Пользовательская документация

Ideco NGFW

апр. 24, 2025

Оглавление

1 Возможности Ideco NGFW: 1

2 Лицензирование 1
- 2.1 Виды лицензий . . . 2
  - 2.1.1 По истечении срока подписки **Security Update** доступ к большинству функций Ideco NGFW сохраняется. Исключением являются: . . . 3
  - 2.1.2 Просмотр информации о лицензиях . . . 3

3 Системные требования и источники обновления данных Ideco NGFW 4
- 3.1 Минимальные системные требования . . . 4
- 3.2 Примеры конфигураций . . . 5
- 3.3 Источники обновлений данных . . . 5
- 3.4 Программно-аппаратный комплекс (ПАК) . . . 6
- 3.5 Выбор аппаратной платформы для Ideco NGFW . . . 6
  - 3.5.1 Сведения о программной платформе . . . 6
  - 3.5.2 Общие рекомендации по чипсетам и производителям . . . 6
  - 3.5.3 Подбор мощности аппаратной платформы . . . 6
  - 3.5.4 Дисковая подсистема . . . 7

4 Техническая поддержка 7
- 4.1 График работы . . . 7
- 4.2 Способы обращения . . . 7
- 4.3 Правила обращения . . . 8
- 4.4 Информация о поддержке версий Ideco NGFW . . . 8
  - 4.4.1 Уровни поддержки . . . 8
  - 4.4.2 Сроки поддержки . . . 9

5 Рекомендации при первоначальной настройке 10
- 5.1 Основное . . . 10

6 MY.IDECO.RU 10
- 6.1 Регистрация на my.ideco . . . 10
- 6.2 Загрузка образа Ideco NGFW . . . 13

7 Настройка программно-аппаратных комплексов Ideco NGFW 13
- 7.1 Описание панелей программно-аппаратных комплексов Ideco NGFW . . . 13
- 7.2 Настройка IPMI . . . 17
- 7.3 Настройка ПАК Ideco NGFW SX+ . . . 20

8 Подготовка к установке на устройство 21
- 8.1 Основное . . . 21
- 8.2 Настройка гипервизора . . . 21
  - 8.2.1 Общие рекомендации . . . 21
  - 8.2.2 Microsoft Hyper-V . . . 22
  - 8.2.3 VMware ESXi 6.7 . . . 22
  - 8.2.4 VMware Workstation 17.0 . . . 25
  - 8.2.5 Citrix XenServer . . . 33
  - 8.2.6 VirtualBox 7.0.12 . . . 33
  - 8.2.7 KVM . . . 34
  - 8.2.8 Proxmox . . . 36
- 8.3 Подготовка загрузочного диска . . . 45
  - 8.3.1 В среде Windows . . . 46
  - 8.3.2 В среде Linux . . . 47

9 Установка **48**
9.1 Процесс установки . . . 48
9.2 Создание учетной записи администратора . . . 49
9.3 Настройка второй ноды кластера . . . 50
9.4 Настройка локального интерфейса . . . 50

10 Первоначальная настройка **52**
10.1 Подключение к веб-интерфейсу Ideco NGFW . . . 52
10.2 Импорт корневого сертификата NGFW в браузер . . . 53
10.3 Настройка **Ethernet-подключения** . . . 55
10.3.1 Настройка других типов подключений . . . 57

11 Регистрация сервера **57**
11.1 Онлайн-регистрация . . . 57
11.2 Офлайн-регистрация . . . 58
11.2.1 Привяжите сервер к личному кабинету в MY.IDECO. Для этого: . . . 58
11.2.2 Привяжите к серверу лицензию: . . . 58
11.3 Офлайн-обновление баз модулей безопасности . . . 60

12 Получение доступа в интернет **60**
12.1 Основное . . . 60

13 Панель мониторинга **61**
13.1 Особенности отображения информации: . . . 62

14 Пользователи **62**
14.1 Учетные записи . . . 62
14.1.1 Основное . . . 62
14.1.2 Управление пользователями . . . 63
14.1.3 Настройка пользователей . . . 66
14.2 Авторизация пользователей . . . 71
14.2.1 Общая информация . . . 72
14.2.2 Веб-аутентификация . . . 73
14.2.3 IP и MAC авторизация . . . 75
14.2.4 Авторизация по подсетям . . . 81
14.2.5 Авторизация пользователей терминальных серверов . . . 83
14.3 Личный кабинет пользователя . . . 89
14.3.1 Настройка доступа в личный кабинет . . . 89
14.3.2 Публикация Личного кабинета . . . 90
14.3.3 Возможности личного кабинета Ideco NGFW . . . 90
14.4 VPN-подключение . . . 92
14.4.1 Основное . . . 93
14.4.2 Доступ по VPN . . . 96
14.4.3 Правила выдачи IP-адресов . . . 98
14.4.4 Двухфакторная аутентификация . . . 100
14.4.5 Подключение по PPTP . . . 107
14.4.6 Подключение по PPPoE . . . 110
14.4.7 Подключение по IKEv2/IPsec . . . 111
14.4.8 Подключение по SSTP . . . 115
14.4.9 Подключение по L2TP/IPsec . . . 117
14.4.10 Особенности маршрутизации и организации доступа . . . 119
14.4.11 Инструкция по запуску PowerShell скриптов . . . 123
14.5 Ideco Client . . . 133
14.5.1 Особенности работы Ideco Client . . . 133
14.5.2 Установка и настройка Ideco Client на Windows . . . 134
14.5.3 Установка и настройка Ideco Client на MacOS . . . 137
14.6 Профили устройств . . . 144
14.6.1 HIP-объекты . . . 145
14.6.2 HIP-профили . . . 146

14.6.3 Примеры использования . . . 148
14.7 Интеграция с Active Directory/Samba DC . . . 153
14.7.1 Поддерживаемые контроллеры домена: . . . 153
14.7.2 Особенности использования интеграции с несколькими контроллерами домена . . . 153
14.7.3 Настройка учетных записей и групп безопасности в качестве объектов правил фильтрации . . . 154
14.7.4 Ввод сервера в домен . . . 155
14.7.5 Аутентификация пользователей AD/Samba DC . . . 158
14.7.6 Скрипты автоматической разавторизации . . . 169
14.7.7 Импорт пользователей . . . 176
14.8 Интеграция с RADIUS-сервером . . . 181
14.8.1 Настройка интеграции . . . 181
14.8.2 Механизм добавления пользователей в дерево Ideco NFGW . . . 182
14.9 ALD Pro . . . 183
14.9.1 Ввод сервера в домен . . . 183
14.9.2 Импорт пользователей . . . 184
14.9.3 Аутентификация пользователей . . . 185
14.10 Обнаружение устройств . . . 186
14.10.1 Основное . . . 186
14.11 Wi-Fi-сети . . . 187
14.11.1 Настройка DHCP: . . . 188
14.11.2 Настройка DHCP: . . . 189

15 Мониторинг **190**
15.1 Авторизованные пользователи . . . 190
15.1.1 Основное . . . 190
15.2 График загруженности . . . 191
15.2.1 Ядро . . . 191
15.2.2 Сеть . . . 192
15.2.3 Диски . . . 192
15.2.4 VPN . . . 192
15.2.5 IPsec . . . 192
15.2.6 WCCP GRE . . . 192
15.3 Монитор трафика . . . 193
15.3.1 По узлам локальной сети . . . 193
15.3.2 По приложениям . . . 194
15.4 Telegram-бот . . . 194
15.4.1 Привязка Ideco Monitoring Bot . . . 195
15.4.2 Настройка оповещений Ideco Monitoring Bot . . . 196
15.5 SNMP . . . 196
15.5.1 Основное . . . 196
15.6 Zabbix-агент . . . 198
15.6.1 Настройка Zabbix-агента . . . 198
15.6.2 Полезные ссылки . . . 200

16 Правила трафика **200**
16.1 Файрвол . . . 200
16.1.1 Принцип работы . . . 200
16.1.2 Настройка и управление правилами . . . 201
16.1.3 Ограничения и особенности . . . 201
16.1.4 Счетчик срабатываний . . . 202
16.1.5 Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT) . . . 202
16.1.6 Логирование . . . 206
16.2 Контроль приложений . . . 209
16.2.1 Создание правил . . . 210
16.3 Контент-фильтр . . . 233
16.3.1 Правила . . . 233
16.3.2 Пользовательские категории . . . 234

16.3.3 Настройки . . . 236
16.3.4 Применение правил . . . 237
16.3.5 Описание категорий Контент-фильтра . . . 240
16.3.6 Настройка фильтрации HTTPS . . . 248
16.4 Ограничение скорости . . . 254
16.4.1 Настройка ограничения скорости . . . 255
16.4.2 Порядок применения правил . . . 257
16.4.3 Особенности . . . 257
16.5 Антивирусы веб-трафика . . . 257
16.5.1 Основное . . . 257
16.6 Предотвращение вторжений . . . 259
16.6.1 Примеры использования . . . 259
16.6.2 Журнал . . . 261
16.6.3 Правила . . . 264
16.6.4 Исключения из правил . . . 268
16.6.5 Настройки . . . 268
16.7 Исключения . . . 269
16.7.1 Основное . . . 269
16.8 Объекты . . . 269
16.8.1 Создание объектов . . . 270
16.9 Квоты . . . 271
16.9.1 Настройка квоты . . . 272
16.9.2 Настройка пользователя и группы . . . 273

17 Профили безопасности **274**
17.1 Что позволят делать профили . . . 275
17.2 Контроль приложений . . . 275
17.2.1 Что изменится с появлением профилей контроля приложений . . . 275
17.2.2 Почему мы отказались от автоматической миграции . . . 276
17.2.3 Особенности создания профилей . . . 276
17.2.4 Пример создания иерархической структуры . . . 280
17.2.5 Настройка фильтрации трафика, для которого в таблице FORWARD нет правил . . . 289

18 Сервисы **291**
18.1 Сетевые интерфейсы . . . 291
18.1.1 Агрегированные интерфейсы . . . 293
18.1.2 Туннельные интерфейсы . . . 294
18.1.3 VCE-интерфейсы . . . 294
18.1.4 Настройка Локального Ethernet . . . 296
18.1.5 Настройка Внешнего Ethernet . . . 298
18.1.6 Настройка подключения по PPTP . . . 301
18.1.7 Настройка подключения по L2TP . . . 302
18.1.8 Настройка подключения по PPPoE . . . 304
18.1.9 Подключение по 3G и 4G . . . 306
18.2 Балансировка и резервирование . . . 306
18.2.1 Основное . . . 307
18.2.2 Адреса для проверки связи . . . 309
18.3 Маршрутизация . . . 310
18.3.1 Маршрутизация локальных сетей . . . 310
18.3.2 Маршрутизация внешних сетей . . . 311
18.4 BGP . . . 315
18.4.1 Настройка своей автономной системы . . . 316
18.4.2 Настройка BGP-соседей . . . 316
18.5 OSPF . . . 318
18.5.1 Особенности работы OSPF в Ideco NGFW . . . 322
18.5.2 Основное . . . 322
18.5.3 Дополнительное . . . 325
18.5.4 Примеры использования . . . 326

18.6 IGMP Proxy . . . 327
18.6.1 Принцип работы . . . 327
18.6.2 Настройка в Ideco NGFW . . . 329
18.7 Прокси . . . 329
18.7.1 Основное . . . 330
18.7.2 ICAP . . . 331
18.7.3 WCCP . . . 332
18.7.4 WCCP Service ID . . . 335
18.7.5 Исключения . . . 336
18.7.6 Исключения . . . 336
18.7.7 Настройка прямого подключения к прокси . . . 339
18.7.8 Настройка прокси с одним интерфейсом . . . 340
18.8 Обратный прокси . . . 342
18.8.1 Создание и настройка правила . . . 342
18.8.2 Защита от DoS-атак . . . 345
18.9 DNS . . . 345
18.9.1 Основное . . . 345
18.9.2 Внешние DNS-серверы . . . 345
18.9.3 Master-зоны . . . 347
18.9.4 Forward-зоны . . . 350
18.9.5 DDNS . . . 351
18.10 DHCP-сервер . . . 354
18.10.1 Интерфейс Ideco NGFW: . . . 354
18.10.2 Настройки . . . 355
18.10.3 Привязка IP к MAC . . . 359
18.10.4 Мониторинг аренды . . . 360
18.11 NTP-сервер . . . 361
18.11.1 Принцип работы . . . 361
18.11.2 Настройка Ideco NGFW . . . 361
18.12 IPsec . . . 361
18.12.1 Устройства . . . 362
18.12.2 Исходящие подключения . . . 362
18.12.3 Входящие подключения . . . 363
18.12.4 Выбор алгоритмов шифрования на удаленных устройствах . . . 363
18.12.5 Изменение настроек созданных IPsec-подключений . . . 365
18.12.6 Подключение между двумя Ideco NGFW в туннельном режиме работы . . . 366
18.12.7 Подключение между двумя Ideco NGFW в транспортном режиме работы . . . 371
18.12.8 Подключение Ideco NGFW и Mikrotik . . . 376
18.12.9 Подключение MikroTik и Ideco NGFW по L2TP/IPsec . . . 398
18.12.10 Подключение Cisco IOS и Ideco NGFW . . . 398
18.12.11 Подключение pfSense к Ideco NGFW по IPsec . . . 408
18.12.12 Подключение Kerio Control и Ideco NGFW по IPsec . . . 414
18.12.13 Подключение Keenetic по SSTP или IPsec . . . 422
18.13 Сертификаты . . . 425
18.13.1 Общая информация . . . 425
18.13.2 Логика работы . . . 426
18.13.3 Загрузка SSL-сертификата на сервер . . . 428
18.13.4 Создание самоподписанного сертификата с помощью PowerShell . . . 431
18.13.5 Создание сертификата с помощью openssl . . . 432

19 Отчеты и журналы **433**
19.1 Трафик . . . 433
19.1.1 Способ отображения информации: . . . 433
19.2 Журнал событий . . . 434
19.2.1 Защита от брутфорс-атак . . . 436
19.3 Журнал веб-доступа . . . 437
19.3.1 Основное . . . 437
19.4 Журнал антивируса . . . 438

19.4.1 Основное . . . 438
19.5 События безопасности . . . 438
19.5.1 Выбор периода . . . 439
19.5.2 Графики IDS/IPS . . . 439
19.5.3 Журнал IDS/IPS . . . 440
19.5.4 Web Application Firewall . . . 441
19.6 Действия администраторов . . . 442
19.6.1 Основное . . . 442
19.7 Журнал авторизации . . . 443
19.7.1 Основное . . . 443
19.8 Конструктор отчетов . . . 445
19.8.1 Мои шаблоны . . . 445
19.8.2 Отчеты по расписанию . . . 446
19.9 Syslog . . . 448
19.9.1 Пересылка системных сообщений . . . 448
19.9.2 Расшифровка передаваемых логов . . . 449

20 Управление сервером **462**
20.1 Администраторы . . . 462
20.1.1 Управление администраторами . . . 462
20.1.2 Доступ к веб-интерфейсу из внешней сети и удаленный доступ по SSH . . . 463
20.1.3 Восстановление пароля администратора . . . 463
20.2 Центральная консоль . . . 463
20.2.1 Подключение Ideco NGFW к Ideco Center . . . 464
20.3 VCE . . . 465
20.3.1 Создание VCE . . . 466
20.3.2 Переход в веб-интерфейс VCE . . . 467
20.3.3 Удаление VCE . . . 468
20.4 Кластеризация . . . 468
20.4.1 Процесс синхронизации нод в кластере . . . 468
20.4.2 Особенности работы кластера . . . 469
20.4.3 Возможные проблемы при работе двух Ideco NGFW в кластере . . . 469
20.4.4 Настройка кластера . . . 470
20.5 Обновления . . . 478
20.5.1 Процесс выхода релизов в каналы обновлений . . . 479
20.5.2 Особенности обновления NGFW . . . 479
20.6 Бекапы . . . 480
20.6.1 Автоматическое создание бекапа . . . 480
20.6.2 Ручное создание бекапа . . . 481
20.6.3 Восстановление конфигурации из бекапа . . . 483
20.7 Терминал . . . 484
20.7.1 Основные команды . . . 485
20.7.2 Таблица служб . . . 485
20.7.3 Примеры использования утилит . . . 486
20.8 Лицензия . . . 489
20.8.1 Добавление коммерческой (Enterprise) лицензии . . . 490
20.8.2 Добавление FREE (бесплатной) лицензии . . . 490
20.8.3 Привязка лицензии к серверу . . . 490
20.8.4 Просмотр информации о лицензиях . . . 492
20.9 Дополнительно . . . 492
20.9.1 Основное . . . 492

21 Почтовый релей **493**
21.1 Основное . . . 493
21.2 Основные настройки . . . 494
21.2.1 Основное . . . 494
21.2.2 Web-почта . . . 495
21.2.3 Настройка почтового релея . . . 497

21.2.4 Настройка почтового сервера . . . 500
21.3 Расширенные настройки . . . 502
21.3.1 Основное . . . 503
21.3.2 Безопасность . . . 504
21.3.3 DKIM-подпись . . . 504
21.3.4 Настройка домена у регистратора/держателя зоны . . . 505
21.4 Антиспам . . . 507
21.4.1 Основное . . . 507
21.4.2 Настройки фильтрации . . . 508
21.5 Правила . . . 511
21.5.1 Переадресация . . . 511
21.5.2 Разрешенные адреса . . . 512
21.5.3 Запрещенные адреса . . . 513
21.5.4 Переадресация почты . . . 513
21.6 Почтовая очередь . . . 515
21.6.1 Проверка настроек почтового сервера . . . 516
21.7 Настройка почтовых клиентов . . . 516
21.7.1 Настройка почтового клиента при работе из локальной сети . . . 516
21.7.2 Настройка почтового клиента при работе из сети интернет . . . 516
21.7.3 Примеры настроек популярных почтовых клиентов . . . 517
21.8 Схема фильтрации почтового трафика . . . 522
21.8.1 Основное . . . 522

22 Публикация ресурсов **523**
22.1 Доступ из внешней сети без NAT . . . 523
22.1.1 Основное . . . 523
22.2 Публикация веб-приложений (обратный прокси-сервер) . . . 527
22.2.1 Основное . . . 527
22.3 Настройка публичного IP-адреса на компьютере в локальной сети . . . 527
22.3.1 Основное . . . 527
22.4 Портмаппинг (проброс портов, DNAT) . . . 527
22.4.1 Основное . . . 527

23 Интеграция NGFW и SkyDNS **532**
23.1 Чем может быть полезна интеграция: . . . 532
23.2 Настройка интеграции Ideco NGFW и SkyDNS . . . 532
23.3 Документация по настройке и активации сервиса SkyDNS . . . 534
23.4 Схема фильтрации веб-трафика при использовании SkyDNS . . . 535

24 О личном кабинете MY.IDECO **535**
24.1 Возможности Ideco NGFW: . . . 535

25 NGFW **536**
25.1 Лицензирование . . . 536
25.1.1 Добавление коммерческой (Enterprise) лицензии . . . 536
25.1.2 Добавление FREE (бесплатной) лицензии . . . 536
25.1.3 Привязка лицензии к серверу . . . 536
25.2 Скачать . . . 538
25.3 Online-демо . . . 538

26 Центральная консоль **538**
26.1 Полезные ссылки . . . 539

27 Monitoring Bot и Security **539**
27.1 Monitoring Bot . . . 539
27.1.1 Привязка Ideco Monitoring Bot . . . 539
27.1.2 Настройка оповещений Ideco Monitoring Bot . . . 541
27.2 Security . . . 541

28 Личные данные и Компании **541**
28.1 Личные данные . . . 542
28.2 Компании . . . 542
28.2.1 Добавление компании . . . 542
28.2.2 Добавление пользователей . . . 542

29 Об Ideco Center **542**
29.1 Основное . . . 542

30 Установка Ideco Center **543**
30.1 Процесс установки . . . 544
30.2 Создание учетной записи администратора . . . 546
30.3 Настройка локального интерфейса . . . 546

31 Серверы **548**
31.1 Переход из веб-интерфейса Ideco Center в веб-интерфейс Ideco NGFW . . . 552
31.2 Группировка серверов Ideco NGFW . . . 552
31.2.1 Создание, редактирование и удаление групп серверов . . . 552
31.2.2 Перемещение серверов Ideco NGFW между группами . . . 553

32 Мониторинг **553**
32.1 SNMP . . . 553
32.2 Zabbix-агент . . . 555

33 Политики и объекты **556**
33.1 Политики безопасности . . . 556
33.1.1 Файрвол . . . 557
33.2 Объекты . . . 558

34 Сервисы **558**
34.1 Сетевые интерфейсы . . . 558
34.2 Маршрутизация . . . 560
34.3 DNS . . . 560
34.4 Сертификаты . . . 560
34.4.1 Действующие сертификаты . . . 560
34.4.2 Загруженные сертификаты . . . 560

35 Отчеты и журналы **561**
35.1 Журнал событий . . . 561
35.2 Действия администраторов . . . 562

36 Управление сервером **562**
36.1 Администраторы . . . 562
36.2 Дополнительно . . . 563

37 FAQ **563**
37.1 Как заблокировать чат-боты? . . . 563
37.2 Как настроить совместную работу ViPNet-Координатора с Ideco NGFW ? . . . 563
37.3 Как настроить автоматическую аутентификацию на Linux через веб-интерфейс ? . . . 563
37.4 Есть ли возможность добавлять сигнатуры IPS? . . . 563
37.5 Как настроить кластеризацию Active/Active? . . . 564
37.6 Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW? . . . 564
37.7 Хочу работать из дома, подключившись по RDP к своем компьютеру в офисе. Можно ли опубликовать RDP, чтобы он был доступен из интернета? . . . 564
37.8 Как создать VPN-подключение? . . . 564
37.9 Что делать, если сети за роутером, находящимся после NGFW, не доступны по VPN? . . . 564
37.10 Что делать, если ваш IP попал в черные списки DNSBL? . . . 564
37.11 Утрачен пароль администратора, как его восстановить? . . . 565
37.12 После обновления потребовалось вернуть предыдущую версию со всеми настройками. Как это сделать? . . . 565

37.13 Как понять, что контент-фильтр настроен эффективно? . . . 565
37.14 Как подобрать аппаратную платформу для Ideco NGFW? . . . 565
37.15 Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW? . . . 565
37.16 Как настроить прямое подключение к прокси-серверу, если ПО его не поддерживает? . . . 565
37.17 Как эффективно заблокировать Ammyy Admin, Анонимайзеры, BitTorrent и т. д.? . . . 566
37.18 Как настроить SSO-авторизацию для Astra Linux в домене AD? . . . 566
37.19 Как перенести данные и настройки с одного сервера на другой? . . . 566
37.20 Инструкции по созданию VPN-подключений . . . 566
37.20.1 Создание VPN-подключения в Alt Linux . . . 566
37.20.2 Создание VPN-подключения в Ubuntu . . . 572
37.20.3 Создание VPN-подключения в Fedora . . . 592
37.20.4 Создание подключения в Astra Linux . . . 605
37.20.5 Создание подключения в Windows . . . 613
37.20.6 Создание VPN-подключения на мобильных устройствах . . . 635
37.20.7 Создание подключения в Mac OS . . . 640
37.20.8 Подключение по SSTP Wi-Fi роутеров Keenetic . . . 650
37.21 Подключение к сертифицированным Ideco EX и настройка Ideco NGFW . . . 652
37.21.1 Подготовка к настройке . . . 652
37.21.2 Процесс подключения . . . 652
37.22 Анализ трафика . . . 653
37.22.1 Описание использования утилиты и ключи tcpdump . . . 653
37.23 Режим удаленного помощника . . . 657
37.23.1 Включение режима удаленного помощника из веб-интерфейса . . . 658
37.23.2 Включение режима удаленного помощника из локального меню сервера . . . 658
37.23.3 Работа с сервером по протоколу SSH в режиме удаленного помощника . . . 658
37.24 Настройка LACP на Hyper-V . . . 659
37.24.1 Настройка на хост системе . . . 659
37.24.2 Настройка на гостевой системе . . . 662
37.25 Разрешить интернет всем: диагностика неполадок . . . 663
37.25.1 Основное . . . 663
37.26 Удаленный доступ к серверу . . . 664
37.26.1 Доступ по SSH к локальному меню сервера . . . 664
37.26.2 Доступ к веб-интерфейсу сервера из сети интернет . . . 664
37.27 Тестирование оперативной памяти сервера . . . 665
37.27.1 Основное . . . 665
37.28 Как избавиться от асимметричной маршрутизации трафика . . . 667
37.28.1 Асимметричная маршрутизация при наличии роутера в локальной сети . . . 667
37.28.2 Асимметричная маршрутизация при публикации сайтов через DNAT . . . 668
37.28.3 Правильная топология сети: . . . 669
37.29 Что делать если ваш IP попал в черные списки DNSBL . . . 675
37.29.1 Порядок действий при попадании в черный список . . . 675
37.29.2 Ideco NGFW . . . 675
37.30 Как восстановить доступ к Ideco NGFW . . . 675
37.30.1 Основное . . . 675
37.31 Как восстановиться на прошлую версию после обновления Ideco NGFW . . . 677
37.31.1 Основное . . . 677
37.32 Проверка настроек фильтрации с помощью security ideco . . . 679
37.32.1 Предварительная проверка . . . 679
37.32.2 Проверка настроек служб . . . 679
37.33 Поддержка устаревших алгоритмов шифрования . . . 680
37.33.1 Основное . . . 680
37.34 Настройка программы Proxifier для прямых подключений к прокси серверу . . . 681
37.34.1 Настройка . . . 681
37.35 Блокировка популярных ресурсов . . . 682
37.35.1 Основное . . . 682
37.36 Настройка прозрачной авторизации на Astra Linux . . . 691
37.36.1 Основное . . . 691

37.37 Настройка автоматической веб-аутентификации на Ideco NGFW на Linux . . . 693
37.37.1 Инструкция по настройке автоматической веб-аутентификации на Ideco NGFW . . . 693
37.37.2 Настройка автозагрузки скрипта . . . 694
37.38 Перенос данных и настроек на другой сервер . . . 695
37.38.1 Этап 1: Копирование бекапа с сервера . . . 695
37.38.2 Этап 2. Установка Ideco NGFW на новый сервер . . . 695
37.38.3 Этап 3: Перенос бекапа на новый сервер . . . 695
37.38.4 Этап 4: Восстановление БД из бекапа . . . 695
37.38.5 Этап 5: Настройка восстановленного сервера . . . 696
37.38.6 Этап 6: Привязка лицензии к восстановленному из бекапа серверу . . . 696
37.38.7 Перенос данных почтового сервера . . . 697
37.39 Порядок обработки веб-трафика в Ideco NGFW . . . 697
37.39.1 Как проверить, что заблокирует трафик первым: Контроль приложений или система Предотвращения вторжений? . . . 698
37.39.2 Как проверить, что система Предотвращения вторжений обрабатывает трафик приоритетнее, чем Файрвол? . . . 700
37.39.3 Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика? . . . 702
37.40 Интеграция Ideco NGFW и брокера сетевых пакетов DS Integrity NG . . . 703
37.40.1 Пример 1 - Два брокера, по одному со стороны локальной и внешней сетей . . . 704
37.40.2 Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW . . . 705
37.40.3 Пример 3 - Один брокер, расположенный перед Ideco NGFW . . . 706
37.41 Настройка совместной работы ViPNet Координатор с Ideco NGFW . . . 706
37.41.1 Настройка Ideco NGFW и ViPNet-координатора . . . 707
37.42 Блокировка чат-ботов . . . 707
37.42.1 Основное . . . 707
37.43 Таблица портов Ideco NGFW, доступных из локальной и внешних сетей . . . 711
37.43.1 Доступные из внешней сети . . . 711
37.43.2 Доступные из локальной сети . . . 711
37.44 Как включить таймер при загрузке Ideco NGFW . . . 711
37.44.1 Основное . . . 711

38 Диагностика проблем **712**
38.1 Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт . 712
38.1.1 Шаг 1. Проверьте, открывается ли сайт в режиме **Разрешить интернет всем** . . . 713
38.1.2 Шаг 2. Проверьте, не блокирует ли сайт модуль Контроль приложений . . . 713
38.1.3 Шаг 3. Проверьте, не блокирует ли сайт система Предотвращения вторжений . . . 714
38.1.4 Шаг 4. Проверьте, не блокируется ли сайт правилом Контент-фильтра . . . 715
38.1.5 Шаг 5. Проверьте, не блокируется ли сайт правилом Файрвола . . . 716
38.1.6 Шаг 6. Определите блокируемый домен или IP-адрес (рассмотрим на примере FireFox) 718
38.1.7 Если решить проблему не удалось . . . 718
38.2 Что делать если не работает интернет . . . 718
38.2.1 Шаг 1. Проверить параметры пользователя . . . 718
38.2.2 Шаг 2. Проверка компьютера пользователя . . . 718
38.2.3 Шаг 3. Проверка доступа к интернету на сервере . . . 719
38.2.4 Шаг 4. Проверка файрвола . . . 719
38.2.5 Шаг 5. Проверка работы веб-трафика . . . 719
38.2.6 Шаг 6. Если вам не удалось решить проблему . . . 719
38.3 Ошибка при авторизации «The browser is outdated» . . . 720
38.3.1 Основное . . . 720
38.4 Если соединение по IPsec не устанавливается . . . 720
38.4.1 Основное . . . 720

39 Описание основных хендлеров **720**
39.1 Получение текущих настроек: . . . 722
39.2 Изменение настроек . . . 723
39.3 Лицензирование . . . 723
39.4 Управление объектами . . . 726

39.4.1 Создание обьектов . . . 727
39.4.2 Изменение обьектов . . . 732
39.4.3 Удаление обьектов . . . 736
39.5 Обнаружение устройств . . . 736
39.6 Распространенные статусы . . . 737

40 Управление интеграцией с Active Directory **737**
40.1 Управление настройками службы . . . 739
40.2 Получение информации об объектах контроллера домена . . . 740
40.3 Управление настройками синхронизации групп . . . 741

41 Управление пользователями **742**
41.1 Управление пользователями . . . 743

42 Управление Ideco Client **746**
42.1 Настройка авторизации через Ideco Client . . . 746
42.2 Настройки авторизации Ideco Client . . . 747
42.3 Протокол подключения и авторизации Ideco Client . . . 747
42.3.1 1. Подключение и запрос соответствия версии Ideco Client . . . 747
42.3.2 2. Авторизация . . . 748
42.4 Протокол обмена информацией для ZTNA . . . 750

43 Управление правилами трафика **753**
43.1 Файрвол . . . 754
43.2 Включенность пользовательских правил . . . 754
43.2.1 Логирование правил . . . 754
43.2.2 Получение списка правил . . . 755
43.3 Управление правилами . . . 759
43.3.1 Счетчик срабатывания правил . . . 760
43.4 Контроль приложений . . . 761
43.5 Предотвращение вторжений . . . 763
43.6 Контент-фильтр . . . 769
43.6.1 Проверить включенность . . . 769
43.6.2 Включить/выключить Контент-фильтр . . . 769
43.6.3 Настройки . . . 769
43.6.4 Категории Контент-фильтра . . . 770
43.6.5 Правила Контент-фильтра . . . 772
43.7 Квоты . . . 775

44 Управление сетевыми интерфейсами **777**
44.1 Внешние и локальные интерфейсы . . . 777
44.1.1 Получение списка всех внешних и локальных интерфейсов . . . 777
44.1.2 Управление внешними и локальными интерфейсами . . . 782
44.2 Агрегированные интерфейсы . . . 784
44.3 Туннельные интерфейсы . . . 785
44.4 VCE-интерфейсы . . . 788

45 DHCP-сервер **789**
45.1 Настройки . . . 790
45.2 Привязка IP к MAC . . . 793

46 DNS-сервер **794**
46.1 Настройки . . . 795
46.1.1 Получение настроек: . . . 795
46.1.2 Изменение настроек: . . . 796
46.2 Управление внешними DNS-серверами . . . 796
46.3 Управление Forward-зонами . . . 798
46.4 Управление Master-зонами . . . 799
46.5 DDNS . . . 800

47 Настройка удаленной передачи системных логов **802**
47.1 Общие настройки . . . 802

48 Центральная консоль **806**
48.1 Настройки Центральной консоли в Ideco NGFW . . . 806
48.2 API Ideco Center . . . 807
48.2.1 Общие настройки . . . 807
48.2.2 Группировка серверов . . . 808
48.2.3 Управление подключенными серверами . . . 809
48.2.4 Управление правилами трафика Ideco Center . . . 811

49 Бекапы **820**
49.1 Управление бекапами . . . 822

50 Примеры использования **824**
50.1 Редактирование пользовательской категории контент-фильтра . . . 824
50.1.1 Основное . . . 824
50.2 Создание правила FORWARD . . . 825
50.2.1 Основное . . . 825

,

1. Возможности Ideco NGFW:

- Межсетевой экран
- Система предотвращения вторжений
- Контент-фильтр
- Контроль приложений
- Многоуровневая антивирусная и антиспам-проверка трафика
- Защита от ботнетов, фишинга и spyware
- VPN site-to-site (GRE, IPSec) и client-to-site (IKEv2/IPSec, L2TP/IPSec, SSTP, Wireguard) с 2FA
- Логирование действий администратора
- Управление через 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

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

У лицензии Ideco NGFW есть три основные характеристики:

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

Подсказка: Особенности лицензирования:

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

2.1 Виды лицензий

В Ideco NGFW доступны лицензии:

Enterprise-demo

Enterprise-demo - бесплатная лицензия сроком на 44 дней.

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

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

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

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

Enterprise

Enterprise - коммерческая лицензия.

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

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

- Обновления на новые версии Ideco NGFW;
- Расширенный модуль **Контент-фильтр**;
- Модуль **Предотвращение вторжений**;
- Модуль **Контроль приложений**;

- Автоматическое обновление модулей;
- Техническая поддержка.

Модуль **Кластеризация** и технологии Лаборатории Касперского приобретаются отдельно в отделе продаж.

Подробнее о лицензировании Кластеризации:

Начиная с 18 версии, в системе лицензирования произошли изменения:

- Все Enterprise-лицензии с действующей подпиской на обновления получат включенный в лицензию кластер до первого июля 2029 года;
- Стоимость продления лицензий не изменится до первого июля 2025 года, после чего лицензия будет учитывать включенный модуль кластера. При этом сама лицензия на **Кластеризацию** станет бессрочной;
- При покупке новой лицензии на Ideco NGFW модуль **Кластеризация** необходимо заказывать дополнительно;
- После окончания срока действия лицензии на **Кластеризацию** работа кластера не нарушается.

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

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

Free

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

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

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

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

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

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

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

2.1.2 Просмотр информации о лицензиях

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

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

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

3. Системные требования и источники обновления данных Ideco NGFW

3.1 Минимальные системные требования

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

Комплектующие	Системные требования
Процессор	Intel i3/i5/i7/i9/Xeon и AMD FX/Ryzen/EPYC с поддержкой SSE 4.2 (минимум 4 ядра)
Объем оперативной памяти	16 ГБ (16-64 ГБ в зависимости от количества пользователей)
Дисковая подсистема	SSD объемом 150 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe. Дополнительный SSD при использовании почтового сервера
Сеть	Две сетевые карты (или два сетевых порта) 100/1000 Mbps. Рекомендуется использовать карты на чипах Intel
Гипервизоры	VMware, Microsoft Hyper-V (виртуальные машины 2-го поколения), VirtualBox, KVM, Citrix XenServer, Proxmox VE
Дополнительно	Монитор и клавиатура
Замечания	Обязательна поддержка UEFI. Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет). Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти

Подсказка: Обязательные условия для работы с Ideco 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.

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

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.

Подсказка: Представленные типы конфигураций относятся ко всем функциональностям продукта.

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

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

3.3 Источники обновлений данных

Ideco NGFW получает обновления из следующих источников:

- Отсылка уведомлений в личный кабинет/телеграм-бот: alerts.v17.ideco.dev;
- Обновление баз **Контент-фильтра**: content-filter.v17.ideco.dev;
- Отсылка анонимной статистики: gatherstat.v17.ideco.dev;
- Обновления баз GeoIP: ip-list.v17.ideco.dev;
- Обмен информации о лицензии: license.v17.ideco.dev;
- Отправка отчетов по почте: send-reports.v17.ideco.dev;
- Обновления suricata: suricata.v17.ideco.dev;
- Обновления системы: sysupdate.v17.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.

3.4 Программно-аппаратный комплекс (ПАК)

Описание линейки программно-аппаратных комплексов доступно по ссылке.

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

3.5 Выбор аппаратной платформы для Ideco NGFW

3.5.1 Сведения о программной платформе

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 39 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 39.

3.5.2 Общие рекомендации по чипсетам и производителям

- Рекомендуем чипсеты и контроллеры фирм Intel и Broadcom. Особенно сетевые карты и наборы логики, используемые в материнских платах;
- Не рекомендуем использовать встроенные сетевые карты, особенно интерфейсы на бюджетных/редких/устаревших/noname чипсетах. NGFW работает с сетью, и зачастую бюджетные сетевые адаптеры для десктопов не справляются с задачами шлюза;
- Не рекомендуем использовать RAID-контроллеры в работе сетевого шлюза. Встроенные в материнские платы программные и полуаппаратные RAID-контроллеры официально не поддерживаются нашим продуктом;
- Материнские платы могут использоваться как серверные, так и десктопные. Желательно использование процессоров Intel;
- Бюджетные, энергоэкономичные платформы для десктопов, полутонких клиентов на базе Intel Atom не подходят для работы Ideco NGFW и не соответствуют минимальным *системным требованиям* продукта.

3.5.3 Подбор мощности аппаратной платформы

Количество ГГц процессора и объем ОЗУ сервера сильно зависят от нагрузки, возлагаемой на Ideco NGFW. При подсчете нагрузки нужно выделить три фактора:

- Количество одновременно авторизованных на NGFW пользователей;
- Задействованные компоненты NGFW (прокси с его сервисами, проверка трафика на спам/вирусы, обширность настройки модуля контентной фильтрации или файрвола);
- Система предотвращения вторжений - при высокоскоростном подключении к провайдеру эта служба может потребовать значительных ресурсов процессора и памяти. Рекомендуется использовать многоядерные процессоры (4 и более ядер с частотой более 3 ГГц) и от 16 ГБ оперативной памяти.

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

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

3.5.4 Дисковая подсистема

RAID-массивы не требуются при типичных схемах использования NGFW. Одного современного жесткого диска SATA от 200 ГБ хватает в большинстве конфигураций. В случае использования почтового сервера на Ideco NGFW требуется подключить отдельный винчестер для хранения почтовой корреспонденции. Рекомендуется использование SSD-дисков и устройств марки Micron.

4. Техническая поддержка

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

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

4.1 График работы

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

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

4.2 Способы обращения

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

4.3 Правила обращения

Техническая поддержка пользователей осуществляется в соответствии с регламентом.

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

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

4.4 Информация о поддержке версий Ideco NGFW

4.4.1 Уровни поддержки

Обозначения:

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

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

4.4.2 Сроки поддержки

Версия Ideco NGFW	Дата релиза	Полная поддержка	Частичная поддержка	Минимальная поддержка
7.9.X	01.11.2019	01.01.2023	01.01.2023	01.11.2024
8	08.09.2020	01.01.2023	01.01.2023	08.09.2025
9	28.12.2020	01.01.2023	01.01.2023	28.12.2025
10	30.07.2021	01.01.2023	01.01.2023	30.07.2026
11	03.11.2021	01.01.2024	01.01.2024	03.11.2026
12	04.05.2022	01.01.2024	01.01.2024	04.05.2027
13	01.09.2022	01.01.2024	01.01.2024	01.09.2027
14	27.01.2023	01.01.2024	01.01.2024	27.01.2028
15	29.08.2023	01.07.2024	01.07.2024	29.08.2028
16	28.12.2023	01.10.2024	01.01.2025	28.12.2028
17	07.05.2024	01.01.2025	01.06.2025	07.05.2029
18	11.10.2024	01.05.2025	01.10.2025	11.10.2029
19	12.03.2025	01.01.2026	01.04.2026	11.10.2029

5. Рекомендации при первоначальной настройке

5.1 Основное

Рекомендуемая последовательность шагов для минимальной настройки Ideco NGFW:

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

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

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

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

5. Выполните первоначальную настройку Ideco NGFW.

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

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

6. MY.IDECO.RU

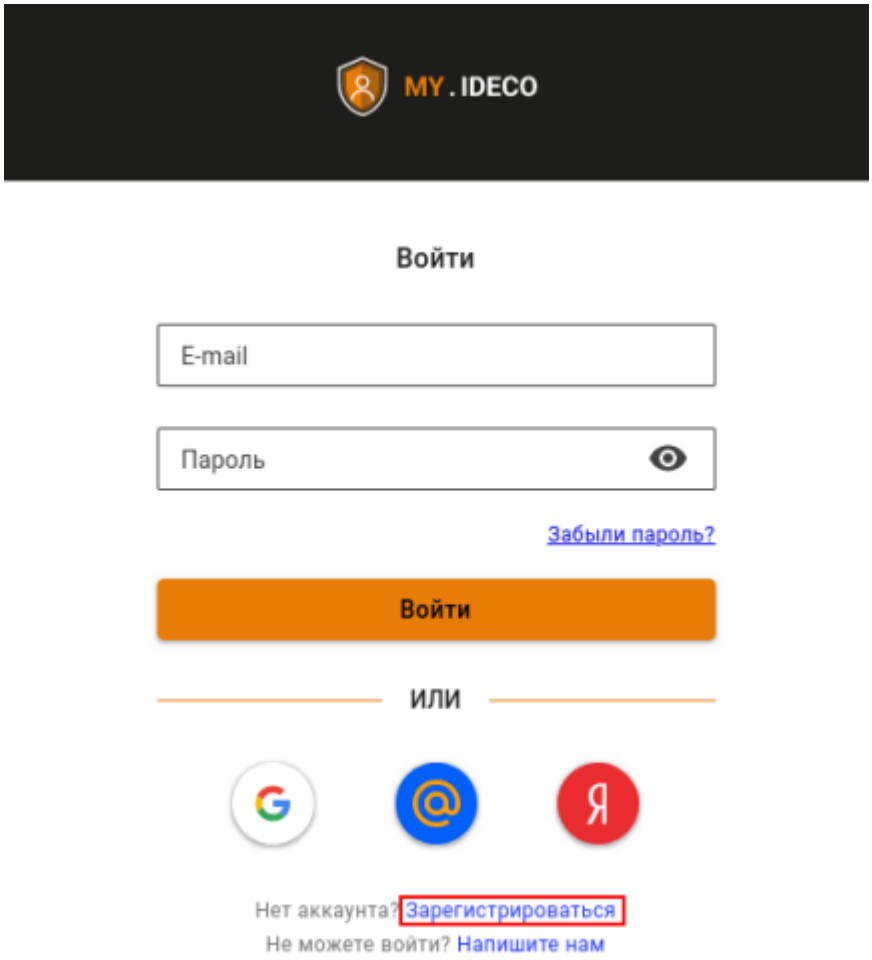
Подсказка: Личный кабинет my.ideco.ru позволяет пользователю получить информацию:

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

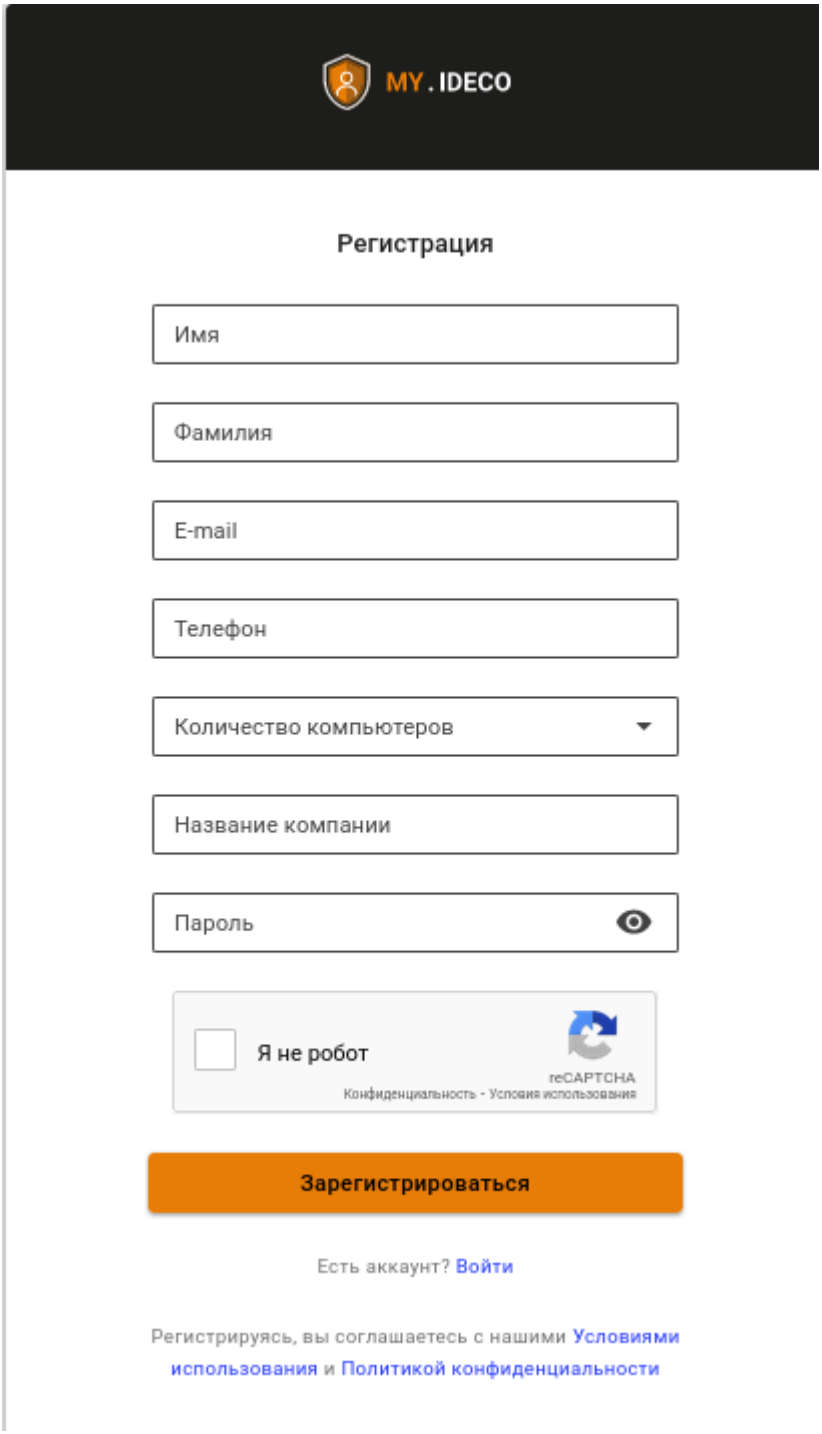
6.1 Регистрация на my.ideco

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. Настройка программно-аппаратных комплексов Ideco NGFW

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

IPMI поддерживают модели:

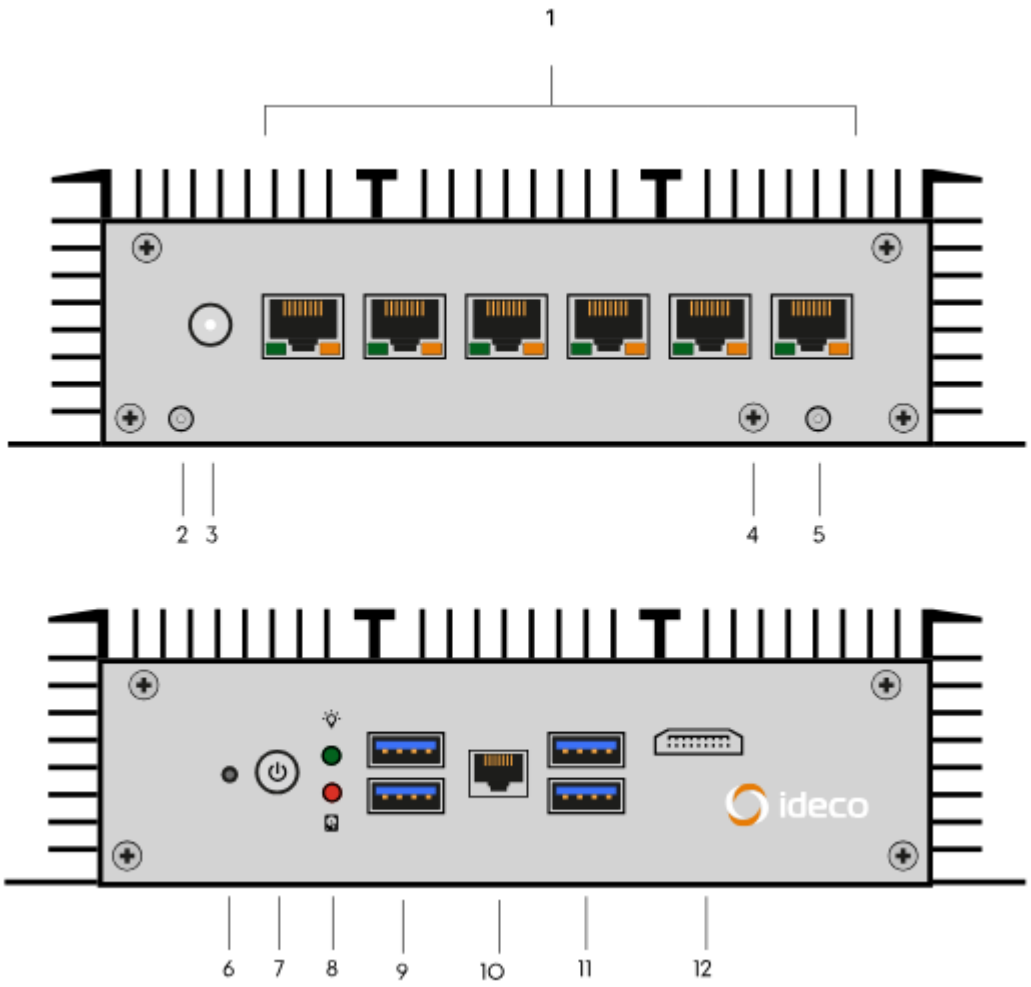
- Ideco NGFW MX;
- Ideco NGFW LX;
- Ideco NGFW LX+.

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

7.1 Описание панелей программно-аппаратных комплексов Ideco NGFW

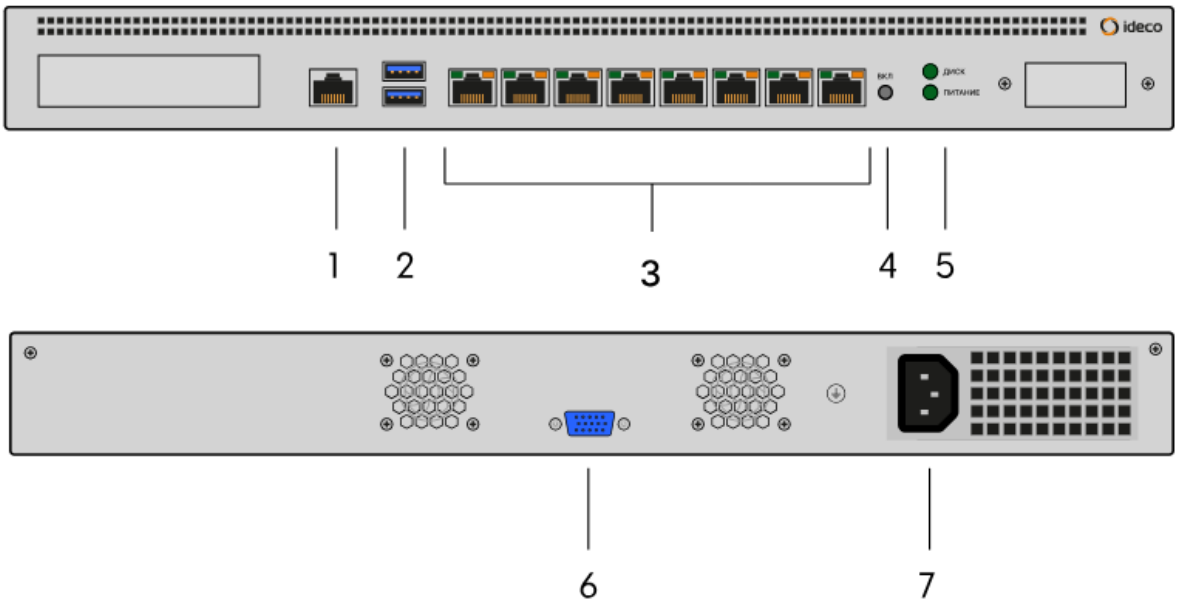
Внешний вид серверов может отличаться от иллюстраций.

Ideco NGFW SX+:



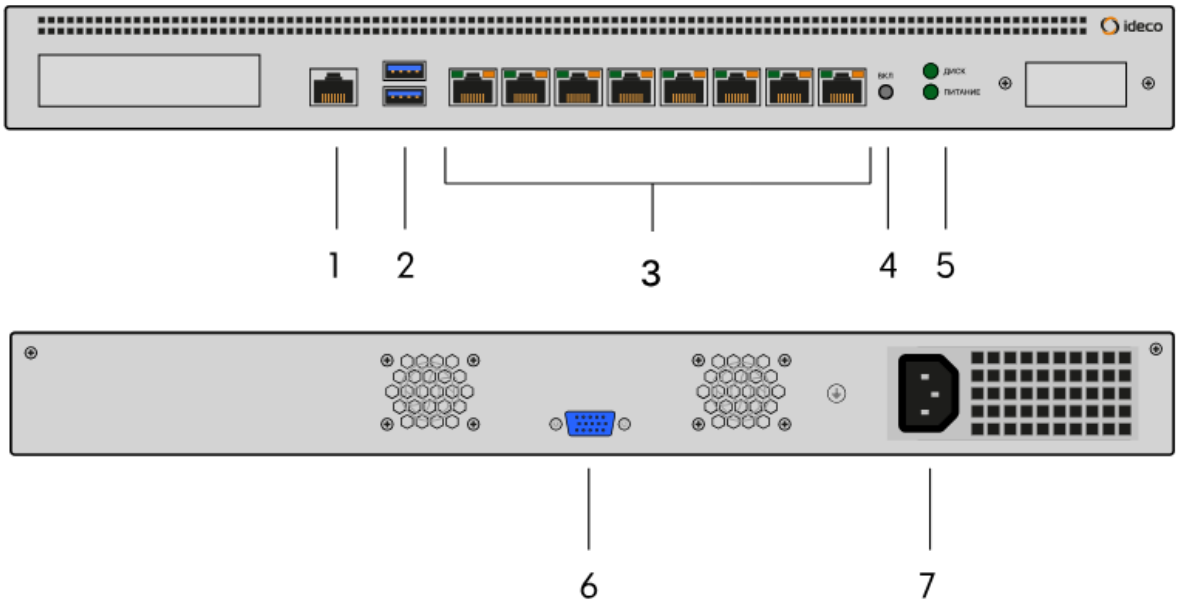
1. Шесть портов LAN (RJ-45);
2. Заглушка для антенны Wi-Fi (RF-разъем);
3. Входной разъем постоянного тока (DC input);
4. Крепление для заземления;
5. Заглушка для антенны Wi-Fi (RF-разъем);
6. Кнопка перезагрузки;
7. Кнопка питания;
8. Светодиодные индикаторы:
    - жесткий диск;
    - питание.
9. Порт USB 3.0;
10. Консольный порт (COM);
11. Порт USB 3.0;
12. HDMI-разъем.

Ideco NGFW MX:



1. Консольный порт;
2. Два порта USB 3.0;
3. Восемь портов LAN (RJ-45);
4. Кнопка питания;
5. Светодиодные индикаторы:
    - жесткий диск;
    - питание.
6. Разъем VGA;
7. Входной разъем питания IEC C14.

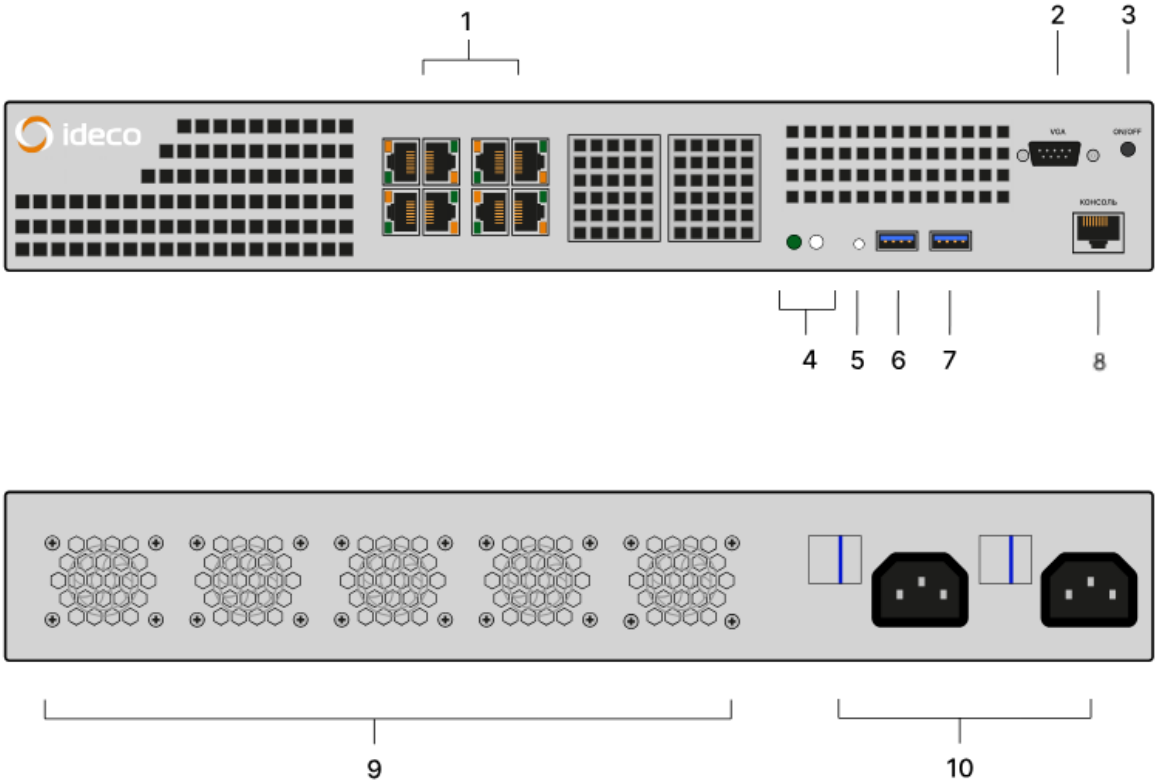
Ideco NGFW LX:



1. Консольный порт;

2. Два порта USB 3.0;
3. Восемь портов LAN (RJ-45);
4. Кнопка питания;
5. Светодиодные индикаторы:
    - жесткий диск;
    - питание.
6. Разъем VGA;
7. Входной разъем питания IEC C14.

Ideco NGFW LX+:



1. Восемь портов LAN (RJ-45);
2. Разъем VGA;
3. Кнопка включения/выключения;
4. Индикаторы:
    - питание;
    - sys.
5. Кнопка перезагрузки;
6. Порт USB 3.0;
7. Порт USB 2.0
8. Консольный порт;
9. Вентиляторы;
10. Два входных разъема питания IEC C14.

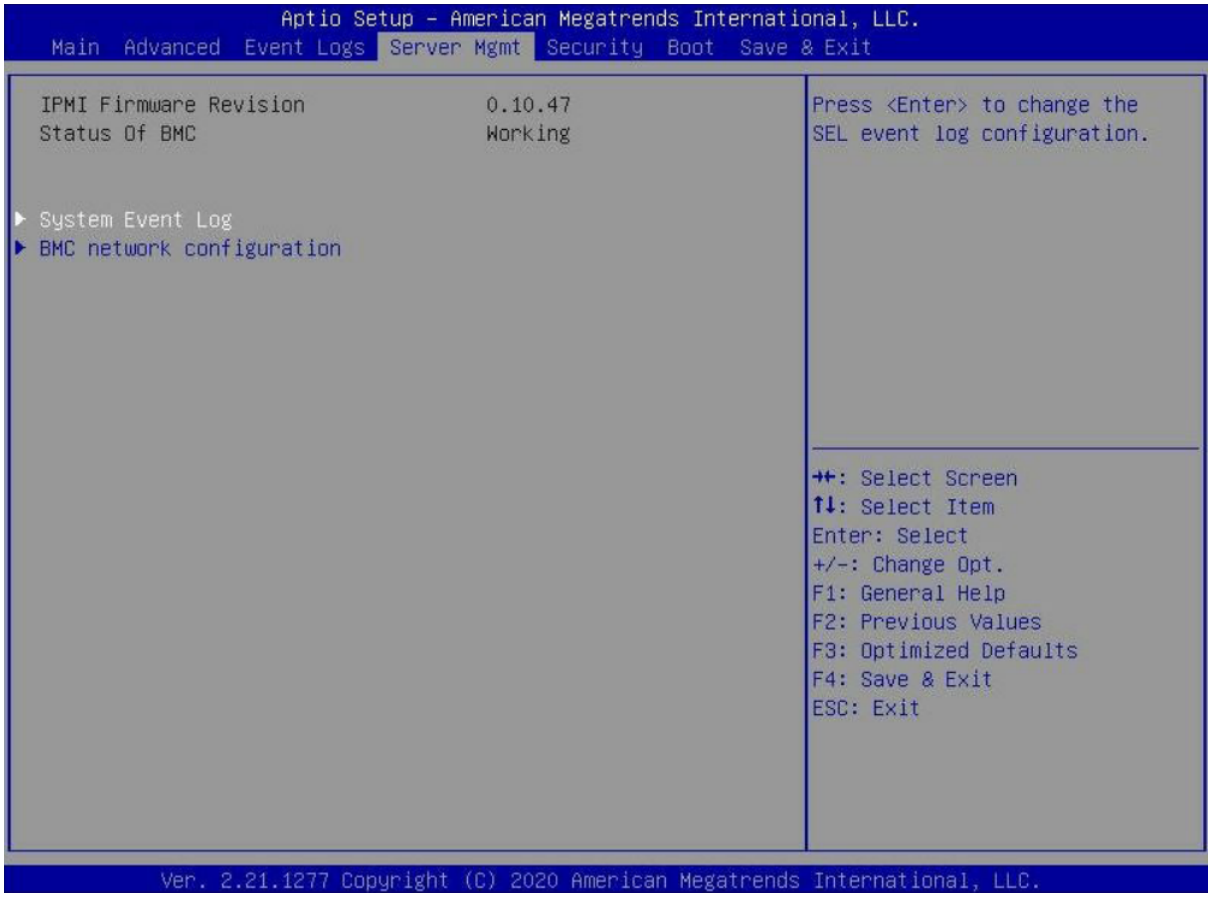
Подсказка: Внешний вид интерфейса UEFI может различаться в зависимости от версии прошивки UEFI или модели/ревизии аппаратной платформы Ideco.

7.2 Настройка IPMI

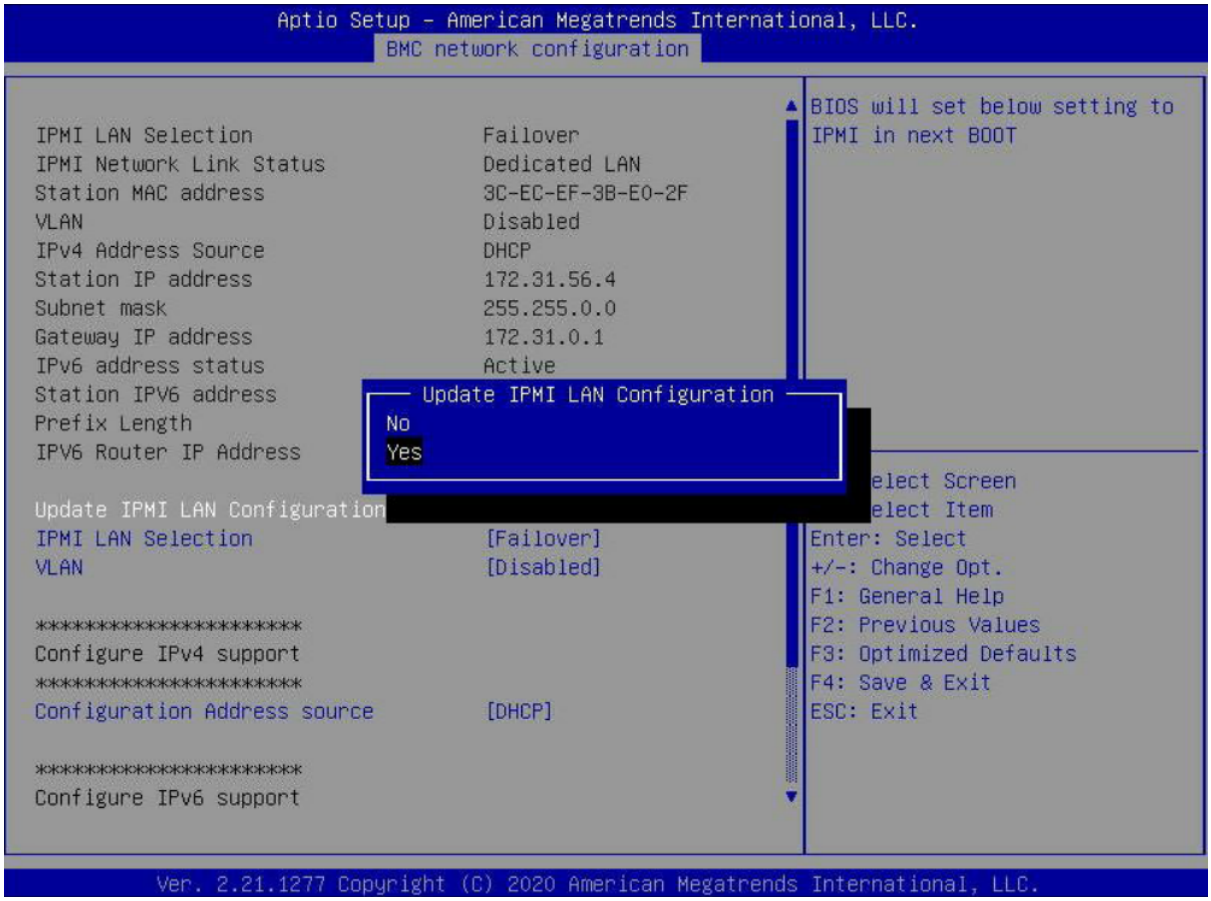
1. Подключите ноутбук или другое устройство к порту IPMI/SHARED сервера.

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

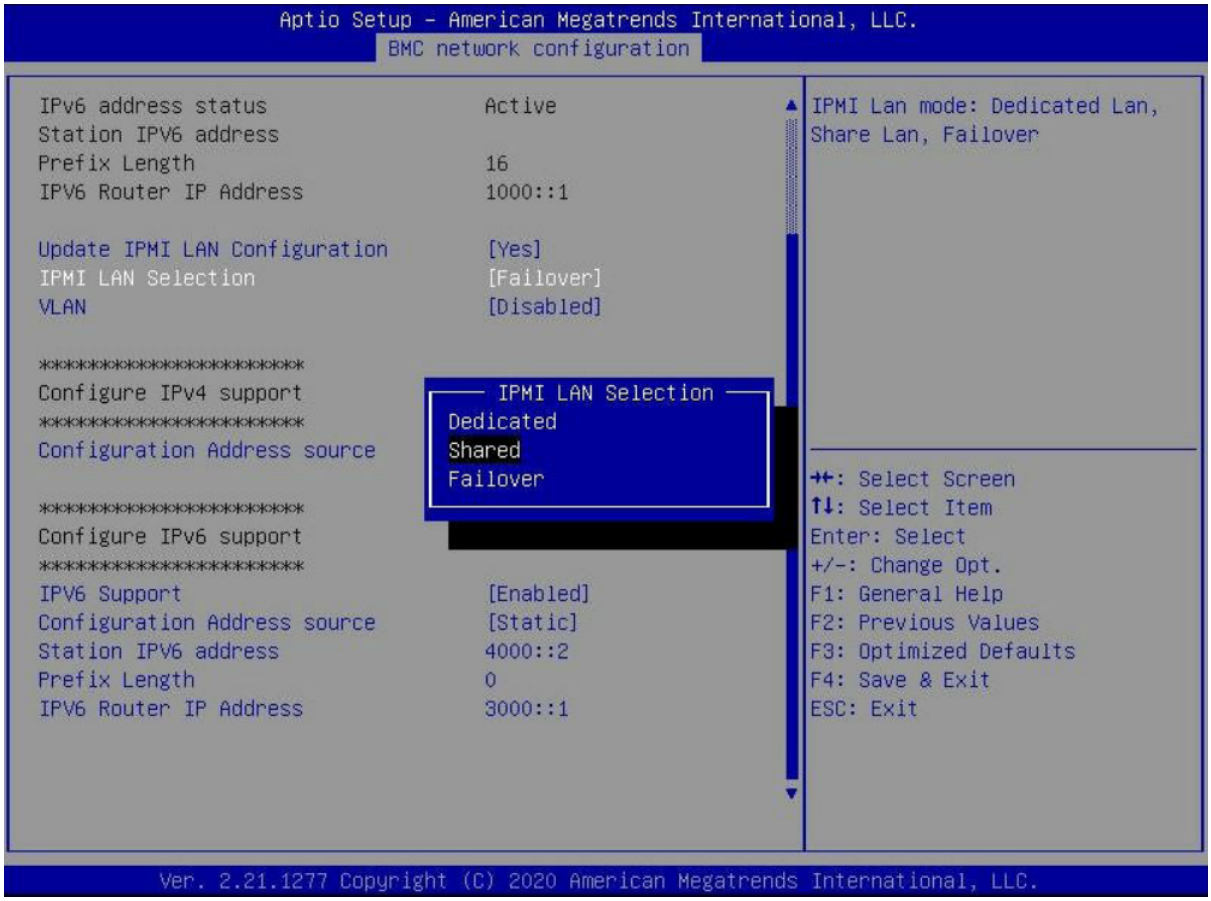
3. Перейдите на вкладку **Server Mgmt** (для навигации в UEFI используйте клавиши со стрелками, для выбора - *Enter*, для возврата к предыдущим экранам - *Esc*) и выберите **BMC Network Configuration**:



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

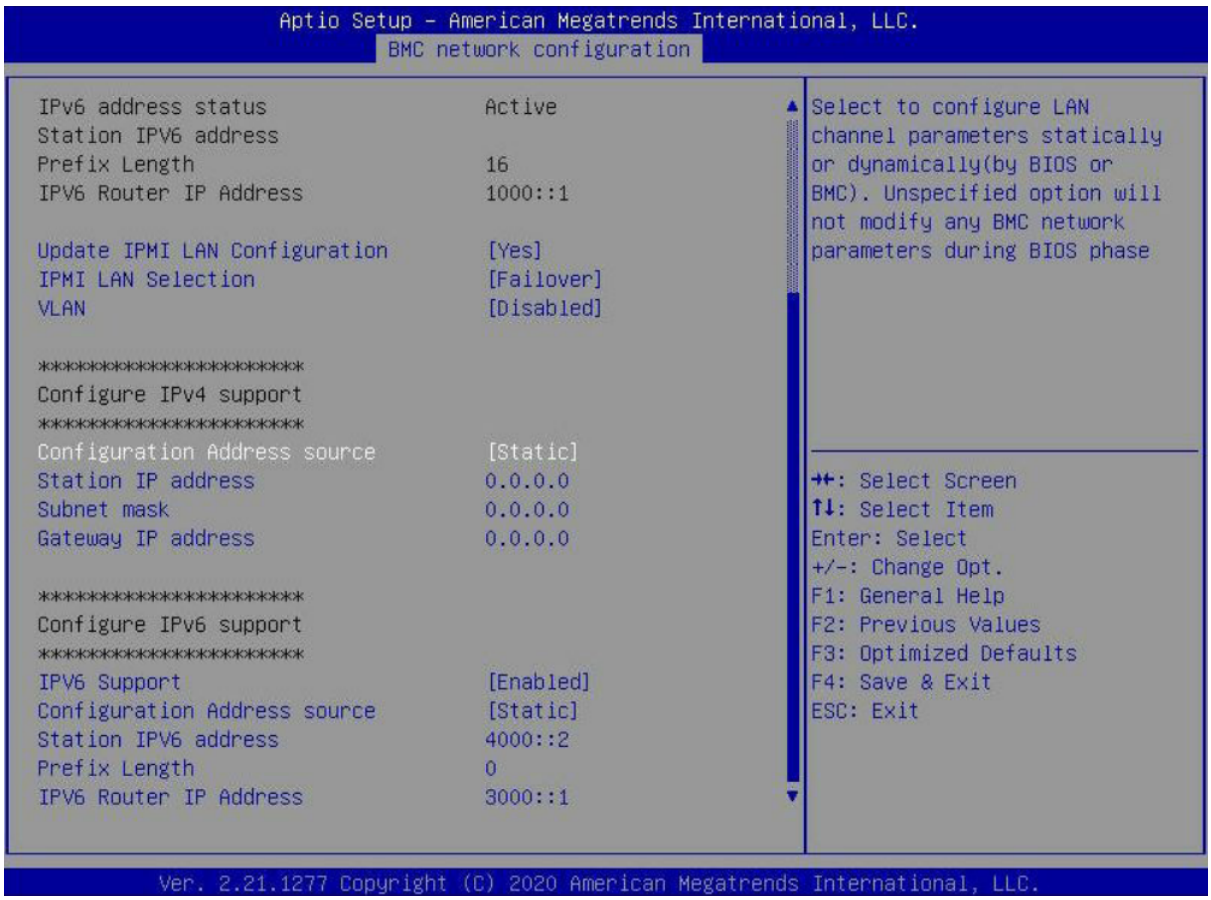


5. Перейдите к пункту **IPMI LAN Selection**, выберите необходимый режим:



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

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



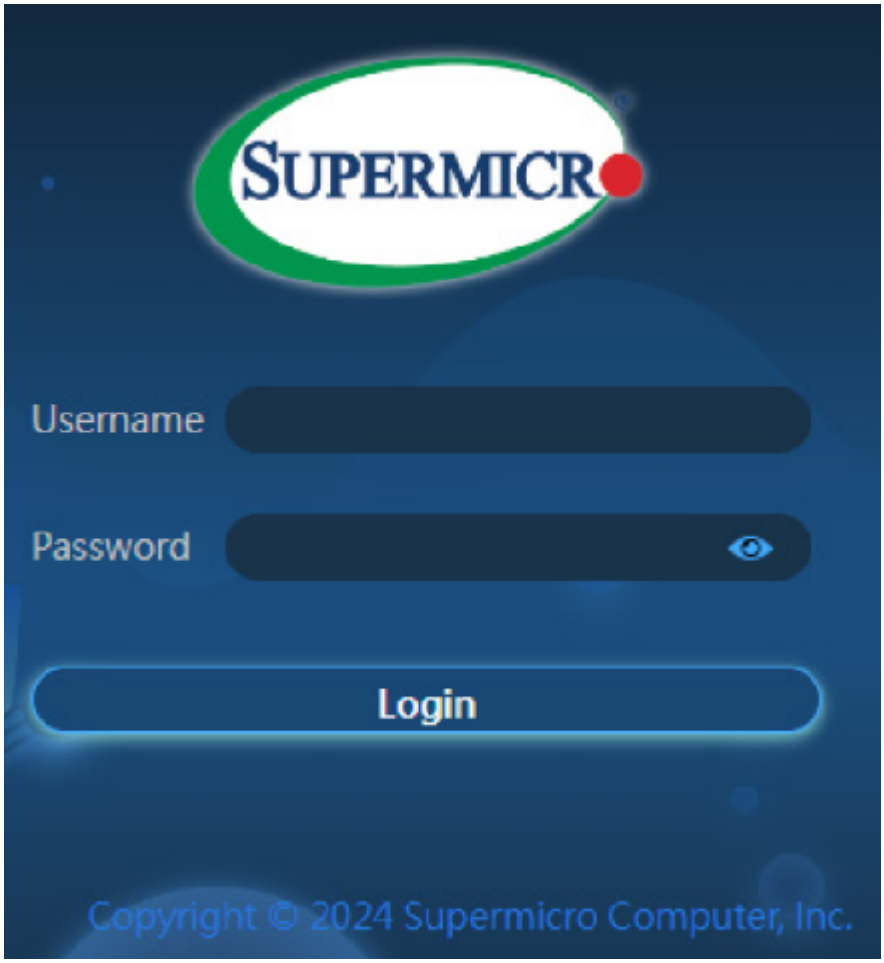
Внимание: Будьте внимательны! IP-адрес IPMI не должен совпадать с IP-адресами локальных или внешних интерфейсов.

7. Сохраните конфигурацию и выйдите из интерфейса UEFI.

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

```
ping <ip-адрес станции>
```

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



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

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

7.3 Настройка ПАК Ideco NGFW SX+

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

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

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

3. Если Ideco NGFW не загружен:

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

4. Перейдите к статье *Установка*.

8. Подготовка к установке на устройство

8.1 Основное

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

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

8.2 Настройка гипервизора

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:

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

8.2.1 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.

8.2.2 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).

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

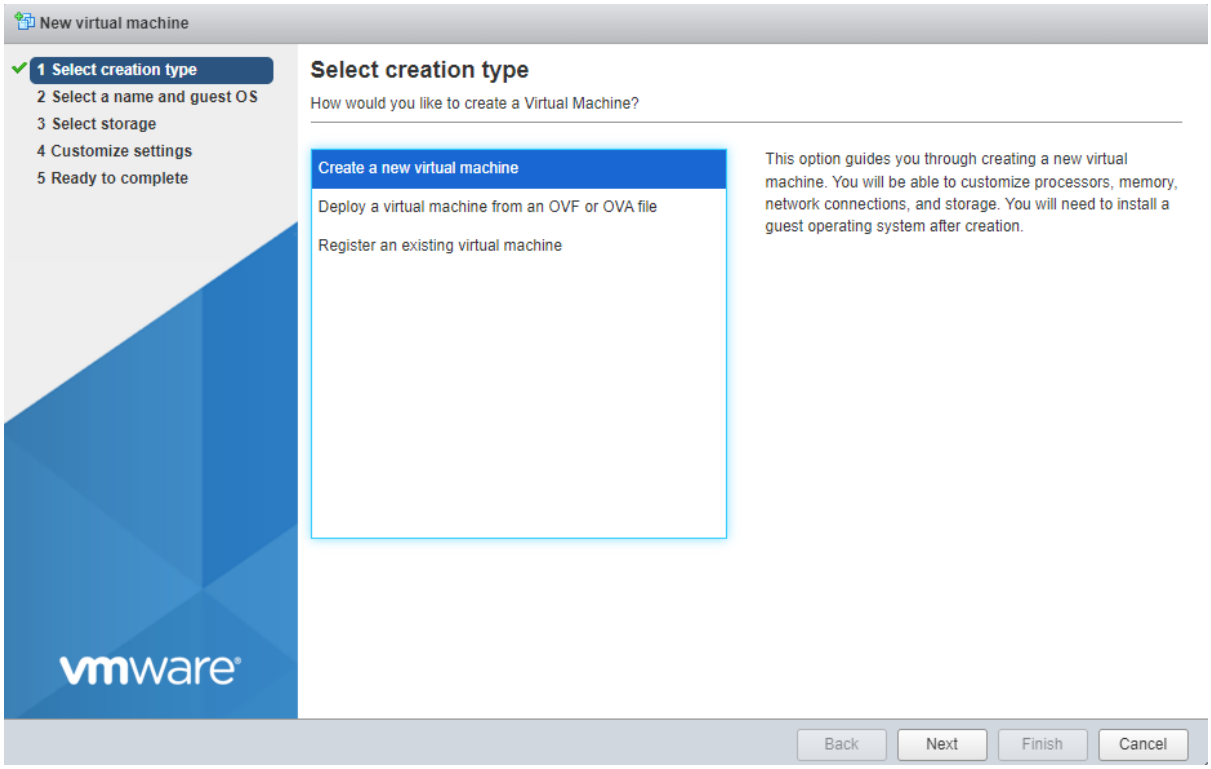
8.2.3 VMware ESXi 6.7

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

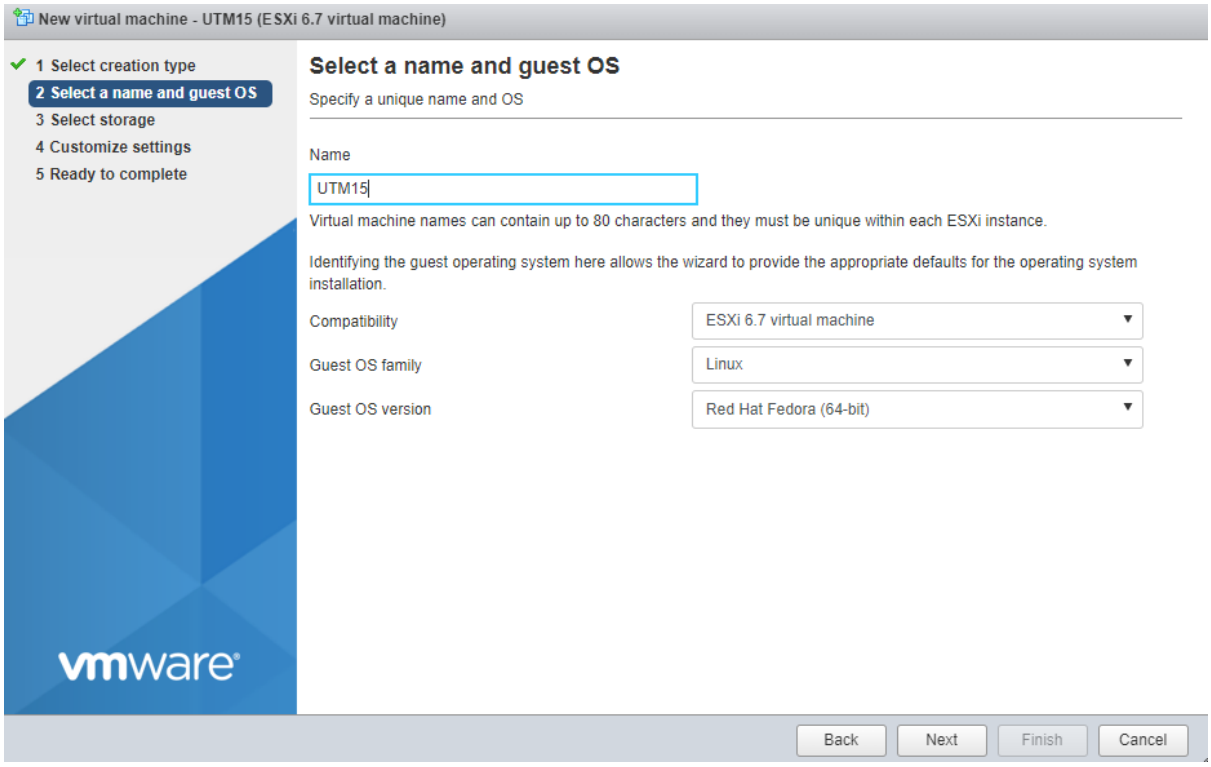
Настройка:

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

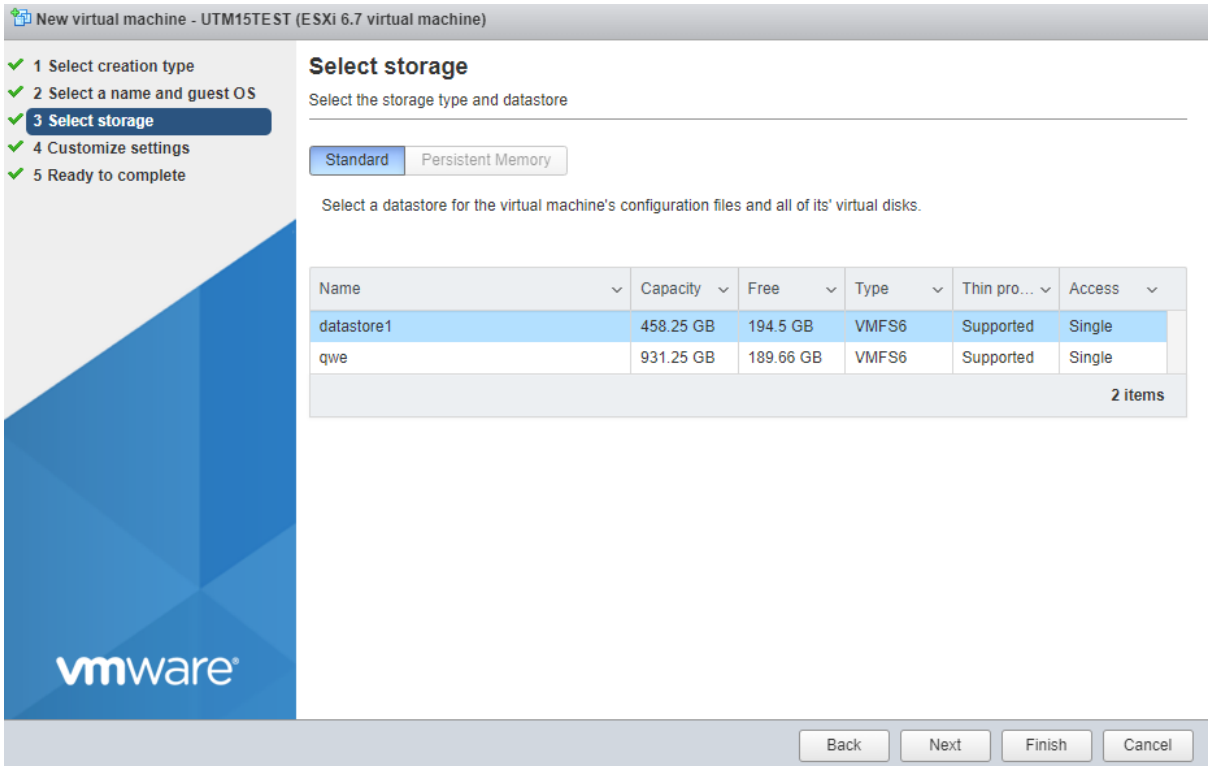
1. Создайте виртуальную машину:



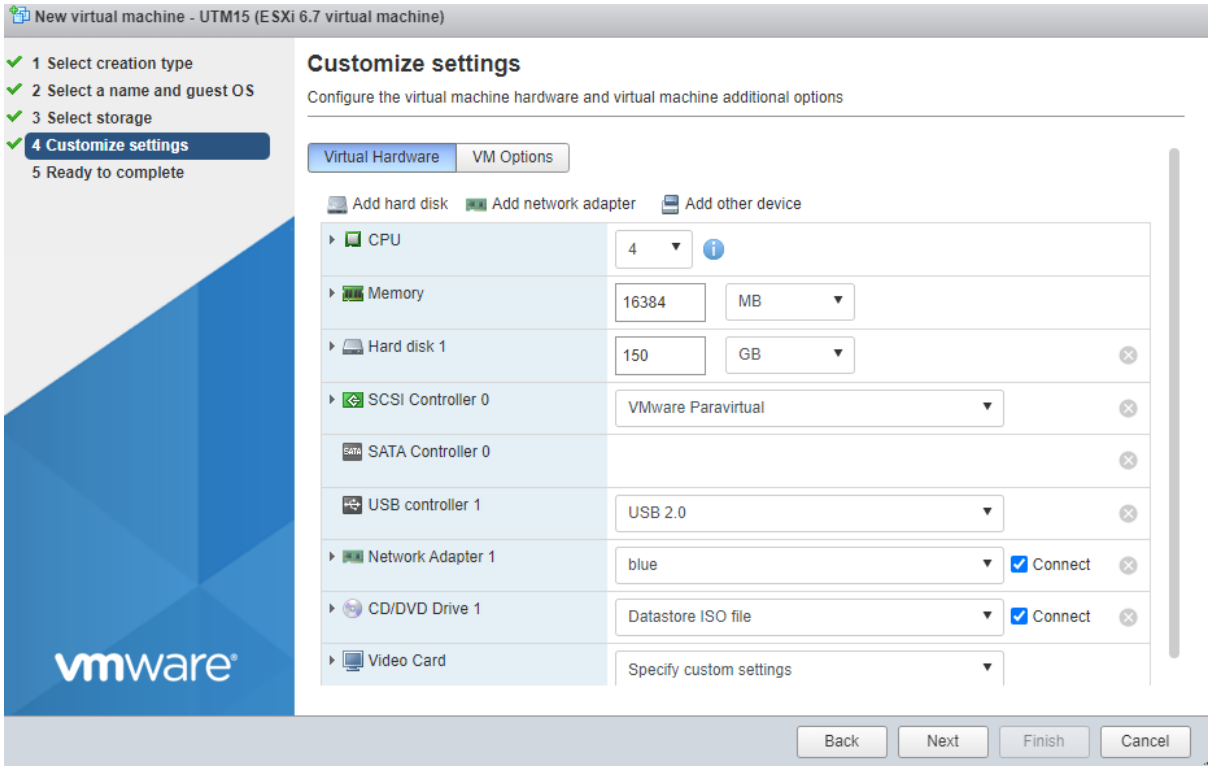
2. Укажите **Имя** виртуальной машине и установите остальные настройки как на скриншоте:



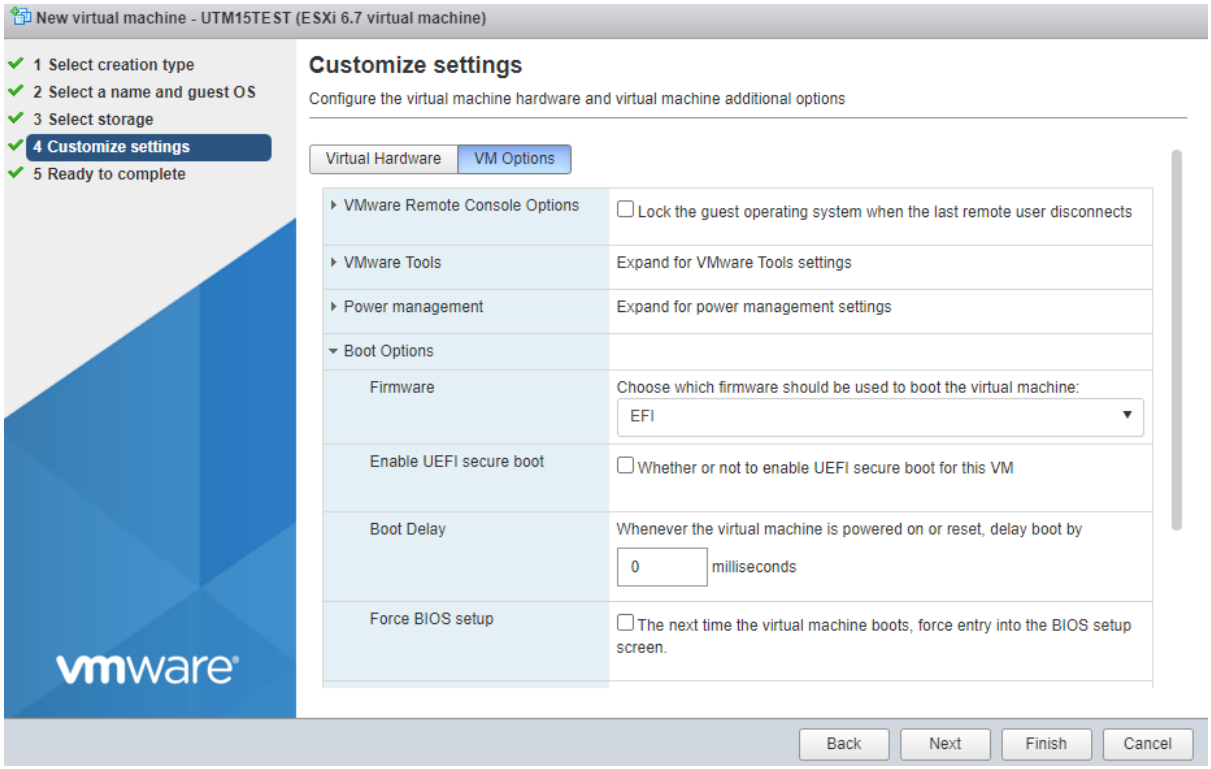
3. Выберите хранилище для виртуальной машины:



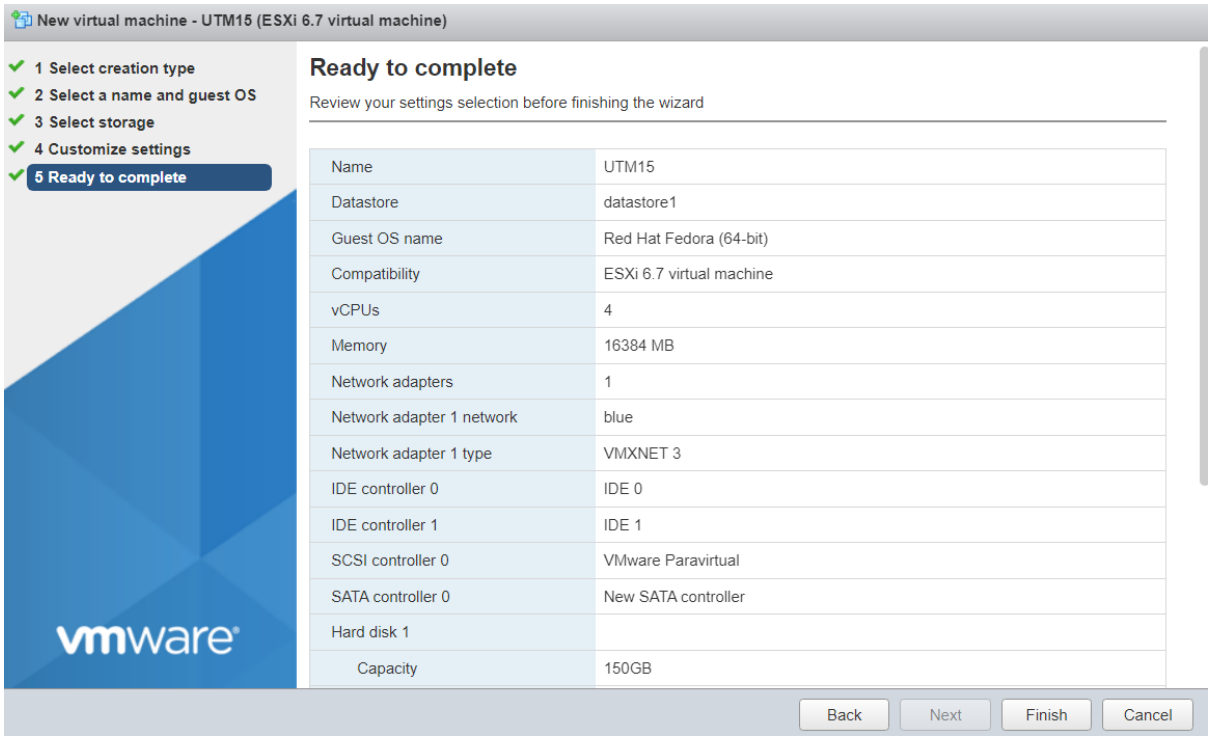
4. Установите размер оперативной памяти **16ГБ** и размер диска **150ГБ**. После выберите в поле **CD/DVD Drive** Datastore ISO file и укажите путь к загрузочному образу:



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



6. Нажмите **Finish**:



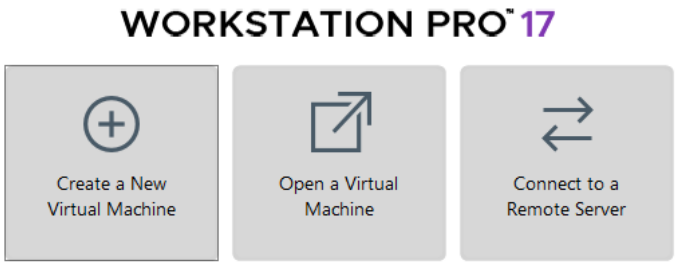
Подсказка: При установке Ideco NGFW на хосты кластера с разными поколениями процессоров укажите в настройках EVC самое старое поколение процессора из хостов, соответствующее минимальным системным требованиям для установки.

8.2.4 VMware Workstation 17.0

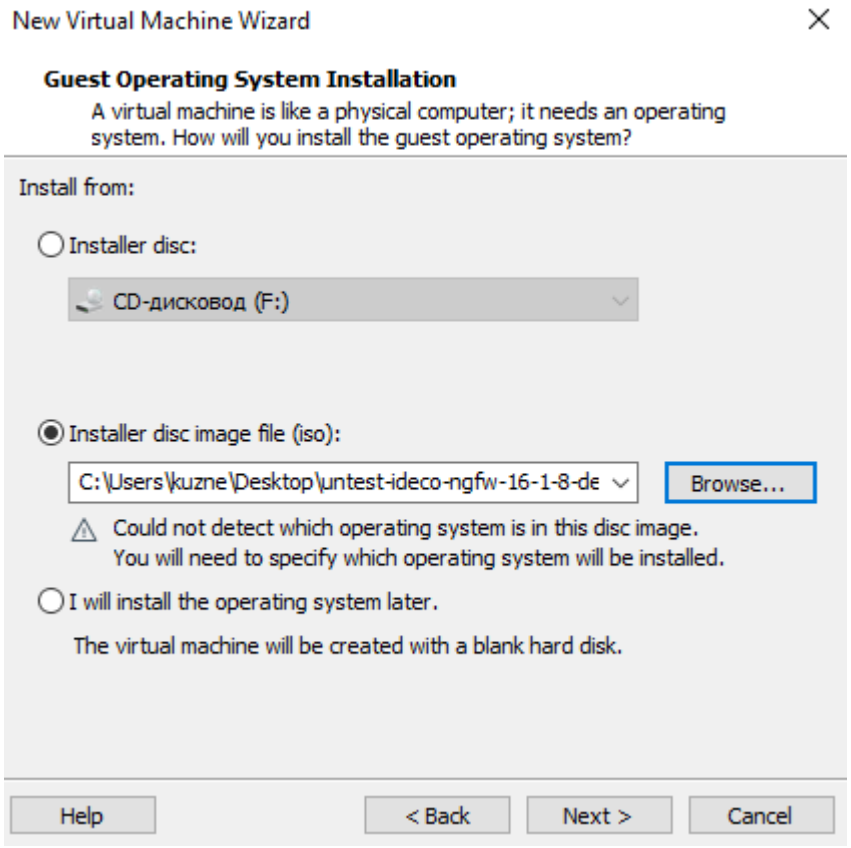
- Перед установкой Ideco NGFW увеличьте размер видеопамяти для виртуальной машины до 16 МБ;
- Используйте виртуальные сетевые адаптеры **vmxnet3**.

Настройка:

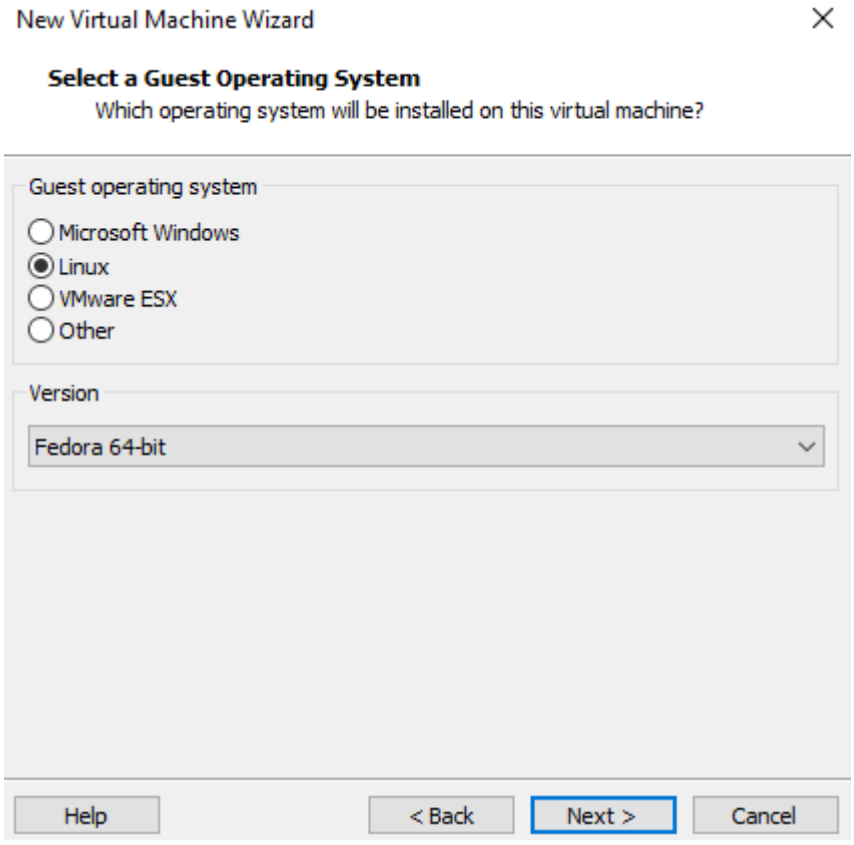
1. Создайте виртуальную машину, нажав **Create a New Virtual Machine**:



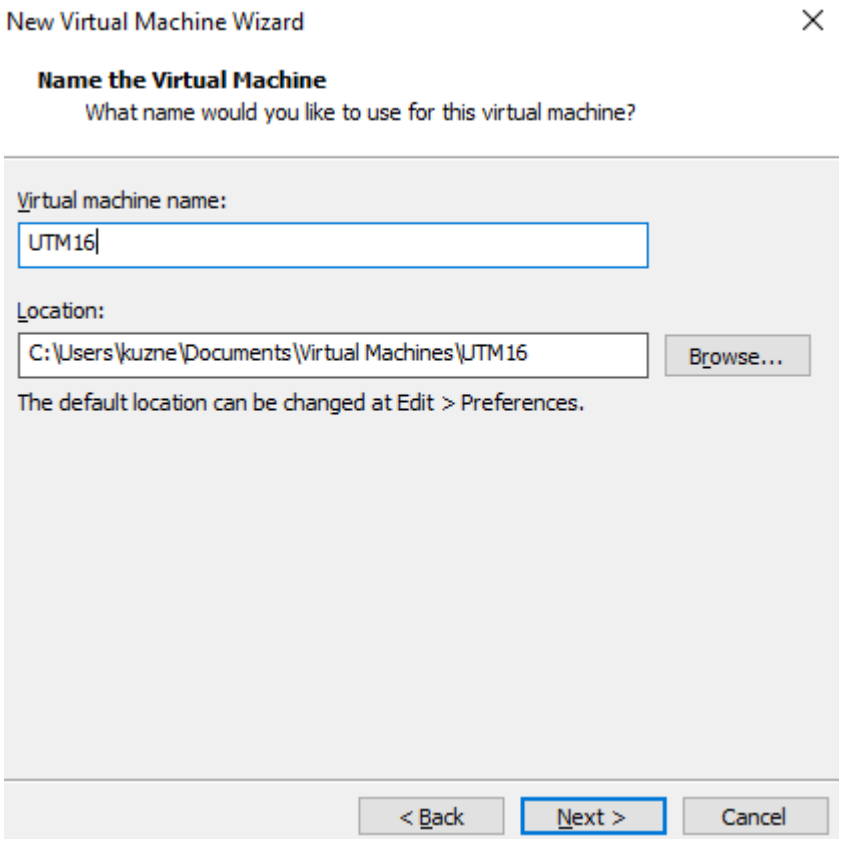
2. Укажите загрузочный ISO-образ:



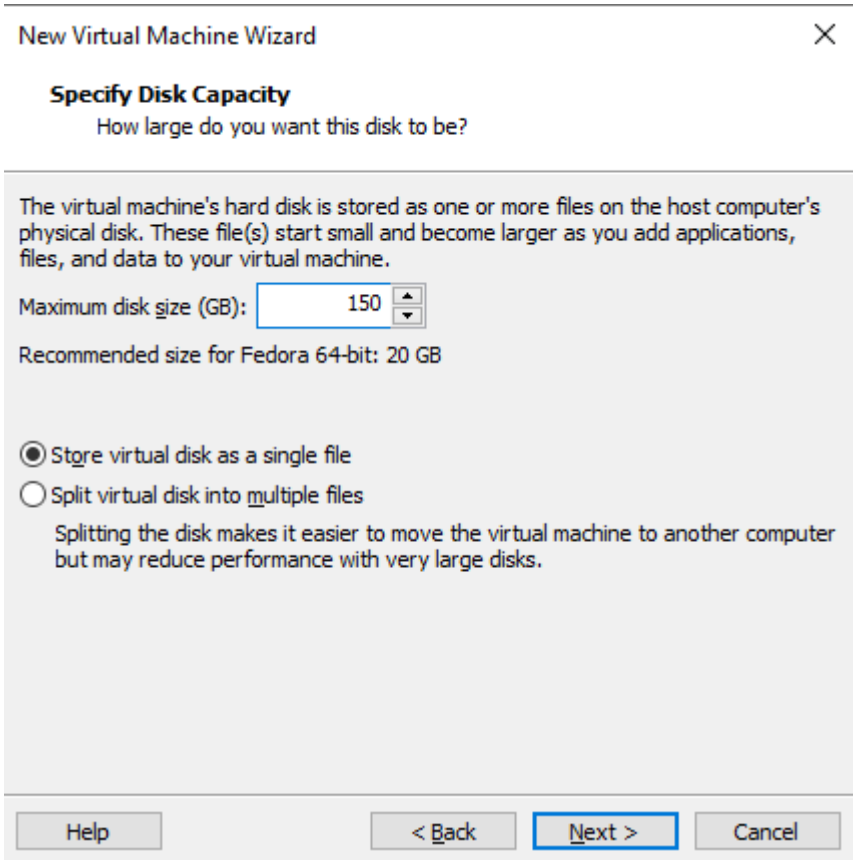
3. Выберите гостевую операционную систему **Linux** и в раскрывающемся списке укажите тип **Fedora 64-bit**:



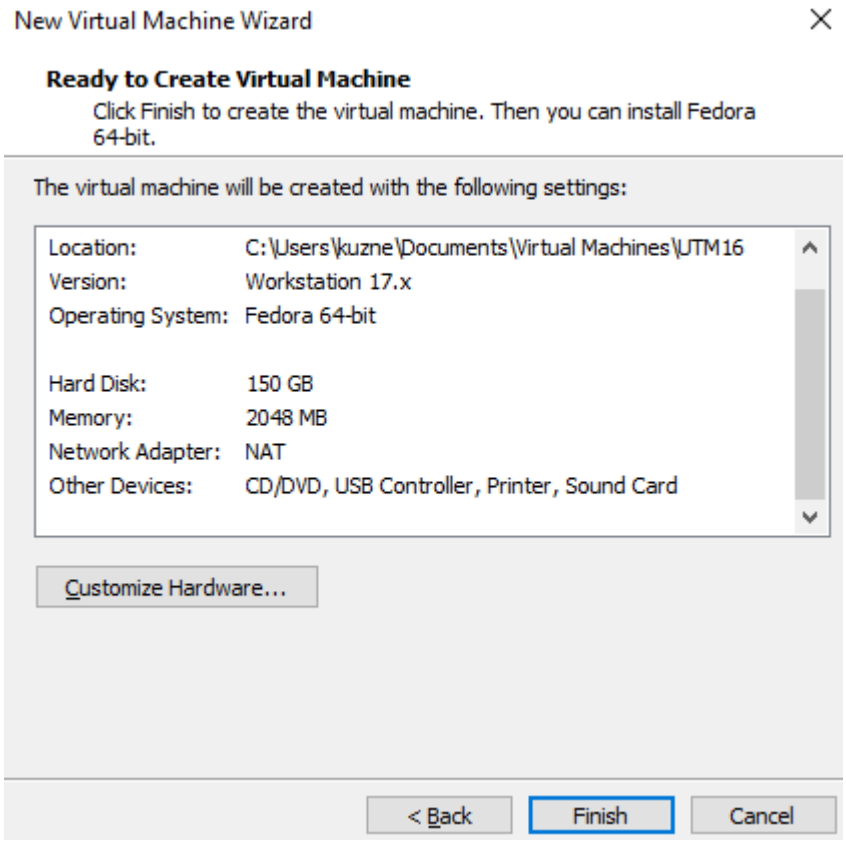
4. Укажите имя виртуальной машины и директорию для создания виртуального диска:



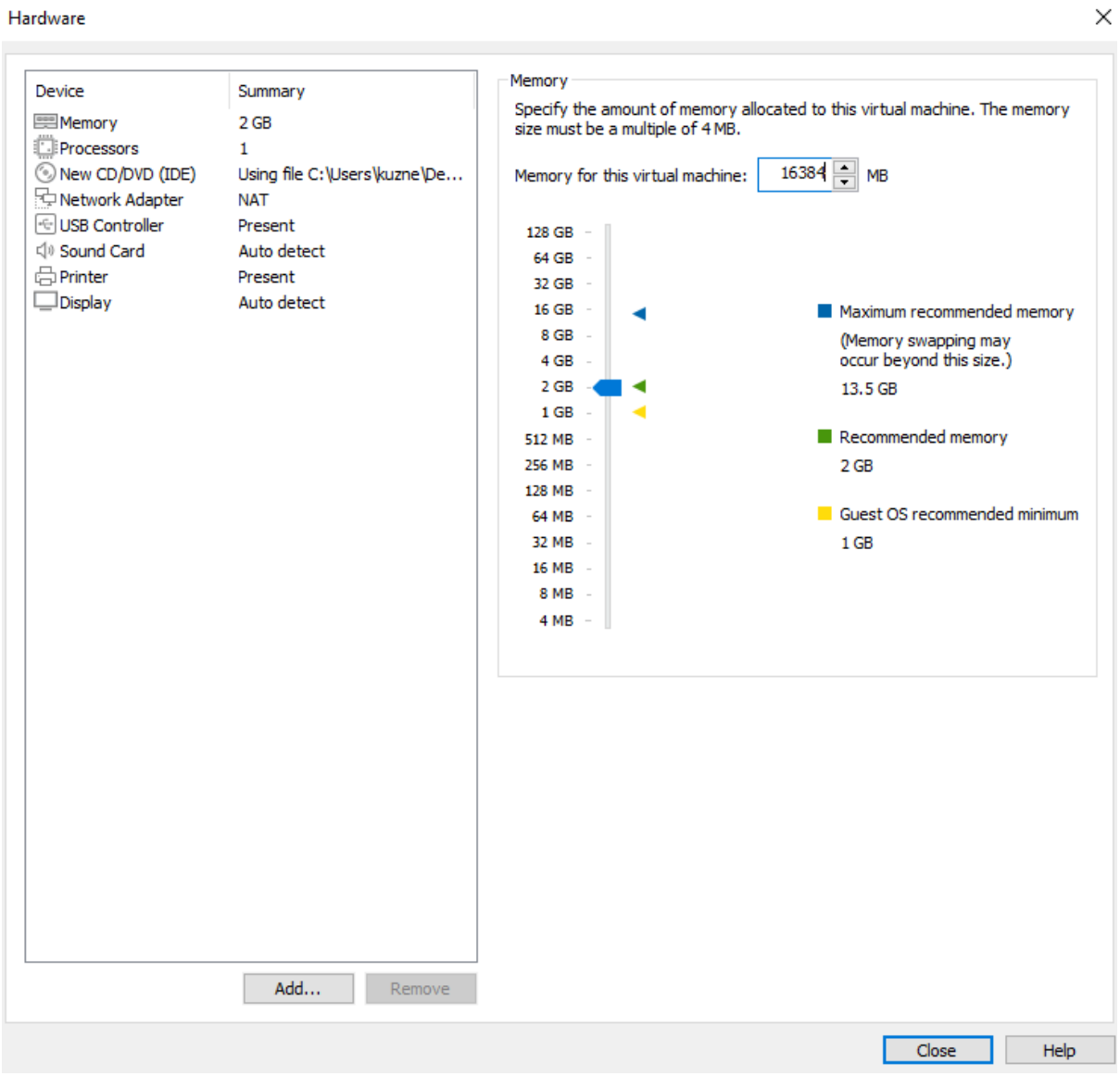
5. Укажите размер вирутального жесткого диска **150ГБ**:



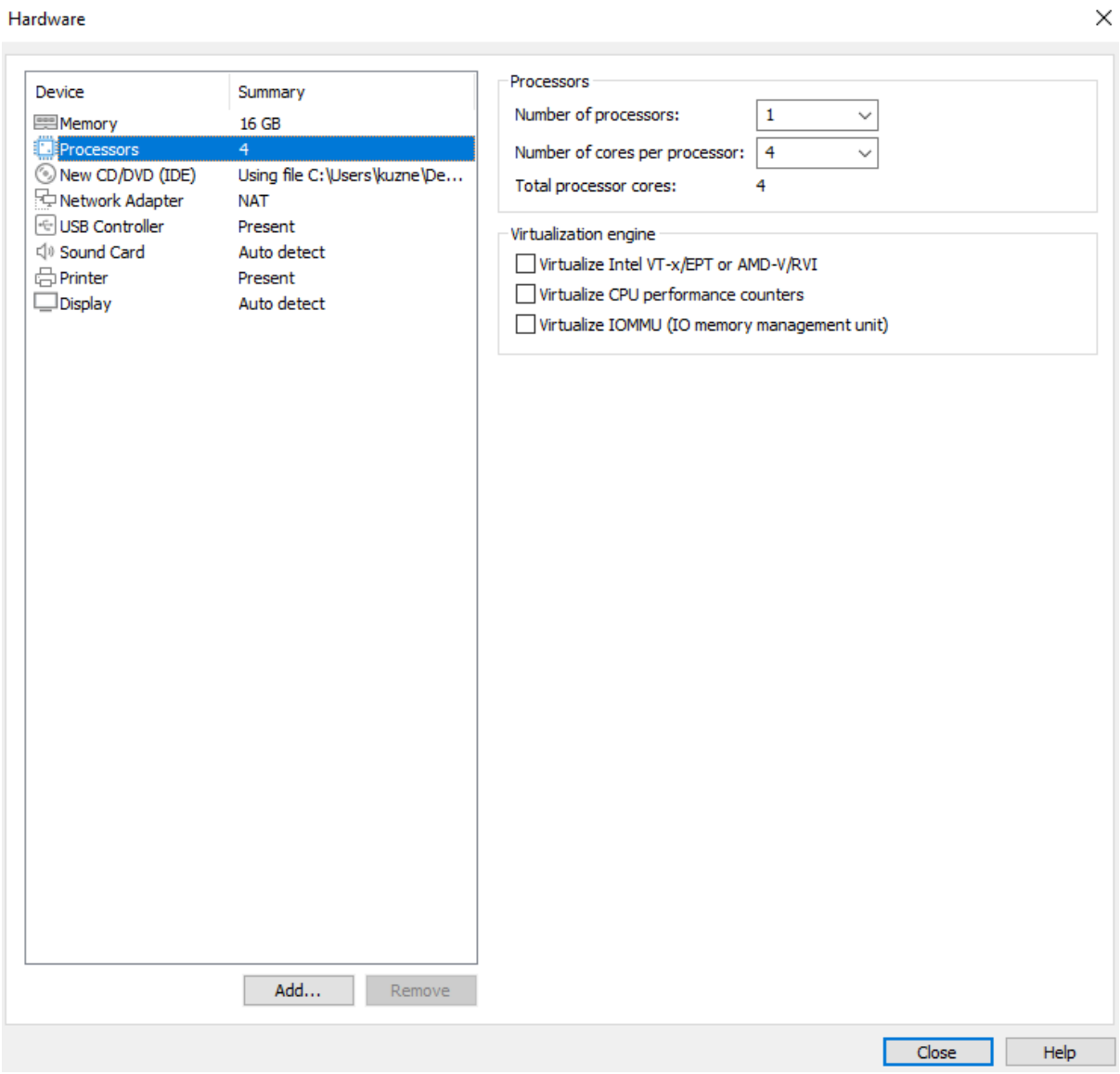
6. Выберите **Customize Hardware** для изменения настроек виртуальной машины:



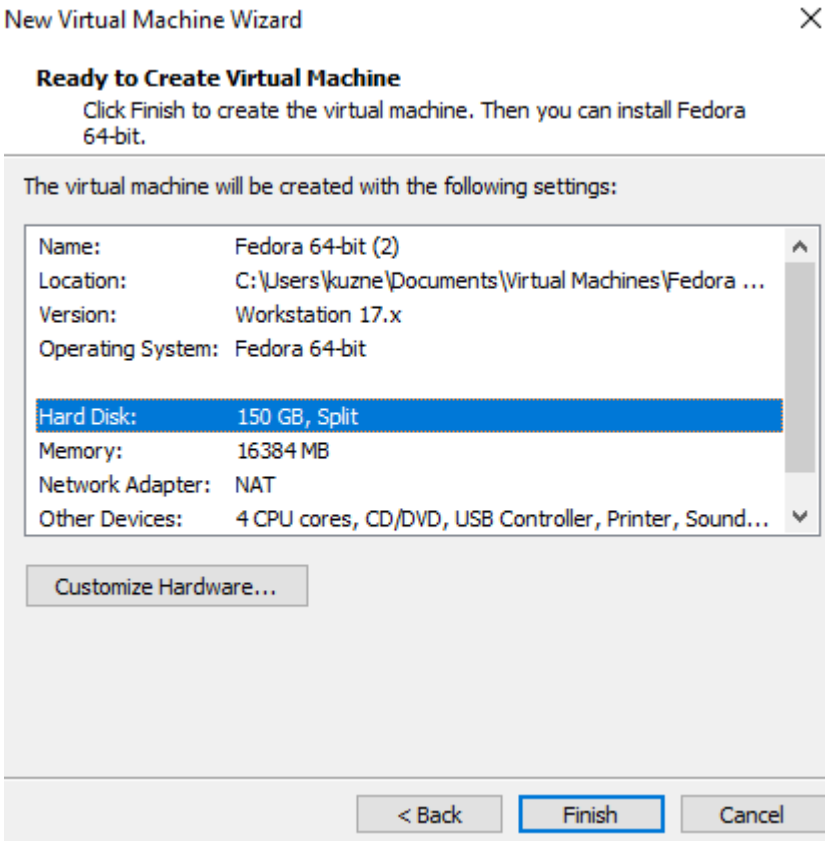
7. Укажите размер виртуальной оперативной памяти **16384МБ**:



8. Укажите количество ядер процесса равное 4:



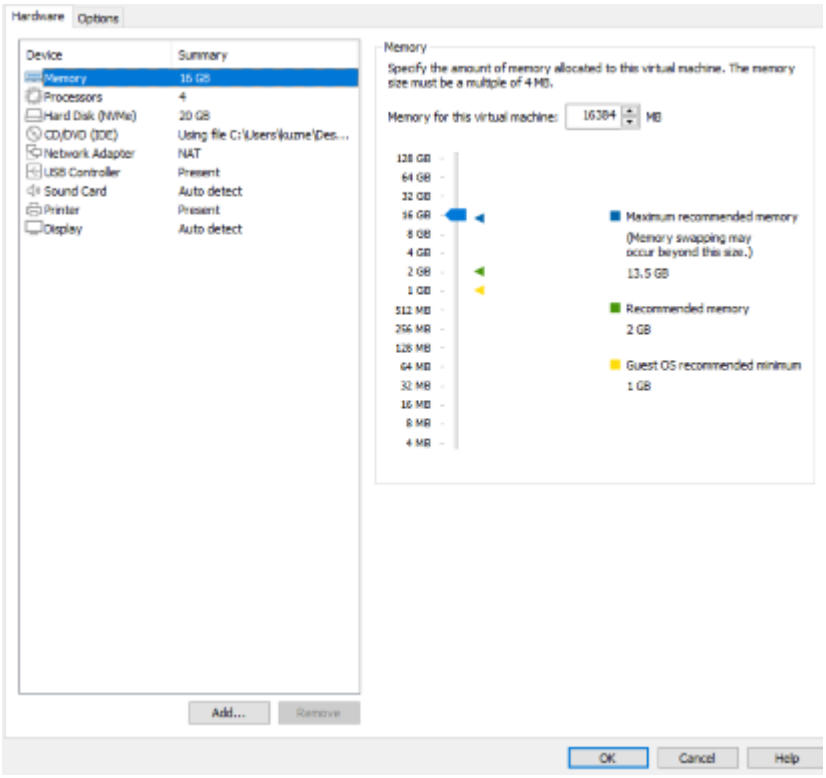
9. Выйдите из меню и нажмите **Finish** для окончания настройки:



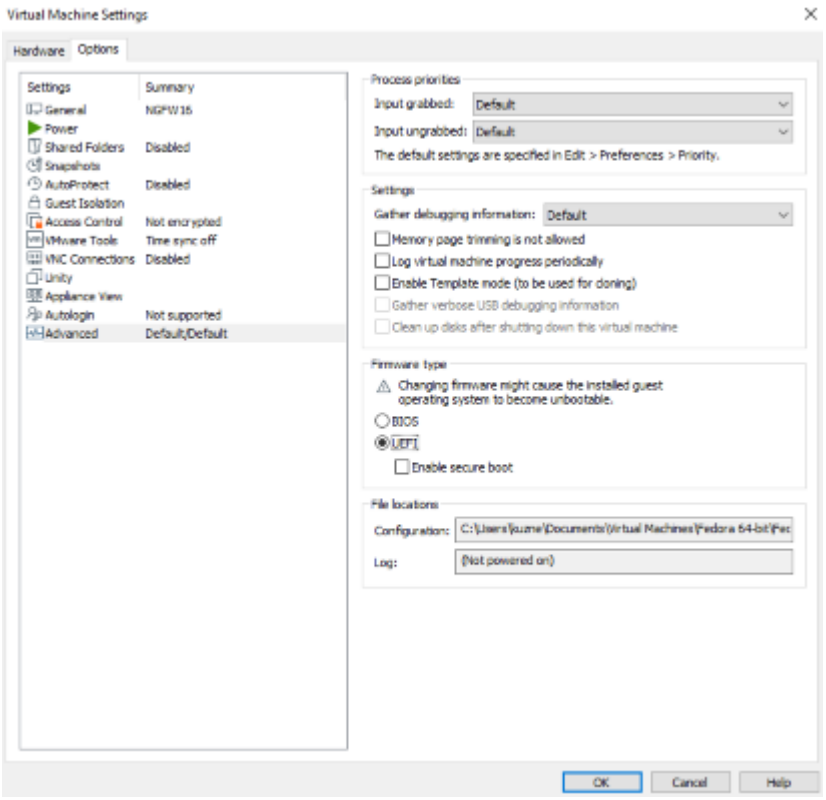
10. Перейдите в окно виртуальной машины и нажмите **Edit virtual machine settings**:



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.

8.2.5 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
```

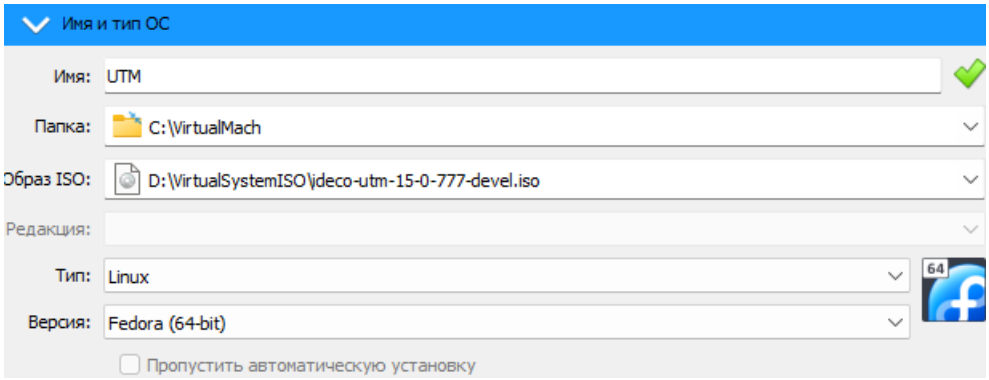
После 3 шага начнется загрузка с установочного носителя.

8.2.6 VirtualBox 7.0.12

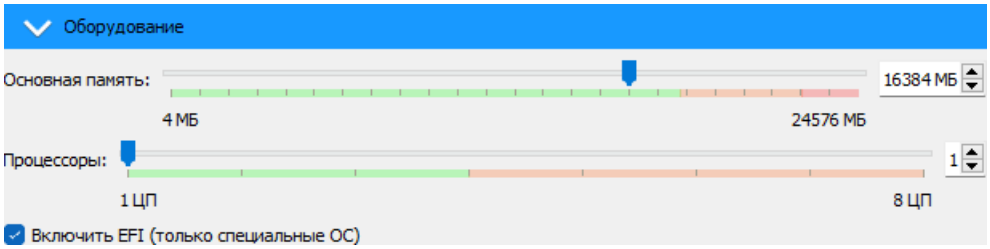
- По умолчанию при создании виртуальной машины создается 1 сетевая карта с типом подключения **NAT**.

Настройка:

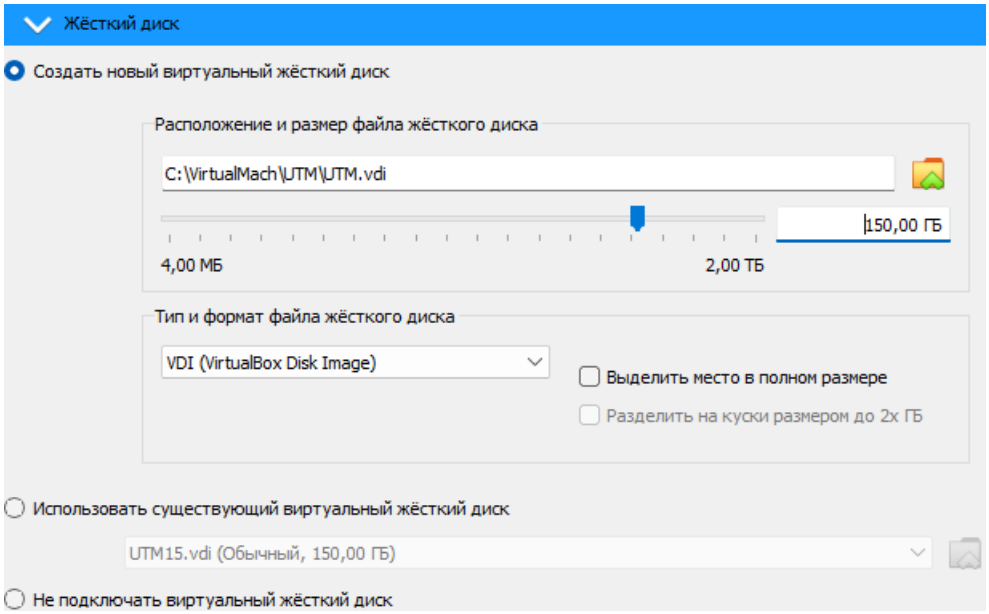
1. Укажите **Имя** виртуальной машины (ВМ), выберите директорию для ВМ и установите путь до загрузочного образа NGFW. Остальные параметры установите как на скриншоте:



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



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



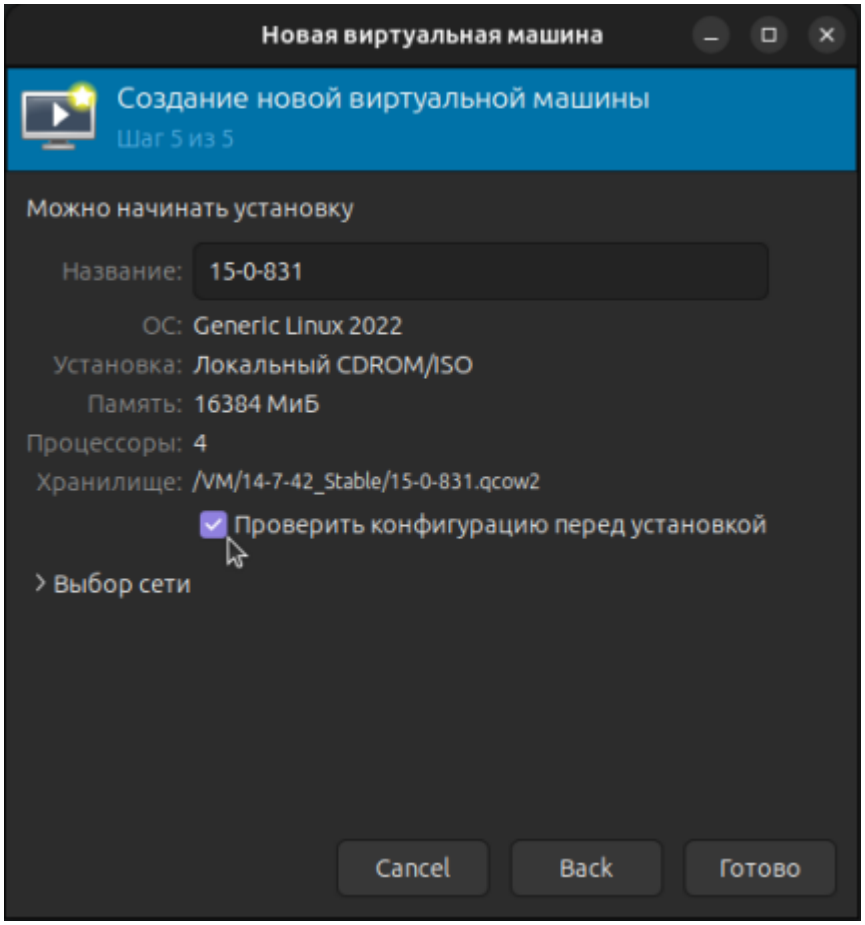
4. Нажмите **Готово**

8.2.7 KVM

Настройка:

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

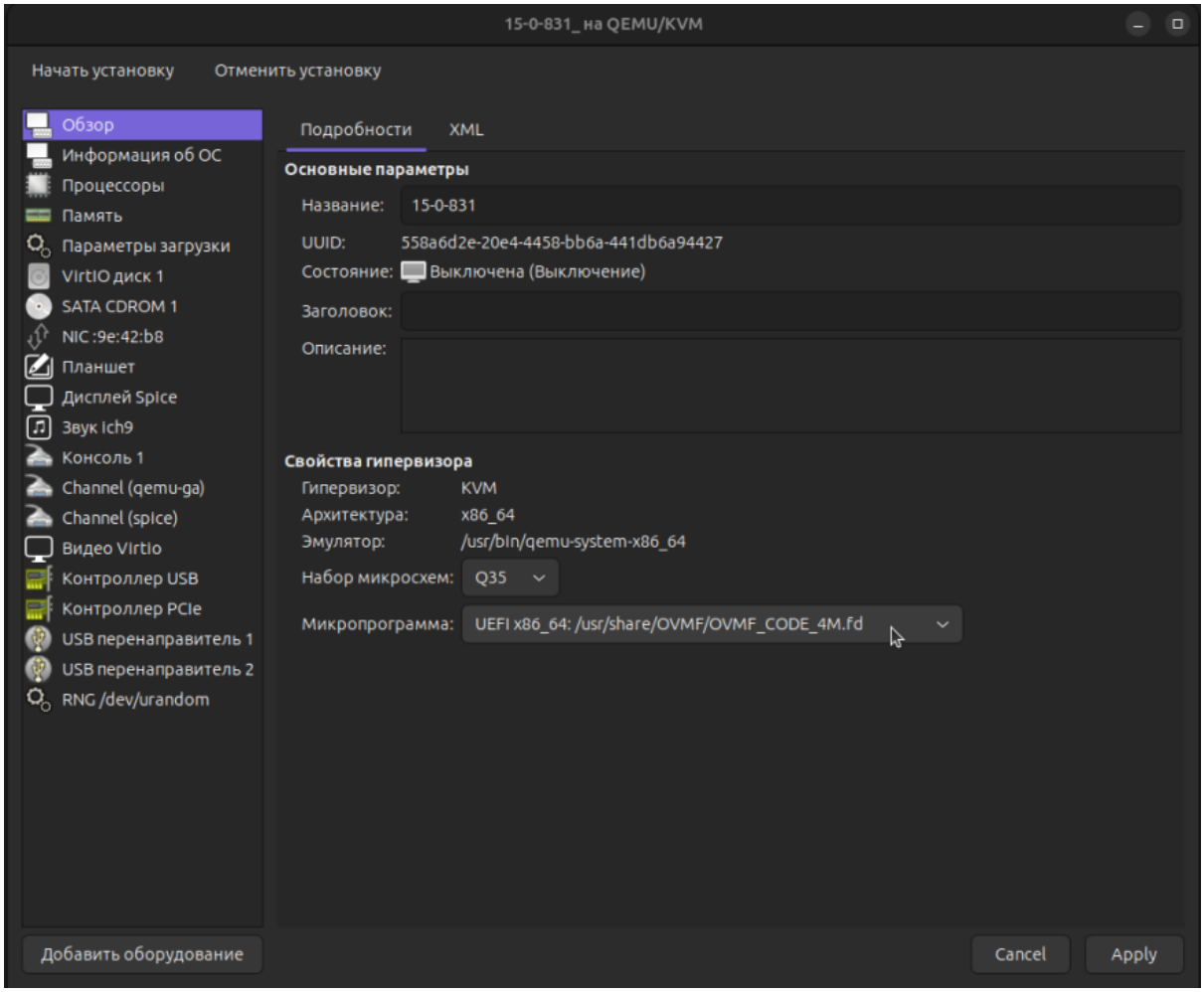
2. На пятом шаге (virtm-manager) установки обязательно включите опцию **Проверить конфигурацию перед установкой** и нажмите кнопку **Готово**.



3. Для дисков и сетевых карт измените интерфейс на **virtio.**

4. Выберите режим кеширования. Если диски имеют формат qcow2 или raw, используйте **writeback**. Если используется другой формат дисков, проконсультируйтесь у своего системного администратора или в нашей технической поддержке.

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



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

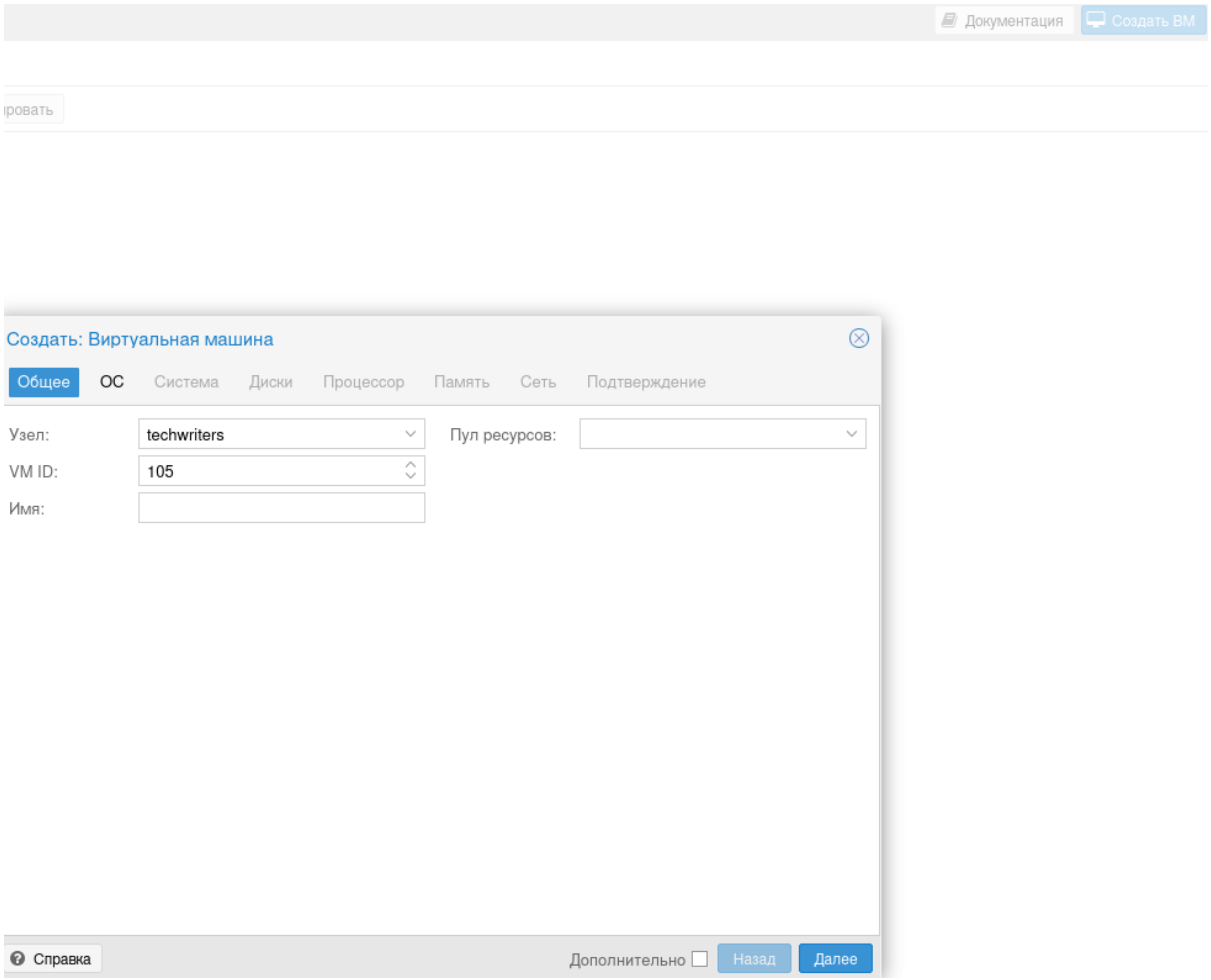
8.2.8 Proxmox

Подсказка: Видеоинструкцию по установке Ideco NGFW на Proxmox смотрите по ссылкам:

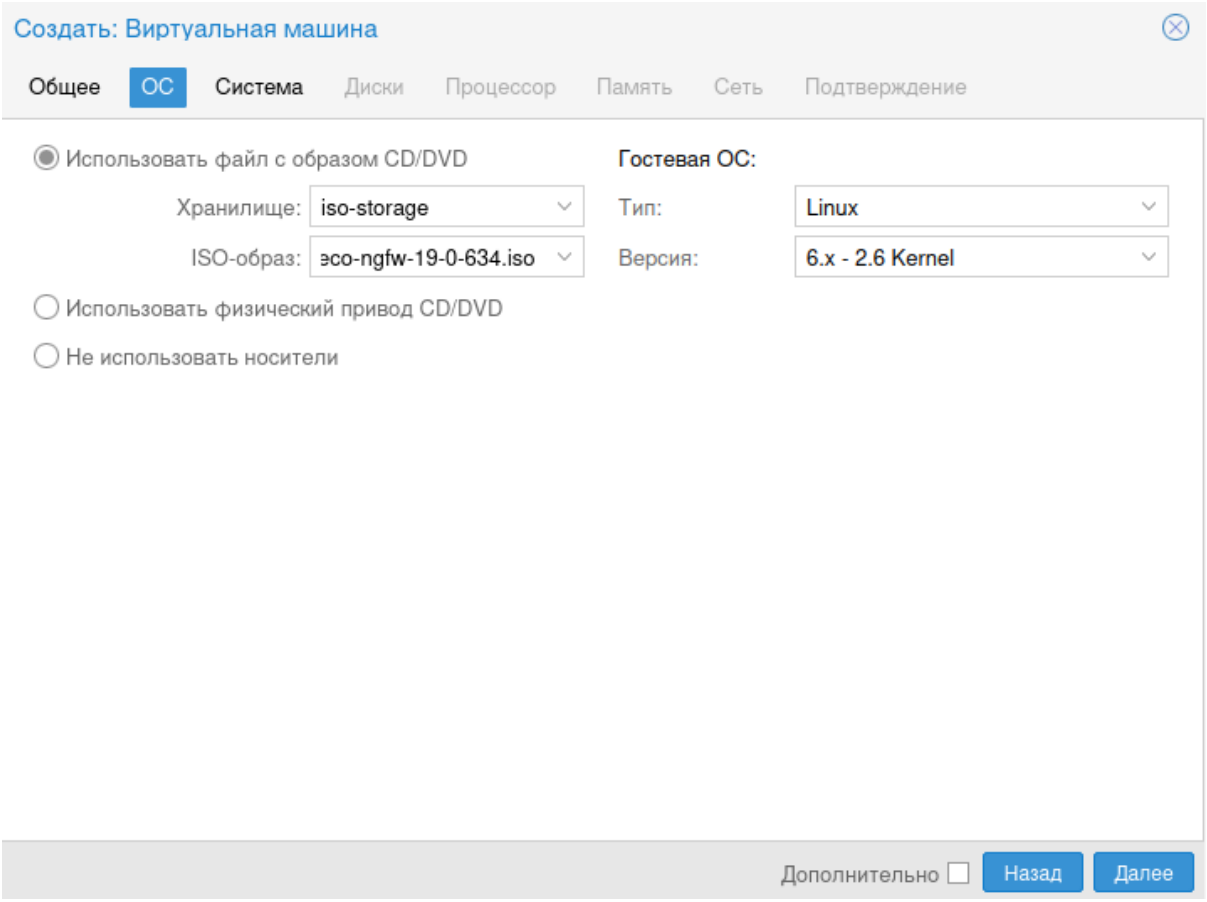
- Rutube
- Youtube

Настройка:

1. Нажмите **Создать ВМ**, введите имя машины:

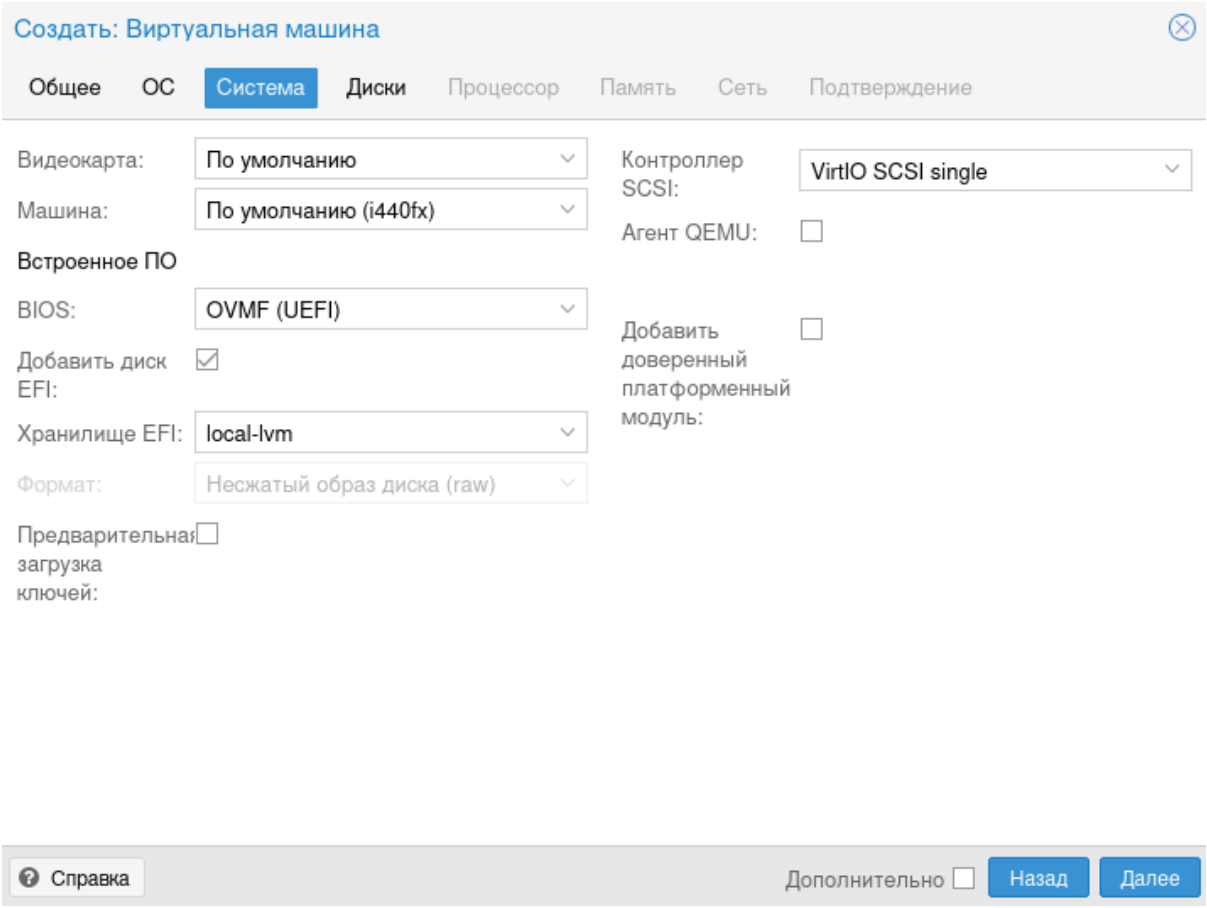


2. В разделе **ОС** выберите хранилище и заполните поля:



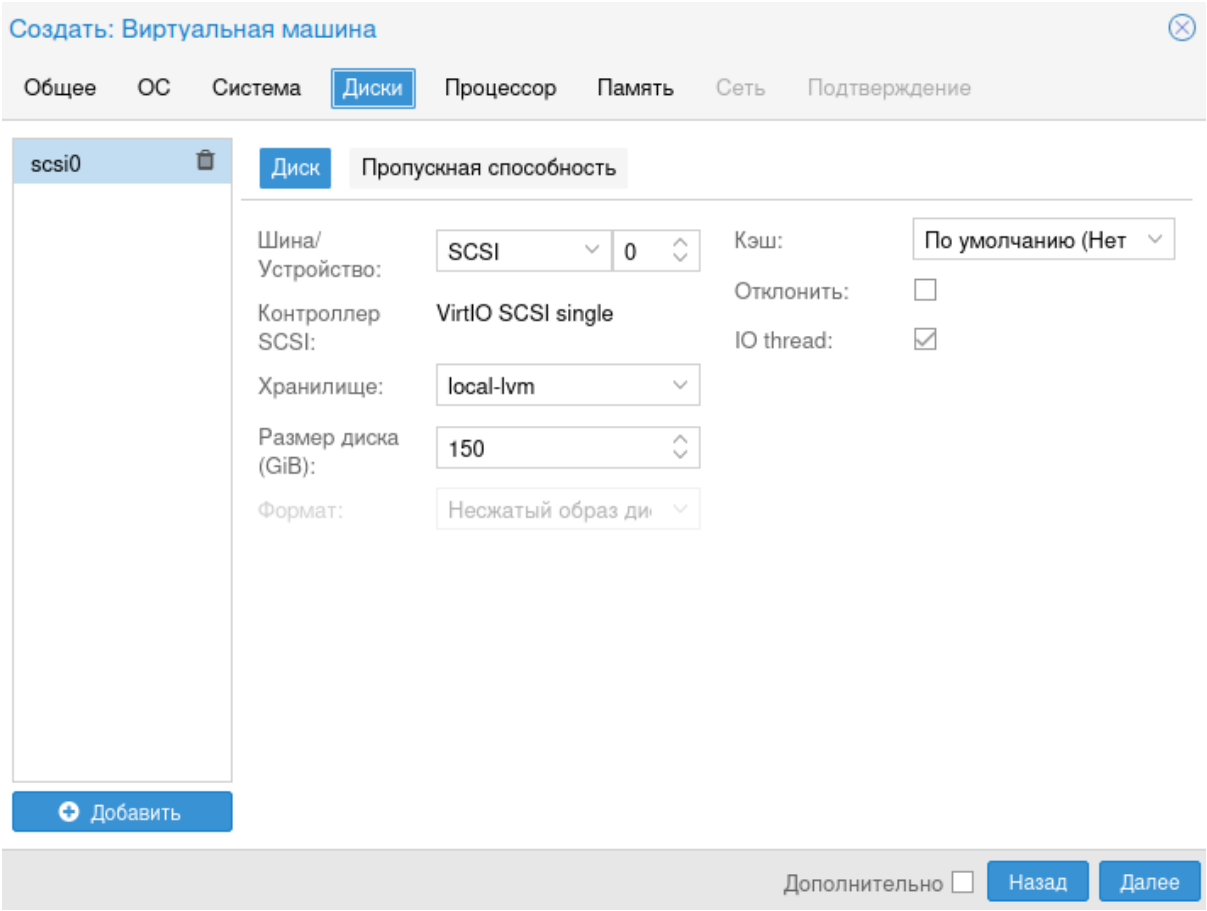
- **ISO-образ** - образ с нужной версией NGFW.
- **Гостевая ОС**:
  - **Тип** - Linux.
  - **Версия** - 6.x - 2.0 Kernel.

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



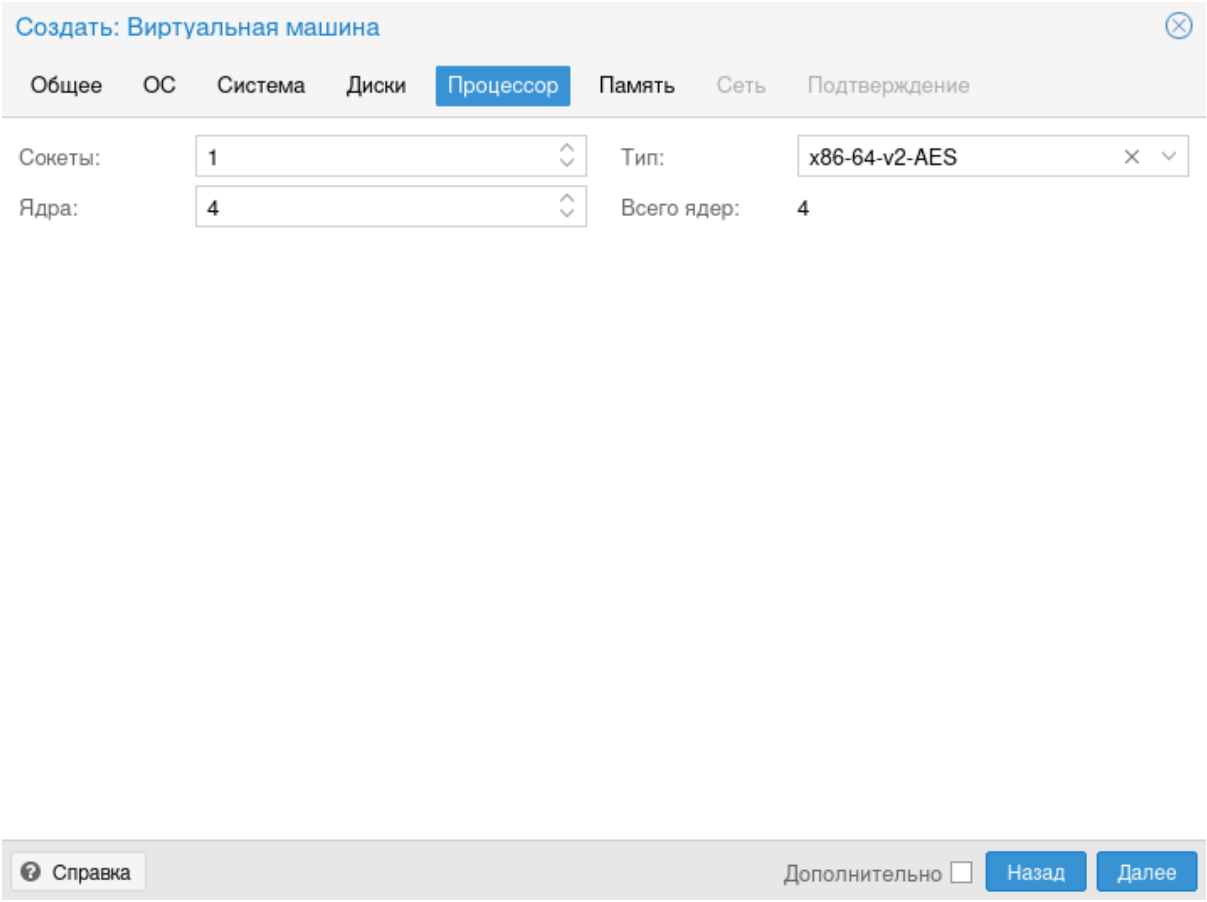
- **BIOS** - OVMF.
- **Хранилище EFI** - хранилище для UEFI-диска.
- **Предварительная загрузка ключей** - отключите опцию.

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

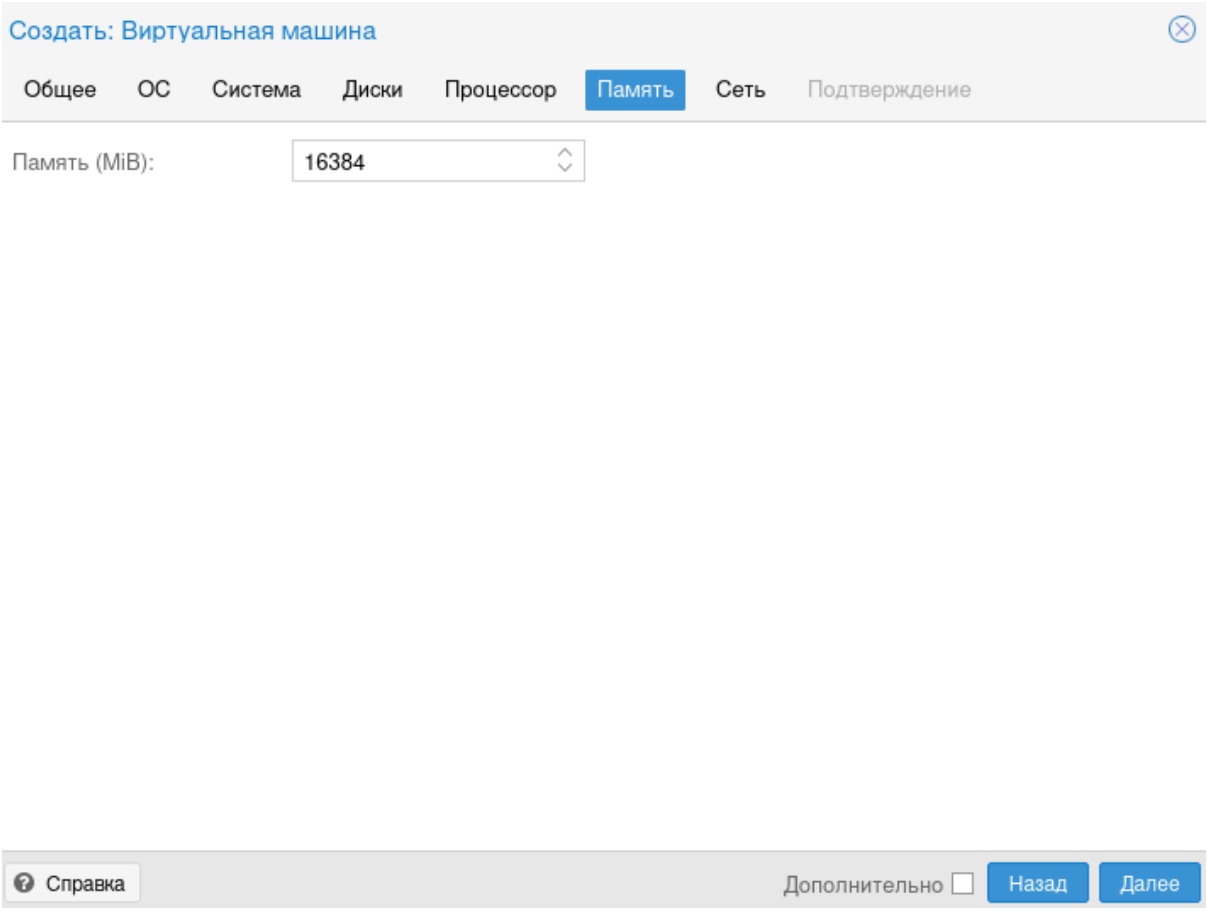


Проверьте свободное место на диске.

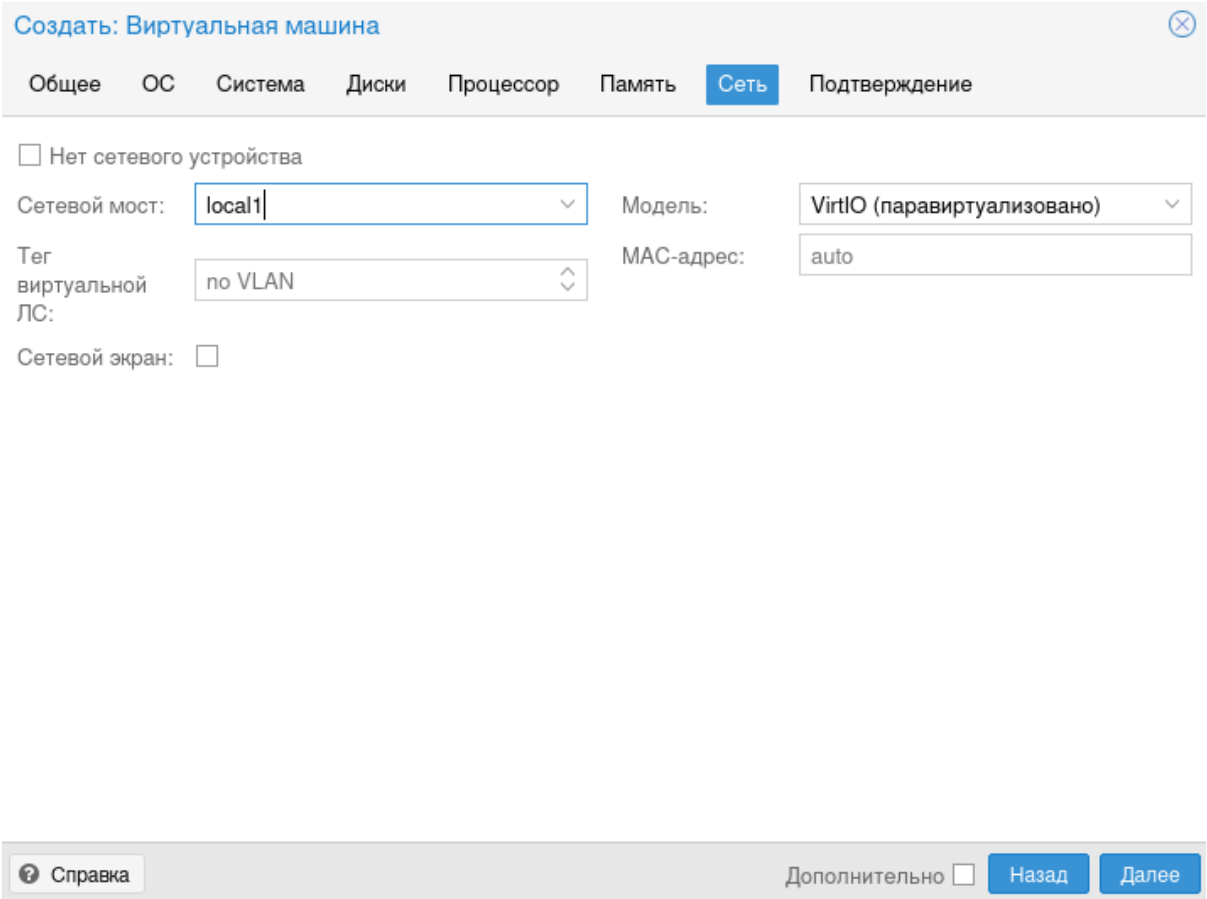
5. В разделе **Процессор** укажите количество сокетов и ядер (от четырех ядер) и выберите тип, который поддерживает SSE 4.2:



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

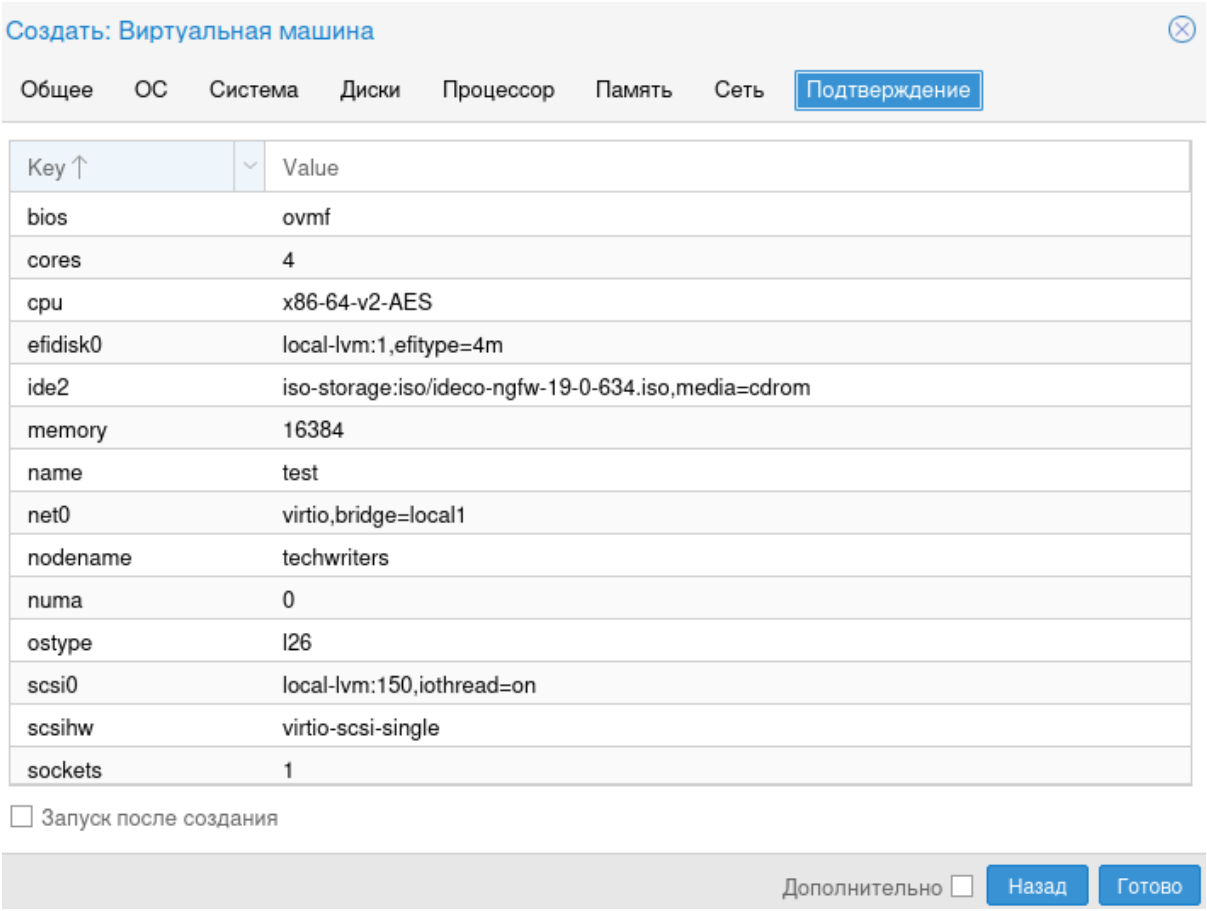


7. В разделе **Сеть** в поле **Сетевой мост** выберите сетевой мост для локального интерфейса:



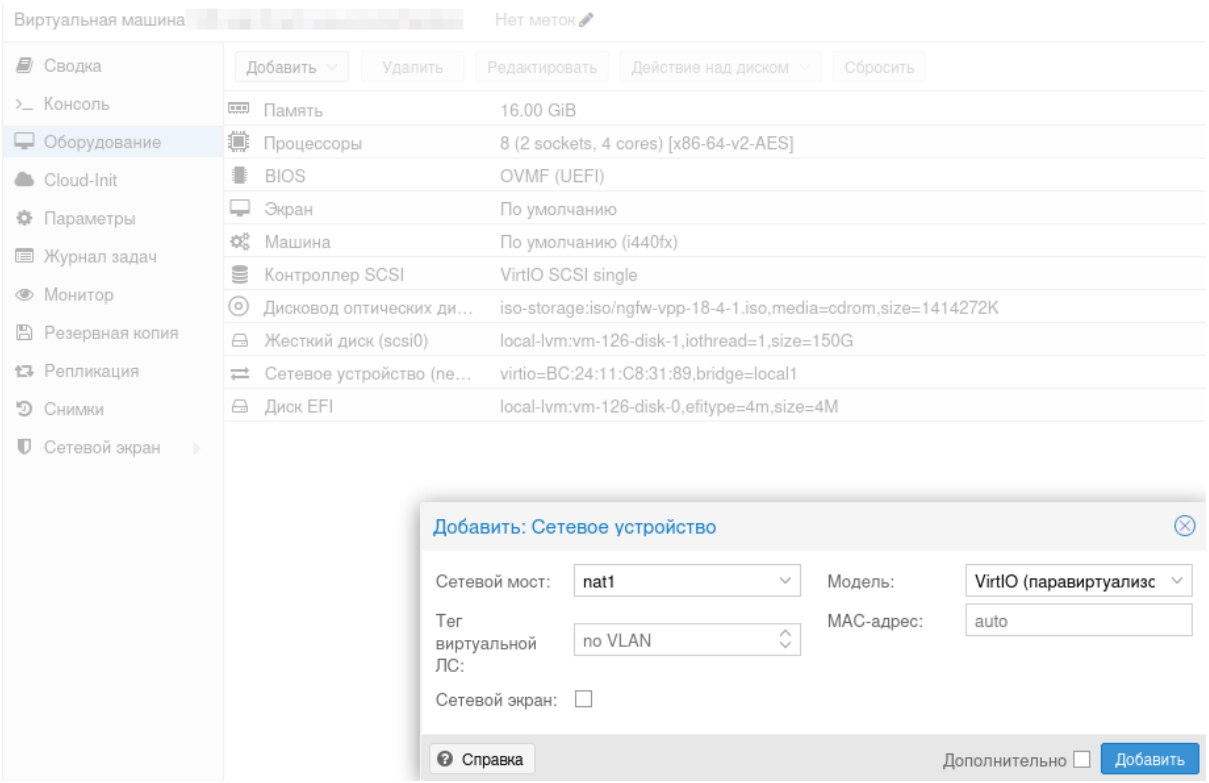
Рекомендуем отключить опцию **Сетевой экран**, чтобы облегчить настройку и отладку файрвола в Ideco NGFW и избежать конфликтов обработки трафика.

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



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

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



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*.

8.3 Подготовка загрузочного диска

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

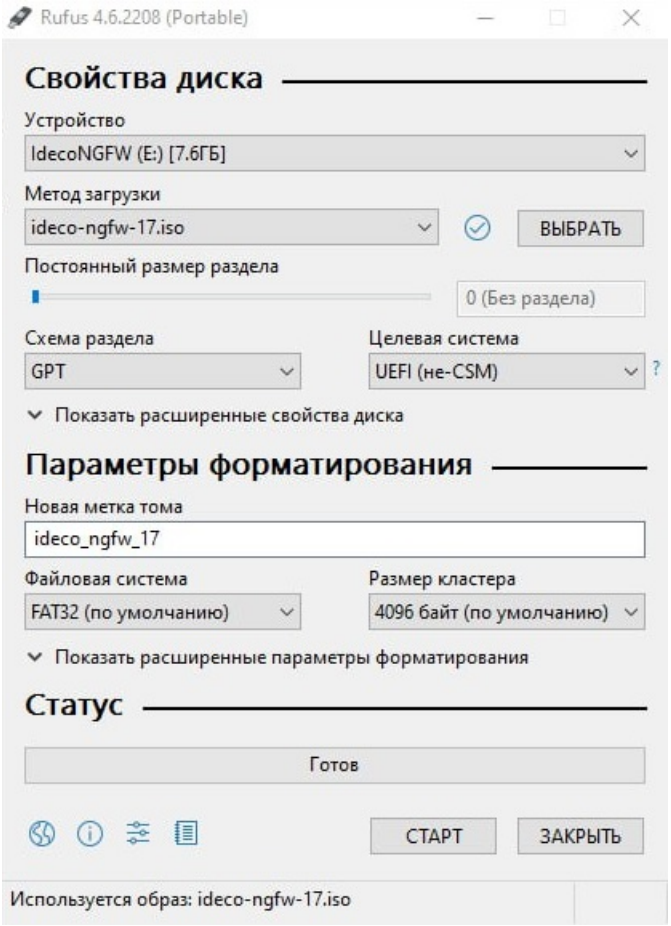
Подсказка: Подробнее об установке Ideco NGFW после создания загрузочного диска можно прочитать в статье *Установка*.

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

8.3.1 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**.

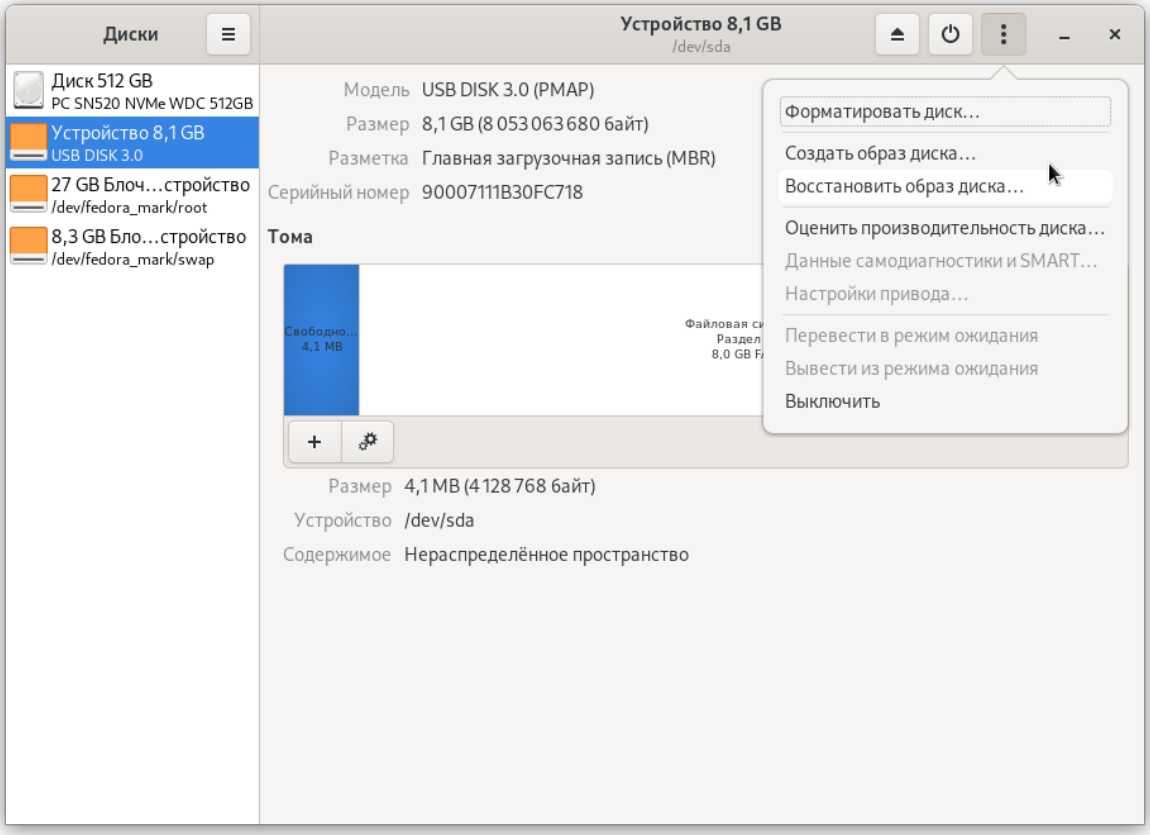
6. В диалоговом окне подтвердите запись на USB-диск.

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

8.3.2 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
```

9. Установка

9.1 Процесс установки

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

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

Для установки Ideco NGFW выполните действия:

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

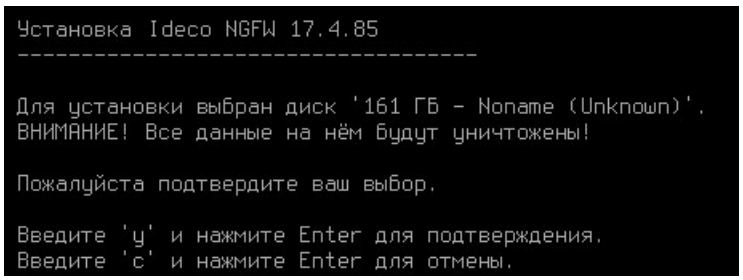


Внимание: При установке или загрузке сервера Ideco NGFW не рекомендуем нажимать на клавиатуре:

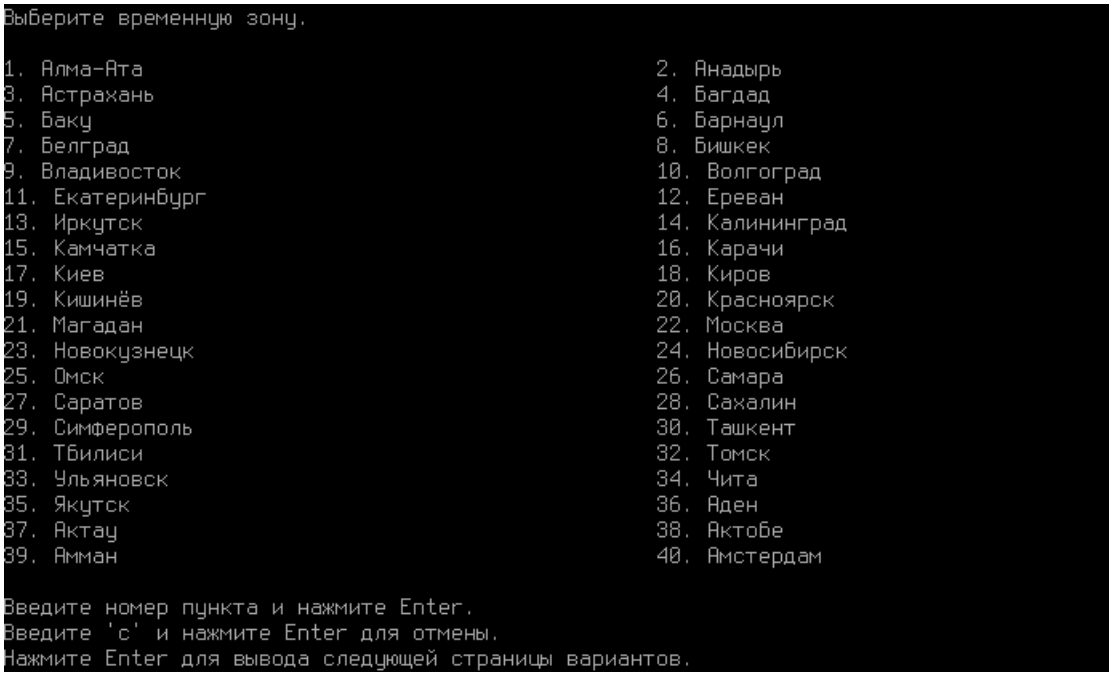
- \- - нажатие кнопки уменьшает количество секунд в таймауте и может привести к отключению таймера;
- \+ - нажатие кнопки увеличивает количество секунд в таймауте.

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

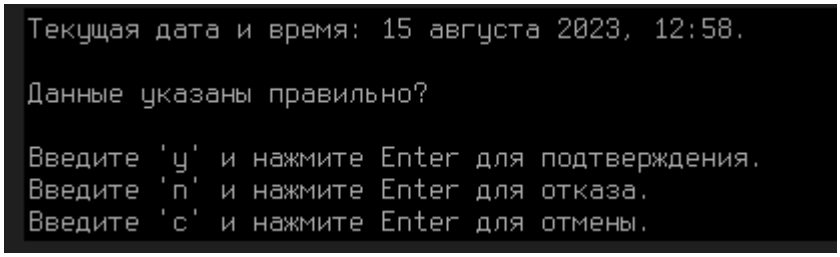
2. Выберите диск и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой вы находитесь:



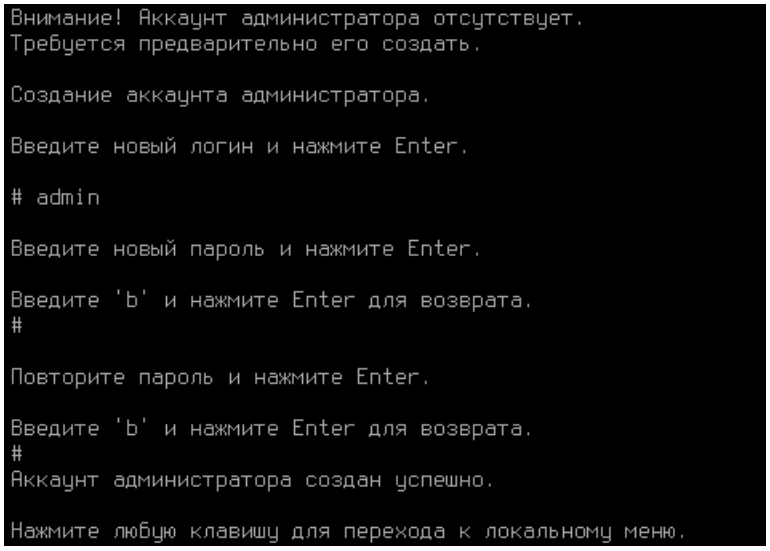
4. Настройте дату и время в соответствии с вашей временной зоной. **Обязательно проверьте правильность даты и времени**:



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

9.2 Создание учетной записи администратора

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



Требования к паролю:

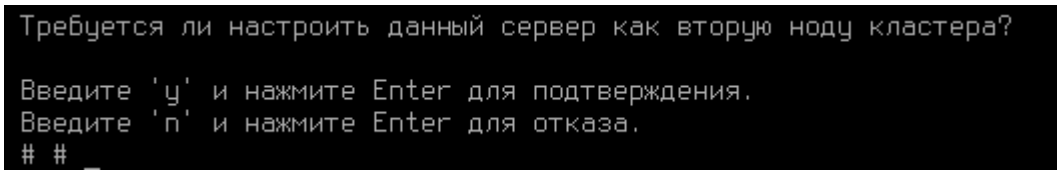
- **Минимальная длина пароля** - 12 символов;
- **Содержит строчные и заглавные латинские буквы**;
- **Содержит цифры**;
- **Содержит специальные символы** (! # $ % & „ * + и другие).

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

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

9.3 Настройка второй ноды кластера

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



2. Для продолжения настройки воспользуйтесь статьей *Кластеризация*.

9.4 Настройка локального интерфейса

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

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

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:

- 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.

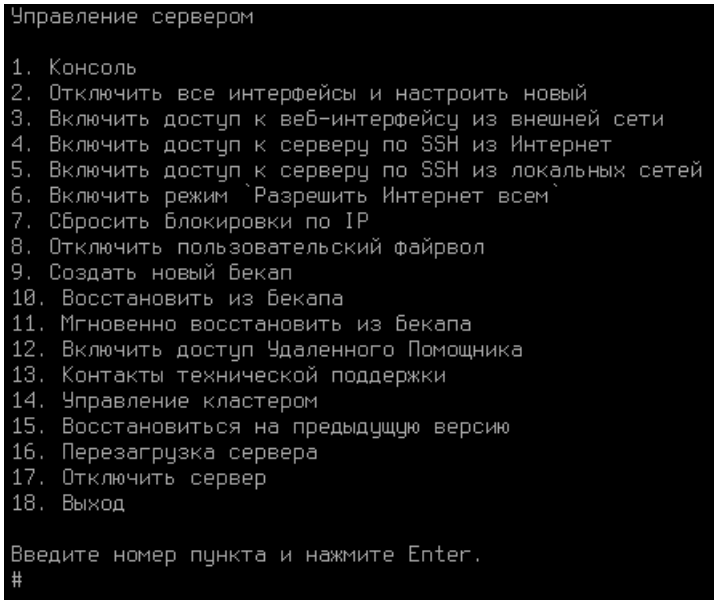
Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# 10.10.0.1
```

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*.

10. 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.

10.1 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`

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

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

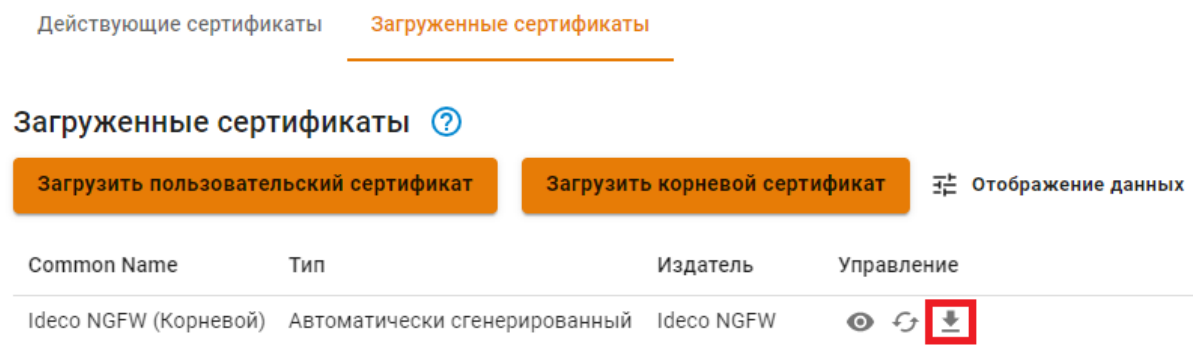
10.2 Импорт корневого сертификата NGFW в браузер

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

**

Из раздела Сервисы:**

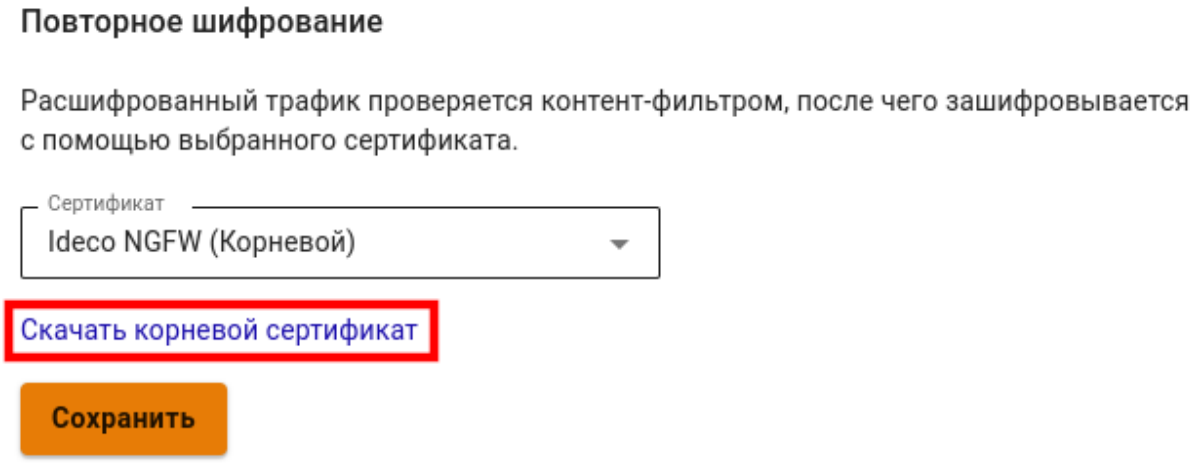
В разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** нажмите на стрелку для скачивания:



**

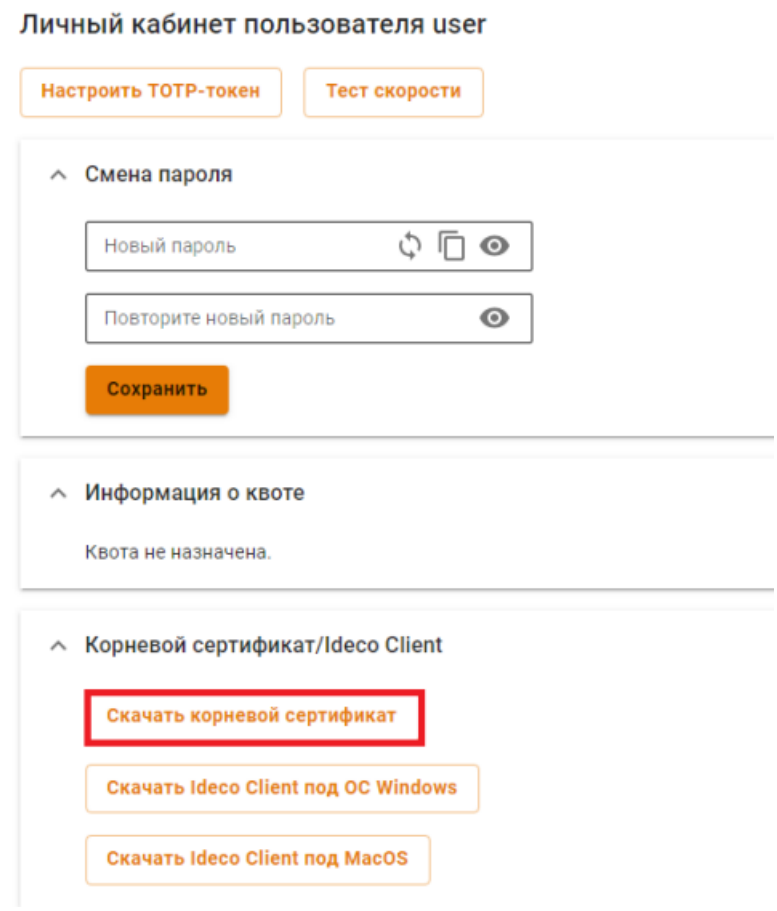
Из раздела Правила трафика:**

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



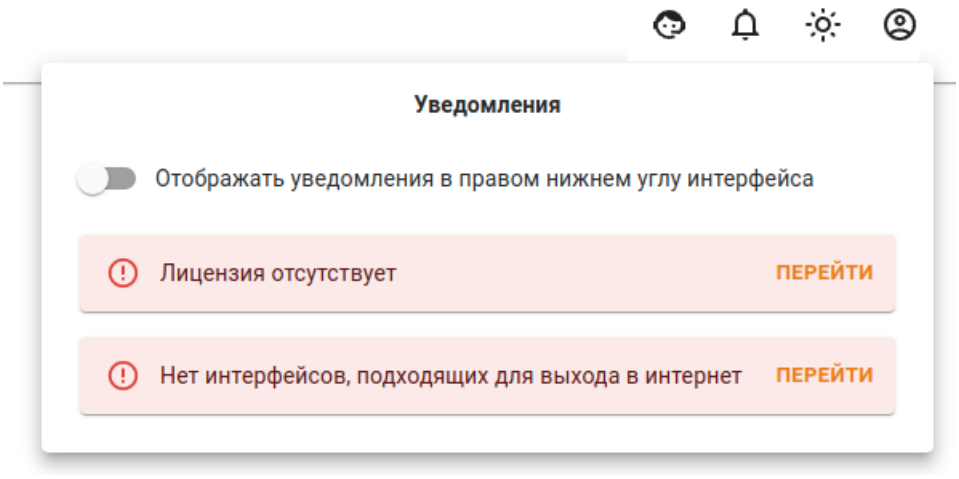
Из личного кабинета пользователя:

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



Для публикации личного кабинета пользователя воспользуйтесь *статьей*.

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



10.3 Настройка Ethernet-подключения

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

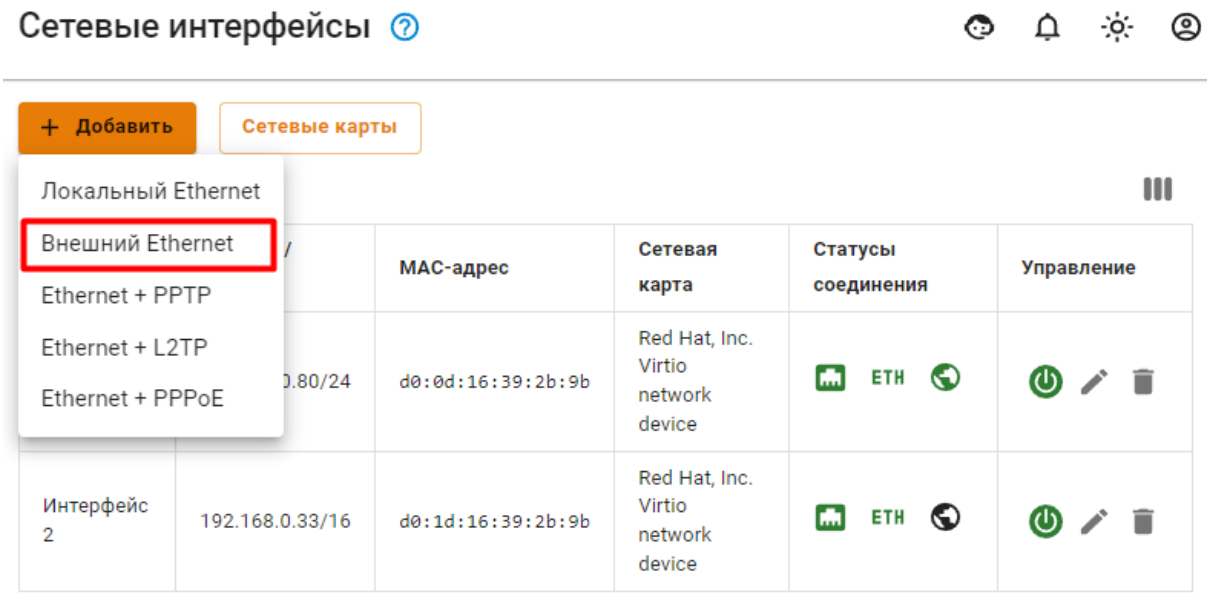
Параметр	Примечание
Сетевая карта	Необходимо указать сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру. Для идентификации адаптера ориентируйтесь на наименование производителя или MAC-адрес
IP-адрес и маска	Сетевые реквизиты, которые были назначены провайдером. Укажите 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 на иконку  в правом верхнем углу и выберите пункт **Внешний Ethernet**:

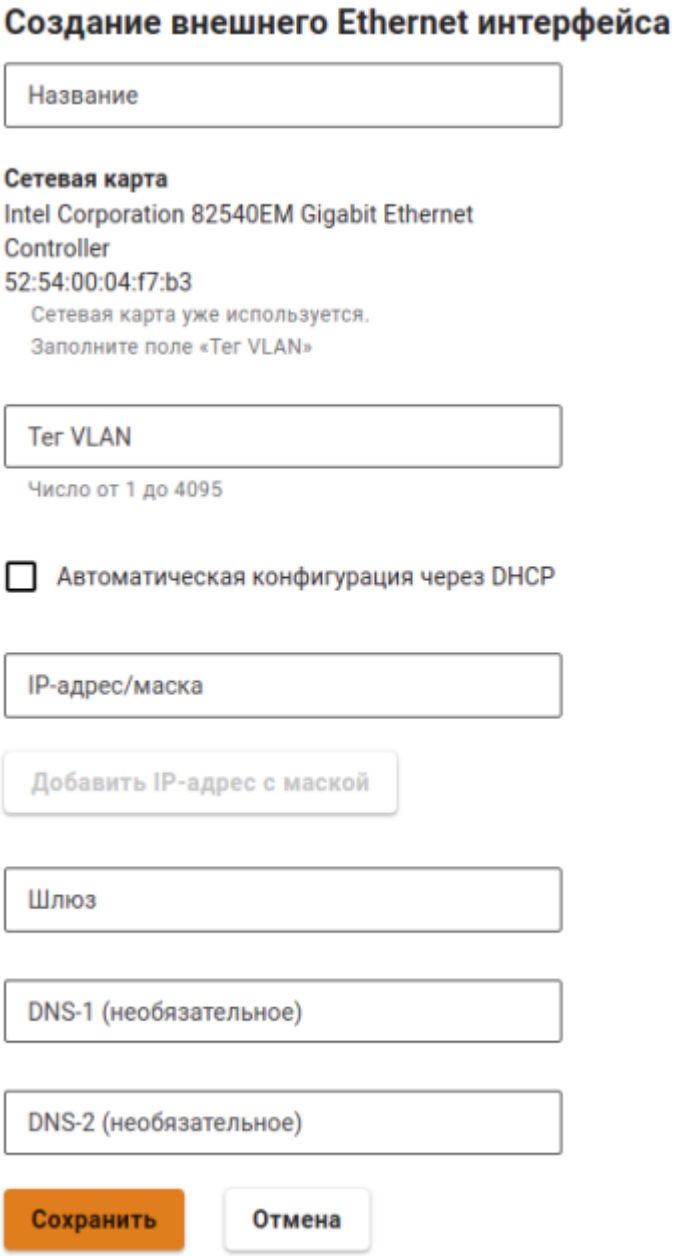


Внимание: Будьте внимательны!

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

3. Выберите подходящую сетевую карту.

4. Заполните 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**.

10.3.1 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*.

11. Регистрация сервера

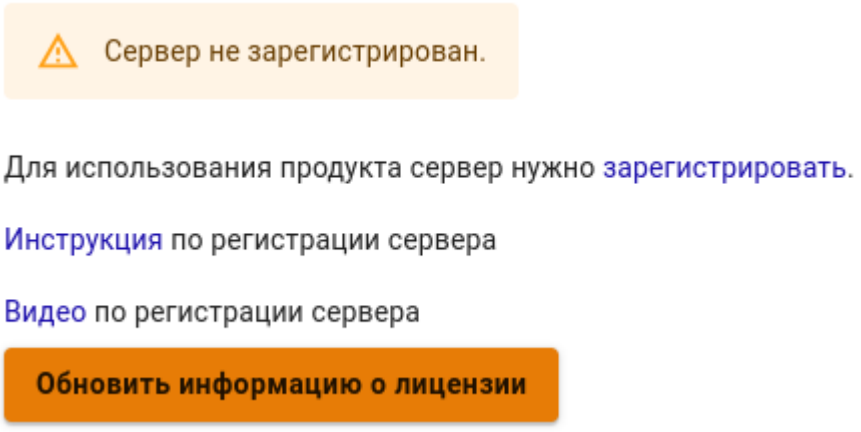
Подсказка: Для активации лицензии необходима обязательная регистрация сервера в личном кабинете.

11.1 Онлайн-регистрация

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

Шаги онлайн-регистрации сервера и привязки лицензии:

1. Перейдите в веб-интерфейс Ideco NGFW в раздел **Управление сервером -> Лицензия** 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.

11.2 Офлайн-регистрация

Подсказка: С выходом Ideco NGFW версии 18 процедура офлайн-регистрации и обновления стала более удобной. Рекомендуем обновить NGFW до последней версии, чтобы воспользоваться всеми преимуществами улучшенной процедуры.

11.2.1 Привяжите сервер к личному кабинету в MY.IDECO. Для этого:

1. Перейдите в веб-интерфейс Ideco NGFW в раздел **Управление сервером -> Терминал**.

2. Выполните команду `cat /usr/share/ideco/license-backend/hwid` и скопируйте **HWID** сервера. Пример: `t7m7H137w-pQXYjXuHmYbLnJw3YyxJAg5wl9FfARlh`.

3. Выполните команду `cat /usr/share/ideco/version.json` и скопируйте Json-объект с версией сервера, например:

```
{"major": 17, "minor": 5, "build": 102, "timestamp": 1724427324, "vendor": "Ideco",
↪"product": "UTM", "kind": "STANDARD", "release_type": "release"}
```

4. Сформируйте ссылку на регистрацию сервера и перейдите по ней на устройстве с доступом в интернет:

```
https://my.ideco.ru/ngfw?server_name=<название сервера (доступно в левом верхнем углу␣
↪веб-интерфейса)>&version=<Json-объект с версией сервера>&hwid=<HWID, полученный в␣
↪пункте 2>
```

Пример ссылки на регистрацию:

```
https://my.ideco.ru/ngfw?server_name=Без названия 23000007-c6c1-3d58-9da2-
↪40ea5128aab5&version={"major": 17, "minor": 5, "build": 102, "timestamp":␣
↪1724427324, "vendor": "Ideco", "product": "UTM", "kind": "STANDARD", "release_type
↪": "release"}&hwid=sGs6OYW2XRm_aK9PRwifKnej3V8YUVw69dtKVkIoPEnD
```

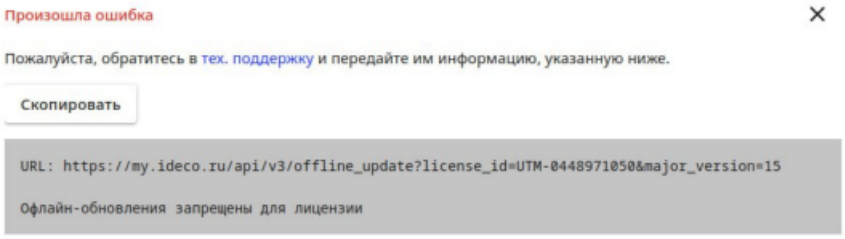
Предупреждение: Не используйте спецсимволы в названии сервера Ideco NGFW, они могут быть некорректно закодированы при переходе по ссылке на регистрацию сервера.

11.2.2 Привяжите к серверу лицензию:

1. Обратитесь к вашему менеджеру для предоставления лицензии.

2. 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:



3. Сформируйте ссылку на скачивание баз и лицензии, перейдите по ней на устройстве с доступом в интернет:

```
https://my.ideco.ru/ngfw?offline-updates&version=<Json-объект с версией сервера>&hwid=
↪<HWID, полученный в пункте 2>
```

Пример ссылки:

```
https://my.ideco.ru/ngfw?offline-updates&version={"major": 17, "minor": 5, "build":␣
↪102, "timestamp": 1724427324, "vendor": "Ideco", "product": "UTM", "kind": "STANDARD
↪", "release_type": "release"}&hwid=sGs6OYW2XRm_aK9PRwifKnej3V8YUVw69dtKVkIoPEnD
```

4. Сохраните файлы лицензии и баз фильтрации, нажав на появившиеся ссылки:



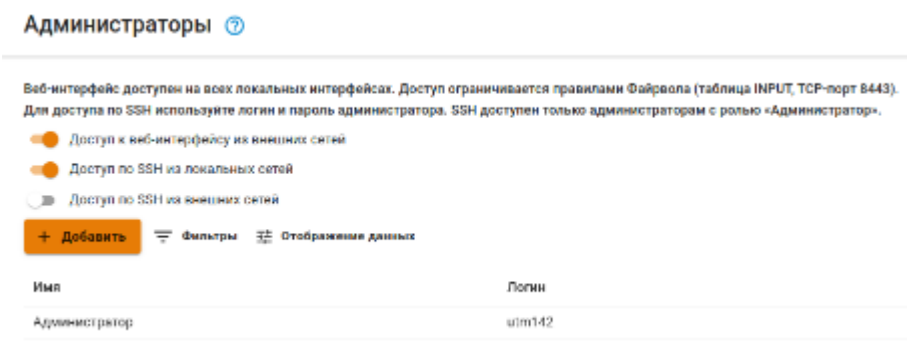
5. Сохраните скрипт для конвертации файлов в папку, в которую сохранили файлы на шаге 4:

6. Откройте терминал на устройстве и перейдите в каталог с помощью команды `cd ~/<название папки со скачанными файлами>`, а затем запустите скрипт командой `python convert.py`.

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/`.

  Для загрузки файла можно использовать команду `scp` или утилиту WinSCP. Чтобы получить доступ к серверу, активируйте возможность подключения к нему по SSH из локальной сети. Это можно сделать через веб-интерфейс в разделе **Управление сервером -> Администраторы**:



- Перезапустите сервис лицензий командой `systemctl restart ideco-license-backend.service`;

- Перейдите в раздел **Управление сервером -> Лицензия** и убедитесь, что лицензия установлена.

11.3 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 `converted` вместе с конвертированными файлами, полученными на шаге 5:

2. Обновите базы модулей безопасности:

- Перенесите папку со скачанными файлами баз на NGFW - `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 ideco-geoip.mmdb`;
  - Базы соответствия подсетей и стран - `python3 iplist.py iplist.tar.gz`;
  - Правила фильтрации модуля **Предотвращение вторжений** - `python3 suricata.py suricata-rules.tar`;
  - Базы модуля **Контент-фильтр** - `python3 content_filter.py sky-db-from-0.sst`.

12. Получение доступа в интернет

12.1 Основное

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

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

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

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

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

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

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

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

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

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

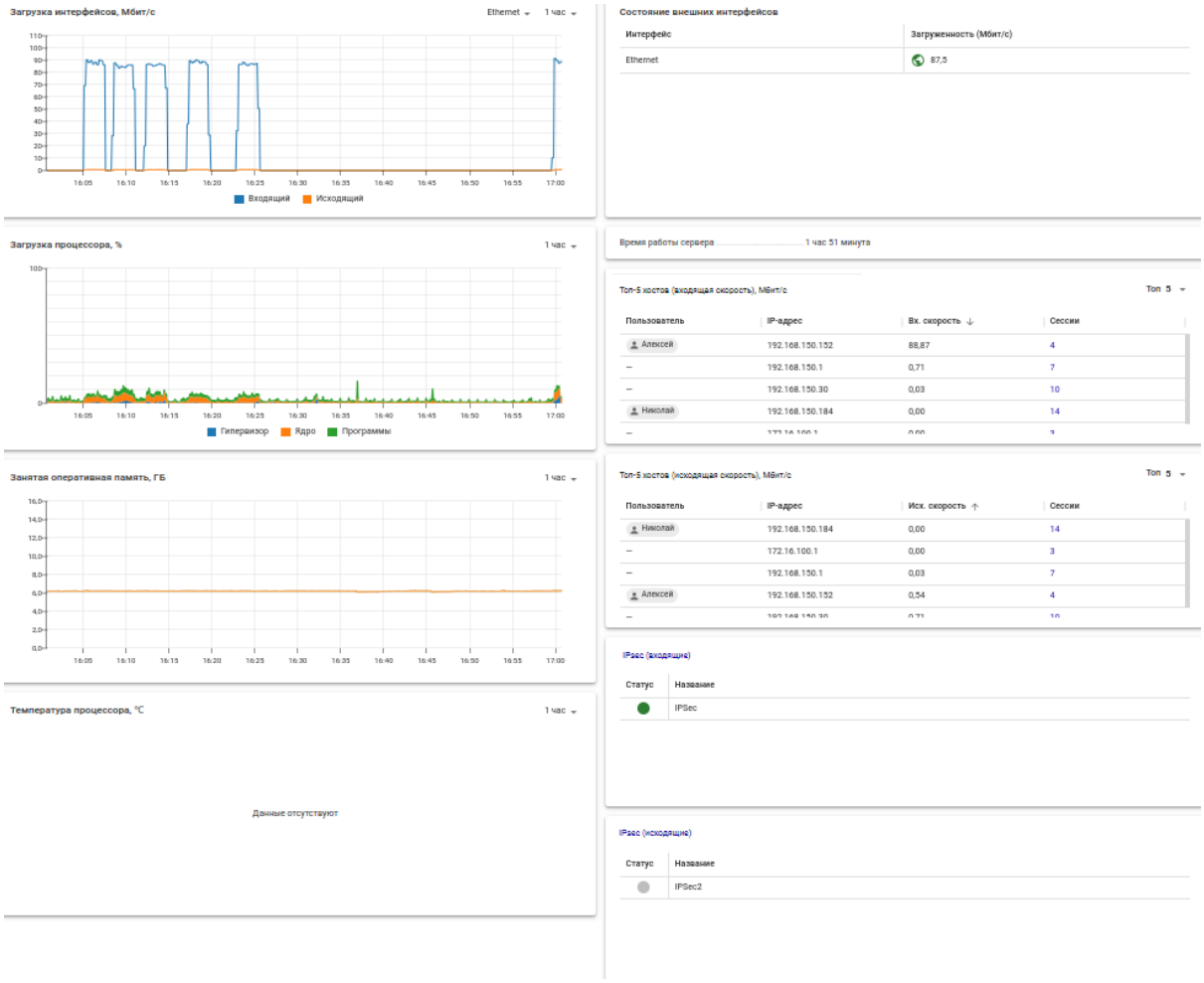
13. Панель мониторинга

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

Параметры модуля Панель мониторинга:

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

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



13.1 Особенности отображения информации:

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

14. Пользователи

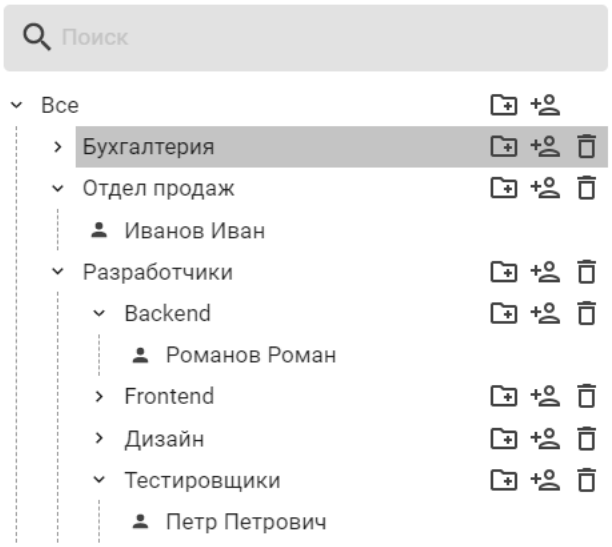
14.1 Учетные записи

14.1.1 Основное

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.

14.1.2 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

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

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

- **В определенной группе** - выберите группу, нажмите кнопку **Создать пользователя** на вкладке **Основное** или  рядом с названием группы в дереве:
- **Вне групп** - выберите группу **Все** в дереве пользователей и нажмите :

Логин необходимо вводить латинскими символами в нижнем регистре, например, i.ivanov.

При заполнении **Дополнительных настроек** будет создано соответствующее правило в карточке пользователя на 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 вам нужно будет 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 . Также можно выбрать нужного вам пользователя и нажать на кнопку **Удалить** на вкладке **Основное**:

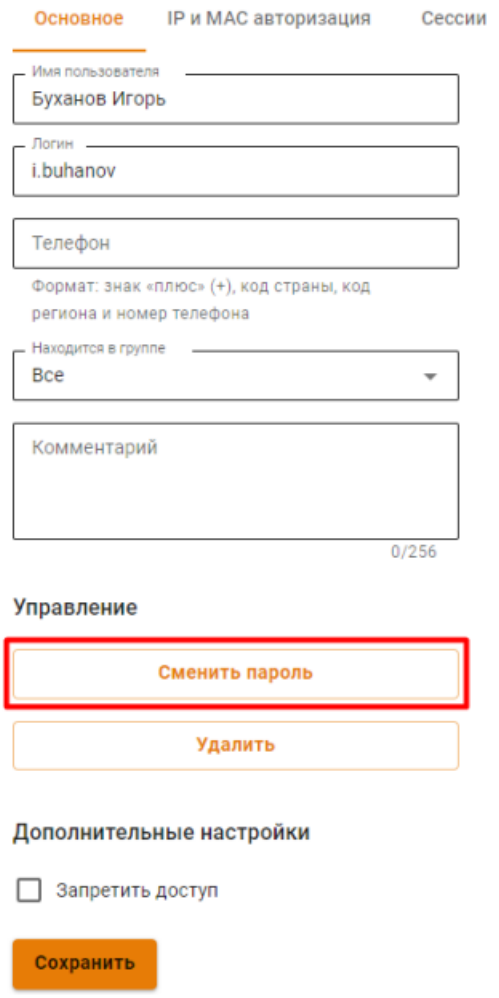
Удаление группы осуществляется аналогичным образом.

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.



14.1.3 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:

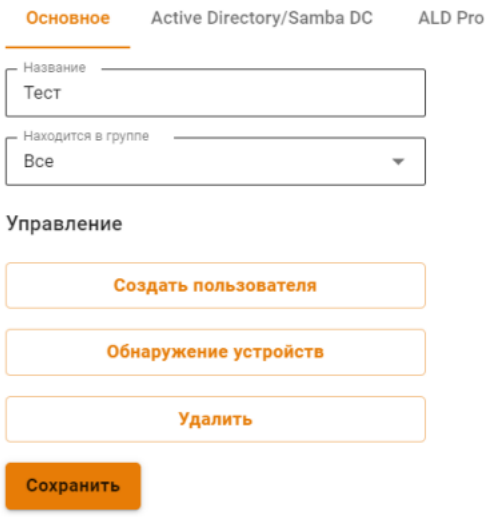
- Основное;
- IP и MAC авторизация;
- Сессии;
- Доступ по VPN;
- Квота.

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.

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

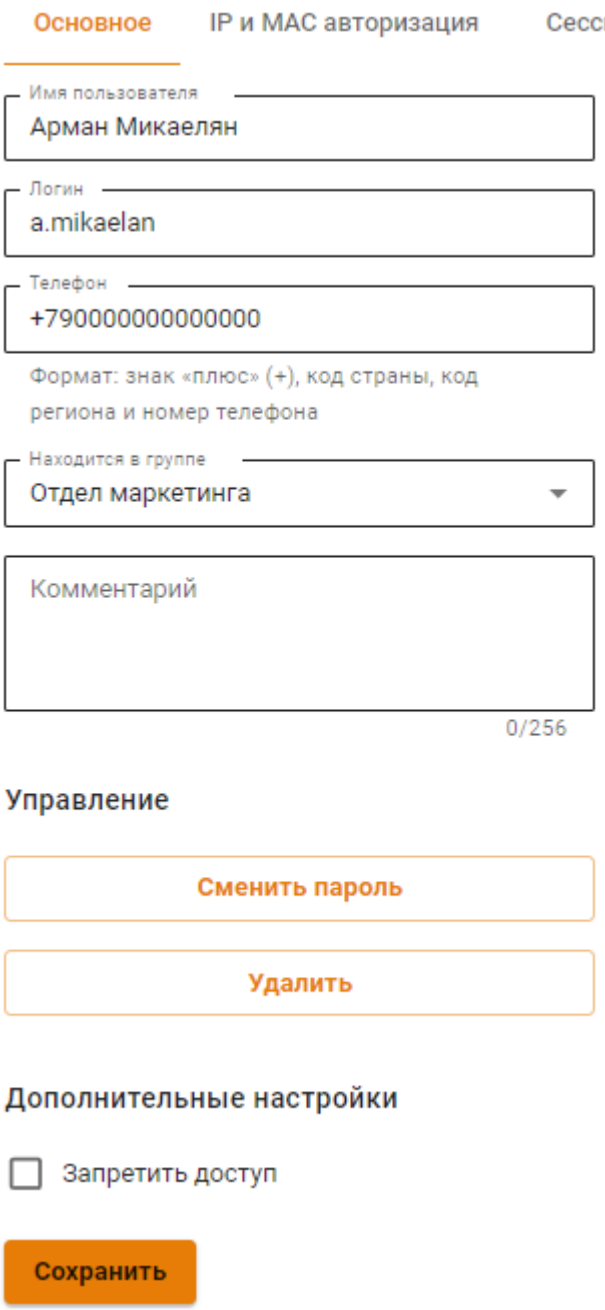
Категория позволяет распространить квоту на всех пользователей этой группы, у которых в персональной квоте включена опция **Наследовать квоту от группы**.
Для каждой группы пользователей есть аналогичная опция. Группы наследуют квоту, установленную в вышестоящей группе.

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

УЗ пользователей

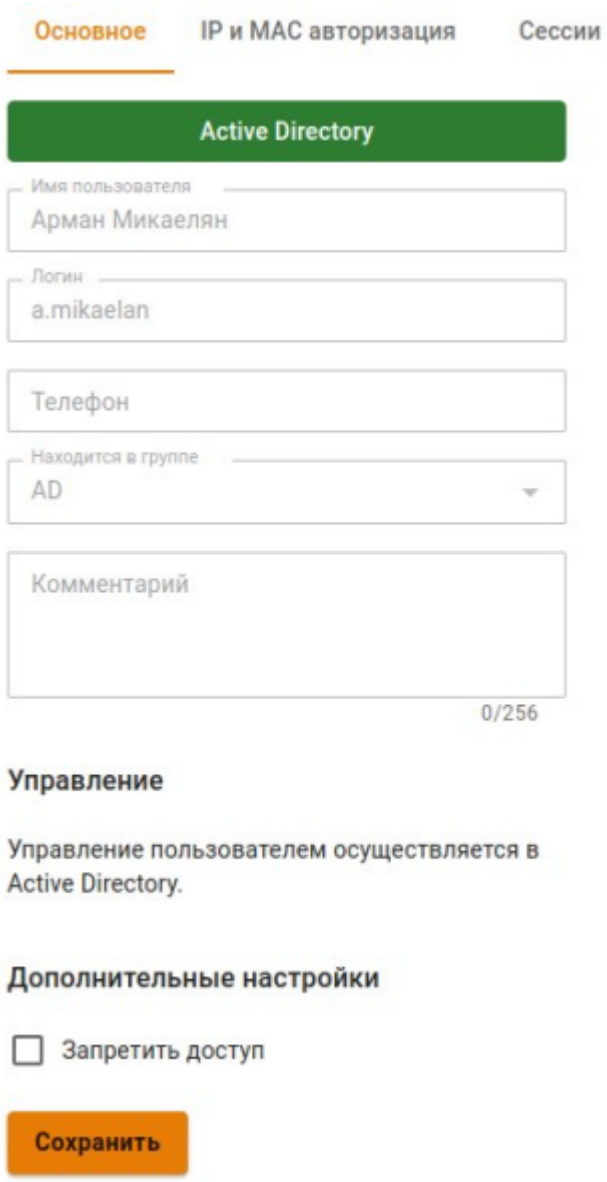
Основное

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. **Не используйте в качестве логина IP-адрес.** 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.

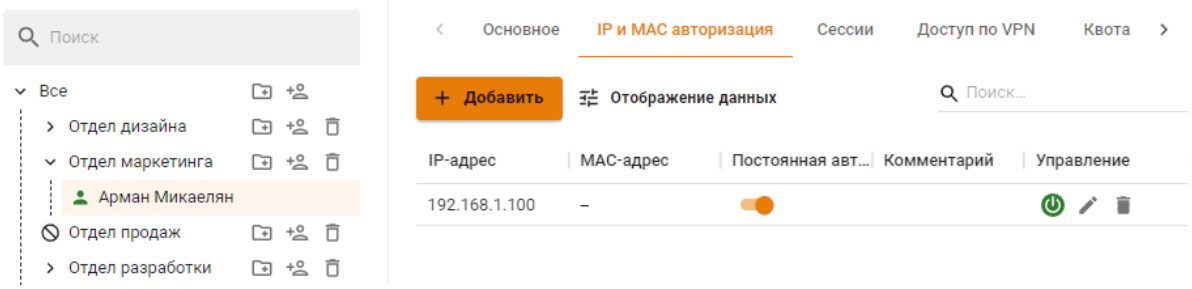
Для пользователей, экспортированных из *Active Directory* и *ALD Pro*, на вкладке **Основное** нельзя редактировать имя, логин, телефон, перемещать в другую группу и менять пароль. Пример импортированного из AD пользователя представлен на скриншоте:



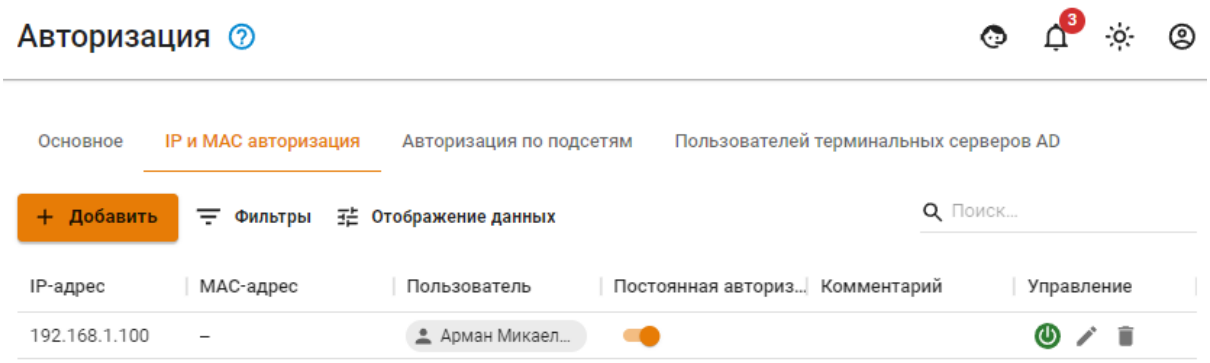
IP и MAC авторизация

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

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



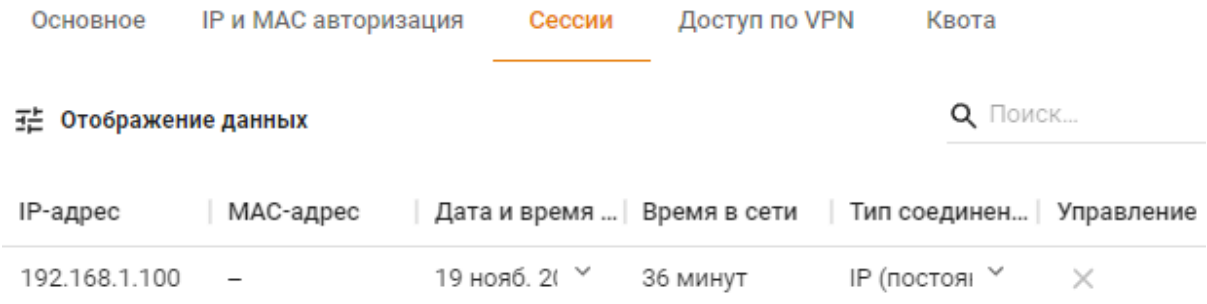
- Пользователи -> *Авторизации -> IP и MAC авторизация*:



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

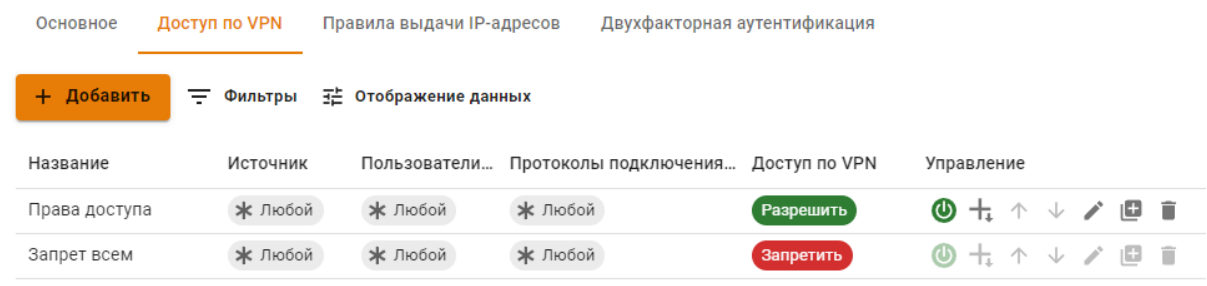
Содержит таблицу с информацией обо всех активных сессиях пользователях:



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

Доступ по VPN

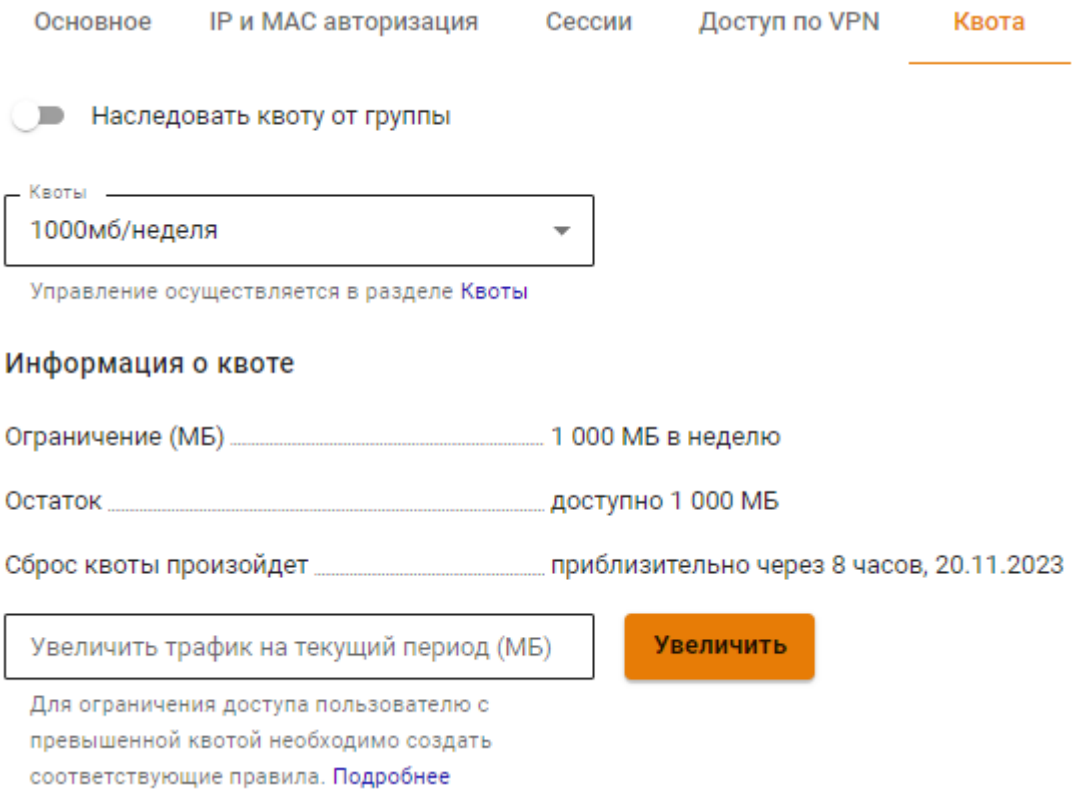
Категория позволяет просматривать правила доступа VPN, которые настраиваются в разделе **VPN-подключения -> Доступ по VPN**.



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*.

14.2 Авторизация пользователей

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

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

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

Особенности авторизации пользователей в Ideco NGFW:

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

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

14.2.1 Общая информация

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

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

При авторизации по VPN:

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

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

Если в первой сессии использовались методы авторизации IP, MAC, IP+MAC, WEB, NTLM, Ideco Agent, Log, Kerberos, то в шестой сессии пользователь проходит авторизацию. При этом статус первой сессии в разделе ***Авторизованные пользователи*** будет обозначаться иконкой , 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*.

14.2.2 Веб-аутентификация

Основное

Подсказка: Поддерживаемые браузеры:

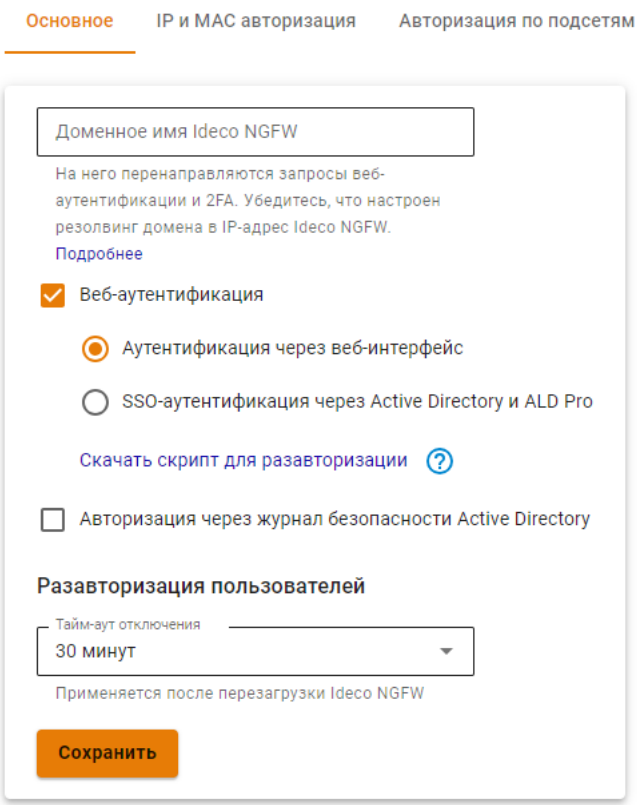
- Google Chrome, версия >= 90;
- Firefox, версия >= 78;
- Safari, версия >= 14.

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.

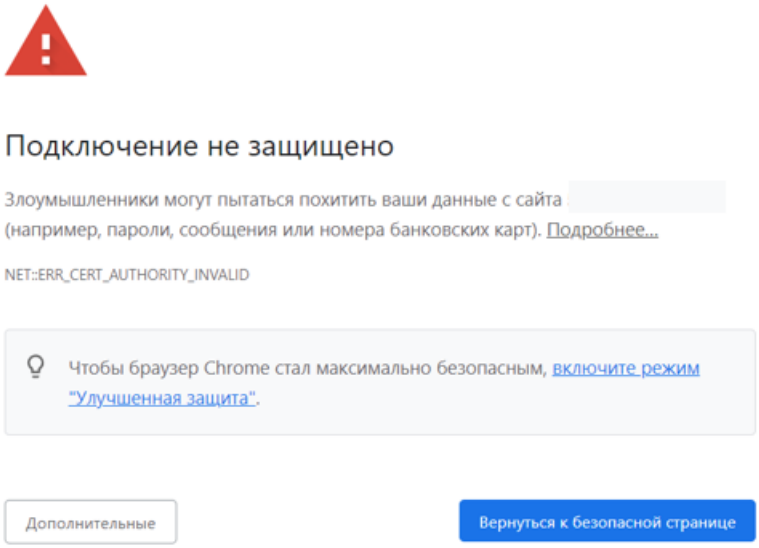
Для этого типа авторизации у пользователя на сетевой карте в качестве шлюза (объединенных в цепочку нескольких шлюзов) или при прямых подключениях к прокси по умолчанию должен быть указан IP-адрес локального сетевого интерфейса Ideco NGFW. Также до подключения к интернету должен работать **DNS-резолвинг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



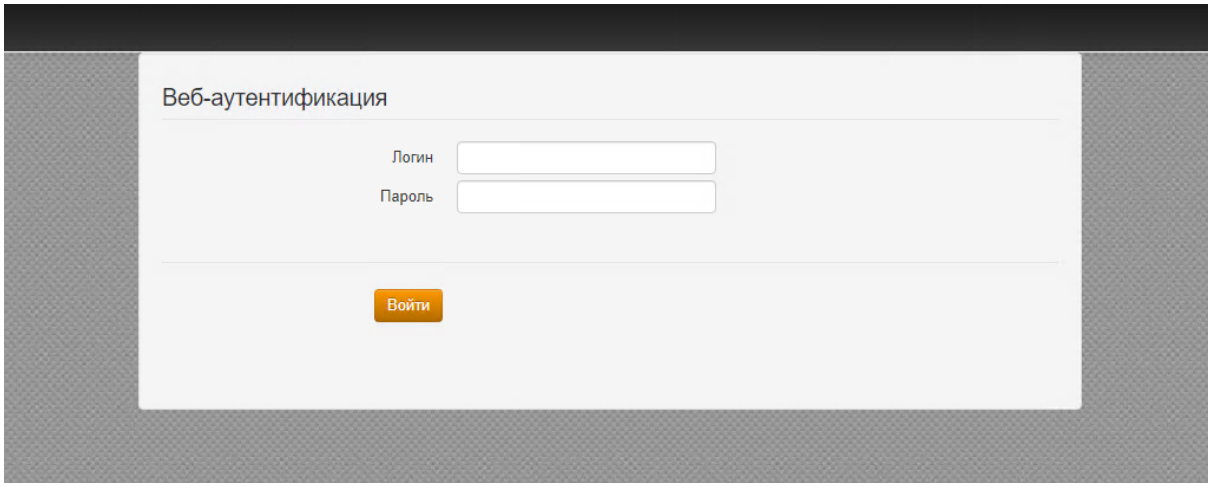
После заполнения поля **Имя домена** и сохранения настроек будет выдан Let's Encrypt сертификат, пользователь будет перенаправляться на окно авторизации, минуя страницу исключения безопасности:



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*.

14.2.3 IP и MAC авторизация

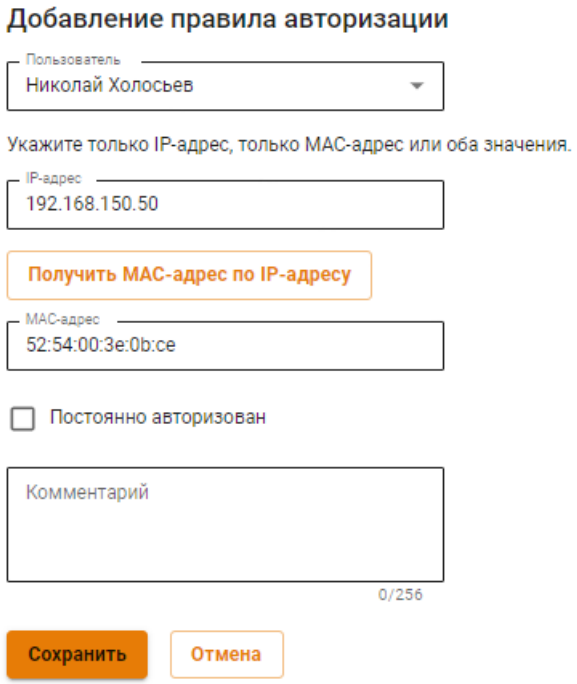
Общая информация

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**:



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

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*.

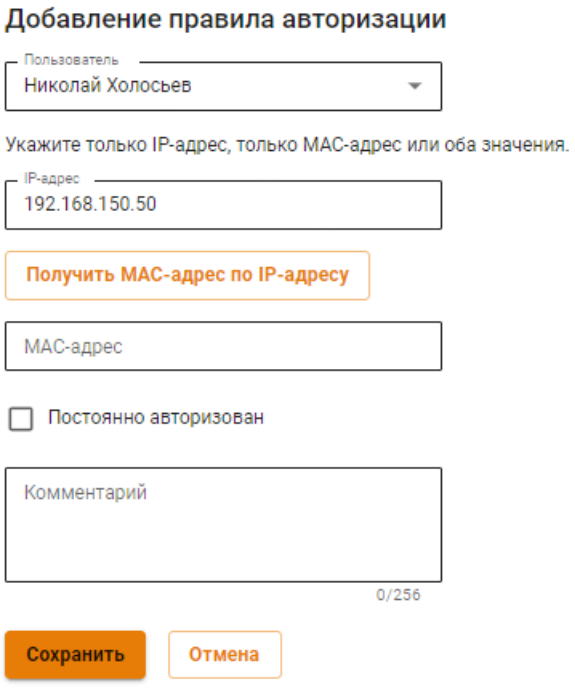
Настройка авторизации по IP

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

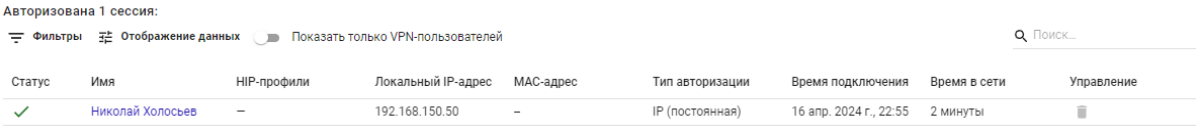
интернет.
Так же рекомендуем настроить статический IP-адрес или DHCP с привязкой по IP-адресу. Это требуется, например, для ресурсов, *опубликованных через DNAT*.

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**:



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

Авторизация по MAC-адресу

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

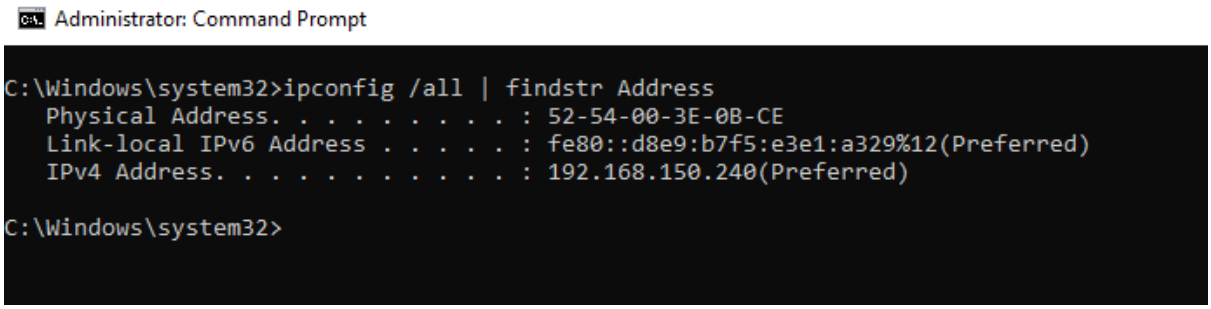
Предупреждение: Чтобы устройство могло авторизоваться на NGFW по MAC-адресу, они оба должны находиться в одном широковещательном домене и NGFW должен выступать шлюзом для устройств.

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

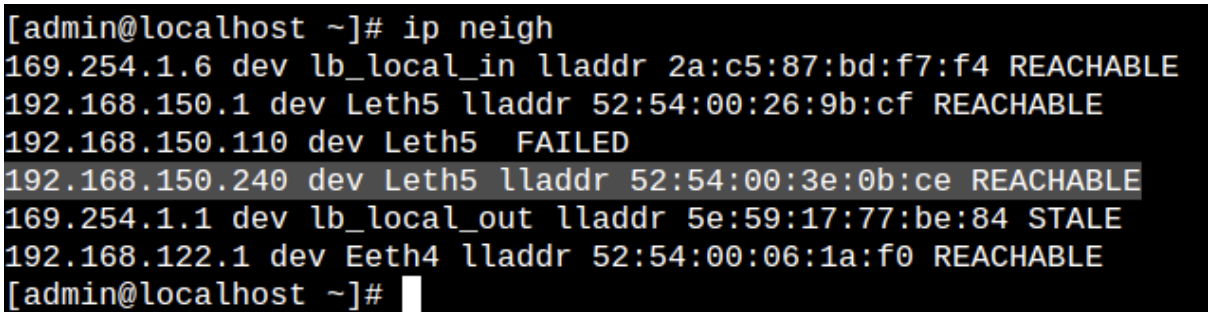
Настройка авторизации по MAC

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`:

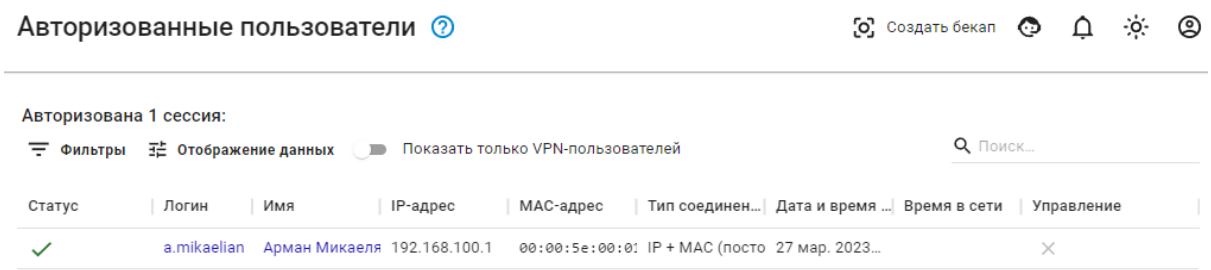


Подсказка: Эта команда выводит ARP-таблицу NGFW. Наличие записи с MAC-адресом устройства и статусом REACHEBLE говорит об имеющейся L2-доступности между NGFW и устройством.

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:



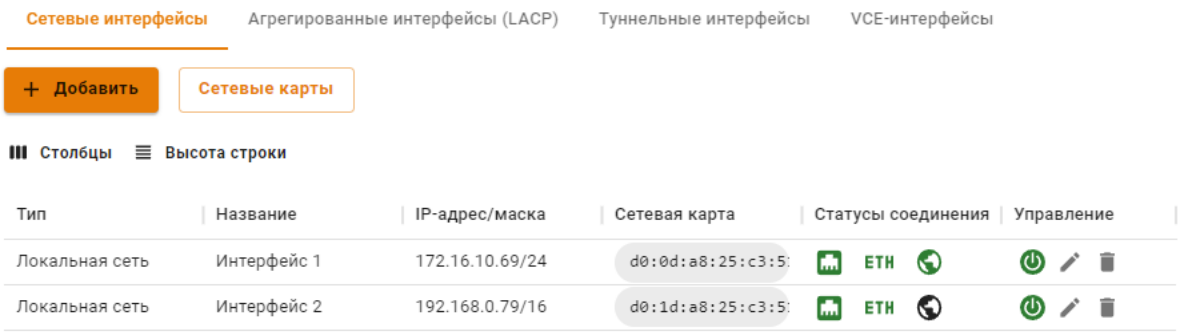
Поведение MAC-авторизации при перемещении устройства между локальными сетями

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.

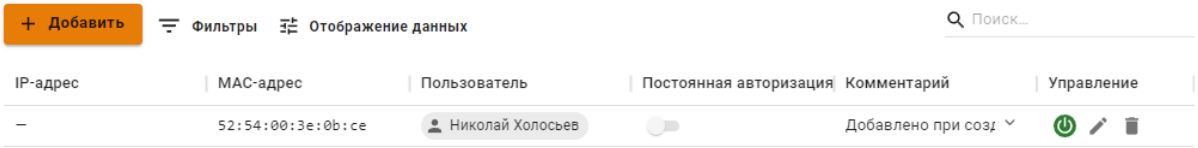
Подсказка: У Вас должен быть настроен собственный DHCP-сервер или на Ideco NGFW. В раздаваемых реквизитах шлюзом должен выступать локальный интерфейс Ideco NGFW.

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

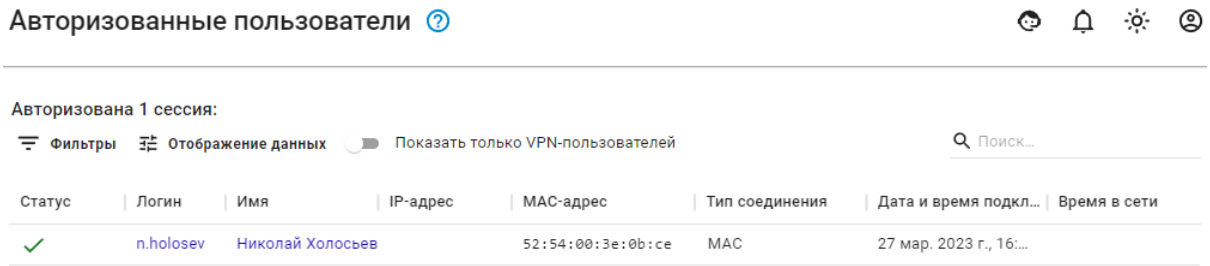
- На NGFW имеются настроенные следующим образом локальные интерфейсы:



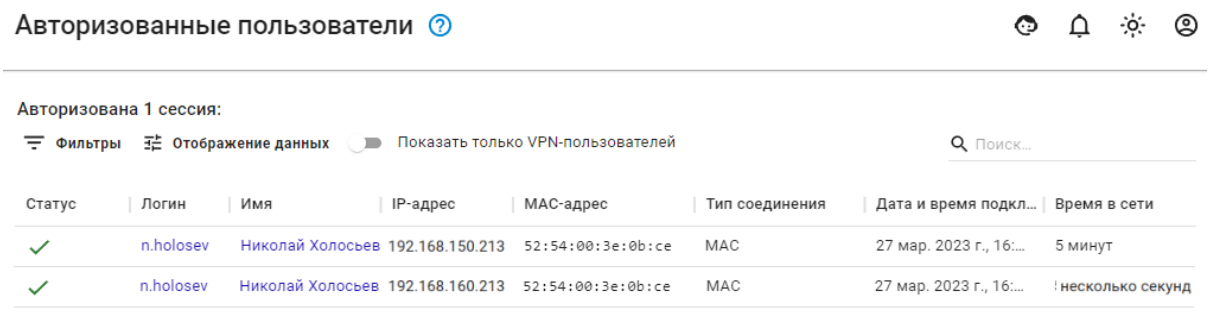
- У пользователя настроено правило авторизации по MAC-адресу:



- 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.

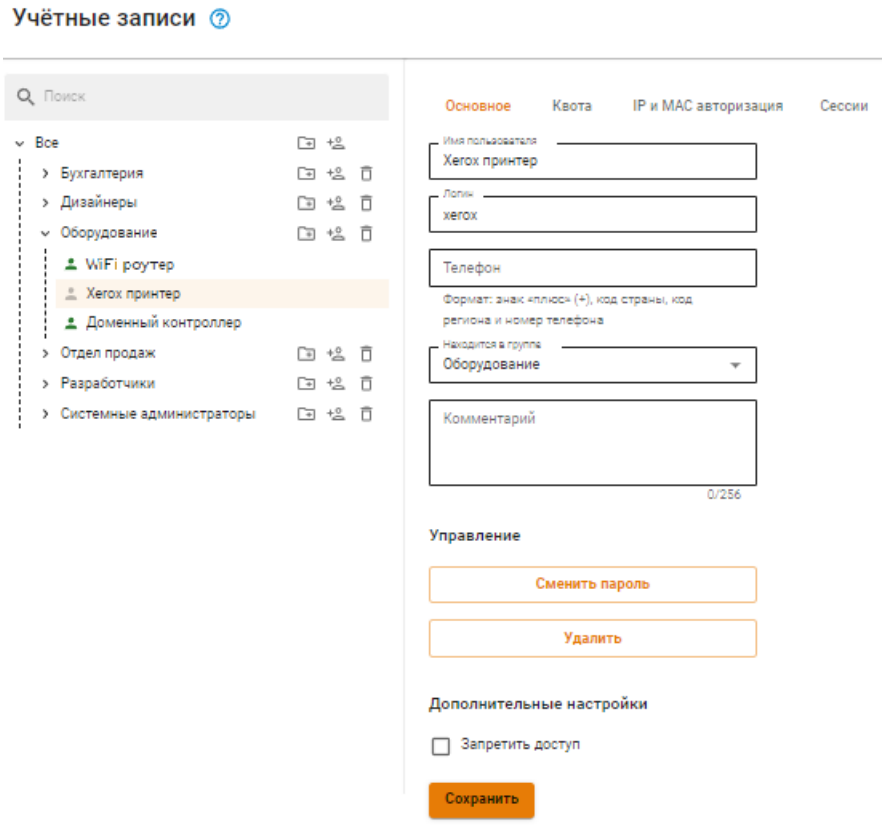
Сбросьте старые сетевые реквизиты от DHCP-сервера и получите новые с помощью команд:

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

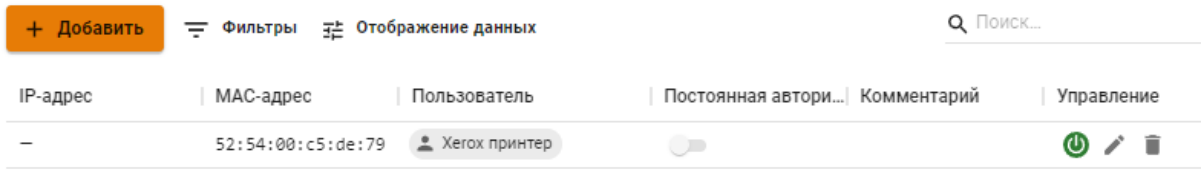
Настройка авторизации по MAC-адресу для сетевого принтера и других сетевых устройств

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.

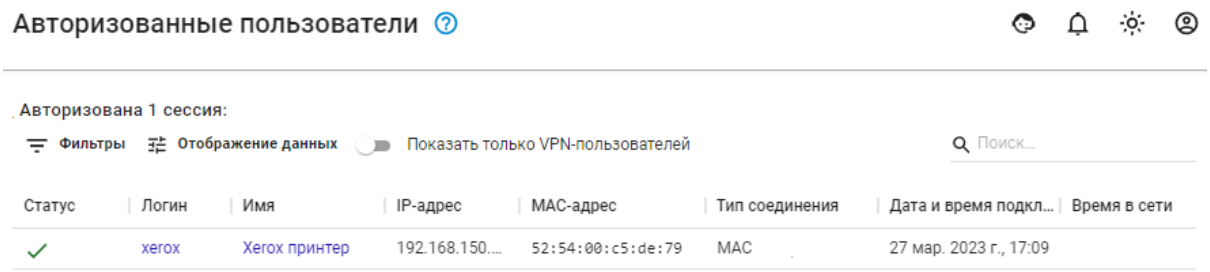
Для авторизации сетевого принтера необходимо создать пользователя для этого принтера вручную или через *Обнаружение устройств*:



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*)

14.2.4 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.

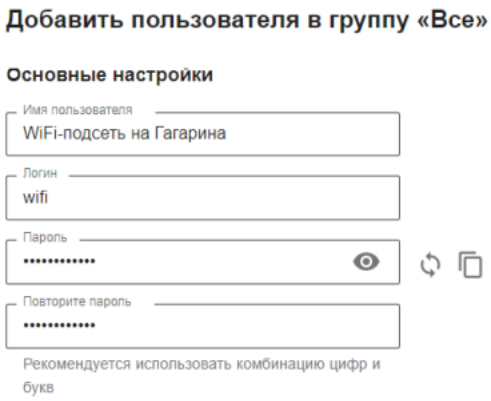
Подсказка: Трафик по всей подсети будет фиксироваться на одного пользователя.

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:

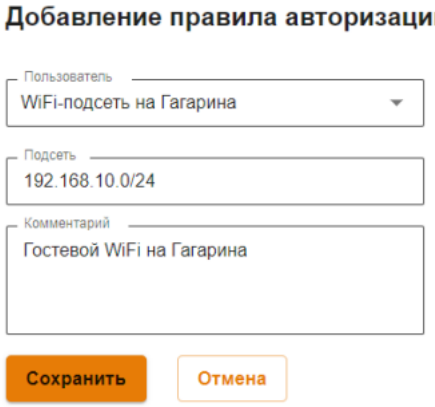
1. Перейдите в раздел **Пользователи –> Учетные записи** и нажмите **Добавить пользователя**.

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 авторизации пользователей по IP-адресам из подсети в правиле *Авторизации по подсетям*;
- Созданы правила в подразделе **Правила выдачи IP-адресов** с привязкой к IP-адресу из подсети правила *Авторизации по подсетям*.

14.2.5 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)*.

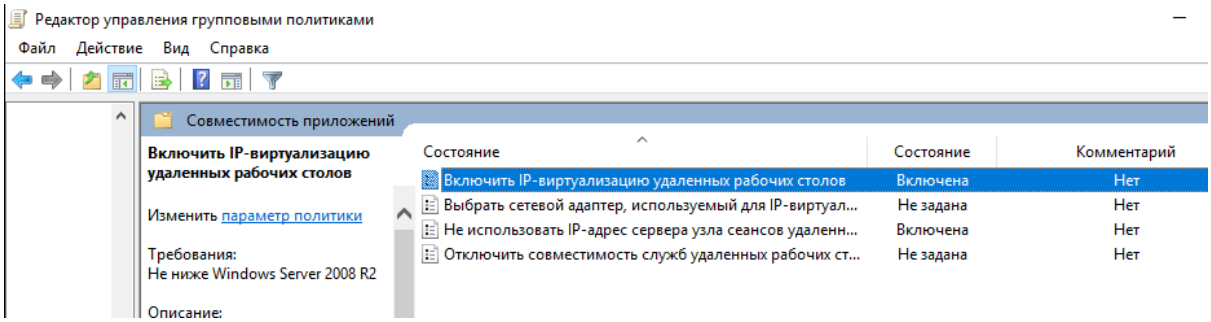
Подсказка: Авторизация пользователей терминального сервера по логам контроллера домена AD пока не реализована.

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"
```

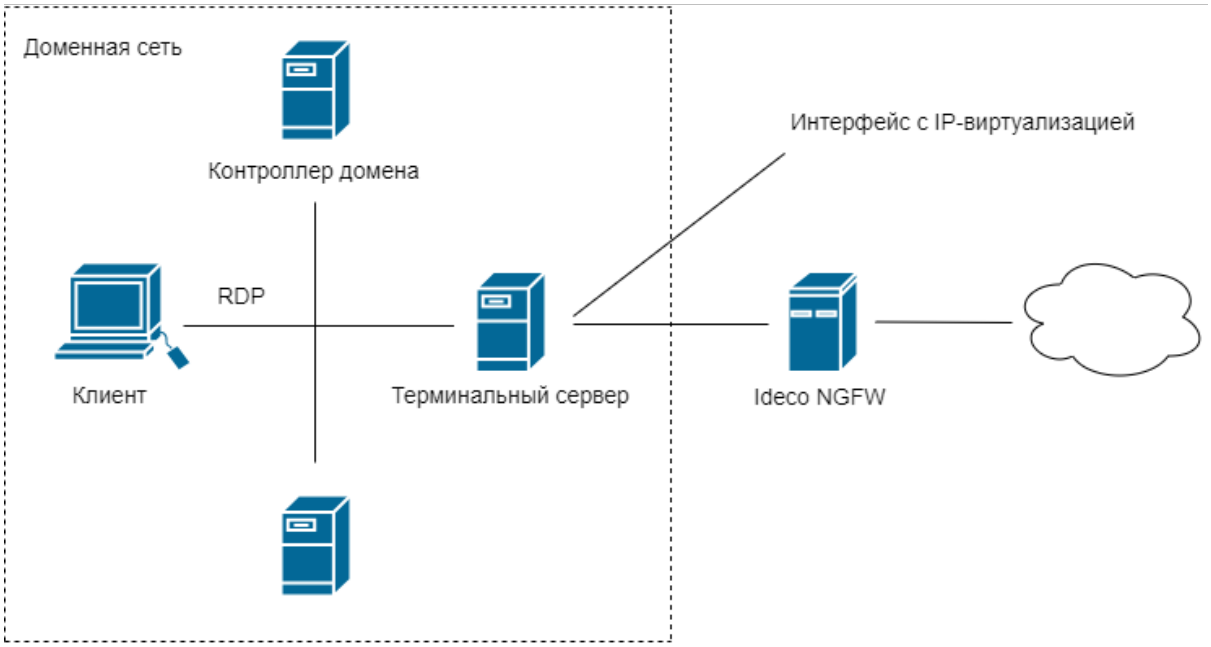
Значения:

- `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**;

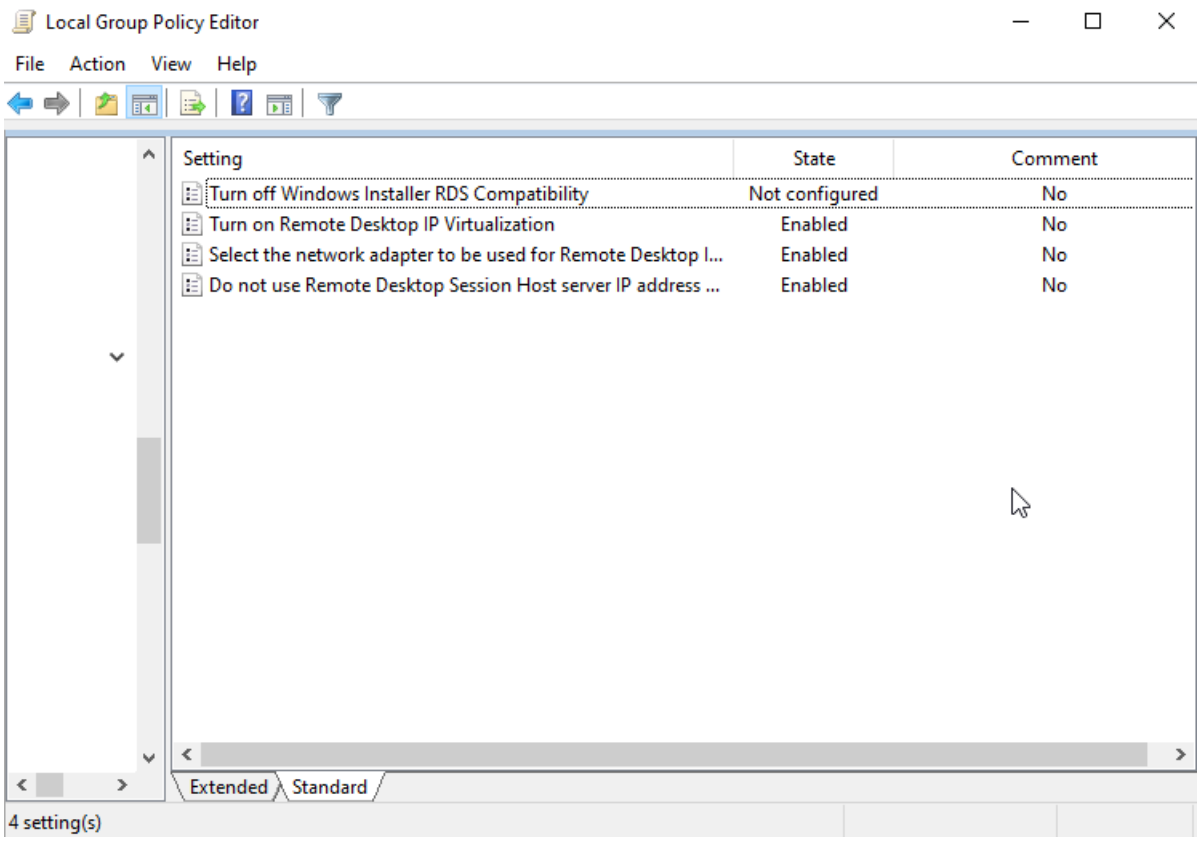
2. Включите параметр политики **Включить IP-виртуализацию удаленных рабочих столов** с параметром **Для сеансов**.

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

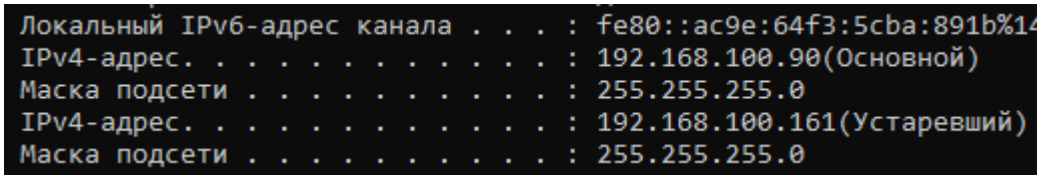
Тип: REG_MULTI_SZ (многострочный параметр)

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.



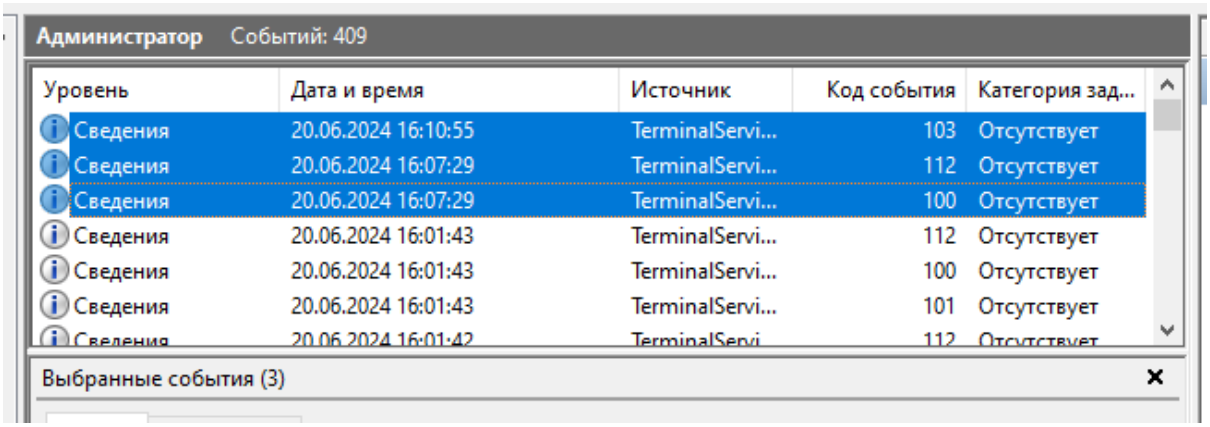
Диагностика

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**).

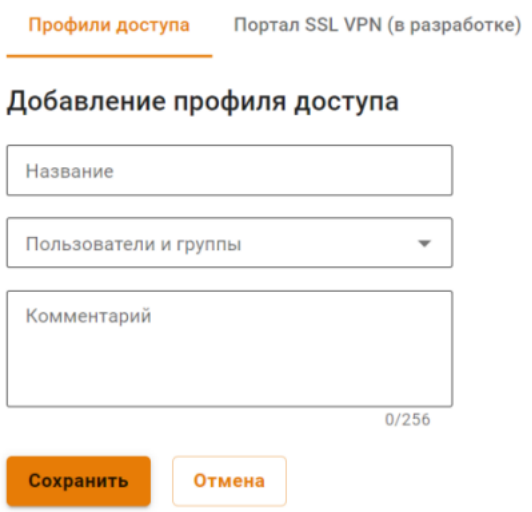
14.3 Личный кабинет пользователя

Настроить доступ пользователей в личный кабинет можно в разделе **Пользователи -> Личный кабинет пользователя**. Для доступа в ЛК необходимо создать **Профили доступа**, а затем опубликовать личный кабинет через обратный прокси, чтобы пользователи получили к нему доступ.

14.3.1 Настройка доступа в личный кабинет

Чтобы создать профиль доступа, выполните действия:

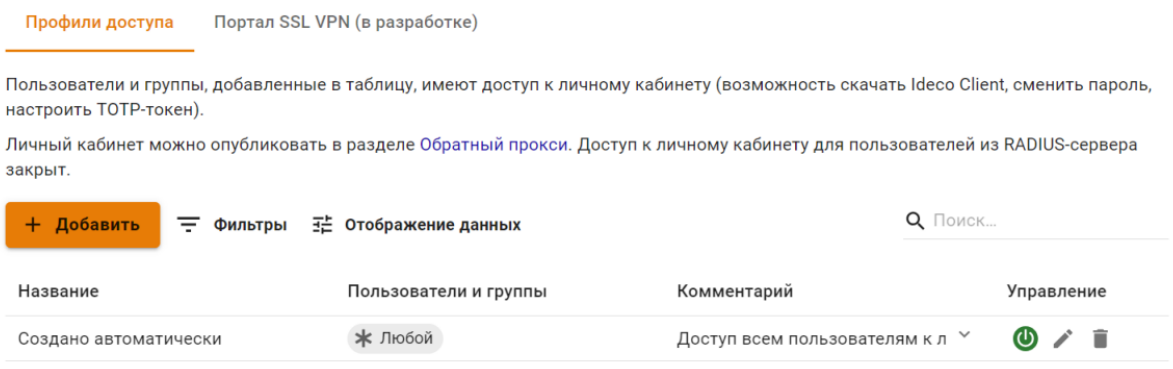
1. Нажмите **Добавить** и заполните следующие поля:



- **Название** - название профиля доступа;
- **Пользователи и группы** - выберите пользователей, группы пользователей, группы безопасности из AD, которым хотите предоставить доступ в личный кабинет;
- **Комментарий** - поле не обязательное.

При наличии большого количества профилей доступа в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: По умолчанию в таблице правил раздела присутствует предустановленное правило, предоставляющее доступ всем пользователям к личному кабинету:



14.3.2 Публикация Личного кабинета

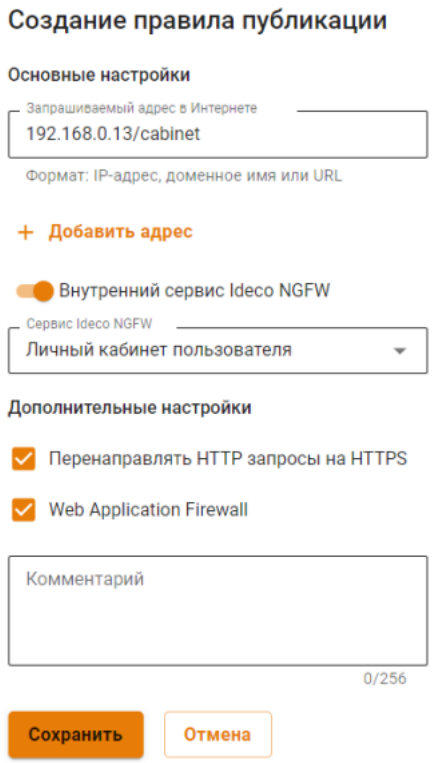
Чтобы пользователи получили доступ в личный кабинет, он должен быть опубликован. Для публикации ЛК перейдите в раздел **Сервисы -> Обратный прокси** и выполните действия:

1. Нажмите **Добавить**.

2. Включите опцию **Внутренний сервис Ideco NGFW**:

В списке сервисов Ideco NGFW выберите **Личный кабинет пользователя**.

3. В поле **Запрашиваемый адрес в интернете** введите адрес, по которому хотите опубликовать личный кабинет:



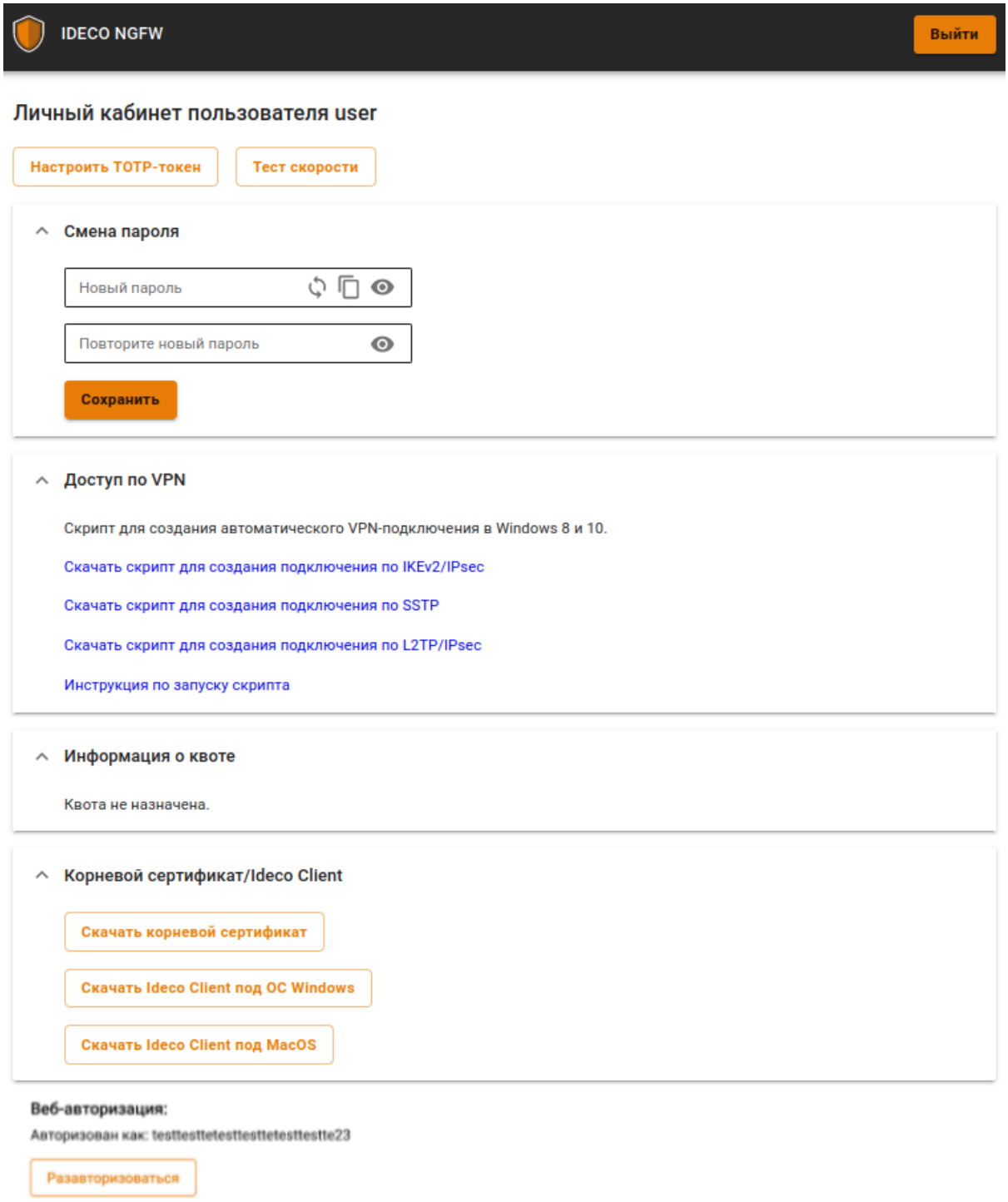
4. Нажмите **Сохранить**.

После этого пользователь сможет зайти в ЛК по логину и паролю, либо через авторизацию в сети NGFW.

14.3.3 Возможности личного кабинета Ideco NGFW

- **Смена пароля**;
- **Скачивание корневого сертификата**;
- **Скачивание скриптов для создания автоматического VPN-подключения в Windows 8 и 10**. Будут доступны скрипты настройки только тех типов подключения, которые указаны для пользователя в таблице **Доступ по VPN** в разделе **Пользователи -> VPN-подключения**;
- **Информация о квоте**;
- **Генерация TOTP-токена**;
- **Скачивание Ideco Client**. Подробнее о работе в Ideco Client в *статье*;
- **Тестирование скорости**. При нажатии на соответствующую кнопку в веб-интерфейсе личного кабинета откроется меню тестирования скорости между хостом и NGFW;

- **Разавторизация**. Разавторизация пользователя в сети NGFW, если он был авторизован через Web/SSO.

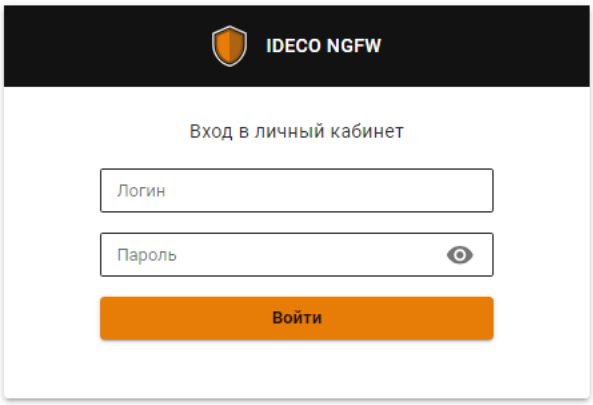


Подсказка: Личный кабинет пользователя будет доступен по ссылке, указанной при публикации ЛК через обратный прокси.

Чтобы зайти в личный кабинет, выполните действия:

1. Перейдите по ссылке, указанной в правиле публикации личного кабинета.

2. В открывшейся форме авторизации введите логин и пароль пользователя:



Подсказка: Если пользователь уже авторизован в сети NGFW, то логин/пароль вводить не потребуется, личный кабинет откроется сразу.

TOTP-токен

TOTP-токен позволяет пройти двухфакторную аутентификацию при подключении по VPN.

Подсказка: Для настройки двухфакторной аутентификации на Ideco NGFW воспользуйтесь *статьей*.

Чтобы воспользоваться TOTP-токеном, выполните действия:

1. Нажмите на кнопку Настроить TOTP-токен.

2. Сгенерируйте QR-код, нажав на кнопку Сгенерировать QR-код.

3. Отсканируйте QR-код с помощью камеры телефона из приложения для аутентификации (Google Authenticator, Яндекс Ключ и т. п.) или введите код в приложение вручную:

Внимание: Если пользователь не отсканирует QR-код и покинет страницу, то код можно будет сгенерировать повторно, только сбросив секретный ключ в карточке пользователя в веб-интерфейсе Ideco NGFW.

14.4 VPN-подключение

Подсказка: Название службы раздела **VPN-подключения**: `ideco-accel-l2tp`; `ideco-accel-pptp`; `ideco-accel-sstp`; `ideco-vpn-servers-backend`; `ideco-vpn-authd`.
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 к локальной сети компании из дома, отеля или другого офиса, необходимо настроить VPN-сервер и подключиться через него. Для этого можно использовать VPN-клиент, который уже есть в

операционной системе, или установить отдельный.

Настройка VPN-сервера включает в себя несколько этапов:

- Настройка протоколов, маршрутов и адресации;
- Настройка политик доступа из внешних сетей;
- Опционально - двухфакторная аутентификация.

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.

14.4.1 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 бит.

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*.

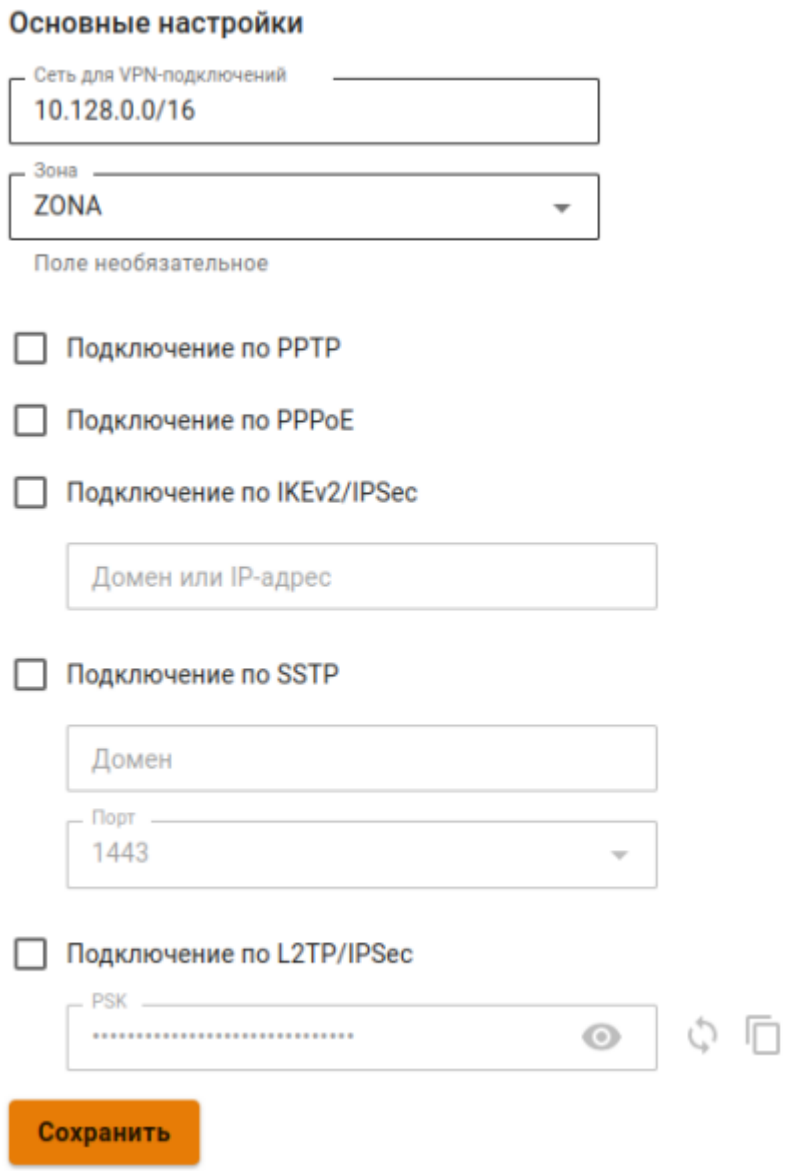
Основные настройки

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:



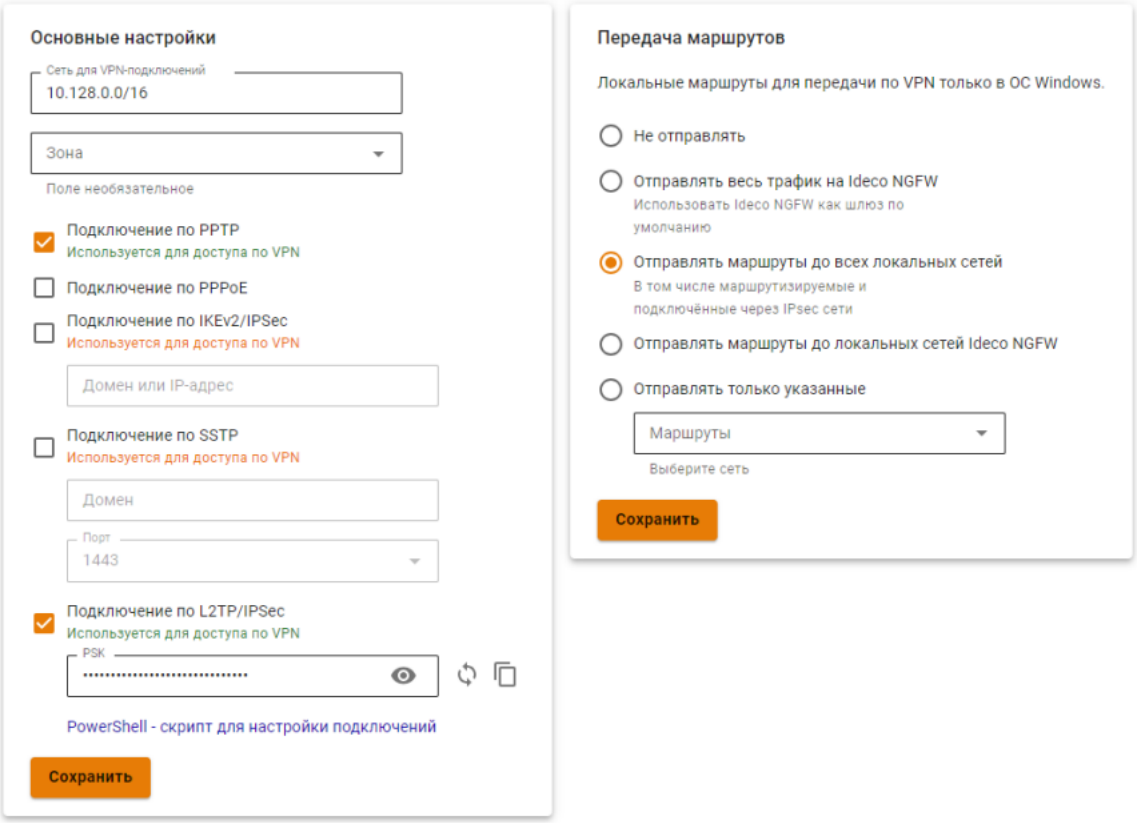
Подсказка: Используйте зоны для настройки конфигурации VPN-подключения сразу нескольких сетевых интерфейсов.

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:

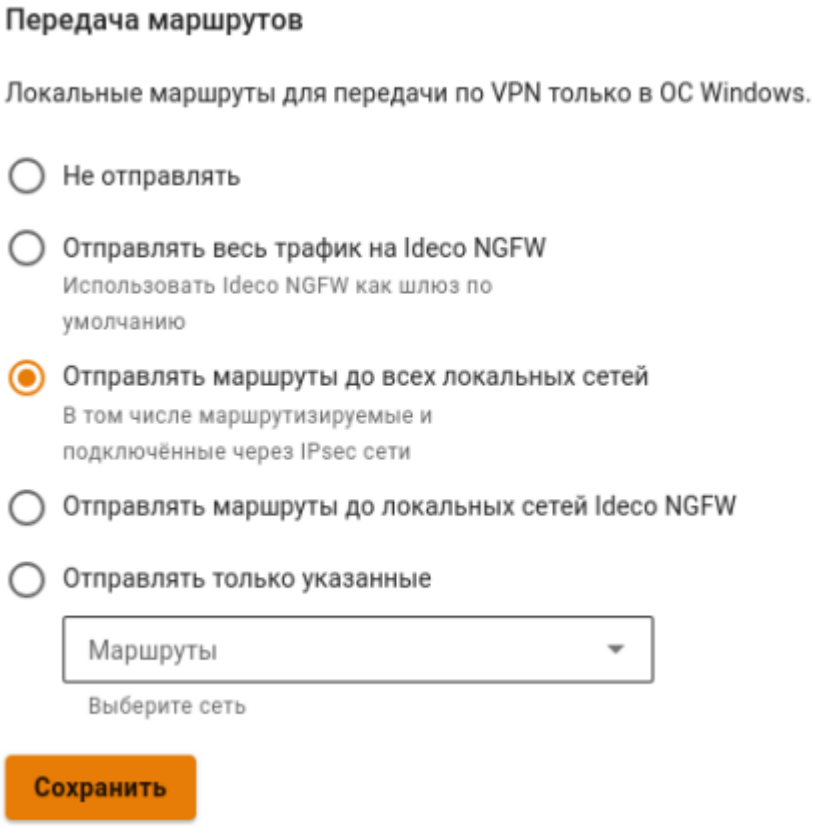
1. **Не отправлять**. При включении данной опции клиентам не будут передаваться никакие маршруты, то есть никакой трафик не будет проходить через NGFW.

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**.

14.4.2 Доступ по VPN

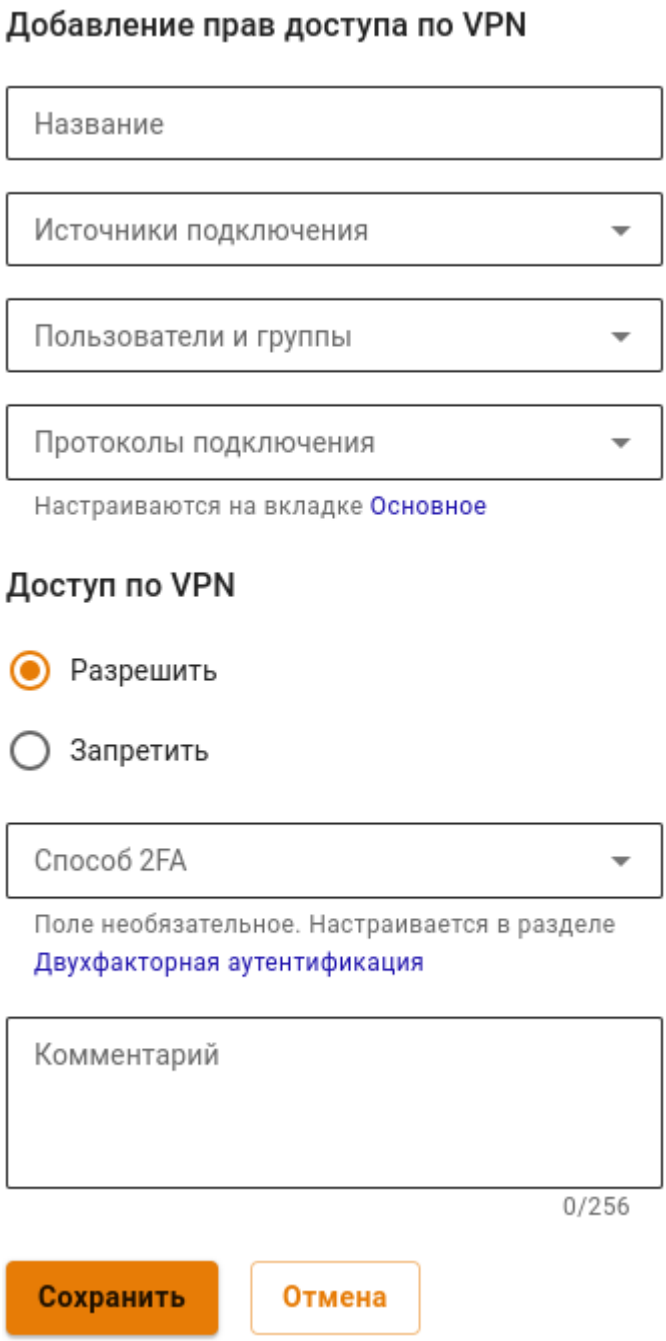
Вкладка содержит таблицу правил, которые действуют сверху вниз. Как только в правиле происходит совпадение полей **Источник подключения**, **Пользователи и группы**, **Протокол подключения** производится действие, выбранное при создании правила. В случае указания **Способа 2FA** будет происходить аутентификация 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**.

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

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

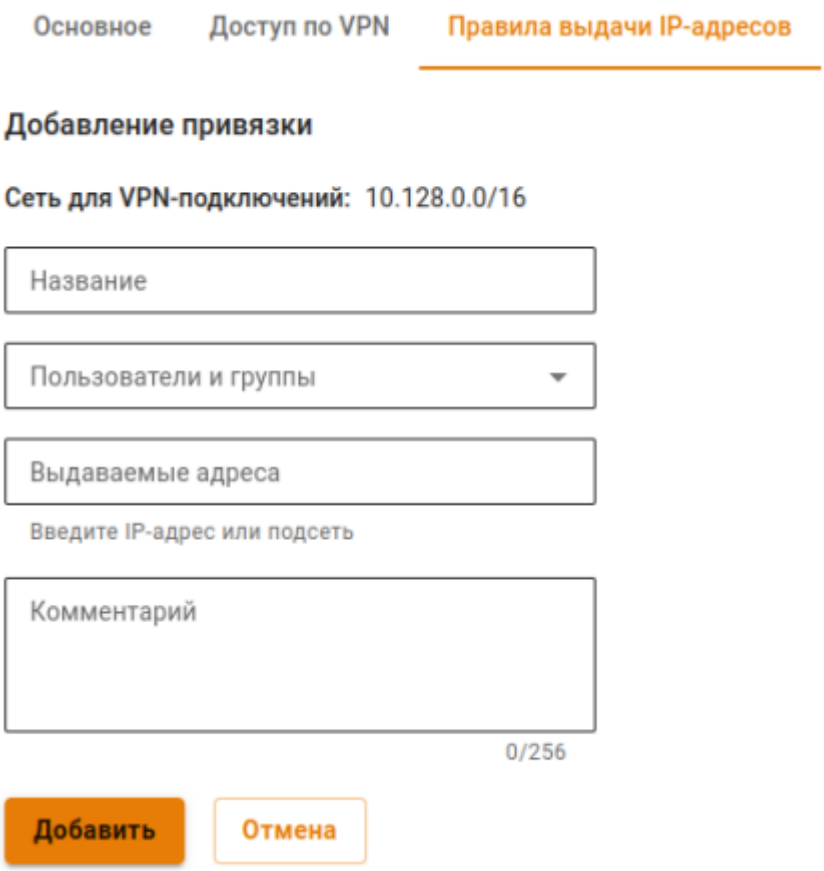
Подсказка: Для разных групп пользователей можно указать разные типы двухфакторной аутентификации. Для настройки двухфакторной аутентификации воспользуйтесь *статьей*

14.4.3 Правила выдачи IP-адресов

На вкладке доступно создание правил для выдачи IP-адресов пользователям, подключающимся по VPN. NGFW просматривает таблицу правил сверху вниз до первого совпадения пользователя.

Подсказка: Если пользователь не попал под условия правил, ему выдается свободный IP-адрес из сети для VPN-подключений. При этом из нее исключаются все подсети и одиночные адреса, указанные во всех правилах таблицы и использующиеся в текущих сессиях. Если ни одного адреса не осталось, соединение разрывается

Чтобы создать правило, нажмите **Добавить** и заполните следующие поля:



- **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.

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

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.

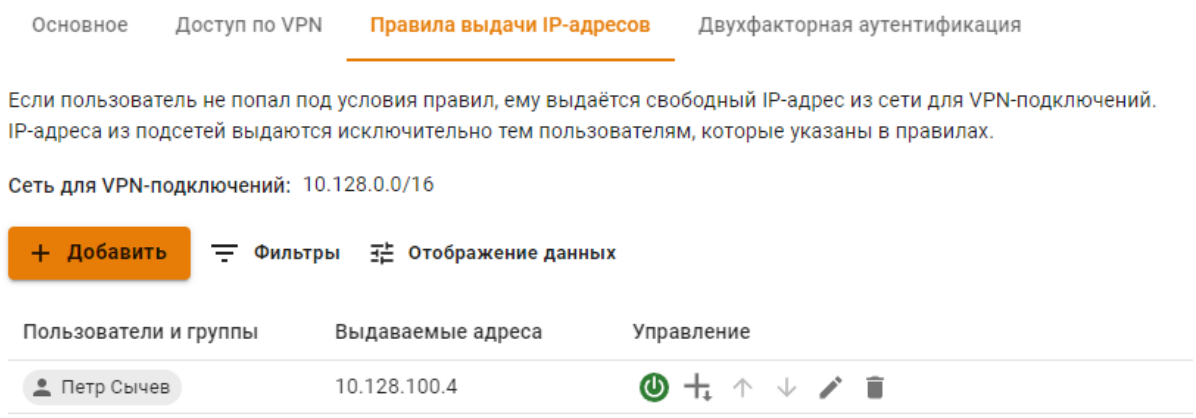
- Если в разных правилах указаны пересекающиеся сети (например, сеть `10.128.1.0/24` является подсетью сети `10.128.0.0/20`), то:
  - адреса из сети `10.128.1.0/24` никогда не будут выдаваться;
  - при выдаче адресов сети `10.128.0.0/20` из нее будут исключаться адреса подсети `10.128.1.0/24`.
- Если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



14.4.4 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.

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

- Rutube;

- Youtube.

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**.

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

- Rutube;
- Youtube.

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**.

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

- Rutube;
- Youtube.

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**:

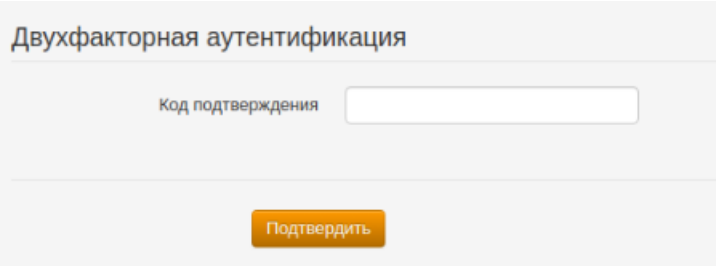
Сгенерированный QR-код появится на экране.

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

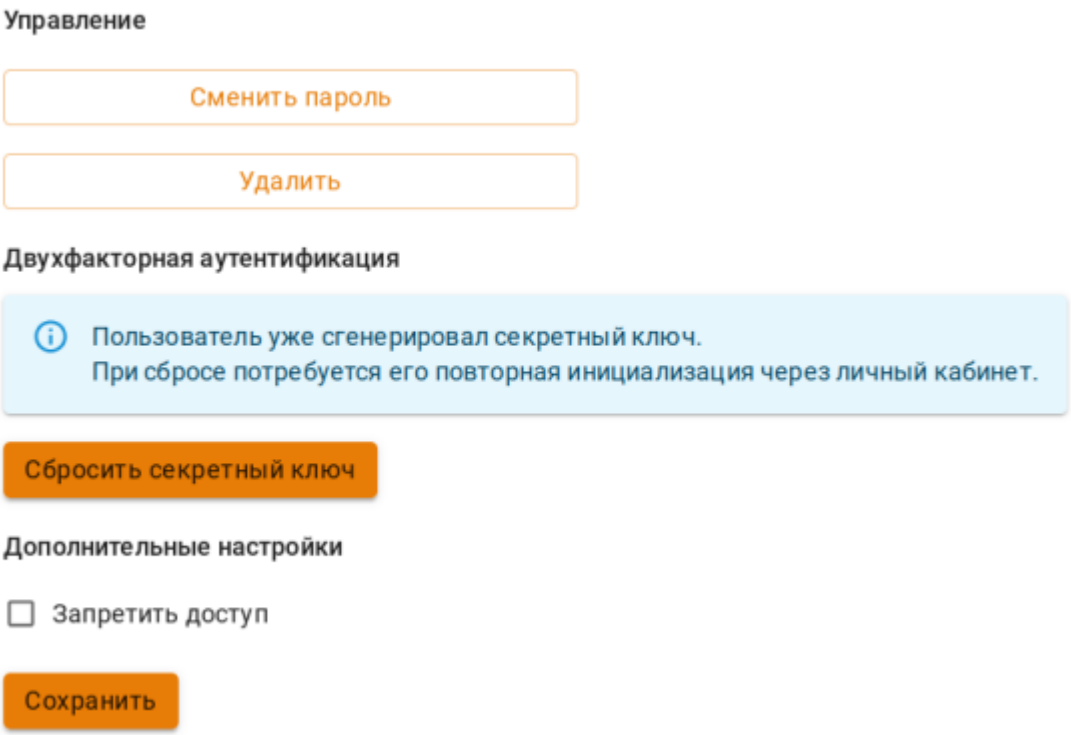
сможет пройти аутентификацию. Убедитесь, что время на устройстве пользователя с приложением и на Ideco NGFW совпадает.

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, не использующий **HSTS**
(например, neverssl.com). 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**;

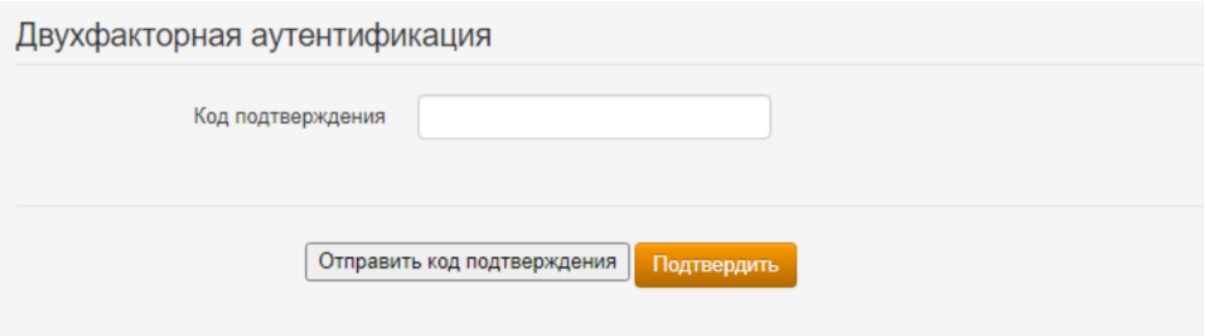
- Перейдите на вкладку **Сеть**;
- Нажмите на **IP версии 4 (TCP/IPv4) -> Свойства -> Дополнительно**;
- Снимите флаг с пункта **Использовать основной шлюз в удаленной сети**;
- Нажмите **ОК**.

Для Ubuntu:

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

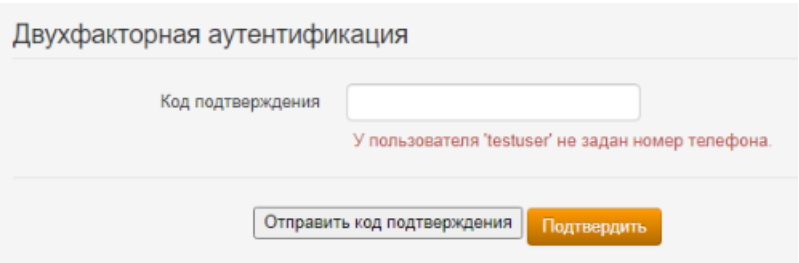
3. Включите созданное VPN-подключение.

4. Перейдете в браузер, откроется страница аутентификации:

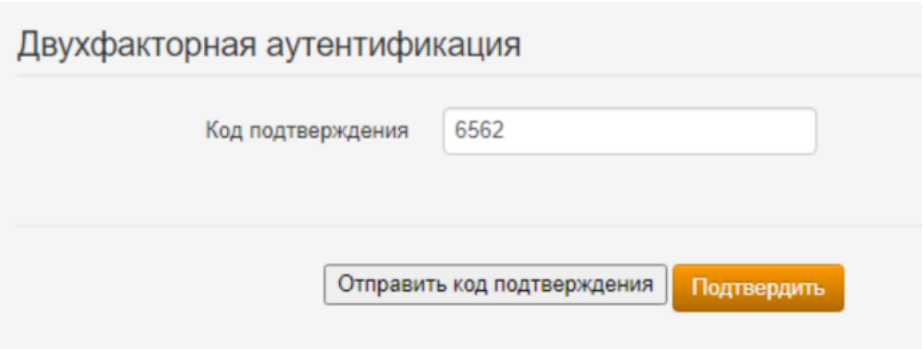


5. Нажмите **Отправить код подтверждения**. На номер телефона, указанный в учетной записи, придет SMS с кодом:

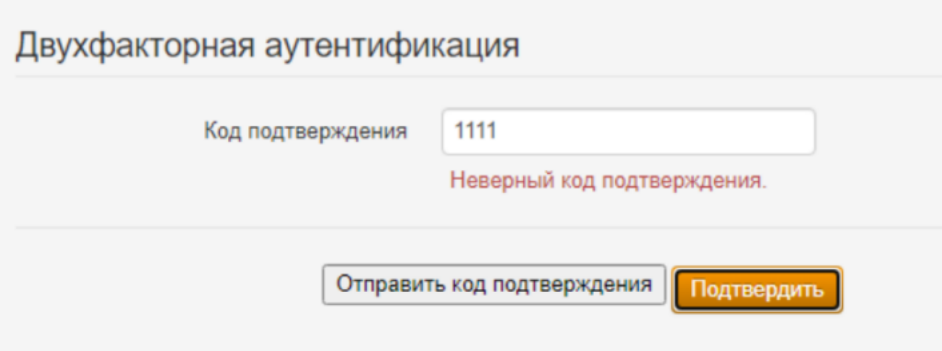
- Если номер телефона в карточке пользователя отсутствует, то на странице аутентификации появится предупреждение:



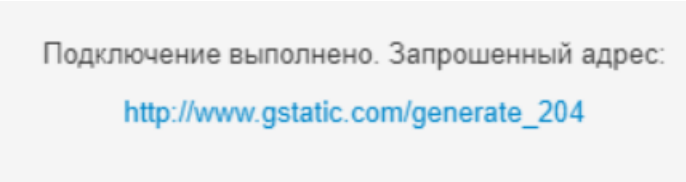
- Если номер телефона сохранен, то на указанный номер телефона поступит SMS. Введите код из SMS и нажмите **Подтвердить**:



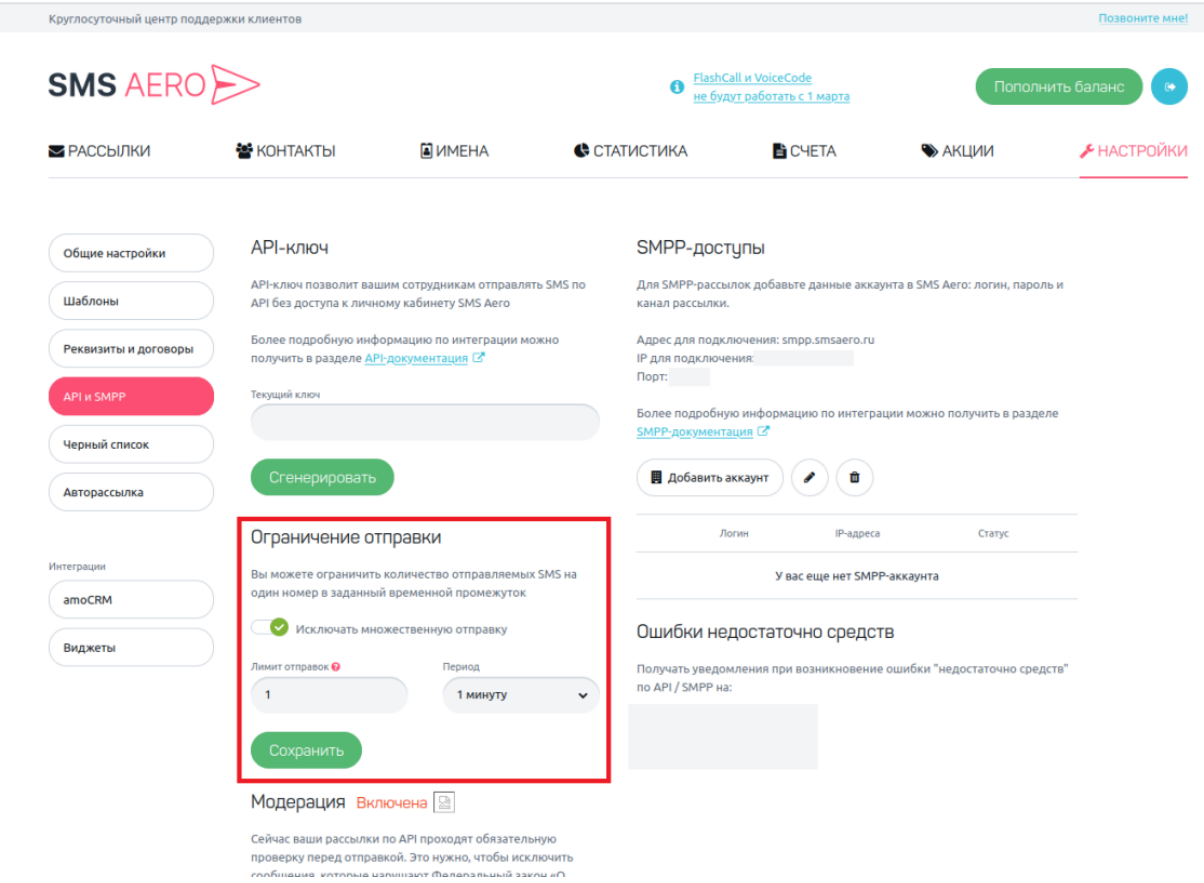
- Если код введен неверно, то появится соответствующее предупреждение:



- Если код введен верно, то появится следующее окно:



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

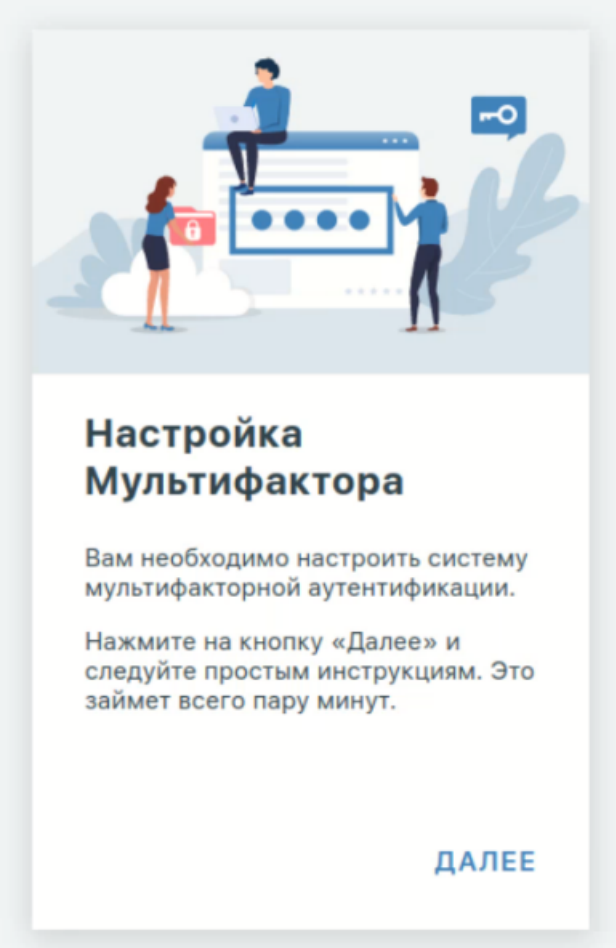


Мультифактор:

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

2. Включите созданное VPN-подключение.

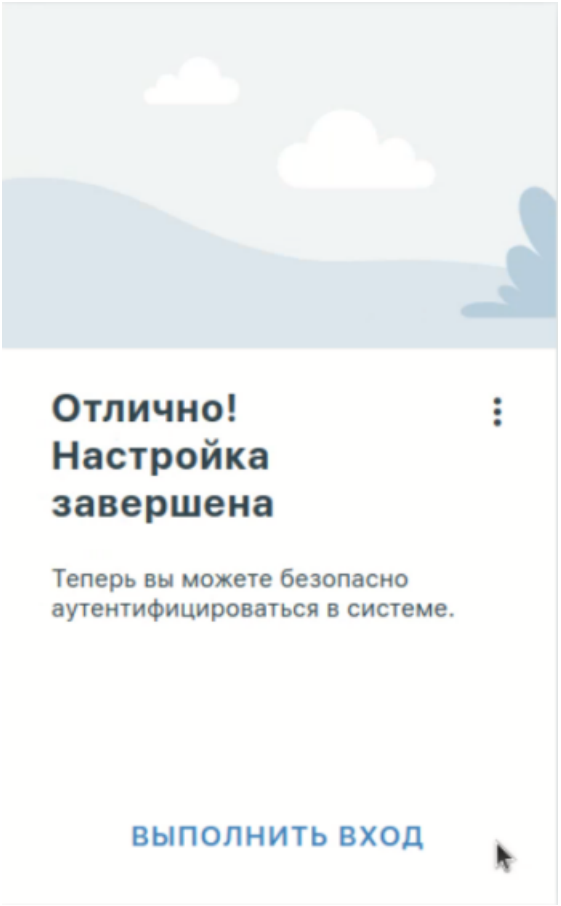
3. При переходе в браузер откроется страница аутентификации:



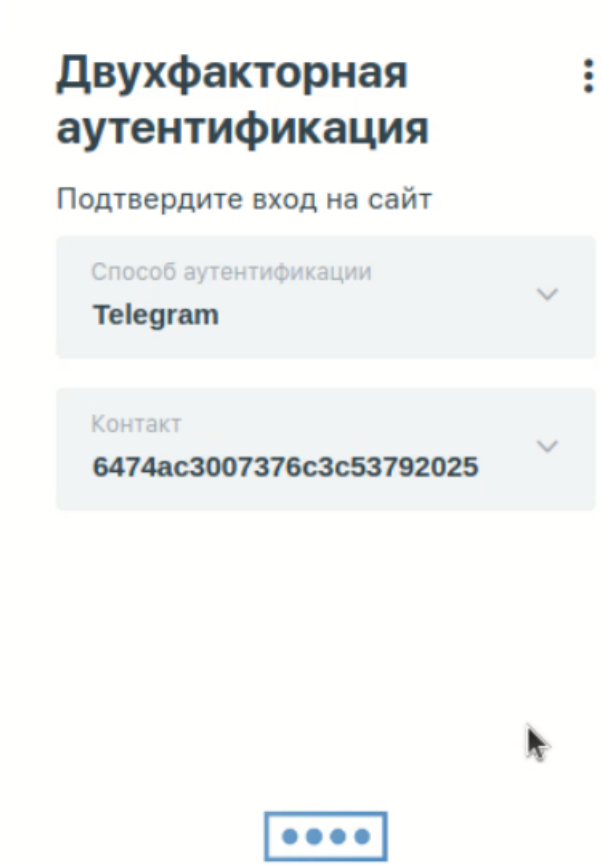
4. После нажатия **Далее** появится страница с предложением установить приложение на устройство пользователя. Если приложение установлено, нажмите **Далее**.

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

6. Нажмите **Выполнить вход**:



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



8. В зависимости от выбранного способа подтвердите вход.

14.4.5 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.

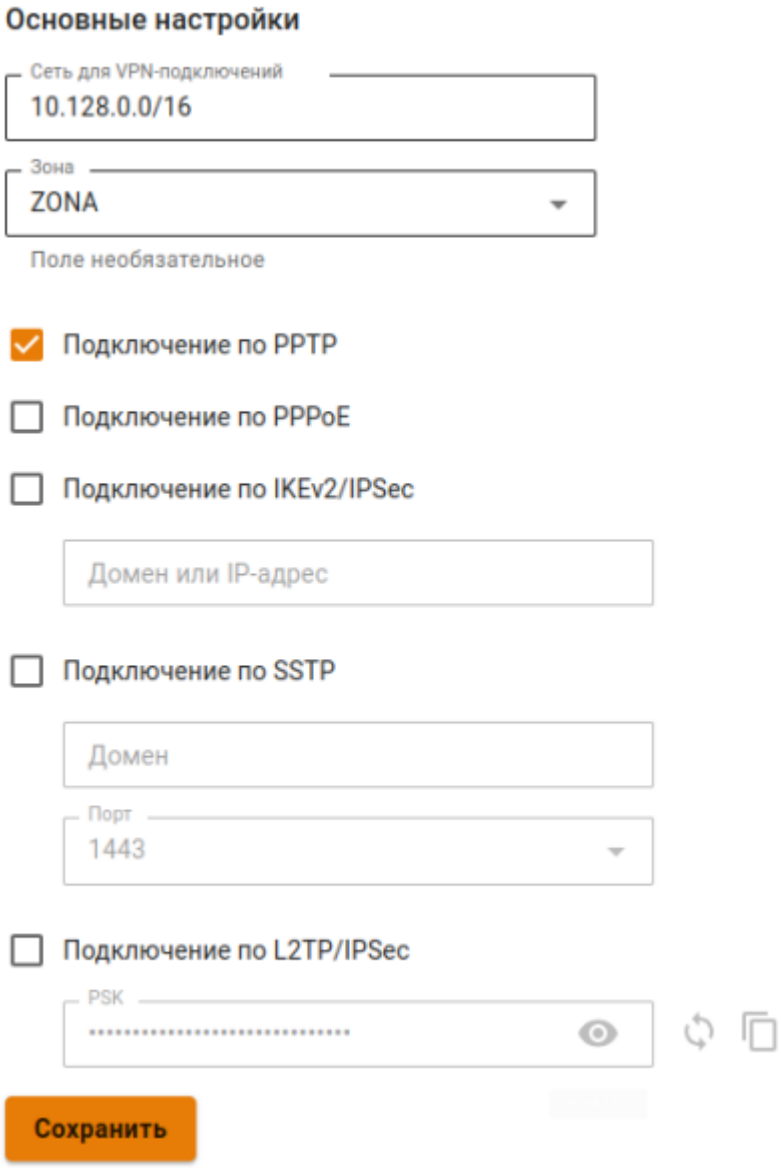
Настройка глобальных параметров Ideco NGFW

Для настройки авторизации по протоколу PPTP необходимо выполнить следующие действия:

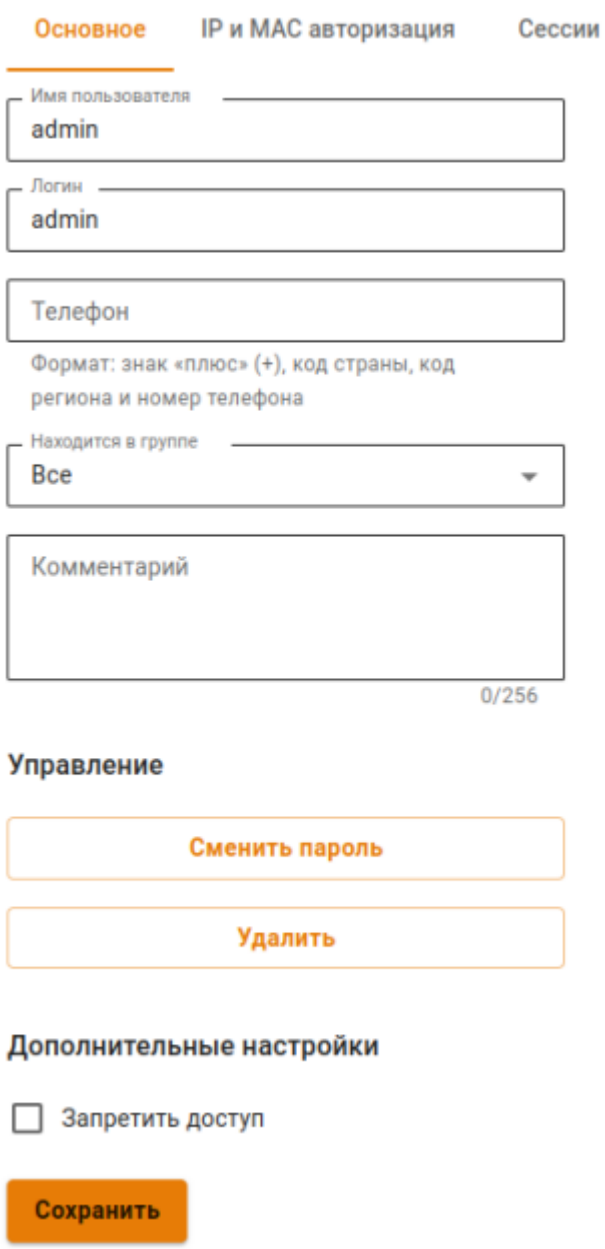
1. Перейти в раздел **Пользователи -> VPN-подключения -> Основное**.

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-подключения** (например, 10.128.0.0/16).

Чтобы настроить **статическую** привязку адресов, выдаваемых по VPN определенным пользователям, необходимо перейти в раздел **Пользователи -> VPN-подключения -> Правила выдачи IP-адресов**, 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 помощью клиента 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*.

14.4.6 Подключение по PPPoE

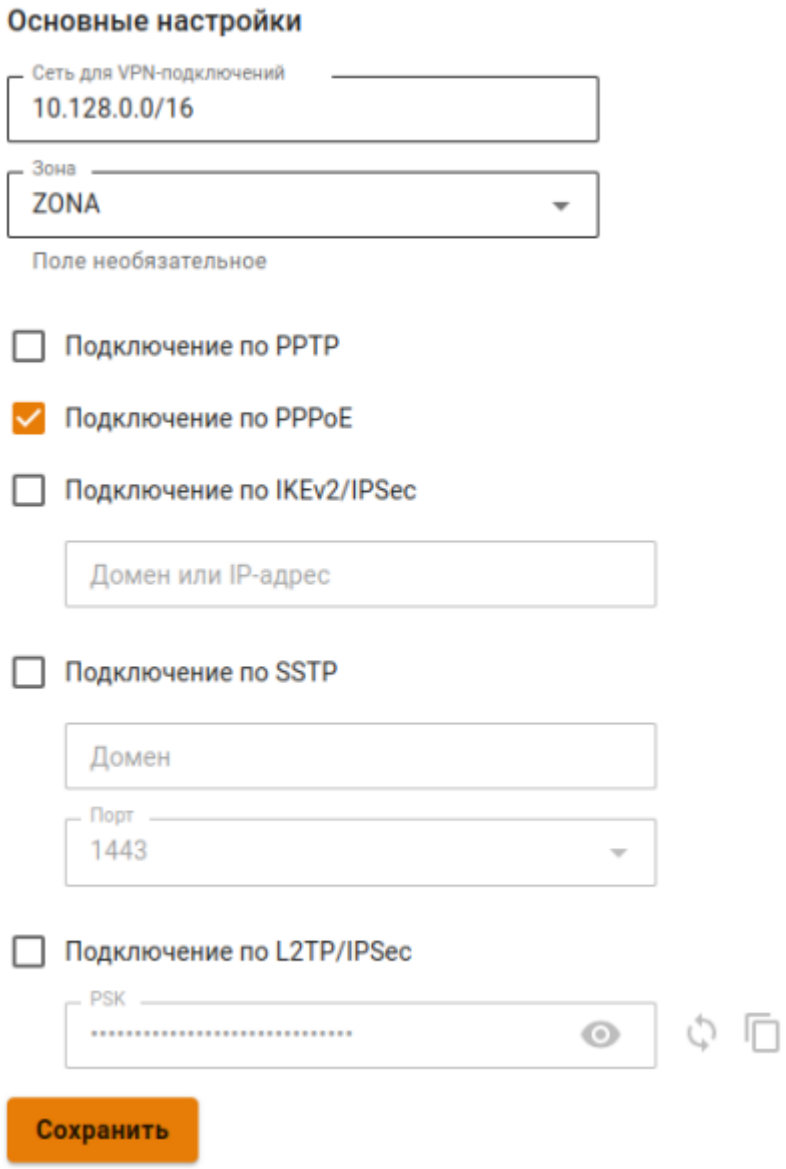
Основное

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.

14.4.7 Подключение по IKEv2/IPsec

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

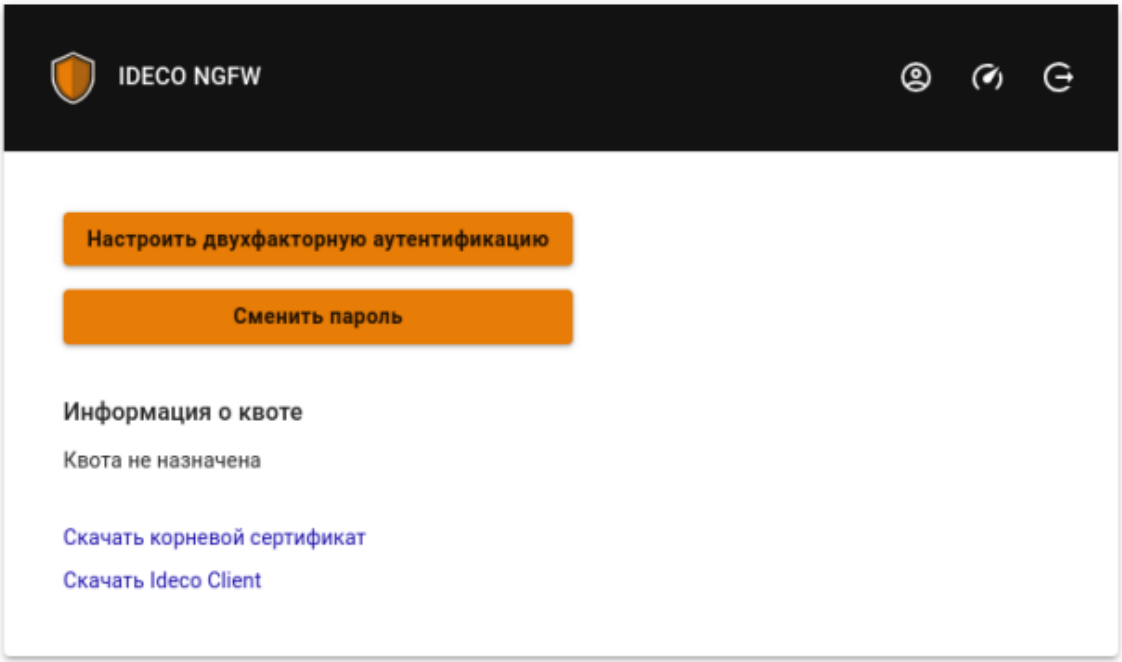
Инструкции по настройке VPN-подключений на разных ОС доступны по *ссылке*.

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

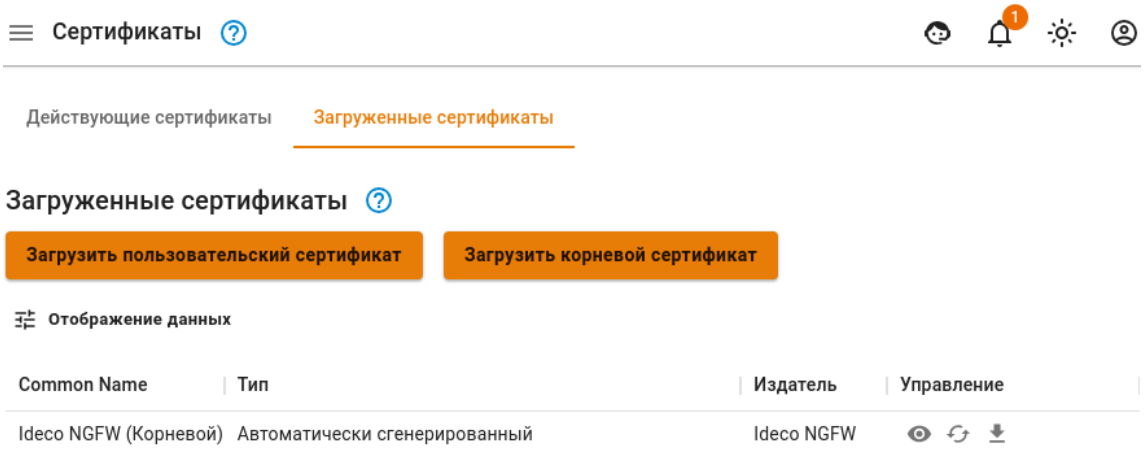
Настройка VPN-сервера в Ideco NGFW

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:

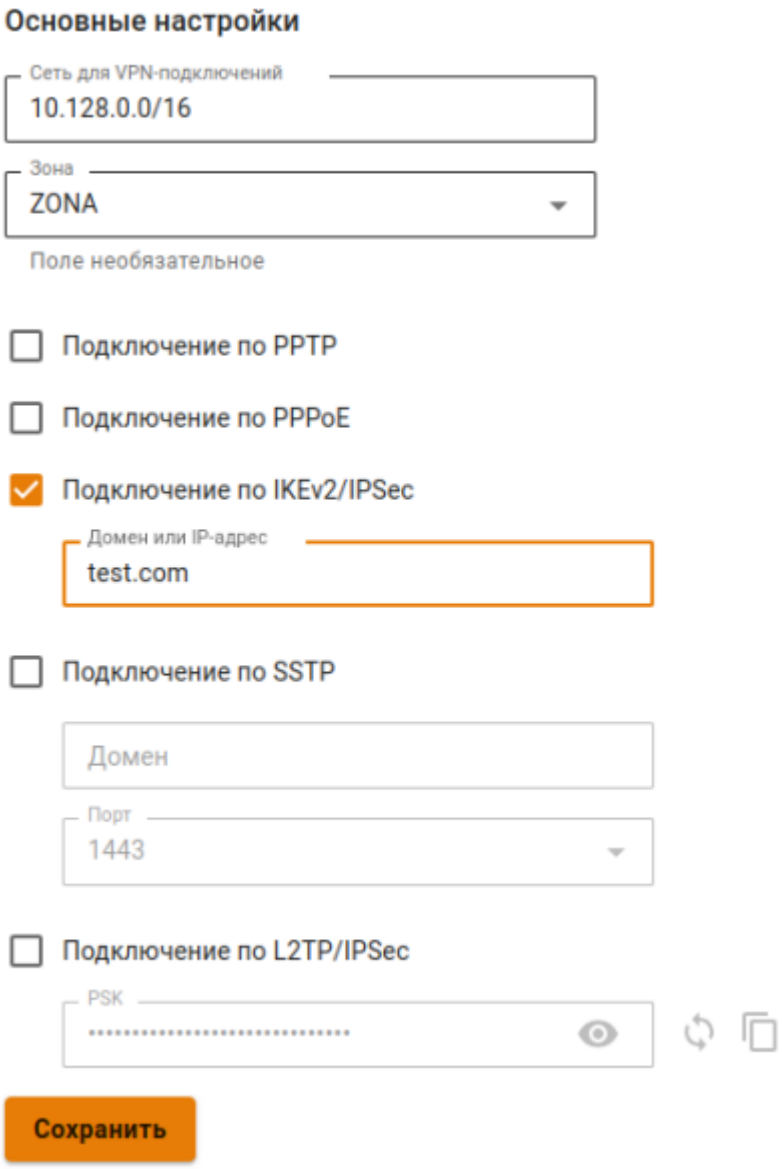


- В разделе **Сервисы -> Сертификаты -> Загруженные сертификаты**:



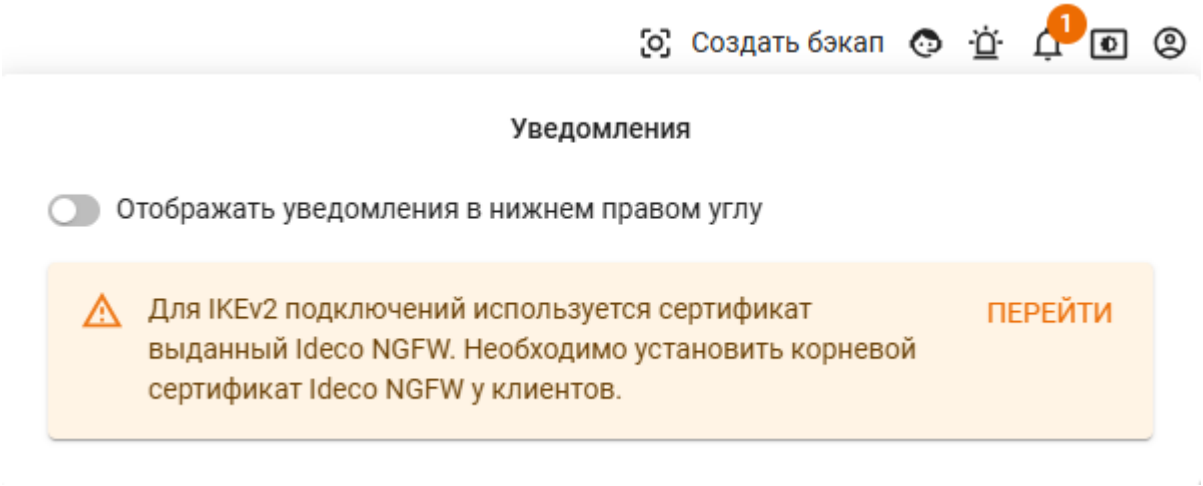
1. Для включения авторизации по IKEv2 установите соответствующий флаг **Подключение по IKEv2/IPsec** в разделе веб-интерфейса **Пользователи -> VPN-подключения -> Основное**.

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



Подсказка:

- Если используется сертификат Let's Encrypt, то дополнительных действий не требуется.
- Если сертификат для VPN-подключений издан NGFW, появится уведомление о необходимости установить корневой сертификат Ideco NGFW у клиентов:



- Если используете сторонний сертификат (например, от коммерческих Certificate Authority), убедитесь, что домен указан в поле **Subject Alternative Name (SAN)**. Загрузите сертификат как пользовательский в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты**. 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.

14.4.8 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.

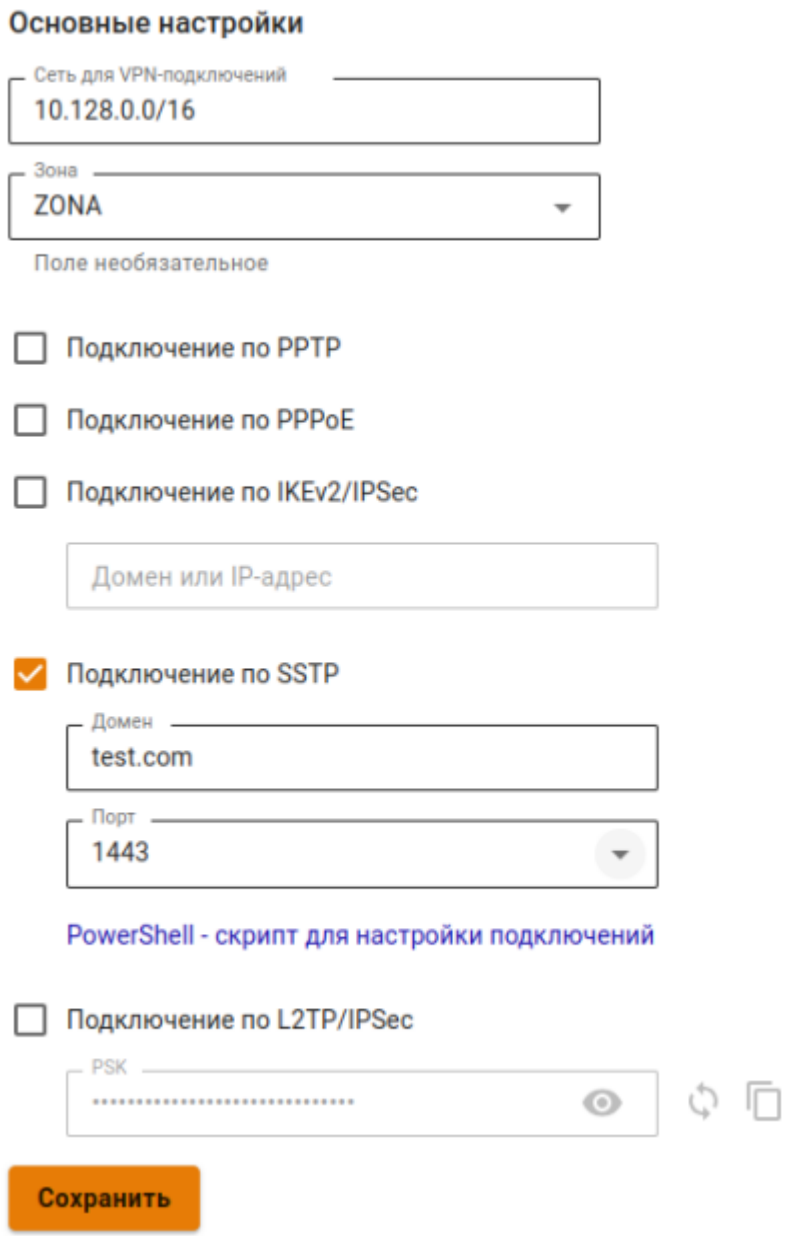
Настройка Ideco NGFW

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-подключения -> 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*.

14.4.9 Подключение по L2TP/IPsec

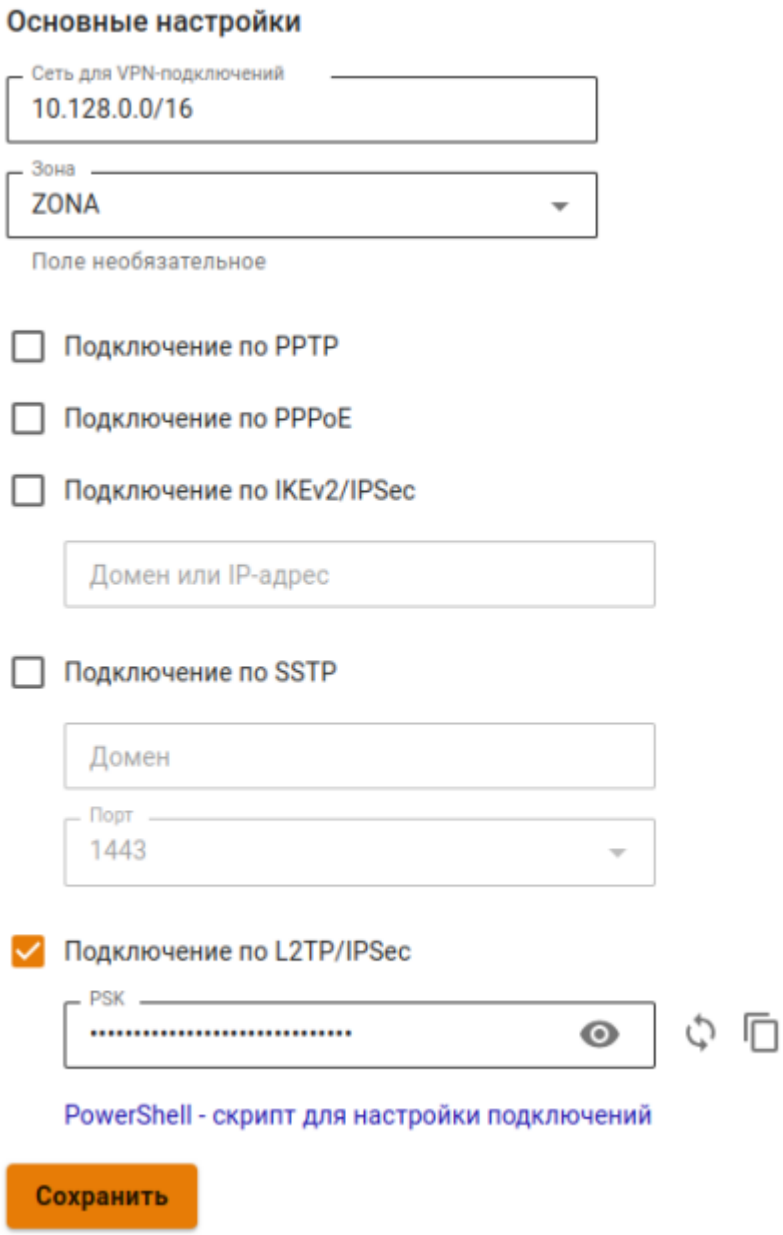
Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

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-подключения -> 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

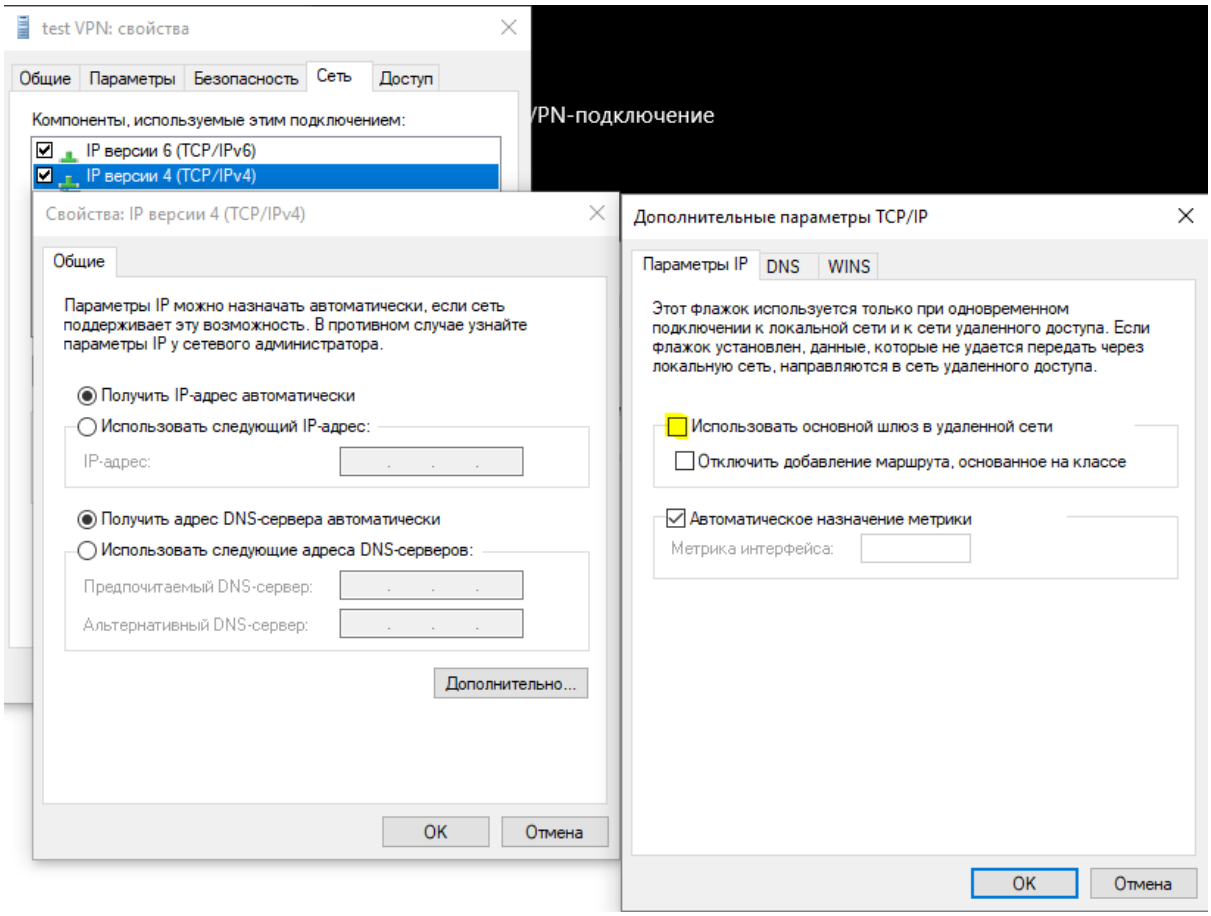
Выполните рекомендации статьи *Особенности маршрутизации и организации доступа*.

14.4.10 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:

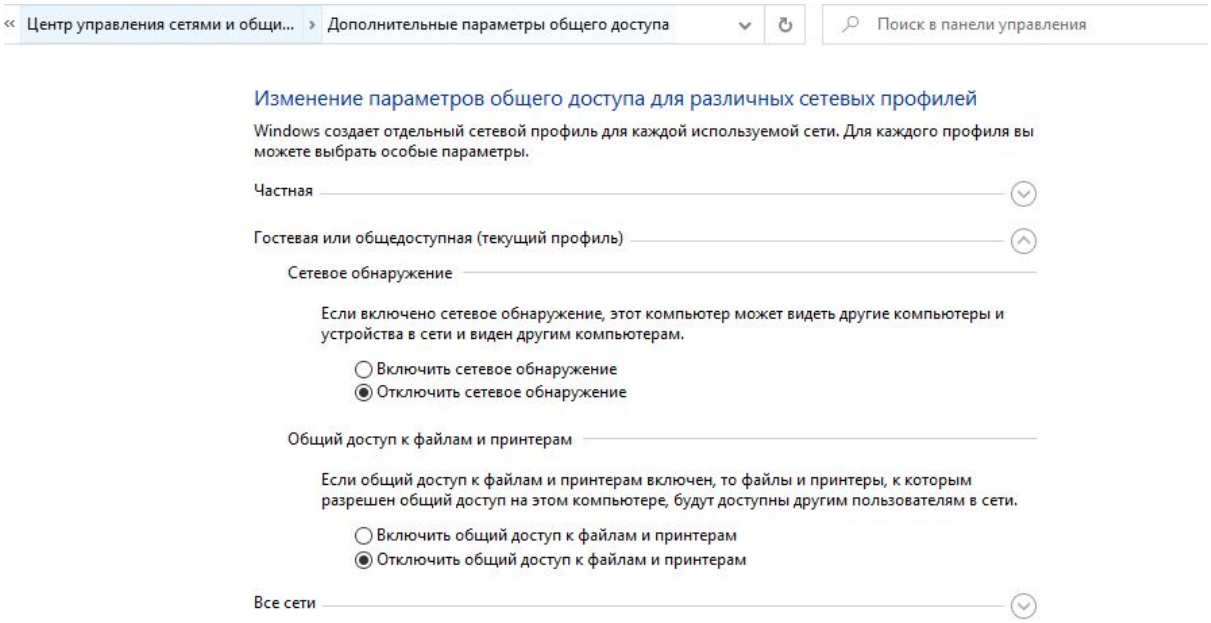
  `route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn`,

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):

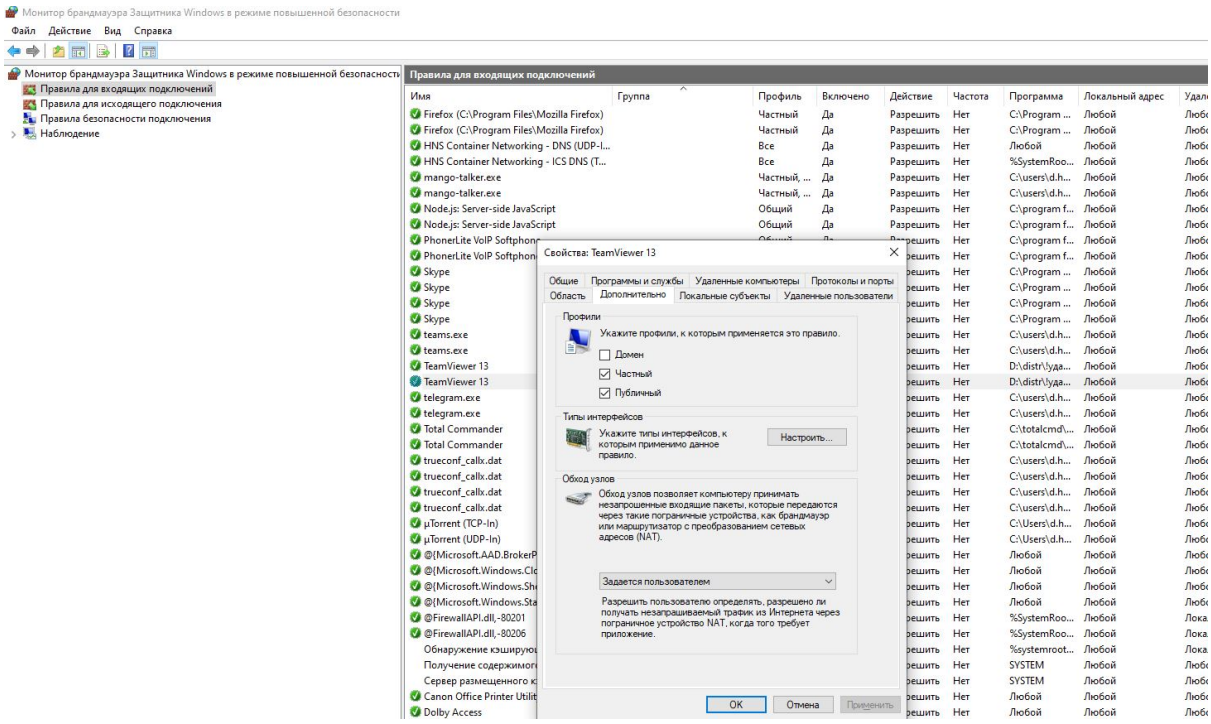


Включите доступ к файлам и принтерам для профиля «Все сети» и «Частных сетей».

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

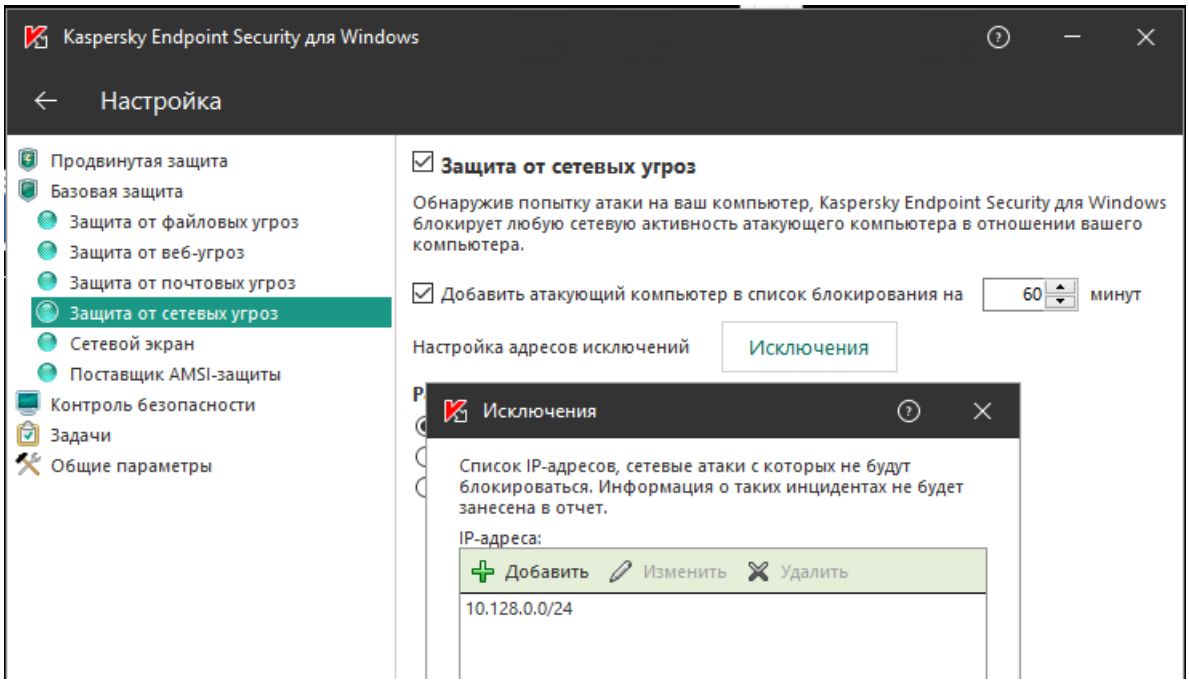
- Брандмауэр Защитника Windows может блокировать доступ определенных программ или сервисов (включая RDP) до внешних сетей;

  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:

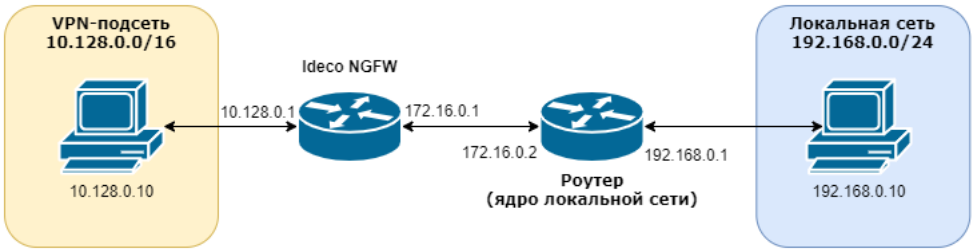


Если нет доступа к локальной сети Филиала

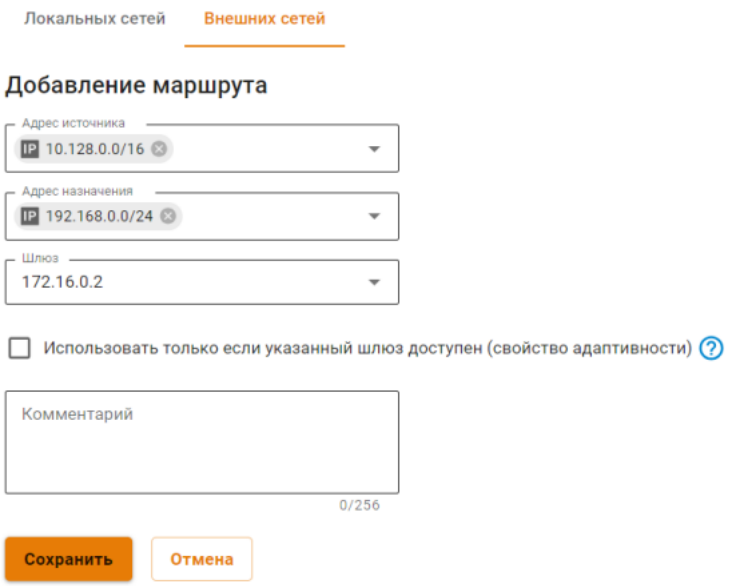
Если нет доступа к локальным сетям другого NGFW при подключении по VPN с основого NGFW (при подключении между двумя NGFW по IPSec):

- 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:

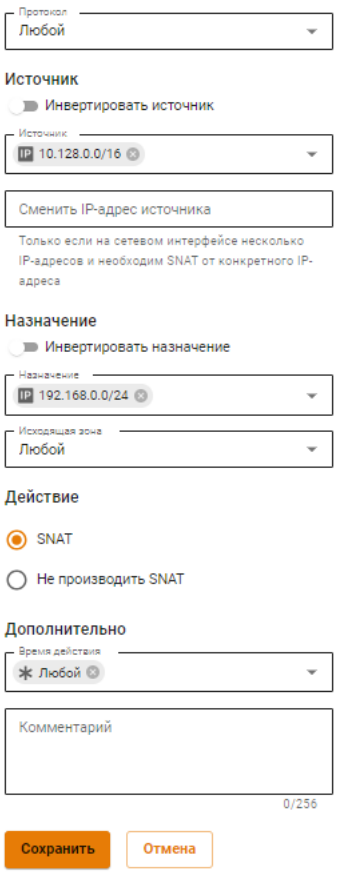


- `192.168.0.0/24` - сеть за роутером, к которой требуется получить доступ из VPN-сети;
- `172.16.0.2` - адрес роутера в локальной сети NGFW.

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`.

14.4.11 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;

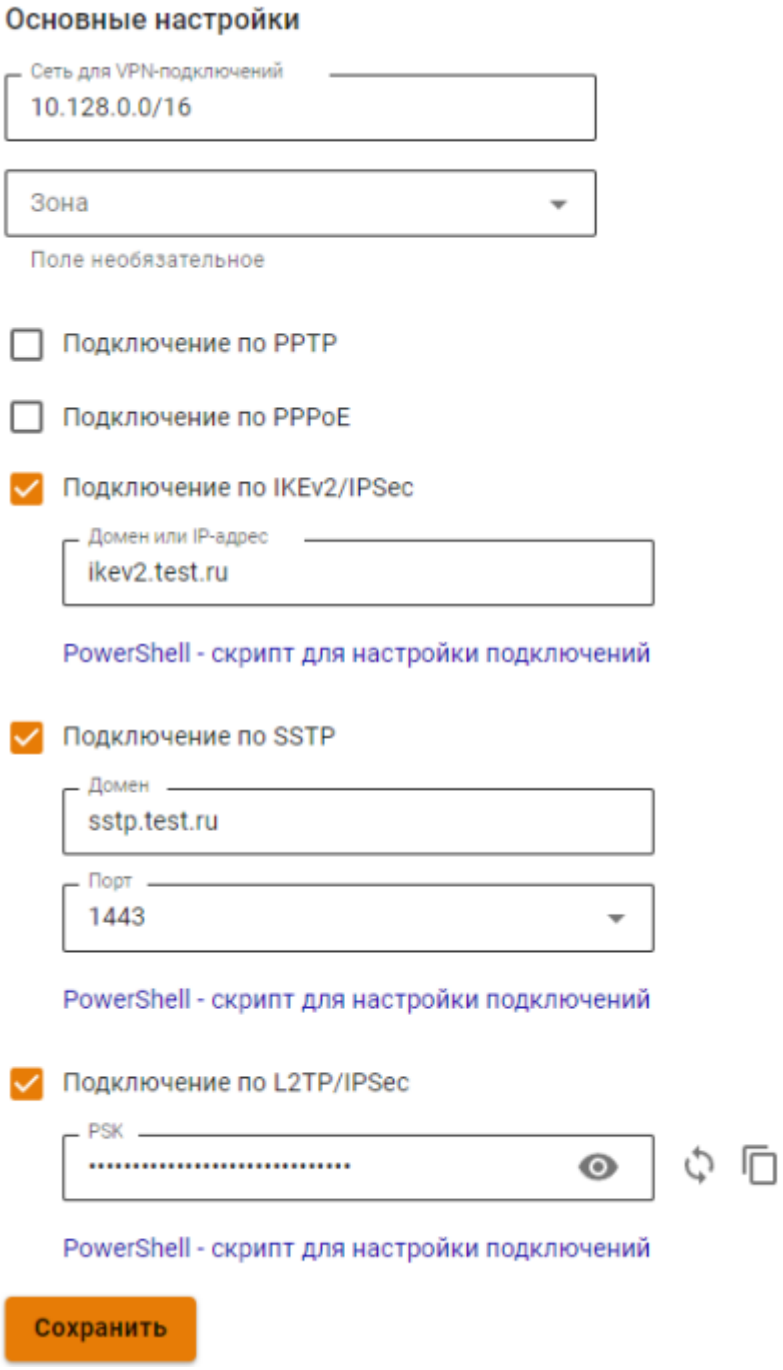
3. **L2TP/IPsec** - надежный в плане шифрования, но не самый оптимальный в плане скорости и производительности протокол.

Как запустить PowerShell-скрипт?

1. Скачайте скрипт одним из вариантов:

Из Ideco NGFW:

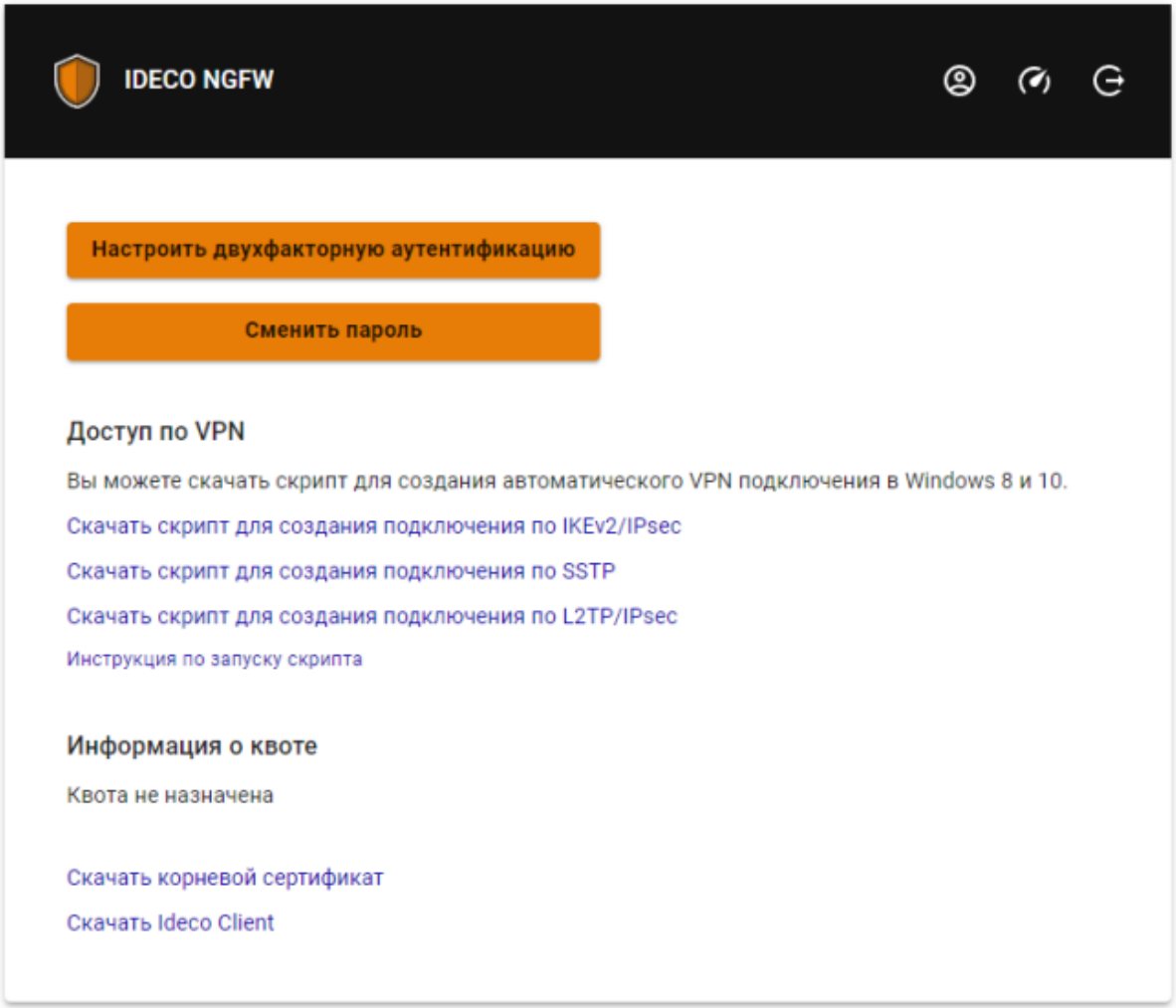
- Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**;
- Установите флаг у требуемого протокола подключения, если требуется, заполните поля и нажмите **Сохранить**;
- Кликните по ссылке **PowerShell - скрипт для настройки подключений**:



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

В личном кабинете пользователя:

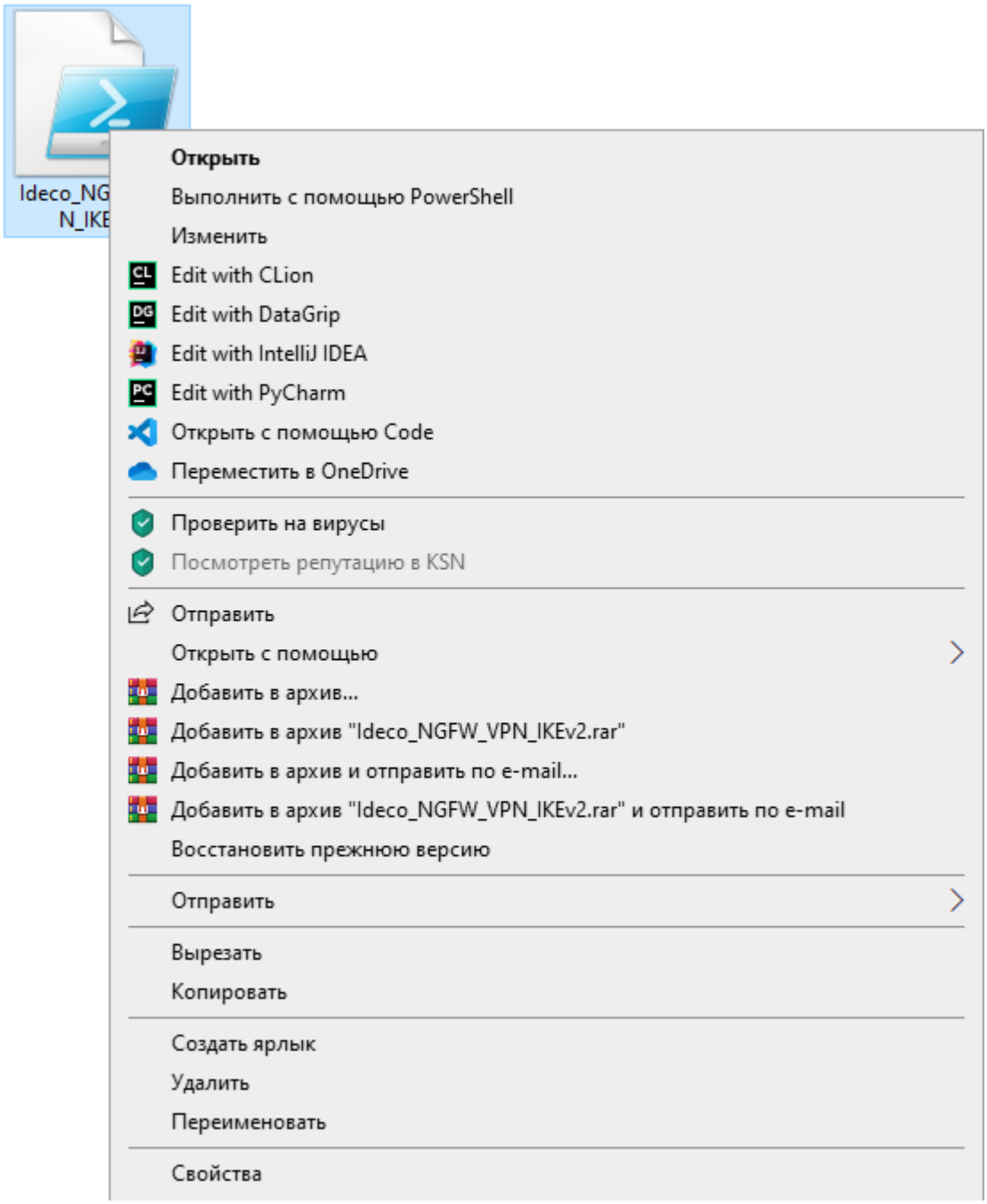
- Скачайте скрипт, кликнув по ссылке **Скачать скрипт для создания подключения**:



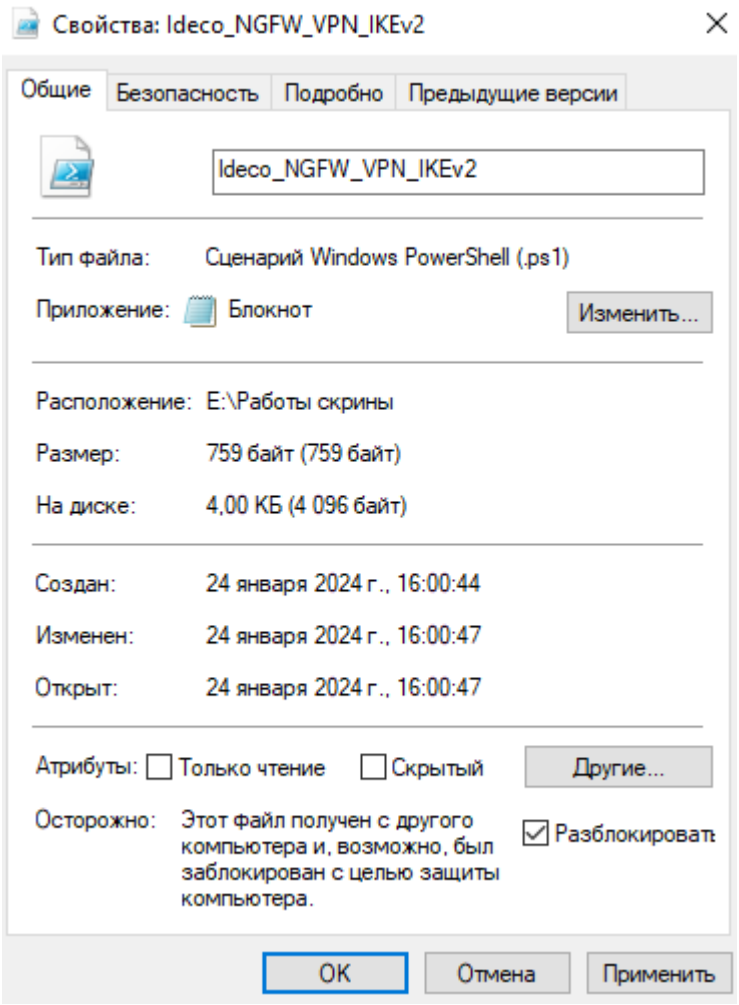
- Перейдите к выполнению пункта 2.

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*.

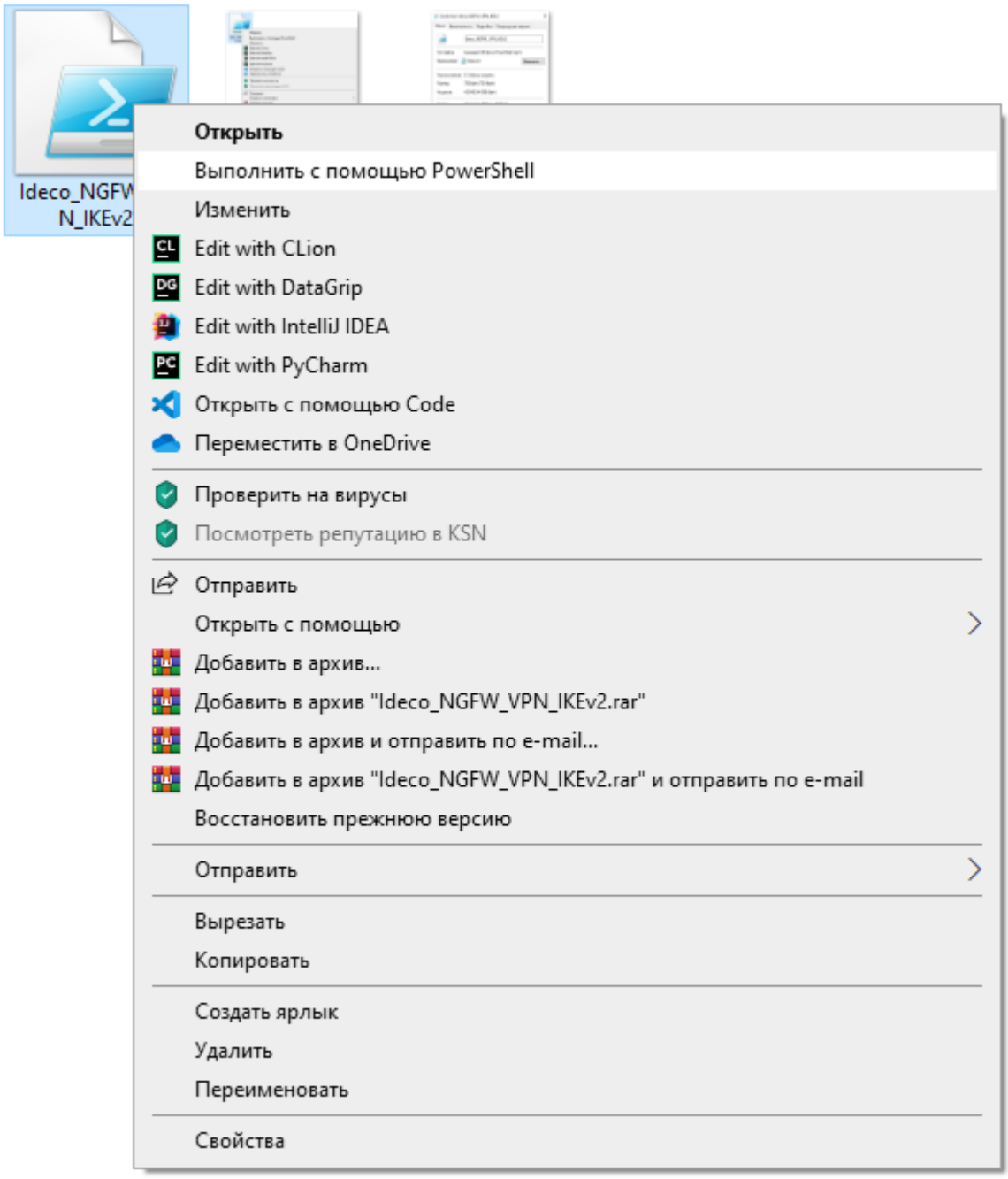
2. Щелкните правой кнопкой мыши по скачанному файлу и в контекстном меню выберите **Свойства**.



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



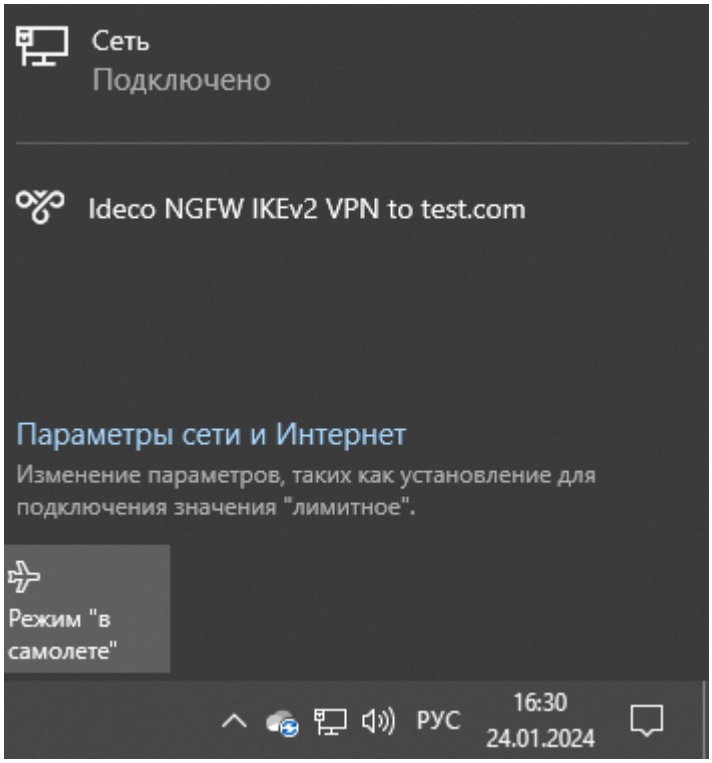
4. Нажмите правой кнопкой мыши на файл и выберите **Выполнить в PowerShell** в контекстном меню:



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.



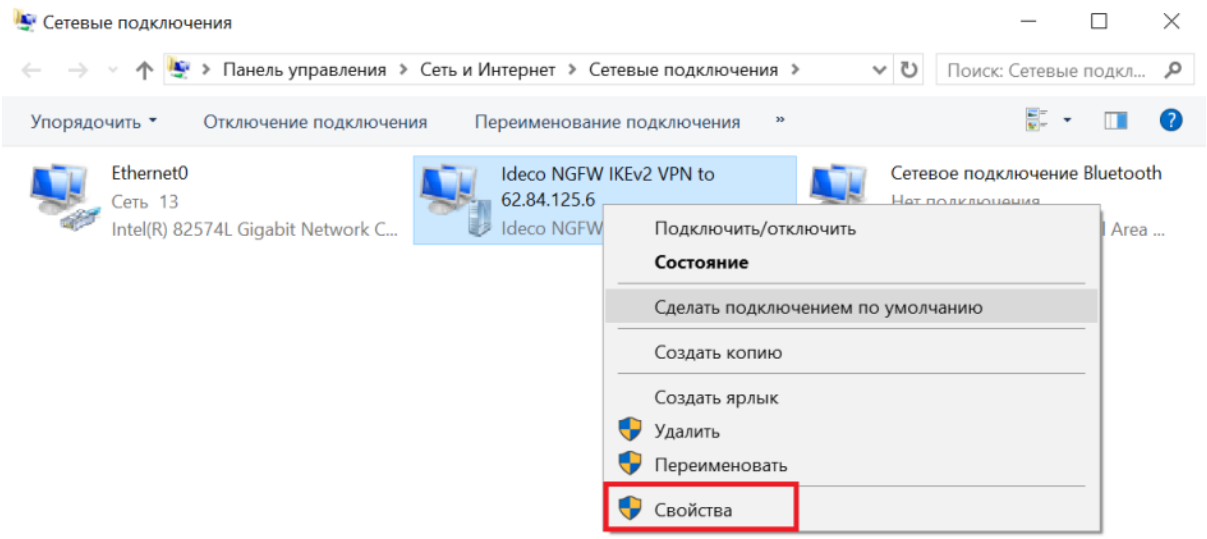
DNS-суффиксы для VPN-подключений

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.

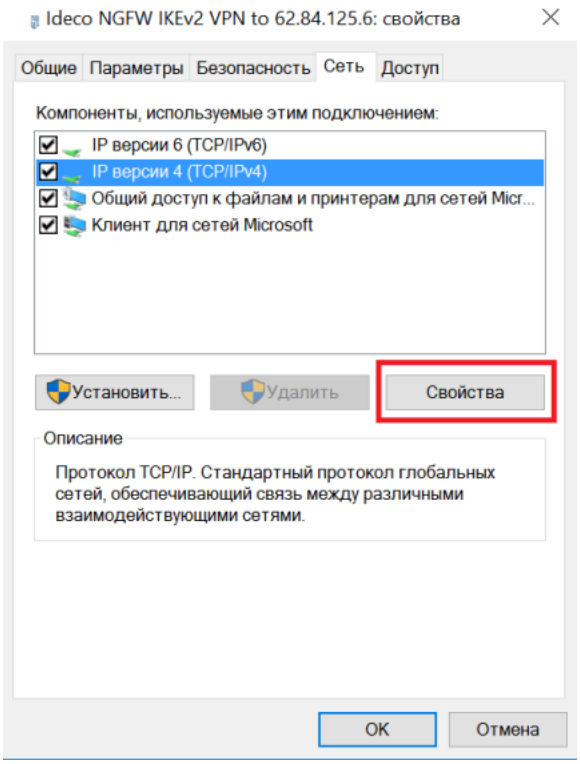
> **Предупреждение:** Если Ideco NGFW введен в несколько доменов, то DNS-суффиксы в PowerShell-скриптах не прописываются, их необходимо настраивать вручную на подключенном по VPN устройстве.

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

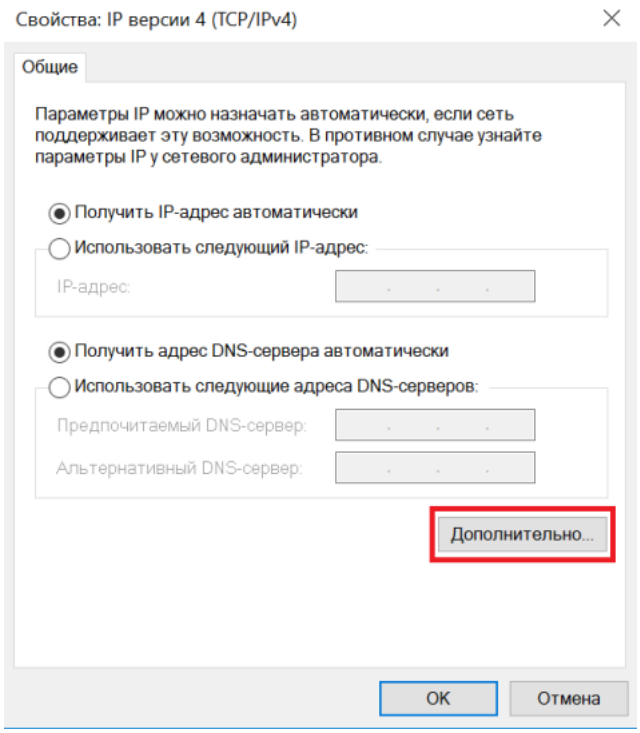
1. Перейдите в **Сетевые подключения**, нажмите правой кнопкой мыши по нужному VPN-подключению и выберите **Свойства**:



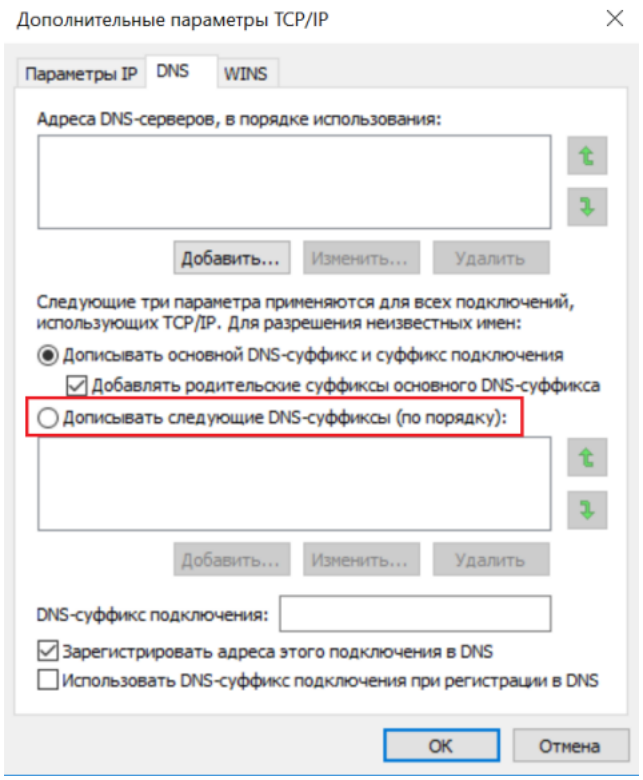
2. В открывшемся окне перейдите на вкладку **Сеть**, выберите компонент **IP версии 4 (TCP/IPv4)** и нажмите кнопку **Свойства**:



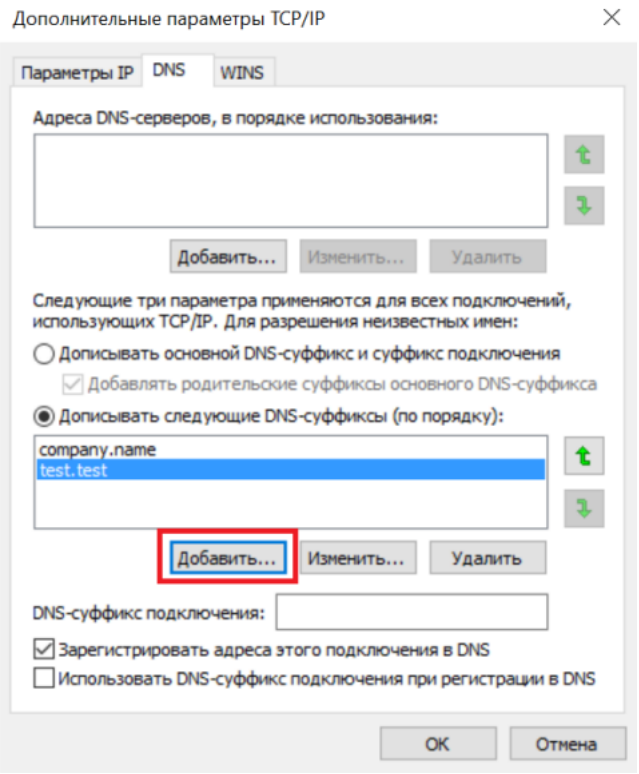
3. В открывшемся окне нажмите на кнопку **Дополнительно**:



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.

4. 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.

14.5 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 на ОС семейства Windows с 10 версии и новее, а также на MacOS версии 12.7 и новее. На MacOS Ideco Client работает с *некоторыми ограничениями*.

Ideco Client управляет авторизацией пользователей при подключении к Ideco NGFW в локальной сети и по VPN из внешних сетей (при использовании Ideco Client на MacOS возможна авторизация только пользователей локальной сети).

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.

14.5.1 Особенности работы Ideco Client

- Опцией автоматического подключения может обладать только один профиль. При активации опции автоподключения другому профилю у предыдущего автоподключение будет отключено;
- Чтобы использовать SSO-профиль с включенным автоподключением, необходимо вручную указать доменное имя в поле **Хост**. Чтобы заранее настроить адрес подключения, воспользуйтесь групповой политикой или запустите файл через командную строку с ключом `IdecoAgent.msi utm_address=адрес_ngfw`;
- 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.

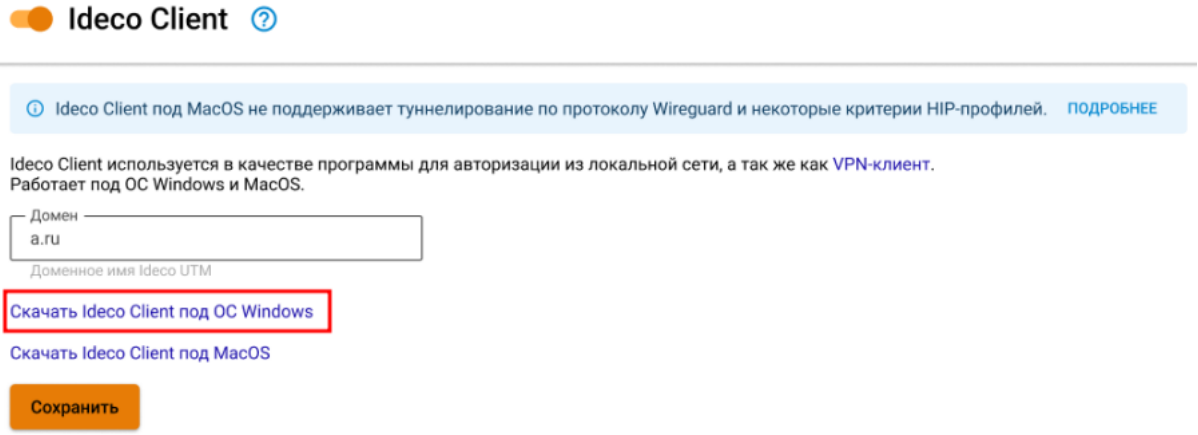
При подключении из локальной и внешней сети пользователи появятся в разных разделах:

- При подключении из внешней сети информация о сессии появится в разделах *Авторизованные пользователи* и *VPN-пользователи*;
- При подключении из локальной сети информация о сессии появится только в разделе *Авторизованные пользователи*.

14.5.2 Установка и настройка Ideco Client на Windows

Чтобы скачать файл установки **Ideco Client** для Windows:

- В личном кабинете пользователя нажмите на кнопку **Скачать Ideco Client под ОС Windows**;
- 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 под Windows**:



Установка

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

Если требуется заранее установить адрес подключения, в командной строке перейдите в директорию с файлом `cd [путь до файла]` и откройте файл с ключом `IdecoAgent.msi utm_address=адрес_ngfw`.

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

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

Настройка профиля для первого запуска

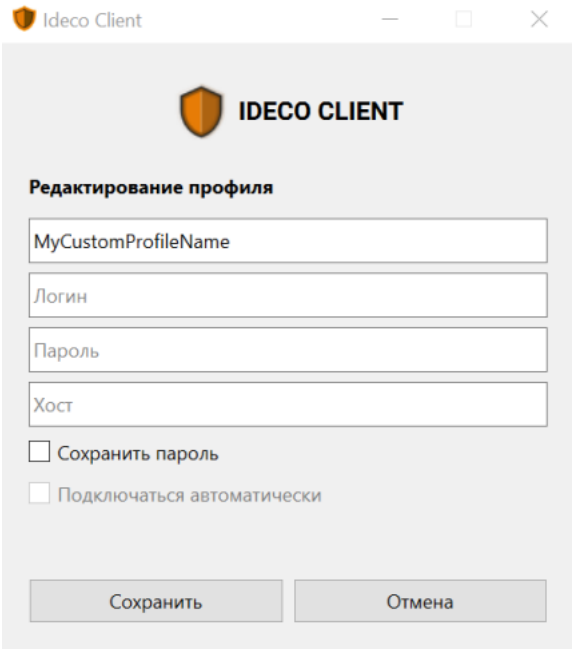
Предупреждение: Перед подключением к Ideco NGFW по внешнему IP-адресу или доменному имени без сертификата `Let's encrypt` импортируйте корневой сертификат Ideco NGFW на компьютер.

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**.

После установки запустите Ideco Client. Программа установит связь с сервером и предложит ввести данные.

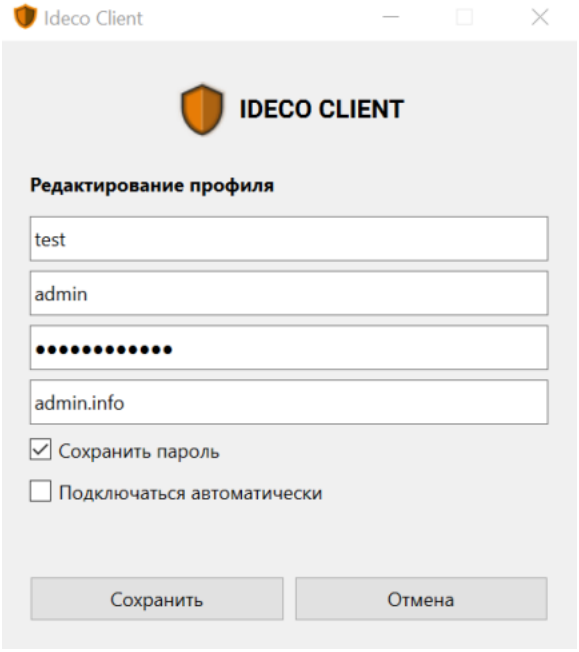
1. Задайте имя профиля. Оно может не совпадать с логином и будет использоваться при выборе профиля для авторизации:



2. Укажите логин и хост в зависимости от количества доменов, в которые введен NGFW:

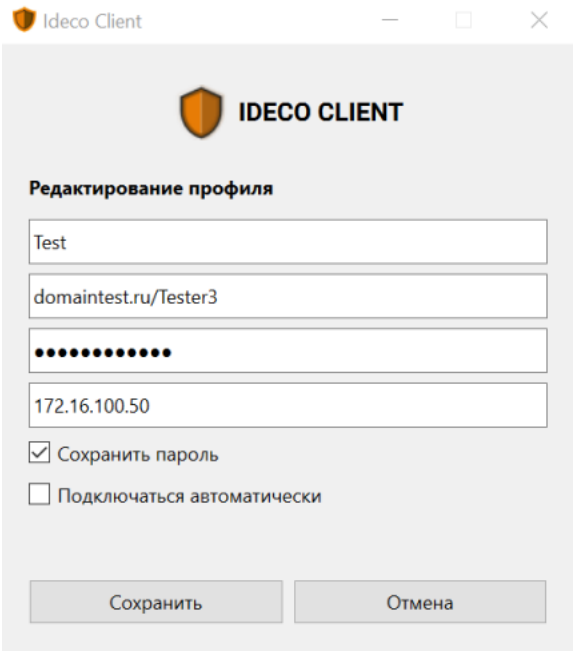
NGFW введен в один домен:

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



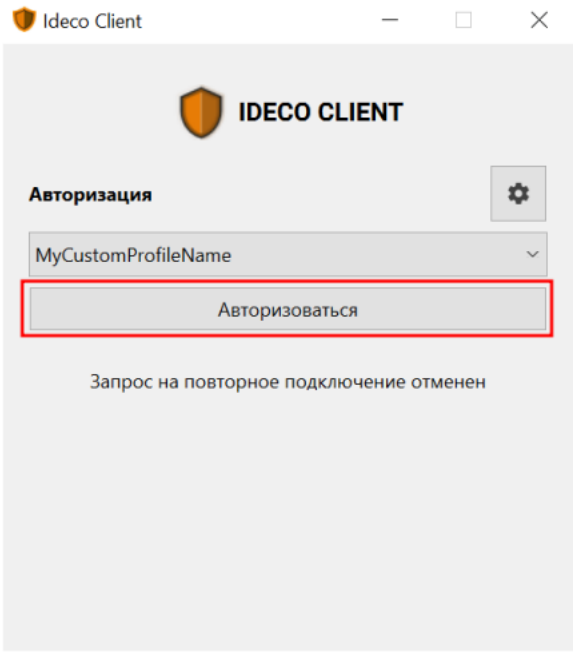
NGFW введен в несколько доменов:

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



3. Нажмите **Сохранить**, чтобы создать новый профиль пользователя для авторизации.

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



Редактирование профиля

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

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

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

14.5.3 Установка и настройка Ideco Client на MacOS

Подсказка: Ideco Client для MacOS требует версии системы 12.7 и выше.

Предупреждение: Особенности работы Ideco Client на MacOS:

1. *HIP-профили* на стороне агента поддерживаются **не в полном объеме**.

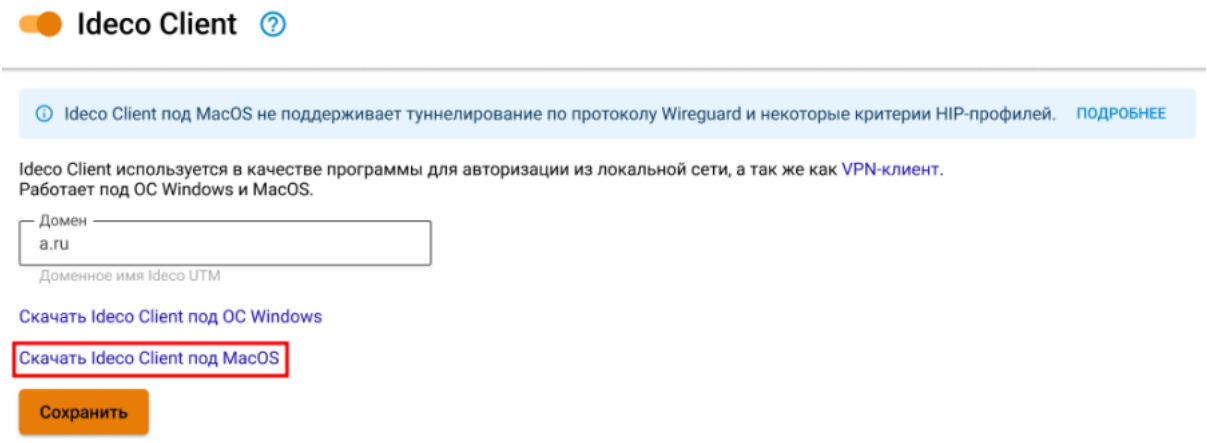
- Доступны только профили:
  - ОС;
  - процесс.
- **Недоступны** следующие HIP-профили:
  - антивирус;
  - домен;
  - межсетевой экран;
  - реестр (всегда только Windows);
  - службы (всегда только Windows);
  - пакет обновлений KB (всегда только Windows).

2. Ideco Client **не поддерживает** туннелирование по протоколу WireGuard. Возможна авторизация клиентов только в локальной сети;

4.**Недоступна** авторизация пользователей через их SSO-профиль в «тихом» режиме автоподключения;

Чтобы скачать файл установки **Ideco Client** для MacOS:

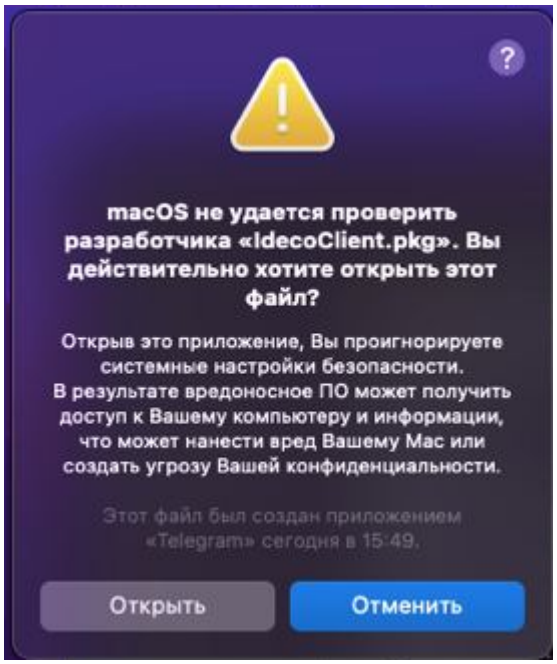
- В личном кабинете пользователя нажмите кнопку **Скачать Ideco Client для MacOS**.
- Перейдите в раздел **Пользователи –> Ideco-Client**, переведите опцию **Ideco Client** в положение включен, введите доменное имя в соответствующей строке и нажмите **Сохранить**. Появится кнопка **Скачать Ideco Client под MacOS**:



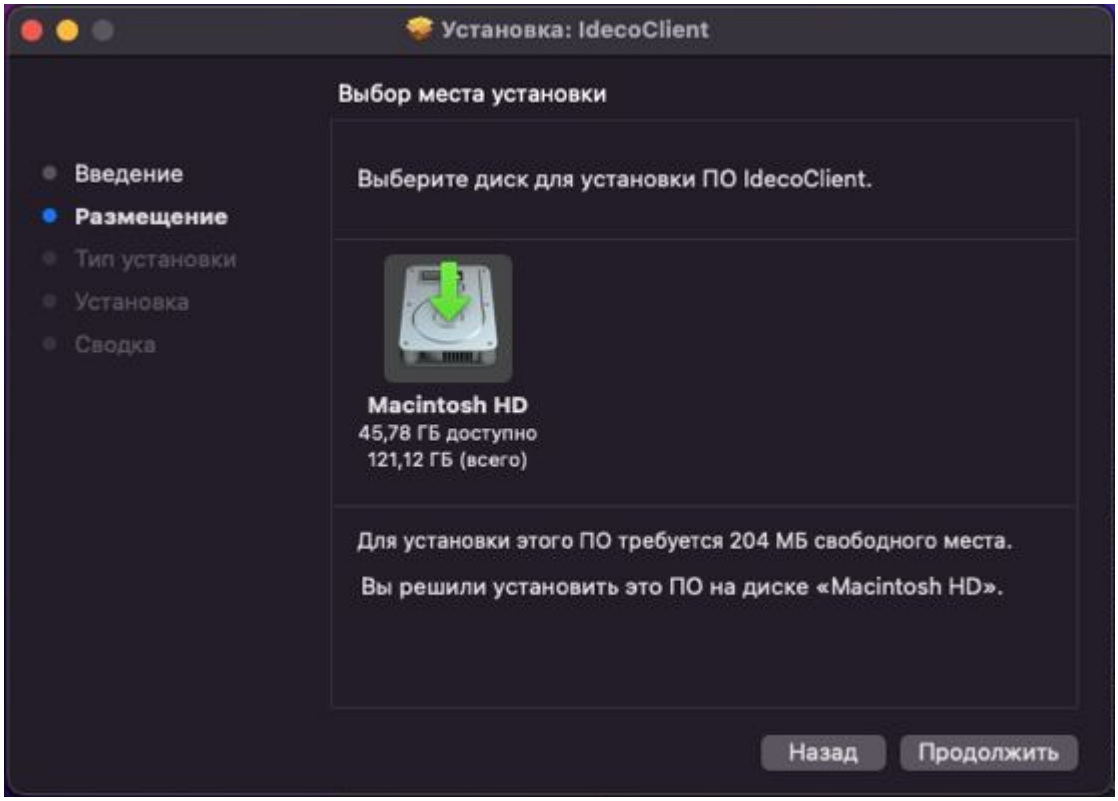
Установка

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

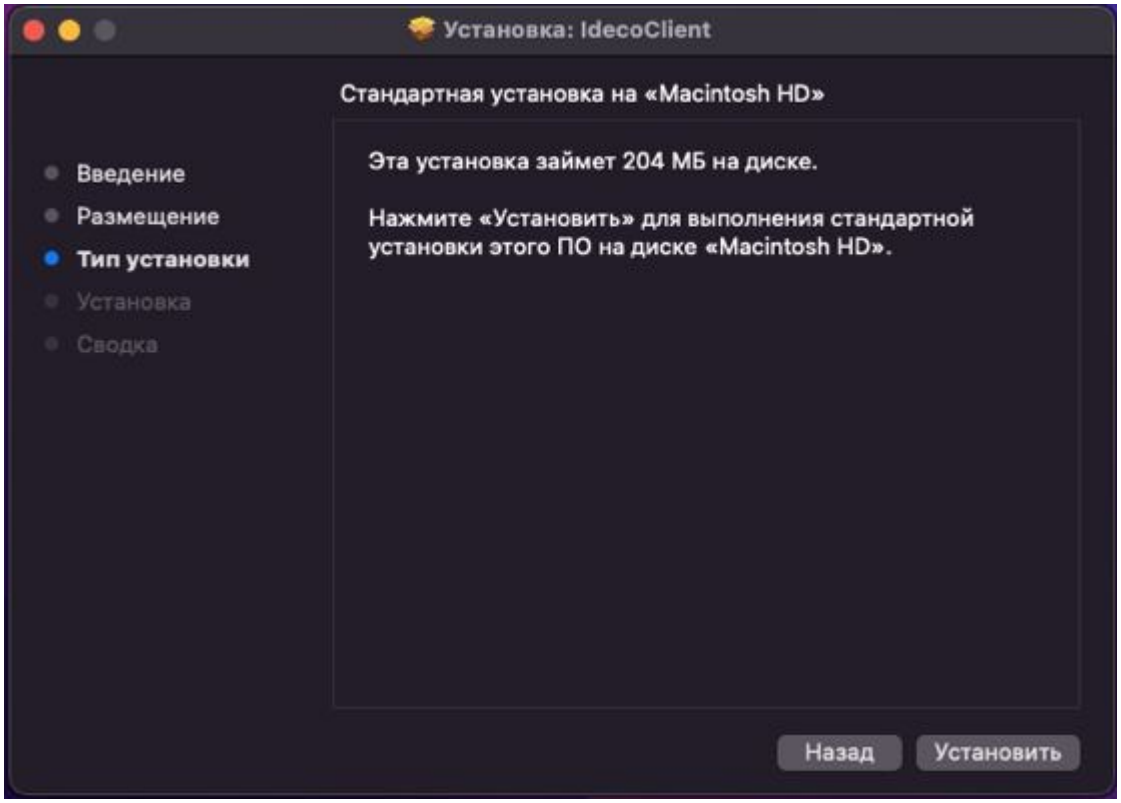
1. Кликните по файлу *IdecoClient.pkg* правой кнопкой мыши и выберите **Открыть**. Если система выдаст предупреждение, подтвердите действие:



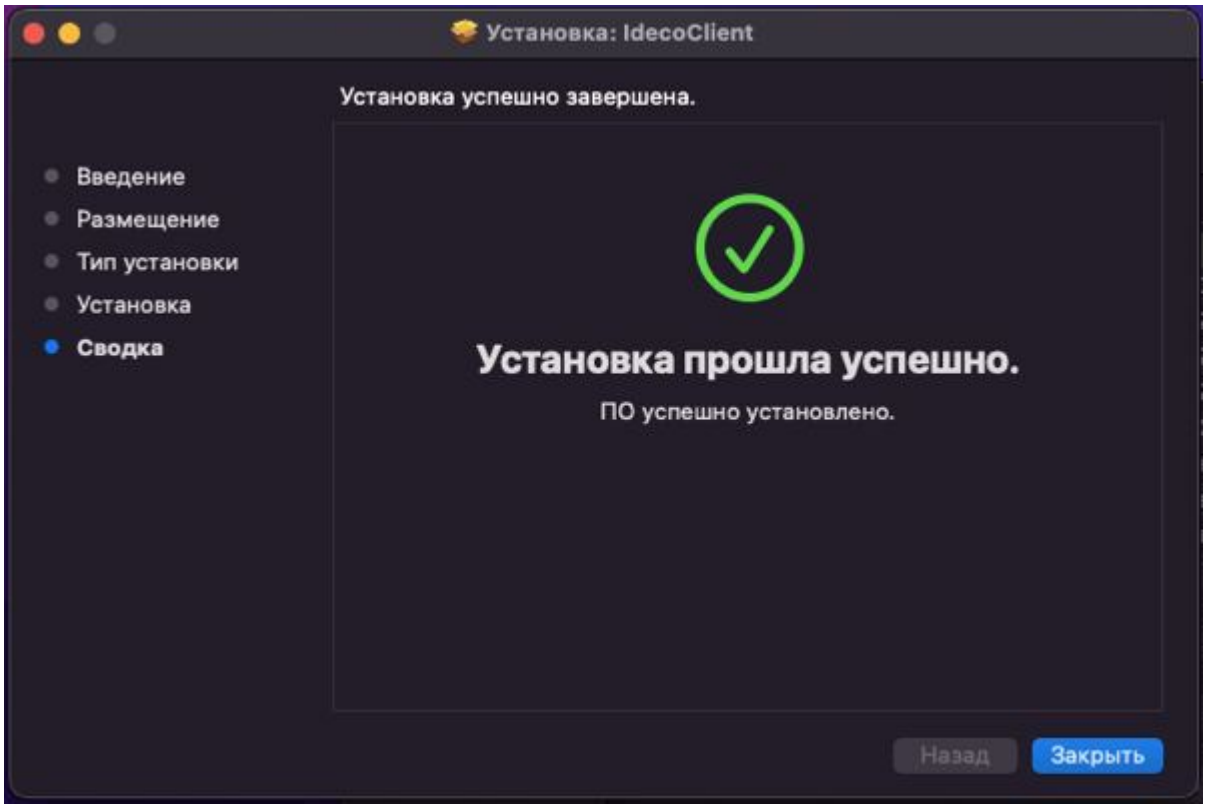
2. Нажмите **Продолжить**. Выберите диск для установки **Ideco Client**:



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



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



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 и убедитесь, что срок действия сертификата на домен или IP-адрес составляет **825 дней**.
>
> Если срок действия сертификата превышает 825 дней, *загрузите* на Ideco NGFW сертификат со сроком действия, не превышающим 825 дней, или *перевыпустите* автоматически сгенерированный сертификат.

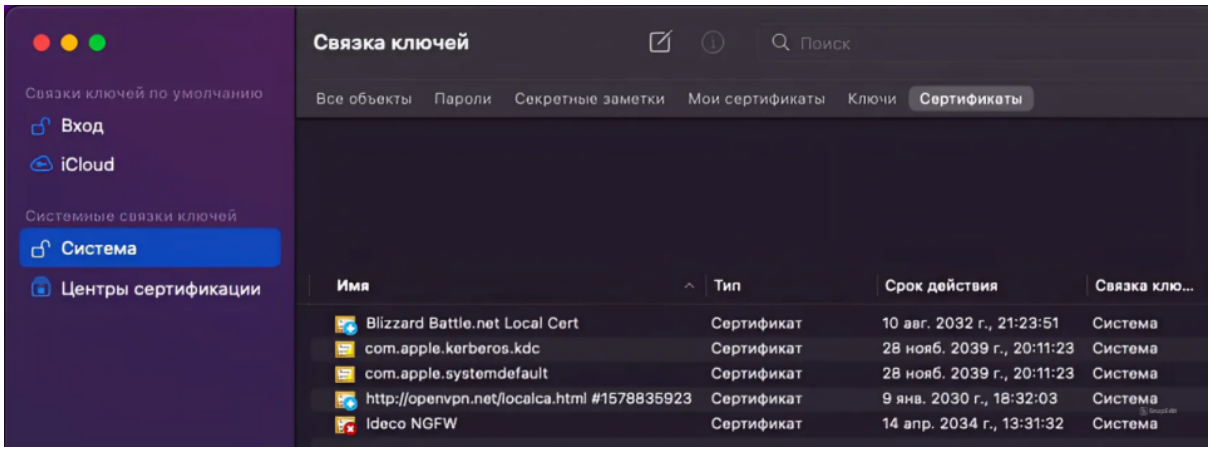
Установка корневого сертификата Ideco NGFW на MacOS:

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

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

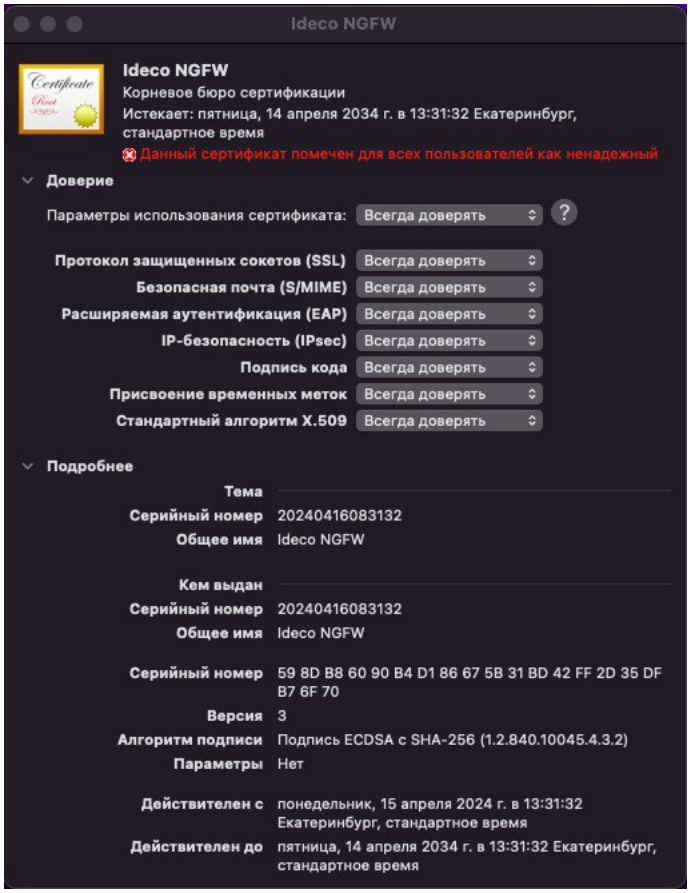
Чтобы установить сертификат на MacOS, выполните действия:

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

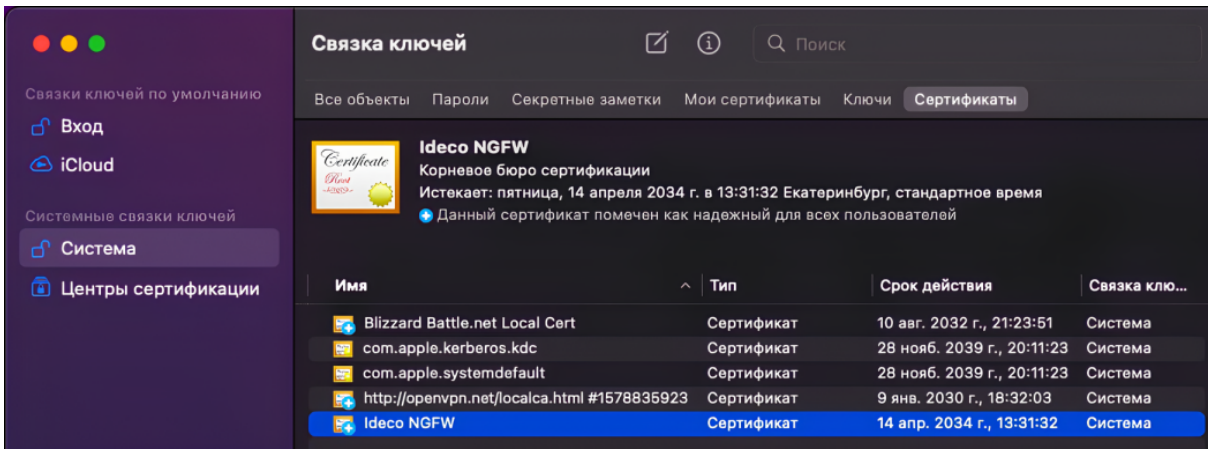


2. Нажмите по сертификату правой кнопкой мыши и выберите **Свойства**.

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



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

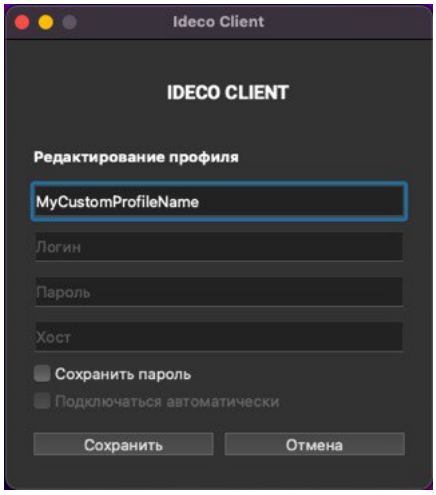


Также сертификат можно добавить с помощью команды:

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

После установки корневого сертификата запустите Ideco Client. Программа установит связь с сервером и предложит ввести данные.

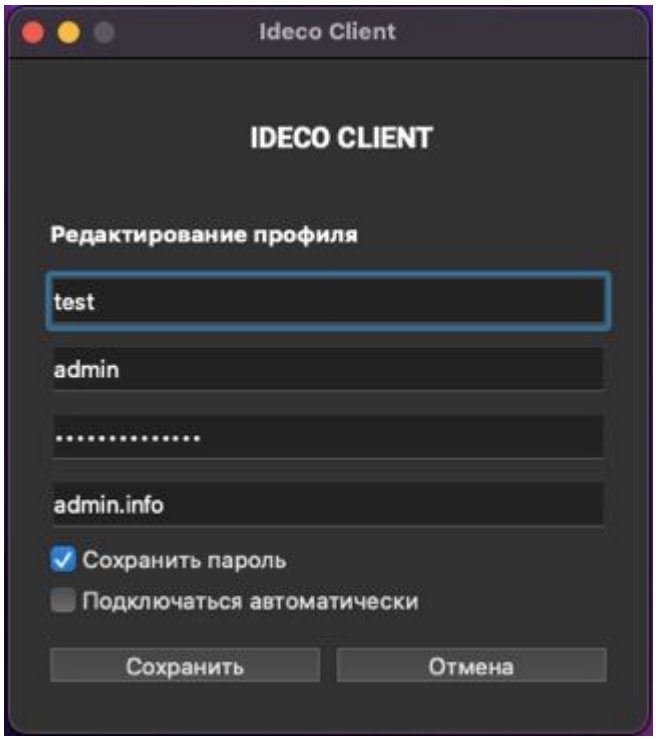
1. Задайте имя профиля. Оно может не совпадать с логином и будет использоваться при выборе профиля для авторизации:



2. Укажите логин и хост в зависимости от количества доменов, в которые введен NGFW:

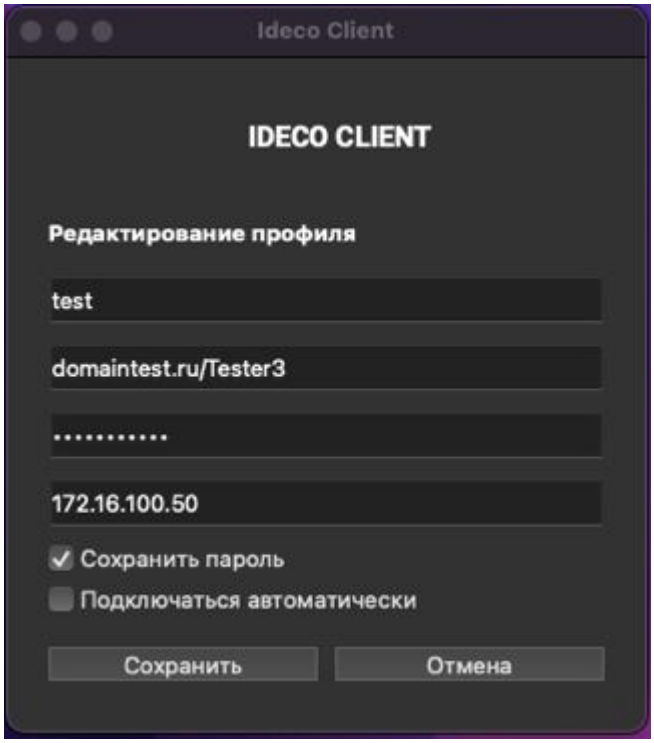
NGFW введен в один домен:

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



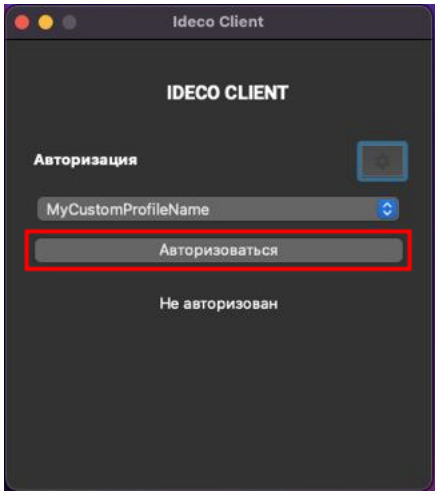
NGFW введен в несколько доменов:

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



3. Нажмите **Сохранить**, чтобы создать новый профиль пользователя для авторизации.

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



Редактирование профиля

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

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

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

14.6 Профили устройств

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

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

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

Информация, собираемая Ideco Client

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

Критерии проверки, доступные на NGFW

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

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

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

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

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

14.6.1 HIP-объекты

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

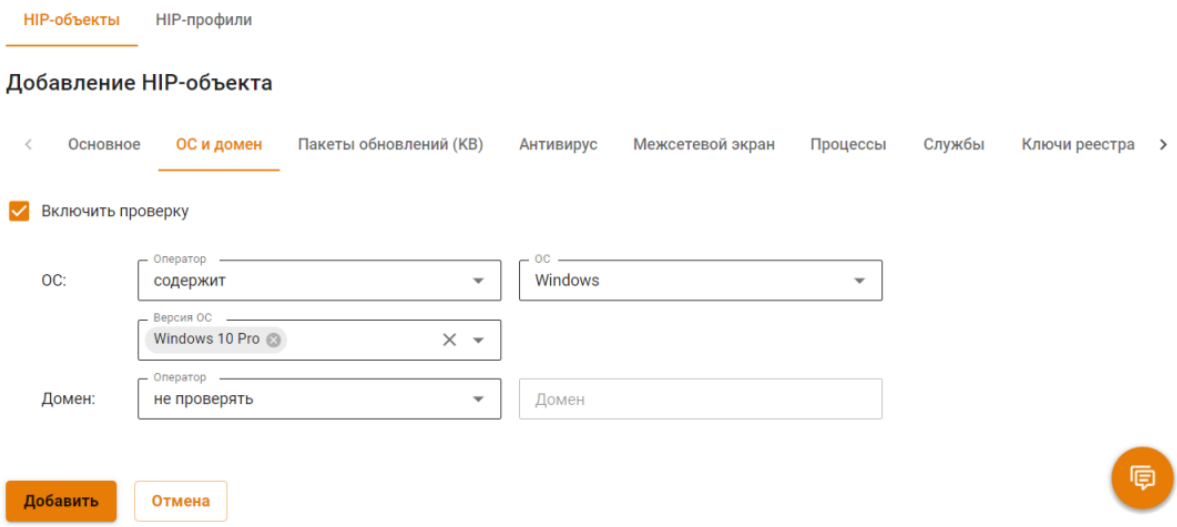
Для создания HIP-объекта выполните действия:

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

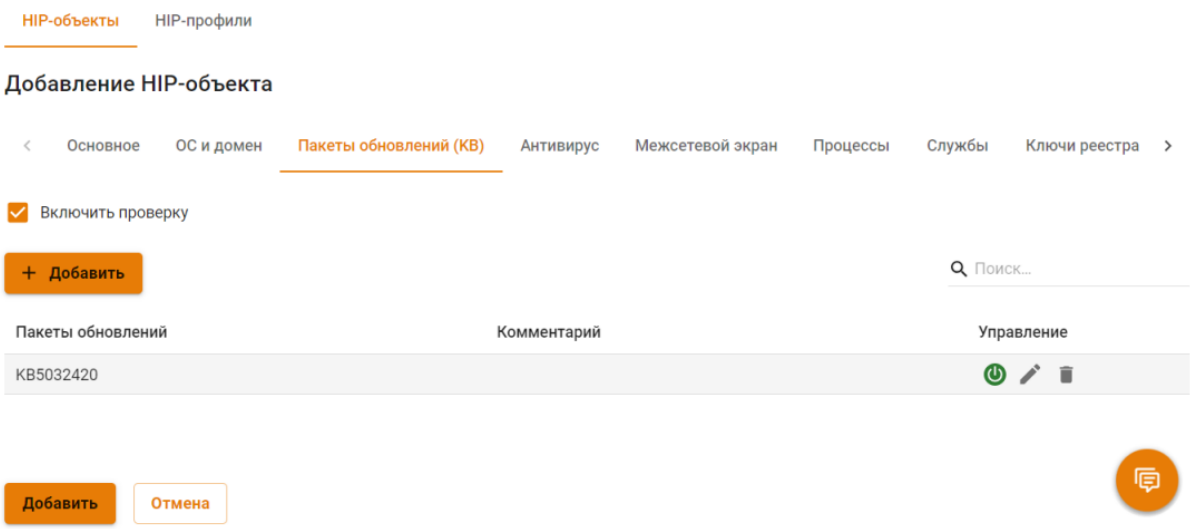
2. Введите **Название HIP-объекта** и выберите критерии для проверки:



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



Критерий может не содержать операторов:



4. После этого нажмите **Добавить**.

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

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

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

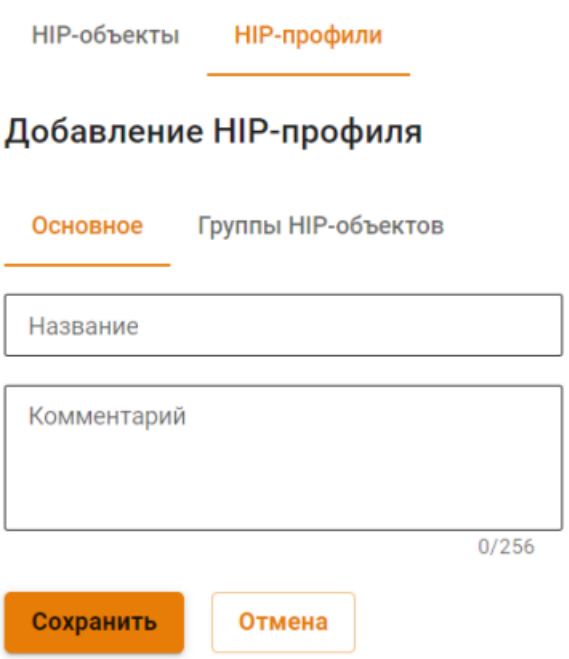
14.6.2 HIP-профили

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

Для создания HIP-профиля выполните действия:

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

2. Введите **Название HIP-профиля**:



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



5. Нажмите **Добавить**.

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

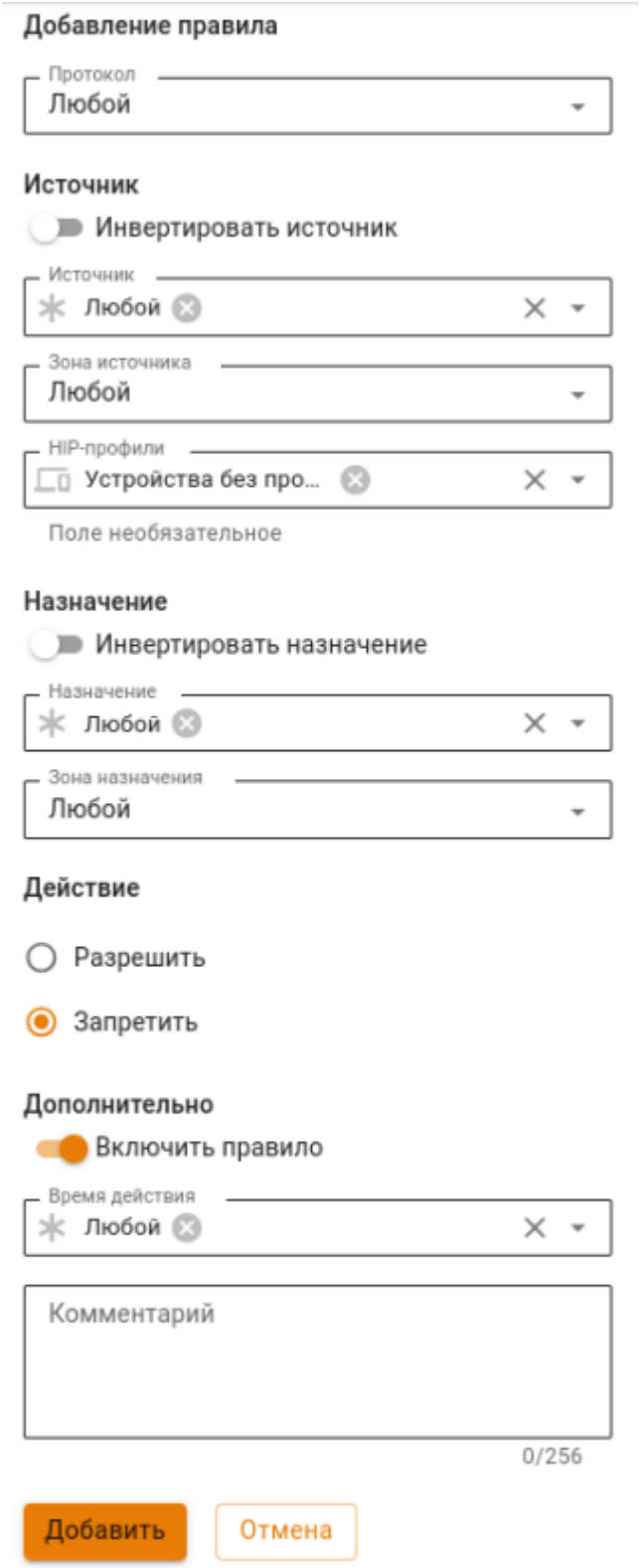
14.6.3 Примеры использования

Запрет доступа к сети устройствам без профиля:

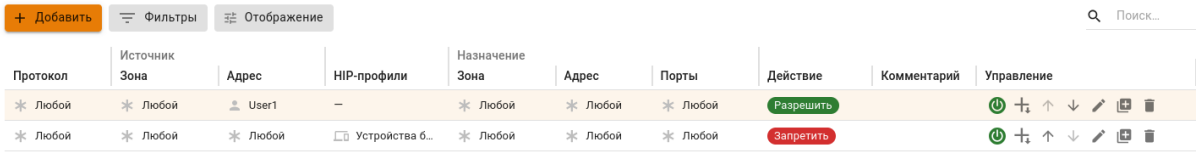
Устройствам, которые не прошли проверку на соответствие ни одному из созданных HIP-профилей, назначается специальный HIP-профиль **Устройство без профиля**. Доступ таких устройств к сети можно ограничить правилом **Файрвола**. Для этого:

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

2. Создадим правило вида:



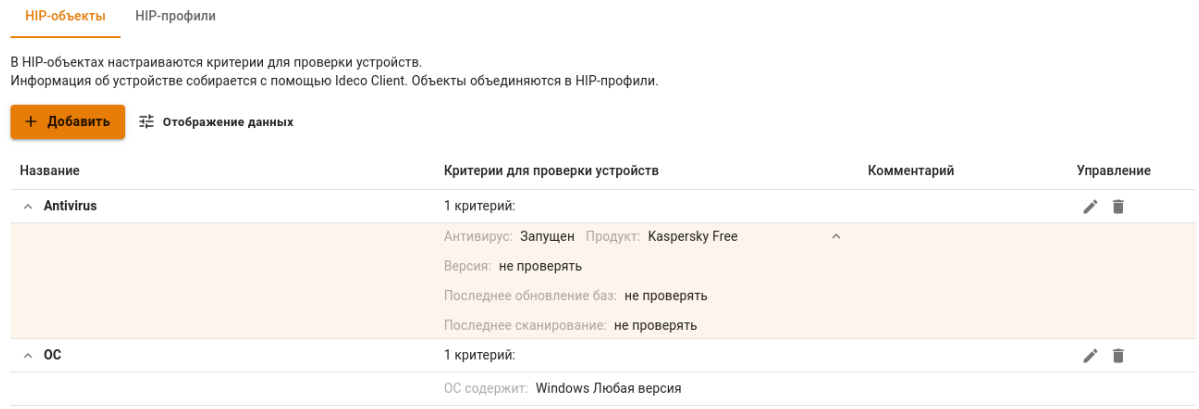
Важно! Если в таблице правил **Файрвола** выше запрещающего правило находится другое правило, которому соответствует трафик одного или нескольких устройств без профиля (например, правило для пользователя или группы пользователей без указания HIP-профиля), то к трафику будет применено правило, расположенное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



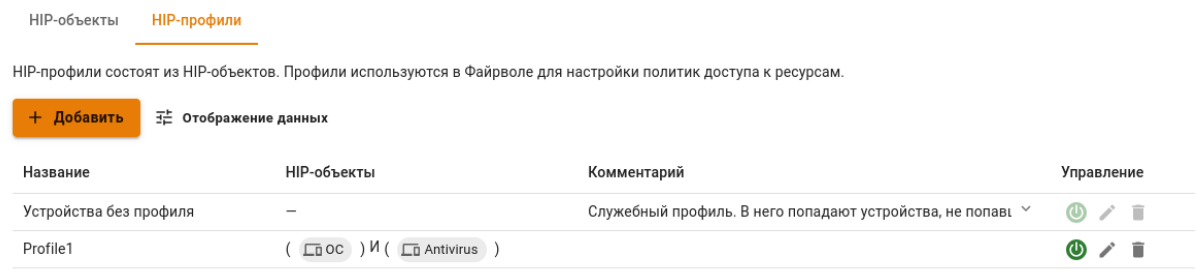
Ограничение доуступа устройств к сети:

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

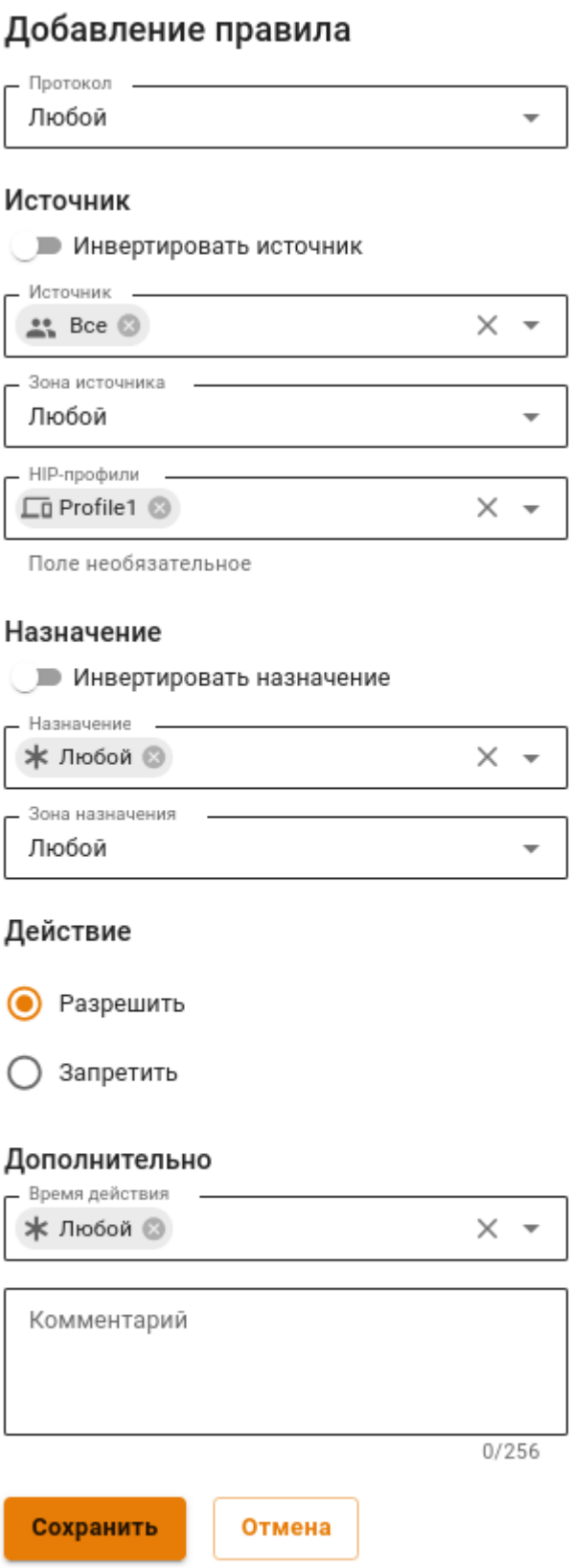
1. Перейдите в разде **Пользователи -> Профили устройств -> HIP-объекты** и создайте требуемые HIP-объекты:



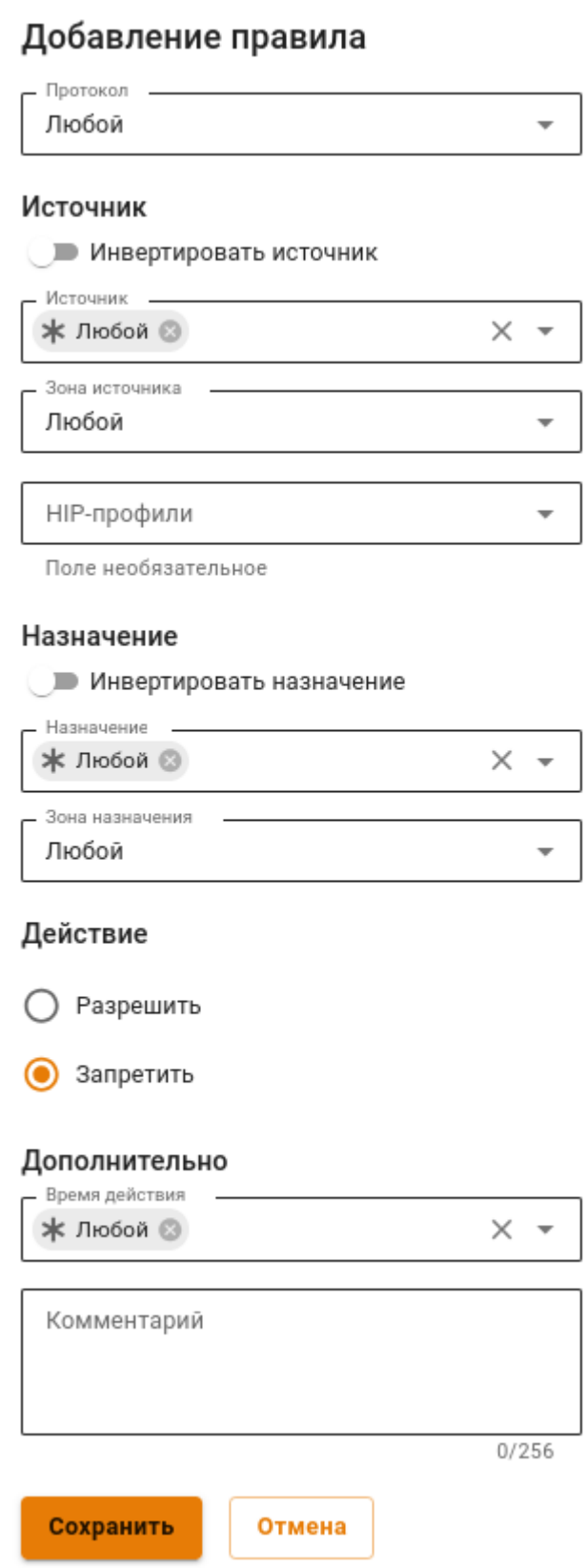
2. Перейдите на вкладку **HIP-профили** и создайте профиль с созданными ранее HIP-объектами:



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



4. Ниже создайте правило, запрещающее весь трафик:



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

14.7 Интеграция с Active Directory/Samba DC

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

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

Предупреждение: При импорте пользователей убедитесь, что учетные записи AD не имеют одинаковых логинов с локальными учетными записями. В противном случае система выдаст сообщение об ошибке.

14.7.1 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: Если локальные пользователи Ideco NGFW находятся в группах AD, приостанавливается синхронизация с контроллером домена. 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.

14.7.2 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 убедитесь, что учетные записи не имеют одинаковых логинов;
- При SSO-авторизации и первом открытии браузера пользователю будет предложен выбор домена для аутентификации. Выбор сохраняется с помощью cookie и используется при следующей авторизации. Если требуется изменить домен, очистите cookie (для локального IP-адреса Ideco NGFW).

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

Подсказка: Видеоинструкцию смотрите по ссылкам:

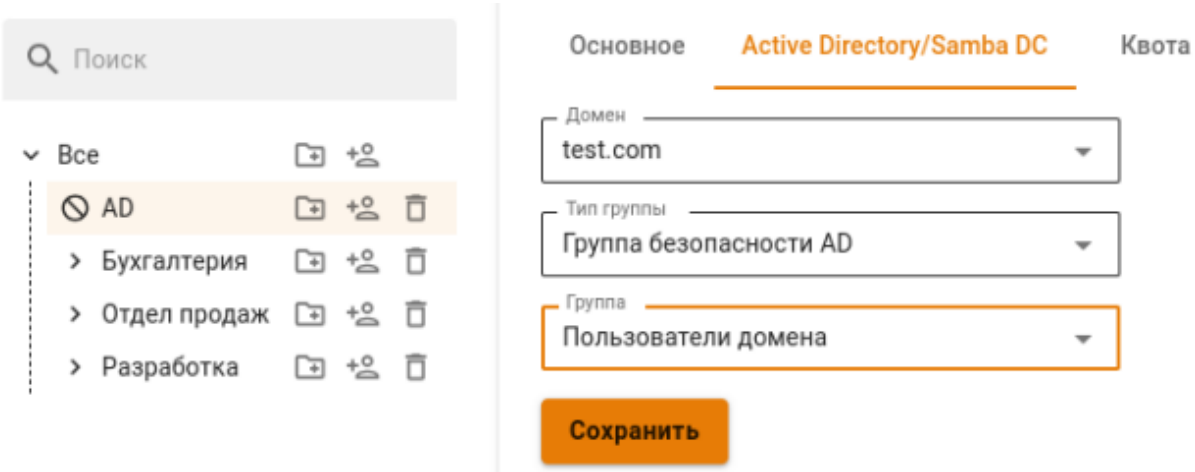
- Rutube;
- Youtube.

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

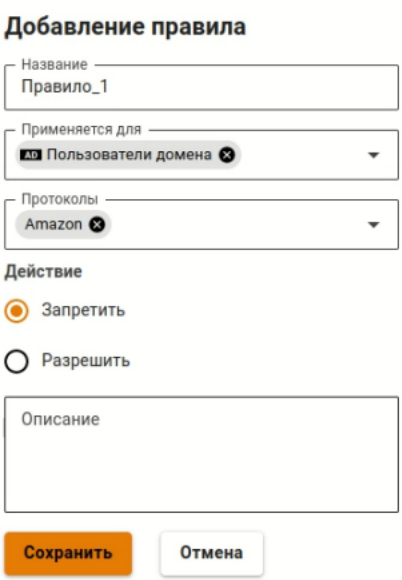
- *Файрвол*;
- *Контроль приложений*;
- *Ограничение скорости*;
- *Контент-фильтр*.

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**.

14.7.4 Ввод сервера в домен

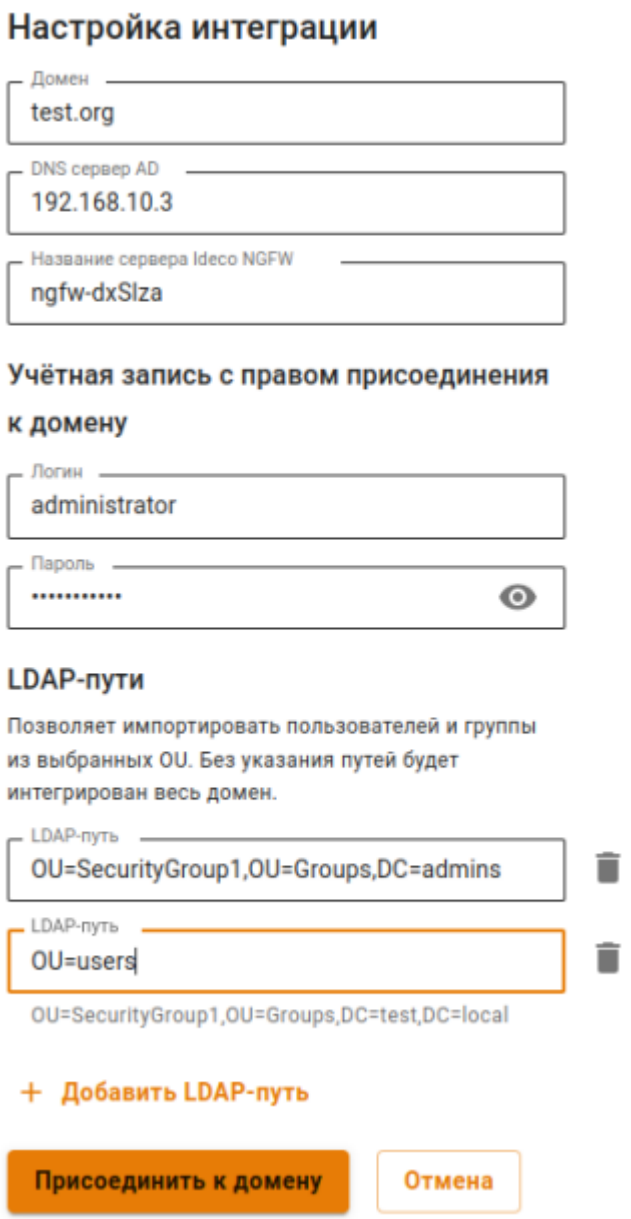
Подсказка: Перед вводом в домен убедитесь, что время на контроллере домена и Ideco NGFW совпадает.

Для ввода сервера в домен выполните действия:

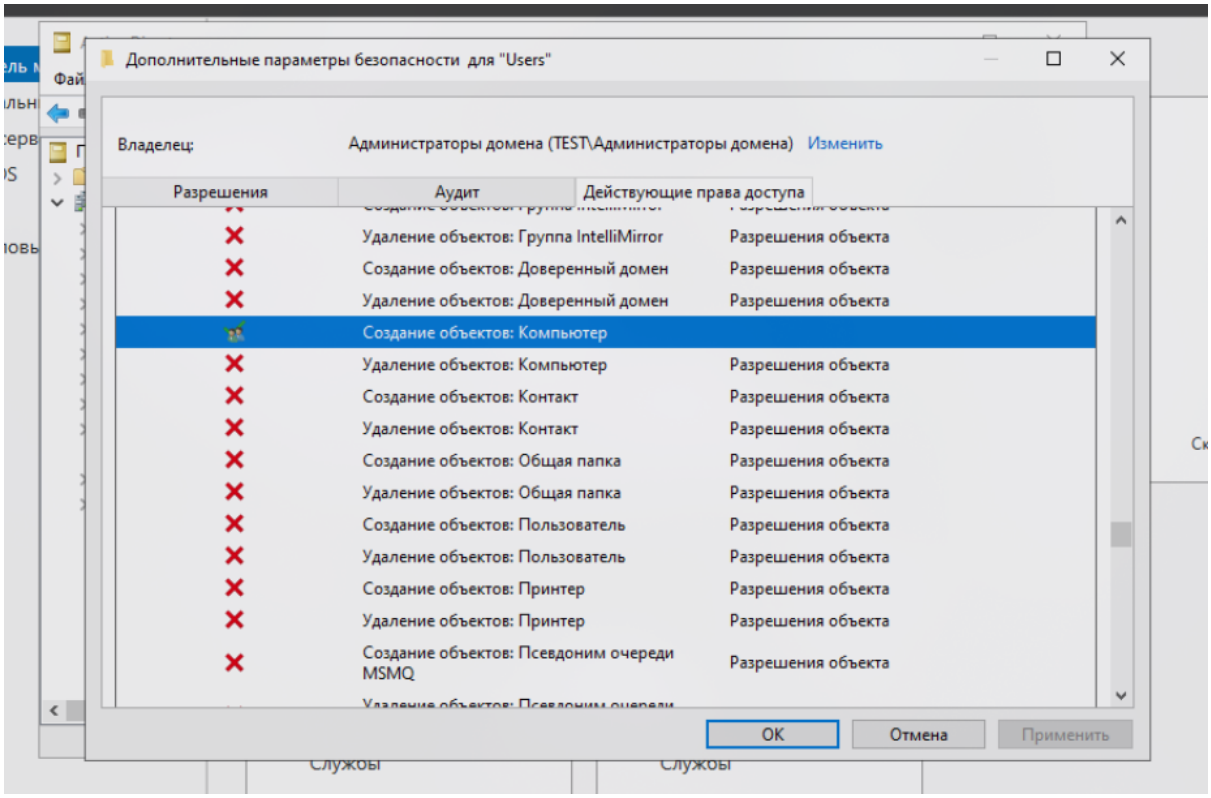
1. Перейдите на вкладку **Пользователи -> Active Directory/Samba DC**.

2. Нажмите кнопку **Добавить**.

3. Заполните следующие поля:



- **Домен**: введите полное наименование домена, длина которого не должна превышать 64 символа. Например: `mydomain.example`;
- **DNS-сервер AD**: введите адрес сервера, обладающий ролью DNS-сервера в контроллере домена, доступный с локального интерфейса Ideco NGFW;
- **Название сервера Ideco NGFW**: введите имя компьютера, под которым Ideco NGFW будет введен в контроллер домена;
- **Учетная запись с правом присоединения к домену**: введите учетную запись AD с правами присоединения к домену (право **Создание объектов: Компьютер**):



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

- **LDAP-пути**: укажите LDAP-пути для импорта пользователей и групп из выбранной организационной единицы (OU). Указание LDAP-путей позволяет импортировать только нужные группы и OU AD, чтобы избежать импорта всего дерева AD.

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

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

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*.

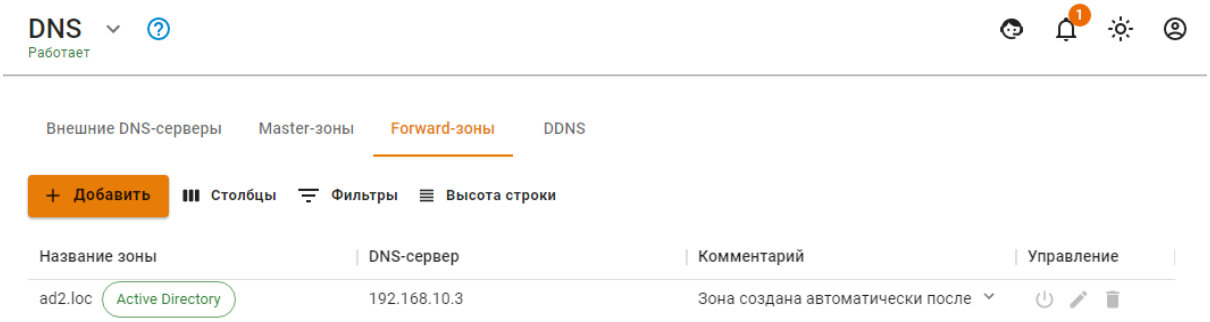
Подсказка: При выходе из домена удаляются все пользователи и группы, импортированные из него.

Настройка DNS для разрешения имен локального домена

Для корректной работы синхронизации и авторизации пользователей на Ideco NGFW настройте разрешение имен локального домена в настройках **Сервисы -> DNS**:

1. Пропишите *Forward-зону*;
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. 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.

14.7.5 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.

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

Настройка авторизации пользователей

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

Подсказка: Авторизацию через журнал безопасности Active Directory рекомендуется использовать совместно с SSO-авторизацией.

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

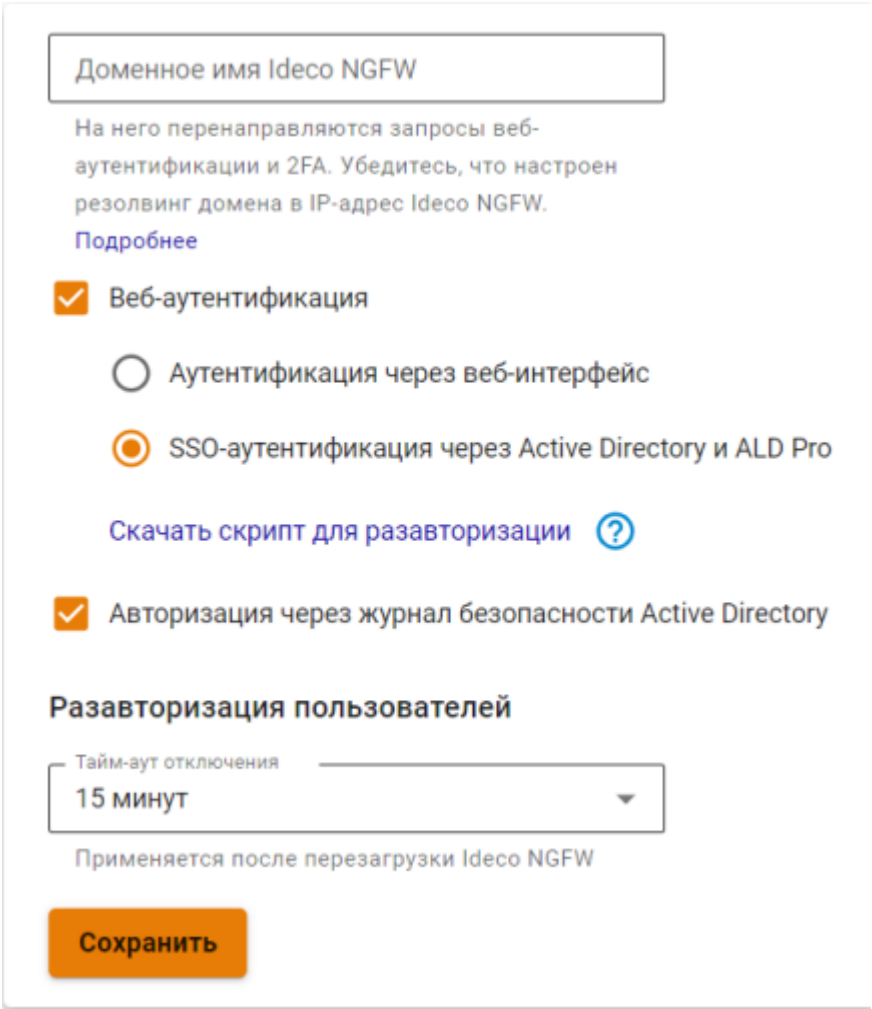
Подсказка: Если у домена, в который введен **NGFW**, настроено доверие с другим доменом, то пользователи доверенного домена смогут авторизоваться на **NGFW** при выполнении условий:

- 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

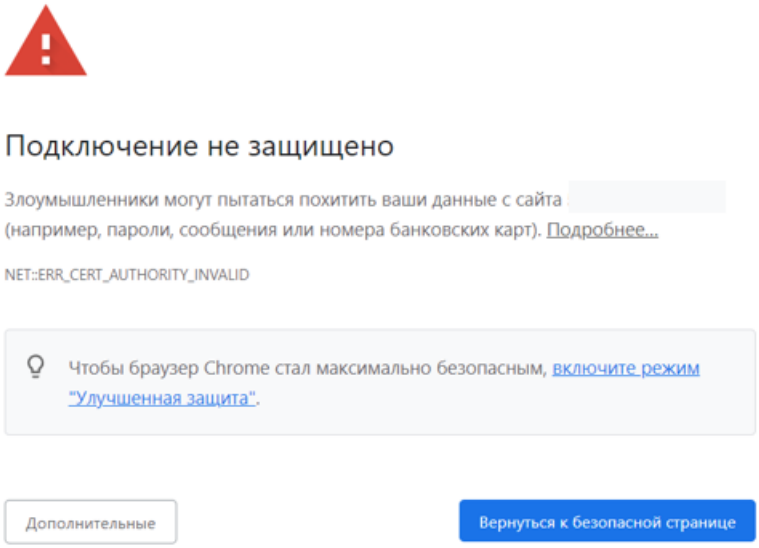
Для включения **SSO-аутентификации** и **Авторизации через журнал безопасности Active Directory** перейдите на вкладку **Пользователи -> Авторизация -> Основное** и заполните поля:



- 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.

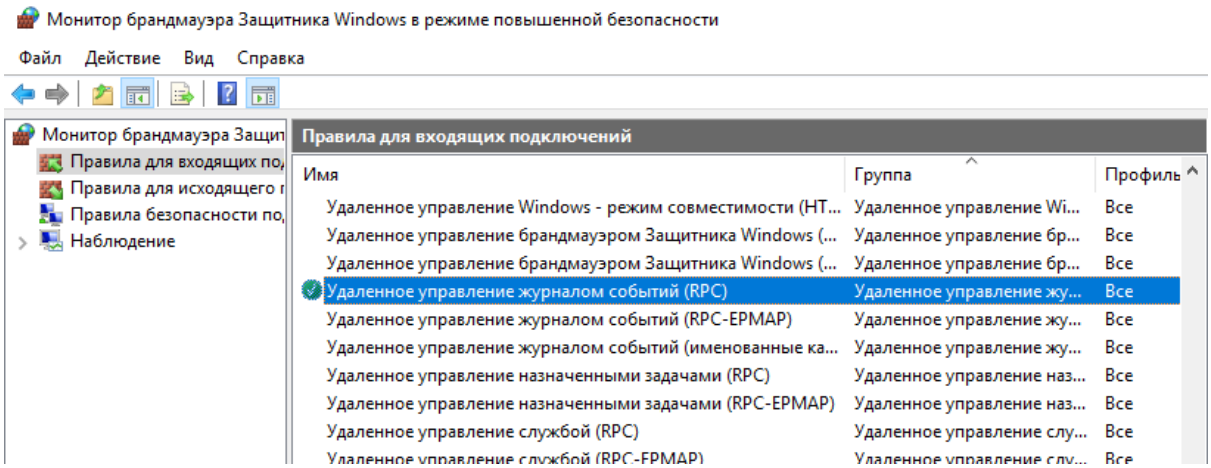
Подсказка: Особенности работы авторизации через журнал безопасности Active Directory:

- 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.

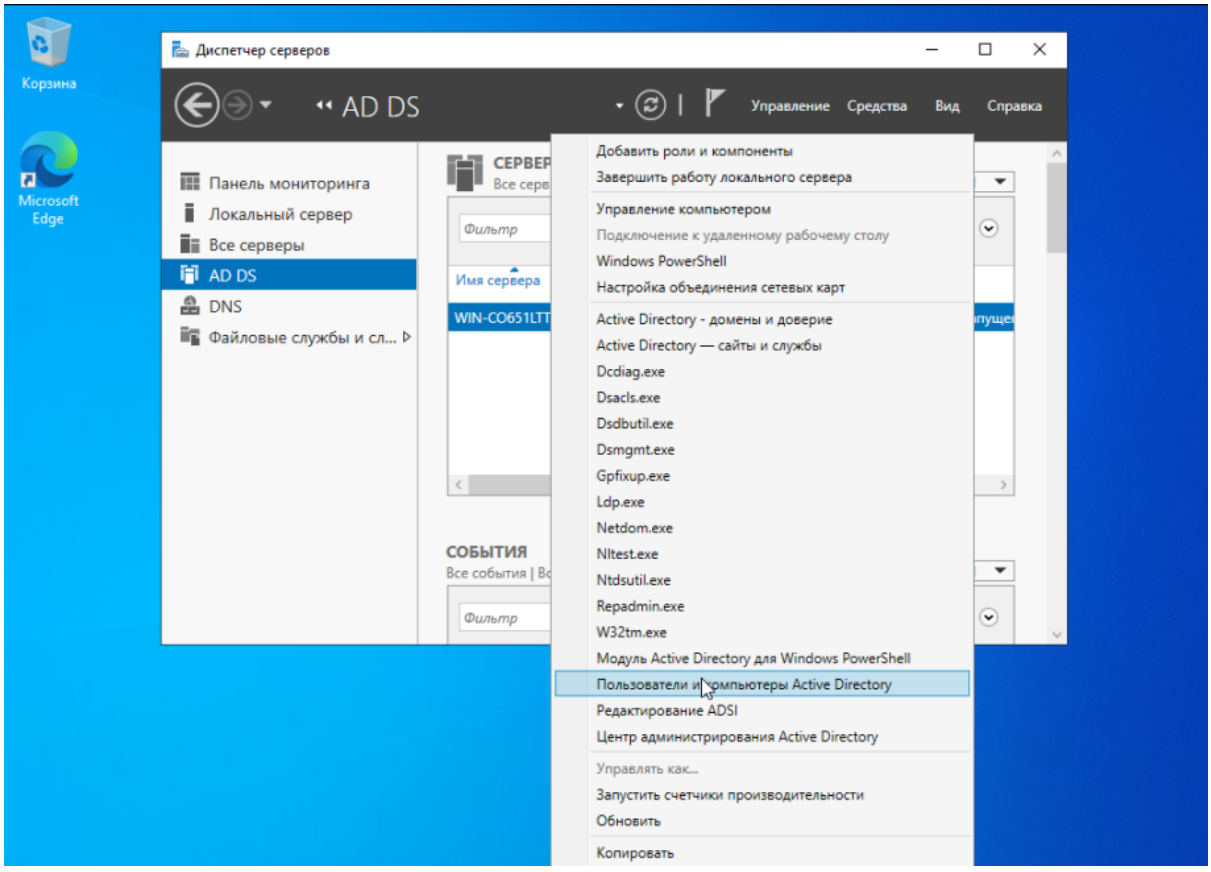
Для работы авторизации через журнал безопасности выполните настройку контроллера домена:

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

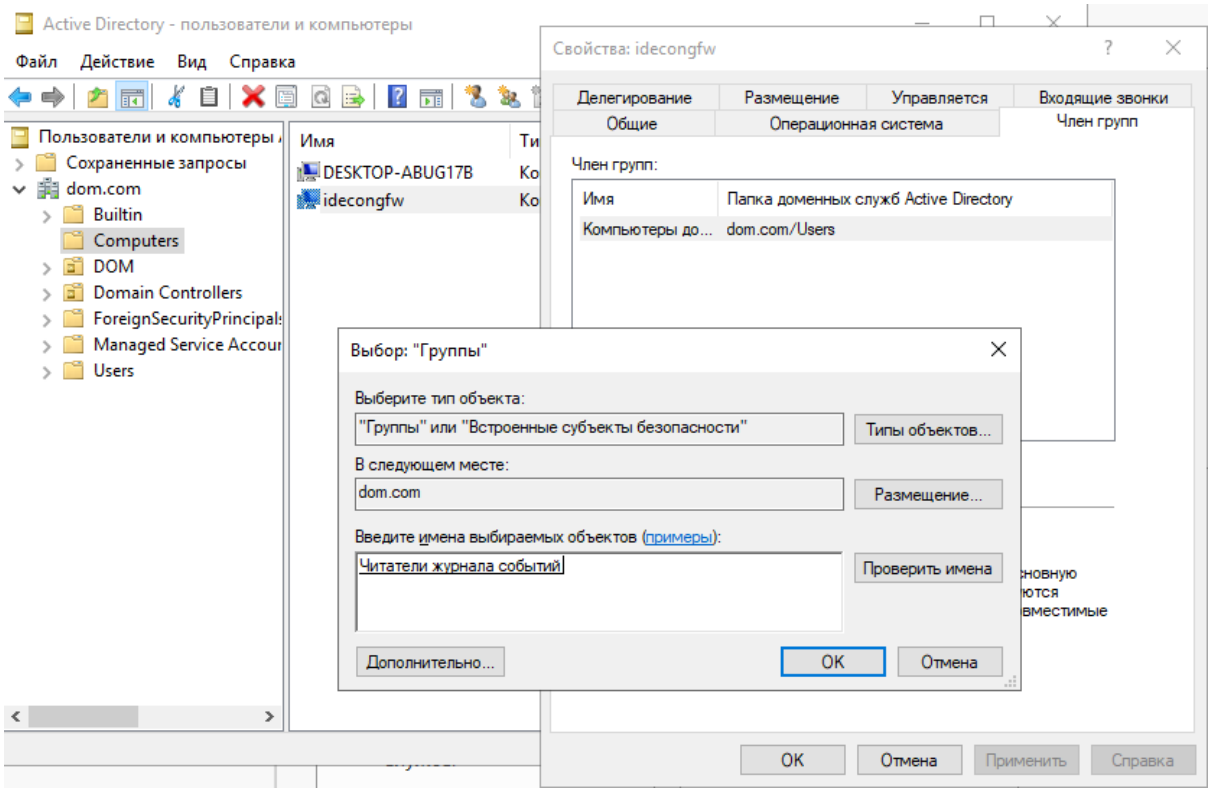


2. Добавьте Ideco NGFW в группу безопасности **Читатели журнала событий (Event Log Readers)**.

Для этого зайдите в **Диспетчер серверов**, выберите **AD DS**, 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.

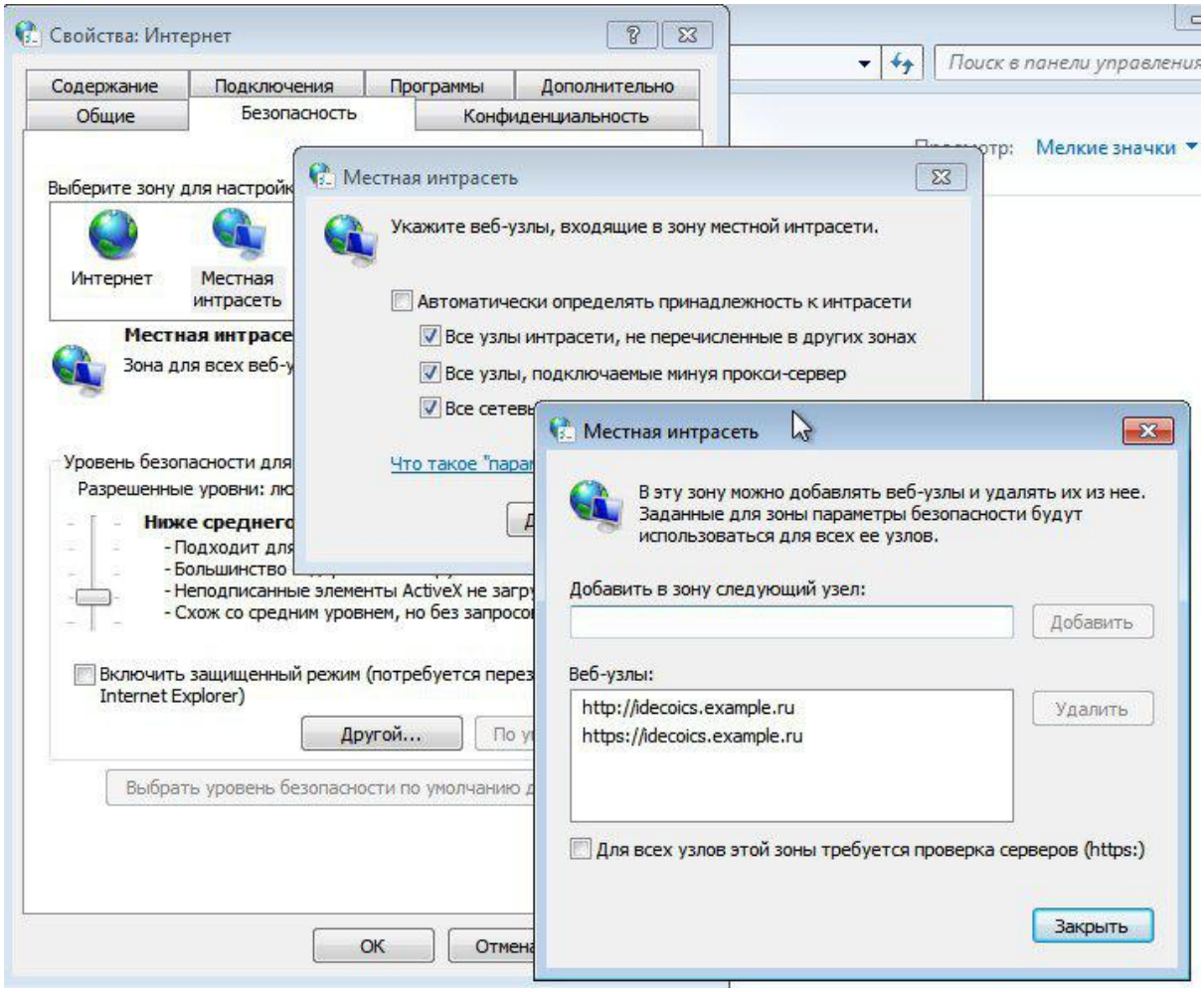
Для настройки аутентификации через веб-браузер выполните следующие действия:

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:

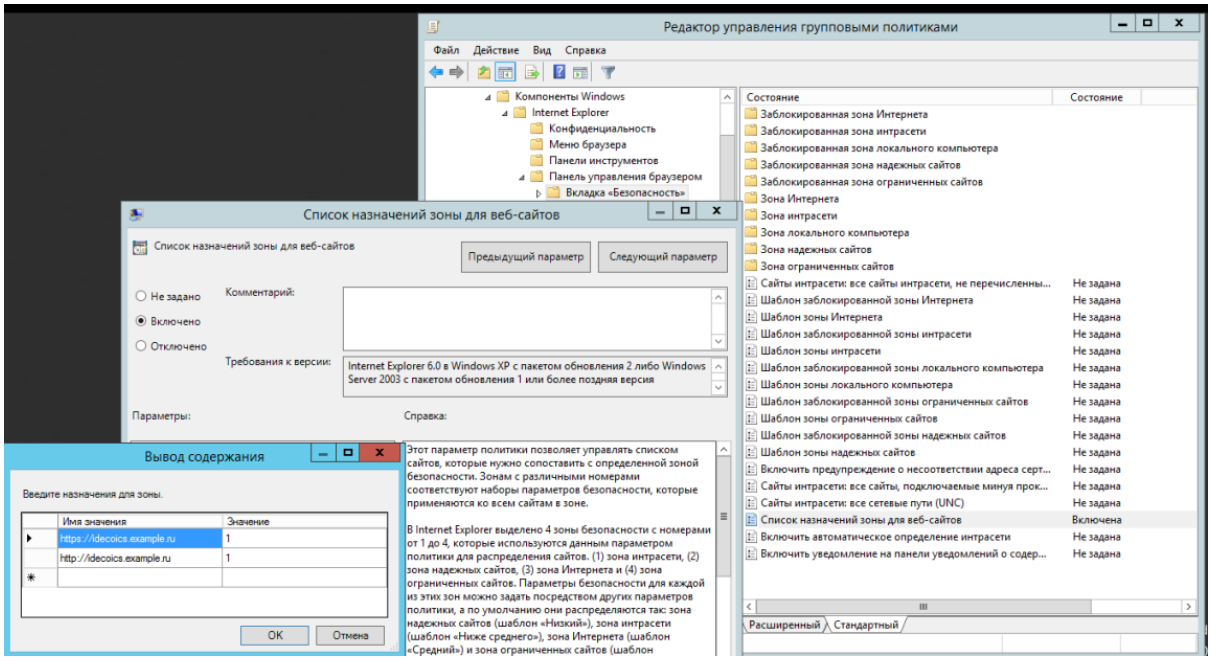
Англоязычная версия:

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.

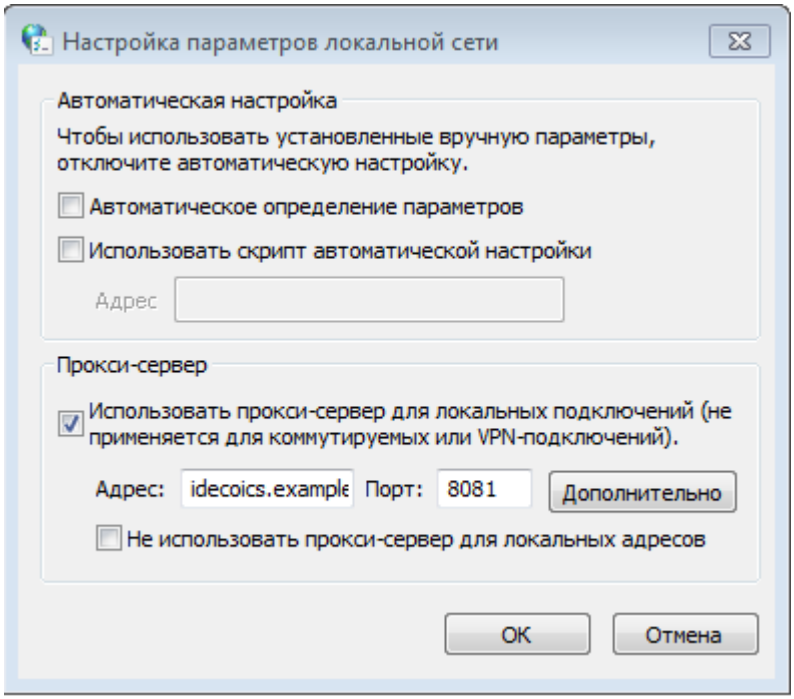
Способы аутентификации импортированных пользователей:

- **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:

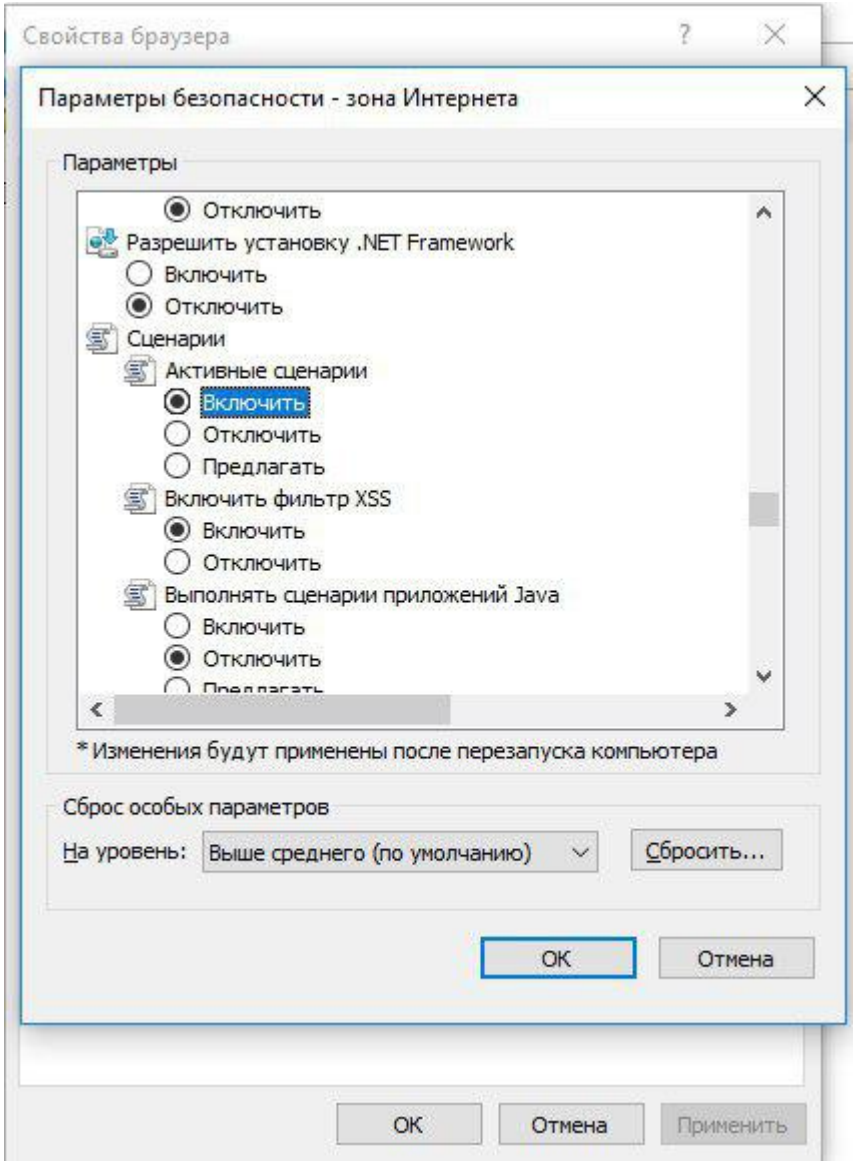
Для аутентификации компьютеров, которые **не находятся в домене**, под доменным пользовательским аккаунтом на странице настроек браузера **Mozilla Firefox** (about:config в адресной строке) укажите следующие параметры:

- **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.

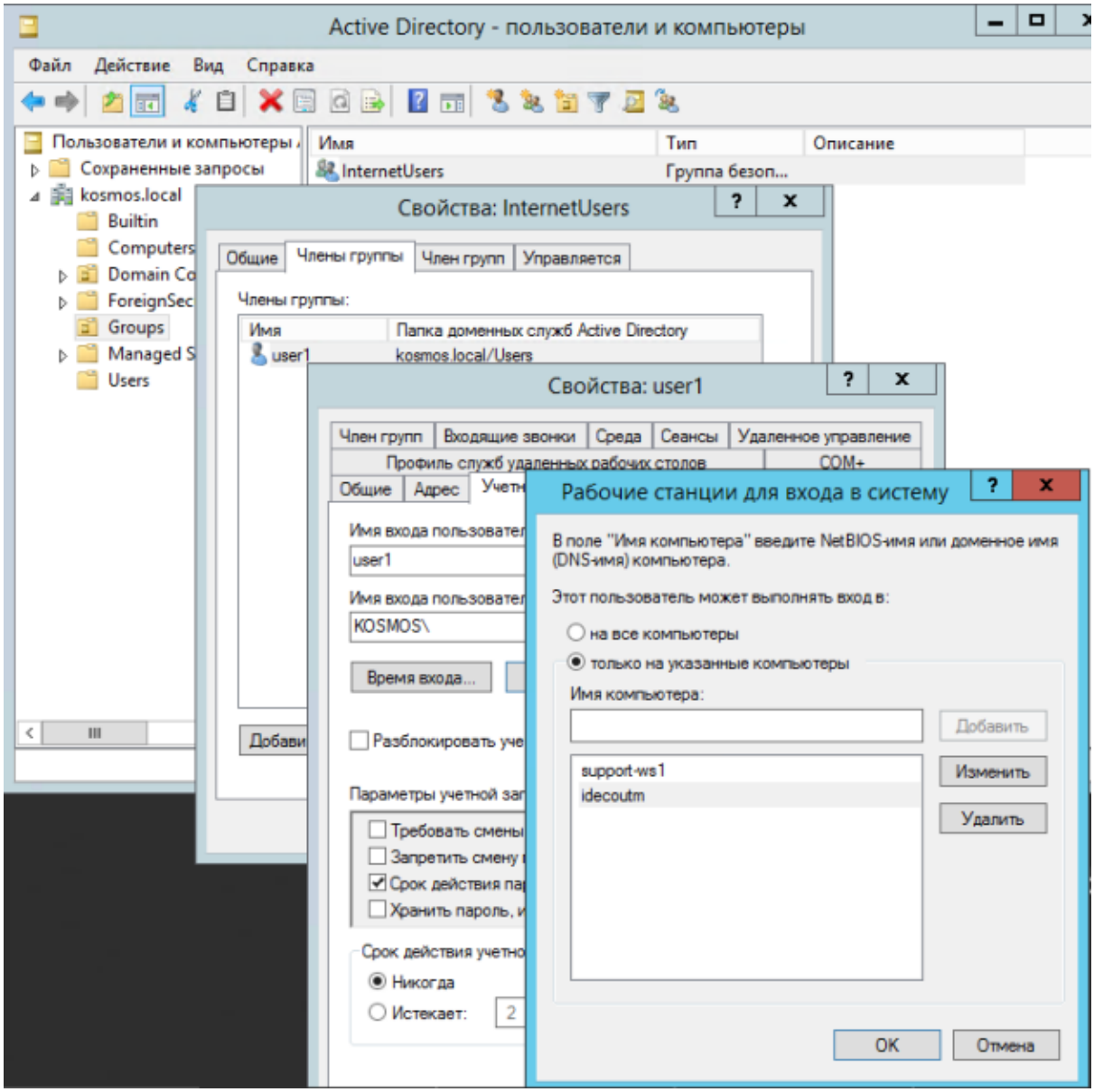
Возможные проблемы:

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:



14.7.6 Скрипты автоматической разавторизации

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

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

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

Для авторизации по SSO используйте *Ideco Client*.

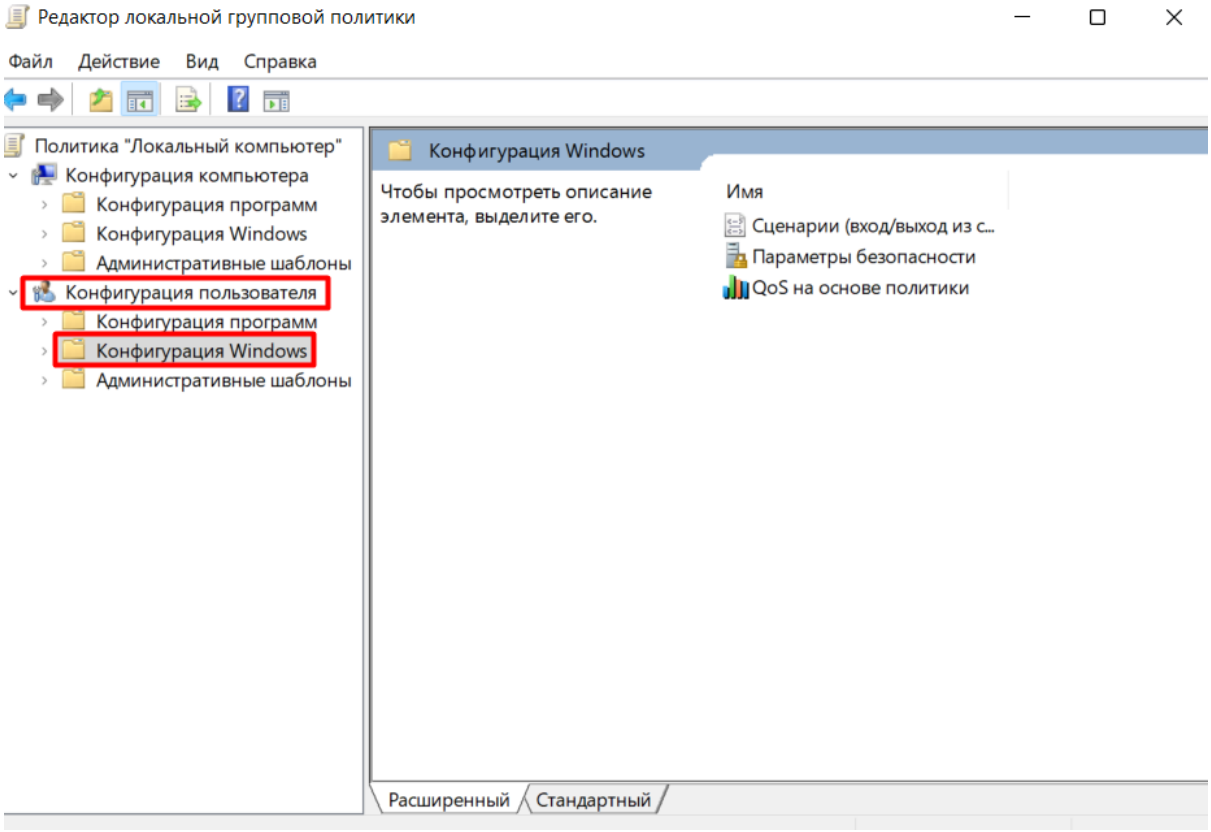
Разавторизация пользователя

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

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

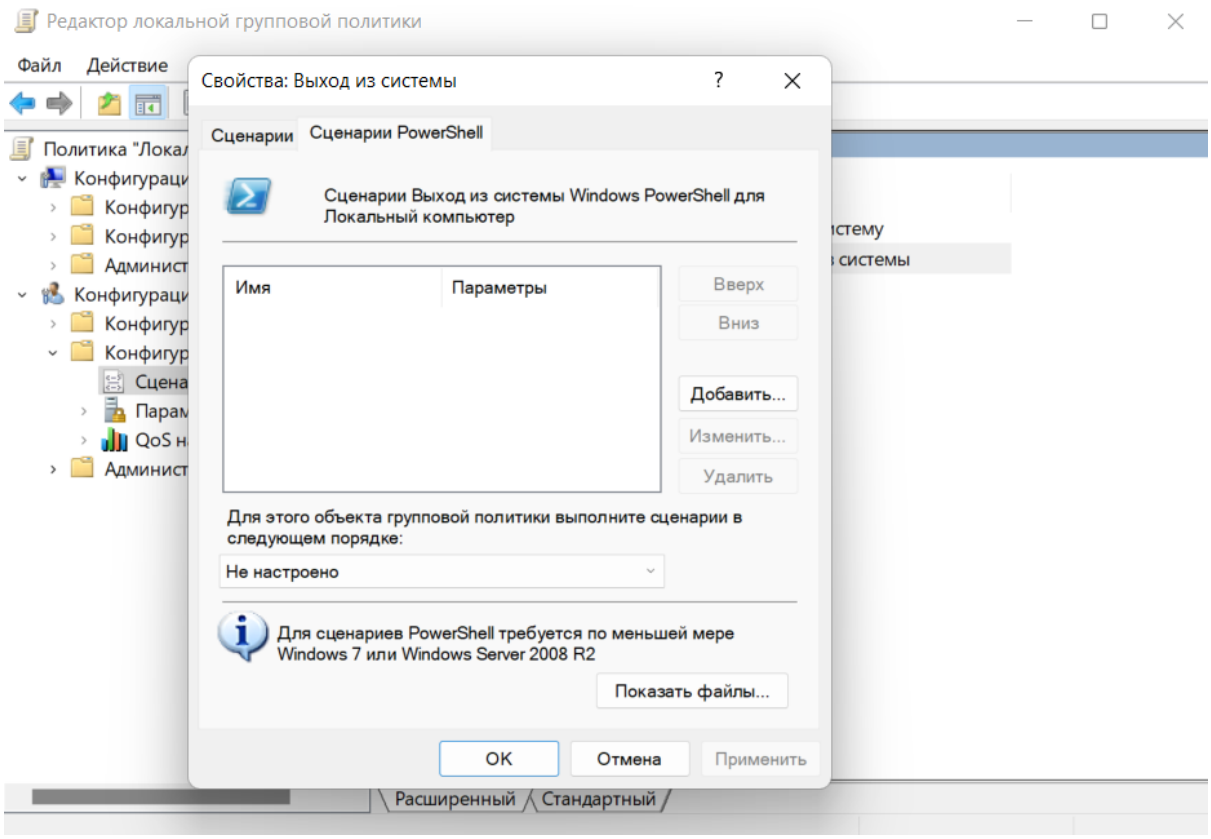
2. Откройте групповые политики (gpedit.msc) от имени администратора на устройстве пользователя.

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

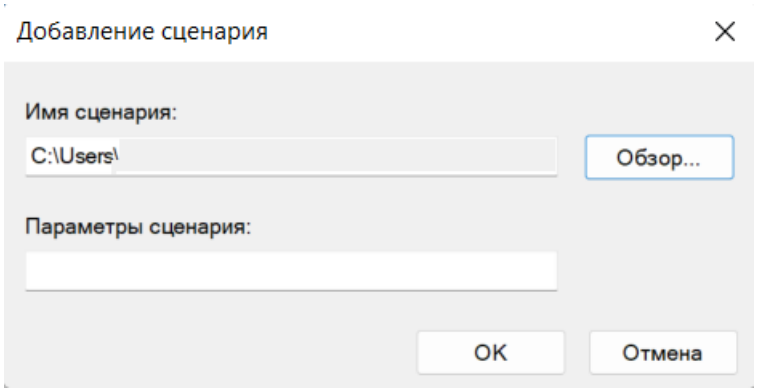


4. Нажмите **Сценарии (вход/выход из системы)**.

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**:

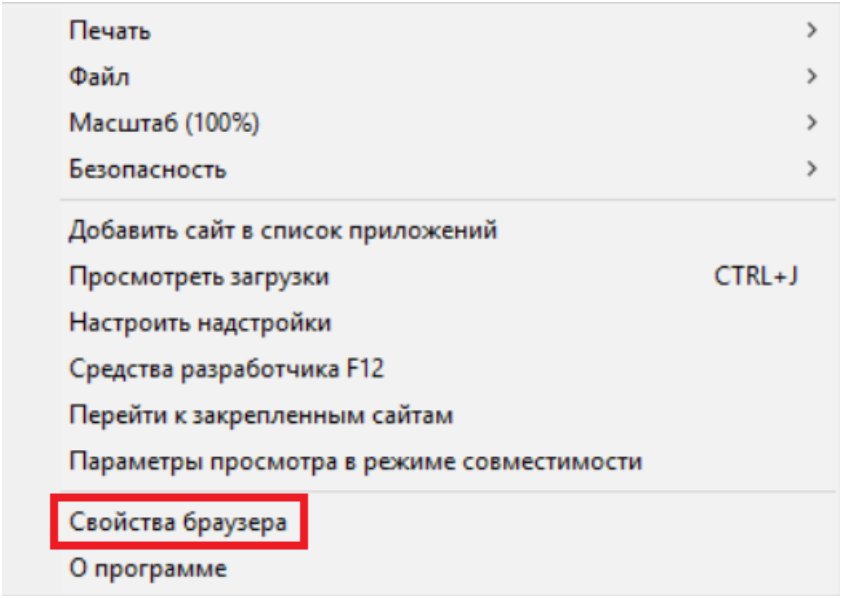


7. Откройте командную строку и обновите групповые политики, введя команду `gpupdate /force`.

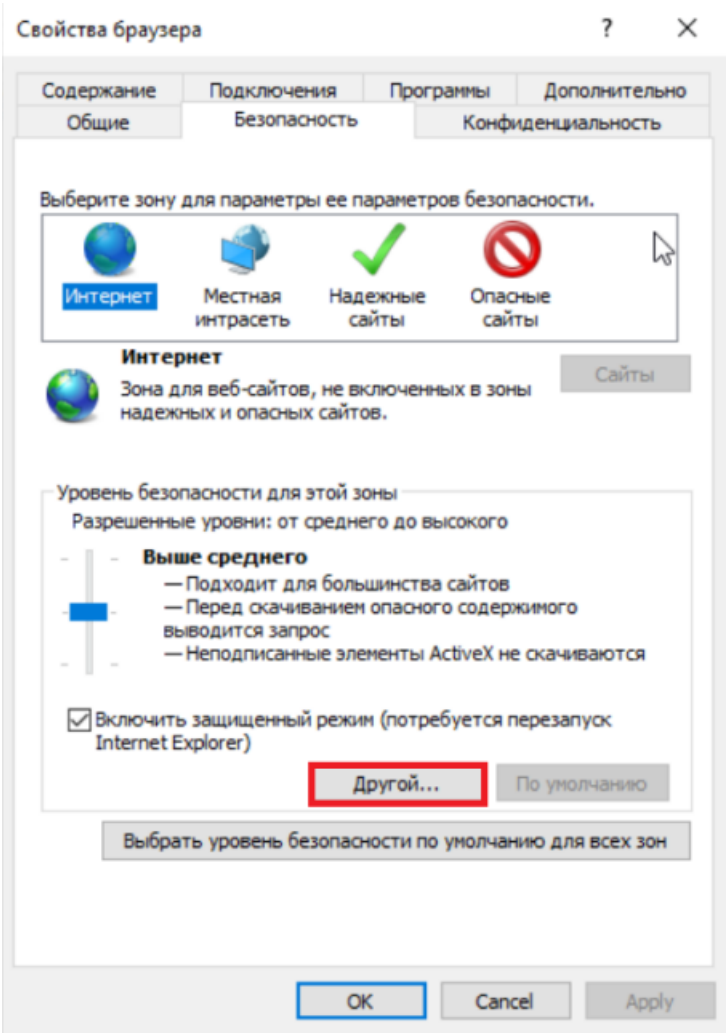
Если в вашем браузере появляется окно с текстом **Для получения доступа требуется аутентификация** и авторизация происходит только при ручном переходе по ссылке, включите JavaScript. Ниже представлены настройки для разных браузеров:

Internet Explorer:

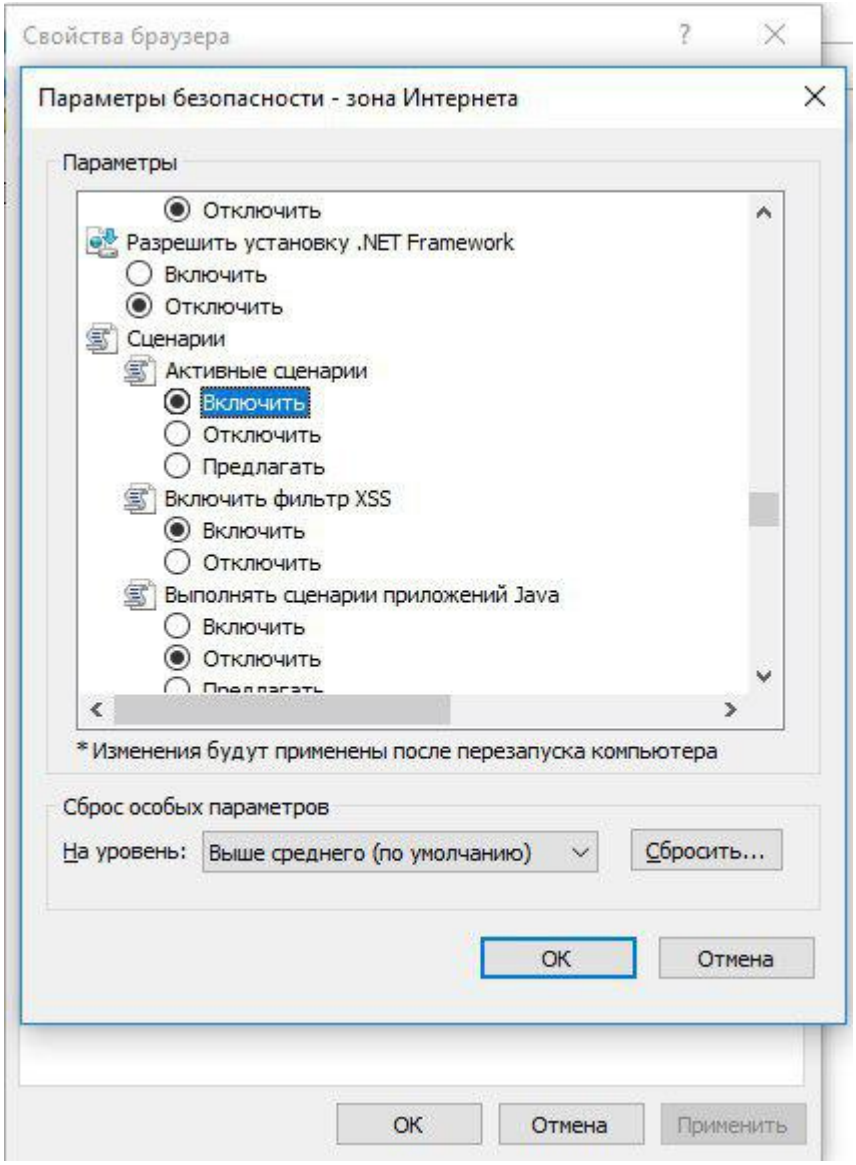
1. В правом верхнем углу браузера нажмите на кнопку **Сервис** в виде шестерни или комбинацию клавиш Alt+X. В выпадающем меню выберите **Свойства браузера**:



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

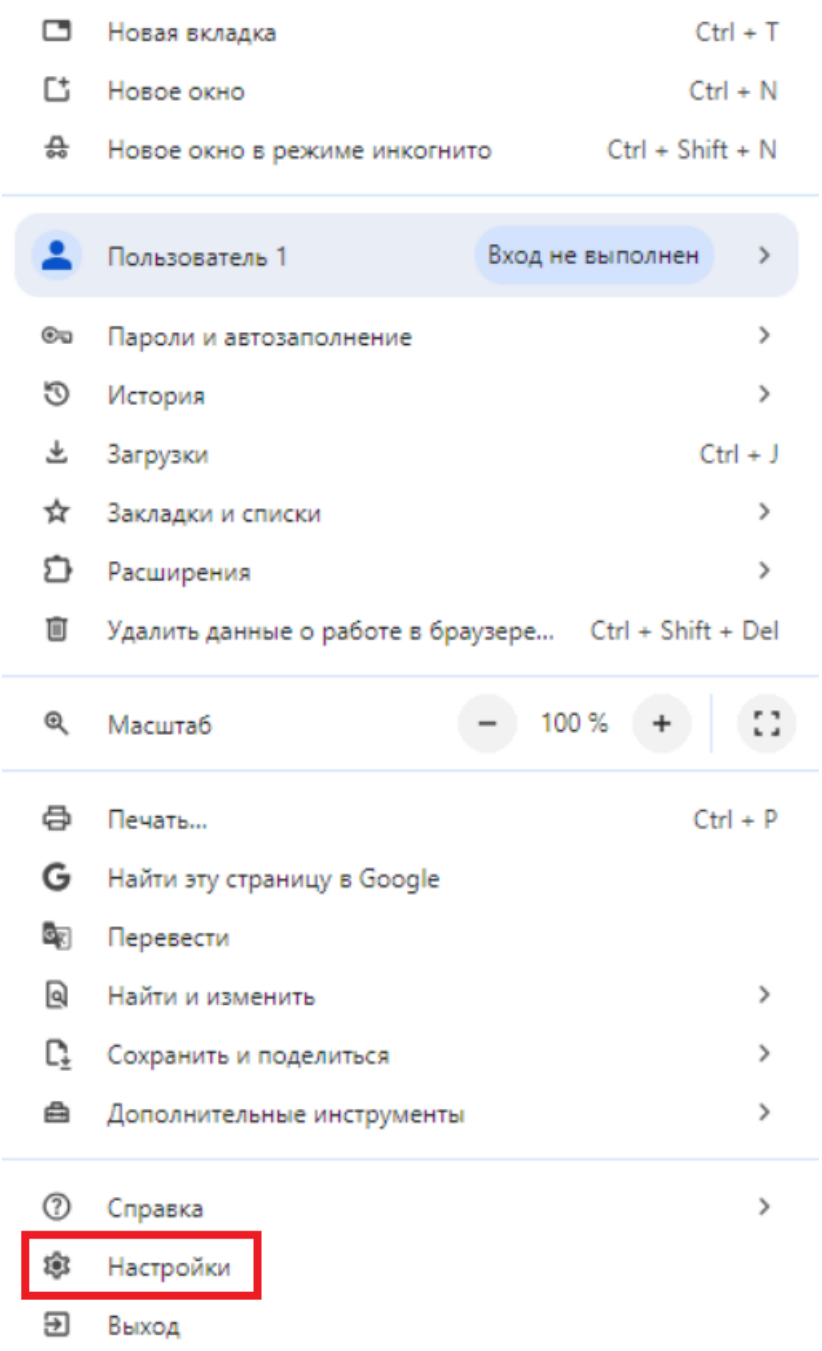


3. В окне **Параметры** переключите параметр **Активные сценарии** в значение **Включить**:

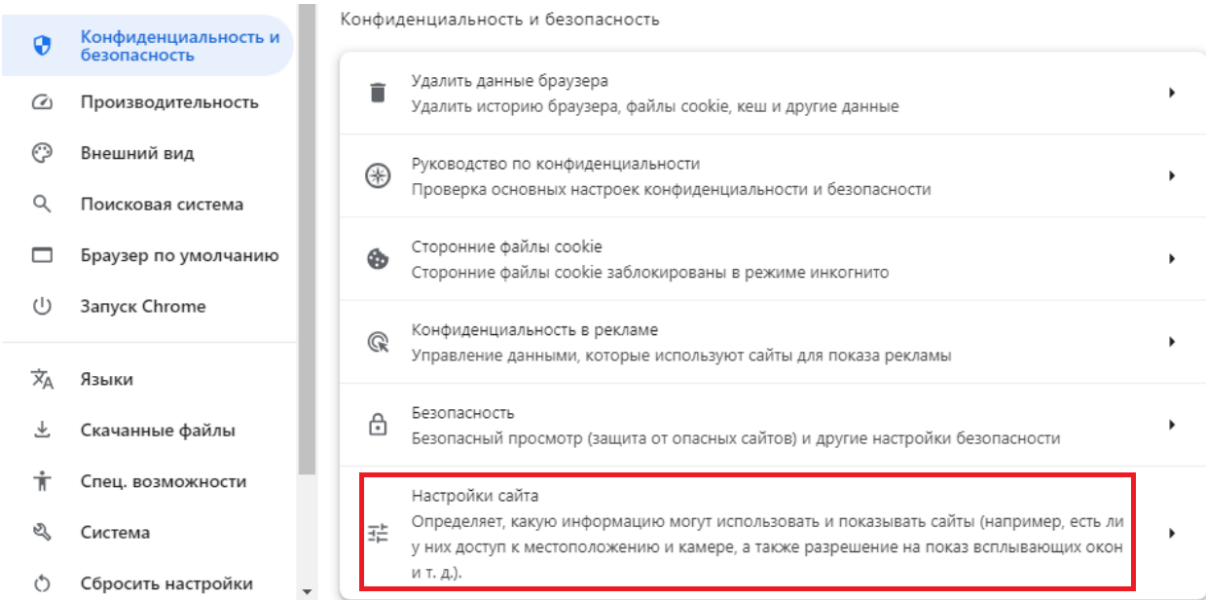


Google Chrome:

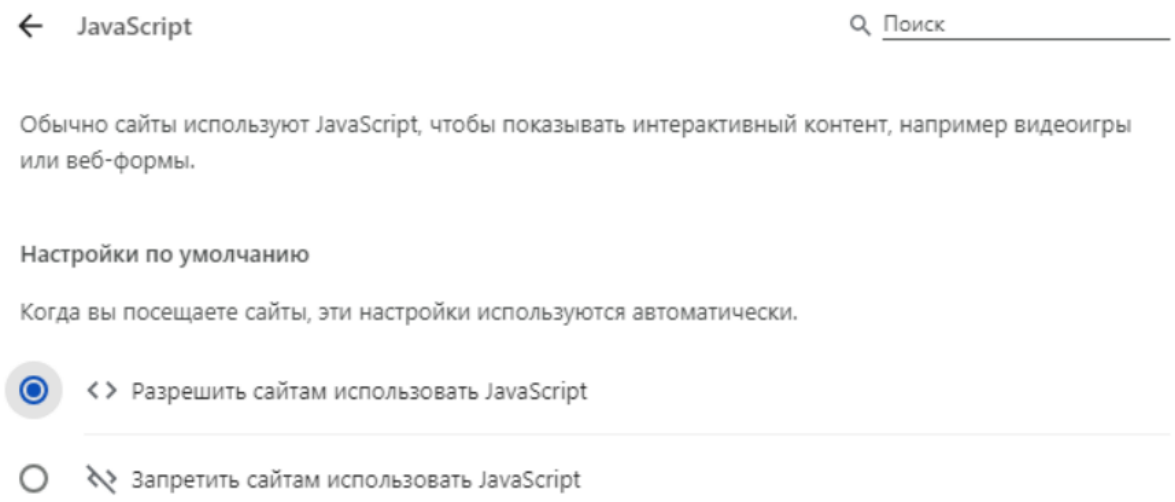
1. В правом верхнем углу браузера нажмите на кнопку с тремя точками и выберите **Настройки** в выпадающем меню:



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

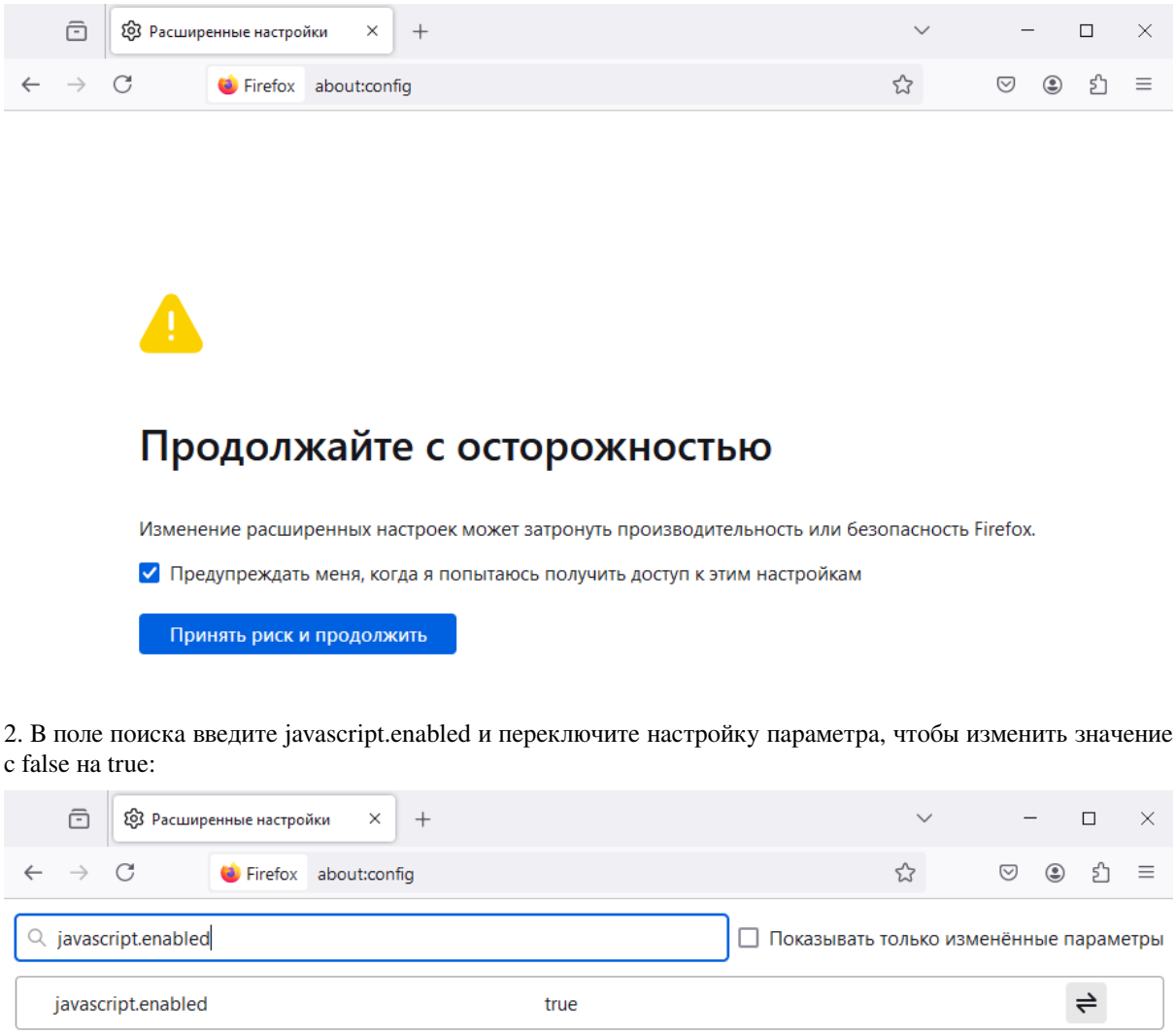


3. В настройках **JavaScript** разрешите сайтам использовать JavaScript:



Firefox:

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



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

3. Обновите страницу в браузере.

14.7.7 Импорт пользователей

Особенности импорта пользователей в Ideco NGFW

Предупреждение: При импорте пользователей убедитесь, что учетные записи AD не имеют одинаковых логинов с локальными учетными записями. В противном случае система выдаст сообщение об ошибке.

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

Предупреждение: При импорте пользователей убедитесь, что учетные записи AD не имеют одинаковых логинов с локальными учетными записями. В противном случае система выдаст сообщение об ошибке.

Внимание: Если локальные пользователи Ideco NGFW находятся в группах AD, приостанавливается синхронизация с контроллером домена.

Импорт учетных записей из LDAP

В Ideco NGFW возможен импорт 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***.

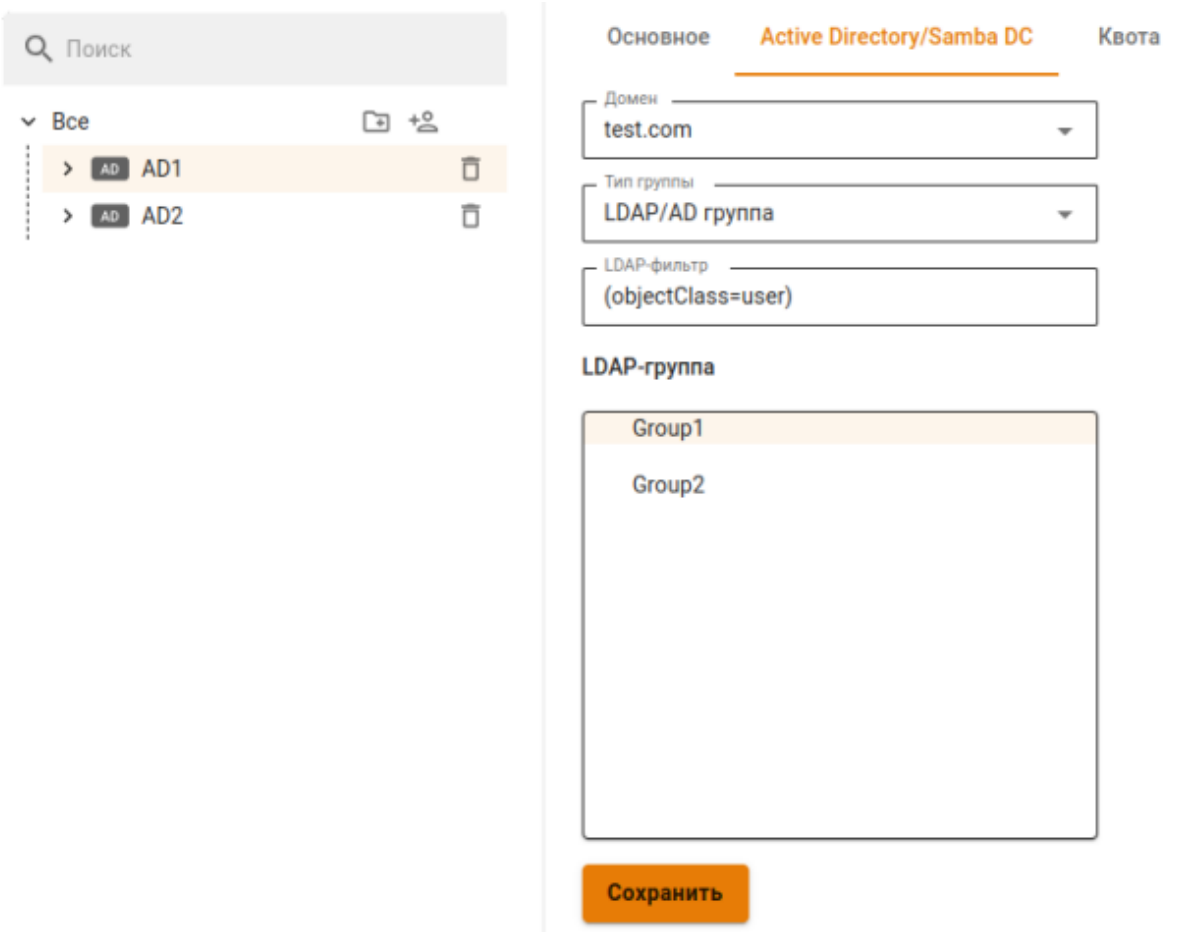
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC** в правой части экрана.

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

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



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 ту группу, которая была импортирована последней.

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

1. Создайте группу в дереве пользователей Ideco NGFW.

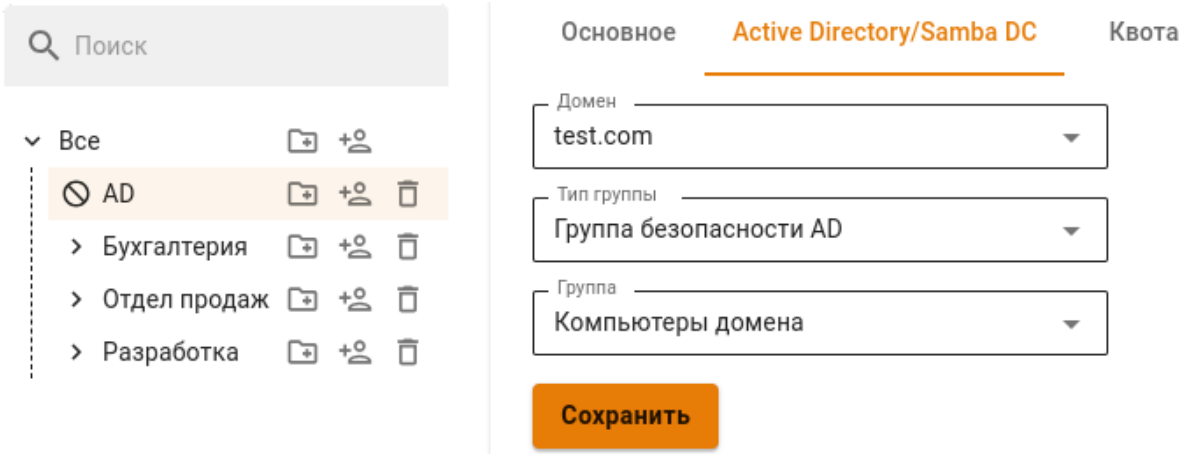
2. Выберите эту группу в дереве и перейдите на вкладку **Active Directory/Samba DC**.

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**.



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.

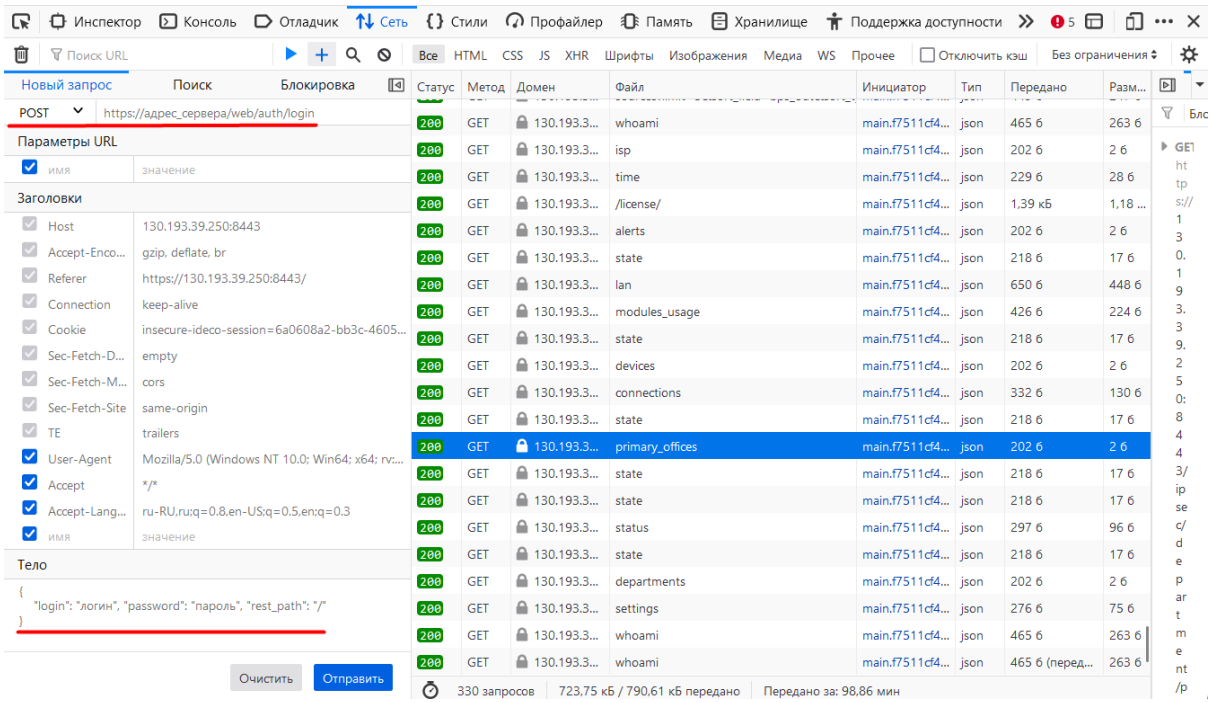
3. В появившемся окне перейдите на вкладку **Новый запрос**.

4. Отправьте запрос авторизации:

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

Тело запроса:

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

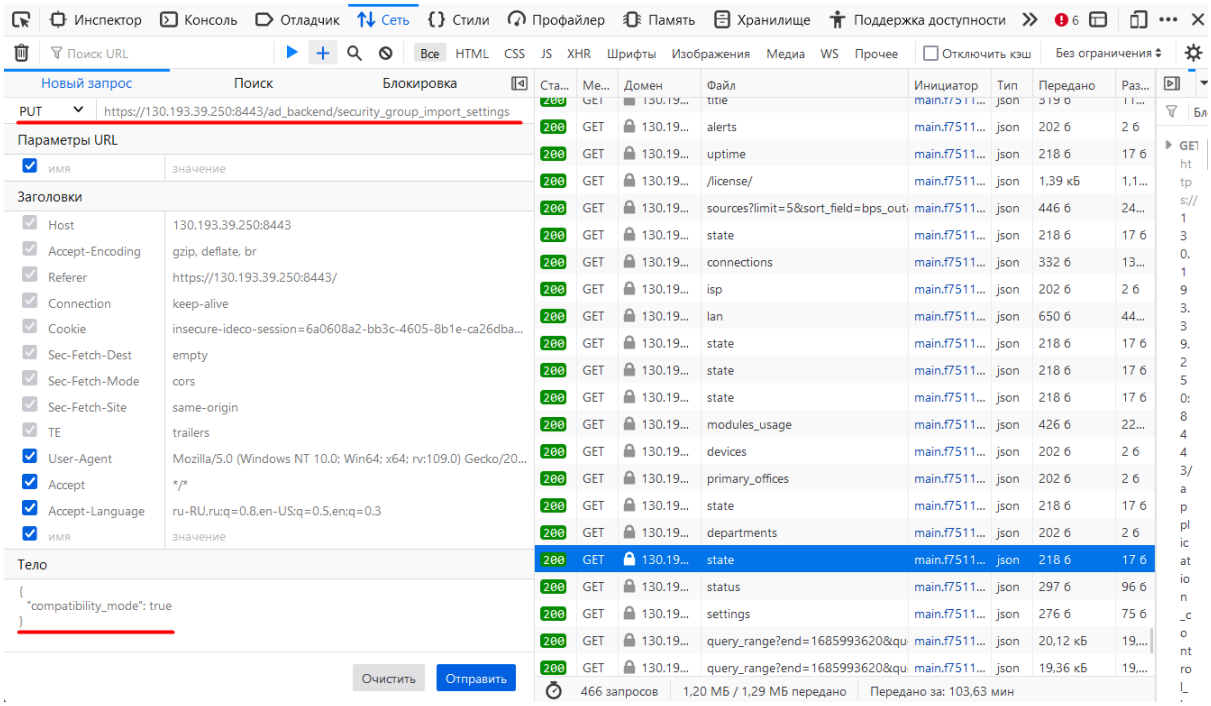


5. Отправьте запрос на включение режима:

```
PUT /ad_backend/security_group_import_settings
```

Тело запроса:

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



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

14.8 Интеграция с RADIUS-сервером

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

14.8.1 Настройка интеграции

Подсказка: Доступна аутентификация только VPN-пользователей NGFW через RADIUS-сервер.

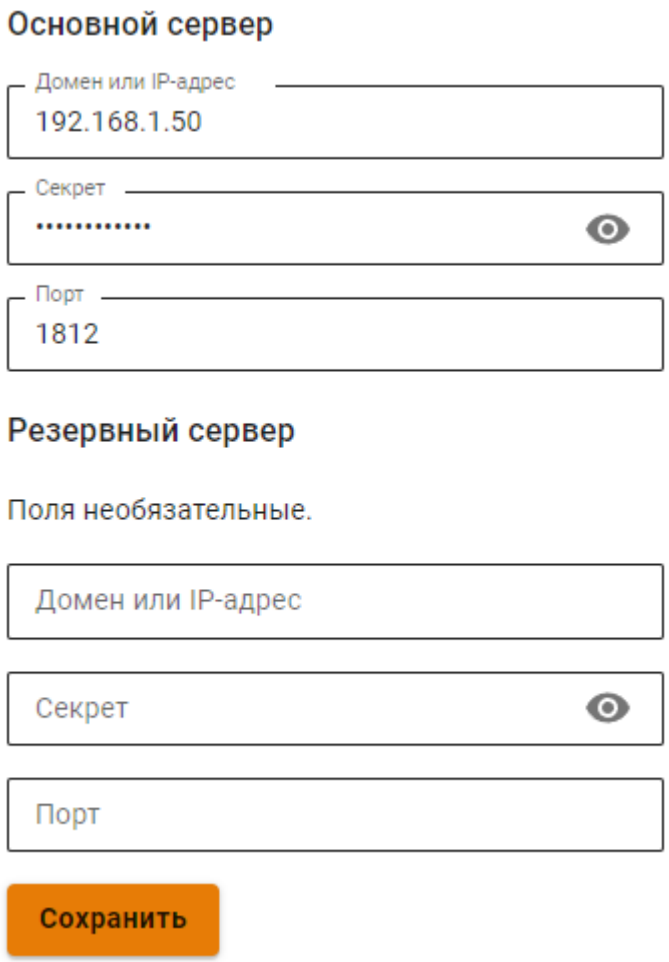
Аутентификация на RADIUS-сервере доступна только по протоколу MS-CHAPv2 с генерацией MPPE-ключей.

Для взаимодействия с основным RADIUS-сервером по умолчанию используется порт 1812.

Для настройки интеграции с RADIUS-сервером выполните действия:

1. Перейдите в раздел **Пользователи -> RADIUS** и включите опцию **RADIUS**.

2. Укажите доменное имя или IP-адрес внутреннего RADIUS-сервера и секрет (пароль доступа). Если требуется, поменяйте порт, по которому будет происходить подключение к серверу:



3. Нажмите **Сохранить**.

Подсказка: При наличии в сети двух RADIUS-серверов настройте один как резервный с указанием порта подключения.

При отсутствии ответа от основного RADIUS-сервера запрос об аутентификации будет перенаправлен на резервный RADIUS-сервер.

14.8.2 Механизм добавления пользователей в дерево Ideco NFGW

1. При подключении пользователя к Ideco NGFW происходит поиск пользователя в дереве пользователей:
   - Если пользователь найден - запрос аутентификации сразу будет отправлен на **RADIUS-сервер**.
   - Если пользователь не найден - Ideco NGFW создаст пользователя и отправит запрос аутентификации на **RADIUS-сервер**.

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

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

Предупреждение: Ограничения для группы и пользователей RADIUS:

- Запрещено менять параметры пользователя (в том числе поля **Имя** и **Комментарий**), за исключением опции **Запретить доступ**;

- Разрешено удалять и переименовывать группу **RADIUS**;
- Запрещено удалять пользователей;
- Запрещено перемещать пользователей в другие группы;
- Запрещено перемещать других пользователей NGFW в группу **RADIUS**;
- Запрещена настройка IP и MAC авторизации для пользователей группы;
- Недоступна двухфакторная аутентификация для пользователей группы;
- Недоступна авторизация пользователей группы в личном кабинете и веб-почте.

14.9 ALD Pro

Подсказка: Название службы раздела **ALD Pro**: `ideco-ald-rest`, `ideco-ald-backend`.
Список служб для других разделов доступен по *ссылке*.

Ideco NGFW поддерживает версии ALD Pro от 1.4 и выше.

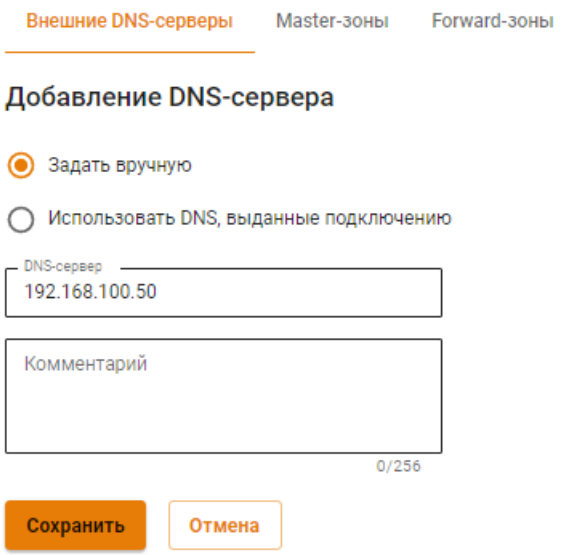
ALD Pro предназначен для централизованного управления ресурсами под управлением ОС Astra Linux и может использоваться в организациях различного масштаба.

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.

14.9.1 Ввод сервера в домен

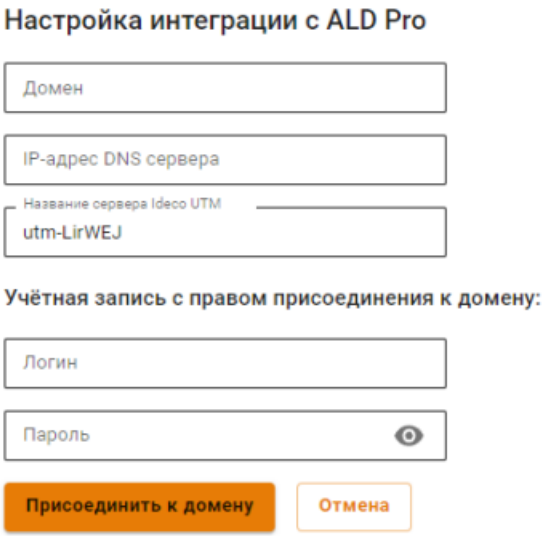
1. Перейдите в раздел **Сервисы -> DNS -> Внешние DNS-серверы** и добавьте IP-адрес DNS-сервера ALD:



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

2. Нажмите на кнопку **Добавить**.

3. Заполните следующие поля:



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

Подсказка: Инструкции по развертыванию и управлению ресурсами через ALD Pro доступны на официальном сайте.

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

14.9.2 Импорт пользователей

ALD Pro поддерживает импорт двух типов групп:

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

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

Для импорта пользователей выполните действия:

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

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

Импортированных пользователей можно использовать в качестве объектов для авторизации, настройки VPN-подключений, создания правил (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.

14.9.3 Аутентификация пользователей

При аутентификации пользователей проверка осуществляется средствами Kerberos.

ALD Pro поддерживает два типа входа в систему:

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

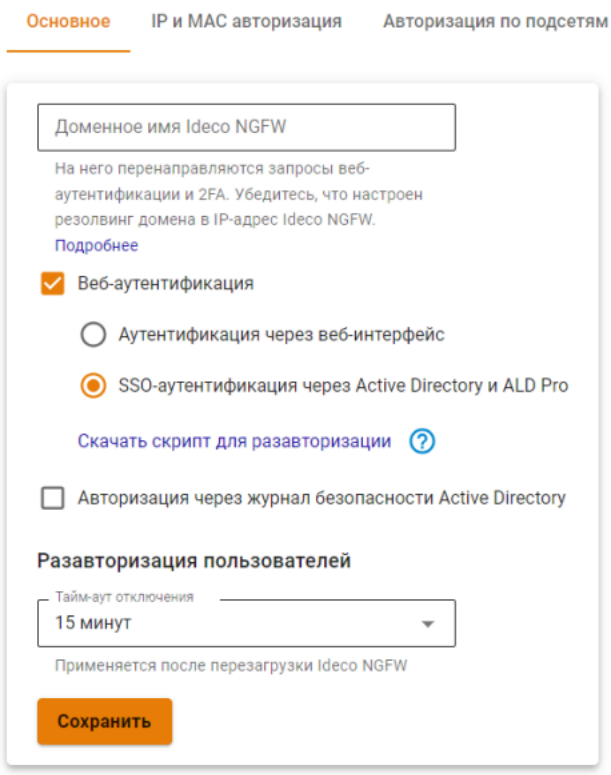
Настройка Ideco NGFW

Для настройки аутентификации выполните действия:

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

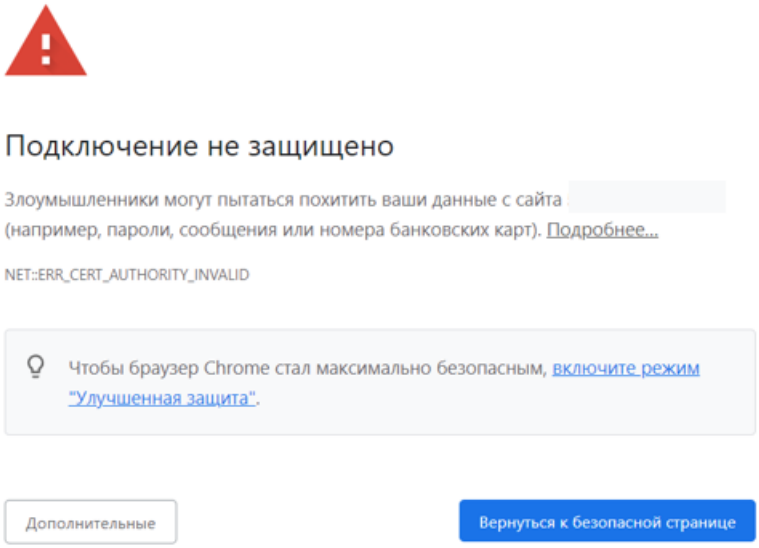
2. Активируйте опцию **Веб-аутентификация**.

3. Выберите тип входа в систему:



- Для входа по логину/паролю активируйте опцию **Аутентификация через веб-интерфейс**.
- Для входа через SSO активируйте опцию **SSO-аутентификация через Active Directory и ALD Pro**.

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



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

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

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 сертификатом 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-подключения*.

14.10 Обнаружение устройств

14.10.1 Основное

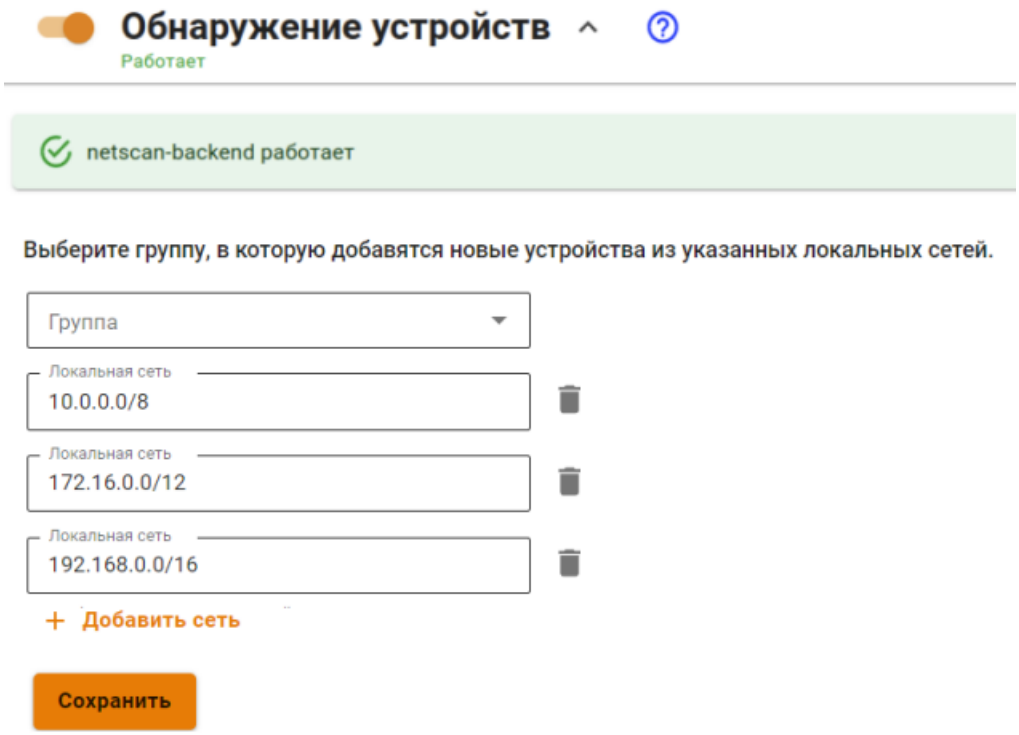
Подсказка: Название службы раздела **Обнаружение устройств**: `ideco-netscan-backend`.
Список служб для других разделов доступен по *ссылке*.

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 в поле Имя пользователя будет записан IP-адрес найденного устройства:



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

14.11 Wi-Fi-сети

В текущей версии Ideco NGFW не поддерживает Wi-Fi-адаптеры. Для работы беспроводных клиентов необходимо использовать беспроводные точки доступа или
Wi-Fi-маршрутизаторы.

Для выхода в интернет пользователей, подключающихся по Wi-Fi, необходима их авторизация на NGFW или авторизация Wi-Fi-роутера - это зависит от режима работы маршрутизатора.

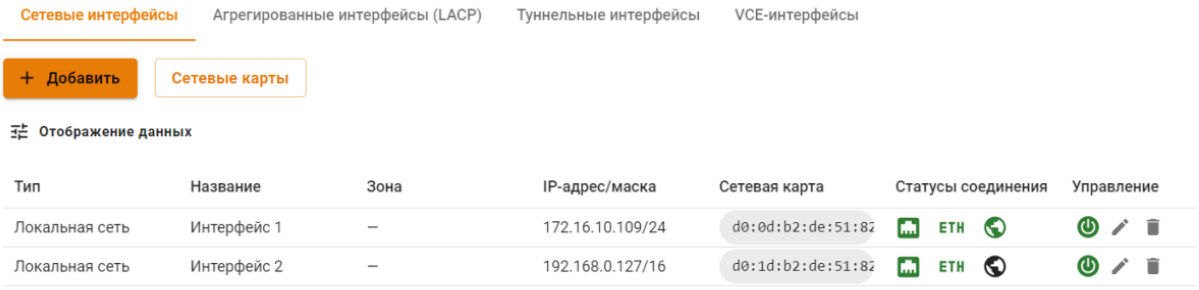
Режим точки доступа или bridge:

В режиме точки доступа или bridge устройство Wi-Fi 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.

14.11.1 Настройка DHCP:

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

2. Добавьте в сетевые интерфейсы шлюз созданной сети;

3. Перейдите в раздел 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.

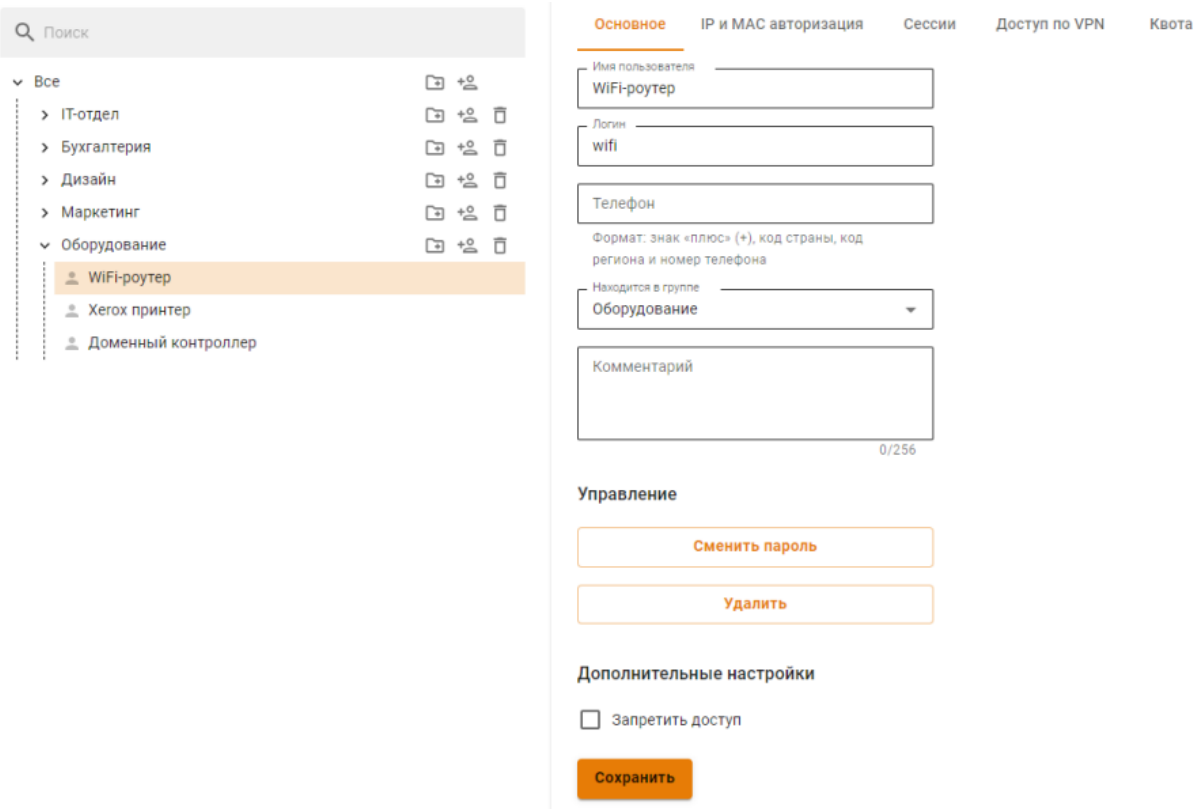
Режим роутера:

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.

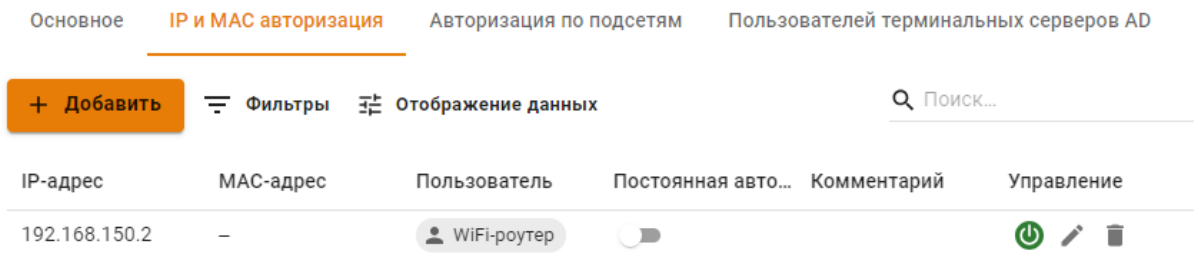
Пример настройки пользователя в режиме роутера представлен на скриншотах ниже:

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.

14.11.2 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.

15. Мониторинг

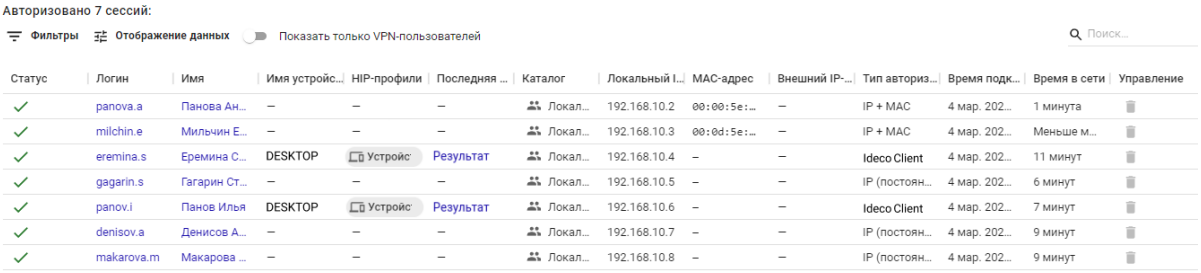
15.1 Авторизованные пользователи

15.1.1 Основное

В разделе **Мониторинг -> Авторизованные пользователи** отображен список всех сессий пользователей, которые авторизовались в NGFW.

Статус	Описание
	**Подключено**. Пользователь авторизован
	**Ожидает второй фактор авторизации**. Пользователь создал и активировал VPN-подключение, но не прошел двухфакторную аутентификацию (подробнее в *статье*)
	**Превышен лимит лицензии**. Данная сессия заблокирована. Появляется в случае, если превышено количество пользователей по лицензий или у пользователя уже есть активные 5 сессий
	**Сессия удаляется**. Появляется в случае, если была разорвана сессия с динамическим IP-адресом. Сессия с таким статусом будет удалена через 30 секунд

Пример пользователей, авторизованных разными способами:

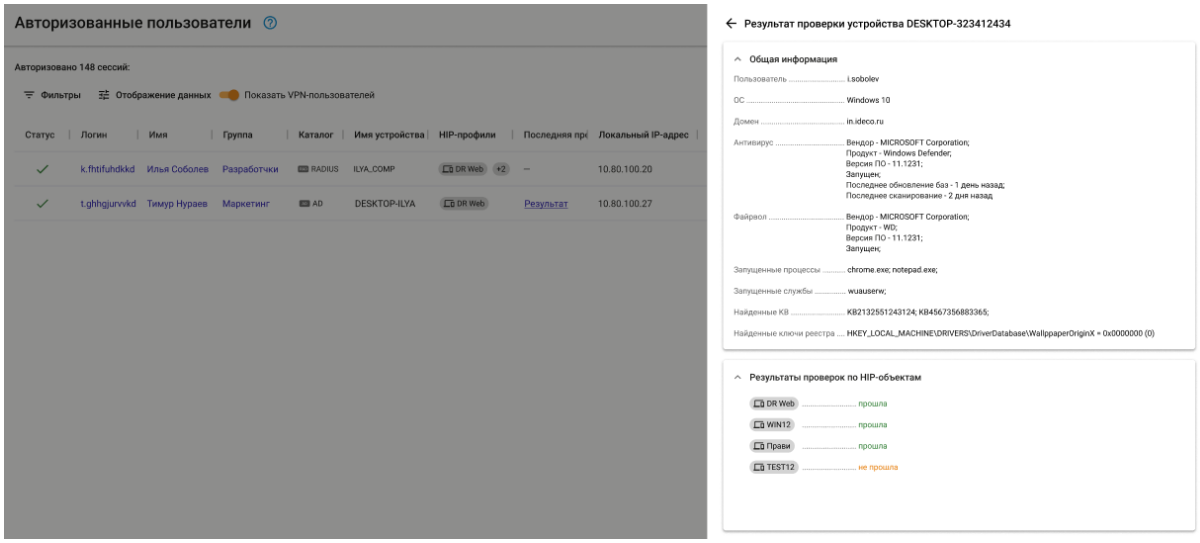


В столбце **Управление** можно разавторизовать пользователя при необходимости.

При наличии большого количества авторизованных пользователей в таблице воспользуйтесь кнопкой **Фильтры**. Включение опции **Показать только VPN-пользователей** отфильтрует в таблице журнала информацию обо всех VPN-сессиях по всем протоколам.

Подсказка: Количество сессий в мониторинге не является количеством занимаемых лицензий, так как под одной пользовательской учетной записью возможна одновременная авторизация до 5 устройств (динамическими способами авторизации, по веб, Kerberos/NTLM, логам безопасности контроллеров домена Active Directory, VPN), что будет считаться как одна пользовательская лицензия.

Для просмотра результата проверки устройства, подключенного через Ideco Client, кликните на **Результат** в столбце **Последняя проверка**, откроется соответствующее окно с общей информацией и результатами проверок по *HIP-объектам*:



15.2 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.

Предупреждение: Обратите внимание, что при отключении опции **Сбор метрик** в некоторых графиках может наблюдаться несогласованность данных по времени. Это связано с внутренней реализацией модуля.

15.2.1 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.

15.2.2 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
```

15.2.3 Диски

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

15.2.4 VPN

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

15.2.5 IPsec

Содержит информацию о входящих, исходящих IPsec-подключениях Ideco NFGW. Показывает загрузку входящего и исходящего IPsec-канала.

15.2.6 WCCP GRE

Содержит информацию о входящей скорости GRE-туннелей.

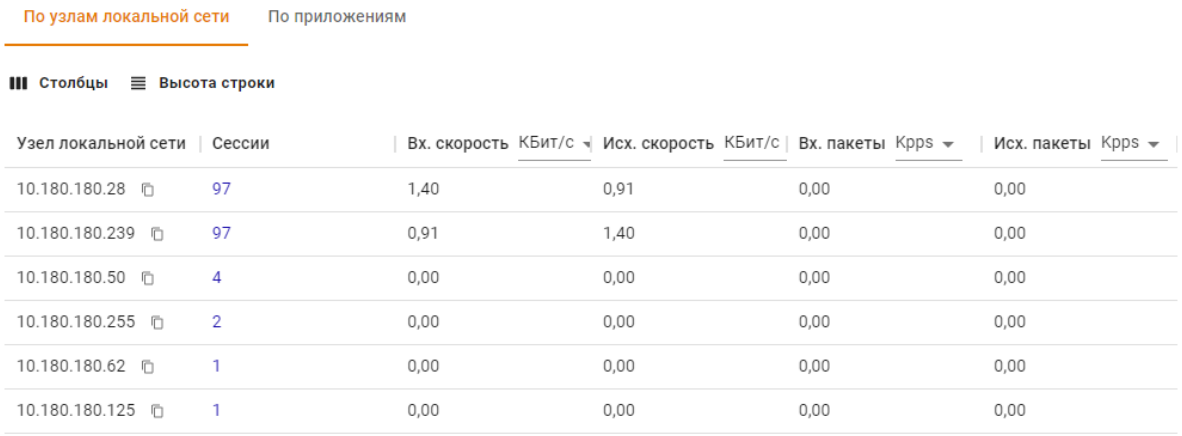
Подсказка: Нельзя получить исходящую скорость для GRE-туннелей из-за особенности протокола GRE.

15.3 Монитор трафика

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

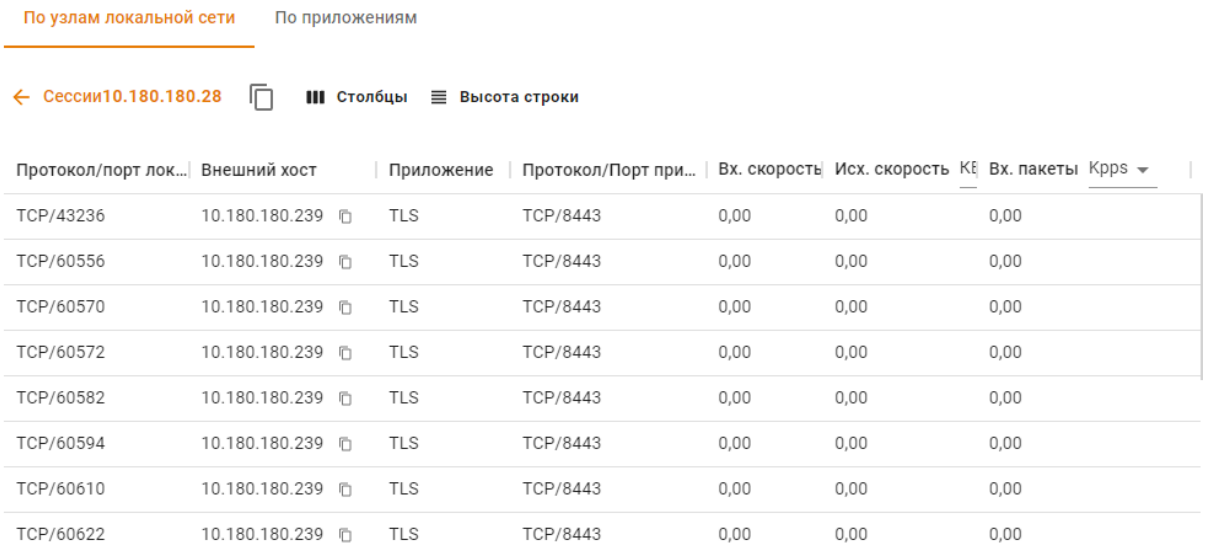
15.3.1 По узлам локальной сети

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:

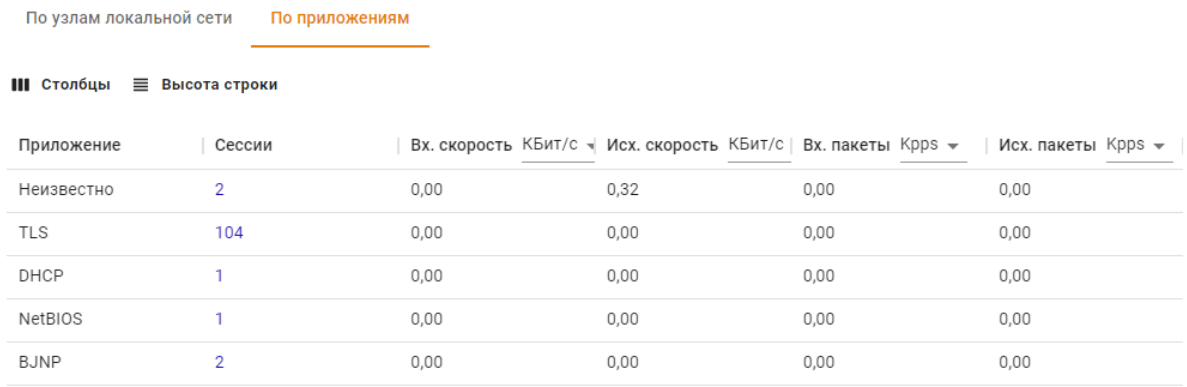


Протокол/порт лок...	Внешний хост	Приложение	Протокол/Порт при...	Вх. скорость	Исх. скорость КБ	Вх. пакеты Kpps
TCP/43236	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60556	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60570	10.180.180.239	TLS	TCP/8443	0,00	0,00	0,00
TCP/60572	10.180.180.239	TLS	TCP/8443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

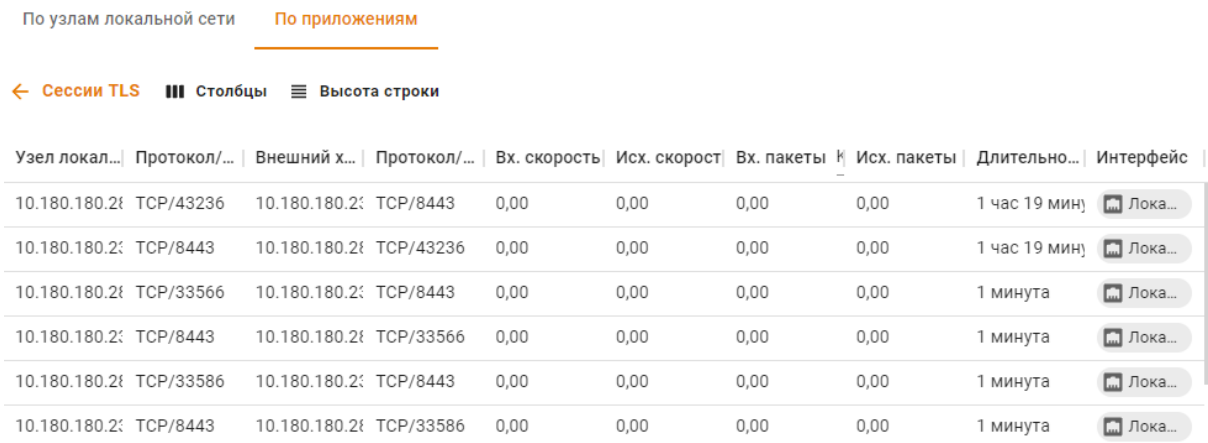
15.3.2 По приложениям

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.



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



15.4 Telegram-бот

Бот может отправлять оповещения:

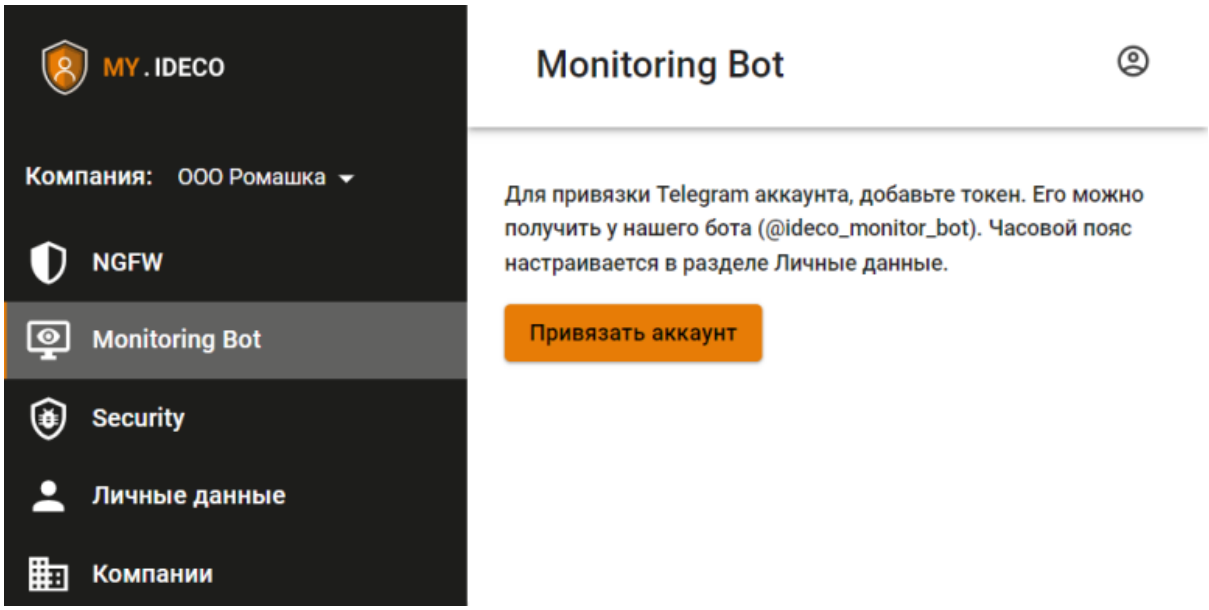
- в личные сообщения;
- в беседы, где 2 и более пользователей (groups).

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

15.4.1 Привязка Ideco Monitoring Bot

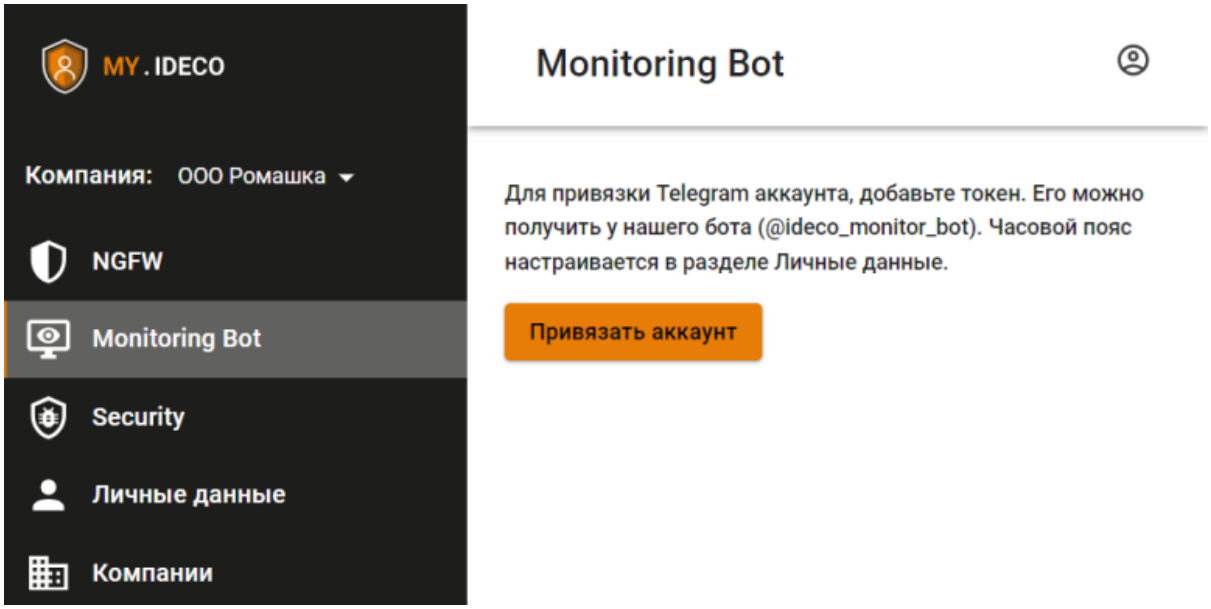
Настройка привязки Ideco Monitoring Bot к одному пользователю:

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_monitor_bot.
4. Написать `/start` в группе.
5. Скопировать код привязки к аккаунту.
6. Перейти в раздел **Ideco Monitoring Bot** в личном кабинете.
7. Нажать на кнопку **Привязать аккаунт**.
8. Ввести код в соответствующее поле и нажать на кнопку **Привязать**.



Подсказка: При настройке подключения Ideco Monitoring Bot к беседе нельзя использовать подсказки для команд, поскольку требуется ввод команды `/start` вручную.

Подсказка: Уведомления начнут приходить в телеграм-аккаунт.

15.4.2 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. Выберите уведомления, которые хотели бы получать в выбранной беседе.

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

15.5 SNMP

15.5.1 Основное

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

Опция переключается в положение Включен

Этот модуль позволяет осуществлять мониторинг работы Ideco NGFW по протоколу SNMP версий 1/2c и 3. Для настройки подключения по протоколу SNMP необходимо:

- Для версии 1/2c указать:

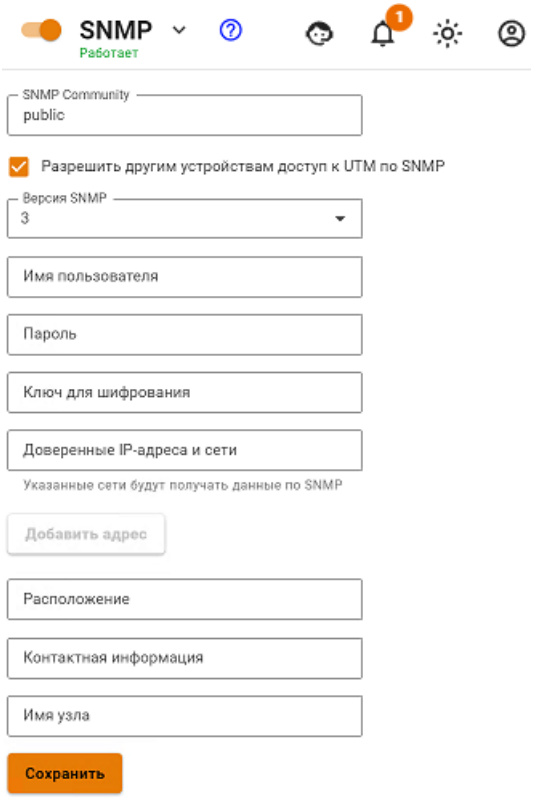
- Имя пользователя;
- Пароль (минимальное количество символов - 8);
- **Доверенные IP-адреса и сети**.

- Для версии 3 указать:
  - Имя пользователя;
  - Пароль (минимальное количество символов - 8);
  - Ключ шифрования;
  - **Доверенные IP-адреса и сети**.

Подсказка: Рекомендуем: На сервере, с которым будет осуществляться соединение по SNMPv3, указать алгоритмы: Auth Algorithm MD5 и Crypto Algorithm AES.

Поле SNMP community для SNMPv3 необязательно для заполнения.

После заполнения поля **Доверенные IP-адреса и сети** устройства, находящиеся в указанных доверенных сетях, получат доступ к данным с Ideco NGFW. Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и являются необязательными:



15.6 Zabbix-агент

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

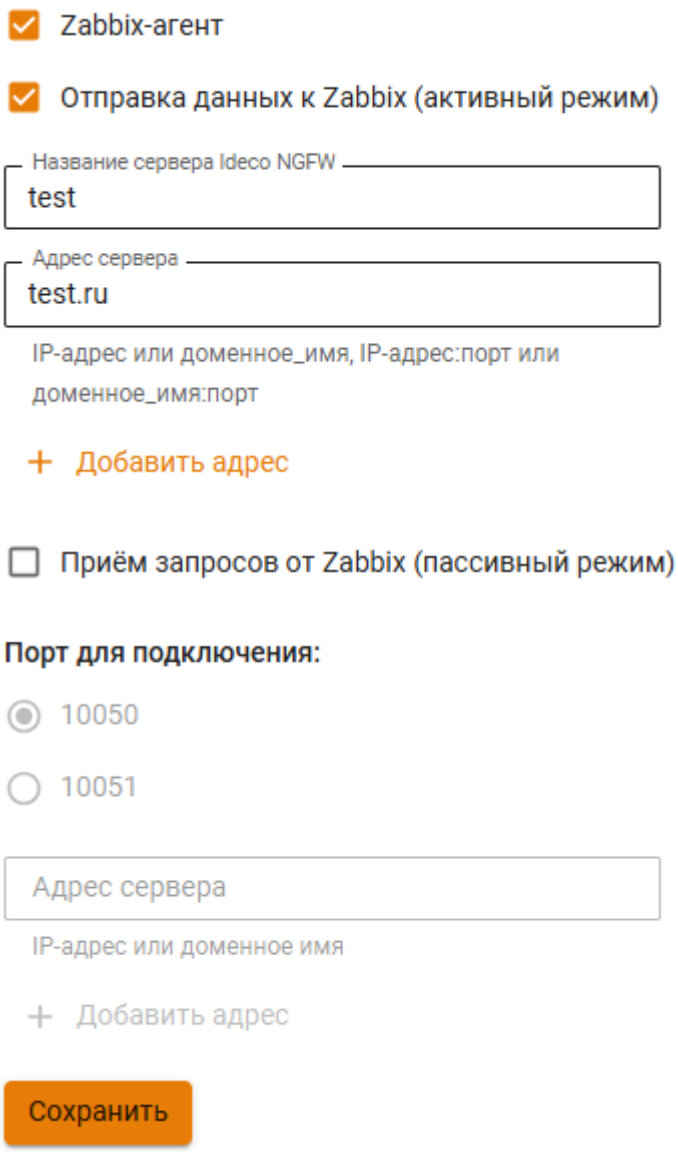
15.6.1 Настройка Zabbix-агента

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

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

Активный

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

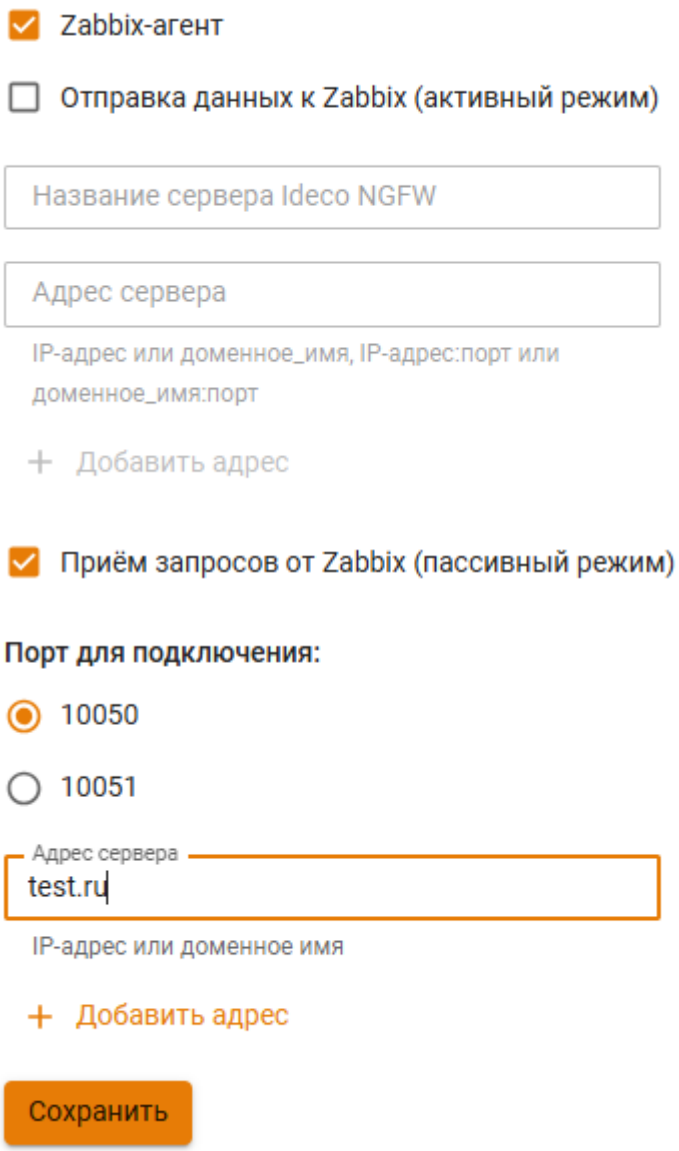


- **Имя сервера Ideco NGFW** - имя, которое будет отображаться на сервере мониторинга.
- **Адрес сервера** - IP-адрес, доменное имя, либо `IP-адрес:порт`, `доменное имя:порт`, если используется нестандартный для Zabbix входящий порт. Для добавления еще одного адреса нажмите **Добавить**

адрес.

Пассивный

Подключение происходит со стороны Zabbix-сервера. Для настройки заполните поля:



- **Порт для подключения** - выберите 10050 или 10051 порт.
- **Адрес сервера** - IP-адрес или доменное имя Zabbix-сервера. Для добавления еще одного адреса нажмите **Добавить адрес**.

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

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

15.6.2 Полезные ссылки

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

16. Правила трафика

16.1 Файрвол

Файрвол - средство управления трафиком на сервере (межсетевой экран). Поддерживает фильтрацию пакетов с контролем состояния соединений (Stateful Inspection).

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

16.1.1 Принцип работы

Файрвол анализирует заголовки IP-пакетов и TCP-сегментов, проходящих через интерфейсы сервера, и фильтрует трафик на основании параметров заголовков (IP-адреса, TCP/UDP-порты и флаги).

С помощью **Файрвола** можно создавать наборы правил, которые разграничивают трафик между различными сетями: локальными, VPN и публичными (интернет). Рекомендуется указывать IP-адрес Ideco NGFW в роли шлюза на клиентских устройствах для оптимальной работы политик безопасности (модулей **Контроль приложений** и **Предотвращение вторжений**).

Фильтрация трафика

Для обеспечения защиты в Ideco NGFW предусмотрены преднастроенные и автоматически включаемые системные правила. Пользовательские правила используются для фильтрации трафика локальной сети и публикации ресурсов.

Для фильтрации трафика **Файрвол** использует как отдельные интерфейсы, так и зоны - логические объединения сетевых интерфейсов. Преимущества такого подхода:

- Гибкость управления правилами при большом количестве интерфейсов;
- Упрощение процесса добавления/удаления интерфейсов без необходимости редактирования множества правил;
- Возможность выбора удобных названий для зон (например, **Разработчики**, **Гости**), что делает правила более читаемыми.

Инспекции DPI/IPS

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

16.1.2 Настройка и управление правилами

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

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

16.1.3 Ограничения и особенности

Сетевой экран не предназначен для решения задач контроля доступа к ресурсам по URL, доменному имени или типу контента на веб-сайтах. Эти задачи решаются с помощью *Контент-фильтра*.

Подключение по SSH

Включение режима удаленного помощника изменяет таблицу правил **Файрвола**, разрешая подключение по SSH из локальных и внешних сетей.

Connection tracking helpers

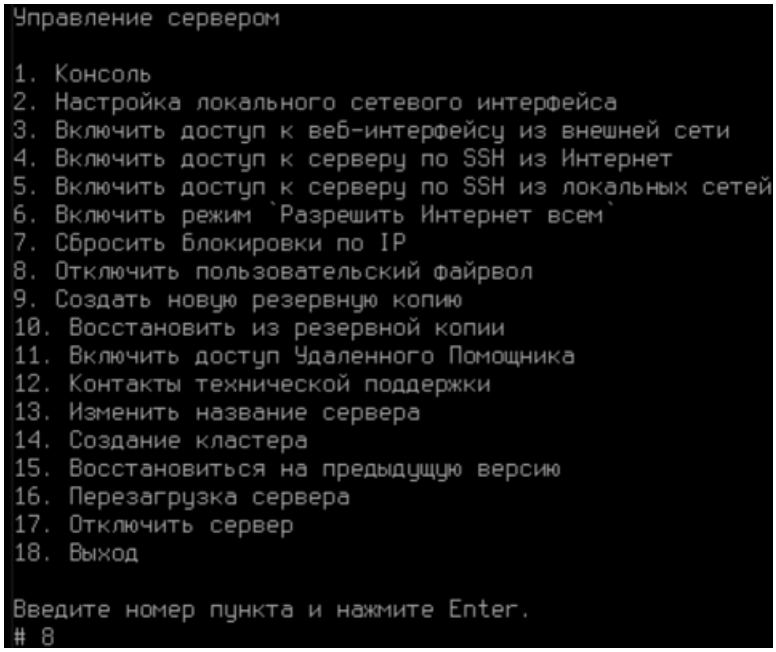
Подсказка: В Ideco NGFW включены connection tracking helpers для протоколов: ftp, sip, netbios-ns, pptp, h323. Для иных протоколов, использующих несколько портов при установлении соединения, работа через NAT не гарантируется.

Использование зон

При использовании зон в **Файрволе** следует учесть, что одна зона не может содержать более 64 интерфейсов, настроенных в разделе **Сервисы -> Сетевые интерфейсы**, а также IPsec- и VPN-подключения.

Устранение проблем

В случае создания некорректных правил (например, запрет доступа в веб-интерфейс Ideco NGFW) в локальном меню сервера выберите пункт **Отключить пользовательский файрвол** (введя цифру 8) и нажмите Enter:



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

16.1.4 Счетчик срабатываний

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

Включить опцию можно, нажав на **Отображение данных**.

16.1.5 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, port-mapping).

INPUT

Таблица для правил входящего трафика на зоны сервера. Как правило, это трафик для служб сервера (например, почтового сервера).

SNAT

Таблица пользовательских правил для управления трансляцией сетевых адресов.

Предупреждение: Правила автоматического **SNAT** работают только для интерфейсов, указанных как внешние.

Чтобы активировать автоматический SNAT для локальных сетей, переведите соответствующую опцию в положение **Включен**. Автоматический SNAT подменяет адреса источников только для следующих диапазонов: `192.168.0.0/16`, `172.16.0.0/12` и `10.0.0.0/8`.

Чтобы подменять адреса источников для других диапазонов или допустить устройства в сеть без сетевой трансляции адресов (правилом «не SNAT»), создайте правило SNAT, нажав на кнопку **Добавить**. Пользовательские правила SNAT имеют приоритет над автоматическим SNAT для локальных сетей.

Создание правил

Для создания правила в нужной таблице нажмите кнопку **Добавить** в левом верхнем углу экрана.

Укажите необходимые параметры и действия правила и нажмите кнопку **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: Важные моменты при создании правил:

- При создании правил для фильтрации веб-трафика из локальных сетей (80, 443 TCP-порты) для полноценной работы правила в поле **Зона источника** должен указываться объект **Любой**. Если будет указан иной объект, то правило не будет обрабатывать веб-трафик;
- Не используйте зону, указанную в разделе **VPN-подключения -> Основное**, для блокировки TCP. В противном случае HTTP- и HTTPS-трафик через эту зону не будет заблокирован.

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 туннельные интерфейсы для подключения к интернету (Ethernet+PPPoE, Ethernet+PPTP, Ethernet+L2TP);
  - **IPsec-интерфейсы** - все IPsec-интерфейсы, используемые для site-to-site-подключений к удаленным офисам;
  - **Локальные интерфейсы** - все интерфейсы, используемые для подключения к клиентам в локальной сети;
  - **Исходящий трафик устройства** - используется для фильтрации исходящего трафика самого устройства Ideco NGFW;
  - **Клиентский VPN-трафик** - используется для фильтрации трафика, идущего от клиентов, подключившихся к NGFW по VPN;
  - **Любой** - не фильтровать трафик по какому-либо типу интерфейса или зоны.

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 файрвола для IPsec-подключений, выберите в поле **Зона источника** или **Зона назначения** настроенное IPsec-подключение.

Портмаппинг, DNAT, публикация сервера в локальной сети:

Примеры данных настроек подробно описаны в статьях раздела *Публикация ресурсов*.

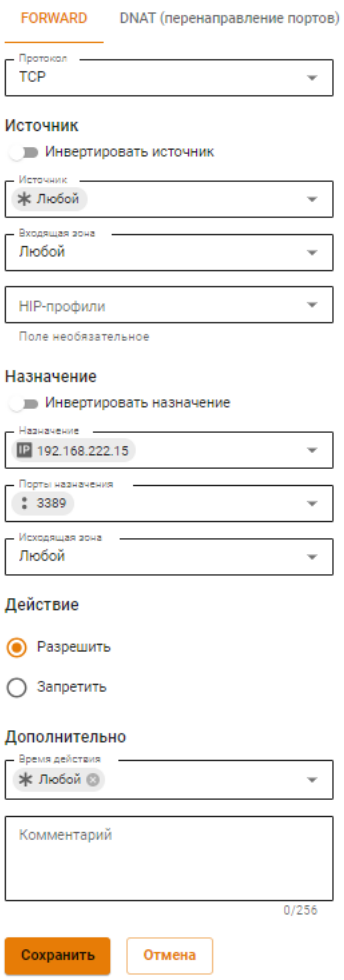
Блокировка различных ресурсов средствами файрвола:

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

Доступ к терминальному серверу для определенного пользователя:

1. На вкладке **FOFWARD** 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**.

16.1.6 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** на 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.

Для просмотра логов перейдите в раздел **Отчеты и журналы ->** ***Системный журнал*** и настройте фильтр событий (Служба - равен - ideco-nflog). Логи могут отправляться в сторонние коллекторы через *syslog*.

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

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

Действия для логирования

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

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

Трафик для логирования

Создайте и включите в таблице правило для трафика. Если сработает правило **Файрвола** с трафиком, подходящим под правило логирования, то срабатывание правила **Файрвола** будет залогировано.

> **Внимание:** Если ни одно правило в таблице не задано, срабатывание правил логироваться не будет.
>
> Правила отметки трафика могут снять отметку с помощью действия **Не логировать** для трафика, помеченного ранее действием **Логировать**.

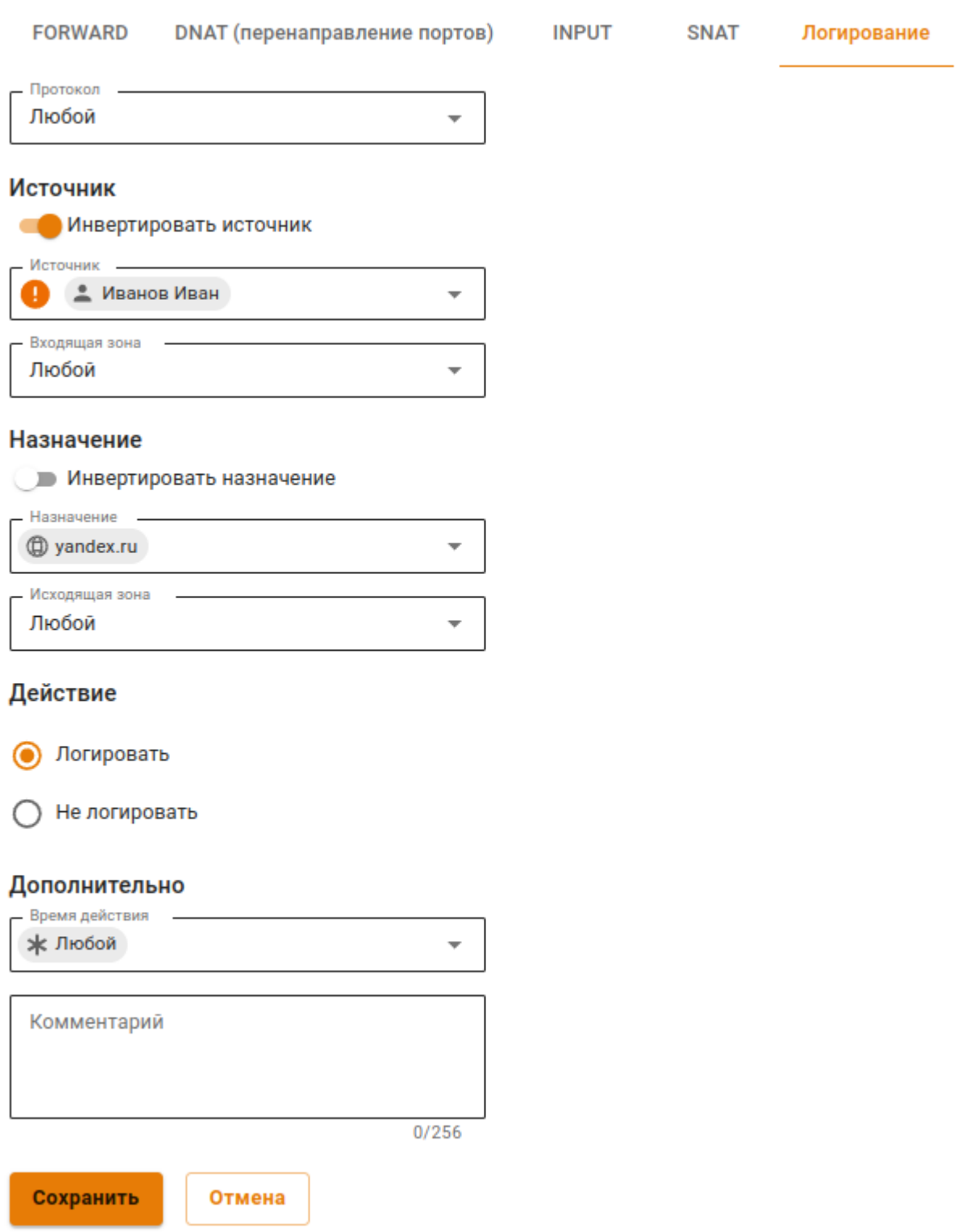
Предоставляется возможность гибкой выборки трафика, который подлежит логированию, за счет правил таблицы **Логирование**.

Пример: требуется настроить логирование всего трафика на yandex.ru, кроме трафика от пользователя Иванова Ивана:

1. В поле **Источник** выберите *Иванова Ивана* и переведите опцию **Инвертировать источник** в положение **Включен**.

2. В поле **Назначение** выберите `yandex.ru`.

3. Выберите действие **Логировать**:


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

16.2 Контроль приложений

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

Внимание: В 18 версии Ideco NGFW все правила из раздела **Правила трафика -> Контроль приложений** будут доступны только для просмотра!

Чтобы подготовиться к изменениям, обновите версию до 17.5 (если у вас 17.4 и ниже), создайте профили в разделе **Профили безопасности -> *Профили контроля приложений*** и выберите их в правилах ***Файрвола***: они не будут влиять на работу существующих правил Файрвола и Контроля приложений, но начнут работать после обновления на 18 версию.

Подсказка: 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 этих разделов добавьте соответствующее правило в **Правила трафика -> Исключения**.

Сессии, установленные, пока **Контроль приложений** был отключен, не будут проверены после включения модуля. Если необходимо, чтобы **Контроль приложений** их проверил, нужно вручную разорвать эти сессии и установить заново.

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

При нажатии раскроется список модулей с их статусами.

Модуль 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**), то будет применено правило, стоящее выше по списку.

Внимание: При отключении модуля **Контроль приложений** в левом верхнем углу:

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

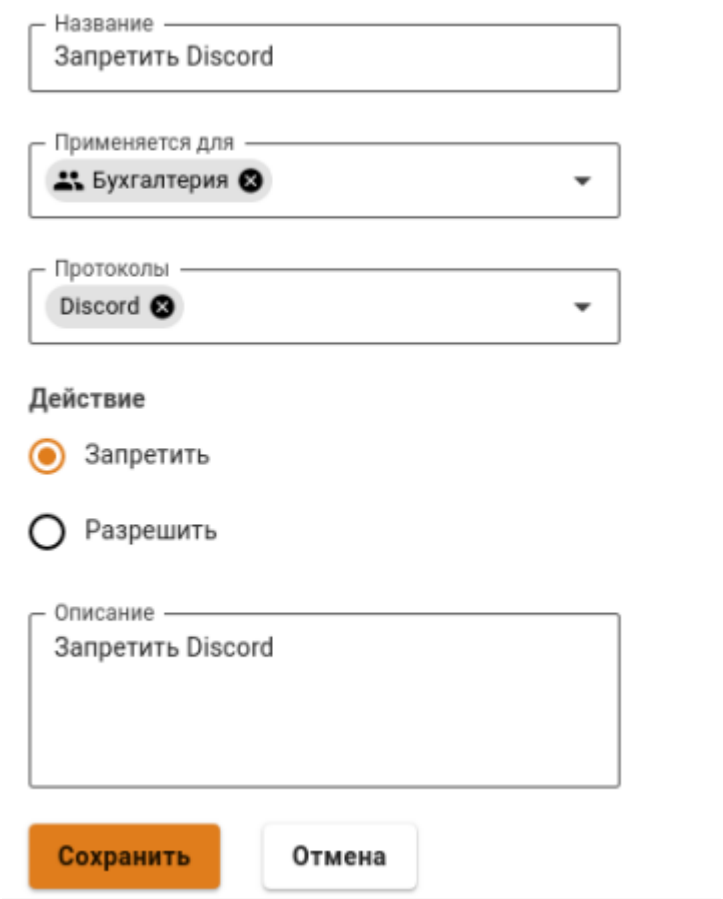
16.2.1 Создание правил

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;
- **Комментарий** - введите описание правила или оставьте поле пустым.

3. Нажмите **Сохранить**.

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

Подсказка: О блокировке программ удаленного доступа, анонимайзеров, торрентов и других популярных

ресурсов смотрите в статье *Блокировка популярных ресурсов*.

Описание протоколов и сервисов, доступных для создания правил:

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

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

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

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

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

ANSI_C1222
Протокол прикладного уровня, предназначенный для использования в сетях электросчетчиков Smart Grid.

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

AVASTSecureDNS
Сервис защищенных DNS-серверов от компании Avast.

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

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

AdobeConnect
Платформа веб-конференций, которая позволяет пользователям проводить онлайн-встречи, вебинары.

AdultContent
Сайты и приложения, связанные с контентом «для взрослых».

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

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

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

AmazonAWS
Коммерческое публичное облако, поддерживаемое и развиваемое компанией Amazon.

AmazonAlexa
Облачная голосовая служба Amazon.

AmazonVideo
Стриминговый сервис компании Amazon.

AmongUs
Многопользовательская компьютерная игра.

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

Apple
Компания-производитель смартфонов и компьютерной техники.

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

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

AppleStore
Онлайн-магазин техники Apple и аксесуаров к ней.

AppleTVPlus
Американский стриминговый сервис, принадлежащий и управляемый компанией Apple.

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

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

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

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

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

BFCP
Протокол предназначен для обмена презентациями и демонстрации рабочего стола в рамках видеоконференции.

BFD
Протокол обнаружения двунаправленной пересылки, который используется для обнаружения неисправностей между двумя маршрутизаторами или коммутаторами.

BGP
Протокол динамической маршрутизации.

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

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

Badoo
Приложение для онлайн-знакомств.

BeckhoffADS
Открытый протокол обмена данными ADS на базе TCP/IP для общения с контроллером, разработанный BECKHOFF.

BitTorrent
Пиринговый протокол для кооперативного обмена файлами через интернет.

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

Bluesky
Bluesky Socialg представляет собой децентрализованную социальную платформу для микроблогов.

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

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

CIP
Информационно-управляющий протокол, который обеспечивает обмен сообщениями ввода/вывода в реальном времени и прямой обмен информационными сообщениями.

CNN
Американский круглосуточный кабельный телеканал новостей.

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

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

Cachefly
Поставщик сети доставки контента.

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

Ceph
Свободная программная объектная сеть хранения, обеспечивающая как файловый, так и блочный интерфейсы доступа.

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

CiscoVPN
Протокол VPN, разработанный компанией Cisco Systems.

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

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

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

CoD_Mobile
Бесплатный шутер для устройств iOS и Android.

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

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

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

Crashlytics
Инструмент отчетности о сбоях, который помогает выявлять ошибки.

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

CryNetwork
Составной модуль для создания многопользовательских игр.

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

DCERPC
Система удаленного вызова процедур, разработанная для Distributed Computing Environment.

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

DHCPV6
Протокол динамического конфигурирования хостов для межсетевого протокола версии 6.

DLEP
Протокол маршрутизации с учетом радиосвязи (RAR).

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

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

DNScrypt
Протокол шифрования DNS-трафика.

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

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

Dailymotion
Французский видеохостинг.

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

Dazn
Спортивный стриминговый сервис.

Deezer
Французский интернет-сервис потоковой передачи музыки.

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

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

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

DisneyPlus
Американский сервис потокового вещания типа OTT на основе подписки.

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.

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

Dota2
Многопользовательская командная компьютерная игра в жанре MOBA, разработанная и изданная корпорацией Valve.

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

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

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

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

EGP
Устаревший протокол обмена информации между маршрутизаторами нескольких автономных систем.

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

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

Elasticsearch
Тиражируемая программная поисковая система.

ElectronicArts
Американская публичная транснациональная корпорация, занимающаяся распространением и изданием компьютерных игр (FIFA, Battlefield).

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

Ether-S-Bus
Промышленный протокол управления, используемый компанией SAIA Burgess.

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

EthernetGlobalData
Протокол связи, разработанный GE Fanuc Automation для обмена данными в реальном времени между устройствами автоматизации и системами управления с использованием стандартной технологии Ethernet.

EthernetIP
Промышленный сетевой стандарт, который поддерживает неявный обмен сообщениями (обмен сообщениями ввода/вывода в реальном времени), явный обмен (обмен сообщениями) или оба и использует широко распространенные коммерческие чипы связи Ethernet и физические носители.

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

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

FLUTE
Доставка файлов по однонаправленному транспорту.

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

FTP_CONTROL
Протокол, предназначенный для передачи файлов в компьютерных сетях.

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

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

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

FacebookVoip
Голосовые и видеозвонки в FaceBook.

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

FbookReelStory
Короткие видеоролики на Facebook.

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

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

GRE
Протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems.

GTP
Протокол туннелирования GPRS.

GTP_C
Группа протоколов соединения на основе IP, используемая в сетях GSM, UMTS и LTE.

GTP_PRIME
Группа протоколов связи на основе IP, используемых для передачи услуг пакетной радиосвязи общего пользования (GPRS) в сетях GSM, UMTS, LTE.

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

GaijinEntertainment
Частная компания, разработчик и издатель компьютерных игр, в частности - War Thunder.

GeForceNow
Облачный игровой сервис компании Nvidia.

Gearman
Платформа приложений с открытым исходным кодом, предназначенная для распределения соответствующих компьютерных задач на несколько компьютеров.

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

Git
Распределенная система управления версиями.

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

GitLab
Веб-инструмент жизненного цикла DevOps с открытым исходным кодом, представляющий систему управления репозиториями кода для Git с собственной вики, системой отслеживания ошибок, CI/CD пайплайном и другими функциями.

Gmail
Бесплатная почтовая служба от компании Google. Предоставляет доступ к почтовым ящикам через веб-интерфейс и по протоколам POP3, SMTP и IMAP, а также в приложении Gmail на Android.

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

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

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

GoogleCall
Аудио- и видеозвонки, совершаемые с помощью (любых) приложений Google (например, Google Meet).

GoogleChat
Коммуникационный сервис, разработанный компанией Google.

GoogleClassroom
Облачная платформа для организации образовательного процесса.

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

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

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

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

GoogleMeet
Сервис видео-телефонной связи и видеоконференций, разработанный компанией Google.

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

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

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

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

HART-IP
Адресуемый по магистрали удаленный преобразователь по IP, в основном используется для обмена данными в качестве стандартного глобального протокола между интеллектуальными устройствами и системой управления и некоторой интеллектуальной системой.

HBO
Американский телеканал, принадлежащий компании WarnerMedia.

HL7
Стандарт обмена, управления и интеграции электронной медицинской информации.

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

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

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

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

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

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

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

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

HiSLIP
Коммуникационный протокол для измерительного и тестового оборудования с использованием технологии VISA.

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

Huawei
Трафик устройств Huawei.

HuaweiCloud
Мобильное облако Huawei.

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

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

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

IceCast
Протокол для организации потокового цифрового аудиовещания и видеовещания.

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

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

ICMPV6
Протокол управляющих сообщений для межсетевого протокола версии 6.

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

IEC62056
Набор стандартов Международной электротехнической комиссии для обмена данными учета электроэнергии.

IEEE-C37118
Потоковый протокол для обмена и передачи данных синхрофазоров (или PMU), которые фиксируют устойчивое состояние или динамический отклик энергосистемы. Обеспечивает высокоскоростную передачу большого количества данных в режиме реального времени.

IFLIX
Малайзийский бесплатный видеосервис.

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

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

IMAP
Протокол для доступа к электронной почте.

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

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

Instagram
Американская социальная сеть для обмена фотографиями и видео.

IPP
Протокол, используемый для передачи документов на печать.

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

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

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

iQIYI
Китайская онлайн-видеоплатформа, предлагающая широкий спектр оригинального и лицензионного контента, включая фильмы, драмы, развлекательные шоу и аниме.

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

ISO9506-1-MMS
Протокол передачи данных реального времени и команд диспетчерского управления между сетевыми устройствами и/или программными приложениями.

JRMI
Протокол удаленного вызова методов Java.

JSON-RPC
Протокол удаленного вызова процедур, использующий JSON для кодирования сообщений.

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

KCP
Протокол связи, который максимально использует полосу пропускания для надежной связи с низкой задержкой.

KNXnet_IP
Протокол автоматизации зданий, который обеспечивает обмен данными и управляющей информацией через IP-сети, расширяя стандарт KNX для автоматизации дома и зданий.

Kafka
Распределенный программный брокер сообщений с открытым исходным кодом.

KakaoTalk
Бесплатное мобильное приложение для мгновенного обмена сообщениями для смартфонов.

KakaoTalk_Voice
Популярный в Южной Корее мессенджер, который поддерживает мгновенную передачу сообщений, позволяет отправлять файлы, а также совершать аудиозвонки и видеозвонки.

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

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

Kontiki
Платформа доставки видео и контента.

LDAP
Протокол для доступа к службе каталогов X.500.

LDP
Протокол маршрутизации, используемый для установления и поддержания путей с коммутацией меток в сети с многопротокольной коммутацией меток (MPLS).

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

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

LastFM
Сервис для прослушивания музыки онлайн.

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

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

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

LinkedIn
Американская социальная сеть для поиска и установления деловых контактов.

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

LoLWildRift
League of Legends: Wild Rift — мобильная игра в жанре MOBA.

LotusNotes
Программный продукт, платформа для автоматизации совместной деятельности рабочих групп, содержащий в себе средства электронной почты, персональных и групповых электронных календарей, службы мгновенных сообщений и среду исполнения приложений делового взаимодействия.

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

MGCP
Протокол управления медиашлюзами.

MPEG_TS
Протокол для передачи аудиоданных и видеоданных, описанных в MPEG2.

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

MS-RPCH
Microsoft RPC-over-HTTP (RPC через HTTP) позволяет клиентам RPC подключаться через интернет к программам сервера RPC и выполнять удаленные вызовы процедур.

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

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

Mastodon
Бесплатное программное обеспечение с открытым исходным кодом для запуска самостоятельных служб социальных сетей. Он имеет функции микроблогов, аналогичные Twitter.

Megaco
Протокол для управления функциями шлюза на границе пакетной сети.

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

MerakiCloud
Сервис компании Cisco, предоставляющий доступ к облачным технологиям.

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

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

Microsoft365
Набор веб-сервисов на основе платформы Microsoft Office, электронная почта, функции для общения и управления документами, которые распространяются на основе подписки по схеме программное обеспечение как услуга.

Mining
Протоколы, использующиеся программами-майнерами.

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

Monero
Криптовалюта на основе протокола CryptoNote, ориентированная на повышенную конфиденциальность транзакций.

MongoDB
Протокол, используемый для взаимодействия клиентов и серверов MongoDB.

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

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

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

Mumble
Свободное кроссплатформенное VoIP-приложение с открытым кодом, включающее особую технологию «позиционирования звука», как основную отличительную особенность.

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

MySQL
Протокол, используемый для взаимодействия клиентов и серверов MySQL.

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

NFS
Протокол сетевого доступа к файловым системам.

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

NTP
Протокол для синхронизации внутренних часов компьютера.

Nats
Система обмена сообщениями с открытым исходным кодом.

NestLogSink
Система логирования для домашней системы пожарной безопасности от Google.

NetBIOS
Протокол, используемый для обнаружения компьютеров в сети.

NetEaseGames
Трафик различных игр NetEase.

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

NetFlix
Стриминговый сервис фильмов и сериалов.

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

NoMachine
Проект итальянской компании Medialogic S.p.A. для дистанционной работы.

Ntop
Программное обеспечение, которое исследует компьютерную сеть.

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

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

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

OICQ
Распространенный в Китае сервис мгновенного обмена сообщениями.

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

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

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

OpenDNS
Протокол, предоставляющий общедоступные DNS-серверы.

OpenFlow
Протокол управления процессом обработки данных, передающихся по сети маршрутизаторами и коммутаторами.

OpenVPN
Протокол VPN с открытым исходным кодом.

OperaVPN
VPN-клиент, встроенный в браузер Opera.

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

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

PFCP
Протокол, используемый для связи между функциями управления (CP) и пользователя (UP) в сетях 4G и 5G.

PGM
Протокол надежной многоадресной передачи данных.

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

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

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

PROFINET_IO
Протокол для связи реального времени (RT) и изохронного реального времени (IRT) с децентрализованной периферией.

PTPv2
Протокол синхронизации для промышленных сетей.

Pandora
Тип цифровой криптовалюты.

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

PathofExile
Бесплатная онлайн-ролевая игра в жанре экшн.

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

PlayStore
Онлайн-магазин приложений для Android.

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

Pluralsight
Платформа для онлайн-обучения.

PostgreSQL
Протокол, используемый для взаимодействия клиентов и серверов PostgreSQL.

PPStream
Китайское программное обеспечение для одноранговой потоковой передачи видео.

PrivateInternetAccess
Персональная служба VPN.

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

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

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

QQ
Протокол мгновенного обмена сообщениями.

QUIC
Экспериментальный интернет-протокол, позволяющий мультиплексировать несколько потоков данных между двумя компьютерами. Протокол работает поверх протокола UDP и содержит возможности шифрования, эквивалентные TLS и SSL.

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

RDP
Протокол удаленного рабочего стола.

RESP
Двоичный протокол, в котором используются управляющие последовательности, закодированные в стандартном ASCII.

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

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

RSYNC
Утилита для удаленной синхронизации и копирования файлов.

RTCP
Протокол управления передачей в реальном времени.

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

RTP
Протокол, используемый при передаче трафика реального времени.

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

RTSP
Протокол реального времени, предназначенный для использования в системах, работающих с мультимедийными данными. Позволяет удаленно управлять потоком данных с сервера.

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

Radmin
Условно бесплатная программа удаленного администрирования ПК для платформы Windows, которая позволяет полноценно работать на нескольких удаленных компьютерах с помощью графического интерфейса.

Raft
Компьютерная игра в жанре симулятор выживания в открытом мире, разработанная шведской компанией Redbeet Interactive и изданная Axolot Games.

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

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

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

RipeAtlas
Протокол зонда RIPE Atlas используется для крупнейшей в мире активной сети измерения Интернета.

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

Roughtime
Протокол с криптографической защитой на базе UDP, который используется для синхронизации времени серверов.

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

S7CommPlus
Собственный протокол Siemens, который позволяет взаимодействовать с программируемыми логическими контроллерами (ПЛК) семейства Siemens S7-300/400. Сложнее протокола S7Comm и использует двухбайтовое поле под названием ID сессии для защиты от атак воспроизведения.

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

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

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

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).

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

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

SMPP
Протокол одноранговой передачи коротких сообщений.

SMTP
Протокол, предназначенный для передачи электронной почты.

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

SNMP
Протокол для управления устройствами в IP-сетях.

SOAP
Протокол обмена структурированными сообщениями в распределенной вычислительной среде.

SOCKS
Протокол сеансового уровня модели OSI, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно для них) и таким образом использовать сервисы за межсетевыми экранами (файрволами).

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

SRTP
Определяет профиль протокола RTP и предназначен для шифрования, установления подлинности сообщения, целостности, защиты от подмены данных RTP в однонаправленных и multicast-передачах медиа и приложениях.

SSDP
Протокол, служащий для объявления и обнаружения сетевых сервисов.

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

STOMP
Simple Text Oriented Messaging Protocol, протокол обмена сообщениями.

STUN
Протокол, который позволяет клиенту, находящемуся за сервером трансляции адресов (или за несколькими такими серверами), определить свой внешний IP-адрес, способ трансляции адреса и порта во внешней сети, связанный с определенным внутренним номером порта.

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

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

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

Showtime
Американский кабельный телевизионный канал.

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

SignalVoip
Протокол голосовой связи в мессенджере Signal.

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

SinaWeibo
Китайский сервис микроблогов, запущенный компанией Sina Corp.

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

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

Skype_TeamsCall
Бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее видеосвязь через интернет. Опционально использует технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны.

Slack
Корпоративный мессенджер.

Snapchat
Мобильное приложение обмена сообщениями с прикрепленными фото и видео.

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

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

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

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

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

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

Steam
Онлайн-сервис цифрового распространения компьютерных игр и программ.

SteamDatagramRelay
Закрытая виртуальная игровая сеть Valve. Используя функции API, позволяет перенести игровой трафик на сетевые магистрали Valve.

Syncthing
Приложение, позволяющее синхронизировать файлы между несколькими устройствами.

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

TES_Online
The Elder Scrolls Online — это MMORPG, действие которой разворачивается в фэнтезийном мире Тамриэля.

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

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

TLS
Протокол защиты транспортного уровня.

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

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

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

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

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

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

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

TelegramVoip
Голосовые и видеозвонки в мессенджере Telegram.

Telnet
Протокол для реализации текстового терминального интерфейса по сети.

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

TencentGames
Подразделение Tencent Interactive Entertainment, выпускающее видеоигры, разработчик PUPG MOBILE.

Tencentvideo
Китайская стриминговая платформа, принадлежащая Tencent.

Teredo
Сетевой протокол, предназначенный для передачи IPv6-пакетов через сети IPv4, в частности, через устройства, работающие по технологии NAT, путем их инкапсуляции в UDP-дейтаграммы.

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

Threads
Онлайн-сервис социальных сетей и социальных сетей, управляемый Meta Platforms.

Threema
Кроссплатформенное зашифрованное приложение для обмена мгновенными сообщениями.

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

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

Tidal
Интернет-сервис подписки на музыку, подкасты и потоковое видео, сочетающий в себе звук без потерь и музыкальные видеоролики высокой четкости с эксклюзивным контентом и специальными функциями для музыки.

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

TocaBoca
Интерактивная мобильная игра.

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

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

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

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

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

TunnelBear
Кроссплатформенный VPN-клиент.

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

TVUplayer
Протокол, используемый для просмотра телевидения через интернет.

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

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

UBNTAC2
Утилита управления оборудованием Ubiquiti airControl, версия 2.

UFTP
Протокол передачи файлов на основе UDP.

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

UbuntuONE
Онлайн-хранилище для обмена файлами и синхронизации между компьютерами и мобильными устройствами.

UltraSurf
Бесплатная утилита для обхода цензурных ограничений в интернете.

Unknown
Не распознанные модулем протоколы и приложения.

Usenet
Протокол, используемый для общения и публикации файлов.

Vevo
Музыкальный видеосайт и видеохостинг.

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

VK
Приложение для взаимодействия с социальной сетью ВКонтакте.

VMware
Американская компания-разработчик программного обеспечения для виртуализации.

VNC
Протокол удаленного доступа к рабочему столу.

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

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

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

ViberVoip
Аудио/видеозвонки, совершаемые с помощью приложения Viber.

Vimeo
Американский сервис для публикации и просмотра видео.

Vudu
Потоковый сервис цифрового видео.

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..

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

Waze
Бесплатное социальное навигационное приложение для мобильных устройств, позволяющее отслеживать ситуацию на дорогах в режиме реального времени, прокладывать оптимальные маршруты, узнавать о расположении радаров скорости.

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

WebDAV
Набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах.

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

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

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

WhatsAppCall
Протокол голосовой передачи, основанный на VoIP.

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

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

Wikipedia
Самая крупная в мире онлайн-энциклопедия.

WindowsUpdate
Сервис обновления операционной системы Windows.

WireGuard
Высокоскоростной и безопасный VPN-протокол.

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

WorldOfWarcraft
Массовая многопользовательская ролевая онлайн-игра.

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

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

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

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

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

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

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

YandexDisk
Сервис для хранения данных в облаке.

YandexMail
Почтовый сервис от компании Яндекс.

YandexMarket
Сервис заказа товаров онлайн.

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

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

Yojimbo
Менеджер личной информации для MacOS от Bare Bones Software. Позволяет хранить заметки, изображения и медиафайлы, URL-адреса, веб-страницы и пароли.

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

YouTubeUpload
Загрузка файлов на видеохостинг YouTube.

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

ZUG
Протокол ZUG является частью консенсусной модели Casper 2.0.

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

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

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

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

16.3 Контент-фильтр

Подсказка: Название службы раздела *Контент-фильтра*: `ideco-content-filter-backend.service`. Список имен служб для других разделов доступен по *ссылке*.

Для записи логов поставьте флаг строке **Включить журналирование** в разделе **Сервисы -> Прокси -> Основное**.

Контент-фильтр проверяет наличие сайта, который хочет открыть пользователь, в списках ресурсов Ideco NGFW. Если адрес находится в этих списках, то применяются настроенные правила фильтрации.

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**.

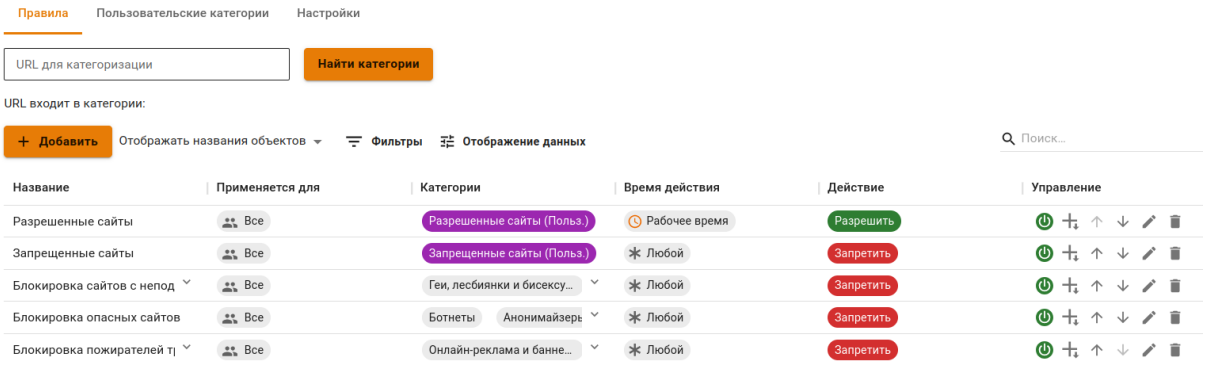
Контент-фильтр состоит из трех вкладок: **Правила**, **Ппользовательские категории** и **Настройки**.

С помощью кнопки **Фильтры** можно отфильтровать значения на вкладках **Правила** и **Пользовательские категории**.

16.3.1 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, выбрать категорию сайтов и указать время действия правила. 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 категории, созданные на вкладке **Пользовательские категории**;

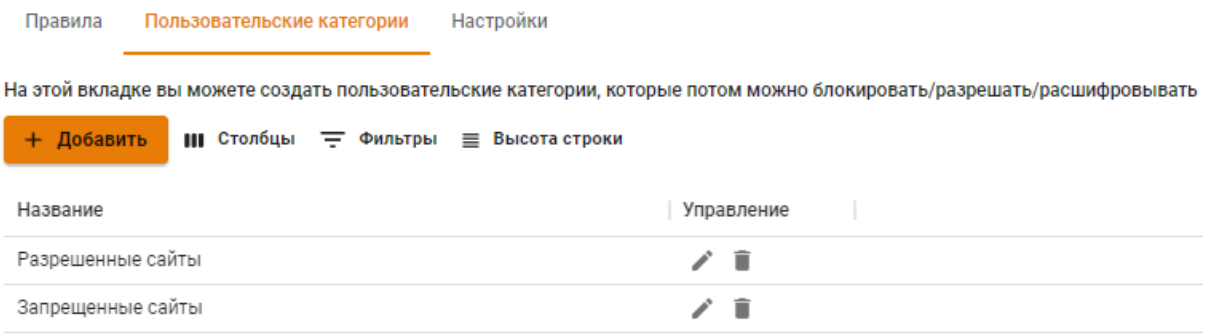
2. **Специальные**. Включает 4 категории: все запросы, все категоризированные запросы, все некатегоризированные запросы и запросы с прямыми обращениями по IP-адресам;

3. **Расширенные**. Правила, включающие расширенные категории, работают только с включенной опцией **Расширенная база категорий** на вкладке **Настройки**;

4. **Файлы**. Восемь сформированных категорий файлов, блокируемых по расширениям и MIME-type. Предустановленные группы файлов (Исполняемые файлы, Архивы, Видеофайлы, Аудиофайлы, Flash-видео, Active-X, Torrent-файлы, Документы) нельзя редактировать. Работа по фильтрации HTTPS-трафика по этому типу категорий возможна только при его расшифровке.

16.3.2 Пользовательские категории

На одноименной вкладке создаются собственные категории правил.

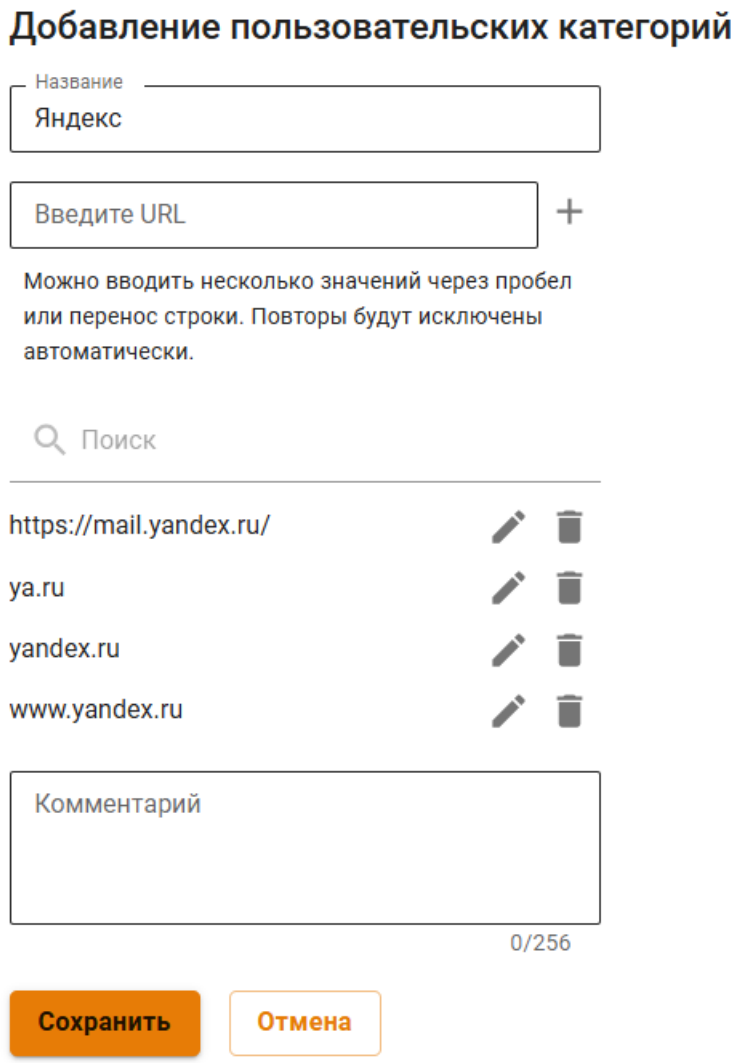


Подробное описание **расширенных** и **специальных** категорий читайте в статье *Описание категорий контент фильтра*.

При создании 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.

Внимание: При создании пользовательских категорий обратите внимание на алгоритм работы **Контент-фильтра**.

Если создать пользовательскую категорию с доменом domain.ru, которая используется в правиле **Контент-фильтра**, то это правило будет корректно работать для domain.ru, www.domain.ru и *.domain.ru.

Однако если создать еще одну пользовательскую категорию с таким же доменом (например, www.domain.ru или *.domain.ru), то правило с пользовательской категорией domain.ru перестанет работать для доменов www.domain.ru и *.domain.ru, **даже если эта созданная категория не используется ни в одном правиле**.

Подсказка: Если URL или домен содержит специальные символы (или •), оставьте их в исходном виде.

Адрес будут автоматически закодирован в формат punycode.

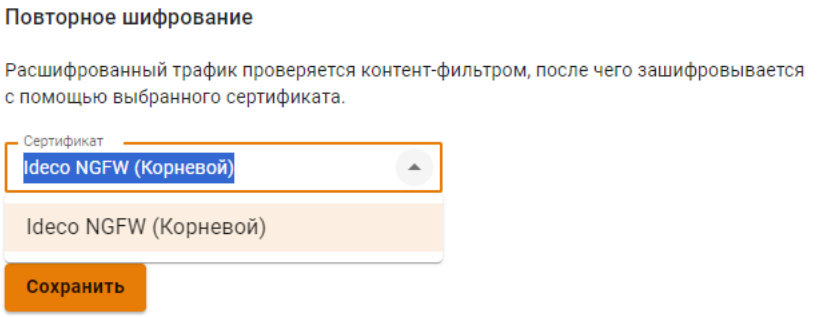
16.3.3 Настройки

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.

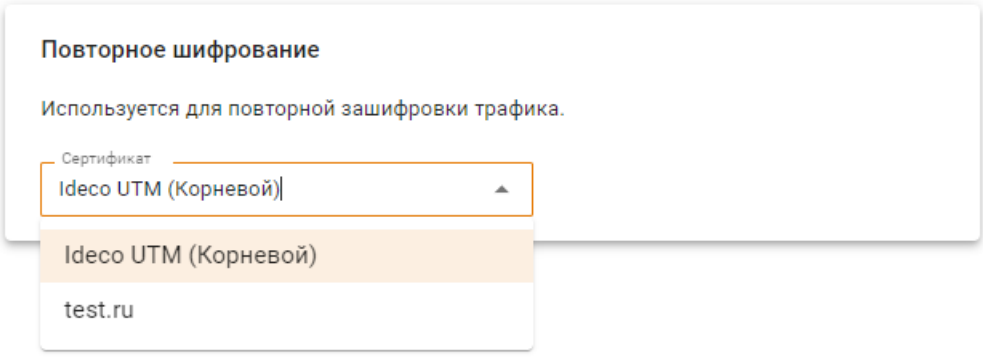
Подсказка: Если отключить опцию **Расширенная база категорий**, то все правила, включающие в себя расширенные категории, перестанут срабатывать.

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. Заблокированный трафик нельзя исключить, добавив IP-адрес в списки исключений на вкладке **Прокси -> Исключения**;
- **Безопасный поиск.** Принудительно включает безопасный поиск в поисковых системах (Google, Yandex, YouTube, Yahoo, Bing, Rambler). **Для работы этой функции нужно включить HTTPS-фильтрацию методом подмены сертификата для данных ресурсов**.



Если для повторного шифрования требуется использовать сертификат, отличный от корневого в NGFW, загрузите нужный сертификат в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** и выберите его для повторного шифрования:



16.3.4 Применение правил

Подсказка: Процесс блокировки ресурсов, взаимодействующих с чат-ботами, описан в *статье*.

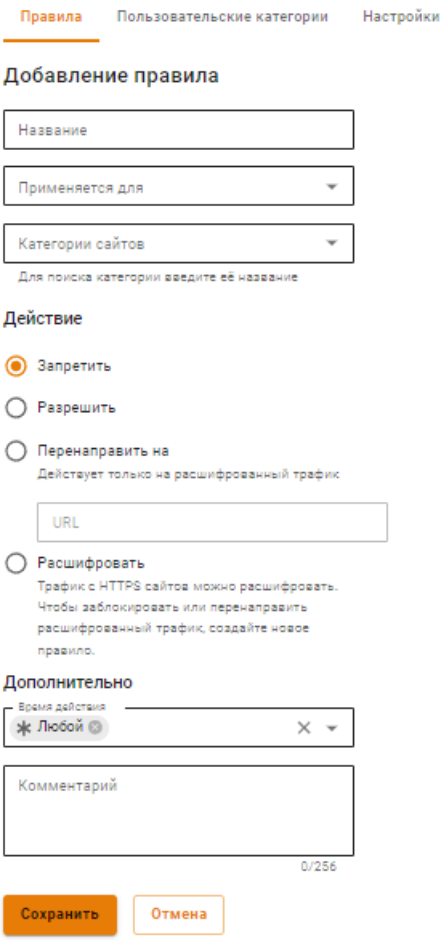
Применение правил фильтрации для пользователей:

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 удалять. Правила контентной фильтрации применяются сразу после их создания или включения.

Чтобы создать новое правило, нажмите **Добавить** в левом верхнем углу над таблицей.

Заполните следующие поля:



- **Название** - наименование правила в списке. Значение не должно быть длиннее 42 символов;
- **Применяется для** - можно выбрать объекты типа: пользователь, группа пользователей, IP-адрес, диапазон IP-адресов, подсеть, список IP-адресов 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.

- Также можно дополнительно указать **Время действия** правила.

Диагностика:

Если правила контентной фильтрации не действуют, проверьте следующие параметры в настройках:

1. IP-адрес компьютера пользователя должен соответствовать его адресу в авторизации (раздел **Мониторинг - Авторизованные пользователи**), пользователь должен находиться в нужной группе, на которую назначено правило.

2. IP-адрес пользователя и ресурса, к которому он обращается, не должен входить в исключения прокси-сервера.

3. Проверьте правильность категоризации ресурса, к которому обращаетесь, в поле **URL для категоризации** на вкладке **Правила**:

Для этого вставьте в поле ссылку на ресурс, который требуется категоризировать, и нажмите **Найти категории**. Категории, в которые входит URL, 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.

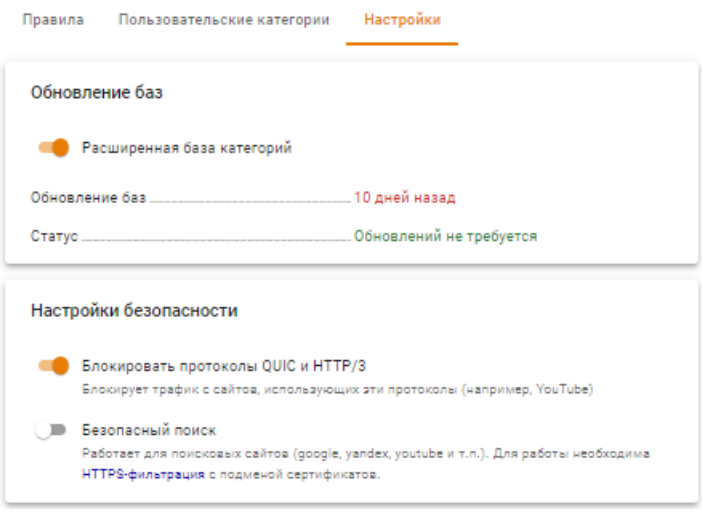
5. Проверить настройки контентной фильтрации по блокировке опасных и потенциально опасных файлов можно с помощью сервиса security.ideco.ru.

Блокировка загрузки файлов в файлообменники:

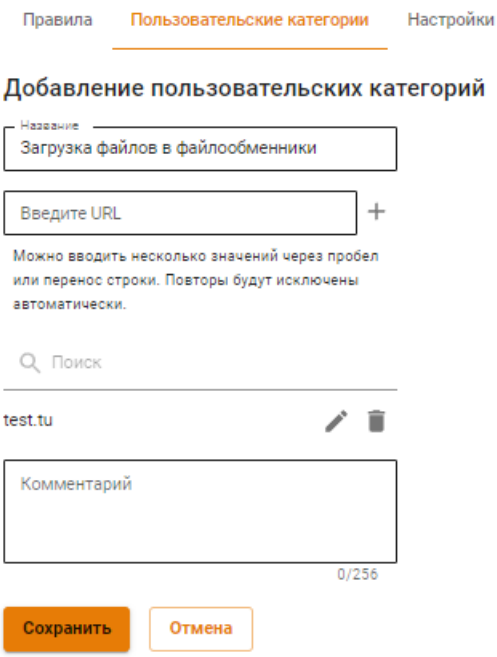
Блокирование этой категории требует особой настройки правил Контент-фильтра. В случае с файлообменниками (Google Drive, Яндекс.Диск, облако Mail.ru, Dropbox.com) расшифровки трафика категорий *Файлообменники*, *Файловые хранилища*, *Файловые архивы* и *Загрузка файлов в файлообменники* может быть недостаточно.

Чтобы заблокировать загрузку файлов в облака через браузер, выполните действия:

1. Включите **Блокировку протоколов Quic/HTTP3** на вкладке **Контент-фильтр -> Настройки**:

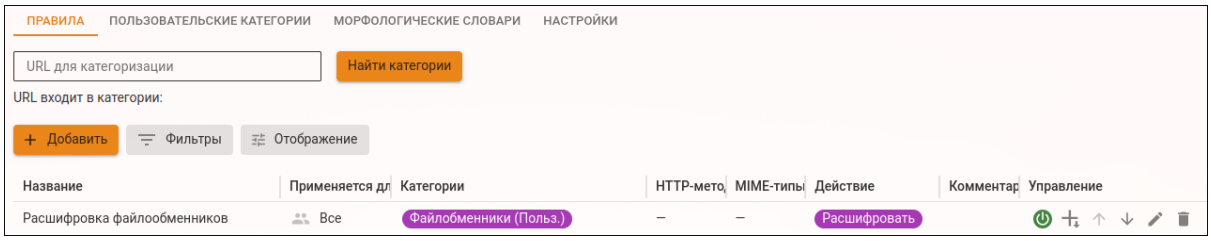


2. Создайте пользовательскую категорию для расшифровки трафика, указав домены нужных файлообменников:

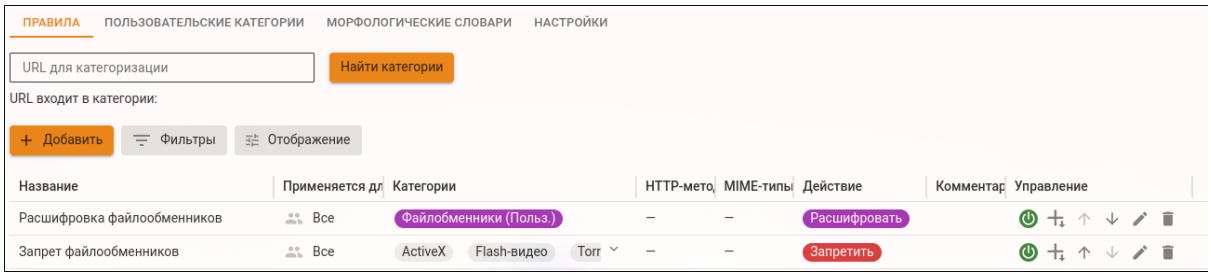


Для указания доменов используйте маски: `*.cloud.mail.ru`, `cloud.mail.ru/home`, `*.mail.ru`, `cloud.mail.ru`.

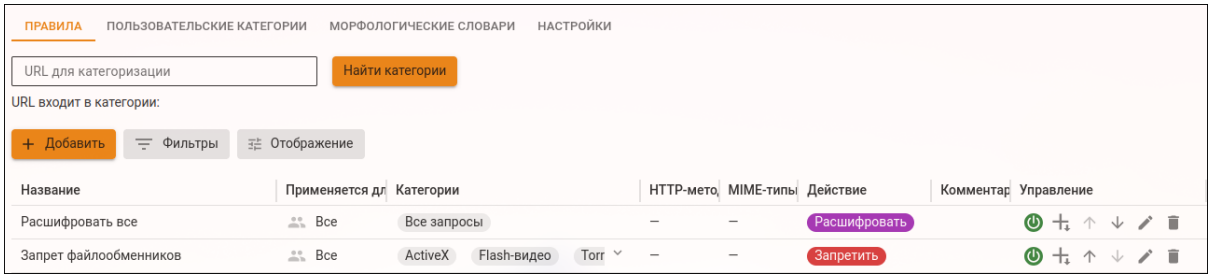
3. Создайте правило, расшифровывающее трафик созданной в п. 2 категории:



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:



16.3.5 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
Аборты	Веб-страницы, на которых обсуждаются аборты с медицинской, юридической, исторической и других точек зрения
Аборты — одобрение	Веб-сайты, одобряющие применение абортов
Аборты — осуждение	Веб-сайты, осуждающие применение абортов
Автомобили/Транспорт	Категория не содержит адресов и будет удалена в будущем
Активность в социальных сетях	Возможность писать/добавлять/загружать что-то в социальные сети
Алкоголь	Веб-сайты, призывающие к употреблению алкоголя (или оправдывающие его употребление), а также сайты, осуществляющие продажу алкогольной продукции, включая пиво, вина и т. д.
Анонимайзеры	Веб-сайты, предназначенные для обхода сетевых фильтров. Такие ресурсы могут быть использованы сотрудниками компании с целью посещения запрещенных сайтов
Архитектура	Веб-сайты, посвященные строительству, проектированию зданий и сооружений, архитектуре, а также организациям или услугам, связанным с дизайном, строительством и строительным проектированием
Астрология и гороскопы	Веб-сайты об астрологии, гороскопах, а также предсказаниях по звездам или знаку зодиака
Атеизм и агностицизм	Веб-сайты, ведущие антирелигиозную пропаганду или подвергающие сомнению религиозные, духовные, метафизические, или сверхъестественные воззрения
Аудио для прослушивания и скачивания	Сайты-хранилища, вещающие музыку или другой аудио контент (может потребить всю доступную ширину канала компании)
Аукционы и рынки	Веб-сайты, посвященные продажам товаров и услуг через объявления, онлайн-аукционы или через другие нетрадиционные каналы
Банки	Веб-сайты банков и иных кредитных учреждений, включая сайты интернет-банков. В эту категорию не входят сайты организаций, предлагающих брокерские услуги

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Безопасность	Сайты, относящиеся к продуктам и услугам, касающимся безопасности, за исключением компьютерной
Бизнес и услуги (общая)	Веб-сайты о бизнесе и услугах. В эту категорию включены ресурсы, которые не подлежат более точному категорированию, чем бизнес и услуги
Бизнес/Сервисы	Категория не содержит адресов и будет удалена в будущем
Биотехнологии	Веб-сайты, посвященные исследованиям в области генетики, а также сайты исследовательских институтов и организаций, работающих в сфере биотехнологий
Благотворительные учреждения	Сайты с информацией о благотворительных учреждениях и других некоммерческих филантропических организациях
Ботнеты	Категория не содержит адресов и будет удалена в будущем
Веб-почта	Службы, предоставляющие пользователям веб-доступ к почтовым ящикам. Как правило, речь идет о бесплатных ящиках
Веб-хостинг, интернет-провайдеры и телекоммуникационные компании	Сайты, предлагающие услуги веб-хостинга, блог-хостинга, интернет-провайдеры и телекоммуникационные компании
Взлом	Веб-сайты, содержащие информацию или утилиты, которые могут быть использованы для совершения онлайн-преступлений
Видео для прослушивания и скачивания	Сайты-хранилища, вещающие видео, в том числе в браузере (может потребить всю доступную ширину канала компании)
Виртуальные открытки	Сайты, позволяющие пользователям отправлять и принимать открытки
Возможный риск	Категория не содержит адресов и будет удалена в будущем
Войска и вооружения	Веб-сайты об оружии и силовых структурах
Вооруженные силы	Веб-сайты, спонсируемые вооруженными силами и иными государственными военными учреждениями
Высокий уровень риска	Категория не содержит адресов и будет удалена в будущем
Геи, лесбиянки и бисексуалы	Веб-сайты, на которых обсуждаются вопросы, связанные с нетрадиционной сексуальной ориентацией
Готовые домашние задания	Сайты с ответами к тестам, готовыми сочинениями, пошаговыми решениями задач и аналогичные ресурсы, которые могут использоваться для списывания
Для взрослых	Категория не содержит адресов и будет удалена в будущем
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Дома престарелых и уход за больными	Сайты о домах престарелых и тематические сообщества, включая уход за больными и хосписную помощь
Домашние животные	Сайты, содержащие информацию, продукты и услуги для домашних животных
Доставка и логистика	Сайты об управлении запасами, включая транспортировку, склад, дистрибуцию, хранение, выполнение и доставку заказов
Еда и рестораны	Сайты о еде: от ресторанов и кафе до рецептов и советов по готовке
Загрузка файлов в файлообменники	Загрузка файлов в файлообменники через браузер, например, в Google Drive, Яндекс.Диск, облако Mail.ru, Dropbox.com
Законодательство и политика	Сайты о законодательстве, политике, партиях, выборах, их результатах и мнениях
Запаркованные	Веб-сайты, которые используются в качестве «заглушек» для приобретенных, но не используемых доменных имен
Здоровье	Категория не содержит адресов и будет удалена в будущем
Здравоохранение и медицина	Веб-сайты, посвященные личному здоровью, медицинским услугам, медицинскому оборудованию, процедурам, психическому здоровью, больницам и клиникам
Знакомства	Веб-сайты, посвященные знакомствам, браку и т. д.
Игрушки	Сайты производителей игрушек, а также маркетинговые ресурсы и онлайн-магазины игрушек
Изображения жестокого обращения с детьми	Веб-сайты с изображениями физического или сексуального насилия над детьми
Интернет и IP-телефония	Веб-сайты, позволяющие совершать звонки через web или сайты программных продуктов, которые предназначены для совершения звонков через интернет
Интернет-магазины	Интернет-магазины и иные сайты, предлагающие совершить онлайн-покупки
Информационная безопасность	Веб-сайты организаций, предоставляющих услуги в сфере информационной безопасности
Искусство	Категория не содержит адресов и будет удалена в будущем
Казино, лотереи, тотализаторы	Сайты казино и прочих игровых систем
Каталоги	Веб-сайты с продуктовыми списками и каталогами без возможности совершить онлайн-покупку
Компьютерные игры	Веб-сайты, посвященные компьютерным играм, а также сайты с онлайн-играми
Компьютеры и технологии	Категория не содержит адресов и будет удалена в будущем
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Криминальные навыки	Веб-сайты, предоставляющие информацию о том, как совершить незаконную деятельность, такую как кража, убийство, создание бомбы, вскрытие замка и т. д.
Криминальные навыки/хакинг	Категория не содержит адресов и будет удалена в будущем
Купальные костюмы	Сайты, содержащие изображения людей в купальных костюмах. Изображения самих костюмов не попадают в эту категорию
Купоны	Веб-сайты, предлагающие приобретение скидочных купонов (купонаторы)
Литература и книги	Сайты, на которых представлена литература, включая беллетристику и документальные романы, стихи и биографии
Марихуана	Сайты, на которых представлена информация о марихуане, ее выращивании или курении, включая сайты, посвященные легальному использованию марихуаны, например, в медицине
Маркетинговые услуги	Сайты рекламных и маркетинговых агентств, кроме баннерных сетей
Мгновенные сообщения	Веб-сайты служб мгновенных сообщений, а также сайтов, призывающих поддерживать контакты с друзьями через сервисы обмена сообщениями
Мебель для дома и офиса	Веб-сайты, которые включают информацию о производителях мебели, розничных магазинах по продаже мебели, столов, стульев, кабинетов и т. д.
Мобильные телефоны	Сайты производителей мобильных телефонов, включая сайты, осуществляющие продажу мобильных телефонов и аксессуаров к ним
Мода и красота	Веб-сайты, посвященные моде и красоте, включая сайты, связанные с модой и содержащие информацию об одежде, ювелирных украшениях, косметике и парфюме
Музыка	Веб-сайты, посвященные музыке. Интернет-радио, файлы в формате mp3, информация о музыкальных группах, клипы и т. д.
Мультфильмы, аниме и комиксы	Веб-сайты, на которых размещены мультипликационные ТВ-шоу, фильмы, комиксы
Наркотики	Веб-сайты, призывающие к употреблению наркотических веществ, включая неправильное употребление лекарственных препаратов
Насилие	Веб-сайты, содержащие призывы к сомнительным действиям, таким как насилие и агрессия
Не для детского просмотра	Материалы, неуместные для детей: безвкусные, жестокие (в том числе, по отношению к животным), туалетный юмор и т. п.
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Некоммерческие организации	Категория не содержит адресов и будет удалена в будущем
Нераспознаваемый контент	Сайты с нераспознаваемым контентом, что не позволяет их категоризировать
Нетрадиционные религии и оккультные верования	Сайты, посвященные религиям, не находящимся в мейнстриме или не входящим в ТОП-10 мировых религий (народные религии, мистика, культы и секты)
Новости	Новостные веб-ресурсы. Сайты газет, журналов, новостные ленты
Обзоры продукции и сравнение цен	Сайты, призванные помочь покупателям сравнить магазины, продукты и цены, но не торгующие онлайн
Оборудование, ПО, электроника	Сайты о компьютерном оборудовании, ПО, периферии, сетях данных, электронике, а также ресурсы производителей соответствующих товаров и услуг
Образование и учебные учреждения	Сайты и ресурсы сообществ, создающих информационные документы, доступные на редактирование всем участникам
Онлайн-офисы	Сайты брокерских компаний, осуществляющих онлайн-торговлю ценными бумагами и т. д.
Онлайн-реклама и баннеры	Веб-страницы, строго посвященные рекламе, баннерам или выскакивающим окнам с рекламой
Онлайн-торговля акциями	Сайты фондовых рынков
Онлайн-управление информацией	Сайты, посвященные программам для управления личной информацией, например, приложения для управления со списками задач, календарями, адресные книги и т. д.
Откровенные изображения	Сайты с фотографиями и видеороликами, на которых изображены девушки в сексуальной провокационной одежде, например, в дамском белье
Парки, зоны отдыха и спортивные залы	Сайты, посвященные паркам и иным зонам, предназначенным для оздоровительных активностей, таких как плавание, скейтбординг, альпинизм и т. д.
Переадресация	Сайты, перенаправляющие посетителя на другие ресурсы
Переводчики	Словари и переводчики с иностранных языков
Персональные страницы	Категория не содержит адресов и будет удалена в будущем
Персональные страницы и блоги	Персональные страницы, включая блоги и другие средства обмена новостями, мнениями и информацией об авторе, а также домашние и семейные страницы
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Плата за серфинг	Сайты компаний, предлагающих оплату за просмотр рекламы в их специализированных приложениях
Платные сайты мобильных операторов	Сайты сотовых операторов, за доступ к которым взимается отдельная плата с абонента
Поиск работы	Веб-сайты, посвященные поиску работы, включая рекрутинговые агентства
Поисковики изображений	Сайты и поисковые машины, используемые для поиска изображений и возвращающие результаты, содержащие миниатюры последних
Поисковые системы	Поисковые системы, осуществляющие поиск по веб-сайтам, новостным группам, картинкам и другому контенту
Политика и закон	Категория не содержит адресов и будет удалена в будущем
Порнография	Сайты, содержащие изображения или видео с откровенной демонстрацией полового акта или обнаженного тела
Порнография/секс	Категория не содержит адресов и будет удалена в будущем
Порталы	Веб-ресурсы, предоставляющие доступ к настраиваемым персональным порталам, включая «желтые страницы» и другие каталоги
Правительство	Категория не содержит адресов и будет удалена в будущем
Природа и ее сохранение	Веб-сайты с информацией об окружающей среде, экологии и т. д.
Производство	Сайты, посвященные бизнесу, связанному с промышленным производством
Профессиональные сообщества	Сайты социальных сетей, ориентированных на профессионалов и выстраивание деловых отношений
Развлекательные места и события	Веб-сайты, посвященные культурным заведениям, таким как театры, кинотеатры, ночные клубы, фестивали и т. д.
Развлекательные новости и сайты про знаменитостей	Веб-сайты, посвященные новостям о знаменитостях, телешоу, фильмах и шоу-бизнесе в целом
Развлечения и видео	Категория не содержит адресов и будет удалена в будущем
Разное	Веб-сайты, которые не могут быть однозначно отнесены ни к одной из категорий
Религии	Сайты об основных мировых религиях, а также общерелигиозной тематики и теологические
Религия	Категория не содержит адресов и будет удалена в будущем
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.)

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
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.
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.)

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
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
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

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Категория	Описание
Финансы (в целом)	Веб-сайты, на страницах которых обсуждаются экономические вопросы, инвестиционные стратегии, пенсионное и налоговое планирование
Фитнес и отдых	Веб-сайты, посвященные фитнесу и другим оздоровительным активностям
Фишинг/мошенничество	Веб-сайты, используемые для мошенничества, также известны как фишинговые. Как правило, представляются официальными веб-страницами финансовых или иных учреждений с целью несанкционированного доступа к конфиденциальной информации, например, пин-кодам банковских карт
Форумы	Сайты форумов, новостных групп, архивы списков рассылки, доски объявлений и аналогичные ресурсы сообществ
Фотогалереи	Сайты с архивами фотографий, фотостоки
Хобби и Досуг	Веб-сайты, содержащие информацию о различных ремеслах и хобби, таких как вышивание, коллекционирование, авиамоделирование и т. д.
Центры распространения вредоносного ПО	Сайты, на которых размещены вирусы, эксплоиты и другое вредоносное ПО
Центры управления и контроля	Интернет-серверы, использующиеся для управления ботнетами
Частные IP-адреса	Сайты, обслуживаемые на частных IP-адресах, зарезервированных для использования внутри организаций и дома
Чаты	Онлайн-чаты
Чаты/Мессенджеры	Категория не содержит адресов и будет удалена в будущем
Шпионские и опасные сайты	Категория не содержит адресов и будет удалена в будущем
Шпионское и сомнительное ПО	Сайты с ПО, пересылающим информацию на центральный сервер, включая шпионское ПО и клавиатурные шпионы
Экстремизм	Веб-сайты, призывающие к экстремизму, дискриминации по половому, расовому, религиозному и другим признакам
Эротика	Веб-сайты, содержащие материалы эротического характера (частичное или полное обнажение), исключая порнографические материалы
Юмор	Веб-сайты, содержащие информацию юмористического характера, такую как комиксы, шутки, смешные картинки

16.3.6 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).

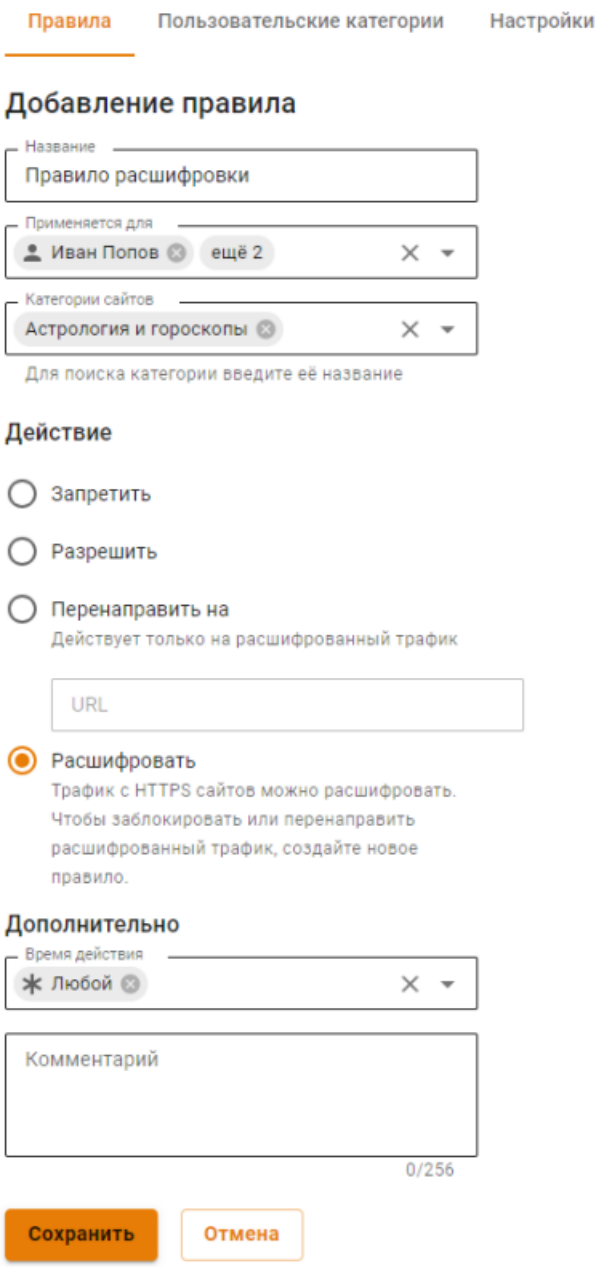
Подсказка: Специфика фильтрации HTTPS-трафика с подменой сертификата требует настройки обеих сторон подключения: сервера Ideco NGFW и рабочей станции каждого пользователя в локальной сети.

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**.

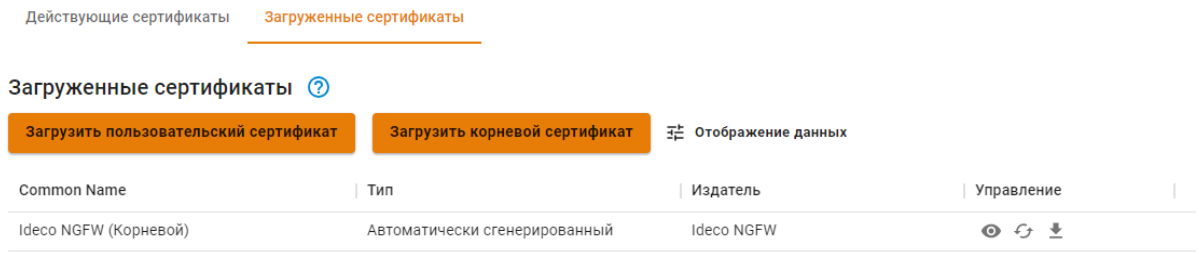
Пример правила для расшифровки:



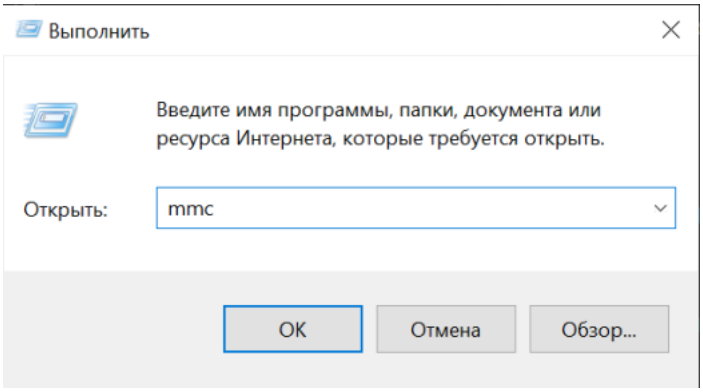
Настройка рабочей станции пользователя

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**:

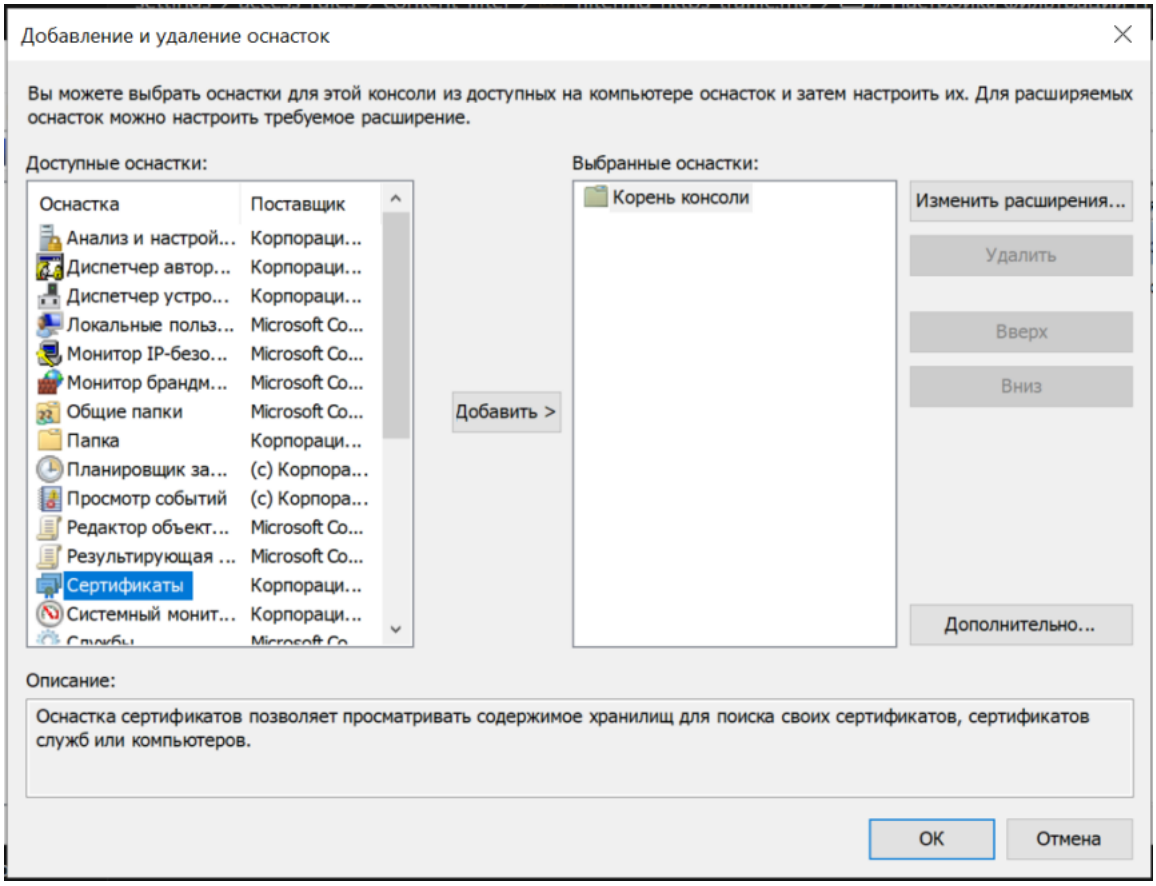


2. Откройте на рабочей станции центр управления сертификатами: **Пуск -> Выполнить**, выполнив в диалоге команду **mmc**:

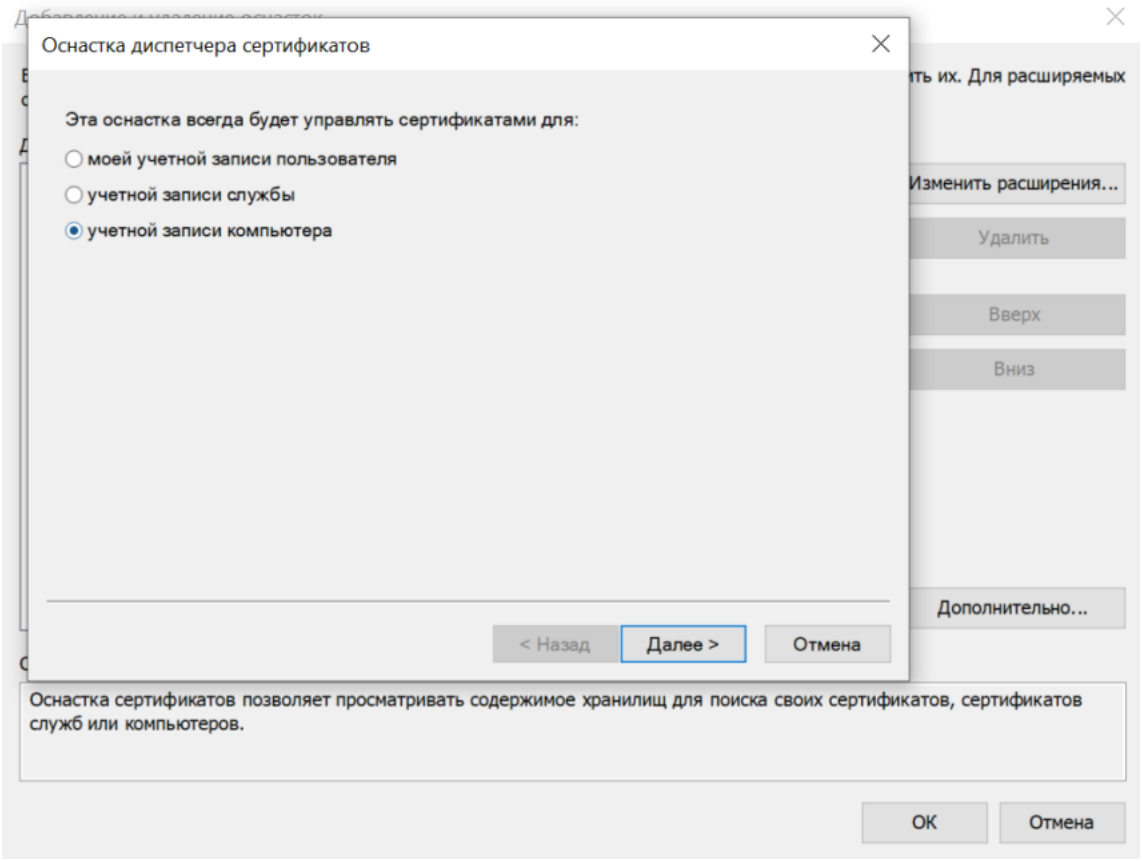


3. В меню **Файл** выберите **Добавить или удалить оснастку**:

4. В списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите кнопку **Добавить**:

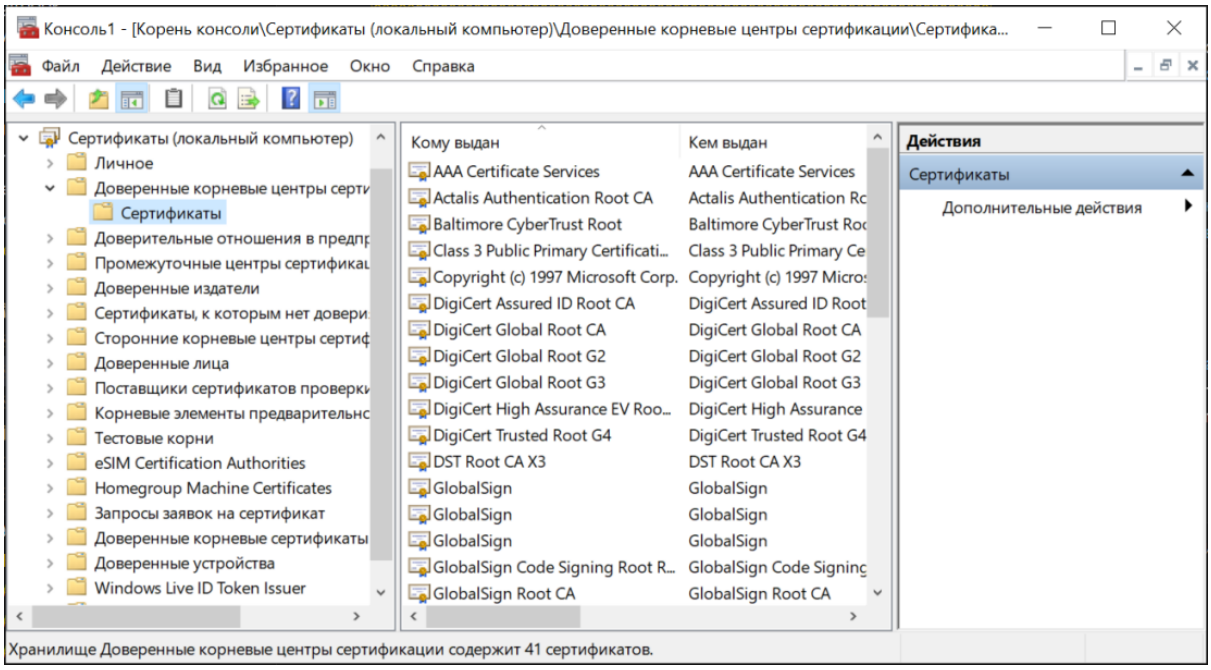


5. В открывшемся окне выберите пункт **Учетная запись компьютера** и нажмите кнопку **Далее**:



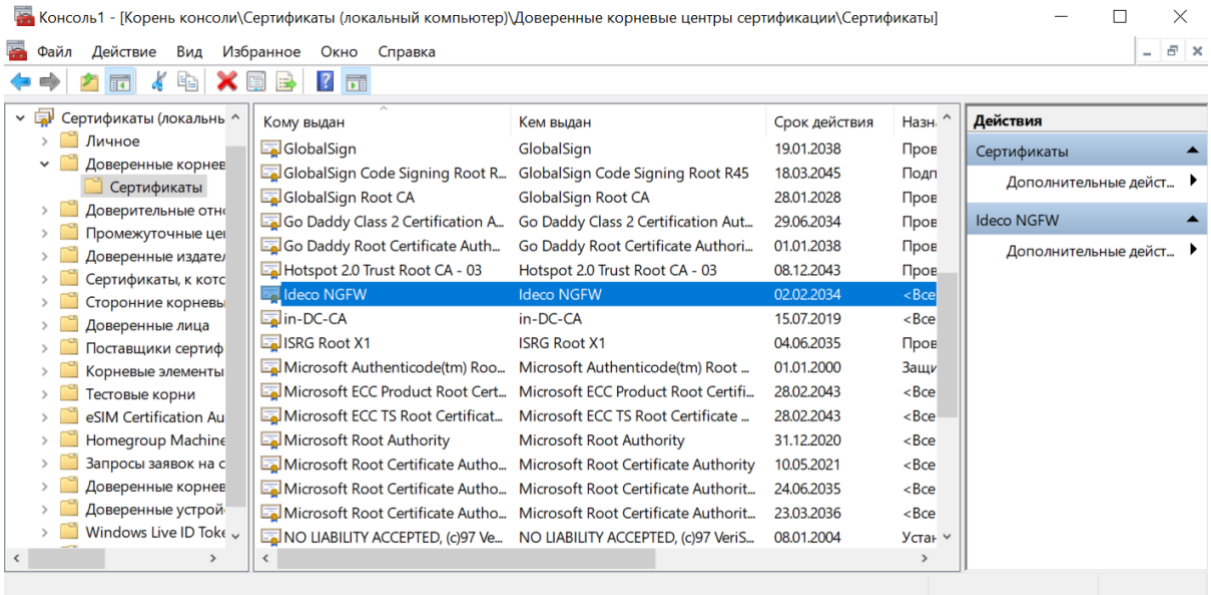
6. В окне **Выбор компьютера** оставьте флаг **Локальный компьютер** и нажмите кнопку **Готово**.

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**:

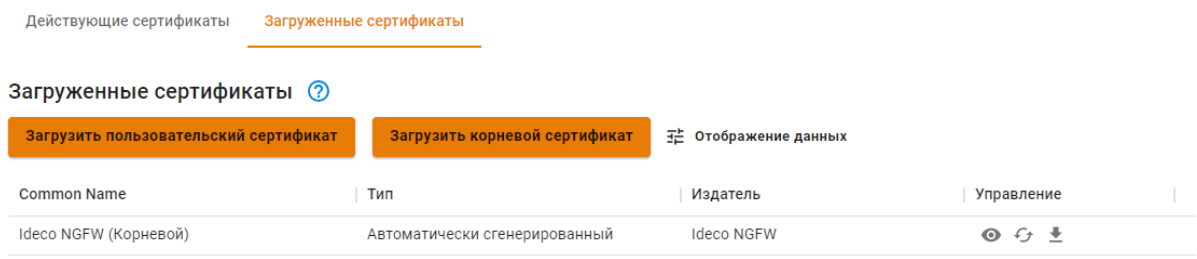
9. Следуя инструкциям Мастера импорта сертификатов, импортируйте корневой сертификат сервера Ideco NGFW. Импортированный сертификат появится в списке в правой части окна:



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**:



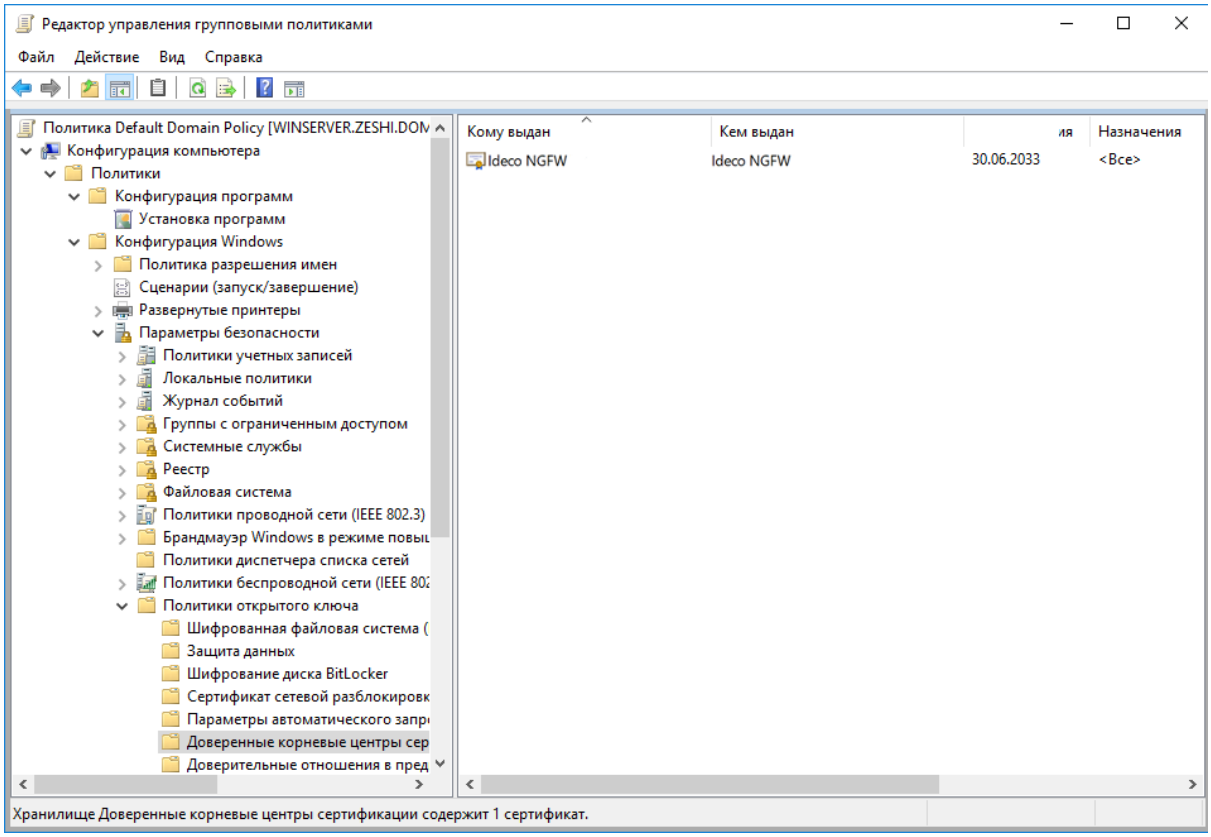
2. Зайдите на контроллер домена с правами администратора.

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.

16.4 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 **Ограничения скорости** не обрабатывают трафик между локальными сетями и сетями филиалов.

Для исключения пользователя или групп пользователей из обработки правил *Предотвращения вторжений*, *Контроля приложений* и **Ограничения скорости**, добавьте соответствующее правило в **Правила трафика -> Исключения**.

16.4.1 Настройка ограничения скорости

Для создания правила, необходимо перейти в раздел **Правила трафика -> Ограничение скорости** и нажать кнопку **Добавить**.

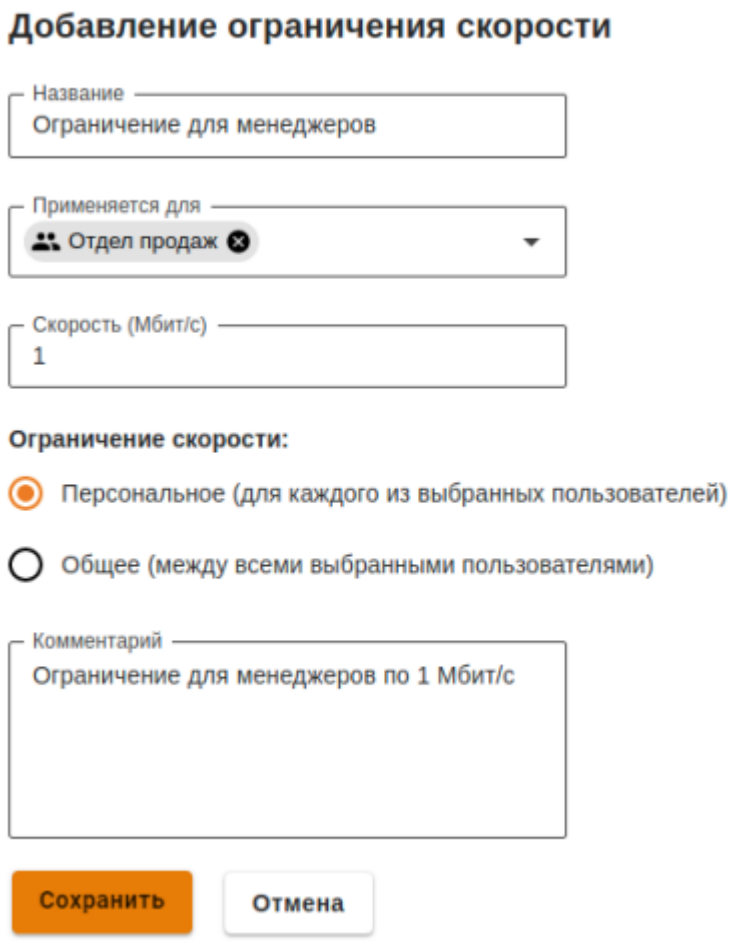
Далее заполните следующие поля:

- **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.

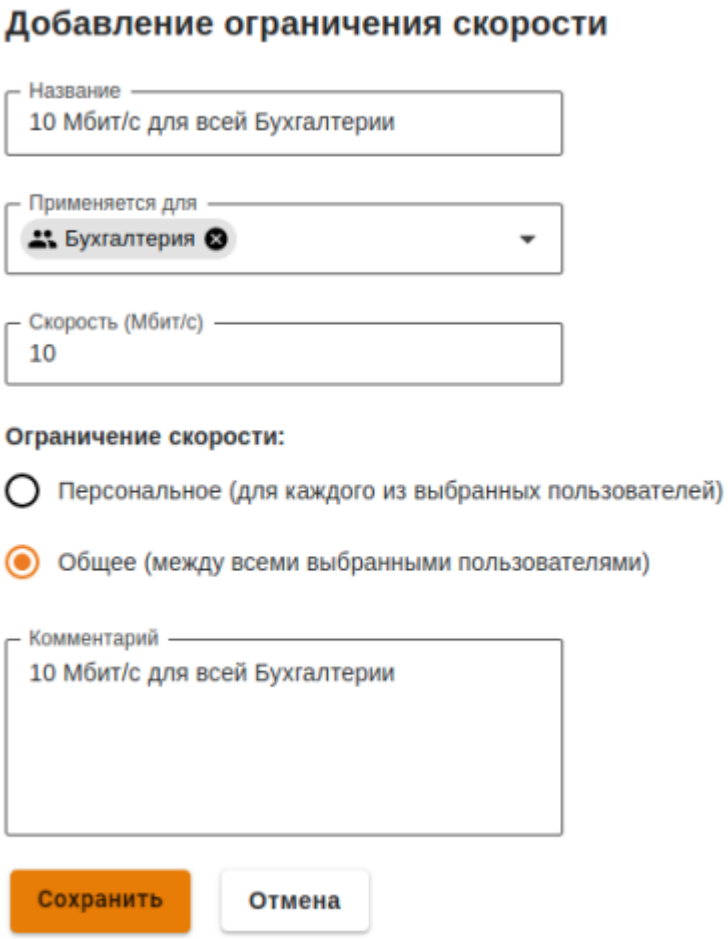
Для удобства настройки существует два типа ограничения скорости. Они могут быть применены для пользователей, групп, IP-адресов и объекта **Превышена квота** (в этот объект попадают пользователи, которые превысили квоту по трафику).

- **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.

Чтобы модуль работал, переведите ползунок в верхней части экрана около надписи **Ограничение скорости** в положение **Включен**.

Подсказка: Если не нажать кнопку **Применить** сверху над списком правил и покинуть раздел **Ограничение скорости**, то созданное правило сохранится, но не будет применяться. Для применения правила вернитесь в раздел **Ограничение скорости** и нажмите кнопку **Применить**.

Также сохраненные, но не примененные правила потеряются в 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**:

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

16.4.2 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.

16.4.3 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.

16.5 Антивирусы веб-трафика

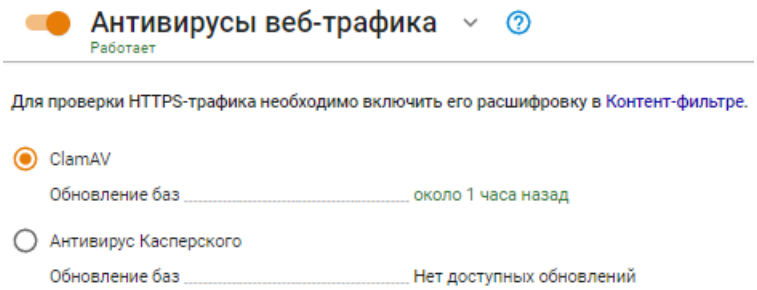
16.5.1 Основное

Подсказка: Название службы раздела *Антивирусы веб-трафика*: `ideco-av-backend`.
Список имен служб для других разделов доступен по *ссылке*.

Внимание: Начиная с 18 версии Ideco NGFW, антивирус ClamAV будет удален из продукта. Рекомендуем заранее перейти на антивирус Касперского.

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).



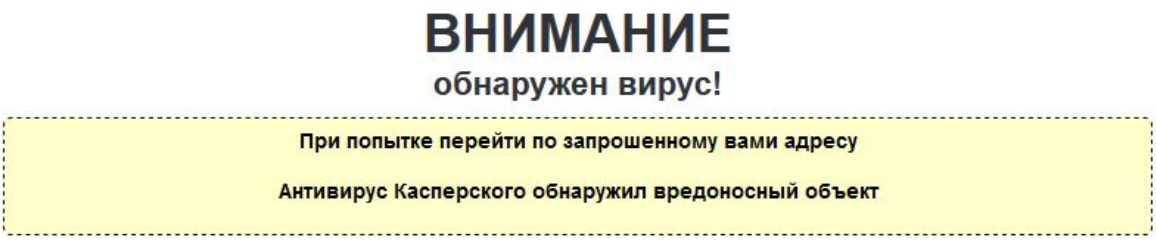
Модуль антивируса связан с прокси-сервером и контент-фильтром, поэтому фильтрует веб-трафик при выполнении следующих условий:

- 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
```

16.6 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:

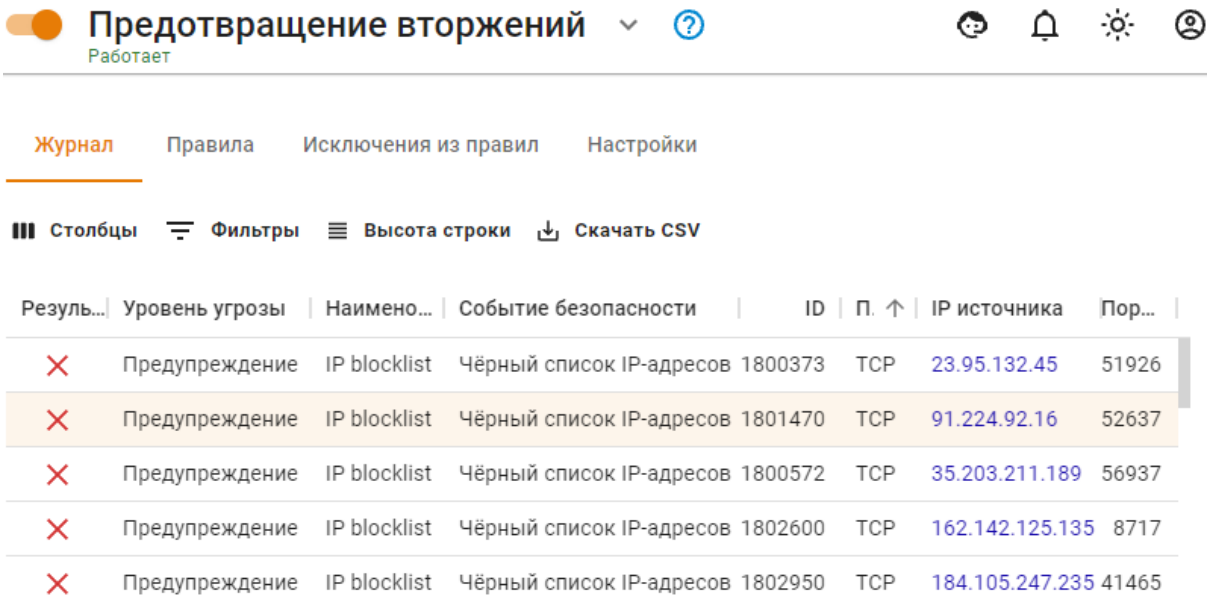
- *Журнал* - фиксирует логи срабатывания правил службы;
- *Правила* - содержит список предустановленных правил;
- *Исключения из правил* - фиксирует в таблицу список отключенных правил службы предотвращения вторжений;
- *Настройки* - на вкладке создаются правила для службы предотвращения вторжений.

На вкладках **Журнал**, **Правила** и **Исключения из правил** доступна фильтрация правил с помощью кнопки **Фильтры**.

16.6.1 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.

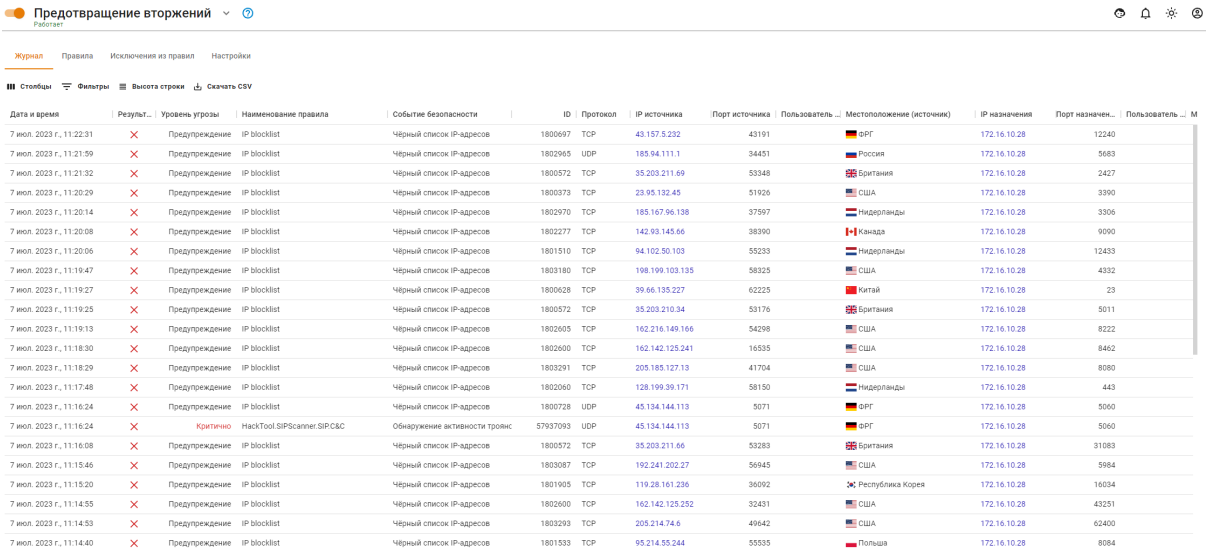
После включения системы проконтролируйте, что мощности вашего процессора достаточно для проверки трафика, следующего через шлюз.
В разделе **Мониторинг -> Графики загруженности** выберите параметр средняя загрузка (за 1, 5 и 15 минут).

Подробнее о Load Average.

16.6.2 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:

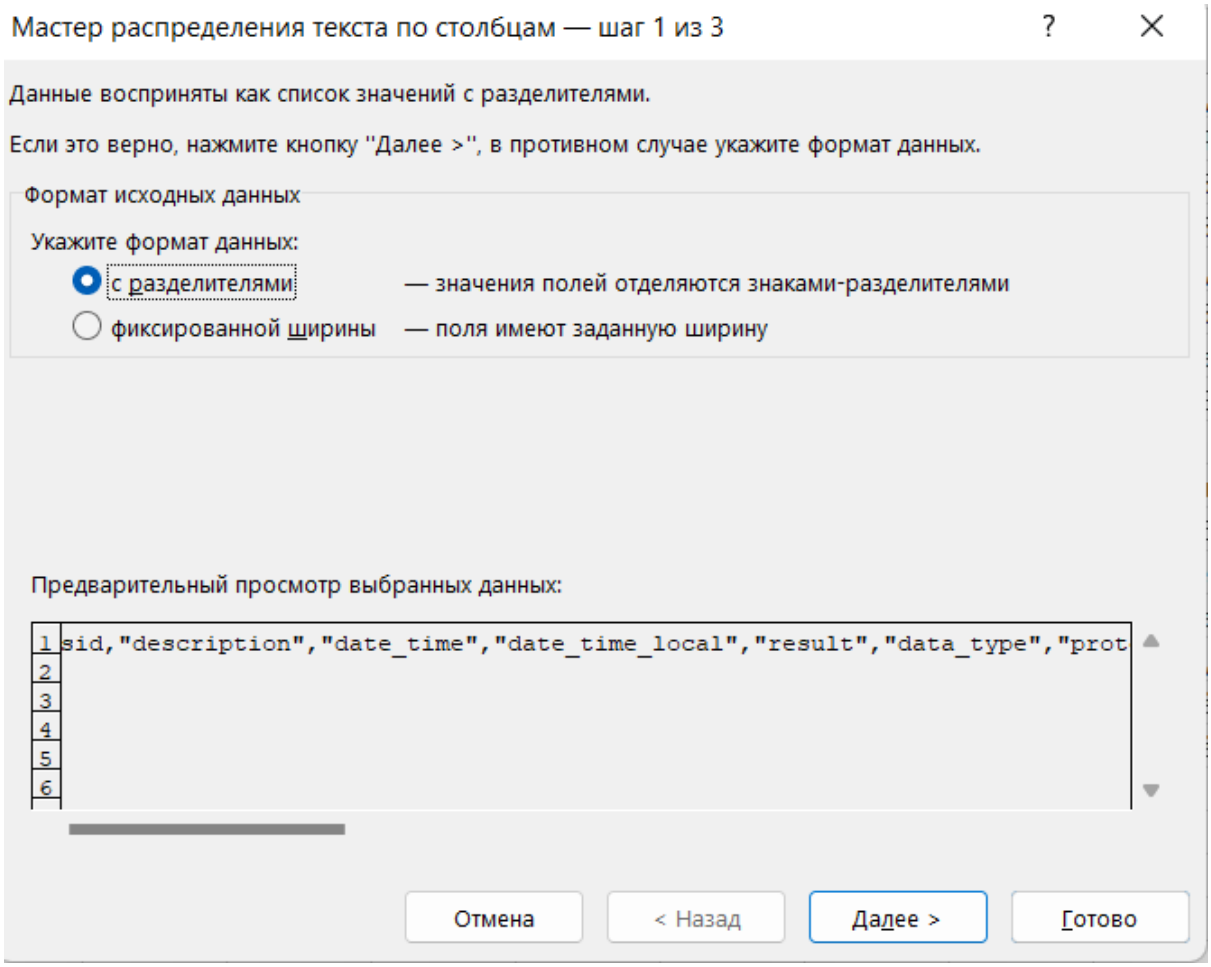
Скачайте CSV-файл с логами службы предотвращения вторжений за определенный период по соответствующей кнопке.

Для корректного отображения информации из CSV-файла в MS Excel повторите действия:

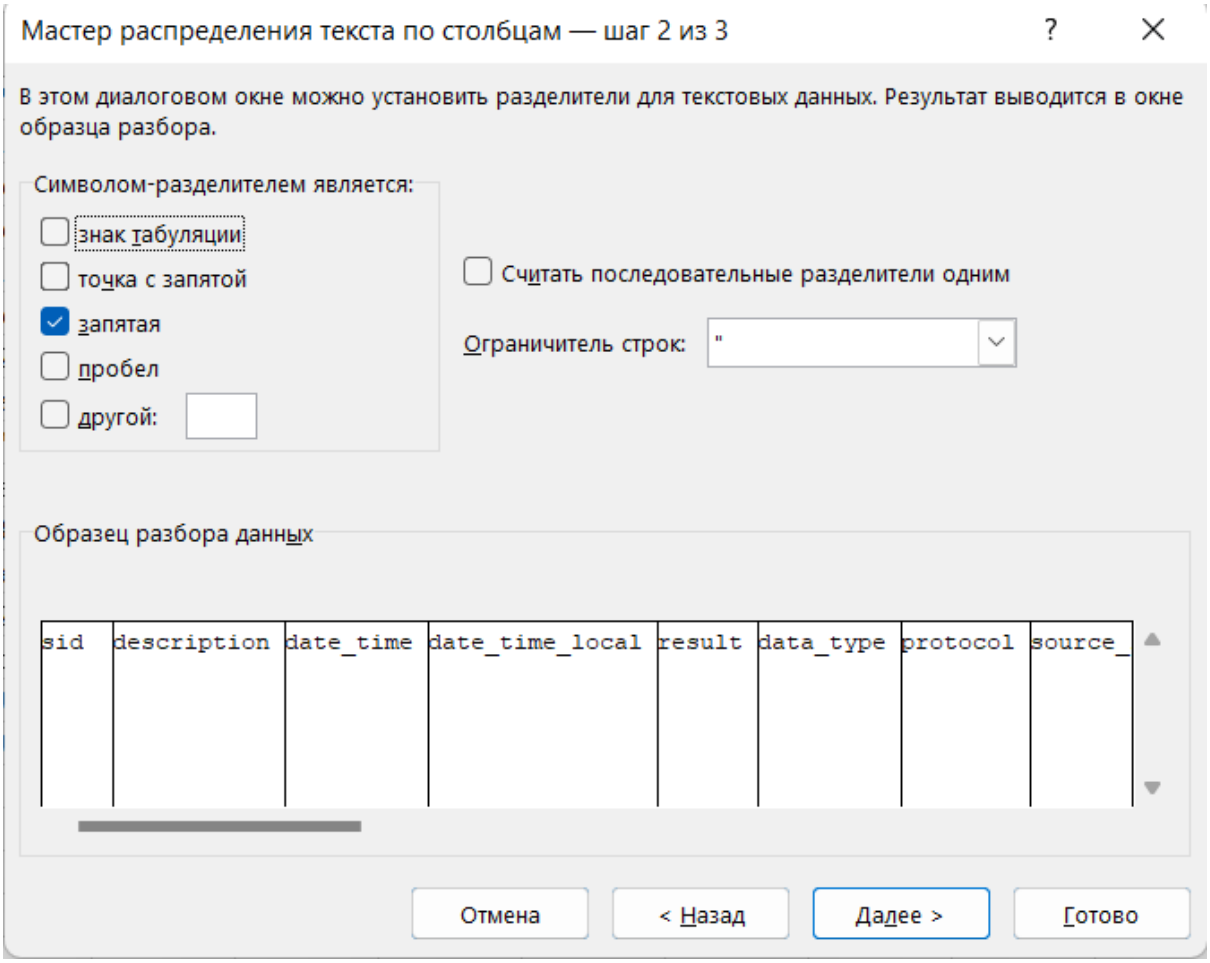
1. Откройте CSV-файл в MS Excel и выделите весь первый столбец.

2. Перейдите во вкладку **Данные** и нажмите кнопку **Текст по столбцам**.

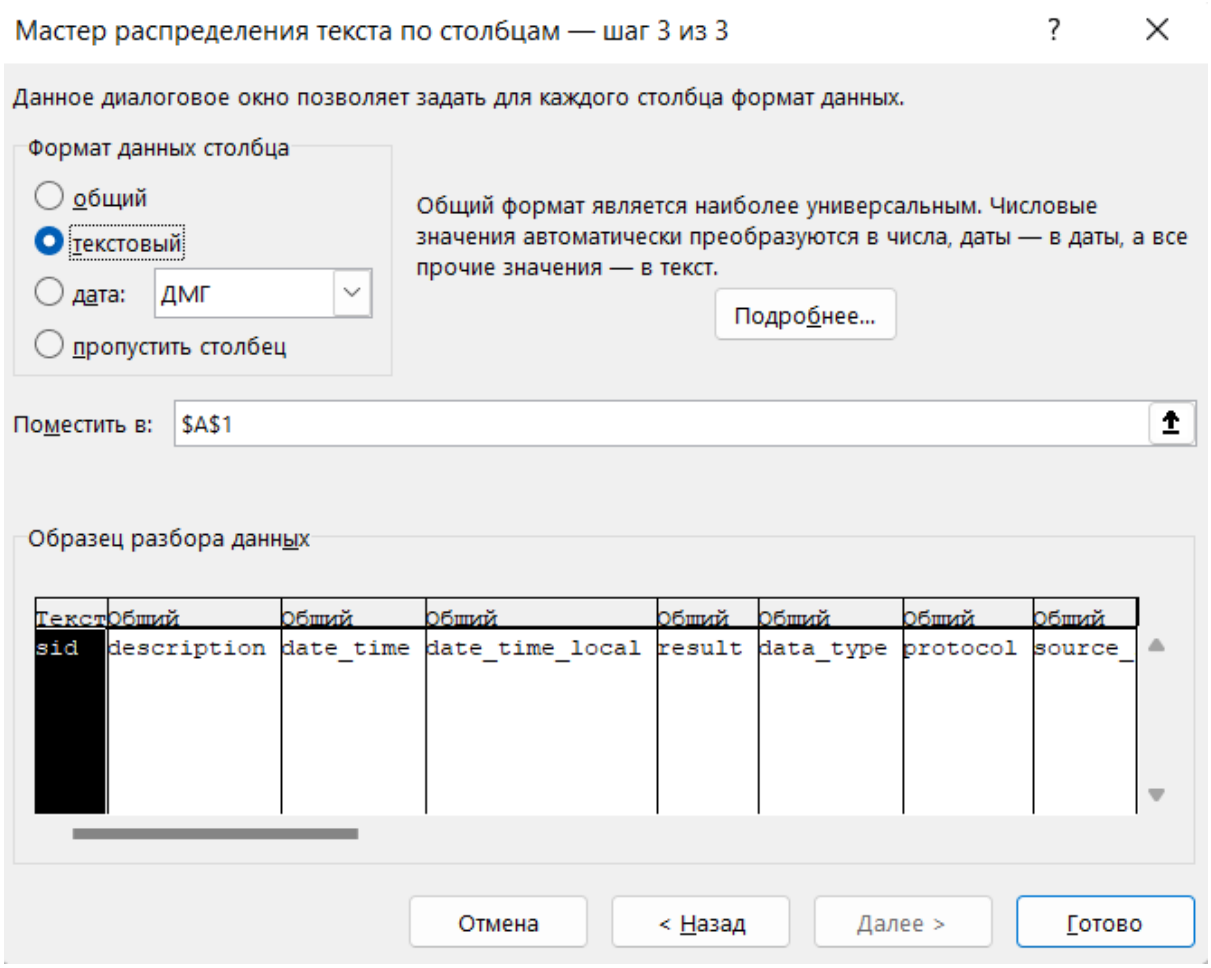
3. В открывшемся окне выберите **с разделителями** и нажмите **Далее**:



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



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



16.6.3 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:

- **DNS поверх HTTPS** - обнаруживает/блокирует попытки сокрытия DNS-запросов по седьмому уровню TLS/SSL;
- **GeoIP Страны Восточной Европы** - обнаруживает/блокирует попытки доступа к IP-адресам, основываясь на базе данных MaxMind's GeoIP databases;
- **SSL-сертификаты, используемые вредоносным ПО и ботнетами** - обнаруживает/блокирует связь с командными центрами злоумышленников (C2);
- **Авторизация с подозрительным логином**;
- **Анонимайзеры** - обнаруживает/блокирует анонимайзеры;
- **Атаки на получение прав пользователя** - обнаруживает/блокирует попытки получить учетные данные пользователя;
- **Атаки на получение привилегий администратора** - обнаруживает/блокирует попытки получить привилегии администратора;
- **Блокирование активности троянских программ** - обнаруживает/блокирует вредоносные трояны;

- **Блокирование атак** - обнаруживает/блокирует подозрительные IP-адреса (IP Reputation);
- **Блокирование крупных утечек информации** - обнаруживает/блокирует попытки получить данные и информацию;
- **Блокирование некорректных попыток получения привилегий пользователя** - обнаруживает/блокирует попытки получить привилегии пользователя;
- **Блокирование подозрительных RPC-запросов** - обнаруживает/блокирует удаленный вызов процедур (обычно используется для вызова удаленных функций на сервере, требующих результата действия);
- **Блокирование попыток запуска исполняемого кода** - обнаруживает/блокирует Remote Code Execution (RCE);
- **Блокирование утечек информации** - обнаруживает/блокирует попытки получить данные и информацию;
- **Запросы на скомпрометированные ресурсы** - обнаруживает/блокирует связи с командными центрами злоумышленников (C2);
- **Использование DNS-трафика для управления вредоносным ПО** - обнаруживает/блокирует связь с инфраструктурой управления и контроля (C2);
- **Нежелательное программное обеспечение** - обнаруживает/блокирует вредоносное ПО;
- **Неизвестный тип трафика** - обнаруживает/блокирует неопознанный/вредоносный трафик;
- **Нецелевое использование стандартных портов** - обнаруживает/блокирует использование стандартных портов в нелегитимных целях;
- **Обнаружение нарушений стандартов сетевых протоколов** - обнаруживает/блокирует обращения по нестандартным/прошитым протоколам;
- **Обнаружение подозрительной сетевой активности** - обнаруживает/блокирует аномалии или нестандартные действия легитимных пользователей в сети;
- **Обнаружение подозрительных команд** - обнаруживает/блокирует нестандартные команды, не характерные системам;
- **Обнаружение успешных краж учетных данных** - обнаруживает/блокирует кражи учетных данных;
- **Определение внешнего IP-адреса** - обнаруживает/блокирует попытки взаимодействия с инфраструктурой из внешних сетей;
- **Ошибки в сетевых протоколах** - обнаруживает/блокирует ошибки сетевых протоколов;
- **Подозрительное обращение к файлам** - обнаруживает/блокирует нестандартное обращение к файлам системы;
- **Попытки авторизации с логином и паролем по-умолчанию** - обнаруживает/блокирует попытки зайти под учетными данными с простыми паролями (аналогично Bruteforce);
- **Попытки использования социальной инженерии** - обнаруживает/блокирует «атаку на человека»;
- **Попытки получения привилегий администратора** - обнаруживает/блокирует попытки повысить привилегии до администратора и получить учетные данные администратора;
- **Попытки получения привилегий пользователя** - обнаруживает/блокирует попытки повысить привилегии и получить учетные данные пользователей;
- **Попытки получения системных файлов** - обнаруживает/блокирует системные конфигурации;
- **Попытки проведения DoS-атак** - обнаруживает/блокирует попытки провести атаки типа «отказ в обслуживании» (denial-of-service attack);
- **Попытки сканирования сети** - обнаруживает/блокирует сканирование сети;
- **Потенциально опасный трафик** - обнаруживает/блокирует зашифрованный или запутанный трафик, нестандартные запросы;

- **Пулы криптомайнеров** - обнаруживает/блокирует взаимодействие с сетями криптомайнеров и обращения для передачи нагрузки, которые криптомайнеры используют для майнинга;
- **Расширенная база правил (от Лаборатории Касперского)** - набор правил по обнаружению/блокировке от Лаборатории Касперского;
- **Телеметрия Windows** - обнаруживает/блокирует Телеметрию Windows;
- **Трафик устаревшего уязвимого ПО** - обнаруживает/блокирует связи с командными центрами злоумышленников (C2);
- **Управление вредоносным ПО** - обнаруживает/блокирует связь с инфраструктурой управления и контроля (C2), которую злоумышленники используют для управления зараженными устройствами и кражи конфиденциальных данных;
- **Целевое использование вредоносного ПО** - обнаруживает/блокирует вредоносное программное обеспечение;
- **Черный список IP-адресов** - обнаруживает/блокирует трафик к IP-адресам из баз safe-surf.ru и cinsarmy.com;
- **Эксплойты** - обнаруживает/блокирует использование уязвимостей систем (с идентификатором CVE-XXXX-XXXXX).

История изменений правил:

31.01.2024

- Улучшена блокировка Hola VPN и Browsec VPN.

14.12.2023

- Оптимизированы правила блокировки анонимайзеров.

11.12.2023

- Удалена категория «Попытки выполнить системный вызов» из IPS.

07.12.2023

- Добавлены новые правила для Windows Telemetry;
- Не блокируется VPN-Browsec (добавлены новые правила для блокировки VPN-Browsec);
- Удалена категория Защита SMTP;
- Телеметрия Windows блокирует Skype (убраны 2 правила телеметрии, которые блокировали функции Skype).

23.11.2023

- Ошибка в формировании правил пула криптомайнеров (исправлена ошибка правил, блокирующая легитимные ресурсы по типу www.fr).

31.10.2023

- Удалено правило «ET EXPLOIT Cisco IOS XE Web Server Possible Authentication Bypass Attempt (CVE-2023-20198) (Outbound)» из-за 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

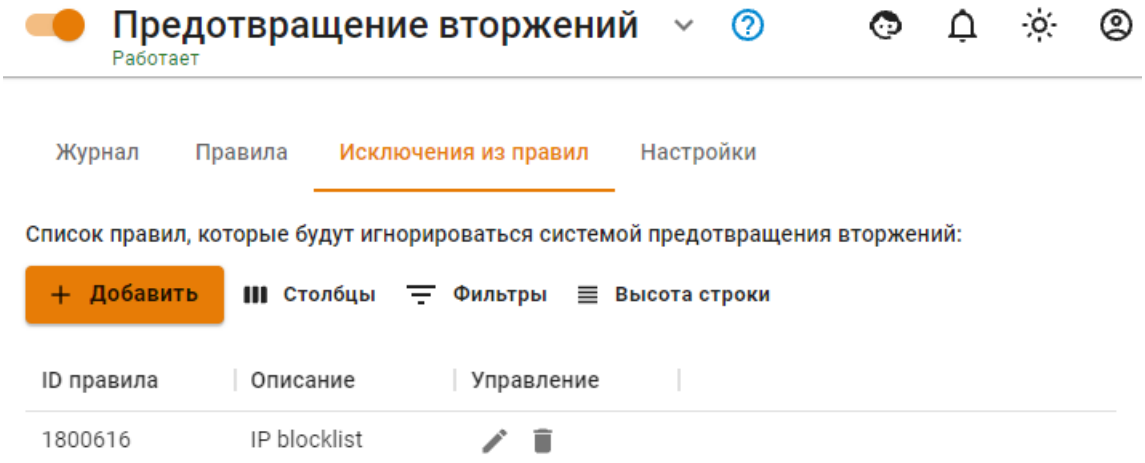
- Удалена группа **Активные ботнеты**. Актуальные угрозы блокируются с помощью «Черных списков IP-адресов».

16.6.4 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.

16.6.5 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).

При наличии большого количества подсетей в таблице воспользуйтесь кнопкой **Фильтры**.

Предупреждение: **Не указывайте** сети, принадлежащие внешним сетевым интерфейсам NGFW и внешним сетям. Указанные здесь сети участвуют в правилах службы предотвращения вторжения как локальные. Локальный межсегментный трафик не исключается из проверок системы.

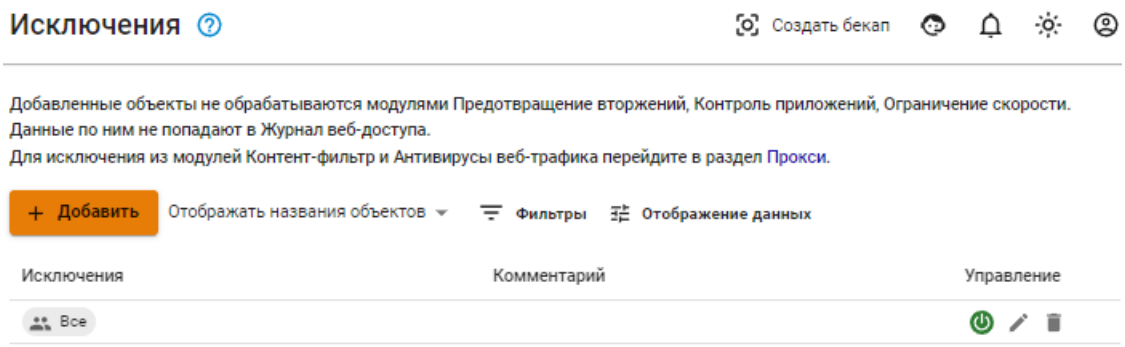
Предупреждение: При работе службы предотвращения вторжений **не используйте** сторонние DNS-серверы для компьютеров, т.к служба определяет зараженные устройства по DNS-запросам, проходящим через нее.
При использовании внутреннего домена AD рекомендуется:

- В компьютерах указать DNS-сервер Ideco NGFW в качестве единственного DNS-сервера;
- В настройках DNS-сервера на NGFW указать Forward-зону для локального домена.

16.7 Исключения

16.7.1 Основное

Правила в разделе **Исключения** отключают трафик из обработки *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 .

При наличии большого количества исключений в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Если в качестве DNS-сервера у пользователя указан локальный адрес сервера Ideco NGFW, то исключения работать не будут. Весь трафик, идущий на адреса локальных и VPN-интерфейсов Ideco NGFW, всегда обрабатывается службой фильтрации трафика.

16.8 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;

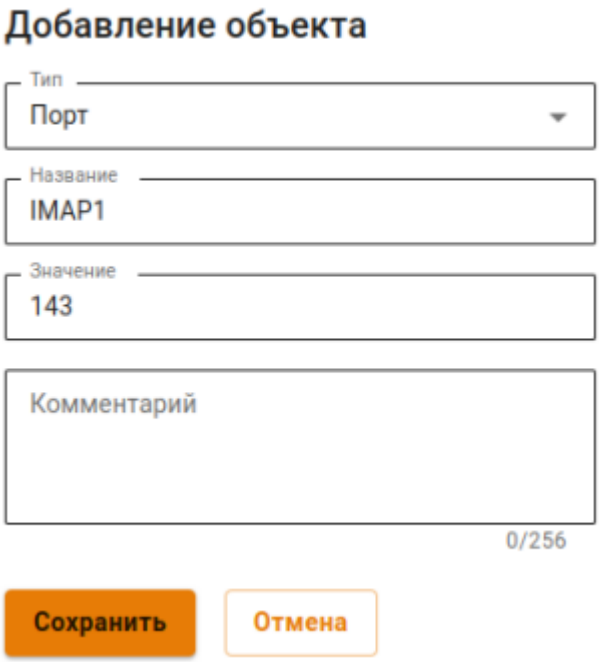
- **Диапазон IP-адресов** - диапазон IP-адресов от первого до последнего, указанного в диапазоне. Пример: 10.0.0.1-10.0.0.25;
- **Подсеть** - логический блок IP-адресации. Префикс маршрутизации выражается в нотации CIDR. Пример: 10.0.0.0/24;
- **Домен** - символьное имя, служащее для идентификации объектов 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.

16.8.1 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**.

При наличии большого количества объектов в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Важно:

- Для создания групп объектов предварительно необходимо создать сами объекты. К группам объектов относятся: список IP-адресов, порты и расписание.
- Для создания объекта типа **Список IP-адресов** используйте любой текстовый файл (например: TXT/CSV), в котором будут перечислены нужные IP-адреса. Правила заполнения:
  - в строке должен быть один адрес;
  - допускается использование маски /24 или 255.255.255.0.
- Для создания объекта типа **Зона** необходимо:
  - Создать соответствующий объект в разделе **Правила трафика -> Объекты**;
  - Перейти в раздел **Сервисы -> Сетевые интерфейсы** и при редактировании интерфейса добавить его в нужную зону.
- Зоны для IPsec-подключений создаются автоматически при создании соответствующих подключений.
- Объекты типа **IP-адрес** и **Порт** можно создавать непосредственно при создании правил файрвола, введя нужный IP-адрес или порт в соответствующих полях.

Подсказка: В Ideco NGFW также испольуется 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.

16.9 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).

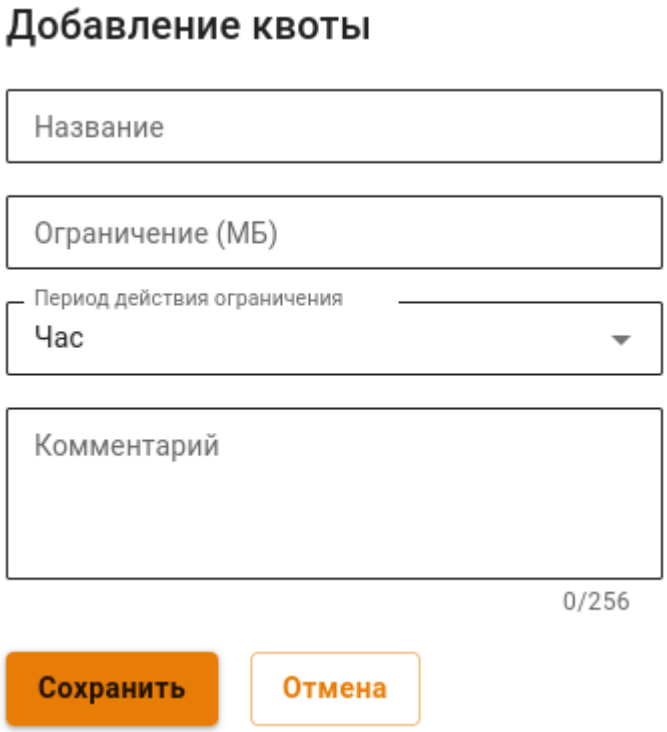
16.9.1 Настройка квоты

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**.

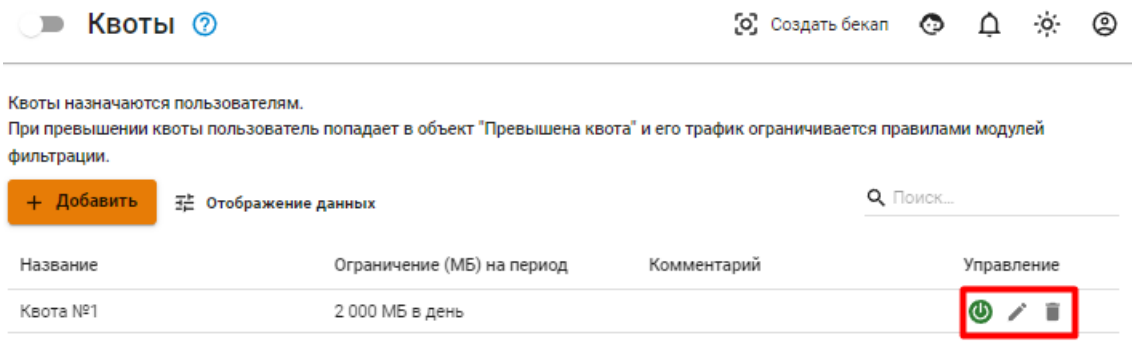
2. В форме добавления квоты заполните обязательные поля:



- **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:



16.9.2 Настройка пользователя и группы

Настройка группы:

Созданные квоты можно применить для групп пользователей на вкладке **Квота**.

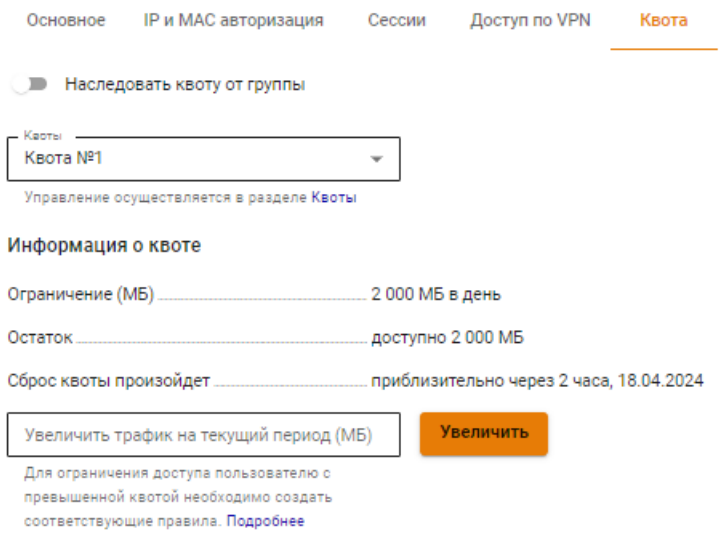
Можно наследовать квоту от вышестоящей группы или выбрать другую квоту, для этого потребуется деактивировать опцию **Наследовать квоту от группы** и выбрать нужную квоту:

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:

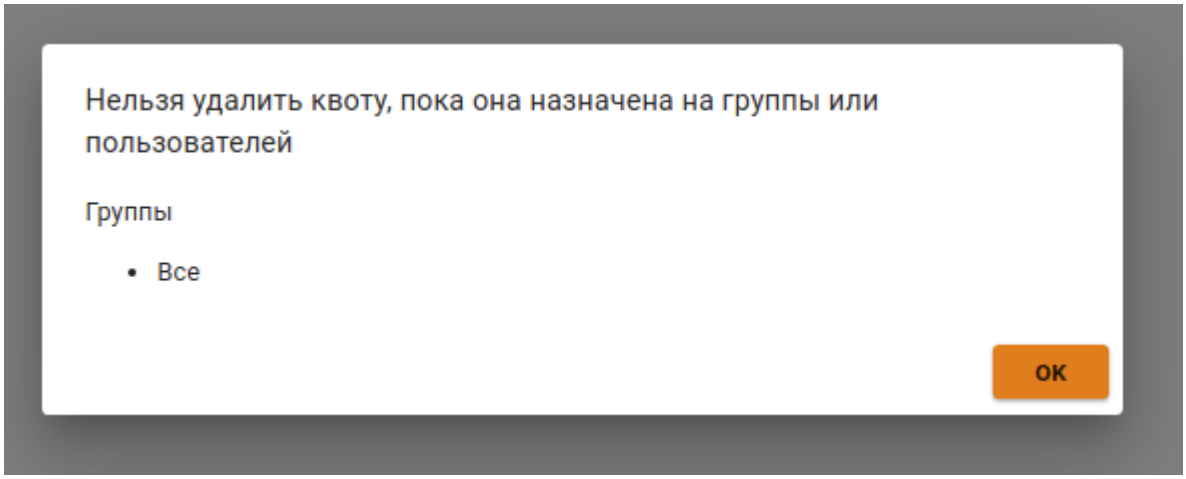
Созданные квоты можно применять для пользователей. Управление квотами происходит на вкладке **Квота** у выбранного пользователя:



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 опцию **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.

17. Профили безопасности

Профили безопасности это наборы параметров для фильтрации трафика различными модулями и позволяет настраивать разные политики безопасности независимо друг от друга.

Профили будут использоваться в правилах раздела *Файрвол*.
Один и тот же профиль будет использоваться в нескольких правилах.

17.1 Что позволят делать профили

- Выбирать, какой трафик отправлять на глубокий анализ и фильтрацию. Это позволит уменьшить нагрузку на модули фильтрации.
- Настраивать независимые друг от друга политики безопасности для модулей фильтрации.

17.2 Контроль приложений

Модуль **Контроль приложений** в 18 версии Ideco NGFW будет настраиваться в разделе **Профили безопасности -> Профили контроля приложений**. Все правила из раздела **Правила трафика -> Контроль приложений** будут доступны только для просмотра.

Чтобы подготовиться к изменениям, обновите версию до 17.5 (если у вас 17.4 и ниже), создайте профили в разделе **Профили безопасности -> Профили контроля приложений** и выберите их в правилах **Файрвола**.

При наличии большого количества профилей в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Созданные профили не будут влиять на работу правил *Файрвола* в 17 версии, но начнут работать после обновления на 18 версию, если применены в правилах **Файрвола**.

Внимание: Будьте внимательны! Несмотря на то, что в 17 версии профили **Контроля приложений** не применяются, выбранное в **Файрволе** действие работает (Разрешить/Запретить). В связи с этим до обновления на 18 версию рекомендуем временно отключить правила, созданные с применением профилей контроля приложений.

17.2.1 Что изменится с появлением профилей контроля приложений

В версиях 17 трафик сначала проходит модуль **Контроль приложений**, а затем **Файрвол**.

В 18 версии в модуль **Контроль приложений** отправится только тот трафик, который попадает под разрешающее правило **Файрвола** с включенной проверкой через профиль контроля приложений согласно настройкам. Очередность обработки трафика в версиях 17 и в 18 версии:

Порядок обработки трафика в 17.X 1. Захват трафика для DPI:

- Контроль приложений;
- Ограничение скорости;
- Система предотвращения вторжений.

2. DNS;

3. Захват трафика для фильтрации (прокси-сервер):

- Контент-фильтр;
- Антивирус веб-трафика.

4. Файрвол.

Порядок обработки трафика в 18.X 1. Ограничение скорости;

2. DNS;

3. Захват трафика для фильтрации (прокси-сервер):

- Контент-фильтр;
- Антивирус веб-трафика.

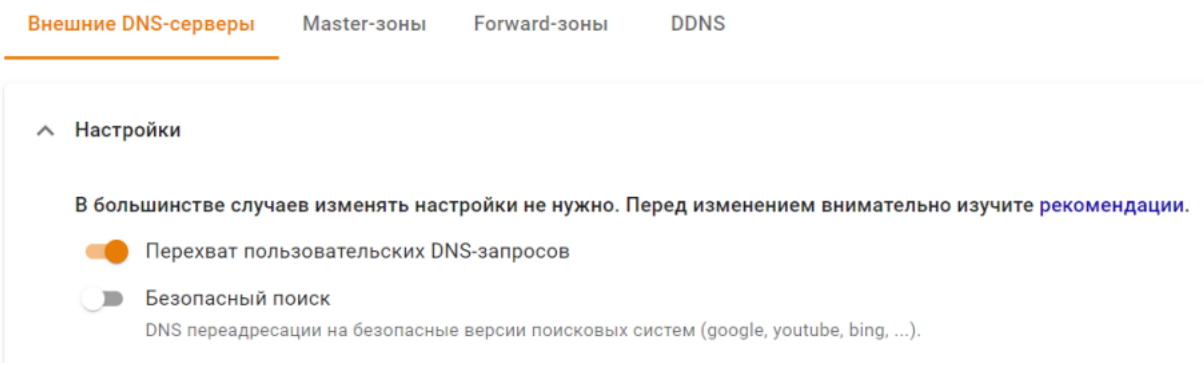
4. Файрвол;

5. Контроль приложений;

6. Система предотвращения вторжений.

Подсказка: Принцип создания **Профилей контроля приложений** в 18 версии Ideco NGFW аналогичен принципу создания правил **Контроля приложений** в более ранних версиях: все протоколы и приложения, которые не были запрещены, остаются разрешены.

Чтобы трафик фильтровался модулем **Контроль приложений**, необходимо для всех локальных интерфейсов создать правило FORWARD, содержащее необходимый профиль безопасности. Если в разделе **Сервисы -> DNS -> Внешние DNS-серверы** включена опция **Перехват пользовательских DNS-запросов** (по умолчанию включена), нужно также создать аналогичное правило INPUT:



17.2.2 Почему мы отказались от автоматической миграции

От автоматической миграции решили отказаться из-за вероятности появления дубликатов правил **FORWARD** и усложнения администрирования таблицы:

- **Контроль приложений** мог бы некорректно определить условия фильтрации, заданные администратором в 17 версии, и для одного правила в таблице **FORWARD** создать несколько профилей;
- Все автоматически созданные профили безопасности были бы применены к существующим правилам **FORWARD**. А так как одному правилу **Файрвола** может соответствовать только один профиль безопасности, появились бы дубликаты.

17.2.3 Особенности создания профилей

Модуль **Контроль приложений** НЕ БУДЕТ обрабатывать трафик в версии 18.X, если в модуле **Файрвол** для этого трафика нет разрешающего правила (действие **Разрешить**) с указанным профилем контроля приложений. Проверьте, что для соответствующего трафика добавлен профиль безопасности.

Предупреждение: ВАЖНО:
Чтобы через модуль **Контроль приложений** проходил трафик, для которого нет разрешающего правила в таблице FORWARD, рекомендуем создать в **Файрволе** правило с источником **Локальные интерфейсы** и назначением **Любой**, разместив его в конец таблицы.

С 18 версии NGFW правила Файрвола, которые блокировали трафик за счет перехвата DNS в предыдущих версиях, не смогут его блокировать. Чтобы это исправить, создайте правила с профилями IPS и DPI в разделе **Правила трафика -> Файрвол -> INPUT**.

Для удобства настройки модуля фильтрации рекомендуем объединить пользователей в несколько групп/подгрупп (например, в соответствии с организационной структурой компании) и настроить профиль

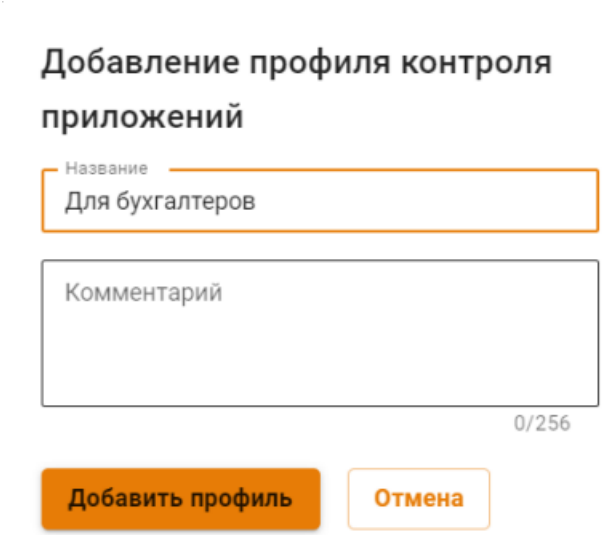
контроля приложений отдельно для каждой группы.

Создание профиля и добавление в правила Файрвола

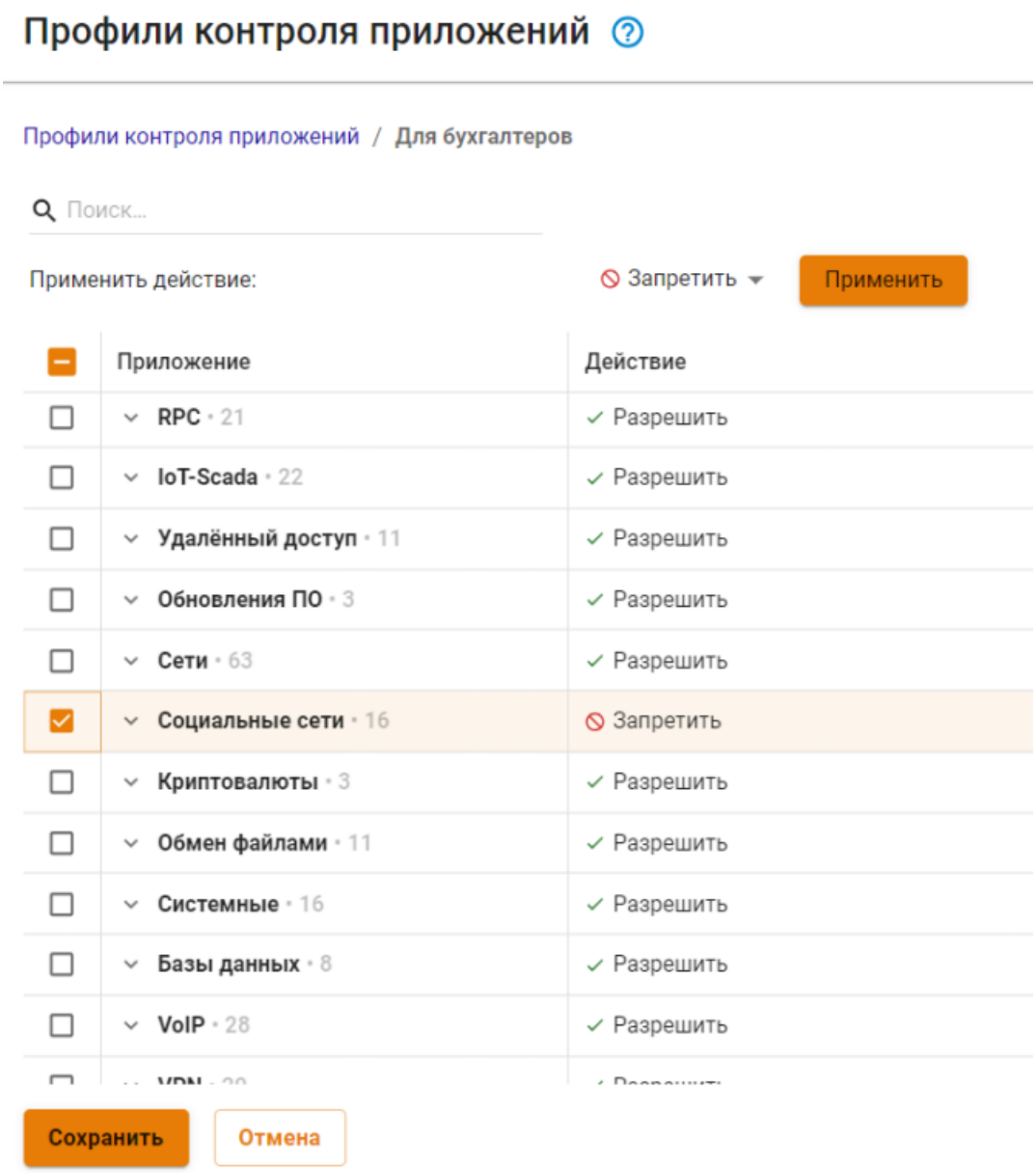
Пример. Необходимо ограничить доступ к социальным сетям пользователям группы «Бухгалтерия».

Создание профиля контроля приложений

1. Перейдите в раздел **Профили безопасности -> Профили контроля приложений** и нажмите **Добавить**.
2. Заполните **Название** и **Комментарий** (необязательно):



3. После добавления профиля нажмите в столбце **Управление** на , а затем **Доступ к приложениям**. Выберите **Социальные сети** и примените действие **Запретить** к группе приложений, нажав на соответствующую кнопку в правом верхнем углу:



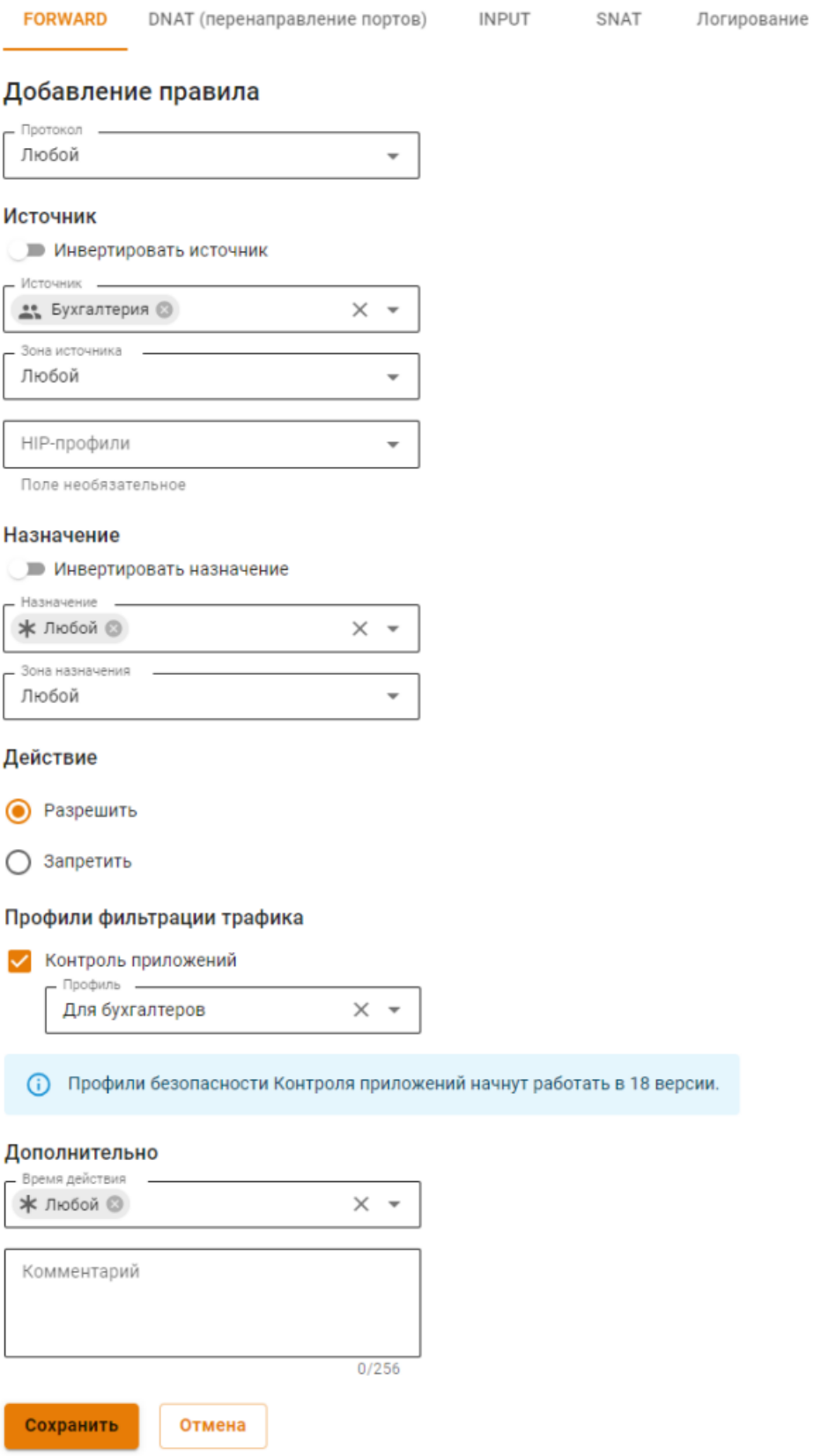
Подсказка: К неизвестным источникам по умолчанию применяется действие **Разрешить** (доступно для редактирования).

4. Нажмите **Сохранить**.

Добавление профиля в правила Файрвола

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

2. Заполните поля:



- **Протокол** - выберите протокол, соответствующий трафику, который требуется фильтровать с помощью профиля контроля приложений;
- **Источник** - выберите **Адрес**, **Зону** и **HIP-профиль** источника трафика;
- **Назначение** - выберите **Адрес** и **Зону** назначения трафика;
- **Действие** - выберите **Разрешить**;

3. Включите опцию **Контроль приложений** и в разделе **Профили для фильтрации** из раскрывающегося списка выберите профиль, запрещающий социальные сети сотрудникам бухгалтерии.

4. Включите правило или оставьте его выключенным.

5. Нажмите **Сохранить**.

6. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичное правило INPUT.

Иерархическая структура Профилей контроля приложений

Один из вариантов корректного применения политик безопасности к вложенной структуре пользователей - построение иерархической структуры **Профилей контроля приложений**:

- Профили для самой большой группы пользователей запрещают наибольшее количество протоколов и приложений;
- Профили для более мелких групп пользователей повторяют запрет для самой большой группы пользователей, но точечно разрешают определенные приложения и протоколы для конкретных подгрупп;
- Профили для конкретных пользователей разрешают опередеренные протоколы и приложения, необходимые этим конкретным пользователям. В этих профилях также остаются запреты, которые должны сохраниться для этих пользователей.

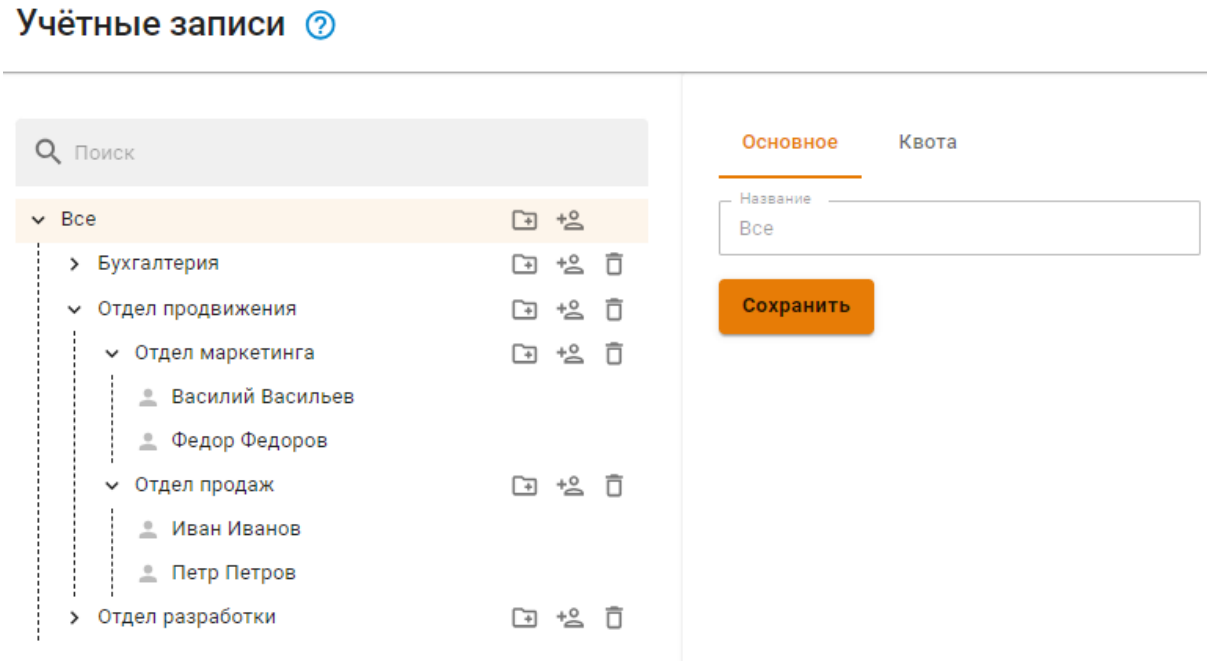
Чтобы настроить фильтрацию трафика, для которого в таблице FORWARD нет правил, воспользуйтесь инструкцией:

17.2.4 Пример создания иерархической структуры

Пример. Необходимо настроить профили контроля приложений в соответствии с требованиями:

- Всем пользователям запрещены компьютерные игры, контент для взрослых, майнинг и криптовалюты;
- Доступ к социальным сетям разрешен только Отделу продвижения;
- Доступ к стриминговым сервисам разрешен только Отделу маркетинга;
- Доступ к музыкальным приложениям разрешен только Федору Федорову из Отдела маркетинга.

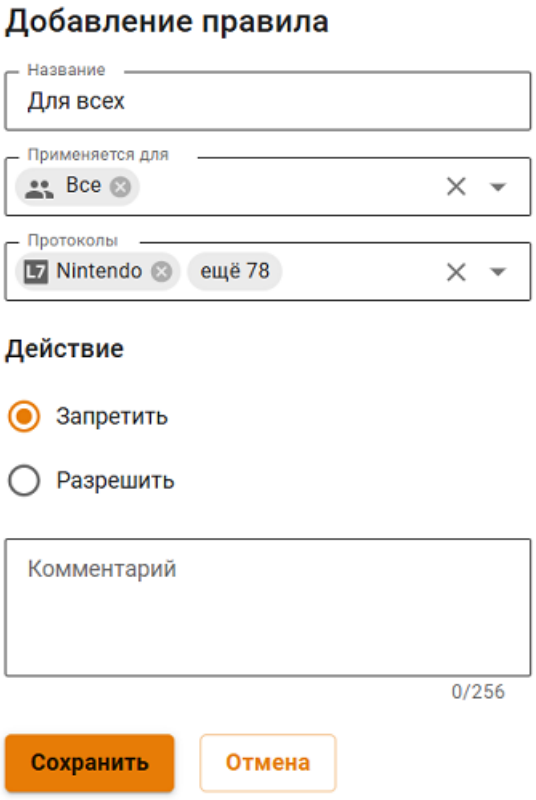
В описанном примере Федор Федоров - сотрудник Отдела маркетинга, а Отдел маркетинга - структурное поздразделение Отдела продвижения:



Настройка в версии 17 (правила)

1. Создайте правило, запрещающее всем сотрудникам социальные сети, стриминговые сервисы, музыкальные приложения, компьютерные игры, контент для взрослых, майнинг и криптовалюты. Для этого:

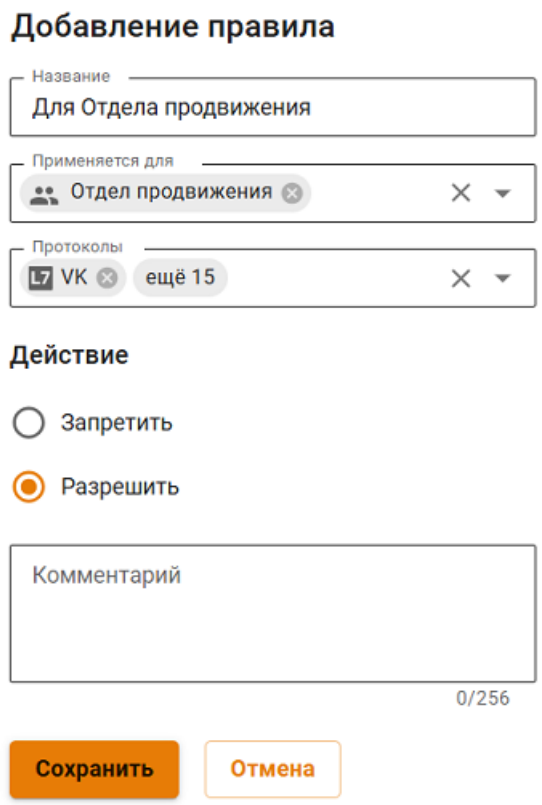
- Перейдите в раздел **Правила трафика -> Контроль приложений** и нажмите **Добавить**;
- Настройте правило с действием **Запретить** для всех пользователей, выбрав протоколы и приложения, соответствующие условиям примера:



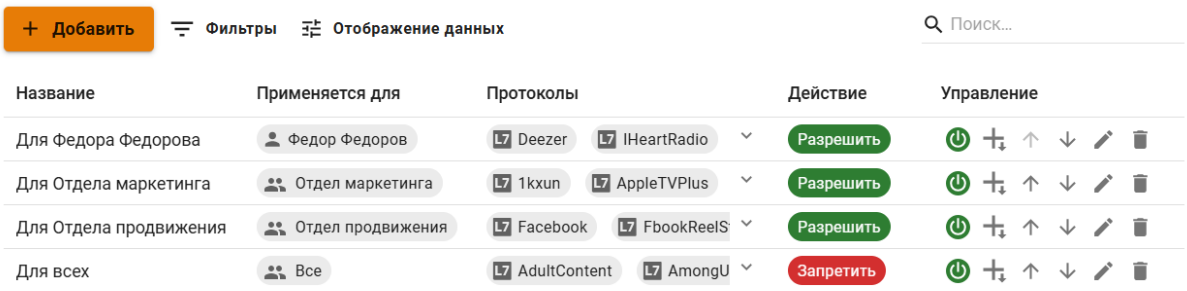
2. Аналогично создайте ряд правил, соответствущих условиям примера:

- Сотрудникам Отдела продвижения разрешен доступ к социальным сетям;
- Сотрудникам Отдела маркетинга разрешен доступ к стриминговым сервисам;
- Федору Федорову из Отдела маркетинга разрешен доступ к музыкальным приложениям.

Пример:



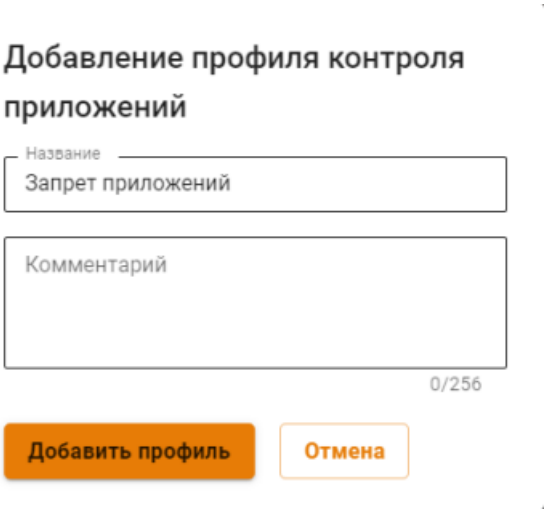
3. Поместите созданные в пункте 2 правила с действием **Разрешить** выше правила, созданного в пункте 1:



Настройка в версии 18 (профили)

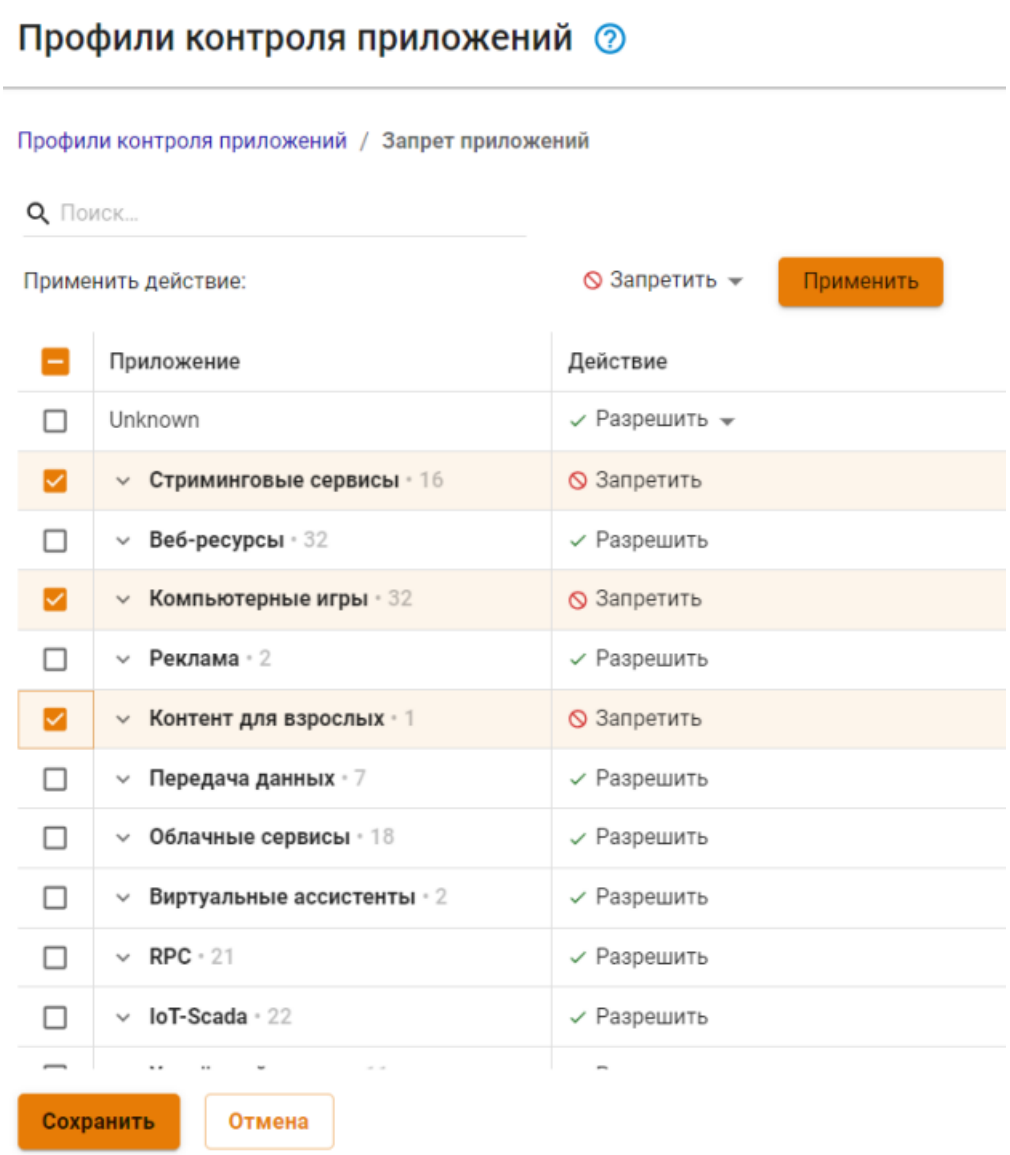
Создайте профили в соответствии с условиями примера:

1. Перейдите в раздел **Профили безопасности -> Контроль приложений**, чтобы создать профиль, запрещающий доступ к социальным сетям, стриминговым сервисам, музыкальным приложениям, компьютерным играм, контенту для взрослых, майнингу и криптовалютам. Нажмите **Добавить** и введите название профиля:



2. Настройте добавленный профиль:

- Нажмите в столбце **Управление** на , а затем **Доступ к приложениям**;
- Выберите группы приложений, которые необходимо запретить (перечислены в описании примера);
- Установите настройку **Запретить** и нажмите **Применить** в правом верхнем углу;
- После применения действия нажмите **Сохранить** в левом нижнем углу:



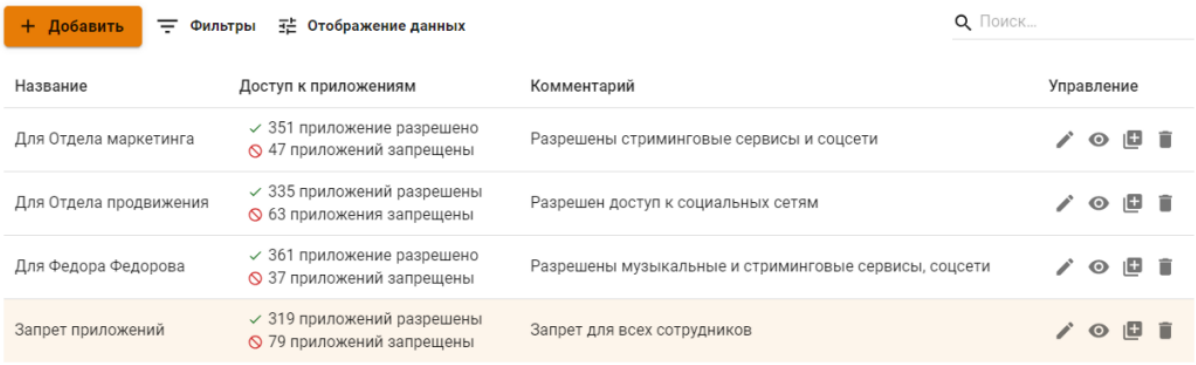
3. Создайте профиль для Отдела продвижения, разрешающий доступ к социальным сетям. Для этого:

- Клонируйте созданный профиль, нажав на в столбце **Управление**;
- Отредактируйте клонированный профиль: поменяйте название (например, на **Для Отдела продвижения**) и настройки доступа к приложениям (разрешите доступ к социальным сетям).

4. Аналогично создайте профиль для Отдела маркетинга, разрешающий доступ к стриминговым сервисам. Для этого клонируйте профиль **Для Отдела продвижения**, введите название (например, **Для Отдела маркетинга**) и разрешите в нем доступ к стриминговым сервисам.

5. Создайте профиль для Федора Федорова, разрешающий доступ к музыкальным сервисам. Для этого клонируйте профиль **Для Отдела маркетинга** и установите необходимые настройки.

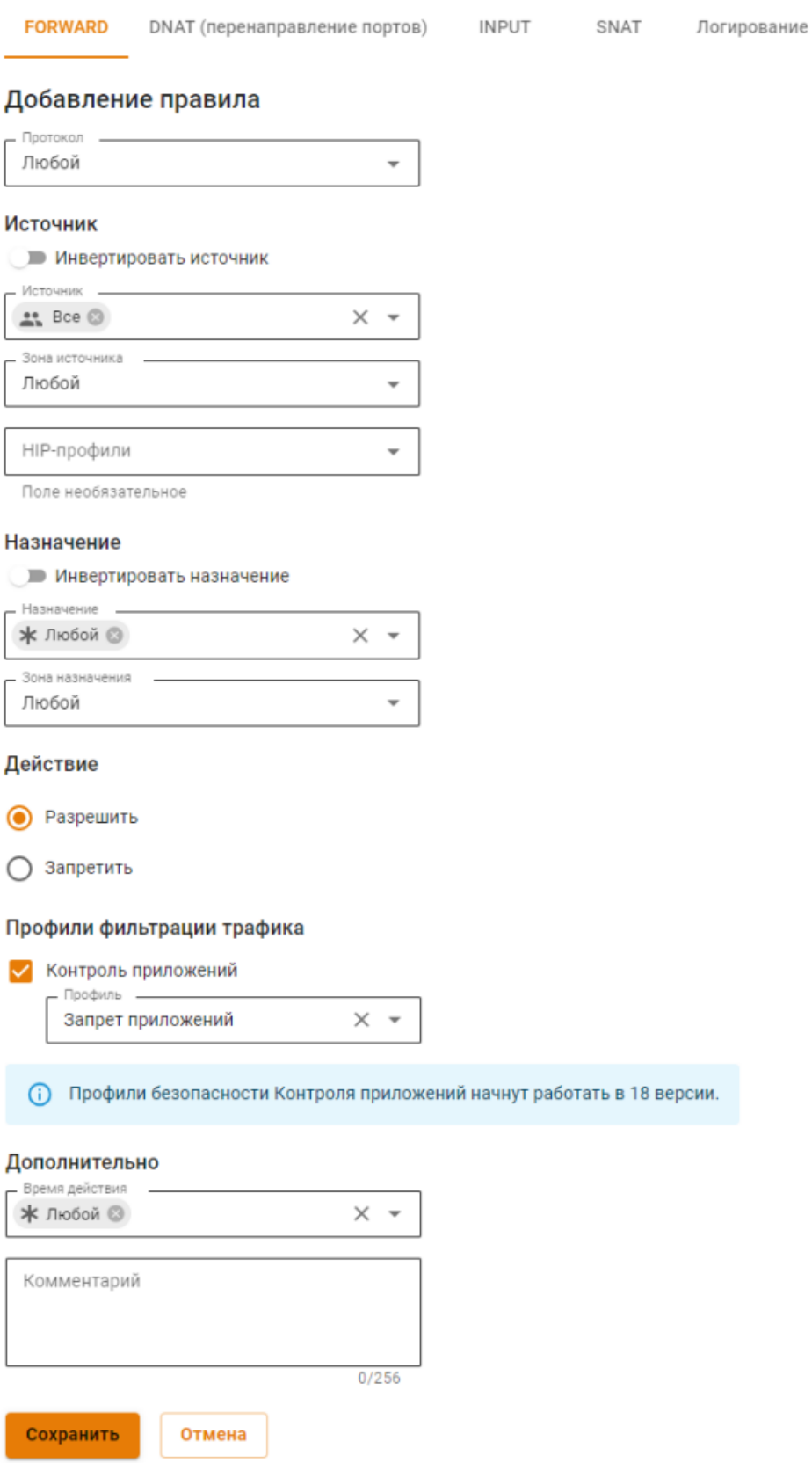
В итоге должен получиться набор профилей, учитывающий настройки, описанные в примере:



Теперь необходимо создать правила в **Файрволе**, чтобы применить настройки для конкретных групп пользователей и установить приоритет прохождения трафика:

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

2. Заполните поля:

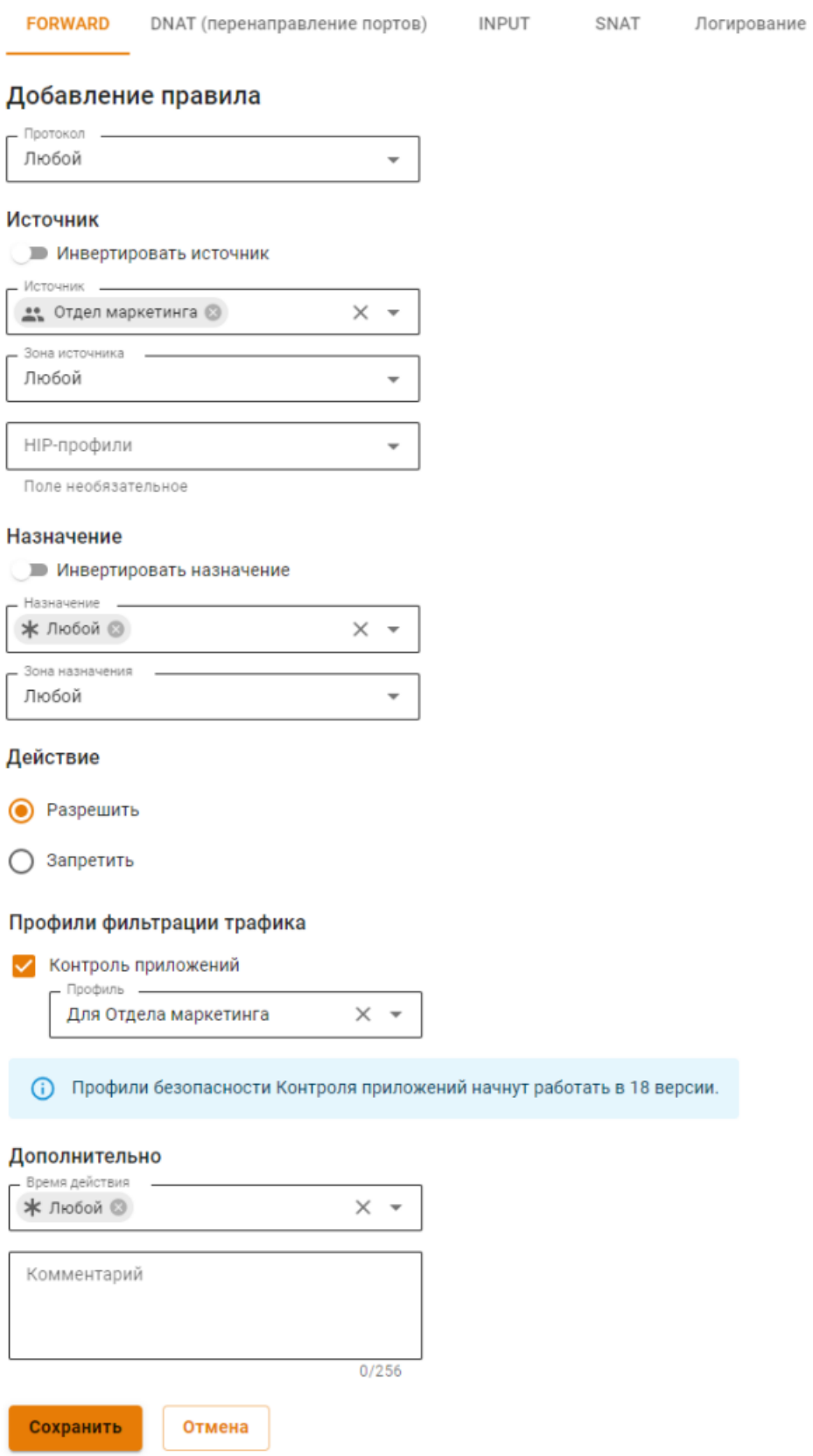


- В поле **Адрес** раздела **Источник** выберите группу **Все**.
- Выберите действие **Разрешить**.
- В профилях фильтрации трафика включите опцию **Контроль приложений** и выберите профиль **Запрет приложений**.

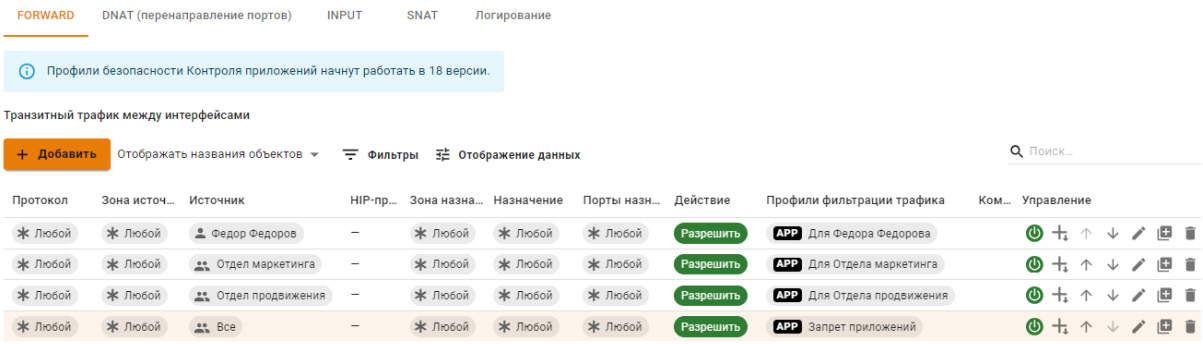
- Включите правило.

3. Нажмите **Сохранить**.

4. Аналогично создайте правила для каждого профиля. При создании правила **Файрвола** укажите соответствующий профилю адрес источника. Например, при создании правила с профилем фильтрации **Для Отдела маркетинга** выберите в поле **Адрес** раздела **Источник** группу **Отдел маркетинга**:



5. Чтобы трафик проходил в соответствии с условиями примера, установите в **Файрволе** следующую последовательность правил:



Чем выше в таблице стоит правило, тем выше его приоритет. Разрешающее правило для сотрудника не сработает, если выше в таблице **Файрвола** находится правило, запрещающее трафик для отдела, в котором работает этот сотрудник.

6. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичные правила INPUT.

17.2.5 Настройка фильтрации трафика, для которого в таблице FORWARD нет правил

Основное

Сначала создайте профиль контроля приложений, соответствующий нужным правилам. Для этого:

1. Перейдите в раздел **Профили безопасности -> Профили контроля приложений** и нажмите **Добавить**.

2. Введите **Название** профиля и **Комментарий**.

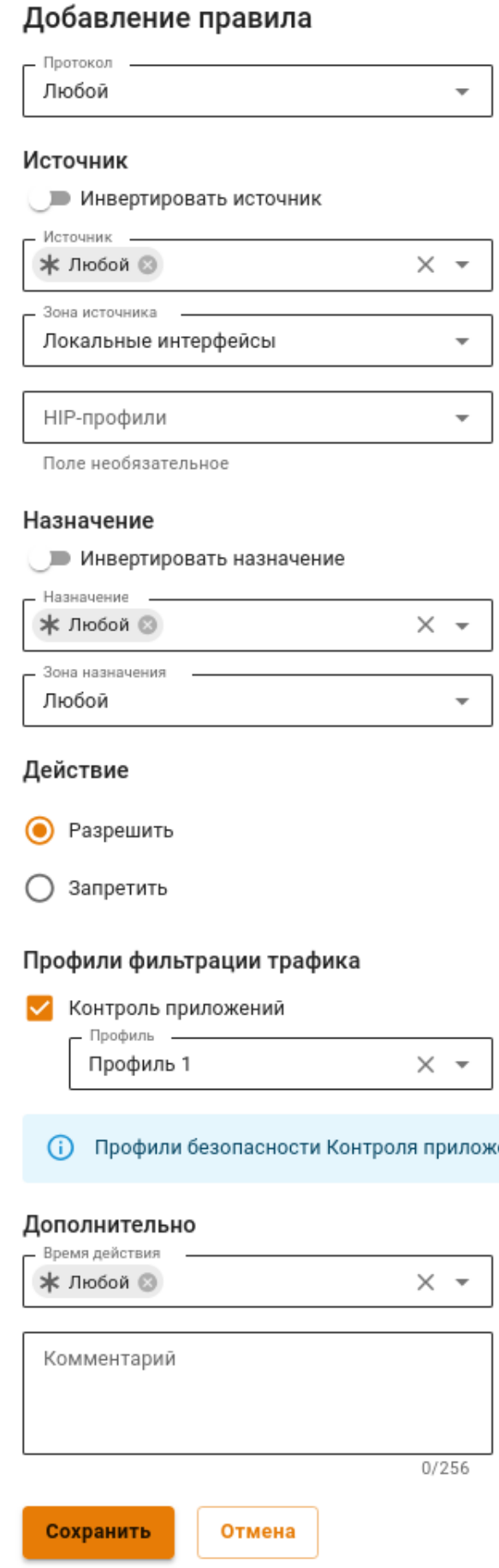
3. После добавления профиля нажмите в столбце **Управление** на , а затем **Доступ к приложениям**. Выберите протоколы или группы протоколов и действия (**Запретить** или **Разрешить**), которые будут к ним применяться.

4. Нажмите **Сохранить**.

Теперь необходимо создать правило **Файрвола** с созданным профилем контроля приложений. Для этого:

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

2. Заполните поля:


Добавление правила
Протокол
Любой
Источник
Инвертировать источник
Источник
Любой
Зона источника
Локальные интерфейсы
HIP-профили
Поле необязательное
Назначение
Инвертировать назначение
Назначение
Любой
Зона назначения
Любой
Действие
Разрешить
Запретить
Профили фильтрации трафика
Контроль приложений
Профиль
Профиль 1
Профили безопасности Контроля приложений начнут работать в 18 версии.
Дополнительно
Время действия
Любой
Комментарий
0/256
Сохранить
Отмена

- **Протокол** - выберите **Любой**;
- **Источник**:
  - **Зона источника** - выберите **Локальные интерфейсы**;
  - При необходимости укажите **Адрес** и **HIP-профиль** источника трафика.
- **Назначение**:
  - **Зона назначения** - выберите **Любой**;
  - При необходимости укажите **Адрес** назначения трафика.
- **Действие** - выберите **Разрешить**.

3. Включите опцию **Контроль приложений** и из раскрывающегося списка выберите созданный ранее профиль.

4. Включите правило.

5. Нажмите **Добавить**.

6. Поместите правило в конец таблицы **Файрвола**. Если в таблице есть правило, запрещающее все, поместите правило с **Профилем контроля приложений** над ним.

7. При включенной опции **Перехват пользовательских DNS-запросов** создайте аналогичное правило INPUT.

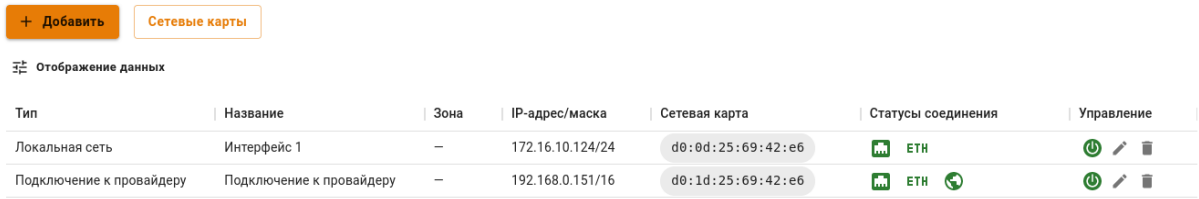
18. Сервисы

18.1 Сетевые интерфейсы

Подсказка: Название службы раздела *Сетевые интерфейсы*: `ideco-network-backend`; `ideco-network-nic`.
Список имен служб для других разделов доступен по *ссылке*.

Сетевой порт становится активным только после создания сетевого интерфейса (внешнего или локального). До этого момента индикаторы на подключенных сетевых портах не горят и Ethernet-кадры не передаются.

Все созданные интерфейсы представлены в виде таблицы:



Статусы соединения:

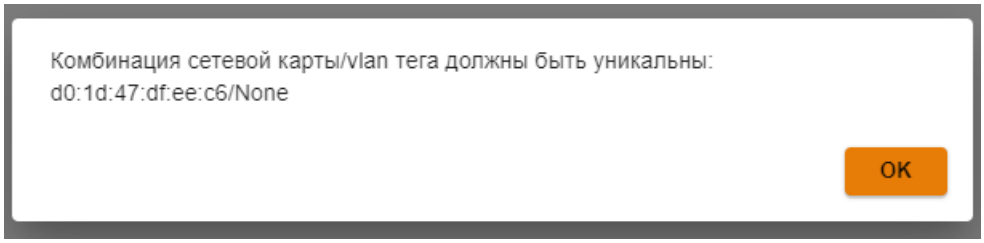
-  - сигнал есть;
-  - статус сигнала не определен;
-  - сигнала нет;
-  - IP-адрес назначен;

-  - соединение с интернетом установлено;
-  - соединение с интернетом отсутствует.

В режиме редактирования 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 бекапа 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.

18.1.1 Агрегированные интерфейсы

Подсказка:

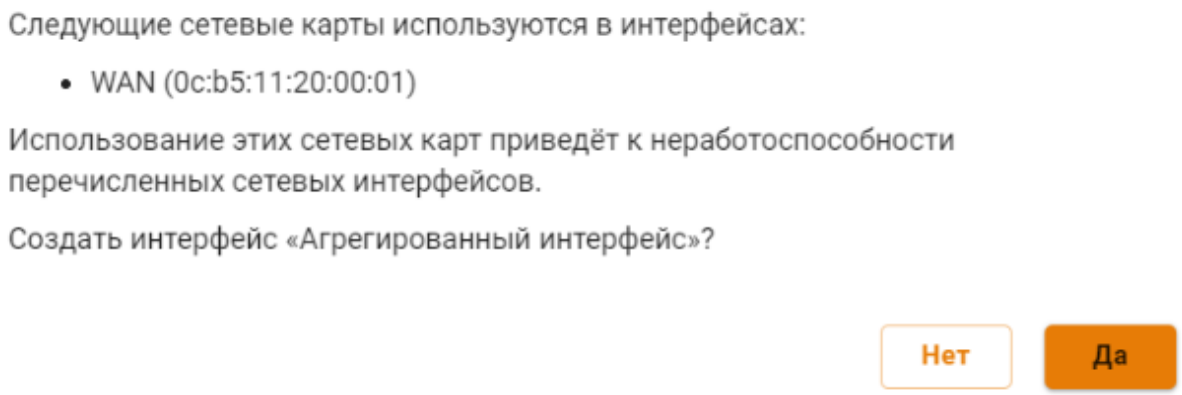
- Агрегированные интерфейсы реализованы по стандарту LACP (IEEE **802.3ad**).
- Используется **active** режим - постоянная рассылка LACP пакетов.
- Проверка соседства осуществляется в режиме **slow** - раз в 30 секунд.
- Количество сетевых карт, объединяемых в агрегированный интерфейс, не ограничено.
- Нельзя добавлять LACP-интерфейсы в VCE.

Чтобы объединить несколько сетевых интерфейсов в один агрегированный, перейдите в раздел **Сервисы -> Сетевые интерфейсы** и в таблице **Агрегированные интерфейсы (LACP)** нажмите **Добавить**. Укажите название, выберите сетевые карты и нажмите **Сохранить**.

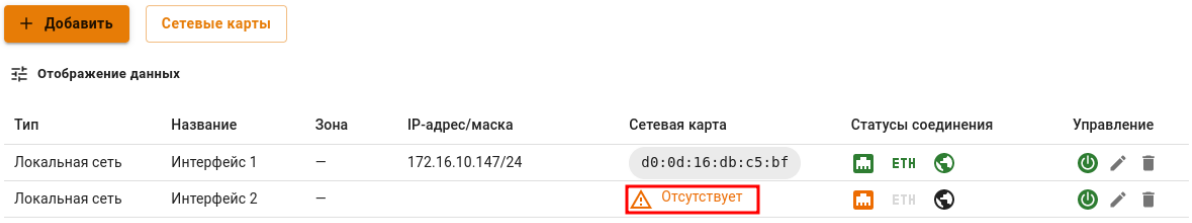
При выборе сетевой карты обращайте внимание на пиктограммы:

-  - 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.

18.1.2 Туннельные интерфейсы

На вкладке настраиваются GRE-туннели.

GRE-туннель - это соединение точка-точка с возможностью передавать широковещательный трафик. На таких интерфейсах может работать протокол динамической маршрутизации OSPF. Пакеты, проходящие внутри GRE, не шифруются.

Для добавления GRE-туннеля нажмите **Добавить**, заполните поля и нажмите **Сохранить**:

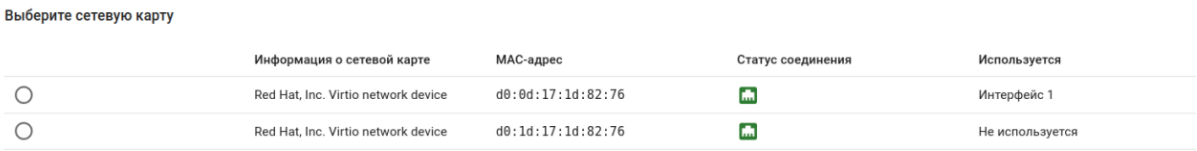
- **Название** - введите название туннельного интерфейса;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый туннельный интерфейс;
- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение;
- **Адрес удаленного интерфейса** - укажите IP-адрес интерфейса, с которым будет производиться соединение;
- **IP-адрес/маска** - укажите данные создаваемого туннеля;
- **Шлюз** - шлюз для направления трафика по умолчанию;
- **Комментарий** - поле может быть пустым.

18.1.3 VCE-интерфейсы

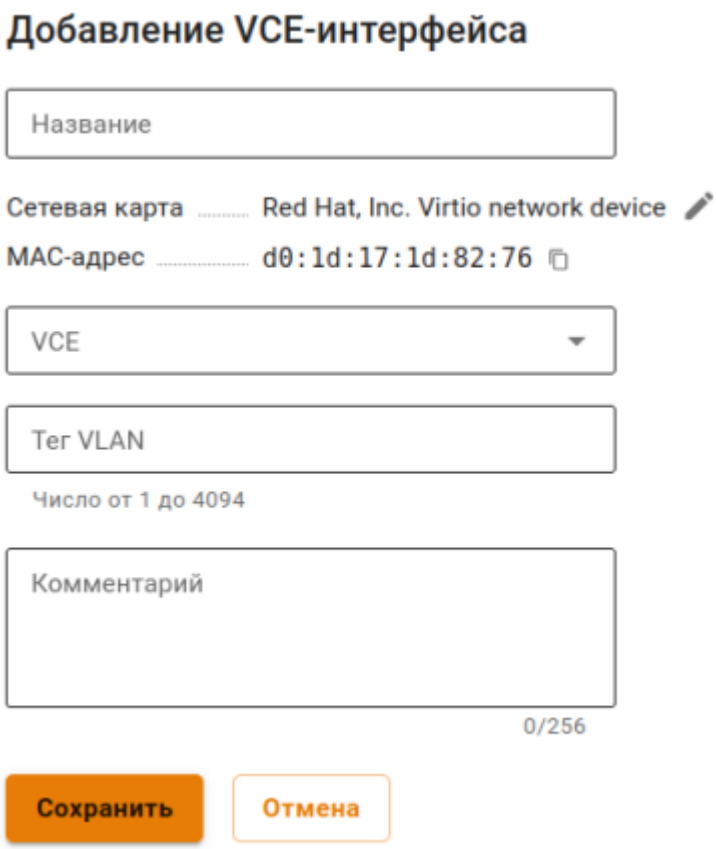
На этой вкладке пробрасываются сетевые карты и VLAN-интерфейсы Ideco NGFW в виртуальные серверы, созданные в разделе **Управление сервером ->** ***VCE***.

Чтобы назначить сетевую карту или VLAN-интерфейс VCE, нажмите **Добавить** и выполните действия:

1. Выберите сетевую карту:



2. Заполните следующие поля:



- **Название** - введите название VCE-интерфейса;
- **VCE** - выберите из списка VCE, созданный в разделе **Управление сервером -> VCE**;
- **Тег VLAN** - если нужно пробросить в VCE порт сетевой карты, оставьте поле пустым. Если нужно пробросить только VLAN, укажите тег VLAN - число от 1 до 4094;
- **Комментарий** - поле может быть пустым.

3. Нажмите **Сохранить**.

При наличии большого количества VCE-интерфейсов в таблице воспользуйтесь кнопкой **Фильтры**.

По кнопке **Сетевые карты** доступны все сетевые карты корневого VCE, еще не проброшенные в дочерние VCE.

Подсказка: Переданная VCE сетевая карта будет недоступна для использования корневым NGFW. Также невозможно будет назначить эту карту другому VCE без указания тега VLAN.

Предупреждение: Не присваивайте VCE сетевые карты, которые используются корневым NGFW, без указания тега VLAN. В противном случае доступ к веб-интерфейсу NGFW будет потерян.

18.1.4 Настройка Локального Ethernet

Внимание: Будьте внимательны!

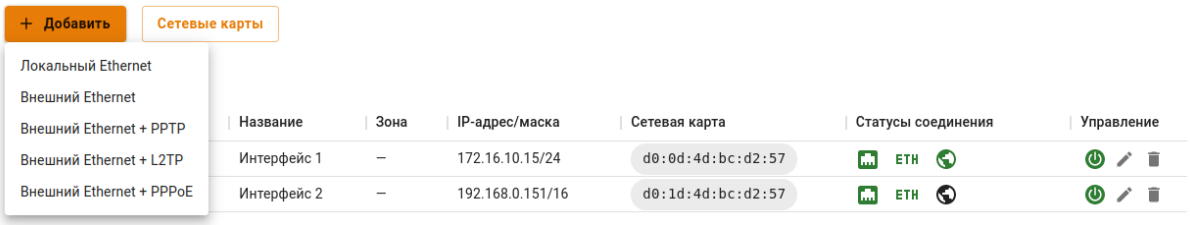
При выборе пункта **Локальный Ethernet** и заполнении поля **Шлюз** доступ в интернет будет отсутствовать. Шлюз указывается для маршрутизации внутри локальной сети или в режиме прямого прокси.

Ручная настройка

Для настройки подключения в веб-интерфейсе необходимо выполнить следующие действия:

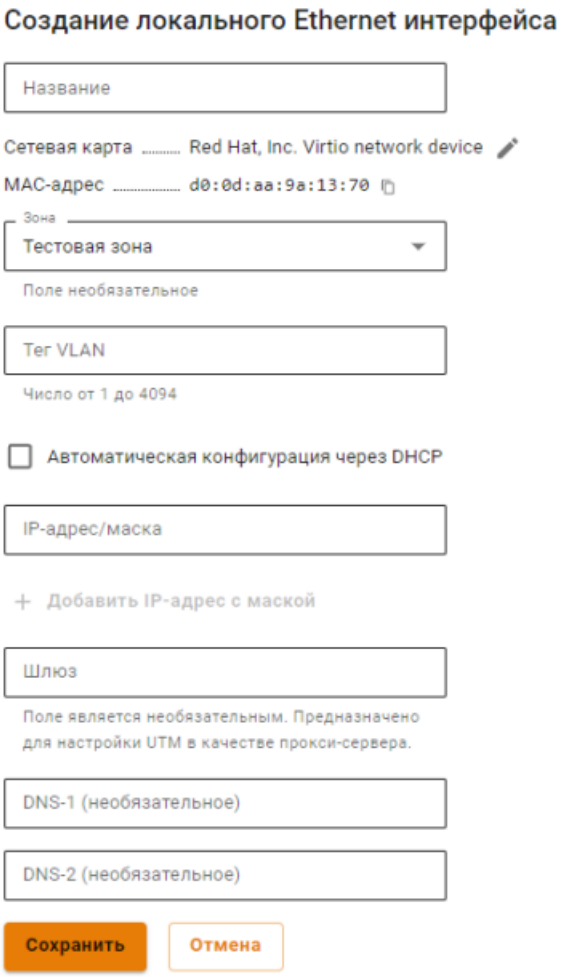
1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Локальный Ethernet**.



3. Выберите сетевую карту.

4. Заполните поля:



- **Название интерфейса** - имя для идентификации интерфейса;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется в том случае, если сетевая карта уже используется;
- **Автоматическая настройка через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Как минимум, должен быть указан хотя бы один IP-адрес;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS сервера (необязательно).

Внимание: Поле **Шлюз** в Локальном интерфейсе задается только, если:

- Нет Внешнего интерфейса NGFW;
- NGFW используется как прокси-сервер.

Автоматическая настройка

Используется, если ваш интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

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

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Локальный Ethernet**.

3. Выберите сетевую карту.

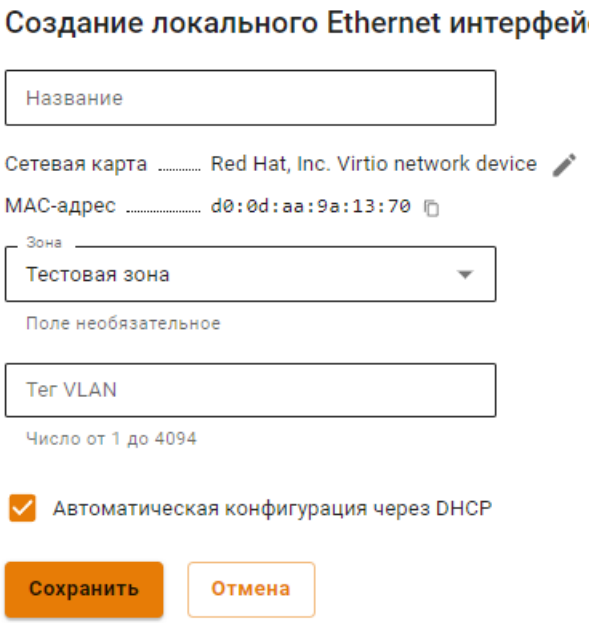
4. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется.

5. При необходимости выберите объект типа **Зона** в одноименном поле.

6. Включите настройку **Автоматическая конфигурация через DHCP**.

7. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Пример настройки:



18.1.5 Настройка Внешнего Ethernet

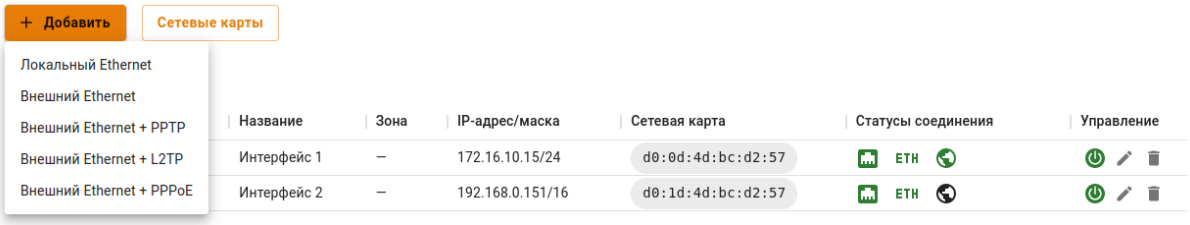
Как правило, вся необходимая информация для настройки содержится в договоре с интернет-провайдером.

Ручная настройка

Для настройки подключения в веб-интерфейсе необходимо выполнить следующие действия:

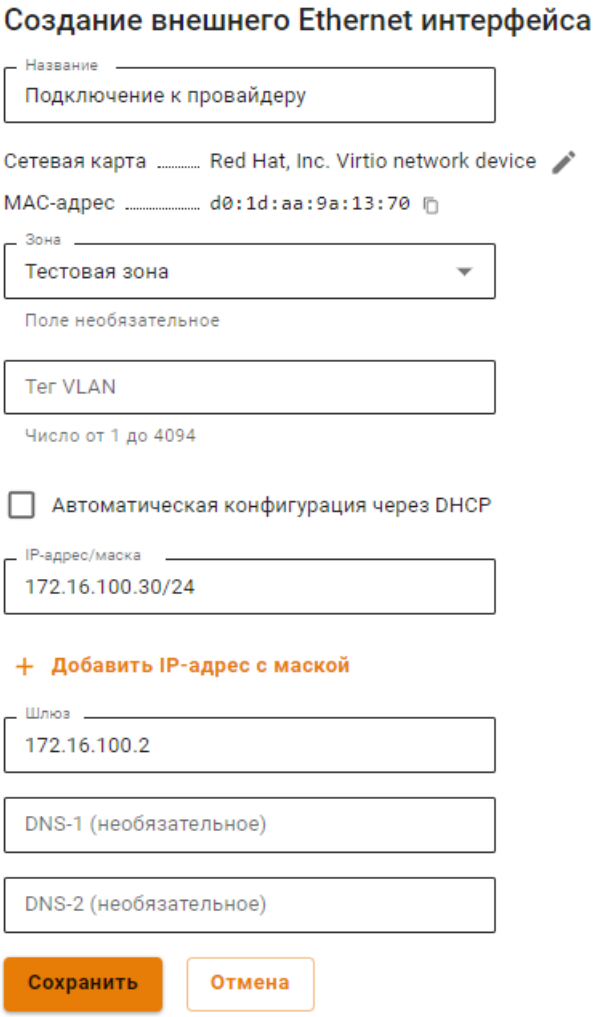
1. Перейдите в меню **Сервисы -> Сетевые интерфейсы**.

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Внешний Ethernet**:



3. Выберите сетевую карту.

4. Заполните поля:



- **Название интерфейса** - имя, с помощью которого возможно в дальнейшем идентифицировать интерфейс;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Также может быть создан один Ethernet-интерфейс без указания VLAN принадлежащий этому сегменту сети, который будет принимать нетегированный трафик. Обычные Ethernet-интерфейсы без указания VLAN ID создаются на физическом интерфейсе только в единичном экземпляре. Поле заполняется только в том случае, если сетевая карта уже используется;
- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - можно назначить на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес;
- **Шлюз** - укажите IP-адрес шлюза интернет-провайдера, через который будет осуществляться подключение к сети интернет;
- **DNS** - доступно два поля для указания DNS-сервера (необязательно).

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.........................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

Автоматическая настройка

Используется, если интернет-провайдер поддерживает возможность автоматической настройки Ethernet-интерфейса с помощью протокола DHCP.

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

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Внешний Ethernet**.

3. Выберите сетевую карту.

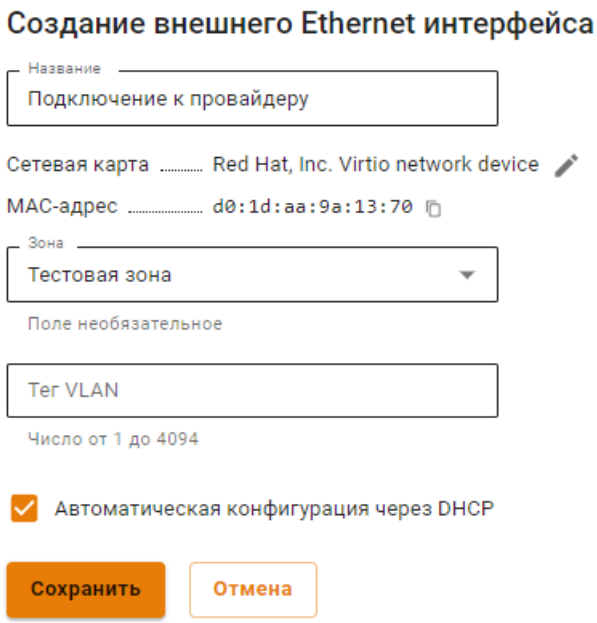
4. Заполните поле **Название**. Поле **Тег VLAN** заполняется только в том случае, если сетевая карта уже используется.

5. При необходимости выберите объект типа **Зона** в одноименном поле.

6. Включите настройку **Автоматическая конфигурация через DHCP**.

7. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Пример настройки:



18.1.6 Настройка подключения по PPTP

Основное

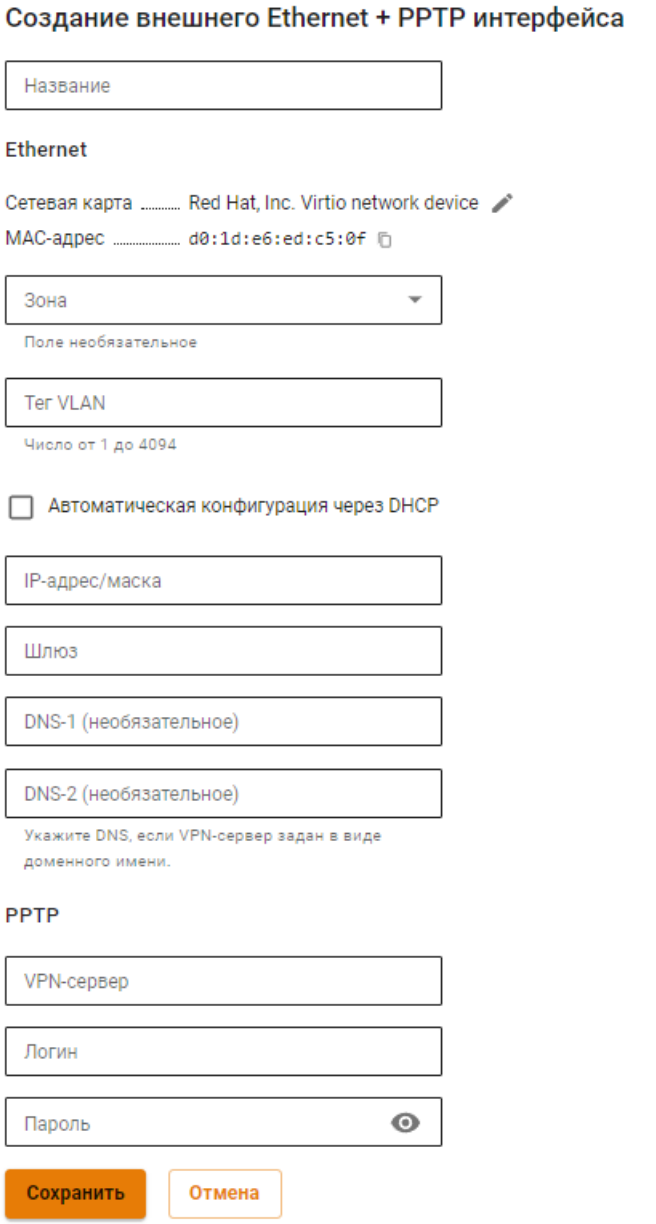
Для настройки такого подключения в веб-интерфейсе необходимо выполнить следующие действия:

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

2. Нажмите **Добавить** в левом верхнем углу окна и выберите **Ethernet + PPTP**.

3. Выберите сетевую карту.

4. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;

- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q;
- **Автоматическая конфигурация через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS-сервера (необязательно);
- **VPN-сервер** - IP-адрес или доменное имя PPTP-сервера;
- **Логин** - имя пользователя для подключения по PPTP;
- **Пароль** - пароль для подключения по PPTP.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.........................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

18.1.7 Настройка подключения по L2TP

Основное

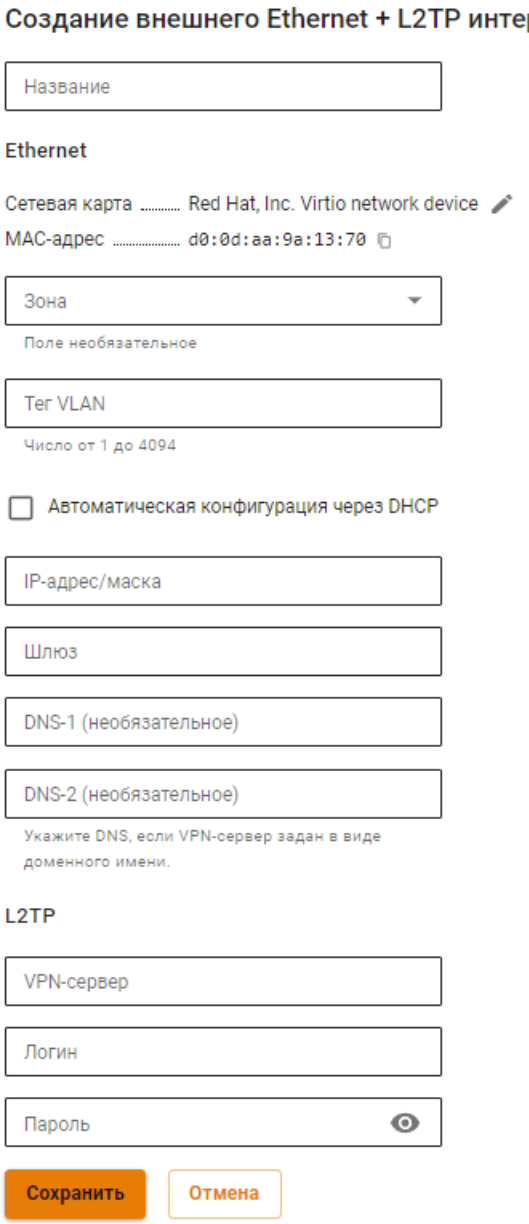
Для настройки такого подключения в веб-интерфейсе необходимо выполнить следующие действия:

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

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Ethernet + L2TP**.

3. Выберите сетевую карту.

4. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае если сетевая карта уже используется. Стандарт VLAN 802.3q;
- **Автоматическая конфигурация через DHCP** - используйте, если ваш интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - назначьте на интерфейс несколько IP-адресов. Должен быть указан хотя бы один IP-адрес;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS-сервера (необязательно);
- **VPN-сервер** - IP-адрес или доменное имя L2TP-сервера;

- **Логин** - имя пользователя для подключения по L2TP;
- **Пароль** - пароль для подключения по L2TP.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.........................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

18.1.8 Настройка подключения по PPPoE

Основное

Для настройки подключения в веб-интерфейсе необходимо выполнить следующие действия:

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

2. Нажмите **Добавить** в левом верхнем углу окна и выберите пункт **Ethernet + PPPoE**.

3. Выберите сетевую карту.

4. Заполните поля:



- **Название** - имя для идентификации интерфейса. Максимальное количество символов - 42;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Зона** - выберите объект типа **Зона**, в состав которой будет входить создаваемый сетевой интерфейс. Максимальное количество сетевых интерфейсов в зоне - 64;
- **Тег VLAN** - VLAN ID, в котором будет присутствовать NGFW. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется только в том случае, если сетевая карта уже используется. Стандарт VLAN 802.3q;
- **Логин** - имя пользователя для подключения по PPPoE;
- **Пароль** - пароль для подключения по PPPoE;
- **Сервис** - идентификатор сервиса. Необязательное поле;
- **Концентратор** - идентификатор концентратора. Необязательное поле.

5. Убедитесь в корректности введенных значений и нажмите на кнопку **Сохранить**.

Подсказка: При подключении к провайдеру с использованием протокола PPPoE настройте DNS-сервер вручную, воспользовавшись *статьей*.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.............................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

18.1.9 Подключение по 3G и 4G

Основное

Сервер Ideco NGFW поддерживает некоторые модели USB-модемов, например, Huawei E8372. При подключении USB-модем будет отображаться в Ideco NGFW как новый ethernet-интерфейс.

Подсказка: Для проверки скорости ранее настроенного интерфейса перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[administrator@localhost ~]# speedtest-cli
Retrieving speedtest.net configuration...
Testing from Mavesa s.a. (158.160.47.205)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by INETCOM LLC (Moscow) [10110.58 km]: 6.1 ms
Testing download speed................................
.............................
Download: 3887.98 Mbit/s
Testing upload speed..................................
.............................................
Upload: 2235.66 Mbit/s
```

18.2 Балансировка и резервирование

Подсказка: Название службы раздела **Балансировка и резервирование**: `ideco-routing-backend`. Список служб для других разделов доступен по *ссылке*.

При наличии нескольких подключений к интернет-провайдерам балансировку и резервирование можно осуществлять следующими способами:

- Резервирование одного из подключений, при отключении которого трафик пойдет через другие доступные подключения.
- Статическая балансировка трафика между несколькими подключениями. При этом часть пользователей локальной сети будет выходить в интернет через одного провайдера, часть - через другого.
- Динамическая балансировка трафика между несколькими подключениями. При этом подключения будут поочередно переключаться в зависимости от нагрузки, а сессии от всех пользователей будут равномерно распределяться между ними.

Перед настройкой убедитесь, что на сервере уже созданы минимум два подключения к сети интернет. Если нет, то создайте дополнительное подключение. Подробнее о создании подключения в статье *Настройка*

Внешнего Ethernet

Подсказка: Если на внешний интерфейс назначено более одного IP-адреса, то при использовании режимов балансировки и резервирования будет использоваться IP-адрес, который был выбран случайным образом при запуске NGFW.

Для работы с трафиком в Ideco NGFW важно учитывать 2 момента: маршрутизация и NAT. Это касается как балансировки, так и резервирования.

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

18.2.1 Основное

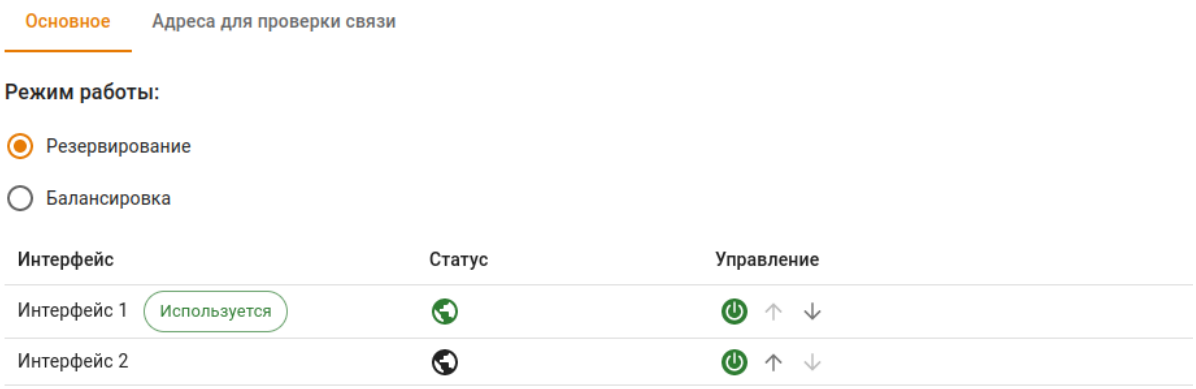
На вкладке доступен выбор одного из двух режимов - **Балансировка** или **Резервирование**.

При **Резервировании** Ideco NGFW использует каналы в соответствии с их приоритетом. Приоритет задается порядком подключений в таблице, сверху вниз. Если интернет стал недоступен через используемое подключение, то NGFW будет перебирать подключения сверху вниз (до первого рабочего подключения).

При **Балансировке** сервер балансирует трафик в зависимости от загрузки подключений.

Резервирование каналов

Перейдите в раздел **Сервисы -> Балансировка и резервирование** и выберите режим **Резервирование**.



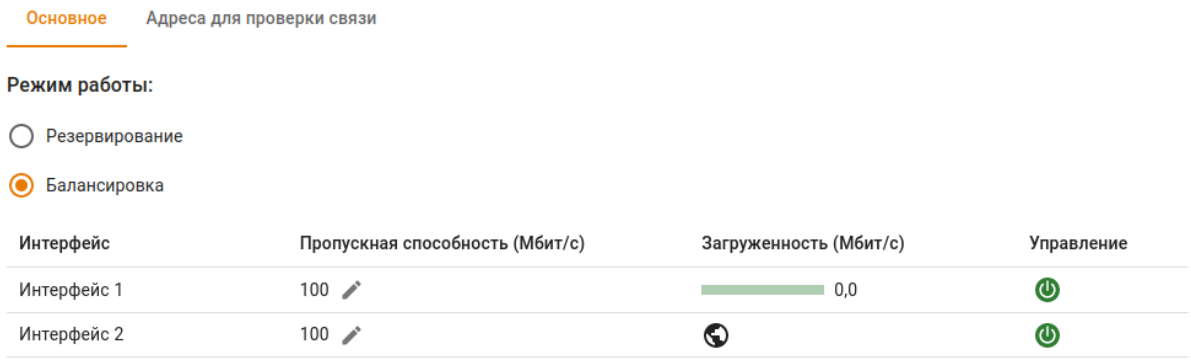
Подключение, которое используется в данный момент, отмечено тегом **Используется**. Для смены приоритета используйте соответствующие элементы управления (↑ ↓).

Динамическая балансировка. Распределение нагрузки по нескольким подключениям

Действия для настройки:

1. Перейдите в раздел **Сервисы -> Балансировка и резервирование**.

2. Выберите режим работы **Балансировка**.



Для равномерного распределения сессий между подключениями необходимо указать значение **Пропускной способности** - максимальной скорости интернета по тарифам провайдеров. Ideco NGFW будет автоматически балансировать трафик в зависимости от загрузки подключений.

Подсказка: Создавать маршруты или выполнять еще какие-либо настройки для динамической балансировки трафика не требуется. Трафик прокси-сервера также будет балансироваться автоматически.

Подсказка: Для проверки скорости подключения перейдите в раздел **Управление сервером -> Терминал** и введите `speedtest-cli`.

Пример вывода команды:

```
[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:

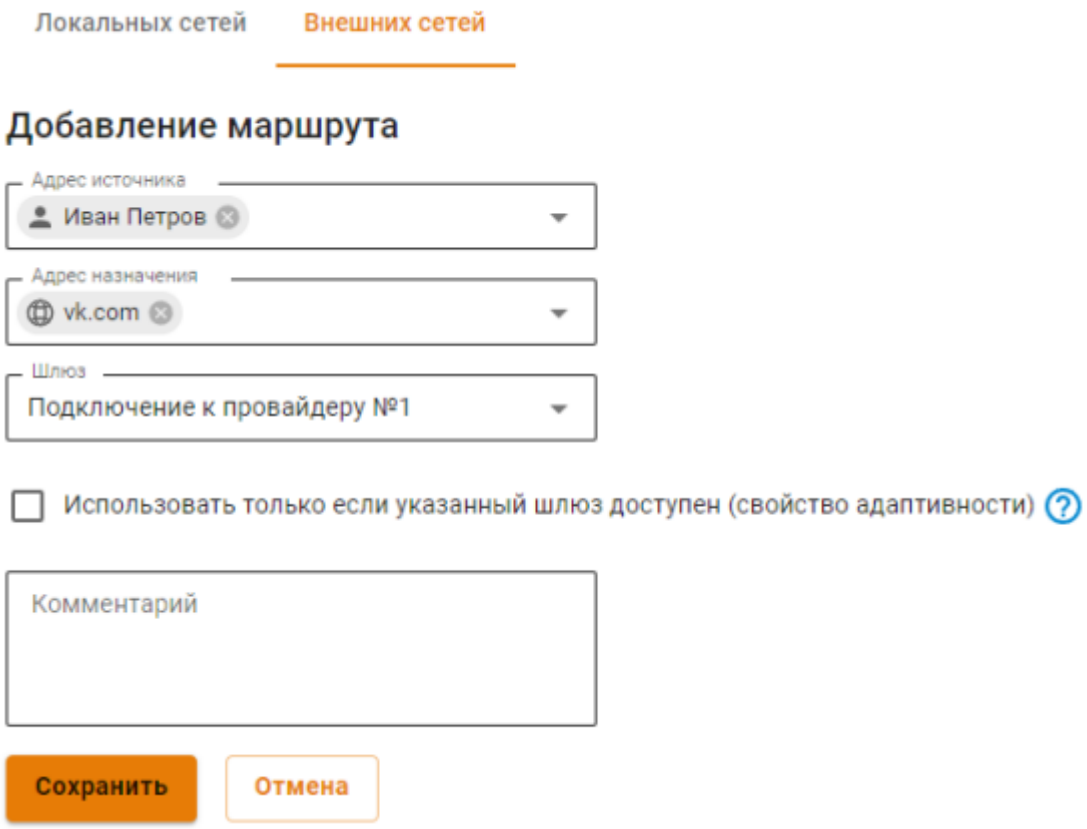
- Направление части трафика через интернет-провайдера, чья тарификация для этого трафика дешевле.
- Предоставление доступа к внутренним сетям одного из провайдеров для определенных пользователей/групп пользователей.

Действия для настройки:

1. Перейдите в раздел меню **Сервисы -> Маршрутизация -> Внешних сетей**.

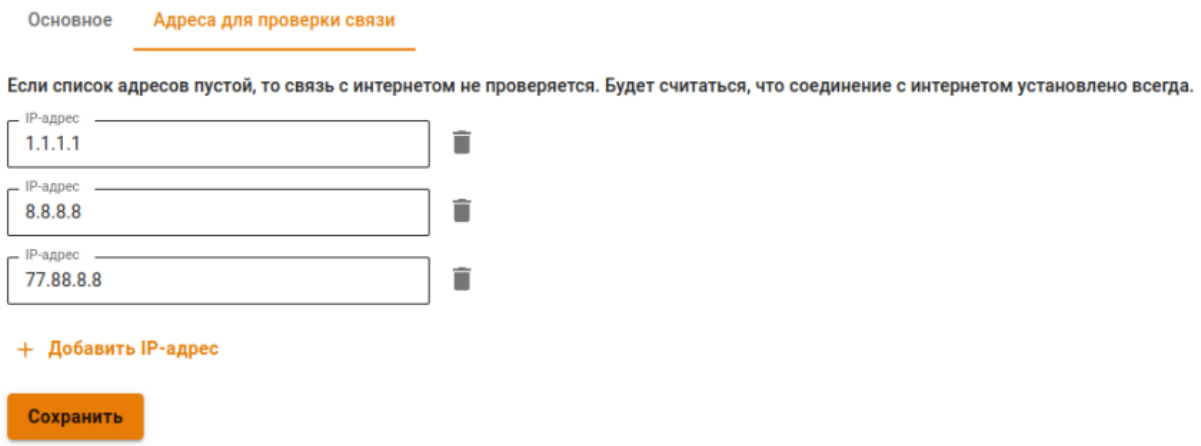
2. Добавьте правила маршрутизации для определенного списка ресурсов, трафик к которым необходимо направить через нужное подключение к провайдеру, нажав кнопку **Добавить**.

Пример направления трафика к ресурсу **vk.com** от пользователя **Иван Петров** через подключение к провайдеру **Подключение к провайдеру №1**:



18.2.2 Адреса для проверки связи

На вкладке задаются IP-адреса, которые Ideco NGFW будет использовать для проверки связи с интернетом. По умолчанию заданы три IP-адреса - DNS-серверы Cloudflare, Google и Яндекс:



Сервер посылает на эти адреса ping-запросы. Соединение с Инернетом считается установленным, если проходит пинг хотя бы до одного адреса из списка. Если этого не происходит, NGFW считает, что соединение с интернетом у интерфейса отсутствует - статус интерфейса меняется с  на .

Подсказка: Если список адресов будет пустым, то связь с интернетом проверяться не будет. Будет считаться, что соединение с интернетом установлено всегда.

18.3 Маршрутизация

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

Преимущества маршрутизации Ideco NGFW:

- Возможность указывать сеть источника при маршрутизации внешних сетей;
- Функция адаптивности (в случае недоступности шлюза или интерфейса поиск маршрута продолжится по следующим правилам в таблице маршрутизации).

Подсказка: Доступность шлюза проверяется с помощью 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*.

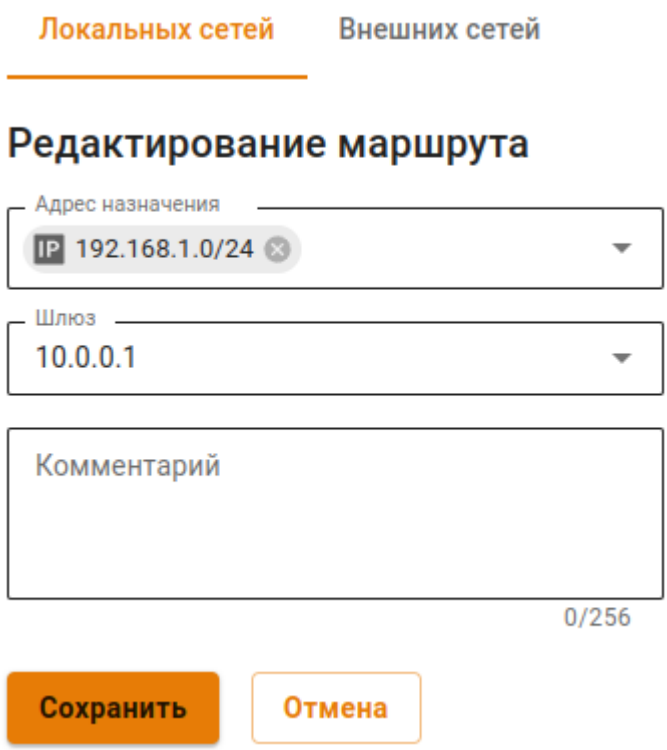
Подсказка: При маршрутизации локальных и внешних сетей доступны GRE-интерфейсы в качестве шлюза.

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

18.3.1 Маршрутизация локальных сетей

Маршрутизация локальных сетей действует внутри локальных сетей. Поэтому при добавлении маршрута отсутствует поле **Адрес источника**. Для добавления нового маршрута перейдите в раздел **Сервисы -> Маршрутизация -> Локальных сетей** и нажмите **Добавить**:



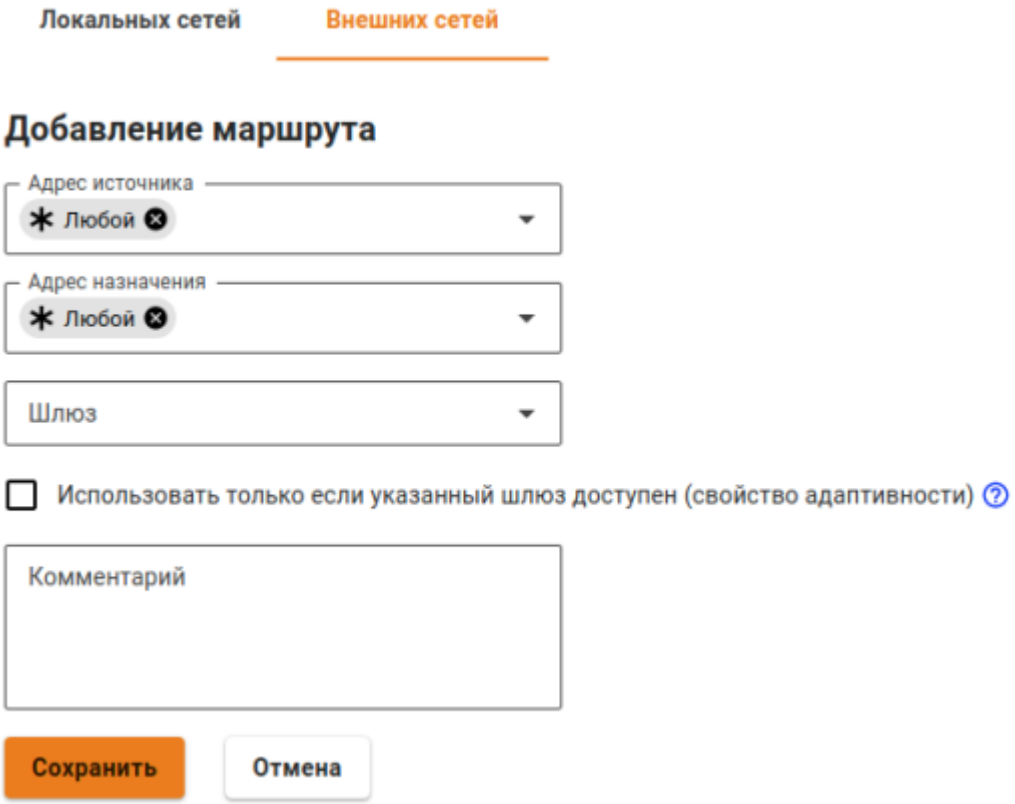
- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться это правило. Возможные типы объектов: IP-адрес, подсеть, домен, список IP-объектов, диапазон IP-адресов;
- **Шлюз** - выберите объект, через который направляется трафик. Возможные типы объектов: IP-адрес, пользователь;
- **Комментарий** - необязательное поле описания маршрута. Значение - не длиннее 128 символов.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: При создании IPSec-подключения в разделе **Сервисы -> IPsec** с включенной опцией **Автоматическое создание маршрутов** будут добавляться маршруты до локальных сетей NGFW в таблицу **Маршрутизации локальных сетей**.

18.3.2 Маршрутизация внешних сетей

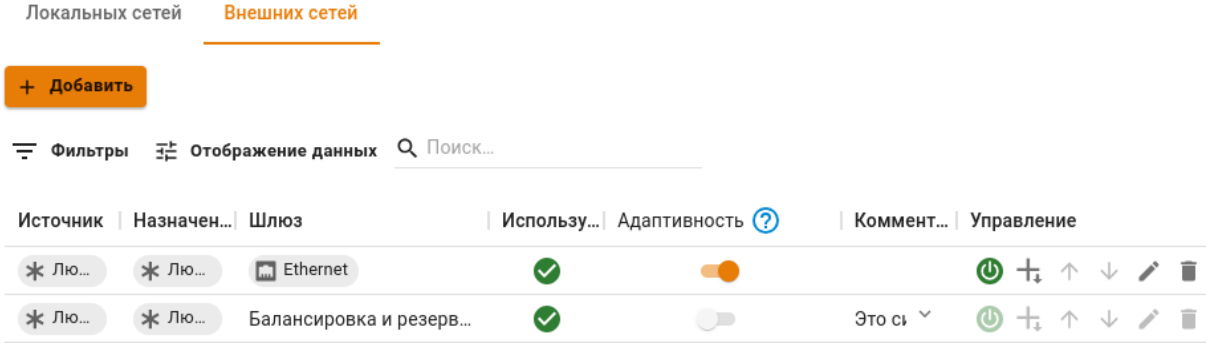
Для добавления нового маршрута перейдите в раздел **Сервисы -> Маршрутизация -> Внешних сетей** и нажмите кнопку **Добавить**. На странице откроется форма создания маршрута:



Опишем назначение каждой опции:

- **Адрес источника** - выберите объекты, для которых будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен;
- **Адрес назначения** - выберите объекты, при обращении к которым будет применяться правило. Возможные типы объектов: группы, пользователи, IP-адрес, список IP-адресов, диапазон IP-адресов, подсеть, домен;
- **Шлюз** - выберите объект, через который будет направлен трафик. Возможные типы объектов: сетевой интерфейс, IP-адрес;
- **Использовать только если шлюз доступен (адаптивность)** - если свойство включено, то при недоступности шлюза или интерфейса поиск маршрута продолжится по следующим правилам маршрутизации. Если свойство отключено (по умолчанию), то трафик отправляется в выбранный шлюз или интерфейс. Если шлюз недоступен или интерфейс не работает, то трафик будет отброшен (destination unreachable);
- **Комментарий** - необязательное поле описания маршрута. Значение не должно быть длиннее 128 символов.

После сохранения маршрута страница выглядит так:



Кнопки и повышают или понижают приоритет правила.

При наличии большого количества маршрутов в таблице воспользуйтесь кнопкой **Фильтры**.

Статусы в столбце **Используется**:

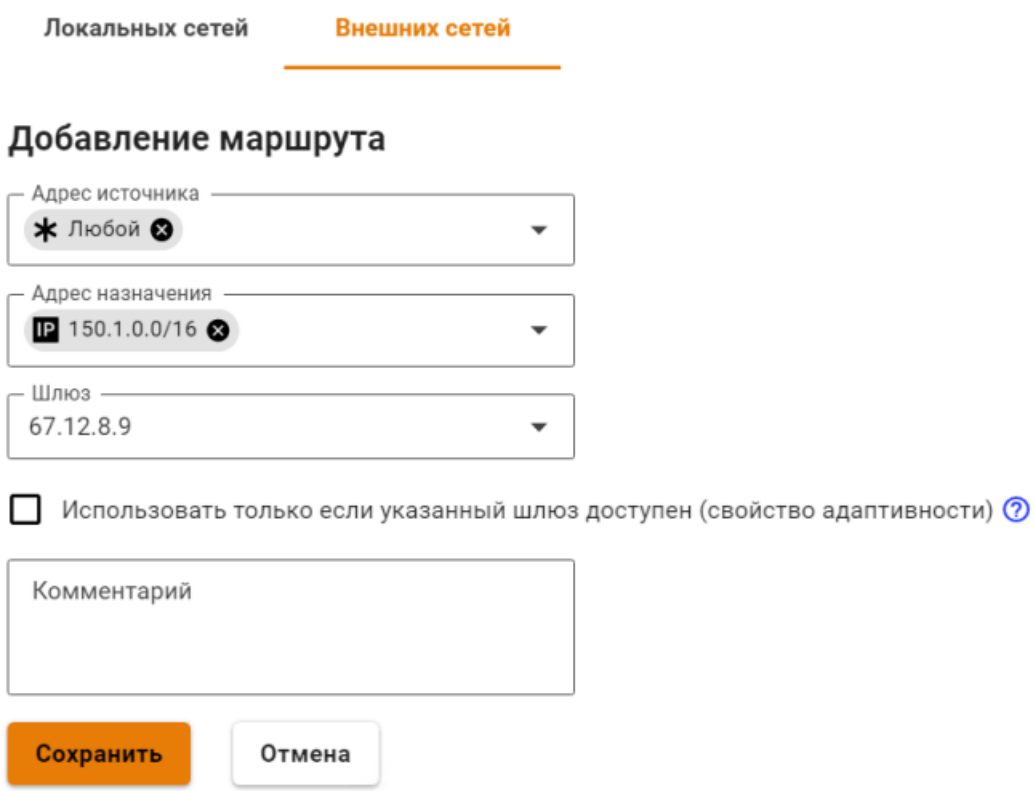
- - маршрут активен и трафик, попадающий под условия маршрута, будет перенаправлен в указанный Шлюз;
- - маршрут не активен и трафик, попадающий под условия маршрута, не будет обработан правилом.

Подсказка: Трафик, не попавший под условия правил маршрутизации, или с объектом **Любой** в качестве шлюза, будет отправлен в *Балансировку и резервирование*.

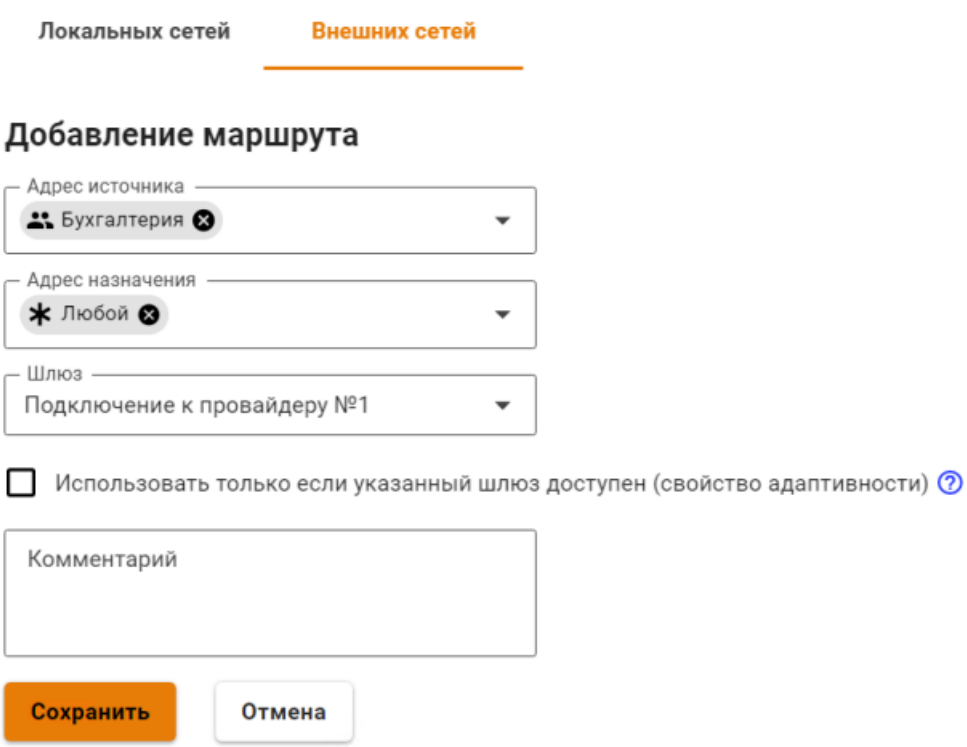
Примеры популярных маршрутов

При маршрутизации трафика через подключения к провайдеру важно понимать, что чаще всего одного маршрута недостаточно. Понадобится также переопределить адрес с помощью SNAT, иначе такой маршрут не будет работать. SNAT можно настроить с помощью *Файрвола*.

Задача: любой трафик в подсеть `150.1.0.0/16` направлять на шлюз `67.12.8.9`:



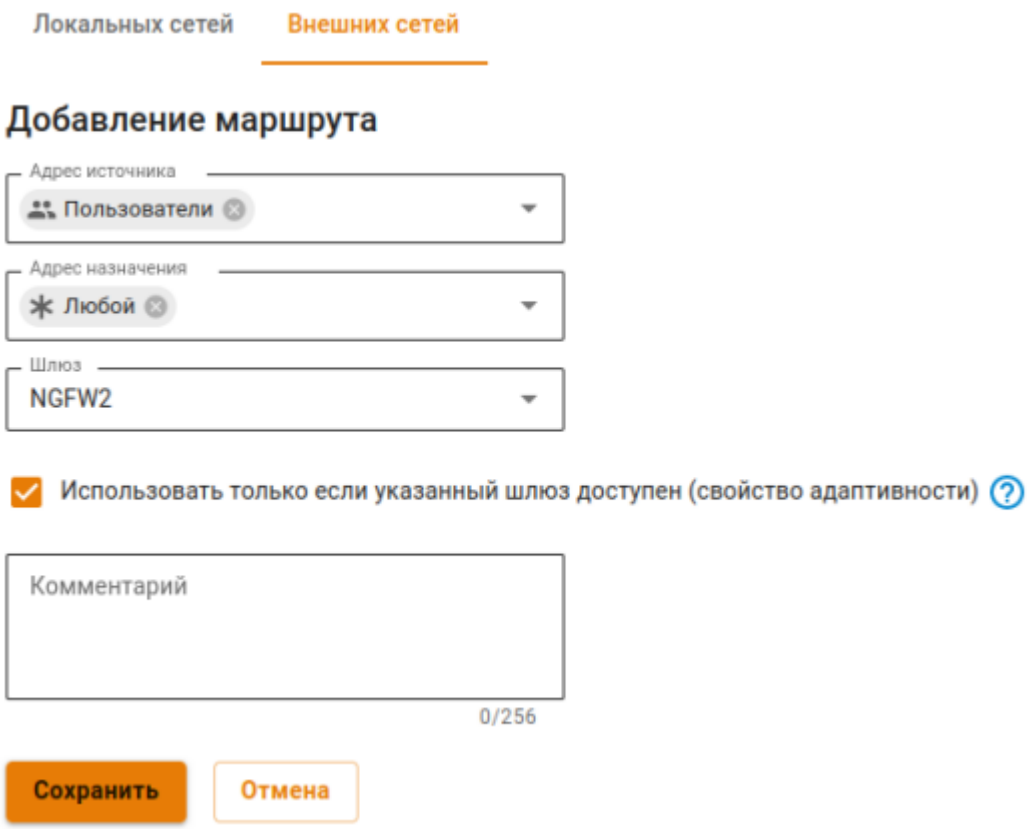
Задача: весь трафик пользователей из группы Бухгалтерия направить через шлюз выбранного сетевого интерфейса:



Если настраивается маршрут в удаленную сеть через дополнительный роутер, расположенный в одной локальной сети с клиентами, то убедитесь, что нет «асимметричной маршрутизации» и роутер вынесен в DMZ. Подробнее в статье *Доступ в удаленные сети через роутер в локальной сети*

Задача: предоставить доступ в интернет пользователям NGFW1, подключенного по IPsec к NGFW2, через внешний интерфейс NGFW2:

Для доступа в интернет пользователям NGFW1 укажите в качестве шлюза IPsec-подключение к NGFW2:



Задача: создать правило маршрутизации до сетей филиала через подключение client-to-site:

Если установка подключения site-to-site до сетей филиала недоступна, в Ideco NGFW можно настроить подключение роутера client-to-site. В этом случае при добавлении маршрута локальных сетей в качестве шлюза используется роутер, который подключается по VPN.

Для настройки подключения выполните действия:

1. В разделе **Пользователи -> Учетные записи** создайте учетную запись для роутера с разрешенным доступом к VPN.

2. При добавлении маршрута в разделе **Сервисы -> Маршрутизация -> Локальных сетей** выберите созданного пользователя в поле **Шлюз**.

Сети за роутером станут доступны после установки VPN-подключения через Ideco NGFW.

Информация об особенностях маршрутизации и организации доступа при настроенном VPN-подключении представлена в *статье*.

18.4 BGP

Подсказка: Название службы раздела **BGP**: `frr.service`; `ideco-routing-backend`.
Список служб для других разделов доступен по *ссылке*.

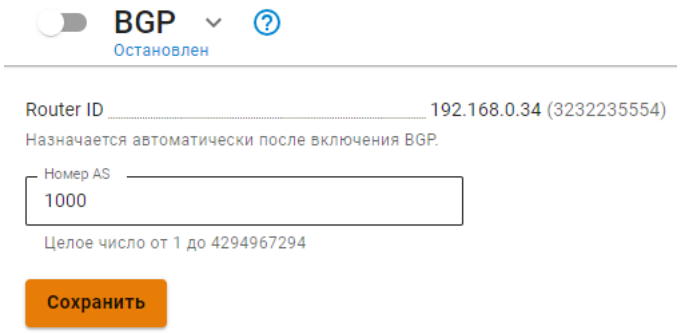
BGP (Border Gateway Protocol) — это основной протокол динамической маршрутизации, который используется в интернете.

Подсказка: При настройке BGP доступны GRE-интерфейсы.

Для запуска сервиса он должен быть не только включен, но и корректно настроен: должен быть создан и включен хотя бы один BGP-сосед.

18.4.1 Настройка своей автономной системы

1. Введите номер автономной системы в строку **Номер AS** и нажмите **Сохранить**:



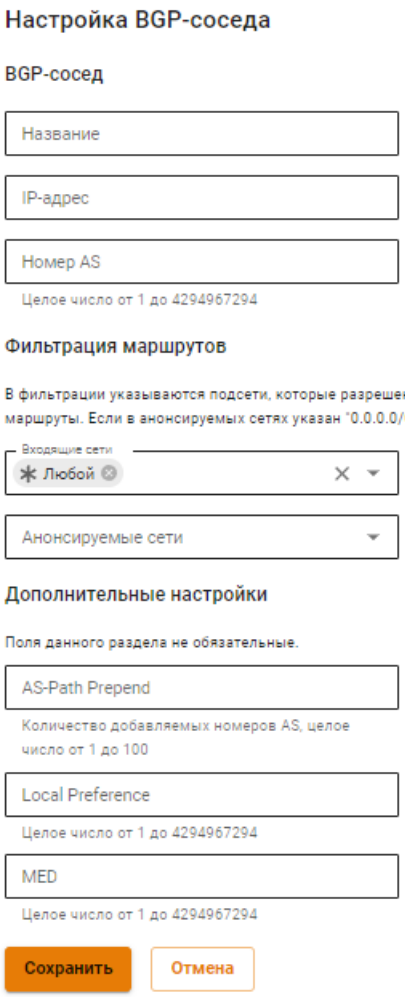
2. Переведите опцию раздела **BGP** в положение **включен**;

3. Ideco NGFW заполнит поле **Router ID** автоматически.

18.4.2 Настройка BGP-соседей

1. Для добавления BGP-соседа нажмите **Добавить** в правом верхнем углу;

2. Заполните поля:



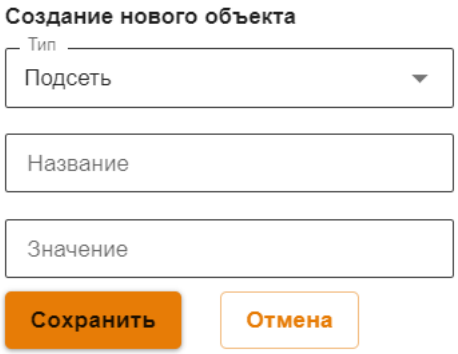
- **Название** - любое значение;
- **IP-адрес** - IP-адрес BGP-соседа;
- **Номер AS** - номер AS BGP-соседа;
- **Входящие сети** - фильтр, в котором нужно выбрать сети, информацию от которых хотите получать. Если выбран объект **Любой**, то фильтрация будет отключена и будут приниматься все сети от BGP-соседа. 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`.

18.5 OSPF

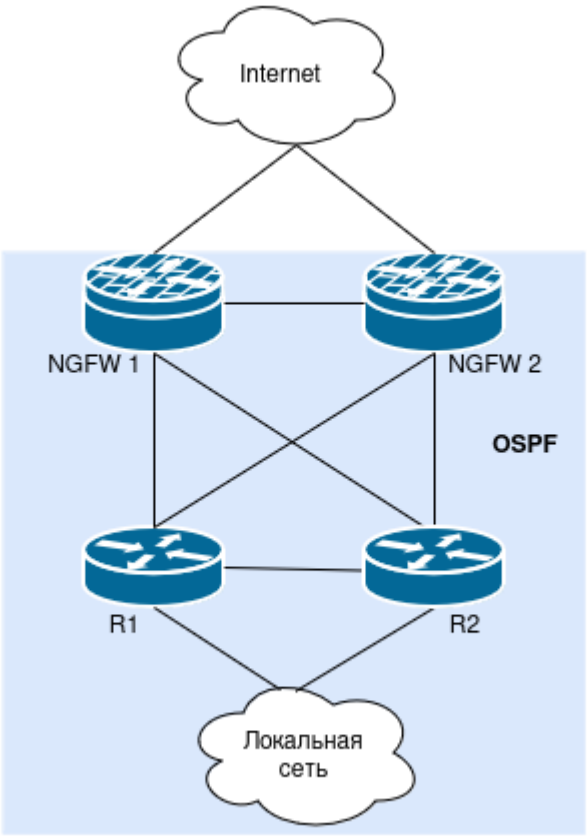
Подсказка: Название службы раздела **OSPF**: `frr.service; ideco-routing-backend`.
Список служб для других разделов доступен по *ссылке*.

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.

Подсказка: При настройке OSPF доступны GRE-интерфейсы.

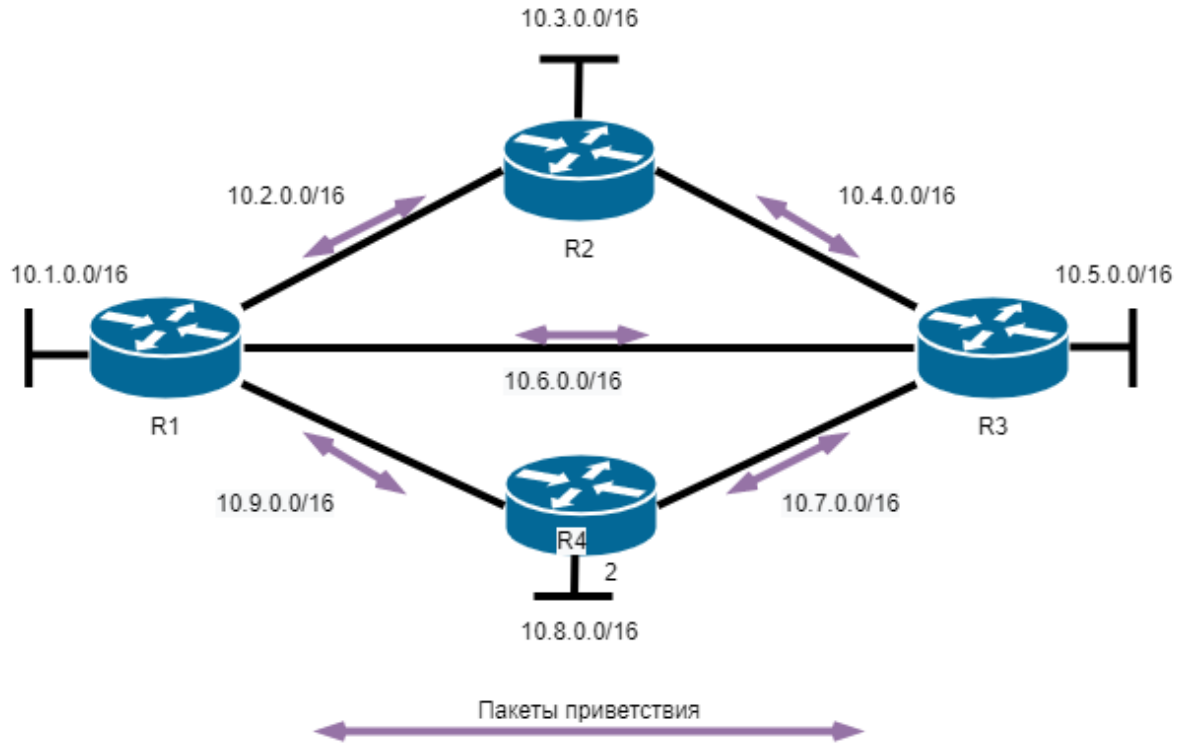
Пример топологии с использованием OSPF представлен на схеме ниже:



Принцип работы маршрутизации по состоянию канала:

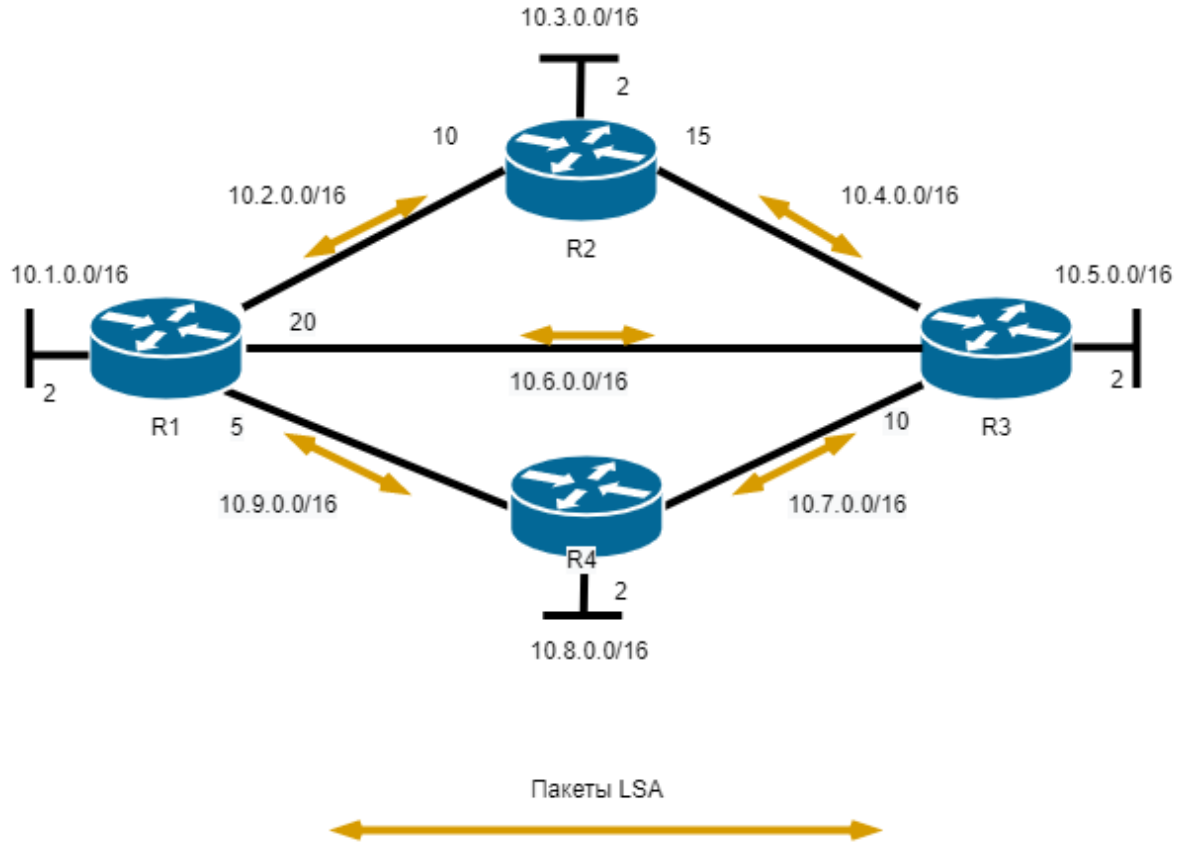
1. Установление отношений смежности с соседними устройствами

Маршрутизатор, использующий OSPF, отправляет hello-пакеты на мультикастовый адрес 224.0.0.5 со всех интерфейсов, где запущен OSPF. При наличии соседнего устройства маршрутизатор пытается установить с ним отношения смежности.



2. Обмен объявлениями о состоянии каналов

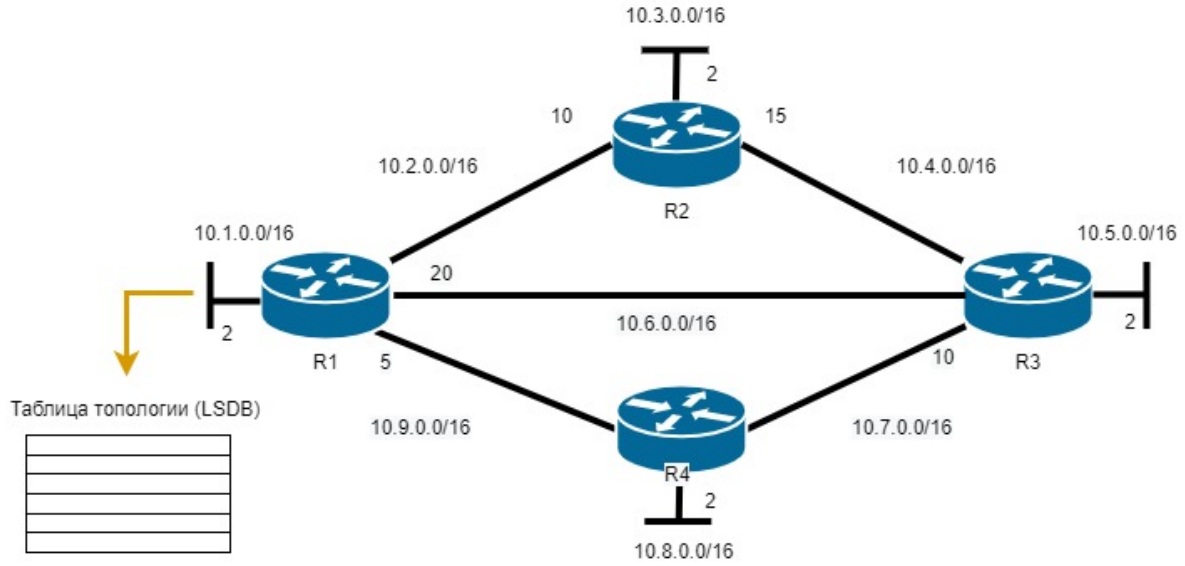
После установления смежности устройства выполняют обмен LSA. LSA содержат информацию о состоянии и стоимости каждого канала с прямым подключением.



3. Создание базы данных состояния связи

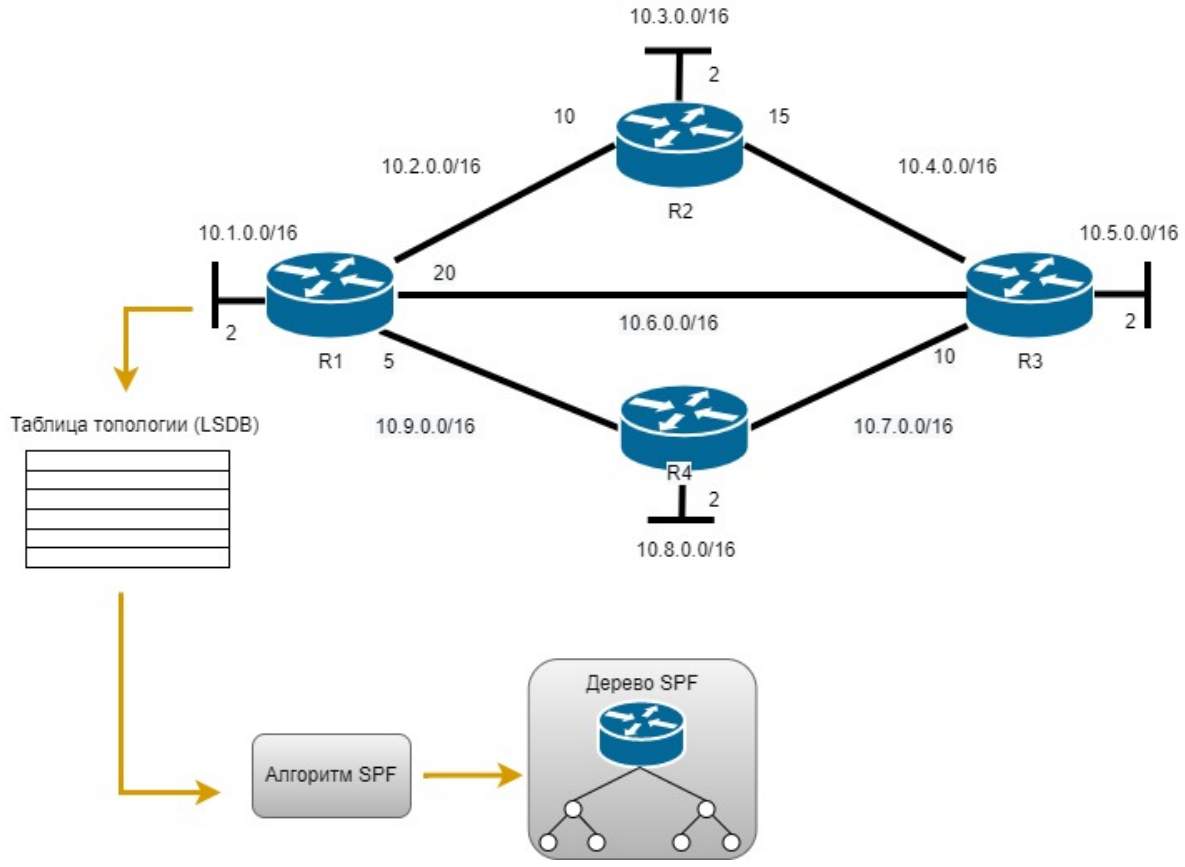
На основе объявления LSA маршрутизаторы собирают базу данных, в которой содержатся данные о топо-

логии сети в области.



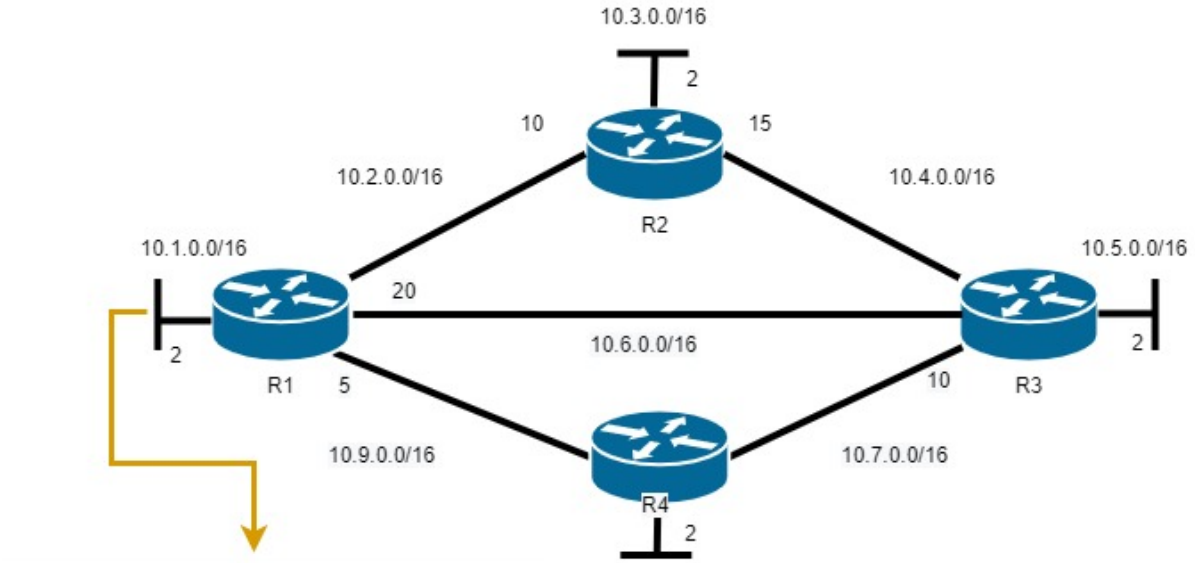
4. Исполнение алгоритма SPF

На устройствах выполняется алгоритм SPF, результатом которого является создание дерева кратчайших путей.



5. Выбор лучшего маршрута

На основании данных дерева SPF обновляются данные в таблице IP-маршрутизации. Маршрут добавляется в таблицу маршрутизации, если отсутствует источник маршрута к той же сети с меньшим административным расстоянием, например, статический маршрут.
Решения по маршрутизации пакетов принимаются на основе записей в таблице маршрутизации.



Название	Кратчайший путь	Стоимость
10.3.0.0/16	R1 -> R2	12
10.4.0.0/16	R1 -> R2	25
10.5.0.0/16	R1 -> R3	22
10.7.0.0/16	R1 -> R4	17
10.8.0.0/16	R1 -> R4	7

18.5.1 Особенности работы OSPF в Ideco NGFW

- Ideco NGFW всегда будет являться шлюзом по умолчанию для других устройств. Считать другие устройства шлюзом по умолчанию NGFW не сможет;
- OSPF работает только на локальных интерфейсах. Локальными считаются локальные *Ethernet-интерфейсы*, *GRE*;
- Значение *Типа сети* (*Network Type*) в Ideco NGFW устанавливается автоматически в зависимости от типа интерфейса, используемого для OSPF: для GRE-интерфейсов - значение p2p, для Ethernet-интерфейсов - значение broadcast.

18.5.2 Основное

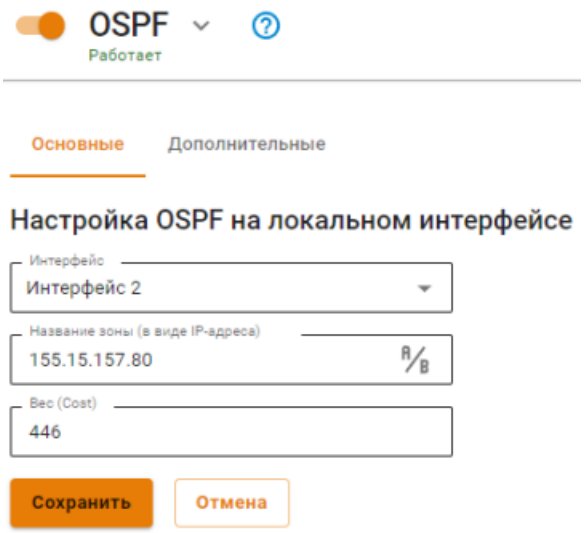
Настройка Ideco NGFW

Router ID - IP-адрес маршрутизатора. Присваивается автоматически в виде самого большого IP-адреса локальной сети, заданной в разделе *Сетевые интерфейсы*.

Для того чтобы настроить OSPF на NGFW, выполните действия:

1. В веб-интерфейсе NGFW перейдите в раздел **Сервисы –> OSPF –> Основные** и нажмите кнопку **Добавить**.

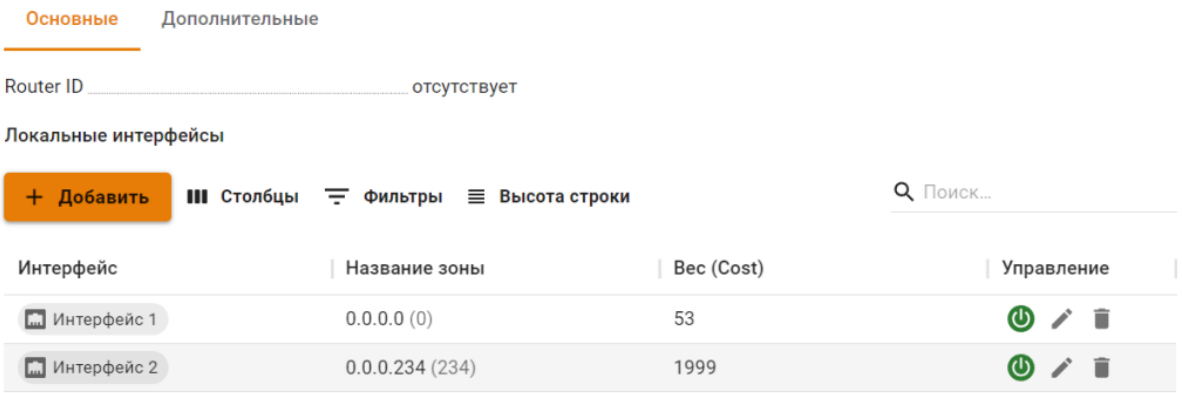
2. Заполните поля:



- **Интерфейс** - выберите локальный интерфейс Ideco NGFW, IP-адрес которого будет использован для обмена маршрутами;
- **Название зоны** - введите номер зоны (значение `area`, для небольших сетей введите 0). Можно ввести в виде числа или IP-адреса, нажав иконку A/B ;
- **Вес** - введите стоимость маршрута.

3. Нажмите **Сохранить.**

Пример готовой таблицы:



При наличии большого количества настроек OSPF в таблице воспользуйтесь кнопкой **Фильтры**.

Настройка MikroTik:

1. Авторизуйтесь на MikroTik и выполните команду:

```
routing ospf area add area-id=x.x.x.x default-cost=1 disabled=no inject-summary-lsa=no
name=area1 type=default
```

- `x.x.x.x` - **название зоны, которое указали при настройке Ideco NGFW**. ID должен быть уникален для каждого роутера;

2. Для передачи любых других сетей соседним устройствам по динамической маршрутизации введите команду:

```
routing ospf network add network=(другая подсеть)/24 area=area1
```

3. Повторите команду из п. 1 для добавления каждой подсети;

4. Для вывода таблицы маршрутизации введите команду:

```
ip route print
```

Настройка Cisco:

1. Настройте локальный интерфейс Cisco:

```
enable
conf t
interface GigabitEthernet0/1
ip address <локальный IP Cisco> <маска подсети>
no shutdown
exit
```

2. Настройте внешний интерфейс Cisco:

```
enable
conf t
interface GigabitEthernet0/0
ip address <внешний IP Cisco> <маска подсети>
no shutdown
exit
```

3. Проверьте наличие связи между Ideco NGFW и Cisco. Для этого в консоли Cisco используйте команду `ping <внешний IP NGFW>`. Результат вывода команды - наличие ICMP-ответов.

4. Сохраните настройки конфигурации:

```
write memory
```

5. Запустите на Cisco процесс OSPF:

```
enable
conf t
router ospf 1
```

6. По умолчанию отключите отправку hello-пакетов на всех интерфейсах и включите на нужных интерфейсах:

```
passive-interface default
no passive-interface GigabitEthernet0/0
```

- `GigabitEthernet0/0` - название интерфейса.

7. Укажите сети, маршруты до которых хотите анонсировать:

```
network <IP-адрес подсети> <wildcart-маска подсети> area <номер зоны, указанный при␣
↪настройке Ideco NGFW>
```

Пример команды:

```
network 192.168.100.0 0.0.255.255 area 0
```

8. Если Cisco получил уведомление вида `*Dec 18 10:02:03.628: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.122.73 on GigabitEthernet0/0 from LOADING to FULL, Loading Done`, соседские отношения установлены.

9. Для просмотра списка соседей воспользуйтесь командой `show ip ospf neighbor`:

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.122.73    1   FULL/DR         00:00:38    192.168.102.11  GigabitEthernet0/0
Router#
```

10. Для вывода таблицы маршрутизации введите команду `show ip route` (в таблице должны появиться маршруты до сетей NGFW):

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.102.11 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      10.0.0.0/16 is subnetted, 1 subnets
O E2     10.128.0.0 [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.100.0/32 is subnetted, 1 subnets
O E2     192.168.100.100
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
      192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.102.0/24 is directly connected, GigabitEthernet0/0
L        192.168.102.79/32 is directly connected, GigabitEthernet0/0
      192.168.103.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.103.0/24 is directly connected, GigabitEthernet0/1
L        192.168.103.130/32 is directly connected, GigabitEthernet0/1
O E2  192.168.122.0/24
           [110/1] via 192.168.102.11, 00:00:52, GigabitEthernet0/0
```

18.5.3 Дополнительное

На вкладке доступны к установке следующие флаги:

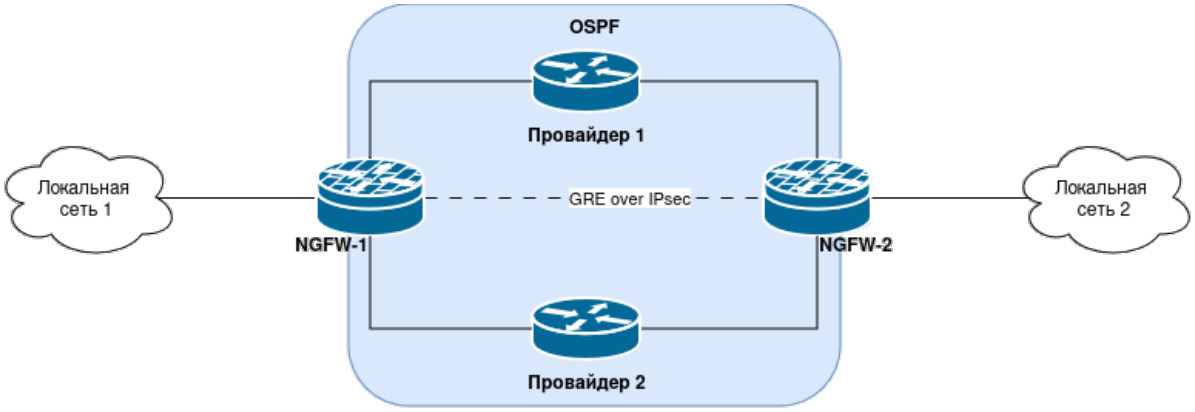
- **Redistribute default** - будут анонсироваться маршруты по умолчанию. Устройство, принявшее эту информацию, будет отправлять на NGFW весь трафик;
- **Redistribute static** - будут анонсироваться статические маршруты, указанные на вкладке **Сервисы -> Маршрутизация -> Локальных сетей**;
- **Redistribute connected** - будут анонсироваться маршруты подсетей, подключенных напрямую.

Подробнее о значении поля **Метрика** - в статье.

Подсказка: Для передачи маршрутов до VPN-сети через OSPF необходимо в разделе **OSPF -> Дополнительные** включить чек-бокс **Redistribute static (передача статических маршрутов)**.

18.5.4 Примеры использования

1. Объединение филиальной сети с резервированием и/или балансировкой

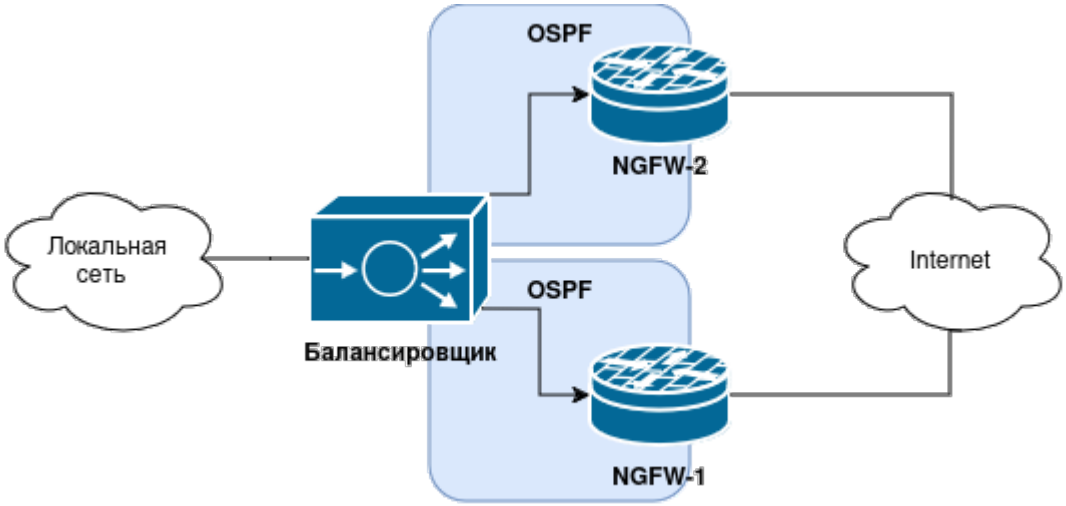


- Между **NGFW-1** в Филиале 1 и **NGFW-2** в Филиале 2 настраивается GRE-over-IPsec и OSPF;
- Каждый NGFW подключен к двум провайдерам (**Провайдер-1** и **Провайдер-2**).

Преимущества настройки:

- Трафик будет автоматически балансироваться между **Провайдером-1** и **Провайдером-2**;
- При неисправности одного из провайдеров трафик автоматически смаршрутизируется через другое соединение;
- Отсутствует необходимость вручную настраивать маршруты до локальных сетей филиалов.

2. Схема с балансировкой доступа из локальной сети в интернет или другую сеть



- И **NGFW-1**, и **NGFW-2** используются в качестве шлюза по умолчанию;
- Между балансировщиком и каждым из NGFW настроена OSPF.

Преимущества настройки:

- Трафик балансируется между **NGFW-1** и **NGFW-2**: часть пользователей из Локальной сети выходят в интернет через **NGFW-1**, часть - через **NGFW-2**;

- При неисправности одного из NGFW трафик автоматически смаршрутизируется через другое соединение;
- Отсутствует необходимость вручную настраивать маршруты для хостов в Локальной сети.

18.6 IGMP Proxy

Подсказка: Название службы раздела **IGMP Proxy**: `igmpproxy`.
Список служб для других разделов доступен по *ссылке*.

Подсказка: IGMP Proxy работает только с Ethernet-интерфейсами и не работает на интерфейсах VLAN, PPPoE или VPN (L2TP, PPTP).

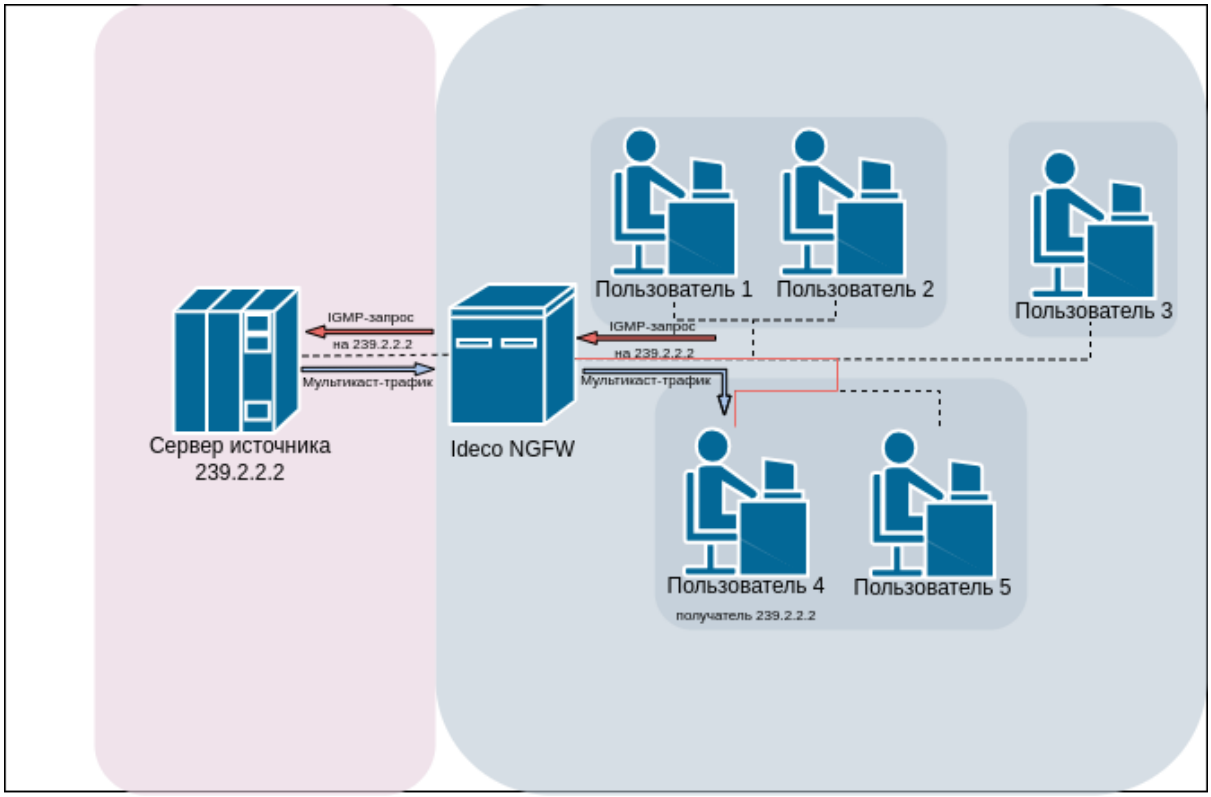
IGMP Proxy - служба, которая проксирует (передает) мультакаст-трафик сквозь роутер. Это сокращает объем трафика, что влияет на скорость работы и нагрузку сети.

18.6.1 Принцип работы

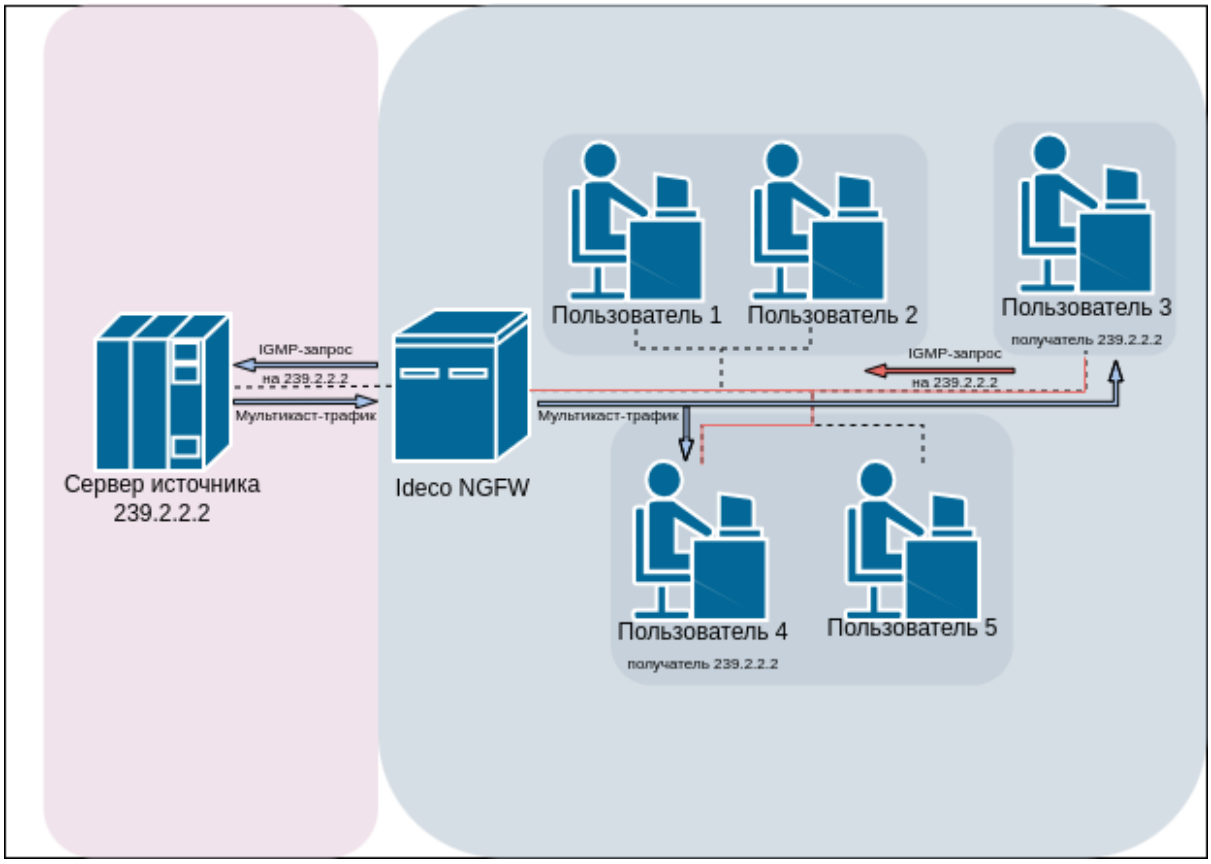
Со стороны клиентов IGMP Proxy поддерживает версии IGMPv1 и IGMPv2.

Принцип работы на примере подключения двух пользователей к мультикаст-потоку одного источника:

- *Сервер источника* начинает трансляцию мультикаст-трафика с адреса из диапазона 224.0.0.0/4.
- *Пользователь 4* хочет подключиться к трафику и генерирует IGMP-запрос (Join) на *Ideco NGFW* для получения мультикаст-трафика от сервера источника.
- *Ideco NGFW* получает IGMP-запрос и отправляет аналогичный запрос к серверу источника;
- Сервер источника получает запрос и начинает транслировать мультикаст-трафик на *Ideco NGFW*;
- *Ideco NGFW* пропускает трафик с адреса 239.2.2.2 в подсеть с *Пользователем 4*, и *Пользователь 4* становится его получателем.



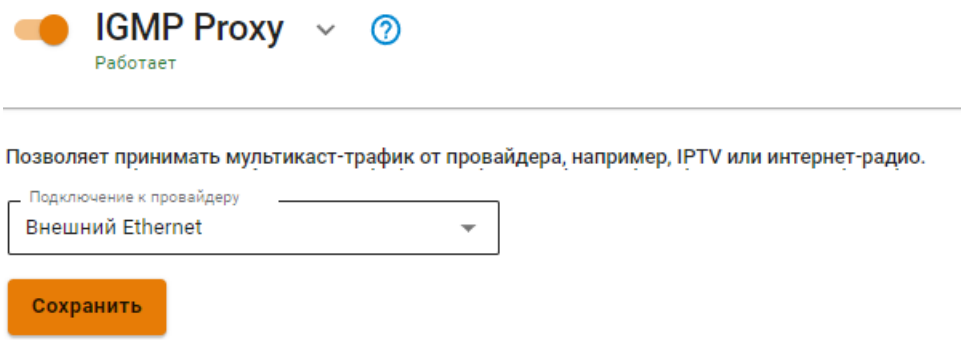
- *Пользователь 3*, находящийся в другой подсети, также решает подключиться к этой трансляции и генерирует IGMP-запрос (Join) на Ideco NGFW;
- *Ideco NGFW* получает этот запрос и дублирует *Пользователю 3* трафик, поступающий *Пользователю 4*;



Ideco NGFW периодически проверяет, есть ли получатели, отправляя пользователям IGMP-запрос (Query). Пользователи в ответ отправляют Join, как при подключении.
Если на Ideco NGFW приходит хотя бы один Join, то мультикаст-трафик продолжает транслироваться получателям.

18.6.2 Настройка в Ideco NGFW

Для настройки перейдите в раздел **Сервисы -> IGMP Proxy**. Переведите опцию **IGMP Proxy** в положение **Включен**. В строке **Подключение к провайдеру** выберите Ethernet-подключение.



18.7 Прокси

Подсказка: Название службы раздела **Прокси**: `ideco-proxy-backend`; `squid`.
Список служб для других разделов доступен по *ссылке*.

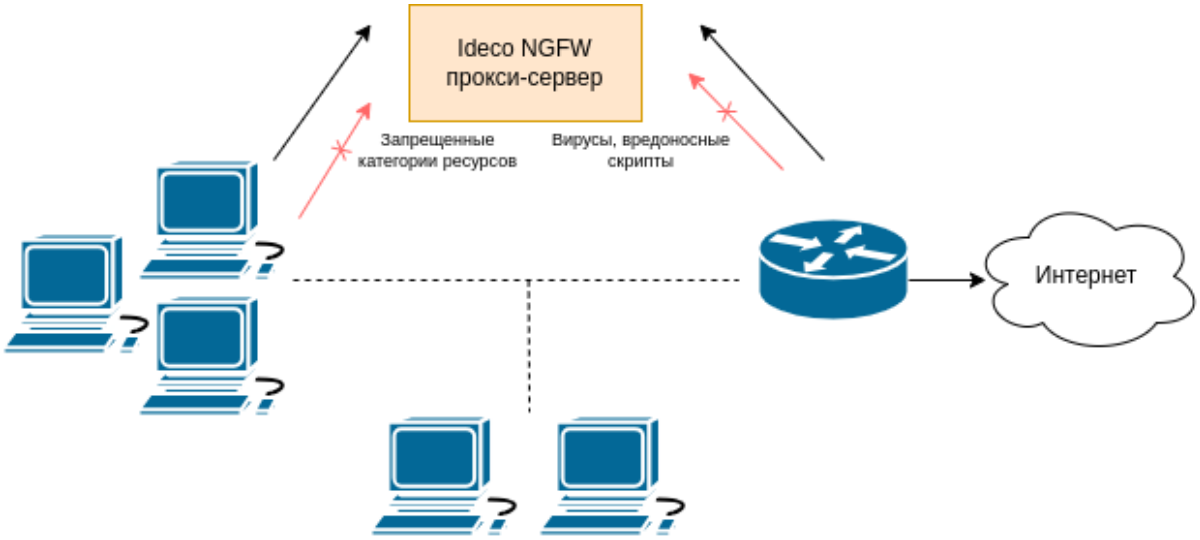
Прокси-сервер, помимо проксирования веб-трафика, используется для передачи трафика следующим сервисам:

- 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*.



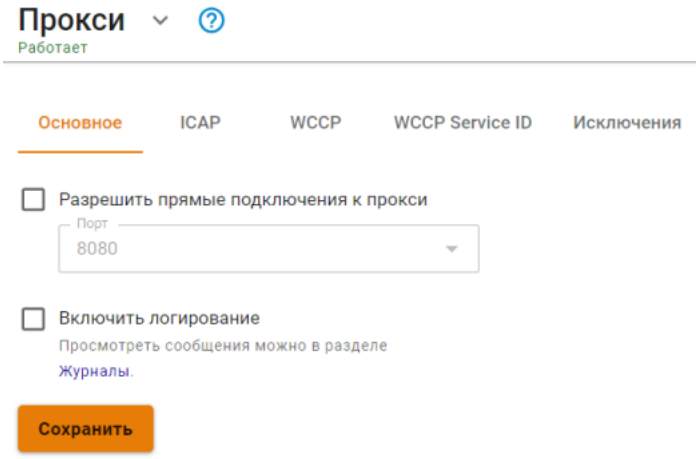
При использовании Ideco NGFW в качестве прокси-сервера с прямыми подключениями к прокси большинство функций будет работать с некоторыми особенностями:

- 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.

18.7.1 Основное

На вкладке **Основное** предоставлены возможности:

- **Разрешить прямые подключения к прокси**
  Этот режим применяется, когда Ideco NGFW не является шлюзом по умолчанию для клиентов сети. Порт, указанный на стороне NGFW, следует указать на сетевых устройствах локальной сети, веб-трафик которых нужно пропускать через прокси.
- **Включить журналирование**
  Включает запись логов Контент-фильтра и Антивирусов веб-трафика.



О настройке прямого подключения к прокси и прокси с одним интерфейсом читайте в *статье*.

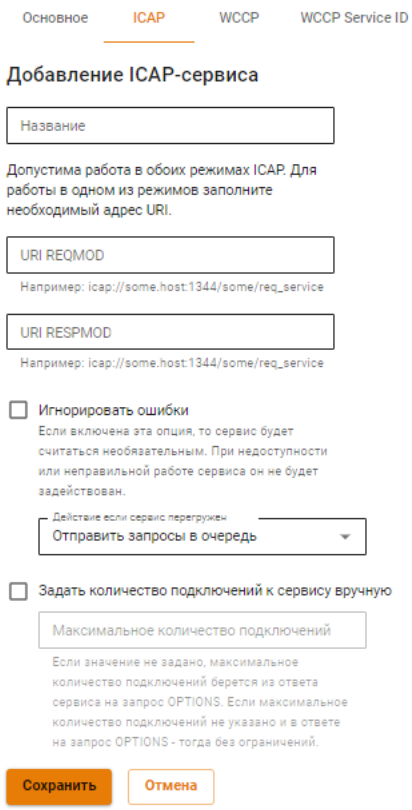
18.7.2 ICAP

Протокол ICAP используется для отправки HTTP(S)-трафика в расшифрованном виде сторонним серверам. ICAP-сервисы будут обрабатывать трафик после антивирусов и контент-фильтра.

При добавлении ICAP-сервиса доступны следующие настройки:

- **Игнорировать ошибки** - если включена эта опция, то сервис будет считаться необязательным. При недоступности или неправильной работе сервиса он не будет задействован.
- **Задать количество подключений к сервису вручную** - если значение не задано, максимальное количество подключений берется из ответа сервиса на запрос OPTIONS. Если максимальное количество подключений не указано в ответе на запрос OPTIONS, тогда - без ограничений.

Предупреждение: Если указать в опции **Задать количество подключений к сервису вручную** значение меньше четырех, то клиентские подключения могут быть нестабильными.



Подсказка: Для корректной работы ICAP-сервиса должна быть настроена расшифровка HTTPS-трафика в **Контент-фильтре**.

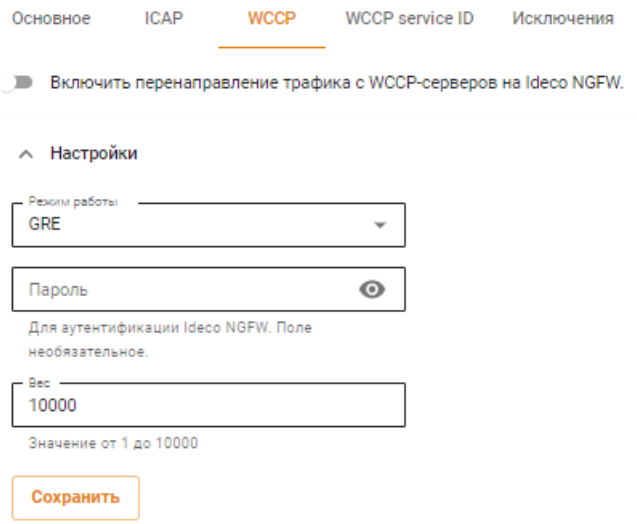
18.7.3 WCCP

Протокол WCCP используется для перенаправления трафика на Ideco NGFW.

По умолчанию перенаправляется только HTTP/HTTPS-трафик.

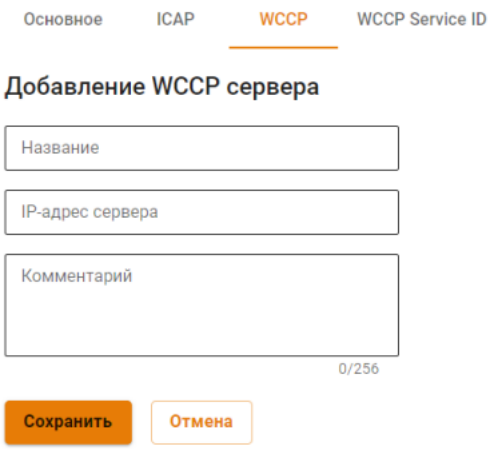
Для активации WCCP переведите опцию **Включить перенаправление трафика с WCCP-серверов на Ideco NGFW** в положение **Включен**. Ideco NGFW запустит процесс согласования параметров с WCCP-сервером.

В NGFW предусмотрено два режима работы WCCP - L2 и GRE. Для выбора режима раскройте блок **Настройки**.
Если на WCCP-сервере задан пароль, сохраните его в соответствующем поле:



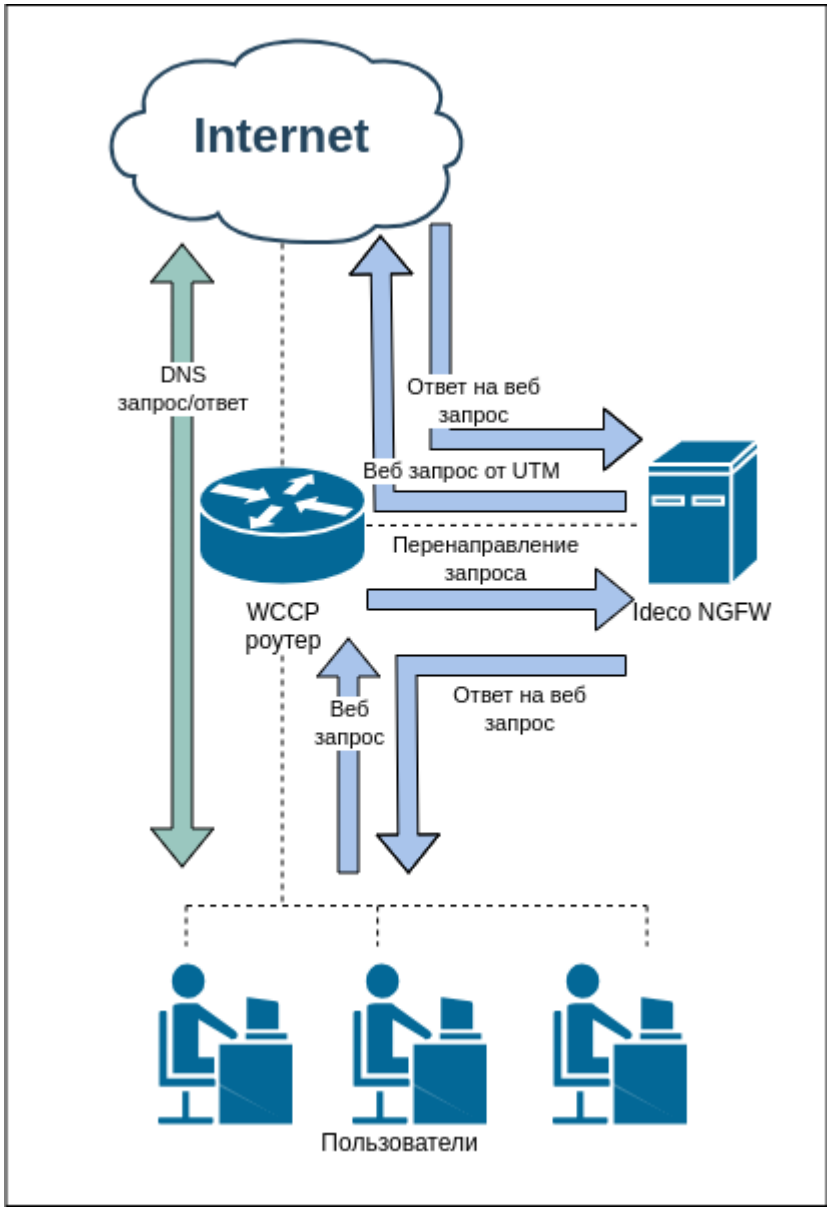
Если роутер использует несколько Ideco NGFW, настройте распределение трафика с помощью указания приоритета в поле **Вес**. Допустимые значения - от 1 до 10000.

Для добавления WCCP-сервера нажмите кнопку **Добавить** и укажите IP-адрес сервера:



L2:

Режим L2 используется, если роутер и Ideco NGFW находятся в одном сетевом сегменте.



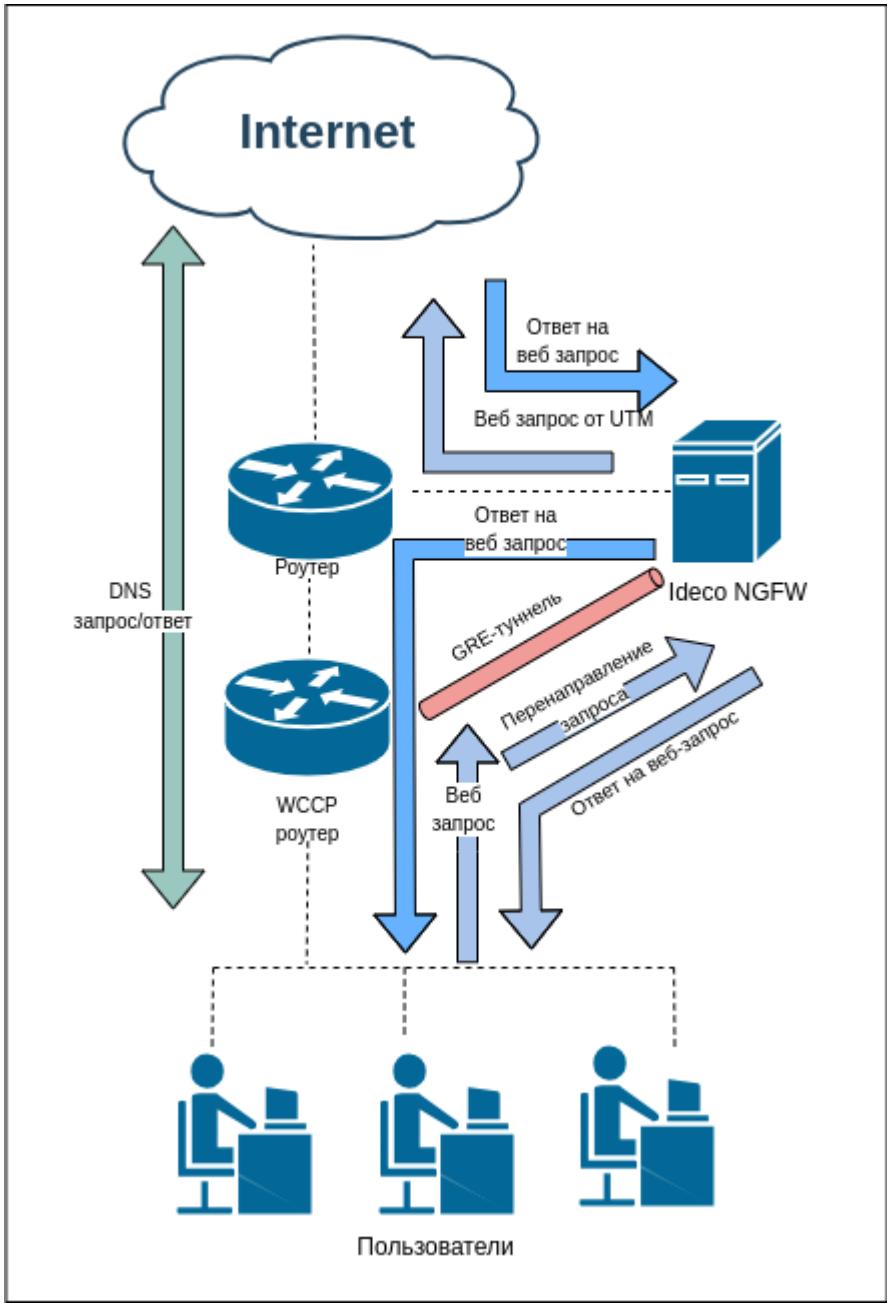
Последовательность обработки веб-запросов на уровне L2:

- Пользователь отправляет веб-запрос;
- Запрос перенаправляется роутером на Ideco NGFW;
- Ideco NGFW обрабатывает запрос;
- Если запрос заблокирован, информация о блокировке отправляется обратно пользователю;
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается обратно по тому же пути, по которому уходил на внешний сервер.

GRE:

Режим GRE используется, если роутер и Ideco NGFW находятся в разных сетевых сегментах.



Последовательность обработки веб-запросов на уровне GRE:

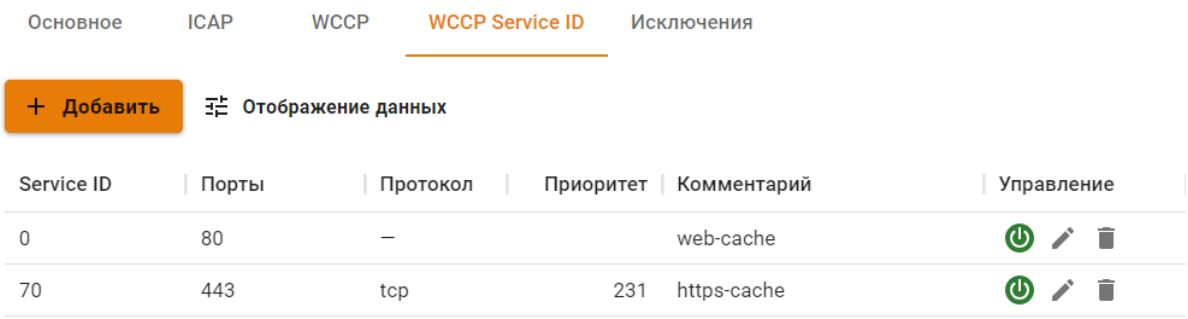
- Пользователь отправляет веб-запрос;
- Запрос перенаправляется по GRE-туннелю на Ideco NGFW;
- Ideco NGFW обрабатывает запрос.
- Если запрос заблокирован, то информация о блокировке отправляется обратно пользователю.
- Если запрос не заблокирован, то Ideco NGFW подменяет IP-адрес источника и направляет запрос на внешний сервер.

Ответ возвращается напрямую от Ideco NGFW пользователю, минуя GRE-туннель.

18.7.4 WCCP Service ID

Service ID - идентификаторы сервисной группы. Настройки на этой вкладке позволяют выбрать службы, трафик которых маршрутизатор WCCP будет перенаправлять на Ideco NGFW.

По умолчанию настроены сервисы для HTTP/HTTPS-трафика:



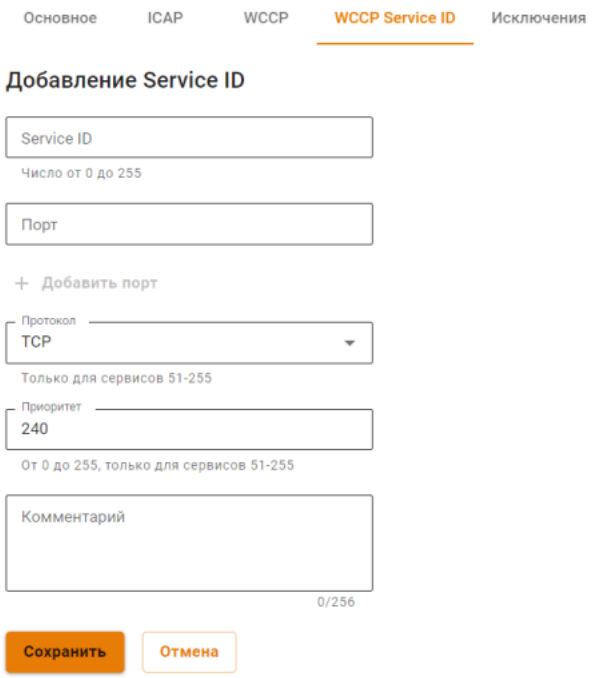
Предупреждение: Service ID с 0 по 50 зарезервированы под фиксированные сервисы. Для них выбирать порты и протоколы нельзя.

Service ID 70 - общепринятое значение для HTTPS-трафика на 443 TCP-порт.

Чтобы настроить Service ID, выполните действия:

1. На вкладке **WCCP Service ID** нажмите кнопку **Добавить**.

2. В открывшейся форме укажите следующие значения:

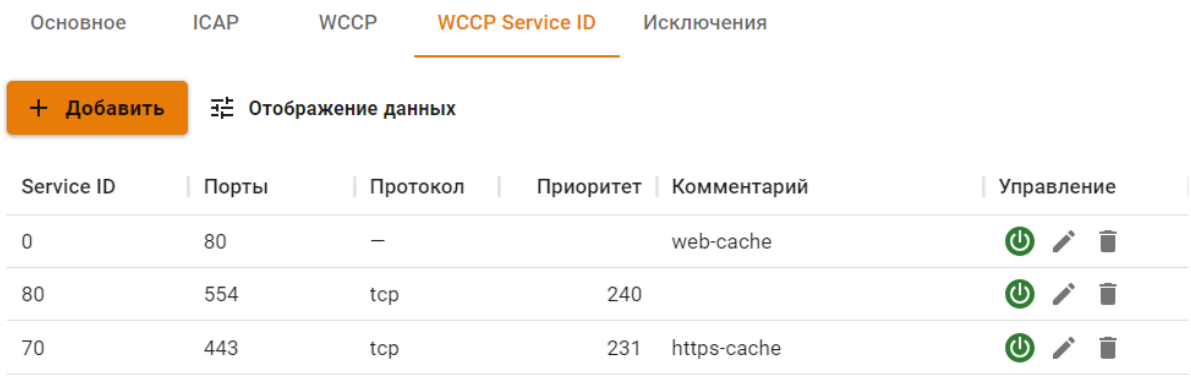


- **Service ID** - идентификатор сервисной группы, трафик которой планируется перенаправлять на прокси-сервер. Выбирайте значения от 51 до 255, чтобы избежать проблем со старыми маршрутизаторами WCCP.
- **Порты** - укажите порты назначения. Максимум 8 значений.
- **Протокол** - укажите протокол для перенаправляемого трафика (TCP, UDP).

- **Приоритет** - укажите приоритет Service ID от 0 до 255. Чем больше число, тем выше приоритет.

Внимание: Service ID должен должен соответствовать идентификатору группы, определенному на маршрутизаторе WCCP.

3. Нажмите **Сохранить**. Созданный Service ID появится в таблице:



18.7.5 Исключения

Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

Подробнее о типах исключений в статье *Исключения*.

18.7.6 Исключения

Подсказка: Исключения ресурсов из обработки прокси-сервером работают только для прозрачного режима прокси. При прямых подключениях к прокси-серверу исключить что-либо из обработки прокси нельзя.

На вкладке **Исключения** можно исключить ресурсы из обработки прокси-сервером и всеми связанными службами (контент-фильтр, веб-отчетность, антивирусы):

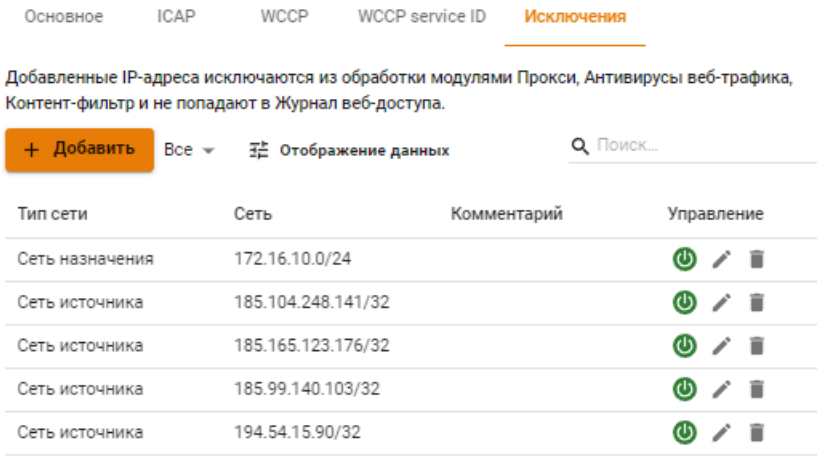
- **Сети источника** - указываются сети, трафик из которых исключается из обработки прокси-сервером;
- **Сети назначения** - указываются внешние сети или IP-адреса (как правило, адреса веб-сайтов или веб-сервисов), трафик до которых из всех локальных сетей NGFW исключается из обработки прокси-сервером.

Внимание: Настоятельно не рекомендуем исключать из обработки прокси-сервером ВСЮ локальную сеть.

Подсказка: При прямом подключении к прокси-серверу нельзя исключить трафик из обработки прокси. Исключать трафик нужно в настройках прокси-сервера на устройстве (в веб-браузере или системных настройках прокси-сервера).

При создании исключений можно указывать только IP-адреса или IP-сети.

Трафик, исключенный из обработки прокси, не будет участвовать в **Отчетах**, проверяться на вирусы и обрабатываться модулем **Контент-фильтра**. В то же время такой трафик будет проверен **Файрволом**, модулями **Предотвращение вторжений** и **Контроль приложений**.



Поиск по таблице исключений

Над таблицей исключений расположена строка поиска. Она позволяет искать среди исключений определенные IP-адреса и сети. Для поиска начните вводить требуемый IP-адрес:

Таблица будет динамически изменяться, отфильтруются только строки, 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.

18.7.7 Настройка прямого подключения к прокси

Настройка прямого подключения к прокси

Для настройки выполните действия:

1. Укажите IP-адрес локального интерфейса Ideco NGFW в качестве веб-прокси в локальной сети на клиентских устройствах;

2. В настройках прокси на Ideco NGFW укажите порт для прямых подключений к прокси (возможен выбор портов из списка: 3128, 1080, 8000, 8080, 8888, 8081, 8088, 10080).

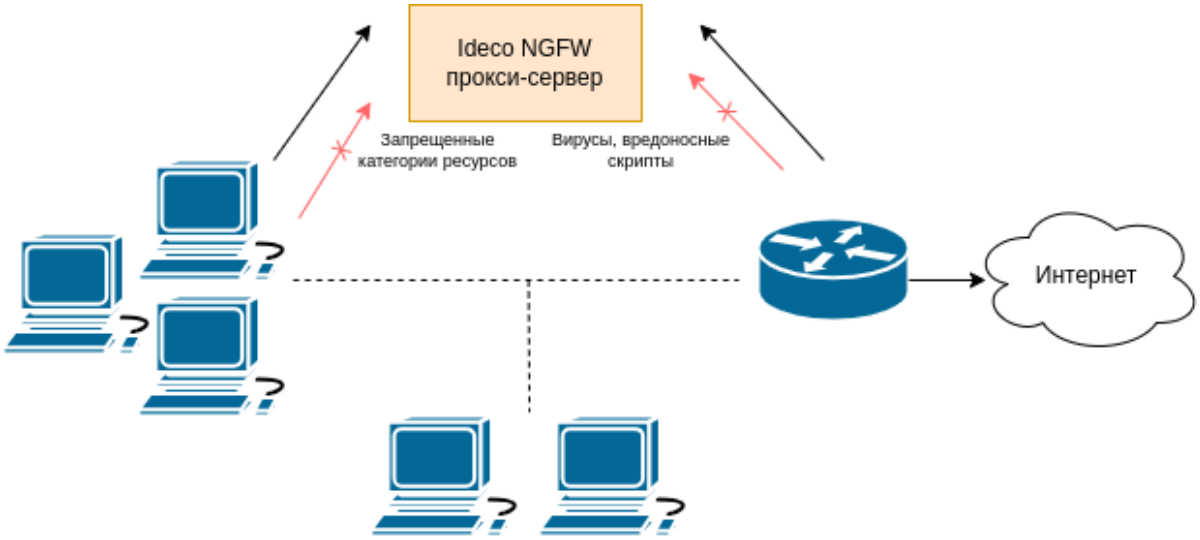
В таком режиме NGFW сможет предоставлять клиентским устройствам веб-трафик по другим портам (по умолчанию - по всем, при необходимости можно закрыть порты файрволом).

Подсказка: Если прямое подключение к прокси требуется только части клиентских устройств или части локальных интерфейсов, то создайте INPUT-правило файрвола.

Подсказка: Если подключиться напрямую к прокси, не указав шлюз на компьютере пользователя, и включив в **Контент-фильтре** расшифровку всех запросов, то аудио- и видеозвонки могут не работать.

Для учета, контроля и проверки веб-трафика на вирусы, требуется соблюдение следующих условий:

- Локальная подсеть не пересекается с внешним интерфейсом NGFW;
- У сервера Ideco NGFW есть доступ в интернет;
- На клиентских устройствах указан адрес веб-прокси (в настройках прокси-сервера в браузерах).



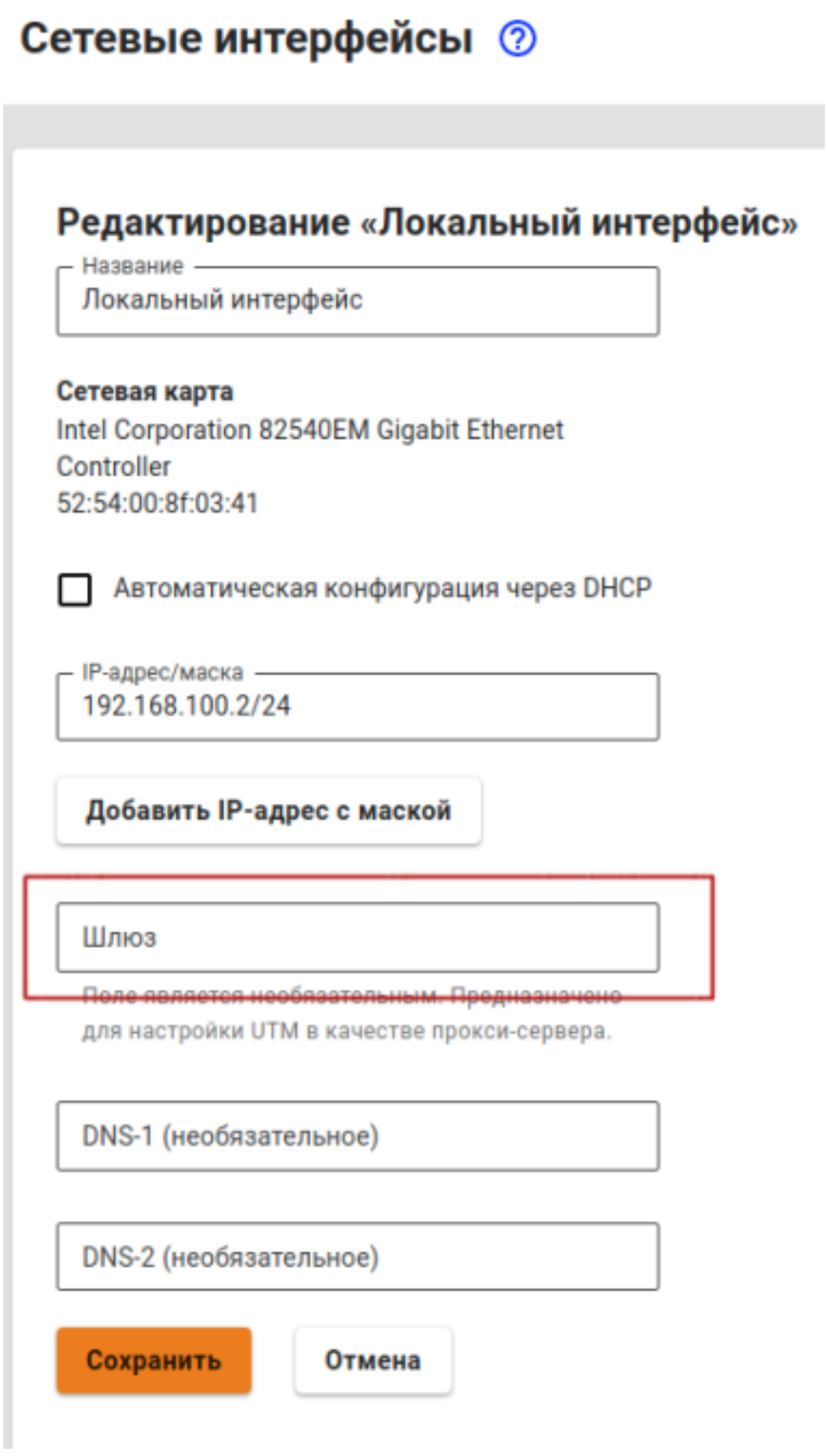
Если в настройках программы под ОС Windows или MacOS X нет возможности указать прокси-сервер, воспользуйтесь сторонним ПО для маршрутизации всего трафика рабочей станции на прокси-сервер. Такую возможность предоставляет программа **Proxifier**, которую можно настроить для прямых подключений к прокси, воспользовавшись *статьей*.

18.7.8 Настройка прокси с одним интерфейсом

Настройка прокси с одним интерфейсом

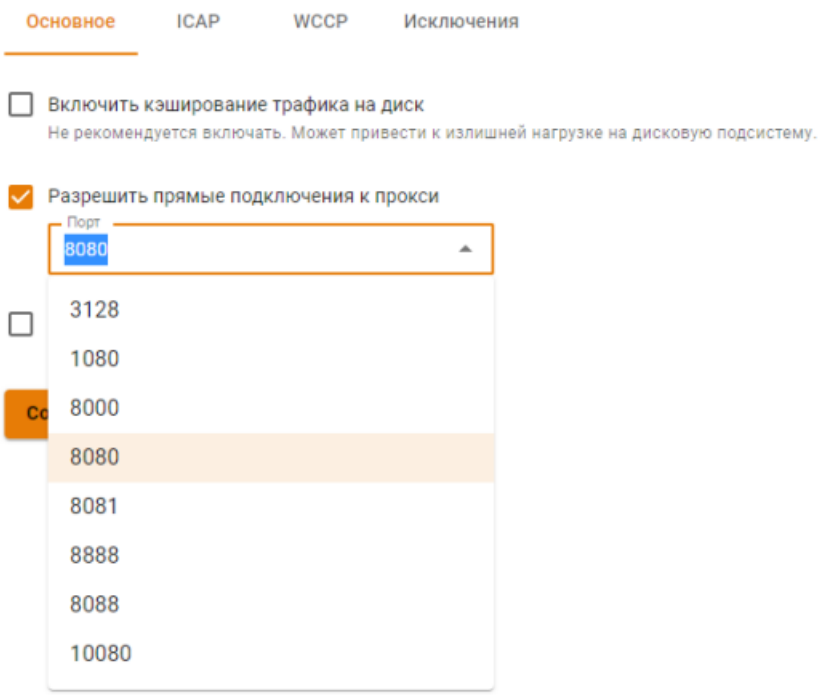
При необходимости можно использовать Ideco NGFW в качестве прокси-сервера с прямыми подключениями клиентов к прокси, с одним интерфейсом. Для этого выполните действия:

1. При создании локального интерфейса в разделе **Сервисы -> Сетевые интерфейсы** укажите **Шлюз**:



2. Разрешите прямые подключения к прокси-серверу в разделе **Сервисы -> Прокси**, выбрав нужный порт

из списка:



18.8 Обратный прокси

Подсказка: Название службы раздела **Обратный прокси**: `ideco-reverse-backend`.
Список служб для других разделов доступен по *ссылке*.

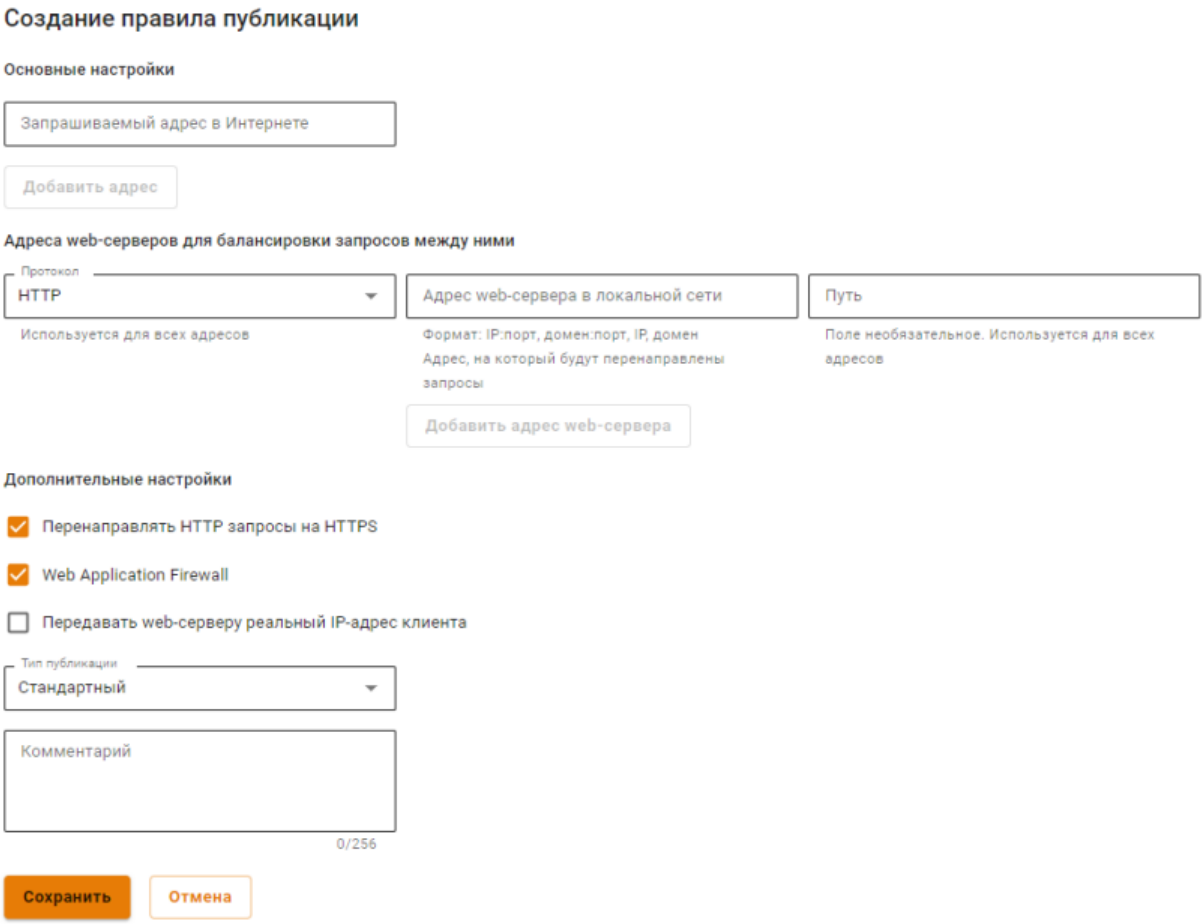
Технология обратного прокси позволяет проксировать веб-трафик из сети интернет в локальную сеть. Отличается от DNAT тем, что работает на более высоком уровне (прикладной протокол HTTP вместо сетевого протокола IP) и позволяет более гибко реализовать публикацию ресурсов.

Обратный прокси позволяет смаршрутизировать запрос на HTTP-сервер в локальной сети из внешней сети. Таким образом, имея одну ресурсную A-запись для внешнего сетевого интерфейса NGFW, можно опубликовать несколько ресурсов в локальной сети, распределив их по нескольким входящим URL.

18.8.1 Создание и настройка правила

Настройка сертификатов для публикуемых ресурсов не требует их ручной загрузки. Ideco NGFW сам отправляет запрос на выпуск сертификата Let's Encrypt. Выпуск сертификата может занять до 20 минут. Выпущенные сертификаты будут доступны в разделе *Сертификаты*.

Для создания правила перейдите в раздел **Сервисы -> Обратный прокси** и нажмите на кнопку **Добавить**. Форма добавления правила разделена на два подраздела: **Основные настройки**, **Адреса web-серверов для балансировки запросов между ними** и **Дополнительные настройки**.



Основные настройки

- **Запрашиваемый адрес в интернете** - введите IP-адрес, доменное имя или URL, который будет запрашиваться пользователями. Для добавления дополнительных адресов нажмите кнопку **Добавить адрес**.

Предупреждение: Если в поле **Запрашиваемый адрес в интернете** нескольких правил будет указан один и тот же IP-адрес/доменное имя/URL, то сработает только одно из созданных правил.

Если нужно создать несколько правил для одного и того же IP-адреса/доменного имени, в поле **Запрашиваемый адрес в интернете** разных правил должны быть указаны разные пути после IP-адреса/доменного имени.

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.

Подсказка: Если указать в поле **Запрашиваемый адрес в интернете** *0.0.0.0*, перенаправление будет работать со всех внешних IP-адресов Ideco NGFW на адрес из поля **Адрес web-сервера в локальной сети**.

Чтобы перенаправление работало с доменов Ideco NGFW на адрес из поля **Адрес web-сервера в локальной**

сети, необходимо явно указать домены в поле **Запрашиваемый адрес в интернете**.

Дополнительные настройки

- 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

Нами протестирована и официально поддерживается публикация сайтов на двух популярных CMS: **Joomla** и **Wordpress**. Подробности публикации каждой CMS описаны ниже.

Joomla:

Joomla в текущей реализации публикуется, если настроить перенаправление с внешнего домена на локальный домен без префикса:

- Ассоциировать с внешним адресом NGFW дополнительное доменное имя специально для публикации Joomla: `joomla.mydomain.ru`;
- Настроить правило публикации `joomla.mydomain.ru` -> `joomla.local:port` (порт не обязателен).

WordPress:

WordPress в текущей реализации публикуется только в конфигурации, когда в WordPress и в обратном прокси настроен один и тот же домен:

- Для домена компании добавить A-запись `wordpress.mydomain.ru`, указывающую на внешний IP-адрес NGFW;
- На локальном сервере, в админ-панели WordPress должен быть настроен домен `wordpress.mydomain.ru` на стандартном порту HTTP;
- Добавить в обратный прокси правило публикации `wordpress.mydomain.ru -> wordpress.mydomain.ru`.

18.8.2 Защита от DoS-атак

Включение опции **Защита от DoS-атак** ограничивает трафик, если:

- скорость - более 200 запросов в секунду с одного IP-адреса;
- количество подключений с одного IP-адреса - более 1000;
- размер запроса - более 50 Мб;
- время ожидания на чтение заголовка и тела запроса - более 5 секунд.

18.9 DNS

18.9.1 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** на следующих вкладках:

Внешние DNS-серверы - позволяют указать DNS-серверы во внешних сетях, через которые будут разрешаться доменные имена, запрашиваемые из локальных сетей.

Forward-зоны - позволяют указать сторонние DNS-серверы (в локальных или внешних сетях относительно NGFW) с указанием конкретных DNS-зон, которые эти серверы обслуживают. Перечисленные возможности DNS-сервера могут использоваться одновременно.

Master-зоны - позволяют настроить полнофункциональный DNS-сервер, разрешающий имена в IP-адреса сетевых устройств в локальной сети.

При наличии большого количества Forward- и Master-зон в таблицах воспользуйтесь кнопкой **Фильтры**.

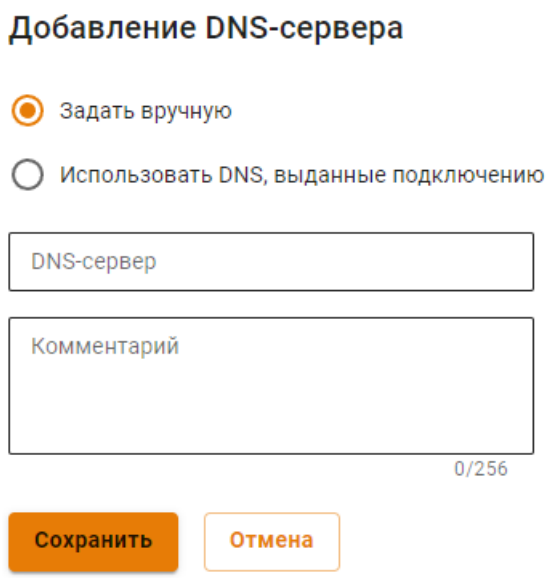
18.9.2 Внешние DNS-серверы

Для корректной работы резолвинга имен через Ideco NGFW указывать DNS-серверы в этом разделе не требуется.

Если DNS-серверы не указаны, то сервер будет разрешать имена в сети интернет, используя корневые DNS-серверы в интернете.

Данная конфигурация не будет работать, если вышестоящий роутер перехватывает DNS-запросы. В этом случае рекомендуем:

- Укажите DNS-серверы вручную (нажмите **Добавить**):
  - Выберите **Задать вручную** и укажите IP-адрес DNS-сервера;
  - Используйте опцию **Использовать DNS, выданные подключению**, указав нужное подключение.



Рекомендации:

1. В Ideco NGFW встроен кеширующий DNS-сервер. Рекомендуется использовать его в качестве DNS-сервера для локальной сети.

2. Не указывайте `8.8.8.8`, `1.1.1.1` или подобные без особой необходимости. Ideco NGFW справится с резолвингом самостоятельно.

3. Не указывайте DNS-серверы от внутреннего сервера Active Directory, даже если он может самостоятельно резолвить доменные имена в интернете. При интеграции с AD Ideco NGFW автоматически настроит все необходимое (Forward-зону) для работы AD и резолвинга внутренних имен домена. Для резолвинга каких-то особых зон, не связанных с AD, создавайте Forward-зону.

4. Не рекомендуем использовать DNS, выданные интернет-провайдером, так как они превышают TTL и долго отвечают. Ideco NGFW настроит автоматически все необходимое для подключения к PPTP/L2TP через доменное имя. Если нужна особая внутренняя доменная зона провайдера, то создавайте Forward-зону.

5. Можно указывать DNS-серверы занимающиеся фильтрацией, если это необходимо (SkyDNS или Яндекс-DNS).

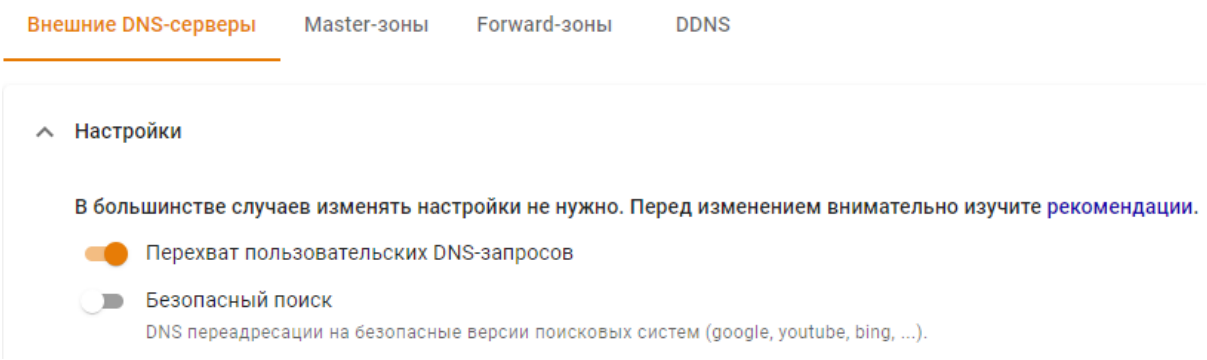
6. Если все DNS-серверы отключены или удалены, то DNS будет работать нормально (Ideco NGFW резолвит имена самостоятельно).

7. Если интернет-провайдер или вышестоящее устройство блокирует DNS-запросы, то использование стандартной конфигурации с корневыми серверами невозможно. Рекомендуем задать серверы вручную или использовать DNS-серверы, выданные подключению.

Перехват DNS-запросов

Подсказка: Включение перехвата пользовательских DNS-запросов блокирует использование DNS-over-TLS (DoT), DNS-over-QUIC (DoQ) и DNS-over-HTTPS (DoH).

Если на рабочей станции пользователя указаны сторонние DNS-серверы (например, с целью обхода блокировок), включите опцию **Перехват пользовательских DNS-запросов** в разделе **Внешние DNS-серверы**.



Опция включается глобально для всех хостов в локальной сети для избежания возможной подмены адреса ресурса при резолвинге его домена.
Также перехват позволит контролировать процесс резолвинга доменных имен в интернете исключительно средствами NGFW. Запрос будет перенаправлен на DNS-сервер NGFW, и он же сформирует ответ (вместо исходного DNS-сервера).

Перехват DNS-запросов также блокирует возможность туннелирования через DNS (DNS-tunneling) и блокирует использование DNS-over-TLS.

Сторонние DNS-серверы для дополнительной фильтрации трафика:

- SkyDNS `193.58.251.251`;
- Yandex DNS `77.88.8.88`, `77.88.8.2`;
- Google DNS `8.8.8.8`, `8.8.4.4`;
- Open DNS `208.67.222.222`, `208.67.220.220`, `208.67.222.220`, `208.67.220.222`;
- Cloudflare DNS `1.1.1.1`, `1.0.0.1`.

Безопасный поиск

При резолвинге через DNS-сервер NGFW будет возвращать адреса поисковых систем с включенной фильтрацией неподобающего контента.

18.9.3 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.

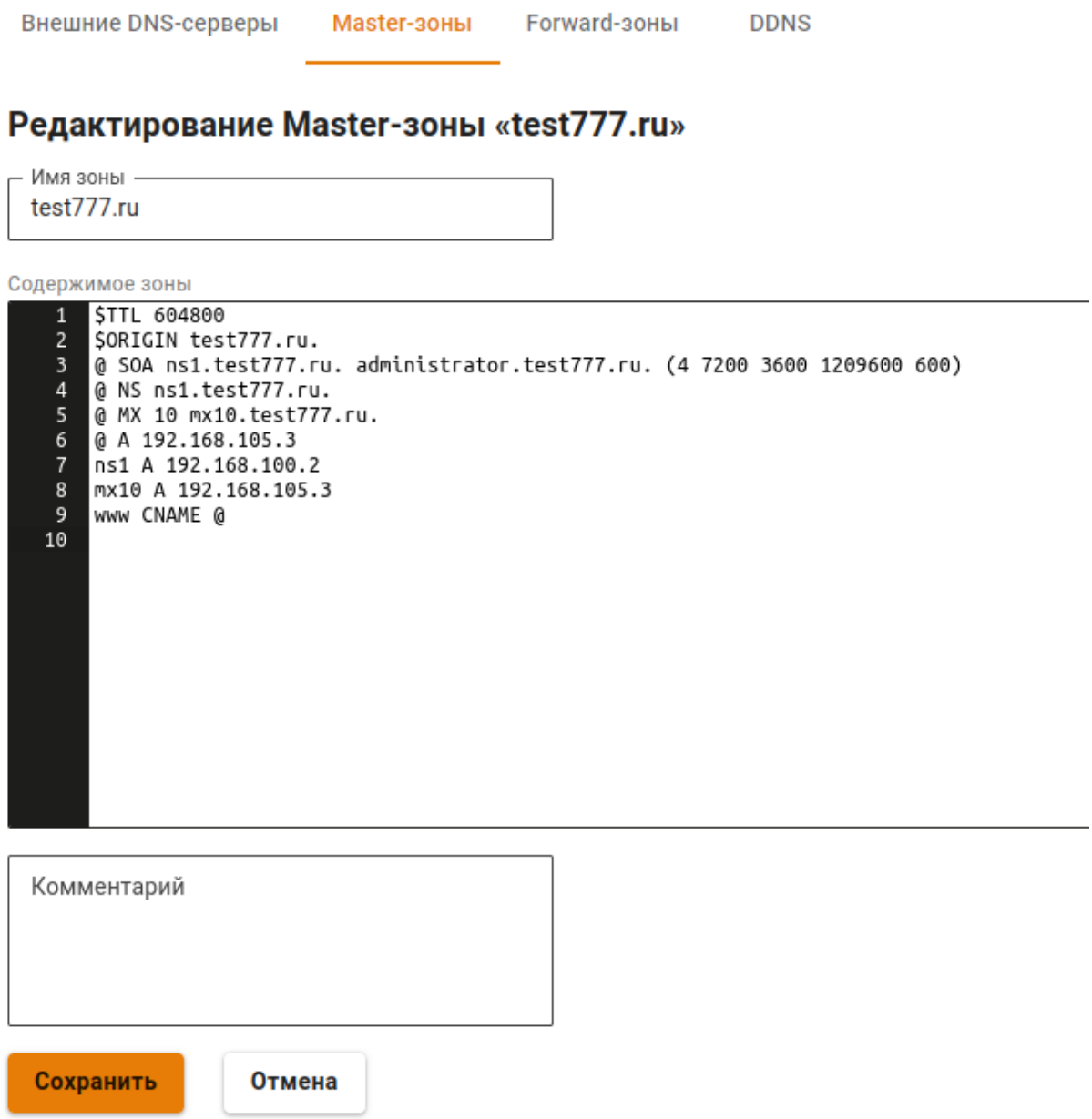
Формат записей для настройки Master-зоны соответствует формату записей DNS-сервера BIND.

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 $SOA указывается primary NS для домена и e-mail контактного лица и далее в скобках:
  1. **Serial** - Серийный номер файла зоны. При изменении данных нужно менять серийный номер, при этом зона обновляется на всех серверах. Используйте следующий формат: ГГГГММДДнн (год, месяц, день, нн — порядковый номер изменения за день). Если второй раз за день вносите изменения в файл зоны, укажите «нн» равным 01, если третий - 02, и т. д.;
  2. **Refresh** - указывает, как часто вторичные серверы должны опрашивать первичный, чтобы узнать, не увеличился ли серийный номер зоны;
  3. **Retry** - время ожидания после неудачной попытки опроса;
  4. **Expiry** - максимальное время, в течение которого вторичный сервер может использовать информацию о полученной зоне;
  5. **TTL** - минимальное время, в течение которого данные остаются в кеше вторичного сервера.
- **$SRV** - указывают на сервера, обеспечивающие работу тех или иных служб в этом домене (например, Jabber и Active Directory);
- **$NS** - DNS-сервер, обслуживающий этот домен. Минимально их необходимо два, причем они должны находится в разных подсетях, а лучше - в географически разных местах. Первым указывайте primary сервер;
- **$PTR** - отображает IP-адрес в доменное имя;
- **$MX** - описывает почтовые шлюзы (обычно один), на которые будет доставляться вся почта этого домена. Для каждого шлюза устанавливается приоритет (по умолчанию - 10). Обычно имя домена почтового шлюза выглядит так: *mx.example.com*. Для MX хостов должны быть соответствующие A-записи;
- **$A** - отображают имя хоста (доменное имя) на адрес IPv4. Для каждого сетевого интерфейса машины должна быть сделана одна **A-запись**;
- **$AAAA** - аналогична записи A, но для IPv6;
- **$CNAME** - отображает алиас на реальное имя (для перенаправления на другое имя).

Со всеми ресурсными записями можно ознакомиться по ссылке.

Пример записи приведен на скриншоте ниже:



Несколько примеров записей в Master-зону:

1. Имя зоны: ms

```
$ORIGIN ms.
$TTL 600
@ SOA ns1.ms. administrator.ms. ( 4 7200 3600 1209600 600 )
@ NS ns1.ms.
@ MX 10 mx10.ms.
@ A 192.168.0.250
ns1 A 192.168.0.250
mx10 A 192.168.0.250
www CNAME @
```

2. Имя зоны: example.com

```
$TTL 86400
@ SOA localhost. root.localhost. ( 991079290 28800 14400 3600000 86400 )
```

(continues on next page)

(продолжение с предыдущей страницы)

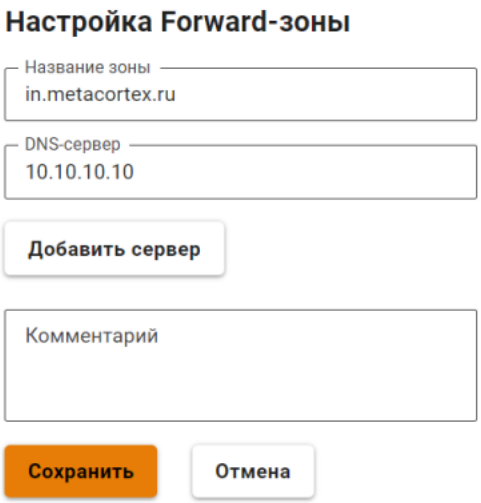
```
@ NS my-dns-server.example.com.
my-dns-server A 1.2.3.4
```

18.9.4 Forward-зоны

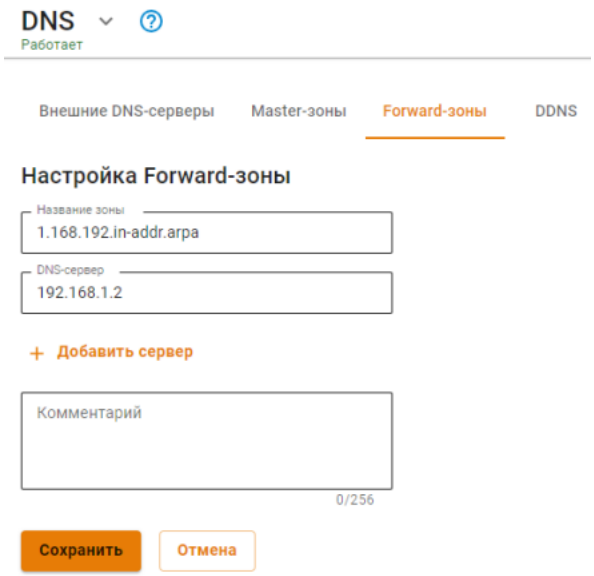
Основное

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.in.metacortex.ru` и использует для этого DNS-сервер 10.10.10.10.
Для возможности доступа к этим ресурсам по доменным именам укажите Forward-зону провайдера как isp и далее задайте DNS-сервер 10.10.10.10:



Подсказка: Для резолвинга PTR при интеграции с Active Directory пропишите обратную Forward-зону. Например, для подсети **192.168.1.0/24** в названии зоны нужно прописать **1.168.192.in-addr.arpa**:



18.9.5 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

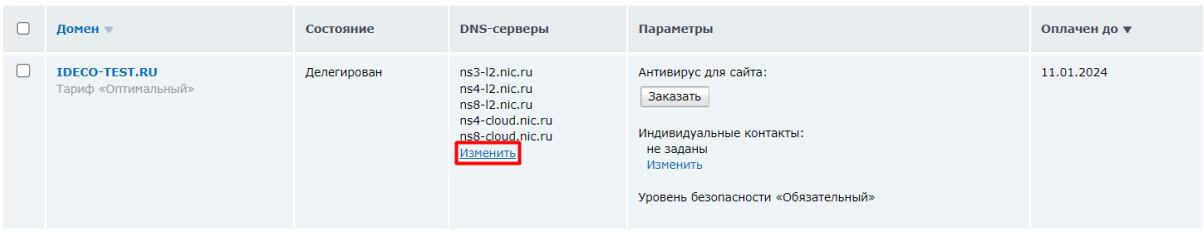
Подсказка: DDNS не будет работать:

- 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**:



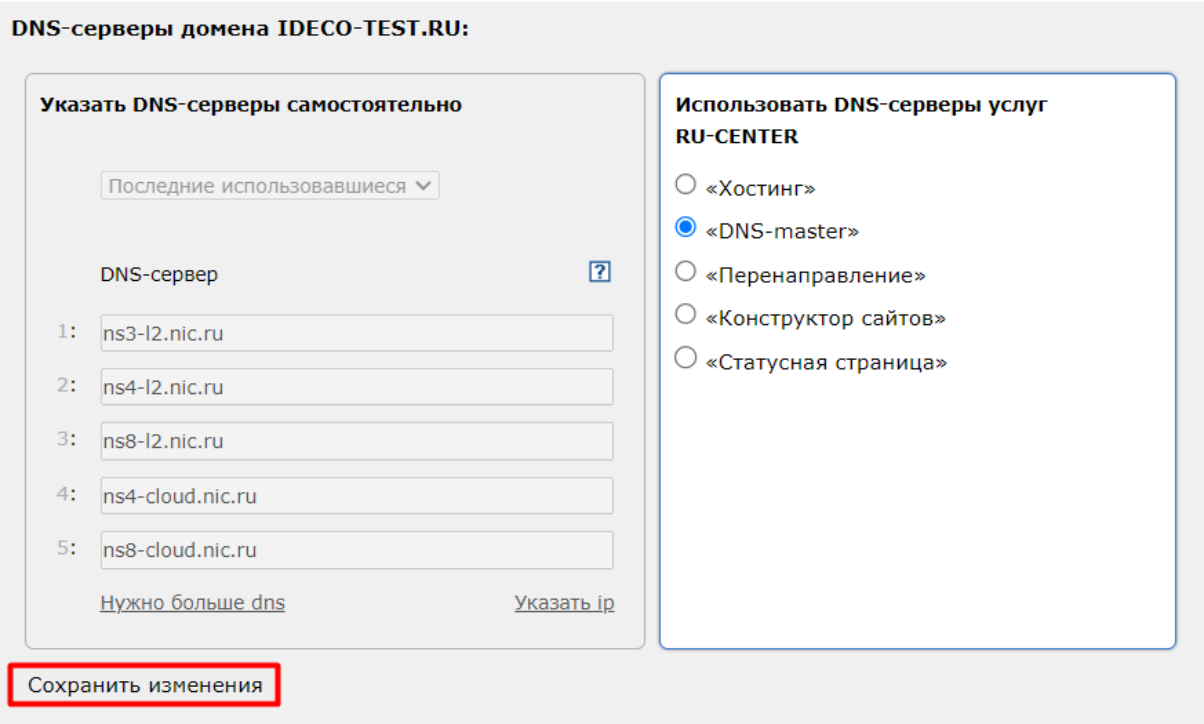
2. В разделе **Мои домены** измените настройки сервера, нажав **Изменить** в столбце **DNS-серверы**:



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.

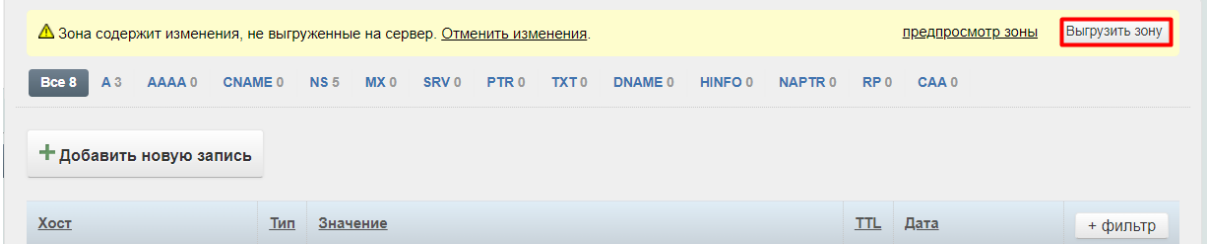
4. Перейдите в раздел **DNS-хостинг** и нажмите **Управление DNS-зонами**.

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.

18.10 DHCP-сервер

Подсказка: Название службы раздела **DHCP**: `ideco-dnsmasq`.
Список служб для других разделов доступен по *ссылке*.

18.10.1 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.

Подсказка: Для сортировки строк таблицы по определенному столбцу нажмите на этот столбец в заголовке таблицы.

Для управления настройками DHCP-сервера перейдите в раздел **Сервисы -> DHCP-сервер**.

> **Предупреждение:** На локальном интерфейсе Ideco NGFW, участвующем в раздаче адресов, должен быть настроен статический IP адрес.

При использовании DHCP-сервера переключите ползунок в левом верхнем углу в положение **Включен**.

18.10.2 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.

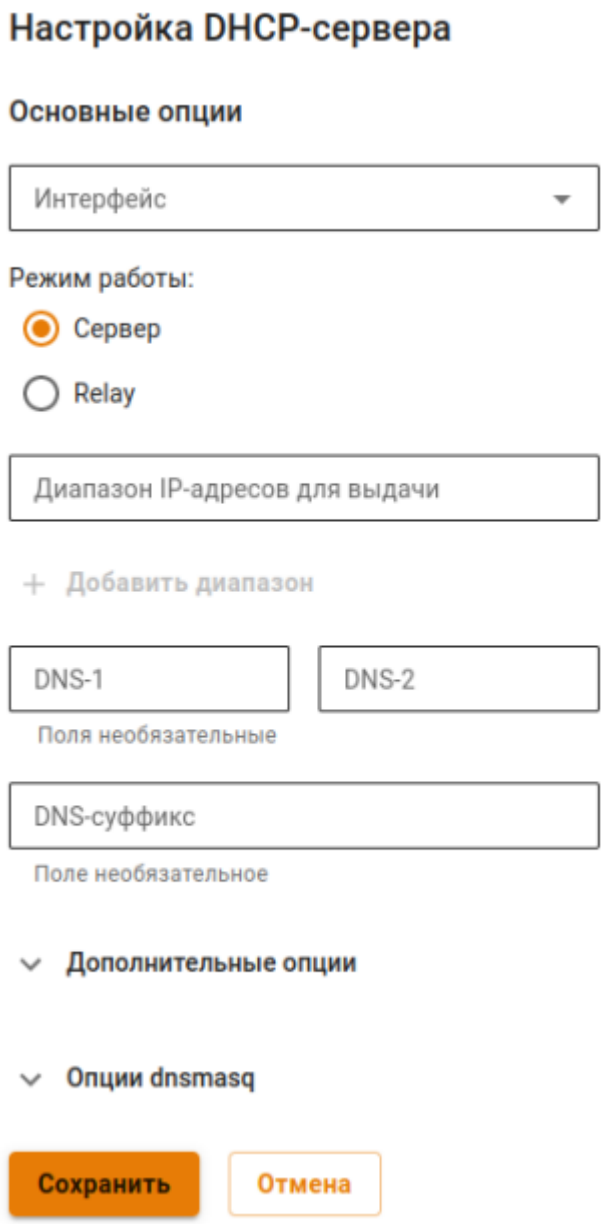
Настройка DHCP-сервера делится на три блока:

- **Основные опции** - задаются диапазоны IP-адресов и DNS-серверы;
- **Дополнительные опции** - статические маршруты, адреса WINS-серверов, время аренды, PXE Boot и WPAD;
- **Опции dnsmasq** - предназначены для ручного задания опций DHCP, передаваемых сервером клиенту при получении сетевых реквизитов от DHCP-сервера.

Основные опции

Режим работы Сервер:

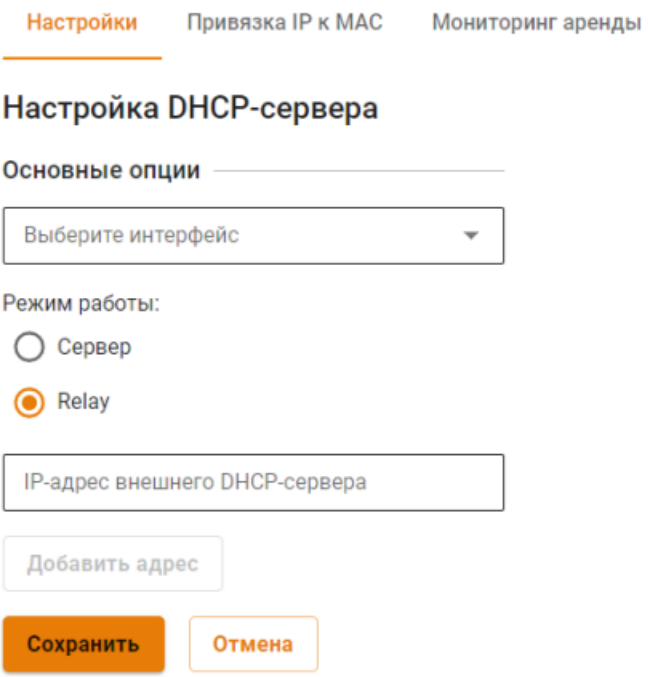
Выберите режим работы **Сервер**, чтобы настроить выдачу IP-адресов на Ideco NGFW. Заполните следующие поля:



- **Интерфейс** - выберите интерфейс, который будет участвовать в раздаче адресов;
- **Диапазон IP-адресов для выдачи** - укажите диапазон IP-адресов, которые будут выданы устройствам в локальной сети, должен входить в одну из подсетей выбранного интерфейса. Размер диапазона не должен превышать 256 адресов;
- **DNS-1** и **DNS-2** - укажите IP-адреса DNS-серверов для устройств локальной сети. Если ни одно из полей не заполнено, то DNS-сервером для всех сетевых устройств локальной сети будет являться Ideco NGFW;
- **DNS-суффикс** - введите домен, прибавляющийся к запрашиваемому имени устройства в локальной сети. Поле не обязательное. Нужен, для того, чтобы в локальной сети вводить не полное имя компьютера вместе с доменом, а только само имя.

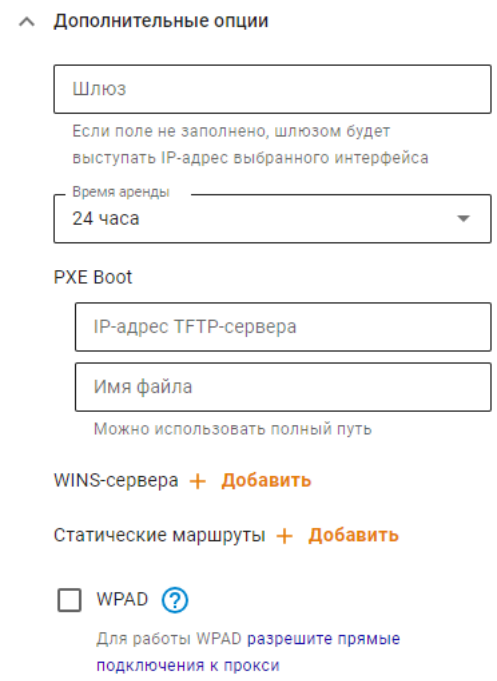
Режим работы Relay:

Выберите режим работы **Relay**, если IP-адреса будет выдавать внешний DHCP-сервер. Выберите интерфейс, который будет участвовать в раздаче IP-адресов, и введите IP-адрес внешнего DHCP-сервера:



Включить/выключить, редактировать или удалить правила для выдачи IP-адресов можно кнопками управления в колонке **Управление**.

Дополнительные опции



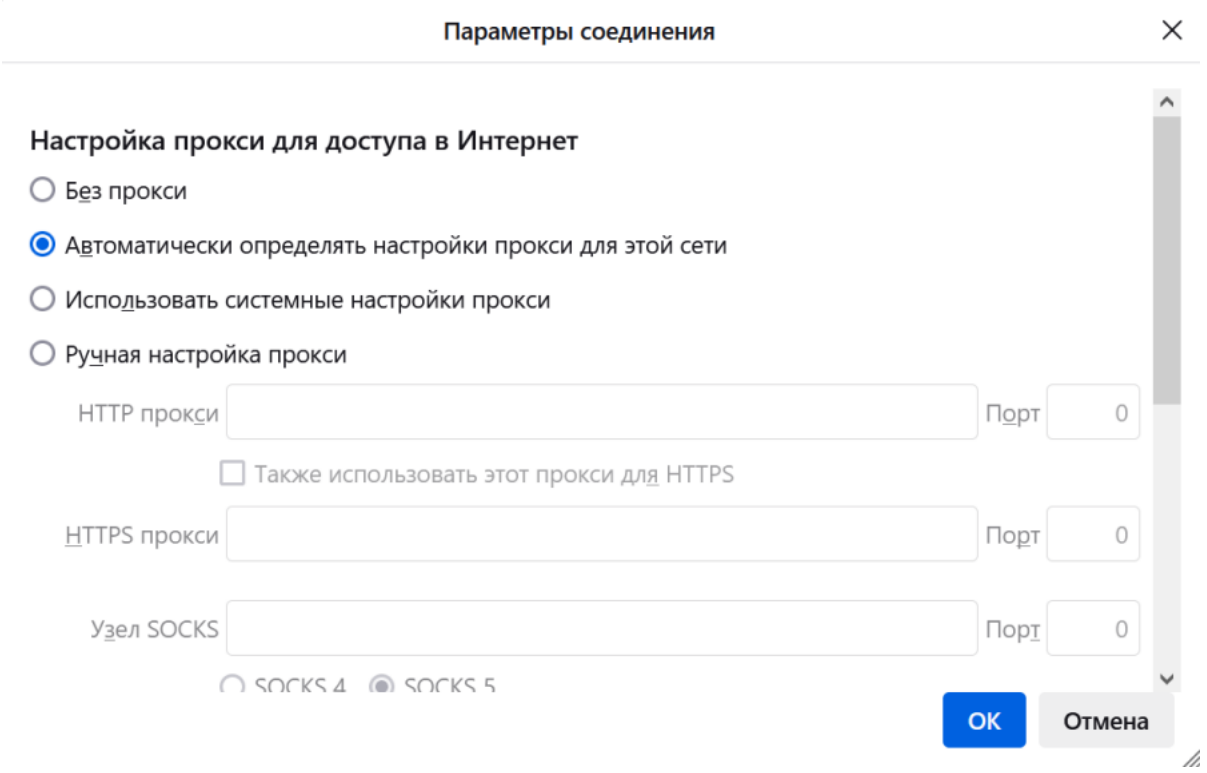
- **Шлюз** - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса;
- **Время аренды** - время, на которое выдается IP-адрес;
- **PXE Boot** - IP-адрес TFTP-сервера для настройки загрузки образа по сети;
- **WINS-сервера** - IP-адрес WINS-сервера;

- **Статические маршруты** - подсеть и шлюз для указания статического маршрута;
- **WPAD** - протокол автоматической настройки прокси.

При включении опции WPAD Ideco NGFW будет автоматически генерировать файл с настройками подключения к прокси и передавать его хостам в локальной сети, на которых настроено получение IP по DHCP. Локальные сети в файле конфигураций будут добавлены в исключения из прокси.

Подсказка: Для работы WPAD необходимо разрешить прямые подключения к прокси в разделе **Сервисы -> Прокси**.

Подсказка: Браузеры Google Chrome и Microsoft Edge автоматически примут настройки прокси, переданные хостам по DHCP. В Mozilla Firefox необходимо будет дополнительно зайти в **Настройки браузера -> Настройки прокси** и выбрать пункт **Автоматически определять настройки прокси для этой сети**:



Опции dnsmasq

Подсказка: Опция dnsmasq имеет больший приоритет чем опция, внесенная в блок **Основные опции** или **Дополнительные опции**.

Строка **Значение** может содержать только одну опцию.

Формат записи опции соответствует части записи опции в конфигурации dnsmasq - `[vendor:[<vendor-class>],][<opt>|option:<opt-name>],[<value>[,<value>]]`, где:

- `[vendor:[<vendor-class>],]` - вендор, необязательно:
- `[<opt>|option:<opt-name>]` - числовое или строковое (напр. option:nis-server) обозначение опции;
- `[<value>[,<value>]]` - одно или несколько значений опции через запятую.

Установите флаг **Force** если требуется отправлять опцию DHCP-клиенту, даже если он ее не запрашивал.

Предупреждение: **Важно**: некорректно заданные dnsmasq-опции могут привести к остановке работы раздела **DHCP-сервер**. Статус раздела сменится на `Модуль "dnsmasq" не смог запуститься` и `Служба 'ideco-dnsmasq' остановлена`.

Для поиска некорректно заданной опции выполните действия:

- Перейдите в раздел **Отчеты и журналы -> 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"
```

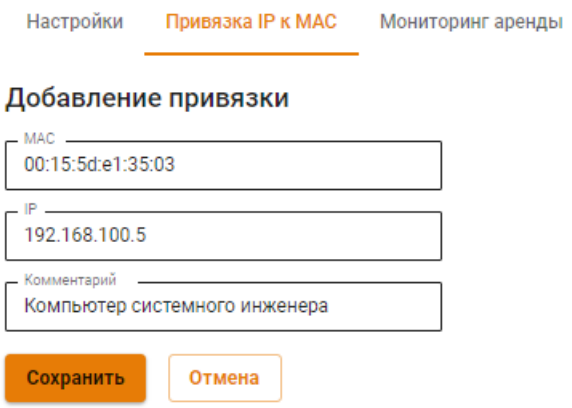
После сохранения настроек IP-телефония Avaya будет получать от DHCP-сервера расширенный список опций.

18.10.3 Привязка IP к MAC

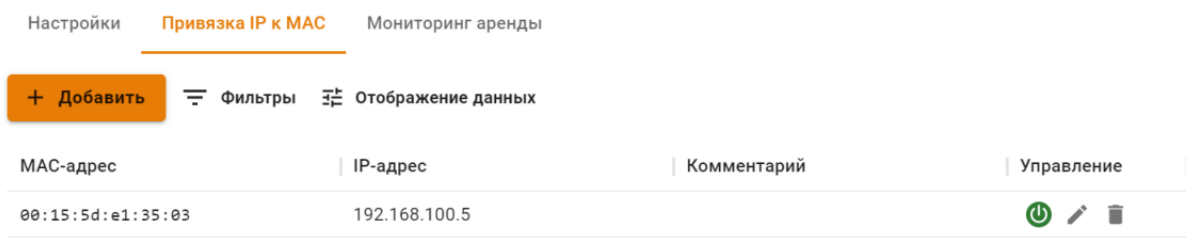
Для настройки в DHCP-сервере привязки IP-адреса к MAC-адресу необходимо:

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` (для операционной системы Windows):

```
C:\Windows\system32>ipconfig /all | findstr адрес
   Физический адрес. . . . . . . . . . . : 00-15-5D-E1-35-03
   Локальный IPv6-адрес канала . . . : fe80::85df:8421:a811:c8be%4(Основной)
   IPv4-адрес. . . . . . . . . . . . . . : 192.168.100.5(Основной)

C:\Windows\system32>
```

При наличии большого количества привязок в таблице воспользуйтесь кнопкой **Фильтры**.

Подсказка: Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW.

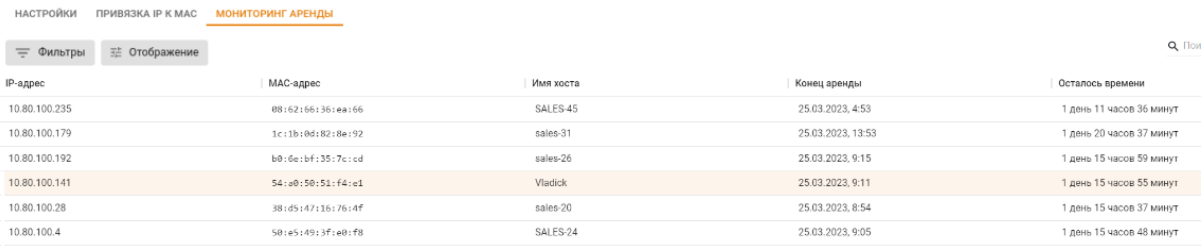
Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (`01-02-03-04-05-06`). В настройках Ideco NGFW октеты MAC-адреса разделяются только двоеточиями (`01:02:03:04:05:06`).

Настройка DHCP-сервера для Wi-Fi сетей:

При настройке Wi-Fi сетей может понадобиться настройка DHCP-сервера. Для получения подробной информации перейдите в раздел *Wi-Fi-сети*.

18.10.4 Мониторинг аренды

Содержит информацию об аренде IP-адресов для устройств. Для поиска воспользуйтесь кнопкой **Фильтры**:



Для привязки IP к MAC нажмите на кнопку  в столбце **Управление**.

18.11 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.

18.11.1 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.

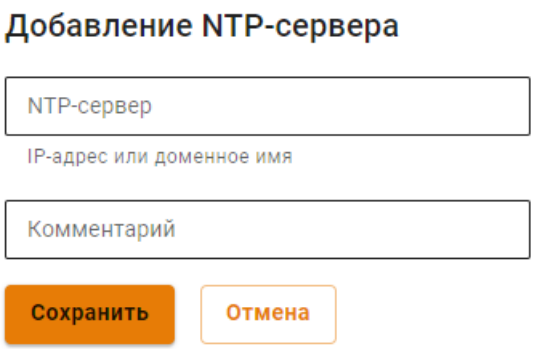
18.11.2 Настройка Ideco NGFW

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:



Если таблица NTP-серверов пустая, то Ideco NGFW синхронизирует время с сервером `ntp.ideco.ru`.

При наличии большого количества NTP-серверов в таблице воспользуйтесь кнопкой **Фильтры**.

18.12 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: В **Туннельном** режиме работы для создания туннелей используются все внешние интерфейсы со шлюзом по умолчанию и все **Адреса удаленного устройства**, указанные при создании IPsec-подключений.

Выбор конкретного туннеля для обмена трафиком зависит от приоритета внешнего интерфейса в таблице раздела **Балансировка и резервирование**. Приоритет интерфейса определяется местом в таблице: чем выше интерфейс, тем больше у него приоритет.

Интерфейсы без выхода в интернет имеют меньший приоритет по сравнению с интерфейсами с доступом в интернет.

Поддерживается неограниченное число туннелируемых IP-адресов.

Туннельный режим не пропускает широковещательные рассылки, поэтому в таком режиме настроить OSPF не получится.

В **Транспортном** режиме трафик не ограничивается IPSec-политиками, необходимо настраивать маршрутизацию вручную. Для подключения используется выбранный в настройках сетевой интерфейс.

Транспортный режим пропускает широковещательные рассылки, рекомендуем в данном режиме использовать маршрутизацию на основе *OSPF*.
Для резервирования канала можно создать несколько IPSec-подключений через разные внешние интерфейсы и определить приоритет направления трафика настройками *OSPF*.

Предупреждение: IPsec использует протокол UDP, порты 500 и 4500. По умолчанию они открыты, но если настроено запрещающее правило во вкладке **INPUT** раздела ***Файрвол***, не забудьте добавить разрешение для IPsec.

18.12.1 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.

18.12.2 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.

18.12.3 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.

18.12.4 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.

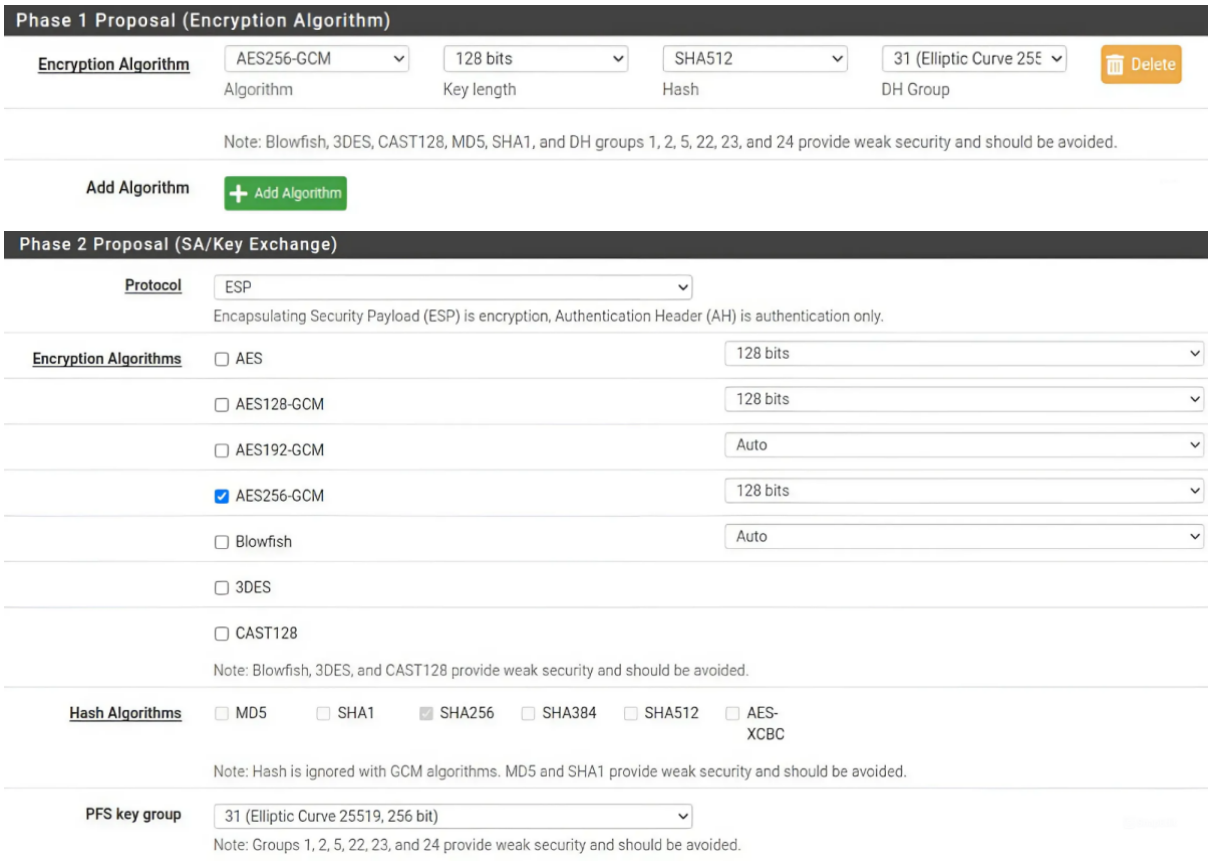
Список алгоритмов и пример использования:

- **Phase 1 (IKE):**
  - encryption (шифрование):
    - **AES256-GCM**.
    - **AES256 (AES256-CBC)**.
  - integrity (hash, целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
    - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA256**.
  - prf (функция генерации случайных значений):
    - как правило, настраивается автоматически в зависимости от выбора алгоритмов integrity (поэтому в примере *ниже* значение prf: PRF-HMAC-SHA512).
    - для AES-GCM может потребоваться указать явно. В этом случае по приоритету: **AESXCBC, SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman):
    - **Curve25519 (group 31)**.
    - **ECP256 (group 19)**.
    - **modp4096 (group 16)**.
    - **modp2048 (group 14)**.
    - **modp1024 (group 2)**.
  - Таймауты:
    - **Lifetime**: 14400 сек.
    - **DPD Timeout** (для L2TP/IPsec): 40 сек.
    - **DPD Delay**: 30 сек.
- **Phase 2 (ESP):**
  - encryption (шифрование):
    - **AES256-GCM**.
    - **AES256 (AES256-CBC)**.
  - integrity (целостность):
    - для **AES256-GCM** - не требуется, поскольку проверка целостности встроена в AEAD-алгоритмы.
    - для **AES256 (AES256-CBC)** - по приоритету: **SHA512, SHA384, SHA256**.
  - DH (Группа Diffie-Hellman, PFS). **ВНИМАНИЕ! Если не указать группу, то подключение будет установлено, но через некоторое время не сработает параметр rekey**:
    - **Curve25519 (group 31)**.
    - **ECP256 (group 19)**.
    - **modp4096 (group 16)**.
    - **modp2048 (group 14)**.
    - **modp1024 (group 2)**.
  - Таймаут:
    - **Lifetime**: 3600 сек.

Пример:

- **Phase 1 (IKE)** (нужна одна из строк)**:**
  - AES256-GCM\PRF-HMAC-SHA512\Curve25519.
  - AES256(AES256-CBC)\SHA512\PRF-HMAC-SHA512\ECP384.
  - AES256(AES256-CBC)\SHA256\PRF-HMAC-SHA256\MODP2048.
- **Phase 2 (ESP)** (нужна одна из строк)**:**
  - AES256-GCM\ECP384.
  - AES256(AES256-CBC)\SHA256\MODP2048.

Пример настройки подключения pfSense к Ideco NGFW по IPsec:

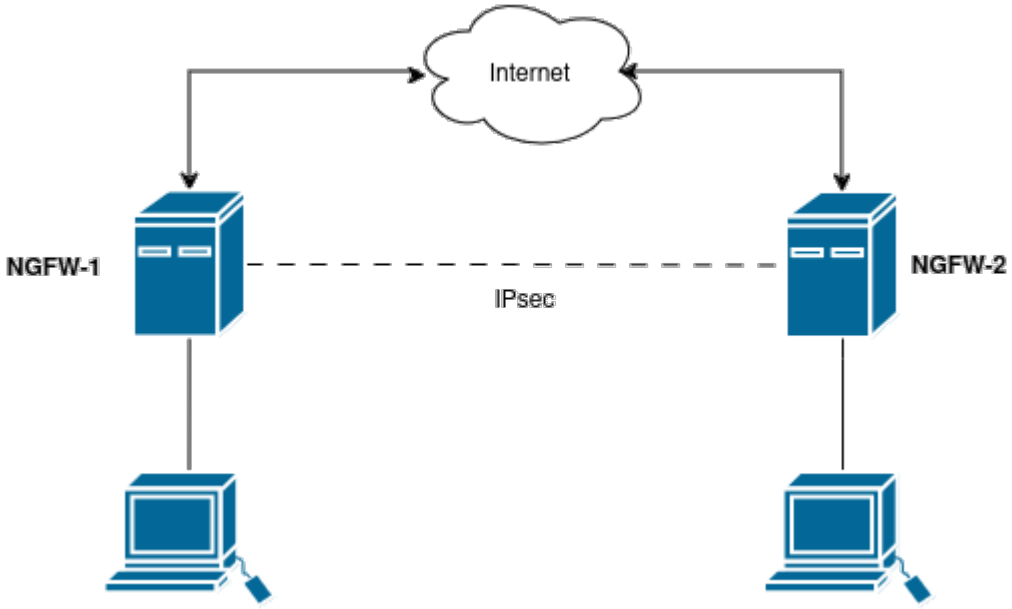


18.12.5 Изменение настроек созданных IPsec-подключений

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**.

18.12.6 Подключение между двумя Ideco NGFW в туннельном режиме работы



Для создания IPsec-подключения между Ideco NGFW нужно настроить на одном NGFW входящее подключение, а на другом NGFW - исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключение, а на **NGFW-2** - входящее подключение.

Шаг 1. Проверка условий подключения

Перед созданием подключения убедитесь, что:

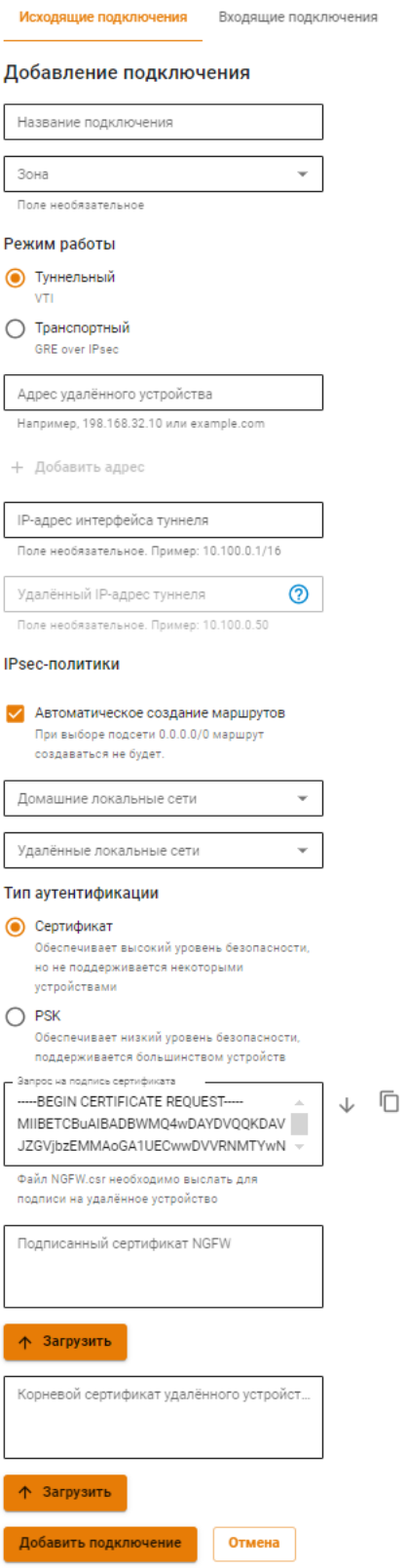
- На **NGFW-1** и **NGFW-2 правильно настроены временные зоны**. Без этого подключение не установится.
- Для работы IPsec все подсети, участвующие в соединениях, не пересекаются.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. **Входящее подключение должно настраиваться на сервере с белым IP-адресом**.
- Пользовательские правила из раздела **Правила трафика -> Файрвол -> INPUT** не блокируют входящий трафик для протоколов ESP и UDP (порты 500 и 4500), поступающий на внешние интерфейсы **NGFW-2**.
- Сети для VPN-подключений у **NGFW-1** и **NGFW-2** не пересекаются.

Шаг 2. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес.

Адресов может быть несколько.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-2**. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:
    * При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW.
    * При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните его для настройки входящего подключения.
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните его для настройки входящего подключения. Заполните поле **Идентификатор UTM**.

Предупреждение: Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно настроить статические маршруты до удаленных локальных сетей NGFW в разделе **Сервисы -> Маршрутизация** или динамическую маршрутизацию через BGP в разделе **Сервисы -> BGP**.

3. Выполните действие для нужного типа аутентификации:

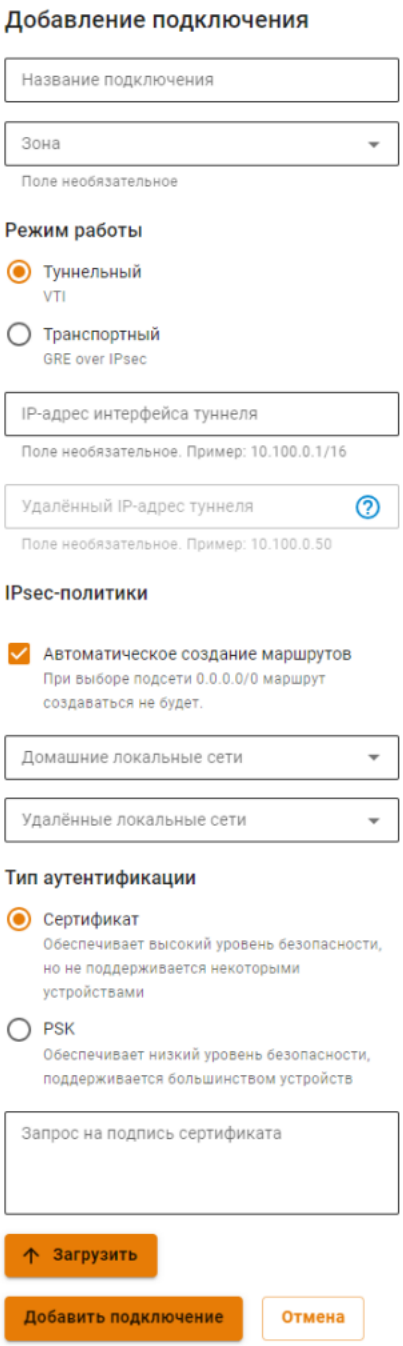
- **PSK** - проверьте правильность заполнения полей, нажмите **Добавить подключение** и перейдите к **Шагу 3**.
- **Сертификат** - **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 3** для настройки входящего подключения на **NGFW-2**.

Шаг 3. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым.
- **Режим работы** - выберите **Туннельный**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля **NGFW-1**. Поле необязательное, заполняется для получения статистики обмена пакетами.
- **IPSec-политики**:
  - **Автоматическое создание маршрутов**:

    * При включении опции автоматически создаются статические маршруты до удаленных локальных сетей NGFW.
    * При отключении опции необходимо настроить статические маршруты до удаленных локальных сетей NGFW или динамическую маршрутизацию через BGP.
  - **Домашние локальные сети** - укажите локальные сети **NGFW-1**, к которым должен быть доступ с другого NGFW.
  - **Удаленные локальные сети** - укажите локальные сети **NGFW-2**, к которым должен быть доступ с текущего NGFW.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните его для настройки входящего подключения.
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните его для настройки входящего подключения. Заполните поле **Идентификатор UTM**.

Предупреждение: Если в поле **Домашние локальные сети** и **Удаленные локальные сети** указаны сети формата `0.0.0.0/0`, то маршруты не будут создаваться автоматически. В этом случае нужно настроить статические маршруты до удаленных локальных сетей NGFW в разделе **Сервисы -> Маршрутизация** или динамическую маршрутизацию через BGP в разделе **Сервисы -> BGP**.

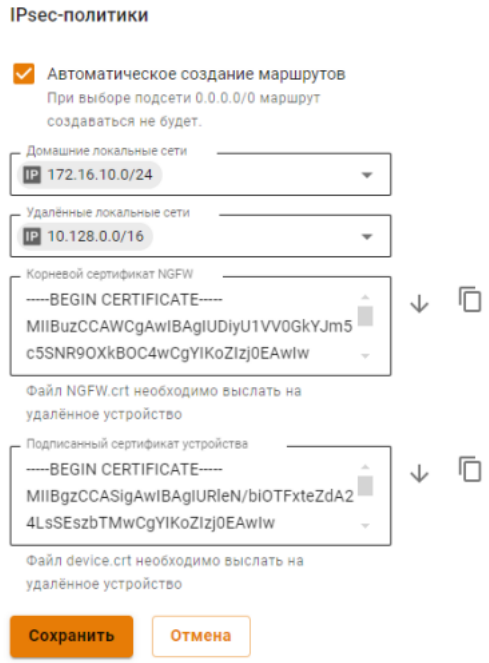
3. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Если был выбран тип аутентификации **PSK**, то настройка завершена.
Если был выбран тип аутентификации **Сертификат**, то выполните **Шаг 4**.

Шаг 4. Донастройка исходящего подключения с типом аутентификации Сертификат

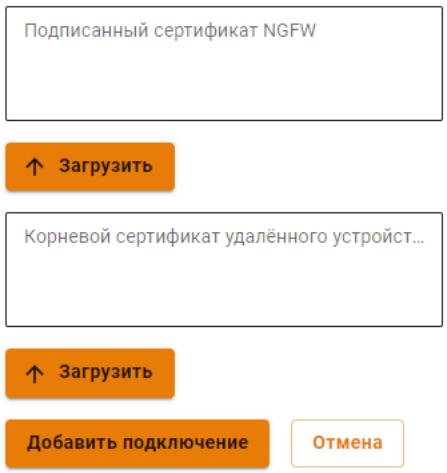
1. В **NGFW-2** перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите  по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** значениями, ранее скопированными из **NGFW-2**:



5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Подсказка: Если соединение по IPsec не устанавливается, воспользуйтесь *статьей*.

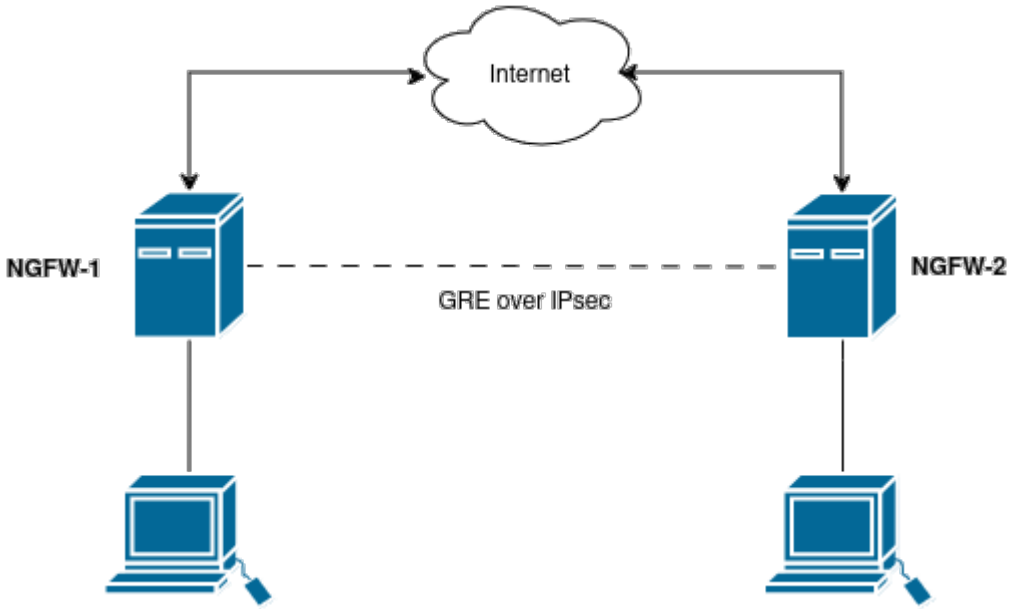
Настройка доступа к локальным сетям по VPN из NGFW-1 к NGFW-2

Для доступа к локальным сетям по VPN из **NGFW-1** к **NGFW-2** выполните действия:

1. Перейдите к редактированию настроенного IPsec-подключения на **NGFW-2**.

2. Укажите в поле **Домашние локальные сети** сеть, используемую для VPN в **NGFW-2**.

18.12.7 Подключение между двумя Ideco NGFW в транспортном режиме работы



Подсказка: GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

При замене/перевыпуске корневого сертификата в разделе *Сертификаты*, IPsec-подключения перестанут работать и их необходимо будет пересоздать.

Предупреждение: Перед настройкой убедитесь, что:

- В каждой из подключаемых сторон **правильно настроена временная зона**. Без этого установить подключение невозможно.
- Пользовательские правила из раздела **Правила трафика -> Файрвол -> INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протоколов ESP и UDP (порты 500 и 4500).
- Пользовательские правила из раздела **Правила трафика -> Файрвол -> INPUT**, не блокируют входящий трафик, поступающий на внешние интерфейсы NGFW для протокола GRE.
- Ни один Ideco NGFW не находится за NAT, так как в таком случае подключение двух Ideco NGFW в транспортном режиме недоступно.
- Все IP-подсети, участвующие в соединениях не должны пересекаться и, тем более, не должны совпадать.
- Один из серверов имеет публичный (белый) IP-адрес от интернет-провайдера. Входящее подключение должно настраиваться на сервере с белым IP-адресом.
- Сети для VPN-подключений у двух NGFW не пересекаются.

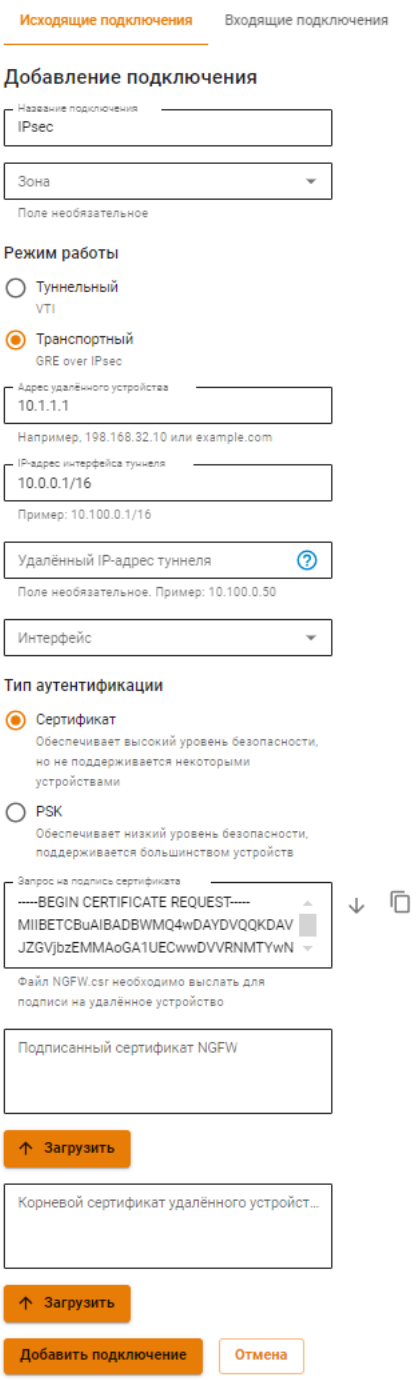
Для создания IPsec подключения между Ideco NGFW нужно настроить на одном NGFW входящее подключение, а на другом NGFW исходящее подключение. Будем настраивать на **NGFW-1** исходящее подключение, а на **NGFW-2** входящее подключение.

Шаг 1. Первоначальные действия при настройке исходящего подключения

Перед настройкой исходящего подключения выполните предварительные действия на **NGFW-1**:

1. Перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Название подключения** - максимальное количество символов 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым.
- **Режим работы** - выберите **Транспортный**.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его белый IP-адрес.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.

- **Интерфейс** - укажите сетевой интерфейс, через который будет выполняться подключение.
- **Адрес удаленного устройства** - введите доменное имя другого Ideco NGFW или его IP-адрес, доступный с сетевого интерфейса, указанного в поле выше.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - При выборе типа аутентификации **Сертификат** скопируйте поле **Запрос на подпись сертификата** и сохраните его для настройки входящего подключения.
  - При выборе типа аутентификации **PSK** скопируйте поле **PSK ключ** и сохраните его для настройки входящего подключения. Заполните поле **Идентификатор NGFW**.

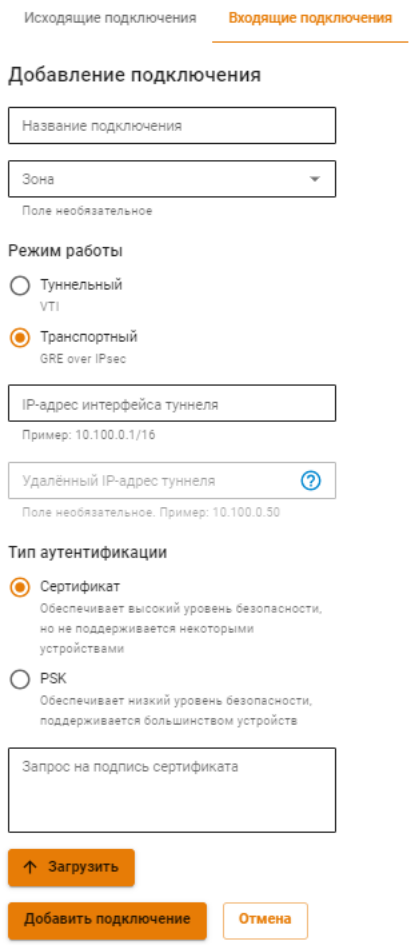
4. Если тип аутентификации - **PSK**, проверьте правильность заполнения полей и нажмите **Добавить подключение** и перейдите к **Шагу 2**. Если тип аутентификации - **Сертификат**, **не закрывайте форму создания исходящего подключения** и перейдите к **Шагу 2** для настройки входящего подключения на другом NGFW.

Шаг 2. Настройка входящего подключения

Для настройки входящего подключения выполните действия на **NGFW-2**:

1. Перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



Расшифровка полей:

- **Название подключения** - максимальное количество символов - 42.
- **Зона** - выберите зону, в которую нужно добавить IPsec подключение, или оставьте поле пустым:

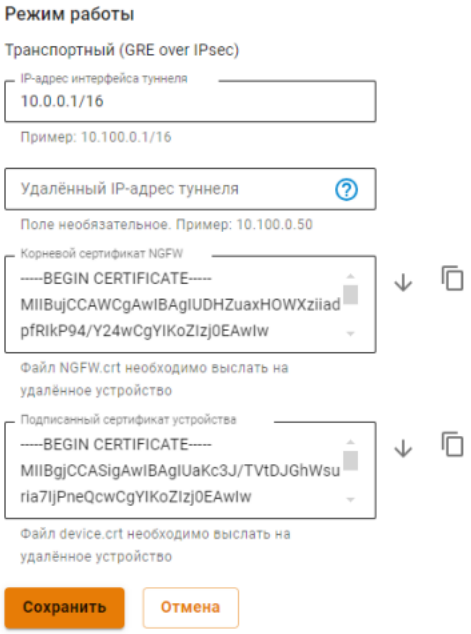
- **Режим работы** - выберите **Транспортный**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат** или **PSK**:
  - **Сертификат** - заполните поле **Запрос на подпись сертификата**, вставив значение сохраненное при первоначальной настройке исходящего подключения.
  - **PSK** - заполните поле **PSK ключ**, вставив значение сохраненное при первоначальной настройке исходящего подключения.Заполните поле **Идентификатор удаленной стороны**.

5. Проверьте правильность заполнения полей и нажмите **Добавить подключение**.

Шаг 3. Донастройка исходящего подключения с типом аутентификации Сертификат

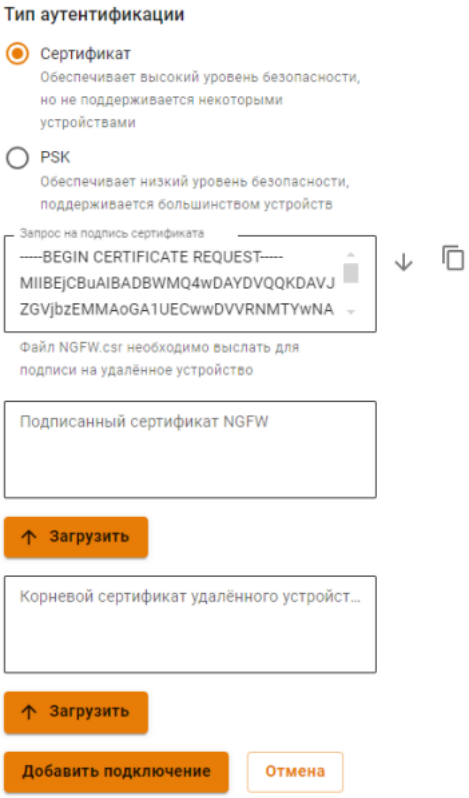
1. В **NGFW-2** перейдите в раздел **Сервисы -> IPsec -> Входящие подключения** и нажмите  по ранее созданному входящему подключению.

2. Скопируйте поля **Корневой сертификат NGFW** и **Подписанный сертификат устройства**:



3. В **NGFW-1** перейдите в раздел **Сервисы -> IPsec -> Исходящие подключения**.

4. Заполните поля **Подписанный сертификат NGFW** и **Корневой сертификат удаленного устройства** ранее скопированным значением при редактировании входящего подключения:



5. Нажмите **Сохранить**.

Шаг 4. Настройка маршрутизации

Маршрутизацию можно настроить тремя способами:

- Статические маршруты до локальных сетей удаленного NGFW в разделе **Сервисы ->** ***Маршрутизация***.
- Динамическая маршрутизация через BGP в разделе **Сервисы ->** ***BGP***.
- Динамическая маршрутизация через OSPF в разделе **Сервисы ->** ***OSPF***.

Подсказка: Рекомендуем для настройки маршрутизации использовать OSPF, в этом случае нет необходимости вручную настраивать маршруты до локальных сетей филиалов.
Также настройками OSPF можно определить приоритет направления трафика для резервирования каналов при создании нескольких IPSec-подключений.

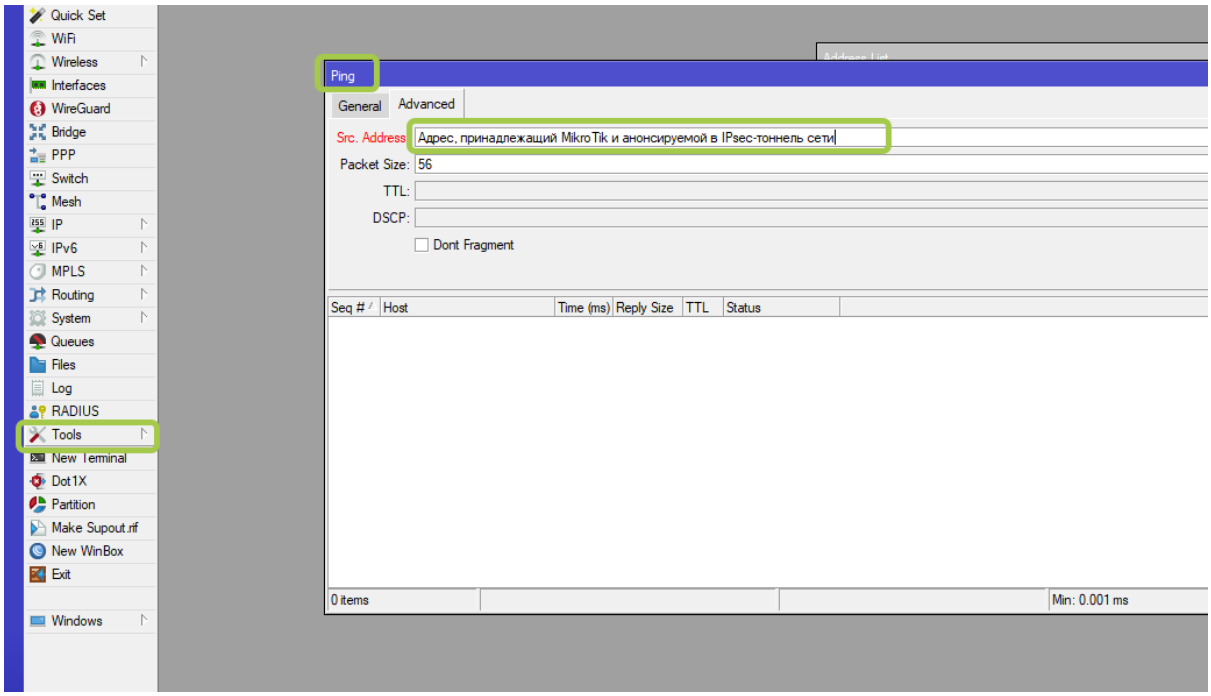
18.12.8 Подключение Ideco NGFW и Mikrotik

Подсказка: При объединении сетей с помощью VPN локальные сети в разных офисах не должны пересекаться.

Для корректной работы подключений по сертификатам синхронизируйте время на MikroTik по NTP (например, предоставьте доступ в интернет).

Исходящие IPsec-подключения по сертификатам к MikroTik ниже версии 6.45 не работают из-за невозможности использования современных криптоалгоритмов.

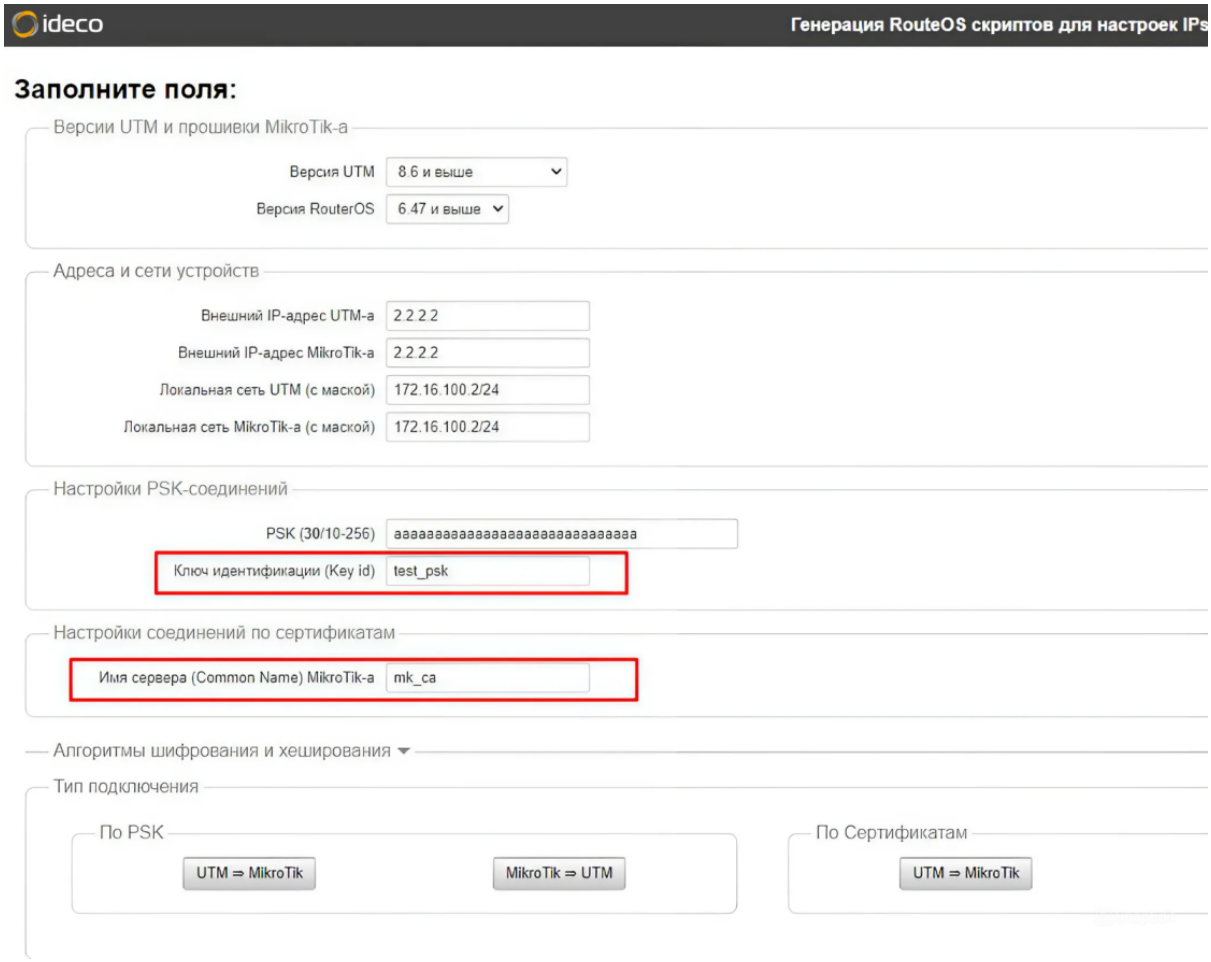
Подсказка: Для проверки доступности анонсируемых сетей Ideco NGFW с MikroTik указывайте IP-адрес источника:



Подключение в Туннельном режиме

При использовании нашего конфигуратора скриптов настроек MikroTik есть несколько особенностей:

- При подключении нескольких устройств MikroTik к одному Ideco NGFW по PSK указывайте разные **Идентификаторы ключа (key-id)** для каждого устройства.
- При подключении нескольких устройств MikroTik к одному Ideco NGFW по сертификатам указывайте разные **Имена сервера** (Common Name) для каждого устройства:

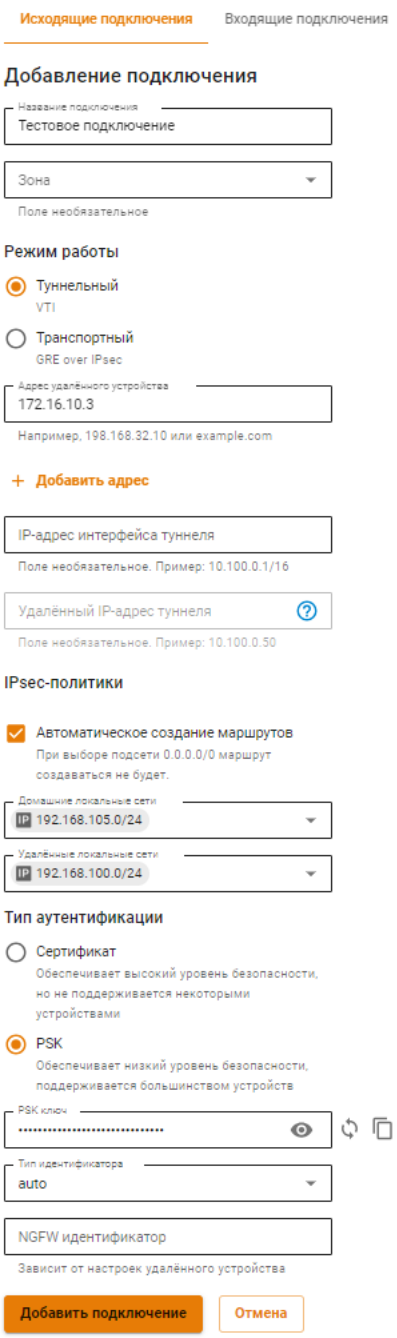


Подключение от Ideco NGFW к MikroTik

Тип аутентификации PSK

Настройка Ideco NGFW:

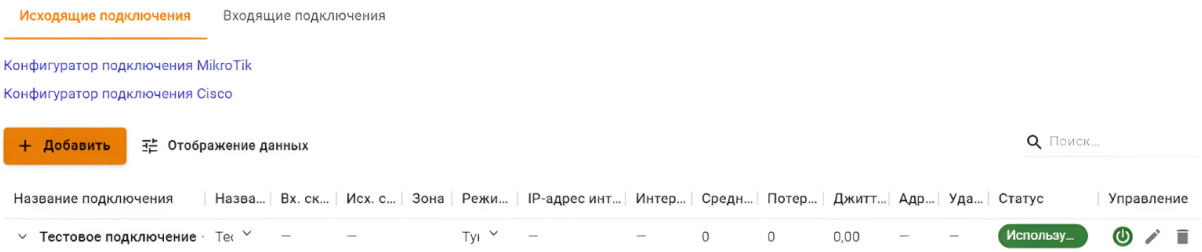
1. Откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**, нажмите **Добавить** и заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.

- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **PSK**. В поле **PSK-ключ** будет сгенерирован случайный PSK-ключ. Он потребуется для настройки подключения в MikroTik.
- **Тип идентификатора** - выберите **auto**.
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего IPsec-подключения в MikroTik.

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.

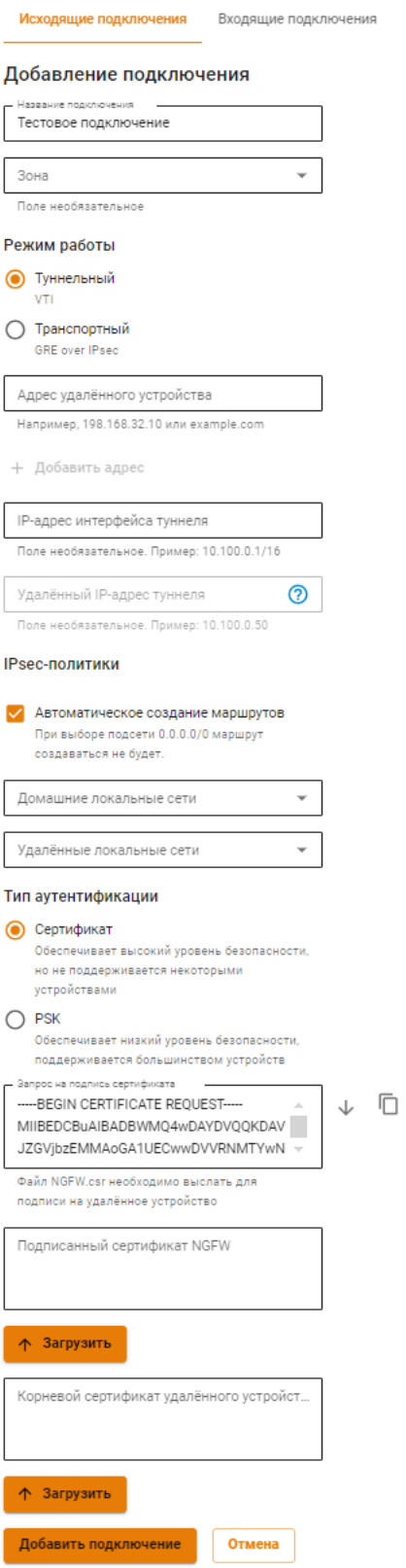
Тип аутентификации Сертификат

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.
- **Режим работы** - выберите **Туннельный**.
- **Адрес удаленного устройства** - укажите внешний IP-адрес MikroTik.

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **Сертификат**.
- **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.

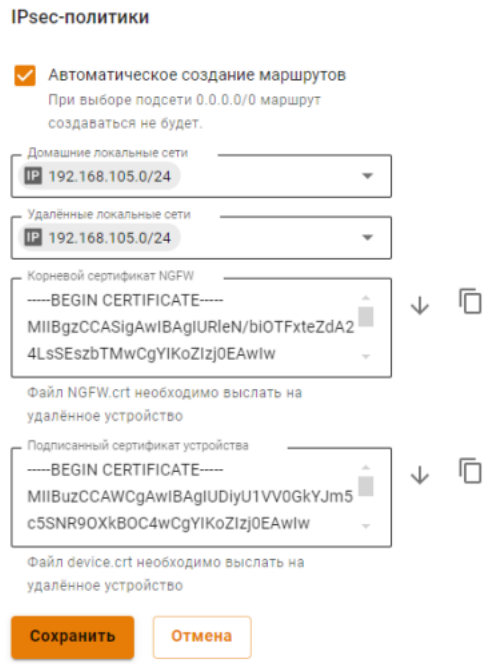
В файловой системе MikroTik появятся два файла, которые необходимо скачать, чтобы впоследствии загрузить на NGFW:



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:

1. 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:

2. Нажмите кнопку **Добавить подключение**.

Подключение от MikroTik к Ideco NGFW

Тип аутентификации PSK

Настройка MikroTik:

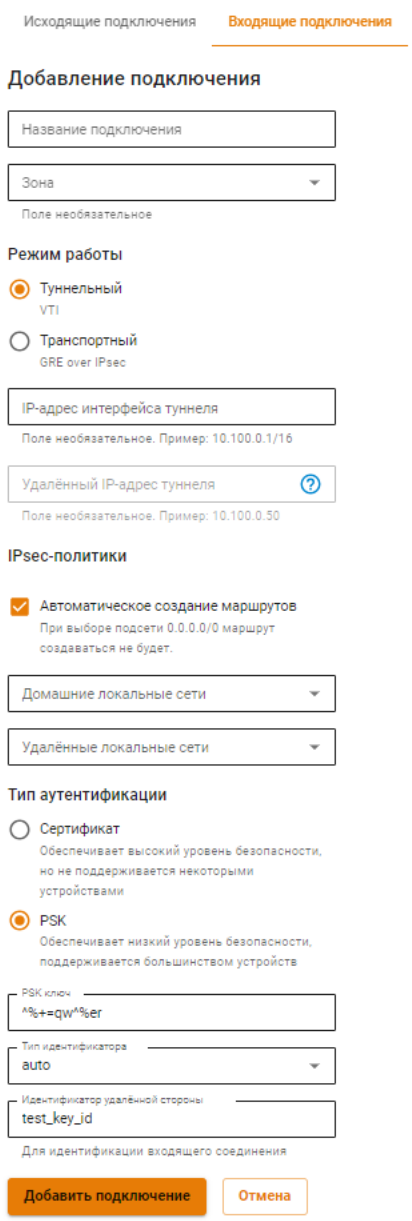
Настроить устройство MikroTik можно:

- 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.
- **Режим работы** - выберите **Туннельный**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.

- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - вставьте PSK-ключ, полученный от MikroTik.
- **Тип идентификатора** - выберите **auto**.
- **Идентификатор удаленной стороны** - вставьте идентификатор MikroTik (параметр key-id в `/ip ipsec peers`).

2. Нажмите кнопку **Добавить подключение**.

Тип аутентификации Сертификат

Подключение по сертификатам является более безопасным, чем подключение по PSK.

Настройка MikroTik:

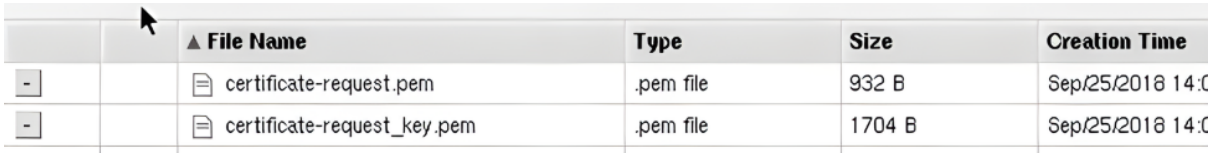
Настроить MikroTik можно:

- 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:



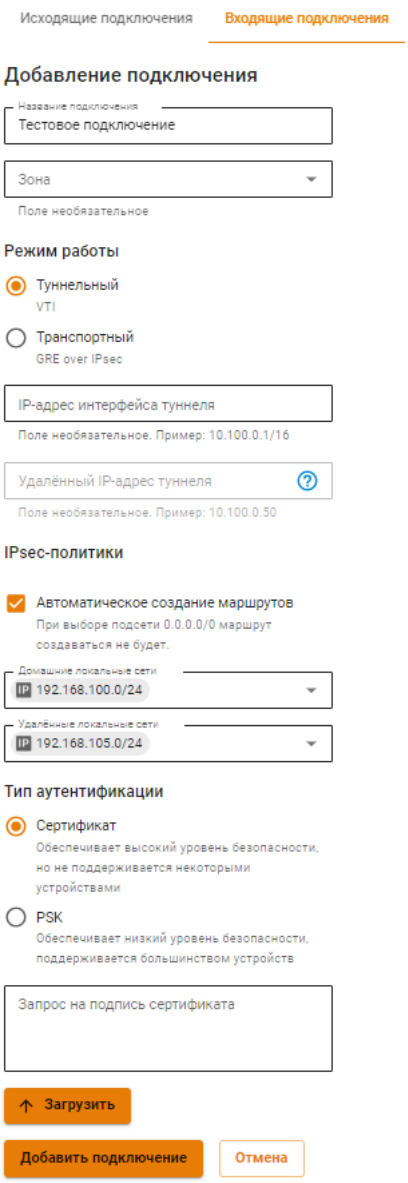
		File Name	Type	Size	Creation Time
-		certificate-request.pem	.pem file	932 B	Sep/25/2018 14:0
-		certificate-request_key.pem	.pem file	1704 B	Sep/25/2018 14:0

- Файл `certificate-request.pem` - **запрос на подпись сертификата**.
- Файл `certificate-request_key.pem` - **приватный ключ**.

Далее переходим к настройке Ideco NGFW.

Настройка Ideco NGFW:

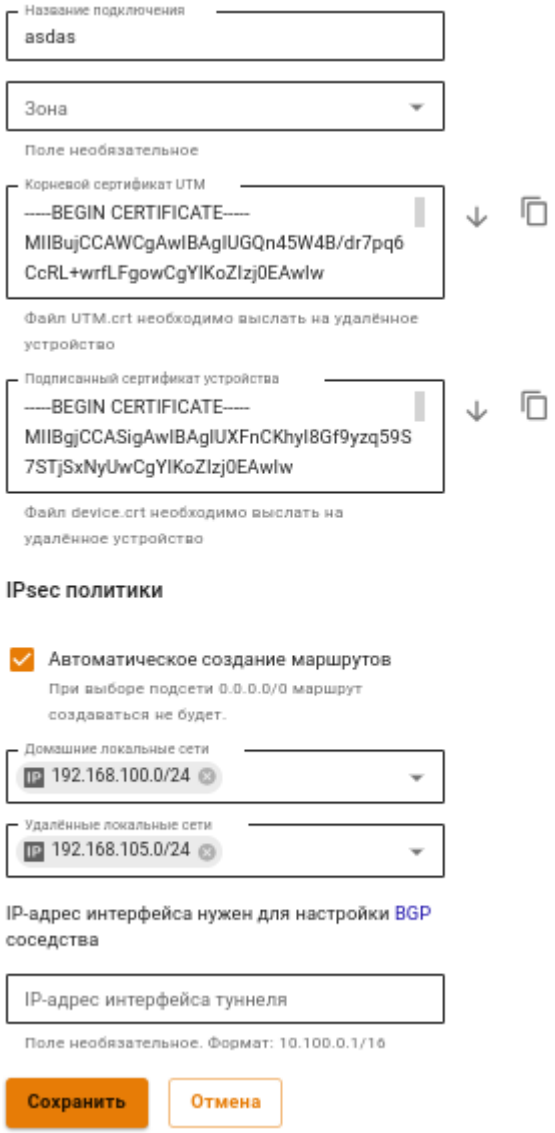
1. В Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**, нажмите **Добавить** и заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону, в которую требуется добавить IPsec-подключение.
- **Режим работы** - выберите **Туннельный**.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное.
- **Домашние локальные сети** - перечислите все **локальные сети NGFW**, которые будут видны противоположной стороне.
- **Удаленные локальные сети** - перечислите все **локальные сети MikroTik**, которые будут видны противоположной стороне.
- **Тип аутентификации** - выберите **Сертификат**.
- **Запрос на подпись сертификата** - загрузите запрос на подпись, **полученный от MikroTik**.

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:

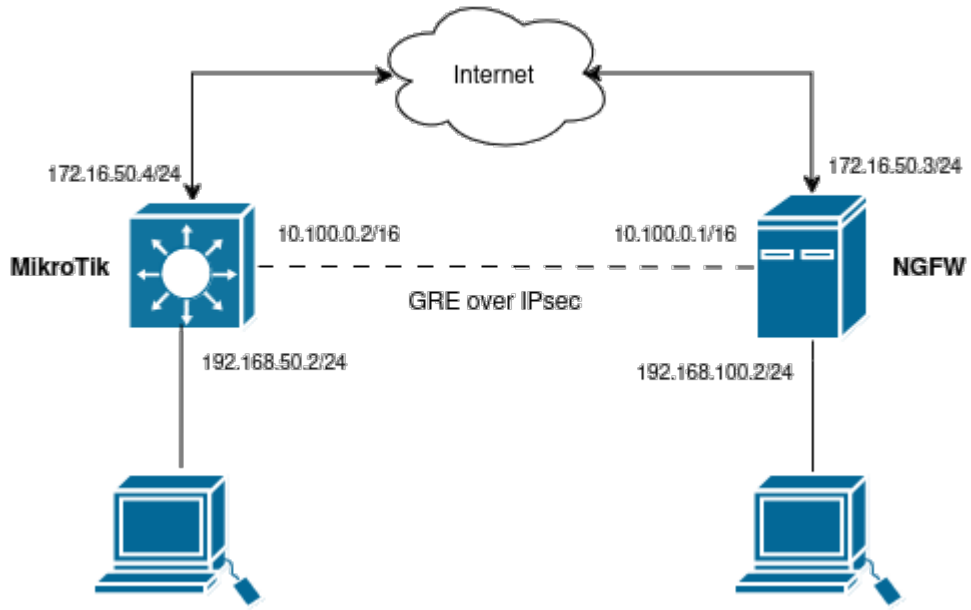


Подключение в Транспортном режиме (GRE over IPsec)

Подсказка: GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

Рассмотрим настройку подключения по схеме:



- `172.16.50.3/24` - внешний IP-адрес NGFW.
- `192.168.100.2/24` - локальный IP-адрес NGFW.
- `10.100.0.1/16` - IP-адрес GRE-туннеля NGFW.
- `172.16.50.4/24` - внешний IP-адрес MikroTik.
- `192.168.50.2/24` - локальный IP-адрес MikroTik.
- `10.100.0.2/16` - IP-адрес GRE-туннеля MikroTik.

Для настройки подключения MikroTik и Ideco NGFW следуйте инструкции в каждом из пунктов.

Подключение от Ideco NGFW к MikroTik

Предварительная настройка MikroTik:

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

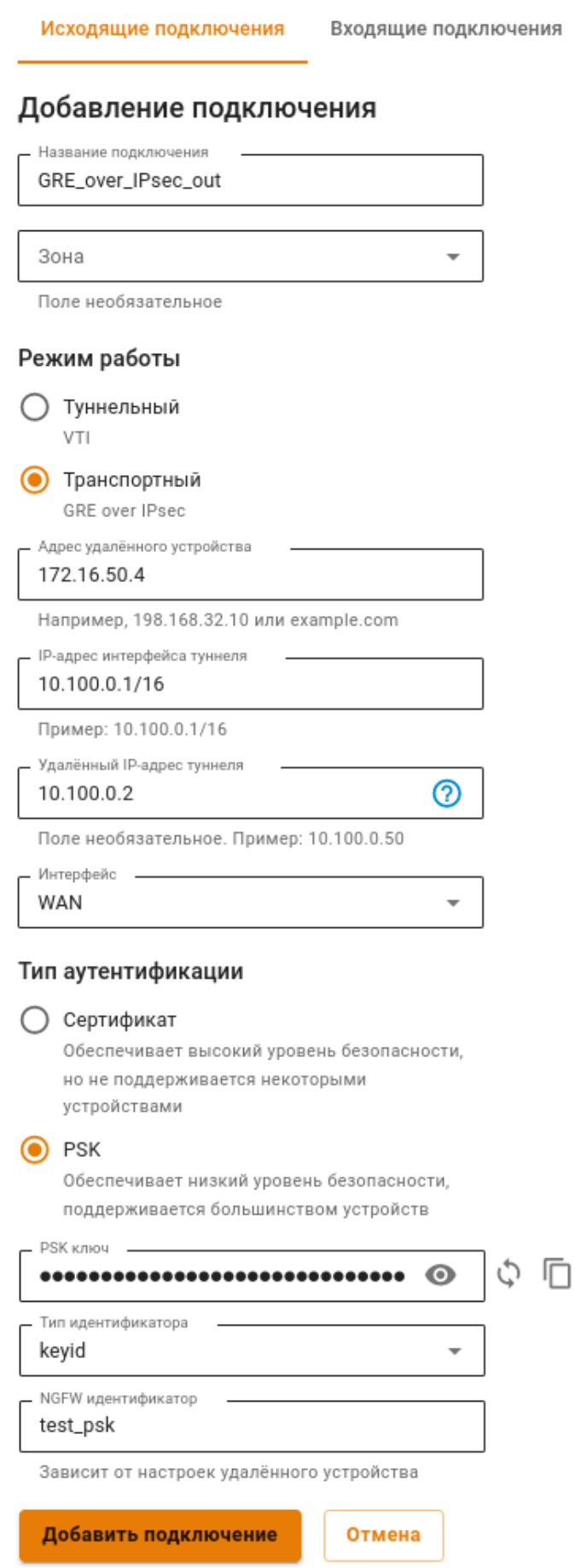
2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1␣
↪remote-address=172.16.50.3
/ip address add address=10.100.0.2/16 interface=gre-tunnel1 network=10.100.0.0
```

Тип аутентификации PSK

Настройка исходящего подключения на Ideco NGFW:

1. Заполните поля:


Исходящие подключения
Входящие подключения
Добавление подключения
Название подключения
GRE_over_IPsec_out
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
Адрес удалённого устройства
172.16.50.4
Например, 198.168.32.10 или example.com
IP-адрес интерфейса туннеля
10.100.0.1/16
Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
10.100.0.2
Поле необязательное. Пример: 10.100.0.50
Интерфейс
WAN
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
PSK ключ
Тип идентификатора
keyid
NGFW идентификатор
test_psk
Зависит от настроек удалённого устройства
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения.
- **Режим работы** - выберите **Транспортный** режим.
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Интерфейс** - выберите внешний интерфейс NGFW.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - будет сгенерирован случайный PSK-ключ. Он потребуется для настройки подключения в MikroTik.
- **Тип идентификатора** - выберите **keyid**.
- **NGFW идентификатор** - введенный ключ (**key-id**) будет использоваться для идентификации входящего подключения в MikroTik.

2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Настройка входящего подключения на MikroTik:

1. Настройте IPsec-подключение со стороны MikroTik:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256␣
↪name=from_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=from_192.168.100.0/24 enc-
↪algorithms=aes-256-cbc name=172.16.50.3 pfs-group=modp4096

/ip ipsec peer add address=172.16.50.3/32 comment=from_192.168.100.0/24 exchange-
↪mode=ike2 name=from_192.168.100.0/24 passive=yes profile=from_192.168.100.0/24

/ip ipsec identity add comment=from_192.168.100.0/24 peer=from_192.168.100.0/24␣
↪secret="<Сгенерированный NGFW PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24␣
↪proposal=172.16.50.3 protocol=gre src-address=172.16.50.4/32
```

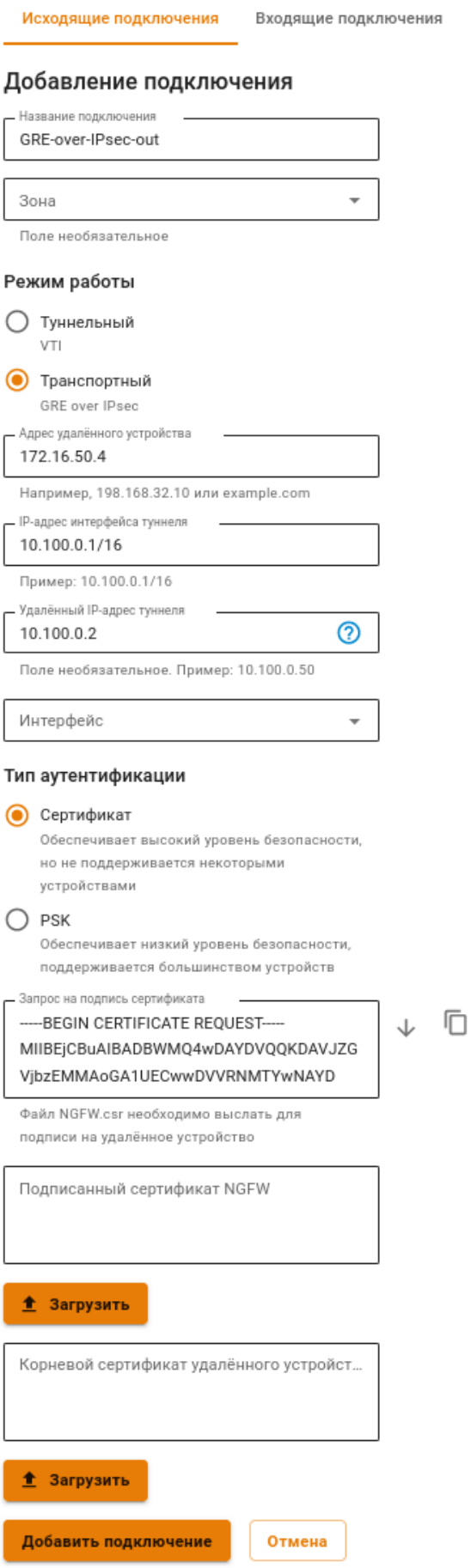
2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Тип аутентификации Сертификат

Настройка исходящего IPsec-подключения на Ideco NGFW:

1. Перейдите в раздел **IPsec -> Исходящие подключения** и нажмите **Добавить**.

2. Заполните поля:


Исходящие подключения
Входящие подключения
Добавление подключения
Название подключения
GRE-over-IPsec-out
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
Адрес удалённого устройства
172.16.50.4
Например, 198.168.32.10 или example.com
IP-адрес интерфейса туннеля
10.100.0.1/16
Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
10.100.0.2
Поле необязательное. Пример: 10.100.0.50
Интерфейс
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
Запрос на подпись сертификата
-----BEGIN CERTIFICATE REQUEST-----
MIIBEjCBuAIBADBWMQ4wDAYDVQQKDAVJZG
VjbzEMMAoGA1UECwwDVVRNMTYwNAYD
Файл NGFW.csr необходимо выслать для подписи на удалённое устройство
Подписанный сертификат NGFW
Загрузить
Корневой сертификат удалённого устройст...
Загрузить
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения.
- **Режим работы** - выберите **Транспортный** режим.
- **Адрес удаленного устройства** - укажите внешний IP-адрес устройства MikroTik.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Интерфейс** - выберите интерфейс NGFW.
- **Тип аутентификации** - выберите **Сертификат**.

3. Загрузите **Запрос на подпись сертификата**.

4. Не закрывая форму создания исходящего подключения NGFW, перейдите к настройке Mikrotik.

Настройка входящего подключения на MikroTik:

1. Загрузите скачанный ранее файл с **Запросом на подпись сертификата** (`NGFW.crt`) на MikroTik через WinBox или по ssh.

2. Создайте корневой сертификат MikroTik:

```
/certificate add common-name=mk_ca name=mk_ca_template key-usage=key-cert-sign,crl-
↪sign,digital-signature,content-commitment
/certificate sign mk_ca_template ca-crl-host=172.16.50.4 name=mk_ca
```

3. Подпишите сертификат Ideco NGFW и сделайте его доверенным:

```
/certificate sign-certificate-request file-name=NGFW.csr ca=mk_ca
/certificate set [find name~"^device_.+\\.ipsec\$"] trusted=yes
```

4. Экспортируйте корневой сертификат MikroTik и подписанный сертификат NGFW в формат `.pem`:

```
/certificate export-certificate mk_ca type=pem
/certificate export-certificate [find name~"^device_.+\\.ipsec\$"] type=pem
```

5. Загрузите с MikroTik корневой сертификат MikroTik и подписанный сертификат NGFW через WinBox или по ssh. Названия файлов содержат `cert_export`.

6. Настройте входящее IPsec-соединение на MikroTik:

```
/ip ipsec profile add name=from_192.168.100.0/24 hash-algorithm=sha256 enc-
↪algorithm=aes-256 dh-group=modp4096 dpd-interval=120s dpd-maximum-failures=5

/ip ipsec peer add name=from_192.168.100.0/24 address=172.16.50.3/32 profile=from_192.
↪168.100.0/24 exchange-mode=ike2 passive=yes comment=from_192.168.100.0/24

/ip ipsec identity add peer=from_192.168.100.0/24 auth-method=digital-signature␣
↪certificate=mk_ca remote-certificate=[: put [/certificate get [/certificate find␣
↪name~"^device_.+\\.ipsec\$"] name]] comment=from_192.168.100.0/24

/ip ipsec proposal add name=172.16.50.3 enc-algorithms=aes-256-cbc auth-
↪algorithms=sha256 pfs-group=modp4096 comment=from_192.168.100.0/24

/ip ipsec policy add dst-address=172.16.50.3/32 peer=from_192.168.100.0/24␣
↪proposal=172.16.50.3 protocol=gre src-address=172.16.50.4/32
```

7. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Донастройка исходящего IPsec-подключение на Ideco NGFW:

Вернитесь к форме создания исходящего IPsec-соединения на Ideco NGFW.

1. Загрузите скачанные ранее файлы **Корневого сертификата MikroTik** (`cert_export_mk_ca.crt`) и **Подписанный сертификат NGFW** (`cert_export_device_53c34ddc6d584d938f2098eae838e6ff.ipsec.crt`) в поля **Корневой сертификат удаленного устройства** и **Подписанный сертификат NGFW** соответственно.

2. Нажмите **Сохранить**.

3. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Подключение от MikroTik к Ideco NGFW

Тип аутентификации PSK

Настройка исходящего подключения на MikroTik:

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1␣
↪remote-address=172.16.50.3
/ip address add address=10.100.0.2/16 interface=gre-tunnel1 network=10.100.0.0
```

3. Настройте IPsec-подключение со стороны MikroTik:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256␣
↪name=to_192.168.100.0/24

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-
↪algorithms=aes-256-cbc name=172.16.50.3 pfs-group=modp4096

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-
↪mode=ike2 name=to_192.168.100.0/24 profile=to_192.168.100.0/24

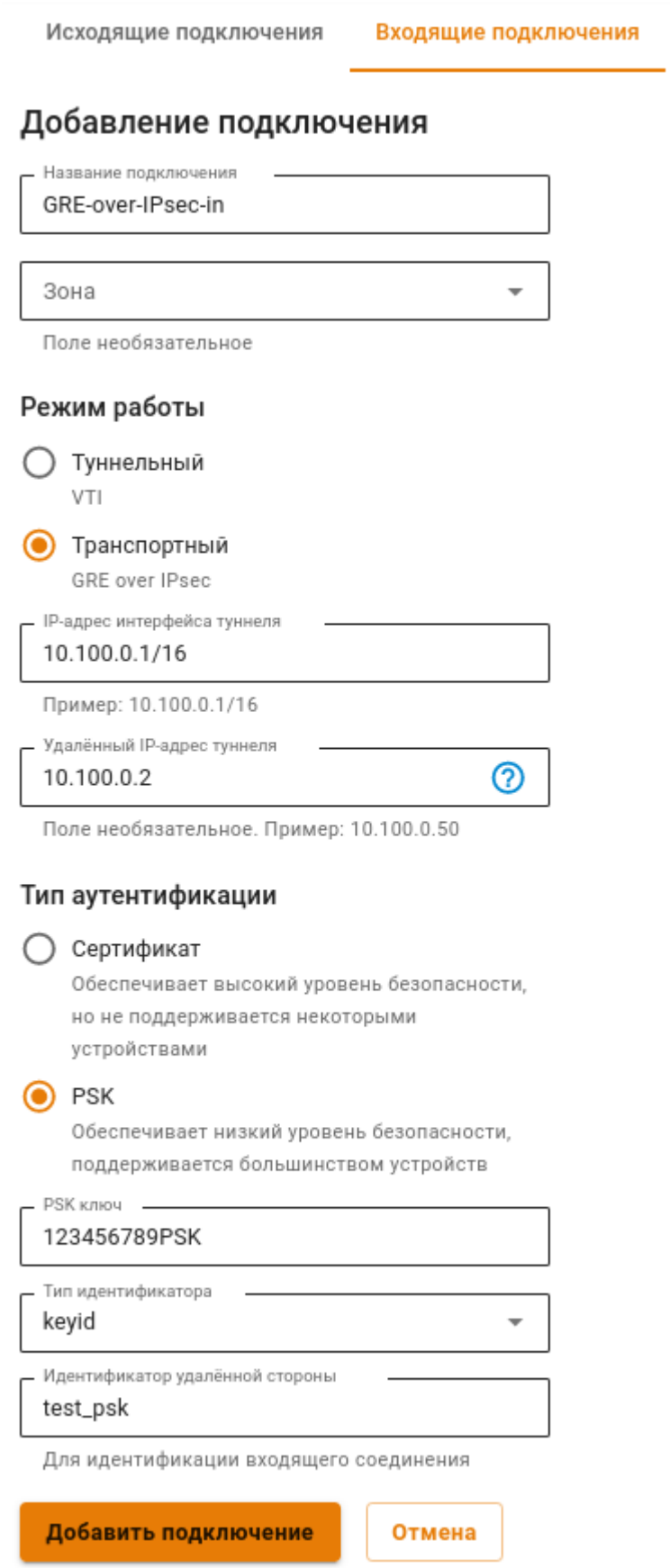
/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 my-id=key-
↪id:"test_psk" secret="<PSK-ключ>"

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.
↪16.50.3 protocol=gre src-address=172.16.50.4/32
```

4. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

Настройка входящего подключения на Ideco NGFW:

1. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.

- **Зона** - укажите зону для добавления IPSec-подключения.
- **Режим работы** - выберите **Транспортный** режим.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **PSK**.
- **PSK-ключ** - введите PSK-ключ, указанный при настройке исходящего IPsec-подключения в MikroTik.
- **Тип идентификатора** - выберите **keyid**.
- **NGFW идентификатор** - введите **key-id**, использованный при настройке исходящего IPsec-подключения в MikroTik.

2. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Тип аутентификации Сертификат

Предварительная настройка MikroTik:

1. Настройте на MikroTik IP-адреса:

```
/ip address add address=172.16.50.4/24 interface=ether1 network=172.16.50.0
/ip address add address=192.168.50.2/24 interface=ether2 network=192.168.50.0
```

2. Создайте GRE-интерфейс и назначьте ему IP-адрес:

```
/interface gre add allow-fast-path=no local-address=172.16.50.4 name=gre-tunnel1␣
↪remote-address=172.16.50.3
/ip address add address=10.100.0.2/16 interface=gre-tunnel1 network=10.100.0.0
```

3. Сгенерируйте запрос на подпись сертификата:

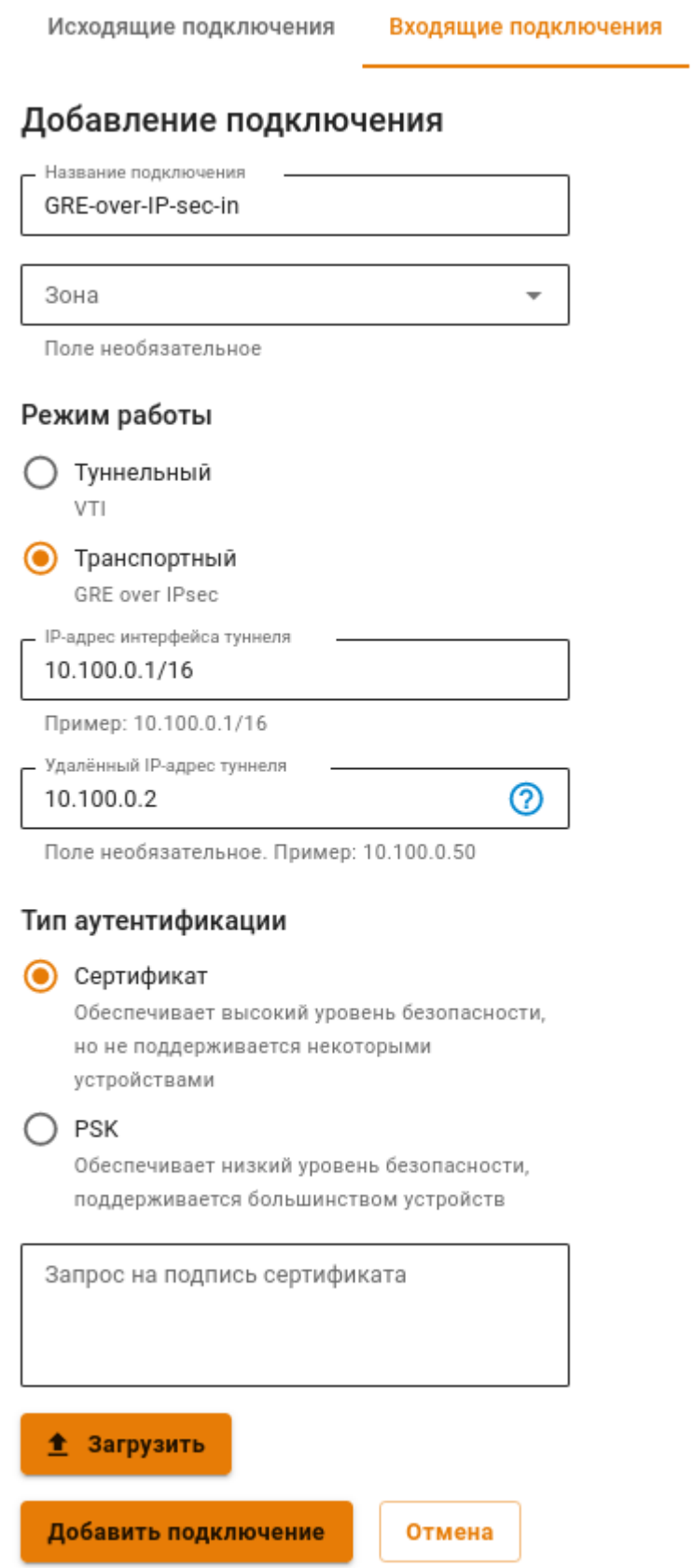
```
/certificate add name=mk_ca common-name=mk_ca key-usage=digital-signature,content-
↪commitment
/certificate create-certificate-request key-passphrase="" template=mk_ca
```

4. Загрузите файл `certificate-request.pem` с MikroTik через WinBox или по ssh.

Настройка входящего IPsec-подключения на Ideco NGFW:

1. Перейдите в раздел **IPsec -> Входящие подключения** и нажмите **Добавить**.

2. Заполните поля:



- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов.
- **Зона** - укажите зону для добавления IPSec-подключения.

- **Режим работы** - выберите **Транспортный** режим.
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW.
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля MikroTik. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере. **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля** должны находиться в одной подсети.
- **Тип аутентификации** - выберите **Сертификат**.

3. Загрузите скачанный ранее с MikroTik файл `certificate-request.pem` в поле **Запрос на подпись сертификата**.

4. Нажмите **Сохранить**.

5. Откройте созданное IPsec-соединение, нажав на  и загрузите файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанный сертификат устройства** (`device.crt`).

6. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного MikroTik.

Настройка исходящего IPsec-подключение на MikroTik:

1. Загрузите на MikroTik скачанные ранее файлы **Корневого сертификата NGFW** (`NGFW.crt`) и **Подписанный сертификат устройства** (`device.crt`) через WinBox или по ssh.

2. Импортируйте сертификаты:

```
/certificate import file-name=NGFW.crt passphrase=""
/certificate import file-name=device.crt passphrase=""
/certificate import file-name=certificate-request_key.pem passphrase=""
```

3. Настройте IPsec-соединение:

```
/ip ipsec profile add dh-group=modp4096 enc-algorithm=aes-256 hash-algorithm=sha256␣
↪name=to_192.168.100.0/24 dpd-interval=120s dpd-maximum-failures=5

/ip ipsec peer add address=172.16.50.3/32 comment=to_192.168.100.0/24 exchange-
↪mode=ike2 name=to_192.168.100.0/24 profile=to_192.168.100.0/24

/ip ipsec identity add comment=to_192.168.100.0/24 peer=to_192.168.100.0/24 auth-
↪method=digital-signature certificate=device.crt_0 remote-certificate=NGFW.crt_0

/ip ipsec proposal add auth-algorithms=sha256 comment=to_192.168.100.0/24 enc-
↪algorithms=aes-256-cbc name=172.16.50.3 pfs-group=modp4096

/ip ipsec policy add dst-address=172.16.50.3/32 peer=to_192.168.100.0/24 proposal=172.
↪16.50.3 protocol=gre src-address=172.16.50.4/32
```

4. Настройте статическую или динамическую маршрутизацию до локальных сетей удаленного NGFW.

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.

18.12.9 Подключение MikroTik и Ideco NGFW по L2TP/IPsec

Подключение MikroTik к Ideco NGFW по L2TP/IPsec

- Настройте VPN-сервер на Ideco NGFW в разделе **Пользователи -> VPN-подключения**. Подробная инструкция по настройке - в статье *Подключение по L2TP/IPsec*;
- Настройте подключение на MikroTik, выполнив команды:

1. Отредактируйте IPsec profile:

```
ip ipsec profile set default hash-algorithm=sha1 enc-algorithm=aes-256 dh-
↪group=modp2048
```

2. Отредактируйте IPsec proposals:

```
ip ipsec proposal set default auth-algorithms=sha1 enc-algorithms=aes-256-cbc,aes-192-
↪cbc,aes-128-cbc pfs-group=modp2048
```

3. Создайте подключение к Ideco NGFW:

```
interface l2tp-client add connect-to=<server> profile=default disabled=no name=
↪<interface_name> password="<password>" user="<login>" use-ipsec="yes" ipsec-secret="
↪<psk>"
```

4. Добавьте маршрут до первого адреса VPN-сети NGFW (remote VPN subnet):

```
ip route add dst-address=<remote VPN subnet> gateway=l2tp-out1
```

Подсказка: Для работы удаленных сетей на NGFW и на MikroTik нужно создавать маршруты на обоих устройствах.

Подсказка: Если у вас в разделе **Правила трафика -> Файрвол -> SNAT** отключен **Автоматический SNAT локальных сетей**, то может понадобиться прописать маршрут до сети VPN, где шлюзом является NGFW.

Пример:

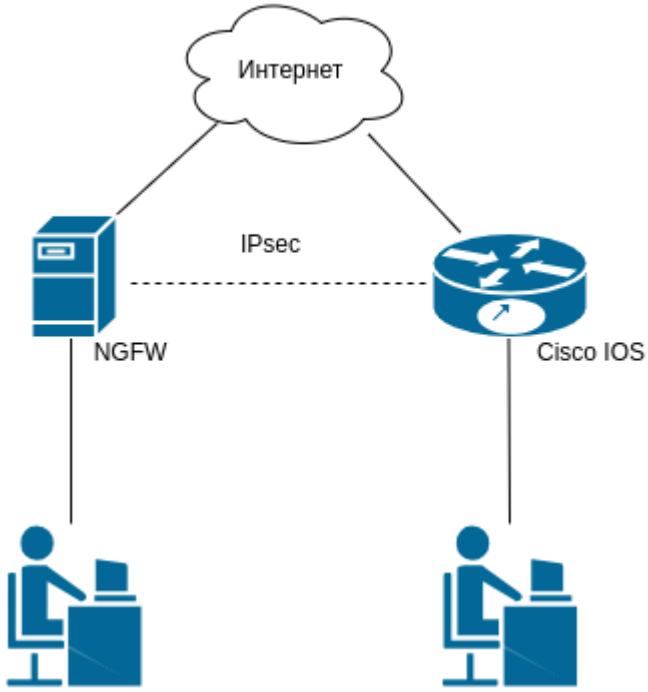
- Адрес NGFW = `169.254.1.5`
- Первый адрес VPN = `10.128.0.1`

```
ip route add dst-address=169.254.1.5 gateway==10.128.0.1
```

18.12.10 Подключение Cisco IOS и Ideco NGFW

Настройка подключения в туннельном режиме

Рассмотрим настройку подключения по схеме 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 XE

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
```

(continues on next page)

(продолжение с предыдущей страницы)

```
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 на Ideco NGFW:

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Режим работы** - выберите **Туннельный**;
- **Адрес удаленного устройства** - введите IP-адрес Cisco;

- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Поле необязательное. Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интрефейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW;
- **Удаленные локальные сети** - укажите локальную сеть Cisco;
- **Тип аутентификации** - PSK;
- **PSK** - будет сгенерирован случайный PSK-ключ. Он потребуется, чтобы настроить подключение в Cisco;
- **Идентификатор NGFW** - введенный вами ключ будет использоваться для идентификации исходящего подключения. Введите также этот идентификатор в Cisco.

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 на Ideco NGFW:

Для настройки входящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Устройства (входящие подключения)**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля Cisco. Поле необязательное. Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интрефейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети. заполняется для получения статистики обмена пакетами;
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW;
- **Удаленные локальные сети** - укажите локальную сеть Cisco;
- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ;
- **Идентификатор удаленной стороны** - вставьте идентификатор Cisco (параметр Key ID).

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
 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

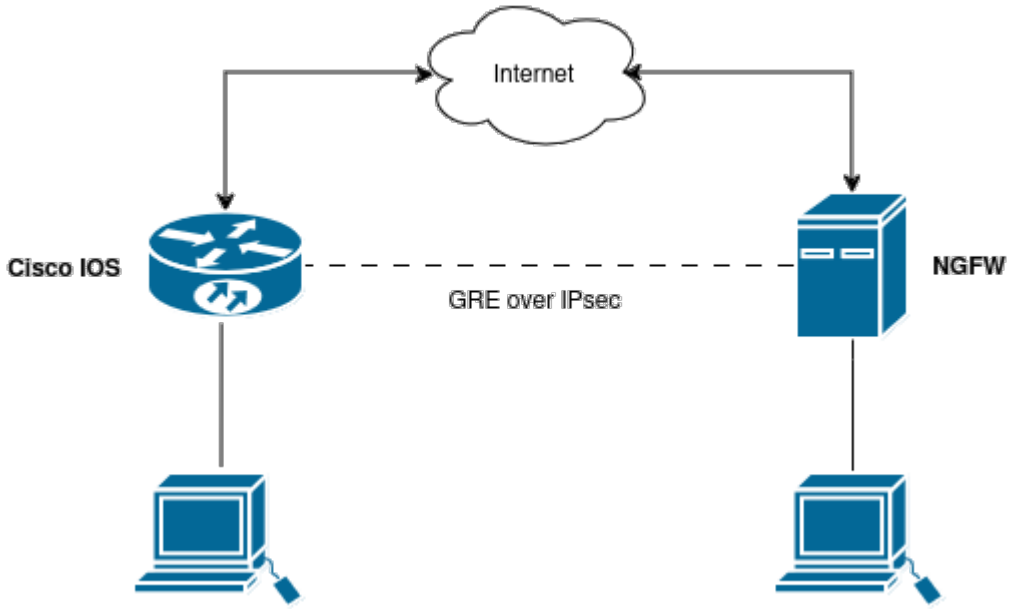
ip access-list extended NAT
 deny   ip 2.2.2.0 0.0.0.255 3.3.3.0 0.0.0.255
 permit ip 2.2.2.0 0.0.0.255 any
ip access-list extended cryptoacl
 permit ip 2.2.2.0 0.0.0.255 3.3.3.0 0.0.0.255
```

Настройка подключения в транспортном режиме

Подсказка: GRE over IPsec поддерживает мультикаст-трафик, что позволяет использовать более сложные механизмы маршрутизации, включая динамическую маршрутизацию через OSPF.

Также в GRE over IPsec не требуется задавать **Домашние локальные сети** и **Удаленные локальные сети**. Транспортный режим IPsec шифрует только то, что выше уровня IP, а заголовок IP оставляет без изменений.

Рассмотрим настройку подключения по схеме 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 через консоль

1. Настройка локального интерфейса:

```
enable
conf t
interface GigabitEthernet2
ip address <локальный IP Cisco> <маска подсети>
no shutdown
exit
```

2. Настройка внешнего интерфейса:

```
interface GigabitEthernet1
ip address <внешний IP Cisco> <маска подсети>
```

(continues on next page)

(продолжение с предыдущей страницы)

```
no shutdown
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. Сохранение настроек конфигурации:

```
write memory
```

5. **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+GRE-over-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 transport
exit
```

6. Настройка профиля IPsec:

```
crypto ipsec profile SECURE-P
set transform-set SECURE-TS
set pfs group2
```

7. Настройка GRE-over-IPsec-туннеля:

```
interface Tunnel1
description to_NGFW
ip address <IP GRE-over-IPsec-интерфейса Cisco> <маска подсети>
tunnel source <внешний IP Cisco>
tunnel destination <внешний IP NGFW>
tunnel mode ipsec ipv4
tunnel protection ipsec profile SECURE-P
```

8. Настройка маршрута:

```
ip route <локальная подсеть за NGFW> <маска подсети> <IP GRE-over-IPsec-интерфейса␣
↪NGFW>
```

9. Сохранение настроек конфигурации:

```
write memory
```

Настройка исходящего подключения на Ideco NGFW:

Для настройки исходящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Режим работы** - выберите **Транспортный**;
- **Адрес удаленного устройства** - введите IP-адрес Cisco;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля Cisco. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере.
- **Тип аутентификации** - PSK;
- **PSK** - будет сгенерирован случайный PSK-ключ. Он потребуется, чтобы настроить подключение в Cisco;
- **NGFW идентификатор** - введенный вами ключ будет использоваться для идентификации исходящего подключения. Введите также этот идентификатор в Cisco.

3. Проверьте, что подключение установилось (в столбце **Статусы** зеленым цветом будет подсвечена надпись **Установлено**).

4. Проверьте наличие трафика между локальными сетями (TCP и web).

Настройка входящего подключения на Ideco NGFW:

Для настройки входящего IPsec-подключения на Ideco NGFW выполните действия:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Устройства(входящие подключения)**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPsec-подключения;
- **Режим работы** - выберите **Транспортный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса GRE-туннеля NGFW;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса GRE-туннеля Cisco. Поле необязательное и заполняется для получения статистики о потере пакетов, средней задержке и джиттере.
- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ;
- **Идентификатор удаленной стороны** - вставьте идентификатор Cisco (параметр Key ID).

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 GRE over 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 172.168.10.25
  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 transport

crypto ipsec profile SECURE-P
 set transform-set SECURE-TS
 set pfs group2
!
interface Tunnel1
 description to_NGFW
 ip address 192.168.200.1 255.255.255.0
 tunnel source 192.168.233.204 # <внешний IP Cisco>
 tunnel destination 172.168.10.25 # <внешний IP NGFW>
```

(continues on next page)

(продолжение с предыдущей страницы)

```
 tunnel protection ipsec profile SECURE-P
!
ip route 192.168.0.0 255.255.255.0 192.168.200.2

interface GigabitEthernet1
! внешний интерфейс
 ip address 192.168.233.204 255.255.255.0
 crypto map cmap

interface GigabitEthernet2
! локальный интерфейс
 ip address 192.168.10.1 255.255.255.0
```

18.12.11 Подключение pfSense к Ideco NGFW по IPsec

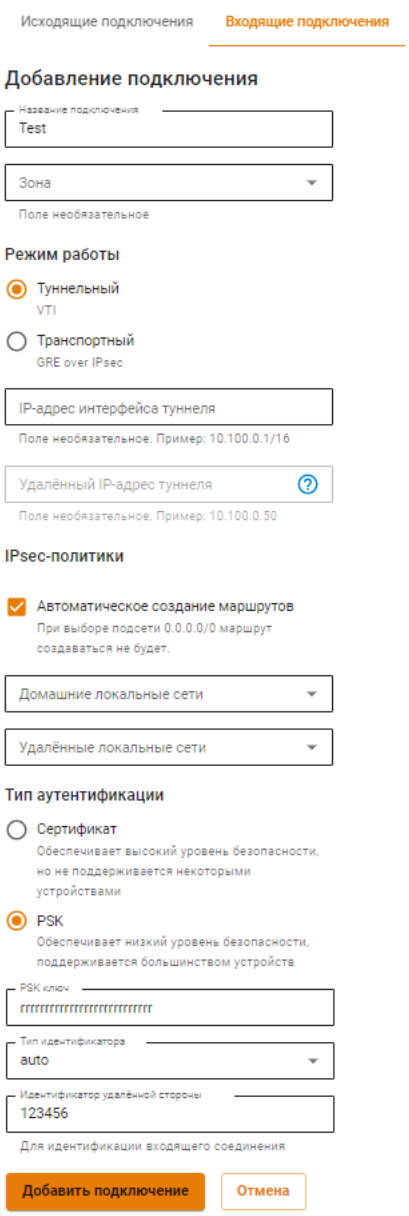
Подсказка: Объединяемые локальные сети не должны пересекаться!

Настройка входящего подключения

Для настройки Ideco NGFW следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**.

2. Добавьте новое подключение:



- **Название подключения** - любое;
- **Зона** - укажите зону для добавления IPSec-подключения;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами;
- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения;
- **Идентификатор удаленной стороны** - любой;
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense;

- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW.

Подсказка: Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интрефейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

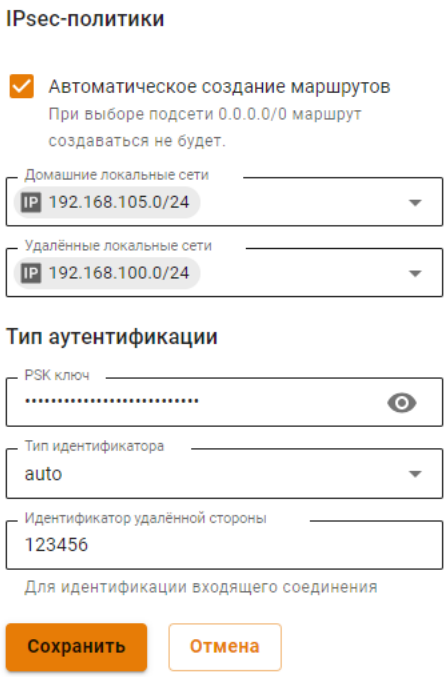
---

3. Сохраните созданное подключение, нажмите на кнопку **Включить**.

4. Скопируйте значение идентификатора удаленной стороны одним из способов:

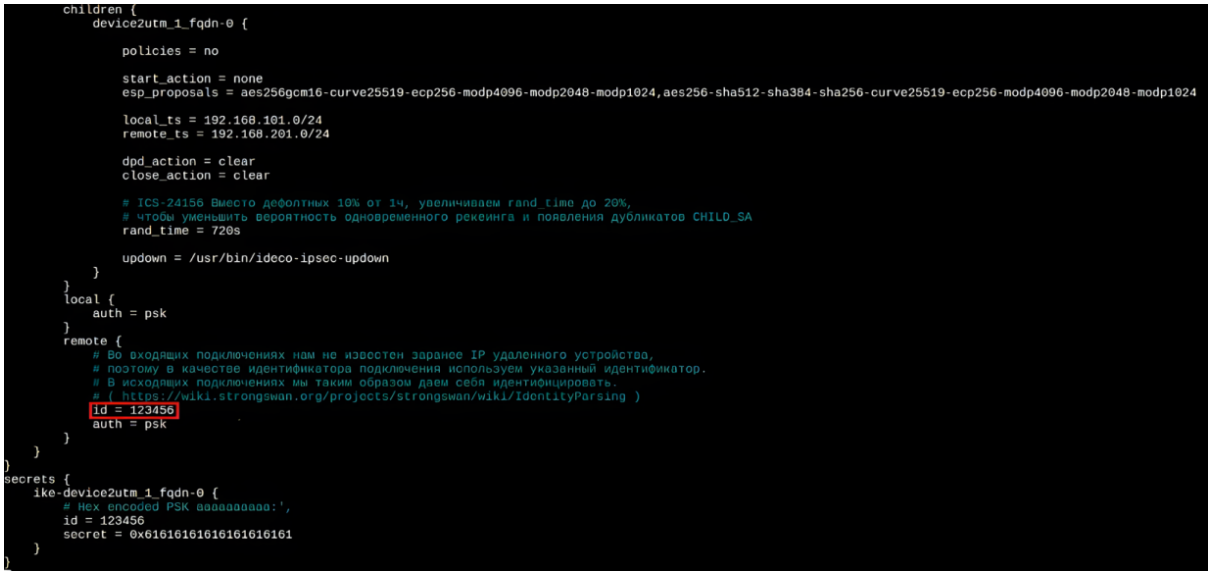
В интерфейсе NGFW:

На вкладке **Сервисы -> IPsec -> Входящие подключения** в строке **Идентификатор удаленной стороны**:



Через терминал:

На Ideco NGFW в папке `/run/ideco-ipsec-backend/strongswan/swanctl/conf.d/` будет сгенерирован конфигурационный файл. Необходимо перейти в консоль и открыть на редактирование файл вида `device_<номер>.conf`. Из этого файла необходимо скопировать значение строки `id`(идентификатор удаленной стороны):



5. Перейдите к настройке pfSense, предварительно записав значение строки `id` (идентификатор удаленной стороны).

Настройка pfSense:

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите на вкладку **VPN –> IPsec –> Tunnels**.

2. Добавьте новое подключение:

- **Description** - любое;
- **Key Exchange version** - IKEv2;
- **Internet Protocol** - IPv4;
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW;
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;
- **Authentication Method** - Mutual PSK;
- **My identifier и Peer identifier** - сюда вставьте значение строки `id` на Ideco NGFW (см. шаг 4 в настройке Ideco NGFW);
- **Pre-Shared Key** - вставьте PSK-ключ, который ранее прописывали на Ideco NGFW;
- **Encryption Algorithm** - используйте следующие параметры: \
  - **Algorithm** - AES256-GCM; \
  - **Key length** - 128 bit; \
  - **Hash** - SHA256; \
  - **DH Group** - Elliptic Curve 25519-256.

Все остальные значения можно оставить по умолчанию.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2. Здесь укажите:

- **Encryption Algorithm** - используйте следующие параметры: \
  - **Algorithm** - AES256-GCM; \
  - **Key length** - 128 bit; \
  - **Hash** - SHA256; \

  - **DH Group** - Elliptic Curve 25519-256.

- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW;
- **Remote Network** - локальную сеть Ideco NGFW, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. Разрешите хождение трафика между локальными сетями pfSense и Ideco NGFW в настройках файрвола pfSense (переходим на вкладку **Firewall -> Rules -> IPsec** и создаем два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense).

Обращаем внимание на раздел файрвола WAN - в нем по умолчанию запрещен входящий трафик из «серых» подсетей, который требуется разрешить.

7. Теперь переходим на вкладку **Status -> IPsec** (там должно появится созданное подключение), нажимаем на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы указали в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

Настройка исходящего подключения

Для настройки Ideco NGFW следуйте пунктам:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**.

2. Добавьте новое подключение:

- **Название** - любое;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Адрес удаленного устройства** - укажите адрес удаленного устройства;
- **Тип аутентификации** - PSK;
- **PSK** - укажите PSK-ключ, который будет использоваться для подключения;
- **NGFW идентификатор** - любой;
- **Домашние локальные сети** - укажите локальную сеть Ideco NGFW, которая будет видна из подсети pfSense;
- **Удаленные локальные сети** - укажите локальную сеть pfSense, которая будет видна из подсети Ideco NGFW;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля при динамической маршрутизации BGP.

Настройка pfSense:

Для настройки следуйте пунктам:

1. В веб-интерфейсе pfSense перейдите на вкладку **VPN > IPsec > Advanced Options** и в поле **Child SA Start Action** выберите параметр **None (Responder Only)**.

2. Добавьте новое подключение:

- **Key Exchange version** - IKEv2;
- **Internet Protocol** - IPv4;
- **Interface** - выберите внешний интерфейс pfSense, который будет использоваться для подключения к Ideco NGFW;
- **Remote Gateway** - IP внешнего интерфейса Ideco NGFW;

- **Description** - любое;
- **Authentication Method** - Mutual PSK;
- **My identifier** - My ip address;
- **Peer identifier** - KeyID tag. Введите идентификатор удаленной стороны, т. е. Ideco NGFW;
- **Pre-Shared Key** - введите PSK-ключ;
- **Encryption Algorithm**:
  - Для **Ideco UTM версии 10.0 и Ideco NGFW версии 16.0 и новее** используйте следующие параметры: \
    * **Algorithm** - AES256-GCM;
    * **Key length** - 128 bit;
    * **Hash** - SHA256;
    * **DH Group** - Elliptic Curve 25519-256.

3. Сохраните подключение.

4. Нажмите на кнопку **Show Phase 2 Entries** и добавьте новую Phase 2 и укажите следующие значения:

- **Encryption Algorithm**:
  - **Для Ideco UTM версии 10.0 и Ideco NGFW версии 16.0 и новее** используйте следующие параметры: \
    * **Algorithm** - AES256-GCM;
    * **Key length** - 128 bit;
    * **Hash** - SHA256;
    * **DH Group** - Elliptic Curve 25519-256.
- **Local Network** - локальную сеть pfSense, которая будет доступна из подсети Ideco NGFW;
- **Remote Network** - локальную сеть Ideco NGFW, которая будет доступна из подсети pfSense.

Все остальные значения можно оставить по умолчанию.

5. Сохраните подключение.

6. В настройках файрвола pfSense перейдите на вкладку **Firewall -> Rules -> IPsec** и создайте два правила, разрешающие хождение трафика между локальными сетями Ideco NGFW и pfSense.

7. Обратите внимание на раздел файрвола **WAN** - в нем по умолчанию запрещен входящий трафик из «серых» подсетей, который требуется разрешить.

8. Перейдите на вкладку **Status -> IPsec** (там должно появится созданное подключение), нажмите на кнопку Connect VPN.

Если соединение установить не удалось, следует пересоздать соединение на NGFW, указав в поле **Идентификатор ключа** значение, которое мы указали в My identifier и Peer identifier у pfSense, и попробовать подключиться еще раз. На стороне pfSense никаких изменений вносить не требуется.

18.12.12 Подключение Kerio Control и Ideco NGFW по IPsec

Подсказка: Объединяемые локальные сети не должны пересекаться!

Предварительная настройка Kerio Control:

1. По умолчанию Kerio Control использует IKEv1 для создания подключений к сторонним устройствам. Включить IKEv2 можно через консоль, выполнив действия:

- Подключиться к Kerio Control по SSH;
- Перейти в папку `/var/winroute`;
- Открыть на редактирование файл `winroute.cfg`;
- В нем найти раздел, начинающийся с текста `<table name="Firewall">`;
- В этом разделе найти строку `<variable name="IKEVersion">ikev1</variable>` и изменить в ней `ikev1` на `ikev2`;
- После этого требуется перезагрузить сервер и убедиться, что изменения в настройках сохранились.

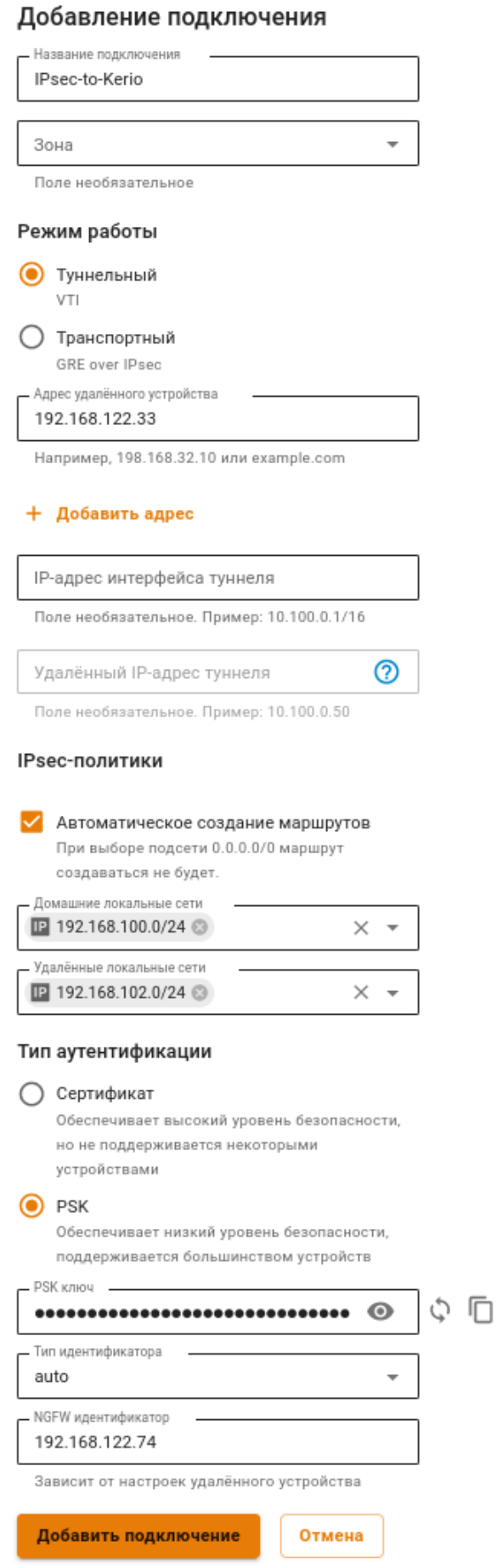
2. В разделе **Правила трафика** разрешите трафик VPN-служб.

Подключение от Ideco NGFW к Kerio Control

Настройка исходящего подключения на Ideco NGFW:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Исходящие подключения**.

2. Добавьте новое подключение и заполните поля:


Добавление подключения
Название подключения
IPsec-to-Kerio
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
Адрес удалённого устройства
192.168.122.33
Например, 198.168.32.10 или example.com
Добавить адрес
IP-адрес интерфейса туннеля
Поле необязательное. Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
Поле необязательное. Пример: 10.100.0.50
IPsec-политики
Автоматическое создание маршрутов
При выборе подсети 0.0.0.0/0 маршрут создаваться не будет.
Домашние локальные сети
192.168.100.0/24
Удалённые локальные сети
192.168.102.0/24
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
PSK ключ
Тип идентификатора
auto
NGFW идентификатор
192.168.122.74
Зависит от настроек удалённого устройства
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Режим работы** - выберите **Туннельный**;
- **Адрес удаленного устройства** - укажите внешний IP-адрес Kerio Control;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами;
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW, которая будет видна из подсети Kerio Control;
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW;
- **Тип аутентификации** - выберите тип PSK;
- **PSK-ключ** - укажите PSK-ключ, который будет использоваться для подключения;
- **Тип идентификатора** - выберите auto;
- **Идентификатор NGFW** - укажите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения:

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

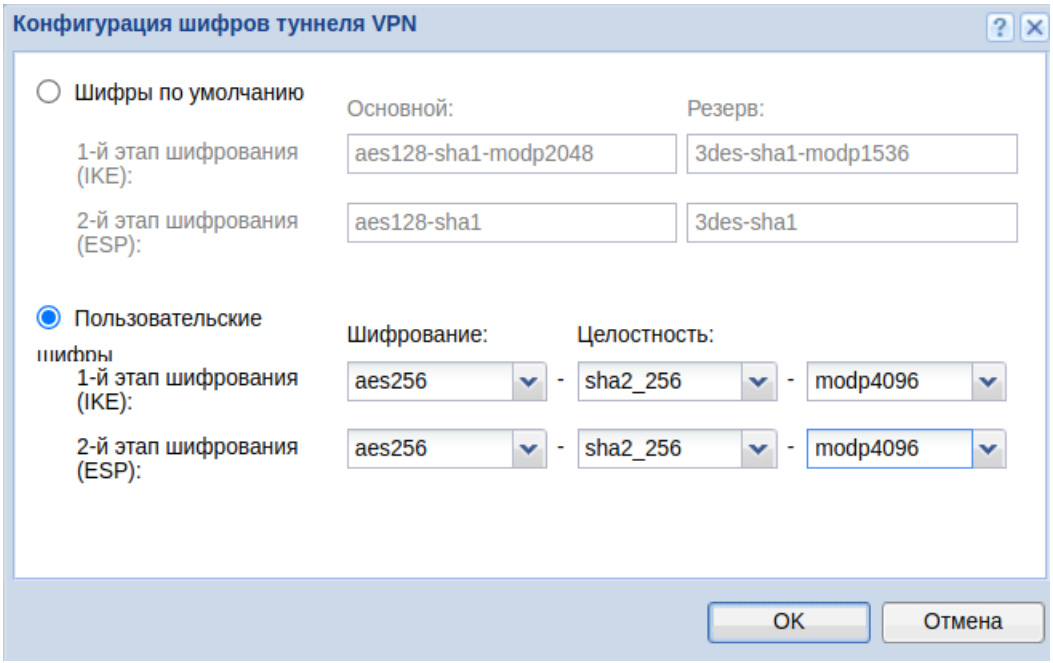
Настройка завершена, теперь переходим к настройке Kerio Control.

Настройка входящего подключения на Kerio Control:

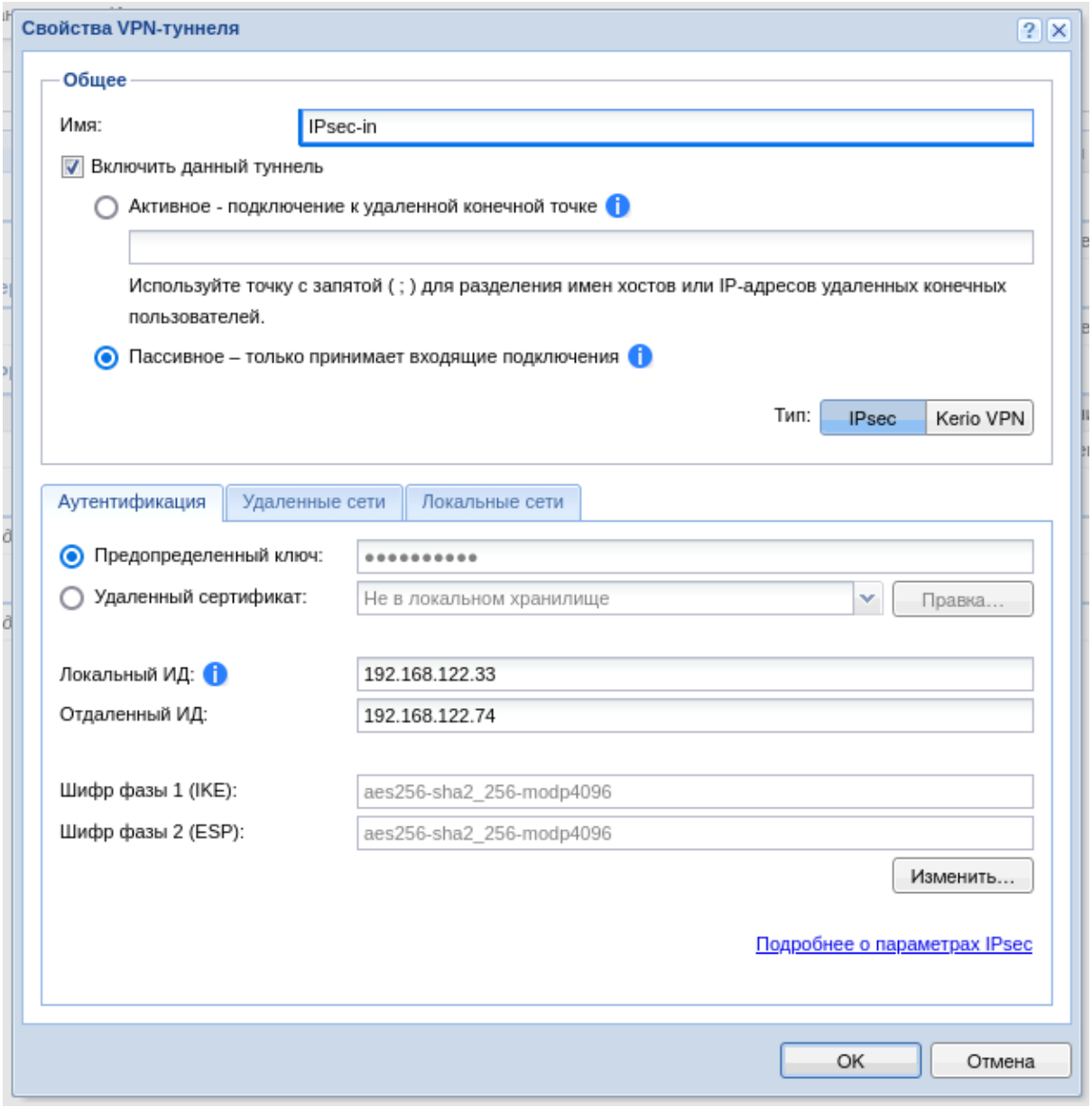
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель. . .** .

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec;
- **Имя** - произвольное;
- **Включить данный туннель**;
- Тип **Пассивное**;
- **Предопределенный ключ** - введите PSK-ключ, который был указан при создании подключения на Ideco NGFW;
- **Локальный ИД** - укажите IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения;
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW;
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



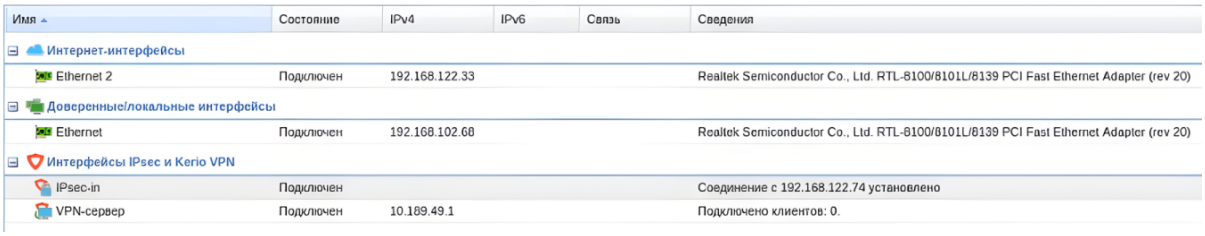
Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW, которая будет видна из подсети Kerio Control.

4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице:



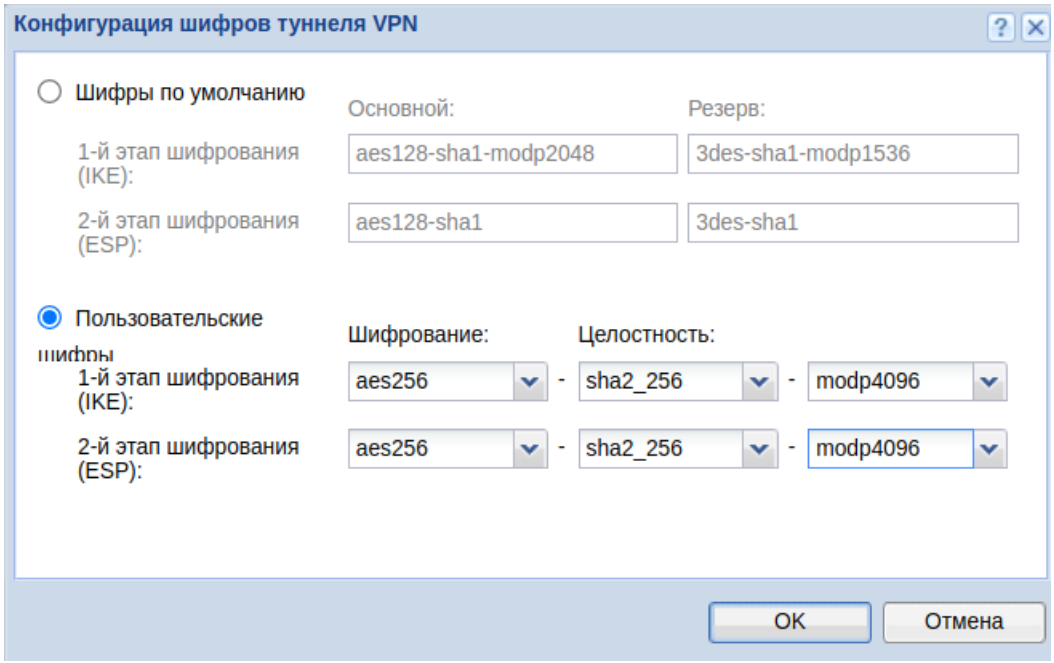
Подключение от Kerio Control к Ideco NGFW

Настройка исходящего подключения на Kerio Control:

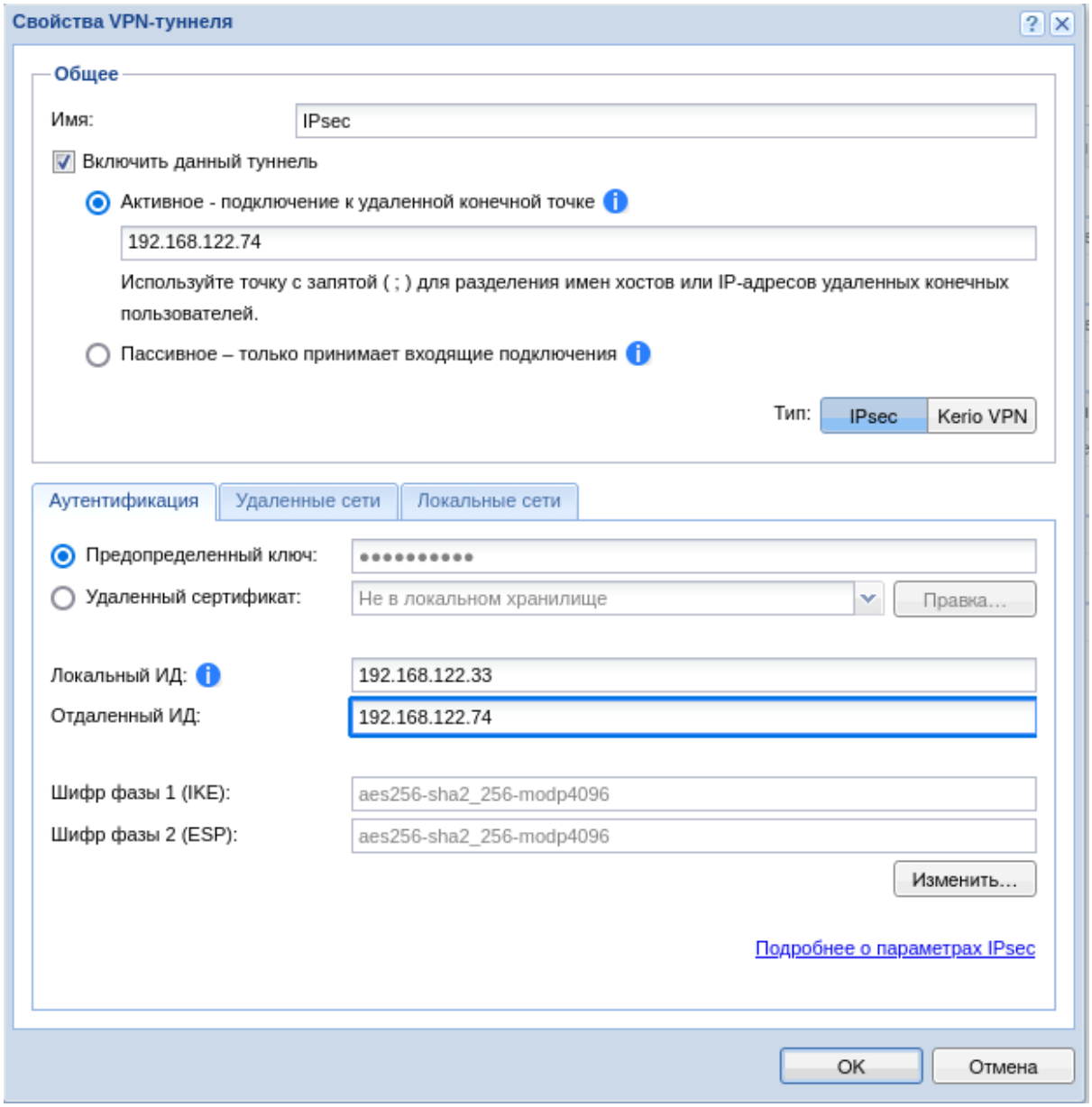
1. Перейдите в раздел **Интерфейсы** и нажмите **Добавить**. В раскрывшемся списке выберите **VPN-туннель. . .** .

2. Откроется окно создания подключения. В нем выберите:

- **Тип** - IPsec;
- **Имя** - произвольное;
- **Включить данный туннель**;
- Выберите тип **Активное** и в поле под ним пропишите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- **Предопределенный ключ** - введите PSK-ключ, который будет использоваться для подключения;
- **Локальный ИД** - укажите ключ, который будет задан в поле **Идентификатор NGFW** при настройке входящего подключения на Ideco NGFW, или IP-адрес внешнего интерфейса Kerio, который будет использоваться для подключения. **Предпочтительное значение - имя хоста Kerio**;
- **Отдаленный ИД** - укажите IP-адрес внешнего интерфейса Ideco NGFW, который будет использоваться для подключения;
- Под заданием шифров нажмите на **Изменить** и задайте шифры, как на скриншоте:



Пример итоговых настроек:



3. Перейдите в раздел **Удаленные сети**, нажмите на кнопку **Добавить** и введите сведения о локальной сети Ideco NGFW, которая будет видна из подсети Kerio Control.

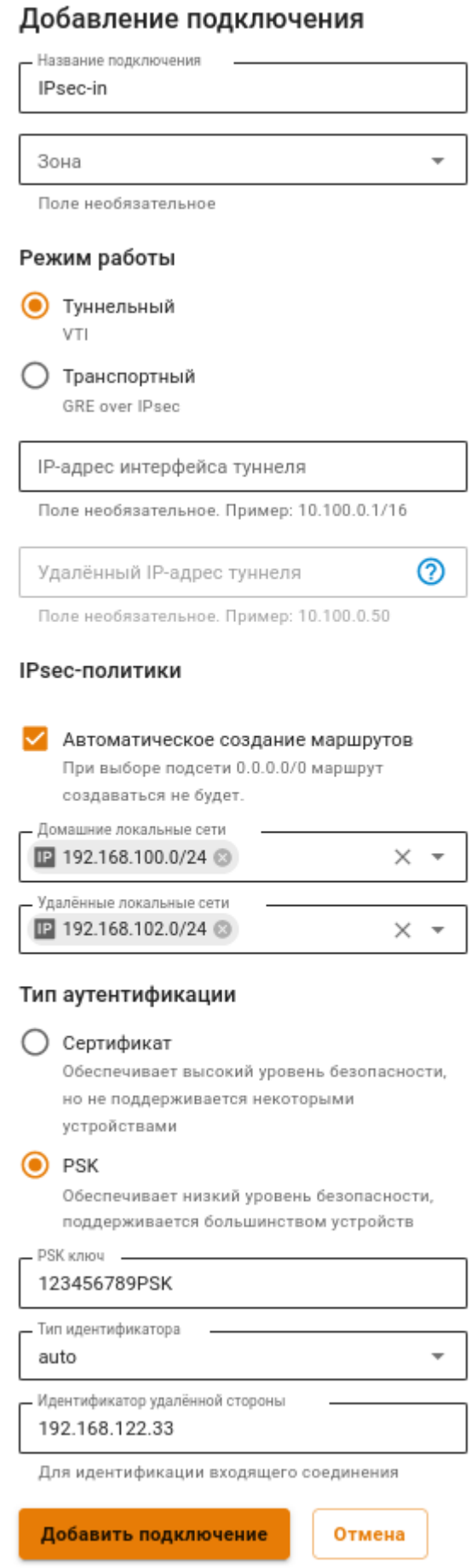
4. В разделе **Локальные сети** настройте сети, которые будут видны из подсети Ideco NGFW, вручную.

5. После добавление нового интерфейса нажмите на кнопку **Применить**. Подключение успешно установится, информация об этом отобразится в таблице.

Настройка входящего подключения на Ideco NGFW:

1. В веб-интерфейсе Ideco NGFW откройте вкладку **Сервисы -> IPsec -> Входящие подключения**.

2. Добавьте новое подключение и заполните поля:


Добавление подключения
Название подключения
IPsec-in
Зона
Поле необязательное
Режим работы
Туннельный
VTI
Транспортный
GRE over IPsec
IP-адрес интерфейса туннеля
Поле необязательное. Пример: 10.100.0.1/16
Удалённый IP-адрес туннеля
Поле необязательное. Пример: 10.100.0.50
IPsec-политики
Автоматическое создание маршрутов
При выборе подсети 0.0.0.0/0 маршрут создаваться не будет.
Домашние локальные сети
192.168.100.0/24
Удалённые локальные сети
192.168.102.0/24
Тип аутентификации
Сертификат
Обеспечивает высокий уровень безопасности, но не поддерживается некоторыми устройствами
PSK
Обеспечивает низкий уровень безопасности, поддерживается большинством устройств
PSK ключ
123456789PSK
Тип идентификатора
auto
Идентификатор удалённой стороны
192.168.122.33
Для идентификации входящего соединения
Добавить подключение
Отмена

- **Название подключения** - укажите произвольное имя для подключения. Значение не должно быть длиннее 42 символов;
- **Зона** - укажите зону для добавления IPSec подключения;
- **Режим работы** - выберите **Туннельный**;
- **IP-адрес интерфейса туннеля** - укажите IP-адрес интерфейса туннеля. Поле необязательное, заполняется при настройке BGP-соседства для динамической маршрутизации и для получения статистики обмена пакетами;
- **Удаленный IP-адрес туннеля** - укажите IP-адрес интерфейса туннеля удаленной стороны. Поле необязательное, заполняется для получения статистики обмена пакетами;
- **Домашние локальные сети** - выберите локальную сеть Ideco NGFW, которая будет видна из подсети Kerio Control;
- **Удаленные локальные сети** - укажите локальную сеть Kerio Control, которая будет видна из подсети Ideco NGFW;
- **Тип аутентификации** - выберите тип PSK;
- **PSK-ключ** - введите PSK-ключ, который был указан при создании подключения в Kerio;
- **Тип идентификатора** - выберите auto;
- **Идентификатор удаленной стороны** - укажите **Локальный ИД**, указанный при настройке исходящего подключения на Kerio.

Важно!
Для получения статистики о потере пакетов, средней задержке и джиттере заполните поля **IP-адрес интерфейса туннеля** и **Удаленный IP-адрес туннеля**. Они должны находиться в одной подсети.

3. Сохраните созданное подключение, затем активируйте подключение, нажав на иконку включения в столбце **Управление**.

Настройка завершена.

Подсказка: При возникновении проблем обратите внимание на настройки файрвола Kerio Control.

18.12.13 Подключение Keenetic по SSTP или IPsec

Основное

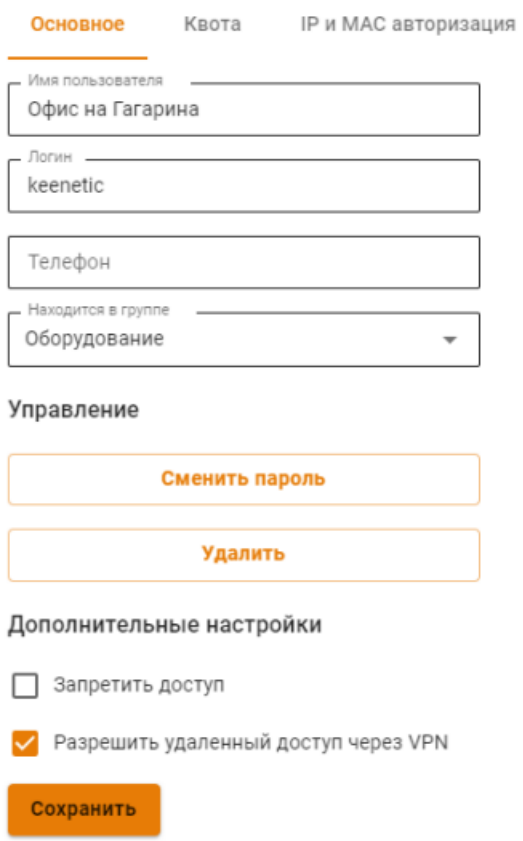
Если доступ из центрального офиса в сеть за Keenetic не нужен, то воспользуйтесь статьей *Подключение по SSTP Wi-Fi роутеров Keenetic* по client-to-site подключению.

Настройка Ideco NGFW:

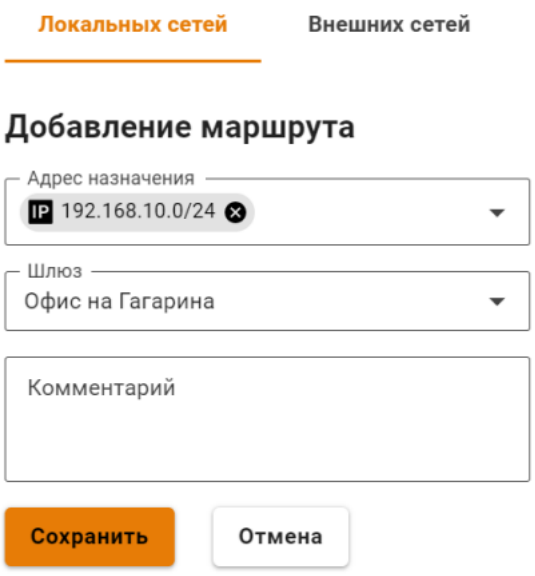
1. Включите и настройте порт и домен для SSTP в разделе **Пользователи -> VPN-подключения**.

2. В разделе **Пользователи -> Учетные записи** создайте специального пользователя для удаленного роутера. **Логин и пароль пользователя будут использоваться на роутере, сохраните или запишите их.**

3. Перейдите в раздел **VPN-подключения -> Доступ по VPN** и создайте правило доступа по VPN для этого пользователя:



4. Пропишите маршруты в удаленную сеть. Например, если сеть за роутером `192.168.10.0/24`, необходимо добавить 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.

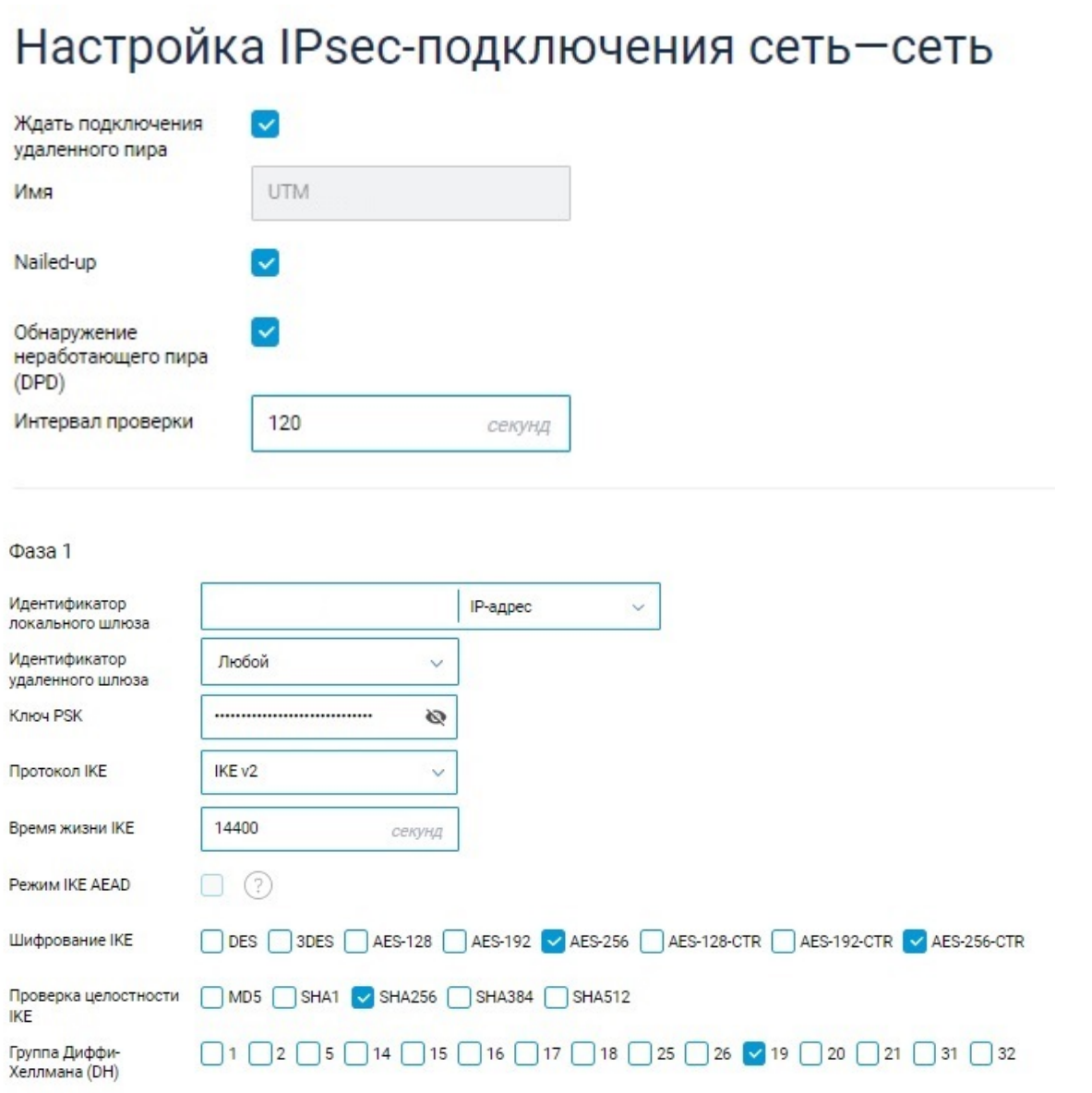
Доступ часто блокируется в Windows из-за настроек сетевых профилей.

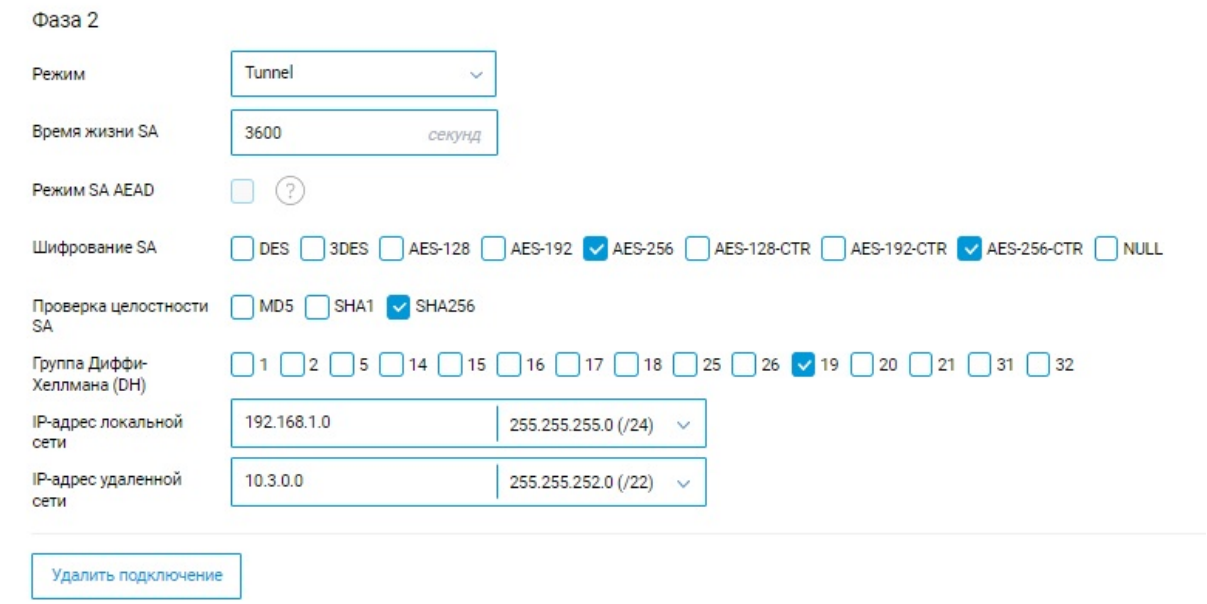
Разрешите доступ до «не локальных» сетей во всех профилях, выполнив команду в PowerShell (запущенного с повышением прав до администратора): `Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`

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:





18.13 Сертификаты

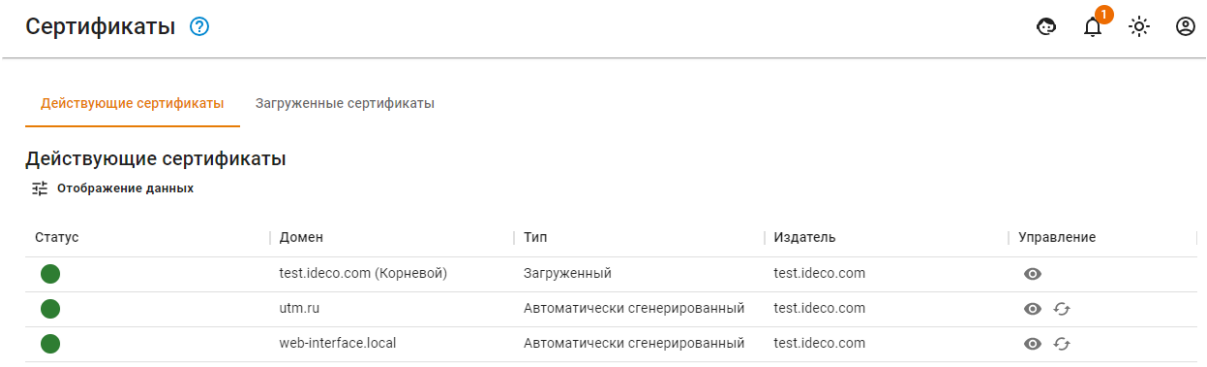
18.13.1 Общая информация

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

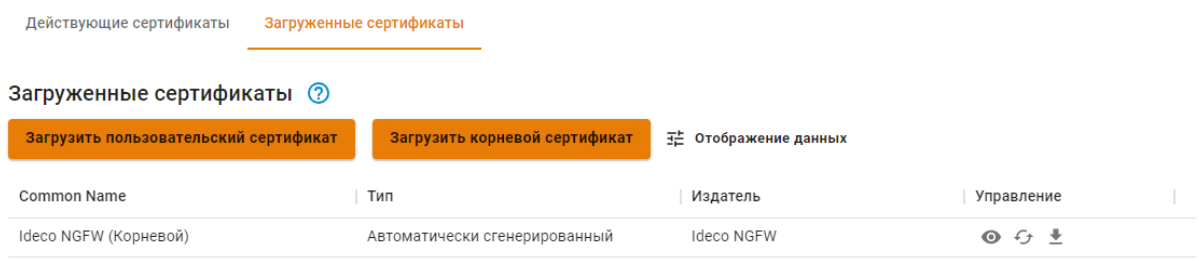


В таблице *Действующие сертификаты* отображаются:

- 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*.

18.13.2 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 отправлет запрос на выпуск цепочки в Let's Encrypt.

Условия автоматического выпуска сертификатов Let's Encrypt:

- Наличие доменного имени, зарегистрированного на статический белый IP-адрес, который назначен на внешний интерфейс Ideco NGFW;
- Открытый 80 TCP-порт на внешнем интерфейсе. После установки Ideco NGFW 80 TCP-порт по умолчанию открыт во внешнюю сеть.

Если при соблюдении перечисленных выше условий сертификат Let's Encrypt не выпускается автоматически, перейдите в раздел **Управление сервером -> Терминал** веб-интерфейса NGFW и воспользуйтесь командой:

```
systemctl restart ideco-cert-backend.service
```

Команда для просмотра логов:

```
journalctl -u ideco-cert-backend.service -f
```

3. При успешном выпуске цепочки сертификатов Let's Encrypt заменяет локальную цепочку.

4. Если выпуск цепочки сертификатов Let's Encrypt завершился неудачей, продолжает использовать локальную цепочку сертификатов.

Если требуется повторить попытку получения сертификата Let's Encrypt вместо самоподписанного, то нужно нажать на кнопку **Перевыпустить** в столбце **Управление**.

Подсказка: Сертификат Let's Encrypt **выпускается на 3 месяца** и будет **автоматически перевыпущен** по окончании срока действия.

С 17 версии Ideco NGFW автоматически сгенерированные NGFW пользовательские сертификаты выпускаются на **825 дней** и будут автоматически перевыпущены по окончании срока действия. В предыдущих версиях срок действия таких сертификатов составлял **10 лет**.

Процесс перевыпуска сертификата

Чтобы перевыпустить не корневую цепочку сертификатов, нажмите кнопку в столбце **Управление** в таблице **Действующие сертификаты**. NGFW 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/перевыпуске корневого сертификата в разделе *Сертификаты*, IPsec-подключения перестанут работать. Для восстановления соединения вам потребуется заменить сертификат в свойствах подключения. Для этого перейдите в раздел **Сервисы -> IPsec** и нажмите на с нужным подключением.

Внимание: Для работы *Ideco Client под MacOS* необходимо, чтобы срок действия сертификата на домен или IP-адрес NGFW, введенный в разделе **Пользователи -> Ideco Client** не превышал 825 дней.

Проверить, что срок действия загруженного пользовательского или сгенерированного NGFW сертификата не превышает **825 дней**, можно в разделе **Сервисы -> Сертификаты -> Действующие сертификаты**, нажав на .

Чтобы перевыпустить локальную цепочку сертификатов, выполните действия:

1. Перейдите в раздел **Управление сервером -> Терминал**.

2. Перейдите в директорию `/var/cache/ideco/cert-backend`, выполнив команду:

```
cd /var/cache/ideco/cert-backend
```

3. Выведите содержимое директории, выполнив команду `ls`.

4. Скопируйте название файла сертификата, который требуется перевыпустить. Названия файлов будут иметь вид:

`test.ideco.ru-self-sign_chain_833bcda78229059d2c2886548c75e9e3.pem`, где `test.ideco.ru` - доменное имя или IP-адрес, на который выпущен сертификат.

5. Удалите файл, выполнив команду:

```
rm test.ideco.ru-self-sign_chain_d1f73bf1fcc4d55ca31004ecb13d19b3.pem
```

6. Перейдите в раздел **Сервисы -> Сертификаты -> Действующие сертификаты** и перевыпустите сертификат на домен или IP-адрес NGFW, нажав на .

Проверить, перевыпустился ли сертификат на новый срок, можно , нажав на .

18.13.3 Загрузка SSL-сертификата на сервер

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

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. Как это сделать описано ниже в разделе **Конвертация сертификата из формата pkcs12 в формат pem с помощью openssl**;
- В составе сертификата **Издатель** и **Субъект** должны содержать поле **CN** (Common Name, общее имя). При загрузке собственной цепочки сертификатов **CN** (общее имя) последнего сертификата в цепочке должно соответствовать домену, для которого сертификат загружается;
- Цепочка сертификата должна быть валидной и соответствовать структуре:

```
Приватный ключ
Сертификат на домен (Common Name)
Сертификат из состава бандла vendor-сертификатов (промежуточный сертификат, если есть)
...
Основной (корневой) сертификат
```

Если сертификат самоподписанный, его структура может содержать всего 2 блока - **Приватный ключ** и **Сертификат на домен (Common Name)**. Если структура сертификата невалидна, переходите к разделу ниже **Подготовка SSL-сертификата для загрузки на NGFW**.

Предупреждение: Если вы хотите загрузить сертификат как корневой, удостоверьтесь, что он может выдавать дочерние сертификаты: *X509v3 Basic Constraints: CA: TRUE* (это можно проверить в открытом ключе сертификата).

Загрузка SSL-сертификата на NGFW

Если сертификат удовлетворяет всем перечисленным выше условиям, загрузите его на NGFW. Для этого:

1. Перейдите в раздел **Сервисы -> Сертификаты -> Загруженные сертификаты**.

2. Нажмите **Загрузить корневой сертификат**.

3. Выберите нужный сертификат.

Подсказка: Загруженный корневой сертификат автоматически переподпишет все пользовательские сертификаты на домены, которые ранее автоматически сгенерировал NGFW. Сертификаты Let's Encrypt и сертификаты, купленные у CA и Центров сертификации, переподписаны не будут.

Если в инфраструктуре компании есть свой корневой центр сертификации, выпустите сертификат с шаблоном **Subordinate Certification Authority** и загрузите его на Ideco NGFW в качестве корневого. Это позволит выстроить цепочку доверия для автоматически выданных сертификатов до корневого центра сертификации. Пользовательские компьютеры будут доверять сертификатам, выданным на стороне NGFW.

Подготовка SSL-сертификата для загрузки на NGFW:

При покупке доверенного SSL-сертификата на домен у Certificate Authority или Центра сертификации данные для его установки как правило высылаются электронным письмом в разрозненном виде. Для 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.

Если Центр сертификации выдал приватный ключ в зашифрованном виде, расшифруйте его с помощью passphrase (фразы-пароля).

3. В каждый из блоков (**BEGIN CERTIFICATE**) добавьте сертификат. В начало - сертификат на домен, следом - сертификаты из бандла vendor-сертификатов (если они есть), в самый конец - корневой сертификат. Файл должен получить такую структуру:

```
Приватный ключ
Сертификат на домен
Сертификат из состава бандла vendor-сертификатов (при наличии)
...
Основной (корневой) сертификат
```

4. Сохраните файл с расширением **.pem** и загрузите его на NGFW.

Подсказка: С общепринятым стандартом создания файла-цепочки сертификатов можно также ознакомиться здесь: https://www.digicert.com/ssl-support/pem-ssl-creation.htm.

Конвертация сертификата из формата pkcs12 в формат pem с помощью openssl:

Подсказка: Для конвертации сертификата с помощью openssl на Windows воспользуйтесь ссылкой для загрузки openssl на компьютер.

Для конвертации сертификата из формата **pkcs12** в формат **pem** выполните действия:

1. Откройте командную строку.

2. Введите команду `openssl pkcs12 -in certificate.pkcs12 -out certificate.pem` (сконвертирует сертификат в нужный формат), где:

- **certificate.pkcs12** - исходный сертификат который был получен у центра сертификации;
- **certificate.pem** - результат конвертации.

3. Откройте полученный файл и убедитесь, что он имеет структуру:

```
-----BEGIN CERTIFICATE-----
..............
..............
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
..............
..............
-----END PRIVATE KEY-----
```

Если в сертификате написано `--BEGIN ENCRYPTED PRIVATE KEY--`, расшифруйте его, введя в openssl команду
`openssl rsa -in certificate.pem -out certificate_decoded.pem`, где:

- **certificate.pem** - файл который был получен после конвертации;
- **certificate_decode.pem** - результат расшифровки.

18.13.4 Создание самоподписанного сертификата с помощью PowerShell

Основное

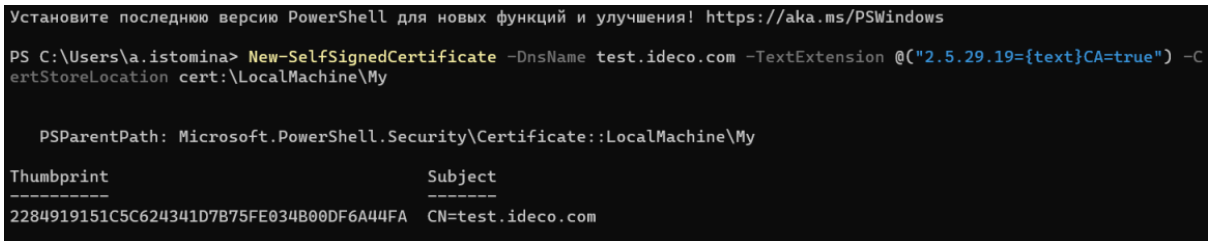
Чтобы создать корневой (самоподписанный) сертификат с помощью PowerShell, выполните следующие действия:

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
```

Где `test.ideco.com` - домен.



Для просмотра сгенерированного сертификата выполните команду `certlm.msc`.

3. Сформируйте пароль для сертификата:

```
$CertPassword = ConvertTo-SecureString -String ‘‘12345’’ -Force -AsPlainText
```

Где 12345 - пароль.

4. Экспортируйте сертификат выполнив команду:

```
Export-PfxCertificate -Cert cert:\LocalMachine\My\
↪2284919151C5C624341D7B75FE034B00DF6A44FA -FilePath C:\Users\pende\ssl\test.ideco.
↪pfx -Password $CertPassword
```

- `2284919151C5C624341D7B75FE034B00DF6A44FA` - идентификатор сертификата полученный на шаге 2;
- `C:\Users\pende\ssl\test.ideco.pfx` - путь до папки, в которую требуется сохранить сертификат (проверьте его корректность во избежание ошибок).

5. Конвертируйте сертификат в расширение .pem (пример конвертора).

Подсказка: Для загрузки сертификата на сервер воспользуйтесь статьей *Загрузка SSL-сертификата на сервер*

18.13.5 Создание сертификата с помощью openssl

Основное

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

Подсказка: Используйте эту статью, если вы пользуетесь операционной системой с ядром Linux. При использовании операционной системы Windows воспользуйтесь статьей *Создание самоподписанного сертификата с помощью PowerShell*.

Для создания самоподписанного сертификата выполните действия:

1. Создайте закрытый ключ для сертификата:

```
openssl genrsa -out ca.key 2048
```

Где `ca.key` - файл с приватным ключом.

2. Создайте запрос на подпись сертификата:

```
openssl req -key ca.key -new -out cert.csr
```

- `ca.key` - файл с приватным ключом;
- `cert.csr` - файл с запросом на подпись.

3. Создайте файл с именем test.txt:

```
cat >> ./test.txt << EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:TRUE
keyUsage = digitalSignature, keyCertSign, cRLSign
subjectAltName=DNS:test.com
EOF
```

- `test.txt` - файл с расширениями сертификата;
- `test.com` - доменное имя сервера.

4. Сгенерируйте самоподписанный сертификат:

```
openssl x509 -extfile ./test.txt -signkey ca.key -in cert.csr -req -days 365 -out ca.
↪crt
```

- `test.txt` - файл, созданный в 3 пункте;
- `ca.key` - файл с приватным ключом;
- `cert.csr` - файл с запросом на подпись сертификата;
- `ca.crt` - файл со сгенерированным сертификатом.

5. Добавьте к сертификату приватный ключ:

```
cat ca.key ca.crt > server.pem
```

Где `server.pem` - самоподписанный сертификат для загрузки на сервер.

Подсказка: Для загрузки сертификата на сервер воспользуйтесь статьей *Загрузка SSL-сертификата на сервер*

---

19. Отчеты и журналы

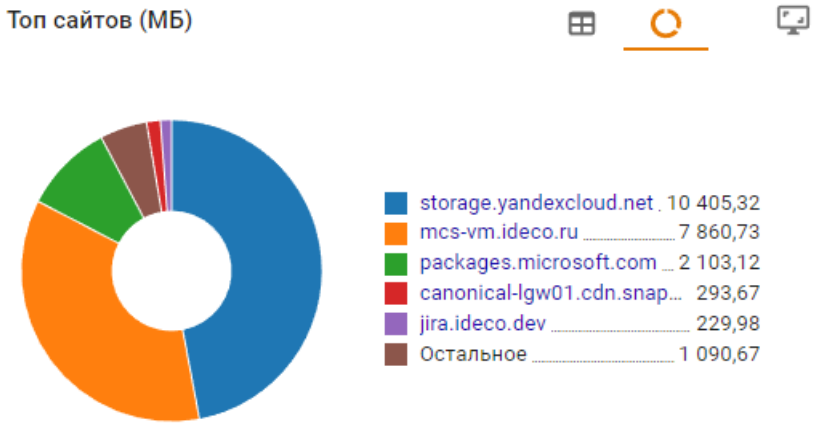
19.1 Трафик

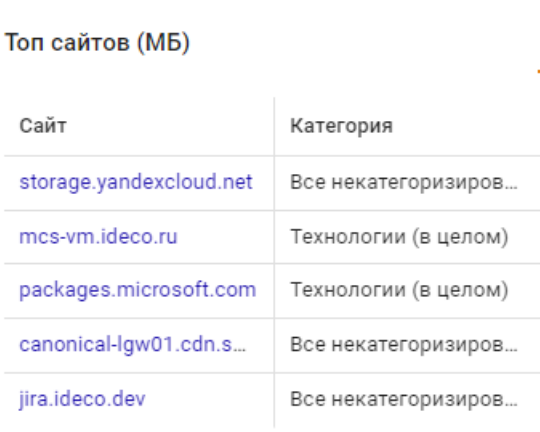
При переводе ползунка **Трафик** в левом верхнем углу в положение **Включен** раздел начинает собирать статистику из *Контент-фильтра* (категории и сайты) и *Контроля приложений* (протоколы) и отображает в виде виджетов.

19.1.1 Способ отображения информации:

Круговая диаграмма ( ) и таблица ( )

Содержит топ-6 объектов. Каждый объект кликабелен и ведет на страницу с виджетами, в которых статистика фильтруется по этому объекту.



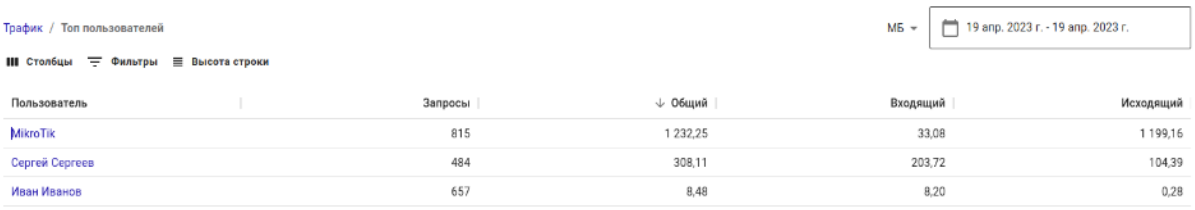


Единицу измерения можно изменить в левом верхнем углу:

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** ( ).

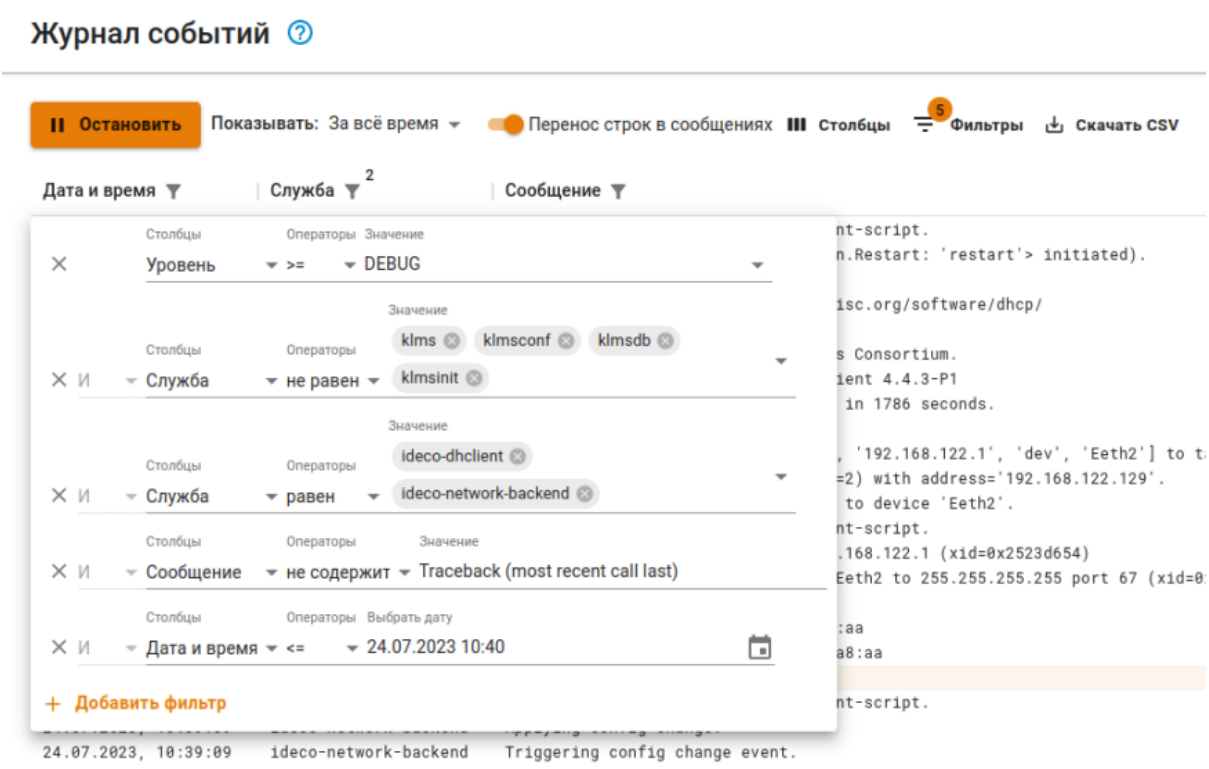
Подробнее о создании собственных шаблонов со статистикой - в статье *Конструктор отчетов*.

19.2 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;
- **Бекапы** - 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.

19.2.1 Защита от брутфорс-атак

Подсказка: Защита от брутфорс-атак (brute force - атака полным перебором) работает только для NGFW.

После 6 неудачных попыток ввода пароля в течение 15 минут IP-адрес подбирающего блокируется на 45 минут.

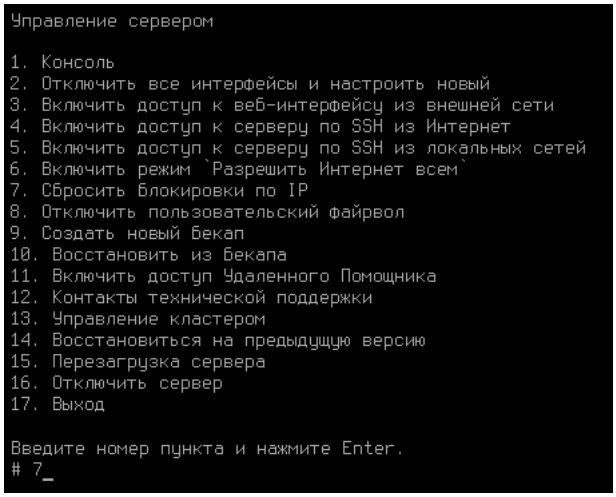
Логи службы `fail2ban` можно увидеть:

- В веб-интерфейсе в разделе **Отчеты и журналы -> 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**:



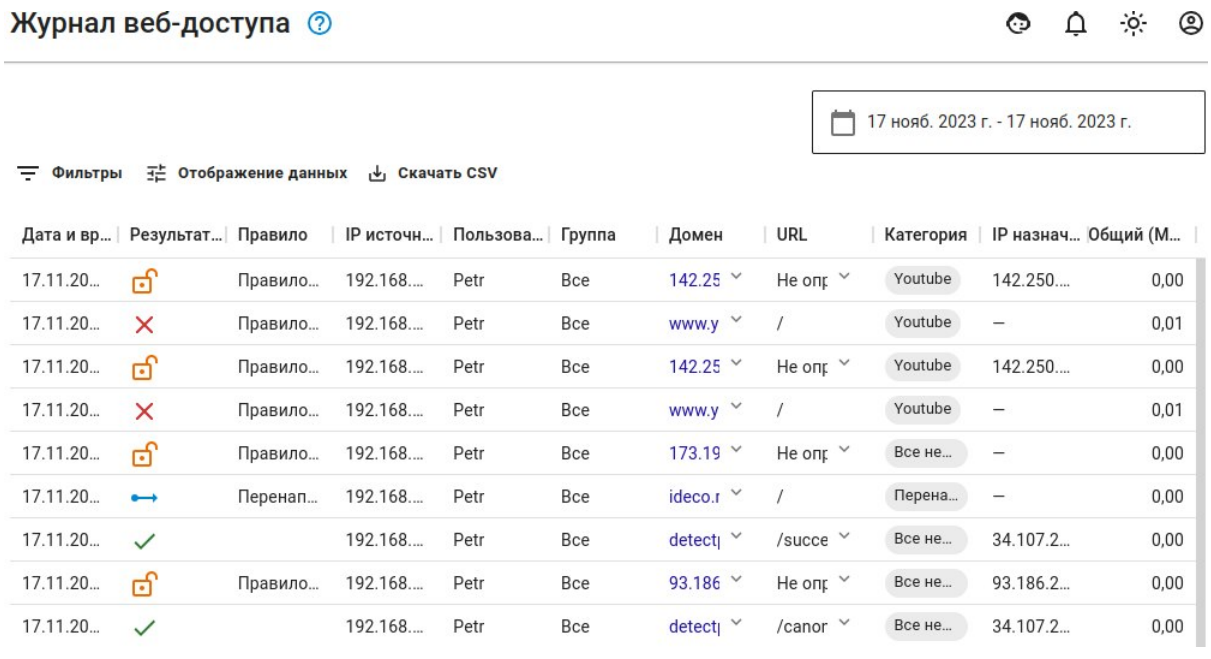
19.3 Журнал веб-доступа

19.3.1 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 кнопкой **Фильтры**, указав в форме наименование правила и оператор.

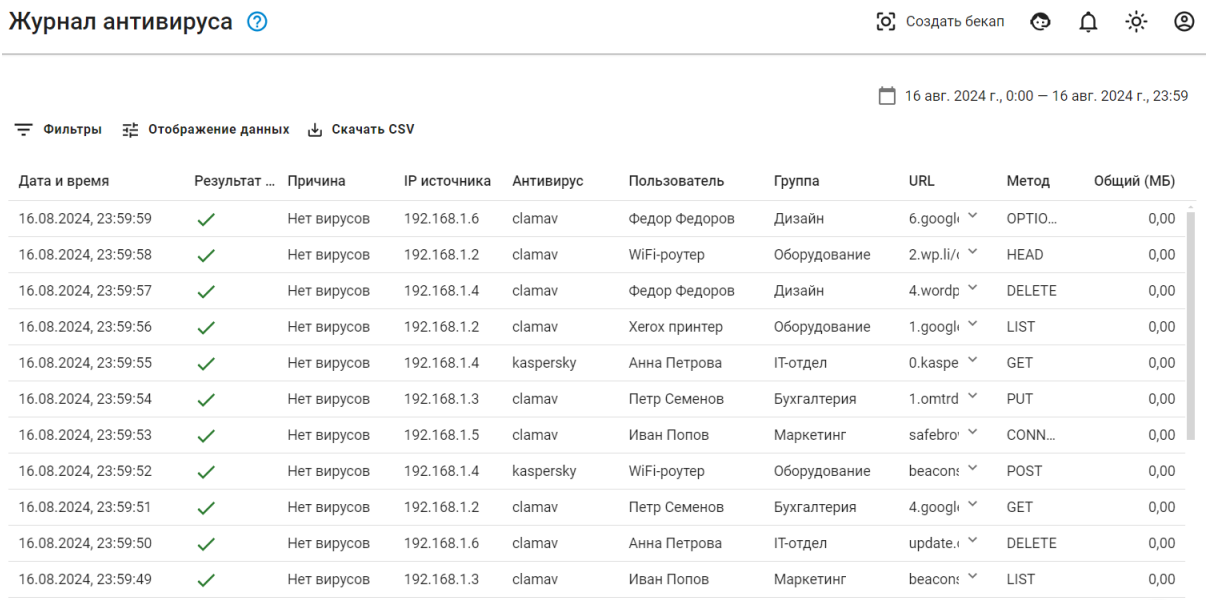
19.4 Журнал антивируса

19.4.1 Основное

Внимание: Для работы антивируса настройте расшифровку трафика на Ideco NGFW и включите антивирус, активировав опцию **Антивирусы веб-трафика** в разделе **Правила трафика -> Антивирусы веб-трафика**.

При отключенной опции **Антивирусы веб-трафика** данные в **Журнал антивируса** попадать не будут.

Раздел позволяет посмотреть логи работы антивируса. При загрузке файла в сеть или скачивании на компьютер Ideco NGFW проверяет содержимое файла антивирусом.



Дата и время	Результат ...	Причина	IP источника	Антивирус	Пользователь	Группа	URL	Метод	Общий (МБ)
16.08.2024, 23:59:59	✓	Нет вирусов	192.168.1.6	clamav	Федор Федоров	Дизайн	6.googl	OPTIO...	0,00
16.08.2024, 23:59:58	✓	Нет вирусов	192.168.1.2	clamav	WiFi-роутер	Оборудование	2.wp.li/	HEAD	0,00
16.08.2024, 23:59:57	✓	Нет вирусов	192.168.1.4	clamav	Федор Федоров	Дизайн	4.wordp	DELETE	0,00
16.08.2024, 23:59:56	✓	Нет вирусов	192.168.1.2	clamav	Xerox принтер	Оборудование	1.googl	LIST	0,00
16.08.2024, 23:59:55	✓	Нет вирусов	192.168.1.4	kaspersky	Анна Петрова	IT-отдел	0.kaspe	GET	0,00
16.08.2024, 23:59:54	✓	Нет вирусов	192.168.1.3	clamav	Петр Семенов	Бухгалтерия	1.omtrd	PUT	0,00
16.08.2024, 23:59:53	✓	Нет вирусов	192.168.1.5	clamav	Иван Попов	Маркетинг	safebro	CONN...	0,00
16.08.2024, 23:59:52	✓	Нет вирусов	192.168.1.4	kaspersky	WiFi-роутер	Оборудование	beacon	POST	0,00
16.08.2024, 23:59:51	✓	Нет вирусов	192.168.1.2	clamav	Петр Семенов	Бухгалтерия	4.googl	GET	0,00
16.08.2024, 23:59:50	✓	Нет вирусов	192.168.1.6	clamav	Анна Петрова	IT-отдел	update.	DELETE	0,00
16.08.2024, 23:59:49	✓	Нет вирусов	192.168.1.3	clamav	Иван Попов	Маркетинг	beacon	LIST	0,00

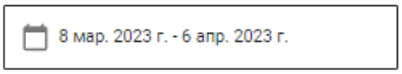
Подсказка: Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

19.5 События безопасности

Подсказка: Все графики формируются в часовом поясе сервера.

В разделе **События безопасности** представлены события модулей WAF и IPS/IDS, а также графики событий IPS/IDS.

19.5.1 Выбор периода

Все отображаемые данные можно фильтровать по дате и времени. Например, выбрать определенный временной период (по кнопке 

) или воспользоваться одним из предустановленных фильтров:

Доступные варианты: сегодня, вчера, текущая неделя, прошлая неделя, текущий месяц, прошлый месяц.

Если не выбран ни один фильтр по дате и времени, то по умолчанию устанавливается интервал **Сегодня** в часовом поясе сервера.

19.5.2 Графики IDS/IPS

В этом разделе представлены графики, содержащие краткую информацию, собранную разделом **Предотвращение вторжений**. Подробные сведения обо всех срабатываниях правил **Предотвращение вторжений** можно найти на вкладке **Журнал IDS/IPS** в виде таблицы.

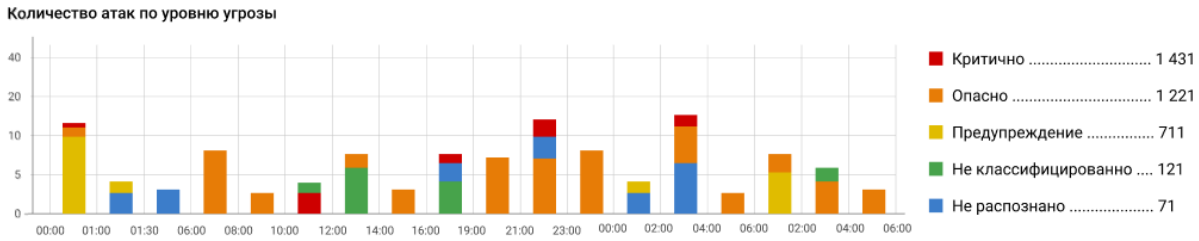
График Количество атак по уровню угрозы

Информация представлена в виде графика с пятью значениями угрозы безопасности:

- **Критично** - уровень угрозы 1;
- **Важно** - уровень угрозы 2;
- **Предупреждение** - уровень угрозы 3;
- **Не классифицировано** - уровень угрозы 4;
- **Не распознано** - уровень угрозы 255.

Если нажать на уровень угрозы в правом списке, все графики будут отфильтрованы в соответствии с этим уровнем. Чтобы отменить фильтрацию, нажмите еще раз на выбранный уровень.

Пример графика *Количество атак по уровню угрозы*:



Описание дополнительных графиков

Топ атакованных адресов:

В топ атакованных попадают как внешние, так и внутренние адреса. Один из примеров, когда атакованный адрес является внешним, - работа трояна изнутри защищаемой сети.

Топ заблокированных типов атак:

График подсчитывает статистику типов атак (например, типы атак *Черный список IP-адресов* или *Попытки получения привилегий администратора*) по количеству срабатываний с этим типом атаки.

Топ внешних узлов по количеству блокировок:

График содержит информацию о внешних адресах и количестве блокировок по ним.

Топ атакующих стран:

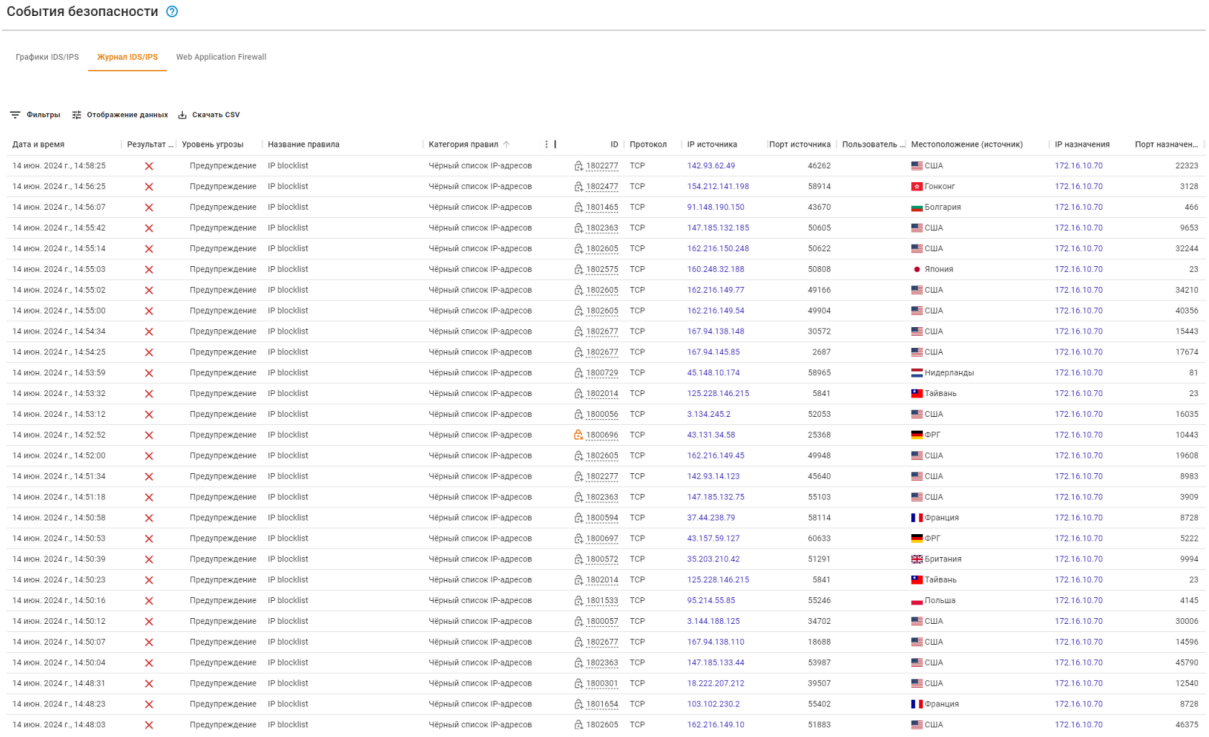
Топ атакующих стран строится по IP-адресам, полученным при срабатывании правил в разделе **Предотвращение вторжений**. Если IP-адрес не геокодируется в наименование страны, такой адрес не отображается в виджете.
По этой причине локальные IP-адреса не отображаются в виджете.

Топ подозрительных локальных узлов:

В топ попадают как авторизованные, так и не авторизованные пользователи, запросы которых блокировались.

19.5.3 Журнал IDS/IPS

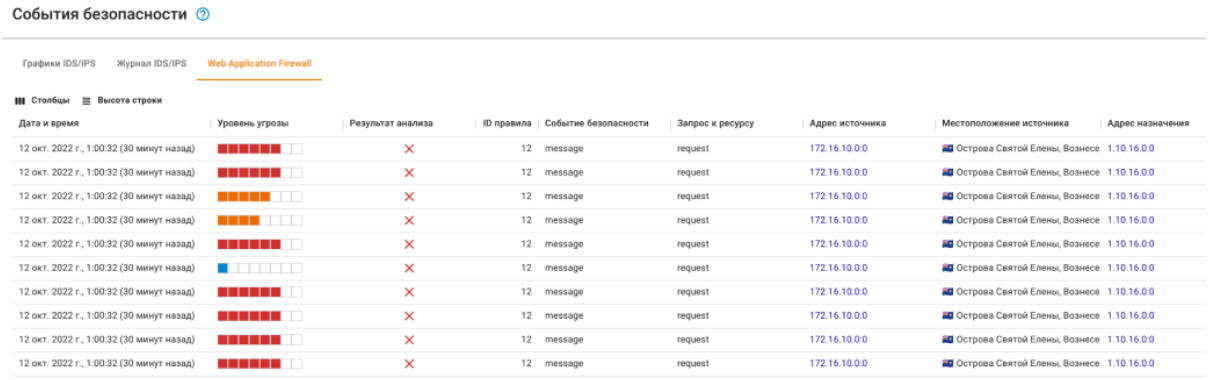
В журнале можно найти ID правил, которые срабатывали, и при необходимости создать исключение, нажав на иконку . Также добавить исключение можно в разделе *Предотвращение вторжений*. IP-адреса в столбцах **Источник** и **Назначение** кликабельны и при нажатии ведут на сервис Whois для получения информации о регистрации домена.



Дата и время	Результат ...	Уровень угрозы	Название правила	Категория правил	ID	Протокол	IP источника	Порт источника	Пользователь ...	Местоположение (источник)	IP назначения	Порт назначен...
14 июн. 2024 г., 14:58:25	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802277	TCP	142.93.62.49	46262		США	172.16.10.70	22323
14 июн. 2024 г., 14:56:25	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802477	TCP	154.212.141.198	58914		Гонконг	172.16.10.70	3128
14 июн. 2024 г., 14:56:07	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801465	TCP	91.148.190.150	43670		Болгария	172.16.10.70	466
14 июн. 2024 г., 14:55:42	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802363	TCP	147.185.132.185	50605		США	172.16.10.70	9653
14 июн. 2024 г., 14:55:14	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802605	TCP	162.216.150.248	50622		США	172.16.10.70	32244
14 июн. 2024 г., 14:55:03	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802575	TCP	160.248.32.188	50808		Япония	172.16.10.70	23
14 июн. 2024 г., 14:55:02	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802605	TCP	162.216.149.77	49166		США	172.16.10.70	34210
14 июн. 2024 г., 14:55:00	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802605	TCP	162.216.149.54	49904		США	172.16.10.70	40356
14 июн. 2024 г., 14:54:34	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802677	TCP	167.94.138.148	30572		США	172.16.10.70	15443
14 июн. 2024 г., 14:54:25	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802677	TCP	167.94.145.85	2687		США	172.16.10.70	17674
14 июн. 2024 г., 14:53:59	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800729	TCP	45.148.10.174	58965		Нидерланды	172.16.10.70	81
14 июн. 2024 г., 14:53:32	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802014	TCP	125.228.146.215	5841		Тайвань	172.16.10.70	23
14 июн. 2024 г., 14:53:12	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800056	TCP	3.134.245.2	52053		США	172.16.10.70	16035
14 июн. 2024 г., 14:52:52	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800696	TCP	43.131.34.58	25368		ФРГ	172.16.10.70	10443
14 июн. 2024 г., 14:52:00	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802605	TCP	162.216.149.45	49948		США	172.16.10.70	19608
14 июн. 2024 г., 14:51:34	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802277	TCP	142.93.14.123	45640		США	172.16.10.70	8983
14 июн. 2024 г., 14:51:18	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802363	TCP	147.185.132.75	55103		США	172.16.10.70	3909
14 июн. 2024 г., 14:50:58	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800594	TCP	37.44.238.79	58114		Франция	172.16.10.70	8728
14 июн. 2024 г., 14:50:53	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800697	TCP	43.157.59.127	60633		ФРГ	172.16.10.70	5222
14 июн. 2024 г., 14:50:39	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800572	TCP	35.203.210.42	51291		Британия	172.16.10.70	9994
14 июн. 2024 г., 14:50:23	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802014	TCP	125.228.146.215	5841		Тайвань	172.16.10.70	23
14 июн. 2024 г., 14:50:16	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801533	TCP	95.214.55.85	55246		Польша	172.16.10.70	4145
14 июн. 2024 г., 14:50:12	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800057	TCP	3.144.188.125	34702		США	172.16.10.70	30006
14 июн. 2024 г., 14:50:07	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802677	TCP	167.94.138.110	18688		США	172.16.10.70	14596
14 июн. 2024 г., 14:50:04	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802363	TCP	147.185.133.44	53987		США	172.16.10.70	45790
14 июн. 2024 г., 14:48:31	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1800301	TCP	18.222.207.212	39507		США	172.16.10.70	12540
14 июн. 2024 г., 14:48:23	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1801654	TCP	103.102.230.2	55402		Франция	172.16.10.70	8728
14 июн. 2024 г., 14:48:03	✕	Предупреждение	IP blocklist	Чёрный список IP-адресов	1802605	TCP	162.216.149.10	51883		США	172.16.10.70	46375

19.5.4 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.

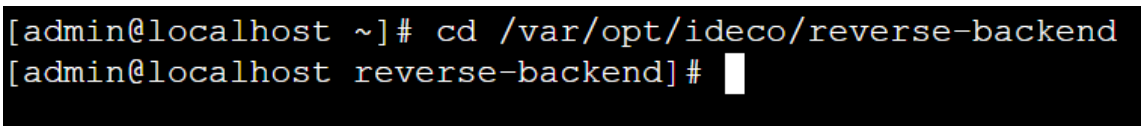
Добавление правила Web Application Firewall в исключения:

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`:

- Если директория есть, она отобразится в терминале:

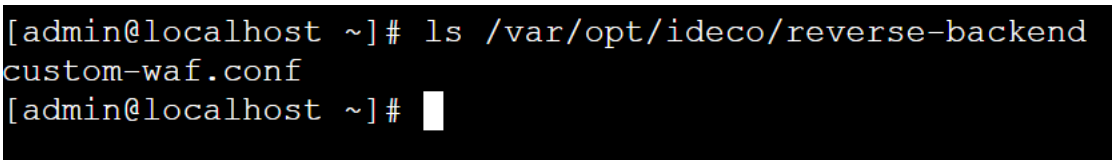


- Если такой директории нет, создайте ее, выполнив команды:

```
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:

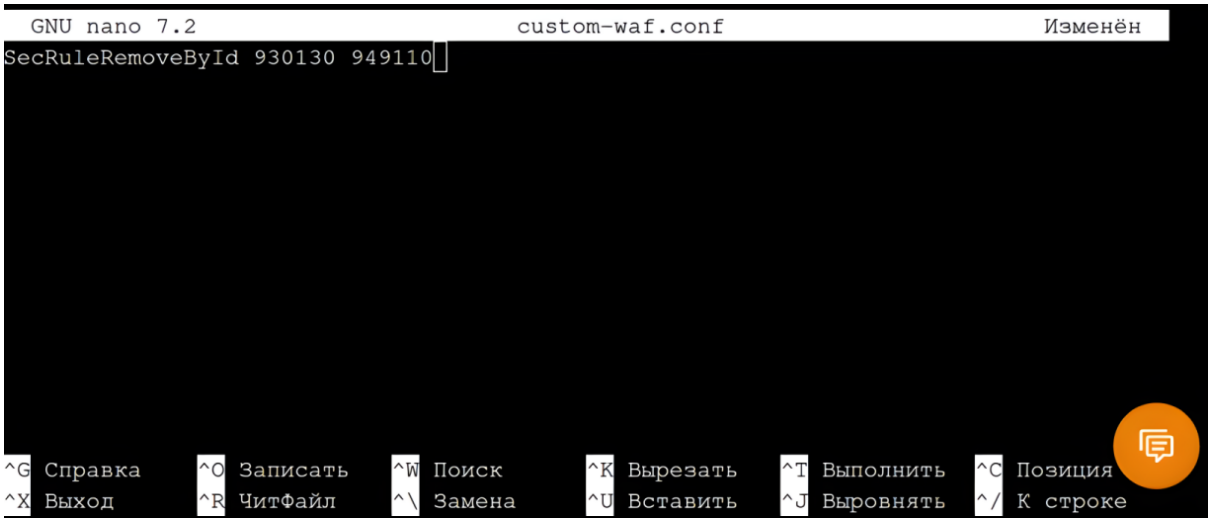


- Если файла нет, создайте его командами:

```
touch /var/opt/ideco/reverse-backend/custom-waf.conf
chown ideco-reverse-backend:ideco-reverse-backend /var/opt/ideco/reverse-backend/
↪custom-waf.conf
```

4. Откройте файл `custom-waf.conf` в режиме редактирования, введя команду `nano custom-waf.conf`.

5. В открывшемся файле введите `SecRuleRemoveById 930130 949110`, где 930130 и 949110 - ID сработавших правил WAF:

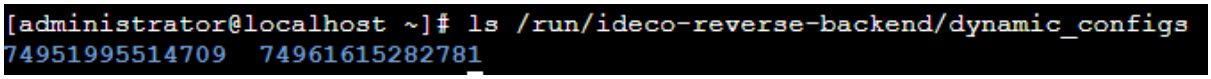


6. Сохраните файл, нажав комбинацию клавиш **Ctrl + X**, и подтвердите нажав **Y**. После этого откроется окно, в котором можно изменить имя файла, нажмите **Enter**.

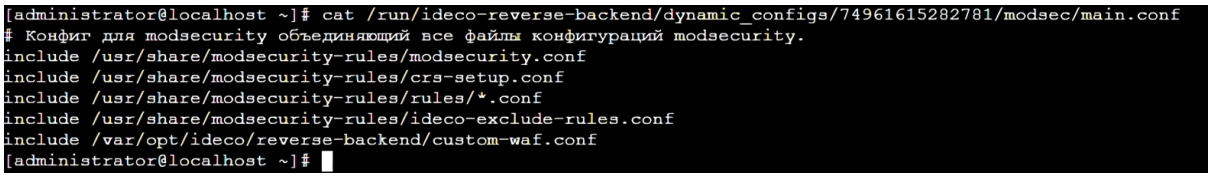
7. Введите команду `sync --file-system /var/opt/ideco/reverse-backend/custom-waf.conf`, чтобы данные записались на диск.

8. Перезапустите службу, введя в терминале команду `systemctl restart ideco-reverse-backend.service`.

9. Введите команду `ls /run/ideco-reverse-backend/dynamic_configs`.
Откроется набор директорий, скопирйуте название директории с максимальным числом:



10. Введите команду `cat /run/ideco-reverse-backend/dynamic_configs/74961615282781/modsec/main.conf`, где 74961615282781 название директории, скопированное в пункте 9:

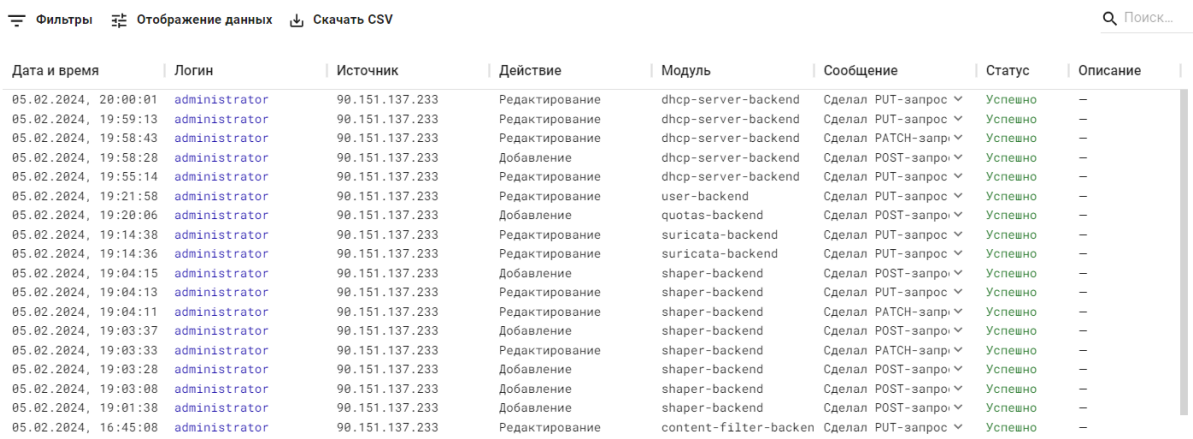


Внесенные в файл `custom-waf.conf` исключения из правил WAF сохранятся при обновлении сервера Ideco NGFW. Создавать директорию и файл необходимо только один раз, новые исключения следует просто в него добавлять.

19.6 Действия администраторов

19.6.1 Основное

Ideco NGFW логирует действия администраторов, которые вносят изменения в конфигурацию NGFW из веб-интерфейса, локального интерфейса и терминала.



Для фильтрации логов воспользуйтесь кнопкой **Фильтры**.

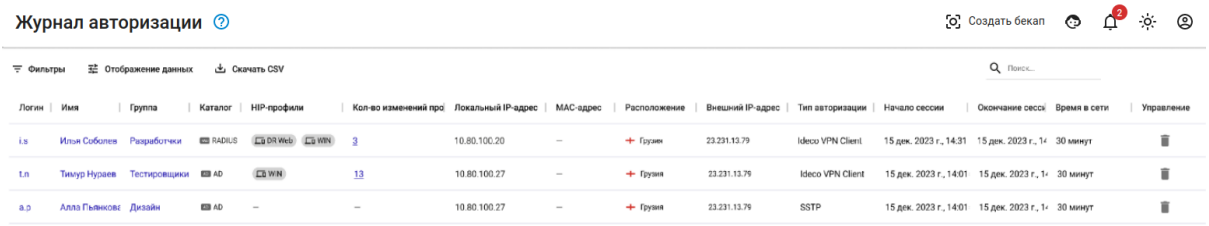
При работе Ideco NGFW в режиме *кластера* логи действия администраторов не передаются резервной ноде.

Подсказка: При бездействии в течение 15 минут администратор будет автоматически разавторизован.

19.7 Журнал авторизации

19.7.1 Основное

Подсказка: Время хранения данных в **Журнале авторизации** составляет 180 дней.

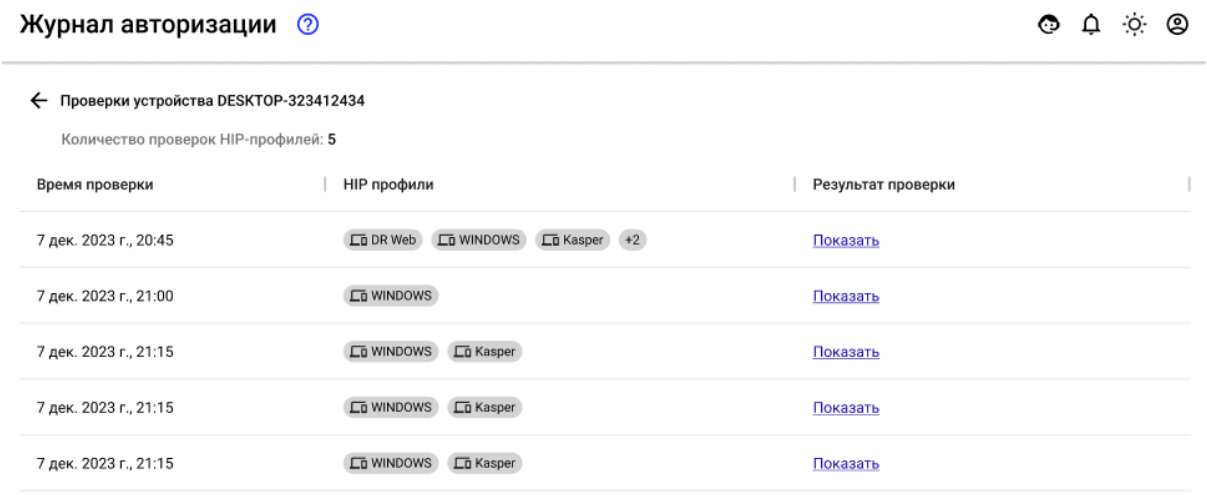


Для поиска авторизованных пользователей нажмите на **Фильтры**, укажите в поле **Столбец** требуемый параметр поиска и в последнем поле - его значение.

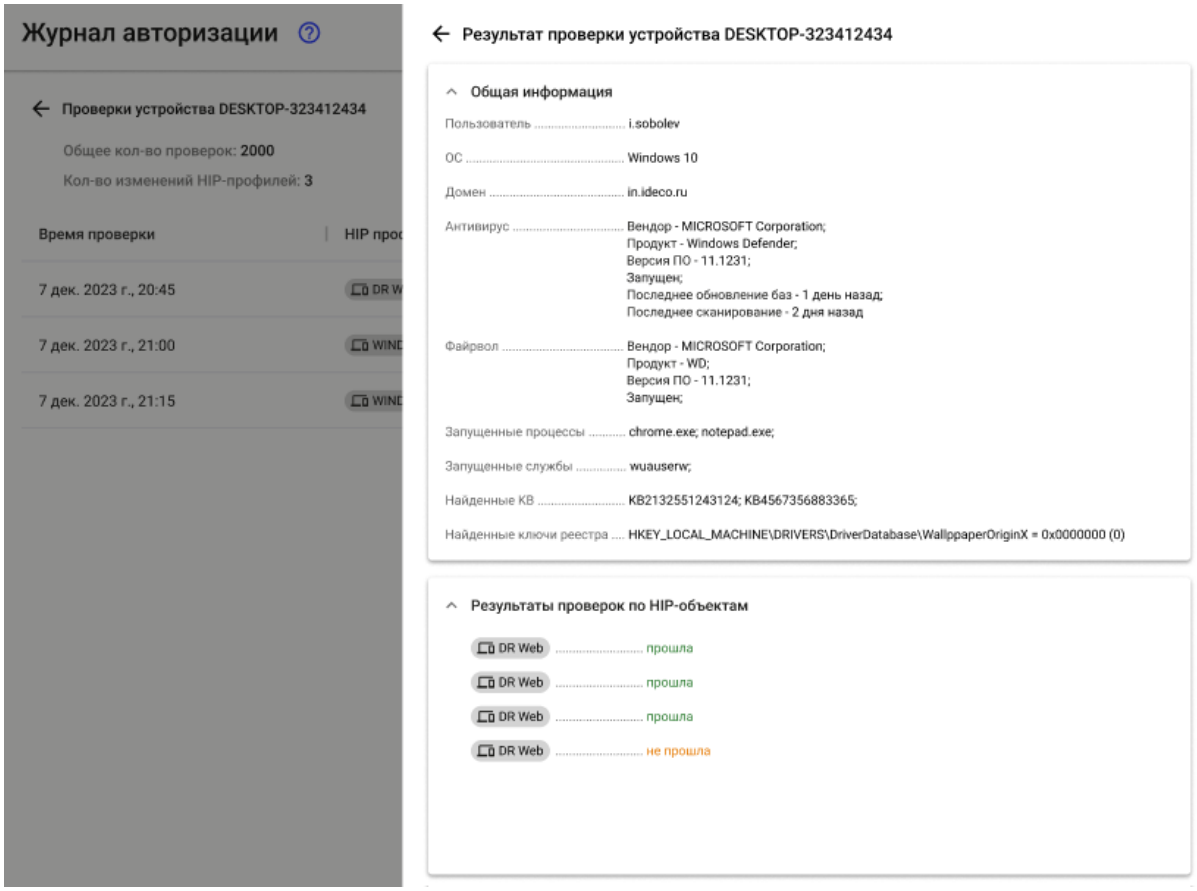
В столбце **Кол-во изменений профилей** указано количество изменений HIP-профилей, зафиксированных в результате проверок устройств, подключенных через Ideco Client. Изменения фиксируются при редактировании HIP-профиля в веб-интерфейсе или изменении соответствия устройств настроенным профилям.

Для просмотра результатов проверок устройств, подключенных через Ideco Client, выполните действия:

1. Кликните на число в столбце **Кол-во изменений профилей**. Откроется список проверок:



2. Кликните **Показать** в столбце **Результат**, чтобы увидеть общую информацию и результат проверки по *HIP-объектам*:



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.

19.8 Конструктор отчетов

NGFW предоставляет возможность создать шаблоны отчетов и настроить их рассылку в формате .pdf на электронную почту.

19.8.1 Мои шаблоны

На этой вкладке создаются шаблоны со статистикой, которую можно просмотреть в браузере, сохранить в формате .pdf или отправить на электронную почту.

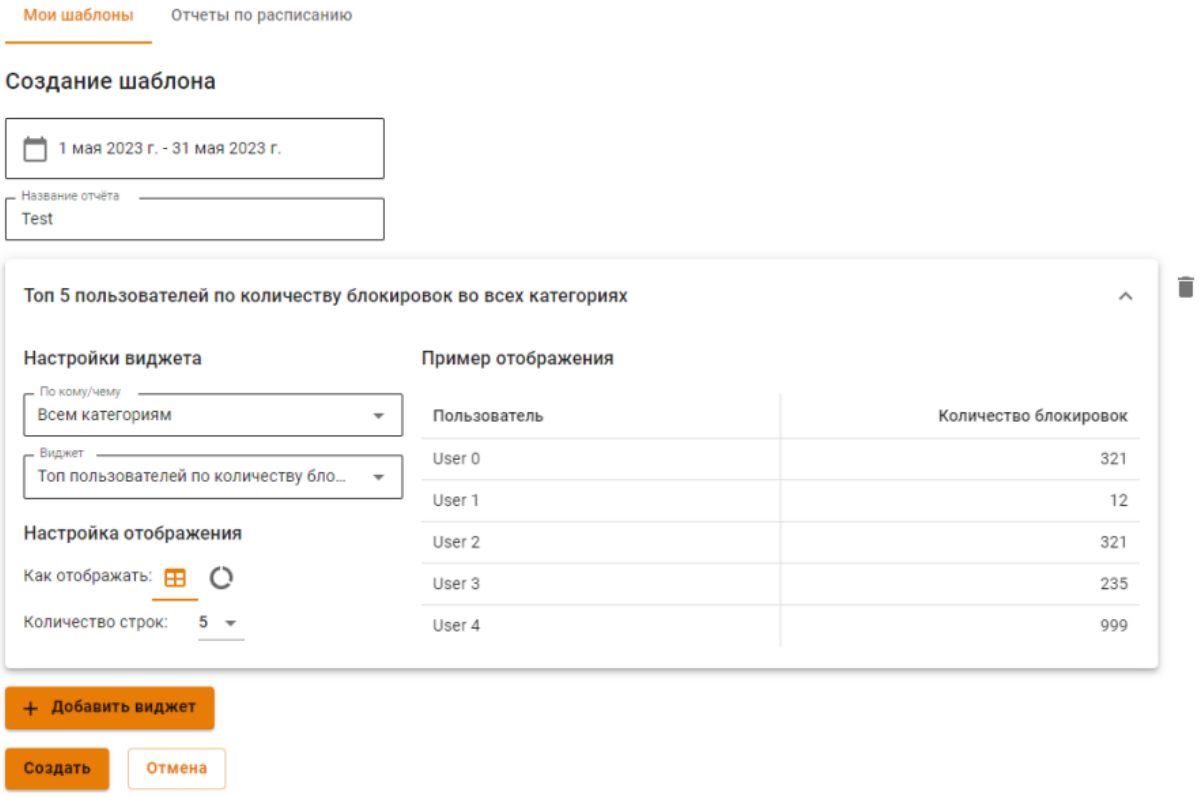
При нажатии на кнопку **Добавить** откроется меню настройки шаблона.

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**.



Подсказка: Будьте внимательны при задании временного промежутка для шаблона отчетов. Ideco NGFW хранит данные в течение определенного времени (TTL), по прошествии которого они безвозвратно удаляются и не могут быть включены в отчеты:

Сроки хранения данных по разделам:

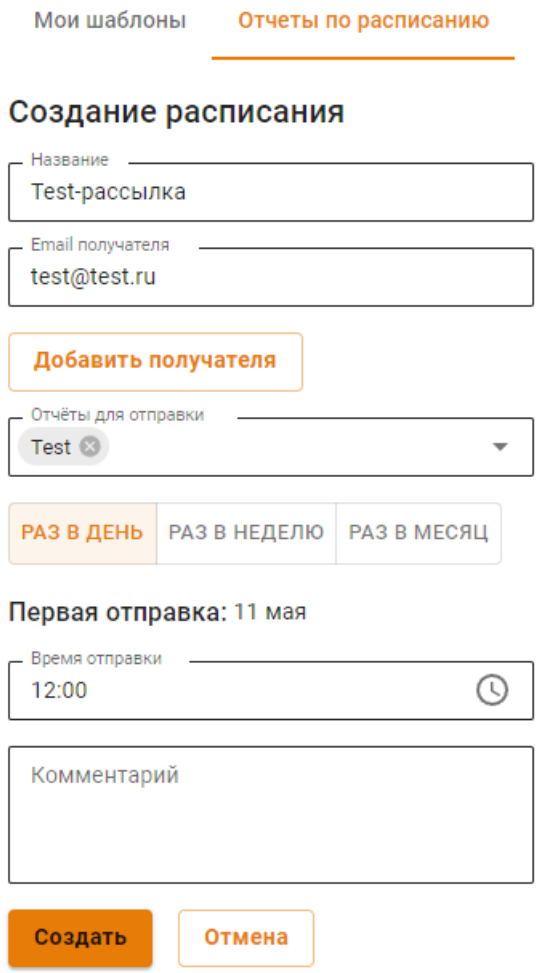
- *Журнал событий* (кроме логов служб `strongswan`, `squid`, `ideco-app-control`, `fail2ban`) - 90 дней;

- Логи *служб* `strongswan`, `squid`, `ideco-app-control`, `fail2ban` (Системный журнал) - 14 дней;
- Данные веб-трафика (Журнал антивируса, Журнал веб-доступа, а также посещенные сайты) - 1 месяц;
- События безопасности (Журнал IDS/IPS и Web application firewall) - 3 месяца;
- Действия администраторов - 1 год;
- Журнал авторизации - 180 дней.

19.8.2 Отчеты по расписанию

На этой вкладке предоставлена возможность создания/редактирования настроек для отправки рассылки на электронную почту, доступна фильтрация по всем столбцам с помощью кнопки **Фильтры**.

Для создания настройки нажмите **Отчеты по расписанию -> Добавить** в левом верхнем углу. В одной настройке можно указать несколько e-mail-получателей (кнопка **Добавить получателя**) и несколько отчетов (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. Перейдите 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** на вкладке **Мои шаблоны**.

2. Выберите временной период, за который следует сформировать отчет, из предложенных фильтров или укажите даты нажав **Выберите дату**.

3. Укажите название отчета (строка *Название отчета*).

4. Кликните по кнопке **Добавить виджет**.

5. Заполните строки:

- **По кому/чему** - выберите **Всем пользователям**;
- **Виджет** - выберите **Топ заблокированных сайтов**;

6. Укажите **Настройки отображения**:

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** на вкладке **Отчеты по расписанию**.

2. Заполните строки:

- **Название** - любое название, которое поможет идентифицировать правило расписания;
- **Email получателя** - электронная почта получателя отчета. Если нужно отправлять отчет нескольким получателям, укажите дополнительные адреса по кнопке **Добавить получателя**.

3. Выберите в выпадающем списке в строке нужный шаблон.

4. Укажите настройки даты/дня и времени отправки отчета получателю.

19.9 Syslog

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

19.9.1 Пересылка системных сообщений

Чтобы настроить пересылку системных сообщений, перейдите в раздел **Отчеты и журналы -> Syslog** и выполните действия:

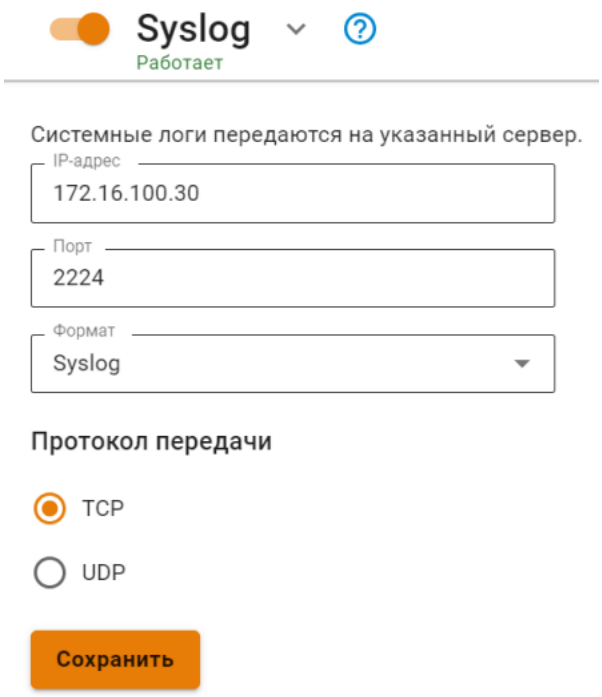
1. Укажите IP-адрес сервера-коллектора (любой локальный «серый» или публичный «белый» IP-адрес);

2. В поле **Порт** укажите любой порт из диапазона от 1 до 65535;

3. Выберите формат передаваемых системных сообщений (Syslog или CEF);

4. Выберите протокол передачи системных логов - TCP или UDP;

5. Нажмите **Сохранить** и включите опцию Syslog:



Подсказка: Рекомендуется передавать логи по протоколу TCP, так как он гарантирует доставку и соблюдает последовательность сообщений.

19.9.2 Расшифровка передаваемых логов

Формат CEF

Логи в CEF-формате начинаются со строки вида:

```
192.168.1.100 Nov 05 14:57:10 daemon warning 2024-11-05T14:44:20+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|
```

где:

- `192.168.1.100` - IP-адрес NGFW отправителя;
- `Nov 05 14:57:10` - время получения события по Syslog;
- `warning` - приоритет сообщения в логах. Другие значения: `info` (информационное сообщение), `notice` (уведомление);
- `2024-11-05T14:44:20+05:00` - время события в Ideco NGFW;
- `ngfw-17` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `CEF:0` - версия формата CEF;
- `Ideco` - вендор;
- `NGFW` - название продукта;
- `17.0` - версия продукта;
- `0|syslog|0` - идентификатор лога, постоянный для NGFW. Состоит из трех полей: идентификатор типа события, описание события, важность события.

Предотвращение вторжений:

```
192.168.1.100 Nov 05 14:57:10 daemon warning 2024-11-05T14:44:20+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730799860 Severity=Warning␣
↪DeviceProcessName=web-proxy DeviceCustomString1=1218332722865011␣
↪DeviceInboundInterface=seq:Leth1{3 DeviceProcessName=suricata_debug␣
↪DeviceCustomString5=alert SourceAddress=192.168.101.25 DeviceCustomString1=local␣
↪DeviceCustomString1Label=Src IP Type SourcePort=38003 SourceCountry=␣
↪DeviceCustomString2= DeviceCustomString2Label=Src Country Code␣
↪DeviceCustomString3=6103759e-5ad6-48b1-81b5-d15894b005ef␣
↪DeviceCustomString3Label=Src session UUID SourceUserID=2 SourceUserName=user␣
↪DestinationAddress=192.168.101.10 DeviceCustomString4=local␣
↪DeviceCustomString4Label=Dst IP Type DestinationPort=53 DestinationCountry=␣
↪DeviceCustomString5= DeviceCustomString5Label=Dst Country Code DeviceCustomString6=␣
↪DeviceCustomString6Label=Dst session UUID DestinationUserID=-1 DestinationUserName=␣
↪TransportProtocol=UDP DeviceEventClassID=1900005 Message=Mining pool␣
↪DeviceEventCategory=Пулы криптомайнеров Severity=2 DeviceCustomString8=1␣
↪DeviceCustomString8Label=Alert GID DeviceCustomString9=blocked␣
↪DeviceCustomString9Label=Alert action DestinationHostName= RequestUrl=␣
↪RequestClientApplication= FlexNumber1=1 FlexNumber1Label=Flow packets to server␣
↪FlexNumber2=0 FlexNumber2Label=Flow packets to client BytesIn=81 BytesOut=0␣
↪StartTime=2024-11-05 09:44:20.021521 EndTime=2024-11-05 09:44:20.021846␣
↪FlexNumber3=0 FlexNumber3Label=flow DeviceCustomString11=␣
↪DeviceCustomString11Label=flow.state DeviceCustomString12=␣
↪DeviceCustomString12Label=flow.reason FlexNumber4=0 FlexNumber4Label=flow.alerted␣
↪DeviceCustomString14= DeviceCustomString14Label=tcp.tcp_flags DeviceCustomString15=␣
↪DeviceCustomString15Label=tcp.tcp_flags_ts DeviceCustomString16=␣
↪DeviceCustomString16Label=tcp.tcp_flags_tc FlexNumber5=0 FlexNumber5Label=tcp.cwr␣
↪FlexNumber6=0 FlexNumber6Label=tcp.ecn FlexNumber7=0 FlexNumber7Label=tcp.urg␣
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪FlexNumber8=0 FlexNumber8Label=tcp.ack FlexNumber9=0 FlexNumber9Label=tcp.psh␣
↪FlexNumber10=0 FlexNumber10Label=tcp.rst FlexNumber11=0 FlexNumber11Label=tcp.syn␣
↪FlexNumber12=0 FlexNumber12Label=tcp.fin DeviceCustomString17=␣
↪DeviceCustomString17Label=tcp.state
```

где:

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `DeviceCustomString1=1218332722865011` - внутренний идентификатор системы предотвращения вторжений flow (сессии);
- `DeviceInboundInterface=seq:Leth1{3` - содержит идентификатор входящего интерфейса;
- `DeviceProcessName=suricata_debug` - имя экземпляра системы предотвращения вторжений;
- `DeviceCustomString5=alert` - тип события;
- `SourceAddress=192.168.101.25` - IP-адрес источника;
- `DeviceCustomString1=local DeviceCustomString1Label=Src IP Type` - тип IP-адреса источника (`local` - локальный, `external` - внешний);
- `SourcePort=38003` - порт источника;
- `SourceCountry` - название местоположения источника;
- `DeviceCustomString2= DeviceCustomString2Label=Src Country Code` - ISO-код страны источника;
- `DeviceCustomString3=6103759e-5ad6-48b1-81b5-d15894b005ef DeviceCustomString3Label=Src session UUID` - внутренний идентификатор сессии Ideco NGFW источника;
- `SourceUserID=2` - идентификатор пользователя источника;
- `SourceUserName=user` - имя пользователя источника;
- `DestinationAddress=192.168.101.10` - IP-адрес назначения;
- `DeviceCustomString4=local DeviceCustomString4Label=Dst IP Type` - тип IP-адреса назначения (`local` - локальный, `external` - внешний);
- `DestinationPort=53` - порт назначения;
- `DestinationCountry` - название местоположения назначения;
- `DeviceCustomString5= DeviceCustomString5Label=Dst Country Code` - ISO-код страны назначения;
- `DeviceCustomString6= DeviceCustomString6Label=Dst session UUID` - внутренний идентификатор сессии Ideco NGFW назначения;
- `DestinationUserID=-1` - идентификатор пользователя назначения;
- `DestinationUserName` - имя пользователя назначения;
- `TransportProtocol=UDP` - протокол;
- `DeviceEventClassID=1900005` - ID правила системы предотвращения вторжений;
- `Message=Mining pool` - сообщение из сработавшего правила;
- `DeviceEventCategory=Пулы криптомайнеров` - описание колонки в веб-интерфейсе События безопасности. Соответствие *alert.category: -> alert.signature* описаны в файле;

- `Severity=2` - уровень угрозы, может принимать значения 1, 2, 3 и 256, где 1 - самый высокий уровень угрозы;
- `DeviceCustomString8=1 DeviceCustomString8Label=Alert GID` - GID угрозы;
- `DeviceCustomString9=blocked DeviceCustomString9Label=Alert action` - действие по отношению к угрозе (блокировать).

Служебные поля результата анализа HTTP-трафика. Заполняются, если в процессе анализа трафика был определен HTTP-протокол:

- `DestinationHostName` - идентификатор хоста;
- `RequestUrl` - URL, на который велось обращение;
- `RequestClientApplication` - информация, идентифицирующая HTTP-клиента.

Служебные поля flow (сессии):

- `FlexNumber1=1 FlexNumber1Label=Flow packets to server` - количество пакетов, переданное от клиента к серверу;
- `FlexNumber2=0 FlexNumber2Label=Flow packets to client` - количество пакетов, переданное от сервера к клиенту;
- `BytesIn=81` - количество байт, переданное от клиента к серверу;
- `BytesOut=0` - количество байт, переданное от сервера к клиенту;
- `StartTime=2024-11-05 09:44:20.021521` - начало;
- `EndTime=2024-11-05 09:44:20.021846` - окончание;
- `FlexNumber3=0 FlexNumber3Label=flow` - возраст;
- `DeviceCustomString11= DeviceCustomString11Label=flow.state` - текущее состояние;
- `DeviceCustomString12= DeviceCustomString12Label=flow.reason` - запущен ли IPsec в режиме отладки;
- `FlexNumber4=0 FlexNumber4Label=flow.alerted` - сгенерировался ли поток alert.

Состояние флага TCP flow (сессии):

- `DeviceCustomString14= DeviceCustomString14Label=tcp.tcp_flags` - значение поля flags в заголовке TCP;
- `DeviceCustomString15= DeviceCustomString15Label=tcp.tcp_flags_ts` - timestamp флаги;
- `DeviceCustomString16= DeviceCustomString16Label=tcp.tcp_flags_tc` - флаг Truncated response;
- `FlexNumber5=0 FlexNumber5Label=tcp.cwr` - флаг TCP-пакета, информирующий отправителя, что получен пакет с установленным флагом ECE (Подробнее в RFC-3186);
- `FlexNumber6=0 FlexNumber6Label=tcp.ecn` - флаг TCP-пакета, информирующий получателя, что узел способен на явное уведомление о перегрузке сети;
- `FlexNumber7=0 FlexNumber7Label=tcp.urg` - флаг TCP-пакета, указывающий важность пакета;
- `FlexNumber8=0 FlexNumber8Label=tcp.ack` - флаг TCP-пакета, указывающий, что пакет получен;
- `FlexNumber9=0 FlexNumber9Label=tcp.psh` - флаг TCP-пакета, информирующий получателя, что все данные переданы и можно передать их приложению;
- `FlexNumber10=0 FlexNumber10Label=tcp.rst` - флаг TCP-пакета, указывающий, что соединение завершено в аварийном режиме;
- `FlexNumber11=0 FlexNumber11Label=tcp.syn` - флаг TCP-пакета, отвечающий за установку соединения;
- `FlexNumber12=0 FlexNumber12Label=tcp.fin` - флаг TCP-пакета, указывающий на завершение соединения в штатном порядке;

- `DeviceCustomString17= DeviceCustomString17Label=tcp.state` - состояния сеанса TCP.

Файрвол:

Логирование включается в разделе **Правила трафика -> Файрвол -> Логирование**.

```
192.168.1.100 Nov 05 16:49:00 daemon notice 2024-11-05T16:48:49+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730807329 Severity=Warning␣
↪DeviceProcessName=ideco-nflog msg=TCP src 192.168.101.25 sport 52416 dst 161.148.
↪164.31 dport 443 table FWD rule 1 action drop
```

где:

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `TCP` - протокол. Это поле принимает значения: UDP, TCP, ICMP, GRE, ESP и AH;
- `src` - IP-адрес источника;
- `sport` - порт источника для UDP и TCP;
- `dst` - IP-адрес назначения;
- `dport` - порт назначения для UDP и TCP;
- `table` - таблица правил, в которой произошло логирование;
- `rule` - ID правила из таблицы;
- `action` - действие, которое произошло.

Контроль приложений:

```
192.168.1.100 Nov 05 16:07:01 daemon info 2024-11-05T16:06:52+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730804812 Severity=Notice␣
↪DeviceProcessName=ideco-app-control msg=(flow_info_rules_was_checked) 192.168.101.
↪25:37936 -> 192.168.101.10:53 [Nintendo] \= 'DROP'.
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `flow_info_rules_was_checked` - идентификатор процесса;
- `192.168.101.25:37936` - IP-адрес и порт источника;
- `192.168.101.10:53` - IP-адрес и порт назначения;
- `DROP` - результат анализа трафика;
- `[Nintendo]` - название приложения, к которому применен результат. Список всех приложений.

Контент-фильтр:

Логирование включается в разделе **Сервисы -> Прокси -> Основное**. Просмотр логов доступен в веб-интерфейсе в разделе **Отчеты и журналы -> Журнал веб-доступа**. Название служб для фильтрации: `ideco-content-filter-backend` и `squid`.

Пример блокировки ресурса:

```
192.168.1.100 Nov 06 16:39:20 daemon info 2024-11-06T18:39:18+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730900358 Severity=Notice␣
↪DeviceProcessName=squid msg=192.168.101.25 - - [06/Nov/2024:18:39:18 +0500] "GET␣
↪https://www.last.fm/ HTTP/1.1" 403 7479 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:131.
↪0) Gecko/20100101 Firefox/131.0" TCP_DENIED:HIER_NONE "Custom deny 2 Запрещенные␣
↪сайты users.id.2 group.id.1 " "av_name": "-", "av_object_infected": "-", "av_object_
↪size": "-", "av_virus_name": "-"
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `192.168.101.25` - IP-адрес пользователя;
- `[06/Nov/2024:18:39:18 +0500]` - дата/время события блокировки;
- `GET` - метод;
- `https://www.last.fm/` - URL заблокированного ресурса;
- `HTTP/1.1` - протокол;
- `403` - код состояния HTTP;
- `7479` - передано байт (в ответ, включая HTTP-заголовок);
- `Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0` - цифровой отпечаток браузера;
- `TCP_DENIED:HIER_NONE` - техническое сообщение от squid;
- `Custom deny 2 Запрещенные сайты users.id.2 group.id.1`:
  - `2 Запрещенные сайты` - название и номер правила блокировки;
  - `users.id.2` - категория сайта;
  - `group.id.1` - значение поля **Применяется для** в сработавшем правиле.

SSO-аутентификация:

```
2024-07-18T17:11:40+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721304700 Severity=Notice DeviceProcessName=ideco-
↪web-authd msg=Subnet 192.168.205.254/32 is authorized as user 'Sanek'. Connection␣
↪made from None, type 'web'.
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `192.168.205.254/32` - IP-адрес пользователя;
- `Sanek` - логин пользователя;
- `type 'web'` - тип авторизации (веб).

Авторизация через журнал безопасности AD:

```
2024-07-18T17:20:22+05:00 Ideco-NGFW CEF:0|Ideco|NGFW|17.
↪0|0|syslog|0|deviceReceiptTime=1721305222 Severity=Notice DeviceProcessName=ideco-
↪auth-backend msg=Subnet 192.168.205.254/32 is authorized as user 'Sanek'.␣
↪Connection made from None, type 'log'.
```

- deviceReceiptTime - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- Severity - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- DeviceProcessName - название службы NGFW;
- 192.168.205.254/32 - IP-адрес пользователя;
- Sanek - логин пользователя;
- type 'log' - тип авторизации (через журнал безопасности AD).

Веб-авторизация:

```
192.168.1.100 Nov 05 18:18:58 daemon info 2024-11-05T18:18:51+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730812731 Severity=Notice␣
↪DeviceProcessName=ideco-web-authd msg=Subnet 192.168.101.25/32 is authorized as␣
↪user 'user'. Connection made from None, type 'web'.
```

- deviceReceiptTime - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- Severity - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- DeviceProcessName - название службы NGFW;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'web' - тип авторизации (веб).

Авторизация по IP:

```
192.168.1.100 Nov 05 19:17:32 daemon info 2024-11-05T19:17:23+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730816243 Severity=Notice␣
↪DeviceProcessName=ideco-auth-backend msg=Subnet 192.168.101.25/32 is authorized as␣
↪user 'user'. Connection made from None, type 'ip'.
```

- deviceReceiptTime - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- Severity - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- DeviceProcessName - название службы NGFW;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'ip' - тип авторизации (IP).

Авторизация по MAC:

```
192.168.1.100 Nov 05 19:23:03 daemon info 2024-11-05T19:22:55+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730816575 Severity=Notice␣
↪DeviceProcessName=ideco-auth-backend msg=Subnet 192.168.101.25/32 is authorized as␣
↪user 'user'. Connection made from None, type 'mac'.
```

- deviceReceiptTime - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- Severity - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- DeviceProcessName - название службы NGFW;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;

- `type 'mac'` - тип авторизации (MAC).

Авторизация по подсети:

```
192.168.1.100 Nov 05 19:27:05 daemon info 2024-11-05T19:26:58+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730816818 Severity=Notice␣
↪DeviceProcessName=ideco-auth-backend msg=Subnet 192.168.101.0/24 is authorized as␣
↪user 'user'. Connection made from None, type 'net'
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `192.168.101.0/24` - подсеть, по которой происходит авторизация;
- `user` - логин пользователя;
- `type 'net'` - тип авторизации (подсеть).

Подключение по VPN:

```
192.168.1.100 Nov 06 12:15:46 daemon info 2024-11-06T14:15:35+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730884535 Severity=Notice␣
↪DeviceProcessName=ideco-vpn-authd msg=Subnet 10.128.0.3/32 is authorized as user
↪'user'. Connection made from '192.168.1.25', type 'pptp'.
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `10.128.0.3/32` - сеть для VPN-подключений;
- `user` - логин пользователя;
- `192.168.1.25` - IP-адрес, откуда установлено подключение;
- `pptp` - протокол.

Служба fail2ban:

```
192.168.1.100 Nov 06 15:02:25 daemon info 2024-11-06T17:02:17+05:00 ngfw-17␣
↪CEF:0|Ideco|NGFW|17.0|0|syslog|0|deviceReceiptTime=1730894537 Severity=Notice␣
↪DeviceProcessName=fail2ban msg=INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-06␣
↪17:02:16
```

- `deviceReceiptTime` - время события в системе NGFW, может не совпадать с временем получения события по Syslog;
- `Severity` - важность события (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug);
- `DeviceProcessName` - название службы NGFW;
- `INFO` или `NOTICE` - приоритет сообщения в логах в виде информационного сообщения или уведомления;
- `INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-06 17:02:16` - факт обнаружения правил безопасности с указанием группы правил ([utm-vpn-authd]), IP-адреса и даты/времени. Список групп правил:
  - `utm-dovecot` - авторизация на почтовом сервере через почтовые клиенты;
  - `utm-postfix-connrate` - превышение лимита подключения к почтовому серверу;

- `utm-postscreen-prgrt` - отслеживание нежелательных подключений (PREGREET) к почтовому серверу;
- `utm-reverse-proxy-conn` - защита от DoS (лимит подключений);
- `utm-reverse-proxy-req` - защита от DoS (лимит запросов в секунду);
- `utm-reverse-proxy` - Web Application Firewall (WAF);
- `utm-roundcube` - авторизация в веб-интерфейсы почтового сервера;
- `utm-smtp` - авторизация по smtp;
- `utm-ssh` - авторизация по ssh;
- `utm-two-factor-codes` - прохождение двухфакторной аутентификации;
- `utm-vpn-authd` - авторизация по VPN;
- `utm-vpn-pppoe-authd` - авторизация по VPN PPPoE;
- `utm-web-interface` - авторизация в административном веб-интерфейсе;
- `utm-user-cabinet` - авторизация в пользовательском веб-интерфейсе.

Формат Syslog

Логи в Syslog-формате начинаются со строки вида:

```
192.168.1.100 Nov 05 19:30:56 1 daemon warning 2024-11-05T19:30:51+05:00
```

где:

- `192.168.1.100` - IP-адрес NGFW отправителя;
- `Nov 05 14:42:25` - время получения события по Syslog;
- `warning` - приоритет сообщения в логах. Другие значения: `info` (информационное сообщение), `notice` (уведомление);
- `2024-11-05T14:36:17+05:00` - время события в Ideco NGFW.

Предотвращение вторжений:

```
192.168.1.100        Nov 05 14:42:25 1 daemon warning 2024-11-05T14:36:17+05:00 ngfw-
↪17 suricata - - - flow_id:534238476293026, in_iface:seq:Leth1{3, sensor_
↪name:suricata_debug, event_type:alert, src_ip:192.168.101.25, src_ip_type:local,␣
↪src_port:36872, src_country:, src_country_code:, src_session_uuid:6103759e-5ad6-
↪48b1-81b5-d15894b005ef, src_user_id:2, src_user_name:user, dest_ip:192.168.101.10,␣
↪dest_ip_type:local, dest_port:53, dest_country:, dest_country_code:, dest_session_
↪uuid:, dest_user_id:-1, dest_user_name:, proto:UDP, alert.signature_id:1900005,␣
↪alert.signature:Mining pool, alert.category:Пулы криптомайнеров, alert.severity:2,␣
↪alert.gid:1, alert.action:blocked, http.hostname:, http.url:, http.http_user_agent:,
↪ flow.pkts_toserver:1, flow.pkts_toclient:0, flow.bytes_toserver:81, flow.bytes_
↪toclient:0, flow.start:2024-11-05 09:36:17.714211, flow.end:2024-11-05 09:36:17.
↪714612, 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:
```

- `ngfw-17` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `suricata` - название службы;
- `flow_id:534238476293026` - внутренний идентификатор системы предотвращения вторжений flow (сессии);
- `in_iface:seq:Leth1{3` - содержит идентификатор входящего интерфейса;

- `sensor_name:suricata_debug` - имя экземпляра системы предотвращения вторжений;
- `event_type:alert` - тип события;
- `src_ip:192.168.101.25` - IP-адрес источника;
- `src_port:36872` - порт источника;
- `src_country:` - название местоположения источника;
- `src_country_code:` - ISO-код страны источника;
- `src_session_uuid:6103759e-5ad6-48b1-81b5-d15894b005ef` - внутренний идентификатор сессии Ideco NGFW источника;
- `src_user_id:2` - идентификатор пользователя источника;
- `src_user_name:user`- имя пользователя источника;
- `dest_ip:192.168.101.10` - 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:1900005` - ID правила системы предотвращения вторжений;
- `alert.signature:Mining pool` - сообщение из сработавшего правила;
- `alert.category:Пулы криптомайнеров` - описание колонки в веб-интерфейсе **События безопасности**. Соответствие *alert.category: -> alert.signature* описаны в файле;
- `alert.severity:2` - уровень угрозы, может принимать значения 1, 2, 3 и 256, где 1 - самый высокий уровень угрозы;
- `alert.gid:1` - GID угрозы;
- `alert.action:blocked` - действие по отношению к угрозе (блокировать).

Служебные поля результата анализа HTTP-трафика. Заполняются, если в процессе анализа трафика был определен HTTP-протокол:

- `http.hostname:` - идентификатор хоста;
- `http.url:` - URL, на который велось обращение;
- `http.http_user_agent:` - информация, идентифицирующая HTTP-клиента.

Служебные поля flow (сессии):

- `flow.pkts_toserver:1` - количество пакетов, переданное от клиента к серверу;
- `flow.pkts_toclient:0` - количество пакетов, переданное от сервера к клиенту;
- `flow.bytes_toserver:81` - количество байт, переданное от клиента к серверу;
- `flow.bytes_toclient:0` - количество байт, переданное от сервера к клиенту;
- `flow.start:2024-11-05 09:36:17.714211` - начало;
- `flow.end:2024-11-05 09:36:17.714612` - окончание;
- `flow.age:0` - возраст;
- `flow.state:` - текущее состояние;

- `flow.reason:` - запущена ли IPsec в режиме отладки;
- `flow.alerted:0` - сгенерировался ли поток alert.

Состояние флага TCP flow(сессии):

- `tcp.tcp_flags:` - значение поля flags в заголовке TCP;
- `tcp.tcp_flags_ts:` - timestamp флаги;
- `tcp.tcp_flags_tc:` - флаг Truncated response;
- `tcp.cwr:0` - флаг TCP-пакета, информирующий отправителя, что получен пакет с установленным флагом ECE (Подробнее в RFC-3186);
- `tcp.ecn:0` - флаг TCP-пакета, информирующий получателя, что узел способен на явное уведомление о перегрузке сети;
- `tcp.urg:0` - флаг TCP-пакета, указывающий важность пакета;
- `tcp.ack:0` - флаг TCP-пакета, указывающий, что пакет получен;
- `tcp.psh:0` - флаг TCP-пакета, информирующий получателя, что все данные переданы и можно передать их приложению;
- `tcp.rst:0` - флаг TCP-пакета, указывающий, что соединение завершено в аварийном режиме;
- `tcp.syn:0` - флаг TCP-пакета, отвечающий за установку соединения;
- `tcp.fin:0` - флаг TCP-пакета, указывающий на завершение соединения в штатном порядке;
- `tcp.state:` - состояния сеанса TCP.

Файрвол:

```
192.168.1.100 Nov 05 16:50:52 1 daemon notice 2024-11-05T16:50:46+05:00 ngfw-17 ideco-
↪nflog - - - TCP src 192.168.101.25 sport 35468 dst 161.148.164.31 dport 443 table␣
↪FWD rule 1 action drop
```

- `ngfw-17` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-nflog` - название службы;
- `TCP` - протокол, принимает значения: UDP, TCP, ICMP, GRE, ESP и AH;
- `src` - IP-адрес источника;
- `sport` - порт источника для UDP и TCP;
- `dst` - IP-адрес назначения;
- `dport` - порт назначения для UDP и TCP;
- `table` - таблица правил, в которой произошло логирование;
- `rule` - ID правила из таблицы;
- `action` - действие, которое произошло.

Контроль приложений:

```
192.168.1.100 Nov 05 16:04:58 1 daemon info 2024-11-05T16:04:51+05:00 ngfw-17 ideco-
↪app-control - - - (flow_info_rules_was_checked) 192.168.101.25:43800 -> 192.168.101.
↪10:53 [Nintendo] = 'DROP'.
```

- `ngfw-17` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-app-control` - название службы;
- `192.168.101.25:43800` - IP-адрес и порт источника;
- `192.168.101.10:53` - IP-адрес и порт назначения;

- DROP - результат анализа трафика;
- [Nintendo] - название приложения, к которому применен результат. Список всех приложений.

Контент-фильтр:

Логирование включается в разделе **Сервисы -> Прокси -> Основное**. Просмотр логов доступен в веб-интерфейсе в разделе **Отчеты и журналы -> Журнал веб-доступа**. Название служб для фильтрации: ideco-content-filter-backend и squid.

Пример блокировки ресурса:

```
192.168.1.100 Nov 06 16:40:56 1 daemon info 2024-11-06T18:40:50+05:00 ngfw-17 squid -␣
↪- - 192.168.101.25 - - [06/Nov/2024:18:40:50 +0500] "GET https://www.last.fm/ HTTP/
↪1.1" 403 7479 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/
↪131.0" TCP_DENIED:HIER_NONE "Custom deny 2 Запрещенные сайты users.id.2 group.id.1
↪" "av_name": "-", "av_object_infected": "-", "av_object_size": "-", "av_virus_name
↪": "-"
```

- ngfw-17 - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- squid - название службы;
- 192.168.101.25 - IP-адрес пользователя;
- [06/Nov/2024:18:40:50 +0500] - дата/время события блокировки;
- GET - метод;
- https://www.last.fm/ - URL заблокированного ресурса;
- HTTP/1.1 - протокол;
- 403 - код состояния HTTP;
- 7479 - передано байт (в ответ, включая HTTP-заголовок);
- Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0 - цифровой отпечаток браузера;
- TCP_DENIED:HIER_NONE - техническое сообщение от squid;
- Custom deny 2 Запрещенные сайты users.id.2 group.id.1:
  - 2 Запрещенные сайты - название и номер правила блокировки;
  - users.id.2 - категория сайта;
  - group.id.1 - значение поля **Применяется для** в сработавшем правиле.

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 - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- ideco-web-authd - название службы;
- 192.168.205.254/32 - IP-адрес пользователя;
- Sanek - логин пользователя;
- type 'web' - тип авторизации (веб).

Авторизация через журнал безопасности AD:

```
2024-07-18T16:19:39+05:00 Ideco-NGFW ideco-auth-backend - - - Subnet 192.168.205.254/
↪32 is authorized as user 'Sanek'. Connection made from None, type 'log'.
```

- Ideco-NGFW - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;

- ideco-auth-backend - название службы;
- 192.168.205.254/32 - IP-адрес пользователя;
- Sanek - логин пользователя;
- type 'log' - тип авторизации (через журнал безопасности AD).

Веб-авторизация:

```
192.168.1.100 Nov 05 18:12:01 1 daemon info 2024-11-05T18:11:48+05:00 ngfw-17 ideco-
↪web-authd - - - Subnet 192.168.101.25/32 is authorized as user 'user'. Connection␣
↪made from None, type 'web'.
```

- ngfw-17 - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- ideco-web-authd - название службы;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'web' - тип авторизации (веб).

Авторизация по IP:

```
192.168.1.100 Nov 05 19:38:58 1 daemon info 2024-11-05T19:38:46+05:00 ngfw-17 ideco-
↪auth-backend - - - Subnet 192.168.101.25/32 is authorized as user 'user'.␣
↪Connection made from None, type 'ip'.
```

- ngfw-17 - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- ideco-auth-backend - название службы;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'ip' - тип авторизации (IP).

Авторизация по MAC:

```
192.168.1.100 Nov 05 19:32:47 1 daemon info 2024-11-05T19:32:34+05:00 ngfw-17 ideco-
↪auth-backend - - - Subnet 192.168.101.25/32 is authorized as user 'user'.␣
↪Connection made from None, type 'mac'.
```

- ngfw-17 - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- ideco-auth-backend - название службы;
- 192.168.101.25/32 - IP-адрес пользователя;
- user - логин пользователя;
- type 'mac' - тип авторизации (MAC).

Авторизация по подсетям:

```
192.168.1.100 Nov 05 19:30:56 1 daemon info 2024-11-05T19:30:51+05:00 ngfw-17 ideco-
↪auth-backend - - - Subnet 192.168.101.0/24 is authorized as user 'user'. Connection␣
↪made from None, type 'net'.
```

- ngfw-17 - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- ideco-auth-backend - название службы;
- 192.168.101.0/24 - подсеть пользователя;
- user - логин пользователя;

- `type 'net'` - тип авторизации (подсеть).

Подключение по VPN:

```
192.168.1.100 Nov 06 12:12:36 1 daemon info 2024-11-06T14:12:24+05:00 ngfw-17 ideco-
↪vpn-authd - - - Subnet 10.128.0.3/32 is authorized as user 'user'. Connection made␣
↪from '192.168.1.25', type 'pptp'.
```

- `ngfw-17` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `ideco-vpn-authd` - название службы;
- `10.128.0.3/32` - сеть для VPN-подключений;
- `user` - логин пользователя;
- `192.168.1.25` - IP-адрес, с которого установлено подключение;
- `pptp` - протокол.

Служба fail2ban:

```
192.168.1.100 Nov 06 15:14:42 1 daemon info 2024-11-06T17:14:30+05:00 ngfw-17␣
↪fail2ban - - - INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-06 17:14:30
```

- `ngfw-17` - hostname сервера NGFW, заданный в левом верхнем углу веб-интерфейса;
- `fail2ban` - название службы;
- `INFO` или `NOTICE` - приоритет сообщения в логах в виде информационного сообщения или уведомления;
- `INFO [utm-vpn-authd] Found 192.168.1.25 - 2024-11-06 17:02:16` - факт обнаружения правил безопасности с указанием группы правил ([utm-vpn-authd]), IP-адреса и даты/времени. Список групп правил:
  - `utm-dovecot` - авторизация на почтовом сервере через почтовые клиенты;
  - `utm-postfix-connrate` - превышение лимита подключения к почтовому серверу;
  - `utm-postscreen-prgrt` - отслеживание нежелательных подключений (PREGREET) к почтовому серверу;
  - `utm-reverse-proxy-conn` - защита от DoS (лимит подключений);
  - `utm-reverse-proxy-req` - защита от DoS (лимит запросов в секунду);
  - `utm-reverse-proxy` - Web Application Firewall (WAF);
  - `utm-roundcube` - авторизация в веб-интерфейсы почтового сервера;
  - `utm-smtp` - авторизация по smtp;
  - `utm-ssh` - авторизация по ssh;
  - `utm-two-factor-codes` - прохождение двухфакторной аутентификации;
  - `utm-vpn-authd` - авторизация по VPN;
  - `utm-vpn-pppoe-authd` - авторизация по VPN PPPoE;
  - `utm-web-interface` - авторизация в административном веб-интерфейсе;
  - `utm-user-cabinet` - авторизация в пользовательском веб-интерфейсе.

20. Управление сервером

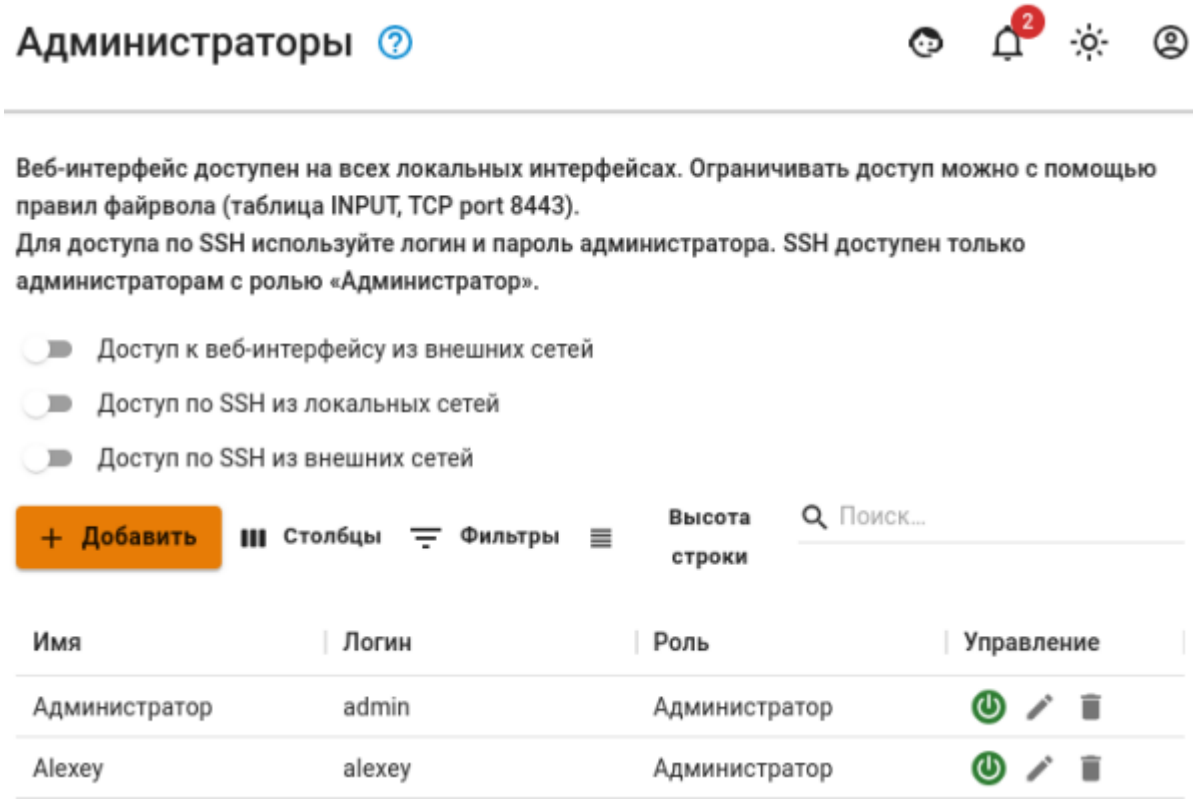
20.1 Администраторы

20.1.1 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 превышать 42 символа и не должно состоять только из цифр;
- **Пароль/повторите пароль** - введите пароль нового администратора. Значение не должно быть короче 11 символов. Рекомендуем использовать сложные пароли, содержащие латинские строчные и заглавные буквы, цифры и специальные символы;
- **Роль** - выберите роль.

Роли:

- **Администратор** - получает полный доступ к настройке NGFW;

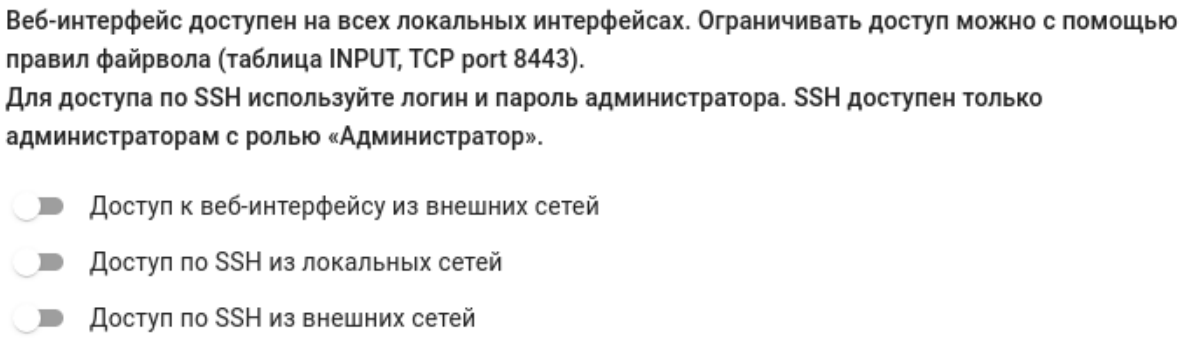
- **Только просмотр** - администратор не сможет производить никаких настроек в веб-интерфейсе, так как при попытке внесения изменений будет появляться окно с ошибкой **Доступ запрещен**;
- **Просмотр отчетов** - администратору будет доступна часть раздела *Отчеты и журналы*, а именно Трафик, Журнал событий, Журнал веб-доступа, Журнал антивируса, События безопасности и Журнал авторизации;
- **Создание отчетов** - администратору будет доступна часть раздела *Отчеты и журналы*, а именно Трафик, Журнал событий, Журнал веб-доступа, Журнал антивируса, События безопасности, Журнал авторизации и Конструктор отчетов.

Подсказка: При бездействии в течение 15 минут администратор будет автоматически разавторизован.

При наличии большого количества администраторов в таблице воспользуйтесь кнопкой **Фильтры**.

20.1.2 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*.

20.1.3 Восстановление пароля администратора

Подробнее о восстановлении пароля администратора смотрите в статье по *ссылке*.

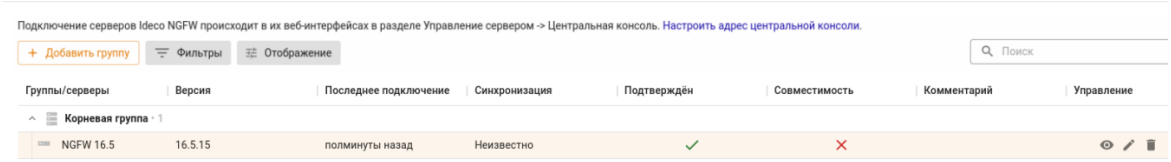
20.2 Центральная консоль

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 нескольких серверов Ideco NGFW. На данный момент не требует лицензирования и не имеет ограничений к использованию. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW, даже если они были подключены после того, как политики были настроены.

20.2.1 Подключение Ideco NGFW к Ideco Center

Внимание: При синхронизации Ideco Center и Ideco NGFW с разными мажорными версиями передача правил с Ideco Center происходить не будет. При этом в разделе **Серверы** будет информация о том, что Ideco Center и Ideco NGFW несовместимы:



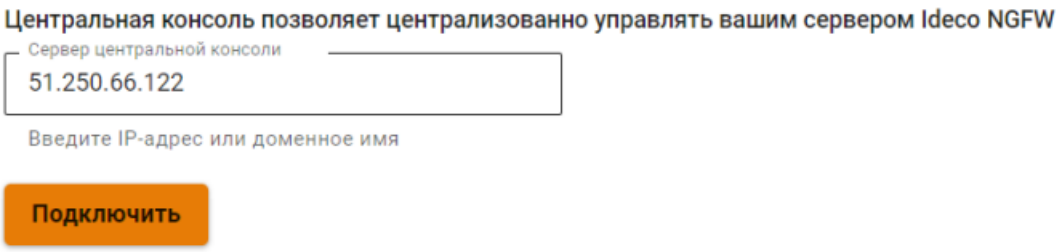
Предупреждение: Особенности работы:

- Если в подключаемом Ideco NGFW используется кластер, достаточно подключить только активную ноду, пассивная автоматически примет эту настройку;
- Сетевое подключение производится в направлении от Ideco NGFW к Ideco Center, т. е. возможна связь и когда Ideco NGFW за NAT;
- Если сервер Ideco Center находится за NAT, укажите IP-адрес NAT-устройства или доменное имя, перейдя в Ideco Center в раздел **Управление сервером -> Дополнительно -> Адрес центральной консоли**.

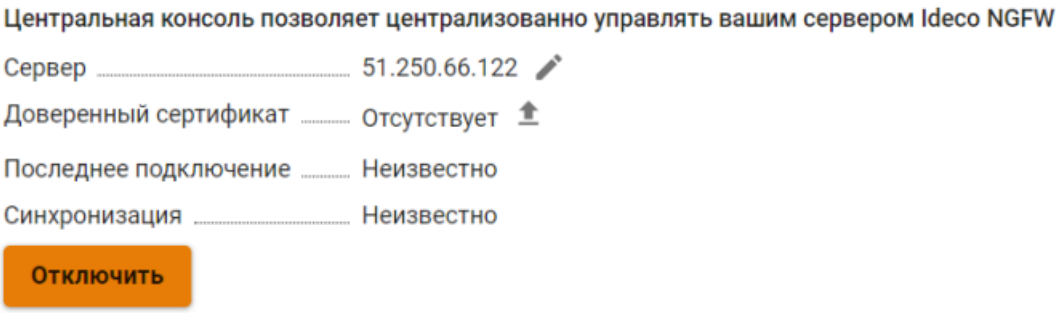
Подключение Ideco NGFW к Ideco Center:

1. Перейдите в раздел **Управление сервером -> Центральная консоль**.

2. Введите IP-адрес или доменное имя в строке **Сервер центральной консоли** и нажмите **Подключить**:

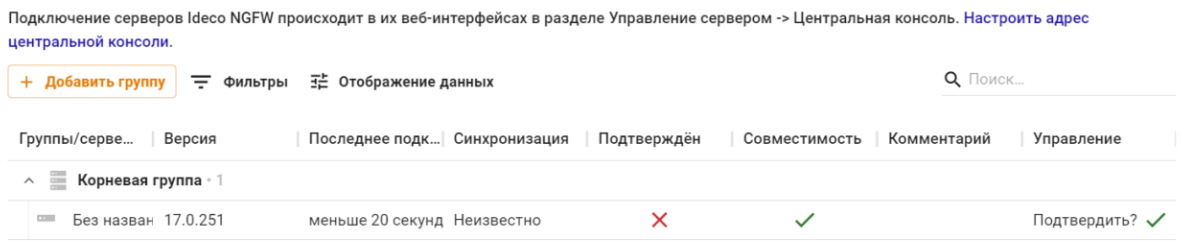


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW:



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

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



Для удаления сервера Ideco NGFW из Ideco Center разорвите привязку в интерфейсе Ideco Center:

Для этого в таблице **Серверы** в столбце **Управление** напротив нужного сервера выберите и подтвердите выбор.

20.3 VCE

VCE (virtual context engine) - это функция Ideco NGFW, которая позволяет создавать виртуальные серверы на одном корневом NGFW. Это дает возможность разбить одну локальную сеть на несколько независимых подсетей, индивидуально создавать для каждой из этих сетей политики безопасности и объекты, а также разграничивать доступ и независимо управлять дочерними VCE. При этом нет необходимости устанавливать и настраивать для этого отдельные физические серверы.

> **Предупреждение:** Не предоставляйте доступ к VCE сторонним организациям, поскольку полная изоляция VCE не реализована и не предусмотрена. Предоставление доступа сторонним организациям может привести к угрозе безопасности сервера.

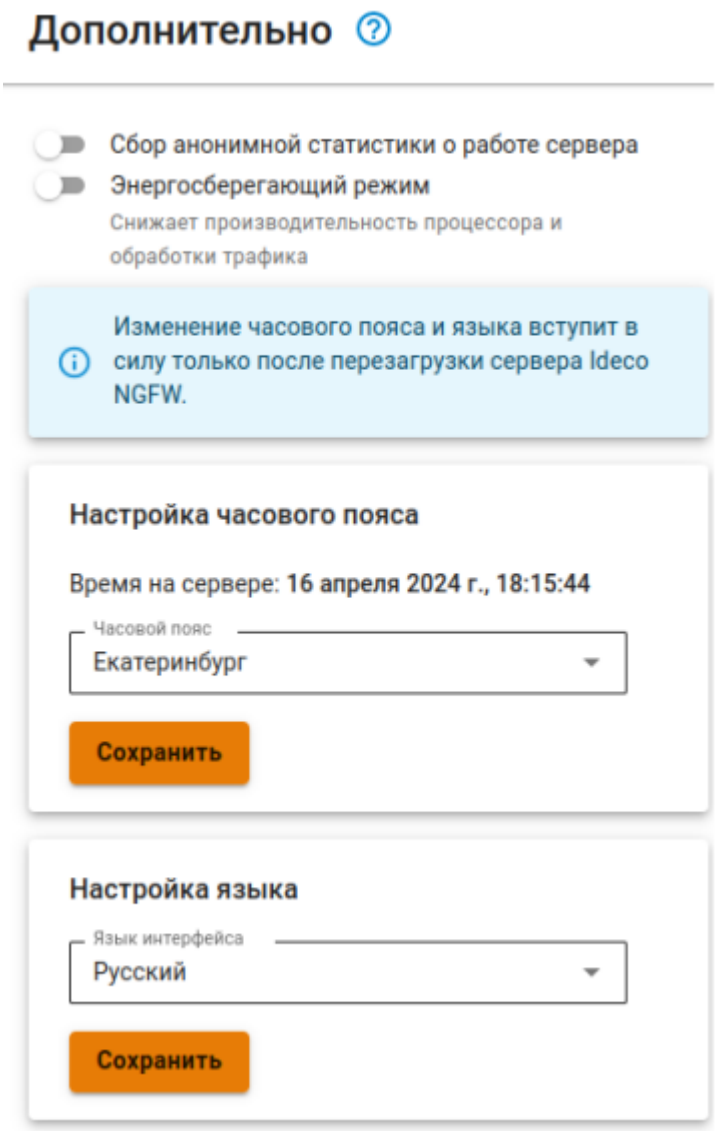
Функциональность созданных внутри NGFW виртуальных VCE почти не отличается от функциональности NGFW.

Возможности VCE:

- Создание виртуальных серверов Ideco NGFW и настройка независимых сетевых интерфейсов;
- Независимая настройка политик безопасности и прав доступа различным виртуальным NGFW;
- Запуск и остановка виртуальных серверов с одного корневого NGFW.

В интерфейсе VCE недоступно:

- Создание *кластера*;
- Полное восстановление из бекапов (как в локальном меню, так и в веб-интерфейсе Ideco NGFW). При этом доступно мгновенное восстановление (с версии 18 полное восстановление доступно);
- Изменение статуса **Разрешить интернет всем**;
- Изменение настроек часового пояса и языка:



Подсказка: В *бекап* корневого VCE не входят данные и настройки, которые содержатся в дочерних VCE. Чтобы обеспечить полное сохранение данных, создайте бекап отдельно по корневому VCE и по каждому из дочерних VCE.

Нельзя добавлять LACP-интерфейсы в VCE.

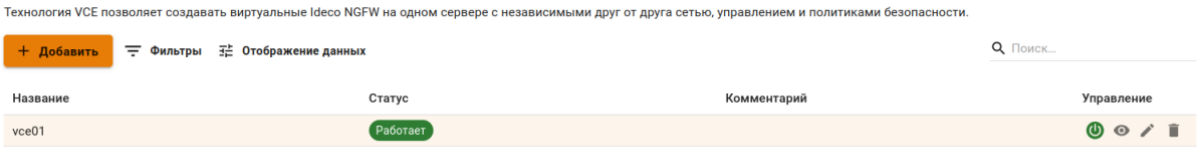
20.3.1 Создание VCE

Подсказка: Для работы VCE требуется не менее 16 ГБ оперативной памяти.

Чтобы создать виртуальный сервер в рамках VCE, перейдите в раздел **Управление сервером -> VCE** и выполните действия:

1. Нажмите кнопку **Добавить**.

2. Введите название сервера и нажмите **Сохранить**. Виртуальный сервер появится в таблице:



3. Перейдите в раздел **Сервисы -> Сетевые интерфейсы** и на вкладке **VCE-интерфейсы** создайте интерфейс для виртуального сервера. Для работы VCE нужен минимум один сетевой интерфейс. Подробнее о создании VCE-интерфейсов в *статье*.

Подсказка: Сетевой интерфейс без тега VLAN, подключенный к VCE, будет недоступен для использования корневым NGFW.

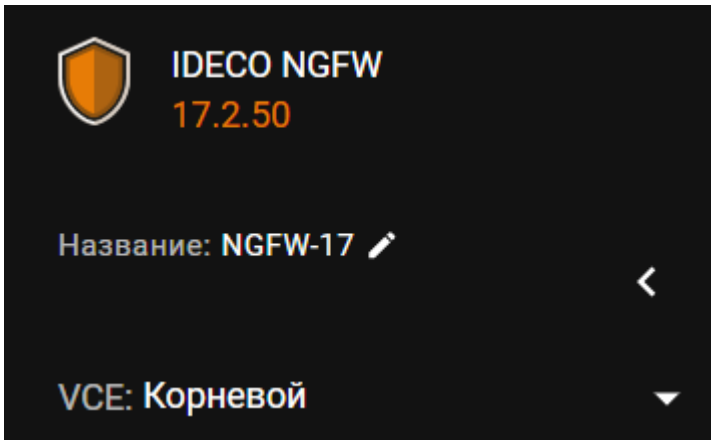
Если VCE выключен, переданные ему сетевые интерфейсы становятся вновь доступны корневому NGFW, их можно использовать для создания нового виртуального сервера. При этом VCE, которому они принадлежали ранее, станет недоступен после включения.

Чтобы отредактировать VCE, нажмите на . При редактировании можно менять название виртуального сервера. Редактирование доступно в том числе для работающего VCE.

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

20.3.2 Переход в веб-интерфейс VCE

После создания VCE текущий сервер Ideco NGFW, в котором VCE был создан, будет обозначен как корневой:



Перейти в веб-интерфейс созданного VCE из веб-интерфейса NGFW можно двумя способами:

1. Перейдите в **Управление сервером -> VCE** и нажмите на :

После этого веб-интерфейс VCE откроется в новой вкладке браузера.

В новой вкладке откроется веб-интерфейс VCE.

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

После этого веб-интерфейс VCE откроется в текущей вкладке браузера. Меню интерфейса корневого NGFW будет свернуто, вернуться к нему можно, кликнув на панель слева.

Также перейти в веб-интерфейс VCE можно из веб-интерфейса Ideco Center. Для этого сначала перейдите из интерфейса Ideco Center в интерфейс корневого NGFW одним из способов, указанных в *статье*.

Пример перехода:

В интерфейсе Ideco Center нажмите на ▼ в левом верхнем углу и выберите нужный NGFW. В открывшемся веб-интерфейсе NGFW нажмите на ▼ в левом верхнем углу и выберите нужный VCE.

20.3.3 Удаление VCE

Удалить VCE можно, нажав на  в корневом VCE.

20.4 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.
- **Резервная** нода находится в предзагруженном состоянии и непрерывно мониторит состояние активной ноды, а при отсутствии связи с ней переводит текущие задачи обработки трафика на себя.

Предупреждение: В любой момент обрабатывать трафик может только одна из нод.

Сетевое взаимодействие между нодами осуществляется по *Кластерной сети*. Это физический канал, под который на каждой из нод резервируется по одному физическому порту. Веб-сервер активной ноды управляет кластером, а резервная нода постоянно готова принимать данные. При переключении нод пассивная нода полностью прогружается и становится активной.

Если IP-адреса кластера настроены вручную, то он имеет один общий IP на внутреннем интерфейсе и другой общий IP на внешнем интерфейсе. В случае автоматической конфигурации по DHCP адреса будут отличаться в зависимости от ноды.

20.4.1 Процесс синхронизации нод в кластере

- При синхронизации двух NGFW данные активной ноды копируются в резервную ноду. Вся информация на резервной ноде перезаписывается;
- Синхронизация данных происходит автоматически в фоновом режиме;
- Автоматические бекапы отключены на резервной ноде. Все бекапы с активной ноды передаются на резервную в момент обмена данными и заменяют те бекапы, которые там присутствовали ранее.

Внимание: Для корректной работы кластера необходимо постоянное наличие связи между нодами. Для моментального переключения ноды следует соединять прямым линком, не используя мост или коммутатор.

Обмен данными между нодами кластера происходит раз в три минуты. Все несинхронизированные пользовательские изменения настроек и бекапы **могут быть потеряны, если с момента внесения изменений на активной ноде до переключения нод не было обмена данными**.

20.4.2 Особенности работы кластера

Особенности работы кластера с синхронизацией сессий:

- При переключении на резервную ноду изменения с активной ноды применяются к etcd, бекапам, ClickHouse на резервной ноде. Изменения не применяются к логам journald и мониторинга, а также аппаратным данным;
- Время переключения нод - 15 сек. В 18 версии при пропадании линка между нодами переключение происходит моментально;
- При переключении происходит синхронизация данных приложений с активной ноды на резервную;
- При отключении линка локальной/внешней сети активная нода становится резервной, резервная становится активной.
- При отключении линка локальной/внешней сети активной становится нода, у которой больше активных линков. Резервной - нода, у которой меньше активных линков.
- При одинаковом количестве отключенных линков на обеих нодах активной становится нода, у которой было меньше всего деградации сети (разрывов). Резервной - нода, у которой было больше всего разрывов.
- При одинаковом количестве отключенных/включенных линков на обеих нодах и одинаковом количестве разрывов сети активной становится нода, у которой больше uptime (запущена раньше). Резервной - нода, у которой uptime меньше (запущена позднее).

Особенности работы кластера без синхронизации сессий:

- При переключении на резервную ноду синхронизируются все данные с диска активной ноды (синхронизация осуществляется за счет копирования файлов в файловой системе);
- Время переключения нод - 15 сек + загрузка резервной ноды;
- При переключении нод не синхронизируются логи мониторинга и journald, а также аппаратные данные.

Особенности работы с бекапами при кластеризации:

Невозможно полное восстановление из бекапов. При этом можно создать резервную копию и после разрушения кластера восстановить на нее ноду, которая была активной.

20.4.3 Возможные проблемы при работе двух Ideco NGFW в кластере

- Почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено;
- Два NGFW с разными версиями не синхронизируются;
- При обновлении Ideco NGFW в кластере сначала обновится активная нода, затем резервная нода с младшей версией принудительно станет активной для обновления до версии активной ноды.
- При различных размерах жестких дисков могут возникнуть проблемы синхронизации из-за нехватки места;
- Если у провайдера имеется привязка по MAC-адресу, то при переключении нод будет отсутствовать доступ в интернет;
- Если с момента создания бекапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения этот бекап будет потерян;
- Если с момента мгновенного восстановления из бекапа на активной ноде до переключения нод не было синхронизации данных между нодами, после переключения вторая нода окажется в состоянии до восстановления.

Внимание: Не рекомендуем создавать VCE на нодах кластера. Если в кластере на одной из нод был создан *VCE*, со второй нодой будут синхронизироваться только данные таблицы раздела **Управление сервером -> VCE**. После переключения на пассивной ноде будет создан VCE с тем же именем и комментарием, но внутренние настройки созданных на первой ноде VCE (администраторы, сетевые интерфейсы, политики безопасности и т. д.) не перенесутся.

20.4.4 Настройка кластера

Если на момент создания кластера у вас уже есть настроенный Ideco NGFW, рекомендуем выбрать его в качестве активной ноды. Все настройки резервной ноды в процессе создания кластера будут удалены.

Требования

Для создания кластера необходимо соблюдение следующих требований:

- В кластере может быть только две ноды Ideco NGFW;
- Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки;
- Количество **используемых** физических сетевых карт на обоих серверах должно совпадать. В ином случае создать кластер нельзя. При этом само наличие дополнительных физических сетевых карт на нодах на создание кластера никак не влияет;
- Сетевые карты для использования в кластере желательно соединять напрямую, т.к. на основе линка происходит ускоренное переключение нод, поэтому не рекомендуется использовать коммутаторы для кластерной сети. Как минимум сеть должна быть изолирована;
- Не рекомендуется объединять в кластер георасределенные ноды;
- При работе NGFW на гипервизорах используйте средства отказоустойчивости гипервизора.

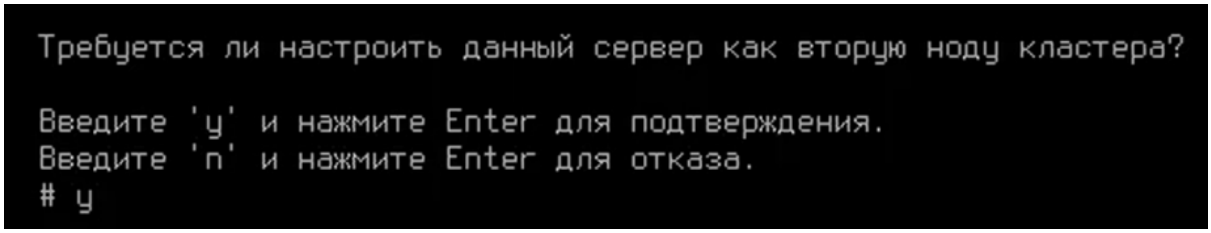
Предупреждение:

- Интерфейсы для создания кластерной сети на каждом Ideco NGFW должны быть в одном сегменте локальной сети, в котором нет других устройств. Не используйте в качестве кластерной сети общедоступную сеть, используемую для передачи стороннего трафика. Обмен данными между нодами не защищен от подмены и прослушивания.
- При настройке кластеризации с использованием гипервизора убедитесь, что сетевая карта, предназначенная для связи между нодами, подключена к изолированной IPv6 сети.
- Запрещено добавлять сетевые интерфейсы, но РАЗРЕШЕНО отключать и редактировать. Удаление сетевого интерфейса, использующегося для связи между нодами, разрушит кластер.

Шаг 1 - Конфигурация резервной ноды

Если только установили сервер Ideco NGFW:

1. При входе в локальное меню резервной ноды, увидев следующее сообщение, введите **y** и нажмите **Enter**:



2. Выберите сетевую карту:

```
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
```

3. Подтвердите создание кластера, введя **y** и нажав **Enter**:

```
Выбрана сетевая карта '52:54:00:e7:e9:06'.
Создание кластера начнётся после подтверждения.

Пожалуйста подтвердите ваш выбор.

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

4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *Изменить название сервера?*, появится надпись с предложением ввести новое название.
Допустимое количество символов в названии - от 2 до 62:

```
Текущее название сервера: UTM-a7c874c8-bdc8-4547-83a4-cdec6de7032a.

Изменить название сервера?

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

После ввода нового названия нажмите **Enter** для продолжения.

5. Появится сообщение, что процесс создания кластера запущен:

```
Процесс создания кластера запущен.
Зайдите в web-интерфейс первой ноды и запустите настройку кластера.
Для этого выделяется 3600 секунд. После того, как настройка кластера на
первой ноде будет завершена, данная нода будет перезагружена автоматически.
Для отмены процесса создания кластера нажмите Ctrl+C.

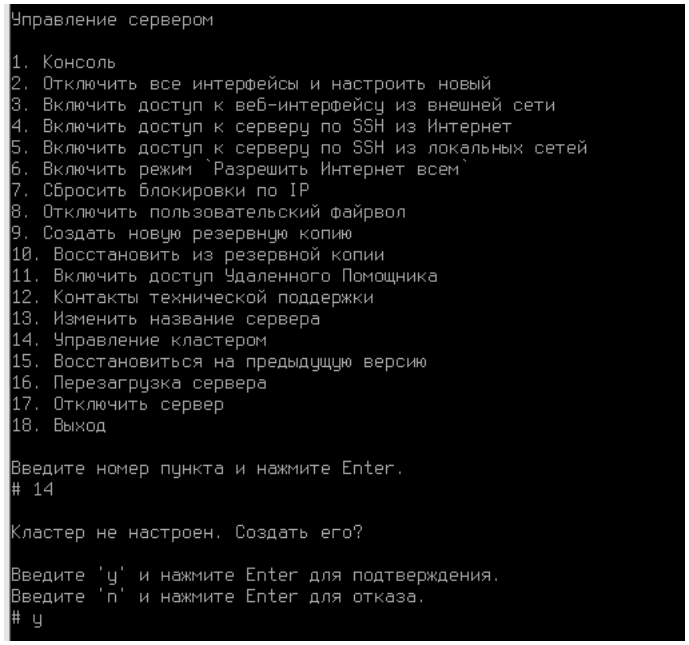
Ожидание завершения настройки кластера, 3599 секунд до отмены.
```

Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Если создаете резервную ноду из уже установленного сервера Ideco NGFW с лицензией и доступом в интернет:

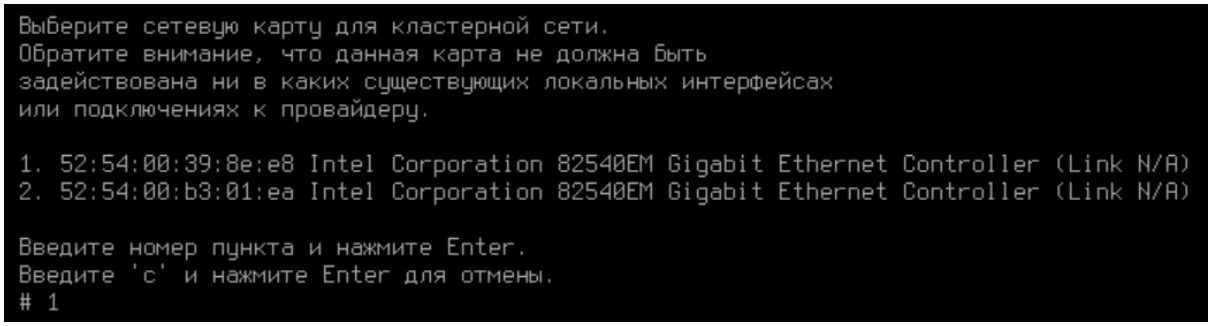
1. Перейдите в локальное меню;

2. Выберите пункт **Управление кластером**. Подтвердите создание кластера, введя **y** и нажав **Enter**:

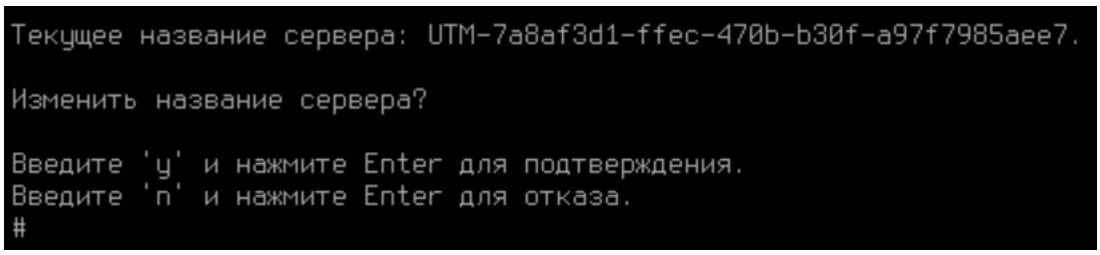


Если на ноде нет свободных сетевых карт, создание кластера будет недоступно.
Если кластер на ноде уже настроен, при выборе пункта *Управление кластером* будет доступно только его разрушение.

3. Выберите свободную физическую сетевую карту для создания кластерной сети и подтвердите выбор:



4. NGFW предложит изменить название сервера. При положительном ответе на вопрос *«Изменить название сервера?»* появится надпись с предложением ввести новое название.
Допустимое количество символов в названии - от 2 до 42:



После ввода нового названия нажмите **Enter** для продолжения.

5. Появится сообщение, что процесс создания кластера запущен:

```
Процесс создания кластера запущен.
Зайдите в web-интерфейс первой ноды и запустите настройку кластера.
Для этого выделяется 3600 секунд. После того, как настройка кластера на
первой ноде будет завершена, данная нода будет перезагружена автоматически.
Для отмены процесса создания кластера нажмите Ctrl+C.

Ожидание завершения настройки кластера, 3599 секунд до отмены.
```

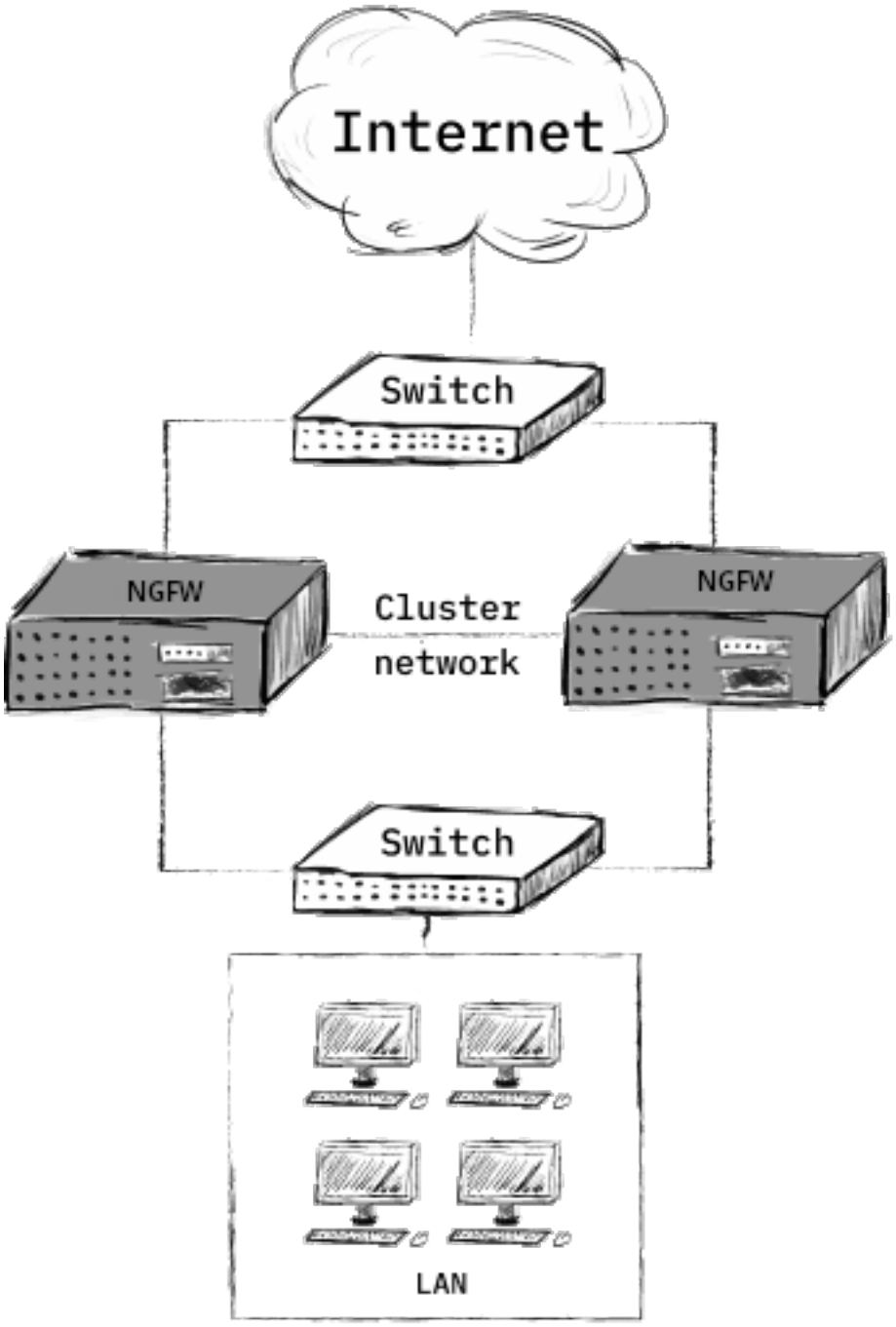
Необходимо зайти в веб-интерфейс активной ноды и выполнить настройки (см. пункт *Конфигурация активной ноды*). Для этого выделяется 3600 секунд.

Шаг 2 - Конфигурация активной ноды

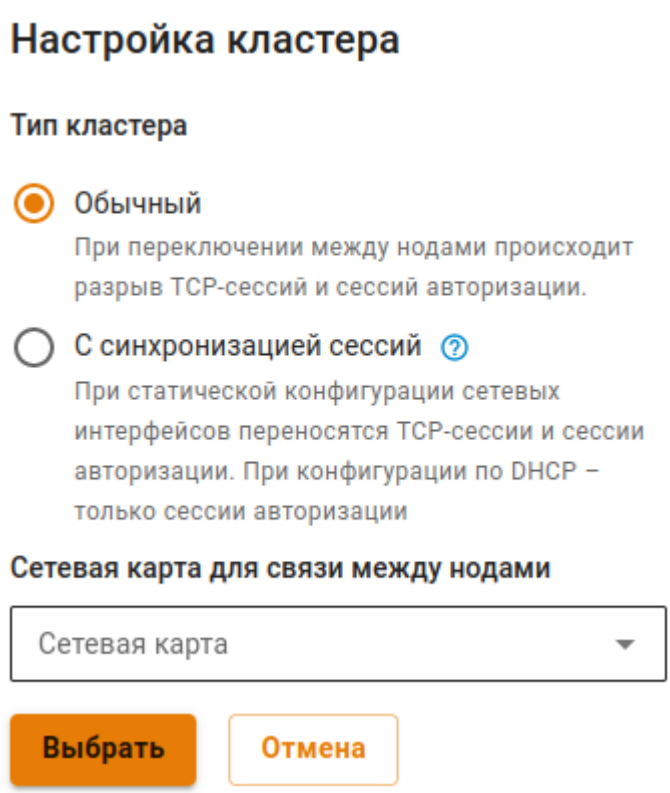
Для конфигурации активной ноды в веб-интерфейсе Ideco NGFW выполните следующие действия:

1. Перейдите в раздел **Управление сервером -> Кластеризация** и нажмите кнопку **Настроить кластер отказоустойчивости**.

2. Подтвердите, что топология сети соответствует схеме:



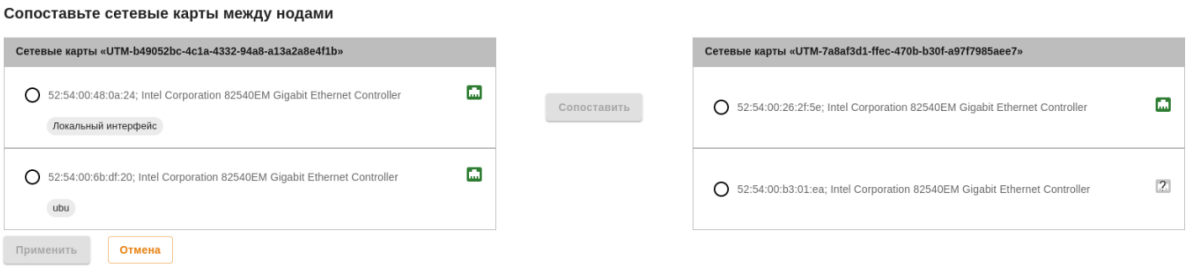
3. Выберите тип кластера и сетевую карту для соединения между нодами:



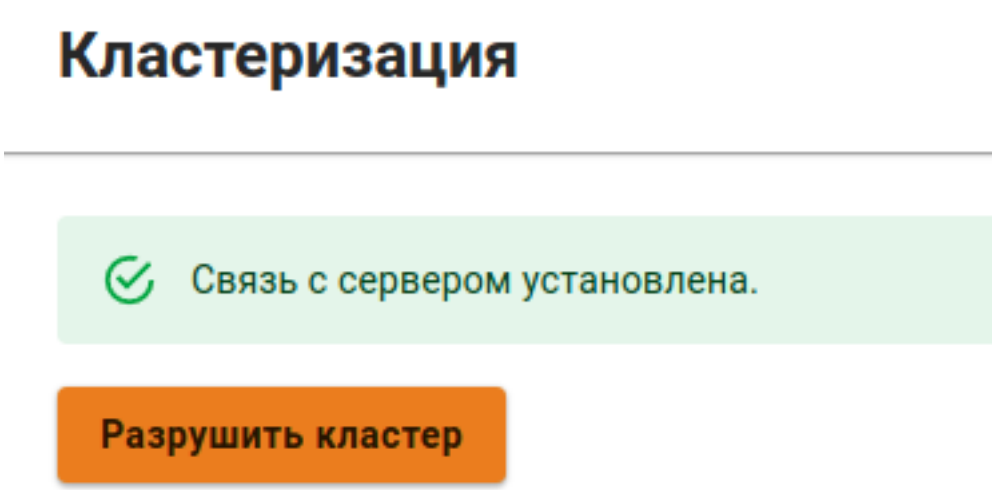
Подсказка: Если был настроен **Обычный** тип кластера, то при переключении между нодами происходит разрыв TCP-сессий пользователей и сессий авторизации.

Если был настроен тип кластера **С синхронизацией сессий**, то при статической конфигурации сетевых интерфейсов все TCP-сессии пользователей и сессии авторизации перенесутся на резервную ноду. При конфигурации по DHCP - перенесутся только сессии авторизации.

4. Сопоставьте сетевые карты. Для этого выберите в каждом столбце по одной сетевой карте и нажмите **Сопоставить**:



5. После применения настроек резервная нода перезагрузится, и в веб-интерфейсе активной ноды отобразится информация о том, что связь с сервером установлена.



Предупреждение: Локальное меню резервной ноды недоступно в NGFW, начиная с версии 16.0.

Изменение названия кластера

Изменить название кластера можно в веб-интерфейсе активной ноды, нажав на кнопку **Редактировать** рядом с названием кластера в левом верхнем углу экрана:

После ввода нового названия нажмите ✓.

Изменение названия сервера

Изменить название сервера можно у активной ноды из веб-интерфейса, нажав кнопку **Редактировать** рядом с названием сервера в левом верхнем углу экрана:

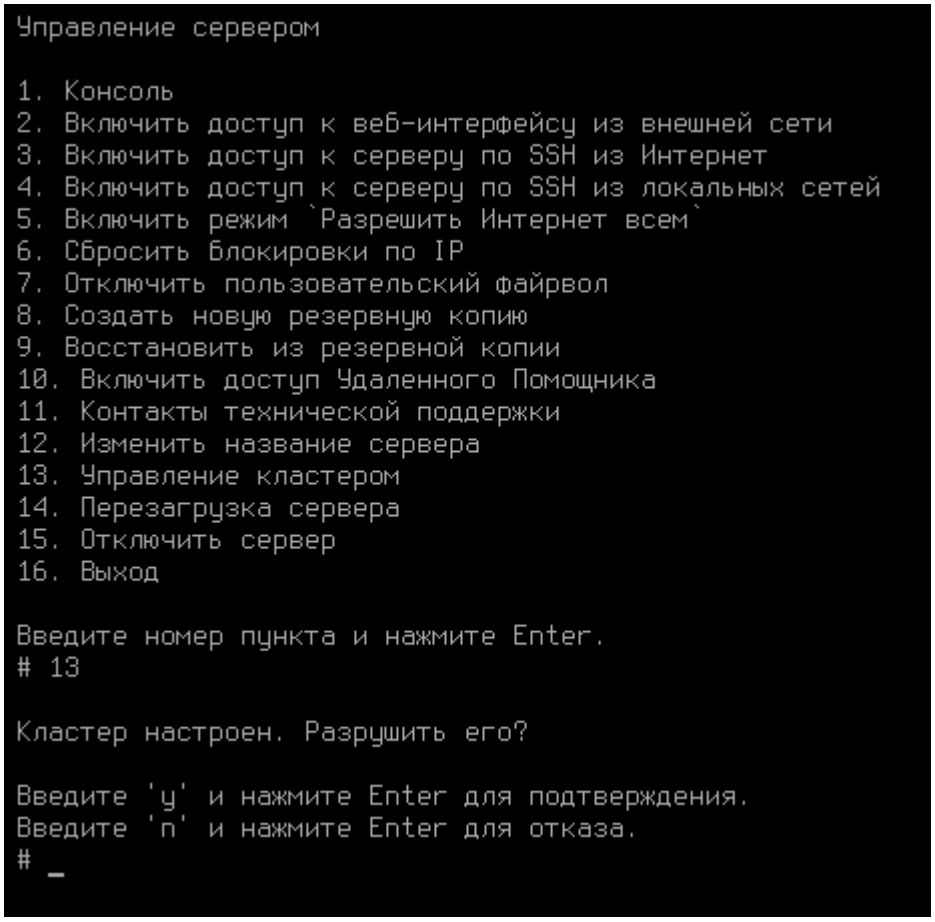
После ввода нового названия нажмите ✓.

Разрушение кластера

Разрушить кластер можно только из локального меню или веб-интерфейса *активной* ноды. При этом она продолжит работать, а вторая нода (резервная) сбросит настройки до состояния только что установленного Ideco NGFW.

Разрушение кластера из локального меню:

1. Выберите пункт локального меню **Управление кластером**, введите **y** и нажмите **Enter**;

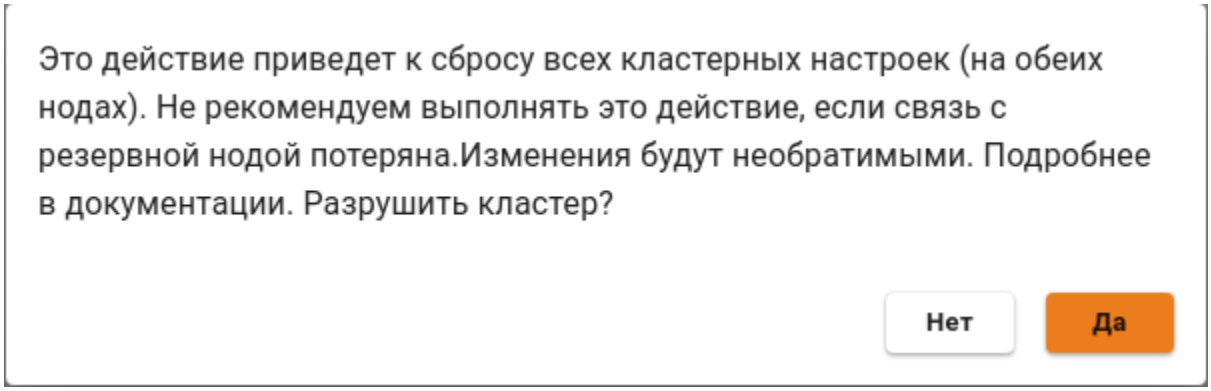


2. Подтвердите выбор.

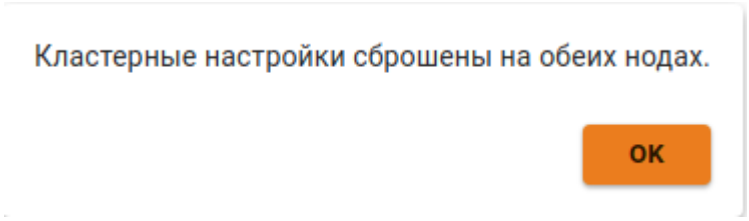
Разрушение кластера из веб-интерфейса:

1. Перейдите в раздел **Управление сервером -> Кластеризация** и нажмите кнопку **Разрушить кластер**.

2. Появится окно с предупреждением:



3. Нажмите **ОК**:



Процедура обновления нод

Чтобы обновить NGFW до последней версии в режиме кластера, выполните действия:

1. Запустите обновление активной ноды - в разделе **Управление сервером -> Автоматическое обновление** нажмите соответствующую кнопку. В процессе обновления произойдет перезагрузка ноды. Резервная нода станет активной, переведя текущие задачи обработки трафика на себя.
Обмен данными между нодами будет остановлен, как только первая нода обновилась и перезагрузилась. Для синхронизации оба устройства должны иметь одну версию системы, идентичную вплоть до номера сборки.

2. Дождитесь, когда активная нода скачает обновление, и запустите его. После завершения обновления кластер вновь будет работоспособен.

Подсказка: Обновление активной ноды кластера будет заблокировано, если она не синхронизирована с резервной нодой или с момента последней синхронизации прошло более 30 минут. В случае блокировки обновлений произойдет переключение нод кластера. Нода с младшей версией сможет обновиться без синхронизации.

20.5 Обновления

Подсказка: Название службы раздела **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.
>
> Можно отключить автоматическое обновление Ideco NGFW.

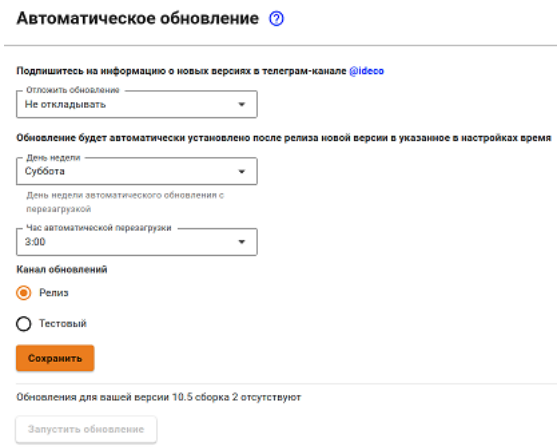
- Поле **Отложить обновления** - время, на которое будет отложено обновление (максимальный срок 6 месяцев с даты релиза последней версии, до которой доступно обновление);
- Поле **День недели** - день недели запуска автоматического обновления;
- Поле **Час автоматической перезагрузки** - позволяет выбрать 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.

20.5.1 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.

20.5.2 Особенности обновления NGFW

Обновление будет автоматически установлено в указанное в настройках время после релиза новой версии.

Обновления можно отложить на срок до шести месяцев или навсегда. Если отложить обновление на определенный срок, то период будет отсчитываться от **даты релиза** последнего доступного обновления и корректироваться в соответствии с указанным для обновления днем недели.

Даты релизов можно посмотреть на сайте или в документации в разделе Changelog.

Номер мажорной версии NGFW - часть номера до точки (например, 14.x), номер минорной версии - часть после точки (например, x.7).

Автоматическое обновление Ideco NGFW на следующую мажорную версию возможно только после обновления до последней выпущенной в релиз минорной версии. Например, UTM 14.2 можно обновить до версии 14.10, а затем - до версии 15.7.

Предупреждение: Если обновление было отложено на шесть месяцев, но за это время вышел новый минорный релиз, дата обновления сдвигается. Шесть месяцев теперь отсчитываются с даты выхода последнего доступного минорного релиза.

20.6 Бекапы

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

Подсказка: Название служб раздела **Бекапы**: `ideco-backup-backend`; `ideco-backup-create`; `ideco-backup-restore`; `ideco-backup-rotate`.
Список служб для других разделов доступен по *ссылке*.

В NGFW создается только полный бекап, который включают в себя все настройки, созданные администратором в веб-интерфейсе.

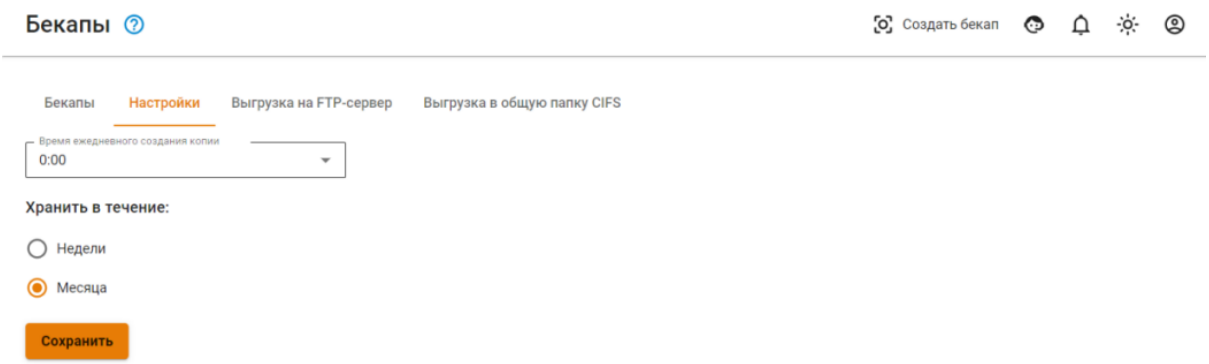
Бекапы не включают в себя:

- Журнал событий;
- Почту;
- Статистику web-трафика и другие отчеты;
- Любые кешируемые данные; базы антивирусов, правила IPS и т. п.;
- Настройки созданных *VCE*;
- Любые данные, генерируемые в процессе работы системы автоматически.

В NGFW бекап создается как автоматически, так и вручную.

20.6.1 Автоматическое создание бекапа

Для настройки автоматического бекапа перейдите в раздел **Управление сервером -> Бекапы -> Настройки**:



Установите время ежедневного создания и продолжительность хранения бекапа на локальном жестком диске. При настройке выгрузки на сетевое файловое хранилище автоматический бекап будет также дублироваться туда.

- **Время ежедневного создания копии** - укажите в настройках час (рекомендуется выбирать ночное время для создания бекапа);
- **Хранить в течение** - хранить бекапы на локальном жестком диске можно в течение недели или месяца.

Подсказка: Рекомендуется хранить бекапы не только на локальном жестком диске, но и на внешних носителях. NGFW предоставляет возможность выгружать бекапы:

- на сетевое файловое хранилище по протоколу FTP;
- на сетевое файловое хранилище по протоколу NetBIOS (CIFS);

- на ПК через кнопку **Скачать** в таблице бекапов ( ) для переноса с сервера на иной внешний носитель вручную.

Бекапы на удаленное файловое хранилище по протоколу FTP

Ключевые параметры, необходимые для настройки бекапа на FTP-сервер, описаны в таблице:

Параметр	Описание
Адрес сервера	IP-адрес удаленного FTP-сервера, на котором будут размещаться бекапы
Логин	Имя пользователя для авторизации на FTP-сервере
Пароль	Пароль для авторизации на FTP-сервере
Путь к каталогу	Каталог, в который будут записываться бекапы

Бекапы на сетевое файловое хранилище по протоколу NetBIOS (CIFS)

Ключевые параметры, необходимые для настройки бекапа на NetBIOS-сервер, описаны в таблице.

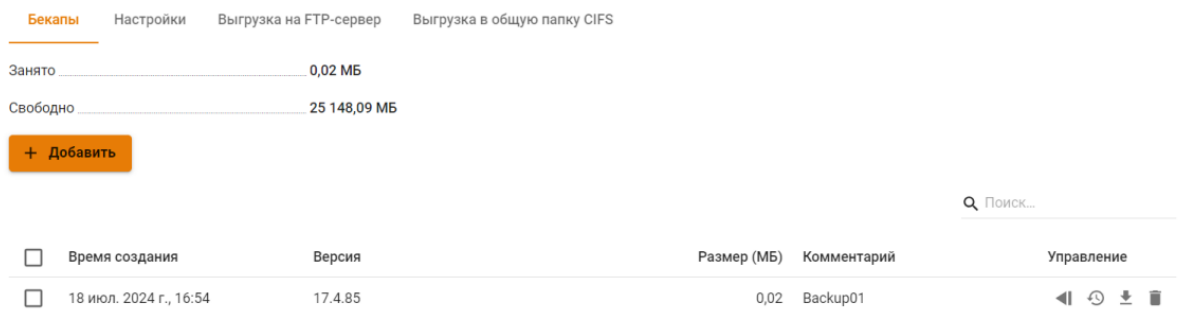
Параметр	Описание
Адрес сервера	IP-адрес удаленного NetBIOS-сервера, на котором будут размещаться бекапы
Логин	Имя пользователя для авторизации на сетевом ресурсе Windows
Пароль	Пароль для авторизации на сетевом ресурсе Windows
Путь к каталогу	Каталог, в который будут записываться бекапы

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

20.6.2 Ручное создание бекапа

Через веб-интерфейс

Для создания бекапа через интерфейс Ideco NGFW перейдите в **Управление сервером -> Бекапы -> Бекапы** и нажмите **Добавить -> Создать**. Введите комментарий и нажмите **Добавить** или нажмите **Создать бекап** в правом верхнем углу веб-интерфейса. Новый бекап появится в таблице:



Через локальное меню

Чтобы создать новый бекап через локальное меню Ideco NGFW, выполните действия:

1. Выберите пункт **9** и нажмите **Enter**.

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

Пример создания бекапа через локальное меню приведен на скриншоте ниже:

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

Введите номер пункта и нажмите Enter.
# 9

Введите комментарий для бекапа и нажмите Enter.

Введите 'c' и нажмите Enter для отмены.
# Copy1
Создание бекапа, пожалуйста подождите...
Бекап создан успешно.
```

Подсказка: Настройка сохранения бекапа в сетевом файловом хранилище возможна только через веб-интерфейс Ideco NGFW. Выгрузка на внешние сетевые хранилища производится только при автоматическом создании бекапа.

20.6.3 Восстановление конфигурации из бекапа

В NGFW восстановление из бекапа возможно полное и мгновенное.

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

При выполнении мгновенного восстановления бекап применяется без перезагрузки. При этом не сохраняются:

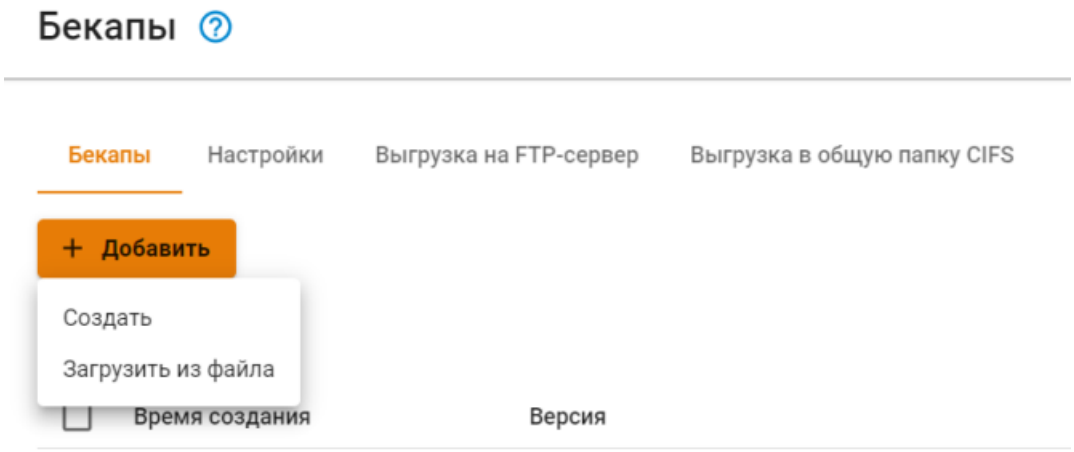
- Пользователи (с версии 17.5 восстановление пользователей доступно);
- Счетчики квот;
- Журнал событий.

Подсказка: Мгновенное восстановление возможно только для бекапа версии, полностью совпадающей с установленной на сервере. :::

Через веб-интерфейс

Перейдите в раздел **Управление сервером -> Бекапы -> Бекапы** и нажмите кнопку **Полное восстановление** ( ) или **Мгновенное восстановление** ( ) в столбце **Управление**.

Также можно загрузить бекап из файла. Например, в случае переноса с другого сервера. Для восстановления конфигураций бекапа, который находится на внешнем носителе, перейдите на **Управление сервером -> Бекапы -> вкладка Бекапы**, нажмите на кнопку **Добавить** и выберите **Загрузить из файла**:



Через локальное меню

Перейдите в локальное меню и выполните действия:

1. Выберите пункт:

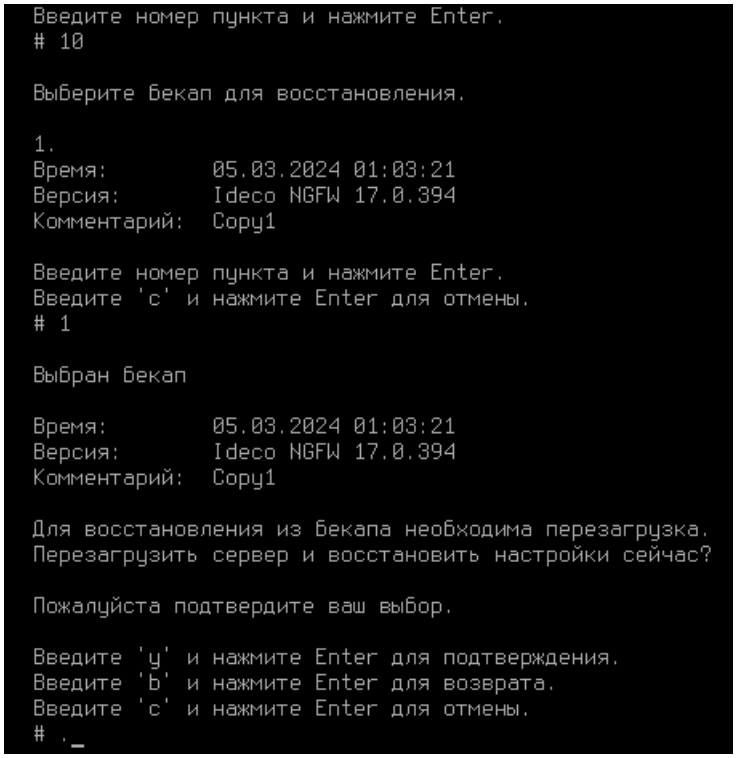
   - **10** - восстановятся все настройки и перезагрузится сервер;
   - **11** - восстановятся все настройки без перезагрузки сервера, кроме использованного трафика по квотам, изменений в списке пользователей и отчетах.

     Нажмите **Enter**.

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

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

Пример восстановления из бекапа через локальное меню:



Подсказка: Чтобы перенести установленный Ideco NGFW с одного сервера на другой с сохранением всех настроек, воспользуйтесь статьей *Перенос данных и настроек на другой сервер*.

Предупреждение: Если на Ideco NGFW настроен кластер, то перед работой с бекапами нужно ознакомиться с особенностями работы бекапов:

- Невозможно полное восстановление из бекапов. При этом можно создать резервную копию и после разрушения кластера восстановить копию на ноде, которая была активной;
- На активной ноде доступно **Мгновенное восстановление из бэкапа**. Восстанавливаются все настройки, кроме использованного трафика по квотам, изменений в списке пользователей и отчетах. Данные на второй ноде также придут в соответствие с восстановленными настройками после синхронизации нод.

20.7 Терминал

Предупреждение: Используйте терминал только для диагностики. Воздержитесь от команд, изменяющих файлы. Система рассчитана на настройку только через веб-интерфейс. Компания «Айдеко» не несет ответственности за негативные последствия работы с Ideco NGFW из терминала. Техническая поддержка вправе отказать в обслуживании, если окажется, что работа системы была нарушена из-за действий пользователя в терминале.

20.7.1 Основные команды

- **Утилиты сетевой диагностики:** `ping`, `host`, `nslookup`, `tracepath`, `tcpdump`, `arping`, `ss` (аналог `netstat`);
- **Файловый редактор:** `nano`;
- **Просмотр логов:** `journalctl -u <название службы>` (например, `journalctl -u ideco-routing-backend`);
- **Проверка скорости интернета:** `speedtest-cli`;
- **Просмотр ARP-таблицы:** `ip neigh show`;
- **Разблокировка в случае срабатывания защиты от брутфорс-атак:**
  - `fail2ban-client unban --all` - команда используется для снятия всех блокировок;
  - `fail2ban-client unban <IP-адрес>` - команда используется для разблокировки конкретного IP-адреса. Укажите нужный IP-адрес в качестве аргумента.
- **Просмотр конфигурации FRR:** `vtysh`.

20.7.2 Таблица служб

Раздел	Имя службы
Файрвол	ideco-nflog;ideco-firewall-backend
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
Бэкапы	ideco-backup-backend; ideco-backup-create; ideco-backup-restore; ideco-backup-rotate
Лицензия	ideco-license-backend
VPN-подключения	ideco-accel-l2tp; ideco-accel-pptp; ideco-accel-sstp; ideco-vpn-servers-backend; ideco-vpn-authd
Авторизация	ideco-auth-backend
Веб-аутентификация, Двухфакторная аутентификация	ideco-web-authd
Active Directory	ideco-ad-backend; ideco-ad-log-collector@<имя домена>

continues on next page

Таблица 1 – продолжение с предыдущей страницы

Раздел	Имя службы
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

20.7.3 Примеры использования утилит

Примеры использования утилиты vtysh

Просмотр таблицы маршрутизации:

1. Перейдите в раздел **Управление сервером -> Терминал**.
2. Введите в терминале:

```
vtysh
```

3. Для просмотра таблицы маршрутизации введите:

```
show ip route
```

Пример вывода утилиты:

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 1.1.1.1/32 [1/0] via 10.10.10.1, Leth1, weight 1, 00:02:32
O   10.10.10.0/24 [110/1] is directly connected, Leth1, weight 1, 00:02:28
C>* 10.10.10.0/24 is directly connected, Leth1, 00:02:33
C>* 10.11.12.0/25 is directly connected, Eeth2, 00:02:33
O>* 10.20.40.0/24 [110/21] via 10.10.10.201, Leth1, weight 1, 00:02:18
S>* 10.128.0.0/16 [1/0] is directly connected, Lvpn0, weight 1, 00:02:32
C>* 169.254.1.0/29 is directly connected, lb_local_in, 00:02:33
C>* 169.254.1.0/29 is directly connected, lb_local_out, 00:02:33
C>* 169.254.1.4/32 is directly connected, Lvpn0, 00:02:33
C>* 169.254.254.254/32 is directly connected, lo, 00:02:33
```

Полезная информация:

- Не все маршруты могут быть выгружены в ядро, поэтому при просмотре таблицы маршрутизации без утилиты `vtsyh` некоторые маршруты могут не отображаться.

Просмотр конфигурации FRR:

1. Перейдите в раздел **Управление сервером -> Терминал**.
2. Введите в терминале:

```
vtysh
```

3. Для просмотра конфигурации введите:

```
show running-config
```

Пример вывода утилиты:

```
Building configuration...

Current configuration:
!
frr version 8.5.3
frr defaults traditional
hostname bez-nazvaniya-23000007-c6d8-01c2-a572-d68497c66441
no ipv6 forwarding
service integrated-vtysh-config
!
ip route 10.128.0.0/16 Lvpn0
!
interface Leth1
 ip ospf cost 125
exit
!
interface lo
 ip ospf passive
exit
!
router ospf
 ospf router-id 192.168.0.200
 redistribute connected
 redistribute static
 network 172.16.10.0/24 area 0.0.0.200
 default-information originate always
exit
!
ip prefix-list DEFAULT seq 5 deny 0.0.0.0/0
ip prefix-list DEFAULT seq 10 permit 0.0.0.0/0 le 32
!
route-map DEFMAP permit 10
 match ip address prefix-list DEFAULT
exit
!
ip protocol ospf route-map DEFMAP
!
end
```

Просмотр OSPF соседства:

1. Перейдите в раздел **Управление сервером -> Терминал**.
2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей OSPF введите:

```
show ip ospf neighbor
```

Пример вывода утилиты:

```
Neighbor ID     Pri State           Up Time         Dead Time Address         ␣
↪Interface                         RXmtL RqstL DBsmL
```

(continues on next page)

(продолжение с предыдущей страницы)

```
10.10.10.201       1 Full/DR         6m35s              34.709s 10.10.10.201    ␣
↪Leth1:10.10.10.126                    0     0     0
```

Просмотр BGP соседства:

1. Перейдите в раздел **Управление сервером -> Терминал**.
2. Введите в терминале:

```
vtysh
```

3. Для просмотра соседей BGP введите:

```
show ip bgp neighbors
```

Пример вывода утилиты:

```
BGP neighbor is 10.10.10.2, remote AS 123, local AS 123, internal link
  Local Role: undefined
  Remote Role: undefined
 Member of peer-group V4_AS123_10_10_10_2 for session parameters
  BGP version 4, remote router ID 10.11.12.2, local router ID 10.11.12.71
  BGP state = Established, up for 00:00:10
  Last read 00:00:10, Last write 00:00:09
  Hold time is 180 seconds, keepalive interval is 60 seconds
  Configured hold time is 180 seconds, keepalive interval is 60 seconds
  Configured conditional advertisements interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Extended Message: advertised
    AddPath:
      IPv4 Unicast: RX advertised
    Long-lived Graceful Restart: advertised
    Route refresh: advertised and received(new)
    Enhanced Route Refresh: advertised
    Address Family IPv4 Unicast: advertised and received
    Hostname Capability: advertised (name: bez-nazvaniya-5f3323c3-6462-4981-b8a0-
↪2b4397e3448a,domain name: n/a) not received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 0 seconds
      Address families by peer:
        none
  Graceful restart information:
    End-of-RIB send: IPv4 Unicast
    End-of-RIB received:
    Local GR Mode: Helper*

    Remote GR Mode: Helper

    R bit: False
    N bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
    IPv4 Unicast:
      F bit: False
      End-of-RIB sent: Yes
      End-of-RIB sent after update: Yes
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      End-of-RIB received: No
      Timers:
        Configured Stale Path Time(sec): 360
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          3
    Keepalives:             1          2
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  3          6
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  V4_AS123_10_10_10_2 peer-group member
  Update group 1, subgroup 1
  Packet Queue length 0
  NEXT_HOP is always this router
  Community attribute sent to this neighbor(all)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *IMPORT_V4_AS123_10_10_10_2
  Route map for outgoing advertisements is *EXPORT_V4_AS123_10_10_10_2
  12 accepted prefixes

  Connections established 1; dropped 0
  Last reset 00:05:26,  No AFI/SAFI activated for peer
  Internal BGP neighbor may be up to 255 hops away.
Local host: 10.10.10.126, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 38445
Nexthop: 10.10.10.126
Nexthop global: ::
Nexthop local: ::
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Estimated round trip time: 1 ms
Read thread: on  Write thread: on  FD used: 25
```

20.8 Лицензия

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

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

Подсказка: Подробнее о видах лицензий в статье *Лицензирование*.

Доступные действия для управления лицензиями:

- регистрация сервера;
- добавление коммерческой или бесплатной лицензии;
- привязка лицензии к серверу;
- просмотр информации об имеющихся лицензиях;
- офлайн-обновление лицензии и баз модулей фильтрации.

20.8.1 Добавление коммерческой (Enterprise) лицензии

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

2. Перейдите в личный кабинет MY.IDECO в раздел **NGFW -> Лицензирование** и нажмите **Добавить коммерческую лицензию**.

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

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

20.8.2 Добавление FREE (бесплатной) лицензии

Для добавления FREE-лицензии нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Свободные лицензии**.

20.8.3 Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн. Онлайн проводится только в MY.IDECO. Офлайн потребует доступ к веб-интерфейсу сервера.

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:

- На вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ . Далее в открывшемся окне выберите нужную лицензию и сохраните изменения, нажав **Привязать лицензию**.
- На вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

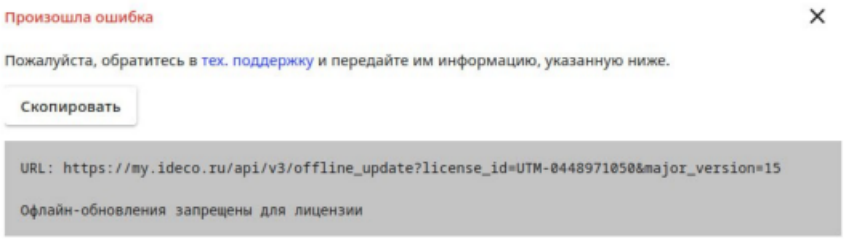
Офлайн-привязка лицензии

1. Для предоставления офлайн-лицензии обратитесь к менеджеру.

2. Привяжите предоставленную лицензию к серверу:

- На вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения, нажав **Привязать лицензию**.
- На вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

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



3. Сформируйте ссылку на скачивание баз и лицензии, перейдите по ней на устройстве с доступом в интернет (подробнее - в *статье*.

Пример ссылки на регистрацию:

```
https://my.ideco.ru/ngfw?offline-updates&version={"major": 17, "minor": 5, "build":␣
↪102, "timestamp": 1724427324, "vendor": "Ideco", "product": "UTM", "kind": "STANDARD
↪", "release_type": "release"}&hwid=sGs6OYW2XRm_aK9PRwifKnej3V8YUVw69dtKVkIoPEnD
```

4. Сохраните файлы лицензии и баз фильтрации, нажав на появившиеся ссылки:



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.

20.8.4 Просмотр информации о лицензиях

Посмотреть информацию о модулях и лицензии можно:

- В личном кабинете *MY.IDECO* в разделе **NGFW -> Лицензирование**, нажав на иконку напротив нужного сервера;
- В веб-интерфейсе Ideco NGFW, в разделе **Управление сервером -> Лицензия**.

Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др.

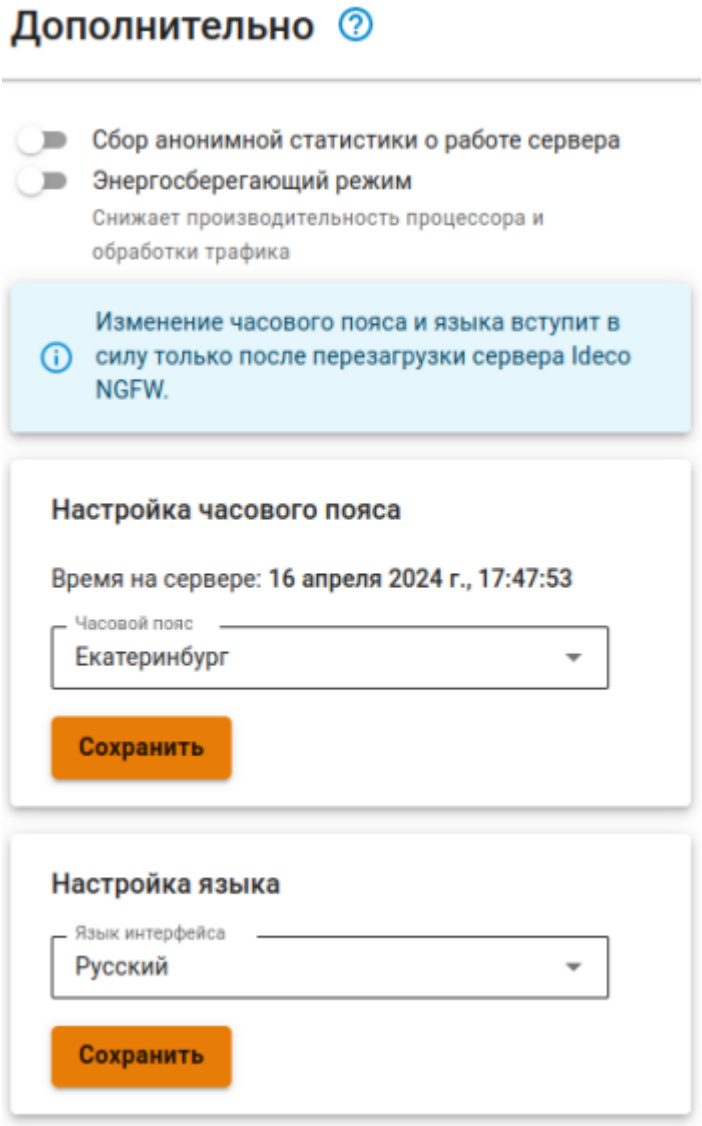
20.9 Дополнительно

20.9.1 Основное

Предупреждение: Изменение часового пояса вступит в силу только после перезагрузки сервера Ideco NGFW.

Подсказка: В интерфейсе *VCE* изменение настроек часового пояса и языка недоступно.

Настройка осуществляется через веб-интерфейс в разделе **Управление сервером -> Дополнительно**.



- **Энергосберегающий режим** - включение этого режима снижает производительность процессора и обработки трафика.
- **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.

21. Почтовый релей

21.1 Основное

Подсказка: Все возможности по фильтрации почтового трафика можно также применить к внутреннему почтовому серверу, опубликовав его через почтовый релей.

Для настройки почтового сервера в веб-интерфейсе Ideco NGFW необходимо перейти в меню **Почтовый релей**. В этом разделе находятся все ключевые параметры, влияющие на работу почтовой службы. Все

настраиваемые параметры разделены по нескольким категориям. Ниже описан каждый раздел почтового сервера.

Если используется почтовый сервер Ideco NGFW как полноценный сервер с хранением почты, обязательным является хранение почты на дополнительном HDD/SSD-диске. Подключите дополнительный жесткий диск к серверу перед использованием почты.

В настройках почтового сервера можно указать максимальный размер почтового ящика и максимальный размер письма. Подробнее в *статье*.

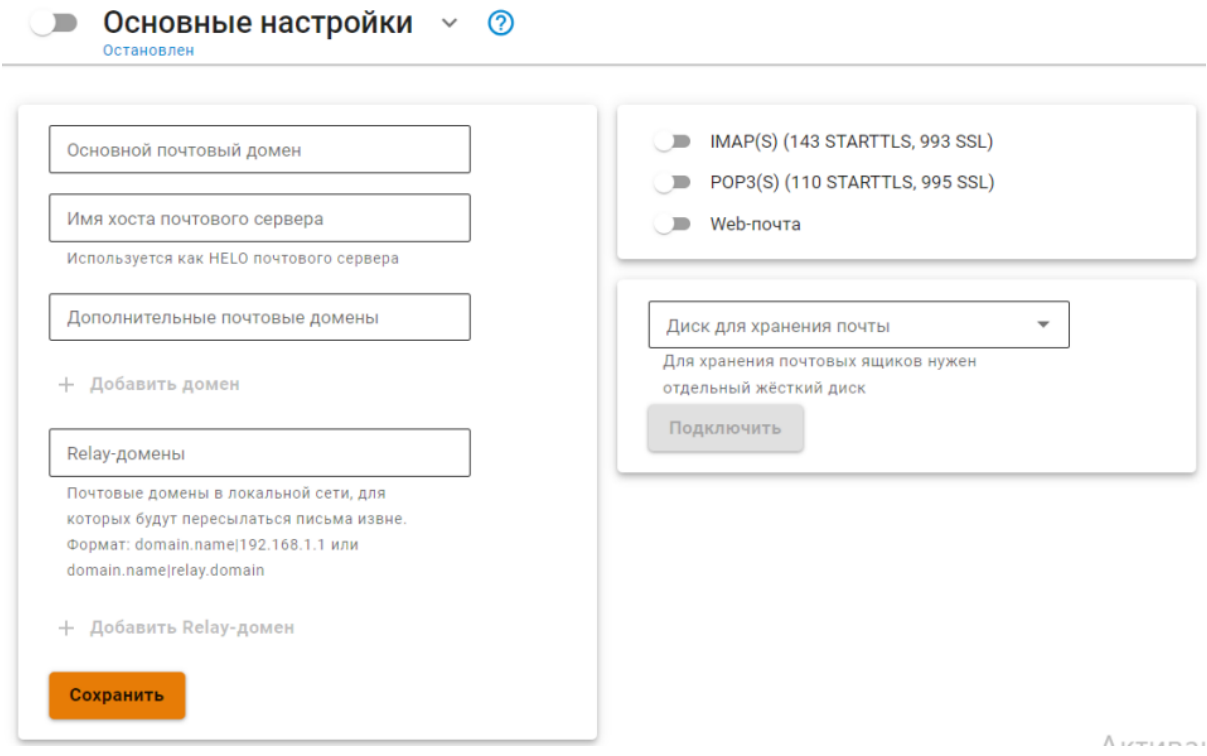
Предупреждение: При настройке *кластера* почта будет доступна для работы только в режиме почтового релея. Хранение почтовых ящиков отключено.

21.2 Основные настройки

21.2.1 Основное

Предупреждение: NGFW не поддерживает кириллические почтовые домены.

В разделе **Основные настройки** представлены базовые параметры, необходимые для настройки почтового сервера, почтового релея и веб-почты.



Ideco NGFW можно настроить, как почтовый сервер, почтовый релей или воспользоваться почтовым клиентом NGFW. В зависимости от необходимой функциональности, следуйте соответствующим инструкциям:

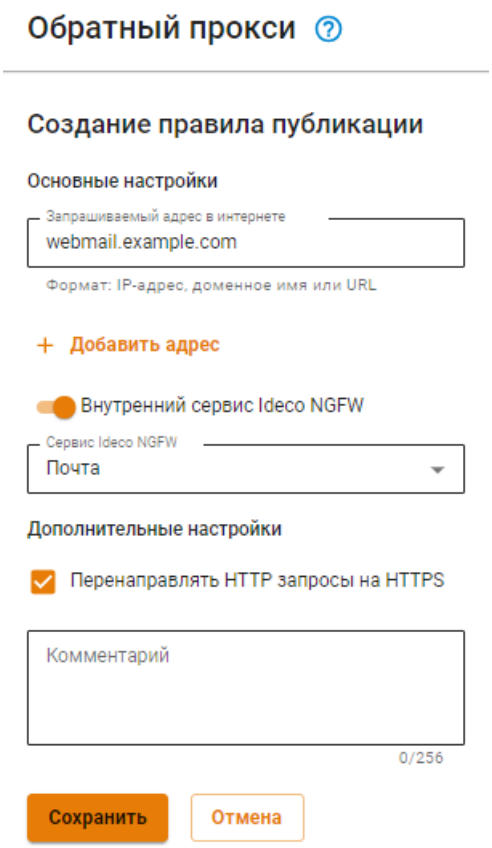
21.2.2 Web-почта

Основное

Подсказка: Перед настройкой веб-почты настройте на Ideco NGFW почтовый сервер.

Для работы веб-почты необходимо активировать опцию **Web-почта** в разделе **Почтовый релей -> Основные настройки** и создать правило публикации в разделе **Сервисы -> Обратный прокси**.

При добавлении правила:



- Включите опцию **Внутренний сервис Ideco NGFW**;
- В качестве сервиса выберите почту;
- В поле **Запрашиваемый адрес в интернете** введите домен, IP-адрес или URL, по которому должна быть доступна веб-почта (например, `webmail.example.com`, `192.168.100.40` или `192.168.100.20/webmail`);
- Нажмите **Сохранить**.

После создания правила из локальной или внешней сети в браузере наберите: `https://<IP-адрес>`, `https://<домен>` или `https://<URL>`.

Предупреждение: Важно:

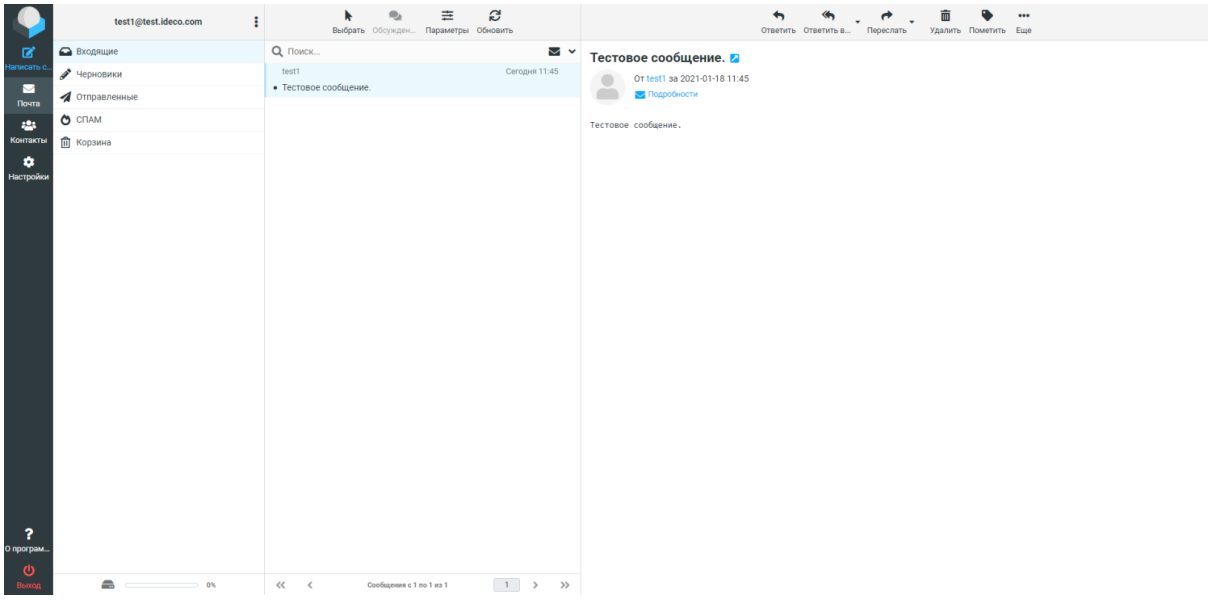
- Чтобы пользователи имели доступ к веб-почте из внешней сети, в правиле публикации в поле **Запрашиваемый адрес в интернете** необходимо указывать белый IP-адрес или зарегистрированный домен.

- Для подключения обязательно использовать HTTPS.
- С 17 версии Ideco NGFW веб-почта не доступна через `IP-адрес_или_домен_веб-интерфейса:8443/webmail`, т. к. не связана с административным веб-интерфейсом NGFW.

- В открывшейся форме входа в почтовый ящик в качестве логина укажите логин от учетной записи пользователя;
- В качестве пароля всегда прописывается пароль от учетной записи пользователя. **Установить отдельный пароль на почту нельзя.**



При успешном входе в браузере откроется веб-интерфейс почтового ящика пользователя:



Веб-интерфейс встроенного почтового клиента работает с почтовым сервером по протоколу IMAP и обладает возможностями:

- Создание и отправка писем. Поддерживается загрузка множественных вложений;
- Просмотр, удаление, перемещение письма. Управление IMAP-папками ящика;
- Персональная (для конкретного ящика) адресная книга, работающая только в рамках веб-приложения;
- Адресная книга поддерживает формат контактов VCARD и может быть экспортирована или сохранена на вашем компьютере;
- Календарь с возможностью создавать события и уведомлять о них сотрудников по почте;
- Цветные метки писем, как это принято в почтовом клиенте Thunderbird. Проставляются клавишами от 1 до 5. Изменения сохраняются на сервере, поэтому в другом почтовом клиенте метки будут видны;
- Расширенный поиск по всем письмам ящика находится в разделе **Еще...** панели инструментов ящика.

21.2.3 Настройка почтового релея

Основное

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

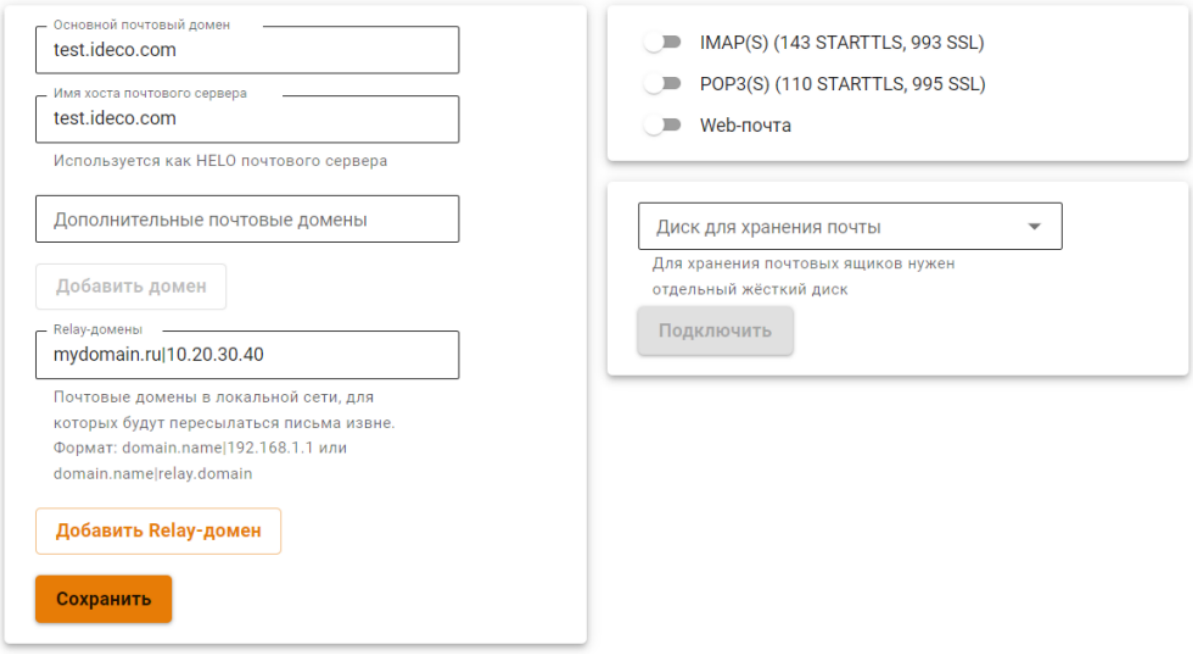
Предупреждение: NGFW не поддерживает кириллические почтовые домены.

Перед настройкой почтового релея убедитесь, что на Ideco NGFW включен почтовый сервер.

Для настройки почтового релея:

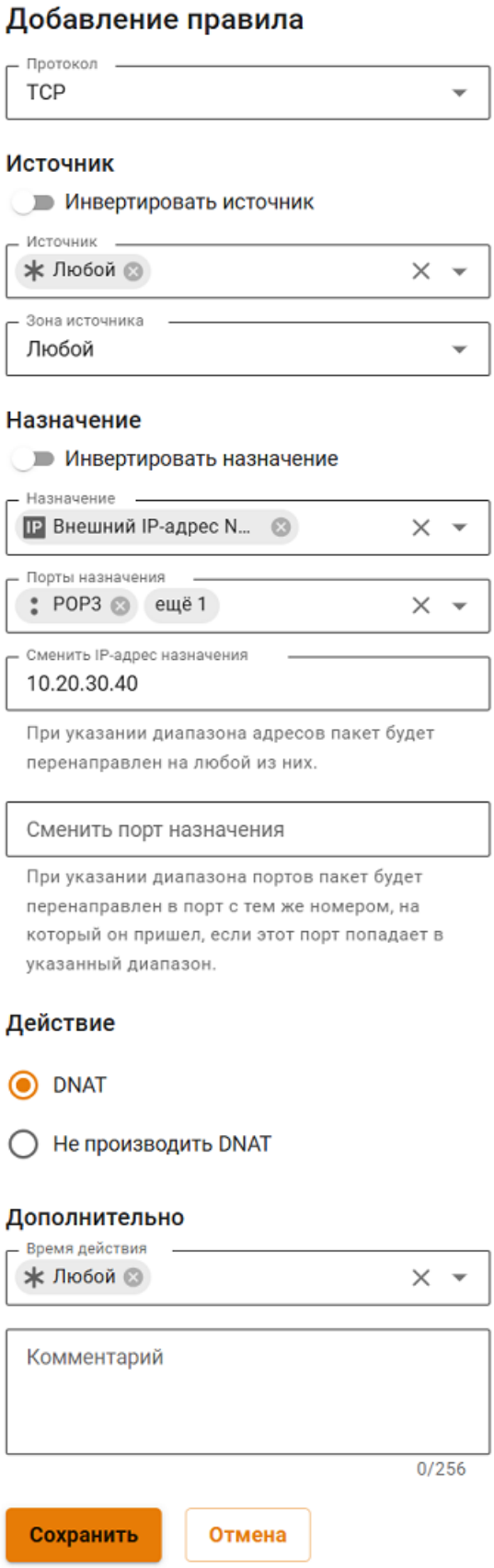
1. Добавьте в поле **Relay-домены** (почтовые домены в локальной сети, для которых будут пересылаться письма извне) запись вида: `mydomain.ru|10.20.30.40`, где:

- `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 (перенаправление портов)** и создайте правило проброса портов POP3(S), IMAP(S) и SMTPS:


Добавление правила
Протокол
TCP
Источник
Инвертировать источник
Источник
Любой
Зона источника
Любой
Назначение
Инвертировать назначение
Назначение
Внешний IP-адрес N...
Порты назначения
POP3
ещё 1
Сменить IP-адрес назначения
10.20.30.40
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

Предупреждение: Не используйте SMTP для настройки почтового релея.

Все почтовые домены должны быть ассоциированы с внешним адресом сервера Ideco NGFW (A- и MX-записи в DNS-зоне).

Работа в режиме открытого почтового релея невозможна, поэтому Ideco NGFW в режиме Relay может принимать почту только в следующих случаях:

- Когда почта адресована исключительно для указанного Relay-домена;
- Из сетей, которые входят в список доверенных в разделе **Расширенные настройки -> Безопасность**.

Вся остальная почта будут отвергнута сервером.

21.2.4 Настройка почтового сервера

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

1. Перейдите в раздел **Почтовый релей -> Основные настройки**, заполните поля **Основной почтовый домен** и **Имя хоста почтового сервера**.

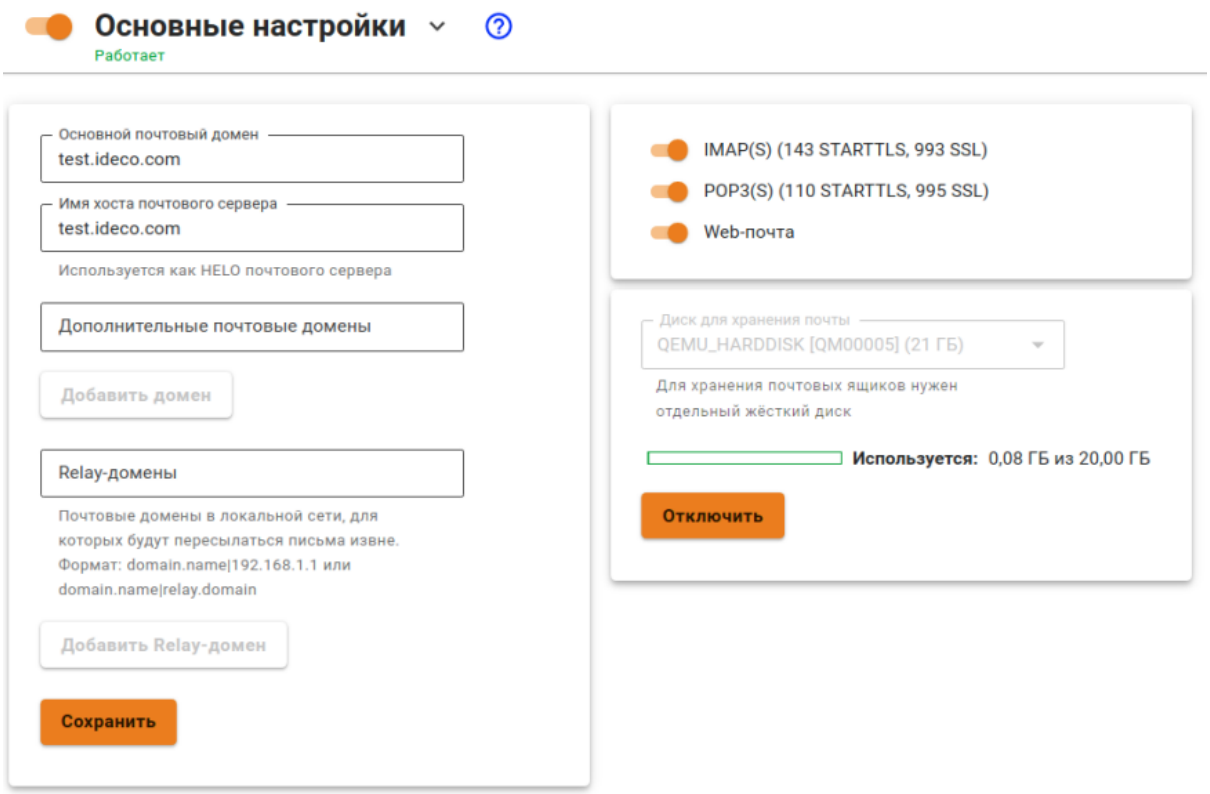
- **Основной почтовый домен** указывает серверу на его почтовый домен, для которого он должен принимать и обрабатывать письма. Все ящики пользователей будут принадлежать этому домену. От имени этого домена будет вестись переписка с корреспондентами.
- **Имя хоста почтового сервера** должно разрешаться 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.

Создание копии диска с почтой:

1. Подключите второй физический диск, на который будет произведено клонирование почты.

2. В терминале выполните команду `lsblk` и посмотрите название дисков:

```
NAME                  MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sr0                    11:0    1   1,8G  0 rom
nvme01                 259:0    0   150G  0 disk
nvme01p1              259:1    0   512M  0 part
nvme01p2              259:2    0     2M  0 part
nvme01p3              259:3    0 149,5G  0 part
  utm_72874-root_one 253:0    0     4G  0 lvm  /run/ideco-erofs
  utm_72874-data     253:1    0  63,7G  0 lvm  /run/ideco-overlay-dir
  utm_72874-logs     253:2    0     2G  0 lvm  /var/log/journal
  utm_72874-root_two 253:3    0     4G  0 lvm
  utm_72874-swap     253:4    0  15,3G  0 lvm  [SWAP]
nvme02                 259:4    0    50G  0 disk /var/spool/mail
nvme03                 259:5    0    55G  0 disk
```

В примеме используются диски:

- `nvme01` - для работы NGFW;

- `nvme02` - для хранения почты;
- `nvme03` - новый диск.

3. Выполните поблочное копирование с помощью утилиты dd, введя следующую команду `dd if=/dev/nvme02 of=/dev/nvme03 bs=4M status=progress`.

- `if=/dev/nvme02` - источник данных для копирования;
- `of=/dev/nvme03` - место назначения для скопированных данных.

Обратите внимание: после выполнения команды все данные на диске `nvme03` будут перезаписаны новыми. Если размер диска `nvme02` превышает размер диска `nvme03`, то копирование завершится неудачно.

SSL-сертификат для почтового домена

После сохранения настроек основного почтового домена и имени хоста почтового сервера Ideco NGFW создает локальный сертификат, подписанный корневым (самоподписанным) сертификатом. Параллельно с созданием локального сертификата отправляется запрос на выпуск сертификата Let's Encrypt.

- Если сертификат Let's Encrypt успешно выпущен, то он заменит собой локальный сертификат.
- Если выпуск сертификата Let's Encrypt завершился неудачей, то будет использоваться локальный сертификат.

Подсказка: Для замены автоматически выпущенного сертификата перейдите в раздел **Сервисы -> Сертификаты -> Загруженные сертификаты** и загрузите собственную цепочку сертификатов. **CN (Общее имя)** последнего сертификата в цепочке должно соответствовать домену, для которого сертификат загружается. Подробнее в *инструкции*.

Проверка настроек почтового сервера

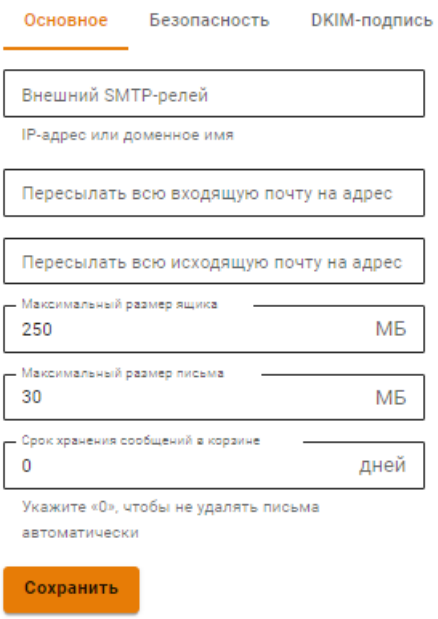
Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса mail-tester.com.

При правильной настройке почтовый сервер на Ideco NGFW должен получить 10 баллов из 10.

21.3 Расширенные настройки

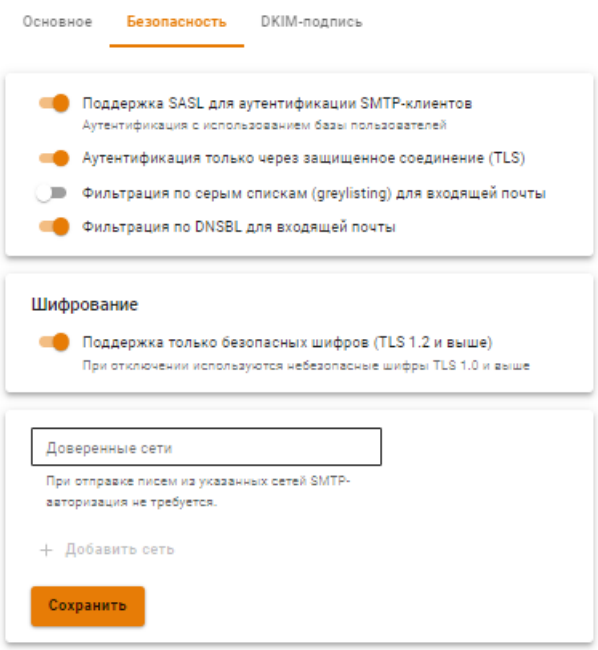
Раздел **Расширенные настройки** состоит из трех подразделов: **Основное, Безопасность, DKIM-подпись**.

21.3.1 Основное



- **Внешний SMTP-релей.** Вся исходящая почта будет отправляться на указанный адрес. Используется, например, если почта должна проходить через вышестоящий сервер провайдера перед отправкой в интернет;
- **Пересылать всю исходящую почту на адрес.** Вся исходящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости;
- **Пересылать всю входящую почту на адрес.** Вся входящая почта будет дублироваться на указанный почтовый ящик. Рекомендуется включать только при крайней необходимости;
- **Максимальный размер ящика.** Ограничение на максимальный размер почтового ящика в мегабайтах (**100ГБ - максимальное значение**);
- **Максимальный размер письма.** Ограничение на максимальный размер формируемого сервером письма в мегабайтах (**150МБ - максимальное значение**);
- **Срок хранения сообщений в корзине.** Количество дней, в течение которых почта хранится в корзине перед удалением. Максимальный срок хранения - 60 дней.

21.3.2 Безопасность

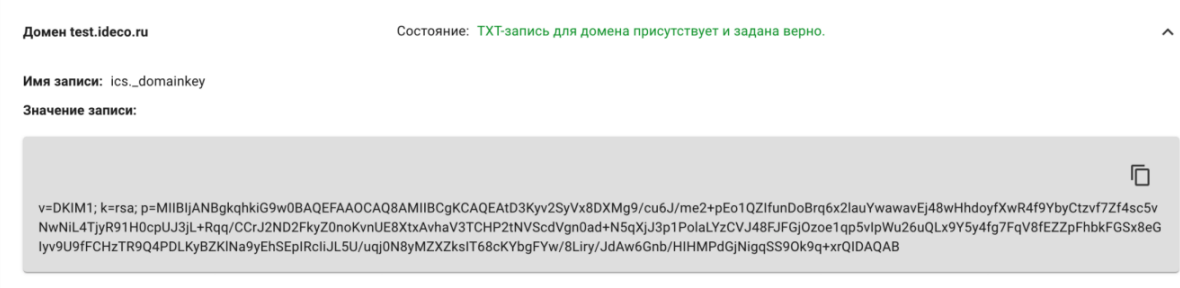


- **Поддержка SASL для аутентификации SMTP-клиентов.** Подключиться к почтовому ящику из интернета и отправить письмо, используя SMTP сервер Ideco, можно будет только, пройдя авторизацию по логину и паролю, заданному для этой учетной записи пользователя на сервере. **Не включайте этот параметр, если используете NGFW в качестве почтового релея**;
- **Разрешить аутентификацию только через защищенное соединение (TLS).** Запрещает незащищенную передачу учетных данных клиента при аутентификации на SMTP сервере;
- **Фильтрация по серым спискам (greylisting) для входящей почты.** Включает фильтрацию по серым спискам (greylisting) для входящей почты. При этом почта от неизвестных доменов отправителей может приходить с небольшой задержкой;
- **Фильтрация по DNSBL для входящей почты.** Включает фильтрацию по DNSBL для входящей почты;
- **Поддержка только безопасных шифров (TLS 1.2 и выше)**. При отключении используются небезопасные шифры TLS 1.0 и выше;
- **Доверенные сети.** Авторизация на сервере для доступа к почтовому ящику не требуется при попытке доступа из этих сетей. Указываются IP-сети и хосты в нотации CIDR или с префиксом сети, например, `10.0.0.5/255.255.255.255` или `192.168.0.0/16`.

21.3.3 DKIM-подпись

Настраивается в разделе **Почтовый релей -> Расширенные настройки -> DKIM-подпись.** Подписывает исходящую с сервера корреспонденцию уникальной для почтового домена подписью так, что другие почтовые серверы в сети интернет могут убедиться, что почта легитимна и заслуживает доверия.

Для функционирования технологии потребуется создать TXT-запись для домена у держателя зоны со значением, которое сформирует для этого почтового домена наш сервер. TXT-записи будут сформированы для основного почтового домена, настроенного на Ideco NGFW, и дополнительных почтовых доменов (если указаны). Сервер также проверит, правильно ли была указана запись и резолвится ли она в интернет.



Подсказка: Объем TXT-записи достаточно велик и многие регистраторы/держатели зон испытывают сложности с предоставлением интерфейса клиентам для указания TXT-записей длиннее 255 символов. Зачастую они предоставляют возможность указания TXT-записей длиной до 256 символов, согласно стандарту RFC1035. Но другой стандарт, RFC4408, предполагает объединение строк в случаях, когда нужно использовать длинные TXT-записи при настройке SPF и DKIM. Оперируйте этой информацией в диалоге с держателем доменной зоны. Как правило, держатели зон находят способ создания длинных TXT-записей.

Подсказка: Подпись содержит сочетание кавычек (кавычка-пробел-кавычка: « «).
Если хостинг не воспринимает такой формат записи, удалите эти символы.

21.3.4 Настройка домена у регистратора/держателя зоны

Основное

Для создания почтового сервера потребуется доменное имя. Зарегистрируйте его у интернет-провайдера или напрямую у регистратора, например, в RUcenter.

После того как было зарегистрировано доменное имя, потребуется внести изменения в описание зоны на DNS-сервере (у держателя доменной зоны, которой зачастую является регистратор).

1. Создайте ресурсную запись типа A с именем для почтового сервера в домене, указывающую на внешний IP-адрес Ideco NGFW. **Убедитесь, что на внешнем интерфейсе NGFW назначен публичный адрес, доступный из сети интернет.**

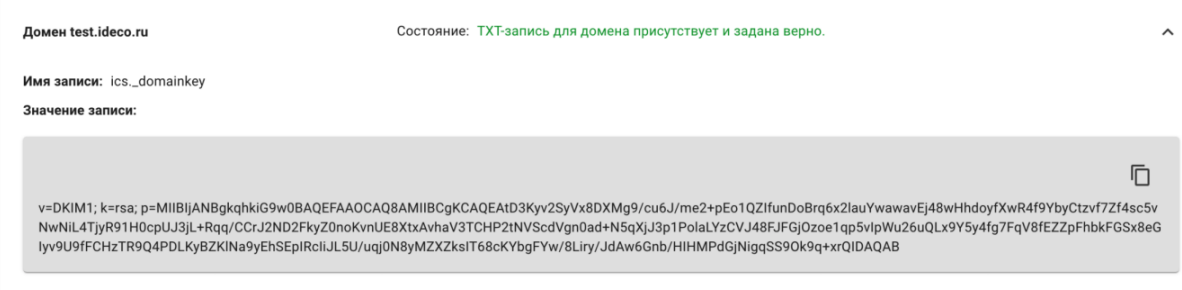
2. Добавьте ресурсную запись типа MX, указывающую на A-запись, которая была создана на предыдущем шаге. Запись типа MX указывает на сетевой узел, который занимается обработкой почтовых сообщений для домена. Она должна ссылаться на доменное имя почтового сервера, а не на IP-адрес.

Рекомендуем:

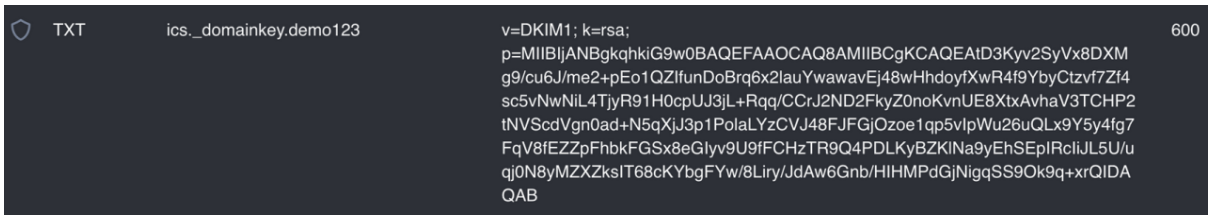
3. Добавить обратную ресурсную запись типа PTR. Эта запись должна быть прописана в файле обратной зоны. Эти изменения должны быть сделаны на стороне интернет-провайдера. Обратитесь к нему с просьбой прописать обратную ресурсную запись для IP-адреса, которая должна ссылаться на запись типа MX.

4. Настроить SPF-запись для почтового сервера.

5. После настройки почтового сервера настроить также DKIM-подпись почтовых сообщений. Для этого перейдите в раздел **Почтовый релей -> Расширенные настройки -> DKIM-подпись** и активируйте пункт **Подписывать исходящую почту с помощью DKIM**.



Также создайте TXT-запись для домена у держателя зоны с именем из строки *Имя записи* и с содержимым, которое было сформировано Ideco NGFW в **Значение записи**:



Рассмотрим набор необходимых записей на примере вымышленного домена `example.net`:

- A-запись вида: `mail.example.net. IN A 23.45.67.89`, где 23.45.67.89 - это внешний IP-адрес Ideco NGFW;
- MX-запись вида: `example.net. MX 10 mail.example.net`;
- Обратитесь на свой хостинг для регистрации PTR-записи для нужного IP-адреса вида: `89.67.45.23.in-addr.arpa IN PTR mail.example.net`;
- SPF-запись, объявляющая другим почтовым серверам в интернет, что отправка писем с домена разрешена только с хоста почтового сервера, указанного в MX-записи: `example.net. IN TXT "v=spf1 a mx -all"`.

Подсказка: Синтаксис SPF:

- «v=spf1» — версия SPF, обязательный параметр, всегда spf1, никакие другие версии не работают;
- «+» — принимать письма (по умолчанию);
- «-» — отклонить;
- «~» — «мягкое» отклонение (письмо будет принято, но будет помечено как спам);
- «?» — нейтральное отношение;
- «mx» — включает в себя все адреса серверов, указанные в MX-записях домена;

При использовании почтового сервера на NGFW в качестве почтового релея ресурсные записи будут выглядеть так же, так как в интернете почтовый сервер в локальной сети будет представлен SMTP-релеем на NGFW.

21.4 Антиспам

Подсказка: Видеоинструкцию смотрите по ссылкам:

- Rutube;
- Youtube.

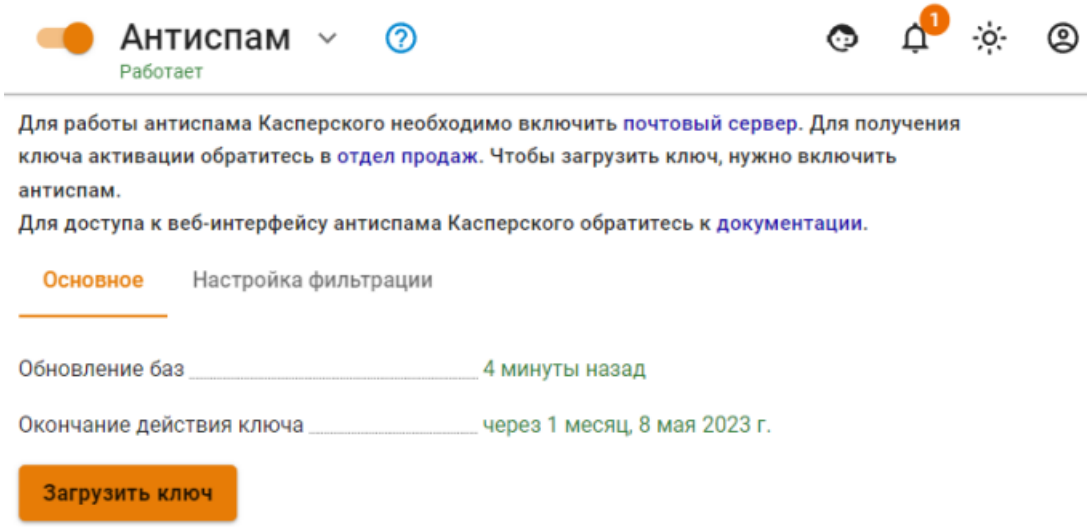
Раздел **Антиспам** состоит из двух подразделов: **Основное** и **Настройки фильтрации**.

21.4.1 Основное

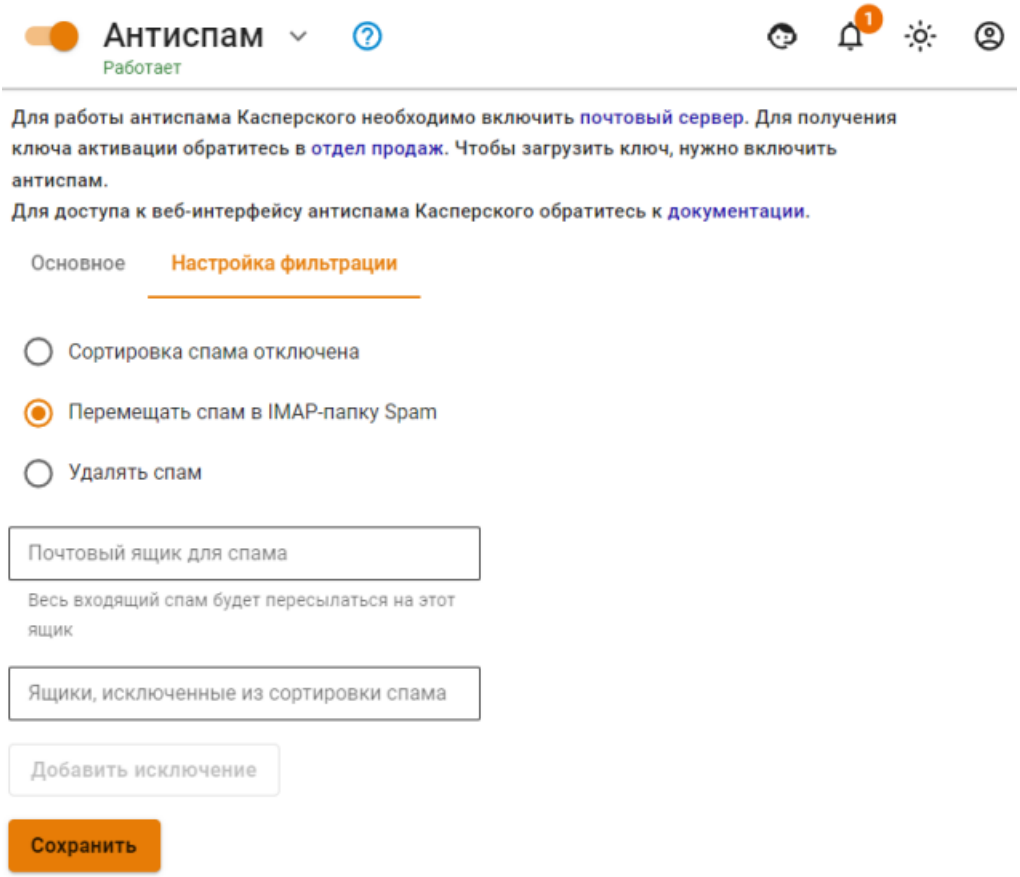
Позволяет управлять работой службы антиспама на основе технологий Лаборатории Касперского с функцией машинного обучения и искусственного интеллекта. Также на этой вкладке предоставлена возможность добавления лицензионного ключа антиспама. Ключ поставляется в файле, имеющем расширение `.key`.

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.



21.4.2 Настройки фильтрации



- **Сортировка спама.** Задание логики сортировки нежелательной корреспонденции (спама). На выбор предоставляются следующие опции: отключение сортировки, перемещение нежелательных отправлений в папку Spam, удаление таких писем с сервера;
- **Почтовый ящик для спама.** Весь входящий спам будет пересылаться на указанный ящик (не используйте ящик Spam);
- **Ящики, исключенные из сортировки спама.** Позволяет задать почтовые адреса, которые не будут проверяться на спам.

Веб-интерфейс для Антиспама

Подсказка: Для включения веб-интерфейса Антиспама требуется, чтобы сам модуль **Антиспам** был включен.

Веб-интерфейс имеет следующие преимущества:

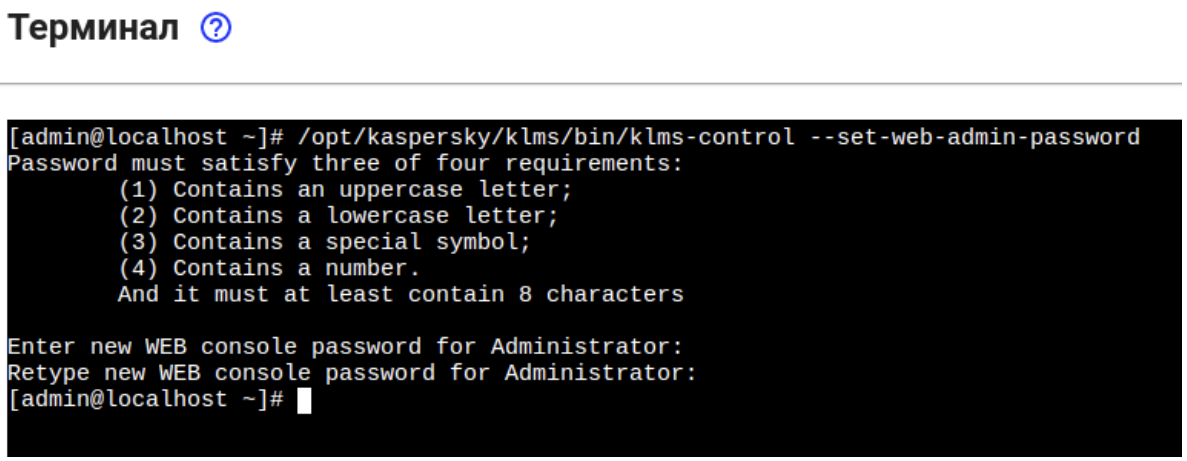
- Отображает статистику по категориям Антиспама Касперского в удобном и понятном виде;
- Генерирует отчеты по работе за определенный период;
- Отображает очередь обрабатываемых сообщений;
- Позволяет задавать правила *Запрещенных и Разрешенных адресов*;
- Ведет аудит всех действий, производимых с Антиспамом.

Чтобы включить веб-интерфейс для Антиспама:

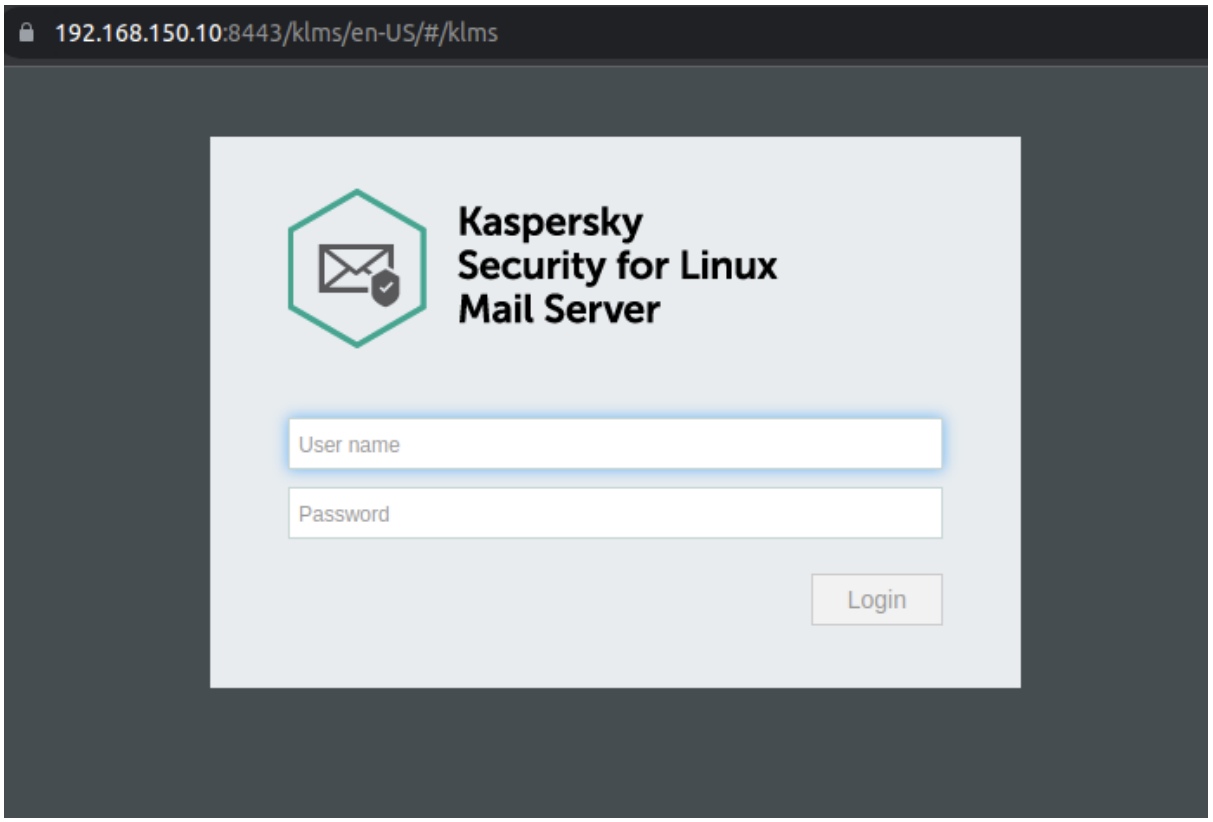
1. Перейдите в раздел **Управление сервером -> Терминал** и выполните следующую команду `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`

2. Задайте пароль для стандартного аккаунта **Administrator**, состоящий минимум из 8 символов:

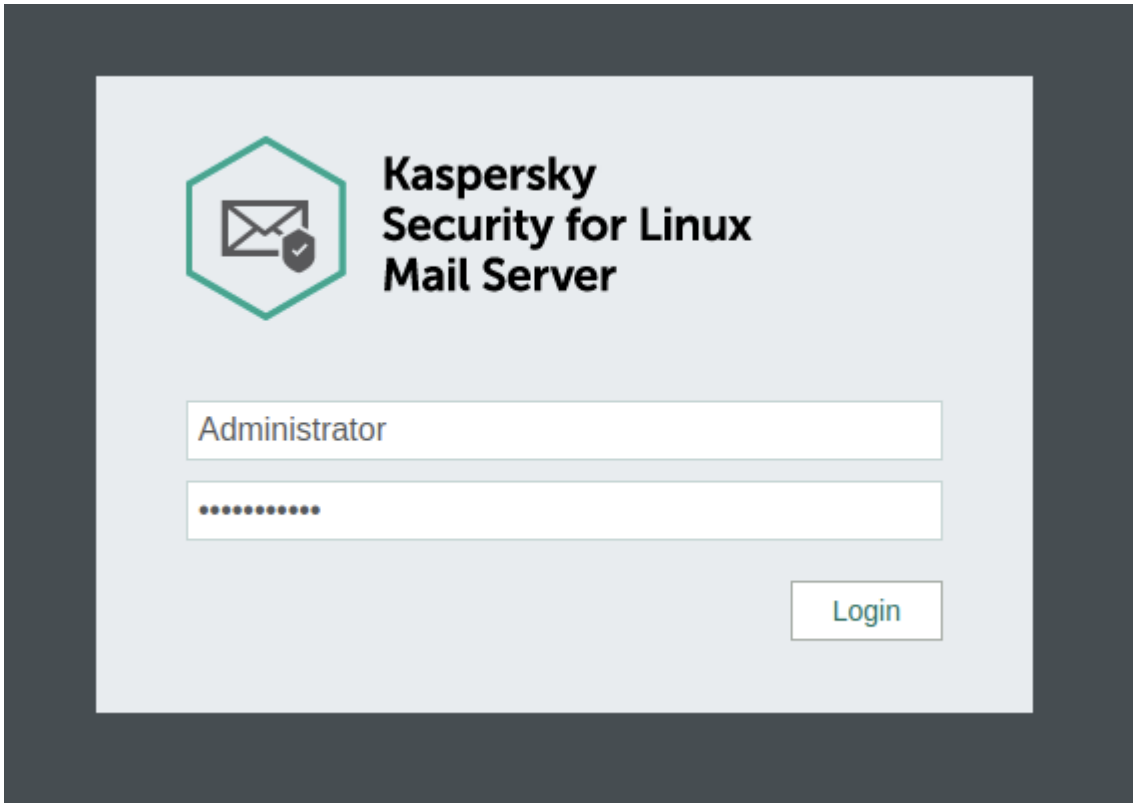
- Строчных букв;
- Заглавных букв;
- Специальных символов;
- Чисел.



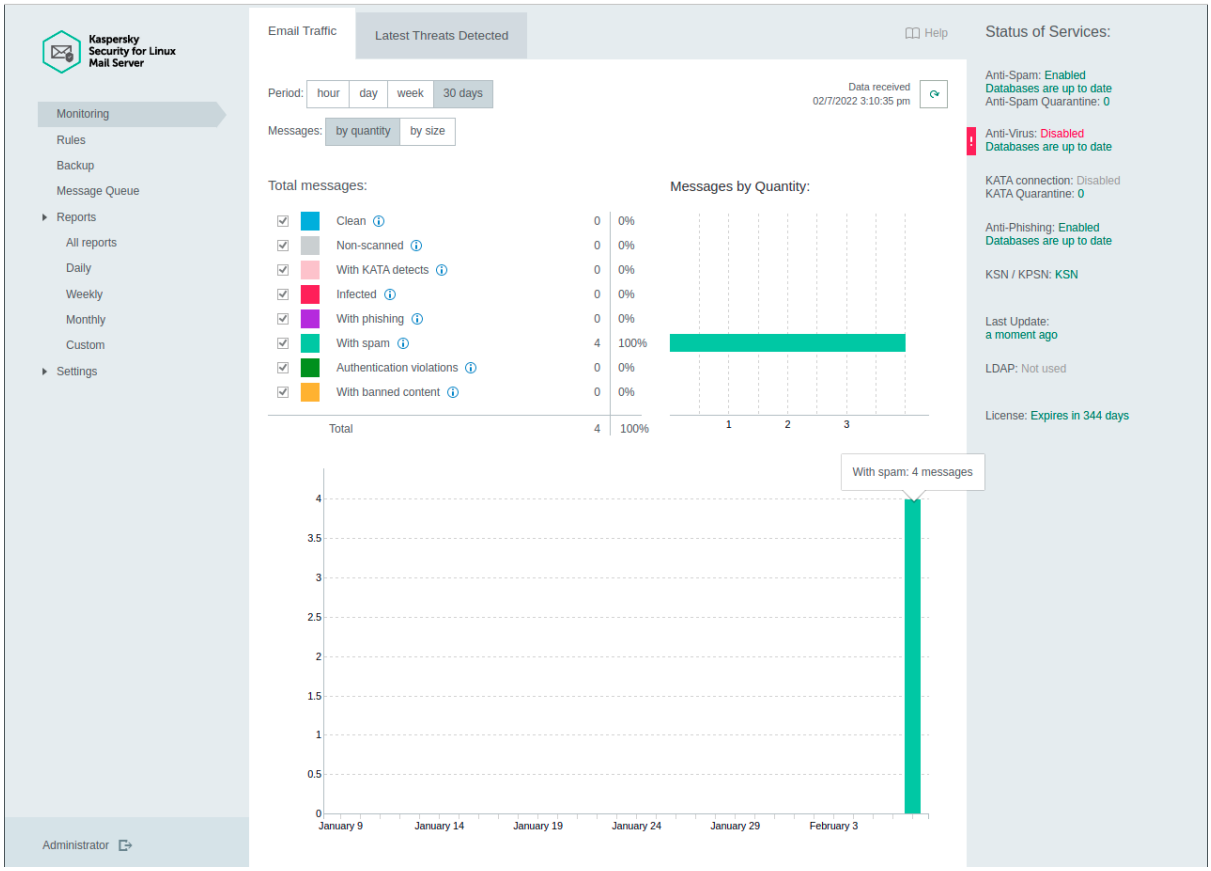
3. Для доступа к веб-интерфейсу перейдите в адресной строке по пути `ngfw_ip_address:8443/klms/`:



4. Войдите в веб-интерфейс с учетной записью **Administrator** и ранее заданным в терминале паролем:



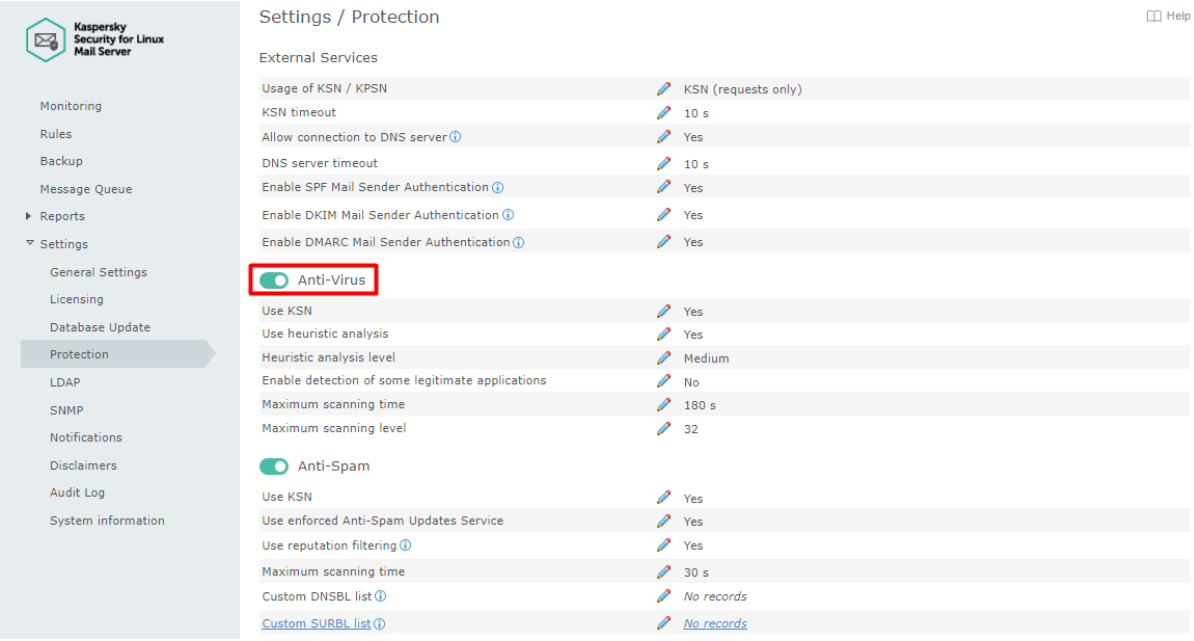
После успешного входа будет отображен дашборд со статистикой работы Антиспама:



Включение Антивируса почтового сервера

1. Перейдите в веб-интерфейс Антиспама. Подробные шаги настройки и входа в веб-интерфейс описаны в статье *Веб-интерфейс для Антиспама*;

2. Включите антивирус почтового сервера, перейдите в раздел **Settings -> Protection** и активируйте опцию **Anti-Virus**:



Предупреждение: Не рекомендуем вносить какие-либо изменения в разделе `Settings`, кроме указанных выше, потому как не можем гарантировать функциональность работы Антиспама в таких случаях.

21.5 Правила

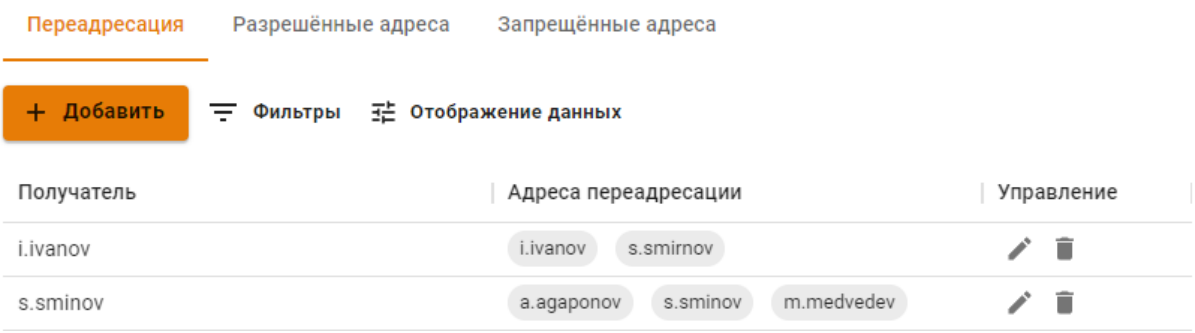
Раздел **Правила** состоит из трех вкладок: **Переадресация, Разрешенные адреса, Запрещенные адреса**. На каждой вкладке доступна фильтрация по кнопке **Фильтры**.

21.5.1 Переадресация

Позволяет настроить переадресацию почты на сервере с помощью почтовых алиасов.

Алиасы, в отличие от почтовых ящиков, не требуют логинов и паролей, они закрепляются за ящиком и служат его копией с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, может служить группой рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в графе **Получатель**, должен реально существовать.

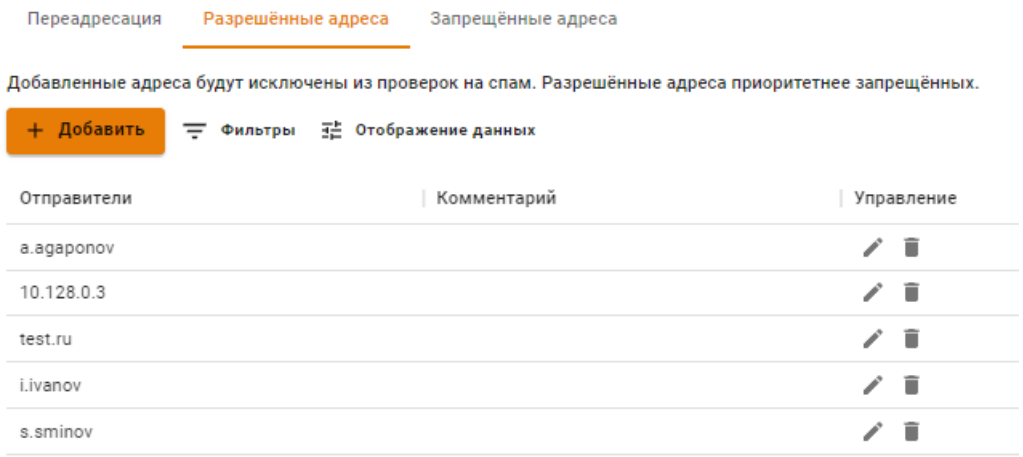
Подробнее с документацией по настройке почтовых алиасов на Ideco NGFW ознакомьтесь в статье *Переадресация почты*.



21.5.2 Разрешенные адреса

Позволяет указывать почтовые домены, IP-адреса почтовых серверов и почтовые ящики, отправления с которых не будут проверяться на спам.

Предупреждение: Если ящик одновременно указан в **Запрещенном адресе** и в **Разрешенном адресе**, то наивысший приоритет имеет **Разрешенный адрес**.



Подсказка: При занесении пересекающихся источников в оба списка корреляции между источниками не происходит. Приоритет будет отдан сначала IP-адресам, затем ящикам и затем доменам. То есть, если запрещен IP-адрес почтового сервера и разрешен домен, который он обслуживает, то письма от него будут блокироваться (блокировка по IP-адресу имеет приоритет). Обратный пример: разрешен IP-адрес, но запрещен домен. Письма блокируются, просто на более поздней стадии, при проверке почтового домена.

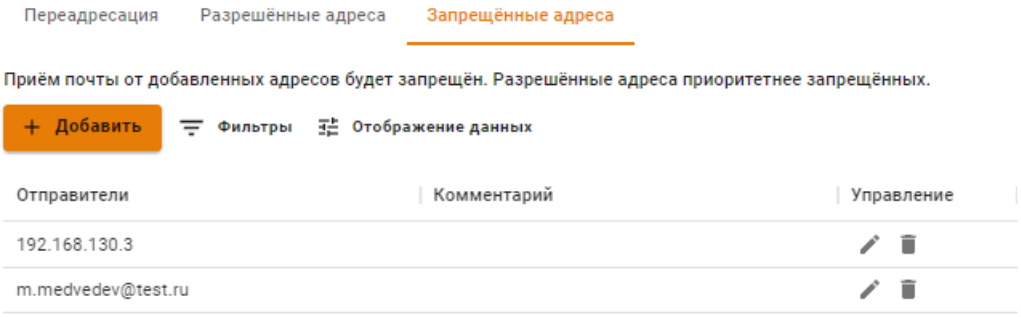
Еще один пример: в **Разрешенные адреса** внесен домен, в **Запрещенные адреса** - ящик из этого домена. Тогда письма с ящика будут заблокированы.

Обратный пример: письма от ящика, занесенного в **Разрешенные адреса**, будут разрешены, даже если домен, которому принадлежит ящик, занесен в **Запрещенные адреса**.

Подсказка: Схема обработки писем в почтовом сервере представлена в статье *Схема фильтрации почтового трафика*. Обратите внимание, что Разрешенные и Запрещенные адреса срабатывают после нескольких предварительных этапов фильтрации.

21.5.3 Запрещенные адреса

Позволяет указывать почтовые домены и ящики, отправления с которых не будут приниматься сервером.



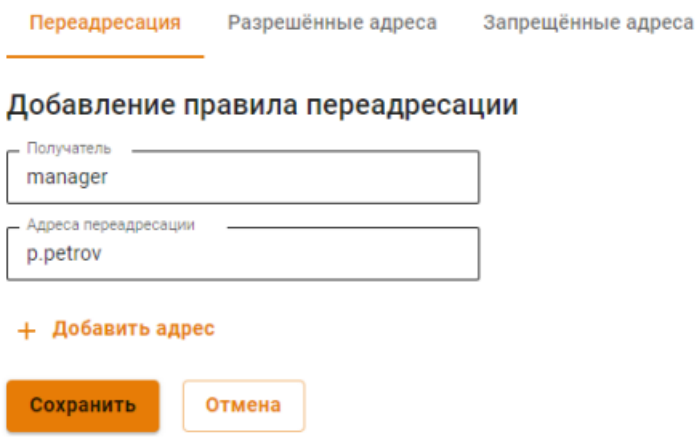
21.5.4 Переадресация почты

Чтобы создавать и редактировать почтовые правила переадресации (алиасы), перейдите в раздел **Почтовый релей -> Правила -> Переадресация**.

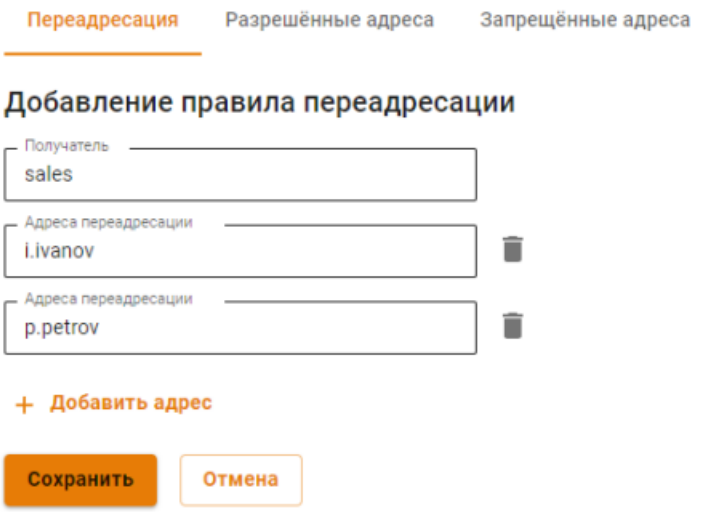
Почтовые алиасы отличаются от почтовых ящиков тем, что не требуют логинов и паролей. Они закрепляются за ящиком и служат его копией с другим именем, или, в случае назначения алиаса нескольким почтовым ящикам, можно сказать что алиас - это группа почтовых ящиков или группа рассылки. Поступающая на алиас почта автоматически пересылается на все реальные почтовые ящики, связанные с этим алиасом. Часть адреса `@yourdomain.com` можно не указывать при создании правил, если ящик расположен на почтовом сервере Ideco NGFW. Если перенаправление делается на какой-либо ящик в другом домене в интернете, то ящик, прописываемый в поле **Получатель**, должен реально существовать.

Примеры:

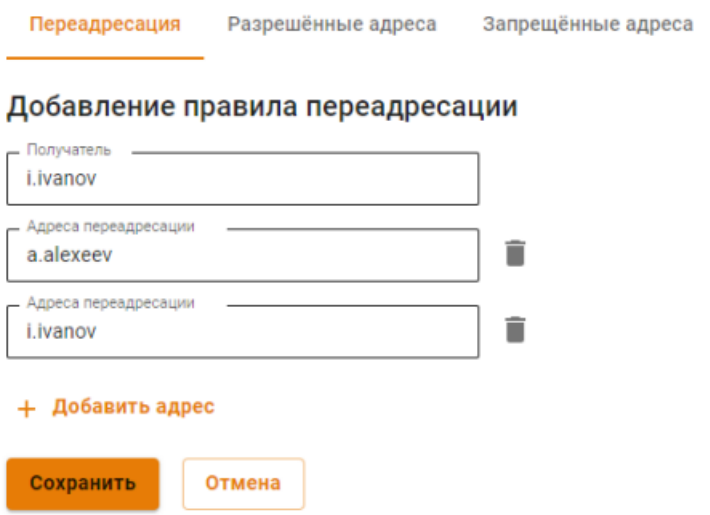
- Создать алиас `manager@yourdomain.ru` для ящика менеджера компании для связи с клиентами и партнерами, у которого реальный почтовый ящик имеет имя `p.petrov@yourmaildomain.ru`:



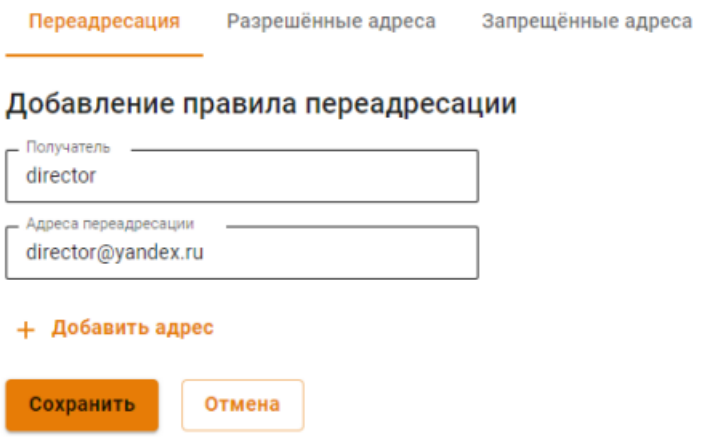
- Создать корпоративный алиас для отдела продаж `sales@yourmaildomail.ru`, чтобы почта пересылалась на всех сотрудников этого отдела:



- Создать временный алиас для переадресации почты сотрудника, который находится в отпуске `i.ivanov@yourmaildomail.ru`, на ящик его коллеги `a.alexeev@yourmaildomain.ru` с сохранением почты на ящике `i.ivanov@yourmaildomail.ru`:



- Создать алиас `director@yourmaildomain.ru`, который будет перенаправлять почту на реальный ящик `director@yandex.ru`:



Работа почты при настроенных правилах переадресации:

Письма, приходящие на несуществующий ящик (алиас) `manager@yourdomain.ru`, будут попадать на реальный `p.petrov@yourmaildomain.ru`. Также есть алиас для отдела продаж `sales@yourmaildomail.ru`, который, по сути, служит алиасом для рассылки почты и сам писем не хранит. Это удобно, если есть информация для отдела продаж, которую надо распространить на каждого сотрудника. Все то же самое можно сделать, если просто указать в письме всех получателей, но использовать алиас намного удобнее. Также сотрудник с почтой `i.ivanov@yourmaildomail.ru` сейчас находится в отпуске, вся приходящая к нему почта попадает на его ящик и дублируется на `a.alexeev@yourmaildomain.ru`. Последнее правило позволяет директору получать почту не на корпоративный ящик, а на его личную почту на Яндексе.

Подсказка: Алиас не является действительным почтовым ящиком. К нему нельзя подключиться почтовым клиентом, используя логин и пароль, как в обычном почтовом аккаунте. Таким образом, создание алиасов не увеличивает максимально возможное количество реальных почтовых аккаунтов на Ideco NGFW.

21.6 Почтовая очередь

Модуль позволяет управлять входящей и исходящей отложенной корреспонденцией. Для анализа возможных причин задержки корреспонденции в очереди можно использовать информацию из соответствующего столбца таблицы для каждого письма. По кнопке **Фильтры** доступна фильтрация по каждому столбцу.

Почтовая очередь позволяет выполнять следующие выборочные и групповые действия с отправлениями:

- Очистка очереди
- Повторная отправка отдельного письма
- Удаление отдельных писем из очереди
- Повторная отправка всей корреспонденции из очереди

Подсказка: Значение в столбце **Время доставки** соответствует времени поступления письма в очередь. Если письмо не будет отправлено в течение 7 дней, то оно будет удалено из почтовой очереди и не будет доставлено получателю.

Предупреждение: При обновлении Ideco NGFW почтовая очередь очищается.

21.6.1 Проверка настроек почтового сервера

Рекомендуется проверить корректность всех настроек DNS и почтового сервера с помощью сервиса mail-tester.com.

При правильной настройке почтовый сервер на Ideco NGFW должен получить 10 баллов из 10.

21.7 Настройка почтовых клиентов

Предупреждение: Начиная с версии UTM 7.0.0, подключиться из сети интернет программой Outlook (любой версии) по протоколу POP3 можно только с типом шифрования SSL. Подключение без шифрования извне запрещено на почтовом сервере.

Остается возможность подключаться по протоколу IMAP с использованием STARTTLS или SSL. Для этого выберите соответствующий тип шифрования в Outlook.

Подсказка: В Ideco NGFW нет ограничений по количеству почтовых клиентов для одного почтового адреса по протоколу imap.

21.7.1 Настройка почтового клиента при работе из локальной сети

1. Сервер входящей почты работает на 995 TCP-порту (POP3) и на 143 TCP-порту (IMAP) с шифрованием STARTTLS/SSL:

- В качестве логина прописывается логин от учетной записи пользователя.
- В качестве пароля всегда прописывается пароль от учетной записи пользователя (в том числе для пользователей, импортированных из Active Directory), задать отдельный пароль на почтовый ящик нельзя.

2. Сервер исходящей почты работает на 587 порту TCP с шифрованием STARTTLS/SSL. Без авторизации возможна отправка почты только из доверенных сетей (их можно настроить в разделе **Почтовый релей -> Расширенные настройки -> Безопасность**).

21.7.2 Настройка почтового клиента при работе из сети интернет

1. Сервер входящей почты работает на 995 TCP-порту (POP3S) и на 143 TCP-порту (IMAP-STARTTLS/SSL), шифрование обязательно:

- В качестве логина прописывается логин от учетной записи пользователя;
- В качестве пароля всегда прописывается пароль от учетной записи пользователя, сделать отдельный пароль на почту нельзя.

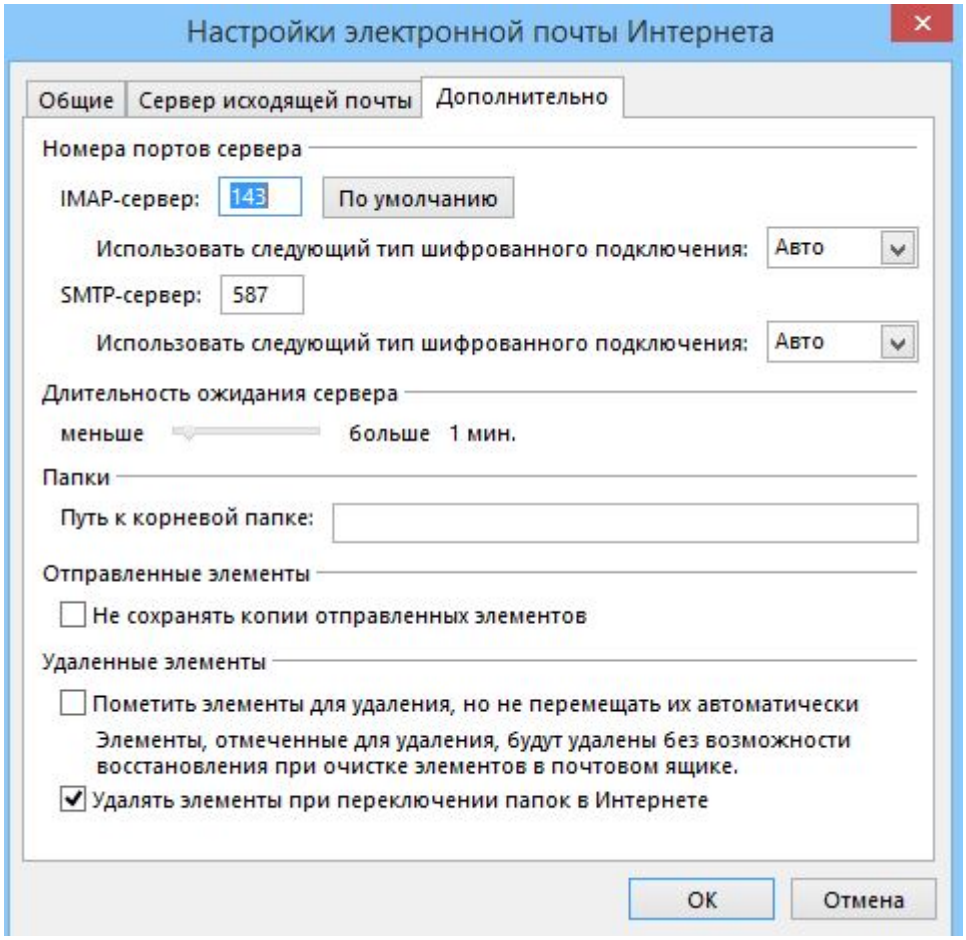
2. Сервер исходящей почты работает только с авторизацией и шифрованием. Необходимо обязательно использовать 587 порт для подключения (а не 25). Тип шифрования, логин и пароль указываются аналогично серверу входящей почты.

Для любого почтового клиента, кроме веб-интерфейса почты в составе NGFW, установите корневой сертификат сервера NGFW, его можно скачать в разделе **Сервисы -> Сертификаты**.

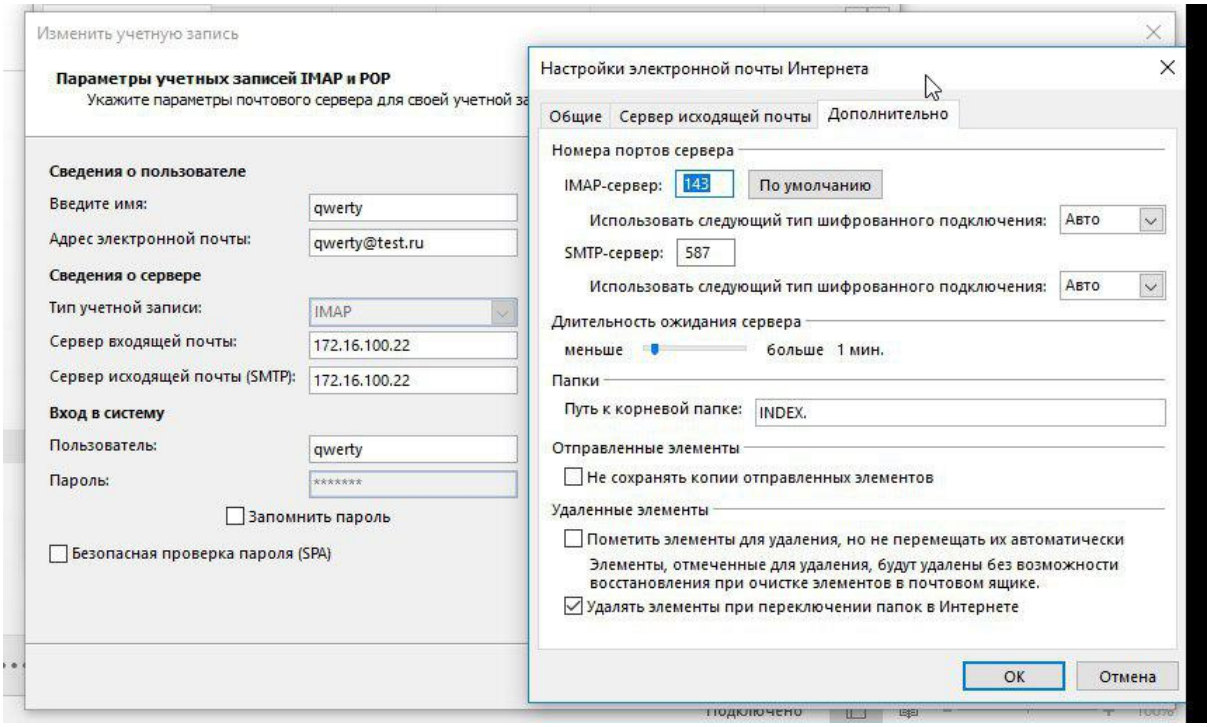
21.7.3 Примеры настроек популярных почтовых клиентов

Настройка почтового клиента Outlook 2013 и 2016:

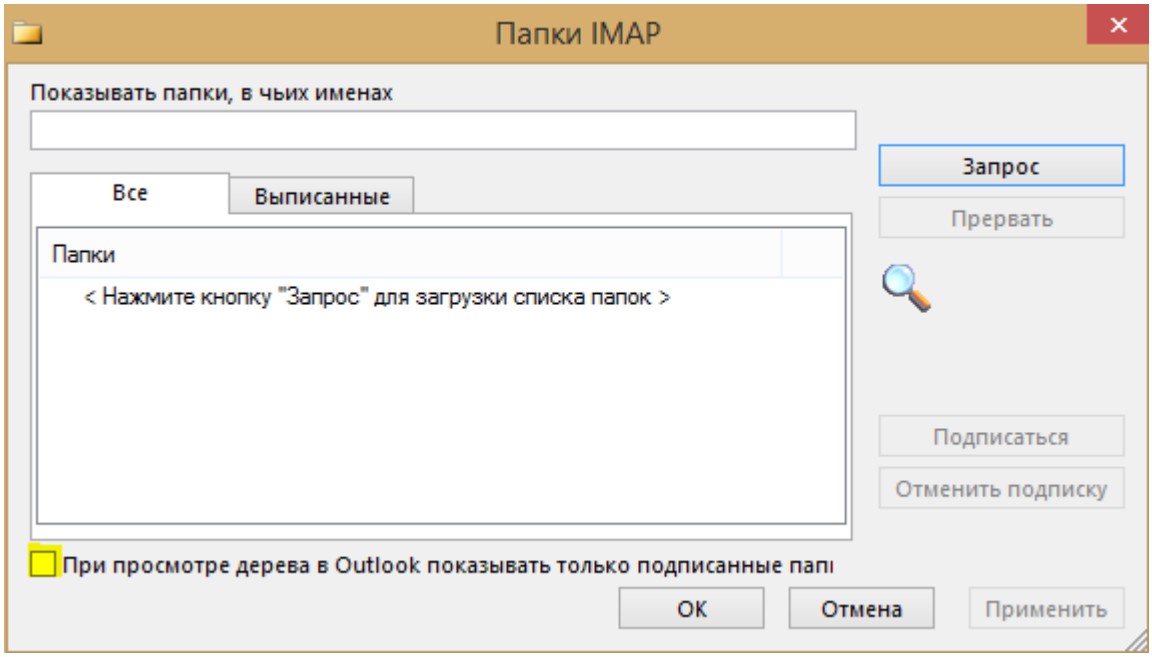
Пример настроек клиента Microsoft Outlook 2013 по протоколу IMAP:



Пример настроек клиента Microsoft Outlook 2016 по протоколу IMAP:



Для отображения IMAP-папок отключите опцию **При просмотре дерева в Outlook показывать только подписанные папки** в свойствах IMAP-папок:



Настройка почтового клиента iPhone:

Процесс настройки делится на два этапа:

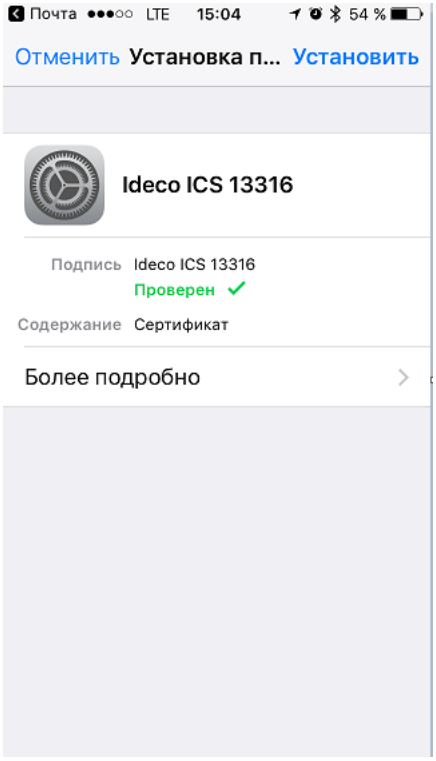
- Установка корневого SSL-сертификат NGFW;
- Настройка почтового ящика.

Установка корневого SSL-сертификат NGFW:

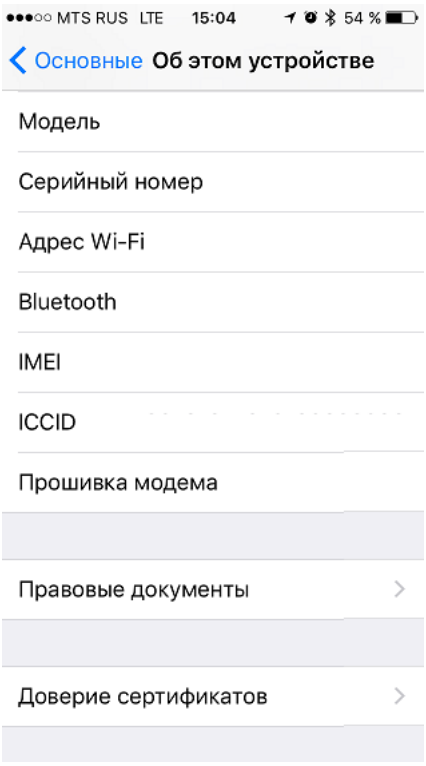
1. Скачайте сертификат в разделе **Сервисы -> Сертификаты** и перенесите на настраиваемое устройство (например, отправив по почте).

2. Нажмите кнопку **Установить**.

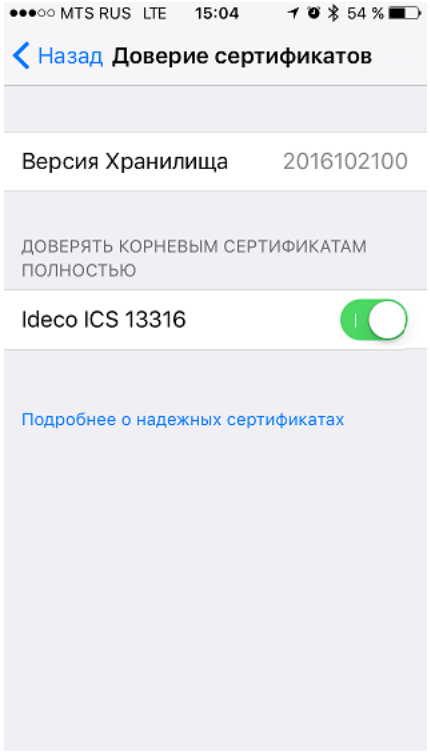
3. Зайдите в раздел **Настройки -> Основные**.



4. Выберите **Об этом устройстве -> Доверие сертификатов**:

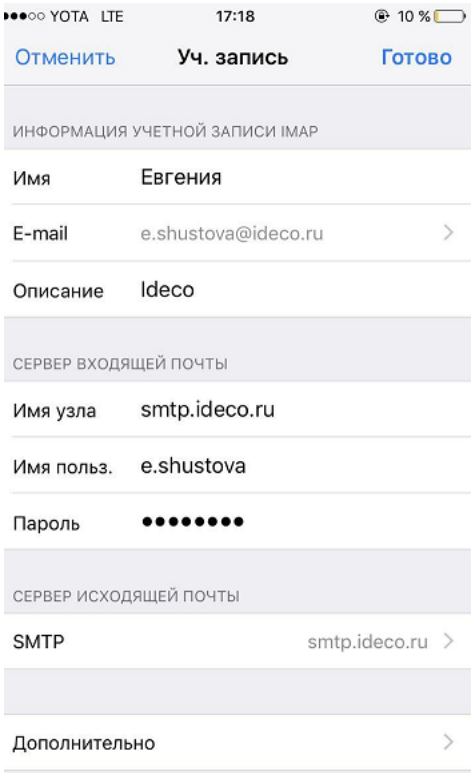


5. Включите настройку **Доверять корневым сертификатам полностью**

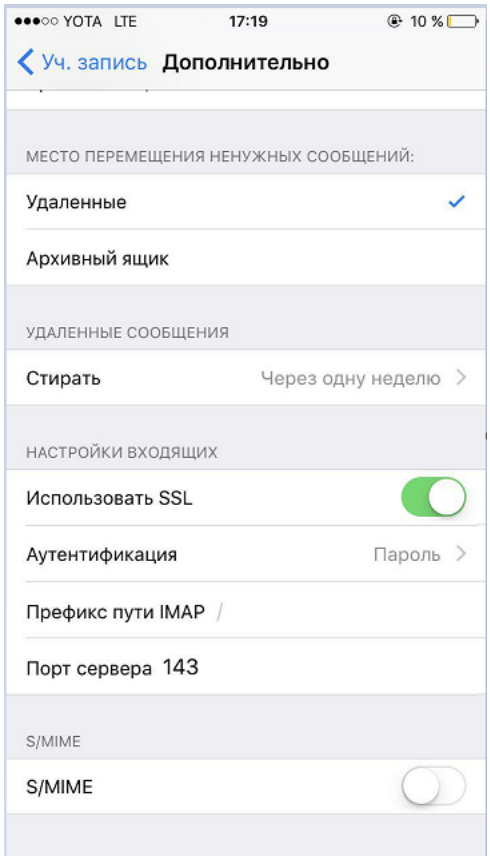


Настройка почтового ящика:

1. Перейдите в Учетную запись почты и нажмите **Дополнительно**:



2. Скорректируйте настройки:



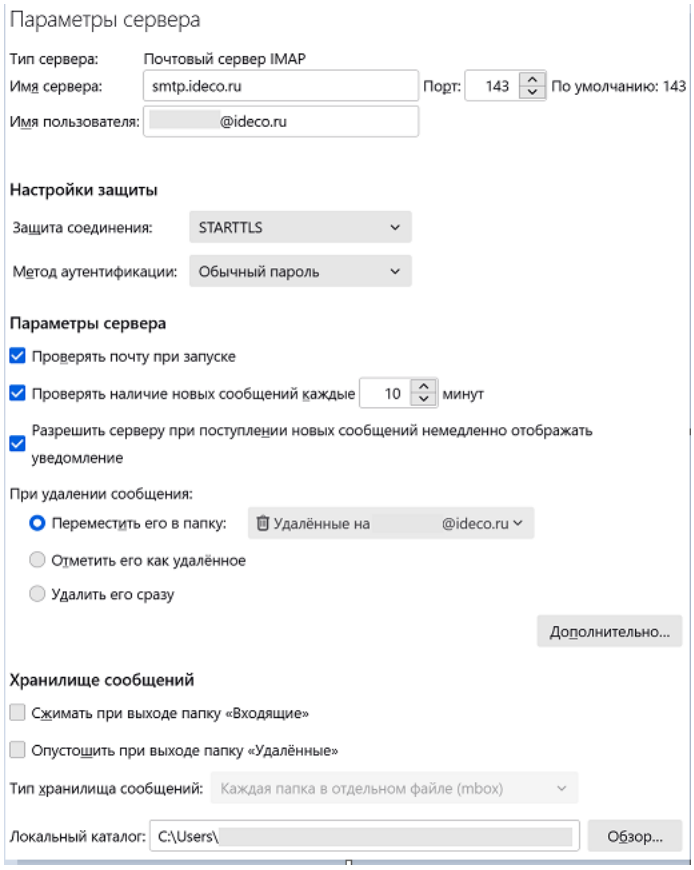
Настройка почтового клиента Thunderbird:

1. Перейдите в **Настройки -> Параметры ученой записи**.

2. Заполните обязательные поля:

   - Имя сервера;
   - Порт;
   - Имя пользователя;
   - Защита соединения;
   - Метод аутентификации (рекомендуем указать **Обычный пароль**).

При необходимости заполните *Параметры сервера* и *Хранилище сообщений*.



21.8 Схема фильтрации почтового трафика

21.8.1 Основное

Полная схема и последовательность фильтрации:



Модуль Антиспама Касперского использует собственный набор методик для фильтрации спама и обеспечивает высокий уровень детектирования спама при низких значениях ложных срабатываний (0,003-0,005% от общего количества сообщений).

Для защиты пользователей используется набор технологий распознавания спама с использованием внешних облачных сервисов (DNSBL, SPF и SURBL) и собственных алгоритмов: сигнатурный анализ текста и графики, лингвистический эвристик, использование UDS-запросов в режиме реального времени. Также проверяются все ссылки в почтовых сообщениях, письма со ссылками на фишинговые ресурсы блокируются.

Белый список в настройках почты обеспечивает прохождение писем без фильтрации, начиная с уровня **Фильтрации по серым спискам и проверки DKIM/SPF**. Предварительные спам-фильтры срабатывают для любых адресатов.

22. Публикация ресурсов

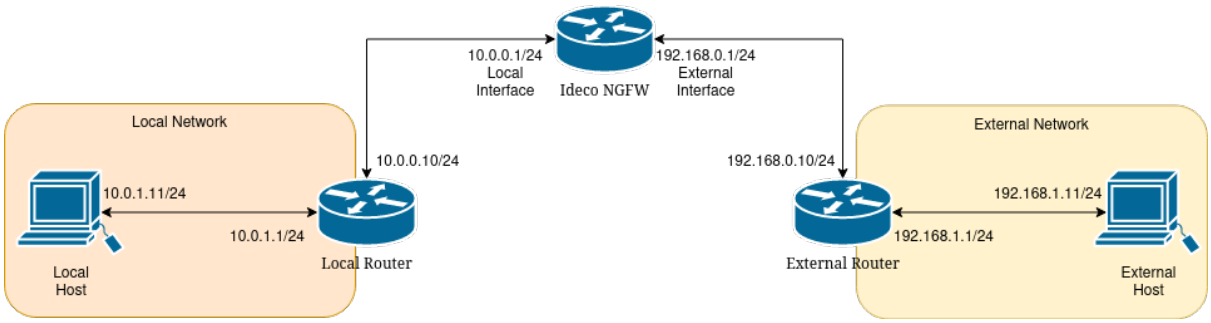
22.1 Доступ из внешней сети без NAT

22.1.1 Основное

При необходимости (как правило, когда Ideco NGFW расположен внутри локальной сети, а не на границе с интернетом) возможно:

- Организовать прямой доступ к ресурсам внешних по отношению к Ideco NGFW сетей без использования NAT;
- Разрешить доступ из внешних относительно Ideco NGFW сетей в локальную сеть с прямым обращением к локальным IP-адресам.

Для примера разберем настройку Ideco NGFW для доступа без NAT в следующей конфигурации сети:



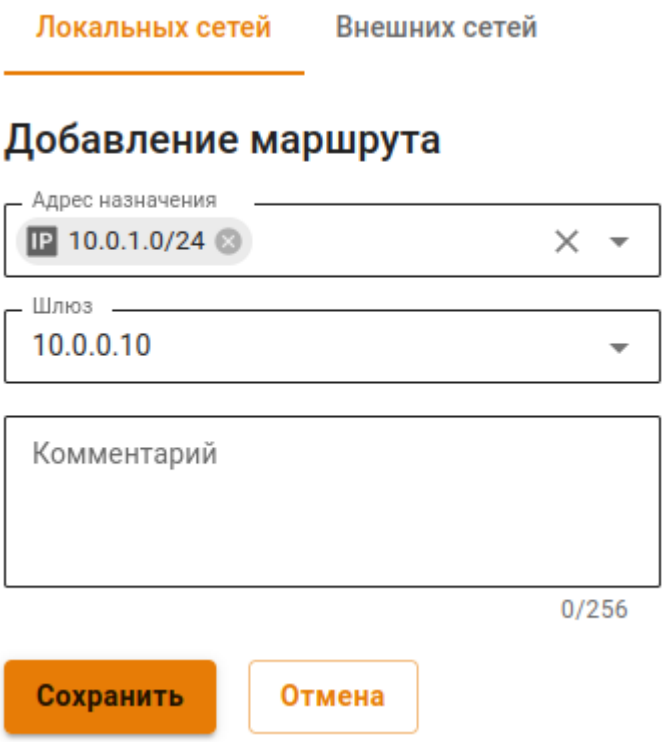
1. Настройте сетевые интерфейсы в разделе **Сервисы -> Сетевые интерфейсы** на Ideco NGFW:



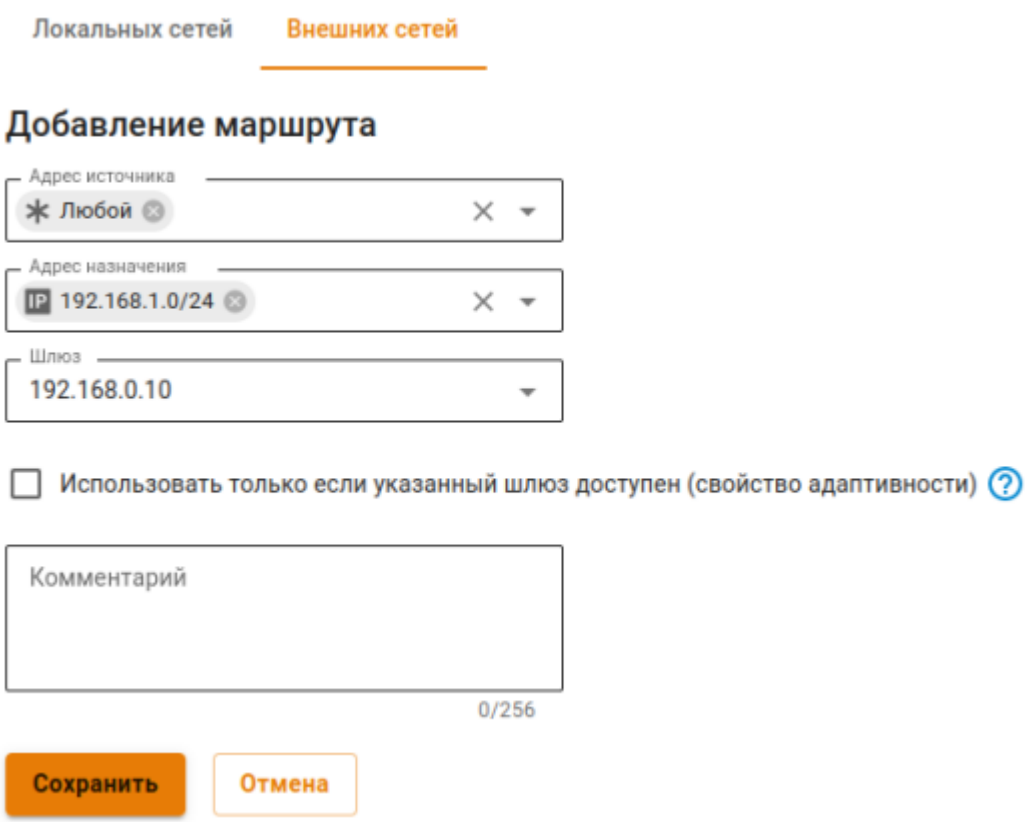
- **local** - интерфейс для доступа в пользовательскую локальную сеть;
- **external** - интерфейс для доступа в пользовательскую внешнюю сеть пользователей.

2. Перейдите в раздел **Сервисы -> Маршрутизация** и создайте правила для доступа к IP-адресам пользователей, которые находятся за маршрутизаторами:

- Для **Локальных сетей**:

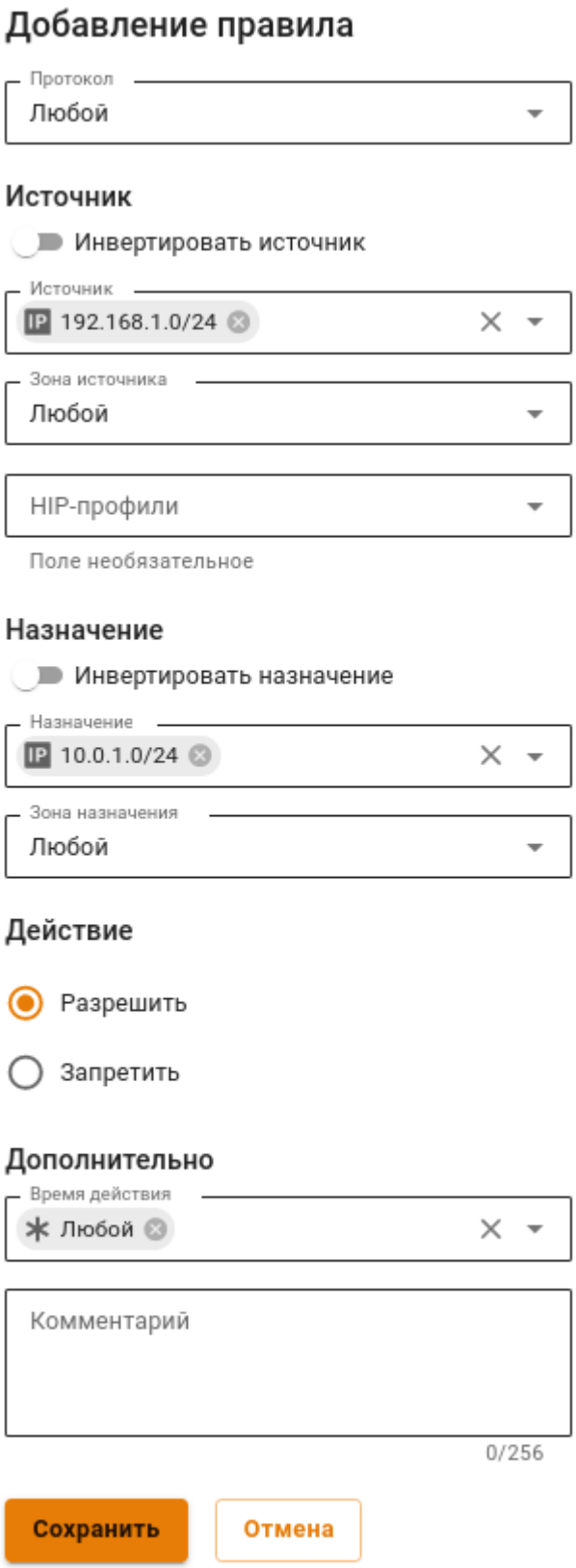


- **Адрес назначения** - адрес локальной сети за маршрутизатором (`10.0.1.0/24`);
- **Шлюз** - адрес машрутизатора (`10.0.0.10`).
- Для **Внешних сетей**:



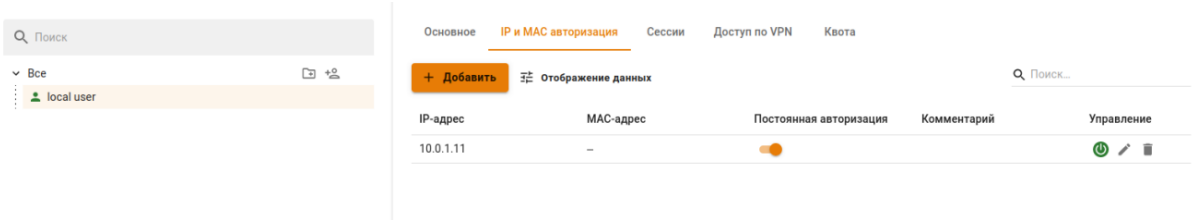
- **Источник** - Любой;
- **Адрес назначения** - адрес внешней сети за маршрутизатором (`192.168.1.0/24`);
- **Шлюз** - адрес машрутизатора (`192.168.0.10`).

3. Перейдите в раздел **Правила трафика -> Файрвол -> FORWARD** 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.

22.2 Публикация веб-приложений (обратный прокси-сервер)

22.2.1 Основное

Публикация веб-серверов возможна через *обратный прокси сервер*.

22.3 Настройка публичного IP-адреса на компьютере в локальной сети

22.3.1 Основное

Для версии Ideco UTM 7.9.0 и старше настройка публичного IP-адреса для компьютеров, находящихся в локальной сети, невозможна.

Используйте *портмаппинг*, чтобы пробросить весь их диапазон от 0 до 65535 для получения эффекта присутствия локального сервера на внешнем IP-адресе.

22.4 Портмаппинг (проброс портов, DNAT)

22.4.1 Основное

Сервер предоставляет доступ к опубликованному в интернете веб-ресурсу (сервису, сетевой службе) на устройстве в локальной сети с серым IP-адресом. Ресурс публикуется путем трансляции (проброса) любого неиспользуемого сетевого порта на публичном IP-адресе сервера Ideco NGFW на порт ресурса, работающего на устройстве в локальной сети. При этом все обращения из внешних сетей на публичный адрес сервера Ideco по транслируемому порту перенаправляются на публикуемый порт данного ресурса. Эта технология называется DNAT, portmapper или port forwarding.

Для настройки портмаппинга в Ideco NGFW добавьте правило в разделе **Правила трафика -> Файрвол -> DNAT (перенаправление портов)**. При создании правила укажите адреса сервера, публикуемой машины и сетевого порта, с которого и на который осуществляется трансляция сетевых запросов извне.

Проверьте, что в таблице FORWARD нет запрещающего прохождение трафика правила. При наличии запрещающего правила создайте разрешающее FORWARD-правило и поместите его выше запрещающего. Укажите при создании правила назначение (адрес устройства в локальной сети) и порт назначения.

Подсказка: Не рекомендуется использовать проброс портов для публикации веб- и почтовых серве-

ров (80, 443 порты). Для их публикации воспользуйтесь *обратным прокси-сервером*.

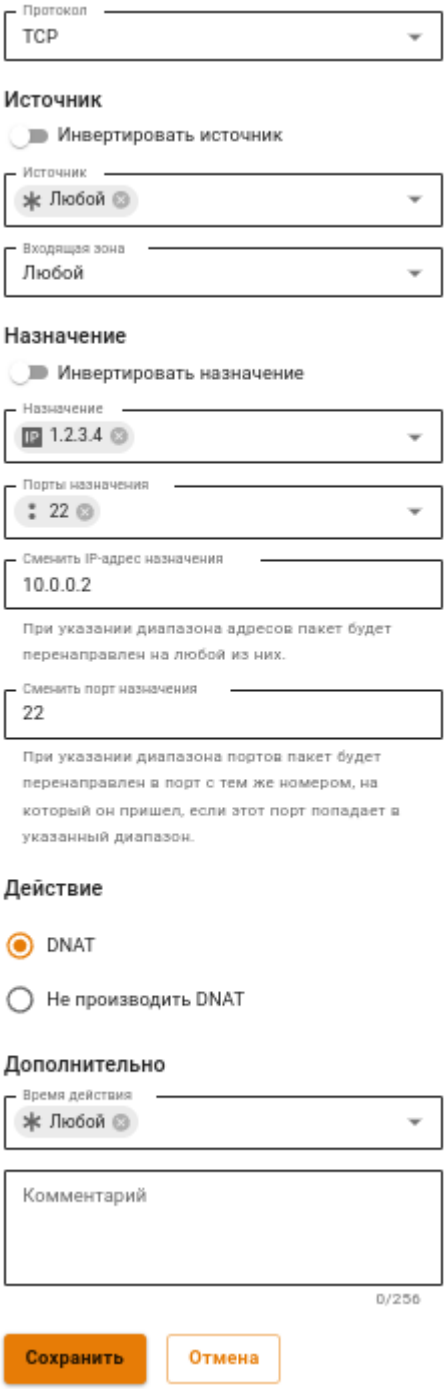
Создание правил DNAT и FORWARD в Файрволе Ideco NGFW:

Пример:

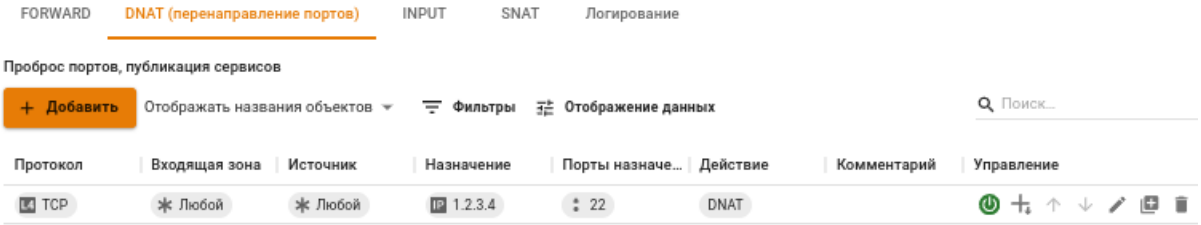
- Публичный адрес сервера Ideco - 1.2.3.4;
- Публикуемая служба - SSH, работающая на 22 TCP-порте;
- Адрес компьютера в локальной сети, где запущена служба, к которой нужен доступ извне - 10.0.0.2.

Для настройки трансляции запросов к службе извне через сервер Ideco NGFW на устройство в локальной сети перейдите в раздел **Правила трафика -> Файрвол -> DNAT (перенаправление портов)** и нажмите **Добавить**.

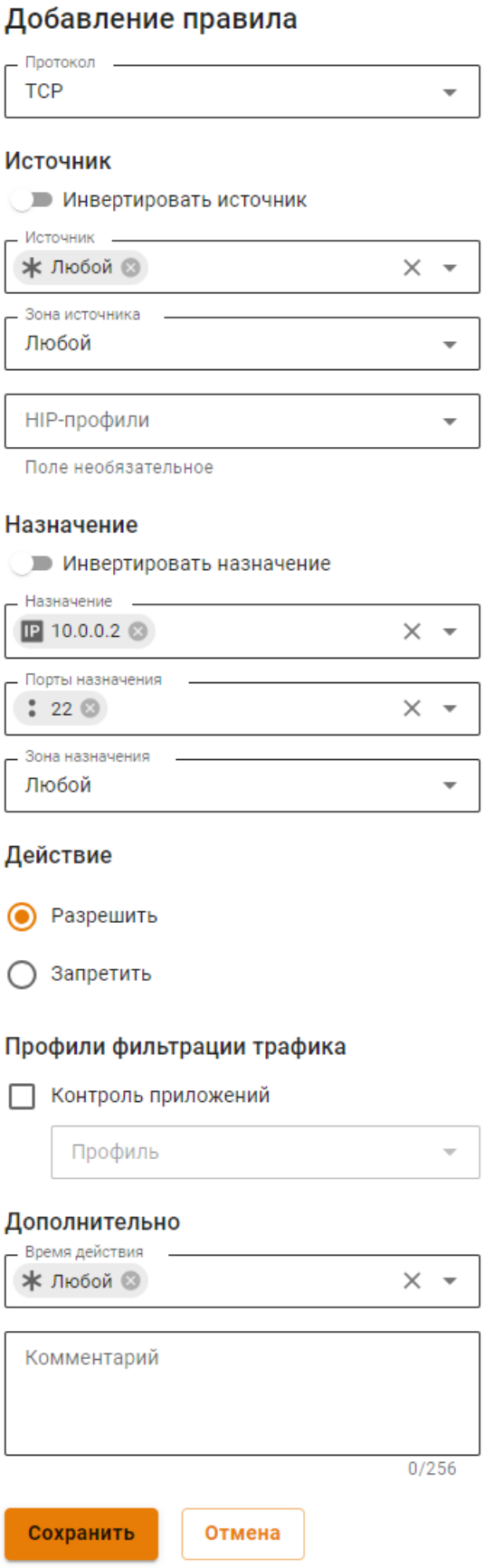
Заполните поля в соответствии с характеристиками, указанными в примере:



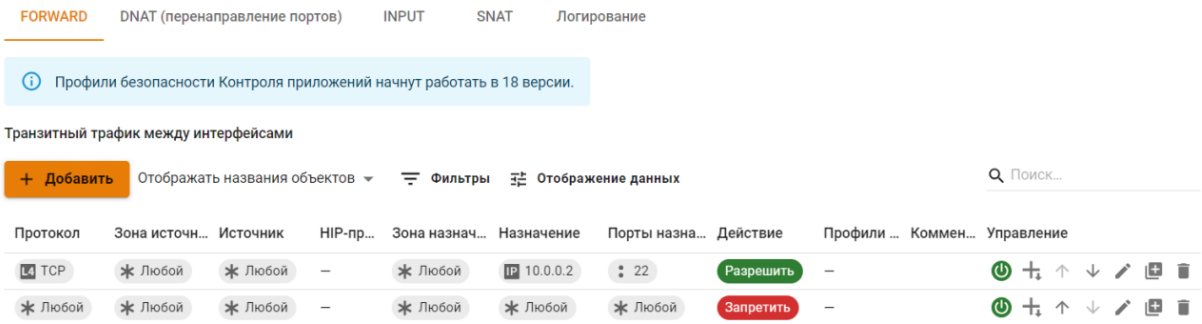
После сохранения созданное правило будет выглядеть следующим образом:



Проверьте наличие запрещающих правил в таблице FORWARD. При необходимости создайте правило, разрешающее трафик:



Поместите созданное правило выше запрещающего:



Настройки **Файрвола** применяются сразу при создании правил.

Частые ошибки:

- Если включен режим **Разрешить интернет всем**, правила **Файрвола**, включая таблицу DNAT, не работают;
- Если в одной локальной сети находятся пользователи и сервер с опубликованным при помощи DNAT-правила ресурсом, вероятна асимметричная маршрутизация. Информация о способах устранения асимметричной маршрутизации трафика представлена в *статье*.

Рекомендации:

- Проверять работу правила DNAT следует из внешней сети. Если необходим доступ из локальной сети, используйте обратный прокси-сервер для публикации веб-ресурсов;
- Порт на внешнем интерфейсе сервера, с которого транслируются запросы, не всегда совпадает с публикуемым портом самой службы. Например, для предотвращения автоматических попыток подключения вредоносного ПО на популярный сервис внешние запросы транслируются на порт 4489, а в локальную сеть - на порт 3389;
- Для защиты от нежелательных подключений к публикуемой службе при создании правила укажите в поле **Источник** IP-адрес или подсеть, с которой разрешено подключаться к этой службе;
- Если трансляция осуществляется 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 сработавшее правило в исключения.

23. Интеграция NGFW и SkyDNS

Подсказка: Если сайт неправильно категоризирован, воспользуйтесь формой обратной связи SkyDNS.

23.1 Чем может быть полезна интеграция:

- **Защита от зараженных сайтов**. Вредоносные скрипты могут содержать сайты, как взломанные злоумышленниками, так и созданные специально для распространения вредоносного ПО.
- **Защита от бот-сетей**. Созданные из зараженных вредоносными программами компьютеров сети используются в DDoS-атаках на серверы, рассылках спама, похищениях паролей от интернет-банков и сервисов и в других целях. DNS-фильтрация ограничивает доступ к выявленным серверам для управления бот-сетями. В результате злоумышленники не смогут управлять компьютером, даже если он заражен вредоносной программой.
- **Защита от нежелательных сайтов**. SkyDNS фильтрует интернет-ресурсы по более чем 50 категориям, что повышает качество фильтрации нежелательного контента.
- **Соблюдение 436-ФЗ О защите детей от информации, причиняющей вред их здоровью и развитию**. Сервис SkyDNS полностью соответствует требованиям Правил подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети интернет Минобрнауки РФ.

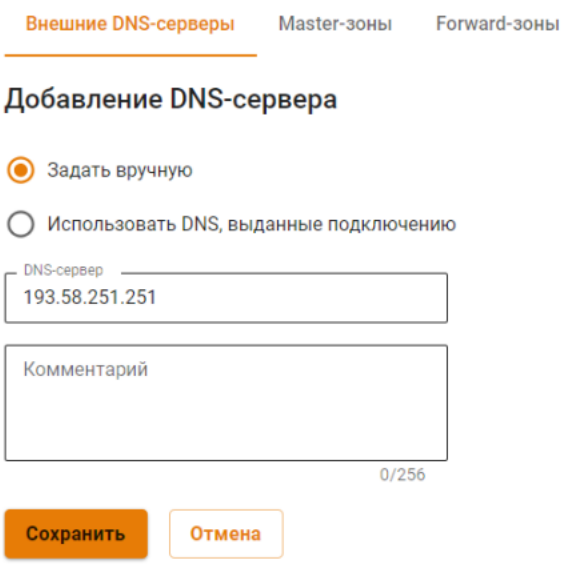
Подсказка: Специально для школ и колледжей можно приобрести комплект Шлюз безопасности Ideco NGFW + контент-фильтр SkyDNS.

23.2 Настройка интеграции Ideco NGFW и SkyDNS

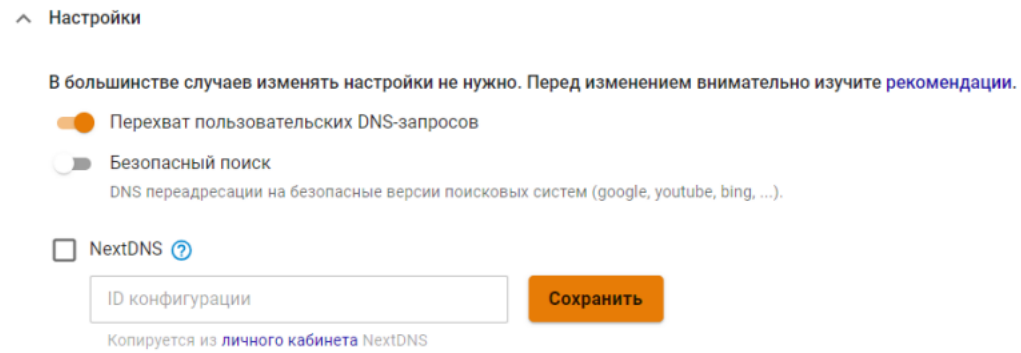
Чтобы настроить интеграцию со SkyDNS, выполните действия:

1. Перейдите в раздел **Сервисы -> DNS -> Внешние DNS-серверы** и нажмите **Добавить**.

2. Выберите пункт **Задать вручную** и в поле **DNS-сервер** введите IP-адрес DNS-сервера SkyDNS (`193.58.251.251`) и нажмите **Сохранить**:

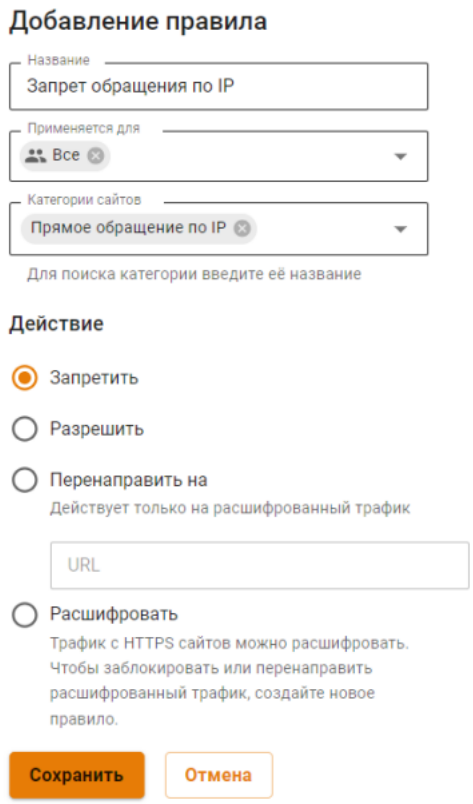


3. В настройках DNS включите опцию **Перехват пользовательских DNS-запросов** для запрета обращения к другим DNS-серверам (если фильтрация через SkyDNS обязательна для всей сети):



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.

23.3 Документация по настройке и активации сервиса SkyDNS

Документация доступна на сайте сервиса.

По вопросам настройки сервиса обращайтесь в техническую поддержку SkyDNS.

23.4 Схема фильтрации веб-трафика при использовании SkyDNS



24. О личном кабинете MY.IDECO

MY.IDECO - это личный кабинет, где вы можете использовать все возможности Ideco NGFW: скачать дистрибутив, добавить лицензию, привязать телеграм-аккаунт к мониторинг-боту и получать мгновенные уведомления о работе Ideco NGFW и многое другое.

24.1 Возможности Ideco NGFW:

- Управлять лицензированием серверов
- Скачивать дистрибутивы
- Привязывать телеграм-аккаунт для получения уведомлений о состоянии работы серверов
- Добавлять компании в учетную запись для управления лицензированием
- Добавлять пользователей в компанию для управления лицензированием
- Настраивать авторизацию в MY.IDECO через социальные сети

25. NGFW

25.1 Лицензирование

Подсказка: Подробнее о видах лицензий в статье *Лицензирование*.

Посмотреть информации о сервере и лицензии можно в разделе **NGFW -> Лицензирование**, нажав на иконку 👁 напротив нужного сервера.

Информация о лицензии содержит сведения о сроке действия лицензии, количестве пользователей, сроке окончания обновлений, технической поддержки продукта и др.

25.1.1 Добавление коммерческой (Enterprise) лицензии

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

2. Перейдите в личный кабинет MY.IDECO в раздел **NGFW -> Лицензирование** и нажмите **Добавить коммерческую лицензию**.

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

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

25.1.2 Добавление FREE (бесплатной) лицензии

Для добавления FREE-лицензии нажмите кнопку **Добавить бесплатную лицензию** в разделе **Лицензирование**. Добавленная лицензия отобразится в таблице **Свободные лицензии**.

25.1.3 Привязка лицензии к серверу

Привязать лицензию к серверу можно двумя способами - онлайн и офлайн. Онлайн проводится только в MY.IDECO. Офлайн потребует доступ к веб-интерфейсу сервера.

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

- Одна лицензия может быть привязана только к одному серверу;
- Демо-лицензию нельзя привязать к другому серверу;
- Демо-лицензию нельзя повторно получить на одну и ту же инсталляцию сервера;
- При удалении сервера с демо-лицензией также удаляется и лицензия.

Онлайн

Выберите удобный вариант привязки:

- На вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения, нажав **Привязать лицензию**.
- На вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

Офлайн

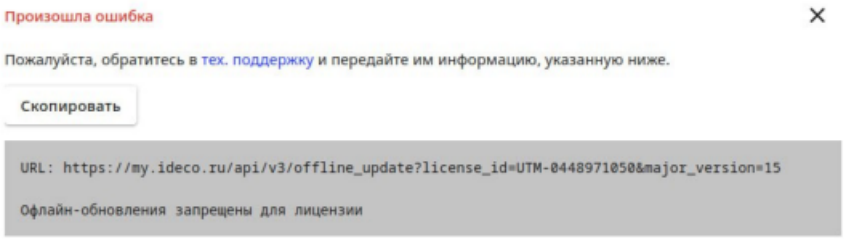
1. Для предоставления офлайн-лицензии обратитесь к менеджеру.

2. Привяжите предоставленную лицензию к серверу:

- На вкладке **Лицензирование** нажмите ПРИВЯЗАТЬ ЛИЦЕНЗИЮ. Далее в открывшемся окне выберите нужную лицензию и сохраните изменения, нажав **Привязать лицензию**.
- На вкладке **Лицензирование** выберите **Свободные лицензии** и нажмите . Далее укажите нужный сервер и сохраните изменения, нажав **Привязать**.

Пример наименования сервера для **офлайн**-регистрации: `UTM (UTM Unknown)`

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



3. Сформируйте ссылку на скачивание баз и лицензии, перейдите по ней на устройстве с доступом в интернет (подробнее - в *статье*.

Пример ссылки на регистрацию:

```
https://my.ideco.ru/ngfw?offline-updates&version={"major": 17, "minor": 5, "build":␣
↪102, "timestamp": 1724427324, "vendor": "Ideco", "product": "UTM", "kind": "STANDARD
↪", "release_type": "release"}&hwid=sGs6OYW2XRm_aK9PRwifKnej3V8YUVw69dtKVkIoPEnD
```

4. Сохраните файлы лицензии и баз фильтрации, нажав на появившиеся ссылки:



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.

25.2 Скачать

Вкладка содержит установочные файлы последних версий разработанных компанией «Айдеко» программных продуктов и их краткое описание.

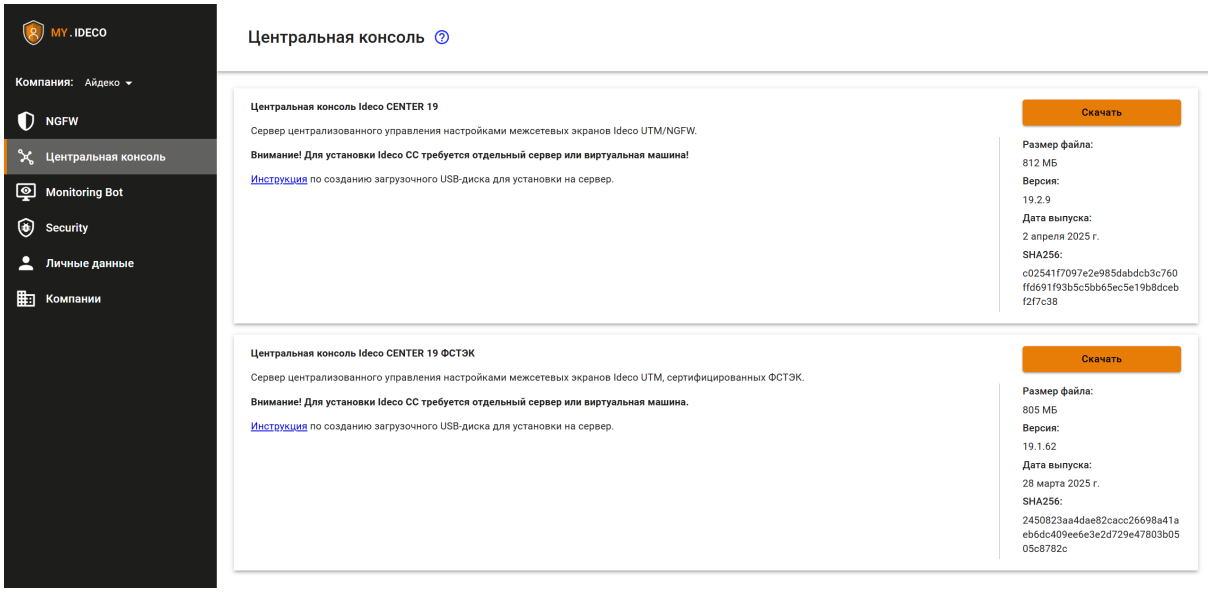
25.3 Online-демо

Чтобы ознакомиться с демоверсией Ideco NGFW, перейдите в раздел **NGFW -> Online-демо** личного кабинета MY.IDECO. Перейдите по ссылке **Реквизиты для доступа на демо-сайт** и введите логин `administrator` и пароль `servicemode`.

Демоверсия Ideco NGFW всегда равна последней реализованной версии. Учетная запись, доступная по логину и паролю выше, имеет права только на просмотр интерфейса. Если необходима учетная запись с правами на редактирование, обратитесь в отдел продаж.

26. Центральная консоль

В MY.IDECO доступно скачивание центральной консоли Ideco Center:



Ideco Center не требует лицензирования, не имеет ограничений к использованию и автоматически распространяет политики безопасности на все подключенные Ideco NGFW.

Подсказка: Для скачивания доступна как обычная, так и ФСТЭК версия.

26.1 Полезные ссылки

- *Создание загрузочного USB-диска для установки на сервер*
- *Установка Ideco Center*
- *Подключение Ideco Center к Ideco NGFW*

27. Monitoring Bot и Security

27.1 Monitoring Bot

Ideco Monitoring Bot присылает уведомления о событиях в Ideco NGFW (уведомления из колокольчика).

Бот может отправлять оповещения:

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

27.1.1 Привязка Ideco Monitoring Bot

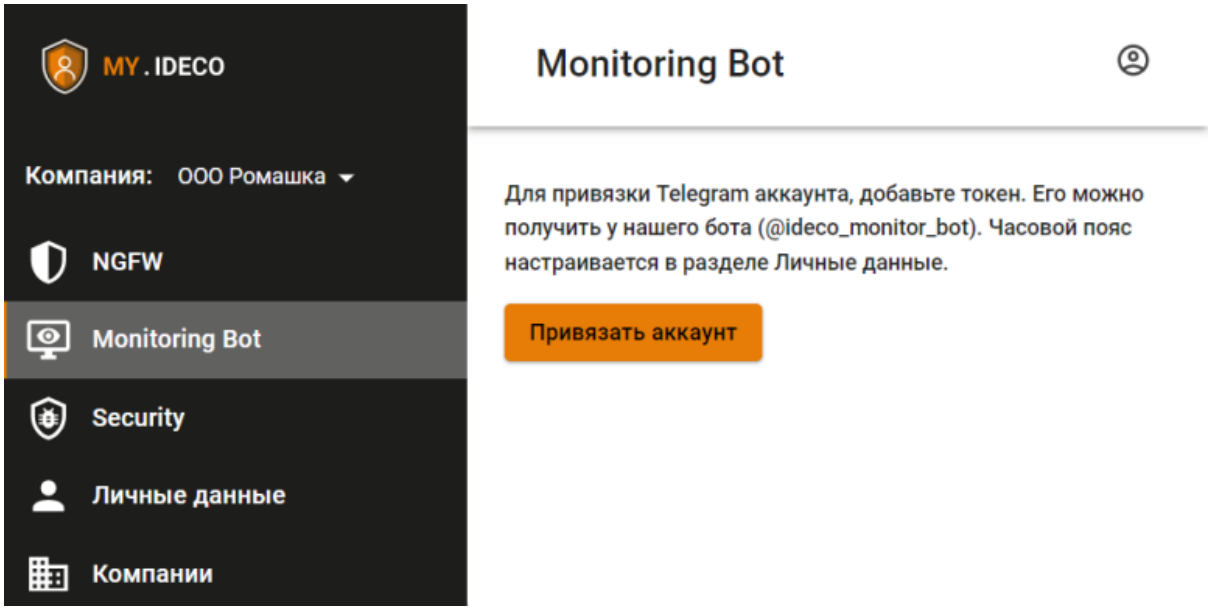
Настройка привязки Ideco Monitoring Bot к одному пользователю:

1. Настроить интернет на Ideco NGFW.
2. *Привязать лицензию* к серверу.
3. Перейти к диалогу с ботом: @ideco_monitor_bot.
4. Написать боту `/start`.
5. Скопировать код привязки к аккаунту.

6. Перейти в раздел **Ideco Monitoring Bot** в личном кабинете.

7. Нажать на кнопку **Привязать аккаунт**.

8. Ввести код в соответствующее поле и нажать на кнопку **Привязать**.



Настройка привязки Ideco Monitoring Bot к беседе:

1. Настроить интернет на Ideco NGFW.

2. *Привязать лицензию* к серверу.

3. Перейти в группу и добавить пользователя @ideco_monitor_bot.

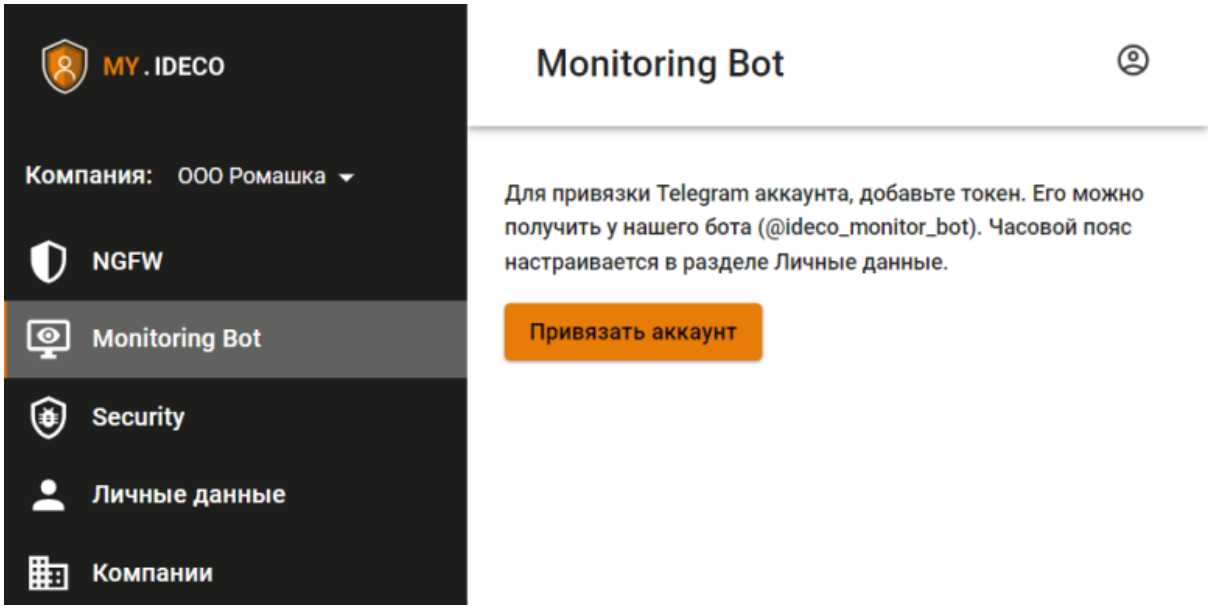
4. Написать `/start` в группе.

5. Скопировать код привязки к аккаунту.

6. Перейти в раздел **Ideco Monitoring Bot**.

7. Нажать на кнопку **Привязать аккаунт**.

8. Ввести код в соответствующее поле и нажать на кнопку **Привязать**.



Подсказка: При настройке подключения Ideco Monitoring Bot к беседе нельзя использовать подсказки для команд, поскольку требуется ввод команды `/start` вручную.

Подсказка: Уведомления начнут приходить в сообщения привязанного аккаунта.

27.1.2 Настройка оповещений Ideco Monitoring Bot

Настройте оповещения, которые приходят от Ideco Monitoring Bot, для каждой отдельной беседы.

Для настройки оповещений:

1. Перейдите в раздел Ideco Monitoring Bot в личном кабинете и нажмите на иконку .

2. Выберите уведомления, которые хотели бы получать в выбранной беседе.

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

27.2 Security

Онлайн-сервис для проверки защиты сетевого периметра, оценки текущего уровня защиты и возможности повышения уровня защиты.

Сервис проверит:

- Есть ли доступ через используемый браузер к сайтам из 15 потенциально опасных категорий;
- Возможность проникновения тестовых образцов вирусов и эксплойтов;
- Открытые порты и ответы сервисов на внешнем интерфейсе вашего интернет-шлюза;
- Торренты, скачанные из сети за последний месяц;
- Есть ли ваш IP-адрес в черных списках зараженных хостов;
- Наличие пароля к почте в известных базах данных хакеров.

Подсказка: Чтобы оценить эффективность работы служб фильтрации и повысить уровень безопасности, рекомендуем ознакомиться с нашей статьей о сервисе *Security Ideco*.

28. Личные данные и Компании

В разделах меняются данные учетной записи, добавляются компании для управления в них лицензиями и пользователи для управления компаниями

28.1 Личные данные

Информация о профиле:

- E-mail - почта, используемая для авторизации;
- Телефон - телефон для звонков по вопросам продления лицензии;
- Временная зона - временная зона региона, в котором находится пользователь. Monitoring Bot будет указывать время в уведомлениях у учетом этой временной зоны.

Авторизация через социальные сети:
При добавлении авторизации через аккаунт социальной сети система получит доступ к имени, адресу электронной почты, языковым настройкам и фото профиля аккаунта.

Смена пароля:
Для смены пароля укажите старый и новый пароль.

28.2 Компании

Раздел содержит информацию о пользователях, добавленных в компанию, и настройки компании.

28.2.1 Добавление компании

Для добавления компании нажмите **Добавить компанию**, заполните название компании, выберите количество пользователей и нажмите **Создать**.

Способы переключения между компаниями:

- В разделе **Компании** в раскрывающемся списке;
- В левом верхнем углу по кнопке .

Чтобы изменить название и количество пользователей, перейдите в **Настройки компании**:

В правой части экрана измените необходимые параметры и нажмите **Сохранить**.

28.2.2 Добавление пользователей

Для добавления пользователя в компанию нажмите **Добавить пользователя**, укажите e-mail и нажмите **Добавить**.

Если у добавляемого пользователя нет учетной записи в MY.IDECO, то на указанную при добавлении электронную почту отправится письмо со ссылкой-приглашением. При переходе по ссылке откроется страница входа в MY.IDECO.
Для задания пароля потребуется нажать **Забыли пароль?** и пройти процедуру восстановления пароля, перейдя по ссылке из отправленного письма.

29. Об Ideco Center

29.1 Основное

Подсказка: Название службы раздела **Центральная консоль**: `ideco-central-console-backend`.
Список служб для других разделов доступен по *ссылке*.

Ideco Center - это центральная консоль, которая поможет в администрировании нескольких серверов Ideco NGFW. На данный момент не требует лицензирования и не имеет ограничений к использованию. Автоматически распространяет политики безопасности по всем подключенным Ideco NGFW, даже если они были подключены после того, как политики были настроены.

Возможности Ideco Center:

- Централизованное управление серверами, подключенными к Ideco Center, с возможностью группировки Ideco NGFW и формирования иерархии из этих групп для совместного управления;
- Создание правил политик безопасности и объектов, которые одновременно переносятся в серверы Ideco NGFW определенной группы. В частности - создание пользовательских категорий контент-фильтра;
- Переход из Ideco Center в веб-интерфейс подключенных Ideco NGFW. Администраторы Ideco Center имеют доступ к подключенными NGFW, но администраторы подключенных NGFW не имеют доступ к Ideco Center.
- Обновление подключенных к Ideco Center NGFW;
- Управление правами доступа администраторов серверов NGFW.

Подсказка: Подробнее о работе политик безопасности и объектов - в статье *Политики и объекты*.

Источники обновления данных для Ideco Center:

Ideco Center получает обновления из следующих источников:

- Отсылка уведомлений в личный кабинет/телеграм-бот: alerts.v17.ideco.dev;
- Обновление баз **Контент-фильтра**: content-filter.v17.ideco.dev;
- Отсылка анонимной статистики: gatherstat.v17.ideco.dev;
- Обновления баз GeoIP: ip-list.v17.ideco.dev;
- Отправка отчетов по почте: send-reports.v17.ideco.dev;
- Обновления системы: sysupdate.v17.ideco.dev;
- Синхронизация времени: ntp.ideco.ru.

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

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

---

30. Установка Ideco Center

Технические требования для серверов и виртуальных машин:

Комплектующие	Минимальные системные требования
Процессор	Intel i3/i5/i7/i9/Xeon с поддержкой SSE 4.2
Объем оперативной памяти	16 ГБ (16-64 ГБ в зависимости от количества пользователей)
Дисковая подсистема	SSD объемом 150 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe
Сеть	Одна сетевая карта. Рекомендуется использовать карты на чипах Intel
Гипервизоры	VMware, Microsoft Hyper-V (виртуальные машины 2-го поколения), VirtualBox, KVM, Citrix XenServer, Proxmox VE
Дополнительно	Монитор и клавиатура
Замечания	Обязательна поддержка UEFI. Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет). Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти

Подсказка: Обязательные условия для работы с Ideco Center:

1. Обязательная поддержка UEFI;
2. Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти;
3. Отключить режим Legacy загрузки, он может называться CSM (Compatability Support Module);
4. Отключить опцию Secure Boot в UEFI.

Файл для установки центральной консоли доступен для скачивания в личном кабинете. Процесс установки Ideco Center аналогичен *процессу установки Ideco NGFW*.

30.1 Процесс установки

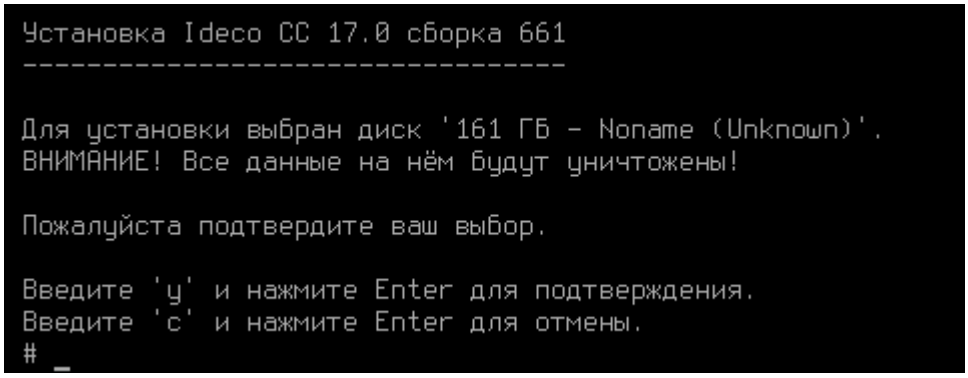
Подсказка: При установке Ideco Center с загрузочного USB диска выберите загрузку с USB диска в настройках UEFI компьютера.

Для установки Ideco Center выполните действия:

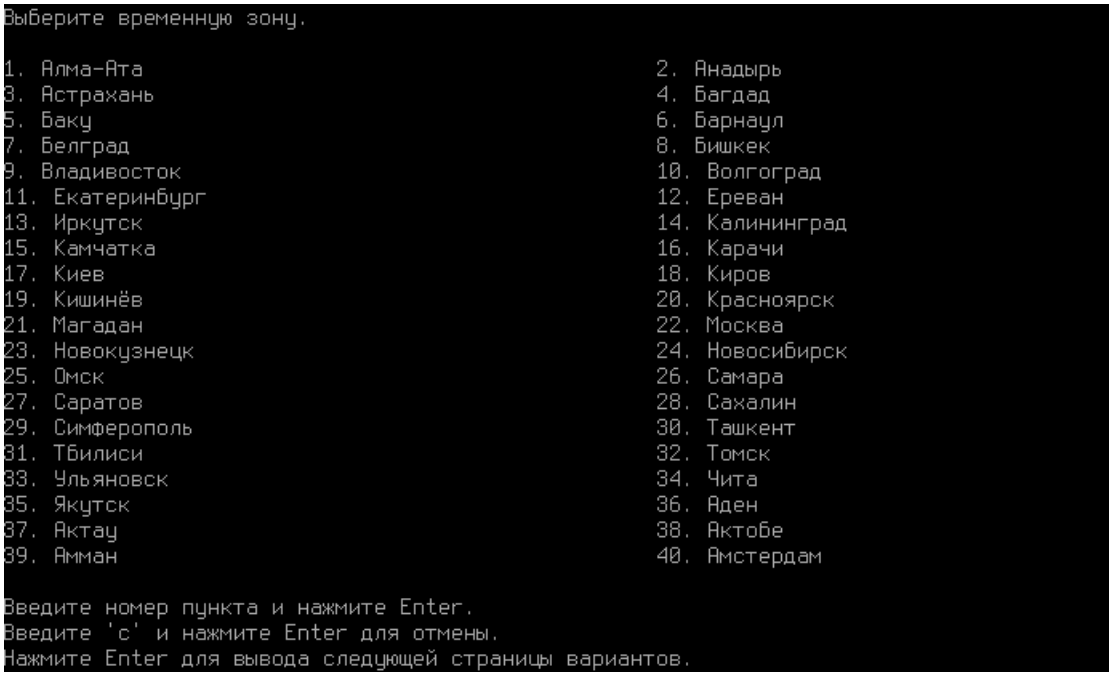
1. Перейдите к установке, нажав **Install Ideco CC**.



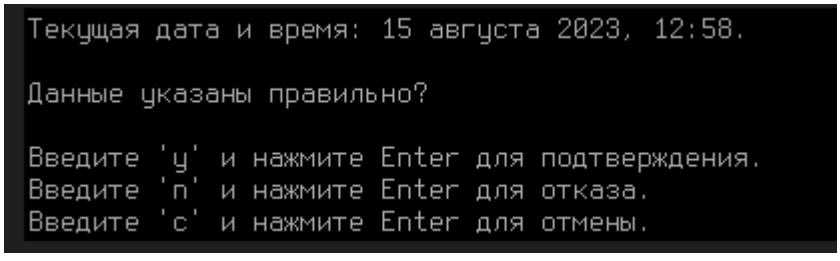
2. Выберите диск для установки и ознакомьтесь с **предупреждением об уничтожении данных на диске**:



3. Выберите временную зону, в которой вы находитесь:



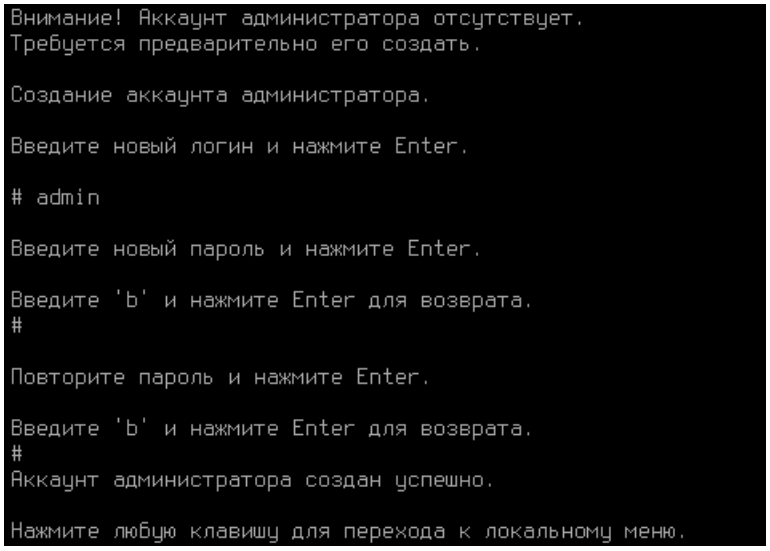
4. Настройте дату и время в соответствии с вашей временной зоной. **Обязательно проверьте правильность даты и времени**:



Подсказка: Не забудьте извлечь USB диск после установки Ideco Center, чтобы загрузка с USB диска не началась заново.

30.2 Создание учетной записи администратора

Для входа в веб-интерфейс Ideco Center нужно создать учетную запись администратора с соблюдением требований к паролю:



Требования к паролю:

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

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

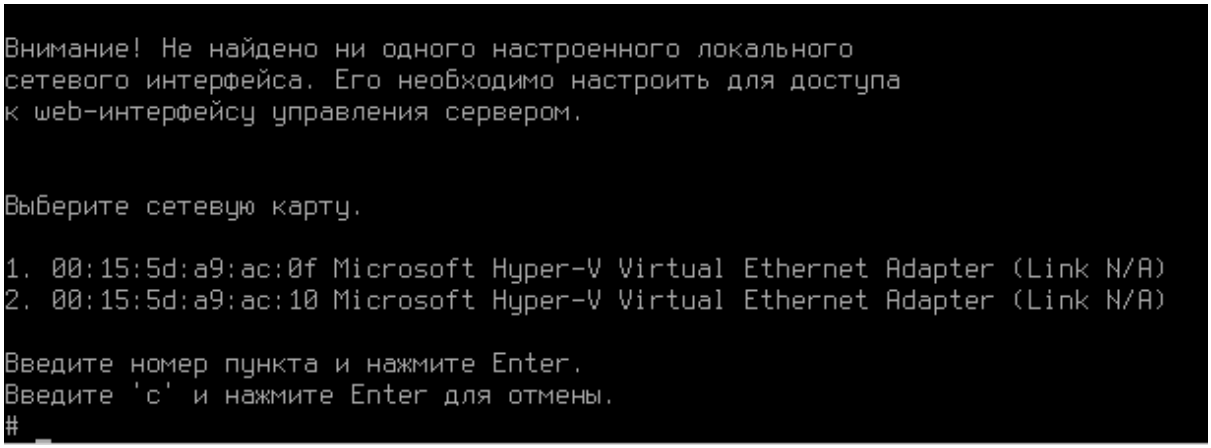
Не используйте Numpad при введении пароля, поскольку в будущем это может привести к проблемам при авторизации администратора.

30.3 Настройка локального интерфейса

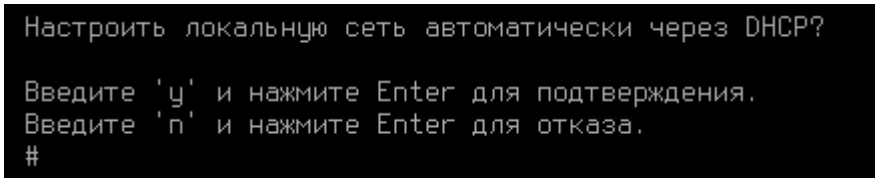
Подсказка: При использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса. Для корректной идентификации сетевой карты используйте ее MAC-адрес.

Для настройки Ideco Center через веб-интерфейс нужно настроить локальный интерфейс в локальном меню:

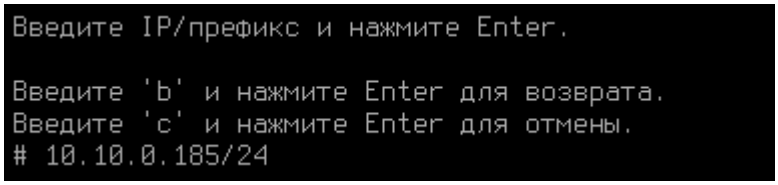
1. Введите номер сетевого адаптера, который будет использоваться в качестве локального сетевого интерфейса:



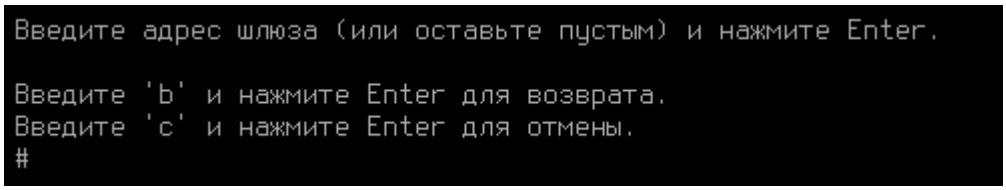
2. Настройте локальную сеть автоматически через DHCP, введя **y**, или настройте вручную, введя **n**:



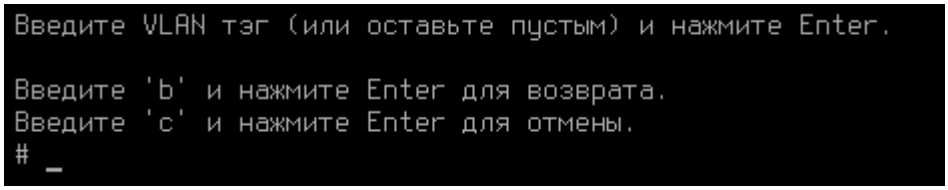
3. Введите локальный IP-адрес и маску подсети в формате `ip/маска` и нажмите **Enter**:



4. Введите адрес шлюза или оставьте поле пустым:



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



После создания локального интерфейса откроется локальное меню управления:

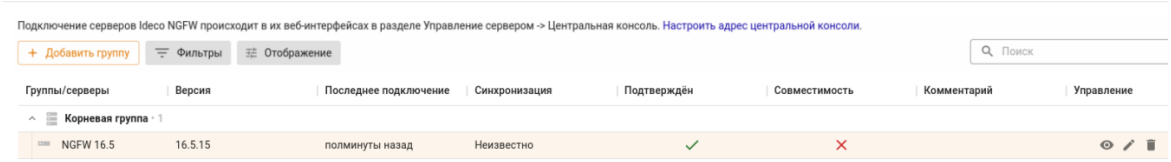
```
Управление сервером

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

Введите номер пункта и нажмите Enter.
#
```

31. Серверы

Внимание: При синхронизации Ideco Center и Ideco NGFW с разными мажорными версиями передача правил с Ideco Center происходить не будет. При этом в разделе **Серверы** будет информация о том, что Ideco Center и Ideco NGFW несовместимы:



В разделе **Серверы** можно группировать синхронизированные с ней серверы NGFW и формировать из них древовидную структуру. Это позволит управлять сразу несколькими серверами, применять правила и политики безопасности ко всем серверам определенной группы.

Предупреждение: Особенности работы:

- Если в подключаемом Ideco NGFW используется кластер, достаточно подключить только активную ноду, пассивная автоматически примет эту настройку;
- Сетевое подключение производится в направлении от Ideco NGFW к Ideco Center, т. е. возможна связь и когда Ideco NGFW за NAT;
- Если сервер Ideco Center находится за NAT, укажите IP-адрес NAT-устройства или доменное имя в разделе **Управление сервером -> Дополнительно -> Адрес центральной консоли**;
- Для обновления серверов, подключенных к центральной консоли, перейдите в интерфейс NGFW одним из указанных выше способов и воспользуйтесь статьей *Автоматическое обновление сервера*;
- Для подключения нескольких Ideco NGFW к Ideco Center рекомендуем настроить VPN-подключение через IPsec. Альтернативный способ - создать правило DNAT в веб-интерфейсе Ideco NGFW.

Портмаппинг при подключении Ideco NGFW к Ideco Center:

Если между офисами отсутствует VPN-подключение, для подключения нескольких Ideco NGFW к Ideco Center можно настроить проброс портов. Вместо подключения по IPsec в этом случае настраивается перенаправление портов.

Чтобы выполнить настройку, необходимо создать два одинаковых правила для протоколов **UDP** и **TCP** в разделе **Правила трафика -> Файрвол -> DNAT**:

Добавление правила

Протокол
UDP

Источник

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

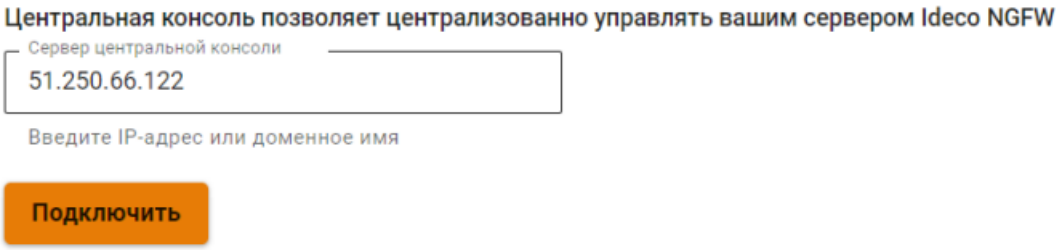
- **Назначение источника** - внешний IP-адрес Ideco NGFW;
- **Сменить IP-адрес назначения** - внутренний IP-адрес Ideco Center;
- **Порт** - только порт 3151.

При применении настроенного правила трафик проходит в локальную сеть через внешний интерфейс и перенаправляется в Ideco Center. При получении трафика Ideco Center отправляет подтверждение.

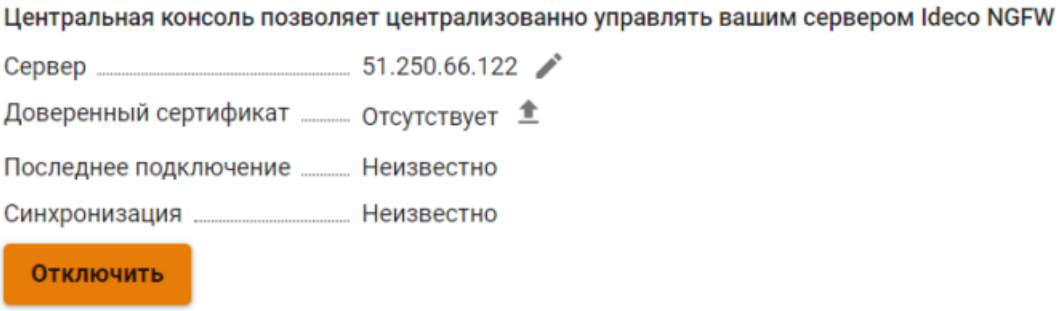
Подключение Ideco NGFW к Ideco Center:

1. Перейдите в раздел **Управление сервером -> Центральная консоль**;

2. Введите IP-адрес или доменное имя в строке **Сервер центральной консоли** и нажмите **Подключить**:

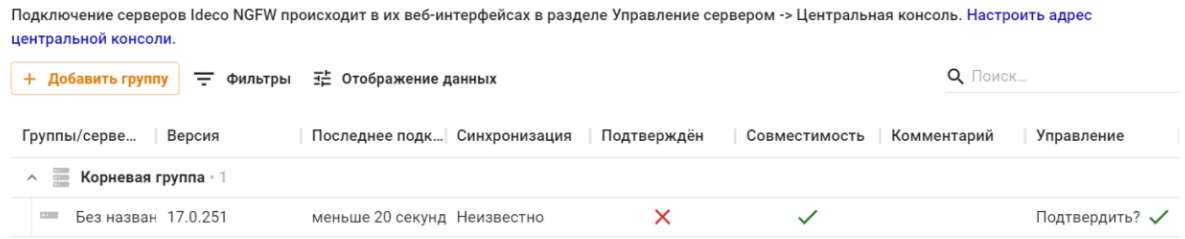


Если вместо доменного имени указан IP-адрес Ideco Center, загрузите корневой сертификат Ideco Center в Ideco NGFW:



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

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



Для удаления сервера Ideco NGFW из Ideco Center разорвите привязку в интерфейсе Ideco Center:

Для этого в таблице **Серверы** в столбце **Управление** напротив нужного сервера выберите 🗑 и подтвердите выбор.

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

В Ideco Center предусмотрено два способа перехода в Ideco NGFW:

1. Перейдите в раздел **Серверы** и нажмите на .В новой вкладке откроется веб-интерфейс Ideco NGFW:

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

Подсказка: Чтобы перейти к веб-интерфейсу VCE подключенных серверов в Ideco Center, выполните следующие действия:

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

2. Затем следуйте инструкциям из *статьи*.

31.2 Группировка серверов Ideco NGFW

Структура групп серверов в Ideco Center предполагает три уровня вложенности. Первый - Корневая группа. В нее по умолчанию попадают все серверы NGFW, впервые синхронизированные с Ideco Center, а также все группы, созданные администратором.

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

Подсказка: Серверы NGFW, подключенные к Ideco Center, и группы по умолчанию, созданные в центральной консоли, являются частью **корневой группы** и не могут быть вынесены оттуда.

31.2.1 Создание, редактирование и удаление групп серверов

Создание группы серверов:

1. Перейдите в раздел **Серверы** и нажмите **Добавить группу**.

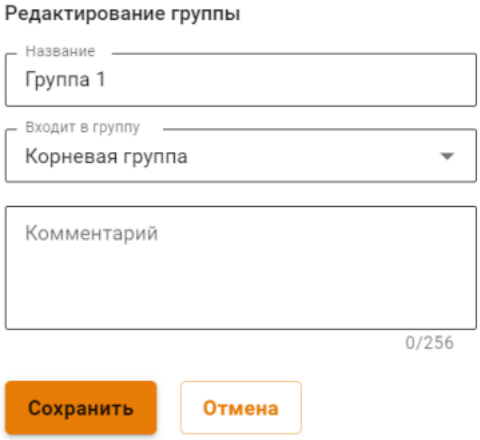
2. В открывшемся окне заполните **Название группы** и выберите родительскую группу из раскрывающегося списка (если это первая создаваемая группа, в нем будет только Корневая группа):

3. Нажмите **Сохранить**.

Редактирование группы серверов:

1. Нажмите на напротив ее названия.

2. В открывшемся окне можно изменить название и родительскую группу:



Удаление группы серверов:

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

31.2.2 Перемещение серверов Ideco NGFW между группами

Чтобы переместить синхронизированный с центральной консолью сервер Ideco NGFW из одной группы в другую, выполните действия:

1. Нажмите на напротив ее названия.

2. В открывшемся окне из раскрывающегося списка выберите группу, в которую хотите переместить сервер:

> **Предупреждение:** При подключении к Ideco Center сервера, настройки которого *восстановлены* из бекапа другого сервера, такой клон не появится в таблице серверов Ideco Center. Возникает конфликт с донором бекапа из-за одинакового claster_id.
>
> В случае возникновения такой проблемы обратитесь в *Техническую поддержку*.

32. Мониторинг

В этом разделе можно настроить интеграцию с системами SNMP или Zabbix для мониторинга устройств и систем.

32.1 SNMP

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

Протокол SNMP позволяет осуществлять мониторинг устройств и систем. С помощью протокола SNMP передается информация:

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

Подсказка: На сервере, с которым будет осуществляться соединение по SNMPv3, укажите алгоритмы Auth Algorithm MD5 и Crypto Algorithm AES.

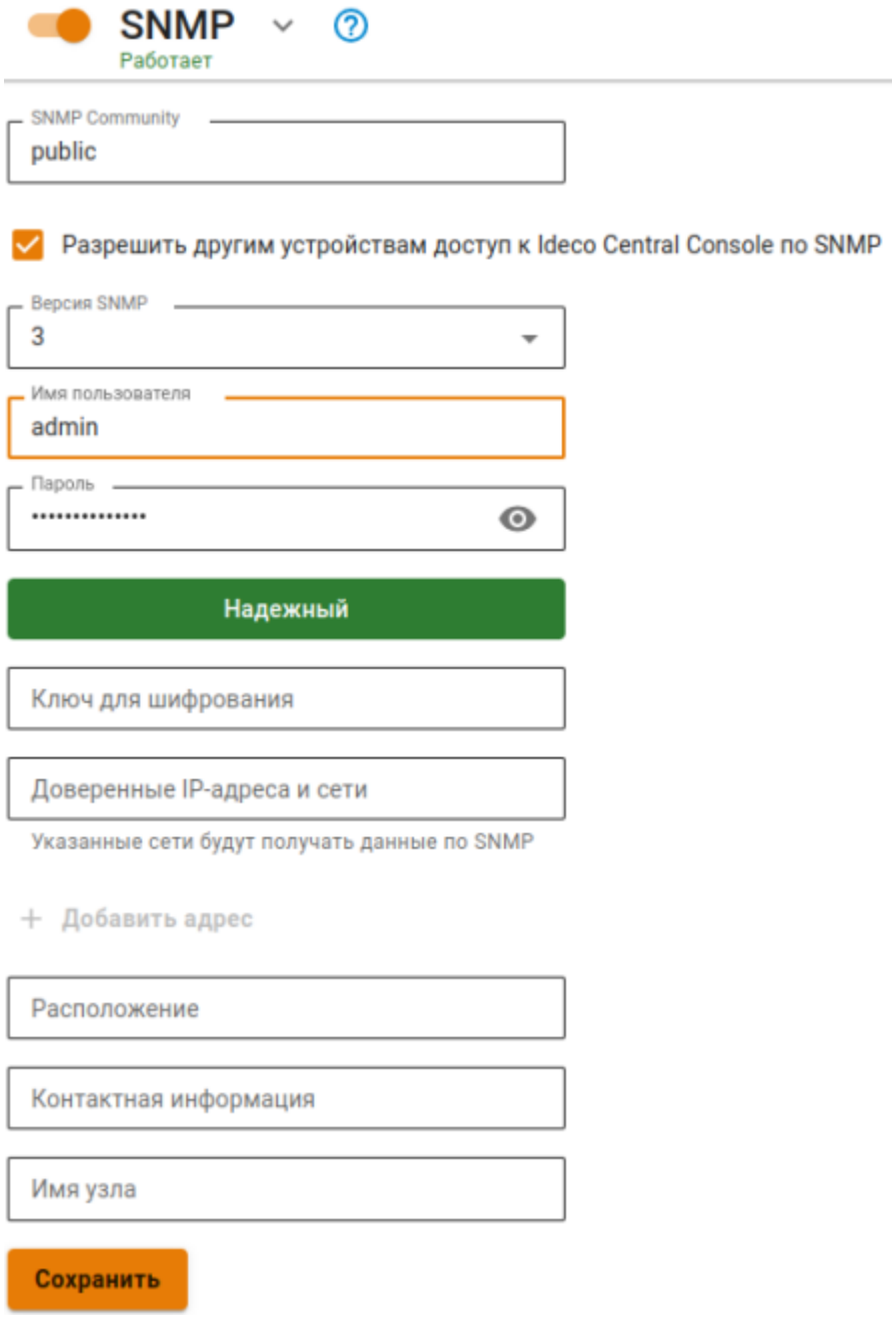
Для версии SNMPv1/v2 необязательно указывать поля **Имя**, **Пароль**, **Ключ шифрования**.

Поле SNMP community для SNMPv3 необязательно для заполнения.

Настройка SNMP:

1. Перейдите в раздел **Мониторинг -> SNMP**.

2. Активируйте опцию **Разрешить другим устройствам доступ к Ideco Central Console по SNMP** и заполните поля:



- **Версия SNMP** - версия протокола SNMP;
- **Имя пользователя** - имя пользователя для подключения по SNMP;

- **Пароль** - пароль для прохождения аутентификации;
- **Ключ для шифрования** - ключ, с помощью которого будет выполняться шифрование информации;
- **Доверенные IP-адреса и сети** - сети, в которые будут передаваться данные по SNMP;
- Поля **Расположение**, **Контактная информация** и **Имя узла** носят информационный характер и являются необязательными:

3. Нажмите **Сохранить** для завершения настройки.

32.2 Zabbix-агент

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

Ознакомиться с Zabbix можно на официальной странице Zabbix.

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

> **Предупреждение:** Для работы системы мониторинга Zabbix активируйте опцию **Zabbix-агент** после настройки интеграции с сервером.

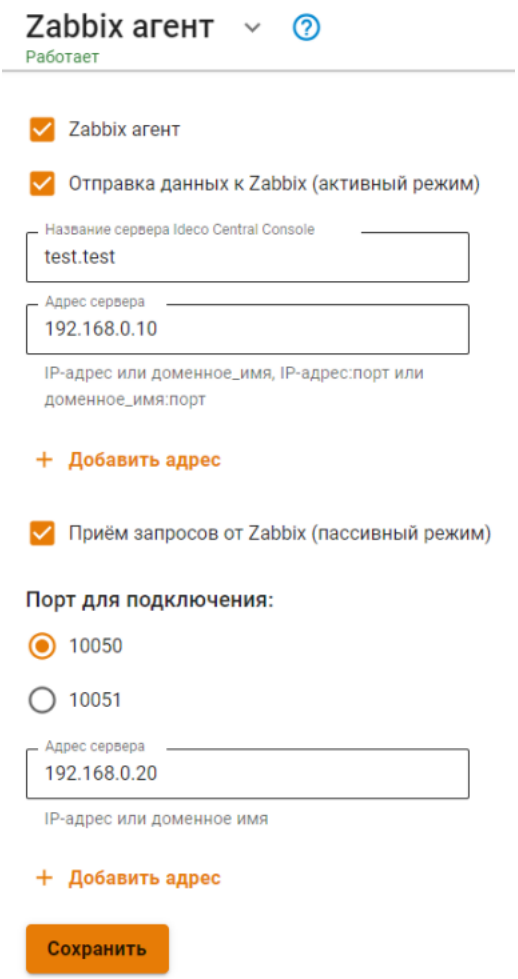
Настройка Zabbix-агент:

Интеграция с системой мониторинга Zabbix возможна в двух режимах:

1. **Активный режим** - соединение с Zabbix-сервером происходит со стороны Ideco Center. Для настройки этого режима заполните следующие поля:

- **Название сервера Ideco Central Console** - имя, которое будет отображаться на сервере мониторинга;
- **Адрес сервера** - IP-адрес, доменное имя, либо `IP-адрес:порт`, `доменное имя:порт`, если используется не стандартный для Zabbix входящий порт. Для добавления еще одного адреса нажмите на кнопку **Добавить адрес**.

2. **Пассивный режим** - подключение происходит со стороны Zabbix-сервера. Для настройки этого режима заполните следующие поля:



- **Порт для подключения** - выберите 10050 или 10051 порт;
- **Адрес сервера** - IP-адрес или доменное имя Zabbix-серверов. Для добавления еще одного адреса нажмите на кнопку **Добавить адрес**.

Zabbix-сервер может находиться как внутри локальной сети Ideco Center, так и за ее пределами. Подключение мониторинга возможно как к локальным, так и к внешним интерфейсам. В качестве шаблонов данных можно использовать стандартные шаблоны для Linux-серверов.

33. Политики и объекты

33.1 Политики безопасности

Управляйте объектами и правилами на всех подключенных Ideco NGFW одновременно.

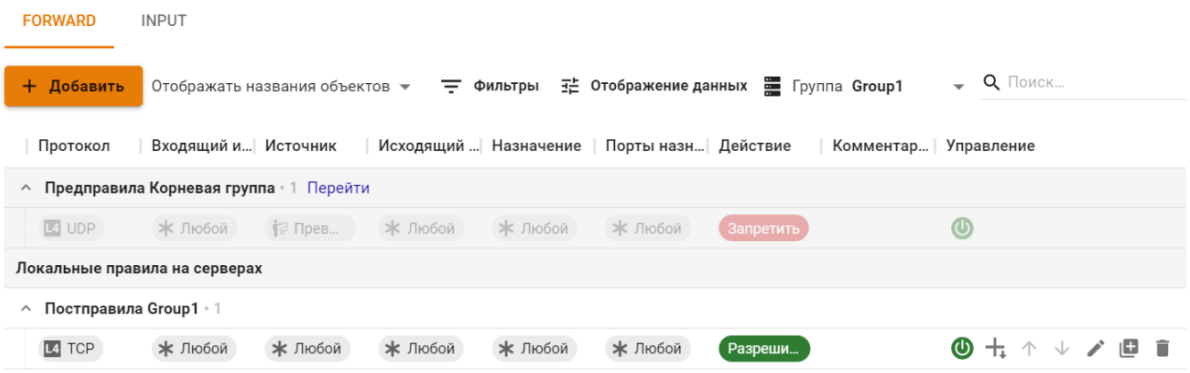
В разделе **Контент-фильтр** можно создать пользовательские категории на одноименной вкладке и использовать их для создания правил контентной фильтрации.

В Ideco NGFW из Ideco Center переносятся только те настройки, которые присутствуют в центральной консоли. Принципы работы разделов **Файрвол**, **Контроль приложений**, **Контент-фильтр** и **Ограничение скорости** с подключенными NGFW идентичен. Рассмотрим на примере раздела **Файрвол**.

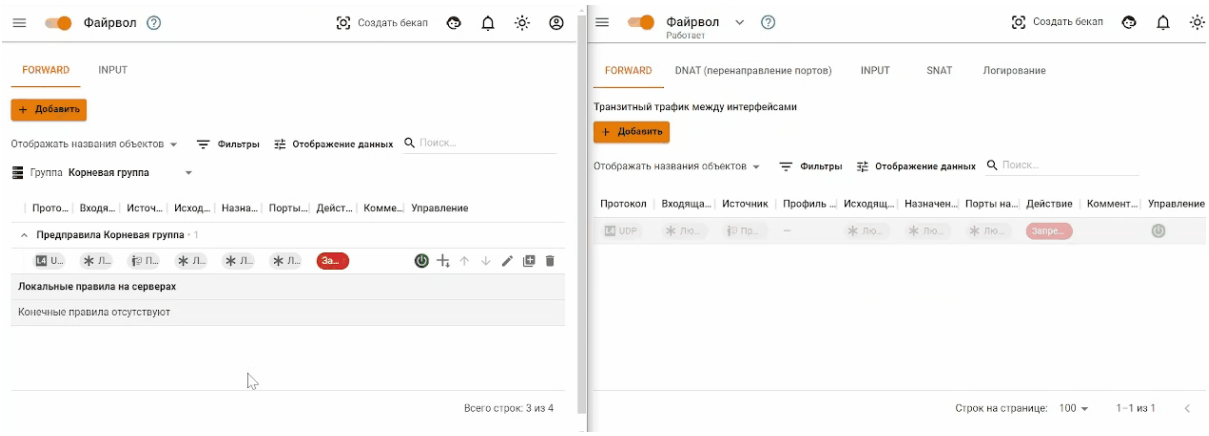
> **Предупреждение:** На Ideco NGFW будут распространяться правила и политики безопасности всех вышестоящих групп в соответствии с вложенностью. Правила **Корневой группы** распространяются на все подключенные NGFW.

33.1.1 Файрвол

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



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



В Ideco Center:

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

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

> **Предупреждение:** Перемещать правила между таблицами **Начальные правила** и **Конечные правила** нельзя.

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

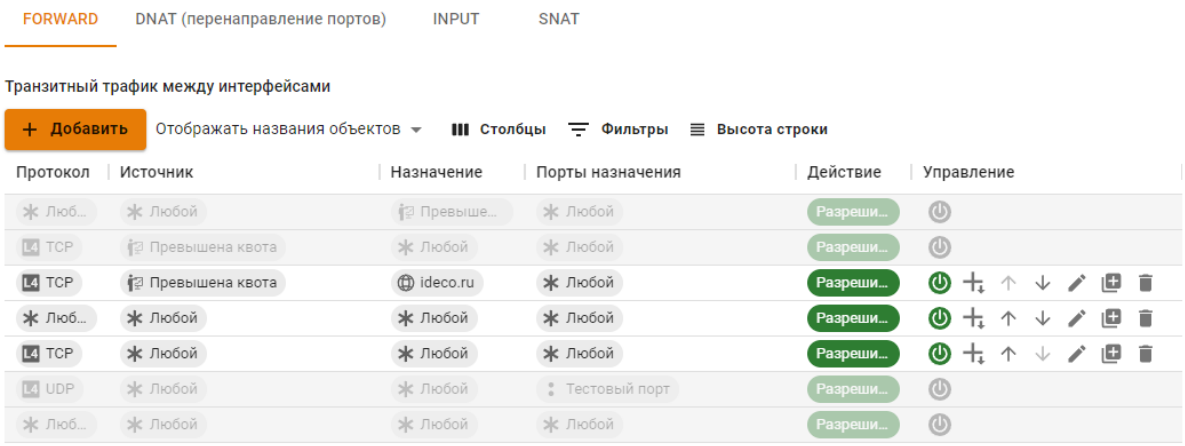
Чтобы увидеть все правила, распространяющиеся на группу серверов, выберите название группы в правом верхнем углу интерфейса:

В таблице отобразятся все правила, распространяющиеся на выбранную группу, с учетом вложенности групп.

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

В Ideco NGFW:

Таблица в Ideco NGFW визуально делится на три части: верхняя, средняя и нижняя.



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

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

Подсказка: Локальные правила на серверах Ideco NGFW не видны в интерфейсе Ideco Center.

Для просмотра перейдите в раздел **Серверы**, нажмите на в строке с нужным Ideco NGFW и перейдите в раздел **Файрвол**.

33.2 Объекты

Объекты, созданные в Ideco Center, переносятся в подключенные Ideco NGFW. Администратор Ideco NGFW может использовать эти объекты для создания правил.

При удалении объекта из Ideco Center, объект удаляется и из Ideco NGFW. Если в Ideco NGFW было создано правило с удаленным объектом, то этот объект будет отмечен иконкой 

.

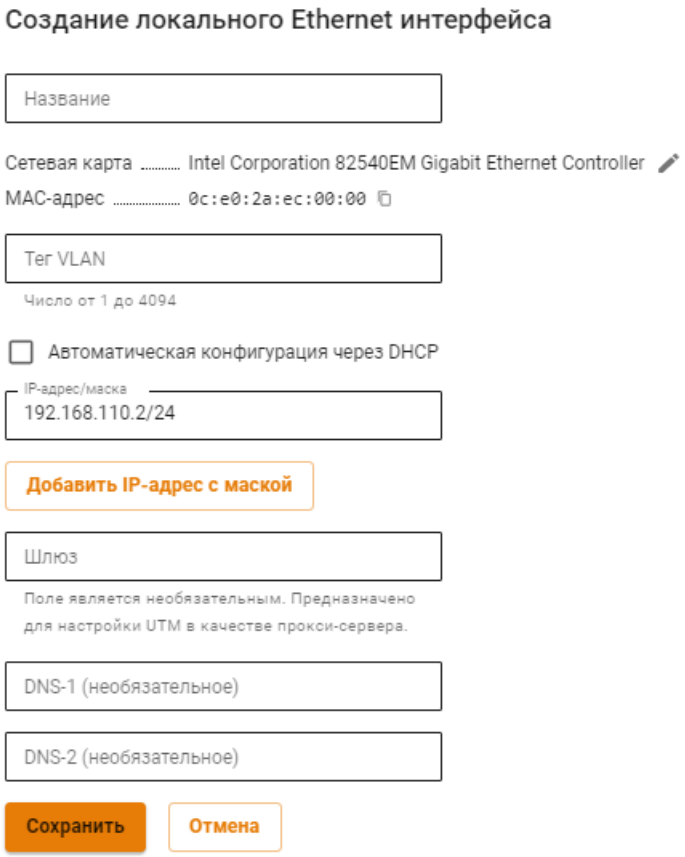
Подсказка: Принцип создания и удаления объектов в Ideco Center соответствуют принципам Ideco NGFW. Подробное описание в статье *Объекты*.

---

34. Сервисы

34.1 Сетевые интерфейсы

В отличие от Ideco NGFW, в Ideco Center создается только локальный Ethernet-интерфейс. Для этого нажмите **Добавить**, выберите сетевую карту и заполните нужные поля:



- **Название интерфейса** - имя для идентификации интерфейса;
- **Сетевая карта** - сетевой адаптер, который будет использоваться для подключения к интернет-провайдеру;
- **Тег VLAN**- VLAN ID. Такой сетевой интерфейс считается VLAN-интерфейсом. Заполняется в том случае если сетевая карта уже используется;
- **Автоматическая настройка через DHCP** - используйте, если интернет-провайдер поддерживает автоматическую настройку Ethernet-интерфейса с помощью протокола DHCP;
- **IP-адрес/маска** - назначьте на интерфейс минимум один IP-адрес. Если нужно, настройте интерфейс с несколькими IP-адресами;
- **Шлюз** - IP-адрес шлюза;
- **DNS** - доступно два поля для указания DNS сервера (необязательно).

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

34.2 Маршрутизация

Маршрутизация работает аналогично маршрутизации Ideco NGFW. Подробное описание по *ссылке*.

34.3 DNS

Принцип работы DNS в Ideco Center аналогичнен принципу работы *Внешних DNS-серверов* в Ideco NGFW. Если вышестоящий роутер перехватывает DNS-запросы Ideco Center, то добавьте внешние DNS-серверы.

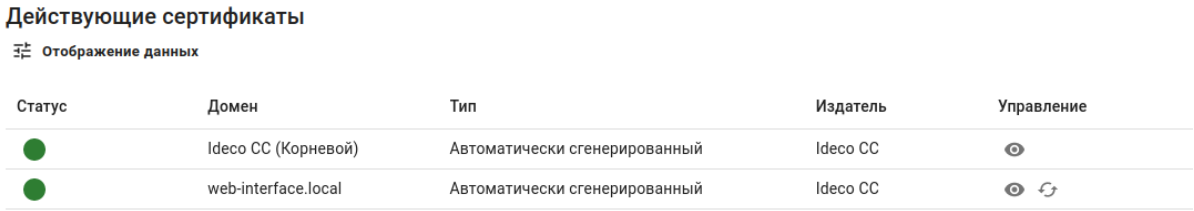
34.4 Сертификаты

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

Для просмотра основной информации о сертификате нажмите кнопку .

Процесс выпуска и перевыпуска сертификата одинаков с Ideco NGFW и описан в *статье*

34.4.1 Действующие сертификаты

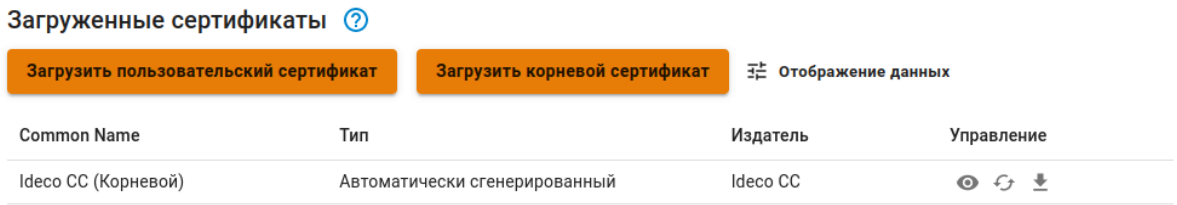


В таблице *Действующие сертификаты* отображаются:

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

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

34.4.2 Загруженные сертификаты



В таблице *Загруженные сертификаты* отображаются:

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

Подсказка: Загрузка SSL-сертификата на Ideco Center аналогична загрузке на Ideco NGFW. Подробная инструкция - в *статье*.

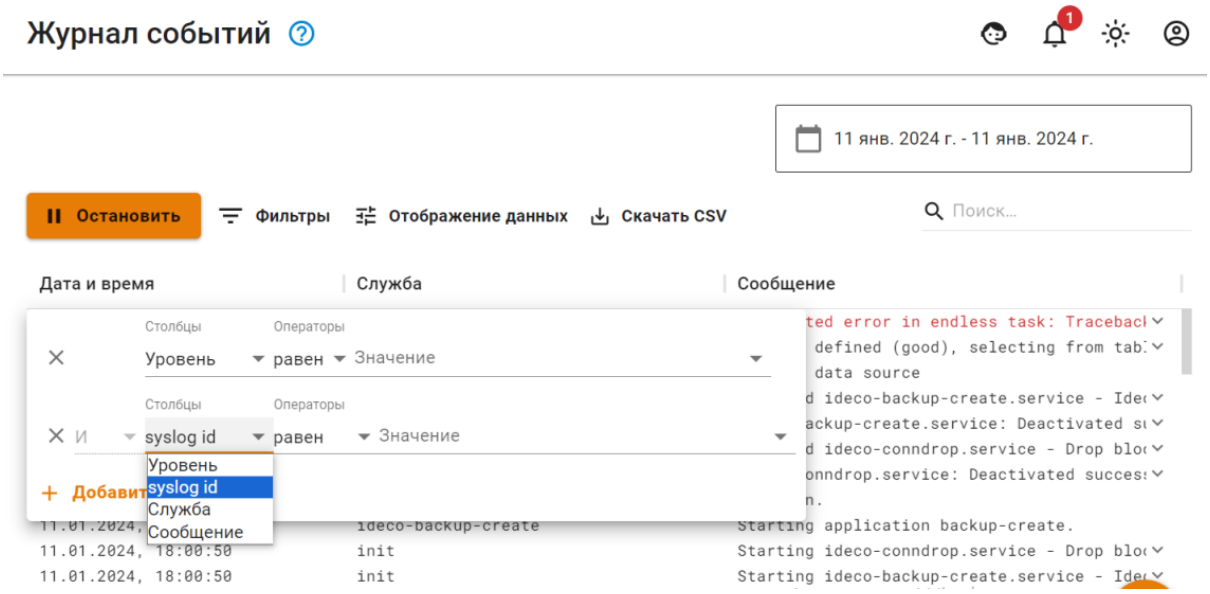
Подсказка: На Ideco Center можно загрузить самоподписанные сертификаты, созданные в *PowerShell* или *OpenSSL*.

35. Отчеты и журналы

35.1 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:



Подсказка: По кнопке **Скачать CSV** сохраняются те строки логов, которые заданы фильтрацией.

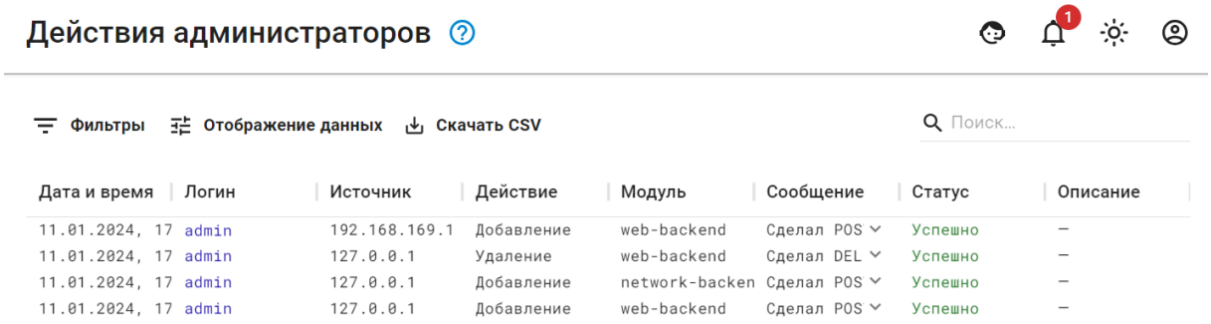
Список служб, доступных в разделе:

- **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;
- **Бекапы** - ideco-backup-backend, ideco-backup-create, ideco-backup-rotate;
- **Лицензия** - ideco-license-backend;
- **Syslog** - ideco-monitor-backend.

35.2 Действия администраторов

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



36. Управление сервером

В Ideco Center разделы *Автоматическое обновление*, *Резервное копирование* и *Терминал* аналогичны этим разделам в Ideco NGFW.

36.1 Администраторы

В Ideco Center можно создать несколько администраторов с разными ролями:

- **Администратор** - администратор с этой ролью имеет доступ ко всем функциональностям Ideco Center;
- **Только просмотр** - администратор с этой ролью не имеет возможности управлять правилами в Ideco Center (создавать, менять приоритет и др.).

Подсказка: Удалять подключенный Ideco NGFW из Ideco Center могут только администраторы с ролью **Администратор**.

Войти в подключенный Ideco NGFW с логином и паролем администратора Ideco Center **невозможно**.

36.2 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 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.

37. FAQ

37.1 Как заблокировать чат-боты?

Заблокировать чат-боты можно, создав правило в Контент-фильтре. О том, как это сделать, написано в статье *Блокировка чат-ботов*.

37.2 Как настроить совместную работу ViPNet-Координатора с Ideco NGFW ?

Процесс настройки подробно описан в *статье*.

37.3 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.

37.4 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*.

37.5 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*.

37.6 Какими модулями и в каком порядке обрабатывается веб-трафик в Ideco NGFW?

Порядок обработки веб-трафика и примеры проверки работоспособности модулей описаны в *статье*.

37.7 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.

37.8 Как создать VPN-подключение?

В зависимости от операционной системы выберите подходящую инструкцию из *Инструкций по созданию VPN-подключений*.

37.9 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*.

37.10 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*.

37.11 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*.

37.12 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*.

37.13 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.

37.14 Как подобрать аппаратную платформу для Ideco NGFW?

Ideco NGFW представляет собой операционную систему, устанавливаемую на сервер или виртуальную машину. Ideco NGFW основан на Fedora 39 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 39. Подробнее в статье *Выбор аппаратной платформы для Ideco NGFW*.

37.15 Есть необходимость использовать устаревшие алгоритмы шифрования. Как настроить Ideco NGFW?

Для настройки Ideco NGFW воспользуйтесь рекомендациями из статьи *Поддержка устаревших алгоритмов шифрования*.

37.16 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*.

37.17 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*.

37.18 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.

37.19 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*.

37.20 Инструкции по созданию VPN-подключений

37.20.1 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.

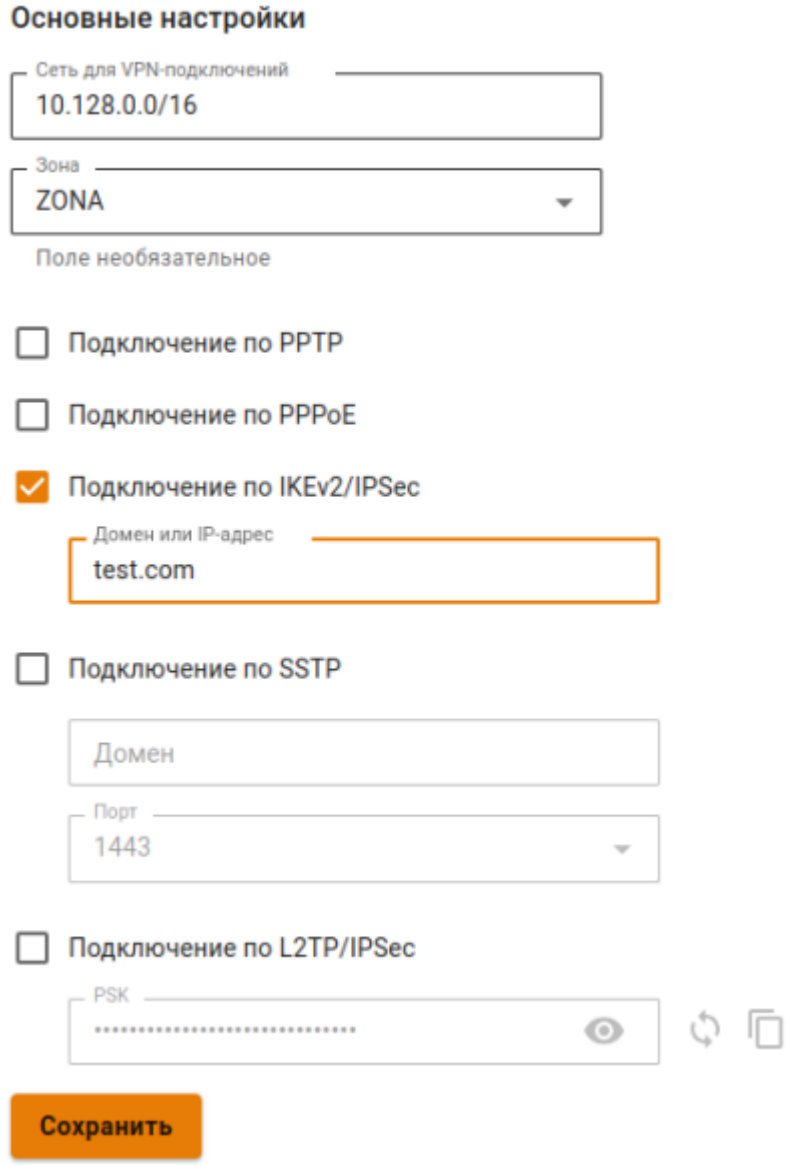
> **Предупреждение:** Не рекомендуем использовать для VPN-подключений кириллические логины.

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:

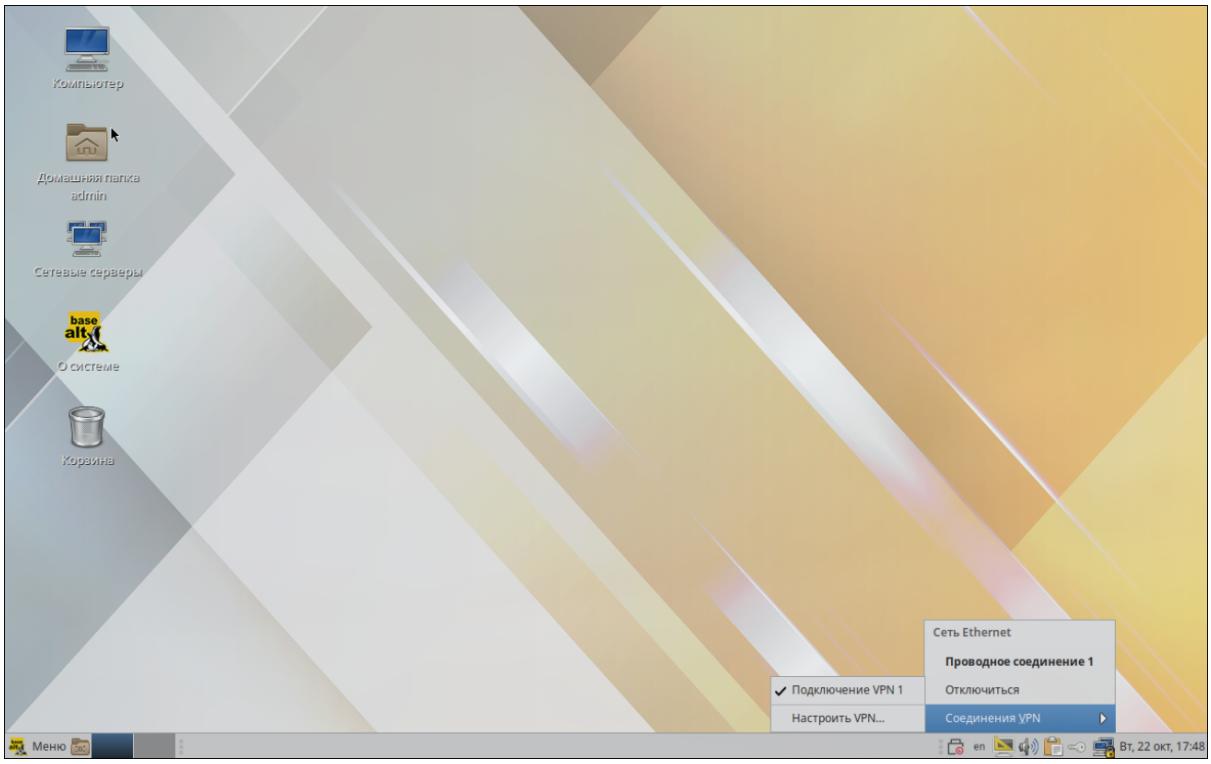
```
apt-get update && apt-get dist-upgrade && apt-get install NetworkManager-strongswan␣
↪NetworkManager-strongswan-gnome strongswan strongswan-charon-nm strongswan-testing
```

2. Установите корневой сертификат на рабочую станцию:

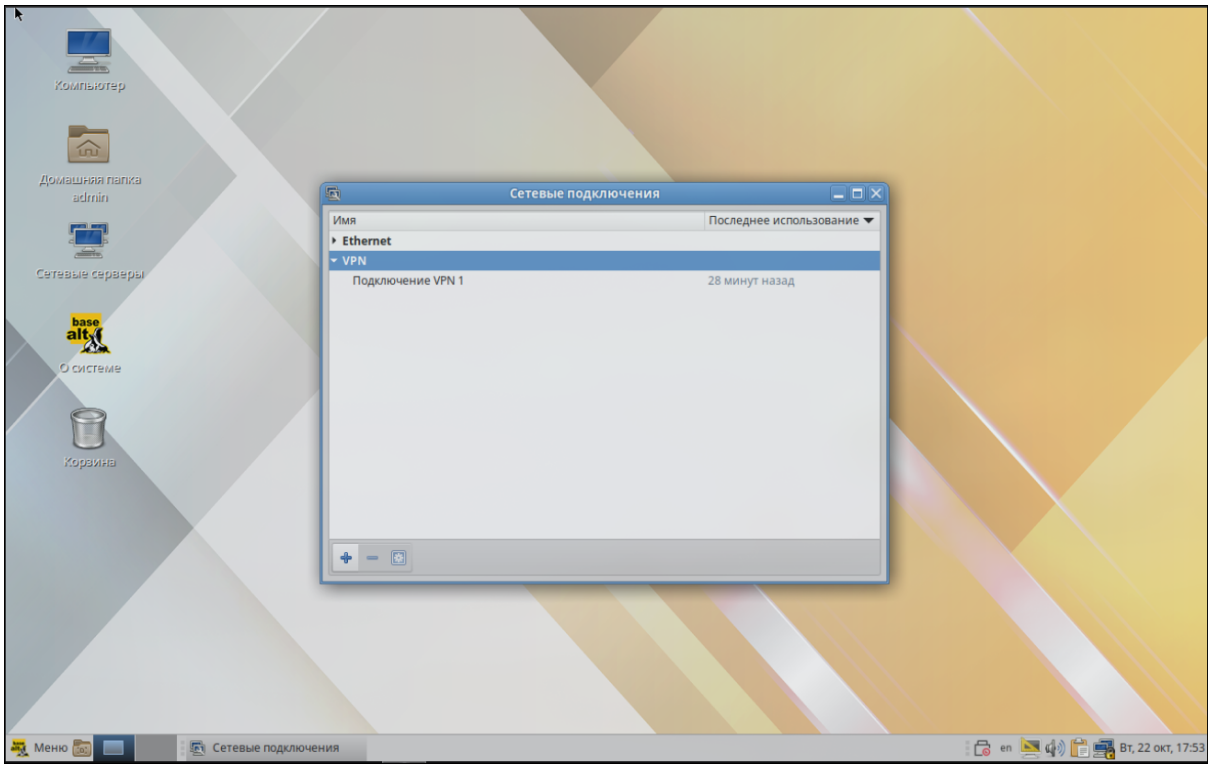
```
cp root-ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

- `root-ca.crt` - путь к сертификату.

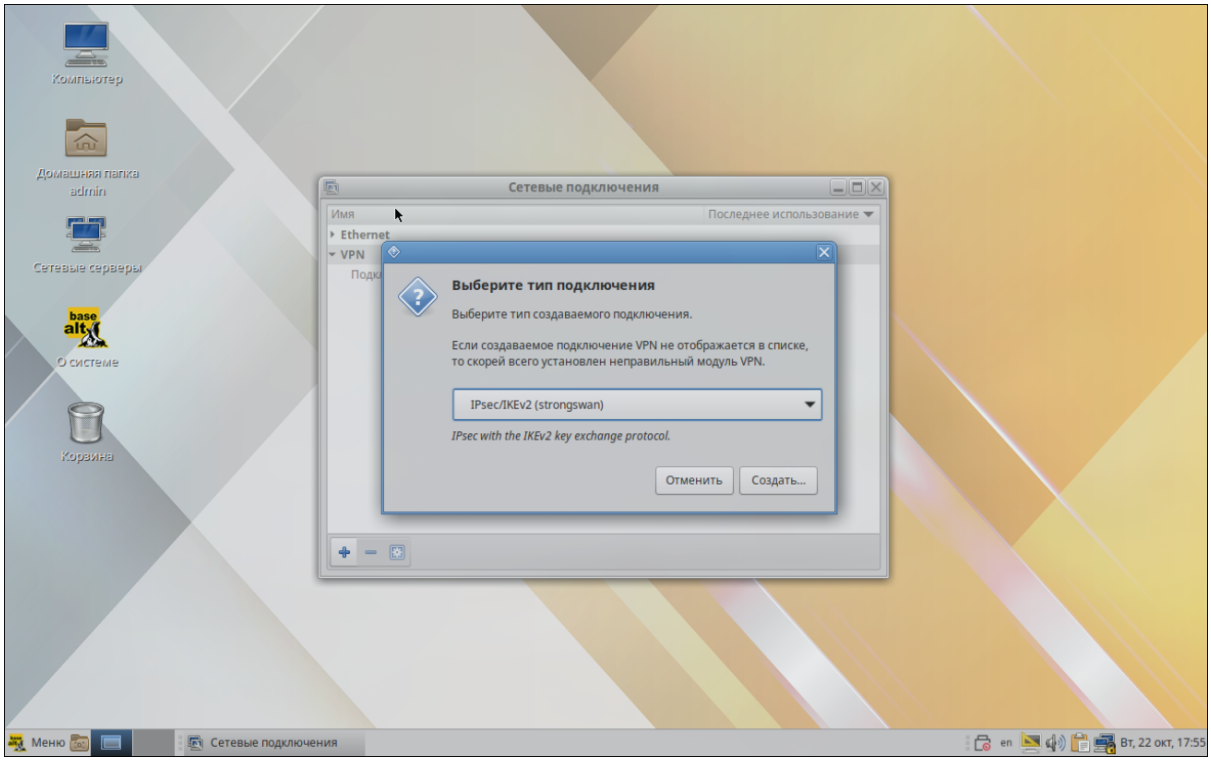
3. Перейдите в **Соединения VPN** и нажмите **Настроить VPN**:



4. Добавьте новое VPN-подключение:

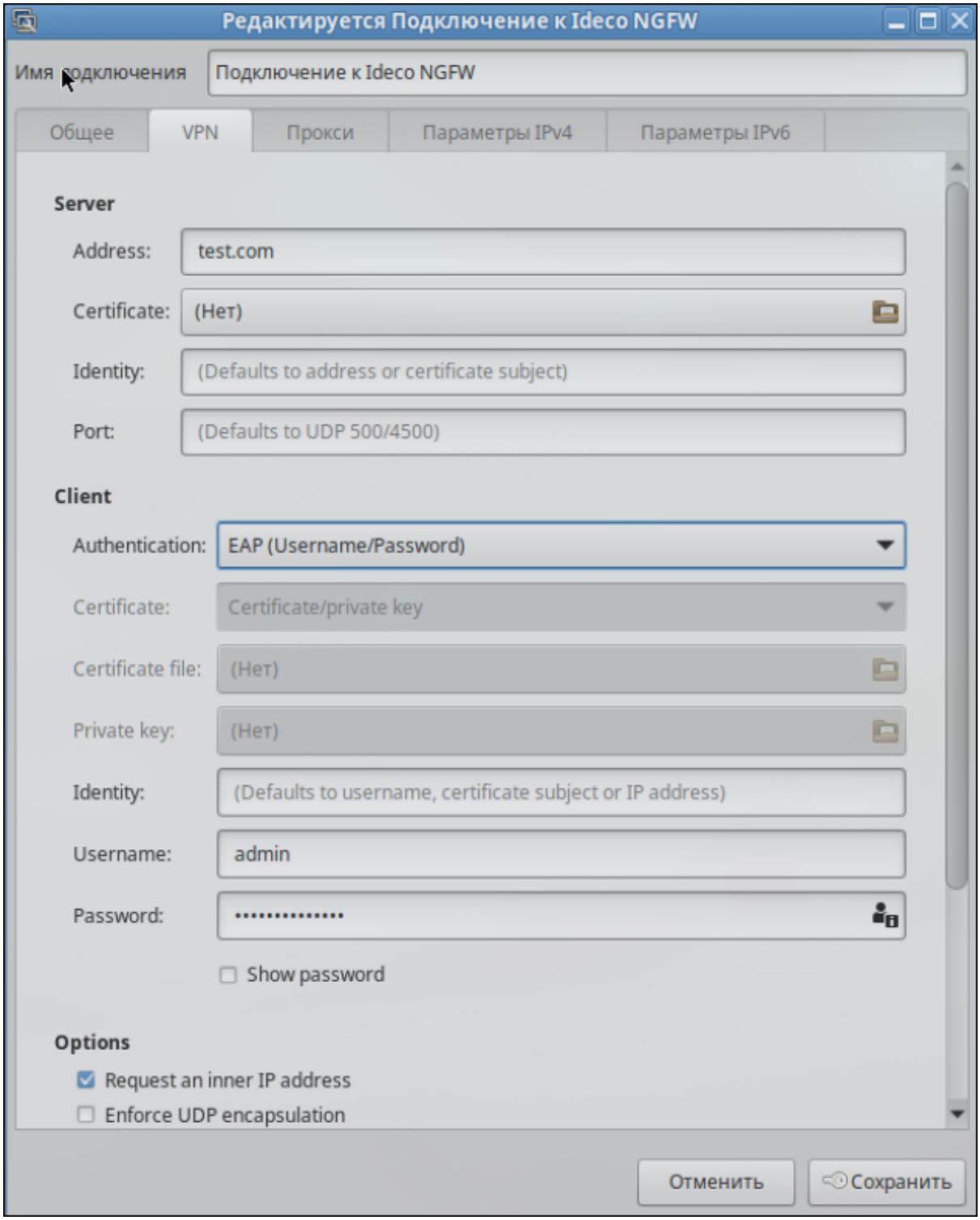


5. Выберите тип VPN-подключения `IPsec/IKEv2 (strongswan)` и нажмите **Создать**:

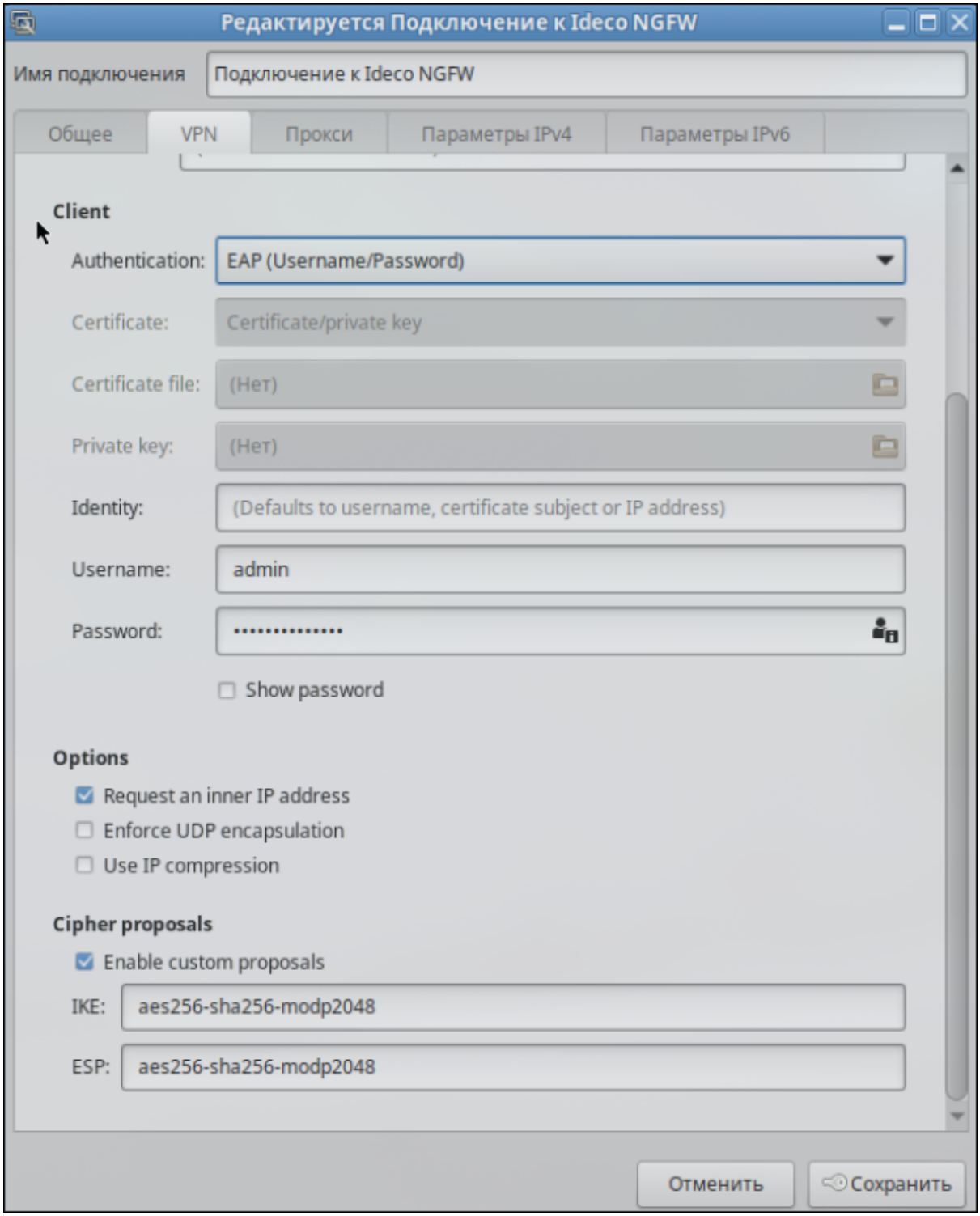


6. Заполните необходимые поля для создания VPN-подключения, как на скриншоте:

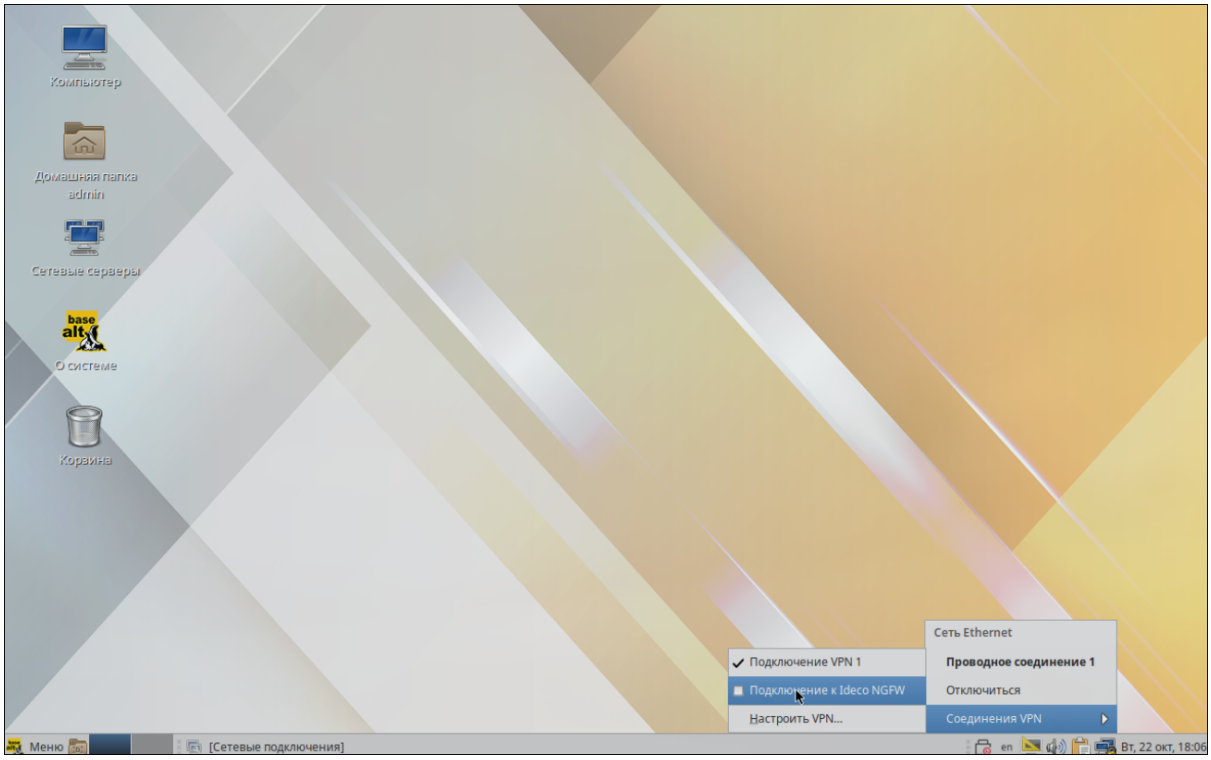
- Address - адрес шлюза;
- Authentication - тип аутентификации;
- Username - логин пользователя на Ideco NGFW;
- Password - пароль пользователя на Ideco NGFW.



7. Заполните параметры шифрования, как на скриншоте, и нажмите **Сохранить**:



8. Включите созданное VPN-подключение:



37.20.2 Создание VPN-подключения в Ubuntu

Основное

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

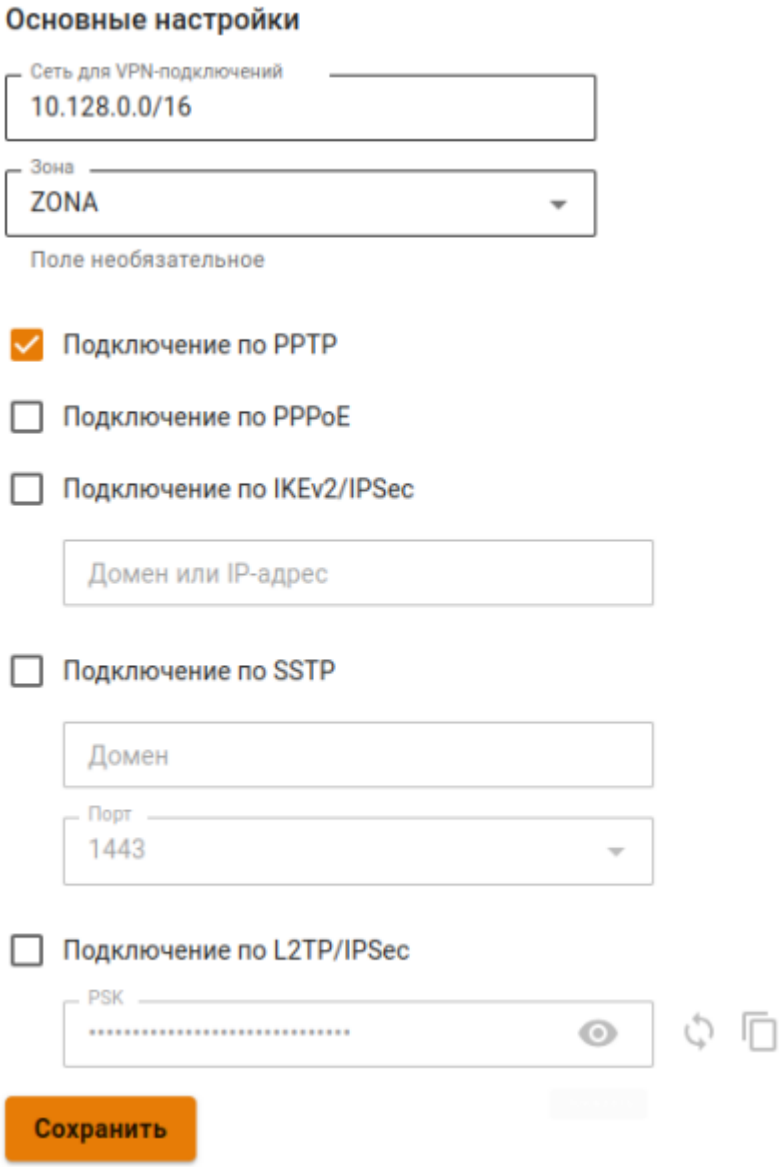
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Предупреждение: Инструкция актуальна для версии Ubuntu 24.04 LTS.

Протокол PPTP:

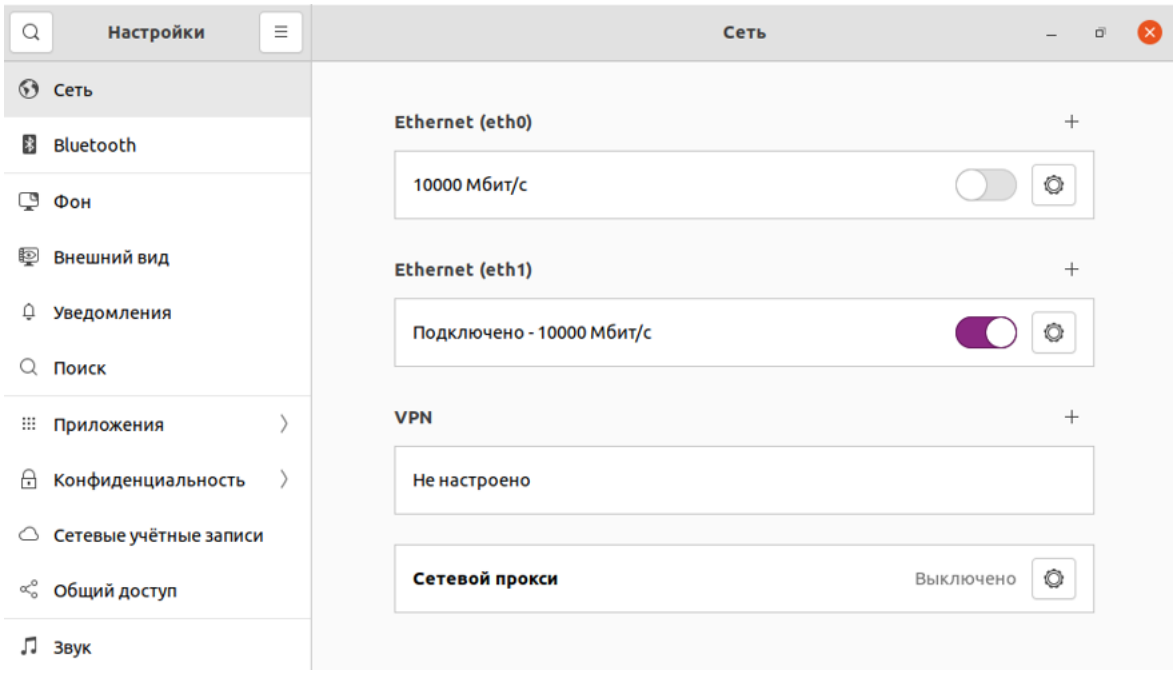
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное** и установите флаг **Подключение по PPTP**:

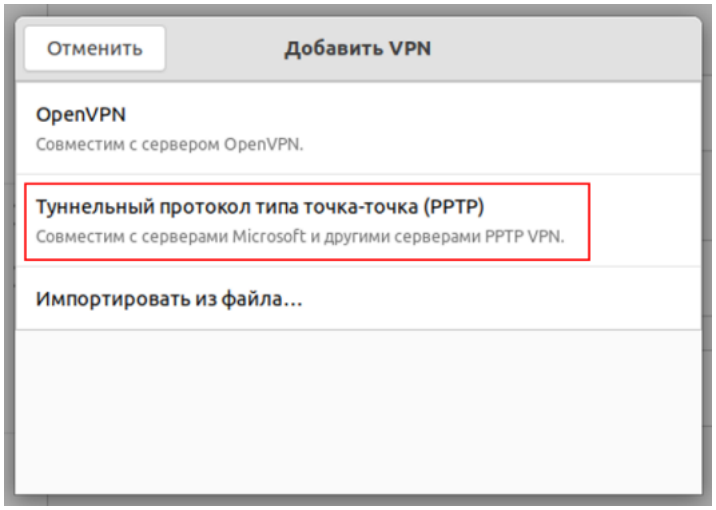


Создание подключения в Ubuntu:

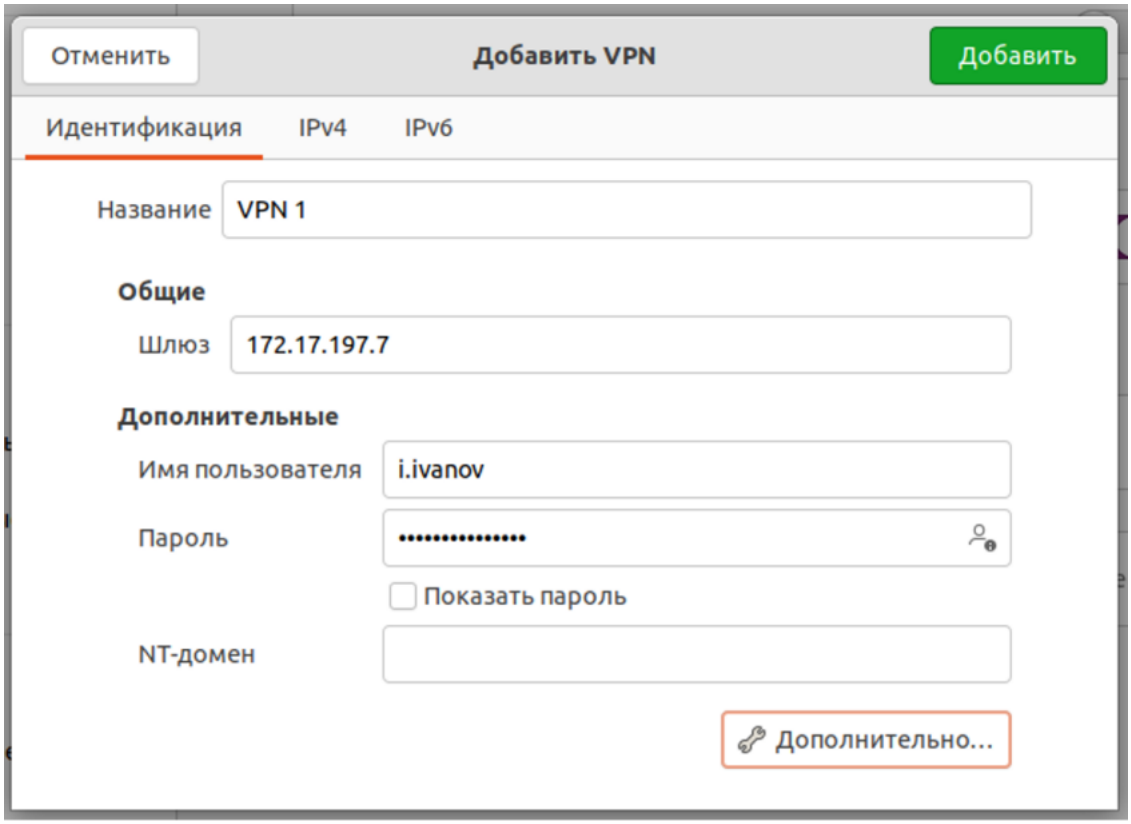
1. Перейдите **Настройки -> Сети** и в строке **VPN** нажмите + :



2. В окне создания подключений выберите пункт **Туннельный протокол типа точка-точка (PPTP)**:

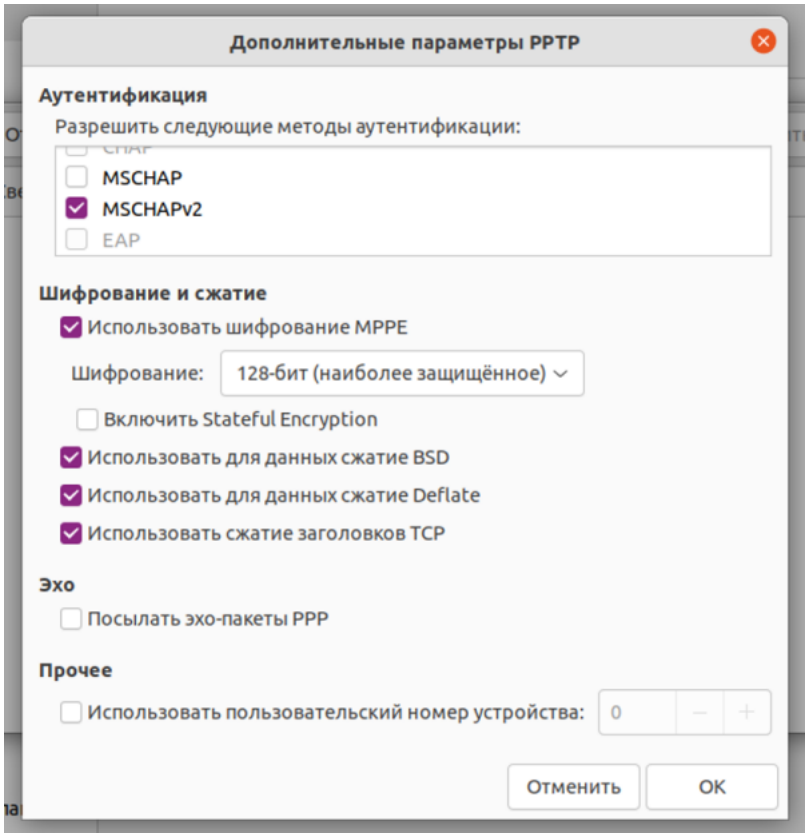


3. В разделе **Идентификация** заполните следующие поля:



- **Название** - имя подключения;
- **Шлюз** - доменное имя или IP-адрес интерфейса NGFW;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

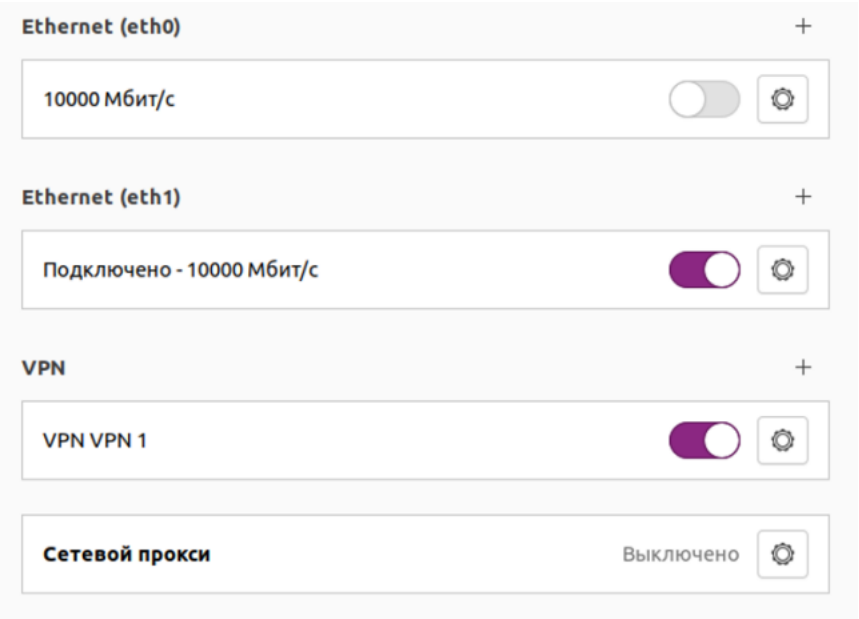
Рекомендуем нажать **Дополнительно** и установить флаги на пунктах:



- **Разрешить следующие методы аутентификации** - установите флаг на *MSCHAPv2*;
- **Использовать шифрование MPPE** - в строке *Шифрование* выберите 128-бит (наиболее защищенное);
- **Использовать для данных сжатие BSD** - использование алгоритма BSD-compress;
- **Использовать для данных сжатие Deflate** - использование алгоритма Deflate;
- **Использовать сжатие заголовков TCP** - использование метода сжатия заголовков TCP/IP Вана Якобсона.

4. Нажмите **ОК** и **Добавить**.

5. Включите созданное VPN-подключение:

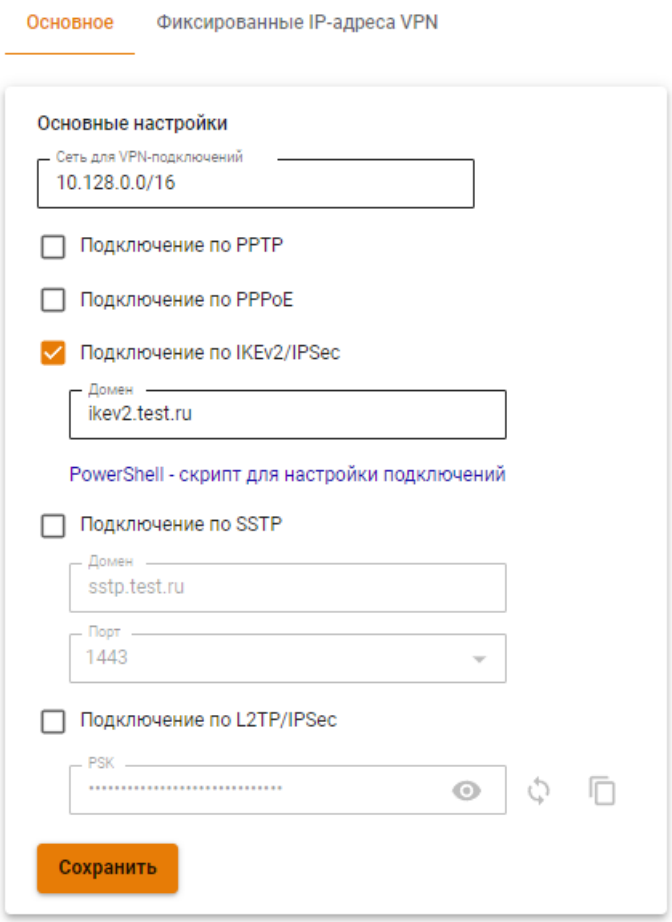


Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

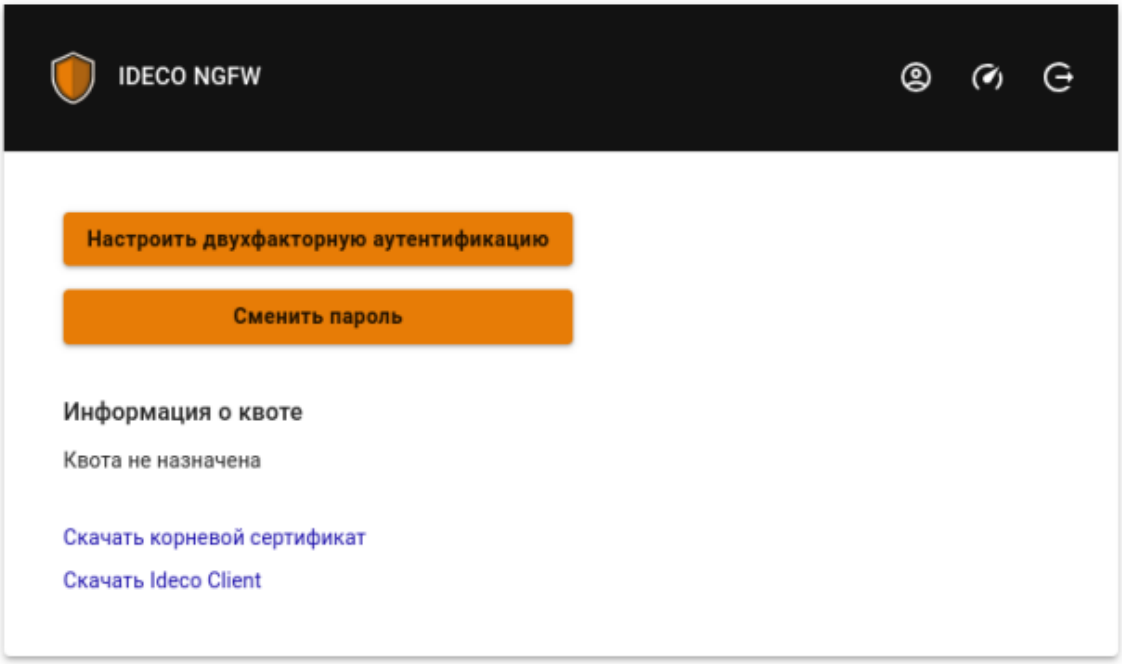
1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:

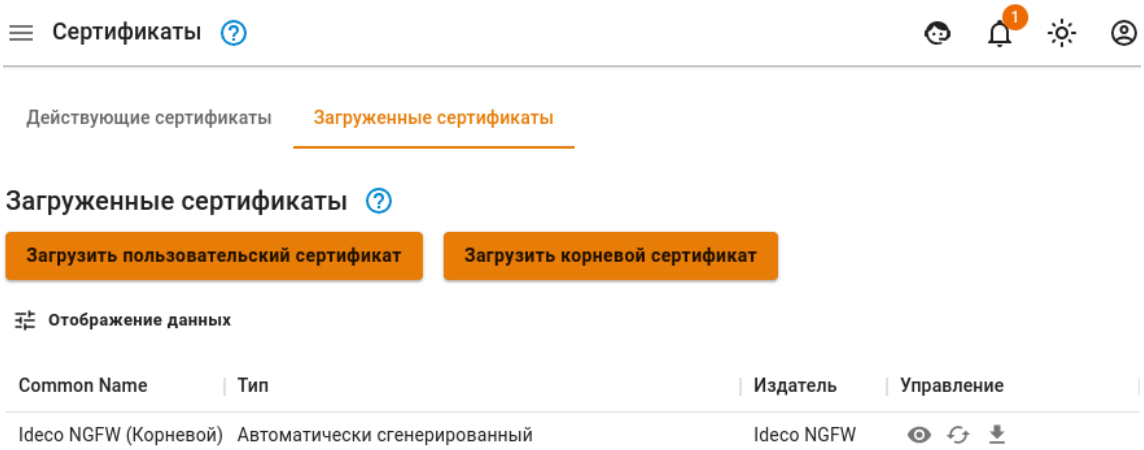


3. Скачайте корневой сертификат одним из способов:

- 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:

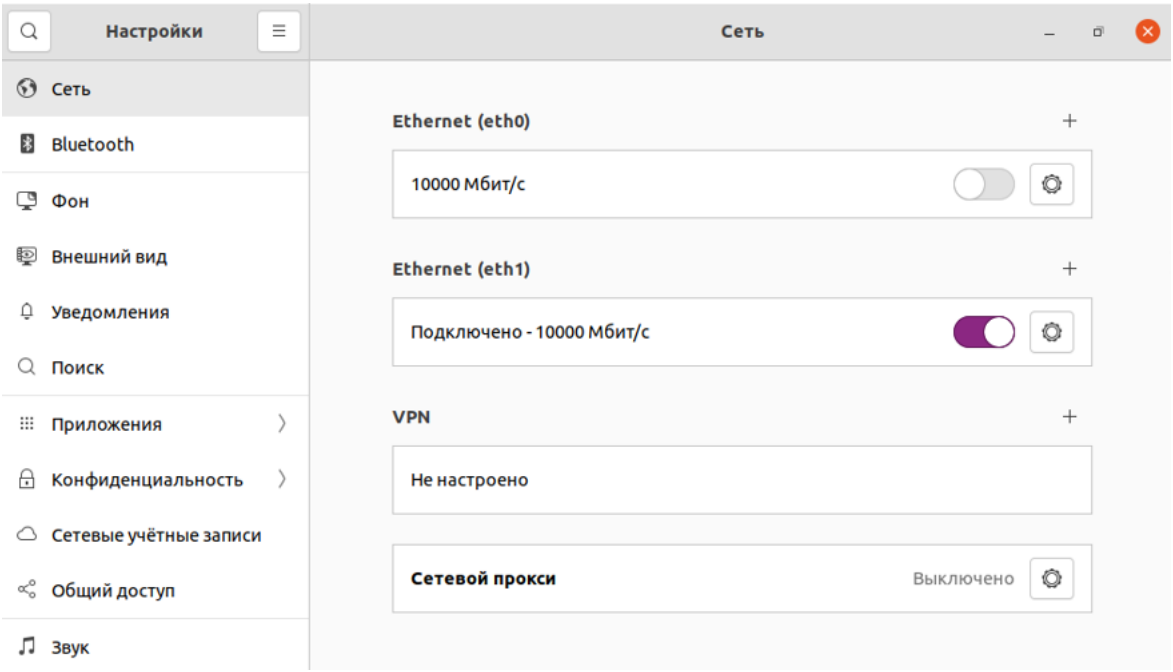
```
sudo cp ca.crt /usr/local/share/ca-certificates/ca.crt
```

- `ca.crt` - имя скачанного сертификата.

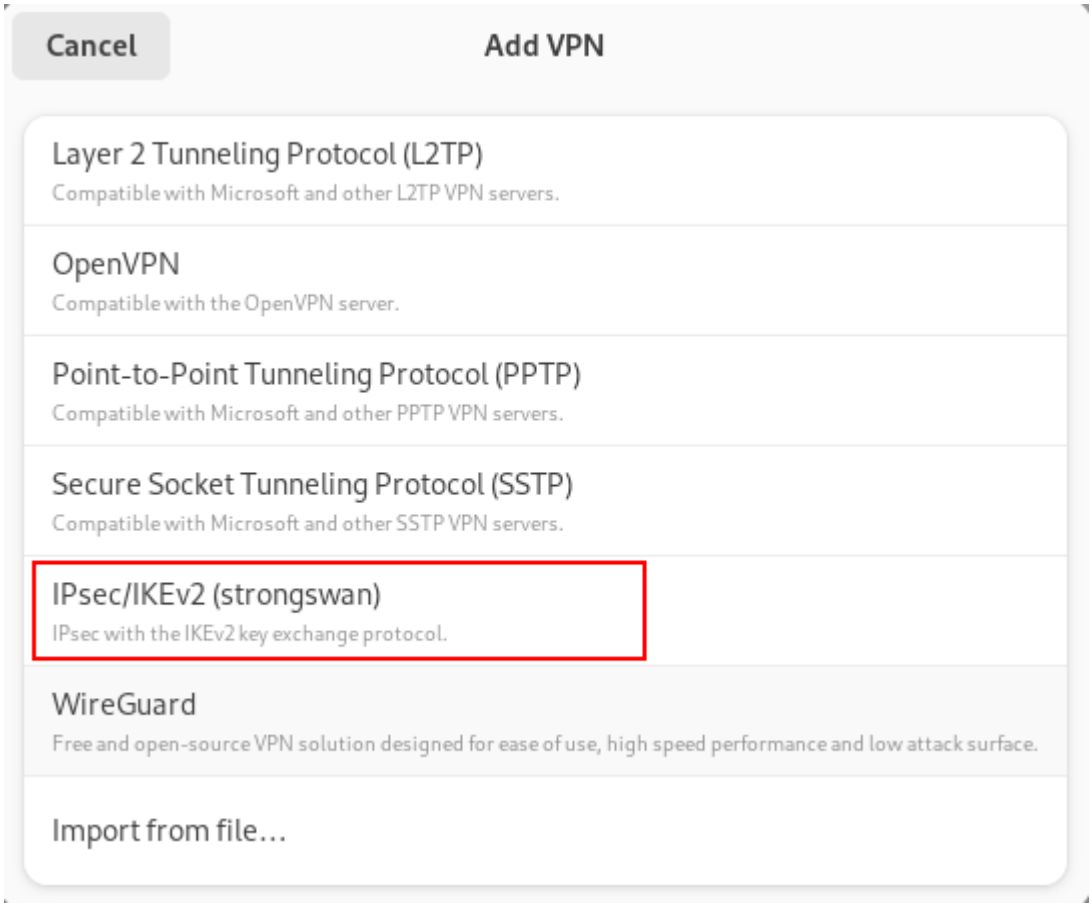
5. Для обновления сертификатов устройства выполните команду:

```
sudo update-ca-certificates
```

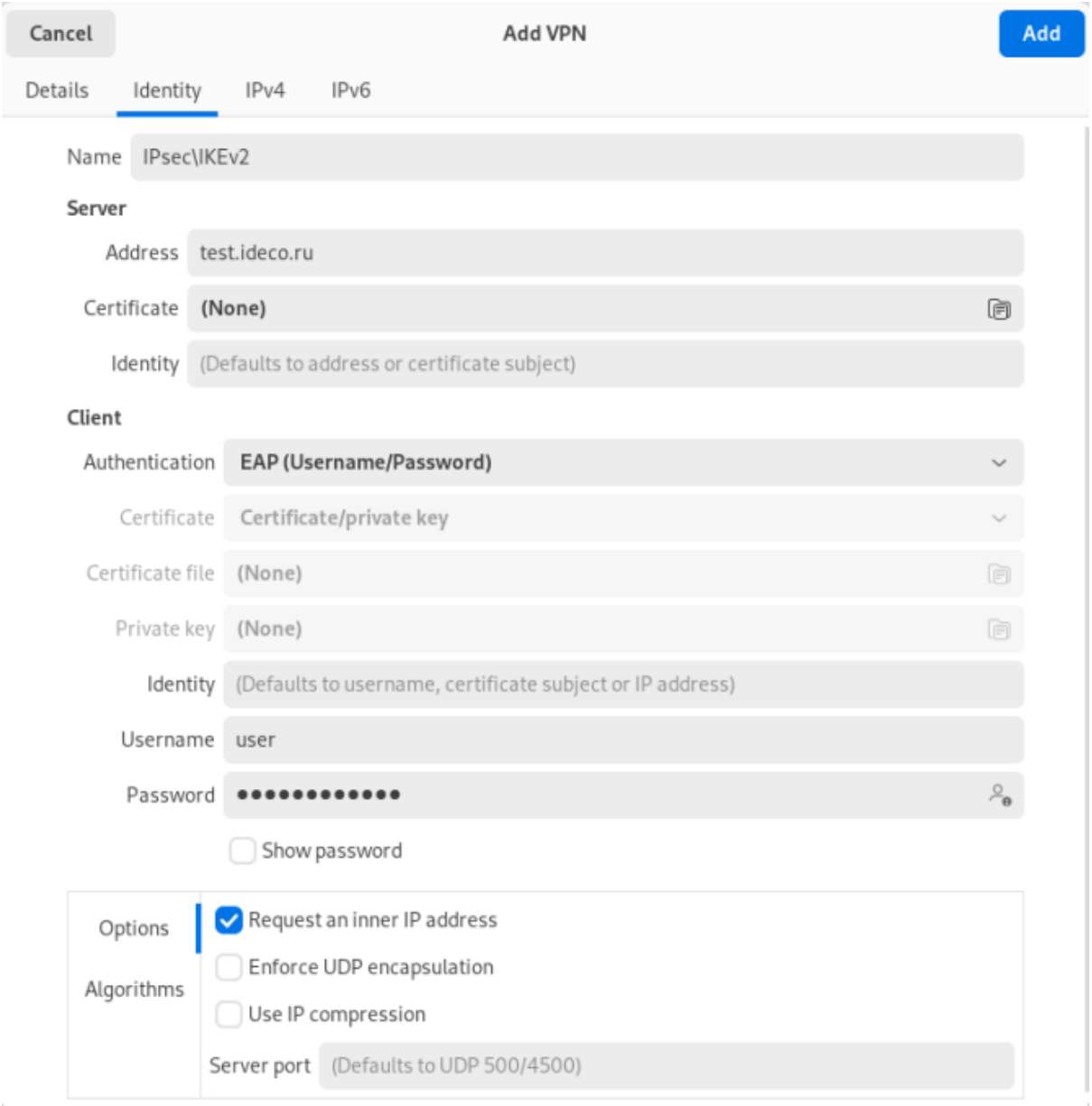
6. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + :



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**.

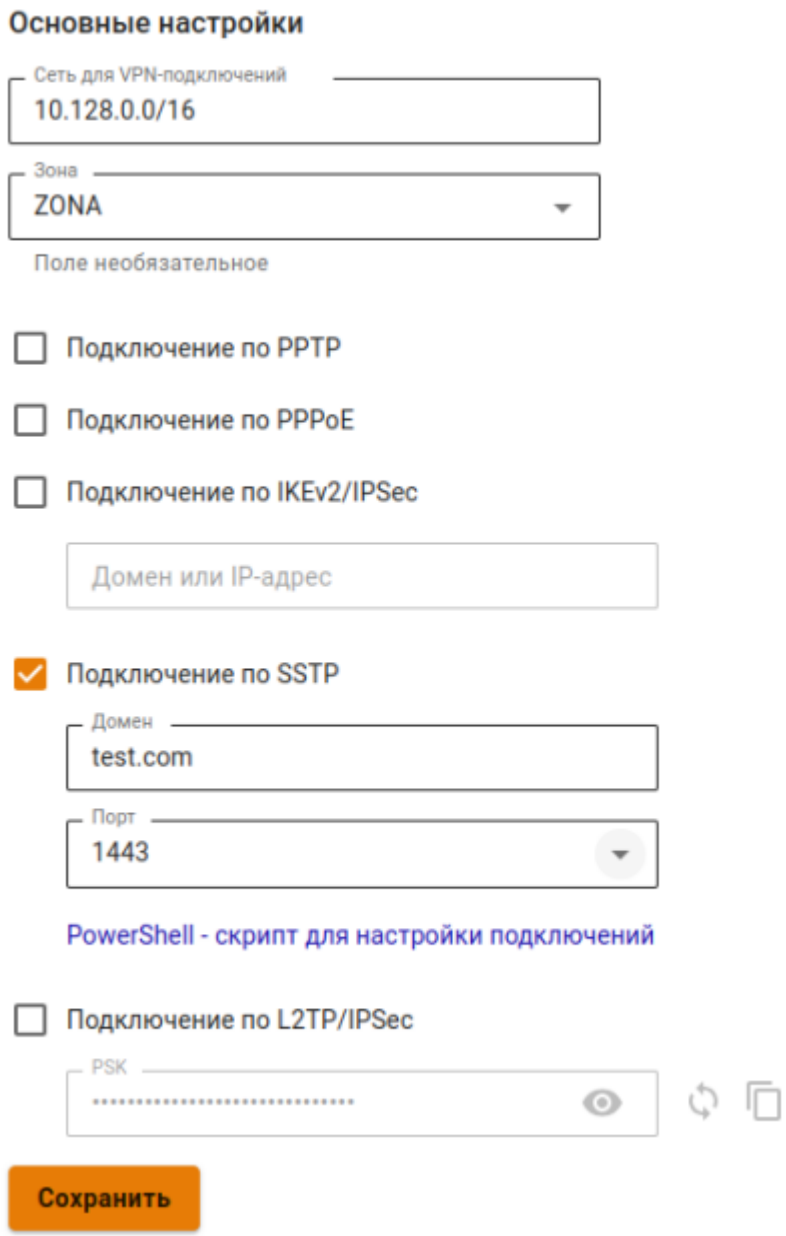
9. Включите созданное VPN-подключение.

Протокол SSTP:

Настройка Ideco NGFW:

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

2. Установите флаг **Подключение по SSTP** и заполните поля **Домен** и **Порт**:



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

Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в Ubuntu:

1. Откройте терминал и выполните две команды:

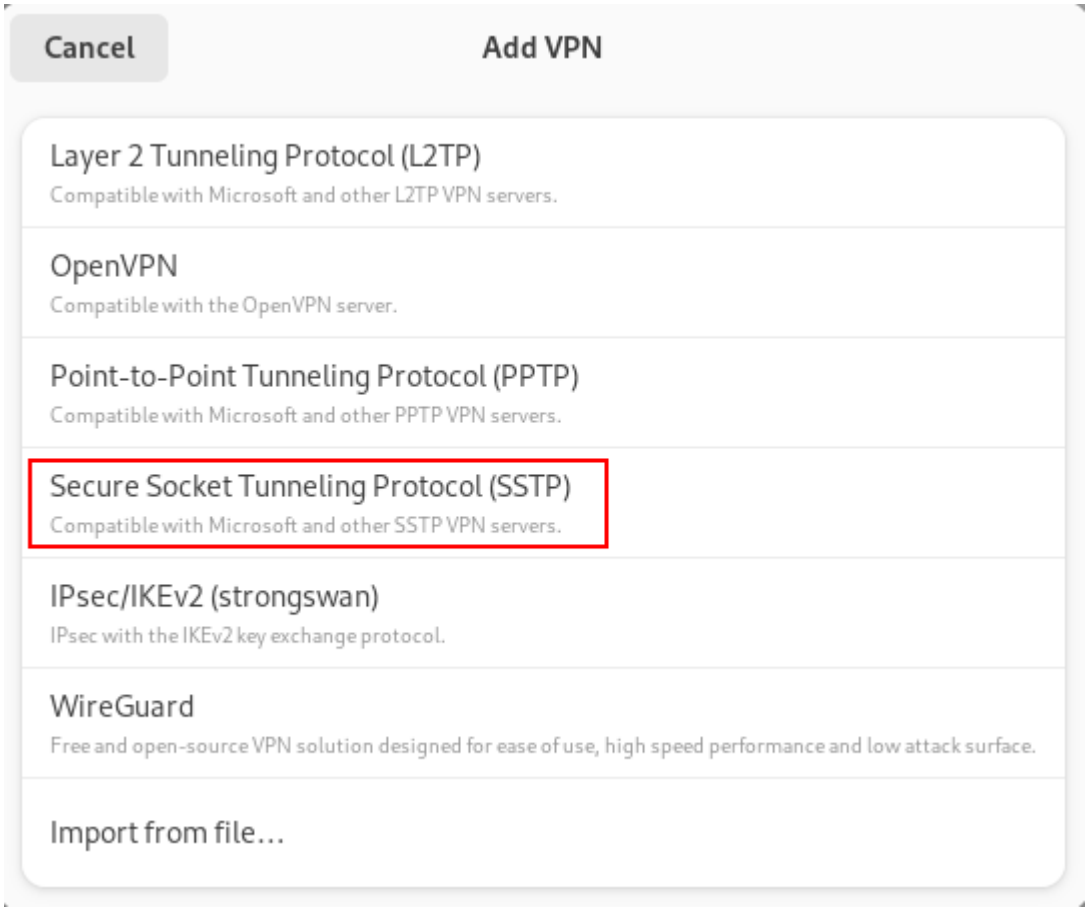
```
sudo apt-add-repository ppa:eivnaes/network-manager-sstp
sudo apt install -y network-manager-sstp sstp-client
```

2. По окончании установки перезагрузите компьютер:

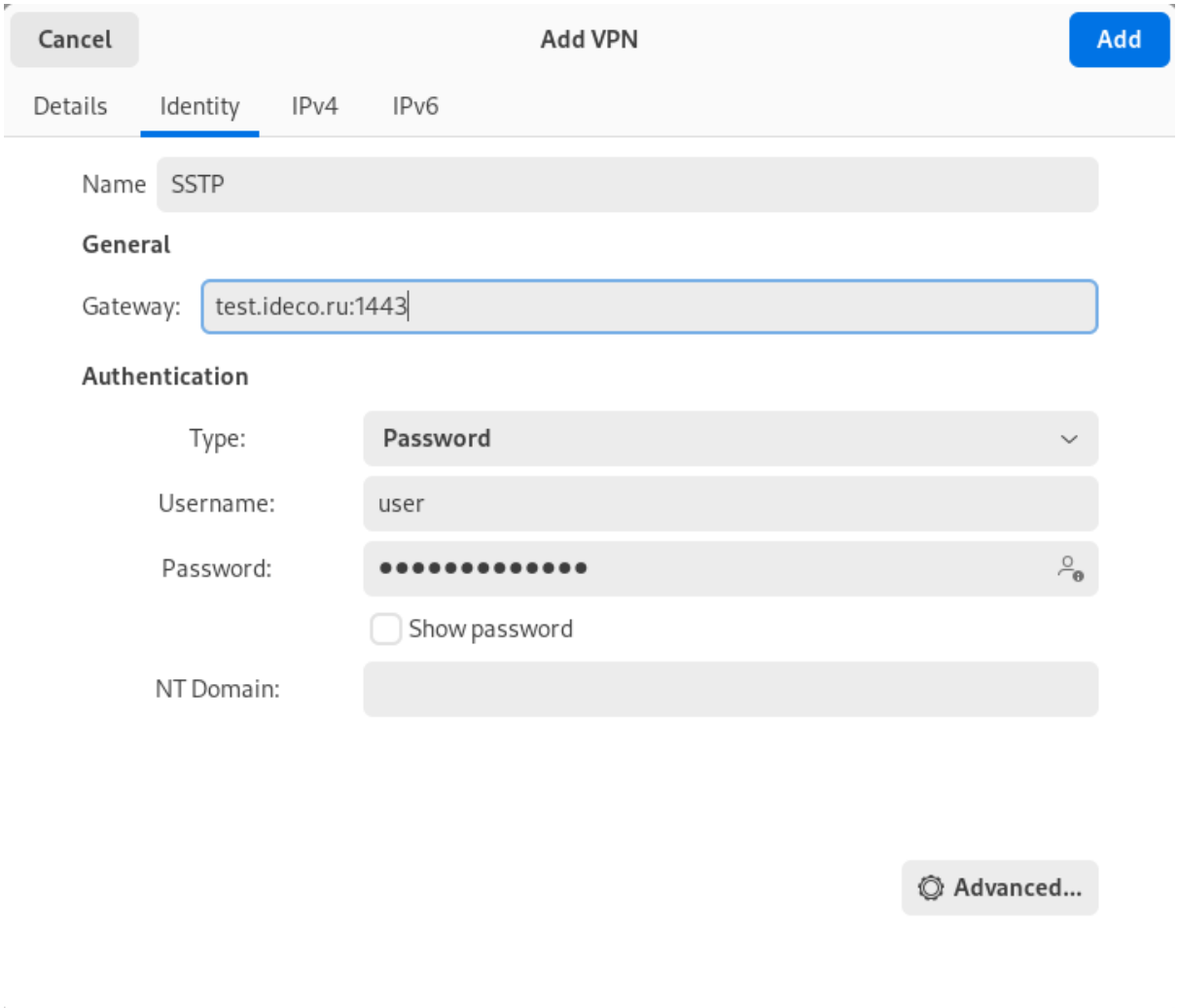
```
sudo reboot
```

3. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + .

4. В появившемся окне выберите **Secure Socket Tunneling Protocol (SSTP)** или **Туннельный протокол типа точка-точка (SSTP)**:



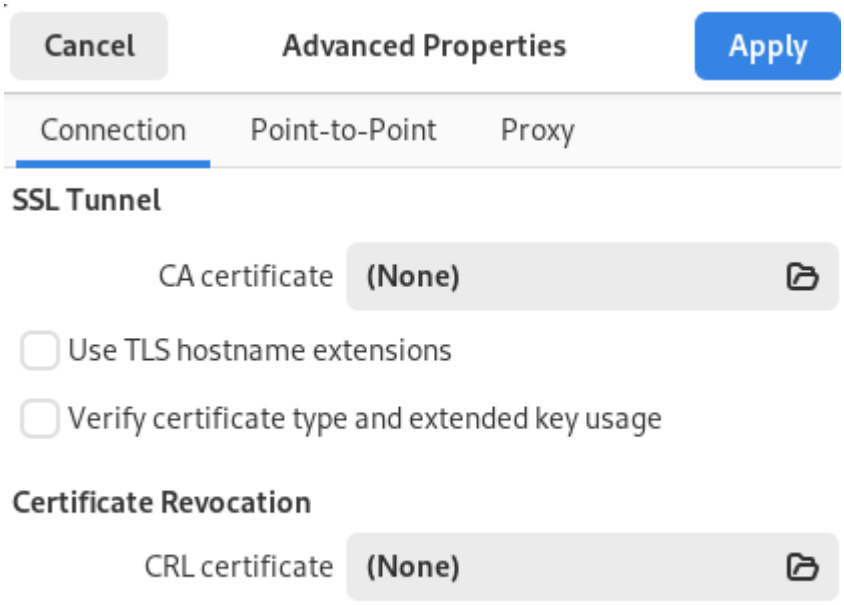
5. В разделе **Identity (Идентификация)** заполните следующие поля:



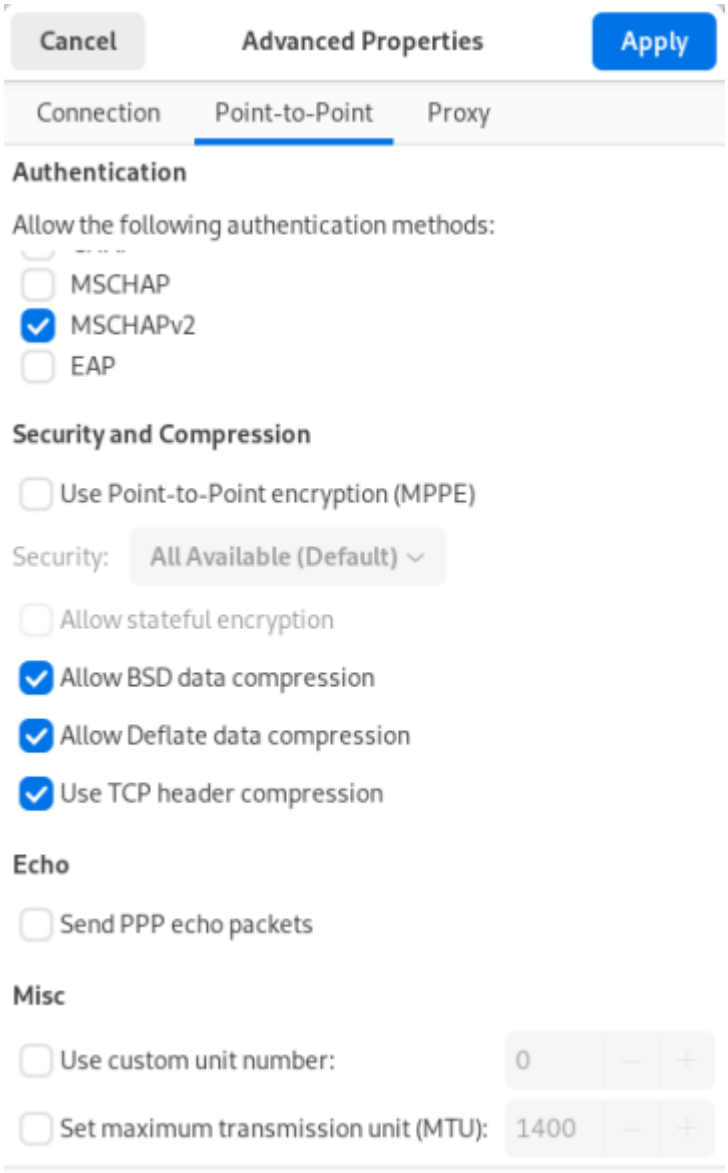
- **Название** - имя подключения;
- **Шлюз** - укажите в формате *домен:[порт, выбранный на NGFW]*;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

6. Нажмите **Advanced**:

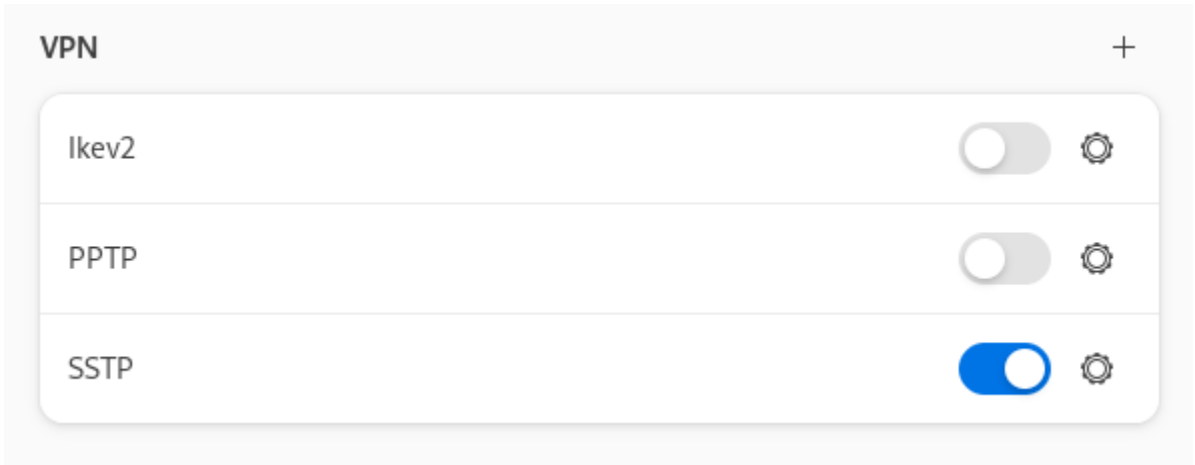
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**;
  - **Verify certificate type and extended key usage**:



- 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:



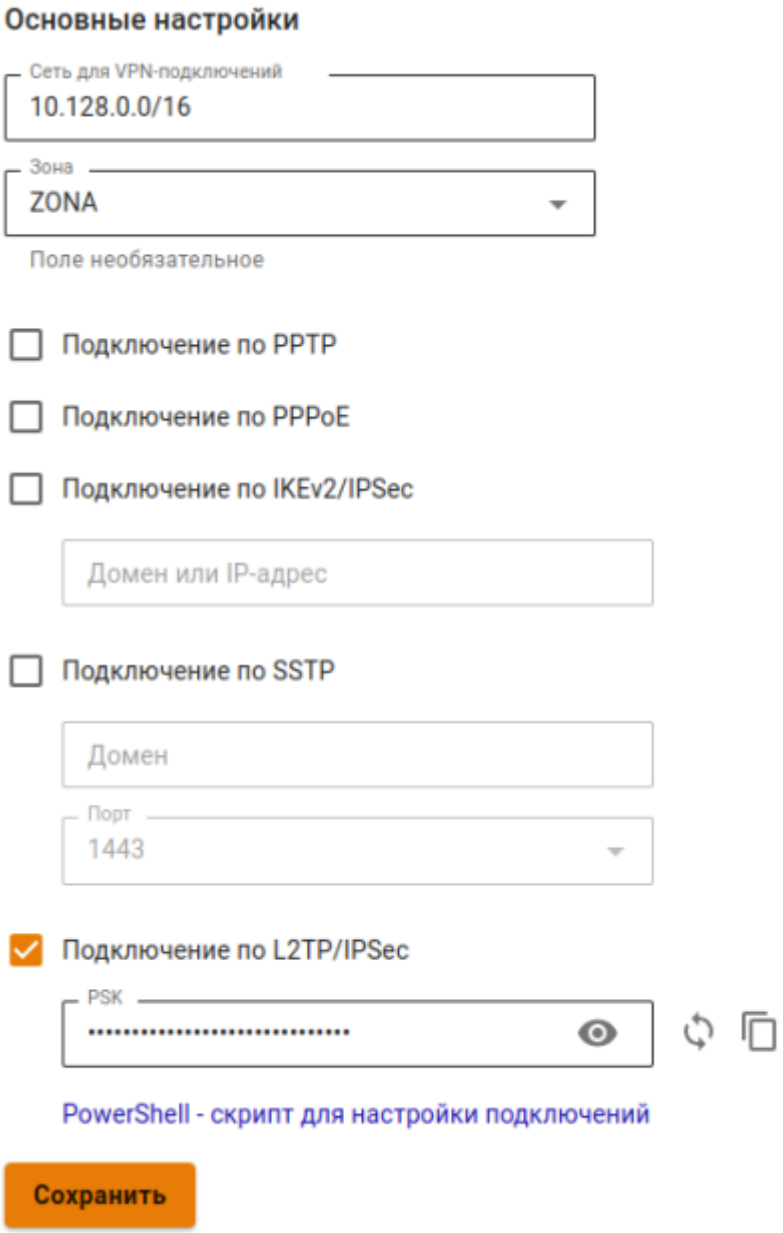
Протокол L2TP/IPsec:

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-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



Создание подключения в Ubuntu:

1. Подключите репозиторий, в котором находятся необходимые пакеты для создания L2TP VPN-соединения, а затем обновите информацию о репозиториях. Для этого выполните следующие команды:

```
sudo add-apt-repository ppa:nm-l2tp/network-manager-l2tp
sudo apt update
```

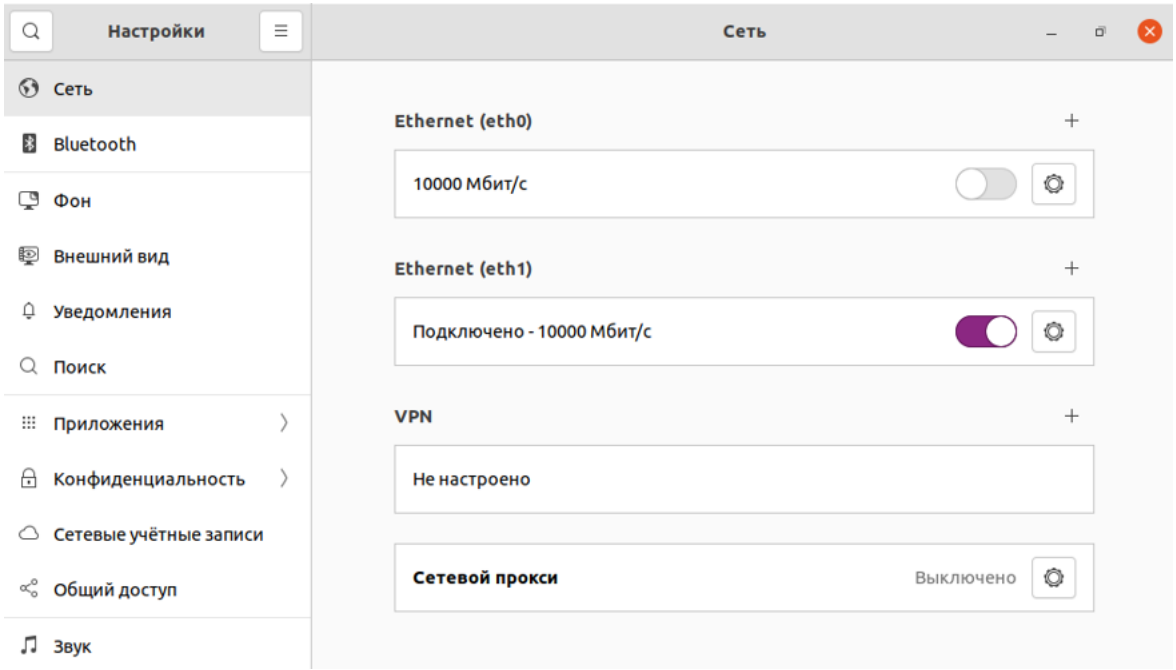
2. Установите дополнение к стандартному NetworkManager с помощью двух пакетов:

```
sudo apt install -y network-manager-l2tp network-manager-l2tp-gnome
```

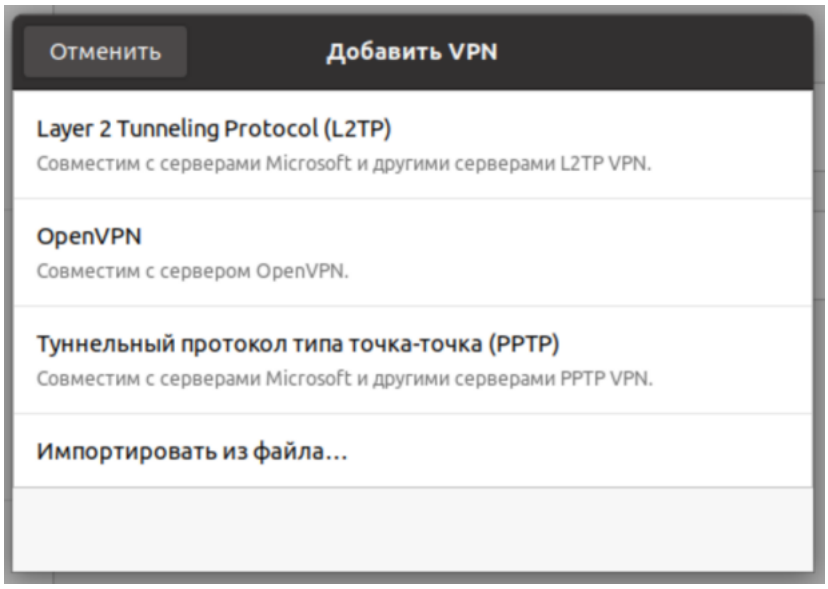
3. После окончания установки перезагрузите компьютер:

```
sudo reboot
```

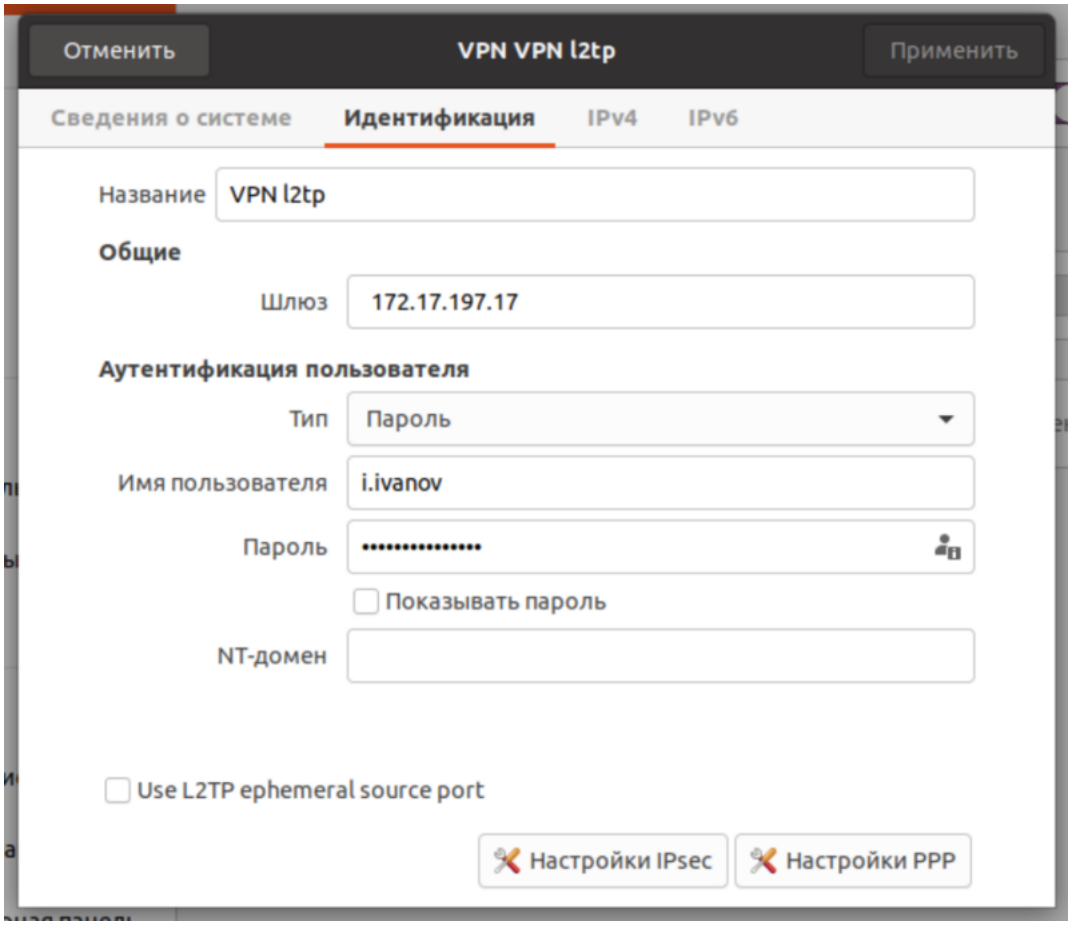
4. После окончания установки пакетов перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + :



5. В окне создания подключений по VPN выберите пункт **Layer 2 Tunneling Protocol (L2TP)**:

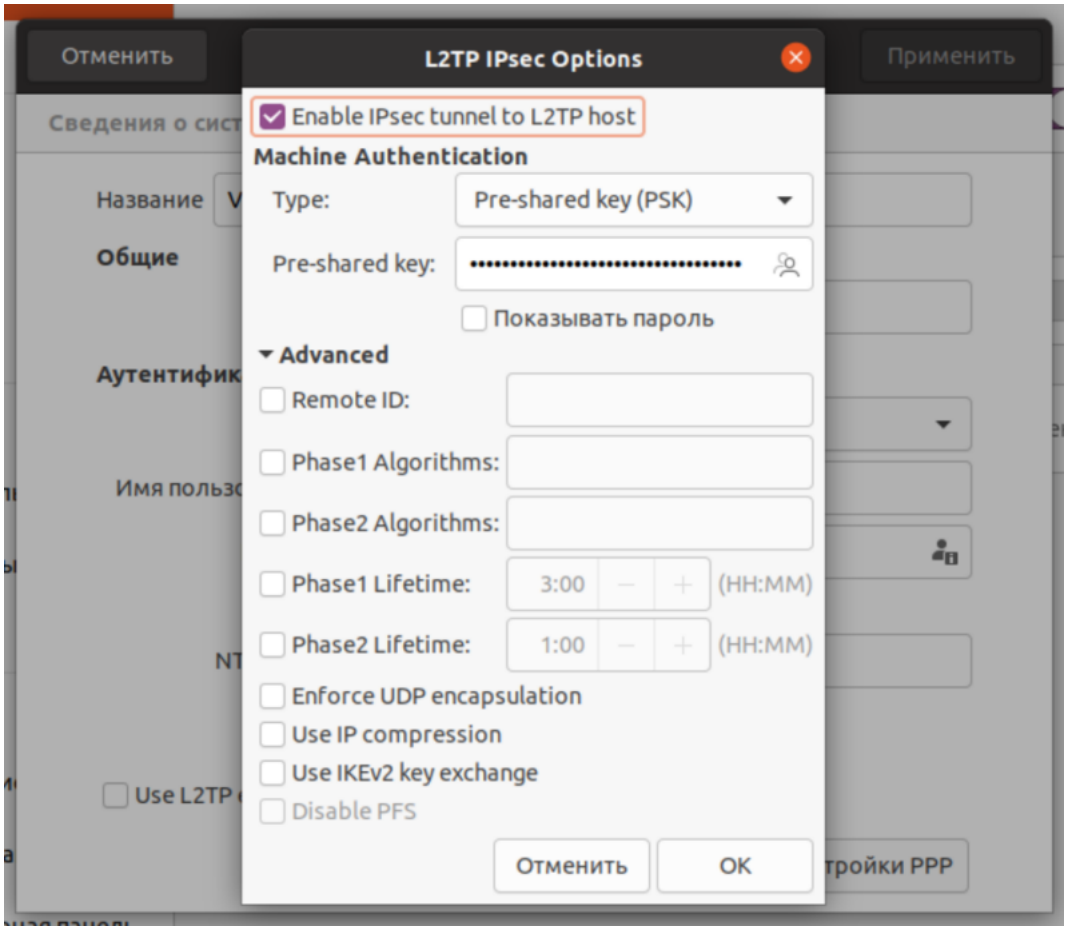


6. На вкладке **Идентификация** заполните следующие поля:



- **Название** - имя подключения;
- **Шлюз** - доменное имя или IP-адрес интерфейса NGFW;
- **Тип** - Password (аутентификация по имени пользователя и паролю);
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

7. Перейдите в **Настройки IPsec** и включите настройку **Enable IPsec tunnel to L2TP host**, чтобы активировалась возможность настраивать остальные параметры:

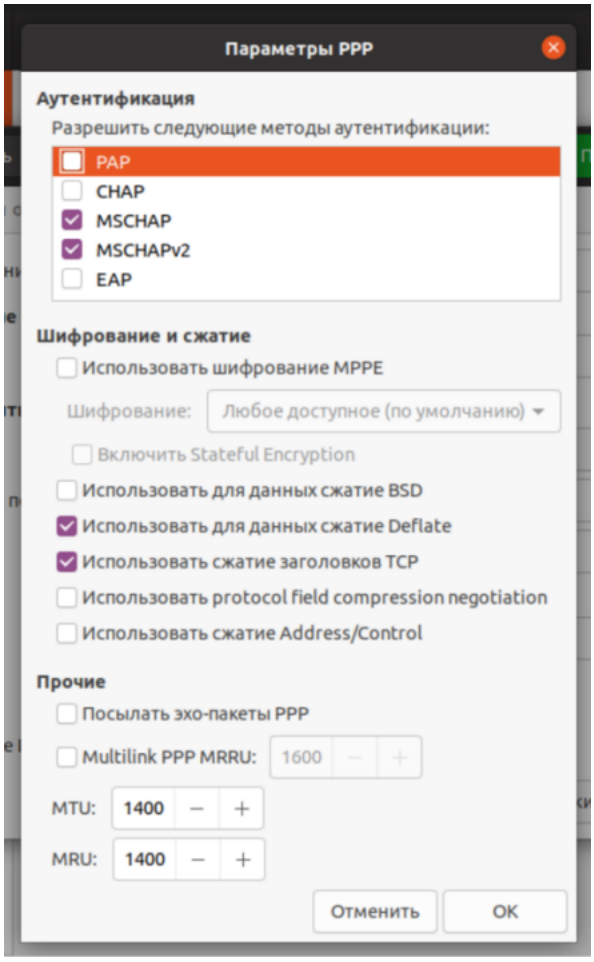


- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу;
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи -> VPN-подключения -> Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения.

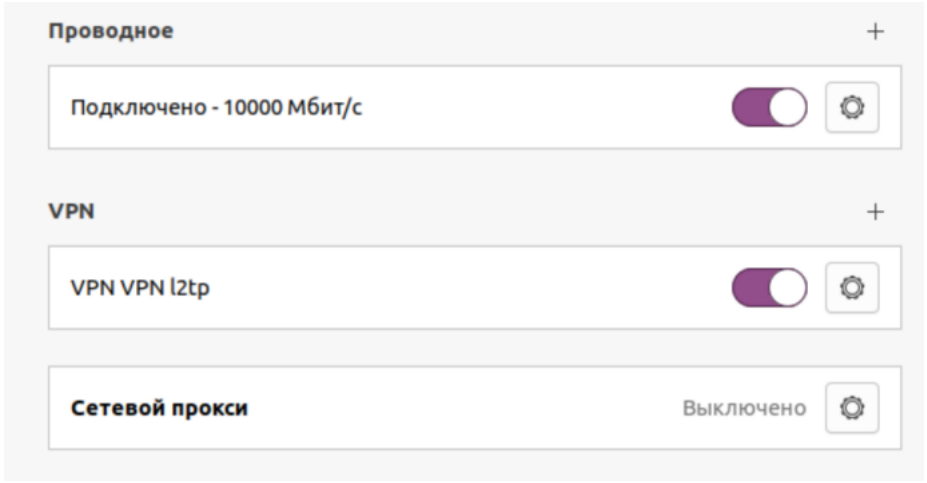
После окончания настройки **L2TP IPsec Options** нажмите **OK**.

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:



37.20.3 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.

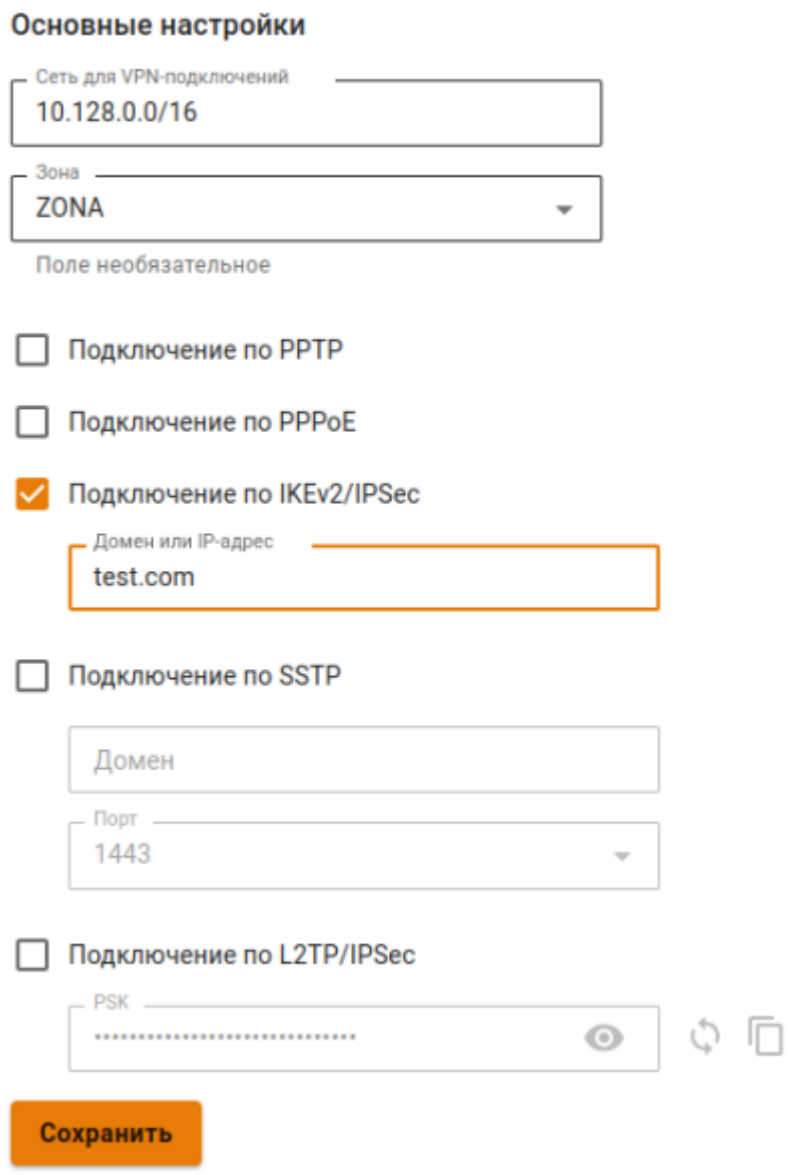
При настройке подключения в Fedora 40 **не требуется** загружать сертификат **ISRG_ROOT_X1**, поскольку он уже есть в системе. Сертификат находится в каталоге `/etc/ssl/certs`

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
```

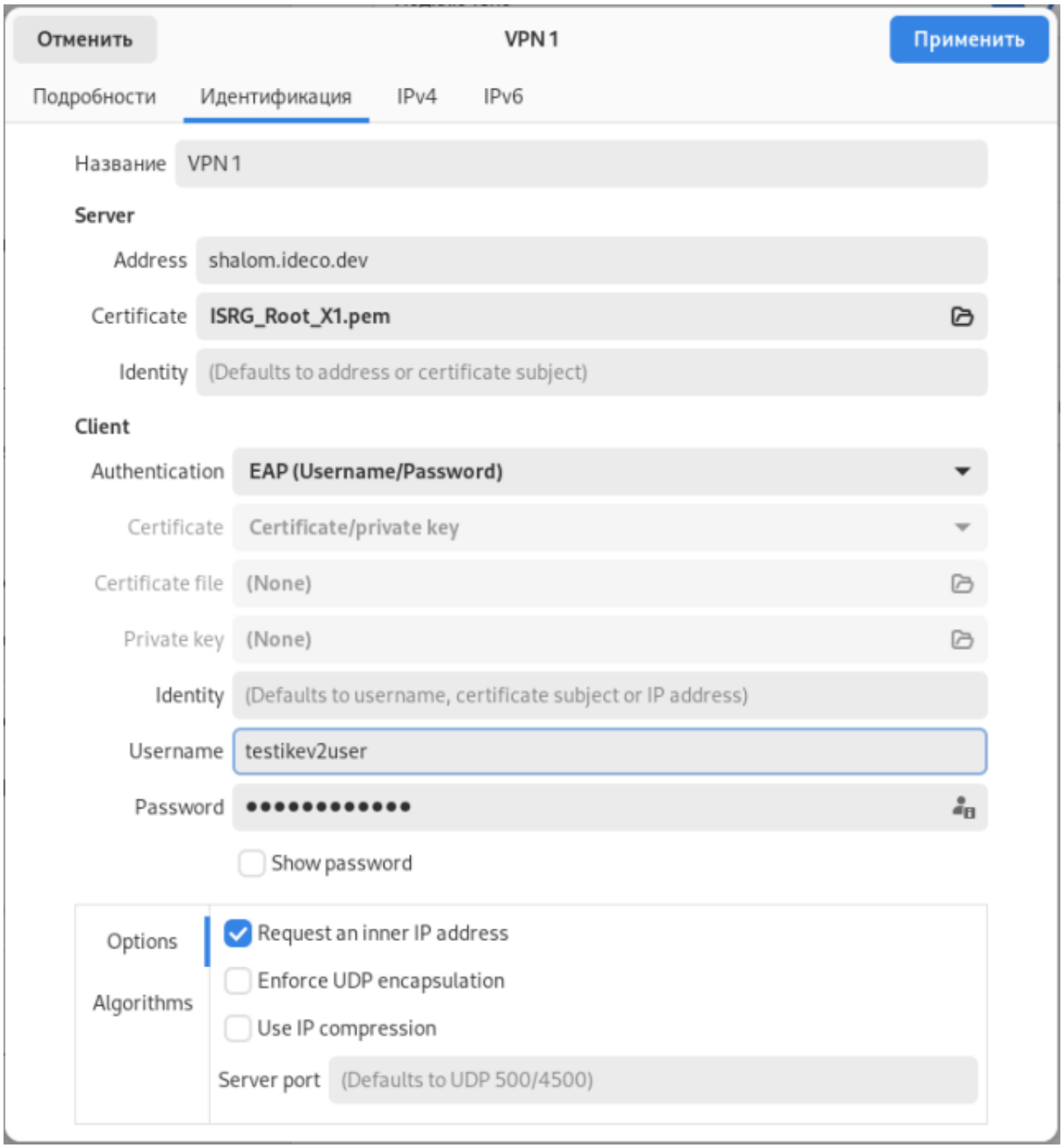
- Окружение рабочего стола KDE:

```
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.

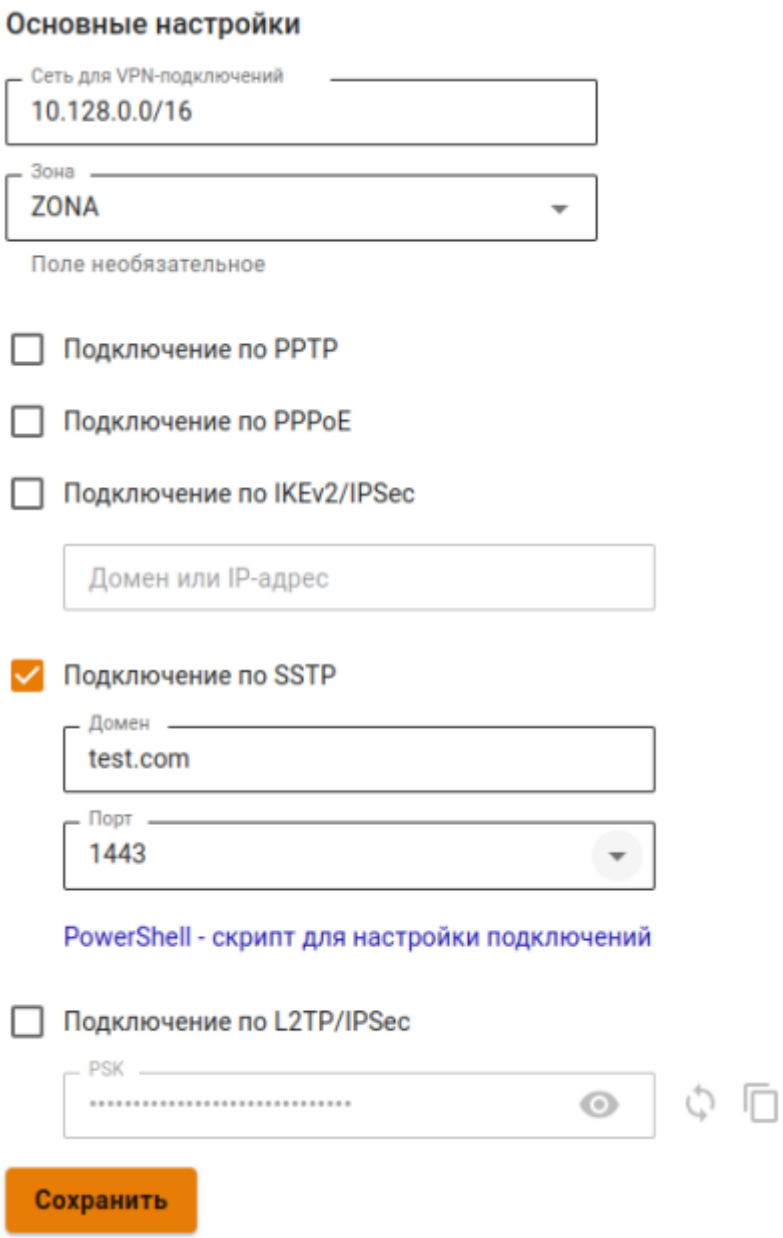
3. Нажмите **Применить** и подключитесь к Ideco NGFW.

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:

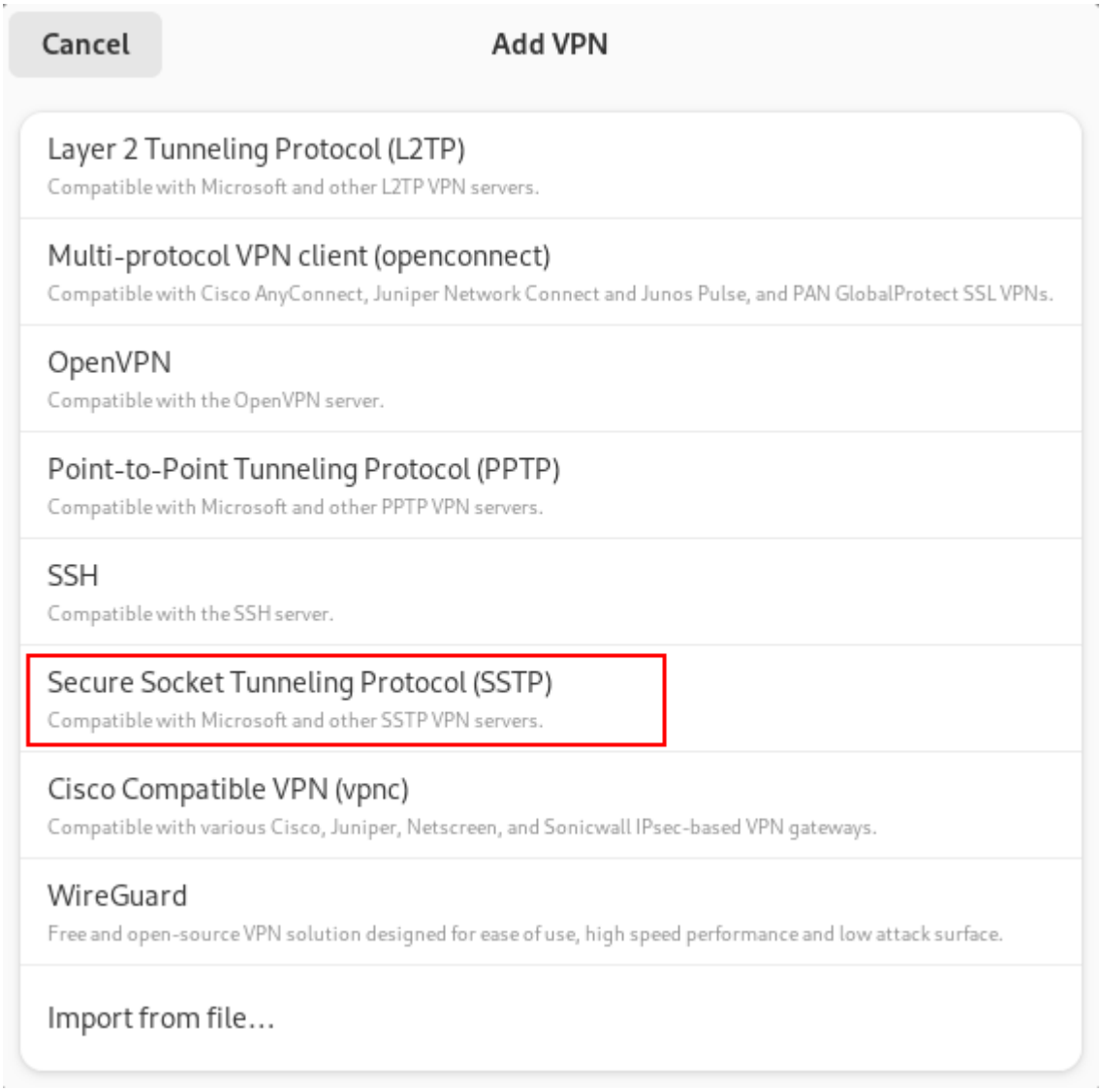
```
sudo dnf install NetworkManager-sstp.x86_64 plasma-nm-sstp.x86_64 sstp-client.x86_64
```

2. По окончании установки перезагрузите компьютер:

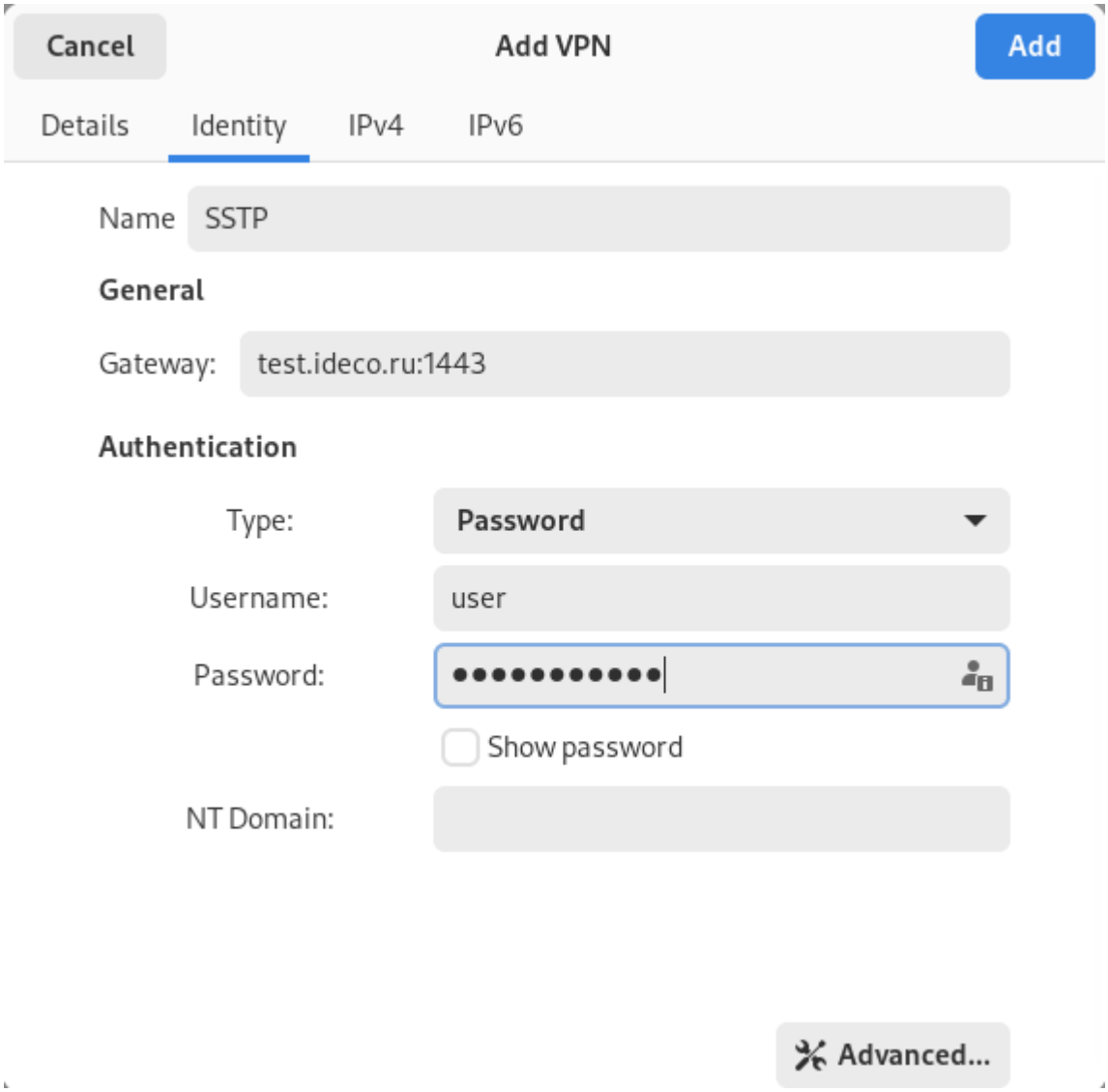
```
sudo reboot
```

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)**:



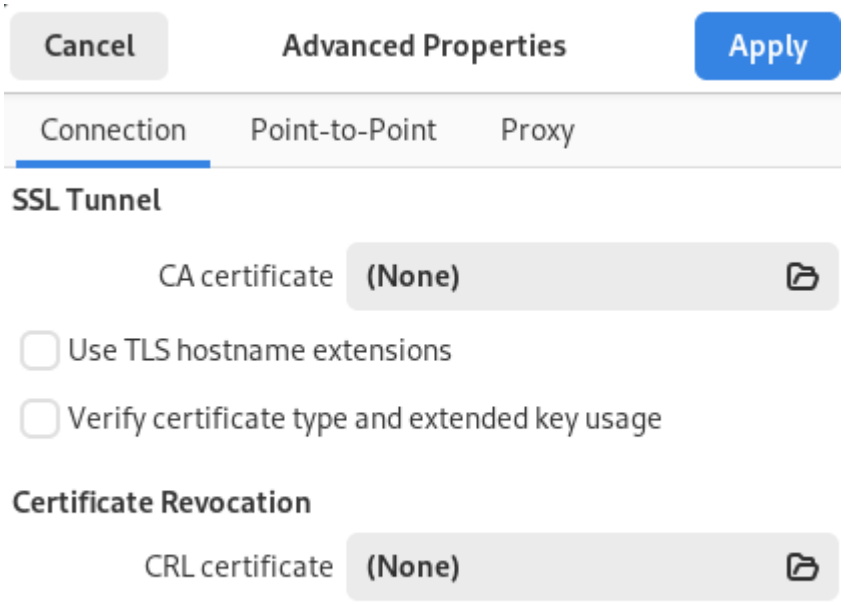
5. В разделе **Identity (Идентификация)** заполните следующие поля:



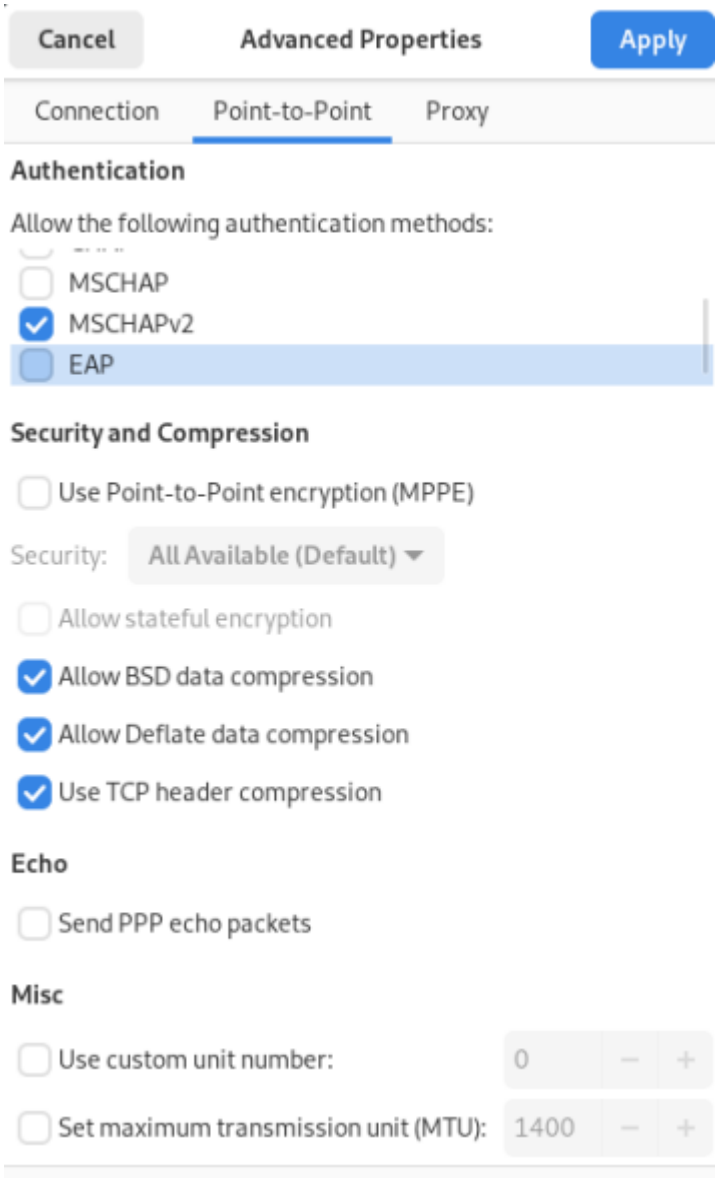
- **Название** - имя подключения;
- **Шлюз** - укажите в формате `домен:<порт, выбранный на NGFW>`;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения;
- **NT-домен** - оставьте поле пустым.

6. Нажмите **Advanced**:

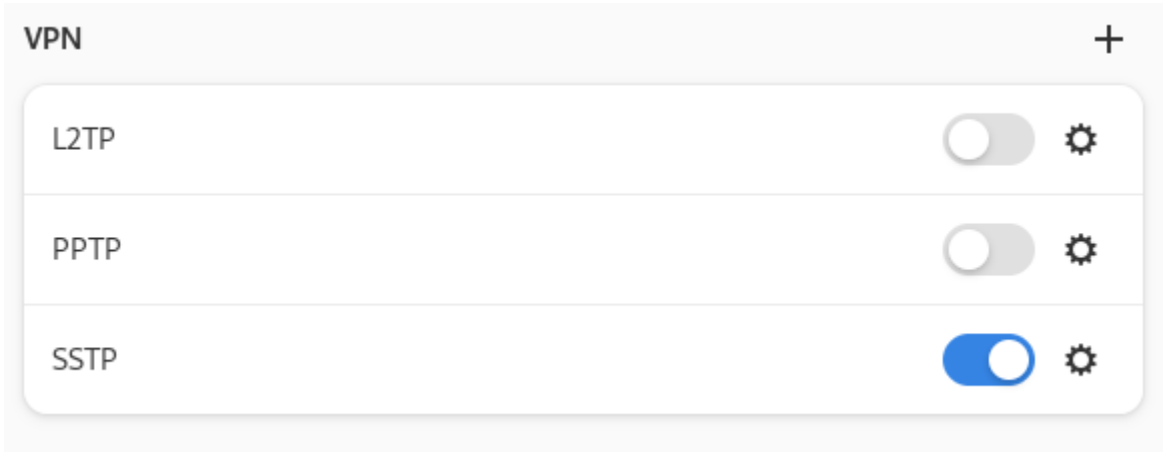
- На вкладке **Connection** отключите настройки:
  - **Use TLS hostname extentions**;
  - **Verify certificate type and extended key usage**:



- 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:



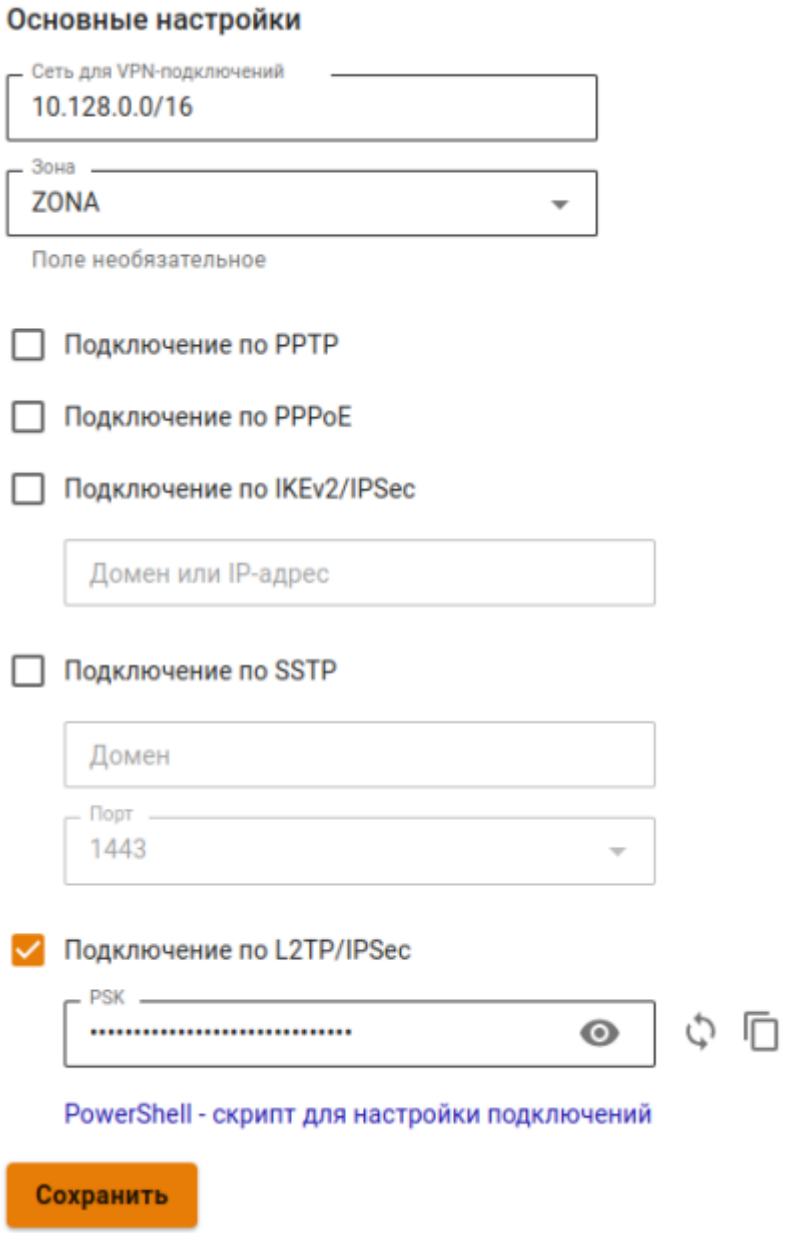
Протокол L2TP/IPsec:

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:

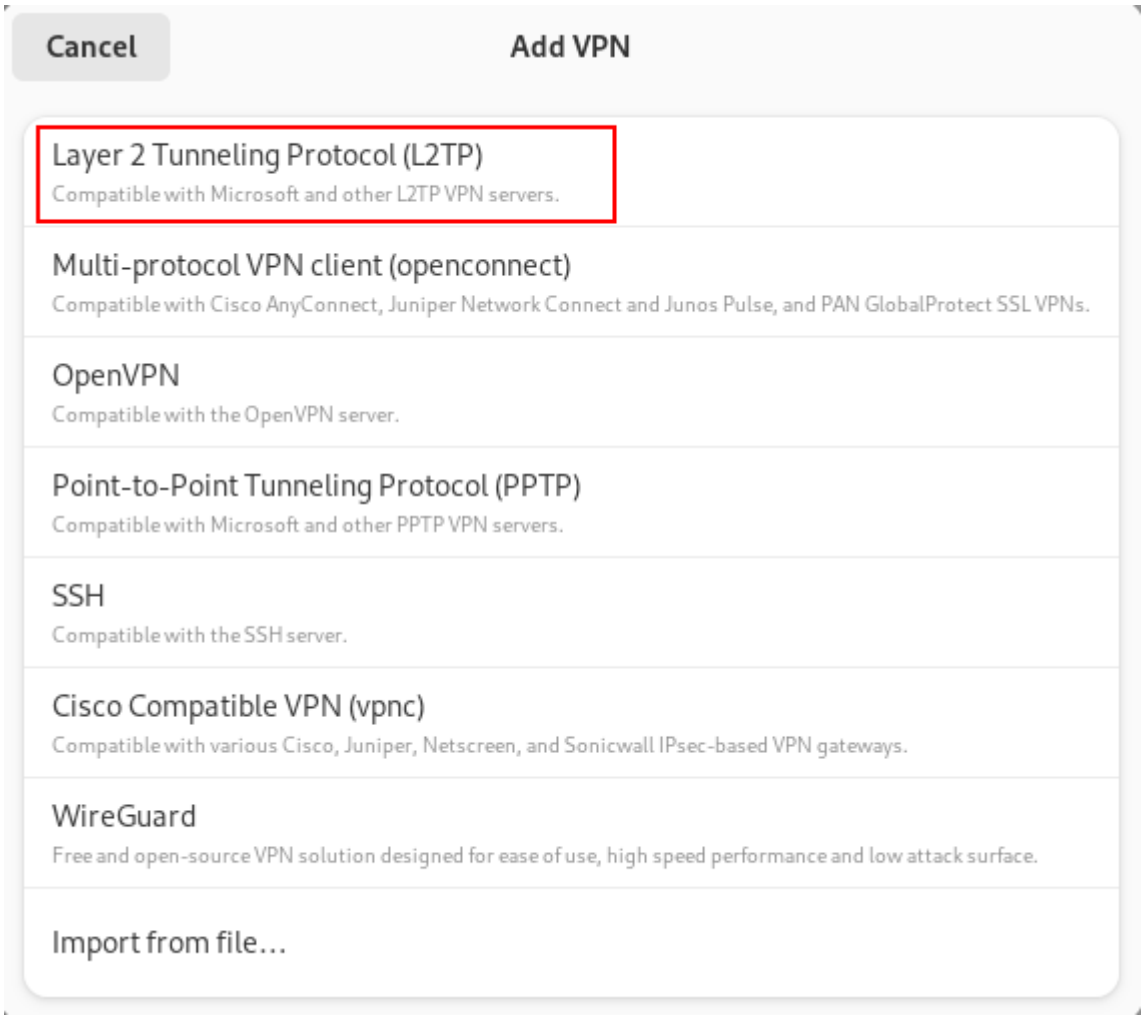
```
sudo dnf install NetworkManager-l2tp.x86_64 plasma-nm-l2tp.x86_64 xl2tpd.x86_64
```

2. После окончания установки перезагрузите компьютер:

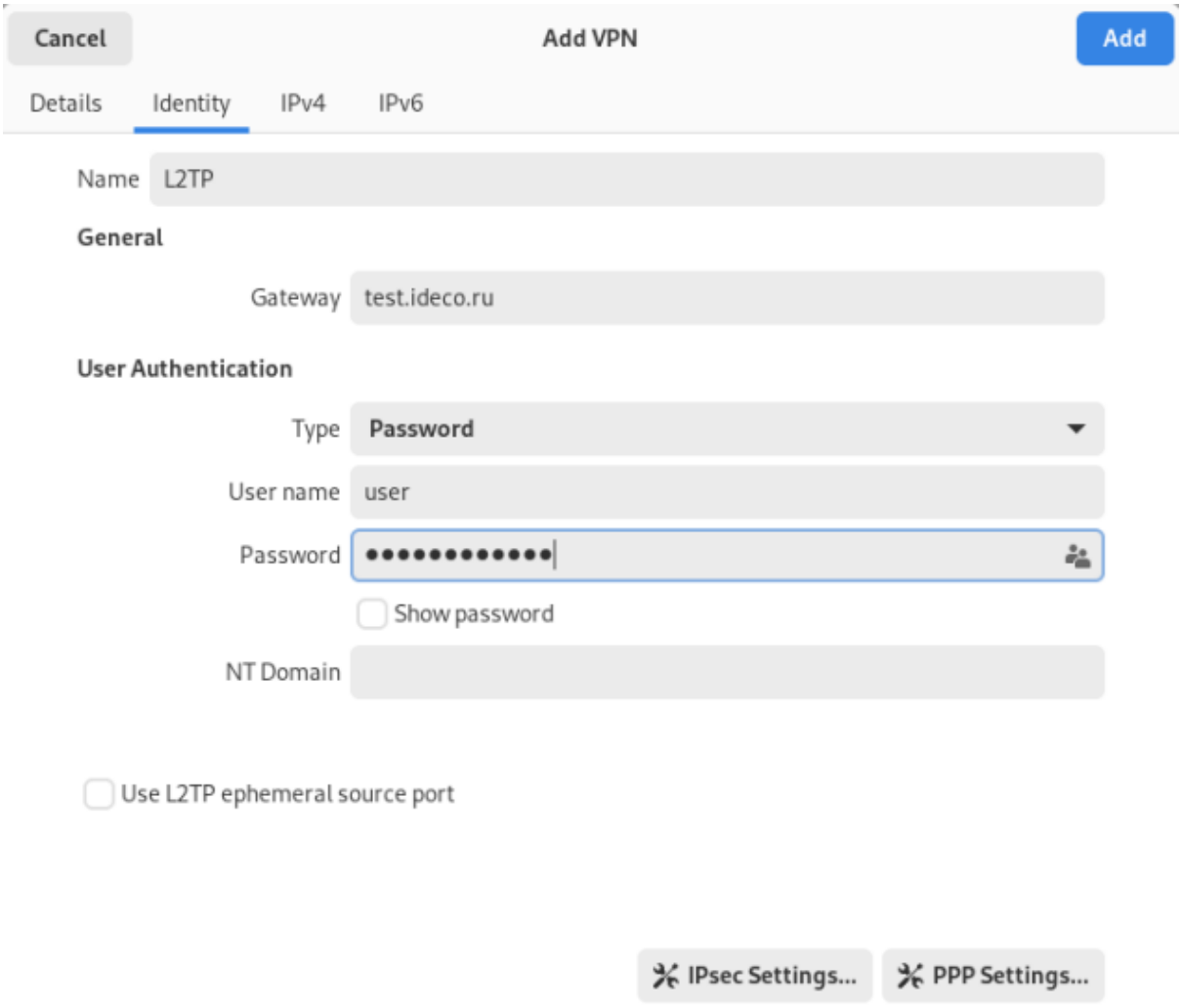
```
sudo reboot
```

4. Перейдите в **Настройки -> Сети** и в строке **VPN** нажмите + .

5. В окне создания подключений по VPN выберите пункт **Layer 2 Tunneling Protocol (L2TP)**:

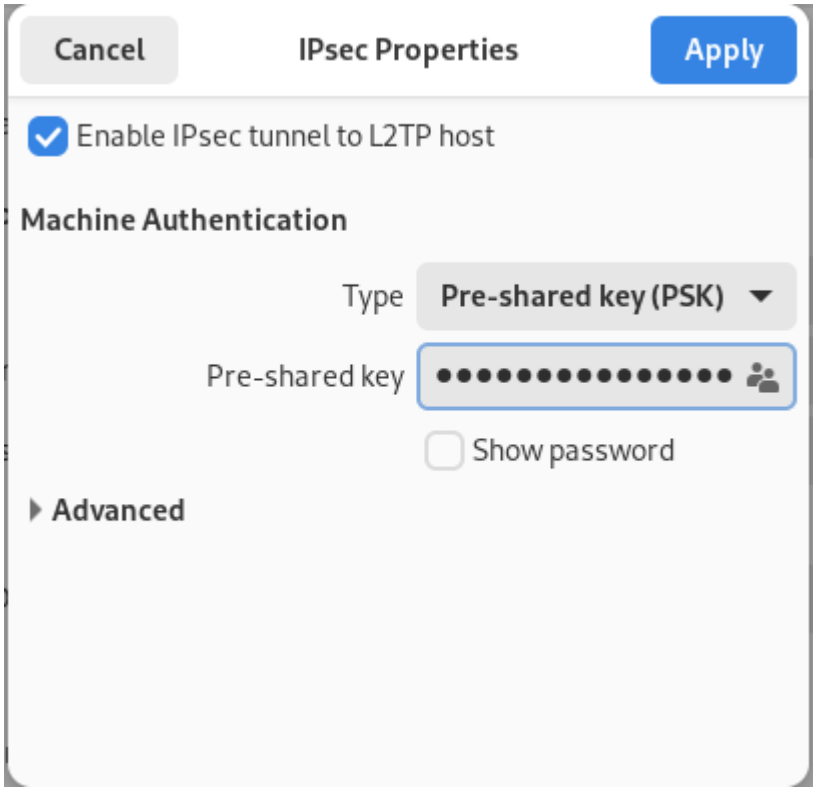


6. На вкладке **Идентификация** заполните следующие поля:



- **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:

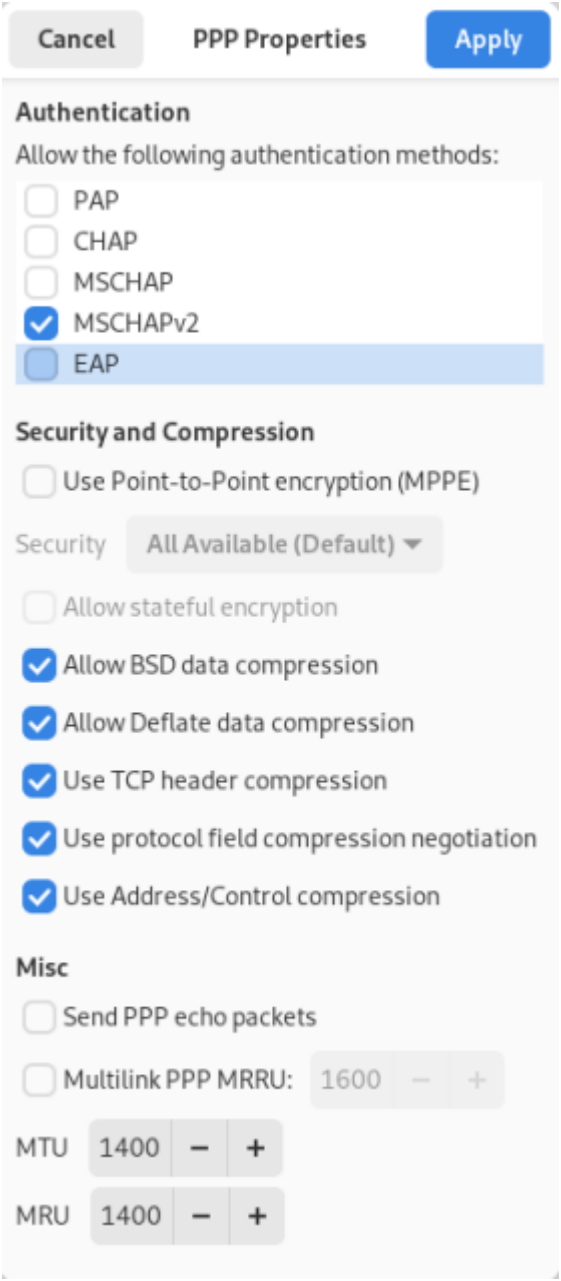


- **Type: Pre-shared key (PSK)** - аутентификация по общему ключу;
- **Pre-shared key** - ключ, который необходимо скопировать по пути **Пользователи -> VPN-подключения -> Основное** из поля **PSK**.

Раздел **Advanced** необязательный для заполнения.

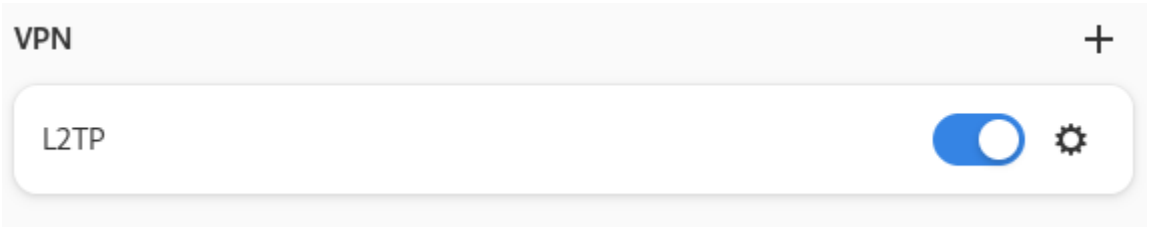
После окончания настройки **L2TP IPsec Options** нажмите **OK**.

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:



37.20.4 Создание подключения в Astra Linux

Основное

Подсказка: Перед настройкой VPN-подключения перейдите в раздел **Пользователи -> VPN-подключения -> Доступ по VPN** и создайте разрешающее VPN-подключение правило.

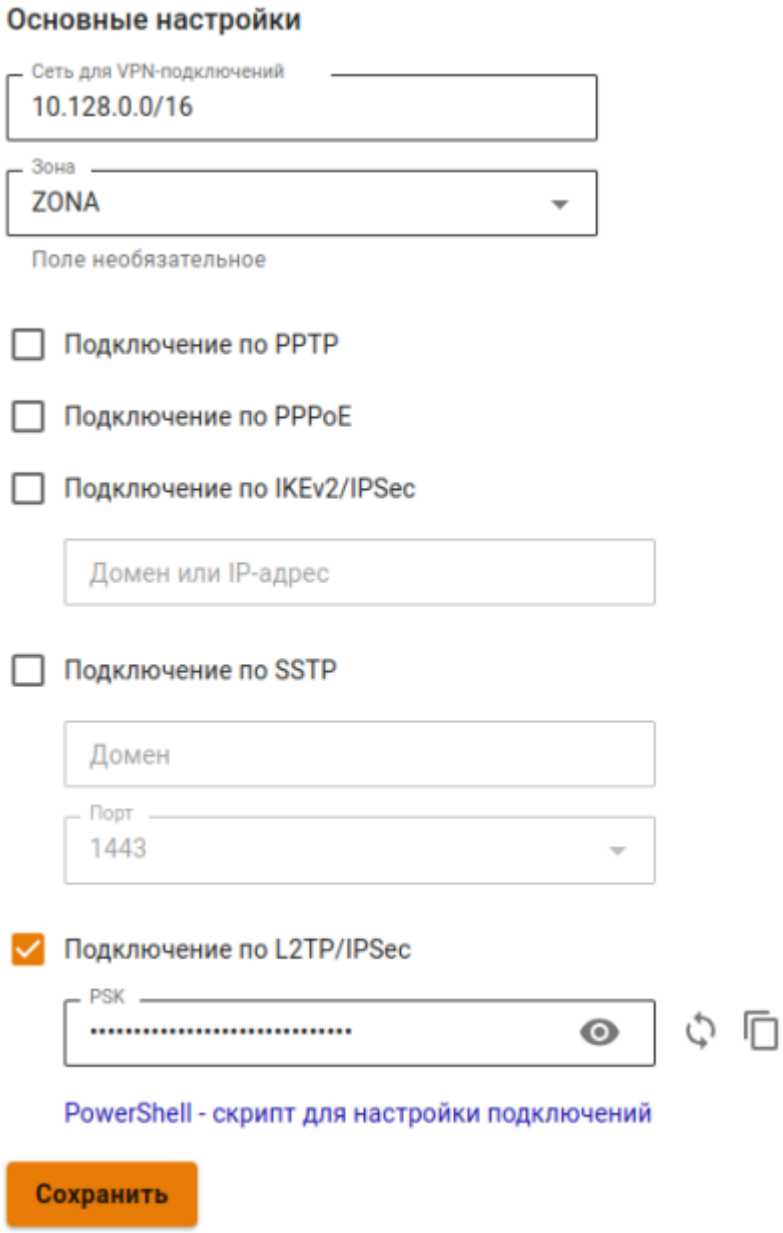
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Протокол L2TP/IPsec:

Настройка Ideco NGFW:

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

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

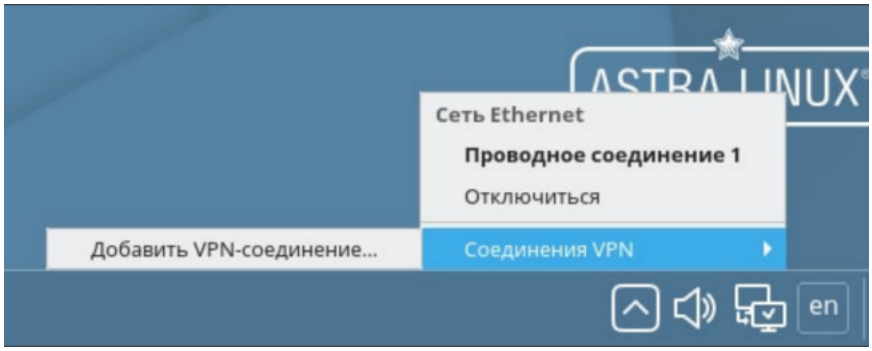


Создание подключения в Astra Linux:

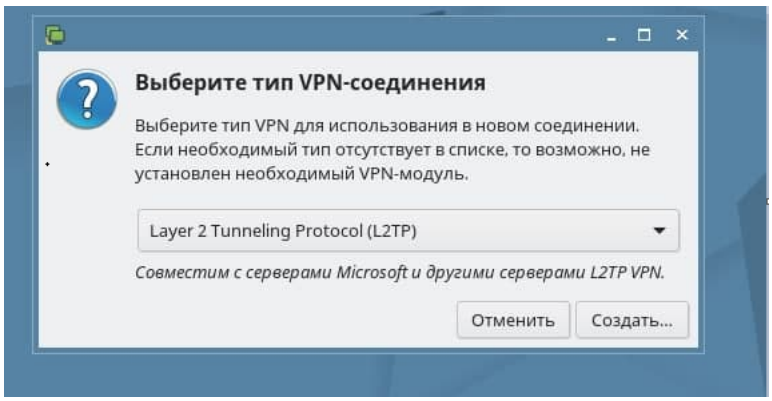
1. Откройте терминал сочетанием клавиш Ctrl+Alt+F1 или через путь **Пуск -> Системные -> Терминал Fly** и выполните три команды:

```
sudo apt update
sudo apt install network-manager-l2tp-gnome
sudo reboot
```

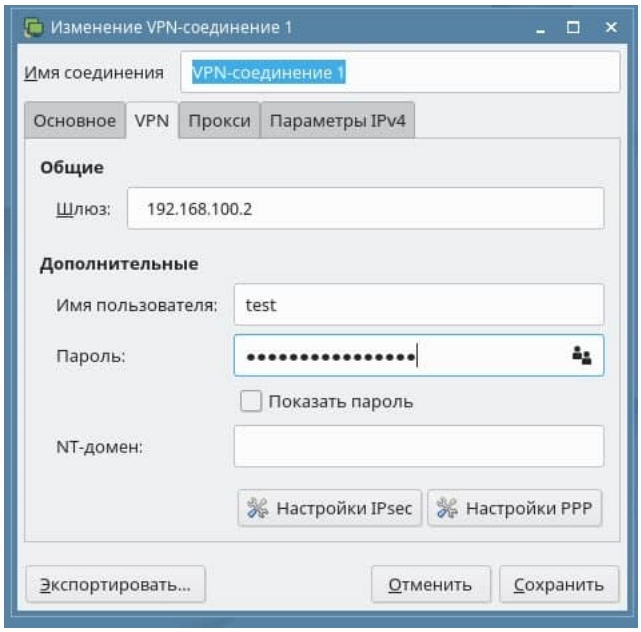
2. В трее (в настройках сети) выберите **Соединение VPN -> Добавить VPN-соединение**:



3. Выберите тип соединения **Layer 2 Tunneling Protocol (L2TP)** и нажмите **Создать**:



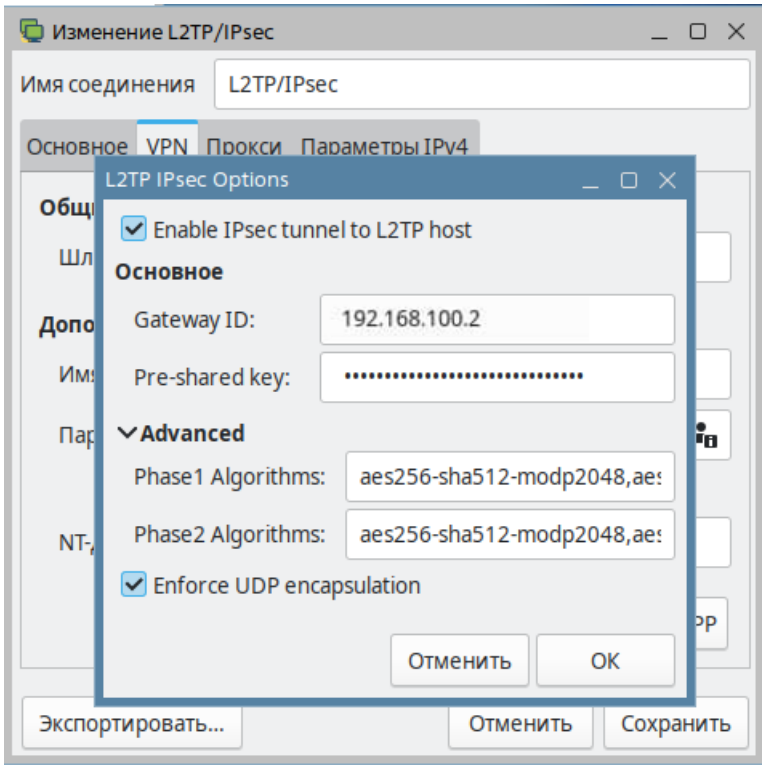
4. На вкладке **VPN** заполните поля:



- **Шлюз** - IP-адрес внешнего интерфейса Ideco NGFW или домен;
- **Имя пользователя**;
- **Пароль**.

5. Нажмите **Настройки IPsec**.

6. Заполните поля:

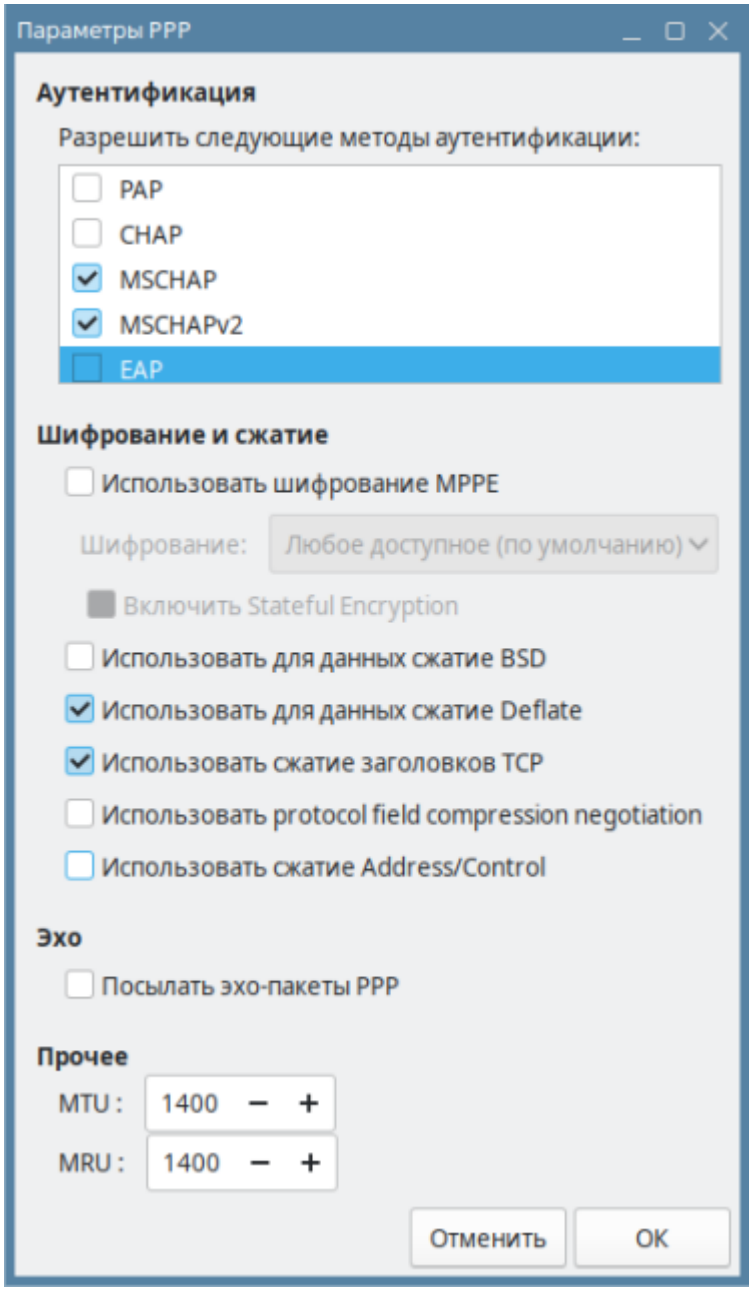


- **Gateway ID** - IP-адрес интерфейса, к которому осуществляется подключение;
- **Pre-shared key** - PSK-ключ из настроек Ideco NGFW (**Пользователи -> VPN-подключение -> Основное**);
- **Phase1 Algorithm** - `aes256-sha512-modp2048,aes256-sha512-modp1024,aes256-sha1-ecp256,aes256-sha1-modp2048,aes256-sha1-modp1024!`; *
- **Phase2 Algorithms** - `aes256-sha512-modp2048,aes256-sha256-modp2048,aes256-sha1-modp2048,aes128-sha1-modp2048,aes256-sha512-modp1024,aes256-sha256-modp1024,aes256-sha1-modp1024,aes128-sha1-modp1024,aes256-sha512,aes256-sha256,aes256-sha1,aes128-sha1!`.*

* Обязательно поставьте восклицательный знак в конце строки.

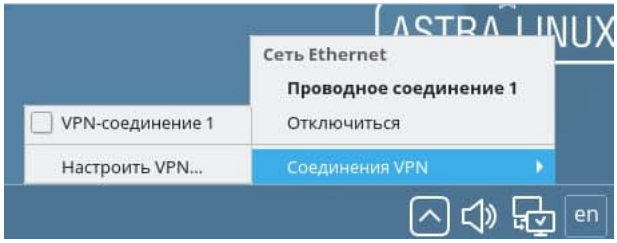
Так как Astra Linux по умолчанию запрашивает не самые защищенные алгоритмы, рекомендуем заполнить их самостоятельно.

7. При необходимости перейдите в Настройки PPP и настройте разделы **Аутентификация**, **Шифрование и сжатие**, **Прочее**:



8. Нажмите **ОК**, затем **Сохранить**.

Далее в трее (в настройках сети) **Соединение VPN** появится VPN-подключение. Для активации включите опцию **VPN-соединение**:



Подсказка: Проверить способы шифрования можно в конфигурации NGFW. Для этого включите в настройках VPN «Подключение по IKEv2/IPsec», откройте терминал NGFW и введите команду:
`cat /run/ideco-ipsec-backend/strongswan/swanctl/conf.d/rw_ikev2.conf`

- дляPhase1 Algorithm ищите значения “proposals=”;

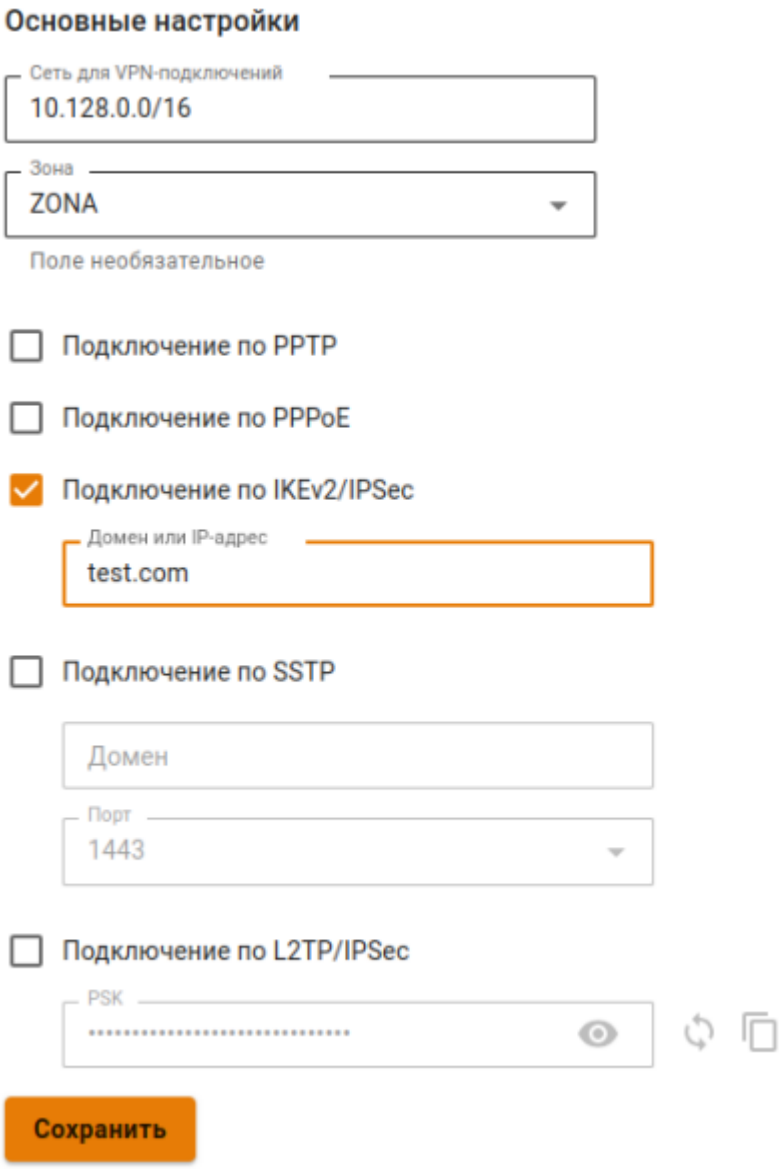
- для Phase2 Algorithms ищите значения “esp_proposals=”.

Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

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

2. Установите флаг **Подключение по IKEv2/IPsec** и заполните поле **Домен и IP-адрес**:



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

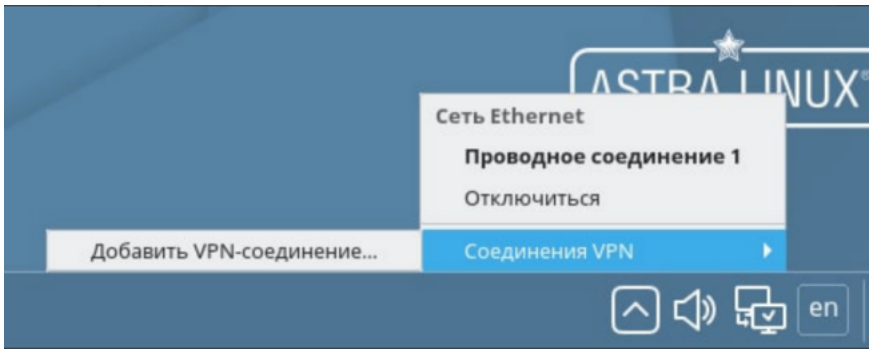
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

Создание подключения в Astra Linux:

1. Откройте терминал сочетанием клавиш Ctrl+Alt+F1 или через путь **Пуск -> Системные -> Терминал Fly** и выполните три команды:

```
sudo apt install libcharon-extra-plugins
sudo apt install -y network-manager-strongswan libcharon-extra-plugins libstrongswan-
↪extra-plugins
sudo reboot
```

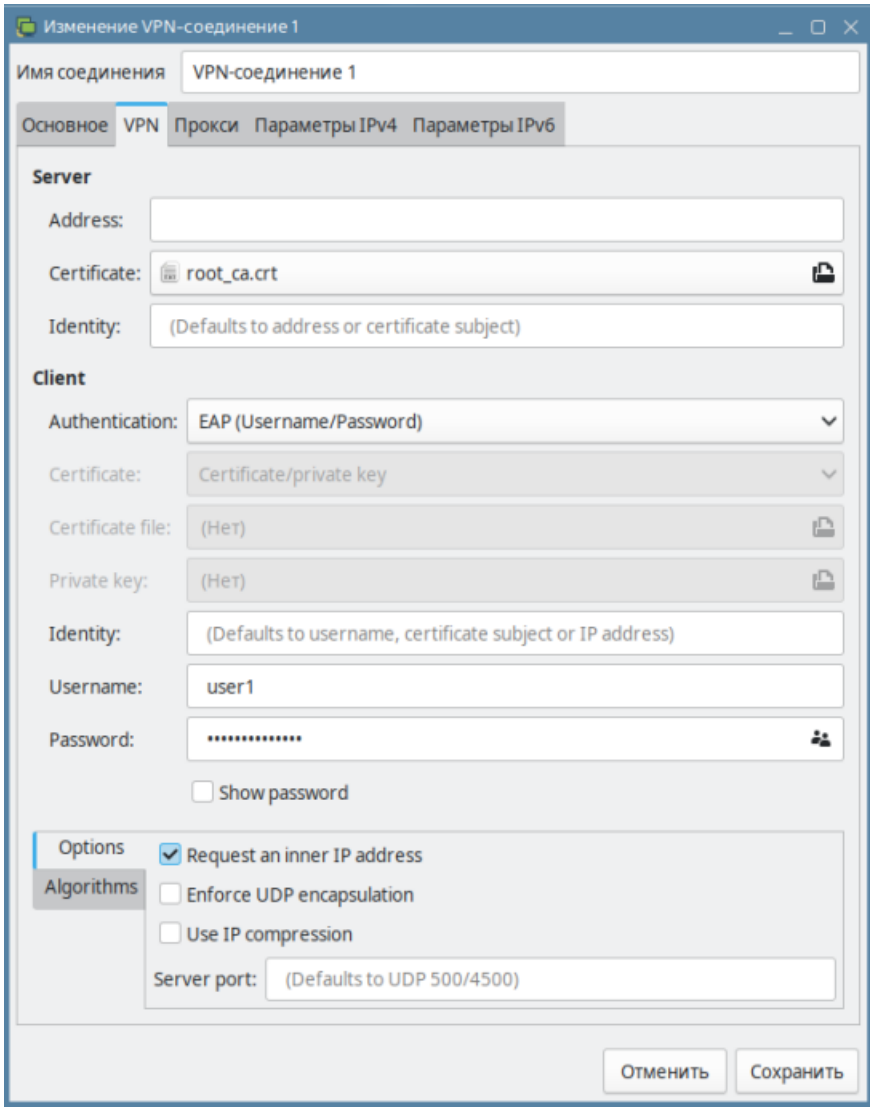
2. В трее (в настройках сети) выберите **Соединение VPN -> Добавить VPN-соединение**:



3. Выберите тип соединения **IPsec/IKEv2 (strongswan)** и нажмите **Создать**:



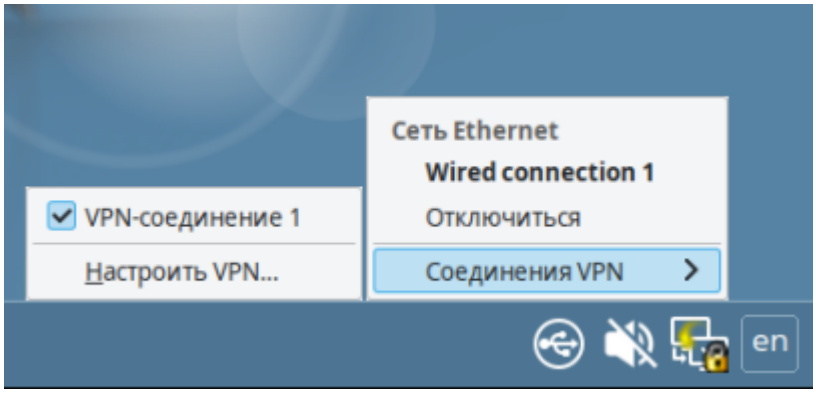
4. На вкладке **VPN** заполните следующие поля:



- **Имя соединения** - имя подключения;
- **Address** - введите домен, который указан в настройках **Пользователи -> VPN-подключения -> Основное -> Подключение по IKEv2/IPsec**;
- **Certificate** - выберите ранее сохраненный корневой сертификат (если он не был выдан Let`s Encrypt);
- **Authentication** - рекомендуем выбрать EAP (Username/Password);
- **Username** - имя пользователя, которому разрешено подключение по VPN;
- **Password** - пароль пользователя. В правой части поля необходимо выбрать вариант хранения для пароля от VPN-соединения.

Установите флаг **Request an inner IP address** и нажмите **Добавить**.

5. В трее (в настройках сети) выберите **Соединение VPN** и установите флаг в строке с созданным соединением.



37.20.5 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.

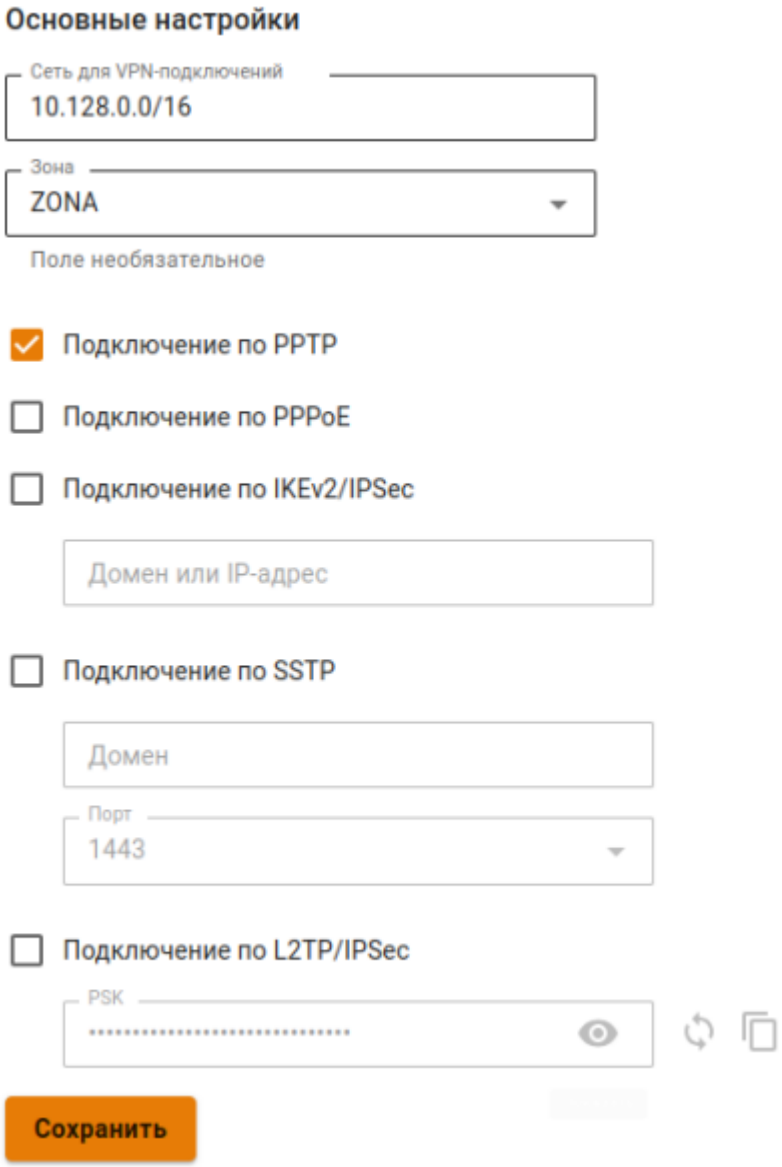
Создание VPN-подключения в Windows

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:

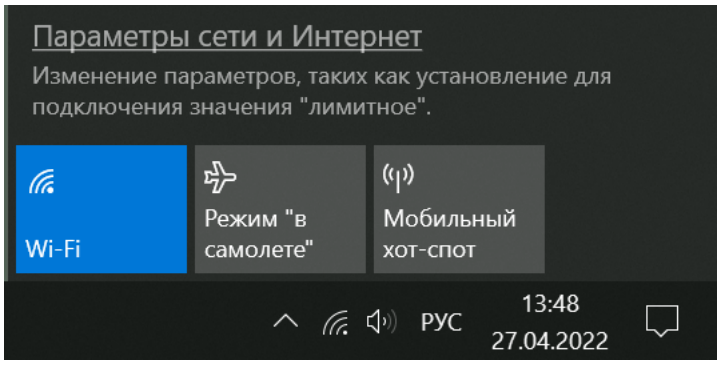
Настройка Ideco NGFW:

1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное** и установите флаг **Подключение по PPTP**:

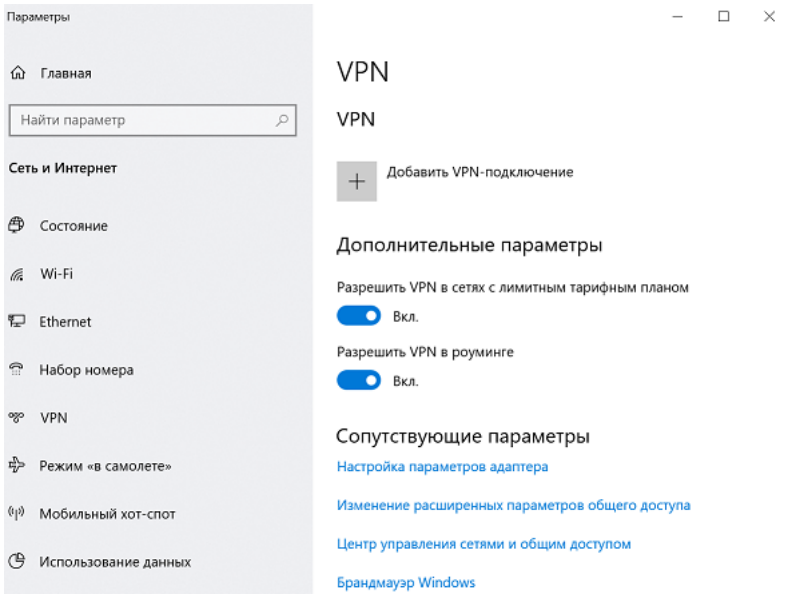


Создание подключения в Windows:

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**:



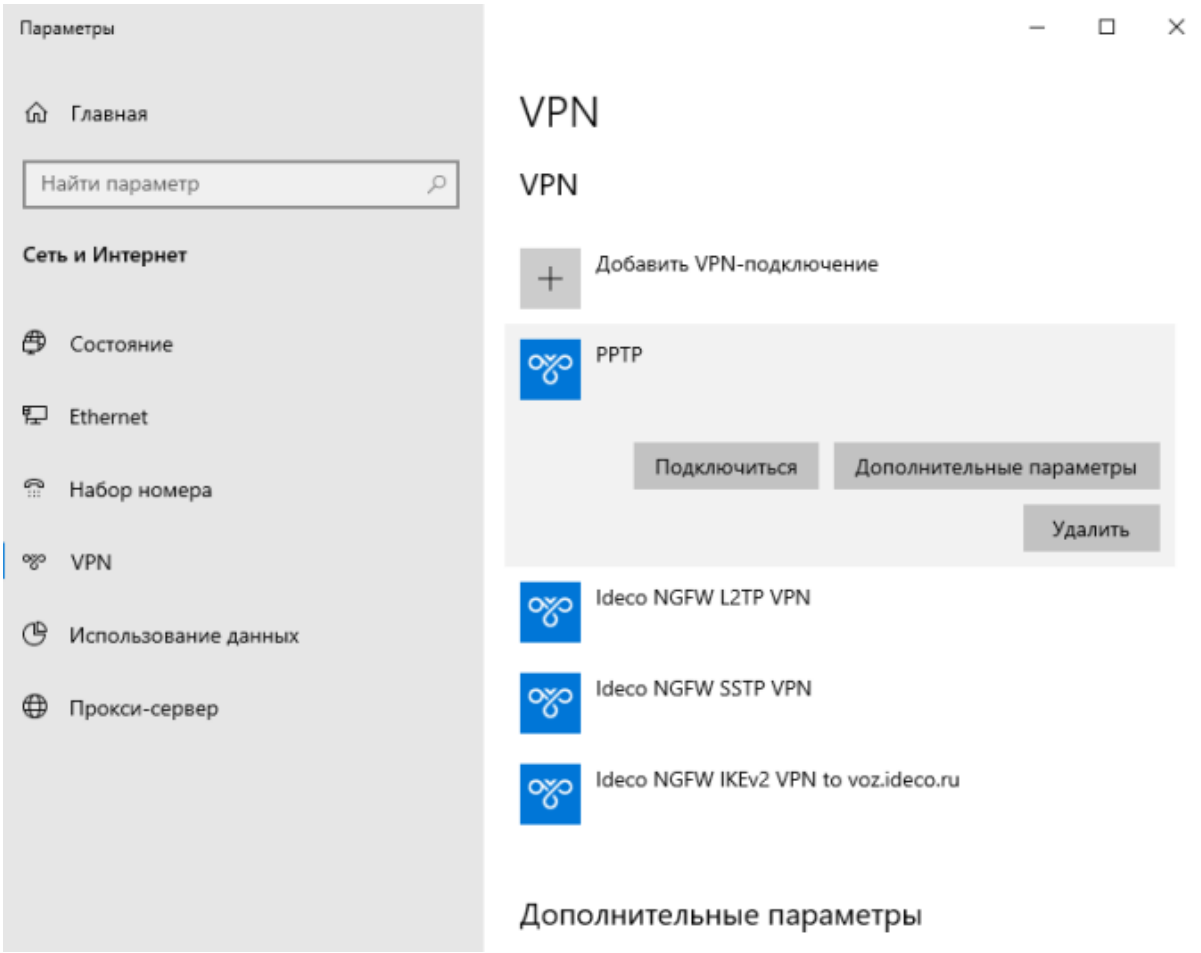
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол PPTP;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

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**.

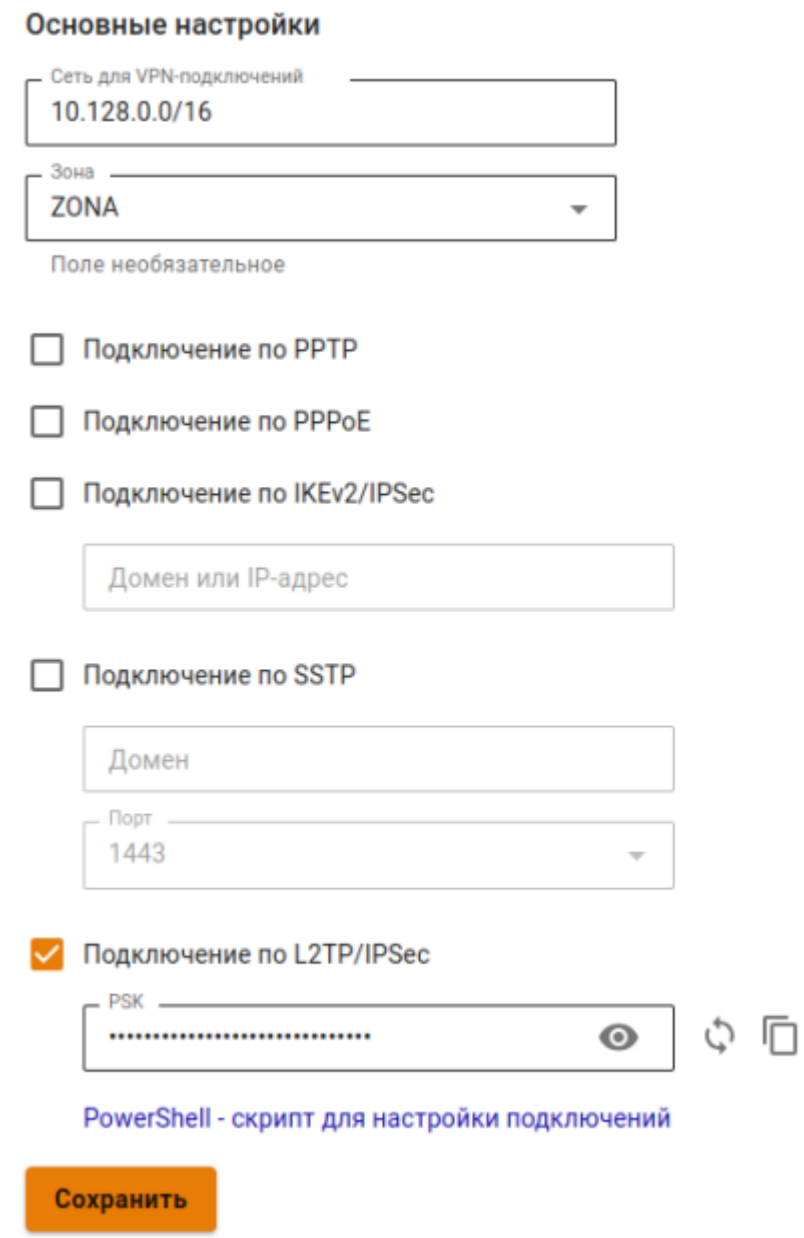
Протокол L2TP/IPsec с общим ключом:

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:

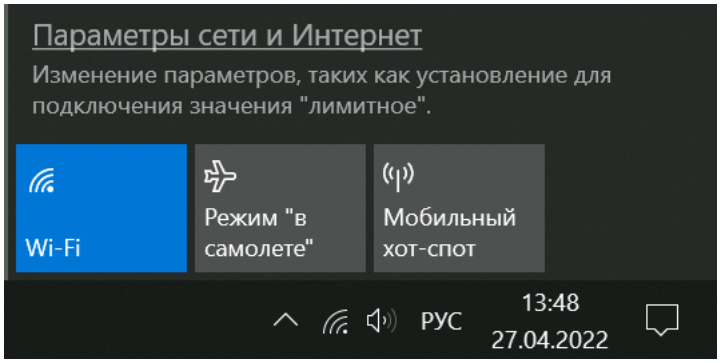
1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:

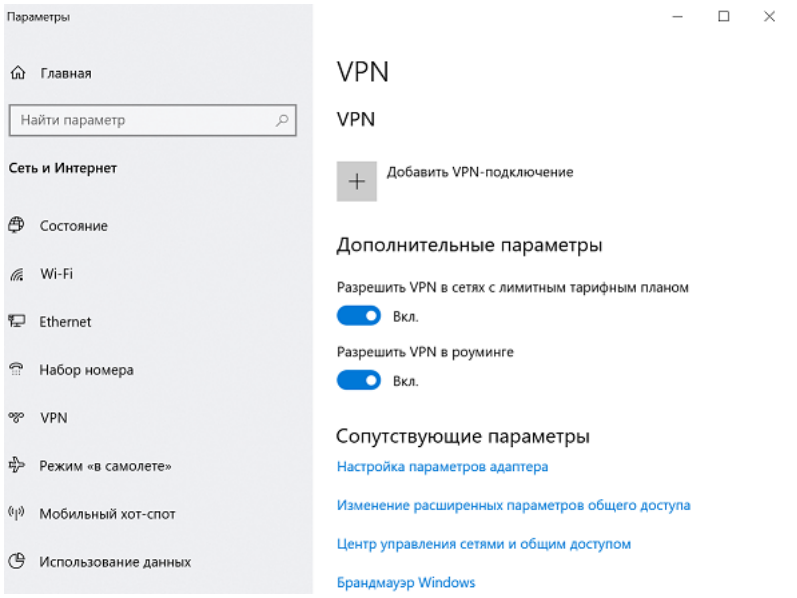


Создание подключения в Windows:

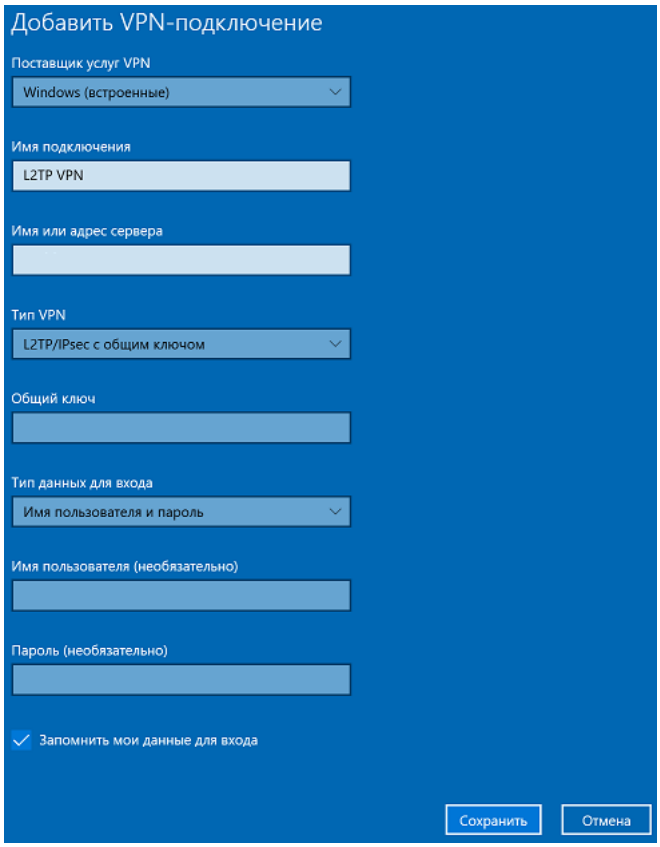
1. Кликните на иконке сетевого подключения в системном трее и в появившемся окне выберите **Параметры сети и интернет**:



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;

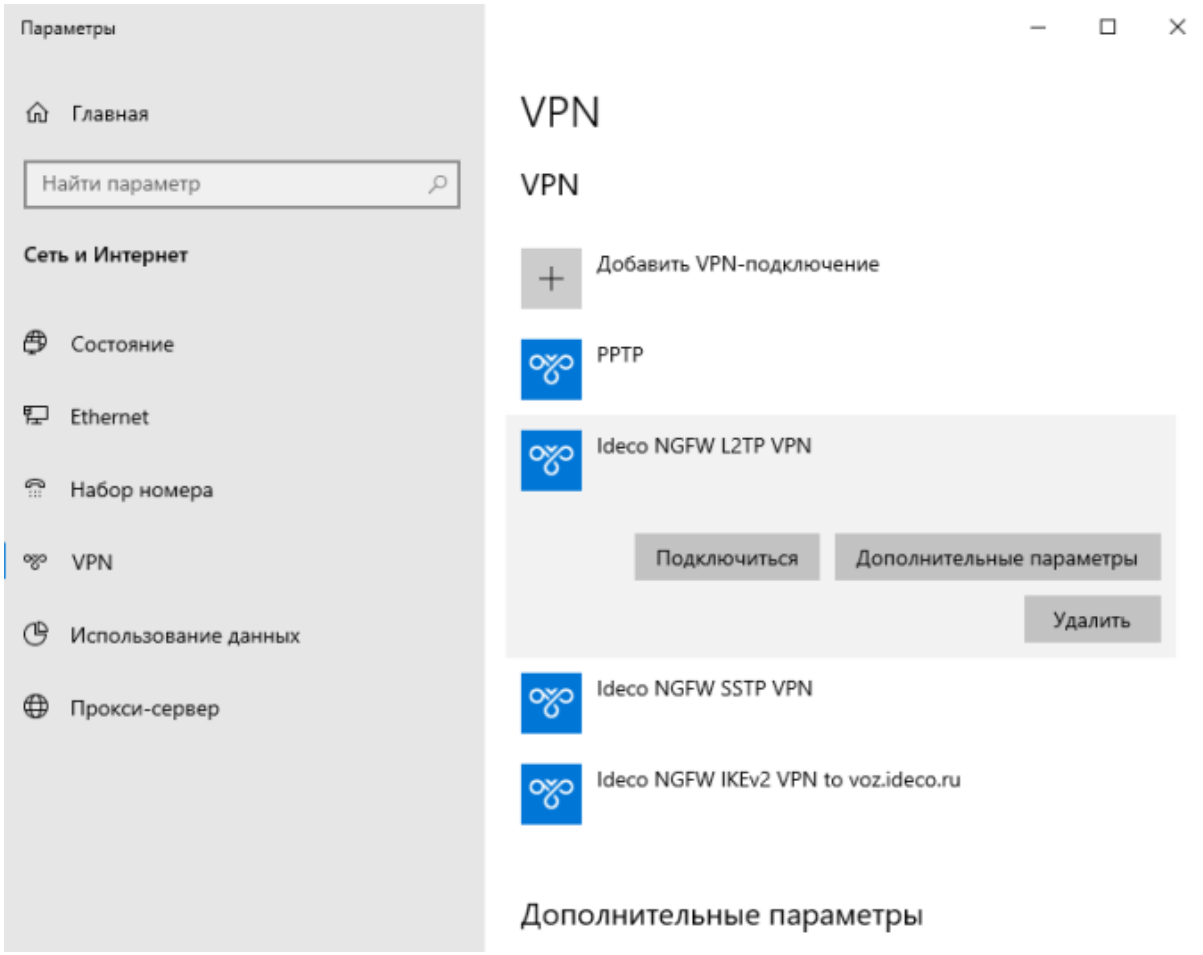
- **Пароль** - пароль пользователя.

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.

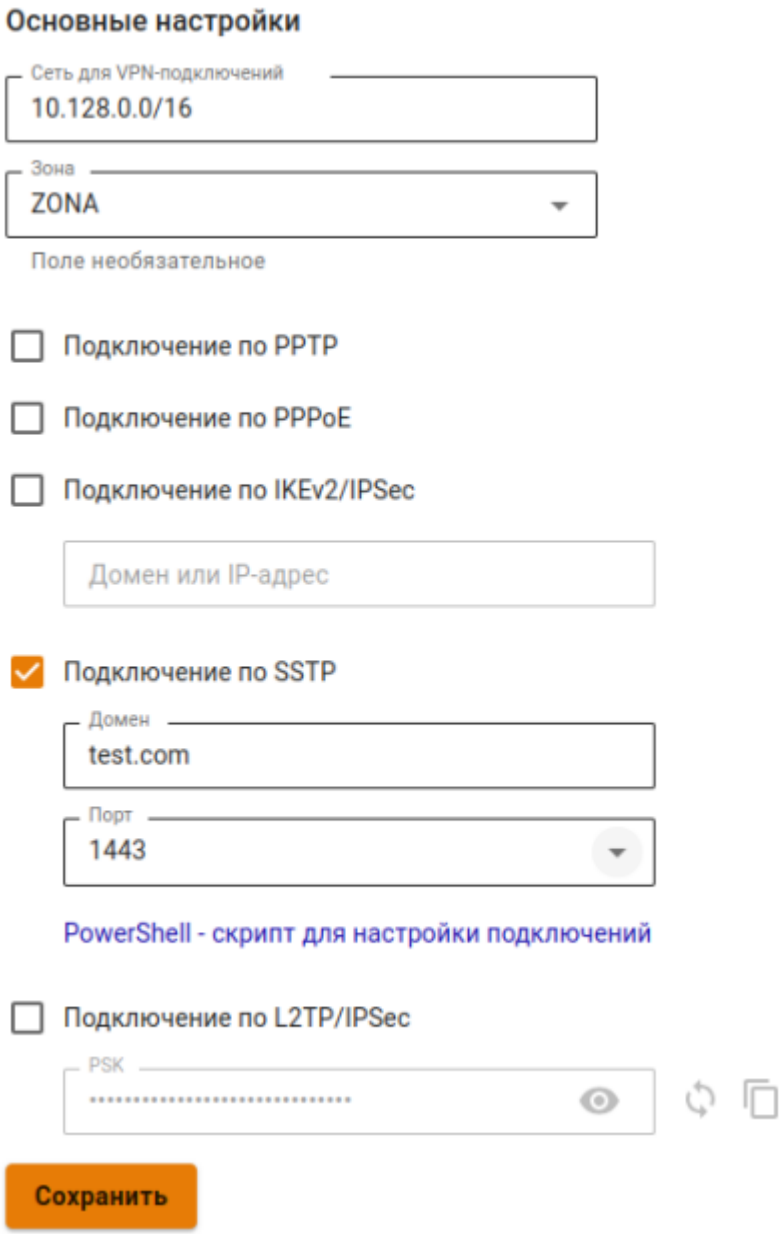
Убедитесь, что локальная сеть (или адрес на сетевой карте) на удаленной машине не пересекается с локальной сетью организации. Если пересекается, то доступа к сети организации не будет (трафик по таблице маршрутизации пойдет в физический интерфейс, а не в VPN). Адресацию необходимо менять.

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**:

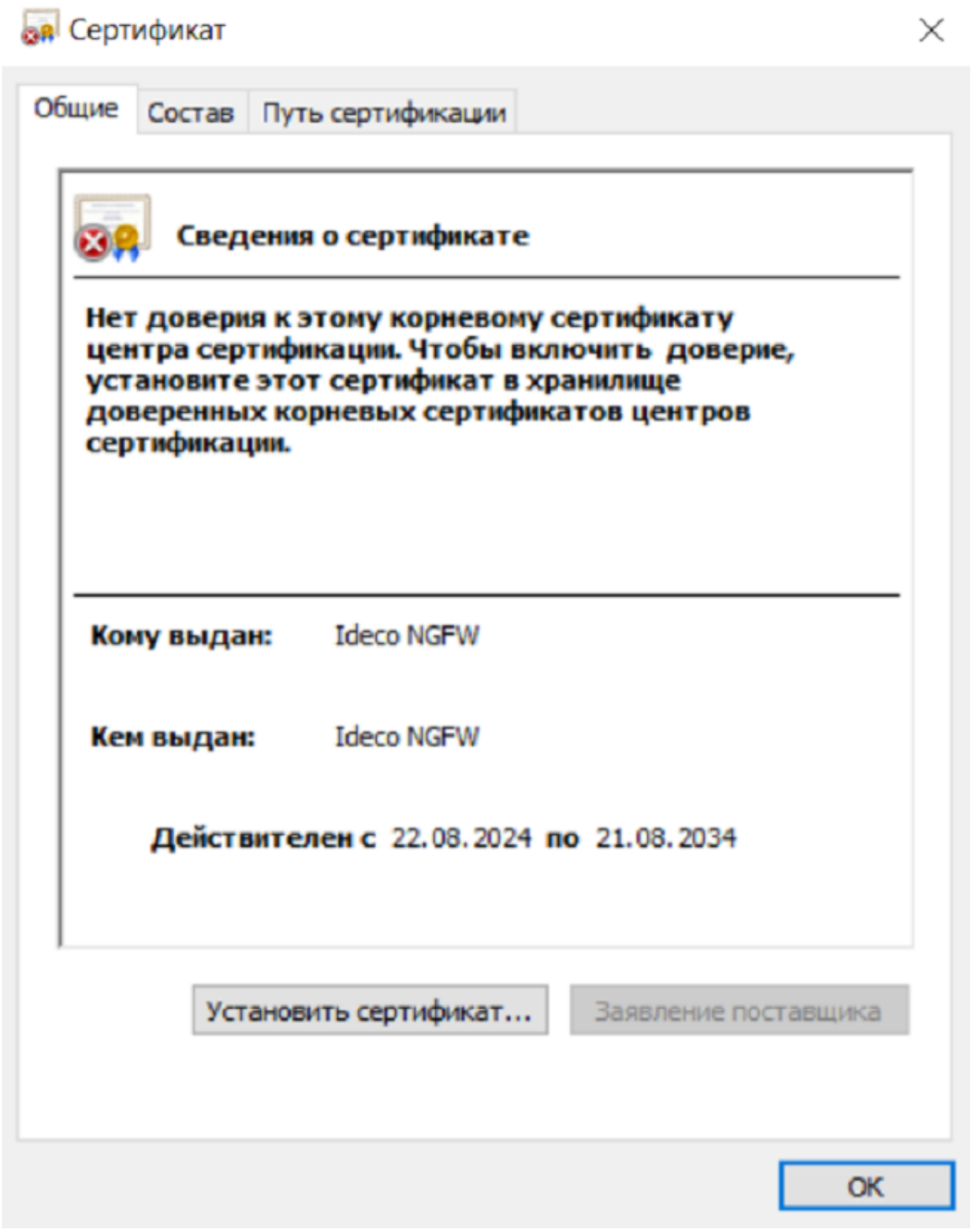


3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

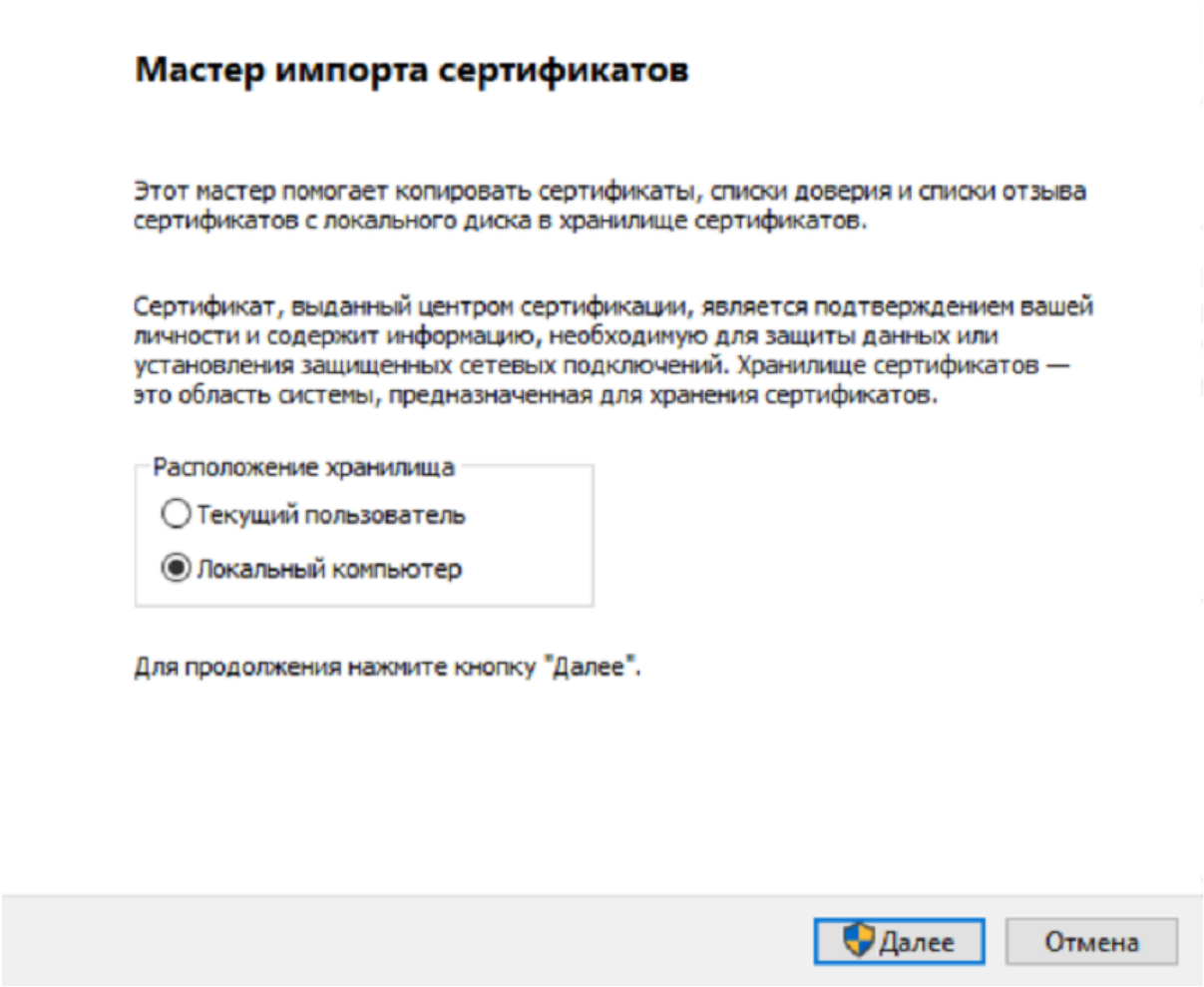
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

4. Импортируйте сертификат Ideco NGFW в Windows. Для этого выполните действия:

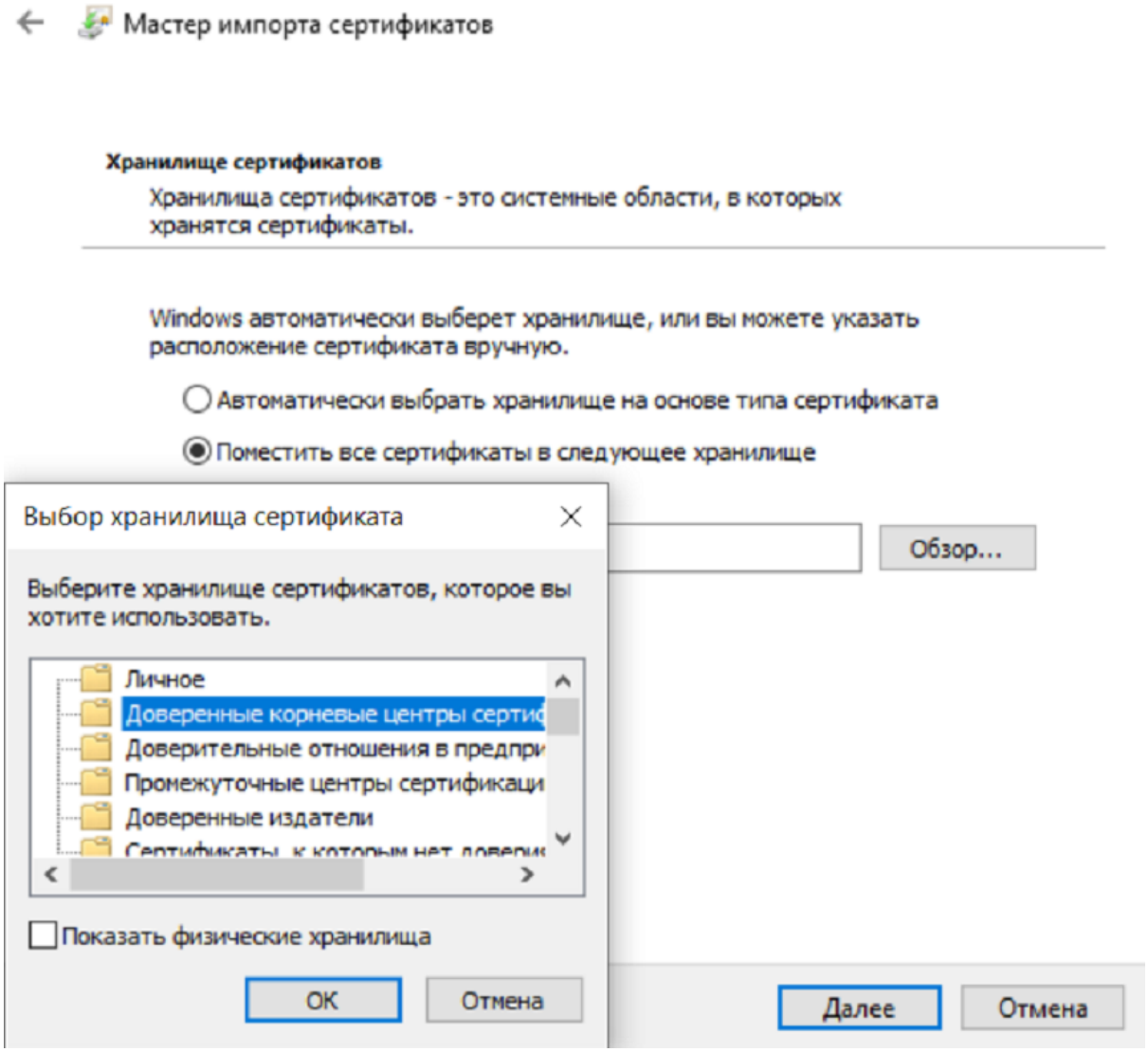
- Откройте скачанный сертификат и нажмите **Установить сертификат**:



- Для корректной настройки выберите расположение хранилища **Локальный компьютер**:

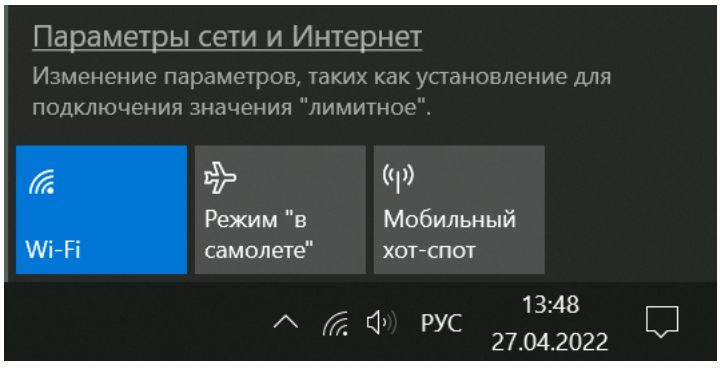


- Установите сертификат в **Доверенные корневые центры сертификации**:

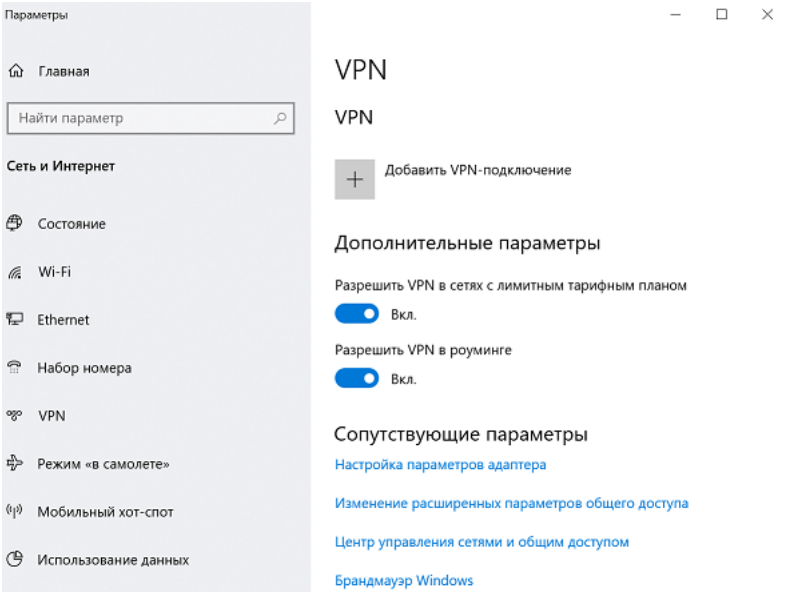


Создание подключения в Windows:

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**:



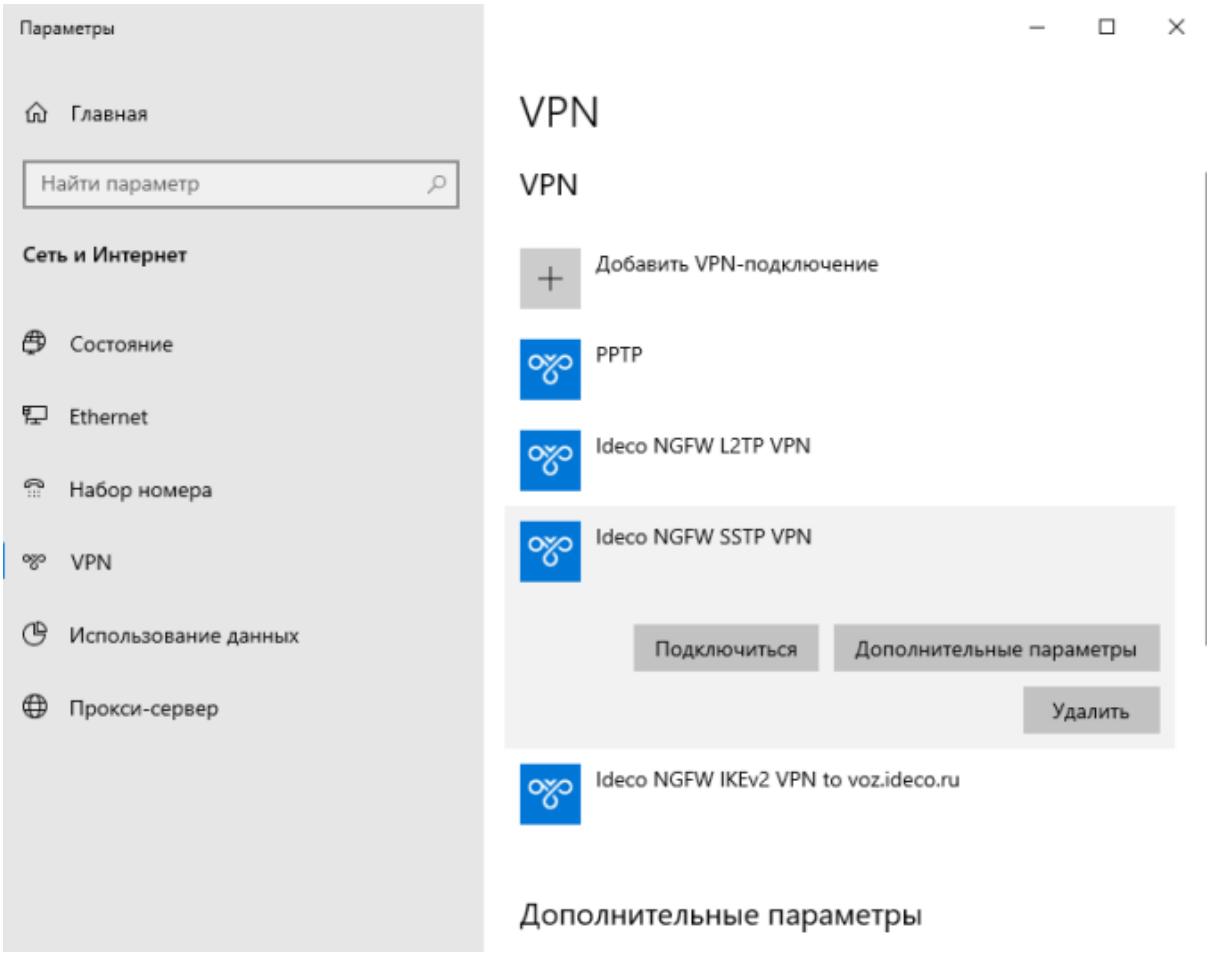
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера в формате *адрес_VPN_сервера:порт*;
- **Тип VPN** - протокол SSTP;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение 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**:



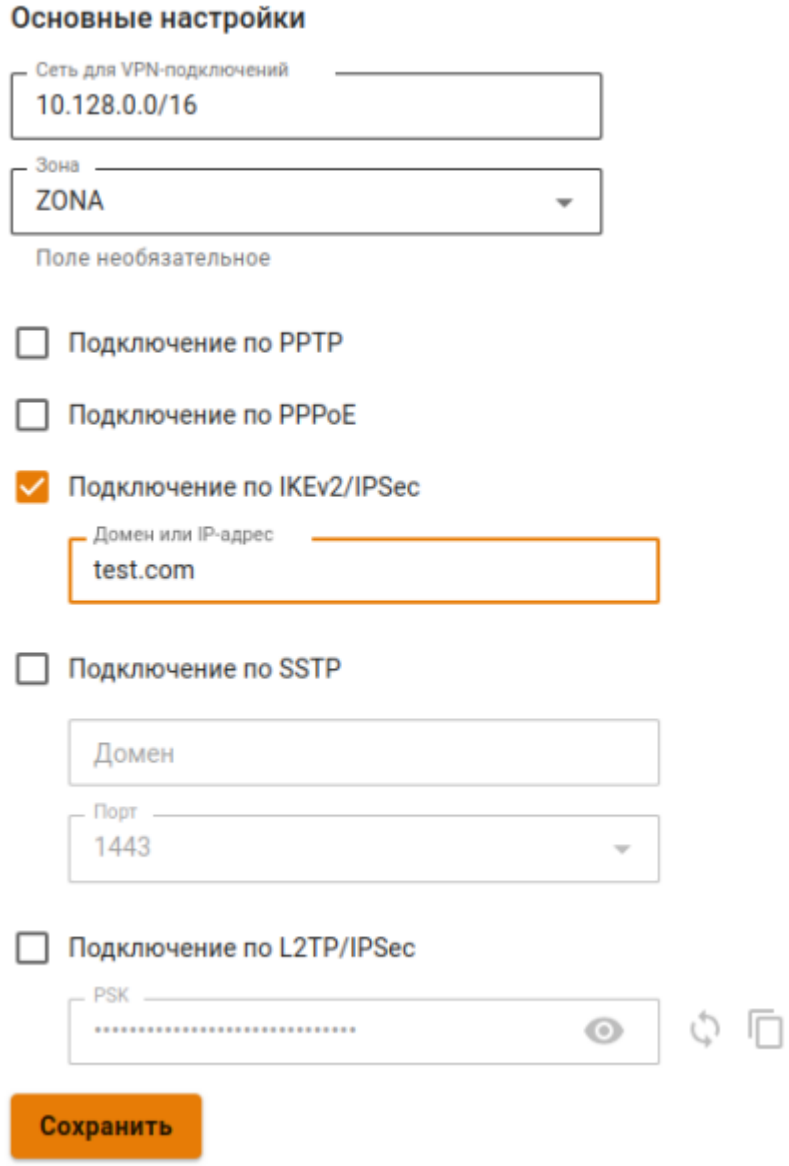
7. Для разрыва подключения нажмите **Отключиться**. Если нужно внести изменение в созданное подключение, нажмите **Дополнительные параметры -> Изменить**.

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**:

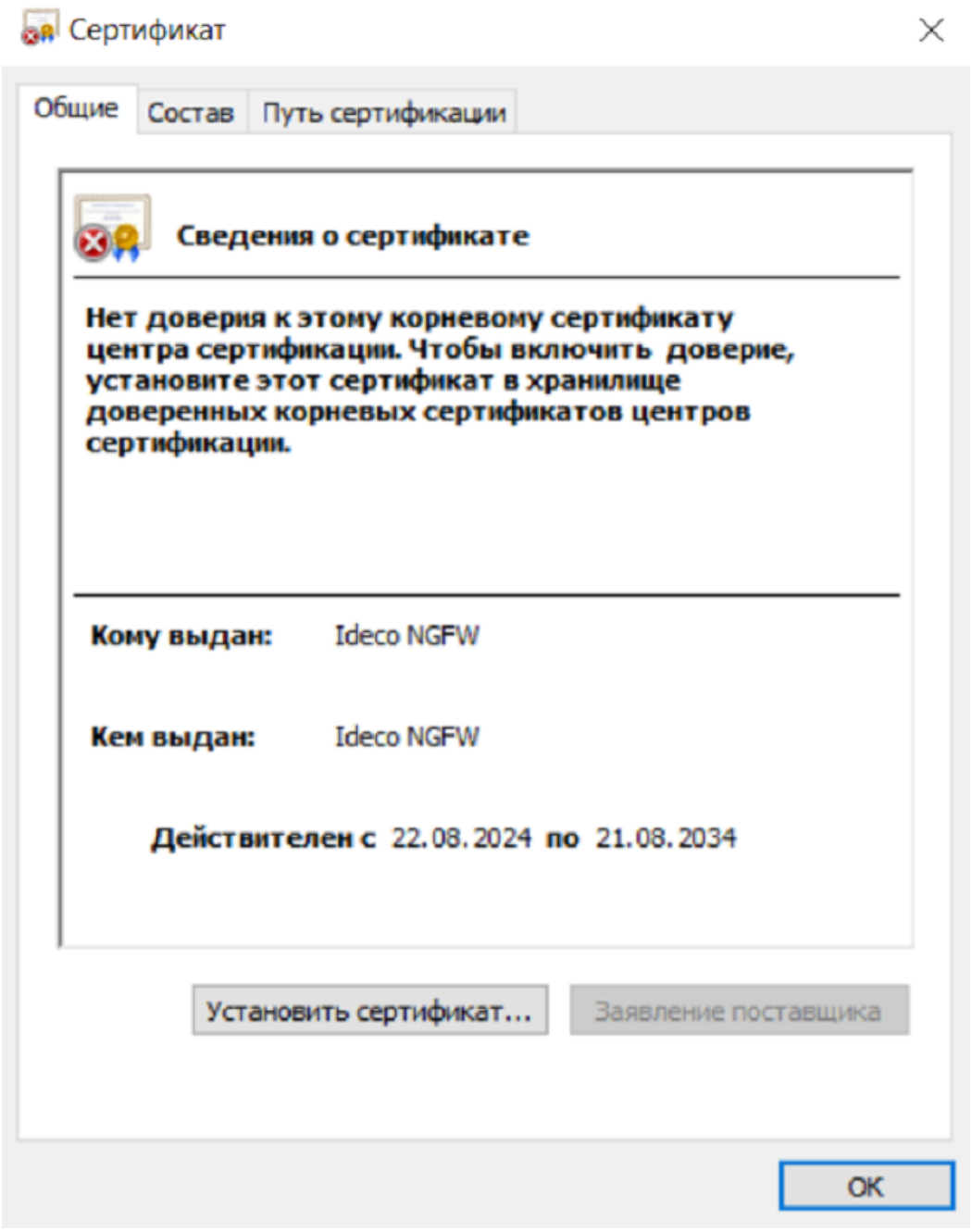


3. Скачайте корневой сертификат Ideco NGFW в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

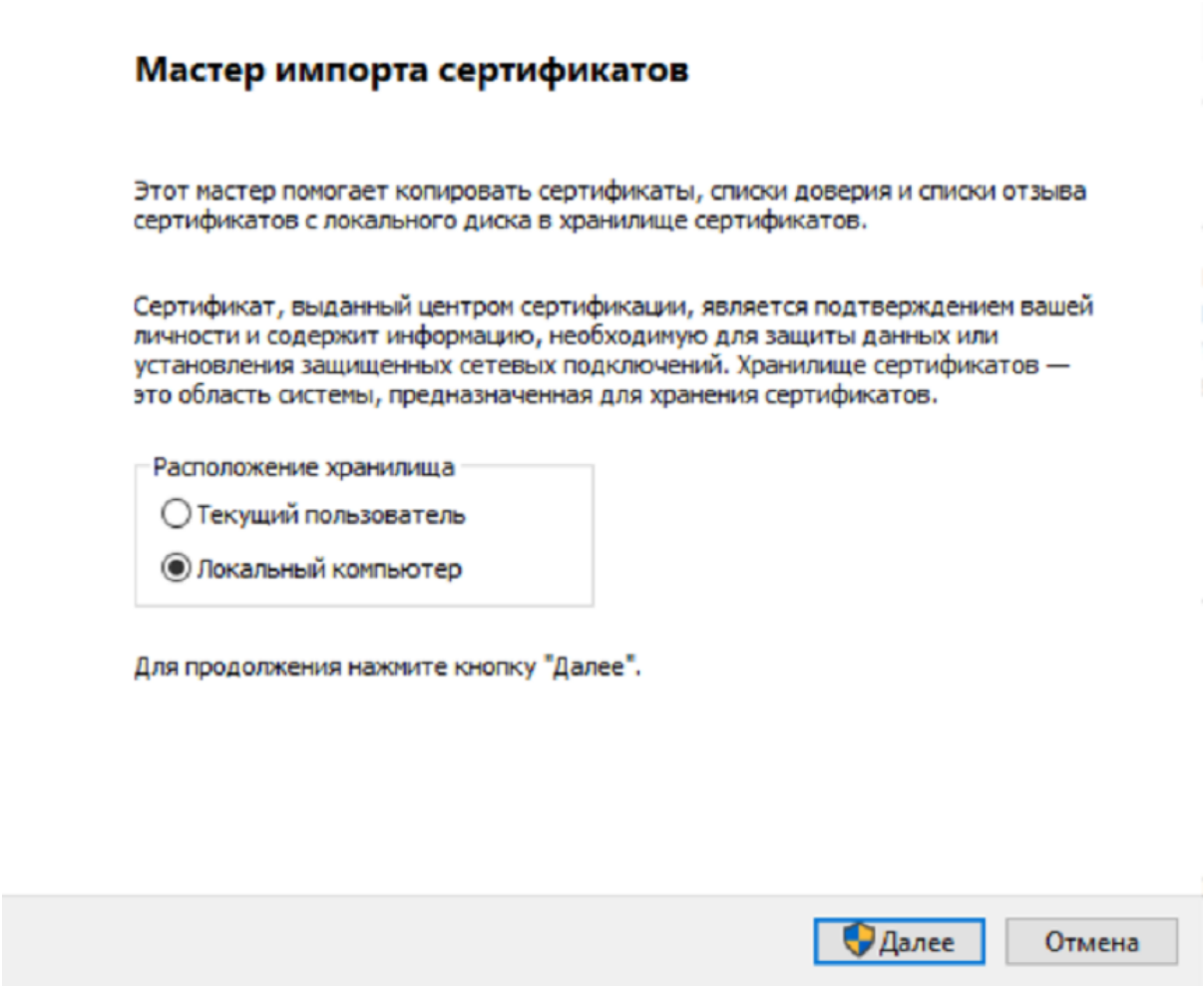
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка корневого сертификата на устройство не требуется.

4. Импортируйте сертификат Ideco NGFW в Windows. Для этого выполните действия:

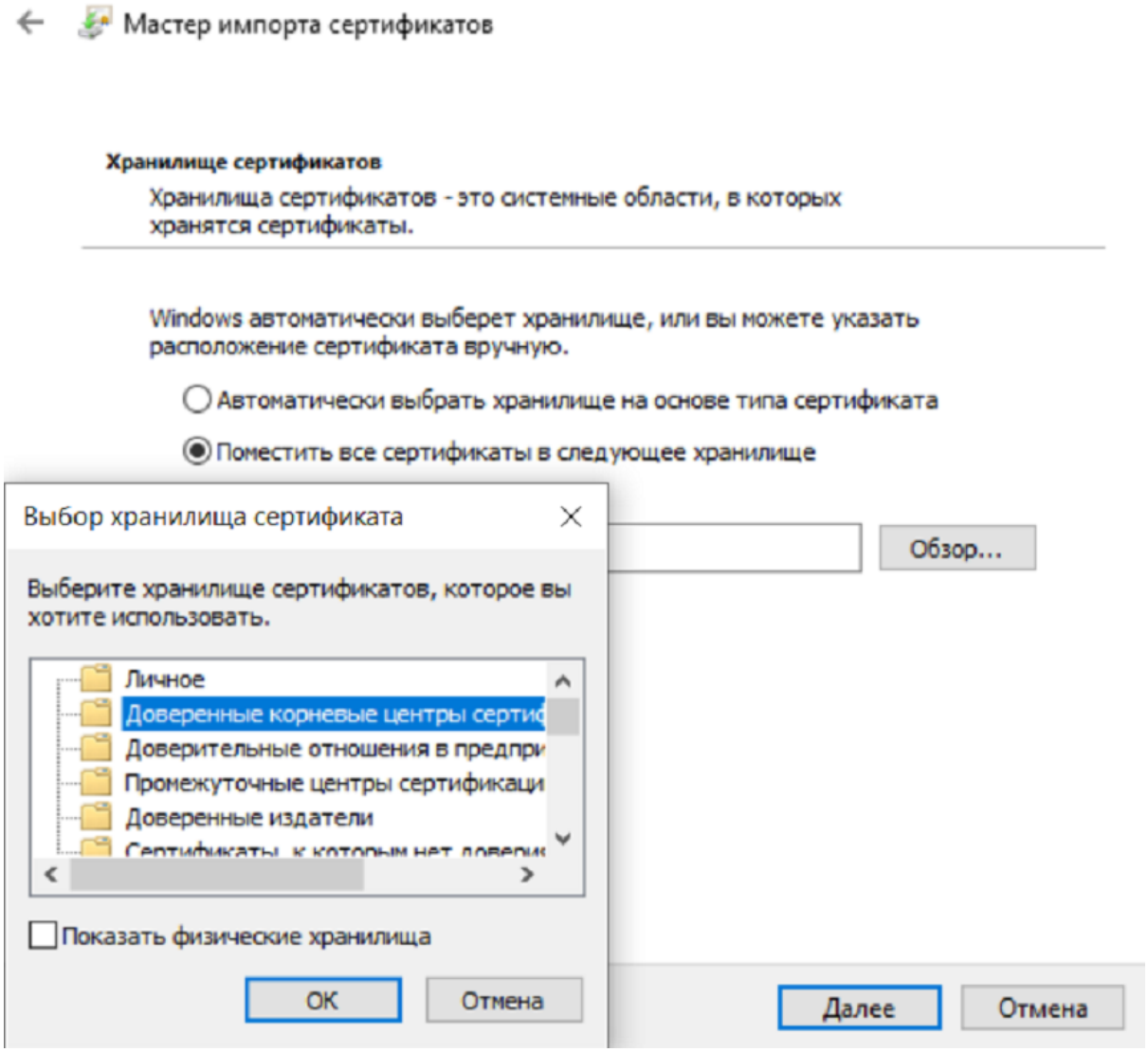
- Откройте скачанный сертификат и нажмите **Установить сертификат**:



- Для корректной настройки выберите расположение хранилища **Локальный компьютер**:

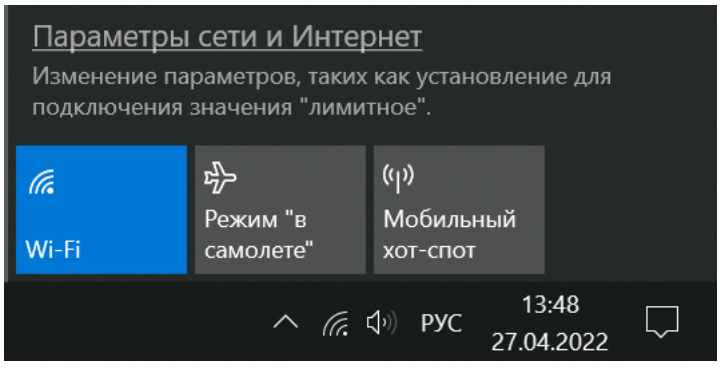


- Установите сертификат в **Доверенные корневые центры сертификации**:

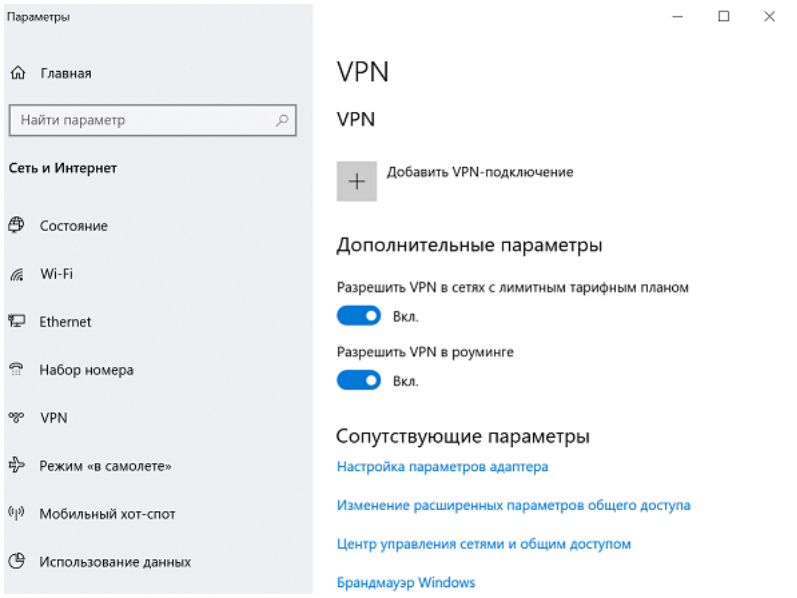


Создание подключения в Windows:

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**:



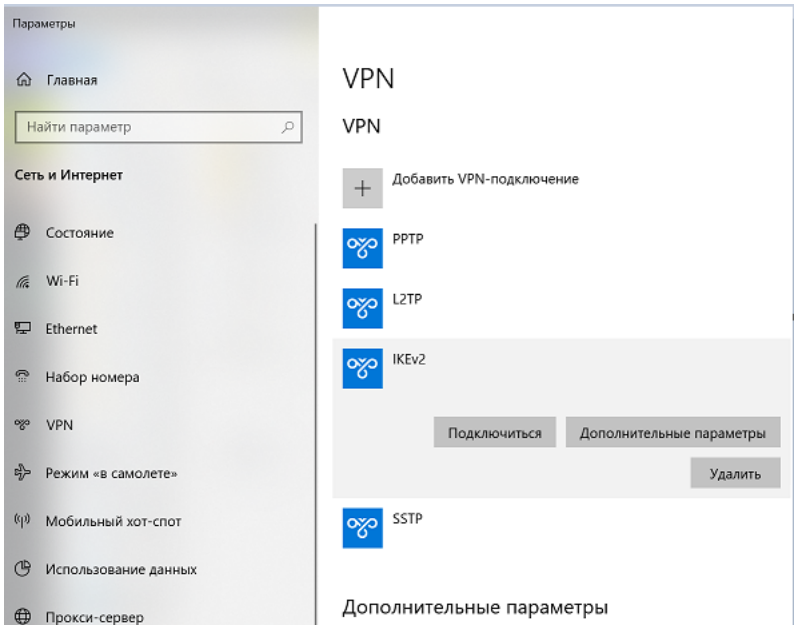
- **Имя подключения** - название создаваемого подключения;
- **Имя или адрес сервера** - адрес VPN-сервера;
- **Тип VPN** - протокол IKEv2;
- **Тип данных для входа** - имя пользователя и пароль;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

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

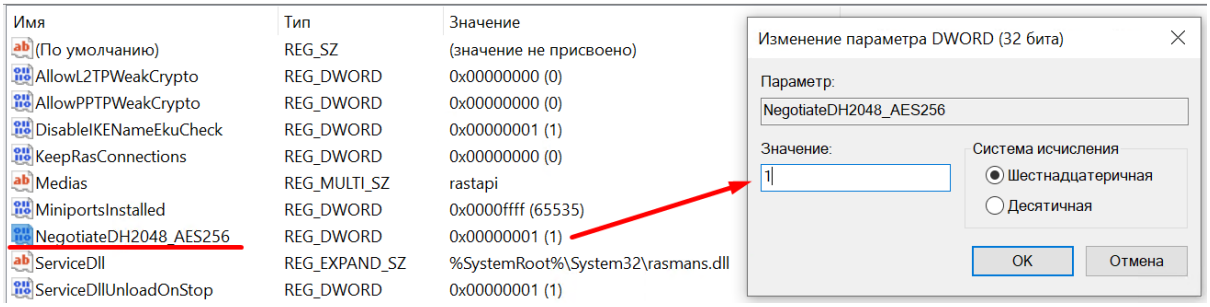
Если при подключении по IKEv2 возникает «Ошибка сопоставления групповой политики» или ошибка с кодом «13868»:

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:

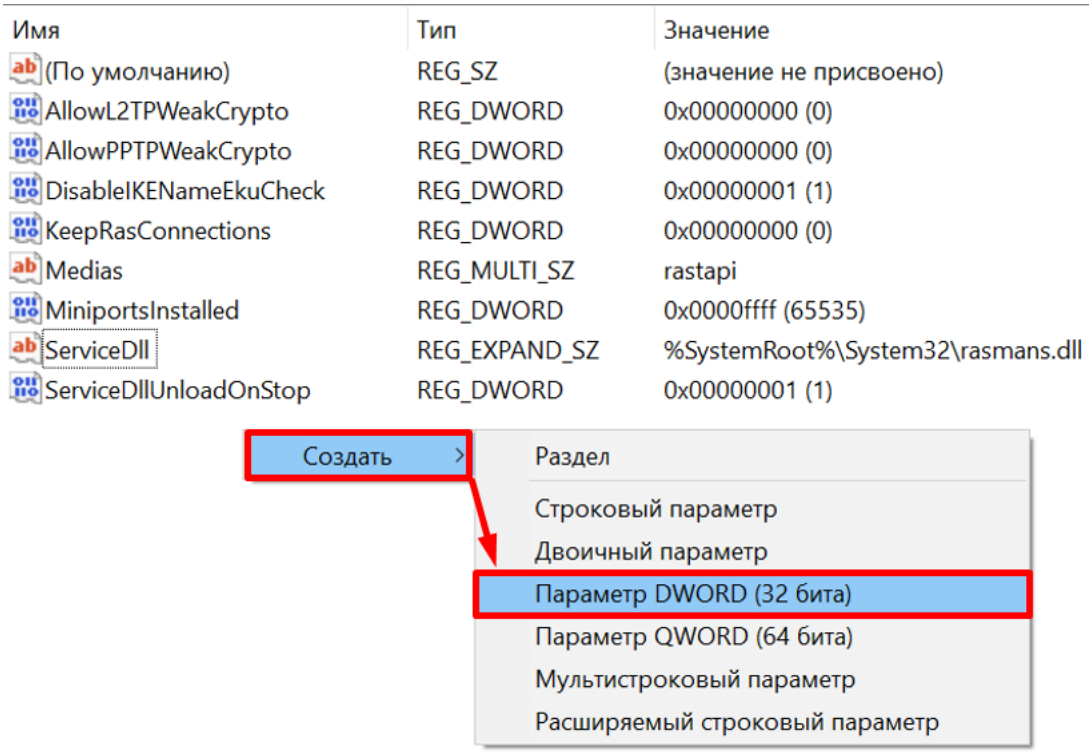
- Откройте **Редактор реестра**;
- Перейдите по пути `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters`;
- Нажмите правой кнопкой мыши по параметру с именем **NegotiateDH2048_AES256** и нажмите **Изменить**;
- В строке **Значение** укажите значение `1`:



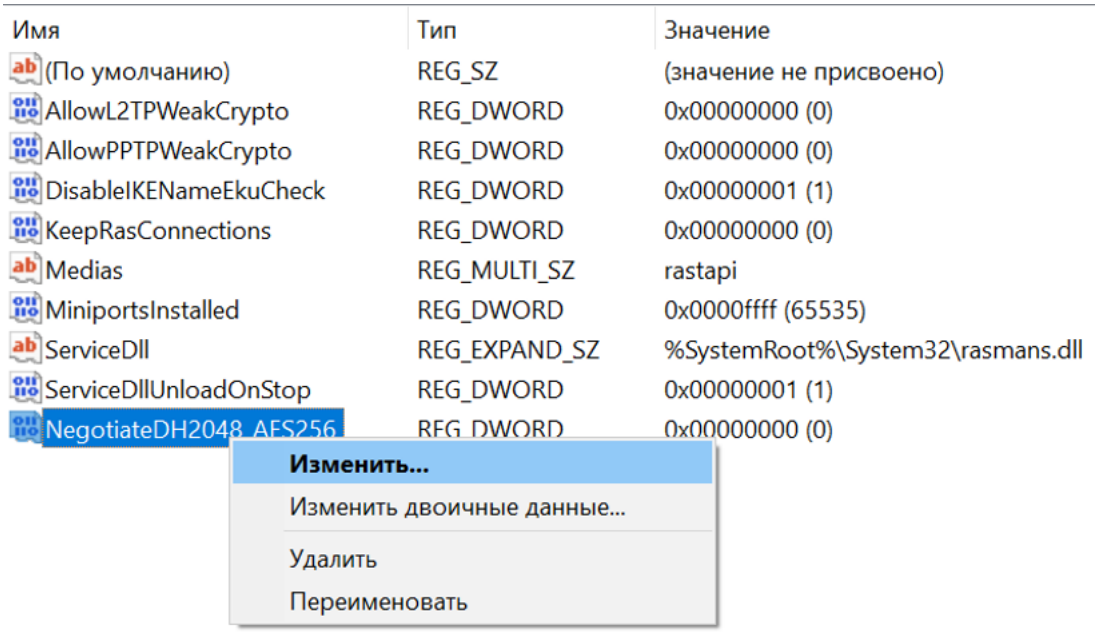
- Нажмите **OK**;
- Перезагрузите Windows.

  Если параметра с именем **NegotiateDH2048_AES256** нет, то создайте его. Для этого:

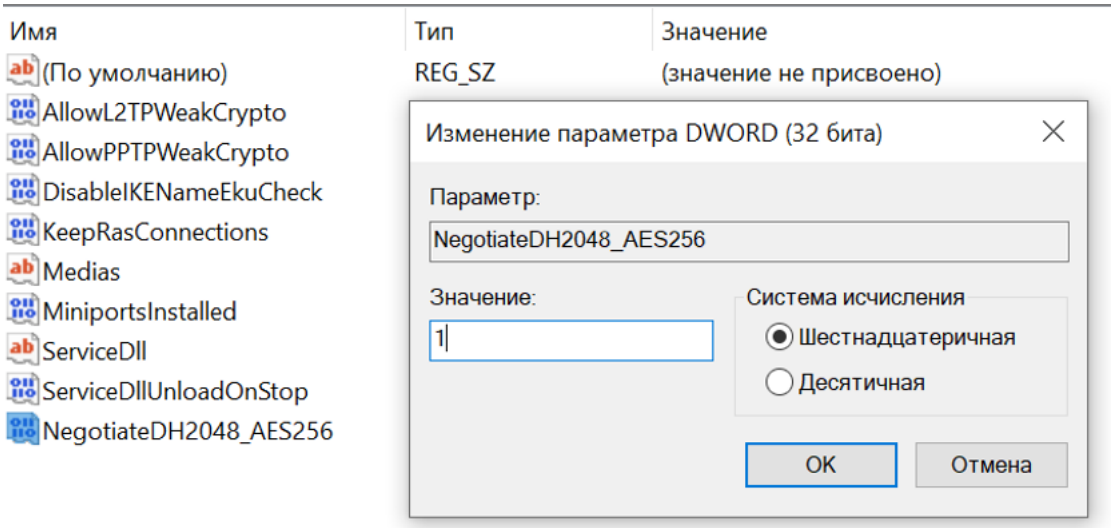
- Нажмите правой кнопкой мыши по свободному месту реестра в **Parameters** и выберите **Создать -> DWORD**:



- 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*.

37.20.6 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.

Для использования протокола IKEv2/IPsec установите корневой сертификат NGFW на устройство пользователя. Корневой сертификат потребуется для настройки подключения рабочей станции пользователя в случае, если не был получен корневой сертификат Let's Encrypt. Скачать сертификат можно в разделе **Сервисы -> Сертификаты -> Загруженные сертификаты** в веб-интерфейсе NGFW или в личном кабинете пользователя по кнопке **Скачать корневой сертификат**.

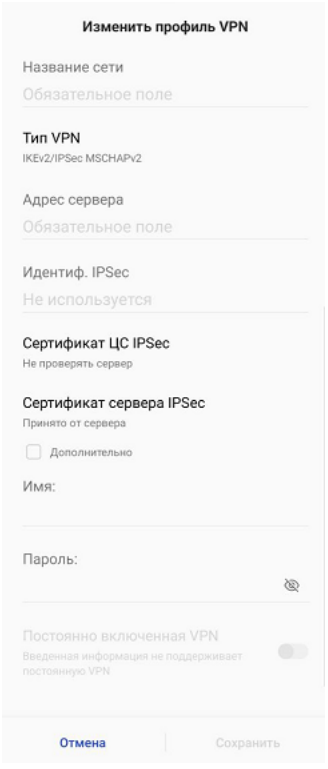
Предупреждение: Не рекомендуем использовать для VPN-подключений кириллические логины.

Подключение 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 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.

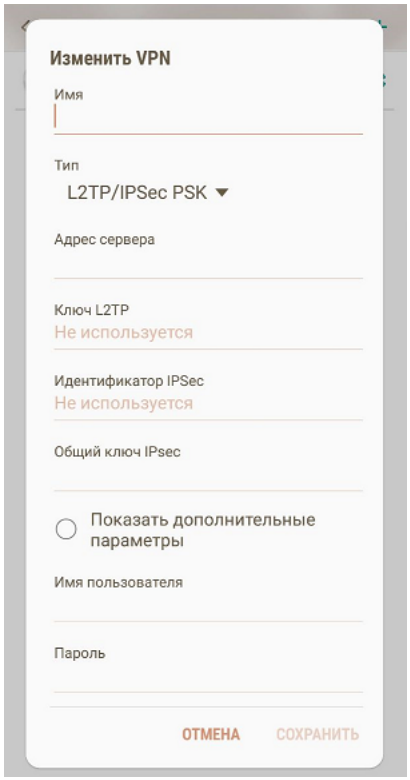
Для PPTP:

Подсказка: Начиная с версии Android 12 была прекращена поддержка протокола PPTP. Для подключения по этим протоколам необходимо использовать сторонние приложения.

- Имя - имя подключения;
- Адрес сервера - адрес VPN-сервера;
- Имя пользователя - имя пользователя, которому разрешено подключение по VPN;
- Пароль - пароль пользователя.

Для L2TP/IPsec PSK:

Подсказка: Начиная с версии Android 12 была прекращена поддержка протокола L2TP. Для подключения по этим протоколам необходимо использовать сторонние приложения.

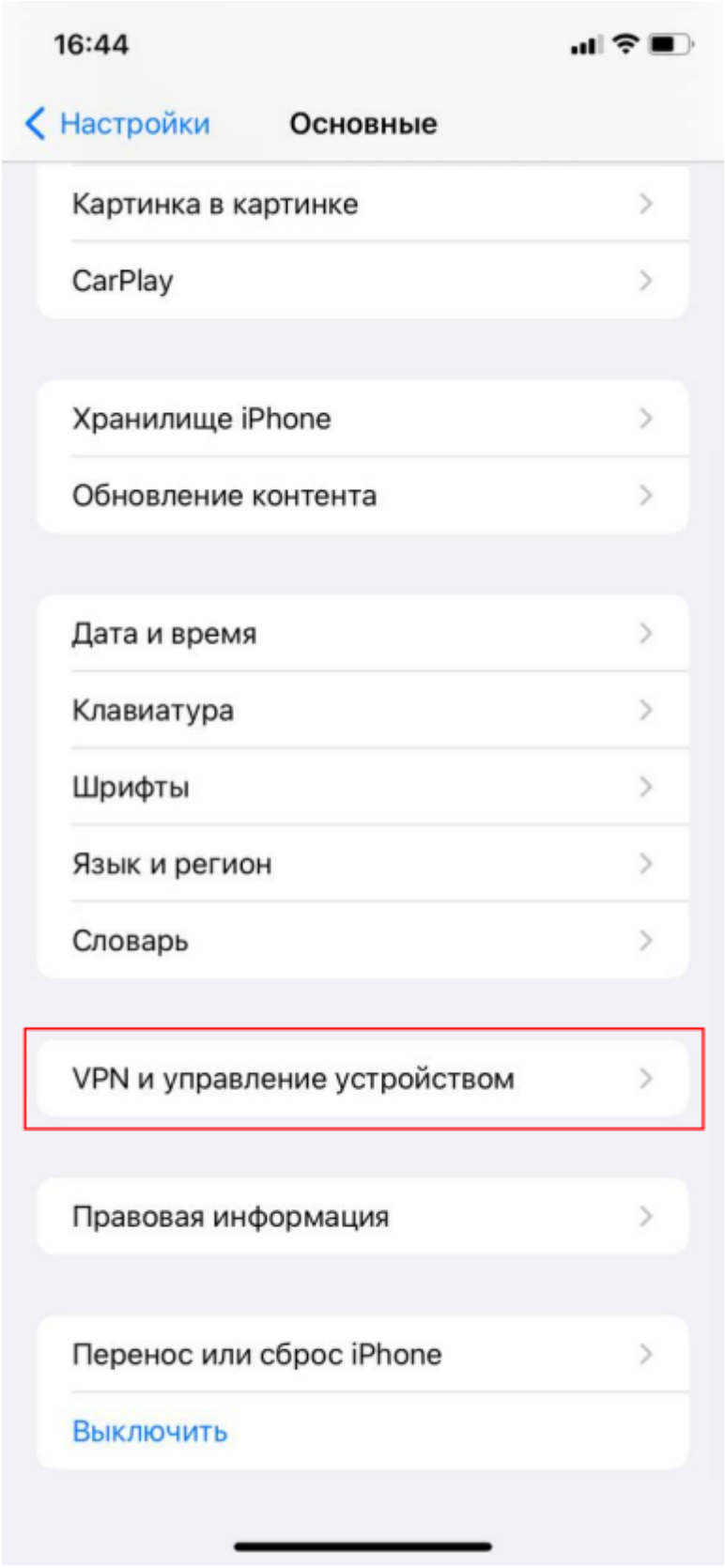


- Имя - имя подключения;
- Адрес сервера - адрес VPN-сервера;
- Общий ключ IPsec - значение строки **PSK** в разделе **Пользователи -> VPN-подключение -> Основное -> Подключение по L2TP/IPsec**.
- **Имя** - имя подключения;
- **Адрес сервера** - адрес VPN-сервера;
- **Общий ключ IPsec** - значение строки **PSK** в разделе **Пользователи -> VPN-подключения -> Основное -> Подключение по L2TP/IPsec**.

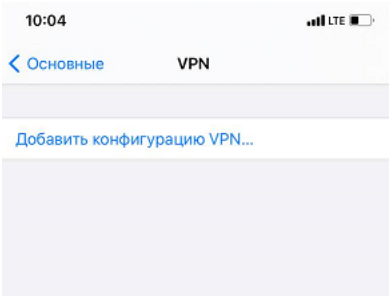
4. Нажмите **Сохранить** и активируйте подключение.

Подключение на iOS (iPhone):

1. Перейдите в раздел **Настройки -> Основные -> VPN и управление устройством -> VPN**:



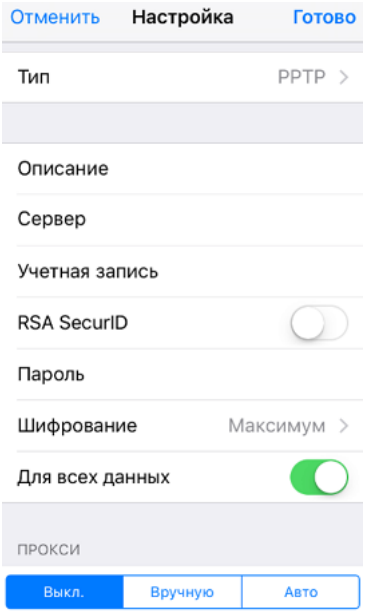
2. Нажмите **Добавить конфигурацию VPN**:



3. Выберите **Тип** подключения и заполните соответствующие поля:

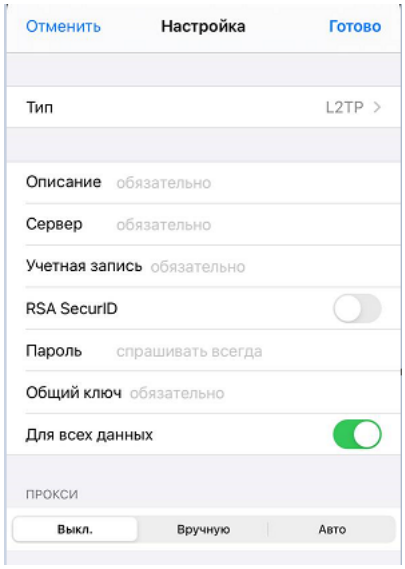
Для PPTP:

Начиная с версии iOS-10 компания Apple убрала поддержку протокола PPTP.



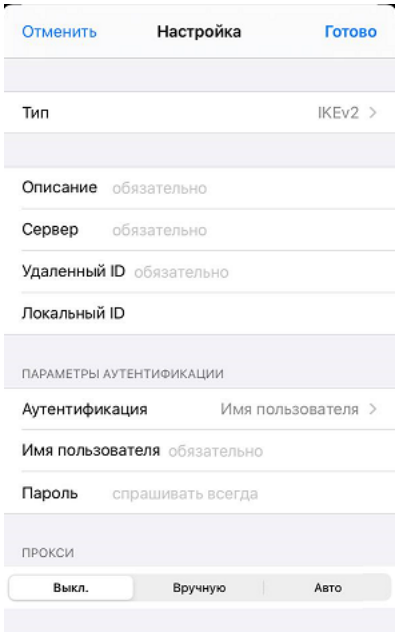
- **Описание** - название соединения;
- **Сервер** - адрес VPN-сервера;
- **Учетная запись** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

Для L2TP:



- **Описание** - название соединения;
- **Сервер** - адрес VPN-сервера;
- **Учетная запись** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя;
- **Общий ключ** - значение строки **PSK** в разделе **Пользователи -> VPN-подключения -> Основное -> Подключение по L2TP/IPsec**.

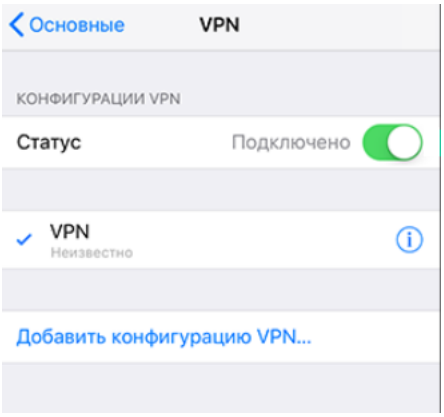
Для IKEv2:



- **Описание** - название соединения;
- **Сервер** - адрес VPN-сервера;
- **Удаленный ID** - адрес VPN-сервера;
- **Имя пользователя** - имя пользователя, которому разрешено подключение по VPN;
- **Пароль** - пароль пользователя.

4. Нажмите **Готово**;

5. Переведите опцию **Статус** вправо:



Подключение через приложение StrongSwan (Android):

Подсказка: Приложение StrongSwan позволяет создавать VPN-подключение только через протокол IKEv2.

---

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.

37.20.7 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.

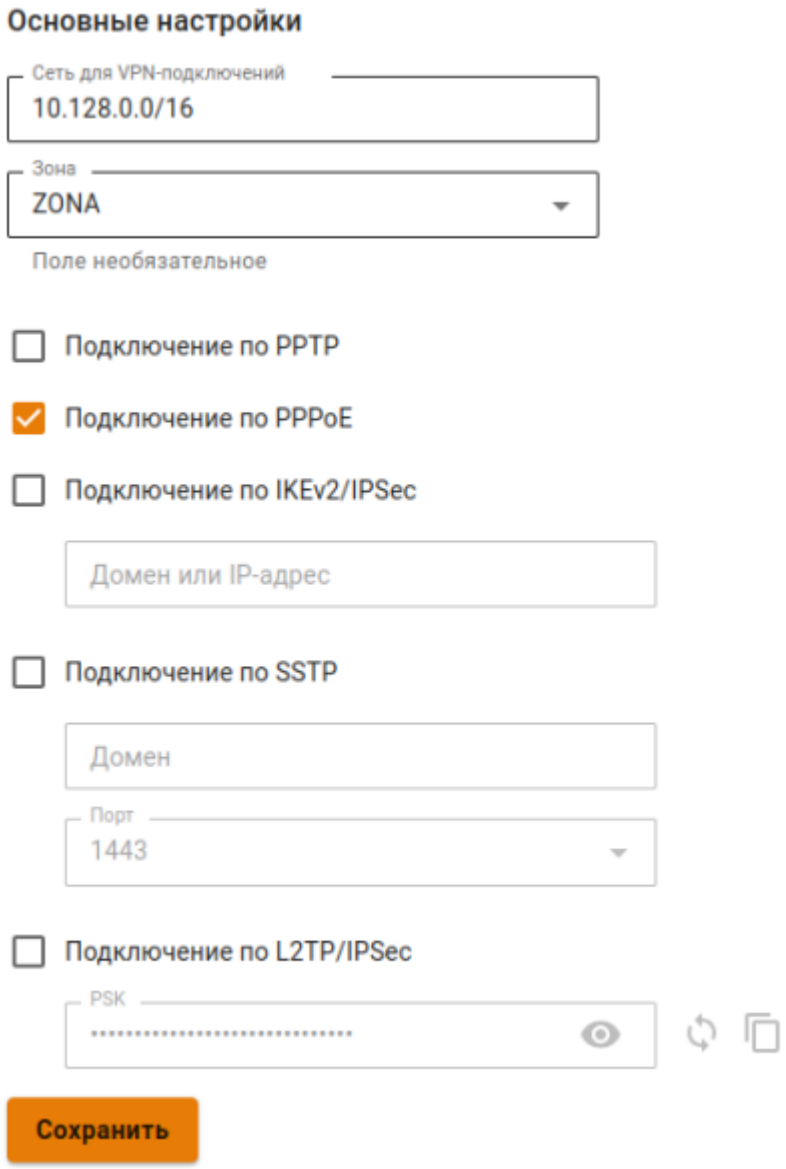
Подсказка: При проблемах с подключением на IOS требуется:

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-подключения -> Основное** и установите флаг **Подключение по PPPoE**:

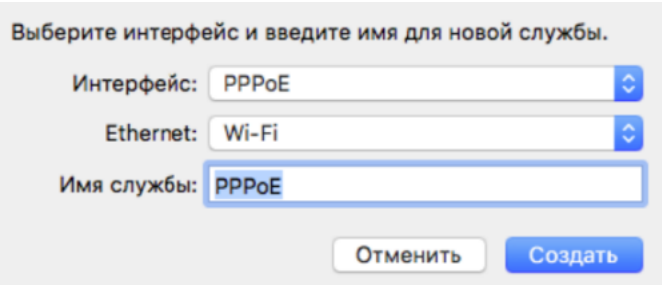


Создание подключения в MacOS

1. Перейдите в раздел **Системные настройки -> Сеть**;

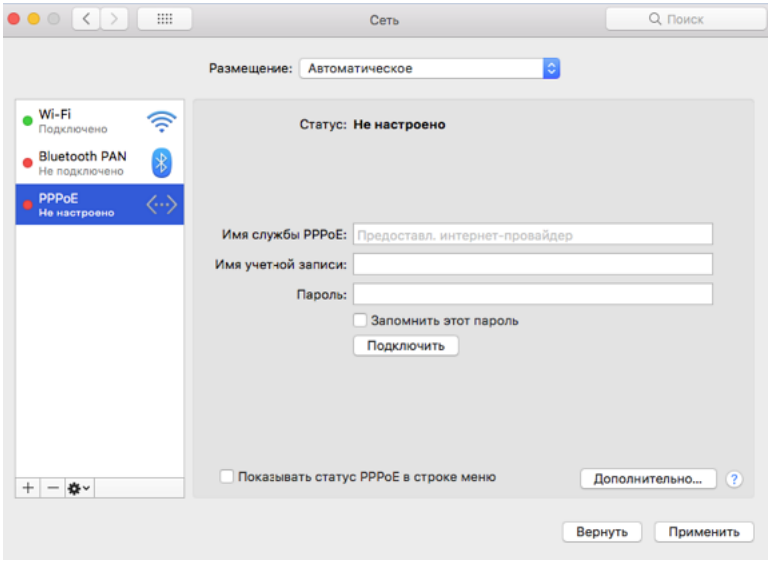
2. Нажмите **Добавить** в левом нижнем углу (иконка +);

3. В появившемся окне заполните поля:



- **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.

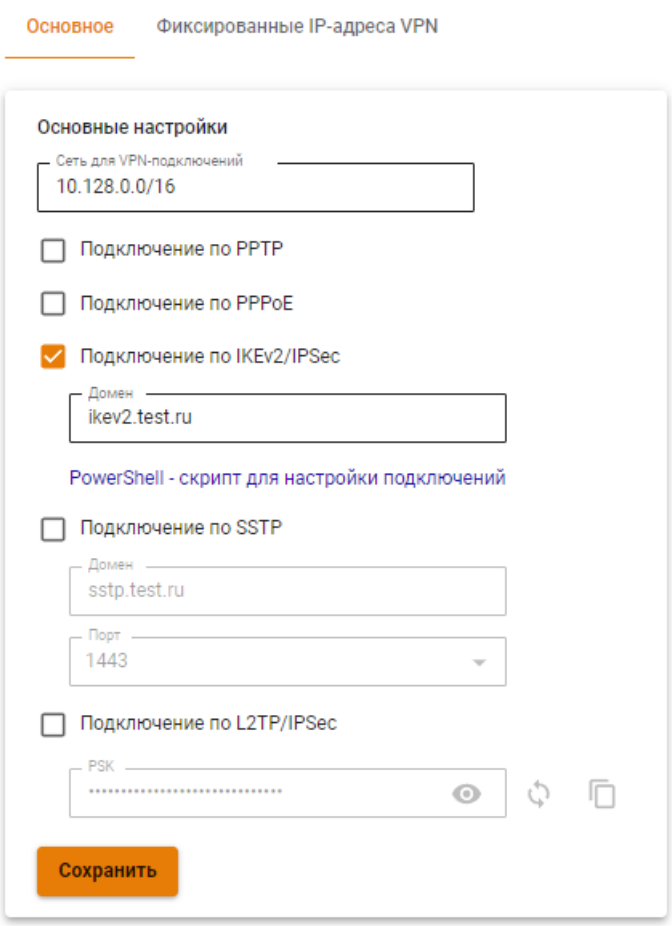
5. Нажмите **Подключить**.

Протокол IKEv2/IPsec:

Настройка Ideco NGFW:

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

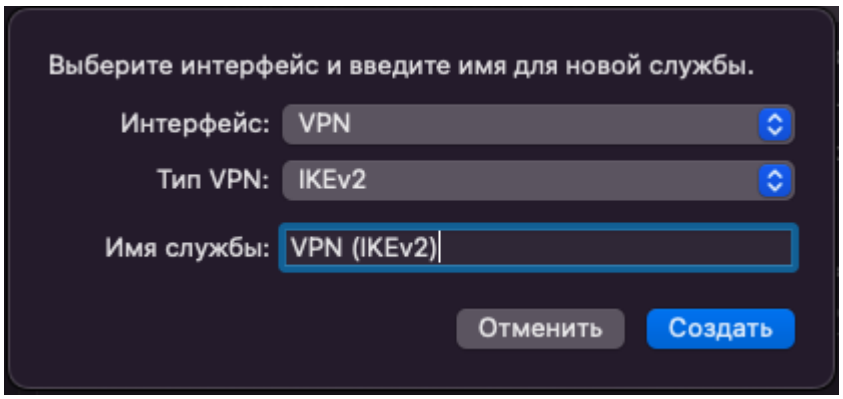
Корневой сертификат потребуется для настройки подключения рабочей станции пользователя, если не был получен корневой сертификат через Let`s Encrypt. При необходимости перенесите файл сертификата на рабочую станцию.
Если для VPN-подключения используется сертификат, выданный Let`s Encrypt, то установка 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 +).

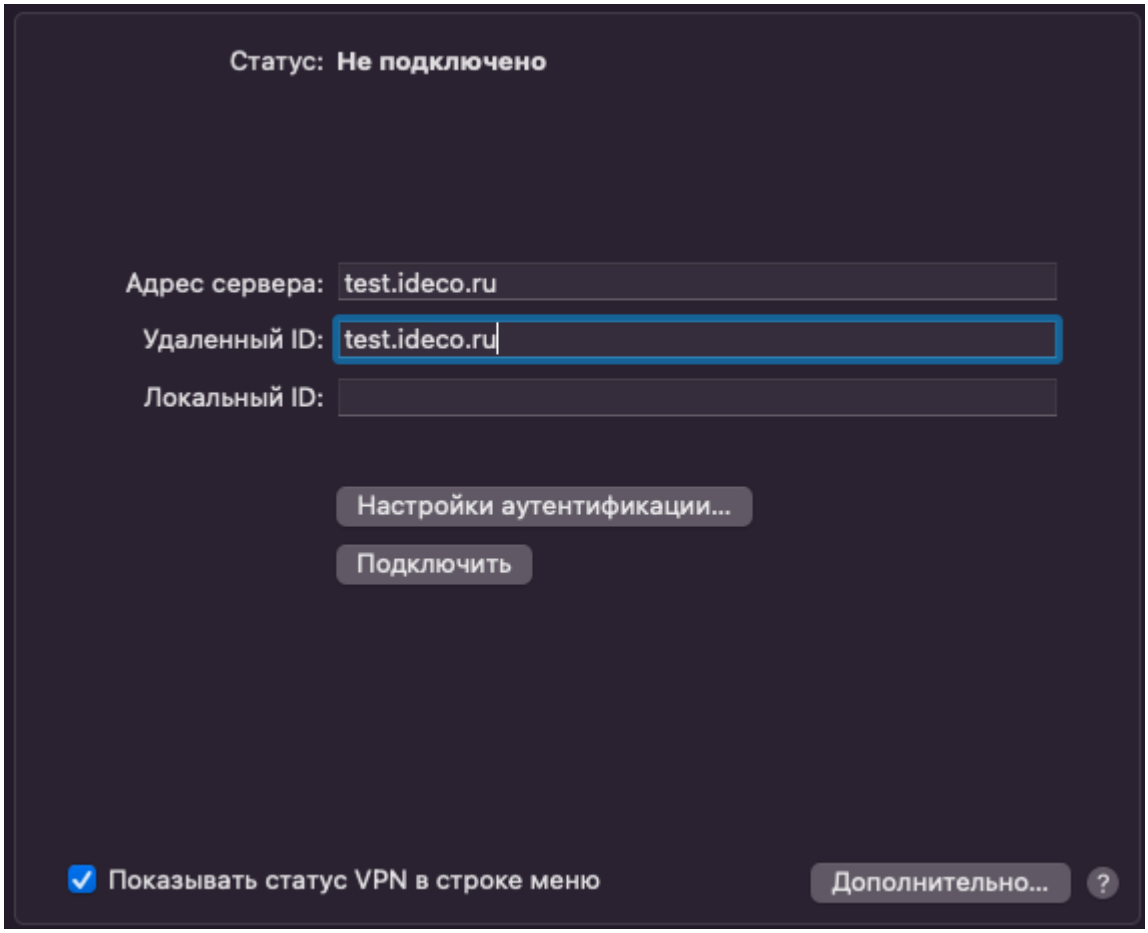
3. Заполните поля:



- **Интерфейс** - VPN;
- **Тип VPN** - IKEv2;
- **Имя службы** - имя подключения.

4. Нажмите **Создать**.

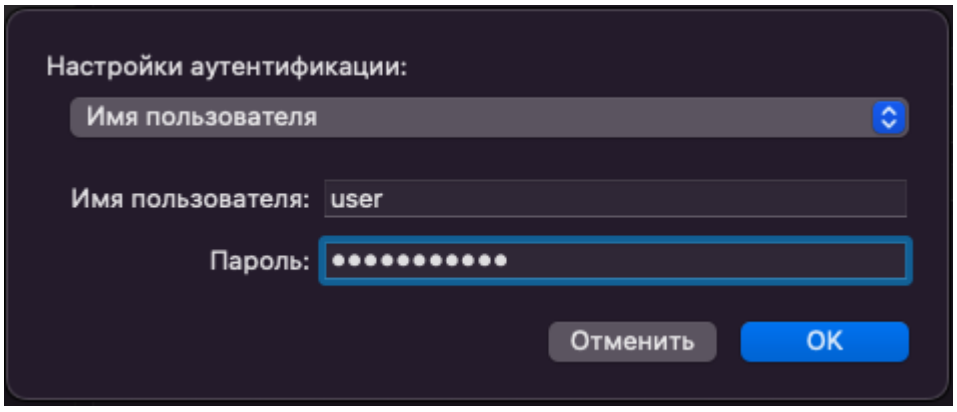
5. Установите параметры подключения:



- **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**.

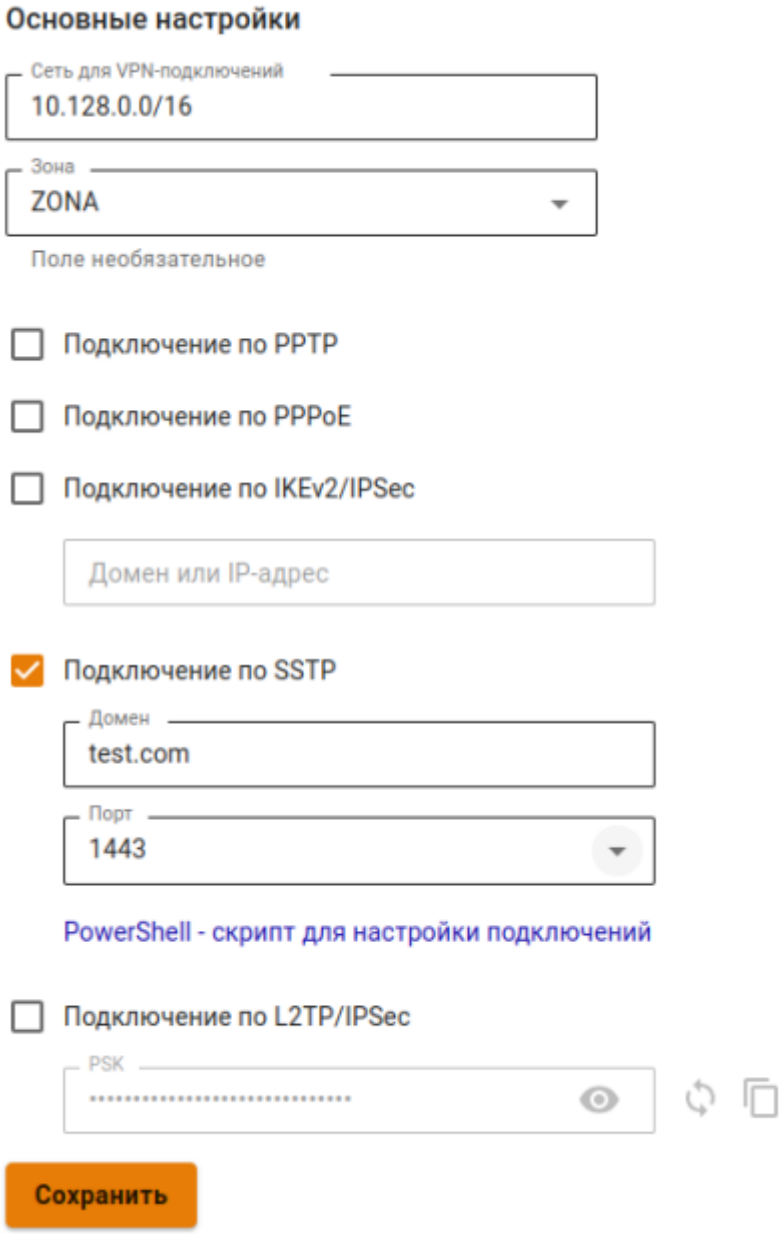
9. Поставьте флаг в пункте **Показывать статус VPN в строке меню**, нажмите **Применить** и включите соединение.

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**.

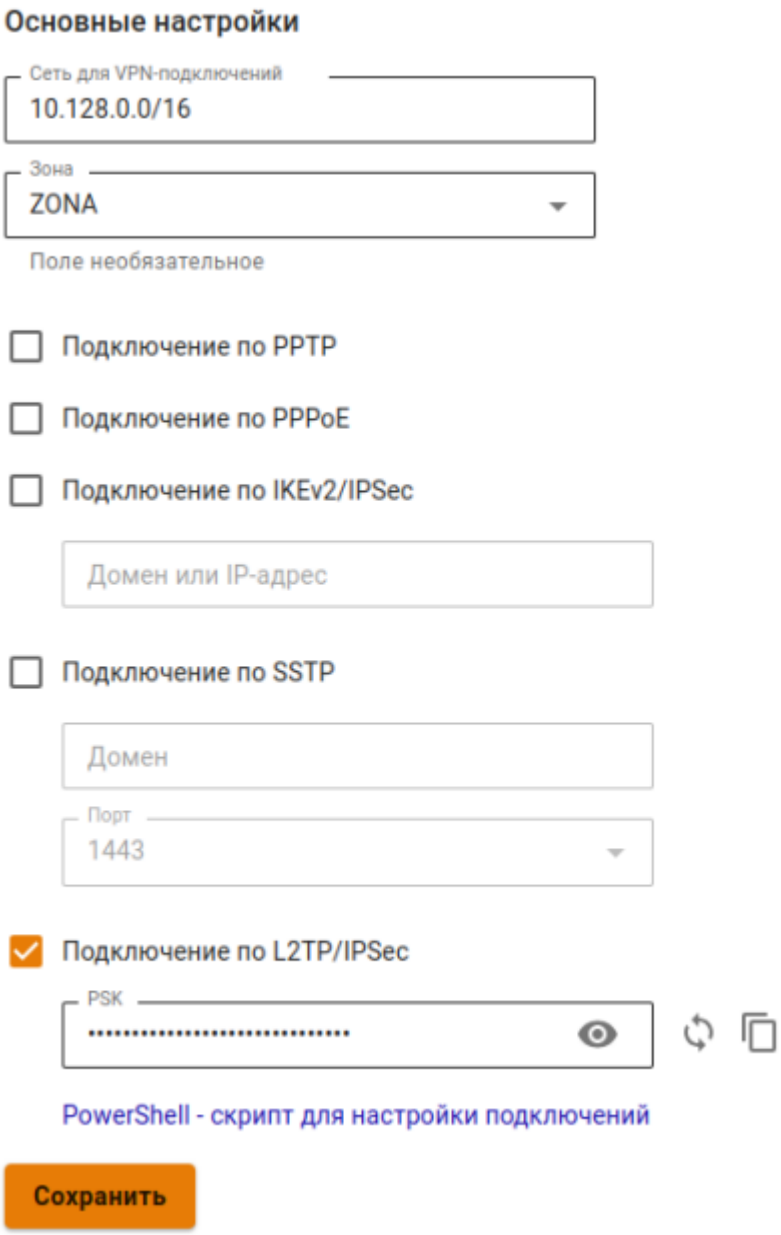
Протокол L2TP/IPsec:

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:

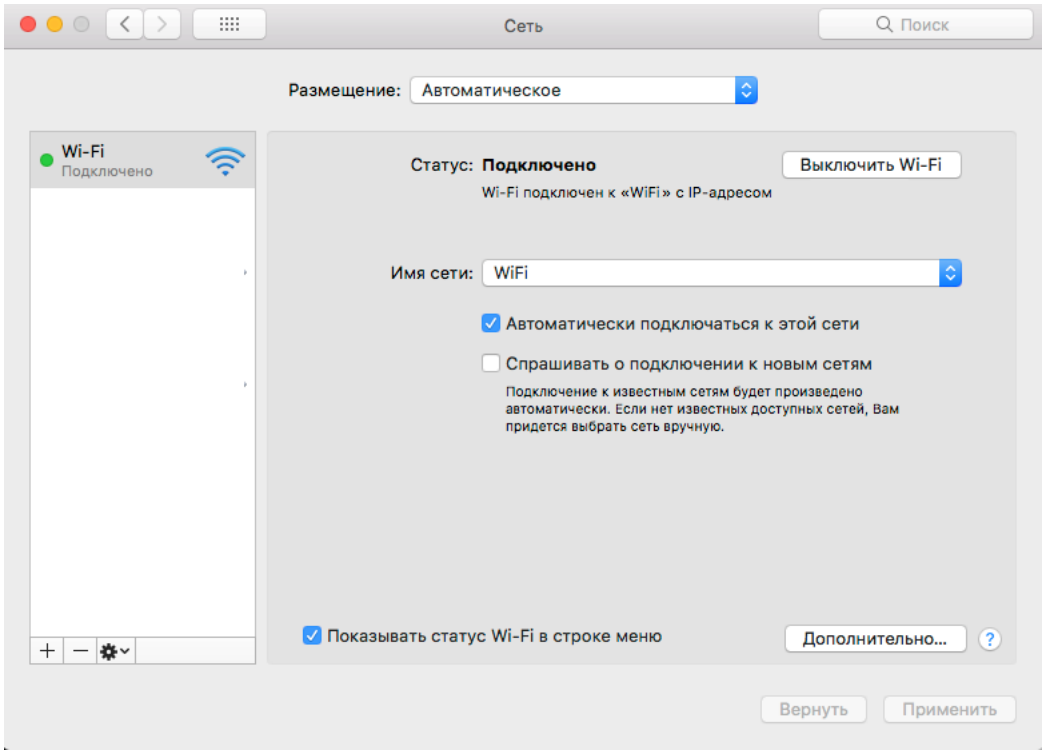
1. Перейдите в раздел **Пользователи -> VPN-подключения -> Основное**.

2. Установите флаг **Подключение по L2TP/IPsec** и скопируйте **PSK**-ключ:



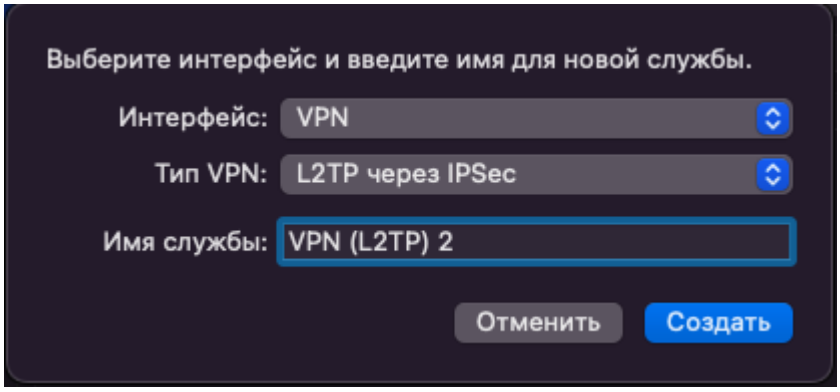
Создание подключения в MacOS:

1. Перейдите в раздел **Системные настройки -> Сеть** и нажмите **Добавить** в левом нижнем углу (иконка +).



2. Нажмите **Добавить** в левом нижнем углу (иконка +);

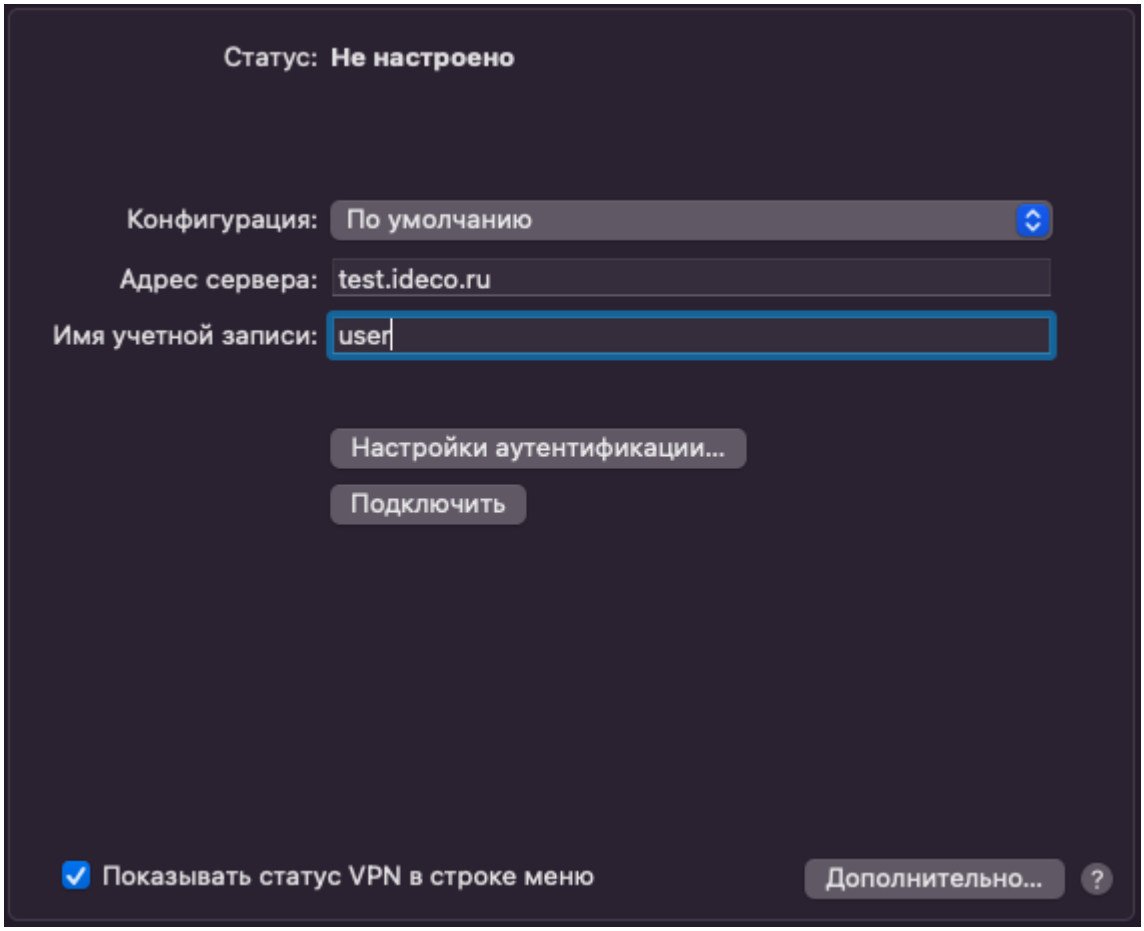
3. Заполните поля:



- **Интерфейс** - VPN;
- **Тип VPN** - L2TP через IPsec;
- **Имя службы** - имя подключения.

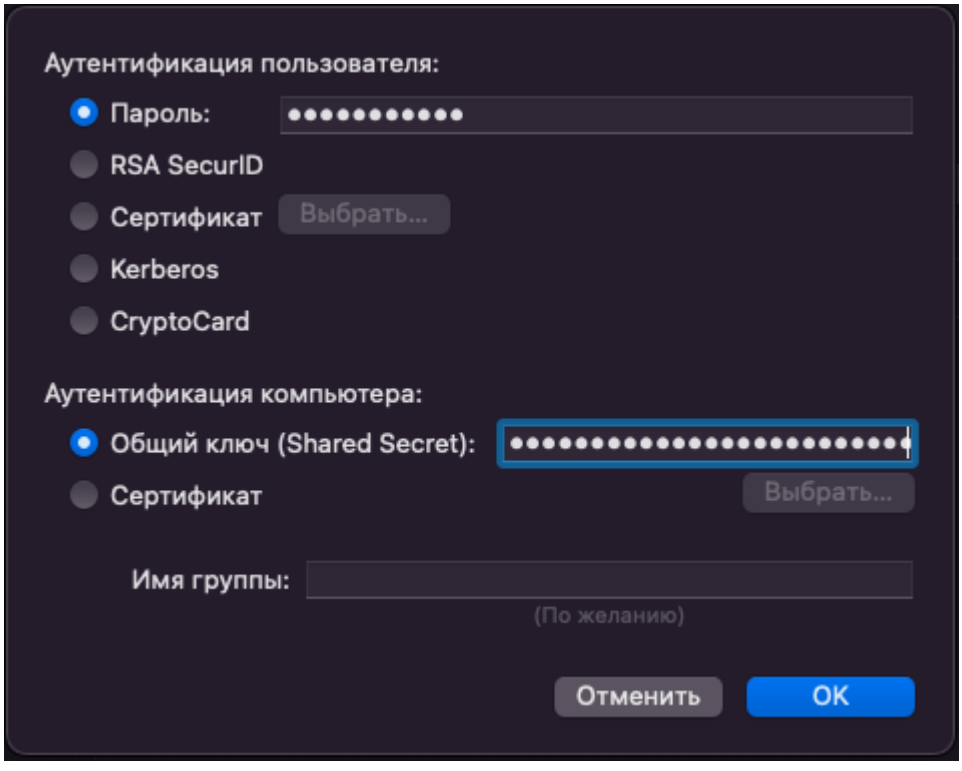
4. Нажмите **Создать**.

5. Заполните **Адрес сервера** и **Имя учетной записи**:



6. Поставьте флаг на пункте **Показывать статус VPN в строке меню** и выберите **Настройки аутентификации**.

7. В **Аутентификации пользователя** заполните **Пароль**, в **Аутентификации компьютера** - **Общий ключ (Shared Secret)**:



8. Нажмите **ОК -> Применить** и включите соединение.

37.20.8 Подключение по SSTP Wi-Fi роутеров Keenetic

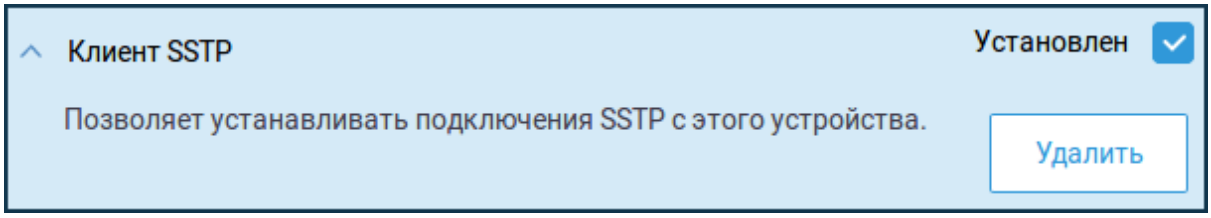
Основное

Поддерживаются все роутеры на базе KeeneticOS 3.x.x.

1. Выполните настройку пользователей в Ideco NGFW и включите SSTP в разделе **Пользователи -> VPN-подключения -> Основное**.

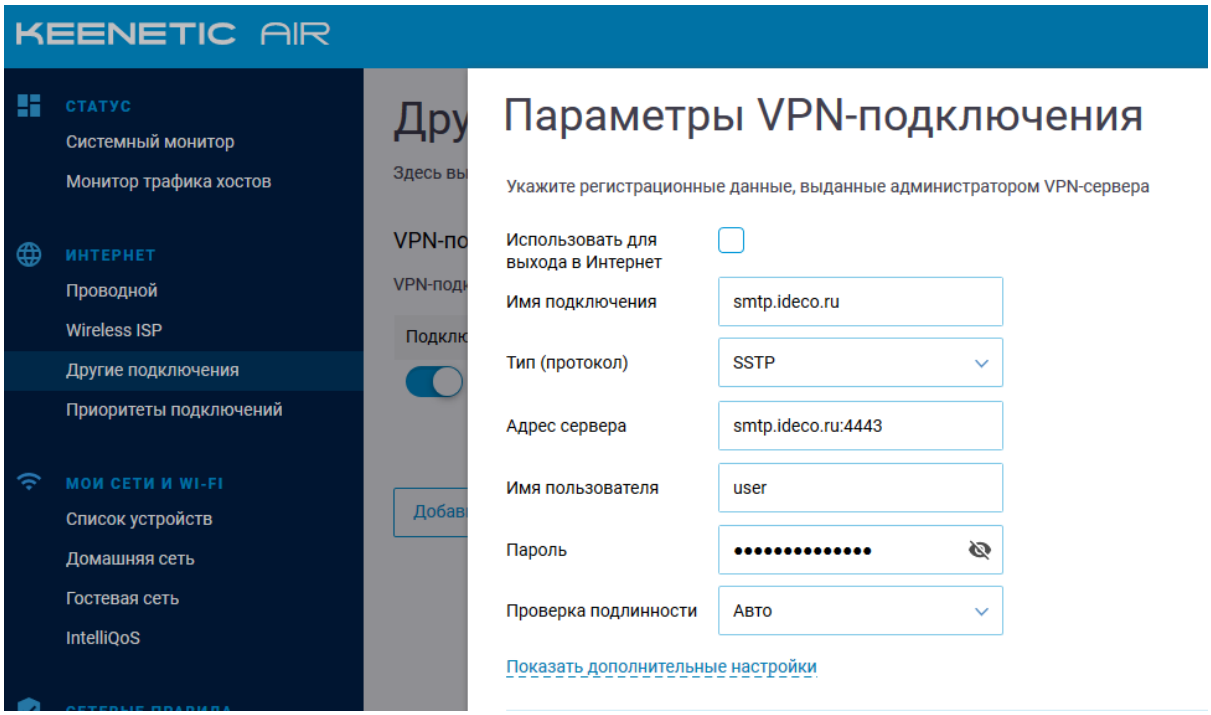
2. Зайдите в веб-интерфейс управления Keenetic: `http://my.keenetic.net`.

3. Установите компонент системы **Клиент SSTP** на странице **Общие настройки** в разделе **Обновления и компоненты**, нажмите **Изменить набор компонентов**.



Подробнее о настройках в документации Keenetic.

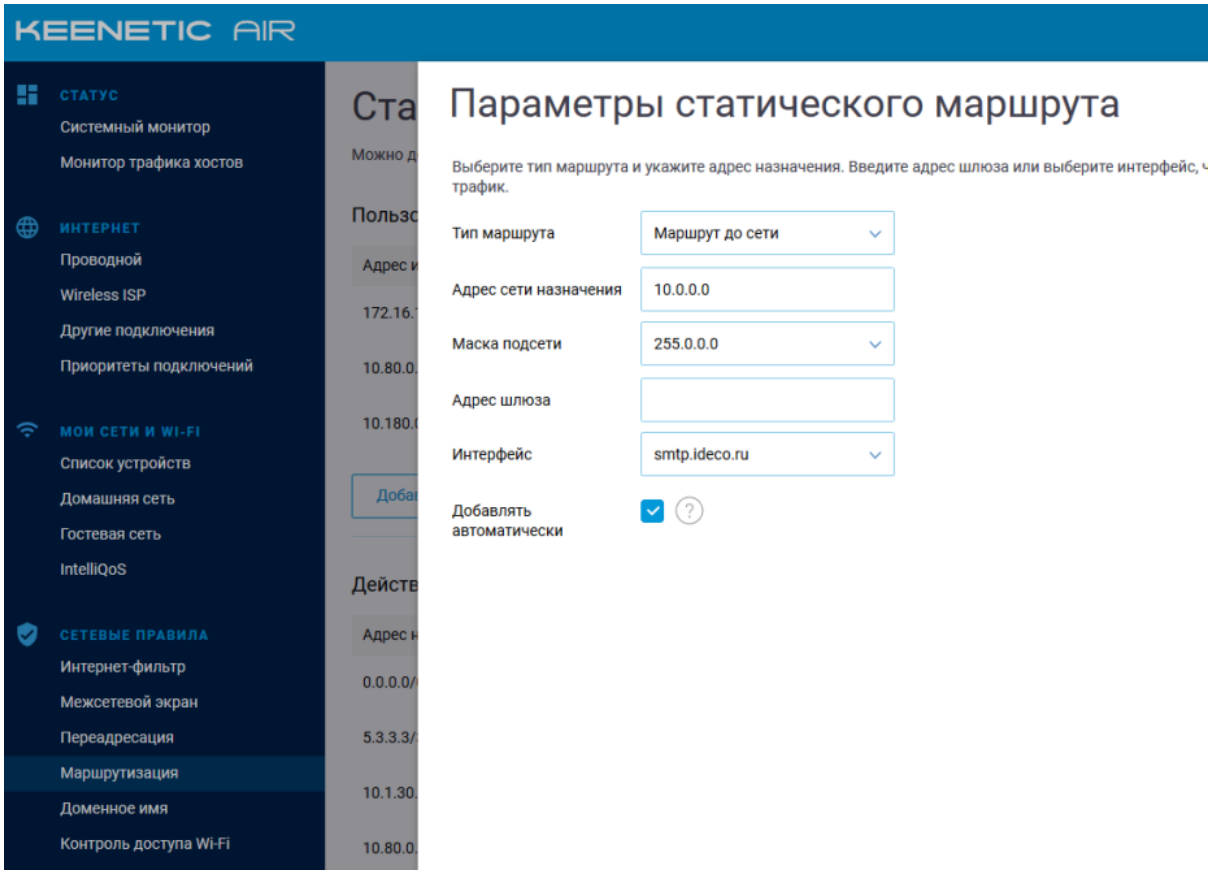
4. Создайте подключение в разделе **Интернет -> Другие подключения** нажмите кнопку **Добавить подключение**



Не устанавливайте флаг **Использовать для выхода в интернет**.

Введите имя подключения, протокол SSTP, адрес сервера (**обязательно укажите в адресе порт через двоеточие**), имя пользователя и пароль.

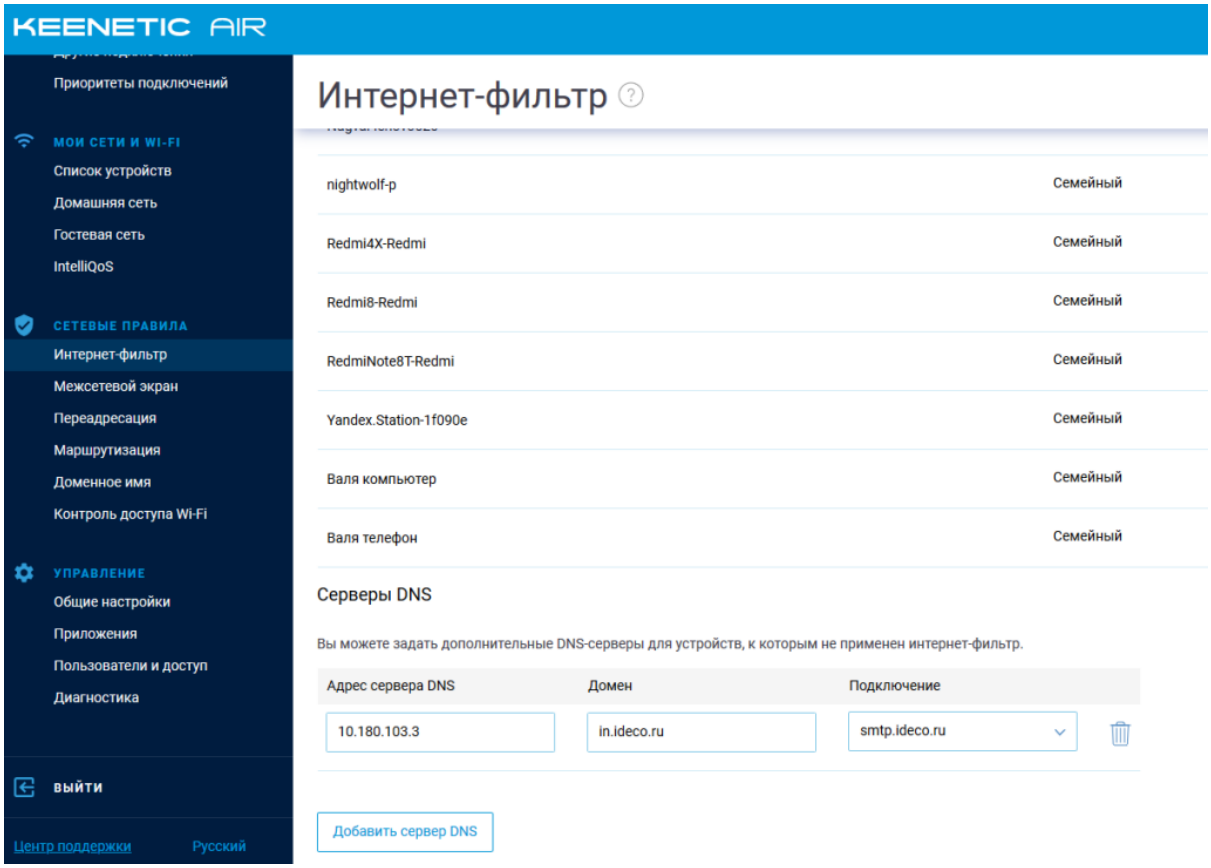
5. В разделе **Сетевые правила -> Маршруты** добавьте маршруты в рабочую сеть. Например, если сеть офиса `10.0.0.0/8`, добавьте следующий маршрут:



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.

37.21 Подключение к сертифицированным Ideco EX и настройка Ideco NGFW

37.21.1 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.

37.21.2 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.

37.22 Анализ трафика

Для анализа трафика на компьютерах или NGFW используйте утилиту `tcpdump`. На Ideco NGFW утилита используется в разделе **Управление сервером -> Терминал**.

Подсказка: Утилита `tcpdump` предустановлена в продукт Ideco NGFW.

37.22.1 Описание использования утилиты и ключи tcpdump

Подсказка: Для работы `tcpdump` требует прав суперпользователя.

При запуске `tcpdump` без каких-либо ключей/параметров произойдет перехват всех пакетов через интерфейс по умолчанию.

Для просмотра всех ключей утилиты введите `tcpdump -h`.

Для более гибкого использования утилиты используйте комбинацию ключей.

Например:

Для вывода и разбора только 5 захваченных пакетов с интерфейса `eth1` введите:

```
tcpdump -i eth1 -c 5
```

Использование tcpdump с применением ключей

Просмотр списка сетевых интерфейсов:

Для просмотра введите в терминале:

```
tcpdump -D
```

Пример вывода утилиты:

```
1.eth0
2.nflog (Linux netfilter log (NFLOG) interface)
3.nfqueue (Linux netfilter queue (NFQUEUE) interface)
4.eth1
5.any (Pseudo-device that captures on all interfaces)
6.lo [Loopback]
```

Захват пакетов, проходящих через определенный интерфейс:

Для захвата пакетов с интерфейса `eth1` введите:

```
tcpdump -i eth1
```

Пример вывода утилиты:

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
01:06:09.278817 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761,␣
↪seq 1, length 64
01:06:09.279374 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 4761,␣
↪seq 1, length 64
01:06:10.281142 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 4761,␣
↪seq 2, length 6
```

Полезная информация:

- Ключ `-v` увеличивает количество отображаемой информации о пакетах (добавляется протокол, флаги пакета)
- Ключ `-vv` дает еще более подробную информацию (полный разбора пакета и вывод в терминал).

Пример использования с ключами:

```
tcpdump -i eth1 -v
```

```
tcpdump -i eth1 -vv
```

Вывод и захват только определенного числа пакетов:

Для захвата и разбора 5 пакетов с интерфейса по-умолчанию введите:

```
tcpdump -c 5
```

Пример вывода утилиты:

```
04:19:07.675216 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq␣
↪2186733178:2186733278, ack 204106815, win 37232, length 100
04:19:07.675497 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 100, win 65535,␣
↪length 0
04:19:07.675747 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 100:136, ack 1, win␣
↪37232, length 36
04:19:07.675902 IP 10.0.2.2.50422 > 10.0.2.15.22: Flags [.], ack 136, win 65535,␣
↪length 0
04:19:07.676142 IP 10.0.2.15.22 > 10.0.2.2.50422: Flags [P.], seq 136:236, ack 1, win␣
↪37232, length 100
5 packets captured
```

Использование tcpdump с применением фильтров

Список часто используемых фильтров `tcpdump`:

- `port` - фильтрация пакетов по номеру порта;
- `host` - фильтрация исходящих и входящих пакетов по IP-адресу;
- `src` - фильтрация пакетов по IP-адресу источника;
- `dst` - фильтрация пакетов по IP-адресу назначения.

Для фильтрации по определенному протоколу укажите его в качестве фильтра:

- `tcp` - фильтрация пакетов с протоколом TCP;

- `udp` - фильтрация пакетов с протоколом `UDP`;
- `icmp` - фильтрация пакетов с протоколом `ICMP`;
- `arp` - фильтрация пакетов с протоколом `ARP`.

Для комбинирования фильтров используйте логические операторы:

- `and` - пакет выведется при совпадении условий у всех указанных фильтров;
- `or` - пакет выведется при совпадении условий у одного указанного фильтра;
- `not` - инвертирует условие фильтра.

Фильтрация пакетов по 80 порту:

Для фильтрации введите:

```
tcpdump port 80
```

Пример вывода утилиты:

```
23:54:24.978612 IP 10.0.0.1.53971 > 10.0.0.50.80: Flags [SEW], seq 53967733, win␣
↪65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 256360128 ecr 0,sackOK,eol],␣
↪length 0
23:54:24.978650 IP 10.0.0.50.80 > 10.0.0.1.53971: Flags [S.E], seq 996967790, ack␣
↪53967734, win 28960, options [mss 1460,sackOK,TS val 5625522 ecr 256360128,nop,
↪wscale 6], length 0
23:54:24.978699 IP 10.0.0.1.53972 > 10.0.0.50.80: Flags [SEW], seq 226341105, win␣
↪65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 256360128 ecr 0,sackOK,eol],␣
↪length 0
23:54:24.978711 IP 10.0.0.50.80 > 10.0.0.1.53972: Flags [S.E], seq 1363851389, ack␣
↪226341106, win 28960, options [mss 1460,sackOK,TS val 5625522 ecr 256360128,nop,
↪wscale 6], length 0
```

Фильтрация пакетов по хосту с IP-адресом 10.0.2.15:

Для фильтрации введите:

```
tcpdump host 10.0.2.15
```

Пример вывода утилиты:

```
03:48:06.087509 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq␣
↪3862934963:3862934999, ack 65355639, win 37232, length 36
03:48:06.087806 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 36, win 65535,␣
↪length 0
03:48:06.088087 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 36:72, ack 1, win␣
↪37232, length 36
03:48:06.088274 IP 10.0.2.2.50225 > 10.0.2.15.22: Flags [.], ack 72, win 65535,␣
↪length 0
03:48:06.088440 IP 10.0.2.15.22 > 10.0.2.2.50225: Flags [P.], seq 72:108, ack 1, win␣
↪37232, length 36
```

Фильтрация пакетов по IP-адресу назначения 8.8.8.8:

Для фильтрации введите:

```
tcpdump dst 8.8.8.8
```

Пример вывода утилиты:

```
17:32:19.642154 IP desktop > dns.google: ICMP echo request, id 1, seq 1, length 64
17:32:20.644231 IP desktop > dns.google: ICMP echo request, id 1, seq 2, length 64
17:32:21.645715 IP desktop > dns.google: ICMP echo request, id 1, seq 3, length 64
17:32:22.647387 IP desktop > dns.google: ICMP echo request, id 1, seq 4, length 64
17:32:23.648814 IP desktop > dns.google: ICMP echo request, id 1, seq 5, length 64
```

Фильтрация пакетов по протоколу ICMP:

Для фильтрации введите:

```
tcpdump icmp
```

Пример вывода утилиты:

```
04:03:47.408545 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812,␣
↪seq 75, length 64
04:03:47.408999 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812,␣
↪seq 75, length 64
04:03:48.408697 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812,␣
↪seq 76, length 64
04:03:48.409208 IP 10.0.0.51 > vagrant-ubuntu-trusty-64: ICMP echo reply, id 2812,␣
↪seq 76, length 64
04:03:49.411287 IP vagrant-ubuntu-trusty-64 > 10.0.0.51: ICMP echo request, id 2812,␣
↪seq 77, length 64
```

Фильтрация пакетов с интерфеса eth1 с IP-адресом источника 10.0.0.1 и 80 портом назначения:

Для фильтрации введите:

```
tcpdump -i eth1 src 10.0.0.1 and dst port 80
```

Пример вывода утилиты:

```
00:18:17.155066 IP 10.0.0.1.54222 > 10.0.0.50.80: Flags [F.], seq 500773341, ack␣
↪2116767648, win 4117, options [nop,nop,TS val 257786173 ecr 5979014], length 0
00:18:17.155104 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [S], seq 904045691, win 65535,
↪ options [mss 1460,nop,wscale 5,nop,nop,TS val 257786173 ecr 0,sackOK,eol], length 0
00:18:17.157337 IP 10.0.0.1.54221 > 10.0.0.50.80: Flags [P.], seq␣
↪4282813257:4282813756, ack 1348066220, win 4111, options [nop,nop,TS val 257786174␣
↪ecr 5979015], length 499: HTTP: GET / HTTP/1.1
00:18:17.157366 IP 10.0.0.1.54225 > 10.0.0.50.80: Flags [.], ack 1306947508, win 4117,
↪ options [nop,nop,TS val 257786174 ecr 5983566], length 0
```

Фильтрация пакетов по всем доступным протоколам, кроме ICMP:

Для фильтрации введите:

```
tcpdump not icmp
```

Пример вывода утилиты:

```
17:45:34.847882 IP desktop.48552 > 149.154.167.41.https: Flags [P.], seq␣
↪3991504547:3991504748, ack 499514727, win 248, options [nop,nop,TS val 1585771305␣
↪ecr 4205201964], length 201
17:45:34.918383 IP 149.154.167.41.https > desktop.48552: Flags [.], ack 201, win 7509,
↪ options [nop,nop,TS val 4205203056 ecr 1585771305], length 0
17:45:34.919444 IP 149.154.167.41.https > desktop.48552: Flags [.], seq 1:1229, ack␣
↪201, win 7509, options [nop,nop,TS val 4205203056 ecr 1585771305], length 1228
17:45:34.919475 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 1229, win 239,
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪ options [nop,nop,TS val 1585771377 ecr 4205203056], length 0
17:45:34.919778 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 1229:2457,␣
↪ack 201, win 7509, options [nop,nop,TS val 4205203056 ecr 1585771305], length 1228
17:45:34.919804 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2457, win 239,
↪ options [nop,nop,TS val 1585771377 ecr 4205203056], length 0
17:45:34.923322 IP 149.154.167.41.https > desktop.48552: Flags [P.], seq 2457:2845,␣
↪ack 201, win 7509, options [nop,nop,TS val 4205203061 ecr 1585771305], length 388
17:45:34.923351 IP desktop.48552 > 149.154.167.41.https: Flags [.], ack 2845, win 239,
↪ options [nop,nop,TS val 1585771381 ecr 4205203061], length 0
17:45:35.644804 IP desktop.49669 > _gateway.domain: 65295+ PTR? 41.167.154.149.in-
↪addr.arpa. (45)
```

Сохранение дампа захваченных пакетов в файл в формате .pcap:

Для сохранения дампа в файл `out.pcap` введите:

```
tcpdump -w out.pcap
```

Подсказка: Для анализа захваченных пакетов в формате `.pcap` используйте Wireshark.

Примеры использования с Ideco NGFW

Проверка работы IPsec-туннелей:

Позволяет понять причину неработоспособности IPsec-туннеля.

1. Для проверки прохождения трафика на всех интерфейсах головного офиса по порту 4500 введите:

```
tcpdump -i any port 4500 -ttttnnn
```

2. Для проверки прохождения трафика на всех интерфейсах филиала по порту 500 введите:

```
tcpdump -i any port 500 -tttnnn
```

37.23 Режим удаленного помощника

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

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

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

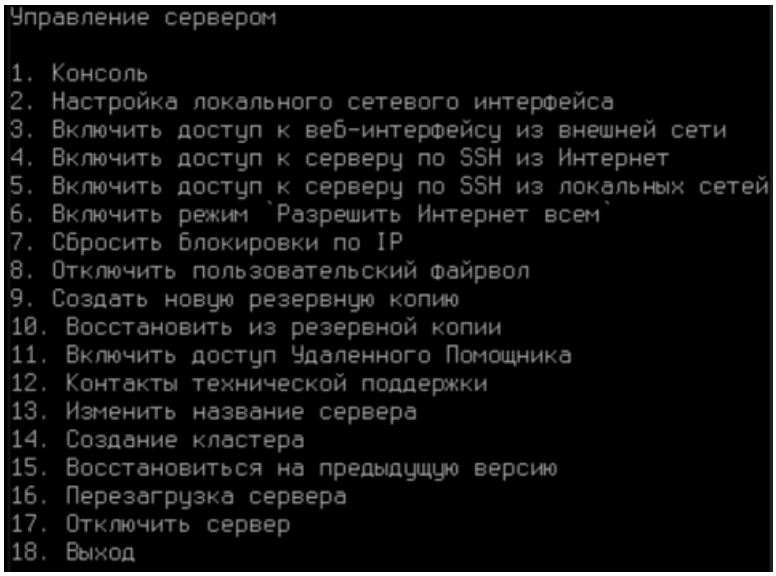
37.23.1 Включение режима удаленного помощника из веб-интерфейса

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

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

37.23.2 Включение режима удаленного помощника из локального меню сервера

Чтобы включить режим удаленного помощника, в локальном меню Ideco NGFW выберите пункт **Включить доступ Удаленного помощника**, введя пункт **13**, затем нажмите **Enter**.
Сгенерируется пароль, который необходимо сообщить технической поддержке для подключения по SSH.



37.23.3 Работа с сервером по протоколу SSH в режиме удаленного помощника

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

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

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

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

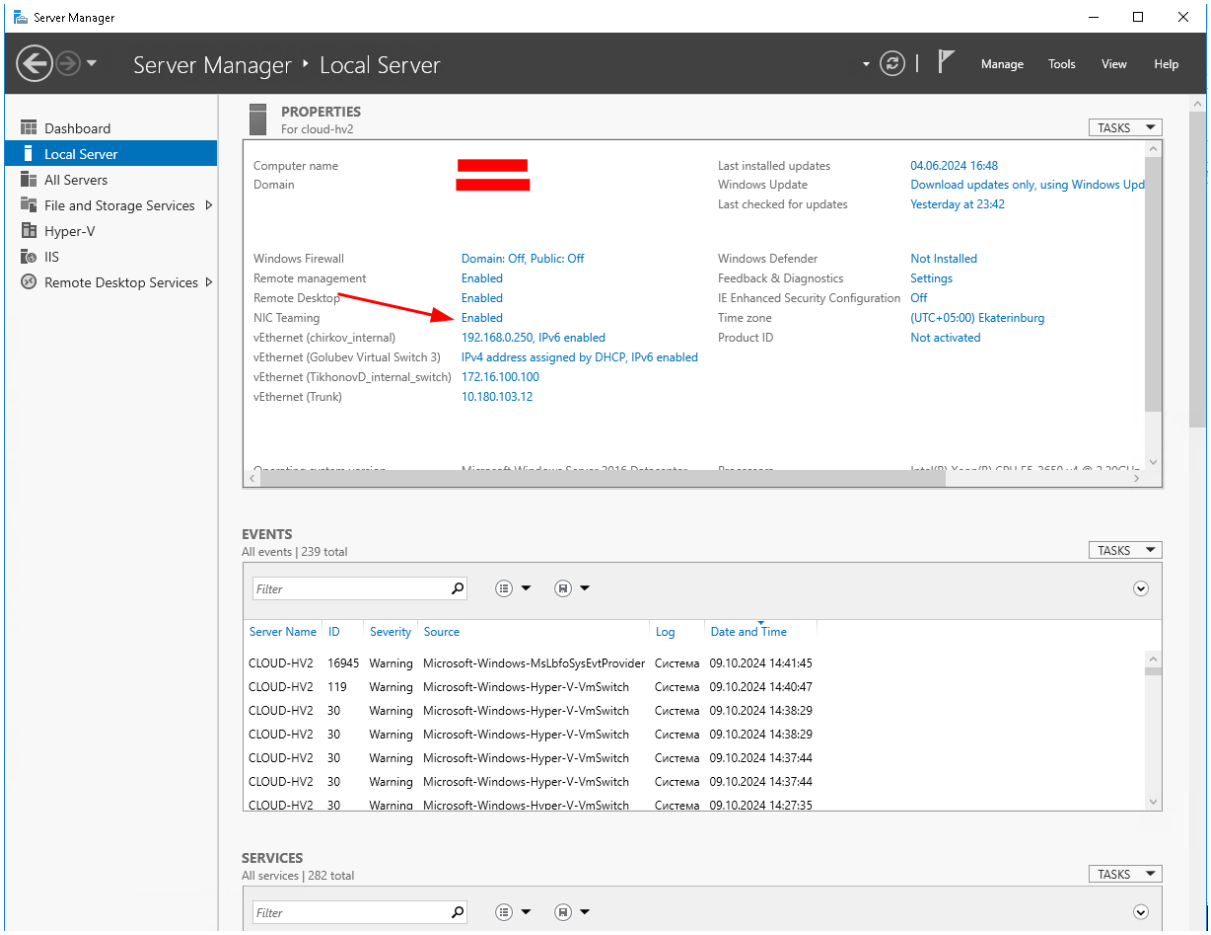
Символ «#» свидетельствует, что работа ведется от имени суперпользователя.

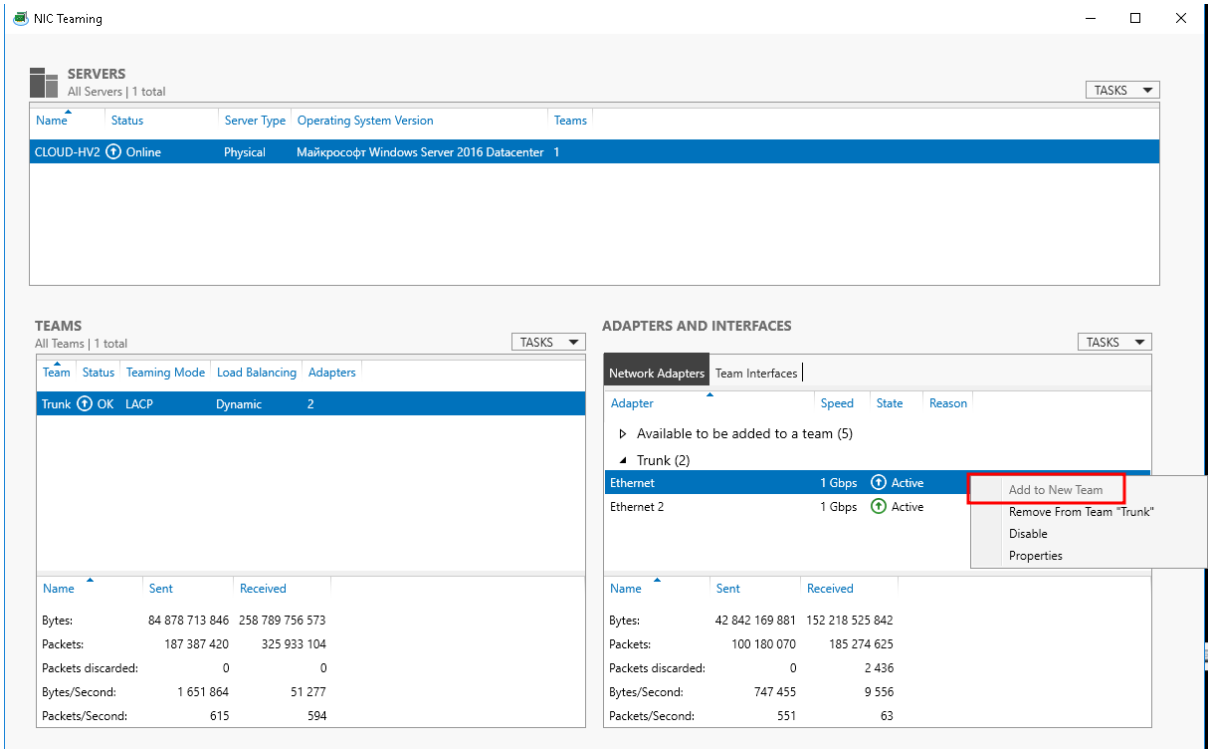
37.24 Настройка LACP на Hyper-V

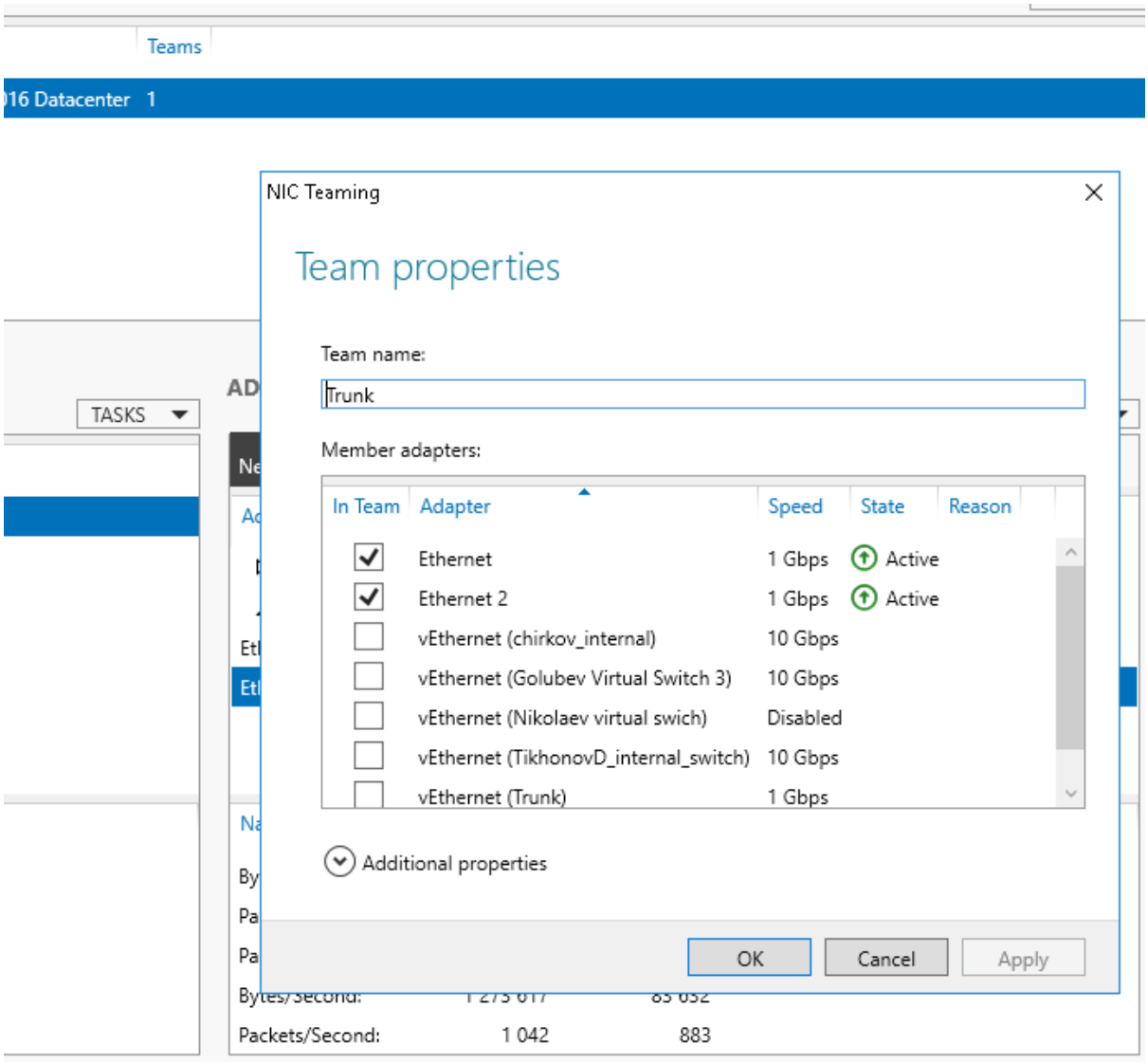
Для настройки LACP на гипервизоре Hyper-V существуют два способа:

37.24.1 Настройка на хост системе

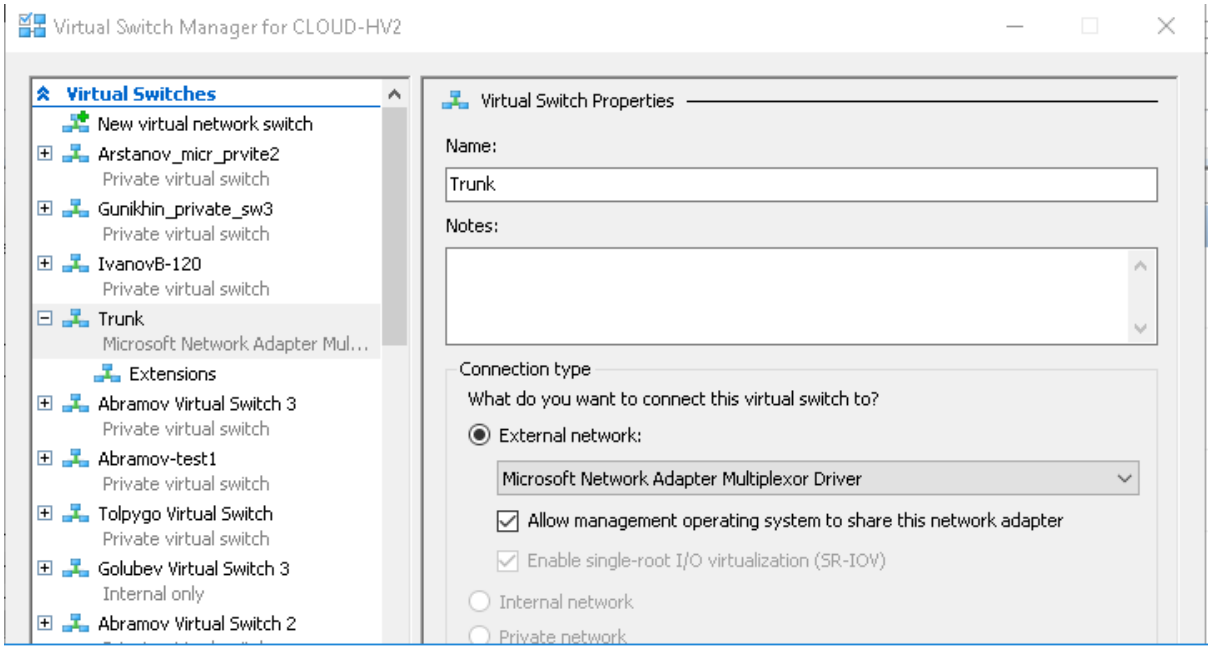
1. Объедините физические интерфейсы:

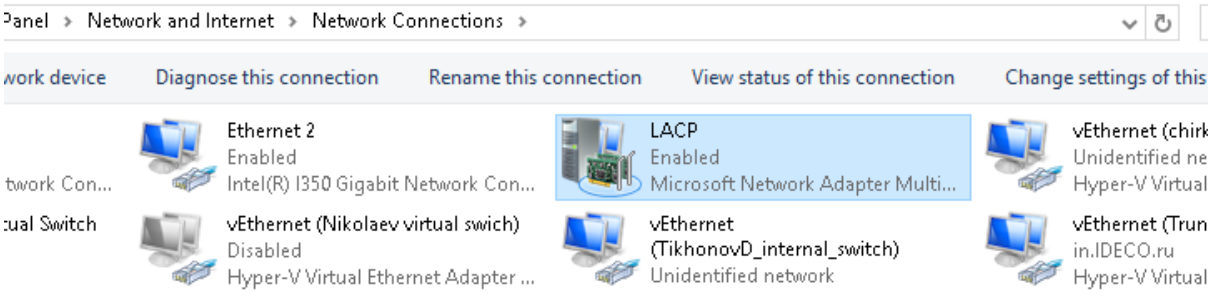



NIC Teaming
SERVERS
All Servers | 1 total
TASKS
Name
Status
Server Type
Operating System Version
Teams
CLOUD-HV2
Online
Physical
Майкрософт Windows Server 2016 Datacenter
1
TEAMS
All Teams | 1 total
TASKS
Team
Status
Teaming Mode
Load Balancing
Adapters
Trunk
OK
LACP
Dynamic
2
Name
Sent
Received
Bytes:
84 878 713 846
258 789 756 573
Packets:
187 387 420
325 933 104
Packets discarded:
0
0
Bytes/Second:
1 651 864
51 277
Packets/Second:
615
594
ADAPTERS AND INTERFACES
TASKS
Network Adapters
Team Interfaces
Adapter
Speed
State
Reason
Available to be added to a team (5)
Trunk (2)
Ethernet
1 Gbps
Active
Ethernet 2
1 Gbps
Active
Add to New Team
Remove From Team "Trunk"
Disable
Properties
Name
Sent
Received
Bytes:
42 842 169 881
152 218 525 842
Packets:
100 180 070
185 274 625
Packets discarded:
0
2 436
Bytes/Second:
747 455
9 556
Packets/Second:
551
63



2. Выберите созданный интерфейс при настройке виртуального свитча:



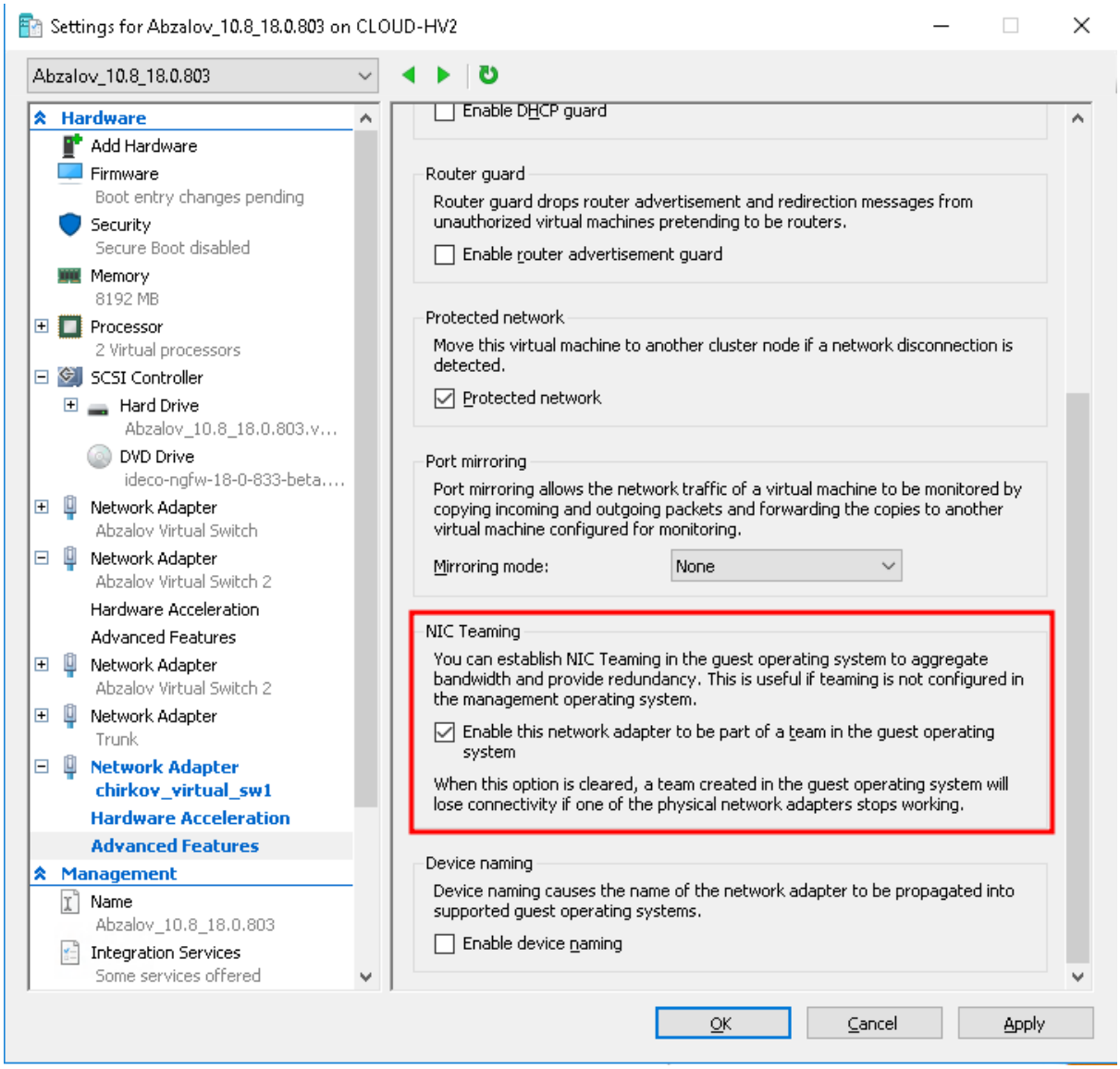


Получившийся виртуальный свитч можно использовать для добавления новых интерфейсов в LACP на гостевую систему.

3. Настройте подключение на вкладке **Сетевые интерфейсы -> Внешние и локальные** для вновь созданного LACP-интерфейса, как для обычного сетевого интерфейса NGFW.

37.24.2 Настройка на гостевой системе

1. Добавьте необходимое количество интерфейсов на гостевую систему, на основе виртуального свитча, например, с названием **Virtual Switch 1**.
2. На каждом добавляемом интерфейсе включите опцию NIC Teaming:



3. Добавьте вновь созданные интерфейсы в LACP-интерфейсы NGFW в разделе **Сетевые интерфейсы -> Агрегированные(LACP)**.
4. Настройте подключения на вкладке **Сетевые интерфейсы -> Внешние и локальные**.

37.25 Разрешить интернет всем: диагностика неполадок

37.25.1 Основное

Этот режим используется для диагностики неполадок.

Активный режим **Разрешить интернет всем** автоматически не отключается и работает, пока его не отключить.

При этом:

- не будут работать правила *файрвола*;
- не будет происходить фильтрация трафика;
- не будет производиться сбор веб-статистики;
- не будет доступа к серым IP-адресам за NGFW из внешней сети;

- пользователям будет разрешен доступ в интернет без авторизации.

Включить режим можно двумя способами:

1. Через веб-интерфейс.

Для этого нажмите на иконку технической поддержки в верхней правой части окна и в открывшемся окне переведите ползунок активации режима в положение **Активно.**

2. Через локальное меню.
Для этого введите номер пункта **6. Включить режим Разрешить интернет всем** и нажмите **Enter** для применения настройки.

37.26 Удаленный доступ к серверу

37.26.1 Доступ по SSH к локальному меню сервера

Для подключения по SSH из внешних или локальных сетей выполните действия:

1. Перейдите в раздел **Управление сервером -> Администраторы**.

2. Уточните сеть, из которой планируется подключение:

- При подключении из внешних сетей активируйте **Доступ по SSH из внешних сетей**.
- При подключении из локальных сетей активируйте **Доступ по SSH из локальных сетей**.

3. Подключитесь к серверу с помощью любого SSH-клиента (например, PuTTY), используя 22 порт. Скачать SSH-клиент PuTTY можно на сайте https://www.putty.org/. Необходимо указать логин **Администратора** и его пароль.

4. Используйте `ideco-local-menu --debug` для доступа к локальному меню или `ls` для вывода каталогов текущей директории.

Пример подключения при помощи OpenSSH через консоль:

```
[test@My-PC home]$ ssh admin@192.168.100.183
admin@192.168.100.183's password:
Last login: Wed Sep  6 11:51:38 2023 from 192.168.100.1
[admin@localhost ~]#
```

37.26.2 Доступ к веб-интерфейсу сервера из сети интернет

Доступ из внешней сети:

- Включите функцию **Доступ к веб-интерфейсу из внешней сети** в разделе **Управление сервером -> Администраторы**. Для доступа введите внешний IP-адрес Ideco NGFW и порт 8443.

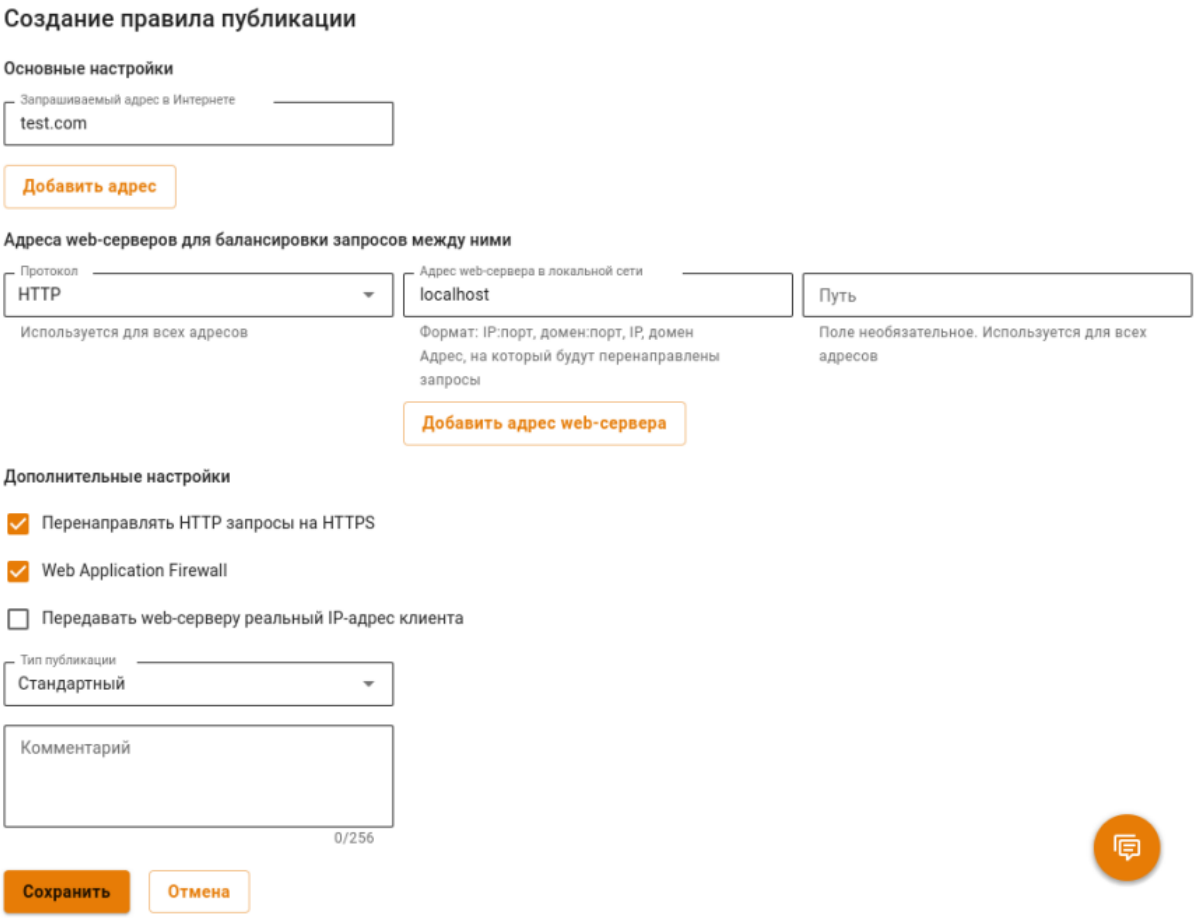
Доступ по VPN:

- Создайте VPN-подключение к серверу, например, по IPsec, IKEv2 или SSTP. После подключения можно перейти в веб-интерфейс по IP-адресу любого локального интерфейса (в том числе IP-адрес из диапазона для VPN-подключений. Адрес по умолчанию - 10.128.0.1).

Публикация через обратный прокси:

1. Перейдите в раздел **Сервисы -> Обратный прокси**.

2. Добавьте новое правило, заполнив поля:



3. Укажите в качестве запрашиваемого адреса IP-адрес или доменное имя внешнего интерфейса Ideco NGFW.

4. Нажмите на кнопку **Сохранить** и зайдите по одному из адресов, которые были указаны в поле **Запрашиваемый адрес в интернете**.

37.27 Тестирование оперативной памяти сервера

37.27.1 Основное

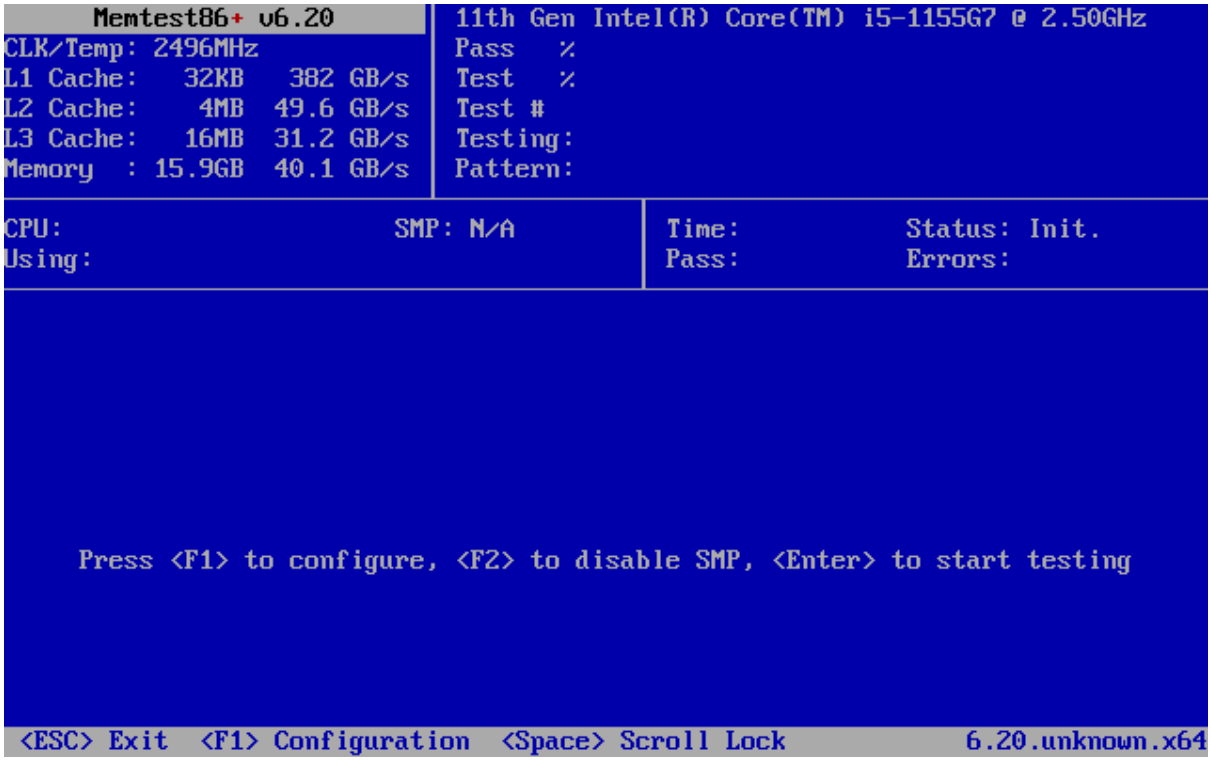
Для корректной работы сервера требуется, чтобы все его аппаратные составляюшие работали исправно. Тестирование памяти позволяет исключить из рассмотрения часть возможных проблем с памятью сервера при поиске неисправностей.

При загрузке GRUB для тестирования оперативной памяти используйте Memtest86+. Для запуска тестирования памяти выполните действия:

1. При загрузке сервера выберите **Memory test**:

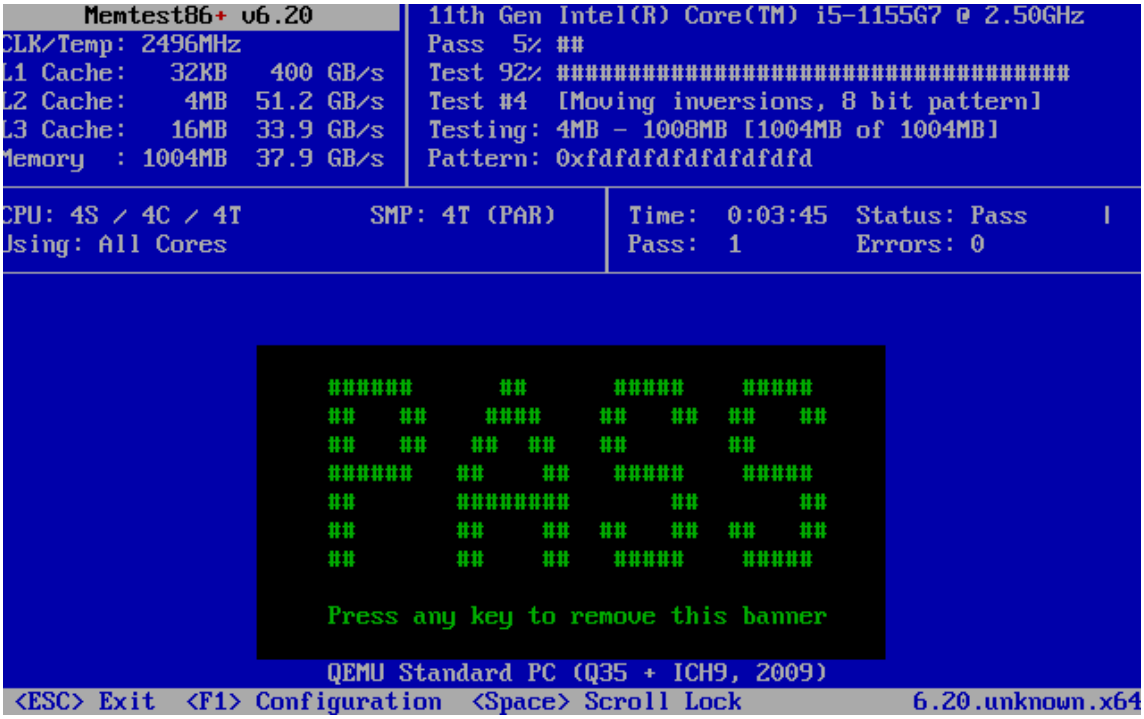


2. Для начала тестов нажмите **Enter** или подождите 5 секунд до автоматического запуска тестирования:

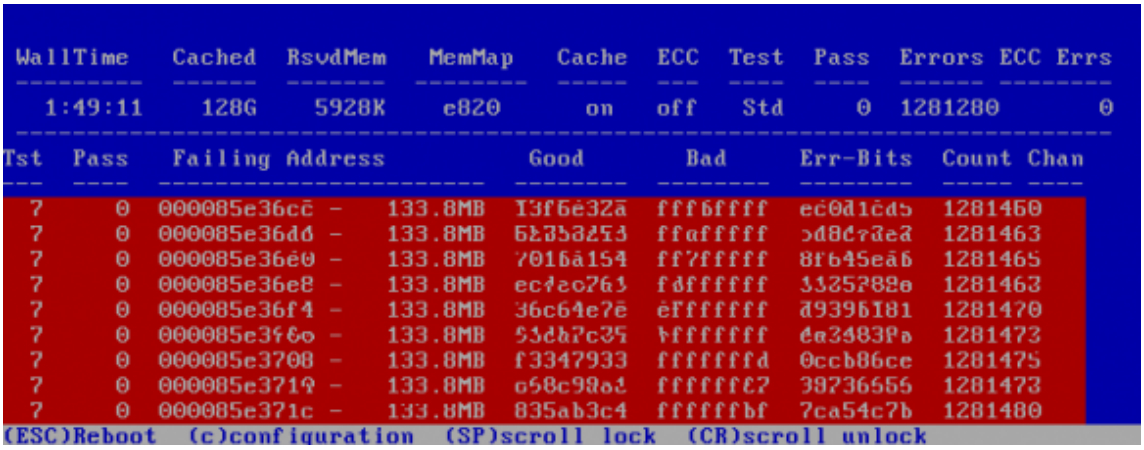


Подсказка: Для выбора режима диагностики **Fail-Safe Mode** нажмите **F1**.
Для выбора режима диагностики **Multi-Threading(SMP)** нажмите **F2**.

- Если появится запись **PASS**, тесты памяти пройдены успешно:



- При ошибке памяти появится запись вида:



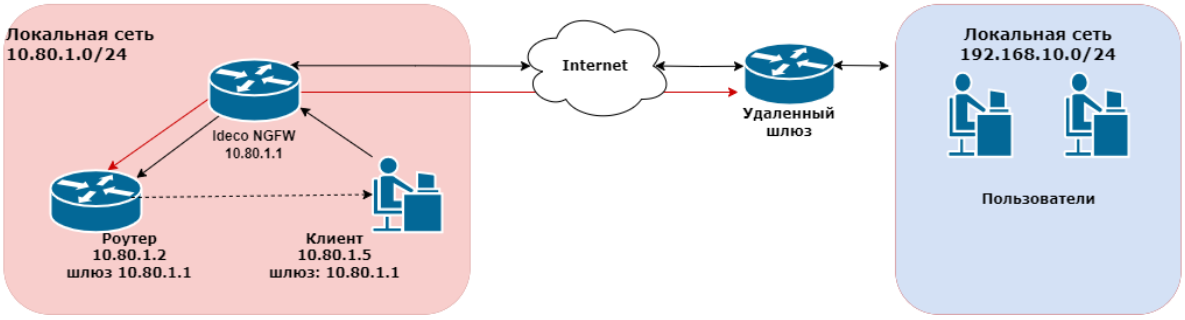
37.28 Как избавиться от асимметричной маршрутизации трафика

При попытке настроить доступ в удаленные сети через роутер в локальной сети может возникнуть асимметричная маршрутизация, препятствующая прохождению пакетов между двумя локальными сетями. В этой статье описаны случаи возникновения асимметричной маршрутизации и способы предотвращения.

Пример. В локальной сети NGFW используется роутер, устанавливающий связь с другими сетями. NGFW - шлюз по умолчанию для клиентов сети. Требуется настроить маршрутизацию на NGFW так, чтобы клиенты сети `10.80.1.0/24` получали доступ в удаленную сеть `192.168.10.0/24` и обратно через роутер.

37.28.1 Асимметричная маршрутизация при наличии роутера в локальной сети

Неправильная топология сети, способствующая асимметричной маршрутизации:

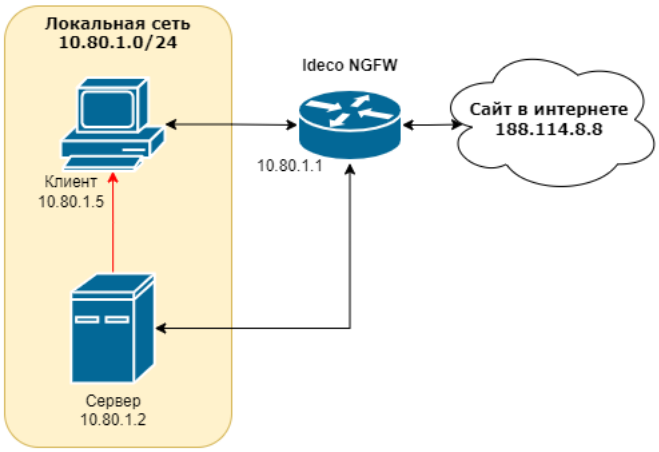


- `10.80.1.1` - шлюз для локальной сети `10.80.1.0/24`;
- `10.80.1.2` - роутер, имеющий доступ в удаленную сеть `192.168.10.0/24`;
- `10.80.1.5` - адрес хоста в локальной сети;
- **Красные стрелки** - двусторонняя связь роутера с удаленным шлюзом или роутером, обеспечивающая доступ к удаленной сети `192.168.10.0/24` (туннель к шлюзу, маршрут до роутера в соседнюю сеть предприятия);
- **Черные стрелки** - трафик от хостов локальной сети `10.80.1.0/24` до удаленной сети `192.168.10.0/24` через шлюз NGFW (`10.80.1.1`) и роутер (`10.80.1.2`);
- **Пунктирная стрелка** - трафик, который роутер возвращает хостам локальной сети в обход NGFW, поэтому хосты этот трафик обратно не принимают.

Предупреждение: Часть трафика от клиентов до роутера идет через шлюз, а часть - непосредственно от роутера до абонентов сети. Разная маршрутизация на разных участках делает прохождение пакетов между двумя локальными сетями невозможной.

37.28.2 Асимметричная маршрутизация при публикации сайтов через DNAT

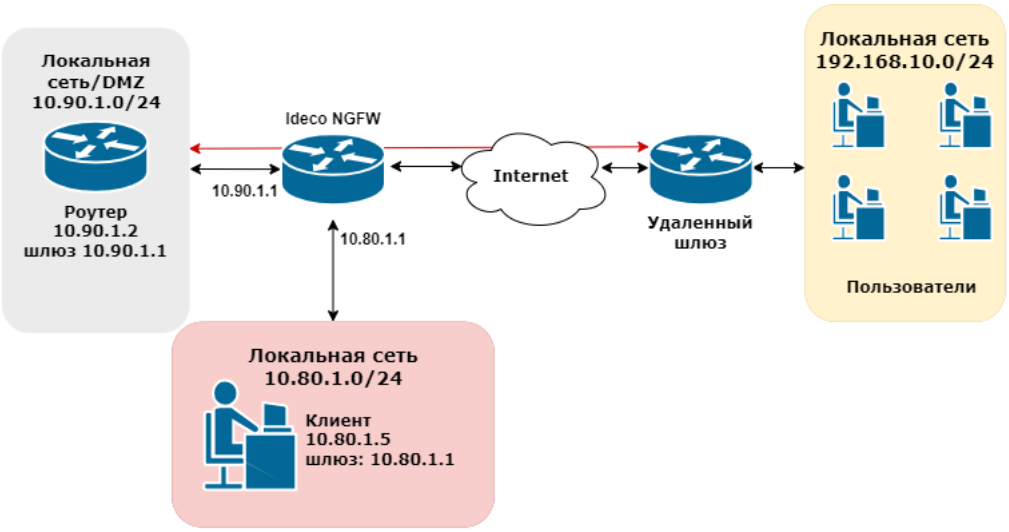
Асимметричная маршрутизация также возникает, когда в одной локальной сети находится хост и сервер, на котором расположен опубликованный при помощи DNAT-правила ресурс:



- `10.80.1.1` - адрес Ideco NGFW в локальной сети;
- `10.80.1.2` - адрес сервера в локальной сети;
- `10.80.1.5` - адрес хоста в локальной сети;
- `188.114.8.8` - адрес сайта в интернете;
- **Красная стрелка** - ответ напрямую от сервера хосту в локальной сети.

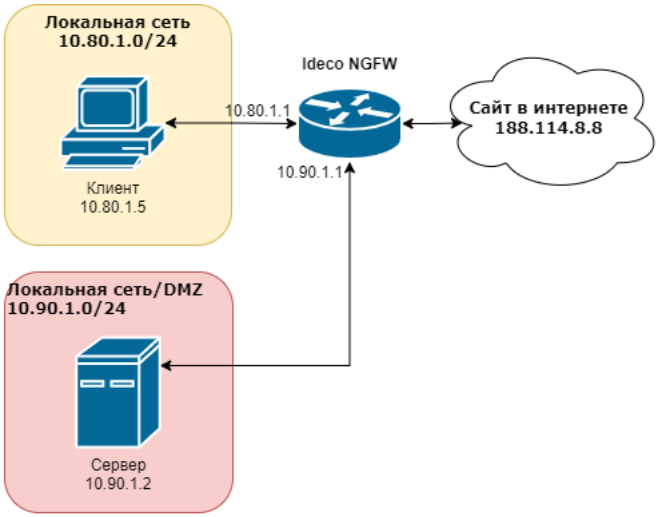
Когда хост `10.80.1.5` обращается на сайт по внешнему адресу `188.114.8.8` (например, в случае обращения по доменному имени, которое разрешено во внешнем IP), трафик проходит через NGFW. На NGFW срабатывает правило DNAT и перенаправляет трафик на сервер `10.80.1.2`, а сервер отвечает хосту, минуя NGFW.

37.28.3 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.

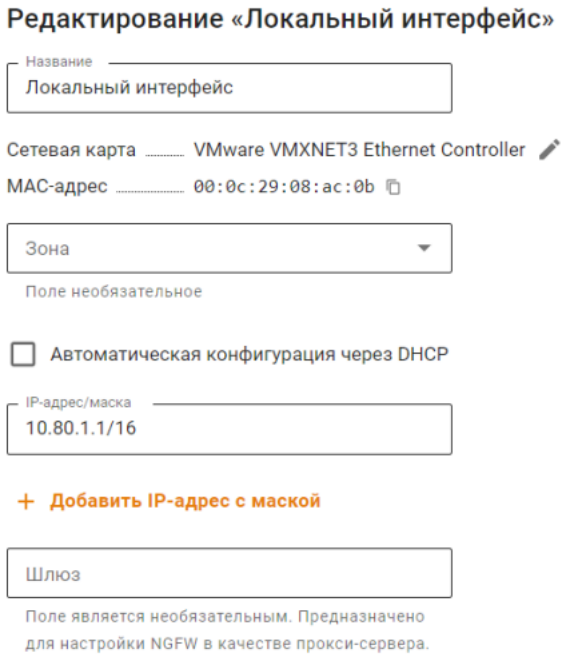
Физически роутер будет находиться в сегменте дополнительной сетевой карты.

Настройка NGFW:

Для настройки нескольких виртуальных локальных сетей на одном физическом локальном интерфейсе NGFW перейдите в раздел **Сервисы -> Сетевые интерфейсы** и выполните действия:

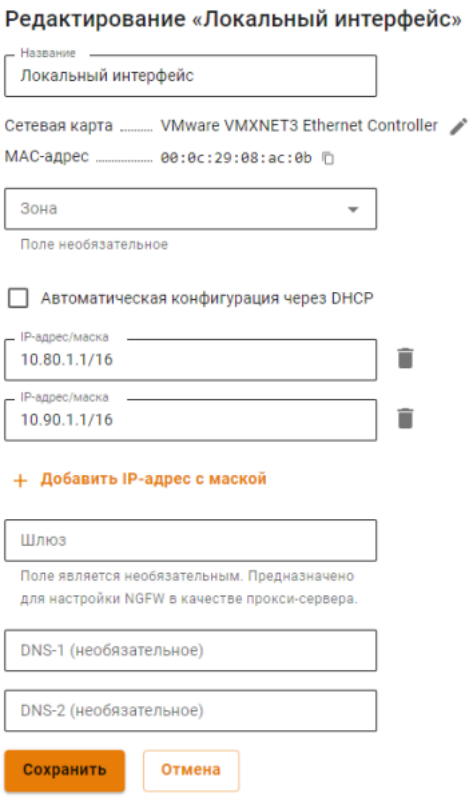
1. Откройте в режиме редактирования **Локальный интерфейс**, к которому подключены пользователи нужной вам локальной сети (`10.80.1.1/24`), нажав на  напротив его названия.

2. Если IP-адрес вашей локальной сети был автоматически сконфигурирован через DHCP, отключите опцию и введите его вручную:



3. Нажмите на 

и введите IP-адрес DMZ для изоляции роутера:

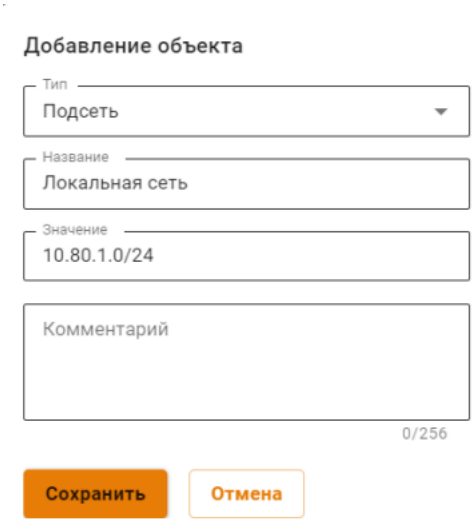


4. Нажмите **Сохранить**.

После изоляции роутера в DMZ нужно указать маршрут на NGFW до удаленной сети. Для этого перейдите в **Сервисы -> Маршрутизация** и выполните действия:

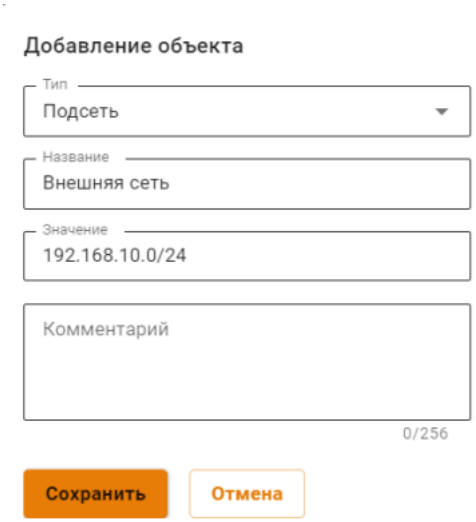
1. Перейдите на вкладку **Внешних сетей** нажмите кнопку **Добавить**.

2. В поле **Адрес источника** нажмите **Добавить объект**, выберите тип **Подсеть** и введите адрес вашей локальной сети (`10.80.1.0/24`):



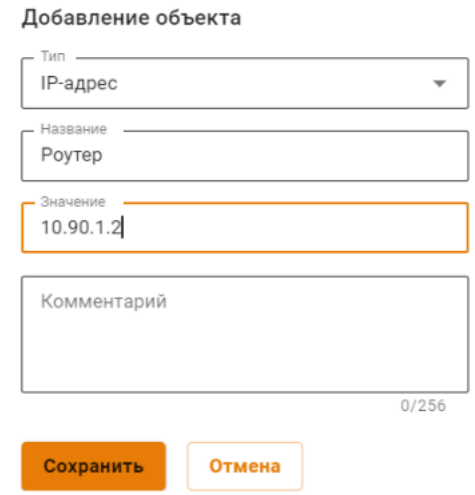
Выберите в качестве источника только что созданный объект.

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:

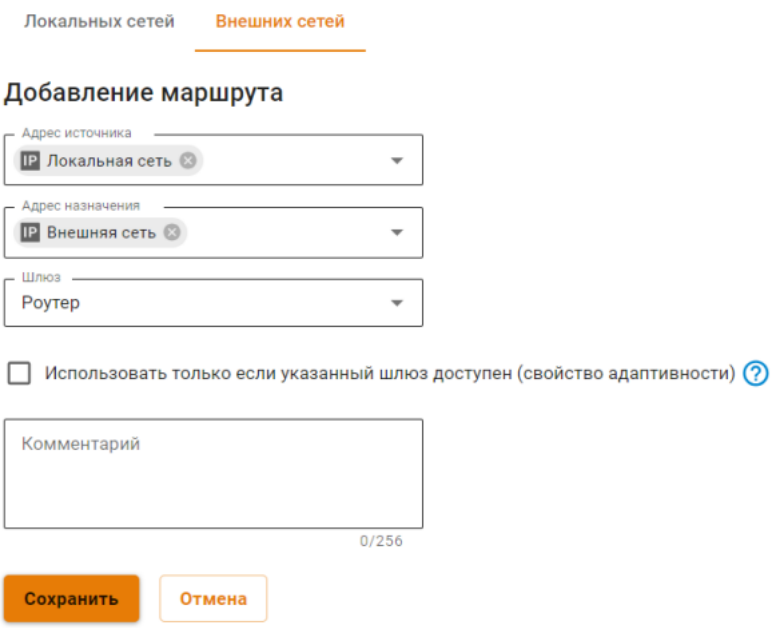


Выберите в качестве назначения только что созданный объект.

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:

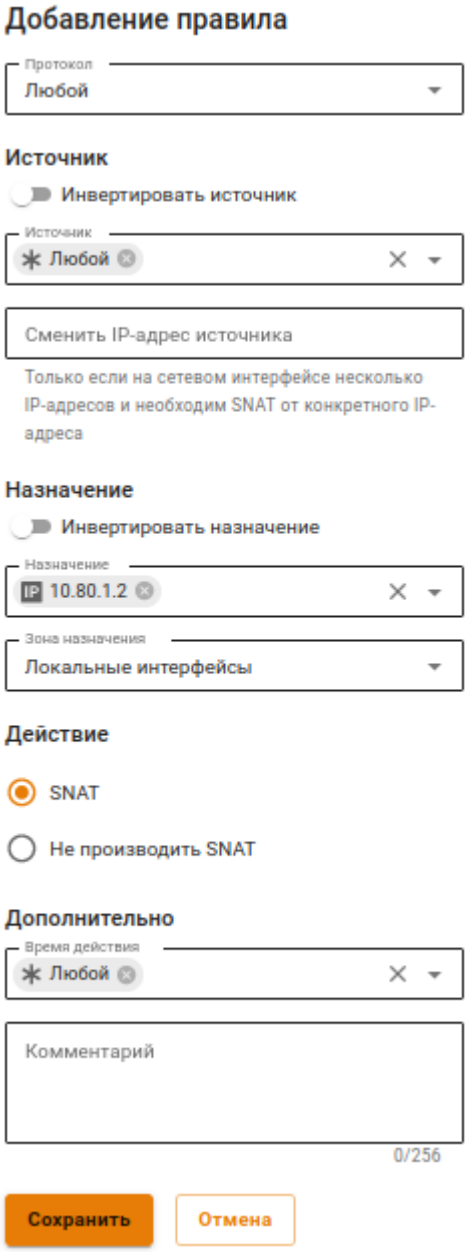
1. Для хостов из подсети `10.80.1.0/24` значение шлюза и DNS-сервера - `10.80.1.1`.

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`.

37.29 Что делать если ваш IP попал в черные списки DNSBL

Если используется белый статический IP-адрес, то попадание IP-адреса в черные списки может означать, что в сети зафиксирована бот-активность, участие в DDoS-атаках либо рассылка спама.

Наличие в черных списках динамического IP-адреса из «домашних» диапазонов IP-адресов провайдеров в целом нормальное явление, т. к. вредоносная активность в таком случае может исходить не из вашей сети.

37.29.1 Порядок действий при попадании в черный список

1. Узнайте причину попадания в DNSBL-список. Часто сервис называет конкретный вирус или сетевой червь и его особенности - используемые порты, протоколы. Выполните рекомендации сервиса.

2. Активируйте систему предотвращения вторжений на шлюзе. Проанализируйте логи, наличие обращений к командным центрам ботнетов.

3. Проверьте все компьютеры сети антивирусом. Убедитесь, что антивирусная защита активирована, базы обновлены (как правило, вирусы мешают обновлению баз или работе антивирусного ПО).

4. После лечения зараженных компьютеров отправьте в DNSBL-сервис сообщение с просьбой исключить IP из черного списка.

37.29.2 Ideco NGFW

Наше решение обладает всей функциональностью, обеспечивающей максимальную защиту от спам-ботов, ботнет-клиентов и предотвращение вирусной активности в сети.

До 22 пользователей - решение предоставляется бесплатно. Для 10000 пользователей доступна 40-дневная пробная версия.

Скачать Ideco NGFW

37.30 Как восстановить доступ к Ideco NGFW

37.30.1 Основное

Для этого нужно выполнить следующие действия:

1. Перезагрузите сервер. При появлении меню загрузчика GRUB с выбором ядра Linux для загрузки системы нажмите англоязычную клавишу **E** на клавиатуре.

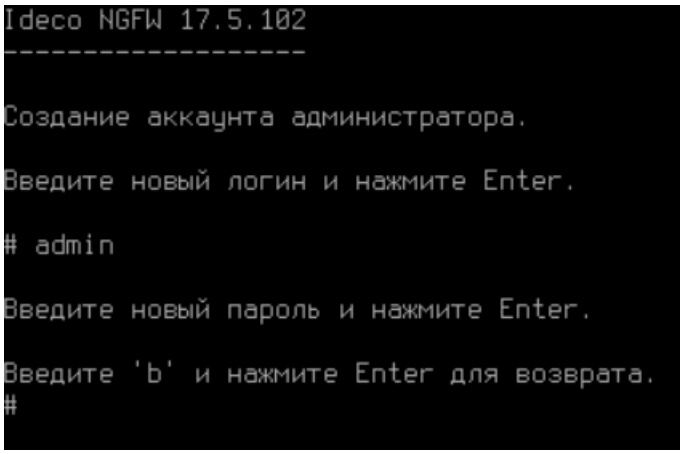


2. Откроется окно параметров ядра с возможностью редактирования. Переместите указатель стрелками на клавиатуре вправо до слова `quiet` и допишите текст `p=1`:

Строка с параметрами отображается внизу экрана.

3. Нажмите `Enter`.

4. После повторной загрузки системы появится окно создания аккаунта администратора. Задайте новый логин и пароль администратора:

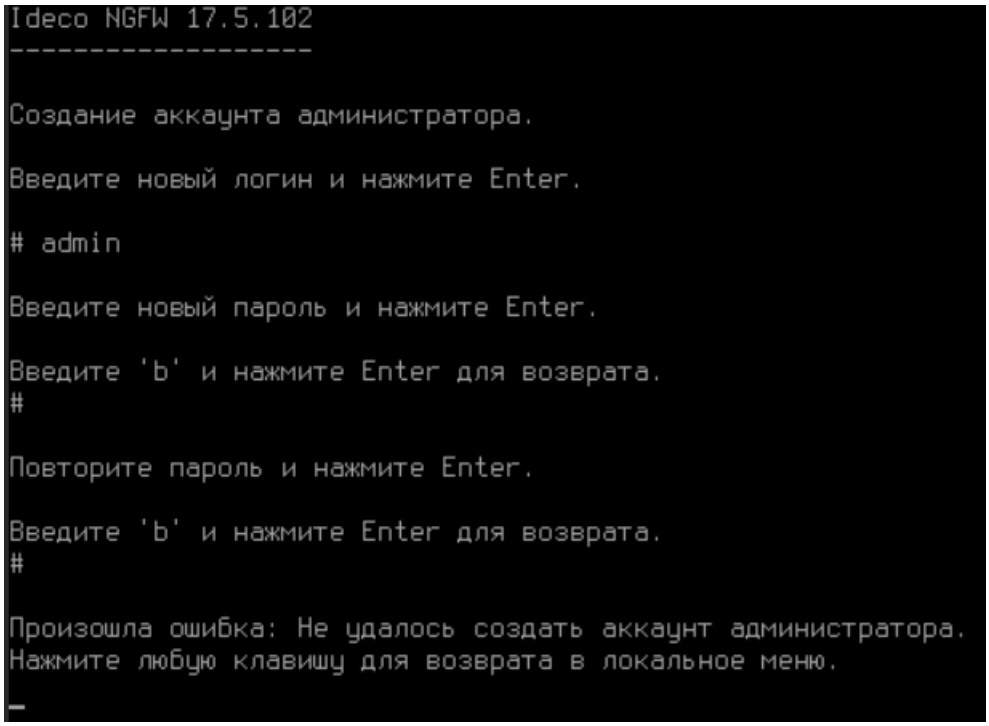


Требования к созданию пароля администратора:

- Минимальная длина пароля - 11 символов;
- Строчные и заглавные латинские символы;
- Цифры;
- Специальные символы (! # $ % & „ * + и т. д.).

Предупреждение: Если при создании нового логина администратора он будет совпадать с предыдущим логином, то будет выведена ошибка. Создайте имя администратора, отличное от предыдущего.

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



37.31 Как восстановиться на прошлую версию после обновления Ideco NGFW

37.31.1 Основное

Рекомендуем использовать эту инструкцию, если после обновления Ideco NGFW работает некорректно.

Подсказка: Возможность восстановиться на предыдущую версию после обновления Ideco NGFW доступна с версии 12.0.

При обновлении NGFW на версию 12.0 и выше вся информация версии, с которой обновляетесь, сохранится на диске NGFW.

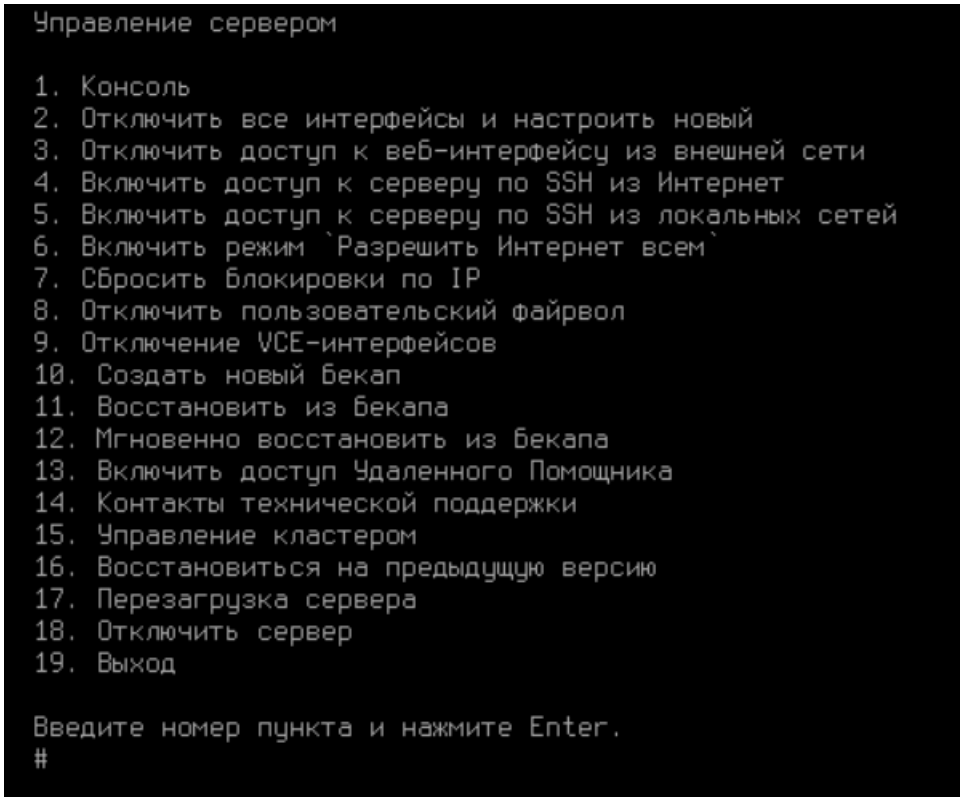
При восстановлении на предыдущую версию данные перенесены не будут. Сохраните бекап на внешнем носителе. Подробную информацию о работе с бекапом можно прочитать по *ссылке*.

Для восстановления на предыдущую версию выполните действия:

1. Перейдите в локальное меню Ideco NGFW.

2. Введите логин и пароль администратора.

3. Укажите номер пункта 16 и нажмите **Enter**:

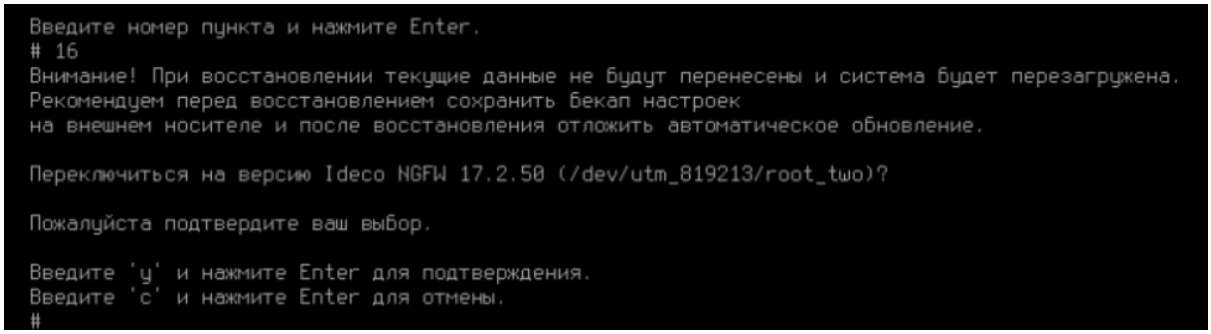


Появится окно с предупреждением и описанием версии, на которую произойдет переключение.

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

---

3. Введите **„y“** для подтверждения выбора и нажмите **Enter**:



4. После перезагрузки Ideco NGFW переключится на предыдущую версию.

37.32 Проверка настроек фильтрации с помощью security ideco

При правильной настройке общий уровень защиты должен показывать зеленый цвет. Если это не так, проверьте с помощью этой статьи настройки **Контент-фильтра** и других служб фильтрации трафика.

37.32.1 Предварительная проверка

Перейдите в веб-интерфейс Ideco NGFW и убедитесь, что все описанные ниже службы включены и функционируют корректно.

Раздел Правила трафика

- *Контент-фильтр*;
- *Контроль приложений*;
- *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*.

37.32.2 Проверка настроек служб

Контент-фильтр

Категории сайтов, которые запрещают правила Контент-фильтра:

- Анонимайзеры;
- Ботнеты;
- Фишинг/мошенничество;
- Казино, лотереи, тотализаторы;
- Порнография;
- Список Минюста;
- Астрология и гороскопы;

- Знакомства;
- Компьютерные игры;
- Мультфильмы, аниме и комиксы;
- Развлекательные новости и сайты про знаменитостей;
- Онлайн-реклама и баннеры;
- Торрент-трекеры.

Чтобы антивирус проверял HTTPS-трафик, необходимо создать правило расшифровки всего HTTPS-трафика для пользователей. Это правило будет применяться, в том числе к тем, кто проверяет настройки на сайте security.ideco.ru.

Проверьте, что **Контент-фильтр** работает. Для этого перейдите с компьютера пользователя на сайт: `sex.com`. Если фильтр работает, то отобразится страница блокировки.

Контроль приложений

Для защиты от «пожирателей времени и трафика» 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.

37.33 Поддержка устаревших алгоритмов шифрования

37.33.1 Основное

Ideco NGFW основан на операционной системе Fedora. В Ideco NGFW используется Fedora 39. 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.

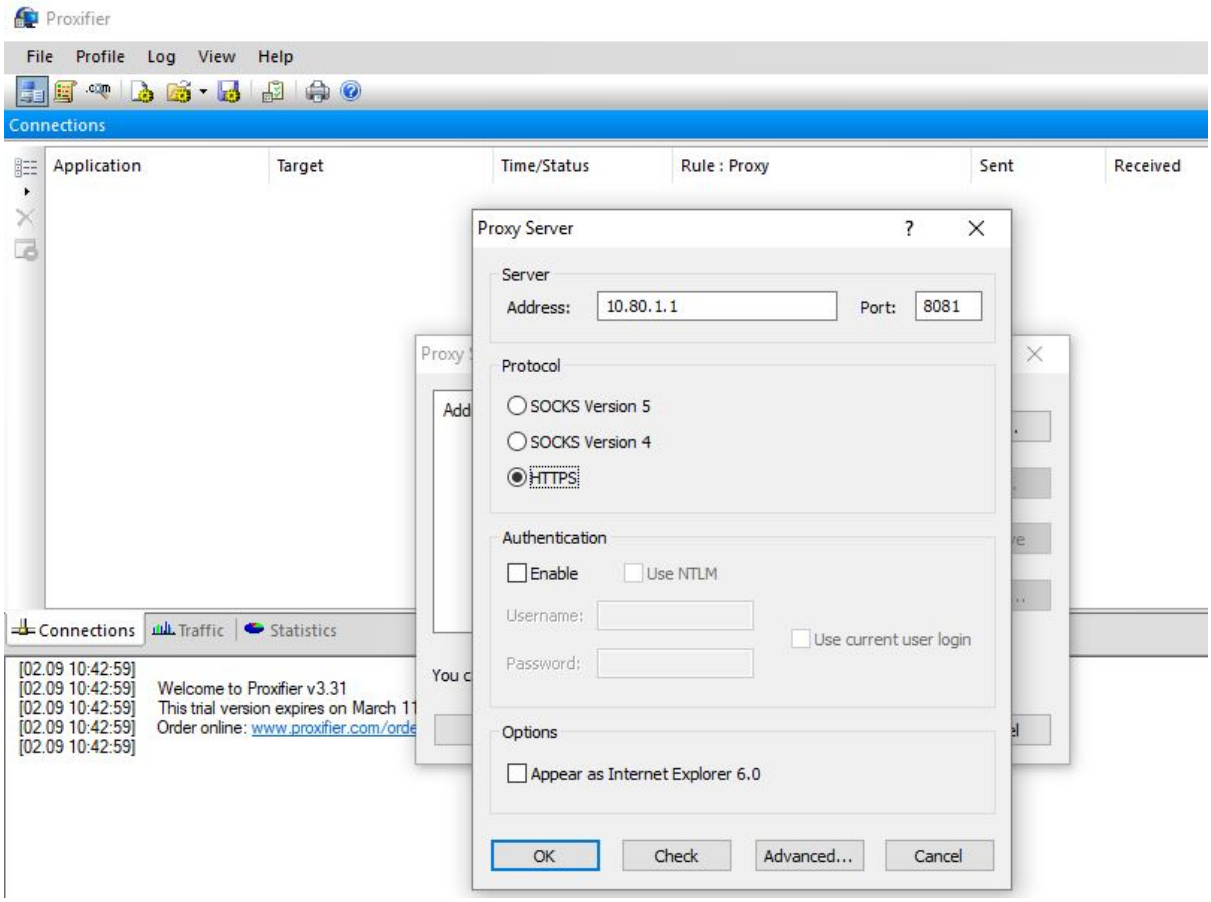
37.34 Настройка программы Proxifier для прямых подключений к прокси серверу

Скачать Proxifier можно с сайта разработчика.

37.34.1 Настройка

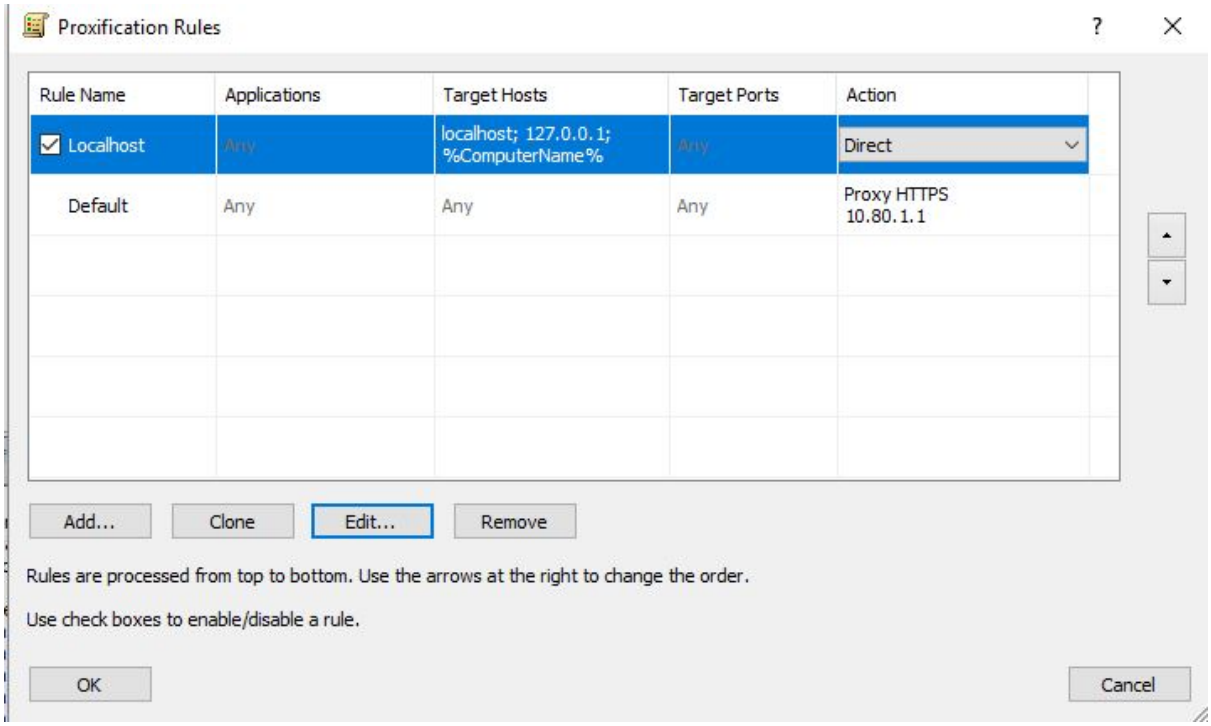
Выполните стандартные настройки браузера для прямых подключений к прокси-серверу, а затем настройте программу для перенаправления остального трафика на прокси-сервер.

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.

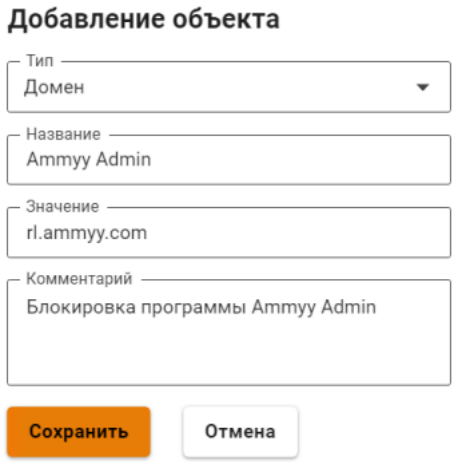
37.35 Блокировка популярных ресурсов

37.35.1 Основное

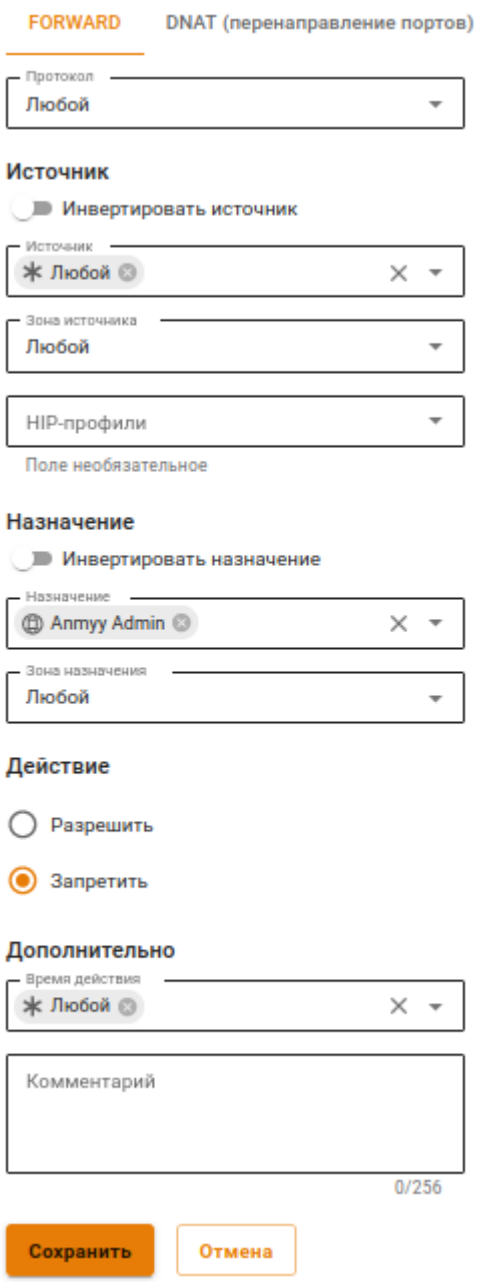
Блокировка Ammyy Admin:

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:



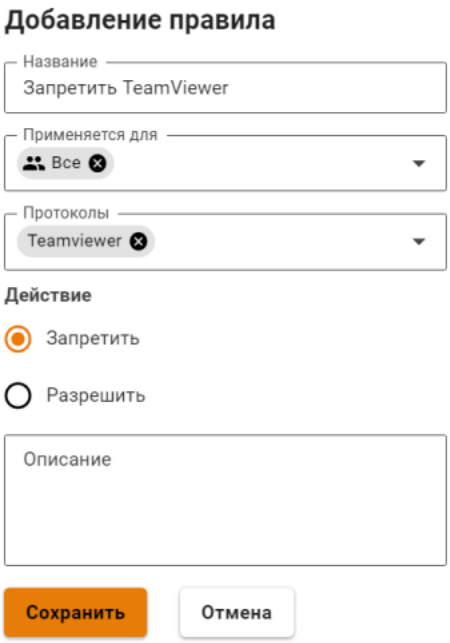
2. Перейдите на вкладку **Правила трафика -> Файрвол -> FORWARD** и создайте правило запрета для нужных пользователей или групп. В поле **Назначение** выберите объект, созданный в пункте 1:



Блокировка TeamViewer:

TeamViewer - это программное обеспечение для удаленного доступа и управления компьютерами. Его можно заблокировать с помощью *Контроль приложений*.

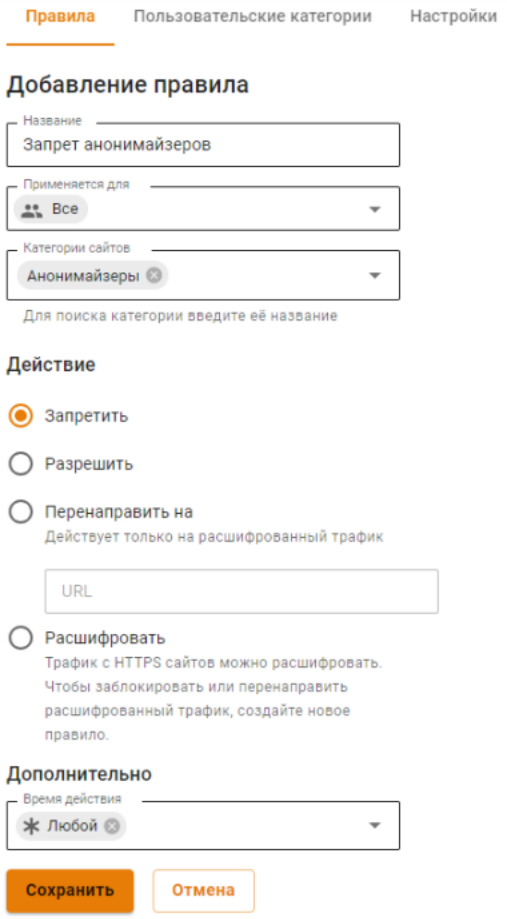
Перейдите в раздел **Правила трафика -> Контроль приложений**. Создайте новое правило, указав в поле **Протоколы** значение TeamViewer:



Блокировка анонимайзеров:

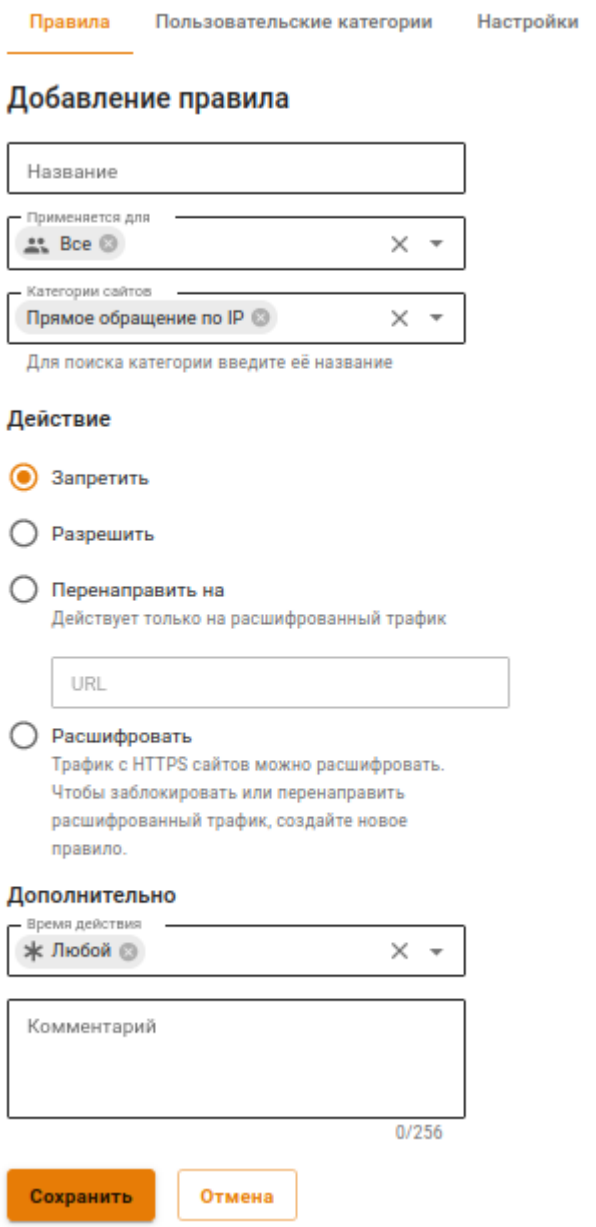
Заблокировать анонимайзеры можно в разделе **Правила трафика** тремя способами:

1. Анонимайзеры, работающие по протоколам HTTP(S), можно заблокировать в разделе *Контент-фильтр*. Для этого создайте правило, в котором запретите категорию сайтов **Анонимайзеры**:

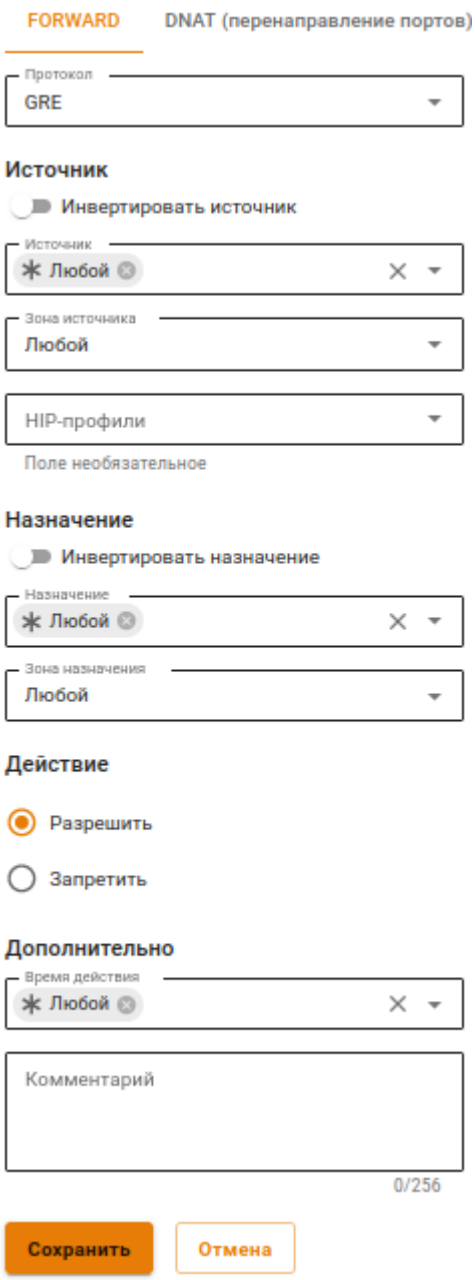


2. Чтобы предотвратить обход Контент-фильтра, создайте правило, которое будет блокировать прямые

обращения по IP-адресам в Контент-фильтре:



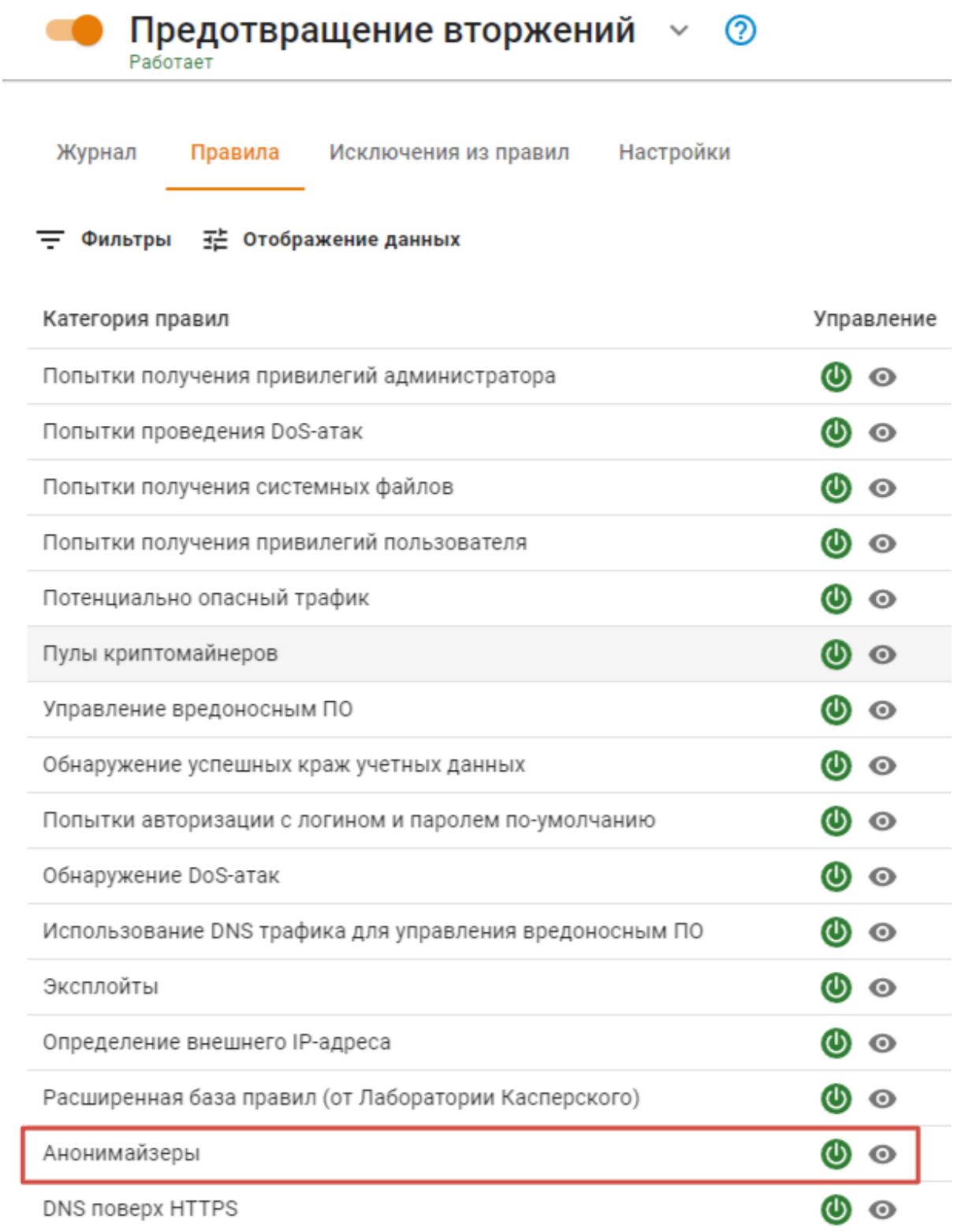
3. Для блокировки VPN-анонимайзеров, использующих протокол PPTP, достаточно заблокировать протокол GRE в правилах *Файрвола*:



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**:

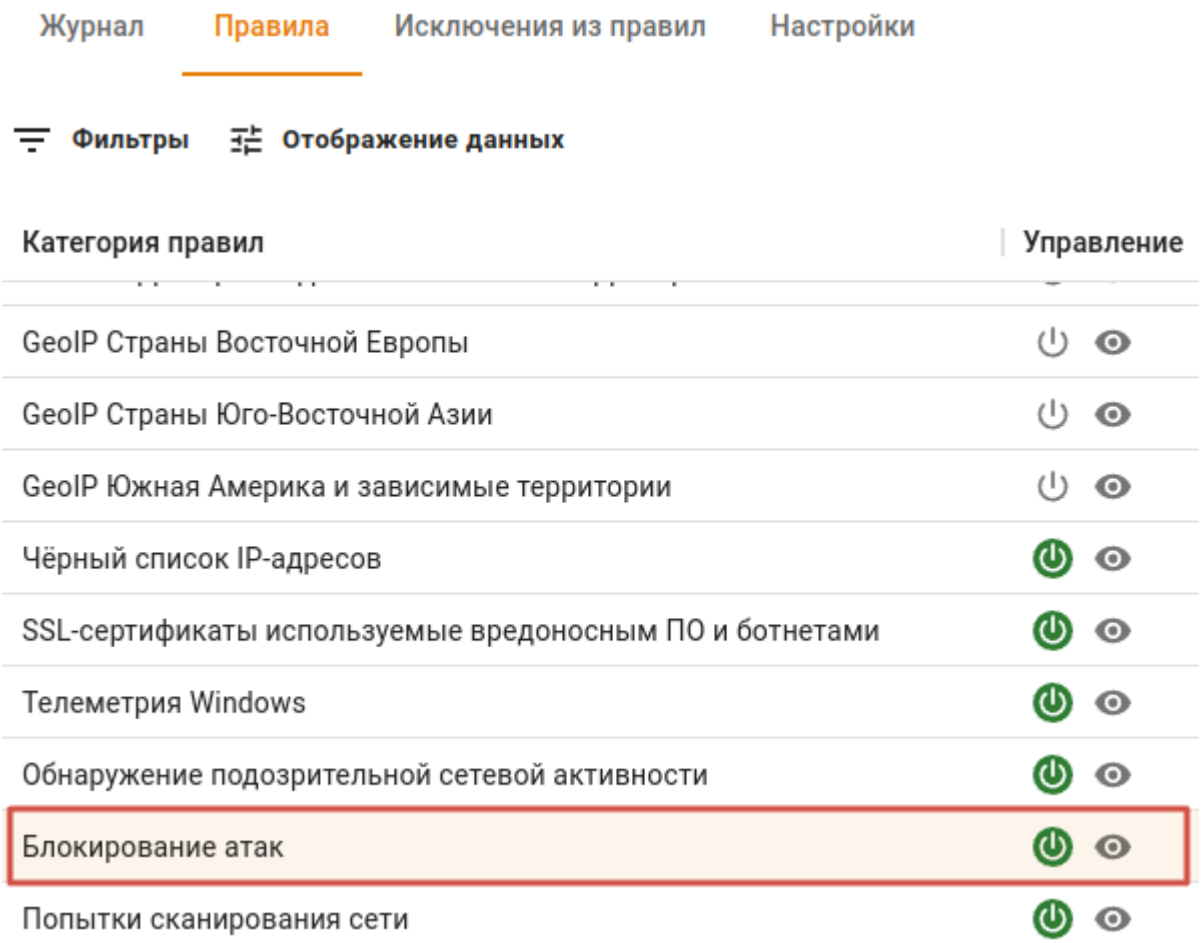


Блокировка Tor:

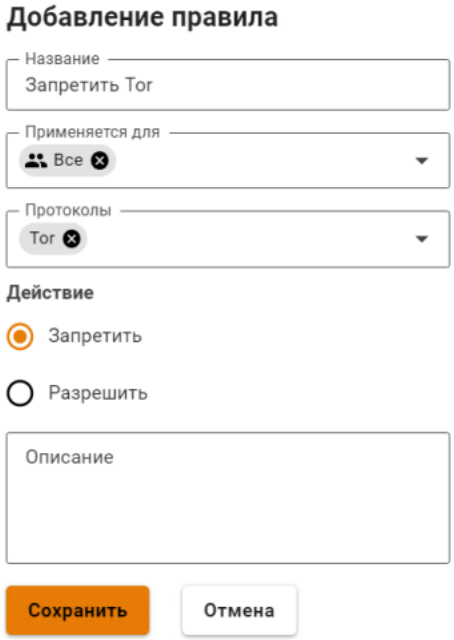
Tor - специально разработанное программное обеспечение и среда прокси-серверов, предназначенная для обхода различного рода блокировок, поэтому полностью заблокировать его сейчас невозможно.

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:

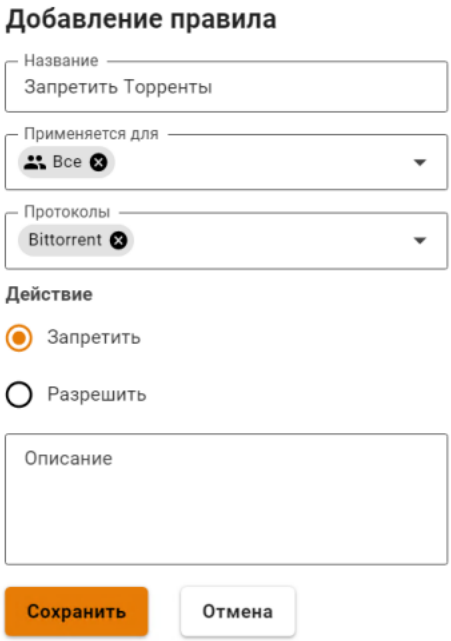


Блокировка торрентов:

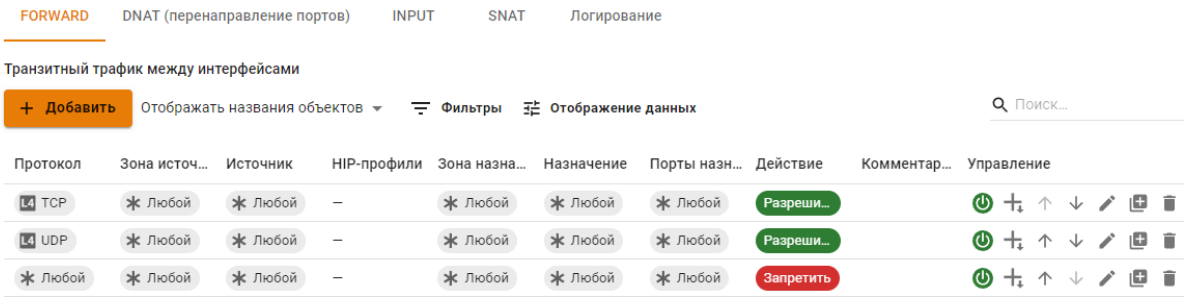
BitTorrent - P2P-протокол, предназначенный для обмена файлами через интернет.

Для ограничения возможности использования торрентов выполните следующие настройки:

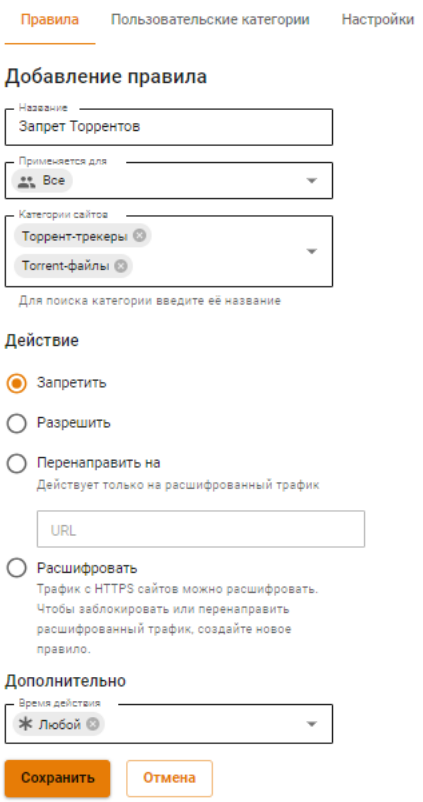
1. Запретите протокол BitTorrent с помощью правила в разделе *Контроль приложений*:



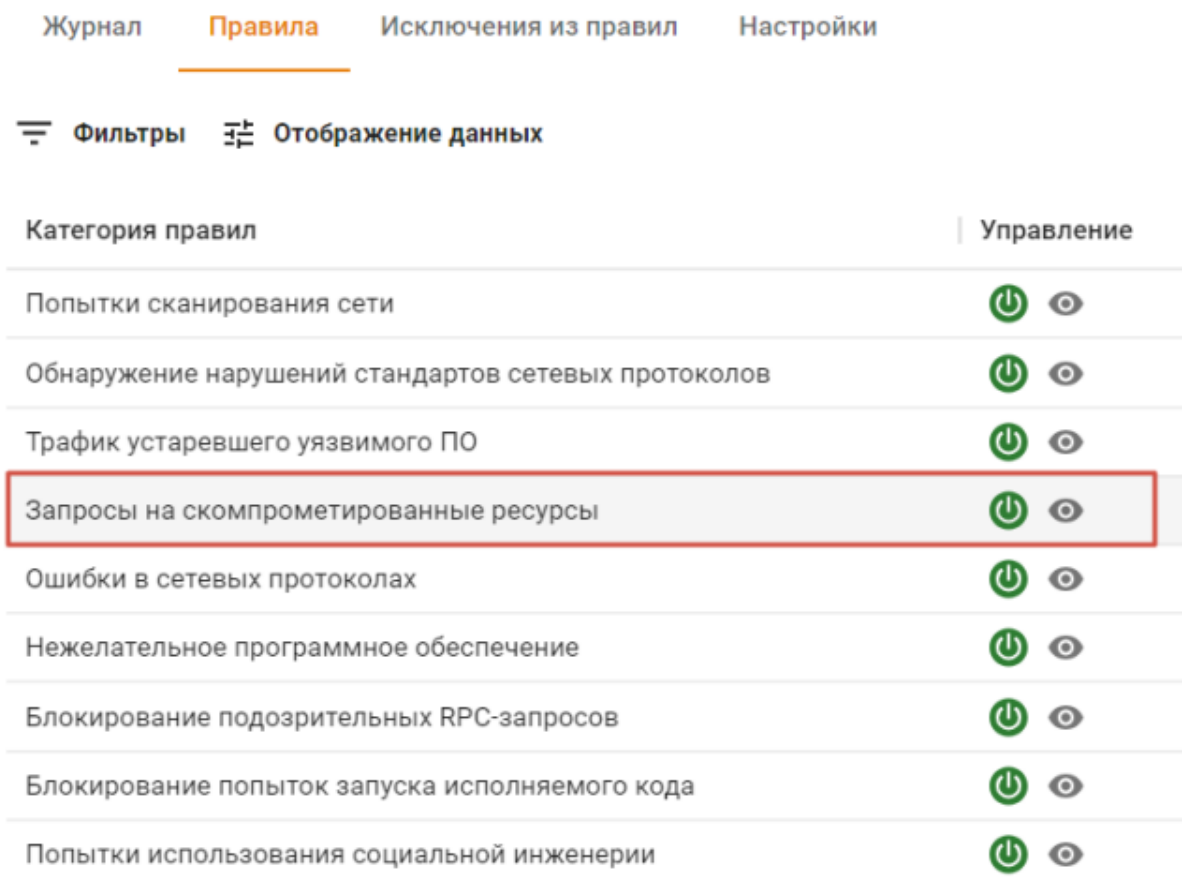
2. Перейдите на вкладку **Правила трафика -> Файрвол -> FORWARD** и разрешите нужные TCP и UDP порты пользователям. Затем создайте правило, которое запрещает все протоколы (правила действуют сверху вниз):



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:



37.36 Настройка прозрачной авторизации на Astra Linux

37.36.1 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**:**

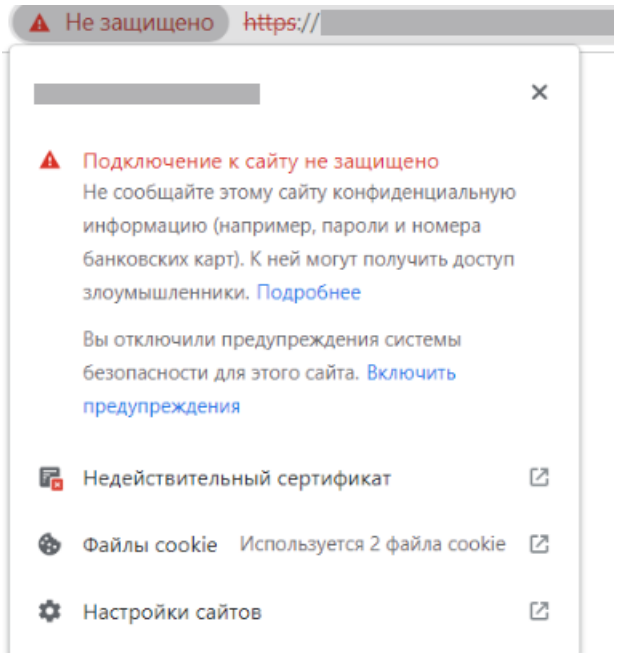
1. Запустите браузер и в адресной строке введите `about:config`, чтобы попасть в режим редактирования расширенных настроек.

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*.

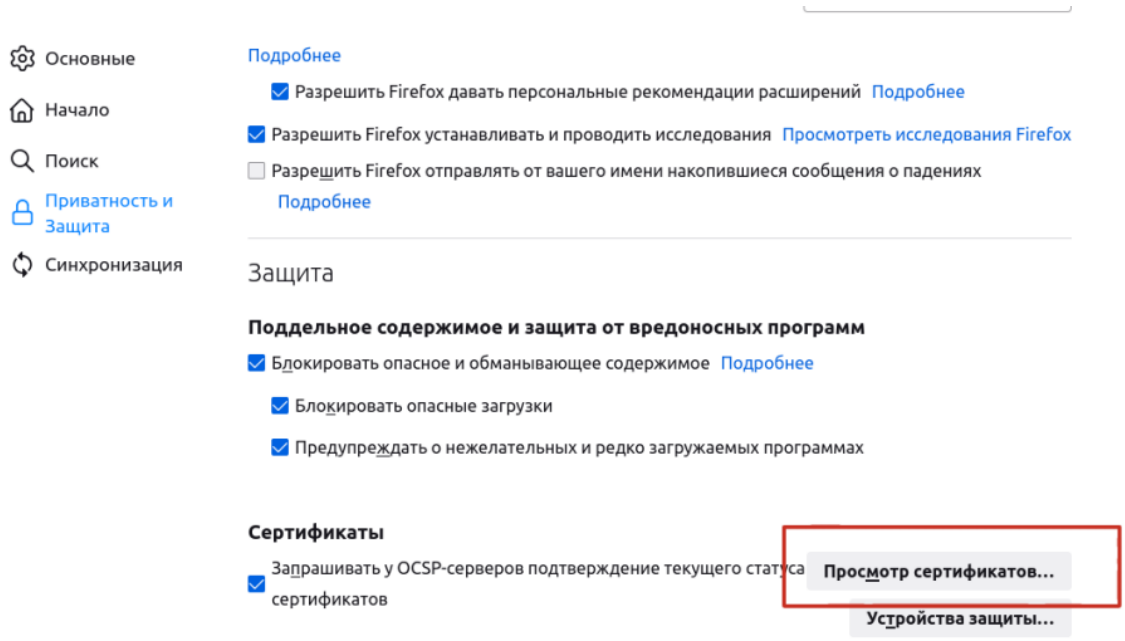
2. В браузере Chromium перейдите на вкладку **Безопасность -> Управление сертификатами -> Центры сертификации -> Импортировать** и добавьте сертификат в список доверенных.

**

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.

37.37 Настройка автоматической веб-аутентификации на Ideco NGFW на Linux

37.37.1 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`.

37.37.2 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.

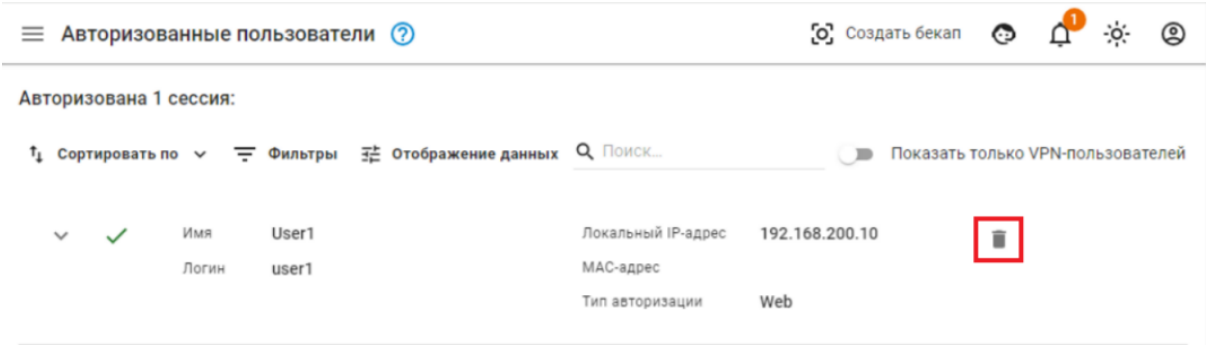
3. Сохраните файл и выйдите из редактора.

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.

37.38 Перенос данных и настроек на другой сервер

Подсказка: Восстановить бекап 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:

37.38.1 Этап 1: Копирование бекапа с сервера

В разделе веб-интерфейса **Управление сервером -> Бекапы -> Бекапы** создайте бекап настроек сервера. Загрузите созданную копию на ваш компьютер, нажав на кнопку **Скачать** в столбце **Управление**.

37.38.2 Этап 2. Установка Ideco NGFW на новый сервер

Инструкция по установке: *Процесс установки*.

37.38.3 Этап 3: Перенос бекапа 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 -> Бекапы -> Бекапы** нажмите кнопку добавления бекапа -> **Загрузить из файла** и выберите выгруженный на первом этапе бекап.

37.38.4 Этап 4: Восстановление БД из бекапа

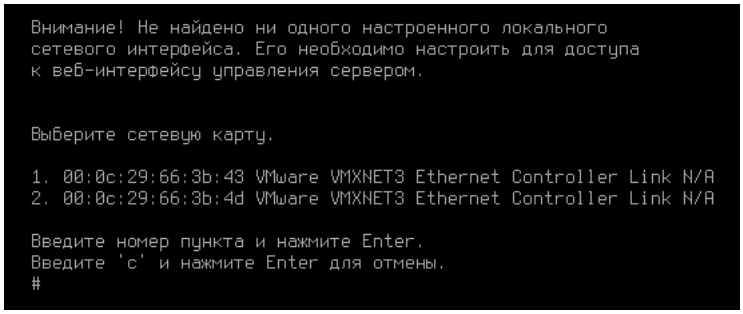
Нажмите кнопку **Применить** (иконка  в столбце **Управление**). Система будет перезагружена для применения настроек сервера.

37.38.5 Этап 5: Настройка восстановленного сервера

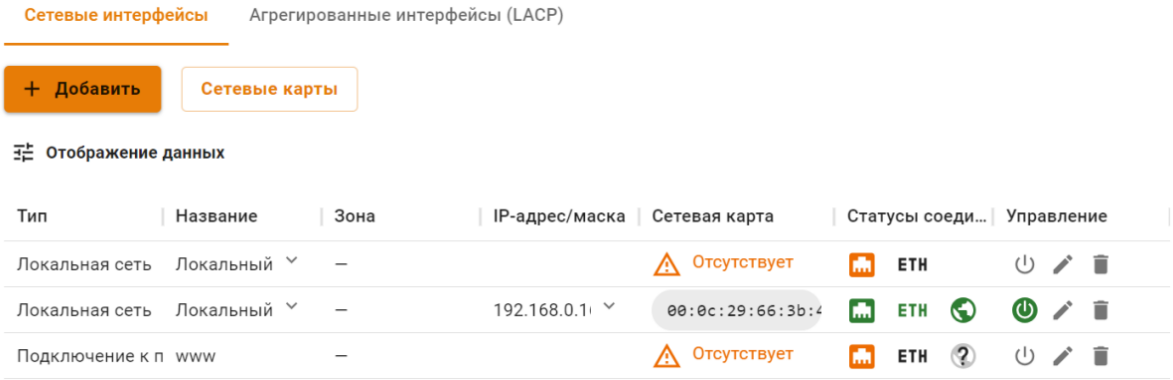
После перезагрузки Ideco NGFW, восстановленного из бекапа, веб-интерфейс будет недоступен, поскольку ни один локальный интерфейс не будет настроен. Для настройки выполните действия:

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;

37.38.6 Этап 6: Привязка лицензии к восстановленному из бекапа серверу

Если вы переносите бекап 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 бекапа из-за одинакового claster_id. Сервер-клон подменяет собой уже подключенный Ideco NGFW:

В случае возникновения такой проблемы обратитесь в *Техническую поддержку*.

37.38.7 Перенос данных почтового сервера

1. Скопируйте всю почту из папки `/var/mail/` на внешнее хранилище. Это можно сделать с помощью различных программ для копирования файлов между локальным компьютером и удаленным сервером (например: rsync, WinSCP, scp от ssh и др.).

2. Установите с загрузочного образа последнюю версию Ideco NGFW на физический диск.

3. Подключите второй физический диск, который будет использоваться для хранения почты.

4. В веб-интерфейсе Ideco NGFW перейдите в 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 выгрузите всю скопированную почту по пути `/var/spool/mail/`.

7. По окончании выгрузки файлов почты выполните команду:

```
chown -R ideco-mail-backend:ideco-mail-backend /var/spool/mail/
```

Подсказка: Команда выше меняет владельца и группу для файлов почты, чтобы почтовый демон `dovecot` мог иметь доступ к этим файлам.

37.39 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.

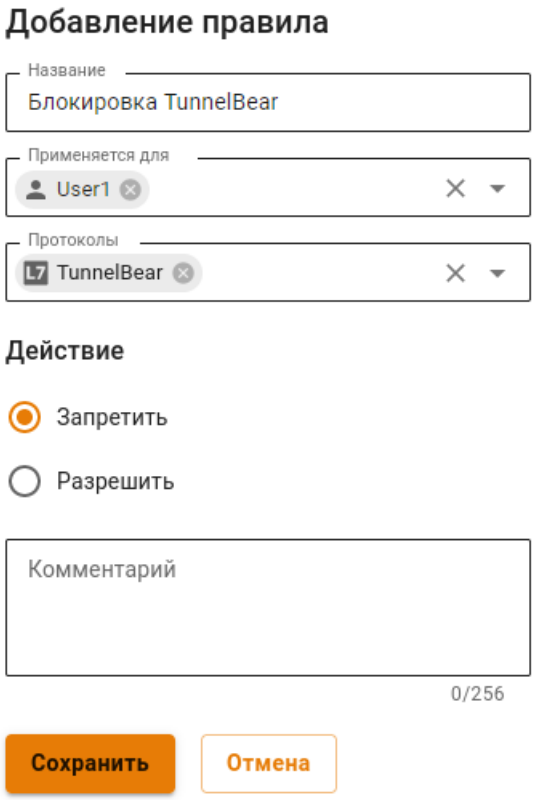
4. Файрвол.

Подсказка: INPUT-правила Файрвола обрабатывают трафик раньше прокси-сервера.

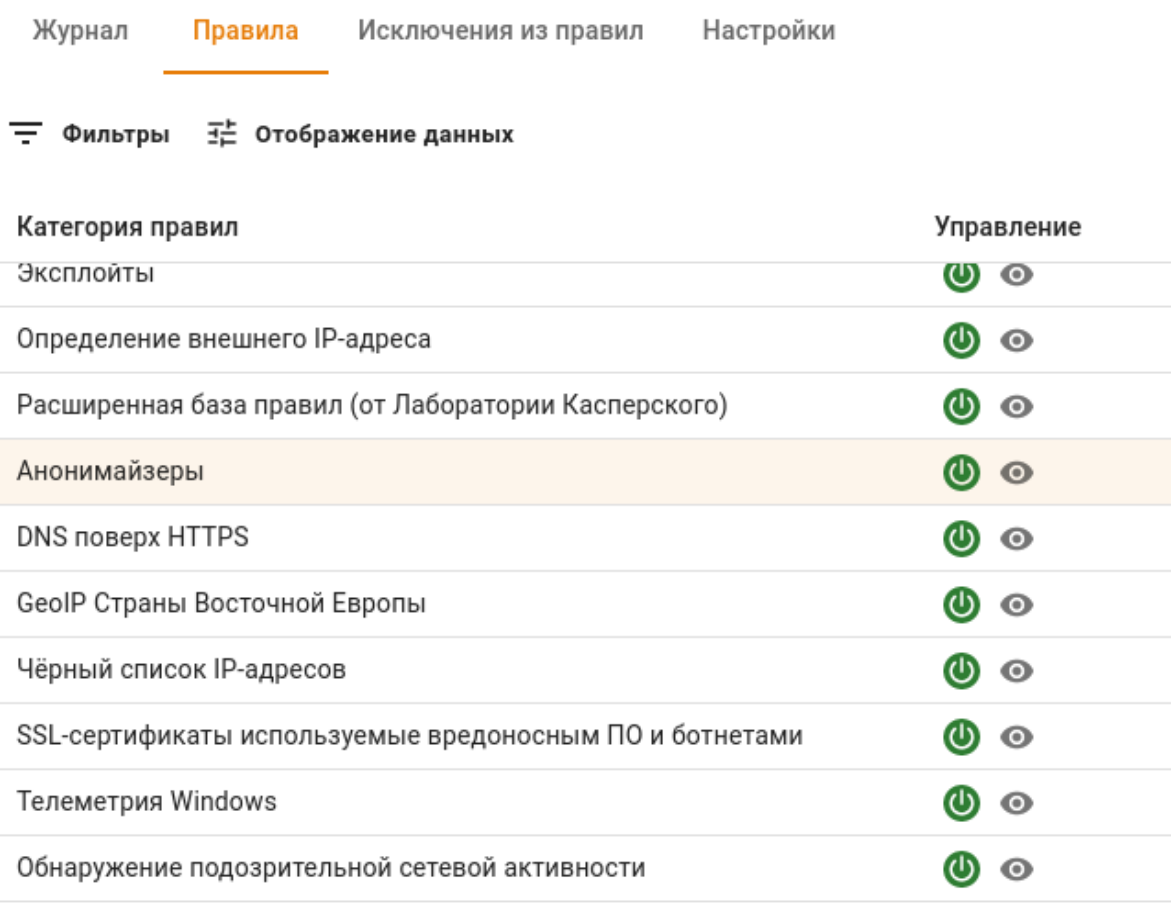
37.39.1 Как проверить, что заблокирует трафик первым: Контроль приложений или система Предотвращения вторжений?

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'.
```

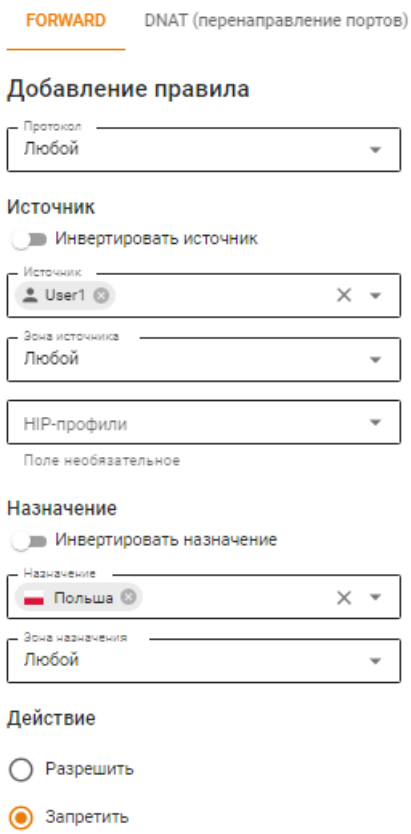
В **Правила трафика -> Предотвращение вторжений -> Журнал** записей о срабатывании правила **Анонимайзеры** нет. Значит, **Контроль приложений** обрабатывает трафик приоритетнее, чем система **Предотвращения вторжений**.

Подсказка: Подробнее о расшифровке передаваемых логов системы **Предотвращения вторжений** и **Контроля приложений** в статье *Syslog*.

37.39.2 Как проверить, что система Предотвращения вторжений обрабатывает трафик приоритетнее, чем Файрвол?

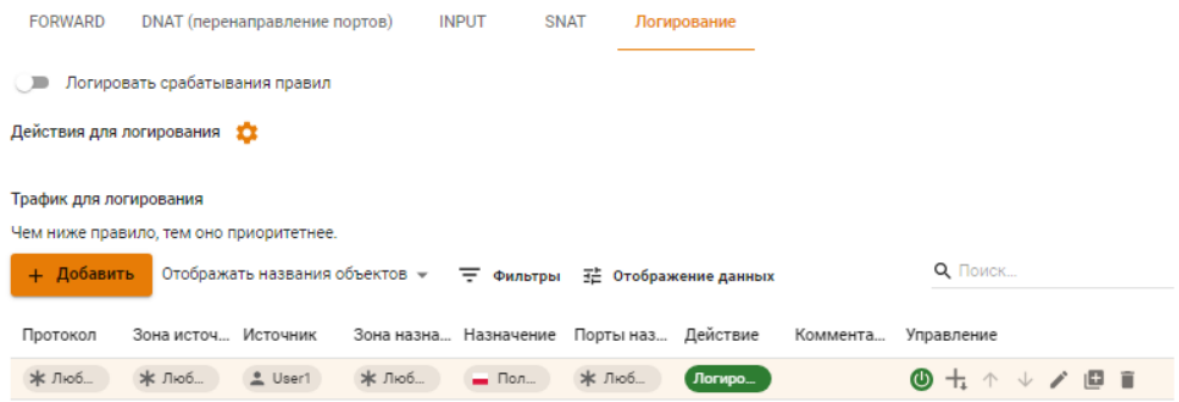
Для примера создайте GeoIP-правила для системы **Предотвращения вторжений** и **Файрвола**, блокирующие запросы к сайтам Польши.

1. В разделе **Правила трафика -> Файрвол** создайте правило, блокирующее запросы к сайтам Польши:

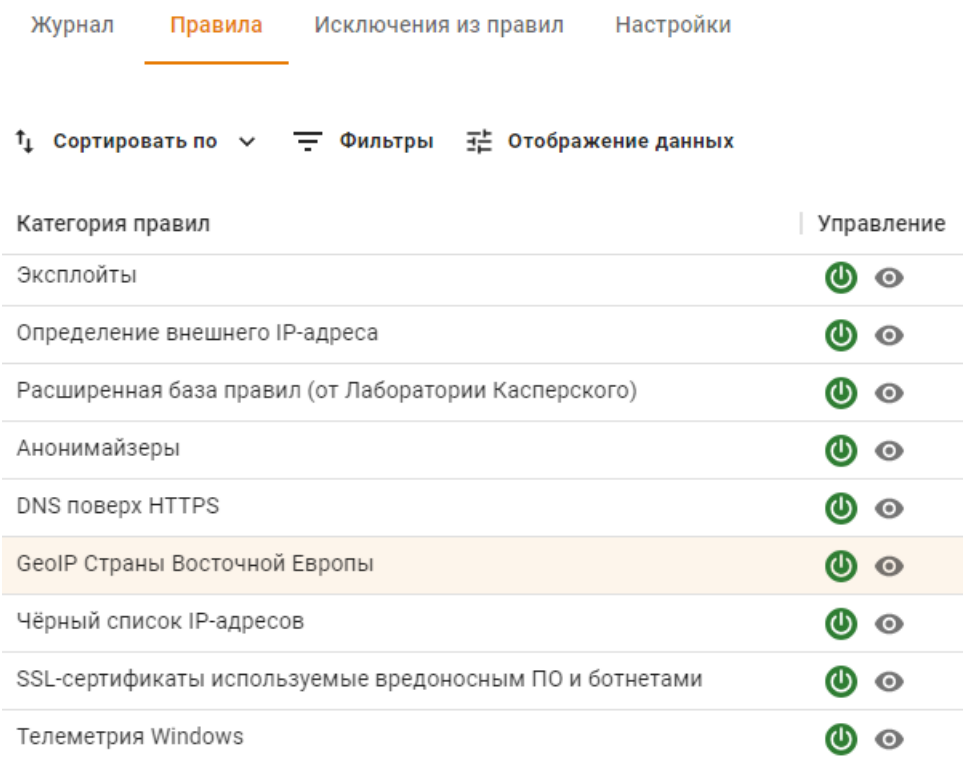


2. Переведите ползунок **Счетчик срабатываний** в **Отображении данных** в положение **Включен**, чтобы отследить, было ли срабатывание правила.

3. Перейдите на вкладку **Логирование**, создайте правило логирования:

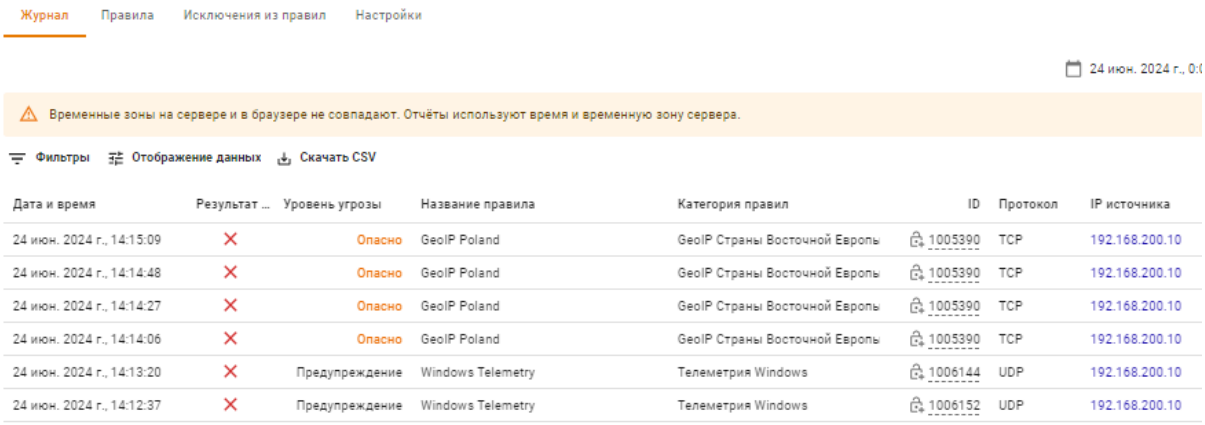


4. Проверьте, что в разделе **Предотвращения вторжений** включен блок правил блокировки стран Восточной Европы по GeoIP:



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:



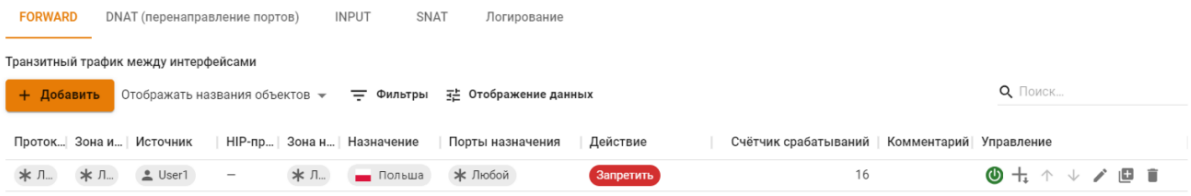
7. Перейдите в раздел **Файрвол** для просмотра счетчика срабатываний. Он должен быть равен нулю.

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**:



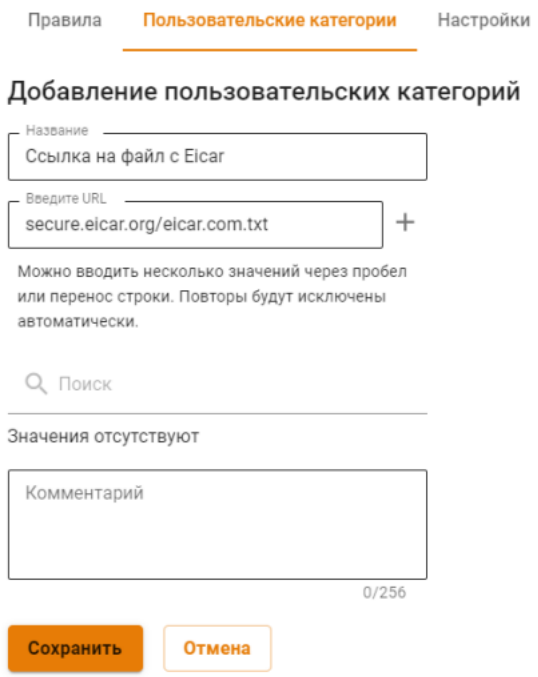
Система **Предотвращения вторжений** обрабатывает трафик приоритетнее, чем **Файрвол**.

37.39.3 Как проверить, что Контент-фильтр обрабатывает трафик приоритетнее, чем Антивирус веб-трафика?

Для примера использовался тестовый файл с Eicar, доступный для скачивания по ссылке.

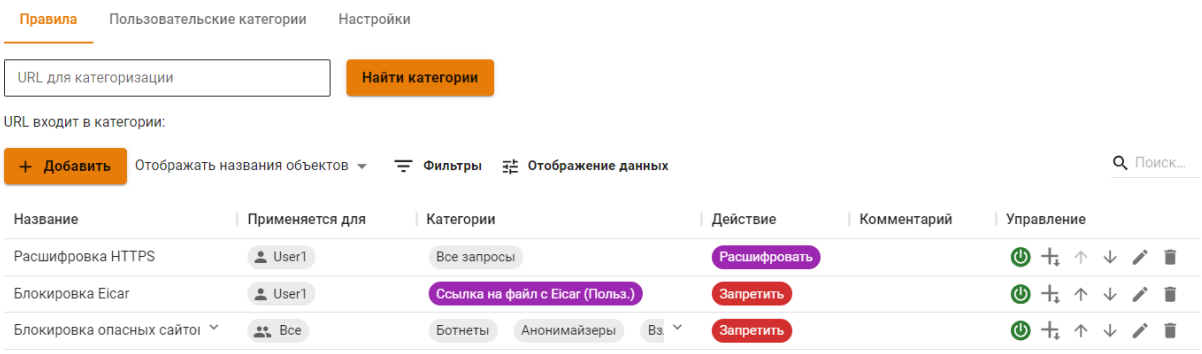
1. Перейдите в раздел **Правила трафика -> Контент фильтр -> Пользовательские категории**. Нажмите **Добавить**.

2. Введите ссылку на ресурс и нажмите + :



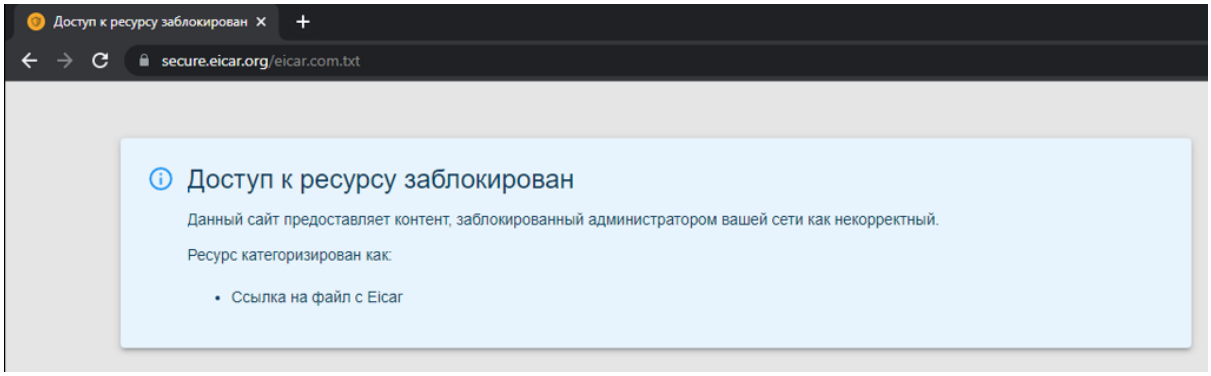
3. Перейдите на вкладку **Правила** и создайте два правила для **User1**:

- 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**.

37.40 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;

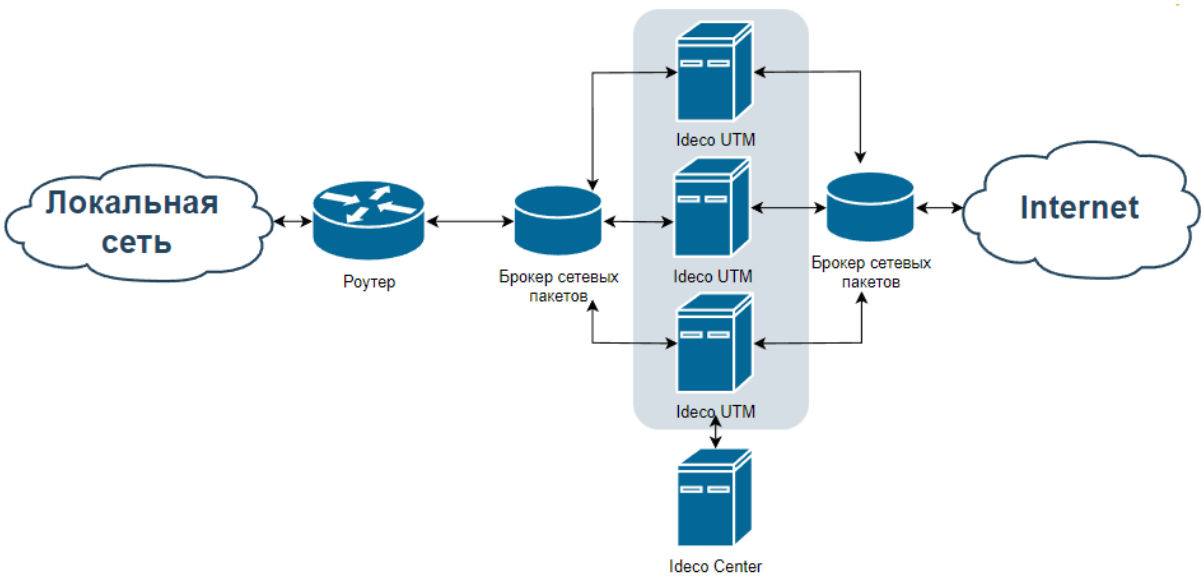
- Данные отчетности, логов и мониторинга не синхронизируются между нодами. В каждой ноде хранятся свои данные;
- Восстановление из бекапа и обновление системы будет затрагивать только одну ноду. Каждую ноду потребуется обновлять отдельно;
- Между локальной сетью и брокером сетевых пакетов потребуется 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».

37.40.1 Пример 1 - Два брокера, по одному со стороны локальной и внешней сетей



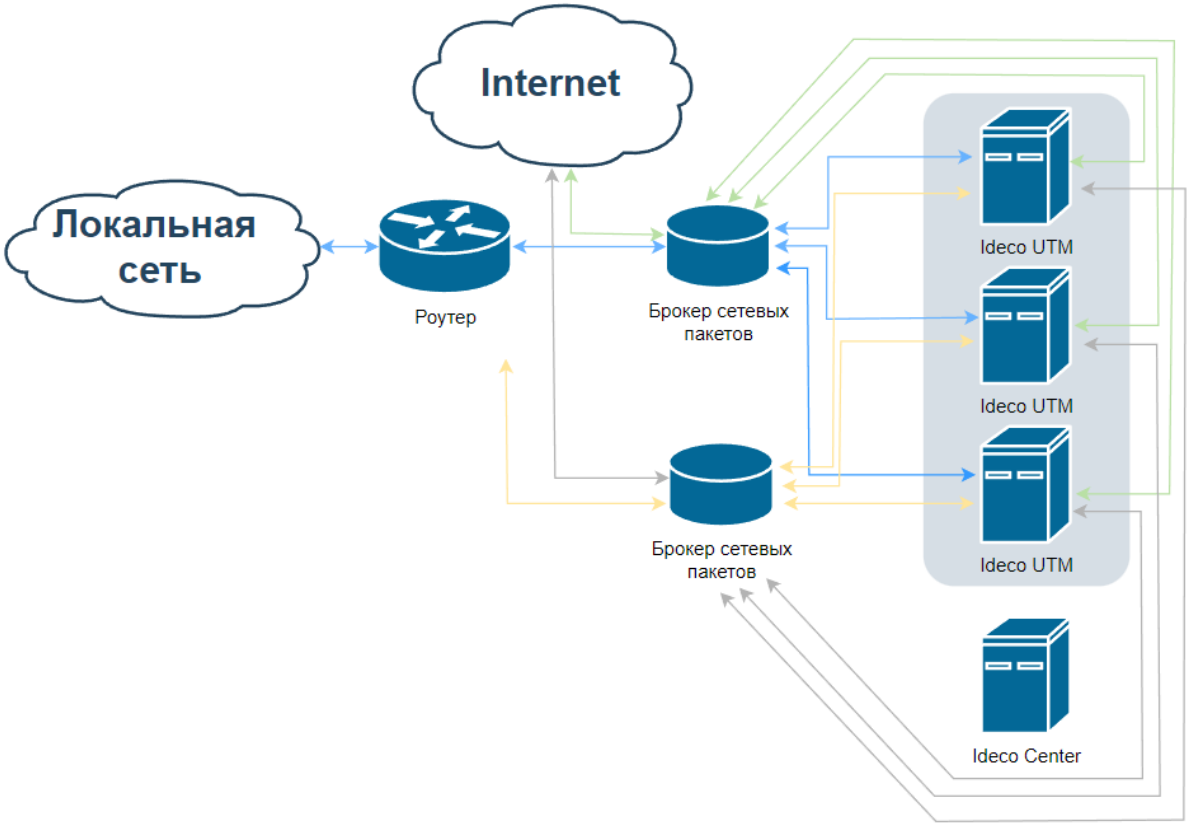
Настройка Ideco NGFW:

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.

37.40.2 Пример 2 - Основной и резервный брокеры, расположенные перед Ideco NGFW



Настройка Ideco NGFW

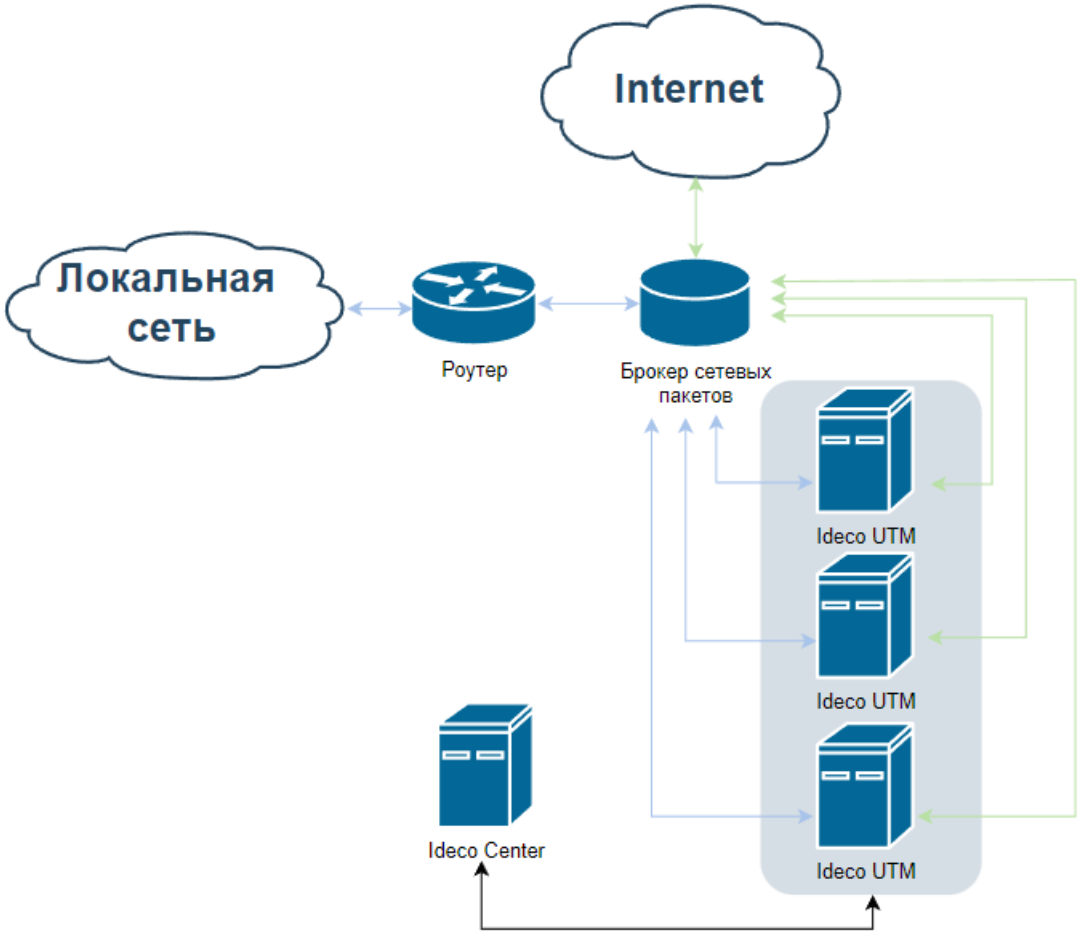
На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку *локального* и *внешнего* интерфейсов.

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.

37.40.3 Пример 3 - Один брокер, расположенный перед Ideco NGFW



Настройка Ideco NGFW

На каждом устройстве Ideco NGFW необходимо выполнить первоначальную настройку *локального* и *внешнего* интерфейсов.

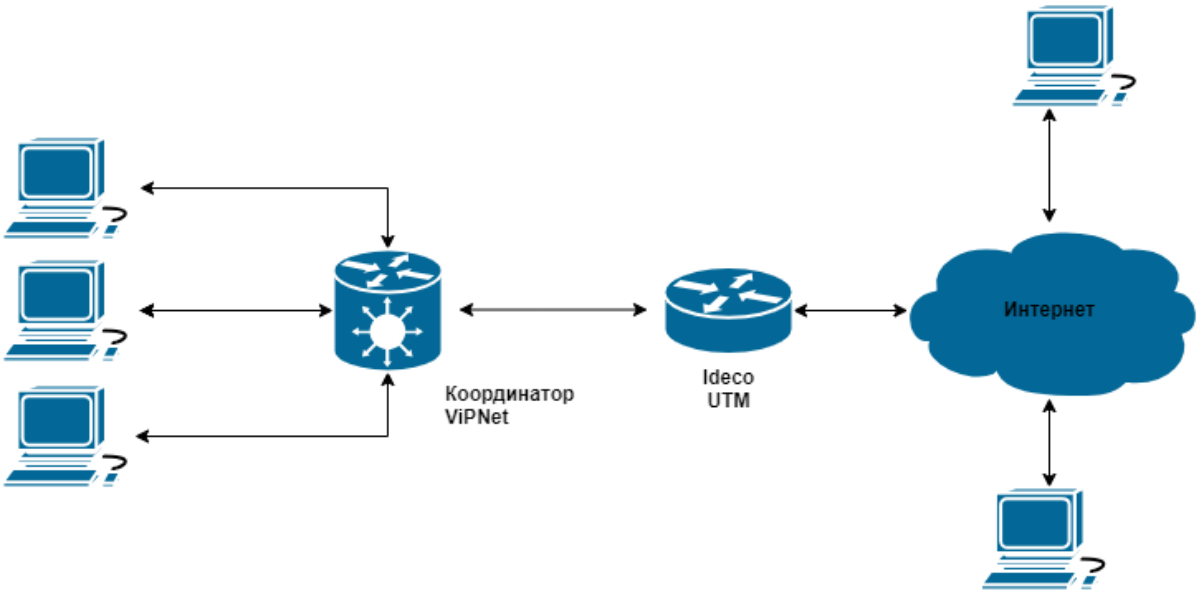
Брокер сетевых пакетов не имеет собственного IP-адреса. Поэтому:

- 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.

37.41 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:



37.41.1 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.

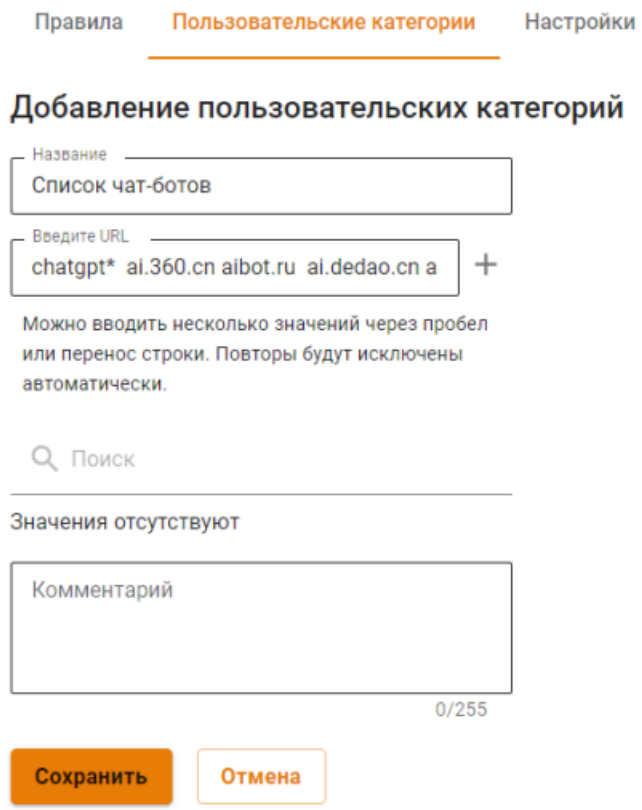
37.42 Блокировка чат-ботов

37.42.1 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 категорию, заполнив следующие поля:



- **Название** - введите любое название;
- **URL** - внесите список URL из блока ниже;
- **Комментарий** - заполнение не обязательно.

Список URL:

```
chatgpt*
ai.360.cn
aibot.ru
ai.dedao.cn
ai.ls
aiservice.vercel.app
aitianhu.com
anse.app
anthropic.com
b.ai-huan.xyz
bard.google.com
bard.google.com
bettergpt.chat
bing.com
bing.com
chadgpt.ru
character.ai
chat4gpt.ru
chat9.yqcloud.top
chat.acytoo.com
chataigpt.org
chat.ai-open.ru
chatboxai.app
chat.dfehub.com
chat.getgpt.world
```

(continues on next page)

(продолжение с предыдущей страницы)

```
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
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
```

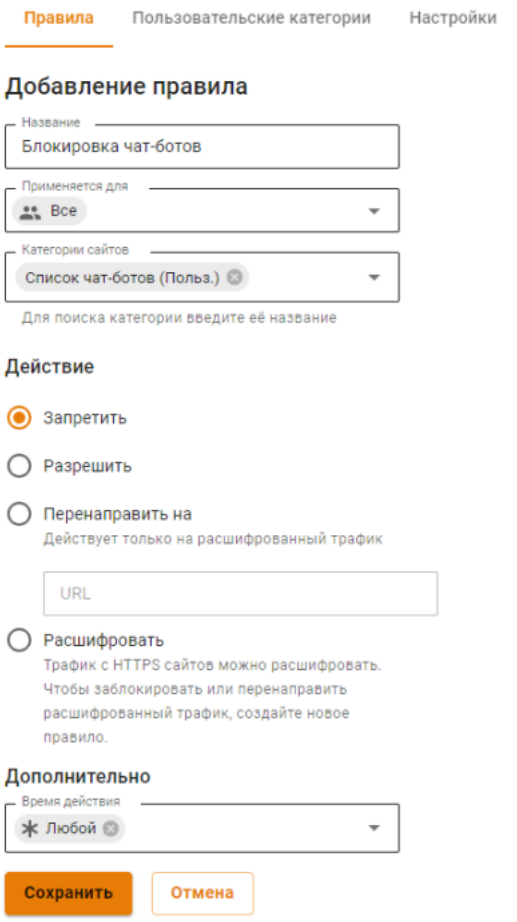
(continues on next page)

(продолжение с предыдущей страницы)

```
openai-gpt.ru
openai-chat-gpt.ru
open-assistant.io
opencat.app
petals.ml
play.vercel.ai
poe.com
ru-chatgpt.ru
rugpt.chat
sdk.vercel.ai
supertest.lockchat.app
tenchat.ru
theb.ai
timeai.ru
tongyi.aliyun.com
tools.zmo.ai
trychatgpt.ru
wewordle.org
xinghuo.xfyun.cn
yandex-gpt.com
yandex-gpt.ru
yiyan.baidu.com
you.com
zhpt.tech
```

4. Сохраните категорию.

3. Перейдите на вкладку **Правила** и добавьте правило с действием **Запретить**:



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

Подсказка:

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

37.43.1 Доступные из внешней сети

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

37.43.2 Доступные из локальной сети

37.44 Как включить таймер при загрузке Ideco NGFW

37.44.1 Основное

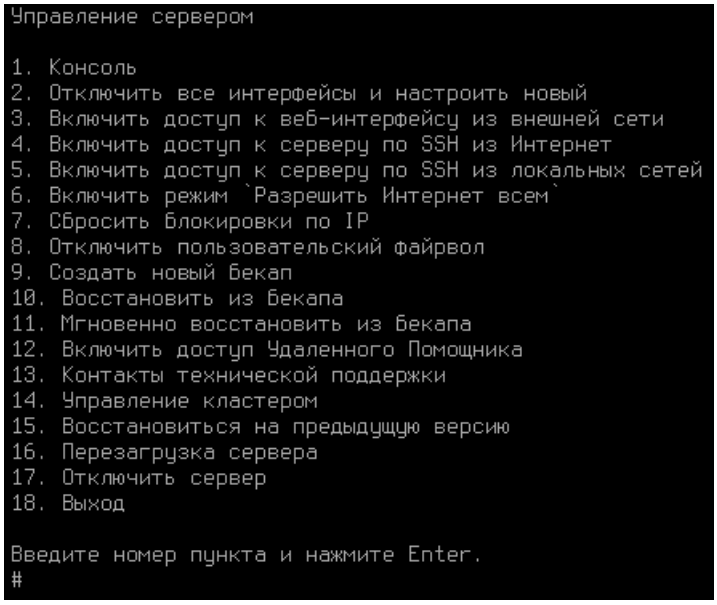
При отключении таймера также отключается автоматический выбор пункта меню. В этом случае система не загрузится сама после обновления, рестарта или переключения ноды в режиме кластеризации до момента нажатия **Enter**.

Для включения таймера выполните действия:

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



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



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



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

38. Диагностика проблем

38.1 Ошибка при открытии сайта ERR_CONNECTION_TIMED_OUT или Не открывается сайт

Перед проверкой модулей фильтрации NGFW убедитесь, что на работу сайта не влияют:

- технические проблемы на самом ресурсе;
- блокировка со стороны провайдера;
- некорректная работа устройства пользователя и т.д.

Откройте сайт с устройства вне локальной сети NGFW. Например, со смартфона через мобильный интернет. Если сайт доступен, перейдите в веб-интерфейс NGFW.

Подсказка: Для определения модуля фильтрации, блокирующего сайт, можно проверить логи в разделах *Системный журнал* и *Syslog*. Это может помочь определить причину возникшей проблемы и более точно ее диагностировать.

38.1.1 Шаг 1. Проверьте, открывается ли сайт в режиме Разрешить интернет всем

1. Нажмите на  в верхней правой части веб-интерфейса NGFW.

2. Переведите опцию **Разрешить интернет всем** в положение **Включен**:

3. Откройте сайт.

Если сайт не открывается, проверьте, откроется ли сайт на другом устройстве с того же IP-адреса:

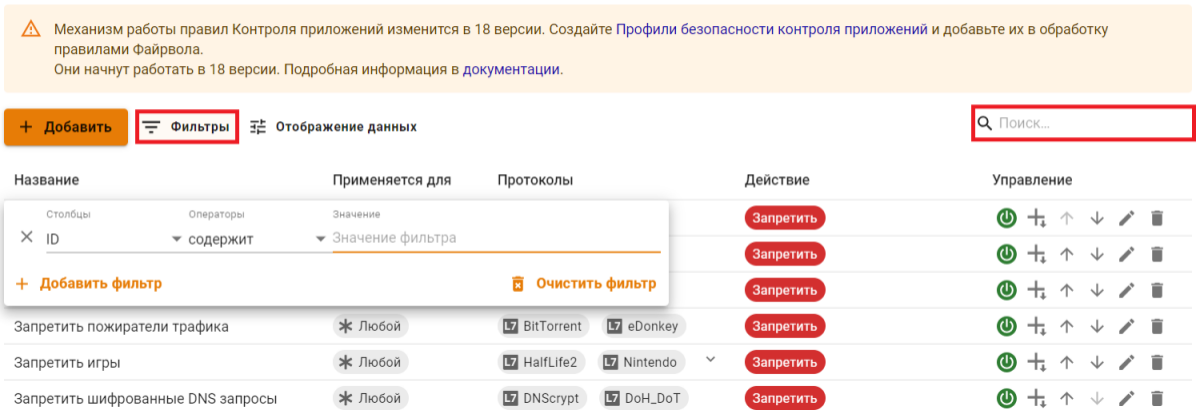
- Если не открывается, рекомендуем обратиться к провайдеру. Скорее всего, провайдер блокирует IP-адрес или адрес сайта;
- Если сайт открывается, проверьте настройки устройства пользователя.

38.1.2 Шаг 2. Проверьте, не блокирует ли сайт модуль Контроль приложений

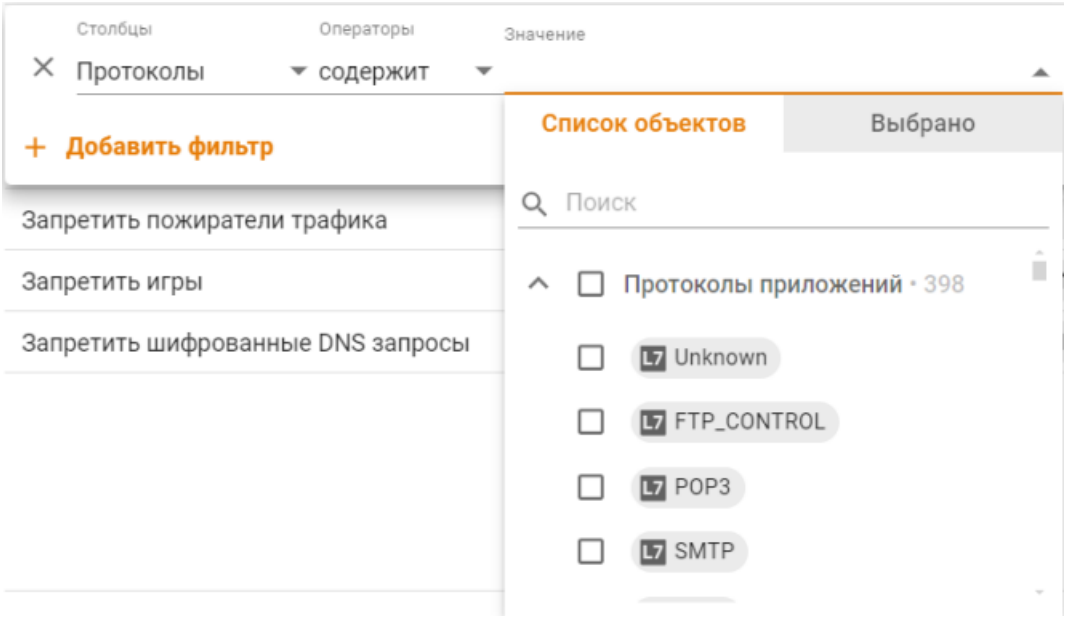
Если сайт входит в *перечень* протоколов и сервисов, доступных для создания правил **Контроля приложений**, выполните действия:

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**:

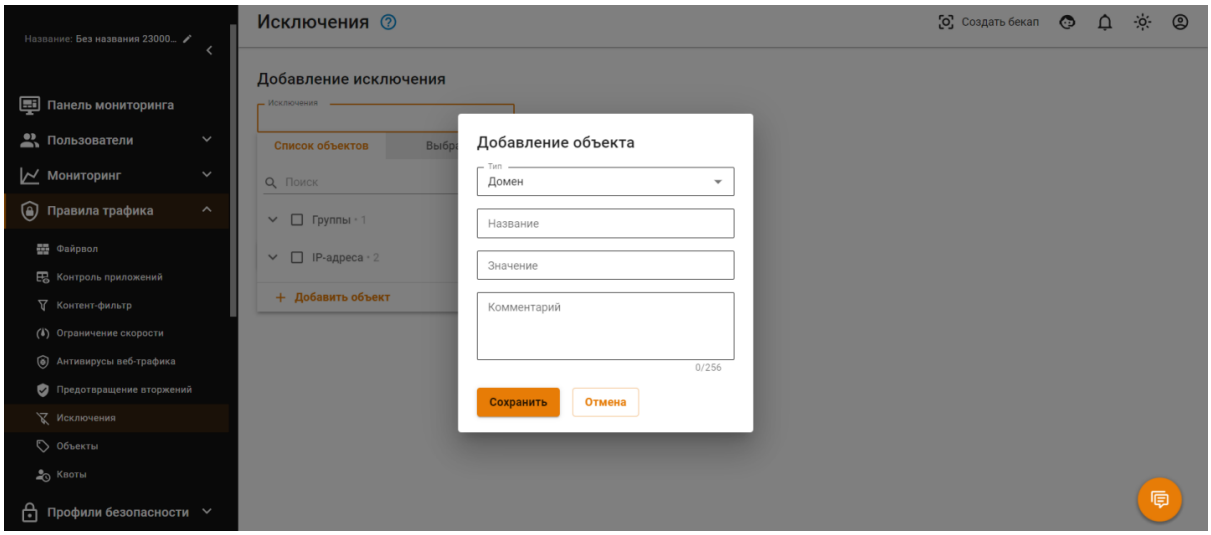


3. В настройках фильтрации выберите столбцы **Протоколы**, в поле **Значение** выберите нужный протокол приложения:



4. Проверьте, блокируют ли сайт найденные правила (действие **Запретить**).

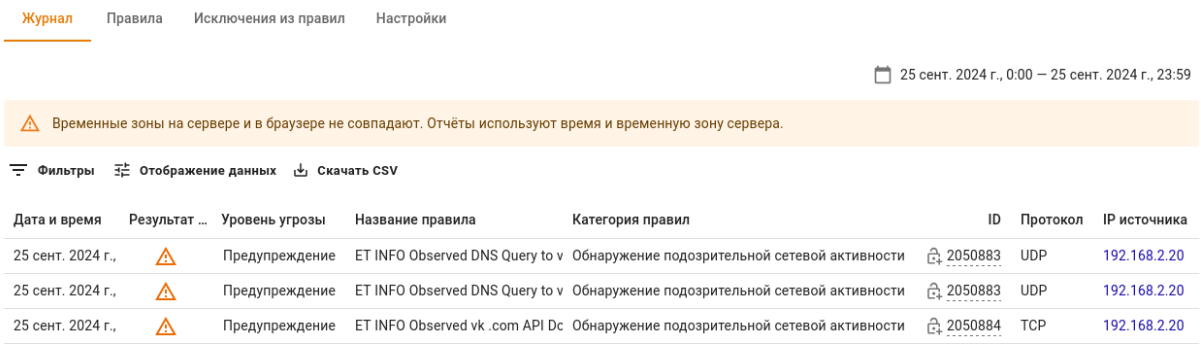
5. Если сайт блокируется правилом **Контроля приложений**, отредактируйте правило или добавьте сайт в исключения в разделе **Правила трафика ->** ***Исключения***:



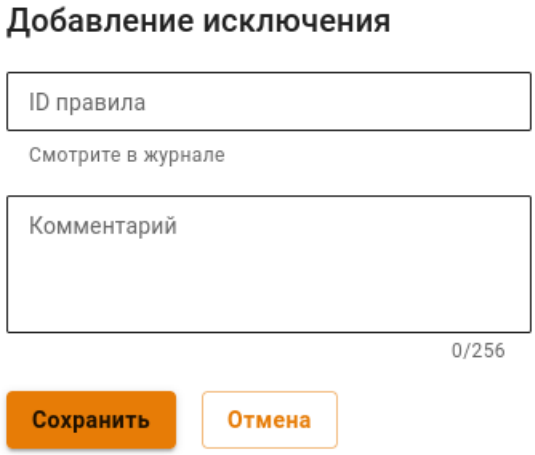
38.1.3 Шаг 3. Проверьте, не блокирует ли сайт система Предотвращения вторжений

1. Повторите попытку входа на сайт с устройства пользователя.

2. Перейдите в раздел **Правила трафика -> Предотвращение вторжений -> Журнал**, найдите в логах ID блокирующего правила:



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**:

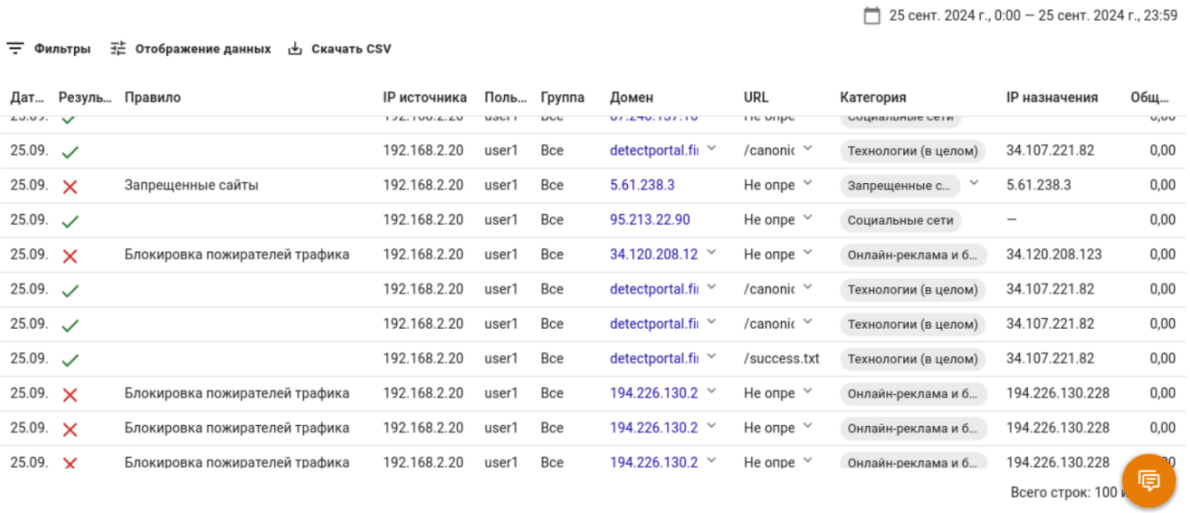


Также можно добавить IP-адрес сайта в исключения по *инструкции*.

38.1.4 Шаг 4. Проверьте, не блокируется ли сайт правилом Контент-фильтра

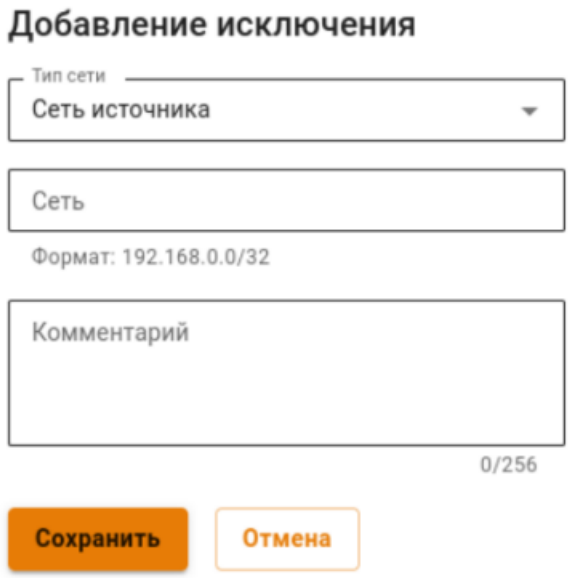
1. Откройте сайт с устройства пользователя.

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.

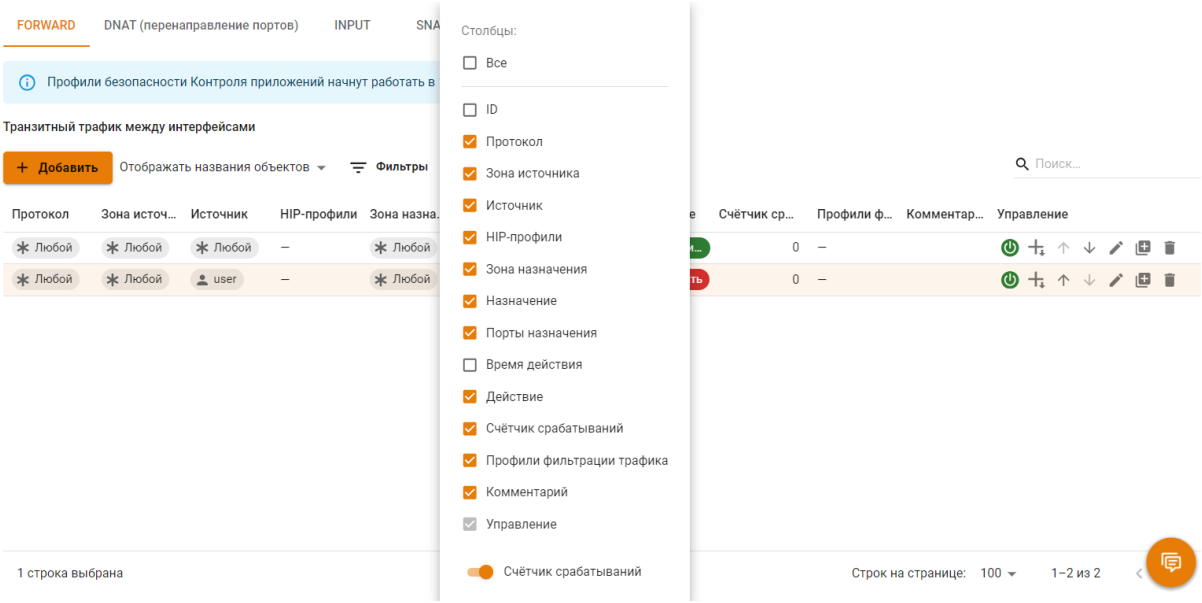
38.1.5 Шаг 5. Проверьте, не блокируется ли сайт правилом Файрвола

Найдите блокирующее правило одним из способов:

Первый способ. Счетчик срабатываний:

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

2. Нажмите на **Отображение данных** и включите **Счетчик срабатываний**:



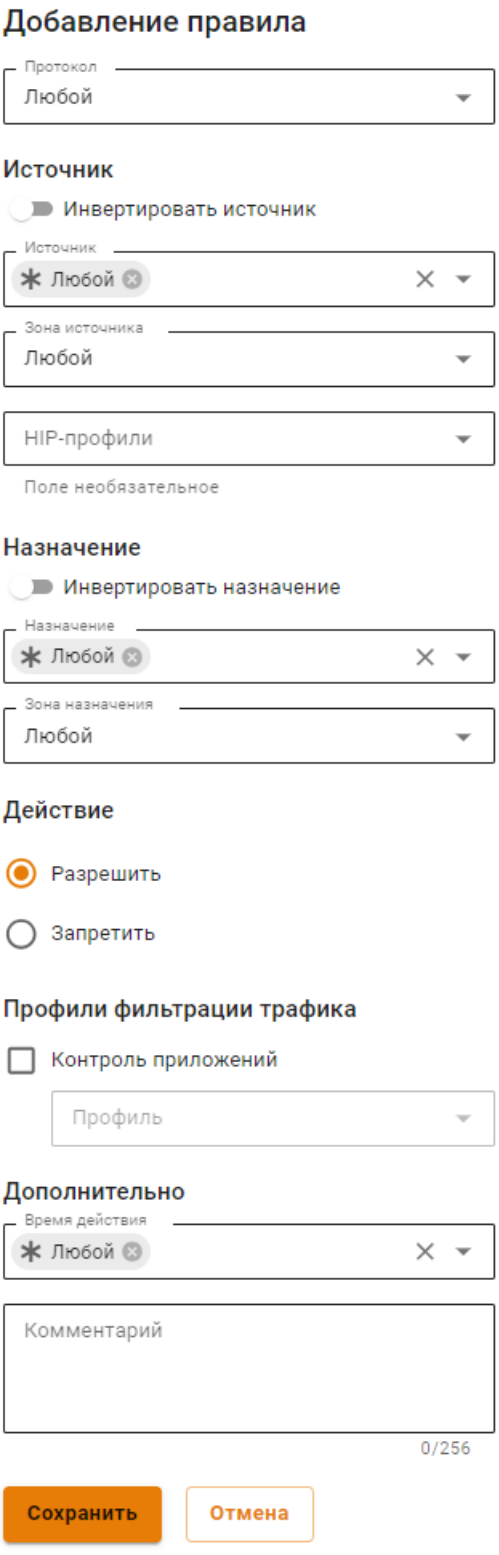
3. Откройте сайт с устройства пользователя.

4. Найдите в таблице FORWARD правило с заметным увеличением количества срабатываний.

Второй способ. Тестовое правило:

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

2. Создайте тестовое правило, разрешающее любой трафик:



3. Правило добавится в конец таблицы. Поместите созданное правило на одну позицию вверх, нажав на кнопку ↑.

4. Откройте сайт с устройства пользователя.

5. Если сайт не открывается, поднимите тестовое правило на позицию выше и повторно откройте сайт с устройства пользователя. Повторяйте эти действия до тех пор, пока сайт не откроется.

6. Если сайт открывается, блокирующее правило расположено ниже тестового.

Если сайт блокируется правилом **Файрвола**, измените его настройки.

38.1.6 Шаг 6. 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.

38.1.7 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.

38.2 Что делать если не работает интернет

38.2.1 Шаг 1. Проверить параметры пользователя

Убедитесь, что проверяемый пользователь авторизован на сервере. Возможные состояния пользователя описаны в главе *Дерево пользователей*.

38.2.2 Шаг 2. Проверка компьютера пользователя

Выполните команду `ping` с компьютера пользователя до адреса `8.8.8.8`: **Пуск -> Выполнить**, введите команду `cmd`, в появившемся окне введите `ping 8.8.8.8`.

1. Если адрес `8.8.8.8` отвечает на эхо-запросы, проверяем `ping ya.ru`;

2. Если адрес `8.8.8.8` не отвечает на эхо-запросы, перейдите к Шагу 3;

3. Если адрес `ya.ru` отвечает на эхо-запросы, перейдите к Шагу 5;

4.Если появилось сообщение **Не удалось обнаружить узел ya.ru**, то, возможно, не работает DNS-провайдер, проверьте командой `nslookup ya.ru 222.222.222.222`, вместо `222.222.222.222` укажите DNS адрес провайдера:

- Если ответа нет - обратитесь к провайдеру;

- Если ответ есть, проверьте адрес первичного DNS на вашем компьютере (должен быть указан локальный адрес Ideco NGFW). Проверьте также, что DNS-сервер работает на Ideco NGFW в разделе **Сервисы -> DNS**.

38.2.3 Шаг 3. Проверка доступа к интернету на сервере

Зайдите в раздел **Терминал** в веб-интерфейсе: выполните команду `ping 8.8.8.8`, для остановки `ctrl+c`.

Если ping не проходит:

1. Проверьте настройки сервера, адреса и маски интерфейсов;

2. Убедитесь, что используемое вами сетевое оборудование является исправным, сетевые кабели правильно обжаты, а также не имеют изломов и обрывов, проверьте индикатор сигнала на сетевой карте (его можно посмотреть в разделе **Сервисы -> Сетевые интерфейсы**), перезагрузите коммутатор и модем (если используется);

3. Если используется подключение по Ethernet, то необходимо выполнить команду `ip neigh | grep <адрес_шлюза_провайдера>`. Если MAC-адрес шлюза провайдера не определился, то имеет смысл попробовать перезагрузить Сервер, переподключив сетевой кабель. После этого проверить наличие MAC-адреса шлюза провайдера. Такое решение помогает, если «подвисает» порт коммутатора провайдера. Если после указанной меры MAC шлюза провайдера не появился в таблице MAC-адресов, обратитесь к провайдеру. Следует отметить, что при смене сетевого оборудования отсутствие доступа к интернету может быть обусловлено использованием вашим интернет-провайдером привязки по MAC-адресу.

Если ping проходит, перейдите к Шагу 4.

38.2.4 Шаг 4. Проверка файрвола

1. Отключите модуль **Файрвол** в разделе веб-интерфейса **Правила трафика -> Файрвол**. Если веб-интерфейс недоступен, то файрвол можно выключить с помощью локального меню;

2. Если доступ к интернету появился, найти правило, запрещающее доступ к сети, в файрволе, поочередно включая правила;

3. Если ничего не помогло, перейдите к следующему шагу.

38.2.5 Шаг 5. Проверка работы веб-трафика

Если пользователь получает ответы на эхо-запросы командой `ping` и по доменному имени, и по IP-адресу, но при этом веб-трафик отсутствует:

1. Проверьте, что в браузере отсутствуют все настройки прокси;

2. Выключите временно файрвол Windows и антивирусное ПО;

3. Если ничего не помогло, перейдите к Шагу 6.

38.2.6 Шаг 6. Если вам не удалось решить проблему

1. Сделайте скриншоты вкладки **Основное** у пользователя в развернутом виде и создайте обращение на портале поддержки или напишите письмо на support@ideco.ru.

2. Включите *режим удаленного помощника* и обратитесь в службу технической поддержки: https://ideco.ru/tekhnicheskaya-podderzhka.

38.3 Ошибка при авторизации «The browser is outdated»

38.3.1 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**.

38.4 Если соединение по IPsec не устанавливается

38.4.1 Основное

1. Перезагрузите сервисы двух NGFW, выполнив команду `systemctl restart ideco-ipsec-backend.service && systemctl restart strongswan.service`.

2. Проверьте работоспособность перезагруженных сервисов:

- выполните команду `systemctl status strongswan.service`;
- перейдите в раздел **Сервисы -> IPsec**.

Если при переходе в раздел IPsec и выполнении команды возникли ошибки, то перейдите к пункту 3.

3. Пересоздайте соединение из веб-интерфейса по инструкции *Настройка подключения между Филиалом и Главным офисом*.

Если пересоздание соединения не помогло, перейдите к пункту 4.

4. Проверьте, ходит ли трафик по портам 500 и 4500, выполнив команды `tcpdump -i any port 4500 -ttttnnn` и `tcpdump -i any port 500 -ttttnnn` в головном офисе и филиале.

Если трафик уходит с одного NGFW и приходит на второй NGFW, то обратитесь в *техническую поддержку*.
Если трафик уходит с одного NGFW и не приходит на второй NGFW, обратитесь к провайдеру.

39. Описание основных хендлеров

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Авторизация:

```
POST /web/auth/login
```

Json-тело запроса:

```
{
    "login": "string",
    "password": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "rest_path": "string",
}
```

- `login` - логин, каталог администратора указывается после `@`. Примеры:
  - `admin` - локальный админ, без `@`;
  - `admin@ad_domain.ru` - AD/ALD администратор;
  - `admin@radius` - для RADIUS-администраторов `@radius`.
- `password` - пароль;
- `rest_path` - префикс URL, на который выставлять cookie. Например, `/` или `/rest`.

Ответ на успешный запрос: 200 OK

После успешной авторизации сервер Ideco NGFW передает в заголовках куки. Пример значений:

```
set-cookie: insecure-ideco-session=02428c1c-fcd5-42ef-a533-5353da743806
set-cookie: __Secure-ideco-3ea57fca-65cb-439b-b764-d7337530f102=df164532-b916-4cda-
↪a19b-9422c2897663:1663839003
```

Эти куки нужно передавать при каждом запросе после авторизации в заголовке запроса Cookie.

Разавторизация администратора:

```
DELETE /web/auth/login
```

Ответ на успешный запрос: 200 OK

После успешной разавторизации сервер Ideco NGFW передает в заголовках куки. Пример значений:

```
set-cookie: insecure-ideco-session=""; expires=Thu, 01 Jan 1970 00:00:00 GMT; Max-
↪Age=0; Path=/
set-cookie: __Secure-ideco-b7e3fb6f-7189-4f87-a4aa-1bdc02e18b34=""; HttpOnly; Max-
↪Age=0; Path=/; SameSite=Strict; Secure
```

Добавление правила авторизации:

```
POST /auth/rules
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "ip": "string" | "null",
    "mac": "string" | "null",
    "user_id":  "integer",
    "always_logged": "boolean",
    "comment": "string"
}
```

- `enabled` - `true` для включения правила, `false` для выключения;
- `ip` - IP-адрес, который нужно авторизовать;
- `mac` - MAC-адрес, который нужно авторизовать;
- `always_logged` - авторизован всегда. Может быть включено только при указанном IP;
- `user_id` - идентификатор пользователя, к которому будет применено правило;
- `comment` - комментарий к правилу, может быть пустым, максимальная длина - 255 символов.

Ответ на успещный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного правила.

Измененение части правила авторизации:

```
PATCH /auth/rules/<id правила>
```

```
{
    "enabled": "boolean",
    "ip": "string" | "null",
    "mac": "string" | "null",
    "user_id":  "integer",
    "always_logged": "boolean",
    "comment": "string"
}
```

- `enabled` - `true` для включения правила, `false` для выключения;
- `ip` - IP-адрес, который нужно авторизовать;
- `mac` - MAC-адрес, который нужно авторизовать;
- `always_logged` - авторизован всегда. Может быть включено только при указанном IP;
- `user_id` - идентификатор пользователя, к которому будет применено правило;
- `comment` - комментарий к правилу, может быть пустым, максимальная длина - 255 символов.

Ответ на успещный запрос: 200 OK

Удаление правила авторизации:

```
DELETE /auth/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

Сбор анонимной статистики о работе сервера:

39.1 Получение текущих настроек:

```
GET /gather_stat/settings
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - если `true`, то сбор анонимной статистики о работе сервера включен, `false` - выключен.

39.2 Изменение настроек

```
PUT /gather_stat/settings
```

Json-тело запроса

```
{
    "enabled": "boolean"
}
```

Ответ на успешный запрос: 200 OK

39.3 Лицензирование

Регистрация сервера:

```
POST /license/register
```

Json-тело запроса:

```
{
    "token": "string"
}
```

- `token` - получить токен лицензии можно в отделе продаж, он высылается в активационном письме;

Ответ на успешный запрос: 200 OK

Чтобы добавить enterprise-demo лицензию, необходимо сначала получить токен лицензии в личном кабинете. Для этого выполните действия:

1. Авторизуйтесь в личном кабинете myideco.ru:

```
POST /20250424123235/docsUTM/api/v3/login
```

Json-тело запроса:

```
{
    "login": "string",
    "password": "string",
    "g_recaptcha_response": "string" | "null"
}
```

2. Выполните запрос на регистрацию сервера:

```
PUT /20250424123235/docsUTM/api/v3/<company_id>/go_to_product
```

- `company_id` - идентификатор компании пользователя, его можно получить по запросу `GET /20250424123235/docsUTM/api/v3/companies`.

Ответ на успешный запрос:

```
{
    "token": "string"
}
```

Используйте полученный токен в теле запроса при регистрации Ideco NGFW.

Получение информации о лицензии:

```
GET /license/info
```

Пример ответа на успешный запрос:


```
{
    "modules": {
        "active_directory": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "kaspersky_av_for_web": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "kaspersky_av_for_mail": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "application_control": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "suricata": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "advanced_content_filter": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "standard_content_filter": {
            "available": false,
            "expiration_date": 0
        },
        "ips_advanced_rules": {
            "available": true,
            "expiration_date": 1712400382.0
        },
        "icsd": {
            "available": true,
            "max_users_count": 10000
        }
    },
    "general": {
        "available": true,
        "reason": "",
        "not_upgrade_after": 1712400382.0,
        "tech_support_end": 1712400382.0,
        "start_date": 1708944382.2658572,
        "expiration_date": 1712400382.0
    },
    "license_type": "enterprise-demo",
    "license_id": "UTM-3883264353",
    "server_name": "UTM",
    "last_update_time": 1708944385.1747465,
    "company_id": "Ideco",
    "server_id": "OQHsviy10sEOOQXWs-8c7tnwJb4AaOvplT2iJc-im677",
```


(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"
}
```

Получение информации о механизме обновления лицензии:

```
GET /license/update-type
```

Ответ на успешный запрос:

```
{
    "update_type": "auto" | "manual"
}
```

- `auto` - при автоматическом получении лицензии;
- `manual` - при ручной загрузке лицензии.

Изменение механизма обновления лицензии:

```
PUT /license/update-type
```

Json-тело запроса:

```
{
    "update_type": "auto" | "manual"
}
```

Ответ на успешный запрос: 200 OK

Получение ссылки для офлайн-регистрации:

```
GET /license/license-get-offline-registration-url
```

Ответ на успешный запрос:

```
{
    "registration_url": "https://my.ideco.ru/offline_register?server_
↪name=ZGF0YSB0byBiZSBlbmNvZGVk&hwid=u-CVv6SSNMXI_Mukgnf3SCIxJz9kcl0i50ARFk4FRz10&
↪version=17.1"
}
```

- `server_name` - имя сервера Ideco NGFW;
- `hwid` - HWID сервера;
- `version` - версия сервера.

Получение ссылки для офлайн-регистрации сервера возможно только при ручном механизме обновления лицензии.

Загрузка файла с лицензией на NGFW:

```
POST /license/license-upload
```

Тело запроса: форма загрузки файла, имя поля в форме загрузки файла `license_file`

Ответ на успешный запрос: 200 OK

39.4 Управление объектами

Получение идентификаторов объектов:

```
GET /aliases/<название обьекта> | all
```

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` - IPsec-интерфейсы;
- `interface.local_any` - все локальные интерфейсы;

- `interface.tunnel_any` - все туннельные интерфейсы;
- `group.id.` - идентификатор группы пользователей;
- `interface.id.`- идентификатор конкретного интерфейса;
- `interface.utm_outgoing` - исходящий трафик устройства;
- `interface.vpn_traffic` - клиентский VPN-трафик;
- `interface.wccp_gre_any` - все WCCP GRE интерфейсы;
- `hip_profile.id.` - устройства без профиля;
- `security_group.guid.` - идентификатор группы безопасности AD;
- `user.id.` - идентификатор пользователя;
- `domain.id.` - идентификатор домена;
- `ip.id.` - идентификатор IP-адреса;
- `ip_range.id.` - идентификатор объекта *Диапазон адресов*;
- `address_list.id.` - идентификатор объекта *Список IP-объектов*;
- `list_of_iplists.id.` - идентификатор объекта *Список стран*;
- `port_list.id.` - идентификатор объекта *Порты*;
- `time_list.id.` - идентификатор объекта *Расписание*;
- `subnet.id.` - идентификатор объекта *Подсеть*;
- `port_range.id.` - идентификатор объекта *Диапазон портов*;
- `port.id.` - идентификатор объекта *Порт*;
- `time_range.id.` - идентификатор объекта *Время*.

39.4.1 Создание обьектов

Создание объекта IP-адрес:

```
POST /aliases/ip_addresses
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;
- `value` - IP-адрес в формате `192.168.0.0`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта IP-адрес.

Создание объекта Диапазон IP-адресов:

```
POST /aliases/ip_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "string",
    "end": "string"
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;
- `start` - первый IP-адрес в диапазоне, например, `192.168.100.2`;
- `end` - последний IP-адрес в диапазоне, например, `192.168.100.15`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Диапазон IP-адресов.

Создание объекта Подсеть:

```
POST /aliases/networks
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - адрес подсети в формате `192.168.0.0/24` либо `192.168.0.0/255.255.255.0`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Подсеть.

Создание объекта Домен:

```
POST /aliases/domains
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - домен в формате mydomain.com.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Домен.

Создание объекта Порт:

```
POST /aliases/ports
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - номер порта в формате `8080`.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Порт.

Создание объекта Диапазон портов:

```
POST /aliases/port_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "integer",
    "end": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `start` - первый порт в диапазоне, например, 8080;
- `end` - последний порт в диапазоне, например, 8090.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Диапазон портов.

Создание объекта Время:

```
POST /aliases/time_ranges
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "weekdays": [ "integer" ],
    "start": "string",
    "end": "string",
    "period": {
            "first": "integer",
            "last": "integer"
        }
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;
- `weekdays` - список дней недели, где 1-пн, 2-вт . . . 7-вс;
- `start` - начало временного отрезка в формате `ЧЧ:ММ`;
- `end` - конец временного отрезка в формате `ЧЧ:ММ`;
- `first` - момент начала срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240215000000`;
- `last` - момент окончания срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240229235959`.

Если для `period` установить значение `null`, у объекта будет включена опция **Бессрочно**.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Время.

Создание объекта Список IP-объектов:

```
POST /aliases/lists/addresses
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;

- value - идентификаторы IP-объектов, через запятую.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- id - идентификатор объекта Список IP-объектов.

Создание объекта Список IP-адресов:

```
POST /aliases/ip_address_lists
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- title - название объекта, максимальная длина - 42 символа;
- comment - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- value - список IP-адресов без указания маски, либо с указанием маски подсети в виде десятичного числа 0. . . 32 или четырех десятичных чисел от 0 до 255. Например: 192.168.0.0, 192.168.0.0/24 или 192.168.0.0/255.255.255.0.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- id - идентификатор объекта Список IP-адресов.

Создание объекта Порты:

```
POST /aliases/lists/ports
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- title - название объекта, максимальная длина - 42 символа;
- comment - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- value - список портов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- id - идентификатор объекта Порты.

Создание объекта Расписание:

```
POST /aliases/lists/times
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;
- `value` - список идентификаторов объектов Время.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор объекта Расписание.

39.4.2 Изменение обьектов

Изменение объекта IP-адрес:

```
PUT /aliases/ip_addresses/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - IP-адрес в формате `192.168.0.0`.

Ответ на успешный запрос: 200 OK

Изменение объекта Диапазон IP-адресов:

```
PUT /aliases/ip_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "string",
    "end": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;

- `start` - первый IP-адрес в диапазоне, например, `192.168.100.2`;
- `end` - последний IP-адрес в диапазоне, например, `192.168.100.15`.

Ответ на успешный запрос: 200 OK

Изменение объекта Подсеть:

```
PUT /aliases/networks/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - адрес подсети в формате `192.168.0.0/24` либо `192.168.0.0/255.255.255.0`.

Ответ на успешный запрос: 200 OK

Изменение объекта Домен:

```
PUT /aliases/domains/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "string"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - домен в формате mydomain.com.

Ответ на успешный запрос: 200 OK

Изменение объекта Порт:

```
PUT /aliases/ports/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "value": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - номер порта в формате 8080.

Ответ на успешный запрос: 200 OK

Изменение объекта Диапазон портов:

```
PUT /aliases/port_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "start": "integer",
    "end": "integer"
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `start` - первый порт в диапазоне, например, 8080;
- `end` - последний порт в диапазоне, например, 8090.

Ответ на успешный запрос: 200 OK

Изменение объекта Время:

```
PUT /aliases/time_ranges/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "weekdays": [ "integer" ],
    "start": "string",
    "end": "string",
    "period": {
            "first": "integer",
            "last": "integer"
        }
}
```

- `title` - название объекта. Максимальная длина - 42 символа;
- `comment` - комментарий к объекту. Может быть пустым, максимальная длина - 255 символов;
- `weekdays` - список дней недели, где 1-пн, 2-вт . . . 7-вс;
- `start` - начало временного отрезка в формате `ЧЧ:ММ`;
- `end` - конец временного отрезка в формате `ЧЧ:ММ`;
- `first` - момент начала срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240215000000`;
- `last` - момент окончания срока действия в формате `ГГГГММДДЧЧММСС`, например, `20240229235959`.

Если для `period` установить значение `null`, у объекта будет включена опция **Бессрочно**.

Ответ на успешный запрос: 200 OK

Изменение объекта Список IP-объектов:

```
PUT /aliases/lists/addresses/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - идентификаторы IP-объектов, через запятую.

Ответ на успешный запрос: 200 OK

Изменение объекта Список IP-адресов:

```
PUT /aliases/ip_address_lists/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список IP-адресов без указания маски, либо с указанием маски подсети в виде десятичного числа 0. . . 32 или четырех десятичных чисел от 0 до 255. Например: `192.168.0.0`, `192.168.0.0/24` или `192.168.0.0/255.255.255.0`.

Ответ на успешный запрос: 200 OK

Изменение объекта Порты:

```
PUT /aliases/lists/ports/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список портов.

Ответ на успешный запрос: 200 OK

Изменение объекта Расписание:

```
PUT /aliases/lists/times/<id объекта>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "values": [ "string" ]
}
```

- `title` - название объекта, максимальная длина - 42 символа;
- `comment` - комментарий к объекту, может быть пустым, максимальная длина - 255 символов;
- `value` - список идентификаторов объектов Время.

Ответ на успешный запрос: 200 OK

39.4.3 Удаление обьектов

Удаление обьектов:

```
DELETE /aliases/<название объекта>/<id объекта>
```

Ответ на успешный запрос: 200 OK

Названия обьектов:

- `ip_addresses` - IP-адрес;
- `ip_ranges` - Диапазон IP-адресов;
- `networks` - Подсеть;
- `domains` - Домен;
- `ports` - Порт;
- `port_ranges` - Диапазон портов;
- `time_ranges` - Время;
- `ip_address_lists` - Список IP-адресов.

Удаление списка обьектов:

```
DELETE /aliases/lists/<название объекта>/<id объекта>
```

Ответ на успешный запрос: 200 OK

Названия обьектов:

- `addresses` - Список IP-объектов;
- `ports` - Порты;
- `times` - Расписание.

39.5 Обнаружение устройств

Получение настроек:

```
GET /netscan_backend/settings
```

Ответ на успешный запрос:

```
{
   "enabled": "boolean",
   "group_id": "integer",
   "networks": [ "string" ]
}
```

- `group_id` - идентификатор группы, в которую будут добавлены обнаруженные устройства;
- `networks` - список локальных сетей, устройства из которых будут автоматически добавлены и авторизованы на Ideco NGFW.

Изменение настроек:

```
PUT /netscan_backend/settings
```

Json-тело запроса:

```
{
   "enabled": "boolean",
   "group_id": "integer",
   "networks": [ "string" ]
}
```

- `group_id` - идентификатор группы, в которую будут добавлены обнаруженные устройства;
- `networks` - список локальных сетей, устройства из которых будут автоматически добавлены и авторизованы на Ideco NGFW.

Ответ на успешный запрос: 200 OK

39.6 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.

40. Управление интеграцией с Active Directory

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Получение статуса работы службы ad_backend:

```
GET /ad_backend/status
```

Ответ на успешный запрос:

```
{
    "msg": [ "string" ]
}
```

- `msg` - список ошибок.

Возможные ошибки:

- **no_license** - Лицензия отсутствует | License is not available

Ввод NGFW в домен:

```
POST /ad_backend/domains
```

Json-тело запроса:

```
{
    "name": "string",
    "computer_name": "string",
    "dns_ips": [ "string" ],
    "user": "string",
    "password": "string",
    "ldap_paths": [ "string" ]
}
```

- `name` - имя домена;
- `computer_name` - имя компьютера (NGFW) в домене;
- `dns_ips` - список IP-адресов контроллеров домена;
- `user` - имя пользователя, имеющего права на ввод компьютера в домен;
- `password` - пароль пользователя `user`;
- `ldap_paths` - список LDAP-путей, по которым будет происходит поиск групп безопасности. Максимум 10 путей, максимальная длина строки - 1024 символа. Если при интеграции передать пустой список, то поиск групп безопасности будет производиться по всему лесу доменов. Если указаны конкретные LDAP-пути, импорт прочих пользователей и групп безопасности будет невозможен.

Ответ на успешный запрос: 200 OK

Получение списка присоединенных контроллеров домена:

```
GET /ad_backend/domains
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "computer_name": "string",
        "dns_ips": [ "string" ],
        "ldap_paths": [ "string" ],
    },
    ...
]
```

- `name` - имя домена;
- `computer_name` - имя компьютера (NGFW) в домене;
- `dns_ips` - список IP-адресов контроллеров домена;

- `ldap_paths` - список LDAP-путей, по которым будет происходит поиск групп безопасности. Максимум 10 путей, максимальная длина строки - 1024 символа. Если при интеграции передать пустой список, то поиск групп безопасности будет производиться по всему лесу доменов. Если указаны конкретные LDAP-пути, импорт прочих пользователей и групп безопасности будет невозможен.

Выполнение «переинтеграции» с AD:

```
PUT /ad_backend/domains/<id домена>
```

Json-тело запроса:

```
{
    "computer_name": "string",
    "user": "string",
    "password": "string",
    "ldap_paths": [ "string" ]
}
```

- `computer_name` - имя компьютера (NGFW) в домене;
- `user` - имя пользователя, имеющего права на ввод компьютера в домен;
- `password` - пароль пользователя `user`;
- `ldap_paths` - список LDAP-путей, по которым будет происходит поиск групп безопасности. Максимум 10 путей, максимальная длина строки - 1024 символа. Если при интеграции передать пустой список, то поиск групп безопасности будет производиться по всему лесу доменов. Если указаны конкретные LDAP-пути, импорт прочих пользователей и групп безопасности будет невозможен.

Ответ на успешный запрос: 200 OK

Удаление интеграции с доменом:

```
DELETE /ad_backend/domains/<id домена>
```

Ответ на успешный запрос: 200 OK

При выводе NGFW из домена удаляются все настройки интеграции с контроллером домена, а также все настройки синхронизируемых групп. При этом сами группы и пользователи в них становятся локальными.

В AD созданный для NGFW компьютер не удаляется.

40.1 Управление настройками службы

Получение настроек авторизации:

```
GET /ad_backend/settings
```

Ответ на успешный запрос:

```
{
    "authorization_by_logs": "boolean"
}
```

Изменение настроек авторизации:

```
PUT /ad_backend/settings
```

Json-тело запроса:

```
{
    "authorization_by_logs": "boolean"
}
```

Ответ на успешный запрос: 200 OK

40.2 Получение информации об объектах контроллера домена

Получение списка групп безопасности в заданном домене:

```
GET /ad_backend/domains/<имя домена>/security_groups
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "guid": "string"
    },
    ...
]
```

- `name` - отображаемое имя группы безопасности;
- `guid` - objectGUID группы безопасности.

Получение дерева OU в заданном домене:

```
GET /ad_backend/domains/<имя домена>/tree
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "guid": "string",
        "parent_guid": "string" | "null"
    }
    ...
]
```

- `name` - отображаемое имя группы;
- `guid` - objectGUID группы;
- `parent_guid` - objectGUID родительской группы.

Дерево представлено в виде линейного списка со всеми узлами. У каждого узла есть его `guid` и `parent_guid`.

Получение списка Forward-зон контроллера домена:

```
GET /ad_backend/forward_zones
```

Ответ на успешный запрос:

```
[
    {
        "id":  "string",
        "name": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "servers": [ "string" ],
        "enabled": "boolean",
        "comment": "string"
    },
    ...
]
```

- `id` - идентификатор зоны;
- `name` - название зоны;
- `servers` - список IP-адресов DNS-серверов;
- `enabled` - включена/выключена зона;
- `comment` - комментарий, может быть пустым.

40.3 Управление настройками синхронизации групп

Получение настройки синхронизации групп:

```
GET /ad_backend/group_settings
```

Ответ на успешный запрос:

```
[
  {
    "id": "integer",
    "group_id": "integer",
    "search_filter": "string",
    "object_guid": "string",
    "domain_name": "string",
    "sync_type": "ldap" | "security"
  },
  ...
]
```

- `id` - идентификатор записи синхронизации;
- `group_id` - идентификатор группы NGFW;
- `search_filter` - фильтр поиска в домене;
- `object_guid` - objectGUID группы из AD, с которой выполняется синхронизация;
- `domain_name` - имя домена, с которым выполняется синхронизация;
- `sync_type` - `security`, если группа синхронизируется с группой безопасности, `ldap` - если группа синхронизируется с OU.

Добавление настроек синхронизации группы с контроллером домена:

Группа безопасности импортируется как плоский список пользователей без сохранения древовидной структуры AD. Синхронизация с OU сохраняет древовидную структуру пользователей.

Если группа была локальной, а после этого запроса - синхронизируемой, то все ее текущие потомки считаются импортированными из AD. Если в домене таких пользователей нет, то они при первой же синхронизации будут перемещены в корзину.

```
POST /ad_backend/group_settings
```

Json-тело запроса:

```
{
    "search_filter": "string",
    "object_guid": "string",
    "group_id": "integer",
    "domain_name": "string",
    "sync_type": "ldap" | "security"
  }
```

Ответ на успешный запрос:

```
{
    "id": "sync_record_id"
}
```

Изменение настроек синхронизации группы с контроллером домена:

Группа безопасности импортируется как плоский список пользователей без сохранения древовидной структуры AD. Синхронизация с OU сохраняет древовидную структуру пользователей.

```
PUT /ad_backend/group_settings/<id записи синхронизации>
```

Json-тело запроса:

```
{
    "search_filter": "string",
    "object_guid": "string",
    "domain_name": "string",
    "group_id": "integer",
    "sync_type": "ldap" | "security"
  }
```

Ответ на успешный запрос: 200 OK

Отмена синхронизации группы с контроллером домена:

После отмены синхронизации группы с доменом все ее потомки считаются локальными. Для авторизации таких пользователей нужно либо ставить тип авторизации «по IP», либо менять всем пароли.

```
DELETE /ad_backend/group_settings/<id группы>
```

Ответ на успешный запрос: 200 OK

41. Управление пользователями

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

41.1 Управление пользователями

Получение списка пользователей:

```
GET /user_backend/users
```

Ответ на успешный запрос:

```
[
    {
        "id": "integer",
        "name": "string",
        "login": "string",
        "parent_id": "integer",
        "enabled": "boolean",
        "domain_type": "local" | "ad" | "ald" | "radius",
        "domain_name": "string",
        "ldap_guid": "string",
        "phone_number": "string",
        "comment": "string"
    }
]
```

- `id` - идентификатор пользователя;
- `name` - имя пользователя;
- `login` - логин пользователя;
- `parent_id` - идентификатор группы;
- `enabled` - соответствует опции **Запретить доступ**: `true` - включена, `false` - выключена;
- `domain_type` - тип домена;
- `domain_name` - имя домена, из которого импортирован пользователь;
- `ldap_guid` - идентификатор объекта AD;
- `phone_number` - номер телефона пользователя;
- `comment` - комментарий.

Создание пользователя:

```
POST /user_backend/users
```

Json-тело запроса:

```
{
    "name": "string",
    "login": "string",
    "psw": "string",
    "parent_id": "integer",
    "phone_number": "string" | null,
    "comment": "string"
}
```

- `name` - имя пользователя;
- `login` - логин пользователя;
- `psw` - пароль пользователя;
- `parent_id` - идентификатор группы;

- `phone_number` - номер телефона пользователя, не обязательно;
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор добавленного пользователя.

Если пользователь с указанным логином или именем существует, то исключение с описанием ошибки.

Изменение одного пользователя:

```
PUT /user_backend/users/<id пользователя>
```

Json-тело запроса:

```
{
    "name": "string",
    "login": "string",
    "parent_id": "integer",
    "enabled": "boolean",
    "domain_type": "string",
    "domain_name": "string",
    "ldap_guid": "string",
    "phone_number": "string" | null,
    "comment": "string"
}
```

- `name` - имя пользователя;
- `login` - логин пользователя;
- `parent_id` - идентификатор группы;
- `enabled` - соответствует опции **Запретить доступ**: `true` - включена, `false` - выключена;
- `domain_type` - тип домена;
- `domain_name` - имя домена, из которого импортирован пользователь;
- `ldap_guid` - идентификатор объекта AD;
- `phone_number` - номер телефона пользователя, не обязательно;
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос: 200 OK

Удаление пользователя:

```
DELETE /user_backend/users/<id пользователя>
```

Ответ на успешный запрос: 200 OK

Запрет удаленного подключения для пользователя:

```
PATCH /user_backend/users/<id пользователя>/disable-vpn
```

Ответ на успешный запрос: 200 OK

Создание группы:

```
POST /user_backend/groups
```

Json-тело запроса:

```
{
    "name": "string",
    "parent_id": "integer"
}
```

- `name` - имя группы;
- `parent_id` - идентификатор группы.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор добавленной группы.

Если группа с указанным именем у указанного предка существует, то код ответа 542 с описанием ошибки.

Получение групп:

```
GET /user_backend/groups
```

Ответ на успешный запрос:

```
[
    {
        "id": "integer",
        "name": "string",
        "parent_id": "integer",
        "domain_type": "string",
        "domain_name": "string",
        "ldap_guid": "string"
    }
]
```

- `id` - идентификатор группы;
- `name` - имя группы;
- `parent_id` - идентификатор родительской группы;
- `domain_type` - тип домена;
- `domain_name` - имя домена, из которого импортирована группа;
- `ldap_guid` - идентификатор объекта AD.

Изменение группы:

```
PUT /user_backend/groups/<id группы>
```

Json-тело запроса:

```
{
    "name": "string",
    "parent_id": "integer",
    "domain_type": "string",
    "domain_name": "string",
```

(continues on next page)

```
    "ldap_guid": "string"
}
```

- `name` - имя группы;
- `parent_id` - идентификатор родительской группы;
- `domain_type` - тип домена;
- `domain_name` - имя домена, из которого импортирована группа;
- `ldap_guid` - идентификатор объекта AD.

Ответ на успешный запрос: 200 OK

Удаление группы:

```
DELETE /user_backend/groups/<id группы>
```

Ответ на успешный запрос: 200 OK

Смена пароля пользователя:

```
PUT /user_backend/change_password/<id пользователя>
```

Json-тело запроса:

```
{
    "password": "string"
}
```

- `password` - новый пароль пользователя, не может быть пустым.

Ответ на успешный запрос: 200 OK

42. Управление Ideco Client

42.1 Настройка авторизации через Ideco Client

Получение настроек авторизации:

```
GET /agent_backend/wireguard/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

`enabled` - если `true`, то авторизация через Ideco Client включена, `false` - выключена.

Изменение настроек авторизации:

```
PUT /agent_backend/wireguard/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

`enabled` - `true` для включения авторизации через Ideco Client, `false` для выключения.

Ответ на успешный запрос: 200 OK

42.2 Настройки авторизации Ideco Client

Получение настроек авторизации Ideco Client:

```
GET /agent_backend/wireguard/setting
```

Ответ на успешный запрос:

```
{
    "auth_domain": "string",
    "local_tunnel": "boolean"
}
```

- `auth_domain` - домен/IP-адрес, в котором будет происходить аутентификация;
- `local_tunnel` - если `true`, то построение туннеля WireGuard для подключений из локальных сетей включено, `false` - выключено.

Изменение настроек авторизации Ideco Client:

```
PUT /agent_backend/wireguard/setting
```

Json-тело запроса:

```
{
    "auth_domain": "string",
    "local_tunnel": "boolean"
}
```

- `auth_domain` - домен/IP-адрес, в котором будет происходить аутентификация;
- `local_tunnel` - включено (`true`) или выключено (`false`) построение туннеля WireGuard для подключений из локальных сетей.

Ответ на успешный запрос: 200 OK

42.3 Протокол подключения и авторизации Ideco Client

Сообщения WebSocket с типом TEXT от Ideco Client принимаются бэкендом и после обработки посылается ответное сообщение с типом TEXT, за исключением обмена информацией для ZTNA. Принимаемые и ответные сообщения содержат информацию в формате JSON.

Процесс подключения и авторизации должен проходить в несколько этапов обмена сообщениями:

42.3.1 1. Подключение и запрос соответствия версии Ideco Client

После установления соединения через WebSocket Ideco Client должен сделать запрос со своей версией и типом операционной системы, чтобы Ideco NGFW удостоверился в соответствии версии Ideco Client и при необходимости обновления передал ссылку на скачивание новой версии.

Если версия Ideco Client не совпадает с той, что требует NGFW, нужно скачать дистрибутив, разорвать соединение и установить уже с актуальной версии.

Json-тело запроса:

```
{
    "type": "version",
    "major": "integer",
    "minor": "integer",
    "build": "integer",
    "os": "windows" | "macos" | "linux"
}
```

- `type` - команда;
- `major` - мажорная версия;
- `minor` - минорная версия;
- `build` - версия сборки;
- `os` - тип ОС Ideco Client.

Ответ на успешный запрос:

```
{
    "type": "update",
    "need_update": "boolean",
    "download_url": "string"| "null",
    "version": {
        "major": "integer",
        "minor": "integer",
        "build": "integer",
        "os": "windows" | "macos" | "linux"
    }
}
```

- `need_update` - требование обновления: `true` - необходимо, `false` - не требуется;
- `download_url` - путь для скачивания дистрибутива актуальной версии Ideco Client для требуемой ОС (пример: `:14765/IdecoAgent_x64.msi`). Если обновление не требуется, то значение поля будет `null`;
- `version` - версия дистрибутива Ideco Client на Ideco NGFW. Значения полей аналогичны описанным в запросе. Если обновление не требуется, поле будет отсутствовать.

42.3.2 2. Авторизация

Если версия Ideco Client совпадает с требуемой Ideco NGFW, то Ideco Client будет разрешено инициировать авторизацию на NGFW и при необходмости установить туннельное соединение WireGuard, если подключение идет из внешних сетей. Доступно два варианта авторизации: по логину и паролю или через SSO.

Авторизация по логину и паролю:

Json-тело запроса:

```
{
    "type": "authorize",
    "login": "string",
    "password": "string"
}
```

- `login` - логин пользователя, может также содержать домен;
- `password` - пароль.

Ответ на успешный запрос:

```
{
    "type": "auth_state",
    "authorized": "boolean",
    "need_tunnel": "boolean",
    "timeout": "integer",
    "message": "string"
}
```

- `authorized` - состояние авторизации: `true` - авторизован, `false` - не авторизован;
- `need_tunnel` - требуется ли установить туннель WireGuard;
- `timeout` - время до повторной попытки авторизации в секундах в случае возникновения ошибок в процессе авторизации. Если повторная попытка авторизации не требуется, то значение будет равно 0;
- `message` - сообщение о состоянии авторизации.

Авторизация с использованием SSO:

Авторизация SSO возможна только с локальных сетей Ideco NGFW. При попытке авторизации с внешних сетей сразу произойдет отказ.

Авторизация проходит в несколько обменов пакетами:

1. Запрос на доступность SSO:

Json-тело запроса:

```
{
    "type": "sso",
    "token": "null",
    "session_token": "null",
    "domain": "string"
}
```

- `token` - SSO токен Kerberos или NTLM, для данного запроса должен быть `null`;
- `session_token` - идентификатор сессии авторизации, для данного запроса должен быть `null`;
- `domain` - домен ActiveDirectory.

Ответ на успешный запрос:

```
{
    "type": "sso",
    "status": "not_authorized" | "challenge",
    "session_token": "null",
    "access_token": "null",
    "computer_name": "string",
    "error": "string" | "null"
}
```

- `status` - статус авторизации для домена: `not_authorized` - недоступна; `challenge` - доступна, необходимо передать токен для авторизации;
- `session_token` - токен сессии авторизации;
- `access_token` - ответный токен доступа SSO;
- `computer_name` - имя сервера контроллера домена. Если `status = "not_authorized"`, поле будет отсутствовать;
- `error` - сообщение об ошибке/причине недоступности SSO авторизации для домена: `null, status = "challenge"`.

2. Запрос на авторизацию SSO:

Json-тело запроса:

```
{
    "type": "sso",
    "token": "string",
    "session_token": "string" | "null",
    "domain": "string"
}
```

- `token` - должнен содержать соответствующий токен;
- `session_token` - идентификатор сессии, если это вторая или более итерация запроса на авторизацию;
- `domain` - домен ActiveDirectory.

Если авторизация SSO еще выполняется и нужно отправить еще один запрос на авторизацию SSO (повторить этот же этап обмена пакетами), ответ на успешный запрос:

```
{
    "type": "sso",
    "status": "in_progress",
    "session_token": "string",
    "access_token": "string",
    "error": "null"
}
```

Назначение полей аналогично первому ответу (см. выше), только session_token и access_token содержат соответствующие значения.

Если авторизациая завершилась, то в ответ NGFW отправит:

```
{
    "type": "auth_state",
    "authorized": "boolean",
    "need_tunnel": "boolean",
    "timeout": "integer",
    "message": "string"
}
```

- `authorized` - состояние авторизации: `true` - авторизован, `false` - не авторизован;
- `need_tunnel` - требуется ли установить туннель WireGuard;
- `timeout` - время до повторной попытки авторизации в секундах в случае возникновения ошибок в процессе авторизации. Если повторная попытка авторизации не требуется, то значение будет равно 0;
- `message` - сообщение о состоянии авторизации.

42.4 Протокол обмена информацией для ZTNA

Запрос Ideco NGFW на получение информации от Ideco Client:

Ideco NGFW отправляет запрос на сбор информации при подключении Ideco Client. В этом запросе указаны списки параметров, которые необходимо собрать, а также интервал, с которым Client должен собирать данные.

Json-тело запроса о сборе информации:

```
{
    "type": "ztna",
    "period": "integer",
    "test_list": [
      "os_type" | "os_version" | "domain" | "kb_list" | "av_active" | "av_name" | "av_
↪version" |" av_update" | "av_scan" | "fw_active" | "fw_name" | "fw_version" |
↪"processes" | "services" | "registry"
    ],
    "kb_list": [ "string"] ,
    "proc_list": [ "string" ],
    "service_list": [ "string" ],
    "reg_key_list": [ "string" ]
}
```

- `type` - тип запроса (`ztna`);
- `period` - интервал в минутах, через который Ideco Client должен собирать и передавать информацию. Если указан интервал, равный 0, проверка и передача собранных параметров выполняется однократно;
- `test_list` - список ключевых слов, определяющий необходимость выполнения проверок заданного типа:
  - `os_type` - проверка типа операционной системы;
  - `os_version` - проверка версии операционной системы;
  - `domain` - проверка включенности в домен;
  - `kb_list` - проверка обновлений операционной системы (в объеме списка, указанного в параметре `kb_list`);
  - `av_active` - проверка, запущен ли антивирус;
  - `av_name` - проверка типа установленного антивируса;
  - `av_version` - проверка версии установленного антивируса;
  - `av_update` - проверка даты последнего обновления баз антивируса;
  - `av_scan` - проверка даты последнего антивирусного сканирования на наличие угроз;
  - `fw_active` - проверка, запущен ли межсетевой экран;
  - `fw_name` - проверка типа установленного межсетевого экрана;
  - `fw_version` - проверка версии установленного межсетевого экрана;
  - `processes` - проверка запущенных процессов (в объеме списка, указанного в параметре `proc_list`);
  - `services` - проверка списка запущенных служб (в объеме списка, указанного в параметре `service_list`);
  - `registry` - проверка наличия и значения ключей реестра Windows (в объеме списка, указанного в параметре `key_list`).
- `kb_list` - список обновлений для выполнения проверки, может быть пустым, если проверка не требуется;
- `proc_list` - список процессов для выполнения проверки, может быть пустым, если проверка не требуется;
- `service_list` - список служб для выполнения проверки, может быть пустым, если проверка не требуется;
- `reg_key_list`: - список ключей реестра для выполнения проверки: путь/имя, может быть пустым, если проверка не требуется.

Ответ Ideco Client с информацией о выполнении проверок:

Ideco Client отправляет ответ с собранной информацией об устройстве в ответ на запрос проверок. Через определенный промежуток времени Ideco Client снова собирает информацию. Если с момента последней проверки ни один из параметров не изменился, то на NGFW ничего не отправляется.

Если хотя бы один из параметров изменился с момента последнего сбора информации, то Ideco Client отправляет обновленный ответ с собранной информацией об устройстве (полный набор запрошенных сведений) и повторяет проверку через указанный интервал времени.

Формат ответа с собраной в результате проверок информацией:

```
{
    "type": "ztna",
    "node_name": "string",
    "operation_system": {
      "type": "string",
      "version": "string",
      "domain": "string"
    },
    "kb_list": [ "string" ],
    "antivirus": [
      {
        "active": "boolean",
        "name": "string",
        "version": "string",
        "last_update": "integer" | "null",
        "last_scan": "integer" | "null",
      },
    ],
    "firewall": [
      {
        "active": "boolean",
        "name": "string",
        "version": "string",
      },
    ],
    "proc_list": [ "string" ],
    "service_list": [ "string" ],
    "reg_key_list": [
      {
        "key": "string",
        "value": "string",
      }
    ],
}
```

- `type` - тип сообщения (`ztna`);
- `node_name` - имя узла (собирается для отчетности, но не проходит никаких проверок);
- `operation_system` - результаты проверки ОС. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствуют ключевые слова `os_type`, `os_version`, `domain`:
  - `type` - тип операционной системы: `Windows`, `Linux`, `MacOS` (пустая строка, если проверка не выполнялась);
  - `version` - редакция и версия операционной системы (пустая строка, если проверка не выполнялась);
  - `domain` - имя домена (если проверка не выполнялась и в случае отсутствия домена - пустая строка).

- `kb_list` - результаты проверки установленных обновлений KB для Windows. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `kb_list`;
- `antivirus` - результаты проверок Антивируса. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`);
- `antivirus` - список результатов проверок Антивирусов (по числу установленных антивирусных пакетов). Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствуют ключевые слова `av_active`, `av_name`, `av_version`, `av_update`, `av_scan`:
  - `active` - если `true` - запущен, `false` - не запущен;
  - `name` - наименование продукта (пустая строка, если проверка не выполнялась);
  - `version` - версия продукта (пустая строка, если проверка не выполнялась);
  - `last_update` - количество полных дней, прошедших с последнего обновления баз (`null`, если проверка не выполнялась);
  - `last_scan` - количество полных дней, прошедших с последнего сканирования (`null`, если проверка не выполнялась или не проводилось сканирование).
- `firewall` - список результатов проверок межсетевых экранов (по числу установленных продуктов). Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствуют ключевые слова `fw_active`, `fw_name`, `fw_version`:
  - `active` - если `true` - активен, `false` - не активен;
  - `name` - наименование продукта (пустая строка, если проверка не выполнялась);
  - `version` - версия продукта (пустая строка, если проверка не выполнялась).
- `proc_list` - список найденных процессов. Может отсутствовать или быть пустым списком, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `processes`;
- `service_list` - список найденных служб Windows. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `services`;
- `reg_key_list` - список найденных ключей реестра. Может отсутствовать, если в списке запрошенных проверок (поле `test_list`) отсутствует ключевое слово `registry`;
  - `key` - ключ реестра (путь/имя);
  - `value` - значение параметра.

43. Управление правилами трафика

Подсказка: API правил трафика Ideco Center описано в статье *Центральная консоль*.

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

43.1 Файрвол

Получение статуса службы:

```
GET /firewall/status
```

Ответ на успешный запрос:

```
[
  {
      "name": "rules-in-kernel",
      "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
      "msg": [ "string" ]
  },
  {
        "msg": [ "string" ],
        "status": "active",
        "name": "auto-snat"
    }
]
```

- `msg` - список строк, поясняющих текущее состояние.

Получение настроек Файрвола:

43.2 Включенность пользовательских правил

```
GET /firewall/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - опция раздела **Файрвол**: `true` - включена, `false` - выключена.

43.2.1 Логирование правил

```
GET /firewall/settings
```

Ответ на успешный запрос:

```
{
    "automatic_snat_enabled": "boolean",
    "log_mode": "nothing" | "all" | "selected",
    "log_actions": [ "accept" | "drop" | "dnat" | "snat" | "mark_log" | "mark_not_log
↪" ]
}
```

- `automatic_snat_enabled` - включение автоматического SNAT: `true` - включен, `false`- выключен;
- `log_mode` - режим логирования;
- `log_actions` - события, которые будут логироваться.

Изменение настроек:

```
PUT /firewall/settings
```

Json-тело запроса:

```
{
    "automatic_snat_enabled": "boolean",
    "log_mode": "nothing" | "all" | "selected",
    "log_actions": [ "accept" | "drop" | "dnat" | "snat" | "mark_log" | "mark_not_log
↪" ]
}
```

- `automatic_snat_enabled` - включение автоматического SNAT: `true` - включен, `false`- выключен;
- `log_mode` - режим логирования;
- `log_actions` - события, которые будут логироваться.

Ответ на успешный запрос: 200 OK

43.2.2 Получение списка правил

Получение списка правил FORWARD и INPUT:

- `GET /firewall/rules/forward` - раздел FORWARD;
- `GET /firewall/rules/input` - раздел INPUT.

Ответ на успешный запрос:

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "hip_profiles": [ "string" ],
    "dpi_profile": "string",
    "dpi_enabled": "boolean",
    "ips_profile": "string",
    "ips_enabled": "boolean",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "drop"
}
```

- `id` - идентификатор правила.
- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;

- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;
- `dpi_profile` - строка в формате UUID, идентификатор профиля DPI. Не может быть пустой строкой, если `dpi_enabled` = `true`;
- `dpi_enabled` - если `true`, то обработка с помощью модуля **Контроль приложений** включена, `false` - выключена;
- `ips_profile` - строка в формате UUID, идентификатор профиля IPS. Не может быть пустой строкой, если `ips_enabled` = `true`;
- `ips_enabled` - если `true`, то обработка с помощью модуля **Предотвращение вторжений** включена, `false` - выключена;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

Получение списка правил DNAT:

```
GET /firewall/rules/dnat
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "dnat",
    "change_destination_address": "null" | "string",
    "change_destination_port": "null" | "string"
}
```

- `id` - идентификатор правила.
- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);

- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `dnat` - производить DNAT.
- `change_destination_address` - IP-адрес или диапазон IP-адресов для замены назначения, или `null`, если `action` = `accept`;
- `change_destination_port` - порт или диапазон портов для замены значения, или `null`, если `action` = `accept`.

Получение списка правил SNAT:

```
GET /firewall/rules/snat
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "snat",
    "change_source_address": "null" | "string"
}
```

- `id` - идентификатор правила.
- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `protocol` - протокол;
- `source_addresses` - адрес источника;

- source_addresses_negate - инвертировать адрес источника;
- source_ports - порты источников, список идентификаторов алиасов;
- destination_addresses - адрес назначения;
- destination_addresses_negate - инвертировать адрес назначения;
- destination_ports - порты назначения;
- outgoing_interface - зона назначения;
- timetable - время действия;
- action - действие:
  - accept - разрешить;
  - snat - производить SNAT.
- change_destination_address - IP-адрес для замены источника, или null, если action = accept.

Получение списка правил Логирования:

```
GET /firewall/rules/log
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "timetable": [ "string" ],
    "comment": "string",
    "action": "mark_log"
}
```

- id - идентификатор правила.
- parent_id - идентификатор группы в Ideco Center, в которую входит сервер, или константа f3ffde22-a562-4f43-ac04-c40fcec6a88c (соответствует Корневой группе);
- enabled - если true, то правило включено, false - выключено;
- protocol - протокол;
- source_addresses - адрес источника;
- source_addresses_negate - инвертировать адрес источника;
- source_ports - порты источников, список идентификаторов алиасов;
- incoming_interface - зона источника;
- destination_addresses - адрес назначения;
- destination_addresses_negate - инвертировать адрес назначения;
- destination_ports - порты назначения;

- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;
- `dpi_profile` - строка в формате UUID, идентификатор профиля DPI. Не может быть пустой строкой, если `dpi_enabled` = `true`;
- `dpi_enabled` - если `true`, то обработка с помощью модуля **Контроль приложений** включена, `false` - выключена;
- `ips_profile` - строка в формате UUID, идентификатор профиля IPS. Не может быть пустой строкой, если `ips_enabled` = `true`;
- `ips_enabled` - если `true`, то обработка с помощью модуля **Предотвращение вторжений** включена, `false` - выключена;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

43.3 Управление правилами

Добавление правила:

- `POST /firewall/rules/forward?anchor_item_id=<id правила>&insert_after={true|false}` - раздел FORWARD;
- `POST /firewall/rules/input?anchor_item_id=<id правила>&insert_after={true|false}` - раздел INPUT;
- `POST /firewall/rules/dnat?anchor_item_id=<id правила>&insert_after={true|false}` - раздел DNAT;
- `POST /firewall/rules/snat?anchor_item_id=<id правила>&insert_after={true|false}` - раздел SNAT;
- `POST /firewall/rules/log?anchor_item_id=<id правила>&insert_after={true|false}` - раздел Логирование.
  - `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое. Если отсутствует, то новое правило будет добавлено в конец таблицы;
  - `insert_after` - вставка до или после. Если значение `true` или отсутствует, то новое правило будет добавлено сразу после указанного в `anchor_item_id`. Если `false` - на месте указанного в `anchor_item_id`.

Json-тело запроса: один из объектов описанных в разделе *Получение списка правил*, без поля `id`.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Редактирование правила:

- `PUT /firewall/rules/forward/<id правила>` - раздел FORWARD;
- `PUT /firewall/rules/input/<id правила>` - раздел INPUT;
- `PUT /firewall/rules/dnat/<id правила>` - раздел DNAT;

- `PUT /firewall/rules/snat/<id правила>` - раздел SNAT;
- `PUT /firewall/rules/log/<id правила>` - раздел Логирование.

Json-тело запроса: один из объектов описанных в разделе ***Получение списка правил***, без поля `id`.

Ответ на успешный запрос: 200 OK

Перемещение правила:

- `PATCH /firewall/rules/forward/move` - раздел FORWARD;
- `PATCH /firewall/rules/input/move` - раздел INPUT;
- `PATCH /firewall/rules/dnat/move` - раздел DNAT;
- `PATCH /firewall/rules/snat/move` - раздел SNAT;
- `PATCH /firewall/rules/log/move` - раздел Логирование.

Json-тело запроса:

```
{
    "params": {
      "id": "integer",
      "anchor_item_id": "integer",
      "insert_after": "boolean"
    }
}
```

- `id` - идентификатор перемещаемого правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно поместить перемещаемое правило;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Удаление правила:

- `DELETE /firewall/rules/forward/<id правила>` - раздел FORWARD;
- `DELETE /firewall/rules/input/<id правила>` - раздел INPUT;
- `DELETE /firewall/rules/dnat/<id правила>` - раздел DNAT;
- `DELETE /firewall/rules/snat/<id правила>` - раздел SNAT;
- `DELETE /firewall/rules/log/<id правила>` - раздел Логирование.

Ответ на успешный запрос: 200 OK

43.3.1 Счетчик срабатывания правил

Проверка включенности счетчика срабатываний правил:

```
GET /firewall/watch
```

Ответ на успешный запрос:

```
{
   "enabled": "boolean"
}
```

- `enabled` - если `true`, то счетчик включен, если `false` - выключен.

Включение/выключение счетчика срабатывания правил:

```
PUT /firewall/watch
```

Json-тело запроса:

```
{
   "enabled": "boolean"
}
```

- `enabled` - `true` для включения, `false` для выключения.

Ответ на успешный запрос: 200 OK

Получение счетчиков по правилам:

- `GET /firewall/counters/forward` - раздел FORWARD;
- `GET /firewall/counters/input` - раздел INPUT;
- `GET /firewall/counters/dnat` - раздел DNAT;
- `GET /firewall/counters/snat` - раздел SNAT;
- `GET /firewall/rules/log` - раздел Логирование.

Ответ на успешный запрос:

```
[
   {
      "id": "integer",
      "packets": "integer"
   },
   ...
]
```

- `id` - идентификатор правила;
- `packets` - количество сработок правила.

43.4 Контроль приложений

Получение списка правил:

```
GET /application_control_backend/rules
```

Ответ на успешный запрос:

```
[
    {
        "action": "drop" | "accept",
        "aliases": [ "string" ],
        "comment": "string",
        "enabled": "boolean",
        "name": "string",
        "parent_id": "string",
        "protocols": [ "string" ],
        "id": "integer"
    },
    ...
 ]
```

- `action` - действие, применяемое к правилу;

- `aliases` - объекты, которые используются в правиле (например, any. Список объектов доступен по *ссылке*;
- `comment` - комментарий правила;
- `enabled` - статус правила: `true` - включено, `false` - выключено;
- `name` - имя правила;
- `parent_id` - идентификатор родительской группы серверов;
- `protocols` - список протоколов;
- `id` - идентификатор правила.

Создание нового правила:

```
POST /application_control_backend/rules
```

Json-тело запроса:

```
{
    "parent_id": "string",
    "name": "string",
    "action": "drop" | "accept",
    "comment": "string",
    "aliases": [ "string" ],
    "protocols": [ "string" ],
    "enabled": "boolean"
}
```

- `parent_id` - идентификатор родительской группы серверов;
- `name` - имя правила;
- `action` - действие, применяемое к правилу;
- `comment` - комментарий правила;
- `aliases` - объекты, которые используются в правиле (например, any. Список объектов доступен по *ссылке*;
- `protocols` - список протоколов;
- `enabled` - статус правила: `true` - включено, `false` - выключено.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Изменение правила:

```
PUT /application_control_backend/rules/<id правила>
```

Json-тело запроса:

```
{
    "parent_id": "string",
    "name": "string",
    "comment": "string",
    "aliases": [ "string" ],
    "protocols": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "action": "drop" | "accept",
    "enabled": "boolean"
}
```

- `parent_id` - идентификатор родительской группы серверов;
- `name` - имя правила;
- `comment` - комментарий правила;
- `aliases` - объекты, которые используются в правиле (например, any. Список объектов доступен по *ссылке*;
- `protocols` - список протоколов;
- `action` - действие, применяемое к правилу;
- `enabled` - статус правила: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Изменение приоритета правила:

```
PATCH /application_control_backend/rules/move
```

Json-тело запроса:

```
{
  "params": {
    "id": "integer",
    "anchor_item_id": "integer",
    "insert_after": "boolean",
  },
}
```

- `id` - идентификатор правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false`, то на месте указанного в `anchor_item_id`.

Удаление правила:

```
DELETE /application_control_backend/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

43.5 Предотвращение вторжений

Получение статуса модуля:

```
GET /ips/status
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
        "msg": [ "string" ]
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    },
  ...
]
```

- `name` - название домена;
- `status` - статус;
- `msg` - список сообщений, объясняющий текущее состояние.

Статус обновления баз правил Suricata и GeoIP:

```
GET /ips/update
```

Ответ на успешный запрос:

```
{
    "status": "up_to_date" | "updating" | "failed_to_update" | "disabled"],
    "msg": "i18n_str",
    "last_update": "float" | "null"
}
```

- `status` - текущий статус обновления баз:
  - `up_to_date` - базы успешно обновлены;
  - `updating` - скачиваем новые базы;
  - `failed_to_update` - последняя попытка обновления баз завершилась неудачно;
  - `disabled` - обновление баз выключено.
- `msg` - текстовое описание статуса обновления баз;
- `last_update` - время последнего успешного обновления баз.

Получение статуса обновления расширенных баз правил Suricata и GeoIP:

```
GET /ips/update_advanced
```

Ответ на успешный запрос:

```
{
    "status": "up_to_date" | "updating" | "failed_to_update" | "disabled",
    "msg": "i18n_str",
    "last_update": "float" | "null"
}
```

- `status` - текущий статус обновления баз:
  - `up_to_date` - базы успешно обновлены;
  - `updating` - скачиваем новые базы;
  - `failed_to_update` - последняя попытка обновления баз завершилась неудачно;
  - `disabled` - обновление баз выключено.
- `msg` - текстовое описание статуса обновления баз;
- `last_update` - время последнего успешного обновления баз.

Запуск принудительного обновления баз:

```
POST /ips/update
```

Ответ на успешный запрос: 200 OK

Получение текущей настройки включенности модуля:

```
GET /ips/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true`, если модуль включен, `false` - выключен.

Изменение настройки включенности модуля:

```
PUT /ips/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` если модуль включен, `false` - выключен.

Ответ на успешный запрос: 200 OK

Получение списка локальных подсетей:

```
GET /ips/nets
```

Ответ на успешный запрос:

```
[
  {
      "id": "string",
      "address": "string"
  },
  ...
]
```

- `id` - идентификатор подсети;
- `address` - адрес подсети (например, `192.168.0.0`).

Добавление новой локальной подсети:

```
POST /ips/nets
```

Json-тело запроса:

```
{
    "address": "string"
}
```

- `address` - адрес подсети (например,`192.168.0.0`).

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор подсети.

Удаление локальной подсети:

```
DELETE /ips/nets/<id подсети>
```

Ответ на успешный запрос: 200 OK

Получение списка наборов правил:

```
GET /ips/rules
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "name": "string",
    "enabled": "boolean"
  },
  ...
]
```

- `id` - идентификатор набора правил;
- `name` - название набора правил;
- `enabled` - состояние набора правил: `true` - включен, `false` - выключен.

Включение/выключение набора правил:

```
PATCH /ips/rules/<id набора правил>
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения набора правил, `false` для выключения.

Ответ на успешный запрос: 200 OK

Получение содержимого правила по sid:

```
GET /ips/rules/sid/<sid правила>
```

Ответ на успешный запрос:

```
{
    "rule": "string"
}
```

- `rule` - текст правила. Если правило не найдено, то пустая строка.

Получение списка исключений:

```
GET /ips/disabled_rules
```

Ответ на успешный запрос:

```
[
  {
    "sid": "integer",
    "comment": "string",
    "id": "string"
  },
  ...
]
```

- `sid` - идентификатор правила;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `id` - идентификатор правила.

Добавление исключения:

```
POST /ips/disabled_rules
```

Json-тело запроса:

```
{
    "sid": "integer",
    "comment": "string"
}
```

- `sid` - идентификатор правила;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор исключения.

Редактирование описания существующего исключения:

```
PATCH /ips/disabled_rules/<id правила (не sid)>
```

Json-тело запроса:

```
{
    "sid": "integer",
    "comment": "string"
}
```

- `sid` - идентификатор правила;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;

Ответ на успешный запрос: 200 OK

Удаление существующего исключения:

```
DELETE /ips/disabled_rules/<id исключения>
```

Ответ на успешный запрос: 200 OK

Получение списка исключений объектов:

```
GET /ips/bypass
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "aliases": [ "string" ],
        "comment": "string",
        "enabled": "boolean",
    },
    ...
]
```

- `id` - идентификатор исключения;
- `aliases` - список идентификаторов объектов. Допустимые типы: IP-адрес, Диапазон IP-адресов, Список IP-объектов, Список IP-адресов, Подсеть, Домен, Пользователь, Группа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - состояние исключения: `true` - включено, `false` - выключено.

Добавление исключения объектов:

```
POST /ips/bypass
```

Json-тело запроса:

```
{
    "aliases": [ "string" ],
    "comment": "string",
    "enabled": "boolean"
}
```

- `aliases` - список идентификаторов объектов. Допустимые типы: IP-адрес, Диапазон IP-адресов, Список IP-объектов, Список IP-адресов, Подсеть, Домен, Пользователь, Группа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - состояние исключения: `true` - включено, `false` - выключено.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного исключения.

Изменение исключения объектов:

```
PATCH /ips/bypass/<id исключения>
```

Json-тело запроса:

```
{
    "aliases": [ "string" ],
    "comment": "string",
    "enabled": "boolean"
}
```

- `aliases` - список идентификаторов объектов. Допустимые типы: IP-адрес, Диапазон IP-адресов, Список IP-объектов, Список IP-адресов, Подсеть, Домен, Пользователь, Группа;
- `comment` - описание, может быть пустым, максимальная длина - 255 символов;
- `enabled` - состояние исключения: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Удаление существующего исключения объектов:

```
DELETE /ips/bypass/<id исключения>
```

Ответ на успешный запрос: 200 OK

43.6 Контент-фильтр

Включение/выключение Контент-фильтра:

43.6.1 Проверить включенность

```
GET /content-filter/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние **Контент-фильтра**: `true` - включен, `false` - выключен.

43.6.2 Включить/выключить Контент-фильтр

```
PUT /content-filter/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения **Контент-фильтра**, `false` для выключения.

Ответ на успешный запрос: 200 OK

43.6.3 Настройки

Получение настроек:

```
GET /content-filter/settings
```

Ответ на успешный запрос:

```
{
    "enabled_extended_categorizer": "boolean",
    "quic_reject_enabled": "boolean"
}
```

- `enabled_extended_categorizer` - расширенная категоризация (SkyDNS): `true` - включена, `false` - выключена;
- `quic_reject_enabled` - запрет трафика по протоколу QUIC: `true` - включен, `false` - выключен.

Изменение настроек:

```
PATCH /content-filter/settings
```

Json-тело запроса:

```
{
    "enabled_extended_categorizer": "boolean",
    "quic_reject_enabled": "boolean"
}
```

- `enabled_extended_categorizer` - расширенная категоризация (SkyDNS): `true` - включена, `false` - выключена;
- `quic_reject_enabled` - запрет трафика по протоколу QUIC: `true` - включен, `false` - выключен.

Ответ на успешный запрос: 200 OK

Получение настройки безопасного поиска:

```
GET /proxy_backend/safe_search
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние безопасного поиска: `true` - включен, `false` - выключен.

Изменение настройки безопасного поиска:

```
PUT /proxy_backend/safe_search
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения, `false` для выключения.

Ответ на успешный запрос: 200 OK

43.6.4 Категории Контент-фильтра

Получение списка категорий (предустановленных и пользовательских):

```
GET /content-filter/categories
```

Json-тело ответа:

```
[
    {
        "id": "string",
        "type": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "name": "string",
        "comment": "string"
    },
    ...
]
```

- `id` - номер категории в формате `users.id.1` или `extended.id.1`;
- `type` - тип категории:
  - `users` - пользовательские категории;
  - `extended` - расширенные категории (SkyDNS);
  - `files` - категории для файлов;
  - `special` - специальные предопределенные категории (Прямое обращение по IP, Все категоризированные запросы, Все некатегоризированные запросы, Все запросы);
  - `other` - остальные категории.
- `name` - имя категории;
- `comment` - описание категории.

Получение списка пользовательских категорий:

```
GET /content-filter/users_categories
```

Json-ответ на запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "comment": "string",
        "urls": [ "string" ]
    },
    ...
]
```

- `id` - идентификатор категории в формате `users.id.1`;
- `name` - название категории, не пустая строка;
- `comment` - комментарий;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Создание пользовательской категории:

```
POST /content-filter/users_categories
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий;

- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор пользовательской категории.

Редактирование пользовательских категорий:

```
PUT /content-filter/users_categories/<id категории>
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string",
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `id` - идентификатор пользовательской категории.

43.6.5 Правила Контент-фильтра

Получение списка правил:

```
GET /content-filter/rules
```

Json-тело ответа:

```
[
    {
        "access": "allow" | "deny" | "bump" | "redirect",
        "aliases": [ "string" ],
        "categories": [ "string" ],
        "comment": "string",
        "enabled": "boolean",
        "name": "string",
        "parent_id": "string",
        "redirect_url": "string" | "null",
        "timetable": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "id": "integer"
    },
    ...
]
```

- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `comment` - комментарий, может быть пустым (максимальная длина - 255 символов);
- `enabled` - статус правила: `true` - включено, `false` выключено;
- `name` - название правила, не пустая строка;
- `parent_id` - идентификатор группы в Ideco Center, в которую входит Ideco NGFW, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `redirect_url` - адрес, на который перенаправляются запросы: `string` при `access` = `redirect`, `null` при остальных вариантах `access`;
- `timetable` - время действия, список идентификаторов алиасов;
- `id` - идентификатор правила.

Создание правила:

```
POST /content-filter/rules?anchor_item_id=123&insert_after={true|false}
```

- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое. Если отсутствует, то новое правило будет добавлено в конец таблицы.
- `insert_after` - вставка до или после. Если значение `true` или отсутствует, то новое правило будет добавлено сразу после указанного в `anchor_item_id`. Если `false` - на месте указанного в `anchor_item_id`.

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "parent_id": "string",
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "access": "allow" | "deny" | "bump" | "redirect",
    "redirect_url": "string" | "null",
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `name` - название правила, не пустая строка;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `parent_id` - идентификатор группы в Ideco Center, в которую входит Ideco NGFW, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);

- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы: `string` при `access` = `redirect`, `null` при остальных вариантах `access`;
- `enabled` - `true` для включения, `false` для выключения;
- `timetable` - время действия, список идентификаторов алиасов.

Редактирование правила:

```
PUT /content-filter/rules/<id правила>
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "parent_id": "string",
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "access": "allow" | "deny" | "bump" | "redirect",
    "redirect_url": "string" | "null",
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `name` - название правила, не пустая строка;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `parent_id` - идентификатор группы в Ideco Center, в которую входит Ideco NGFW, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`.
- `redirect_url` - адрес, на который перенаправляются запросы: `string` при `access` = `redirect`, `null` при остальных вариантах `access`;
- `enabled` - `true` для включения, `false` для выключения;
- `timetable` - время действия, список идентификаторов алиасов.

Ответ на успешный запрос: 200 OK

Перемещение правила:

```
PATCH /content-filter/rules/move
```

Json-тело запроса:

```
{
  "params": {
    "id": "integer",
    "anchor_item_id": "integer",
    "insert_after": "boolean"
  }
}
```

- `id` - идентификатор правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно вставить правило, которое перемещаем;
- `insert_after` - вставка до или после. Если `true`, то правило будет вставлено сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление правила:

```
DELETE /content-filter/rules/<id правила>
```

Ответ на успешный запрос: 200 OK

43.7 Квоты

Проверить включенность подсчета квот:

```
GET /quotas/state
```

Ответ на успешный запрос:

```
{
  "enabled": "boolean"
}
```

- `enabled` - если `true`, то подсчет квот включен, если `false` - выключен.

Включение/выключение подсчета квот:

```
PUT /quotas/state
```

Json-тело запроса:

```
{
  "enabled": "boolean"
}
```

- `enabled` - `true` для включения, `false` для выключения.

Ответ на успешный запрос: 200 OK

Получение списка квот:

```
GET /quotas/quotas
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string",
    "comment": "string",
    "quota": "integer",
    "enabled": "boolean",
    "interval": "hour" | "day" | "week" | "month" | "quarter"
  },
  ...
]
```

- `id` - идентификатор квоты;
- `title` - название квоты, максимальная длина - 42 символа;
- `comment` - комментарий, максимальная длина - 255 символов;
- `quota` - ограничение трафика в байтах;
- `enabled` - применяется ли квота;
- `interval` - период действия квоты (час, день, неделя, месяц, квартал).

Создание квоты:

```
POST /quotas/quotas
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string",
    "quota": "integer",
    "enabled": "boolean",
    "interval": "string"
}
```

- `title` - название квоты, максимальная длина - 42 символа;
- `comment` - комментарий, максимальная длина - 255 символов;
- `quota` - ограничение трафика в байтах;
- `enabled` - применяется ли квота;
- `interval` - период действия квоты (час, день, неделя, месяц, квартал).

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор квоты.

Редактирование квоты:

```
PATCH /quotas/quotas/<id квоты>
```

Json-тело запроса (все или некоторые поля):

```
{
    "title": "string",
    "comment": "string",
    "quota": "integer",
    "enabled": "boolean",
    "interval": "string"
}
```

- `title` - название квоты, максимальная длина - 42 символа;
- `comment` - комментарий, максимальная длина - 255 символов;
- `quota` - ограничение трафика в байтах;
- `enabled` - применяется ли квота;
- `interval` - период действия квоты (час, день, неделя, месяц, квартал).

Ответ на успешный запрос: 200 OK

Удаление квоты:

```
DELETE /quotas/quotas/<id квоты>
```

Ответ на успешный запрос: 200 OK

44. Управление сетевыми интерфейсами

44.1 Внешние и локальные интерфейсы

44.1.1 Получение списка всех внешних и локальных интерфейсов

LAN (Локальный Ethernet-интерфейс):

```
GET /network/connections
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "type": "lan",
    "title": "string",
    "enabled": "boolean",
    "mac": "string",
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;

- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP;
- `dns` - список IP-адресов DNS. Может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть равен `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN.

WAN (Подключение к провайдеру по Ethernet):

```
GET /network/connections
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "type": "wan",
    "title": "string",
    "enabled": "boolean",
    "mac": "string",
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `enable_dhcp` - получать ли адрес интерфейса и адрес шлюза от провайдера по DHCP;
- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP;
- `dns` - список IP-адресов DNS, может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно), `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN.

PPTP (Подключение к провайдеру по PPTP):

Ответ на успешный запрос:

```
GET /network/connections
```

```
{
    "id": "integer",
    "type": "pptp",
    "title": "string",
    "enabled": "boolean",
    "server": "string",
    "login": "string",
    "password": "string",
    "mac": "string",
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `server` - IP-адрес или доменное имя PPTP-сервера, к которому осуществляется подключение;
- `login` - логин на сервере PPTP, не может быть пустым;
- `password` - пароль на сервере PPTP, не может быть пустым;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `enable_dhcp` - получать ли адрес интерфейса и адрес шлюза от провайдера по DHCP;
- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP или PPTP-сервер находится в той же подсети, что назначена на интерфейс;
- `dns` - список IP-адресов DNS, может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть `null` если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN.

L2TP (Подключение к провайдеру по L2TP):

```
GET /network/connections
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "type": "l2tp",
    "title": "string",
    "enabled": "boolean",
    "server": "string",
    "login": "string",
    "password": "string",
    "mac": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "enable_dhcp": "boolean",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "dns": [ "string" ],
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `server` - IP-адрес или доменное имя L2TP-сервера, к которому осуществляется подключение;
- `login` - логин на сервере L2TP, не может быть пустым;
- `password` - пароль на сервере L2TP, не может быть пустым;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `enable_dhcp` - получать ли адрес интерфейса и адрес шлюза от провайдера по DHCP;
- `addresses` - список адресов в формате `IP/prefix`. Может быть пустым, если включено получение адресов по DHCP;
- `gateway` - IP-адрес шлюза. Может быть `null`, если включено получение адресов по DHCP или L2TP-сервер находится в той же подсети, что назначена на интерфейс;
- `dns` - список IP-адресов DNS, может быть пустым независимо от флага включения DHCP;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно), `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN.

PPPoE (Подключение к провайдеру по PPPoE):

```
GET /network/connections
```

Ответ на успешный запрос:

```
{
    "id": "integer",
    "type": "pppoe",
    "title": "string",
    "enabled": "boolean",
    "login": "string",
    "password": "string",
    "service": "string",
    "concentrator": "string",
    "mac": "string",
    "vlan_tag": "null" | "integer",
    "zone": "null" | "string",
    "is_vce_vlan": "boolean"
}
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;

- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `login` - логин на сервере PPPoE, не может быть пустым;
- `password` - пароль на сервере PPPoE, не может быть пустым;
- `service` - название сервиса, может быть пустым;
- `concentrator` - название концентратора, может быть пустым;
- `mac` - MAC-адрес сетевой карты или идентификатор агрегированного интерфейса. MAC-адрес в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно), `null`, если не назначен;
- `zone` - алиас зоны. Может быть `null`, если не назначен;
- `is_vce_vlan` - `true`, если подключение создано на основе проброшенного в VCE VLAN.

Loopback:

```
GET /network/connections
```

Ответ на успешный запрос:

```
{
    "mac": "string",
    "osdevname": "string",
    "addresses": [ "string" ],
    "comment": "string",
    "enabled": "boolean",
    "is_vce_vlan": "boolean",
    "title": "string",
    "type": "loopback",
    "vlan_tag": "integer",
    "zone": "string",
    "id": "integer"
}
```

- `mac` - MAC-адрес интерфейса. Для Loopback-интерфейса - `null`;
- `osdevname` - название Loopback-интерфейса в операционной системе (например, `Oloopback3`). Значение создается автоматически, является уникальным и доступно только для чтения;
- `addresses` - список адресов в формате `IP/prefix`.
- `comment` - комментарий, может быть пустым. Максимальное количество символов - 256;
- `enabled` - статус активности интерфейса:
  - `true` - включен;
  - `false` - выключен.
- `is_vce_vlan` - признак подключения, созданного на основе проброшенного в VCE VLAN. Для Loopback-интерфейса - `false`;
- `title` - название интерфейса, не может быть пустым;
- `type` - тип подключения;
- `vlan_tag` - тэг VLAN. Для Loopback-интерфейса - `null`;
- `zone` - идентификатор зоны, к которой относится интерфейс. Для Loopback-интерфейса - `null`;
- `id` - идентификатор интерфейса.

44.1.2 Управление внешними и локальными интерфейсами

Получение состояния локальных интерфейсов и подключений:

```
GET /network/states
```

Ответ на успешный запрос:

```
[
  {
    "id": "integer",
    "type": "lan" | "wan" | "pptp" | "l2tp" | "pppoe",
    "ether": {
        "device": "null" | "string",
        "vlan_tag": "null" | "integer",
        "addresses": [ "string" ],
        "gateway": "null" | "string",
        "dns": [ "string" ],
        "status": "down" | "going-up" | "up",
        "errors": [ "string" ]
    },
    "ppp": {
        "device": "null" | "string",
        "remote_address": "null" | "string",
        "local_address": "null" | "string",
        "dns": [ "string" ],
        "status": "down" | "going-up" | "up",
        "errors": [ "string" ]
    },
    "summary": {
        "device": "null" | "string",
        "addresses": [ "string" ],
        "dns": [ "string" ],
        "gateway": "null" | "string",
        "zone": "null" | "string",
        "ifindex": "null" | "integer",
        "scope": "kernel" | "vpp"
    }
  },
...
]
```

- `id` - идентификатор интерфейса;
- `type` - тип подключения;
- `ether` - состояние Ethernet или VLAN:
  - `device` - название устройства в системе, например, `Leth1`;
  - `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно) или `null`, если не назначен;
  - `addresses` - список адресов, может быть пустым. Адреса в формате `IP/prefix`;
  - `gateway` - IP-адрес шлюза, может быть равен `null`, если шлюза нет;
  - `dns` - адреса DNS, выданные по DHCP или назначенные пользователем;
  - `status` - текущее состояние интерфейса;
  - `errors` - список ошибок.

- `ppp` - состояние PPP-подключения. Поле определено только для интерфейсов с полем `type` равным `pptp | l2tp | pppoe`, для всех остальных типов `lan | wan` равно `null`:
  - `device` - название устройства в системе, например `Eppp4`;
  - `remote_address` - туннельный IP-адрес сервера;
  - `local_address` - туннельный IP-адрес клиента (IP-адрес NGFW);
  - `dns` - адреса DNS, выданные из PPP;
  - `status` - текущее состояние интерфейса;
  - `errors` - список ошибок.
- `summary` - общее состояние подключение:
  - `device` - итоговое активное устройство, например, `Eppp4` или `Eeth3`;
  - `addresses` - список адресов интерфейса или подключения к провайдеру;
  - `dns` - адреса DNS, пригодные к использованию для сервера DNS и других целей;
  - `gateway` - IP-адрес шлюза, может быть равен `null`, если шлюза нет;
  - `zone` - алиас зоны. Может быть равен `null`, если не назначен;
  - `ifindex` - числовой индентификатор интерфейса;
  - `scope` - принадлежность интерфейса сетевому стеку: kernel - ядро.

Создание внешнего или локального интерфейса:

```
POST /network/connections
```

Json-тело запроса: один из объектов описанных в разделе *Получение списка всех внешних и локальных интерфейсов*:

- LAN | WAN | PPTP | L2TP | PPPoE - без поля `id`.
- Loopback - без полей `id` и `osdevname`.

Ответ на успешный запрос:

```
{
    "id": "number"
}
```

- `id` - идентификатор созданного интерфейса.

Редактирование внешнего или локального интерфейса:

```
PATCH /network/connections/<id интерфейса>
```

Json-тело запроса: один из объектов описанных в разделе *Получение списка всех внешних и локальных интерфейсов*.

Ответ на успешный запрос: 200 OK

Удаление внешнего или локального интерфейса:

```
DELETE /network/connections/<id интерфейса>
```

Ответ на успешный запрос: 200 OK

44.2 Агрегированные интерфейсы

Получение списка агрегированных интерфейсов:

```
GET /network/aggregated
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "enabled": "boolean",
    "title": "string",
    "comment": "string",
    "nics": [ "string" ]
  },
...
]
```

- `id` - идентификатор агрегированного интерфейса;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `title` - название, не может быть пустым;
- `comment` - комментарий, может быть пустым;
- `nics` - список MAC-адресов в формате `11:22:33:44:55:66`, все буквы в нижнем регистре, может быть пустым.

Получение состояния агрегированных интерфейсов:

```
GET /network/aggregated_states
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "link": "up" | "down"
  },
...
]
```

- `id` - идентификатор агрегированного интерфейса;
- `link` - состояние соединения на агрегированном интерфейсе.

Создание нового агрегированного интерфейса:

```
POST /network/aggregated
```

Json-тело запроса:

```
{
  "enabled": "boolean",
  "title": "string",
  "comment": "string",
  "nics": [ "string" ]
  }
```

- `enabled` - если `true`, то интерфейс включен, `false` - выключен;

- `title` - название, не может быть пустым;
- `comment` - комментарий, может быть пустым;
- `nics` - список MAC-адресов в формате `11:22:33:44:55:66`, все буквы в нижнем регистре, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного агрегированного интерфейса.

Редактирование агрегированного интерфейса:

```
PUT /network/aggregated/<id агрегированного интерфейса>
```

Json-тело запроса:

```
{
  "enabled": "boolean",
  "title": "string",
  "comment": "string",
  "nics": [ "string" ]
  }
```

- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `title` - название, не может быть пустым;
- `comment` - комментарий, может быть пустым;
- `nics` - список MAC-адресов в формате `11:22:33:44:55:66`, все буквы в нижнем регистре, может быть пустым.

Ответ на успешный запрос: 200 OK

Удаление агрегированного интерфейса:

```
DELETE /network/aggregated/<id агрегированного интерфейса>
```

Ответ на успешный запрос: 200 OK

44.3 Туннельные интерфейсы

Получение списка всех туннельных интерфейсов:

```
GET /network/tunnels
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string",
    "enabled": "boolean",
    "comment": "string",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "parent_interface": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "osdevname": "string",
    "server": "string",
    "zone": "null" | "string"
  },
...
]
```

- `id` - идентификатор интерфейса, строка в формате UUID;
- `title` - название интерфейса, не может быть пустым, максимальная длина - 42 символа;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `comment` - комментарий, может быть пустым;
- `addresses` - список адресов в формате `IP/prefix`;
- `gateway` - IP-адрес шлюза, может быть равен `null`;
- `parent_interface` - алиас родительского интерфейса, его IP-адрес будет источником туннеля;
- `osdevname` - название существующего или планируемого сетевого интерфейса в ядре (например, `Gre00000001`). Значение создается автоматически, является уникальным и **доступно только для чтения**;
- `server` - IP-адрес или доменное имя устройства, к которому осуществляется подключение;
- `zone` - алиас зоны. Может быть `null`, если не назначен.

Важно: Для каждого родительского интерфейса все настроенные туннели должны иметь уникальные значения в поле `server`. Не допускается создание туннельных интерфейсов с повторяющимися значениями в полях `parent_interface` и `server`!

Получение состояния туннельных интерфейсов:

```
GET /network/tunnel_states
```

Ответ на успешный запрос:

```
{
  "id": "string",
  "link": "up" | "down" | "inactive",
  "local_ip": "string"
}
```

- `id` - идентификатор интерфейса;
- `link` - состояние туннельного интерфейса, `inactive` при недоступности родительского интерфейса;
- `local_ip` - IP-адрес родительского интерфейса запущенного туннеля.

Создание нового туннельного интерфейса:

```
POST /network/tunnels
```

Json-тело запроса:

```
{
    "title": "string",
    "enabled": "boolean",
    "comment": "string",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "parent_interface": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "osdevname": "string",
    "server": "string",
    "zone": "null" | "string"
}
```

- `title` - название интерфейса, не может быть пустым, максимальная длина - 42 символа;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `comment` - комментарий, может быть пустым;
- `addresses` - список адресов в формате `IP/prefix`;
- `gateway` - IP-адрес шлюза, может быть равен `null`;
- `parent_interface` - алиас родительского интерфейса, его IP-адрес будет источником туннеля;
- `osdevname` - название существующего или планируемого сетевого интерфейса в ядре (например, `Gre00000001`). Значение создается автоматически, является уникальным и **доступно только для чтения**;
- `server` - IP-адрес или доменное имя устройства, к которому осуществляется подключение;
- `zone` - алиас зоны. Может быть `null`, если не назначен.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданного туннельного интерфейса.

Редактирование туннельного интерфейса:

```
PUT /network/tunnels/<id туннельного интерфейса>
```

Json-тело запроса:

```
{
    "title": "string",
    "enabled": "boolean",
    "comment": "string",
    "addresses": [ "string" ],
    "gateway": "null" | "string",
    "parent_interface": "string",
    "osdevname": "string",
    "server": "string",
    "zone": "null" | "string"
}
```

- `title` - название интерфейса, не может быть пустым, максимальная длина - 42 символа;
- `enabled` - если `true`, то интерфейс включен, `false` - выключен;
- `comment` - комментарий, может быть пустым;
- `addresses` - список адресов в формате `IP/prefix`;
- `gateway` - IP-адрес шлюза, может быть равен `null`;
- `parent_interface` - алиас родительского интерфейса, его IP-адрес будет источником туннеля;
- `osdevname` - название существующего или планируемого сетевого интерфейса в ядре (например, `Gre00000001`). Значение создается автоматически, является уникальным и **доступно только для чтения**;

- `server` - IP-адрес или доменное имя устройства, к которому осуществляется подключение;
- `zone` - алиас зоны. Может быть `null`, если не назначен.

Ответ на успешный запрос: 200 OK

Удаление туннельного интерфейса:

```
DELETE /network/tunnels/<id туннельного интерфейса>
```

Ответ на успешный запрос: 200 OK

44.4 VCE-интерфейсы

Получение списка всех сетевых интерфейсов, пробрасываемых в VCE:

```
GET /network/vce_conns
```

Ответ на успешный запрос:

```
[
  {
    "id": "string",
    "title": "string",
    "vce_id": "string",
    "mac": "string",
    "vlan_tag": "null" | "integer",
    "comment": "string"
  },
  ...
]
```

- `id` - идентификатор интерфейса;
- `title` - название интерфейса, не может быть пустым;
- `vce_id` - идентификатор VCE, для которого создан интерфейс;
- `mac` - MAC-адрес сетевой карты в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть `null`, если пробрасывается сетевой интерфейс целиком;
- `comment` - комментарий, может быть пустым.

Важно: Изменяемыми являются только поля `title` и `comment`.

Создание пробрасываемого в VCE интерфейса:

```
POST /network/vce_conns
```

Json-тело запроса:

```
{
    "title": "string",
    "vce_id": "string",
    "mac": "string",
    "vlan_tag": "null" | "integer",
    "comment": "string"
}
```

- `title` - название интерфейса, не может быть пустым;
- `vce_id` - идентификатор VCE, для которого создан интерфейс;

- `mac` - MAC-адрес сетевой карты в формате `11:22:33:44:55:66`, все буквы в нижнем регистре;
- `vlan_tag` - тэг VLAN, число от 1 до 4095 (включительно). Может быть `null`, если пробрасывается сетевой интерфейс целиком;
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор созданного интерфейса.

Редактирование пробрасываемого в VCE интерфейса:

```
PATCH /network/vce_conns/<id пробрасываемого интерфейса>
```

Json-тело запроса:

```
{
    "title": "string",
    "comment": "string"
}
```

- `title` - название интерфейса, не может быть пустым;
- `comment` - комментарий, может быть пустым.

Поля опциональны, можно передавать любое из них отдельно или оба сразу.

Ответ на успешный запрос: 200 OK

Удаление пробрасываемого в VCE интерфейса:

```
DELETE /network/vce_conns/<id пробрасываемого интерфейса>
```

Ответ на успешный запрос: 200 OK

45. DHCP-сервер

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Получение статуса службы DHCP-сервера:

```
GET /dhcp_server/status
```

Ответ на успешный запрос:

```
[
  {
      "name": "string",
      "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
      "msg": [ "string" ]
  }
]
```

- `name` - название службы;

- `status` - текущее состояние службы;
- `msg` - список строк, подробно описывающих состояние службы.

45.1 Настройки

Получение настроек:

```
GET /dhcp_server/settings
```

Пример ответа на успешный запрос:

```
[
  {
      "enabled": "boolean",
      "interface": "string",
      "relay": {
          "external_servers": [
              "string"
          ]
      },
      "server": null,
      "id": "string"
    },
  {
      "enabled": "boolean",
      "interface": "string",
      "relay": null,
      "server": {
          "dns": [ "string" ],
          "domain": "string",
          "gateway": "string",
          "lease_time": "integer",
          "options": [
              {
                  "comment": "string",
                  "enabled": "boolean",
                  "forced": "boolean",
                  "option": "string"
                }
            ],
          "ranges": [ "string" ],
          "routes": [ {
                  "destination": "string",
                  "gateway": "string"
                } ],
          "tftp_filename": "string",
          "tftp_server": "string",
          "wins": [ "string" ],
          "wpad_enabled": "boolean"
        },
      "id": "string"
    },
    ...
]
```

- `id` - идентификатор настройки;
- `enabled` - если `true`, то настройка включена, `false` - выключена;

- `interface` - интерфейс Ideco NGFW;
- `relay` - режим работы (если активен `server`, должен быть `null`):
  - `external_servers` - IP-адрес внешнего DHCP-сервера.
- `server` - режим работы (если активен `relay`, должен быть `null`):
  - `dns` - поля DNS-1 и DNS-2 в веб-интерфейсе. Если не задано значение в поле DNS-1 или DNS-2, то DNS-сервером для всех сетевых устройств локальной сети будет являться Ideco NGFW;
  - `domain` - DNS-суффикс;
  - `gateway` - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса;
  - `lease_time` - время аренды (в минутах);
  - `options` - опции dnsmasq (`comment` - комментарий, может быть пустым; `enabled` - включена или отключена опция; `forced` - принудительная отправка опции клиенту; `option` - значение опции);
  - `ranges` - диапазон IP-адресов для выдачи;
  - `routes` - статические маршруты (`destination` - хост, `gateway` - шлюз);
  - `tftp_filename` - имя файла для загрузки по TFTP;
  - `tftp_server` - IP-адрес TFTP-сервера для настройки загрузки образа по сети;
  - `wins` - IP-адрес WINS-сервера;
  - `wpad_enabled` - включение протокола автоматической настройки прокси. Для работы WPAD необходимо разрешить прямые подключения к прокси.

Создание настроек:

```
POST /dhcp_server/settings
```

Json-тело запроса для режима сервера:

```
{
      "enabled": "boolean",
      "interface": "string",
      "relay": null,
      "server": {
          "dns": [ "string" ],
          "domain": "string",
          "gateway": "string",
          "lease_time": "integer",
          "options": [
              {
                  "comment": "string",
                  "enabled": "boolean",
                  "forced": "boolean",
                  "option": "string"
              }
          ],
          "ranges": [ "string" ],
          "routes": [ {
                  "destination": "string",
                  "gateway": "string"
              } ],
          "tftp_filename": "string",
          "tftp_server": "string",
          "wins": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "wpad_enabled": "boolean"
    }
}
```

- `enabled` - если `true`, то настройка включена, `false` - выключена;
- `interface` - интерфейс Ideco NGFW;
- `relay` - режим работы (если активен `server`, должен быть `null`):
  - `external_servers` - IP-адрес внешнего DHCP-сервера.
- `server` - режим работы (если активен `relay`, должен быть `null`):
  - `dns` - поля DNS-1 и DNS-2 в веб-интерфейсе. Если не задано значение в поле DNS-1 или DNS-2, то DNS-сервером для всех сетевых устройств локальной сети будет являться Ideco NGFW;
  - `domain` - DNS-суффикс;
  - `gateway` - шлюз для направления трафика по умолчанию. Если поле не заполнено, шлюзом будет выступать IP-адрес выбранного интерфейса;
  - `lease_time` - время аренды (в минутах);
  - `options` - опции dnsmasq (`comment` - комментарий, может быть пустым; `enabled` - включена или отключена опция; `forced` - принудительная отправка опции клиенту; `option` - значение опции);
  - `ranges` - диапазон IP-адресов для выдачи;
  - `routes` - статические маршруты (`destination` - хост, `gateway` - шлюз);
  - `tftp_filename` - имя файла для загрузки по TFTP;
  - `tftp_server` - IP-адрес TFTP-сервера для настройки загрузки образа по сети;
  - `wins` - IP-адрес WINS-сервера;
  - `wpad_enabled` - включение протокола автоматической настройки прокси. Для работы WPAD необходимо разрешить прямые подключения к прокси.

Json-тело запроса для режима релея:

```
{
    "enabled": "boolean",
    "interface": "string",
    "relay": {
        "external_servers": [
            "string"
        ]
    },
    "server": null
}
```

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор настройки.

Изменение настроек:

```
PATCH /dhcp_server/20250424123235/docsUTM/settings/<id настройки>
```

Json-тело запроса - все или некоторые поля для создания настроек, например:

```
{
    "relay": {
        "external_servers": [
            "string"
        ]
    }
  }
```

- `relay` - режим работы (если активен `server`, должен быть `null`):
  - `external_servers` - IP-адрес внешнего DHCP-сервера.

Ответ на успешный запрос: 200 OK

Удаление настроек:

```
DELETE /dhcp_server/20250424123235/docsUTM/settings/<id настройки>
```

Ответ на успешный запрос: 200 OK

45.2 Привязка IP к MAC

Получение статических привязок:

```
GET /dhcp_server/static_leases
```

Пример ответа на успешный запрос:

```
[
  {
      "comment": "",
      "enabled": true,
      "ip_address": "192.168.0.40",
      "mac": "50:46:5d:6e:8c:20",
      "id": "3e4827dd-5e0c-4932-98b1-fa2d9826b0ce"
  },
  ...
]
```

- `ip_address` - IP-адрес;
- `mac` - MAC-адрес;
- `enabled` - если `true`, то запись включена, `false` - выключена;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов;
- `id` - идентификатор статической привязки.

Создание статической привязки:

```
POST /dhcp_server/static_leases
```

Json-тело запроса:

```
{
    "comment": "string",
    "enabled": "boolean",
    "ip_address": "string",
    "mac": "string"
  }
```

- `ip_address` - IP-адрес;
- `mac` - MAC-адрес;
- `enabled` - если `true`, то запись включена, `false` - выключена;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Будьте внимательны при согласовании настроек клиентских устройств и DHCP-сервера на Ideco NGFW. Некоторые устройства предоставляют MAC-адрес с разделенными с помощью дефиса октетами (01-02-03-04-05-06). В настройках Ideco NGFW октеты MAC-адреса разделяются только двоеточиями (01:02:03:04:05:06).

Ответ на успешный запрос:

```
{
  "id": "string"
}
```

- `id` - идентификатор статической привязки.

Редактирование статической привязки:

```
PATCH /dhcp_server/static_leases/<id статической привязки>
```

Json-тело запроса (все или некоторые поля):

```
{
    "comment": "string",
    "enabled": "boolean",
    "ip_address": "string",
    "mac": "string"
  }
```

- `ip_address` - IP-адрес;
- `mac` - MAC-адрес;
- `enabled` - если `true`, то запись включена, `false` - выключена;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление статической привязки:

```
DELETE /dhcp_server/static_leases/<id статической привязки>
```

Ответ на успешный запрос: 200 OK

46. DNS-сервер

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Получение статуса службы DNS:

```
GET /dns/status
```

Ответ на успешный запрос:

```
[
  {
    "name": "string",
    "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
    "msg": [ "string" ]
  },
  ...
]
```

- `name` - название службы;
- `status` - состояние службы;
- `msg` - список ошибок, может быть пустым.

46.1 Настройки

Получение настроек DNS-сервера:

```
GET /dns/settings
```

Ответ на успешный запрос:

```
{
        "intercept_enabled": "boolean"
}
```

- `intercept_enabled` - перехватывать DNS-запросы на серверы в интернет.

Включение/выключение DNS-сервера:

```
PUT /dns/settings
```

Json-тело запроса:

```
{
    "intercept_enabled": "boolean"
}
```

- `intercept_enabled` - перехватывать DNS-запросы на серверы в интернет.

Ответ на успешный запрос: 200 OK

Включение/выключение переадресации DNS для безопасного поиска:

46.1.1 Получение настроек:

```
GET /dns/safesearch
```

Ответ на успешный запрос:

```
{
        "enabled": "boolean"
}
```

- `enabled` - переадресовывать DNS-запросы на безопасные домены поиска Google, Yandex, YouTube, Bing, DuckDuckGo, Qwant и Pixabay.

46.1.2 Изменение настроек:

```
PUT /dns/safesearch
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - переадресовывать DNS-запросы на безопасные домены поиска Google, Yandex, YouTube, Bing, DuckDuckGo, Qwant и Pixabay.

Ответ на успешный запрос: 200 OK

46.2 Управление внешними DNS-серверами

Получение списка:

```
GET /dns/zones/root
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "enabled": "boolean",
    "type": "ip" | "interface",
    "object": "string",
    "comment": "string"
},
...
]
```

- `id` - идентификатор объекта;
- `enabled` - если `true`, то элемент включен, `false` - выключен;
- `type` - принимает два значения:
  - `ip` - IP-адрес DNS-сервера, заданного вручную;
  - `interface` - идентификатор алиаса подключения к провайдеру (DNS-серверы, выданные подключению). Тип алиаса - `isp`.
- `object` - IP-адрес, если тип `ip`, или идентификатор алиаса подключения к провайдеру, если тип `interface`;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Добавление корневого DNS-сервера:

```
POST /dns/zones/root
```

Json-тело запроса:

```
{
    "enabled": "boolean",
    "type": "ip" | "interface",
    "object": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "comment": "string"
}
```

- `enabled` - если `true`, то элемент включен, `false` - выключен;
- `type` - принимает два значения:
  - `ip` - IP-адрес DNS-сервера, заданного вручную;
  - `interface` - идентификатор алиаса подключения к провайдеру (DNS-серверы, выданные подключению). Тип алиаса - `isp`.
- `object` - IP-адрес, если тип `ip`, или идентификатор алиаса подключения к провайдеру, если тип `interface`;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор DNS-сервера.

Редактирование корневого DNS-сервера:

```
PATCH /dns/zones/root/<id DNS-сервера>
```

Json-тело запроса (все или некоторые поля):

```
{
    "enabled": "boolean",
    "type": "ip" | "interface",
    "object": "string",
    "comment": "string"
}
```

- `enabled` - если `true`, то элемент включен, `false` - выключен;
- `type` - принимает два значения:
  - `ip` - IP-адрес DNS-сервера, заданного вручную;
  - `interface` - идентификатор алиаса подключения к провайдеру (DNS-серверы, выданные подключению). Тип алиаса - `isp`.
- `object` - IP-адрес, если тип `ip`, или идентификатор алиаса подключения к провайдеру, если тип `interface`;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление корневого DNS-сервера:

```
DELETE /dns/zones/root/<id DNS-сервера>
```

Ответ на успешный запрос: 200 OK

46.3 Управление Forward-зонами

Получение списка:

```
GET /dns/zones/forward
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "name": "string",
    "enabled": "boolean",
    "servers": [ "string" ],
    "comment": "string",
},
    ...
]
```

- `id` - идентификатор объекта;
- `name` - название зоны;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `servers` - список IP-адресов DNS-серверов, заданных вручную;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Добавление Forward-зоны:

```
POST /dns/zones/forward
```

Json-тело запроса:

```
{
    "name": "string",
    "enabled": "boolean",
    "servers": [ "string" ],
    "comment": "string"
}
```

- `name` - название зоны;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `servers` - список IP-адресов DNS-серверов, заданных вручную;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор Forward-зоны.

Редактирование Forward-зоны:

```
PATCH /dns/zones/forward/<id Forward-зоны>
```

Json-тело запроса (все или некоторые поля):

```
{
    "name": "string",
    "enabled": "boolean",
    "servers": [ "string" ],
    "comment": "string"
}
```

- `name` - название зоны;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `servers` - список IP-адресов DNS-серверов, заданных вручную;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление Forward-зоны:

```
DELETE /dns/zones/forward/<id Forward-зоны>
```

Ответ на успешный запрос: 200 OK

46.4 Управление Master-зонами

Получение списка:

```
GET /dns/zones/master
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "name": "string",
    "enabled": "boolean",
    "config": "string",
    "comment": "string",
},
    ...
]
```

- `id` - идентификатор объекта;
- `name` - уникальное название зоны, имеет вид домена example.com;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `config` - текст с параметрами зоны, не может быть пустым. Максимальная длина - 10000 символов;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Подробнее о формате записей для настройки Master-зоны - в статье *Master-зоны*.

Добавление Master-зоны:

```
POST /dns/zones/master
```

Json-тело запроса:

```
{
    "name": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "enabled": "boolean",
    "config": "string",
    "comment": "string",
}
```

- `name` - уникальное название зоны, имеет вид домена example.com;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `config` - текст с параметрами зоны, не может быть пустым. Максимальная длина - 10000 символов;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор Master-зоны.

Редактирование Master-зоны:

```
PATCH /dns/zones/master/<id Master-зоны>
```

Json-тело запроса (все или некоторые поля):

```
{
    "name": "string",
    "enabled": "boolean",
    "config": "string",
    "comment": "string",
}
```

- `name` - уникальное название зоны, имеет вид домена example.com;
- `enabled` - если `true`, то зона включена, `false` - выключена;
- `config` - текст с параметрами зоны, не может быть пустым. Максимальная длина - 10000 символов;
- `comment` - комментарий, может быть пустым, максимальная длина - 255 символов.

Ответ на успешный запрос: 200 OK

Удаление Master-зоны:

```
DELETE /dns/zones/master/<id Master-зоны>
```

Ответ на успешный запрос: 200 OK

46.5 DDNS

Подсказка: DDNS в Ideco NGFW реализован через интеграцию с хостингом RU-CENTER. Перед настройкой DDNS зарегистрируйтесь на сайте RU-CENTER и приобретите DNS-хостинг.

Подробнее о DDNS - в *статье*.

Получение состояния:

```
GET /dns/ddns/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние DDNS: `true` - включено, `false` - выключено.

Включение/выключение DDNS:

```
PUT /dns/ddns/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - состояние DDNS: `true` - включено, `false` - выключено.

Ответ на успешный запрос: 200 OK

Получение настроек:

```
GET /dns/ddns
```

Ответ на успешный запрос:

```
{
    "domain": "string",
    "service_login": "string",
    "service_password": "string"
}
```

- `domain` - домен, который администратор хочет видеть в адресной строке. Формат: `domain.com` (без `https://` и `www`);
- `service_login` - логин для доступа к API сервиса DDNS;
- `service_password` - пароль для доступа к API сервиса DDNS, до 42 символов.

Изменение настроек:

```
PUT /dns/ddns
```

Json-тело запроса:

```
{
    "domain": "string",
    "service_login": "string",
    "service_password": "string"
}
```

- `domain` - домен, который администратор хочет видеть в адресной строке. Формат: `domain.com` (без `https://` и `www`);
- `service_login` - логин для доступа к API сервиса DDNS;
- `service_password` - пароль для доступа к API сервиса DDNS, до 42 символов.

Ответ на успешный запрос: 200 OK

47. Настройка удаленной передачи системных логов

Получение статуса работы службы:

```
GET /logs_backend/remote_syslog/status
```

Ответ на успешный запрос:

```
[
    {
        "name": "string",
        "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
        "msg": [ "string" ]
    },
    ...
]
```

- `name` - название модуля;
- `status` - статус;
- `msg` - список сообщений, объясняющий текущее состояние.

47.1 Общие настройки

Включение/выключение службы:

Проверка состояния:

```
GET /logs_backend/remote_syslog/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `msg` - `true` для включения, `false` для выключения.

Включение/выключение

```
PUT /logs_backend/remote_syslog/state
```

Json-тело запроса:

```
{
  "enabled": "boolean"
}
```

Ответ на успешный запрос: 200 OK

Получение настроек удаленной передачи системных логов:

```
GET /logs_backend/remote_syslog
```

Ответ на успешный запрос:

```
{
  "host": "string",
  "port": "integer",
  "protocol": "tcp" | "udp",
  "format": "syslog" | "cef"
}
```

- `host` - IP-адрес сервера;
- `port` - порт;
- `protocol` - протокол, допустимые значения: `tcp` или `udp`;
- `format` - формат, допустимые значения: `syslog` или `cef`.

Изменение настроек удаленной передачи системных логов:

```
PATCH /logs_backend/remote_syslog
```

Json-тело запроса:

```
{
  "host": "string" | "null",
  "port": "integer" | "null",
  "protocol": "tcp" | "udp",
  "format": "syslog" | "cef",
}
```

- `host` - IP-адрес сервера;
- `port` - порт;
- `protocol` - протокол, допустимые значения: `tcp` или `udp`;
- `format` - формат, допустимые значения: `syslog` или `cef`.

Пустые значения «» не допускаются.

Ответ на успешный запрос: 200 OK

Получение данных о логировании для таблицы:

```
GET /logs_backend/logs?<GET-параметры, разделенные знаком &>
```

Список GET-параметров, которые не являются обязательными:

- `limit: integer` - ограничение на количество записей, выбираемых из базы данных;
- `offset: integer` - количество строк, которые необходимо пропустить перед выводом записей указанных в `limit`;
- `sort: [Sort]` - Список параметров для сортировки данных. Сортировка производится в прямом порядке следования в массиве;
- `filter: [Filter]` - Список параметров для фильтрации данных. Фильтры применяются в прямом порядке следования в массиве, с логикой `and` между объектами `Filter`;
- `search: Search` - объект с параметрами поиска подстроки в данных;
- `last_reboot_only: bool` - параметр типа `bool` со значениями: `false` - выводить все записи лога, `true` - только записи после последней загрузки;
- `format_type:` - формат возвращаемых данных:
  - `CSV` - CSV-файл;
  - `JSON` - тип по умолчанию.

Объект Sort:

```
{
  "field": "string",
  "direction": "asc" | "desc"
}
```

- `field` - столбец, по которому производится сортировка;
- `direction` - направление сортировки: `asc` - по возрастанию, `desc` - по убыванию.

Объект Filter:

```
{
  "items": [
      {
        "column_name": "string",
        "operator": "contains" | "not_contains" | "equals" | "not_equals" | "greater"␣
↪| "greater_equal" | "less" | "less_equal",
        "value": ["string" | "integer" | "boolean"]
      },
    ],
  "link_operator": "and" | "or"
}
```

- `items` - массив фильтров FilterItem:
  - `column_name` - поле для фильтрации;
  - `operator` - одно из значений:
    - `contains` - содержит подстроку (без учета регистра);
    - `not_contains` - не содержит подстроку (без учета регистра);
    - `equals` - равно;
    - `not_equals` - не равно;
    - `greater` - больше, в `values` передаётся массив, содержащий только одно значение;
    - `greater_equal` - больше или равно, в `values` передается массив, содержащий только одно значение;
    - `less` - меньше, в `values` передаётся массив, содержащий только одно значение;
    - `less_equal` - меньше или равно, в `values` передается массив, содержащий только одно значение.
  - `value` - массив значений фильтра. Максимальное количество передаваемых в массиве значений - 255. Данные отбираются по логике `or`.
- `link_operator` - логика наложения фильтров items.

Объект Search:

```
{
  "text": "string",
  "columns": ["string"]
}
```

- `text` - искомая строка;
- `columns` - набор полей, по которым ведется поиск.

Ответ на успешный запрос:

```
{
  "meta": [
    {
      "name": "string",
      "type": "string"
    }
  ],
  "data": [
    {
      "id": "string",
      "date_time": "integer",
      "microseconds": "integer",
      "priority": "integer",
      "message": "string",
      "syslog_id": "string",
      "unit": "string"
    }
  ],
  "rows": "integer",
  "rows_before_limit_at_least": "integer"
}
```

- `meta` - массив метаданных, описывающих поля запроса:
  - `name` - имя поля данных;
  - `type` - тип данных.
- `data` - массив, содержащий `Log` - объект, представляющий собой данные, соответствующие одной строке таблицы:
  - `id` - уникальный идентификатор строки;
  - `date_time` - время возникновения события в формате YYYYMMDDhhmmss;
  - `microseconds` - микросекунды во времени возникновения события (0. . . 999999);
  - `priority` - число от 0 до 7:
    - `0` - LOG_EMERG;
    - `1` - LOG_ALERT;
    - `2` - LOG_CRIT;
    - `3` - LOG_ERR;
    - `4` - LOG_WARNING;
    - `5` - LOG_NOTICE;
    - `6` - LOG_INFO;
    - `7` - LOG_DEBUG.
  - `message` - сообщение логирования;
  - `syslog_id` - название исполняемой программы;
  - `unit` - название сервиса, сообщение которого было сохранено в журнале.
- `rows` - количество строк `Log`;
- `rows_before_limit_at_least` - количество строк `Log`, которое вернет запрос, если использовать ограничение на количество записей из базы данных (GET-параметры `limit` или `offset`).

48. Центральная консоль

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

48.1 Настройки Центральной консоли в Ideco NGFW

Получение настроек Ideco Center:

```
GET /central_console/settings
```

Ответ на успешный запрос:

```
{
    "cc_server": "string" | "null",
    "last_connect": "integer" | "null",
    "last_sync": "integer" | "null",
    "root_ca": "string" | "null"
}
```

- `cc_server` - доменное имя или IP-адрес центральной консоли;
- `last_connect` - timestamp последней успешной синхронизации данных;
- `last_sync` - timestamp;
- `root_ca` - корневой сертификат в формате PEM.

Изменение настроек Ideco Center:

```
PATCH /central_console/settings
```

Json-тело запроса:

```
{
  "cc_server": "string" | "null"
}
```

Загрузка корневого сертификата Ideco Center на NGFW:

```
POST /central_console/root_ca
```

В тело запроса поместите содержимое корневого сертификата, скачанного в Ideco Center. Для этого откройте сертификат в текстовом редакторе и скопируйте текст.

Удаление корневого сертификата Ideco Center:

```
DELETE /central_console/root_ca
```

Ответ на успешный запрос: 200 OK

Отключение NGFW от Ideco Center:

```
DELETE /central_console/settings
```

Ответ на успешный запрос: 200 OK

48.2 API Ideco Center

Получение статуса службы:

```
GET /servers/status
```

Ответ на успешный запрос:

```
{
    "name": "string",
    "status": "active" | "activating" | "deactivating" | "failed" | "inactive" |
↪"reloading",
    "msg": [ "string" ]
}
```

- `name` - название службы;
- `status` - текущее состояние службы;
- `msg` - список строк, описывающих состояние службы.

48.2.1 Общие настройки

Получение общих настроек:

```
GET /servers/setting
```

Ответ на успешный запрос:

```
{
    "domain": "string" | "null"
}
```

- `domain` - внешний адрес Ideco Center (IP-адрес или доменное имя).

Изменение общих настроек:

```
PUT /servers/setting
```

Json-тело запроса:

```
{
    "domain": "string" | "null"
}
```

- `domain` - внешний адрес Ideco Center (IP-адрес или доменное имя).

Ответ на успешный запрос: 200 OK

Получение настройки включенности синхронизации правил:

```
GET /servers/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - если `true`, то синхронизация правил включена, `false` - выключена.

Включение/выключение синхронизации правил:

```
PUT /servers/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения синхронизации правил, `false` для выключения.

Ответ на успешный запрос: 200 OK

48.2.2 Группировка серверов

Получение списка групп серверов в Ideco Center:

```
GET /servers/groups
```

Пример ответа на успешный запрос:

```
[
    {
        "comment": "",
        "name": "Группа 1",
        "parent_id": "f3ffde22-a562-4f43-ac04-c40fcec6a88c",
        "id": "e37ec0bb-fc27-406f-bd24-d0e89200561d"
    },
    {
        "comment": "",
        "name": "Корневая группа",
        "parent_id": null,
        "id": "f3ffde22-a562-4f43-ac04-c40fcec6a88c"
    },
    ...
]
```

- `id` - идентификатор группы;
- `comment` - комментарий, может быть пустым;
- `name` - название группы серверов;
- `parent_id` - идентификатор родительской группы серверов.

Создание группы серверов:

```
POST /servers/groups
```

Json-тело запроса:

```
{
    "comment": "string",
    "name": "string",
    "parent_id": "string"
}
```

- `name` - название группы;
- `parent_id` - идентификатор родительской группы (если группа входит в Корневую группу, идентификатор Корневой группы);

- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор созданной группы.

Редактирование группы серверов:

```
PATCH /servers/groups/<id группы серверов>
```

Json-тело запроса:

```
{
    "comment": "string",
    "name": "string",
    "parent_id": "string"
}
```

- `name` - название группы;
- `parent_id` - идентификатор родительской группы (если группа входит в Корневую группу, идентификатор Корневой группы);
- `comment` - комментарий, может быть пустым.

Ответ на успешный запрос: 200 OK

Удаление группы серверов:

```
DELETE /servers/groups/<id группы серверов>
```

Ответ на успешный запрос: 200 OK

48.2.3 Управление подключенными серверами

Получение списка подключенных серверов:

```
GET /servers/servers
```

Ответ на успешный запрос:

```
[
    {
    "id": "string",
    "parent_id": "string",
    "version": {
      "major": "integer",
      "minor": "integer",
      "build": "integer",
      "timestamp": "integer",
      "vendor": "Ideco",
      "product": "UTM",
      "kind": "FSTEK" | "VPP" | "STANDARD" | "BPF",
      "release_type": "release" | "beta" | "devel"
   },
    "cl_tunnel_addr": "string",
    "title": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "approved": "boolean",
    "last_sync": "integer" | "null",
    "last_connect": "integer",
    "utm_login_secret": "string",
    "comment": "string",
  },
  ...
]
```

- `id` - идентификатор сервера;
- `parent_id` - идентификатор группы, в которую входит сервер;
- `version` - версия сервера:
  - `major` - мажорный номер версии;
  - `minor` - минорный номер версии;
  - `build` - номер сборки;
  - `timestamp` - время выхода версии;
  - `vendor` - вендор («Ideco»);
  - `product` - код продукта;
  - `kind` - вид продукта;
  - `release_type` - тип релиза.
- `cl_tunnel_addr` - IPv6-адрес сервера внутри WireGuard-туннеля;
- `title` - название сервера;
- `approved` - флаг, означающий, подтверждено ли подключение сервера в Ideco Center;
- `last_sync` - timestamp последней успешной синхронизации данных;
- `last_connect` - timestamp последнего успешного подключения;
- `utm_login_secret` - секретное значение для отправки в URL авторизации Ideco Center в Ideco NGFW;
- `version_diff` - разница мажорных версий Ideco Center и NGFW. Если значение равно нулю - мажор одинаковый, больше нуля - версия Ideco Center выше, меньше нуля - версия NGFW выше.
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым.

Перемещение подключенных серверов между группами/подтверждение подключения сервера к Ideco Center:

```
PATCH /servers/servers/<id сервера>
```

Json-тело запроса:

```
{
    "parent_id": "string",
    "approved": "boolean"
}
```

- `parent_id` - идентификатор группы, в которую входит сервер;
- `approved` - флаг, означающий, подтверждено ли подключение сервера в Ideco Center.

Ответ на успешный запрос: 200 OK

При добавлении нового сервера ему автоматически присваивается parent_id Корневой группы.

После подтверждения подключения сервера (установки approved=true) менять это свойство нельзя (для удаления сервера вызывается метод DELETE)

Удаление сервера из Ideco Center:

```
DELETE /servers/servers/<id сервера>
```

Ответ на успешный запрос: 200 OK

48.2.4 Управление правилами трафика Ideco Center

Контент-фильтр

Получение списка категорий (предустановленных и пользовательских):

```
GET /content-filter/categories
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "type": "string",
        "name": "string",
        "comment": "string"
    },
    ...
]
```

- `id` - номер категории в формате `users.id.1` или `extended.id.1`;
- `type` - тип категории:
  - `users` - пользовательские категории;
  - `extended` - расширенные категории (SkyDNS);
  - `files` - категории для файлов;
  - `special` - специальные предопределенные категории (Прямое обращение по IP, Все категоризированные запросы, Все некатегоризированные запросы, Все запросы).
  - `other` - остальные категории.
- `name` - имя категории;
- `comment` - описание категории.

Получение списка пользовательских категорий:

```
GET /content-filter/users_categories
```

Ответ на успешный запрос:

```
[
    {
        "id": "string",
        "name": "string",
        "comment": "string",
        "urls": [ "string" ]
    },
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    ...
]
```

- `id` - номер категории в формате `users.id.1`;
- `name` - название категории, не пустая строка;
- `comment` - комментарий, может быть пустым;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Создание пользовательской категории:

```
POST /content-filter/users_categories
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий, может быть пустым;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

Редактирование пользовательских категорий:

```
PUT /content-filter/users_categories/<id категории>
```

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "urls": [ "string" ]
}
```

- `name` - название категории, не пустая строка;
- `comment` - комментарий, может быть пустым;
- `urls` - список адресов. Полный путь до страницы или только доменное имя, любое количество любых символов.

Ответ на успешный запрос:

```
{
    "id": "string",
    "name": "string",
    "comment": "string",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "urls": [ "string" ]
}
```

Получение списка правил:

- `GET /content-filter/rules/before?groups=[UUID1,UUID2]` - начальные правила;
- `GET /content-filter/rules/after?groups=[UUID1,UUID2]` - конечные правила.
  - `UUID1` - идентификатор группы серверов в Центральной консоли (`id`).

```
[
    {
        "id": "integer",
        "parent_id": "string",
        "name": "string",
        "comment": "string",
        "aliases": [ "string" ],
        "categories": [ "string" ],
        "access": "allow" | "deny" | "bump" | "redirect",
        "redirect_url": "string" | "null",
        "enabled": "boolean",
        "timetable": [ "string" ]
    },
    ...
]
```

- `id` - идентификатор правила;
- `parent_id` - идентификатор группы серверов, к которой применяется правило;
- `name` - название правила, не пустая строка;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым;
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`;
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия.

Создание правила:

- `POST /content-filter/rules/before?anchor_item_id=123&insert_after={true|false}` - создание начального правила;
- `POST /content-filter/rules/after?anchor_item_id=123&insert_after={true|false}` - создание конечного правила.

Json-тело запроса:

```
{
    "parent_id": "string",
    "name": "string",
    "comment": "string",
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "access": "allow" | "deny" | "bump" | "redirect",
    "redirect_url": "string" | "null",
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `parent_id` - идентификатор группы серверов, к которой применяется правило;
- `name` - название правила, не пустая строка;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым;
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`;
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Редактирование правила:

- `PUT /content-filter/rules/before/<id правила>` - изменение начального правила;
- `PUT /content-filter/rules/after/<id правила>` - изменение конечного правила.

Json-тело запроса:

```
{
    "name": "string",
    "comment": "string",
    "parent_id": "string",
    "aliases": [ "string" ],
    "categories": [ "string" ],
    "access": "allow" | "deny" | "bump" | "redirect",
    "redirect_url": "string" | "null",
    "enabled": "boolean",
    "timetable": [ "string" ]
}
```

- `name` - название правила, не пустая строка;
- `comment` - комментарий, максимальная длина - 255 символов, может быть пустым;
- `parent_id` - идентификатор группы серверов, к которой применяется правило;
- `aliases` - список идентификаторов алиасов (поле Применяется для);
- `categories` - список идентификаторов категорий сайтов;
- `access` - действие, которое необходимо выполнить в правиле:
  - `allow` - разрешить данный запрос;
  - `deny` - запретить запрос и показать страницу блокировки;
  - `bump` - расшифровать запрос;
  - `redirect` - перенаправить запрос на `redirect_url`;
- `redirect_url` - адрес, на который перенаправляются запросы. `String` при `access = redirect` и `null` при остальных вариантах `access`;
- `enabled` - правило включено (true) или выключено (false);
- `timetable` - время действия.

Ответ на успешный запрос: 200 OK

Важно! Чтобы переместить правило между группами серверов, измените его `parent_id`.

Перемещение правила:

- `PATCH /content-filter/rules/before/move` - перемещение начального правила;
- `PATCH /content-filter/rules/after/move` - перемещение конечного правила.

Json-тело запроса:

```
{
  "params": {
    "id": "integer",
    "anchor_item_id": "integer",
    "insert_after": "boolean"
  }
}
```

- `id` - идентификатор перемещаемого правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно поместить перемещаемое правило;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление правила:

- `DELETE /content-filter/rules/before/move` - перемещение начального правила;
- `DELETE /content-filter/rules/after/move` - перемещение конечного правила.

Ответ на успешный запрос: 200 OK

Файрвол

Получение настроек Файрвола:

```
GET /firewall/state
```

Ответ на успешный запрос:

```
{
    "enabled": "boolean"
}
```

- `enabled` - опция раздела **Файрвол**: `true` - включена, `false` - выключена.

Изменение настроек:

```
PUT /firewall/state
```

Json-тело запроса:

```
{
    "enabled": "boolean"
}
```

- `enabled` - `true` для включения, `false` для выключения.

Ответ на успешный запрос: 200 OK

Получение списка правил:

- `GET /firewall/rules/forward/before?groups=[UUID1, UUID2]` - начальные правила раздела FORWARD;
- `GET /firewall/rules/forward/after?groups=[UUID1, UUID2]` - конечные правила раздела FORWARD;
- `GET /firewall/rules/input/before?groups=[UUID1, UUID2]` - начальные правила раздела INPUT;
- `GET /firewall/rules/input/after?groups=[UUID1, UUID2]` - конечные правила раздела INPUT.

Ответ на успешный запрос:

```
[
   {
      "action": "accept" | "drop",
      "comment": "string",
      "destination_addresses": [ "string" ],
      "destination_addresses_negate": "boolean",
      "destination_ports": [ "string" ],
      "enabled": "boolean",
      "hip_profiles": ["string"],
      "incoming_interface": "string",
      "outgoing_interface": "string",
      "parent_id": "string",
      "protocol": "string",
      "source_addresses": [ "string" ],
      "source_addresses_negate": "boolean",
      "timetable": [ "string" ],
      "id": "integer"
    },
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    ...
]
```

- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.
- `comment` - комментарий, может быть пустым;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `enabled` - если `true`, то правило включено, `false` - выключено;
- `hip_profiles` - HIP-профили;
- `incoming_interface` - входящий интерфейс;
- `outgoing_interface` - исходящий интерфейс;
- `parent_id` - идентификатор группы, к которой применяется правило;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `timetable` - время действия;
- `id` - идентификатор правила.

Правила возвращаются в порядке их применения.

Создание правила:

- `POST /firewall/rules/forward/before?anchor_item_id=123&insert_after={true|false}` - начальное правило в раздел FORWARD;
- `POST /firewall/rules/forward/after?anchor_item_id=123&insert_after={true|false}` - конечное правило в раздел FORWARD;
- `POST /firewall/rules/input/before?anchor_item_id=123&insert_after={true|false}` - начальное правило в раздел INPUT;
- `POST /firewall/rules/input/after?anchor_item_id=123&insert_after={true|false}` - конечное правило в раздел INPUT.
  - `anchor_item_id` - идентификатор правила, ниже или выше которого нужно создать новое. Если отсутствует, то новое правило будет добавлено в конец таблицы;
  - `insert_after` - вставка до или после. Если значение `true` или отсутствует, то новое правило будет добавлено сразу после указанного в `anchor_item_id`. Если `false` - на месте указанного в `anchor_item_id`.

Json-тело запроса:

```
{
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "hip_profiles": [ "string" ],
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "drop"
}
```

- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа `f3ffde22-a562-4f43-ac04-c40fcec6a88c` (соответствует Корневой группе);
- `enabled` - включено (`true`) или выключено (`false`) правило;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

Ответ на успешный запрос:

```
{
    "id": "integer"
}
```

- `id` - идентификатор созданного правила.

Редактирование правила:

- `PUT /firewall/rules/forward/before/<id правила>` - раздел FORWARD, начальное правило;
- `PUT /firewall/rules/forward/after/<id правила>` - раздел FORWARD, конечное правило;
- `PUT /firewall/rules/input/before/<id правила>` - раздел INPUT, начальное правило;
- `PUT /firewall/rules/input/after/<id правила>` - раздел INPUT, конечное правило.

Json-тело запроса:

```
{
    "parent_id": "string",
    "enabled": "boolean",
    "protocol": "string",
    "source_addresses": [ "string" ],
    "source_addresses_negate": "boolean",
    "source_ports": [ "string" ],
    "incoming_interface": "string",
    "destination_addresses": [ "string" ],
    "destination_addresses_negate": "boolean",
    "destination_ports": [ "string" ],
    "outgoing_interface": "string",
    "hip_profiles": [ "string" ],
    "timetable": [ "string" ],
    "comment": "string",
    "action": "accept" | "drop"
}
```

- `parent_id` - идентификатор группы в Ideco Center, в которую входит сервер, или константа «f3ffde22-a562-4f43-ac04-c40fcec6a88c» (соответствует Корневой группе);
- `enabled` - включено (`true`) или выключено (`false`) правило;
- `protocol` - протокол;
- `source_addresses` - адрес источника;
- `source_addresses_negate` - инвертировать адрес источника;
- `source_ports` - порты источников, список идентификаторов алиасов;
- `incoming_interface` - зона источника;
- `destination_addresses` - адрес назначения;
- `destination_addresses_negate` - инвертировать адрес назначения;
- `destination_ports` - порты назначения;
- `outgoing_interface` - зона назначения;
- `hip_profiles` - HIP-профили;
- `timetable` - время действия;
- `comment` - комментарий, может быть пустым;
- `action` - действие:
  - `accept` - разрешить;
  - `drop` - запретить.

Ответ на успешный запрос: 200 OK

Важно! Чтобы переместить правило между группами серверов, измените его `parent_id`.

Перемещение правила:

- `PATCH /firewall/rules/forward/before/move` - раздел FORWARD, начальное правило;
- `PATCH /firewall/rules/forward/after/move` - раздел FORWARD, конечное правило;
- `PATCH /firewall/rules/input/before/move` - раздел INPUT, начальное правило;
- `PATCH /firewall/rules/input/after/move` - раздел INPUT, конечное правило.

Json-тело запроса:

```
{
  "params": {
    "id": "integer",
    "anchor_item_id": "integer",
    "insert_after": "boolean"
  }
}
```

- `id` - идентификатор перемещаемого правила;
- `anchor_item_id` - идентификатор правила, ниже или выше которого нужно поместить перемещаемое правило;
- `insert_after` - вставка до или после. Если `true`, то вставить правило сразу после указанного в `anchor_item_id`, если `false` - на месте указанного в `anchor_item_id`.

Ответ на успешный запрос: 200 OK

Удаление правила:

- `DELETE /firewall/rules/forward/before/<id правила>` - раздел FORWARD, начальное правило;
- `DELETE /firewall/rules/forward/after/<id правила>` - раздел FORWARD, конечное правило;
- `DELETE /firewall/rules/input/before/<id правила>` - раздел INPUT, начальное правило;
- `DELETE /firewall/rules/input/after/<id правила>` - раздел INPUT, конечное правило.

Ответ на успешный запрос: 200 OK

49. Бекапы

Подсказка: Длина комментариев (`comment`) при API-запросах ограничена 255 символами.

Получение настроек бекапов:

```
GET /backup/settings
```

Ответ на успешный запрос:

```
{
   "common": {
      "hour": "integer",
      "rotate": "weekly" | "monthly"
   },
   "ftp": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
   },
   "cifs": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
```

(continues on next page)

(продолжение с предыдущей страницы)

```
   }
}
```

- `common` - общие настройки бекапов:
  - `hour` - час, в который делается автоматический бекап, число от 0 до 23;
  - `rotate` - удалять бекапы старше недели (`weekly`) или месяца (`monthly`).
- `ftp` - настройки выгрузки бекапов на FTP:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.
- `cifs` - настройки выгрузки бекапов в общую папку CIFS:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.

Изменение настроек бекапов и настройка выгрузки на FTP-сервер или в общую папку CIFS:

```
PUT /backup/settings
```

Json-тело запроса:

```
{
   "common": {
      "hour": "integer",
      "rotate": "weekly | monthly"
   },
   "ftp": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
   },
   "cifs": {
      "enabled": "boolean",
      "server": "string",
      "login": "string",
      "password": "string",
      "remote_dir": "string"
   }
}
```

- `common` - общие настройки бекапов:
  - `hour` - час, в который делается автоматический бекап, число от 0 до 23;
  - `rotate` - удалять бекапы старше недели (`weekly`) или месяца (`monthly`).

- `ftp` - настройки выгрузки бекапов на FTP:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.
- `cifs` - настройки выгрузки бекапов в общую папку CIFS:
  - `enabled` - если `true`, то выгрузка включена, `false` - выключена;
  - `server` - адрес сервера, валидный домен или IP-адрес;
  - `login` - логин, не пустая строка;
  - `password` - пароль, не пустая строка, до 42 символов;
  - `remote_dir` - удаленный каталог, не пустая строка.

Ответ на успешный запрос: 200 OK

49.1 Управление бекапами

Создание бекапа:

```
POST /backup/backups
```

Json-тело запроса:

```
{
   "comment": "string"
}
```

- `comment` - комментарий, произвольный текст.

Ответ на успешный запрос:

```
{
    "id": "string"
}
```

- `id` - идентификатор бекапа.

Получение списка бекапов:

```
GET /backup/backups
```

Ответ на успешный запрос:

```
[
   {
      "id": "string",
      "version": {
         "major": "integer",
         "minor": "integer",
         "build": "integer",
         "timestamp": "integer",
         "vendor": "Ideco",
         "product": "UTM" | "CC",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "kind": "FSTEK" | "VPP" | "STANDARD" | "BPF",
        "release_type": "release" | "beta" | "devel"
     },
     "timestamp": "float",
     "comment": "string",
     "md5": "string",
     "size": "integer",
     "fast_restore_allowed": "boolean"
  }
...
]
```

- `id` - идентификатор бекапа;
- `version` - версия системы:
  - `major` - мажорный номер версии;
  - `minor` - минорный номер версии;
  - `build` - номер сборки;
  - `timestamp` - время выхода версии;
  - `vendor` - вендор («Ideco»);
  - `product` - код продукта;
  - `kind` - вид продукта;
  - `release_type` - тип релиза.
- `timestamp` - дата/время создания бекапа в формате UNIX timestamp;
- `comment` - комментарий, произвольный текст;
- `md5` - контрольная сумма файла бекапа (`data.tar`);
- `size` - размер бекапа, байт;
- `fast_restore_allowed` - можно ли выполнить быстрое восстановление из данного бекапа (версия идентична системной).

Скачивание бекапа:

```
GET /backup/download/<id бекапа>
```

Ответ на успешный запрос: тело бекапа.

Загрузка бекапа на Ideco NGFW из файла:

```
POST /backup/upload
```

Используйте стандартный POST-запрос на загрузку файла. Название поля в форме должно быть `backup_file`.

Ответ на успешный запрос:

```
{
   "id": "string"
}
```

- `id` - идентификатор бекапа.

Восстановление из бекапа:

```
POST /backup/backups/<id бекапа>/apply
```

Ответ на успешный запрос: 200 OK

Быстрое восстановление из бекапа:

```
POST /backup/backups/<id бекапа>/apply/fast
```

Ответ на успешный запрос: 200 OK

Удаление бекапа:

```
DELETE /backup/backups/<id бекапа>
```

Ответ на успешный запрос: 200 OK

50. Примеры использования

50.1 Редактирование пользовательской категории контент-фильтра

50.1.1 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 -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",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪"urls": []}, {"id": "users.id.3", "name": "Запрещенные для бухгалтеров", "comment":
↪"комментарий", "urls": ["https://yandex.ru"]}
```

3. Отредактируйте список URL:

```
curl -k -b /tmp/cookie -X PUT https://x.x.x.x:8443/content-filter/users_categories/
↪users.id.3 --data '{"name": "Запрещенные для бухгалтеров", "description":
↪"комментарий", "urls": ["https://yandex.ru", "https://wrong-url.com"]}'
```

Ответ на успешный запрос: 200 OK

Предупреждение: Запрос перезапишет ранее созданную пользовательскую категорию. Поэтому при выполнении запроса следует указать все URL (старые и новые - указанные при создании категории и те, которые хотите добавить).

Результат: Правило **Контент-фильтра**, которое использует эту пользовательскую категорию, будет запрещать пользователям переходить на сайты `https://yandex.ru` и `https://wrong-url.com/`

50.2 Создание правила FORWARD

50.2.1 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", "period": null}'
```

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, "hip_profiles": [], "incoming_interface": "any", "outgoing_
↪interface": "any", "protocol": "protocol.tcp", "source_addresses": ["address_list.
↪id.2"], "source_addresses_negate": false, "timetable": ["any"], "parent_id":
↪"f3ffde22-a562-4f43-ac04-c40fcec6a88c"}'
```

Значение `action`:

- `accept` - принять пакет;
- `drop` - отклонить пакет.

Ответ на успешный запрос:

```
{
    "id": 2
}
```

6. Отредактируйте созданное правило, указав время действия:

```
curl -k -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, "hip_profiles": [], "incoming_
↪interface": "any", "outgoing_interface": "any", "protocol": "protocol.tcp", "source_
↪addresses": ["address_list.id.2"], "source_addresses_negate": false, "timetable": [
↪"time_range.id.1"], "parent_id": "f3ffde22-a562-4f43-ac04-c40fcec6a88c"}'
```

Ответ на успешный запрос: 200 OK