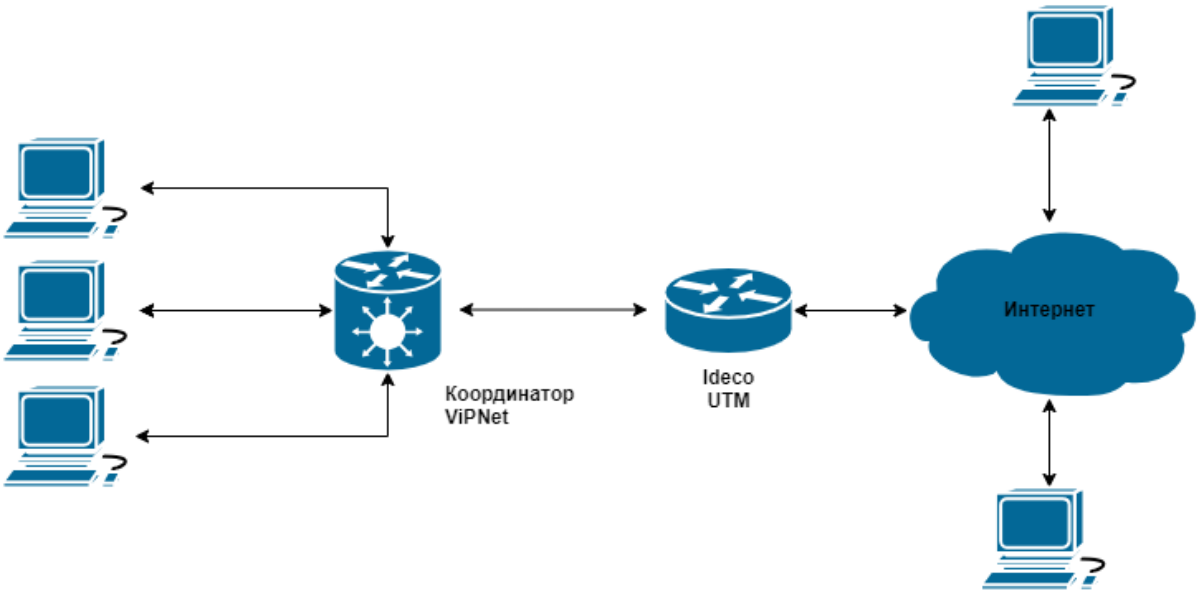
Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- 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.

22.41 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:



22.41.1 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.

22.42 Блокировка чат-ботов

22.42.1 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 правило, 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
```

(continues on next page)

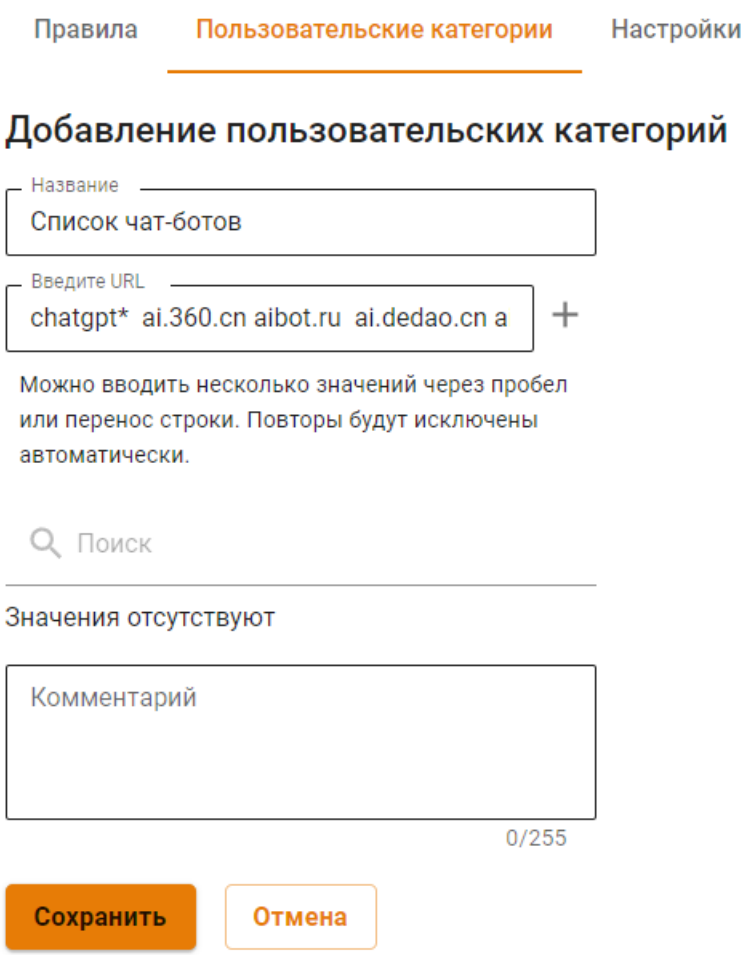
(продолжение с предыдущей страницы)

```
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
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
```

(continues on next page)

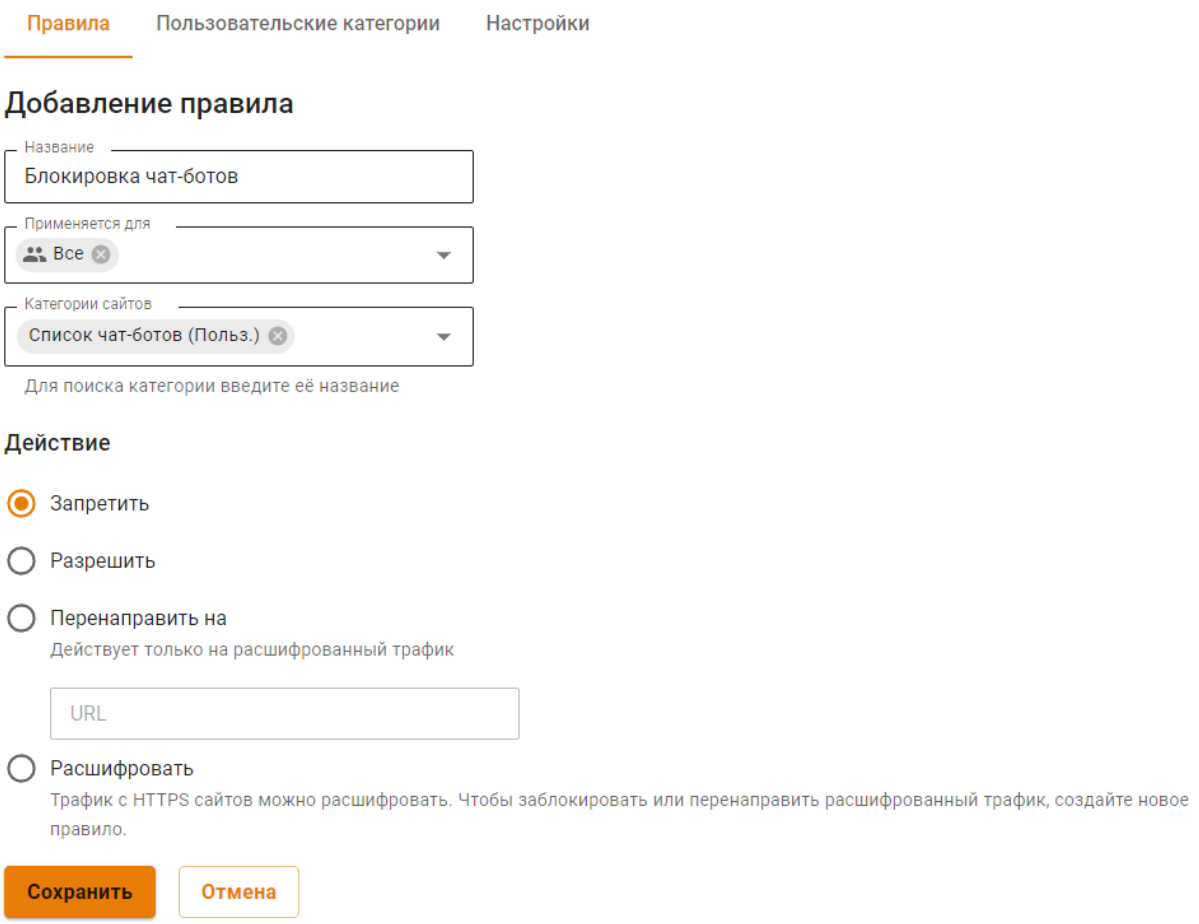
(продолжение с предыдущей страницы)

```
free.easychat.work
gpt2.ru
gpt4all.io
gpt-chatbot.ru
gptchatbot.ru
gptchatly.com
gpt-gm.h2o.ai
gptgo.ai
gpt-open.ru
gptschat.ru
gradio.app
h2o.ai
huggingface.co
iask.ai
liaobots.com
liftweb.ru
lmsys.org
macgpt.com
mashagpt.ru
moss.fastnlp.top
neice.tiangong.cn
openai.ru
openai-gpt.ru
openai-chat-gpt.ru
open-assistant.io
opencat.app
petals.ml
play.vercel.ai
poe.com
ru-chatgpt.ru
rugpt.chat
sdk.vercel.ai
supertest.lockchat.app
tenchat.ru
theb.ai
timeai.ru
tongyi.aliyun.com
tools.zmo.ai
trychatgpt.ru
wewordle.org
xinghuo.xfyun.cn
yandex-gpt.com
yandex-gpt.ru
yiyan.baidu.com
you.com
zhpt.tech
```



4. Сохраните правило.

3. Перейдите на вкладку **Правила** и добавьте правило с действием **Запретить**:



22.43 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.

22.43.1 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
SMTP(S)	25, 587 TCP
Веб-почта	443 TCP
Обратный прокси	443, 80 TCP
POP(3)	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.

22.43.2 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.

22.43.3 Как проверить, открыт ли порт

Чтобы проверить, открыт ли порт, можно воспользоваться инструментом nmap. Для этого используйте команду:

```
nmap -v 192.168.0.150
```

- 192.168.0.150 - адрес локального или внешнего интерфейса Ideco NGFW.

23. Диагностика проблем

23.1 Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

23.1.1 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:

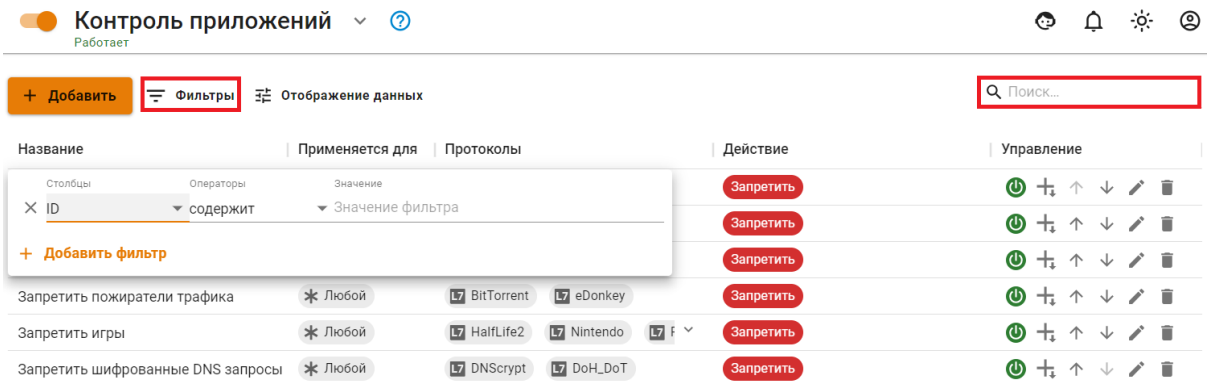
- Если не открывается, рекомендуем обратиться к провайдеру. Скорее всего, провайдер блокирует IP-адрес или адрес сайта;
- Если сайт открывается, обратитесь в техническую поддержку.

23.1.2 Шаг 2. Проверьте, не блокирует ли сайт модуль Контроль приложений

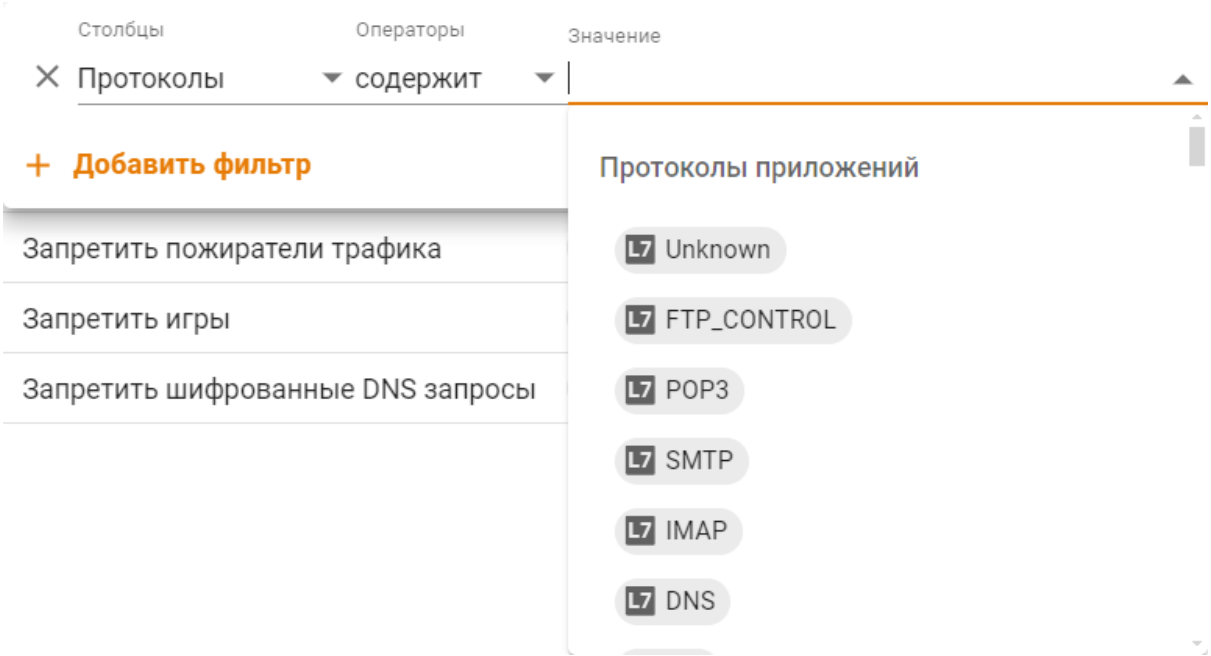
Если сайт входит в *перечень* протоколов и сервисов, доступных для создания правил **Контроля приложений**, выполните действия:

1. Перейдите в раздел **Правила трафика -> Контроль приложений**.

2. Введите название протокола или сервиса в поле **Поиск** или установите настройки фильтрации с помощью кнопки **Фильтры**:

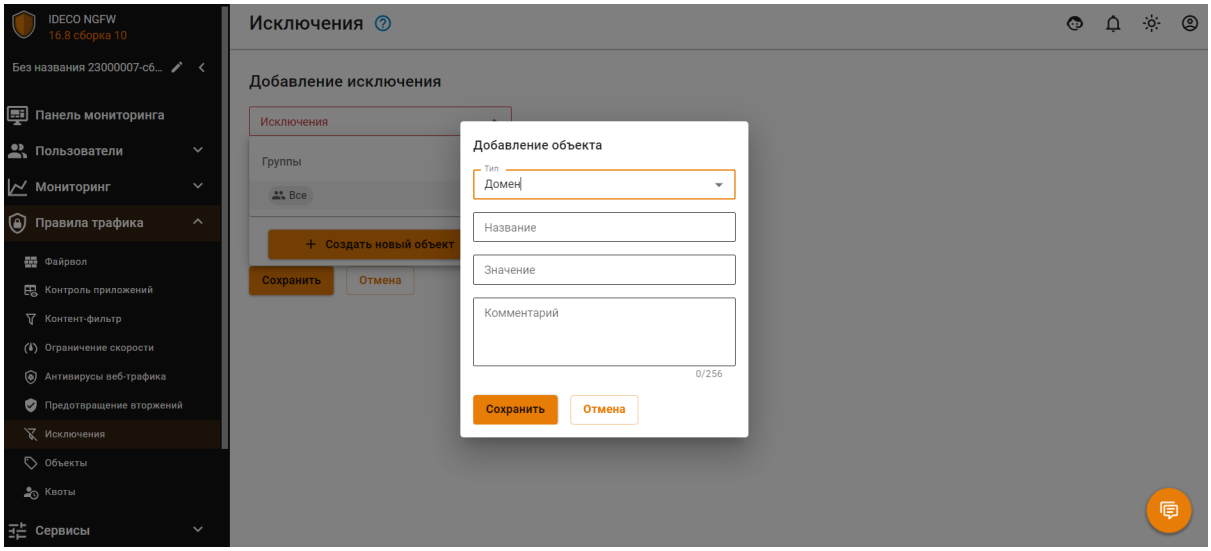


3. В настройках фильтрации выберите столбцы **Протоколы**, в поле **Значение** выберите нужный протокол приложения:



4. Проверьте, блокируют ли сайт найденные правила (действие **Запретить**).

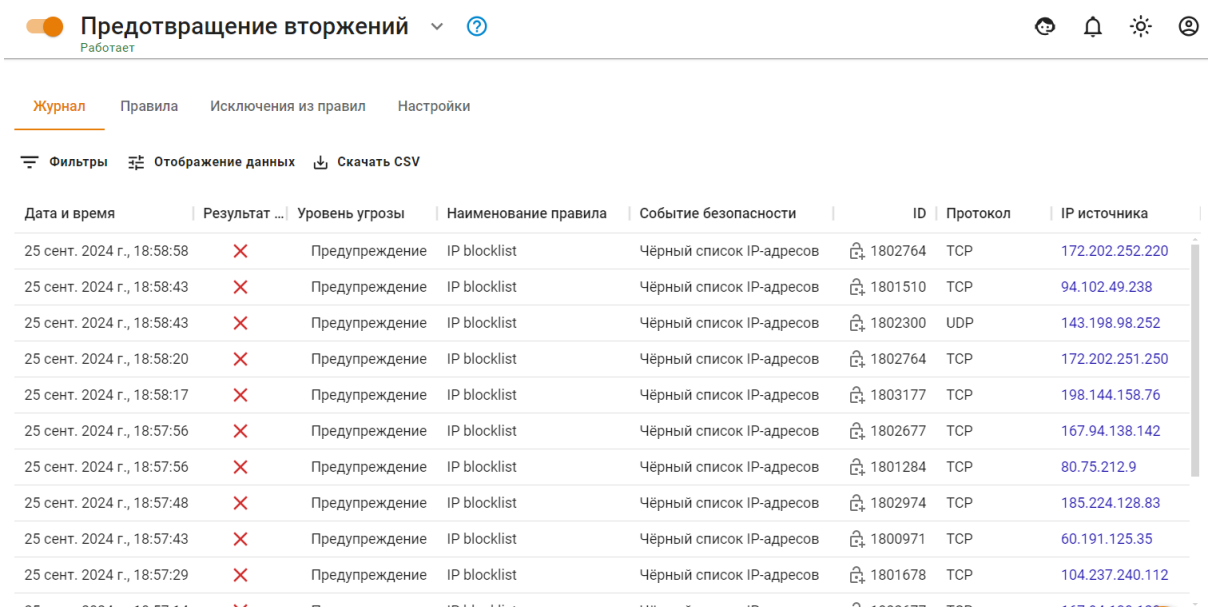
5. Если сайт блокируется правилом **Контроля приложений**, отредактируйте правило или добавьте сайт в исключения в разделе **Правила трафика -> *Исключения***:



23.1.3 Шаг 3. Проверьте, не блокирует ли сайт система Предотвращения вторжений

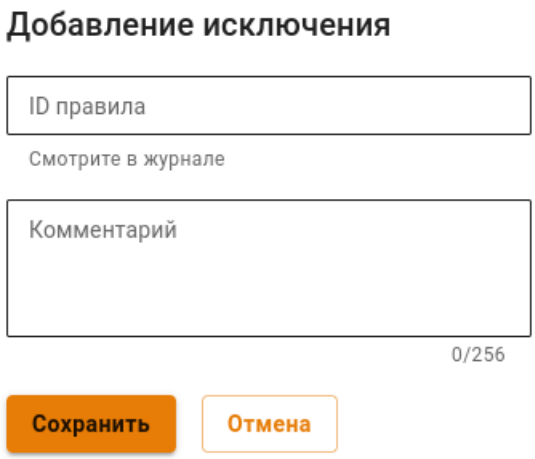
1. Повторите попытку входа на сайт с устройства пользователя.

2. Перейдите в раздел **Правила трафика -> Предотвращение вторжений -> Журнал**, найдите в логах ID блокирующего правила:



Дата и время	Результат ...	Уровень угрозы	Наименование правила	Событие безопасности	ID	Протокол	IP источника
25 сент. 2024 г., 18:58:58	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802764	TCP	172.202.252.220
25 сент. 2024 г., 18:58:43	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801510	TCP	94.102.49.238
25 сент. 2024 г., 18:58:43	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802300	UDP	143.198.98.252
25 сент. 2024 г., 18:58:20	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802764	TCP	172.202.251.250
25 сент. 2024 г., 18:58:17	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1803177	TCP	198.144.158.76
25 сент. 2024 г., 18:57:56	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802677	TCP	167.94.138.142
25 сент. 2024 г., 18:57:56	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801284	TCP	80.75.212.9
25 сент. 2024 г., 18:57:48	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802974	TCP	185.224.128.83
25 сент. 2024 г., 18:57:43	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800971	TCP	60.191.125.35
25 сент. 2024 г., 18:57:29	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801678	TCP	104.237.240.112

3. Если сайт блокируется системой **Предотвращения вторжений**, добавьте блокирующее правило в исключения. Для этого нажмите  в столбце ID или добавьте правило на вкладке **Исключения из правил**:

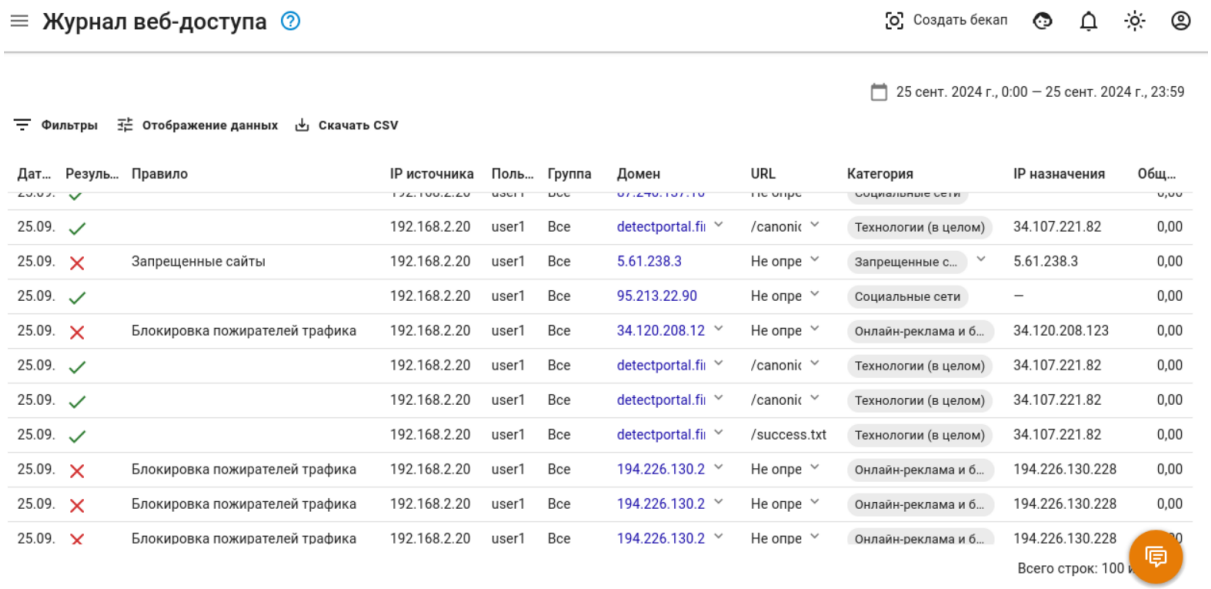


Также можно добавить IP-адрес сайта в исключения по *инструкции*.

23.1.4 Шаг 4. Проверьте, не блокируется ли сайт правилом Контент-фильтра

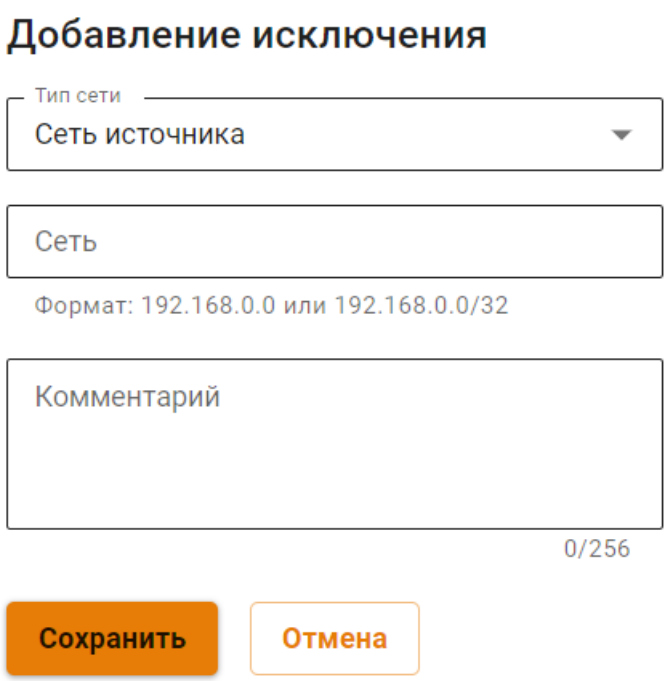
1. Откройте сайт с устройства пользователя.

2. В NGFW перейдите в раздел **Отчеты и журналы -> Журнал веб-доступа** 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.

23.1.5 Шаг 5. 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 мышки. Обратите внимание на коды состояния 4xx и 5xx. Часто именно эти запросы блокируются NGFW.

23.1.6 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.

23.2 Что делать если не работает интернет

23.2.1 Шаг 1. Проверить параметры пользователя

Убедитесь, что проверяемый пользователь авторизован на сервере. Возможные состояния пользователя описаны в главе *Дерево пользователей*.

23.2.2 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`.

- Если адрес `8.8.8.8` отвечает на эхо-запросы, проверяем `ping ya.ru`;
- Если адрес `8.8.8.8` не отвечает на эхо-запросы, перейдите к Шагу 3;
- Если адрес `ya.ru` отвечает на эхо-запросы, перейдите к Шагу 5;
- 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**.

23.2.3 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:

- Проверьте настройки сервера, адреса и маски интерфейсов;
- 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);
- 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.

23.2.4 Шаг 4. Проверка файрвола

- Отключите модуль **Файрвол** в разделе веб-интерфейса **Правила трафика -> Файрвол**. Если веб-интерфейс недоступен, то файрвол можно выключить с помощью локального меню;
- Если доступ к интернету появился, найти правило, запрещающее доступ к сети, в файрволе, поочередно включая правила;
- Если ничего не помогло, перейдите к Шагу 6.

23.2.5 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:

- Проверьте, что в браузере отсутствуют все настройки прокси;
- Выключите временно файрвол Windows и антивирусное ПО;
- Если ничего не помогло, перейдите к Шагу 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.

23.3 Ошибка при авторизации «The browser is outdated»

23.3.1 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**.

23.4 Если соединение по IPsec не устанавливается

23.4.1 Основное

1) Перезагрузите сервисы на стороне головного офиса и филиала, 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.

24. Описание хендлеров

Авторизация:

```
POST /web/auth/login
```

Json-тело запроса:

```
{
    "login": "string",
    "password": "string",
    "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/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
```

Получение информации о лицензии:

```
GET /license
```

Пример ответа на успешный запрос:


```
{
    "modules": {
        "active_directory": {
            "available": true,
            "expiration_date": 1713084779.0
        },
        "kaspersky_av_for_web": {
            "available": true,
            "expiration_date": 1713084779.0
        },
        "kaspersky_av_for_mail": {
            "available": true,
            "expiration_date": 1713084779.0
        },
        "application_control": {
            "available": true,
            "expiration_date": 1713084779.0
        },
        "suricata": {
            "available": true,
            "expiration_date": 1713084779.0
        },
        "advanced_content_filter": {
            "available": true,
            "expiration_date": 1713084779.0
        },
        "standard_content_filter": {
            "available": false,
            "expiration_date": 0
        },
        "ips_advanced_rules": {
            "available": true,
            "expiration_date": 1713084779.0
        },
        "icsd": {
            "available": true,
            "max_users_count": 10000
        }
    },
    "general": {
        "available": true,
        "reason": "",
        "not_upgrade_after": 1713084779.0,
        "tech_support_end": 1713084779.0,
        "start_date": 1709628779.7338443,
        "expiration_date": 1713084779.0
    },
    "license_type": "enterprise-demo",
    "license_id": "UTM-1098592203",
    "server_name": "UTM",
    "last_update_time": 1709628781.5150864,
    "company_id": "Ideco",
    "server_id": "CI-GYYWDwzjGBZ8by3drEAwdYMLIVWTa9RD-AsMGk63h",
```


(continues on next page)

(продолжение с предыдущей страницы)

```
    "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"
}
```

Сбор анонимной статистики о работе сервера:

24.1 Получение текущих настроек:

```
GET /gather_stat
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - если `true`, то сбор анонимной статистики о работе сервера включен, `false` - выключен.

24.2 Изменение настроек

```
PUT /gather_stat
```

Json-тело запроса

```
{
    "enabled": "boolean"
}
```

Ответ на успешный запрос: 200 OK

24.3 Управление объектами

Создание объекта IP-адрес:

```
POST /aliases/ip_addresses
```

Json-тело запроса:

```
{
    "comment": "string",
    "title": "string",
    "value": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `value` - IP-адрес.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта IP-адрес.

Создание объекта Список IP-адресов:

```
POST /aliases/ip_address_lists
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - список IP-адресов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Список IP-адресов.

Создание объекта Диапазон IP-адресов:

```
POST /aliases/ip_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "string",
    "end": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `start` - первый IP-адрес диапазона;
- `end` - последний IP-адрес диапазона.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Диапазон IP-адресов.

Создание объекта Список IP-объектов:

```
POST /aliases/lists/addresses
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - идентификаторы IP-объектов через запятую.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Список IP-объектов.

Создание объекта Подсеть:

```
POST /aliases/networks
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, 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` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `value` - домен.

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` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `value` - номер порта.

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` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `start` - первый порт диапазона;

- `end` - последний порт диапазона.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Диапазон портов.

Создание объекта Порты:

```
POST /aliases/lists/ports
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - список портов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Порты.

Создание объекта Время:

```
POST /aliases/time_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "weekdays": [ "integer" ],
    "start": "string",
    "end": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, 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`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Время.

Создание объекта Расписание:

```
POST /aliases/lists/times
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - список идентификаторов объектов Время.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Расписание.

Получение идентификаторов объектов:

```
GET /aliases
```

Ответ на успешный запрос:

```
[
    {
        "comment": "string",
        "title": "string",
        "type": "string",
        "values": [
            "string" | "integer",
            "string" | "integer",
        ],
        "id": "type.id.1"
    },
{
        "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` - все IPsec-интерфейсы;
- `interface.local_any` - все локальные интерфейсы;
- `interface.utm_outgoing` - исходящий трафик устройства;
- `interface.vpn_traffic` - клиентский VPN трафик;
- `group.id.` - идентификатор группы пользователей;
- `interface.id.` - идентификатор конкретного интерфейса;
- `security_group.guid.` - идентификатор группы безопасности AD;
- `user.id.` - идентификатор пользователя;
- `domain.id.` - идентификатор домена;
- `ip.id.` - идентификатор IP-адреса;
- `iplist.` - идентификатор объекта *GeoIP (Страна)*;
- `list_of_iplists.id.` - идентификатор объекта *Список стран*;
- `ip_range.id.` - идентификатор объекта *Диапазон IP-адресов*;
- `ip_address_list.id.` - идентификатор объекта *Список IP-адресов*;
- `address_list.id.` - идентификатор объекта *Список IP-объектов*;
- `port_list.id.` - идентификатор объекта *Список портов*;
- `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*;
- `zero_subnet` - сеть `0.0.0.0/0`.

Редактирование объекта IP-адрес:

```
PUT /aliases/ip_addresses/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;

- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `value` - IP-адрес.

Ответ на успешный запрос: 200 OK

Редактирование объекта Список IP-адресов:

```
PUT /aliases/ip_address_lists/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - список IP-адресов.

Ответ на успешный запрос: 200 OK

Редактирование объекта Диапазон IP-адресов:

```
PUT /aliases/ip_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "string",
    "end": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `start` - первый IP-адрес диапазона;
- `end` - последний IP-адрес диапазона.

Ответ на успешный запрос: 200 OK

Редактирование объекта Список IP-объектов:

```
PUT /aliases/lists/addresses/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - идентификаторы IP-объектов через запятую.

Ответ на успешный запрос: 200 OK

Редактирование объекта Подсеть:

```
PUT /aliases/networks/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, 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

Редактирование объекта Домен:

```
PUT /aliases/domains/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `value` - домен.

Ответ на успешный запрос: 200 OK

Редактирование объекта Порт:

```
PUT /aliases/ports/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "integer"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `value` - номер порта.

Ответ на успешный запрос: 200 OK

Редактирование объекта Диапазон портов:

```
PUT /aliases/port_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "integer",
    "end": "integer"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `start` - первый порт диапазона;
- `end` - последний порт диапазона.

Ответ на успешный запрос: 200 OK

Редактирование объекта Порты:

```
PUT /aliases/lists/ports/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - список портов.

Ответ на успешный запрос: 200 OK

Редактирование 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" } | "null"
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, 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`;
- `period` - срок действия. Может быть `null`, если бессрочно.

Ответ на успешный запрос: 200 OK

Редактирование объекта Расписание:

```
PUT /aliases/lists/times/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - заголовок, максимальная длина - 42 символа;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `values` - список идентификаторов объектов Время.

Ответ на успешный запрос: 200 OK

24.4 Пользовательские категории Контент-фильтра

Создание пользовательской категории:

```
POST /content-filter/users_categories
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название пользовательской категории;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `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.

Получение пользовательских категорий:

```
GET /content-filter/users_categories
```

Json-ответ на запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "comment": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "urls": [ "string" ]
    },
    ...
]
```

- `id` - номер категории в формате `users.id.1`;
- `name` - название категории, не пустая строка;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

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, максимальная длина - 255 символов;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string",
    "name": "string",
    "description": "string",
    "urls": [ "string" ]
}
```

- `id` - идентификатор пользовательской категории;
- `description` - описание пользовательской категории.

24.5 Обнаружение устройств

Получение настроек:

```
GET /netscan_backend
```

Ответ на успешный запрос:

```
{
   "enabled": "boolean",
   "group_id": "integer",
   "networks": [ "string" ]
}
```

- `enabled` - статус: `true` - включен, `false` - выключен;

- `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
```

Json-тело запроса:

```
{
   "enabled": "boolean",
   "group_id": "integer",
   "networks": [ "string" ]
}
```

- `enabled` - статус: `true` - включен, `false` - выключен;
- `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

24.6 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.

25. Примеры использования

25.1 Редактирование пользовательской категории контент-фильтра

25.1.1 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.

Подсказка: 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 -c /tmp/cookie -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 -c /tmp/cookie -b /tmp/cookie -X PUT https://x.x.x.x:8443/content-filter/
↪users_categories/users.id.3 --data '{"name": "Запрещенные для бухгалтеров", "comment
↪": "комментарий", "urls": ["https://yandex.ru", "https://wrong-url.com"]}'
```

Ответ на успешный запрос: 200 OK

> **Внимание:** 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).

Результат: Правило **Контент-фильтра**, которое использует эту пользовательскую категорию, будет запрещать пользователям переходить на сайты `https://yandex.ru` и `https://wrong-url.com/`

25.2 Создание правила Forward

25.2.1 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).

Подсказка: 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 -c /tmp/cookie -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 -c /tmp/cookie -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 -c /tmp/cookie -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 -c /tmp/cookie -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"}'
```

Ответ на успешный запрос:

```
{
    "id": "time_range.id.3"
}
```

5. Создайте правило файрвола, используя *id* из пунктов 2 и 3:

```
curl -k -c /tmp/cookie -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, "incoming_interface": "any", "outgoing_interface": "any", "protocol
↪": "protocol.tcp", "source_addresses": ["address_list.id.3"], "source_addresses_
↪negate": false, "timetable": ["any"]}'
```

Значение `action`:

- accept - принять пакет;
- drop - отклонить пакет.

Ответ на успешный запрос:

```
{
    "id": 2
}
```

6. Отредактируйте созданное правило, указав время действия:

```
curl -k -c /tmp/cookie -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, "incoming_interface": "any",
↪"outgoing_interface": "any", "protocol": "protocol.tcp", "source_addresses": [
↪"address_list.id.3"], "source_addresses_negate": false, "timetable": ["time_range.
↪id.3"]}'
```

Ответ на успешный запрос: 200 OK